時刻認証基盤技術実験装置
―統合化プラットフォームシステム―

セキュリティ評価報告書

平成 18 年 2 月 28 日

【セキュリティ評価報告書の構成】

統合化プラットフォームシステム

・TOE： NTA1

・TOE： TA1

・TOE： NTA2

・TOE： TA2

・TOE： CA

・TOE： VA

・TOE： TSA1

・TOE： TSA2

セキュリティ評価報告書

（TOE：NTA1 ）

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

本章では、TOE の機能概要、TOE 構成図、利用する暗号技術と暗号コンポーネント構成図、関与者、資産について記載する。

1. TOE の機能概要

1-1 TOE の機能

以下に、TOE を構成する機能の概要を示す。

(1)時刻配信機能（時刻配信プロトコルを含む）

TOE は、時刻配信プロトコル（認証連鎖方式*1）により時刻の配信・監査を行う機能を持つ。

(2)時刻受信機能

TOE は、NTP によって配信される時刻情報を受信するための機能を持つ。受信した時刻情報により、システム時刻が補正される。

(3)時刻管理機能

TOE の時刻配信機能・時刻受信機能やログ管理機能の時刻には、システム時刻が使用される。

(4)ログ管理機能

TOE は、TOE の動作記録、時刻配信記録、操作記録などをログとして保管することが可能である。ログは、署名を付与し保護することが可能である。

(5)鍵管理機能

TOE は、通信用(TLS)の秘密鍵および署名用の秘密鍵を管理する機能を持つ。

(6)証明書管理機能

TOE は、通信(TLS)および署名・検証に関わる証明書を管理する機能を持つ。

(7)設定管理機能

TOE は、TOE の機能に関わる設定を管理する機能を持つ。

(8)TOE 管理機能

TOE の設定・操作は、ブラウザから管理画面にアクセスして実施する。

＊１：ここでいう認証連鎖方式とは、PKI(Public Key Infrastructure)認証技術を利用し

て TA が時刻配信先の時計を特定すると同時に時刻の計測と配信を行い、その計測結果を時刻監査記録として更に時刻配信先の時計に連鎖していく方式。

1-2 TOE 構成図

以下に、統合化プラットフォームシステムにおいて TOE が使用される際のシステム構成図を示す。(強調表示されたコンポーネントは、評価対象外である。)

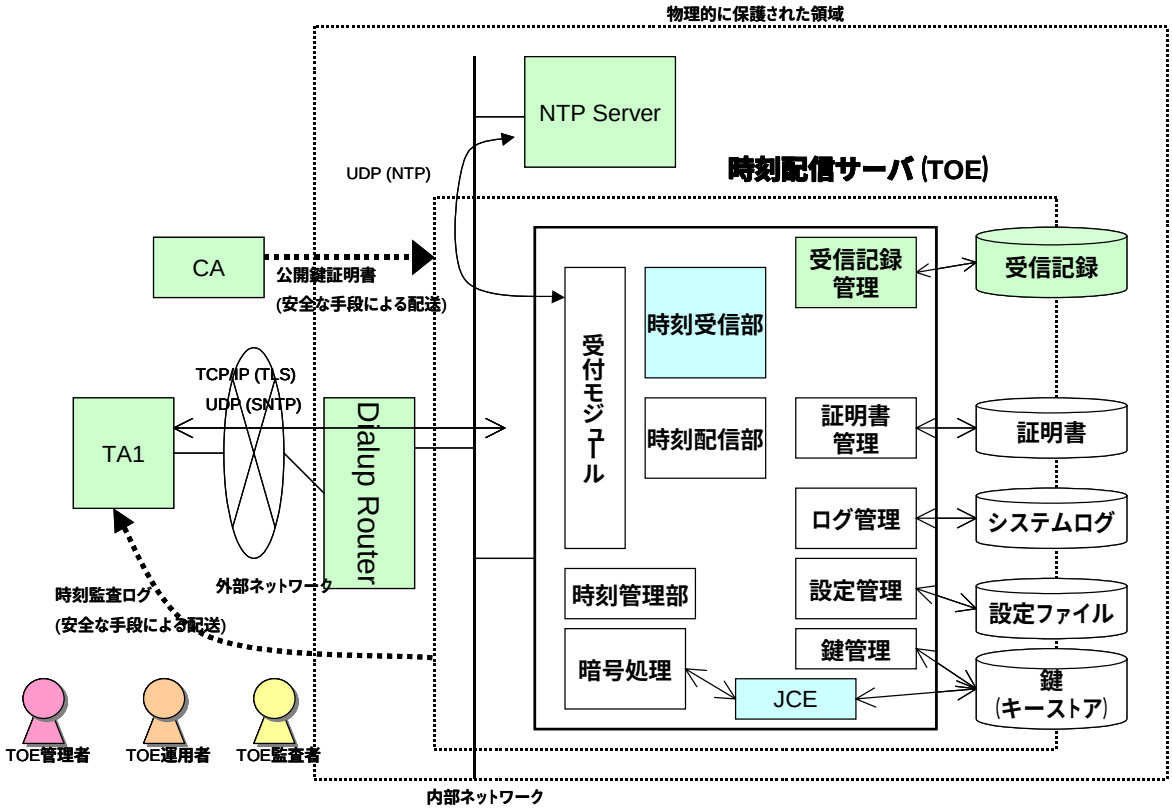


図 1-1　システム構成図

1-3 利用する暗号技術と暗号コンポーネント

以下に、TOE の利用する暗号技術と、暗号コンポーネント構成図を示す。

表 1-1　TOE の利用する暗号技術

#	システム	使用している暗号技術		使用目的
1	NTA1	TLS	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット RSAES-PKCS1-v1_5 鍵長 1024 ビット 【共通鍵暗号方式】 128-bit RC4 【ハッシュ関数】 MD5	通信先の認証・通信データの改ざん防止 (時刻配信)
		SNTP	【メッセージ認証方式】 HMAC(MD5)	通信データの改ざん防止
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	時刻監査証明書への署名
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	ログへの署名
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット、鍵長 2048 ビット 【ハッシュ関数】 SHA-1	公開鍵証明書の検証、ARL/CRL の検証、時刻監査証明書の検証
		ハッシュ関数	SHA-1	ログの改ざん防止

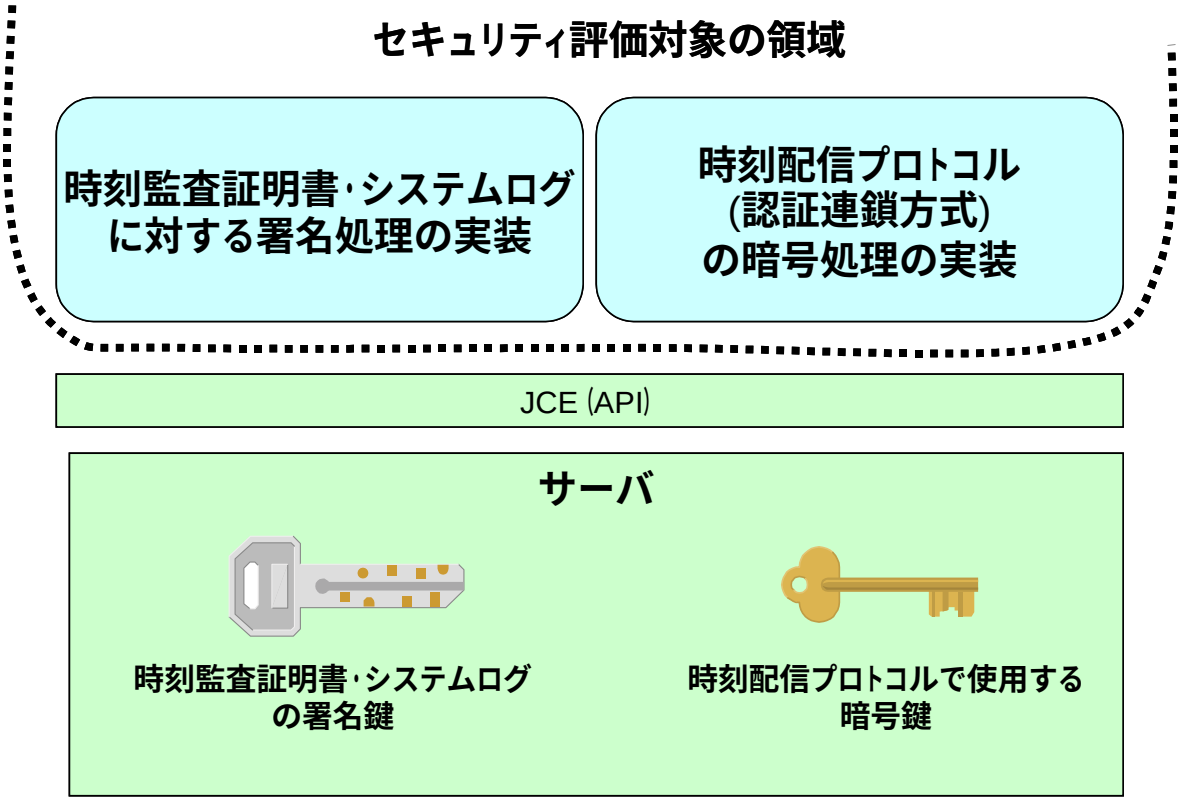


図 1-2　セキュリティ評価対象の領域

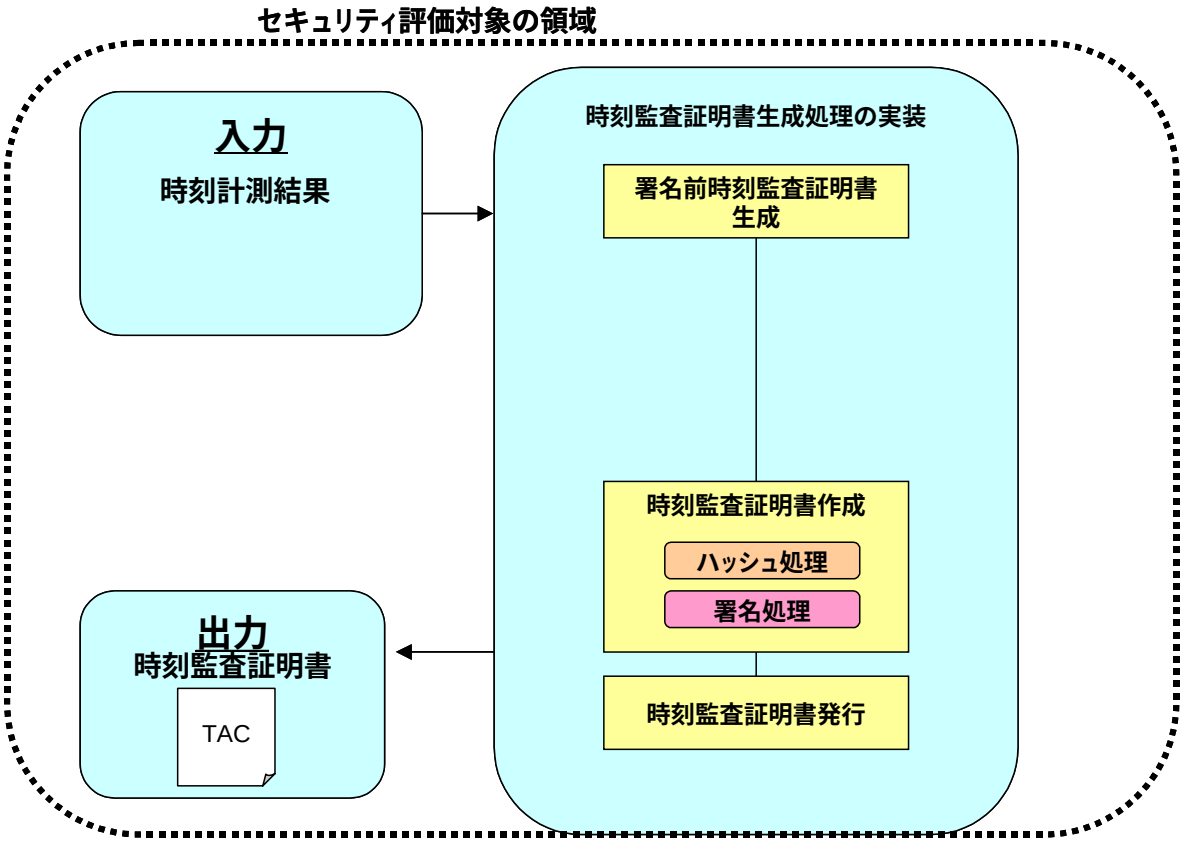


図 1-3　時刻監査証明書生成処理概要

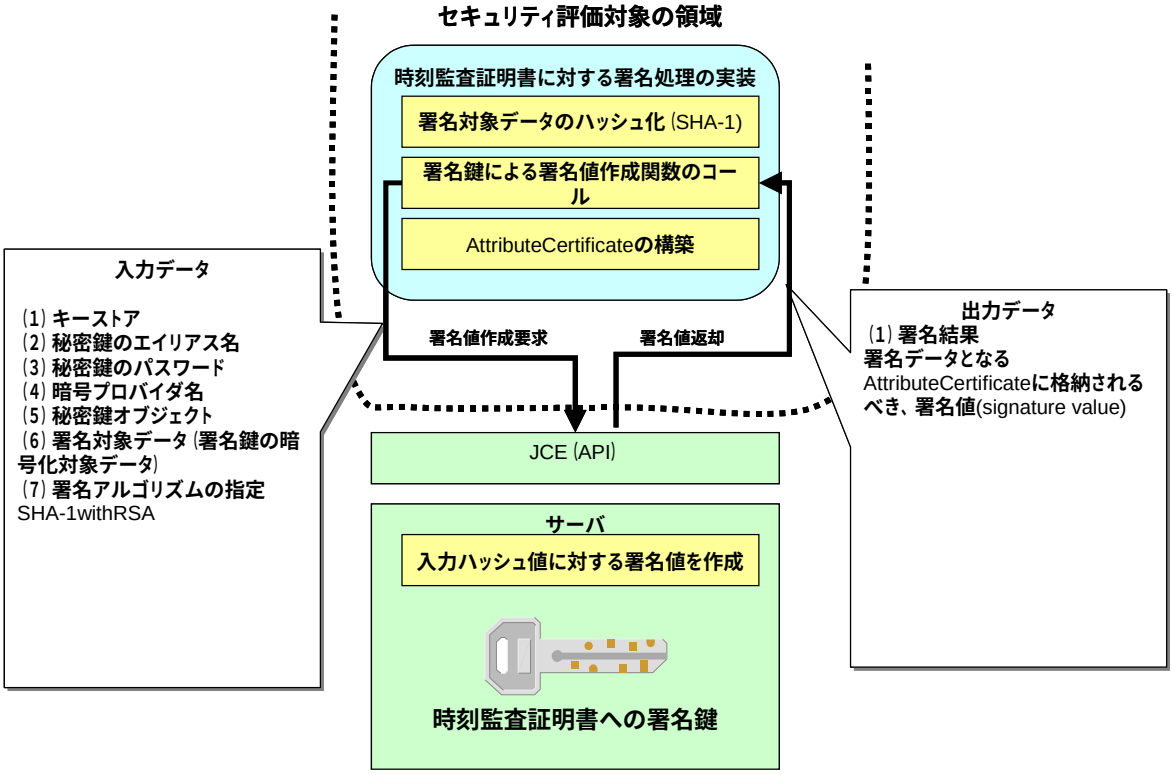
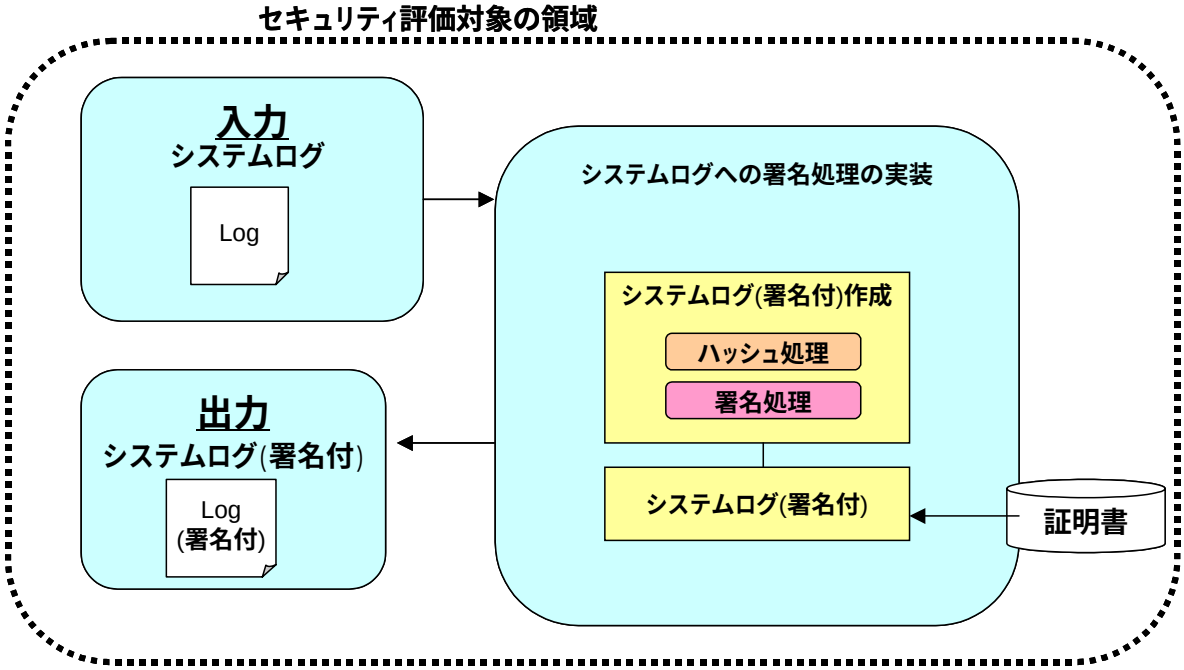


図 1-4　時刻監査証明書生成処理実装（署名処理実装）概要



※署名対象データは、システムログ内のハッシュ値

図 1-5　システムログへの署名処理概要

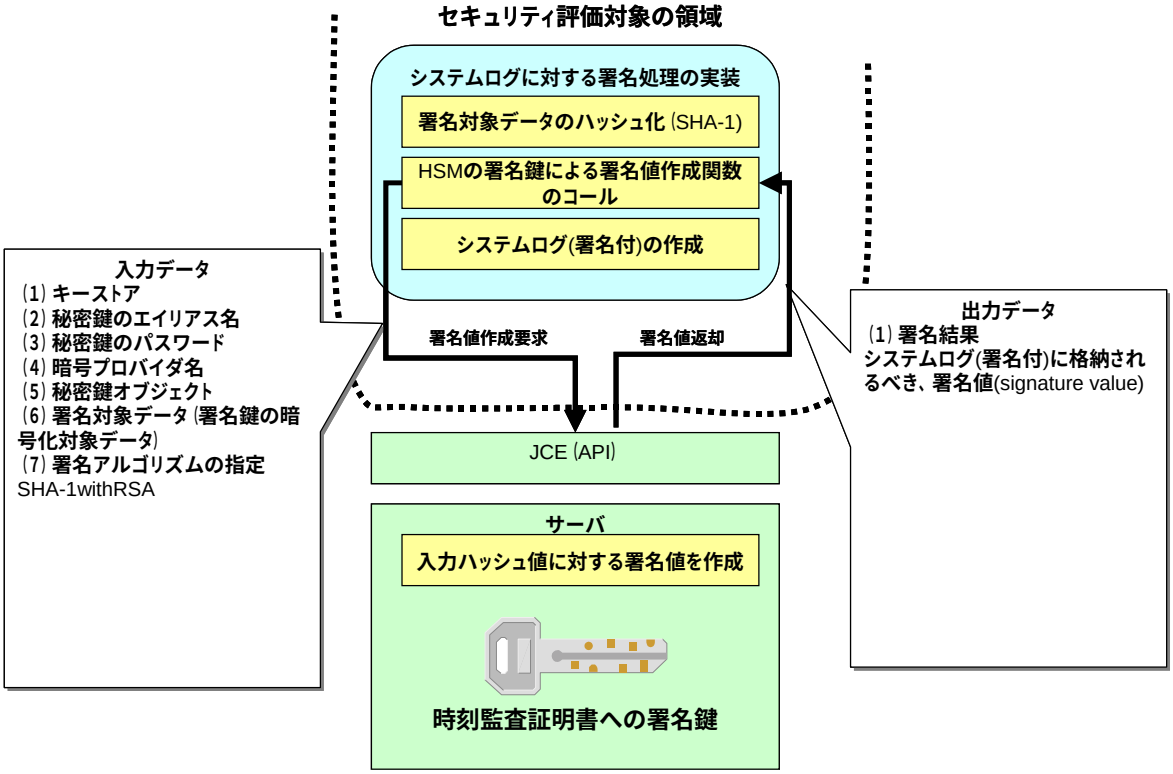


図 1-6　システムログへの署名処理実装概要

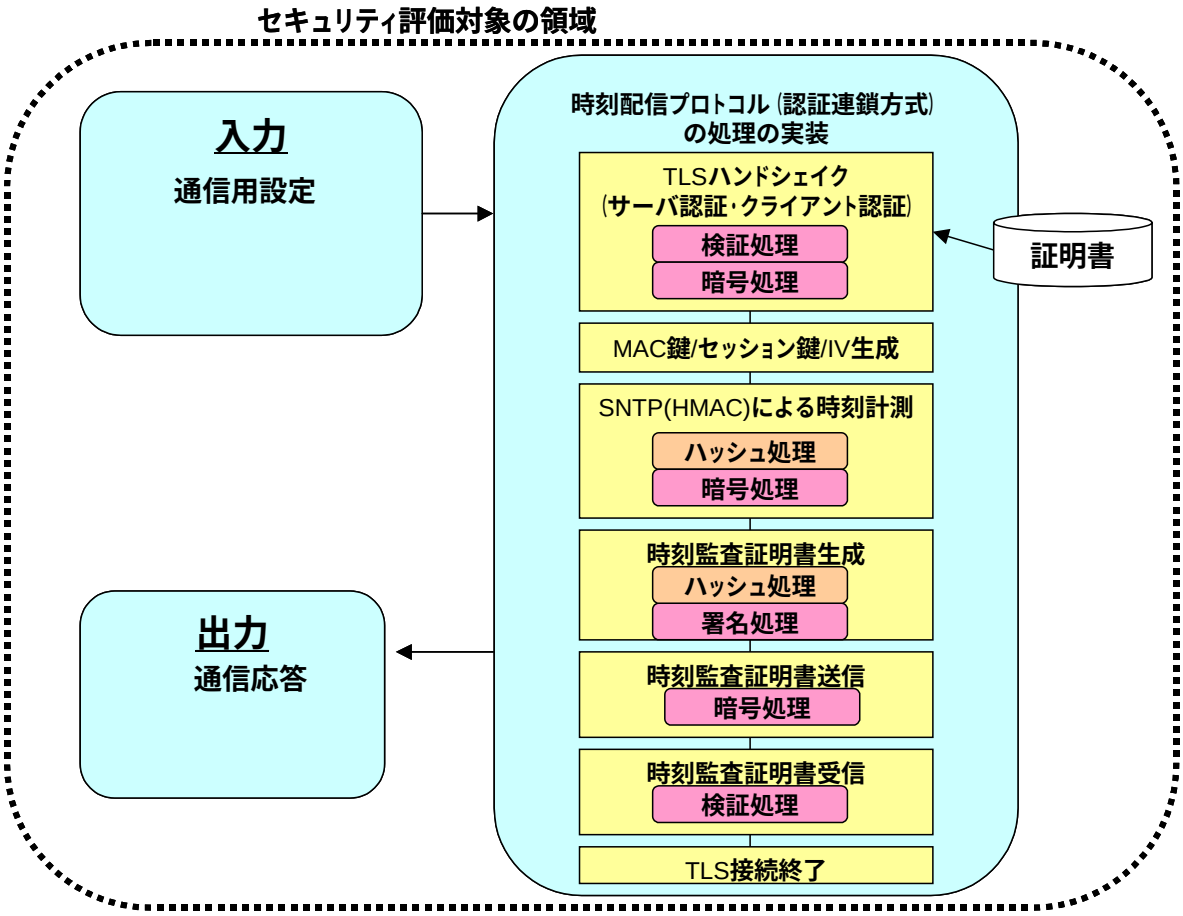


図 1-7　時刻配信プロトコル（認証連鎖方式：配信）処理概要

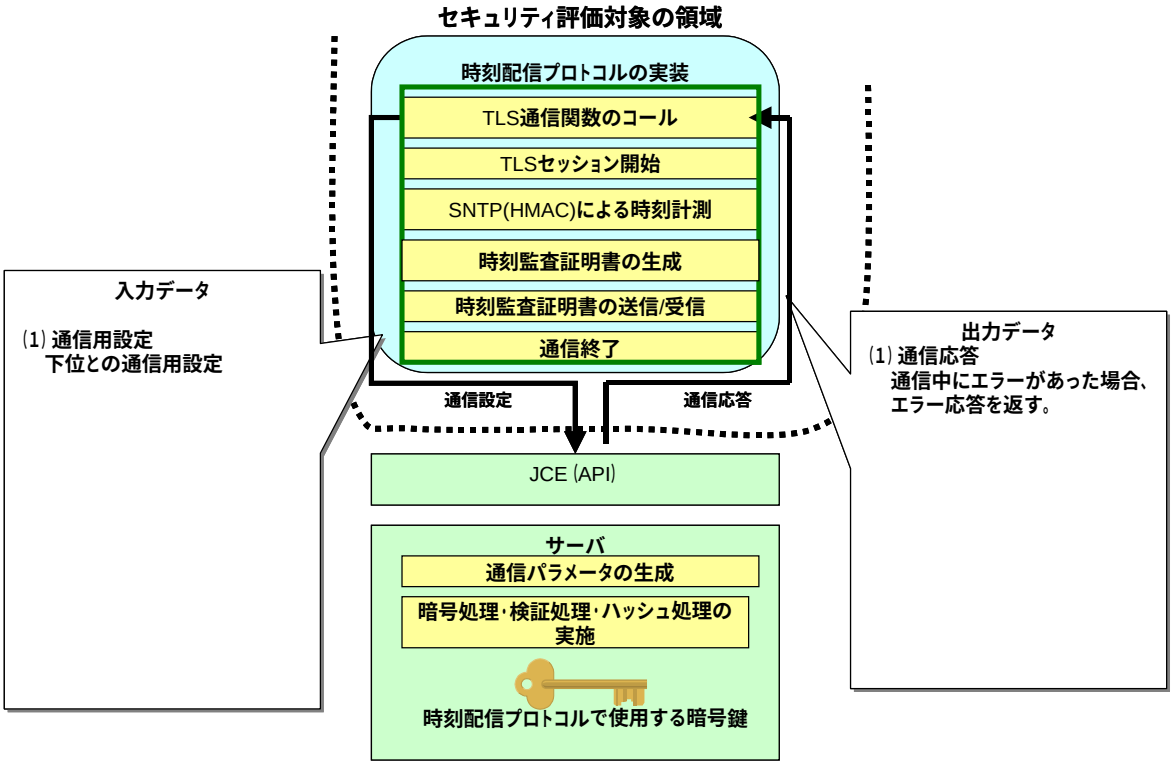


図 1-8　時刻配信プロトコル(認証連鎖方式：配信)処理実装（暗号処理実装）概要

1-4 関与者

以下に、TOE の関与者を示す。

表 1-2　TOE の関与者

#	関与者	説明
1	TOE 管理者	TOE に関わるユーザ/役割を管理する。 時刻に関する管理業務を行う。 暗号機能に関わる初期化及び管理業務を行う。 悪意のあるソフトウェアが動作しないようにする。 適切なディスクスペースを用意する。 データベースを適切に管理する。
2	TOE 運用者	TOE の起動・停止を実行する。 TOE 管理者の指示の元で各種設定など運用業務を行う。
3	TOE 監査者	TOE が生成する監査データの分析等の監査業務を行う。
4	TA1	認証連鎖方式の時刻配信局。 TOE から認証連鎖方式による時刻の配信および監査を受ける。

1-5 資産

以下に、TOE の資産を示す。

表 1-3　TOE の資産

No.	分類	データ名	資産名
1	鍵/キーストア	秘密鍵(NTA-署名)	秘密鍵
2		秘密鍵(NTA-TLS)	秘密鍵
3		証明書(CA)	設定情報
4		証明書(NTA-署名)	設定情報
5		証明書(NTA-TLS)	設定情報
6	設定ファイル	配信先設定	設定情報
7		ポリシ設定	設定情報
8		うるう秒設定	設定情報
9		ID･パスワード	ID･パスワード
10		各種設定	設定情報
11	システムログ	システムログ	ログ
12		時刻監査ログ	ログ
13		操作ログ	ログ
14	証明書	CA証明書	設定情報
15		TA証明書(署名)	設定情報
16		TA証明書(TLS)	設定情報
17		ARL	設定情報
18		CRL	設定情報
19	時刻	時刻受信	システム時刻
20		時刻配信	システム時刻
21		ロギング	システム時刻
22	ソフトウェア	時刻情報配信ソフトウェア	ソフトウェア
23	時刻監査ログ	時刻監査ログ	ログ
24	時刻監査証明書	時刻監査証明書	時刻監査証明書

第2章 セキュリティ環境

本章では、内部不正を考慮しないセキュリティ環境（前提、脅威、組織のセキュリティポリシー）について記載する。

1. 前提

以下に、TOE を使用する際のセキュリティ環境の前提を示す。

表 2-1　前提

No.	分類	項目	説明
1	物理的な前提	A.Location	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティの中に設置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2	人的な前提	A.TOE_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOEとTOEに含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOEを安全に導入、管理する。 ・TOEに関わるユーザ/役割を管理する。 ・時刻に関する管理業務を行う。 ・暗号機能に関わる初期化及び管理業務を行う。 ・TOE上で悪意のあるソフトウェアが動作しないようにする。 ・TOEの用件を満たす適切なディスクスペースを用意する。 ・TOEのデータベースを適切に管理する。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
3	人的な前提	A.TOE_Operator	一人以上の許可された運用者が割り当てられる。 ・TOEの起動・停止を実行する。 ・TOE管理者の指示の元で各種設定など運用業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
4	人的な前提	A.TOE_Auditor	一人以上の許可された監査者が割り当てられる。 ・TOEが生成する監査データの分析等の監査業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
5	人的な前提	A.TA1_TAC	TA1(認証連鎖方式の時刻配信局)は、時刻監査証明書を検証する。この中には、アウト・オブ・バンドの方法を用いて、NTA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なNTAによって行われたものかどうかの確認、が含まれる。
6	人的な前提	A.TOE_Separation	TOEが動作するサーバマシンには、TOEの動作に必要なソフトウェア以外はインストールされないものとする。
7	接続に関する前提	A.Device	周辺機器への接続は、コントロールされたアクセス・ファシリティ内に存在する。
8	接続に関する前提	A.FIREWALL	TOEと他システムとの接続には、専用線を用いる。TOEとセグメントが異なる場合は、ファイアウォールを設置する。
9	接続に関する前提	A.PEER	TOEと通信する意図された他システムは、信頼できる。
10	その他	A.Abstract	TOEが動作するために必要なOSや依存するライブラリは、不正な改変から保護され、正しく動作する。
11	接続に関する前提	A.TA1_NTA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
12	接続に関する	A.TimeSource_NTA	時刻ソースとTOEの間の通信路は、時刻ソースやTOEの成りすまし、データの改ざん、データの盗

	前提	1_Connection	聴を防止する。
13	物理的な前提	A.Environment	TOE の設置場所は、電磁波対策、電力対策、温度･湿度対策が行われている。
14	物理的な前提	A.MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。

2. 脅威

以下に、TOE および環境に対する脅威を示す。

なお、脅威の分類は以下のように区分した。

・分類：TOE

TOE のセキュリティ機能（例：時刻配信プロトコルなど）により対策可能。

・分類：環境

TOE のセキュリティ機能では対策不可能、環境の IT/非 IT 機能（例：外部の IDS システムにより対策、運用により対策）により対策可能。

※TOE のログ管理機能、TOE 管理機能を利用して対策する脅威は、こちらの区分に含めている。

表 2-2　脅威

No.	分類	項目	説明
1	環境	T.SystemClock_TOEuser_Modify_TimeSource	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。
2	環境	T.SystemClock_Inaccuracy_gradually	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。)
3	環境	T.SystemClock_Inaccuracy_immediately	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が故障し、急に時刻がずれる。)
4	環境	T.SystemClock_TOEuser_Modify_Clock_byTOE	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
5	環境	T.SystemClock_TOEuser_Modify_Clock_byOS	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(OSの機能を利用)
6	環境	T.SystemClock_Cracker_Modify_Clock	外部の不正者が、ネットワーク経由でTOEが参照する時計の時刻をずらす。
7	環境	T.TAC_NTA_Crypto_Compromise_gradually	過去に発行した時刻監査証明書に使用されている暗号アルゴリズムが脆弱化する。(計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。)
8	環境	T.TAC_NTA_Crypto_Compromise_immediately	過去に発行した時刻監査証明書に使用されている暗号アルゴリズムが脆弱化する。(暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。)
9	環境	T.TAC_Line	TA-TOE間のネットワークが、事故などにより遮断され、TOEの送信した時刻監査証明書がTAに到達しない。
10	環境	T.Key_TOEuser_Compromise	許可された利用者が、不注意によりTOEの秘密鍵を暴露する。
11	環境	T.Key_Cracker_Compromise	外部の不正者が、ネットワーク経由でTOEの秘密鍵を盗む。
12	環境	T.Config_TOEuser_Modify_byTOE	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。(TOEの機能を利用)

13	環境	T.Config_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。(OSの機能を利用)
14	環境	T.Config_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定情報を変更･削除･暴露する。
15	環境	T.Config_badTAC_TOEuser_Modify	許可された利用者が、不注意によりTOEの設定を変更し、不正な時刻監査証明書を発行する。
16	環境	T.Config_badTAC_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正な時刻監査証明書を発行する。
17	環境	T.Config_stopTAC_TOEuser_Modify	許可された利用者が、不注意によりTOEの設定を変更し、時刻監査証明書の発行を停止させる。
18	環境	T.Config_stopTAC_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定を変更し、時刻監査証明書の発行を停止させる。
19	TOE	T.Config_badTAC_TOEuser_ModifyTA	許可された利用者が、不注意によりTOEの設定を変更し、異なるTAに時刻監査証明書を送信する。
20	環境	T.Config_badTAC_Cracker_ModifyTA	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正なTAに時刻監査証明書を送信する。
21	環境	T.Log_TOEuser_Delete_byTOE	許可された利用者が、不注意により、TOEのログを削除･暴露する。(TOEの機能を利用) ※ログの変更は、TOEの機能を利用して実施することはできない。
22	環境	T.Log_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEのログを変更･削除･暴露する。(OSの機能を利用)
23	環境	T.Log_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEのログを変更･削除･暴露する。
24	環境	T.SW_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEのソフトウェアを変更･削除･暴露する。(OSの機能を利用)
25	環境	T.SW_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEのソフトウェアを変更･削除･暴露する。
26	環境	T.Password_TOEuser_Secret_byOS	許可された利用者が、不注意により、TOEのID･パスワードを暴露する。(OSの機能を利用)
27	環境	T.Password_TOEuser_Secret_byMemo	許可された利用者が、不注意により、TOEのID･パスワードを暴露する。(口頭、メモ、メール等)
28	環境	T.Password_Cracker_Secret	外部の不正者が、ネットワーク経由でTOEのID･パスワードを暴露する。
29	環境	T.Virus_TOEuser	許可された利用者が、不注意により、TOEにウィルスを感染させる。
30	環境	T.Virus_Cracker	外部の不正者が、ネットワーク経由でTOEにウィルスを感染させる。
31	環境	T.DoS	外部の不正者から大量のアクセスが行われ、TOEをサービス不能にさせる。
32	環境	T.BufferOverFlow_Attack	外部の不正者が、バッファ･オーバーフローの脆弱性を利用し、TOEの管理者権限を取得する。
33	環境	T.Hardware_Failure	･経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産が失われる。 ･経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産の完全性が保証できなくなる。 ･経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、TOEが提供するサービスが継続できない。
34	環境	T.TOE_Bug	TOEのIT実装にソフトウェア不良が存在するため、TOEの資産の信頼性が乏しくなる。 例) ･ある条件下で、ログの書き込みが行われない。 ･ある条件下で、ログファイルを破壊する。
35	環境	T.Peer_Failure_Asset	通信相手となる他システムのダウンにより、TOEの資産が失われる。
36	環境	T.Peer_Failure_TimeSource	時刻ソースのダウンにより、TOEが提供するサービスが継続できない。
37	環境	T.Connection_Failure_Asset	TOEと通信相手となる他システムの間の通信回線の故障により、TOEの資産が失われる。
38	環境	T.Connection_Failure_TimeSource	時刻ソースとの間の通信回線の故障により、TOEが提供するサービスが継続できない。

3. 組織のセキュリティポリシー

以下に、TOE を使用するにあたっての、組織のセキュリティポリシーを示す。

表 2-3　組織のセキュリティポリシー

No.	項目	説明
1	P.Cryptography	署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって実装されなければならない。
2	P.PKI_Management	安全に管理されたPKIの中で、TOEを運用すること。全ての鍵と証明書は、安全に発行、失効される。
3	P.Password_Management	TOEのパスワードは、TOE管理者およびTOE運用者によって適切に管理され、TOE管理者およびTOE運用者以外に知られてはならない。
4	P.Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。
5	P.Time_Source	TOEは、信頼のできる時刻ソースを参照すること。また、時刻ソースの信頼性と正確性は、TOE所有者にとって受容可能であること。
6	P.System_Clock_Management	TOEが参照する時計を信頼のできる時刻ソースと同期させる。
7	P.Check_Virus	定期的なウィルスチェックを実行する。 外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_TA1	TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
9	P.Dual_Control	TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
10	P.Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

第3章 セキュリティ目標・対策と実装システムの評価

本章では、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を記載する。また、セキュリティ環境の前提と組織のセキュリティポリシーに関する実現方法例を記載する。

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

以下に、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を示す。

表 3-1　脅威のセキュリティ目標・対策及び実装システムに対する評価

No.	脅威名	セキュリティ目標･対策		統合化システムにおける実現
1	T.SystemClock_TOEuser_Modify_TimeSource	防止	･教育 (･複数人による操作(運用または機能での実現)) (･罰則)	･教育 (･複数人による操作(運用)) (･罰則)
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査
		回復	･正しい時刻ソースからの時刻配信を受ける。	･正しい時刻ソースからの時刻配信を受ける。
2	T.SystemClock_Inaccuracy_gradually	防止	･時刻ソースからの時刻配信を受ける。	･時刻ソースからの時刻配信を受ける。
		検出	･ログの確認 (定期的な時刻誤差の確認)	･ログの確認 (定期的な時刻誤差の確認)
		回復	ー	ー
3	T.SystemClock_Inaccuracy_immediately	防止	ー	ー
		検出	･ログの確認 (定期的な時刻誤差の確認)	･ログの確認 (定期的な時刻誤差の確認)
		回復	･時刻ソースからの時刻配信を受ける。	･時刻ソースからの時刻配信を受ける。
4	T.SystemClock_TOEuser_Modify_Clock_byTOE	防止	･教育 (･複数人による操作(運用または機能での実現)) (･罰則)	･教育 (･複数人による操作(運用)) (･罰則)
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能:ログ管理機能
		回復	･時刻ソースからの時刻配信を受ける。	･時刻ソースからの時刻配信を受ける。

5	T.SystemClock_TOEuser_Modify_Clock_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・時刻ソースからの時刻配信を受ける。	・時刻ソースからの時刻配信を受ける。
6	T.SystemClock_Cracker_Modify_Clock	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・時刻ソースからの時刻配信を受ける。	・時刻ソースからの時刻配信を受ける。
7	T.TAC_NTA_Crypto_Compromise_gradually	防止	・TA側で、あらかじめ時刻監査証明書をセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・暗号アルゴリズムが完全に危殆化する前に、TA側で、時刻監査証明書に対して、安全な暗号アルゴリズムを使用したタイムスタンプを取得する。 ・TA側で、あらかじめ時刻監査証明書に対しタイムスタンプを取得する。 (時刻監査証明書とは異なる暗号アルゴリズムを使用したタイムスタンプを取得する。) ・NTAが時刻監査証明書を保管する。	・TA側で、あらかじめ時刻監査証明書をセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・NTAが時刻監査証明書を保管する。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー
8	T.TAC_NTA_Crypto_Compromise_immediately	防止	・TA側で、あらかじめ時刻監査証明書をセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・TA側で、あらかじめ時刻監査証明書に対しタイムスタンプを取得する。 (時刻監査証明書とは異なる暗号アルゴリズムを使用したタイムスタンプを取得する。) ・NTAが時刻監査証明書を保管する。	・TA側で、あらかじめ時刻監査証明書をセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・NTAが時刻監査証明書を保管する。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー
9	T.TAC_Line	防止	・TA-TOE間の通信路を冗長構成とする。	・TA-TOE間の通信路を冗長構成とすることで実現可能。
		検出	ー	ー

		回復	ー	ー
10	T.Key_TOEuser_Compromise	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作（運用）) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
11	T.Key_Cracker_Compromise	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
12	T.Config_TOEuser_Modify_byTOE	防止	・教育 (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 (・複数人による操作（運用）) (・罰則)
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
13	T.Config_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作（運用）) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
14	T.Config_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
15	T.Config_badTAC_TOEuser_Modify	防止	・教育 ・複数人による操作（運用または機能での実現） (・罰則)	・教育 ・複数人による操作（運用） (・罰則)
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
16	T.Config_badTAC_Cra	防止	・ファイアウォール	・ファイアウォール

	cker_Modify			
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
17	T.Config_stopTAC_TOEuser_Modify	防止	・教育 ・複数人による操作（運用または機能での実現） （・罰則）	・教育 ・複数人による操作（運用） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
18	T.Config_stopTAC_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
19	T.Config_badTAC_TOEuser_ModifyTA	防止	・TLSによる相互認証 ・教育 ・複数人による操作（運用または機能での実現） （・罰則）	・TLSによる相互認証 ※関連するTOEの機能：時刻配信プロトコル ・教育 ・複数人による操作（運用） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
20	T.Config_badTAC_Cracker_ModifyTA	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
21	T.Log_TOEuser_Delete_byTOE	防止	・教育 （・複数人による操作（運用または機能での実現）） （・罰則）	・教育 （・複数人による操作（運用）） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
22	T.Log_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) （・複数人による操作（運用または機能での実現）） （・罰則）	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) （・複数人による操作（運用）） （・罰則）

		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
23	T.Log_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
24	T.SW_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
25	T.SW_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
26	T.Password_TOEuser_Secret_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
27	T.Password_TOEuser_Secret_byMemo	防止	・教育 (・罰則)	・教育 (・罰則)
		検出	ー	ー
		回復	ー	ー
28	T.Password_Cracker_Secret	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー

29	T.Virus_TOEuser	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ・ウィルスチェック (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) ・ウィルスチェック (・複数人による操作 (運用)) (・罰則)
		検出	ー	ー
		回復	ー	ー
30	T.Virus_Cracker	防止	・ウィルスチェック	・ウィルスチェック
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
31	T.DoS	防止	・システムの冗長構成	・システムを冗長構成とすることで実現可能。
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
32	T.BufferOverFlow_Attack	防止	・脆弱性の確認とセキュリティパッチの適用	・脆弱性の確認とセキュリティパッチの適用
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
33	T.Hardware_Failure	防止	・システムの冗長構成	・システムを冗長構成とすることで実現可能。
		検出	ー	ー
		回復	ー	ー
34	T.TOE_Bug	防止	・TOE開発者が、ソフトウェア不良を防ぐ開発プロセスを採用する。 ・TOE利用者(TOEの管理者や運用者)は、TOEの導入に際し、十分な試験を行う。	・TOE開発者が、ソフトウェア不良を防ぐ開発プロセスを採用することで実現可能。 ・TOE利用者(TOEの管理者や運用者)は、TOEの導入に際し、十分な試験を行う。
		検出	ー	ー
		回復	・TOE開発者が、パッチの作成・配布・適用を適切に実施する。また、TOE利用者(TOEの管理者や運用者)は、TOEに、TOE開発者の提供するパッチを適用する。	・TOE開発者が、パッチの作成・配布・適用を適切に実施し、TOE利用者(TOEの管理者や運用者)は、TOEに、TOE開発者の提供するパッチを適用することで実現可能。
35	T.Peer_Failure_Asset	防止	ー	ー
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能：ログ管理機能
		回復	・TA復旧後の、TAへの再接続。 (対象資産：時刻監査証明書)	・TA復旧後の、TAへの再接続。 (対象資産：時刻監査証明書)
36	T.Peer_Failure_TimeSource	防止	・複数の時刻ソースを利用する。	・複数の時刻ソースを利用することで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認)

		回復	・時刻ソース復旧後の、時刻ソースとの再接続。	・時刻ソース復旧後の、時刻ソースとの再接続。
37	T.Connection_Failure_Asset	防止	・他システム-TOE間の通信路を冗長構成とする。	・他システム-TOE間の通信路を冗長構成とすることで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能：ログ管理機能
		回復	・通信回線復旧後の、TAへの再接続。 (対象資産：時刻監査証明書)	・通信回線復旧後の、TAへの再接続。 (対象資産：時刻監査証明書)
38	T.Connection_Failure_TimeSource	防止	・通信回線の異なる複数の時刻ソースを利用する。	・通信回線の異なる複数の時刻ソースを利用することで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認)
		回復	・通信回線復旧後の、時刻ソースとの再接続。	・通信回線復旧後の、時刻ソースとの再接続。

2. 前提の実現方法例

以下に、セキュリティ環境の前提に関する実現方法例を記載する。

表 3-2　前提の実現方法例

No.	前提名	実現方法例
1	A.Location	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
2	A.TOE_Administrator	・TOE管理者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE管理者は、TOEとTOEに含まれる情報のセキュリティを維持するようにTOEを導入し、管理することを保証する。 ・TOE管理者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
3	A.TOE_Operator	・TOE運用者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE運用者は、TOE管理者の指示の元で、TOEとTOEに含まれる情報のセキュリティを維持するようにTOEを管理・運用することを保証する。 ・TOE運用者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
4	A.TOE_Auditor	・TOE監査者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE監査者は、TOEを運用する組織の規定に従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。

5	A.TA1_TAC	TA1(認証連鎖方式の時刻配信局)は、時刻監査証明書を検証する責任を持つ。この中には、アウト･オブ･バンドの方法を用いて、NTA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なNTAによって行われたものかどうかの確認、が含まれる。 ･TA1は、時刻監査証明書を検証するためのソフトウェアを持つ。
6	A.TOE_Separation	･TOE管理者は、TOE 及びTOE のIT環境の取扱説明書を熟読した上で、取扱説明書が定める手順に従って、TOE 及びTOE のIT 環境を構築する。この際、TOEが動作するサーバマシンには、TOE の動作に関係ないソフトウェアはインストールしない。
7	A.Device	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
8	A.FIREWALL	･TOEとTA1、時刻ソースは、専用線で接続し、TOEとセグメントが異なる場合は、ファイアウォールを設置する。 ･ファイアウォールの設定は、適切に維持･管理される。
9	A.PEER	･TOEと通信する意図された他システムは、信頼できる第三者(TTP)の運用するシステムであることを保証する。 ･TOEは、NTA1内のネットワークに接続された、日本標準時と同期した時刻ソースを参照する。
10	A.Abstract	･TOE 管理者は、TOE が動作するために必要なOSや依存するライブラリが不正な改変から保護され、正しく動作するよう適切に管理する。 ･TOE 管理者は、TOE が動作するサーバマシンに、TOE の動作を干渉するようなソフトウェアがインストールされないように、適切に管理する。 ･TOE 管理者は、TOE 及びTOE のIT 環境が正常な動作を維持するように、適切に管理する。
11	A.TA1_NTA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、専用線である。
12	A.TimeSource_NTA1_Connection	･時刻ソースとTOEの間の通信路は、専用線である。
13	A.Environment	･TOE の設置場所として、電磁波対策、電力対策、温度･湿度対策が行われている設備を利用する。
14	A.MEDIA	･定期的なデータのバックアップと、適切なシステムマイグレーションを行う。

3. 組織のセキュリティポリシーの実現方法例

以下に、組織のセキュリティポリシーに関する実現方法例を記載する。

表 3-3　組織のセキュリティポリシーの実現方法例

No.	ポリシー名	実現方法例
1	P.Cryptography	･TOEの署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって行われる。
2	P.PKI_Management	TOEは、安全に管理されたPKIの中で運用されることを保証する。鍵/証明書は、運用マニュアルに基づき、安全に発行･失効される。
3	P.Password_Management	･TOE管理者およびTOE運用者は、パスワードを記憶し、他人に漏らさない。また、運用マニュアルに基づき、適切なパスワードを設定し、適切な頻度でパスワードを変更する。 ･TOE管理者およびTOE運用者は、ソーシャルエンジニアリングの教育を受けている。
4	P.Protect_Log	･TOE を利用する組織は、TOEの監査ログの暴露･改ざんまたは削除を防止するよう、TOE管理者、TOE運用者、TOE監査者に対して教育を行う。 ･TOEは、TOEの出力するシステムログにハッシュ値やデジタル署名を付与し、改ざんを検出可能な機能を持つ。 ･TOEは、TOEの保護対象資産へのアクセスを許可する前に、全ての利用者に対して識別･認証情報の入力を要求し、識別･認証を実施する。

5	P.Time_Source	TOEは、NTA1内のネットワークに接続された、日本標準時と同期した時刻ソースを参照する。
6	P.System_Clock_Management	TOEは、NTA1内のネットワークに接続された、日本標準時と同期した時刻ソースを参照する。
7	P.Check_Virus	TOE管理者は、運用マニュアルに基づき、定期的にTOEの全ファイルに対してウィルスチェックを行う。また、外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_TA1	TOEは、TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
9	P.Dual_Control	運用マニュアルに基づき、TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行う。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行う。
10	P.Check_Abstract_Vulnerability	TOE管理者は、運用マニュアルに基づき、定期的にOS やライブラリなどの脆弱性を確認し、対策を行う。

第4章 脅威ツリー及びリスク評価一覧

本章では、内部不正のないセキュリティ評価における脅威ツリー、リスク評価格付けの考え方、リスク評価点を記述する。

1. 脅威ツリー

以下に、脅威ツリーを示す。
※欄の不足を補うため、一部「下位の条件→上位の条件」と矢印で表現している場合がある。

表 4-1　脅威ツリー

No.	資産	脅威	上位レベルが実現するための条件			脅威名
			条件1	条件2	条件3	
1	システム時刻	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。	許可された利用者が、不注意により、TOEの設定情報を変更する。	—	—	T.SystemClock_TOEuser_Modify_TimeSource
2	システム時刻	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。	TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。	—	—	T.SystemClock_Inaccuracy_gradually
3	システム時刻		TOEが参照する時計が故障し、急に時刻がずれる。	—	—	T.SystemClock_Inaccuracy_immediately
4	システム時刻		時刻ソースが不正な時刻を配信し、これをもとにTOEが時刻を補正することで、時刻がずれる。	※前提A.PEERとして、時刻ソースは信頼できるので脅威から除外。	—	—
5	システム時刻	許可された利用者が、不注意により、または外部の不正者が、TOEが参照する時計の時刻をずらす。	許可された利用者が、不注意によりTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	—	T.SystemClock_TOEuser_Modify_Clock_byTOE
6	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	OSにログインする	T.SystemClock_TOEuser_Modify_Clock_byOS
7	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	—

8	システム時刻		外部の不正者が、ネットワーク経由でTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	T.SystemClock_Cracker_Modify_Clock
9	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	同上
10	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	同上
11	システム時刻		外部の不正者が、物理的に侵入し、TOEの時刻を設定する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―
12	システム時刻	外部の不正者が、時刻ソースに成りすまして、TOEに時刻を配信する。	TOEにネットワーク経由でアクセスする。	※前提A.TimeSource_NTA1_Connectionとして、時刻ソース-TOE間の通信路は、時刻ソースやTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―
13	システム時刻	外部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	※前提A.TimeSource_NTA1_Connectionとして、時刻ソース-TOE間の通信路は、時刻ソースやTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	ー
14	時刻監査証明書	過去に発行した時刻監査証明書に使用されている暗号アルゴリズムが脆弱化する。	暗号アルゴリズムの攻撃方法が発見され、暗号アルゴリズムが脆弱化する。	計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。	―	T.TAC_NTA_Crypto_Compromise_gradually
15	時刻監査証明書			暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。	―	T.TAC_NTA_Crypto_Compromise_immediately
16	時刻監査証明書	外部の不正者が、TAに成りすまして、TOEの送信する時刻監査証明書を受信する。	TOEにネットワーク経由でアクセスする。	※前提A.TA1_NTA1_Connectionとして、TA-TOE間の通信路は、TAやTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―

17	時刻監査証明書	外部の不正者が、TOEとTAの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEとTAの間のネットワークにアクセスする。	※前提A.TA1_NTA1_Connectionとして、TA-TOE間の通信路は、TAやTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	—	—
18	時刻監査証明書	TOEの送信した時刻監査証明書が、不正者もしくは事故などにより改ざんされる。	時刻監査証明書を改ざんし、TAに送付する。	TA-TOE間のネットワークにアクセスする。 →ネットワーク中のパケットから、TOEの送付した時刻監査証明書を取得する。	※前提A.TA1_TACにより、TAは受信した時刻監査証明書の検証を行うため、脅威とはならない。	—
19	時刻監査証明書	TOEの送信した時刻監査証明書が、不正者もしくは事故などにより暴露される。	ネットワーク中のパケットから、TOEの送付した時刻監査証明書を取得する。	TA-TOE間のネットワークにアクセスする。	※時刻監査証明書の内容は、暴露されても問題のない内容であるため、脅威とはならない。	—
20	時刻監査証明書	TOEの送信した時刻監査証明書が、事故などによりTAに到達しない。	TA-TOE間のネットワークが、事故などにより遮断される。	—	—	T.TAC_Line
23	秘密鍵	TOEの秘密鍵が脆弱化する。	許可された利用者が、不注意によりTOEの秘密鍵を暴露する。	[通信用鍵･署名用鍵] OSの機能を用いてTOEの秘密鍵を取得する。	OSにログインする	T.Key_TOEuser_Compromise
24	秘密鍵		外部の不正者が、ネットワーク経由でTOEの秘密鍵を盗む。	[通信用鍵･署名用鍵] TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Key_Cracker_Compromise
25	秘密鍵		外部の不正者が、物理的に侵入し、TOEの秘密鍵を盗む。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—
26	設定情報	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。	TOEの機能を用いてTOEの設定情報を変更･削除･暴露する。	—	—	T.Config_TOEuser_Modify_byTOE
27	設定情報		OSの機能を用いてTOEの設定情報を変更･削除･暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	—	T.Config_TOEuser_Modify_byOS
28	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	—	—

29	設定情報	外部の不正者が、ネットワーク経由でTOEの設定情報を変更･削除･暴露する。	TOEの機能を用いてTOEの設定情報を変更･削除･暴露する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_Cracker_Modify
30	設定情報		OSの機能を用いてTOEの設定情報を変更･削除･暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
31	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
32	設定情報	外部の不正者が、物理的に侵入し、TOEの設定情報を変更･削除･暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
33	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、不正な時刻監査証明書を発行する。	TOEの設定情報を変更する。 ※[不正な時刻監査証明書の例] 本来のポリシ(OID,時刻監査規格(Offset,Delay)等)と異なる時刻監査証明書など。	TOEにアクセスする。	―	T.Config_badTAC_TOEuser_Modify
34	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正な時刻監査証明書を発行する。	TOEの設定情報を変更する。 ※[不正な時刻監査証明書の例] 本来のポリシ(OID,時刻監査規格(Offset,Delay)等)と異なる時刻監査証明書など。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_badTAC_Cracker_Modify
35	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、不正な時刻監査証明書を発行する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
36	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、時刻監査証明書の発行を停止させる。	TOEの設定情報を変更する。	TOEにアクセスする。	―	T.Config_stopTAC_TOEuser_Modify

37	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、時刻監査証明書の発行を停止させる。	TOEの設定情報を変更する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_stopTAC_Cracker_Modify
38	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、時刻監査証明書の発行を停止させる。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
39	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、異なるTAに時刻監査証明書を送信する。	TOEの設定情報を変更する。	TOEにアクセスする。	—	T.Config_badTAC_TOEuser_ModifyTA
40	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正なTAに時刻監査証明書を送信する。	TOEの設定情報を変更する。	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	—	T.Config_badTAC_Cracker_ModifyTA
41	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、不正なTAに時刻監査証明書を送信する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
42	ログ	許可された利用者が、不注意により、TOEのログを変更・削除・暴露する。	TOEの機能を用いてTOEのログを削除・暴露する。 ※ログの変更は、TOEの機能を利用して実施することはできない。	—	—	T.Log_TOEuser_Delete_byTOE
43	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	—	T.Log_TOEuser_Modify_byOS
44	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	—	—
45	ログ	外部の不正者が、ネットワーク経由でTOEのログを変更・削除・暴露する。	TOEの機能を用いてTOEのログを削除・暴露する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Log_Cracker_Modify

46	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
47	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。） ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
48	ログ	外部の不正者が、物理的に侵入し、TOEのログを変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
49	ソフトウェア	許可された利用者が、不注意により、TOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：OSのコマンドを利用して削除する。	OSにログインする	―	T.SW_TOEuser_Modify_byOS
50	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
51	ソフトウェア	外部の不正者が、ネットワーク経由でTOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.SW_Cracker_Modify
52	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
53	ソフトウェア	外部の不正者が、物理的に侵入し、TOEのソフトウェアを変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―

54	ID・パスワード	許可された利用者が、不注意により、TOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	OSにログインする	―	T.Password_TOEuser_Secret_byOS
55	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
56	ID・パスワード		その他、口頭、メモ、メール等で情報が漏洩する。	―	―	T.Password_TOEuser_Secret_byMemo
57	ID・パスワード	外部の不正者が、ネットワーク経由でTOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Password_Cracker_Secret
58	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
59	ID・パスワード	外部の不正者が、物理的に侵入し、TOEのID・パスワードを暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
60	その他	許可された利用者が、不注意により、TOEにウィルスを感染させる。	ウィルスに感染した外部メディアにアクセスする。	OSにログインする	ウィルスに感染した外部メディアを持ち込む。	T.Virus_TOEuser
61	その他		外部からウィルスをダウンロードする。	外部にアクセスする。	OSにログインする	同上
62	その他	外部の不正者が、ネットワーク経由でTOEにウィルスを感染させる。	TOEにウィルスをダウンロードさせる。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Virus_Cracker
63	その他	外部の不正者から大量のアクセスが行われ、TOEをサービス不能にさせる。	ネットワーク経由でTOEに大量のアクセスを行う。	―	―	T.DoS
64	その他	外部の不正者が、バッファ・オーバーフローの脆弱性を利用し、TOEの管理者権限を取得する。	TOEにネットワーク経由でアクセスする。	―	―	T.BufferOverFlow_Attack
65	その他	TOEのハードウェア故障	経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産が失われる。	―	―	T.Hardware_Failure

66	その他		経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産の完全性が保証できなくなる。	―	―	同上
67	その他		経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、TOEが提供するサービスが継続できない。	―	―	同上
68	その他	TOEのソフトウェアのバグ	TOEのIT実装にソフトウェア不良が存在するため、TOEの資産の信頼性が乏しくなる。 例) ・ある条件下で、ログの書き込みが行われない。 ・ある条件下で、ログファイルを破壊する。	TOEの開発時に、ソフトウェア不良を発見できない。	―	T.TOE_Bug
69	その他	通信相手となる他システムのダウン	通信相手となる他システムのダウンにより、TOEの資産が失われる。	―	―	T.Peer_Failure_Asset
70	その他		時刻ソースのダウンにより、TOEが提供するサービスが継続できない。	―	―	T.Peer_Failure_TimeSource
71	その他		TA1(認証連鎖方式の時刻配信局)のダウンにより、TOEが提供するサービスが継続できない。	※TOEに対する脅威とはならないため、脅威から除外。	―	―
73	その他	TOEと通信相手となる他システム間の通信回線の故障	TOEと通信相手となる他システムの間の通信回線の故障により、TOEの資産が失われる。	―	―	T.Connection_Failure_Asset
74	その他		時刻ソースとの間の通信回線の故障により、TOEが提供するサービスが継続できない。	―	―	T.Connection_Failure_TimeSource
75	その他		TA1(認証連鎖方式の時刻配信局)との間の通信回線の故障により、TOEが提供するサービスが継続できない。	※TOEに対する脅威とはならないため、脅威から除外。	―	―

2. リスク評価格付けの考え方

以下に、リスク評価格付けの考え方を示す。

表 4-2 リスク評価格付けの考え方

	格付け	高(3)	中(2)	低(1)
D	潜在的損失(Damage potential)	<方針> ・信頼性・サービスレベルに影響のあるもの。 ・データを直接悪用できるもの。 ＜対象＞ その他	<方針> ・データを直接は悪用できないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
R	再現性(Reproducibility)	＜方針＞ ・時期によらないもの。 ・内部不正など、攻撃者の意図でいつでも実施できるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ＜対象＞ ・内部不正 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・その他	＜方針＞ ・攻撃者の意図によらないもの。 ・TOE開発時のソフトウェア不良 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ＜対象＞ ・不注意（基本的に発生率は低い、という前提。） ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。) ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断（基本的に発生率は低い、という前提。）	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・暗号脆弱化 ・パケットの暴露・改ざん ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化
E	攻撃利用可能性(Exploitability)	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃できるもの。 ・攻撃方法が容易なもの。 ・比較的攻撃ツールが入手しやすいと思われるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの	＜方針＞ なし ＜対象＞ なし	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

		事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他		
A	影響ユーザ（Affected users）	<方針> ・TOEのサービスの利用者に関わるもの。 ・TOE利用者自身に大きな影響があるもの。 ＜対象＞ ・その他	<方針> ・TOEのサービスの利用者に対する直接的な影響がないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
D	発見可能性（Discoverability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃方法を知る事ができるもの。 ・攻撃方法が容易に思いつくもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他	＜方針＞ ・TOE開発時のソフトウェア不良 ＜対象＞ ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

3. リスク評価点

以下に、脅威に対するリスク評価点を示す。

表 4-3　リスク評価点

No.	名称	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.SystemClock_TOEuser_Modify_TimeSource	3	2	3	3	3	14
2	T.SystemClock_Inaccuracy_gradually	3	3	3	3	3	15
3	T.SystemClock_Inaccuracy_immediately	3	3	3	3	3	15
4	T.SystemClock_TOEuser_Modify_Clock_byTOE	3	2	3	3	3	14
5	T.SystemClock_TOEuser_Modify_Clock_byOS	3	2	3	3	3	14
6	T.SystemClock_Cracker_Modify_Clock	3	3	3	3	3	15
7	T.TAC_NTA_Crypto_Compromise_gradually	3	1	1	3	1	9
8	T.TAC_NTA_Crypto_Compromise_immediately	3	1	1	3	1	9
9	T.TAC_Line	3	2	3	3	3	14
10	T.Key_TOEuser_Compromise	3	2	3	3	3	14
11	T.Key_Cracker_Compromise	3	3	3	3	3	15
12	T.Config_TOEuser_Modify_byTOE	3	3	3	3	3	15
13	T.Config_TOEuser_Modify_byOS	3	3	3	3	3	15
14	T.Config_Cracker_Modify	3	3	3	3	3	15
15	T.Config_badTAC_TOEuser_Modify	3	2	3	3	3	14
16	T.Config_badTAC_Cracker_Modify	3	3	3	3	3	15
17	T.Config_stopTAC_TOEuser_Modify	3	2	3	3	3	14
18	T.Config_stopTAC_Cracker_Modify	3	3	3	3	3	15
19	T.Config_badTAC_TOEuser_ModifyTA	3	2	3	3	3	14
20	T.Config_badTAC_Cracker_ModifyTA	3	3	3	3	3	15
21	T.Log_TOEuser_Delete_byTOE	2	2	3	2	3	12
22	T.Log_TOEuser_Modify_byOS	2	2	3	2	3	12
23	T.Log_Cracker_Modify	2	3	3	2	3	13
24	T.SW_TOEuser_Modify_byOS	3	2	3	3	3	14
25	T.SW_Cracker_Modify	3	2	3	3	3	14
26	T.Password_TOEuser_Secret_byOS	3	2	3	3	3	14
27	T.Password_TOEuser_Secret_byMemo	3	2	3	3	3	14
28	T.Password_Cracker_Secret	3	3	3	3	3	15
29	T.Virus_TOEuser	3	3	3	3	3	15
30	T.Virus_Cracker	3	3	3	3	3	15
31	T.DoS	3	3	3	3	3	15
32	T.BufferOverFlow_Attack	3	3	3	3	3	15
33	T.Hardware_Failure	3	2	3	3	3	14
34	T.TOE_Bug	3	2	3	3	2	13
35	T.Peer_Failure_Asset	3	2	3	3	3	14

36	T.Peer_Failure_TimeSource	3	2	3	3	3	14
37	T.Connection_Failure_Asset	3	2	3	3	3	14
38	T.Connection_Failure_TimeSource	3	2	3	3	3	14

第5章 内部不正を考慮したセキュリティ評価

本章では、内部不正の考え方及び内部不正を考慮したセキュリティ環境を記載する。また、脅威に関する対策を記載する。

1. 内部不正の考え方

内部不正を考慮したセキュリティ評価として、内部不正のモデルを以下のように位置づける。

- 内部不正の範囲
  内部不正として、内部者の単独による不正を考慮する。
  下記のケースについては除外する。
  -外部者との結託
  -内部者の結託
  -内部者の単独による不正が同時に発生するケース

- セキュリティ環境
  内部不正を考慮しないセキュリティ環境を、内部不正を考慮した場合のセキュリティ環境にカスタマイズする。

2. 内部不正を考慮したセキュリティ環境

2-1 前提

以下に、TOE を使用する際のセキュリティ環境の前提を示す。

表 5-1　前提

No.	分類	項目	説明
1	物理的な前提	A.Location	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティの中に設置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2	人的な前提	A.TOE_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOEとTOEに含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOEを安全に導入、管理する。 ・TOEに関わるユーザ/役割を管理する。 ・時刻に関する管理業務を行う。 ・暗号機能に関わる初期化及び管理業務を行う。 ・TOE上で悪意のあるソフトウェアが動作しないようにする。 ・TOEの用件を満たす適切なディスクスペースを用意する。 ・TOEのデータベースを適切に管理する。 彼らは、単独による内部不正を行う可能性があるものとする。

3	人的な前提	A.TOE_Operator	一人以上の許可された運用者が割り当てられる。 ・TOEの起動・停止を実行する。 ・TOE管理者の指示の元で各種設定など運用業務を行う。 彼らは、単独による内部不正を行う可能性があるものとする。
4	人的な前提	A.TOE_Auditor	一人以上の許可された監査者が割り当てられる。 ・TOEが生成する監査データの分析等の監査業務を行う。 彼らは、単独による内部不正を行う可能性があるものとする。
5	人的な前提	A.TA1_TAC	TA1(認証連鎖方式の時刻配信局)は、時刻監査証明書を検証する。この中には、アウト・オブ・バンドの方法を用いて、NTA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なNTAによって行われたものかどうかの確認、が含まれる。
6	接続に関する前提	A.Device	周辺機器への接続は、コントロールされたアクセス・ファシリティ内に存在する。
7	接続に関する前提	A.FIREWALL	TOEと他システムとの接続には、専用線を用いる。TOEとセグメントが異なる場合は、ファイアウォールを設置する。
8	接続に関する前提	A.PEER	TOEと通信する意図された他システムは、信頼できる。
9	接続に関する前提	A.TA1_NTA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
10	接続に関する前提	A.TimeSource_NTA1_Connection	時刻ソースとTOEの間の通信路は、時刻ソースやTOEの成りすまし、データの改ざん、データの盗聴を防止する。
11	物理的な前提	A.Environment	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
12	物理的な前提	A.MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。

2-2 脅威

以下に、TOE および環境に対する脅威を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

なお、脅威の分類は以下のように区分した。

・分類：TOE

TOE のセキュリティ機能（例：時刻配信プロトコルなど）により対策可能。

・分類：環境

TOE のセキュリティ機能では対策不可能、環境の IT/非 IT 機能（例：外部の IDS システムにより対策、運用により対策）により対策可能。

※TOE のログ管理機能、TOE 管理機能を利用して対策する脅威は、こちらの区分に含めている。

表 5-2　脅威

No.	分類	項目	説明
1	環境	T.SystemClock_TOEuser_Modify_TimeSource_Malice	内部の不正者が、TOEが参照する時刻ソースを変更する。
2	環境	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が内部の不正者の攻撃により機能低下（故障）し、時刻がずれる。)

3	環境	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
4	環境	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(OSの機能を利用)
5	環境	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(外部から持ち込んだソフトウェアを利用)
6	環境	T.SystemClock_TOEuser_Imperson_Server_Malice	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。
7	環境	T.SystemClock_TOEuser_Modify_Data_Line_Malice	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。
8	TOE	T.TAC_TOEuser_Imperson_TOE_Malice	内部の不正者が、TOEに成りすましたサーバを利用してTAと通信を行う。
9	TOE	T.TAC_TOEuser_Modify_Data_Line_Malice	内部の不正者が、TOEとTAの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。
10	環境	T.Key_TOEuser_Compromise_Malice	内部の不正者がTOEの秘密鍵を暴露する。
11	環境	T.Config_TOEuser_Modify_byTOE_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(TOEの機能を利用)
12	環境	T.Config_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(OSの機能を利用)
13	環境	T.Config_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
14	環境	T.Config_badTAC_TOEuser_Modify_Malice	内部の不正者が、TOEの設定を変更し、不正な時刻監査証明書を発行する。
15	環境	T.Config_stopTAC_TOEuser_Modify_Malice	内部の不正者が、TOEの設定を変更し、時刻監査証明書の発行を停止させる。
16	環境	T.Config_badTAC_TOEuser_ModifyTA_Malice	内部の不正者が、TOEの設定を変更し、不正なTAに時刻監査証明書を送信する。
17	環境	T.Log_TOEuser_Delete_byTOE_Malice	内部の不正者が、TOEのログを削除･暴露する。(TOEの機能を利用) ※ログの変更は、TOEの機能を利用して実施することはできない。
18	環境	T.Log_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEのログを変更･削除･暴露する。(OSの機能を利用)
19	環境	T.Log_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEのログを変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
20	環境	T.SW_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEのソフトウェアを変更･削除･暴露する。(OSの機能を利用)
21	環境	T.SW_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEのソフトウェアを変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
22	環境	T.Password_TOEuser_Secret_byOS_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(OSの機能を利用)
23	環境	T.Password_TOEuser_Secret_byImportSW_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(外部から持ち込んだソフトウェアを利用)
24	環境	T.Password_TOEuser_Secret_byMemo_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(口頭、メモ、メール等)
25	環境	T.Virus_TOEuser_Malice	内部の不正者が、TOEにウィルスを感染させる。

26	環境	T.Crash_TOEuser_Malice	内部の不正者が、TOEを破壊し、サービスを停止させる。

2-3 組織のセキュリティポリシー

以下に、TOE を使用するにあたっての、組織のセキュリティポリシーを示す。

表 5-3　組織のセキュリティポリシー

No.	項目	説明
1	P.Cryptography	署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって実装されなければならない。
2	P.PKI_Management	安全に管理されたPKIの中で、TOEを運用すること。全ての鍵と証明書は、安全に発行、失効される。
3	P.Password_Management	TOEのパスワードは、TOE管理者およびTOE運用者によって適切に管理され、TOE管理者およびTOE運用者以外に知られてはならない。
4	P.Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。
5	P.Time_Source	TOEは、信頼のできる時刻ソースを参照すること。また、時刻ソースの信頼性と正確性は、TOE所有者にとって受容可能であること。
6	P.System_Clock_Management	TOEが参照する時計を信頼のできる時刻ソースと同期させる。
7	P.Check_Virus	定期的なウィルスチェックを実行する。 外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_TA1	TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
9	P.Dual_Control	TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
10	P.Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

3. セキュリティ目標・対策と実装システムの評価

3-1 脅威のセキュリティ目標・対策及び実装システムに対する評価

以下に、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

表 5-4　脅威のセキュリティ目標・対策及び実装システムに対する評価

No.	脅威名	セキュリティ目標･対策		統合化システムにおける実現
1	T.SystemClock_TOEuser_Modify_TimeSource_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査
		回復	･正しい時刻ソースからの時刻配信を受ける。	･正しい時刻ソースからの時刻配信を受ける。
2	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査
		回復	･時刻ソースからの時刻配信を受ける。	･時刻ソースからの時刻配信を受ける。
3	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	･時刻ソースからの時刻配信を受ける。	･時刻ソースからの時刻配信を受ける。
4	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則 ･運用管理(操作は、管理用端末からブラウザを利用して行う。)	･複数人による操作（運用） ･罰則 ･運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	･運用記録の監査	･運用記録の作成 ･運用記録の監査
		回復	･時刻ソースからの時刻配信を受ける。	･時刻ソースからの時刻配信を受ける。

5	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・時刻ソースからの時刻配信を受ける。	・時刻ソースからの時刻配信を受ける。
6	T.SystemClock_TOEuser_Imperson_Server_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
7	T.SystemClock_TOEuser_Modify_Data_Line_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・時刻ソースから再度時刻配信を受ける。	・時刻ソースから再度時刻配信を受ける。
8	T.TAC_TOEuser_Imperson_TOE_Malice	防止	・TLSによる相互認証 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる相互認証 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー

9	T.TAC_TOEuser_Modify_Data_Line_Malice	防止	・TLSによる通信路の保護 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる通信路の保護 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・NTAからTAに再度時刻配信を行う。	・NTAからTAに再度時刻配信を行う。
10	T.Key_TOEuser_Compromise_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
11	T.Config_TOEuser_Modify_byTOE_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
12	T.Config_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
13	T.Config_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア

14	T.Config_badTAC_TOEuser_Modify_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
15	T.Config_stopTAC_TOEuser_Modify_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
16	T.Config_badTAC_TOEuser_ModifyTSA_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
17	T.Log_TOEuser_Delete_byTOE_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
18	T.Log_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
19	T.Log_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー

20	T.SW_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
21	T.SW_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
22	T.Password_TOEuser_Secret_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
23	T.Password_TOEuser_Secret_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
24	T.Password_TOEuser_Secret_byMemo_Malice	防止	・罰則	・罰則
		検出	ー	ー
		回復	ー	ー

25	T.Virus_TOEuser_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ・ウィルスチェック	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) ・ウィルスチェック
		検出	ー	ー
		回復	ー	ー
26	T.Crash_TOEuser_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー

3-2 前提の実現方法例

以下に、セキュリティ環境の前提に関する実現方法例を記載する。

表 5-5　前提の実現方法例

No.	前提名	実現方法例
1	A.Location	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
2	A.TOE_Administrator	・TOE管理者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
3	A.TOE_Operator	・TOE運用者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
4	A.TOE_Auditor	・TOE監査者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
5	A.TA1_TAC	TA1(認証連鎖方式の時刻配信局)は、時刻監査証明書を検証する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、NTA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なNTAによって行われたものかどうかの確認、が含まれる。 ・TA1は、時刻監査証明書を検証するためのソフトウェアを持つ。
6	A.Device	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
7	A.FIREWALL	・TOEとTA1、時刻ソースは、専用線で接続し、TOEとセグメントが異なる場合は、ファイアウォールを設置する。 ・ファイアウォールの設定は、適切に維持・管理される。
8	A.PEER	・TOEと通信する意図された他システムは、信頼できる第三者(TTP)の運用するシステムであることを保証する。 ・TOEは、NTA1内のネットワークに接続された、日本標準時と同期した時刻ソースを参照する。
9	A.TA1_NTA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、専用線である。
10	A.TimeSource_NTA1_Connection	・時刻ソースとTOEの間の通信路は、専用線である。
11	A.Environment	・TOE の設置場所として、電磁波対策、電力対策、温度・湿度対策が行われている設備を利用する。
12	A.MEDIA	・定期的なデータのバックアップと、適切なシステムマイグレーションを行う。

3-3 組織のセキュリティポリシーの実現方法例

以下に、組織のセキュリティポリシーに関する実現方法例を記載する。

表 5-6　組織のセキュリティポリシーの実現方法例

No.	ポリシー名	実現方法例
1	P.Cryptography	･TOEの署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって行われる。
2	P.PKI_Management	TOEは、安全に管理されたPKIの中で運用されることを保証する。鍵/証明書は、運用マニュアルに基づき、安全に発行･失効される。
3	P.Password_Management	･TOE管理者およびTOE運用者は、パスワードを記憶し、他人に漏らさない。また、運用マニュアルに基づき、適切なパスワードを設定し、適切な頻度でパスワードを変更する。 ･TOE管理者およびTOE運用者は、ソーシャルエンジニアリングの教育を受けている。
4	P.Protect_Log	･TOE を利用する組織は、TOEの監査ログの暴露･改ざんまたは削除を防止するよう、TOE管理者、TOE運用者、TOE監査者に対して教育を行う。 ･TOEは、TOEの出力するシステムログにハッシュ値やデジタル署名を付与し、改ざんを検出可能な機能を持つ。 ･TOEは、TOEの保護対象資産へのアクセスを許可する前に、全ての利用者に対して識別･認証情報の入力を要求し、識別･認証を実施する。
5	P.Time_Source	TOEは、NTA1内のネットワークに接続された、日本標準時と同期した時刻ソースを参照する。
6	P.System_Clock_Management	TOEは、NTA1内のネットワークに接続された、日本標準時と同期した時刻ソースを参照する。
7	P.Check_Virus	TOE管理者は、運用マニュアルに基づき、定期的にTOEの全ファイルに対してウィルスチェックを行う。また、外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_TA1	TOEは、TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
9	P.Dual_Control	運用マニュアルに基づき、TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行う。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行う。
10	P.Check_Abstract_Vulnerability	TOE管理者は、運用マニュアルに基づき、定期的にOS やライブラリなどの脆弱性を確認し、対策を行う。

4. 脅威ツリー及びリスク評価一覧

4-1 脅威ツリー

以下に、脅威ツリーを示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

※欄の不足を補うため、一部「下位の条件→上位の条件」と矢印で表現している場合がある。

表 5-7　脅威ツリー

No.	資産	脅威	上位レベルが実現するための条件			脅威名
			条件1	条件2	条件3	
1	システム時刻	内部の不正者が、TOEが参照する時刻ソースを変更する。	内部の不正者が、TOEの設定情報を変更する。	—	—	T.SystemClock_TOEuser_Modify_TimeSource_Malice
2	システム時刻		TOEが参照する時計が内部の不正者の攻撃により機能低下（故障）し、時刻がずれる。	※具体的な攻撃方法は特に規定しない。	—	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice
3	システム時刻	内部の不正者が、TOEが参照する時計の時刻をずらす。	内部の不正者が、TOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	—	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice
4	システム時刻			OSの機能を用いてTOEの時刻を設定する。（TOEの機能以外の方法を用いてTOEの時刻を設定する。）※例：OSの時刻設定コマンド	OSにログインする	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice
5	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。（TOEの機能以外の方法を用いてTOEの時刻を設定する。）※例：悪意のソフトウェア	—	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice
6	システム時刻	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。	TOEと時刻ソースの間のネットワークにアクセスする。	TOEに成りすましたサーバを用意する。※秘密鍵は除外。秘密鍵以外についての成りすまし。	—	T.SystemClock_TOEuser_Imperson_Server_Malice
7	システム時刻	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	—	—	T.SystemClock_TOEuser_Modify_Data_Line_Malice
8	時刻監査証明書	内部の不正者が、TOEに成りすましたサーバを利用してTAと通信を行う。	TOEとTAの間のネットワークにアクセスする。	TOEに成りすましたサーバを用意する。※秘密鍵は除外。秘密鍵以外についての成りすまし。	—	T.TAC_TOEuser_Imperson_TOE_Malice

9	時刻監査証明書	内部の不正者が、TOEとTAの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEとTAの間のネットワークにアクセスする。	—	—	T.TAC_TOEuser_Modify_Data_Line_Malice
10	秘密鍵		内部の不正者がTOEの秘密鍵を暴露する。	[通信用鍵・署名用鍵] OSの機能を用いてTOEの秘密鍵を取得する。	OSにログインする	T.Key_TOEuser_Compromise_Malice
11	設定情報	内部の不正者が、TOEの設定情報を変更・削除・暴露する。	TOEの機能を用いてTOEの設定情報を変更・削除・暴露する。	—	—	T.Config_TOEuser_Modify_byTOE_Malice
12	設定情報		OSの機能を用いてTOEの設定情報を変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	—	T.Config_TOEuser_Modify_byOS_Malice
13	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：悪意のソフトウェア	—	—	T.Config_TOEuser_Modify_byImportSW_Malice
14	設定情報	内部の不正者が、TOEの設定を変更し、不正な時刻監査証明書を発行する。	TOEの設定情報を変更する。 ※[不正な時刻監査証明書の例] 本来のポリシ(OID,時刻監査規格(Offset,Delay)等)と異なる時刻監査証明書など。	TOEにアクセスする。	—	T.Config_badTAC_TOEuser_Modify_Malice
15	設定情報	内部の不正者が、TOEの設定を変更し、時刻監査証明書の発行を停止させる。	TOEの設定情報を変更する。	TOEにアクセスする。	—	T.Config_stopTAC_TOEuser_Modify_Malice
16	設定情報	内部の不正者が、TOEの設定を変更し、不正なTAに時刻監査証明書を送信する。	TOEの設定情報を変更する。	TOEにアクセスする。	—	T.Config_badTAC_TOEuser_ModifyTA_Malice
17	ログ	内部の不正者が、TOEのログを変更・削除・暴露する。	TOEの機能を用いてTOEのログを削除・暴露する。 ※ログの変更は、TOEの機能を利用して実施することはできない。	—	—	T.Log_TOEuser_Delete_byTOE_Malice

18	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例：設定ファイルを直接編集する。	OSにログインする	—	T.Log_TOEuser_Modify_byOS_Malice
19	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例：悪意のソフトウェア	—	—	T.Log_TOEuser_Modify_byImportSW_Malice
20	ソフトウェア	内部の不正者が、TOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：OSのコマンドを利用して削除する。	OSにログインする	—	T.SW_TOEuser_Modify_byOS_Malice
21	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	—	—	T.SW_TOEuser_Modify_byImportSW_Malice
22	ID・パスワード	内部の不正者が、TOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	OSにログインする	—	T.Password_TOEuser_Secret_byOS_Malice
23	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	—	—	T.Password_TOEuser_Secret_byImportSW_Malice
24	ID・パスワード		その他、口頭、メモ、メール等で情報が漏洩する。	—	—	T.Password_TOEuser_Secret_byMemo_Malice
25	その他	内部の不正者が、TOEにウィルスを感染させる。	ウィルスに感染した外部メディアにアクセスする。	OSにログインする	ウィルスに感染した外部メディアを持ち込む。	T.Virus_TOEuser_Malice
26	その他		外部からウィルスをダウンロードする。	外部にアクセスする。	OSにログインする	同上
27	その他	内部の不正者が、TOEを破壊し、サービスを停止させる。	TOEを破壊する。	TOEの設置された部屋に入室する。	—	T.Crash_TOEuser_Malice

4-2 リスク評価格付けの考え方

以下に、リスク評価格付けの考え方を示す。

表 5-8　リスク評価格付けの考え方

	格付け	高(3)	中(2)	低(1)
D	潜在的損失（Damage potential）	<方針> ・信頼性・サービスレベルに影響のあるもの。 ・データを直接悪用できるもの。 ＜対象＞ その他	<方針> ・データを直接は悪用できないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
R	再現性（Reproducibility）	＜方針＞ ・時期によらないもの。 ・内部不正など、攻撃者の意図でいつでも実施できるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ＜対象＞ ・内部不正 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・その他	＜方針＞ ・攻撃者の意図によらないもの。 ・TOE開発時のソフトウェア不良 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ＜対象＞ ・不注意（基本的に発生率は低い、という前提。） ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。) ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断（基本的に発生率は低い、という前提。）	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・暗号脆弱化 ・パケットの暴露・改ざん ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化

E	攻撃利用可能性（Exploitability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃できるもの。 ・攻撃方法が容易なもの。 ・比較的攻撃ツールが入手しやすいと思われるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他	＜方針＞ なし ＜対象＞ なし	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん
A	影響ユーザ（Affected users）	<方針> ・TOEのサービスの利用者に関わるもの。 ・TOE利用者自身に大きな影響があるもの。 ＜対象＞ ・その他	<方針> ・TOEのサービスの利用者に対する直接的な影響がないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
D	発見可能性（Discoverability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃方法を知る事ができるもの。 ・攻撃方法が容易に思いつくもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退	＜方針＞ ・TOE開発時のソフトウェア不良 ＜対象＞ ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

		・他システムの秘密鍵危殆化 ・その他		

4-3 リスク評価点

以下に、脅威に対するリスク評価点を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

表 5-9　リスク評価点

No.	名称	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.SystemClock_TOEuser_Modify_TimeSource_Malice	3	3	3	3	3	15
2	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice	3	3	3	3	3	15
3	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	3	3	3	3	3	15
4	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	3	3	3	3	3	15
5	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	3	3	3	3	3	15
6	T.SystemClock_TOEuser_Imperson_Server_Malice	3	3	3	3	3	15
7	T.SystemClock_TOEuser_Modify_Data_Line_Malice	3	3	3	3	3	15
8	T.TAC_TOEuser_Imperson_TOE_Malice	3	3	3	3	3	15
9	T.TAC_TOEuser_Modify_Data_Line_Malice	3	3	3	3	3	15
10	T.Key_TOEuser_Compromise_Malice	3	3	3	3	3	15
11	T.Config_TOEuser_Modify_byTOE_Malice	3	3	3	3	3	15
12	T.Config_TOEuser_Modify_byOS_Malice	3	3	3	3	3	15
13	T.Config_TOEuser_Modify_byImportSW_Malice	3	3	3	3	3	15
14	T.Config_badTAC_TOEuser_Modify_Malice	3	3	3	3	3	15
15	T.Config_stopTAC_TOEuser_Modify_Malice	3	3	3	3	3	15
16	T.Config_badTAC_TOEuser_ModifyTA_Malice	3	3	3	3	3	15
17	T.Log_TOEuser_Delete_byTOE_Malice	2	3	3	2	3	13
18	T.Log_TOEuser_Modify_byOS_Malice	2	3	3	2	3	13
19	T.Log_TOEuser_Modify_byImportSW_Malice	2	3	3	2	3	13
20	T.SW_TOEuser_Modify_byOS_Malice	3	3	3	3	3	15
21	T.SW_TOEuser_Modify_byImportSW_Malice	3	3	3	3	3	15
22	T.Password_TOEuser_Secret_byOS_Malice	3	3	3	3	3	15
23	T.Password_TOEuser_Secret_byImportSW_Malice	3	3	3	3	3	15
24	T.Password_TOEuser_Secret_byMemo_Malice	3	3	3	3	3	15
25	T.Virus_TOEuser_Malice	3	3	3	3	3	15

26	T.Crash_TOEuser_Malice	3	3	3	3	3	15

セキュリティ評価報告書

（TOE：TA1 ）

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

本章では、TOE の機能概要、TOE 構成図、利用する暗号技術と暗号コンポーネント構成図、関与者、資産について記載する。

1. TOE の機能概要

1-1 TOE の機能

以下に、TOE を構成する機能の概要を示す。

(1)時刻配信機能（時刻配信プロトコルを含む）

TOE は、時刻配信プロトコル（認証連鎖方式*1）により時刻の配信・監査を行う機能を持つ。

(2)時刻受信機能（時刻配信プロトコルを含む）

TOE は、時刻配信プロトコル（認証連鎖方式）によって配信される時刻情報を受信するための機能を持つ。受信した時刻情報により、システム時刻が補正される。

(3)時刻管理機能

TOE の時刻配信機能・時刻受信機能やログ管理機能の時刻には、システム時刻が使用される。

(4)ログ管理機能

TOE は、TOE の動作記録、時刻配信・時刻受信記録、操作記録などをログとして保管することが可能である。ログは、署名を付与し保護することが可能である。

(5)鍵管理機能

TOE は、通信用(TLS)の秘密鍵および署名用の秘密鍵を管理する機能を持つ。

(6)証明書管理機能

TOE は、通信(TLS)および署名・検証に関わる証明書を管理する機能を持つ。

(7)設定管理機能

TOE は、TOE の機能に関わる設定を管理する機能を持つ。

(8)TOE 管理機能

TOE の設定・操作は、ブラウザから管理画面にアクセスして実施する。

＊１：ここでいう認証連鎖方式とは、PKI(Public Key Infrastructure)認証技術を利用し

て TA が時刻配信先の時計を特定すると同時に時刻の計測と配信を行い、その計測結果を時刻監査記録として更に時刻配信先の時計に連鎖していく方式。

1-2 TOE 構成図

以下に、統合化プラットフォームシステムにおいて TOE が使用される際のシステム構成図を示す。(強調表示されたコンポーネントは、評価対象外である。)

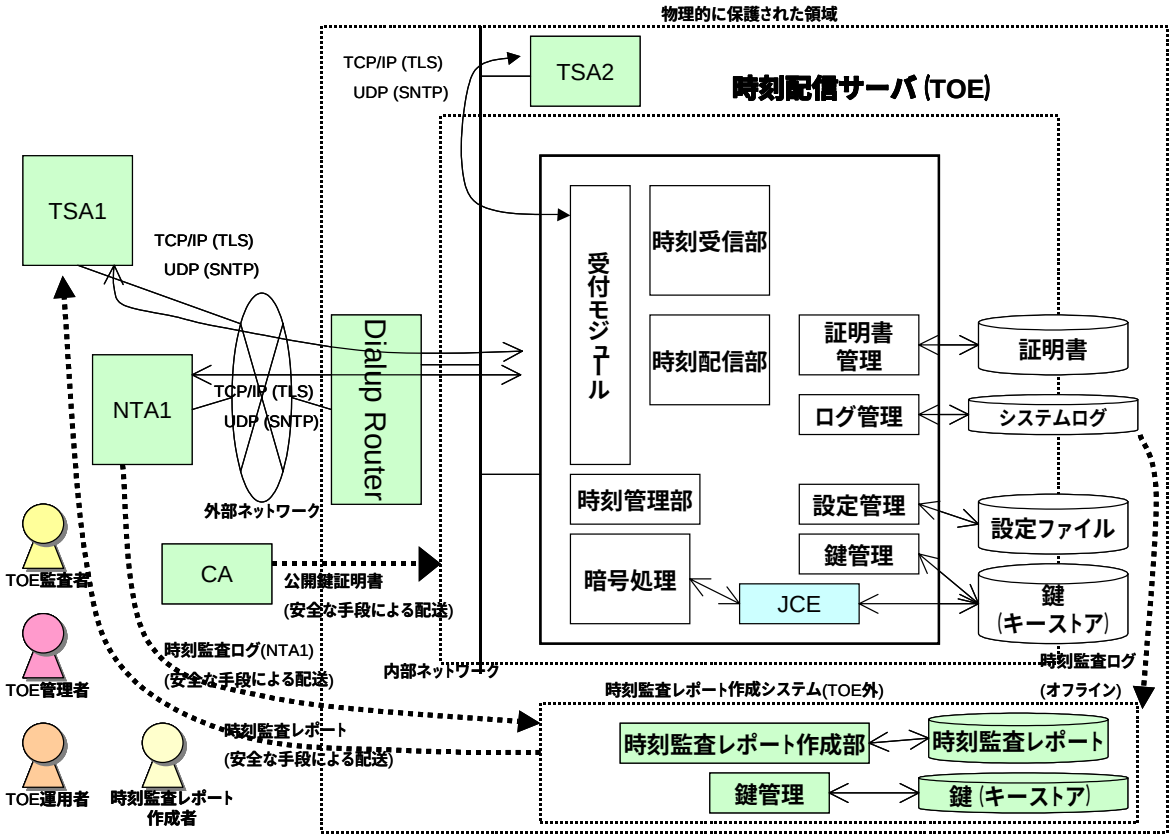


図 1-1　システム構成図

1-3 利用する暗号技術と暗号コンポーネント

以下に、TOE の利用する暗号技術と、暗号コンポーネント構成図を示す。

表 1-1　TOE の利用する暗号技術

#	システム	使用している暗号技術		使用目的
1	TA1	TLS	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット RSAES-PKCS1-v1_5 鍵長 1024 ビット 【共通鍵暗号方式】 128-bit RC4 【ハッシュ関数】 MD5	通信先の認証・通信データの改ざん防止 (時刻配信・受信)
		SNTP	【メッセージ認証方式】 HMAC(MD5)	通信データの改ざん防止
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	時刻監査証明書への署名
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	ログへの署名
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット、鍵長 2048 ビット 【ハッシュ関数】 SHA-1	公開鍵証明書の検証、ARL/CRL の検証、時刻監査証明書の検証
		ハッシュ関数	SHA-1	ログの改ざん防止
		時刻監査レポート	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	時刻監査レポートへの署名

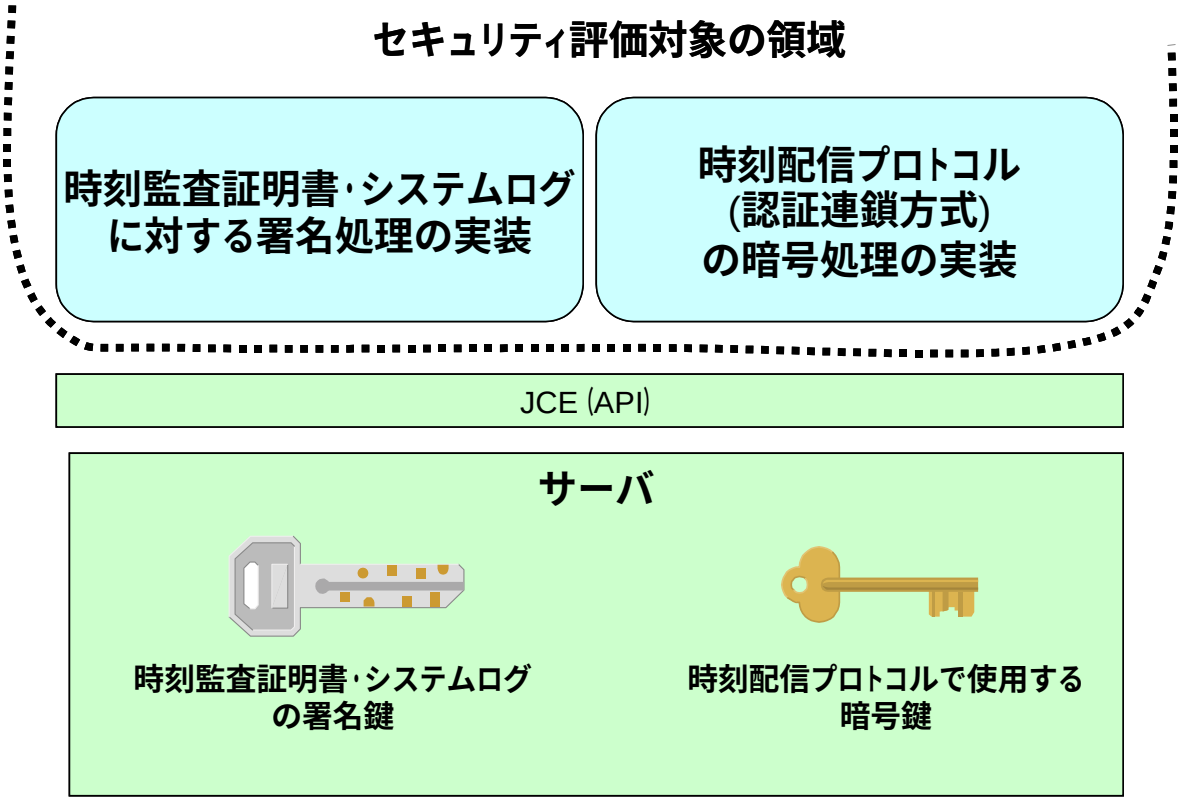


図 1-2　セキュリティ評価対象の領域

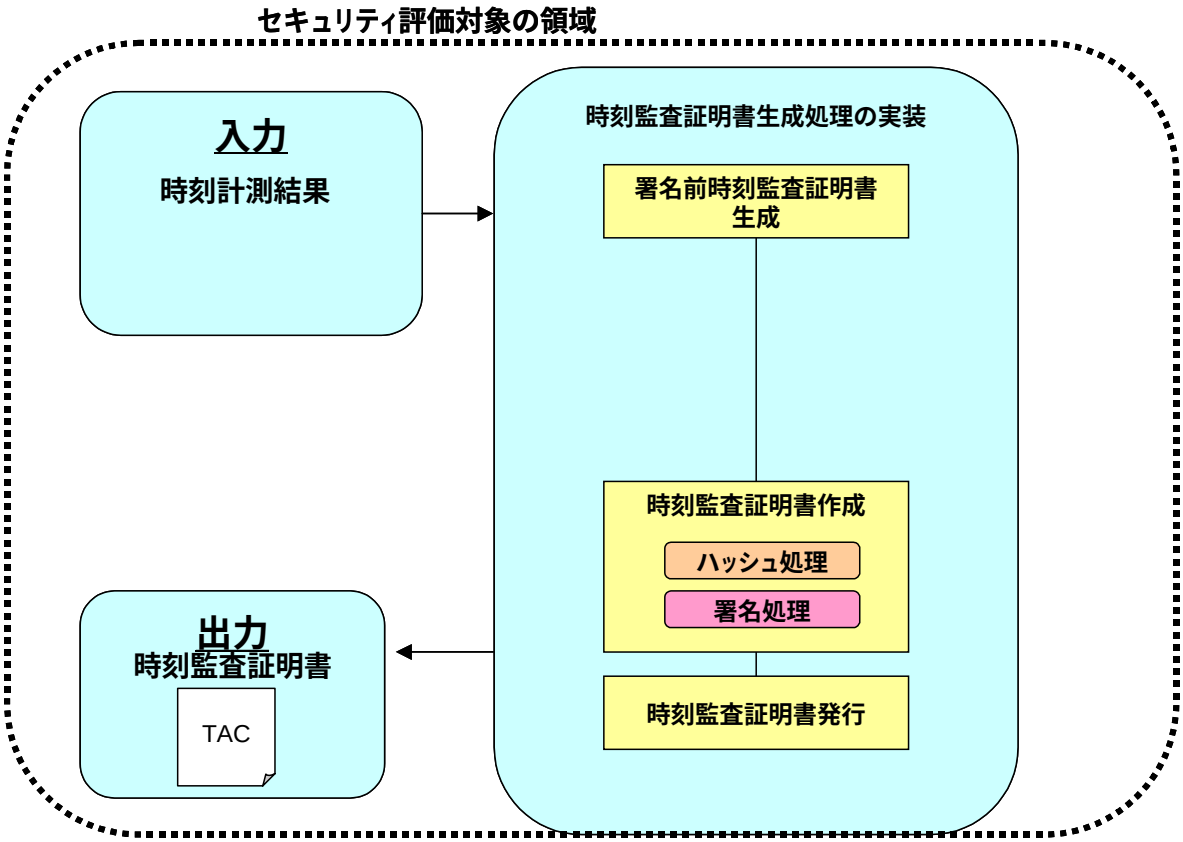


図 1-3　時刻監査証明書生成処理概要

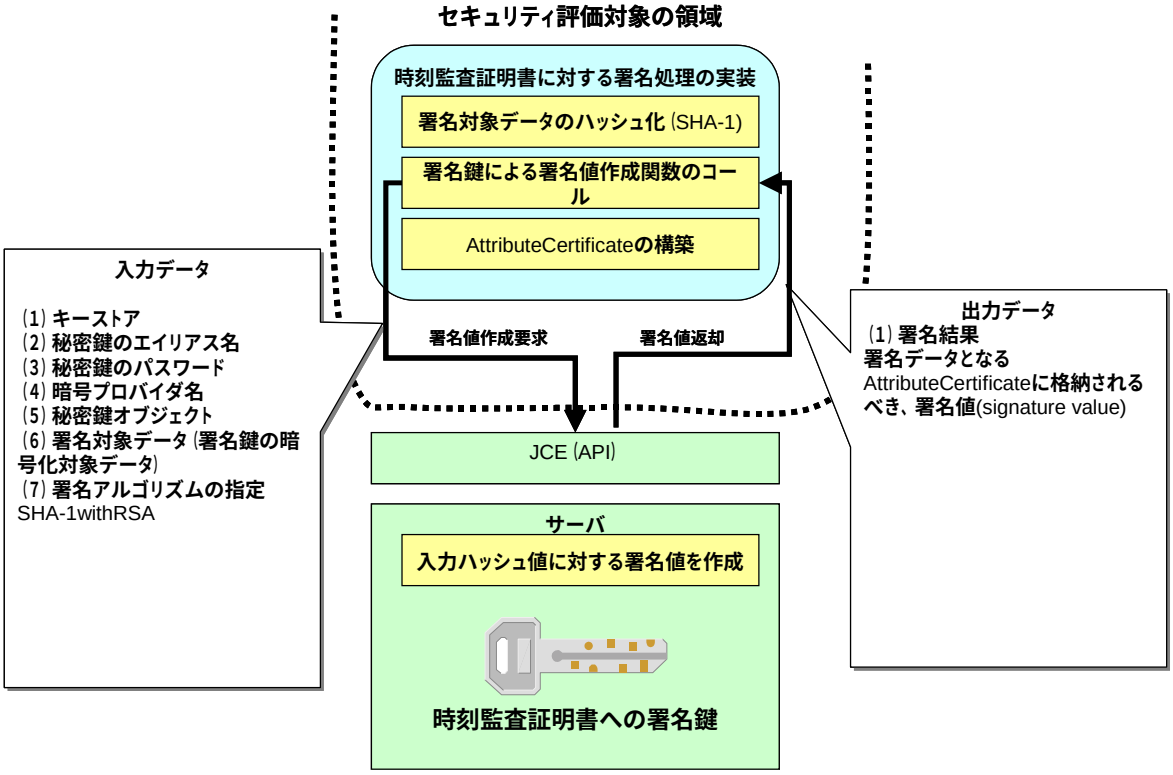
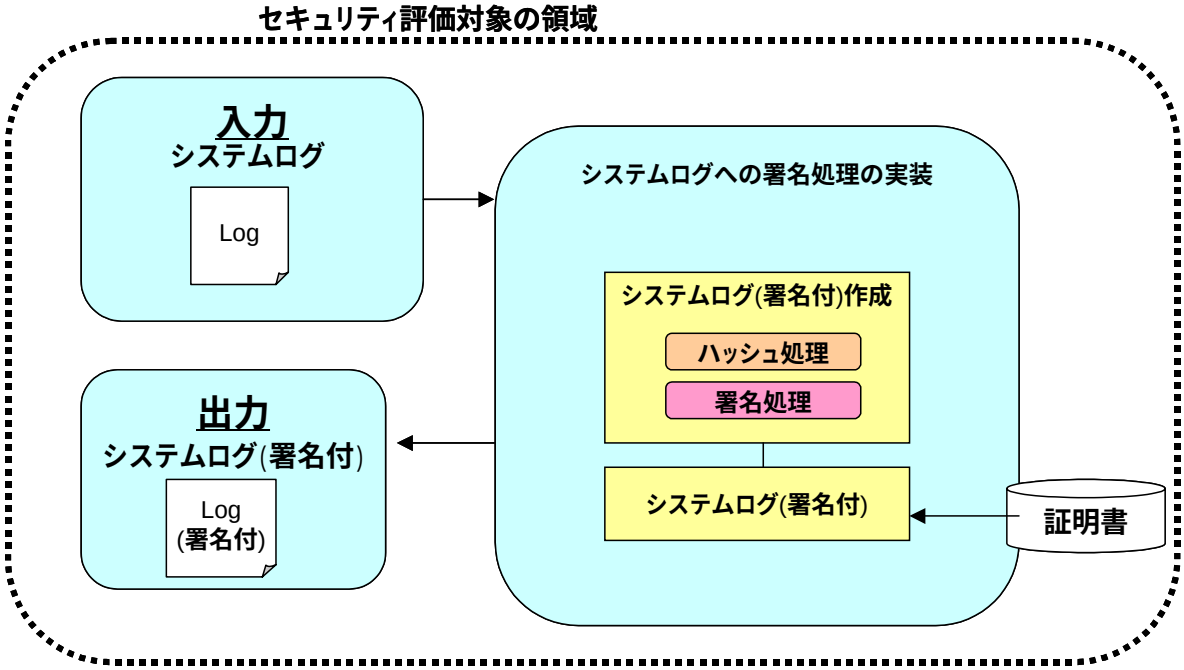


図 1-4　時刻監査証明書生成処理実装（署名処理実装）概要



※署名対象データは、システムログ内のハッシュ値

図 1-5　システムログへの署名処理概要

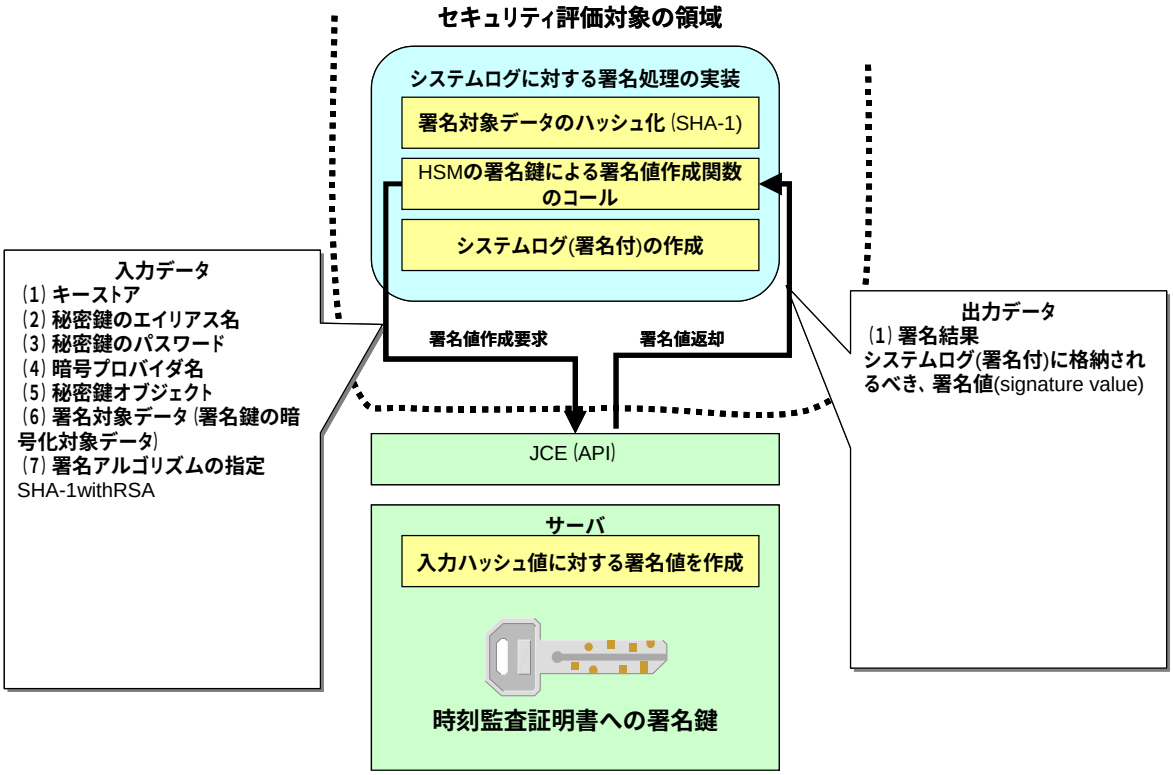


図 1-6　システムログへの署名処理実装概要

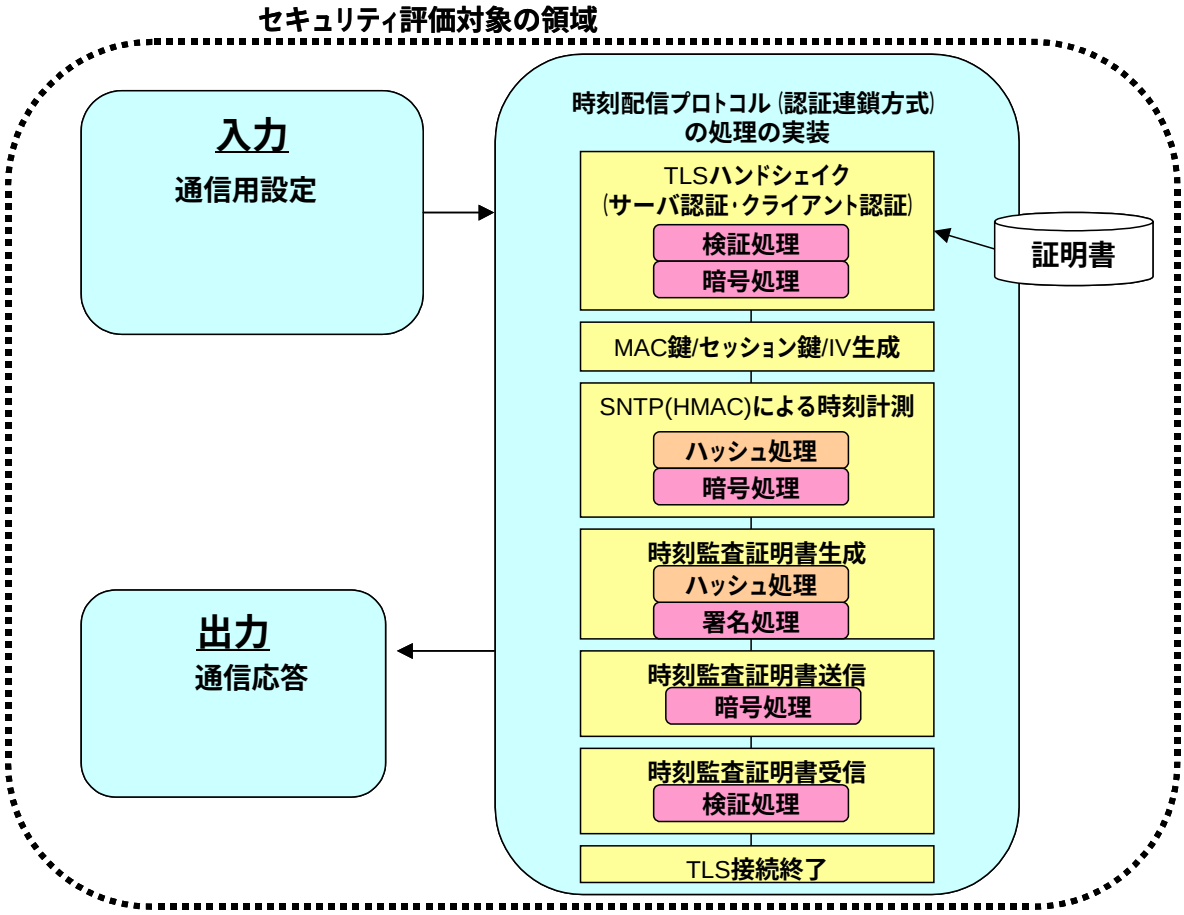


図 1-7　時刻配信プロトコル（認証連鎖方式：配信）処理概要

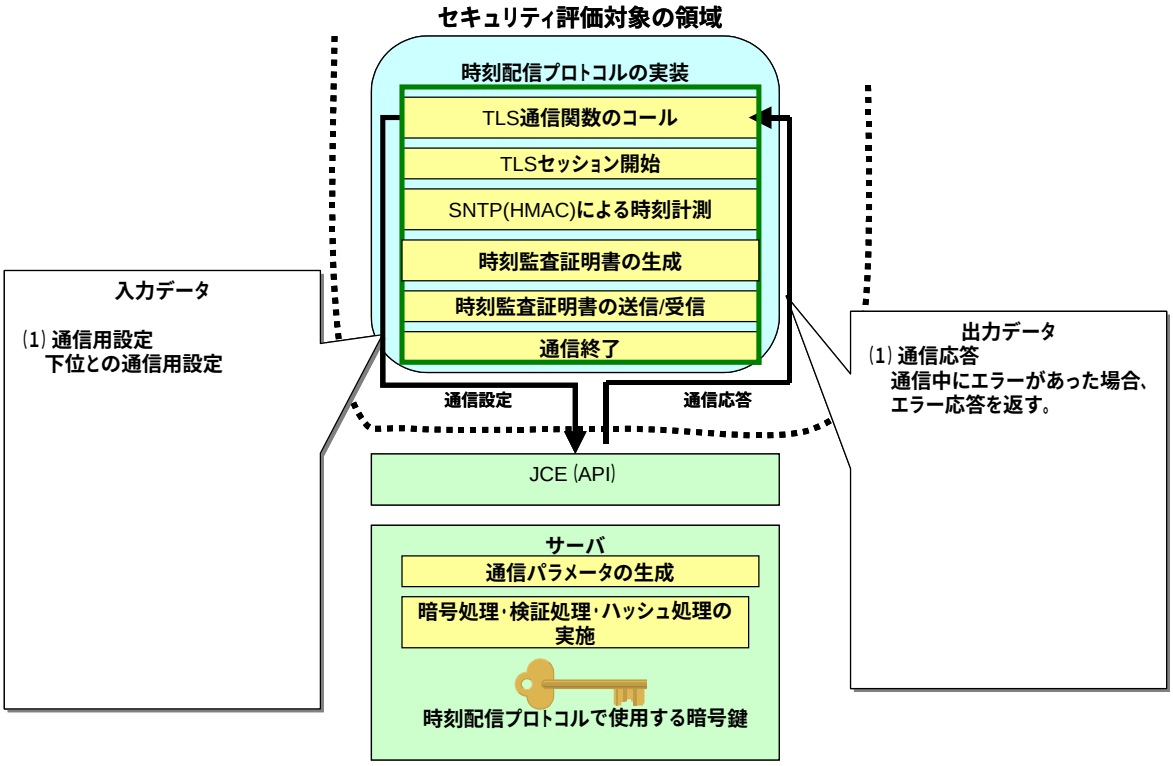


図 1-8　時刻配信プロトコル(認証連鎖方式：配信)処理実装（暗号処理実装）概要

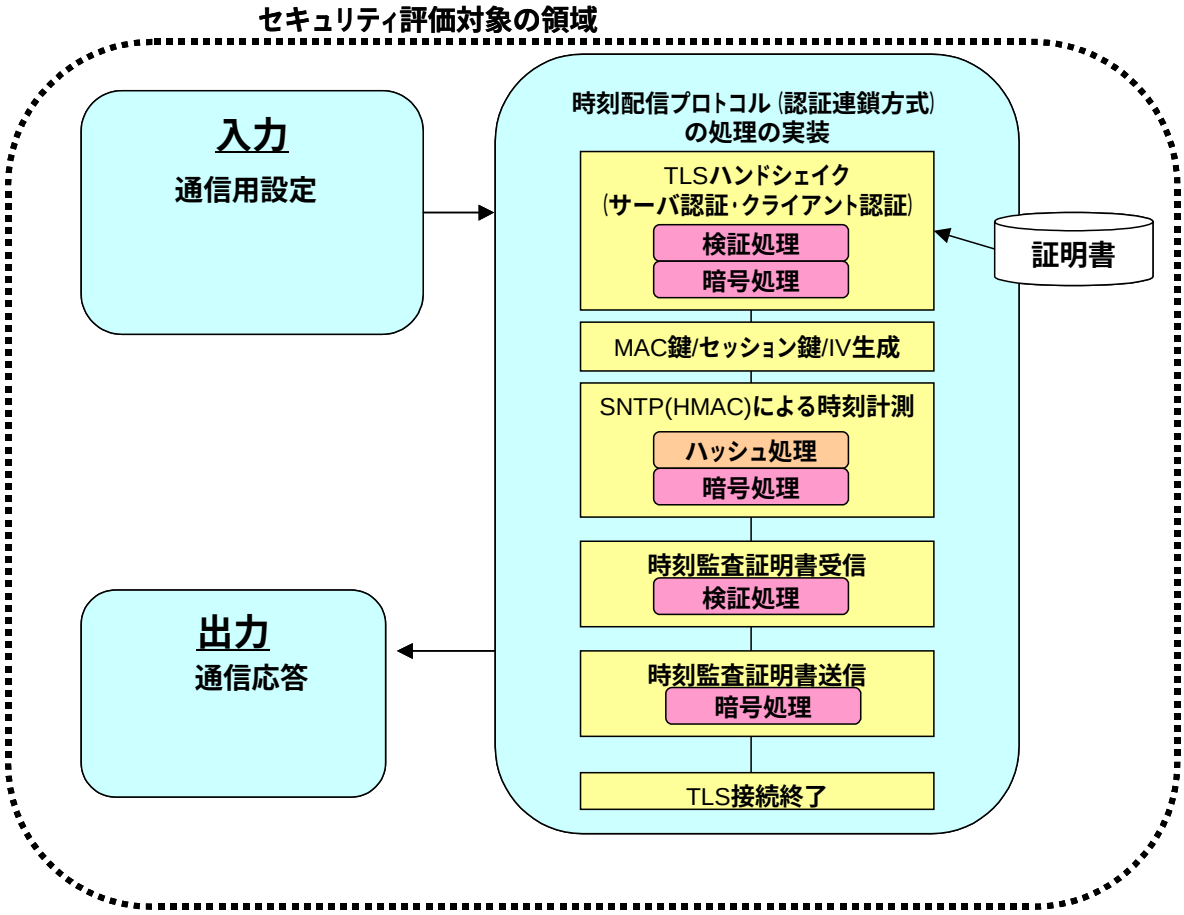


図 1-9　時刻配信プロトコル（認証連鎖方式：受信）処理概要

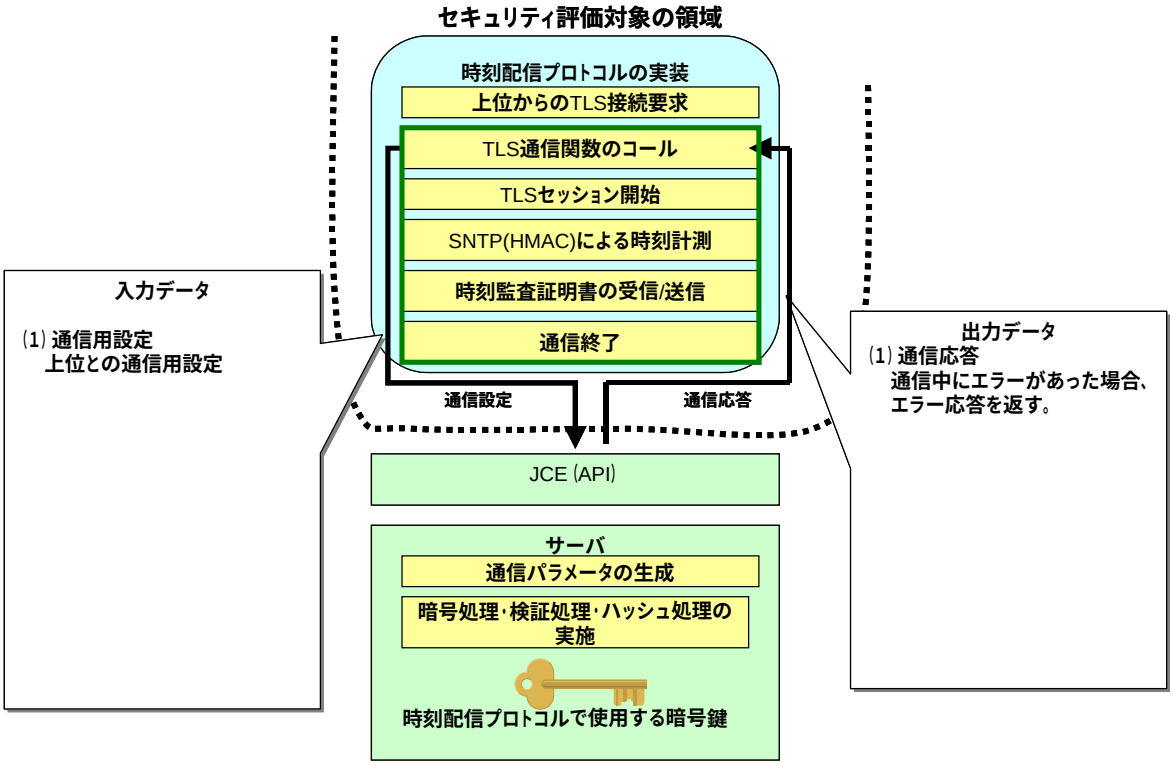


図 1-10　時刻配信プロトコル(認証連鎖方式：受信)処理実装（暗号処理実装）概要

1-4 関与者

以下に、TOE の関与者を示す。

表 1-2　TOE の関与者

#	関与者	説明
1	TOE 管理者	TOE に関わるユーザ/役割を管理する。 時刻に関する管理業務を行う。 暗号機能に関わる初期化及び管理業務を行う。 悪意のあるソフトウェアが動作しないようにする。 適切なディスクスペースを用意する。 データベースを適切に管理する。 時刻監査レポート作成者を管理する。
2	TOE 運用者	TOE の起動・停止を実行する。 TOE 管理者の指示の元で各種設定など運用業務を行う。
3	TOE 監査者	TOE が生成する監査データの分析等の監査業務を行う。
4	時刻監査レポート作成者	TOE 管理者の指示の元で時刻監査レポートの作成･送付を行う。
5	TSA1	リンクトークン方式＊1の時刻認証局。 TOE から認証連鎖方式による時刻の配信および監査を受ける。
6	TSA2	独立トークン方式＊2の時刻認証局。 TOE から認証連鎖方式による時刻の配信および監査を受ける。

＊１：ここでいうリンクトークン方式タイムスタンプとは、TSA がタイムスタンプ対象データのハッシュ値に対して他のハッシュ値と関連付けるリンク情報を生成し、その時点までに生成したタイムスタンプと関連性を明らかにして有効性を証明する方式。

＊２：ここでいう独立トークン方式タイムスタンプとは、TSA がタイムスタンプ対象データのハッシュ値に対してデジタル署名を行い、それぞれのタイムスタンプの有効性を証明する方式。

1-5 資産

以下に、TOE の資産を示す。

表 1-3　TOE の資産

No.	分類	データ名	資産名
1	鍵/キーストア	秘密鍵(TA-署名)	秘密鍵
2		秘密鍵(TA-TLS)	秘密鍵
3		証明書(CA)	設定情報
4		証明書(TA-署名)	設定情報
5		証明書(TA-TLS)	設定情報
6	設定ファイル	配信先設定	設定情報
7		ポリシ設定	設定情報
8		上位TA設定	設定情報
9		うるう秒設定	設定情報
10		ID･パスワード	ID･パスワード
11		各種設定	設定情報
12	システムログ	システムログ	ログ
13		時刻監査ログ	ログ
14		操作ログ	ログ
15	証明書	CA証明書	設定情報
16		NTA証明書(署名)	設定情報
17		NTA証明書(TLS)	設定情報
18		TSA証明書(署名)	設定情報
19		TSA証明書(TLS)	設定情報
20		ARL	設定情報
21		CRL	設定情報
22	時刻	時刻受信	システム時刻
23		時刻配信	システム時刻
24		ロギング	システム時刻
25	時刻監査レポート	時刻監査レポート	時刻監査レポート
26	ソフトウェア	時刻情報配信ソフトウェア	ソフトウェア
27	時刻監査証明書	時刻監査証明書	時刻監査証明書

第2章 セキュリティ環境

本章では、内部不正を考慮しないセキュリティ環境（前提、脅威、組織のセキュリティポリシー）について記載する。

1. 前提

以下に、TOE を使用する際のセキュリティ環境の前提を示す。

表 2-1 前提

No.	分類	項目	説明
1	物理的な前提	A.Location	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティの中に設置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2	人的な前提	A.TOE_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOEとTOEに含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOEを安全に導入、管理する。 ・TOEに関わるユーザ/役割を管理する。 ・時刻に関する管理業務を行う。 ・暗号機能に関わる初期化及び管理業務を行う。 ・TOE上で悪意のあるソフトウェアが動作しないようにする。 ・TOEの用件を満たす適切なディスクスペースを用意する。 ・TOEのデータベースを適切に管理する。 ・時刻監査レポート作成者を管理する。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
3	人的な前提	A.TOE_Operator	一人以上の許可された運用者が割り当てられる。 ・TOEの起動・停止を実行する。 ・TOE管理者の指示の元で各種設定など運用業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
4	人的な前提	A.TOE_Auditor	一人以上の許可された監査者が割り当てられる。 ・TOEが生成する監査データの分析等の監査業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
5	人的な前提	A.TSA_TAC	TSA1(リンクトークン方式の時刻認証局)およびTSA2(独立トークン方式の時刻認証局)は、時刻監査証明書を検証する。この中には、アウト・オブ・バンドの方法を用いて、TA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なTAによって行われたものかどうかの確認、が含まれる。
6	人的な前提	A.TSA_Report	TSA1(リンクトークン方式の時刻認証局)は、時刻監査レポートを検証及び保持する。この中には、アウト・オブ・バンドの方法を用いて、TAの時刻監査レポート用証明書が失効していないかどうかの確認、時刻監査レポートの署名は、正当なTAによって行われたものかどうかの確認、が含まれる。
7	人的な前提	A.TOE_Separation	TOEが動作するサーバマシンには、TOEの動作に必要なソフトウェア以外はインストールされないものとする。
8	接続に関する前提	A.Device	周辺機器への接続は、コントロールされたアクセス・ファシリティ内に存在する。
9	接続に関する前提	A.FIREWALL	TOEと他システムとの接続には、専用線を用いる。TOEとセグメントが異なる場合は、ファイアウォールを設置する。
10	接続に関する前提	A.PEER	TOEと通信する意図された他システムは、信頼できる。

11	その他	A.Abstract	TOEが動作するために必要なOSや依存するライブラリは、不正な改変から保護され、正しく動作する。
12	接続に関する前提	A.TSA1_TA1_Connection	TSA1(リンクトークン方式の時刻認証局)とTOEの間の通信路は、TSA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
13	接続に関する前提	A.TSA2_TA1_Connection	TSA2(独立トークン方式の時刻認証局)とTOEの間の通信路は、TSA2やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
14	接続に関する前提	A.NTA1_TA1_Connection	NTA1(認証連鎖方式の国家時刻標準局)とTOEの間の通信路は、NTA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
15	物理的な前提	A.Environment	TOE の設置場所は、電磁波対策、電力対策、温度･湿度対策が行われている。
16	物理的な前提	A.MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
17	その他	A.Report_Editor	･時刻監査レポートの作成には、一人以上の許可された時刻監査レポート作成者が割り当てられる。さらに時刻監査レポート作成者は、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
18	その他	A.Report_System	･時刻監査レポート作成システム(TOE外)は、セキュリティ上安全なものとする。

2. 脅威

以下に、TOE および環境に対する脅威を示す。

なお、脅威の分類は以下のように区分した。

・分類：TOE

TOE のセキュリティ機能（例：時刻配信プロトコルなど）により対策可能。

・分類：環境

TOE のセキュリティ機能では対策不可能、環境の IT/非 IT 機能（例：外部の IDS システムにより対策、運用により対策）により対策可能。

※TOE のログ管理機能、TOE 管理機能を利用して対策する脅威は、こちらの区分に含めている。

表 2-2　脅威

No.	分類	項目	説明
1	TOE	T.SystemClock_TOEuser_Modify_TimeSource	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。
2	TOE	T.SystemClock_Inaccuracy_gradually	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。)
3	TOE	T.SystemClock_Inaccuracy_immediately	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が故障し、急に時刻がずれる。)
4	TOE	T.SystemClock_TOEuser_Modify_Clock_byTOE	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
5	TOE	T.SystemClock_TOEuser_Modify_Clock_byOS	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(OSの機能を利用)
6	TOE	T.SystemClock_Cracker_Modify_Clock	外部の不正者が、ネットワーク経由でTOEが参照する時計の時刻をずらす。
7	環境	T.TAC_TA_Crypto_Compromise_gradually	過去に発行した時刻監査証明書に使用されている暗号アルゴリズムが脆弱化する。(計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。)

8	環境	T.TAC_TA_Crypto_Compromise_immediately	過去に発行した時刻監査証明書に使用されている暗号アルゴリズムが脆弱化する。 (暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。)
9	環境	T.TAC_Line	TSA-TOE間のネットワークが、事故などにより遮断され、TOEの送信した時刻監査証明書がTSAに到達しない。
10	環境	T.Report_TA_Crypto_Compromise_gradually	過去に発行した時刻監査レポートに使用されている暗号アルゴリズムが脆弱化する。 (計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。)
11	環境	T.Report_TA_Crypto_Compromise_immediately	過去に発行した時刻監査レポートに使用されている暗号アルゴリズムが脆弱化する。 (暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。)
12	環境	T.Key_TOEuser_Compromise	許可された利用者が、不注意によりTOEの秘密鍵を暴露する。
13	環境	T.Key_Cracker_Compromise	外部の不正者が、ネットワーク経由でTOEの秘密鍵を盗む。
14	環境	T.Config_TOEuser_Modify_byTOE	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。(TOEの機能を利用)
15	環境	T.Config_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。(OSの機能を利用)
16	環境	T.Config_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定情報を変更･削除･暴露する。
17	環境	T.Config_badTAC_TOEuser_Modify	許可された利用者が、不注意によりTOEの設定を変更し、不正な時刻監査証明書を発行する。
18	環境	T.Config_badTAC_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正な時刻監査証明書を発行する。
19	環境	T.Config_stopTAC_TOEuser_Modify	許可された利用者が、不注意によりTOEの設定を変更し、時刻監査証明書の発行を停止させる。
20	環境	T.Config_stopTAC_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定を変更し、時刻監査証明書の発行を停止させる。
21	TOE	T.Config_badTAC_TOEuser_ModifyTSA	許可された利用者が、不注意によりTOEの設定を変更し、異なるTSAに時刻監査証明書を送信する。
22	環境	T.Config_badTAC_Cracker_ModifyTSA	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正なTSAに時刻監査証明書を送信する。
23	環境	T.Log_TOEuser_Delete_byTOE	許可された利用者が、不注意により、TOEのログを削除･暴露する。(TOEの機能を利用) ※ログの変更は、TOEの機能を利用して実施することはできない。
24	環境	T.Log_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEのログを変更･削除･暴露する。(OSの機能を利用)
25	環境	T.Log_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEのログを変更･削除･暴露する。
26	環境	T.SW_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEのソフトウェアを変更･削除･暴露する。(OSの機能を利用)
27	環境	T.SW_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEのソフトウェアを変更･削除･暴露する。
28	環境	T.Password_TOEuser_Secret_byOS	許可された利用者が、不注意により、TOEのID･パスワードを暴露する。(OSの機能を利用)
29	環境	T.Password_TOEuser_Secret_byMemo	許可された利用者が、不注意により、TOEのID･パスワードを暴露する。(口頭、メモ、メール等)
30	環境	T.Password_Cracker_Secret	外部の不正者が、ネットワーク経由でTOEのID･パスワードを暴露する。
31	環境	T.Virus_TOEuser	許可された利用者が、不注意により、TOEにウィルスを感染させる。
32	環境	T.Virus_Cracker	外部の不正者が、ネットワーク経由でTOEにウィルスを感染させる。
33	環境	T.DoS	外部の不正者から大量のアクセスが行われ、TOEをサービス不能にさせる。
34	環境	T.BufferOverFlow_Attack	外部の不正者が、バッファ･オーバーフローの脆弱性を利用し、TOEの管理者権限を取得する。
35	環境	T.Hardware_Failure	･経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産が失われる。 ･経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産の完全性が保証できなくなる。 ･経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、TOEが提供するサービスが継続できない。

36	環境	T.TOE_Bug	TOEのIT実装にソフトウェア不良が存在するため、TOEの資産の信頼性が乏しくなる。 例) ・ある条件下で、ログの書き込みが行われない。 ・ある条件下で、ログファイルを破壊する。
37	環境	T.Peer_Failure_Asset	通信相手となる他システムのダウンにより、TOEの資産が失われる。
38	環境	T.Peer_Failure_NTA1	NTA1(認証連鎖方式の国家時刻標準局)のダウンにより、TOEが提供するサービスが継続できない。
39	環境	T.Connection_Failure_Asset	TOEと通信相手となる他システムの間の通信回線の故障により、TOEの資産が失われる。
40	環境	T.Connection_Failure_NTA1	NTA1(認証連鎖方式の国家時刻標準局)との間の通信回線の故障により、TOEが提供するサービスが継続できない。

3. 組織のセキュリティポリシー

以下に、TOE を使用するにあたっての、組織のセキュリティポリシーを示す。

表 2-3　組織のセキュリティポリシー

No.	項目	説明
1	P.Cryptography	署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって実装されなければならない。
2	P.PKI_Management	安全に管理されたPKIの中で、TOEを運用すること。全ての鍵と証明書は、安全に発行、失効される。
3	P.Password_Management	TOEのパスワードは、TOE管理者およびTOE運用者によって適切に管理され、TOE管理者およびTOE運用者以外に知られてはならない。
4	P.Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。
5	P.Time_Source	TOEは、信頼のできる時刻ソースを参照すること。また、時刻ソースの信頼性と正確性は、TOE所有者にとって受容可能であること。
6	P.System_Clock_Management	TOEが参照する時計を信頼のできる時刻ソースと同期させる。
7	P.Check_Virus	定期的なウィルスチェックを実行する。 外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_NTA1	NTA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
9	P.Check_Received_Data_TSA1	TSA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
10	P.Check_Received_Data_TSA2	TSA2から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
11	P.Dual_Control	TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
12	P.Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

第3章 セキュリティ目標・対策と実装システムの評価

本章では、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を記載する。また、セキュリティ環境の前提と組織のセキュリティポリシーに関する実現方法例を記載する。

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

以下に、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を示す。

表 3-1　脅威のセキュリティ目標・対策及び実装システムに対する評価

No.	脅威名	セキュリティ目標･対策		統合化システムにおける実現
1	T.SystemClock_TOEuser_Modify_TimeSource	防止	･教育 (･複数人による操作(運用または機能での実現)) (･罰則)	･教育 (･複数人による操作(運用)) (･罰則)
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能:ログ管理機能
		回復	･正しいNTAからの時刻配信を受ける。	･正しいNTAからの時刻配信を受ける。 ※関連するTOEの機能:時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
2	T.SystemClock_Inaccuracy_gradually	防止	･NTAからの時刻配信を受ける。	･NTAからの時刻配信を受ける。 ※関連するTOEの機能:時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
		検出	･ログの確認 (定期的な時刻誤差の確認) ･NTAが時刻監査の結果をTAに伝える。	･ログの確認 (定期的な時刻誤差の確認) ※関連するTOEの機能:ログ管理機能 ･NTAが時刻監査の結果をTAに伝える。
		回復	ー	ー
3	T.SystemClock_Inaccuracy_immediately	防止	ー	ー
		検出	･ログの確認 (定期的な時刻誤差の確認) ･NTAが時刻監査の結果をTAに伝える。	･ログの確認 (定期的な時刻誤差の確認) ※関連するTOEの機能:ログ管理機能 ･NTAが時刻監査の結果をTAに伝える。
		回復	･NTAからの時刻配信を受ける。	･NTAからの時刻配信を受ける。 ※関連するTOEの機能:時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
4	T.SystemClock_TOEuser_Modify_Clock_byTOE	防止	･教育 (･複数人による操作(運用または機能での実現)) (･罰則)	･教育 (･複数人による操作(運用)) (･罰則)

		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・NTAからの時刻配信を受ける。	・NTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
5	T.SystemClock_TOEuser_Modify_Clock_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作（運用）) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・NTAからの時刻配信を受ける。	・NTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
6	T.SystemClock_Cracker_Modify_Clock	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・NTAからの時刻配信を受ける。	・NTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
7	T.TAC_TA_Crypto_Compromise_gradually	防止	・TSA側で、あらかじめ時刻監査証明書をセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・暗号アルゴリズムが完全に危殆化する前に、TSA側で、時刻監査証明書に対して、安全な暗号アルゴリズムを使用したタイムスタンプを取得する。 ・TSA側で、あらかじめ時刻監査証明書に対しタイムスタンプを取得する。 (時刻監査証明書とは異なる暗号アルゴリズムを使用したタイムスタンプを取得する。) ・TAが時刻監査証明書を保管する。	・TSA側で、あらかじめ時刻監査証明書をセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・TAが時刻監査証明書を保管する。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー

8	T.TAC_TA_Crypto_Compromise_immediately	防止	・TSA側で、あらかじめ時刻監査証明書をセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・TSA側で、あらかじめ時刻監査証明書に対しタイムスタンプを取得する。 (時刻監査証明書とは異なる暗号アルゴリズムを使用したタイムスタンプを取得する。) ・TAが時刻監査証明書を保管する。	・TSA側で、あらかじめ時刻監査証明書をセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・TAが時刻監査証明書を保管する。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー
9	T.TAC_Line	防止	・TSA-TOE間の通信路を冗長構成とする。	・TSA-TOE間の通信路を冗長構成とすることで実現可能。
		検出	ー	ー
		回復	ー	ー
10	T.Report_TA_Crypto_Compromise_gradually	防止	・TSA側で、あらかじめ時刻監査レポートをセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・暗号アルゴリズムが完全に危殆化する前に、TSA側で、時刻監査レポートに対して、安全な暗号アルゴリズムを使用したタイムスタンプを取得する。 ・TSA側で、あらかじめ時刻監査レポートに対しタイムスタンプを取得する。 (時刻監査レポートとは異なる暗号アルゴリズムを使用したタイムスタンプを取得する。) ・TAが時刻監査レポートを保管する。	・TSA側で、あらかじめ時刻監査レポートをセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・TAが時刻監査レポートを保管する。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー
11	T.Report_TA_Crypto_Compromise_immediately	防止	・TSA側で、あらかじめ時刻監査レポートをセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・TSA側で、あらかじめ時刻監査レポートに対しタイムスタンプを取得する。 (時刻監査レポートとは異なる暗号アルゴリズムを使用したタイムスタンプを取得する。) ・TAが時刻監査レポートを保管する。	・TSA側で、あらかじめ時刻監査レポートをセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・TAが時刻監査レポートを保管する。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー

12	T.Key_TOEuser_Compromise	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
13	T.Key_Cracker_Compromise	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
14	T.Config_TOEuser_Modify_byTOE	防止	・教育 (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 (・複数人による操作 (運用)) (・罰則)
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
15	T.Config_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
16	T.Config_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
17	T.Config_badTAC_TOEuser_Modify	防止	・教育 ・複数人による操作 (運用または機能での実現) (・罰則)	・教育 ・複数人による操作 (運用) (・罰則)
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
18	T.Config_badTAC_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール

		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
19	T.Config_stopTAC_TOEuser_Modify	防止	・教育 ・複数人による操作（運用または機能での実現） （・罰則）	・教育 ・複数人による操作（運用） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
20	T.Config_stopTAC_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
21	T.Config_badTAC_TOEuser_ModifyTSA	防止	・TLSによる相互認証 ・教育 ・複数人による操作（運用または機能での実現） （・罰則）	・TLSによる相互認証 ※関連するTOEの機能：時刻配信プロトコル ・教育 ・複数人による操作（運用） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
22	T.Config_badTAC_Cracker_ModifyTSA	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
23	T.Log_TOEuser_Delete_byTOE	防止	・教育 （・複数人による操作（運用または機能での実現）） （・罰則）	・教育 （・複数人による操作（運用）） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
24	T.Log_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) （・複数人による操作（運用または機能での実現）） （・罰則）	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) （・複数人による操作（運用）） （・罰則）
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査

		回復	ー	ー
25	T.Log_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
26	T.SW_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
27	T.SW_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
28	T.Password_TOEuser_Secret_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
29	T.Password_TOEuser_Secret_byMemo	防止	・教育 (・罰則)	・教育 (・罰則)
		検出	ー	ー
		回復	ー	ー
30	T.Password_Cracker_Secret	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー

31	T.Virus_TOEuser	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ・ウィルスチェック (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) ・ウィルスチェック (・複数人による操作 (運用)) (・罰則)
		検出	ー	ー
		回復	ー	ー
32	T.Virus_Cracker	防止	・ウィルスチェック	・ウィルスチェック
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
33	T.DoS	防止	・システムの冗長構成	・システムを冗長構成とすることで実現可能。
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
34	T.BufferOverFlow_Attack	防止	・脆弱性の確認とセキュリティパッチの適用	・脆弱性の確認とセキュリティパッチの適用
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
35	T.Hardware_Failure	防止	・システムの冗長構成	・システムを冗長構成とすることで実現可能。
		検出	ー	ー
		回復	ー	ー
36	T.TOE_Bug	防止	・TOE開発者が、ソフトウェア不良を防ぐ開発プロセスを採用する。 ・TOE利用者(TOEの管理者や運用者)は、TOEの導入に際し、十分な試験を行う。	・TOE開発者が、ソフトウェア不良を防ぐ開発プロセスを採用することで実現可能。 ・TOE利用者(TOEの管理者や運用者)は、TOEの導入に際し、十分な試験を行う。
		検出	ー	ー
		回復	・TOE開発者が、パッチの作成・配布・適用を適切に実施する。また、TOE利用者(TOEの管理者や運用者)は、TOEに、TOE開発者の提供するパッチを適用する。	・TOE開発者が、パッチの作成・配布・適用を適切に実施し、TOE利用者(TOEの管理者や運用者)は、TOEに、TOE開発者の提供するパッチを適用することで実現可能。
37	T.Peer_Failure_Asset	防止	ー	ー
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能：ログ管理機能
		回復	・TSA復旧後の、TSAへの再接続。 (対象資産：時刻監査証明書)	・TSA復旧後の、TSAへの再接続。 (対象資産：時刻監査証明書)
38	T.Peer_Failure_NTA1	防止	・複数の時刻配信サーバを利用する。	・複数の時刻配信サーバを用意することで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能：ログ管理機能

		回復	・NTA1(認証連鎖方式の国家時刻標準局)復旧後の、NTA1からの再接続。	・NTA1(認証連鎖方式の国家時刻標準局)復旧後の、NTA1からの再接続。
39	T.Connection_Failure_Asset	防止	・他システム-TOE間の通信路を冗長構成とする。	・他システム-TOE間の通信路を冗長構成とすることで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能:ログ管理機能
		回復	・通信回線復旧後の、TSAへの再接続。 (対象資産:時刻監査証明書)	・通信回線復旧後の、TSAへの再接続。 (対象資産:時刻監査証明書)
40	T.Connection_Failure_NTA1	防止	・通信回線の異なる複数の時刻配信サーバを利用する。	・通信回線の異なる複数の時刻配信サーバを用意することで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能:ログ管理機能
		回復	・通信回線復旧後の、NTA1(認証連鎖方式の国家時刻標準局)からの再接続。	・通信回線復旧後の、NTA1(認証連鎖方式の国家時刻標準局)からの再接続。

2. 前提の実現方法例

以下に、セキュリティ環境の前提に関する実現方法例を記載する。

表 3-2　前提の実現方法例

No.	前提名	実現方法例
1	A.Location	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
2	A.TOE_Administrator	・TOE管理者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE管理者は、TOEとTOEに含まれる情報のセキュリティを維持するようにTOEを導入し、管理することを保証する。 ・TOE管理者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
3	A.TOE_Operator	・TOE運用者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE運用者は、TOE管理者の指示の元で、TOEとTOEに含まれる情報のセキュリティを維持するようにTOEを管理・運用することを保証する。 ・TOE運用者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
4	A.TOE_Auditor	・TOE監査者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE監査者は、TOEを運用する組織の規定に従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。

5	A.TSA_TAC	・TSA1(リンクトークン方式の時刻認証局)およびTSA2(独立トークン方式の時刻認証局)は、時刻監査証明書を検証する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なTAによって行われたものかどうかの確認、が含まれる。 ・TSA1(リンクトークン方式の時刻認証局)およびTSA2(独立トークン方式の時刻認証局)は、時刻監査証明書を検証するためのソフトウェアを持つ。
6	A.TSA_Report	・TSA1(リンクトークン方式の時刻認証局)は、時刻監査レポートを検証及び保持する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TAの時刻監査レポート用証明書が失効していないかどうかの確認、時刻監査レポートの署名は、正当なTAによって行われたものかどうかの確認、が含まれる。 ・TSA1(リンクトークン方式の時刻認証局)は、時刻監査レポートを検証するためのソフトウェアを持つ。また、時刻監査レポートを保管するためのストレージを持つ。
7	A.TOE_Separation	・TOE管理者は、TOE 及びTOE のIT環境の取扱説明書を熟読した上で、取扱説明書が定める手順に従って、TOE 及びTOE のIT 環境を構築する。この際、TOEが動作するサーバマシンには、TOE の動作に関係ないソフトウェアはインストールしない。
8	A.Device	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
9	A.FIREWALL	・TOEとTSA1,TSA2,NTA1は、専用線で接続し、TOEとセグメントが異なる場合は、ファイアウォールを設置する。 ・ファイアウォールの設定は、適切に維持・管理される。
10	A.PEER	・TOEと通信する意図された他システムは、信頼できる第三者(TTP)の運用するシステムであることを保証する。
11	A.Abstract	・TOE 管理者は、TOE が動作するために必要なOSや依存するライブラリが不正な改変から保護され、正しく動作するよう適切に管理する。 ・TOE 管理者は、TOE が動作するサーバマシンに、TOE の動作を干渉するようなソフトウェアがインストールされないように、適切に管理する。 ・TOE 管理者は、TOE 及びTOE のIT 環境が正常な動作を維持するように、適切に管理する。
12	A.TSA1_TA1_Connection	TSA1(リンクトークン方式の時刻認証局)とTOEの間の通信路は、専用線である。
13	A.TSA2_TA1_Connection	TSA2(独立トークン方式の時刻認証局)とTOEの間の通信路は、専用線である。
14	A.NTA1_TA1_Connection	NTA1(認証連鎖方式の国家時刻標準局)とTOEの間の通信路は、専用線である。
15	A.Environment	・TOE の設置場所として、電磁波対策、電力対策、温度・湿度対策が行われている設備を利用する。
16	A.MEDIA	・定期的なデータのバックアップと、適切なシステムマイグレーションを行う。
17	A.Report_Editor	・時刻監査レポート作成者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・時刻監査レポート作成者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、時刻監査レポート作成システム(TOE外)の運用を妨害するような、特殊な機器を持ち込んだ攻撃や、システムを構成する機器への攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
18	A.Report_System	・時刻監査レポート作成システムは、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。

3. 組織のセキュリティポリシーの実現方法例

以下に、組織のセキュリティポリシーに関する実現方法例を記載する。

表 3-3　組織のセキュリティポリシーの実現方法例

No.	ポリシー名	実現方法例
1	P.Cryptography	・TOEの署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって行われる。
2	P.PKI_Management	TOEは、安全に管理されたPKIの中で運用されることを保証する。鍵/証明書は、運用マニュアルに基づき、安全に発行・失効される。
3	P.Password_Management	・TOE管理者およびTOE運用者は、パスワードを記憶し、他人に漏らさない。また、運用マニュアルに基づき、適切なパスワードを設定し、適切な頻度でパスワードを変更する。 ・TOE管理者およびTOE運用者は、ソーシャルエンジニアリングの教育を受けている。
4	P.Protect_Log	・TOE を利用する組織は、TOEの監査ログの暴露・改ざんまたは削除を防止するよう、TOE管理者、TOE運用者、TOE監査者に対して教育を行う。 ・TOEは、TOEの出力するシステムログにハッシュ値やデジタル署名を付与し、改ざんを検出可能な機能を持つ。 ・TOEは、TOEの保護対象資産へのアクセスを許可する前に、全ての利用者に対して識別・認証情報の入力を要求し、識別・認証を実施する。
5	P.Time_Source	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
6	P.System_Clock_Management	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
7	P.Check_Virus	TOE管理者は、運用マニュアルに基づき、定期的にTOEの全ファイルに対してウィルスチェックを行う。また、外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_NTA1	TOEは、NTA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
9	P.Check_Received_Data_TSA1	TOEは、TSA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
10	P.Check_Received_Data_TSA2	TOEは、TSA2から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
11	P.Dual_Control	運用マニュアルに基づき、TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行う。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行う。
12	P.Check_Abstract_Vulnerability	TOE管理者は、運用マニュアルに基づき、定期的にOS やライブラリなどの脆弱性を確認し、対策を行う。

第4章 脅威ツリー及びリスク評価一覧

本章では、内部不正のないセキュリティ評価における脅威ツリー、リスク評価格付けの考え方、リスク評価点を記述する。

1. 脅威ツリー

以下に、脅威ツリーを示す。
※欄の不足を補うため、一部「下位の条件→上位の条件」と矢印で表現している場合がある。

表 4-1　脅威ツリー

No.	資産	脅威	上位レベルが実現するための条件			脅威名
			条件1	条件2	条件3	
1	システム時刻	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。	許可された利用者が、不注意により、TOEの設定情報を変更する。	—	—	T.SystemClock_TOEuser_Modify_TimeSource
2	システム時刻	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。	TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。	—	—	T.SystemClock_Inaccuracy_gradually
3	システム時刻		TOEが参照する時計が故障し、急に時刻がずれる。	—	—	T.SystemClock_Inaccuracy_immediately
4	システム時刻		時刻ソースが不正な時刻を配信し、これをもとにTOEが時刻を補正することで、時刻がずれる。	※前提A.PEERとして、時刻ソースは信頼できるので脅威から除外。	—	—
5	システム時刻	許可された利用者が、不注意により、または外部の不正者が、TOEが参照する時計の時刻をずらす。	許可された利用者が、不注意によりTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	—	T.SystemClock_TOEuser_Modify_Clock_byTOE
6	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	OSにログインする	T.SystemClock_TOEuser_Modify_Clock_byOS
7	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	—

8	システム時刻		外部の不正者が、ネットワーク経由でTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	T.SystemClock_Cracker_Modify_Clock
9	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	同上
10	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	同上
11	システム時刻		外部の不正者が、物理的に侵入し、TOEの時刻を設定する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―
12	システム時刻	外部の不正者が、時刻ソースに成りすまして、TOEに時刻を配信する。	TOEにネットワーク経由でアクセスする。	※前提A.TSA2_TA1_Connectionとして、TA1-TOE間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―
13	システム時刻	外部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	※前提A.TSA2_TA1_Connectionとして、TA1-TOE間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―
14	時刻監査証明書	過去に発行した時刻監査証明書に使用されている暗号アルゴリズムが脆弱化する。	暗号アルゴリズムの攻撃方法が発見され、暗号アルゴリズムが脆弱化する。	計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。	―	T.TAC_TA_Crypto_Compromise_gradually
15	時刻監査証明書			暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。	―	T.TAC_TA_Crypto_Compromise_immediately
16	時刻監査証明書	外部の不正者が、TSAに成りすまして、TOEの送信する時刻監査証明書を受信する。	TOEにネットワーク経由でアクセスする。	※前提A.TSA1_TA1_Connection および A.TSA2_TA1_Connectionとして、TSA-TOE間の通信路は、TSAやTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―

17	時刻監査証明書	外部の不正者が、TOEとTSAの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEとTSAの間のネットワークにアクセスする。	※前提A.TSA1_TA1_Connection および A.TSA2_TA1_Connectionとして、TSA-TOE間の通信路は、TSAやTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―
18	時刻監査証明書	TOEの送信した時刻監査証明書が、不正者もしくは事故などにより改ざんされる。	時刻監査証明書を改ざんし、TSAに送付する。	TSA-TOE間のネットワークにアクセスする。 →ネットワーク中のパケットから、TOEの送付した時刻監査証明書を取得する。	※前提A.TSA_TACにより、TSAは受信した時刻監査証明書の検証を行うため、脅威とはならない。	―
19	時刻監査証明書	TOEの送信した時刻監査証明書が、不正者もしくは事故などにより暴露される。	ネットワーク中のパケットから、TOEの送付した時刻監査証明書を取得する。	TSA-TOE間のネットワークにアクセスする。	※時刻監査証明書の内容は、暴露されても問題のない内容であるため、脅威とはならない。	―
20	時刻監査証明書	TOEの送信した時刻監査証明書が、事故などによりTSAに到達しない。	TSA-TOE間のネットワークが、事故などにより遮断される。	―	―	T.TAC_Line
21	時刻監査レポート	過去に発行した時刻監査レポートに使用されている暗号アルゴリズムが脆弱化する。	暗号アルゴリズムの攻撃方法が発見され、暗号アルゴリズムが脆弱化する。	計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。	―	T.Report_TA_Crypto_Compromise_gradually
22	時刻監査レポート			暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。	―	T.Report_TA_Crypto_Compromise_immediately
23	秘密鍵	TOEの秘密鍵が脆弱化する。	許可された利用者が、不注意によりTOEの秘密鍵を暴露する。	[通信用鍵･署名用鍵] OSの機能を用いてTOEの秘密鍵を取得する。	OSにログインする	T.Key_TOEuser_Compromise
24	秘密鍵		外部の不正者が、ネットワーク経由でTOEの秘密鍵を盗む。	[通信用鍵･署名用鍵] TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Key_Cracker_Compromise
25	秘密鍵		外部の不正者が、物理的に侵入し、TOEの秘密鍵を盗む。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―
26	設定情報	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。	TOEの機能を用いてTOEの設定情報を変更･削除･暴露する。	―	―	T.Config_TOEuser_Modify_byTOE
27	設定情報		OSの機能を用いてTOEの設定情報を変更･削除･暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	―	T.Config_TOEuser_Modify_byOS

28	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
29	設定情報	外部の不正者が、ネットワーク経由でTOEの設定情報を変更・削除・暴露する。	TOEの機能を用いてTOEの設定情報を変更・削除・暴露する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_Cracker_Modify
30	設定情報		OSの機能を用いてTOEの設定情報を変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
31	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
32	設定情報	外部の不正者が、物理的に侵入し、TOEの設定情報を変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
33	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、不正な時刻監査証明書を発行する。	TOEの設定情報を変更する。 ※[不正な時刻監査証明書の例] 本来のポリシ(OID,時刻監査規格(Offset,Delay)等)と異なる時刻監査証明書など。	TOEにアクセスする。	―	T.Config_badTAC_TOEuser_Modify
34	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正な時刻監査証明書を発行する。	TOEの設定情報を変更する。 ※[不正な時刻監査証明書の例] 本来のポリシ(OID,時刻監査規格(Offset,Delay)等)と異なる時刻監査証明書など。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_badTAC_Cracker_Modify

35	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、不正な時刻監査証明書を発行する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
36	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、時刻監査証明書の発行を停止させる。	TOEの設定情報を変更する。	TOEにアクセスする。	—	T.Config_stopTAC_TOEuser_Modify
37	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、時刻監査証明書の発行を停止させる。	TOEの設定情報を変更する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_stopTAC_Cracker_Modify
38	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、時刻監査証明書の発行を停止させる。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
39	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、異なるTSAに時刻監査証明書を送信する。	TOEの設定情報を変更する。	TOEにアクセスする。	—	T.Config_badTAC_TOEuser_ModifyTSA
40	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正なTSAに時刻監査証明書を送信する。	TOEの設定情報を変更する。	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	—	T.Config_badTAC_Cracker_ModifyTSA
41	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、不正なTSAに時刻監査証明書を送信する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
42	ログ	許可された利用者が、不注意により、TOEのログを変更・削除・暴露する。	TOEの機能を用いてTOEのログを削除・暴露する。 ※ログの変更は、TOEの機能を利用して実施することはできない。	—	—	T.Log_TOEuser_Delete_byTOE
43	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	—	T.Log_TOEuser_Modify_byOS

44	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
45	ログ	外部の不正者が、ネットワーク経由でTOEのログを変更・削除・暴露する。	TOEの機能を用いてTOEのログを削除・暴露する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Log_Cracker_Modify
46	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
47	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
48	ログ	外部の不正者が、物理的に侵入し、TOEのログを変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
49	ソフトウェア	許可された利用者が、不注意により、TOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：OSのコマンドを利用して削除する。	OSにログインする	―	T.SW_TOEuser_Modify_byOS
50	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
51	ソフトウェア	外部の不正者が、ネットワーク経由でTOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.SW_Cracker_Modify

52	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
53	ソフトウェア	外部の不正者が、物理的に侵入し、TOEのソフトウェアを変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
54	ID・パスワード	許可された利用者が、不注意により、TOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	OSにログインする	―	T.Password_TOEuser_Secret_byOS
55	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
56	ID・パスワード		その他、口頭、メモ、メール等で情報が漏洩する。	―	―	T.Password_TOEuser_Secret_byMemo
57	ID・パスワード	外部の不正者が、ネットワーク経由でTOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Password_Cracker_Secret
58	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
59	ID・パスワード	外部の不正者が、物理的に侵入し、TOEのID・パスワードを暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
60	その他	許可された利用者が、不注意により、TOEにウィルスを感染させる。	ウィルスに感染した外部メディアにアクセスする。	OSにログインする	ウィルスに感染した外部メディアを持ち込む。	T.Virus_TOEuser
61	その他		外部からウィルスをダウンロードする。	外部にアクセスする。	OSにログインする	同上
62	その他	外部の不正者が、ネットワーク経由でTOEにウィルスを感染させる。	TOEにウィルスをダウンロードさせる。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Virus_Cracker
63	その他	外部の不正者から大量のアクセスが行われ、TOEをサービス不能にさせる。	ネットワーク経由でTOEに大量のアクセスを行う。	―	―	T.DoS

64	その他	外部の不正者が、バッファ・オーバーフローの脆弱性を利用し、TOEの管理者権限を取得する。	TOEにネットワーク経由でアクセスする。	ー	ー	T.BufferOverFlow_Attack
65	その他	TOEのハードウェア故障	経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産が失われる。	―	―	T.Hardware_Failure
66	その他		経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産の完全性が保証できなくなる。	―	―	同上
67	その他		経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、TOEが提供するサービスが継続できない。	―	―	同上
68	その他	TOEのソフトウェアのバグ	TOEのIT実装にソフトウェア不良が存在するため、TOEの資産の信頼性が乏しくなる。 例) ・ある条件下で、ログの書き込みが行われない。 ・ある条件下で、ログファイルを破壊する。	TOEの開発時に、ソフトウェア不良を発見できない。	―	T.TOE_Bug
69	その他	通信相手となる他システムのダウン	通信相手となる他システムのダウンにより、TOEの資産が失われる。	―	―	T.Peer_Failure_Asset
70	その他		NTA1(認証連鎖方式の国家時刻標準局)のダウンにより、TOEが提供するサービスが継続できない。	―	―	T.Peer_Failure_NTA1
71	その他		TSA1(リンクトークン方式の時刻認証局)のダウンにより、TOEが提供するサービスが継続できない。	※TOEに対する脅威とはならないため、脅威から除外。	―	―
72	その他		TSA2(独立トークン方式の時刻認証局)のダウンにより、TOEが提供するサービスが継続できない。	※TOEに対する脅威とはならないため、脅威から除外。	―	―
73	その他	TOEと通信相手となる他システム間の通信回線の故障	TOEと通信相手となる他システムの間の通信回線の故障により、TOEの資産が失われる。	―	―	T.Connection_Failure_Asset

74	その他		NTA1(認証連鎖方式の国家時刻標準局)との間の通信回線の故障により、TOEが提供するサービスが継続できない。	―	―	T.Connection_Failure_NTA1
75	その他		TSA1(リンクトークン方式の時刻認証局)との間の通信回線の故障により、TOEが提供するサービスが継続できない。	※TOEに対する脅威とはならないため、脅威から除外。	―	―
76	その他		TSA2(独立トークン方式の時刻認証局)との間の通信回線の故障により、TOEが提供するサービスが継続できない。	※TOEに対する脅威とはならないため、脅威から除外。	―	―

2. リスク評価格付けの考え方

以下に、リスク評価格付けの考え方を示す。

表 4-2 リスク評価格付けの考え方

	格付け	高(3)	中(2)	低(1)
D	潜在的損失(Damage potential)	<方針> ・信頼性・サービスレベルに影響のあるもの。 ・データを直接悪用できるもの。 ＜対象＞ その他	<方針> ・データを直接は悪用できないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
R	再現性(Reproducibility)	＜方針＞ ・時期によらないもの。 ・内部不正など、攻撃者の意図でいつでも実施できるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ＜対象＞ ・内部不正 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・その他	＜方針＞ ・攻撃者の意図によらないもの。 ・TOE開発時のソフトウェア不良 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ＜対象＞ ・不注意(基本的に発生率は低い、という前提。) ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。) ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断(基本的に発生率は低い、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・暗号脆弱化 ・パケットの暴露・改ざん ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化

E	攻撃利用可能性（Exploitability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃できるもの。 ・攻撃方法が容易なもの。 ・比較的攻撃ツールが入手しやすいと思われるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他	＜方針＞ なし ＜対象＞ なし	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん
A	影響ユーザ（Affected users）	<方針> ・TOEのサービスの利用者に関わるもの。 ・TOE利用者自身に大きな影響があるもの。 ＜対象＞ ・その他	<方針> ・TOEのサービスの利用者に対する直接的な影響がないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
D	発見可能性（Discoverability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃方法を知る事ができるもの。 ・攻撃方法が容易に思いつくもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退	＜方針＞ ・TOE開発時のソフトウェア不良 ＜対象＞ ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

		・他システムの秘密鍵危殆化 ・その他		

3. リスク評価点

以下に、脅威に対するリスク評価点を示す。

表 4-3　リスク評価点

No.	名称	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.SystemClock_TOEuser_Modify_TimeSource	3	2	3	3	3	14
2	T.SystemClock_Inaccuracy_gradually	3	3	3	3	3	15
3	T.SystemClock_Inaccuracy_immediately	3	3	3	3	3	15
4	T.SystemClock_TOEuser_Modify_Clock_byTOE	3	2	3	3	3	14
5	T.SystemClock_TOEuser_Modify_Clock_byOS	3	2	3	3	3	14
6	T.SystemClock_Cracker_Modify_Clock	3	3	3	3	3	15
7	T.TAC_TA_Crypto_Compromise_gradually	3	1	1	3	1	9
8	T.TAC_TA_Crypto_Compromise_immediately	3	1	1	3	1	9
9	T.TAC_Line	3	2	3	3	3	14
10	T.Report_TA_Crypto_Compromise_gradually	3	1	1	3	1	9
11	T.Report_TA_Crypto_Compromise_immediately	3	1	1	3	1	9
12	T.Key_TOEuser_Compromise	3	2	3	3	3	14
13	T.Key_Cracker_Compromise	3	3	3	3	3	15
14	T.Config_TOEuser_Modify_byTOE	3	3	3	3	3	15
15	T.Config_TOEuser_Modify_byOS	3	3	3	3	3	15
16	T.Config_Cracker_Modify	3	3	3	3	3	15
17	T.Config_badTAC_TOEuser_Modify	3	2	3	3	3	14
18	T.Config_badTAC_Cracker_Modify	3	3	3	3	3	15
19	T.Config_stopTAC_TOEuser_Modify	3	2	3	3	3	14
20	T.Config_stopTAC_Cracker_Modify	3	3	3	3	3	15
21	T.Config_badTAC_TOEuser_ModifyTSA	3	2	3	3	3	14
22	T.Config_badTAC_Cracker_ModifyTSA	3	3	3	3	3	15
23	T.Log_TOEuser_Delete_byTOE	2	2	3	2	3	12
24	T.Log_TOEuser_Modify_byOS	2	2	3	2	3	12
25	T.Log_Cracker_Modify	2	3	3	2	3	13
26	T.SW_TOEuser_Modify_byOS	3	2	3	3	3	14
27	T.SW_Cracker_Modify	3	2	3	3	3	14
28	T.Password_TOEuser_Secret_byOS	3	2	3	3	3	14
29	T.Password_TOEuser_Secret_byMemo	3	2	3	3	3	14
30	T.Password_Cracker_Secret	3	3	3	3	3	15
31	T.Virus_TOEuser	3	3	3	3	3	15
32	T.Virus_Cracker	3	3	3	3	3	15
33	T.DoS	3	3	3	3	3	15
34	T.BufferOverFlow_Attack	3	3	3	3	3	15
35	T.Hardware_Failure	3	2	3	3	3	14

36	T.TOE_Bug	3	2	3	3	2	13
37	T.Peer_Failure_Asset	3	2	3	3	3	14
38	T.Peer_Failure_NTA1	3	2	3	3	3	14
39	T.Connection_Failure_Asset	3	2	3	3	3	14
40	T.Connection_Failure_NTA1	3	2	3	3	3	14

第5章 内部不正を考慮したセキュリティ評価

本章では、内部不正の考え方及び内部不正を考慮したセキュリティ環境を記載する。また、脅威に関する対策を記載する。

1. 内部不正の考え方

内部不正を考慮したセキュリティ評価として、内部不正のモデルを以下のように位置づける。

- 内部不正の範囲
  内部不正として、内部者の単独による不正を考慮する。
  (時刻監査レポート作成者は、時刻監査レポート作成システム(TOE 外)の作業者であるため、内部不正の範囲から除く。)
  下記のケースについては除外する。
  -外部者との結託
  -内部者の結託
  -内部者の単独による不正が同時に発生するケース

- セキュリティ環境
  内部不正を考慮しないセキュリティ環境を、内部不正を考慮した場合のセキュリティ環境にカスタマイズする。

2. 内部不正を考慮したセキュリティ環境

2-1 前提

以下に、TOE を使用する際のセキュリティ環境の前提を示す。

表 5-1　前提

No.	分類	項目	説明
1	物理的な前提	A.Location	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティの中に設置される。これにより、権限のないユーザからの物理アクセスを防ぐ。

2	人的な前提	A.TOE_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOEとTOEに含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOEを安全に導入、管理する。 ･TOEに関わるユーザ/役割を管理する。 ･時刻に関する管理業務を行う。 ･暗号機能に関わる初期化及び管理業務を行う。 ･TOE上で悪意のあるソフトウェアが動作しないようにする。 ･TOEの用件を満たす適切なディスクスペースを用意する。 ･TOEのデータベースを適切に管理する。 ･時刻監査レポート作成者を管理する。 彼らは、単独による内部不正を行う可能性があるものとする。
3	人的な前提	A.TOE_Operator	一人以上の許可された運用者が割り当てられる。 ･TOEの起動･停止を実行する。 ･TOE管理者の指示の元で各種設定など運用業務を行う。 彼らは、単独による内部不正を行う可能性があるものとする。
4	人的な前提	A.TOE_Auditor	一人以上の許可された監査者が割り当てられる。 ･TOEが生成する監査データの分析等の監査業務を行う。 彼らは、単独による内部不正を行う可能性があるものとする。
5	人的な前提	A.TSA_TAC	TSA1(リンクトークン方式の時刻認証局)およびTSA2(独立トークン方式の時刻認証局)は、時刻監査証明書を検証する。この中には、アウト･オブ･バンドの方法を用いて、TA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なTAによって行われたものかどうかの確認、が含まれる。
6	人的な前提	A.TSA_Report	TSA1(リンクトークン方式の時刻認証局)は、時刻監査レポートを検証及び保持する。この中には、アウト･オブ･バンドの方法を用いて、TAの時刻監査レポート用証明書が失効していないかどうかの確認、時刻監査レポートの署名は、正当なTAによって行われたものかどうかの確認、が含まれる。
7	接続に関する前提	A.Device	周辺機器への接続は、コントロールされたアクセス･ファシリティ内に存在する。
8	接続に関する前提	A.FIREWALL	TOEと他システムとの接続には、専用線を用いる。TOEとセグメントが異なる場合は、ファイアウォールを設置する。
9	接続に関する前提	A.PEER	TOEと通信する意図された他システムは、信頼できる。
10	接続に関する前提	A.TSA1_TA1_Connection	TSA1(リンクトークン方式の時刻認証局)とTOEの間の通信路は、TSA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
11	接続に関する前提	A.TSA2_TA1_Connection	TSA2(独立トークン方式の時刻認証局)とTOEの間の通信路は、TSA2やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
12	接続に関する前提	A.NTA1_TA1_Connection	NTA1(認証連鎖方式の国家時刻標準局)とTOEの間の通信路は、NTA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。
13	物理的な前提	A.Environment	TOE の設置場所は、電磁波対策、電力対策、温度･湿度対策が行われている。
14	物理的な前提	A.MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
15	その他	A.Report_Editor	･時刻監査レポートの作成には、一人以上の許可された時刻監査レポート作成者が割り当てられる。さらに時刻監査レポート作成者は、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
16	その他	A.Report_System	･時刻監査レポート作成システム(TOE外)は、セキュリティ上安全なものとする。

2-2 脅威

以下に、TOE および環境に対する脅威を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

なお、脅威の分類は以下のように区分した。

・分類：TOE

TOE のセキュリティ機能（例：時刻配信プロトコルなど）により対策可能。

・分類：環境

TOE のセキュリティ機能では対策不可能、環境の IT/非 IT 機能（例：外部の IDS システムにより対策、運用により対策）により対策可能。

※TOE のログ管理機能、TOE 管理機能を利用して対策する脅威は、こちらの区分に含めている。

表 5-2　脅威

No.	分類	項目	説明
1	TOE	T.SystemClock_TOEuser_Modify_TimeSource_Malice	内部の不正者が、TOEが参照する時刻ソースを変更する。
2	TOE	T.SystemClock_Inaccuracy_TOEuser__Crash_Malice	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が内部の不正者の攻撃により機能低下 (故障) し、時刻がずれる。)
3	TOE	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
4	TOE	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(OSの機能を利用)
5	TOE	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(外部から持ち込んだソフトウェアを利用)
6	TOE	T.SystemClock_TOEuser_Imperson_Server_Malice	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。
7	TOE	T.SystemClock_TOEuser_Modify_Data_Line_Malice	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。
8	TOE	T.TAC_TOEuser_Imperson_TOE_Malice	内部の不正者が、TOEに成りすましたサーバを利用してTSAと通信を行う。
9	TOE	T.TAC_TOEuser_Modify_Data_Line_Malice	内部の不正者が、TOEとTSAの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。
10	環境	T.Key_TOEuser_Compromise_Malice	内部の不正者がTOEの秘密鍵を暴露する。
11	環境	T.Config_TOEuser_Modify_byTOE_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(TOEの機能を利用)
12	環境	T.Config_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(OSの機能を利用)

13	環境	T.Config_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
14	環境	T.Config_badTAC_TOEuser_Modify_Malice	内部の不正者が、TOEの設定を変更し、不正な時刻監査証明書を発行する。
15	環境	T.Config_stopTAC_TOEuser_Modify_Malice	内部の不正者が、TOEの設定を変更し、時刻監査証明書の発行を停止させる。
16	環境	T.Config_badTAC_TOEuser_ModifyTSA_Malice	内部の不正者が、TOEの設定を変更し、不正なTSAに時刻監査証明書を送信する。
17	環境	T.Log_TOEuser_Delete_byTOE_Malice	内部の不正者が、TOEのログを削除･暴露する。(TOEの機能を利用) ※ログの変更は、TOEの機能を利用して実施することはできない。
18	環境	T.Log_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEのログを変更･削除･暴露する。(OSの機能を利用)
19	環境	T.Log_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEのログを変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
20	環境	T.SW_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEのソフトウェアを変更･削除･暴露する。(OSの機能を利用)
21	環境	T.SW_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEのソフトウェアを変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
22	環境	T.Password_TOEuser_Secret_byOS_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(OSの機能を利用)
23	環境	T.Password_TOEuser_Secret_byImportSW_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(外部から持ち込んだソフトウェアを利用)
24	環境	T.Password_TOEuser_Secret_byMemo_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(口頭、メモ、メール等)
25	環境	T.Virus_TOEuser_Malice	内部の不正者が、TOEにウィルスを感染させる。
26	環境	T.Crash_TOEuser_Malice	内部の不正者が、TOEを破壊し、サービスを停止させる。

2-3 組織のセキュリティポリシー

以下に、TOE を使用するにあたっての、組織のセキュリティポリシーを示す。

表 5-3　組織のセキュリティポリシー

No.	項目	説明
1	P.Cryptography	署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって実装されなければならない。
2	P.PKI_Management	安全に管理されたPKIの中で、TOEを運用すること。全ての鍵と証明書は、安全に発行、失効される。
3	P.Password_Management	TOEのパスワードは、TOE管理者およびTOE運用者によって適切に管理され、TOE管理者およびTOE運用者以外に知られてはならない。
4	P.Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。

5	P.Time_Source	TOEは、信頼のできる時刻ソースを参照すること。また、時刻ソースの信頼性と正確性は、TOE所有者にとって受容可能であること。
6	P.System_Clock_Management	TOEが参照する時計を信頼のできる時刻ソースと同期させる。
7	P.Check_Virus	定期的なウィルスチェックを実行する。 外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_NTA1	NTA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
9	P.Check_Received_Data_TSA1	TSA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
10	P.Check_Received_Data_TSA2	TSA2から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
11	P.Dual_Control	TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
12	P.Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

3. セキュリティ目標・対策と実装システムの評価
3-1 脅威のセキュリティ目標・対策及び実装システムに対する評価

以下に、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

表 5-4　脅威のセキュリティ目標・対策及び実装システムに対する評価

No.	脅威名	セキュリティ目標･対策		統合化システムにおける実現
1	T.SystemClock_TOEuser_Modify_TimeSource_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	･正しいNTAからの時刻配信を受ける。	･正しいNTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 （-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。）
2	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	･NTAからの時刻配信を受ける。	･NTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 （-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。）
3	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	･NTAからの時刻配信を受ける。	･NTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 （-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。）
4	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則 ･運用管理(操作は、管理用端末からブラウザを利用して行う。)	･複数人による操作（運用） ･罰則 ･運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	･運用記録の監査	･運用記録の作成 ･運用記録の監査

		回復	・NTAからの時刻配信を受ける。	・NTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
5	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・NTAからの時刻配信を受ける。	・NTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
6	T.SystemClock_TOEuser_Imperson_Server_Malice	防止	・TLSによる相互認証 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる相互認証 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
7	T.SystemClock_TOEuser_Modify_Data_Line_Malice	防止	・TLSによる通信路の保護 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる通信路の保護 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・NTAから再度時刻配信を受ける。	・NTAから再度時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)

8	T.TAC_TOEuser_Impersonation_TOE_Malice	防止	・TLSによる相互認証 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる相互認証 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
9	T.TAC_TOEuser_Modify_Data_Line_Malice	防止	・TLSによる通信路の保護 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる通信路の保護 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからTSAに再度時刻配信を行う。	・TAからTSAに再度時刻配信を行う。
10	T.Key_TOEuser_Compromise_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
11	T.Config_TOEuser_Modify_byTOE_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
12	T.Config_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)

		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
13	T.Config_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
14	T.Config_badTAC_TOEuser_Modify_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
15	T.Config_stopTAC_TOEuser_Modify_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
16	T.Config_badTAC_TOEuser_ModifyTSA_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
17	T.Log_TOEuser_Delete_byTOE_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
18	T.Log_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)

		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
19	T.Log_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
20	T.SW_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
21	T.SW_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
22	T.Password_TOEuser_Secret_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
23	T.Password_TOEuser_Secret_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)

		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
24	T.Password_TOEuser_Secret_byMemo_Malice	防止	・罰則	・罰則
		検出	ー	ー
		回復	ー	ー
25	T.Virus_TOEuser_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ・ウィルスチェック	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) ・ウィルスチェック
		検出	ー	ー
		回復	ー	ー
26	T.Crash_TOEuser_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー

3-2 前提の実現方法例

以下に、セキュリティ環境の前提に関する実現方法例を記載する。

表 5-5　前提の実現方法例

No.	前提名	実現方法例
1	A.Location	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
2	A.TOE_Administrator	・TOE管理者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
3	A.TOE_Operator	・TOE運用者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
4	A.TOE_Auditor	・TOE監査者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
5	A.TSA_TAC	・TSA1(リンクトークン方式の時刻認証局)およびTSA2(独立トークン方式の時刻認証局)は、時刻監査証明書を検証する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TA証明書が失効していないかどうかの確認、時刻監査証明書の署名は、正当なTAによって行われたものかどうかの確認、が含まれる。 ・TSA1(リンクトークン方式の時刻認証局)およびTSA2(独立トークン方式の時刻認証局)は、時刻監査証明書を検証するためのソフトウェアを持つ。
6	A.TSA_Report	・TSA1(リンクトークン方式の時刻認証局)は、時刻監査レポートを検証及び保持する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TAの時刻監査レポート用証明書が失効していないかどうかの確認、時刻監査レポートの署名は、正当なTAによって行われたものかどうかの確認、が含まれる。 ・TSA1(リンクトークン方式の時刻認証局)は、時刻監査レポートを検証するためのソフトウェアを持つ。また、時刻監査レポートを保管するためのストレージを持つ。
7	A.Device	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
8	A.FIREWALL	・TOEとTSA1,TSA2,NTA1は、専用線で接続し、TOEとセグメントが異なる場合は、ファイアウォールを設置する。 ・ファイアウォールの設定は、適切に維持・管理される。
9	A.PEER	・TOEと通信する意図された他システムは、信頼できる第三者(TTP)の運用するシステムであることを保証する。
10	A.TSA1_TA1_Connection	TSA1(リンクトークン方式の時刻認証局)とTOEの間の通信路は、専用線である。
11	A.TSA2_TA1_Connection	TSA2(独立トークン方式の時刻認証局)とTOEの間の通信路は、専用線である。
12	A.NTA1_TA1_Connection	NTA1(認証連鎖方式の国家時刻標準局)とTOEの間の通信路は、専用線である。
13	A.Environment	・TOE の設置場所として、電磁波対策、電力対策、温度・湿度対策が行われている設備を利用する。
14	A.MEDIA	・定期的なデータのバックアップと、適切なシステムマイグレーションを行う。
15	A.Report_Editor	・時刻監査レポート作成者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・時刻監査レポート作成者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、時刻監査レポート作成システム(TOE外)の運用を妨害するような、特殊な機器を持ち込んだ攻撃や、システムを構成する機器への攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
16	A.Report_System	・時刻監査レポート作成システムは、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。

3-3 組織のセキュリティポリシーの実現方法例

以下に、組織のセキュリティポリシーに関する実現方法例を記載する。

表 5-6　組織のセキュリティポリシーの実現方法例

No.	ポリシー名	実現方法例
1	P.Cryptography	・TOEの署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって行われる。
2	P.PKI_Management	TOEは、安全に管理されたPKIの中で運用されることを保証する。鍵/証明書は、運用マニュアルに基づき、安全に発行・失効される。
3	P.Password_Management	・TOE管理者およびTOE運用者は、パスワードを記憶し、他人に漏らさない。また、運用マニュアルに基づき、適切なパスワードを設定し、適切な頻度でパスワードを変更する。 ・TOE管理者およびTOE運用者は、ソーシャルエンジニアリングの教育を受けている。
4	P.Protect_Log	・TOE を利用する組織は、TOEの監査ログの暴露・改ざんまたは削除を防止するよう、TOE管理者、TOE運用者、TOE監査者に対して教育を行う。 ・TOEは、TOEの出力するシステムログにハッシュ値やデジタル署名を付与し、改ざんを検出可能な機能を持つ。 ・TOEは、TOEの保護対象資産へのアクセスを許可する前に、全ての利用者に対して識別・認証情報の入力を要求し、識別・認証を実施する。
5	P.Time_Source	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
6	P.System_Clock_Management	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
7	P.Check_Virus	TOE管理者は、運用マニュアルに基づき、定期的にTOEの全ファイルに対してウィルスチェックを行う。また、外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
8	P.Check_Received_Data_NTA1	TOEは、NTA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
9	P.Check_Received_Data_TSA1	TOEは、TSA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
10	P.Check_Received_Data_TSA2	TOEは、TSA2から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
11	P.Dual_Control	運用マニュアルに基づき、TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行う。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行う。
12	P.Check_Abstract_Vulnerability	TOE管理者は、運用マニュアルに基づき、定期的にOS やライブラリなどの脆弱性を確認し、対策を行う。

4. 脅威ツリー及びリスク評価一覧

4-1 脅威ツリー

以下に、脅威ツリーを示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

※欄の不足を補うため、一部「下位の条件→上位の条件」と矢印で表現している場合がある。

表 5-7　脅威ツリー

No.	資産	脅威	上位レベルが実現するための条件			脅威名
			条件1	条件2	条件3	
1	システム時刻	内部の不正者が、TOEが参照する時刻ソースを変更する。	内部の不正者が、TOEの設定情報を変更する。	—	—	T.SystemClock_TOEuser_Modify_TimeSource_Malice
2	システム時刻		TOEが参照する時計が内部の不正者の攻撃により機能低下（故障）し、時刻がずれる。	※具体的な攻撃方法は特に規定しない。	—	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice
3	システム時刻	内部の不正者が、TOEが参照する時計の時刻をずらす。	内部の不正者が、TOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	—	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice
4	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	OSにログインする	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice
5	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	—	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice
6	システム時刻	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。	TOEと時刻ソースの間のネットワークにアクセスする。	TOEに成りすましたサーバを用意する。 ※秘密鍵は除外。秘密鍵以外についての成りすまし。	—	T.SystemClock_TOEuser_Imperson_Server_Malice
7	システム時刻	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	—	—	T.SystemClock_TOEuser_Modify_Data_Line_Malice
8	時刻監査証明書	内部の不正者が、TOEに成りすましたサーバを利用してTSAと通信を行う。	TOEとTSAの間のネットワークにアクセスする。	TOEに成りすましたサーバを用意する。 ※秘密鍵は除外。秘密鍵以外についての成りすまし。	—	T.TAC_TOEuser_Imperson_TOE_Malice

9	時刻監査証明書	内部の不正者が、TOEとTSAの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEとTSAの間のネットワークにアクセスする。	―	―	T.TAC_TOEuser_Modify_Data_Line_Malice
10	秘密鍵		内部の不正者がTOEの秘密鍵を暴露する。	[通信用鍵･署名用鍵] OSの機能を用いてTOEの秘密鍵を取得する。	OSにログインする	T.Key_TOEuser_Compromise_Malice
11	設定情報	内部の不正者が、TOEの設定情報を変更･削除･暴露する。	TOEの機能を用いてTOEの設定情報を変更･削除･暴露する。	―	―	T.Config_TOEuser_Modify_byTOE_Malice
12	設定情報		OSの機能を用いてTOEの設定情報を変更･削除･暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	―	T.Config_TOEuser_Modify_byOS_Malice
13	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：悪意のソフトウェア	―	―	T.Config_TOEuser_Modify_byImportSW_Malice
14	設定情報	内部の不正者が、TOEの設定を変更し、不正な時刻監査証明書を発行する。	TOEの設定情報を変更する。 ※[不正な時刻監査証明書の例] 本来のポリシ(OID,時刻監査規格(Offset,Delay)等)と異なる時刻監査証明書など。	TOEにアクセスする。	―	T.Config_badTAC_TOEuser_Modify_Malice
15	設定情報	内部の不正者が、TOEの設定を変更し、時刻監査証明書の発行を停止させる。	TOEの設定情報を変更する。	TOEにアクセスする。	―	T.Config_stopTAC_TOEuser_Modify_Malice
16	設定情報	内部の不正者が、TOEの設定を変更し、不正なTSAに時刻監査証明書を送信する。	TOEの設定情報を変更する。	TOEにアクセスする。	―	T.Config_badTAC_TOEuser_ModifyTSA_Malice
17	ログ	内部の不正者が、TOEのログを変更･削除･暴露する。	TOEの機能を用いてTOEのログを削除･暴露する。 ※ログの変更は、TOEの機能を利用して実施することはできない。	―	―	T.Log_TOEuser_Delete_byTOE_Malice

18	ログ		OSの機能を用いてTOEのログを変更･削除･暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更･削除･暴露する。) ※例：設定ファイルを直接編集する。	OSにログインする	―	T.Log_TOEuser_Modify_byOS_Malice
19	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更･削除･暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更･削除･暴露する。) ※例：悪意のソフトウェア	―	―	T.Log_TOEuser_Modify_byImportSW_Malice
20	ソフトウェア	内部の不正者が、TOEのソフトウェアを変更･削除･暴露する。	OSの機能を用いてTOEのソフトウェアを変更･削除･暴露する。 ※例：OSのコマンドを利用して削除する。	OSにログインする	―	T.SW_TOEuser_Modify_byOS_Malice
21	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更･削除･暴露する。 ※例：悪意のソフトウェア	―	―	T.SW_TOEuser_Modify_byImportSW_Malice
22	ID･パスワード	内部の不正者が、TOEのID･パスワードを暴露する。	OSの機能を用いてTOEのID･パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	OSにログインする	―	T.Password_TOEuser_Secret_byOS_Malice
23	ID･パスワード		外部から持ち込んだソフトウェアを用いてTOEのID･パスワードを暴露する。 ※例：悪意のソフトウェア	―	―	T.Password_TOEuser_Secret_byImportSW_Malice
24	ID･パスワード		その他、口頭、メモ、メール等で情報が漏洩する。	―	―	T.Password_TOEuser_Secret_byMemo_Malice
25	その他	内部の不正者が、TOEにウィルスを感染させる。	ウィルスに感染した外部メディアにアクセスする。	OSにログインする	ウィルスに感染した外部メディアを持ち込む。	T.Virus_TOEuser_Malice
26	その他		外部からウィルスをダウンロードする。	外部にアクセスする。	OSにログインする	同上
27	その他	内部の不正者が、TOEを破壊し、サービスを停止させる。	TOEを破壊する。	TOEの設置された部屋に入室する。	―	T.Crash_TOEuser_Malice

4-2 リスク評価格付けの考え方

以下に、リスク評価格付けの考え方を示す。

表 5-8　リスク評価格付けの考え方

	格付け	高(3)	中(2)	低(1)
D	潜在的損失（Damage potential）	<方針> ・信頼性・サービスレベルに影響のあるもの。 ・データを直接悪用できるもの。 ＜対象＞ その他	<方針> ・データを直接は悪用できないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
R	再現性（Reproducibility）	＜方針＞ ・時期によらないもの。 ・内部不正など、攻撃者の意図でいつでも実施できるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ＜対象＞ ・内部不正 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・その他	＜方針＞ ・攻撃者の意図によらないもの。 ・TOE開発時のソフトウェア不良 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ＜対象＞ ・不注意（基本的に発生率は低い、という前提。） ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。) ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断（基本的に発生率は低い、という前提。）	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・暗号脆弱化 ・パケットの暴露・改ざん ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化

E	攻撃利用可能性（Exploitability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃できるもの。 ・攻撃方法が容易なもの。 ・比較的攻撃ツールが入手しやすいと思われるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他	＜方針＞ なし ＜対象＞ なし	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん
A	影響ユーザ（Affected users）	<方針> ・TOEのサービスの利用者に関わるもの。 ・TOE利用者自身に大きな影響があるもの。 ＜対象＞ ・その他	<方針> ・TOEのサービスの利用者に対する直接的な影響がないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
D	発見可能性（Discoverability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃方法を知る事ができるもの。 ・攻撃方法が容易に思いつくもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退	＜方針＞ ・TOE開発時のソフトウェア不良 ＜対象＞ ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

		・他システムの秘密鍵危殆化 ・その他		

4-3 リスク評価点

以下に、脅威に対するリスク評価点を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

表 5-9　リスク評価点

No.	名称	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.SystemClock_TOEuser_Modify_TimeSource_Malice	3	3	3	3	3	15
2	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice	3	3	3	3	3	15
3	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	3	3	3	3	3	15
4	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	3	3	3	3	3	15
5	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	3	3	3	3	3	15
6	T.SystemClock_TOEuser_Imperson_Server_Malice	3	3	3	3	3	15
7	T.SystemClock_TOEuser_Modify_Data_Line_Malice	3	3	3	3	3	15
8	T.TAC_TOEuser_Imperson_TOE_Malice	3	3	3	3	3	15
9	T.TAC_TOEuser_Modify_Data_Line_Malice	3	3	3	3	3	15
10	T.Key_TOEuser_Compromise_Malice	3	3	3	3	3	15
11	T.Config_TOEuser_Modify_byTOE_Malice	3	3	3	3	3	15
12	T.Config_TOEuser_Modify_byOS_Malice	3	3	3	3	3	15
13	T.Config_TOEuser_Modify_byImportSW_Malice	3	3	3	3	3	15
14	T.Config_badTAC_TOEuser_Modify_Malice	3	3	3	3	3	15
15	T.Config_stopTAC_TOEuser_Modify_Malice	3	3	3	3	3	15
16	T.Config_badTAC_TOEuser_ModifyTSA_Malice	3	3	3	3	3	15
17	T.Log_TOEuser_Delete_byTOE_Malice	2	3	3	2	3	13
18	T.Log_TOEuser_Modify_byOS_Malice	2	3	3	2	3	13
19	T.Log_TOEuser_Modify_byImportSW_Malice	2	3	3	2	3	13
20	T.SW_TOEuser_Modify_byOS_Malice	3	3	3	3	3	15
21	T.SW_TOEuser_Modify_byImportSW_Malice	3	3	3	3	3	15
22	T.Password_TOEuser_Secret_byOS_Malice	3	3	3	3	3	15
23	T.Password_TOEuser_Secret_byImportSW_Malice	3	3	3	3	3	15
24	T.Password_TOEuser_Secret_byMemo_Malice	3	3	3	3	3	15
25	T.Virus_TOEuser_Malice	3	3	3	3	3	15

26	T.Crash_TOEuser_Malice	3	3	3	3	3	15

セキュリティ評価報告書

(TOE： NTA2)

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

1. TOE の機能概要

TOE は、「時刻情報配信機能」、「時刻情報検証機能」、「時刻情報監査機能」の 3 つの機能から構成される。

1-1 時刻情報配信機能

1-1-1 時刻情報生成機能

現在一般的に使用されているシステムの時刻は、権限を持ったユーザであれば容易に変更することが可能となっており、かつ、変更したことを検出することは困難である。また、TA などの時刻の提供を行う機関から監査を受けることにより、時刻の不正操作を防止することは可能であるが、過去の特定の時刻において、その時点での時刻が正確であったことを示すことは困難である。

本機能において生成される時刻情報（以下、「時刻認証子」と記す）は、過去に生成された時刻認証子を元に生成されており、時刻認証子を改ざんするには、過去に生成された時刻認証子も改ざんさせる必要がある。そのため、時刻認証子の改ざんは困難であり、改ざんの検出も可能となっている。また、時刻認証子に第三者が予測不能なデータを付加することにより、時刻認証子の先読みによる不正生成が困難となっている。

TOE 利用者に提供される時刻認証子には、一般的な時刻表記（例：2004 年 6 月 11 日 15 時 29 分 41 秒）に加え、TOE 機器からの時刻配信経路上の機関の情報と誤差が記されており、TOE 利用者は自身の配信した時刻認証子の配信経路を特定することが可能となっている。

1-1-2 時刻配信機能

TOE にて生成された時刻認証子は、時刻同期の標準的なプロトコルである NTPv4 を用いることにより TA2 に配信される。NTPv4 により時刻の配信を受けた TA2 は、受信した時刻認証子を元にして時刻認証子を生成する。TOE 機器から受け取る時刻認証子を予測することは非常に困難であるため、TA2 は時刻認証子の偽造・改ざんを行うことはほぼ不可能と考えられる。TOE 機器内で保存されている時刻認証子を用いることにより、TA2 の不正を検出することが可能となる。

1-1-3 時刻補正機能

時刻認証子の配信には NTPv4 を用いているため、TA2 は時刻認証子の受信時に TOE 機器と時刻同期を行う。

1-2 時刻情報検証機能

TA2 が受け取った時刻認証子の TOE 機器までの配信経路と誤差を検証する。

時刻認証子に記載されている配信パス上の各機関を特定する情報（IP アドレス）が正しいか確認する。確認方法は、配信経路上の各機関の保有する配信ログの情報と検証対象の時刻認証子とのハッシュリンクの整合性を確認することにより行う。

1-3 時刻情報監査機能

TOE は、TA2 における時刻認証子の改竄防止および検出のため、定期的に監査を行う（時刻受信装置から監査要求があった場合も監査を行う）。

監査方法は、TA2 が過去に生成した時刻認証子のリンクの整合性を確かめることにより、時刻認証子が TA2 で不正なく保存されていたか否かを確認することである。監査結果は、TOE にて保存される。

2. TOE 構成図

以下の図 1-1 に TOE 構成図を記す。

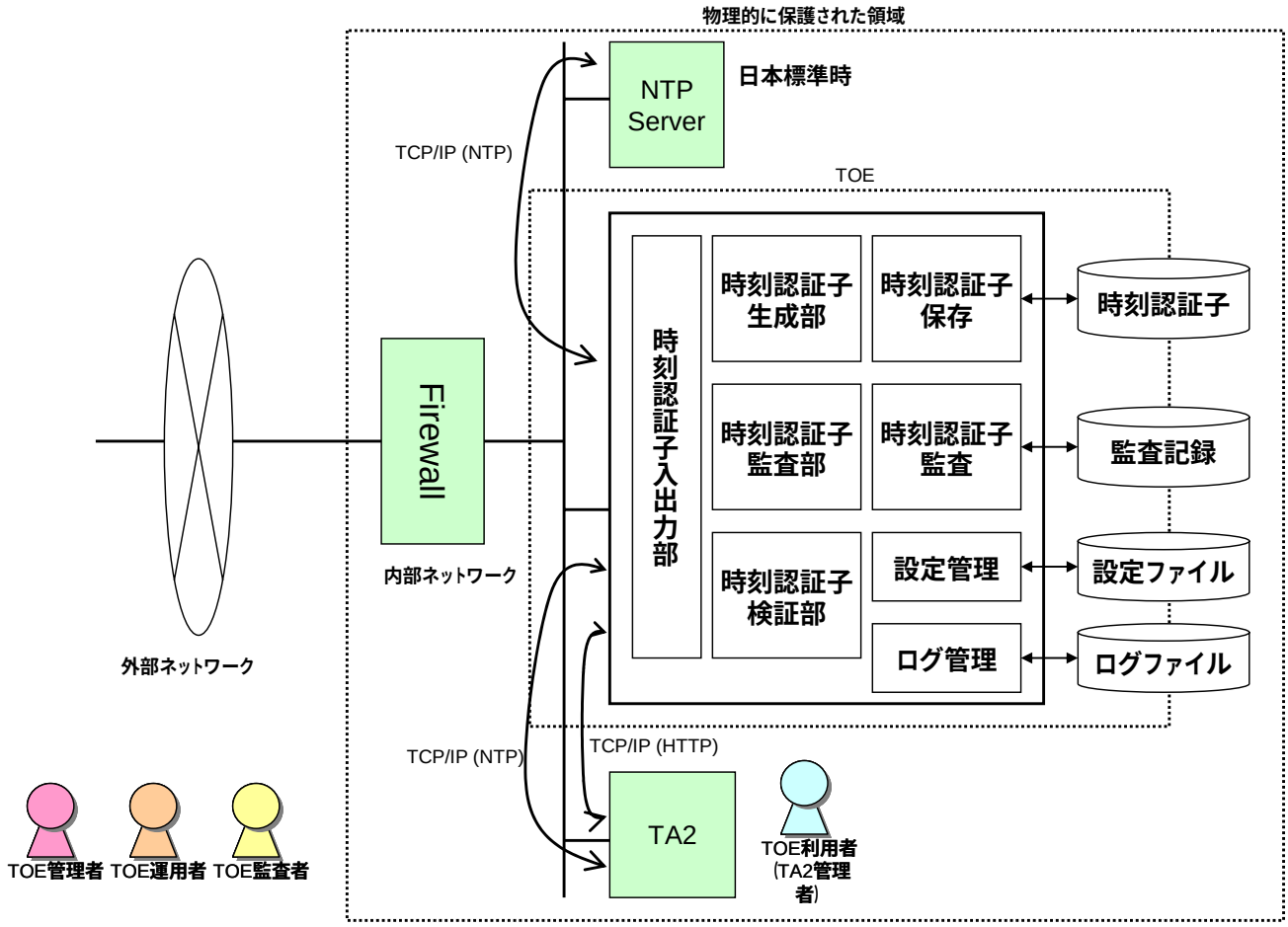


図 1-1：TOE 構成図

3. 利用する暗号技術と暗号コンポーネント構成図

以下に TOE で使用する暗号技術と暗号コンポーネントの構成図を記す。

表 1-1：使用する暗号技術

#	使用している暗号技術		使用目的
暗号技術 1	ハッシュ関数	SHA256、SHA384、SHA512	時刻認証子の結合（ハッシュリンク生成）
暗号技術 2	公開鍵暗号	RSA (512bit)	NTP の autokey 機能における鍵交換に使用
暗号技術 3	ハッシュ関数	MD5	NTP パケットのメッセージ認証

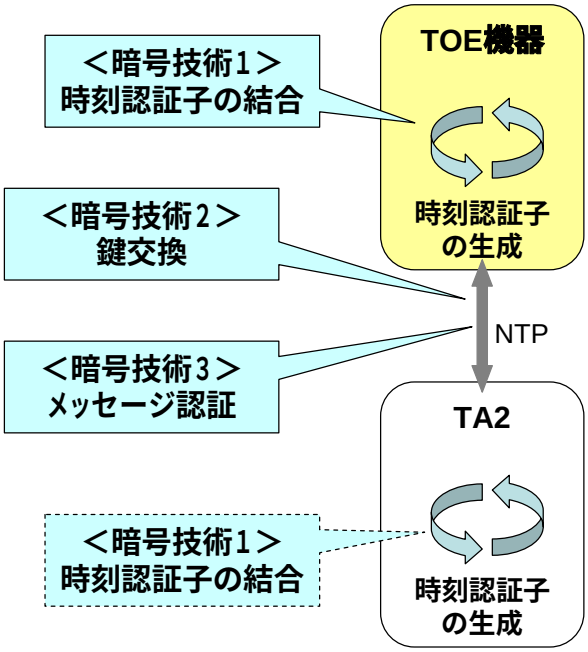


図 1-2：TOE で使用される暗号技術

上記の暗号技術は、TOE で時刻認証子のトレーサビリティ検証及び時刻認証子監査で使用される。以下の図にトレーサビリティ検証の処理の流れ、図に時刻認証子監査を処理の流れを記す。

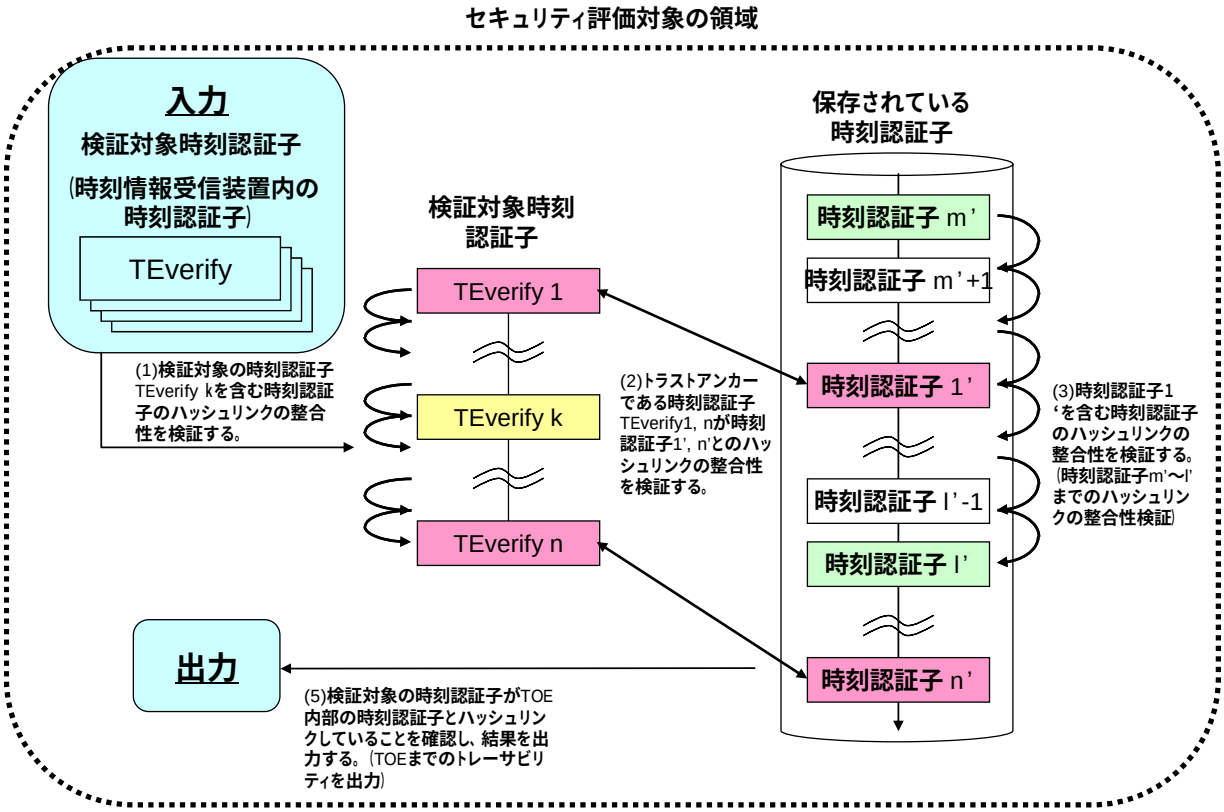


図 1-3：トレーサビリティ検証処理の流れ

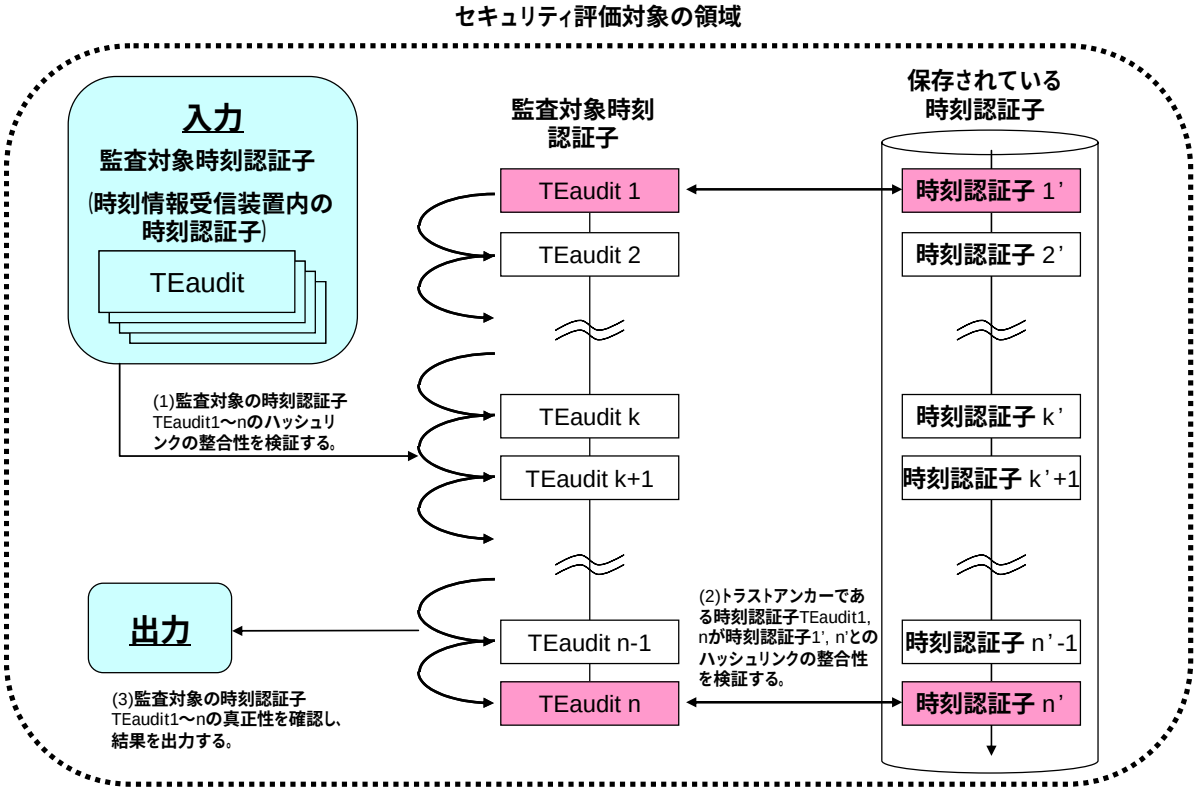


図 1-4：時刻認証子監査処理の流れ

4. TOE 関与者

表 1-2 に本 TOE 関与者を記す。

表 1-2：TOE 関与者

#	関与者	説明
1	TOE 管理者	• TOE の起動・停止を実行する。 • TOE に関わるユーザ/役割を管理する。具体的には、以下の作業を行う。 – ユーザの登録/削除 – 設定ファイルのアクセス権変更
2	TOE 運用者	• TOE 管理者の指示の元で以下の運用業務を行う。具体的には、以下の作業を行う。 – NTA2 のインストール – NTA2 を使用するためのセットアップ – 時刻情報配信先への時刻認証子監査を実施 – 設定ファイルの変更 – 時刻認証子の閲覧/複製/削除 – NTA2 で生成される NTA2 利用者に関する時刻認証子監査記録の閲覧/削除
3	TOE 監査者	• TOE の時刻認証子監査を実施し、生成される時刻認証子監査記録の分析を行う。具体的には、以下の作業を行う。 – 時刻認証子監査記録ファイルの分析 – 時刻認証子監査記録ファイルの取り出し/削除
4	TOE 利用者(TA2)	• TOE が提供する時刻認証子を取得する。 • TOE から取得した時刻認証子を基に時刻情報を生成および保存する。 • TOE から時刻認証子監査を受ける。

5. 資産

以下に TOE の資産として情報資産及び IT 実装を記す。

■情報資産

(1) TOE 設定情報

TOE が動作するために必要な設定情報である。TA2 との時刻同期および時刻認証子の送受信および時刻認証子監査に必要な情報が含まれる。TOE 設定情報は、TOE 機器の OS の管理下にあるファイルとして保管される。

設定情報は、以下のファイルに記録されている。

– ntp.conf

ntpd の設定ファイル

- host.conf
  TOE で生成する時刻認証子のパラメータや動作モードを設定

- host.list
  TOE の監査対象となるホスト（IP アドレス）を設定

(2) システムクロック
TOE のシステムクロックは日本標準時から時刻の提供を受けて、正確な時刻を保持している。システムクロックは、TOE 機器の OS の管理下にある。

(3) 保存される時刻認証子
時刻認証子は、ある時点の時刻の証拠となるデータであり、TA2 の時刻認証子監査および時刻認証子のトレーサビリティの検証に使用される。保存される時刻認証子は、TOE 機器の OS の管理下にあるファイルとして保管される。

(4) TA2 から受信する時刻認証子
TA2 で生成された時刻情報認証子で、ローカルネットワークにて、TOE 機器が受信する。

(5) TA2 に送信される時刻認証子
TOE 機器で生成された時刻認証子で、ローカルネットワークにて、TA2 に送信する。

(6) 時刻認証子監査記録
時刻認証子監査記録は、TOE 機器が TA2 に対して行った時刻認証子監査の結果を記録したものである。時刻認証子監査記録は、TOE 機器の OS の管理下にあるファイルとして保管される。

(7) TA2 へ送信される時刻認証子監査/検証結果
TOE 機器が時刻受信装置に対して実施した時刻認証子監査および時刻時刻認証子検証の結果である。この結果は、ローカルネットワークにて、TOE 機器から時刻受信装置に送信される。

(8) TOE 操作 ID
TOE 関与者（TOE 管理者、TOE 運用者、TOE 監査者）の情報である。TOE 機器の OS により管理される。

(9) TOE 関与者パスワード

TOE 関与者（TOE 管理者、TOE 運用者、TOE 監査者）の情報である。TOE 機器の OS により管理される。

(10) ログ

TOE 機器のログである。ログの内容は下記である。

- システムログ
- OS 起動ログ
- セキュリティ関連ログ（認証）
- ファイル転送に関するログ
- 時刻同期に関するログ

ログは TOE 機器の OS の管理下にあるファイルとして保管される。

(11) Autokey 用私有鍵

NTP の Autokey で使用される私有鍵である。TOE 機器の OS の管理下にあるファイルとして保管される。

■IT 実装

○NTA2

時刻認証子システムソフトウェア

第2章 セキュリティ環境

本 TOE のセキュリティ環境である前提、脅威、組織のセキュリティポリシーを記す。

1. 前提

表 2-1：セキュリティ環境前提

#	分類	項目	説明
1	物理的な前提	A.NTE_LOCATION	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティに設定される。サブシステム管理者の許可のない物理アクセスを防ぐ。
2	物理的な前提	A.NTE_ENVIRONMENT	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
3	物理的な前提	A.NTE_MEDIA	TOE（及び関連するコンポーネント）で使用するストレージ・メディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
4	接続	A.NTE_FIREWALL	ファイヤーウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
5	接続	A.NTE_TA2_CONNECTION	TA2 と TOE の間の通信路は、TA2 の成りすまし、データの改ざん、データの盗聴を防止する。
6	接続	A.NTE_PEER	TOE と通信する意図された TA2 は、信頼できる。
7	人的な前提	A.NTE_ADMINISTRATOR	一つ以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報セキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 • TOE の起動・停止を実行する。 • TOE に関わるユーザ/役割を管理する。 • 暗号機能に関わる初期化及び管理業務を行う。 • TOE 上で悪意のあるソフトウェアが動作しないようにする。 • TOE の要件を満たす適切なディスクスペースを用意する。 さらに彼らは、信頼できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
8	人的な前提	A.NTE_OPERATOR	一人以上の許可された運用者が割り当てられる。 • TOE 管理者の指示の元で各種設定など運用業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
9	人的な前提	A.NTE_AUDITOR	一人以上の許可された監査者が割り当てられる。 • 時刻認証子監査記録を取得し、分析を行う。

			• TOE に関するログを取得し、分析を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
10	人的な前提	A.NTE_USER	一人以上の許可された TOE 利用者が割り当てられる。 • TOE から時刻認証子を受信する。 • 時刻認証子を生成･保存する。 • TOE へ時刻認証子を送信する。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
11	その他	A.NTE_ABSTRACT	TOE（及び関連するコンポーネント） が動作するために必要な OS は、システムクロックを除き、不正な改変から保護され、正しく動作するものと仮定する。
12	その他	A.NTE_SEPARATION	TOE が動作する機器には、TOE の動作に必要なソフトウェア以外はインストールされないものとする。

2. 脅威

表 2-2：脅威

#	項目	説明
1	T.NTE_SECRET_1	ハッカーが、TOE が動作する機器の OS にネットワークを介して、アクセスすることによって、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
2	T.NTE_SECRET_2	ハッカーが、TOE が動作する機器の画面や放射する電磁波を解析することにより、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
3	T.NTE_SECRET_3	ハッカーが、TOE が動作する機器間の通信を傍受することにより、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
4	T.NTE_TAMP_1	ハッカーが、TOE が動作する機器の OS にネットワークを介してアクセスすることによって、TOE が動作する機器の保護対象資産を改ざん/削除するかもしれない。
5	T.NTE_TAMP_2	ハッカーが、TOE が動作する機器を破壊することにより、保護対象資産を削除するかもしれない。
6	T.NTE_TAMP_3	ハッカーが、TOE が動作する機器間の通信を傍受することにより、保護対象資産を改ざん/削除するかもしれない。
7	T.NTE_MISS	サブシステム管理者またはサブシステム運用者が、操作ミスによって、アクセスが許可されている保護対象資産を改ざんまたは削除してしまうかもしれない。
8	T.NTE_WEAK_CRYPT_1	ハッカーが、暗号アルゴリズムの脆弱性により、過去に生成した時刻認証子を改竄するかもしれない。
9	T.NTE_WEAK_CRYPT_2	TOE 機器が時刻認証子生成に脆弱化した暗号アルゴリズムを使用しているため、改竄可能な時刻認証子を発行するかもしれない。
10	T.NTE_MODIFY_	ハッカーにより、ネットワークを介してアクセスすることによって、

	CLOCK_1	TOE が動作する機器のシステムクロックを改竄されてしまうかもしれない。
11	T.NTE_MODIFY_CLOCK_2	ハッカーにより、TOE が動作する機器を破壊することにより、TOE が動作する機器のシステムクロックを停止されてしまうかもしれない。
12	T.NTE_MODIFY_CLOCK_3	TOE が動作する機器のシステムクロックが、自然に日本標準時との誤差が大きくなるかもしれない。
13	T.NTE_TIME_SOURCE	ハッカーが、ネットワークを介してアクセスすることによって、TOE が動作する機器の参照する時刻ソース源を変更してしまうかもしれない。
14	T.NTE_HARDWARE_FAILURE	経年劣化や偶然に引き起こされる障害により、TOE のハードウェアが故障し、資産が失われる。
15	T.NTE_PEER_FAILURE	通信相手となる他システムのダウンにより、TOE の資産が失われる。
16	T.NTE_CONNECTION_FAILURE	通信回線の故障により、TOE の資産が失われる。
17	T.NTE_TOE_BUG	TOE の IT 実装にソフトウェア不良が存在するため、TOE の資産の信頼性が乏しくなる。
18	T.NTE_BUFFEROVERFLOW_ATTACK	ネットワーク上の悪意者が、バッファ・オーバーフローの脆弱性を利用し、TOE の管理者権限を取得する。
19	T.NTE_DOS_ATTACK	ネットワーク上の悪意者が、不正なデータを送信して TOE を使用不能に陥らせるかもしれない。

3. 組織のセキュリティポリシー

表 2-3：組織のセキュリティポリシー

#	項目	説明
1	P.NTE_DUAL_CONTROL（合議）	TOE の管理業務における重要な操作は、サブシステム管理者による合議の上で行うこととする。 また TOE の運用業務における重要な操作は、複数のサブシステム運用者による合議の上で行うこととする。
2	P.NTE_CRYPTOGRAPHY（暗号アルゴリズムの管理）	TOE が動作する機器で時刻認証子の結合に使用される暗号アルゴリズムは、「電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省）」に記載されたアルゴリズムによって実装されなければならない。
3	P.NTE_CHECK_VIRUS（ウイルス対策）	定期的なウイルスチェックを実行する。
4	P.NTE_SYSTEM_CLOCK_MANAGEMENT（システムクロックの管理）	TOE が動作する機器のシステム時計を信頼のできる時刻ソースと同期させる。
5	P.NTE_TIMESOURCE（時刻ソース）	TOE は、信頼できる時刻ソースを参照する。この時刻ソースは、TOE 管理者にとってアベイラブルである。また、時刻ソースの信頼性と正確性は TOE 管理者にとって受容可能である。
6	P.NTE_KEY_STORAGE（鍵の管理）	すべての私有鍵は、安全に保管される。TOE 管理者以外の人間からのアクセスを防ぐ。
7	P.NTE_PASSWORD_	TOE 関与者のパスワードは、TOE 関与者本人によって適切に管理さ

	MANAGEMENT（パスワードの管理）	れ、本人以外に知られてはならない。
8	P.NTE_PROTECT_LOG（ログの保護）	TOE を利用する組織は、ログの暴露、改ざん、または削除の防止のために必要な措置をとることとする。
9	P.NTE_CHECK_ABSTRUCT _VULNERABILITY（脆弱性確認）	定期的に、OS、ライブラリおよび暗号アルゴリズムの脆弱性を確認し、対策を行う。

第3章 セキュリティ目標・対策と実装システムの評価

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

本 TOE に対するセキュリティの目標と対策を記し、実装システムの評価を行う。

表 3-1：セキュリティ目標・対策及び評価

#	脅威名	セキュリティ目標・対策		統合化システムにおける実現
1	T.NTE_SECRET_1	防止	ファイヤーウォールの設置をする。	A.NTE_FIREWALL により実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.nTE_PROTECT_LOG により実現可能である。
		回復	なし	
2	T. NTE_SECRET_2	防止	TOE 機器を物理的に侵入困難な場所に設置する。	A.NTE_LOCATION、A.NTE_ENVIRONMENT により実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	なし	
3	T. NTE_SECRET_3	防止	通信をローカルネットワークのみで行う。	ローカルネットワークでのみ通信を行うことにより実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	なし	
4	T. NTE_TAMP_1	防止	ファイヤーウォールの設置をする。	A.NTE_FIREWALL により実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。
5	T. NTE_TAMP_2	防止	TOE 機器を物理的に侵入困難な場所に設置する。	A.NTE_LOCATION、A.NTE_ENVIRONMENT により実現可能である。
		検出	なし	
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。

6	T. NTE_TAMP_3	防止	通信をローカルネットワークのみで行う。	ローカルネットワークでのみ通信を行うことにより実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	なし	
7	T.NTE_MISS	防止	TOE 関与者に教育を行う。 運用を複数で行う。	P.NTE_DUAL_CONTROL により実現可能である。
		検出	ログの記録をする。 時刻認証子監査を実施し、正常に動作していることを確認する。	ログ生成機能により実現 P.NTE_PROTECT_LOG 、 A.NTE_AUDITOR により実現可能である。
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。
8	T. NTE_WEAK_CRYPT_1	防止	時刻認証子をセキュア保管する。	A.NTE_LOCATION 、 A.NTE_FIREWALL により実現可能である。
		検出	定期的に、暗号アルゴリズムの脆弱性を確認する。	P.NTE_CHECK_ABSTRUCT_VULNERABILITY により実現可能である。
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。
9	T. NTE_WEAK_CRYPT_2	防止	脆弱化した暗号アルゴリズムを使用しない。	P.NTE_CRYPTOGRAPHY により実現している。
		検出	定期的に、暗号アルゴリズムの脆弱性を確認する。	P.NTE_CHECK_ABSTRUCT_VULNERABILITY により実現可能である。
		回復	なし	
10	T. NTE_MODIFY_CLOCK_1	防止	ファイヤーウォールの設置をする。	A.NTE_FIREWALL により実現している。
		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
11	T. NTE_MODIFY_CLOCK_2	防止	TOE 機器を物理的に侵入困難な場所に設置する。	A.NTE_LOCATION 、 A.NTE_ENVIRONMENT により実現可能である。

		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	NTPD を再起動させることにより、信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
12	T. NTE_MODIFY_CLOCK_3	防止	NTP によって、時刻の補正を行う。	時刻補正機能により実現している。
		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現している。
		回復	信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
13	T. NTE_TIME_SOURCE	防止	ファイヤーウォールの設置をする。	A.NTE_FIREWALL により実現している。
		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現している。
		回復	信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
14	T. NTE_HARDWARE_ FAILURE	防止	機器を 2 重化する。	マシンを 2 重化し、常時待機させることにより実現可能である。
		検出	なし	
		回復	機器を入れ替える。	TOE 機器と同等のハードウェアを用意し、故障したハードウェアと入れ替えることにより実現可能である。
15	T. NTE_PEER_FAILURE	防止	他の TA 相当システムからも時刻認証子の送受信を行う。	TA2 以外に TA 相当システムを準備し、TA 相当システムからも時刻認証子の送受信を行うことにより実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	通信相手の復帰後、再接続する。	通信相手の復帰後、再接続することにより実現可能である。
16	T. NTE_CONNECTION_ FAILURE	防止	複数の通信手段を用意する。	電話回線、専用回線等複数の通信手段を用意することにより実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。

		回復	通信復帰後、再接続する。	通信相手の復帰後、再接続することにより実現可能である。
17	T. NTE_TOE_BUG	防止	ソフトウェア不良を防ぐ、開発プロセスを採用する。	A.NTE_ADMINISTRATOR により実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	パッチ作成・配布・適用を適切に実施する。 （システムを停止させた場合）安全確認後、システムを再起動する。	パッチ作成・配布・適用を適切に実施し、（システムを停止させた場合）安全確認後、システムを再起動することにより実現可能である。
18	T. NTE_BUFFEROVERFLOW_ATTACK	防止	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。	P.NTE_CHECK_ABSTRACT_VULNERABILITY により実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	（システムを停止させた場合）安全確認後、システムを再起動する。	（システムを停止させた場合）安全確認後、システムを再起動することにより実現可能である。
19	T. NTE_DOS_ATTACK	防止	TOE 機器のシステムを冗長構成にし、負荷を分散する。	TOE 機器を複数用意し、同一のサービスを実行させることにより実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.NTE_PROTECT_LOG により実現可能である。
		回復	なし	

2. 前提の実現方法例

第 2 章セキュリティ環境の 1. 前提の実現方法例を以下に記す。

表 3-2：前提の実現方法例

#	前提名	実現方法例
1	A.NTE_LOCATION	TOE の設置場所は、ID カード等を用いた入退出管理が施された居室である。 ID カードは、TOE にアクセスすることを許可されたユーザにのみ配布される。
2	A.NTE_ENVIRONMENT	TOE の設置場所は、適切に電磁波対策、電力対策がなされた居室であ

		る。また、温度･湿度の管理が行われている。
3	A.NTE_MEDIA	TOE（及び関連するコンポーネント）で使用するストレージ･メディアは、動作確認を行ったものを使用しており、データの損失と破壊はないものとしている。また、定期的にメディアを入れ替えることのより、データの損失と破壊を防止する。
4	A.NTE_FIREWALL	TOE 機器と外部ネットワークとの接続にはファイヤーウォールを介して行っている。
5	A.NTE_TA2_CONNECTION	TOE 機器と TA2 の間の通信は、プライベートネットワーク内で行われているため、データの改ざん、データの盗聴を防止している。
6	A.NTE_PEER	TOE と通信する TA2 は、信頼できる第三者機関である。
7	A.NTE_ADMINISTRATOR	TOE 管理者は、情報処理推進機構(IPA)等の情報システムの管理･運用に関する公的資格を持ち、TOE の運用規定、運用マニュアル、管理規定、管理マニュアル、利用規定、利用マニュアルの策定を行う。TOE 管理者は、TOE 運用規定、運用マニュアルを遵守する人物を TOE 運用者として選出する。TOE 管理者は、TOE 管理規定、管理マニュアルを遵守する人物を TOE 管理者として選出する。TOE 管理者は、TOE 利用規定、利用マニュアルを遵守する人物を TOE 利用者として選出する。
8	A.NTE_OPERATOR	TOE 運用者は、TOE 運用規定、運用マニュアルを遵守し、TOE 管理者の指示の下で TOE の運用を行う。
9	A.NTE_AUDITOR	TOE 監査者は、TOE 管理規定、管理マニュアルを遵守し、TOE 管理の行う。
10	A.NTE_USER	TOE 利用者は、TOE 利用規定、利用マニュアルを遵守し、TOE を利用する。
11	A.NTE_ABSTRACT	TOE（及び関連するコンポーネント）が動作するために必要な OS は、TOE 運用者による動作確認がなされているため、正しく動作している。
12	A.NTE_SEPARATION	TOE 関与者は信頼できるため、彼らが故意に不必要なソフトウェアをインストールすることはない。

3. 組織のセキュリティポリシーの実現方法例

第 2 章セキュリティ環境の 3.　組織のセキュリティポリシーの実現例を以下に記す。

表 3-3：組織のセキュリティポリシーの実現方法例

#	セキュリティポリシー名	実現方法例
1	P.NTE_DUAL_CONTROL	TOE の管理業務における重要な操作は、統合化プラットフォームシステムのそれぞれの管理者の合議の上で行われている。 また TOE の運用業務における重要な操作は、複数のサブシステム運用者による合議の上で行われている。
2	P.NTE_CRYPTOGRAPHY	TOE が動作する機器で使用する暗号アルゴリズムは、「電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省）」に記載されたアルゴリズムによってのみ実装されている。
3	P.NTE_CHECK_VIRUS	TOE 機器にウイルス対策ソフトウェアがインストールされており、定期的にウイルス定義ファイルをアップデートし、ウイルスチェックを実行している。
4	P.NTE_SYSTEM_CLOCK_MANAGEMENT	TOE の時刻同期機能によって、TOE のシステム時計は日本標準時と同期している。

5	Ｐ.NTIMESOURCE	TOE が動作する機器のシステム時計の参照する時刻ソースは、NTA2 であり、NTA2 のシステム時計は、日本標準時と同期しているため信頼性と正確性を保持している。
6	Ｐ.NTE_KEY_STORAGE	TOE で使用している私有鍵は、OS のファイルアクセス制御機能により、TOE 管理者以外の人間からのアクセスを防いでいる。
7	P.NTE_PASSWORD_MANAGEMENT	TOE 関与者のパスワードは、TOE 関与者本人によって適切に管理され、本人以外には知られていない。
8	P.NTE_PROTECT_LOG	TOE の機器のログファイルは、OS のファイルアクセス制御機能により、TOE 管理者以外の人間からのアクセスを防いでいる。
9	P.NTE_CHECK_ABSTRUCT_VULNERABILITY	定期的に情報処理推進機構(IPA)等の Web ページをチェックし、OS、ライブラリおよび暗号アルゴリズム等の脆弱性を確認する。使用している OS、ライブラリおよび暗号アルゴリズム等に脆弱性を確認した場合、アップデートおよび暗号アルゴリズム変更等の対策を実行する。

第4章 脅威ツリー及びリスク評価一覧

1. 脅威ツリー

以下に攻撃シナリオのモデリングに使用した脅威ツリーを記載する。

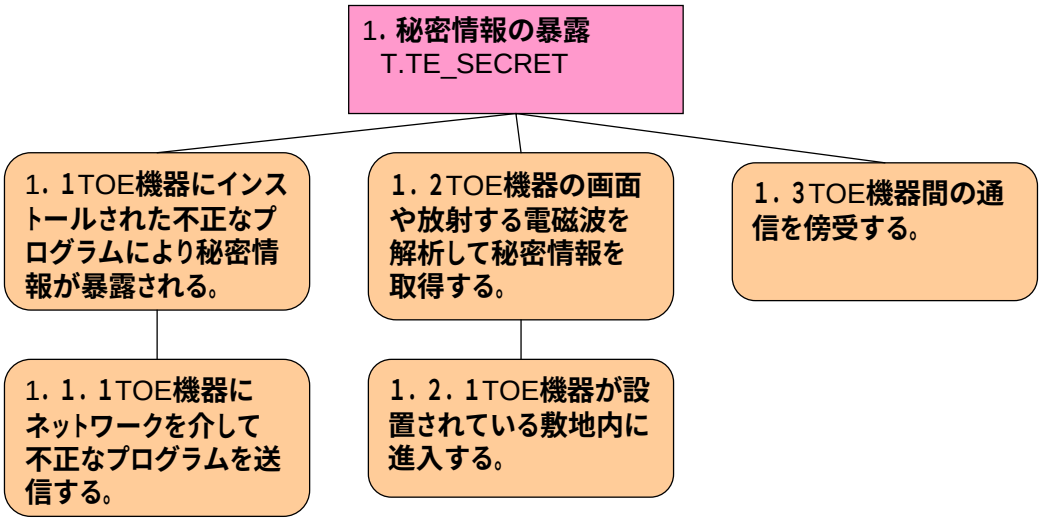


図 4-1：脅威ツリー（秘密情報の暴露）

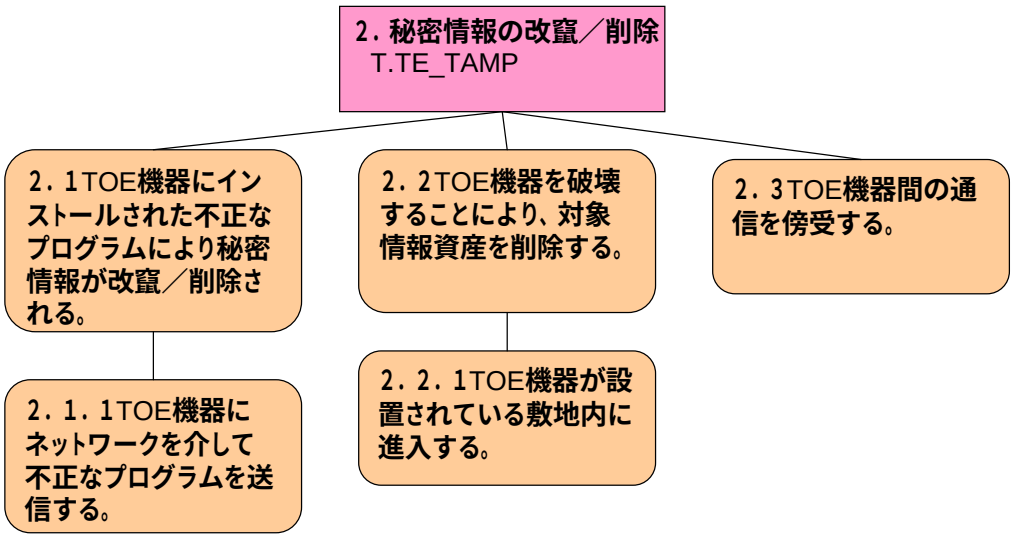


図 4-2：脅威ツリー（秘密情報の改竄／削除）

図 4-3：脅威ツリー（操作ミスによるデータ改竄／削除）

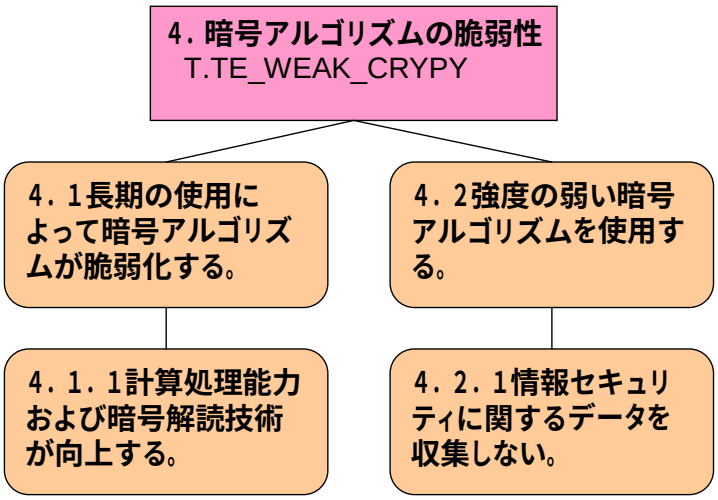


図 4-4：脅威ツリー（暗号アルゴリズムの脆弱性）

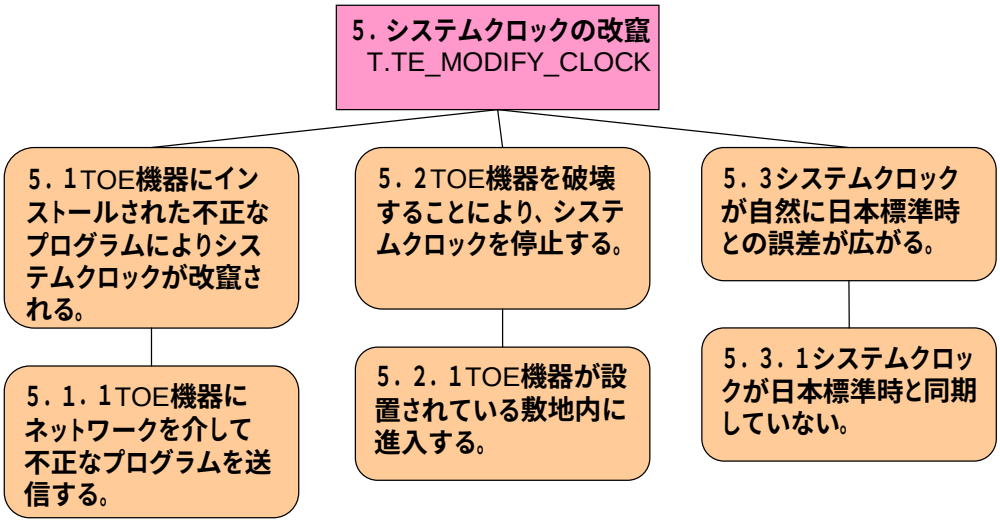


図 4-5：脅威ツリー（システムクロックの改竄）

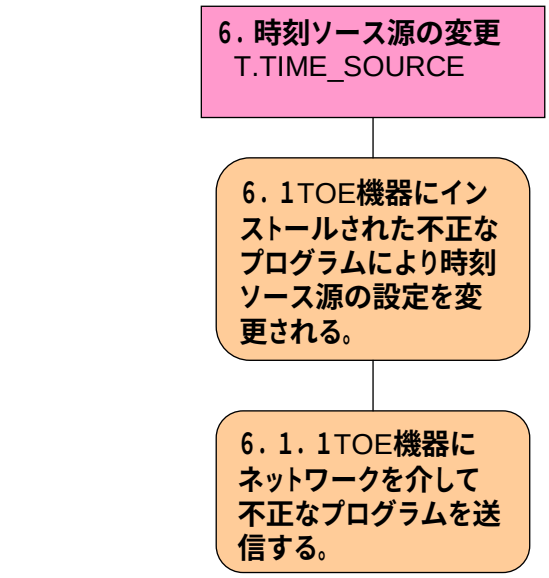


図 4-6：脅威ツリー（時刻ソース源の変更）

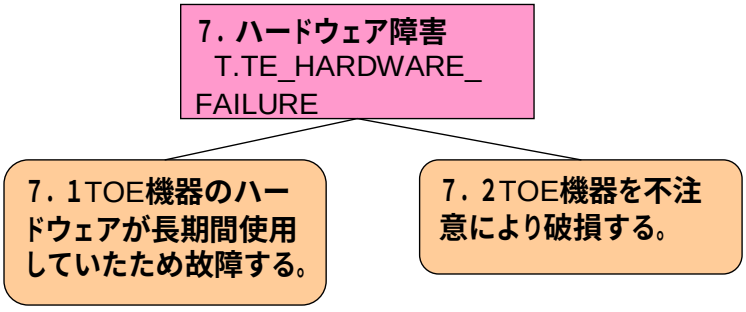


図 4-7：脅威ツリー（ハードウェア障害）

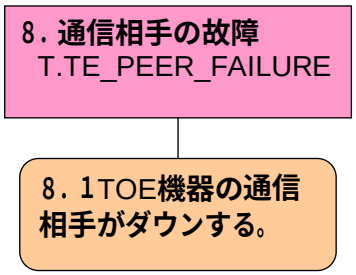


図 4-8：脅威ツリー（通信相手の故障）

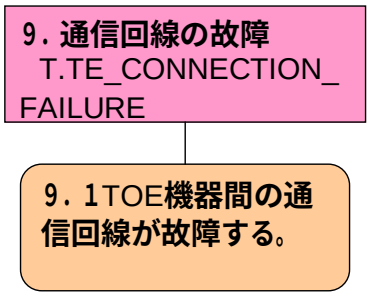


図 4-9：脅威ツリー（通信回線の故障）

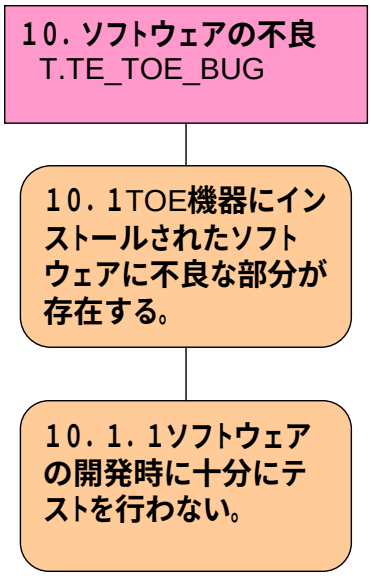


図 4-10：脅威ツリー（ソフトウェアの不良）

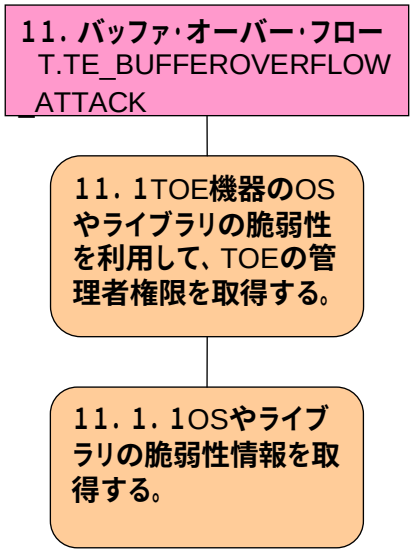


図 4-11：脅威ツリー（バッファ・オーバー・フロー）

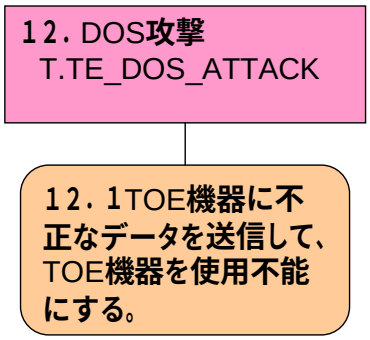


図 4-12：脅威ツリー（DOS 攻撃）

2. リスク格付けの考え方

抽出した今日に対してリスク評価を行う。リスク評価のために私用した脅威格付け表を以下に記す。

表 4-1：脅威格付け表

	格付け	高 (3)	中 (2)	低 (1)
D	潜在的損失 (Damage potential)	TOE に係わる機密情報。改竄･漏洩により、TOE の機器が正常に動作しない可能性がある。	TOE に係わる機密情報が改竄･漏洩する。	機密性の低い情報が改竄･漏洩する。
R	再現性 (Reproducibility)	いつでも攻撃を再現することが可能である。	ある時間帯、かつ、特定の条件において、攻撃を再現することが可能である。	セキュリティホールの知識があったとしても、攻撃を再現することは非常に困難である。
E	攻撃利用可能性 (Exploitability)	初心者のプログラマーであったとしても短時間で攻撃可能である。	習熟したプログラマーであれば、攻撃可能である。攻撃が成功すれば繰り返すことが可能。	非常に習熟したプログラマーであれば攻撃可能。攻撃の度に高度な知識が必要。
A	影響ユーザ (Affected users)	全てのTOE関与者	多数のサブシステム利用者	非常に少数のサブシステム利用者
D	発見可能性 (Discoverability)	攻撃に関する公開情報がある。脆弱性は一般的であり、気付かれやすい。	製品のほとんど使用されない部分に脆弱性がある。少数のユーザがその脆弱性を見つける。	そのバグは、知られていない。ユーザは潜在的損失を分析できない。

3. リスク評価点

表の脅威格付け表に基づき、各脅威に対するリスク評価点を以下に記す。

表 4-2：リスク評価点

#	脅威	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.TE_SECRET_1	中(2)	低(1)	低(1)	高(3)	中(2)	9
2	T.TE_SECRET_2	中(2)	中(2)	低(1)	高(3)	中(2)	10
3	T.TE_SECRET_3	中(2)	低(1)	低(1)	高(3)	低(1)	8
4	T.TE_TAMP_1	中(2)	低(1)	低(1)	高(3)	中(2)	9
5	T.TE_TAMP_2	中(2)	低(1)	低(1)	高(3)	低(1)	8
6	T.TE_TAMP_3	中(2)	低(1)	低(1)	高(3)	低(1)	8
7	T.TE_MISS	高(3)	低(1)	高(3)	高(3)	高(3)	13
8	T.TE_WEAK_CRYPT_1	中(2)	低(1)	中(2)	高(3)	高(3)	11
9	T.TE_WEAK_CRYPT_2	高(3)	低(1)	中(2)	高(3)	高(3)	12

10	T.TE_MODIFY_CLOCK_1	高(3)	低(1)	低(1)	高(3)	中(2)	10
11	T.TE_MODIFY_CLOCK_2	高(3)	低(1)	低(1)	高(3)	低(1)	9
12	T.TE_MODIFY_CLOCK_3	高(3)	中(2)	中(2)	高(3)	高(3)	13
13	T.TE_TIME_SOURCE	高(3)	低(1)	低(1)	高(3)	低(1)	9
14	T.TE_HARDWARE_ FAILURE	高(3)	低(1)	中(2)	高(3)	低(1)	10
15	T.TE_PEER_FAILURE	高(3)	低(1)	中(2)	高(3)	低(1)	10
16	T.TE_CONNECTION_ FAILURE	高(3)	低(1)	中(2)	高(3)	低(1)	10
17	T.TE_TOE_BUG	高(3)	中(2)	中(2)	高(3)	低(1)	11
18	T.TE_BUFFEROVERFLOW _ATTACK	高(3)	高(3)	中(2)	高(3)	高(3)	14
19	T.TE_DOS_ATTACK	中(2)	高(3)	高(3)	高(3)	高(3)	14

第5章 内部不正を考慮したセキュリティ評価

上記では、TOE 関与者を信頼できるため内部不正による脅威は考慮する必要が無かった。しかし、本セクションでは、TOE 関与者を信頼できないと仮定した場合の脅威抽出及びセキュリティ目標・対策を記す。

ただし、内部不正を単独で行われるものとし、TOE 関与者の結託はないものとする。また、TOE 関与者と外部者との連携した不正はないものとする。

1. 前提

本 TOE の内部不正を考慮したセキュリティ環境の前提を以下に記す。

表 5-1：内部不正を考慮した前提

#	分類	項目	説明
1	物理的な前提	A.NTE_LOCATION	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティに設定される。サブシステム管理者の許可のない物理アクセスを防ぐ。
2	物理的な前提	A.NTE_ENVIRONMENT	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
3	物理的な前提	A.NTE_MEDIA	TOE（及び関連するコンポーネント）で使用するストレージ・メディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
4	接続	A.NTE_FIREWALL	ファイヤーウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
5	接続	A.NTE_TA2_CONNECTION	TA2 と TOE の間の通信路は、NTA2 の成りすまし、データの改ざん、データの盗聴を防止する。
6	接続	A.NTE_PEER	TOE と通信する意図された TA2 は、信頼できる。
7	人的な前提	A.NTE_ADMINISTRATOR	一つ以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報セキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 • TOE の起動・停止を実行する。 • TOE に関わるユーザ/役割を管理する。 • 暗号機能に関わる初期化及び管理業務を行う。 • TOE 上で悪意のあるソフトウェアが動作しないようにする。 • TOE の要件を満たす適切なディスクスペースを用意する。 ただし彼らは、権限を濫用し、故意にセキュリティを低めないとは限らない。
8	人的な前提	A.NTE_OPERATOR	一人以上の許可された運用者が割り当てられる。 • TOE 管理者の指示の元で各種設定など運用業務を行う。 ただし彼らは、権限を濫用し、故意にセキュリティを低め

			ないとは限らない。
9	人的な前提	A.NTE_AUDITOR	一人以上の許可された監査者が割り当てられる。 • 時刻認証子監査記録を取得し、分析を行う。 • TOE に関するログを取得し、分析を行う。 ただし彼らは、権限を濫用し、故意にセキュリティを低めないとは限らない。
10	人的な前提	A.NTE_USER	一人以上の許可された TOE 利用者が割り当てられる。 • TOE から時刻認証子を受信する。 • 時刻認証子を生成･保存する。 • TOE へ時刻認証子を送信する。 ただし彼らは、権限を濫用し、故意にセキュリティを低めないとは限らない。

2. 内部不正による脅威

本 TOE の内部不正を考慮した場合に追加される脅威を以下に記す。

表 5-2：内部不正を考慮した脅威

#	項目	説明
1	T.NTE_SECRET_4	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
2	T.NTE_SECRET_5	TOE 関与者が、TOE が動作する機器のデータをメディア等にコピーすることにより、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
3	T.NTE_TAMP_4	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、TOE が動作する機器の保護対象資産を改竄/削除するかもしれない。
4	T.NTE_TAMP_5	TOE 関与者が、TOE が動作する機器のデータファイル等をコマンド等から操作することにより、保護対象資産を改竄/削除するかもしれない。
5	T.NTE_WEAK_CRYPT_3	TOE 関与者が、意図的に強度の弱い暗号アルゴリズムを使用するかもしれない。
6	T.NTE_MODIFY_CLOCK_4	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、システムクロックを改竄されてしまうかもしれない。
7	T.NTE_MODIFY_CLOCK_5	TOE 関与者が、TOE が動作する機器のコマンドにより、システムクロックを改竄されてしまうかもしれない。
8	T.NTE_TIME_SOURCE_2	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、TOE の参照する時刻ソース源を変更してしまうかもしれない。

9	T.NTE_TIME_SOURCE_3	TOE 関与者が、TOE が動作する機器の設定を変更し、時刻ソース源を変更してしまうかもしれない。
10	T.NTE_HARDWARE_2 FAILURE	TOE 関与者が、意図的に TOE 機器を破壊してしまうかもしれない。
11	T.NTE_CONNECTION_ FAILURE_2	TOE 関与者が、意図的に通信回線を破壊することにより、TOE の資産が失われる。
12	T.NTE_TOE_BUG_2	TOE 関与者が、意図的に TOE の IT 実装を不良が埋め込まれたソフトウェアにすり替えたため、TOE の資産の信頼性が乏しくなる。

3. 組織のセキュリティポリシー

本 TOE の内部不正を考慮した組織のセキュリティポリシーを以下に記す。

表 5-3：内部不正を考慮した組織のセキュリティポリシー

#	項目	説明
1	P.NTE_DUAL _CONTROL（合議）	TOE の管理業務における重要な操作は、サブシステム管理者による合議の上で行うこととする。 また TOE の運用業務における重要な操作は、複数のサブシステム運用者による合議の上で行うこととする。
2	P.NTE_CRYPTOGRAPHY（暗号アルゴリズムの管理)	TOE が動作する機器で時刻認証子の結合に使用される暗号アルゴリズムは、「電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されなければならない。
3	P.NTE_CHECK_VIRUS（ウイルス対策）	定期的なウイルスチェックを実行する。
4	P.NTE_SYSTEM_CLOCK _MANAGEMENT（システムクロックの管理）	TOE が動作する機器のシステム時計を信頼のできる時刻ソースと同期させる。
5	P.NTE_TIMESOURCE（時刻ソース）	TOE は、信頼できる時刻ソースを参照する。この時刻ソースは、TOE 管理者にとってアベイラブルである。また、時刻ソースの信頼性と正確性は TOE 管理者にとって受容可能である。
6	P.NTE_KEY_STORAGE（鍵の管理）	すべての私有鍵は、安全に保管される。TOE 管理者以外の人間からのアクセスを防ぐ。
7	P.NTE_PASSWORD_ MANAGEMENT（パスワードの管理）	TOE 関与者のパスワードは、TOE 関与者本人によって適切に管理され、本人以外に知られてはならない。
8	P.NTE_PROTECT_LOG（ログの保護）	TOE を利用する組織は、ログの暴露、改ざん、または削除の防止のために必要な措置をとることとする。
9	P.NTE_CHECK_ABSTRUCT _VULNERABILITY（脆弱性確認）	定期的に、OS、ライブラリおよび暗号アルゴリズムの脆弱性を確認し、対策を行う。

4. 内部不正による脅威のツリー

以下に内部不正を考慮した攻撃シナリオに使用した脅威ツリーを記載する。着色されたものが、内部不正を考慮した部分である。

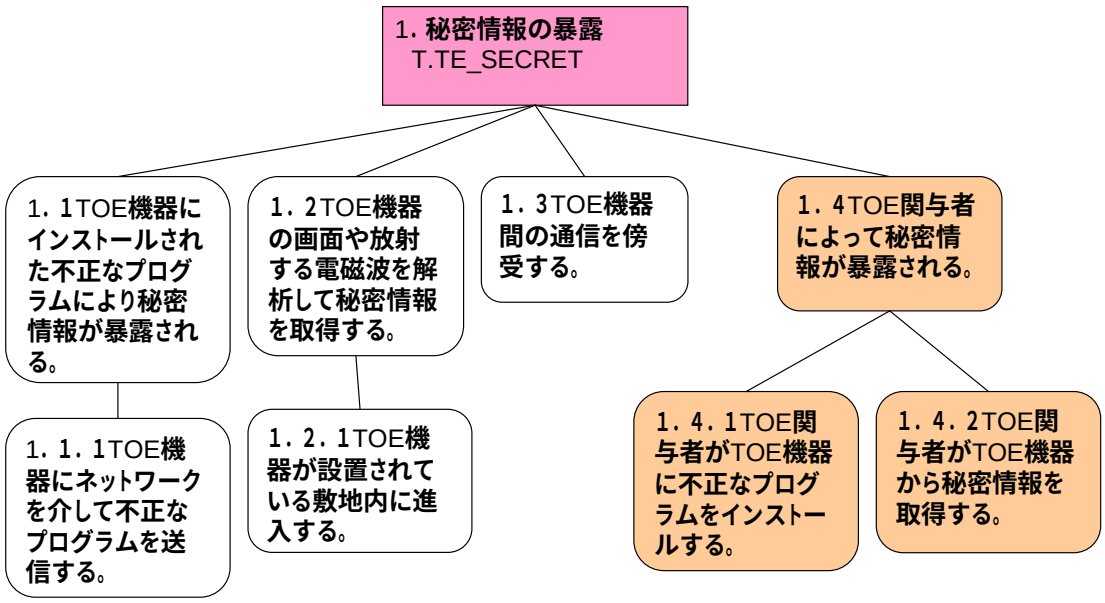


図 5-1：内部不正を考慮した脅威ツリー（秘密情報の暴露）

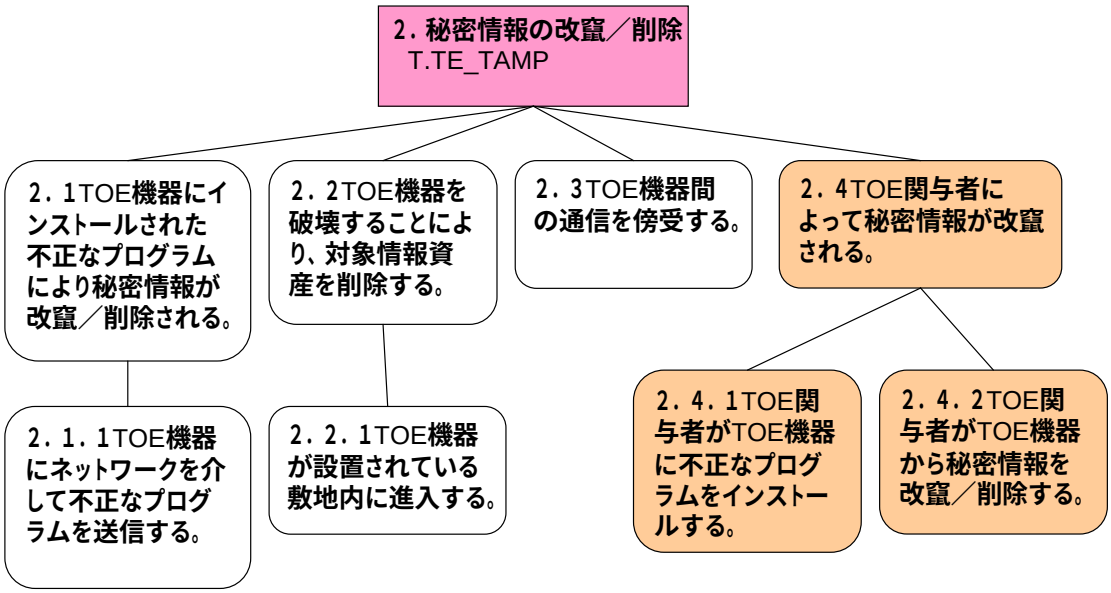


図 5-2：内部不正を考慮した脅威ツリー（秘密情報の改竄／削除）

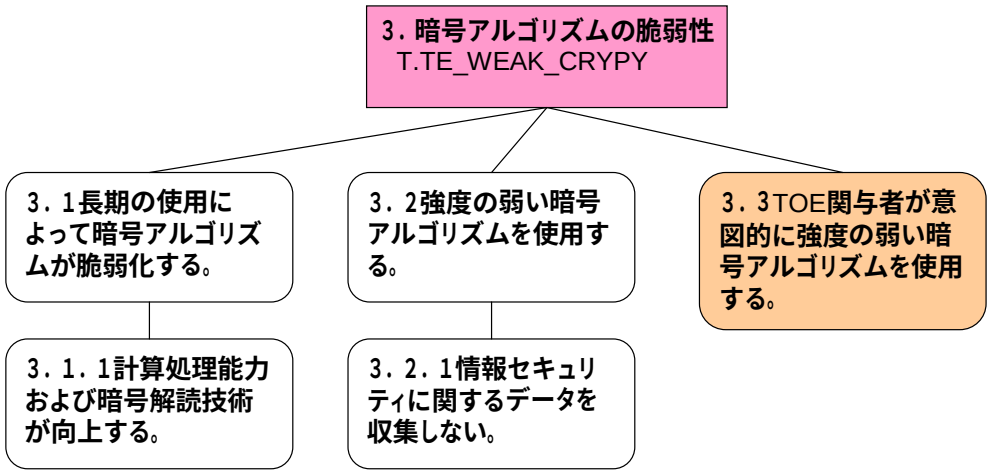


図 5-3：内部不正を考慮した脅威ツリー（暗号アルゴリズムの脆弱性）

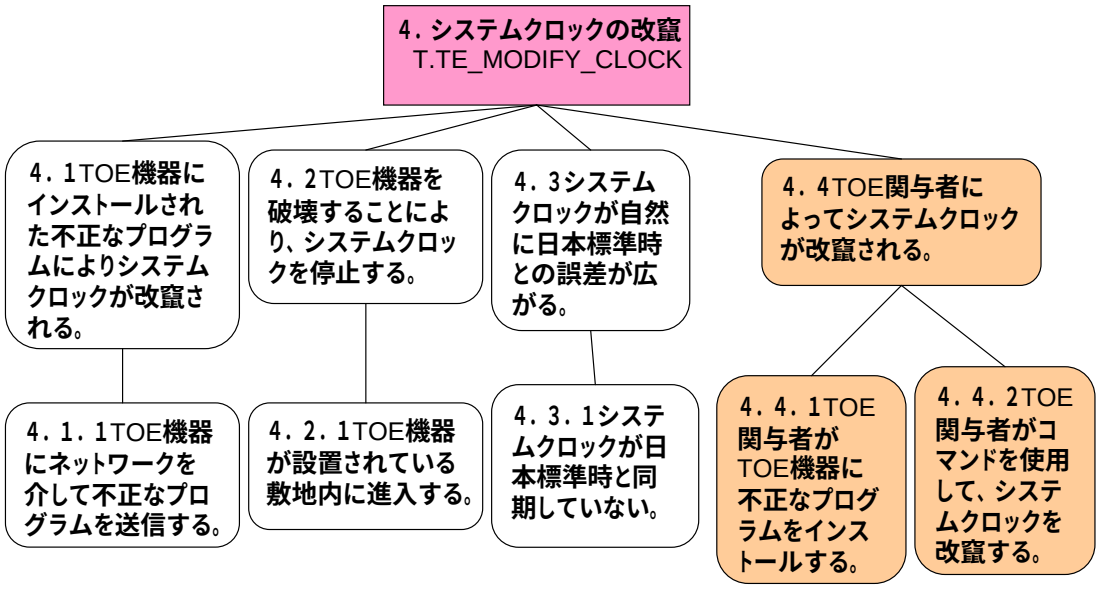


図 5-4：内部不正を考慮した脅威ツリー（システムクロックの改竄）

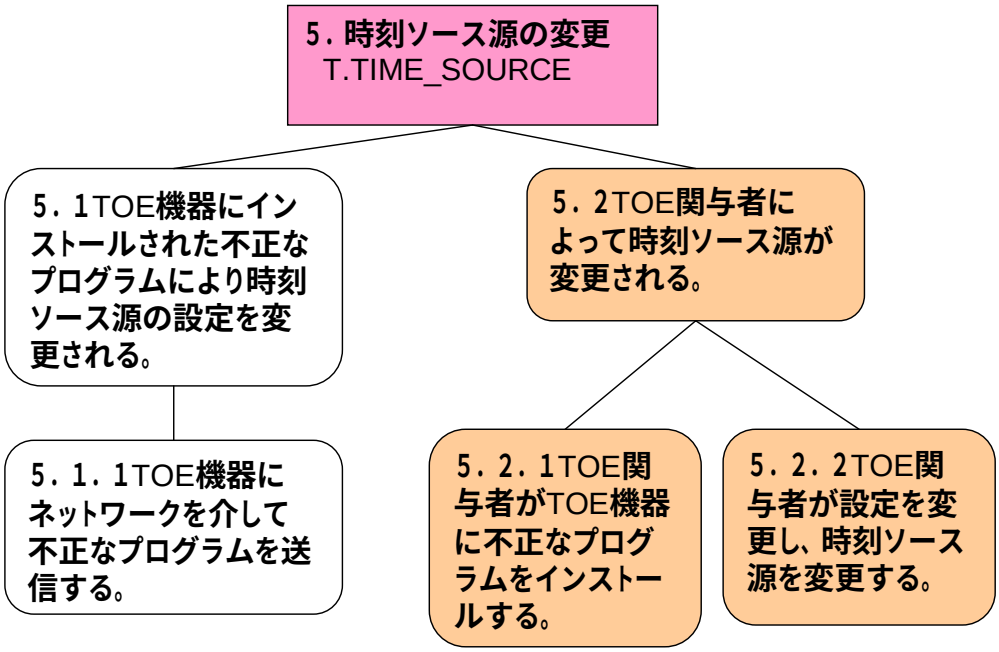


図 5-5：内部不正を考慮した脅威ツリー（時刻ソース源の変更）

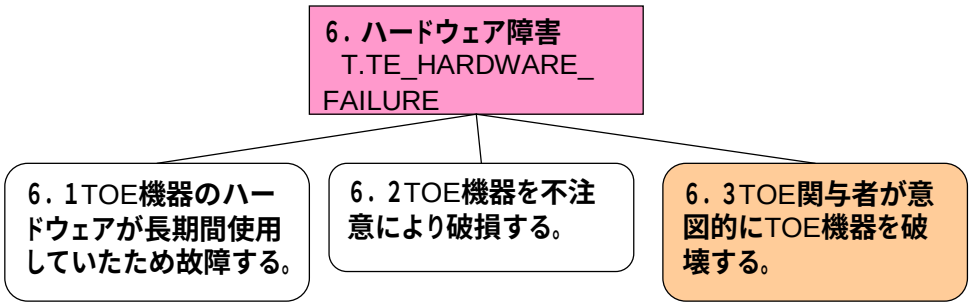


図 5-6：内部不正を考慮した脅威ツリー（ハードウェア障害）

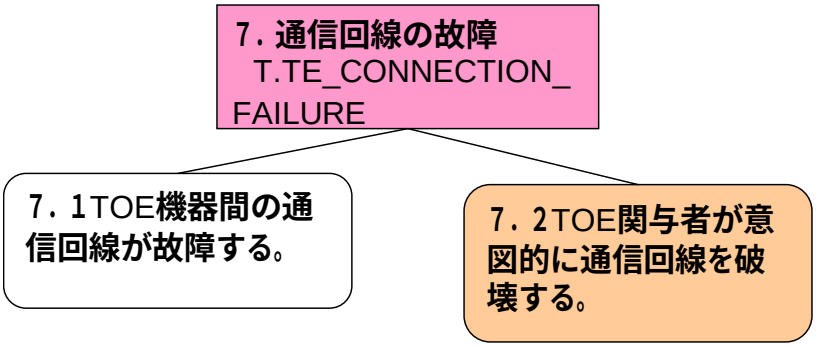


図 5-7：内部不正を考慮した脅威ツリー（通信回線の故障）

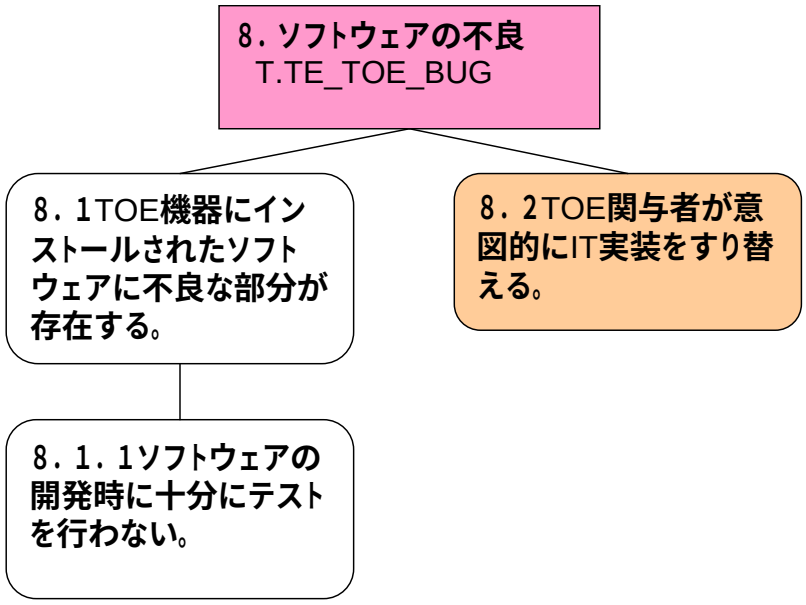


図 5-8：内部不正を考慮した脅威ツリー（ソフトウェアの不良）

5. 内部不正による脅威のセキュリティ目標・対策

本 TOE の内部不正を考慮したセキュリティ目標と対策を以下に記す。

表 5-4：内部不正を考慮したセキュリティ目標・対策

#	脅威名	セキュリティ目標・対策	
1	T.NTE_SECRET_4	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存を信頼できる第三者が行うものとする。
		回復	なし
2	T. NTE_SECRET_5	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存を信頼できる第三者が行うものとする。
		回復	なし
3	T. NTE_TAMP_4	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。

		検出	ログの記録をし、ログの保存を信頼できる第三者が行うものとする。
		回復	データのバックアップをし、バックアップデータの保存を信頼できる第三者が行うものとする。保存されてバックアップデータでリストアを実施する。
4	T. NTE_TAMP_5	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	データのバックアップをし、バックアップデータの保存を信頼できる第三者が行うものとする。保存されてバックアップデータでリストアを実施する。
5	T. NTE_WEAK_CRYPT_3	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	データのバックアップをし、バックアップデータの保存を信頼できる第三者が行うものとする。保存されてバックアップデータでリストアを実施する。
6	T. NTE_MODIFY_CLOCK_4	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
7	T. NTE_MODIFY_CLOCK_5	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
8	T. NTE_TIME_SOURCE_2	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
9	T. NTE_TIME_SOURCE_3	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
10	T. NTE_HARDWARE_FAILURE_2	防止	TOE 機器の設置場所の入場には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	TOE 機器の設置場所の入場の記録をし、記録されたログの保存は信頼できる第三者が行うものとする。
		回復	機器を入れ替える。
11	T. NTE_CONNECTION_	防止	TOE 機器の設置場所の入場には、複数の TOE 関与者の合議の上でのみ可能とする。

	FAILURE_2	検出	TOE 機器の設置場所の入場の記録をし、記録されたログの保存は信頼できる第三者が行うものとする。
		回復	通信復帰後、再接続する。
12	T. NTE_TOE_BUG_2	防止	TOE 機器内のソフトウェアが改竄されていないか否かを定期的に確認する。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	パッチ作成・配布・適用を適切に実施する。 （システムを停止させた場合）安全確認後、システムを再起動する。

以上

セキュリティ評価報告書

(TOE： TA2)

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

1. TOE の機能概要

TOE は、「時刻情報配信機能」、「時刻情報検証機能」、「時刻情報監査機能」の 3 つの機能から構成される。

1-1 時刻情報配信機能

1-1-1 時刻情報生成機能

現在一般的に使用されているシステムの時刻は、権限を持ったユーザであれば容易に変更することが可能となっており、かつ、変更したことを検出することは困難である。また、TA などの時刻の提供を行う機関から監査を受けることにより、時刻の不正操作を防止することは可能であるが、過去の特定の時刻において、その時点での時刻が正確であったことを示すことは困難である。

本機能において生成される時刻情報（以下、「時刻認証子」と記す）は、過去に生成された時刻認証子を元に生成されており、時刻認証子を改ざんするには、過去に生成された時刻認証子も改ざんさせる必要がある。そのため、時刻認証子の改ざんは困難であり、改ざんの検出も可能となっている。また、時刻認証子に第三者が予測不能なデータを付加することにより、時刻認証子の先読みによる不正生成が困難となっている。

TOE 利用者に提供される時刻認証子には、一般的な時刻表記（例：2004 年 6 月 11 日 15 時 29 分 41 秒）に加え、NTA2 からの時刻配信経路上の機関の情報と誤差が記されており、TOE 利用者は自身の受け取った時刻認証子の配信経路を特定することが可能となっている。

1-1-2 時刻配信機能

TOE にて生成された時刻認証子は、時刻同期の標準的なプロトコルである NTPv4 を用いることにより時刻受信装置に配信される。NTPv4 により時刻の配信を受けた時刻受信装置は、受信した時刻認証子を元にして時刻認証子を生成する。TOE 機器から受け取る時刻認証子を予測することは非常に困難であるため、時刻受信装置は時刻認証子の偽造・改ざんを行うことはほぼ不可能と考えられる。TOE 機器内で保存されている時刻認証子を用いることにより、時刻受信装置の不正を検出することが可能となる。

1-1-3 時刻補正機能

時刻認証子の配信には NTPv4 を用いているため、時刻受信装置は時刻認証子の受信時に TOE 機器と時刻同期を行う。

1-2 時刻情報検証機能

時刻受信装置が受け取った時刻認証子の NTA2 までの配信経路と誤差を検証する。

時刻認証子に記載されている配信パス上の各機関を特定する情報（IP アドレス）が正しいか確認する。確認方法は、配信経路上の各機関の保有する配信ログの情報と検証対象の時刻認証子とのハッシュリンクの整合性を確認することにより行う。

1-3 時刻情報監査機能

TOE は、時刻受信装置における時刻認証子の改竄防止および検出のため、定期的に監査を行う（時刻受信装置から監査要求があった場合も監査を行う）。

監査方法は、時刻受信装置が過去に生成した時刻認証子のリンクの整合性を確かめることにより、時刻認証子が時刻受信装置で不正なく保存されていたか否かを確認することである。監査結果は、TOE にて保存される。

2. TOE 構成図

以下の図 1-1 に TOE 構成図を記す。

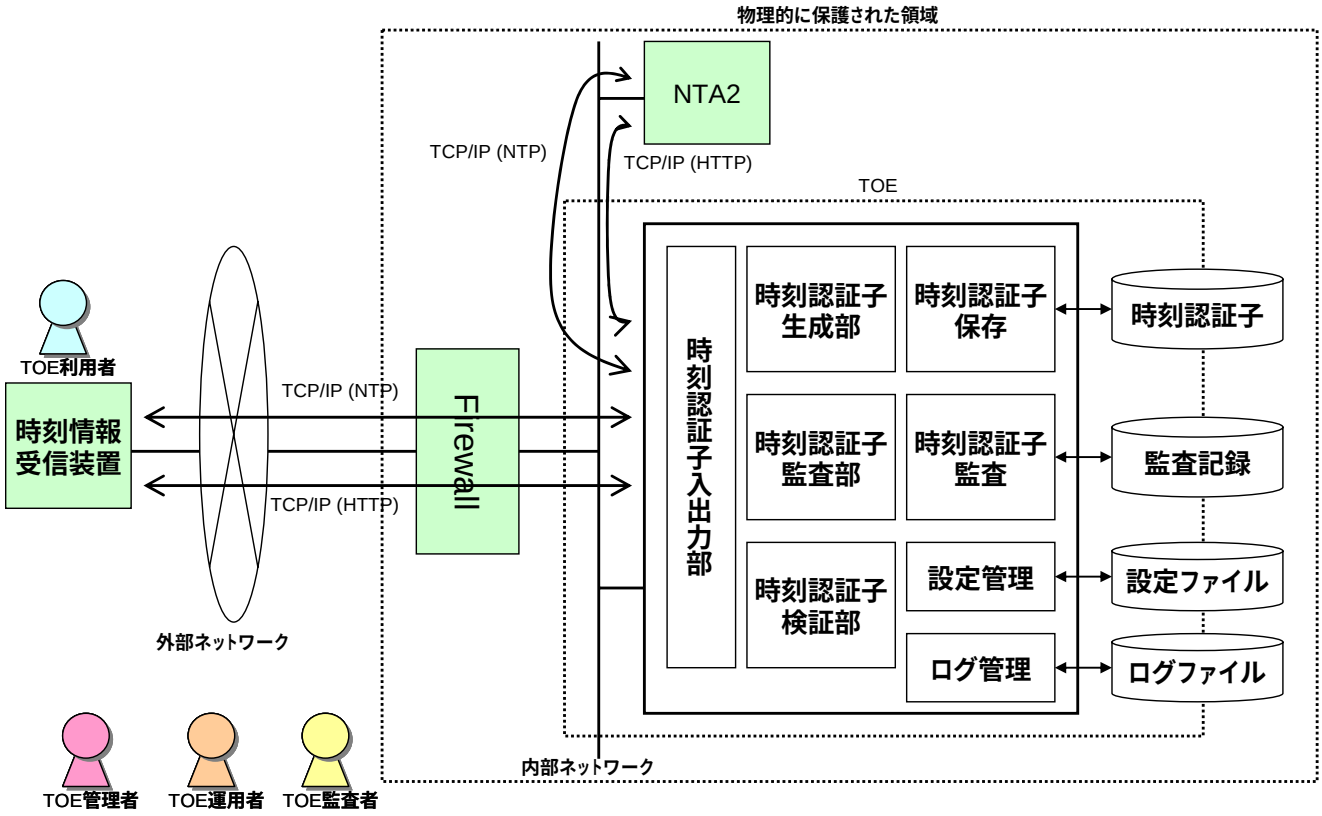


図 1-1：TOE 構成図

3. 利用する暗号技術と暗号コンポーネント構成図

以下に TOE で使用する暗号技術と暗号コンポーネントの構成図を記す。

表 1-1：使用する暗号技術

#	使用している暗号技術	使用目的

暗号技術１	ハッシュ関数	SHA256、SHA384、SHA512	時刻認証子の結合（ハッシュリンク生成）
暗号技術２	公開鍵暗号	RSA (512bit)	NTP の autokey 機能における鍵交換に使用
暗号技術３	ハッシュ関数	MD5	NTP パケットのメッセージ認証

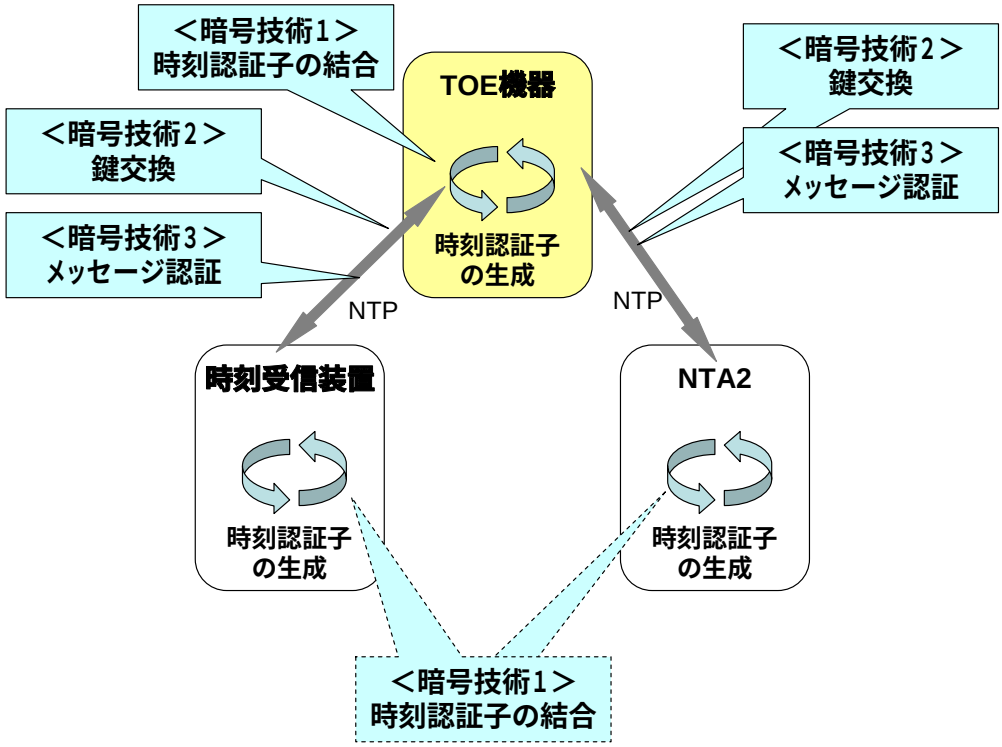


図 1-2：TOE で使用される暗号技術

上記の暗号技術は、TOE で時刻認証子のトレーサビリティ検証及び時刻認証子監査で使用される。以下の図にトレーサビリティ検証の処理の流れ、図に時刻認証子監査を処理の流れを記す。

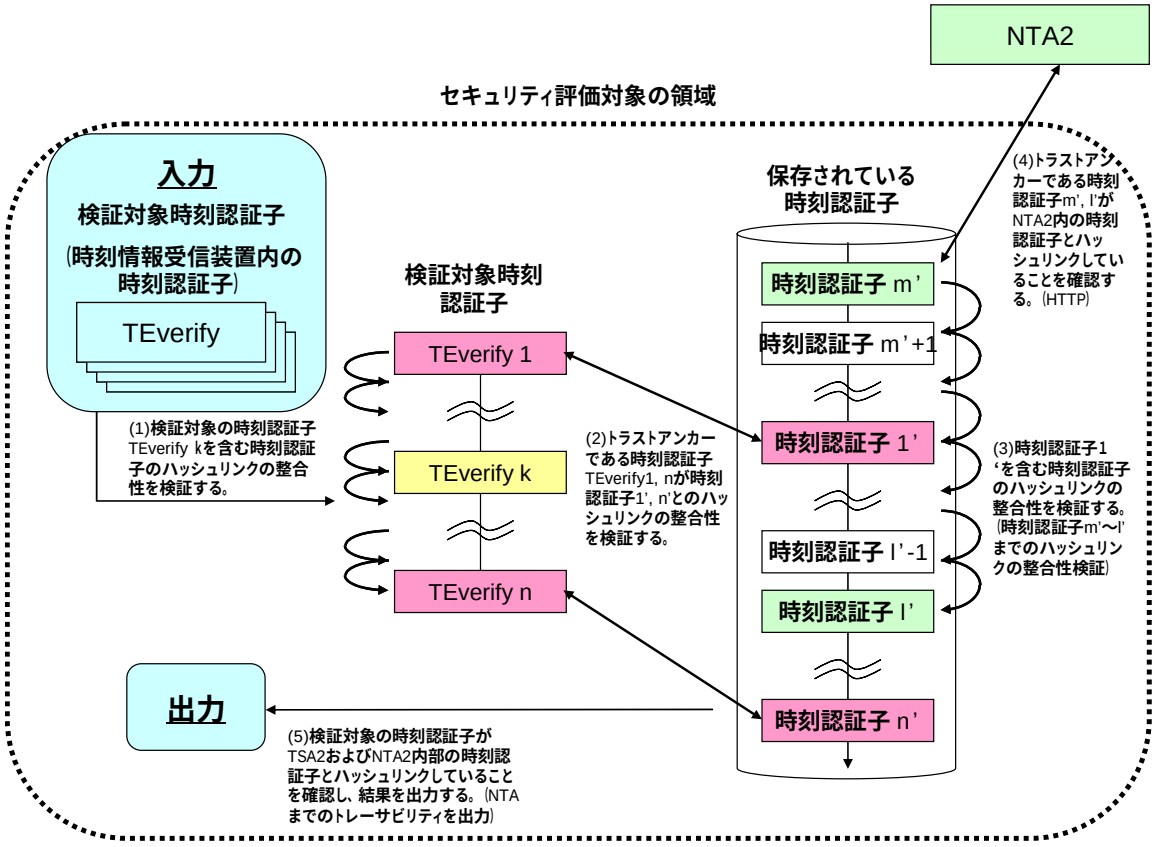


図 1-3：トレーサビリティ検証処理の流れ

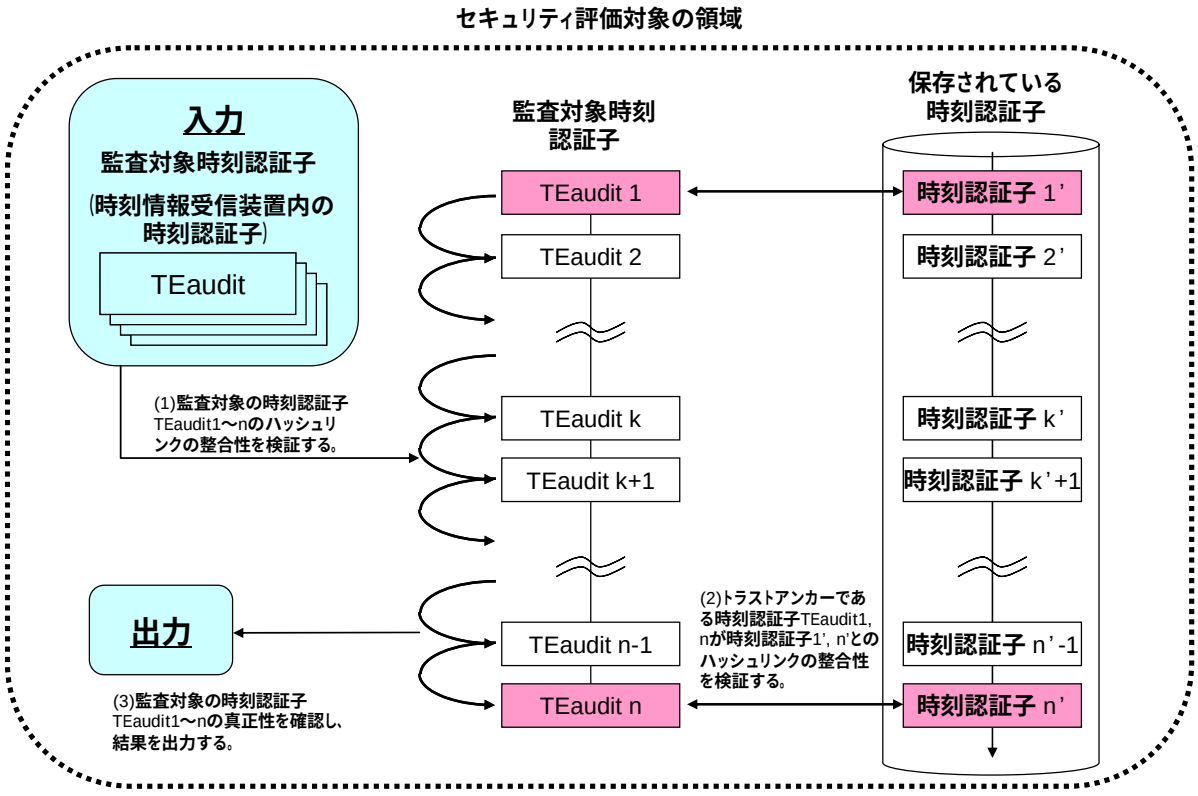


図 1-4：時刻認証子監査処理の流れ

4. TOE 関与者

表 1-2 に本 TOE 関与者を記す。

表 1-2：TOE 関与者

#	関与者	説明
1	TOE 管理者	• TOE の起動・停止を実行する。 • TOE に関わるユーザ/役割を管理する。具体的には、以下の作業を行う。 – ユーザの登録/削除 – 設定ファイルのアクセス権変更
2	TOE 運用者	• TOE 管理者の指示の元で以下の運用業務を行う。具体的には、以下の作業を行う。 – TA2 のインストール – TA2 を使用するためのセットアップ – 時刻情報配信先への時刻認証子監査を実施 – 設定ファイルの変更 – 時刻認証子の閲覧/複製/削除 – TA2 で生成される TA2 利用者に関する時刻認証子監査記録の閲覧/削除
3	TOE 監査者	• NTA2 からの時刻認証子監査記録を取得し、分析を行う。 • TOE の時刻認証子監査を実施し、生成される時刻認証子監査記録の分析を行う。具体的には、以下の作業を行う。 – 時刻認証子監査記録ファイルの分析 – 時刻認証子監査記録ファイルの取り出し/削除
4	TOE 利用者	• TOE が提供する時刻認証子を取得する。 • TOE から取得した時刻認証子を基に時刻情報を生成および保存する。 • TOE から時刻認証子監査を受ける。
5	NTA2	• TOE へ時刻認証子を提供する。 • TOE は NTA2 から取得した時刻認証子を基に時刻認証子を生成および保存する。 • TOE は NTA2 から時刻認証子監査を受ける。

5. 資産

以下に TOE の資産として情報資産及び IT 実装を記す。

■情報資産

(1) TOE 設定情報

TOE が動作するために必要な設定情報である。NTA2、時刻受信装置との時刻同期およ

び時刻認証子の送受信および時刻認証子監査に必要な情報が含まれる。TA2 設定情報は、TOE 機器の OS の管理下にあるファイルとして保管される。

設定情報は、以下のファイルに記録されている。

- ntp.conf
  ntpd の設定ファイル

- host.conf
  TOE で生成する時刻認証子のパラメータや動作モードを設定

- host.list
  TOE の監査対象となるホスト（IP アドレス）を設定

(2) システムクロック
TA2 のシステムクロックは日本標準時から時刻の提供を受けて、正確な時刻を保持している。システムクロックは、TOE 機器の OS の管理下にある。

(3) 保存される時刻認証子
時刻認証子は、ある時点の時刻の証拠となるデータであり、時刻受信装置の時刻認証子監査および時刻認証子のトレーサビリティの検証に使用される。保存される時刻認証子は、TOE 機器の OS の管理下にあるファイルとして保管される。

(4) NTA2 から受信する時刻認証子
NTA2 で生成された時刻情報認証子で、ローカルネットワークにて、TOE 機器が受信する。

(5) NTA2 に送信される時刻認証子
TOE 機器で生成された時刻認証子で、ローカルネットワークにて、NTA2 に送信する。

(6) 時刻受信装置から受信する時刻認証子
時刻受信装置で生成された時刻認証子で、インターネットを介して、TOE 機器にて受信する。

(7) 時刻受信装置に送信される時刻認証子
TOE で生成された時刻認証子で、インターネットを介して、時刻受信装置に送信する。

(8) 時刻認証子監査記録

時刻認証子監査記録は、TOE 機器が時刻受信装置に対して行った時刻認証子監査の結果を記録したものである。時刻認証子監査記録は、TOE 機器の OS の管理下にあるファイルとして保管される。

(9) NTA2 から受信する時刻認証子監査結果
NTA2 が TOE 機器に対して実施した時刻認証子監査の結果である。この結果は、ローカルネットワークにて、TOE 機器が NTA2 から受信する。

(10) 時刻受信装置へ送信される時刻認証子監査/検証結果
TOE 機器が時刻受信装置に対して実施した時刻認証子監査および時刻時刻認証子検証の結果である。この結果は、インターネットを介して、TOE 機器から時刻受信装置に送信される。

(11) TOE 操作 ID
TOE 関与者（TOE 管理者、TOE 運用者、TOE 監査者）の情報である。TOE 機器の OS により管理される。

(12) TOE 関与者パスワード
TOE 関与者（TOE 管理者、TOE 運用者、TOE 監査者）の情報である。TOE 機器の OS により管理される。

(13) ログ
TOE 機器のログである。ログの内容は下記である。

- システムログ
- OS 起動ログ
- セキュリティ関連ログ（認証）
- ファイル転送に関するログ
- 時刻同期に関するログ

ログは TOE 機器の OS の管理下にあるファイルとして保管される。

(14) Autokey 用私有鍵
NTP の Autokey で使用される私有鍵である。TOE 機器の OS の管理下にあるファイルとして保管される。

■IT 実装
○TA2
時刻認証子システムソフトウェア

第2章 セキュリティ環境

本 TOE のセキュリティ環境である前提、脅威、組織のセキュリティポリシーを記す。

1. 前提

表 2-1：セキュリティ環境前提

#	分類	項目	説明
1	物理的な前提	A.TE_LOCATION	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティに設定される。サブシステム管理者の許可のない物理アクセスを防ぐ。
2	物理的な前提	A.TE_ENVIRONMENT	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
3	物理的な前提	A.TE_MEDIA	TOE（及び関連するコンポーネント）で使用するストレージ・メディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
4	接続	A.TE_FIREWALL	ファイアウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
5	接続	A.TE_NTA2_CONNECTION	NTA2 と TOE の間の通信路は、NTA2 の成りすまし、データの改ざん、データの盗聴を防止する。
6	接続	A.TE_PEER	TOE と通信する意図された NTA2 は、信頼できる。
7	人的な前提	A.TE_ADMINISTRATOR	一つ以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報セキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 • TOE の起動・停止を実行する。 • TOE に関わるユーザ/役割を管理する。 • 暗号機能に関わる初期化及び管理業務を行う。 • TOE 上で悪意のあるソフトウェアが動作しないようにする。 • TOE の要件を満たす適切なディスクスペースを用意する。 さらに彼らは、信頼できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
8	人的な前提	A.TE_OPERATOR	一人以上の許可された運用者が割り当てられる。 • TOE 管理者の指示の元で各種設定など運用業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
9	人的な前提	A.TE_AUDITOR	一人以上の許可された監査者が割り当てられる。 • 時刻認証子監査記録を取得し、分析を行う。

			• TOE に関するログを取得し、分析を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
10	人的な前提	A.TE_USER	一人以上の許可された TOE 利用者が割り当てられる。 • TOE から時刻認証子を受信する。 • 時刻認証子を生成･保存する。 • TOE へ時刻認証子を送信する。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
11	その他	A.TE_ABSTRACT	TOE（及び関連するコンポーネント） が動作するために必要な OS は、システムクロックを除き、不正な改変から保護され、正しく動作するものと仮定する。
12	その他	A.TE_SEPARATION	TOE が動作する機器には、TOE の動作に必要なソフトウェア以外はインストールされないものとする。

2. 脅威

表 2-2：脅威

#	項目	説明
1	T.TE_SECRET_1	ハッカーが、TOE が動作する機器の OS にネットワークを介して、アクセスすることによって、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
2	T.TE_SECRET_2	ハッカーが、TOE が動作する機器の画面や放射する電磁波を解析することにより、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
3	T.TE_SECRET_3	ハッカーが、TOE が動作する機器間の通信を傍受することにより、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
4	T.TE_TAMP_1	ハッカーが、TOE が動作する機器の OS にネットワークを介してアクセスすることによって、TOE が動作する機器の保護対象資産を改ざん/削除するかもしれない。
5	T.TE_TAMP_2	ハッカーが、TOE が動作する機器を破壊することにより、保護対象資産を削除するかもしれない。
6	T.TE_TAMP_3	ハッカーが、TOE が動作する機器間の通信を傍受することにより、保護対象資産を改ざん/削除するかもしれない。
7	T.TE_MISS	サブシステム管理者またはサブシステム運用者が、操作ミスによって、アクセスが許可されている保護対象資産を改竄または削除してしまうかもしれない。
8	T.TE_WEAK_CRYPT_1	ハッカーが、暗号アルゴリズムの脆弱性により、過去に生成した時刻認証子を改竄するかもしれない。
9	T.TE_WEAK_CRYPT_2	TOE 機器が時刻認証子生成に脆弱化した暗号アルゴリズムを使用しているため、改竄可能な時刻認証子を発行するかもしれない。
10	T.TE_MODIFY_	ハッカーにより、ネットワークを介してアクセスすることによって、

	CLOCK_1	TOE が動作する機器のシステムクロックを改竄されてしまうかもしれない。
11	T.TE_MODIFY_CLOCK_2	ハッカーにより、TOE が動作する機器を破壊することにより、TOE が動作する機器のシステムクロックを停止されてしまうかもしれない。
12	T.TE_MODIFY_CLOCK_3	TOE が動作する機器のシステムクロックが、自然に日本標準時との誤差が大きくなるかもしれない。
13	T.TE_TIME_SOURCE	ハッカーが、ネットワークを介してアクセスすることによって、TOE が動作する機器の参照する時刻ソース源を変更してしまうかもしれない。
14	T.TE_HARDWARE_FAILURE	経年劣化や偶然に引き起こされる障害により、TOE のハードウェアが故障し、資産が失われる。
15	T.TE_PEER_FAILURE	通信相手となる他システムのダウンにより、TOE の資産が失われる。
16	T.TE_CONNECTION_FAILURE	通信回線の故障により、TOE の資産が失われる。
17	T.TE_TOE_BUG	TOE の IT 実装にソフトウェア不良が存在するため、TOE の資産の信頼性が乏しくなる。
18	T.TE_BUFFEROVERFLOW_ATTACK	ネットワーク上の悪意者が、バッファ・オーバーフローの脆弱性を利用し、TOE の管理者権限を取得する。
19	T.TE_DOS_ATTACK	ネットワーク上の悪意者が、不正なデータを送信して TOE を使用不能に陥らせるかもしれない。

3. 組織のセキュリティポリシー

表 2-3：組織のセキュリティポリシー

#	項目	説明
1	P.TE_DUAL_CONTROL（合議）	TOE の管理業務における重要な操作は、サブシステム管理者による合議の上で行うこととする。 また TOE の運用業務における重要な操作は、複数のサブシステム運用者による合議の上で行うこととする。
2	P.TE_CRYPTOGRAPHY（暗号アルゴリズムの管理)	TOE が動作する機器で時刻認証子の結合に使用される暗号アルゴリズムは、「電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されなければならない。
3	P.TE_CHECK_VIRUS（ウイルス対策）	定期的なウイルスチェックを実行する。
4	P.TE_SYSTEM_CLOCK_MANAGEMENT（システムクロックの管理）	TOE が動作する機器のシステム時計を信頼のできる時刻ソースと同期させる。
5	P.TE_TIMESOURCE（時刻ソース）	TOE は、信頼できる時刻ソースを参照する。この時刻ソースは、TOE 管理者にとってアベイラブルである。また、時刻ソースの信頼性と正確性は TOE 管理者にとって受容可能である。
6	P.TE_KEY_STORAGE（鍵の管理）	すべての私有鍵は、安全に保管される。TOE 管理者以外の人間からのアクセスを防ぐ。
7	P.TE_PASSWORD_MANAGEMENT（パスワ	TOE 関与者のパスワードは、TOE 関与者本人によって適切に管理され、本人以外に知られてはならない。

	ードの管理)	
8	P.TE_PROTECT_LOG (ログの保護)	TOE を利用する組織は、ログの暴露、改ざん、または削除の防止のために必要な措置をとることとする。
9	P.TE_CHECK_ABSTRUCT _VULNERABILITY (脆弱性確認)	定期的に、OS、ライブラリおよび暗号アルゴリズムの脆弱性を確認し、対策を行う。

第3章 セキュリティ目標・対策と実装システムの評価

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

本 TOE に対するセキュリティの目標と対策を記し、実装システムの評価を行う。

表 3-1：セキュリティ目標・対策及び評価

#	脅威名	セキュリティ目標・対策		統合化システムにおける実現
1	T.TE_SECRET_1	防止	ファイヤーウォールの設置をする。	A.TE_FIREWALL により実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	なし	
2	T. TE_SECRET_2	防止	TOE 機器を物理的に侵入困難な場所に設置する。	A.TE_LOCATION 、A.TE_ENVIRONMENT により実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	なし	
3	T. TE_SECRET_3	防止	通信の暗号化を行う。	SSL（バージョン 3.0 以上）/TLS（バージョン 1.0 以上）で通信内容を暗号化することで実現可能である。なお、鍵交換に使用するアルゴリズムは RSA1024bit 以上の強度を持ち、暗号化に使用するアルゴリズムは RC4 128bit 以上の強度を持ち、使用するハッシュ関数は SHA-1 以上の強度を持つものとする。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	なし	
4	T. TE_TAMP_1	防止	ファイヤーウォールの設置をする。	A.TE_FIREWALL により実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。
5	T. TE_TAMP_2	防止	TOE 機器を物理的に侵入困難な場所に設置する。	A.TE_LOCATION 、A.TE_ENVIRONMENT により実現可能である。

		検出	なし	
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。
6	T. TE_TAMP_3	防止	通信の暗号化を行う。	SSL（バージョン 3.0 以上）/TLS（バージョン 1.0 以上）で通信内容を暗号化することで実現可能である。なお、鍵交換に使用するアルゴリズムは RSA1024bit 以上の強度を持ち、暗号化に使用するアルゴリズムは RC4 128bit 以上の強度を持ち、使用するハッシュ関数は SHA-1 以上の強度を持つものとする。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	なし	
7	T.TE_MISS	防止	TOE 関与者に教育を行う。 運用を複数で行う。	P.TE_DUAL_CONTROL により実現可能である。
		検出	ログの記録をする。 時刻認証子監査を実施し、正常に動作していることを確認する。	ログ生成機能により実現 P.TE_PROTECT_LOG、A.TE_AUDITOR により実現可能である。
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。
8	T. TE_WEAK_CRYPT_1	防止	時刻認証子をセキュア保管する。	A.TE_LOCATION、A.TE_FIREWALL により実現可能である。
		検出	定期的に、暗号アルゴリズムの脆弱性を確認する。	P.TE_CHECK_ABSTRUCT_VULNERABILITY により実現可能である。
		回復	データのバックアップ/リストアを実施する。	定期的に情報資産のバックアップを行うことで実現可能である。
9	T. TE_WEAK_CRYPT_2	防止	脆弱化した暗号アルゴリズムを使用しない。	P.TE_CRYPTOGRAPHY により実現している。
		検出	定期的に、暗号アルゴリズムの脆弱性を確認する。	P.TE_CHECK_ABSTRUCT_VULNERABILITY により実現可能である。
		回復	なし	
10	T. TE_MODIFY_CLOCK_1	防止	ファイヤーウォールの設置をする。	A.TE_FIREWALL により実現している。

		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
11	T. TE_MODIFY_CLOCK_2	防止	TOE 機器を物理的に侵入困難な場所に設置する。	A.TE_LOCATION 、 A.TE_ENVIRONMENT により実現可能である。
		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	NTPD を再起動させることにより、信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
12	T. TE_MODIFY_CLOCK_3	防止	NTP によって、時刻の補正を行う。	時刻補正機能により実現している。
		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現している。
		回復	信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
13	T. TE_TIME_SOURCE	防止	ファイヤーウォールの設置をする。	A.TE_FIREWALL により実現している。
		検出	ログの記録をする。 時刻認証子監査を実施する。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現している。
		回復	信頼できる時刻配信局と時刻同期させる。	信頼できる時刻配信局と時刻同期させることにより実現可能である。
14	T. TE_HARDWARE_FAILURE	防止	機器を 2 重化する。	マシンを 2 重化し、常時待機させることにより実現可能である。
		検出	なし	
		回復	機器を入れ替える。	TOE 機器と同等のハードウェアを用意し、故障したハードウェアと入れ替えることにより実現可能である。
15	T. TE_PEER_FAILURE	防止	他の NTA 相当システムからも時刻認証子の送受信を行う。	NTA2 以外に NTA 相当システムを準備し、NTA 相当システムからも時刻認証子の送受信を行うことにより実現可能である。

		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	通信相手の復帰後、再接続する。	通信相手の復帰後、再接続することにより実現可能である。
16	T. TE_CONNECTION_ FAILURE	防止	複数の通信手段を用意する。	電話回線、専用回線等複数の通信手段を用意することにより実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	通信復帰後、再接続する。	通信相手の復帰後、再接続することにより実現可能である。
17	T. TE_TOE_BUG	防止	ソフトウェア不良を防ぐ、開発プロセスを採用する。	A.TE_ADMINISTRATOR により実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	パッチ作成・配布・適用を適切に実施する。（システムを停止させた場合）安全確認後、システムを再起動する。	パッチ作成・配布・適用を適切に実施し、（システムを停止させた場合）安全確認後、システムを再起動することにより実現可能である。
18	T. TE_BUFFEROVERFLOW_ATTACK	防止	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。	P.TE_CHECK_ABSTRACT_VULNERABILITY により実現している。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	（システムを停止させた場合）安全確認後、システムを再起動する。	（システムを停止させた場合）安全確認後、システムを再起動することにより実現可能である。
19	T. TE_DOS_ATTACK	防止	TOE 機器のシステムを冗長構成にし、負荷を分散する。	TOE 機器を複数用意し、同一のサービスを実行させることにより実現可能である。
		検出	ログの記録をする。	ログ作成機能により実現している。 P.TE_PROTECT_LOG により実現可能である。
		回復	なし	

2. 前提の実現方法例

第 2 章セキュリティ環境の 1. 前提の実現方法例を以下に記す。

表 3-2：前提の実現方法例

#	前提名	実現方法例
1	A.TE_LOCATION	TOE の設置場所は、ID カード等を用いた入退出管理が施された居室である。 ID カードは、TOE にアクセスすることを許可されたユーザにのみ配布される。
2	A.TE_ENVIRONMENT	TOE の設置場所は、適切に電磁波対策、電力対策がなされた居室である。また、温度･湿度の管理が行われている。
3	A.TE_MEDIA	TOE（及び関連するコンポーネント）で使用するストレージ･メディアは、動作確認を行ったものを使用しており、データの損失と破壊はないものとしている。また、定期的にメディアを入れ替えることのより、データの損失と破壊を防止する。
4	A.TE_FIREWALL	TOE 機器と外部ネットワークとの接続にはファイヤーウォールを介して行っている。
5	A.TE_NTA2_CONNECTION	NTA2 と TA2 の間の通信は、プライベートネットワーク内で行われているため、データの改ざん、データの盗聴を防止している。
6	A.TE_PEER	TOE と通信する NTA2 は、信頼できる第三者機関である。
7	A.TE_ADMINISTRATOR	TOE 管理者は、情報処理推進機構(IPA)等の情報システムの管理･運用に関する公的資格を持ち、TOE の運用規定、運用マニュアル、管理規定、管理マニュアル、利用規定、利用マニュアルの策定を行う。TOE 管理者は、TOE 運用規定、運用マニュアルを遵守する人物を TOE 運用者として選出する。TOE 管理者は、TOE 管理規定、管理マニュアルを遵守する人物を TOE 管理者として選出する。TOE 管理者は、TOE 利用規定、利用マニュアルを遵守する人物を TOE 利用者として選出する。
8	A.TE_OPERATOR	TOE 運用者は、TOE 運用規定、運用マニュアルを遵守し、TOE 管理者の指示の下で TOE の運用を行う。
9	A.TE_AUDITOR	TOE 監査者は、TOE 管理規定、管理マニュアルを遵守し、TOE 管理の行う。
10	A.TE_USER	TOE 利用者は、TOE 利用規定、利用マニュアルを遵守し、TOE を利用する。
11	A.TE_ABSTRACT	TOE（及び関連するコンポーネント）が動作するために必要な OS は、TOE 運用者による動作確認がなされているため、正しく動作している。
12	A.TE_SEPARATION	TOE 関与者は信頼できるため、彼らが故意に不必要なソフトウェアをインストールすることはない。

3. 組織のセキュリティポリシーの実現方法例

第 2 章セキュリティ環境の 3.　組織のセキュリティポリシーの実現例を以下に記す。

表 3-3：組織のセキュリティポリシーの実現方法例

#	セキュリティポリシー名	実現方法例
1	P.TE_DUAL_CONTROL	TOE の管理業務における重要な操作は、統合化プラットフォームシステムのそれぞれの管理者の合議の上で行われている。

		また TOE の運用業務における重要な操作は、複数のサブシステム運用者による合議の上で行われている。
2	P.TE_CRYPTOGRAPHY	TOE が動作する機器で使用する暗号アルゴリズムは、、「電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省)」に記載されたアルゴリズムによってのみ実装されている。
3	P.TE_CHECK_VIRUS	TOE 機器にウイルス対策ソフトウェアがインストールされており、定期的にウイルス定義ファイルをアップデートし、ウイルスチェックを実行している。
4	Ｐ.TE_SYSTEM_CLOCK_MANAGEMENT	TOE の時刻同期機能によって、TOE のシステム時計は NTA2 と同期している。NTA2 のシステム時計は、日本標準時と同期しているため信頼できる。
5	Ｐ .TE_TIMESOURCE	TOE が動作する機器のシステム時計の参照する時刻ソースは、NTA2 であり、NTA2 のシステム時計は、日本標準時と同期しているため信頼性と正確性を保持している。
6	Ｐ.TE_KEY_STORAGE	TOE で使用している私有鍵は、OS のファイルアクセス制御機能により、TOE 管理者以外の人間からのアクセスを防いでいる。
7	P.TE_PASSWORD_MANAGEMENT	TOE 関与者のパスワードは、TOE 関与者本人によって適切に管理され、本人以外には知られていない。
8	P.TE_PROTECT_LOG	TOE の機器のログファイルは、OS のファイルアクセス制御機能により、TOE 管理者以外の人間からのアクセスを防いでいる。
9	P.TE_CHECK_ABSTRUCT_VULNERABILITY	定期的に情報処理推進機構(IPA)等の Web ページをチェックし、OS、ライブラリおよび暗号アルゴリズム等の脆弱性を確認する。使用している OS、ライブラリおよび暗号アルゴリズム等に脆弱性を確認した場合、アップデートおよび暗号アルゴリズム変更等の対策を実行する。

第4章 脅威ツリー及びリスク評価一覧

1. 脅威ツリー

以下に攻撃シナリオのモデリングに使用した脅威ツリーを記載する。

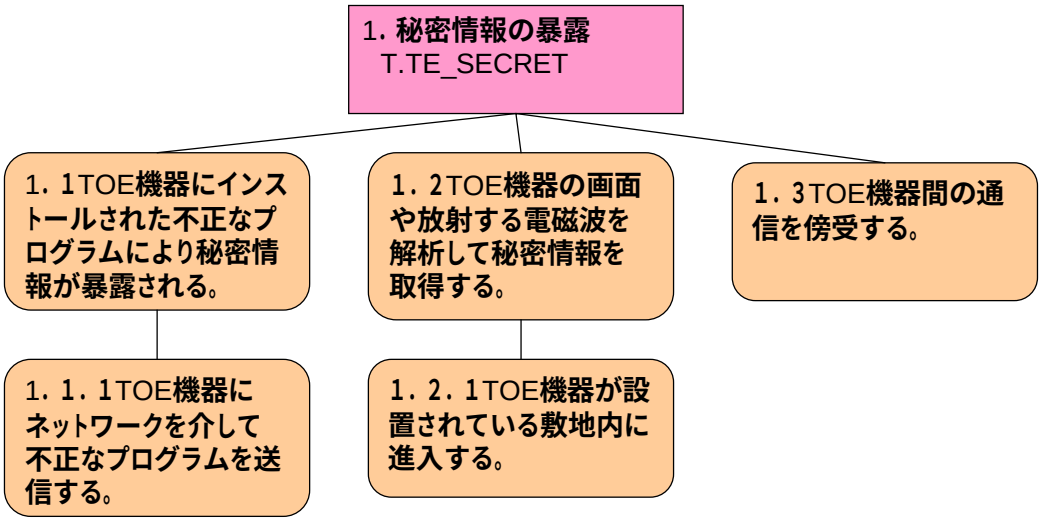


図 4-1：脅威ツリー（秘密情報の暴露）

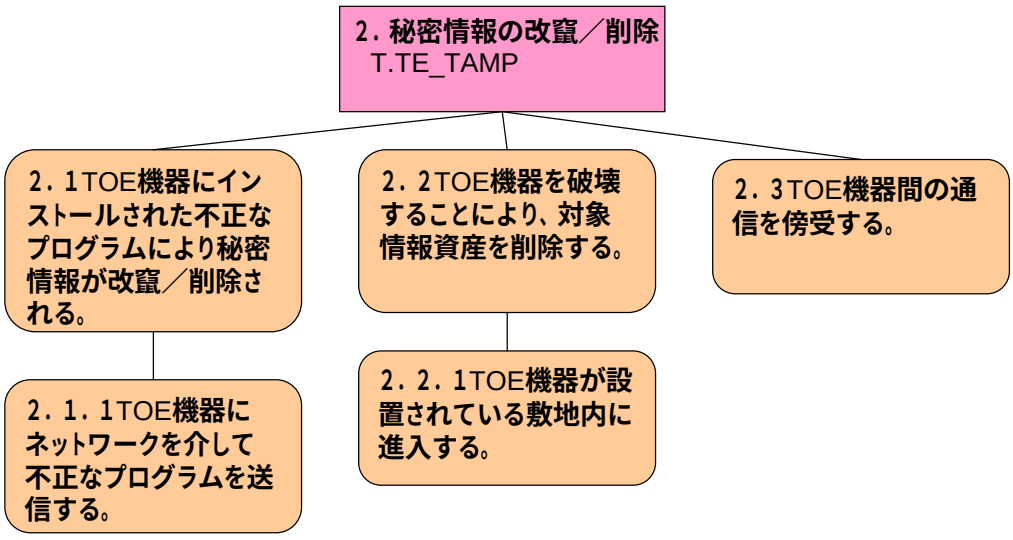


図 4-2：脅威ツリー（秘密情報の改竄／削除）

図 4-3：脅威ツリー（操作ミスによるデータ改竄／削除）

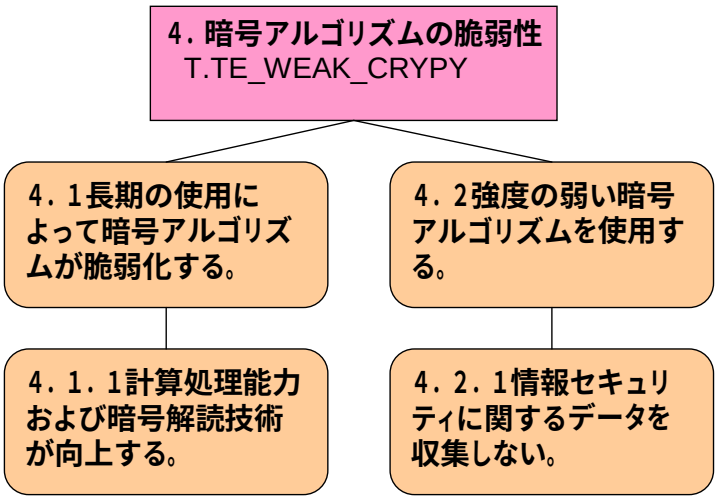


図 4-4：脅威ツリー（暗号アルゴリズムの脆弱性）

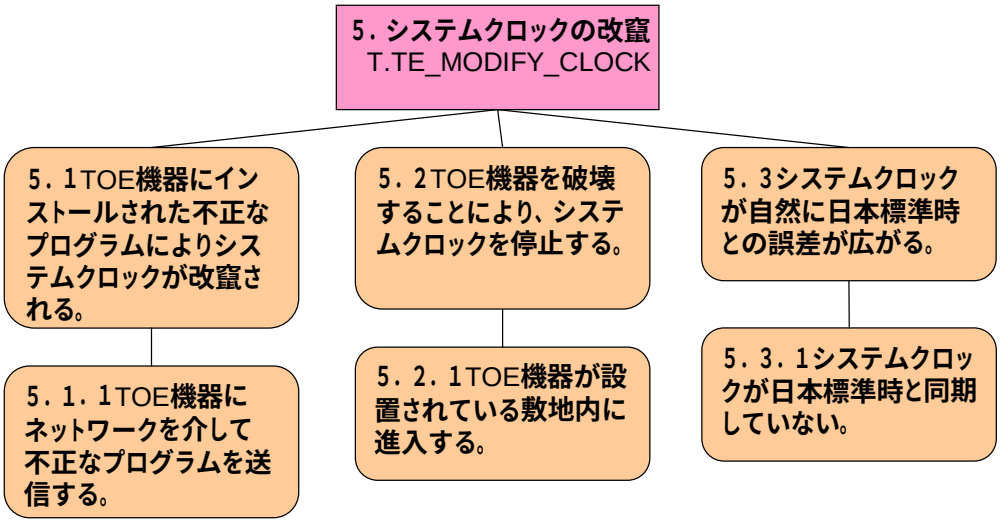


図 4-5：脅威ツリー（システムクロックの改竄）

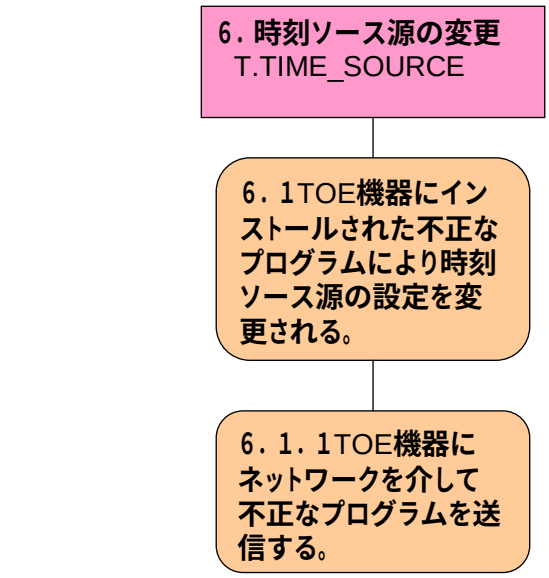


図 4-6：脅威ツリー（時刻ソース源の変更）

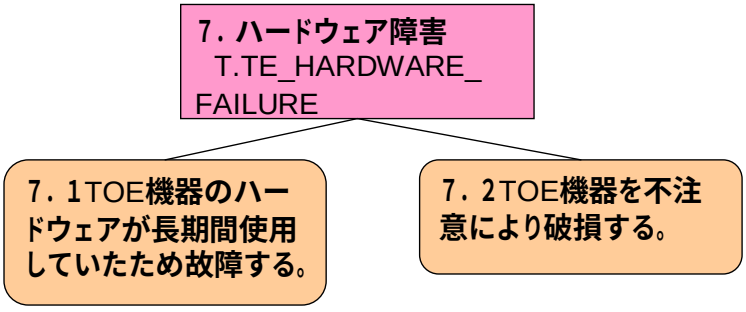


図 4-7：脅威ツリー（ハードウェア障害）

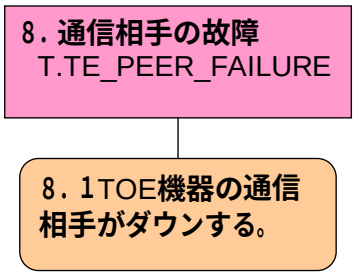


図 4-8：脅威ツリー（通信相手の故障）

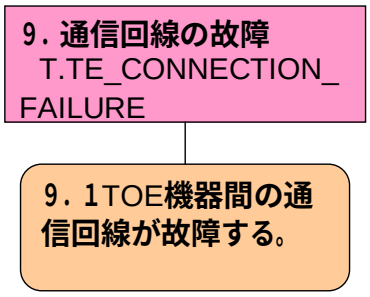


図 4-9：脅威ツリー（通信回線の故障）

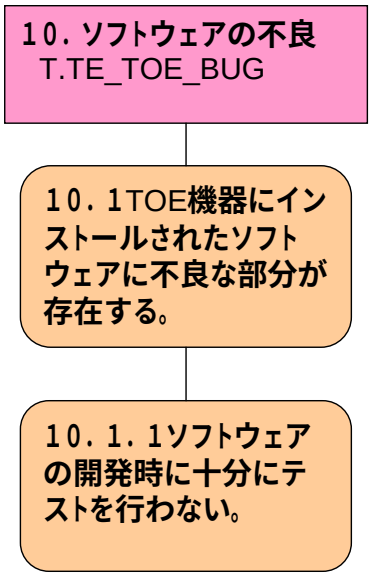


図 4-10：脅威ツリー（ソフトウェアの不良）

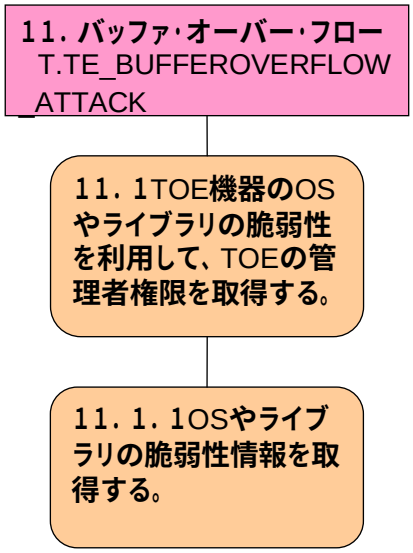


図 4-11：脅威ツリー（バッファ・オーバー・フロー）

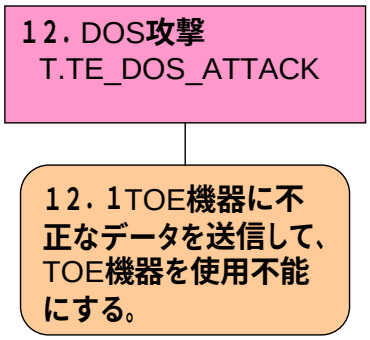


図 4-12：脅威ツリー（DOS 攻撃）

2. リスク格付けの考え方

抽出した今日にに対してリスク評価を行う。リスク評価のために私用した脅威格付け表を以下に記す。

表 4-1：脅威格付け表

	格付け	高 (3)	中 (2)	低 (1)
D	潜在的損失 (Damage potential)	TOE に係わる機密情報。改竄・漏洩により、TOE の機器が正常に動作しない可能性がある。	TOE に係わる機密情報が改竄・漏洩する。	機密性の低い情報が改竄・漏洩する。
R	再現性 (Reproducibility)	いつでも攻撃を再現することが可能である。	ある時間帯、かつ、特定の条件において、攻撃を再現することが可能である。	セキュリティホールの知識があったとしても、攻撃を再現することは非常に困難である。
E	攻撃利用可能性 (Exploitability)	初心者のプログラマーであったとしても短時間で攻撃可能である。	習熟したプログラマーであれば、攻撃可能である。攻撃が成功すれば繰り返すことが可能。	非常に習熟したプログラマーであれば攻撃可能。攻撃の度に高度な知識が必要。
A	影響ユーザ (Affected users)	全てのTOE関与者	多数のサブシステム利用者	非常に少数のサブシステム利用者
D	発見可能性 (Discoverability)	攻撃に関する公開情報がある。脆弱性は一般的であり、気付かれやすい。	製品のほとんど使用されない部分に脆弱性がある。少数のユーザがその脆弱性を見つける。	そのバグは、知られていない。ユーザは潜在的損失を分析できない。

3. リスク評価点

表の脅威格付け表に基づき、各脅威に対するリスク評価点を以下に記す。

表 4-2：リスク評価点

#	脅威	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.TE_SECRET_1	中(2)	低(1)	低(1)	高(3)	中(2)	9
2	T.TE_SECRET_2	中(2)	中(2)	低(1)	高(3)	中(2)	10
3	T.TE_SECRET_3	中(2)	高(3)	高(3)	高(3)	高(3)	13
4	T.TE_TAMP_1	中(2)	低(1)	低(1)	高(3)	中(2)	9
5	T.TE_TAMP_2	中(2)	低(1)	低(1)	高(3)	低(1)	8
6	T.TE_TAMP_3	中(2)	中(2)	高(3)	高(3)	高(3)	13
7	T.TE_MISS	高(3)	低(1)	高(3)	高(3)	高(3)	13
8	T.TE_WEAK_CRYPT_1	中(2)	低(1)	中(2)	高(3)	高(3)	11
9	T.TE_WEAK_CRYPT_2	高(3)	低(1)	中(2)	高(3)	高(3)	12

10	T.TE_MODIFY_CLOCK_1	高(3)	低(1)	低(1)	高(3)	中(2)	10
11	T.TE_MODIFY_CLOCK_2	高(3)	低(1)	低(1)	高(3)	低(1)	9
12	T.TE_MODIFY_CLOCK_3	高(3)	中(2)	中(2)	高(3)	高(3)	13
13	T.TE_TIME_SOURCE	高(3)	低(1)	低(1)	高(3)	中(2)	10
14	T.TE_HARDWARE_ FAILURE	高(3)	低(1)	中(2)	高(3)	低(1)	10
15	T.TE_PEER_FAILURE	高(3)	低(1)	中(2)	高(3)	低(1)	10
16	T.TE_CONNECTION_ FAILURE	高(3)	低(1)	中(2)	高(3)	低(1)	10
17	T.TE_TOE_BUG	高(3)	中(2)	中(2)	高(3)	低(1)	11
18	T.TE_BUFFEROVERFLOW _ATTACK	高(3)	高(3)	中(2)	高(3)	高(3)	14
19	T.TE_DOS_ATTACK	中(2)	高(3)	高(3)	高(3)	高(3)	14

第5章 内部不正を考慮したセキュリティ評価

上記では、TOE 関与者を信頼できるため内部不正による脅威は考慮する必要が無かった。しかし、本セクションでは、TOE 関与者を信頼できないと仮定した場合の脅威抽出及びセキュリティ目標・対策を記す。

ただし、内部不正を単独で行われるものとし、TOE 関与者の結託はないものとする。また、TOE 関与者と外部者との連携した不正はないものとする。

1. 前提

本 TOE の内部不正を考慮したセキュリティ環境の前提を以下に記す。

表 5-1：内部不正を考慮した前提

#	分類	項目	説明
1	物理的な前提	A.TE_LOCATION	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティに設定される。サブシステム管理者の許可のない物理アクセスを防ぐ。
2	物理的な前提	A.TE_ENVIRONMENT	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
3	物理的な前提	A.TE_MEDIA	TOE（及び関連するコンポーネント）で使用するストレージ・メディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
4	接続	A.TE_FIREWALL	ファイアウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
5	接続	A.TE_NTA2_CONNECTION	NTA2 と TOE の間の通信路は、NTA2 の成りすまし、データの改ざん、データの盗聴を防止する。
6	接続	A.TE_PEER	TOE と通信する意図された NTA2 は、信頼できる。
7	人的な前提	A.TE_ADMINISTRATOR	一つ以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報セキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 • TOE の起動・停止を実行する。 • TOE に関わるユーザ/役割を管理する。 • 暗号機能に関わる初期化及び管理業務を行う。 • TOE 上で悪意のあるソフトウェアが動作しないようにする。 • TOE の要件を満たす適切なディスクスペースを用意する。 ただし彼らは、権限を濫用し、故意にセキュリティを低めないとは限らない。
8	人的な前提	A.TE_OPERATOR	一人以上の許可された運用者が割り当てられる。 • TOE 管理者の指示の元で各種設定など運用業務を行う。 ただし彼らは、権限を濫用し、故意にセキュリティを低め

			ないとは限らない。
9	人的な前提	A.TE_AUDITOR	一人以上の許可された監査者が割り当てられる。 • 時刻認証子監査記録を取得し、分析を行う。 • TOE に関するログを取得し、分析を行う。 ただし彼らは、権限を濫用し、故意にセキュリティを低めないとは限らない。
10	人的な前提	A.TE_USER	一人以上の許可された TOE 利用者が割り当てられる。 • TOE から時刻認証子を受信する。 • 時刻認証子を生成･保存する。 • TOE へ時刻認証子を送信する。 ただし彼らは、権限を濫用し、故意にセキュリティを低めないとは限らない。

2. 内部不正による脅威

本 TOE の内部不正を考慮した場合に追加される脅威を以下に記す。

表 5-2：内部不正を考慮した脅威

#	項目	説明
1	T.TE_SECRET_4	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
2	T.TE_SECRET_5	TOE 関与者が、TOE が動作する機器のデータをメディア等にコピーすることにより、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
3	T.TE_TAMP_4	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、TOE が動作する機器の保護対象資産を改竄/削除するかもしれない。
4	T.TE_TAMP_5	TOE 関与者が、TOE が動作する機器のデータファイル等をコマンド等から操作することにより、保護対象資産を改竄/削除するかもしれない。
5	T.TE_WEAK_CRYPT_3	TOE 関与者が、意図的に強度の弱い暗号アルゴリズムを使用するかもしれない。
6	T.TE_MODIFY_CLOCK_4	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、システムクロックを改竄されてしまうかもしれない。
7	T.TE_MODIFY_CLOCK_5	TOE 関与者が、TOE が動作する機器のコマンドにより、システムクロックを改竄されてしまうかもしれない。
8	T.TE_TIME_SOURCE_2	TOE 関与者が、TOE が動作する機器に不正なプログラムをインストールすることによって、TOE の参照する時刻ソース源を変更してしまうかもしれない。

9	T.TE_TIME_SOURCE_3	TOE 関与者が、TOE が動作する機器の設定を変更し、時刻ソース源を変更してしまうかもしれない。
10	T.TE_HARDWARE_2 FAILURE	TOE 関与者が、意図的に TOE 機器を破壊してしまうかもしれない。
11	T.TE_CONNECTION_ FAILURE_2	TOE 関与者が、意図的に通信回線を破壊することにより、TOE の資産が失われる。
12	T.TE_TOE_BUG_2	TOE 関与者が、意図的に TOE の IT 実装を不良が埋め込まれたソフトウェアにすり替えたため、TOE の資産の信頼性が乏しくなる。

3. 組織のセキュリティポリシー

本 TOE の内部不正を考慮した組織のセキュリティポリシーを以下に記す。

表 5-3：内部不正を考慮した組織のセキュリティポリシー

#	項目	説明
1	P.TE_DUAL _CONTROL（合議）	TOE の管理業務における重要な操作は、サブシステム管理者による合議の上で行うこととする。 また TOE の運用業務における重要な操作は、複数のサブシステム運用者による合議の上で行うこととする。
2	P.TE_CRYPTOGRAPH Y（暗号アルゴリズムの管理）	TOE が動作する機器で時刻認証子の結合に使用される暗号アルゴリズムは、「電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省）」に記載されたアルゴリズムによって実装されなければならない。
3	P.TE_CHECK_VIRUS（ウイルス対策）	定期的なウイルスチェックを実行する。
4	P.TE_SYSTEM_CLOCK _MANAGEMENT（システムクロックの管理）	TOE が動作する機器のシステム時計を信頼のできる時刻ソースと同期させる。
5	P.TE_TIMESOURCE（時刻ソース）	TOE は、信頼できる時刻ソースを参照する。この時刻ソースは、TOE 管理者にとってアベイラブルである。また、時刻ソースの信頼性と正確性は TOE 管理者にとって受容可能である。
6	P.TE_KEY_STORAGE（鍵の管理）	すべての私有鍵は、安全に保管される。TOE 管理者以外の人間からのアクセスを防ぐ。
7	P.TE_PASSWORD_ MANAGEMENT（パスワードの管理）	TOE 関与者のパスワードは、TOE 関与者本人によって適切に管理され、本人以外に知られてはならない。
8	P.TE_PROTECT_LOG（ログの保護）	TOE を利用する組織は、ログの暴露、改ざん、または削除の防止のために必要な措置をとることとする。
9	P.TE_CHECK_ABSTRU CT _VULNERABILITY（脆弱性確認）	定期的に、OS、ライブラリおよび暗号アルゴリズムの脆弱性を確認し、対策を行う。

4. 内部不正による脅威のツリー

以下に内部不正を考慮した攻撃シナリオに使用した脅威ツリーを記載する。着色されたものが、内部不正を考慮した部分である。

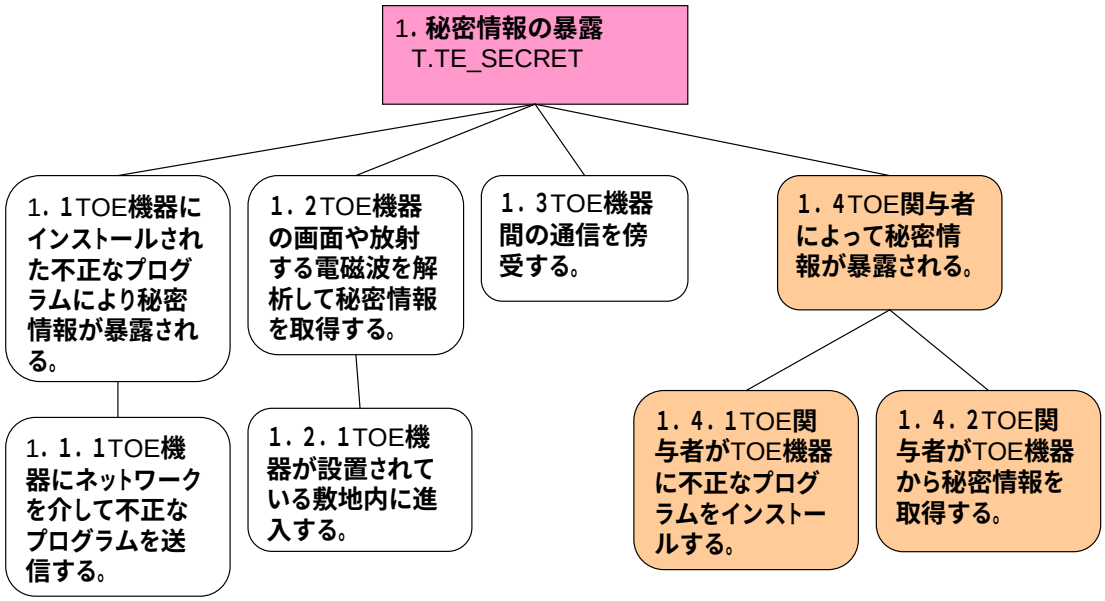


図 5-1：内部不正を考慮した脅威ツリー（秘密情報の暴露）

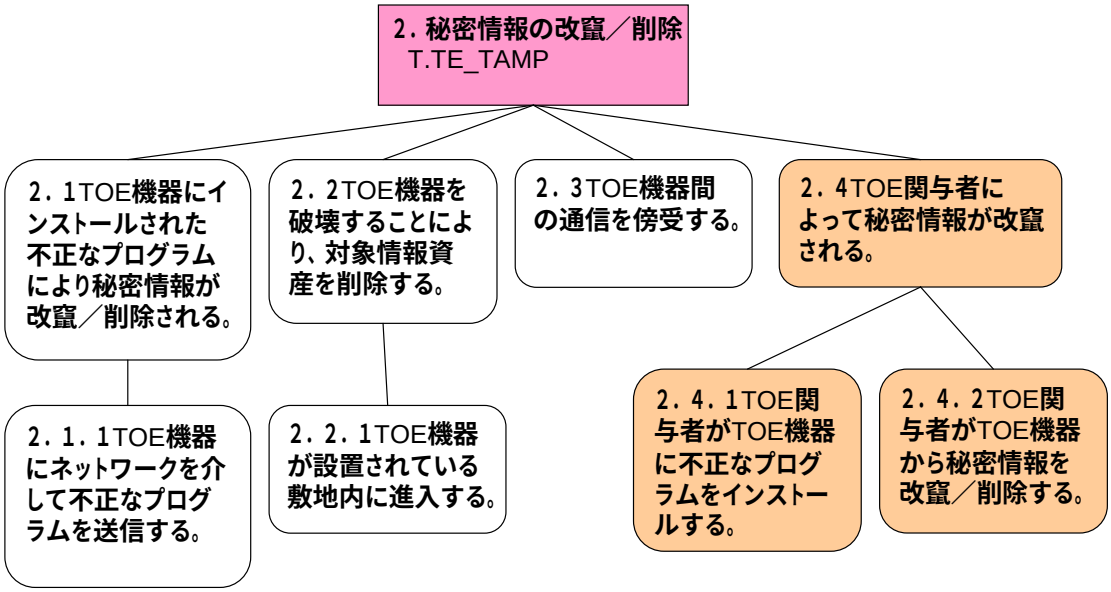


図 5-2：内部不正を考慮した脅威ツリー（秘密情報の改竄／削除）

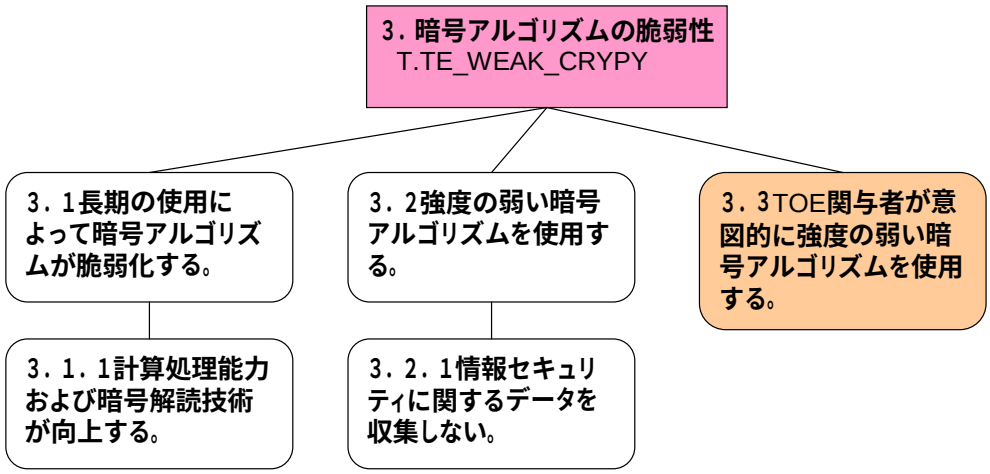


図 5-3：内部不正を考慮した脅威ツリー（暗号アルゴリズムの脆弱性）

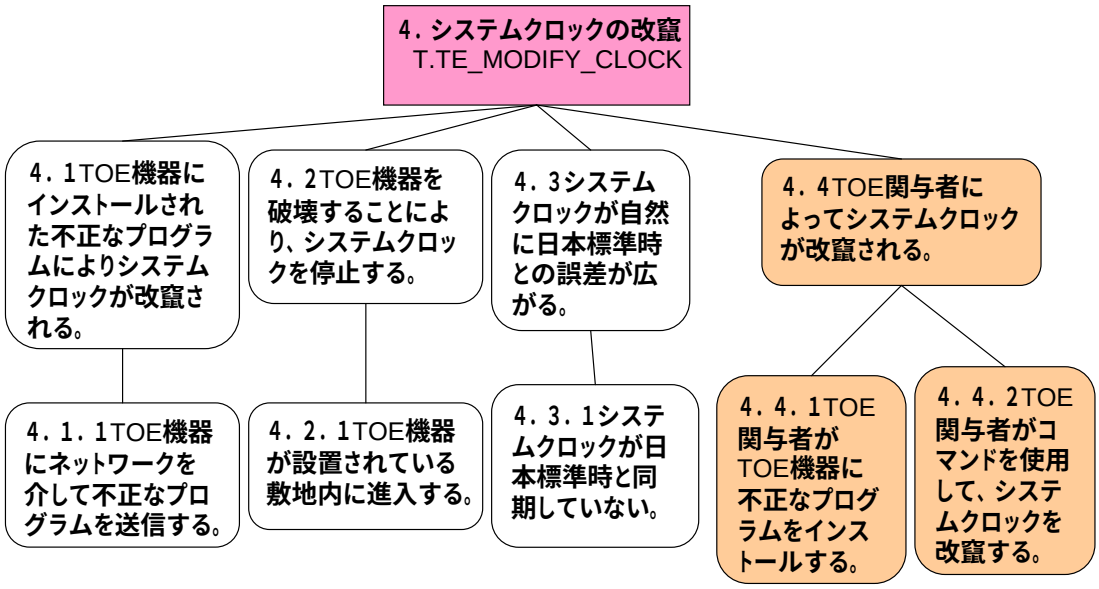


図 5-4：内部不正を考慮した脅威ツリー（システムクロックの改竄）

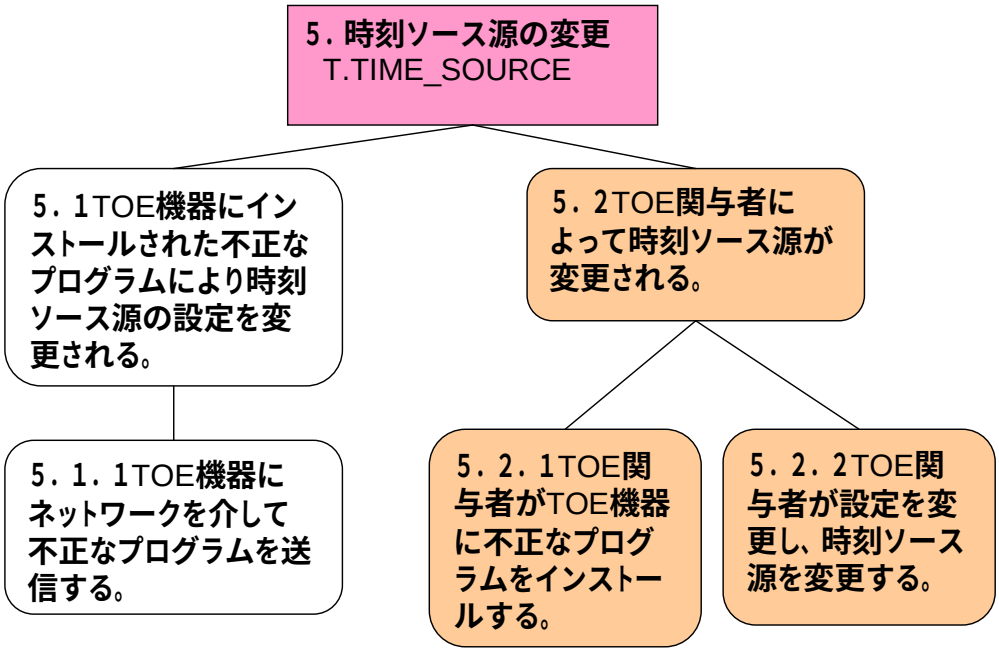


図 5-5：内部不正を考慮した脅威ツリー（時刻ソース源の変更）

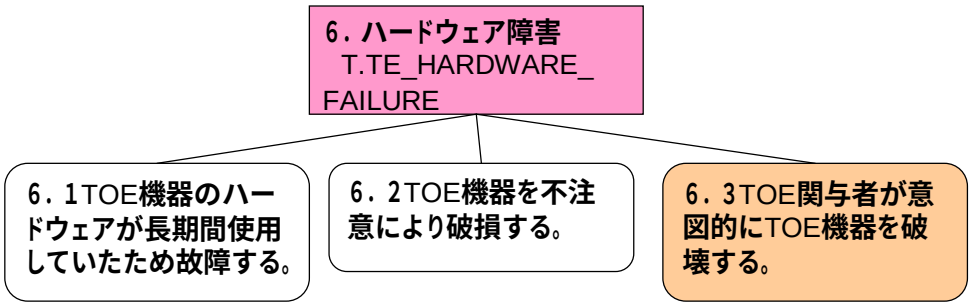


図 5-6：内部不正を考慮した脅威ツリー（ハードウェア障害）

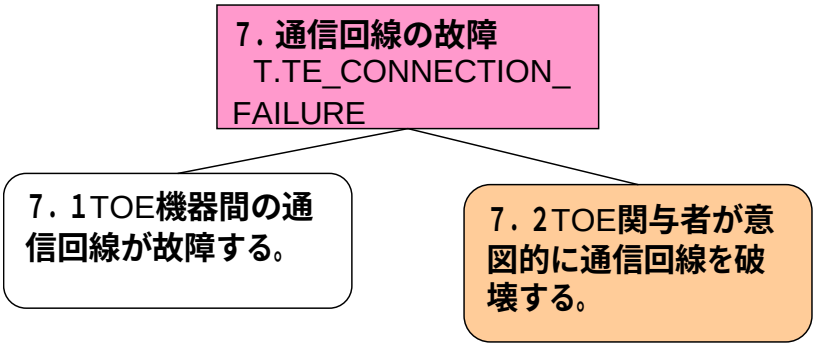


図 5-7：内部不正を考慮した脅威ツリー（通信回線の故障）

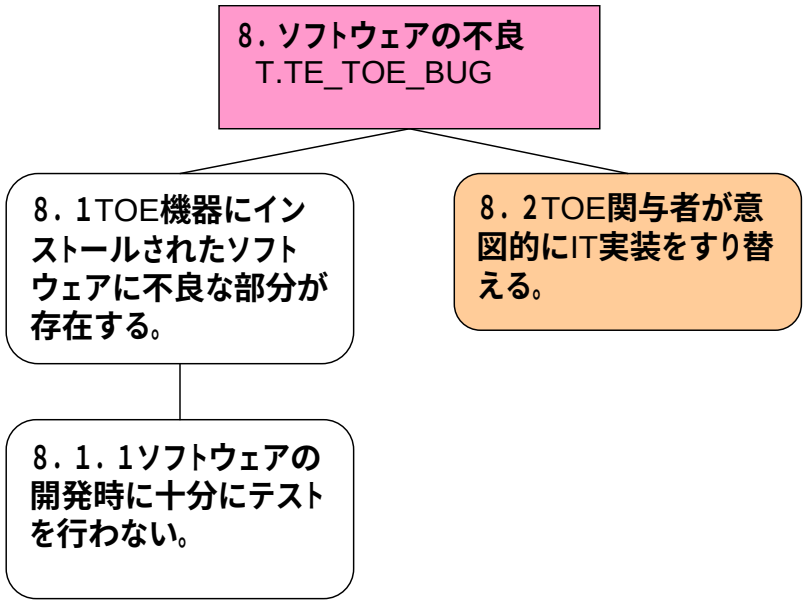


図 5-8：内部不正を考慮した脅威ツリー（ソフトウェアの不良）

5. 内部不正による脅威のセキュリティ目標・対策

本 TOE の内部不正を考慮したセキュリティ目標と対策を以下に記す。

表 5-4：内部不正を考慮したセキュリティ目標・対策

#	脅威名	セキュリティ目標・対策	
1	T.TE_SECRET_4	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存を信頼できる第三者が行うものとする。
		回復	なし
2	T. TE_SECRET_5	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存を信頼できる第三者が行うものとする。
		回復	なし
3	T. TE_TAMP_4	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。

		検出	ログの記録をし、ログの保存を信頼できる第三者が行うものとする。
		回復	データのバックアップをし、バックアップデータの保存を信頼できる第三者が行うものとする。保存されてバックアップデータでリストアを実施する。
4	T. TE_TAMP_5	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	データのバックアップをし、バックアップデータの保存を信頼できる第三者が行うものとする。保存されてバックアップデータでリストアを実施する。
5	T. TE_WEAK_CRYPT_3	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	データのバックアップをし、バックアップデータの保存を信頼できる第三者が行うものとする。保存されてバックアップデータでリストアを実施する。
6	T. TE_MODIFY_CLOCK_4	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
7	T. TE_MODIFY_CLOCK_5	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
8	T. TE_TIME_SOURCE_2	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
9	T. TE_TIME_SOURCE_3	防止	TOE 機器の操作には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	信頼できる時刻配信局と時刻同期させることにより実現可能である。
10	T. TE_HARDWARE_FAILURE_2	防止	TOE 機器の設置場所の入場には、複数の TOE 関与者の合議の上でのみ可能とする。
		検出	TOE 機器の設置場所の入場の記録をし、記録されたログの保存は信頼できる第三者が行うものとする。
		回復	機器を入れ替える。
11	T. TE_CONNECTION_FAILURE_2	防止	TOE 機器の設置場所の入場には、複数の TOE 関与者の合議の上でのみ可能とする。

		検出	TOE 機器の設置場所の入場の記録をし、記録されたログの保存は信頼できる第三者が行うものとする。
		回復	通信復帰後、再接続する。
12	T. TE_TOE_BUG_2	防止	TOE 機器内のソフトウェアが改竄されていないか否かを定期的に確認する。
		検出	ログの記録をし、ログの保存は信頼できる第三者が行うものとする。
		回復	パッチ作成・配布・適用を適切に実施する。 （システムを停止させた場合）安全確認後、システムを再起動する。

以上

セキュリティ評価報告書

（TOE： CA ）

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

1. TOE の機能概要

1-1 証明書発行・失効機能（CaServer）

NTA/TA/TSA/VA からの証明書発行要求(PKCS#10)に対して公開鍵証明書を発行する。また、NTA/TA/TSA/VA からの証明書失効要求に対して該当証明書を失効する。

1-2 失効リスト発行機能（CaServer）

最新の失効リストを、証明書失効の都度 又は定期的に発行する。

1-3 公開鍵証明書・失効リスト公開機能（DirectoryServer）

タイムスタンプ検証に必要な公開鍵証明書、及び最新の失効リストをディレクトリサーバにて公開する。

2. TOE 構成図

TOE の構成図を以下の図 1-1に示す。

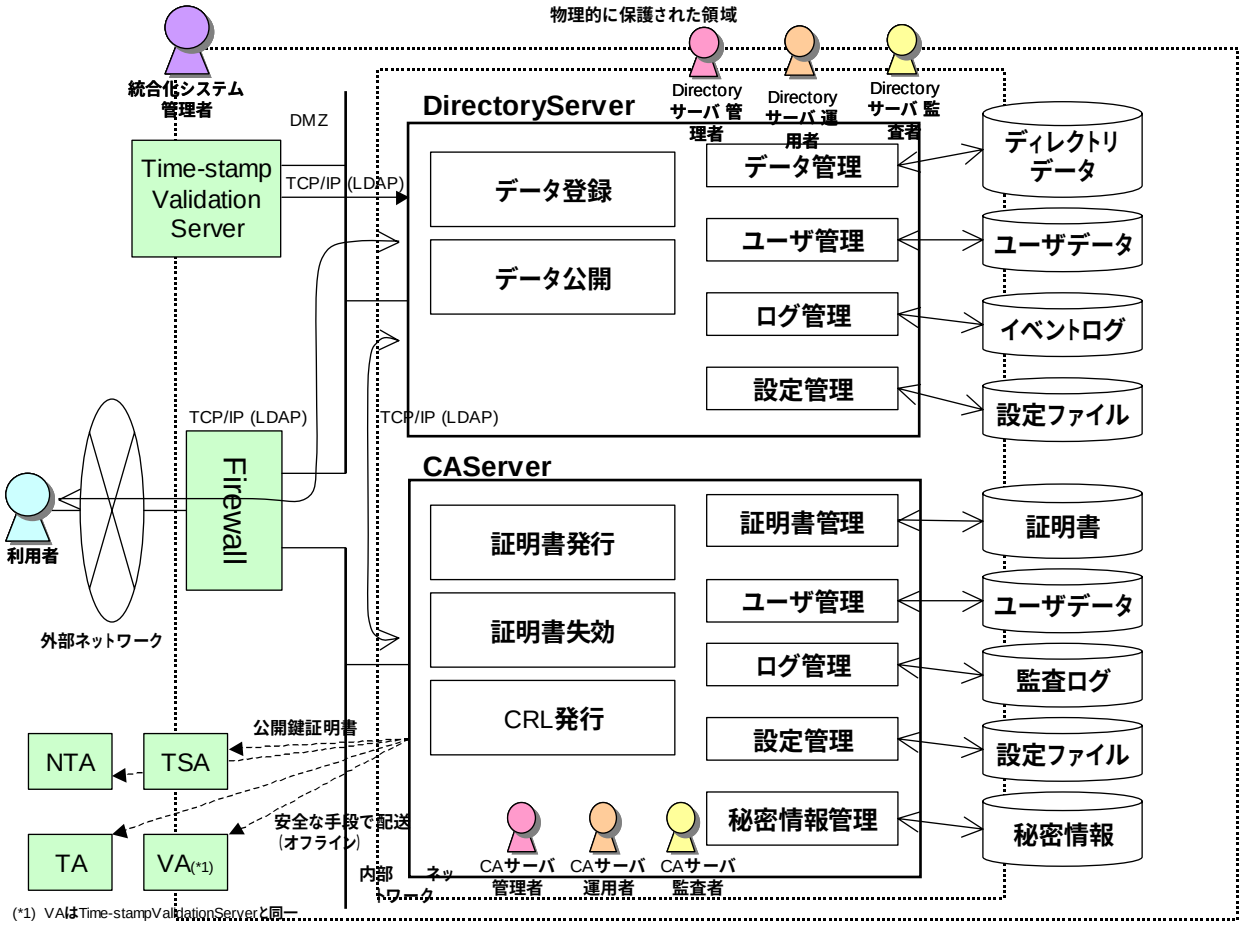


図 1-1 TOE の構成図

3. 利用する暗号技術

#	システム	使用目的	使用している暗号技術
1	CA Server	CA 公開鍵証明書の作成 (自己署名証明書)	【証明書内の鍵】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　RSASSA-PKCS1-v1_5 鍵長　：　2048bit 【署名方式】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　RSASSA-PKCS1-v1_5 鍵長　：　2048bit ﾊｯｼｭ関数　：　SHA-1
2		その他公開鍵証明書の作成	【証明書内の鍵】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　RSASSA-PKCS1-v1_5 鍵長　：　1024bit 【署名方式】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　RSASSA-PKCS1-v1_5 鍵長　：　2048bit ﾊｯｼｭ関数　：　SHA-1
3		失効リストの作成	【署名方式】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　RSASSA-PKCS1-v1_5 鍵長　：　2048bit ﾊｯｼｭ関数　：　SHA-1
4		監査ログへの署名	【署名方式】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　RSASSA-PKCS1-v1_5 鍵長　：　1024bit ﾊｯｼｭ関数　：　SHA-1
5		秘密情報格納ディレクトリの暗号	【暗号方式】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　ＤＥＳ 鍵長　：　56bit
6		ＤＢの暗号	【暗号方式】 暗号ｱﾙｺﾞﾘｽﾞﾑ　：　ＭＵＬＴＩ2 鍵長　：　256bit

DirectoryServer では、暗号アルゴリズムは利用していない。

4. 暗号コンポーネント構成図

4-1 CA 公開鍵証明書の作成

CA 公開鍵証明書の作成に係る、概要図を図 1-2に示す。

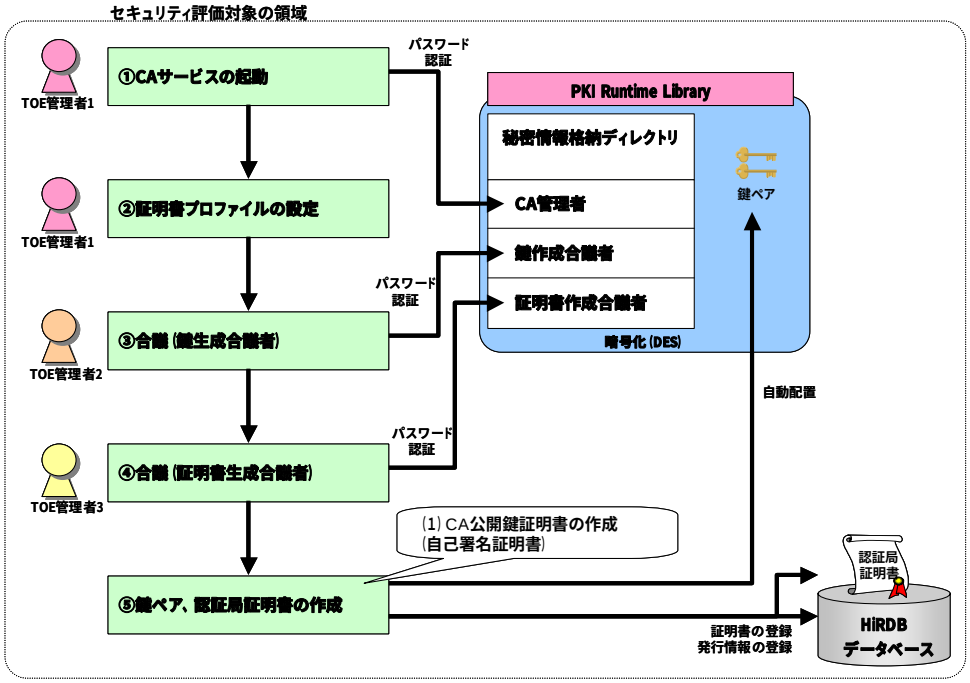


図 1-2 CA 公開鍵証明書の作成の概念図

4-2 その他公開鍵証明書の作成

その他公開鍵証明書の作成に係る、概要図を図 1-3に示す。

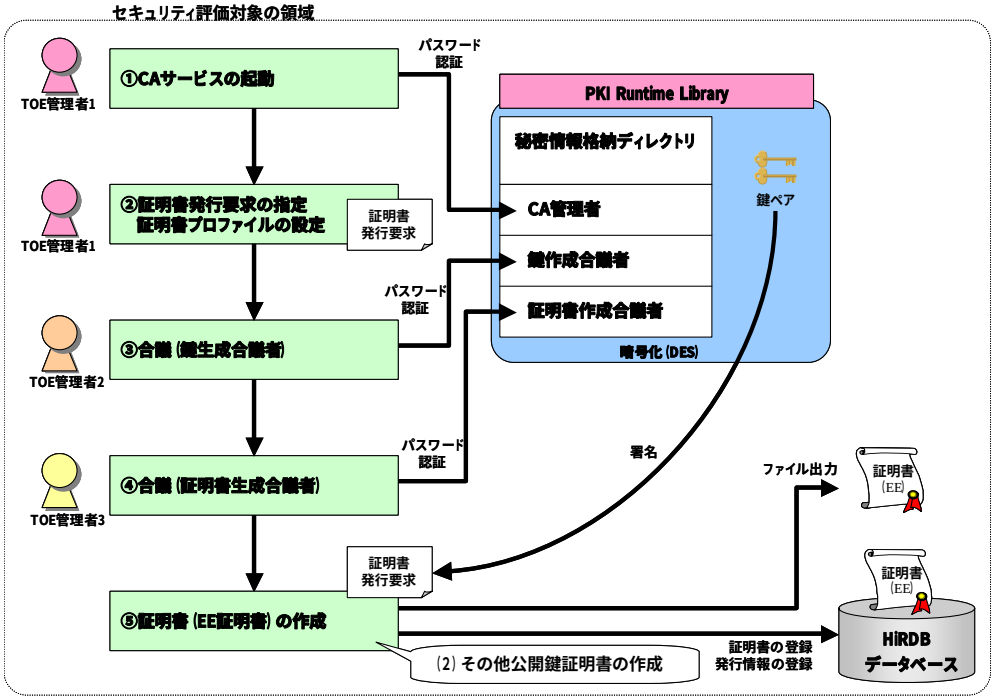


図 1-3 その他公開鍵証明書の作成の概要図

4-3 失効リストの作成

失効リストの作成に係る、概要図を図 1-4に示す。

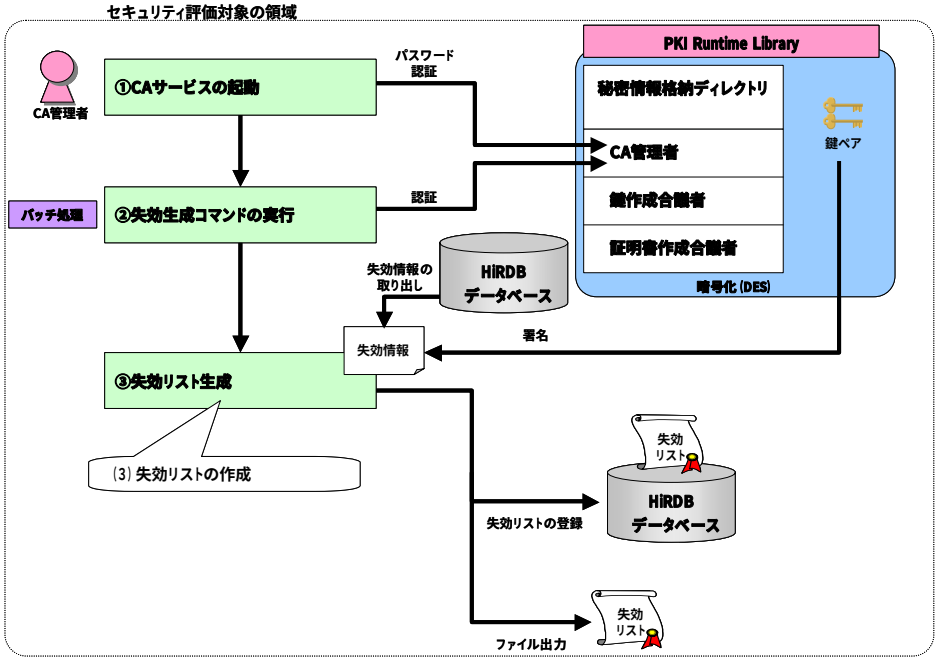


図 1-4 失効リスト作成の概要図

4-4 監査ログへの署名

監査ログへの署名に係る、概要図を図 1-5に示す。

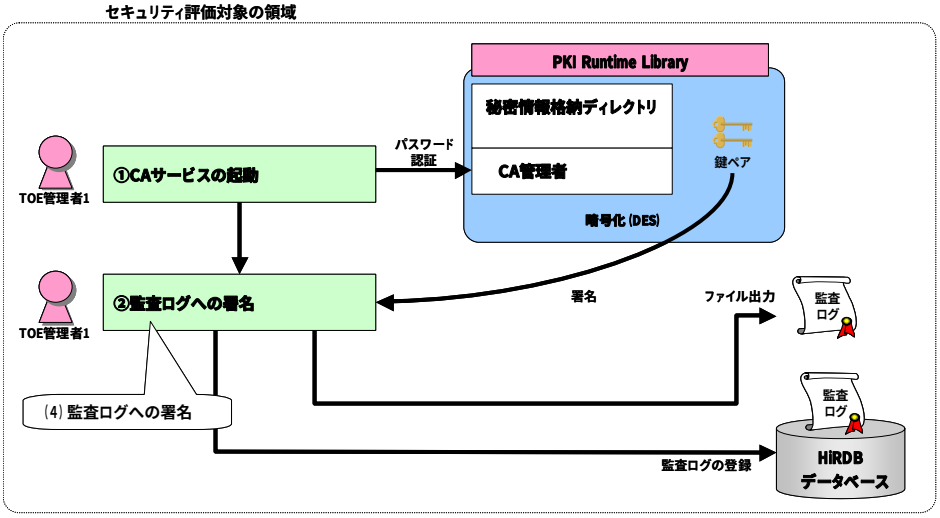


図 1-5 監査ログへの署名の概要図

4-5 秘密情報格納ディレクトリの暗号

秘密情報格納ディレクトリの暗号に係る、概要図を図 1-6に示す。

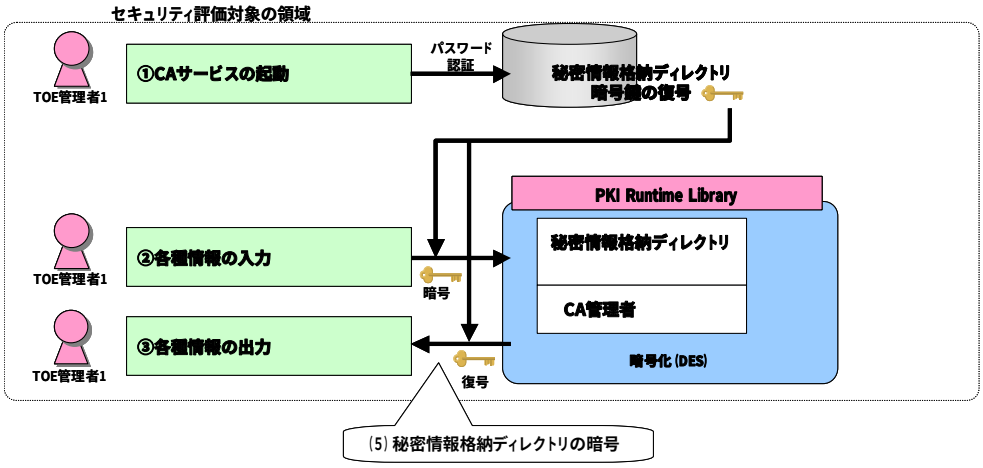


図 1-6 秘密情報格納ディレクトリの暗号の概要図

4-6 DB の暗号

DB の暗号に係る、概要図を図 1-7に示す。

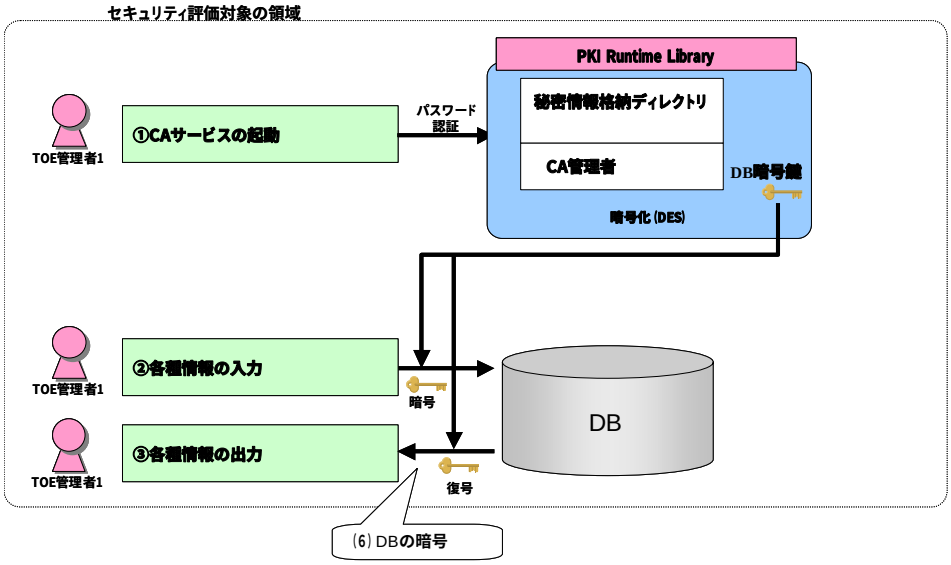


図 1-7 DB の暗号の概要図

5. 関与者

TOE に係る関与者一覧を、以下の表 1-1に示す。

表 1-1　TOE に係る関与者

#	関与者	説明
1	ＴＯＥ管理者	TOE に関する全ての権限をもつユーザ。 証明書発行などの重要な業務では、合議者としての運用を行う。

2	ＴＯＥ運用者	管理者の指示のもと運用業務を行うユーザ。 合議制操作により証明書の失効処理などの運用業務を担当する。
3	ＴＯＥ監査者	TOE の内部監査を行うユーザ。 ユーザアカウントは持たず、直接運用業務は担当しない。
4	利用者	TOE のサービスを利用するユーザ。 証明書や失効リストを利用して各々サービスを提供する。具体的には、NTA／TA／TSA／VA(又は検証者)である。

6. 資産

TOE に係る資産一覧を、以下の表 1-2に示す。

表 1-2 TOE に係る資産一覧

#	分類		資産名	内容
1	情報資産	利用者データ(CA)	公開鍵証明書	CaServer で発行した公開鍵証明書
2			失効リスト	CaServer で発行した失効リスト情報
3		利用者データ(DIR)	公開鍵証明書	DirectoryServer で公開する公開鍵証明書
4			失効リスト	DirectoryServer で公開する失効リスト
5		TSF データ(CA)	システム時計	CaServer のシステム時計
6			設定データ	CaServer の設定データ
7			私有鍵データ	CaServer で管理する CA 鍵、監査鍵
8			監査ログ	CaServer の監査ログ
9			一般ログ	CaServer の OS などの一般的なログ
10			ユーザ識別情報とユーザ認証データ	CaServer で登録されるアカウント情報と認証データ。
11		TSF データ(DIR)	システム時計	DirectoryServer のシステム時計
12			設定データ	DirectoryServer の設定データ
13			ログデータ	DirectoryServer のログ（OS ログ含む）
14			ユーザ識別情報とユーザ認証データ	DirectoryServer で登録されるアカウント情報と認証データ。
15	IT 実装	IT 実装(CA)	認証局サービス	CaServer のサービス。
16			認証局管理ツール・証明書発行ツール	各種設定や証明書発行など CaServer の管理を行うツール。
17			運用ツール	証明書の検索、失効処理などの CaServer の運用を行うツール。
18			失効リスト自動作成・DIR 登録ツール	定期的に最新の失効リストを作成し、DirectoryServer に登録するツール。
19		IT 実装(DIR)	ディレクトリサービス	DirectoryServer のサービス。
20			管理ツール	各種設定など DirectoryServer の管理を行うツール。

第2章 セキュリティ環境

1. 前提

TOE に係るセキュリティ環境の前提一覧を、以下の表 2-1に示す

表 2-1　TOE に係るセキュリティ環境の前提一覧

#	分類	項目	説明
1	物理的な前提	A.CaDir_Location	TOE の処理リソースは、コントロールされたアクセス・ファシリティの中に配置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2		A.CaDir_Environment	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
3		A.CaDir_Media	ストレージメディアの経年変化や不良の対策が行われ、データ損失と破壊はないものとする。
4	人的な前提	A.CaDir_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 ・ TOE に関わるユーザ/役割を管理する。 ・ 暗号機能に関わる初期化及び管理業務を行う ・ TOE 上で悪意のあるソフトウェアが動作しないようにする。 ・ TOE の要件を満たす適切なディスクスペースを用意する ・ TOE のデータベースを適切に管理する。 ・ TOE の起動・停止を実行する。 さらに彼らは、信用できる。そのため、彼らは、権限を乱用し、故意にセキュリティを低めることはしない。
5		A.CaDir_Operator	一人以上の許可された運用者が割り当てられる。 ・ TOE 管理者の指示の元で運用業務を行う さらに彼らは、信用できる。そのため、彼らは、権限を乱用し、故意にセキュリティを低めることはしない。

6		A.CaDir_Auditor	一人以上の許可された監査者が割り当てられる。 ・　TOE に関するログ等を入手し、分析を行う さらに彼らは、信用できる。そのため、彼らは、権限を乱用し、故意にセキュリティを低めることはしない。
7		A.Dir_Service_Requestor	公開鍵証明書・失効リスト要求者は、公開鍵証明書及び失効リストを検証及び保持する。
8	接続の前提	A.CaDir_Device	周辺機器への全接続は、コントロールされたアクセス・ファシリティに存在する。
9		A.CaDir_Firewall	ファイアウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
10		A.PEER	TOE と通信する意図された他システムは、信頼できる。
11		A.CaDir_Abstract	TOE が動作するために必要な OS や依存するライブラリは、不正な改変から保護され、正しく動作する。
12		A.CaDir_Separation	TOE が動作するマシンには、TOE の動作に必要なソフトウェア以外はインストールされないものとする。

2. 脅威

TOE に係るセキュリティ環境の脅威一覧を、以下の表 2-2に示す。なお、表 2-2の「項目」欄は脅威をカテゴリ化した大分類を示している。

表 2-2　TOE に係るセキュリティ環境の脅威一覧

#	項目（脅威の大分類）	説明
1	T.Spoof	TOE の IT 実装に対して、許可無くなりすます。
2	T.Tamper	TOE の情報資産もしくは IT 実装に対して、許可されていない改変の加える。 （機器内の情報及び通信路上の情報を含む）
3	T.Repudiation	TOE の情報資産に対して、作成した事実などを否認する。
4	T.Information_disclosure	TOE の情報資産もしくは IT 実装に対して、許可無く情報を暴露する。 （機器内の情報及び通信路上の情報を含む）
5	T.Denial_of_service	TOE の IT 実装に対して、許可無く大量の負荷をかけ、使用不能や性能劣化に陥らせる。
6	T.Forgery	TOE の情報資産もしくは IT 実装に対して、許可無く偽造する。
7	T. Valnerability_of_Crypto	現在使用している暗号アルゴリズム又は鍵長が将来危殆化し、TOE の脅威となる。 または、危殆化された暗号アルゴリズムを使用する。
8	T.Spontaneous_Change	情報資産が、時の流れとともに自然に変化することにより、TOE の脅威となる。
9	T.Valnerability_of_Software	IT 実装に脆弱性が発見され、TOE の脅威となる。

10	TE.Hardware_Failure	経年変化や偶然に引き起こされる障害により、TOE のハードウェアが故障し、資産が失われる。

3. 組織のセキュリティポリシー

TOE に係るセキュリティ環境の組織のセキュリティポリシー一覧を、以下の表 2-3に示す。

表 2-3 TOE に係るセキュリティ環境の組織のセキュリティポリシー一覧

#	項目	説明
1	P.CaDir_Time_Source	TOE は、信頼のできる時刻ソースを参照すること。この時刻ソースは、TOE 所有者にとってアベイラブルであること。また、時刻ソースの信頼性と正確性は TOE 所有者にとって受容可能であること。
2	P.CaDir_Clock_Management	TOE が参照するシステム時計を信頼のできる時刻ソースと同期させる。
3	P.CaDir_Cryptography	暗号処理(署名と検証)は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されなければならない。 「電子政府推奨暗号リスト」に記載されていないアルゴリズムを使用する場合は、別の対策により安全性を保証する必要がある。
4	P.CaDir_Password_Management	TOE 利用者のパスワードは、TOE 利用者本人によって適切に管理され、本人以外に知られてはならない。
5	P.Ca_DUALCTL	TOE の管理業務における重要な操作は、複数の CA 管理者による合議の上で行うものとする。 また、TOE の運用業務における重要な操作は、複数の CA 運用者による合議の上で行うものとする。
6	P.CaDir_PROTECT_LOG	TOE は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。
7	P.CaDir_Check_Virus	定期的なウィルスチェックを実行する。 また、媒体などを持ち込む場合は、ウィルスチェックを実行する。
8	P.CaDir_Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

第3章 セキュリティ目標・対策と実装システムの評価

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

別紙「脅威に対する対策及びリスク評価」参照。

2. 前提の実現方法例

TOE に係るセキュリティ環境の前提の実現方法例一覧を、以下の表 3-1に示す

表 3-1 TOE に係るセキュリティ環境の前提の実現方法例一覧

#	分類	項目	実現方法例
1	物理的な前提	A.CaDir_Location	TOE が設置された施設へは、あらかじめ許可された人員のみICカードによる認証により入室が可能となるようにする。
2		A.CaDir_Environment	電磁波が盗聴されないようケーブル類が施錠管理されたラック内に配線されるとともに、瞬断や停電に備えて二重化された電源装置へ接続され、長時間停電した場合は、自家発電装置による電源供給を行い、空調設備により、機器類の動作に適した環境に維持される。
3		A.CaDir_Media	ストレージを冗長化し、一部に経年劣化や不良が生じた場合には速やかに部品の交換を実施する。
4	人的な前提	A.CaDir_Administrator	認証業務及びセキュリティに関する専門知識を有する者、または専門知識を修得するための教育研修を受講した者が、管理者として任命される。 また、運用マニュアルに基づき操作を行うものとし、不正を働いた場合は罰則を受ける。
5		A.CaDir_Operator	認証業務及びセキュリティに関する専門知識を有する者、または専門知識を修得するための教育研修を受講した者が、運用者として任命される。 また、運用マニュアルに基づき操作を行うものとし、不正を働いた場合は罰則を受ける。
6		A.CaDir_Auditor	認証業務及びセキュリティに関する専門知識を有する者、または専門知識を修得するための教育研修を受講した者が、監査者として任命される。 また、運用マニュアルに基づき操作を行うものとし、不正を働いた場合は罰則を受ける。
7		A.Dir_Service_Requestor	認証局の CP/CPS「依存者の義務」にて、証明書の有効性確認を実施する旨を記載されており、従う必要がある。
8	接続の前提	A.CaDir_Device	周辺機器への全接続は施錠管理されたラック内に収められる。
9		A.CaDir_Firewall	TOE とインターネットとの接続箇所においては、ファイアウォール機器を持つネットワーク機器が設置され、不要な通信を遮断する。

10		A.PEER	TOE と通信する他システムは TOE と同様にセキュリティ評価が実施され、信頼できる。
11		A.CaDir_Abstract	OS や依存するライブラリに変更を加える作業は、管理者による承認のもとでのみ実施される。
12		A.CaDir_Separation	運用規程により、不要なソフトウェアのインストールを認めないものとする。

3. 組織のセキュリティポリシーの実現方法例

セキュリティ環境の組織のセキュリティポリシー実現方法例を、以下の表 3-2に示す。

表 3-2 セキュリティ環境の組織のセキュリティポリシー実現方法例一覧

#	項目	実現方法例
1	P.CaDir_Time_Source	日本標準時と同期した信頼の出来る第三者(TTP)が運用する NTP サーバを時刻ソースとする。
2	P.CaDir_Clock_Management	定期的に NTP サーバとの通信を行い、システム時計を日本標準時と同期させる。
3	P.CaDir_Cryptography	暗号処理(署名と検証)は、「電子政府推奨暗号リスト(平成15年2月 20 日、総務省、経済産業省)」に記載されたアルゴリズムを使用する旨、システム設計されている。 「電子政府推奨暗号リスト」に記載されていないアルゴリズムを使用する場合は、厳密な入退室管理、合議制操作によって、安全性が確保されている。
4	P.CaDir_Password_Management	認証業務及びセキュリティに関する専門知識を有する者、または専門知識を修得するための教育研修を受講した者が、管理者及び運用者として任命される。
5	P.Ca_DUALCTL	重要な操作については複数人運用を行う旨、運用規程に記載されており、規程通りに運用されている。
6	P.CaDir_PROTECT_LOG	監査ログの管理は複数人運用によって実施されるとともに、定期的にバックアップを保管する旨、運用規程に記載されており、規程通りに運用されている。
7	P.CaDir_Check_Virus	アンチウィルスソフトをインストールし、定期的なパターンファイル更新とウィルスチェックを実施する旨、運用規程に記載されており、規程通りに運用されている。
8	P.CaDir_Check_Abstract_Vulnerability	定期的に、公開されている脆弱性情報を確認する旨、運用規程に記載されており、規程通りに運用されている。

第4章 脅威ツリー及びリスク評価一覧

1. リスク格付けの考え方

リスク格付の考え方に関して、表 4-1に示す。

表 4-1 リスク格付の考え方

	格付け	視点	高 (3)	中 (2)	低 (1)
D	潜在的損失	サービス継続性	異常なサービス提供	正常なサービス継続不可能	正常なサービス継続可能
		資産の流出		機密情報が漏洩する	重要情報が漏洩する
		資産の信頼性		機密情報の改ざん、偽造、消去	重要情報の改ざん、偽造、消去
R	再現性	攻撃時間帯	任意の時間に脅威が発生	ある時間帯のみ脅威が発生	ある限られた条件において脅威が発生
		脅威エージェント	悪意を持った内部者	外部者、あるいは利用者 自然 (ある程度予知可能な要因による脅威発生)	不注意な内部者 自然や偶然 (予知不可能な要因による脅威発生
E	攻撃利用可能性	脅威エージェント	悪意を持った内部者	外部者、あるいは利用者	不注意な内部者、あるいは、自然や偶然 (予知不可能な要因による脅威発生)
		脅威エージェントが使用する攻撃ツールの入手･使用の容易性	TOE、あるいは、TOEの下位抽象マシンなどに標準的に備わる機能を直接利用	TOE、あるいは、TOEの下位抽象マシンに比較的入手可能な攻撃用のツールを導入要	TOE、あるいは、TOEの下位抽象マシンに攻撃者が新規に作成した独自の攻撃用ツールが必要
A	影響ユーザ	影響を受ける利用者の範囲	全ての利用者に影響が出る	一部の利用者に影響が出る	ごく少数の利用者に影響が出る管理者/運用者/監査者の業務に影響が出る
D	発見可能性	攻撃方法の公知性	脅威エージェントが外部者、あるいは、利用者である場	脅威エージェントが外部者、あるいは、利用者である場	脅威エージェントが外部者、あるいは、利用者である

			合、攻撃方法は公知である 脅威エージェントが内部者（悪意）の場合、正規の運用方法で攻撃可能である。	合、攻撃方法は、少数のユーザに知られている 脅威エージェントが内部者（悪意）である場合、攻撃を行う際、正規の運用方法以外の手法も用いる必要がある	場合、攻撃方法は、ほとんど未知である 脅威エージェントが内部者（不注意）である場合、正規の運用方法で脅威が発生する

1-1 リスク評価

別紙「脅威に対する対策及びリスク評価」参照。

DREAD 分類において、複数の視点が存在し、それぞれの評価の点が異なる場合は、一番リスクの高い評価点にあわせることとする。

第5章 内部不正を考慮したセキュリティ評価

1. 内部不正の考え方

管理者、運用者及び監査者からなる内部関係者に関して、不正を行う可能性があることを想定して評価を実施する。但し、複数人運用時において、内部関係者の結託による不正は行われないことと想定する。

2. 内部不正を考慮したセキュリティ環境

2-1 前提

内部不正を考慮したセキュリティ環境の前提について、「表 2-1　TOE に係るセキュリティ環境の前提一覧」及び「表 3-1 TOE に係るセキュリティ環境の前提の実現方法例一覧」に対して差異がある前提一覧について、以下の表 5-1に示す。

表 5-1 内部不正を考慮した場合のセキュリティ環境の前提の差異一覧

#	分類	項目	前提
4	人的な前提	A.CaDir_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 さらに彼らは、信用できる。そのため、彼らは、権限を乱用し、故意にセキュリティを低める可能性は低いとともに、複数人運用時において他の管理者･運用者･監査者と結託はしない。
5		A.CaDir_Operator	一人以上の許可された運用者が割り当てられる。さらに彼らは、信用できる。そのため、彼らは、権限を乱用し、故意にセキュリティを低める可能性は、低いとともに、複数人運用時において他の管理者･運用者･監査者と結託はしない。
6		A.CaDir_Auditor	一人以上の許可された監査者が割り当てられる。さらに彼らは、信用できる。そのため、彼らは、権限を乱用し、故意にセキュリティを低める可能性は、低いとともに、複数人運用時において他の管理者･運用者･監査者と結託はしない。
11	接続の前提	A.CaDir_Abstract	TOE が動作するために必要な OS や依存するライブラリは、不正に改変され誤動作する可能性は低い。
12		A.CaDir_Separation	TOE が動作するマシンには、TOE の動作に必要なソフトウェア以外を故意にインストールする可能性は低い。

2-2 脅威

内部不正を考慮したセキュリティ環境の脅威については、「表 2-2　TOE に係るセキュリティ環境の脅威一覧」と同一であるが、悪意を持った TOE 管理者・運用者・監査者が脅威エージェントとなる脅威が追加される。

2-3 組織のセキュリティポリシー

内部不正を考慮したセキュリティ環境の組織のセキュリティポリシーについては、「表 2-3 TOE に係るセキュリティ環境の組織のセキュリティポリシー一覧」と同一であると想定する。

3. 脅威のセキュリティ目標・対策及び実装システムに対する評価

別紙「脅威に対する対策及びリスク評価」参照。

なお、別紙の一覧表における、「内部不正該当」列に「○」の記載がある行が、内部不正を考慮した評価結果である。

4. 脅威ツリー及びリスク評価一覧

4-1 リスク格付けの考え方

リスク格付の考え方に関しては、「表 4-1 リスク格付の考え方」と同一である。

4-2 リスク評価

別紙「脅威に対する対策及びリスク評価」参照。なお、別紙の一覧表における、「内部不正該当」列に「○」の記載がある行が、内部不正を考慮した評価結果である。

以上

セキュリティ評価報告書

（TOE： VA）

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

本報告書における、TOE(Target of Evaluation)とは、複数方式タイムスタンプ検証サブシステムの構成要素である複数方式タイムスタンプ検証サーバ装置である。

複数方式タイムスタンプ検証サーバ装置は、利用者に対して、独立トークン方式及びリンクトークン方式のタイムスタンプを対象としたタイムスタンプ検証サービスを提供する。

1. TOE の機能概要

TOE は、利用者に対して、以下の機能を提供する。

表 1-1：機能概要

#	機能名		説明
1	独立トークン方式タイムスタンプ検証機能	正当性検証	タイムスタンプトークンの形式検証、正当性検証、電子データとタイムスタンプトークンの対応検証を実行する。
2		時刻トレーサビリティ検証	タイムスタンプトークンに含まれる時刻情報の信頼性を検証する。時刻配信経路と時刻精度を確認する。
3		検証結果検証	セキュア保管型のタイムスタンプ長期真正性保証機能が作成した検証結果に基づき、過去時点におけるタイムスタンプトークンの正当性検証と時刻トレーサビリティ検証結果を評価する。
4		再タイムスタンプ検証	再タイムスタンプ方式のタイムスタンプ長期真正性保証機能が作成した再タイムスタンプ（アーカイブタイムスタンプ）検証を実行する。
5	リンクトーク方式タイムスタンプ検証機能	正当性検証	タイムスタンプトークンの形式検証、正当性検証、電子データとタイムスタンプトークンの対応検証を実行する。
6		時刻トレーサビリティ検証	タイムスタンプトークンに含まれる時刻に関わる時刻配信経路と時刻精度を示す時刻監査レポートの格納場所（URL）を通知する。
7	独立トークン方式タイムスタンプ長期真正性保証機能	セキュア保管方式	タイムスタンプ検証サーバが検証時に作成する検証記録をヒステリシス署名技術により長期保証する。
8		再タイムスタンプ方式	正当性検証及び時刻トレーサビリティ検証に成功したタイムスタンプに対して再タイムスタンプ（アーカイブタイムスタンプ）により長期保証する。長期保証したタイムスタンプは、検証結果の拡張領域に格納される。

2. TOE 構成図

TOE 構成図を以下に示す。意図されたインタフェースを介してタイムスタンプ検証サーバ装置と通信する外部システム、及びタイムスタンプ検証サーバ装置に含まれる周辺機器などのコンポーネントの一部は、セキュリティ評価対象外である。下記の例では、TSA1、TSA2、検証 Client（検証クライアント）、Firewall（ファイアウォール）、Directory Server（ディレクトリサーバ）、CA Server

（CA サーバ）、NTP Server（日本標準時と同期した NTP サーバ）、PKCS#11 モジュール及びハードウェア暗号モジュールは、評価対象外である。

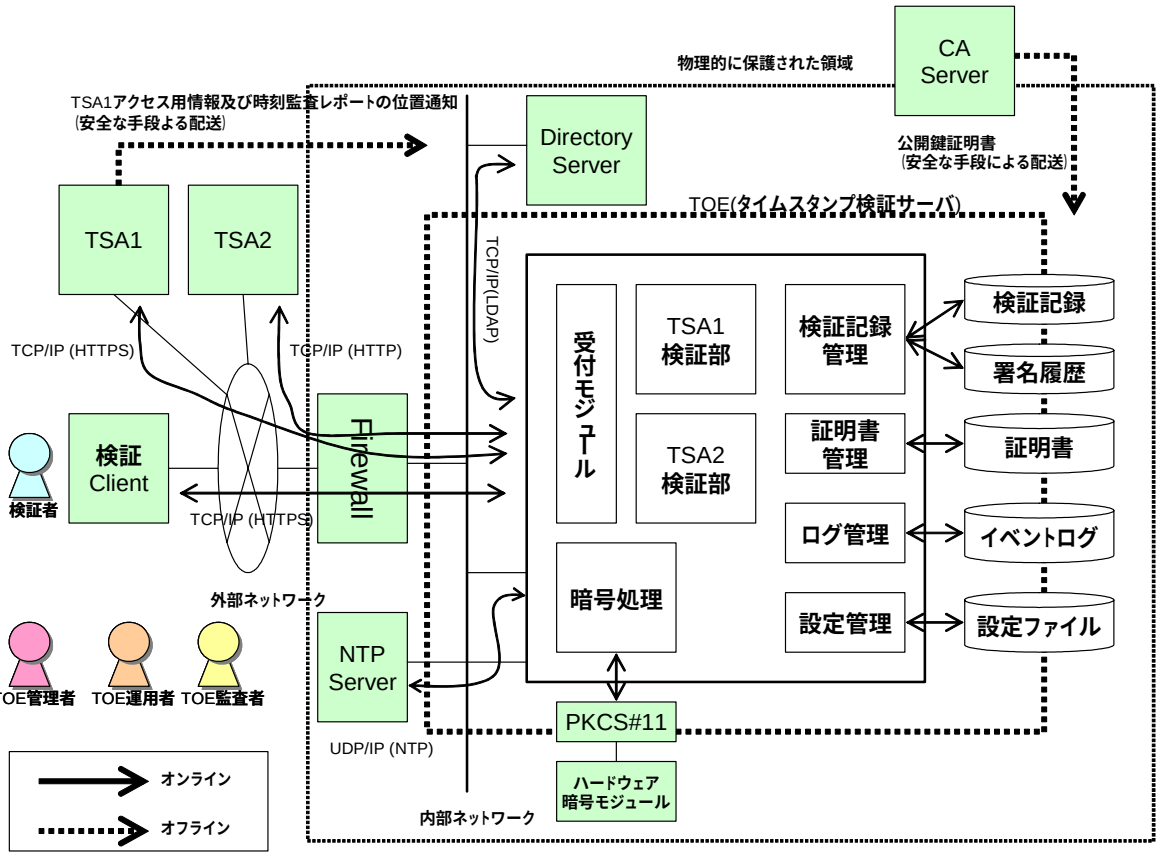


図 1-1：TOE 構成図

3. 利用する暗号技術と暗号コンポーネント構成図

TOE にて、利用される暗号技術は、以下の通りである。

表 1-2：使用される暗号技術

#	使用している暗号技術		使用目的
1	SSLv3/TLSv1.0	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 RSAES_PKCS1_v1_5 鍵長 1024 ビット 【共通鍵暗号方式】 128 ビット (RC4) 【ハッシュ関数】 SHA-1	通信路の暗号化 通信データの改竄検知 認証（タイムスタンプ検証サーバの認証、TSA1 の認証）
2	PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	独立トークン方式タイムスタンプ検証 時刻トレーサビリティ検証

3	PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	検証結果（DVC）への署名
4	PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	検証記録へのヒステリシス署名の作成/検証
5	ハッシュ関数	SHA-1(H15/H16 レガシー対応) SHA-512(H17)	独立トークン方式タイムスタンプ検証（電子データとタイムスタンプトークンの間の照合）
6	ハッシュ関数	RIPEMD-160/SHA-512	リンクトークン方式タイムスタンプ検証（電子データとタイムスタンプトークンの間の照合）
7	ハッシュ関数	SHA-1	検証記録へのヒステリシス署名の作成/検証（署名の結合）
8	ハッシュ関数	SHA-1	検証要求に含まれるタイムスタンプ情報に対応するタイムスタンプ検証サーバに格納される検証記録を特定するための識別情報を作成

TOE における暗号コンポーネント構成図を以降にて示す。図に含まれる番号は、表 1-2の項番と対応する。

3-1 検証クライアントと TOE 及び TOE と TSA の間の通信

検証クライアントと TOE 間、および、TOE と TSA1 の間の通信は、SSLv3.0/TLSv1.0 である。SSL のライブラリは、TOE の下位抽象マシンに位置づけられる。

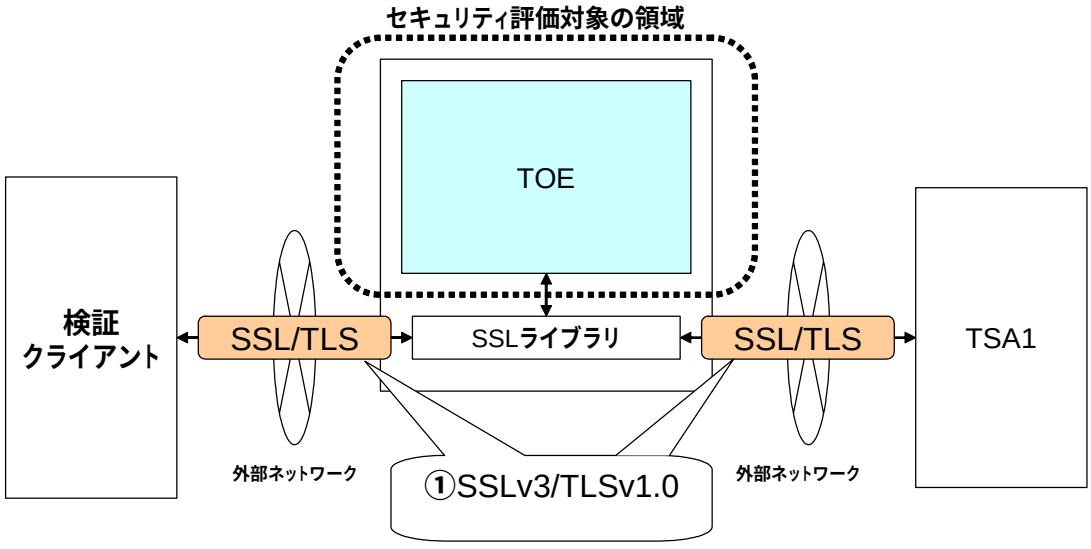


図 1-2：利用者(検証クライアント)と TOE 間、及び TOE と TSA1 間の SSL/TLS 通信

3-2 独立トークン方式タイムスタンプ検証

TOE は、独立トークン方式のタイムスタンプを検証するとき、PKI 技術に基づく、公開鍵証明書検証、署名値検証、などを実行する。また、検証の結果となる DVC に対して、デジタル署名を付与する。

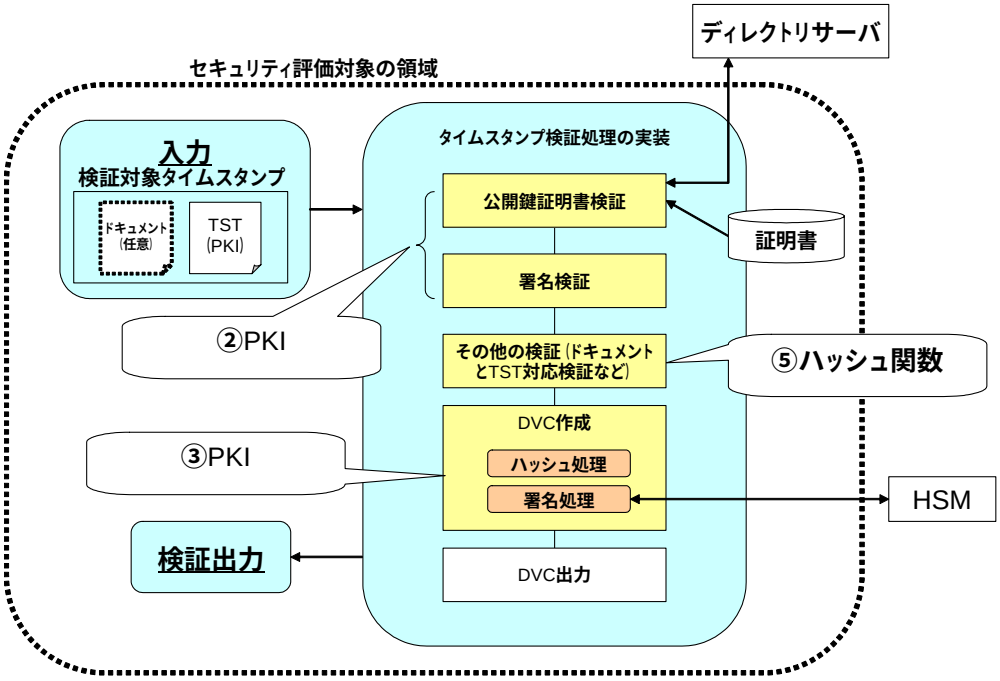


図 1-3：独立トークン方式タイムスタンプ検証

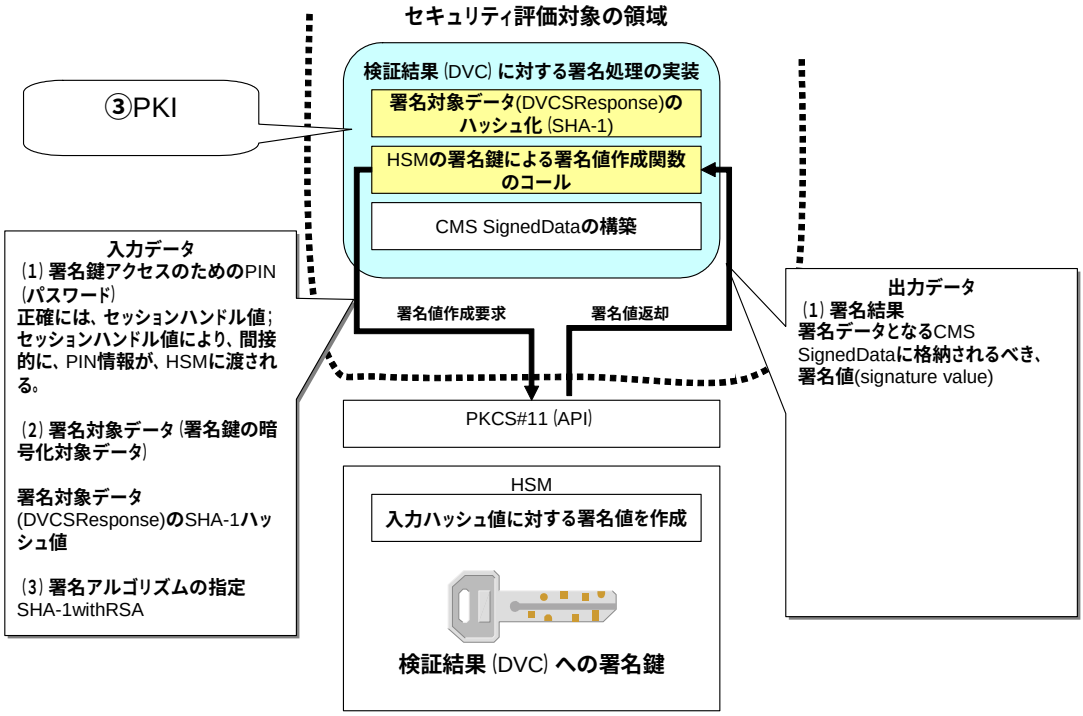


図 1-4：検証結果の署名作成（署名値作成）

3-3 リンクトークン方式タイムスタンプ検証

TOE は、リンクトークン方式のタイムスタンプを検証するとき、ハッシュ関数を用いて、タイムスタンプ対象データとタイムスタンプトークンの関連性を確認する。また、検証の結果となる DVC に対して、デジタル署名を付与する。

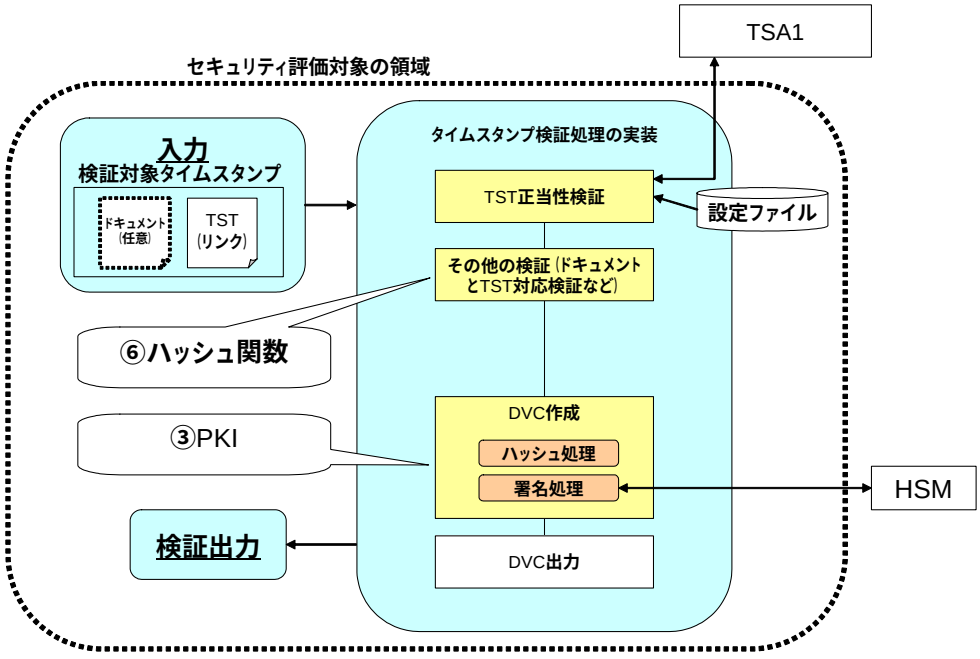


図 1-5：リンクトークン方式タイムスタンプ検証

3-4 ヒステリシス署名作成

TOE は、検証記録に対して、PKI 技術、及びハッシュ関数に基づくヒステリシス署名データを作成する。

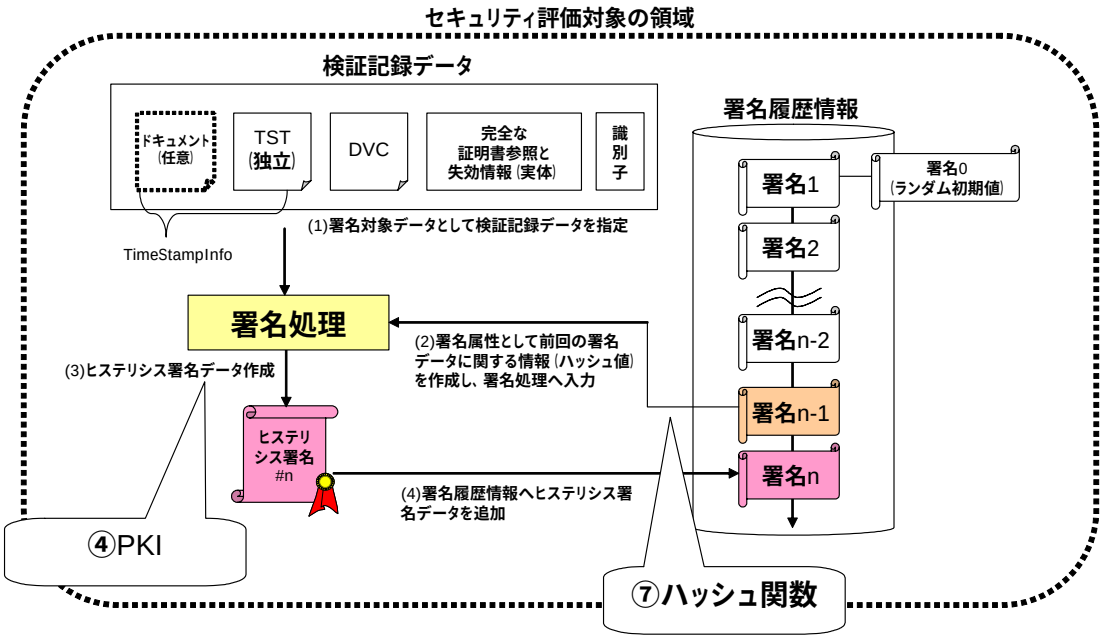


図 1-6：ヒステリシス署名作成（概要）

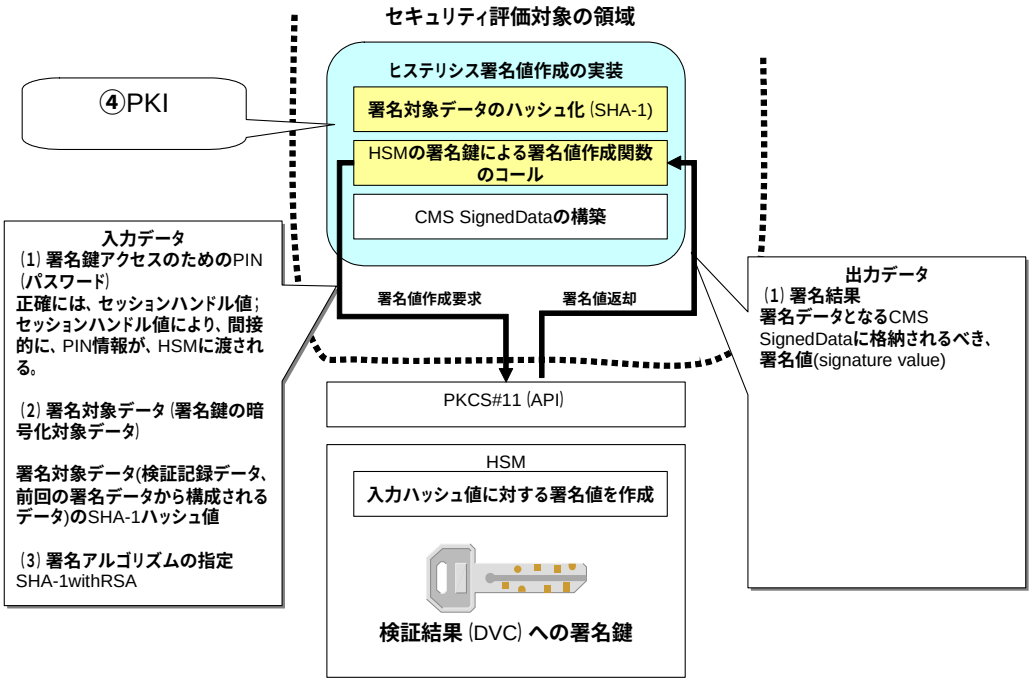


図 1-7：ヒステリシス署名作成（署名値作成）

3-5 ヒステリシス署名検証

TOE は、検証記録に関連づけられたヒステリシス署名を検証するとき、PKI 技術、及びハッシュ関数を用いて検証を実行する。

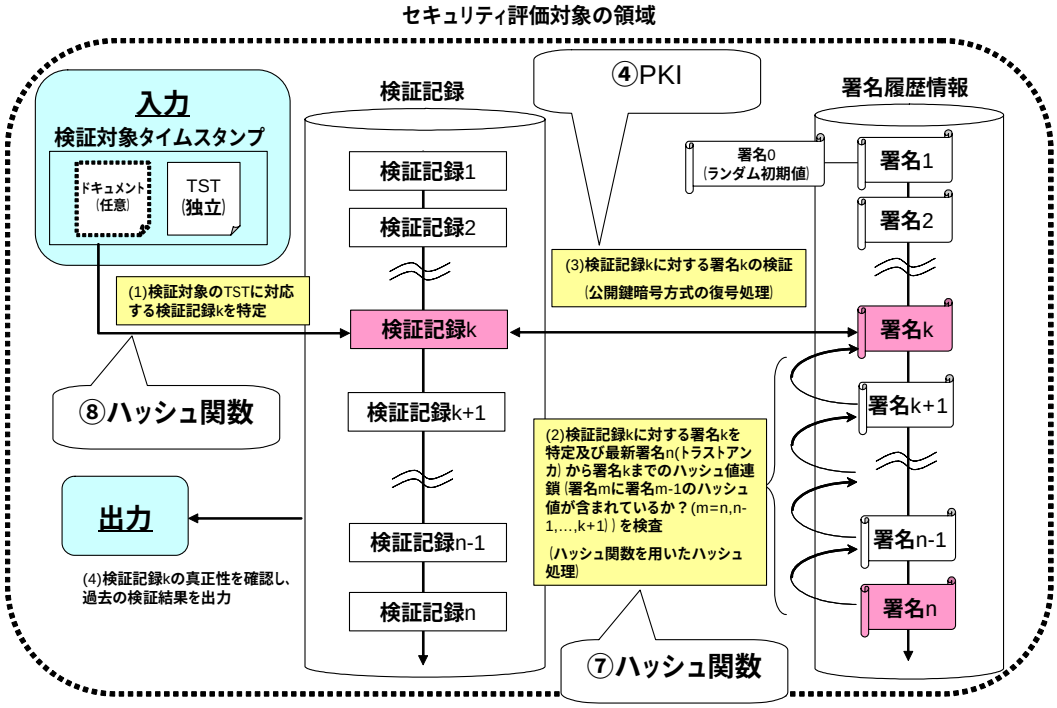


図 1-8：ヒステリシス署名の検証

4. 関与者

TOE の関与者は、TOE サービス利用者、TOE サービス提供者に大きく分かれる。また、TOE サービス提供者が使用する外部の信頼できる機関も含まれる。なお、外部の悪意者は含めていない。

表 1-3：関与者

#	関与者	説明
1	TOE 管理者	暗号機能に関わる初期化及び管理業務を行う。 TOE に関わるユーザ/役割を管理する。
2	TOE 運用者	TOE の起動･停止を実行する。 TOE 管理者の指示の元で各種設定など運用業務を行う。
3	TOE 監査者	TOE が生成するログデータなどの監査データの分析等の監査業務を行う。 管理者と運用者と同じ組織に所属し、TOE 設置場所へ入室することができる。但し、TOE にアクセスすることは許可されない。
4	利用者	TOE が提供する検証サービスを利用する。検証者
5	CA	信頼のできる第三者機関、及び装置。TOE は、この CA から、利用する公開鍵証明書を発行してもらう。また、CA が公開するディレクトリサーバを使用し、公開鍵証明書の情報取得、有効性検証を実行する。
6	TSA1	信頼のできる第三者機関、及び装置。TOE は、この TSA1 に対して、リンクトークン方式のタイムスタンプトークン検証を委任する。
7	TSA2	信頼のできる第三者機関、及び装置。TOE は、この TSA2 が提供する独立トークン方式のタイムスタンプサービスを利用し、タイムスタンプ長期保証（再タイムスタンプ方式）を実現する。

5. 資産

TOE に関する資産は、下記の通りである。

表 1-4：資産

#	分類		資産名
1	情報資産	利用者データ	タイムスタンプ情報（検証クライアントから受信する検証対象タイムスタンプトークンとタイムスタンプ適用先のドキュメントから構成される情報）
2			DVC(検証結果：検証結果証明書)
3		TSF データ	システム時計
4			検証サーバ設定データ
5			検証記録データ
6			署名履歴データ（ヒステリシス署名データ）
7			トラストアンカ公開鍵証明書 ※PKI 方式のタイムスタンプ検証で使用

8			検証サーバの公開鍵証明書 • DVC（検証結果）検証用公開鍵証明書 • ヒステリシス署名検証用公開鍵証明書 • SSL サーバ公開鍵証明書
9			私有鍵データ • DVC 署名鍵 • ヒステリシス署名鍵
10			私有鍵データ • SSL サーバ私有鍵
11			ログデータ
12			ユーザ識別情報とユーザ認証データ（パスワードデータ） ※依存する OS の機能により管理 ※検証サーバのシステム管理者、運用者、監査者に対応
13			TSA1 アクセス用 ID と認証データ（パスワードデータ） ※設定ファイルに格納
14			HSM アクセス用パスワード ※設定ファイルに格納
15	IT 実装	スクリプトファイル	検証サーバ制御ツール（シェルスクリプト）
16		バイナリファイル	検証サーバ

第2章 セキュリティ環境

本章では、内部不正を考慮しない場合の TOE のセキュリティ環境（前提、脅威、組織のセキュリティポリシー）について記載する。

1. 前提

TOE が使用される上で想定される前提を以下に示す。前提は、大きく三つに分類される。TOE が設置される場所に関する物理的な前提、TOE を操作する人に関する人的な前提、TOE の接続環境や前提とする下位抽象マシンに関する接続的な前提である。

表 2-1：前提

#	分類	項目	説明
1	物理的	A.VA_Location	TOE の処理リソースは、コントロールされたアクセス・ファシリティの中に配置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2	物理的	A.VA_Environment	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
3	物理的	A.VA_MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
4	人的	A.VA_Administrator	一つ以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 • TOE に関わるユーザ/役割を管理する • 暗号機能に関わる初期化及び管理業務を行う • TOE 上で悪意のあるソフトウェアが動作しないようにする • TOE の要件を満たす適切なディスクスペースを用意する • TOE のデータベースを適切に管理する さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
5	人的	A.VA_Operator	一人以上の許可された運用者が割り当てられる。 • TOE の起動・停止を実行する • TOE 管理者の指示の元で各種設定など運用業務を行う さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
6	人的	A.VA_Auditor	一人以上の許可された監査者が割り当てられる。 • TOE に関するログを取得し、分析を行う さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。

7	人的	A.VA_Service_Requestor	タイムスタンプ検証者は、タイムスタンプ検証結果を検証及び保持する。
8	接続	A.VA_Device	周辺機器への全接続は、コントロールされたアクセス・ファシリティ内に存在する。
9	接続	A.VA_Firewall	ファイアウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
10	接続	A.VA_Peer	検証クライアントを除く TOE と通信する意図された他システムは、信頼できる。
11	接続	A.VA_Requestor_Connection	タイムスタンプ検証者が操作するマシンとTOEの間の通信路は、TOE の成りすまし、データの改ざん、データの盗聴を防止する。
12	接続	A.VA_TSA1_Connection	TSA1（リンキング方式のタイムスタンプ局）と TOE の間の通信路は、TSA1 の成りすまし、データの改ざん、データの盗聴を防止する。
13	接続	A.VA_Abstract	TOE が動作するために必要な OS（システムクロックを除く）や依存するライブラリは、不正な改変から保護され、正しく動作する。
14	接続	A.VA_Separation	TOE が動作するマシンには、TOE の動作に必要なソフトウェア以外はインストールされないものとする。

2. 脅威

TOE の脅威を以下に示す。基本的に、「前提」に矛盾する脅威を含めていないが、暗号技術や時刻情報などに関するものは、「前提」の記載内容に関わらず脅威として含めている。また、TOE の資産に共通的な概念である改ざんや情報漏えい（情報暴露）に関わる脅威に関しては抽象化した名称とし、記載した。後述する脅威ツリーでは、より具体的な脅威として記述する。

表 2-2：脅威

#	項目	説明
1	T.VA_DVC_Crypto_Compromise1	検証者や外部の不正者が、脆弱化したハッシュ関数が用いられたタイムスタンプを利用し、改ざんされたデータがあたかもタイムスタンプが示す時刻に存在し、それ以降改ざんがなかったことを主張する。
2	T.VA_DVC_Crypto_Compromise2	現在の DVC(検証結果)に使用された暗号アルゴリズムの信頼性が乏しいため、発行された DVC の証明力が低くなる。
3	T.VA_DVC_Crypto_Compromise3	過去の DVC(検証結果)に使用された暗号アルゴリズムの信頼性が乏しいため、過去に発行された DVC の証明力が低くなる。
4	T.VA_DVC_SigHistory_Compromise	過去に作成されたヒステリシス署名に使用された暗号アルゴリズム（ハッシュ関数）が脆弱化し、署名履歴の信頼性が乏しくなる
5	T.VA_System_Clock_Modify1.1	外部の悪意者が、物理的に TOE にアクセスし、システム時刻を変更する。日本標準時と大きくずれたシステム時刻になり、情報資産(例：検証結果、ログなど)に含まれる時刻情報の信頼性が乏しくなる。

6	T.VA_System_Clock_Modify1.2	外部の悪意者が、ネットワークを介して TOE にアクセスし、システム時刻を変更する。日本標準時と大きくずれたシステム時刻になり、情報資産(例：検証結果、ログなど)に含まれる時刻情報の信頼性が乏しくなる。
7	T.VA_Time_Source1.1	外部の悪意者が、物理的に TOE にアクセスし、TOE が参照する時刻ソースを変更する。日本標準時と大きくずれたシステム時刻となる。日本標準時と大きくずれたシステム時刻になり、情報資産(例：検証結果、ログなど)に含まれる時刻情報の信頼性が乏しくなる。
8	T.VA_Time_Source1.2	外部の悪意者が、ネットワークを介して TOE にアクセスし、TOE が参照する時刻ソースを変更する。日本標準時と大きくずれたシステム時刻となる。日本標準時と大きくずれたシステム時刻になり、情報資産(例：検証結果、ログなど)に含まれる時刻情報の信頼性が乏しくなる。
9	T.VA_System_Clock_Inaccuracy	システム時計の品質、あるいは、TOE の設置環境の温度変化により、日本標準時と大きくずれたシステム時刻になり、情報資産(例：検証結果、ログなど)に含まれる時刻情報の信頼性が乏しくなる。
10	T.VA_Time_Source_Unavailable	時刻ソース参照先のマシンの停止、あるいは、時刻ソース参照先への通信路に障害が発生し、時刻ソースが参照できない。日本標準時と大きくずれたシステム時刻となり、情報資産(例：検証結果、ログなど)に含まれる時刻情報の信頼性が乏しくなる。
11	T.VA_Data_Mod_Undetect	許可されたユーザ（管理者、運用者）が、不注意で、情報資産の内容を改変する。 ※抽象化脅威であり、後述する脅威ツリーにて、資産に応じた具体的な脅威を示す。
12	T.VA_Crack_Mod_Data1.1	外部の悪意者が、物理的に TOE にアクセスし、情報資産を改竄する。 ※抽象化脅威であり、後述する脅威ツリーにて、資産に応じた具体的な脅威を示す。
13	T.VA_Crack_Mod_Data1.2	外部の悪意者が、ネットワークを介して TOE にアクセスし、情報資産を改竄する。 ※抽象化脅威であり、後述する脅威ツリーにて、資産に応じた具体的な脅威を示す。
14	T.VA_Crack_Disclose_Data1.1	外部の悪意者が、物理的に TOE にアクセスし、情報資産を情報漏洩する。
15	T.VA_Crack_Disclose_Data1.2	外部の悪意者が、ネットワークを介して TOE にアクセスし、情報資産を漏洩（暴露）する。 ※抽象化脅威であり、後述する脅威ツリーにて、資産に応じた具体的な脅威を示す。
16	T.VA_DoS_Attack	検証者、あるいは、外部の悪意者が、DoS 攻撃を行う。
17	T.VA_BufferOverFlow_Attack	検証者、あるいは、外部の悪意者が、バッファー・オーバー・フロー攻撃を行う。
18	T.VA_Crack_Imperson_TOE	外部の悪意者が、TOE に成りすまし、検証者に対して偽のサービスを提供する。
19	T.VA_TOE_Bug	タイムスタンプ検証サーバのプログラム不良により、情報資

		産の信頼性が失われる。
20	T.VA_Unauth_Access	外部の悪意者が、TOE に対して物理的にアクセスする。
21	T.VA_Imperson_Admin	外部の悪意者が、ユーザ認証情報を入手し、管理者に成りすます。
22	T.VA_Hack_Imperson_TSA2	外部の悪意者が、TOE と TSA2 の通信間に割り込み、TSA2 に成りすます。
23	T.VA_Hardware_Failure	消耗や劣化のため、ハードウェアが故障し、検証サービスが実行できない。
24	T.VA_Peer_Failure	他システムの想定外のシステムダウンが継続し、検証サービスが実行できない。
25	T.VA_Connection_Failure	他システム間との通信回線が消耗や劣化のため故障し、検証サービスが実行できない。
26	T.VA_Cracker_Repudiation	検証者や外部の悪意者が、不正行為を否認する。

3. 組織のセキュリティポリシー

TOE が使用される上で、組織として採用すべきセキュリティポリシーは、以下の通りである。

表 2-3：組織のセキュリティポリシー

#	項目	説明
1	P.VA_Time_Source	TOE は、信頼のできる時刻ソースを参照すること。この時刻ソースは、TOE 所有者にとってアベイラブルであること。また、時刻ソースの信頼性と正確性は TOE 所有者にとって受容可能であること。
2	P.VA_System_Clock_Management	TOE が参照するシステム時計を信頼のできる時刻ソースと同期させる。
3	P. VA_HSM	TOE を使用する組織は、FIPS 140-2 level3 相当の機能を持つ HSM により、物理的に保護された検証サーバの私有鍵を利用した、検証結果や検証記録に対する暗号操作及び私有鍵のライフサイクル管理を行うこととする。
4	P. VA_PKI_Management	安全に管理された PKI の中で、TOE を運用すること。 全ての鍵と証明書は、安全に発行、失効される。 全ての鍵と証明書の状態は、使用前にチェックされる。
5	P. VA_Cryptography	全ての暗号処理（署名と検証等）は、「電子政府推奨暗号リスト（平成15年2月20日、総務省、経済産業省）」に記載されたアルゴリズムによって実装されなければならない。
6	P.VA_Password_Management	TOE 利用者のパスワードは、TOE 利用者本人によって適切に管理され、本人以外に知られてはならない。
7	P.VA_Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄、または削除の防止のために必要な措置をとることとする。
8	P.VA_Dual_Control	TOE の管理業務における重要な操作は、複数の TOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
9	P.VA_Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。
10	P.VA_Check_Virus	最新のウィルスチェックソフトを用いて、定期的なウィルスチ

		ェックを実行する。
11	P.VA_Check_Received_Data	他サブシステムから送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。

第3章 セキュリティ目標・対策と実装システムの評価

セキュリティ環境の脅威のセキュリティ目標･対策及び実装システムに対する評価を記す。さらに、セキュリティ環境の前提と組織のセキュリティポリシーに関する実現方法例を記述する。

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

脅威のセキュリティ目標・対策及び実装システムに対する評価を以下に示す。

表 3-1：脅威に対するセキュリティ目標・対策及び実装システムに対する評価

#	脅威名	セキュリティ目標・対策		統合化システムにおける実現
1	T.VA_DVC_Crypto_Compromise1	防止	使用された暗号アルゴリズムが受容可能かどうかを確認する。	使用された暗号アルゴリズムが受容可能かどうかを確認する機能
		検出	権威のある機関による評価情報（例：NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報）により暗号アルゴリズムの脆弱性を確認する。	NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報により暗号アルゴリズムの脆弱性を確認することで実現可能。
		回復	-	-
2	T.VA_DVC_Crypto_Compromise2	防止	受容可能な暗号アルゴリズム（例：電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省）に掲載されたもの）を使用する。	受容可能な暗号アルゴリズム（例：電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省）に掲載されたもの）を使用する。
		検出	権威のある機関による評価情報（例：NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報）により暗号アルゴリズムの脆弱性を確認する。	NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報により暗号アルゴリズムの脆弱性を確認することで実現可能。
		回復	-	-
3	T.VA_DVC_Crypto_Compromise3	防止	検証記録を長期保証（例：長期保証の要件としては、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成 17 年 10 月)」を参照。）。 複数の暗号アルゴリズムを使用する。	ヒステリシス署名技術を用いた検証記録長期保証機能 また、複数の暗号アルゴリズムを使用することで実現可能。
		検出	権威のある機関による評価情報（例：NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報）により暗号アルゴリズムの脆弱性を確認する。	NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報により暗号アルゴリズムの脆弱性を確認することで実現可能。
		回復	-	-

4	T.VA_DVC_SigHistory_Compromise	防止	検証記録とヒステリシス署名から構成されるデータに対して最新のヒステリシス署名を適用する。 複数の暗号アルゴリズムを使用する。	検証記録とヒステリシス署名から構成されるデータに対して最新のヒステリシス署名を適用することで実現可能。 複数の暗号アルゴリズムを使用することで実現可能。
		検出	権威のある機関による評価情報（例：NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報）により暗号アルゴリズムの脆弱性を確認する。	NIST の Computer Security Resource Center や IPA セキュリティセンターの公開情報により暗号アルゴリズムの脆弱性を確認することで実現可能。
		回復	-	-
5	T.VA_System_Clock_Modify1.1	防止	入退室管理を行う。	入退室管理を行うことで実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	時刻源(NTP サーバ)と時刻同期させる。	時刻源(NTP サーバ)と時刻同期させる。
6	T.VA_System_Clock_Modify1.2	防止	ファイアウォールを設置する。 OS やライブラリなどを最新な状態にする。	ファイアウォールを設置する。OS やライブラリなどを最新な状態にすることで実現可能。
		検出	侵入監視システム（IDS）を設置する。	侵入監視システム（IDS）を設置することで実現可能。
		回復	時刻源(NTP サーバ)と時刻同期させる。	時刻源(NTP サーバ)と時刻同期する機能。
7	T.VA_Time_Source1.1	防止	入退室管理を行う。	入退室管理を行うことで実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	時刻源(NTP サーバ)が含まれた設定情報のバックアップ/リストア後、時刻源(NTP サーバ)と時刻同期させる。	設定情報のバックアップ/リストアで実現可能。 時刻源(NTP サーバ)と時刻同期する機能
8	T.VA_Time_Source1.2	防止	ファイアウォールを設置する。 OS やライブラリなどを最新な状態にする。	ファイアウォールを設置する。OS やライブラリなどを最新な状態にすることで実現可能。
		検出	侵入監視システム（IDS）を設置する。	侵入監視システム（IDS）を設置することで実現可能。
		回復	時刻源(NTP サーバ)が含まれた設定情報のバックアップ/リストア後、時刻源(NTP サーバ)と時刻同期させる。	設定情報のバックアップ/リストアすることで実現可能。 時刻源(NTP サーバ)と時刻同期する機能
9	T.VA_System_Clock_Inaccuracy	防止	定期的に時刻源(NTP サーバ)と時刻同期させる	定期的に時刻源(NTP サーバ)と時刻同期させる機能
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	時刻源(NTP サーバ)と時刻同期させる。	時刻源(NTP サーバ)と時刻同期する機能
10	T.VA_Time_Source_Unavailable	防止	時刻ソースの冗長化（例：複数の時刻ソース、また、時刻ソースに対する複数の通信路を用意する）	時刻ソースの冗長化（例：複数の時刻ソース、また、時刻ソースに対する複数の通信路を用意する）により、実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。

		回復	復旧後、時刻源(NTP サーバ)と時刻同期させる。	復旧後、時刻源(NTP サーバ)と時刻同期させる。
11	T.VA_Data_Mod_Undetect	防止	複数人による操作	複数人による操作により実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	バックアップ/リストア	バックアップ/リストアにより実現可能。
12	T.VA_Crack_Mod_Data1.1	防止	入退室管理を行う。	入退室管理を行うことで実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	バックアップ/リストア	バックアップ/リストアにより実現可能。
13	T.VA_Crack_Mod_Data1.2	防止	ファイアウォールを設置する。 OS やライブラリなどを最新な状態にする。	ファイアウォールを設置する。OS やライブラリなどを最新な状態にすることで実現可能。
		検出	侵入監視システム（IDS）を設置する。	侵入監視システム（IDS）を設置することで実現可能。
		回復	バックアップ/リストア	バックアップ/リストアにより実現可能。
14	T.VA_Crack_Disclose_Data1.1	防止	入退室管理を行う。 データの暗号化。	入退室管理を行うことで実現可能。 データを暗号化することで実現可能。 ※一部のデータは暗号化済み。例えば、SSL サーバ私有鍵は、3-key トリプル DES で暗号化。
		検出	外部からの通知により確認する。 ログデータにより確認する。	外部からの通知により確認することで実現可能。 ログデータにより確認することで実現可能。
		回復	-	-
15	T.VA_Crack_Disclose_Data1.2	防止	ファイアウォールを設置する。 OS やライブラリなどを最新な状態にする。 データの暗号化。	ファイアウォールを設置する。OS やライブラリなどを最新な状態にすることで実現可能。 データを暗号化することで実現可能。 ※一部のデータは暗号化済み。例えば、SSL サーバ私有鍵は、3-key トリプル DES で暗号化。
		検出	外部からの通知により確認する。 ログデータにより確認する。	外部からの通知により確認することで実現可能。 ログデータにより確認することで実現可能。
		回復	-	-
16	T.VA_DoS_Attack	防止	システム構成を冗長化する。 DoS 対策機能を持つ IDS システムを設置する。	システム構成を冗長化することで実現可能。 DoS 対策機能を持つ IDS システムを設置することで実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	-	-

17	T.VA_BufferOverFlow_Attack	防止	OS やライブラリなどを最新な状態にする。	OS やライブラリなどを最新な状態にする。
		検出	OS やライブラリベンダによる脆弱性公開情報を確認する。	OS やライブラリベンダによる脆弱性公開情報を確認することで実現可能。
		回復	-	-
18	T.VA_Crack_Imperson_TOE	防止	検証者は、検証結果（DVC）を検証し、検証結果発行元を確認する。	検証者は、検証結果（DVC）を検証し、検証結果発行元を確認する。
		検出	検証者は、検証結果（DVC）を検証し、検証結果発行元を確認する。	検証者は、検証結果（DVC）を検証し、検証結果発行元を確認する。
		回復	-	-
19	T.VA_TOE_Bug	防止	TOE 開発者が、ソフトウェア不良を防ぐ開発プロセスを採用する。	TOE 開発者が、ソフトウェア不良を防ぐ開発プロセスを採用することで実現可能。
		検出	-	-
		回復	ソフトウェア不具合のパッチ作成・配布・適用を適切に実施する。	ソフトウェア不具合のパッチ作成・配布・適用を適切に実施することで実現可能。
20	T.VA_Unauth_Access	防止	入退室管理を行う。	入退室管理を行うことで実現可能。
		検出	-	-
		回復	-	-
21	T.VA_Imperson_Admin	防止	ユーザ認証情報の管理教育を徹底する。	ユーザ認証情報の管理教育を徹底することで実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	ユーザ認証情報を変更する。	ユーザ認証情報を変更することで実現可能。
22	T.VA_Hack_Imperson_TSA2	防止	TSA2 から送信されるタイムスタンプトークンを検証する。	TSA2 から送信されるタイムスタンプトークンの検証機能
		検出	TSA2 から送信されるタイムスタンプトークンを検証する。	TSA2 から送信されるタイムスタンプトークンの検証機能
		回復	-	-
23	T.VA_Hardware_Failure	防止	システム構成の冗長化。	システム構成の冗長化により実現可能。
		検出	-	-
		回復	-	-
24	T.VA_Peer_Failure	防止	システム冗長化構成を持つ通信相手（複数装置を持つタイムスタンプ局、複数のディレクトリサーバ）を利用する。	システム冗長化構成を持つ通信相手（複数装置を持つタイムスタンプ局、複数のディレクトリサーバ）を利用することで実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	-	-
25	T.VA_Connection_Failure	防止	システム冗長化構成を持つ通信相手（複数の通信手段を持つタイムスタンプ局、複数のディレクトリサーバ）を利用する。	システム冗長化構成を持つ通信相手（複数の通信手段を持つタイムスタンプ局、複数のディレクトリサーバ）を利用することで実現可能。
		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	-	-
	T.VA_Cracker_Repudiation	防止	-	-

		検出	ログデータにより確認する。	ログデータにより確認することで実現可能。
		回復	-	-

2. 前提の実現方法例

セキュリティ環境における前提の実現方法例を以下に示す。

表 3-2：前提の実現方法例

#	分類	項目	実現方法例
1	物理的	A.VA_Location	IC カードによる入退出管理を行う iDC（インターネットデータセンター）に TOE を設置する。
2	物理的	A.VA_Environment	電磁波対策、電力対策、温度･湿度対策が行われている iDC（インターネットデータセンター）に TOE を設置する。
3	物理的	A.VA_MEDIA	定期的なデータのバックアップと適切なシステムマイグレーションを行う。
4	人的	A.VA_Administrator	組織が策定する安全規定や運用管理規定に基づく教育を十分に受ける。 罰則規定を設ける。 TOE に関する操作は運用マニュアルに基づき実行する。
5	人的	A.VA_Operator	組織が策定する安全規定や運用管理規定に基づく教育を十分に受ける。 罰則規定を設ける。 TOE に関する操作は運用マニュアルに基づき実行する。
6	人的	A.VA_Auditor	組織が策定する安全規定や運用管理規定に基づく教育を十分に受ける。 罰則規定を設ける。 TOE に関する操作は運用マニュアルに基づき実行する。
7	人的	A.VA_Service_Requestor	タイムスタンプ検証者は、安全性が確保された PC(*1)及び信頼の出来る検証クライアント(*2)を用いて、タイムスタンプ検証結果を検証及び保持する。 (*1) 最新の OS とライブラリの状態とする、最新のウィルス定義ファイルを用いてウィルスチェックを行う。 (*2)信頼のできる相手から検証クライアントを入手する。あるいは、自身で検証クライアントを開発し、使用する。
8	接続	A.VA_Device	接続される周辺機器は、TOE と同じく、入退出管理が行われる iDC（インターネットデータセンター）に設置される。 また、HSM に関しては、FIPS140-2 Level3 認定を受けたものを使用する。
9	接続	A.VA_Firewall	プライベートネットワークと外部ネットワークを結ぶファ

			イアウォール装置を用意する。 ファイアウォール装置の設定、及び管理を適切に実施する。
10	接続	A.VA_Peer	信頼のできる第三者（TTP）が運用するシステムを利用する。
11	接続	A.VA_Requestor_Connection	タイムスタンプ検証者が操作するマシンとTOEの間の通信路をSSLv3.0/TLSv1.0(RC4 128ビット強)とし、TOE の成りすまし、データの改ざん、データの盗聴を防止する。
12	接続	A.VA_TSA1_Connection	TSA1（リンキング方式のタイムスタンプ局）と TOE の間の通信路をSSLv3.0/TLSv1.0(RC4 128ビット強)とし、TSA1 の成りすまし、データの改ざん、データの盗聴を防止する。
13	接続	A.VA_Abstract	運用管理規定に従い、TOEが動作するために必要なOS（システムクロックを除く）や依存するライブラリは、不正な改変から保護され、正しく動作するように管理する。
14	接続	A.VA_Separation	運用管理規定に従い、TOE が動作するマシンには、TOE の動作に必要なソフトウェア以外はインストールしない。

3. 組織のセキュリティポリシーの実現方法例

セキュリティ環境における組織のセキュリティポリシーの実現方法例を以下に示す。

表 3-3：セキュリティポリシーの実現方法例

#	項目	実現方法例
1	P.VA_Time_Source	日本標準時と同期した信頼の出来る第三者（TTP）が運用する NTP サーバを時刻ソースとする。
2	P.VA_System_Clock_Management	定期的に NTP サーバと通信を行い、システム時計を日本標準時と同期させる。
3	P. VA_HSM	TOE を使用する組織は、FIPS 140-2 level3 相当の機能を持つ HSM を採用し、物理的に保護された検証サーバの私有鍵を利用した、検証結果や検証記録に対する暗号操作及び私有鍵のライフサイクル管理を行う。
4	P. VA_PKI_Management	信頼のできる認証局を利用し、運用マニュアルに従い、以下を実施する。 安全に管理された PKI の中で、TOE を運用する。 全ての鍵と証明書の状態を使用前にチェックする。
5	P. VA_Cryptography	全ての暗号処理（署名と検証等）は、「電子政府推奨暗号リスト（平成15年2月20日、総務省、経済産業省）」に記載されたアルゴリズムによって実装する。 • SSLv3.0/TLSv1.0：RC4 の 128 ビット長さ • PKI：RSASSA-PKCS1-v1_5、鍵長 1024 ビット、SHA-1 • ハッシュ関数：SHA-1/SHA-512
6	P.VA_Password_Management	許可されない他人へのパスワード漏洩を防ぐため、運用管理規定に従い、パスワード管理を行う。

		ソーシャルエンジニアリングを含む安全性教育を徹底する。
7	P.VA_Protect_Log	TOEを利用する組織は、アクセスコントロール技術、電子署名技術、WORM（Write-Once-Read Many）デバイス、などを用いて、監査ログの暴露、改竄、または削除の防止のために必要な措置をとる。
8	P.VA_Dual_Control	運用マニュアルに従い、TOE の管理業務における重要な操作は、複数の TOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
9	P.VA_Check_Abstract_Vulnerability	OS やライブラリベンダの公表情報、及び公的な評価機関（例：NISTのComputer Security Resource CenterやIPAセキュリティセンターの公開情報）を定期的に監視し、OSやライブラリなどの脆弱性を確認し、対策を行う。
10	P.VA_Check_Virus	信頼のできるウィルスチェックソフトウェアを導入する。 ウィルスチェックソフトウェアのウィルス定義情報更新機能を用いて、ウィルス定義ファイルを最新のものとする。 また、定期的なウィルスチェックを実行する。
11	P.VA_Check_Received_Data	他サブシステムから受信したデータにおいて、デジタル署名やハッシュ関数などの暗号技術が使用されている場合、その暗号技術の仕様に基づき、そのデータの真正性と完全性を確認する。

第4章 脅威ツリー及びリスク評価一覧

内部不正を考慮しない場合のセキュリティ評価における脅威ツリー、リスク評価格付けの考え方、リスク評価点を記述する。

1. 脅威ツリー

脅威ツリーを以下に示す。

#	資産	脅威	説明	上位レベルが実現するための条件			
				条件 1	条件 2	条件 3	条件 4
1	タイムスタンプ情報	T.VA_DVC_Crypto_Compromise1	検証者が、電子データを改ざんし、そのデータがあたかもタイムスタンプが示す時刻に存在し、それ以降改ざんがなかったことを主張する	タイムスタンプ検証者が脆弱性のある暗号技術が使用されたタイムスタンプトークンを含むタイムスタンプ情報を検証要求として送信する	電子データのハッシュ化に使用したハッシュ関数の脆弱性を利用し、正当な電子データと同一のハッシュ値を持つ改ざんデータを作成する		
2		T.VA_Crack_Mod_TimeStampInfo	悪意者が、検証者が送信するタイムスタンプ要求に含まれるタイムスタンプ情報（電子データとタイムスタンプトークン）を改ざんする	ネットワーク上で捕捉したタイムスタンプ情報を改ざんし、TOE へ転送する			
3		T.VA_Crack_Disclose_TimeStampInfo	悪意者が、検証者が送信するタイムスタンプ要求に含まれるタイムスタンプ情報（電子データとタイムスタンプトークン）を暴露する	ネットワーク上で捕捉したタイムスタンプ情報を外部に暴露する			
4	DVC	T.VA_Crack_Mod_DVC	悪意者が DVC に含まれる検証結果を改ざんする	悪意者が、ネットワーク上で送信される DVC を捕捉し、改ざん後、検証者へ送信する			
5		T.VA_Crack_Disclose_DVC	悪意者が DVC に含まれる電子データに含まれる情報を漏洩する	悪意者が、ネットワーク上で送信される DVC を捕捉し、情報漏洩する			

6		T.VA_DVC_Crypto_Compromise2	現在の DVC(検証結果)に使用された暗号アルゴリズムの信頼性が乏しいため、発行された DVC の証明力が低くなる	脆弱化した暗号アルゴリズムを使用した DVC（検証結果）を作成する			
7		T.VA_DVC_Crypto_Compromise3.1	過去の DVC(検証結果)に使用された暗号アルゴリズムの信頼性が乏しいため、過去に発行された DVC の証明力が低くなる	過去に発行した DVC（検証結果）に使用されている暗号鍵、あるいは、暗号アルゴリズムが脆弱化する。	計算機能力の向上		
8		T.VA_DVC_Crypto_Compromise3.2			暗号解読技術の向上		
9		T.VA_DVC_Crypto_Compromise3.3			暗号鍵の漏洩		
10	システム時計	T.VA_System_Clock_Modify1.1	日本標準時と大きくずれたシステム時刻になる	システムクロック設定コマンドで修正する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
11		T.VA_System_Clock_Modify1.2				脆弱性（e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
12		T.VA_Time_Source1.1	日本標準時と大きくずれたシステム時刻になる	時刻ソース参照先を修正する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
13		T.VA_Time_Source1.2				脆弱性（e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
14		T.VA_System_Clock_Inaccuracy	日本標準時と大きくずれたシステム時刻になる	時計品質のため、あるいは、温度環境が劣悪なため時刻がずれる			
15		T.VA_Time_Source_Unavailable	日本標準時と大きくずれたシステム時刻になる	時刻ソースが参照できないため時刻がずれる	時刻ソース参照先のマシン、あるいは、通信路に障害が発生する		
16	検証サーバ設定データ	T.VA_Mod_ConfigData_Undetec	運用者が設定項目の値を間違え、VA サービスの動作が正常ではなくなる	TOE の下位抽象マシンに備わったファイル操作機能で設定内容を変更する	不注意で作業する		

17		T.VA_Crack_Mod_ConfigData1.1	悪意者が、設定情報内容を改ざんする	TOE の下位抽象マシンに備わったファイル操作機能で設定内容を変更する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
18		T.VA_Crack_Mod_ConfigData1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
19		T.VA_Crack_Disclose_ConfigData1.1	悪意者が、設定情報内容を外部に暴露する	TOE に備わるファイル操作機能を用いて設定情報を閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
20		T.VA_Crack_Disclose_ConfigData1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
21	検証記録データ	T.VA_Mod_ValidationRecord_Undetect	運用者が、検証記録を改ざんする	TOE の下位抽象マシンに備わったファイル操作機能を用いて検証記録を修正、あるいは、削除する	不注意で作業する		
22		T.VA_Crack_Mod_ValidationRecord1.1	悪意者が、検証記録を改ざんする	TOE の下位抽象マシンに備わったファイル操作機能を用いて検証記録を修正、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
23		T.VA_Crack_Mod_ValidationRecord1.2				脆弱性(e.g. バッファオーバフローなど) を利用し、ネットワーク攻撃する	
24		T.VA_Crack_Disclose_ValidationRecord1.1	悪意者が、検証記録を外部に暴露する	TOE に備わるファイル操作機能を用いて検証記録を閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する

25		T.VA_Crack_Disclose_ValidationRecord1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
26	署名履歴データ	T.VA_Mod_SignatureHistory_Undetect	運用者が、署名履歴を改ざんする	TOE の下位抽象マシンに備わったファイル操作機能を用いて署名履歴を修正、あるいは、削除する	不注意で作業する		
27		T.VA_Crack_Mod_SignatureHistory1.1	悪意者が、署名履歴を改ざんする	TOE の下位抽象マシンに備わったファイル操作機能を用いて署名履歴を修正、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
28		T.VA_Crack_Mod_SignatureHistory1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
29		T.VA_Crack_Disclose_SignatureHistory1.1	悪意者が、署名履歴を暴露する	TOE に備わるファイル操作機能を用いて署名履歴を閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
30		T.VA_Crack_Disclose_SignatureHistory1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
31		T.VA_DVC_SigHistory_Compromise	計算機能力の向上 暗号解読技術の向上				
32	トラストアンカ公開鍵証明書	T.VA_Mod_TrustAnchor_Undetect	運用者が、トラストアンカを取り替える、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いてトラストアンカを取り替える、あるいは、削除する	不注意で作業する		

33		T.VA_Crack_Mod_TrustAnchor1.1	悪意者が、トラストアンカを取り替える、修正する、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いてトラストアンカを取替る、修正する、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
34		T.VA_Crack_Mod_TrustAnchor1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
35	検証サーバの効果鍵証明書	T.VA_Mod_VA-PKC_Undetect	運用者が、検証サーバの公開鍵証明書を取り替える、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いて検証サーバの公開鍵証明書を取り替える、あるいは、削除する	不注意で作業する		
36		T.VA_Crack_Mod_VA-PKC1.1	悪意者が、検証サーバの公開鍵証明書を取り替える、修正する、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いて検証サーバの公開鍵証明書を取り替える、修正する、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
37		T.VA_Crack_Mod_VA-PKC1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
38	DVC、署名向けの私有鍵データ	T.VA_Mod_PrivateKeys-Sig_Undetect	管理者が、検証サーバの私有鍵を取り替える、あるいは、削除する	TOE の下位抽象マシンに備わった鍵操作機能を用いて検証サーバの私有鍵を取り替える、あるいは、削除する	不注意で作業する		
39		T.VA_Crack_Mod_PrivateKeys-Sig1.1	悪意者が、検証サーバの私有鍵を取り替える、修正する、あるいは、削除する	TOE の下位抽象マシンに備わった鍵操作機能を用いて検証サーバの私有鍵を取り替える、修正する、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する

40		T.VA_Crack_Mod_PrivateKeys-Sig1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
41		T.VA_Crack_Disclose_PrivateKeys-Sig1.1	悪意者が、検証サーバの私有鍵を漏洩する	TOE の下位抽象マシンに備わった鍵操作機能を用いて検証サーバの私有鍵を閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
42		T.VA_Crack_Disclose_PrivateKeys-Sig1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
43	SSL サーバ向けの私有鍵データ	T.VA_Mod_PrivateKey-SSL_Undetect	管理者が、SSL サーバの私有鍵を取り替える、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いて SSL サーバの私有鍵を取り替える、あるいは、削除する	不注意で作業する		
44		T.VA_Crack_Mod_PrivateKey-SSL1.1	悪意者が、SSL サーバの私有鍵を取り替える、修正する、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いて SSL サーバの私有鍵を取り替える、修正する、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
45		T.VA_Crack_Mod_PrivateKey-SSL1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
46		T.VA_Crack_Disclose_PrivateKey-SSL1.1	悪意者が、SSL サーバの私有鍵を漏洩する	TOE に備わるファイル操作機能を用いて SSL サーバの私有鍵を閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する

47		T.VA_Crack_Disclose_PrivateKey-SSL1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
48	ログデータ	T.VA_Mod_Log_Undetect	運用者が、ログを修正、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いてログを修正、あるいは、削除する	不注意で作業する		
49		T.VA_Crack_Mod_Log1.1	悪意者が、ログを修正、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いてログを修正、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
50		T.VA_Crack_Mod_Log1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
51		T.VA_Crack_Disclose_Log1.1	検証者が、ログを漏洩する	TOE に備わるファイル操作機能を用いてログを閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
52		T.VA_Crack_Disclose_Log1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
53	ユーザ識別情報とユーザ認証データ	T.VA_Crack_Mod_UserID_AuthenticationData1.1	悪意者が、ユーザ識別情報とパスワードを修正、あるいは削除する	TOE の下位抽象マシンに備わったユーザアカウント管理機能を用いてユーザ識別情報とパスワードを修正、あるいは削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
54		T.VA_Crack_Mod_UserID_AuthenticationData1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	

55		T.VA_Crack_Disclose_UserID_AuthenticationData1.1	悪意者が、ユーザ識別情報とパスワードを漏洩する	TOE に備わるファイル操作機能を用いてユーザ識別情報を閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
56		T.VA_Crack_Disclose_UserID_AuthenticationData1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
57	TSA1 アクセス用 ID と認証データ	T.VA_Mod_TSA1AccessInfo_Undetect	運用者が、TSA1 アクセス用 ID とパスワードを変更する	TOE の下位抽象マシンに備わったファイル操作機能で TSA1 アクセス用 ID とパスワードを変更する	不注意で作業する		
58		T.VA_Crack_Mod_TSA1AccessInfo1.1	悪意者が、TSA1 アクセス用 ID とパスワードを変更する	TOE の下位抽象マシンに備わったファイル操作機能で TSA1 アクセス用 ID とパスワードを変更する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
59		T.VA_Crack_Mod_TSA1AccessInfo1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
60		T.VA_Crack_Disclose_TSA1AccessInfo1.1	悪意者が、TSA1 アクセス用 ID とパスワードを漏洩する	TOE に備わる端末を操作してアクセス用 ID とパスワードを閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
61		T.VA_Crack_Disclose_TSA1AccessInfo1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
62	HSM アクセス用パスワード	T.VA_Mod_HSMAccessInfo_Undetect	運用者が、HSM アクセス用 ID とパスワードを変更する	TOE の下位抽象マシンに備わったファイル操作機能で HSM アクセス用 ID とパスワードを変更する	不注意で作業する		

63		T.VA_Crack_Mod_HSMAccessInfo1.1	悪意者が、HSM アクセス用 ID とパスワードを変更する	TOE の下位抽象マシンに備わったファイル操作機能で HSM アクセス用 ID とパスワードを変更する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
64		T.VA_Crack_Mod_HSMAccessInfo1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
65		T.VA_Crack_Disclose_HSMAccessInfo1.1	検証者が、HSM アクセス用 ID とパスワードを漏洩する	TOE に備わる端末を操作してアクセス用 ID とパスワードを閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
66		T.VA_Crack_Disclose_HSMAccessInfo1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
67	検証サーバ制御ツール	T.VA_Mod_VA-Tool_Undetect	運用者が、検証サーバ制御ツールを修正、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能を用いて検証サーバ制御ツールを修正、あるいは、削除する	不注意で作業する		
68		T.VA_Crack_Mod_VA-Mgmt-Tool1.1	悪意者が、検証サーバ制御ツールを修正、あるいは、削除する	TOE の下位抽象マシンに備わったファイル操作機能で検証サーバ制御ツールを修正、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
69		T.VA_Crack_Mod_VA-Mgmt-Tool1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
70		T.VA_Crack_Disclose_VA-Mgmt-Tool1.1	悪意者が、検証サーバ制御ツールを情報漏洩する	TOE に備わる端末を操作して検証サーバ制御ツールを閲覧、あるいは、持ち込まれた USB メモリに格納する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する

71		T.VA_Crack_Disclose_VA-Mgmt-Tool1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
72	検証サーバ	T.VA_Crack_Mod_VA-Process1.1	悪意者が、検証サーバプログラムを修正、あるいは、削除する	TOE の下位抽象マシンに備わったファイルし操作機能で検証サーバプログラムを修正、あるいは、削除する	管理者権限を得る	TOE に物理的にアクセスする	TOE 設置部屋に侵入する
73		T.VA_Crack_Mod_VA-Process1.2				脆弱性(e.g. BufferOverflow など)を利用し、ネットワーク攻撃する	
74		T.VA_DoS_Attack	悪意者が、検証サーバプログラムに DoS 攻撃をしかけ、検証サービスを停止させる	DoS ツールを利用して、ネットワークを介して DoS 攻撃を実行する			
75		T.VA_BufferOverFlow_Attack	悪意者が、検証サーバプログラムに BufferOverflow 攻撃をしかけ、検証サーバを乗っ取る	殆ど知られていない脆弱性を用いて、ネットワークを介して BufferOverflow 攻撃を実行する			
76		T.VA_Crack_Imperson_TOE	悪意者が、TOE に成りすまし、検証者に偽の検証サービスを提供する	検証者と TOE の通信間に割り込み、TOE に成りすます			
77		T.VA_TOE_Bug	検証サーバのプログラム不良により、情報資産の信頼性が失われる	開発プロセス時にバグの要因が含まれる			
78	その他	T.VA_Hack_Imperson_TSA2	悪意者が、TOE と TSA2 の通信間に割り込み、TSA2 に成りすます				
79		T.VA_Hardware_Failure	消耗や劣化のため、ハードウェアが故障する				
80		T.VA_Peer_Failure	他システムの想定外のシステムダウンが継続する				
81		T.VA_Connection_Failure	他システム間との通信回線が消耗や劣化のため故障する				
82		T.VA_Cracker_Repudiation	検証者や外部者が、不正行為を否認する				

2. リスク評価格付けの考え方

リスク評価格付けの基本的な考え方を以下に示す。DREAD 分類において、複数の視点が存在し、それぞれの評価の点が異なる場合は、一番リスクの高い評価点に合わせることとする。

リスク格付けの考え方の記述例

#	DREAD 分類	視点	高(3)	中(2)	低(1)
1	Damage potential（潜在的損失）	サービス継続性	異常なサービス提供	異常なサービス提供をすることはないが、正常なサービス継続不可能	正常なサービス継続可能
		資産の流出		機密情報が漏洩する	重要情報が漏洩する
		資産の信頼性		機密情報の改ざん、偽造、消去	重要情報の改ざん、偽造、消去
2	Reproducibility（再現性）	攻撃時間帯	任意の時間に脅威が発生	ある時間帯のみ脅威が発生	ある限られた条件において脅威が発生
		脅威エージェント	悪意を持った内部者	外部者、あるいは利用者 自然（ある程度予知可能な要因による脅威発生）	不注意な内部者 自然や偶然（予知不可能な要因による脅威発生）
3	Exploitability（攻撃利用可能性）	脅威エージェント	悪意を持った内部者	外部者、あるいは利用者	不注意な内部者、あるいは、自然や偶然（予知不可能な要因による脅威発生）
		脅威エージェントが使用する攻撃ツールの入手・使用の容易性	TOE、あるいは、TOE の下位抽象マシンなどに標準的に備わる機能を直接利用	TOE、あるいは、TOE の下位抽象マシンに比較的入手可能な攻撃用のツールを導入要	TOE、あるいは、TOE の下位抽象マシンに攻撃者が新規に作成した独自の攻撃用ツールが必要
4	Affected users（影響ユーザ）	影響を受ける利用者の範囲	全ての利用者に影響が出る	一部の利用者に影響が出る	ごく少数の利用者に影響が出る 管理者/運用者/監査者の業務に影響が出る
5	Discoverability（発見可能性）	攻撃方法の公知性	脅威エージェントが外部者、あるいは、利用者である場合、攻撃方法は公知である 脅威エージェントが内部者（悪意）の場合、正規の運用方	脅威エージェントが外部者、あるいは、利用者である場合、攻撃方法は、少数のユーザに知られている 脅威エージェントが内部者（悪意）であ	脅威エージェントが外部者、あるいは、利用者である場合、攻撃方法は、ほとんど未知である 脅威エージェントが内部者（不注意）で

			法で攻撃可能である。	る場合、攻撃を行う際、正規の運用方法以外の手法も用いる必要がある	ある場合、正規の運用方法で脅威が発生する

3. リスク評価点

前述したリスク評価格付けの考え方に基づき、リスク評価を行った結果を以下に示す。

リスク評価点の記述例

#	脅威	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.VA_DVC_Crypto_Compromise1	3	1	2	1	2	9
2	T.VA_Crack_Mod_TimeStampInfo	3	1	2	1	2	9
3	T.VA_Crack_Disclose_TimeStampInfo	3	1	2	1	2	9
4	T.VA_Crack_Mod_DVC	1	1	2	1	2	7
5	T.VA_Crack_Disclose_DVC	1	1	2	1	2	7
6	T.VA_DVC_Crypto_Compromise2	3	1	1	3	1	9
7	T.VA_DVC_Crypto_Compromise3.1	1	1	1	3	1	7
8	T.VA_DVC_Crypto_Compromise3.2	1	1	1	3	1	7
9	T.VA_DVC_Crypto_Compromise3.3	1	1	1	3	1	7
10	T.VA_System_Clock_Modify1.1	3	1	2	3	1	10
11	T.VA_System_Clock_Modify1.2	3	1	2	3	1	10
12	T.VA_Time_Source1.1	3	1	2	3	1	10
13	T.VA_Time_Source1.2	3	1	2	3	1	10
14	T.VA_System_Clock_Inaccuracy	3	1	1	3	1	9
15	T.VA_Time_Source_Unavailable	3	1	1	3	1	9
16	T.VA_Mod_ConfigData_Undetec	3	1	1	3	1	9
17	T.VA_Crack_Mod_ConfigData1.1	3	1	2	3	1	10
18	T.VA_Crack_Mod_ConfigData1.2	3	1	2	3	1	10
19	T.VA_Crack_Disclose_ConfigData1.1	2	1	2	3	1	9
20	T.VA_Crack_Disclose_ConfigData1.2	2	1	2	3	1	9
21	T.VA_Mod_ValidationRecord_Undetect	3	1	1	2	1	8
22	T.VA_Crack_Mod_ValidationRecord1.1	3	1	2	2	1	9
23	T.VA_Crack_Mod_ValidationRecord1.2	3	1	2	2	1	9
24	T.VA_Crack_Disclose_ValidationRecord1.1	2	1	2	2	1	8
25	T.VA_Crack_Disclose_ValidationRecord1.2	2	1	2	2	1	8
26	T.VA_Mod_SignatureHistory_Undetect	3	1	2	2	1	9
27	T.VA_Crack_Mod_SignatureHistory1.1	3	2	2	2	1	10
28	T.VA_Crack_Mod_SignatureHistory1.2	3	2	2	2	1	10
29	T.VA_Crack_Disclose_SignatureHistory1.1	2	2	2	1	1	8
30	T.VA_Crack_Disclose_SignatureHistory1.2	2	2	2	1	1	8
31	T.VA_DVC_SigHistory_Compromise	1	1	1	2	1	6
32	T.VA_Mod_TrustAnchor_Undetect	3	1	1	3	1	9
33	T.VA_Crack_Mod_TrustAnchor1.1	3	1	2	3	1	10
34	T.VA_Crack_Mod_TrustAnchor1.2	3	1	2	3	1	10
35	T.VA_Mod_VA-PKC_Undetect	3	1	1	3	1	9
36	T.VA_Crack_Mod_VA-PKC1.1	3	1	2	3	1	10
37	T.VA_Crack_Mod_VA-PKC1.2	3	1	2	3	1	10

38	T.VA_Mod_PrivateKeys-Sig_Undetect	3	1	1	3	1	9
39	T.VA_Crack_Mod_PrivateKeys-Sig1.1	3	2	2	3	1	11
40	T.VA_Crack_Mod_PrivateKeys-Sig1.2	3	2	2	3	1	11
41	T.VA_Crack_Disclose_PrivateKeys-Sig1.1	3	2	2	3	1	11
42	T.VA_Crack_Disclose_PrivateKeys-Sig1.2	3	2	2	3	1	11
43	T.VA_Mod_PrivateKey-SSL_Undetect	3	1	1	3	1	9
44	T.VA_Crack_Mod_PrivateKey-SSL1.1	3	2	2	3	1	11
45	T.VA_Crack_Mod_PrivateKey-SSL1.2	3	2	2	3	1	11
46	T.VA_Crack_Disclose_PrivateKey-SSL1.1	3	2	2	3	1	11
47	T.VA_Crack_Disclose_PrivateKey-SSL1.2	3	2	2	3	1	11
48	T.VA_Mod_Log_Undetect	1	2	2	1	1	7
49	T.VA_Crack_Mod_Log1.1	1	2	2	1	1	7
50	T.VA_Crack_Mod_Log1.2	1	2	2	1	1	7
51	T.VA_Crack_Disclose_Log1.1	1	2	2	1	1	7
52	T.VA_Crack_Disclose_Log1.2	1	2	2	1	1	7
53	T.VA_Crack_Mod_UserID_AuthenticationData1.1	2	2	2	3	1	10
54	T.VA_Crack_Mod_UserID_AuthenticationData1.2	2	2	2	3	1	10
55	T.VA_Crack_Disclose_UserID_AuthenticationData1.1	2	2	2	3	1	10
56	T.VA_Crack_Disclose_UserID_AuthenticationData1.2	2	2	2	3	1	10
57	T.VA_Mod_TSA1AccessInfo_Undetect	3	1	1	3	1	9
58	T.VA_Crack_Mod_TSA1AccessInfo1.1	3	2	2	3	1	11
59	T.VA_Crack_Mod_TSA1AccessInfo1.2	3	2	2	3	1	11
60	T.VA_Crack_Disclose_TSA1AccessInfo1.1	2	2	2	1	1	8
61	T.VA_Crack_Disclose_TSA1AccessInfo1.2	2	2	2	1	1	8
62	T.VA_Mod_HSMAccessInfo_Undetect	3	1	1	3	1	9
63	T.VA_Crack_Mod_HSMAccessInfo1.1	3	2	2	3	1	11
64	T.VA_Crack_Mod_HSMAccessInfo1.2	3	2	2	3	1	11
65	T.VA_Crack_Disclose_HSMAccessInfo1.1	2	2	2	1	1	8
66	T.VA_Crack_Disclose_HSMAccessInfo1.2	2	2	2	1	1	8
67	T.VA_Mod_VA-Tool_Undetect	1	1	1	1	1	5
68	T.VA_Crack_Mod_VA-Mgmt-Tool1.1	3	2	2	3	1	11
69	T.VA_Crack_Mod_VA-Mgmt-Tool1.2	3	2	2	3	1	11
70	T.VA_Crack_Disclose_VA-Mgmt-Tool1.1	1	2	2	1	1	7
71	T.VA_Crack_Disclose_VA-Mgmt-Tool1.2	1	2	2	1	1	7
72	T.VA_Crack_Mod_VA-Process1.1	3	2	2	3	1	11
73	T.VA_Crack_Mod_VA-Process1.2	3	2	2	3	1	11
74	T.VA_DoS_Attack	2	3	2	3	3	13
75	T.VA_BufferOverFlow_Attack	3	3	2	3	3	14
76	T.VA_Crack_Imperson_TOE	3	2	2	3	1	11
77	T.VA_TOE_Bug	3	1	1	3	1	9
78	T.VA_Hack_Imperson_TSA2	3	2	2	3	3	13
79	T.VA_Hardware_Failure	3	1	1	3	1	9
80	T.VA_Peer_Failure	3	1	1	3	1	9
81	T.VA_Connection_Failure	3	1	1	3	1	9
82	T.VA_Cracker_Repudiation	1	2	2	1	3	9

第5章 内部不正を考慮したセキュリティ評価

内部不正の考え方及び内部不正を考慮したセキュリティ環境を記述する。さらに、脅威に関する対策を記す。

1. 内部不正の考え方

内部不正の考え方は、以下の通りである。

- 不正は単独で行われる
- 複数の内部者による結託は無い
- 内部者と外部者が連携した不正行為は無い

2. 内部不正を考慮したセキュリティ環境

内部者が単独で行う不正行為を考慮したセキュリティ環境を記述する。

2-1 前提

内部不正を考慮しない前提（表 2-1）と異なる項目のみを以下に記載する。人的な前提と接続的な前提の一部が異なっている。異なる部分を太字かつ、斜体で示す。

表 5-1：内部不正を考慮した前提（内部不正を考慮しない前提との差異）

#	分類	項目	説明
1	人的	A.VA_Administrator	一つ以上の許可された管理者が割り当てられる。彼らは、TOE と TOE に含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOE を安全に導入、管理する。 • TOE に関わるユーザ/役割を管理する • 暗号機能に関わる初期化及び管理業務を行う • TOE 上で悪意のあるソフトウェアが動作しないようにする • TOE の要件を満たす適切なディスクスペースを用意する • TOE のデータベースを適切に管理する ***さらに彼らは、権限を濫用し、故意にセキュリティを低める可能性は存在する（単独による不正のみ）。***
2	人的	A.VA_Operator	一人以上の許可された運用者が割り当てられる。 • TOE の起動･停止を実行する • TOE 管理者の指示の元で各種設定など運用業務を行う ***さらに彼らは、権限を濫用し、故意にセキュリティを低める可能性は存在する（単独による不正のみ）。***
3	人的	A.VA_Auditor	一人以上の許可された監査者が割り当てられる。

			• TOE に関するログを取得し、分析を行う ***さらに彼らは、権限を濫用し、故意にセキュリティを低める可能性は存在する（単独による不正のみ）。***
4	接続	A.VA_Abstract	TOE が動作するために必要な OS（システムクロックを除く）や依存するライブラリは、不正な改変から保護され、正しく動作する。 ***ただし、内部不正者による不正な改変の可能性は残る。***
5	接続	A.VA_Separation	TOE が動作するマシンには、TOE の動作に必要なソフトウェア以外はインストールされないものとする。 ***ただし、内部不正者による不正なソフトウェア導入の可能性は残る。***

2-2 脅威

内部不正を考慮した脅威は、以下の通りである。資産毎の脅威を具体化している。なお、内部不正を考慮しない脅威（表 2-2）は、含めていない。

表 5-2：内部不正を考慮した脅威（内部不正を考慮しない脅威は含まず）

#	項目	説明
1	T.VA_Internal_Crack_Mod_TimeStampInfo	管理者、あるいは、運用者が、不正なプログラム（例：検証プログラムへの入力に対するフッキングプログラム）を導入し、受信直後のタイムスタンプ情報を改ざんする。
2	T.VA_Internal_Crack_Disclose_TimeStampInfo	管理者、あるいは、運用者が、不正なプログラム（例：検証プログラムへの入力に対するフッキングプログラム）を導入し、受信直後のタイムスタンプ情報を取得する。その情報を閲覧する。また、USB メモリなどの外部デバイスに出力する。
3	T.VA_Auditor_Crack_Mod_TimeStampInfo	監査者が、管理者権限を不正に入手する。その後、不正なプログラム（例：検証プログラムへの入力に対するフッキングプログラム）を導入し、受信直後のタイムスタンプ情報を改ざんする。
4	T.VA_Auditor_Crack_Disclose_TimeStampInfo	監査者が、管理者権限を不正に入手する。その後、不正なプログラム（例：検証プログラムへの入力に対するフッキングプログラム）を導入し、受信直後のタイムスタンプ情報を取得する。その情報を閲覧する。また、USB メモリなどの外部デバイスに出力する。
5	T.VA_Internal_Crack_Mod_DVC	管理者、あるいは、運用者が、不正なプログラムを導入し、検証サーバ内で送信直前の DVC（検証結果）を改ざんする。
6	T.VA_Internal_Crack_Disclose_DVC	管理者、あるいは、運用者が、不正なプログラムを導入し、検証サーバ内で送信直前の DVC（検証結果）を取得する。その情報を閲覧する。また、USB メモリなどの外部デバイスに出力する。
7	T.VA_Auditor_Crack_Mod_DVC	監査者が、管理者権限を不正に入手する。その後、正なプログラムを導入し、検証サーバ内で送信直前の DVC（検証結果）を改ざんする。
8	T.VA_Auditor_Crack_Disclose_DVC	監査者が、管理者権限を不正に入手する。その後、不正なプログラムを導入し、検証サーバ内で送信直前の DVC（検証結果）を取得する。その情報を閲覧する。また、USB メモリなどの外部デバイスに出力する。
9	T.VA_Internal_Crack_System_Clock	管理者、あるいは、運用者が、システム時計の設定コマンドや不正なプログラムを用いて、システム時計を変更する。
10	T.VA_Internal_Crack_Time_Source	管理者、あるいは、運用者が、エディタを用いて、時刻ソースの設定内容を改ざんする。また、不正なプログラムを用いて時刻ソースの設定内容を改ざんする。
11	T.VA_Auditor_Crack_System_Clock	監査者が、管理者権限を不正に入手する。その後、システム時計の設定コマンドや不正なプログラムを用いて、システム時計を変更する。

12	T.VA_Auditor_Crack_Time_Source	監査者が、管理者権限を不正に入手する。その後、エディタを用いて、時刻ソースの設定内容を改ざんする。また、不正なプログラムを用いて時刻ソースの設定内容を改ざんする。
13	T.VA_Internal_Crack_Mod_ConfigData	管理者、あるいは、運用者が、エディタを用いて、検証サーバの設定情報を改ざんする。
14	T.VA_Internal_Crack_Disclose_VA-ConfigData	管理者、あるいは、運用者が、検証サーバの設定情報を漏洩する。
15	T.VA_Auditor_Crack_Mod_ConfigData	監査者が、管理者権限を不正に入手する。その後、エディタを用いて、検証サーバの設定情報を改ざんする。
16	T.VA_Auditor_Crack_Disclose_VA-ConfigData	監査者が、管理者権限を不正に入手する。その後、検証サーバの設定情報を漏洩する。
17	T.VA_Internal_Crack_ValidationRecord	管理者、あるいは、運用者が、エディタを用いて、検証記録の内容を改ざんする。
18	T.VA_Internal_Crack_Disclose_ValidationRecords	管理者、あるいは、運用者が、検証記録の内容を漏洩する。
19	T.VA_Auditor_Crack_ValidationRecord	監査者が、管理者権限を不正に入手する。その後、エディタを用いて、検証記録の内容を改ざんする。
20	T.VA_Auditor_Crack_Disclose_ValidationRecords	監査者が、管理者権限を不正に入手する。その後、検証記録の内容を漏洩する。
21	T.VA_Internal_Crack_SignatureHistory	管理者、あるいは、運用者が、エディタを用いて、署名履歴の内容を改ざんする。
22	T.VA_Internal_Crack_Disclose_SignatureHistory	管理者、あるいは、運用者が、署名履歴の内容を漏洩する。
23	T.VA_Auditor_Crack_SignatureHistory	監査者が、管理者権限を不正に入手する。その後、エディタを用いて、署名履歴の内容を改ざんする。
24	T.VA_Auditor_Crack_Disclose_SignatureHistory	監査者が、管理者権限を不正に入手する。その後、署名履歴の内容を漏洩する。
25	T.VA_Internal_Crack_TrustAnchor	管理者、あるいは、運用者が、ファイル操作機能、あるいは、エディタを用いて、トラストアンカ証明書を入れ替える、あるいは、内容を改ざん･削除する。
26	T.VA_Auditor_Crack_TrustAnchor	監査者が、管理者権限を不正に入手する。その後、ファイル操作機能、あるいは、エディタを用いて、トラストアンカ証明書を入れ替える、あるいは、内容を改ざん･削除する。
27	T.VA_Internal_Crack_VA-PKC	管理者、あるいは、運用者が、ファイル操作機能、あるいは、エディタを用いて、検証サーバの公開鍵証明書を入れ替える、あるいは、内容を改ざん･削除する。
28	T.VA_Auditor_Crack_VA-PKC	監査者が、管理者権限を不正に入手する。その後、ファイル操作機能、あるいは、エディタを用いて、検証サーバの公開鍵証明書を入れ替える、あるいは、内容を改ざん･削除する。
29	T.VA_Internal_Crack_PrivateKeys-Sig	管理者、あるいは、運用者が、鍵操作機能を用いて、検証サーバの署名用私有鍵を入れ替える、あるいは、改ざん･削除する。
30	T.VA_Internal_Crack_Disclose_PrivateKeys-Sig	管理者、あるいは、運用者が、検証サーバの署名用私有鍵を漏洩する。
31	T.VA_Auditor_Crack_PrivateKeys-Sig	監査者が、管理者権限を不正に入手する。その後、鍵操作機能を用いて、検証サーバの署名用私有鍵を入れ替える、あるいは、改ざん･削除する。
32	T.VA_Auditor_Crack_Disclose_PrivateKey-Sig	監査者が、管理者権限を不正に入手する。その後、検証サーバの署名用私有鍵を漏洩する。
33	T.VA_Internal_Crack_PrivateKey-SSL	管理者、あるいは、運用者が、ファイル操作機能を用いて、SSL サーバ用の私有鍵を入れ替える、あるいは、改ざん･削除する。
34	T.VA_Internal_Crack_Disclose_PrivateKey-SSL	管理者、あるいは、運用者が、SSL サーバ用の私有鍵を漏洩する。
35	T.VA_Auditor_Crack_PrivateKey-SSL	監査者が、管理者権限を不正に入手する。その後、ファイル操作機能を用いて、SSL サーバ用の私有鍵を入れ替える、あるいは、改ざん･削除する。
36	T.VA_Auditor_Crack_Disclose_PrivateKey-SSL	監査者が、管理者権限を不正に入手する。その後、SSL サーバ用の私有鍵を漏洩する。
37	T.VA_Internal_Crack_Log	管理者、あるいは、運用者が、ファイル操作機能を用いて、ログデータを改ざん･削除する。
38	T.VA_Internal_Crack_Disclose_Log	管理者、あるいは、運用者が、ログデータを漏洩する。
39	T.VA_Auditor_Crack_Log	監査者が、管理者権限を不正に入手する。その後、ファイル操作機能を用いて、ログデータを改ざん･削除する。

40	T.VA_Auditor_Crack_Disclose_Log	監査者が、管理者権限を不正に入手する。その後、ログデータを漏洩する。
41	T.VA_Internal_Crack_Disclose_UserID-AuthenticationData	管理者、あるいは、運用者が、ユーザ（管理者、あるいは、運用者）のパスワードを漏洩する。
42	T.VA_Auditor_Crack_Disclose_UserID-AuthenticationData	監査者が、管理者権限を不正に入手する。その後、ユーザ（管理者、あるいは、運用者）のパスワードを漏洩する。
43	T.VA_Internal_Crack_Disclose_TSA1AccessInfo	管理者、あるいは、運用者が、TSA1アクセス用IDとパスワードを漏洩する。
44	T.VA_Auditor_Crack_Disclose_TSA1AccessInfo	監査者が、管理者権限を不正に入手する。その後、TSA1 アクセス用 ID とパスワードを漏洩する。
45	T.VA_Internal_Crack_Disclose_HSMAccessInfo	管理者、あるいは、運用者が、HSM アクセス用 ID とパスワードを漏洩する。
46	T.VA_Auditor_Crack_Disclose_HSMAccessInfo	監査者が、管理者権限を不正に入手する。その後、HSM アクセス用 ID とパスワードを漏洩する。
47	T.VA_Internal_Crack_Mod_VA-Mgmt-Tool	管理者、あるいは、運用者が、ファイル操作機能を用いて、検証サーバのツール（スクリプトファイル）を改ざんする。
48	T.VA_Internal_Crack_Disclose_VA-Mgmt-Tool	管理者、あるいは、運用者が、検証サーバのツール（スクリプトファイル）を漏洩する。
49	T.VA_Auditor_Crack_Mod_VA-Mgmt-Tool	監査者が、管理者権限を不正に入手する。その後、ファイル操作機能を用いて、検証サーバのツール（スクリプトファイル）を改ざんする。
50	T.VA_Auditor_Crack_Disclose_VA-Mgmt-Tool	監査者が、管理者権限を不正に入手する。その後、検証サーバのツール（スクリプトファイル）を漏洩する。
51	T.VA_Internal_Crack_Mod_VA-Process	管理者、あるいは、運用者が、検証サーバのプログラムを入れ替える、あるいは、削除する。
52	T.VA_Internal_Crack_Disclose_VA-Process	管理者、あるいは、運用者が、検証サーバのプログラムを漏洩する。
53	T.VA_Internal_DoS_Attack	管理者、あるいは、運用者が、不正なプログラムを導入し、TOE のリソースを大量に消費させる。
54	T.VA_Auditor_Crack_Mod_VA-Process	監査者が、管理者権限を不正に入手する。その後、検証サーバのプログラムを入れ替える、あるいは、削除する。
55	T.VA_Auditor_Crack_Disclose_VA-Process	監査者が、管理者権限を不正に入手する。その後、検証サーバのプログラムを漏洩する。
56	T.VA_Auditor_DoS_Attack	監査者が、管理者権限を不正に入手する。その後、不正なプログラムを導入し、TOE のリソースを大量に消費させる。
57	T.VA_Internal_Repudiation	管理者、運用者、あるいは、監査者が、不正行為を否認する。

2-3 組織のセキュリティポリシー

組織のセキュリティポリシーは、内部不正者の有無に関わらず、組織として採用する方針となる。そのため、内部不正を考慮しないもの（表 2-3）と同一であるとする。

表 5-3：内部不正を考慮した組織のセキュリティポリシー

#	項目	説明
1	P.VA_Time_Source	TOE は、信頼のできる時刻ソースを参照すること。この時刻ソースは、TOE 所有者にとってアベイラブルであること。また、時刻ソースの信頼性と正確性は TOE 所有者にとって受容可能であること。
2	P.VA_System_Clock_Management	TOE が参照するシステム時計を信頼のできる時刻ソースと同期させる。
3	P. VA_HSM	TOE を使用する組織は、FIPS 140-2 level3 相当の機能を持つ HSM により、物理的に保護された検証サーバの私有鍵を利用した、検証結果や検証記録に対する暗号操作及び私有鍵のライフサイクル管理を行うこととする。
4	P. VA_PKI_Management	安全に管理された PKI の中で、TOE を運用すること。

		全ての鍵と証明書は、安全に発行、失効される。 全ての鍵と証明書の状態は、使用前にチェックされる。
5	P. VA_Cryptography	全ての暗号処理（署名と検証等）は、「電子政府推奨暗号リスト（平成15年2月20日、総務省、経済産業省）」に記載されたアルゴリズムによって実装されなければならない。
6	P.VA_Password_Management	TOE 利用者のパスワードは、TOE 利用者本人によって適切に管理され、本人以外に知られてはならない。
7	P.VA_Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄、または削除の防止のために必要な措置をとることとする。
8	P.VA_Dual_Control	TOE の管理業務における重要な操作は、複数の TOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
9	P.VA_Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。
10	P.VA_Check_Virus	最新のウィルスチェックソフトを用いて、定期的なウィルスチェックを実行する。
11	P.VA_Check_Received_Data	他サブシステムから送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。

3. 脅威に対するセキュリティ目標・対策

内部不正を考慮した脅威に対するセキュリティ目標・対策を以下に示す。なお、内部不正を考慮しない脅威（表 2-2）との差異のみを記述する。

表 5-4：内部不正を考慮した脅威に対するセキュリティ目標・対策

#	脅威名	セキュリティ目標・対策	
1	T.VA_Internal_Crack_Mod_TimeStampInfo	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
2	T.VA_Internal_Crack_Disclose_TimeStampInfo	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
3	T.VA_Auditor_Crack_Mod_TimeStampInfo	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
4	T.VA_Auditor_Crack_Disclose_TimeStampInfo	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
5	T.VA_Internal_Crack_Mod_DVC	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視

		回復	-
6	T.VA_Internal_Crack_Disclose_DVC	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
7	T.VA_Auditor_Crack_Mod_DVC	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
8	T.VA_Auditor_Crack_Disclose_DVC	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
9	T.VA_Internal_Crack_System_Clock	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	時刻源(NTP サーバ)と時刻同期させる。
10	T.VA_Internal_Crack_Time_Source	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	時刻源(NTP サーバ)が含まれた設定情報のバックアップ/リストア後、時刻源(NTP サーバ)と時刻同期させる。
11	T.VA_Auditor_Crack_System_Clock	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	時刻源(NTP サーバ)と時刻同期させる。
12	T.VA_Auditor_Crack_Time_Source	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	時刻源(NTP サーバ)が含まれた設定情報のバックアップ/リストア後、時刻源(NTP サーバ)と時刻同期させる。
13	T.VA_Internal_Crack_Mod_ConfigData	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
14	T.VA_Internal_Crack_Disclose_VA-ConfigData	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
15	T.VA_Auditor_Crack_Mod_ConfigData	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
16	T.VA_Auditor_Crack_Disclose_VA-ConfigData	防止	管理者権限パスワード管理 罰則規定の強化

		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
17	T.VA_Internal_Crack_ValidationRecord	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
18	T.VA_Internal_Crack_Disclose_ValidationRecords	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
19	T.VA_Auditor_Crack_ValidationRecord	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
20	T.VA_Auditor_Crack_Disclose_ValidationRecords	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
21	T.VA_Internal_Crack_SignatureHistory	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
22	T.VA_Internal_Crack_Disclose_SignatureHistory	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
23	T.VA_Auditor_Crack_SignatureHistory	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
24	T.VA_Auditor_Crack_Disclose_SignatureHistory	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
25	T.VA_Internal_Crack_TrustAnchor	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
26	T.VA_Auditor_Crack_TrustAnchor	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
27	T.VA_Internal_Crack_VA-PKC	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア

28	T.VA_Auditor_Crack_VA-PKC	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
29	T.VA_Internal_Crack_PrivateKeys-Sig	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
30	T.VA_Internal_Crack_Disclose_PrivateKeys-Sig	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
31	T.VA_Auditor_Crack_PrivateKeys-Sig	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
32	T.VA_Auditor_Crack_Disclose_PrivateKey-Sig	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
33	T.VA_Internal_Crack_PrivateKey-SSL	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
34	T.VA_Internal_Crack_Disclose_PrivateKey-SSL	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
35	T.VA_Auditor_Crack_PrivateKey-SSL	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
36	T.VA_Auditor_Crack_Disclose_PrivateKey-SSL	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	私有鍵の新規作成
37	T.VA_Internal_Crack_Log	防止	複数人による操作 罰則規定の強化 安全なログ管理システム（例：他組織が管理するログ管理システム）の導入
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
38	T.VA_Internal_Crack_Disclose_Log	防止	複数人による操作 罰則規定の強化 安全なログ管理システム（例：他組織が管理するログ管理システム）の導入
		検出	操作ログデータの記録と監査 不正プログラムの監視

		回復	-
39	T.VA_Auditor_Crack_Log	防止	管理者権限パスワード管理 罰則規定の強化 安全なログ管理システム（例：他組織が管理するログ管理システム）の導入
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
40	T.VA_Auditor_Crack_Disclose_Log	防止	管理者権限パスワード管理 罰則規定の強化 安全なログ管理システム（例：他組織が管理するログ管理システム）の導入
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
41	T.VA_Internal_Crack_Disclose_UserID-AuthenticationData	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	パスワードの変更
42	T.VA_Auditor_Crack_Disclose_UserID-AuthenticationData	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	パスワードの変更
43	T.VA_Internal_Crack_Disclose_TSA1AccessInfo	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	アクセス用 ID とパスワードの変更
44	T.VA_Auditor_Crack_Disclose_TSA1AccessInfo	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	アクセス用 ID とパスワードの変更
45	T.VA_Internal_Crack_Disclose_HSMAccessInfo	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	アクセス用 ID とパスワードの変更
46	T.VA_Auditor_Crack_Disclose_HSMAccessInfo	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	アクセス用 ID とパスワードの変更
47	T.VA_Internal_Crack_Mod_VA-Mgmt-Tool	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
48	T.VA_Internal_Crack_Disclose_VA-Mgmt-Tool	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
49	T.VA_Auditor_Crack_Mod_VA-Mgmt-Tool	防止	管理者権限パスワード管理 罰則規定の強化

		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
50	T.VA_Auditor_Crack_Disclose_VA-Mgmt-Tool	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
51	T.VA_Internal_Crack_Mod_VA-Process	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
52	T.VA_Internal_Crack_Disclose_VA-Process	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
53	T.VA_Internal_DoS_Attack	防止	複数人による操作 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
54	T.VA_Auditor_Crack_Mod_VA-Process	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	バックアップ/リストア
55	T.VA_Auditor_Crack_Disclose_VA-Process	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
56	T.VA_Auditor_DoS_Attack	防止	管理者権限パスワード管理 罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-
57	T.VA_Internal_Repudiation	防止	罰則規定の強化
		検出	操作ログデータの記録と監査 不正プログラムの監視
		回復	-

セキュリティ評価報告書

（TOE：TSA1）

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

1. TOE の機能概要

TOE は、タイムスタンプ発行処理により、利用者から送付されたタイムスタンプ要求に対してリンクトークン方式タイムスタンプ（ここでいうリンクトークン方式タイムスタンプとは、TSA がタイムスタンプ対象データのハッシュ値に対して他のハッシュ値と関連付けるリンク情報を生成し、その時点までに生成したタイムスタンプと関連性を明らかにして有効性を証明する方式。）を発行するとともに、タイムスタンプ検証処理により、利用者から送付されリンクトークン方式タイムスタンプの検証要求に対して、検証結果を返信する。また、時刻監査／配信受付処理により、TA による認証連鎖方式（ここでいう認証連鎖方式とは、PKI(Public Key Infrastructure) 認証技術を利用して TA が時刻配信先の時計を特定すると同時に時刻の計測と配信を行い、その計測結果を時刻監査記録として更に時刻配信先の時計に連鎖していく方式。）の時刻監査／配信を受付るとともに、時刻トレーサビリティ機能により、時刻監査レポート確認方式による時刻トレーサビリティの確認を可能とする。

2. TOE 構成図

TOE の構成図を、以下の図 1に示す

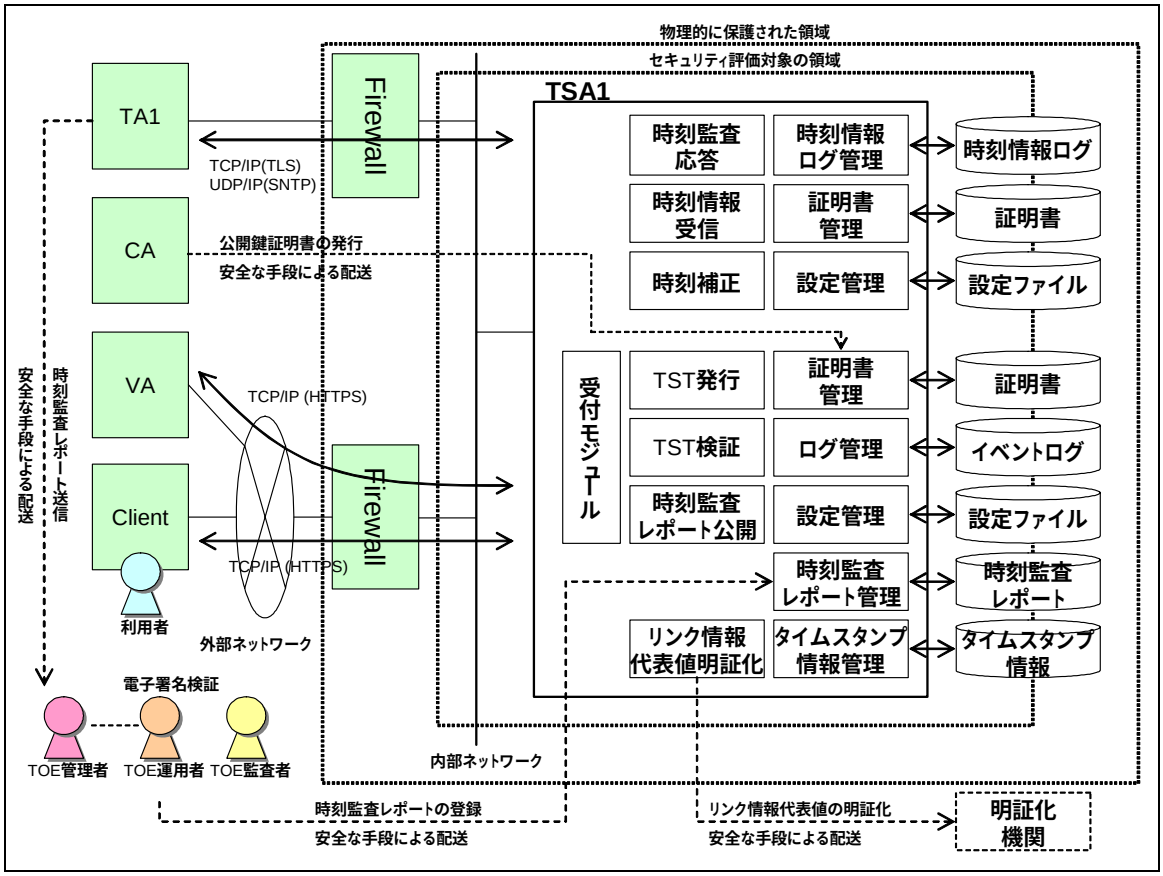


図 1　TOE の構成図

3. 利用する暗号技術と暗号コンポーネント構成図

3-1 利用する暗号技術

TOE で使用している暗号技術を、以下の表 1に示す。

表 1 TOE で使用している暗号技術

#	システム	#	使用している暗号技術		使用目的
1	TSA1	C1-1	TLS	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 RSAES-PKCS1-v1_5 鍵長 1024 ビット 【共通鍵暗号方式】 128bit-RC4 【ハッシュ関数】 SHA-1	TA1-TSA1 間の時刻配信時の通信経路
		C1-2	HMAC	【共通鍵】 鍵長 128 ビット 【ハッシュ関数】 MD5	NTP 通信パケットの改竄検出
		C1-3	ハッシュ関数	SHA-1	TA1-TSA1 間の時刻監査・配信時のログレコード作成
		C1-4	PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	TA1-TSA1 間の時刻監査・配信時のログファイルへの署名
		C1-5	SSL	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 RSAES-PKCS1-v1_5 鍵長 1024 ビット 【共通鍵暗号方式】 鍵長 128 ビット以上 【ハッシュ関数】 SHA-1	TSA1-クライアント間の通信経路
		C1-6	ハッシュ関数	SHA-512/ RIPEMD-160	リンク情報生成
		C1-7	PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	TSA1 サーバの運用者が時刻監査レポートの電子署名が有効であることを確認する時に使用する (TSA1 の機能とは別に運用で使用する)
		C1-8	PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	時刻監査証明書の検証

2	クライアント	C2-1	SSL	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 RSAES-PKCS1-v1_5 鍵長 1024 ビット 【共通鍵暗号方式】 鍵長 128 ビット以上 【ハッシュ関数】 SHA-1	TSA1-クライアント間の通信経路
		C2-2	PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット 【ハッシュ関数】 SHA-1	時刻監査レポートの署名の検証
		C2-3	ハッシュ関数	SHA-512/ RIPEMD-160	タイムスタンプ発行要求作成、タイムスタンプと対象ドキュメントの結び付き確認

3-2 暗号コンポーネント構成図

3-2-1 セキュリティ評価対象の領域

TOE に係るセキュリティ評価対象の領域を、以下の図 2に示す。

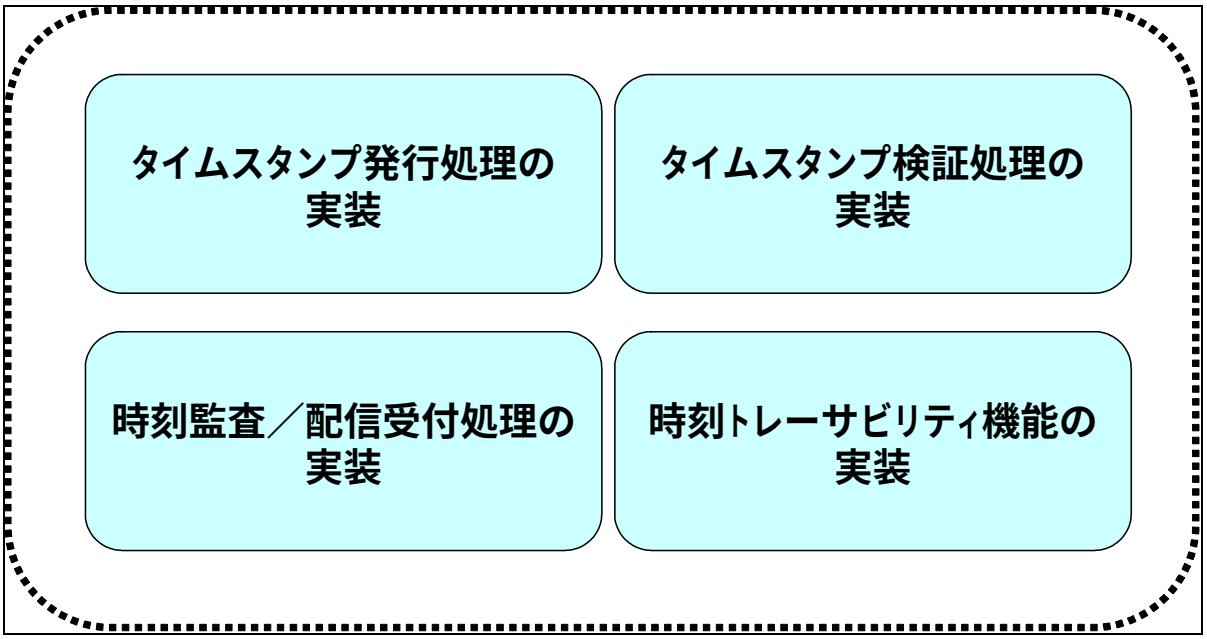


図 2 セキュリティ評価対象の領域

3-2-2 タイムスタンプ発行処理の実装

(1) タイムスタンプ発行要求機能の実装概要

TOE に係るセキュリティ評価対象の領域の中のタイムスタンプ発行処理の実装に含まれるタイムスタンプ発行要求機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 3に示す。

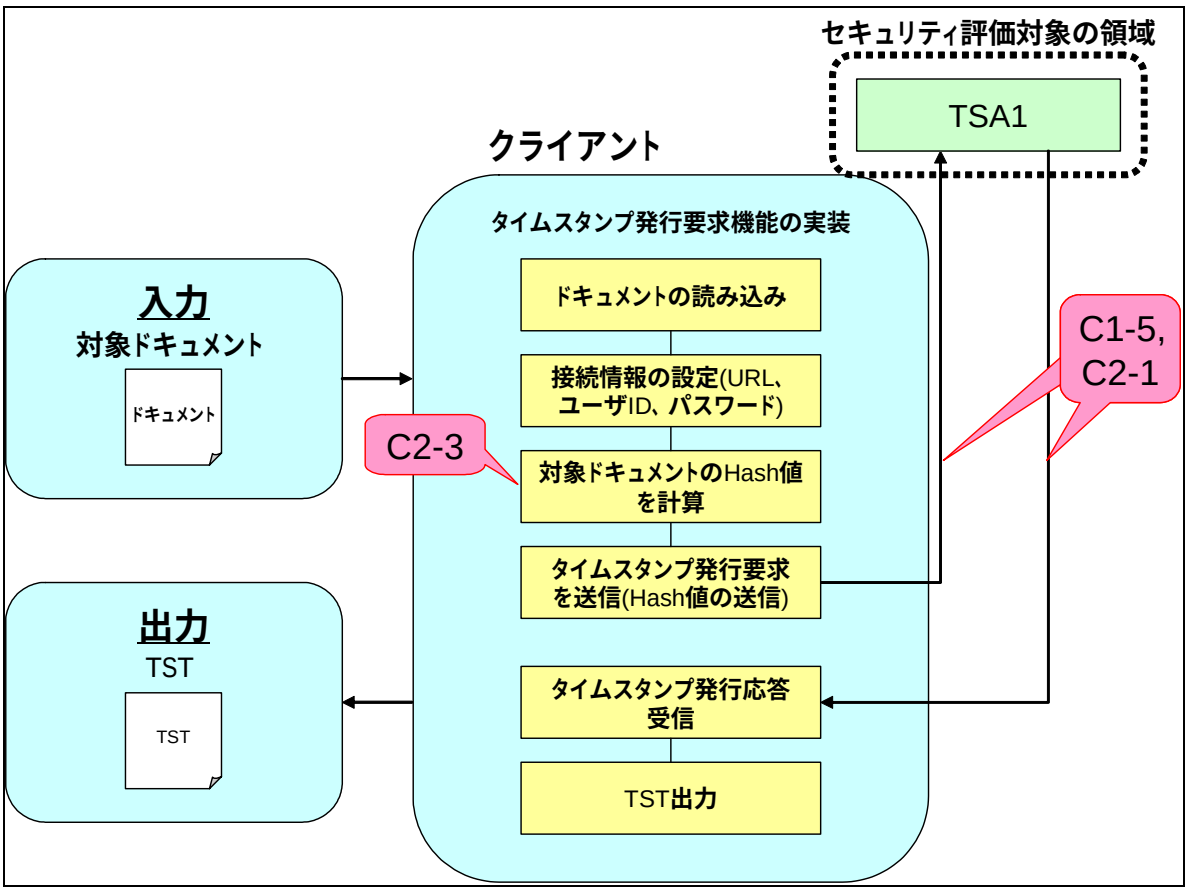


図 3　タイムスタンプ発行要求機能の実装概要

(2) タイムスタンプ発行機能の実装概要

TOE に係るセキュリティ評価対象の領域の中のタイムスタンプ発行処理の実装に含まれるタイムスタンプ発行機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 4に示す。

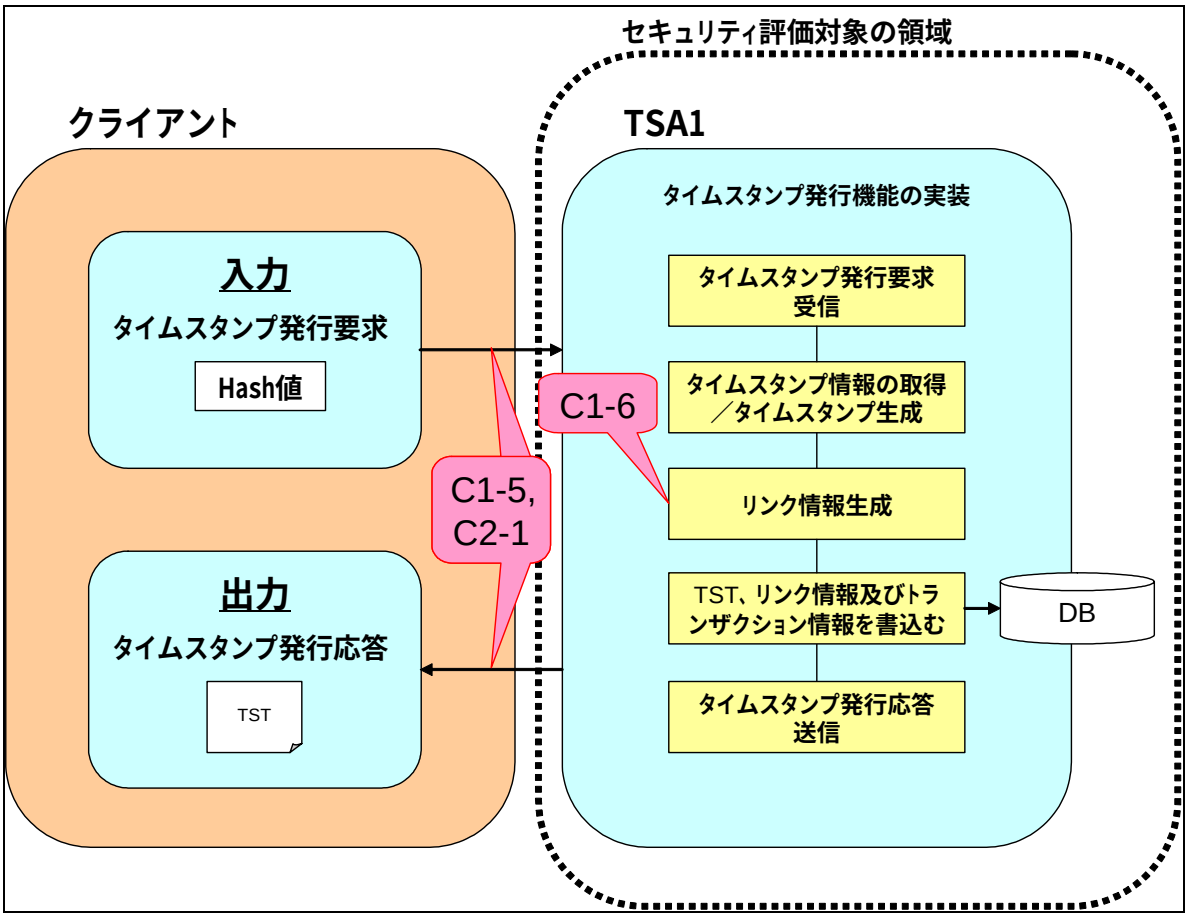


図 4　タイムスタンプ発行機能の実装概要

3-2-3 タイムスタンプ検証処理の実装

(1) タイムスタンプ検証要求機能の実装概要

TOE に係るセキュリティ評価対象の領域の中のタイムスタンプ検証処理の実装に含まれるタイムスタンプ検証要求機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 5に示す。

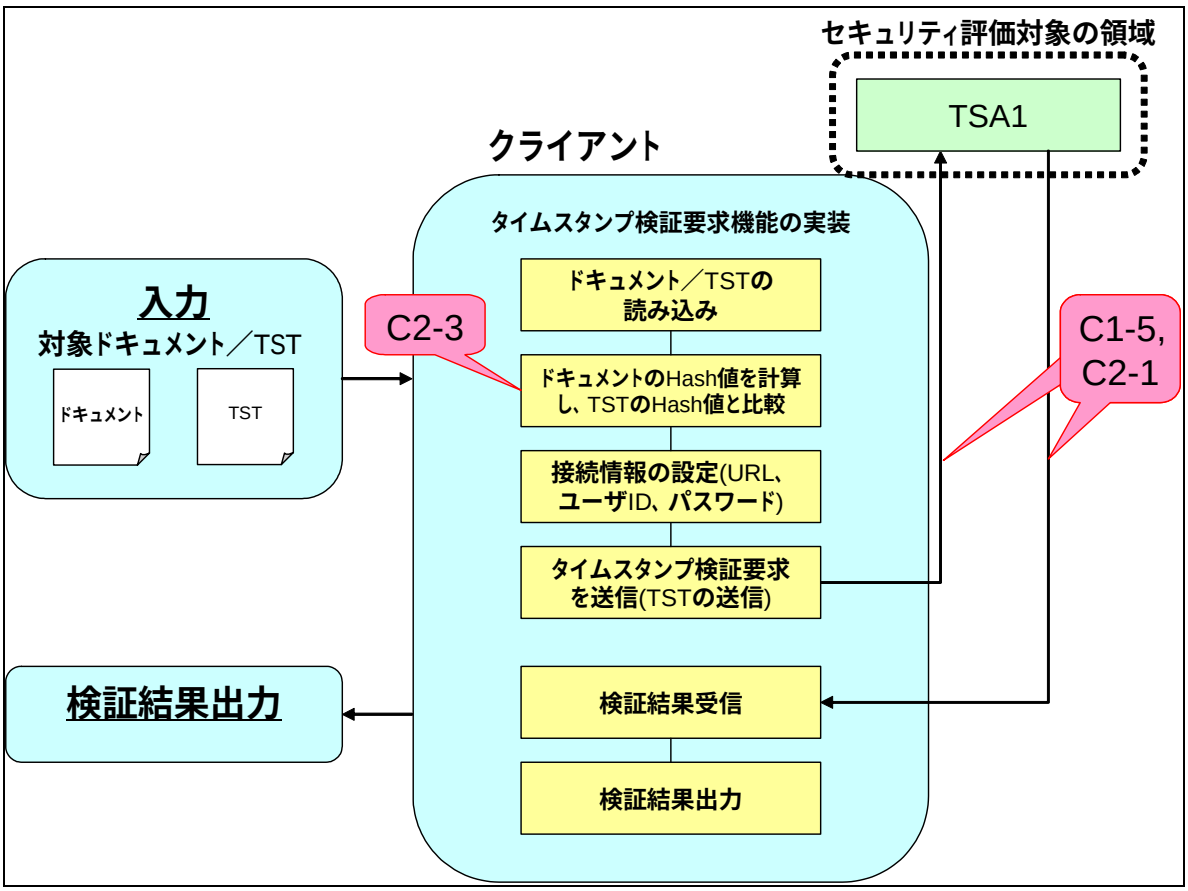


図 5　タイムスタンプ検証要求機能の実装概要

(2) タイムスタンプ検証機能の実装概要

TOE に係るセキュリティ評価対象の領域の中のタイムスタンプ検証処理の実装に含まれるタイムスタンプ検証機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 6に示す。

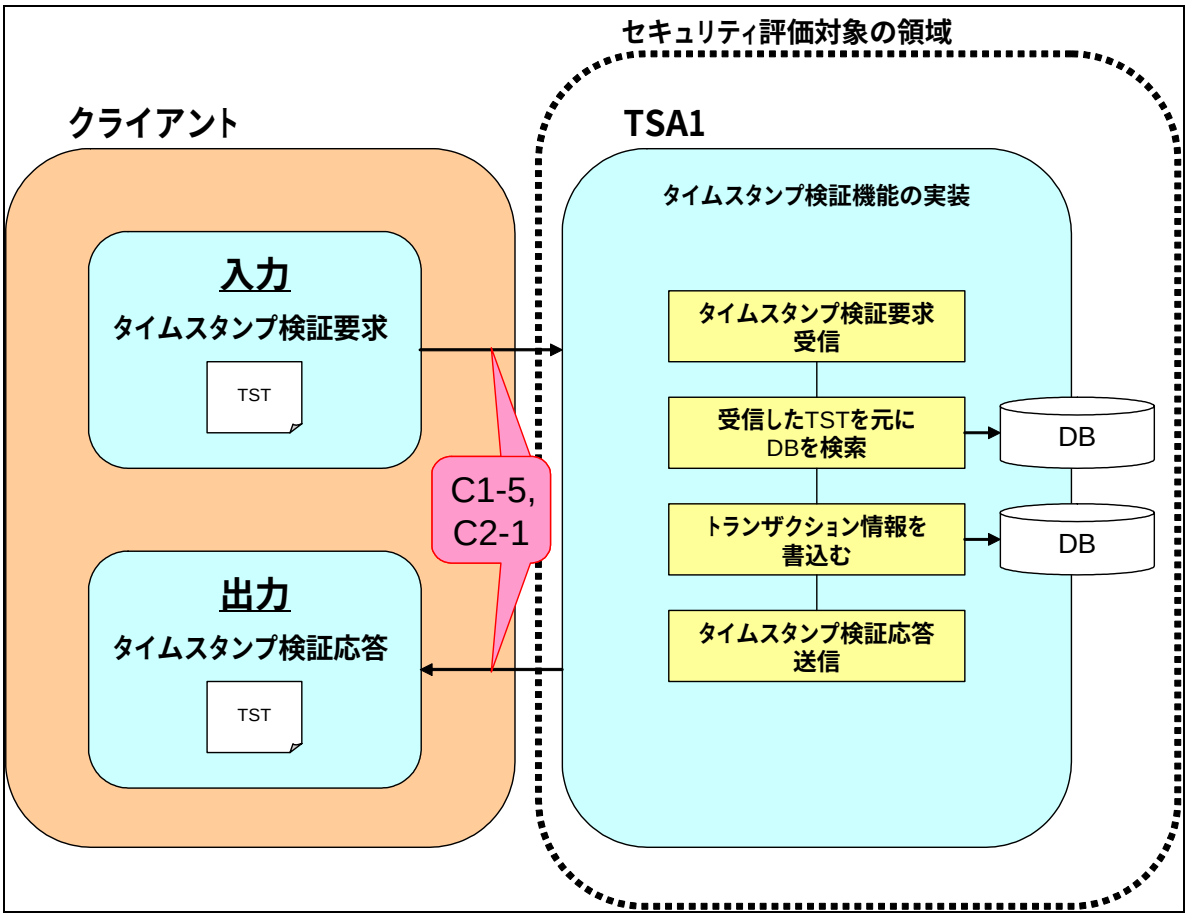


図 6　タイムスタンプ検証機能の実装概要

3-2-4 時刻監査／配信受付機能の実装

(1) TLS 接続受付機能の実装概要

TOE に係るセキュリティ評価対象の領域の中の時刻監査／配信受付処理の実装に含まれる TLS 接続受付機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 7に示す。

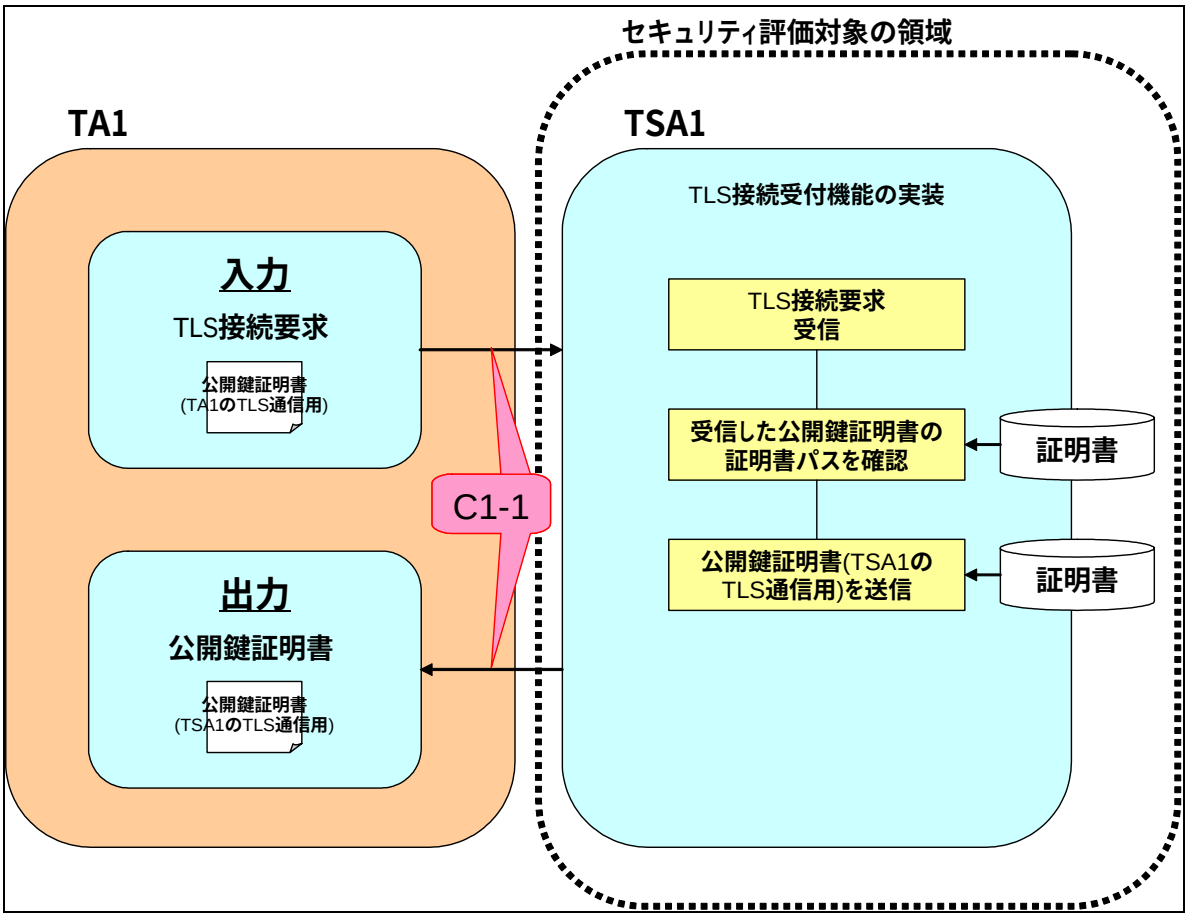


図 7　TLS 接続受付機能の実装概要

(2) 時刻監査受付機能の実装概要

TOE に係るセキュリティ評価対象の領域の中の時刻監査／配信受付処理の実装に含まれる時刻監査受付機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 8に示す。

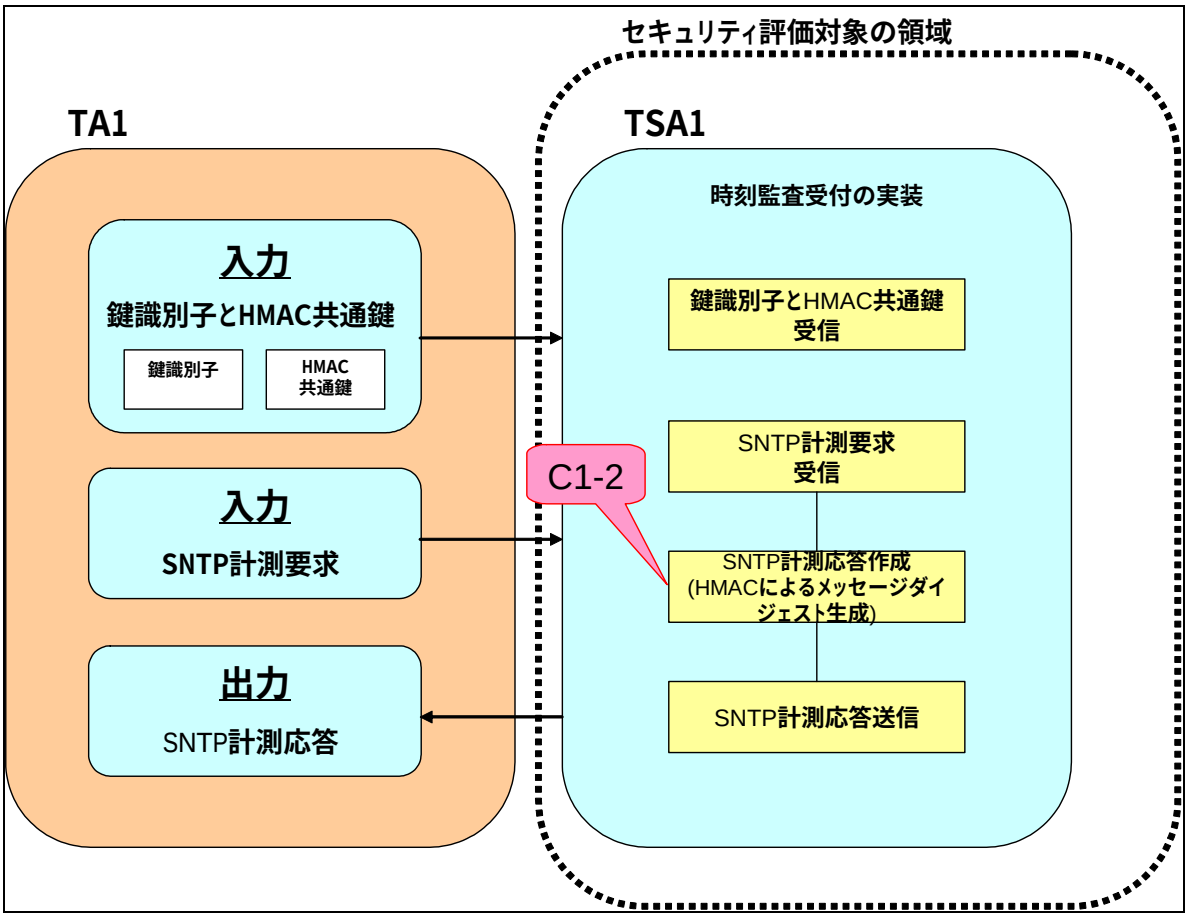


図 8　時刻監査受付機能の実装概要

(3) 時刻補正受付機能の実装概要

TOE に係るセキュリティ評価対象の領域の中の時刻監査／配信受付処理の実装に含まれる時刻監査受付機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 9に示す。

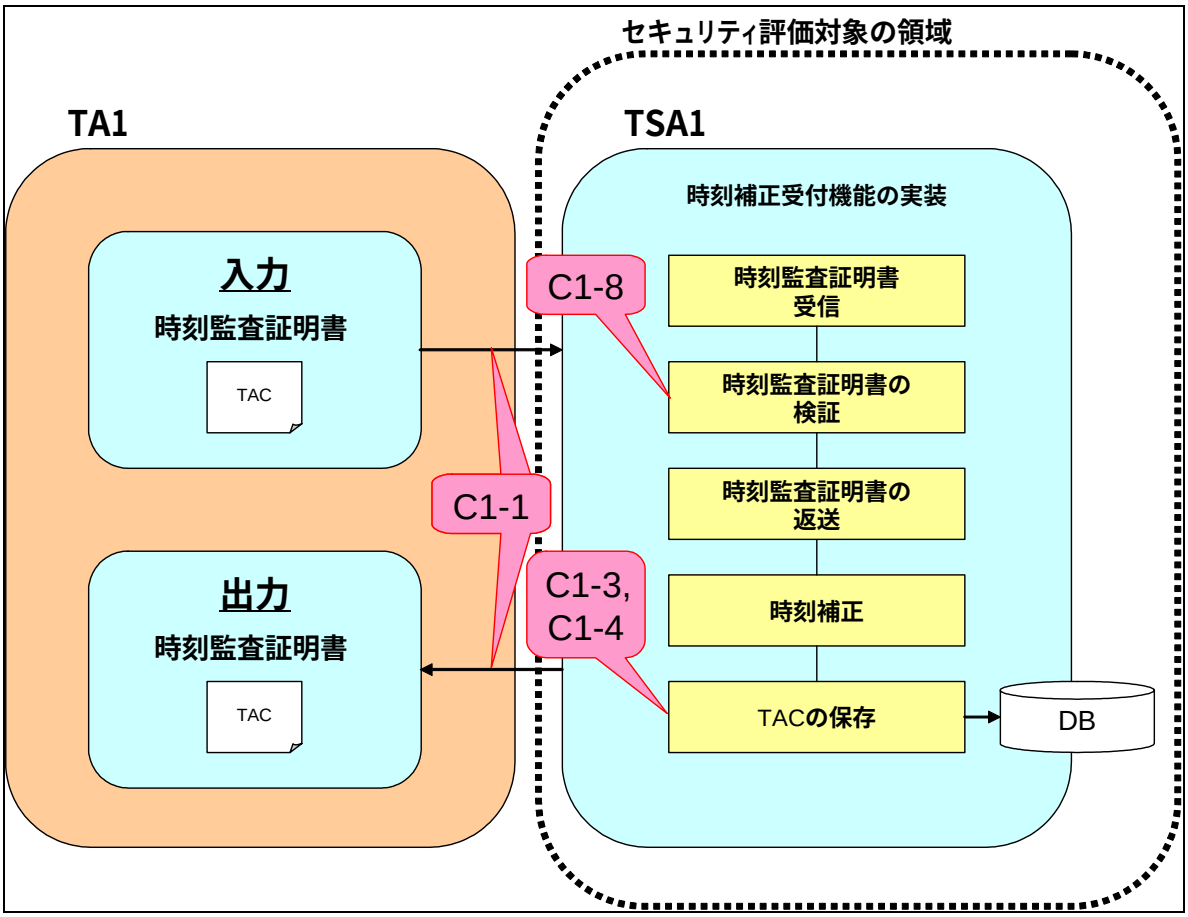


図 9　時刻補正受付機能の実装概要

3-2-5 時刻トレーサビリティ機能の実装
(1) 時刻トレーサビリティ機能の実装概要

TOE に係るセキュリティ評価対象の領域の中の時刻トレーサビリティ機能の実装に含まれる時刻トレーサビリティ機能の実装概要及び「表 1　TOE で使用している暗号技術」に記載されている暗号技術が使用されている箇所について、以下の図 10に示す。

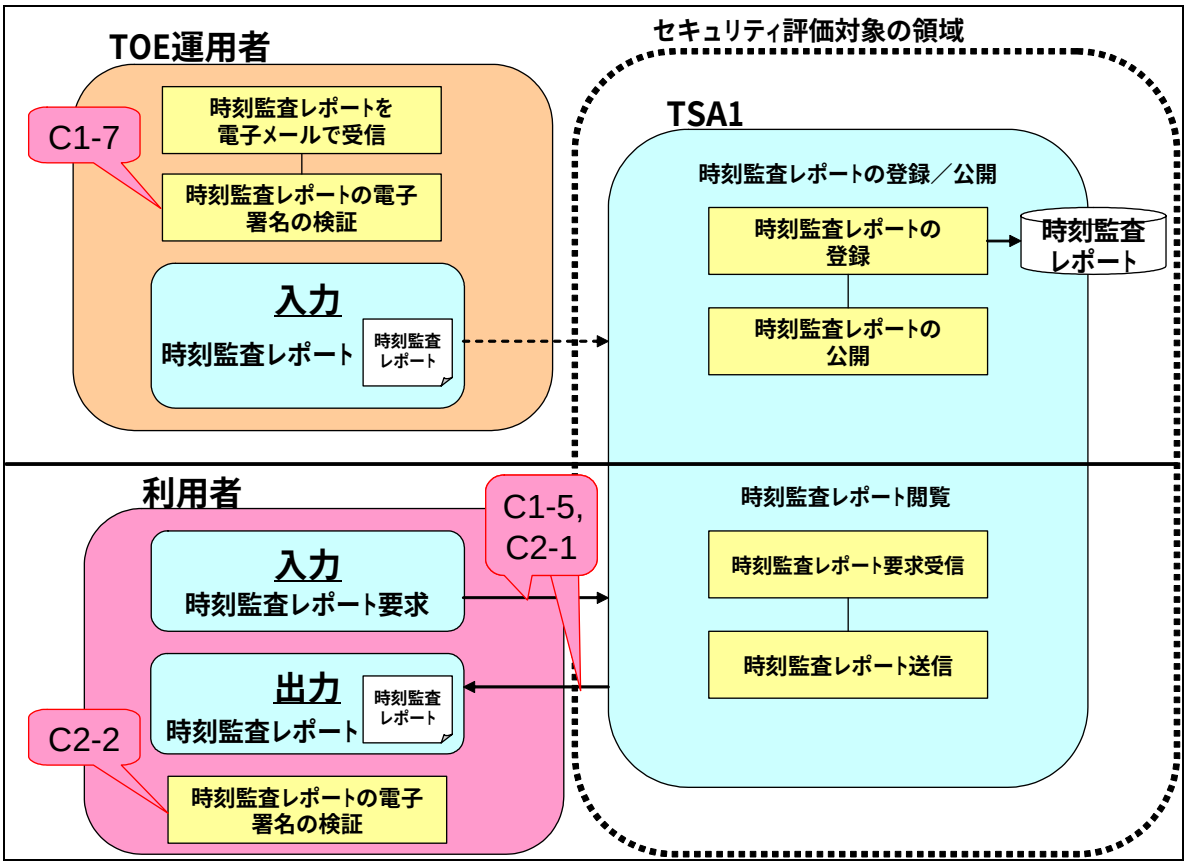


図 10　時刻トレーサビリティ機能の実装概要

4. 関与者

TOE に係る関与者一覧を、以下の表 2に示す。

表 2 TOE に係る関与者一覧

#	項目	内容	説明
1	ADMIN	TOE 管理者	TOE に関わるユーザ/役割を管理する。
2	OPE	TOE 運用者	TOE の起動・停止を実行する。 TOE 管理者の指示の元で各種設定・リンク情報の代表値の明証化・時刻監査レポートの登録等の運用業務を行う。
3	AUDIT	TOE 監査者	TOE が生成する監査データの分析やリンク情報の整合性確認等の監査業務を行う。
4	USER	利用者(TST 要求)	タイムスタンプ発行要求を送信しタイムスタンプを取得する。
5		利用者(TST 検証)	タイムスタンプ検証要求を送信しタイムスタンプ検証を行う。
6		利用者(トレーサビリティ確認)	時刻監査レポートを閲覧し、時刻のトレーサビリティを確認する。
7	TA1	時刻配信サブシステム1	TOE に対して、時刻配信／監査を行う。
8	VA	検証サブシステム	TOE の発行したタイムスタンプについて、検証を行う。
9	CA	認証サブシステム	TOE が行う TLS／SSL 通信に必要な公開鍵証明書を発行・管理する。
10	PROVE	明証化機関	TOE が生成するリンク情報の代表値を明証化する。

5. 資産

TOE に係る資産一覧を、以下の表 3に示す。

表 3 TOE に係る資産一覧

#	分類		項目	内容	説明
1	情報資産	利用者データ	USER-ID-PW	利用者のユーザ ID、パスワード	TSA1 のサービスを利用可能なユーザであるかを識別する為に使用する。
2			TST	タイムスタンプトークン	タイムスタンプ発行要求を元に TSA1 が利用者に対して発行する。
3		TSF データ	TAC	時刻監査証明書	TA1 が行う時刻監査の結果を元に TA1 で作成され、その後 TSA1 に送信される時刻情報。 時刻監査証明書の情報を元に TSA1 の時刻補正が行われる。
4			TAC-LOG	時刻監査証明書受信ログ	TA1 から受信した時刻監査証明書の記録。
5			TAR	時刻監査レポート	TA1 が行う時刻監査の一定期間の結果をまとめたレポート。TA1 で作成されて TSA1 に送付され、TSA1 において公開される。
6			KEYST	keystore ファイル	CA、TSA1、TSA1(通信用)の証明書が登録されている。 時刻監査、配信時に使用される。
7			KEYST-PW	keystore アクセス用パスワード	keystore へのアクセスに必要とされる。
8			CERT	証明書	安全な通信経路を確立、時刻監査証明書の検証等に使用する。
9			CRL-ARL	CRL/ARL	証明書の有効性確認時に使用する。
10			PRI-KEY	秘密鍵	安全な通信経路を確立等に使用する。
11			PRI-KEY-PW	秘密鍵アクセス用パスワード	暗号化された秘密鍵の復号に必要とされる。
12			OPE-ID-PW	TSA1 のユーザ ID、パスワード	TSA1 の各種設定の変更や動作確認時にログインする為に使用する。
13			DB-SERIAL	タイムスタンプ情報 (シリアル No)	発行したタイムスタンプのシリアル No。 タイムスタンプ発行時にデータベースに格納される。
14			DB-USER-ID	タイムスタンプ情報 (ユーザ ID)	タイムスタンプの発行を要求したユーザの ID。 タイムスタンプ発行時にデータベースに格納される。

#	分類		項目	内容	説明
15			DB-TIME	タイムスタンプ情報(タイムスタンプ発行時刻)	タイムスタンプを発行した時刻。 タイムスタンプ発行時にデータベースに格納される。
16			DB-TST	タイムスタンプ情報(TST)	発行した TST。 タイムスタンプ発行時にデータベースに格納される。
17			LINK	リンク情報	発行された全ての TST に依存するようにハッシュ値を相互に関連付けたもの。 タイムスタンプ発行時にデータベースに格納される。
18			CONFIG	各種設定ファイル	httpd.conf、tslp.conf、postgresql.conf 等の TSA1 の動作を制御する設定ファイル。
19			DB-ID-PW	DB アクセス用の ID、パスワード	データベースへのアクセスに使用する。
20			LINK-PROV	明証化した情報	内部不正がないことを証明する為に明証化するリンク情報の代表値。
21			EVENT	イベント情報	サーバへのアクセスやイベントに関するログ。
22			CLOCK	システムクロック	TST 作成時に時刻情報源として使用される。
23	IT 実装		MOD-CRE-TS	タイムスタンプ生成プログラム	時刻情報の取得からタイムスタンプの生成に至るまでの処理を行う。
24			MOD-STORE	照合用データ保管プログラム	タイムスタンプの生成から照合用データの保管に至るまでの処理を行う。
25			MOD-COM-TS	タイムスタンプ照合プログラム	タイムスタンプの照合処理と行う。
26			MOD-TIME	時刻情報受信・補正プログラム	TA からの時刻情報及び時刻監査結果の受信処理ならびに TSA のシステムクロックの補正処理を行う。

第2章 セキュリティ環境

1. 前提

TOE に係るセキュリティ環境の前提一覧を、以下の表 4に示す。

表 4　TOE に係るセキュリティ環境の前提一覧

#	分類	項目	説明
1	物理的な前提（Physical assumptions）	A.LOCATE	TOE は、設置された室の入退室管理により、権限のないユーザからの物理アクセスを防ぐ。
2		A.ENVIRONMENT	TOE の設置場所は、電磁波対策、電力対策、温度･湿度対策が行われている。
3		A.MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。
4	人的な前提（Personnel assumptions）	A.ADMIN	一人以上の許可された管理者が、割り当てられる。彼らは、TOE と TOE に含まれる情報のセキュリティを管理する資格を持つ。さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
5		A.OPERATOR	一人以上の許可された運用者が、割り当てられる。彼らは、TOE を操作する資格を持つ。さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
6		A.AUDITOR	一人以上の許可された監査者が、割り当てられる。TOE に関するログを取得し、分析を行う。また、リンク情報の整合性の確認を行う。さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
7		A.USER	TOE の利用者は、定められた手順に従ってタイムスタンプの付与及び検証操作を行うこととする。TOE 利用者のパスワードは、TOE 利用者本人によって適切に管理され、本人以外に知られてはならない。
8	接続に関する前提（Connectivity assumptions）	A.DEVICE	周辺機器への全接続は、コントロールされたアクセス･ファシリティ内に存在する。
9		A.FIREWALL	TOE は、専用ネットワークに設置される。外部ネットワークからのネットワークに対する攻撃を防ぐ装置が設置される。
10		A.PEER	TOE と通信する意図された他システムは、信頼できる。
11		A.REQUESTER_CONNECTION	タイムスタンプ要求者、検証者及び時刻監査レポート要求者が操作するマシンと TOE の間の通信路は、TOE の成りすまし、データの改ざん、データの盗聴を防止する。
12		A.VA_CONNECTION	VA と TOE の間の通信路は、TOE の成りすまし、データの改ざん、データの盗聴を防止する。
13		A.TA1_CONNECTION	TA1 と TOE の間の通信路は、TOE の成りすまし、データの改ざん、データの盗聴を防止する。
14		A.ABSTRACT	TOE が動作するために必要な OS や依存するライブラリは、不正な改変から保護され、正しく動作する。

#	分類	項目	説明
15		A.SEPARATION	TOE が動作するマシンには、TOE の動作に必要なソフトウェア以外はインストールされないものとする。

2. 脅威

TOE に係るセキュリティ環境の脅威一覧を、以下の表 5に示す。ここで、環境及び TOE（個別）に分類される脅威は、それぞれ単体でリスク評価する脅威を示し、TOE（共通）に分類される脅威は、攻撃者及び攻撃対象となる情報資産との組合せでリスク評価する脅威を示す。

表 5　TOE に係るセキュリティ環境の脅威一覧

#	分類	項目	説明
1	環境	T.VIRUS	コンピュータ･ウイルスの感染により、TOE の情報資産もしくは IT 実装の一貫性やアベイラビリティが脆弱化する。
2	TOE（個別）	T.SYSTEM_CLOCK_INACCURACY	TOE が参照するシステム時計の時刻の誤差が TOE 管理者の受容範囲を超える。
3		T.HASH_COMPROMISE_FUTURE	将来、ハッシュ関数のアルゴリズムが脆弱化し、ハッシュ関数に求められる安全性が損なわれることにより、タイムスタンプの有効性に影響を与える。
4		T.HASH_COMPROMISE_CLIENT	クライアントより、脆弱化したハッシュ関数のアルゴリズムを使用して計算されたドキュメントハッシュを含むタイムスタンプ要求が送られる。
5		T.HASH_COMPROMISE_SERVER	TOE において、脆弱化したハッシュ関数のアルゴリズムを使用してリンク情報の生成等が行われる。
6		T.DOS	DoS 攻撃により、サーバがダウンしたり、正当なユーザへのサービスを妨げたりする。
7		T.HACK_IMPERSON_TOE	外部のネットワークに位置するハッカーが、TOE に成りすまし、偽のタイムスタンプトークンを発行する。
8		T.CLIENT_REFUTE_ORIGIN	タイムスタンプの意図された受信者が、タイムスタンプ生成元に関して意義を唱える。
9		T.HARDWARE_FAILURE	経年劣化や偶然に引き起こされる障害により、TOE のハードウェアが故障し、資産が失われる。 経年劣化や偶然に引き起こされる障害により、TOE のハードウェアが故障し、資産の完全性が保証できなくなる。
10		T.PEER_FAILURE	通信相手となる他システムのダウンにより、TOE の資産が失われる。 通信相手となる他システムのダウンにより、TOE が提供するサービスが継続できない。
11		T.CONNECTION_FAILURE	TOE と通信相手となる他システムの間の通信回線の故障により、TOE の資産が失われる。 TOE と通信相手となる他システムの間の通信回線の故障により、TOE が提供するサービスが継続できない。
12		T.TOE_BUG	TOE の IT 実装にソフトウェア不良が存在するため、TOE の資産の信頼性が乏しくなる。
13		T.BUFFEROVERFLOW_ATTACK	ネットワーク上の悪意者が、バッファ･オーバーフローの脆弱性を利用し、TOE の管理者権限を取得する。
14		T.TSQ_LINE	タイムスタンプ要求者-TOE 間のネットワークが、事故などにより、遮断され、タイムスタンプ要求者の送信したタイムスタンプ要求が、TOE に到達しない。

#	分類	項目	説明
15		T.TSR_LINE	タイムスタンプ要求者-TOE 間のネットワークが、事故などにより、遮断され、TOE の送信したタイムスタンプ応答が、タイムスタンプ要求者に到達しない。
16	TOE（共通）	T.FORGERY	TOE の情報資産もしくは IT 実装を偽造する。
17		T.MODIFY	TOE の情報資産もしくは IT 実装に対して許可されていない改変を加える。
18		T.ERACE	TOE の情報資産もしくは IT 実装に対して許可されていない消去を行う。
19		T.IMPERSON	攻撃者が他の主体に成りすましてアクセスする、もしくはアクセスを受け付ける。
20		T.STEAL	TOE の情報資産もしくは IT 実装に対して許可されていない閲覧を行う。
21		T.DISCLOSE	TOE の情報資産もしくは IT 実装について、閲覧が許可されていない者への漏洩を行う。

「表 5　TOE に係るセキュリティ環境の脅威一覧」において TOE（共通）に分類されている脅威に係る個別の組合せも含めた、TOE に係るセキュリティ環境の脅威名一覧を、以下の表 6に示す。なお、表中において、「表 2　TOE に係る関与者一覧」に記載されていない主体として「THIRD」が記載されているが、これは通常 TOE に関与していない第三者を示す。

表 6　TOE に係るセキュリティ環境の脅威名一覧

項番	資産	主体	汎用脅威	脅威名	脅威内容
1	－	－	－	T.VIRUS	コンピュータ･ウィルスの感染
2	－	－	－	T.SYSYTEM_CLOCK_INACCURACY	システム時計の時刻誤差が受容範囲外
3	－	－	－	T.HASH_COMPROMISE_FUTURE	将来的なハッシュアルゴリズムの脆弱化
4	－	－	－	T.HASH_COMPROMISE_CLIENT	脆弱化した関数の文書ハッシュによる要求
5	－	－	－	T.HASH_COMPROMISE_SERVER	脆弱化した関数によるリンク情報の生成
6	－	－	－	T.DOS	サーバへのDOS攻撃
7	－	－	－	T.HACK_IMPERSON_TOE	外部者が発行者に成り済まし偽のTSTを発行
8	－	－	－	T.CLIENT_REFUTE_ORIGIN	タイムスタンプ受信者が発行者に異議を唱える
9	－	－	－	T.HARDWARE_FAILURE	ハードウェアの故障
10	－	－	－	T.PEER_FAILURE	通信相手の他システムのダウン
11	－	－	－	T.CONNECTION_FAILURE	通信相手の他システムの間の通信回線故障
12	－	－	－	T.TOE_BUG	TOEのIT実装のソフトウェア不良
13	－	－	－	T.BUFFEROVERFLOW_ATTACK	サーバへのバッファーオーバーフロー攻撃
14	－	－	－	T.TSQ_LINE	タイムスタンプ要求時のネットワーク遮断
15	－	－	－	T.TSR_LINE	タイムスタンプ応答時のネットワーク遮断
16	USER-ID-PW	USER	T.FORGERY	T.FORGERY_USER-ID-PW_USER	偽造した自分のID/PWをサーバに登録
17	USER-ID-PW	USER	T.MODIFY	T.MODIFY_USER-ID-PW_USER	サーバに登録された自分のID/PWを改竄
18	USER-ID-PW	USER	T.ERACE	T.ERACE_USER-ID-PW_USER	サーバに登録された自分のID/PWを消去
19	USER-ID-PW	USER	T.IMPERSON	T.IMPERSON_USER-ID-PW_USER	権限者に成りすまして自分のID/PWにアクセス
20	USER-ID-PW	USER	T.STEAL	T.STEAL_USER-ID-PW_USER	情報所有者のため脅威外
21	USER-ID-PW	USER	T.DISCLOSE	T.DISCLOSE_USER-ID-PW_USER	自分のID/PWを不正に漏洩
22	USER-ID-PW	THIRD	T.FORGERY	T.FORGERY_USER-ID-PW_THIRD	偽造したID/PWをサーバに登録
23	USER-ID-PW	THIRD	T.MODIFY	T.MODIFY_USER-ID-PW_THIRD	サーバに登録されたID/PWを改竄
24	USER-ID-PW	THIRD	T.ERACE	T.ERACE_USER-ID-PW_THIRD	サーバに登録されたID/PWを消去
25	USER-ID-PW	THIRD	T.IMPERSON	T.IMPERSON_USER-ID-PW_THIRD	権限者に成りすましてID/PWにアクセス
26	USER-ID-PW	THIRD	T.STEAL	T.STEAL_USER-ID-PW_THIRD	サーバに登録されたID/PWを不正に取得
27	USER-ID-PW	THIRD	T.DISCLOSE	T.DISCLOSE_USER-ID-PW_THIRD	サーバに登録されたID/PWを不正に漏洩
28	TST	USER	T.FORGERY	T.FORGERY_TST_USER	偽造したＴＳＴを本物と偽って流通
29	TST	USER	T.MODIFY	T.MODIFY_TST_USER	改竄したＴＳＴを本物と偽って流通
30	TST	USER	T.ERACE	T.ERACE_TST_USER	発行されたＴＳＴを消去
31	TST	USER	T.IMPERSON	T.IMPERSON_TST_USER	発行者への成り済まし
32	TST	USER	T.STEAL	T.STEAL_TST_USER	機密性不要のため脅威外
33	TST	USER	T.DISCLOSE	T.DISCLOSE_TST_USER	機密性不要のため脅威外
34	TST	THIRD	T.FORGERY	T.FORGERY_TST_THIRD	偽造したＴＳＴを本物と偽って流通
35	TST	THIRD	T.MODIFY	T.MODIFY_TST_THIRD	改竄したＴＳＴを本物と偽って流通
36	TST	THIRD	T.ERACE	T.ERACE_TST_THIRD	発行されたＴＳＴを消去
37	TST	THIRD	T.IMPERSON	T.IMPERSON_TST_THIRD	発行者への成り済まし
38	TST	THIRD	T.STEAL	T.STEAL_TST_THIRD	機密性不要のため脅威外
39	TST	THIRD	T.DISCLOSE	T.DISCLOSE_TST_THIRD	機密性不要のため脅威外
40	TAC	USER	T.FORGERY	T.FORGERY_TAC_USER	偽造したTACを登録もしくは流通
41	TAC	USER	T.MODIFY	T.MODIFY_TAC_USER	改竄したTACを登録もしくは流通
42	TAC	USER	T.ERACE	T.ERACE_TAC_USER	サーバに登録されたTACの消去
43	TAC	USER	T.IMPERSON	T.IMPERSON_TAC_USER	発行者への成り済まし
44	TAC	USER	T.STEAL	T.STEAL_TAC_USER	機密性不要のため脅威外
45	TAC	USER	T.DISCLOSE	T.DISCLOSE_TAC_USER	機密性不要のため脅威外
46	TAC	THIRD	T.FORGERY	T.FORGERY_TAC_THIRD	偽造したTACを登録もしくは流通
47	TAC	THIRD	T.MODIFY	T.MODIFY_TAC_THIRD	改竄したTACを登録もしくは流通
48	TAC	THIRD	T.ERACE	T.ERACE_TAC_THIRD	サーバに登録されたTACの消去
49	TAC	THIRD	T.IMPERSON	T.IMPERSON_TAC_THIRD	発行者への成り済まし
50	TAC	THIRD	T.STEAL	T.STEAL_TAC_THIRD	機密性不要のため脅威外
51	TAC	THIRD	T.DISCLOSE	T.DISCLOSE_TAC_THIRD	機密性不要のため脅威外

項番	資産	主体	汎用脅威	脅威名	脅威内容
52	TAC-LOG	USER	T.FORGERY	T.FORGERY_TAC-LOG_USER	偽造したTACログを登録
53	TAC-LOG	USER	T.MODIFY	T.MODIFY_TAC-LOG_USER	改竄したTACログを登録
54	TAC-LOG	USER	T.ERACE	T.ERACE_TAC-LOG_USER	サーバに保管されたTACログの消去
55	TAC-LOG	USER	T.IMPERSON	T.IMPERSON_TAC-LOG_USER	アクセス権所有者への成り済まし
56	TAC-LOG	USER	T.STEAL	T.STEAL_TAC-LOG_USER	TACログを不正に取得
57	TAC-LOG	USER	T.DISCLOSE	T.DISCLOSE_TAC-LOG_USER	TACログを不正に漏洩
58	TAC-LOG	THIRD	T.FORGERY	T.FORGERY_TAC-LOG_THIRD	偽造したTACログを登録
59	TAC-LOG	THIRD	T.MODIFY	T.MODIFY_TAC-LOG_THIRD	改竄したTACログを登録
60	TAC-LOG	THIRD	T.ERACE	T.ERACE_TAC-LOG_THIRD	サーバに保管されたTACログの消去
61	TAC-LOG	THIRD	T.IMPERSON	T.IMPERSON_TAC-LOG_THIRD	アクセス権所有者への成り済まし
62	TAC-LOG	THIRD	T.STEAL	T.STEAL_TAC-LOG_THIRD	TACログを不正に取得
63	TAC-LOG	THIRD	T.DISCLOSE	T.DISCLOSE_TAC-LOG_THIRD	TACログを不正に漏洩
64	TAR	USER	T.FORGERY	T.FORGERY_TAR_USER	偽造したTARを登録もしくは流通
65	TAR	USER	T.MODIFY	T.MODIFY_TAR_USER	改竄したTARを登録もしくは流通
66	TAR	USER	T.ERACE	T.ERACE_TAR_USER	サーバに登録されたTARの消去
67	TAR	USER	T.IMPERSON	T.IMPERSON_TAR_USER	発行者への成り済まし
68	TAR	USER	T.STEAL	T.STEAL_TAR_USER	機密性不要のため脅威外
69	TAR	USER	T.DISCLOSE	T.DISCLOSE_TAR_USER	機密性不要のため脅威外
70	TAR	THIRD	T.FORGERY	T.FORGERY_TAR_THIRD	偽造したTARを登録もしくは流通
71	TAR	THIRD	T.MODIFY	T.MODIFY_TAR_THIRD	改竄したTARを登録もしくは流通
72	TAR	THIRD	T.ERACE	T.ERACE_TAR_THIRD	サーバに登録されたTARの消去
73	TAR	THIRD	T.IMPERSON	T.IMPERSON_TAR_THIRD	発行者への成り済まし
74	TAR	THIRD	T.STEAL	T.STEAL_TAR_THIRD	機密性不要のため脅威外
75	TAR	THIRD	T.DISCLOSE	T.DISCLOSE_TAR_THIRD	機密性不要のため脅威外
76	KEYST	USER	T.FORGERY	T.FORGERY_KEYST_USER	偽造したキーストアを登録
77	KEYST	USER	T.MODIFY	T.MODIFY_KEYST_USER	改竄したキーストアを登録
78	KEYST	USER	T.ERACE	T.ERACE_KEYST_USER	サーバに登録されたキーストアの消去
79	KEYST	USER	T.IMPERSON	T.IMPERSON_KEYST_USER	アクセス権所有者への成り済まし
80	KEYST	USER	T.STEAL	T.STEAL_KEYST_USER	キーストアの中身を不正に取得
81	KEYST	USER	T.DISCLOSE	T.DISCLOSE_KEYST_USER	キーストアの中身を不正に漏洩
82	KEYST	THIRD	T.FORGERY	T.FORGERY_KEYST_THIRD	偽造したキーストアを登録
83	KEYST	THIRD	T.MODIFY	T.MODIFY_KEYST_THIRD	改竄したキーストアを登録
84	KEYST	THIRD	T.ERACE	T.ERACE_KEYST_THIRD	サーバに登録されたキーストアの消去
85	KEYST	THIRD	T.IMPERSON	T.IMPERSON_KEYST_THIRD	アクセス権所有者への成り済まし
86	KEYST	THIRD	T.STEAL	T.STEAL_KEYST_THIRD	キーストアの中身を不正に取得
87	KEYST	THIRD	T.DISCLOSE	T.DISCLOSE_KEYST_THIRD	キーストアの中身を不正に漏洩
88	KEYST-PW	USER	T.FORGERY	T.FORGERY_KEYST-PW_USER	偽造したPWをサーバに登録
89	KEYST-PW	USER	T.MODIFY	T.MODIFY_KEYST-PW_USER	サーバに登録されたPWを改竄
90	KEYST-PW	USER	T.ERACE	T.ERACE_KEYST-PW_USER	サーバに登録されたPWを消去
91	KEYST-PW	USER	T.IMPERSON	T.IMPERSON_KEYST-PW_USER	アクセス権所有者への成り済まし
92	KEYST-PW	USER	T.STEAL	T.STEAL_KEYST-PW_USER	サーバに登録されたPWを不正に取得
93	KEYST-PW	USER	T.DISCLOSE	T.DISCLOSE_KEYST-PW_USER	サーバに登録されたPWを不正に漏洩
94	KEYST-PW	THIRD	T.FORGERY	T.FORGERY_KEYST-PW_THIRD	偽造したPWをサーバに登録
95	KEYST-PW	THIRD	T.MODIFY	T.MODIFY_KEYST-PW_THIRD	サーバに登録されたPWを改竄
96	KEYST-PW	THIRD	T.ERACE	T.ERACE_KEYST-PW_THIRD	サーバに登録されたPWを消去
97	KEYST-PW	THIRD	T.IMPERSON	T.IMPERSON_KEYST-PW_THIRD	アクセス権所有者への成り済まし
98	KEYST-PW	THIRD	T.STEAL	T.STEAL_KEYST-PW_THIRD	サーバに登録されたPWを不正に取得
99	KEYST-PW	THIRD	T.DISCLOSE	T.DISCLOSE_KEYST-PW_THIRD	サーバに登録されたPWを不正に漏洩
100	CERT	USER	T.FORGERY	T.FORGERY_CERT_USER	偽造した証明書をサーバに登録
101	CERT	USER	T.MODIFY	T.MODIFY_CERT_USER	サーバに登録された証明書を改竄
102	CERT	USER	T.ERACE	T.ERACE_CERT_USER	サーバに登録された証明書を消去
103	CERT	USER	T.IMPERSON	T.IMPERSON_CERT_USER	発行者への成り済まし
104	CERT	USER	T.STEAL	T.STEAL_CERT_USER	機密性不要のため脅威外
105	CERT	USER	T.DISCLOSE	T.DISCLOSE_CERT_USER	機密性不要のため脅威外
106	CERT	THIRD	T.FORGERY	T.FORGERY_CERT_THIRD	偽造した証明書をサーバに登録
107	CERT	THIRD	T.MODIFY	T.MODIFY_CERT_THIRD	サーバに登録された証明書を改竄
108	CERT	THIRD	T.ERACE	T.ERACE_CERT_THIRD	サーバに登録された証明書を消去
109	CERT	THIRD	T.IMPERSON	T.IMPERSON_CERT_THIRD	発行者への成り済まし
110	CERT	THIRD	T.STEAL	T.STEAL_CERT_THIRD	機密性不要のため脅威外
111	CERT	THIRD	T.DISCLOSE	T.DISCLOSE_CERT_THIRD	機密性不要のため脅威外
112	CRL-ARL	USER	T.FORGERY	T.FORGERY_CRL-ARL_USER	偽造したCRL･ARLをサーバに登録

項番	資産	主体	汎用脅威	脅威名	脅威内容
113	CRL-ARL	USER	T.MODIFY	T.MODIFY_CRL-ARL_USER	サーバに登録されたCRL･ARLを改竄
114	CRL-ARL	USER	T.ERACE	T.ERACE_CRL-ARL_USER	サーバに登録されたCRL･ARLを消去
115	CRL-ARL	USER	T.IMPERSON	T.IMPERSON_CRL-ARL_USER	発行者への成り済まし
116	CRL-ARL	USER	T.STEAL	T.STEAL_CRL-ARL_USER	機密性不要のため脅威外
117	CRL-ARL	USER	T.DISCLOSE	T.DISCLOSE_CRL-ARL_USER	機密性不要のため脅威外
118	CRL-ARL	THIRD	T.FORGERY	T.FORGERY_CRL-ARL_THIRD	偽造したCRL･ARLをサーバに登録
119	CRL-ARL	THIRD	T.MODIFY	T.MODIFY_CRL-ARL_THIRD	サーバに登録されたCRL･ARLを改竄
120	CRL-ARL	THIRD	T.ERACE	T.ERACE_CRL-ARL_THIRD	サーバに登録されたCRL･ARLを消去
121	CRL-ARL	THIRD	T.IMPERSON	T.IMPERSON_CRL-ARL_THIRD	発行者への成り済まし
122	CRL-ARL	THIRD	T.STEAL	T.STEAL_CRL-ARL_THIRD	機密性不要のため脅威外
123	CRL-ARL	THIRD	T.DISCLOSE	T.DISCLOSE_CRL-ARL_THIRD	機密性不要のため脅威外
124	PRI-KEY	USER	T.FORGERY	T.FORGERY_PRI-KEY_USER	偽造した秘密鍵を登録
125	PRI-KEY	USER	T.MODIFY	T.MODIFY_PRI-KEY_USER	改竄した秘密鍵を登録
126	PRI-KEY	USER	T.ERACE	T.ERACE_PRI-KEY_USER	サーバに登録された秘密鍵の消去
127	PRI-KEY	USER	T.IMPERSON	T.IMPERSON_PRI-KEY_USER	アクセス権所有者への成り済まし
128	PRI-KEY	USER	T.STEAL	T.STEAL_PRI-KEY_USER	平文の秘密鍵を不正に取得
129	PRI-KEY	USER	T.DISCLOSE	T.DISCLOSE_PRI-KEY_USER	平文の秘密鍵の中身を不正に漏洩
130	PRI-KEY	THIRD	T.FORGERY	T.FORGERY_PRI-KEY_THIRD	偽造した秘密鍵を登録
131	PRI-KEY	THIRD	T.MODIFY	T.MODIFY_PRI-KEY_THIRD	改竄した秘密鍵を登録
132	PRI-KEY	THIRD	T.ERACE	T.ERACE_PRI-KEY_THIRD	サーバに登録された秘密鍵の消去
133	PRI-KEY	THIRD	T.IMPERSON	T.IMPERSON_PRI-KEY_THIRD	アクセス権所有者への成り済まし
134	PRI-KEY	THIRD	T.STEAL	T.STEAL_PRI-KEY_THIRD	平文の秘密鍵を不正に取得
135	PRI-KEY	THIRD	T.DISCLOSE	T.DISCLOSE_PRI-KEY_THIRD	平文の秘密鍵の中身を不正に漏洩
136	PRI-KEY-PW	USER	T.FORGERY	T.FORGERY_PRI-KEY-PW_USER	偽造したPWをサーバに登録
137	PRI-KEY-PW	USER	T.MODIFY	T.MODIFY_PRI-KEY-PW_USER	サーバに登録されたPWを改竄
138	PRI-KEY-PW	USER	T.ERACE	T.ERACE_PRI-KEY-PW_USER	サーバに登録されたPWを消去
139	PRI-KEY-PW	USER	T.IMPERSON	T.IMPERSON_PRI-KEY-PW_USER	アクセス権所有者への成り済まし
140	PRI-KEY-PW	USER	T.STEAL	T.STEAL_PRI-KEY-PW_USER	サーバに登録されたPWを不正に取得
141	PRI-KEY-PW	USER	T.DISCLOSE	T.DISCLOSE_PRI-KEY-PW_USER	サーバに登録されたPWを不正に漏洩
142	PRI-KEY-PW	THIRD	T.FORGERY	T.FORGERY_PRI-KEY-PW_THIRD	偽造したPWをサーバに登録
143	PRI-KEY-PW	THIRD	T.MODIFY	T.MODIFY_PRI-KEY-PW_THIRD	サーバに登録されたPWを改竄
144	PRI-KEY-PW	THIRD	T.ERACE	T.ERACE_PRI-KEY-PW_THIRD	サーバに登録されたPWを消去
145	PRI-KEY-PW	THIRD	T.IMPERSON	T.IMPERSON_PRI-KEY-PW_THIRD	アクセス権所有者への成り済まし
146	PRI-KEY-PW	THIRD	T.STEAL	T.STEAL_PRI-KEY-PW_THIRD	サーバに登録されたPWを不正に取得
147	PRI-KEY-PW	THIRD	T.DISCLOSE	T.DISCLOSE_PRI-KEY-PW_THIRD	サーバに登録されたPWを不正に漏洩
148	OPE-ID-PW	USER	T.FORGERY	T.FORGERY_OPE-ID-PW_USER	偽造したID/PWをサーバに登録
149	OPE-ID-PW	USER	T.MODIFY	T.MODIFY_OPE-ID-PW_USER	サーバに登録されたID/PWを改竄
150	OPE-ID-PW	USER	T.ERACE	T.ERACE_OPE-ID-PW_USER	サーバに登録されたID/PWを消去
151	OPE-ID-PW	USER	T.IMPERSON	T.IMPERSON_OPE-ID-PW_USER	アクセス権所有者への成り済まし
152	OPE-ID-PW	USER	T.STEAL	T.STEAL_OPE-ID-PW_USER	サーバに登録されたID/PWを不正に取得
153	OPE-ID-PW	USER	T.DISCLOSE	T.DISCLOSE_OPE-ID-PW_USER	サーバに登録されたID/PWを不正に漏洩
154	OPE-ID-PW	THIRD	T.FORGERY	T.FORGERY_OPE-ID-PW_THIRD	偽造したID/PWをサーバに登録
155	OPE-ID-PW	THIRD	T.MODIFY	T.MODIFY_OPE-ID-PW_THIRD	サーバに登録されたID/PWを改竄
156	OPE-ID-PW	THIRD	T.ERACE	T.ERACE_OPE-ID-PW_THIRD	サーバに登録されたID/PWを消去
157	OPE-ID-PW	THIRD	T.IMPERSON	T.IMPERSON_OPE-ID-PW_THIRD	アクセス権所有者への成り済まし
158	OPE-ID-PW	THIRD	T.STEAL	T.STEAL_OPE-ID-PW_THIRD	サーバに登録されたID/PWを不正に取得
159	OPE-ID-PW	THIRD	T.DISCLOSE	T.DISCLOSE_OPE-ID-PW_THIRD	サーバに登録されたID/PWを不正に漏洩
160	DB-SERIAL	USER	T.FORGERY	T.FORGERY_DB-SERIAL_USER	偽造したシリアル番号をDBに登録
161	DB-SERIAL	USER	T.MODIFY	T.MODIFY_DB-SERIAL_USER	DB内のシリアル番号を改竄
162	DB-SERIAL	USER	T.ERACE	T.ERACE_DB-SERIAL_USER	DB内のシリアル番号を消去
163	DB-SERIAL	USER	T.IMPERSON	T.IMPERSON_DB-SERIAL_USER	アクセス権所有者への成り済まし
164	DB-SERIAL	USER	T.STEAL	T.STEAL_DB-SERIAL_USER	DB内のシリアル番号を不正に取得
165	DB-SERIAL	USER	T.DISCLOSE	T.DISCLOSE_DB-SERIAL_USER	DB内のシリアル番号を不正に漏洩
166	DB-SERIAL	THIRD	T.FORGERY	T.FORGERY_DB-SERIAL_THIRD	偽造したシリアル番号をDBに登録
167	DB-SERIAL	THIRD	T.MODIFY	T.MODIFY_DB-SERIAL_THIRD	DB内のシリアル番号を改竄
168	DB-SERIAL	THIRD	T.ERACE	T.ERACE_DB-SERIAL_THIRD	DB内のシリアル番号を消去
169	DB-SERIAL	THIRD	T.IMPERSON	T.IMPERSON_DB-SERIAL_THIRD	アクセス権所有者への成り済まし
170	DB-SERIAL	THIRD	T.STEAL	T.STEAL_DB-SERIAL_THIRD	DB内のシリアル番号を不正に取得
171	DB-SERIAL	THIRD	T.DISCLOSE	T.DISCLOSE_DB-SERIAL_THIRD	DB内のシリアル番号を不正に漏洩
172	DB-USER-ID	USER	T.FORGERY	T.FORGERY_DB-USER-ID_USER	偽造した利用者IDをDBに登録
173	DB-USER-ID	USER	T.MODIFY	T.MODIFY_DB-USER-ID_USER	DB内の利用者IDを改竄

項番	資産	主体	汎用脅威	脅威名	脅威内容
174	DB-USER-ID	USER	T.ERACE	T.ERACE_DB-USER-ID_USER	DB内の利用者IDを消去
175	DB-USER-ID	USER	T.IMPERSON	T.IMPERSON_DB-USER-ID_USER	アクセス権所有者への成り済まし
176	DB-USER-ID	USER	T.STEAL	T.STEAL_DB-USER-ID_USER	DB内の利用者IDを不正に取得
177	DB-USER-ID	USER	T.DISCLOSE	T.DISCLOSE_DB-USER-ID_USER	DB内の利用者IDを不正に漏洩
178	DB-USER-ID	THIRD	T.FORGERY	T.FORGERY_DB-USER-ID_THIRD	偽造した利用者IDをDBに登録
179	DB-USER-ID	THIRD	T.MODIFY	T.MODIFY_DB-USER-ID_THIRD	DB内の利用者IDを改竄
180	DB-USER-ID	THIRD	T.ERACE	T.ERACE_DB-USER-ID_THIRD	DB内の利用者IDを消去
181	DB-USER-ID	THIRD	T.IMPERSON	T.IMPERSON_DB-USER-ID_THIRD	アクセス権所有者への成り済まし
182	DB-USER-ID	THIRD	T.STEAL	T.STEAL_DB-USER-ID_THIRD	DB内の利用者IDを不正に取得
183	DB-USER-ID	THIRD	T.DISCLOSE	T.DISCLOSE_DB-USER-ID_THIRD	DB内の利用者IDを不正に漏洩
184	DB-TIME	USER	T.FORGERY	T.FORGERY_DB-TIME_USER	偽造した発行時刻をDBに登録
185	DB-TIME	USER	T.MODIFY	T.MODIFY_DB-TIME_USER	DB内の発行時刻を改竄
186	DB-TIME	USER	T.ERACE	T.ERACE_DB-TIME_USER	DB内の発行時刻を消去
187	DB-TIME	USER	T.IMPERSON	T.IMPERSON_DB-TIME_USER	アクセス権所有者への成り済まし
188	DB-TIME	USER	T.STEAL	T.STEAL_DB-TIME_USER	DB内の発行時刻を不正に取得
189	DB-TIME	USER	T.DISCLOSE	T.DISCLOSE_DB-TIME_USER	DB内の発行時刻を不正に漏洩
190	DB-TIME	THIRD	T.FORGERY	T.FORGERY_DB-TIME_THIRD	偽造した発行時刻をDBに登録
191	DB-TIME	THIRD	T.MODIFY	T.MODIFY_DB-TIME_THIRD	DB内の発行時刻を改竄
192	DB-TIME	THIRD	T.ERACE	T.ERACE_DB-TIME_THIRD	DB内の発行時刻を消去
193	DB-TIME	THIRD	T.IMPERSON	T.IMPERSON_DB-TIME_THIRD	アクセス権所有者への成り済まし
194	DB-TIME	THIRD	T.STEAL	T.STEAL_DB-TIME_THIRD	DB内の発行時刻を不正に取得
195	DB-TIME	THIRD	T.DISCLOSE	T.DISCLOSE_DB-TIME_THIRD	DB内の発行時刻を不正に漏洩
196	DB-TST	USER	T.FORGERY	T.FORGERY_DB-TST_USER	偽造したTSTをDBに登録
197	DB-TST	USER	T.MODIFY	T.MODIFY_DB-TST_USER	DB内のTSTを改竄
198	DB-TST	USER	T.ERACE	T.ERACE_DB-TST_USER	DB内のTSTを消去
199	DB-TST	USER	T.IMPERSON	T.IMPERSON_DB-TST_USER	アクセス権所有者への成り済まし
200	DB-TST	USER	T.STEAL	T.STEAL_DB-TST_USER	DB内のTSTを不正に取得
201	DB-TST	USER	T.DISCLOSE	T.DISCLOSE_DB-TST_USER	DB内のTSTを不正に漏洩
202	DB-TST	THIRD	T.FORGERY	T.FORGERY_DB-TST_THIRD	偽造したTSTをDBに登録
203	DB-TST	THIRD	T.MODIFY	T.MODIFY_DB-TST_THIRD	DB内のTSTを改竄
204	DB-TST	THIRD	T.ERACE	T.ERACE_DB-TST_THIRD	DB内のTSTを消去
205	DB-TST	THIRD	T.IMPERSON	T.IMPERSON_DB-TST_THIRD	アクセス権所有者への成り済まし
206	DB-TST	THIRD	T.STEAL	T.STEAL_DB-TST_THIRD	DB内のTSTを不正に取得
207	DB-TST	THIRD	T.DISCLOSE	T.DISCLOSE_DB-TST_THIRD	DB内のTSTを不正に漏洩
208	LINK	USER	T.FORGERY	T.FORGERY_LINK_USER	偽造したリンク情報をサーバに登録
209	LINK	USER	T.MODIFY	T.MODIFY_LINK_USER	サーバに登録されたリンク情報を改竄
210	LINK	USER	T.ERACE	T.ERACE_LINK_USER	サーバに登録されたリンク情報を消去
211	LINK	USER	T.IMPERSON	T.IMPERSON_LINK_USER	アクセス権所有者への成り済まし
212	LINK	USER	T.STEAL	T.STEAL_LINK_USER	機密性不要のため脅威外
213	LINK	USER	T.DISCLOSE	T.DISCLOSE_LINK_USER	機密性不要のため脅威外
214	LINK	THIRD	T.FORGERY	T.FORGERY_LINK_THIRD	偽造したリンク情報をサーバに登録
215	LINK	THIRD	T.MODIFY	T.MODIFY_LINK_THIRD	サーバに登録されたリンク情報を改竄
216	LINK	THIRD	T.ERACE	T.ERACE_LINK_THIRD	サーバに登録されたリンク情報を消去
217	LINK	THIRD	T.IMPERSON	T.IMPERSON_LINK_THIRD	アクセス権所有者への成り済まし
218	LINK	THIRD	T.STEAL	T.STEAL_LINK_THIRD	機密性不要のため脅威外
219	LINK	THIRD	T.DISCLOSE	T.DISCLOSE_LINK_THIRD	機密性不要のため脅威外
220	CONFIG	USER	T.FORGERY	T.FORGERY_CONFIG_USER	偽造した設定情報をサーバに登録
221	CONFIG	USER	T.MODIFY	T.MODIFY_CONFIG_USER	サーバ内の設定情報を改竄
222	CONFIG	USER	T.ERACE	T.ERACE_CONFIG_USER	サーバ内の設定情報を消去
223	CONFIG	USER	T.IMPERSON	T.IMPERSON_CONFIG_USER	アクセス権所有者への成り済まし
224	CONFIG	USER	T.STEAL	T.STEAL_CONFIG_USER	サーバ内の設定情報を不正に取得
225	CONFIG	USER	T.DISCLOSE	T.DISCLOSE_CONFIG_USER	サーバ内の設定情報を不正に漏洩
226	CONFIG	THIRD	T.FORGERY	T.FORGERY_CONFIG_THIRD	偽造した設定情報をサーバに登録
227	CONFIG	THIRD	T.MODIFY	T.MODIFY_CONFIG_THIRD	サーバ内の設定情報を改竄
228	CONFIG	THIRD	T.ERACE	T.ERACE_CONFIG_THIRD	サーバ内の設定情報を消去
229	CONFIG	THIRD	T.IMPERSON	T.IMPERSON_CONFIG_THIRD	アクセス権所有者への成り済まし
230	CONFIG	THIRD	T.STEAL	T.STEAL_CONFIG_THIRD	サーバ内の設定情報を不正に取得
231	CONFIG	THIRD	T.DISCLOSE	T.DISCLOSE_CONFIG_THIRD	サーバ内の設定情報を不正に漏洩
232	DB-ID-PW	USER	T.FORGERY	T.FORGERY_DB-ID-PW_USER	偽造したID/PWをサーバに登録
233	DB-ID-PW	USER	T.MODIFY	T.MODIFY_DB-ID-PW_USER	サーバに登録されたID/PWを改竄
234	DB-ID-PW	USER	T.ERACE	T.ERACE_DB-ID-PW_USER	サーバに登録されたID/PWを消去

項番	資産	主体	汎用脅威	脅威名	脅威内容
235	DB-ID-PW	USER	T.IMPERSON	T.IMPERSON_DB-ID-PW_USER	アクセス権所有者への成り済まし
236	DB-ID-PW	USER	T.STEAL	T.STEAL_DB-ID-PW_USER	サーバに登録されたID/PWを不正に取得
237	DB-ID-PW	USER	T.DISCLOSE	T.DISCLOSE_DB-ID-PW_USER	サーバに登録されたID/PWを不正に漏洩
238	DB-ID-PW	THIRD	T.FORGERY	T.FORGERY_DB-ID-PW_THIRD	偽造したID/PWをサーバに登録
239	DB-ID-PW	THIRD	T.MODIFY	T.MODIFY_DB-ID-PW_THIRD	サーバに登録されたID/PWを改竄
240	DB-ID-PW	THIRD	T.ERACE	T.ERACE_DB-ID-PW_THIRD	サーバに登録されたID/PWを消去
241	DB-ID-PW	THIRD	T.IMPERSON	T.IMPERSON_DB-ID-PW_THIRD	アクセス権所有者への成り済まし
242	DB-ID-PW	THIRD	T.STEAL	T.STEAL_DB-ID-PW_THIRD	サーバに登録されたID/PWを不正に取得
243	DB-ID-PW	THIRD	T.DISCLOSE	T.DISCLOSE_DB-ID-PW_THIRD	サーバに登録されたID/PWを不正に漏洩
244	LINK-PROV	USER	T.FORGERY	T.FORGERY_LINK-PROV_USER	リンク情報の代表値を偽造
245	LINK-PROV	USER	T.MODIFY	T.MODIFY_LINK-PROV_USER	明証化されたリンク情報の代表値を改竄
246	LINK-PROV	USER	T.ERACE	T.ERACE_LINK-PROV_USER	明証化されたリンク情報の代表値を消去
247	LINK-PROV	USER	T.IMPERSON	T.IMPERSON_LINK-PROV_USER	明証化主体やアクセス権所有者への成り済まし
248	LINK-PROV	USER	T.STEAL	T.STEAL_LINK-PROV_USER	機密性不要のため脅威外
249	LINK-PROV	USER	T.DISCLOSE	T.DISCLOSE_LINK-PROV_USER	機密性不要のため脅威外
250	LINK-PROV	THIRD	T.FORGERY	T.FORGERY_LINK-PROV_THIRD	リンク情報の代表値を偽造
251	LINK-PROV	THIRD	T.MODIFY	T.MODIFY_LINK-PROV_THIRD	明証化されたリンク情報の代表値を改竄
252	LINK-PROV	THIRD	T.ERACE	T.ERACE_LINK-PROV_THIRD	明証化されたリンク情報の代表値を消去
253	LINK-PROV	THIRD	T.IMPERSON	T.IMPERSON_LINK-PROV_THIRD	明証化主体やアクセス権所有者への成り済まし
254	LINK-PROV	THIRD	T.STEAL	T.STEAL_LINK-PROV_THIRD	機密性不要のため脅威外
255	LINK-PROV	THIRD	T.DISCLOSE	T.DISCLOSE_LINK-PROV_THIRD	機密性不要のため脅威外
256	EVENT	USER	T.FORGERY	T.FORGERY_EVENT_USER	偽造した動作記録をサーバに登録
257	EVENT	USER	T.MODIFY	T.MODIFY_EVENT_USER	サーバ内の動作記録を改竄
258	EVENT	USER	T.ERACE	T.ERACE_EVENT_USER	サーバ内の動作記録を消去
259	EVENT	USER	T.IMPERSON	T.IMPERSON_EVENT_USER	アクセス権所有者への成り済まし
260	EVENT	USER	T.STEAL	T.STEAL_EVENT_USER	サーバ内の動作記録を不正に取得
261	EVENT	USER	T.DISCLOSE	T.DISCLOSE_EVENT_USER	サーバ内の動作記録を不正に漏洩
262	EVENT	THIRD	T.FORGERY	T.FORGERY_EVENT_THIRD	偽造した動作記録をサーバに登録
263	EVENT	THIRD	T.MODIFY	T.MODIFY_EVENT_THIRD	サーバ内の動作記録を改竄
264	EVENT	THIRD	T.ERACE	T.ERACE_EVENT_THIRD	サーバ内の動作記録を消去
265	EVENT	THIRD	T.IMPERSON	T.IMPERSON_EVENT_THIRD	アクセス権所有者への成り済まし
266	EVENT	THIRD	T.STEAL	T.STEAL_EVENT_THIRD	サーバ内の動作記録を不正に取得
267	EVENT	THIRD	T.DISCLOSE	T.DISCLOSE_EVENT_THIRD	サーバ内の動作記録を不正に漏洩
268	CLOCK	USER	T.FORGERY	T.FORGERY_CLOCK_USER	偽造したシステムクロックの登録
269	CLOCK	USER	T.MODIFY	T.MODIFY_CLOCK_USER	システムクロックの改竄
270	CLOCK	USER	T.ERACE	T.ERACE_CLOCK_USER	システムクロックの消去
271	CLOCK	USER	T.IMPERSON	T.IMPERSON_CLOCK_USER	アクセス権所有者への成り済まし
272	CLOCK	USER	T.STEAL	T.STEAL_CLOCK_USER	機密性不要のため脅威外
273	CLOCK	USER	T.DISCLOSE	T.DISCLOSE_CLOCK_USER	機密性不要のため脅威外
274	CLOCK	THIRD	T.FORGERY	T.FORGERY_CLOCK_THIRD	偽造したシステムクロックの登録
275	CLOCK	THIRD	T.MODIFY	T.MODIFY_CLOCK_THIRD	システムクロックの改竄
276	CLOCK	THIRD	T.ERACE	T.ERACE_CLOCK_THIRD	システムクロックの消去
277	CLOCK	THIRD	T.IMPERSON	T.IMPERSON_CLOCK_THIRD	アクセス権所有者への成り済まし
278	CLOCK	THIRD	T.STEAL	T.STEAL_CLOCK_THIRD	機密性不要のため脅威外
279	CLOCK	THIRD	T.DISCLOSE	T.DISCLOSE_CLOCK_THIRD	機密性不要のため脅威外
280	MOD-CRE-TS	USER	T.FORGERY	T.FORGERY_MOD-CRE-TS_USER	偽造したTS生成モジュールへの差替え
281	MOD-CRE-TS	USER	T.MODIFY	T.MODIFY_MOD-CRE-TS_USER	TS生成モジュールを改竄
282	MOD-CRE-TS	USER	T.ERACE	T.ERACE_MOD-CRE-TS_USER	TS生成モジュールを消去
283	MOD-CRE-TS	USER	T.IMPERSON	T.IMPERSON_MOD-CRE-TS_USER	アクセス権所有者への成り済まし
284	MOD-CRE-TS	USER	T.STEAL	T.STEAL_MOD-CRE-TS_USER	TS生成モジュールを不正に取得
285	MOD-CRE-TS	USER	T.DISCLOSE	T.DISCLOSE_MOD-CRE-TS_USER	TS生成モジュールを不正に漏洩
286	MOD-CRE-TS	THIRD	T.FORGERY	T.FORGERY_MOD-CRE-TS_THIRD	偽造したTS生成モジュールへの差替え
287	MOD-CRE-TS	THIRD	T.MODIFY	T.MODIFY_MOD-CRE-TS_THIRD	TS生成モジュールを改竄
288	MOD-CRE-TS	THIRD	T.ERACE	T.ERACE_MOD-CRE-TS_THIRD	TS生成モジュールを消去
289	MOD-CRE-TS	THIRD	T.IMPERSON	T.IMPERSON_MOD-CRE-TS_THIRD	アクセス権所有者への成り済まし
290	MOD-CRE-TS	THIRD	T.STEAL	T.STEAL_MOD-CRE-TS_THIRD	TS生成モジュールを不正に取得
291	MOD-CRE-TS	THIRD	T.DISCLOSE	T.DISCLOSE_MOD-CRE-TS_THIRD	TS生成モジュールを不正に漏洩
292	MOD-STORE	USER	T.FORGERY	T.FORGERY_MOD-STORE_USER	偽造した保管モジュールへの差替え
293	MOD-STORE	USER	T.MODIFY	T.MODIFY_MOD-STORE_USER	保管モジュールを改竄
294	MOD-STORE	USER	T.ERACE	T.ERACE_MOD-STORE_USER	保管モジュールを消去
295	MOD-STORE	USER	T.IMPERSON	T.IMPERSON_MOD-STORE_USER	アクセス権所有者への成り済まし

項番	資産	主体	汎用脅威	脅威名	脅威内容
296	MOD-STORE	USER	T.STEAL	T.STEAL_MOD-STORE_USER	保管モジュールを不正に取得
297	MOD-STORE	USER	T.DISCLOSE	T.DISCLOSE_MOD-STORE_USER	保管モジュールを不正に漏洩
298	MOD-STORE	THIRD	T.FORGERY	T.FORGERY_MOD-STORE_THIRD	偽造した保管モジュールへの差替え
299	MOD-STORE	THIRD	T.MODIFY	T.MODIFY_MOD-STORE_THIRD	保管モジュールを改竄
300	MOD-STORE	THIRD	T.ERACE	T.ERACE_MOD-STORE_THIRD	保管モジュールを消去
301	MOD-STORE	THIRD	T.IMPERSON	T.IMPERSON_MOD-STORE_THIRD	アクセス権所有者への成り済まし
302	MOD-STORE	THIRD	T.STEAL	T.STEAL_MOD-STORE_THIRD	保管モジュールを不正に取得
303	MOD-STORE	THIRD	T.DISCLOSE	T.DISCLOSE_MOD-STORE_THIRD	保管モジュールを不正に漏洩
304	MOD-COM-TS	USER	T.FORGERY	T.FORGERY_MOD-COM-TS_USER	偽造したTS照合モジュールへの差替え
305	MOD-COM-TS	USER	T.MODIFY	T.MODIFY_MOD-COM-TS_USER	TS照合モジュールを改竄
306	MOD-COM-TS	USER	T.ERACE	T.ERACE_MOD-COM-TS_USER	TS照合モジュールを消去
307	MOD-COM-TS	USER	T.IMPERSON	T.IMPERSON_MOD-COM-TS_USER	アクセス権所有者への成り済まし
308	MOD-COM-TS	USER	T.STEAL	T.STEAL_MOD-COM-TS_USER	TS照合モジュールを不正に取得
309	MOD-COM-TS	USER	T.DISCLOSE	T.DISCLOSE_MOD-COM-TS_USER	TS照合モジュールを不正に漏洩
310	MOD-COM-TS	THIRD	T.FORGERY	T.FORGERY_MOD-COM-TS_THIRD	偽造したTS照合モジュールへの差替え
311	MOD-COM-TS	THIRD	T.MODIFY	T.MODIFY_MOD-COM-TS_THIRD	TS照合モジュールを改竄
312	MOD-COM-TS	THIRD	T.ERACE	T.ERACE_MOD-COM-TS_THIRD	TS照合モジュールを消去
313	MOD-COM-TS	THIRD	T.IMPERSON	T.IMPERSON_MOD-COM-TS_THIRD	アクセス権所有者への成り済まし
314	MOD-COM-TS	THIRD	T.STEAL	T.STEAL_MOD-COM-TS_THIRD	TS照合モジュールを不正に取得
315	MOD-COM-TS	THIRD	T.DISCLOSE	T.DISCLOSE_MOD-COM-TS_THIRD	TS照合モジュールを不正に漏洩
316	MOD-TIME	USER	T.FORGERY	T.FORGERY_MOD-TIME_USER	偽造した時刻受信モジュールへの差替え
317	MOD-TIME	USER	T.MODIFY	T.MODIFY_MOD-TIME_USER	時刻受信モジュールを改竄
318	MOD-TIME	USER	T.ERACE	T.ERACE_MOD-TIME_USER	時刻受信モジュールを消去
319	MOD-TIME	USER	T.IMPERSON	T.IMPERSON_MOD-TIME_USER	アクセス権所有者への成り済まし
320	MOD-TIME	USER	T.STEAL	T.STEAL_MOD-TIME_USER	時刻受信モジュールを不正に取得
321	MOD-TIME	USER	T.DISCLOSE	T.DISCLOSE_MOD-TIME_USER	時刻受信モジュールを不正に漏洩
322	MOD-TIME	THIRD	T.FORGERY	T.FORGERY_MOD-TIME_THIRD	偽造した時刻受信モジュールへの差替え
323	MOD-TIME	THIRD	T.MODIFY	T.MODIFY_MOD-TIME_THIRD	時刻受信モジュールを改竄
324	MOD-TIME	THIRD	T.ERACE	T.ERACE_MOD-TIME_THIRD	時刻受信モジュールを消去
325	MOD-TIME	THIRD	T.IMPERSON	T.IMPERSON_MOD-TIME_THIRD	アクセス権所有者への成り済まし
326	MOD-TIME	THIRD	T.STEAL	T.STEAL_MOD-TIME_THIRD	時刻受信モジュールを不正に取得
327	MOD-TIME	THIRD	T.DISCLOSE	T.DISCLOSE_MOD-TIME_THIRD	時刻受信モジュールを不正に漏洩

3. 組織のセキュリティポリシー

TOE に係るセキュリティ環境の組織のセキュリティポリシー一覧を、以下の表 7に示す。

表 7　TOE に係るセキュリティ環境の組織のセキュリティポリシー一覧

#	項目	説明
1	P.CRYPTO	全ての暗号処理は、「電子政府推奨暗号リスト(平成 15 年 2 月 20 日、総務省、経済産業省)」に記載されたアルゴリズムによって実装される。
2	P.PUBLISH	リンクデータ及び照合用データの関連性と完全性を証明するため、リンクデータの代表値は定期的に明証化される。
3	P.TIME_ SOURCE	TOE は、信頼できる時刻ソースを参照すること。この時刻ソースは、TOE 所有者にとってアベイラブルであること。また、時刻ソースの信頼性と正確性は TOE 所有者にとって受容可能であること。
4	P.SYSTM_CLOCK_ MANAGEMENT	TOE が参照するシステム時計を TA1 の時刻ソースと同期させる。
5	P.PKI_ MANAGEMENT	安全に管理された PKI の中で、TOE を運用すること。 全ての鍵と証明書は、安全に発行、失効される。
6	P.PROTECT_LOG	TOE を利用する組織は、監査ログの暴露、改竄、または削除の防止のために必要な措置をとることとする。
7	P.PASSWORD_ MANAGEMENT	TOE の管理者及び運用者のパスワードは、本人によって適切に管理され、本人以外に知られることはないものとする。 SSL アクセスパスワード及び DB アクセスパスワードは、適切に管理される。
8	P.CHECK_VIRUS	定期的なウイルスチェックを実行する。
9	P.DUAL_CONTROL	TOE の管理業務における重要な操作は、TOE 管理者を含む複数人による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
10	P.CHECK_ABSTRACT_ VULNERABILITY	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

第3章 セキュリティ目標・対策と実装システムの評価

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

脅威のセキュリティ目標に含まれる対策名と実装システムに対する評価一覧を、以下の表 8に示す。

表 8　脅威のセキュリティ目標に含まれる対策名と実装システムに対する評価一覧

項番	種別	対策名	説明	統合化システムにおける実現
1	防止	M.AC	TOEに対する適切なアクセス管理	OS等によるファイルアクセスの設定により実施。
2	防止	M.CA_SIGN	認証局によるデジタル署名付与	公開鍵証明書、CRL及びARLに対して、認証局によるデジタル署名の付与を実施。
3	防止	M.CRY_MULTI	暗号アルゴリズムの二重化	ドキュメントハッシュ及びリンク情報の計算において、2種類のハッシュ関数を並列に使用。
4	防止	M.CRY_RECOM	公的な評価機関により推奨されている暗号アルゴリズムの利用	全ての暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」に記載されたアルゴリズムによって実装。
5	防止	M.DUAL	複数人による相互牽制の下での運用	複数人運用に係る運用手順の整備と徹底により、実現可能。
6	防止	M.FAC_ISO	隔離され入退室管理が施された室へのサーバ機器の設置	入退室管理が施されたiDCへの設置等により、実現可能。
7	防止	M.FW	TOEと外部ネットワークとの接続点におけるファイアウォールによる不要通信遮断	TOEとインターネット及び他サブシステムとの接続点において、ファイアウォールによる不要通信遮断を実施。
8	防止	M.HASH_REJECT	不正な長さもしくはアルゴリズムのハッシュ値を含むタイムスタンプ要求の棄却	タイムスタンプ付与要求の受領時に、規定外のハッシュ値を含むタイムスタンプ要求の棄却を実施。
9	防止	M.HW_RED	TOEの機器の冗長化構成	TOEの機器の追加による冗長化等により実現可能。
10	防止	M.KEEP_TST_NOT	タイムスタンプの効力を確保する上でのタイムスタンプトークンの保持の必要性に関する利用者通知	利用規約等により説明事項を通知することにより、実現可能。
11	防止	M.LINK_GEN	TSTの非改竄性と順序性を証明するリンク情報の生成	タイムスタンプ発行時にリンク情報の生成を実施。
12	防止	M.LINK_PROV	リンク情報の代表値の明証化	新聞等の定期刊行物にリンク情報の代表値を掲載することにより、実現可能。
13	防止	M.NW_RED	通信回線の冗長化構成	複数の冗長な通信回線の利用により、実現可能。
14	防止	M.NW_REL	高信頼な通信回線の利用	高信頼な通信サービスの採用により、実現可能。
15	防止	M.PEER_RED	複数の他システムの冗長な使用	複数の冗長な同業サービスの利用等により、実現可能。
16	防止	M.PEER_REL	通信相手の他システムの高信頼化	通信相手の他システムの冗長化構成等により、実現可能。
17	防止	M.PROV	定期刊行物掲載（国会図書館への納本）等の長期間正しく保持される媒体による明証化	出版社との定常的な契約により実現可能。
18	防止	M.PW_LOCK	パスワードによるデータの暗号化	鍵データ等についてパスワードによる暗号化を実施。
19	防止	M.SSL_AUTH	タイムスタンプの発行及び検証時のSSL通信によるサーバ認証	タイムスタンプ発行及び検証時に、SSL通信によるサーバ認証を実施。
20	防止	M.SYS_TEST	TOEのシステムの動作試験	システムの動作試験を実施。
21	防止	M.TA_DELI	TAによる時刻配信	TAによる時刻配信を受信。

項番	種別	対策名	説明	統合化システムにおける実現
22	防止	M.TA_SIGN	TAによるデジタル署名付与	時刻監査結果を証明するデータに対して、TAによるデジタル署名の付与を実施。
23	防止	M.TS_ARCH	タイムスタンプの再付与による長期保証	「タイムスタンプ長期保証ガイドラインVer.1.2(平成17年10月、タイムビジネス推進協議会)」に記載された方法に対応したモジュールを準備することにより、実施可能。
24	防止	M.TST_VAL_PUB	タイムスタンプトークンのプロファイル及び検証方法の公表	TSAポリシー等により公表することにより、実現可能。
25	防止	M.USER_PW	ID/パスワードによる利用者認証	タイムスタンプ発行及び検証時に、ID/パスワードによる利用者認証を実施。
26	防止	M.USER_PW_NOT	利用者へのID/パスワードの機密性管理の必要性に係る通知	利用規約等により説明事項を通知することにより、実現可能。
27	防止	M.VUL_CHECK	セキュリティ診断によるシステムの脆弱性チェック及び対策	セキュリティ診断によるシステムの脆弱性チェック及び対策を実施。
28	検出	M.AUTH_FAIL	TOE自らの認証処理失敗の検出	TAとの通信時にはTLS、VA及び利用者との通信時にはSSLによる認証を実施。
29	検出	M.CA_SIGN_VERI	認証局により付与されたデジタル署名の検証	標準的なブラウザ等により、デジタル署名の検証を実施可能。
30	検出	M.CLI_ERR	クライアントモジュールにおけるエラー出力	エラーが確認できるクライアントアプリケーションを準備することにより、実現可能。
31	検出	M.CRY_CHECK	公的な評価機関による暗号アルゴリズムの評価結果のチェック	最新の「電子政府推奨暗号リスト」の内容をチェックすることにより、実施可能。
32	検出	M.ERR_CHECK	TOEで出力されるエラーの常時チェック	エラーの監視サービスの利用等により、実現可能。
33	検出	M.HASH_CHECK	TOEでのタイムスタンプ要求に含まれるハッシュ値のチェック	タイムスタンプ付与要求の受領時に、TOEにおいてハッシュ値のチェックを実施。
34	検出	M.HW_CHECK	TOEの機器の稼働状況のチェック	機器の稼働状況の監視サービスの利用等により、実現可能。
35	検出	M.IDS	TOEと外部ネットワークとの接続点における侵入検知システムによる攻撃検知	IDSを準備し、設置及び運用することにより、実現可能。
36	検出	M.LINK_AUDIT	リンク情報の整合性に関する監査	リンク情報を再計算し比較することにより、実現可能。
37	検出	M.LINK_PROV_COMP	明証化されたリンク情報の代表値との比較	リンク情報の代表値の定期刊行物への掲載等により、実現可能。
38	検出	M.LINK_PROV_LOST	明証化されたリンク情報の代表値の紛失の検出	リンク情報の代表値の定期的な確認により、実現可能。
39	検出	M.LOG_AUDIT	TOEの動作ログの監査	動作ログの定期的な確認により実現可能。
40	検出	M.MOD_WATCH	TOEのプログラムの完全性及びプロセスの稼働状態の監視	プログラム及びプロセスの監視システムの利用により、実現可能。
41	検出	M.NW_FAIL_DET	通信不能の検出	通信状態の監視等により実現可能。
42	検出	M.NW_NOT	通信回線の運営者からの通知	障害発生時の通知規定のある通信サービスの利用により、実現可能。
43	検出	M.PEER_FAIL_DET	通信相手の他システムの無応答もしくは異常応答の検出	通信相手とのやり取りの監視等により、実現可能。
44	検出	M.PEER_NOT	通信相手の他システムからの通知	障害発生時の通知規定のあるサービスの利用により、実現可能。
45	検出	M.SSL_AUTH_FAIL	SSL通信時のサーバ認証失敗の検出	VA及び利用者との通信時にはSSLによる認証を実施。
46	検出	M.SSL_AUTH_PUB	検証手順におけるサーバ認証結果確認の必要性の公表	TSAポリシー等により説明事項を公表することにより、実現可能。
47	検出	M.SSL_BEG_FAIL	SSL通信開始失敗の検出	VA及び利用者との通信時にはSSLによる認証を実施。
48	検出	M.TA_AUDIT	TAによる時刻監査	TAによる時刻監査を受信。
49	検出	M.TA_FAIL_AUTH	TAによるTOEの認証失敗の検出	TLSにより通信相手の認証を実施。

項番	種別	対策名	説明	統合化システムにおける実現
50	検出	M.TA_SIGN_VERI	TAにより付与されたデジタル署名の検証	AcrobatReaderの機能により、デジタル署名の検証を実施可能。
51	検出	M.TSA_VERI	正当なTSAを介した正当な手順による検証の実施	TOEにおいて、検証要求に対して検証処理を実施。
52	検出	M.USER_CONT	利用者からの連絡	TSAポリシー等による問い合わせ先の公表もしくは通知により、実現可能。
53	検出	M.USER_DOUBT	特定の利用者アカウントの不審な挙動の検知	利用状況の監視により、実現可能。
54	検出	M.USER_INQ	利用者からの問い合わせ	TSAポリシー等による問い合わせ先の公表もしくは通知により、実現可能。
55	検出	M.VIRUS_CHECK	アンチウィルスソフトによる定期的なウィルスチェック	各サブシステムにおいて定期的なウィルスチェックを実施可能。
56	回復	M.AC_REST	TOEのアクセス管理設定の復旧	OS等によるファイルアクセスの管理機能により実施可能。
57	回復	M.ATTACK_NOT	利用者への攻撃の存在の通知	リポジトリ等による公表や利用契約者への連絡により、実現可能。
58	回復	M.ATTACK_REM	攻撃者の特定及び攻撃除去の働きかけ	IDSの設置及び攻撃内容の解析により実現可能。
59	回復	M.CERT_REISSUE	公開鍵証明書の再取得	認証局による公開鍵証明書発行機能により、実施可能。
60	回復	M.CERT_REVOKE	公開鍵証明書の失効	認証局により公開鍵証明書管理機能により、実施可能。
61	回復	M.CLOCK_REST	システムクロックの復旧	システムクロックの設定修復、TAによる時刻配信、機器の修理や交換等により、実現可能。
62	回復	M.CONF_REG	正常な設定ファイルの再生成	設計書等に従い、正当な設定ファイルの再生成を実施可能。
63	回復	M.DATA_REST	TOEが保持するデータのバックアップからの復旧	定期的なバックアップの保管により、実現可能。
64	回復	M.FAC_INC	TOEの設備増強	TOEの機器の追加による並列化等により実現可能。
65	回復	M.ID_CHANGE	不正なID/パスワードの削除及び正当なID/パスワードの登録	ID/パスワード管理機能により、実施可能。
66	回復	M.ID_ERACE	不正なID/パスワードの削除	ID/パスワード管理機能により、実施可能。
67	回復	M.ID_REGI	正当なID/パスワードの登録	ID/パスワード管理機能により、実施可能。
68	回復	M.ILL_TST_NOT	不正なタイムスタンプトークンの存在に関する利用者通知	リポジトリにおける公表や利用者への個別通知により、実現可能。
69	回復	M.KEY_CERT_REG	秘密鍵の再生成及び公開鍵証明書の再発行	秘密鍵の生成機能及び認証局による公開鍵証明書発行機能により、実施可能。
70	回復	M.LINK_AUDIT_PUB	リンク情報の整合性に関する監査結果の公開	リンク情報を再計算し比較した結果を公開することにより、実現可能。
71	回復	M.LINK_PROV_COPY	明証化されたリンク情報の代表値からの複製	リンク情報の代表値の定期刊行物への掲載等により、実現可能。
72	回復	M.LINK_REG	過去のリンク情報及びTSTからのリンク情報の再計算	定められた計算手順に従い、リンク情報の再計算を実施可能。
73	回復	M.MOD_REP	TOEのプログラムの改修	プログラムの改修を実施可能。
74	回復	M.NW_BLOCK	ネットワーク経由の攻撃の検知に応じた攻撃の遮断	ファイアウォールの設定変更等により実現可能。
75	回復	M.NW_REST	通信回線の復旧	サービス復旧に係る規定のある通信サービスの利用により、実現可能。
76	回復	M.OS_REST	OS及びソフトウェアの再インストールならびにバックアップデータからの復旧	ウィルス検出時に、アンチウィルスソフトによる駆除が難しい場合には、OS及びソフトウェアの再インストールにより復旧可能。
77	回復	M.PATCH	TOEへのセキュリティパッチの適用	発見された脆弱性に応じたセキュリティパッチの適用を実施可能。

項番	種別	対策名	説明	統合化システムにおける実現
78	回復	M.PEER_REST	通信相手の他システムの復旧	サービス復旧に係る規定のあるサービスの利用により、実現可能。
79	回復	M.PW_CHANGE	パスワードの変更	パスワード管理機能により、実施可能。
80	回復	M.PW_REGI	パスワードの再登録	パスワード管理機能により、実施可能。
81	回復	M.RECOMP	ソフトウェアのソースからの再生成	ソフトウェアのソースよりモジュールのリコンパイルを実施可能。
82	回復	M.REPAIR	TOEの機器の修理もしくは交換	ハード故障時等においては、機器の修理もしくは交換を実施可能。
83	回復	M.REQ_RETRY	タイムスタンプ要求の再実施	リトライに対応したクライアントアプリケーションを準備することにより、実現可能。
84	回復	M.RL_REISSUE	CRL及びARLの再取得	認証局によるCRL及びARLの公開機能により、実施可能。
85	回復	M.STOP	正常状態復旧までのサービスの一時停止	障害発生時等においては、正常状態復旧まで、サービスの一時停止を実施可能。
86	回復	M.SW_REST	ソフトウェアのバックアップからの再インストールによる復旧	ソフトウェアのバックアップより再インストールの実施可能。
87	回復	M.TA_DELI_BC	時刻監査に失敗する時計に対するTAによる時刻配信	時刻監査の成功･失敗に依らず、TAによる時刻配信を受信。
88	回復	M.TA_REISSUE	TAによる再発行	TAの保持するデータの再送付により、実施可能。
89	回復	M.VIRUS_EXT	アンチウィルスソフトによるウィルス駆除	各サブシステムにアンチウィルスソフトを導入しており、ウィルス検出時には駆除の試行を実施可能。

脅威のセキュリティ目標・対策一覧を、以下の表 9に示す。なお、表中網掛けの項目は、実質的なリスクを伴わない脅威を示す。

表 9　脅威のセキュリティ目標・対策一覧

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
1	T.VIRUS	有	防止	M.FW
			検出	M.VIRUS_CHECK
			回復	M.VIRUS_EXT；M.OS_REST
2	T.SYSYTEM_CLOCK_INACCURACY	有	防止	M.TA_DELI
			検出	M.TA_AUDIT
			回復	M.STOP；M.REPAIR
3	T.HASH_COMPROMISE_FUTURE	有	防止	M.CRY_RECOM；M.CRY_MULTI；M.TS_ARCH
			検出	M.CRY_CHECK
			回復	ー
4	T.HASH_COMPROMISE_CLIENT	有	防止	M.HASH_REJECT
			検出	M.HASH_CHECK
			回復	ー
5	T.HASH_COMPROMISE_SERVER	有	防止	M.CRY_RECOM；M.CRY_MULTI；M.TS_ARCH
			検出	M.CRY_CHECK
			回復	ー
6	T.DOS	有	防止	M.FW；M.USER_PW
			検出	M.IDS；M.LOG_AUDIT
			回復	M.NW_BLOCK；M.ATTACK_REM；M.FAC_INC
7	T.HACK_IMPERSON_TOE	有	防止	M.SSL_AUTH
			検出	M.TSA_VERI；M.SSL_AUTH_PUB
			回復	M.ATTACK_NOT；M.ATTACK_REM
8	T.CLIENT_REFUTE_ORIGIN	有	防止	M.LINK_GEN；M.LINK_PROV
			検出	ー
			回復	M.LINK_AUDIT_PUB
9	T.HARDWARE_FAILURE	有	防止	M.HW_RED
			検出	M.HW_CHECK
			回復	M.REPAIR
10	T.PEER_FAILURE	有	防止	M.PEER_REL；M.PEER_RED
			検出	M.PEER_FAIL_DET；M.PEER_NOT
			回復	M.PEER_REST
11	T.CONNECTION_FAILURE	有	防止	M.NW_REL；M.NW_RED
			検出	M.NW_FAIL_DET；M.NW_NOT
			回復	M.NW_REST
12	T.TOE_BUG	有	防止	M.SYS_TEST
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.MOD_REP
13	T.BUFFEROVERFLOW_ATTACK	有	防止	M.FW；M.VUL_CHECK
			検出	M.IDS；M.LOG_AUDIT
			回復	M.PATCH；M.NW_BLOCK；M.ATTACK_REM；M.MOD_REP
14	T.TSQ_LINE	有	防止	M.NW_RED
			検出	M.CLI_ERR
			回復	M.REQ_RETRY
15	T.TSR_LINE	有	防止	M.NW_RED
			検出	M.CLI_ERR
			回復	M.REQ_RETRY
16	T.FORGERY_USER-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_ERACE
17	T.MODIFY_USER-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_CHANGE
18	T.ERACE_USER-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_REGI

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
19	T.IMPERSON_USER-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
20	T.STEAL_USER-ID-PW_USER	無	防止	－
			検出	－
			回復	－
21	T.DISCLOSE_USER-ID-PW_USER	有	防止	M.USER_PW_NOT
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
22	T.FORGERY_USER-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_ERACE
23	T.MODIFY_USER-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_CHANGE
24	T.ERACE_USER-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_REGI
25	T.IMPERSON_USER-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
26	T.STEAL_USER-ID-PW_THIRD	有	防止	M.USER_PW_NOT
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
27	T.DISCLOSE_USER-ID-PW_THIRD	有	防止	M.USER_PW_NOT
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
28	T.FORGERY_TST_USER	有	防止	M.TST_VAL_PUB
			検出	M.TSA_VERI；M.LINK_AUDIT
			回復	M.ILL_TST_NOT
29	T.MODIFY_TST_USER	有	防止	M.TST_VAL_PUB
			検出	M.TSA_VERI；M.LINK_AUDIT
			回復	M.ILL_TST_NOT
30	T.ERACE_TST_USER	有	防止	M.KEEP_TST_NOT
			検出	M.USER_CONT
			回復	－
31	T.IMPERSON_TST_USER	有	防止	M.SSL_AUTH
			検出	M.TSA_VERI；M.SSL_AUTH_PUB
			回復	M.ATTACK_NOT；M.ATTACK_REM
32	T.STEAL_TST_USER	無	防止	－
			検出	－
			回復	－
33	T.DISCLOSE_TST_USER	無	防止	－
			検出	－
			回復	－
34	T.FORGERY_TST_THIRD	有	防止	M.TST_VAL_PUB
			検出	M.TSA_VERI；M.LINK_AUDIT
			回復	M.ILL_TST_NOT
35	T.MODIFY_TST_THIRD	有	防止	M.TST_VAL_PUB
			検出	M.TSA_VERI；M.LINK_AUDIT
			回復	M.ILL_TST_NOT
36	T.ERACE_TST_THIRD	有	防止	M.KEEP_TST_NOT
			検出	M.USER_CONT
			回復	－
37	T.IMPERSON_TST_THIRD	有	防止	M.SSL_AUTH
			検出	M.TSA_VERI；M.SSL_AUTH_PUB
			回復	M.ATTACK_NOT；M.ATTACK_REM
38	T.STEAL_TST_THIRD	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
39	T.DISCLOSE_TST_THIRD	無	防止	－
			検出	－
			回復	－
40	T.FORGERY_TAC_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
41	T.MODIFY_TAC_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
42	T.ERACE_TAC_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.USER_CONT
			回復	M.DATA_REST；M.TA_REISSUE
43	T.IMPERSON_TAC_USER	有	防止	M.TA_SIGN
			検出	M.TA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
44	T.STEAL_TAC_USER	無	防止	－
			検出	－
			回復	－
45	T.DISCLOSE_TAC_USER	無	防止	－
			検出	－
			回復	－
46	T.FORGERY_TAC_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
47	T.MODIFY_TAC_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
48	T.ERACE_TAC_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.USER_CONT
			回復	M.DATA_REST；M.TA_REISSUE
49	T.IMPERSON_TAC_THIRD	有	防止	M.TA_SIGN
			検出	M.TA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
50	T.STEAL_TAC_THIRD	無	防止	－
			検出	－
			回復	－
51	T.DISCLOSE_TAC_THIRD	無	防止	－
			検出	－
			回復	－
52	T.FORGERY_TAC-LOG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
53	T.MODIFY_TAC-LOG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
54	T.ERACE_TAC-LOG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.USER_CONT
			回復	M.DATA_REST；M.TA_REISSUE
55	T.IMPERSON_TAC-LOG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
56	T.STEAL_TAC-LOG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
57	T.DISCLOSE_TAC-LOG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
58	T.FORGERY_TAC-LOG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
59	T.MODIFY_TAC-LOG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
60	T.ERACE_TAC-LOG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.USER_CONT
			回復	M.DATA_REST；M.TA_REISSUE
61	T.IMPERSON_TAC-LOG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
62	T.STEAL_TAC-LOG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
63	T.DISCLOSE_TAC-LOG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
64	T.FORGERY_TAR_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
65	T.MODIFY_TAR_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
66	T.ERACE_TAR_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.USER_CONT
			回復	M.DATA_REST；M.TA_REISSUE
67	T.IMPERSON_TAR_USER	有	防止	M.TA_SIGN
			検出	M.TA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
68	T.STEAL_TAR_USER	無	防止	－
			検出	－
			回復	－
69	T.DISCLOSE_TAR_USER	無	防止	－
			検出	－
			回復	－
70	T.FORGERY_TAR_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
71	T.MODIFY_TAR_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.TA_REISSUE
72	T.ERACE_TAR_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.USER_CONT
			回復	M.DATA_REST；M.TA_REISSUE
73	T.IMPERSON_TAR_THIRD	有	防止	M.TA_SIGN
			検出	M.TA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
74	T.STEAL_TAR_THIRD	無	防止	－
			検出	－
			回復	－
75	T.DISCLOSE_TAR_THIRD	無	防止	－
			検出	－
			回復	－
76	T.FORGERY_KEYST_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.TA_FAIL_AUTH；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG；M.DATA_REST
77	T.MODIFY_KEYST_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.TA_FAIL_AUTH；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG；M.DATA_REST
78	T.ERACE_KEYST_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.TA_FAIL_AUTH；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG；M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
79	T.IMPERSON_KEYST_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
80	T.STEAL_KEYST_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
81	T.DISCLOSE_KEYST_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
82	T.FORGERY_KEYST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.KEY_CERT_REG;M.DATA_REST
83	T.MODIFY_KEYST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.KEY_CERT_REG;M.DATA_REST
84	T.ERACE_KEYST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.KEY_CERT_REG;M.DATA_REST
85	T.IMPERSON_KEYST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
86	T.STEAL_KEYST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
87	T.DISCLOSE_KEYST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
88	T.FORGERY_KEYST-PW_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
89	T.MODIFY_KEYST-PW_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
90	T.ERACE_KEYST-PW_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
91	T.IMPERSON_KEYST-PW_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
92	T.STEAL_KEYST-PW_USER	有	防止	M.FAC_ISO;M.FW;M.AC
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.KEY_CERT_REG
93	T.DISCLOSE_KEYST-PW_USER	有	防止	M.FAC_ISO;M.FW;M.AC
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.KEY_CERT_REG
94	T.FORGERY_KEYST-PW_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
95	T.MODIFY_KEYST-PW_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
96	T.ERACE_KEYST-PW_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
97	T.IMPERSON_KEYST-PW_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
98	T.STEAL_KEYST-PW_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.KEY_CERT_REG

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
99	T.DISCLOSE_KEYST-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
100	T.FORGERY_CERT_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.CERT_REISSUE；M.KEY_CERT_REG
101	T.MODIFY_CERT_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.CERT_REISSUE；M.KEY_CERT_REG
102	T.ERACE_CERT_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.CERT_REISSUE；M.KEY_CERT_REG
103	T.IMPERSON_CERT_USER	有	防止	M.CA_SIGN
			検出	M.CA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
104	T.STEAL_CERT_USER	無	防止	－
			検出	－
			回復	－
105	T.DISCLOSE_CERT_USER	無	防止	－
			検出	－
			回復	－
106	T.FORGERY_CERT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.CERT_REISSUE；M.KEY_CERT_REG
107	T.MODIFY_CERT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.CERT_REISSUE；M.KEY_CERT_REG
108	T.ERACE_CERT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.CERT_REISSUE；M.KEY_CERT_REG
109	T.IMPERSON_CERT_THIRD	有	防止	M.CA_SIGN
			検出	M.CA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
110	T.STEAL_CERT_THIRD	無	防止	－
			検出	－
			回復	－
111	T.DISCLOSE_CERT_THIRD	無	防止	－
			検出	－
			回復	－
112	T.FORGERY_CRL-ARL_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.RL_REISSUE
113	T.MODIFY_CRL-ARL_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.RL_REISSUE
114	T.ERACE_CRL-ARL_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.RL_REISSUE
115	T.IMPERSON_CRL-ARL_USER	有	防止	M.CA_SIGN
			検出	M.CA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
116	T.STEAL_CRL-ARL_USER	無	防止	－
			検出	－
			回復	－
117	T.DISCLOSE_CRL-ARL_USER	無	防止	－
			検出	－
			回復	－
118	T.FORGERY_CRL-ARL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.RL_REISSUE

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
119	T.MODIFY_CRL-ARL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.CA_SIGN
			検出	M.CA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.RL_REISSUE
120	T.ERACE_CRL-ARL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.RL_REISSUE
121	T.IMPERSON_CRL-ARL_THIRD	有	防止	M.CA_SIGN
			検出	M.CA_SIGN_VERI
			回復	M.ATTACK_NOT；M.ATTACK_REM
122	T.STEAL_CRL-ARL_THIRD	無	防止	－
			検出	－
			回復	－
123	T.DISCLOSE_CRL-ARL_THIRD	無	防止	－
			検出	－
			回復	－
124	T.FORGERY_PRI-KEY_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.SSL_AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.KEY_CERT_REG
125	T.MODIFY_PRI-KEY_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.SSL_AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.KEY_CERT_REG
126	T.ERACE_PRI-KEY_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.SSL_BEG_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.KEY_CERT_REG
127	T.IMPERSON_PRI-KEY_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
128	T.STEAL_PRI-KEY_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
129	T.DISCLOSE_PRI-KEY_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
130	T.FORGERY_PRI-KEY_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.SSL_AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.KEY_CERT_REG
131	T.MODIFY_PRI-KEY_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.SSL_AUTH_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.KEY_CERT_REG
132	T.ERACE_PRI-KEY_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.SSL_BEG_FAIL；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST；M.KEY_CERT_REG
133	T.IMPERSON_PRI-KEY_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
134	T.STEAL_PRI-KEY_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
135	T.DISCLOSE_PRI-KEY_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.PW_LOCK；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
136	T.FORGERY_PRI-KEY-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.PW_CHANGE；M.KEY_CERT_REG；M.DATA_REST
137	T.MODIFY_PRI-KEY-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.PW_CHANGE；M.KEY_CERT_REG；M.DATA_REST
138	T.ERACE_PRI-KEY-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.PW_REGI；M.KEY_CERT_REG；M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
139	T.IMPERSON_PRI-KEY-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
140	T.STEAL_PRI-KEY-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
141	T.DISCLOSE_PRI-KEY-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
142	T.FORGERY_PRI-KEY-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.PW_CHANGE；M.KEY_CERT_REG；M.DATA_REST
143	T.MODIFY_PRI-KEY-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.PW_CHANGE；M.KEY_CERT_REG；M.DATA_REST
144	T.ERACE_PRI-KEY-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.PW_REGI；M.KEY_CERT_REG；M.DATA_REST
145	T.IMPERSON_PRI-KEY-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
146	T.STEAL_PRI-KEY-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
147	T.DISCLOSE_PRI-KEY-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.KEY_CERT_REG
148	T.FORGERY_OPE-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_ERACE
149	T.MODIFY_OPE-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_CHANGE
150	T.ERACE_OPE-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_REGI
151	T.IMPERSON_OPE-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
152	T.STEAL_OPE-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
153	T.DISCLOSE_OPE-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
154	T.FORGERY_OPE-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_ERACE
155	T.MODIFY_OPE-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_CHANGE
156	T.ERACE_OPE-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_REGI
157	T.IMPERSON_OPE-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
158	T.STEAL_OPE-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
159	T.DISCLOSE_OPE-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
160	T.FORGERY_DB-SERIAL_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
161	T.MODIFY_DB-SERIAL_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
162	T.ERACE_DB-SERIAL_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
163	T.IMPERSON_DB-SERIAL_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
164	T.STEAL_DB-SERIAL_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
165	T.DISCLOSE_DB-SERIAL_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
166	T.FORGERY_DB-SERIAL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
167	T.MODIFY_DB-SERIAL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
168	T.ERACE_DB-SERIAL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
169	T.IMPERSON_DB-SERIAL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
170	T.STEAL_DB-SERIAL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
171	T.DISCLOSE_DB-SERIAL_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
172	T.FORGERY_DB-USER-ID_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
173	T.MODIFY_DB-USER-ID_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
174	T.ERACE_DB-USER-ID_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
175	T.IMPERSON_DB-USER-ID_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
176	T.STEAL_DB-USER-ID_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
177	T.DISCLOSE_DB-USER-ID_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
178	T.FORGERY_DB-USER-ID_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
179	T.MODIFY_DB-USER-ID_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
180	T.ERACE_DB-USER-ID_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
181	T.IMPERSON_DB-USER-ID_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
182	T.STEAL_DB-USER-ID_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
183	T.DISCLOSE_DB-USER-ID_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
184	T.FORGERY_DB-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
185	T.MODIFY_DB-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
186	T.ERACE_DB-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
187	T.IMPERSON_DB-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
188	T.STEAL_DB-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
189	T.DISCLOSE_DB-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
190	T.FORGERY_DB-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
191	T.MODIFY_DB-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
192	T.ERACE_DB-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
193	T.IMPERSON_DB-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
194	T.STEAL_DB-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
195	T.DISCLOSE_DB-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
196	T.FORGERY_DB-TST_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL；M.LINK_GEN
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
197	T.MODIFY_DB-TST_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL；M.LINK_GEN
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
198	T.ERACE_DB-TST_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
199	T.IMPERSON_DB-TST_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
200	T.STEAL_DB-TST_USER	有	防止	M.FAC_ISO;M.FW;M.AC
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	－
201	T.DISCLOSE_DB-TST_USER	有	防止	M.FAC_ISO;M.FW;M.AC
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	－
202	T.FORGERY_DB-TST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.DATA_REST
203	T.MODIFY_DB-TST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.DATA_REST
204	T.ERACE_DB-TST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.DATA_REST
205	T.IMPERSON_DB-TST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
206	T.STEAL_DB-TST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	－
207	T.DISCLOSE_DB-TST_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	－
208	T.FORGERY_LINK_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.LINK_REG;M.DATA_REST
209	T.MODIFY_LINK_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.LINK_REG;M.DATA_REST
210	T.ERACE_LINK_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.LINK_REG;M.DATA_REST
211	T.IMPERSON_LINK_USER	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
212	T.STEAL_LINK_USER	無	防止	－
			検出	－
			回復	－
213	T.DISCLOSE_LINK_USER	無	防止	－
			検出	－
			回復	－
214	T.FORGERY_LINK_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.LINK_REG;M.DATA_REST
215	T.MODIFY_LINK_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.LINK_REG;M.DATA_REST
216	T.ERACE_LINK_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK
			回復	M.LINK_REG;M.DATA_REST
217	T.IMPERSON_LINK_THIRD	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL
			検出	M.LOG_AUDIT;M.ERR_CHECK
			回復	M.AC_REST
218	T.STEAL_LINK_THIRD	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
219	T.DISCLOSE_LINK_THIRD	無	防止	－
			検出	－
			回復	－
220	T.FORGERY_CONFIG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.CONF_REG；M.DATA_REST
221	T.MODIFY_CONFIG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.CONF_REG；M.DATA_REST
222	T.ERACE_CONFIG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.CONF_REG；M.DATA_REST
223	T.IMPERSON_CONFIG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
224	T.STEAL_CONFIG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
225	T.DISCLOSE_CONFIG_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
226	T.FORGERY_CONFIG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.CONF_REG；M.DATA_REST
227	T.MODIFY_CONFIG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.CONF_REG；M.DATA_REST
228	T.ERACE_CONFIG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.CONF_REG；M.DATA_REST
229	T.IMPERSON_CONFIG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
230	T.STEAL_CONFIG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
231	T.DISCLOSE_CONFIG_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
232	T.FORGERY_DB-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_ERACE
233	T.MODIFY_DB-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_CHANGE
234	T.ERACE_DB-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_REGI
235	T.IMPERSON_DB-ID-PW_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
236	T.STEAL_DB-ID-PW_USER	有	防止	M.USER_PW_NOT
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
237	T.DISCLOSE_DB-ID-PW_USER	有	防止	M.USER_PW_NOT
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
238	T.FORGERY_DB-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_ERACE

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
239	T.MODIFY_DB-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_CHANGE
240	T.ERACE_DB-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.ID_REGI
241	T.IMPERSON_DB-ID-PW_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
242	T.STEAL_DB-ID-PW_THIRD	有	防止	M.USER_PW_NOT
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
243	T.DISCLOSE_DB-ID-PW_THIRD	有	防止	M.USER_PW_NOT
			検出	M.USER_DOUBT；M.USER_CONT
			回復	M.PW_CHANGE
244	T.FORGERY_LINK-PROV_USER	有	防止	M.PROV
			検出	M.LINK_PROV_COMP
			回復	M.LINK_PROV_COPY
245	T.MODIFY_LINK-PROV_USER	有	防止	M.PROV
			検出	M.LINK_PROV_COMP
			回復	M.LINK_PROV_COPY
246	T.ERACE_LINK-PROV_USER	有	防止	M.PROV
			検出	M.LINK_PROV_LOST
			回復	M.LINK_PROV_COPY
247	T.IMPERSON_LINK-PROV_USER	有	防止	M.PROV
			検出	M.USER_INQ
			回復	M.ATTACK_REM
248	T.STEAL_LINK-PROV_USER	無	防止	－
			検出	－
			回復	－
249	T.DISCLOSE_LINK-PROV_USER	無	防止	－
			検出	－
			回復	－
250	T.FORGERY_LINK-PROV_THIRD	有	防止	M.PROV
			検出	M.LINK_PROV_COMP
			回復	M.LINK_PROV_COPY
251	T.MODIFY_LINK-PROV_THIRD	有	防止	M.PROV
			検出	M.LINK_PROV_COMP
			回復	M.LINK_PROV_COPY
252	T.ERACE_LINK-PROV_THIRD	有	防止	M.PROV
			検出	M.LINK_PROV_LOST
			回復	M.LINK_PROV_COPY
253	T.IMPERSON_LINK-PROV_THIRD	有	防止	M.PROV
			検出	M.USER_INQ
			回復	M.ATTACK_REM
254	T.STEAL_LINK-PROV_THIRD	無	防止	－
			検出	－
			回復	－
255	T.DISCLOSE_LINK-PROV_THIRD	無	防止	－
			検出	－
			回復	－
256	T.FORGERY_EVENT_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
257	T.MODIFY_EVENT_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
258	T.ERACE_EVENT_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
259	T.IMPERSON_EVENT_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
260	T.STEAL_EVENT_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
261	T.DISCLOSE_EVENT_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
262	T.FORGERY_EVENT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
263	T.MODIFY_EVENT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
264	T.ERACE_EVENT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.DATA_REST
265	T.IMPERSON_EVENT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
266	T.STEAL_EVENT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
267	T.DISCLOSE_EVENT_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
268	T.FORGERY_CLOCK_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.TA_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.TA_DELI_BC；M.CLOCK_REST
269	T.MODIFY_CLOCK_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.TA_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.TA_DELI_BC；M.CLOCK_REST
270	T.ERACE_CLOCK_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.TA_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.TA_DELI_BC；M.CLOCK_REST
271	T.IMPERSON_CLOCK_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
272	T.STEAL_CLOCK_USER	無	防止	－
			検出	－
			回復	－
273	T.DISCLOSE_CLOCK_USER	無	防止	－
			検出	－
			回復	－
274	T.FORGERY_CLOCK_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.TA_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.TA_DELI_BC；M.CLOCK_REST
275	T.MODIFY_CLOCK_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.TA_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.TA_DELI_BC；M.CLOCK_REST
276	T.ERACE_CLOCK_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.TA_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.TA_DELI_BC；M.CLOCK_REST
277	T.IMPERSON_CLOCK_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
278	T.STEAL_CLOCK_THIRD	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
279	T.DISCLOSE_CLOCK_THIRD	無	防止	－
			検出	－
			回復	－
280	T.FORGERY_MOD-CRE-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
281	T.MODIFY_MOD-CRE-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
282	T.ERACE_MOD-CRE-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
283	T.IMPERSON_MOD-CRE-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
284	T.STEAL_MOD-CRE-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
285	T.DISCLOSE_MOD-CRE-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
286	T.FORGERY_MOD-CRE-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
287	T.MODIFY_MOD-CRE-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
288	T.ERACE_MOD-CRE-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
289	T.IMPERSON_MOD-CRE-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
290	T.STEAL_MOD-CRE-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
291	T.DISCLOSE_MOD-CRE-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
292	T.FORGERY_MOD-STORE_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
293	T.MODIFY_MOD-STORE_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
294	T.ERACE_MOD-STORE_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
295	T.IMPERSON_MOD-STORE_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
296	T.STEAL_MOD-STORE_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
297	T.DISCLOSE_MOD-STORE_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
298	T.FORGERY_MOD-STORE_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
299	T.MODIFY_MOD-STORE_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
300	T.ERACE_MOD-STORE_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
301	T.IMPERSON_MOD-STORE_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
302	T.STEAL_MOD-STORE_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
303	T.DISCLOSE_MOD-STORE_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
304	T.FORGERY_MOD-COM-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
305	T.MODIFY_MOD-COM-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
306	T.ERACE_MOD-COM-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
307	T.IMPERSON_MOD-COM-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
308	T.STEAL_MOD-COM-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
309	T.DISCLOSE_MOD-COM-TS_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
310	T.FORGERY_MOD-COM-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
311	T.MODIFY_MOD-COM-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
312	T.ERACE_MOD-COM-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
313	T.IMPERSON_MOD-COM-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
314	T.STEAL_MOD-COM-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
315	T.DISCLOSE_MOD-COM-TS_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
316	T.FORGERY_MOD-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
317	T.MODIFY_MOD-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
318	T.ERACE_MOD-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
319	T.IMPERSON_MOD-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
320	T.STEAL_MOD-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
321	T.DISCLOSE_MOD-TIME_USER	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
322	T.FORGERY_MOD-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
323	T.MODIFY_MOD-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
324	T.ERACE_MOD-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.MOD_WATCH
			回復	M.SW_REST；M.RECOMP
325	T.IMPERSON_MOD-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	M.AC_REST
326	T.STEAL_MOD-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－
327	T.DISCLOSE_MOD-TIME_THIRD	有	防止	M.FAC_ISO；M.FW；M.AC
			検出	M.LOG_AUDIT；M.ERR_CHECK
			回復	－

2. 前提の実現方法例

TOE に係るセキュリティ環境の前提の実現方法例一覧を、以下の表 10に示す。

表 10　TOE に係るセキュリティ環境の前提の実現方法例一覧

#	分類	項目	実現方法例
1	物理的な前提（Physical assumptions）	A.LOCATE	TOE が設置された施設内への入室は、あらかじめ許可された人員のみが可能となるようにする。
2		A.ENVIRONMENT	電磁波が盗聴されないようケーブル類が施錠管理されたラック内に配線されるとともに、瞬断や停電に備えて二重化された電源装置へ接続され、長時間停電した場合は、自家発電装置による電源供給を行い、空調設備により、機器類の動作に適した環境に維持される。
3		A.MEDIA	ストレージを冗長化し、一部に経年劣化や不良が生じた場合には速やかに部品の交換を実施する。
4	人的な前提（Personnel assumptions）	A.ADMIN	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、管理者として任命される。
5		A.OPERATOR	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、運用者として任命される。
6		A.AUDITOR	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、監査者として任命される。
7		A.USER	利用者はタイムスタンプの付与及び検証手順ならびに利用者パスワードの管理について記載された TSA ポリシー及びサービス利用規約に同意の上、サービスを利用する。
8	接続に関する前提（Connectivity assumptions）	A.DEVICE	周辺機器への全接続は施錠管理されたラック内に収められる。
9		A.FIREWALL	TOE とインターネット及び他システムとの接続箇所においては、ファイアウォール機能を持つネットワーク機器が設置され、不要な通信を遮断する。
10		A.PEER	TOE と通信する他システムは TOE と同様にセキュリティ評価が実施され、信頼できる。
11		A.REQUESTER_CONNECTION	タイムスタンプ要求者、検証者及び時刻監査レポート要求者が操作するマシンと TOE の間の通信路は、SSL により、サーバ認証、メッセージ認証、メッセージ暗号化が行われている。
12		A.VA_CONNECTION	VA と TOE の間の通信路は、SSL により、相互認証、メッセージ認証、メッセージ暗号化が行われている。
13		A.TA1_CONNECTION	TA1 と TOE の間の通信路は、TLS 及びダイアルアップにより、相互認証、メッセージ認証、メッセージ暗号化が行われている。

#	分類	項目	実現方法例
14		A.ABSTRACT	OS や依存するﾗｲﾌﾞﾗﾘに変更を加える作業は、管理者による承認のもとでのみ実施される。
15		A.SEPARATION	TOE が動作するマシンには、TOE の動作に必要なｿﾌﾄｳｪｱ以外はｲﾝｽﾄｰﾙされていない。

3. 組織のセキュリティポリシーの実現方法例

TOE に係るセキュリティ環境の組織のセキュリティポリシーの実現方法例一覧を、以下の表 11 に示す。

表 11　TOE に係るセキュリティ環境の組織のセキュリティポリシーの実現方法例一覧

#	項目	実現方法例
1	P.CRYPTO	ドキュメントハッシュ及びリンク情報の生成においては、SHA-512 と RIPEMD-160 を並列に使用している。利用者との SSL 通信においては、公開鍵暗号として鍵長 1024 ビットの RSASSA-PKCS1-v1_5、鍵長 128 ビット以上の共通鍵暗号を使用している。
2	P.PUBLISH	リンクデータの代表値を新聞等の定期刊行物に掲載し、公表する。
3	P.TIME_ SOURCE	信頼できる時刻ソースとして、TA1 からの時刻配信を受けている。
4	P.SYSTM_CLOCK_ MANAGEMENT	TA1 からの時刻配信を受けている。
5	P.PKI_MANAGEMENT	鍵の管理は複数人運用によって実施される。また、証明書は信頼できる認証局により管理される。
6	P.PROTECT_LOG	監査ログの管理は複数人運用によって実施されるとともに、定期的にバックアップを保管する。
7	P.PASSWORD_ MANAGEMENT	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、管理者及び運用者として任命される。
8	P.CHECK_VIRUS	アンチウィルスソフトをインストールし、定期的なパターンファイル更新とウィルスチェックを実施している。
9	P.DUAL_CONTROL	重要な操作については複数人運用を行う。
10	P.CHECK_ABSTRACT_ VULNERABILITY	定期的に、公開されている脆弱性情報を確認している。

第4章 脅威ツリー及びリスク評価一覧

1. 内部不正のないセキュリティ評価における脅威ツリー

TOE に係るセキュリティ評価において、「タイムスタンプの偽造」、「タイムスタンプの無効化」、「許容範囲外の時計の誤差」及び「暗号技術の脆弱化」という４つの代表的な攻撃の目的について作成した脅威ツリーを、以下の表 12に示す。

表 12　セキュリティ評価における脅威ツリー

項番	攻撃の目的	条件1	条件2	条件3	脅威名
1	タイムスタンプを偽造し、他者に正当なものと認めさせる。				
1-1		TSAの正当な手順による検証が成功となるようなタイムスタンプを偽造する。			
1-1-1			TSAの時計を不正に変更し、タイムスタンプを取得する。		
1-1-1-1				TSAの時計に対するアクセス権限を不正に取得する。	T.IMPERSON_CLOCK_USER, T.IMPERSON_CLOCK_THIRD
1-1-1-2				TAに成り済まし、TSAの時計を不正に操作する。	T.IMPERSON_TAC_USER, T.IMPERSON_TAC_THIRD
1-1-2			TSAのタイムスタンプ生成処理に不正な機能を持たせる。		
1-1-2-1				TSAのタイムスタンプ生成モジュールを偽造または改竄する。	T.FORGERY_MOD-CRE-TS_USER, T.MODIFY_MOD-CRE-TS_USER, T.FORGERY_MOD-CRE-TS_THIRD, T.MODIFY_MOD-CRE-TS_THIRD
1-1-2-2				TSAのタイムスタンプ発行に係る設定ファイルを偽造または改竄する。	T.FORGERY_CONFIG_USER, T.MODIFY_CONFIG_USER, T.FORGERY_CONFIG_THIRD, T.MODIFY_CONFIG_THIRD
1-1-3			タイムスタンプの生成手順における脆弱性を利用し、偽造する。		
1-1-3-1				タイムスタンプ生成に使用されているハッシュ関数の脆弱性を利用し、タイムスタンプを偽造する。	T.HASH_COMPROMISE_CLIENT, T.HASH_COMPROMISE_SERVER

項番	攻撃の目的	条件1	条件2	条件3	脅威名
1-1-4			不正なタイムスタンプを登録する。		
1-1-4-1				タイムスタンプの発行処理に対する権限を不正に取得し、TSAサーバで直接不正なタイムスタンプを発行する。	T.IMPERSON_MOD-CRE-TS_USER, T.IMPERSON_MOD-CRE-TS_THIRD
1-1-4-2				照合用データの保管用モジュールに対する権限を不正に取得し、偽造した照合用データを登録する。	T.IMPERSON_MOD-STORE_USER, T.IMPERSON_MOD-STORE_THIRD
1-2		偽造タイムスタンプについて、TSAにおける検証がOKとなるように手順や方法を細工する。			
1-2-1			TSAの検証処理に使用する照合用データを改竄し、タイムスタンプを検証する。		T.MODIFY_DB-TST_USER, T.MODIFY_DB-TST_THIRD
1-2-2			TSAのタイムスタンプ検証処理に不正な機能を持たせる。		
1-2-2-1				TSAのタイムスタンプ照合モジュールを偽造または改竄する。	T.FORGERY_MOD-COM-TS_USER, T.MODIFY_MOD-COM-TS_USER, T.FORGERY_MOD-COM-TS_THIRD, T.MODIFY_MOD-COM-TS_THIRD
1-2-2-2				TSAのタイムスタンプ照合に係る設定ファイルを偽造または改竄する。	T.FORGERY_CONFIG_USER, T.MODIFY_CONFIG_USER, T.FORGERY_CONFIG_THIRD, T.MODIFY_CONFIG_THIRD
1-2-3			TSAに成り済ましたサーバを構築し、タイムスタンプを検証する。		T.IMPERSON_TST_USER, T.IMPERSON_TST_THIRD
1-3		TSAによるNGの検証結果に誤りがあると主張する。			T.CLIENT_REFUTE_ORIGIN
2	タイムスタンプを無効化する。				

項番	攻撃の目的	条件1	条件2	条件3	脅威名
2-1		タイムスタンプの効力が失われるような事象を発生させる。			
2-1-1			タイムスタンプの検証を不可能とする。		
2-1-1-1				照合用データを消去する。	T.ERACE_DB-TST_USER, T.ERACE_DB-TST_THIRD
2-1-1-2				リンク情報の代表値の明証化の確認の元となる記録を全て廃棄する。	T.ERACE_LINK-PROV_USER, T.ERACE_LINK-PROV_THIRD
2-1-2			リンク情報の整合性が確保されない状態にする。		
2-1-2-1				ある時点で最新のリンク情報（次のリンク情報生成に使用されるもの）を改竄する。	T.MODIFY_LINK_USER, T.MODIFY_LINK_THIRD
2-1-2-2				リンク情報を生成するモジュールを偽造または改竄する。	T.FORGERY_MOD-CRE-TS_USER, T.MODIFY_MOD-CRE-TS_USER, T.FORGERY_MOD-CRE-TS_THIRD, T.MODIFY_MOD-CRE-TS_THIRD
2-1-2-3				TSAに成り済まし、偽造または改竄したリンク情報の代表値を明証化する。	T.IMPERSON_TST_USER, T.IMPERSON_TST_THIRD
2-1-3			タイムスタンプに係る処理手順にセキュリティ上の欠陥があると主張する。		
2-1-3-1				タイムスタンプの処理に利用されているハッシュ関数の脆弱性を発見し公表する。	T.HASH_COMPROMISE_FUTURE, T.HASH_COMPROMISE_CLIENT, T.HASH_COMPROMISE_SERVER
2-2		タイムスタンプが無効であると主張する。			
2-2-1			不正なタイムスタンプが発行されていると主張する。		T.CLIENT_REFUTE_ORIGIN
2-2-2			TSAにおいて不正な検証処理が実行されていると主張する。		T.CLIENT_REFUTE_ORIGIN
2-3		正当なタイムスタンプの検証が成功しないようにする。			

項番	攻撃の目的	条件1	条件2	条件3	脅威名
2-3-1			正当なタイムスタンプの検証が一時的に実行できないようにする。		
2-3-1-1				TSAに対するDOS攻撃により、検証要求の受付けを不可能とする。	T.DOS
2-3-1-2				TSAをウィルス感染させることにより、検証処理を実行不可能とする。	T.VIRUS
2-3-2			正当なタイムスタンプの検証が一時的に失敗するようにする。		
2-3-2-1				TSAの保有する照合用データを偽造または改竄する。	T.FORGERY_DB-TST_USER, T.MODIFY_DB-TST_USER, T.FORGERY_DB-TST_THIRD, T.MODIFY_DB-TST_THIRD
2-3-2-2				TSAのタイムスタンプ照合モジュールを偽造または改竄する。	T.FORGERY_MOD-COM-TS_USER, T.MODIFY_MOD-COM-TS_USER, T.FORGERY_MOD-COM-TS_THIRD, T.MODIFY_MOD-COM-TS_THIRD
2-4		利用者に発行されたタイムスタンプトークンを消去する。			
2-4-1			ネットワーク上で利用者に送信されたタイムスタンプトークンを消去する。		T.TSR_LINE
2-4-2			利用者の保有するタイムスタンプトークンを消去する。		T.ERACE_TST_USER, T.ERACE_TST_THIRD
2-5		時刻情報の正当性の確認を不可能とする。			
2-5-1			時刻監査の記録を消去する。		T.ERACE_TAC_USER, T.ERACE_TAC_THIRD, T.ERACE_TAR_USER, T.ERACE_TAR_THIRD
2-5-2			失敗となっている時刻監査の記録を偽造または改竄する。		T.FORGERY_TAC_USER, T.MODIFY_TAC_USER, T.FORGERY_TAC_THIRD, T.MODIFY_TAC_THIRD, T.FORGERY_TAR_USER, T.MODIFY_TAR_USER, T.FORGERY_TAR_THIRD, T.MODIFY_TAR_THIRD
3	TSAの時計の誤差が受容範囲外となる。				

項番	攻撃の目的	条件1	条件2	条件3	脅威名
3-1		人為的な操作により誤差が発生する。			
3-1-1			TSAの時計に対するアクセス権限を不正に取得する。		T.IMPERSON_CLOCK_USER, T.IMPERSON_CLOCK_THIRD
3-1-2			TAに成り済まし、TSAの時計を不正に操作する。		T.IMPERSON_TAC_USER, T.IMPERSON_TAC_THIRD
3-2		TAからの時刻配信が長時間受けられないことにより、誤差が発生する。			
3-2-1			TAのシステムのダウンが発生する。		T.PEER_FAILURE
3-2-2			TAとの間の通信回線の故障が発生する。		T.CONNECTION_FAILURE
3-3		TSAの機器の故障により誤差が発生する。			T.HARDWARE_FAILURE
4	タイムスタンプに使用されている暗号技術が脆弱化する。				
4-1		ドキュメントハッシュを生成するハッシュアルゴリズムが脆弱化する。			T.HASH_COMPROMISE_CLIENT
4-1-1			アルゴリズムの欠陥及び攻撃方法の発見により脆弱化する。		
4-1-2			計算機性能の飛躍的な向上により脆弱化する。		
4-2		リンク情報を生成するハッシュアルゴリズムが脆弱化する。			T.HASH_COMPROMISE_SERVER
4-2-1			アルゴリズムの欠陥及び攻撃方法の発見により脆弱化する。		
4-2-2			計算機性能の飛躍的な向上により脆弱化する。		

2. リスク評価格付けの考え方

TOE のセキュリティ評価における各脅威のリスク評価格付けの考え方について、以下の表 13 に示す。

表 13　リスク評価格付けの考え方

#	脅威格付項目	格付	格付基準
1	潜在的損失	高 (3)	・全てのタイムスタンプやサービス全体の信頼性の毀損に相当する損失の場合
		中 (2)	・一部の範囲のタイムスタンプやサービスの一部の信頼性の毀損に相当する損失の場合 ・他の脅威との組合せにより全てのタイムスタンプやサービス全体の信頼性の毀損に相当する損失につながる事項の場合 (例：対象資産への攻撃に利用できるPWに係る不正等) ・信頼性以外の中規模以上の (事業継続に影響する) 損失の場合
		低 (1)	・単一もしくはごく少数のタイムスタンプの信頼性の毀損に相当する損失の場合 ・他の脅威との組合せにより一部の範囲のタイムスタンプやサービスの一部の信頼性の毀損に相当する損失につながる事項の場合 (例：対象資産への攻撃に利用できるPWに係る不正等) ・信頼性以外の小規模な (事業継続に影響しない) 損失の場合 (例：サービスの無断利用等の財務的損失、積極的に公開していない情報や一部の営業秘密の流出、アカウント再設定や鍵の再生成等の手順で稼働状態に復旧可能な状況等)
2	再現性	高 (3)	・対象資産に対するアクセス権を持っており単独で操作できる場合
		中 (2)	・機器に単独でアクセスできる機会はあるが、対象資産に対するアクセス権は持っていない場合 ・対象資産に対するアクセス権を持っているが、複数人による相互牽制を実施している場合 ・機器、対象資産に対するアクセス権は無いが、ネットワーク経由で常時攻撃が試行できる場合
		低 (1)	・入退室管理・ファイアウォールにより、物理アクセス・不正ネットワークアクセスが困難な場合 ・機器にアクセスする機会はあるが、対象資産に対するアクセス権は持っておらず、かつアクセス時には複数人による相互牽制を実施している場合 ・攻撃者が明らかとなる場合
3	攻撃利用可能性	高 (3)	・対象資産に対するアクセス権を持っている場合 ・高度な知識を要さず、攻撃が実施可能な場合
		中 (2)	・機器にアクセスする機会はあるが、対象資産に対するアクセス権は持っていない場合 ・機器、対象資産に対するアクセス権は無いが、ネットワーク経由で常時攻撃が試行できる場合

#	脅威格付項目	格付	格付基準
			・ある程度高度な知識により、攻撃が実施可能な場合
		低 (1)	・入退室管理・ファイアウォールにより、物理アクセス・不正ネットワークアクセスが困難な場合 ・非常に高度な知識により、攻撃が実施可能な場合
4	影響ユーザ	高 (3)	・全てのタイムスタンプや利用者、サービス全体に影響する場合
		中 (2)	・一部の範囲のタイムスタンプや利用者、サービスの一部に影響する場合 ・他の脅威との組合せにより全てのタイムスタンプや利用者、サービス全体に影響する事項の場合 (例：対象資産への攻撃に利用できるPWに係る不正等)
		低 (1)	・単一もしくはごく少数のタイムスタンプや利用者に影響する場合 ・他の脅威との組合せにより一部の範囲のタイムスタンプや利用者、サービスの一部に影響する事項の場合 (例：対象資産への攻撃に利用できるPWに係る不正等)
5	発見可能性	高 (3)	・対象資産に対するアクセス権を持っている場合 ・攻撃方法が一般に知られている場合
		中 (2)	・機器にアクセスする機会はあるが、対象資産に対するアクセス権は持っていない場合 ・機器、対象資産に対するアクセス権は無いが、ネットワーク経由で常時攻撃が試行できる場合 ・攻撃方法がごく少数に知られている場合
		低 (1)	・入退室管理・ファイアウォールにより、物理アクセス・不正ネットワークアクセスが困難な場合 ・攻撃方法が知られていない場合

3. リスク評価点

TOE のセキュリティ評価における「表 13　リスク評価格付けの考え方」に沿って得られた各脅威のリスク評価点について、以下のに示す。なお、表中リスク有無判定欄「無」となっている網掛けの脅威は、対象資産及び攻撃主体との組合せにおいて、実質的に脅威とならないことを示す。

表 14　リスク評価点

項番	脅威名	リスク	脅威格付					
		有無判定	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.VIRUS	有	高 (3)	中 (2)	中 (2)	高 (3)	中 (2)	12
2	T.SYSYTEM_CLOCK_INACCURACY	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
3	T.HASH_COMPROMISE_FUTURE	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
4	T.HASH_COMPROMISE_CLIENT	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
5	T.HASH_COMPROMISE_SERVER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
6	T.DOS	有	高 (3)	中 (2)	中 (2)	高 (3)	中 (2)	12
7	T.HACK_IMPERSON_TOE	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
8	T.CLIENT_REFUTE_ORIGIN	有	高 (3)	低 (1)	高 (3)	高 (3)	高 (3)	13
9	T.HARDWARE_FAILURE	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
10	T.PEER_FAILURE	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
11	T.CONNECTION_FAILURE	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
12	T.TOE_BUG	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
13	T.BUFFEROVERFLOW_ATTACK	有	高 (3)	中 (2)	中 (2)	高 (3)	中 (2)	12
14	T.TSQ_LINE	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
15	T.TSR_LINE	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
16	T.FORGERY_USER-ID-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
17	T.MODIFY_USER-ID-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
18	T.ERACE_USER-ID-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
19	T.IMPERSON_USER-ID-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
20	T.STEAL_USER-ID-PW_USER	無	－	－	－	－	－	0
21	T.DISCLOSE_USER-ID-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
22	T.FORGERY_USER-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
23	T.MODIFY_USER-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
24	T.ERACE_USER-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
25	T.IMPERSON_USER-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
26	T.STEAL_USER-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
27	T.DISCLOSE_USER-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
28	T.FORGERY_TST_USER	有	高 (3)	高 (3)	高 (3)	高 (3)	高 (3)	15
29	T.MODIFY_TST_USER	有	高 (3)	高 (3)	高 (3)	高 (3)	高 (3)	15
30	T.ERACE_TST_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
31	T.IMPERSON_TST_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
32	T.STEAL_TST_USER	無	－	－	－	－	－	0
33	T.DISCLOSE_TST_USER	無	－	－	－	－	－	0
34	T.FORGERY_TST_THIRD	有	高 (3)	高 (3)	高 (3)	高 (3)	高 (3)	15
35	T.MODIFY_TST_THIRD	有	高 (3)	高 (3)	高 (3)	高 (3)	高 (3)	15
36	T.ERACE_TST_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
37	T.IMPERSON_TST_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
38	T.STEAL_TST_THIRD	無	－	－	－	－	－	0
39	T.DISCLOSE_TST_THIRD	無	－	－	－	－	－	0
40	T.FORGERY_TAC_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
41	T.MODIFY_TAC_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
42	T.ERACE_TAC_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
43	T.IMPERSON_TAC_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
44	T.STEAL_TAC_USER	無	－	－	－	－	－	0

項番	脅威名	リスク	脅威格付					
		有無判定	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
45	T.DISCLOSE_TAC_USER	無	ー	ー	ー	ー	ー	0
46	T.FORGERY_TAC_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
47	T.MODIFY_TAC_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
48	T.ERACE_TAC_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
49	T.IMPERSON_TAC_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
50	T.STEAL_TAC_THIRD	無	ー	ー	ー	ー	ー	0
51	T.DISCLOSE_TAC_THIRD	無	ー	ー	ー	ー	ー	0
52	T.FORGERY_TAC-LOG_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
53	T.MODIFY_TAC-LOG_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
54	T.ERACE_TAC-LOG_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
55	T.IMPERSON_TAC-LOG_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
56	T.STEAL_TAC-LOG_USER	有	低 (1)	低 (1)	低 (1)	ー	低 (1)	4
57	T.DISCLOSE_TAC-LOG_USER	有	低 (1)	低 (1)	低 (1)	ー	低 (1)	4
58	T.FORGERY_TAC-LOG_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
59	T.MODIFY_TAC-LOG_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
60	T.ERACE_TAC-LOG_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
61	T.IMPERSON_TAC-LOG_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
62	T.STEAL_TAC-LOG_THIRD	有	低 (1)	低 (1)	低 (1)	ー	低 (1)	4
63	T.DISCLOSE_TAC-LOG_THIRD	有	低 (1)	低 (1)	低 (1)	ー	低 (1)	4
64	T.FORGERY_TAR_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
65	T.MODIFY_TAR_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
66	T.ERACE_TAR_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
67	T.IMPERSON_TAR_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
68	T.STEAL_TAR_USER	無	ー	ー	ー	ー	ー	0
69	T.DISCLOSE_TAR_USER	無	ー	ー	ー	ー	ー	0
70	T.FORGERY_TAR_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
71	T.MODIFY_TAR_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
72	T.ERACE_TAR_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
73	T.IMPERSON_TAR_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
74	T.STEAL_TAR_THIRD	無	ー	ー	ー	ー	ー	0
75	T.DISCLOSE_TAR_THIRD	無	ー	ー	ー	ー	ー	0
76	T.FORGERY_KEYST_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
77	T.MODIFY_KEYST_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
78	T.ERACE_KEYST_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
79	T.IMPERSON_KEYST_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
80	T.STEAL_KEYST_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
81	T.DISCLOSE_KEYST_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
82	T.FORGERY_KEYST_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
83	T.MODIFY_KEYST_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
84	T.ERACE_KEYST_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
85	T.IMPERSON_KEYST_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
86	T.STEAL_KEYST_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
87	T.DISCLOSE_KEYST_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
88	T.FORGERY_KEYST-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
89	T.MODIFY_KEYST-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
90	T.ERACE_KEYST-PW_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
91	T.IMPERSON_KEYST-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
92	T.STEAL_KEYST-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
93	T.DISCLOSE_KEYST-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
94	T.FORGERY_KEYST-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
95	T.MODIFY_KEYST-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
96	T.ERACE_KEYST-PW_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
97	T.IMPERSON_KEYST-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6

項番	脅威名	リスク	脅威格付					
		有無判定	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
98	T.STEAL_KEYST-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
99	T.DISCLOSE_KEYST-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
100	T.FORGERY_CERT_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
101	T.MODIFY_CERT_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
102	T.ERACE_CERT_USER	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
103	T.IMPERSON_CERT_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
104	T.STEAL_CERT_USER	無	－	－	－	－	－	0
105	T.DISCLOSE_CERT_USER	無	－	－	－	－	－	0
106	T.FORGERY_CERT_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
107	T.MODIFY_CERT_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
108	T.ERACE_CERT_THIRD	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
109	T.IMPERSON_CERT_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
110	T.STEAL_CERT_THIRD	無	－	－	－	－	－	0
111	T.DISCLOSE_CERT_THIRD	無	－	－	－	－	－	0
112	T.FORGERY_CRL-ARL_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
113	T.MODIFY_CRL-ARL_USER	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
114	T.ERACE_CRL-ARL_USER	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
115	T.IMPERSON_CRL-ARL_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
116	T.STEAL_CRL-ARL_USER	無	－	－	－	－	－	0
117	T.DISCLOSE_CRL-ARL_USER	無	－	－	－	－	－	0
118	T.FORGERY_CRL-ARL_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
119	T.MODIFY_CRL-ARL_THIRD	有	中 (2)	低 (1)	低 (1)	高 (3)	低 (1)	8
120	T.ERACE_CRL-ARL_THIRD	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
121	T.IMPERSON_CRL-ARL_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
122	T.STEAL_CRL-ARL_THIRD	無	－	－	－	－	－	0
123	T.DISCLOSE_CRL-ARL_THIRD	無	－	－	－	－	－	0
124	T.FORGERY_PRI-KEY_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
125	T.MODIFY_PRI-KEY_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
126	T.ERACE_PRI-KEY_USER	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
127	T.IMPERSON_PRI-KEY_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
128	T.STEAL_PRI-KEY_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
129	T.DISCLOSE_PRI-KEY_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
130	T.FORGERY_PRI-KEY_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
131	T.MODIFY_PRI-KEY_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
132	T.ERACE_PRI-KEY_THIRD	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
133	T.IMPERSON_PRI-KEY_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
134	T.STEAL_PRI-KEY_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
135	T.DISCLOSE_PRI-KEY_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
136	T.FORGERY_PRI-KEY-PW_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
137	T.MODIFY_PRI-KEY-PW_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
138	T.ERACE_PRI-KEY-PW_USER	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
139	T.IMPERSON_PRI-KEY-PW_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
140	T.STEAL_PRI-KEY-PW_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
141	T.DISCLOSE_PRI-KEY-PW_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
142	T.FORGERY_PRI-KEY-PW_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
143	T.MODIFY_PRI-KEY-PW_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
144	T.ERACE_PRI-KEY-PW_THIRD	有	低 (1)	低 (1)	低 (1)	中 (2)	低 (1)	6
145	T.IMPERSON_PRI-KEY-PW_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
146	T.STEAL_PRI-KEY-PW_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
147	T.DISCLOSE_PRI-KEY-PW_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
148	T.FORGERY_OPE-ID-PW_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
149	T.MODIFY_OPE-ID-PW_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
150	T.ERACE_OPE-ID-PW_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5

項番	脅威名	リスク	脅威格付					
		有無判定	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
151	T.IMPERSON_OPE-ID-PW_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
152	T.STEAL_OPE-ID-PW_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
153	T.DISCLOSE_OPE-ID-PW_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
154	T.FORGERY_OPE-ID-PW_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
155	T.MODIFY_OPE-ID-PW_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
156	T.ERACE_OPE-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
157	T.IMPERSON_OPE-ID-PW_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
158	T.STEAL_OPE-ID-PW_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
159	T.DISCLOSE_OPE-ID-PW_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
160	T.FORGERY_DB-SERIAL_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
161	T.MODIFY_DB-SERIAL_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
162	T.ERACE_DB-SERIAL_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
163	T.IMPERSON_DB-SERIAL_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
164	T.STEAL_DB-SERIAL_USER	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
165	T.DISCLOSE_DB-SERIAL_USER	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
166	T.FORGERY_DB-SERIAL_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
167	T.MODIFY_DB-SERIAL_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
168	T.ERACE_DB-SERIAL_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
169	T.IMPERSON_DB-SERIAL_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
170	T.STEAL_DB-SERIAL_THIRD	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
171	T.DISCLOSE_DB-SERIAL_THIRD	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
172	T.FORGERY_DB-USER-ID_USER	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
173	T.MODIFY_DB-USER-ID_USER	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
174	T.ERACE_DB-USER-ID_USER	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
175	T.IMPERSON_DB-USER-ID_USER	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
176	T.STEAL_DB-USER-ID_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
177	T.DISCLOSE_DB-USER-ID_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
178	T.FORGERY_DB-USER-ID_THIRD	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
179	T.MODIFY_DB-USER-ID_THIRD	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
180	T.ERACE_DB-USER-ID_THIRD	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
181	T.IMPERSON_DB-USER-ID_THIRD	有	低 (1)	低 (1)	低 (1)	高 (3)	低 (1)	7
182	T.STEAL_DB-USER-ID_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
183	T.DISCLOSE_DB-USER-ID_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
184	T.FORGERY_DB-TIME_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
185	T.MODIFY_DB-TIME_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
186	T.ERACE_DB-TIME_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
187	T.IMPERSON_DB-TIME_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
188	T.STEAL_DB-TIME_USER	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
189	T.DISCLOSE_DB-TIME_USER	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
190	T.FORGERY_DB-TIME_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
191	T.MODIFY_DB-TIME_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
192	T.ERACE_DB-TIME_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
193	T.IMPERSON_DB-TIME_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
194	T.STEAL_DB-TIME_THIRD	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
195	T.DISCLOSE_DB-TIME_THIRD	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
196	T.FORGERY_DB-TST_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
197	T.MODIFY_DB-TST_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
198	T.ERACE_DB-TST_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
199	T.IMPERSON_DB-TST_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
200	T.STEAL_DB-TST_USER	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
201	T.DISCLOSE_DB-TST_USER	有	低 (1)	低 (1)	低 (1)	－	低 (1)	4
202	T.FORGERY_DB-TST_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
203	T.MODIFY_DB-TST_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9

項番	脅威名	リスク	脅威格付					
		有無 判定	潜在的 損失	再現性	攻撃利用 可能性	影響 ユーザ	発見 可能性	合計 点
204	T.ERACE_DB-TST_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
205	T.IMPERSON_DB-TST_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
206	T.STEAL_DB-TST_THIRD	有	低 (1)	低 (1)	低 (1)	ー	低 (1)	4
207	T.DISCLOSE_DB-TST_THIRD	有	低 (1)	低 (1)	低 (1)	ー	低 (1)	4
208	T.FORGERY_LINK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
209	T.MODIFY_LINK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
210	T.ERACE_LINK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
211	T.IMPERSON_LINK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
212	T.STEAL_LINK_USER	無	ー	ー	ー	ー	ー	0
213	T.DISCLOSE_LINK_USER	無	ー	ー	ー	ー	ー	0
214	T.FORGERY_LINK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
215	T.MODIFY_LINK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
216	T.ERACE_LINK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
217	T.IMPERSON_LINK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
218	T.STEAL_LINK_THIRD	無	ー	ー	ー	ー	ー	0
219	T.DISCLOSE_LINK_THIRD	無	ー	ー	ー	ー	ー	0
220	T.FORGERY_CONFIG_USER	有	高 (3)	低 (1)	低 (1)	中 (2)	低 (1)	8
221	T.MODIFY_CONFIG_USER	有	高 (3)	低 (1)	低 (1)	中 (2)	低 (1)	8
222	T.ERACE_CONFIG_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
223	T.IMPERSON_CONFIG_USER	有	高 (3)	低 (1)	低 (1)	中 (2)	低 (1)	8
224	T.STEAL_CONFIG_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
225	T.DISCLOSE_CONFIG_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
226	T.FORGERY_CONFIG_THIRD	有	高 (3)	低 (1)	低 (1)	中 (2)	低 (1)	8
227	T.MODIFY_CONFIG_THIRD	有	高 (3)	低 (1)	低 (1)	中 (2)	低 (1)	8
228	T.ERACE_CONFIG_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
229	T.IMPERSON_CONFIG_THIRD	有	高 (3)	低 (1)	低 (1)	中 (2)	低 (1)	8
230	T.STEAL_CONFIG_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
231	T.DISCLOSE_CONFIG_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
232	T.FORGERY_DB-ID-PW_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
233	T.MODIFY_DB-ID-PW_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
234	T.ERACE_DB-ID-PW_USER	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
235	T.IMPERSON_DB-ID-PW_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
236	T.STEAL_DB-ID-PW_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
237	T.DISCLOSE_DB-ID-PW_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
238	T.FORGERY_DB-ID-PW_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
239	T.MODIFY_DB-ID-PW_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
240	T.ERACE_DB-ID-PW_THIRD	有	低 (1)	低 (1)	低 (1)	低 (1)	低 (1)	5
241	T.IMPERSON_DB-ID-PW_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
242	T.STEAL_DB-ID-PW_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
243	T.DISCLOSE_DB-ID-PW_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
244	T.FORGERY_LINK-PROV_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
245	T.MODIFY_LINK-PROV_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
246	T.ERACE_LINK-PROV_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
247	T.IMPERSON_LINK-PROV_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
248	T.STEAL_LINK-PROV_USER	無	ー	ー	ー	ー	ー	0
249	T.DISCLOSE_LINK-PROV_USER	無	ー	ー	ー	ー	ー	0
250	T.FORGERY_LINK-PROV_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
251	T.MODIFY_LINK-PROV_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
252	T.ERACE_LINK-PROV_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
253	T.IMPERSON_LINK-PROV_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
254	T.STEAL_LINK-PROV_THIRD	無	ー	ー	ー	ー	ー	0
255	T.DISCLOSE_LINK-PROV_THIRD	無	ー	ー	ー	ー	ー	0
256	T.FORGERY_EVENT_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7

項番	脅威名	リスク	脅威格付					
		有無判定	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
257	T.MODIFY_EVENT_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
258	T.ERACE_EVENT_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
259	T.IMPERSON_EVENT_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
260	T.STEAL_EVENT_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
261	T.DISCLOSE_EVENT_USER	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
262	T.FORGERY_EVENT_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
263	T.MODIFY_EVENT_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
264	T.ERACE_EVENT_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
265	T.IMPERSON_EVENT_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
266	T.STEAL_EVENT_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
267	T.DISCLOSE_EVENT_THIRD	有	中 (2)	低 (1)	低 (1)	中 (2)	低 (1)	7
268	T.FORGERY_CLOCK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
269	T.MODIFY_CLOCK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
270	T.ERACE_CLOCK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
271	T.IMPERSON_CLOCK_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
272	T.STEAL_CLOCK_USER	無	―	―	―	―	―	0
273	T.DISCLOSE_CLOCK_USER	無	―	―	―	―	―	0
274	T.FORGERY_CLOCK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
275	T.MODIFY_CLOCK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
276	T.ERACE_CLOCK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
277	T.IMPERSON_CLOCK_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
278	T.STEAL_CLOCK_THIRD	無	―	―	―	―	―	0
279	T.DISCLOSE_CLOCK_THIRD	無	―	―	―	―	―	0
280	T.FORGERY_MOD-CRE-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
281	T.MODIFY_MOD-CRE-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
282	T.ERACE_MOD-CRE-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
283	T.IMPERSON_MOD-CRE-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
284	T.STEAL_MOD-CRE-TS_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
285	T.DISCLOSE_MOD-CRE-TS_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
286	T.FORGERY_MOD-CRE-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
287	T.MODIFY_MOD-CRE-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
288	T.ERACE_MOD-CRE-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
289	T.IMPERSON_MOD-CRE-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
290	T.STEAL_MOD-CRE-TS_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
291	T.DISCLOSE_MOD-CRE-TS_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
292	T.FORGERY_MOD-STORE_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
293	T.MODIFY_MOD-STORE_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
294	T.ERACE_MOD-STORE_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
295	T.IMPERSON_MOD-STORE_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
296	T.STEAL_MOD-STORE_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
297	T.DISCLOSE_MOD-STORE_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
298	T.FORGERY_MOD-STORE_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
299	T.MODIFY_MOD-STORE_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
300	T.ERACE_MOD-STORE_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
301	T.IMPERSON_MOD-STORE_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
302	T.STEAL_MOD-STORE_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
303	T.DISCLOSE_MOD-STORE_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
304	T.FORGERY_MOD-COM-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
305	T.MODIFY_MOD-COM-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
306	T.ERACE_MOD-COM-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
307	T.IMPERSON_MOD-COM-TS_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
308	T.STEAL_MOD-COM-TS_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
309	T.DISCLOSE_MOD-COM-TS_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6

項番	脅威名	リスク	脅威格付					
		有無 判定	潜在的 損失	再現性	攻撃利用 可能性	影響 ユーザ	発見 可能性	合計 点
310	T.FORGERY_MOD-COM-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
311	T.MODIFY_MOD-COM-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
312	T.ERACE_MOD-COM-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
313	T.IMPERSON_MOD-COM-TS_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
314	T.STEAL_MOD-COM-TS_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
315	T.DISCLOSE_MOD-COM-TS_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
316	T.FORGERY_MOD-TIME_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
317	T.MODIFY_MOD-TIME_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
318	T.ERACE_MOD-TIME_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
319	T.IMPERSON_MOD-TIME_USER	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
320	T.STEAL_MOD-TIME_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
321	T.DISCLOSE_MOD-TIME_USER	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
322	T.FORGERY_MOD-TIME_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
323	T.MODIFY_MOD-TIME_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
324	T.ERACE_MOD-TIME_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
325	T.IMPERSON_MOD-TIME_THIRD	有	高 (3)	低 (1)	低 (1)	高 (3)	低 (1)	9
326	T.STEAL_MOD-TIME_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6
327	T.DISCLOSE_MOD-TIME_THIRD	有	中 (2)	低 (1)	低 (1)	低 (1)	低 (1)	6

第5章 内部不正を考慮したセキュリティ評価

1. 内部不正の考え方

管理者、運用者及び監査者からなる内部関係者に関して、不正を行う可能性があることを想定して評価を実施する。但し、複数人運用時において、内部関係者の結託による不正は行われないことと想定する。

2. 内部不正を考慮したセキュリティ環境

2-1 前提

内部不正を考慮したセキュリティ環境の前提について、「表 4　TOE に係るセキュリティ環境の前提一覧」及び「表 10　TOE に係るセキュリティ環境の前提の実現方法例一覧」に対して差異がある前提一覧について、以下の表 15に示す。

表 15　内部不正を考慮した場合のセキュリティ環境の前提の差異一覧

#	分類	項目	説明	実現方法例
4	人的な前提（Personnel assumptions）	A.ADMIN	一人以上の許可された管理者が、割り当てられる。彼らは、TOE と TOE に含まれる情報のセキュリティを管理する資格を持つ。さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低める可能性は低いとともに、複数人運用時において他の管理者･運用者･監査者と結託はしない。	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、管理者として任命される。
5		A.OPERATOR	一人以上の許可された運用者が、割り当てられる。彼らは、TOE を操作する資格を持つ。さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低める可能性は低いとともに、複数人運用時において他の管理者･運用者･監査者と結託はしない。	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、運用者として任命される。
6		A.AUDITOR	一人以上の許可された監査者が、割り当てられる。TOE に関するログを取得し、分析を行う。また、リンク情報の整合性の確認を行う。さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低める可能性は低いとともに、複数人運用時において他の管理者･運用者･監査者と結託はしない。	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、監査者として任命される。

#	分類	項目	説明	実現方法例
14	接続に関する前提（Connectivity assumptions）	A.ABSTRACT	TOE が動作するために必要な OS や依存するﾗｲﾌﾞﾗﾘは、部外者により不正に改変される可能性はないとともに、複数人運用時においては、内部関係者による不正な改変も防止される。	時刻認証業務及びセキュﾘﾃｨに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、管理者、運用者もしくは監査者として任命され、結託による不正は行わない。
15		A.SEPARATION	TOE が動作するマシンには、TOE の動作に必要なｿﾌﾄｳｪｱ以外が部外者により不正にｲﾝｽﾄｰﾙされる可能性はないとともに、複数人運用時においては、内部関係者による不正なｲﾝｽﾄｰﾙも防止される。	時刻認証業務及びセキュﾘﾃｨに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者が、管理者、運用者もしくは監査者として任命され、結託による不正は行わない。

2-2 脅威

内部不正を考慮したセキュリティ環境の脅威については、「表 5　TOE に係るセキュリティ環境の脅威一覧」における TOE（共通）に分類される脅威について、攻撃者を管理者、運用者及び監査者からなる内部関係者とした場合のそれぞれの脅威が、新たに追加される脅威となると想定する。

内部不正を考慮した場合のセキュリティ環境において追加される脅威名一覧を、以下の表 16に示す。

表 16　内部不正を考慮した場合のセキュリティ環境の脅威名の追加一覧

項番	資産	主体	汎用脅威	脅威名	脅威内容
1	USER-ID-PW	ADMIN	T.FORGERY	T.FORGERY_USER-ID-PW_ADMIN	偽造したID/PWをサーバに登録
2	USER-ID-PW	ADMIN	T.MODIFY	T.MODIFY_USER-ID-PW_ADMIN	サーバに登録されたID/PWを改竄
3	USER-ID-PW	ADMIN	T.ERACE	T.ERACE_USER-ID-PW_ADMIN	サーバに登録されたID/PWを消去
4	USER-ID-PW	ADMIN	T.IMPERSON	T.IMPERSON_USER-ID-PW_ADMIN	アクセス権が有るため脅威外
5	USER-ID-PW	ADMIN	T.STEAL	T.STEAL_USER-ID-PW_ADMIN	サーバに登録されたID/PWを不正に取得
6	USER-ID-PW	ADMIN	T.DISCLOSE	T.DISCLOSE_USER-ID-PW_ADMIN	サーバに登録されたID/PWを不正に漏洩
7	USER-ID-PW	OPE	T.FORGERY	T.FORGERY_USER-ID-PW_OPE	偽造したID/PWをサーバに登録
8	USER-ID-PW	OPE	T.MODIFY	T.MODIFY_USER-ID-PW_OPE	サーバに登録されたID/PWを改竄
9	USER-ID-PW	OPE	T.ERACE	T.ERACE_USER-ID-PW_OPE	サーバに登録されたID/PWを消去
10	USER-ID-PW	OPE	T.IMPERSON	T.IMPERSON_USER-ID-PW_OPE	アクセス権が有るため脅威外
11	USER-ID-PW	OPE	T.STEAL	T.STEAL_USER-ID-PW_OPE	サーバに登録されたID/PWを不正に取得
12	USER-ID-PW	OPE	T.DISCLOSE	T.DISCLOSE_USER-ID-PW_OPE	サーバに登録されたID/PWを不正に漏洩
13	USER-ID-PW	AUDIT	T.FORGERY	T.FORGERY_USER-ID-PW_AUDIT	偽造したID/PWをサーバに登録
14	USER-ID-PW	AUDIT	T.MODIFY	T.MODIFY_USER-ID-PW_AUDIT	サーバに登録されたID/PWを改竄
15	USER-ID-PW	AUDIT	T.ERACE	T.ERACE_USER-ID-PW_AUDIT	サーバに登録されたID/PWを消去
16	USER-ID-PW	AUDIT	T.IMPERSON	T.IMPERSON_USER-ID-PW_AUDIT	権限者に成りすましてID/PWにアクセス
17	USER-ID-PW	AUDIT	T.STEAL	T.STEAL_USER-ID-PW_AUDIT	サーバに登録されたID/PWを不正に取得
18	USER-ID-PW	AUDIT	T.DISCLOSE	T.DISCLOSE_USER-ID-PW_AUDIT	サーバに登録されたID/PWを不正に漏洩
19	TST	ADMIN	T.FORGERY	T.FORGERY_TST_ADMIN	偽造したＴＳＴを本物と偽って流通
20	TST	ADMIN	T.MODIFY	T.MODIFY_TST_ADMIN	改竄したＴＳＴを本物と偽って流通
21	TST	ADMIN	T.ERACE	T.ERACE_TST_ADMIN	発行されたＴＳＴを消去
22	TST	ADMIN	T.IMPERSON	T.IMPERSON_TST_ADMIN	発行者への成り済まし
23	TST	ADMIN	T.STEAL	T.STEAL_TST_ADMIN	機密性不要のため脅威外
24	TST	ADMIN	T.DISCLOSE	T.DISCLOSE_TST_ADMIN	機密性不要のため脅威外
25	TST	OPE	T.FORGERY	T.FORGERY_TST_OPE	偽造したＴＳＴを本物と偽って流通
26	TST	OPE	T.MODIFY	T.MODIFY_TST_OPE	改竄したＴＳＴを本物と偽って流通
27	TST	OPE	T.ERACE	T.ERACE_TST_OPE	発行されたＴＳＴを消去
28	TST	OPE	T.IMPERSON	T.IMPERSON_TST_OPE	発行者への成り済まし
29	TST	OPE	T.STEAL	T.STEAL_TST_OPE	機密性不要のため脅威外
30	TST	OPE	T.DISCLOSE	T.DISCLOSE_TST_OPE	機密性不要のため脅威外
31	TST	AUDIT	T.FORGERY	T.FORGERY_TST_AUDIT	偽造したＴＳＴを本物と偽って流通
32	TST	AUDIT	T.MODIFY	T.MODIFY_TST_AUDIT	改竄したＴＳＴを本物と偽って流通
33	TST	AUDIT	T.ERACE	T.ERACE_TST_AUDIT	発行されたＴＳＴを消去
34	TST	AUDIT	T.IMPERSON	T.IMPERSON_TST_AUDIT	発行者への成り済まし
35	TST	AUDIT	T.STEAL	T.STEAL_TST_AUDIT	機密性不要のため脅威外
36	TST	AUDIT	T.DISCLOSE	T.DISCLOSE_TST_AUDIT	機密性不要のため脅威外
37	TAC	ADMIN	T.FORGERY	T.FORGERY_TAC_ADMIN	偽造したTACを登録もしくは流通
38	TAC	ADMIN	T.MODIFY	T.MODIFY_TAC_ADMIN	改竄したTACを登録もしくは流通
39	TAC	ADMIN	T.ERACE	T.ERACE_TAC_ADMIN	サーバに登録されたTACの消去
40	TAC	ADMIN	T.IMPERSON	T.IMPERSON_TAC_ADMIN	発行者への成り済まし
41	TAC	ADMIN	T.STEAL	T.STEAL_TAC_ADMIN	機密性不要のため脅威外
42	TAC	ADMIN	T.DISCLOSE	T.DISCLOSE_TAC_ADMIN	機密性不要のため脅威外
43	TAC	OPE	T.FORGERY	T.FORGERY_TAC_OPE	偽造したTACを登録もしくは流通
44	TAC	OPE	T.MODIFY	T.MODIFY_TAC_OPE	改竄したTACを登録もしくは流通
45	TAC	OPE	T.ERACE	T.ERACE_TAC_OPE	サーバに登録されたTACの消去
46	TAC	OPE	T.IMPERSON	T.IMPERSON_TAC_OPE	発行者への成り済まし
47	TAC	OPE	T.STEAL	T.STEAL_TAC_OPE	機密性不要のため脅威外

項番	資産	主体	汎用脅威	脅威名	脅威内容
48	TAC	OPE	T.DISCLOSE	T.DISCLOSE_TAC_OPE	機密性不要のため脅威外
49	TAC	AUDIT	T.FORGERY	T.FORGERY_TAC_AUDIT	偽造したTACを登録もしくは流通
50	TAC	AUDIT	T.MODIFY	T.MODIFY_TAC_AUDIT	改竄したTACを登録もしくは流通
51	TAC	AUDIT	T.ERACE	T.ERACE_TAC_AUDIT	サーバに登録されたTACの消去
52	TAC	AUDIT	T.IMPERSON	T.IMPERSON_TAC_AUDIT	発行者への成り済まし
53	TAC	AUDIT	T.STEAL	T.STEAL_TAC_AUDIT	機密性不要のため脅威外
54	TAC	AUDIT	T.DISCLOSE	T.DISCLOSE_TAC_AUDIT	機密性不要のため脅威外
55	TAC-LOG	ADMIN	T.FORGERY	T.FORGERY_TAC-LOG_ADMIN	偽造したTACログを登録
56	TAC-LOG	ADMIN	T.MODIFY	T.MODIFY_TAC-LOG_ADMIN	改竄したTACログを登録
57	TAC-LOG	ADMIN	T.ERACE	T.ERACE_TAC-LOG_ADMIN	サーバに保管されたTACログの消去
58	TAC-LOG	ADMIN	T.IMPERSON	T.IMPERSON_TAC-LOG_ADMIN	アクセス権が有るため脅威外
59	TAC-LOG	ADMIN	T.STEAL	T.STEAL_TAC-LOG_ADMIN	TACログを不正に取得
60	TAC-LOG	ADMIN	T.DISCLOSE	T.DISCLOSE_TAC-LOG_ADMIN	TACログを不正に漏洩
61	TAC-LOG	OPE	T.FORGERY	T.FORGERY_TAC-LOG_OPE	偽造したTACログを登録
62	TAC-LOG	OPE	T.MODIFY	T.MODIFY_TAC-LOG_OPE	改竄したTACログを登録
63	TAC-LOG	OPE	T.ERACE	T.ERACE_TAC-LOG_OPE	サーバに保管されたTACログの消去
64	TAC-LOG	OPE	T.IMPERSON	T.IMPERSON_TAC-LOG_OPE	アクセス権が有るため脅威外
65	TAC-LOG	OPE	T.STEAL	T.STEAL_TAC-LOG_OPE	TACログを不正に取得
66	TAC-LOG	OPE	T.DISCLOSE	T.DISCLOSE_TAC-LOG_OPE	TACログを不正に漏洩
67	TAC-LOG	AUDIT	T.FORGERY	T.FORGERY_TAC-LOG_AUDIT	偽造したTACログを登録
68	TAC-LOG	AUDIT	T.MODIFY	T.MODIFY_TAC-LOG_AUDIT	改竄したTACログを登録
69	TAC-LOG	AUDIT	T.ERACE	T.ERACE_TAC-LOG_AUDIT	サーバに保管されたTACログの消去
70	TAC-LOG	AUDIT	T.IMPERSON	T.IMPERSON_TAC-LOG_AUDIT	アクセス権所有者への成り済まし
71	TAC-LOG	AUDIT	T.STEAL	T.STEAL_TAC-LOG_AUDIT	TACログを不正に取得
72	TAC-LOG	AUDIT	T.DISCLOSE	T.DISCLOSE_TAC-LOG_AUDIT	TACログを不正に漏洩
73	TAR	ADMIN	T.FORGERY	T.FORGERY_TAR_ADMIN	偽造したTARを登録もしくは流通
74	TAR	ADMIN	T.MODIFY	T.MODIFY_TAR_ADMIN	改竄したTARを登録もしくは流通
75	TAR	ADMIN	T.ERACE	T.ERACE_TAR_ADMIN	サーバに登録されたTARの消去
76	TAR	ADMIN	T.IMPERSON	T.IMPERSON_TAR_ADMIN	発行者への成り済まし
77	TAR	ADMIN	T.STEAL	T.STEAL_TAR_ADMIN	機密性不要のため脅威外
78	TAR	ADMIN	T.DISCLOSE	T.DISCLOSE_TAR_ADMIN	機密性不要のため脅威外
79	TAR	OPE	T.FORGERY	T.FORGERY_TAR_OPE	偽造したTARを登録もしくは流通
80	TAR	OPE	T.MODIFY	T.MODIFY_TAR_OPE	改竄したTARを登録もしくは流通
81	TAR	OPE	T.ERACE	T.ERACE_TAR_OPE	サーバに登録されたTARの消去
82	TAR	OPE	T.IMPERSON	T.IMPERSON_TAR_OPE	発行者への成り済まし
83	TAR	OPE	T.STEAL	T.STEAL_TAR_OPE	機密性不要のため脅威外
84	TAR	OPE	T.DISCLOSE	T.DISCLOSE_TAR_OPE	機密性不要のため脅威外
85	TAR	AUDIT	T.FORGERY	T.FORGERY_TAR_AUDIT	偽造したTARを登録もしくは流通
86	TAR	AUDIT	T.MODIFY	T.MODIFY_TAR_AUDIT	改竄したTARを登録もしくは流通
87	TAR	AUDIT	T.ERACE	T.ERACE_TAR_AUDIT	サーバに登録されたTARの消去
88	TAR	AUDIT	T.IMPERSON	T.IMPERSON_TAR_AUDIT	発行者への成り済まし
89	TAR	AUDIT	T.STEAL	T.STEAL_TAR_AUDIT	機密性不要のため脅威外
90	TAR	AUDIT	T.DISCLOSE	T.DISCLOSE_TAR_AUDIT	機密性不要のため脅威外
91	KEYST	ADMIN	T.FORGERY	T.FORGERY_KEYST_ADMIN	偽造したキーストアを登録
92	KEYST	ADMIN	T.MODIFY	T.MODIFY_KEYST_ADMIN	改竄したキーストアを登録
93	KEYST	ADMIN	T.ERACE	T.ERACE_KEYST_ADMIN	サーバに登録されたキーストアの消去
94	KEYST	ADMIN	T.IMPERSON	T.IMPERSON_KEYST_ADMIN	アクセス権が有るため脅威外
95	KEYST	ADMIN	T.STEAL	T.STEAL_KEYST_ADMIN	キーストアの中身を不正に取得
96	KEYST	ADMIN	T.DISCLOSE	T.DISCLOSE_KEYST_ADMIN	キーストアの中身を不正に漏洩
97	KEYST	OPE	T.FORGERY	T.FORGERY_KEYST_OPE	偽造したキーストアを登録
98	KEYST	OPE	T.MODIFY	T.MODIFY_KEYST_OPE	改竄したキーストアを登録
99	KEYST	OPE	T.ERACE	T.ERACE_KEYST_OPE	サーバに登録されたキーストアの消去
100	KEYST	OPE	T.IMPERSON	T.IMPERSON_KEYST_OPE	アクセス権所有者への成り済まし
101	KEYST	OPE	T.STEAL	T.STEAL_KEYST_OPE	キーストアの中身を不正に取得
102	KEYST	OPE	T.DISCLOSE	T.DISCLOSE_KEYST_OPE	キーストアの中身を不正に漏洩
103	KEYST	AUDIT	T.FORGERY	T.FORGERY_KEYST_AUDIT	偽造したキーストアを登録
104	KEYST	AUDIT	T.MODIFY	T.MODIFY_KEYST_AUDIT	改竄したキーストアを登録
105	KEYST	AUDIT	T.ERACE	T.ERACE_KEYST_AUDIT	サーバに登録されたキーストアの消去
106	KEYST	AUDIT	T.IMPERSON	T.IMPERSON_KEYST_AUDIT	アクセス権所有者への成り済まし
107	KEYST	AUDIT	T.STEAL	T.STEAL_KEYST_AUDIT	キーストアの中身を不正に取得
108	KEYST	AUDIT	T.DISCLOSE	T.DISCLOSE_KEYST_AUDIT	キーストアの中身を不正に漏洩

項番	資産	主体	汎用脅威	脅威名	脅威内容
109	KEYST-PW	ADMIN	T.FORGERY	T.FORGERY_KEYST-PW_ADMIN	偽造したPWをサーバに登録
110	KEYST-PW	ADMIN	T.MODIFY	T.MODIFY_KEYST-PW_ADMIN	サーバに登録されたPWを改竄
111	KEYST-PW	ADMIN	T.ERACE	T.ERACE_KEYST-PW_ADMIN	サーバに登録されたPWを消去
112	KEYST-PW	ADMIN	T.IMPERSON	T.IMPERSON_KEYST-PW_ADMIN	アクセス権が有るため脅威外
113	KEYST-PW	ADMIN	T.STEAL	T.STEAL_KEYST-PW_ADMIN	サーバに登録されたPWを不正に取得
114	KEYST-PW	ADMIN	T.DISCLOSE	T.DISCLOSE_KEYST-PW_ADMIN	サーバに登録されたPWを不正に漏洩
115	KEYST-PW	OPE	T.FORGERY	T.FORGERY_KEYST-PW_OPE	偽造したPWをサーバに登録
116	KEYST-PW	OPE	T.MODIFY	T.MODIFY_KEYST-PW_OPE	サーバに登録されたPWを改竄
117	KEYST-PW	OPE	T.ERACE	T.ERACE_KEYST-PW_OPE	サーバに登録されたPWを消去
118	KEYST-PW	OPE	T.IMPERSON	T.IMPERSON_KEYST-PW_OPE	アクセス権所有者への成り済まし
119	KEYST-PW	OPE	T.STEAL	T.STEAL_KEYST-PW_OPE	サーバに登録されたPWを不正に取得
120	KEYST-PW	OPE	T.DISCLOSE	T.DISCLOSE_KEYST-PW_OPE	サーバに登録されたPWを不正に漏洩
121	KEYST-PW	AUDIT	T.FORGERY	T.FORGERY_KEYST-PW_AUDIT	偽造したPWをサーバに登録
122	KEYST-PW	AUDIT	T.MODIFY	T.MODIFY_KEYST-PW_AUDIT	サーバに登録されたPWを改竄
123	KEYST-PW	AUDIT	T.ERACE	T.ERACE_KEYST-PW_AUDIT	サーバに登録されたPWを消去
124	KEYST-PW	AUDIT	T.IMPERSON	T.IMPERSON_KEYST-PW_AUDIT	アクセス権所有者への成り済まし
125	KEYST-PW	AUDIT	T.STEAL	T.STEAL_KEYST-PW_AUDIT	サーバに登録されたPWを不正に取得
126	KEYST-PW	AUDIT	T.DISCLOSE	T.DISCLOSE_KEYST-PW_AUDIT	サーバに登録されたPWを不正に漏洩
127	CERT	ADMIN	T.FORGERY	T.FORGERY_CERT_ADMIN	偽造した証明書をサーバに登録
128	CERT	ADMIN	T.MODIFY	T.MODIFY_CERT_ADMIN	サーバに登録された証明書を改竄
129	CERT	ADMIN	T.ERACE	T.ERACE_CERT_ADMIN	サーバに登録された証明書を消去
130	CERT	ADMIN	T.IMPERSON	T.IMPERSON_CERT_ADMIN	発行者への成り済まし
131	CERT	ADMIN	T.STEAL	T.STEAL_CERT_ADMIN	機密性不要のため脅威外
132	CERT	ADMIN	T.DISCLOSE	T.DISCLOSE_CERT_ADMIN	機密性不要のため脅威外
133	CERT	OPE	T.FORGERY	T.FORGERY_CERT_OPE	偽造した証明書をサーバに登録
134	CERT	OPE	T.MODIFY	T.MODIFY_CERT_OPE	サーバに登録された証明書を改竄
135	CERT	OPE	T.ERACE	T.ERACE_CERT_OPE	サーバに登録された証明書を消去
136	CERT	OPE	T.IMPERSON	T.IMPERSON_CERT_OPE	発行者への成り済まし
137	CERT	OPE	T.STEAL	T.STEAL_CERT_OPE	機密性不要のため脅威外
138	CERT	OPE	T.DISCLOSE	T.DISCLOSE_CERT_OPE	機密性不要のため脅威外
139	CERT	AUDIT	T.FORGERY	T.FORGERY_CERT_AUDIT	偽造した証明書をサーバに登録
140	CERT	AUDIT	T.MODIFY	T.MODIFY_CERT_AUDIT	サーバに登録された証明書を改竄
141	CERT	AUDIT	T.ERACE	T.ERACE_CERT_AUDIT	サーバに登録された証明書を消去
142	CERT	AUDIT	T.IMPERSON	T.IMPERSON_CERT_AUDIT	発行者への成り済まし
143	CERT	AUDIT	T.STEAL	T.STEAL_CERT_AUDIT	機密性不要のため脅威外
144	CERT	AUDIT	T.DISCLOSE	T.DISCLOSE_CERT_AUDIT	機密性不要のため脅威外
145	CRL-ARL	ADMIN	T.FORGERY	T.FORGERY_CRL-ARL_ADMIN	偽造したCRL･ARLをサーバに登録
146	CRL-ARL	ADMIN	T.MODIFY	T.MODIFY_CRL-ARL_ADMIN	サーバに登録されたCRL･ARLを改竄
147	CRL-ARL	ADMIN	T.ERACE	T.ERACE_CRL-ARL_ADMIN	サーバに登録されたCRL･ARLを消去
148	CRL-ARL	ADMIN	T.IMPERSON	T.IMPERSON_CRL-ARL_ADMIN	発行者への成り済まし
149	CRL-ARL	ADMIN	T.STEAL	T.STEAL_CRL-ARL_ADMIN	機密性不要のため脅威外
150	CRL-ARL	ADMIN	T.DISCLOSE	T.DISCLOSE_CRL-ARL_ADMIN	機密性不要のため脅威外
151	CRL-ARL	OPE	T.FORGERY	T.FORGERY_CRL-ARL_OPE	偽造したCRL･ARLをサーバに登録
152	CRL-ARL	OPE	T.MODIFY	T.MODIFY_CRL-ARL_OPE	サーバに登録されたCRL･ARLを改竄
153	CRL-ARL	OPE	T.ERACE	T.ERACE_CRL-ARL_OPE	サーバに登録されたCRL･ARLを消去
154	CRL-ARL	OPE	T.IMPERSON	T.IMPERSON_CRL-ARL_OPE	発行者への成り済まし
155	CRL-ARL	OPE	T.STEAL	T.STEAL_CRL-ARL_OPE	機密性不要のため脅威外
156	CRL-ARL	OPE	T.DISCLOSE	T.DISCLOSE_CRL-ARL_OPE	機密性不要のため脅威外
157	CRL-ARL	AUDIT	T.FORGERY	T.FORGERY_CRL-ARL_AUDIT	偽造したCRL･ARLをサーバに登録
158	CRL-ARL	AUDIT	T.MODIFY	T.MODIFY_CRL-ARL_AUDIT	サーバに登録されたCRL･ARLを改竄
159	CRL-ARL	AUDIT	T.ERACE	T.ERACE_CRL-ARL_AUDIT	サーバに登録されたCRL･ARLを消去
160	CRL-ARL	AUDIT	T.IMPERSON	T.IMPERSON_CRL-ARL_AUDIT	発行者への成り済まし
161	CRL-ARL	AUDIT	T.STEAL	T.STEAL_CRL-ARL_AUDIT	機密性不要のため脅威外
162	CRL-ARL	AUDIT	T.DISCLOSE	T.DISCLOSE_CRL-ARL_AUDIT	機密性不要のため脅威外
163	PRI-KEY	ADMIN	T.FORGERY	T.FORGERY_PRI-KEY_ADMIN	偽造した秘密鍵を登録
164	PRI-KEY	ADMIN	T.MODIFY	T.MODIFY_PRI-KEY_ADMIN	改竄した秘密鍵を登録
165	PRI-KEY	ADMIN	T.ERACE	T.ERACE_PRI-KEY_ADMIN	サーバに登録された秘密鍵の消去
166	PRI-KEY	ADMIN	T.IMPERSON	T.IMPERSON_PRI-KEY_ADMIN	アクセス権が有るため脅威外
167	PRI-KEY	ADMIN	T.STEAL	T.STEAL_PRI-KEY_ADMIN	平文の秘密鍵を不正に取得
168	PRI-KEY	ADMIN	T.DISCLOSE	T.DISCLOSE_PRI-KEY_ADMIN	平文の秘密鍵の中身を不正に漏洩
169	PRI-KEY	OPE	T.FORGERY	T.FORGERY_PRI-KEY_OPE	偽造した秘密鍵を登録

項番	資産	主体	汎用脅威	脅威名	脅威内容
170	PRI-KEY	OPE	T.MODIFY	T.MODIFY_PRI-KEY_OPE	改竄した秘密鍵を登録
171	PRI-KEY	OPE	T.ERACE	T.ERACE_PRI-KEY_OPE	サーバに登録された秘密鍵の消去
172	PRI-KEY	OPE	T.IMPERSON	T.IMPERSON_PRI-KEY_OPE	アクセス権所有者への成り済まし
173	PRI-KEY	OPE	T.STEAL	T.STEAL_PRI-KEY_OPE	平文の秘密鍵を不正に取得
174	PRI-KEY	OPE	T.DISCLOSE	T.DISCLOSE_PRI-KEY_OPE	平文の秘密鍵の中身を不正に漏洩
175	PRI-KEY	AUDIT	T.FORGERY	T.FORGERY_PRI-KEY_AUDIT	偽造した秘密鍵を登録
176	PRI-KEY	AUDIT	T.MODIFY	T.MODIFY_PRI-KEY_AUDIT	改竄した秘密鍵を登録
177	PRI-KEY	AUDIT	T.ERACE	T.ERACE_PRI-KEY_AUDIT	サーバに登録された秘密鍵の消去
178	PRI-KEY	AUDIT	T.IMPERSON	T.IMPERSON_PRI-KEY_AUDIT	アクセス権所有者への成り済まし
179	PRI-KEY	AUDIT	T.STEAL	T.STEAL_PRI-KEY_AUDIT	平文の秘密鍵を不正に取得
180	PRI-KEY	AUDIT	T.DISCLOSE	T.DISCLOSE_PRI-KEY_AUDIT	平文の秘密鍵の中身を不正に漏洩
181	PRI-KEY-PW	ADMIN	T.FORGERY	T.FORGERY_PRI-KEY-PW_ADMIN	偽造したPWをサーバに登録
182	PRI-KEY-PW	ADMIN	T.MODIFY	T.MODIFY_PRI-KEY-PW_ADMIN	サーバに登録されたPWを改竄
183	PRI-KEY-PW	ADMIN	T.ERACE	T.ERACE_PRI-KEY-PW_ADMIN	サーバに登録されたPWを消去
184	PRI-KEY-PW	ADMIN	T.IMPERSON	T.IMPERSON_PRI-KEY-PW_ADMIN	アクセス権が有るため脅威外
185	PRI-KEY-PW	ADMIN	T.STEAL	T.STEAL_PRI-KEY-PW_ADMIN	サーバに登録されたPWを不正に取得
186	PRI-KEY-PW	ADMIN	T.DISCLOSE	T.DISCLOSE_PRI-KEY-PW_ADMIN	サーバに登録されたPWを不正に漏洩
187	PRI-KEY-PW	OPE	T.FORGERY	T.FORGERY_PRI-KEY-PW_OPE	偽造したPWをサーバに登録
188	PRI-KEY-PW	OPE	T.MODIFY	T.MODIFY_PRI-KEY-PW_OPE	サーバに登録されたPWを改竄
189	PRI-KEY-PW	OPE	T.ERACE	T.ERACE_PRI-KEY-PW_OPE	サーバに登録されたPWを消去
190	PRI-KEY-PW	OPE	T.IMPERSON	T.IMPERSON_PRI-KEY-PW_OPE	アクセス権所有者への成り済まし
191	PRI-KEY-PW	OPE	T.STEAL	T.STEAL_PRI-KEY-PW_OPE	サーバに登録されたPWを不正に取得
192	PRI-KEY-PW	OPE	T.DISCLOSE	T.DISCLOSE_PRI-KEY-PW_OPE	サーバに登録されたPWを不正に漏洩
193	PRI-KEY-PW	AUDIT	T.FORGERY	T.FORGERY_PRI-KEY-PW_AUDIT	偽造したPWをサーバに登録
194	PRI-KEY-PW	AUDIT	T.MODIFY	T.MODIFY_PRI-KEY-PW_AUDIT	サーバに登録されたPWを改竄
195	PRI-KEY-PW	AUDIT	T.ERACE	T.ERACE_PRI-KEY-PW_AUDIT	サーバに登録されたPWを消去
196	PRI-KEY-PW	AUDIT	T.IMPERSON	T.IMPERSON_PRI-KEY-PW_AUDIT	アクセス権所有者への成り済まし
197	PRI-KEY-PW	AUDIT	T.STEAL	T.STEAL_PRI-KEY-PW_AUDIT	サーバに登録されたPWを不正に取得
198	PRI-KEY-PW	AUDIT	T.DISCLOSE	T.DISCLOSE_PRI-KEY-PW_AUDIT	サーバに登録されたPWを不正に漏洩
199	OPE-ID-PW	ADMIN	T.FORGERY	T.FORGERY_OPE-ID-PW_ADMIN	偽造したID/PWをサーバに登録
200	OPE-ID-PW	ADMIN	T.MODIFY	T.MODIFY_OPE-ID-PW_ADMIN	サーバに登録されたID/PWを改竄
201	OPE-ID-PW	ADMIN	T.ERACE	T.ERACE_OPE-ID-PW_ADMIN	サーバに登録されたID/PWを消去
202	OPE-ID-PW	ADMIN	T.IMPERSON	T.IMPERSON_OPE-ID-PW_ADMIN	アクセス権が有るため脅威外
203	OPE-ID-PW	ADMIN	T.STEAL	T.STEAL_OPE-ID-PW_ADMIN	サーバに登録されたID/PWを不正に取得
204	OPE-ID-PW	ADMIN	T.DISCLOSE	T.DISCLOSE_OPE-ID-PW_ADMIN	サーバに登録されたID/PWを不正に漏洩
205	OPE-ID-PW	OPE	T.FORGERY	T.FORGERY_OPE-ID-PW_OPE	偽造したID/PWをサーバに登録
206	OPE-ID-PW	OPE	T.MODIFY	T.MODIFY_OPE-ID-PW_OPE	サーバに登録されたID/PWを改竄
207	OPE-ID-PW	OPE	T.ERACE	T.ERACE_OPE-ID-PW_OPE	サーバに登録されたID/PWを消去
208	OPE-ID-PW	OPE	T.IMPERSON	T.IMPERSON_OPE-ID-PW_OPE	アクセス権所有者への成り済まし
209	OPE-ID-PW	OPE	T.STEAL	T.STEAL_OPE-ID-PW_OPE	サーバに登録されたID/PWを不正に取得
210	OPE-ID-PW	OPE	T.DISCLOSE	T.DISCLOSE_OPE-ID-PW_OPE	サーバに登録されたID/PWを不正に漏洩
211	OPE-ID-PW	AUDIT	T.FORGERY	T.FORGERY_OPE-ID-PW_AUDIT	偽造したID/PWをサーバに登録
212	OPE-ID-PW	AUDIT	T.MODIFY	T.MODIFY_OPE-ID-PW_AUDIT	サーバに登録されたID/PWを改竄
213	OPE-ID-PW	AUDIT	T.ERACE	T.ERACE_OPE-ID-PW_AUDIT	サーバに登録されたID/PWを消去
214	OPE-ID-PW	AUDIT	T.IMPERSON	T.IMPERSON_OPE-ID-PW_AUDIT	アクセス権所有者への成り済まし
215	OPE-ID-PW	AUDIT	T.STEAL	T.STEAL_OPE-ID-PW_AUDIT	サーバに登録されたID/PWを不正に取得
216	OPE-ID-PW	AUDIT	T.DISCLOSE	T.DISCLOSE_OPE-ID-PW_AUDIT	サーバに登録されたID/PWを不正に漏洩
217	DB-SERIAL	ADMIN	T.FORGERY	T.FORGERY_DB-SERIAL_ADMIN	偽造したシリアル番号をDBに登録
218	DB-SERIAL	ADMIN	T.MODIFY	T.MODIFY_DB-SERIAL_ADMIN	DB内のシリアル番号を改竄
219	DB-SERIAL	ADMIN	T.ERACE	T.ERACE_DB-SERIAL_ADMIN	DB内のシリアル番号を消去
220	DB-SERIAL	ADMIN	T.IMPERSON	T.IMPERSON_DB-SERIAL_ADMIN	アクセス権が有るため脅威外
221	DB-SERIAL	ADMIN	T.STEAL	T.STEAL_DB-SERIAL_ADMIN	DB内のシリアル番号を不正に取得
222	DB-SERIAL	ADMIN	T.DISCLOSE	T.DISCLOSE_DB-SERIAL_ADMIN	DB内のシリアル番号を不正に漏洩
223	DB-SERIAL	OPE	T.FORGERY	T.FORGERY_DB-SERIAL_OPE	偽造したシリアル番号をDBに登録
224	DB-SERIAL	OPE	T.MODIFY	T.MODIFY_DB-SERIAL_OPE	DB内のシリアル番号を改竄
225	DB-SERIAL	OPE	T.ERACE	T.ERACE_DB-SERIAL_OPE	DB内のシリアル番号を消去
226	DB-SERIAL	OPE	T.IMPERSON	T.IMPERSON_DB-SERIAL_OPE	アクセス権が有るため脅威外
227	DB-SERIAL	OPE	T.STEAL	T.STEAL_DB-SERIAL_OPE	DB内のシリアル番号を不正に取得
228	DB-SERIAL	OPE	T.DISCLOSE	T.DISCLOSE_DB-SERIAL_OPE	DB内のシリアル番号を不正に漏洩
229	DB-SERIAL	AUDIT	T.FORGERY	T.FORGERY_DB-SERIAL_AUDIT	偽造したシリアル番号をDBに登録
230	DB-SERIAL	AUDIT	T.MODIFY	T.MODIFY_DB-SERIAL_AUDIT	DB内のシリアル番号を改竄

項番	資産	主体	汎用脅威	脅威名	脅威内容
231	DB-SERIAL	AUDIT	T.ERACE	T.ERACE_DB-SERIAL_AUDIT	DB内のシリアル番号を消去
232	DB-SERIAL	AUDIT	T.IMPERSON	T.IMPERSON_DB-SERIAL_AUDIT	アクセス権所有者への成り済まし
233	DB-SERIAL	AUDIT	T.STEAL	T.STEAL_DB-SERIAL_AUDIT	DB内のシリアル番号を不正に取得
234	DB-SERIAL	AUDIT	T.DISCLOSE	T.DISCLOSE_DB-SERIAL_AUDIT	DB内のシリアル番号を不正に漏洩
235	DB-USER-ID	ADMIN	T.FORGERY	T.FORGERY_DB-USER-ID_ADMIN	偽造した利用者IDをDBに登録
236	DB-USER-ID	ADMIN	T.MODIFY	T.MODIFY_DB-USER-ID_ADMIN	DB内の利用者IDを改竄
237	DB-USER-ID	ADMIN	T.ERACE	T.ERACE_DB-USER-ID_ADMIN	DB内の利用者IDを消去
238	DB-USER-ID	ADMIN	T.IMPERSON	T.IMPERSON_DB-USER-ID_ADMIN	アクセス権が有るため脅威外
239	DB-USER-ID	ADMIN	T.STEAL	T.STEAL_DB-USER-ID_ADMIN	DB内の利用者IDを不正に取得
240	DB-USER-ID	ADMIN	T.DISCLOSE	T.DISCLOSE_DB-USER-ID_ADMIN	DB内の利用者IDを不正に漏洩
241	DB-USER-ID	OPE	T.FORGERY	T.FORGERY_DB-USER-ID_OPE	偽造した利用者IDをDBに登録
242	DB-USER-ID	OPE	T.MODIFY	T.MODIFY_DB-USER-ID_OPE	DB内の利用者IDを改竄
243	DB-USER-ID	OPE	T.ERACE	T.ERACE_DB-USER-ID_OPE	DB内の利用者IDを消去
244	DB-USER-ID	OPE	T.IMPERSON	T.IMPERSON_DB-USER-ID_OPE	アクセス権が有るため脅威外
245	DB-USER-ID	OPE	T.STEAL	T.STEAL_DB-USER-ID_OPE	DB内の利用者IDを不正に取得
246	DB-USER-ID	OPE	T.DISCLOSE	T.DISCLOSE_DB-USER-ID_OPE	DB内の利用者IDを不正に漏洩
247	DB-USER-ID	AUDIT	T.FORGERY	T.FORGERY_DB-USER-ID_AUDIT	偽造した利用者IDをDBに登録
248	DB-USER-ID	AUDIT	T.MODIFY	T.MODIFY_DB-USER-ID_AUDIT	DB内の利用者IDを改竄
249	DB-USER-ID	AUDIT	T.ERACE	T.ERACE_DB-USER-ID_AUDIT	DB内の利用者IDを消去
250	DB-USER-ID	AUDIT	T.IMPERSON	T.IMPERSON_DB-USER-ID_AUDIT	アクセス権所有者への成り済まし
251	DB-USER-ID	AUDIT	T.STEAL	T.STEAL_DB-USER-ID_AUDIT	DB内の利用者IDを不正に取得
252	DB-USER-ID	AUDIT	T.DISCLOSE	T.DISCLOSE_DB-USER-ID_AUDIT	DB内の利用者IDを不正に漏洩
253	DB-TIME	ADMIN	T.FORGERY	T.FORGERY_DB-TIME_ADMIN	偽造した発行時刻をDBに登録
254	DB-TIME	ADMIN	T.MODIFY	T.MODIFY_DB-TIME_ADMIN	DB内の発行時刻を改竄
255	DB-TIME	ADMIN	T.ERACE	T.ERACE_DB-TIME_ADMIN	DB内の発行時刻を消去
256	DB-TIME	ADMIN	T.IMPERSON	T.IMPERSON_DB-TIME_ADMIN	アクセス権が有るため脅威外
257	DB-TIME	ADMIN	T.STEAL	T.STEAL_DB-TIME_ADMIN	DB内の発行時刻を不正に取得
258	DB-TIME	ADMIN	T.DISCLOSE	T.DISCLOSE_DB-TIME_ADMIN	DB内の発行時刻を不正に漏洩
259	DB-TIME	OPE	T.FORGERY	T.FORGERY_DB-TIME_OPE	偽造した発行時刻をDBに登録
260	DB-TIME	OPE	T.MODIFY	T.MODIFY_DB-TIME_OPE	DB内の発行時刻を改竄
261	DB-TIME	OPE	T.ERACE	T.ERACE_DB-TIME_OPE	DB内の発行時刻を消去
262	DB-TIME	OPE	T.IMPERSON	T.IMPERSON_DB-TIME_OPE	アクセス権が有るため脅威外
263	DB-TIME	OPE	T.STEAL	T.STEAL_DB-TIME_OPE	DB内の発行時刻を不正に取得
264	DB-TIME	OPE	T.DISCLOSE	T.DISCLOSE_DB-TIME_OPE	DB内の発行時刻を不正に漏洩
265	DB-TIME	AUDIT	T.FORGERY	T.FORGERY_DB-TIME_AUDIT	偽造した発行時刻をDBに登録
266	DB-TIME	AUDIT	T.MODIFY	T.MODIFY_DB-TIME_AUDIT	DB内の発行時刻を改竄
267	DB-TIME	AUDIT	T.ERACE	T.ERACE_DB-TIME_AUDIT	DB内の発行時刻を消去
268	DB-TIME	AUDIT	T.IMPERSON	T.IMPERSON_DB-TIME_AUDIT	アクセス権所有者への成り済まし
269	DB-TIME	AUDIT	T.STEAL	T.STEAL_DB-TIME_AUDIT	DB内の発行時刻を不正に取得
270	DB-TIME	AUDIT	T.DISCLOSE	T.DISCLOSE_DB-TIME_AUDIT	DB内の発行時刻を不正に漏洩
271	DB-TST	ADMIN	T.FORGERY	T.FORGERY_DB-TST_ADMIN	偽造したTSTをDBに登録
272	DB-TST	ADMIN	T.MODIFY	T.MODIFY_DB-TST_ADMIN	DB内のTSTを改竄
273	DB-TST	ADMIN	T.ERACE	T.ERACE_DB-TST_ADMIN	DB内のTSTを消去
274	DB-TST	ADMIN	T.IMPERSON	T.IMPERSON_DB-TST_ADMIN	アクセス権が有るため脅威外
275	DB-TST	ADMIN	T.STEAL	T.STEAL_DB-TST_ADMIN	DB内のTSTを不正に取得
276	DB-TST	ADMIN	T.DISCLOSE	T.DISCLOSE_DB-TST_ADMIN	DB内のTSTを不正に漏洩
277	DB-TST	OPE	T.FORGERY	T.FORGERY_DB-TST_OPE	偽造したTSTをDBに登録
278	DB-TST	OPE	T.MODIFY	T.MODIFY_DB-TST_OPE	DB内のTSTを改竄
279	DB-TST	OPE	T.ERACE	T.ERACE_DB-TST_OPE	DB内のTSTを消去
280	DB-TST	OPE	T.IMPERSON	T.IMPERSON_DB-TST_OPE	アクセス権が有るため脅威外
281	DB-TST	OPE	T.STEAL	T.STEAL_DB-TST_OPE	DB内のTSTを不正に取得
282	DB-TST	OPE	T.DISCLOSE	T.DISCLOSE_DB-TST_OPE	DB内のTSTを不正に漏洩
283	DB-TST	AUDIT	T.FORGERY	T.FORGERY_DB-TST_AUDIT	偽造したTSTをDBに登録
284	DB-TST	AUDIT	T.MODIFY	T.MODIFY_DB-TST_AUDIT	DB内のTSTを改竄
285	DB-TST	AUDIT	T.ERACE	T.ERACE_DB-TST_AUDIT	DB内のTSTを消去
286	DB-TST	AUDIT	T.IMPERSON	T.IMPERSON_DB-TST_AUDIT	アクセス権所有者への成り済まし
287	DB-TST	AUDIT	T.STEAL	T.STEAL_DB-TST_AUDIT	DB内のTSTを不正に取得
288	DB-TST	AUDIT	T.DISCLOSE	T.DISCLOSE_DB-TST_AUDIT	DB内のTSTを不正に漏洩
289	LINK	ADMIN	T.FORGERY	T.FORGERY_LINK_ADMIN	偽造したリンク情報をサーバに登録
290	LINK	ADMIN	T.MODIFY	T.MODIFY_LINK_ADMIN	サーバに登録されたリンク情報を改竄
291	LINK	ADMIN	T.ERACE	T.ERACE_LINK_ADMIN	サーバに登録されたリンク情報を消去

項番	資産	主体	汎用脅威	脅威名	脅威内容
292	LINK	ADMIN	T.IMPERSON	T.IMPERSON_LINK_ADMIN	アクセス権が有るため脅威外
293	LINK	ADMIN	T.STEAL	T.STEAL_LINK_ADMIN	機密性不要のため脅威外
294	LINK	ADMIN	T.DISCLOSE	T.DISCLOSE_LINK_ADMIN	機密性不要のため脅威外
295	LINK	OPE	T.FORGERY	T.FORGERY_LINK_OPE	偽造したリンク情報をサーバに登録
296	LINK	OPE	T.MODIFY	T.MODIFY_LINK_OPE	サーバに登録されたリンク情報を改竄
297	LINK	OPE	T.ERACE	T.ERACE_LINK_OPE	サーバに登録されたリンク情報を消去
298	LINK	OPE	T.IMPERSON	T.IMPERSON_LINK_OPE	アクセス権が有るため脅威外
299	LINK	OPE	T.STEAL	T.STEAL_LINK_OPE	機密性不要のため脅威外
300	LINK	OPE	T.DISCLOSE	T.DISCLOSE_LINK_OPE	機密性不要のため脅威外
301	LINK	AUDIT	T.FORGERY	T.FORGERY_LINK_AUDIT	偽造したリンク情報をサーバに登録
302	LINK	AUDIT	T.MODIFY	T.MODIFY_LINK_AUDIT	サーバに登録されたリンク情報を改竄
303	LINK	AUDIT	T.ERACE	T.ERACE_LINK_AUDIT	サーバに登録されたリンク情報を消去
304	LINK	AUDIT	T.IMPERSON	T.IMPERSON_LINK_AUDIT	アクセス権所有者への成り済まし
305	LINK	AUDIT	T.STEAL	T.STEAL_LINK_AUDIT	機密性不要のため脅威外
306	LINK	AUDIT	T.DISCLOSE	T.DISCLOSE_LINK_AUDIT	機密性不要のため脅威外
307	CONFIG	ADMIN	T.FORGERY	T.FORGERY_CONFIG_ADMIN	偽造した設定情報をサーバに登録
308	CONFIG	ADMIN	T.MODIFY	T.MODIFY_CONFIG_ADMIN	サーバ内の設定情報を改竄
309	CONFIG	ADMIN	T.ERACE	T.ERACE_CONFIG_ADMIN	サーバ内の設定情報を消去
310	CONFIG	ADMIN	T.IMPERSON	T.IMPERSON_CONFIG_ADMIN	アクセス権が有るため脅威外
311	CONFIG	ADMIN	T.STEAL	T.STEAL_CONFIG_ADMIN	サーバ内の設定情報を不正に取得
312	CONFIG	ADMIN	T.DISCLOSE	T.DISCLOSE_CONFIG_ADMIN	サーバ内の設定情報を不正に漏洩
313	CONFIG	OPE	T.FORGERY	T.FORGERY_CONFIG_OPE	偽造した設定情報をサーバに登録
314	CONFIG	OPE	T.MODIFY	T.MODIFY_CONFIG_OPE	サーバ内の設定情報を改竄
315	CONFIG	OPE	T.ERACE	T.ERACE_CONFIG_OPE	サーバ内の設定情報を消去
316	CONFIG	OPE	T.IMPERSON	T.IMPERSON_CONFIG_OPE	アクセス権所有者への成り済まし
317	CONFIG	OPE	T.STEAL	T.STEAL_CONFIG_OPE	サーバ内の設定情報を不正に取得
318	CONFIG	OPE	T.DISCLOSE	T.DISCLOSE_CONFIG_OPE	サーバ内の設定情報を不正に漏洩
319	CONFIG	AUDIT	T.FORGERY	T.FORGERY_CONFIG_AUDIT	偽造した設定情報をサーバに登録
320	CONFIG	AUDIT	T.MODIFY	T.MODIFY_CONFIG_AUDIT	サーバ内の設定情報を改竄
321	CONFIG	AUDIT	T.ERACE	T.ERACE_CONFIG_AUDIT	サーバ内の設定情報を消去
322	CONFIG	AUDIT	T.IMPERSON	T.IMPERSON_CONFIG_AUDIT	アクセス権所有者への成り済まし
323	CONFIG	AUDIT	T.STEAL	T.STEAL_CONFIG_AUDIT	サーバ内の設定情報を不正に取得
324	CONFIG	AUDIT	T.DISCLOSE	T.DISCLOSE_CONFIG_AUDIT	サーバ内の設定情報を不正に漏洩
325	DB-ID-PW	ADMIN	T.FORGERY	T.FORGERY_DB-ID-PW_ADMIN	偽造したID/PWをサーバに登録
326	DB-ID-PW	ADMIN	T.MODIFY	T.MODIFY_DB-ID-PW_ADMIN	サーバに登録されたID/PWを改竄
327	DB-ID-PW	ADMIN	T.ERACE	T.ERACE_DB-ID-PW_ADMIN	サーバに登録されたID/PWを消去
328	DB-ID-PW	ADMIN	T.IMPERSON	T.IMPERSON_DB-ID-PW_ADMIN	アクセス権が有るため脅威外
329	DB-ID-PW	ADMIN	T.STEAL	T.STEAL_DB-ID-PW_ADMIN	サーバに登録されたID/PWを不正に取得
330	DB-ID-PW	ADMIN	T.DISCLOSE	T.DISCLOSE_DB-ID-PW_ADMIN	サーバに登録されたID/PWを不正に漏洩
331	DB-ID-PW	OPE	T.FORGERY	T.FORGERY_DB-ID-PW_OPE	偽造したID/PWをサーバに登録
332	DB-ID-PW	OPE	T.MODIFY	T.MODIFY_DB-ID-PW_OPE	サーバに登録されたID/PWを改竄
333	DB-ID-PW	OPE	T.ERACE	T.ERACE_DB-ID-PW_OPE	サーバに登録されたID/PWを消去
334	DB-ID-PW	OPE	T.IMPERSON	T.IMPERSON_DB-ID-PW_OPE	アクセス権所有者への成り済まし
335	DB-ID-PW	OPE	T.STEAL	T.STEAL_DB-ID-PW_OPE	サーバに登録されたID/PWを不正に取得
336	DB-ID-PW	OPE	T.DISCLOSE	T.DISCLOSE_DB-ID-PW_OPE	サーバに登録されたID/PWを不正に漏洩
337	DB-ID-PW	AUDIT	T.FORGERY	T.FORGERY_DB-ID-PW_AUDIT	偽造したID/PWをサーバに登録
338	DB-ID-PW	AUDIT	T.MODIFY	T.MODIFY_DB-ID-PW_AUDIT	サーバに登録されたID/PWを改竄
339	DB-ID-PW	AUDIT	T.ERACE	T.ERACE_DB-ID-PW_AUDIT	サーバに登録されたID/PWを消去
340	DB-ID-PW	AUDIT	T.IMPERSON	T.IMPERSON_DB-ID-PW_AUDIT	アクセス権所有者への成り済まし
341	DB-ID-PW	AUDIT	T.STEAL	T.STEAL_DB-ID-PW_AUDIT	サーバに登録されたID/PWを不正に取得
342	DB-ID-PW	AUDIT	T.DISCLOSE	T.DISCLOSE_DB-ID-PW_AUDIT	サーバに登録されたID/PWを不正に漏洩
343	LINK-PROV	ADMIN	T.FORGERY	T.FORGERY_LINK-PROV_ADMIN	リンク情報の代表値を偽造
344	LINK-PROV	ADMIN	T.MODIFY	T.MODIFY_LINK-PROV_ADMIN	明証化されたリンク情報の代表値を改竄
345	LINK-PROV	ADMIN	T.ERACE	T.ERACE_LINK-PROV_ADMIN	明証化されたリンク情報の代表値を消去
346	LINK-PROV	ADMIN	T.IMPERSON	T.IMPERSON_LINK-PROV_ADMIN	明証化主体やアクセス権所有者への成り済まし
347	LINK-PROV	ADMIN	T.STEAL	T.STEAL_LINK-PROV_ADMIN	機密性不要のため脅威外
348	LINK-PROV	ADMIN	T.DISCLOSE	T.DISCLOSE_LINK-PROV_ADMIN	機密性不要のため脅威外
349	LINK-PROV	OPE	T.FORGERY	T.FORGERY_LINK-PROV_OPE	リンク情報の代表値を偽造
350	LINK-PROV	OPE	T.MODIFY	T.MODIFY_LINK-PROV_OPE	明証化されたリンク情報の代表値を改竄
351	LINK-PROV	OPE	T.ERACE	T.ERACE_LINK-PROV_OPE	明証化されたリンク情報の代表値を消去
352	LINK-PROV	OPE	T.IMPERSON	T.IMPERSON_LINK-PROV_OPE	明証化主体やアクセス権所有者への成り済まし

項番	資産	主体	汎用脅威	脅威名	脅威内容
353	LINK-PROV	OPE	T.STEAL	T.STEAL_LINK-PROV_OPE	機密性不要のため脅威外
354	LINK-PROV	OPE	T.DISCLOSE	T.DISCLOSE_LINK-PROV_OPE	機密性不要のため脅威外
355	LINK-PROV	AUDIT	T.FORGERY	T.FORGERY_LINK-PROV_AUDIT	リンク情報の代表値を偽造
356	LINK-PROV	AUDIT	T.MODIFY	T.MODIFY_LINK-PROV_AUDIT	明証化されたリンク情報の代表値を改竄
357	LINK-PROV	AUDIT	T.ERACE	T.ERACE_LINK-PROV_AUDIT	明証化されたリンク情報の代表値を消去
358	LINK-PROV	AUDIT	T.IMPERSON	T.IMPERSON_LINK-PROV_AUDIT	明証化主体やアクセス権所有者への成り済まし
359	LINK-PROV	AUDIT	T.STEAL	T.STEAL_LINK-PROV_AUDIT	機密性不要のため脅威外
360	LINK-PROV	AUDIT	T.DISCLOSE	T.DISCLOSE_LINK-PROV_AUDIT	機密性不要のため脅威外
361	EVENT	ADMIN	T.FORGERY	T.FORGERY_EVENT_ADMIN	偽造した動作記録をサーバに登録
362	EVENT	ADMIN	T.MODIFY	T.MODIFY_EVENT_ADMIN	サーバ内の動作記録を改竄
363	EVENT	ADMIN	T.ERACE	T.ERACE_EVENT_ADMIN	サーバ内の動作記録を消去
364	EVENT	ADMIN	T.IMPERSON	T.IMPERSON_EVENT_ADMIN	アクセス権が有るため脅威外
365	EVENT	ADMIN	T.STEAL	T.STEAL_EVENT_ADMIN	サーバ内の動作記録を不正に取得
366	EVENT	ADMIN	T.DISCLOSE	T.DISCLOSE_EVENT_ADMIN	サーバ内の動作記録を不正に漏洩
367	EVENT	OPE	T.FORGERY	T.FORGERY_EVENT_OPE	偽造した動作記録をサーバに登録
368	EVENT	OPE	T.MODIFY	T.MODIFY_EVENT_OPE	サーバ内の動作記録を改竄
369	EVENT	OPE	T.ERACE	T.ERACE_EVENT_OPE	サーバ内の動作記録を消去
370	EVENT	OPE	T.IMPERSON	T.IMPERSON_EVENT_OPE	アクセス権が有るため脅威外
371	EVENT	OPE	T.STEAL	T.STEAL_EVENT_OPE	サーバ内の動作記録を不正に取得
372	EVENT	OPE	T.DISCLOSE	T.DISCLOSE_EVENT_OPE	サーバ内の動作記録を不正に漏洩
373	EVENT	AUDIT	T.FORGERY	T.FORGERY_EVENT_AUDIT	偽造した動作記録をサーバに登録
374	EVENT	AUDIT	T.MODIFY	T.MODIFY_EVENT_AUDIT	サーバ内の動作記録を改竄
375	EVENT	AUDIT	T.ERACE	T.ERACE_EVENT_AUDIT	サーバ内の動作記録を消去
376	EVENT	AUDIT	T.IMPERSON	T.IMPERSON_EVENT_AUDIT	アクセス権所有者への成り済まし
377	EVENT	AUDIT	T.STEAL	T.STEAL_EVENT_AUDIT	サーバ内の動作記録を不正に取得
378	EVENT	AUDIT	T.DISCLOSE	T.DISCLOSE_EVENT_AUDIT	サーバ内の動作記録を不正に漏洩
379	CLOCK	ADMIN	T.FORGERY	T.FORGERY_CLOCK_ADMIN	偽造したシステムクロックの登録
380	CLOCK	ADMIN	T.MODIFY	T.MODIFY_CLOCK_ADMIN	システムクロックの改竄
381	CLOCK	ADMIN	T.ERACE	T.ERACE_CLOCK_ADMIN	システムクロックの消去
382	CLOCK	ADMIN	T.IMPERSON	T.IMPERSON_CLOCK_ADMIN	アクセス権が有るため脅威外
383	CLOCK	ADMIN	T.STEAL	T.STEAL_CLOCK_ADMIN	機密性不要のため脅威外
384	CLOCK	ADMIN	T.DISCLOSE	T.DISCLOSE_CLOCK_ADMIN	機密性不要のため脅威外
385	CLOCK	OPE	T.FORGERY	T.FORGERY_CLOCK_OPE	偽造したシステムクロックの登録
386	CLOCK	OPE	T.MODIFY	T.MODIFY_CLOCK_OPE	システムクロックの改竄
387	CLOCK	OPE	T.ERACE	T.ERACE_CLOCK_OPE	システムクロックの消去
388	CLOCK	OPE	T.IMPERSON	T.IMPERSON_CLOCK_OPE	アクセス権所有者への成り済まし
389	CLOCK	OPE	T.STEAL	T.STEAL_CLOCK_OPE	機密性不要のため脅威外
390	CLOCK	OPE	T.DISCLOSE	T.DISCLOSE_CLOCK_OPE	機密性不要のため脅威外
391	CLOCK	AUDIT	T.FORGERY	T.FORGERY_CLOCK_AUDIT	偽造したシステムクロックの登録
392	CLOCK	AUDIT	T.MODIFY	T.MODIFY_CLOCK_AUDIT	システムクロックの改竄
393	CLOCK	AUDIT	T.ERACE	T.ERACE_CLOCK_AUDIT	システムクロックの消去
394	CLOCK	AUDIT	T.IMPERSON	T.IMPERSON_CLOCK_AUDIT	アクセス権所有者への成り済まし
395	CLOCK	AUDIT	T.STEAL	T.STEAL_CLOCK_AUDIT	機密性不要のため脅威外
396	CLOCK	AUDIT	T.DISCLOSE	T.DISCLOSE_CLOCK_AUDIT	機密性不要のため脅威外
397	MOD-CRE-TS	ADMIN	T.FORGERY	T.FORGERY_MOD-CRE-TS_ADMIN	偽造したTS生成モジュールへの差替え
398	MOD-CRE-TS	ADMIN	T.MODIFY	T.MODIFY_MOD-CRE-TS_ADMIN	TS生成モジュールを改竄
399	MOD-CRE-TS	ADMIN	T.ERACE	T.ERACE_MOD-CRE-TS_ADMIN	TS生成モジュールを消去
400	MOD-CRE-TS	ADMIN	T.IMPERSON	T.IMPERSON_MOD-CRE-TS_ADMIN	アクセス権が有るため脅威外
401	MOD-CRE-TS	ADMIN	T.STEAL	T.STEAL_MOD-CRE-TS_ADMIN	TS生成モジュールを不正に取得
402	MOD-CRE-TS	ADMIN	T.DISCLOSE	T.DISCLOSE_MOD-CRE-TS_ADMIN	TS生成モジュールを不正に漏洩
403	MOD-CRE-TS	OPE	T.FORGERY	T.FORGERY_MOD-CRE-TS_OPE	偽造したTS生成モジュールへの差替え
404	MOD-CRE-TS	OPE	T.MODIFY	T.MODIFY_MOD-CRE-TS_OPE	TS生成モジュールを改竄
405	MOD-CRE-TS	OPE	T.ERACE	T.ERACE_MOD-CRE-TS_OPE	TS生成モジュールを消去
406	MOD-CRE-TS	OPE	T.IMPERSON	T.IMPERSON_MOD-CRE-TS_OPE	アクセス権所有者への成り済まし
407	MOD-CRE-TS	OPE	T.STEAL	T.STEAL_MOD-CRE-TS_OPE	TS生成モジュールを不正に取得
408	MOD-CRE-TS	OPE	T.DISCLOSE	T.DISCLOSE_MOD-CRE-TS_OPE	TS生成モジュールを不正に漏洩
409	MOD-CRE-TS	AUDIT	T.FORGERY	T.FORGERY_MOD-CRE-TS_AUDIT	偽造したTS生成モジュールへの差替え
410	MOD-CRE-TS	AUDIT	T.MODIFY	T.MODIFY_MOD-CRE-TS_AUDIT	TS生成モジュールを改竄
411	MOD-CRE-TS	AUDIT	T.ERACE	T.ERACE_MOD-CRE-TS_AUDIT	TS生成モジュールを消去
412	MOD-CRE-TS	AUDIT	T.IMPERSON	T.IMPERSON_MOD-CRE-TS_AUDIT	アクセス権所有者への成り済まし
413	MOD-CRE-TS	AUDIT	T.STEAL	T.STEAL_MOD-CRE-TS_AUDIT	TS生成モジュールを不正に取得

項番	資産	主体	汎用脅威	脅威名	脅威内容
414	MOD-CRE-TS	AUDIT	T.DISCLOSE	T.DISCLOSE_MOD-CRE-TS_AUDIT	TS生成モジュールを不正に漏洩
415	MOD-STORE	ADMIN	T.FORGERY	T.FORGERY_MOD-STORE_ADMIN	偽造した保管モジュールへの差替え
416	MOD-STORE	ADMIN	T.MODIFY	T.MODIFY_MOD-STORE_ADMIN	保管モジュールを改竄
417	MOD-STORE	ADMIN	T.ERACE	T.ERACE_MOD-STORE_ADMIN	保管モジュールを消去
418	MOD-STORE	ADMIN	T.IMPERSON	T.IMPERSON_MOD-STORE_ADMIN	アクセス権が有るため脅威外
419	MOD-STORE	ADMIN	T.STEAL	T.STEAL_MOD-STORE_ADMIN	保管モジュールを不正に取得
420	MOD-STORE	ADMIN	T.DISCLOSE	T.DISCLOSE_MOD-STORE_ADMIN	保管モジュールを不正に漏洩
421	MOD-STORE	OPE	T.FORGERY	T.FORGERY_MOD-STORE_OPE	偽造した保管モジュールへの差替え
422	MOD-STORE	OPE	T.MODIFY	T.MODIFY_MOD-STORE_OPE	保管モジュールを改竄
423	MOD-STORE	OPE	T.ERACE	T.ERACE_MOD-STORE_OPE	保管モジュールを消去
424	MOD-STORE	OPE	T.IMPERSON	T.IMPERSON_MOD-STORE_OPE	アクセス権所有者への成り済まし
425	MOD-STORE	OPE	T.STEAL	T.STEAL_MOD-STORE_OPE	保管モジュールを不正に取得
426	MOD-STORE	OPE	T.DISCLOSE	T.DISCLOSE_MOD-STORE_OPE	保管モジュールを不正に漏洩
427	MOD-STORE	AUDIT	T.FORGERY	T.FORGERY_MOD-STORE_AUDIT	偽造した保管モジュールへの差替え
428	MOD-STORE	AUDIT	T.MODIFY	T.MODIFY_MOD-STORE_AUDIT	保管モジュールを改竄
429	MOD-STORE	AUDIT	T.ERACE	T.ERACE_MOD-STORE_AUDIT	保管モジュールを消去
430	MOD-STORE	AUDIT	T.IMPERSON	T.IMPERSON_MOD-STORE_AUDIT	アクセス権所有者への成り済まし
431	MOD-STORE	AUDIT	T.STEAL	T.STEAL_MOD-STORE_AUDIT	保管モジュールを不正に取得
432	MOD-STORE	AUDIT	T.DISCLOSE	T.DISCLOSE_MOD-STORE_AUDIT	保管モジュールを不正に漏洩
433	MOD-COM-TS	ADMIN	T.FORGERY	T.FORGERY_MOD-COM-TS_ADMIN	偽造したTS照合モジュールへの差替え
434	MOD-COM-TS	ADMIN	T.MODIFY	T.MODIFY_MOD-COM-TS_ADMIN	TS照合モジュールを改竄
435	MOD-COM-TS	ADMIN	T.ERACE	T.ERACE_MOD-COM-TS_ADMIN	TS照合モジュールを消去
436	MOD-COM-TS	ADMIN	T.IMPERSON	T.IMPERSON_MOD-COM-TS_ADMIN	アクセス権が有るため脅威外
437	MOD-COM-TS	ADMIN	T.STEAL	T.STEAL_MOD-COM-TS_ADMIN	TS照合モジュールを不正に取得
438	MOD-COM-TS	ADMIN	T.DISCLOSE	T.DISCLOSE_MOD-COM-TS_ADMIN	TS照合モジュールを不正に漏洩
439	MOD-COM-TS	OPE	T.FORGERY	T.FORGERY_MOD-COM-TS_OPE	偽造したTS照合モジュールへの差替え
440	MOD-COM-TS	OPE	T.MODIFY	T.MODIFY_MOD-COM-TS_OPE	TS照合モジュールを改竄
441	MOD-COM-TS	OPE	T.ERACE	T.ERACE_MOD-COM-TS_OPE	TS照合モジュールを消去
442	MOD-COM-TS	OPE	T.IMPERSON	T.IMPERSON_MOD-COM-TS_OPE	アクセス権所有者への成り済まし
443	MOD-COM-TS	OPE	T.STEAL	T.STEAL_MOD-COM-TS_OPE	TS照合モジュールを不正に取得
444	MOD-COM-TS	OPE	T.DISCLOSE	T.DISCLOSE_MOD-COM-TS_OPE	TS照合モジュールを不正に漏洩
445	MOD-COM-TS	AUDIT	T.FORGERY	T.FORGERY_MOD-COM-TS_AUDIT	偽造したTS照合モジュールへの差替え
446	MOD-COM-TS	AUDIT	T.MODIFY	T.MODIFY_MOD-COM-TS_AUDIT	TS照合モジュールを改竄
447	MOD-COM-TS	AUDIT	T.ERACE	T.ERACE_MOD-COM-TS_AUDIT	TS照合モジュールを消去
448	MOD-COM-TS	AUDIT	T.IMPERSON	T.IMPERSON_MOD-COM-TS_AUDIT	アクセス権所有者への成り済まし
449	MOD-COM-TS	AUDIT	T.STEAL	T.STEAL_MOD-COM-TS_AUDIT	TS照合モジュールを不正に取得
450	MOD-COM-TS	AUDIT	T.DISCLOSE	T.DISCLOSE_MOD-COM-TS_AUDIT	TS照合モジュールを不正に漏洩
451	MOD-TIME	ADMIN	T.FORGERY	T.FORGERY_MOD-TIME_ADMIN	偽造した時刻受信モジュールへの差替え
452	MOD-TIME	ADMIN	T.MODIFY	T.MODIFY_MOD-TIME_ADMIN	時刻受信モジュールを改竄
453	MOD-TIME	ADMIN	T.ERACE	T.ERACE_MOD-TIME_ADMIN	時刻受信モジュールを消去
454	MOD-TIME	ADMIN	T.IMPERSON	T.IMPERSON_MOD-TIME_ADMIN	アクセス権が有るため脅威外
455	MOD-TIME	ADMIN	T.STEAL	T.STEAL_MOD-TIME_ADMIN	時刻受信モジュールを不正に取得
456	MOD-TIME	ADMIN	T.DISCLOSE	T.DISCLOSE_MOD-TIME_ADMIN	時刻受信モジュールを不正に漏洩
457	MOD-TIME	OPE	T.FORGERY	T.FORGERY_MOD-TIME_OPE	偽造した時刻受信モジュールへの差替え
458	MOD-TIME	OPE	T.MODIFY	T.MODIFY_MOD-TIME_OPE	時刻受信モジュールを改竄
459	MOD-TIME	OPE	T.ERACE	T.ERACE_MOD-TIME_OPE	時刻受信モジュールを消去
460	MOD-TIME	OPE	T.IMPERSON	T.IMPERSON_MOD-TIME_OPE	アクセス権所有者への成り済まし
461	MOD-TIME	OPE	T.STEAL	T.STEAL_MOD-TIME_OPE	時刻受信モジュールを不正に取得
462	MOD-TIME	OPE	T.DISCLOSE	T.DISCLOSE_MOD-TIME_OPE	時刻受信モジュールを不正に漏洩
463	MOD-TIME	AUDIT	T.FORGERY	T.FORGERY_MOD-TIME_AUDIT	偽造した時刻受信モジュールへの差替え
464	MOD-TIME	AUDIT	T.MODIFY	T.MODIFY_MOD-TIME_AUDIT	時刻受信モジュールを改竄
465	MOD-TIME	AUDIT	T.ERACE	T.ERACE_MOD-TIME_AUDIT	時刻受信モジュールを消去
466	MOD-TIME	AUDIT	T.IMPERSON	T.IMPERSON_MOD-TIME_AUDIT	アクセス権所有者への成り済まし
467	MOD-TIME	AUDIT	T.STEAL	T.STEAL_MOD-TIME_AUDIT	時刻受信モジュールを不正に取得
468	MOD-TIME	AUDIT	T.DISCLOSE	T.DISCLOSE_MOD-TIME_AUDIT	時刻受信モジュールを不正に漏洩

2-3 組織のセキュリティポリシー

内部不正を考慮したセキュリティ環境の組織のセキュリティポリシーについては、「表 7 TOE に係るセキュリティ環境の組織のセキュリティポリシー一覧」及び「表 11　TOE に係るセキュリティ環境の組織のセキュリティポリシーの実現方法例一覧」と特に差異はないものと想定する。

3. 脅威に関する対策

内部不正を考慮した脅威のセキュリティ目標に含まれる対策名と実装システムに対する評価一覧について、「表 8　脅威のセキュリティ目標に含まれる対策名と実装システムに対する評価一覧」に対して追加される対策名一覧を、以下の表 17に示す。

表 17　内部不正を考慮した場合の対策名と実装システムに対する評価の追加一覧

項番	種別	対策名	説明	統合化システムにおける実現
1	防止	M.CONT	他の業務と独立した組織による作業承認手順・権限分離等の人的統制が確保された運用体制	作業承認手順の明確化及び権限分離の徹底等により、実現可能。
2	防止	M.EDU	時刻認証業務及びセキュリティに関する専門的知識を有する者、または専門的知識を習得するための教育研修を受講した者の任命	内部関係者に対する必要知識の確認、または教育の徹底により、実現可能。
3	防止	M.PENA	不正を行った内部関係者に対する罰則規定	罰則規定の制定により、実現可能。
4	検出	M.AUDIT	内部関係者と独立した監査者による定期的な業務監査	外部の監査者への定期的な業務監査の委託により、実現可能。
5	検出	M.MOD_CHECK	TOEで動作するソフトウェアの仕様、機能及び動作等の第三者機関によるチェック	ソフトウェアチェックの外部機関への委託等により、実現可能。

内部不正を考慮した場合に追加される脅威のセキュリティ目標・対策一覧を、以下の表 18に示す。なお、表中網掛けの項目は、実質的なリスクを伴わない脅威を示す。

表 18　内部不正を考慮した場合に追加される脅威のセキュリティ目標・対策一覧

項番	脅威名	リスク有無	目標種別	セキュリティ目標
1	T.FORGERY_USER-ID-PW_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_ERACE
2	T.MODIFY_USER-ID-PW_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_CHANGE
3	T.ERACE_USER-ID-PW_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_REGI
4	T.IMPERSON_USER-ID-PW_ADMIN	無	防止	－
			検出	－
			回復	－
5	T.STEAL_USER-ID-PW_ADMIN	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE
6	T.DISCLOSE_USER-ID-PW_ADMIN	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE
7	T.FORGERY_USER-ID-PW_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_ERACE
8	T.MODIFY_USER-ID-PW_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_CHANGE
9	T.ERACE_USER-ID-PW_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_REGI
10	T.IMPERSON_USER-ID-PW_OPE	無	防止	－
			検出	－
			回復	－
11	T.STEAL_USER-ID-PW_OPE	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE
12	T.DISCLOSE_USER-ID-PW_OPE	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE
13	T.FORGERY_USER-ID-PW_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_ERACE
14	T.MODIFY_USER-ID-PW_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_CHANGE
15	T.ERACE_USER-ID-PW_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_REGI
16	T.IMPERSON_USER-ID-PW_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.AC_REST
17	T.STEAL_USER-ID-PW_AUDIT	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE
18	T.DISCLOSE_USER-ID-PW_AUDIT	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE

項番	脅威名	リスク有無	目標種別	セキュリティ目標
19	T.FORGERY_TST_ADMIN	有	防止	M.TST_VAL_PUB；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.LINK_AUDIT；M.AUDIT
			回復	M.ILL_TST_NOT
20	T.MODIFY_TST_ADMIN	有	防止	M.TST_VAL_PUB；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.LINK_AUDIT；M.AUDIT
			回復	M.ILL_TST_NOT
21	T.ERACE_TST_ADMIN	有	防止	M.KEEP_TST_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_CONT；M.AUDIT
			回復	－
22	T.IMPERSON_TST_ADMIN	有	防止	M.SSL_AUTH；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.SSL_AUTH_PUB；M.AUDIT
			回復	M.ATTACK_NOT；M.ATTACK_REM
23	T.STEAL_TST_ADMIN	無	防止	－
			検出	－
			回復	－
24	T.DISCLOSE_TST_ADMIN	無	防止	－
			検出	－
			回復	－
25	T.FORGERY_TST_OPE	有	防止	M.TST_VAL_PUB；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.LINK_AUDIT；M.AUDIT
			回復	M.ILL_TST_NOT
26	T.MODIFY_TST_OPE	有	防止	M.TST_VAL_PUB；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.LINK_AUDIT；M.AUDIT
			回復	M.ILL_TST_NOT
27	T.ERACE_TST_OPE	有	防止	M.KEEP_TST_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_CONT；M.AUDIT
			回復	－
28	T.IMPERSON_TST_OPE	有	防止	M.SSL_AUTH；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.SSL_AUTH_PUB；M.AUDIT
			回復	M.ATTACK_NOT；M.ATTACK_REM
29	T.STEAL_TST_OPE	無	防止	－
			検出	－
			回復	－
30	T.DISCLOSE_TST_OPE	無	防止	－
			検出	－
			回復	－
31	T.FORGERY_TST_AUDIT	有	防止	M.TST_VAL_PUB；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.LINK_AUDIT；M.AUDIT
			回復	M.ILL_TST_NOT
32	T.MODIFY_TST_AUDIT	有	防止	M.TST_VAL_PUB；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.LINK_AUDIT；M.AUDIT
			回復	M.ILL_TST_NOT
33	T.ERACE_TST_AUDIT	有	防止	M.KEEP_TST_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_CONT；M.AUDIT
			回復	－
34	T.IMPERSON_TST_AUDIT	有	防止	M.SSL_AUTH；M.EDU；M.CONT；M.PENA
			検出	M.TSA_VERI；M.SSL_AUTH_PUB；M.AUDIT
			回復	M.ATTACK_NOT；M.ATTACK_REM
35	T.STEAL_TST_AUDIT	無	防止	－
			検出	－
			回復	－
36	T.DISCLOSE_TST_AUDIT	無	防止	－
			検出	－
			回復	－
37	T.FORGERY_TAC_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN；M.EDU；M.CONT；M.PENA
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST；M.TA_REISSUE
38	T.MODIFY_TAC_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.TA_SIGN；M.EDU；M.CONT；M.PENA
			検出	M.TA_SIGN_VERI；M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST；M.TA_REISSUE

項番	脅威名	リスク有無	目標種別	セキュリティ目標
39	T.ERACE_TAC_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
40	T.IMPERSON_TAC_ADMIN	有	防止	M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
41	T.STEAL_TAC_ADMIN	無	防止	－
			検出	－
			回復	－
42	T.DISCLOSE_TAC_ADMIN	無	防止	－
			検出	－
			回復	－
43	T.FORGERY_TAC_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
44	T.MODIFY_TAC_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
45	T.ERACE_TAC_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
46	T.IMPERSON_TAC_OPE	有	防止	M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
47	T.STEAL_TAC_OPE	無	防止	－
			検出	－
			回復	－
48	T.DISCLOSE_TAC_OPE	無	防止	－
			検出	－
			回復	－
49	T.FORGERY_TAC_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
50	T.MODIFY_TAC_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
51	T.ERACE_TAC_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
52	T.IMPERSON_TAC_AUDIT	有	防止	M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
53	T.STEAL_TAC_AUDIT	無	防止	－
			検出	－
			回復	－
54	T.DISCLOSE_TAC_AUDIT	無	防止	－
			検出	－
			回復	－
55	T.FORGERY_TAC-LOG_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
56	T.MODIFY_TAC-LOG_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
57	T.ERACE_TAC-LOG_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
58	T.IMPERSON_TAC-LOG_ADMIN	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
59	T.STEAL_TAC-LOG_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
60	T.DISCLOSE_TAC-LOG_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
61	T.FORGERY_TAC-LOG_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
62	T.MODIFY_TAC-LOG_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
63	T.ERACE_TAC-LOG_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
64	T.IMPERSON_TAC-LOG_OPE	無	防止	－
			検出	－
			回復	－
65	T.STEAL_TAC-LOG_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
66	T.DISCLOSE_TAC-LOG_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
67	T.FORGERY_TAC-LOG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
68	T.MODIFY_TAC-LOG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
69	T.ERACE_TAC-LOG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
70	T.IMPERSON_TAC-LOG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
71	T.STEAL_TAC-LOG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
72	T.DISCLOSE_TAC-LOG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
73	T.FORGERY_TAR_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
74	T.MODIFY_TAR_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
75	T.ERACE_TAR_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
76	T.IMPERSON_TAR_ADMIN	有	防止	M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
77	T.STEAL_TAR_ADMIN	無	防止	－
			検出	－
			回復	－
78	T.DISCLOSE_TAR_ADMIN	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
79	T.FORGERY_TAR_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
80	T.MODIFY_TAR_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
81	T.ERACE_TAR_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
82	T.IMPERSON_TAR_OPE	有	防止	M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
83	T.STEAL_TAR_OPE	無	防止	－
			検出	－
			回復	－
84	T.DISCLOSE_TAR_OPE	無	防止	－
			検出	－
			回復	－
85	T.FORGERY_TAR_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
86	T.MODIFY_TAR_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
87	T.ERACE_TAR_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.USER_CONT;M.AUDIT
			回復	M.DATA_REST;M.TA_REISSUE
88	T.IMPERSON_TAR_AUDIT	有	防止	M.TA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.TA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
89	T.STEAL_TAR_AUDIT	無	防止	－
			検出	－
			回復	－
90	T.DISCLOSE_TAR_AUDIT	無	防止	－
			検出	－
			回復	－
91	T.FORGERY_KEYST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
92	T.MODIFY_KEYST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
93	T.ERACE_KEYST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
94	T.IMPERSON_KEYST_ADMIN	無	防止	－
			検出	－
			回復	－
95	T.STEAL_KEYST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
96	T.DISCLOSE_KEYST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
97	T.FORGERY_KEYST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
98	T.MODIFY_KEYST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標
99	T.ERACE_KEYST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
100	T.IMPERSON_KEYST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
101	T.STEAL_KEYST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
102	T.DISCLOSE_KEYST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
103	T.FORGERY_KEYST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
104	T.MODIFY_KEYST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
105	T.ERACE_KEYST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG;M.DATA_REST
106	T.IMPERSON_KEYST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_FAIL_AUTH;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
107	T.STEAL_KEYST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
108	T.DISCLOSE_KEYST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CERT_REVOKE;M.KEY_CERT_REG
109	T.FORGERY_KEYST-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
110	T.MODIFY_KEYST-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
111	T.ERACE_KEYST-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
112	T.IMPERSON_KEYST-PW_ADMIN	無	防止	－
			検出	－
			回復	－
113	T.STEAL_KEYST-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
114	T.DISCLOSE_KEYST-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
115	T.FORGERY_KEYST-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
116	T.MODIFY_KEYST-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
117	T.ERACE_KEYST-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
118	T.IMPERSON_KEYST-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標
119	T.STEAL_KEYST-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
120	T.DISCLOSE_KEYST-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
121	T.FORGERY_KEYST-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
122	T.MODIFY_KEYST-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
123	T.ERACE_KEYST-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
124	T.IMPERSON_KEYST-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
125	T.STEAL_KEYST-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
126	T.DISCLOSE_KEYST-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
127	T.FORGERY_CERT_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
128	T.MODIFY_CERT_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
129	T.ERACE_CERT_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
130	T.IMPERSON_CERT_ADMIN	有	防止	M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
131	T.STEAL_CERT_ADMIN	無	防止	－
			検出	－
			回復	－
132	T.DISCLOSE_CERT_ADMIN	無	防止	－
			検出	－
			回復	－
133	T.FORGERY_CERT_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
134	T.MODIFY_CERT_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
135	T.ERACE_CERT_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
136	T.IMPERSON_CERT_OPE	有	防止	M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
137	T.STEAL_CERT_OPE	無	防止	－
			検出	－
			回復	－
138	T.DISCLOSE_CERT_OPE	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
139	T.FORGERY_CERT_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
140	T.MODIFY_CERT_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
141	T.ERACE_CERT_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.CERT_REISSUE;M.KEY_CERT_REG
142	T.IMPERSON_CERT_AUDIT	有	防止	M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
143	T.STEAL_CERT_AUDIT	無	防止	－
			検出	－
			回復	－
144	T.DISCLOSE_CERT_AUDIT	無	防止	－
			検出	－
			回復	－
145	T.FORGERY_CRL-ARL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
146	T.MODIFY_CRL-ARL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
147	T.ERACE_CRL-ARL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
148	T.IMPERSON_CRL-ARL_ADMIN	有	防止	M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
149	T.STEAL_CRL-ARL_ADMIN	無	防止	－
			検出	－
			回復	－
150	T.DISCLOSE_CRL-ARL_ADMIN	無	防止	－
			検出	－
			回復	－
151	T.FORGERY_CRL-ARL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
152	T.MODIFY_CRL-ARL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
153	T.ERACE_CRL-ARL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
154	T.IMPERSON_CRL-ARL_OPE	有	防止	M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
155	T.STEAL_CRL-ARL_OPE	無	防止	－
			検出	－
			回復	－
156	T.DISCLOSE_CRL-ARL_OPE	無	防止	－
			検出	－
			回復	－
157	T.FORGERY_CRL-ARL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
158	T.MODIFY_CRL-ARL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE

項番	脅威名	リスク有無	目標種別	セキュリティ目標
159	T.ERACE_CRL-ARL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.RL_REISSUE
160	T.IMPERSON_CRL-ARL_AUDIT	有	防止	M.CA_SIGN;M.EDU;M.CONT;M.PENA
			検出	M.CA_SIGN_VERI;M.AUDIT
			回復	M.ATTACK_NOT;M.ATTACK_REM
161	T.STEAL_CRL-ARL_AUDIT	無	防止	－
			検出	－
			回復	－
162	T.DISCLOSE_CRL-ARL_AUDIT	無	防止	－
			検出	－
			回復	－
163	T.FORGERY_PRI-KEY_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
164	T.MODIFY_PRI-KEY_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
165	T.ERACE_PRI-KEY_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_BEG_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
166	T.IMPERSON_PRI-KEY_ADMIN	無	防止	－
			検出	－
			回復	－
167	T.STEAL_PRI-KEY_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
168	T.DISCLOSE_PRI-KEY_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
169	T.FORGERY_PRI-KEY_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
170	T.MODIFY_PRI-KEY_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
171	T.ERACE_PRI-KEY_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_BEG_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
172	T.IMPERSON_PRI-KEY_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
173	T.STEAL_PRI-KEY_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
174	T.DISCLOSE_PRI-KEY_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
175	T.FORGERY_PRI-KEY_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
176	T.MODIFY_PRI-KEY_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_AUTH_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
177	T.ERACE_PRI-KEY_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.SSL_BEG_FAIL;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST;M.KEY_CERT_REG
178	T.IMPERSON_PRI-KEY_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標
179	T.STEAL_PRI-KEY_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
180	T.DISCLOSE_PRI-KEY_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.PW_LOCK;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
181	T.FORGERY_PRI-KEY-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
182	T.MODIFY_PRI-KEY-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
183	T.ERACE_PRI-KEY-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
184	T.IMPERSON_PRI-KEY-PW_ADMIN	無	防止	－
			検出	－
			回復	－
185	T.STEAL_PRI-KEY-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
186	T.DISCLOSE_PRI-KEY-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
187	T.FORGERY_PRI-KEY-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
188	T.MODIFY_PRI-KEY-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
189	T.ERACE_PRI-KEY-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
190	T.IMPERSON_PRI-KEY-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
191	T.STEAL_PRI-KEY-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
192	T.DISCLOSE_PRI-KEY-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
193	T.FORGERY_PRI-KEY-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
194	T.MODIFY_PRI-KEY-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_CHANGE;M.KEY_CERT_REG;M.DATA_REST
195	T.ERACE_PRI-KEY-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.PW_REGI;M.KEY_CERT_REG;M.DATA_REST
196	T.IMPERSON_PRI-KEY-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
197	T.STEAL_PRI-KEY-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG
198	T.DISCLOSE_PRI-KEY-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.KEY_CERT_REG

項番	脅威名	リスク有無	目標種別	セキュリティ目標
199	T.FORGERY_OPE-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_ERACE
200	T.MODIFY_OPE-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_CHANGE
201	T.ERACE_OPE-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_REGI
202	T.IMPERSON_OPE-ID-PW_ADMIN	無	防止	－
			検出	－
			回復	－
203	T.STEAL_OPE-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
204	T.DISCLOSE_OPE-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
205	T.FORGERY_OPE-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_ERACE
206	T.MODIFY_OPE-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_CHANGE
207	T.ERACE_OPE-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_REGI
208	T.IMPERSON_OPE-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
209	T.STEAL_OPE-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
210	T.DISCLOSE_OPE-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
211	T.FORGERY_OPE-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_ERACE
212	T.MODIFY_OPE-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_CHANGE
213	T.ERACE_OPE-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_REGI
214	T.IMPERSON_OPE-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
215	T.STEAL_OPE-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
216	T.DISCLOSE_OPE-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
217	T.FORGERY_DB-SERIAL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
218	T.MODIFY_DB-SERIAL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標
219	T.ERACE_DB-SERIAL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
220	T.IMPERSON_DB-SERIAL_ADMIN	無	防止	―
			検出	―
			回復	―
221	T.STEAL_DB-SERIAL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	―
222	T.DISCLOSE_DB-SERIAL_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	―
223	T.FORGERY_DB-SERIAL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
224	T.MODIFY_DB-SERIAL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
225	T.ERACE_DB-SERIAL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
226	T.IMPERSON_DB-SERIAL_OPE	無	防止	―
			検出	―
			回復	―
227	T.STEAL_DB-SERIAL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	―
228	T.DISCLOSE_DB-SERIAL_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	―
229	T.FORGERY_DB-SERIAL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
230	T.MODIFY_DB-SERIAL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
231	T.ERACE_DB-SERIAL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
232	T.IMPERSON_DB-SERIAL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
233	T.STEAL_DB-SERIAL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	―
234	T.DISCLOSE_DB-SERIAL_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	―
235	T.FORGERY_DB-USER-ID_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
236	T.MODIFY_DB-USER-ID_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
237	T.ERACE_DB-USER-ID_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
238	T.IMPERSON_DB-USER-ID_ADMIN	無	防止	―
			検出	―
			回復	―

項番	脅威名	リスク有無	目標種別	セキュリティ目標
239	T.STEAL_DB-USER-ID_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−
240	T.DISCLOSE_DB-USER-ID_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−
241	T.FORGERY_DB-USER-ID_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
242	T.MODIFY_DB-USER-ID_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
243	T.ERACE_DB-USER-ID_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
244	T.IMPERSON_DB-USER-ID_OPE	無	防止	−
			検出	−
			回復	−
245	T.STEAL_DB-USER-ID_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−
246	T.DISCLOSE_DB-USER-ID_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−
247	T.FORGERY_DB-USER-ID_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
248	T.MODIFY_DB-USER-ID_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
249	T.ERACE_DB-USER-ID_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
250	T.IMPERSON_DB-USER-ID_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
251	T.STEAL_DB-USER-ID_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−
252	T.DISCLOSE_DB-USER-ID_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−
253	T.FORGERY_DB-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
254	T.MODIFY_DB-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
255	T.ERACE_DB-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
256	T.IMPERSON_DB-TIME_ADMIN	無	防止	−
			検出	−
			回復	−
257	T.STEAL_DB-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−
258	T.DISCLOSE_DB-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	−

項番	脅威名	リスク有無	目標種別	セキュリティ目標
259	T.FORGERY_DB-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
260	T.MODIFY_DB-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
261	T.ERACE_DB-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
262	T.IMPERSON_DB-TIME_OPE	無	防止	－
			検出	－
			回復	－
263	T.STEAL_DB-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
264	T.DISCLOSE_DB-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
265	T.FORGERY_DB-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
266	T.MODIFY_DB-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
267	T.ERACE_DB-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
268	T.IMPERSON_DB-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
269	T.STEAL_DB-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
270	T.DISCLOSE_DB-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
271	T.FORGERY_DB-TST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
272	T.MODIFY_DB-TST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
273	T.ERACE_DB-TST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
274	T.IMPERSON_DB-TST_ADMIN	無	防止	－
			検出	－
			回復	－
275	T.STEAL_DB-TST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
276	T.DISCLOSE_DB-TST_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
277	T.FORGERY_DB-TST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
278	T.MODIFY_DB-TST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST

項番	脅威名	リスク有無	目標種別	セキュリティ目標
279	T.ERACE_DB-TST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
280	T.IMPERSON_DB-TST_OPE	無	防止	－
			検出	－
			回復	－
281	T.STEAL_DB-TST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
282	T.DISCLOSE_DB-TST_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
283	T.FORGERY_DB-TST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
284	T.MODIFY_DB-TST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_GEN;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
285	T.ERACE_DB-TST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.DATA_REST
286	T.IMPERSON_DB-TST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
287	T.STEAL_DB-TST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
288	T.DISCLOSE_DB-TST_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
289	T.FORGERY_LINK_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.LINK_REG;M.DATA_REST
290	T.MODIFY_LINK_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.LINK_REG;M.DATA_REST
291	T.ERACE_LINK_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.LINK_REG;M.DATA_REST
292	T.IMPERSON_LINK_ADMIN	無	防止	－
			検出	－
			回復	－
293	T.STEAL_LINK_ADMIN	無	防止	－
			検出	－
			回復	－
294	T.DISCLOSE_LINK_ADMIN	無	防止	－
			検出	－
			回復	－
295	T.FORGERY_LINK_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.LINK_REG;M.DATA_REST
296	T.MODIFY_LINK_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.LINK_PROV;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.LINK_REG;M.DATA_REST
297	T.ERACE_LINK_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LINK_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.LINK_REG;M.DATA_REST
298	T.IMPERSON_LINK_OPE	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
299	T.STEAL_LINK_OPE	無	防止	－
			検出	－
			回復	－
300	T.DISCLOSE_LINK_OPE	無	防止	－
			検出	－
			回復	－
301	T.FORGERY_LINK_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL；M.LINK_PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.LINK_REG；M.DATA_REST
302	T.MODIFY_LINK_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL；M.LINK_PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.LINK_REG；M.DATA_REST
303	T.ERACE_LINK_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL；M.EDU；M.CONT；M.PENA
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.LINK_REG；M.DATA_REST
304	T.IMPERSON_LINK_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.AC_REST
305	T.STEAL_LINK_AUDIT	無	防止	－
			検出	－
			回復	－
306	T.DISCLOSE_LINK_AUDIT	無	防止	－
			検出	－
			回復	－
307	T.FORGERY_CONFIG_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.CONF_REG；M.DATA_REST
308	T.MODIFY_CONFIG_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.CONF_REG；M.DATA_REST
309	T.ERACE_CONFIG_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.CONF_REG；M.DATA_REST
310	T.IMPERSON_CONFIG_ADMIN	無	防止	－
			検出	－
			回復	－
311	T.STEAL_CONFIG_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
312	T.DISCLOSE_CONFIG_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
313	T.FORGERY_CONFIG_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.CONF_REG；M.DATA_REST
314	T.MODIFY_CONFIG_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.CONF_REG；M.DATA_REST
315	T.ERACE_CONFIG_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.CONF_REG；M.DATA_REST
316	T.IMPERSON_CONFIG_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.AC_REST
317	T.STEAL_CONFIG_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
318	T.DISCLOSE_CONFIG_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
319	T.FORGERY_CONFIG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CONF_REG;M.DATA_REST
320	T.MODIFY_CONFIG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CONF_REG;M.DATA_REST
321	T.ERACE_CONFIG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.CONF_REG;M.DATA_REST
322	T.IMPERSON_CONFIG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
323	T.STEAL_CONFIG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
324	T.DISCLOSE_CONFIG_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	－
325	T.FORGERY_DB-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_ERACE
326	T.MODIFY_DB-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_CHANGE
327	T.ERACE_DB-ID-PW_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_REGI
150	T.IMPERSON_DB-ID-PW_ADMIN	無	防止	－
			検出	－
			回復	－
151	T.STEAL_DB-ID-PW_ADMIN	有	防止	M.USER_PW_NOT;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
152	T.DISCLOSE_DB-ID-PW_ADMIN	有	防止	M.USER_PW_NOT;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
153	T.FORGERY_DB-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_ERACE
154	T.MODIFY_DB-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_CHANGE
155	T.ERACE_DB-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_REGI
156	T.IMPERSON_DB-ID-PW_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
157	T.STEAL_DB-ID-PW_OPE	有	防止	M.USER_PW_NOT;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
158	T.DISCLOSE_DB-ID-PW_OPE	有	防止	M.USER_PW_NOT;M.EDU;M.CONT;M.PENA
			検出	M.USER_DOUBT;M.USER_CONT;M.AUDIT
			回復	M.PW_CHANGE
159	T.FORGERY_DB-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_ERACE
160	T.MODIFY_DB-ID-PW_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.ID_CHANGE

項番	脅威名	リスク有無	目標種別	セキュリティ目標
161	T.ERACE_DB-ID-PW_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.ID_REGI
162	T.IMPERSON_DB-ID-PW_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.AC_REST
163	T.STEAL_DB-ID-PW_AUDIT	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE
164	T.DISCLOSE_DB-ID-PW_AUDIT	有	防止	M.USER_PW_NOT；M.EDU；M.CONT；M.PENA
			検出	M.USER_DOUBT；M.USER_CONT；M.AUDIT
			回復	M.PW_CHANGE
165	T.FORGERY_LINK-PROV_ADMIN	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_COMP；M.AUDIT
			回復	M.LINK_PROV_COPY
166	T.MODIFY_LINK-PROV_ADMIN	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_COMP；M.AUDIT
			回復	M.LINK_PROV_COPY
167	T.ERACE_LINK-PROV_ADMIN	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_LOST；M.AUDIT
			回復	M.LINK_PROV_COPY
168	T.IMPERSON_LINK-PROV_ADMIN	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.USER_INQ；M.AUDIT
			回復	M.ATTACK_REM
169	T.STEAL_LINK-PROV_ADMIN	無	防止	－
			検出	－
			回復	－
170	T.DISCLOSE_LINK-PROV_ADMIN	無	防止	－
			検出	－
			回復	－
171	T.FORGERY_LINK-PROV_OPE	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_COMP；M.AUDIT
			回復	M.LINK_PROV_COPY
172	T.MODIFY_LINK-PROV_OPE	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_COMP；M.AUDIT
			回復	M.LINK_PROV_COPY
173	T.ERACE_LINK-PROV_OPE	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_LOST；M.AUDIT
			回復	M.LINK_PROV_COPY
174	T.IMPERSON_LINK-PROV_OPE	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.USER_INQ；M.AUDIT
			回復	M.ATTACK_REM
175	T.STEAL_LINK-PROV_OPE	無	防止	－
			検出	－
			回復	－
176	T.DISCLOSE_LINK-PROV_OPE	無	防止	－
			検出	－
			回復	－
177	T.FORGERY_LINK-PROV_AUDIT	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_COMP；M.AUDIT
			回復	M.LINK_PROV_COPY
178	T.MODIFY_LINK-PROV_AUDIT	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_COMP；M.AUDIT
			回復	M.LINK_PROV_COPY
179	T.ERACE_LINK-PROV_AUDIT	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.LINK_PROV_LOST；M.AUDIT
			回復	M.LINK_PROV_COPY
180	T.IMPERSON_LINK-PROV_AUDIT	有	防止	M.PROV；M.EDU；M.CONT；M.PENA
			検出	M.USER_INQ；M.AUDIT
			回復	M.ATTACK_REM

項番	脅威名	リスク有無	目標種別	セキュリティ目標
181	T.STEAL_LINK-PROV_AUDIT	無	防止	－
			検出	－
			回復	－
182	T.DISCLOSE_LINK-PROV_AUDIT	無	防止	－
			検出	－
			回復	－
183	T.FORGERY_EVENT_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
184	T.MODIFY_EVENT_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
185	T.ERACE_EVENT_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
186	T.IMPERSON_EVENT_ADMIN	無	防止	－
			検出	－
			回復	－
187	T.STEAL_EVENT_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
188	T.DISCLOSE_EVENT_ADMIN	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
189	T.FORGERY_EVENT_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
190	T.MODIFY_EVENT_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
191	T.ERACE_EVENT_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
192	T.IMPERSON_EVENT_OPE	無	防止	－
			検出	－
			回復	－
193	T.STEAL_EVENT_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
194	T.DISCLOSE_EVENT_OPE	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
195	T.FORGERY_EVENT_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
196	T.MODIFY_EVENT_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.DATA_REST
197	T.ERACE_EVENT_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
	T.IMPERSON_EVENT_AUDIT	有	回復	M.DATA_REST
198	T.IMPERSON_EVENT_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	M.AC_REST
199	T.STEAL_EVENT_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－
200	T.DISCLOSE_EVENT_AUDIT	有	防止	M.FAC_ISO；M.FW；M.AC；M.EDU；M.CONT；M.PENA
			検出	M.LOG_AUDIT；M.ERR_CHECK；M.AUDIT
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
201	T.FORGERY_CLOCK_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
202	T.MODIFY_CLOCK_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
203	T.ERACE_CLOCK_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
204	T.IMPERSON_CLOCK_ADMIN	無	防止	－
			検出	－
			回復	－
205	T.STEAL_CLOCK_ADMIN	無	防止	－
			検出	－
			回復	－
206	T.DISCLOSE_CLOCK_ADMIN	無	防止	－
			検出	－
			回復	－
207	T.FORGERY_CLOCK_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
208	T.MODIFY_CLOCK_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
209	T.ERACE_CLOCK_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
210	T.IMPERSON_CLOCK_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
211	T.STEAL_CLOCK_OPE	無	防止	－
			検出	－
			回復	－
212	T.DISCLOSE_CLOCK_OPE	無	防止	－
			検出	－
			回復	－
213	T.FORGERY_CLOCK_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
214	T.MODIFY_CLOCK_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
215	T.ERACE_CLOCK_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.TA_AUDIT;M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.TA_DELI_BC;M.CLOCK_REST
216	T.IMPERSON_CLOCK_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT
			回復	M.AC_REST
217	T.STEAL_CLOCK_AUDIT	無	防止	－
			検出	－
			回復	－
218	T.DISCLOSE_CLOCK_AUDIT	無	防止	－
			検出	－
			回復	－
219	T.FORGERY_MOD-CRE-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
220	T.MODIFY_MOD-CRE-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP

項番	脅威名	リスク有無	目標種別	セキュリティ目標
221	T.ERACE_MOD-CRE-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
222	T.IMPERSON_MOD-CRE-TS_ADMIN	無	防止	－
			検出	－
			回復	－
223	T.STEAL_MOD-CRE-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
224	T.DISCLOSE_MOD-CRE-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
225	T.FORGERY_MOD-CRE-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
226	T.MODIFY_MOD-CRE-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
227	T.ERACE_MOD-CRE-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
228	T.IMPERSON_MOD-CRE-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
229	T.STEAL_MOD-CRE-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
230	T.DISCLOSE_MOD-CRE-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
231	T.FORGERY_MOD-CRE-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
232	T.MODIFY_MOD-CRE-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
233	T.ERACE_MOD-CRE-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
234	T.IMPERSON_MOD-CRE-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
235	T.STEAL_MOD-CRE-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
236	T.DISCLOSE_MOD-CRE-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
237	T.FORGERY_MOD-STORE_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
238	T.MODIFY_MOD-STORE_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
239	T.ERACE_MOD-STORE_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
240	T.IMPERSON_MOD-STORE_ADMIN	無	防止	－
			検出	－
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
241	T.STEAL_MOD-STORE_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
242	T.DISCLOSE_MOD-STORE_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
243	T.FORGERY_MOD-STORE_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
244	T.MODIFY_MOD-STORE_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
245	T.ERACE_MOD-STORE_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
246	T.IMPERSON_MOD-STORE_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
247	T.STEAL_MOD-STORE_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
248	T.DISCLOSE_MOD-STORE_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
249	T.FORGERY_MOD-STORE_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
250	T.MODIFY_MOD-STORE_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
251	T.ERACE_MOD-STORE_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
252	T.IMPERSON_MOD-STORE_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
253	T.STEAL_MOD-STORE_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
254	T.DISCLOSE_MOD-STORE_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
255	T.FORGERY_MOD-COM-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
256	T.MODIFY_MOD-COM-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
257	T.ERACE_MOD-COM-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
258	T.IMPERSON_MOD-COM-TS_ADMIN	無	防止	－
			検出	－
			回復	－
259	T.STEAL_MOD-COM-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
260	T.DISCLOSE_MOD-COM-TS_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－

項番	脅威名	リスク有無	目標種別	セキュリティ目標
261	T.FORGERY_MOD-COM-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
262	T.MODIFY_MOD-COM-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
263	T.ERACE_MOD-COM-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
264	T.IMPERSON_MOD-COM-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
265	T.STEAL_MOD-COM-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
266	T.DISCLOSE_MOD-COM-TS_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
267	T.FORGERY_MOD-COM-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
268	T.MODIFY_MOD-COM-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
269	T.ERACE_MOD-COM-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
270	T.IMPERSON_MOD-COM-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
271	T.STEAL_MOD-COM-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
272	T.DISCLOSE_MOD-COM-TS_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
273	T.FORGERY_MOD-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
274	T.MODIFY_MOD-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
275	T.ERACE_MOD-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
276	T.IMPERSON_MOD-TIME_ADMIN	無	防止	－
			検出	－
			回復	－
277	T.STEAL_MOD-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
278	T.DISCLOSE_MOD-TIME_ADMIN	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
279	T.FORGERY_MOD-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
280	T.MODIFY_MOD-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP

項番	脅威名	リスク有無	目標種別	セキュリティ目標
281	T.ERACE_MOD-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
282	T.IMPERSON_MOD-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
283	T.STEAL_MOD-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
284	T.DISCLOSE_MOD-TIME_OPE	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
285	T.FORGERY_MOD-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
286	T.MODIFY_MOD-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
287	T.ERACE_MOD-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.MOD_WATCH;M.AUDIT;M.MOD_CHECK
			回復	M.SW_REST;M.RECOMP
288	T.IMPERSON_MOD-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.DUAL;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	M.AC_REST
289	T.STEAL_MOD-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－
290	T.DISCLOSE_MOD-TIME_AUDIT	有	防止	M.FAC_ISO;M.FW;M.AC;M.EDU;M.CONT;M.PENA
			検出	M.LOG_AUDIT;M.ERR_CHECK;M.AUDIT;M.MOD_CHECK
			回復	－

第6章 タイムスタンプ検証不可能時の考察

1. 利用者側のセキュリティ環境

1-1 前提

利用者側のセキュリティ環境の前提一覧を、以下の表 19に示す。

表 19　利用者側のセキュリティ環境の前提一覧

#	分類	項目	説明	実現方法例
1	—	A.CLIENT	クライアントソフトウェアは正しく動作する。	利用者は TSA が正常動作を確認したクライアントモジュールを使用する。
2		A.DATA_MANAGE	タイムスタンプとタイムスタンプ対象データの対応は正しく管理される。	利用者はタイムスタンプトークン及びタイムスタンプ対象データの保管は利用者の責任であることを明記したサービス利用規約に同意の上、サービスを利用する。
3		A.DATA_INTEGRITY	タイムスタンプ、タイムスタンプ対象データの完全性は保証される。	利用者はタイムスタンプトークン及びタイムスタンプ対象データの保管は利用者の責任であることを明記したサービス利用規約に同意の上、サービスを利用する。
4		A.PROTOCOL_DISCLOSE	タイムスタンプの付与及び検証の方式は利用者に公開される。	TSA ポリシーもしくは技術資料等において、タイムスタンプの付与及び検証の方式が公開される。
5		A.TSA1_TTP	利用者と通信する TSA1 は信頼できる。	TSA1 セキュリティ評価が実施され、信頼できる。
6		A.TSA1_CONNECTION	利用者と TSA1 の間の通信路は、TSA1 への成りすまし、データの改ざん、データの盗聴を防止する。	利用者と TSA1 の間の通信路は、SSL により、相互認証、メッセージ認証、メッセージ暗号化が行われている。

1-2 脅威

利用者側のセキュリティ環境の脅威一覧を、以下の表 20に示す。

表 20　利用者側のセキュリティ環境の脅威一覧

#	分類	項目	説明
1	TOE（個別）	T.OS_CHANGE	利用者側のデファクト OS の変遷により、クライアントソフトが非対応となる。
2		T.OS_RENEW	利用者側の OS のメジャーな改版により、クライアントソフトが非対応となる。
3		T.HARD_CHANGE	利用者側のデファクトハードウェアの変遷により、保管データ及びクライアントソフトが対応している OS が動作しなくなる。
4		T.HARD_RENEW	利用者側のハードウェアのメジャーな改版により、保管データ及びクライアントソフトが対応している OS が動作しなくなる。
5		T.TSA_CEASE	事業者の事業判断により、TSA が事業を引き継がず撤退する。
6		T.TSA_VANISH	事業主体の消滅により、TSA が事業を引き継がず撤退する。
7		T.TA_CEASE	事業者の事業判断により、TA が事業を引き継がず撤退する。
8		T.TA_VANISH	事業主体の消滅により、TA が事業を引き継がず撤退する。
9		T.CA_CEASE	事業者の事業判断により、TA が使用する CA が事業を引き継がず撤退する。
10		T. CA_VANISH	事業主体の消滅により、 TA が使用する CA が事業を引き継がず撤退する。
11		T.VENDOR_ CEASE	事業者の事業判断により、TSA に対するハードウェア・ソフトウェアの供給事業者が事業を引き継がず撤退する。
12		T. VENDOR_ VANISH	事業主体の消滅により、TSA に対するハードウェア・ソフトウェアの供給事業者が事業を引き継がず撤退する。
13		T.DOC_HASH_ COMP_ALG_ DEFECT	アルゴリズムの欠陥及び攻撃方法の発見による、ドキュメントハッシュを生成するハッシュアルゴリズムの脆弱化。
14		T.DOC_HASH_ COMP_CALC_POWER	計算機性能の飛躍的向上による、ドキュメントハッシュを生成するハッシュアルゴリズムの脆弱化。
15		T.LINK_HASH_ COMP_ALG_DEFECT	アルゴリズムの欠陥及び攻撃方法の発見による、リンク情報を生成するハッシュアルゴリズムの脆弱化。
16		T.LINK_HASH_ COMP_CALC_POWER	計算機性能の飛躍的向上による、リンク情報を生成するハッシュアルゴリズムの脆弱化。
17		T.TAR_CRYPT_ COMP_ALG_DEFECT	アルゴリズムの欠陥及び攻撃方法の発見による、時刻監査レポートに使用されている暗号技術の脆弱化。

#	分類	項目	説明
18		T.TAR_CRYPT_COMP_CALC_POWER	計算機性能の飛躍的向上による、時刻監査レポートに使用されている暗号技術の脆弱化。
19		T.DB-TST_LOSS_ERACE	照合用データの不正な消去操作による、照合用データの一部または全部の消失。
20		T.DB-TST_LOSS_FAULT	操作ミス、災害等による、照合用データの一部または全部の消失。
21		T.DB-TST_INCONSISTENT_MODIFY	照合用データの偽造・改竄による、リンク情報の関連性における不整合。
22		T.DB-TST_INCONSISTENT_CHANGE	操作ミス、災害等による、照合用データの改変に起因するリンク情報の関連性における不整合。
23		T.DB-TST_INCONSISTENT_FAULT	システムの誤動作等に起因するリンク情報の誤計算による、リンク情報の関連性における不整合。

1-3 組織のセキュリティーポリシー

利用者側のセキュリティ環境の組織のセキュリティポリシー一覧を、以下の表 21に示す。

表 21　利用者側のセキュリティ環境の組織のセキュリティポリシー一覧

#	項目	説明	実現方法例
1	P.CLI_CRYPTO	利用者側での全ての暗号処理は、「電子政府推奨暗号リスト(平成 15 年 2 月 20 日、総務省、経済産業省)」に記載されたアルゴリズムによって実装される。	ドキュメントハッシュ及びリンク情報の生成においては、SHA-512 と RIPEMD-160 を並列に使用している。利用者との SSL 通信においては、公開鍵暗号として鍵長 1024 ビットの RSASSA-PKCS1-v1_5、鍵長 128 ビット以上の共通鍵暗号を使用している。

2. タイムスタンプ検証不可能時の脅威ツリー

タイムスタンプ検証不可能時の脅威ツリーを、以下の図 11に示す。

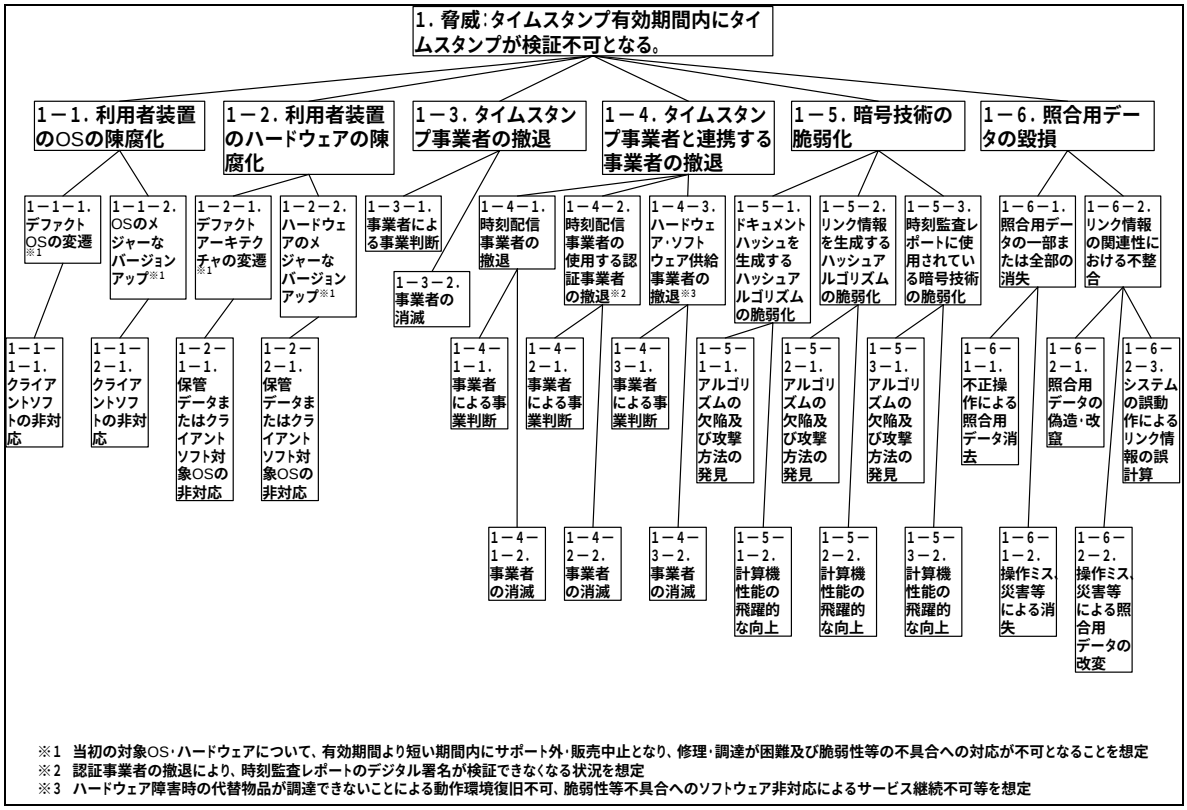


図 11　タイムスタンプ検証不可能時の脅威ツリー

3. 対策に関する考察

利用者側の脅威のセキュリティ目標に含まれる対策名一覧を以下の表 22に示す。

表 22　利用者側の脅威のセキュリティ目標に含まれる対策名一覧

項番	種別	対策名	説明
1	防止	M.AC	サーバ内のデータに対する適切なアクセス管理
2	防止	M.CLI_MULTI_LANG	クライアントソフトのマルチプラットフォーム言語への対応
3	防止	M.CLI_MULTI_OS	クライアントソフトの複数OSへの対応
4	防止	M.CRY_MULTI	暗号アルゴリズムの二重化
5	防止	M.CRY_RECOM	公的な評価機関により推奨されている暗号アルゴリズムの利用
6	防止	M.DUAL	複数人による相互牽制の下での運用
7	防止	M.FAC_ISO	隔離され入退室管理が施された室へのサーバ機器の設置
8	防止	M.FAC_SOL	災害対策の施されたビルへの設置
9	防止	M.FW	サーバと外部ネットワークとの接続点におけるファイアウォールによる不要通信遮断
10	防止	M.INDIR_SUC	引継ぎ規定のあるベンダ製品、TA及びCA等を利用したTSAの提供するサービスの利用
11	防止	M.SYS_TEST	システムの動作試験
12	防止	M.TS_ARCH	タイムスタンプの再付与による長期保証
13	防止	M.TSA_SUC	引継ぎ規定のあるTSAの提供するサービスの利用
14	防止	M.TST_VAL_PUB	タイムスタンプトークンのプロファイル及び検証方法の公表
15	検出	M.CLI_CHECK	クライアントソフトの動作検証
16	検出	M.CRY_CHECK	公的な評価機関による暗号アルゴリズムの評価結果のチェック
17	検出	M.ERR_CHECK	サーバで出力されるエラーの常時チェック
18	検出	M.HW_RESEARCH	ハードウェアの利用動向の調査
19	検出	M.LINK_AUDIT	リンク情報の整合性に関する監査
20	検出	M.LOG_AUDIT	サーバを構成する機器の動作ログの監査
21	検出	M.NOTIFY	TSA、TA及びCA等のサービス提供者ならびにベンダーによる通知･公表
22	検出	M.OS_CHECK	OSの動作検証
23	検出	M.OS_RESEARCH	OSの利用動向の調査
24	回復	M.CLI_RENEW	新しいプラットフォームに対応したクライアントソフトの提供
25	回復	M.EMU	エミュレータの利用
26	回復	M.REST	バックアップからのデータの復旧
27	回復	M.SYS_CHANGE	別のベンダの製品を利用したシステムへの移行
28	回復	M.TA_CHANGE	別TAへの移行
29	回復	M.VAL_DEV	検証用ツールの自己開発
30	回復	M.VAL_PROVIDE	照合用データ及びリンク情報等からなる検証に必要な全てのデータならびにこれらを用いたローカルでの検証方法の詳細な手順もしくは検証用ツールの提供

利用者側の脅威のセキュリティ目標・対策一覧を以下の表 23に示す。

表 23　利用者側の脅威のセキュリティ目標・対策一覧

項番	脅威名	リスク有無	目標種別	セキュリティ目標･対策
1	T.OS_CHANGE	有	防止	M.CLI_MULTI_OS；M.CLI_MULTI_LANG；M.TST_VAL_PUB
			検出	M.OS_RESEARCH；M.CLI_CHECK
			回復	M.EMU；M.CLI_RENEW；M.VAL_DEV
2	T.OS_RENEW	有	防止	M.CLI_MULTI_OS；M.CLI_MULTI_LANG；M.TST_VAL_PUB
			検出	M.NOTIFY；M.CLI_CHECK
			回復	M.EMU；M.CLI_RENEW；M.VAL_DEV
3	T.HARD_CHANGE	有	防止	M.CLI_MULTI_OS；M.CLI_MULTI_LANG；M.TST_VAL_PUB
			検出	M.HW_RESEARCH；M.OS_CHECK
			回復	M.EMU；M.CLI_RENEW；M.VAL_DEV
4	T.HARD_RENEW	有	防止	M.CLI_MULTI_OS；M.CLI_MULTI_LANG；M.TST_VAL_PUB
			検出	M.NOTIFY；M.OS_CHECK
			回復	M.EMU；M.CLI_RENEW；M.VAL_DEV
5	T.TSA_CEASE	有	防止	M.TSA_SUC
			検出	M.NOTIFY
			回復	M.VAL_PROVIDE
6	T.TSA_VANISH	有	防止	M.TSA_SUC
			検出	M.NOTIFY
			回復	M.VAL_PROVIDE
7	T.TA_CEASE	有	防止	M.INDIR_SUC
			検出	M.NOTIFY
			回復	M.TA_CHANGE
8	T.TA_VANISH	有	防止	M.INDIR_SUC
			検出	M.NOTIFY
			回復	M.TA_CHANGE
9	T.CA_CEASE	有	防止	M.INDIR_SUC
			検出	M.NOTIFY
			回復	－
10	T.CA_VANISH	有	防止	M.INDIR_SUC
			検出	M.NOTIFY
			回復	－
11	T.VENDOR_CEASE	有	防止	M.INDIR_SUC
			検出	M.NOTIFY
			回復	M.SYS_CHANGE
12	T. VENDOR_VANISH	有	防止	M.INDIR_SUC
			検出	M.NOTIFY
			回復	M.SYS_CHANGE
13	T.DOC_HASH_COMP_ALG_DEFECT	有	防止	M.CRY_RECOM；M.CRY_MULTI；M.TS_ARCH
			検出	M.CRY_CHECK
			回復	－
14	T.DOC_HASH_COMP_CALC_POWER	有	防止	M.CRY_RECOM；M.CRY_MULTI；M.TS_ARCH
			検出	M.CRY_CHECK
			回復	－
15	T.LINK_HASH_COMP_ALG_DEFECT	有	防止	M.CRY_RECOM；M.CRY_MULTI；M.TS_ARCH
			検出	M.CRY_CHECK
			回復	－
16	T.LINK_HASH_COMP_CALC_POWER	有	防止	M.CRY_RECOM；M.CRY_MULTI；M.TS_ARCH
			検出	M.CRY_CHECK
			回復	－
17	T.TAR_CRYPT_COMP_ALG_DEFECT	有	防止	M.CRY_RECOM
			検出	M.CRY_CHECK
			回復	－
18	T.TAR_CRYPT_COMP_CALC_POWER	有	防止	M.CRY_RECOM
			検出	M.CRY_CHECK
			回復	－
19	T.DB-TST_LOSS_ERACE	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL

項番	脅威名	リスク有無	目標種別	セキュリティ目標・対策
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.REST
20	T.DB-TST_LOSS_FAULT	有	防止	M.SYS_TEST；M.FAC_SOL；M.AC；M.DUAL
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.REST
21	T.DB-TST_INCONSISTENT_MODIFY	有	防止	M.FAC_ISO；M.FW；M.AC；M.DUAL
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.REST
22	T.DB-TST_INCONSISTENT_CHANGE	有	防止	M.SYS_TEST；M.FAC_SOL；M.AC；M.DUAL
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.REST
23	T.DB-TST_INCONSISTENT_FAULT	有	防止	M.SYS_TEST
			検出	M.LINK_AUDIT；M.LOG_AUDIT；M.ERR_CHECK
			回復	M.REST

セキュリティ評価報告書

（TOE：TSA2 ）

平成 18 年 2 月 28 日

目次

第1章 TOE の概要

本章では、TOE の機能概要、TOE 構成図、利用する暗号技術と暗号コンポーネント構成図、関与者、資産について記載する。

1. TOE の機能概要

1-1 TOE の機能

以下に、TOE を構成する機能の概要を示す。

(1)タイムスタンプ発行機能（受諾ハッシュアルゴリズム選択機能を含む）

TOE は、RFC3161 に基づいた独立トークン方式*1のタイムスタンプトークンを発行する。

また、TOE は、タイムスタンプ要求に含まれるハッシュ値のハッシュアルゴリズムに応じて、そのタイムスタンプ要求を受け付けるか否かを選択する機能を持つ（受諾ハッシュアルゴリズム選択機能）。

(2)時刻受信機能

TOE は、時刻配信プロトコル（認証連鎖方式*2）によって配信される時刻情報を受信するための機能を持つ。受信した時刻情報により、時刻配信プロトコルおよびタイムスタンプの発行に使用される HSM 時刻（HSM の時計の時刻と、受信した時刻情報をもとに生成した時刻）と、ログに使用されるシステム時刻が補正される。

(3)時刻管理機能

TOE のタイムスタンプ発行機能および時刻受信機能には、HSM 時刻（HSM の時計の時刻と、受信した時刻情報をもとに生成した時刻）が使用される。ログ管理機能の時刻には、システム時刻が使用される。

(4)ログ管理機能

TOE は、TOE の動作記録、時刻受信記録、操作記録などをログとして保管することが可能である。ログは、署名を付与し保護することが可能である。

(5)鍵管理機能

TOE は、通信用(TLS)の秘密鍵および署名用の秘密鍵を管理する機能を持つ。TOE の署名用の秘密鍵は、HSM によって保護されている。

(6)シリアル番号管理機能

タイムスタンプトークンのシリアル番号は、HSM 内に保管される。

(7)証明書管理機能

TOE は、通信(TLS)および署名・検証に関わる証明書を管理する機能を持つ。

(8)設定管理機能

TOE は、TOE の機能に関わる設定を管理する機能を持つ。

(9)TOE 管理機能

TOE の設定・操作は、ブラウザから管理画面にアクセスして実施する。

＊１：ここでいう独立トークン方式タイムスタンプとは、TSA がタイムスタンプ対象データのハッシュ値に対してデジタル署名を行い、それぞれのタイムスタンプの有効性を証明する方式。

＊２：ここでいう認証連鎖方式とは、PKI(Public Key Infrastructure)認証技術を利用して TA が時刻配信先の時計を特定すると同時に時刻の計測と配信を行い、その計測結果を時刻監査記録として更に時刻配信先の時計に連鎖していく方式。

1-2 TOE 構成図

以下に、統合化プラットフォームシステムにおいて TOE が使用される際のシステム構成図を示す。(強調表示されたコンポーネントは、評価対象外である。)

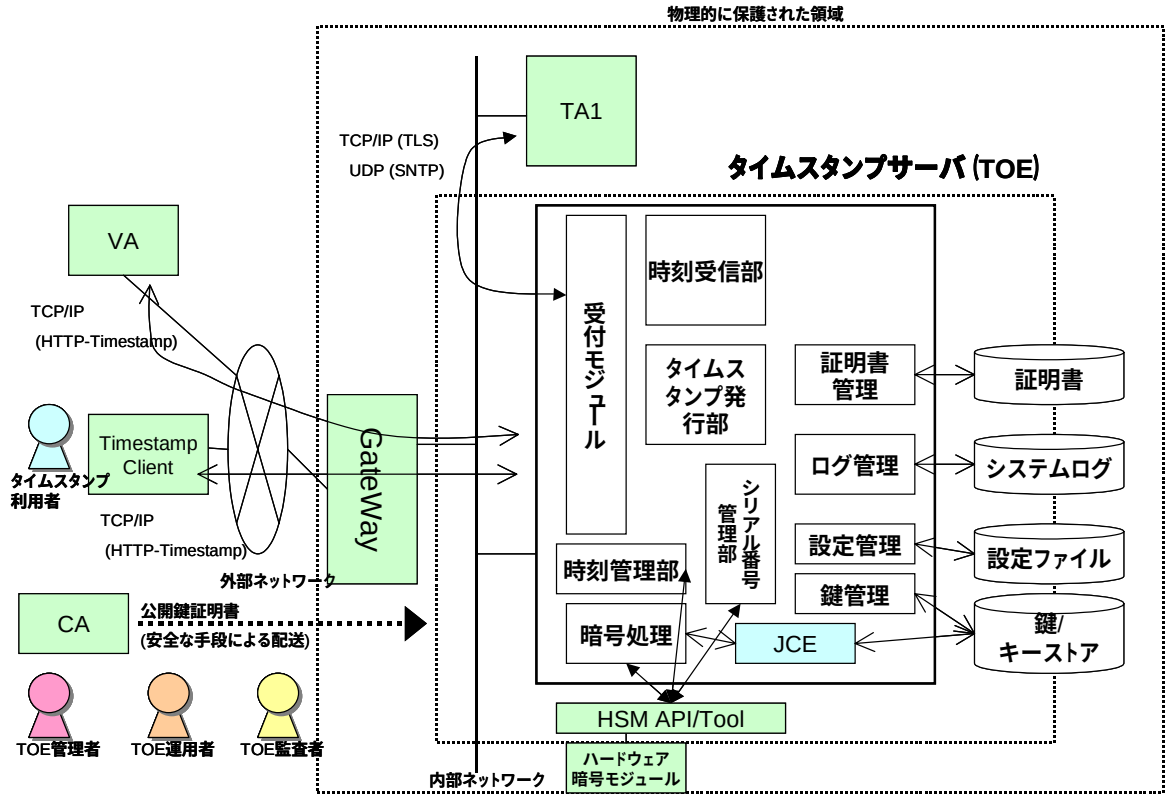


図 1-1　システム構成図

1-3 利用する暗号技術と暗号コンポーネント

以下に、TOE の利用する暗号技術と、暗号コンポーネント構成図を示す。

表 1-1 TOE の利用する暗号技術

#	システム	使用している暗号技術		使用目的
1	TSA2	TLS	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット RSAES-PKCS1-v1_5 鍵長 1024 ビット 【共通鍵暗号方式】 128-bit RC4 【ハッシュ関数】 MD5	通信先の認証・通信データの改ざん防止 (時刻受信)
		SNTP	【メッセージ認証方式】 HMAC(MD5)	通信データの改ざん防止
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット、2048 ビット 【ハッシュ関数】 SHA-1	タイムスタンプトークンへの署名
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット、2048 ビット 【ハッシュ関数】 SHA-1	ログへの署名
		PKI	【公開鍵暗号方式】 RSASSA-PKCS1-v1_5 鍵長 1024 ビット、鍵長 2048 ビット 【ハッシュ関数】 SHA-1	公開鍵証明書の検証、ARL/CRL の検証、時刻監査証明書の検証
		ハッシュ関数	SHA-1	ログの改ざん防止
		受付ハッシュ関数	SHA-1,SHA-512	タイムスタンプに含めるメッセージダイジェスト

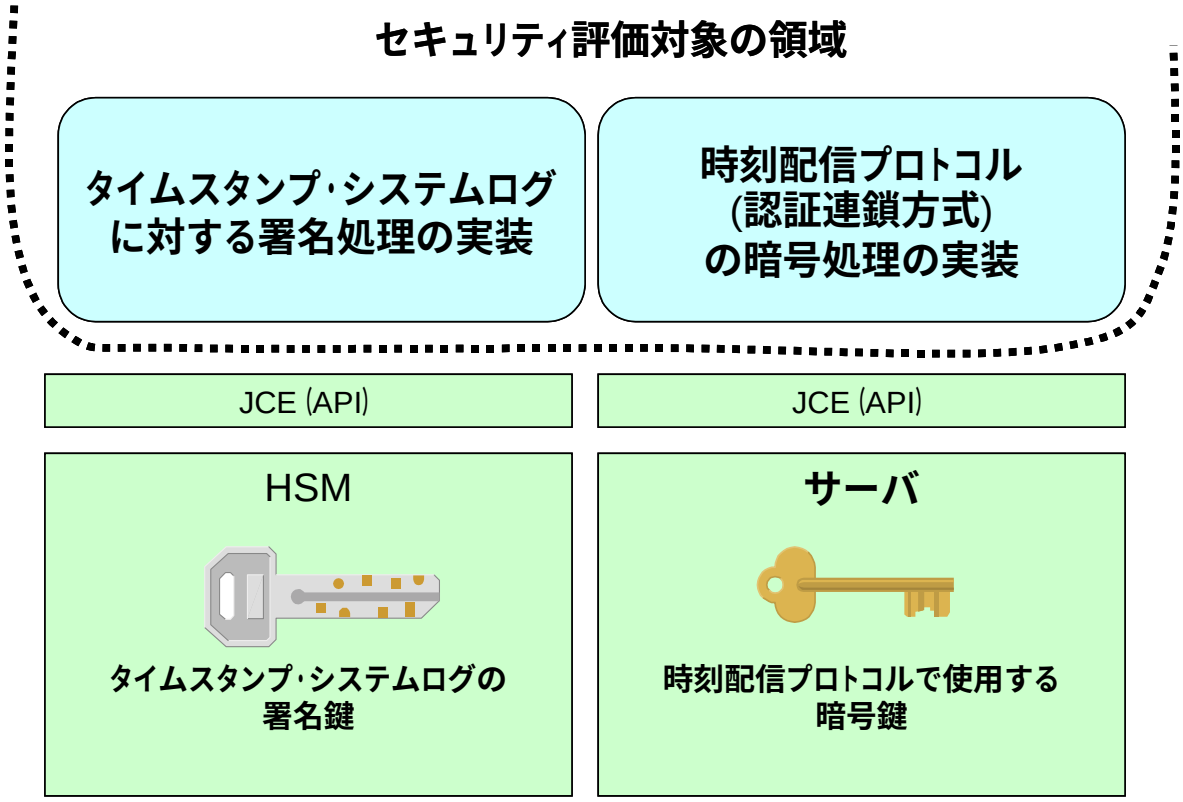
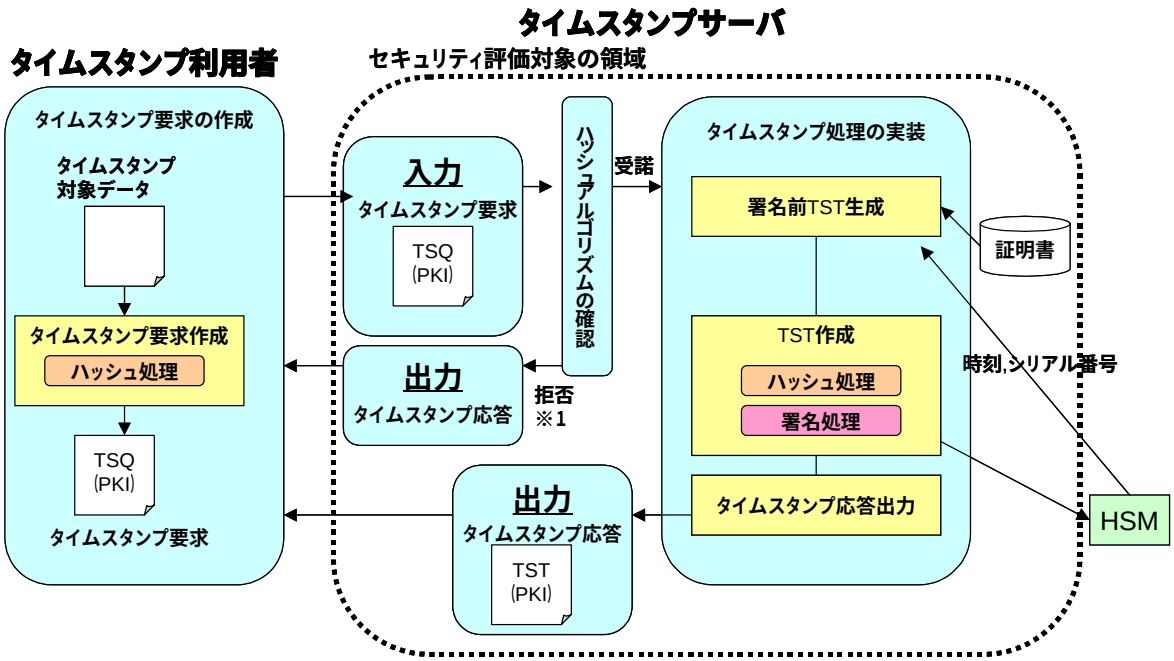


図 1-2　セキュリティ評価対象の領域



※1：タイムスタンプ要求に含まれるハッシュ値のハッシュアルゴリズムが、
受諾可能なハッシュアルゴリズムではない場合、そのタイムスタンプ
要求を拒否する旨のタイムスタンプ応答を返す。

図 1-3　タイムスタンプ（PKI 方式）処理概要

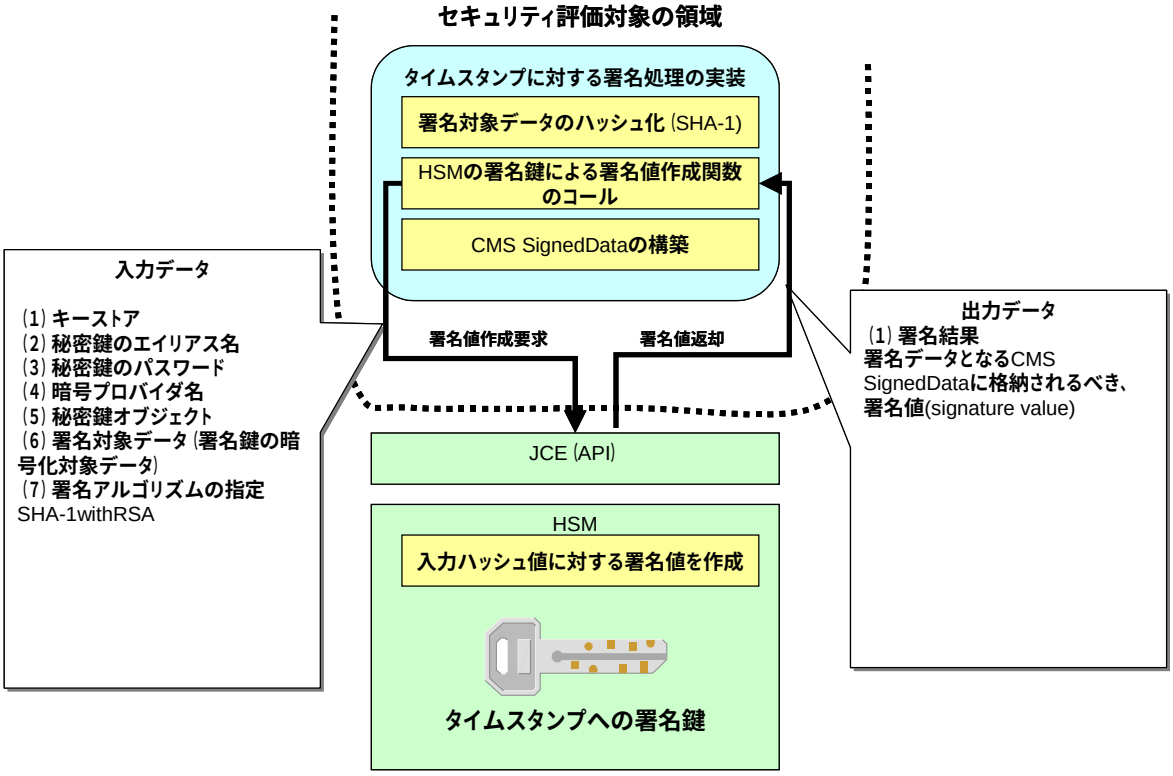


図 1-4　タイムスタンプ（PKI 方式）処理実装（署名処理実装）概要

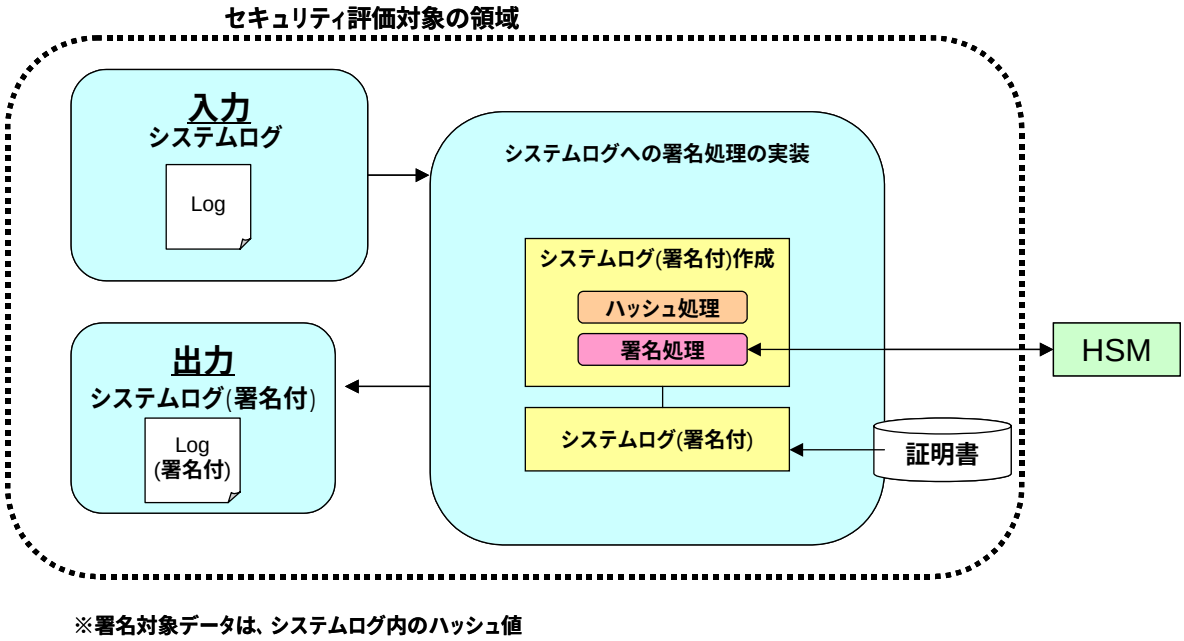


図 1-5　システムログへの署名処理概要

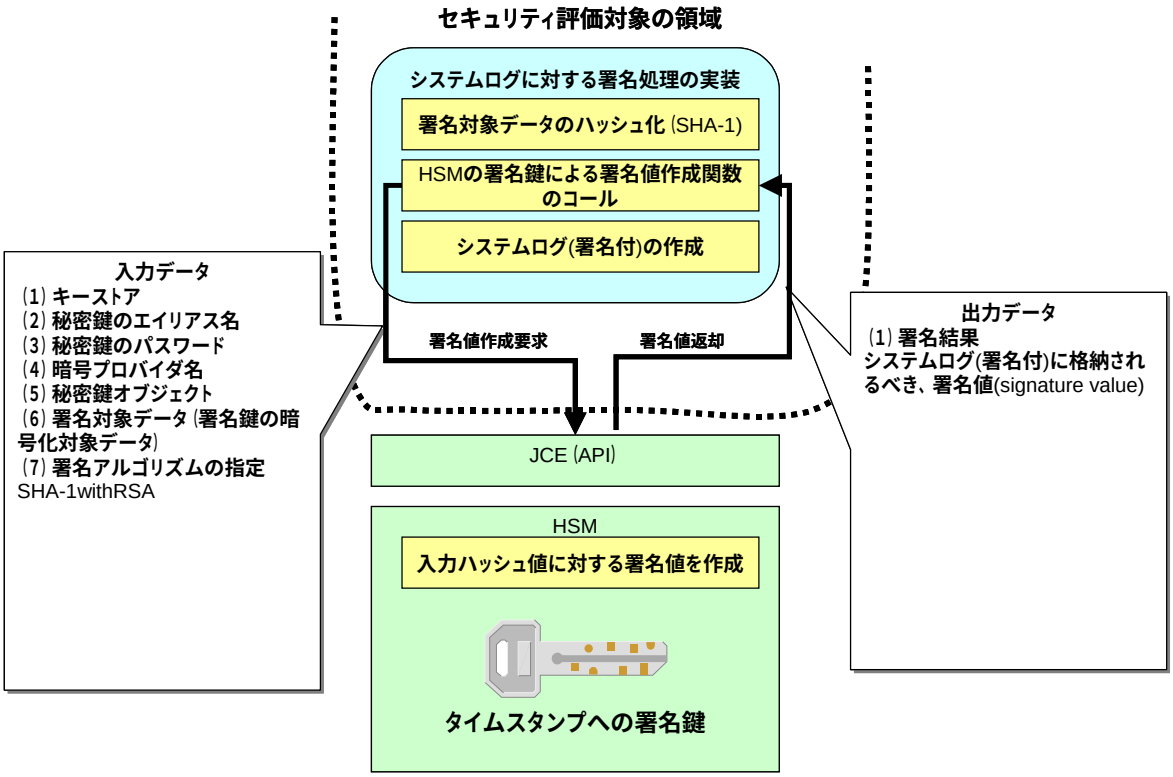


図 1-6　システムログへの署名処理実装概要

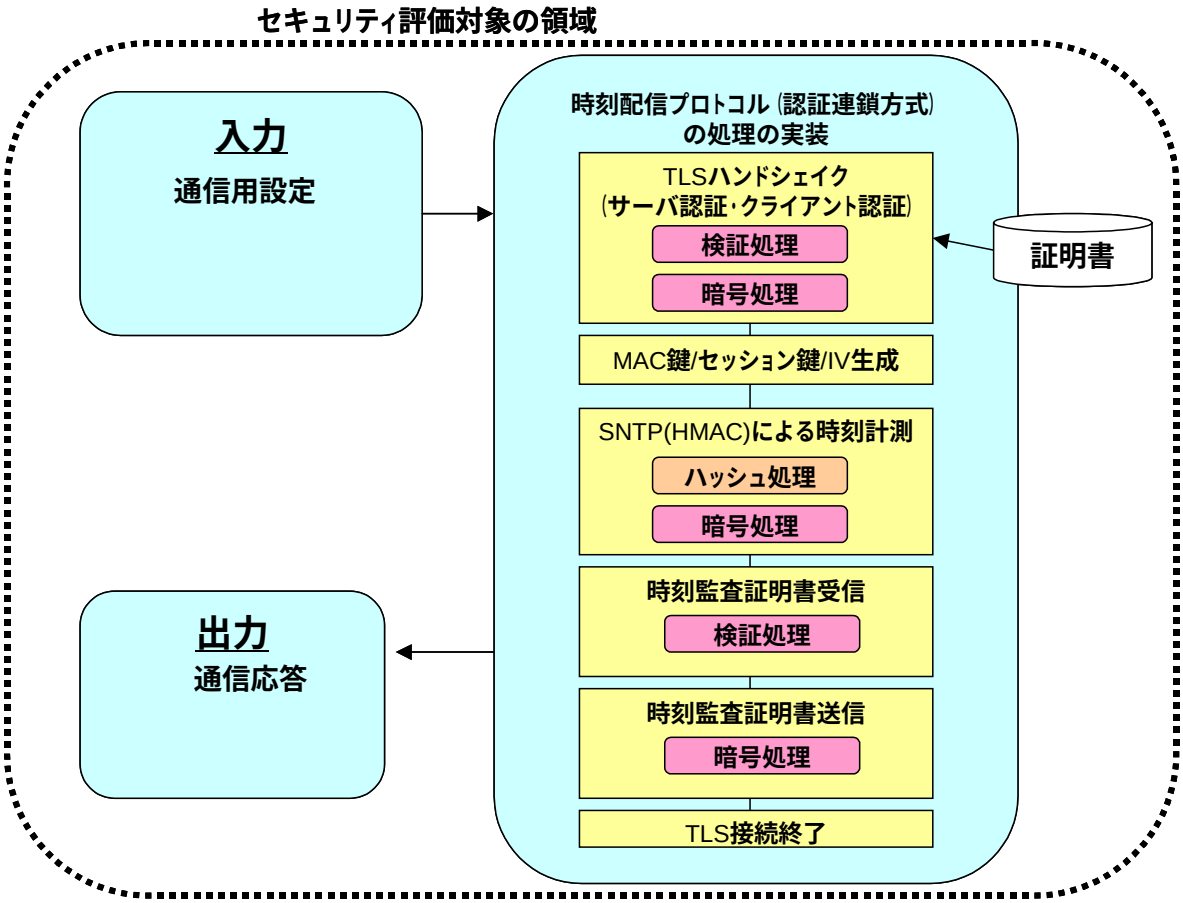


図 1-7　時刻配信プロトコル（認証連鎖方式：受信）処理概要

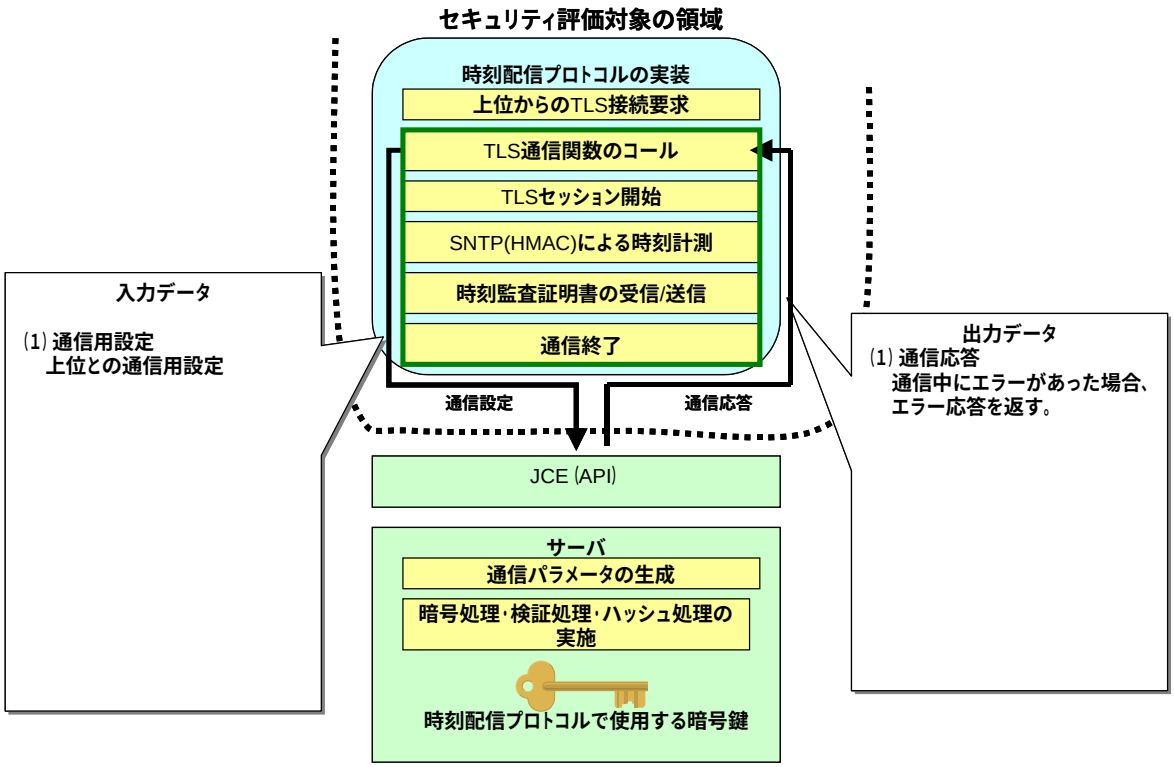


図 1-8　時刻配信プロトコル(認証連鎖方式：受信)処理実装（暗号処理実装）概要

1-4 関与者

以下に、TOE の関与者を示す。

表 1-2　TOE の関与者

#	関与者	説明
1	TOE 管理者	TOE に関わるユーザ/役割を管理する。 時刻・シリアル番号に関する管理業務を行う。 暗号機能に関わる初期化及び管理業務を行う。 悪意のあるソフトウェアが動作しないようにする。 適切なディスクスペースを用意する。 データベースを適切に管理する。
2	TOE 運用者	TOE の起動・停止を実行する。 TOE 管理者の指示の元で各種設定など運用業務を行う。
3	TOE 監査者	TOE が生成する監査データの分析等の監査業務を行う。
4	タイムスタンプ利用者	TOE が提供するタイムスタンプを利用する。
5	TA1	認証連鎖方式の時刻配信局。TOE に対し、認証連鎖方式による時刻の配信および監査を行う。
6	VA	検証局。タイムスタンプの検証を行う。また、タイムスタンプ利用者の一人として、TOE が提供するタイムスタンプを利用する。

1-5 資産

以下に、TOE の資産を示す。

表 1-3　TOE の資産

No.	分類	データ名	資産名
1	鍵/キーストア	秘密鍵(TSA-署名)	秘密鍵
2		秘密鍵(TSA-TLS)	秘密鍵
3		証明書(CA)	設定情報
4		証明書(TSA-署名)	設定情報
5		証明書(TSA-TLS)	設定情報
6	設定ファイル	ポリシ設定	設定情報
7		上位TA設定	設定情報
8		うるう秒設定	設定情報
9		ID･パスワード	ID･パスワード
10		各種設定	設定情報
11	システムログ	システムログ	ログ
12		時刻監査ログ	ログ
13		操作ログ	ログ
14	証明書	CA証明書	設定情報
15		TA証明書(署名)	設定情報
16		TA証明書(TLS)	設定情報
17		NTA証明書(署名)	設定情報
18		ARL	設定情報
19		CRL	設定情報
20	時刻	時刻受信	HSM時刻
21		タイムスタンプ	HSM時刻
22		ロギング	システム時刻
23	シリアル番号	シリアル番号	シリアル番号
24	HSM	ICカード(管理)パスワード	ID･パスワード
25		ICカード(運用)パスワード	ID･パスワード
26	ソフトウェア	タイムスタンプソフトウェア	ソフトウェア
27	タイムスタンプトークン	タイムスタンプトークン	タイムスタンプトークン
28	タイムスタンプ要求	タイムスタンプ要求	タイムスタンプ要求
29	タイムスタンプ応答	タイムスタンプ応答	タイムスタンプ応答

第2章 セキュリティ環境

本章では、内部不正を考慮しないセキュリティ環境（前提、脅威、組織のセキュリティポリシー）について記載する。

1. 前提

以下に、TOE を使用する際のセキュリティ環境の前提を示す。

表 2-1　前提

No.	分類	項目	説明
1	物理的な前提	A.Location	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティの中に設置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2	人的な前提	A.TOE_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOEとTOEに含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOEを安全に導入、管理する。 ・TOEに関わるユーザ/役割を管理する。 ・時刻・シリアル番号に関する管理業務を行う。 ・暗号機能に関わる初期化及び管理業務を行う。 ・TOE上で悪意のあるソフトウェアが動作しないようにする。 ・TOEの用件を満たす適切なディスクスペースを用意する。 ・TOEのデータベースを適切に管理する。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
3	人的な前提	A.TOE_Operator	一人以上の許可された運用者が割り当てられる。 ・TOEの起動・停止を実行する。 ・TOE管理者の指示の元で各種設定など運用業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
4	人的な前提	A.TOE_Auditor	一人以上の許可された監査者が割り当てられる。 ・TOEが生成する監査データの分析等の監査業務を行う。 さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
5	人的な前提	A.TS_Requestor	タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証及び保持する。この中には、アウト・オブ・バンドの方法を用いて、TSA証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当なTSAによって行われたものかどうかの確認、が含まれる。
6	人的な前提	A.TOE_Separation	TOEが動作するサーバマシンには、TOEの動作に必要なソフトウェア以外はインストールされないものとする。
7	接続に関する前提	A.Device	周辺機器への接続は、コントロールされたアクセス・ファシリティ内に存在する。
8	接続に関する前提	A.FIREWALL	ファイアウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
9	接続に関する前提	A.PEER	タイムスタンプ利用者（タイムスタンプ要求者）を除くTOEと通信する意図された他システムは、信頼できる。
10	その他	A.Abstract	TOEが動作するために必要なOSや依存するライブラリは、不正な改変から保護され、正しく動作する。
11	接続に関する前提	A.TSA2_TA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。

12	物理的な前提	A.Environment	TOE の設置場所は、電磁波対策、電力対策、温度･湿度対策が行われている。
13	物理的な前提	A.MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。

2. 脅威

以下に、TOE および環境に対する脅威を示す。

なお、脅威の分類は以下のように区分した。

・分類：TOE

TOE のセキュリティ機能（例：時刻配信プロトコルなど）により対策可能。

・分類：環境

TOE のセキュリティ機能では対策不可能、環境の IT/非 IT 機能（例：外部の IDS システムにより対策、運用により対策）により対策可能。

※TOE のログ管理機能、TOE 管理機能を利用して対策する脅威は、こちらの区分に含めている。

表 2-2　脅威

No.	分類	項目	説明
1	TOE	T.HSMClock_TOEuser_Modify_TimeSource	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。
2	TOE	T.HSMClock_Inaccuracy_gradually	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。)
3	TOE	T.HSMClock_Inaccuracy_immediately	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が故障し、急に時刻がずれる。)
4	TOE	T.HSMClock_TOEuser_Modify_Clock_by TOE	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
5	TOE	T.HSMClock_TOEuser_Modify_Clock_by HSM	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(HSMの機能を利用)
6	TOE	T.HSMClock_Cracker_Modify_Clock	外部の不正者が、ネットワーク経由でTOEが参照する時計の時刻をずらす。
7	TOE	T.SystemClock_TOEuser_Modify_Time Source	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。
8	TOE	T.SystemClock_Inaccuracy_gradually	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。)
9	TOE	T.SystemClock_Inaccuracy_immediatel y	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が故障し、急に時刻がずれる。)
10	TOE	T.SystemClock_TOEuser_Modify_Clock _byTOE	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
11	TOE	T.SystemClock_TOEuser_Modify_Clock _byOS	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(OSの機能を利用)
12	TOE	T.SystemClock_TOEuser_Modify_Clock _byHSM	許可された利用者が、不注意により、TOEが参照する時計の時刻をずらす。(HSMの機能を利用)

13	TOE	T.SystemClock_Cracker_Modify_Clock	外部の不正者が、ネットワーク経由でTOEが参照する時計の時刻をずらす。
14	環境	T.TimeStamp_TSA_Crypto_Compromise_gradually	過去に発行したタイムスタンプトークンに使用されている暗号アルゴリズムが脆弱化する。 (計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。)
15	環境	T.TimeStamp_TSA_Crypto_Compromise_immediately	過去に発行したタイムスタンプトークンに使用されている暗号アルゴリズムが脆弱化する。 (暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。)
16	TOE	T.TimeStamp_TSrequestor_Crypto_Compromise	タイムスタンプ要求者が、不注意もしくは悪意により、脆弱化したアルゴリズムを利用したタイムスタンプ要求を送信し、TOEが脆弱化したアルゴリズムを利用したタイムスタンプトークンを発行してしまう。
17	環境	T.Key_TLS_TOEuser_Compromise	許可された利用者が、不注意によりTOEの秘密鍵を暴露する。(通信用鍵)
18	環境	T.Key_Sign_TOEuser_Compromise	許可された利用者が、不注意によりTOEの秘密鍵を暴露する。(署名用鍵)
19	環境	T.Key_TLS_Cracker_Compromise	外部の不正者が、ネットワーク経由でTOEの秘密鍵を盗む。(通信用鍵)
20	環境	T.Config_TOEuser_Modify_byTOE	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。(TOEの機能を利用)
21	環境	T.Config_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEの設定情報を変更･削除･暴露する。(OSの機能を利用)
22	環境	T.Config_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定情報を変更･削除･暴露する。
23	環境	T.Config_badTST_TOEuser_Modify	許可された利用者が、不注意によりTOEの設定を変更し、不正なタイムスタンプトークンを発行する。
24	環境	T.Config_badTST_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正なタイムスタンプトークンを発行する。
25	環境	T.Config_stopTS_TOEuser_Modify	許可された利用者が、不注意によりTOEの設定を変更し、タイムスタンプトークンの発行を停止させる。
26	環境	T.Config_stopTS_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEの設定を変更し、タイムスタンプトークンの発行を停止させる。
27	環境	T.Log_TOEuser_Delete_byTOE	許可された利用者が、不注意により、TOEのログを削除･暴露する。(TOEの機能を利用) ※ログの変更は、TOEの機能を利用して実施することはできない。
28	環境	T.Log_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEのログを変更･削除･暴露する。(OSの機能を利用)
29	環境	T.Log_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEのログを変更･削除･暴露する。
30	環境	T.SW_TOEuser_Modify_byOS	許可された利用者が、不注意により、TOEのソフトウェアを変更･削除･暴露する。(OSの機能を利用)
31	環境	T.SW_Cracker_Modify	外部の不正者が、ネットワーク経由でTOEのソフトウェアを変更･削除･暴露する。
32	環境	T.Password_TOEuser_Secret_byOS	許可された利用者が、不注意により、TOEのID･パスワードを暴露する。(OSの機能を利用)
33	環境	T.Password_TOEuser_Secret_byMemo	許可された利用者が、不注意により、TOEのID･パスワードを暴露する。(口頭、メモ、メール等)
34	環境	T.Password_Cracker_Secret	外部の不正者が、ネットワーク経由でTOEのID･パスワードを暴露する。
35	環境	T.Serial_TOEuser_Modify_byHSM	許可された利用者が、不注意によりTOEが参照するシリアル番号を変更･削除する。(HSMの機能を利用)
36	環境	T.TSQ_Line	タイムスタンプ要求者-TOE間のネットワークが、事故などにより遮断され、タイムスタンプ要求者の送信したタイムスタンプ要求が、TOEに到達しない。
37	環境	T.TSR_Modify	TOEの送信したタイムスタンプ応答が、不正者もしくは事故などにより改ざんされる。
38	環境	T.TSR_Line	タイムスタンプ要求者-TOE間のネットワークが、事故などにより遮断され、TOEの送信したタイムスタンプ応答がタイムスタンプ要求者に到達しない。
39	環境	T.Virus_TOEuser	許可された利用者が、不注意により、TOEにウィルスを感染させる。
40	環境	T.Virus_Cracker	外部の不正者が、ネットワーク経由でTOEにウィルスを感染させる。
41	環境	T.Virus_TSrequestor	タイムスタンプ要求者が、ネットワーク経由でTOEにウィルスを感染させる。
42	環境	T.DoS	外部の不正者が、大量のタイムスタンプ要求を行い、TOEをサービス不能にさせる。
43	環境	T.BufferOverFlow_Attack	外部の不正者が、バッファ･オーバーフローの脆弱性を利用し、TOEの管理者権限を取得する。

44	環境	T.Hardware_Failure	・経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産が失われる。 ・経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産の完全性が保証できなくなる。 ・経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、TOEが提供するサービスが継続できない。
45	環境	T.TOE_Bug	TOEのIT実装にソフトウェア不良が存在するため、TOEの資産の信頼性が乏しくなる。 例) ・ある条件下で、ログの書き込みが行われない。 ・ある条件下で、ログファイルを破壊する。
46	環境	T.Peer_Failure	TA1(認証連鎖方式の時刻配信局)のダウンにより、TOEが提供するサービスが継続できない。
47	環境	T.Connection_Failure	TOEとTA1(認証連鎖方式の時刻配信局)の間の通信回線の故障により、TOEが提供するサービスが継続できない。

3. 組織のセキュリティポリシー

以下に、TOE を使用するにあたっての、組織のセキュリティポリシーを示す。

表 2-3　組織のセキュリティポリシー

No.	項目	説明
1	P.Cryptography	署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって実装されなければならない。
2	P.PKI_Management	安全に管理されたPKIの中で、TOEを運用すること。全ての鍵と証明書は、安全に発行、失効される。
3	P.Password_Management	TOEのパスワードは、TOE管理者およびTOE運用者によって適切に管理され、TOE管理者およびTOE運用者以外に知られてはならない。
4	P.HSM	TOEを利用する組織は、FIPS140-2 level3相当の機能を持つHSMにより、物理的に保護された署名鍵を利用した、タイムスタンプトークンやシステムログに対する暗号操作及び署名鍵のライフサイクル管理を行うこととする。
5	P.Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。
6	P.Time_Source	TOEは、信頼のできる時刻ソースを参照すること。また、時刻ソースの信頼性と正確性は、TOE所有者にとって受容可能であること。
7	P.System_Clock_Management	TOEが参照する時計を信頼のできる時刻ソースと同期させる。
8	P.Check_Virus	定期的なウィルスチェックを実行する。 外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
9	P.Check_Received_Data	TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。
10	P.Dual_Control	TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
11	P.Check_Abstract_Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

第3章 セキュリティ目標・対策と実装システムの評価

本章では、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を記載する。また、セキュリティ環境の前提と組織のセキュリティポリシーに関する実現方法例を記載する。

1. 脅威のセキュリティ目標・対策及び実装システムに対する評価

以下に、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を示す。

表 3-1　脅威のセキュリティ目標・対策及び実装システムに対する評価

No.	脅威名	セキュリティ目標･対策		統合化システムにおける実現
1	T.HSMClock_TOEuser_Modify_TimeSource	防止	･教育 (･複数人による操作(運用または機能での実現)) (･罰則)	･教育 (･複数人による操作(運用)) (･罰則)
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能:ログ管理機能
		回復	･正しいTAからの時刻配信を受ける。	･正しいTAからの時刻配信を受ける。 ※関連するTOEの機能:時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
2	T.HSMClock_Inaccuracy_gradually	防止	･TAからの時刻配信を受ける。	･TAからの時刻配信を受ける。 ※関連するTOEの機能:時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
		検出	･ログの確認 (定期的な時刻誤差の確認) ･TAが時刻監査の結果をTSAに伝える。	･ログの確認 (定期的な時刻誤差の確認) ※関連するTOEの機能:ログ管理機能 ･TAが時刻監査の結果をTSAに伝える。
		回復	ー	ー
3	T.HSMClock_Inaccuracy_immediately	防止	ー	ー
		検出	･ログの確認 (定期的な時刻誤差の確認) ･TAが時刻監査の結果をTSAに伝える。	･ログの確認 (定期的な時刻誤差の確認) ※関連するTOEの機能:ログ管理機能 ･TAが時刻監査の結果をTSAに伝える。
		回復	･TAからの時刻配信を受ける。	･TAからの時刻配信を受ける。 ※関連するTOEの機能:時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
4	T.HSMClock_TOEuser_Modify_Clock_byTOE	防止	･教育 (･複数人による操作(運用または機能での実現)) (･罰則)	･教育 (･複数人による操作(運用)) (･罰則)

		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
5	T.HSMClock_TOEuser_Modify_Clock_byHSM	防止	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作（運用）) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
6	T.HSMClock_Cracker_Modify_Clock	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
7	T.SystemClock_TOEuser_Modify_TimeSource	防止	・教育 (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 (・複数人による操作（運用）) (・罰則)
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・正しいTAからの時刻配信を受ける。	・正しいTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
8	T.SystemClock_Inaccuracy_gradually	防止	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
		検出	・ログの確認 (定期的な時刻誤差の確認) ・TAが時刻監査の結果をTSAに伝える。	・ログの確認 (定期的な時刻誤差の確認) ※関連するTOEの機能：ログ管理機能 ・TAが時刻監査の結果をTSAに伝える。
		回復	ー	ー

9	T.SystemClock_Inaccuracy_immediately	防止	ー	ー
		検出	・ログの確認 (定期的な時刻誤差の確認) ・TAが時刻監査の結果をTSAに伝える。	・ログの確認 (定期的な時刻誤差の確認) ※関連するTOEの機能：ログ管理機能 ・TAが時刻監査の結果をTSAに伝える。
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
10	T.SystemClock_TOEuser_Modify_Clock_byTOE	防止	・教育 (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 (・複数人による操作 (運用)) (・罰則)
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
11	T.SystemClock_TOEuser_Modify_Clock_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
12	T.SystemClock_TOEuser_Modify_Clock_byHSM	防止	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)

13	T.SystemClock_Cracker_Modify_Clock	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
14	T.TimeStamp_TSA_Crypto_Compromise_gradually	防止	・タイムスタンプ利用者側で、あらかじめタイムスタンプ対象データおよびタイムスタンプトークンをセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・暗号アルゴリズムが完全に危殆化する前に、タイムスタンプ利用者側で、タイムスタンプトークンやタイムスタンプ対象データに対して、安全な暗号アルゴリズムを使用したタイムスタンプを取得する。 ・タイムスタンプ利用者側で、あらかじめ異なる暗号アルゴリズムを使用したタイムスタンプを複数取得する。 ・TSAがタイムスタンプトークンを保管する。 (タイムスタンプ対象データのメッセージダイジェストに使用されるアルゴリズムの脆弱化には対応できない。)	・タイムスタンプ利用者側で、あらかじめタイムスタンプ対象データおよびタイムスタンプトークンをセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー
15	T.TimeStamp_TSA_Crypto_Compromise_immediately	防止	・タイムスタンプ利用者側で、あらかじめタイムスタンプ対象データおよびタイムスタンプトークンをセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・タイムスタンプ利用者側で、あらかじめ異なる暗号アルゴリズムを使用したタイムスタンプを複数取得する。 ・TSAがタイムスタンプトークンを保管する。 (タイムスタンプ対象データのメッセージダイジェストに使用されるアルゴリズムの脆弱化については対応できない。)	・タイムスタンプ利用者側で、あらかじめタイムスタンプ対象データおよびタイムスタンプトークンをセキュアに保管することで実現可能。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー	ー
16	T.TimeStamp_TSrequestor_Crypto_Compromise	防止	・電子政府推奨暗号リストに記載されていない暗号アルゴリズムを使用したタイムスタンプ要求は受け付けない。	・電子政府推奨暗号リストに記載されていない暗号アルゴリズムを使用したタイムスタンプ要求は受け付けない。 ※関連するTOEの機能：受諾ハッシュアルゴリズム選択機能 (タイムスタンプ要求に含まれるメッセージダイジェストのハッシュアルゴリズムが、TOEで設定した受諾ハッシュアルゴリズムと異なる場合、そのタイムスタンプ要求を拒否する。)

		検出	ー	ー
		回復	ー	ー
17	T.Key_TLS_TOEuser_Compromise	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作（運用）) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
18	T.Key_Sign_TOEuser_Compromise	防止	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作（運用）) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
19	T.Key_TLS_Cracker_Compromise	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
20	T.Config_TOEuser_Modify_byTOE	防止	・教育 (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 (・複数人による操作（運用）) (・罰則)
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
21	T.Config_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作（運用または機能での実現）) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作（運用）) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア

22	T.Config_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
23	T.Config_badTST_TOEuser_Modify	防止	・教育 ・複数人による操作（運用または機能での実現） （・罰則）	・教育 ・複数人による操作（運用） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
24	T.Config_badTST_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
25	T.Config_stopTS_TOEuser_Modify	防止	・教育 ・複数人による操作（運用または機能での実現） （・罰則）	・教育 ・複数人による操作（運用） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
26	T.Config_stopTS_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
27	T.Log_TOEuser_Delete_byTOE	防止	・教育 （・複数人による操作（運用または機能での実現）） （・罰則）	・教育 （・複数人による操作（運用）） （・罰則）
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
28	T.Log_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) （・複数人による操作（運用または機能での実現）） （・罰則）	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) （・複数人による操作（運用）） （・罰則）
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査

		回復	ー	ー
29	T.Log_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
30	T.SW_TOEuser_Modify_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
31	T.SW_Cracker_Modify	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
32	T.Password_TOEuser_Secret_byOS	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
33	T.Password_TOEuser_Secret_byMemo	防止	・教育 (・罰則)	・教育 (・罰則)
		検出	ー	ー
		回復	ー	ー
34	T.Password_Cracker_Secret	防止	・ファイアウォール	・ファイアウォール
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー

35	T.Serial_TOEuser_Modify_byHSM	防止	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・HSMの機能にアクセスするためのICカードの管理 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) (・複数人による操作 (運用)) (・罰則)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
36	T.TSQ_Line	防止	・タイムスタンプ要求者-TOE間の通信路を冗長構成とする。	・タイムスタンプ要求者-TOE間の通信路を冗長構成とすることで実現可能。
		検出	ー	ー
		回復	ー	ー
37	T.TSR_Modify	防止	・タイムスタンプ要求者-TOE間の通信路を保護する。(TLSやVPN接続など。)	・タイムスタンプ要求者-TOE間の通信路を保護する(VPN接続)ことで実現可能。
		検出	ー	ー
		回復	ー	ー
38	T.TSR_Line	防止	・タイムスタンプ要求者-TOE間の通信路を冗長構成とする。	・タイムスタンプ要求者-TOE間の通信路を冗長構成とすることで実現可能。
		検出	ー	ー
		回復	ー	ー
39	T.Virus_TOEuser	防止	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ・ウィルスチェック (・複数人による操作 (運用または機能での実現)) (・罰則)	・教育 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) ・ウィルスチェック (・複数人による操作 (運用)) (・罰則)
		検出	ー	ー
		回復	ー	ー
40	T.Virus_Cracker	防止	・ウィルスチェック	・ウィルスチェック
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
41	T.Virus_TSrequestor	防止	・ウィルスチェック	・ウィルスチェック
		検出	ー	ー
		回復	ー	ー
42	T.DoS	防止	・システムの冗長構成	・システムを冗長構成とすることで実現可能。
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
43	T.BufferOverFlow_Att	防止	・脆弱性の確認とセキュリティパッチの適用	・脆弱性の確認とセキュリティパッチの適用

	ack			
		検出	・不正アクセス監視システム ・ネットワークのアクセスログの監査	・不正アクセス監視システム ※不正アクセス監視システムを用意することで実現可能。 ・ネットワークのアクセスログの監査
		回復	ー	ー
44	T.Hardware_Failure	防止	・システムの冗長構成	・システムを冗長構成とすることで実現可能。
		検出	ー	ー
		回復	ー	ー
45	T.TOE_Bug	防止	・TOE開発者が、ソフトウェア不良を防ぐ開発プロセスを採用する。 ・TOE利用者(TOEの管理者や運用者)は、TOEの導入に際し、十分な試験を行う。	・TOE開発者が、ソフトウェア不良を防ぐ開発プロセスを採用することで実現可能。 ・TOE利用者(TOEの管理者や運用者)は、TOEの導入に際し、十分な試験を行う。
		検出	ー	ー
		回復	・TOE開発者が、パッチの作成・配布・適用を適切に実施する。また、TOE利用者(TOEの管理者や運用者)は、TOEに、TOE開発者の提供するパッチを適用する。	・TOE開発者が、パッチの作成・配布・適用を適切に実施し、TOE利用者(TOEの管理者や運用者)は、TOEに、TOE開発者の提供するパッチを適用することで実現可能。
46	T.Peer_Failure	防止	・複数の時刻配信サーバまたは複数の時刻配信局を利用する。	・複数の時刻配信サーバを用意することで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能:ログ管理機能
		回復	・TA1(認証連鎖方式の時刻配信局)復旧後の、TA1からの再接続。	・TA1(認証連鎖方式の時刻配信局)復旧後の、TA1からの再接続。
47	T.Connection_Failure	防止	・通信回線の異なる複数の時刻配信サーバまたは複数の時刻配信局を利用する。	・通信回線の異なる複数の時刻配信サーバを用意することで実現可能。
		検出	・ログの確認 (定期的な接続状態の確認)	・ログの確認 (定期的な接続状態の確認) ※関連するTOEの機能:ログ管理機能
		回復	・通信回線復旧後の、TA1(認証連鎖方式の時刻配信局)からの再接続。	・通信回線復旧後の、TA1(認証連鎖方式の時刻配信局)からの再接続。

2. 前提の実現方法例

以下に、セキュリティ環境の前提に関する実現方法例を記載する。

表 3-2　前提の実現方法例

No.	前提名	実現方法例
1	A.Location	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
2	A.TOE_Administrator	・TOE管理者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE管理者は、TOEとTOEに含まれる情報のセキュリティを維持するようにTOEを導入し、管理することを保証する。 ・TOE管理者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。

3	A.TOE_Operator	・TOE運用者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE運用者は、TOE管理者の指示の元で、TOEとTOEに含まれる情報のセキュリティを維持するようにTOEを管理・運用することを保証する。 ・TOE運用者は、TOEを運用する組織の規定・運用マニュアルに従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
4	A.TOE_Auditor	・TOE監査者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。 ・TOE監査者は、TOEを運用する組織の規定に従って業務を行う。 ・TOEを運用する組織の管理者は、TOEの運用を妨害するような、特殊な機器を持ち込んだ攻撃や、サーバマシンへの攻撃などの悪質な攻撃が行われないよう、TOEを運用する組織に属するものを適切に管理する。
5	A.TS_Requestor	・タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証及び保持する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TSA証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当なTSAによって行われたものかどうかの確認、が含まれる。 ・タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証するためのソフトウェアを持つ。また、タイムスタンプトークンを保管するためのストレージを持つ。
6	A.TOE_Separation	・TOE管理者は、TOE 及びTOE のIT環境の取扱説明書を熟読した上で、取扱説明書が定める手順に従って、TOE 及びTOE のIT 環境を構築する。この際、TOEが動作するサーバマシンには、TOE の動作に関係ないソフトウェアはインストールしない。
7	A.Device	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
8	A.FIREWALL	・プライベートネットワークと外部ネットワークを結ぶネットワークには、ファイアウォールを設置する。 ・ファイアウォールの設定は、適切に維持・管理される。
9	A.PEER	・タイムスタンプ利用者（タイムスタンプ要求者）を除くTOEと通信する意図された他システムは、信頼できる第三者(TTP)の運用するシステムであることを保証する。
10	A.Abstract	・TOE 管理者は、TOE が動作するために必要なOSや依存するライブラリが不正な改変から保護され、正しく動作するよう適切に管理する。 ・TOE 管理者は、TOE が動作するサーバマシンに、TOE の動作を干渉するようなソフトウェアがインストールされないように、適切に管理する。 ・TOE 管理者は、TOE 及びTOE のIT 環境が正常な動作を維持するように、適切に管理する。
11	A.TSA2_TA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、専用線である。
12	A.Environment	・TOE の設置場所として、電磁波対策、電力対策、温度・湿度対策が行われている設備を利用する。
13	A.MEDIA	・定期的なデータのバックアップと、適切なシステムマイグレーションを行う。

3. 組織のセキュリティポリシーの実現方法例

以下に、組織のセキュリティポリシーに関する実現方法例を記載する。

表 3-3　組織のセキュリティポリシーの実現方法例

No.	ポリシー名	実現方法例
1	P.Cryptography	・TOEの署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって行われる。

2	P.PKI_Management	TOEは、安全に管理されたPKIの中で運用されることを保証する。鍵/証明書は、運用マニュアルに基づき、安全に発行･失効される。
3	P.Password_Management	･TOE管理者およびTOE運用者は、パスワードを記憶し、他人に漏らさない。また、運用マニュアルに基づき、適切なパスワードを設定し、適切な頻度でパスワードを変更する。 ･TOE管理者およびTOE運用者は、ソーシャルエンジニアリングの教育を受けている。
4	P.HSM	TOEを利用する組織は、FIPS140-2 level3相当の機能を持つHSMにより、物理的に保護された署名鍵を利用した、タイムスタンプトークンやシステムログに対する暗号操作及び署名鍵のライフサイクル管理を行うことを保証する。
5	P.Protect_Log	･TOE を利用する組織は、TOEの監査ログの暴露･改ざんまたは削除を防止するよう、TOE管理者、TOE運用者、TOE監査者に対して教育を行う。 ･TOEは、TOEの出力するシステムログにハッシュ値やデジタル署名を付与し、改ざんを検出可能な機能を持つ。 ･TOEは、TOEの保護対象資産へのアクセスを許可する前に、全ての利用者に対して識別･認証情報の入力を要求し、識別･認証を実施する。
6	P.Time_Source	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
7	P.System_Clock_Management	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
8	P.Check_Virus	TOE管理者は、運用マニュアルに基づき、定期的にTOEの全ファイルに対してウィルスチェックを行う。また、外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
9	P.Check_Received_Data	TOEは、TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
10	P.Dual_Control	運用マニュアルに基づき、TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行う。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行う。
11	P.Check_Abstract_Vulnerability	TOE管理者は、運用マニュアルに基づき、定期的にOS やライブラリなどの脆弱性を確認し、対策を行う。

第4章 脅威ツリー及びリスク評価一覧

本章では、内部不正のないセキュリティ評価における脅威ツリー、リスク評価格付けの考え方、リスク評価点を記述する。

1. 脅威ツリー

以下に、脅威ツリーを示す。
※欄の不足を補うため、一部「下位の条件→上位の条件」と矢印で表現している場合がある。

表 4-1　脅威ツリー

No.	資産	脅威	上位レベルが実現するための条件			脅威名
			条件1	条件2	条件3	
1	HSM時刻	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。	許可された利用者が、不注意により、TOEの設定情報を変更する。	—	—	T.HSMClock_TOEuser_Modify_TimeSource
2	HSM時刻	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。	TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。	—	—	T.HSMClock_Inaccuracy_gradually
3	HSM時刻		TOEが参照する時計が故障し、急に時刻がずれる。	—	—	T.HSMClock_Inaccuracy_immediately
4	HSM時刻		時刻ソースが不正な時刻を配信し、これをもとにTOEが時刻を補正することで、時刻がずれる。	※前提A.PEERとして、時刻ソースは信頼できるので脅威から除外。	—	—
5	HSM時刻	許可された利用者が、不注意により、または外部の不正者が、TOEが参照する時計の時刻をずらす。	許可された利用者が、不注意によりTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	—	T.HSMClock_TOEuser_Modify_Clock_byTOE
6	HSM時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	※OSの機能からHSM時刻を設定することはできないので脅威から除外。	—
7	HSM時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	—

8	HSM時刻			HSMの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。）	物理的にHSMにアクセス→HSMの機能へのアクセス(管理者用ICカードが必要)	T.HSMClock_TOEuser_Modify_Clock_byHSM
9	HSM時刻		外部の不正者が、ネットワーク経由でTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	T.HSMClock_Cracker_Modify_Clock
10	HSM時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	※OSの機能からHSM時刻を設定することはできないので脅威から除外。	―
11	HSM時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	同上 (T.HSMClock_Cracker_Modify_Clock)
12	HSM時刻			HSMの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。）	TOEにネットワーク経由でアクセスする。 かつ、物理的にHSMにアクセスする。 →HSMの機能へのアクセス(管理者用ICカードが必要) ※前提A.Locationとして、権限のないユーザは物理的にHSMにアクセスできないので脅威から除外。	―
13	HSM時刻		外部の不正者が、物理的に侵入し、TOEの時刻を設定する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―
14	HSM時刻	外部の不正者が、時刻ソースに成りすまして、TOEに時刻を配信する。	TOEにネットワーク経由でアクセスする。	※前提A.TSA2_TA1_Connectionとして、TA1-TOE間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―
15	HSM時刻	外部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	※前提A.TSA2_TA1_Connectionとして、TA1-TOE間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	―	―
16	システム時刻	許可された利用者が、不注意により、TOEが参照する時刻ソースを変更する。	許可された利用者が、不注意により、TOEの設定情報を変更する。	―	―	T.SystemClock_TOEuser_Modify_TimeSource

17	システム時刻	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。	TOEの周囲の温度変化等により、時間が経過するにつれて、TOEが参照する時計が、UTCに対して徐々にずれていく。	―	―	T.SystemClock_Inaccuracy_gradually
18	システム時刻		TOEが参照する時計が故障し、急に時刻がずれる。	ー	―	T.SystemClock_Inaccuracy_immediately
19	システム時刻		時刻ソースが不正な時刻を配信し、これをもとにTOEが時刻を補正することで、時刻がずれる。	※前提A.PEERとして、時刻ソースは信頼できるので脅威から除外。	―	―
20	システム時刻	許可された利用者が、不注意により、または外部の不正者が、TOEが参照する時計の時刻をずらす。	許可された利用者が、不注意によりTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	―	T.SystemClock_TOEuser_Modify_Clock_byTOE
21	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	OSにログインする	T.SystemClock_TOEuser_Modify_Clock_byOS
22	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―
23	システム時刻			HSMの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。）	物理的にHSMにアクセス →HSMの機能へのアクセス(管理者用ICカードが必要)	T.SystemClock_TOEuser_Modify_Clock_byHSM
24	システム時刻		外部の不正者が、ネットワーク経由でTOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	T.SystemClock_Cracker_Modify_Clock
25	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	同上
26	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。	同上

27	システム時刻			HSMの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。）	TOEにネットワーク経由でアクセスする。 かつ、物理的にHSMにアクセスする。 →HSMの機能へのアクセス(管理者用ICカードが必要) ※前提A.Locationとして、権限のないユーザは物理的にHSMにアクセスできないので脅威から除外。	—
28	システム時刻		外部の不正者が、物理的に侵入し、TOEの時刻を設定する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—
29	システム時刻	外部の不正者が、時刻ソースに成りすまして、TOEに時刻を配信する。	TOEにネットワーク経由でアクセスする。	※前提A.TSA2_TA1_Connectionとして、TA1-TOE間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	—	—
30	システム時刻	外部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	※前提A.TSA2_TA1_Connectionとして、TA1-TOE間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止しているので脅威から除外。	—	ー
31	タイムスタンプトークン	過去に発行したタイムスタンプトークンに使用されている暗号アルゴリズムが脆弱化する。	暗号アルゴリズムの攻撃方法が発見され、暗号アルゴリズムが脆弱化する。	計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。	—	T.TimeStamp_TSA_Crypto_Compromise_gradually
32	タイムスタンプトークン			暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。	—	T.TimeStamp_TSA_Crypto_Compromise_immediately
33	タイムスタンプトークン	タイムスタンプ要求者が、不注意もしくは悪意により、脆弱化したアルゴリズムを利用したタイムスタンプ要求を送信し、TOEが脆弱化したアルゴリズムを利用したタイムスタンプトークンを発行してしまう。	TOEにネットワーク経由でアクセスする。	タイムスタンプ要求者が、脆弱化したアルゴリズムを利用したメッセージダイジェストを含むタイムスタンプ要求を送信する。	—	T.TimeStamp_TSrequestor_Crypto_Compromise
34	秘密鍵	TOEの秘密鍵が脆弱化する。	許可された利用者が、不注意によりTOEの秘密鍵を暴露する。	[通信用鍵] OSの機能を用いてTOEの秘密鍵を取得する。	OSにログインする	T.Key_TLS_TOEuser_Compromise
35	秘密鍵			[署名用鍵] 物理的にTOEにアクセス →HSMを持ち出す。	OSにログインする →OSの機能を用いてTOEの鍵データを取得する。	T.Key_Sign_TOEuser_Compromise

36	秘密鍵		外部の不正者が、ネットワーク経由でTOEの秘密鍵を盗む。	[通信用鍵] TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Key_TLS_Cracker_Compromise
37	秘密鍵			[署名用鍵] 物理的にTOEにアクセス →HSMを持ち出す。 ※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	TOEにネットワーク経由でアクセスする。 →TOEの管理者権限を得る。 →OSにログインする →OSの機能を用いてTOEの鍵データを取得する。	―
38	秘密鍵		外部の不正者が、物理的に侵入し、TOEの秘密鍵を盗む。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―
39	設定情報	許可された利用者が、不注意により、TOEの設定情報を変更・削除・暴露する。	TOEの機能を用いてTOEの設定情報を変更・削除・暴露する。	―	―	T.Config_TOEuser_Modify_byTOE
40	設定情報		OSの機能を用いてTOEの設定情報を変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	―	T.Config_TOEuser_Modify_byOS
41	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
42	設定情報	外部の不正者が、ネットワーク経由でTOEの設定情報を変更・削除・暴露する。	TOEの機能を用いてTOEの設定情報を変更・削除・暴露する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_Cracker_Modify
43	設定情報		OSの機能を用いてTOEの設定情報を変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上

44	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更・削除・暴露する。） ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
45	設定情報	外部の不正者が、物理的に侵入し、TOEの設定情報を変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
46	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、不正なタイムスタンプトークンを発行する。	TOEの設定情報を変更する。 ※[不正なタイムスタンプトークンの例] 本来のポリシ(OID,accuracy,ordering等)と異なるタイムスタンプトークンなど。	TOEにアクセスする。	—	T.Config_badTST_TOEuser_Modify
47	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、不正なタイムスタンプトークンを発行する。	TOEの設定情報を変更する。 ※[不正なタイムスタンプトークンの例] 本来のポリシ(OID,accuracy,ordering等)と異なるタイムスタンプトークンなど。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_badTST_Cracker_Modify
48	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、不正なタイムスタンプトークンを発行する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
49	設定情報	許可された利用者が、不注意によりTOEの設定を変更し、タイムスタンプトークンの発行を停止させる。	TOEの設定情報を変更する。	TOEにアクセスする。	—	T.Config_stopTS_TOEuser_Modify
50	設定情報	外部の不正者が、ネットワーク経由でTOEの設定を変更し、タイムスタンプトークンの発行を停止させる。	TOEの設定情報を変更する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Config_stopTS_Cracker_Modify
51	設定情報	外部の不正者が、物理的に侵入してTOEの設定を変更し、タイムスタンプトークンの発行を停止させる。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—

52	ログ	許可された利用者が、不注意により、TOEのログを変更・削除・暴露する。	TOEの機能を用いてTOEのログを削除・暴露する。 ※ログの変更は、TOEの機能を利用して実施することはできない。	―	―	T.Log_TOEuser_Delete_byTOE
53	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例:設定ファイルを直接編集する。	OSにログインする	―	T.Log_TOEuser_Modify_byOS
54	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例:悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
55	ログ	外部の不正者が、ネットワーク経由でTOEのログを変更・削除・暴露する。	TOEの機能を用いてTOEのログを削除・暴露する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Log_Cracker_Modify
56	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例:設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
57	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 (TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。) ※例:悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
58	ログ	外部の不正者が、物理的に侵入し、TOEのログを変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
59	ソフトウェア	許可された利用者が、不注意により、TOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例:OSのコマンドを利用して削除する。	OSにログインする	―	T.SW_TOEuser_Modify_byOS

60	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
61	ソフトウェア	外部の不正者が、ネットワーク経由でTOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：設定ファイルを直接編集する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.SW_Cracker_Modify
62	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
63	ソフトウェア	外部の不正者が、物理的に侵入し、TOEのソフトウェアを変更・削除・暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―
64	ID・パスワード	許可された利用者が、不注意により、TOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	OSにログインする	―	T.Password_TOEuser_Secret_byOS
65	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	―	―
66	ID・パスワード		その他、口頭、メモ、メール等で情報が漏洩する。	―	―	T.Password_TOEuser_Secret_byMemo
67	ID・パスワード	外部の不正者が、ネットワーク経由でTOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Password_Cracker_Secret
68	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	同上
69	ID・パスワード	外部の不正者が、物理的に侵入し、TOEのID・パスワードを暴露する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	―	―	―

70	シリアル番号	許可された利用者が、不注意により、TOEが参照するシリアル番号を変更・削除する。	許可された利用者が、不注意によりシリアル番号を変更・削除する。	外部から持ち込んだソフトウェアを用いてTOEの参照するシリアル番号を変更・削除する。 （TOEの機能以外の方法を用いてTOEの参照するシリアル番号を変更・削除する。） ※例：悪意のソフトウェア	※前提A.TOE_Separationとして、TOEに必要でないソフトウェアはインストールされないので脅威から除外。	—
71	シリアル番号			HSMの機能を用いてTOEの参照するシリアル番号を変更・削除する。 （TOEの機能以外の方法を用いてTOEの参照するシリアル番号を変更・削除する。）	物理的にHSMにアクセス →HSMの機能へのアクセス(管理者用ICカードが必要) →HSMに保管されるシリアル番号を不正な値にセットする。	T.Serial_TOEuser_Modify_byHSM
72	シリアル番号	外部の不正者が、ネットワーク経由でTOEの参照するシリアル番号を変更・削除する。	外部から持ち込んだソフトウェアを用いてTOEのシリアル番号を設定する。 （TOEの機能以外の方法を用いてTOEの参照するシリアル番号を変更・削除する。） ※例：悪意のソフトウェア	TOEにネットワーク経由でアクセスする。 かつ、物理的にHSMにアクセスする。 →HSMの機能へのアクセス(管理者用ICカードが必要)	※前提A.Locationとして、権限のないユーザは物理的にHSMにアクセスできないので脅威から除外。	—
73	シリアル番号	外部の不正者が、物理的に侵入し、TOEの参照するシリアル番号を変更・削除する。	※前提A.Locationとして、権限のないユーザは物理的にTOEにアクセスできないので脅威から除外。	—	—	—
74	タイムスタンプ要求	タイムスタンプ要求者の送信したタイムスタンプ要求が、不正者もしくは事故などにより改ざんされる。	タイムスタンプ要求を改ざんし、TOEに送付する。	タイムスタンプ要求者-TOE間のネットワークにアクセスする。 →ネットワーク中のパケットから、タイムスタンプ要求者の送付したタイムスタンプ要求を取得する。	※前提A.TS_Requestorより、タイムスタンプユーザ(タイムスタンプ要求者)はタイムスタンプトークンを検証するので、脅威とはならない。	—
75	タイムスタンプ要求	タイムスタンプ要求者の送信したタイムスタンプ要求が、不正者もしくは事故などにより暴露される。	ネットワーク中のパケットから、タイムスタンプ要求者の送付したタイムスタンプ要求を取得する。	タイムスタンプ要求者-TOE間のネットワークにアクセスする。	※タイムスタンプ要求の内容は、暴露されても問題のない内容であるため、脅威とはならない。	—
76	タイムスタンプ要求	タイムスタンプ要求者の送信したタイムスタンプ要求が、事故などによりTOEに到達しない。	タイムスタンプ要求者-TOE間のネットワークが、事故などにより遮断される。	タイムスタンプ要求者-TOE間のネットワークにアクセスする。	—	T.TSQ_Line
77	タイムスタンプ応答	TOEの送信したタイムスタンプ応答が、不正者もしくは事故などにより改ざんされる。	タイムスタンプ応答を改ざんし、タイムスタンプ要求者に送付する。	タイムスタンプ要求者-TOE間のネットワークにアクセスする。 →ネットワーク中のパケットから、TOEの送付したタイムスタンプ応答を取得する。	—	T.TSR_Modify

78	タイムスタンプ応答	TOEの送信したタイムスタンプ応答が、不正者もしくは事故などにより暴露される。	ネットワーク中のパケットから、TOEの送付したタイムスタンプ応答を取得する。	タイムスタンプ要求者-TOE間のネットワークにアクセスする。	※タイムスタンプ応答の内容は、暴露されても問題のない内容であるため、脅威とはならない。	—
79	タイムスタンプ応答	TOEの送信したタイムスタンプ応答が、事故などによりタイムスタンプ要求者に到達しない。	タイムスタンプ要求者-TOE間のネットワークが、事故などにより遮断される。	—	—	T.TSR_Line
80	その他	許可された利用者が、不注意により、TOEにウィルスを感染させる。	ウィルスに感染した外部メディアにアクセスする。	OSにログインする	ウィルスに感染した外部メディアを持ち込む。	T.Virus_TOEuser
81	その他		外部からウィルスをダウンロードする。	外部にアクセスする。	OSにログインする	同上
82	その他	外部の不正者が、ネットワーク経由でTOEにウィルスを感染させる。	TOEにウィルスをダウンロードさせる。	TOEの管理者権限を得る。	TOEにネットワーク経由でアクセスする。	T.Virus_Cracker
83	その他	タイムスタンプ要求者が、ネットワーク経由でTOEにウィルスを感染させる。	TOEに、ウィルスに感染したデータを送る。	—	—	T.Virus_TSrequestor
84	その他	外部の不正者が、大量のタイムスタンプ要求を行い、TOEをサービス不能にさせる。	ネットワーク経由でTOEに大量のタイムスタンプ要求を行う。	ー	ー	T.DoS
85	その他	外部の不正者が、バッファ･オーバーフローの脆弱性を利用し、TOEの管理者権限を取得する。	TOEにネットワーク経由でアクセスする。	ー	ー	T.BufferOverFlow_Attack
86	その他	TOEのハードウェア故障	経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産が失われる。	—	—	T.Hardware_Failure
87	その他		経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、資産の完全性が保証できなくなる。	—	—	同上
88	その他		経年劣化や偶然に引き起こされる障害により、TOEのハードウェアが故障し、TOEが提供するサービスが継続できない。	—	—	同上
89	その他	TOEのソフトウェアのバグ	TOEのIT実装にソフトウェア不良が存在するため、TOEの資産の信頼性が乏しくなる。 例) ･ある条件下で、ログの書き込みが行われない。 ･ある条件下で、ログファイルを破壊する。	TOEの開発時に、ソフトウェア不良を発見できない。	—	T.TOE_Bug

90	その他	通信相手となる他システムのダウン	通信相手となる他システムのダウンにより、TOEの資産が失われる。	※特に失われる資産はないため、脅威から除外。	—	—
91	その他		TA1(認証連鎖方式の時刻配信局)のダウンにより、TOEが提供するサービスが継続できない。	—	—	T.Peer_Failure
92	その他	TOEと通信相手となる他システム間の通信回線の故障	TOEと通信相手となる他システムの間の通信回線の故障により、TOEの資産が失われる。	※特に失われる資産はないため、脅威から除外。	—	—
93	その他		TA1(認証連鎖方式の時刻配信局)との間の通信回線の故障により、TOEが提供するサービスが継続できない。	—	—	T.Connection_Failure

2. リスク評価格付けの考え方

以下に、リスク評価格付けの考え方を示す。

表 4-2　リスク評価格付けの考え方

	格付け	高(3)	中(2)	低(1)
D	潜在的損失（Damage potential）	<方針> ・信頼性・サービスレベルに影響のあるもの。 ・データを直接悪用できるもの。 ＜対象＞ その他	<方針> ・データを直接は悪用できないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
R	再現性（Reproducibility）	＜方針＞ ・時期によらないもの。 ・内部不正など、攻撃者の意図でいつでも実施できるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ＜対象＞ ・内部不正 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・その他	＜方針＞ ・攻撃者の意図によらないもの。 ・TOE開発時のソフトウェア不良 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ＜対象＞ ・不注意（基本的に発生率は低い、という前提。） ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。) ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断（基本的に発生率は低い、という前提。）	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・暗号脆弱化 ・パケットの暴露・改ざん ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化

E	攻撃利用可能性（Exploitability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃できるもの。 ・攻撃方法が容易なもの。 ・比較的攻撃ツールが入手しやすいと思われるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他	＜方針＞ なし ＜対象＞ なし	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん
A	影響ユーザ（Affected users）	<方針> ・TOEのサービスの利用者に関わるもの。 ・TOE利用者自身に大きな影響があるもの。 ＜対象＞ ・その他	<方針> ・TOEのサービスの利用者に対する直接的な影響がないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
D	発見可能性（Discoverability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃方法を知る事ができるもの。 ・攻撃方法が容易に思いつくもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退	＜方針＞ ・TOE開発時のソフトウェア不良 ＜対象＞ ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

		・他システムの秘密鍵危殆化 ・その他		

3. リスク評価点

以下に、脅威に対するリスク評価点を示す。

表 4-3　リスク評価点

No.	名称	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.HSMClock_TOEuser_Modify_TimeSource	3	2	3	3	3	14
2	T.HSMClock_Inaccuracy_gradually	3	3	3	3	3	15
3	T.HSMClock_Inaccuracy_immediately	3	3	3	3	3	15
4	T.HSMClock_TOEuser_Modify_Clock_byTOE	3	2	3	3	3	14
5	T.HSMClock_TOEuser_Modify_Clock_byHSM	3	2	3	3	3	14
6	T.HSMClock_Cracker_Modify_Clock	3	3	3	3	3	15
7	T.SystemClock_TOEuser_Modify_TimeSource	2	2	3	2	3	12
8	T.SystemClock_Inaccuracy_gradually	2	3	3	2	3	13
9	T.SystemClock_Inaccuracy_immediately	2	3	3	2	3	13
10	T.SystemClock_TOEuser_Modify_Clock_byTOE	2	2	3	2	3	12
11	T.SystemClock_TOEuser_Modify_Clock_byOS	2	2	3	2	3	12
12	T.SystemClock_TOEuser_Modify_Clock_byHSM	2	2	3	2	3	12
13	T.SystemClock_Cracker_Modify_Clock	2	3	3	2	3	13
14	T.TimeStamp_TSA_Crypto_Compromise_gradually	3	1	1	3	1	9
15	T.TimeStamp_TSA_Crypto_Compromise_immediately	3	1	1	3	1	9
16	T.TimeStamp_TSrequestor_Crypto_Compromise	3	3	3	3	3	15
17	T.Key_TLS_TOEuser_Compromise	3	2	3	3	3	14
18	T.Key_Sign_TOEuser_Compromise	3	2	3	3	3	14
19	T.Key_TLS_Cracker_Compromise	3	3	3	3	3	15
20	T.Config_TOEuser_Modify_byTOE	3	3	3	3	3	15
21	T.Config_TOEuser_Modify_byOS	3	3	3	3	3	15
22	T.Config_Cracker_Modify	3	3	3	3	3	15
23	T.Config_badTST_TOEuser_Modify	3	2	3	3	3	14
24	T.Config_badTST_Cracker_Modify	3	3	3	3	3	15
25	T.Config_stopTS_TOEuser_Modify	3	2	3	3	3	14
26	T.Config_stopTS_Cracker_Modify	3	3	3	3	3	15
27	T.Log_TOEuser_Delete_byTOE	2	2	3	2	3	12
28	T.Log_TOEuser_Modify_byOS	2	2	3	2	3	12
29	T.Log_Cracker_Modify	2	3	3	2	3	13
30	T.SW_TOEuser_Modify_byOS	3	2	3	3	3	14
31	T.SW_Cracker_Modify	3	2	3	3	3	14
32	T.Password_TOEuser_Secret_byOS	3	2	3	3	3	14
33	T.Password_TOEuser_Secret_byMemo	3	2	3	3	3	14

34	T.Password_Cracker_Secret	3	3	3	3	3	15
35	T.Serial_TOEuser_Modify_byHSM	3	2	3	3	3	14
36	T.TSQ_Line	3	2	3	3	3	14
37	T.TSR_Modify	3	1	1	3	1	9
38	T.TSR_Line	3	2	3	3	3	14
39	T.Virus_TOEuser	3	3	3	3	3	15
40	T.Virus_Cracker	3	3	3	3	3	15
41	T.Virus_TSrequestor	3	3	3	3	3	15
42	T.DoS	3	3	3	3	3	15
43	T.BufferOverFlow_Attack	3	3	3	3	3	15
44	T.Hardware_Failure	3	2	3	3	3	14
45	T.TOE_Bug	3	2	3	3	2	13
46	T.Peer_Failure	3	2	3	3	3	14
47	T.Connection_Failure	3	2	3	3	3	14

第5章 内部不正を考慮したセキュリティ評価

本章では、内部不正の考え方及び内部不正を考慮したセキュリティ環境を記載する。また、脅威に関する対策を記載する。

1. 内部不正の考え方

内部不正を考慮したセキュリティ評価として、内部不正のモデルを以下のように位置づける。

- 内部不正の範囲
  内部不正として、内部者の単独による不正を考慮する。
  下記のケースについては除外する。
  -外部者との結託
  -内部者の結託
  -内部者の単独による不正が同時に発生するケース

- セキュリティ環境
  内部不正を考慮しないセキュリティ環境を、内部不正を考慮した場合のセキュリティ環境にカスタマイズする。

2. 内部不正を考慮したセキュリティ環境

2-1 前提

以下に、TOE を使用する際のセキュリティ環境の前提を示す。

表 5-1　前提

No.	分類	項目	説明
1	物理的な前提	A.Location	TOE（及び関連するコンポーネント）は、コントロールされたアクセス・ファシリティの中に設置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2	人的な前提	A.TOE_Administrator	一人以上の許可された管理者が割り当てられる。彼らは、TOEとTOEに含まれる情報のセキュリティを管理する資格を持つ。評価対象の設定において、TOEを安全に導入、管理する。 ・TOEに関わるユーザ/役割を管理する。 ・時刻・シリアル番号に関する管理業務を行う。 ・暗号機能に関わる初期化及び管理業務を行う。 ・TOE上で悪意のあるソフトウェアが動作しないようにする。 ・TOEの用件を満たす適切なディスクスペースを用意する。 ・TOEのデータベースを適切に管理する。 彼らは、単独による内部不正を行う可能性があるものとする。

3	人的な前提	A.TOE_Operator	一人以上の許可された運用者が割り当てられる。 ・TOEの起動・停止を実行する。 ・TOE管理者の指示の元で各種設定など運用業務を行う。 彼らは、単独による内部不正を行う可能性があるものとする。
4	人的な前提	A.TOE_Auditor	一人以上の許可された監査者が割り当てられる。 ・TOEが生成する監査データの分析等の監査業務を行う。 彼らは、単独による内部不正を行う可能性があるものとする。
5	人的な前提	A.TS_Requestor	タイムスタンプユーザ（タイムスタンプ要求者）は、タイムスタンプトークンを検証及び保持する。この中には、アウト・オブ・バンドの方法を用いて、TSA証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当なTSAによって行われたものかどうかの確認、が含まれる。
6	接続に関する前提	A.Device	周辺機器への接続は、コントロールされたアクセス・ファシリティ内に存在する。
7	接続に関する前提	A.FIREWALL	ファイアウォールは、プライベートネットワークと外部ネットワークを結ぶ唯一のネットワーク接続である。
8	接続に関する前提	A.PEER	タイムスタンプユーザ（タイムスタンプ要求者）を除くTOEと通信する意図された他システムは、信頼できる。
9	接続に関する前提	A.TSA2_TA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、TA1やTOEの成りすまし、データの改ざん、データの盗聴を防止する。 ただし、内部不正によるTOEの成りすまし、データの改ざん、データの盗聴の可能性があるものとする。
10	物理的な前提	A.Environment	TOE の設置場所は、電磁波対策、電力対策、温度・湿度対策が行われている。
11	物理的な前提	A.MEDIA	ストレージメディアの経年劣化や不良の対策が行われ、データ損失と破壊はないものとする。

2-2 脅威

以下に、TOE および環境に対する脅威を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

なお、脅威の分類は以下のように区分した。

・分類：TOE

TOE のセキュリティ機能（例：時刻配信プロトコルなど）により対策可能。

・分類：環境

TOE のセキュリティ機能では対策不可能、環境の IT/非 IT 機能（例：外部の IDS システムにより対策、運用により対策）により対策可能。

※TOE のログ管理機能、TOE 管理機能を利用して対策する脅威は、こちらの区分に含めている。

表 5-2 脅威

No.	分類	項目	説明
1	TOE	T.HSMClock_TOEuser_Modify_TimeSource_Malice	内部の不正者が、TOEが参照する時刻ソースを変更する。
2	TOE	T.HSMClock_Inaccuracy_TOEuser_Crash_Malice	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が内部の不正者の攻撃により機能低下（故障）し、時刻がずれる。)

3	TOE	T.HSMClock_TOEuser_Modify_Clock_byTOE_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
4	TOE	T.HSMClock_TOEuser_Modify_Clock_byImportSW_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(外部から持ち込んだソフトウェアを利用)
5	TOE	T.HSMClock_TOEuser_Modify_Clock_byHSM_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(HSMの機能を利用)
6	TOE	T.HSMClock_TOEuser_Imperson_Server_Malice	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。
7	TOE	T.HSMClock_TOEuser_Modify_Data_Line_Malice	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。
8	TOE	T.SystemClock_TOEuser_Modify_TimeSource_Malice	内部の不正者が、TOEが参照する時刻ソースを変更する。
9	TOE	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice	TOEが参照する時計の時刻と協定世界時(UTC)の時刻差が、TOE管理者の受容範囲を超える。(TOEが参照する時計が内部の不正者の攻撃により機能低下（故障）し、時刻がずれる。)
10	TOE	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(TOEの機能を利用)
11	TOE	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(OSの機能を利用)
12	TOE	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(外部から持ち込んだソフトウェアを利用)
13	TOE	T.SystemClock_TOEuser_Modify_Clock_byHSM_Malice	内部の不正者が、TOEが参照する時計の時刻をずらす。(HSMの機能を利用)
14	TOE	T.SystemClock_TOEuser_Imperson_Server_Malice	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。
15	TOE	T.SystemClock_TOEuser_Modify_Data_Line_Malice	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。
16	環境	T.Key_TLS_TOEuser_Compromise_Malice	内部の不正者がTOEの秘密鍵を暴露する。（通信用鍵）
17	環境	T.Key_Sign_TOEuser_Compromise_Malice	内部の不正者がTOEの秘密鍵を暴露する。（署名用鍵）
18	環境	T.Config_TOEuser_Modify_byTOE_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(TOEの機能を利用)
19	環境	T.Config_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(OSの機能を利用)
20	環境	T.Config_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEの設定情報を変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
21	環境	T.Config_badTST_TOEuser_Modify_Malice	内部の不正者が、TOEの設定を変更し、不正なタイムスタンプトークンを発行する。
22	環境	T.Config_stopTS_TOEuser_Modify_Malice	内部の不正者が、TOEの設定を変更し、タイムスタンプトークンの発行を停止させる。
23	環境	T.Log_TOEuser_Delete_byTOE_Malice	内部の不正者が、TOEのログを削除･暴露する。(TOEの機能を利用) ※ログの変更は、TOEの機能を利用して実施することはできない。
24	環境	T.Log_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEのログを変更･削除･暴露する。(OSの機能を利用)

25	環境	T.Log_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEのログを変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
26	環境	T.SW_TOEuser_Modify_byOS_Malice	内部の不正者が、TOEのソフトウェアを変更･削除･暴露する。(OSの機能を利用)
27	環境	T.SW_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEのソフトウェアを変更･削除･暴露する。(外部から持ち込んだソフトウェアを利用)
28	環境	T.Password_TOEuser_Secret_byOS_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(OSの機能を利用)
29	環境	T.Password_TOEuser_Secret_byImportSW_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(外部から持ち込んだソフトウェアを利用)
30	環境	T.Password_TOEuser_Secret_byMemo_Malice	内部の不正者が、TOEのID･パスワードを暴露する。(口頭、メモ、メール等)
31	環境	T.Serial_TOEuser_Modify_byImportSW_Malice	内部の不正者が、TOEが参照するシリアル番号を変更･削除する。(外部から持ち込んだソフトウェアを利用)
32	環境	T.Serial_TOEuser_Modify_byHSM_Malice	内部の不正者が、TOEが参照するシリアル番号を変更･削除する。(HSMの機能を利用)
33	環境	T.Virus_TOEuser_Malice	内部の不正者が、TOEにウィルスを感染させる。
34	環境	T.Crash_TOEuser_Malice	内部の不正者が、TOEを破壊し、サービスを停止させる。

2-3 組織のセキュリティポリシー

以下に、TOE を使用するにあたっての、組織のセキュリティポリシーを示す。

表 5-3　組織のセキュリティポリシー

No.	項目	説明
1	P.Cryptography	署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって実装されなければならない。
2	P.PKI_Management	安全に管理されたPKIの中で、TOEを運用すること。全ての鍵と証明書は、安全に発行、失効される。
3	P.Password_Management	TOEのパスワードは、TOE管理者およびTOE運用者によって適切に管理され、TOE管理者およびTOE運用者以外に知られてはならない。
4	P.HSM	TOEを利用する組織は、FIPS140-2 level3相当の機能を持つHSMにより、物理的に保護された署名鍵を利用した、タイムスタンプトークンやシステムログに対する暗号操作及び署名鍵のライフサイクル管理を行うこととする。
5	P.Protect_Log	TOE を利用する組織は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。
6	P.Time_Source	TOEは、信頼のできる時刻ソースを参照すること。また、時刻ソースの信頼性と正確性は、TOE所有者にとって受容可能であること。
7	P.System_Clock_Management	TOEが参照する時計を信頼のできる時刻ソースと同期させる。
8	P.Check_Virus	定期的なウィルスチェックを実行する。 外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
9	P.Check_Received_Data	TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する。

10	P.Dual_Control	TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行うこととする。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。
11	P.Check_Abstract_ Vulnerability	定期的に、OS やライブラリなどの脆弱性を確認し、対策を行う。

3. セキュリティ目標・対策と実装システムの評価
3-1 脅威のセキュリティ目標・対策及び実装システムに対する評価

以下に、セキュリティ環境の脅威のセキュリティ目標・対策及び実装システムに対する評価を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

表 5-4　脅威のセキュリティ目標・対策及び実装システムに対する評価

No.	脅威名	セキュリティ目標･対策		統合化システムにおける実現
1	T.HSMClock_TOEuser_Modify_TimeSource_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	･正しいTAからの時刻配信を受ける。	･正しいTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 （-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。）
2	T.HSMClock_Inaccuracy_TOEuser_Crash_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	･TAからの時刻配信を受ける。	･TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 （-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。）
3	T.HSMClock_TOEuser_Modify_Clock_byTOE_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則	･複数人による操作（運用） ･罰則
		検出	･ログ/運用記録の監査	･運用記録の作成 ･ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	･TAからの時刻配信を受ける。	･TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 （-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。）
4	T.HSMClock_TOEuser_Modify_Clock_byImportSW_Malice	防止	･複数人による操作（運用または機能での実現） ･罰則 ･運用管理(操作は、管理用端末からブラウザを利用して行う。)	･複数人による操作（運用） ･罰則 ･運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)

		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
5	T.HSMClock_TOEuser_Modify_Clock_byHSM_Malice	防止	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
6	T.HSMClock_TOEuser_Imperson_Server_Malice	防止	・TLSによる相互認証 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる相互認証 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
7	T.HSMClock_TOEuser_Modify_Data_Line_Malice	防止	・TLSによる通信路の保護 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる通信路の保護 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAから再度時刻配信を受ける。	・TAから再度時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
8	T.SystemClock_TOEuser_Modify_TimeSource_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則

		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・正しいTAからの時刻配信を受ける。	・正しいTAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
9	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
10	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
11	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
12	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査

		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
13	T.SystemClock_TOEuser_Modify_Clock_byHSM_Malice	防止	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAからの時刻配信を受ける。	・TAからの時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)
14	T.SystemClock_TOEuser_Imperson_Server_Malice	防止	・TLSによる相互認証 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる相互認証 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
15	T.SystemClock_TOEuser_Modify_Data_Line_Malice	防止	・TLSによる通信路の保護 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・TLSによる通信路の保護 ※関連するTOEの機能：時刻配信プロトコル ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・TAから再度時刻配信を受ける。	・TAから再度時刻配信を受ける。 ※関連するTOEの機能：時刻受信機能 (-時刻ソースから、TOEの時刻監査を受ける。 -TOEの時刻を補正する。)

16	T.Key_TLS_TOEuser_Compromise_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
17	T.Key_Sign_TOEuser_Compromise_Malice	防止	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
18	T.Config_TOEuser_Modify_byTOE_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
19	T.Config_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア
20	T.Config_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・設定情報のバックアップ/リストア	・設定情報のバックアップ/リストア

21	T.Config_badTST_TOEuser_Modify_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
22	T.Config_stopTS_TOEuser_Modify_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
23	T.Log_TOEuser_Delete_byTOE_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則	・複数人による操作（運用） ・罰則
		検出	・ログ/運用記録の監査	・運用記録の作成 ・ログ/運用記録の監査 ※関連するTOEの機能：ログ管理機能
		回復	ー	ー
24	T.Log_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
25	T.Log_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
26	T.SW_TOEuser_Modify_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)

		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
27	T.SW_TOEuser_Modify_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	・ソフトウェアのリストア	・ソフトウェアのリストア
28	T.Password_TOEuser_Secret_byOS_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
29	T.Password_TOEuser_Secret_byImportSW_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
30	T.Password_TOEuser_Secret_byMemo_Malice	防止	・罰則	・罰則
		検出	ー	ー
		回復	ー	ー
31	T.Serial_TOEuser_Modify_byImportSW_Malice	防止	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー

32	T.Serial_TOEuser_Modify_byHSM_Malice	防止	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・HSMの機能にアクセスするためのICカードの管理 ・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー
33	T.Virus_TOEuser_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ・ウィルスチェック	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理) ・ウィルスチェック
		検出	ー	ー
		回復	ー	ー
34	T.Crash_TOEuser_Malice	防止	・複数人による操作（運用または機能での実現） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。)	・複数人による操作（運用） ・罰則 ・運用管理(操作は、管理用端末からブラウザを利用して行う。) ※管理用端末を用意することで実現可能。 ※関連するTOEの機能：TOE管理機能(ブラウザを利用した運用管理)
		検出	・運用記録の監査	・運用記録の作成 ・運用記録の監査
		回復	ー	ー

3-2 前提の実現方法例

以下に、セキュリティ環境の前提に関する実現方法例を記載する。

表 5-5　前提の実現方法例

No.	前提名	実現方法例
1	A.Location	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
2	A.TOE_Administrator	・TOE管理者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
3	A.TOE_Operator	・TOE運用者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。

4	A.TOE_Auditor	・TOE監査者は、責務を実行できるよう、必要な知識を持ち十分な訓練を受けている。
5	A.TS_Requestor	・タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証及び保持する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TSA証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当なTSAによって行われたものかどうかの確認、が含まれる。 ・タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証するためのソフトウェアを持つ。また、タイムスタンプトークンを保管するためのストレージを持つ。
6	A.Device	TOE（及び関連するコンポーネント）は、入退室管理の行われている部屋に設置され、権限の無いユーザからの物理アクセスを防ぐ。
7	A.FIREWALL	・プライベートネットワークと外部ネットワークを結ぶネットワークには、ファイアウォールを設置する。 ・ファイアウォールの設定は、適切に維持・管理される。
8	A.PEER	・タイムスタンプ利用者（タイムスタンプ要求者）を除くTOEと通信する意図された他システムは、信頼できる第三者(TTP)の運用するシステムであることを保証する。
9	A.TSA2_TA1_Connection	TA1(認証連鎖方式の時刻配信局)とTOEの間の通信路は、専用線である。
10	A.Environment	・TOE の設置場所として、電磁波対策、電力対策、温度・湿度対策が行われている設備を利用する。
11	A.MEDIA	・定期的なデータのバックアップと、適切なシステムマイグレーションを行う。

3-3 組織のセキュリティポリシーの実現方法例

以下に、組織のセキュリティポリシーに関する実現方法例を記載する。

表 5-6 組織のセキュリティポリシーの実現方法例

No.	ポリシー名	実現方法例
1	P.Cryptography	・TOEの署名と検証の暗号処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」されたアルゴリズムによって行われる。
2	P.PKI_Management	TOEは、安全に管理されたPKIの中で運用されることを保証する。鍵/証明書は、運用マニュアルに基づき、安全に発行・失効される。
3	P.Password_Management	・TOE管理者およびTOE運用者は、パスワードを記憶し、他人に漏らさない。また、運用マニュアルに基づき、適切なパスワードを設定し、適切な頻度でパスワードを変更する。 ・TOE管理者およびTOE運用者は、ソーシャルエンジニアリングの教育を受けている。
4	P.HSM	TOEを利用する組織は、FIPS140-2 level3相当の機能を持つHSMにより、物理的に保護された署名鍵を利用した、タイムスタンプトークンやシステムログに対する暗号操作及び署名鍵のライフサイクル管理を行うことを保証する。
5	P.Protect_Log	・TOE を利用する組織は、TOEの監査ログの暴露・改ざんまたは削除を防止するよう、TOE管理者、TOE運用者、TOE監査者に対して教育を行う。 ・TOEは、TOEの出力するシステムログにハッシュ値やデジタル署名を付与し、改ざんを検出可能な機能を持つ。 ・TOEは、TOEの保護対象資産へのアクセスを許可する前に、全ての利用者に対して識別・認証情報の入力を要求し、識別・認証を実施する。

6	P.Time_Source	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
7	P.System_Clock_Management	TOEは、時刻ソースの信頼性と正確性を受容可能な、信頼できる第三者の運用する時刻ソースを参照する。
8	P.Check_Virus	TOE管理者は、運用マニュアルに基づき、定期的にTOEの全ファイルに対してウィルスチェックを行う。また、外部からメディアを持ち込む場合は、事前にウィルスチェックを行う。
9	P.Check_Received_Data	TOEは、TA1から送信されたデータを受信した場合、そのデータの真正性と完全性を確認する機能を持つ。
10	P.Dual_Control	運用マニュアルに基づき、TOE の管理業務における重要な操作は、複数のTOE 管理者による合議の上で行う。 また、TOE 運用業務における重要な操作は、複数の運用者による合議の上で行う。
11	P.Check_Abstract_Vulnerability	TOE管理者は、運用マニュアルに基づき、定期的にOS やライブラリなどの脆弱性を確認し、対策を行う。

4. 脅威ツリー及びリスク評価一覧

4-1 脅威ツリー

以下に、脅威ツリーを示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

※欄の不足を補うため、一部「下位の条件→上位の条件」と矢印で表現している場合がある。

表 5-7　脅威ツリー

No.	資産	脅威	上位レベルが実現するための条件			脅威名
			条件1	条件2	条件3	
1	HSM時刻	内部の不正者が、TOEが参照する時刻ソースを変更する。	内部の不正者が、TOEの設定情報を変更する。	—	—	T.HSMClock_TOEuser_Modify_TimeSource_Malice
2	HSM時刻		TOEが参照する時計が内部の不正者の攻撃により機能低下（故障）し、時刻がずれる。	※具体的な攻撃方法は特に規定しない。	—	T.HSMClock_Inaccuracy_TOEuser_Crash_Malice
3	HSM時刻	内部の不正者が、TOEが参照する時計の時刻をずらす。	内部の不正者が、TOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	—	T.HSMClock_TOEuser_Modify_Clock_byTOE_Malice
4	HSM時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	※OSの機能からHSM時刻を設定することはできないので脅威から除外。	—
5	HSM時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	—	T.HSMClock_TOEuser_Modify_Clock_byImport SW_Malice

6	HSM時刻			HSMの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。）	物理的にHSMにアクセス→HSMの機能へのアクセス(管理者用ICカードが必要)	T.HSMClock_TOEuser_Modify_Clock_byHSM_Malice
7	HSM時刻	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。	TOEと時刻ソースの間のネットワークにアクセスする。	TOEに成りすましたサーバを用意する。 ※秘密鍵は除外。秘密鍵以外についての成りすまし。	—	T.HSMClock_TOEuser_Imperson_Server_Malice
8	HSM時刻	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	—	—	T.HSMClock_TOEuser_Modify_Data_Line_Malice
9	システム時刻	内部の不正者が、TOEが参照する時刻ソースを変更する。	内部の不正者が、TOEの設定情報を変更する。	—	—	T.SystemClock_TOEuser_Modify_TimeSource_Malice
10	システム時刻		TOEが参照する時計が内部の不正者の攻撃により機能低下（故障）し、時刻がずれる。	※具体的な攻撃方法は特に規定しない。	—	T.SystemClock_Inaccuracy_TOEuser_Crash_Malice
11	システム時刻	内部の不正者が、TOEが参照する時計の時刻をずらす。	内部の不正者が、TOEの時刻を設定する。	TOEの機能を用いてTOEの時刻を設定する。	—	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice
12	システム時刻			OSの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：OSの時刻設定コマンド	OSにログインする	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice
13	システム時刻			外部から持ち込んだソフトウェアを用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。） ※例：悪意のソフトウェア	—	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice
14	システム時刻			HSMの機能を用いてTOEの時刻を設定する。 （TOEの機能以外の方法を用いてTOEの時刻を設定する。）	物理的にHSMにアクセス→HSMの機能へのアクセス(管理者用ICカードが必要)	T.SystemClock_TOEuser_Modify_Clock_byHSM_Malice
15	システム時刻	内部の不正者が、TOEに成りすましたサーバを利用して時刻ソースと通信を行う。	TOEと時刻ソースの間のネットワークにアクセスする。	TOEに成りすましたサーバを用意する。 ※秘密鍵は除外。秘密鍵以外についての成りすまし。	—	T.SystemClock_TOEuser_Imperson_Server_Malice

16	システム時刻	内部の不正者が、TOEと時刻ソースの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改ざんする。	TOEと時刻ソースの間のネットワークにアクセスする。	―	―	T.SystemClock_TOEuser_Modify_Data_Line_Malice
17	秘密鍵		内部の不正者がTOEの秘密鍵を暴露する。	[通信用鍵] OSの機能を用いてTOEの秘密鍵を取得する。	OSにログインする	T.Key_TLS_TOEuser_Compromise_Malice
18	秘密鍵			[署名鍵] 物理的にTOEにアクセス→HSMを持ち出す。	OSにログインする →OSの機能を用いてTOEの鍵データを取得する。	T.Key_Sign_TOEuser_Compromise_Malice
19	設定情報	内部の不正者が、TOEの設定情報を変更･削除･暴露する。	TOEの機能を用いてTOEの設定情報を変更･削除･暴露する。	―	―	T.Config_TOEuser_Modify_byTOE_Malice
20	設定情報		OSの機能を用いてTOEの設定情報を変更･削除･暴露する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	―	T.Config_TOEuser_Modify_byOS_Malice
21	設定情報		外部から持ち込んだソフトウェアを用いてTOEの設定情報を変更する。 （TOEの機能以外の方法を用いてTOEの設定情報を変更･削除･暴露する。） ※例：悪意のソフトウェア	―	―	T.Config_TOEuser_Modify_byImportSW_Malice
22	設定情報	内部の不正者が、TOEの設定を変更し、不正なタイムスタンプトークンを発行する。	TOEの設定情報を変更する。 ※[不正なタイムスタンプトークンの例] 本来のポリシ(OID,accuracy,ordering等)と異なるタイムスタンプトークンなど。	TOEにアクセスする。	―	T.Config_badTST_TOEuser_Modify_Malice
23	設定情報	内部の不正者が、TOEの設定を変更し、タイムスタンプトークンの発行を停止させる。	TOEの設定情報を変更する。	TOEにアクセスする。	―	T.Config_stopTS_TOEuser_Modify_Malice
24	ログ	内部の不正者が、TOEのログを変更･削除･暴露する。	TOEの機能を用いてTOEのログを削除･暴露する。 ※ログの変更は、TOEの機能を利用して実施することはできない。	―	―	T.Log_TOEuser_Delete_byTOE_Malice

25	ログ		OSの機能を用いてTOEのログを変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。） ※例：設定ファイルを直接編集する。	OSにログインする	―	T.Log_TOEuser_Modify_byOS_Malice
26	ログ		外部から持ち込んだソフトウェアを用いてTOEのログを変更・削除・暴露する。 （TOEの機能以外の方法を用いてTOEのログを変更・削除・暴露する。） ※例：悪意のソフトウェア	―	―	T.Log_TOEuser_Modify_byImportSW_Malice
27	ソフトウェア	内部の不正者が、TOEのソフトウェアを変更・削除・暴露する。	OSの機能を用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：OSのコマンドを利用して削除する。	OSにログインする	―	T.SW_TOEuser_Modify_byOS_Malice
28	ソフトウェア		外部から持ち込んだソフトウェアを用いてTOEのソフトウェアを変更・削除・暴露する。 ※例：悪意のソフトウェア	―	―	T.SW_TOEuser_Modify_byImportSW_Malice
29	ID・パスワード	内部の不正者が、TOEのID・パスワードを暴露する。	OSの機能を用いてTOEのID・パスワードを暴露する。 ※例：OSのファイル内容表示コマンドを利用する。	OSにログインする	―	T.Password_TOEuser_Secret_byOS_Malice
30	ID・パスワード		外部から持ち込んだソフトウェアを用いてTOEのID・パスワードを暴露する。 ※例：悪意のソフトウェア	―	―	T.Password_TOEuser_Secret_byImportSW_Malice
31	ID・パスワード		その他、口頭、メモ、メール等で情報が漏洩する。	―	―	T.Password_TOEuser_Secret_byMemo_Malice
32	シリアル番号	内部の不正者が、TOEが参照するシリアル番号を変更・削除する。	内部の不正者が、シリアル番号を変更・削除する。	外部から持ち込んだソフトウェアを用いてTOEの参照するシリアル番号を変更・削除する。 （TOEの機能以外の方法を用いてTOEの参照するシリアル番号を変更・削除する。） ※例：悪意のソフトウェア	―	T.Serial_TOEuser_Modify_byImportSW_Malice

33	シリアル番号			HSMの機能を用いてTOEの参照するシリアル番号を変更･削除する。 （TOEの機能以外の方法を用いてTOEの参照するシリアル番号を変更･削除する。）	物理的にHSMにアクセス→HSMの機能へのアクセス(管理者用ICカードが必要) →HSMに保管されるシリアル番号を不正な値にセットする。	T.Serial_TOEuser_Modify_byHSM_Malice
34	その他	内部の不正者が、TOEにウィルスを感染させる。	ウィルスに感染した外部メディアにアクセスする。	OSにログインする	ウィルスに感染した外部メディアを持ち込む。	T.Virus_TOEuser_Malice
35	その他		外部からウィルスをダウンロードする。	外部にアクセスする。	OSにログインする	同上
36	その他	内部の不正者が、TOEを破壊し、サービスを停止させる。	TOEを破壊する。	TOEの設置された部屋に入室する。	―	T.Crash_TOEuser_Malice

4-2 リスク評価格付けの考え方

以下に、リスク評価格付けの考え方を示す。

表 5-8　リスク評価格付けの考え方

	格付け	高(3)	中(2)	低(1)
D	潜在的損失（Damage potential）	<方針> ･信頼性･サービスレベルに影響のあるもの。 ･データを直接悪用できるもの。 ＜対象＞ その他	<方針> ･データを直接は悪用できないもの。 ＜対象＞ ･システム時刻(評価対象がTSA2の場合のみ) ･ログ	＜方針＞ なし ＜対象＞ なし
R	再現性（Reproducibility）	＜方針＞ ･時期によらないもの。 ･内部不正など、攻撃者の意図でいつでも実施できるもの。 ･外部ネットワークからの攻撃 ･自然に時刻がずれる場合。 ＜対象＞ ･内部不正 ･DoS ･バッファオーバーフロー ･外部ネットワークからの不正アクセス ･自然に時刻がずれる場合 ･その他	＜方針＞ ･攻撃者の意図によらないもの。 ･TOE開発時のソフトウェア不良 ･ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ＜対象＞ ･不注意（基本的に発生率は低い、という前提。） ･TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見･修正されている、という前提。) ･ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断（基本的に発生率は低い、という前提。）	<方針> ･攻撃が困難なもの。 ･専門的な知識が必要なもの。 ･事業撤退 ･他システムの秘密鍵危殆化 ＜対象＞ ･暗号脆弱化 ･パケットの暴露･改ざん ･ハードウェア･ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ･他システムの秘密鍵危殆化

E	攻撃利用可能性（Exploitability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃できるもの。 ・攻撃方法が容易なもの。 ・比較的攻撃ツールが入手しやすいと思われるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他	＜方針＞ なし ＜対象＞ なし	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん
A	影響ユーザ（Affected users）	<方針> ・TOEのサービスの利用者に関わるもの。 ・TOE利用者自身に大きな影響があるもの。 ＜対象＞ ・その他	<方針> ・TOEのサービスの利用者に対する直接的な影響がないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
D	発見可能性（Discoverability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃方法を知る事ができるもの。 ・攻撃方法が容易に思いつくもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退	＜方針＞ ・TOE開発時のソフトウェア不良 ＜対象＞ ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

		・他システムの秘密鍵危殆化 ・その他		

4-3 リスク評価点

以下に、脅威に対するリスク評価点を示す。(内部不正を考慮しないセキュリティ評価の結果に対して、内部不正を考慮した場合に追加となる項目のみ記載する。)

表 5-9　リスク評価点

No.	名称	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.HSMClock_TOEuser_Modify_TimeSource_Malice	3	3	3	3	3	15
2	T.HSMClock_Inaccuracy_TOEuser__Crash_Malice	3	3	3	3	3	15
3	T.HSMClock_TOEuser_Modify_Clock_byTOE_Malice	3	3	3	3	3	15
4	T.HSMClock_TOEuser_Modify_Clock_byImportSW_Malice	3	3	3	3	3	15
5	T.HSMClock_TOEuser_Modify_Clock_byHSM_Malice	3	3	3	3	3	15
6	T.HSMClock_TOEuser_Imperson_Server_Malice	3	3	3	3	3	15
7	T.HSMClock_TOEuser_Modify_Data_Line_Malice	3	3	3	3	3	15
8	T.SystemClock_TOEuser_Modify_TimeSource_Malice	2	3	3	2	3	13
9	T.SystemClock_Inaccuracy_TOEuser__Crash_Malice	2	3	3	2	3	13
10	T.SystemClock_TOEuser_Modify_Clock_byTOE_Malice	2	3	3	2	3	13
11	T.SystemClock_TOEuser_Modify_Clock_byOS_Malice	2	3	3	2	3	13
12	T.SystemClock_TOEuser_Modify_Clock_byImportSW_Malice	2	3	3	2	3	13
13	T.SystemClock_TOEuser_Modify_Clock_byHSM_Malice	2	3	3	2	3	13
14	T.SystemClock_TOEuser_Imperson_Server_Malice	2	3	3	2	3	13
15	T.SystemClock_TOEuser_Modify_Data_Line_Malice	2	3	3	2	3	13
16	T.Key_TLS_TOEuser_Compromise_Malice	3	3	3	3	3	15
17	T.Key_Sign_TOEuser_Compromise_Malice	3	3	3	3	3	15
18	T.Config_TOEuser_Modify_byTOE_Malice	3	3	3	3	3	15
19	T.Config_TOEuser_Modify_byOS_Malice	3	3	3	3	3	15
20	T.Config_TOEuser_Modify_byImportSW_Malice	3	3	3	3	3	15
21	T.Config_badTST_TOEuser_Modify_Malice	3	3	3	3	3	15
22	T.Config_stopTS_TOEuser_Modify_Malice	3	3	3	3	3	15
23	T.Log_TOEuser_Delete_byTOE_Malice	2	3	3	2	3	13
24	T.Log_TOEuser_Modify_byOS_Malice	2	3	3	2	3	13

25	T.Log_TOEuser_Modify_byImportSW_Malice	2	3	3	2	3	13
26	T.SW_TOEuser_Modify_byOS_Malice	3	3	3	3	3	15
27	T.SW_TOEuser_Modify_byImportSW_Malice	3	3	3	3	3	15
28	T.Password_TOEuser_Secret_byOS_Malice	3	3	3	3	3	15
29	T.Password_TOEuser_Secret_byImportSW_Malice	3	3	3	3	3	15
30	T.Password_TOEuser_Secret_byMemo_Malice	3	3	3	3	3	15
31	T.Serial_TOEuser_Modify_byImportSW_Malice	3	3	3	3	3	15
32	T.Serial_TOEuser_Modify_byHSM_Malice	3	3	3	3	3	15
33	T.Virus_TOEuser_Malice	3	3	3	3	3	15
34	T.Crash_TOEuser_Malice	3	3	3	3	3	15

第6章 タイムスタンプ検証不可能時の考察

本章では、タイムスタンプ利用者が、タイムスタンプ検証不可能となる脅威について、セキュリティ評価を行う。

1. タイムスタンプ利用者側のセキュリティ環境

1-1 前提

以下に、タイムスタンプ利用者のセキュリティ環境の前提を示す。

表 6-1　前提

No.	分類	項目	説明
1	その他	A.VerifySoftware	検証ソフトウェアの入手先および入手経路は信頼できる。また、検証ソフトウェアは正しく動作する。 検証ソフトウェアが動作するマシンには、検証ソフトウェアの動作に必要なソフトウェア以外はインストールされないものとする。 検証ソフトウェアが動作するために必要なOSや依存するライブラリは、不正な改変から保護され、正しく動作する。
2	その他	A.Data_Storage_TimeStamp	タイムスタンプとタイムスタンプ対象データの対応は正しく管理される。
3	その他	A.Data_Storage_Backup	タイムスタンプ、タイムスタンプ対象データ、タイムスタンプ関連データ（検証に関する情報など）の完全性は保証される。
4	人的な前提	A.TS_Requestor	タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証及び保持する。この中には、アウト･オブ･バンドの方法を用いて、TSA証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当なTSAによって行われたものかどうかの確認、が含まれる。
5	その他	A.PEER	タイムスタンプ利用者（タイムスタンプ要求者）と通信するTSAは、信頼できる。
6	その他	A.TimeStamp	タイムスタンプ利用者（タイムスタンプ要求者）の受信するタイムスタンプトークンは、正当である。
7	その他	A.TSA	タイムスタンプ利用者（タイムスタンプ要求者）は、RFC3161に準拠した独立トークン方式のタイムスタンプトークンを発行するTSAを利用する。 また、タイムスタンプトークンに使用されているハッシュ処理および署名処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されているものとする。

1-2 脅威

以下に、タイムスタンプ利用者がタイムスタンプ検証不可能となる脅威を示す。

表 6-2　脅威

No.	項目	説明
1	T.TimeStamp_Verify_Platform_Unavailable_OS	タイムスタンプ有効期間内にタイムスタンプ検証が不可となる。(プラットフォームOSベンダが事業を撤退し、検証ソフトウェアを稼動させるために必要なOSの更新版を入手できなくなる。)

2	T.TimeStamp_Verify_Platform_Unavailable_HW	タイムスタンプ有効期間内にタイムスタンプ検証が不可となる。(プラットフォームハードウェアベンダが事業を撤退し、検証ソフトウェアを稼動させるために必要なOSに適した新規のハードウェアを入手できなくなる。)
3	T.TimeStamp_Verify_Information_Unavailable	タイムスタンプ有効期間内にタイムスタンプ検証が不可となる。(タイムスタンプ事業者と連携する認証局が事業引継ぎを行わずに事業を撤退し、タイムスタンプ検証ができなくなる。)
4	T.TimeStamp_TSA_Crypto_Compromise_gradually	タイムスタンプ有効期間内にタイムスタンプ検証が不可となる。(計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化し、タイムスタンプの信用性が低下する。)
5	T.TimeStamp_TSA_Crypto_Compromise_immediately	タイムスタンプ有効期間内にタイムスタンプ検証が不可となる。(暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化し、タイムスタンプの信用性が低下する。)
6	T.TimeStamp_Key_Compromise	タイムスタンプ有効期間内にタイムスタンプ検証が不可となる。(CAまたはTSAの秘密鍵が危殆化し、タイムスタンプの信用性が低下する。)

1-3 組織のセキュリティポリシー

以下に、タイムスタンプ利用者の、組織のセキュリティポリシーを示す。

表 6-3　組織のセキュリティポリシー

No.	項目	説明
1	P.Cryptography	タイムスタンプ要求に含めるメッセージダイジェストのハッシュ処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されなければならない。

2. セキュリティ対策

2-1 脅威のセキュリティ対策

以下に、セキュリティ環境の脅威のセキュリティ対策を示す。

表 6-4　脅威のセキュリティ対策

No.	脅威名	セキュリティ対策	
1	T.TimeStamp_Verify_Platform_Unavailable_OS	防止	・検証ソフトウェアの提供元から、他のOSで動作する検証ソフトウェアを入手する。 ・複数のOSに対応した(またはOSに依存しない)検証ソフトウェアの利用
		検出	・事業の撤退に関する情報の定期的な確認
		回復	・エミュレータの利用 ・プラットフォームの移行(ソフトウェアの改修)
2	T.TimeStamp_Verify_Platform_Unavailable_HW	防止	・あらかじめ予備のハードウェアを複数準備しておく。
		検出	・事業の撤退に関する情報の定期的な確認
		回復	・エミュレータの利用 ・プラットフォームの移行(ソフトウェアの改修)

3	T.TimeStamp_Verify_Information_Unavailable	防止	・信頼できる認証局と連携したTSAを利用する。（認証局のポリシー上に、事業の引継ぎが明記されている、またそれを実践する見込みのある認証局。） ・事前に、検証に必要な情報を集め、安全に保管しておく。
		検出	・事業の撤退に関する情報の定期的な確認
		回復	ー
4	T.TimeStamp_TSA_Crypto_Compromise_gradually	防止	・タイムスタンプ利用者側で、あらかじめタイムスタンプ対象データおよびタイムスタンプトークンをセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・暗号アルゴリズムが完全に危殆化する前に、タイムスタンプ利用者側で、タイムスタンプトークンやタイムスタンプ対象データに対して、安全な暗号アルゴリズムを使用したタイムスタンプを取得する。 ※TSA側の対応が必要。 ・タイムスタンプ利用者側で、あらかじめ異なる暗号アルゴリズムを使用したタイムスタンプを複数取得する。 ※TSA側の対応が必要。 ・TSAがタイムスタンプトークンを保管する。（タイムスタンプ対象データのメッセージダイジェストに使用されるアルゴリズムの脆弱化には対応できない。） ※TSA側の対応が必要。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー
5	T.TimeStamp_TSA_Crypto_Compromise_immediately	防止	・タイムスタンプ利用者側で、あらかじめタイムスタンプ対象データおよびタイムスタンプトークンをセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。 ・タイムスタンプ利用者側で、あらかじめ異なる暗号アルゴリズムを使用したタイムスタンプを複数取得する。 ※TSA側の対応が必要。 ・TSAがタイムスタンプトークンを保管する。(タイムスタンプ対象データのメッセージダイジェストに使用されるアルゴリズムの脆弱化については対応できない。) ※TSA側の対応が必要。
		検出	ー
		回復	ー
6	T.TimeStamp_Key_Compromise	防止	・タイムスタンプ利用者側で、あらかじめタイムスタンプ対象データおよびタイムスタンプトークンをセキュアに保管する。 ※セキュア保管の要件については、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン(平成17年10月)」を参照。
		検出	・暗号アルゴリズムの脆弱性の監視(公的な評価機関による暗号アルゴリズムの評価結果のチェック)
		回復	ー

2-2 前提の実現方法例

以下に、セキュリティ環境の前提に関する実現方法例を記載する。

表 6-5　前提の実現方法例

No.	前提名	実現方法例
1	A.VerifySoftware	・タイムスタンプ利用者（タイムスタンプ要求者）は、検証ソフトウェアの入手先および入手経路は信頼できることを保証する。また、検証ソフトウェアの入手先は、検証ソフトウェアが正しく動作することを保証する。 ・タイムスタンプ利用者（タイムスタンプ要求者）は、検証ソフトウェアおよび検証ソフトウェアのIT環境の取扱説明書を熟読した上で、取扱説明書が定める手順に従って、検証ソフトウェアおよび検証ソフトウェアのIT 環境を構築する。この際、検証ソフトウェアが動作するマシンには、検証ソフトウェアの動作に関係ないソフトウェアはインストールしない。 ・タイムスタンプ利用者（タイムスタンプ要求者）は、検証ソフトウェアが動作するために必要なOSや依存するライブラリが不正な改変から保護され、正しく動作するよう適切に管理する。 ・タイムスタンプ利用者（タイムスタンプ要求者）は、検証ソフトウェアが動作するマシンに、検証ソフトウェアの動作を干渉するようなソフトウェアがインストールされないように、適切に管理する。 ・タイムスタンプ利用者（タイムスタンプ要求者）は、検証ソフトウェアおよび検証ソフトウェアのIT環境が正常な動作を維持するように、適切に管理する。
2	A.Data_Storage_TimeStamp	タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプとタイムスタンプ対象データの対応を正しく管理する責任を持つ。
3	A.Data_Storage_Backup	・定期的なデータのバックアップと、適切なシステムマイグレーションを行う。
4	A.TS_Requestor	タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証及び保持する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TSA証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当なTSAによって行われたものかどうかの確認、が含まれる。 ・タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証するためのソフトウェアを持つ。また、タイムスタンプトークンを保管するためのストレージを持つ。
5	A.PEER	・タイムスタンプ利用者（タイムスタンプ要求者）と通信するTSAは、信頼できる第三者(TTP)の運用するTSAであることを保証する。
6	A.TimeStamp	タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプトークンを検証及び保持する責任を持つ。この中には、アウト・オブ・バンドの方法を用いて、TSA証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当なTSAによって行われたものかどうかの確認、が含まれる。
7	A.TSA	・タイムスタンプ利用者（タイムスタンプ要求者）は、タイムスタンプ要求に含めるメッセージダイジェストのハッシュ処理が、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されることを保証する。 ・TSAは、RFC3161に準拠した独立トークン方式のタイムスタンプトークンを発行することを保証する。また、タイムスタンプトークンに使用されているハッシュ処理および署名処理は、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されていることを保証する。

2-3 組織のセキュリティポリシーの実現方法例

以下に、組織のセキュリティポリシーに関する実現方法例を記載する。

表 6-6　組織のセキュリティポリシーの実現方法例

No.	ポリシー名	実現方法例
1	P.Cryptography	・タイムスタンプユーザ（タイムスタンプ要求者）は、タイムスタンプ要求に含めるメッセージダイジェストのハッシュ処理が、「電子政府推奨暗号リスト(平成15年2月20日、総務省、経済産業省)」に記載されたアルゴリズムによって実装されることを保証する。

3. 脅威ツリー及びリスク評価一覧

3-1 脅威ツリー

以下に、脅威ツリーを示す。
※欄の不足を補うため、一部「下位の条件→上位の条件」と矢印で表現している場合がある。

表 6-7　脅威ツリー

No.	資産	脅威	上位レベルが実現するための条件			脅威名
			条件1	条件2	条件3	
1	タイムスタンプトークン	タイムスタンプ有効期間内にタイムスタンプ検証が不可となる。	プラットフォームOSベンダが事業を撤退し、検証ソフトウェアを稼動させるために必要なOSの更新版を入手できなくなる。	—	—	T.TimeStamp_Verify_Platform_Unavailable_OS
2			プラットフォームハードウェアベンダが事業を撤退し、検証ソフトウェアを稼動させるために必要なOSに適した新規のハードウェアを入手できなくなる。	—	—	T.TimeStamp_Verify_Platform_Unavailable_HW
3			タイムスタンプ事業者が事業引継ぎを行わずに事業を撤退し、タイムスタンプ検証ができなくなる。	※独立トークン方式のタイムスタンプでは、TSAと連携するCAが検証に必要な情報（証明書・CRLなど）を提供していればよいので、脅威とはならない。	—	—
4			時刻配信事業者が事業引継ぎを行わずに事業を撤退し、タイムスタンプ検証ができなくなる。	※独立トークン方式のタイムスタンプでは、TSAと連携するCAが検証に必要な情報（証明書・CRLなど）を提供していればよいので、脅威とはならない。	—	—
5			タイムスタンプ事業者と連携する認証局が事業引継ぎを行わずに事業を撤退し、タイムスタンプ検証ができなくなる。	—	—	T.TimeStamp_Verify_Information_Unavailable
6			過去に取得したタイムスタンプに使用された暗号アルゴリズムや鍵などが危殆化し、タイムスタンプの信用性が低下する。	計算機性能の向上などにより、暗号アルゴリズムが徐々に脆弱化する。	—	T.TimeStamp_TSA_Crypto_Compromise_gradually
7				暗号アルゴリズムの解読方法の発見、量子計算機の実現などにより、暗号アルゴリズムが突然脆弱化する。	—	T.TimeStamp_TSA_Crypto_Compromise_immediately

8				CAまたはTSAの秘密鍵が危殆化する。	―	T.TimeStamp_Key_Compromise
9				TAの秘密鍵が危殆化する。	※TAの秘密鍵はタイムスタンプの署名とは関わらないため、脅威とはならない。	―

3-2 リスク評価格付けの考え方

以下に、リスク評価格付けの考え方を示す。

表 6-8　リスク評価格付けの考え方

	格付け	高(3)	中(2)	低(1)
D	潜在的損失（Damage potential）	<方針> ・信頼性・サービスレベルに影響のあるもの。 ・データを直接悪用できるもの。 ＜対象＞ その他	<方針> ・データを直接は悪用できないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
R	再現性（Reproducibility）	＜方針＞ ・時期によらないもの。 ・内部不正など、攻撃者の意図でいつでも実施できるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ＜対象＞ ・内部不正 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・その他	＜方針＞ ・攻撃者の意図によらないもの。 ・TOE開発時のソフトウェア不良 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ＜対象＞ ・不注意（基本的に発生率は低い、という前提。） ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。) ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断（基本的に発生率は低い、という前提。）	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・暗号脆弱化 ・パケットの暴露・改ざん ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化

E	攻撃利用可能性（Exploitability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃できるもの。 ・攻撃方法が容易なもの。 ・比較的攻撃ツールが入手しやすいと思われるもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退 ・他システムの秘密鍵危殆化 ・その他	＜方針＞ なし ＜対象＞ なし	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん
A	影響ユーザ（Affected users）	<方針> ・TOEのサービスの利用者に関わるもの。 ・TOE利用者自身に大きな影響があるもの。 ＜対象＞ ・その他	<方針> ・TOEのサービスの利用者に対する直接的な影響がないもの。 ＜対象＞ ・システム時刻(評価対象がTSA2の場合のみ) ・ログ	＜方針＞ なし ＜対象＞ なし
D	発見可能性（Discoverability）	<方針> ・内部不正、不注意など、攻撃者が容易に攻撃方法を知る事ができるもの。 ・攻撃方法が容易に思いつくもの。 ・外部ネットワークからの攻撃 ・自然に時刻がずれる場合。 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・事業撤退 ・他システムの秘密鍵危殆化 ＜対象＞ ・内部不正 ・不注意 ・DoS ・バッファオーバーフロー ・外部ネットワークからの不正アクセス ・自然に時刻がずれる場合 ・ハードウェア故障や他システムのダウン、事故などによるネットワークの遮断 ・ハードウェア・ソフトウェアベンダの事業撤退や、サービス事業者の、事業引継ぎを行わない事業撤退	＜方針＞ ・TOE開発時のソフトウェア不良 ＜対象＞ ・TOE開発時のソフトウェア不良(再現性の高い不良は、開発時に発見・修正されている、という前提。)	<方針> ・攻撃が困難なもの。 ・専門的な知識が必要なもの。 ＜対象＞ 暗号脆弱化 パケットの暴露・改ざん

		・他システムの秘密鍵危殆化 ・その他		

3-3 リスク評価点

以下に、脅威に対するリスク評価点を示す。

表 6-9 リスク評価点

No.	名称	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.TimeStamp_Verify_Platform_Unavailable_OS	3	1	3	3	3	13
2	T.TimeStamp_Verify_Platform_Unavailable_HW	3	1	3	3	3	13
3	T.TimeStamp_Verify_Information_Unavailable	3	1	3	3	3	13
4	T.TimeStamp_TSA_Crypto_Compromise_gradually	3	1	1	3	1	9
5	T.TimeStamp_TSA_Crypto_Compromise_immediately	3	1	1	3	1	9
6	T.TimeStamp_Key_Compromise	3	1	3	3	3	13