統合化プラットフォーム・セキュリティ評価報告書

2006 年 3 月 30 日

NICT

電磁波計測部門 タイムアプリケーショングループ

目次

1 セキュリティ評価方法とセキュリティ評価対象

本章では、統合化プラットフォームシステムのセキュリティ評価方法及びセキュリティ評価対象について述べる。

1.1 セキュリティ評価の方法

セキュリティ評価に関する国際標準ISO/IEC 15408 の考え方に基づいて、統合化プラットフォームシステムのセキュリティ評価を実施した。NICTが策定した『統合化プラットフォーム・セキュリティ評価ガイドライン 0.9 版』に従い、統合化プラットフォームシステムのサブシステム毎の評価対象(Target of Evaluation: TOE)を明確化し、そのTOEに対してセキュリティ評価を実施した。具体的なセキュリティ評価手順は、以下の通りである(表 1-1)。

表 1-1:セキュリティ評価手順

#	項目	説明
1	評価システムの明確化	セキュリティ評価対象の物理配置構成、ネットワーク構成、システム構成、ソフトウェア構成、及び外部インタフェース(物理、論理、組織)を明確化する。
2	関与者の明確化	システムの関与者及び役割を明確化する。
3	資産の明確化	保護が必要な資産(一般的には、IT 環境の中の情報やリソース、あるいは、TOE 自体)を記述する。
4	セキュリティ環境の明確化	ISO/IEC 15408 で規定された「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)」を記述する。 ※ここで述べる「脅威」はあくまで、雛形をベースにカスタマイズしたものである。網羅性を高めるため、下記の「脅威分析」で、再度、脅威を抽出・検討する。
5	脅威分析	Microsoft 社の STRIDE モデルや DREAD モデルを用いて、脅威抽出、リスク評価を行う。 • 手順 3 で明確化した資産に対する脅威を STRIDE モデルの観点から抽出 • 抽出した脅威を DREAD モデルにより格付け
6	セキュリティ目標の決定	セキュリティ環境のうち、「脅威」への対策としての「セキュリティ目標」を決定する。 ISO/IEC 15408 の考え方に基づき「セキュリティ目標」を決定する。
7	セキュリティ機能の策定	セキュリティ目標に対するセキュリティ機能を決定する。 ISO/IEC 15408 の考え方に基づき「セキュリティ機能」を策定する。
8	セキュリティ機能の評価	実装されたセキュリティ機能を評価する。セキュリティ環境に対して以下の観点から評価を実施する。 • 前提:どのような実現例が考えられるのか? • 脅威:TOE の機能によって対策済みなのか?、また、対策済みではない場合、どのような対策が想定されるのか? • 組織のセキュリティポリシー:どのような実現例が考えられるのか?

なお、手順の 6(セキュリティ目標の決定)と手順の 7(セキュリティ機能の策定)は、並行的に実施され、厳密に区分されていない。そのため、本セキュリティ評価では、これらの手順は、「セキュリティ目標・対策」策定手順として、まとめられている。また、「セキュリティ目標・対策」の策定における記述内容は、以下のドキュメントをベースにしたものであり、ISO/IEC 15408 Part2 のセキュリティ機能要件のカタログを参照したものではない。

- ISO/IEC TR 15446 の Annex B(informative) Generic examples における「B.7 Example mapping of security objectives to threats」

1.2 統合化プラットフォームのサブシステムと評価対象

統合化プラットフォームシステムは、複数のサブシステムから構成されたシステムである(図 1-1)。

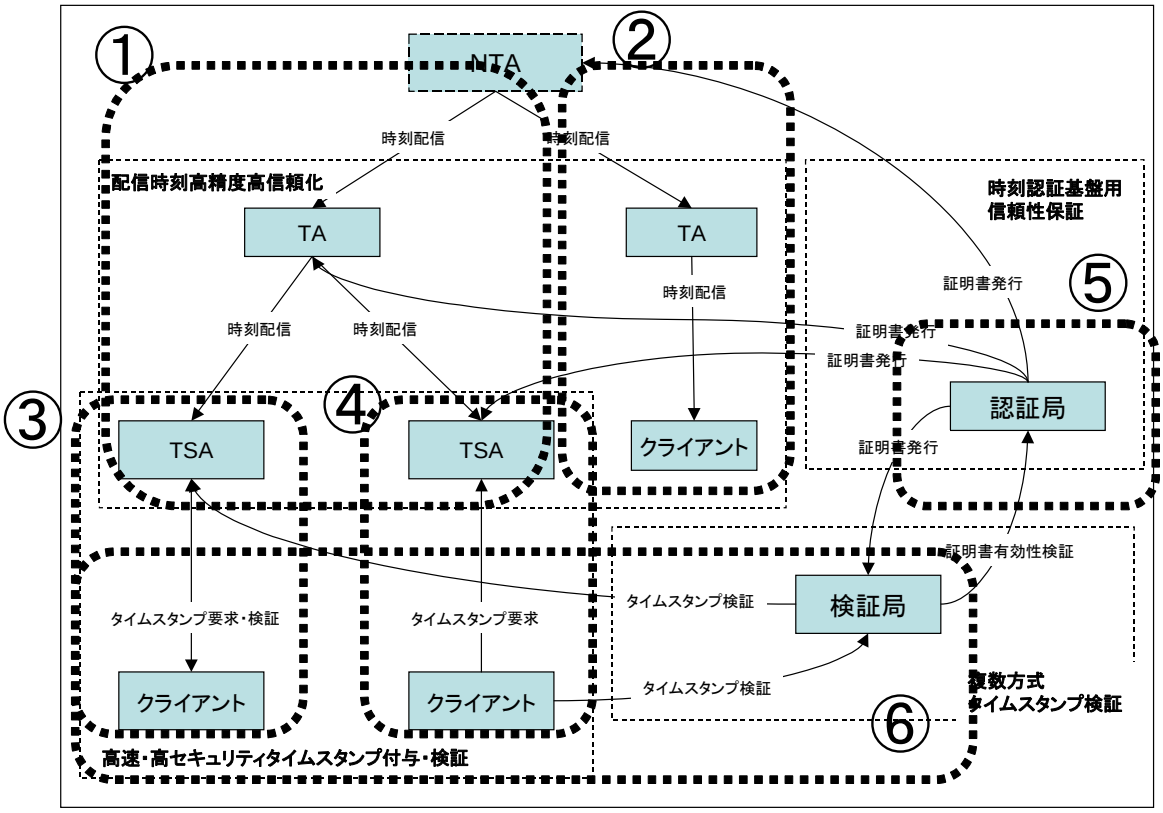

図 1-1:統合化プラットフォームシステム(出典:NICT:時刻認証基盤技術実験装置ー統合化プロトタイプシステムー仕様書, 2004)

図 1-1に含まれる番号に対応するサブシステムの説明は、表 1-2の通りである。これらのサブシステムは、予め意図されたインタフェースを介して関係するサブシステムと通信を行う。

表 1-2:統合化プラットフォームシステムにおけるサブシステム

#	サブシステム名	説明
1	配信時刻高精度高信頼化サブシステム-2	配信時刻の高信頼化を実現するサブシステムである。 認証連鎖方式の時刻配信サービスを提供する。サービスを実施する主体は、TA(Time Authority)と呼ばれる。
2	配信時刻高精度高信頼化サブシステム-3	時刻情報のトレーサビリティを保証するサブシステムである。 時刻リンク方式の時刻配信サービスを提供する。時刻情報のトレーサビリティを保証する主体は、TA(Time Authority)と呼ばれる。
3	高速・高セキュリティタイムスタンプ付与・検証サブシステム-1	リンクトークン方式のタイムスタンプトークンを発行するサブシステムである。 タイムスタンプトークンを発行する主体は、TSA(Time-Stamping Authority)と呼ばれる。
4	高速・高セキュリティタイムスタンプ付与・検証サブシステム-2	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サブシステムである。 タイムスタンプトークンを発行する主体は、TSA(Time-Stamping Authority)と呼ばれる。
5	時刻認証基盤用信頼性保証	統合化プラットフォームシステムで使用される公開鍵証明書を発行するサブシステム

	サブシステム	である。 公開鍵証明書を発行する主体は、認証局（CA: Certification Authority）と呼ばれる。
6	複数方式タイムスタンプ検証サブシステム	独立トーク方式とリンクトークン方式のタイムスタンプを統一的に検証するサブシステムである。 検証サービスの主体は、検証局（VA: Validation Authority）と呼ばれる。

サブシステムは、複数のTOEを含む場合がある。例えば、配信時刻高精度高信頼化サブシステム-2 は、二つのTOEを含む。NTA1 は、仮想的な国家時刻標準機関の時刻配信サーバシステムを示す。TA1 は、認証連鎖方式を採用したTAの時刻配信サーバシステムを示す。各サブシステムにおけるTOEは、表 1-3の通りである。

表 1-3：各サブシステムの TOE

#	サブシステム名	TOE の識別子	説明
1	配信時刻高精度高信頼化サブシステム-2	NTA1	仮想的な国家時刻標準機関、あるいは、国家時刻標準機関の時刻配信サーバシステムを示す。このサーバシステムは、認証連鎖方式を採用している。
2		TA1	認証連鎖方式を採用した TA の時刻配信サーバシステムを示す。
3	配信時刻高精度高信頼化サブシステム-3	NTA2	仮想的な国家時刻標準機関、あるいは、国家時刻標準機関の時刻配信サーバシステムを示す。このサーバシステムは、時刻リンク方式を採用している。
4		TA2	時刻リンク方式を採用した TA の時刻配信サーバシステムを示す。
5	高速・高セキュリティタイムスタンプ付与・検証サブシステム-1	TSA1	リンクトークン方式のタイムスタンプトークンを発行する TSA のタイムスタンプサーバシステムを示す。
6	高速・高セキュリティタイムスタンプ付与・検証サブシステム-2	TSA2	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 のタイムスタンプサーバシステムを示す。
7	時刻認証基盤用信頼性保証サブシステム	CA	公開鍵証明書の発行や公開鍵証明書の失効情報発行・公開を実施する CA サーバとディレクトリサーバから構成される。
8	複数方式タイムスタンプ検証サブシステム	VA	リンクトークン方式のタイムスタンプトークンと独立トークン方式のタイムスタンプトークンを検証するサーバシステムである。

1.3 セキュリティ評価対象に関する特記事項

セキュリティ評価における特記事項を以下に示す。

（1）暗号コンポーネント
統合化プラットフォームシステムでは、暗号技術を実装した暗号コンポーネントが含まれている。例えば、高速・高セキュリティタイムスタンプ付与・検証サブシステム-2（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 システム）では、タイムスタンプトークンの作成に際して、ハッシュ関数やデジタル署名技術が利用されている。本セキュリティ評価では、TOE に関する暗号コンポーネントを明確化した。そして、暗号技術そのものの安全性を評価するのではなく、「セキュリティ環境」の「組織のセキュリティポリシー」にて定められた「暗号技術の使用に関するセキュリティポリシーへの準拠性」への観点から評価した。

また、暗号技術の脆弱化に関する脅威も検討した。例えば、独立トークン方式のタイムスタンプの有効期間（公開鍵証明書の有効期間）が満了する前に、タイムスタンプに使用された暗号技術の脆弱化を想定した脅威を想定し、セキュリティ評価を実施した。

（2）時刻情報

統合化プラットフォームシステムでは、時刻情報が重要である。例えば、高速・高セキュリティタイムスタンプ付与・検証サブシステム-2（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 システム）が発行するタイムスタンプトークンには、タイムスタンプ作成時刻を示す時刻情報が含まれている。この時刻情報は、TSA システムの資産である「時刻情報」に基づいて作成されている。本セキュリティ評価では、TOE に関する時刻情報を明確化し、その情報に対する脅威及び対策を検討した。

（3）内部不正

統合化プラットフォームシステムは、信頼される管理者・運用者によって運用されることを想定している。そのため、内部不正の可能性は限りなくゼロに近い。このような考えに基づき、基本的に内部不正は存在しないという前提を置き、セキュリティ評価を実施した。

なお、可能性としては限りなく小さいが、内部不正を考慮したセキュリティ評価も重要であるとの考えから、オプション的なセキュリティ評価作業として、内部不正を踏まえた脅威の検討も行った。この場合、複数の悪意者の結託は考慮せず、単独犯による内部不正を想定した。

（4）将来的にタイムスタンプが検証できなくなる脅威

タイムスタンプは、署名文書や電子文書の長期保証に有効な技術であると言われている。ところが、将来的にタイムスタンプが検証できない状況が生じた場合、長期保証の役割を果たせなくなる可能性がある。本セキュリティ評価では、このような状況を別途、考察し、脅威及びその対策を検討した。具体的には、タイムスタンプサービス利用者側のセキュリティ環境を想定し、セキュリティ評価を行った。

2 セキュリティ評価結果

本章では、統合化プラットフォームシステムに対するセキュリティ評価結果について記す。統合化プラットフォームシステムの構成要素となるサブシステム毎に定義された TOE に対するセキュリティ評価結果を示す。

2.1 配信時刻高精度高信頼化サブシステム-2

本サブシステムでは、二つの TOE に対してセキュリティ評価を実施した。

2.1.1 NTA1

NTA1 は、仮想的な国家標準機関が運用する時刻配信サーバである。このサーバは、認証連鎖方式を採用している。評価対象は、時刻配信サーバのサブセットである。具体的には、図 2-1における白地のコンポーネントから構成される領域である。

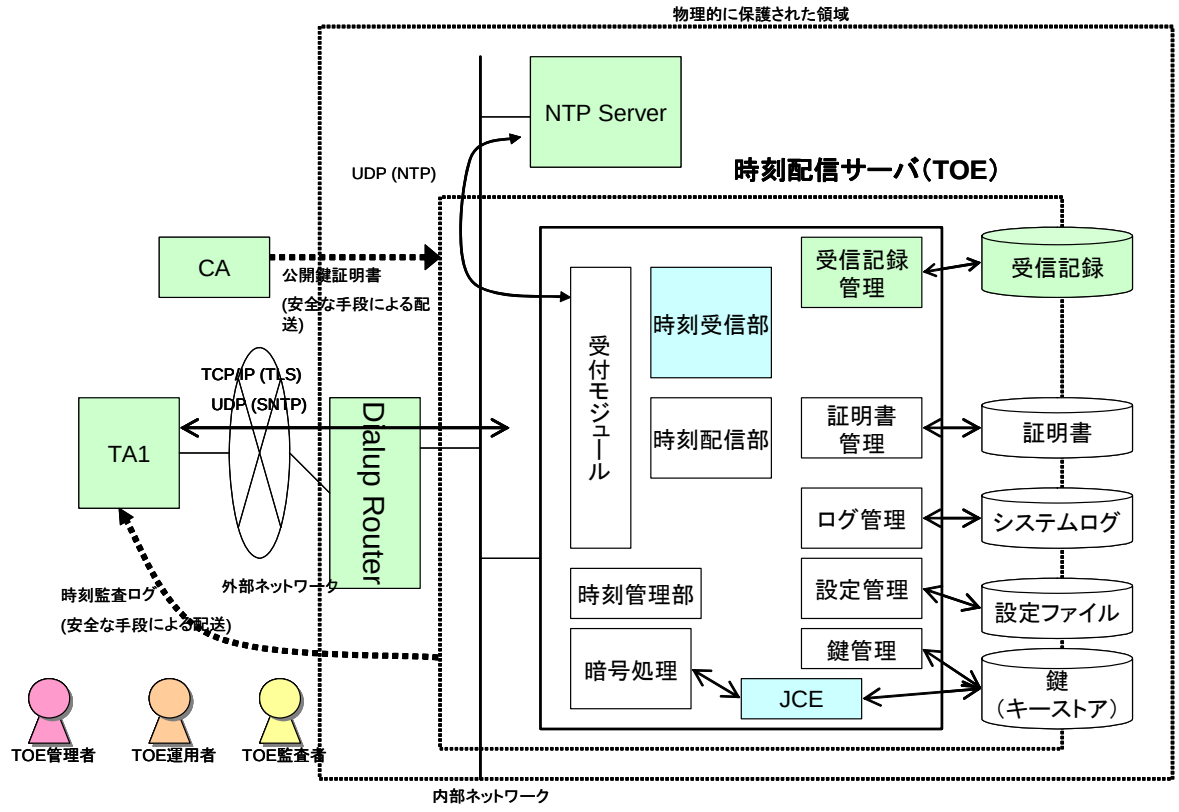

図 2-1:NTA1 のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書(TOE: NTA1)』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

(1)暗号技術コンポーネントの安全性

TOE は、署名や検証処理において暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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。』に準拠していることを確認した。

また、署名と検証以外で使用される暗号技術コンポーネントに関しては、「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)」に掲載されていないものも存在した。この場合、別の担保により安全性が保たれていることを確認した。例えば、TOE と TA1 の間は、MD5 を用いた SNTP が使用されるが、この時の通信回線は、成りすまし・改ざん・盗聴などを防ぐ専用線などを用いることを前提とすれば問題がないと思われる。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

(2)時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース(NTP サーバ)と安全な通信路上で定期的に同期していること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

(3)内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものが多かった。内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

(4)暗号技術の脆弱化に対する対策

TOE は、暗号技術が使用された「時刻監査証明書」を作成・配付・蓄積する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「時刻監査証明書」の信頼性が失われる可能性がある。このような脅威に関しては、「時刻監査証明書」の所有者による長期保証の必要性があることが明らかになった。

2.1.2 TA1

TA1 は、認証連鎖方式を採用したTAの時刻配信サーバである。評価対象は、時刻配信サーバのサブセットである。具体的には、図 2-2における白地のコンポーネントから構成される領域である。

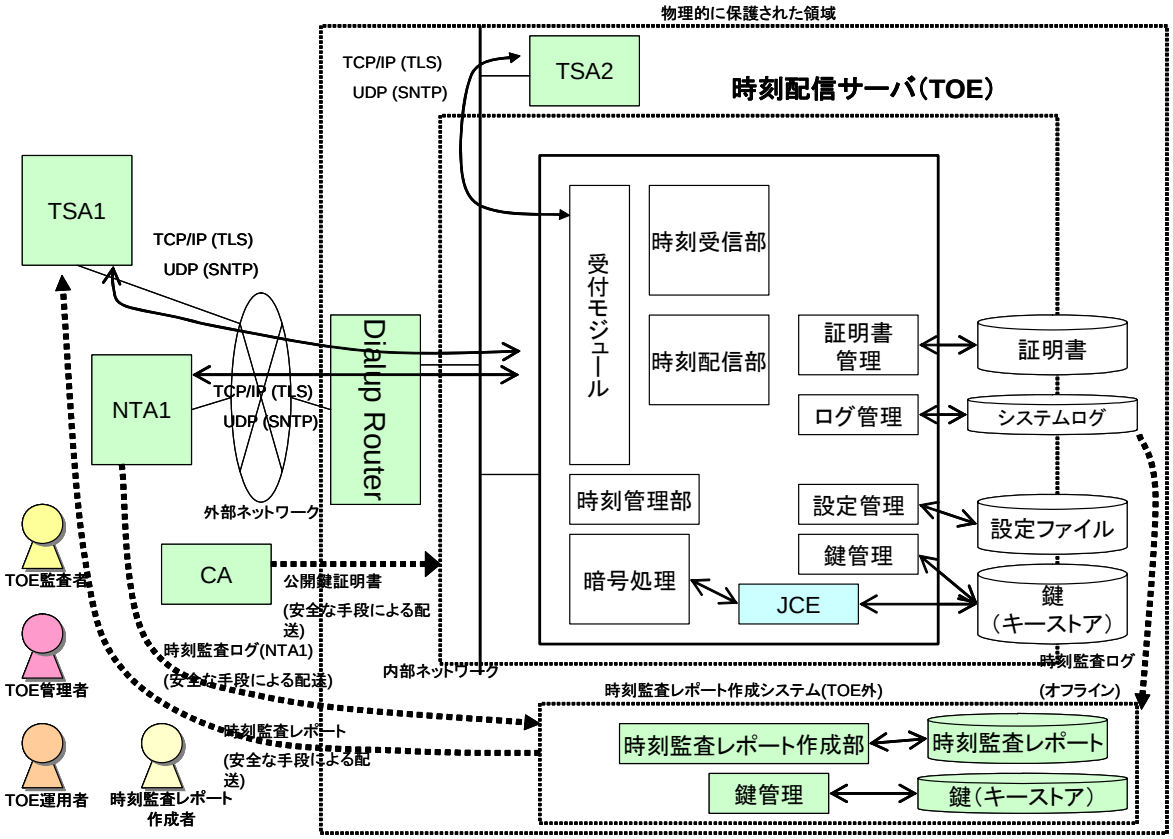

図 2-2:TA1 のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書(TOE: TA1)』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

(1)暗号技術コンポーネントの安全性

TOE は、署名や検証処理において暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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。』に準拠していることを確認した。

また、署名と検証以外で使用される暗号技術コンポーネントに関しては、「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)」に掲載されていないものも存在した。この場合、別の担保により安全性が保たれていることを確認した。例えば、TOE と TSA1 の間は、MD5 を用いた SNTP が使用されるが、この時の通信回線は、成りすまし・改ざん・盗聴などを防ぐ専用線などを用いることを前提とすれば問題がないと思われる。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

(2)時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース(NTA1)と安全な通信路上で定期的に同期していること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

(3)内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものが多かった。内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

(4)暗号技術の脆弱化に対する対策

TOE は、暗号技術が使用された「時刻監査証明書」を作成・配付・蓄積する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「時刻監査証明書」の信頼性が失われる可能性がある。このような脅威に関しては、「時刻監査証明書」の所有者による長期保証の必要性があることが明らかになった。

2.2 配信時刻高精度高信頼化サブシステム-3

本サブシステムでは、二つの TOE に対してセキュリティ評価を実施した。

2.2.1 NTA2

NTA2 は、仮想的な国家時刻標準機関の時刻配信サーバである。このサーバは、時刻リンク方式を採用している。評価対象は、時刻配信サーバのサブセットである。具体的には、図 2-3における白地のコンポーネントから構成される領域である。

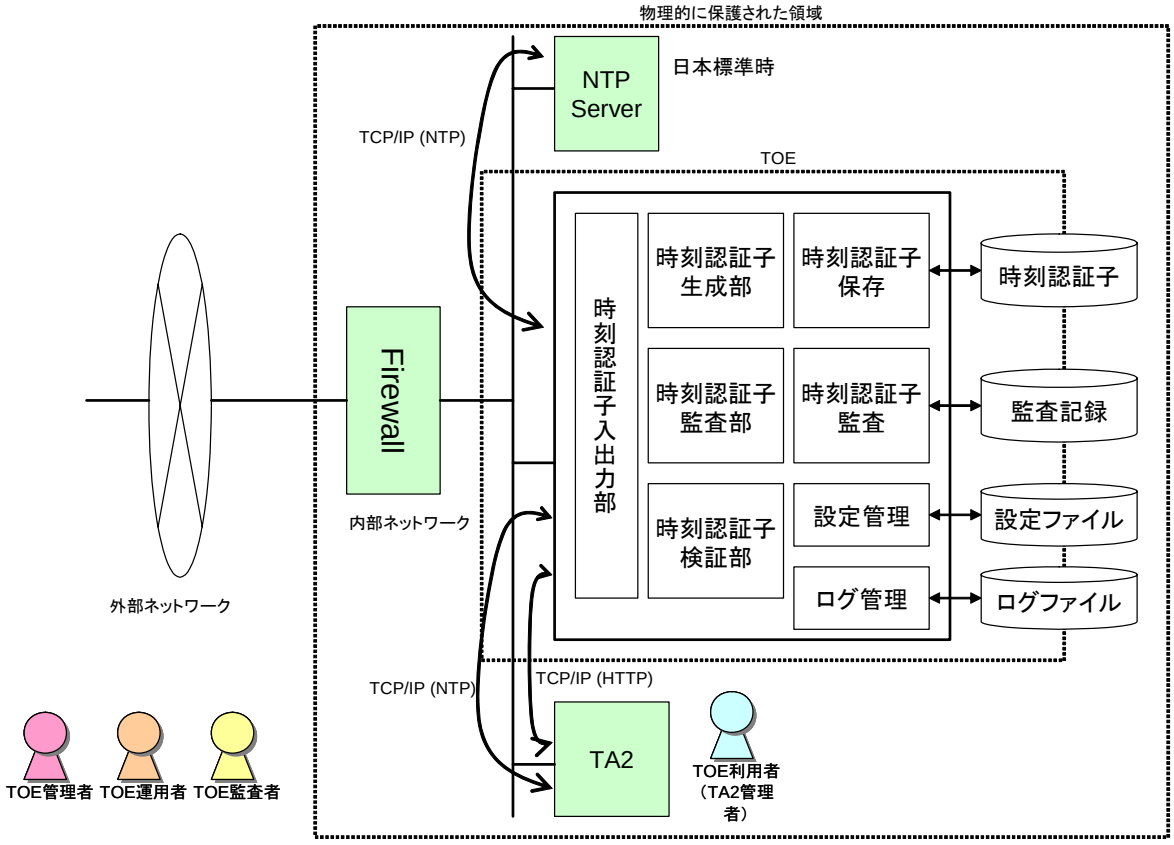

図 2-3:NTA2 のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリ

ティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書（TOE: NTA2）』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

（1）暗号技術コンポーネントの安全性

TOE は、暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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。』に準拠していることを確認した。

また、上記以外で使用される暗号技術コンポーネントに関しては、「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)」に掲載されていないものも存在した。この場合、別の担保により安全性が保たれていることを確認した。例えば、TOE と TA2 の間は、MD5 を用いた NTP が使用されるが、この時の通信回線は、成りすまし・改ざん・盗聴などを防ぐ専用線などを用いることを前提とすれば問題がないと思われる。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

（2）時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース（NTP サーバ）と安全な通信路上で定期的に同期していること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

（3）内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものが多かった。内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

（4）暗号技術の脆弱化に対する対策

TOE は、暗号技術が使用された「時刻認証子」を作成・配付・蓄積する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「時刻認証子」の信頼性が失われる可能性がある。このような脅威に関しては、「時刻認証子」の所有者による長期保証の必要性があることが明らかになった。

2.2.2 TA2

TA2 は、時刻リンク方式を採用した時刻配信サーバである。評価対象は、時刻配信サーバのサブセットである。具体的には、図 2-4における白地のコンポーネントから構成される領域である。

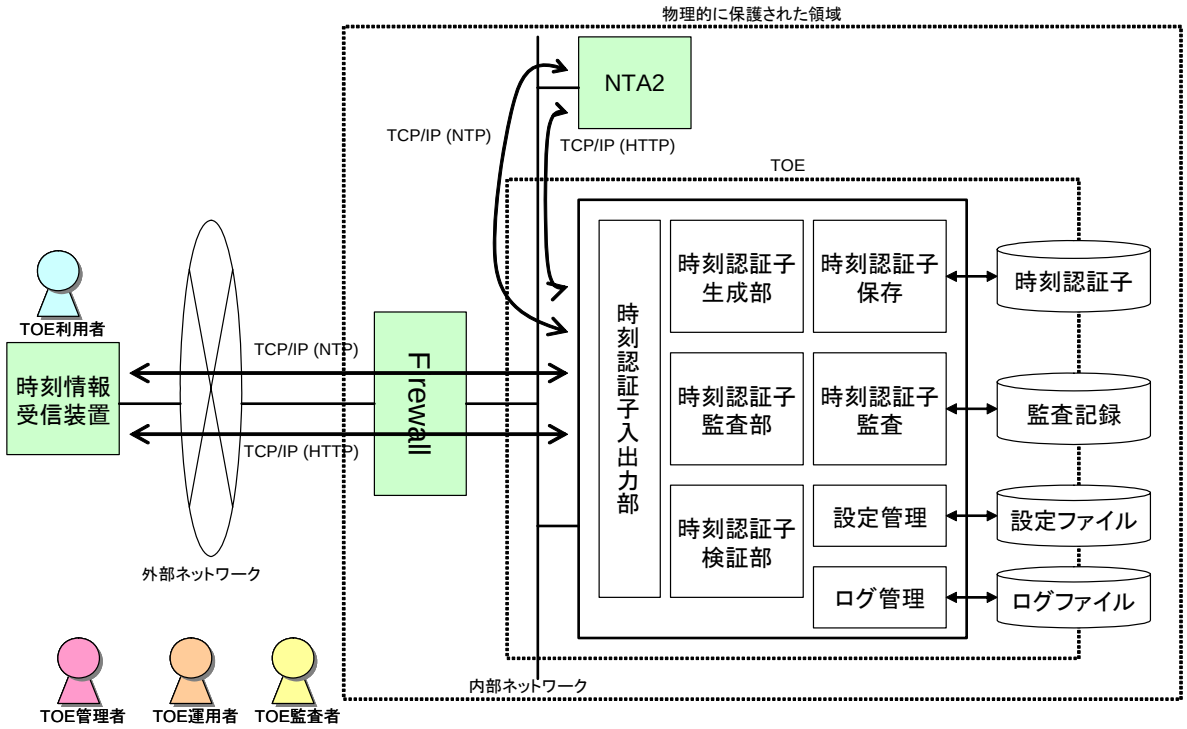

図 2-4:TA2 のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書(TOE: TA2)』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

(1)暗号技術コンポーネントの安全性

TOE は、暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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。』に準拠していることを確認した。

また、上記以外で使用される暗号技術コンポーネントに関しては、「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)」に掲載されていないものも存在した。この場合、別の担保により安全性を確保しなければならないことを明確化した。例えば、TOE と時刻受信装置の間は、インターネットを前提としており、MD5 を用いた NTP が使用されている。この場合、NTP パケットの改ざんなどの脅威が存在するため、今後は、TOE と時刻受信装置の間を(1)成りすまし・改ざん・盗聴などを防ぐ専用線にする、あるいは、(2)SSL/TLS などの安全性が確保された通信路を用いる、などの対策が必要である。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

(2)時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース(NTA2)と安全な通信路上で定期的に同期していること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

(3)内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものが多かった。内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

(4)暗号技術の脆弱化に対する対策

TOE は、暗号技術が使用された「時刻認証子」を作成・配付・蓄積する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「時刻認証子」の信頼性が失われる可能性がある。このような脅威に関しては、「時刻認証子」の所有者による長期保証の必要性があることが明らかになった。

2.3 高速・高セキュリティタイムスタンプ付与・検証サブシステム-1

本サブシステムでは、一つの TOE に対してセキュリティ評価を実施した。

TSA1 は、リンクトークン方式のタイムスタンプトークンを発行するタイムスタンプサーバである。評価対象は、タイムスタンプサーバのサブセットである。具体的には、図 2-5における白地のコンポーネントから構成される領域である。

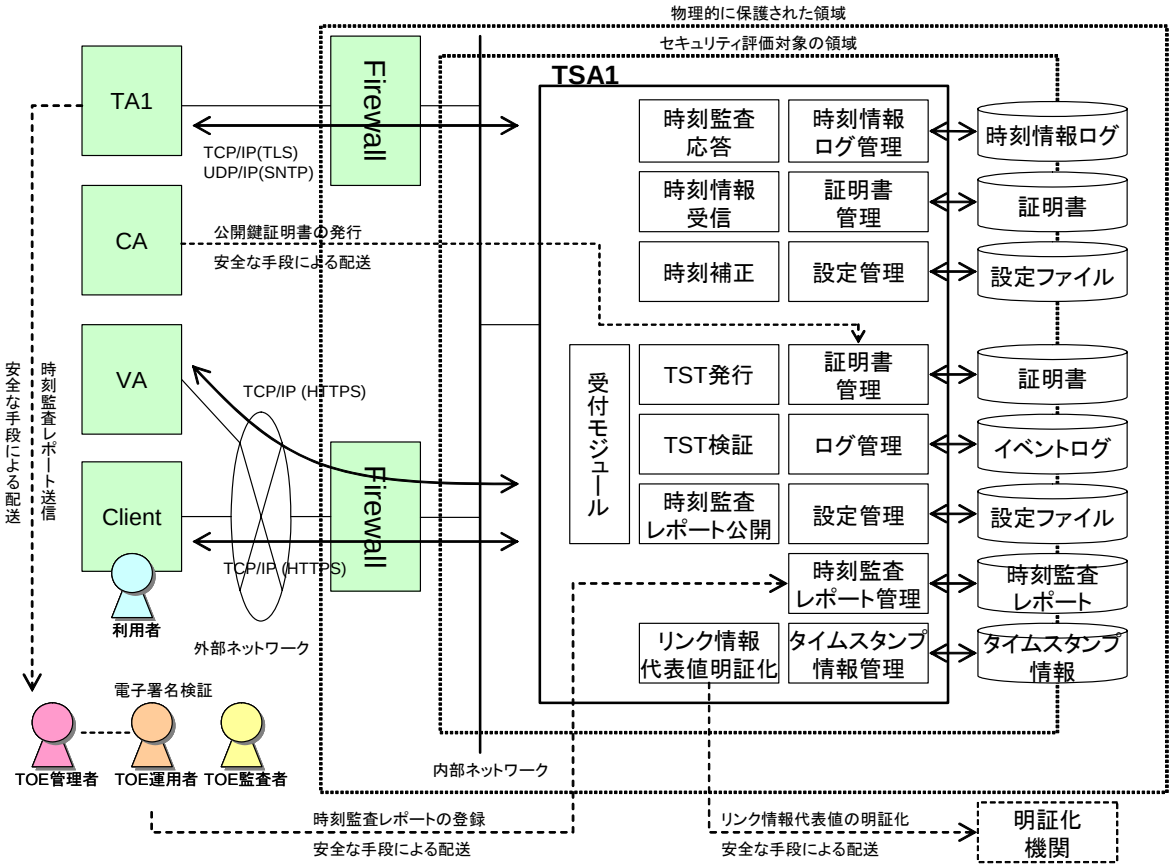

図 2-5:TSA1 のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書（TOE: TSA1）』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

（1）暗号技術コンポーネントの安全性

TOE は、タイムスタンプ発行などにおいて暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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。』にほぼ準拠していることを確認した。例外は、TOE と TA1 間の SNTP に使用される MD5 である。この場合、改ざん・成りすまし・盗聴などを防ぐ専用線を利用することにより、安全性が確保されていることを確認した。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

（2）時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース（TA1）と安全な通信路上で定期的に同期していること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

（3）内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものが多かった。内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、が考えられる。

（4）将来的にタイムスタンプが検証できなくなる脅威に対する対策

TOE は、暗号技術が使用された「タイムスタンプ（タイムスタンプトークン）」を作成・送信・蓄積する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「タイムスタンプ」の信頼性が失われる可能性がある。また、本 TOE を使用したタイムスタンプ事業者及び関連するエンティティ・装置などの存在が仮定できなくなる可能性もある。このような状況を踏まえ、脅威を洗い出し、対策を明確化した。

2.4 高速・高セキュリティタイムスタンプ付与・検証サブシステム-2

本サブシステムでは、一つの TOE に対してセキュリティ評価を実施した。

TSA2 は、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タイムスタンプサーバである。評価対象は、タイムスタンプサーバのサブセットである。具体的には、図 2-6における白地のコンポーネントから構成される領域である。

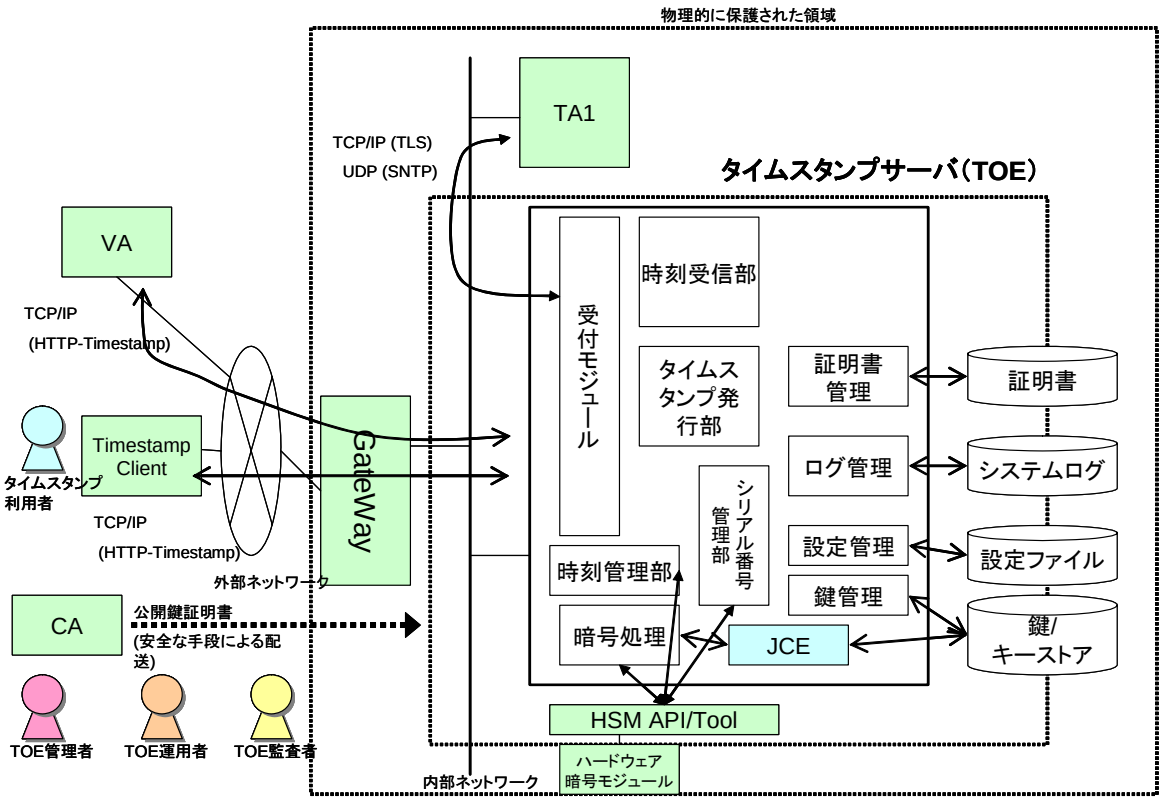

図 2-6:TSA2 のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書（TOE: TSA2）』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

（1）暗号技術コンポーネントの安全性

TOE は、タイムスタンプ発行などにおいて暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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)」に記載されたアルゴリズムによって実装される。』に準拠していることを確認した。例外は、TOE とTA1 間の SNTP に使用される MD5 である。この場合、改ざん・成りすまし・盗聴などを防ぐ専用線を利用することにより、安全性が確保されていることを確認した。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

また、最近報告されている SHA-1 の脆弱化（衝突困難性の特性に関わる脆弱化）の対策として、TOE は、タイムスタンプクライアントから送信される電子データのメッセージダイジェストが SHA-1 であるものを受け付けないという安全対策がとられていることを確認した。

（2）時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース（TA1）と安全な通信路上で定期的に同期していること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

（3）内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものが多かった。内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

(4)将来的にタイムスタンプが検証できなくなる脅威に対する対策

TOE は、暗号技術が使用された「タイムスタンプ(タイムスタンプトークン)」を作成・送信する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「タイムスタンプ」の信頼性が失われる可能性がある。また、本 TOE を使用したタイムスタンプ事業者及び関連するエンティティ・装置などの存在が仮定できなくなる可能性もある。このような状況を踏まえ、脅威を洗い出し、対策を明確化した。

2.5 時刻認証基盤用信頼性保証サブシステム

本サブシステムでは、一つの TOE に対してセキュリティ評価を実施した。
CAは、公開鍵証明書サーバとディレクトリサーバからなるシステムである。図 2-7における白地のコンポーネントから構成される領域である。

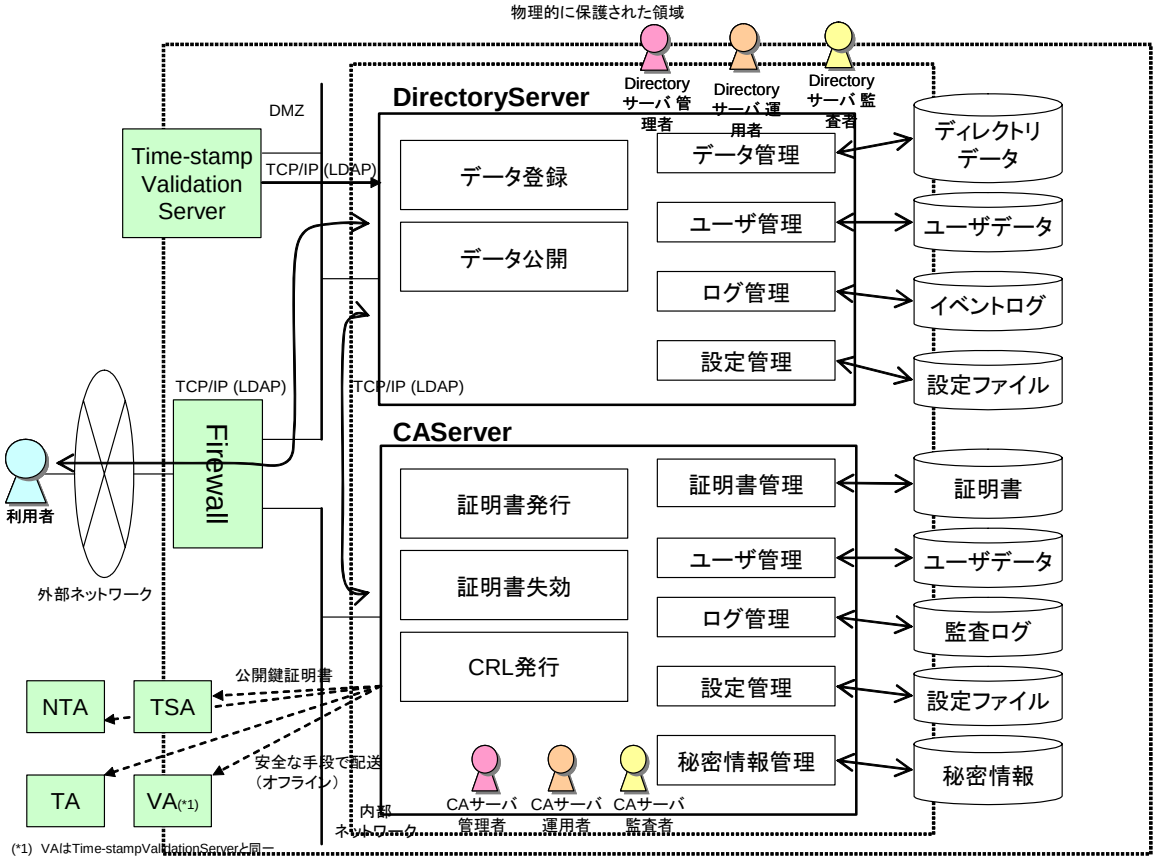

図 2-7:CA のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書(TOE: CA)』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

（1）暗号技術コンポーネントの安全性

TOE は、公開鍵証明書発行処理などにおいて暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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。』に準拠していることを確認した。

「電子政府推奨暗号リスト」に掲載されていない暗号アルゴリズムは、TOE の「秘密情報格納ディレクトリの暗号」に使用される DES(56 ビット)である。この場合の対策としては、TOE 操作における合議制操作、厳密な入退出管理などが明確化された。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

（2）時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース（NTP サーバ）と定期的に同期させる運用、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

（3）内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものもあった。基本的に、内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

（4）暗号技術の脆弱化に対する対策

TOE は、暗号技術が使用された「公開鍵証明書」と「公開鍵証明書失効リスト」作成する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「公開鍵証明書」や「公開鍵証明書失効リスト」の信頼性が失われる可能性がある。このような脅威に対しては、「公開鍵証明書」、あるいは、「公開鍵証明書失効リスト」の長期保証の必要性が明確化された。

2.6 複数方式タイムスタンプ検証サブシステム

本サブシステムでは、一つの TOE に対してセキュリティ評価を実施した。
VAは、タイムスタンプ検証サーバである。評価対象は、図 2-8における白地のコンポーネントから構成される領域である。

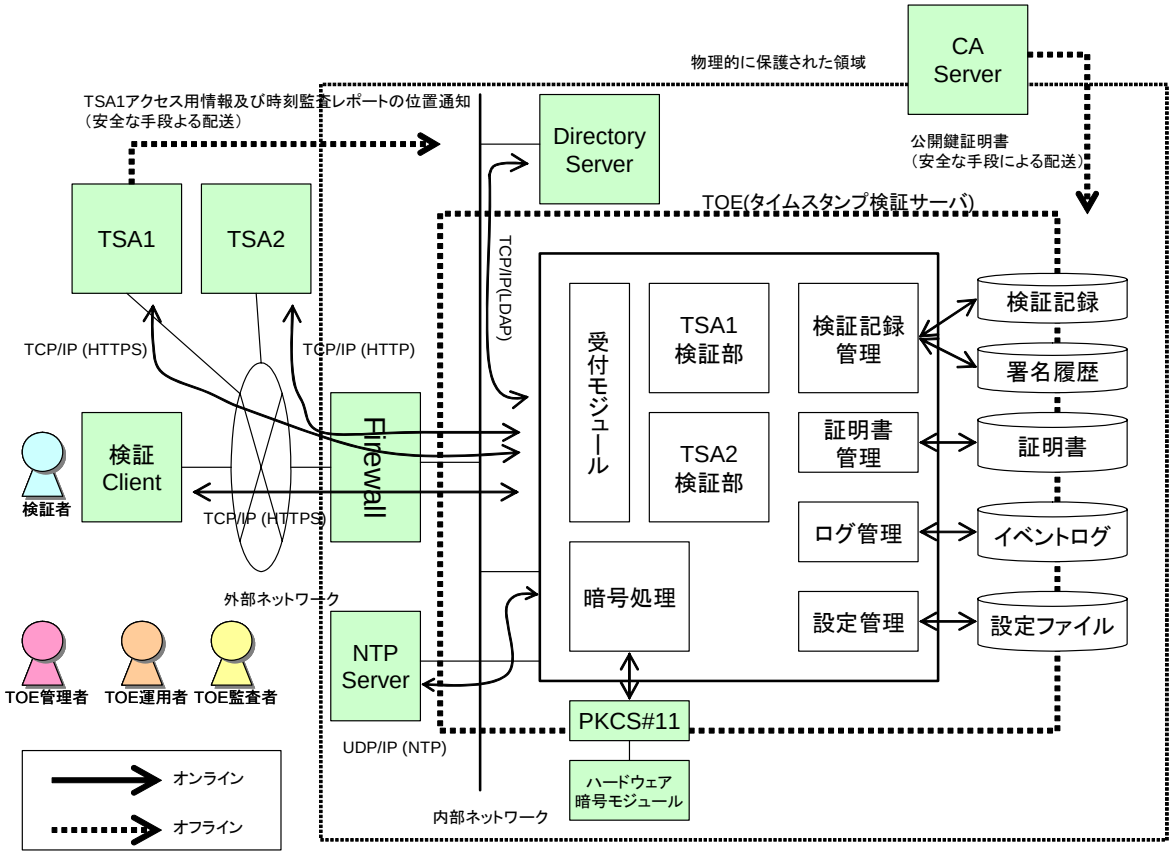

図 2-8:VA のシステム構成

上記のTOEに対して、二つの視点からセキュリティ評価を実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。それぞれの視点に対して、表 1-2に示すセキュリティ評価手順を実施した。その結果、セキュリティ環境が示すセキュリティ課題に対して、実装されたセキュリティ対策機能、今後実装すべきセキュリティ対策などの見通しを明確化した。セキュリティ評価の詳細内容は、別冊である『セキュリティ評価報告書（TOE: VA）』に示される。

本評価報告書では、セキュリティ評価における補足事項を以下に示す。

（1）暗号技術コンポーネントの安全性

TOE は、公開鍵証明書発行処理などにおいて暗号技術コンポーネントを使用する。組織のセキュリティポリシーの一つである『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。』に準拠していることを確認した。

暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。

（2）時刻情報の安全性

TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース（NTP サーバ）と定期的に同期させる運用、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

（3）内部不正の対策

内部不正に対する TOE の対策機能は、未実装のものが多かった。基本的に、内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

（4）暗号技術の脆弱化に対する対策

TOE は、暗号技術が使用された「タイムスタンプ検証結果」作成する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「タイムスタンプ検証結果」の信頼性が失われる可能性がある。このような脅威に対しては、「タイムスタンプ検証結果」の所有者は、長期保証の必要性があることが明確化された。

3 まとめと提言

本章では、統合化プラットフォームシステムに対するセキュリティ評価のまとめと提言について述べる。

3.1 まとめ

セキュリティ評価に関する国際標準 ISO/IEC 15408 の考え方に基づいて、統合化プラットフォームシステムのセキュリティ評価を実施した。NICT が策定した『統合化プラットフォーム・セキュリティ評価ガイドライン 0.9 版』に従い、統合化プラットフォームシステムのサブシステム毎の評価対象（Target of Evaluation: TOE）を明確化し、その TOE に対してセキュリティ評価を実施した。

セキュリティ評価は大きく二つの視点で実施した。一つは、内部不正を考慮しないセキュリティ評価、もう一つは、内部不正を考慮したセキュリティ評価である。また、タイムスタンププラットフォーム技術に特有と思われる項目として、（1）TOE が使用する暗号技術コンポーネントに関わる課題、（2）時刻情報に関するセキュリティの課題、（3）タイムスタンプが将来的に検証できなくなる状況を想定したセキュリティの課題も考察した。

セキュリティ評価の結果、統合化プラットフォームシステムにおけるセキュリティ課題に対する対策の実施を確認するとともに、一部のセキュリティ課題に対する対策の見通しを明らかにすることができた。

3.2 提言

3.2.1 実運用への提言

統合化プラットフォームシステムは、タイムスタンププラットフォーム技術の研究開発のための試作品である。これらの試作品を実運用で使用する場合は、本セキュリティ評価で明らかになった対策、あるいは、同等な対策を確実に実施することが望ましいと考える。

3.2.2 タイムビジネス信頼・安心認定制度への提言

本セキュリティ評価で得られた知見は、先行するタイムビジネスへの適用が考えられる。（財）日本データ通信協会は、「タイムビジネス信頼・安心認定制度」を 2005 年 2 月より、実施している。この制度は、時刻配信事業者やタイムスタンプ事業者などの業務を技術・運用・ファシリティ・システム安全性などの観点から認定するものであり、事業者の安全・安心を担保するものであると考えられる。

今後は、本セキュリティ評価で得られた知見をこの制度へフィードバックすることが考えられる。フィードバックとしては、以下のことが想定される。

直接的には、

- 既存の審査項目への追加、補強、あるいは、修正など
- 新規の審査項目の追加

間接的には、

- 安全性に関わる審査項目の拠り所となる資料(セキュリティ課題が明確になっている)としての反映

が、考えられる。

3.2.3 PP 策定への提言

本セキュリティ評価は、ISO/IEC 15408 の考え方に基づいて実施された。本評価の知見は、タイムスタンププラットフォーム技術に関わる各装置、例えば、タイムスタンプサーバ装置、時刻配信サーバ装置、検証サーバ装置、などに対するPP(Protection Profile)策定に役立つものと考える。