資料１３－２

リモート署名ガイドライン(案)の状況

2019年10月28日

日本トラストテクノロジー協議会（JT2A）
小川 博久

1.状況報告

1 目的・背景
2 用語
3 ガイドラインの構成と想定読者
4 リモート署名の概要
5 セキュリティ検討事項
6 セキュリティ要件
7 設置・環境
8 組織・運営
9 参照情報
附録A1. 電子署名法研究会における重要検討項目の考え方について
附録B1. 鍵管理について
附録C1. 利用停止処理ついて

1章 目的・背景 ～ 3章 本ガイドラインの構成と想定読者

1 目的・背景
2 用語
3 ガイドラインの構成と想定読者
- 3.1 本ガイドラインの構成
- 3.2 本ガイドラインの想定読者
- 3.3 重要項目（署名鍵の生成・インポート・活性化）

3.2 本ガイドラインの想定読者

- リモート署名の利用者：電子契約などを利用する契約の当事者　など
- リモート署名の事業者：電子契約事業者（設計開発事業者、管理運用事業者）　など

章	事業者	利用者
1章　目的・背景	○	○
2章　用語	○	○
3章　ガイドラインの構成と想定読者	○	○
4章　リモート署名の概要	○	○
5章　セキュリティ検討事項	○	
6章　セキュリティ機能要件	○	
7章　設置・環境	○	
8章　組織・運営	○	
9章　参照情報	○	○
附録	○	

3.3 ガイドラインの重要項目

3.3 重要項目（署名鍵の生成・インポート・活性化）

6 セキュリティ要件

6.1 一般的セキュリティ要件

→　リモート署名事業者が共通で対策すべき内容
→　一部（署名鍵の活性化のみ）最低限/推奨/附帯の定義

6.2 署名活性化モジュール（SAM※1）のセキュリティ要件

→　リモート署名事業者が共通で対策すべき内容
→　一部（署名鍵のインポートのみ）最低限/推奨/附帯の定義

6.3 署名値生成モジュール（Cm※2）のセキュリティ要件

→　リモート署名事業者が共通で対策すべき内容
→　一部（署名鍵の生成のみ）最低限/推奨/附帯の定義

※1：Signature Activation Module
※2：Cryptographic module

3.3 ガイドラインの重要項目

3.3 重要項目（署名鍵の生成・インポート・活性化）

項目	最低限	推奨	附帯
鍵生成	• 署名鍵の生成可能（HSM※1に限らない）	• 署名鍵の生成可能（HSMのみ可能であり、署名鍵の保管はHSMに限定）	• 署名鍵の生成可能（欧州の署名生成デバイスの評価・認証取得品※2のみ可能）
鍵設置	• 署名鍵のインポート可能	• 認定認証事業者など信頼できるCA（認証局）からの署名鍵のみインポート可能	• 署名鍵のインポート不可
鍵認可（活性化）	• 鍵認可は単要素認証 • 利用者認証で鍵認可を行ってもよい	• 鍵認可は複数要素認証 • 利用者認証と別に鍵認可を行わなければいけない	• 推奨に追加して、評価・認証取得※3し、耐タンパー領域に実装した署名鍵活性化モジュールの鍵認可が必要

※1：Hardware Security Moduleの略称。耐タンパ性を有する頑強なモジュールであり、CMVPの認証取得製品。
※2：署名生成デバイス（SCDev）の欧州規格。
※3：署名活性化を行うモジュール（SAM）の欧州規格（耐タンパな環境での設置が必須）

4章 リモート署名の概要 ～ 5章 セキュリティ検討事項

6章 セキュリティ要件

6 セキュリティ要件

6.1 一般的セキュリティ要件
- 6.1.1 役割・組織の管理
- 6.1.2 識別及び認証
- 6.1.3 システムへのアクセスコントロール
- 6.1.4 監査及びログ
- 6.1.5 アーカイブ
- 6.1.6 内部不正
- 6.1.7 バックアップ・リカバリ　※追加検討
- 6.1.8 コアコンポーネント　※追加検討

6.2 署名活性化モジュール（Signature Activation Module）のセキュリティ要件
- 6.2.1 登録
- 6.2.2 署名利用時
- 6.2.3 利用停止

6.3 署名値生成モジュール（Cryptographic module）のセキュリティ要件

6章 セキュリティ要件

6.1 一般的セキュリティ要件

SRG_M.1.8J 特権を持つ役割のユーザは適切に指名を受け、訓練を受けたものであること。

SRG_M.1.9J 特権をもつ役割のユーザのみが、ハードウェアへの物理的にアクセス可能であり、リモート署名サービスの管理ができること

SRG_AA.1.1J 少なくとも以下のイベントを記録すること：

- 重要なリモート署名サービス環境、鍵管理イベント（生成、使用及び破壊）
- ユーザ署名イベント（署名者の署名鍵を使った正常な署名及びDTBS/Rリクエスト管理）
- SAP中のユーザ認証
- リモート署名サービスによる署名者のSAD管理
- 監査データ生成機能の開始及び停止
- 監査パラメータの変更

6.2 署名活性化モジュール（Signature Activation Module）のセキュリティ要件

OTSAM_UR.5 SIGNATURE_INTEGRITY

SAMは、SAM内部で署名を改変できないことを保証しなければならない。

OTSAM_UR.2 SAP

SAMは、以下を提供するシグネチャアクティベーションプロトコル（SAP）のサーバ側エンドポイントを実装しなければならない。

- 署名者認証
- 送信されたSADの整合性
- 少なくとも機密情報を含むSADの要素の機密性
- リプレイ、バイパス、偽造からの保護

6.3 署名値生成モジュール（Cryptographic module）のセキュリティ要件

OTCM_UR.2 Algorithms

CMは、信頼できる第三者機関によって使用に適していると認められ承認された暗号アルゴリズム※を提供しなければいけない。

※電子署名法施行規則第二条、及びCRYPTREC暗号リスト等

OTCM_UR.8 DataMod

CMは、クライアントアプリケーションとCMの間の伝送中に機密データ（署名されるデータ、認証/許可データ、または公開鍵証明書など）の保全性を保護するために使用できる安全なチャネルをクライアントアプリケーションに提供しなければいけない。

この対策方針は6.1.3の一部として求められる対策である。

7 章 設置・環境 ～ 9 章 参照情報

7 設置・環境

7.1 物理的セキュリティの考え方

7.2 情報セキュリティポリシーセキュリティを保つべき領域

- 7.2.1 物理セキュリティの境界
- 7.2.2 物理的入退管理策
- 7.2.3 オフィス、部屋及び施設のセキュリティ
- 7.2.4 外部及び環境の脅威からの保護
- 7.2.5 セキュリティを保つべき領域での作業

7.3 装置

- 7.3.1 装置の設置及び保護
- 7.3.2 資産の移動
- 7.3.3 構外にある装置及び資産のセキュリティ
- 7.3.4 無人状態にある利用者装置
- 7.3.5 装置のセキュリティを保った処分又は再利用

8 組織・運営

8.1 職務の分離

8.2 事業継続管理

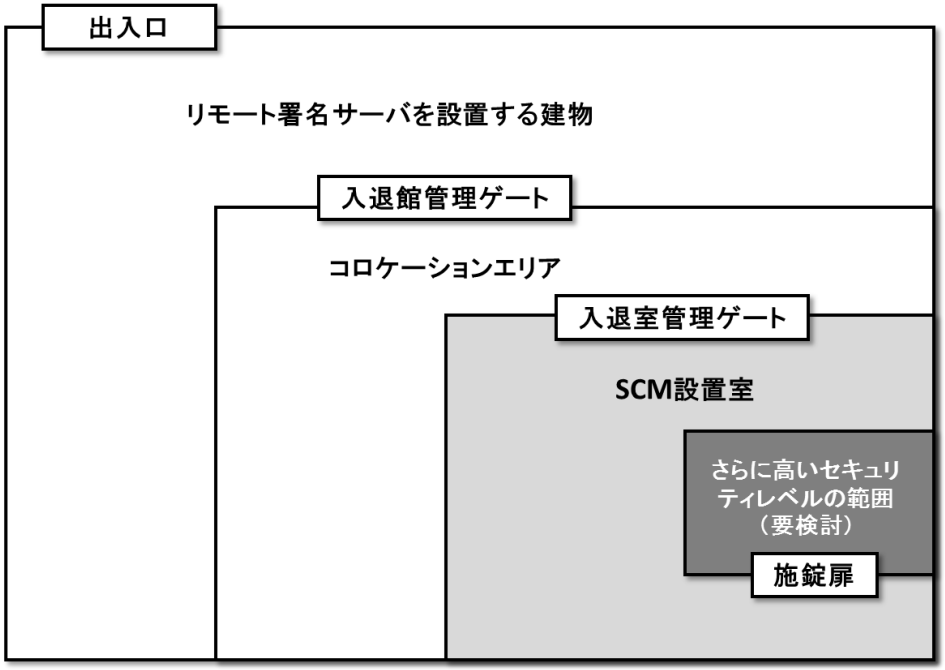
8.3 コンプライアンス

9 参照情報

7章 設置・環境 ～ 9章 参照情報

7.2.1 物理セキュリティの境界

- 「リモート署名サーバ」を設置する建物、当該建物内の「CM設置室」、及びその「コロケーションエリア」を物理的セキュリティ境界として定める。
- 「リモート署名サーバ」を設置する建物（又は敷地）、当該建物内の「CM設置室」、及び「CM設置室」の「コロケーションエリア」を物理的セキュリティ境界として定める。
- 「CM設置室」に、より高いセキュリティレベルが要求される場合に「コロケーションエリア」を設けることがある。「CM設置室」と「コロケーションエリア」がある場合、「コロケーションエリア」を通過しなくては「CM設置室」にアクセスすることはできないものと定義する。



附録A1 ～ 附録C1

附録A1．電子署名法研究会における重要検討項目の考え方について

A1.1　署名鍵活性化
A1.2　署名結果の確認
A1.3　システムログと監査ログ
A1.4　CSC クラウド署名コンソーシアムのAPI仕様
A1.5　署名鍵の生成環境の区別

附録B1．鍵管理について

B1.1　鍵の生成
B1.2　鍵のインポート
B1.3　鍵の属性管理
B1.4　鍵の利用
B1.5　鍵のエクスポート
B1.6　鍵の破棄
B1.7　鍵の利用に関するログ

附録C1．利用停止処理ついて

参考：リモート署名ガイドの構成

- ガイドラインの構成とEN規格との関係