リモート署名ガイドライン

パートIII．署名値生成モジュール

日本トラストテクノロジー協議会（JT2A）

第一版：2020 年 4 月 30 日

目　　次

1 署名値生成モジュールの概要

リモート署名事業者（RSSP）で実装する暗号モジュール・署名値生成モジュール（CM）の概要を以下に示す。署名値生成モジュールは、署名者または署名生成アプリケーション（SCA）との鍵認可の処理に基づいて、署名活性化モジュール（SAM）によって署名鍵が活性化した状態で署名値を生成するモジュールである。本ガイドラインでは、鍵認可を検討対象とするが、利用認証は検討対象外とする。下図において示したとおり利用認証のパターンは３つあり（図中の青線）、鍵認可のパターンは４つある（図中の橙色線）。下図において青線で示した利用認証の対策については、リモート署名の対象となる情報の重要度やリスク分析の結果を考慮して検討する必要がある。なお、下図は論理的な構成例である。

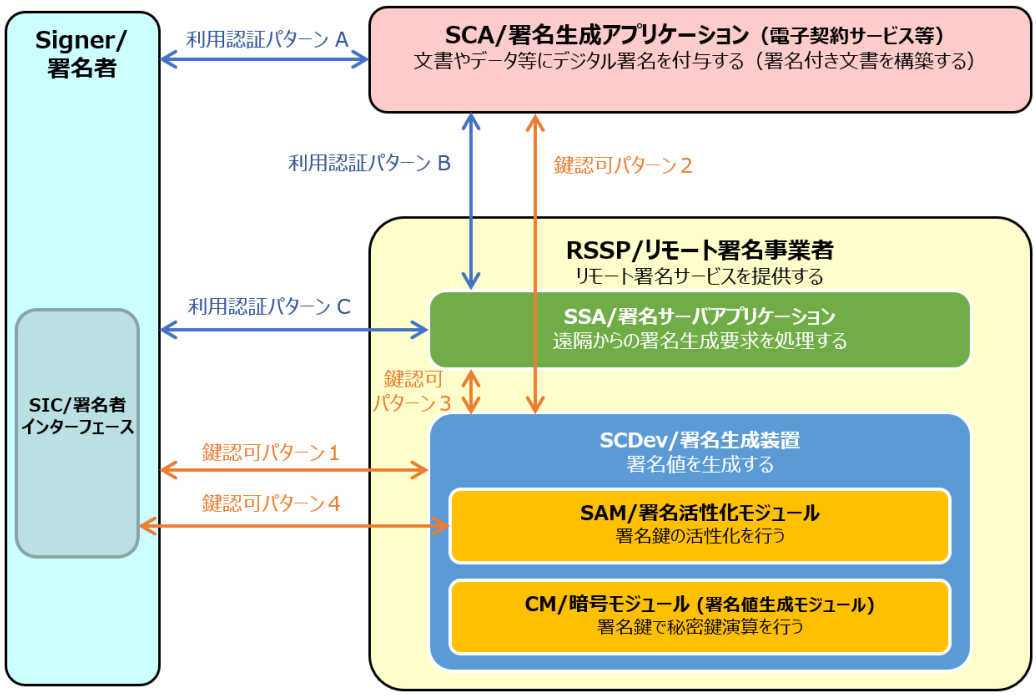

図 1-1　リモート署名サービスの構成例と本ガイドラインのスコープ

なお、用語については、本ガイドライン・パート I の 2. 用語を参照。

2 署名値生成モジュールにおいてセキュリティ対策を検討すべき事項

以下に本ガイドライン・パートⅠの 6 章のセキュリティ検討事項から署名値生成モジュールに関する脅威のみを示す。

1. 攻撃者は平文の共通鍵／秘密鍵に不正にアクセスし開示する。
2. 攻撃者は共通鍵／秘密鍵を導出する。
3. 攻撃者は CM 格納時に、鍵及び鍵の属性を不正に変更する。
4. 攻撃者は CM 管理時に、鍵を誤用（許可されてない暗号機能・署名機能に利用）する。
5. 攻撃者は鍵を乱用（許可されていない鍵を利用）する。
6. 攻撃者はクライアントアプリケーションデータから送信中の機密データを不正に開示する。
7. 攻撃者はクライアントアプリケーションデータから送信中の機密データを不正に変更する。
8. 攻撃者は CM ハードウェアまたはソフトウェアの機能不全を発生させる。(温度、電力、HW の故障、SW の破損)

3 署名値生成モジュールのセキュリティ機能要件

2 章のセキュリティ検討事項に対する署名値生成モジュールに関するセキュリティ機能要件を示す。

1. 平文の秘密鍵を CM の外部に持ち出し利用できないようにしなければならない。（鍵が後述する本章（本ガイドライン・パートⅢの 3 章）の 9 の方法で安全にエクスポートされている場合を除く)。

2 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※を提供しなければならない。
※電子署名法施行規則第二条、及び CRYPTREC 暗号リスト等

3 鍵および重要な属性（秘密または公開）は、その完全性が許可なく変更されることがないよう、CM によって保護しなければならない。

4 CM は、CM の使用を許可する前に、次のすべてのサブジェクトに対して認証/許

可のチェックを実行しなければならない。

- CM の管理者
- CM の暗号機能を利用するアプリケーション(セキュアチャネルを使用するクライアントアプリケーション)。
- 秘密鍵の利用者である署名者

※この対策方針は本ガイドライン・パートⅠの 6 章の一部として求められる対策である。

5　任意の鍵（秘密または公開）は、それが使用されることが許可されている暗号機能または操作（例えば暗号化または署名等）の目的が定義されていなければならない。

6　CM は、秘密鍵を使用するために承認と再承認が必要とされる場合に、明確に規定された制限を定義し適用することを要求しなければならない。
※この対策方針は本ガイドライン・パートⅠの 6 章の一部として求められる対策である。

7　CM は、クライアントアプリケーションと CM との間の伝送中に機密データ（認証/許可データなど）の機密性を保護するために使用できるクライアントアプリケーションへの安全なチャネルを提供しなければならない。
※この対策方針は本ガイドライン・パートⅠの 6 章の一部として求められる対策である。

8　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）の完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ならない。
※この対策方針は本ガイドライン・パートⅠの 6 章の一部として求められる対策である。

9　CM は、送信中のデータの機密性と完全性を保護する安全な方法を使用することによってのみ、秘密鍵のインポートとエクスポートを許可しなければならない。なお、利用者属性等が割り当てられた秘密鍵はインポートまたはエクスポートできないことが望ましい。※この対策方針は本ガイドライン・パートⅠの 6 章の一部として求められる対策である。

10　秘密鍵を含む、署名者データをバックアップするために CM によって提供される

いかなる方法も、データのセキュリティを保護し、許可された管理者によって制御されなければならない。
※この対策方針は本ガイドライン・パートⅠの 6 章の一部として求められる対策である。

11　鍵、認証/許可データに使用する乱数、及びこれらの目的で使用される他の乱数ジェネレータのシードデータとして使用するために生成され、クライアントアプリケーションに提供される乱数は、乱数が予測不可能であり、十分なエントロピーがなければならない。

12　CM は、改ざんからセキュリティ機能を保護するための機能を提供しなければならない。特に CM は、意図された環境の範囲内でのあらゆる物理的操作を CM の管理者が検出できるようにしなければならない。

13　CM は、以下のような他のセキュリティプロパティの弱体化または失敗を引き起こす可能性のある障害を検出しなければならない。

- 通常の動作範囲外の環境条件（温度および電力を含む）。
- 重要な CM ハードウェアコンポーネント（RNG[3]を含む）の故障。
- CM ソフトウェアの破損。

また、障害が検出されると、CM はそのセキュリティと、それに含まれ管理されているデータのセキュリティを維持するための措置をとらなければならない。

14　CM は、セキュリティ関連イベントの監査記録を作成し、イベントの詳細とそのイベントに関連するサブジェクトを記録しなければならない。
CM は、監査ログの改ざん防止（防止または検出）を提供することによって、監査レコードが偶発的または悪意のあるレコードの削除または変更から保護されることを保証しなければならない。
※この対策方針は本ガイドライン・パートⅠの 6 章の一部として求められる対策である。

15　署名鍵のインポート

対策レベル	対策事項
レベル 1	• 署名者を確認した署名鍵をインポートしなければならない。

[3] 乱数生成器

レベル 2	• 上記のレベル 1 に追加し、署名鍵のインポートは、電子署名法に基づく認定認証事業者など信頼できる CA(認証局)からのみに限定しなければならない。
レベル 3	• 署名鍵をインポートしてはならない。

16　署名鍵生成

対策レベル	対策事項
レベル 1	• 署名鍵ペアの生成は、本章（本ガイドライン・パートⅢの 3 章）の 2 で指定した暗号アルゴリズム、鍵長、パラメータで生成しなければならない。
レベル 2	• 上記のレベル 1 に追加し、署名鍵ペアの生成は、第三者の評価や認証を受けた HSM で生成しなければならない。
レベル 3	• 署名鍵ペアの生成は、国際的に承認されうる評価や認証を受けた HSM 及び本章（本ガイドライン（パートⅢ））の要件に適合したデバイスで生成しなければならない。

17　署名鍵保持

対策レベル	対策事項
レベル 1	• 署名鍵に対する適切なアクセス制御策を講じ、ストレージに格納しなければならない。
レベル 2	• HSM のセキュア な境界内で署名鍵を保持し、HSM 内でのみ署名生成処理を実行しなければならない。 • HSM のセキュア な境界を越えた、署名鍵のエクスポートをしてはならない。
レベル 3	• レベル 2 と同じ

4 参照情報

[1] EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

[2] ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

[3] ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

[4] Cloud Signature Consortium (CSC), Architectures, Protocols and API Specifications for Remote Signature applications

[5] 電子署名及び認証業務に関する法律

[6] 電子署名及び認証業務に関する法律施行規則

附録１　鍵管理等に関する参考情報

リモート署名の検討については、経済産業省の「平成２８年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））報告書」において、リモート署名のガイドラインを作成する際には、より詳細な検討を行うことが示されている、この重要検討項目は、リモート署名の利用を考えるうえでも重要な項目であるため、以下にこれらの重要検討項目について、本ガイドラインで検討した結果を参考として説明する。

鍵管理について

鍵管理は、CM で実施する内容であり、以下の CM は論理的なコンポーネントである。そのため、実際には複数のハードウェアやソフトウェアで構成される場合もある。

1　鍵の生成

- 安全なアルゴリズム（電子署名法施行規則第二条、及び CRYPTREC 暗号リスト等）を利用して鍵生成を行う必要がある。
- 鍵生成時に鍵の属性を考慮に入れて生成を行う必要がある。

2　鍵のインポート

- 署名アプリケーション（SAP）と署名生成モジュール（CM）間はセキュアチャネルを利用することが望ましい。
  - 例）通信の暗号化（TLS）等のセキュリティプロトコルを利用する。デバイスドライバと CM 間のデータについて暗号化機能などを検討する。
- インポート対象の鍵は暗号化されていることが望ましい。
  - 例）PKCS#11 が定義しているラップ（暗号化）を利用する。HSM が提供するインポート機能を利用する。
- 暗号化に利用する鍵は暗号対象の鍵と同等のセキュリティ強度を持つことが望ましい。

3　鍵の属性管理

- 鍵は、アルゴリズム、利用用途、許可設定などを特定する属性情報と紐付けた状態

で管理する。
- 例えば、署名鍵は署名のみ利用可能とする等、鍵の属性を設定することで用途を限定的にする。

4 鍵の利用

- CM 内の鍵を利用する場合は CM に対して認証処理が必要であること。
- 鍵は認定された暗号アルゴリズム（電子署名法施行規則第二条、及び CRYPTREC 暗号リスト等）で処理すること。
- 暗号処理の演算過程で生成される中間値には CM 外部からアクセスできないこと。

4.1 鍵の保管

鍵の保管に関しては、ISO/IEC 27002 と同等の対策が必要である。

- 全ての暗号鍵は、改変及び紛失から保護することが望ましい。さらに、署名鍵は、認可されていない利用及び開示から保護する必要がある。
- 鍵の生成、保管及び保存のために用いられる装置は、物理的に保護されることが望ましい。

4.2 鍵に関する設定変更

HSM において鍵を利用可能または利用不可にする等の設定変更については、別の管理策が必要となる（この管理策は、技術的な対策だけではなく、組織・運用の対策も含まれる）。以下に詳細を示す。

- HSM を利用可能に設定変更する場合、及び HSM を利用不可に設定変更する場合には、複数の者によって行う必要がある。
- 一方、上記以外のすべての HSM に関する作業を複数人で作業しなくともよい。
  - 例えば、署名者本人の署名鍵の HSM へのインポートが必要と仮定すると、その作業（インポート作業）はシステムやアプリケーションで対応する場合も想定できる。

5 鍵のエクスポート

- 署名アプリケーション（SAP）と署名生成モジュール（CM）間はセキュアチャネルを利用することが望ましい。
  - 例）通信の暗号化（TLS）等のセキュリティプロトコルを利用する。
- エクスポート対象の鍵は暗号化されることが望ましい。
  - 例）PKCS#11 が定義しているラップ（暗号化）を利用する。HSM が提供す

るエクスポート機能を利用する。

6　鍵の破棄

- 利用廃止時に鍵は廃棄され、鍵が不正利用されるリスクをなくすこと。
  - 例えば、HSM を用いている場合に、HSM 内部の鍵を廃棄する場合は、HSM が提供する鍵消去方法を利用すること。
- バックアップした鍵については、鍵が不正利用されるリスクをなくすこと。

7 鍵の利用に関するログ

- 以下の作業時には CM を利用する署名アプリケーション（SAP）もしくは CM（HSM 等）が提供するログ機能を利用してログを取得することが望ましい。
  - HSM 設定（HSM 設定ポリシー等など含む）
  - 鍵生成
  - 鍵廃棄
- HSM 自体にログをアーカイブ保存する機能がない場合には、アーカイブされたログを管理するシステムを用意する必要がある。

8 署名鍵の生成環境の区別

署名鍵の生成環境により、署名鍵の存在場所すなわち署名の生成場所（リモート署名事業者かそれ以外か）を明らかにできる場合があり、このことが、署名への信頼性、署名時刻への信頼性、不正な署名があった場合の責任の所在などに影響を及ぼす。

署名鍵の存在場所がリモート署名事業者に限定される場合、次の効果が期待できる。

効果１：リモート署名事業者が署名鍵を安全に管理することにより署名者による署名鍵の杜撰な管理に起因した不正署名の可能性が排除されるため、署名への信頼性が高まる。

効果２：リモート署名事業者が署名生成処理で取得する時刻の発生源である時計を厳密に管理していることにより、署名生成時に付与される時刻への信頼性が高まるため、長期署名における署名タイムスタンプの取得を省略できる可能性がある。

効果３：不正な署名が生成された場合、署名鍵の存在場所がリモート署名事業者に限定される場合は責任の所在をリモート署名事業者に求めることができるが、そうでない場合、責任の所在を明らかにすることは困難になる。（そもそも、リモート署名

事業者により署名鍵が安全に管理されている場合、不正な署名が生成されるリスクが生じる機会は極めて小さくなるはずである）

本ガイドラインではリモート署名で利用する署名鍵の 3 通りの生成パターンにおいて、署名鍵が存在する場所に対する考え方は次の通りである。

①リモート署名事業者が鍵生成する場合
- i 一定の要件を満足する HSM を利用する場合、署名鍵の唯一性（HSM 内にのみ存在すること）が保証される。
- ii HSM を利用しないが安全な鍵の運用管理がなされている場合、署名鍵の唯一性（リモート事業者内のみに存在すること）が保たれていると考えて良い。

②認証局が鍵生成する場合
- i 署名鍵が認証局からリモート署名事業者のみに送付する場合、認証局が安全な鍵の運用管理を行なっていれば、署名鍵の唯一性（リモート事業者内のみに存在すること）が保たれていると考えて良い。
- ii 署名鍵が認証局から署名者を経由してリモート署名事業者に渡す場合、署名鍵の唯一性は保証されない。

③署名者の環境で鍵生成する場合
- i 署名鍵の唯一性は保証されない。

つまり、署名鍵を①リモート署名事業者が生成する場合、及び②-i 認証局が生成する場合でかつ署名鍵が認証局からリモート署名事業者のみに送付される場合には、署名鍵の存在場所はリモート署名事業者に限定される。

ただし、リモート署名事業者内で署名を生成する場合、署名者の署名に対する多重署名としてリモート署名事業者の署名を付与することにより、②-ii や③の場合であっても、署名の生成場所を明らかにできるため、効果１～３が生じることとなる。

このように署名鍵の生成環境は重要な要素である。リモート署名を安全に利用するためには、リモート署名事業者の HSM で鍵生成したものか否かについて署名者や署名検証者及び第三者から区別できるような対策を検討する必要がある。また、署名鍵の生成環境の情報や設定を変更できないようにする必要も考えられるため、これらに求められる要件を具体化し、対応方法を検討することが必要となる。さらに、既存の認定制度や監査制度においても、これらの情報を監査や認定の対象とし、監査結果や認定結果を公表することも検討する必要がある。

作成メンバ

新井　聡　　株式会社エヌ・ティ・ティ ネオメイト
雨宮　明　　日本電気株式会社
稲葉　厚志　GMO グローバルサイン株式会社
小川　博久　日本トラストテクノロジー協議会
小田嶋　昭浩　株式会社帝国データバンク
酒巻　一紀　三菱電機インフォメーションシステムズ株式会社
佐藤　雅史　セコム株式会社
手塚　悟　　慶応義塾大学
中村　克巳　三菱電機インフォメーションネットワーク株式会社
西山　晃　　セコムトラストシステムズ株式会社　プロフェッショナルサポート 1 部
濱口　総志　株式会社 コスモス・コーポレイション
舟木　康浩　タレス　DIS CPL ジャパン株式会社
政本　廣志　JNSA 電子署名 WG
南　芳明　　デジサート・ジャパン合同会社
宮脇　勝哉　日本電子認証株式会社
宮内　宏　　宮内・水町 IT 法律事務所
宮崎　一哉　三菱電機株式会社
宮地　直人　有限会社ラング・エッジ
山神　真吾　Utimaco IS GmbH
山中　忠和　三菱電機株式会社

オブザーバー

総務省　サイバーセキュリティ総括官室
法務省　民事局　商事課
経済産業省　商務情報政策局　サイバーセキュリティ課
一般財団法人日本情報経済社会推進協会