リモート署名ガイドライン

パートⅡ．署名活性化モジュール

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 署名活性化モジュールの概要

リモート署名事業者（RSSP）で実装する署名活性化モジュール（SAM）の概要を以下に示す。署名活性化モジュールは、署名者または署名生成アプリケーション（SCA）の鍵認可要求を処理し、署名鍵を活性化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。

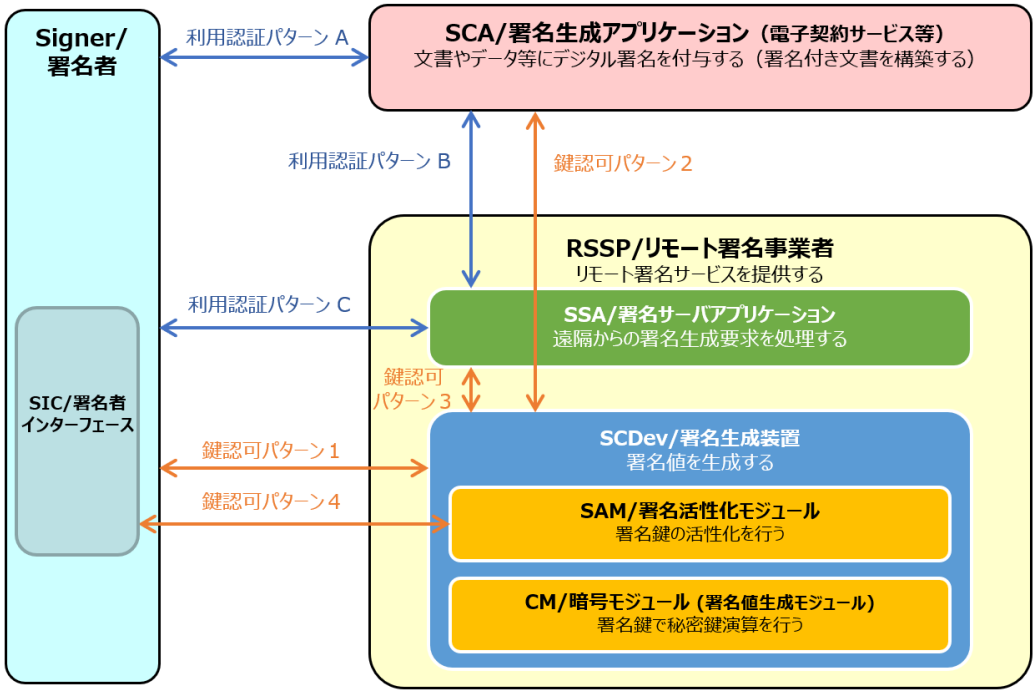

図 1-1　リモート署名サービスの構成例と本ガイドラインのスコープ

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 署名活性化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活性化モジュールに関する脅威のみを示す。

2.1 登録フェーズにおける脅威

2.1.1 署名者登録等における脅威

2.1.1.1 RSSP において、RSSP の署名者 ID と RS-C を対応づける過程で、攻撃者が RS-C を不正取得する[2]。

2.1.1.2 攻撃者は、RA または CA への送信中に署名検証データを変更する。

2.1.1.3 攻撃者は登録中に登録情報を取得する。

2.1.1.4 攻撃者は登録時に署名者になりすます。

2.1.2 署名者管理における脅威

2.1.2.1 攻撃者は特権ユーザを偽装し、登録情報を更新する。

2.1.2.2 攻撃者は更新中に認証情報を開示する。

（注記１）認証局に対する一般的な脅威について
認証局における署名者の電子証明書発行時の本人確認時におけるなりすましや、不正な電子証明書発行などといった認証局に対する脅威分析やリスク評価、それらを踏まえた運用規程の議論は従来からなされており、リモート署名固有ではないため、本書ではスコープ外とする。認証局運用規程に関する別の文書を参照のこと。

[2] これらの脅威は「署名鍵は署名者本人と対応づけられ、それ以外の者とは対応づけられない」の性質を覆す要因となる。

2.1.3 証明書署名要求における脅威

2.1.3.1　攻撃者が CSR のデータを変更する。

2.1.3.2　攻撃者が詐称して CSR を行う。

2.1.4 署名鍵のインポートにおける脅威

2.1.4.1　署名鍵と署名鍵情報（鍵の属性や利用目的など）があり、攻撃者はこれらを扱い不正にインポートする。

2.1.4.2　攻撃者が他人の署名鍵を自らの鍵情報でインポートする。

2.1.4.3　攻撃者が自分の鍵を他人の鍵情報でインポートする。

2.1.4.4　攻撃者が同じ鍵を複数回インポートする。

なお、署名者属性等を割り当てた署名鍵もインポート可能である。

2.2 署名利用フェーズにおける脅威

署名利用フェーズにおける脅威は、署名利用フェーズと内部不正者による脅威がある。

2.2.1 利用フェーズにおける脅威

2.2.1.1　攻撃者は、認証情報を変更する。

2.2.1.2　攻撃者は、（SAP の 1 つ以上の）ステップをバイパスし、署名する。

2.2.1.3　攻撃者は、（SAP の 1 つ以上の手順を）再生し、署名する。

2.2.1.4　攻撃者は、偽造された認証情報を使用して署名者に偽装し、署名する。

2.2.1.5　攻撃者は、SAM への転送中に R.DTBS/R または R.SAD の情報を得る。

2.2.1.6　攻撃者は、SAM への転送中に R.DTBS/R を偽造し、署名する。

2.2.1.7　攻撃者は、（SAP での転送中に R.SAD を）偽造し、署名する。

2.2.1.8　攻撃者は、作成中または作成後または転送中に、署名を SAM 外で修正する。

2.2.2 内部不正者による脅威

2.2.2.1　攻撃者（内部者）が運用管理者に詐称し署名鍵を利用する。

2.2.2.2　攻撃者（内部者）が監査者に詐称しログを得る。

2.2.2.3　攻撃者（内部者）が署名鍵の活性化情報を得る。

2.3 利用停止(破棄)フェーズにおける脅威

2.3.1.1　攻撃者（本人以外）が利用停止（破棄依頼）する。

2.3.1.2　利用停止の再送攻撃（利用停止依頼を傍受し、変更して再送する)。

3 署名活性化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活性化モジュールに関するセキュリティ機能要件を示す。

3.1 登録

3.1.1 署名者登録等における機能要件

3.1.1.1 SAM は、署名者情報に関連するデータが完全性で保護され、必要に応じて機密性が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 7.1.3 の一部として求められる対策である。

3.1.1.2 SAM は、署名者情報の一部として署名認証データをセキュアに扱うことができなければならない。

3.1.1.3 SAM は、署名モジュール署名鍵ペアを生成するために暗号モジュールを安全に使用でき、署名鍵 ID と署名検証鍵（公開鍵）を署名者情報に割り当てることができなければならない。

3.1.1.4 SAM は、署名検証鍵（公開鍵）が認証前に変更されていないことを保証するものとする。

3.1.2 署名者管理における機能要件

3.1.2.1 SAM は、SAM に対するアクションが実行される前に特権ユーザを持つ管理者が認証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 7.1.1 の一部として求められる対策である。

3.1.2.2 SAM は、署名者又は特権ユーザの制御下で、署名者情報、署名認証データ、署名鍵 ID 及び署名検証鍵（公開鍵）に対する変更が行わ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 7.1.1 の一部として求められる対策である。

3.1.3 証明書署名要求における機能要件

3.1.3.1　CSR はセキュアチャネルで通信をする。

3.1.3.2　本人と CSR の内容を確認する。

3.1.4 署名鍵活性化（鍵認可）における機能要件

対策レベル	対策事項
レベル 1	• 署名鍵の活性化（鍵認可）を行うために、単要素認証しなければならない。 • 利用認証で鍵認可（RSSP へのログインに基づいて鍵認可）を行ってもよい。
レベル 2	• 署名鍵の活性化（鍵認可）を行うために、複数要素認証しなければならない。 • 利用認証と別に鍵認可（認証クレデンシャルを用いた RSSP へのログイン）を行わなければならない。
レベル 3	• 上記のレベル 2 に追加して、本ガイドライン（パート II）で示した要件への適合認証した署名活性化モジュールで署名鍵の活性化（鍵認可）しなければならない。

3.2 署名利用時

3.2.1 署名利用（一般）の機能要件

3.2.1.1　SAM は、SAD を検証しなければならない。つまり、SAD 要素間にリンクが存在することを確認し、署名者が強く認証されていることを確認する必要がある。
※この対策方針は本ガイドライン・パート I の 7.1.2 の一部として求められる対策である。

3.2.1.2 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

3.2.1.3 SAM は、SAM への送信時に、認証用データの使用を危うくする攻撃に対してシグネチャ認証データが確実に保護されることを保証しなければならない。

3.2.1.4 SAM は、R.DTBS/R が SAM に送信されたときに完全性を保証されることを保証しなければならない。

3.2.1.5 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。

3.2.1.6 SAM は、特権ユーザの制御下で特権ユーザ及び特権ユーザの認証情報の変更が行われることを保証するものとする。
※この対策方針は本ガイドライン・パートⅠの 7.1.1 の一部として求められる対策である。

3.2.1.7 SAM は、特権ユーザに関連するデータが完全性で保護され、必要に応じて機密性が保護されることを保証しなければならない。

3.2.2 共通（システム）における機能要件

3.2.2.1 SAM は、特権ユーザが SAM の操作を実行するときに、SAM が特権ユーザを認証す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 7.1.1 の一部として求められる対策である。
※この対策方針は本ガイドライン・パートⅠの 7.1.2 の一部として求められる対策である。

3.2.2.2 これらの目的のために使用される別の乱数発生器のプロトコルまたはシードデータにおいて、鍵として使用するために SAM によって生成された乱数は、乱数が予測できず、十分なエントロピーを有することを保証するために定義された品質基準を満たさなければならない。

3.2.2.3　SAM は、特権ユーザにより署名活性化モジュールの構成データの改変が許可され、不正な改変が検出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 7.1.1 の一部として求められる対策である。

3.2.2.4　SAM は、監査データに対する改変が検出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 7.1.4 の一部として求められる対策である。

3.3 利用停止

3.3.1　利用停止を依頼した署名者を確認しなければならない

3.3.2　利用停止の再送攻撃への耐性がなければいない

4 参照情報

[1] EN 419 241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

[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　署名鍵の活性化及びクラウド署名コンソーシアムの情報

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。

署名鍵活性化

リモート署名で署名を行うためには、リモート署名の利用認証後に、署名対象文書と署名指示及び署名鍵を活性化するクレデンシャル（SAD）を利用するアクセス認可が必要である。リモート署名の具体的なサービスを想定した場合、署名者はリモート署名サービスにログインして署名を行うが、多量の署名を行う場合に、署名の都度 SAD の入力を行う場合と、一度の SAD の入力で多量の署名を処理する場合が考えられる。理想を言えば署名の都度 SAD の入力を行うことが望ましいが、ここでは複数署名を 1 回の SAD により行う処理に関して整理する。なお、同じ SAD の利用は 1 回のみに限定すべきであり、同じ SAD を繰り返し利用可能とすることは、中間者攻撃等を容易くする可能性があり推奨されない。

SCA が CM に対して SAD を使って署名鍵活性化する場合、一度に複数の署名対象文書（ハッシュ値）と署名指示を指定する方法と、SAD から SAD トークンを生成し SAD トークンを更新しつつ繰り返し署名要求を行う方法の、2 通りが考えられる。また両方を組み合わせることでより多量の署名要求に応えることも可能となる。

方法１）一度に複数の署名対象文書と署名指示を指定する方法

SCA が複数の署名対象文書のハッシュ値を計算して、CM へ対する署名要求時に複数のハッシュ値を指定する処理方法。結果として SCA は複数の署名値を受け取り、各署名値を利用して複数の署名文書を作成する。なお、先に SAD から SAD トークンを発行して利用しても良い。

図 B-1 一度に複数の署名対象を指定する場合のシーケンス図

方法 2）トークンの更新を利用して繰り返し署名要求をする方法

最初の SAD から SAD トークンを生成して、署名要求にはトークンを利用する。CM に対する 1 回の署名要求の終了後に、利用済みトークンから新たなトークンを更新して取得することで、繰り返し署名要求を行えるようにする処理方法。

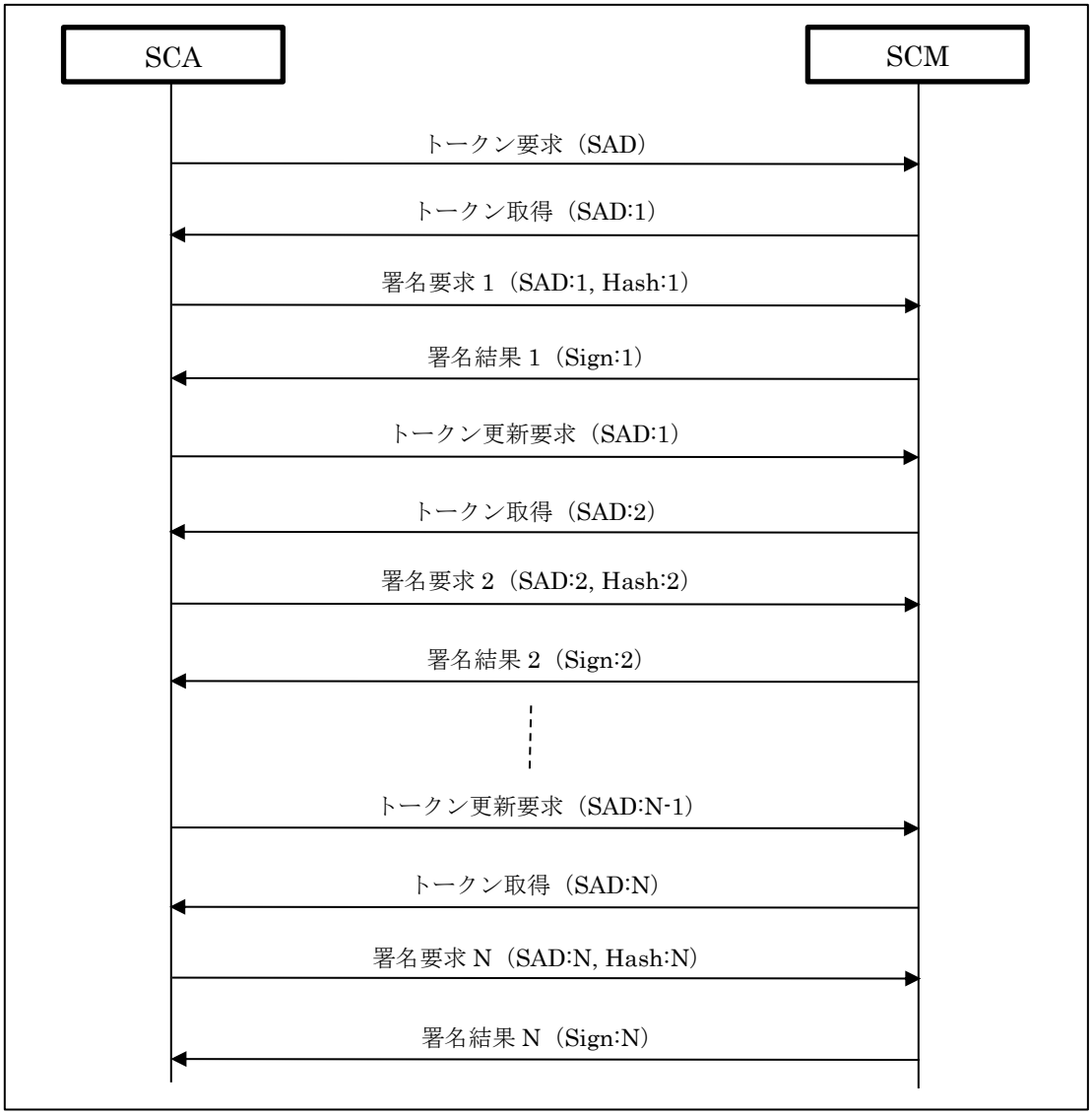

図 B-2 トークンを更新しつつ複数の署名対象を指定する場合のシーケンス図

附録２　クラウド署名コンソーシアムの情報

1 クラウド署名コンソーシアムの API 仕様

クラウド署名コンソーシアム（CSC）は、ソリューション、テクノロジー、トラストサービスプロバイダを含む業界や学術界の専門家から成る国際的な協力グループによって設立された団体で、以下を目的として活動している。CSC の API 仕様書はメールアドレスを登録することで、無償で取得できる。

(1) 共通のアーキテクチャ設計と構成要素構築によって、ソリューション、テクノロジー、トラストサービスプロバイダ間の相互運用性を実現
(2) サービス間の連携を相互運用可能にするべくプロトコルと API の技術仕様開発
(3) オープンスタンダードとして API 仕様を公開
(4) クラウド署名のコンセプトを促進

CSC の API 仕様は、署名利用フェーズのみとなっている。将来的には鍵生成登録フェーズと利用停止フェーズも追加される可能性はあるが、現時点では標準化されていない。CSC の API 仕様に準拠することで、署名サービスとトラストサービスプロバイダ等のサービス間の署名利用フェーズにおける相互運用性が保証される。API 仕様は HTTP/HTTPS を使った RESTful な API と JSON の電文から構成される。

CSC の API 仕様は、欧州の eIDAS に準拠している。この為に CSC の API 仕様を eIDAS 準拠の実装例として見ることもできるが、Qualified（認定）レベルだけでは無く、Advanced（高度）レベルでもあり、レベルによって要求される仕様が異なる点には注意して読み解く必要がある。CSC 仕様に準拠したサービスは、欧州以外の米国や日本でも既に提供されている。その点ではグローバル仕様に対応していると言える。リモート署名を検討する際には目を通すべき API 仕様の１つであるだろう。

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