参考資料２

リモート署名ガイドライン

パートⅠ．リモート署名サービスにおける
全般的セキュリティ対策

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 目的・背景

最近の国際的なデジタルエコノミー進展の中で、事業者環境に署名鍵を預けて契約書等にリモートで署名できるサービスが普及しつつある。本ガイドラインはリモート署名サービスの概要を解説するとともに、リモート署名にて作成された電子署名文書の信頼性を確保するためリモート署名事業者や関係事業者及びリモート署名の利用者が留意すべき基準をとりまとめた。

日本政府の施策によって、2016 年からマイナンバーカードの利活用が進み、2017 年にマイナポータルにおいて各種の申請や手続きの電子化が促進され、また、2019 年 1 月に電子委任状の普及の促進に関する法律が施行され、国民にとっても電子証明書及び電子署名がより身近に利用できる環境が整った。これらの環境を利用したサービスの中でも、特に電子的な契約では、署名者の IT 環境の変化や電子的に契約を行う上での署名鍵の管理の負担軽減のために、リモート署名サービス（リモート署名事業者のサーバに署名者の署名鍵を設置・保管し、署名者の指示に基づきリモート署名サーバ上で自ら（署名者）の署名鍵で電子署名を行うサービス）を活用した電子契約サービスも存在している。

我が国では電子署名及び認証業務に関する法律（以下、電子署名法）の認定認証業務を行う法人が認証局とは別のサービスとして 2009 年 11 月にリモート署名を採用した Web 型の署名サービスを開始したのが最初の利用事例であった。その後、2016 年 2 月に大手金融機関によりリモート署名を使用した融資契約の電子化サービスが開始された。現在では民間事業者が提供する多くの電子契約サービスの中でリモート署名が採用されているがその方法は様々である。電子契約では、利便性が高く、かつ安全なサービスが求められるが、その安全性や信頼性の指標が定まっていない。

一方、経済産業省では 2015 年度、2016 年度の電子署名法研究会においてリモート署名の関連動向やその在り方の検討を行い、その実施のために必要となる事項が整理された。日本トラストテクノロジー協議会（以下、JT2A）では、この検討を受けてリモート署名事業者や関係事業者及びリモート署名の利用者がリモート署名の理解を深め、一定の指標として参照可能なリモート署名サービスのガイドラインを作成することとした。また、2018 年 7 月「日 EU 経済連携協定（EPA）」の中で電子商取引における電子署名、電子認証に関する基本ルールが規定され、2019 年 1 月の世界経済フォーラム年次総会（「ダボス会議」）にて国際間で「信頼ある自由なデータ流通（DFFT：データ・フリー・フロー・ウィズ・トラスト）」の確立が最重要課題であるべきことが我が国から提唱されている。そのため、本ガイドラインでは、リモート署名を用いた電子商取引に関する EU などとの国際相互連携も踏まえつつ、リモート署名サービスのあるべき内容の検討結果をまとめた。

今後のデジタルトランスフォーメーションの推進に向けて、リモート署名を利用した電子契約や電子申請などの信頼性を確保するため、本書を参考にされたい。

日本トラストテクノロジー協議会　一同

2 用語

用語・略称	説明
CA（認証局）	Certification Authority、署名鍵（秘密鍵）と対になる公開鍵に対する電子証明書を発行する機関。例えば、電子署名法に基づく認定認証業務における認証局など。一般に認証局は、発行局（IA）、登録局（RA）、電子証明書の失効情報等を公開するリポジトリなどで構成される。
CM	Cryptographic Module、暗号モジュールの略称であり、本書では署名値生成モジュールとも言う。Cryptographic Module の認証を行う制度には CMVP(Cryptographic Module Validation Program)や、日本の JCMVP がある。さらに、欧州においては EN 419 221-5 [3]で定められた要件に基づいてセキュリティ評価を行っている。
CSP（認証クレデンシャル発行機関）	Credential Service Provider、認証クレデンシャルを発行する機関。例えば、JPKI 利用者証明用電子証明書、認証局が発行する利用者証明用電子証明書等がある。また、オンラインサービスの利用申請を受付け、利用者に対して ID/パスワードを発行するオンラインサービス提供者などを含む。サービス提供形態によっては認証局とは異なる事業体もありえる。
CSR	Certificate Signing Request、電子証明書の発行を要求する者が送信するデータであり、電子証明書を発行する際の元となるデータ。CSR には電子証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して電子証明書を発行する。データ形式として、PKCS#10 などがある。
DTBS	Data to be Signed、署名対象データ。（参照情報[2]で定義されている）また、単体及び複数のセットで構成する場合には、DTBS/R(s)とする。
HSM	Hardware Security Module、ハードウェアの暗号モジュールであり、ハードウェア内で鍵を保管し、暗号化機能や署名機能を有する装置。
IA（発行局）	Issuing Authority、電子証明書発行や失効等を行う機関。
PIN	Personal Identification Number、本人確認のために用いる本人のみが知る番号などの情報。
PKCS#10	Public Key Cryptography Standards 10 であり、Certification Request Standard を意味する。CSR の項を参照。
PKCS#11	Public Key Cryptography Standards 11 であり、Cryptographic Token Interface を意味する。暗号トークンへの汎用インタフェースを定義する API。
PKI	Public Key Infrastructure、公開鍵をベースに秘匿性、完全性、認証、否認防止を確実にするための公開鍵基盤。
RA（登録局）	Registration Authority、署名者の本人確認を行い、IA へ電子証明書の発行を依頼する機関。本書では、署名用の電子証明書の登録局を意味する。
RP（リライングパーティ）	Relying Party（依拠当事者）、（署名の真正性に）依拠する当事者。本書では、署名の受領者（署名受領者）を指す。
RS-C	認証クレデンシャルの項を参照。
RSSP（リモート署名事業者）	Remote Signature Service Provider、署名者の署名鍵を設置・保管するサーバとそのサーバ上で署名者の指示に基づき、電子署名を行う機能を提供する者

用語・略称	説明
SAD	Signature Activation Data、署名鍵を活性化するデータであり、署名用の認可クレデンシャルである。IC カードでは PIN 等である。（参照情報[2]で定義されている）
SAM	Signature Activation Module、署名鍵の活性化を行うモジュール。
SAP	Signature Activation Protocol、署名対象データへの署名を制御するための SAD を収集するプロトコル
SCA	Signature Creation Application、SCDev を用いて電子署名を生成するアプリケーション。（参照情報[2]で定義されている）
SCDev	Signature Creation Device、署名値を生成するためのソフトウェアまたはハードウェア。（参照情報[2]で定義されている）
SCM	Signature Creation Module、電子署名を生成するモジュール。（日本国内のリモート署名を検討するために新たに定義したモジュールである）
SIC	Signer's Interaction Component、SAP をサポートする署名者側のソフトウェアあるいはハードウェアモジュール
SSA	Server Signing Application、SCA に対して署名値生成に対するリモートアクセスを提供するアプリケーション。（参照情報[2]で定義されている）
SSASC	Server Signing Application Service Component、サーバ署名アプリケーションを使用して署名者に代わって署名値を生成する TSP サービスコンポーネント
TSP	Trust Service Providers、トラストサービス事業者
リモート署名サーバ	リモート署名事業者が管理するサーバであり、署名者の署名鍵を保管し、リモート署名を実施する。
リモート署名事業者（RSSP）	「事業者」と略すこともある。RSSP の項を参照。
検証鍵	署名検証に用いる鍵（公開鍵）。電子署名法施行規則では「利用者署名検証符号」と称される。
署名鍵	署名に用いる鍵（秘密鍵・私有鍵）。署名サーバ内で HSM 等により安全に管理される。署名を行う際に署名鍵に設定された PIN などにより活性化される。電子署名法では「利用者署名符号」と称される。
署名者（Signer）	署名を行う者。本書では、リモート署名サービスを利用して署名を行う者を指す。
電子証明書	ある公開鍵が署名者などの対象に帰属していることを証明するために認証局が発行する電子的な証明書。公開鍵証明書ともいう。
認証クレデンシャル（RS-C）	署名者が署名サーバを利用する際の認証に用いるための情報（リモート署名（RSSP）の提供するサービスへのログインに用いるクレデンシャルについては RS-C と表記する）。例えば、JPKI 利用者証明用証明書、ID/パスワード、ワンタイムパスワードなど。
利用者 ID	利用者の識別子。

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

本ガイドラインの分冊構成を以下に示す。パートⅠはリモート署名の概要及びサービスとして提供するための一般的なセキュリティ対策について述べる。パートⅡ以降はリモート署名サービスを構成するうえで重要なモジュールの要件について述べる。パートⅡは署名活性化モジュール、パートⅢは署名値生成モジュールである。

表 3-1 本ガイドラインの分冊構成

分冊	内容
パートⅠ	リモート署名の概要とセキュリティ対策事項 ・共通対策：リモート署名事業者が共通で対策すべき事項 ・対策レベル分け：署名鍵の活性化（鍵認可）のレベル定義
パートⅡ	署名活性化モジュールのセキュリティ機能要件 ・共通対策：リモート署名事業者が共通で対策すべき事項 ・要件レベル分け：署名鍵のインポート（鍵設置）のレベル定義
パートⅢ	署名値生成モジュールのセキュリティ機能要件 ・共通対策：リモート署名事業者が共通で対策すべき事項 ・要件レベル分け：署名鍵生成のレベル定義

3.2 本ガイドラインの想定読者

本ガイドラインは、リモート署名サービスを開発及び提供する事業者、及びそれを利用する者を想定読者とする。利用する者としては、リモート署名サービスを利用して署名する署名者と、電子署名を使うアプリケーションを開発・提供するアプリケーションサービス事業者（以下、アプリ事業者とする）がある。アプリケーションサービスの例として、電子契約サービス等を考えると下図となる。

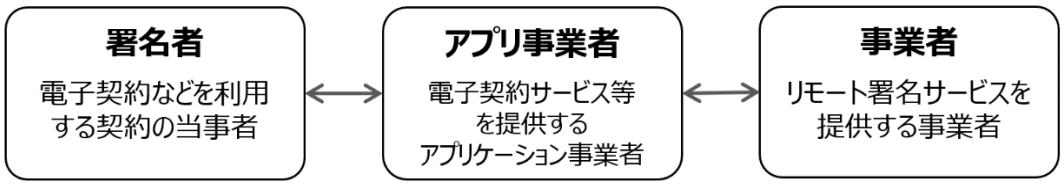


図 3-1　電子契約サービス等を想定した想定読者の概要

本ガイドラインの章構成と想定読者の関係を下表に示す。リモート署名を行う署名者はリモート署名の概要を知り、自らの署名鍵を安全に管理し、利用するために、リモート署名事業者が提供するサービスを選定する必要がある。そのため、本ガイドライン・パートⅠの1章から 4 章及び附録を参考にリモート署名サービスを選定する必要がある。特にリモート署名サービスや電子契約サービスを選定する際に確認すべき重要項目については、各事業者が予め公開するか署名者に対して事前に提供する情報であり、署名者は自らの署名鍵が安全に生成、利用できるかを必ず確認する必要がある。この署名者が確認すべき情報は、本ガイドラインの附録 2 に示す。

リモート署名サービスを利用してアプリケーションサービスを提供する事業者は、パートⅠを参考にリモート署名事業者が提供する機能とレベルを理解して、安全に利用する必要がある。リモート署名事業者（事業者）は、本ガイドラインのすべての章を参考に対策を行う必要がある。

表 3-2 本ガイドラインの章構成

分冊	章	署名者	アプリ事業者	事業者
パートⅠ	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　リモート署名のリファレンスモデル	―	○	○
	6章　セキュリティ検討事項	―	○	○
	7章　セキュリティ対策事項	―	○	○
	8章　参照情報	―	○	○
	附録	○	○	○
パートⅡ	1章　署名活性化モジュールの概要	―	―	○
	2章　セキュリティ検討事項	―	―	○
	3章　セキュリティ機能要件	―	―	○
	4章　参照情報	―	―	○
	附録	―	○	○
パートⅢ	1章　署名値生成モジュールの概要	―	―	○
	2章　セキュリティ検討事項	―	―	○
	3章　セキュリティ機能要件	―	―	○
	4章　参照情報	―	―	○
	附録	―	○	○

3.3 リモート署名とは

経済産業省の電子署名法研究会の平成 28 年度の事業報告書では、リモート署名を以下のように定義している。

> リモート署名とは、一般にリモート署名事業者のサーバに署名者の署名鍵を設置・保管し、署名者の指示に基づきリモート署名サーバ上で自ら（署名者）の署名鍵で電子署名を行うことをいう。

本ガイドラインにおいても、これに基づいて記述する。

3.3.1 リモート署名の背景

日本における“電子署名”は、紙媒体に対する署名や捺印と同様に署名者が署名鍵を手元に保管し、署名者の手元で行うモデルであった。本ガイドラインではこれを「ローカル署名」と呼ぶことにする。

一方で、デジタル化とネットワークの発展は、クラウドサービスなどデータ処理の形態を多様化し、電子署名の利用環境も大きく変化した。従来の電子署名は、署名鍵の取得の手間や、耐タンパデバイスによる安全な保管が普及の妨げとなっていたが、署名鍵をサーバ等に預け、遠隔から利用する形態（リモート署名）がこの課題の一つの解決策となることが期待される。リモート署名は、単に鍵の場所をローカルからリモートにした以上に大きな意味を持つ。そのメリットは、一般のクラウドサービスと同様に、デバイスフリー化、いつでもどこでも利用可能なこと、所有（管理）から利用への転換である。これにより、紙では手元でしかできなかった“署名“が、リモートで可能となることでデジタル化の促進とビジネスモデルの変革につながる可能性を秘めている。

3.3.2 ローカル署名とリモート署名の違い

実際にリモートで署名を行うためには、安全に署名鍵を預ける先としての事業者（以後、「リモート署名事業者」(RSSP)と呼ぶ）が必要となる。リモート署名と、ローカル署名の対比を図 3-2 に示す。

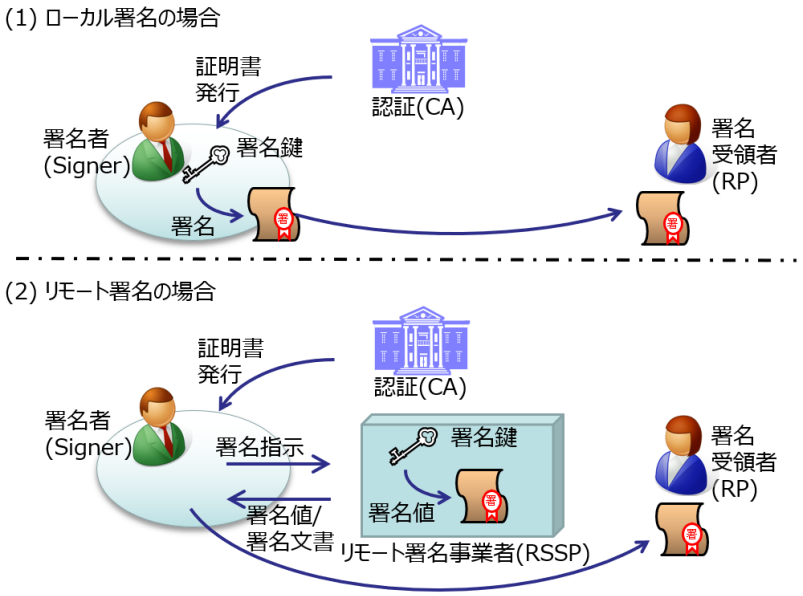


図 3-2　ローカル署名とリモート署名の利用イメージ

また、リモート署名を利用するにあたり、ローカル署名との大きな違いの一つは、リモートで署名を指示する人が確かに署名者本人かを確認（認証）する必要が生じる。そのため、署名者の認証クレデンシャルが必要となり、それを発行するクレデンシャル発行者が必要となる(図 3-3)。

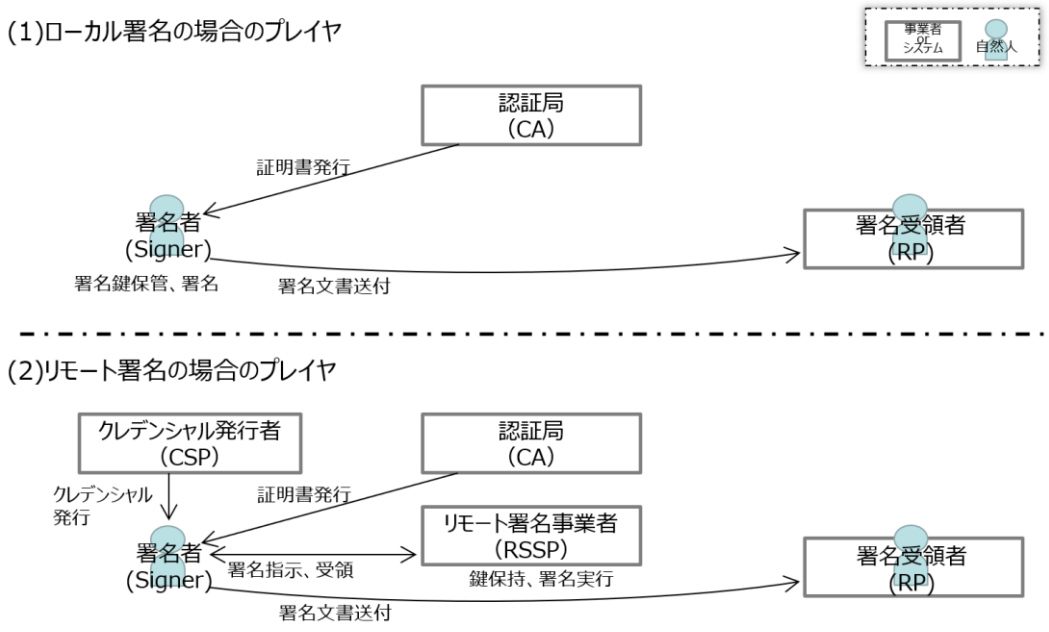


図 3-3　ローカル署名モデルとリモート署名モデルの比較（プレイヤと保有情報）

3.4 リモート署名の提供形態と本ガイドラインのスコープ

リモート署名をビジネスに利用する場合、特定のサービスのアプリケーションと密接に連携する形態が考えられる。例えば、現状のリモート署名の利用例の多くは、電子契約及び電子契約を含む保管サービスである。これは、汎用的な署名鍵をリモート環境（外部）に置いて汎用的な用途で利用するケースよりも利用方法や用途が明確になっているため、リモート署名のニーズが顕在化しているものと考えられる。この場合、署名者が行う手続きを電子契約サービス等のアプリケーションが仲介して進める形態となるが、署名者の意思に基づく処理を確保するという点に着目すれば、処理の流れの主要な点で図 3-4 の(1)と(2)に違いはない。

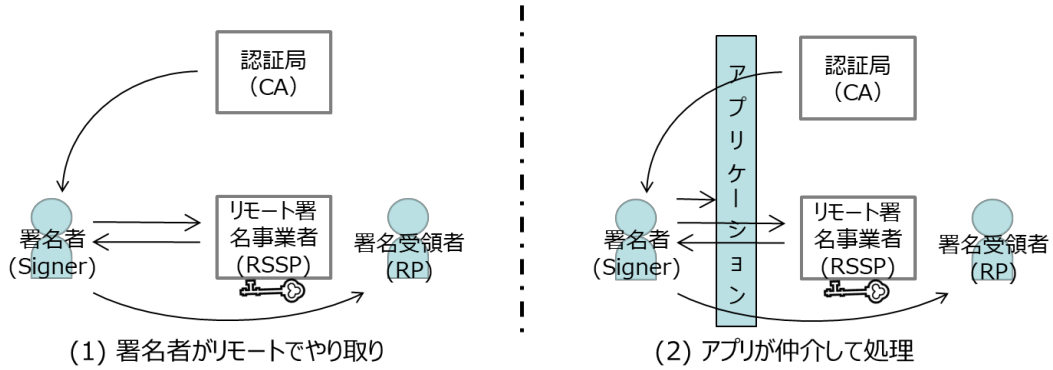


図 3-4　リモート署名の利用形態の例

ここで、リモート署名サービスを利用し、電子契約サービス等を提供するものを署名生成アプリケーション（SCA）と呼ぶ。

以上より、リモート署名の世界の登場人物は多岐にわたり、それらの関わり方も多様である。例えば、誰が署名鍵を生成し、どのように RSSP に渡すのか等は様々な方法が考えられる。また、署名者について、認証クレデンシャル発行時、電子証明書発行時、リモート署名サービス利用時のそれぞれの本人確認レベルをどう定義するかも重要である。実際に、署名者がリモートで署名を行う場合は、サービス提供を受けるための利用者の認証（以降、利用認証）と署名鍵を利用するための鍵認可が必要となる。この利用認証と鍵認可についても署名者と RSSP が直接行う場合と、SCA を介して行う場合がある。

このような多様性に鑑みて、本ガイドラインでは、リモート署名を実現するうえで特有の課題についての対策を規定することし、一般的な利用者の認証のように他の標準等を参照することにより実現できる事項はスコープ外とした。具体的には、図 3-5 の太線で示した鍵認可を規定対象とし、曲線で示した利用認証等は規定対象外とする。なお、利用者の認証及び登録時の本人確認はスコープ外ではあるが、リモート署名を実現するうえでの重要項目でもあるため、リモート署名サービスの提供事業者が、対象となる情報の重要度や SCA の有無などを踏まえリスク分析の結果を考慮して設計する必要があると考えられる。その

ため、参照すべきガイドラインとして 8 章の参考情報 [6]などを挙げておくとともに、特にリモート署名において注意すべき本人確認の内容を本ガイドライン（パート Ⅰ）の附録 1 に示す。

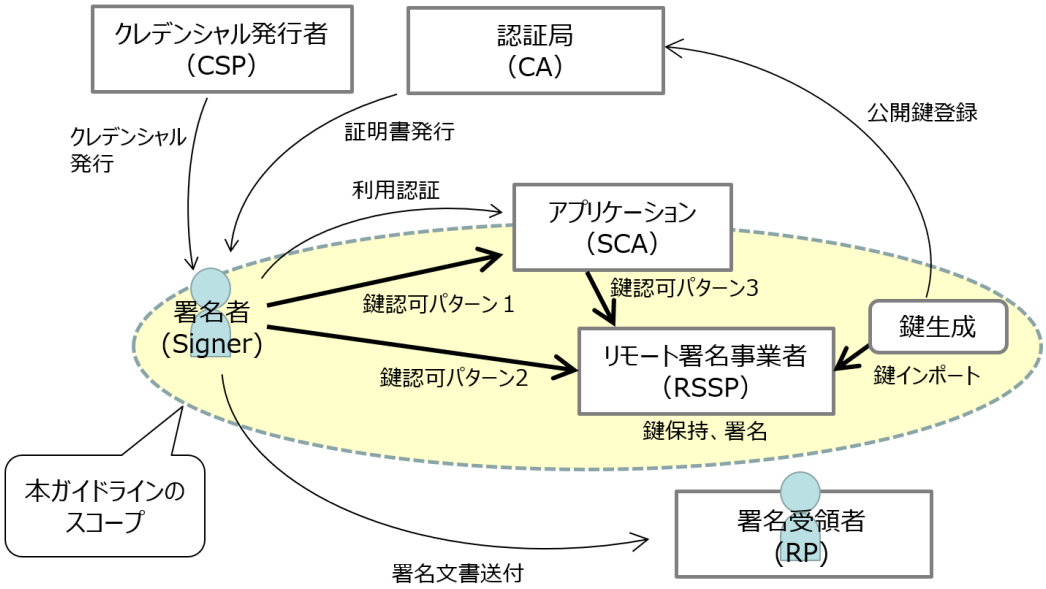


図 3-5　リモート署名における本ガイドラインのスコープ

ここまでに述べた本ガイドラインのスコープを、より明確にするため、4 章で述べるリモート署名のフェーズや処理と、本ガイドラインのスコープとの関係を表 3-3 に示しておく。

表 3-3　リモート署名の一般的な項目と本ガイドラインのスコープ

フェーズ	項目	スコープ内	スコープ外
鍵生成登録フェーズ	クレデンシャル発行	—	○
	サービス利用登録	—	○
	鍵生成	○	—
	鍵インポート、鍵保持	○	—
	証明書発行	—	○
署名利用フェーズ	利用認証	—	○
	鍵認可	○	—
	署名	○	—
	検証	—	○
利用停止フェーズ	停止	—	○
	退会	—	○
	鍵廃棄	—	○

3.5 本ガイドラインで扱うレベル分類

リモート署名サービスは様々な要素で構成され、その組み合わせであるサービスの安全性、信頼性も多様になる。そこで、署名者やアプリ事業者がサービスを選定する一助とするため、いくつかのセキュリティのレベルを定める。詳細な要件は後述するが、ここでは、3 つのレベルを規定する。どのレベルにおいても、リモート署名事業者は、電子署名としての性質を損なわないために、適切なセキュリティ対策を行う必要がある。リモート署名事業者に求められるセキュリティ対策は、レベル 1 からレベル 3 の順に応じて、より技術的な対策に重点が置かれ、リモート署名事業者や署名者による人的な運用や環境への依存性がより少なくなる。

表 3-4　レベル分類

レベル	概要
レベル 1	電子署名に利用する署名者の署名鍵を安全に管理するために最低限必要な対策を施したレベル
レベル 2	電子署名法における認定認証業務において発行する電子証明書に基づいたリモート署名サービスを提供するにあたり、リモート署名サービスが認定認証業務の信頼性と同等の信頼性を達成するために必要なレベル
レベル 3	リモート署名サービスが欧州 eIDAS 規則における適格電子署名と同等の信頼性を達成するために必要なレベル

3.5.1 重要項目におけるセキュリティレベル

リモート署名の重要事項は、鍵生成（署名鍵の生成）、鍵インポート、鍵保持、鍵認可（署名鍵の活性化）の 4 つである。署名鍵の生成及び鍵インポート、鍵保持は、署名者の署名鍵を安全に設置し、管理するために重要であり、利用する署名鍵は、正しく生成されたこと、または正しくインポートされ、安全に保持することが求められる。また、署名鍵の活性化は、署名者の署名鍵を安全に管理し、署名者だけが署名鍵を活性化でき、署名者以外は署名鍵を利用できないことが求められる。

表 3-5　重要項目（鍵生成、鍵インポート、鍵保持、鍵認可）のレベル

項目	レベル 1	レベル 2	レベル 3
鍵生成	• HSM※1 を利用せずに署名鍵の生成が可能	• 第三者の評価や認証を受けた HSM※2 でのみ署名鍵の生成が可能	• 国際的に承認されうる評価や認証を受けた HSM※3 でのみ署名鍵の生成が可能
鍵インポート	• 署名鍵のインポート可能	• 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)からのみ署名鍵※4 のインポートが可能	• 外部からのインポート不可。HSM※3 内で生成した署名鍵のみを利用する
鍵保持	• 署名鍵に対する適切なアクセス制御策を講じ、ストレージに格納する	• HSM※2 のセキュアな境界内※5 で署名鍵を保持し、HSM 内でのみ署名生成処理を実行する • HSM※2 のセキュアな境界を越えた、署名鍵のエクスポートは不可	• HSM※3 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する • HSM※3 のセキュアな境界を越えた、署名鍵のエクスポートは不可
鍵認可	• 鍵認可は単要素認証 • 利用認証で鍵認可を行ってもよい（＊1）	• 鍵認可は複数要素認証 • 利用認証と別に鍵認可を行わなければいけない（＊2）	• レベル 2 に追加して、評価・認証取得※6 し、耐タンパ領域に実装した署名活性化モジュールでの鍵認可が必要（＊3）

※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る。

※2：例えば、Cryptographic Moduleの認証を行う制度であるCMVP(Cryptographic Module Validation Program)や、日本のJCMVPがある。

※3：一般的なCryptographic Moduleとしての評価や認定だけでなく、各国の電子署名関連法規制に従った追加の要件が必要となる場合がある。例えば、欧州におけるQualified Electronic Signature相当として受け入れられるためには、署名生成デバイス（SCDev）に関する欧州規格に従って、Common Criteriaで評価されることが求められる。

※4：CAが署名鍵生成を行う場合、CAがレベル 2 の鍵生成の要件を満たす必要がある。

※5：HSMによって設定されたセキュアな境界を指す。

※6：国際的な相互承認について考慮すべきである。例えば、欧州におけるQualified Electronic Signature相当として受け入れられるためには、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）に従い、Common Criteriaで評価されることが求められる。

3.5.2 利用認証と鍵認可について

リモート署名で想定する利用シーンの例としては署名対象となる電子的な契約書ファイル等を作成、保管する電子契約サービス等がある。この時、署名対象となる電子的な契約書ファイル等を作成、保管する電子契約サービス等で署名者の利用認証を行い、その後、リモートで署名を行う際に、署名鍵を活性化（鍵認可）を行うこととなる。そのため、リモートで署名の対象となる情報の重要度やリスクに応じて、利用認証と鍵認可の対策が異なる。表 3-5 の鍵認可の対策及び考え方について想定される利用認証のパターンと鍵認可のパターンについて説明する。下図に示したとおり、利用認証のパターンはパターン A からパターン C の 3 つ（図中の青線）、鍵認可のパターンはパターン 1 からパターン 4 の 4 つ（図中の橙色線）である。

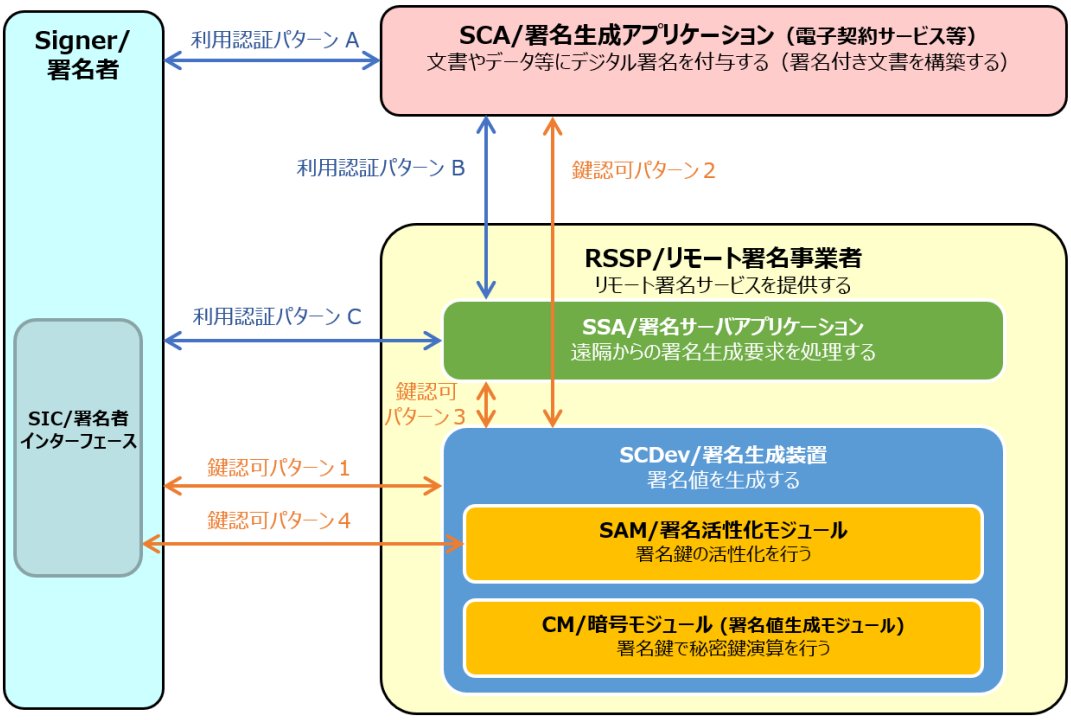


図 3-6　リモート署名サービスの構成例

表 3-5 の鍵認可との対応は以下のとおりである。

（＊1）鍵認可レベル 1：利用認証で鍵認可を行ってもよい

- SCA への利用認証パターン A により、RSSP への利用認証パターン B を兼ねてもよいし、RSSP への利用認証を別途行う場合（利用認証パターン C）も考えられる。

- 鍵認可は直接（鍵認可パターン１または鍵認可パターン４）行ってもよい。
- SCA（鍵認可パターン２）あるいは SSA（鍵認可パターン３）が代行してもよい。

（＊２）鍵認可レベル２：利用認証と別に鍵認可を行わなければいけない

- 鍵認可は必ず利用認証とは別に行わなければならない（鍵認可パターン１または鍵認可パターン４）。

（＊３）鍵認可レベル３：署名活性化モジュールでの鍵認可が必要

- 鍵認可は必ず SAM 経由で行わなければならない（鍵認可パターン４）。

4 リモート署名の概要

4.1 リモート署名の利用形態

前章で述べた、アプリケーションを介した利用については、単一のアプリケーションを介してリモート署名事業者を利用するケース（図 3-4(2)）に加えて、電子契約等の（複数の）アプリケーション提供者が汎用のリモート署名事業者を利用するケース（図 4-1(3)）と、アプリケーション提供者が個々に自社サービス用にリモート署名機能を提供するケース（図 4-1 (4)）が考えられる。前者のケースでは、アプリケーションが複数あるだけの違いであって個々のアプリケーションの機能、要件は単一の場合と違いがない。また、後者の場合、アプリケーションとリモート署名が一体となっているが、論理的には別の構成要素と位置付けられるので、アプリケーションが独立しているケースと比べて、リモート署名を行ううえで満たすべき機能、要件に変わりはない。したがって、以下ではこれらのケースを代表するものとして、 図 3-4(2)のアプリケーションを対象に議論を進めることとする。

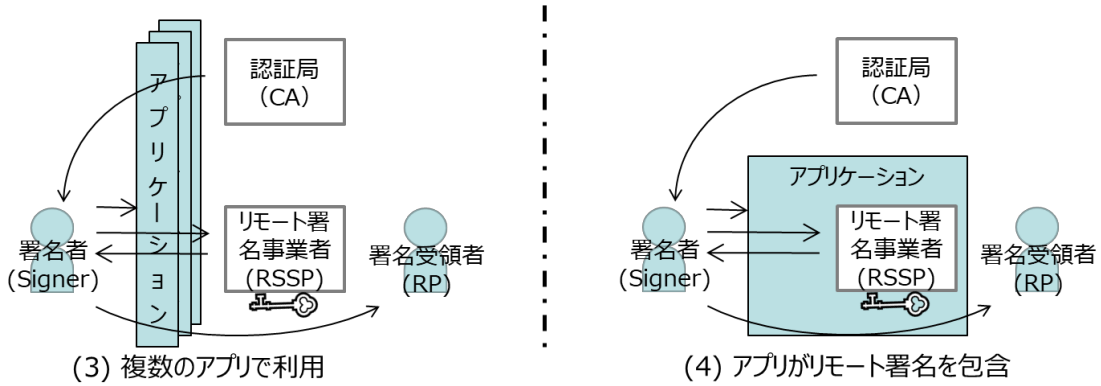


図 4-1　リモート署名の利用形態の例（複数のアプリケーション）

4.2 リモート署名のプレイヤとライフサイクル

4.2.1 プレイヤと役割

前節で述べたリモート署名に関連するプレイヤについて、その役割を表 4-1 にまとめる。

表 4-1 リモート署名のプレイヤと役割

プレイヤ	役割
リモート署名事業者 （Remote Signature Service Provider：RSSP）	署名者の署名鍵の設置・保管及び署名者の指示に基づく電子署名生成の機能を持つサーバの提供
リモート署名アプリケーション （Signature Creation Application：SCA）	署名対象ドキュメント等の準備と、リモート署名を利用して長期署名等の生成（例：電子契約サービス）
クレデンシャル発行者 （Credential Service Provider：CSP）	リモート署名事業者のサーバを利用するための認証クレデンシャルの発行
認証局 （Certification Authority：CA）	署名者の署名鍵に紐づく電子証明書の発行
署名者 （Signer）	リモート署名サービスを利用した署名の実施
署名受領者 （Relying Party：RP）	署名（署名された文書等）の受領

実際の利用形態を考えると、署名者が電子契約等のリモート署名アプリケーション（サービス）を利用して電子署名を行う場合（図 4-2 (1)）と、署名者が直接、端末アプリ等によりリモート署名する場合（図 4-2 (2)）が考えられる。これらを基本モデル１、基本モデル２とする。リモート署名アプリケーション（アプリ事業者）とリモート署名事業者が同一の場合もあるが、この２つを分離してサービス提供することが可能となっているため、同一事業者のケースも基本モデル１に包含して考えることができる。リモート署名事業者は、署名者によるリモート署名事業者への鍵認可に基づいて、署名対象に対する署名値の生成を行う。リモート署名アプリケーションは、署名対象をリモート署名事業者に提供し、リモート署名事業者から署名を受け取って、最終的な署名済み文書等を構成して署名者に提供する。

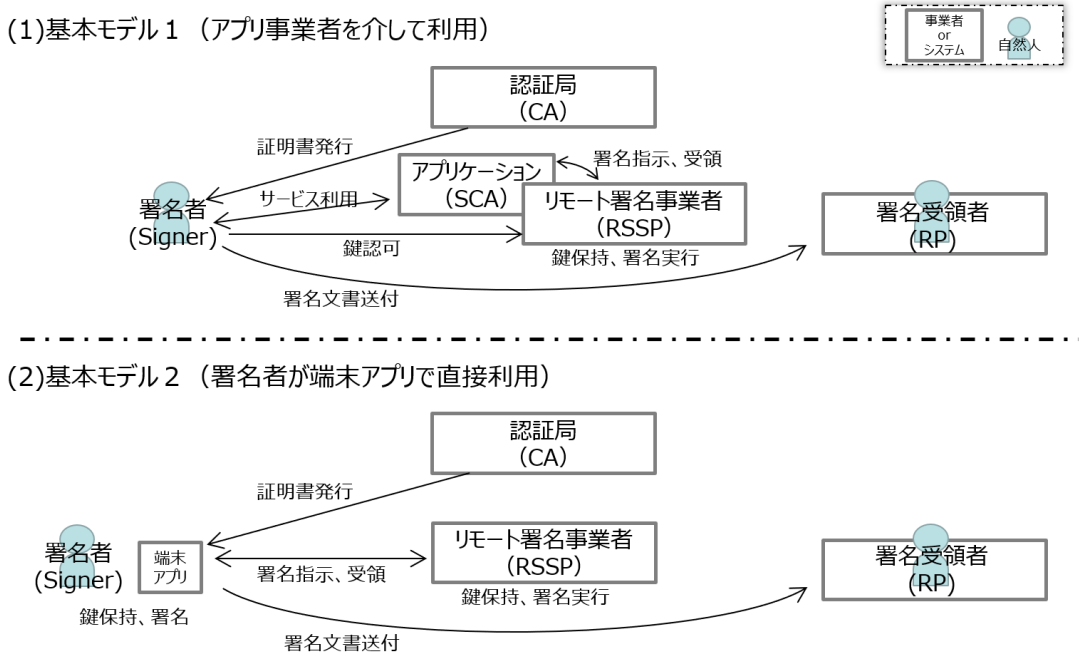


図 4-2　リモート署名の基本ロールモデル（プレイヤと役割）

ここで役割について補足する。上記モデルは主に署名生成時の処理に関するものであるが、その準備段階として、署名生成に必要な署名鍵の生成と、リモート署名事業者へのインポート及び保持が必要であり、これらに関するモデルが必要である。

ローカル署名の場合、署名鍵を持つのは署名者であるが、鍵を生成するのは署名者とは限らない。電子署名法施行規則第 6 条第 3 号及び第 3 号の 2 では、認定認証事業者（CA）が署名鍵を作成する場合及び署名者が署名鍵を作成する場合における基準について規定している。リモート署名の場合も同様に、署名者及び CA が鍵生成の候補となるが、さらに、鍵の移送の便を考えると、リモート署名事業者も鍵生成の候補として考えるべきである。

従来のローカル署名のモデルとリモート署名のモデルによる役割と保有情報の違い、電子署名法との関係を図 4-3 に示す。従来のローカルで署名を行うモデル（図 4-3(1)）では、署名者が署名鍵と署名鍵を活性化する鍵認可クレデンシャル（SAD）及び公開鍵証明書を保有する。一方、リモート署名のモデル（図 4-3(2)）では、署名者は鍵認可クレデンシャルと公開鍵証明書及びリモート署名（RSSP）のサービスを利用するための利用 ID と利用 ID に対応する認証クレデンシャル（RS-C）を保有する。さらに、RSSP は、署名サービスを提供先として正当な署名者であることを認証するため、署名者の認証クレデンシャルを検証するための情報を保持する。さらに、署名者に対応した署名鍵を保持する。

また、電子署名法がカバーする範囲と定める要件を下図に、赤枠（四角枠）で示す。リモート署名の場合に、それらに追加して担保すべき範囲を青枠（丸枠）で示す。

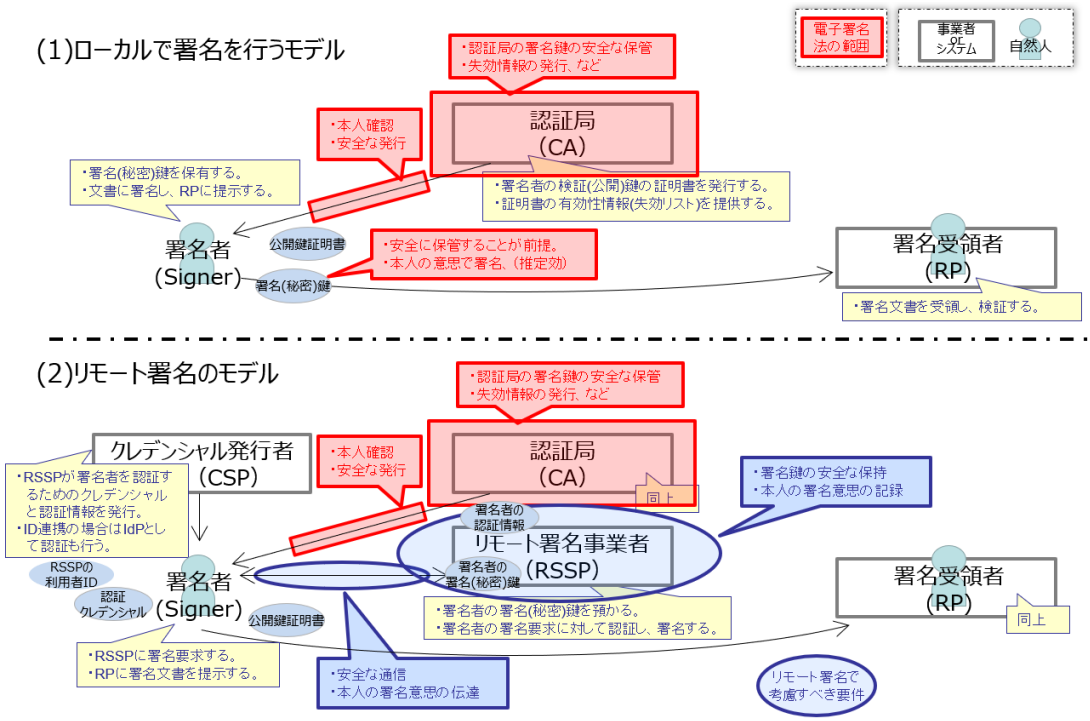


図 4-3　ローカル署名モデルとリモート署名モデルの比較（電子署名法要件との関係）

4.2.2 鍵のライフサイクルと関連処理

リモート署名鍵のライフサイクルに着目し、それに関連する処理と要件を整理する。リモート署名の場合、ローカル署名との違いは、署名鍵を安全にリモート署名事業者に登録（設置）するための処理や、預けた鍵を本人の意思に基づいて使うための処理が加わることである。鍵のライフサイクルに従って、鍵生成登録フェーズ、署名利用フェーズ及び利用停止フェーズが行われる。その具体的内容は次に示すとおりである。

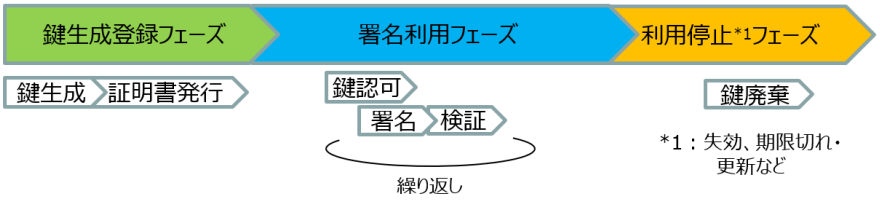
① 鍵生成登録フェーズ：署名鍵ペアを生成し CA が電子証明書を発行するとともに、リモート署名サービスを利用するための各種手続きと署名鍵のリモート署名サーバへの登録（設置）を行うフェーズ

② 署名利用フェーズ：署名者がリモート署名サービスにアクセスし、署名対象データとリモート署名鍵を指定して電子署名を指示するフェーズ

③ 利用停止フェーズ：署名者が利用中止する場合や鍵の期限切れ（更新の場合も含む）、失効などにより、リモート署名鍵に関する情報を廃棄するフェーズ

各フェーズとその時のリモート署名関連の処理を図 4-4 に示す。

(1)ローカル署名のモデル



(2)リモート署名のモデル

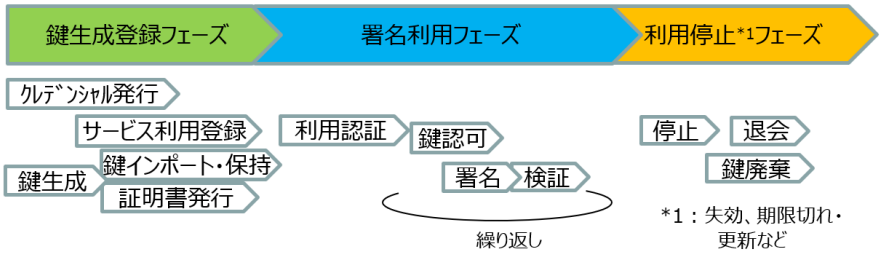
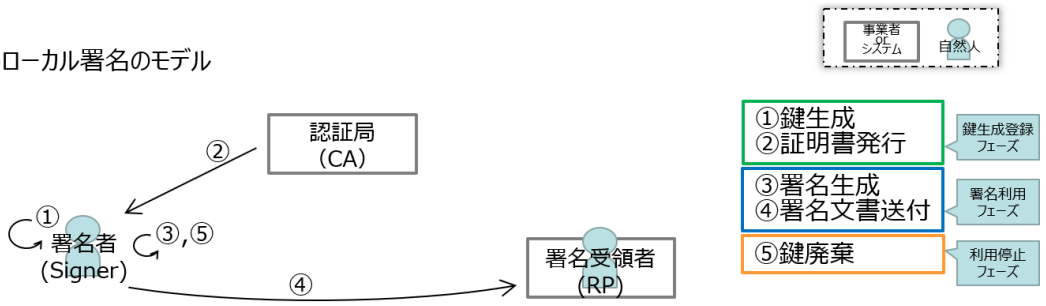


図 4-4　署名鍵のライフサイクルと関連の処理

これらの処理を、ローカル署名とリモート署名のモデルに表すと下図となる。以下、それに基づいて説明する。

(1)ローカル署名のモデル



(2)リモート署名のモデル

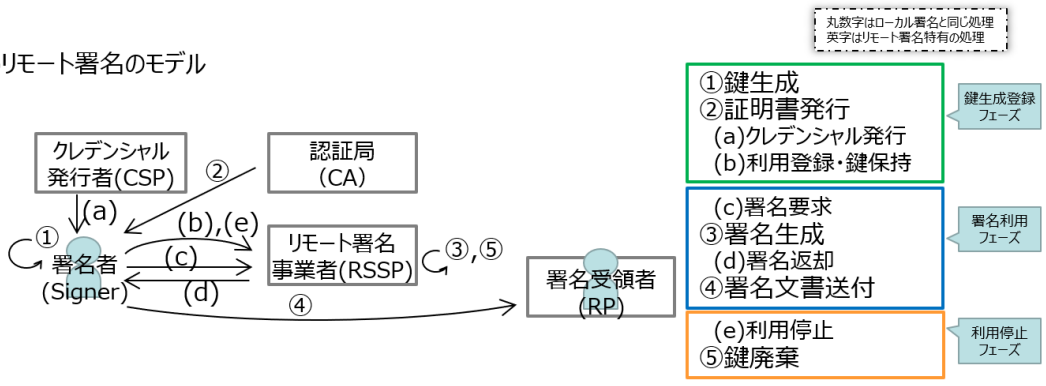


図 4-5　ローカル署名モデルとリモート署名モデルの比較（処理フロー）

（ア）鍵生成登録フェーズの処理

鍵生成登録フェーズにおいてローカル署名のモデルでは、①署名鍵生成・IC カード等への格納、②公開鍵証明書発行を行うが、リモート署名のモデルではそれに加えて、(a) 利用認証用クレデンシャルの発行、(b) RSSP への、サービス利用のためのアカウント開設や署名鍵登録（インポート/設置)、公開鍵証明書登録を行う。

(A) 鍵生成処理

前述のように、鍵生成する主体は 3 通り考えられるが、いずれも署名者の申請がトリガーとなって行われる。CA に生成依頼した場合は、生成された鍵を署名者がいったん受け取って RSSP に登録する方法と、CA から直接 RSSP に（署名者の指示の下で）渡す方法が考えられる。RSSP で鍵生成した場合は、いったん公開鍵（検証鍵）を署名者が受け取ってから CA に公開鍵証明書発行依頼する方法と、RSSP から直接 CA に依頼する方法が考えられる。署名者が鍵生成した場合も、公開鍵証明書発行申請は署名者が直接行う方法に加えて RSSP に代行してもらう方法も考えられる。いずれの方法においても、署名者の意思のもとで行われることが必要である。

また、署名鍵は新たに生成した鍵に限られるわけではなく、署名者が保持している既存の鍵を利用することも可能である。(鍵重複や脆弱性などをどう確認するかは RSSP の課題である)

なお、署名鍵の移送による漏えいや鍵重複の防止に関しては、RSSP で署名鍵を生成し移送しない方法の安全性が高いと言える。

(B) 各種登録処理

署名者は、リモート署名サービスを利用するために必要な各種手続きと、署名鍵を RSSP へ登録する。まず、署名者の本人性担保のための認証クレデンシャルを発行する。なお、認証クレデンシャルは RSSP が発行した ID で認証してもよいが、保証レベルを高めるには第三者の発行するクレデンシャル（マイナンバーカードなど）を用いることが望ましい。リモート署名を利用するために取得するものでなく、既存のクレデンシャルでもよい。本ガイドラインでは、認証クレデンシャルの発行はサービスに応じて様々な場合が考えられるため、スコープ外とするが、本人確認で注意すべき点については、本ガイドライン（パート Ⅰ）の附録 1 に示す。

次に、RSSP に利用者登録（アカウント開設）を行い、署名鍵と公開鍵証明書を登録するとともに、本人と登録する署名鍵の紐付け（鍵認可クレデンシャル SAD（PIN 等）の発行）を行う。(A)の鍵生成を RSSP が行う場合は、鍵インポートは不要となる。

RSSP は署名鍵を、自らが管理するサーバ（以下「リモート署名サーバ」という）に、適切に保管、管理する必要がある。(5 章以降に詳細を示す。)

(イ) 署名利用フェーズの処理

ローカル署名のモデルでは、署名対象を選択して③署名生成を行うが、リモート署名のモデルでは、リモート署名を利用するために RSSP にログインした後、(c)署名要求として署名対象データと署名指示（鍵の活性化・鍵認可）をリモート署名事業者に送信し、リモート署名事業者が③署名生成し、(d)署名（署名付き文書）が返却される。その後、署名者は署名付き文書の利用（署名受領者への④署名付き文書送付等）を行う。

(A) 認証処理

署名者が登録フェーズにおいて登録した本人であることをクレデンシャル RS-C で認証する。RSSP は必要に応じて、CSP に確認を行う。

(B) 署名処理

署名者は署名対象データのアップロードと署名する鍵の指定、署名指示を行い、RSSP では、署名鍵の活性化（鍵認可)、署名対象データに対する電子署名の生成を行う。この際、署名指示として対象文書ごとに署名者から RSSP に鍵認可クレデンシャル SAD(PIN 等)を送信する方法と、あるまとまりの単位で署名アプリに RSSP への送信を委ねる（署名者は署名アプリに SAD を一回だけ入力する）方法がある。

署名対象データの送信の代わりに、そのハッシュ値のみを送信してもよい。

(C) 署名検証処理

署名生成後、署名文書は署名者に返却され、署名者は利用する（必要に応じて署名者は、RP に送付する)。ここで、署名者は、意図した文書に意図したとおりの署名が付与されているか確認することが望ましく、署名検証を行うことが推奨される。

(ウ) 利用停止フェーズの処理

これは、何らかの理由により、そのリモート署名鍵の利用を停止又は終了するフェーズである。その理由としては、たとえば、有効期限の終了（更新を伴う場合もある)、失効（更新または新規発行を伴う場合もある)、リモート署名サービスの利用終了、リモート署名事業者都合による停止又は終了がある。

署名者は RSSP に停止申請するとともに、場合によっては認証局に失効申請を行う。

リモート署名事業者は、署名者の指示に基づき、リモート署名サーバ上に保管されている署名者の署名鍵等の安全な破棄などが必要である。

5 リモート署名のリファレンスモデル

5.1 リモート署名サービスの機能構成

5.1.1 機能モデル

前節で、リモート署名に関わるプレイヤの役割と処理を述べたが、ここでは、主にリモート署名を実現するリモート署名事業者の機能について述べる。

欧州の EN 419 241-1 等に基づき、署名者とリモート署名事業者、電子契約等の署名利用アプリケーションの関係と、それらが備える機能を図 5-1 に示す。

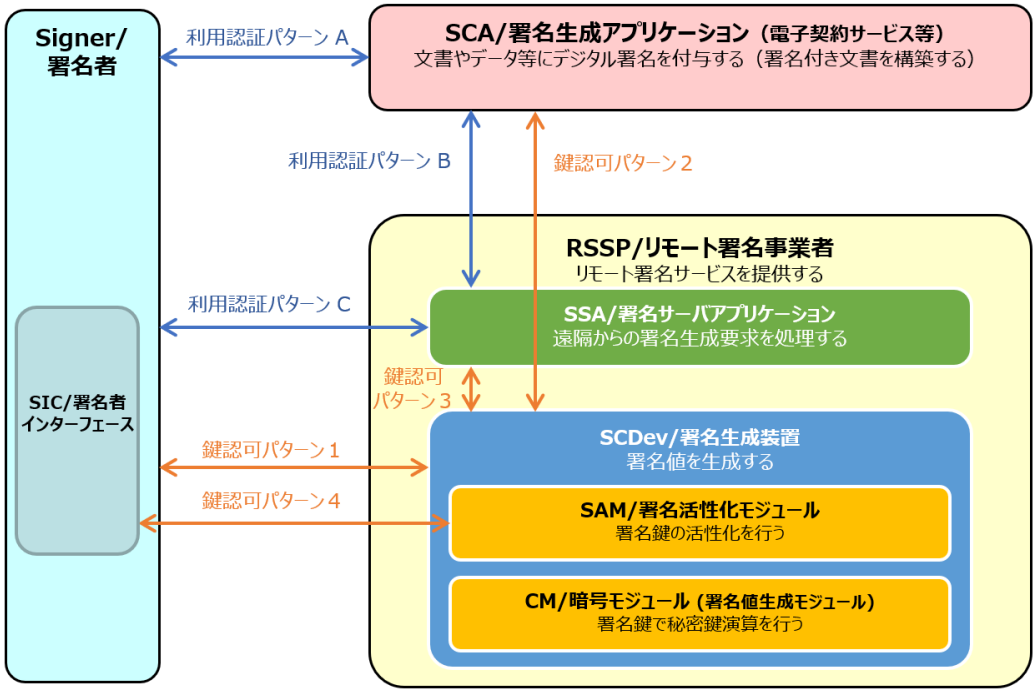


図 5-1　リモート署名の機能モデルと本ガイドラインのスコープ

5.2 リモート署名のリファレンスモデル

5.2.1 リファレンスモデルの概要

この節ではリモート署名サービスの代表的なモデルを示す。基本的なモデルとして署名者が電子契約サービス等を介してリモート署名サービスの利用を開始する基本モデル 1 と、署名者のローカル環境で実行される署名アプリからリモート署名サービスを利用する基本モデル 2 を定める。また、参考として基本モデルの派生型をいくつか例示する。

5.2.2 基本モデル 1(SCA からのリモート署名サービス利用)

このモデルでは署名者は SCA(電子契約サービス等)からリモート署名サービスの利用を開始する。SCA を経由したリモート署名サービス利用は様々なバリエーションがあり得るが、このモデルはその基本形として定める。このモデルの派生形を 5.2.4 で例示する。

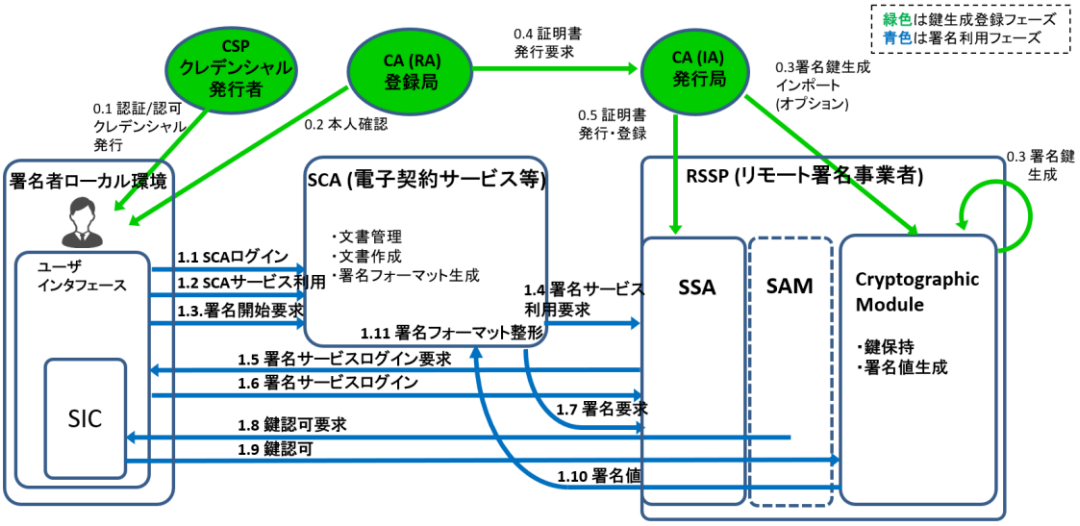


図 5-2　基本モデル 1 (SCA からのリモート署名サービス利用)

署名者は鍵生成登録フェーズにおいて、署名鍵の生成と登録、リモート署名サービスログインのための認証クレデンシャルの発行、署名実行のための認可クレデンシャルの発行、RA による本人確認を経た電子証明書発行を受ける。リモート署名サービスログインのための認証クレデンシャルと、署名実行のための認可クレデンシャルは複数要素の認証方法の組み合わせもあり得る。各クレデンシャルの発行者が別の主体であることもあり得る。

また、SCA の利用に関しても、署名者は SCA 自身の要求に従った利用登録と SCA のサービスにログインするための認証クレデンシャルの発行を受ける。

署名利用のフェーズでは、署名者はまず SCA のサービスを通じて、署名対象文書を選択し、SCA に対して署名指示を行う（図 5-2 1.1〜1.3）。そして、SCA から RSSP に対してその署名者に対する署名サービス利用開始を指示する（図 5-2 1.4）。その後、RSSP は、例えば HTTP のリダイレクション等の手法を用いて、署名者のユーザインタフェースを通じてリモート署名サービスへのログインを要求する（図 5-2 1.5）。署名者はリモート署名サービスログイン用の認証クレデンシャルを用いてログインし、リモート署名サービス利用のセッションを開始する（図 5-2 1.6）。その後、SCA から RSSP に対して署名要求が行われる（図 5-2 1.7）。この署名要求には署名対象文書のハッシュ値が指定されることが考えられる。RSSP は署名実行の認可を署名者に対して求める（図 5-2 1.8）。署名者は鍵認可のための認可クレデンシャルを用いて、署名実行を認可する（図 5-2 1.9）。この鍵認可用の認可クレデンシャルは PIN や、PIN を含んだ複数要素の認証方法を採用することがある。鍵認可の後、RSSP は Cryptographic Module で管理されている署名者の署名鍵を活性化し署名対象のハッシュ値に対して署名演算を行う。そして、その署名値を SCA に返却する（図 5-2 1.10）。その後、SCA はその署名値を署名フォーマット等に格納するなどによって文書と対応付けて管理する（図 5-2 1.11）。

リモート署名サービスへのログインから署名要求に至るフローについては、サービスによって異なる。異なるバリエーションについては 5.2.4 節を参照されたい。

5.2.3 基本モデル 2 (署名アプリからの直接利用)

このモデルでは署名者はスマートフォンや PC、デバイスのローカル環境にインストールされた署名アプリからリモート署名サービスに接続し署名値生成を行う。

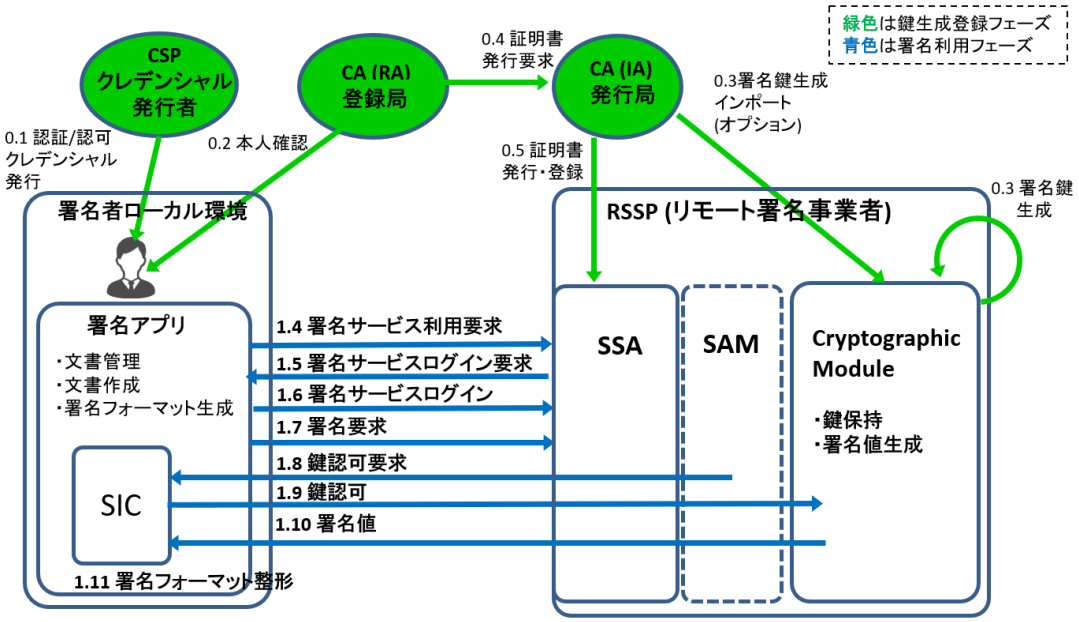


図 5-3　基本モデル 2 (署名アプリからの直接利用)

署名登録フェーズは基本モデル 1 と同様である。

署名利用のフェーズでは、署名者はまず署名アプリを起動し、RSSP にログインする（図 5-3 1.4～1.6)。その後、署名者は署名対象文書を選択し、RSSP に対して署名要求を行う（図 5-3 1.7)。このとき、署名アプリは署名対象文書を持ち、その文書データからハッシュ値を演算し、そのハッシュ値を署名要求に含めることが考えられる。その後、RSSP は署名実行の認可を署名者に対して求める（図 5-3 1.8)。署名者は鍵認可のための認可クレデンシャルを用いて、署名実行を認可する（図 5-3 1.9)。図 5-3 1.7～1.9 のフローはサービスにより、一組の要求応答メッセージとなっている場合も考えられる。

この鍵認可用の認可クレデンシャルは PIN や、PIN を含んだ複数要素の認証方法を採用することがある。鍵認可の後、RSSP は Cryptographic Module で管理されている署名者の署名鍵を活性化し署名対象のハッシュ値に対して署名演算を行う。そして、その署名値を署名アプリに返却する（図 5-3 1.10)。その後、署名アプリはその署名値を署名フォーマット等に格納するなどによって文書と対応付けて管理する（図 5-3 1.11)。

5.2.4 基本モデルの派生形（参考）

5.2.4.1 SCA を介した認証認可のケース

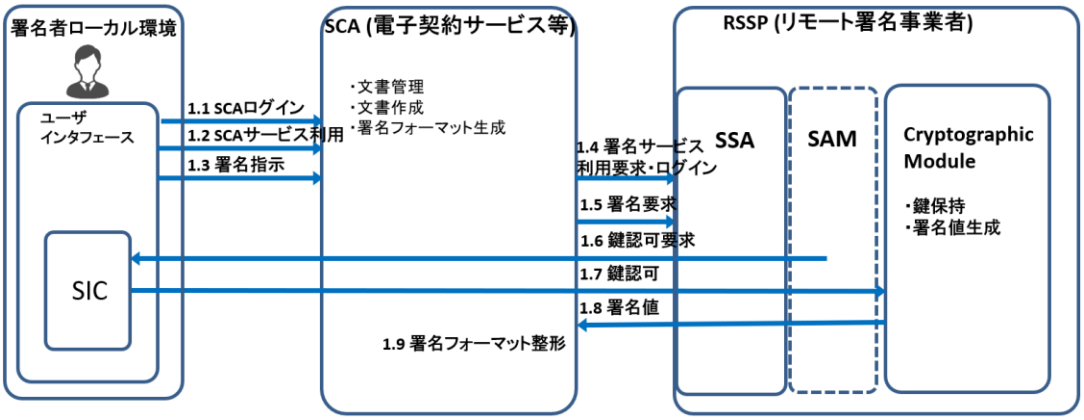


図 5-4　派生形（SCA を介した認証認可の例）

このモデルは RSSP のログイン時の認証や鍵認可のフローを SCA が仲介するケースである。この場合、SCA が、認証クレデンシャルを用いた RSSP のログインや、署名者と RSSP の間のセッション、鍵認可などの通信内容、クレデンシャルに関連する秘密の情報を SCA によって知られる可能性があるため、RSSP による技術的な対策や SCA での適切な運用が求められる。

図 5-4 1.4 での SCA から RSSP へのログイン要求は、署名者ごとの ID を使う場合もあれば、SCA と RSSP との間で契約された契約ごとの ID(例えば、あるユーザグループごとに割り振られた ID や、企業や組織ごとに割り振られた ID など)が用いられることもが考えられる。一方、鍵認可については署名者ごとに割り当てられた認可クレデンシャルが用いられる。

5.2.4.2 認証連携を用いるケース

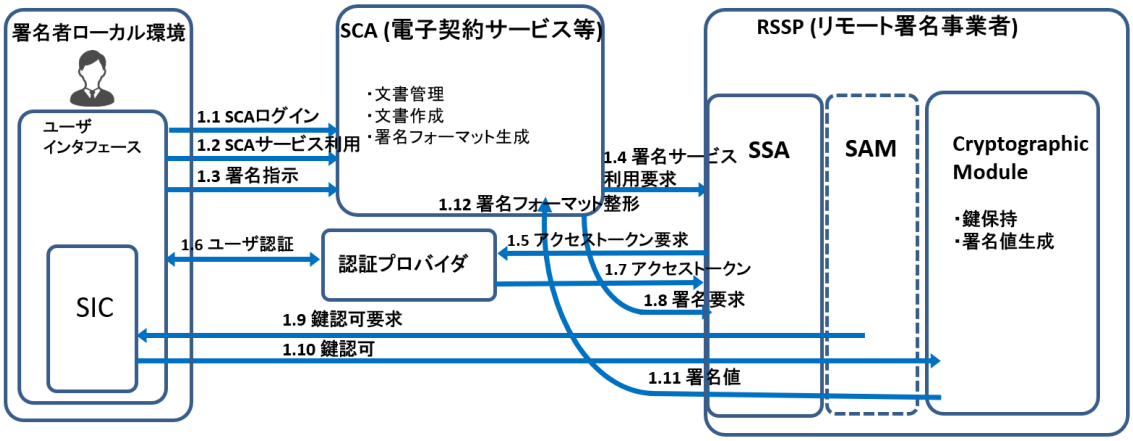


図 5-5　派生形（認証連携の例）

図 5-5 は RSSP のログイン時に外部の認証プロバイダ（IdP）を用いた認証連携を行う場合のモデルを示したものである。基本モデル 1 とほぼ同じフローであるが、RSSP のログイン時に認証プロバイダによるアクセストークンを使用する点が異なっている。RSSP は署名者のログインのために認証プロバイダにアクセストークンを要求する。署名者の認証やアクセストークン発行の認可が必要な場合には、認証プロバイダは署名者に認証やアクセストークン発行の確認を行った上で、RSSP に対してアクセストークンを発行する。RSSP はそのアクセストークンをもって署名者に対し RSSP のサービス利用を許可する。このモデルは SCA と異なる主体が認証プロバイダを運営する場合、5.2.4.1 のように、RSSP のログインのための秘密の情報を SCA に知られる可能性がないことが利点である。

6 セキュリティ対策を検討すべき事項

6.1 電子署名の要件

電子署名には一般的に以下の性質が要求される。

- 電子署名によって意思を示す本人（署名者）を特定できること。
- 電子署名の対象となった文書が署名者本人の意図したものであること。
- 署名者本人が意図しない文書に対して電子署名が作成されないこと。

電子署名を PKI によって実現する場合、上記の性質は以下のより具体的な要件で示される。

- 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。
- 署名者本人は自身の署名鍵を用いて、意図したデータに対して署名を生成することができる。
- 署名者本人以外の者がその署名鍵を用いて、署名者本人が意図しないデータに対して署名データを生成することができない。

4 章及び 5 章で述べたように、リモート署名は署名鍵を第三者機関が管理するモデルであり、認証局から署名者の公開鍵証明書の発行やリモート署名サービスでの署名鍵管理、署名鍵利用などで複数のシステム要素にまたがった処理フローによって成り立っている。各システム要素や処理フローの過程において、上記の電子署名として成立するための要件が覆される脅威への対策が必要となる。次節以降では、5.2 節の基本モデル 1 と基本モデル 2 を前提として、電子署名として成立するための要件を覆す要因となる脅威について整理する。

なお、SCA 及び署名者のローカル環境（署名アプリなど）については今後の課題である。

6.2 登録フェーズにおける脅威

登録フェーズにおける脅威は、署名者登録、署名者管理、証明書署名要求、署名鍵のインポートがある。

6.2.1 署名者登録等における脅威

6.2.1.1 RSSP において、RSSP の利用者 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[1]。

6.2.1.2 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。

6.2.1.3 攻撃者は登録中に登録情報を取得する。

6.2.1.4 攻撃者は登録時に署名者になりすます。

（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定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。

6.2.2 署名者管理における脅威

6.2.2.1 攻撃者は特権ユーザを偽装し、登録情報を更新する。

6.2.2.2 攻撃者は更新中に認証情報を開示する。

6.2.3 証明書署名要求における脅威

6.2.3.1 攻撃者が CSR のデータを変更する。

6.2.3.2 攻撃者が詐称して CSR を行う。

[1] 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。

6.2.4 署名鍵のインポートにおける脅威

6.2.4.1　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。

6.2.4.2　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。

6.2.4.3　攻撃者が自分の鍵を他人の鍵情報でインポートする。

6.2.4.4　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。

6.3 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、署名利用フェーズ全般、鍵利用・管理における脅威と内部不正者による脅威がある。

6.3.1 利用フェーズにおける脅威

6.3.1.1　攻撃者は、認証情報を変更する。

6.3.1.2　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。

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

6.3.1.4　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。

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

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

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

6.3.1.8　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。

6.3.1 鍵利用・管理における脅威

6.3.1.1　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。

6.3.1.2　攻撃者は共通鍵／秘密鍵を導出する。

6.3.1.3　攻撃者は CM 格納時に、鍵及び鍵の属性を不正に変更する。

6.3.1.4　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。

6.3.1.5　攻撃者は鍵を乱用（許可されていない鍵を利用）する。

6.3.1.6　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。

6.3.1.7　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。

6.3.1.8　攻撃者は CM に対して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）

6.3.2 内部不正者による脅威

6.3.2.1　攻撃者（内部者）が運用管理者に詐称し署名鍵を利用する。

6.3.2.2　攻撃者（内部者）が監査者に詐称しログを得る。

6.3.2.3　攻撃者（内部者）が署名鍵の活性化情報を得る。

6.4 利用停止(破棄)フェーズにおける脅威

6.4.1.1　攻撃者（本人以外）が利用停止（破棄依頼）する。

6.4.1.2　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）。

7 セキュリティ対策事項

6 章のセキュリティ検討事項に対するセキュリティ要件を示す。セキュリティ対策事項は、一般的なセキュリティ要件（本ガイドライン・パート I の 7.1 節)、セキュリティ機能要件として署名活性化モジュールに関する要件（本ガイドライン・パート II の 3 章)、署名値生成モジュールに関する要件（本ガイドライン・パート III の 3 章）で構成する。

7.1 一般的セキュリティ要件

7.1.1 役割・組織の管理

7.1.1.1 リモート署名サービスは異なる特権をもつ役割をサポートすること。

7.1.1.2 リモート署名サービスは少なくとも次の特権を持つ役割をサポートすること。

セキュリティ統括責任者（Security Officers）： セキュリティポリシーの確実な実施に対する責任を有し、セキュリティ関連情報を管理する者。

システム管理者（System Administrators）：リモート署名サービス関連システムのインストール、設定及びメンテナンスの権限を有する者。セキュリティ関連情報へのアクセス権はない。

システム運用担当者（System Operators）：リモート署名サービスの運用に関する責任を有し、システムバックアップ及びリカバリの権限を有する者。

システム監査者（System Auditors）：システム運用がセキュリティポリシーに従った運用であるか監査し、其の為にアーカイブや監査ログを確認する権限を有する者。

7.1.1.3 リモート署名サービスは少なくとも以下の特権をもたない非特権役割をサポートすること。

署名者（Signer）：SAP によって SAD をリモート署名サービスに受け渡すことにより、文書又は DTBS/R に署名する者。
秘密鍵と公開鍵をリモート署名サービスに送ることが認められている。

SCA：署名者による署名を得るために、リモート署名サービスに DTBS/R リクエストを

送ることが認められている。

RA：CSR（証明書署名要求）に対して、リモート署名サービスに公開鍵証明書を送ることが認められている。

CA：署名者からの要請に従い、リモート署名サービスに署名者の秘密鍵と公開鍵及び電子証明書を送ることが認められている。

7.1.1.4 全ての特権をもつ役割を一人で担ってはならない。また、一人で二つ以上の特権を持つ役割を担うべきではない。

7.1.1.5 特権を持つ役割のユーザと特権を持たない役割に係るユーザは互いに関与しないこと。

7.1.1.6 リモート署名サービスはセキュリティ統括責任者とシステム監査者を兼任しないことを保証すること。

7.1.1.7 リモート署名サービスは、システム管理者の役割及び/又はシステム運用者の役割を担うユーザがシステム監査者及び/又はセキュリティ責任者の役割を担うことないことを保証すること。

7.1.1.8 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。

7.1.1.9 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。

Note：非特権ユーザのアクセスの際には、特権を持つ役割を担う者が同行し監視すること。

7.1.1.10 特権をもつシステムユーザのみが全ての関連するアプリケーション及びインタフェースを通してリモート署名サービスを管理する広範な権限をもつこと。

7.1.1.11 システム運用

7.1.1.11.1. リモート署名サービスは以下を実現する為に必要な内容を含むマニュアル

を提供すること。

- 正しく安全な運用
- システム故障のリスクが最小限となるような方法での設置
- システム及び扱う情報の完全性を保証するために、ウィルス及び悪意のあるソフトウェアから保護

7.1.1.11.2. リモート署名事業者は、7.1.1.2 で要求されている 4 つの特権をもつ役割の責任を対象とするシステム文書を提供すること。それには次を含むべきである。

- インストールガイダンス
- 管理ガイダンス
- ユーザガイダンス

7.1.1.12 時刻同期

電子署名の生成と検証には時刻が重要な要素となっている為、リモート署名サービスが標準時刻に適切に同期していることが必要である。

7.1.1.12.1. リモート署名事業者は、リモート署名サービスの時刻精度とその確認方法を表明すること。

7.1.1.12.2. 監査済みイベントの時刻精度を確認するために、標準時刻源と適切に同期している時刻源を使用するべきである。

7.1.1.12.3. 電子証明書の有効期限が切れているかどうかを確認するために、UTC と適切に同期している時刻源を使用すること。

7.1.2 識別及び認証

7.1.2.1 リモート署名サービスは各ユーザがリモート署名サービスに対してアクションを認める際に、各ユーザの識別と認証を実施すること。

7.1.2.2　ログアウト後の再認証を必須とすること。

7.1.2.3　認証データの組み合わせを使用する場合、容易に予測できないものであること。

7.1.2.4　特権ユーザについては、有効なセッションの時間を定義し、一定時間以上の経過によってセッションを停止する等の措置を取り、セッション乗っ取りのリスクを低減すること。

7.1.2.5 認証失敗

7.1.2.5.1. ユーザ認証エラーの回数を管理し、限度を超えたユーザ認証エラーが発生した場合、一定期間或いは管理者によるアンロックが行われるまで、同一ユーザによるユーザ認証を認めないこと。

7.1.3 システムへのアクセスコントロール

7.1.3.1　リモート署名サービスは、特定のユーザだけがアクセスを許可されたシステム及びユーザオブジェクトに対し、アクセスコントロールを実施すること。

7.1.3.2　リモート署名サービスは機密性の高い残存情報へのアクセスコントロールを実施すること。

7.1.4 監査及びログ

7.1.4.1　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

ユーザ署名イベントには、署名鍵に関連付けられた公開鍵証明書に関する情報を含むこと。

リモート署名サービスへのすべてのアクセス試行をログするべきである。

7.1.4.2　リモート署名サービスは、外部記憶装置への監査情報伝達に失敗した場合の措置を定めること。

7.1.4.3 監査データ可用性の保証

7.1.4.3.1. リモート署名サービスは監査データを保持し、すべての監査データを保管する措置をとること。

7.1.4.3.2. 監査機能は情報を追記するのみであること。

7.1.4.3.3. リモート署名サービスは、監査証跡に保存された監査レコードに不正削除が行われないよう保護すること。

7.1.4.3.4. 監査レコードは、外部記憶装置にアーカイブしたときに削除することができる。

7.1.4.4 監査データパラメータ

7.1.4.4.1. すべての監査レコード（サービス別監査ログを含む）は、次のパラメータを含むこと。

- イベントの日時
- イベントのタイプ
- アクションに対して責任を負う実体（ユーザ、管理者、プロセス等）の識別
- イベントの成否

7.1.4.5 選択可能な監査レビュー

7.1.4.5.1. リモート署名サービスは、イベントの日付、タイプ及び/又は利用者 ID による監査ログの検索を可能にすること。

7.1.4.5.2. 監査レコードは、システム監査者が理解しやすい形式で処理及び提示が可能であること。

7.1.4.6 制限付き監査レビュー

7.1.4.6.1. リモート署名サービスは、監査記録へのアクセスについて、システム監査者等一部のユーザを除きデフォルト設定で拒否すること。

7.1.4.7 警告の生成

7.1.4.7.1. リモート署名サービスは、リモート署名システムの本章で識別されているセキュリティ要件を満たす能力に影響を与える可能性のある異常イベントに対して通知する警告を適時に生成すること。

その他の異常イベントについても検知されたときに警告を発するメカニズムを実行するべきである。警告は関連のある管理者への通知のきっかけとなるべきである。

警告はまた、潜在的な攻撃パスをカットするなど、潜在的な攻撃に対応する措置を始動させることができる。

ユーザアクティビティに関係する異常イベントの例には次があげられる（がこれに限られるものではない）：

- 標準的な使用時間を超えたユーザアクション
- 異常速度で行われるユーザアクション（人以外の介入を検知するため）
- 規定プロセス内の標準的なアクティビティを省いたユーザアクション
- 重複するユーザセッション

7.1.4.8 監査データの完全性の保証

7.1.4.8.1. リモート署名サービスは、監査データの完全性を保証すること。

7.1.4.8.2. リモート署名サービスは、監査データの完全性を検証する機能を提供すること。

7.1.4.9 監査タイミングの保証

7.1.4.9.1. 監査イベントの時刻精度を保証するために、要件 7.1.1.12 を適用する。

7.1.5 アーカイブ

7.1.5.1 アーカイブ

7.1.5.1.1. リモート署名サービスは、外部メディアでのアーカイブ生成の能力をもつこ

と。保存及び情報提供の観点から適切な外部メディアを選択するべきである。

7.1.5.1.2. すべての監査ログをアーカイブすること。

7.1.5.1.3. 各アーカイブエントリにはアーカイブの時刻を含むこと。

7.1.5.1.4. アーカイブには、リモート署名サービスユーザパスワードなどの機密性の高いセキュリティパラメータを含まないこと。

7.1.5.2 アーカイブデータの完全性

7.1.5.2.1. アーカイブにおけるエントリの不正変更が行われないよう防止すること。不正変更を検知するために、完全性を検証するメカニズムを実行すること。

7.1.6 内部不正対策

内部不正対策は、7.1.1 役割・組織の管理及び 7.1.4 監査及びログを参照。

7.1.7 バックアップ・リカバリ

7.1.7.1 バックアップ情報の完全性及び機密性

7.1.7.1.1. バックアップ情報の完全性の検証を可能にするメカニズムによる変更からバックアップを保護すること。

7.1.7.1.2. 高感度のセキュリティパラメータ及びその他機密情報は、機密性及び完全性を確保するために保護された形で保管すること。

7.1.7.2 リカバリ

7.1.7.2.1. リモート署名サービスは、バックアップからシステムの状態を復元できる回復機能をもつこと。

7.1.7.2.2. 十分な特権を持つ役割にリンクしているユーザは、要求に応じてバックアップからの回復機能を起動することができること。

7.2 組織・運営

組織のセキュリティ対策及び運営に関しては、主に ISO/IEC27002（JIS Q 27002）の「6 情報セキュリティのための組織」に規定する管理策の推奨基準を適用するものとする。以下に、リモート署名事業に係る管理対策を示す。

リモート署名に関係するプレイヤであるリモート署名事業者、クレデンシャル発行者、認証局については、組織・運営のために ISO/IEC27002 を参照して情報セキュリティ管理策を実施する。
なお、以下に ISO/IEC27002 に記載されていない詳細を以下に説明する。

7.2.1 職務の分離

リモート署名に関係するプレイヤであるリモート署名事業者、クレデンシャル発行者、認証局については、同一法人がすべての機能の提供を行う事が可能である。また、リモート署名事業者においては特に重要な職務の権限の分離を行う必要がある。（詳細は 7.1.1 役割・組織の管理、参照）

7.2.2 事業継続管理

リモート署名事業者は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。特に、署名者の署名鍵の管理については、危殆化が疑われる状況を生み出さないよう必要な要求事項をあらかじめ定めておく必要がある。（例示：危殆化が疑われた状況では、鍵を失効する等の対策を行うこと）

7.2.3 コンプライアンス

リモート署名の利用分野は、電子商取引、電子契約、電子申請など様々であるが、リモート署名の応用分野は、電子署名済みデジタルドキュメントの長期的な保存などもあり、利用分野の個別法を遵守する必要がある。リモート署名事業者やリモート署名を利用したアプリケーションサービス提供者などは、自らのサービスが個別法の、どの要件に対してどのように対応しているか、またリモート署名サービスの利用を行う企業や組織、署名者（以降、利用関係者）に対しては、どのような運用や追加的対策が求められるか示す必要がある。自らのサービスポリシーに重要項目を記載し、利用関係者に対して自らのサービスの理解を促す必要がある。

8 参照情報

[1] EN 419 241-1 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

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

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

[4] 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

[5] 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

[6] NIST Special Publication 800-63 Revision 3 Digital Identity Guidelines

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

[8] 日本データセンター協会、 Japan Data Center Council（JDCC)、データセンターセキュリティガイドブック、データセンターファシリティスタンダード

[9] ISO/IEC 27002 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範 Information technology -- Security techniques -- Code of practice for information security management

[10] ISO/IEC 27017:2015 情報技術－セキュリティ技術－ISO/IEC27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[11] 電子署名及び認証業務に関する法律

[12] 電子署名及び認証業務に関する法律施行規則

[13] 電子証明書に格納された属性情報の信頼性と利用に関するガイドライン、電子認証局会議

[14] 行政手続におけるオンラインによる本人確認の手法に関するガイドライン、2019 年（平成 31 年）2 月 25 日、各府省情報化統括責任者（ＣＩＯ）連絡会議決定

[15] 電子契約活用ガイドライン Ver.1.0（2019 年 5 月)、公益社団法人日本文書情報マネジメント協会

[16] 電子文書の信頼性向上ガイドライン第 1 版（2019 年 3 月)、公益社団法人日本文書情報マネジメント協会

附録１　本人確認

リモート署名サービスを選定する際に参考となるリモート署名事業者のサービスポリシーの例示として事項及び内容を説明する。はじめに、リモート署名を利用する署名者の本人確認、RA による電子証明書発行の為の本人確認を示し、その後、附録 2 に事業者のサービスポリシーの例示を示す。

1　リモート署名を利用する署名者の本人確認

リモート署名における署名者の本人確認には、RA による電子証明書発行の為の本人確認とリモート署名事業者によるアカウント登録のための本人確認の二つを分けて考える必要がある。

- RA は電子証明書に記載される本人の身元確認及び電子証明書の記載内容が真正なものであることの確認に責任を負う。
- RSSP は、鍵生成をした者が鍵を利用する署名者と同一であること、及び、当該署名者の秘密鍵と公開鍵の紐づけて管理することに責任を負う。
- RSSP が鍵ペアを生成するモデルで、CA が直接署名者に電子証明書を交付しないケースでは、RSSP は署名者が秘密鍵と電子証明書を利用する際のアカウント登録の当人認証やリモート署名を利用する際の当人認証に責任を負う。

2　RA による電子証明書発行の為の本人確認

本ガイドラインの 6.2 節の記載と同様に、RA における電子証明書発行時の本人確認時におけるなりすまし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定の議論は従来からなされており、認証局運用規程に関する別の文書を参照のこと。

附録 2　サービスポリシーで署名者が確認すべき事項

リモート署名事業者は、署名者あるいは依拠当事者が事業者の提供するリモート署名サービスが特定の用途に対して信頼できるサービスであるか判断出来るように、提供するリモート署名サービスに関する以下の文書類を策定／維持／公開すべきである。

- リモート署名サービスポリシー
- リモート署名サービス運用規定
- サービス利用規約

リモート署名サービスポリシーは本ガイドラインの 7 章で定めるセキュリティ要件に対して事業者がどのような方針でサービスを運用しているかを示す文書であり、リモート署名サービス運用規定は、方針に対する実際の実装及び運用を規定するものである。サービス利用規約についてはサービス利用に係る制限やリモート署名サービスを直接利用する企業・組織や署名者、リモート署名サービスを用いたアプリケーション提供事業者の責任等を規定する文書である。

ここでは署名者あるいは依拠当事者がポリシー文書類を確認する際に特に重要な点について解説する。

1 本ガイドラインを含む特定のセキュリティ要件やポリシーへの適合宣言

全ての署名者あるいは依拠当事者が特定のリモート署名サービスを利用開始する前に、上述のリモート署名サービスポリシー及び運用規程を隈なく確認し、リモート署名サービスのセキュリティ対策等が期待しているレベルにあるか確認することを期待するのは非現実的である。一方で本ガイドラインや ETSI 規格等では専門家によってリモート署名サービスが満たすべき要件を規定しており、リモート署名事業者が本ガイドラインや ETSI 規格等の特定の基準（例えば本ガイドラインであれば、レベル 1、レベル 2、レベル 3 の何れかの基準）に対して適合性をリモート署名サービスポリシー内で主張することで、リモート署名サービスを直接利用する企業・組織や署名者及び依拠当事者がサービスを信頼する際に容易に評価できるようになる。従ってリモート署名サービスを直接利用する企業・組織や署名者及び依拠当事者は、まずリモート署名サービスポリシー内で特定のセキュリティ要件やポリシーへの適合宣言を確認すべきである。

2 第三者監査及び認証

本ガイドラインを含む特定のセキュリティ要件やポリシーへの適合宣言については自己宣言に加えて信頼できる第三者機関による監査及び認証によってその適合性が保証されることによって、より高い信頼性を主張することができる。署名者及び依拠当事者は、特定のセキュリティ要件やポリシーに対する適合性の自己宣言だけでなく、その適合性が信頼できる第三者機関によって定期的に監査されていることを確認すべきである。その為にリモート署名事業者はリモート署名サービスポリシー内に第三者監査及び認証に関する方針を定め、また、当該第三者機関が発行する監査証あるいは認証証へのリンクを示すべきである。

3 署名者の義務

リモート署名サービスはサービスの署名者が一定の義務を満たすことを前提に設計／運営されており、署名者はサービスが求める署名者が果たすべき義務についての情報を事前に確認すべきである。

リモート署名サービスにおける署名者の義務については、一般に以下が考えられる。

a)サービス利用申請
誤った情報に基づいた利用申請の禁止
b)認証クレデンシャルの管理
認証クレデンシャルの適切な管理と危殆化時の迅速な連絡
c)署名鍵の管理
署名者の署名鍵を署名者あるいはその代理人がリモート署名サービスにインポートする場合、その署名鍵の適切な管理
d)失効要求
署名者の登録情報の変更やクレデンシャル及び署名鍵の危殆化に伴う迅速な失効要求

4 SLA（Service Level Agreement）

署名者は提供されるサービスの品質、可用性及び性能について、署名者及び依拠当事者の用途に対して適切なレベルであるかを確認すべきである。

5 署名検証方法

署名者及び依拠当事者はリモート署名サービスによって生成される電子署名の検証方法

について、署名者及び依拠当事者の用途に対して適当な方法で検証可能かを確認すべきである。

6 電子証明書の失効・鍵の破棄等の手続き

署名者は電子証明書の失効及び鍵の破棄について、署名者の用途に対して適当な方法で失効要求及び破棄の要求が可能かを確認すべきである。また、失効要求及び鍵の破棄の受付時間に関しても制限がある場合がある。どのような手順で失効及び鍵の破棄手続きを行えるのかを確認すべきである。

7 サービスの利用制限

署名者及び依拠当事者は、リモート署名サービスの利用に係る制限について、事前に確認すべきである。例えば、契約書への署名において、上限額等が定められている場合がある。

8 サービスの利用終了・終了・移行の案内

署名者がサービスの利用を終了する場合（サービスの利用終了)、事業者がサービスを終了する（サービスの終了）又は、他の事業者のサービスに移行する（サービスの移行）場合を想定し、署名者はリモート署名サービスのサービス利用終了・終了・移行に関して、署名者及び依拠当事者への事前の通知やサービス終了後にどのような情報提供等を受けられるか（例：事前の別サービスへの移行案内等）について、確認すべきである。

9 個人情報の取り扱い

署名者はリモート署名事業者における署名者の個人情報の取り扱いについて、受け入れられる内容であるか確認すべきである。例えば、リモート署名サービスの提供用途外での個人情報の利用や、第三者への個人情報の提供等について定められており、同意を求められる場合がある。

10 苦情申し立て

署名者及び依拠当事者はリモート署名サービスに関する苦情の申し立て手続き、苦情受付窓口及びリモート署名事業者における苦情処理プロセスに関する情報を確認すべきである。

11 適用法令

リモート署名サービスについてはそのサービスの一部または全てが国外の事業者によって提供されている場合もあり、署名者は提供されるサービスがどの法令に従って提供されているかを確認する必要がある。また、係争時の管轄裁判所と適用法令についても確認すべきである。

12 記録の保管期間と提供

リモート署名サービスは、リモート署名が付された電子文書の真正性について疑義が生じた際や係争時に、そのリモート署名が署名者の意図に基づいて生成されていることに関する記録を提供することが求められる。その為、署名者及び依拠当事者は、署名の用途に応じて適切な期間記録が保管されるかを確認すべきである。またリモート署名事業者がどのような場合において記録を提供するかを確認すべきである。

13 補償内容

署名者及び依拠当事者はリモート署名サービスを利用あるいは依拠することで生じる損害の補償と補償条件、その限度額について確認すべきである。

14 リモート署名サービスの連絡窓口

署名者及び依拠当事者はリモート署名事業者の連絡先情報が公開されていること、およびその連絡の手段について確認すべきである。

附録 3　署名結果の確認

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。

リモート署名では、署名者が意図した署名対象文書に正しく署名されたことを確認する必要がある。少なくとも、誰が（署名者 ID）、何に（署名対象）、署名処理を行った（処理結果）であるかを表示する。その他、署名時刻や検証結果等も表示して署名結果を署名者に確認させる。これらの確認項目の詳細化を検討し、必要応じて求められる要件を検討する必要がある。

表 A-1 署名結果の表示項目

項目	要求	概要
処理結果	必須	正常に署名処理が完了したかどうか
署名者 ID	任意	認証クレデンシャル（RS-C）のうち署名者識別の ID 等 ※ ただし署名者 ID が秘匿対象であれば表示しない。
署名対象	任意	署名の対象となるファイル名、または署名する内容等
署名文書	任意	生成された署名文書のファイル名等
署名時刻	任意	リモート署名を行った時刻 ※ タイムスタンプの時刻が望ましいがシステム時刻でも良い。
署名者名	任意	公開鍵証明書の Subject 要素等 ※ 判別が付く場合には CN 項目だけでも良い。
検証結果	任意	署名の検証結果（改ざん有無や署名フォーマット準拠等）を表示 ※ 第三者による検証（認証局による検証等）が望ましい。 ※ 必要に応じて検証レポートを表示できるとなお良い。

附録 4　利用停止処理

利用停止の要因としては、有効期限の終了（更新を伴う場合もある）、失効（更新または新規発行を伴う場合もある）、リモート署名サービスの利用終了、リモート署名事業者都合による終了がある。

(1) 有効期限の終了（更新を伴う場合もある）の場合

- RSSP は、鍵の有効期限を管理している場合、期限前に署名者に通知し、更新を要求される場合は、旧鍵を廃棄し、鍵生成登録時の手順に従い新鍵を生成・登録する。旧鍵の署名を継続する必要がある場合、新鍵による旧鍵の公開鍵証明書の相互認証証明書を発行してもらうケース等もある。

(2) 失効（更新または新規発行を伴う場合もある）

- 署名者または CA 等から何らかの要因（危殆化など）で鍵の失効を通知された場合、RSSP は速やかに旧鍵を廃棄する。

(3) リモート署名サービスの利用終了

- 署名者からリモート署名サービスの利用終了を通知された場合、RSSP は速やかに鍵を廃棄、または署名者に引き渡して廃棄する。

(4) リモート署名事業者都合による終了

- RSSP のサービス終了やインシデント（漏洩など）が発生した場合、鍵が継続利用できる場合は署名者に引き渡し、鍵の継続利用不可の場合は速やかに廃棄するとともに然るべき措置を講じる。

いずれの場合も、リモート署名事業者は使用しなくなった署名者の署名鍵等の重要情報を安全かつ確実に破棄（削除）する必要がある。

附録５　システムログと監査ログ

リモート署名は、電子契約や電子申請などの利用も想定されている為に、自動的に保存されるシステムログの他に、監査ログが必要となる。監査ログでは監査人が調査を行う際に必要となる情報、つまり「いつ」「だれが」「何をしたか」を確認できる必要がある。また法規制や運用ポリシーに違反をしていないか、また標準に準拠しているかを判断する材料となる情報である。

自動的に保存されるシステムログは、例えば NIST SP 800-92 「コンピュータセキュリティログ管理ガイド」等の標準仕様を参考にして適切かつ必要な情報が保存されるように設定と運用を行う。SP 800-92 ではセキュリティログとして、「セキュリティソフトウェア」「オペレーティングシステム」「アプリケーション」の 3 種類が定義されているが、これらがシステムログの分類と言える。以下の利用者は、本ガイドラインの主に署名者を想定する。

表 A-2 NIST SP 800-92 によるシステムログの分類

システムログの分類	概要
セキュリティソフトウェア	認証サーバ、侵入検知、ウイルス・マルウェア対策等の独立したセキュリティソフトウェアが生成するログ。
オペレーティングシステム	システムイベント等のログ。適切な OS 設定により必要なログを出力する。
アプリケーション	利用されるアプリケーションと連携する全サーバ・システムの利用ログ。利用者の要求とその応答、アカウントの情報操作（認証成否や変更等）、利用状況（トランザクション数等）、重要な運用アクション（アプリケーション起動・終了や運用状況、設定変更情報等）を保存。

システムログを保護する為には、システム時刻の同期、改ざん防止策、アーカイブとローテーション等のポリシーを適切に設定して運用を行う必要がある。またパスワード等の認証秘匿情報は保管してはならない。

監査ログは大別すると、利用者や管理者の行動を追う為の「トランザクションログ」と、リソースアクセスに関する「アクセスログ」に分けられる。時間帯や ID 等を指定して監査ログの生成を可能にすべきである。監査ログは、なりすましや改ざんの有無等の判断材料となる情報である。

表 A-3 監査ログの分類

監査ログの分類	概要
トランザクション	利用者および管理者の行動を追跡する為のログ情報。

アクセス	システムイベント等のログ。適切な OS 設定により必要なログを出力する。

システムログから監査ログを生成する際のシステムログの項目等は、事前に検討を行い決めておく必要がある。またシステムログを解析するツールの利用も検討すべきである。監査人は監査証跡の 1 つとして監査ログを利用することができる。監査証跡は監査ログ以外にも、入手可能なあらゆる情報を使い構成された情報である。

附録 6　設置・環境

電子署名を行うために必要な符号類を適正に管理できるようにするという観点からリモート署名サーバの設備環境の詳細を検討した結果を参考として示す。なお、詳細化の検討については、ISO/IEC 27002、ISO/IEC 27017 をベースに特定認証業務の認定に係る調査表（一般財団法人日本情報経済社会推進協会）、データセンターセキュリティガイドブック（日本データセンター協会、 Japan Data Center Council（JDCC））を参照した。これらの参照文献を基に検討した結果、物理的及び環境的セキュリティについては、以下を前提とする。

- 該当する地域標準、国内標準及び国際標準が要求するレベルの抵抗力を確立するために、隔壁と併せて、警報機能を備え、監視し、試験する。
- ハウジング、クラウド環境の両方においては、本事項は契約等によりサービス提供企業にて対応されるものとする。

1　物理的セキュリティの考え方

署名者の署名鍵、または署名者の署名鍵の暗号化で使用する共通鍵を保護するために、署名を行う装置（CM を構成するための設定済みソフトウェアまたはハードウェア）は、通常のデータセンター環境よりも高いセキュリティが必要である。このため、一般のコンピュータラックを設置する環境を「コロケーションエリア」と定義する。この「コロケーションエリア」よりも高いセキュリティの環境を定義して、当該エリア（または領域）を「CM 設置室」（仮称）と呼んで明確に区別する。

なお、上記の高いセキュリティの環境で CM をハードウェア（HSM）またはソフトウェアで構成する場合に、以下の考え方があるが、ビジネスモデルに基づき検討が必要。

1. 高いセキュリティの「CM 設置室」の領域に設置することが望ましい。
2. HSM を組み込むサーバ類は一般環境である「コロケーションエリア」に置いても良いものとする。
3. CM をソフトウェアで構成する場合には、不正アクセスを行おうとすると自己破壊（署名鍵などの重要情報のゼロ化）を行う HSM の耐タンパ性の特性と同等のレベルでのデータ保護が可能かをリモート署名事業者が検討する必要がある。

2　セキュリティを保つべき領域

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。

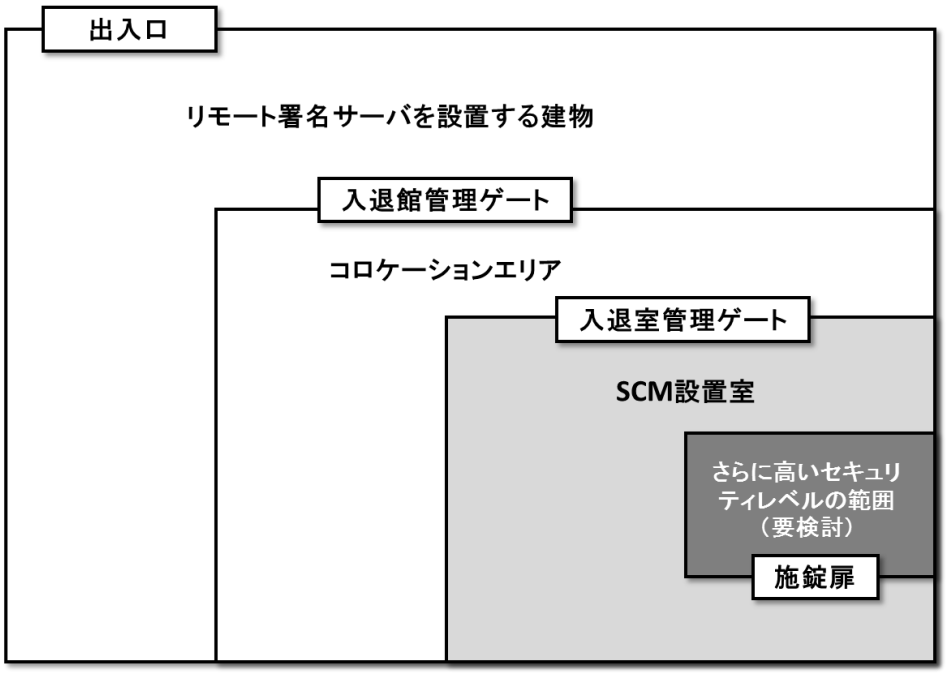


図 A-1 物理的セキュリティ境界のイメージ図

2.2 物理的入退管理策

「リモート署名サーバを設置する室」には、認可されたものだけにアクセスを許可するために以下の事項を考慮することが望ましい。

イ　入室する二以上の者の身体的特徴の識別（あらかじめ登録された指紋、虹彩その他の個人の身体的特徴の照合を行うことをいう。）によって入室が可能となること。

ロ　入室者の数と同数の者の退室を管理すること。

2.3 オフィス、部屋及び施設のセキュリティ

「リモート署名サーバ」の設備の所在を示す掲示をしてはならない。

2.4 外部及び環境の脅威からの保護

自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用しなければなら

ない。

イ 「リモート署名を行うサーバを設置する室」を建築物の 2 階以上に設置することが望ましい。建築物の 1 階以下に設置する場合には、水害に対して十分な対策を講じる。特に、過去に水害がある場合又は海抜ゼロメートル地帯等である場合には、浸水対策を講ずる。

2.5　セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関して手順を設計し、適用することが望ましい。

イ 「リモート署名サーバを設置する室」から署名者の署名鍵、または署名者の署名鍵の暗号化で使用する共通鍵を作業者が取得できない対策を講じることが望ましい。

附録 7　装置

1　装置の設置及び保護

装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護しなければならない。

2　資産の移動

「リモート署名サーバ」は「リモート署名サーバを設置する室」から事前の許可なしで持ち出してはならない。又、事前の許可なしに「リモート署名サーバを設置する室」に持ち込みを行ってはならない。

3　構外にある装置及び資産のセキュリティ

構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用しなければならない。

4　無人状態にある署名値生成モジュール

署名者の署名鍵、または署名者の署名鍵の暗号化で使用する共通鍵を保管している記憶媒体は、物理破壊することが望ましい。又、「リモート署名サーバを設置する室」内で実施することが望ましい。

5　装置のセキュリティを保った処分又は再利用

リモート署名サーバ管理は、無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない。

イ　退室完了後、認証設備室内はモーションセンサを働かせるなどで、無人の「リモート署名サーバを設置する室」内で動きを検出した場合に警報が発せられる。

ロ　遠隔監視カメラで撮影している映像及び記録された映像は被写体が明確に確認できる。無人の場合にも常夜灯を点灯させて、被写体が明確に確認できるようにする。

附録８　関連ガイドライン

リモート署名の提供には本人確認と利用認証（ログインのための認証）が必要不可欠であるが、本節では、米国国立標準技術研究所が米国政府システムにおける電子認証の基準となるガイドラインとして 2017 年 6 月に策定した「Digital Identity Guidelines」の第 3 版(NIST SP 800-63-3)について、及び eIDAS 規則で規定されている eID の保証レベル(Low、Substantial、High)本ガイドラインとの関連性を述べる。一方で JT2A では「民間電子サービスにおける真正性保証のための解説書」を纏めており、その中で本人確認について、NIST SP 800-63-3 の紹介及び、電子認証に関する詳細な解説があり、本節と合わせて参照すべきである。

NIST SP 800-63-3 は全部で 4 つの文書で構成されており、各文書の概要は以下の通りである。

- Digital Identity Guidelines (NIST SP 800-63-3)
  認証に関するフレームワークの概要とリスクに基づいたレベルの選択方法
- Enrollment and Identity Proofing (NIST SP 800-63-3A)
  利用者の本人確認と登録について 3 段階のレベル(Identity Assurance Level, IAL 1-3)に分け、それぞれの保証レベル毎の要件を規定
- Authentication and Lifecycle Management (NIST SP 800-63-3B)
  認証プロセスの堅牢制とオーセンティケータに関する要件を 3 段階のレベル(Authentication Assurance Level, AAL1-3)に分けて規定
- Federation and Assertions (NIST SP 800-63C)
  認証情報を伝達するためのアサーションの強度について 3 段階のレベル（Federation Assertion Level, FAL1-3）に分けて規定

また、IAL、AAL 及び FAL の各レベルの概説は以下のとおりである。

表 A-4　各 IAL の概説

IAL1	申請者を特定の個人に紐づける必要がない。自己表明型であり、CSP は本人の属性情報を検証しない。
IAL2	証拠をもって申請者が特定の個人であることを証明する。Remote あるいは対面での本人確認が必須。
IAL3	対面での本人確認が必須。より厳格な本人確認資料とその確認が求められる。

表 A-5 各 AAL の概説

AAL1	認証要求者がアカウントに紐づいたオーセンティケータを管理していることをある程度の確信度で保証する。単一要素認証可。
AAL2	認証要求者がアカウントに紐づいたオーセンティケータを管理していることを高い確信度で保証する。多要素認証と承認された暗号技術の使用が必須。
AAL3	認証要求者がアカウントに紐づいたオーセンティケータを管理していることを非常に高い確信度で保証する。ハードウェアベースのオーセンティケータとなりすまし耐性を備えるオーセンティケータが必要（同じデバイスで両方の要件を充足してもよい）。暗号プロトコルに基づいた鍵の所有の証明が必須。承認された暗号技術の使用が必須。

表 A-6 各 FAL の概説

FAL1	IdP から署名されたベアラーアサーション。
FAL2	IdP から署名され、RP の公開鍵で暗号化されたベアラーアサーション。
FAL3	IdP から署名され、RP の公開鍵で暗号化された HOK アサーション。FAL2 に加え、サブスクライバによる暗号技術に基づいたアサーションに紐づく鍵の所有証明が求められる。

eIDAS 規則では実施規則 2015/1502 において eID の保証レベルに対する技術基準及び手続を定めている。この実施規則は ETSI 及び CEN のリモート署名関連規格において利用認証の要件として参照されており、また、正式に通知された加盟国の eID スキームであれば、信頼できる方式として適合性調査の対象外となっている。

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

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。

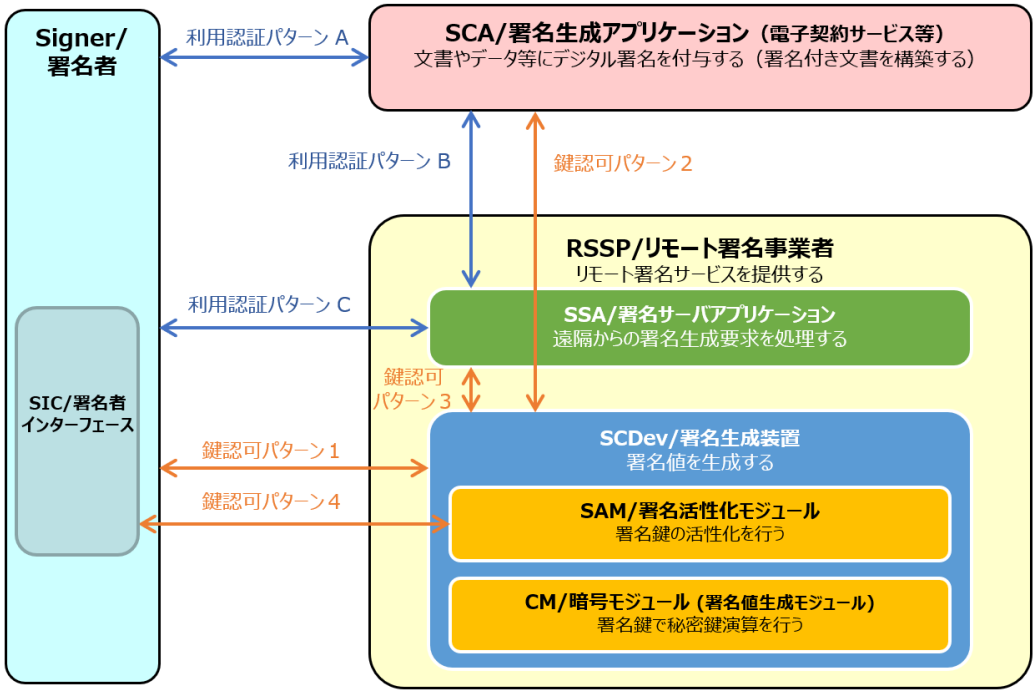


図 1-1　リモート署名サービスの構成例と本ガイドラインのスコープ

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 DTBS/R または SAD の情報を得る。

2.2.1.6　攻撃者は、SAM への転送中に 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 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 SAD 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、暗号モジュールで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、SAD の使用を危うくする攻撃に対して SAD 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、DTBS/R が SAM に送信されたときに完全性が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。

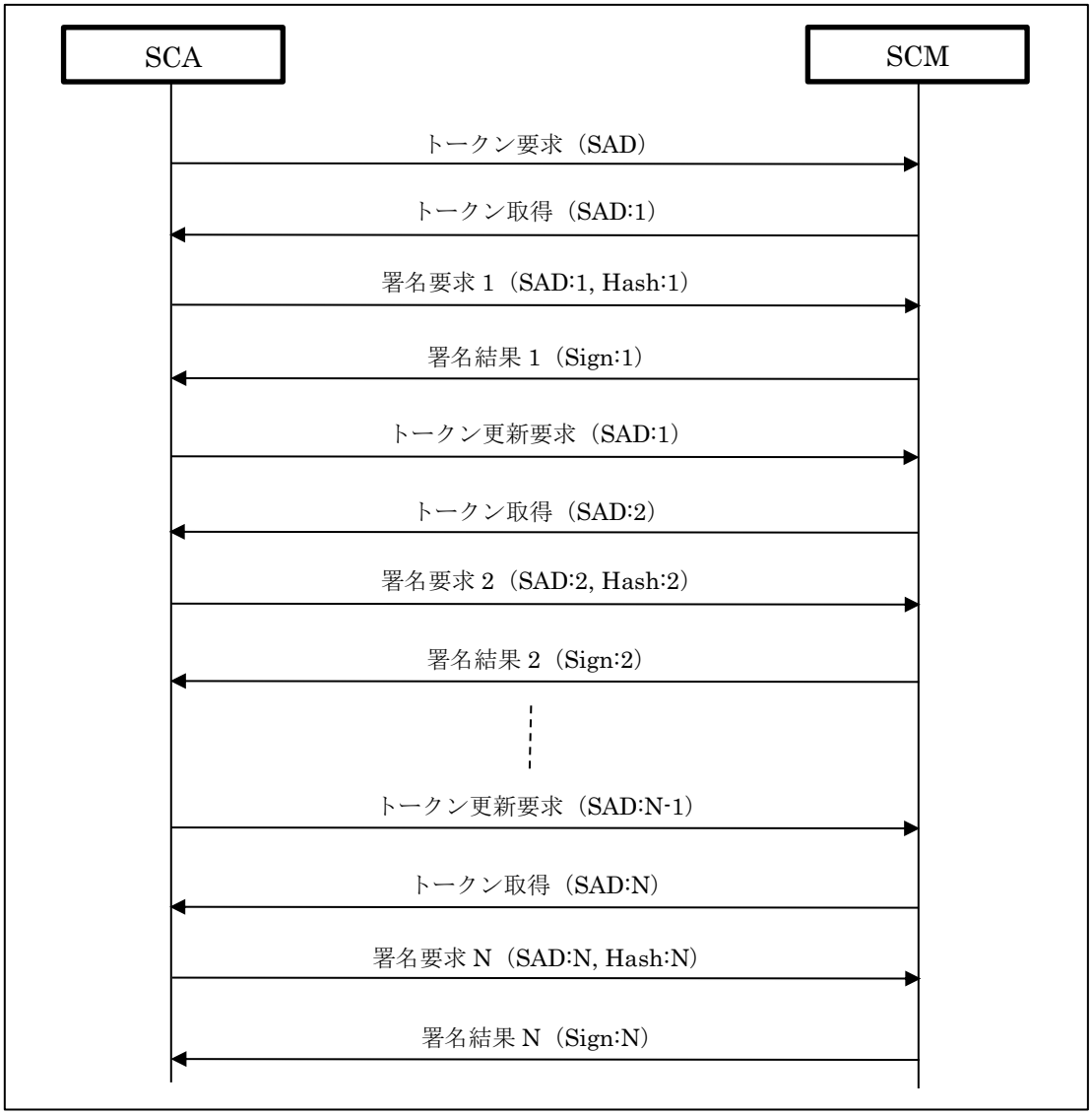


図 B-2 トークンを更新しつつ複数の署名対象を指定する場合のシーケンス図

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（適格）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

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。

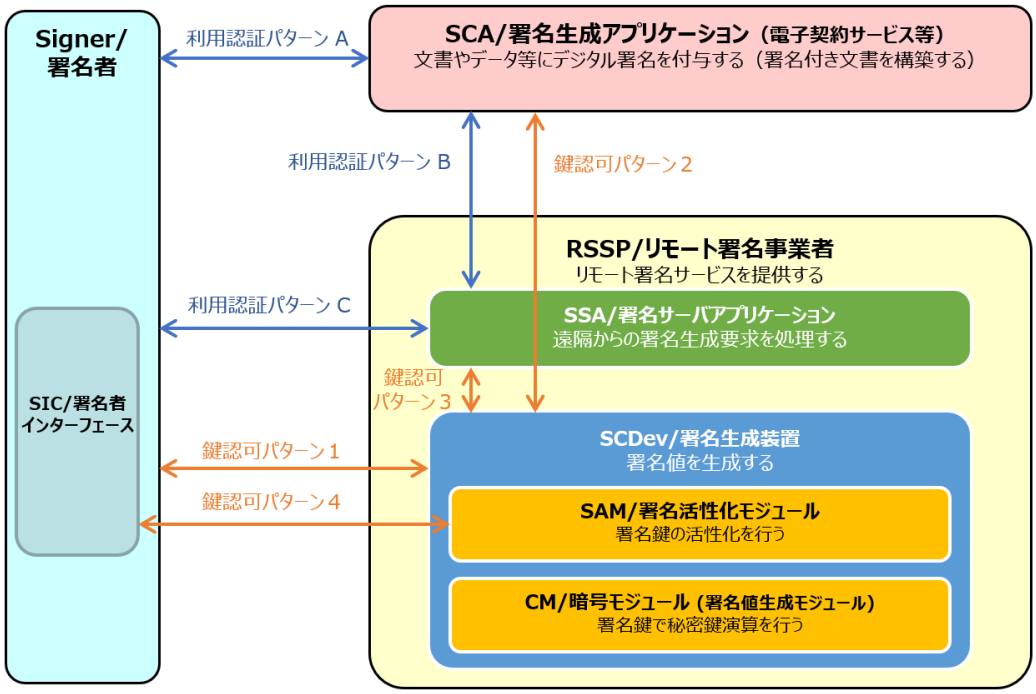


図 1-1　リモート署名サービスの構成例と本ガイドラインのスコープ

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