2026年4月1日

JIPDECトラステッド・サービス登録
（リモート署名サービス：Verifiable Credentials 対応）
登録基準

1. 総則

1.1 本文書の位置づけ

一般財団法人日本情報経済社会推進協会（以下、「JIPDEC」という）が運営する「JIPDECトラステッド・サービス登録」の遂行のため、Verifiable Credentials（以下、「VCs」という）及びVerifiable Presentations（以下、「VPs」という）への電子署名又はeシール（以下、「電子署名等」という）を行うリモート署名サービスを登録する際に用いる基準を定めるものとする。

1.2 用語の定義

本基準における用語の定義を以下のとおりとする。

1.2.1 暗号鍵

秘密鍵を暗号化するために用いられる鍵のこと。

1.2.2 暗号装置

利用者から預託された秘密鍵を安全に管理し、利用者からの指示に基づき、署名値の生成等の処理を行う装置をいう。代表的なものとして、HSM（Hardware Security Module の略称）がある。

1.2.3 クレデンシャル

個人の認証に用いられる情報の総称。利用者がリモート署名サービスを利用する際に必要となるパスワード、生体情報、公開鍵情報等をいう。

1.2.4 検証者（Relying Party）

利用者が提示するVCs又はVPsを検証し、その内容を信頼して各種の判断や処理を行う主体をいう。なお、VCsの技術モデルにおける検証者（Verifier）と同等のものである。

1.2.5 コンプライアンス監査
業務の手順等に基づき、適正に業務が運営されていることを確認するために、定期的に実施する内部監査のこと。

1.2.6 署名活性化データ
利用者がリモート署名サービス又はそれを含む外部のサービスにログインした後、秘密鍵を活性化し、改ざん防止の措置等を行うために必要な符号のこと。

1.2.7 署名値
秘密鍵で暗号化等されたメッセージダイジェスト（電子署名、改ざん防止の措置等の対象となる電子文書のハッシュ値）のこと。

1.2.8 電子署名
W3C 等の国際的な標準仕様、又は電子署名及び認証業務に関する法律第 2 条第 1 項等に準拠した技術を用いたもの。 電子文書等（特定のデータ構造を有するデータセットを含む）に電子署名又は e シール（以下、「電子署名等」という）を行うことで、当該情報の出所（作成者又は作成組織）を証明し、改ざんされていないことを確認できるもの。

1.2.9 公開鍵情報等
電子文書のデータ構造内に直接含まれる公開鍵情報、およびその公開鍵に関連する属性情報や有効性等を示す記述情報（メタデータ等、および電子証明書※1 の記録事項を含む）を総称していう。発行元（Issuer）や認証局等が、これらの情報の正当性を保証する。
※1 X.509 規格に準拠した電子証明書（e シール証明書を含む）もこれに含まれる

1.2.10 電子文書
電磁的方法により作成、保管される文書、及び特定のデータ構造（JSON-LD、SD-JWT、ISO/IEC mdoc※2 等）を有するデータセットのこと。
※2 正式な規格番号は「ISO/IEC 18013-5」

1.2.11 リモート署名サービス
利用者から、電子署名等のために必要な秘密鍵と公開鍵情報等の預託を受け、利用者の指示に基づき、VC/VP 等の発行リクエストまたは提示リクエストに際して、暗号装置に預託された利用者の秘密鍵を用いて電子署名等を提供するサービスをいう。
一般的には、以下の機能を有する。
①利用者の認証・認可を行う機能（利用者からの VC/VP 等の発行・提示リクエストに基づき、秘密鍵の利用を承認する機能を含む）
②利用者に代わって署名値を生成する機能
③署名値を用いて電子署名等を提供（VC/VP 等への署名付与等）する機能

1.2.12 リモート署名サービス事業者
リモート署名サービスを事業として行う者をいう。

1.2.13 利用者
リモート署名サービスを利用する主体をいう。署名権限者（発行元（Issuer）及び保持者（Holder））と、署名代行者（あらかじめ定められた規程や委任に基づき、自動的に電子署名等処理を指示するプログラムやシステム）の両方を指す。

1.2.14 利用申請者

リモート署名サービス事業者に対しリモート署名サービスの利用に係る申請を行う者をいう。

1.2.15 VCs

1.2.10 に定める電子文書のうち、W3C 等の国際的な標準仕様に準拠した、改ざん防止の措置が講じられたクレデンシャル（1.2.3 参照）の一種。発行元（Issuer）が、利用者の属性情報及び公開鍵情報等（1.2.9 参照）に対して電子署名を付与することで、その情報の正当性を検証可能にしたデータセットをいう。なお、本基準の名称における「Verifiable Credentials 対応」は、この VCs 及び次項に定める VPs の双方を扱うサービス形態を指す。また本文書において「VC」と表記する場合は、署名や発行の対象となる個別のデータセット（Verifiable Credential）を指すものとする。

1.2.16 VPs

利用者が、保有する VC の中から必要な情報のみを抽出し、検証者へ送付するために生成するデータセットのこと。送付の際、利用者の秘密鍵を用いて「その情報の持ち主（本人）であることの証明」を付与することで、提示された VC が正当な持ち主によって扱われていることを保証する。なお、本文書において「VP」と表記する場合は、提示や署名の対象となる個別のデータセット（Verifiable Presentation）を指すものとする。

2. 登録のための基準

2.1 運用基準

リモート署名サービスを運用にあたって、以下の基準を満たさなければならない。

2.1.1 利用者の管理に関する手順書

リモート署名サービスの利用者を適正に管理するために、以下の事項を含む手順書を作成しなければならない。

(1)リモート署名サービスの利用に係る申請手続
(2)利用者及び利用申請者の真偽の確認の方法
(3)リモート署名サービスの利用に係る申請について、利用申請者が利用者から委任されていることを確認する方法(利用者自身が利用申請者である場合を除く)
(4)リモート署名サービスへのアクセス制御
(5)利用者へのリモート署名サービスのクレデンシャルの発行及び配付の方法
(6)利用者がリモート署名サービスの利用の終了又は変更をした場合の措置
(7)利用者の秘密鍵及び公開鍵情報等の管理
(8)その他利用者の管理について必要な事項

2.1.2 関係要員

リモート署名サービスの運用に係る要員及びそれらの運用体制については、以下の措置を講じなければならない。

(1)関係要員の教育については、任命時の教育や、定期的なリモート署名サービス業務の教育を実施する。その教育記録を作成し、保存すること。
(2)運用体制については、内部牽制を考慮して、責任、権限、指揮命令系統を定めること。
(3)関係要員については、業務に係る技術に関し十分な知識及び経験を有する者を配置すること。

2.1.3 運用管理

リモート署名サービスの運用管理については、以下の措置を講じなければならない。

(1)リモート署名サービスの運用規程の作成及び公開
(2)リモート署名サービスの利用規約/利用約款の作成及び公開
(3)コンプライアンス監査
(4)リモート署名サービス事業者の信頼性評価
(5)個人情報の管理
(6)運用セキュリティ
(7)リスクアセスメント
(8)インシデント管理
(9)事業継続マネジメント
(10)リモート署名サービス事業者の終了の際の措置
(11)文書管理／エビデンス管理
(12)内部不正対策
(13)バックアップ・リカバリ

（14）関係要員の役割に応じた認証・認可
（15）本番環境とテスト環境等の分離
（16）利用者の秘密鍵及び公開鍵情報等管理

2.2 技術基準

リモート署名サービスに係る技術については、以下の基準を満たさなければならない。

2.2.1 利用者の認証・認可を行う機能

利用者からの指示を受けて、利用者の当人認証及び署名値生成に係る認可（以下、「認証・認可」という）を行うために、以下の措置を講じなければならない。

（1） 利用者に対して、事前に認証・認可のためのクレデンシャルを発行し、本人に安全に配付すること。また、e シールを用いて組織が自動的に電子署名等を付与する場合（VC の自動発行等）は、指示を行うシステムに対する適切な認証・認可措置を講じること。署名値生成に係る認可のための署名活性化データを生成する操作を利用者に行わせることが望ましい。
（2）当該クレデンシャルの発行及び配付については、利用目的に対応した適切な手段を採用しなければならない。特に、利用者のなりすまし等の脅威への対策として十分な手段であることを担保する。
（3）認証に係る外部のサービスに依存する場合は、当該外部のサービスがクレデンシャルの発行・配付を含めた必要な措置の実施を確実なものにしなければならない。
（4）認証に係るセッションが悪意のある第三者に乗っ取られることを防止する。さらに、有効なセッションの時間を定義し、定義された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講じなければならない。

2.2.2 利用者に代わって署名値を生成する機能

利用者からの指示に基づき署名値を生成するため、以下の要件を含む規程を作成し、必要な措置を講じなければならない。

（1）暗号装置

JIS X 19790 又は相当する規格（例えば CEN EN 419 221-5 あるいは FIPS 140-2 以上）に基づき製造され、第三者による認証を取得していること。

（2）秘密鍵の生成と保管

ア　秘密鍵を発行元（Issuer）等で生成する場合

①発行元等との連携の方法（認証局を運営する事業者との契約締結を含む）
②秘密鍵等及び公開鍵情報等のリモート署名サービス事業者への配送におけるデータの改ざんや盗聴が起こらない安全な通信経路の利用
③秘密鍵を暗号装置で保管する場合における暗号鍵による暗号化又は安全性が担保される形式での保管
④秘密鍵を暗号装置以外で保管する場合における当該装置でのみ復号できる形式による暗号化又は署名値を生成する機能を構成する設備においてのみ使用でき安全性が担保される形式での保管
⑤秘密鍵と公開鍵情報等の対応の確認

イ　秘密鍵をリモート署名サービス内で生成する場合

①独立した（外部からアクセスできない）環境での秘密鍵の生成

②発行元等との連携の方法（認証局を運営する事業者との契約締結を含む）

③リモート署名サービス事業者への配送においてデータの改ざんや盗聴が起こらない安全な通信経路の利用

④秘密鍵を暗号装置で保管する場合における暗号鍵による暗号化又は安全性が担保される形式での保管

⑤秘密鍵を暗号装置以外で保管する場合における当該装置でのみ復号できる形式による暗号化又は署名値を生成する機能を構成する設備においてのみ使用でき、安全性が担保される形式での保管

なお、連携する認証局がある場合は第三者評価機関による評価を受けた認証局、又は国が認めている認証局であること。

（3）秘密鍵の廃棄

以下の場合、秘密鍵を廃棄すること。

ア　秘密鍵を更新した場合（公開鍵情報等の記載事項の変更、有効期限切れ等）

イ　秘密鍵に対応する公開鍵情報等がステータスリスト等において無効化・失効されたことを確認した場合

ウ　利用者がリモート署名サービスの利用を終了する旨、利用者から通知があった場合

（4）秘密鍵のバックアップ・リカバリ

秘密鍵のバックアップ・リカバリを行う場合には以下の措置を講じること。なお利用者の秘密鍵をバックアップ・リカバリする場合には、その条件を通知すること。

ア　バックアップについては、その機密性及び完全性を確保するために十分に保護された形で保管するとともに、完全性の検証を可能にするメカニズムの変更からバックアップを保護する。

イ　リカバリについては、利用者の要求に応じて適切に行う。

2.2.3　署名値を用いて電子署名等を提供する機能

電子署名等を提供するために、以下の措置を講じなければならない。

（1）署名値の生成

ア　利用者の指示に基づいて署名値を生成する。

イ　署名値を生成する時点において、公開鍵情報等及びそれに対応する秘密鍵が、ステータスリスト等により有効であることを確認する。

（2）電子署名等の指示

ア　署名活性化データを利用する場合

①電子署名等の指示として、利用者に署名活性化データを生成する操作を求める。なお、電子署名等の指示には、利用者が直接電子署名等を行う場合のほか、利用者が発行元に対して VC の発行要求や、検証者から利用者へ VP の提示要求があり、利用者が同意することを受けて、システムが自動的に電子署名等を行う場合を含む。

②利用者とリモート署名サービスの通信経路において、署名活性化データが改ざんや盗聴がされないように暗号化する。

③署名対象情報、指示を行った利用者の認証情報及び秘密鍵の利用確認（承認）を記録する。

イ　署名活性化データを利用しない場合

①電子署名等の指示として、リモート署名サービスが秘密鍵を活性化し使用することの「確認（承認）」を求める。

②署名対象情報、指示を行った利用者の認証情報及び秘密鍵の利用確認（承認）を記録する。

（3）電子署名等の事後的措置

ア　電子署名等が行われた情報（VC/VP 等）を利用者に返却、または指定の配付先へ送出する方法を定める。

イ　電子署名等が行われた情報（VC/VP 等）の返却後、または送出後における当該情報の取り扱いを定める。

ウ　電子署名等が行われた事実について、事後に確認できる手段を定める。

2.2.4 ネットワークセキュリティ対策

ネットワークセキュリティ対策として、以下の措置を講じなければならない。

（1）「2.2.1」、「2.2.2」又は「2.2.3」の機能を構成する各機器の間及びそれらの機器と利用者の間の通信を保護しなければならない。特に、利用者と電子署名等の対象情報のメッセージダイジェストの関係性を保護すること。

（2）通信がリモート署名サービス事業者の敷設した通信回線以外を経由する場合は、「2.2.1」、「2.2.2」又は「2.2.3」の機能を構成する各機器の相互認証を行うこと。

（3）「2.2.1」、「2.2.2」及び「2.2.3」の機能を構成する各機器の間の通信は、暗号化すること。

（4）本番環境とテスト環境等を分離すること。

2.3 設備基準

リモート署名サービスを適正に運用するために必要な設備は、以下の基準を満たさなければならない。

2.3.1 建物

2.3.1.1 建物（オンプレミス環境）

「2.2.1」、「2.2.2」、「2.2.3」の機能を提供する設備（以下、「基幹設備」という）への物理的及び環境的なセキュリティ対策において、その資産への物理的リスクを最小化するための措置を講じなければならない。

（1）基幹設備を設置した室の所在が公開されていないこと。

（2）基幹設備を有する建物の耐震措置を行うこと。

（3）基幹設備が設置されたラックを建物構造体に固定すること。

（4）基幹設備を設置した室の防火対策及び防水対策を行うこと。

（5）基幹設備のために UPS を設置すること。

2.3.1.2 建物（クラウド環境）

基幹設備がクラウド環境に設置されている場合は、委託先であるクラウドサービスプロバイダーが当該クラウド環境を適用範囲に含む ISMS 認証、ISMS クラウドセキュリティ認証等（以下、「ISMS 等の認証」という）を取得していること、及び適用範囲が「2.3.1.1」を含むことを確かなも

のにするとともに、以下の措置を講じなければならない。
（1）「2.3.1.1」の各項目に対応したクラウドサービスプロバイダーによる対策をセキュリティポリシーに記載すること。
（2）基幹設備に係るリスクを適切に評価し、対策を講じること。

2.3.2 設備への物理的アクセス制御

2.3.2.1 設備へのアクセス制御（オンプレミス環境）

基幹設備への物理的アクセスを制御するとともに、その資産への物理的リスクを最小化するため、以下の措置を講じなければならない。
（1）基幹設備については、関係要員以外の者が近づいて操作したり、操作画面をのぞき見したりすることができないようにすること。
（2）基幹設備については、環境上の脅威及び災害からのリスクを低減するように設置すること。
（3）基幹設備を、当該設備を設置する室から事前の許可なしで持ち出したり、持ち込んだりしないようにすること。
（4）基幹設備を設置した室の外にある資産については、当該室外での作業等に伴うリスクを考慮して、適切なセキュリティ対策を行うこと。
（5）秘密鍵、暗号鍵又は利用者情報を保管している設備、暗号装置を廃棄する場合は、それらが復元できない方法で廃棄すること。
（6）基幹設備を設置した室は入退室管理装置の制限により、権限者 2 名以上でないと入退室できないこと。
（7）基幹設備を設置した室はモーションセンサを設置していること。
（8）基幹設備を設置した室の扉解放時間が必要最小限に制限していること。
（9）基幹設備を設置した室には監視カメラを設置していること。
（10）基幹設備を設置した室の監視カメラの映像を一週間以上記録していること。

2.3.2.2 設備へのアクセス制御（クラウド環境）

基幹設備がクラウド環境に設置されている場合は、委託先であるクラウドサービスプロバイダーが当該クラウド環境を適用範囲に含む ISMS 等の認証を取得していること、及び適用範囲が「2.3.2.1」を含むことを確かなものにするとともに、以下の措置を講じなければならない。
（1）基幹設備に対して、アクセス制御、暗号化、バックアップ等、セキュリティコントロールを実施し、情報セキュリティ管理策が機能していること。
（2）基幹設備に係るリスクを適切に評価し、対策を講じること。

2.3.3 運用・保守端末

運用・保守端末の物理的アクセスを制御するとともに、その資産への物理的リスクを最小化するため、以下の措置を講じなければならない。
（1）運用・保守端末は特定されていること。
（2）運用・保守端末の操作者は特定され、特定された操作者以外の者は利用できないこと。
（3）関係要員以外が運用・保守端末を操作したり、その画面をのぞき見したりすることができないようにすること。
（4）環境上の脅威及び災害からのリスクを特定し、リモート署名サービスとして許容できるリスクま

で低減すること。

（5）運用・保守端末の操作については、操作者個人を特定し、その操作内容について記録及び追跡できること。特に不正や錯誤については、後日の調査を可能とすること。

以上