2024年2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）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）が運営するトラストサービス評価事業「JIPDECトラステッド・サービス登録」の遂行のため、トラストサービスのうち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 トラストサービス

インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組みをいう。

1.2.2 電子署名

電子署名及び認証業務に関する法律第2条第1項に定められた措置等のうち、ITU-Tが定めた公開鍵基盤（PKI）に関する国際規格であるX.509に準拠したデジタル署名技術を用いたもの。電子文書等に電子署名を行うことで、当該文書が「誰によって」作成されたものであるか証明するとともに、改ざんされていないことを確認することができる。

1.2.3 eシール

電子文書等の発行元の組織を示すとともに、当該電子文書等が改ざんされていないことを確認するためのものであり、総務省が公表した「eシールに係る指針」において定義されたものとする。

1.2.4 電子証明書

ITU-Tが定めた公開鍵基盤（PKI）に関する国際規格であるX.509に準拠した公開鍵証明書をいう。電子証明書を発行する認証局が、その記録事項（発行者名、利用者名、当該電子証明書の有効期間等）の正当性を保証する。

1.2.5 リモート署名サービス

利用者から、電子署名又はeシール（以下、「電子署名等」という）のために必要な秘密鍵と電子証明

書の預託を受け、利用者からの指示に基づき、利用者の指定する電子文書等に対して、当該秘密鍵を用いて電子署名等をインターネット上で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
②利用者に代わって署名値を生成する機能
③上記②の署名値を用いて電子署名等を提供する機能

1.2.6 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。

1.2.7 利用者
リモート署名サービスを利用する者をいう。署名権限者(電子証明書で指定された公開鍵に対応する秘密鍵の所有者(電子証明書の名義人:subject))と署名代行者(署名権限者から委任を受け、署名権限者に代わって署名を行う者)の両方を指す。

1.2.8 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。

1.2.9 暗号鍵
秘密鍵を暗号化するために用いられる鍵のことをいう。

1.2.10 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専用装置をいう。HSM(Hardware Security Module の略称)と呼ばれることもある。

1.2.11 クレデンシャル
個人の認証に用いられる情報の総称。リモート署名サービスの利用者が、当該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、電子証明書等をいう。

1.2.12 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、電子署名等を行うために必要な符号をいう。

1.2.13 署名値
秘密鍵で暗号化されたメッセージダイジェスト(電子署名等の対象となる電子文書等のハッシュ値)をいう。

2. 登録のための要件

2.1 運用基準
リモート署名サービスを運用するために必要な措置は、以下の要件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)利用者情報としての秘密鍵の管理
(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充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
(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
(12)内部不正対策
(13)バックアップ・リカバリ
(14)関係要員の認証・認可

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、以下の要件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、本人に安全に配付しなければならない。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こと。

（3）認証・認可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を実施することを確実なものにしなければならない。

（4）認証・認可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ために、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受けていなければならない。

（2）秘密鍵の生成と保管

ア　秘密鍵を認証局で生成する場合

①認証局との連携の方法（認証局を運営する事業者との契約締結を含む）

②秘密鍵及び電子証明書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秘密鍵と電子証明書の対応の確認

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認証局との連携の方法（認証局を運営する事業者との契約締結を含む）

③電子証明書の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

（3）秘密鍵の廃棄

以下の場合、秘密鍵を廃棄しなければならない。

ア　秘密鍵を更新した（電子証明書の記載内容に係る利用者情報の変更、電子証明書の有効期限切れ等）。

イ　秘密鍵に対応する電子証明書が失効された。

ウ　利用者がリモート署名サービスの利用を中止した。

（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、利用者に対してバックアップ・リカバリの条件を通知した上で、以下の措置を講じること。

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、電子署名等の提供に用いられる秘密鍵が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。

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を利用者に返却する方法を定める。

イ　電子署名等が行われた情報の返却後の電子署名等の対象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しなければならない。

（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わなければならない。

（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、暗号化されなければ

ならない。

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、以下の要件を満たさなければならない。

2.3.1 建物

重要なサービス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) リモート署名サービスに係る設備を設置した室の所在が公開されていないこと。
(2)リモート署名サービスに係る設備を有する建物の耐震措置を行うこと。
(3)リモート署名サービスに係る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)リモート署名サービスに係る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)リモート署名サービスに係る設備のために UPS を設置すること。

2.3.2 設備への物理的アクセス制御

重要なサービス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)リモート署名サービスに係る設備については、関係要員以外の者が近づいて操作したり、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。
(2) リモート署名サービスに係る設備については、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)リモート署名サービスに係る設備を、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)リモート署名サービスに係る設備を設置する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、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。

以上