2025年3月31日

JIPDECトラステッド・サービス登録（認証局）
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、認証局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 暗号装置
認証局の秘密鍵を安全に生成し保管する装置をいう。HSM（Hardware Security Module の略称）と呼ばれることもある。

1.2.2 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。

1.2.3 組織
法人、個人事業主、権利能力なき社団・財団、その他任意の団体等をいう。

1.2.4 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、他者による改ざんを検知することができる。

1.2.5 電子署名等検証者
利用者から電子署名、e シールが行われた情報を受け取り、当該利用者が当該電子署名、e シールを行った者を確認する者のことをいう。

1.2.6 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。このうち総務省大臣告示（総務省告示第百十三号）で示された e シール

のために発行される電子証明書のことを「e シール用電子証明書」という。

1.2.7 認証局

電子証明書の発行・更新・失効、認証局の秘密鍵の生成・保護及び利用者の登録を行う機関（CA：Certificate Authority）をいう。一般に、利用者の審査・登録を行う登録局（RA：Registration Authority）、電子証明書の発行・管理を行う発行局（IA：Issuing Authority）、電子証明書の失効情報等を公開するリポジトリ等により構成される。

1.2.8 利用者

電子証明書で指定された公開鍵と関連する秘密鍵の所有者であり、当該認証局から発行された電子証明書に係る電子署名等を行う者をいう。利用者には、自然人、組織に結びついて識別される自然人、組織、組織の中で特定の役割を果たすエンティティ（組織内部の役職や部署を含む）等がある。

1.2.9 利用者申請者

認証局に対し電子証明書の発行又は失効に係る申請を行う者をいう。

1.2.10 CA 室

CA 設備等を設置した室をいう。

1.2.11 CA 設備

認証局の設備のうち電子証明書の作成又は管理に用いる電子計算機その他の設備をいう。

1.2.12 CP/CPS

証明書ポリシー（CP：Certificate Policy）及び認証局運用規程（CPS：Certification Practice Statement）をいう。本基準においては、IETF の RFC3647（インターネット X.509 PKI： 証明書ポリシーと認証実施フレームワーク）に準じて作成されることを前提とする。

1.2.13 CP/CPS

電子証明書の有効期間中に、電子証明書の記録事項の変更、秘密鍵の紛失・盗難等の事由により、発行した電子証明書を失効した際に、認証局が公表する証明書失効リスト（CRL：Certificate Revocation List）のことをいう。

1.2.14 CRL

電子証明書の有効期間中に、電子証明書の記録事項の変更、秘密鍵の紛失・盗難等の事由により、発行した電子証明書を失効した際に、認証局が公表する証明書失効リスト（CRL：Certificate Revocation List）のことをいう。

1.2.15 e シール

総務省大臣告示（総務省告示第百十三号）には、以下のとおり定義されている。

「eシール」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録された情報（以下「電子データ」という。）に付与された又は論理的に関連付けられた電子データであって、次の要件のいずれにも該当するものをいう。

一当該情報の出所又は起源を示すためのものであること。

二当該情報について改変が行われていないかどうか確認することができるものであること。

”1.2.16 OCSP

OCSP（Online Certificate Status Protocol）は、電子証明書の失効状態を取得する通信プ

ロトコルのことをいう。

1.2.17 RA 端末

専ら電子証明書の利用者を登録するために用いられる端末をいう。

2. 登録のための基準

2.1 運用基準

認証局を運用するために必要な措置は、以下の基準を満たさなければならない。

2.1.1 利用者の真偽の確認

認証局は、利用申請者からの電子証明書の発行に係る申請手続について、予め決められた方法(対面、郵送、オンライン等)で行われることを確かにするとともに、電子証明書に記録される利用者の名称及び関連情報の真偽の確認の方法について、以下の要件を満たさなければならない。

(1) 利用者が自然人、組織に結びついて識別される自然人、組織の中で特定の役割を果たすエンティティ(組織内部の役職や部署を含む)等である場合

ア 電子証明書の発行に係る申請手続について、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こと(利用者自身が利用申請者である場合を除く)。

イ 利用者の実在性及び申請に係る利用者の意思の確認において、直接的な証拠又は適切に確認された情報源からの証明を用いて、利用者及びその属性を識別し特定すること。

ウ 利用者の実在性の確認の結果と電子証明書の紐付けを正確に行うとともに、利用者の氏名等を確認できる直接的な証拠又は適切に確認された情報源からの証明について、適切に管理すること。

エ 利用者が属する組織に関する情報(法人、部署の名称等)を電子証明書に記録する場合は、利用者が当該組織に所属することを、直接的な証拠又は適切に確認された情報源からの証明を用いて確認すること。

(2)利用者が組織である場合(e シール用電子証明書)

ア 電子証明書の発行に係る申請手続について、利用申請者が組織の代表者から委任されていることを確認すること(利用者自身が組織の代表者であり利用申請者である場合を除く)。

イ 組織の実在性及び申請に係る組織の代表者の意思の確認において、直接的な証拠又は適切に確認された情報源からの証明を用いて、組織の実在性を確認し、組織及びその属性を識別し特定すること。

ウ 組織の実在性の確認の結果と電子証明書の紐付けを正確に行うとともに、組織の名称を確認できる直接的な証拠又は適切に確認された情報源からの証明について、適切に管理すること。

エ 電子証明書には組織を特定するための識別子を必ず記録するとともに、当該識別子の種類を明らかにすること。(例:法人番号、会社法人等番号、TDB 企業コード、TSR 企業コード、D-U-N-S® Number、LEI、標準企業コード、OSI オブジェクト識別子等)

2.1.2 関係要員

認証局は、関係要員及びそれらの運用体制について、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、定期的に認証局業務に関する教育を実施する。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て、十分な知識及び経験を有する者を配置すること。

2.1.3 アクセス制御

認証局は、利用者のデータ入力用の端末及び電子証明書発行システム等に関する装置並びに利用者の秘密鍵の生成から配付まで関連する装置へのアクセスは、権限を有する特定の個人に制限されることを確実にするため、以下の措置を講じなければならない。
(1) 利用者のデータ入力用の端末及び電子証明書発行システム等に関する業務の手順書を作成し、アカウント及びその権限、パスワードの強度、認証トークン等を適切に管理すること。
(2) 利用者の秘密鍵を利用者以外が生成する場合は、当該利用者の秘密鍵を第三者に知られることなく、確実に利用者に渡す方法(利用者のみが使用できる環境への格納を含む。)を採用すること。

2.1.4 運用管理

認証局は、信頼性のある運用体制を構築するために、以下の措置を講じなければならない。
(1) 運用規程
ア CP/CPS の適合性について自ら確認し、規定された内容に則し適切に実施すること。
イ 2.1.1 における真偽の確認の方法、電子証明書の発行作業等について、CP/CPS に則した業務の手順書を作成すること。
ウ 電子証明書に関するすべての関連情報について、特に訴訟目的用の認証のエビデンスを提供するために、CP/CPS に規定した上で、適切な期間、記録を確実に保存されること。
エ CP/CPS の重要事項を変更する場合には、事前に JIPDEC に通知すること。
オ CP/CPS は RFC3647 に準じて作成すること。
(2) コンプライアンス監査
ア 業務の手順等のとおりに実施されていることについて、定期的に内部監査を実施すること。
イ 情報等の管理について定期的に監査等を実施し、その結果を記録すること。
(3) 認証局を運営する組織の信頼性
ア CP/CPS に沿って運用するために、必要な安定した財源やリソースが確保されている、債権超過でないこと等。
イ 保険の加入や十分な財政的基盤等により、その運営や活動から生じる債務を賄う適正な用意があること。
(4) 個人情報の管理
ア 個人情報の保護に関する規程を作成し、個人情報を適切に管理すること。
イ 外部委託が行われる場合、契約により外部委託組織は利用者の情報等を適切に管理すること。
(5) 運用セキュリティ
ア 認証局の運用にあたり、関係要員以外による施設・設備へのアクセス物理的、論理的に制御

し、セキュリティの確保・維持すること。

イ　システム開発及び保守について文書化し、テストを実施したうえで、これを承認し、適切に実行すること。

ウ　システムを、ウイルスや悪意のあるソフトウェアから保護するため、検出と被害防止の対策を認証局、又は委託された第三者のコントロールで実施すること。

エ　脆弱性対策のプロセス（脆弱性を特定する、レビューを実施し対応する、脆弱性を解消する）について文書化し、それに従って実施すること。

オ　以下のタイミングで脆弱性調査を実施すること。

（ア）JIPDEC の要請があってから一週間以内

（イ）認証局が重要であると判断したシステム又はネットワーク変更を実施した後

（ウ）認証局、又は委託された第三者の証明書システムであるプライベート及びパブリック IP アドレスに対して、少なくとも四半期に一度

カ　認証局及び委託されたサードパーティ製の PKI アプリケーションは、少なくとも年に一回、及びアプリケーションのアップグレードや認証局が重要であると判断した改修の後に、侵入テスト（Penetration Test）を受けていること。

キ　他社に委託して実施する脆弱性調査と侵入テストは、十分なスキル、ツール、実力、倫理基準、独立性を備えた個人又は組織によって実行し、その証跡を記録すること。

ク　脆弱性が発見された場合、以下のいずれかの対策を実施すること

（ア）速やかに脆弱性を解消する。

（イ）96 時間以内に脆弱性を解消することができない場合には、脆弱性の影響を最小化する計画を作成し、実行する。

（ウ）認証局が脆弱性の改修が必要ないと決定した場合には、その根拠を文書化する。

（6）リスクアセスメント

ア　認証局の運用にあたり、経営陣や情報セキュリティ委員会等により、セキュリティマネジメントを計画・管理し、組織内でサポートすること

イ　認証局の運用にあたり、経営陣や情報セキュリティ委員会等により、セキュリティリスクを洗い出し、リスク分析、評価等を管理すること。

（7）インシデント管理

ア　リスクマネジメントとして、システム障害、セキュリティインシデント、誤操作に対するリスクを最小化すること。

イ　インシデント対応として、迅速に事故等に対応し、セキュリティ侵害の影響を抑えるために、適時、調整された方法で行動すること。なお、認証局業務の信頼性を損なう、又はその恐れがあるインシデントが発生した場合は、発生後速やかに JIPDEC に報告すること。必要に応じて利用者等に通知すること。

ウ　インシデントに関して、JIPDEC が必要と判断した場合、JIPDEC による調査（現地調査を含む）を早急に受け入れること。

（8）事業継続マネジメント

BCP（事業継続計画）として、災害時に、どこまで認証局として業務を継続するかの目標を定め、目

標を達成するための計画を作成し、また、その訓練を行うこと。

(9)認証局の終了の際の措置

ア　利用者と電子署名等検証者への混乱を最小化することを保証し、訴訟の目的のために電子証明書のエビデンスを提供するために必要な記録の保持を保証すること。

イ　業務の終了をすべての利用者と電子署名等検証者に知らせること。

ウ　認証局の秘密鍵を破棄するか、使用できなくすること。

(10) 文書管理／エビデンス管理

ア　文書及びエビデンスの管理は、漏洩、滅失、棄損の防止対策を行うこと。

イ　文書の改訂履歴を作成しており、改訂内容が管理され、確認できること。

2.1.5 電子証明書のライフサイクル管理

認証局は、電子証明書の真正性を維持するため、電子証明書の安全な発行を確実に実施しなければならない。

(1) 電子証明書の利用に係る説明事項

ア　利用者に対して、利用者の秘密鍵の管理が重要であることを周知すること。特に電子署名は、自署や押印に相当する法的効果が認められ得るものであり、十分な注意をもって利用者の秘密鍵及びその活性化に使用する PIN 等の管理を行い、秘匿性を維持することを説明すること。

イ　利用者の秘密鍵は生成・活性化・保管・廃棄等について管理され、利用者がその管理方法を知ることができること。また CP/CPS に規定していること。

ウ　利用者及び利用申請者の義務について、以下の同意を求めること。

（ア）CP/CPS に従って、特に登録について正確で、完全な情報を認証局に提出する。

（イ）利用者の秘密鍵が第三者に使用されないように十分な注意を払う。

（ウ）利用者の秘密鍵が、紛失、盗難、危殆化した場合、又は電子証明書の記録事項の誤り及び変更が生じた場合には速やかに認証局に通知する。

エ　e シール用電子証明書を発行する場合は、利用者又は利用申請者に対して e シールの定義、e シールと電子署名の異同等について説明すること。

(2)電子証明書の発行

ア　利用者に発行する電子証明書は、CP/CPS で規定されている事項を満たすこと。

イ　認証局が利用者の秘密鍵を生成する場合、利用者の秘密鍵の生成から配付まで、当該利用者の秘密鍵を第三者に知られることなく、安全かつ確実に利用者に渡す(利用者のみが使用できる環境への格納を含む)ことができる方法により実施すること。また、利用者に秘密鍵を交付後不要となった利用者の秘密鍵及びその複製は、直ちに削除すること。

ウ　利用者が秘密鍵を生成する場合、認証局は当該利用者が当該秘密鍵を保持していることを確認すること。

(3)電子証明書の更新

ア　電子証明書の更新をサポートしている場合、電子証明書の更新申請が正確で、承認されており、完全であるという合理的な保証を提供する内部統制を保持すること。

(4)電子証明書の再発行(Rekey)

ア　電子証明書の再発行の場合、電子証明書の再発行申請（失効要求や有効期限を含む）は、正確で、承認されており、完全であるという合理的な保証を提供する内部統制を保持すること。

（5）電子証明書の失効

ア　失効請求者の真偽の確認方法、失効に関する情報の記録の手続等を定めた上で、電子証明書の有効期間内において、利用者から電子証明書の失効の請求があったとき、又は電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該電子証明書を失効すること。また、失効に関する情報は、受付日や対応日、その他の失効に関する情報を記録、管理し、CRL 又は OCSP 等で公開すること。

イ　利用者等による電子証明書の失効事由、及び認証局自身に起因する電子証明書の失効事由を、それぞれ CP/CPS 等に定めること。

ウ　電子証明書の有効期間内において、電子署名等検証者からの求めに応じ、自動的に送信する方法その他の方法により、電子署名等検証者が失効に関する情報を容易に確認することができるようにすること。

エ　電子証明書の失効通知の方法や手順を定めた上で、電子証明書を失効した場合には、遅滞なく利用者に通知すること。

2.2 技術基準

認証局を適正に運用するために必要な技術は、以下の要件を満たさなければならない。

2.2.1 ネットワーク管理

認証局は、ネットワーク及びシステムを保護するため、以下の措置を行わなければならない。

（1）電子証明書の発行、失効を行う操作において、RA 端末からの発行、失効申請の通信時に盗聴、改変、設備の誤認防止策を実施すること。

（2）CA 設備（RA 端末を除く。）が外部のネットワークと接続している場合、その CA 設備は、不正アクセス行為を防御するためのファイアウォール（以下、「FW」という。）機能及びネットワークベースの侵入検知機能を備えた通信機器を有し、それらを介して通信を行うこと。

（3）CA 設備が接続するネットワークドメインを FW で保護すること。FW はそのログを 1 年以上保存する（不正なアクセス等があったときのもの）こと。

（4）CA 設備間の通信が外部ネットワークを経由する場合には TLS1.2 以上等のセキュアな通信プロトコルにより盗聴、改変、設備の誤認防止策を実施すること。

（5）CA 設備が接続しているネットワークドメインを侵入検知システム（以下、「IDS」という。）/侵入防御システム（以下、「IPS」という。）で保護すること。当該 IDS/IPS はそのログ（不正なアクセス等があったときのもの）を取得すること。

（6）利用者の秘密鍵をダウンロードする設備間の通信が外部ネットワークを経由する場合には盗聴、改変、設備の誤認防止策を実施すること。

（7）ダウンロード方式で利用者の秘密鍵を配付する場合は、通信経路の途中で利用者の秘密鍵が不正に取得されない措置を講じること。

（8）文書／エビデンスをネットワーク上の共有フォルダに保管する場合には、アクセス権限を設定し、関係要員以外の閲覧が不可になること。

2.2.2 認証・権限確認

認証局は、システムへのアクセスをアクセスコントロールポリシーに従って制限するとともに、その業務において十分なセキュリティ管理を行うため、以下の措置を行わなければならない。

(1) 業務に使用する端末のオペレーティングシステム(OS)のアカウントやアクセス権限は操作者ごとに設定すること。
(2) 業務で使用するシステムのアカウントは、操作者の認証が行える機能を備えること。
(3) 業務で使用するシステムのアクセスログ・操作ログは 1 年以上保存すること。
(4) 原則、リモートデスクトップ、telnet 等ネットワーク機能による遠隔操作を不可に設定すること。遠隔操作をする場合には、適切なセキュリティ対策を講じていること。
(5) 利用者の秘密鍵の活性化に使用する PIN 等の生成、転送、出力等を行う場合は、アクセス権限管理、内部牽制等により、盗聴、改変防止等の措置を講じること。
(6) PIN の生成に関しては、適切な関数やアルゴリズムを用いた乱数を使用すること。
(7) 認証局の鍵管理に係る関連システムへの認証方法は、ISO/IEC15408 で規定する情報技術セキュリティの評価基準(CC:Common Criteria)EAL4 以上かこれらと同等と認められる IC カード、又はトークン等によるオペレータ認証(二要素認証)を行うこと。
(8) 認証局に係る記録・データが含まれたファイルのアクセス権を設定し、関係要員以外の閲覧を不可にすること。

2.2.3 認証局の秘密鍵の管理

認証局の秘密鍵の機密性の保持及び完全性の維持を確保し、その秘密鍵が不適切に使用されることがないように、以下の措置を行わなければならない。

(1) 暗号装置は、移動(配送)、保存されている間に改ざんされないこと。
(2) 暗号装置内の認証局の秘密鍵の生成・活性化・複製・回復は、同時に少なくとも 2 名の権限が割り当てられた要員により管理すること。
(3) 暗号装置は正しく機能していること。特に初期導入時には事前に自己診断テストを実施し、暗号装置が正しく動作することを確認すること。
(4) 認証局の鍵管理について、JIS X 19790 若しくはこれと同等な規格におけるセキュリティレベル 3 相当(FIPS140-2 レベル3相当)の暗号装置又は ISO/IEC15408 の EAL4+若しくはこれらと同等と認める暗号装置、IC カード若しくはトークン等によるオペレータ認証(二要素認証)によって厳格に行うこと。
(5) 認証局の秘密鍵の漏えいを防止するための技術的な措置、例えば秘密分散方式によるバックアップを行い、CA 室で保管すること。
(6) 認証局の暗号装置に保管されている認証局の秘密鍵は、認証局の終了時に消去する。当該暗号装置内に保管されている認証局の秘密鍵を消去した上で、バックアップした認証局の秘密鍵も消去すること。
(7) 利用者の電子証明書及び CRL への電子署名に使うアルゴリズムは、SHA-256、RSA2048bit 以上、又は SHA-256、ECDSA224bit 以上とすること。ただし、楕円曲線の選択は、FIPS 186-4 に準拠すること。

2.3 設備基準

認証局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

重要なサービスへの物理的及び環境的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、以下の措置を行わなければならない。

(1) CA 室の所在が公開されていないこと。
(2) CA設備が設置された建物は耐震措置を講じること。
(3) CA 設備が設置されたラックは建物構造体に固定すること。
(4) CA 室は漏水センサを設置し、24 時間監視すること。
(5) CA 室は防火区画内に設置すること。
(6) CA 室でケーブルが防火区画を貫通する場合は、延焼防止措置を講じること。
(7) CA 室において防火区画をダクトが貫通する箇所には、防火上有効なダンパを設けること。
(8) 認証局の建物は消防設備の点検を実施していること。
(9) CA 設備のために UPS を設置していること。

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な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、以下の措置を行わなければならない。

(1) 登録局の事務室は入退室の管理すること。
(2) RA 端末は容易に持ちだせないこと。
(3) CA室への入退室は入退室管理装置の制限により、権限者 2 名以上であること。
(4) CA 室にモーションセンサを設置していること。
(5) CA 室の扉の解放時間は必要最小限に設定していること。
(6) CA 室のモーションセンサ・扉解放時間に異常があった場合、24 時間監視しているところへ警報が発報されること。
(7) CA 室には監視カメラを設置していること。
(8) CA 室の監視カメラの映像は、24 時間記録し、当該映像記録の保存期間は 1 週間以上記録されていること。

以 上