令和6年度電子署名法認定基準の
モダナイズ検討会
報告書（案）

令和7年〇月

目次

1. 検討の背景

1－1. 電子署名法について

円滑なデータの流通は、現代のデジタル社会における不可欠な要素であり、我が国においても、これらを支える様々な仕組み・サービスが展開・検討されている。その中で、電子署名については、電子署名及び認証業務に関する法律（以下「電子署名法」という。）が平成 13 年4月に施行された。これは、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的としている。

電子署名法では、電子署名等の定義（第2条）や電磁的記録の真正な成立の推定（第3条）、特定認証業務の認定（第4条）などが規定されている。この認定に係る具体的な基準については、電子署名及び認証業務に関する法律施行規則（以下単に「規則」という。）、電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（以下単に「指針」という。）、電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針（以下単に「方針」という。）で定めているが、これらの基準については法施行当初から大きな改正が行われていない。

1－2. 検討の経緯

デジタル庁による委託業務「令和4年度電子署名及び認証業務に係る利用促進業務」を通じて、これまでの調査等を通じて把握してきた実情等を踏まえつつ認定認証事業者にアンケートを実施した。その結果として、技術動向やセキュリティに関する考え方の変化等を踏まえた特定認証業務の認定基準に関する課題や、その課題解決のための基準見直しの必要性が示唆された。

上記を踏まえ、デジタル庁による委託業務「令和5年度電子委任状の普及及びリモート電子署名基準等に関する調査研究業務」により、認定基準のモダナイズのあり方に関して、短期的に対応しうるものから長期的な検討を要するものまで幅広く論点を抽出し、その内容を骨子として整理した。

2. 検討会について

2－1. 検討会の目的

今年度は、1－2で整理した論点を踏まえつつ、長期的検討の結果をいたずらに待つことなく、可能な部分から順次モダナイズを進めていくべく、「令和6年度電子署名法認定基準のモダナイズ検討会」を開催し、ニーズの把握や要件の明確化、運用へ

の影響度合い等の観点から、２－２に掲げる論点に関して、必要な情報整理と追加検討を実施した。本報告書は、その議論の結果をとりまとめたものである。

２－２. 検討会の論点

論点❶　情報セキュリティに関するリスクマネジメントの国際基準に照らし合わせた規定

論点❷　認証局の秘密鍵を管理する暗号装置の技術基準の更新

論点❸　国際的な基準を満たしつつクラウドサービスへの拡張等が可能となるようなセキュリティ基準の検討

論点❹　認証設備室の外からの遠隔操作やパブリッククラウドサービスの利用の規定

論点❺　利用者の真偽の確認における自動化の規定

論点❻　公的個人認証法に基づいて署名検証者の認定を受ける特定認証業務を行う者の基準との差異の解消

3. 論点に係る対応の方向性

本検討会で議論した内容について、２－２で掲げた論点に沿って、以下のとおり整理する。

3－1. 情報セキュリティに関するリスクマネジメントの国際基準に照らし合わせた規定

（1）検討事項

社会全体のデジタルトランスフォーメーションが加速し、我々を取り巻く様々な分野においてデジタル技術の利活用が進んでいる一方で、サイバー攻撃はその発生頻度の増加と高度化が続く状況下にあり、サイバーセキュリティ対策のさらなる強化が不可欠となってきている。このような状況を踏まえ、情報システムを取り扱う企業等においては、情報セキュリティに係るリスクへの対応が求められている。

しかしながら、電子署名法に基づく認定認証業務の認定基準は、法施行当初から大きな改正を行っていないため、近年の情報セキュリティに対する考え方の変化等を踏まえた基準となっていない状況にある。

以上を踏まえ、国内外の標準や規格等を踏まえながら、情報セキュリティに関するリスクマネジメントについて電子署名法の認定基準として規定すべきかを整理する。

（2）対応の方向性

関係する国内外の標準や規格等[1]を踏まえると、以下の図1とおり整理できる。

各標準/規格におけるガバナンスに関する内容　※青字は共通項

標準/規格参照の考え方	ISO/IEC 27001	システム管理基準	EN 319 401	SP800-53	ISMAP管理基準
5つの標準/規格を参照 • ISO/IEC 27001 • システム管理基準（METI） • EN 319 401 (ETSI) • SP800-53 (NIST) • ISMAP管理基準（ISMAP運営委員会） 標準規格の内容からガバナンス（企業のセキュリティ品質を向上させるための管理体制と監督の仕組み）に関する部分を抜粋	•運用 - 運用の計画策定及び管理 - 情報セキュリティリスクアセスメント - 情報セキュリティリスク対応 •パフォーマンス評価 - 監視、測定、分析及び評価 - 内部監査 - マネジメントレビュー •改善 - 継続的改善 - 不適合及び是正処置	•ITガバナンスの実践 - 経営戦略とビジネスモデルの確認 - IT戦略の策定 - 効果的なITパフォーマンスの確認と是正 - 実行責任及び説明責任の明確化 •ITガバナンス実践に必要な要件 - ステークホルダーへの対応 - 取締役会等のリーダーシップ - データ利活用と意思決定 - リスクの評価と対応 - 社会的責任と持続性	•TSPの管理と運営 - 内部組織 - 人的資源 - 資産管理 - アクセス制御 - 暗号制御 - 物理的および環境的セキュリティ - 運用セキュリティ - ネットワークセキュリティ - 脆弱性とインシデント管理 - 証拠の収集 - 事業継続管理 - TSPの終了および終了計画 - コンプライアンス - サプライチェーン	•GOVERN - 組織のコンテキスト - リスク管理戦略 - 役割、責任、および権限 - ポリシー - 監督 - サイバーセキュリティサプライチェーンリスク管理	•情報セキュリティガバナンスのプロセス - 概要 - 評価 - 指示 - モニタ - コミュニケーション - 保証

図 1　各標準/規格におけるガバナンスに関する基準

[1] 日本規格協会「JIS Q 27001（ISO/IEC 27001）」、経済産業省「システム管理基準」、ETSI「EN 319 401 – V3.1.1」、米国国立標準技術研究所「The NIST Cybersecurity Framework (CSF) 2.0」、ISMAP運営委員会「ISMAP 管理基準」

認定事業者等に対して最低限要求すべき事項を検討する観点で各標準/規格を整理すると、図１が示す通り、少なくとも「情報セキュリティに係るリスクの評価と対応」及び非常時を念頭に置いた「責任や権限の明確化」の２点は情報セキュリティに関するリスクマネジメントの規定に係る共通項であると言える。

まず、情報セキュリティに係るリスクの評価と対応については、電子署名法に基づく特定認証業務の認定基準として、新たに求めるべきである。具体的には、基準として、適時に情報セキュリティに係るリスク評価を実施するとともに、当該リスクへの対応方針・計画を定めること、またこれらについて組織管理に関する書類として記録することを求めるべきである。この調査においては、記録された書類を直接確認することで、リスク評価を実施し当該リスクへの対応方針・計画を定めていることを確認する方法、又は関連する第三者認証を取得していることを確認する方法のいずれかの方法でよいと考えられる。

次に、非常時を念頭に置いた責任や権限の明確化について、同様に重要であるため、電子署名法に基づく特定認証業務の認定基準に位置づけられる必要がある。このとき、現行の認定基準として、既に、平時・非常時の限定なく「業務に従事する者の責任及び権限並びに指揮命令系統」[2]を定めてその内容を実施することを求めている。また「危機管理に関する事項」[3]として何らかの事象が発生した場合に適切に対応するために必要な者に対して教育訓練が行われていることも調査の中で確認している。以上を踏まえれば、非常時を念頭に置いた責任や権限の明確化は、現行の認定基準において既に認定認証事業者に求め、その内容を調査の中で確認していることから、新たな規定を設ける必要はないと考えられる。その上で、情報セキュリティに係るリスクへの対応方針・計画の中で、非常時を念頭に置いた責任や権限の明確化等が改めて図られることは、円滑なリスクへの対応を行う観点で推奨される。

３－２．認証局の秘密鍵を管理する暗号装置の技術基準の更新

（1）検討事項

電子署名は一般に公開鍵暗号技術を利用したデジタル署名技術を活用して実現されており、具体的には、秘密鍵（署名鍵）を用いて、電子署名の措置、つまり、その秘密鍵の持ち主にしか作成することができないデータ（署名データ）を作成し、さらに、その秘密鍵と対になる公開鍵（署名検証鍵）を用いて、データに改ざんが行われていないことの検証及び秘密鍵との結びつきに関する検証を行うことによって、データの信頼性を担保することができる。さらに、この利用者の秘密鍵について、信頼でき

[2] 電子署名及び認証業務に関する法律施行規則（平成十三年総務省・法務省・経済産業省令第二号）第六条第十五号ロ

[3] 同号ト

る機関（認証局）が本人確認等を行った上で発行ないし認証局の秘密鍵との紐づけを行うことにより、利用者とその秘密鍵の紐づけを行うことができるとともに、失効の管理等も行うことにより、この利用に係る信頼性を担保することができる（これら全体の仕組みのことは、PKI（公開鍵基盤：Public Key Infrastructure）と呼ばれる。）。

この認証局と利用者の秘密鍵の紐づけについても、認証局が持つ秘密鍵を用いて、利用者の電子証明書に電子署名を行うことによって実施されており、この秘密鍵の管理が極めて重要となる。耐タンパ性の確保等によりセキュリティが確保された状態で鍵を保管・利用することができる暗号装置はハードウェア・セキュリティ・モジュール（HSM）と呼ばれ、電子署名法に基づく認定に際しても、認証局の秘密鍵（発行者署名符号）を管理する暗号装置（HSM）について、一定の基準を設けている。

しかし、この基準は法制定当時に最新であった米国基準 FIPS140-1 のレベル3を参考とした規定であり、法施行当初から大きな改正を行っていないため、HSM の技術基準の更新が急務である。

（2）対応の方向性

制定当時の考え方、また、暗号装置に係る業界の一般的な基準であることを踏まえ、米国連邦政府の情報処理標準規格である FIPS140 シリーズを参考とすると、以下の図のとおり、FIPS140 シリーズは技術の進化による危殆化や包括的な要件の必要性により二度改訂が行われている。

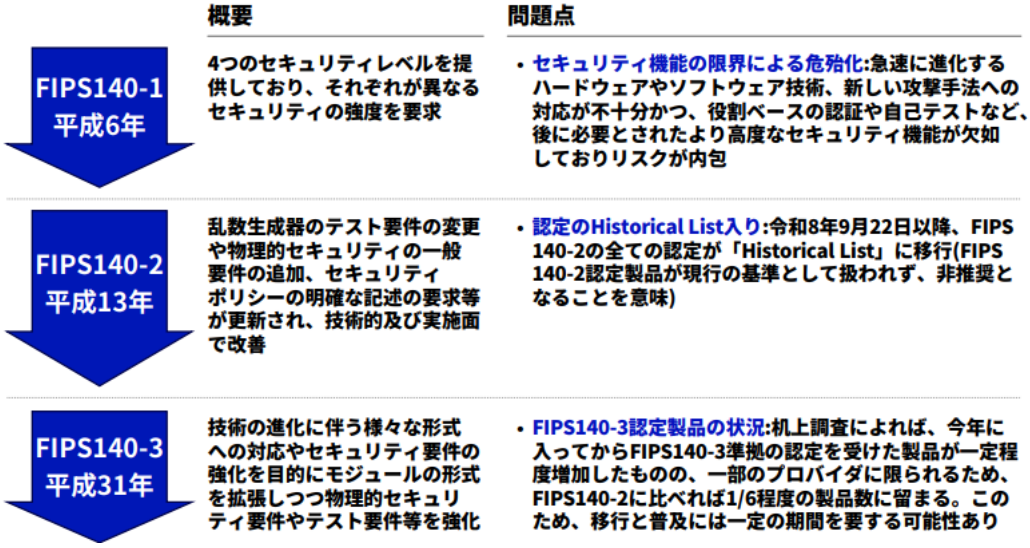

図 2　FIPS140 シリーズの変遷

最新のセキュリティ基準の適用という観点からは、図2のとおり、FIPS140-2 が令和8年（2026 年）9 月 22 日以降 Historical List に移行することも踏まえれば、適用可能な最新の基準である FIPS140-3 のレベル3と同等のものに更新することが必要であ

る。この際、「GPKI ブリッジ認証局との相互認証を行う認定認証業務については、令和 10 年（2028 年）中を目途に新暗号に対応した認証局の運用を開始すること」[4]としていることを踏まえれば、認定認証事業者に短期間で複数回の移行を求めることがないよう、同時期に FIPS140-3 のレベル3と同等以上の機器への移行を求めることが基本的な考え方になる。

その上で、現時点では FIPS140-3 の基準に準拠した製品が限られていることも踏まえ、足下では FIPS140-2 のレベル3と同等以上とすることを認定基準として求めるべきである。この調査においては、現在の製品の普及状況等に鑑みれば、FIPS140-2 のレベル3に準拠するものとして認定を受けた製品を使っていることを確認すればよいと考えられる。

3－3. 国際的な基準を満たしつつクラウドサービスへの拡張等が可能となるようなセキュリティ基準の検討

（1）検討事項

現行の電子署名法関係法令においては、発行者署名符号を作成し又は管理する電子計算機（以下「認証局の秘密鍵を管理する HSM」という。）を含む認証業務用設備 [5]について、同設備が設置された認証設備室への出入場の管理に関する措置、同設備への不正なアクセスを防止するために必要な措置、正当な権限を有しない者による同設備の作動を防止するための措置、同設備の災害の被害を防止するために必要な措置等を求めており、事実上、認定認証事業者及びこの委託先が管理するオンプレミス環境の利用を前提としている。

このような鍵管理に用いる HSM について、近年のパブリッククラウドの利活用拡大のトレンドの中、ストレージの暗号化や暗号化通信、一部認証局における利用等において、クラウドサービスプロバイダー（CSP）や HSM ベンダーが提供するクラウドサービス（以下「クラウド HSM」という。）の利用が拡大している。また、自社のリソース管理の効率化等のため、自社又はその委託先が直接管理を行い、一部のリソースの共有を行う例（以下「共同利用型 HSM」という。）も増加している。

本論点においては、上記のような背景及び1－2で述べた認定認証事業者へのアンケート等調査結果を踏まえ、認定認証業務の認証局の秘密鍵を管理する HSM としての、①クラウド HSM 及び②共同利用型 HSM の利用に関する議論を行った。

---

[4] 事務連絡「特定認証業務の基準の改正スケジュール等の周知について」（令和6年6月デジタル庁デジタル社会共通機能グループ 参事官（トラスト担当）・法務省 民事局商事課）

[5] 規則第4条第1項第4号

加えて、①及び②に関連して、③ネットワークを介して操作を行う HSM（以下「ネットワーク型 HSM」という。）の利用[6]についても議論した。

（2）対応の方向性

まず、①のクラウド HSM の利用について議論[7]を行ったが、CSP が管理する設備に対する主務省庁及び指定調査機関による調査が困難である、クラウドサービスの操作画面と実際の挙動・ログが一致していることを担保するための調査の方法等に関する課題が残る等の指摘が挙げられた。このため、当面は現行の基準とし、クラウド HSM の利活用拡大や HSM に特化した監査に関する基準等の動向に注視しつつ、必要に応じて改めて検討を行うべきである。

その際には、本検討会における議論を踏まえ、下記の論点に留意すべきである。

- 認証局の秘密鍵を管理する HSM に関する従来の管理基準との整合性を確保しつつ、クラウド HSM 特有のリスクにも対応した基準とできるか。
  - 認証局の秘密鍵（発行者署名符号）の運用は、可用性よりも機密性を重視したアーキテクチャであり、可用性も重視するクラウドのアーキテクチャにより失われる要素について、特に慎重な検討が必要。
  - BYOK（Bring Your Own Key）を利用する場合、しない場合の整理が必要な可能性がある。
  - ネットワーク経由での HSM へのアクセスは、サイバー攻撃等の新たな対象となる可能性が高いため、通信経路の保護状況の確認及びこの適切な調査・審査方法を確立する必要がある。
    - ✧ 通信に限らず、HSM を遠隔で操作する画面等と実際の指示・結果の一致等、HSM と連携するすべての面において、確実性を確保する必要がある。
- クラウド HSM 提供事業者が確保すべき機密性と、認定基準への適合性確認のための調査のバランスをどのように整理すべきか。

---

[6] ①②③の整理に関して、具体的には、HSM の操作形態に関わらず、リソースの共同利用が行われる形態のうち、いわゆるクラウドサービスとして一般に提供されるもの（運用者（委託先）を含む調査及び統制・ガバナンスに関する課題が限定的であるものを除く。）を①、同様の形態のうち、主務大臣及び指定調査機関による立入調査を行うことができる等、調査・審査方法及び統制・ガバナンスに関する課題が限定的であるものを②と整理したうえ、近年主流な HSM の操作形態であり、①及び②においても一般的なネットワークを介して操作を行う HSM 一般に関する論点（オンプレミス環境の認証設備室を含む）を③として想定している。

[7] あくまでも認証局の秘密鍵を管理する HSM における議論であって、リモート署名における利用者の鍵保管・鍵利用等におけるクラウド HSM の活用を妨げるものではない。

次に、②共同利用型 HSM については、パブリッククラウドと比較して、設備に対する主務省庁及び指定調査機関による調査の困難性に関する課題・懸念は比較的少ない。一方で、管理運営者が自社であることによらない別途の論点も多くあることから、①と同様に当面は現行の基準とし、必要に応じて改めて検討を行うべきである。

その際には、本検討会における議論を踏まえて、①で掲げた点のほかに、以下の論点に留意すべきである。

- クラウドのアーキテクチャ、共有型のサービスという性質に起因する問題
  - 同一事業者か否か
    - ✧ 同一の事業者（認定認証事業者）が自社の他サービスを含めて HSM の共同利用を行う場合
    - ✧ 異なる認定認証事業者が HSM の共同利用を行う場合
  - HSM が設置された室への立ち入りに関する基準・証跡等
- 認証局の秘密鍵を管理する HSM の利用の場面ごとにリスクを整理する必要がある。また、これらの操作を行う HSM のポートが物理的に分離されていること等も踏まえて、作業環境等が異なる場合があることにも留意する必要がある。
  - 認証局の秘密鍵を管理する HSM の利用の場面の例
    - ✧ 認証局の秘密鍵の状態を変化させる操作
      - ✓ 鍵の生成・キーセレモニー時及び鍵更新時
      - ✓ 鍵のバックアップ時
      - ✓ 保守（起動時・停止時）
    - ✧ 認証局の秘密鍵の状態を変化させない操作
      - ✓ 証明書発行時や失効リストの発行時等の署名生成時
      - ✓ その他の保守・監視時
- 認証設備室内で作業をしていた際に働いていた相互牽制の存在について

③ネットワーク型 HSM の利用については、３－４における「C）認証局の保守・運用における利用」のうち、保守における認証業務用設備への遠隔操作に関する論点とも深く関係する内容である。上記における認証局の秘密鍵を管理する HSM の利用の場面ごとのリスクの違い、HSM のポートの分離・実際のネットワーク構成等に留意しながら、「C）認証局の保守・運用における利用」と合わせて、今後必要に応じて改めて整理を実施し、ネットワーク型 HSM 利用時特有のリスクへの対処・利用時の基準の明確化に向けた検討をすることが考えられる。

３－４. 認証設備室の外からの遠隔操作やパブリッククラウドサービスの利用の規定

（1）検討事項

現行の電子署名法関係法令においては、指針第6条第1号第3条のとおり、認証設備室の外から電気通信回線経由の遠隔操作を許容しておらず、日常の保守・メンテナンスにおいても、認証設備室の中に入らなければ行うことができない。また、帳簿書類の保管や、その他認証局の設備についても、認定認証事業者又はこの委託先が運用するオンプレミス環境に設置することを基本としてきた。

近年の情報サービス一般におけるクラウドサービスの利用拡大も踏まえ、１－２. で述べた認定認証事業者へのアンケート等調査においても、遠隔操作の許容範囲の拡大や、クラウドサービスの利用に関する基準を求める声が上がっている。

本論点においては、認証局設備（３－３で議論した認証局のルート秘密鍵を管理する HSM を除く。）におけるクラウドサービスの利用及び遠隔操作について整理した。本論点については、その議論の対象となりうる機器や利用の場面は多岐にわたることから、下記 A～D のとおりに分類して検討した。

A） 認証局のリポジトリにおける利用

B） 利用者の申込み／利用者の本人確認における利用

C） 認証局の保守・運用における利用

D） 認証局の帳簿書類の保管のクラウド化

（2）対応の方向性

（1）で示したとおり、本論点の議論の対象となりうる機器や利用の場面は多岐にわたることから、本検討会の目的に沿って、早期に対応可能と考えられる点を特に優先して議論することとした。このとき、３－3における整理を踏まえると、対象となる機器や利用の場面に関して求められる機密性等の基準上の要求事項の整理やこれに係る調査のあり方の検討には慎重な検討が必要であり、一定の期間を要するものと考えられる。また、認定認証事業者におけるニーズが最も高かったことも考慮して、「A）認証局のリポジトリにおける利用」について優先して検討・整理を進め、B）～D)については本年度の議論では今後深掘りすべき論点の整理に留めることとした。

A） 認証局のリポジトリにおける利用

リポジトリにおいて利用している情報は原則として公開情報であり、また認証局によるデジタル署名が行われたデータである。このような場合に求められる機能は可用性のみであると考えられるため、パブリッククラウドの利用における課題は限定的

である。従って、リポジトリにおいてこのような情報を取り扱うことについては、認定認証業務を行う方法として認められるべきであると考えられる。

ただし、認証局のリポジトリにおける利用であったとしても、例えば以下のように可用性以外にも確保されるべき機能があると考えられる場合には、現時点で認めるべきではない。

- OCSP レスポンスを生成するロジックを含む OCSP レスポンダ自体をクラウド上に設置する場合
  - OCSP レスポンスに対しデジタル署名を行う、認証局の鍵及びこの署名を行うロジック自体をクラウド上に設置する形となるため、可用性以外の機密性・完全性も含めて担保する必要があるシステムのクラウド利用であると整理される。従って、B)～D)に係る継続的検討の結果に従うべきであり、現時点では利用を認められない。
  - なお、OCSP であっても、可用性のみが求められる部分に限ってクラウドを利用する場合[8]は、認められるべきであると考えられる。
- 認証局の帳簿書類
  - 認証局のリポジトリにおいて公開する情報であっても、規則第 12 条第1項各号に掲げる帳簿書類に該当するものについては、滅失又は毀損の防止のために必要な措置が求められている[9]。このため、D として別途の分類とし今後必要な検討を行うこととしたものであるから、現時点では利用を認められない。
  - なお、正本は別途記録媒体の互換性等を担保した保存方式による保存を行った上で、リポジトリ等において公開する副本についてクラウドを利用することは妨げられない。この場合、調査においては正本と副本が一致していること及び関連するログを確認することが必要である[10]。

リポジトリにおけるクラウド利用を採用するにあたっては、公開情報であること、クラウドを利用することでオンプレミス環境より可用性は高まっていること、調査において現に正しく認定認証業務に係る電子証明書、CP/CPS、CRL 等が公開されていること及び稼働実績の確認が必要だが現行規定の内数である[11]と考えられるため、現時点では特段の基準を設ける必要性はないと考えられる。

---

[8] 例えば、署名済みの OCSP レスポンスを CDN 等に配置する手法などが考えられる。

[9] 規則第6条第1項第 15 号へ

[10] 調査表項番 3C56 関係

[11] 調査表項番 3713 関係

他方で、諸外国及び民間の業界団体における認証局に関する監査基準やクラウドの利用基準等の動向を注視しつつ、将来的に、採用するクラウドサービスの可用性に関する基準やクラウドサービス自体のセキュリティの担保に関する基準を設ける必要性がある場合、改めて速やかに検討を行い、基準を設ける等の所要の措置を講じるべきである。

B) 利用者の申込み／利用者の本人確認における利用

C) 認証局の保守・運用における利用

D) 認証局の帳簿書類の保管のクラウド化

B)～D)に掲げたものについても、利用者の利便性向上や事業者の事務軽減に繋がること等を踏まえ、クラウドサービスの利用等については前向きに検討することが考えられる。一方でこれらは、A とは異なり公表情報ではなく、可用性のみならず機密性等を確保する必要があるため、前述のとおり基準上の要求事項の整理やこれに係る調査のあり方については慎重な検討が必要[12]であり、またその検討を経てから遠隔操作が認められうる範囲についてニーズとともに整理する必要があることから、一定の期間を要するものと考えられる。その上で、本検討会において一定の議論を行ったところ、その論点を以下のとおり整理する。なお、下記は論点を網羅的にカバーしたものではないことに留意すべきである。

- 利用を認めることが考えられるクラウドサービス
  - 論点３－3における認証局の秘密鍵の取扱いとは異なり、一般的な情報となるため、その多くの場合において、クラウドサービス自体の安全性を担保する認証制度やクラウドサービス運用者のセキュリティマネジメントの担保等に関する認証制度（ISMS、ISMS クラウドセキュリティ認証、SOC2、ISMAP 等）を活用できるのではないか。
    - ISO/IEC27000 シリーズ、特に ISO/IEC27017 を参照するべきではないか。
    - クラウドサービスの安全性に関する既存の基準についても、それぞれ確認を行っている内容が同一ではないため、観点ごとに個別に十分か否かの判断を行う必要があるのではないか。

[12] 認証局におけるリスクを踏まえた整理（具体的には、認証局で利用される個々のシステム及びそのシステムにおいて取り扱われる情報の性質ごとに異なる可能性があり、個別に判断が異なる可能性がある点に関する整理）を行った上で、クラウドサービスのセキュリティ確保に関する各種認証制度がこのリスクプロファイルへの対処として適切であるかを検討を行った上でこれを採用する必要があるという意味であって、機密性を求めるデータをクラウドサービス上で取り扱ってはならないという意味ではない。

- ✧ エビデンスやテストケースの援用についても、同様に、個別の判断となるのではないか。

- 例えば、政府情報システムにおけるクラウドサービス利用基準では、公開情報（機密性1）を取り扱うシステムについては ISMAP の取得までは求めておらず、一定程度取り扱いに注意が必要であり関係者だけが知り得るべき情報（機密性2以上）を取り扱うシステムにおいて ISMAP 等を求めている。電子署名法による認定認証業務は政府情報システムではないため、当然、これらに係る基準は適用されないものの、この考え方を参考として、A)については求めていなかったクラウドサービス自体の安全性に関する規定について、B)～D)については求めることが基本となる（また、この逆も言える）のではないか。[13]
- また、プライベートクラウド等、主務省庁及び指定調査機関による調査等を容易に実施でき、運用者（委託先）を含む統制・ガバナンスに関する課題が限定的である場合には、特別の認証制度等を求めず、既存の電子署名法の基準を適用することもありうるのではないか。
- なお、既に業務の一部にクラウドサービスを活用している事例（ヘルプデスクにおけるクラウドサービスの利用等）については、クラウドサービス利用に関する基準検討の影響を最小限とするため、クラウドサービスの利用形態を踏まえ求められる機密性やその影響度等を慎重に検討すべきではないか。
- クラウド間、クラウドへの接続における通信の安全性の確保については、閉域網接続や CSP が提供するインターネットを経由しない方法を利用することとし、インターネット経由での接続は（アタックサーフェスを増大させるため）可能な限り避けた方が良いのではないか。
- ログ・死活監視サービス等の SaaS の恩恵が大きい利用形態も考えられるため、SaaS の利用を妨げないような形で整理を行う必要があるのではないか。

- 保守における認証業務用設備への遠隔操作
  - 「C）認証局の保守・運用における利用」のうち、保守における認証業務用設備への遠隔操作（ログ・死活監視サービスに関するクラウドサービスの利用を除く。）については、クラウドサービスとの利用とは直接関係がない論点であり、個別に検討を進めることが適当である。本点につい

[13] 認定認証業務の多くは政府認証基盤とブリッジ認証を行っており、これを介して多くの政府情報システムとも接続していることから、政府情報システムに準ずるシステムとして、これらに関する基準及び考え方を参考として利用できるという趣旨。

ては、利用者の電子証明書の発行といった、発行者署名符号（認証局の秘密鍵）に係る操作を含まない、CA システムの実行状況の確認等に関する遠隔操作については、一定のセキュリティ（通信に関するセキュリティ、相互牽制等）の担保を条件に許容する方向として検討を進めることができるのではないか。

- なお、その場合であったとしても、HSM の詳細な仕様（保守用ポートにおいて実行できる操作等の限定の程度等）・実際の運用状況を踏まえた更なる整理等、引き続き検討が必要な課題がある点には留意が必要ではないか。
- 「C）認証局の保守・運用における利用」であって、ログ・死活監視サービスに関するクラウドサービスを利用する場合において、認証業務用設備とクラウドサービス（クラウド上に存在するログ・死活監視サーバー）との通信が発生することが考えられるが、監視対象の閉域にエージェント等を設置し、内部から外部へアクセスを行う形とする等により、リスクを低減することができるのではないか。
- 保守のための遠隔操作において、インターネット環境より VPN・ランディングサーバー等を経由して行える範囲については、特に慎重に検討した方が良いのではないか。
  - ✧ インターネットとは独立した専用の監視 NW を利用した遠隔操作と区別して考えるべきではないか。

３－５. 利用者の真偽の確認における自動化の規定

（1）検討事項

認定認証業務による電子証明書の発行プロセスの中でも、利用者の真偽を確認すること（利用者の身元確認）は特に重要なプロセスの一つである。その重要性に鑑み、また、発行に係るプロセスを事後で検証・監査可能とするために、特定認証業務の認定基準においては、様々な証跡を保存すること（帳簿等の保存）を求めている。これまで、この基準の一つとして、利用の申込書を「受領した者」を記録することが求めている点[14]については、自然人が受領することを前提として運用されていた。

その後、技術的進歩やマイナンバーカード等の電子的に身元確認及び本人の意思の確認を行う手段の普及により、利用者の真偽の確認を容易に自動化することが可能となったことを踏まえ、認定認証業務の利用者の利便性向上等の観点から、令

[14] 方針第６１.（1）

和5年6月に運用を見直し、適切な業務プロセスや人員配置がなされる場合にあっては、その帳簿記入を含めた自動化を認めることとした。

この時、迅速性を優先したことから、指定調査機関からの通知[15]により運用の見直しを行ったため、電子署名法関係法令等において改めて取り扱いの明確化を検討する必要がある。

（2）対応の方向性

自動化によって、利用者の真偽の確認のみならず関連する事務手続（証明書の発行指示や受領確認等）も自動化又はプロセス自体の削除が可能であり、従前のフローよりも利用者の利便性向上や事業者の事務軽減に繋がると考えられる。従って、認定認証業務の利活用を促す観点からも引き続き自動化を認めるべきであり、その運用をより明確にするため、電子署名法関係法令等において改めて明確化すべきである。

なお、自動化した場合であっても必要な本人確認の強度を担保する、サイバー攻撃に対して脆弱なプロセスとならないよう必要な対応を行う等、実際の導入に際しては様々なリスクに留意することも必要である。

3－6．公的個人認証法に基づいて署名検証者の認定を受ける特定認証業務を行う者の基準との差異の解消

（1）検討事項

現行の電子署名法関係法令では、電子署名を行うために用いる符号（以下「利用者署名符号」という。）を利用者が作成する場合には、当該利用者署名符号に対応する利用者署名検証符号を認定認証事業者が受信する際に、あらかじめ利用者識別符号の送受を行って利用申請者と利用者識別符号の受信者が同一であることを確認することで、間違いなく電子証明書が利用者に送付されていることを確保するよう求めている[16]。すなわち、認定認証事業者と利用者との間で2往復の事務プロセスを必須としている。

しかしながら、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（以下「公的個人認証法施行規則」という。）では、上記の方法に加えて、利用者が電子証明書の利用申込と同時に利用者署名検証符号を送付する方式も認めている[17]。この方式は、認定認証事業者と利用者との間の事務プロ

---

[15] JIPDEC「利用者の申込みに対する諾否を決定した者の氏名」を記録した帳簿を保存することを求めていることに関する真偽の確認の自動化について（令和5年6月1日）

[16] 規則第6条第3号の2

[17] 公的個人認証法施行規則第 26 条第5号イ

セスを1往復とすることができるため、利用者の利便性向上や事業者の事務軽減に資すると考えられる。

このため、利用者が電子証明書の利用申込と同時に利用者署名検証符号を送付する方式を電子署名法でも認めることが可能かを検討する。

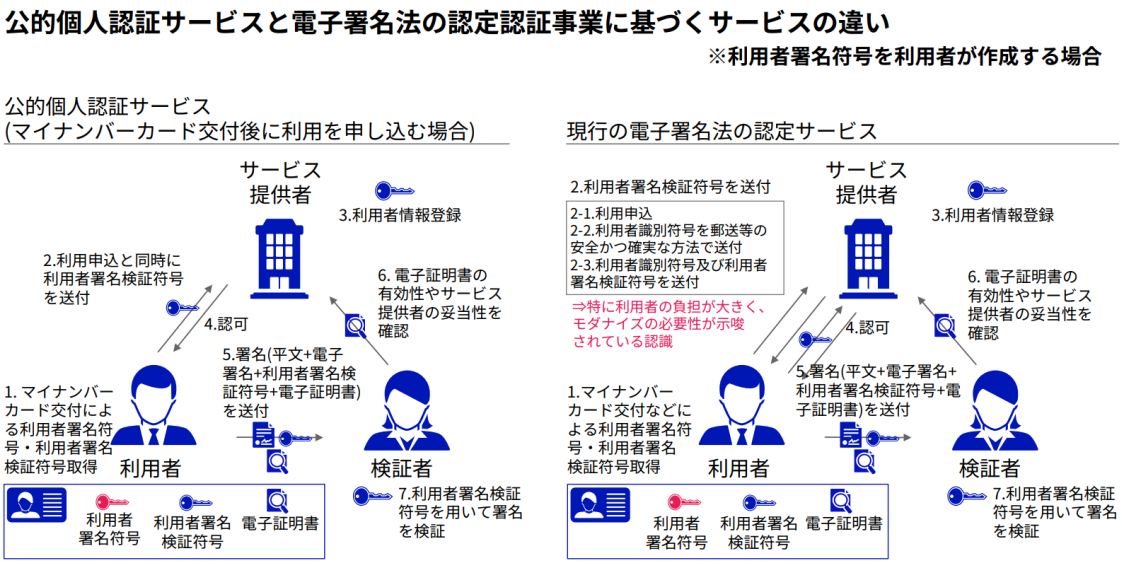

図 3 各法令に基づくサービスの違い

(2) 対応の方向性

認証事業者が利用者署名符号を生成する場合には、当該符号及び電子証明書が①改変されることなく利用者の手に渡ること、②認証事業者の手元に残らないこと、③利用者本人以外の第三者の手に渡らないこと、を求めている。一方で、利用者が利用者署名符号を生成する場合には、利用者署名符号を認定認証事業者から利用者に交付又は送付することはないため、①及び②を満たす必要はそもそもなく、③を確保することが電子署名法の関係法令における要求だと考えられる。このため、利用者が電子証明書の利用申込と同時に利用者署名検証符号を送付する方式がこの要求を満たす場合、当該方式を電子署名法でも認めることが可能である。

上記要件を満たすのは、現時点では、利用の申込みに際して、マイナンバーカード署名用電子証明書又は認定認証業務によって発行された電子証明書のいずれかによる電子署名がなされた場合のみだと考えられる。このため、本人確認のためにいずれかに該当する電子署名を付して利用の申込みを行う場合に限り、利用者が電子証明書の利用申込と同時に利用者署名検証符号を送付する方式を認めるべきである。

なお、利用者の真偽の確認のために提出された書類等については既に記録を求めており[18]、新たに何らかの規定を設ける必要はないと考えられる。この調査においては、既に認証事業者に対しては調査表において公的個人証明書及び有効性確認記録（OCSPを用いた確認及びOCSPレスポンスの証跡の記録）の保管を求めていることから、当該証跡を確認すればよいと考えられる。

３－７．その他

３－１から３－６までで整理した対応の方向性については、長期的検討の結果をいたずらに待つことなく、可能な部分から順次モダナイズを進めていく、という本検討会の目的に沿って、所要の措置を講じるべきである。ただし、３－１で示したリスクの評価と対応、及び３－２で示したHSMに関する基準改正については、リスク評価の新たな実施や機器更新が必要な事業者もいること等から、これらに必要な期間に限り、適切な経過措置を設けるべきである。

なお、本検討会の論点とは別途、中長期的な事項として以下について指摘する意見もあった。今後、３－１から３－６までで継続的な検討が必要だと整理された課題とともに、拙速な議論とならないよう留意しつつ、適切な時機にその要否も含めて検討することが考えられる。

・法令構造等の整理

・リモート署名等に係る対応　等

[18] 規則第１２条第１項第１号ハ

（参考1）　令和6年度電子署名法認定基準のモダナイズ検討会　開催実績

第1回　令和6年9月20日

議事：　1. 電子署名法について
　　2. 昨年度事業の振り返り
　　3. 本検討会における検討の方針と内容
　　4. モダナイズの方向性課題①と課題②に関する議論
　　5. 次回以降の進め方について

第2回　令和6年11月1日

議事：　1. 第 1 回検討会の振り返り
　　2. モダナイズの方向性③から⑥に関する議論
　　3. 次回開催について

第3回　令和6年11月26日

議事：　1. モダナイズの方向性に関する追加議論
　　2. 次回開催について

第4回　令和7年1月17日

議事：　1. モダナイズの方向性についてのとりまとめ

（参考2）　令和6年度電子署名法認定基準のモダナイズ検討会　委員名簿

氏名	所属
漆嶌　賢二	GMO　グローバルサイン株式会社事業企画部　フェロー
小田嶋　昭浩	電子認証局会議　理事
松本　泰	特定非営利活動法人日本ネットワークセキュリティ協会 フェロー
満塩　尚史	順天堂大学健康データサイエンス学部　准教授
宮内　宏	宮内・水町 IT 法律事務所　弁護士

（敬称略、令和7年〇月時点）

※オブザーバー

一般財団法人 日本情報経済社会推進協会（JIPDEC）

総務省

法務省

（参考3）　令和6年度電子署名法認定基準のモダナイズ検討会　結果概要

3－1．　情報セキュリティに関するリスクマネジメントの国際基準に照らし合わせた規定

○情報セキュリティに係るリスクの評価と対応について、認定基準として新たに求めるべき（この際、非常時を念頭に置いた責任や権限の明確化等が改めて図られることは、円滑なリスクへの対応を行う観点で推奨される）

3－2．　認証局の秘密鍵を管理する暗号装置の技術基準の更新

○令和 10 年（2028 年）中を目途に FIPS140-3 のレベル3と同等以上の機器への移行を求めることが基本的な考え方

○その上で、現時点では FIPS140-3 の基準に準拠した製品が限られていることも踏まえ、足下では FIPS140-2 のレベル3と同等以上とすることを認定基準として求めるべき

3－3．　国際的な基準を満たしつつクラウドサービスへの拡張等が可能となるようなセキュリティ基準の検討

○当面は現行の基準とし、クラウド HSM の利活用拡大や HSM に特化した監査に関する基準等の動向に注視しつつ、必要に応じて改めて検討を行うべき

3－4．　認証設備室の外からの遠隔操作やパブリッククラウドサービスの利用の規定

○認証局のリポジトリにおける公開情報の取り扱いについては、パブリッククラウドの利用が認められるべき

○その他については、利用に係る諸課題について前向きに検討

3－5．　利用者の真偽の確認における自動化の規定

○引き続き自動化を認めるべく電子署名法関係法令等において改めて明確化すべき

3－6．　公的個人認証法に基づいて署名検証者の認定を受ける特定認証業務を行う者の基準との差異の解消

○利用の申込みに際して本人確認のためにマイナンバーカード署名用電子証明書等による電子署名が付される場合は、利用者が電子証明書の利用申込と同時に利用者署名検証符号を送付する方式を認めるべき