電子署名法における認定基準のモダナイズに関する検討会 第二回

モダナイズの方向性に関する追加議論

2024-11-01　　デジタル庁 デジタル社会共通機能グループ

デジタル庁
Digital Agency

第2回検討会の位置づけ

本年度事業の議論対象となる認定基準のモダナイズ案は以下の６テーマ

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
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
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
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
❺ 利用者の真偽の確認における自動化の規定
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

- 前回の検討会では検討会の方針とゴール及び、モダナイズの方向性❶・❷について議論したためその振り返りをしつつ、❸～❻のモダナイズ案について議論を進める

第二回検討会の目次

1.　第一回検討会の振り返り　P4

2.　モダナイズの方向性 ❸ ～ ❻ に関する議論　P6

第一回検討会の振り返り

第一回検討会の振り返り

論点❶のご意見：リスクマネジメントではなく組織全体のガバナンスとして認定基準を導入すべき。

論点❷のご意見：FIPS140-3への移行自体は必要だが、そのタイミングについては整理が必要。

議論テーマ	議論内容	決定事項及び本検討会での追加議論内容
検討会の方針・ゴール	技術動向を踏まえたモダナイズの必要性や、昨年度事業の振り返り、検討会の方針を事務局から説明したうえで、それに対する各委員からの意見を招集	• 本検討会の方針として、提示したモダナイズの方向性❶～❻を優先して議論を進めることを合意 • 委員からは以下についてもご意見あり - 法令構造や認定基準のスキーム - リモート署名やAATL等のその他モダナイズの可能性について
モダナイズの方向性❶	リスクマネジメントを電子署名法に盛り込むための基準改正の範囲及び、改正する際に盛り込むべき内容について議論	• 法改正は不要だが、施行規則でリスク管理の義務を明示することが必要 • リスクマネジメントは単なるセキュリティ対策ではなく、組織全体のガバナンスとして位置付け、盛り込むべき - 盛り込む際は、ESTIだけではなくISMSやNIST指令、ISMAPといったガバナンスに関する基準が規定されたものを参照
モダナイズの方向性❷	認証局の秘密鍵を管理する暗号装置の技術基準を更新することの必要性及び、適合すべきFIPS140のバージョンについて議論	• 暗号装置の技術基準をFIPS140-3に更新すること自体は必要 • 一方、FIPS140-3準拠の製品は市場に少ないため、現時点ではFIPS140-2相当とし、FIPS140-3への移行時期は国内の関連製品の動向等を踏まえることも必要

モダナイズの方向性 ❸ ～ ❻ に関する議論

❸ に関するR5年検討事項と本検討会での議論の方針

R5年度検討事項：成果の振り返り

現行の施行規則では、HSMを搭載し発行者署名符号を持つサーバ設備や電子証明書を発行する**認証業務用設備は認証設備室に設置する**ことを要件としており、**クラウドHSMの利用は同要件に適合しないが、同様の項目の審査を行い、利用できる形とするべきではないか。**

そのため、クラウドHSMの審査方針(ハードウェアの管理体制等)の検討が必要

本検討会での議論の方針

ネットワークを介したHSMの利用の可否について、R5年度に検討した内容に対する追加のコメントを受けつつ、**具体の基準や審査の変更点等**を検討

上記を踏まえ、ニーズの把握、遠隔操作の要件、調査・審査の方法の３つの観点を議論

ニーズの把握	3-1 特定認証業務におけるクラウドHSMの利用のニーズ及びメリット並びに緊要性について
遠隔操作の要件	3-2 ネットワークを介し（遠隔操作を行い）、クラウドHSMを利用する場合の基準
調査・審査の方法	3-3 本点について設けられる基準への準拠を担保するための調査・審査の方法における課題について

❸ の論点詳細

観点	論点	論点詳細
ニーズの把握	3-1 クラウドHSMの利用に関するニーズ及びメリット並びに対応の緊要性	• 本点については、将来的にリモート署名（今年度の検討会のスコープ外）に関する基準を整備する際に特に求められる観点という理解でよいか • 主たるメリットは、特定認証業務を営む事業者によるHSM周辺設備の維持管理に係るコスト等の低減か • その他のニーズ・メリットとしてどのようなものがあるか
遠隔操作の要件	3-2 ネットワークを介したHSMの利用の可能にする場合、利用の基準はどのようにするべきか	• ネットワークを介し（遠隔操作により）クラウドHSMを利用する場合の基準について、論点 ❷ と同様にFIPS140シリーズ相当を満たすHSMの利用を求めることでよいか • その他にクラウドHSMを利用する場合に特別に求める要件はないか • 遠隔操作に関する基準として必要な要素は何か
調査・審査の方法	3-3 ❸ に関して設けられる基準への準拠を担保するための調査・審査の方法における課題は?	• クラウドHSMの提供事業者が示すユーザーガイドや、外部監査の認定の事実等の確認だけで、現在実施している実地調査と同程度の確認が可能か - より具体の調査が必要な場合、クラウドHSMの提供事業者の協力が必須だが、セキュリティ等の観点から懸念があるのではないか • その他の課題、審査方法としてどのようなものがあるか - 報告徴収や立入検査等の対象として整理すべきか

3-2：HSM及び認証業務用設備に関する認定基準
3-3：調査・審査の方法

の論点について

- 電子署名法の各種認定基準を踏まえれば、HSM及び認証業務用設備に関連する基準は大まかに下記の３種類に分類されると考えられる。

A) HSM自体の安全性等に関する基準

・ 暗号装置に関する基準（論点②において議論）

B) HSMを設置する部屋（認証設備室）及び建物に関する基準

・ 入退室管理の設備、災害被害を防止するための対策（防火・水害・停電等）

C) HSM等の運用に関する基準

・ 入退室管理や指揮系統、管理基準等のルール整備・徹底の状況、操作の履歴の記録　等

クラウドHSMに特別に求めるべき基準はあるか？
遠隔操作に関する基準として必要な要素が何か？

3-3：調査・審査の方法に関する論点について

項目	従来のHSM	クラウドHSM
設置場所	特定認証業務を営む事業者又はその委託先等のデータセンター等に設置	プロバイダーが提供するデータセンター内に設置
管理と運用	特定認証業務を営む事業者等がHSMの物理的な管理、運用、メンテナンスを実施	プロバイダーがハードウェアの運用・管理を実施し、ユーザーはAPIやコンソールを通じてHSMの機能にアクセスし管理
第三者による運用確認方法・対象	物理的に設置されたHSM自体及びこれが設置された場所への物理的なアクセス制御、関連する規程類の整備状況、運用等の状況を現地へ赴き確認	クラウドHSMは物理的なインフラをクラウドサービスのプロバイダーが管理 →従来のような指定調査機関による直接の確認はどの程度困難か。クラウドHSM提供事業者の協力（実地調査受入、運用状況の開示等）がどの程度必要か サービスの使用状況、アクセス制御、設定、ログ管理等については確認可能 →これらでは十分ではない点なども含め、どのような観点で何を確認するべきか

議論すべきポイント

❹ に関するR5年検討事項と本検討会での議論の方針

R5年度検討事項：成果の振り返り

認証業務用設備の操作による電子証明書の発行や失効等の操作について、適切な遠隔操作の環境が担保されている際の認証業務用設備のメンテナンス作業等において、遠隔操作を認めるような基準を検討するべきではないか。

また、その他の一部場面においても遠隔操作を認め、パブリッククラウドサービスの利活用を許容するための基準を検討するべきでないか。

それを受けた本検討会での議論の方針

認証局の運営において、リモート操作を許容できる範囲、許容する際の措置、クラウド上にある機器の審査の方法等について検討

上記を踏まえ、ニーズの把握、要件の明確化、運用への影響の観点で以下を議論

ニーズの把握	4-1	（適切な遠隔操作の環境を担保したうえで）パブリッククラウドの利用が考えられる範囲について、具体的な機器・機器のカテゴリごとにどの程度のニーズがあるか
遠隔操作の範囲・要件	4-2	認証局の運営において、パブリッククラウドの利用（遠隔操作）を許容できる範囲、また、許容する際の措置としてどのような基準を求めるか?
調査・審査の方法	4-3	本点について設けられる基準への準拠を担保するための調査・審査の方法における課題について

(参考)認証局の設備の説明

設置場所[1]	認証局の設備	定義	設備例
高セキュリティゾーン	認証業務用設備	発行者署名符号を格納、或いは制御可能な設備	CA システム，登録用RA サーバ， CA システム制御用端末，証明書発行用端末
セキュアゾーン	登録用端末設備	高セキュリティ・ゾーンのCAシステムに対して、適切なアクセス制御下で電子証明書のユーザー情報（個人情報）を登録する端末設備	ユーザー登録用端末
	本人確認用設備	適切なアクセス制御下で利用者から提出された電子証明書の発行申請に係るユーザー情報（個人情報）を記載した利用申込書、及びそれを証明する本人確認書類と照合し、本人確認審査を実施した結果及びユーザー情報（個人情報）を保管する設備	利用申込書審査システム，審査データベースシステム
	利用者識別設備	高セキュリティ・ゾーンのCAシステムに対して、適切なアクセス制御下で、専ら電子証明書発行要求を送付する利用者を識別するための設備	利用者識別専用Web サーバ
フロントエンド / インターナルサポートシステム	利用申込用利用者情報入力設備	電子証明書利用者がインターネット上でアクセスし、自らの電子証明書の発行申請に係るユーザー情報（個人情報）を入力するWeb システム設備	利用申込書情報入力Web システム
	リポジトリ設備	電子認証局の運用に係る認証局運用規程類、認証局の認証局証明書、電子証明書の失効情報等の情報公開を行うパブリックIP アドレスを持つ設備	Web サーバ，LDAP サーバ

1. 言葉の定義は”Network and Certificate System Security Requirements Version1.7”2のDefinitionsを要参照

パブリッククラウドやVPN等の利用による遠隔操作を認めるには、セキュアな環境の確保が肝要

ゴール	方針	具体設備例	備考
適切な遠隔操作の環境が用意されている条件下における認証業務用設備のメンテナンス作業などにおける遠隔操作を認めるような基準	パブリッククラウドの利用	• 利用者識別設備、リポジトリサーバ、利用申込書用利用者情報入力設備、などセキュアゾーンに設置されるもの • 本人確認審査システム用DBサーバ • マイナンバーカードに格納されている署名用証明書と利用者証明用証明書の署名検証を行う署名検証サーバ	適切なセキュリティ対策の実施が前提 なお、マイナンバーカード（JPKI）における民間署名検証者（PF事業者）の認定要件においては、オンプレミスの署名検証サーバが求められているため、本点につき先にモダナイズを実施した場合には差異が生じる。
パブリッククラウドの利用と、VPN等を用いたセキュアな環境での遠隔操作により実現する方針で検討	VPN等によるセキュアな環境での遠隔操作	• 高セキュリティ・ゾーンに設置される認証業務用設備	適切なセキュリティ対策の実施が前提 CA システムの実行状況の確認（プロセスの実行確認、ログファイルの確認／収集など）するものに限り、発行者署名符号に対する操作については引き続き禁止とする

Source:株式会社コスモス・コーポレイション, 一般社団法人デジタルトラスト協議会「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」

❹ の論点詳細

観点	論点	論点詳細
ニーズの把握	4-1 認証局の運営において、クラウド利用／遠隔操作を行うニーズが高い点（機器、機器のカテゴリ）はどこか?	• 認証局にとって、クラウド利用／遠隔操作の需要が高いカテゴリはA)～D)どこか。 • 特に、事業者のみならず利用者に対してもメリットがあるカテゴリはどこか。
遠隔操作の範囲・要件	4-2 認証局の運営において、リモート操作を許容できる範囲、許容する際の措置はどのようにするのが良いか?	• 以下の基準を念頭に置くとき、P15の整理及び具体の設備例のうちリモート操作を許容できる範囲はどこか。 ➢ 現行の電子署名法で求める要件等を担保できるもの ➢ 他の基準（CA/Browser Forum・WebTrust、eIDAS等） • クラウド利用を許容する際に求めるべき基準は。 • また許容する際に、適切なセキュリティ対策が実施されていることが前提となるが、この具体的な内容は。
調査・審査の方法	4-3 ❹に関して設けられる基準への準拠を担保するための調査・審査の方法における課題は?	• クラウド上にある機器の審査方法は、3-3と同様、パブリッククラウド事業者が提供するユーザーガイドなどの情報を基に参照する方針でよいか?またその際の懸念点は? • その他の審査方法としてどのようなものがあるか?

4-1：ニーズの把握
4-2：遠隔操作の範囲・要件

の論点について

- クラウド利用／遠隔操作を念頭に置くと、特定認証業務に関する機器等は以下のとおり分類できるのではないか。また、以下のような観点で検討することが必要ではないか。
  - 認証局の運営の観点から特に需要が高いのは、A) ～ D) のどこか。
  - 利用者にとってもメリットがある点はどこか。
  - 既存の基準が担保している内容及び特定認証業務の認定制度の目的を踏まえて、クラウド利用／遠隔操作が許容可能な範囲はどこか。
  - 他の関連する基準（CA/Browser Forum・WebTrust、eIDAS等）において利用が認められている範囲を踏まえると、クラウド利用／遠隔操作が許容可能な範囲はどこか。

A)　認証局のリポジトリにおける利用
●認証局の公開鍵やCRL、CP/CPSの公開

B)　利用者の申込み／利用者の本人確認における利用
●利用者の審査システム、利用者の本人確認情報に関するDBの設置
●利用者の申込みに関する情報を保管する場合 D) にも関係

C)　認証局の保守・運用における利用
●ログ・死活管理サーバの設置、遠隔での保守における利用

D)　認証局の帳簿書類等の保管のクラウド化
i.　利用者に関する情報が含まれるもの
●利用者の申込に関する情報（ B)にも関係）
ii.　利用者に関する情報が含まれないもの
●入退室履歴の管理簿等の保管等

4-2：遠隔操作の範囲・要件
4-3：調査・審査の方法 } の論点について

- クラウド利用／遠隔操作の基準の観点の例として、下記が考えられるが、それぞれにつきどういった内容を求めるか。前ページA)～D)それぞれの利用形態において求める内容・基準は異なるものとなるか、共通となるか。これ以外の観点もあるか。

1. 技術的な基準について（論点4-2）
   - i. 通信の安全性等の情報セキュリティの確保（VPN等の利用、異常通信の監視等）
   - ii. 高可用性の担保
     - ➢ これまでもバックアップサーバの設置を求めていた用途について、クラウド化する場合に高可用性を担保する構成を求めるか。

2. クラウド利用／遠隔操作の調査の方法について（論点4-2、論点4-3）
   - i. クラウドの具体的な構成図と実態等の比較、権限・ログ等の確認
   - ii. 利用するクラウドサービスが一定のセキュリティの確保されたクラウドサービスであること
     - ➢ ISMAP、ISMS/ISMSクラウドセキュリティ認証（ISO27xxx系）、SOC2/SOC3等一般的なクラウドサービスに関する監査基準及びこれに相当する基準を満たすサービスの利用を求めることでよいか。
       - ・ これらの監査基準及び制度よって担保される範囲には差異があるが、特定認証業務に利用されるクラウドサービスとして求めるべき範囲は？また、その範囲をカバーしている制度は？
     - ➢ 調査・審査の場面においては、上記の監査・認定等を受けている事実を確認することになるか？（論点4-3関係）

❺ のR5年検討事項とそれを受けた本検討会での議論の方針

R5年度検討事項：成果の振り返り

認定認証業務に関し、電子署名の利用者の真偽の確認及びこれを踏まえた利用申込の許諾決定について、従前は自然人による必要があるものとして運用

技術動向や利便性向上等の観点から、次頁に記載したような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、その帳簿記入も含めた自動化を認めることとした

現在は指定調査機関からの通知により対応しているが、明確化の観点から所管官庁名の文書（方針等）に記載

それを受けた本検討会での議論の方針

左記のとおり、明確化の観点から所管官庁名の文書（方針等）に記載

明確化に際して適切な規定を設ける観点から、自動化の具体化な適合例について情報収集

- 左記解釈を踏まえ、既にmy FinTech株式会社がこの方法に沿った業務を実施中

上記を踏まえ、ニーズの把握の観点で以下を議論

ニーズの把握	5-1 マイナンバーカード使用時等の身元確認の結果を受けた諾否の自動化の具体化な適合例としてどのようなものがあるか?

(参考)自動化に関する指定調査機関の通知（概要）

利用者の真偽確認に係る自動化

- CP/CPSにおいて電子署名の真正性の検証、電子証明書の記載内容、形式等を確認するとともに、利用者が入力した申請情報と電子証明書の記載内容の一致確認を行うなど具体的な確認手法が明記されているのであれば、それを機械的に行うことについて特に問題ない
- 他方、CP/CPSにおいて「利用者の真偽確認」が不備なく完了した場合には必ず利用を応諾する決定をするとの取扱いを定めた上、当該取扱いに従ってシステムが動作することについて、システムの瑕疵等により不適切な発行がなされていないことの定期的な確認や、障害発生時の対応について責任を有する要人を配置するされているのであれば、といった前提が必要

諾否決定者の帳簿記入に係る自動化

- 諾否の決定をした者として、その責任者の氏名を自動で帳簿に記入することについて特に問題ない

参照：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）

LRAによる利用者の真偽確認が必要な業務について自動化

LRAによる真偽確認が必要な業務	従来（認定取得時）のLRA業務		現在のLRA業務
	オペレーション１回目	オペレーション２回目	
新規発行（スマホアプリ）	本人確認及び利用申込の許諾 →	利用者識別符号の突合及び証明書発行指示	全ての業務を自動化
再発行（スマホアプリ）	本人確認及び再発行申込の許諾 →	利用者識別符号の突合及び証明書発行指示	全ての業務を自動化※
スマホアプリによる失効申請	本人確認及び失効申込の許諾		全ての業務を自動化※

※FPoSライブラリによる申請に限定

参照：my FinTech株式会社「利用者真偽の確認に係る自動化対応について」

審査自動化後のフロー：新規発行

自動化による事務軽減

プロセスの削除による事務軽減

従来のフロー

スマホ	RAシステム	LRA	スマホ	LRA	IAシステム	スマホ
証明書発行の申込	マイナンバーカードの証明書・署名の検証	申込の諾否を決定	鍵ペアの生成 & 利用者識別符号の送付	証明書の発行指示	証明書の発行	証明書の受領確認

申込の諾否をシステムで自動決定するように変更

利用者識別符号によってIAを自動で作動させるように変更

受領確認の送信プロセスを削除

変更後のフロー

スマホ	RAシステム	LRA	スマホ	LRA	IAシステム	スマホ
証明書発行の申込	マイナンバーカードの証明書・署名の検証	申込の諾否を決定	鍵ペアの生成 & 利用者識別符号の送付	証明書の発行指示	証明書の発行	証明書の受領確認

参照：my FinTech株式会社「利用者真偽の確認に係る自動化対応について」

❺ の論点詳細

観点	論点	論点詳細
ニーズの把握	5-1 マイナンバーカード使用時等の身元確認の結果を受けた諾否の自動化の具体化な適合例としてどのようなものがあるか?	• my FinTech株式会社の事例では「 新規発行/再発行時/アプリからの失効の申し込みの諾否決定 」や「古い証明書の失効通知」等を自動化しているが、そのような取組を実施している他の事例はあるか。（認定認証業務以外の事例も含む。以下同じ。） • 「利用者の真偽の確認」という範囲で、上記と異なる業務フローの自動化事例はあるか。

❻ のR5年検討事項とそれを受けた本検討会での議論の方針

R5年度検討事項：成果の振り返り

現行の施行規則においては、利用者署名符号を利用者が作成する場合、利用者による申し込みと同時に利用者署名検証符号を送信する方法が規定されておらず、利用者識別符号の交付あるいは送付を行う必要がある
利用者と事業者双方の負担軽減のため、公的個人認証法施行規則において認められている同時送付も可能とすべき

一方で、電子署名法と公的個人認証法とでは、認定に係る調査方法、監査方法等に差異があり、**方法の統一には電子署名法の認定手続の大幅な変更が必要となる可能性**

それを受けた本検討会での議論の方針

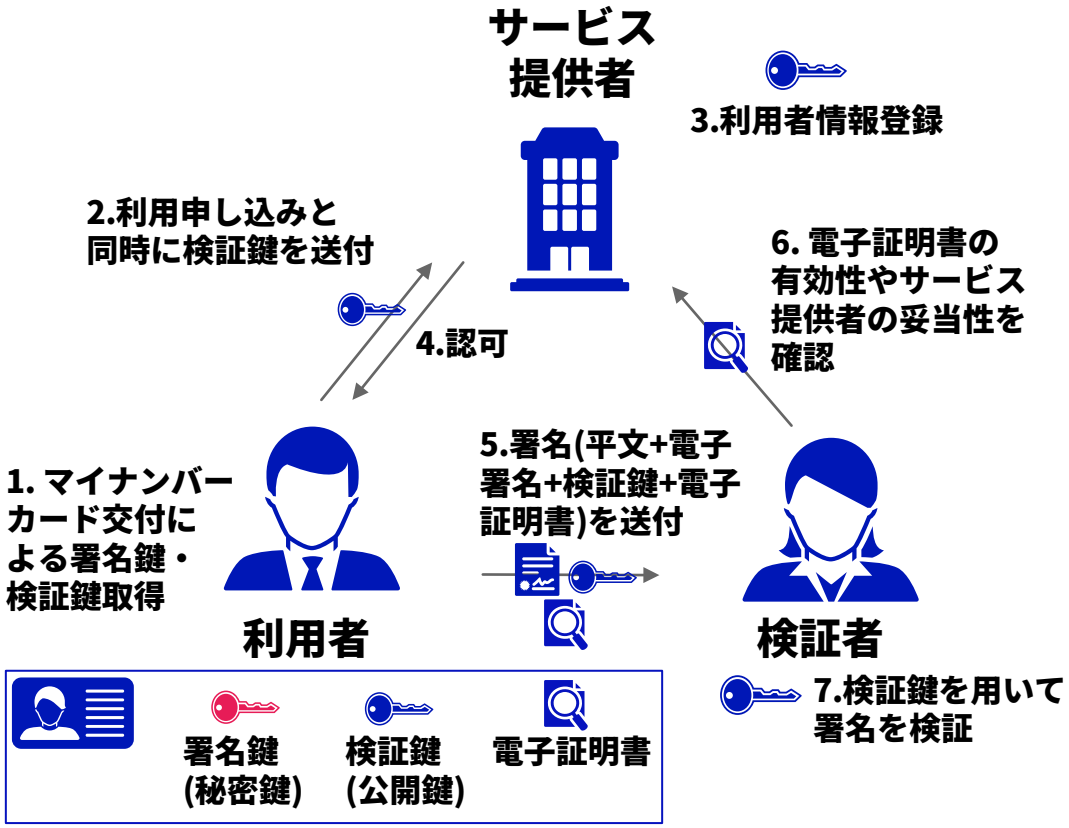
そもそも公的個人認証法施行規則の方法に統一する必要があるか（基準として公的個人認証法で認められている方法を追加するのは既定路線と見込まれる一方で、調査・監査の方法については未定の状況であるため）検討が必要
また、公的個人認証法で認められている方法を追加するとした場合、電子署名法の特定認証業務をどのように変更する必要があるか併せて検討

上記を踏まえ、ニーズの把握、運用への影響の観点で以下を議論

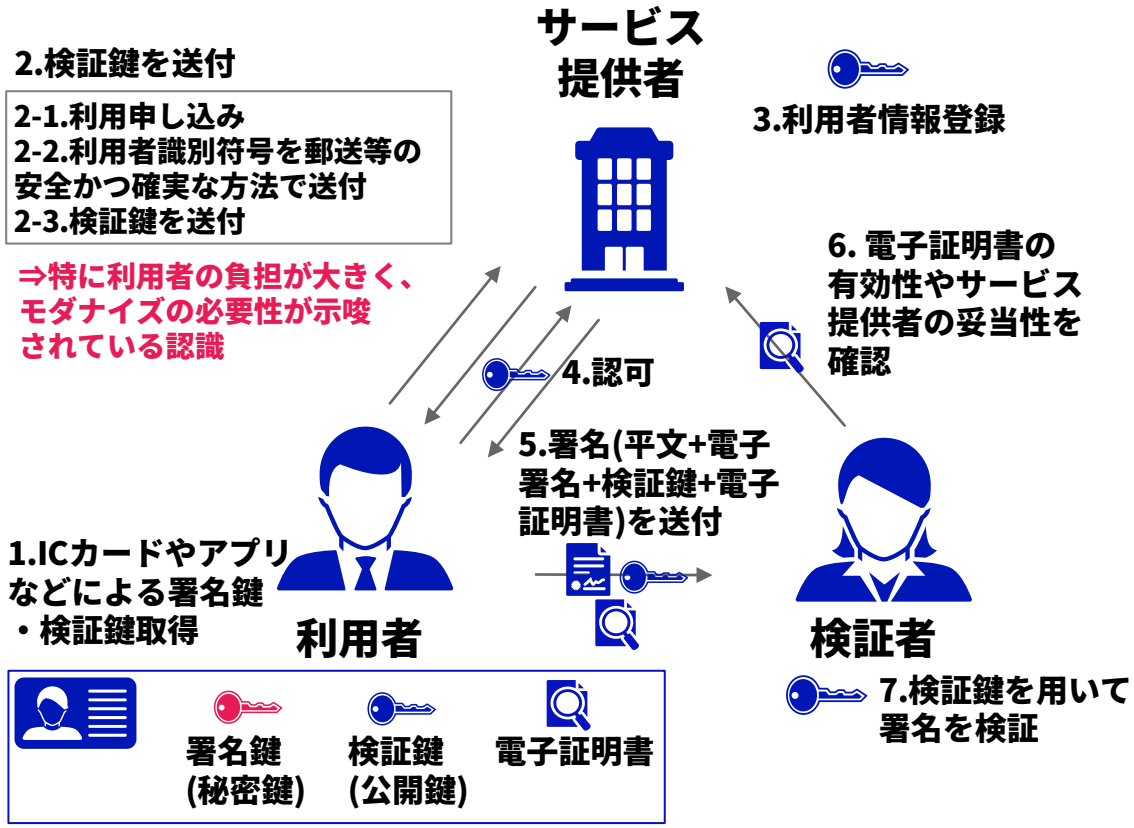
ニーズの把握	6-1	電子署名法の特定認証業務について、公的個人認証法施行規則において認められている方法に統一する必要があるか?
運用への影響	6-2	❻ のモダナイズを行う場合、電子署名法の特定認証業務をどのように変更する必要があるか?

公的個人認証サービスと電子署名法の認定認証事業に基づくサービスの違い

公的個人認証サービス
(マイナンバーカード交付後に利用を申し込む場合)



現行の電子署名法の認定サービス



(参考)施行規則第６条第３号の２改正の経緯

- 施行当初、利用者署名符号を認証事業者が作成する場合に、当該符号を安全かつ確実に利用者へ渡すことができるように、本人限定受取郵便を使用し、ICカード等を送付することを想定していた。
- 平成15年、認証業務が利用者の真偽確認を行った後に、当該利用者が自ら作成した鍵ペアのうち利用者署名検証符号を電気通信回線を通じて認証事業者に送信することで電子証明書が自動的に作成されるケースが見られるようなってきたため、このビジネスモデルを対象とするための認定基準を整備することとなった。
- 認定基準に必要な要件として、「公開鍵を送信した利用者の識別に係る要件」を以下のとおり定義。
  - 鍵ペアを自ら作成した利用者が電気通信回線を通じて認証事業者に公開鍵を送信したとしても、認証事業者が当該利用者を識別できなければ、電子証明書を作成することはできない。そこで、真偽確認が行われた利用者に対し、認証事業者がPIN（当該利用者の識別に必要な容易に類推されない符号）を付与し、当該利用者が公開鍵を送信する際に併せて利用者情報（利用者の氏名やID等）及びPINを送信し、認証事業者は当該利用者情報及びPINを識別することによって電子証明書を作成することになる。この場合、次の要件が必要となる。
    ① 認証事業者は利用者ごとにPINを作成すること。
    ② 認証事業者は真偽確認した利用者にPINを安全かつ確実に渡すこと。
    ③ PINは当該利用者以外の者が知り得ないようにすること。
- 上記経緯を踏まえ、前ページに記載されているように利用者識別符号を利用者から返させることで、利用者本人を識別し、電子証明書を作成することを認めるための規則改正が行われた。

(参考)施行規則の条文の比較

電子署名法施行規則

- 施行規則第６条第３号の２
利用者署名符号を利用者が作成する場合において、当該利用者識別符号に対応する利用者署名検証符号を認証事業者が電気通信回線を通じて受信する方法によるときは、あらかじめ、利用者識別符号（認証事業者において、一回に限り利用者の識別に用いる符号であって、容易に推測されないように作成されたものをいう。）を安全かつ確実に当該利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者の識別に用いるまでの間、当該利用者以外の者が知り得ないようにすること。

同義

公的個人認証法施行規則

- 施行規則第26条第５号
利用者署名符号を利用者が作成する場合において、当該利用者署名符号に対応する利用者署名検証符号（電子署名及び認証業務に関する法律施行規則第四条第一号に規定する利用者署名検証符号をいう。）を認定申請者が電気通信回線を通じて受信する方法によるときは、次に掲げる場合の区分に応じそれぞれ次に掲げるものであること。

イ　当該利用者から電子署名が行われた情報が送信される場合であって、当該利用者となるための申込み（令第八条第二号に規定する利用者となるための申込みをいう。第十五号及び第八十二条第二号において同じ。）の際に当該利用者署名検証符号を認定申請者に電気通信回線を通じて送信する場合当該電子署名により当該利用者の真偽の確認を行うこと。

ロ　イに該当しない場合あらかじめ、利用者識別符号（電子署名及び認証業務に関する法律施行規則第六条第三号の二に規定する利用者識別符号をいう。）を安全かつ確実に当該利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者の識別に用いるまでの間、当該利用者以外の者が知り得ないようにすること。

公的個人認証法と電子署名法の調査項目の違い

電子署名法の特定認証業務の内容

- 業務の用に供する設備の基準
  - 認証設備室への入出場を管理するために必要な措置
  - 認証業務用設備への不正なアクセス等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認証業務用設備の作動を防止するための措置等
  - 発行者署名符号の生成管理に使用する暗号装置
  - 認証業務用設備等の災害の被害を防止するために必要な措置
- 利用者の真偽の確認の方法
  - 認証業務の利用申込み等
  - 利用者の真偽の確認方法等
- その他の業務の方法
  - 利用申込者に対する説明事項
  - 利用申込書等の記載事項等
  - 利用者署名符号及び利用者識別符号の生成等
  - 電子証明書に係る事項
  - 認定認証業務と他の業務との誤認を防止するための措置
  - 電子証明書への属性の記録
  - 署名検証者への情報提供
  - 電子証明書の失効に係る事項
  - 認証業務の実施に関する規程
  - 認証業務の廃止
  - 電子証明書名義人への情報の開示
  - 認証業務実施のための組織及び体制等
  - 認証業務用設備の操作等に関する許諾等
  - 発行者署名符号の漏えいを防止するために必要な措置
- 帳簿書類
  - 認証業務利用申込に関する帳簿書類関係
  - 電子証明書の失効に関する帳簿書類関係
  - 認証事業者の組織管理に関する帳簿書類関係
  - 設備及び安全対策措置に関する帳簿書類関係

公的個人認証法の特定認証業務の調査項目※ ()で記載された項目を抽出

- 電子署名等確認設備室への入出場を管理するために必要な措置
- 電子署名等確認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電子署名等確認設備の作動を防止するための措置等
- 電子署名等確認設備等の災害を防止するために必要な措置
- 電子署名又は電子利用者証明の確認に係るその他の業務の方法
  - 情報の漏えい防止等のために必要な措置
  - 情報漏えいのおそれがある場合におけるデジタル庁及び総務省への報告
- 軽微な変更
- 変更の認定
- 署名利用者本人が電子署名を行ったことの確認のための措置
- 法第十八条第三項に規定する署名利用者の同意の方法等

電子署名等確認業務受託者（PF事業者）を希望する場合、以下も追加

- 電子署名又は電子利用者証明の確認に係るその他の業務の方法
  - 情報の漏えい防止等のために必要な措置
- 電子署名等確認業務の全部を委託する場合の特例

関連する調査項目についてはほぼ同様であり大きな差異は見当たらない

Source:JIPDEC「特定認証業務の認定に係る調査表」, 総務省「公的個人認証サービスにおける主務大臣認定に係る調査票」

❻ の論点詳細

観点	論点	論点詳細
ニーズの把握	6-1 電子署名法の特定認証業務について、公的個人認証法施行規則において認められている方法に統一する必要があるか?	• P24で整理した通り、 特に利用者から検証鍵を送る前に利用者識別符号を郵送等で送付しなければならないため負担が大きく、モダナイズの必要性が示唆されているという理解でよいか。 • 公的個人認証法で認められている方法を追加することについて懸念はあるか。
要件の明確化	6-2 ❻ のモダナイズを行う場合、電子署名法の特定認証業務をどのように変更する必要があるか?	• 認定基準の統一(利用者が鍵ペア―を作成する場合の検証鍵の送付要件の修正)に伴い、申込に付される電子署名について基準を設ける必要はないか。また、他に認定基準として設けるべき事項はないか。 • 電子署名法の認定に係る調査方法、監査方法等を実施する際に確認するべき事項は何か。また、どのような方法があるか。

今後の進め方について

検討会のアジェンダ		実施時期
第1回	• 検討会の目的と議論内容、各アジェンダの説明 • モダナイズの方向性 ❶・❷ に関する議論	2024年9月20日(済)
第2回	• 第1回の議論内容の振り返り • モダナイズの方向性 ❸～❻ に関する議論	2024年11月1日
第3回	• 残論点の追加議論	2024年11月26日
第4回	• 報告書を基にした検討内容の振り返り	2024年12月前半

デジタル庁

Digital Agency