電子署名法認定基準のモダナイズに関する検討会 第一回

検討会の方針及びモダナイズの方向性に関する議論

2024-09-20　　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1回検討会の位置づけ

電子署名法及び昨年度実施された「電子署名法令上の基準のモダナイズの検討」の内容を振り返りつつ、**本検討会のゴールと検討方針について認識を合わせることを目的**とする

また、本年度事業の議論対象である以下6つのモダナイズの方向性の内、❶ と ❷ について**議論**を進める(詳細の議論内容については後述)

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

第一回検討会資料の目次

電子署名法について

電磁的記録の真正性/特定認証業務の認定制度化を目的に制定

■経緯：電子署名及び認証業務に関する法律（以下「電子署名法」又は紛れが無い場合は単に「法」という。）は、平成12年5月31日に公布、
平成13年4月1日に施行

■目的：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

■主務省庁：デジタル庁・法務省
総務省、経産省、法務省の共管として制定したが、総務省、経産省所管部分をデジタル庁へ移管

電子署名法の概要

■ 電子署名の定義（第２条）

- 電磁的記録に記録することができる情報について行われる措置であって、次のいずれにも該当するもの
  - ➢ 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること（本人性）
  - ➢ 当該情報について改変が行われていないかどうかを確認することができるものであること（非改竄性）

■ 電磁的記録の真正な成立の推定（第３条）

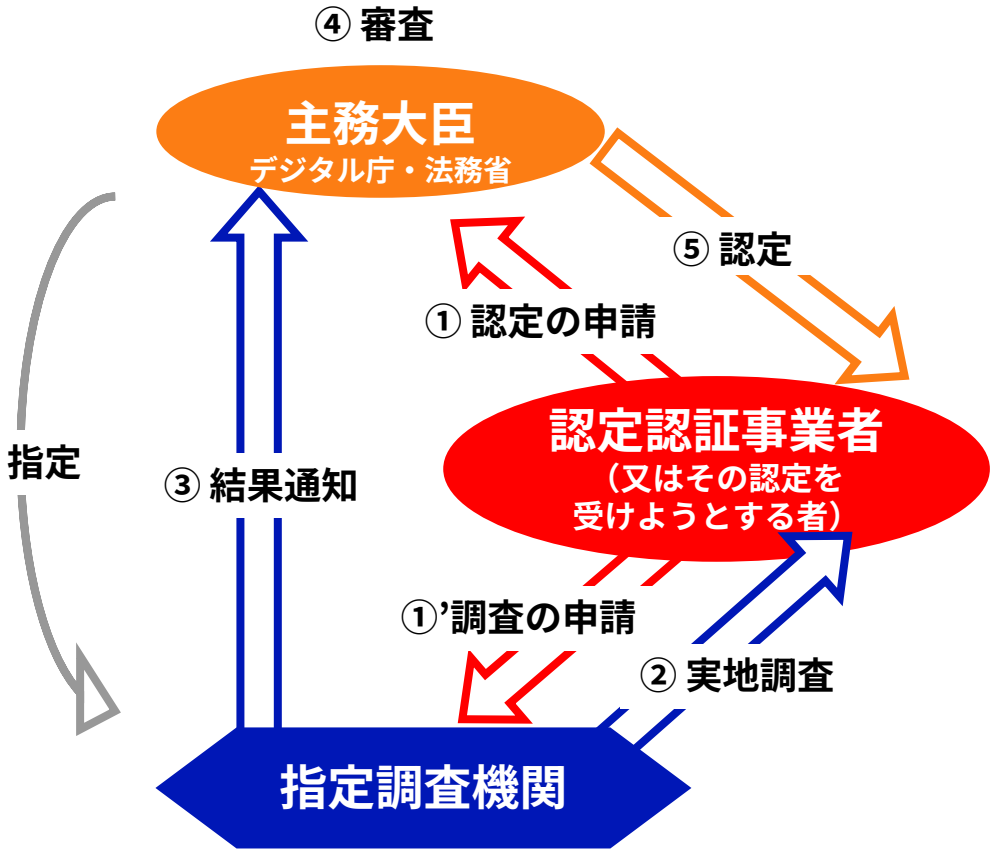
- 本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われている電磁的記録は、真正性を推定

■ 特定認証業務の認定（第４条）

- 法令に定める技術基準等を満たす特定認証業務（※）について、主務大臣による認定制度を実施
  - ➢ 業許可や規制ではない

（※）使用している暗号アルゴリズムがRSA2048bit以上等の安全性を有するもの

（参考）認定認証業務の概要



指定調査機関：一般財団法人 日本情報経済社会推進協会（JIPDEC）

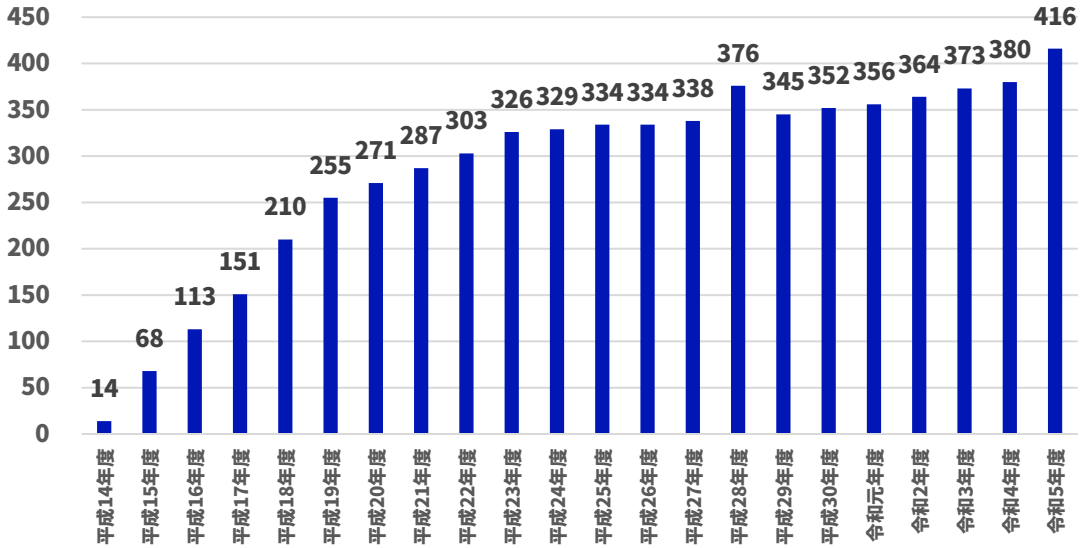
認定の有効期間は１年間。

認定認証事業者：７事業者（９業務）

（令和6年8月31日時点）

- セコムトラストシステムズ（株）
- （株）トインクス
- （株）帝国データバンク
- NTTビジネスソリューションズ（株）（２業務）
- 三菱電機インフォメーションネットワーク（株）（２業務）
- 日本電子認証（株）
- my FinTech（株）

認定認証業務　電子証明書有効枚数（千枚）



電子署名法に基づく政省令等

政省令等において、認定基準や調査方針等の具体を規定

項番	政省令名	概要
1	電子署名及び認証業務に関する法律施行令	4条から構成され、業務の認定や指定調査機関の指定の有効期間、認定申請に係る手数料の額と認可について定める政令
2	電子署名及び認証業務に関する法律施行規則（以下「施行規則」という。）	法第6条から第11条までの規定等に基づき、認定基準等について定めた命令
3	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等に関する省令	指定調査機関等の調査に必要な事項等について定めた命令
4	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「指針」という。）	14条から構成され、施行規則をより詳細化し、認定基準の細目を定めた告示
5	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「方針」という。）	指定調査機関の調査方針を明確化し、認定制度の円滑な運営を資するための通知

昨年度事業の振り返り

規制/技術の変遷によるニーズの変化へ対応することが目的

電子署名法に求められるモダナイズの課題 (規制/技術の変遷による影響、R4年度報告書より)

情報セキュリティに関するリスクマネジメントの概念がないこと

認証局の秘密鍵を管理する暗号装置(HSM) に関する技術基準が20年以上前の米国基準のままであること

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が認められていないこと

利用者の真偽の確認における自動化が認められていないこと

リモート署名に関する規定がないこと

マルウェア対策に関する規定がないこと

R5年度にて示されたモダナイズの方向性

1. 国際基準に照らし合わせた情報セキュリティに関するリスクマネジメントの規定
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
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
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
5. 利用者の真偽の確認における自動化の規定
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

R5年度事業の振り返り(1/3)

モダナイズの方向性	R4年度報告書のポイント	課題のポイント	R5年度事業の検討結果
❶国際基準に照らし合わせた情報セキュリティに関するリスクマネジメントの規定	信頼性を確保するために国際基準に照らし合わせた規定は必要だが、更なる設備投資と更新調査費の増大は懸念材料	国際的な基準に照らすと、EUにおけるETSI EN 319 401トラストサービスプロバイダの一般ポリシー要件、先般発行されたISO/IEC 27099公開鍵基盤の実践と方針において、情報セキュリティのリスクマネジメントが必須となっている	（案１）法第６条及び施行規則第６条にリスクマネジメントについての条項を追加 （案２）リスクマネジメントが電子署名法第６条第３号に含まれるものとして施行規則・方針を改正 • （案２-１）施行規則・方針の改正 - 施行規則第6条に、リスクマネジメントの条項を追加 - 方針第4.8に、リスクマネジメントの要件を追加 • （案２-２）方針のみの改正 - 方針第4.8に、リスクマネジメントの要件を追加
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	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を検討する必要がある	暗号装置（HSM）に関する技術基準が、20年以上前の米国の基準であるFIPS 140-1の規定と同等のままとなっており、国際的な水準を満たさない状況にある	方針第2.2を、FIPS140-2及びISO/IEC15408に言及する規定に置き替え、方針第2.2(2)に相当する内容（暗号装置と同等の安全性を満たすセキュリティ対策）は削除

R5年度事業の振り返り(2/3)

モダナイズの方向性	R4年度報告書のポイント	課題のポイント	R5年度事業の検討結果
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	認証設備室の外からの遠隔操作については、認証業務用設備の危機的な設定変更等を除き、十分なセキュリティ対策を条件とした上で認められるよう検討する必要がある	発行者署名符号を、認証設備室の外において保管及び使用できるか、という点が主たる論点である。施行規則第６条第17号及び指針第14条第１号に発行者署名符号は認証設備室内で行う旨の規定が置かれている	施行規則第４条第４号（発行者署名符号の生成・管理）に係る方針第2.2の改正が必要となる。具体的には、例えば、クラウドHSMに関する規定を(2)として追加する。ただし、ネットワークを介したHSMの利用の可否については、なお慎重な検討が必要
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	帳簿書類に関するデータファイル管理のためのサーバや、認証局特定に要するフィンガープリントのデータ公開のためのWebサーバについて、パブリッククラウドサービス等の利用が認められるよう検討する必要がある	特定認証業務における電気通信回線経由の遠隔操作やパブリッククラウドサービスの利用による業務改善については、施行規則第６条第15号へ、指針第６条第１項第３号及び第10条第２号によって、基準に適合しないと解釈される	設備のパブリッククラウドを許容する文言を、指針第４条第２号（登録用端末設備、利用者識別設備）、指針第５条（認証業務用設備への不正アクセス防止等）、指針第６条第１項第２号（認証業務用設備の自動作動）及び同項第３号（遠隔操作防止）に追加する

R5年度事業の振り返り(3/3)

モダナイズの方向性	R4年度報告書のポイント	課題のポイント	R5年度事業の検討結果
❺利用者の真偽の確認における自動化の規定	自動化することにより、真偽確認ミスによる誤発行リスクが軽減でき、業務負荷軽減やテレワーク導入にもつながる 「利用者の真偽の確認における自動化の規定」は必要	帳簿等の保存に際して、認定認証事業者の利用者の真偽の確認に係る要員の識別に関する情報が、人を介さない利用者の真偽の確認は認められないと解釈されてきている	方針第6.1(１)及び(２)について、システムによる自動的な受領及び実施を許容していることを明示する文言に修正する。例えば、「者」を「者（電子計算機により自動的に受領される場合にはその旨）」に変更する
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	電子署名法と公的個人認証法で取り得る手段に差異がある状態は是正が必要	施行規則第６条第３号の２（利用者署名符号の利用者からの送信における、利用者識別符号による利用者確認）については、公的個人認証法施行規則第26条第５号イにおいて認められている方法を追加すべきではないか	施行規則第６条３号の２を同号イと口に書き分け、同号イとして電子署名による方法を追加する

本検討会における検討の方針と内容

今までの検討を踏まえ、実行に向けた方針を具体化することがゴール

課題の洗い出し

令和4年度事業にて以下2つの必要性が示唆
- リモート電子署名の認定基準の策定
- 電子署名法認定基準のモダナイズの必要性

課題解決方法の検討

令和5年度事業の成果
- リモート電子署名の認定基準案と電子署名法認定基準のモダナイズ案を作成

本年度認定基準のモダナイズに関する検討会を開催し、**課題解決方法に関する裏付けを取りつつ施策の実行に向けた方針を具体化すること**がゴール

具体的には、令和５年度事業の成果を踏まえ、６つのモダナイズの方向性についてニーズの把握や要件の明確化、運用への影響度合いの観点から議論

施策の実行

本検討会での議論において、速やかに対応することとされたものは、令和７年４月１日施行を目指す
引き続き検討が必要な内容は来年度以降も検討を継続

モダナイズの実効性向上のため、ニーズの把握や要件の明確化、運用への影響の観点から議論

ニーズの把握：モダナイズ実行の必要性の明確化

要件の明確化：モダナイズに必要な運用や技術要件を整理
※法令解釈についての整理も含む

運用への影響：モダナイズ後の調査への影響度合いを議論

方針を合わせたうえで各課題を検討し、最後に結果をとりまとめ

大枠の進めかた

- 検討会の目的と議論内容、各アジェンダを説明した上で、各モダナイズの方向性に対するニーズや要件、運用への影響度合いの観点から議論
- 最後に議論した内容の総括を検討会報告書としてまとめ、内容に齟齬がないかを検討会にて確認

検討会のアジェンダと実施時期

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	令和6年9月20日
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	令和6年11月上旬
第3回	• 残論点の追加議論（予備日）	令和6年11月下旬
第4回	• 報告書を基にした検討内容の振り返り	令和6年12月頃

モダナイズの方向性 ❶ と ❷ に関する議論

❶ 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

国際的基準に照らすと、情報セキュリティのリスクマネジメントが必須となっている中、特定認証業務の認定に係る基準においても、**情報セキュリティに係るリスクを評価し、適切な管理策を実施するマネジメントシステムの概念を盛り込むべき**

各認証事業者自身がアセスメントをし、各認証事業者自身がその結果に基づいた対策を実施することが必要

それを受けた本検討会での議論の方針

危機管理等の観点により、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は現行規定においても存在するとも考えられるが、この点を議論する

他制度との整合も踏まえつつ、リスクマネジメントの基準として規定すべき内容を整理する

要件の明確化

1-1 法解釈上、**リスクマネジメントが法第６条第１項第３号が委任する範囲に含まれるか?**

1-2 事業者に求めるリスクマネジメントに係る基準としてどのような内容を盛り込むべきか?

現行の施行規則等において、危機管理に関する規定は既に存在

関連法令・ 政省令	内容(青太字が議論のポイントに関わる箇所。分かりやすさ等の観点で、一部を省略)
法第６条第１項第３号	…次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。 一 申請に係る業務の用に供する設備が主務省令で定める基準に適合するものであること。 二 …利用者の真偽の確認が主務省令で定める方法により行われるものであること。 三 前号に掲げるもののほか、申請に係る業務が主務省令で定める基準に適合する方法により行われるものであること。
施行規則第6条第1項	十三 認証事業者の連絡先、業務の提供条件その他の認証業務の実施に関する規程を適切に定め…利用者その他の者が当該規程を容易に閲覧することができるようにすること。 十五 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 ト 危機管理に関する事項
指針第12条第1項第7号	…認証業務の実施に関する規程は、次の各号に掲げる事項に関する規定を含むこと…。 七 認証業務に係るセキュリティに関する事項（利用者に係る個人情報の取扱い…を含む。）
方針第4 8.(3)	規則第６条第15号トに規定する「危機管理に関する事項」とは、発行者署名符号の危殆化又は災害等による障害の発生に対する対応策及び回復手順であって、以下の事項を含む…。
方針第5 (4)	…「認証業務に係るセキュリティに関する事項（利用者に係る個人情報の取扱い…を含む。）」には、当該認証業務が採用しているセキュリティ基準、技術標準等に関する事項が含まれる…。

(参考) 法第６条第１項第３号の趣旨等について

法第６条第１項第３号の趣旨

- 法第６条第１項では、特定認証業務の認定要件として、業務の用に供する設備に関する基準（同項第１号）、利用者の真偽の確認方法に関する基準（同項第２号）に加え、その他の業務の方法に関する基準（同項第３号）を定めている。

現行施行規則第６条の規定内容

現行施行規則第６条では、法第６条第１項第３号の規定に基づき、以下のような内容を定めている。

- 利用申込者の意思確認のために必要な重要事項の説明、電子証明書の送信等
- 利用者署名符号の適切な作成や管理
- 有効期間、記録事項、失効確認等、電子証明書の適切な発行や管理
- 業務手順、指揮命令系統、業務監査、危機管理等、業務の適切な実施
- 認証業務用設備が設置された部屋への入退室の管理
- 発行者署名符号の漏えい防止　　等

ETSIは標準規格上で、TSPにリスクのアセスメント/評価/軽減措置/定期的な見直し/文書化と記録を要求

EN 319 401とは

欧州電気通信標準化機構(ETSI)が策定した信頼サービスプロバイダ(Trust Service Providers, TSP)に関する標準規格

これはETSIの「電子署名及びインフラストラクチャー(Electronic Signatures and Infrastructures, ESI)」の枠組みに基づいており、**特に信頼サービスプロバイダのリスクアセスメントなどの基本的な要件を規定**

EN 319 401におけるリスクアセスメントの定義

実施項目	内容
リスクアセスメント	提供する信頼サービスに関連するリスクを特定し、それを評価するために、サービスの特性や運用環境に応じて適切にリスクアセスメントを実施しなければならない
リスク評価	特定されたリスクがサービスのセキュリティや信頼性にどの程度影響を与えるかを評価し、その深刻度を判断しなければならない
軽減措置	評価されたリスクに対して、TSPはリスクを軽減するための適切な措置(リスクの受容、回避、低減、転嫁)を実施しなければならない
定期的な見直し	アセスメント結果は定期的に見直され、必要に応じて更新しなければならない
文書化と記録	結果や関連する対策は文書化され、適切に記録しなければならない

Source:欧州電気通信標準化機構「EN 319 401 V3.1.1」

(参考) ETSI EN 319 401 V3.1.1の原文

5 Risk Assessment

- REQ-5-01: The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.
- REQ-5-02: The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.
  - NOTE: See ISO/IEC 27005:2022 [i.12] for guidance on information security risk management as part of an information security management system.
- REQ-5-03: The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).
- REQ-5-04: The risk assessment shall be regularly reviewed and revised.
- REQ-5-05: The TSP's management shall approve the risk assessment and accept the residual risk identified.

Source:欧州電気通信標準化機構「EN 319 401 V3.1.1」

❶ の論点まとめ

観点	論点	論点詳細
要件の明確化	1-1 法解釈上、**リスクマネジメントが法第６条第１項第３号が委任する範囲に含まれるか?**	• 法第６条第１項第３号の規定に基づき、施行規則第６条第１項第15号トに「危機管理に関する事項」が規定されていることを踏まえれば、**情報セキュリティに係るリスクマネジメントは法委任の範囲に含まれると解してよいか?** • 施行規則の**「危機管理に関する事項」について、リスクマネジメントの意味を含むものとして解釈できるか?**
	1-2 事業者に求めるリスクマネジメントに係る基準としてどのような内容を盛り込むべきか?	• ETSIは標準規格上で事業者に**リスクのアセスメント/評価/軽減措置/定期的な見直し/文書化と記録を要求しているが、電子署名法に取り込むべき項目は何か?** • 上記以外に盛り込むべき内容はあるか?また、ある場合はその理由は?

❷ 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

暗号装置（HSM）に関する技術基準が20年以上前の米国の基準と同等のままとなっているため、現行の方針をFIPS140-2及びISO/IEC15408に言及する規定に置き換える必要がある

それを受けた本検討会での議論の方針

FIPS140-2への更新であれば、暗号基準の更新を行うこと自体には、新規参入の障壁にならないと思われるが、FIPS140-2、FIPS140-3いずれの内容に合わせるべきか、FIPS140シリーズの変遷を踏まえ検討する

上記を踏まえ、要件の明確化、運用への影響の観点で以下を議論

要件の明確化	2-1	FIPS140シリーズの変遷を踏まえどのようなタイミング/内容でモダナイズを実施するべきか?
運用への影響	2-2	モダナイズによる特定認証業務への影響はどのようなものがあるか?

❷ に関する補足資料:FIPS140シリーズの変遷について

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2度改訂

FIPS140シリーズの概要

米国国立標準技術研究所（NIST）が発行した暗号モジュールのセキュリティ要件を定めた米国の標準規格

特に政府機関や防衛産業での使用を前提にしており、様々なレベルのセキュリティを確保するための基準を提供

FIPS140シリーズの変遷

	概要	問題点
FIPS140-1 平成6年	4つのセキュリティレベルを提供しており、それぞれが異なるセキュリティの強度を要求	• セキュリティ機能の限界による危殆化:急速に進化するハードウェアやソフトウェア技術、新しい攻撃手法への対応が不十分かつ、役割ベースの認証や自己テストなど、後に必要とされたより高度なセキュリティ機能が欠如しておりリスクが内包
FIPS140-2 平成13年	乱数生成器のテスト要件の変更や物理的セキュリティの一般要件の追加、セキュリティポリシーの明確な記述の要求等が更新され、技術的及び実施面で改善	• 認定のHistorical List入り:令和8年9月22日以降、FIPS 140-2の全ての認定が「Historical List」に移行(FIPS 140-2認定製品が現行の基準として扱われず、非推奨となることを意味)
FIPS140-3 平成31年	技術の進化に伴う様々な形式への対応やセキュリティ要件の強化を目的にモジュールの形式を拡張しつつ物理的セキュリティ要件やテスト要件等を強化	• FIPS140-3認定製品の状況:机上調査によれば、今年に入ってからFIPS140-3準拠の認定を受けた製品が一定程度増加したものの、一部のプロバイダに限られるため、FIPS140-2に比べれば1/6程度の製品数に留まる。このため、移行と普及には一定の期間を要する可能性あり

Source: 米国国立標準技術研究所「FIPS 140-1, 2, 3」

❷ の論点詳細

観点	論点	論点詳細
要件の明確化	2-1 FIPS140シリーズの変遷を踏まえどのようなタイミング/内容でモダナイズを実施するべきか?	• 早々(例えば令和7年4月1日施行)にFIPS140-2又はFIPS140-3に合わせた暗号基準へ更新すべきか? - FIPS140-2に合わせた場合、令和8年9月にHistorical List入りするためその前にFIPS140-3に合わせた基準への更新が必要か？ - FIPS140-3に合わせた場合、FIPS 140-3準拠の認定を受けた製品が必ずしも多いとは言えない状況のため、同製品の普及状況とのミスマッチを避ける観点から移行期間を設けるべきか？
運用への影響	2-2 モダナイズによる特定認証業務への影響はどのようなものがあるか?	• FIPS140-2に合わせた暗号基準にした場合、特定認証業務への影響はどのようなものが考えられるか? - 現行の基準との差分内容として、乱数生成器のテスト要件の変更や物理的セキュリティの要件、セキュリティポリシーの明確などがあり • FIPS140-3に合わせた暗号基準にした場合に、特定認証業務への影響はどのようなものが考えられるか? - 現行の基準との差分内容として、物理的セキュリティ要件やテスト要件の強化があり

今後のワークプラン

	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	令和6年9月20日
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	令和6年11月上旬
第3回	• 残論点の追加議論（予備日）	令和6年11月下旬
第4回	• 報告書を基にした検討内容の振り返り	令和6年12月頃

デジタル庁

Digital Agency