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 第三回

モダナイズの方向性に関する追加議論

2024-11-26　　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

第三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、モダナイズの方向性 ❸ ～ ❻について議論
- 今回の検討会では、モダナイズの方向性 ❶ ❷ ❸ ❹ ❻ の残論点について議論

※議論は、❶→❷→❻→❸→❹ の順に実施する予定。

第三回検討会の目次

これまでの検討会の振り返り

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相当以上とし、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

第二回検討会の振り返り

❺は明確化のための規定を設ける方向を確認。 ❸はセキュリティ上の懸念から現時点では実現が困難。❹はクラウド利用等を認める対象やその要件、❻は利用申込と利用者署名検証符号の紐づけの確認方法等、の検討がそれぞれ必要

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
モダナイズの方向性 ❸	クラウドHSMの利用許容と課題について、ニーズやメリット、セキュリティ懸念、調査・審査の難しさを議論	• クラウドHSM利用のニーズは一部あるものの必ずしも高いわけではなく、また、パブリッククラウドサービスに対する調査・審査に関するハードルや、認定認証業務のルートに求める鍵管理のレベル等の問題から現時点での実現は困難と考えられる • クラウドHSMのニーズや上記のセキュリティ上の懸念について、継続的な調査と検討が必要 →第三回では、プライベートクラウド及びネットワーク型HSMに関する観点のみ議論
モダナイズの方向性 ❹	認証局のクラウド利用・遠隔操作の範囲と要件について、設備ごとのニーズやセキュリティ確保、調査方法を議論	• Aは、可用性が求められるが、その他のリスクについては限定的であり、実現の可能性が高い • B、C、Dのクラウド移行においては、現行調査基準と他のセキュリティ認証制度基準の項目等を踏まえた要件整理が必要 ※A～Dの分類については、P38参照
モダナイズの方向性 ❺	マイナンバーカードを用いた利用者真偽確認の自動化について、メリット、規定の明確化、懸念点を議論	• 利用者真偽確認の自動化について、明確化のための規定を設ける • 本人確認ガイドラインとの整合性や、自動化によるリスクへの配慮に係るコメントあり
モダナイズの方向性 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を確認し、規定変更やセキュリティ影響を議論	• 公的個人認証法において認められている方法を、電子署名法においても認める方向で検討すべき • これにあたり、利用申込と利用者署名検証符号の紐づけの確認方法の検討・整理が必要

モダナイズの方向性 ❶ に関する議論

❶ の本検討会での議論の方針

第一回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?

議論の結果

- 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

本検討会での追加議論内容

要件の明確化

1-3 組織全体のガバナンスとして盛り込むべき基準は何か?

(参考) 各標準/規格の目次一覧

※青字はガバナンスに関する部分

ISO/IEC 27001

1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 組織の状況
5. リーダーシップ
6. 計画策定
7. 支援
8. 運用
9. パフォーマンス評価
10. 改善

システム管理基準

- ITガバナンス編
  1. ITガバナンスの実践
  2. ITガバナンス実践に必要な要件
- ITマネジメント編
  1. 推進・管理体制
  2. プロジェクト管理
  3. 企画プロセス
  4. 開発プロセス
  5. 運用プロセス
  6. 保守プロセス
  7. 廃棄プロセス
  8. 外部サービス管理
  9. 事業継続管理
  10. 人的資源管理

ETSI EN 319 401

- 適用範囲
- 参照
- 用語、記号、省略語および表記の定義
- 概要
- リスクアセスメント
- 方針と実務
- TSPの管理と運営

NIST SP800-53

- サイバーセキュリティフレームワークの概要
- CSFコアの紹介
  - GOVERN
- CSFプロファイルとティアの紹介
- CSFを補完するオンラインリソースの紹介
- サイバーセキュリティリスクのコミュニケーションと統合の改善

ISMAP管理基準

1.
   - ISMAP 管理基準の目的
   - 基準の特質
   - 用語及び定義
2.
   - 管理基準の構成
   - 言明書に記載すべき内容
3. ガバナンス基準
   - 情報セキュリティガバナンスのプロセス
4. マネジメント基準
5. 管理策基準

Source: 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」

各標準/規格におけるガバナンスに関する基準

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

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

ISO/IEC 27001

- 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

システム管理基準

- 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

EN 319 401

- 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

SP800-53

- 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

ISMAP管理基準

- 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

次ページ以降の概要を参考に、認定事業者等に対して最低限要求すべき事項を整理する観点で各標準/規格を整理すると、少なくとも**「責任や権限の明確化」**及び**「情報セキュリティに係るリスクの評価と対応」**の**2点は共通項**であると言えるのではないか。

(参考) ISO/IEC 27001で規定された要求事項のうちガバナンスに関連する事項

※青字は共通項

運用	運用の計画策定及び管理	IT戦略ビジョンを経営戦略とビジネスモデルに基づき策定し、全体に周知し、新技術の影響を定期的に評価して見直すこと
		変更の影響を評価・管理し、アウトソーシングされたプロセスも含め統制すること
	情報セキュリティリスクアセスメント	定期的および重大な変更時に情報セキュリティリスク評価を実施し、結果を文書化すること
	情報セキュリティリスク対応	リスク処理計画を実施し、結果を文書化して保持すること
パフォーマンス評価	監視、測定、分析及び評価	情報セキュリティのパフォーマンスと有効性を監視・評価し、結果を証拠として文書化すること
	内部監査	情報セキュリティ管理システムの適合性と有効性を確認するため、定期的に内部監査を実施し、結果を文書化・報告すること
	マネジメントレビュー	経営層は情報セキュリティ管理システムの適合性と有効性を確認し、改善事項を決定し文書化すること
改善	継続的改善	不適合発生時に適切な是正措置を実施し、その結果を文書化すること
	不適合及び是正処置	情報セキュリティ管理システムの適合性と有効性を継続的に改善すること

Source: 日本規格協会「JIS Q 27001（ISO/IEC 27001）」

❶ に関する補足資料:参考標準規格

(参考)システム管理基準におけるガバナンスに関する基準

※青字は共通項

ITガバナンスの実践	経営戦略とビジネスモデルの確認	情報セキュリティ要件を満たすためのプロセスを計画・実施し、必要な文書を保持すること
	IT戦略の策定	取締役会の意図を反映したIT戦略を策定し、デジタル活用能力や技術陳腐化対策を含む目標を設定し、適切なITガバナンス方針を示すこと
	効果的なITパフォーマンスの確認と是正	ITパフォーマンスを管理し、取締役会の期待に沿ったコンプライアンスとリスク報告体制を確立し、必要に応じて是正措置を指示すること
	実行責任及び説明責任の明確化	ITガバナンスにおける最終責任が取締役会にあることを明確にし、権限委譲があっても取締役会が説明責任を果たし、IT戦略ビジョンを外部に開示すること
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	ステークホルダーのニーズに沿ったITガバナンスを実践し、満足度評価と良好な関係を構築すること
	取締役会等のリーダーシップ	取締役会が倫理規範と変革のリーダーシップを発揮し、IT知識を向上させつつ新技術対応を推進すること
	データ利活用と意思決定	データ利活用の方針を組織全体に周知し、データ品質や法規制遵守、リスク管理体制を整えること
	リスクの評価と対応	ITリスクを認識し、迅速に対応する管理体制と事業継続方針を整備し、ITサービスのレジリエンスを確保すること
	社会的責任と持続性	IT意思決定の透明性を確保し、ステークホルダーや環境への責任を果たし、倫理的なITシステム活用を行うこと

Source: 経済産業省「システム管理基準」

(参考) EN 319 401におけるガバナンスに関する基準

※青字は共通項

TSPの管理と運営	内部組織	TSPは信頼性があり、公平で、アクセス可能な運営体制を確保し、財政的・法的な責任を果たすとともに、苦情対応と競合職務の分離により信頼サービスの安定性を維持すること
	人的資源	TSPはセキュリティポリシーに従う適切な専門知識を持つスタッフを確保し、責任者の配置や適切な訓練、必要な懲戒手続を整えること
	資産管理	TSPは情報資産を含む全ての資産を保護し、インベントリの作成と分類を行い、適切な管理体制を維持すること
	アクセス制御	TSPシステムのアクセスを許可された者に限定し、特権アカウントには強力な認証手続きを適用すること
	暗号制御	暗号鍵、アルゴリズム、デバイスのライフサイクルを通じたセキュリティ管理を確立すること
	物理的および環境的なセキュリティ	TSPシステムへの物理的アクセスを制限し、リスクを最小限に抑える管理を行うこと
	運用セキュリティ	信頼性の高いシステムと変更管理手続きを用い、プロセスの技術的なセキュリティを維持すること
	ネットワークセキュリティ	TSPはネットワークとシステムを保護し、リスク評価に基づきネットワークの分割を行うこと
	脆弱性およびインシデント管理	継続的なモニタリングとログ管理によりインシデント検出と対応体制を整備し、重大なインシデントは24時間以内に報告すること
	証拠の収集	法的手続やサービス継続のために、関連データを適切な期間保持すること
	事業継続管理	災害時に発動する継続計画とバックアップ体制を確立し、リスクに応じた資源を維持すること
	TSPの終了と終了計画	サービス終了時に利用者への影響を最小限に抑える計画を策定し、必要な情報を維持すること
	コンプライアンス	TSPは合法かつ信頼できる方法で運営し、障がい者対応を考慮した信頼サービスを提供すること
	サプライチェーン	サプライチェーンに伴うセキュリティリスクに対応する手続と、ICT製品やサービス取得に適用される情報セキュリティ要件を定義すること

Source: ETSI「EN 319 401 - V3.1.1」

❶ に関する補足資料:参考標準規格

(参考) NIST SP800-53におけるガバナンスに関する基準

※青字は共通項

GOVERN	組織のコンテキスト	組織は使命、ステークホルダーの期待、依存関係、法的・規制的・契約上の要件を理解し、サイバーセキュリティリスク管理の意思決定に反映すること
	リスク管理戦略	組織の優先事項、リスク許容度、リスク対応方針、リスク管理手法を明確にし、サイバーセキュリティリスク管理を組織全体で支援すること
	役割、責任、および権限	サイバーセキュリティに関する責任をリーダーシップに持たせ、役割や権限を明確にし、パフォーマンス評価と継続的改善を推進すること
	ポリシー	サイバーセキュリティリスク管理のためのポリシーを確立し、組織の状況と戦略に基づき伝達・施行し、定期的に見直すこと
	監督	サイバーセキュリティリスク管理戦略の活動と結果をレビューし、リスク管理の方向性と戦略の調整に活用すること
	サイバーセキュリティサプライチェーンリスク管理	供給チェーンのサイバーセキュリティリスクを管理するためのプロセスを確立し、リスク評価と対応を供給業者や関連第三者との契約に統合し、関係のライフサイクル全体でパフォーマンスを監視すること

Source: 米国国立標準技術研究所「The NIST Cybersecurity Framework (CSF) 2.0」

(参考) ISMAP管理基準におけるガバナンスに関する基準

※青字は共通項

情報セキュリティガバナンスのプロセス	概要	経営陣は、情報セキュリティを統治するため、評価、指示、モニタ、コミュニケーション、保証の各プロセスを実施し、客観的な意見を得て統治の適切性を確保すること
	評価	経営陣は、情報セキュリティの目的達成度を考慮し、必要な調整を行い、事業の取り組みへのサポートや新規プロジェクトへの対応を確実にすること
	指示	経営陣は、情報セキュリティの目的と戦略を承認し、リスク選好を定め、資源配分と活動の優先順位付けを行い、情報セキュリティ文化を推進すること
	モニタ	経営陣は、情報セキュリティの活動の有効性を評価し、法規制や環境変化に対応し、新規開発案件の影響を考慮して、必要な監視と調整を行うこと
	コミュニケーション	経営陣は、利害関係者との双方向の情報交換を通じて、組織の情報セキュリティのレベルを報告し、課題や決定に基づく行動を説明すること
	保証	経営陣は、独立した監査やレビューを委託し、情報セキュリティ活動の妥当性を検証し、要求される水準に対する説明責任を果たすこと

Source: ISMAP運営委員会「ISMAP管理基準」

❶ の論点詳細

観点	論点	論点詳細
要件の明確化	1-1 組織全体のガバナンスとして盛り込むべき基準は何か?	• 組織全体のガバナンスとして、「責任や権限の明確化」及び「情報セキュリティに係るリスクの評価と対応」の２点は必要な事項だと考えられるが、そのほかに要求すべき事項はあるか。 • 「責任や権限の明確化」について、施行規則第６条第１５号ロにおいて業務に従事する者の責任及び権限並びに指揮命令系統を適切に定め業務を実施することを求めているが、これに加えて、更に取締役会等に関する「責任や権限の明確化」（ITガバナンス）に関する規定を設ける必要があるか。 • 「情報セキュリティに係るリスクの評価と対応」について、具体的にどのような基準を設け、また調査すべきか。 　• 基準として、例えば、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ことなどが考えらえるが、どのような基準とすべきか。 　• 調査について、例えば、上記基準について記録された書類の内容を直接確認する方法、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などが考えられるが、どのような調査方法とすべきか。

モダナイズの方向性 ❷ に関する議論

❷ の本検討会での議論の方針

第一回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、具体案への意見収集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?

議論の結果

- 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相当以上とし、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
- 暗号装置の技術基準として、どのようなものを規定する必要があるかの議論が必要

本検討会での追加議論内容

要件の明確化

2-1 どのような内容でモダナイズを実施するべきか?

❷ に関する補足資料:FIPS140シリーズの要件比較

(参考) FIPS140-1 セキュリティ要件の概要

※青枠は現行基準相当
※赤字は現行の方針で明記されている項目

項目	セキュリティ・レベル1	セキュリティ・レベル2	セキュリティ・レベル3	セキュリティ・レベル4
暗号モジュールの仕様	同右		暗号モジュールおよび暗号境界の仕様、すべてのハードウェア、ソフトウェア、ファームウェア・コンポーネントを含む暗号モジュールの説明、モジュールのセキュリティ・ポリシーの記述	同左
暗号モジュールのポート及びインターフェース	必須およびオプションのインターフェース、すべてのインターフェースとすべての内部データバスの仕様		重要なセキュリティ・パラメータ用のデータ・ポートは、他のデータ・ポートから物理的に分離されていること	同左
役割、サービス及び認証	必須オプションの役割、役割ベースのオペレータ認証	役割ベースのオペレータ認証	IDベースのオペレータ認証	同左
有限状態モデル	同右		有限状態機械モデルの仕様、必須状態とオプション状態、状態遷移図と状態遷移の仕様	同左
物理的セキュリティ	製造グレードの設備	ロックまたは改ざん証拠	カバーやドアのタンパ検知と対応	タンパー検知と応答エンベロープ
	同右		条件はない	温度と電圧
設計保証	ソフトウェア設計の仕様がソフトウェアを有限状態機械モデルに関連付ける		高レベル言語の実装	正式なモデル、事前条件と事後条件
動作環境	実行可能なコード、認証済み、単ユーザー、単プロセス	管理されたアクセス保護 (C2または同等のもの)	ラベルド・プロテクション (B1または同等のもの)、信頼できる通信路	ストラクチャード・プロテクション (B2または同等のもの)
暗号鍵管理	FIPSが認証した生成/配布技術		暗号化された形式での鍵の入出力、または分割された知識手順による直接の入出力	同左
暗号アルゴリズム	同右		情報を保護するためのFIPS認可の暗号アルゴリズム	同左
EMI/EMC	FCC Part 15 サブパートA、クラスA（業務用）、適用されるFCC要件（音声用）		FCC Part 15 サブパートJ、クラスB（家庭用）	同左
セルフテスト	同右		パワーアップテストと条件付きテスト	同左

Source: 米国国立標準技術研究所「FIPS 140-1」

(参考) FIPS140-2 セキュリティ要件の概要

※青字は前シリーズからの主な変更項目

項目	セキュリティ・レベル1	セキュリティ・レベル2	セキュリティ・レベル3	セキュリティ・レベル4
暗号モジュールの仕様	同右		暗号モジュール、暗号境界、承認されたアルゴリズム、および承認された動作モードの仕様、すべてのハードウェア、ソフトウェア、ファームウェアコンポーネントを含む暗号モジュールの説明、モジュールのセキュリティポリシーの記述	同左
暗号モジュールのポート及びインターフェース	必須およびオプションのインターフェース、すべてのインターフェースとすべての出力データパスの仕様		保護されていない重要なセキュリティ・パラメータ用のデータ・ポートは、他のデータ・ポートから物理的に又は論理的に分離されていること	同左
役割、サービス及び認証	必須オプションの役割とサービスを識別的に分離	役割ベースまたはIDベースのオペレータ認証	IDベースのオペレータ認証	同左
有限状態モデル	同右		有限状態モデルの仕様、必須状態とオプション状態、状態遷移図と状態遷移の仕様	同左
物理的セキュリティ	製造グレードの設備	ロックまたは改ざん証拠	カバー及びドアに対してのタンパー検出及びタンパー応答 **（自動での抹消等、規定内容の強化あり）**	タンパー検知および応答エンベロープ
動作環境	単一の演算子、実行可能なコード、承認された完全性テクニック	EAL2で評価されたPPで、アクセス制御の仕組みと監査が指定されている	**参照PP＋EAL3で評価されたトラステッド・パス＋セキュリティ・ポリシーモデリング**	参照PPとEAL4で評価されたトラステッド・パス
暗号鍵管理	同右		鍵管理メカニズム：**乱数生成**、鍵生成、鍵の更新、鍵の配布、鍵の削除	同左
	手動の方法で確立された秘密鍵および秘密鍵は、平文で入力または出力される可能性がある		手作業で確立された秘密鍵および秘密鍵は、暗号化された状態で入力または出力されるか、または分割された知識手順で入力または出力されるものとする	同左
EMI/EMC	47 CFR FCC Part 15 サブパートA、クラスA（業務用）、適用されるFCC要件（無線用）		47 CFR FCC Part 15 サブパートB、クラスB（家庭用）	同左
セルフテスト	同右		パワーアップテスト：暗号アルゴリズムテスト、ソフトウェア／ファームウェアの完全性テスト、重要機能テスト、条件付きテスト	同左
設計保証	情報管理基準（CM）、安全なインストールと生成に対するポリシーの対応ガイダンス文書	CMシステム、安全な配布、機能性検査	高レベル言語の実装	形式モデリング、詳細な説明（非公式な証明）、事前条件と事後条件
その他の攻撃の軽減	同右		**現在、テスト可能な要件がない攻撃の緩和の仕様**	同左

Source: 米国国立標準技術研究所「FIPS 140-2」

❷ の論点詳細

観点	論点	論点詳細

要件の明確化	2-1 どのような内容でモダナイズを実施するべきか?	• FIPS140-2 相当以上に変更するにあたり、求めるセキュリティレベルについては、引き続きレベル３として良いか？
		• 上記のセキュリティレベルを求めるとした場合、方針の改正にあたって、FIPS-140-2レベル３相当以上を要求するにあたって欠かせない重要な要求事項は何か？
		  • 「物理的セキュリティ」「暗号鍵管理」については一定の変更が確認できるが、この変更をどの程度取り込むべきか？
		  • 「その他の攻撃の軽減」に相当する基準を新たに求めるか？
		  • 上記項目以外に要求すべき内容がないか？

モダナイズの方向性 ❻ に関する議論

❻ の本検討会での議論の方針

第二回検討会での議論の方針

公的個人認証法で認められている方法を追加する必要があるか検討
また、追加するとした場合、電子署名法の特定認証業務の認定にあたって、どこを確認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で認められている方法を追加する必要があるか?

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の認定にあたって確認すべき事項はどこか?

議論の結果

- 公的個人認証法と電子署名法の基準を統一したほうが良いが、マイナンバーカードとの仕様の差異は要考慮
- 事業者ごとの通信結果がデータベースやログから正確に確認する方法の模索が必要

本検討会での追加議論内容

運用への影響

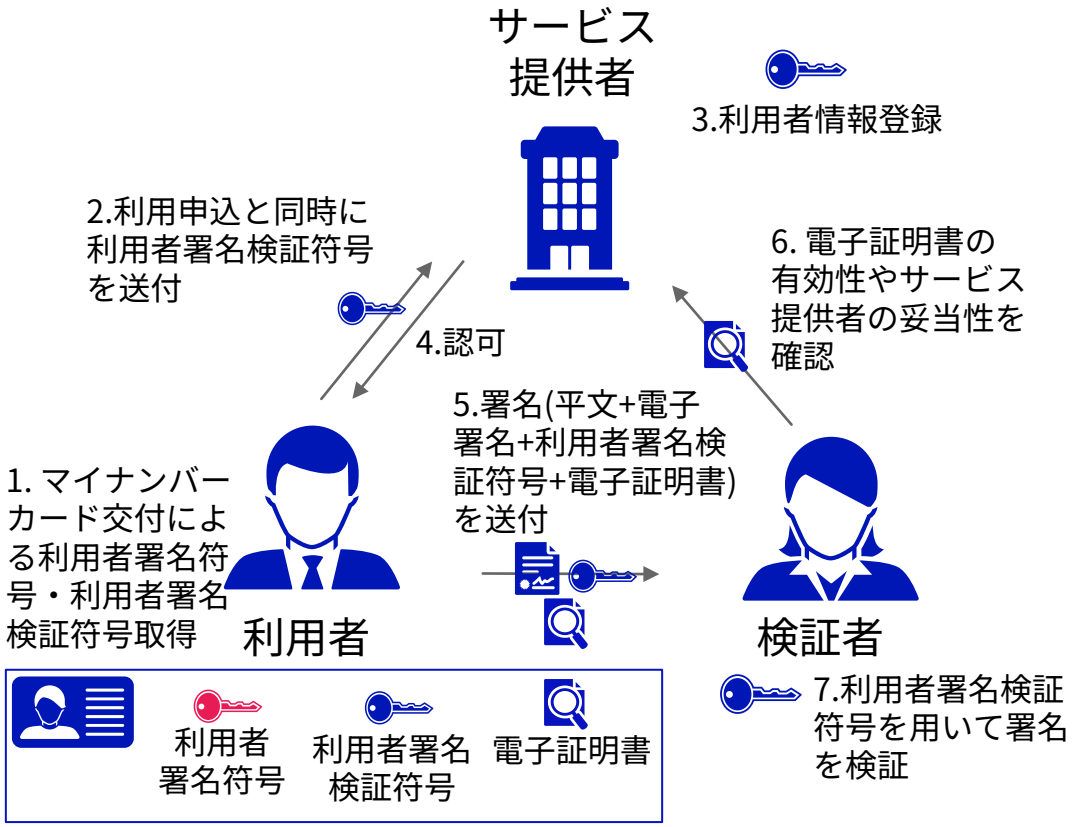
6-2 ❻ のモダナイズを行う場合、電子署名法の特定認証業務の認定にあたって、確認すべき事項はどこか?

❻ に関する補足資料：差異の解消の目的の整理

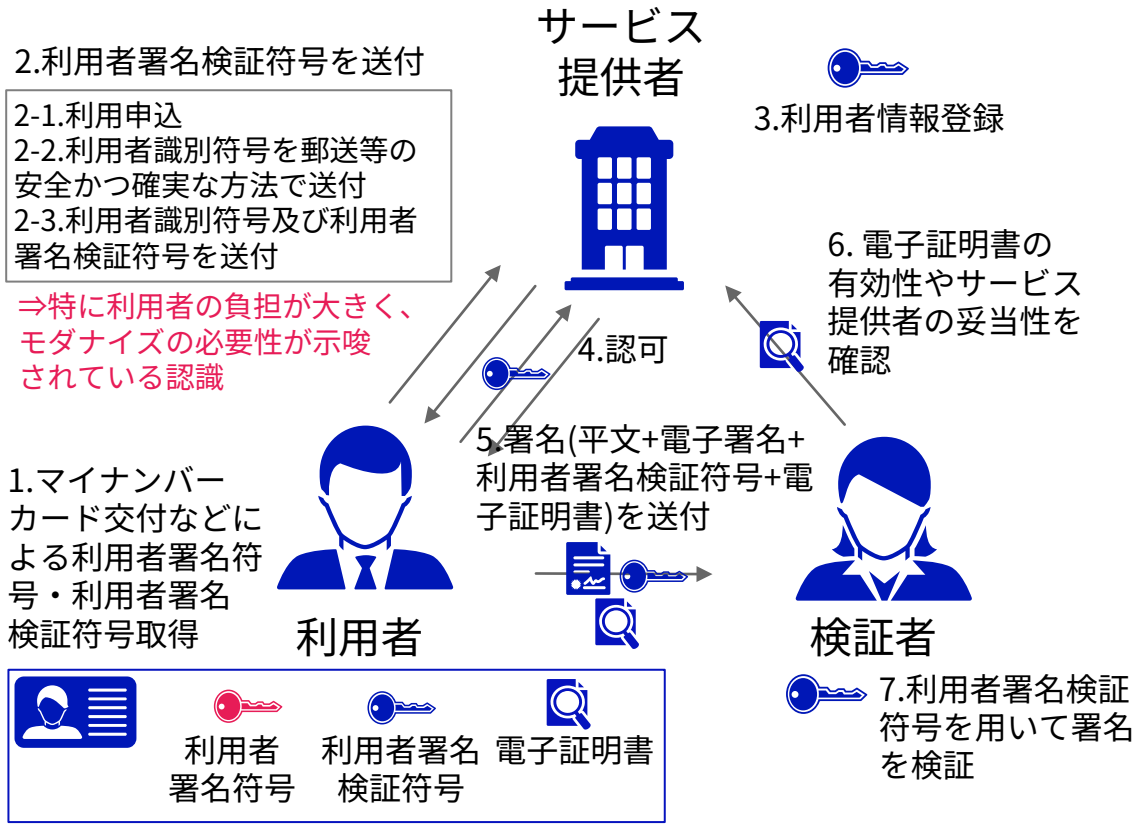
公的個人認証サービスと電子署名法の認定認証事業に基づくサービスの違い

※利用者署名符号を利用者が作成する場合

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



❻ に関する補足資料

(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。

（参考）電子署名法施行規則第６条第３号及び第３号の２への適合性に関する審査内容

第６条第３号

3301.利用者署名符号を認証事業者が生成する場合は、以下の3302.～3305.の事項に関して、認証業務規程及び事務取扱要領等に明確かつ適切に規定し、実施している。

3302.利用者署名符号の生成を、認証設備室内又は同等の安全性が確保できる環境において、複数人の捜査者によって行い、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ている。

3303.利用者署名符号の転送や出力等を行う場合は、生成時と同等の安全性が確保された環境において、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ている。
また、生成及び転送や出力等に用いた装置等から取り出した後、遅滞なく利用者署名符号を完全に廃棄、もしくは消去している。

3304.利用者署名符号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ている。
また、生成及び転出や出力等に用いた装置等から取り出した後、遅滞なく利用者署名符号の活性化に使用するPIN等を完全に廃棄、もしくは消去している。

3305.生成された利用者署名符号を、安全かつ確実な方法で利用者本人に渡し、利用者から、利用者本人を特定できる自筆署名、又は印鑑登録証明書に係る印鑑等利用者本人を特定できる印鑑による押印、又は電子署名が付された受領書を受け取る。

第６条第３号の２

3311.利用者署名符号を利用者が作成し、認証業務用設備を利用者情報及び利用者識別符号の識別によって自動的に作動させる場合において、当該利用者署名符号に対応する利用者署名検証符号を認証事業者が電気通信回線を通じて受信を行う場合は、以下の2.～6.の事項に関して、認証業務規程及び事務取扱要領等に明確かつ適切に規定し、実施している。但し、5.の事項に関しては、認証業務用設備を利用者情報及び利用者識別符号の識別によって自動的に作動させない場合も含むものとする。

3312.利用者の識別に用いる利用者識別符号は、安全な擬似乱数生成アルゴリズムを用いて生成するものとし、認証設備室又は同等の安全性が確保できる環境において、複数人によって行われている。

3313.利用者識別符号は、安全かつ確実な方法で利用者本人に渡され、かつ、当該利用者へ電子証明書を発行する際には、当該利用者識別符号の受領の確認が行われている。

3314.利用者識別符号は、認証設備室又は同等の安全性が確保できる環境に暗号化等の措置を講じて保管されている。

3315.利用者が利用者識別符号を送信する際には、利用者識別符号等受信設備の誤認並びに通信内容の盗聴及び改変を防止する措置が講じられている。

3316.利用者の識別に用いた利用者識別符号がそれ以降の識別処理に用いられないような措置(認証業務用設備内に設定されている識別された利用者に対応した利用者識別符号を、廃棄又は使用済フラグを立てることなどにより使用できないようにすることなど)が直ちに講じられている。

参照：JIPDEC「特定認証業務の認定に係る調査表」

❻ の論点詳細に関する補足資料

第二回の議論の振り返り

- 公的個人認証法で認められている方法を、電子署名法においても認める方向で検討すべき
- この時、**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した場合の、発行申請書と利用者署名検証符号の紐付けや改ざん防止等の措置**の取り扱いについて、あらかじめ整理する必要がある。
  - 利用者が電気通信回線を通じて発行申請書と同時に利用者署名検証符号を送付する場合、改ざんされていないと判断できるか
  - マイナンバーカード署名用電子証明書により電子署名を付し発行申請を行っている場合、発行申請者＝利用者本人と言えるか　等

上記の取り扱いを整理した上で、以下についても整理する必要性があるのではないか。

- 認定事業者が、認定業務の実施において、上記の紐づけや改ざん防止の措置についてどのような方法で何を確認しなければならないか。
- 指定調査機関は、認定業務において適切な方法で適切な確認が行われていることをどのように調査すべきか。

❻ の論点詳細

観点	論点	論点詳細
運用への影響	6-1 ❻ のモダナイズを行う場合、電子署名法の特定認証業務の認定にあたって、確認すべき事項はどこか?	• 「電子証明書の発行申請と利用者署名検証符号を一度に送付する」とした場合、発行申請書と利用者署名検証符号の関連付けや改ざん防止等の措置について、どのように担保されている必要があるか。 • 認定基準の統一(利用者が鍵ペア―を作成する場合の利用者署名検証符号の送付要件の修正)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。

モダナイズの方向性 ❸ に関する議論

第２回検討会資料再掲

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

第２回検討会資料再掲

❸ に関する補足資料：クラウドHSMの概要と主要論点

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？

論点❸に関する方向性整理

第２回検討会において、頂いたご意見を踏まえて、方向性及び今回において深掘りを行う点の整理を実施。

⇒下記の方向性にて問題ないかご確認・ご意見頂きたい。

検討の方向性

- 特定認証業務の認定における、**クラウドHSMの利用**（CSPやHSMベンダーが提供するパブリッククラウドにおけるクラウドHSMサービスの利用）については、将来的な検討課題とし、本検討会において整理を行った課題の解決を図るための整理を進める。
- **プライベートクラウドに設置されたHSMの利用・ネットワーク型HSMの利用**については、本検討会において再度議論の機会を設け、整理を進める。（今回）
- 本論点に関する議論においては、次の点（次々ページ「論点❸ ：第２回検討会におけるご意見の整理のご確認」の(1)～(8)）に留意するべきである。

（参考）HSMの利用形態の違い

（いずれも一般的な例）	通常のHSM	ネットワーク型HSM	クラウドHSM
設置場所 ※1	オンプレミス環境	オンプレミス環境／ 自社クラウド等	クラウド環境
アクセス方法	直接（PCIe、USB）	ネットワーク経由	API/SDK経由、ブラウザ経由
管理責任	自社	自社	クラウドサービスプロバイダー
初期コスト	高い	高い	低い
可用性	限定的（重要ではない）	中程度	高い（重視）
セキュリティレベル ※2	最高	高	中～高

※1 クラウドHSMサービスを提供する事業者内においてネットワーク型HSM等が利用される場合もあるが、HSMの最終的な利用者である事業者の立場から見た形態の違いの観点より整理。

※2 HSMが設置された部屋への立入、操作者の限定、接触機会等、アタックサーフェスとなり得る要素を踏まえた総合的な観点として。

論点❸：第２回検討会におけるご意見の整理のご確認

（1）従来の管理基準との整合性を確保しつつ、クラウドHSM特有のリスクに対応できる基準を策定する必要がある。

（2）BYOKを利用する場合、利用しない場合の整理が必要なのではないか。

（3）クラウドHSM提供事業者に対する立入検査の難しさ、法的な規範の範囲外となる課題への対策を検討する必要がある。

（4）認証局のルート秘密鍵（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るため、可用性も重視しているクラウドのアーキテクチャにより失われる要素につき、慎重な検討が必要がある。

（5）クラウドHSMの利用自体は、リモート署名にも深く関係するものの、リモート署名においてクラウドHSMに利用者の署名鍵を保管することと、認証局のルート秘密鍵を保管することは、重要性、可用性と機密性のバランス等、考慮する観点が異なるため、分けて議論を行うべき。

（6）ネットワーク経由でのHSMへのアクセスは、新たなアタックサーフェス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適切な調査・審査方法を確立する必要がある。

（7）また、通信に限らず、HSMを遠隔で操作するGUI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。

（8）HSMの設置場所が海外である場合のリスクについては、現に、電子署名法において海外における特定認証業務の認定を行うことができ、法目的を踏まえると本検討会のスコープ外となるが、将来的な検討課題となる可能性がある。

※太字で示した(1)(4)(6)(7)は、プライベートクラウドに設置されたHSMの利用・ネットワーク型HSMの利用における議論でも留意が必要。

論点❸：プライベートクラウドに設置されたHSM
ネットワーク型HSM } の利用について

- プライベートクラウドに設置されたHSMの利用、ネットワーク型HSMの利用については、主務大臣及び指定調査機関による調査を実施する上での課題が比較的少なく、パブリッククラウドサービス等が提供するクラウドHSMサービスの利用よりも、早期に認定制度に反映できる可能性が高い。
- 第２回検討会においてご議論頂いた内容につき、「プライベートクラウドに設置されたHSM／ネットワーク型HSMの利用」に範囲を限定した場合に、考え方に変化が生じる点、留意点が解消する点、依然留意しなければならない点をご議論いただきたい。

第２回検討会で頂いたご意見を踏まえた留意点の整理（抜粋再掲）

（１）従来の管理基準との整合性を確保しつつ、クラウドHSM特有のリスクに対応できる基準を策定する必要がある。

（４）認証局のルート秘密鍵（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るため、可用性も重視しているクラウドのアーキテクチャにより失われる要素につき、慎重な検討が必要がある。

（６）ネットワーク経由でのHSMへのアクセスは、新たなアタックサーフェス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適切な調査・審査方法を確立する必要がある。

（７）また、通信に限らず、HSMを遠隔で操作するGUI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。

モダナイズの方向性 ❹ に関する議論

第２回検討会資料再掲

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?

第２回検討会資料再掲

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

第２回検討会資料再掲

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）

論点❹の議論について

- 論点❹については、早期に検討可能な点を優先しつつ、今後整理・調査が必要な点に関する整理を進めるため、下記の順番で進めることとしたい。（以下、❹-1.～❹-4.と呼称。）
  1. ニーズが高い、認証局のリポジトリにおける利用（A）に関する整理のご確認・補足等
  2. B～Dに関する調査・審査の方法についてに関する整理のご確認・補足等
     （Aに関する調査・審査の観点の整理は1.において実施。）
  3. ニーズが高い、認証局の保守・運用における利用（C）のご意見整理・深掘り
  4. 第２回検討会におけるご意見の整理のご確認・補足等

❹-1. 認証局のリポジトリにおける利用（A）に関する整理のご確認・補足等

ご意見の整理

- 認証局のリポジトリは可用性が求められ、また、機密性・完全性に関するリスクは限定的（公開しているデータには電子署名が行われているため。）であるため、パブリッククラウド利用における問題点は少ない。
  - CP/CPSのPDFについても電子署名を実施すれば、非改ざん性を担保することが可能。
  - OCSPの場合においても、予め生成したOCSPレスポンスをCDNに配置することにより、OCSPレスポンダ自体をパブリックにせず、可用性のみに着目した利用方法が考えられる。

確認事項

- 認証局のリポジトリにおける利用については、利用するパブリッククラウドサービスについて、ISMAPやISO27017等のセキュリティ認証を取得したクラウドの利用までは求めない形でも問題ないか。
  - 認証局のリポジトリにおける利用に関してプライベートクラウドの利用を認めた前例においては、プライバシーマーク、品質マネージメントシステム認証、情報セキュリティーマネージメントシステム（ISMS）、環境マネージメントシステム認証の取得も踏まえて実施。
- 認証業務用設備以外については、ハード面での災害対策やバックアップ等を明示的に求めておらず、バックアップサーバの設置等も任意で行われてきたが、クラウド利用において、冗長性や可用性の基準を求める必要はないか。
  - 高可用性・冗長性を担保した構成においては、別クラウドサービスプロバイダー（CSP）の利用、別リージョンの利用、別のアベイラビリティゾーン（AZ）の利用等が考えられるが、Aにおいてはどの程度を求めるか。
  - 事業者自身で冗長性を担保した構成を実施せず、 CDN等の（外見上冗長性がどのように担保されているか不明な場合もある）SaaS等を利用する場合も考えられるが、この場合において、当該サービスが公開しているSLAを参考として採用することができるか。その他の方法として、どのような基準が考えられるか。

（参考）関係する調査表項番

調査表項番	施行規則	指針	適合例	必要書類
3513	認証業務に関し、利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置を講じていること。(第六条第七号)	発行者署名検証符号に係る電子証明書の値をＳＨＡ－２５６、ＳＨＡ－３８４又はＳＨＡ－５１２のうちいずれか一以上で変換した値によって認定認証業務を特定すること。(第十条第二号)	(3)当該発行者署名符号に対応した発行者署名検証符号に係る電子証明書の値をSHA-256、SHA-384又はSHA-512のうちいずれか1以上で変換した値（フィンガープリント）を記録し、改ざん防止措置を講じて公開している。	・電子証明書の値をSHA-256、SHA-384又はSHA-512のうちいずれか1以上で変換した値
3C56	利用者の真偽の確認に際して知り得た情報の目的外使用の禁止及び第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又は毀損の防止のために必要な措置(第六条第十五号へ)		(6) 各記録は漏えい、滅失又は毀損防止のため、以下の措置を講じている。 ① 共通要件 ・各記録は、施錠可能な出入口を持ち、間仕切り又は壁等によって区分された室の中に保存する。 ・各記録が保存される室には、自動火災報知器及び消火装置が備えられている。 ・各記録は直射日光が直接当たらない場所に保存するか、直射日光が当たらないよう、遮蔽措置を講ずる。 ② 紙媒体により原本で保存される資料等における追加要件 ・原本上の記録が判読不能とならない環境を備えている。 ・専用のファイルにとじ込む。 ③ 電磁的記録で保存される記録における追加要件 ・当該記録媒体の内容を表示することが出来るように、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを維持・保存しておくこと。特に、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを更新する場合は、当該記録媒体との互換性を確保すること等により、表示不能を生じさせないこと。 ・記録媒体は、データの表示不能にならないように適切なケース等に保管する。さらに記憶媒体の特徴に合わせて適宜記録し直すなどの措置が実施されるようになっている。ただし、その際、保存内容の完全性・機密性を損なわない方法でなされている。	・認証業務規程 ・事務取扱要領 ・教育訓練計画書

❹-2. 観点「調査・審査の方法について」に関する整理のご確認・補足等

（B～D共通）調査・審査の方法について

- 利用者の申込み／利用者の本人確認における利用（B）、認証局の保守・運用における利用（C）のうちログ・死活監視サーバ等の設置について、認証局の帳簿書類等の保管のクラウド化（D）については、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、電子署名法における調査基準について、項目・観点等の整理を行った後に判断する形で問題ないか。
- B～Dいずれの場合においても、プライベートクラウドであり、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る場合は、ISMAP等クラウドサービスのセキュリティに関する認証を求めない形（既存の電子署名法の調査基準を適用する形）でも問題ないか。

❹-3. 認証局の保守・運用における利用（C）のご意見整理・深掘り

クラウド環境にログ・監視サーバ等を設置すること自体について（クラウド利用の観点）

（第２回検討会においては、本観点については特にご異議はなかったとの認識。）

- SaaSの利用を妨げないような整理を行う必要があるのではないか。

クラウドに設置されたログ・死活監視サーバの利用について（遠隔操作の観点／クラウド利用の観点）

- ログ・死活監視サーバがクラウド上に設置されている場合、クラウド間（監視対象がクラウド上に存在する場合）、クラウドへの接続（管理対象がオンプレミス環境に存在する場合）の通信が発生するが、これには、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可能な限り避けた方が良いのではないか。
  - 監視対象の閉域にエージェント等を設置し、内部から外部へのアクセスを行う場合については問題ないのではないか。

保守のための遠隔操作について（遠隔操作の観点）

- （オンプレミス環境への遠隔操作について）リモートで保守運用を行う際に、インターネット環境よりVPN等を経由してランディングサーバにアクセスし、ランディングサーバより認証業務用設備の遠隔操作を実施する場合において、ランディングサーバに脆弱性が存在する場合の影響が大きいため、遠隔操作を許容する範囲について考慮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については、許容可能ではないか。

❹-4. 第２回検討会におけるご意見の整理のご確認

A～D共通

- 政府情報システムにおけるクラウドサービス利用基準としては、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、機密性２以上においてISMAP等を求めていることは考え方の参考になるのではないか。
  - 具体的には、Aは公開情報であるためクラウドサービス自体の安全性に関する規定は特段不要であるが、BやDにおいては、ISMAP等の規定を求めるという考え方ができるのではないか。
  - 論点③における認証局のルート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、ISMAP等クラウドサービスの安全性に関する既存の基準を活用できるのではないか。
  - 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、それぞれ確認している内容が同一ではないため、観点ごとに十分か否かの整理を行う必要があるのではないか。エビデンスやテストケースの援用についても、同様に、個別判断になるのではないか。
- 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等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可能な限り避けた方が良いのではないか。

❹-4. 第２回検討会におけるご意見の整理のご確認

B：利用者の申込み／利用者の本人確認における利用

D：認証局の帳簿書類等の保管のクラウド化

- B、Dにおいては、利用者の個人情報を取り扱う観点が加わるが、本点については、これまでオンプレミスの設備等でセキュリティが担保されている点が存在したため、クラウド利用においては、新たにクラウドの安全性を担保する基準を求める形になるのではないか。
  - 特にBについては、認証局のRAに関する内容であるため、一定の水準を保証する必要があると考えられるのではないか。
  - 具体的には、ISO27000シリーズ、特にISO27017を参照するのが良いのではないか。（これは、ISMAPやISMSのセキュリティ基準とほぼ同等のものとなる。）
  - ISMAPやISO27017は、コンピュータに関する要件が対象となっているため、登録用端末設備を取り扱う人に関しても基準を求める場合は、従来の要件を参考にした方が良いのではないか。

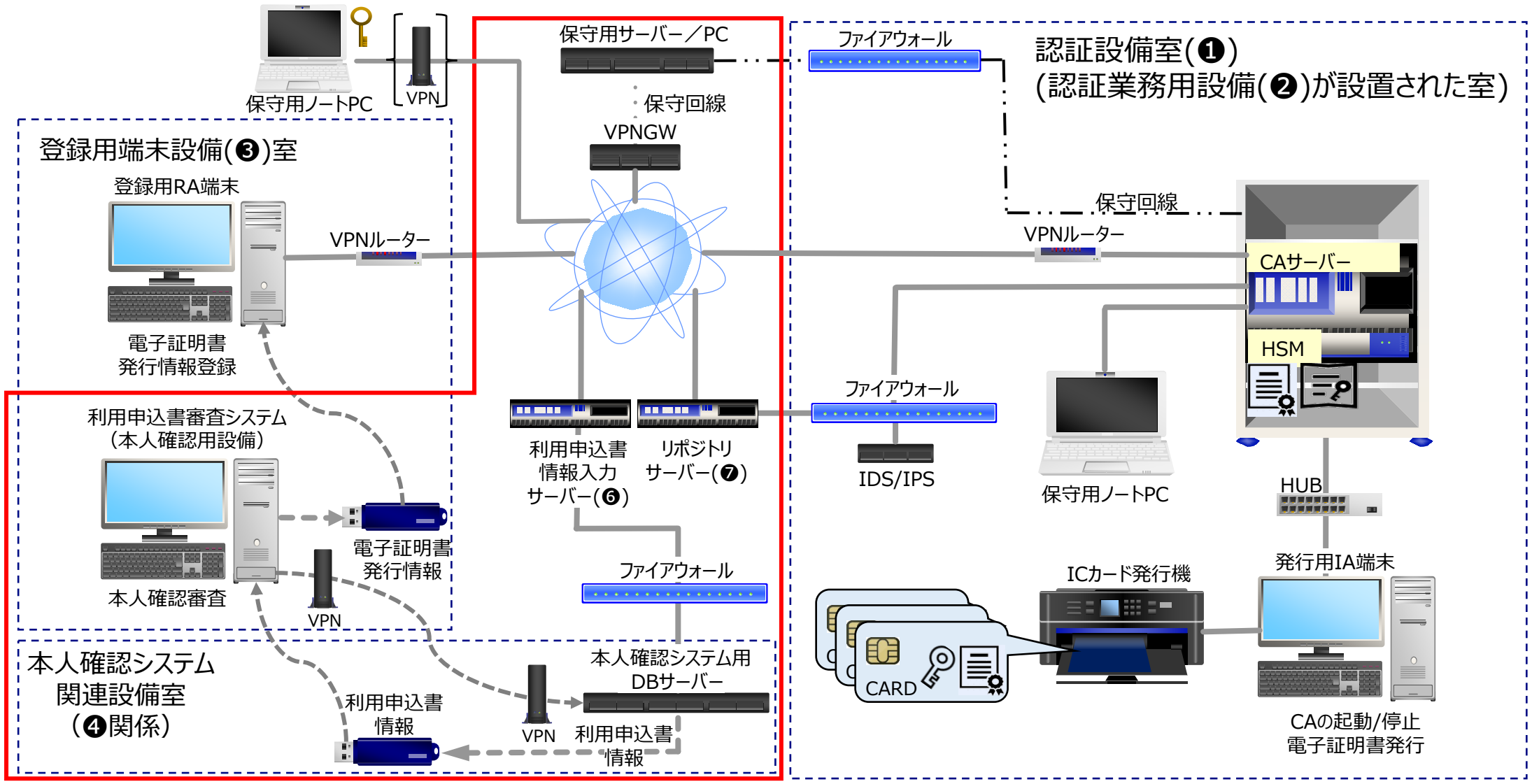
(参考)認証局の設備の説明

設置場所[1]	用語	定義等の概要	設備例
高セキュリティゾーン	❶認証設備室	❷認証業務用設備が設置された室（❸登録用端末設備のみ、❺利用者識別設備のみが設置されている室を除く。）（指針第4条第1号）	
	❷認証業務用設備	申請に係る業務の用に供する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（規則第4条第1項）	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	❸登録用端末設備	専ら電子証明書の利用者を登録するために用いられる設備（指針第4条第1項） 説明：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
	❹本人確認用設備	（明文の定義なし） 説明：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
	❺利用者識別設備	専ら利用者情報及び利用者識別符号を識別するために用いられる設備（指針第4条第1項） 説明：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	❻利用申込用利用者情報入力設備	（明文の定義なし） 説明：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
	❼リポジトリ設備	（明文の定義なし） 説明：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

（参考）令和５年度報告書における認証局の構成例（改変）

センター発行方式の場合

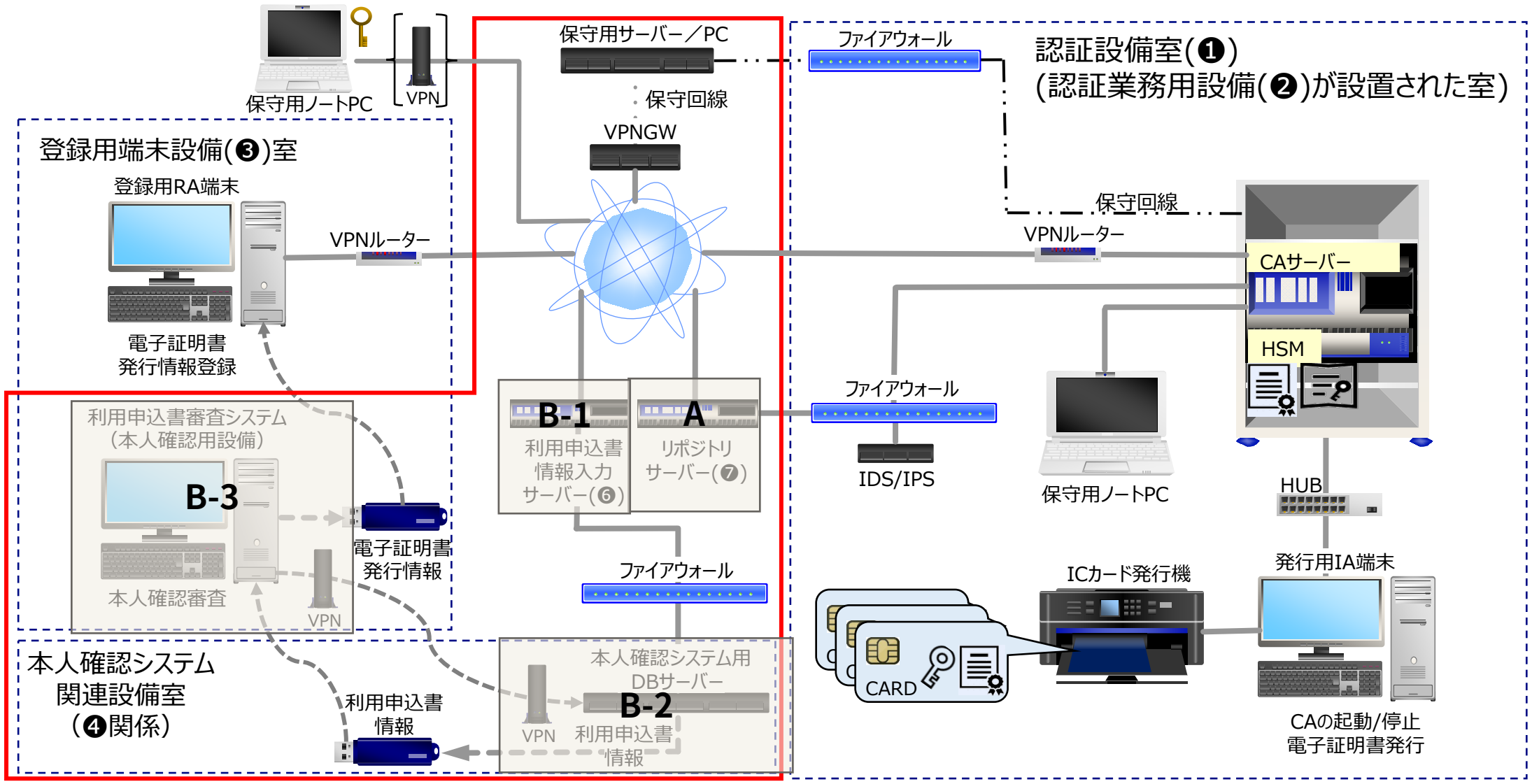


（赤枠）論点④においてクラウド利用が考えられる点

※本方式においては、❺利用者識別設備は存在しない。

（参考）令和５年度報告書における認証局の構成例（改変）

センター発行方式の場合

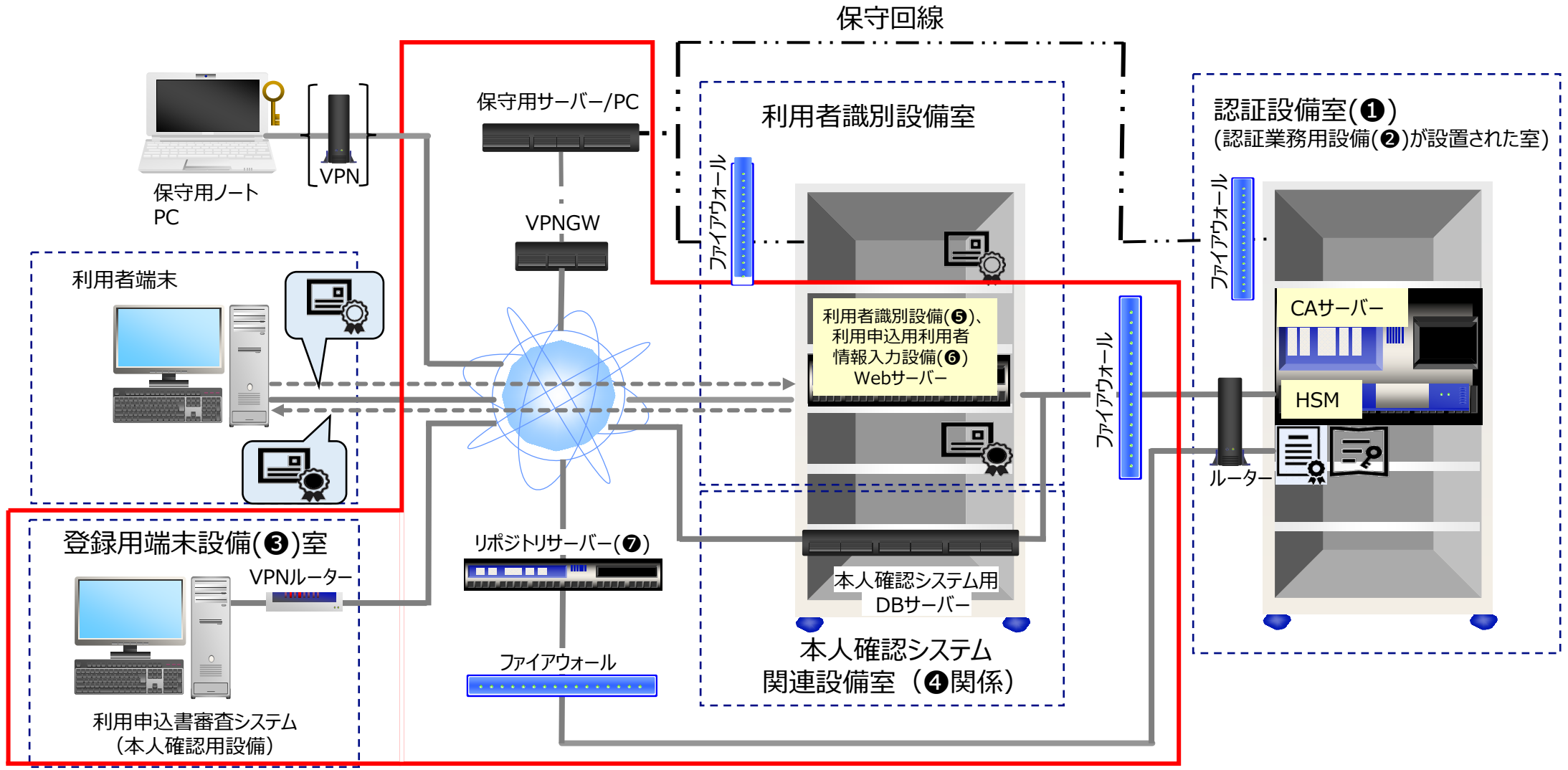


（赤枠）論点④においてクラウド利用が考えられる点

※本方式においては、❺利用者識別設備は存在しない。

（参考）令和５年度報告書における認証局の構成例（改変）

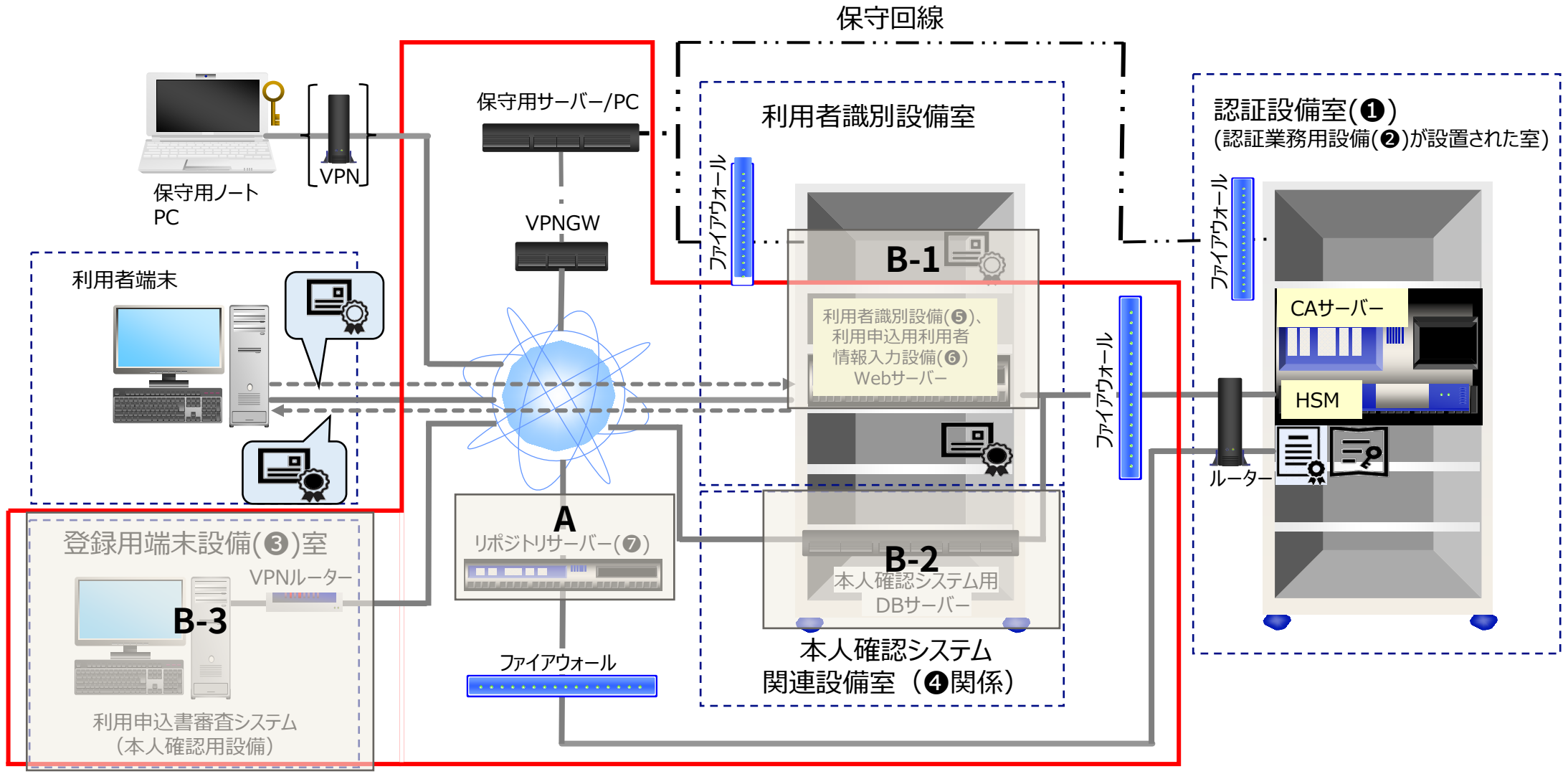
ユーザー鍵生成方式の場合



（赤枠）論点④においてクラウド利用が考えられる点

（参考）令和５年度報告書における認証局の構成例（改変）

ユーザー鍵生成方式の場合



（赤枠）論点④においてクラウド利用が考えられる点

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(済)
第3回	• モダナイズの方向性 ❶ ❷ ❸ ❹ ❻ の残論点について議論	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12〜1月（調整中）

デジタル庁

Digital Agency