資料１

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第12回健康・医療・介護情報利活用検討会

医療等情報利活用ワーキンググループ

２０２２（令和４）年９月５日

「医療情報システムの安全管理に関するガイドライン」について

医政局特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

Ministry of Health, Labour and Welfare of Japan

ガイドライン 第5.2版 について

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

医療情報システムの安全管理に関するガイドライン　改定の経緯

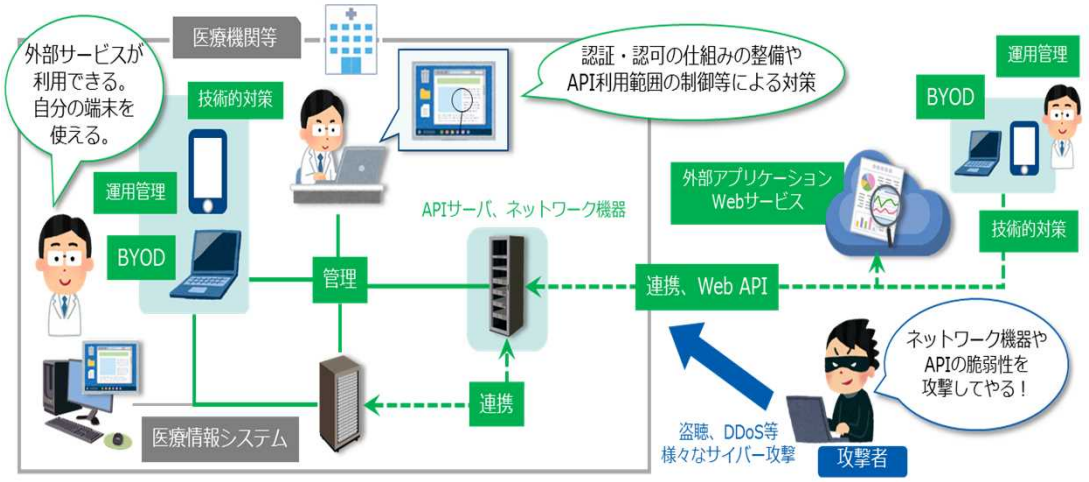
- 医療情報システムの安全管理に関するガイドラインは、e-文書法、個人情報保護等への対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第1版を策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定。直近では令和４年３月に第5.2版を策定。

	第1版	第2版	第3版	第4版（4.1、4.2、4.3）	第5版（5.1）	第5.2版
策定・改定時期	平成17年3月	平成19年3月	平成20年3月	平成21年3月 平成22年2月（4.1版） 平成25年10月（4.2版） 平成28年3月（4.3版）	平成29年5月 令和3年1月（5.1版）	令和4年3月
策定・改定概要	・医療情報システムのセキュリティ管理を目的とて策定	・重要インフラとしての医療情報システムという観点からの対応	・個人情報施策の議論およびモバイル端末普及への対応	第4版 ・個人情報保護施策の議論およびモバイル端末普及への対応 第4.1版 ・民間事業者のデータセンターにおける外部保存に関する対応 第4.2版 ・調剤済み処方せん及び調剤録等の外部保存への対応 第4.3版 ・「電子処方せんの運用ガイドライン」への対応	第5版 ・医療機関等の範囲の明確化 ・改正個人情報保護法対応 ・サイバー攻撃の動向への対応 第5.1版 ・クラウドサービスへの対応 ・認証・パスワードに関する対応 ・サイバー攻撃等による対応 ・外部保存受託事業者の選定基準対応	制度的な動向 ・２省（総務省、経産省）ガイドライン等との整合性 ・改正個人情報保護法への対応　等 技術的な動向 ・医療機関へのサイバー攻撃の多様化・巧妙化　等 「規制改革実施計画」等への対応 ・電子署名 ・外部ネットワーク

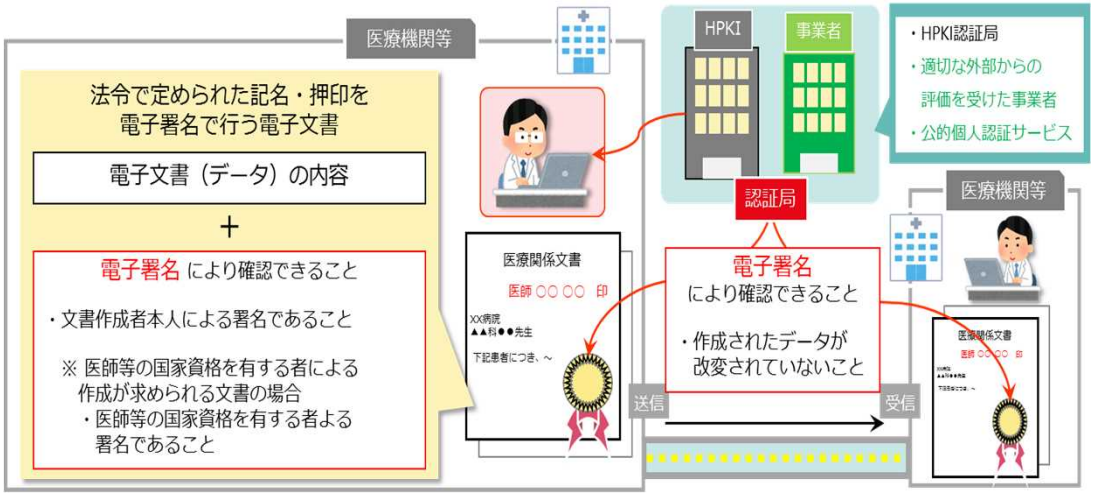
第5.2版 概要

ガイドラインの読みやすさの工夫：本編＋別冊編の分冊化

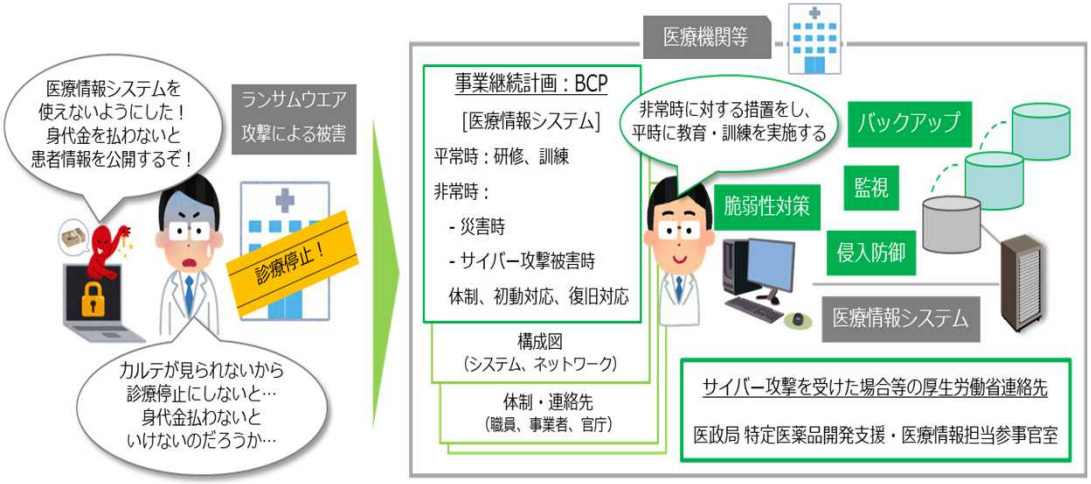
外部ネットワーク接続（外部アプリケーション連携）やBYODの管理



法令で署名又は記名・押印が義務付けられた文書に対する電子署名



不正ソフトウエア対策を含むサイバー攻撃対策の強化



第5.2版 中長期的な改定の論点

以下の項目は十分な検討が必要と考え、中長期的な論点として検討を継続する。

概要	背景
クラウドサービス利用の拡大	○　院内の多様なシステムに関して、オンプレミスとの関係を整理し、クラウド利用を想定し、現行ガイドラインに不足している内容を検討 ○　端末の持ち出しだけでなく、クラウドサービスによる情報の持ち出しについて現行の課題を抽出し、対策を検討
多様化するサイバー攻撃への対応	○ 医療機関等における内部ネットワークについて、「ゼロトラスト」の考え方を参考にした記載や、セキュリティ自動監視などについても検討
新技術への対応	○ PHSサービスに代わり、５Gサービスが今後使用される可能性を考え、前もって議論
制度・規格関係	○ 医療情報連携ネットワークを通じた、情報提供について、共同利用型などを想定し、記載を検討

ガイドラインの改定 について

- 作業班
- 改定方針
- 論点、対応方針(案)
- スケジュール(案)

第6.0版 への改定作業班

委託事業：「医療情報システムの安全管理に関するガイドライン」改定に向けた調査等一式

	氏名・所属等		
構成員 （五十音順・敬称略）	座長	山本　隆一	医療情報システム開発センター 理事長
		秋山　祐治	川崎医療福祉大学　副学長・教授
		新垣　淑仁	保健医療福祉情報システム工業会 電子カルテ委員会
		小尾　高史	東京工業大学 科学技術創成研究院　准教授
		門林　雄基	奈良先端科学技術大学院大学 情報科学領域　教授
		河野　行満	日本薬剤師会 医療情報管理部　部長
		武田　理宏	日本病院会、大阪大学医学部附属病院 医療情報部　教授
		田中　勝弥	国立がん研究センター 情報統括センター　センター長
		玉川　裕夫	日本歯科医師会　情報管理担当
		樋口　範雄	武蔵野大学 法学部　特任教授
		矢野　一博	日本医師会 総合政策研究機構　主任研究員
オブザーバー		総　務　省	情報流通行政局 地域通信振興課 デジタル経済推進室
		経済産業省	商務・サービスグループ ヘルスケア産業課
		厚生労働省	医政局 特定医薬品開発支援・医療情報担当参事官室
事務局		株式会社 エヌ・ティ・ティ・データ経営研究所	

開催予定：2022年７月～2023年１月に、６回程度開催

第5.2版 から 第6.0版 への改定方針

2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ねすべての医療機関等において、本ガイドラインに記載されているネットワーク関連のセキュリティ対策が必要となる。これを踏まえ、第6.0版への改定では、第5.2版で中長期的に検討を継続することとした論点を中心に、全体構成の見直しとともに検討してはどうか。

○ 外部委託、外部サービスの利用に関する整理

・クラウドサービスの特徴を踏まえたリスクや対策の考え方
・医療機関等のシステム類型別に対応した責任等の整理　　等

○ 情報セキュリティに関する考え方の整理

・ネットワーク境界防御型思考／ゼロトラストネットワーク型思考
・災害、サイバー攻撃、システム障害等の非常時に対する対応や対策
・本人確認を要する場面での運用（eKYCの活用）　　等

○ 新技術、制度・規格の変更への対応

・オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置
・新たなネットワーク技術（ローカル５G）の利用可能性、利用場面
・医療情報の共有・提供に関連する法令等の規定や技術・規格の動向

○ 全体構成の見直し

・経営管理編、運用管理編、管理実装編の３編構成を想定
・Q&Aの整備、読者類型ごとの参照先等を示した読み方支援文書等の作成

※ 各編は数十ページ程度を想定（第5.2版の文章等を全面的に精査）
第5.2版 6.12章（電子署名）は、策定時に詳細な検討・調整を行ったため、原則、現行版を踏襲

改定方針に基づく、具体的な論点と検討背景・対応方針(案)

外部委託、外部サービスの利用に関する整理

論点	背景	対応方針（案）
クラウドサービスの特徴を踏まえたリスクや対策の考え方	・第5.2版では、必ずしもクラウドサービスにおける対策等を個別に分けて記載していない。	・クラウド技術を利用したサービス固有のリスクや対策について整理する。（例えば仮想技術を利用した資源の利用、共同利用等） ・クラウドサービスにおける対策の特殊性（作業に関する報告等、ソフトウェアのバージョンアップ等）について整理する。
医療機関等のシステム類型別に対応した責任等の整理	・第5.2版では、複数ベンダが関与する場合の責任分界についての基本的な考え方が示されているものの、必ずしもオンプレミスとクラウドサービスの利用関係は示されていない。 ・複数ベンダーのシステム・サービスを多重的に利用する際に、医療機関等が行うべきベンダーに対する責任管理が、システムの利用形態の複雑化から難しくなっている。	・医療機関等におけるオンプレミスとクラウドサービスの利用形態等について整理する。 ・複数のベンダが関与する場合の責任の取決め等に関する考え方などを整理する。 ・オンプレミスを含めたサービス間連携（API）や、責任分界の考え方等を整理する。 ・医療機関等における複数ベンダーにおける責任管理等の考え方を示す。

改定方針に基づく、具体的な論点と検討背景・対応方針(案)　2／5

情報セキュリティに関する考え方の整理　1／2

論点	論点の背景	対応方針（案）
ネットワーク境界防御型思考／ゼロトラストネットワーク型思考 ※ ゼロトラストとは「何も信頼しない」を前提に対策を講じるセキュリティの考え方。閉域ネットワークであれば安全であるなどの境界防御前提には立たない。	・第5.2版では、内部脅威監視など、ゼロトラストの考え方の一端は示しているものの、境界防御を踏まえた対策等の考え方が中心となっている。	・ネットワークの安全性のあり方や認証のあり方を踏まえて、ゼロトラストの考えに則した対策の考え方を示す。 ・内部ネットワークによる利用を中心としている医療機関等と外部サービスの利用を中心としている医療機関等などの違いを踏まえた具体的な対策の考え方を示す。 ・医療情報システムに関わる全ての利用者（保守事業者、患者等を含む。）等を想定した考え方を整理する。
災害、サイバー攻撃、システム障害等の非常時に対する対応や対策	・第5.2版では、ランサムウェア対応のほか、マルウェアによる攻撃への対応や、サイバー攻撃時における通報体制等について示されている。 ・医療機関等に対するサイバー攻撃は、さらに巧妙さや対象の拡大が予想される中で、必須の対策があればそれを示す必要がある。	・ゼロトラストの議論と併せ、検知の考え方について整理し、実行力がある対応のあり方を整理する。 ・攻撃ルートの多様性を確認し、各ルートにおいて想定されるリスクや対策の考え方を整理する。

改定方針に基づく、具体的な論点と検討背景・対応方針(案)　3／5

情報セキュリティに関する考え方の整理　2／2

論点	論点の背景	対応方針（案）
本人確認を要する場面での運用（eKYCの活用）	・オンラインでの本人確認のための技術であるeKYC（electronic Know Your Customer）は、我が国では犯罪収益移転防止法において、利用が認められている。 ・医療情報システムでの利活用においては、様々な場面で利用者の本人確認が求められるが、eKYCの利用について、第5.2版では示されていない。	・eKYCの技術的な特徴・役割の特徴等を整理して、eKYCが利用可能と考えられる領域について検討する。 ・医療情報システムの利用（または、そのための手続等）において、eKYCの利用可能性等を検討するほか、これを利用する場合に想定されるリスク等について整理する。

規制改革実施計画（令和４年６月７日 閣議決定）　より抜粋

＜医療・介護・感染症対策＞（２）医療DXの基盤整備（在宅での医療や健康管理の充実）

４．電子処方箋の普及及び医療分野における資格確認・本人確認の円滑化

d）厚生労働省は、医療現場で利用される電子署名について、クラウド型電子署名等を利用しようとする医師が、当該クラウド型電子署名等の利用申込を行う際の本人確認手段として医師が自宅等から手続きを完結できるようにするため、オンラインで完結可能な本人確認方法であるeKYC（electronic Know Your Customer）を活用できることとする方向で所要の検討を行う。　[令和４年度上期検討・結論]

改定方針に基づく、具体的な論点と検討背景・対応方針(案)　4／5

新技術、制度・規格の変更への対応

論点	論点の背景	対応方針（案）
オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置	・2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ねすべての医療機関等において、ネットワーク関連のセキュリティ対策が必要となることから、導入に必要なネットワーク機器等の安全管理措置を示す必要がある。	・オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置をまとめ、Q&A等に記載する。
新たなネットワーク技術（ローカル５G）の利用可能性、利用場面	・PHSサービスに代わり、ローカル5Gサービスが院内ネットワークとして採用される可能性があるため、その対応を図る必要がある。	・2019年度ガイドライン改定作業班において新規のセキュリティ課題はないと整理されている一方で、ローカル5Gを導入する場合の無線局免許取得に必要なセキュリティ対応などにおいて、対策を検討すべき旨が指摘されていることを踏まえ、具体的なセキュリティ課題を整理し、検討する。 ・ローカル５G導入に伴う対応と５Gを利用する場合の対応策は異なるところ、ローカル５Gの利用可能性を鑑みて、ガイドライン、Q&A等での記載要否を判断する。
医療情報の共有・提供に関連する法令等の規定や技術・規格の動向	・医療情報連携ネットワークを通じた情報提供について、共同利用型などを想定し、記載を検討する必要がある。	・個人情報保護法等の情報資産管理に関連する法令等の規定や技術・規格の動向を踏まえた考え方や手法の更新があれば、随時検討する。

改定方針に基づく、全体構成の見直し

医療機関等の様々な規模と多様なシステム構成・サービス提供形態を踏まえ、安全な情報資産管理を基礎とし、方針策定・戦略立案（Governance）、運営管理・システム運用（Management）、管理手法・運用手段（Control）の３つの視点で整理してはどうか。

はじめに（概説）Overview	ガイドラインの各編を読むに際して、まずはじめに、前提として必要な知識や各編の基本的な概要をまとめる。	・ガイドラインの目的 ・対象とする情報・文書・システム ・関連する法令等の規定との関係や経緯 ・各編の位置付けと目次構成、概要 等
経営管理 編 Governance	組織の経営方針を策定し、情報化戦略を立案する経営管理層に必要な考え方や関連法制度等をまとめる。	・取り扱う情報の重要性と関連法規 ・情報資産管理や情報システム運用に伴い生じる責任・責務 ・情報システムの有用性と安全管理 等
運用管理 編 Management	経営方針・情報化戦略に基づき、システム利用者・管理者・事業者で情報資産を運営、情報化を管理する考え方や方法論をまとめる。	・情報資産管理体制と責任分界 ・リスクアセスメントと対策 ・情報の種類に応じた管理・監査 ・非常時の対応と非常時への対策 等
管理実装 編 Control	安全な情報資産管理やシステム運用を実現するために、関連法制度を遵守した考え方とその実装手法、活用する技術等、具体的な考え方や技術をまとめる。	・個人情報保護法、e-文書法、電子署名法等により求められる技術 ・システム利用者、クライアント/サーバ/インフラ領域等それぞれで活用する安全管理対策・措置技術 等

別添　Appendix

・Q&A　・用語集
・改定経緯と関連法規の遷移
・5.2版からの遷移
・サイバーセキュリティ対策チェックリスト
・システム障害発生時の対応フローチャート
・医療機関規模別、医療情報システムの構成・形式別で確実に、又は、主に確認すべきガイドライン内の項目まとめ　等

本ガイドラインが準拠する関連法令等の規定を整理し、5.2版からの改定で、混乱や困惑が生じないよう、別添資料を工夫・充実する。

第6.0版 への改定スケジュール(案)

		令和４年 ７月	８月	９月	10月	11月	12月	令和５年 １月
WG	開催			本日 ● 9/5		○		○
作業班	開催	●	●	○	○ ○			○
パブコメ	パブコメ案 作成					→		
	パブコメ 実施						→	
	パブコメ 対応							→
改定								○

※ 現時点での予定

・11月中を目途に、改定(案)を作成予定
・12月中を目途に、パブリックコメントを開始予定
・令和４年度中に、第6.0版を発出し、Q＆A及び
チェックリスト、フローチャート等を改定予定

関連事項

・保健医療福祉分野での電子署名等

環境整備専門家会議

保健医療福祉分野における電子署名等の環境整備

現状・背景

ガイドライン 第5.2版 「6.12. 法令で定められた記名・押印を電子署名で行うことについて」

法令で医師等の国家資格を有する者による作成が求められている文書に対する電子署名として、「保健医療福祉分野PKI認証局の発行する電子証明書（HPKI）」のほか、「適切な外部からの評価を受けた事業者」や「電子的な資格確認に対応した公的個人認証サービス」による電子証明書を用いる方法を整理。

規制改革実施計画（令和４年６月７日 閣議決定）　より抜粋

＜医療・介護・感染症対策＞（２）医療DXの基盤整備（在宅での医療や健康管理の充実）

４．電子処方箋の普及及び医療分野における資格確認・本人確認の円滑化

b）厚生労働省は、電子処方箋の発行に必要な資格確認・本人認証の手段として、HPKI（Healthcare Public Key Infrastructure：保健医療福祉分野の公開鍵基盤）以外にどのような方法があり得るか、医療機関による本人確認の活用やクラウド電子署名など幅広く、現場のニーズを踏まえて検討し、結論を得る。　[措置済み]

e）厚生労働省は、上記bの結論を踏まえ、社会保険診療報酬支払基金が令和５年１月から運用を開始する電子処方箋システムについて、HPKI以外の資格確認・本人認証の方法に運用開始時から対応できるよう検討する。　[引き続き検討を進め、令和５年１月までに措置]

対応方針

- 事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者）による利用者の実在性、本人性及び利用者個人の申請意思の確認並びに当人認証、並びに、医師等の国家資格保有の確認の適切な実施を確保する仕組みが必要。
- 今後の保健医療福祉分野における適切で円滑な電子署名等が可能となる環境整備に当たり、本人確認及び資格確認の適切な実施を公正に評価するための方針・基準・規則等の策定、評価体制等の検討を行う専門家会議を設置。

保健医療福祉分野における電子署名等環境整備専門家会議

（案）

・保健医療福祉分野において、「保健医療福祉分野PKI認証局の発行する電子証明書」(HPKI)以外の電子署名を用いた運用へのニーズを踏まえ、事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者）による利用者の実在性、本人性及び利用者個人の申請意思の確認並びに当人認証、並びに、医師等の国家資格保有状況の確認の適切な実施を確保する仕組みが必要である。

・電子署名に関する技術や制度は、高度かつ専門的であること等から、当該分野の専門家・有識者の意見等を踏まえ、今後の保健医療福祉分野における適切で円滑な電子署名等の環境整備に当たり、本人確認及び資格確認の適切な実施を公正に評価するための方針・基準・規則の策定、評価体制等の検討を行う必要がある。

会議構成

【構成員】

・電子署名等に関する技術面・法律面の専門家・有識者

・保健医療福祉分野における情報セキュリティ有識者

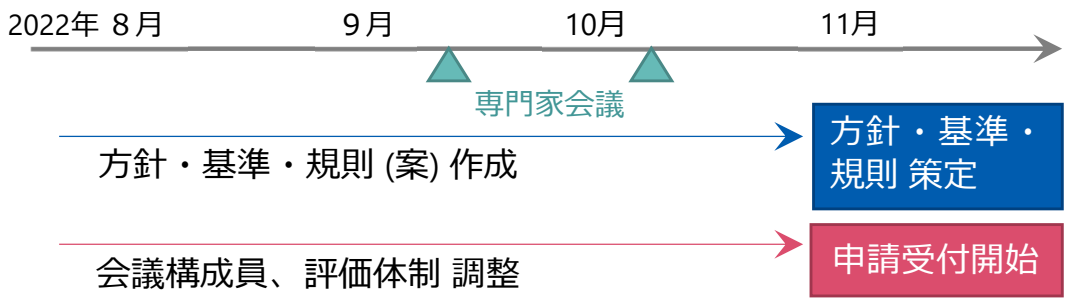
【事務局】

・デジタル庁　デジタル社会共通機能グループ

・厚生労働省

医政局 特定医薬品開発支援・医療情報担当参事官室

予定



検討事項

・外部評価 **方針** の **策定**

保健医療福祉分野における電子署名等サービスを提供予定の新規申請事業者を評価する基準・規則の策定及び評価する体制の整備、並びに、当該評価にて認定された事業者を定期的に評価する基準・規則の策定及び評価する体制の整備に関する指針

・外部（定期）評価 **基準・規則** の **策定**

事業者に対する、新規申請時や定期評価時における、電子署名の方式、電子証明書の発行・管理等の認証業務の評価基準や手順等を具体的にまとめたもの

・外部（定期）評価**体制** の **検討・整備**