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

最終報告書（詳細版）
電子署名法令上の基準のモダナイズの検討

令和 6 年 3 月 22 日

株式会社コスモス・コーポレイション

目次

用語

本報告書では、以下の用語（略称等）を用いる。

・電子署名法： 電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）
・施行規則： 電子署名及び認証業務に関する法律施行規則（平成 13 年総務省、法務省、経済産業省令第 2 号）
・指針： 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（平成 13 年総務省、法務省、経済産業省告示第 2 号）
・方針： 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（デジタル庁デジタル社会共通機能グループ、法務省民事局。令和 3 年 9 月 1 日）
・タイムスタンプ告示： 時刻認証業務の認定に関する規程（令和 3 年外総務省告示第 146 号）
・タイムスタンプ実施要領： 時刻認証業務の認定に関する 実施要項（総務省、令和 3 年 11 月 8 日）
・公的個人認証法： 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（平成 14 年法律第 153 号）
・令和 4 年度報告書： 令和 4 年度電子署名及び認証業務に係る利用促進業務 報告書
・特定認証業務の認定基準に関する調査：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基準に関する調査（令和 4 年度電子署名及び認証業務に係る利用促進業務の一環として行われたもの）
・仕様書： 仕様書（件名：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）
・TF： 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　電子署名法令上の基準のモダナイズの検討タスクフォース
・AATL： Adobe Approved Trust List

電子署名法令上の基準のモダナイズの検討タスクフォースの構成員

	新井　聡	NTT ビジネスソリューションズ株式会社　バリューデザイン部 バリューインテグレーション部門　ソーシャルイノベーション担当 トラストビジネスグループマネージャ
	漆嶌　賢二	GMO グローバルサイン株式会社　事業企画部　部長
	大澤　昭彦	一般財団法人日本情報経済社会推進協会（JIPDEC） デジタルトラスト評価センター　副センター長
	小田嶋　昭浩	株式会社帝国データバンク　プロダクトデザイン部　ネットソリューション課 副課長
	手塚　悟	慶應義塾大学　環境情報学部　教授
	中村　克巳	三菱電機インフォメーションネットワーク株式会社（MIND） シニアプロフェッショナル
	成田　ミキ	一般財団法人日本情報経済社会推進協会（JIPDEC） デジタルトラスト評価センター
	西山　晃	フューチャー・トラスト・ラボ　代表
	濱口　総志	株式会社 コスモス・コーポレイション　取締役
○	宮内　宏	宮内・水町 IT 法律事務所　弁護士

（○：TF リーダー）

1. はじめに

令和 4 年度にデジタル庁が調達した令和 4 年度報告書の一環として、特定認証業務の認定基準に関する調査が実施され、次の 6 つの課題が整理されている。

(1) 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
(2) 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
(3) 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
(4) 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
(5) リモート 署名 に関する規定がないこと
(6) マルウェア 対策に関する規定がないこと

仕様書ではデジタル庁が次の 6 つの点についてモダナイズの必要性を検討することを求めている（これら 6 項目を総称して、以下「本件各課題」という。）。上記(3)については、その内容を二つに区分し、下記(3)(4)として記載されている。

(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

TF では、これらの点についてその詳細を整理した上で、対応の必要性を検討することとした。

2. 優先順位の付け方

2.1 優先順位の考え方

最初に、本件各課題について、検討の必要性等に鑑みて優先順位付けを行う。ここでは、優先順位の設定にあたって、順位付けの考え方を整理する。

まず、電子署名に関するステークホルダーとしては、電子署名の実行者（以下「署名者」という。）、電子署名を用いて真正な成立の推定を得ようとする者（Relying Party のこと。以下「依拠者」

という。）及び事業者（認証局等）がある。

このうち、署名者と依拠者に係る観点が、国民生活（企業等の法人を含む）への寄与が大きい。まず、署名者においては、電子証明書の発行申請・受領及び電子署名実施が容易になることにより、電子署名利用の範囲が拡大し、広い範囲での DX の推進に貢献できる。また、依拠者においては、電子証明書の有効性検証を含む電子署名の検証が重要な観点となる（訴訟における証拠提出との関係については、下記の「補論」で述べる）。一方、ステークホルダーの一翼を担う事業者に係る観点は、事業者に置ける効率性やコストダウンにより、間接的に署名者や依拠者の利益（利用の迅速性、負担の軽減等）につながる。

このような考察により、本報告では、最も重視すべきは国民生活に直接的に寄与する観点であり、それに次いで認証局を含む事業者へのメリットを重視すべきだと位置づけた。

なお、一般的なアプリケーションを用いることによる、電子署名の正当性検証が可能なことは、訴訟等を意識した国民生活において重要な観点となる。この意味で AATL との関係は、取り上げる意義のある観点であると考えられる。この他にも、第 1 章に上げた各観点以外に、重要な観点がある。

したがって、本報告書では、第 1 章で示した 6 つの観点について優先順位付けを行うが、優先順位の低いものについても、検討を行う。また、これらの観点以外についても、重要なものについては、「その他」として検討することとする。

補論「訴訟への証拠提出との関係」

訴訟に証拠として提出する際には、電子署名法第 3 条による真正な成立の推定を容易に得られるかどうかが重要な論点になる。ここで、署名への押印における二段の推定の一段目（本人の印章により顕出された印影により、本人による押印を推定する）に相当する枠組みが存在しないため、

何を用意すれば「本人による電子署名」と認められるか

につき、訴訟当事者において考えなければならないのが現状である。

電子署名法においては、特定認証業務の認定の制度を規定しているが、かかる認定が行われた認証局が発行する電子証明書であっても、特別な法的効果は規定されていない。その一方で、電子署名の検証は、実務的には Adobe Reader 等の広く普及したアプリケーションで行われており、かかるアプリケーションで正当性が検証されることが、実際上の有効性の確認として用いられているため、訴訟においても重視される可能性が高い。こうした現状に鑑みると、次の 2 点についての検討が必要だと思われる。

(1) 認定認証業務が発行した電子証明書に基づく電子署名であれば、本人による電子署名であると認めるべきかどうか。また、他の要件（署名生成装置の利用など）を設けるべきかどうか。

(2) 認定認証業務が発行した電子証明書に基づく電子署名であれば、一般的なアプリケーションでの正当性確認が可能になるべきかどうか。

このうち(1)については、実現のためには法令で規定する必要のある内容であって、電子署名法の

考え方を変革するようなものであるため、短期間で実現できるものではない。これは、中期的な課題であると考えられる。一方(2)は、認定基準の変更により、認定認証業務であれば、一般的なアプリケーションでの正当性検証が可能となるようにすることが可能であると考えられる。本報告においては、(2)の意味から、AATL への対応を一つの重要な観点として取り上げることにする。

2.2 優先順位の設定

上記の考え方に基づいて、本件各課題に対して、以下の方法で優先度をつけた。

1. 国民生活への寄与について、大、中、小の三段階に振り分け、優先順位を決める
2. 同じ優先順位となったものについて、さらに事業者へのメリットという観点で重みづけを行う

モダナイズが必要とされる観点	国民生活への寄与	事業者へのメリット	優先順位
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	大	－	1
認証局の秘密鍵を管理する暗号装置の技術基準の更新	大	－	1
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	小	○	5
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	小	○	5
利用者の真偽の確認における自動化の規定	中	○	3

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	中	－	4

3. 各観点に係る改訂骨子案

本章では、本件各課題について、令和４年度報告書において示された主なコメント、特定認証業務の認定基準に関する調査で示された課題、TF での整理及び法令改正の骨子について示す。なお、2.1 にて述べたとおり、優先順位の低い課題についても検討を行う他、本件各課題に示されていないものであっても重要な課題を取り上げることとする。

3.1 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

3.1.1 令和４年度報告書における認定認証事業者からの主なコメント

必要	不要	どちらでもない
・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。ただし、さらなる設備投資と更新調査費の増大は懸念材料。ISMS を取得していることで、リスクマネジメントがなされていると認められることが望ましい。 ・無条件に認証の取得を義務づけるのではなく、事業者によるリスク評価の結果を加味する考え方も必要。	・必要であれば別途これを満たすよう努めるべきであり、その概念の全部もしくは大部分を電子署名法に融合させる必要はない。	・単純にリスクマネジメントの実施の有無が規定に追加されることは本質ではない。

3.1.2 特定認証業務の認定基準に関する調査で示された課題

以下の様に課題が整理されている。

(1) 電子署名法の制定時において、まだ一般的に認識されていなかった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含まれていない。

(2) 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。

(3) 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（ISO/IEC 27001 に基づく ISMS など）の概念を盛り込むべきではないか。

3.1.3 TF での整理

(1) リスクマネジメントの概念がないという言い方であるが、ここでは単純にリスクを評価せよと言うだけで解決するものではない。各認証事業者がリスクアセスメントを実施して、認証事業者自身が、そのリスクアセスメントの結果に基づいて、セキュリティ管理対策（例えば、脆弱性対策において、インターネット上でサービスを提供する一般的なサービス事業者と最初から発行者署名符号を厳重に管理するためにインターネット上に公開することなく、場合によりオフラインで管理する認証業務用設備とでは、認証事業者のセキュリティ対策の取り方に大きな差が出る）を決定することを認めることが必要となる。例えば、ETSI EN 319 401「5.Risk Assessment」が参考となる。

(2) 認証業務における代表的なリスク（電子証明書の誤発行、情報漏洩、CA 鍵の危殆化、リポジトリーの停止、災害発生等）の定義の共通化が必要か。

(3) AATL 対応の一環としての視点も必要ではないか。

3.1.4 改正の骨子

リスクアセスメントについては法律に規定がないため、電子署名法第 6 条第 1 項にリスクアセスメントについて項目を加える方法が直截（ちょくせつ）的ではあるが、同項第 3 号（「前号に定めるもののほか」の一環として）に関する施行規則の条項として追加することも可能であると考えられる。

電子署名法

（認定の基準）

第六条　主務大臣は、第四条第一項の認定の申請が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　申請に係る業務における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

（その他の業務の方法）

第六条

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

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、以下の事項を含むものをいう。

法令改正の骨子案

案１

リスクマネジメントの電子署名法第 6 条に「第 2 号の 2」として次の内容の条項を追加する。（又は、これを第 3 号とし、現在の第 3 号を第 4 号に繰り下げる）

電子署名法第 6 条 二の二　申請に係る業務における危険の評価，管理等が、主務省令で定める基準に適合すること。

この場合、電子署名法施行規則第 6 条の次に，第 6 条の 2 として，リスクマネジメントに関する条項を追加する。追加の内容は，案 2 に記載するものと同じである。

案２

電子署名法第 6 条は変更せず，同条第 3 号の一環としてリスクマネジメントを扱う。リスクマネジメントの内容を規定するため，同法施行規則第 6 条第 1 項に新たな「号」を追加する，又は，新たな第 6 条第 1 項第 15 号トの一環としてリスクマネジメントをとらえ，方針に関連する条項を追加することが考えられる。

案２－１ 施行規則の第 6 条第 15 号の次に新しい号を加え、危険の評価、管理等の詳細は，方針に記載する。

電子署名法施行規則第 6 条 十五の二 認証業務に係る危険の評価，管理等を適切に行うこと。

案２－２ 施行規則第 6 条第 1 項第 15 号ト（危機管理に関する事項）の一環として取扱い，具体的

な内容は，「方針」に記載する。

方針の改正

案１，案２－１，案２－２のいずれであっても，リスクマネジメントの具体的内容（下記）は，方針に記載されることになる（方針の既存の条項に記載を追加するか，条項を追加するかは，案によって異なるが，内容は同じである)。たとえば、第４　８(4)として、次の内容を記載する。

方針 第４　８ (4) 規則第 6 条第 15 号の 2 に定める「危険の評価、管理等」には、リスクマネジメントに関する以下の事項を含むものとする。 ア 認証業務のリスクを特定、分析、評価するためのリスクアセスメントを行うこと。 イ リスクアセスメントの結果を考慮して、適切なリスク対応策をとること。 ウ リスク対応策を実装するためのセキュリティ要件と運用手順を決定すること。 エ リスクアセスメントを定期的に見直し、改訂すること。 オ リスクアセスメントに求められる力量を適切な教育、訓練及び経験に基づいて定め、その力量を有する者によりリスクアセスメントが行われること。 カ リスクアセスメントの結果を考慮して、認証業務用設備および登録用端末設備のシステムとネットワークに分割し、侵入テスト、ウィルス対策、マルウェア対策、脆弱性診断を行うこと。 キ 必要に応じてセキュリティパッチを適用すること。 ク 重大な脆弱性を発見した場合、遅滞なく対処すること。 ケ あらゆる脆弱性について、潜在的な影響を考慮して、脆弱性を軽減する計画を作成して実装するか、脆弱性は修復する必要がないと判断した事実に基づく根拠を記録すること。

以下は、参照した基準（ETSI EN 319 401 V2.3.1 (2021-05) General Policy Requirements for Trust Service Providers）である。なお REQ-5-02 で指示されている ISO/IEC 27005:2011 は ISO/IEC 27005:2018 と読み替えられる必要がある。

ETSI EN 319 401 V2.3.1 (2021-05) General Policy Requirements for Trust Service Providers	
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 27005:2011 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.*
• REQ-7.2-13	*Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.*
REQ-7.6-01	*The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security.*
• REQ-7.7-09	*The TSP shall specify and apply procedures for ensuring that:* *a) security patches are applied within a reasonable time after they come available;* *b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and* *c) the reasons for not applying any security patches are documented.* *NOTE 5: Further specific recommendations are given in the CA/Browser Forum network security guide [i.7], item 1 l.*
• REQ-7.8-02	*The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.*
• REQ-7.8-13	*The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.*
• REQ-7.8-14	*The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.*
• REQ-7.9-10	*The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.*
• REQ-7.9-11	*For any vulnerability, given the potential impact, the TSP shall [CHOICE]:* *- create and implement a plan to mitigate the vulnerability; or* *- document the factual basis for the TSP's determination that the vulnerability does not require remediation.* *EXAMPLE: The TSP can determine that the vulnerability does not require remediation when the cost of the potential impact does not warrant the cost of mitigation.* *NOTE 4: Further recommendations are given in the CA/Browser Forum network security guide [i.7] item 4 f).*

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

3.2.1 令和４年度報告書における主なコメント

必要	不要	どちらでもない
・秘密鍵を管理する装置の技術基準をアップデートすることに賛成。 **・技術基準については、FIPS だけでなくコモンクライテリアや JCMVP など、複数の技術基準が参照できる状態が望ましい。** ・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。	－	・事業継続の観点で採用可能な基準であることを前提に検討頂きたい。 ・HSM との接続がネットワーク経由である場合（Cloud 環境利用の場合も含む）も考慮いただきたい。

3.2.2 特定認証業務の認定基準に関する調査で示された課題

以下の様に整理されている。

(1) 「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」（主務省庁局長級通知）において規定された、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。

(2) 国内の認証事業者のほとんどが、FIPS 140-2 以上の基準に適合する暗号装置を設置・運用しているが、国際的には、既に FIPS 140-3（ISO/IEC 19790:2012 及び ISO/IEC 24759:2017 に準拠）に移行しつつある。

(3) また、近年、クラウドサービスを活用するケースも散見される。このため、認証局の秘密鍵を管理する暗号装置（HSM）に対する基準を見直すべきではないか。

3.2.3 TF での整理

国際的な基準の同等性という観点では、FIPS140-2 レベル 3、或いはそれ以上の CC（コモンクライテリア）が必要となっている。

JDTF の AATL 認証 TF では、現状の手法として調査表の適合例を満たすことで FIPS140-2 相当と確認ができ、それにより認定が取得できる手法を踏襲できるよう、FIPS140-2 の「4. SECURITY REQUIREMENTS」の内容を調査表の項目に取り込むことにより、相当ではなく、同等（equivalent）と出来るようにすることを検討したが、「4. SECURITY REQUIREMENTS」の内容が非常に細かく、詳細、かつレベル 1 ～レベル 4 毎に要件がマトリックス状になっているため、調査表に入れ込むのは非常に難しい。例え出来たとしても、内容があまりに複雑なため FIPS140-2 の認定に委ねることでも大差ないことが判明し、断念している。

既に、FIPS 140-2 について、新規の認定申請受付は終了しており、2026/9/22 には、すべての認定が historical list 入りとなる為、2026 年までに調査表の HSM の要求事項について、FIPS 140-3 と同等の表現にすべき。

現行の方針 第２　2.(2)は削除すべきである。削除理由は，(1)の内容（暗号装置に必要な機能）との同等性について指定調査機関において評価を実施するのは困難であると考えられるためである。また、(2)による対策は，海外の基準との乖離が大きいことも挙げられる。

3.2.4 改正の骨子

現行の方針 第２　2.を次のものに置き替える。

(1) 認証局の秘密鍵を管理する暗号装置については、FIPS140-2、ISO/IEC 15408(EAL4+)或いは、これらと同等の技術基準に対して信頼できる第三者によるセキュリティ評価を受けた暗号装置を用いること。

また、上述のとおり、現行の方針第 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）は削除する。

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

3.3.1 令和 4 年度報告書における主なコメント

令和 4 年度報告書「(3) 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」における課題について、仕様書では「(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」及び「(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」の 2 項目が割り当てられた。本節では、電子証明書の発行に関する機能、とりわけ、発行者署名符号の管理に焦点をあてて論じる。

次に掲げる、令和 4 年度報告書における主なコメントは、同報告書の(3)に対するものである。このコメントは、3.4 節においても参照することにする。

必要	不要	どちらでもない
・遠隔操作の環境が適切に保たれているか、といった観点での確認が増える事やパブリッククラウド側で構築する際に取る措置についての変更や更新認定時調査をどのように進めるのかといったことが懸念。 ・保守作業やリリース作業等の利便性向上が期待できる。リモートアクセスを採用できないことがテレワーク導入の障壁にもなっており、緩和が望ましい。 ・パブリッククラウド利用が認可されるべき。同時に遠隔操作についても認められるべき。ドキュメント保管もネットワーク保管（Cloud 利用）も認められるべき。	－	・IA サーバのセキュリティを確保する観点から遠隔での操作はできないようにするべき。IA サーバについてパブリッククラウドは適用できない認識。

3.3.2 特定認証業務の認定基準に関する調査で示された課題

以下の様に整理されている。

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。

これに関しては、電子署名法施行規則第 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。

電子署名法施行規則
第六条　法第六条第一項第三号の主務省令で定める基準は、次のとおりとする。
（1号～16号を省略）
十七　複数の者による発行者署名符号の作成及び管理その他当該発行者署名符号の漏えいを防止するために必要な措置が講じられていること。

指針

第十四条 規則第六条第十七号に規定する発行者署名符号の漏えいを防止するために必要な措置とは、次の各号に掲げる要件を満たすものをいうものとする。

一 発行者署名符号の生成及び管理は、認証設備室内で複数の者によって規則第四条第四号に規定する専用の電子計算機を用いて行われること。

（2 号以下を省略）

3.3.3 TF における整理

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する（ただし、後述のように、クラウド HSM 等の利用については検討を要する）。但し、認証業務用設備とは異なり、帳簿書類のファイル管理やフィンガープリント等のデータを公開するリポジトリサーバに係る設備は、パブリッククラウドの利用を認めるような明確な基準を検討する。

クラウド HSM であるというだけの理由で、不適合とはなるべきではない。クラウドであっても方針に示される項目（ハードウェアの管理体制等）に対して審査が出来れば良いと考えられる。

パブリッククラウドに関連する検討項目の中で、どのような設備であれば認証設備室でなければならないか、パブリッククラウドへの設置でも良いかの基準を明確にする検討項目として、項番 3 に分けた意図と認識する。

補論：「クラウド HSM についての考え方」

パブリッククラウドの事業者が提供するクラウド HSM は、Web サイト上に”HSMs are FIPS 140-2 level-3 validated”のような、ハードウェアのセキュリティ基準に関する記載がなされていたり、或いは同じ内容をドキュメント化した”AWS CloudHSM User Guide[1]”などの詳細な技術文書が公開され、この中には実際に使用している HSM の機種名、FIPS 認定番号等も明記されている。これらの技術文書の提示をもって、「調査可能な状態」と判断することも考えられる。一方、そのような技術情報だけではなく、発行者署名符号 CA 秘密鍵を生成し、セキュアに保管する HSM の調査に当たっては、実際に認定調査の時点で正に使用されている HSM のステータスを確認する手段として、ファームウェアのバージョン番号の確認までを実地で確認している現在の調査手法を要件とするという考え方も、絶対的なセキュリティ基準の維持という観点では非常に重要な要素であり、否定し切れるものではない。

なお、これらのクラウド HSM は必要に応じて柔軟に HSM を追加、削除が可能となっているが、その課金体系は時間単位での支払いとなっている。不要な時には時間単位で HSM をバックアップ

して、シャットダウンすることでコストを下げられることを売りにしている。然るに、国内の認定認証事業者はルート CA が発行 CA という構造を取り、発行 CA は CRL への署名に毎日使用する必要があるため、発行者署名符号 CA 秘密鍵をシャットダウンすることは難しく、コスト削減策は取れない可能性がある。特に発行者署名符号 CA 秘密鍵の活性化／非活性化は鍵管理者の複数人／多要素認証等で切り替えるべきで、タスクスケジューリングして自動切替えはあり得ないと考えられることがこれを難しくしている。

3.3.4 改正の骨子

施行規則第 4 条第 4 号にかかる方針第２　２の改正が必要となる。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と思われる。具体的には，たとえば、(2)【2.4 の改正を行わない場合には(3)】を追加し，次の内容を記載する。HSM 等を認証設備室以外の場所への設置については、設置の可能性を示す文言として「認証設備室に置かれるか否かにかかわらず」を入れてあるが、この採否については、なお検討が必要である。

(2) 暗号装置は，***認証設備室に置かれるか否かにかかわらず***，(1) 【及び(2】を満たし調査可能であることが条件となる。たとえば，クラウドでアクセス可能な HSM をネットワークを介して利用する場合，HSM の物理的管理体制等が調査可能な状態でなければならない。

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

3.4.1 令和 4 年度報告書における主なコメント

前述のとおり、令和 4 年度報告書「(3) 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」における課題について、今回の報告書では「(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」及び「(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」の 2 項目が割り当てられた。本節では、電子証明書発行機能（発行者署名符号の管理など）以外の機能について、パブリッククラウドの利用の可能性を論じる。

次に掲げる、令和 4 年度報告書における主なコメントは、同報告書の(3)に対するものである。このコメントは、3.3 節において参照したもの同じである。

必要	不要	どちらでもない
・遠隔操作の環境が適切に保たれているか、といった観点での確認が増える事やパブリッククラウド側で構築する措置についての変更や更新認定	－	・IA サーバのセキュリティを確保する観点から遠隔での操作はできないようにするべき。IA サーバについてパブリッククラウドは適用できない

時調査をどのように進めるのかといったことが懸念。 ・保守作業やリリース作業等の利便性向上が期待できる。リモートアクセスを採用できないことがテレワーク導入の障壁にもなっており、緩和が望ましい。 ・パブリッククラウド利用が認可されるべき。同時に遠隔操作についても認められるべき。ドキュメント保管もネットワーク保管（Cloud利用）も認められるべき。		認識。

3.4.2 特定認証業務の認定基準に関する調査で示された課題

以下の様に整理されている。

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、以下の規定によって、基準に適合しないと解釈される。

(1) 指針について

指針第 6 条第 1 項第 3 号の規定に基づき、電気通信回線経由の遠隔操作が不可能であるように設定されていなければならないこと。認証設備室の中に設置された各種サーバ類の日常のメンテナンスが同一建屋内の要員の居室からでさえも行えないことから、操作要員の作業が煩雑であることに加えて、新型コロナウイルス対策等としてのテレワークが実施できないといった問題も想定される。このため、認証設備室の外からの遠隔操作については、認証業務用設備のクリティカル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、認められるべきではないか。

また、帳簿書類に関するデータのファイル管理のためのサーバや、認証局の特定のためのフィンガープリントのデータ公開のための Web サーバについても、パブリッククラウドサービス等の利用が 認められないと解釈されている。

(2) 施行規則について

施行規則第 6 条第 15 号に基づき、「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 12 条第 1 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」が求められる。

➡パブリッククラウドサービスの利用については、記載されていない。

(3) 電子署名法について

指針第 10 条第 2 号に基づき、認定認証事業者は「発行者署名検証符号に係る電子証明書の値を・・・変換した値によって認定認証業務を特定すること」が求められている。

➡「特定認証業務の認定に係る調査表」の適合例に基づき、フィンガープリントの記録及び改ざん防止措置を講じた Web 公開を確認しているが、オンプレミスの Web サーバ以外は認められないと解釈されてきた。

3.4.3 TF における整理

認証業務用設備の操作による電子証明書の発行や、失効等の直接の操作ではなく、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いては、遠隔操作を認めるような基準を検討する。

以下の検討ではパブリッククラウドが登場しているが、あくまでもそのようなメンテナンス作業に関連する場合のログやデータの保管場所として、パブリッククラウドの利用を可能とするような基準を検討することの例として扱う。

3.4.3.1 用語の整理

以下の表に電子署名法が定義する認証業務で使用するコンピュータやネットワーク関連設備の名称とその設備の具体例をまとめている。これに、TF における整理でクラウドでの利用の可能性が考えられる設備に対して、その名称を規定し、その設備の定義と具体的な設備の例をまとめている。この定義にあたっては、トラストサービスに係る専門用語を使った定義が必要になるため、その専門用語に関する用語説明を出典と共に示している。

設備の名称	定義	設備の例
認証業務用設備	高セキュリティ・ゾーンに設置されている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
登録用端末設備	セキュアゾーンに設置され、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	セキュアゾーンに設置され、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	セキュアゾーンに設置され、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
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（フロントエンド / インターナルサポートシステム）	利用申込書情報入力 Web システム
リポジトリー設備	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	Web サーバ，LDAP サーバ，

	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（フロントエンド / インターナルサポートシステム）	
保守用設備	各種システム保守作業に使用する主にテキストベースの入力を行う操作端末	ダム端末（Dumb Terminal），PC（RS-232C，IBM3270/5250 エミュレータ），管理コンソール（X 端末),
ネットワーク機器	ネットワークを構築する為の各種の機器	ファイアウォール，IPS，IDS，ネットワークルーター，ネットワークスイッチ，スイッチング Hub

用語説明

【"Network and Certificate System Security Requirements Version1.7"[2]の Definitions によるもの】

高セキュリティ・ゾーン：認証局または委任を受けた第三者の、秘密鍵または暗号ハードウェアが設置されている物理的な領域。

セキュアゾーン：証明書システムの機密性、完全性、及び可用性を適切に保護する物理的及び論理的管理によって 保護される領域（物理的または論理的)。

証明書管理システム：CA または委任された第三者が、証明書または証明書のステータス情報を処理、発行承認、または保存するために使用する、データベース、データベース・サーバー、ストレージを含むシステム。

証明書システム：本人確認、登録、加入、証明書の承認、発行、有効性ステータス、サポート、およびその他の PKI 関連サービスを提供する際に CA または委任されたサードパーティが使用するシステム。

フロントエンド / インターナルサポートシステム: ウェブサーバー、メールサーバー、DNS サーバ、ジャンプホスト、認証サーバなど、パブリック IP アドレスを持つシステム。

【"Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificate Version2.0.1"[3]の Definitions によるもの】

[2] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Guidelines-v1.7.pdf

[3] https:// https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-v2.0.1.pdf

リポジトリ：情報**開示**された PKI 運用を統制する公開文書（証明書ポリシー、および認証業務運用規程など)、および CRL または OCSP レスポンス形式の証明書ステータス情報を含むオンライン・データベース。

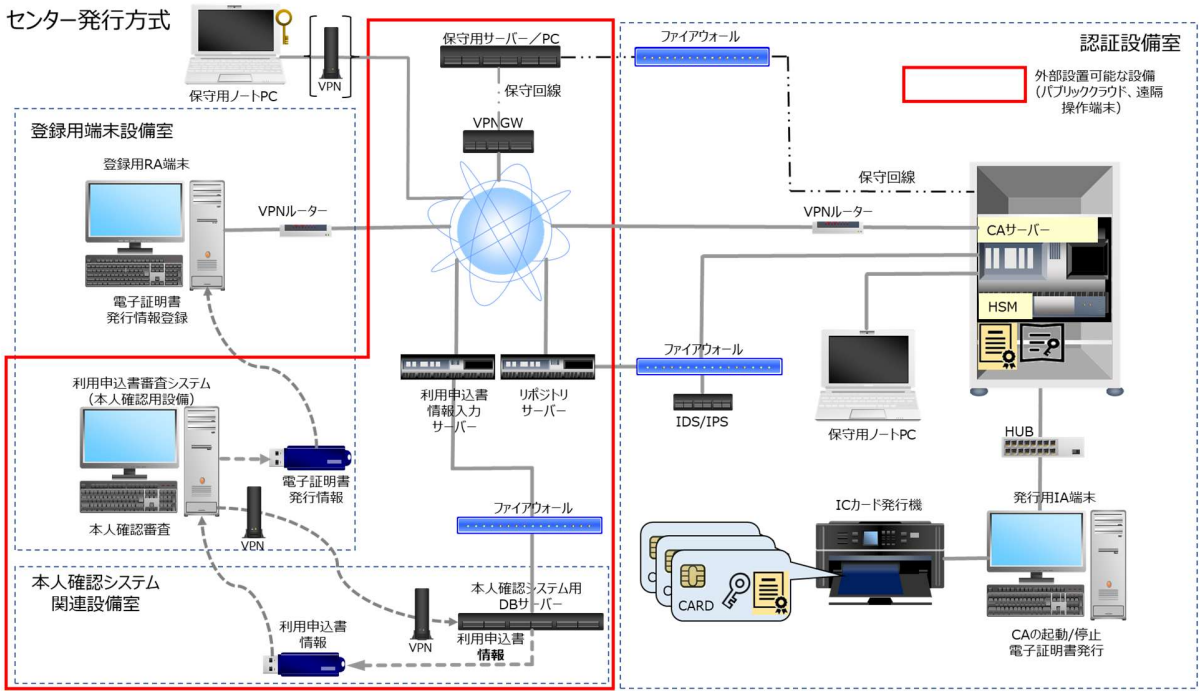
3.4.3.2 認証局システムの構成例

現在の電子署名法に基づく認定認証業務において運用されている認定認証事業者が実施している代表的な認証局システムのシステム構成例を次ページ以降に示す。

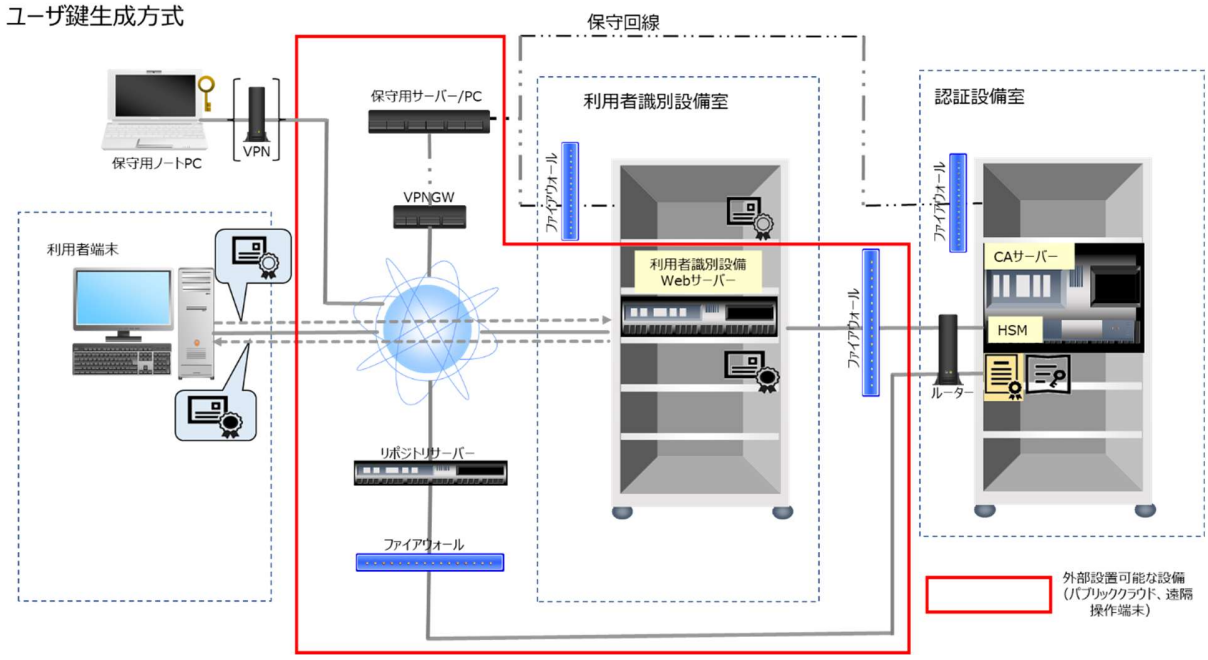
電子署名法では、利用者署名符号を認証事業者が作成する場合と、利用者自身が作成する場合を規定している（同法施行規則第 6 条第 3 号及び第 3 号の 2)。また、利用者署名符号を認証事業者が作成する場合において、発行者署名符号を生成し、専用ハードウェアで保管して、利用者署名符号への電子署名を付与する部分だけに特化して外部委託を受ける事業者を利用するモデルが広く使われているので、これを MPKI 発行方式として例示に追加した。更に、マイナンバーカードを使用したオンラインによる本人確認を実施する事業者も登場しているので、これも併せて例示した。

なお、図中の赤線は、設備についての外部設置可能範囲の提案である。外部設置可能範囲についての詳細は 3.4.3.4 で論じる。

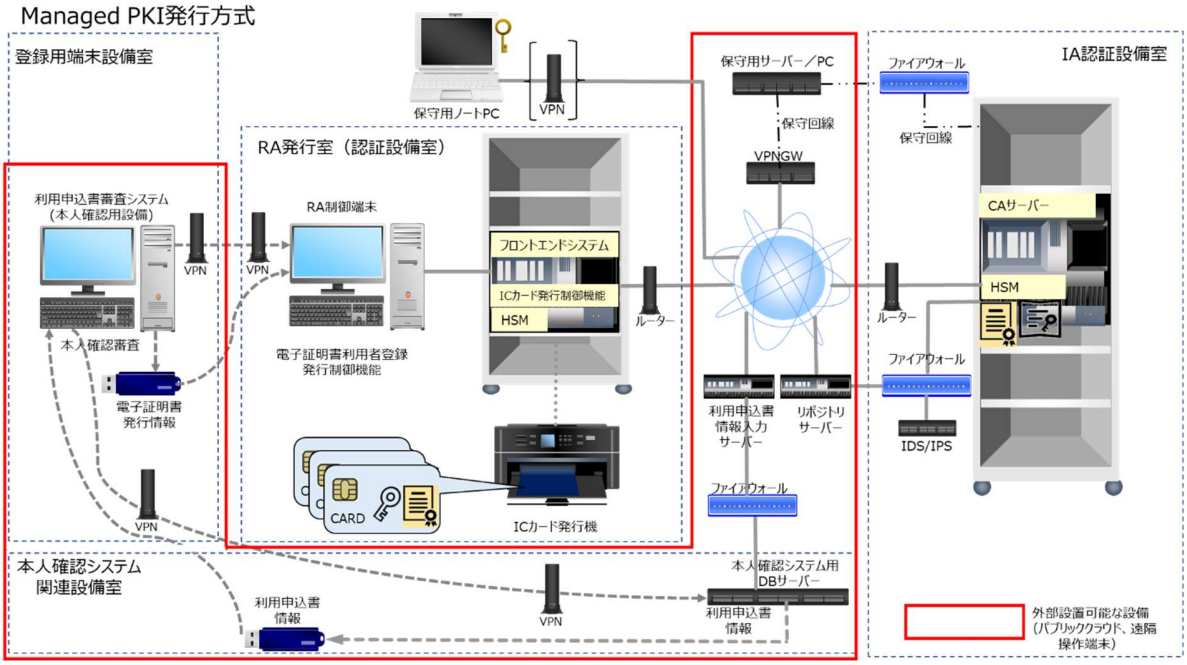
(1) センター発行方式



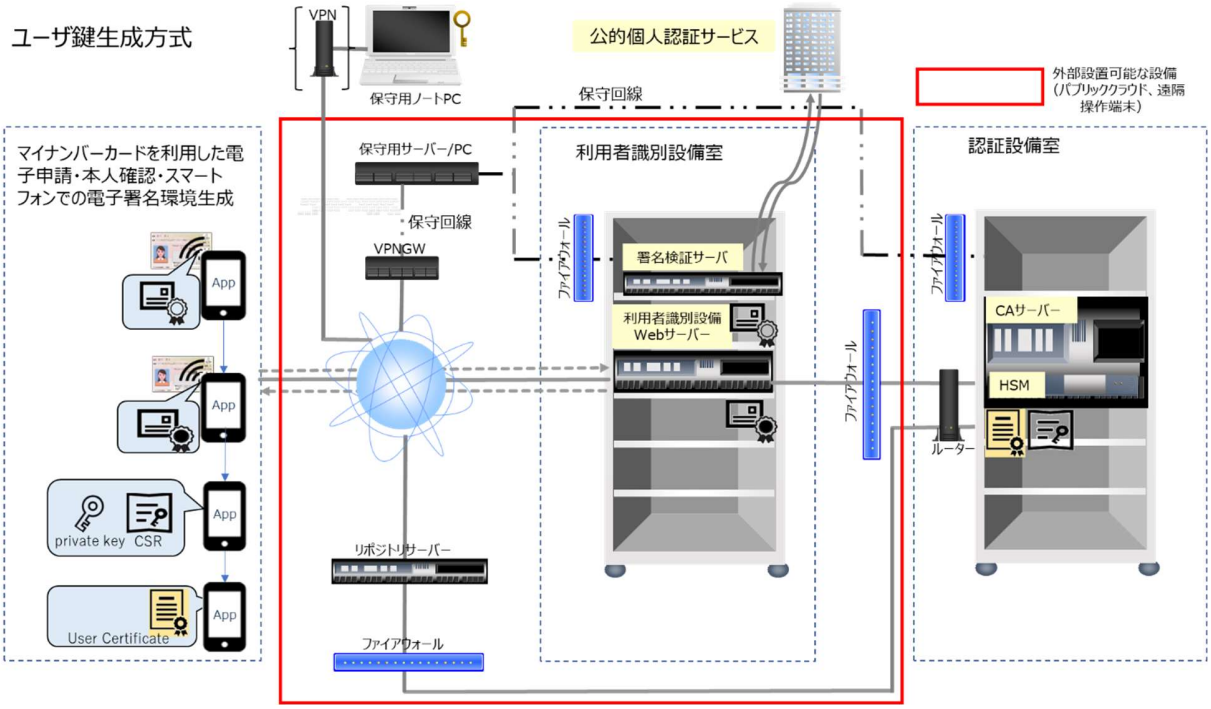
(2) ユーザー側鍵ペア生成方式



(3)MPKI 発行方式（IA 外部委託方式）



(4)マイナンバーカードを利用した発行方式



3.4.3.3 クラウド利用、遠隔操作に関する考察

3.4.3.2(1)～(4)は、電子署名法に基づく認定認証業務における代表的な認証局システムのシステム構成例である。このシステム構成例に基づいて、認証業務で利用される認証業務用設備を始めとする設備が認証業務で利用されるネットワークを含めたシステム構成上のいずれの領域に設置されるべきものか、或いはそれぞれのシステムへのアクセス制御の方法などのモデル化を試みる。

基本的には、「高セキュリティ・ゾーンに設置される発行者署名符号または暗号ハードウェアを持つ設備」、及び「セキュアゾーンに設置される発行者署名符号に対する操作が可能な設備」については、一切のクラウド利用を禁止するという原則をおく。

リポジトリサーバがクラウド上で認証局運用規程（CP/CPS）やCA証明書などを公開する情報公開サーバとして」機能する場合には、幾つかのパブリッククラウドは CDN（Contents Delivery Network）として、負荷分散した可用性の高い実装とすることも可能となっている。また、電子証明書の失効情報を公開する場合には、CRL を公開する方式と OCSP レスポンダと呼ばれる方式がある。いずれの方法による失効情報の公開においても情報公開用のサーバをパブリッククラウドに置くことにより、その可用性の利点を享受することが可能となると考えられる。

更に、パブリッククラウドは、そのオプション機能としてネットワーク機器、ファイアウォールシステム、IDS（不正侵入検知システム）、或いは IPS（不正侵入防止システム）など高いセキュリティ機能を提供するものがあり、これらのネットワーク機能を活用することも可能と考えられる。

なお、日本の電子署名法に基づく認定認証業務の CA は、その認定基準や政府認証基盤（GPKI）の相互認証基準に基づき、eIDAS や AATL の定める個別ルート CA の階層構造ではなく、基本的にルート CA かつ発行 CA で高セキュリティゾーンに配置される前提 となっている。将来的に、この前提が変更される場合においては、近年、活用が進んでいるゼロトラストセキュリティに基づくEDR(Endpoint Detection and Response)といった高度なセキュリティ対策も有効となると考えられる。

3.4.3.4 外部設置可能範囲の考え方

以上の考察に基づいて、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の Web サーバとして実装されるシステム／設備など一部のシステムについては、セキュアゾーン設置のものと定義されるものであっても、パブリッククラウドのセキュリティ施策を活用することで一定のセキュリティの確保が可能とみなし、クラウド設置が可能なものと分類した。また、利用者情報入力設備に入力された利用者の個人情報は、Web サーバ上に保持する実装はないと考えられ、別の本人確認データを保管する DB サーバに転送することが考えられる。また、それを使って本人確認審査を行う本人確認審査システム用 DB サーバについてもクラウド利用が可能とすることで BCP 対策として可用性の高いシステムが実現可能となる。

このような考え方にしたがって、(1)～(4)の図中、パブリッククラウドへの設置が可能な設備を赤枠で示した。

なお、3.4.3.2(4)においては、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をパブリッククラウドに設置することを可能とすることを提案するものとした。その理由としては、署名検証システムは、既に送られて来ている電子証明書の情報に基づいて、当該電子証明書による電子署名のパス検証を行い、その結果を返すものにすぎないことと、パブリッククラウドがもたらすシステムの可用性による BCP 対策等の利点とが挙げられる。ただし、現段階においては、マイナンバーカードの署名検証を行うプラットフォーム事業者の認定要件においては、オンプレの署名検証サーバが求められているため、現行法令には合致しない点があることに注意が必要である。

3.4.3.5 外部設置可能範囲についてのまとめ

ここまで、パブリッククラウドサービス、及びプライベートクラウドサービスの利用可否について述べてきたが、最初に述べた通り、利用可能と判断できるのは、あくまでも発行者署名符号 CA 秘密鍵または暗号ハードウェアを持つ設備、発行者署名符号 CA 秘密鍵に対する直接の操作が可能な認証業務用設備や登録用端末設備については、クラウド利用を禁止するという原則に基づくものである。これら以外の設備については、該当するクラウドサービスの技術情報の開示のレベルを判断材料として、適用可能性の検討を進めるものと考える。

一方、保守用設備による遠隔操作については、閉域網の IP-VPN や、インターネット VPN サービスを使用する等、一定のセキュリティが確保される前提で、高セキュリティ・ゾーンへのアクセスも可能なものとする。但し、その操作については CA システムの実行状況を確認（例として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禁止とする。これは電子証明書の発行のみならず、発行者署名符号の活性化／非活性化など起動／再起動の操作を含む。

パブリッククラウドを活用する場合についての、指定調査機関等が認定調査を実施における従来と異なる点を指摘しておく。

実施にあたって、クラウドサービス事業者の設置場所や技術面の開示における機密上の問題、或いはクラウドシステムの耐障害性と安定性を得るためのリージョン、アベイラビリティーゾーン（以下、補論「リージョンとアベイラビリティーゾーン」を参照）と呼ばれる複数の地域を定められた時間やスループットで切り替えて利用可能とする機能により、実地に於ける実体の調査が困難、不可能となることも考えられる。パブリッククラウドが開示している情報のレベルを整理して、適用可能性を検討していくことも必要となると思われる。

なお、指定調査機関等が認定調査を実施する場合は、クラウドサービス事業者から提供されるレポートを確認し、判断することも可能と想定される。これまでの議論では、ワールドワイドの利用を前提とした、比較的技術情報を広くWeb サイト上に公開している、いわゆるパブリッククラウドを中心に記載しているが、指定調査機関等に対して、機密情報の開示を行ない、適合性評価に必要な技術情報を提供できるのでれば、プライベートクラウドサービスと分類されるサービスの活用を否定するものではなく、いずれのサービスの活用においても技術情報の開示のレベルが適用可能性

の判断材料となると考えられる。

補論：「リージョンとアベイラビリティーゾーン」

代表的なパブリッククラウドサービスでは、提供するデータセンターの地域や場所を定義するリージョンとアベイラビリティーゾーンという 2 種類の地域的境界を定義している。複数のデータセンターが配置されるワールドワイドの物理的な場所をリージョンと定義し、更にそのリージョンの中に最低でも 3 つ程度の論理的なアベイラビリティーゾーンという論理的なデータセンターのグループを配置するとしている。それぞれのアベイラビリティーゾーンは地理的にも切り離された冗長的な電源、ネットワーク、相互間の接続機能を個別に持ち、それぞれの間で定められた応答時間やスループットを保証して切り替えられるようになっており、ソフトウェアやハードウェアの障害や地震、水害、火災などの自然災害による事象において、高い可用性、耐障害性、拡張性を備えた運用が可能なように構成されている。このため、実地調査において、この論理的なデータセンターの存在が前提の場合、その時点における有効な実体が何処にあるのかの定義が難しく、その実体調査が困難、或いは不可能と言うことが起こり得る。その対応で論理的なデータセンターの全ての調査をする場合を考えた場合、移動距離や時間、移動コストを考えた場合の認定調査費用の高騰という問題も出てくる。

なお、リージョン、及びアベイラビリティーゾーンの詳細は以下から引用したものである。

「リージョンとアベイラビリティーゾーン」

https://aws.amazon.com/jp/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2

「Azure リージョンと可用性ゾーンとは」

https://learn.microsoft.com/ja-jp/azure/reliability/availability-zones-overview

3.4.4 改正の骨子

設備のパブリッククラウドへの適用反映箇所としては、指針第 4 条第 2 号、第 5 条および第 6 条第 1 項第 2 号が挙げられる。が挙げられる。

（認証設備室への入出場を管理するために必要な措置） （指針第 4 条第 2 号） 登録用端末設備又は利用者識別設備が設置された室であって、認証設備室に該当しないもの　関係者以外が容易に登録用端末設備又は利用者識別設備又は本人確認用設備、利用申込用利用者情報入力設備、リポジトリー設備、保守用設備、ネットワーク機器に触れることができないようにするための施錠等の措置が講じられていること。但し、管理体制等が調査可能な状態であるクラウドサービスの利用を妨げられるものではない。

（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）

（指針第５条）規則第４条第２号に規定する電気通信回線を通じた不正なアクセス等を防止するために必要な措置とは、次の各号に掲げるものをいうものとする。但し、管理体制等が調査可能な状態であるクラウドサービスの利用を妨げられるものではない。

１ 認証業務用設備が電気通信回線に接続している場合においては、認証業務用設備（登録用端末設備を除く。）に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するためのファイアウォール及び不正なアクセス等を検知するシステムを備えること。

２ 認証業務用設備が二以上の部分から構成される場合においては、一の部分から他の部分への通信に関し、送信をした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

（指針第６条第１項第２号）

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は、各利用者に対する利用者識別符号の設定、利用者署名検証符号、利用者情報及び当該利用者識別符号を電気通信回線を通じて受信するために用いられる電子計算機（施錠等の措置が講じられた室に設置されたものに限る。）の設置、当該電子計算機から電気通信回線を通じて送信された当該利用者情報及び当該利用者識別符号を識別する機能の設定並びに当該利用者情報及び利用者識別符号の確認ができること。但し、管理体制等が審査可能な状態であるクラウドサービスの利用を妨げられるものではない。

遠隔保守操作に関する適用反映箇所としては、指針第６条第１項第３号が挙げられる。

（指針第６条第１項第３号）

電気通信回線経由の遠隔操作が不可能であるように設定されていること。ただし、電子証明書の発行及び失効の要求その他の電子証明書の管理に必要な登録用端末設備の操作、および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保守作業に必要な保守用設備の操作については、この限りでない。

3.5 利用者の真偽の確認における自動化の規定

3.5.1 令和４年度報告書における主なコメント

必要	不要	どちらでもない
・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** **・相当程度の業務削減（結果として利用者への還元）が可能** ・機械的な判定結果を人為的に確認するという、本来必要でない業務が発生している。利用者識別符号送付時の確認・利用者端末アプリからの失効申請の確認についても同様	－	・真偽確認のために自動で確認できる文字列マッチング程度については、最終的にその結果を「人」が確認して発行の諾否を判断する運用は可能

3.5.2 特定認証業務の認定基準に関する調査で示された課題

以下の様に整理されている。

「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」（主務省庁局長級通知）において、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、以下の規定に基づき、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。

【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】

第６帳簿等の保存関係

１．総論

(1) 規則第１２条第１項各号に掲げる帳簿書類中、利用の申込書又は電子証明書の失効の請求書その他の利用者等から提出される書類又は送信される情報については、その受領の日付及び受領を

した者の識別に関する情報が関連づけられて記録されていることとする。

➡「受領をした者」を「人」と解釈してきた。

(2) 規則第１２条第１項各号中、電子証明書の作成に関する記録その他の認証業務の実施に関する記録については、その実施の日付並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていることとする。

➡「当該業務を実施した者及び当該業務について責任を有する者」を「人」と解釈してきた。

利用者の電子署名が行われた申請書の処理に際しては、機械的に確認して判断することが可能であり、人手による確認は基本的には必要ないと考えられる。そのようなケースに該当する特定認証業務の認定に係る基準を設けるべきではないか。

3.5.3 TF における整理

元々は利用者の真偽の確認における自動化の規定とは、「人を介さない利用者の真偽確認は認められないと解釈されてきている。」ことの見直しの為に出て来たものであり、既に、指定調査機関から、2023 年 6 月 1 日付けで、『「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』の文書が出されており、解決済みと思われる。

但し、例えばマイナンバーカードを使った時の自動化の具体的な適合例を追加で検討すること等を否定するものではない。

3.5.4 改正の骨子

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。たとえば，「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。

方針第６　１(1)及び(2)をこの中に引用する。 (1) 規則第１２条第１項各号に掲げる帳簿書類中、利用の申込書又は電子証明書の失効の請求書その他の利用者等から提出される書類又は送信される情報については、その受領の日付及び受領をした者の識別に関する情報（電子計算機により自動的に受領される場合にはその旨）が関連づけられて記録されていることとする。電子計算機によって自動的に受領される場合においては、「諾否の決定」手続きの自動化にあたり、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失効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失効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員を配置することとする。 (2) 規則第１２条第１項各号中、電子証明書の作成に関する記録その他の認証業務の実施に関する記録については、その実施の日付並びに当該業務を実施した者の識別に関する情報（電子計算機に

より自動的に受領される場合にはその旨）及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていることとする。

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

3.6.1 令和 4 年度報告書における主なコメント

必要	不要	どちらでもない
・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 **・利用者端末アプリの操作が煩雑になることから、特に利用者側に負担を強いる状態となっております。** ・利用申請と署名検証符号を同時に送信する方法の追加を検討いただければと存じます。	－	・政府の本人確認の基準の一端として再議論いただき、位置づけを明確にしていただきたい。 ・早急に差異の解消が必要とまでは考えておりません。 ・利用者の操作ミスなどにより利用者識別符号を紛失してしまうなどの事象が発生して、ユーザーサポートの負担が増すことが想定されます。

3.6.2 特定認証業務の認定基準に関する調査で示された課題

以下の様に整理されている。

公的個人認証法において、同法第 17 条第 1 項第 6 号の規定による総務大臣の認定を受けようとする者が行う特定認証業務の条件として、同法施行規則第 26 条第 5 号イでは、利用者署名符号を利用者が作成する場合において、利用者による申込みと同時に利用者署名検証符号を電気通信回線を通じて送信する方法が規定されている。この方法であれば同号ロに規定された利用者識別符号（利用者だけが知り得る情報）の交付あるいは送付が不要となる。

【公的個人認証法施行規則第 26 条第 5 号】

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。第十三号及び第八十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。

他方、電子署名法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、同法施行規則第 6 条第 3 号の 2 に従い、利用者識別符号の交付あるいは送付を行う必要があり、利用者と事業者双方に負担を強いる結果となっている。したがって、電子署名法施行規則第 6 条第 3 号の 2 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。

3.6.3 TF における整理

基準については単純化するには公的個人認証法施行規則の第 26 条第 5 号に統一すべきである。なお、電子署名法における認定と、公的個人認証法第 17 条第 1 項第 5 号の認定とでは、認定に係る調査方法、監査方法等に差異がある。しかし、これを統一するためには、電子署名法の認定手続きを大幅に変更し、調査の多くの部分を削ることになる。したがって、認定に係る調査方法等の統一については、今後の課題として認識するに留めて、改正の骨子には含めないこととする。

3.6.4 改正の骨子

施行規則第 6 条 3 号の 2 を次のように変更する。

三の二 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、次にあげる方法のいずれかにより行うこと。

イ当該利用者署名検証符号を内容として含む申込みに、あらかじめ発行を受けている電子証明書（公的個人認証基盤又は認定認証業務によって発行されたものに限る。）に基づく電子署名を行って、認証事業者に電気通信回線を通じて送信し、認証事業者が当該電子署名により当該利用者の真偽の確認を行う方法。

ロ 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方法。

3.7 その他

3.7.1 AATL 対応

電子署名法関連施行規則、調査表と AATL の要求事項に乖離があるため、日本の認証局は認

定認証業務であることのみを理由に AATL への登録ができない状況である。他方で、EU では、eIDAS 規則における認証局の実質的な技術基準である ETSI 基準と AATL の要求事項間で整合性が取れているため、トラステッドリストに掲載されている認証局であれば、Adobe 製品において信頼される認証局として扱われる。

提案：

大分類、中分類及び小分類のレベルでこの報告書に取り込む。法律、規則、方針のどの部分に、どのような内容の追記、修正が必要かというレベルでまとめることとする。

組織の信頼性については、タイムスタンプの制度（タイムスタンプ告示 第 3 条 1 項 7 号、タイムスタンプ実施要項 第 23 条）を参考にする。

3.7.1.1 組織の責任

(1) 責任

課題：組織の信頼性、業務の公平性、申請者の非差別性について規定すべき。

TF における整理：

電子署名法5条に欠格事項が記載されているが、どの条項にも施行規則等への委任がない（他の条項でも信頼性等に関する規定がない)。

電子署名法6条3号の業務の方法の規定に含めるのがよさそう。ただし、組織の信頼性が「業務の方法」に含まれるかどうかには注意が必要。

タイムスタンプ告示には、指定調査機関の規定として、第 15 条各号に組織の要件が挙げられている（実施要領第 62 条以下で詳細に規定)。第 15 条第 2 号～第 4 号が、「責任」に関わる内容である。

第十五条　総務大臣は、指定の申請が次の各号に掲げる要件のいずれにも適合すると認められるときには、その指定を行うことができる。

一　調査等及び確認の業務を適確かつ円滑に実施するに足りる経理的基礎及び技術的能力その他の能力を有すること。

二　法人にあっては、その役員又は構成員の構成が調査等及び確認の業務の公正な実施に支障を及ぼすおそれがないものであること。

三　調査等及び確認の業務以外の業務を行っている場合には、その業務を行うことによって調査等及び確認の業務が不公正になるおそれがないものであること。

四　その指定をすることによって調査等及び確認の業務の適確かつ円滑な実施を阻害することとならないこと。

改正の骨子：

タイムスタンプ告示第 15 条第 2 号ないし第 3 号の内容を、施行規則第 6 条に新たな号として追加する。ただし、業務の方法の規定として記載する必要があるため、たとえば次のものが考えられる。

施行規則第 6 条 十八 業務を行うにあたり、次の事項を満たすこと ア　法人にあっては、その役員又は構成員の構成が調査等及び確認の業務の公正な実施に支障を及ぼすおそれがない状態を維持すること イ　認証業務以外の他の業務を行っている場合には、当該他の業務を行うことによって認証業務が不公正になるおそれがないものであること。

(2) 財政的要件

課題： AATL に記載されている財政安定性、賠償責任について規定すべき。

TF における整理：

指針第 12 条第 3 号は「認証事業者が負担する保証又は責任について制限を設ける場合においては、その制限に関する事項」を実施規規程に含める、という内容である。ここに、財政安定性や賠償責任保険についての要件を定めるのは難しい。

電子署名法第5条は、内容を施行規則に委任していないので、財政的要件を定めるためには、電子署名法の改正が必要なのではないか。

やや無理があるかもしれないが、法第6条第1項第3号に含まれるものと考えて、施行規則第6条に新たな号を加えることも考えられる。(「能力を有する」を「能力を維持する」等の業務の方法っぽい書き方にする)

タイムスタンプ告示第3条第1項

七 当該時刻認証業務を継続的に安定して遂行するに足りる経理的基礎及び技術的能力その他の能力を有すること。

タイムスタンプ実施要領

(経理的基礎)

第 23 条 経理的基礎について、財政の状況（過事業年度に係るものを含む 財産目録、貸借対照表、損益計算書、事業計画書 等）は 次の 各号に掲げる 要件を満たすこととする 。

一 継続的な債務超過がないなど、 認定 業務の継続的かつ安定した遂行が担保できること。

二 賠償責任保険に加入しているなど、損害賠償請求をされた場合に対応できる能力があること。

2 前項第 1 号に係る情報については、認定事業者においては、認定事業者において公表することとする。

(技術的能力)

第 24 条 技術的能力については、時刻やサイバーセキュリティに関する専門性の優れた要員

を配置し、認定業務を継続的に安定して遂行するための教育訓練を行うこととする。

改正の骨子：

可能であれば、タイムスタンプ告示 3 条 1 項 7 号及び同実施要領 23 条～24 条の内容を、新たに追加する（たとえば、施行規則 6 条 18 号、指針 15 条あたりが適切だと思われる）。

施行規則 第 6 条第 18 号を追加 十八 当該認証業務を継続的に安定して遂行するに足りる経理的基礎及び技術的能力その他の能力を維持すること。 指針に追加 （経済的基礎及び技術的能力） 第 15 条 規則第 6 条第 18 号に規定する経理的基礎について、財政の状況（過事業年度に係るものを含む財産目録、貸借対照表、損益計算書、事業計画書等）は次の各号に掲げる要件を満たすこととする。 一 継続的な債務超過がないなど、認証業務の継続的かつ安定した遂行が担保できること。 二 賠償責任保険に加入しているなど、損害賠償請求をされた場合に対応できる能力があること。 2 前項第 1 号に係る情報に係る情報については、認定事業者においては、認定事業者において公表することとする。 3 規則第 6 条第 18 号に規定する技術的能力については、認証事業に関する専門性の優れた要員を配置し、認証業務を継続的に安定して遂行するための教育訓練を行うこととする。

(3) 組織・責務

課題： 準拠法に関して規定すべき。

TF における整理：

改正の骨子：

指針第 12 条第 1 項第 11 号に、準拠法についての記載を追加する。たとえば、

十一 認証事業者との間で係争が生じた場合に適用される法令（準拠法の指定を含む）及び解決のための手続に関する事項

3.7.1.2 技術基準

(1) ネットワークセキュリティ

課題： 侵入テスト、ウィルス対策、脆弱性診断について規定すべき。セキュリティパッチを 6

か月以内に適用することを規定すべき。

TF における整理：

本報告書 3.1 のリスクマネジメントに追加する

指針

第五条 規則第四条第二号に規定する電気通信回線を通じた不正なアクセス等を防止するために必要な措置とは、次の各号に掲げるものをいうものとする。

一 認証業務用設備が電気通信回線に接続している場合においては、認証業務用設備（登録用端末設備を除く。）に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するためのファイアウォール及び不正なアクセス等を検知するシステムを備えること。

改正の骨子：本報告書 3.1 を参照

(2) 情報資産管理

課題： 情報漏えい対策（リムーバブルメディアの使用・セキュリティ対策の情報提供など）について規定すべき。

TF における整理：

施行規則第 6 条第 15 号へ の一環として、方針 第 4 8(2)と並べて記載を追加する方法でよい。

施行規則第 6 条第 15 号へ　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

方針 第 4 8(2) 規則第 6 条第 1 5 号へに規定する「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のために必要な措置」とは、以下のものをいう。

ア 個人情報の取扱い及び保護に関する規定が明確に定められていること。

イ 当該情報の取扱いの方法、電子証明書への記載範囲について利用者の承認を受けること。

改正の骨子：

方針 第 4 8(2)の次に(2)の 2 を追加【(3)として追加し、現(3)以下を繰り下げてもよい】

方針 第 4 8(2)の 2 規則第 6 条 15 号へに規定する「帳簿書類の記載の漏えい、滅失又は毀損の防止のために必要な措置」とは、以下のものをいう。 ア リムーバブルメディアを使用する場合には、その管理に係る規程を定めること。

イ 滅失又は毀損を防止するために行う措置を利用者に情報提供すること

3.7.1.3 運用基準

(1) リスクアセスメント（利用者署名符号の生成）

課題：3.1.4 の改正の骨子に加えて、利用者署名符号の生成に係る規定をおくべき。

TF における整理：

WebTrust for CA Criteria の 5.1.1 に記載の内容（Illustrative Controls は基準を満たすための方策の例示に過ぎず、基準そのものではない）自体が省令レベルの記載としては技術基準の詳細としては過剰と考えられ、調査表への反映で良いのではないか。

なお AATL Technical Requirements では、EE4 において「利用者署名符号はセキュアトークンで保護されなければならない」旨が示されている。

現行法令においては利用者署名符号の格納媒体について特段の指定が無く、影響は相当程度にある。このため法令等改正においては、認定認証事業者のみならず、現状ソフトウェアトークンに基づく電子署名を受け入れる電子申請システム側との調整も必要となる。これらを踏まえて、日本の電子署名法では認められてきたことから、Adobe 社とソフトウェアトークンでの利用者署名符号の取り扱いに条件を付けて容認する可能性の議論であるとか、また、将来的には、日本国内における eIDAS の適格電子署名に対応する認定レベルを設けること、その格納媒体を規定した QSCD に対応する具体的な検討を進めて行く必要があるのではないかという意見があった。

改正の骨子：

施行規則等の法令の変更は行わず、調査表の変更で対応する。なお、関連情報として 3.1 を参照。

(2) 利用規約

課題：証明書ポリシーOID を記載すべきとする規定をおくべき。

TF における整理：

施行規則第 6 条第 5 号に追加する。

改正の骨子：

施行規則第 6 条第 5 号に「ホ」として証明書ポリシーOID を追加

施行規則第 6 条 五　電子証明書には、次の事項が記録されていること。 イ　当該電子証明書の発行者の名称及び発行番号 ロ　当該電子証明書の発行日及び有効期間の満了日

ハ　当該電子証明書の利用者の氏名
ニ　当該電子証明書に係る利用者署名検証符号及び当該利用者署名検証符号に係るアルゴリズムの識別子
ホ　当該電子証明書の証明書ポリシーの識別子

(3) 情報セキュリティポリシー

課題：経営陣による承認、情報セキュリティを管理するための組織のアプローチ等を規定すべき。

TF における整理：

ISO/IEC 27002：2013 の 5.1.1 節を参照すべき。

脆弱性・脅威の観点からの措置（WebTrust）、脆弱性修正プロセスの合理的保証（Network Security Principle4）、システム設定に関する週次のレビュー（AATL）

指針 12 条 1 項 7 号に変更を加えることや 組織の信頼性に含めることが考えらえる。

改正の骨子：セキュリティに関する事項は指針第 12 条第 1 項第 7 号に存在するので、以下のように追記する。

（指針 第 12 条第 1 項第 7 号）
認証業務に係るセキュリティに関する事項（情報セキュリティポリシー、及び利用者に係る個人情報の取扱いに関する事項を含む。）

(4) 組織管理と運用

課題：人的資源、情報システムの運用セキュリティ、インシデント管理、業務継続・復旧計画について規定すべき。

TF における整理：

人的資源は規則 6 条 15 号ホ、インシデント管理は同号ト、および 3.1.4 を参照、業務継続・復旧計画は「調査に関する方針」第 4 の 8.(3)にあるとおり。

施行規則第６条

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。

イ　業務の手順
ロ　業務に従事する者の責任及び権限並びに指揮命令系統
ホ　業務に係る技術に関し充分な知識及び経験を有する者の配置
ト　危機管理に関する事項

「調査に関する方針」第４の 8.(3)

(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、以下の事項を含むものをいう。

ア 発行者署名符号が危殆化し、又は危殆化したおそれがある場合には、直ちに発行したすべての電子証明書について失効の手続を行うこと。

イ 発行者署名符号の危殆化又は災害等による障害の発生の事実を利用者に通知し、かつ、署名検証者に開示すること及びその方法

ウ 発行者署名符号が危殆化し、又は危殆化したおそれがある場合及び災害又は認証業務用設備の故障等により署名検証者に対する電子証明書の失効に係る情報の提供が規則第６条第１３号に規定する認証業務の実施に関する規程に定める時間を超えて停止し、かつ、署名検証者に対しその停止の事実の開示が行われなかった場合においては、直ちに、当該障害の内容、発生日時、措置状況等確認されている事項を主務大臣に通報すること。

改正の骨子：3.1.4 を参照。

3.7.2 時刻同期

認証局のログや、アーカイブ等に使用される時刻について UTC への同期を求める。

方針に追記、或いは、施行規則 6 条に追加する。

たとえば、第 6 条第 5 号（電子証明書の記載内容）に係る規定として、指針第 9 条と第 10 条の間に新たな条を追加する方法が考えられる。

改正の骨子：

指針第 9 条の 2 規則第六条第五号ロに規定する発行日及び満了日を確実にするため、日本標準時通報機関である国立研究開発法人情報通信研究機構が生成する協定世界時（ＵＴＣ（NICT））を時刻源とし、当該時刻源との時刻差が 1 秒以内となるよう、時刻の品質を管理及び証明する措置を講じること。

3.7.3 リモート署名対応（鍵管理等）

現在の電子署名法施行規則等の法令においては、近年普及しつつあるリモート署名サービス（注）の利用に関する規定がない。具体的には、利用者が電子署名を行うために用いる「利用者署名符号」及びこれを検証するための「利用者署名検証符号」（両者を合わせて、以下「鍵ペア」という。）について、これらを認証事業者が作成する場合を規定する同規則 6 条 3 号と利用者が作成する場合を規定する同条第 3 号の 2 しかおかれていない。すなわち、リモ

ート署名サービスで鍵ペアを生成するケースや、リモート署名サービス外で鍵ペアを生成しリモート署名サービスに利用者署名符号を提供するケースにおいて、利用者署名符号や利用者署名検証符号の送信を可能とする規定がない。このため、認定認証事業者が発行する電子証明書に基づいてリモート署名サービスを行うことが困難になっている。

（注）リモート署名とは事業者のサーバに利用者署名符号を設置・保管し、利用者がサーバにリモートでログインし、当該署名符号で事業者のサーバ上で電子署名を行うこと（経産省平成２７年度、電子署名・認証業務利用促進事業調査報告書での定義より抜粋加筆）

この問題については、リモート署名 TF において検討が行われた（「**リモート署名サービスの評価基準概説**」参照)。これに基づいて、以下に、改正の骨子案を示す。

改正の骨子：

リモート署名事業者（リモート署名サービスを行う事業者）において鍵ペアを生成する場合の規定、同事業者に係る利用者署名符号又は利用者署名検証符号の安全な受け渡しのための規定、および、利用者がリモート署名サービスを利用し、電子署名を行う際の利用者の識別と認可に関する規定を追加する。このため、

① 認証事業者において鍵ペアを生成し、利用者署名符号をリモート署名事業者に送付する場合（現行法令では、利用者本人にしか送付できない利用者署名符号を、リモート署名事業者にも送付できるようにする)。

②リモート署名事業者において鍵ペアを生成し、利用者署名検証符号を認証事業者に送付する場合（直接送付する場合と、利用者を介して送付する場合の双方）

について、鍵ペアの生成並びに利用者署名符号及び利用者署名検証符号の送付を可能にする規定を電子署名法施行規則第 6 条第 3 号及び第 3 号の 3 に追加する。

また、リモート署名サービスの運用の便宜をはかるため、リモート署名サービスで用いる次の符号等を定義し、認証事業者における取扱を規定する。

①利用者鍵認可用識別符号（利用者本人だけが知る符号であって、利用者署名符号の利用が本人によるものであることを確認するために用いるもの）

②利用者鍵認可用識別符号確認情報（リモート署名事業者等において、利用者鍵認可用識別符号の正当性を検証するために用いる情報）

すなわち、認証事業者その他によるこれら符号等の生成・送付等及びこれを用いた利用者署名符号の当該利用者のみによる利用の規定を電子署名法施行規則 6 条 4 として追加する。これに伴い、方針第４　２に(3)として規定を追加する。

さらに、認証事業者及びリモート署名事業者以外の者が利用者鍵認可用識別符号を発行する場合の発行者に関する規定を電子署名法施行規則第 6 条 5 として追加する。これに伴い、方針第４　２に(4)として、同符号の発行者に関する規定を追加するとともに、２の２として

利用者鍵認可用識別符号の生成についての規定を追加する。

（下記の第 6 条第 3 号の 2 は、3.6.4 において提案した改正案である）。

電子署名法施行規則

第六条　法第六条第一項第三号の主務省令で定める基準は、次のとおりとする。

…中略…

三　利用者が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。）を認証事業者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者、または利用者が指定するリモート署名事業者（国や、国により認められた国内外の基準への適合性が、独立した監査機関等の監査で確認されたリモート署名サービス（仮称）に限る。以下同じ。）のどちらか一方に渡すことができる方法により交付し、又は送付し、かつ、当該利用者署名符号及びその複製を直ちに消去すること。

三の二　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、次にあげる方法のいずれかにより行うこと。

イ 当該利用者署名検証符号を内容として含む申込みに、あらかじめ発行を受けている電子証明書（公的個人認証サービス又は認定認証業務によって発行されたものに限る。）に基づく電子署名を行って、認証事業者に電気通信回線を通じて送信し、認証事業者が当該電子署名により当該利用者の真偽の確認を行う方法。

ロ 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。

三の三　利用者署名符号を認証事業者又は利用者が、リモート署名サービスを利用して作成する場合において、認証事業者は、当該利用者署名符号に対応する利用者署名検証符号を次の各号のいずれかの方法で受信するものとする。

イ リモート署名事業者より、電気通信回線を通じて安全、確実に受信する方法。

ロ 当該利用者から受信するときには、第三号の二イ又はロの方法。

三の四　認証事業者が、利用者鍵認可用識別符号（リモート署名事業者において、利用者が電子署名を行う際の鍵認可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。以下本条において同じ。）又は利用者鍵認可用識別符号確認情報（利用者鍵認可用識別符号の正当性の確認に用いる情報をいう。以下本条において同じ。）を取扱う場合には、次の各号のいずれかによるものとする。

イ 認証事業者以外が作成した電子的識別手段（利用者本人の識別に用いる符号等の手段をいう。）を利用者鍵認可用識別符号として用いるときには、認証事業者は、当該利用者により指定された利用者鍵認可用識別符号確認情報を、その有効性を確認した上で、リモ

ート署名事業者に電気通信回線を通じて安全、確実に送信する。

ロ 認証事業者が利用者鍵認可用識別符号及び利用者鍵認可用識別符号確認情報を生成するときには、利用者鍵認可用識別符号を容易に推測されないように生成し、これに対応する利用者鍵認可用識別符号確認情報を生成した上で、利用者に第三号に規定する方法で利用者鍵認可用識別符号を交付又は送付し、リモート署名事業者に利用者鍵認可用識別符号確認情報を電気通信回線を通じて安全、確実に送信する。

三の五　前号イに規定する電子的識別手段は、国や、国により認められた国内外の基準への適合性が、独立した監査機関等の監査で確認された事業者が発行するものに限る。

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

第４ 認証業務の実施の方法（利用者の真偽の確認方法を除く。）関係

２．認定認証事業者による利用者署名符号及び利用者識別符号の生成等

(3)　利用者署名符号を認証事業者または利用者がリモート署名サービスを利用して作成する場合においては、次の措置を含むものとする。

ア 利用者署名符号の生成は、認証設備室内と同等の安全性が確保できるリモート署名事業者の環境において複数人で行われること。

イ 当該利用者署名符号の転送や出力等の取扱いは、生成時と同等の安全性が確保されたリモート署名事業者の環境内のみで行われること。

ウ 当該利用者が自らの署名鍵を利用する際の識別に用いる利用者鍵認可用識別符号を作成する者は、安全な乱数を用いて同符号を生成するものとし、認証設備室と同等の安全性が確保された環境において、複数人で行われること。

エ 利用者鍵認可用識別符号を作成する者は当該利用者識別符号を安全、確実に利用者に交付又は送付し、利用者から受領書又はこれに準ずるものを受領すること。

オ　電子証明書の発行に際しては、リモート署名事業者から電子証明書に記載を求める利用者の情報と利用者署名検証符号の全体に対して利用者署名符号を用いて電子署名を付した証明書発行要求を安全に受領するものとする。

カ　利用者の電子証明書は、利用者鍵認可用識別符号を用いて利用者の認証を行った上で発行するものとし、当該利用者を指定する情報とともにリモート署名事業者に安全、確実に送信し、受領の確認を行うものとする。

(4)　認証事業者以外が作成した電子識別手段を利用者鍵認可用識別符号として利用する場合においては、次の措置を含むものとする。

ア 国から発行された電子的識別手段とは、公的個人認証サービスにより発行された電子証明書またはｇBiz ID プライムを用いるものとする。

イ 国により認められた国内の基準への適合性が、独立した監査機関等の監査で確認された認証サービス等から発行された電子的識別手段とは、公的個人認証法第１７条５号、６号認定を取得した事業者が認証サービス（IAS)を行う場合に発行する電子的識別手段とする。

ウ 国により認められた国外の基準への適合性が独立した監査機関等の監査で確認された認証サービス等から発行された電子的識別手段とは、SP800-63　の AAL２以上、FAL２以上を満たすことが監査機関により確認されたものとする。
２の２．認定認証事業者による利用者鍵認可用識別符号の生成等
規則第６条第 3 号の４ロに規定する利用者鍵認可用識別符号の生成に、２．(1)の利用者署名符号生成の規定を準用する。

4. まとめ

本報告書では、令和 4 年度報告書及び特定認証業務の認定基準に関する調査に基づき「１．はじめに」に記載の６個の課題についてそれぞれ検討し、法令改正の骨子を示した。また、本報告書では、認定認証業務と AATL との関係について検討し、AATL に対応するために必要な方策を提示した。これに加えて、認定認証事業者の時刻同期についての規定についても提案した。本報告書では、さらに、本調査研究業務のリモート署名 TF での検討に基づいて、認定認証業務が、リモート署名サービスと協調するために必要な法令改正の案を示した。

今後、これらの改正案に基づいて、電子署名法が近代化されることを期待する。なお、将来的には、e シール等の関連制度の基準との整合、国際的な技術基準への協調、維持管理の容易性などの観点から、認定に係る技術、運用、設備等の基準を独立した認定基準文書として立て付け、省令等から参照する構造とすることで、タイムスタンプや e シールを始めとする他のトラストサービスとの基準の共通検討の端緒となるとともに、海外の制度との相互関係も促進できるものと思われる。この点についても、今後の継続検討が必要と思われる。

以上