# 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（概要版）
## 電子署名法令上の基準のモダナイズの検討

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

# 用語 1/2

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）

# 用語 2/2

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

# TF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<br>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<br>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）<br>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<br>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）<br>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）<br>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
# モダナイズの必要性を検討する6つの観点

令和4年度報告書における6つの課題

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

本調査における6つの課題

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

# 2.1 優先順位の考え方

**電子署名に係るステークホルダーについて、次のとおりモダナイズの影響を分析。**

- 署名者：電子署名の実行者
  電子署名の利用拡大によるDX推進が期待できる。
- 依拠者：電子署名を用いて真正な成立の推定を得ようとする者
  電子署名の検証が容易になれば電子署名の利用拡大につながる。
- 事業者：認証局等
  効率的なサービス提供によりコストダウンが可能になり、間接的に電子署名の利用拡大につながる。

**結論**

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。

署名者と依拠者に係る観点が、直接的に企業活動を含む国民生活への寄与が大きい。

# 2.2 優先順位の設定

2.1の考え方に基づき、各課題に対して、次の方法で優先度及び検討項目を設定。

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、優先順位を決定
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った。
3.優先順位の低い項目についても検討を行う。

| 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 | ー | 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 | ー | 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 | ー | 4 |

# 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

**課題：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。**

### 3.1.1 令和4年度報告書における認定認証事業者からコメントのポイント

・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、さらなる設備投資と更新調査費の増大は懸念材料。

### 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のポイント

・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。

### 3.1.3 TFでの整理のポイント

・各認証事業者がリスクアセスメントを実施し、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。

# 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

### 3.1.4 改正の骨子のポイント

**（案１）**

・電子署名法第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３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

# 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

**課題：認証局の秘密鍵を管理する暗号装置の技術基準の更新について、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。**

### 3.2.1 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のポイント

- 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。

### 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のポイント

- 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。

# 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

### 3.2.3 TFでの整理のポイント

- 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。
- (1)の内容（暗号装置に必要な機能）の該当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、現行の方針 第２　２.(の同等２)（暗号装置と同等の安全性を満たすセキュリティ対策）は削除すべき。また、(2)による対策は海外の基準との乖離が大きい。

### 3.2.4 改正の骨子のポイント

- 現行の方針 第２　２.を、FIPS140-2及びISO/IEC15408に言及する規定に置き替える。
- 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

**課題：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。**

### 3.3.1 令和4年度報告書における主なコメントのポイント

- 「(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。3.3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を焦点とする。

### 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のポイント

- 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。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。

# 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

### 3.3.3 TFにおける整理のポイント

- 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。但し、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。

### 3.3.4 改正の骨子のポイント

- 施行規則第４条第４号（発行者署名符号の生成・管理）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、クラウドHSMに関する規定を(2)として追加する。骨子案に、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」を入れるが、この採否については、なお検討が必要である。

# 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

**課題：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。**

### 3.4.1 令和4年度報告書における主なコメントのポイント

- 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（クラウド利用）も認められるべき

### 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のポイント

- 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、規則第６条第１５条へ、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。

### 3.4.3 TFにおける整理のポイント

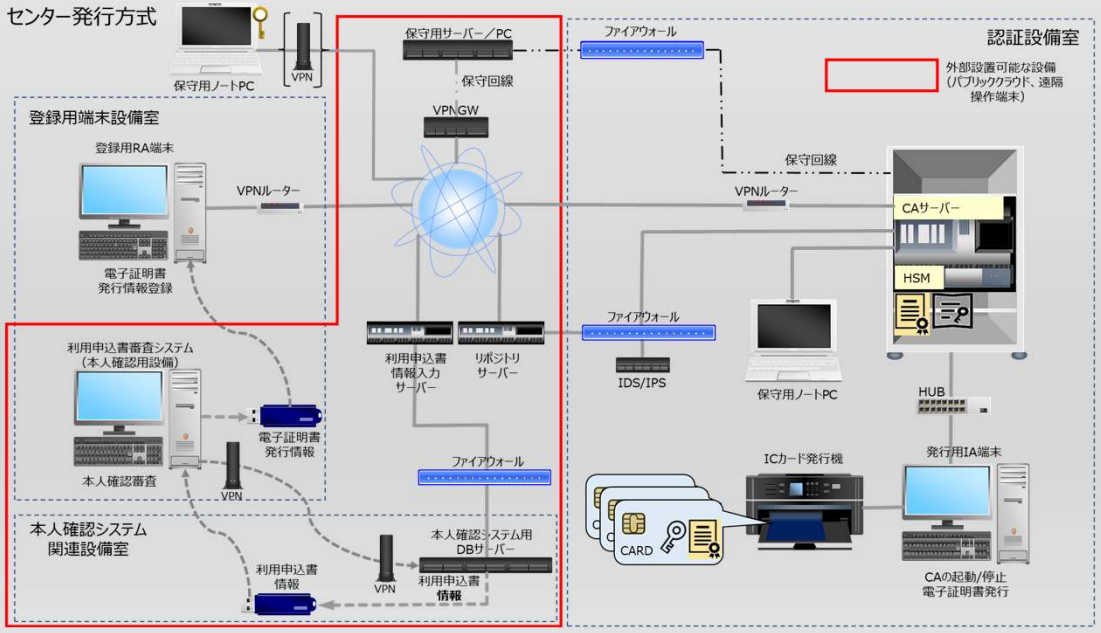
- 認証業務用設備の操作による電子証明書の発行や、失効等の直接の操作ではなく、適切な遠隔操作の環境が用意されている条件下における認証業務用設備のメンテナンス作業などにおいては、遠隔操作を認めるような基準を検討する。

# 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

### 3.4.3 TFにおける整理

### 3.4.3.2 認証局システムの構成例

（1） センター発行方式

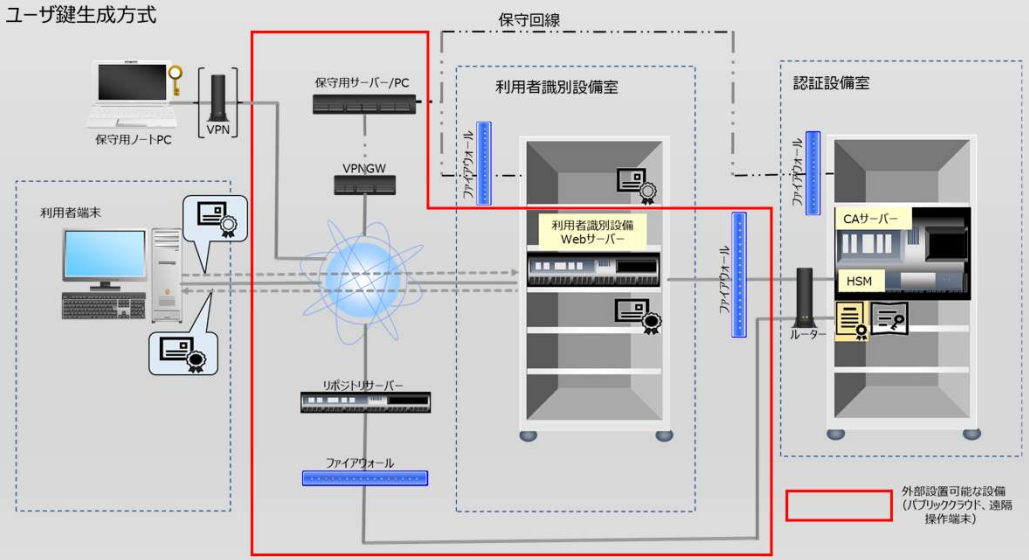


# 3.4 認証設備室の外からの遠隔操作やパブリッククラウドサービスの利用の規定

### 3.4.3 TFにおける整理

### 3.4.3.2 認証局システムの構成例

(2)　ユーザー側鍵ペア生成方式

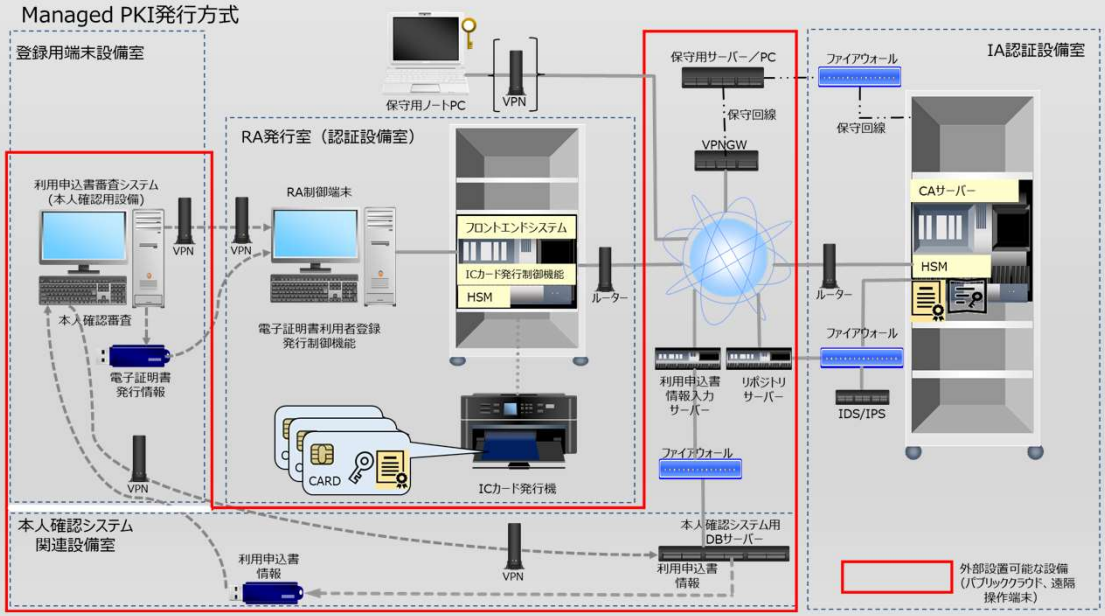


# 3.4 認証設備室の外からの遠隔操作やパブリッククラウドサービスの利用の規定

### 3.4.3 TFにおける整理

### 3.4.3.2 認証局システムの構成例

(3)　MPKI発行方式（IA外部委託方式）

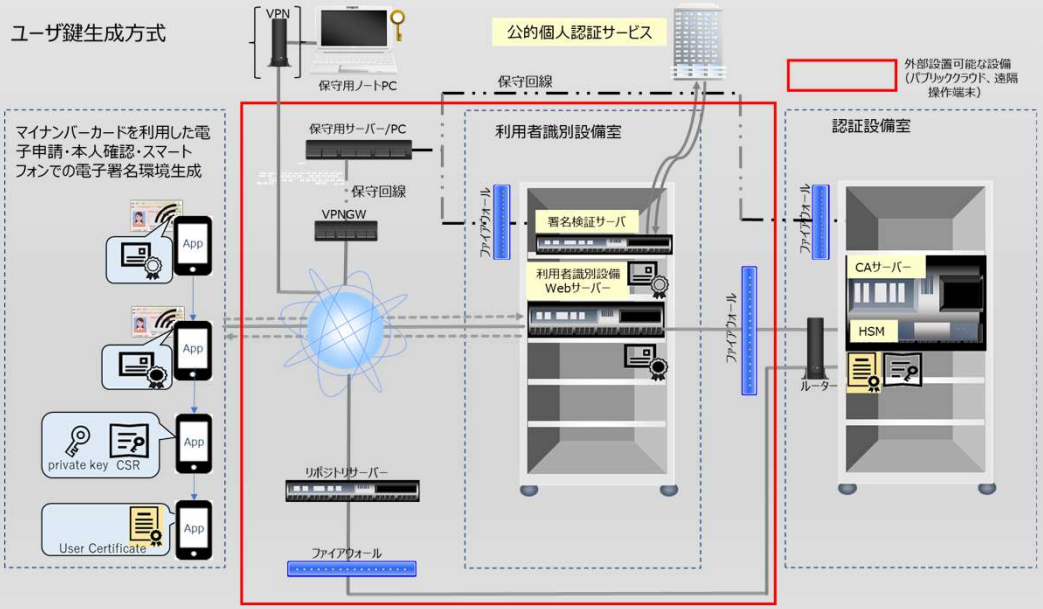


# 3.4 認証設備室の外からの遠隔操作やパブリッククラウドサービスの利用の規定

### 3.4.3 TFにおける整理

### 3.4.3.2 認証局システムの構成例

(4)　マイナンバーカードを利用した発行方式



# 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

### 3.4.4 改正の骨子のポイント

- 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）、第５条（認証業務用設備への不正アクセス防止等）、第６条第１項第２号（認証業務用設備の自動作動）及び、第６条第１項第３号（遠隔操作防止）に追加する。

# 3.5 利用者の真偽の確認における自動化の規定

**課題：利用者の真偽の確認における自動化の規定について、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。**

### 3.5.1 令和4年度報告書における主なコメントのポイント

- 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

### 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のポイント

- 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。

### 3.5.3 TFによる整理のポイント

- 既に、指定調査機関から、『利用者の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 利用者の真偽の確認における自動化の規定

### 3.5.4 改正の骨子のポイント

- 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。

# 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

**課題：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。**

### 3.6.1 令和4年度報告書における主なコメントのポイント

- 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

### 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のポイント

- 電子署名法施行規則第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。

### 3.6.3 TFにおける整理のポイント

- 基準について単純化するには、公的個人認証法施行規則の第２６条第５号（利用者識別符号による利用者確認と、電子署名を用いた利用者確認の双方を許容する規定）に統一すべきである。

# 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

### 3.6.4 改正の骨子のポイント

- 現行の施行規則第６条３号の２を同号イとロに書き分け、同号イとして電子署名による方法を追加する。

# 3.7 その他

**3.1～3.6以外の課題について、課題とTFでの整理及び改正の骨子のポイントを以下に示す。**

### 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。

**提案**

- AATLの大分類、中分類及び小分類のレベルでこの報告書で取扱い、追加・修正が必要な、法律、規則、方針の改正案（改正箇所・改正内容）を提案する。

# 3.7 その他

### 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**

- 電子署名法第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）。
- 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２号～４号が、「責任」に関わる内容である。

**改正の骨子のポイント**

- タイムスタンプ告示第１５条第２号ないし第３号の内容（指定調査機関の構成員又は同機関の他の業務との関係により公正が損なわれないこと）を、施行規則第６条に新たな号として追加する。

# 3.7 その他

### 3.7.1.2 組織の責任 (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での整理**

- 法第６条第１項第３号（申請に係る業務が、施行規則に規定する基準を満たすこと）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が考えられる。

**改正の骨子のポイント**

- タイムスタンプ告示第３条第１項第７号及び同実施要領第２３条～第２４条の内容（経理的基礎及び技術的能力）を、新たに追加する（たとえば、施行規則第６条第１８号、指針第１５条あたりが適切だと思われる）。

# 3.7 その他

### 3.7.1.2 組織の責任 (3)組織、責務

**課題**

- 準拠法に関して規定すべき。

**TFでの整理**

- 準拠法に関して規定することについて、特段の問題はない。

**改正の骨子のポイント**

- 指針第１２条第１項第１１号（係争対応手続に関する事項）に、準拠法についての記載を追加する。

# 3.7 その他

### 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での整理

- 本報告書3. 1のリスクマネジメントに追加する

#### 改正の骨子のポイント

- 3. 1参照

# 3.7 その他

### 3.7.1.2 技術基準 (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での整理**

- 施行規則第６条第１５号ヘ（利用者の真偽確認情報の目的外利用の禁止、漏えい、滅失の防止）の一環として、方針　第４　８（２）（個人情報保護の規定の明記、電子証明書の記載範囲についての利用者からの承認など）と並べて記載を追加する。

**改正の骨子のポイント**

- 方針　第４　８（２）の（２）の２として、リムーバブルメディアの利用に関する規定及び滅失等の防止措置の利用者への情報提供の規定を追加する。

# 3.7 その他

### 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での整理

- 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。
- ファイルタイプの電子署名とAATLの関係について調整が必要。将来的には、QSCD対応の検討も必要になりそう。

#### 改正の骨子のポイント

- 施行規則等の法令の変更は行わず、調査表票の変更で対応する。

# 3.7 その他

### 3.7.1.3 運用基準 (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での整理**

- 施行規則第６条第５号に追加する。

**改正の骨子のポイント**

- 施行規則第６条第５号（電子証明書の記録事項）に「ホ」として証明書ポリシーOIDを追加する。

# 3.7 その他

### 3.7.1.3 運用基準 (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での整理**

- ISO/IEC 27002：2013の5.1.1節を参照すべき。

**改正の骨子のポイント**

- 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、ここに情報セキュリティポリシを含む旨を追記する。

# 3.7 その他

### 3.7.1.3 運用基準 (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での整理

- 人的資源は規則第６条第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。

#### 改正の骨子のポイント

- 3.1.4で対応。

# 3.7 その他

### 3.7.2 時刻同期のポイント

- 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、施行規則第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UTC同期に係る新たな条を追加する方法が考えられる。

# 3.7 その他

## 3.7.3 リモート署名対応（鍵管理等）のポイント

### 課題

- 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の利用に関する規定がない。具体的には、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。

### TFでの整理

- リモート署名TFにて別途整理した内容に従う。

### 改正の骨子のポイント

- 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

# 3.7 その他

### 3.7.3 リモート署名対応（鍵管理等）のポイント

**改正の骨子のポイント**

- リモート署名事業者による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２に追加する
- 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第６条第３号の３として追加する。
- 認証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条第３号の４として追加する。

# 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。

# 付録： 改正骨子の内容

**リスクマネジメントに関する改正の骨子（3.1.4関係）**

**（案１）電子署名法及び施行規則の改正（これに加えて方針を改正する）**

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。

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２-1）施行規則の改正（これに加えて方針を改正する）**

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。

# 付録： 改正骨子の内容

**（案２−２）方針のみの改正**

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。

（案１，案２－１、案２－２の全てに関する改正案）方針の改正

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。

# 付録： 改正骨子の内容

**暗号装置の技術基準の改正の骨子　(3.2.4関係)**

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。

**セキュリティ基準の改正の骨子(3.3.4関係)**

(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。

# 付録： 改正骨子の内容

**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改正の骨子(3.4.4関係)**

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。

(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。

# 付録： 改正骨子の内容

**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改正の骨子(3.4.4関係)**

（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

# 付録： 改正骨子の内容

**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改正の骨子(3.4.4関係)**

(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。

# 付録： 改正骨子の内容

**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改正の骨子(3.4.4関係)**

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。

# 付録： 改正骨子の内容

**利用者の真偽の確認における自動化の規定の改正の骨子　(3.5.4関係)**

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。

# 付録： 改正骨子の内容

**特定認証業務を行う者の基準との差異の解消の規定の改正の骨子　(3.6.4関係)**

施行規則第６条第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。

# 付録： 改正骨子の内容

**タイムスタンプの規定の改正の骨子　(3.7.1関係)**

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。

**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。**

**タイムスタンプの規定の改正の骨子(3.7.1関係)**

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

# 付録： 改正骨子の内容

**準拠法の規定の改正の骨子　(3.7.1関係)**

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。

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

**技術基準の規定の改正の骨子　(3.7.1関係)**

方針　第４　８(2)の次に(2)の２を追加する。

方針　第４　８(2)の2
規則第６条第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

# 付録： 改正骨子の内容

**運用基準（リスクアセスメント）の改正の骨子　(3.7.1関係)**

施行規則等の法令の変更は行わず、調査表票の変更で対応する。

**運用基準（証明書ポリシー）の改正の骨子　(3.7.1関係)**

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

# 付録： 改正骨子の内容

**運用基準（情報セキュリティポリシー）の改正の骨子　(3.7.1関係)**

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、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、およ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。）

**運用基準の改正の骨子　(3.7.1関係)**

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、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。）

# 付録： 改正骨子の内容

**運用基準（情報セキュリティポリシー）の改正の骨子　(3.7.1関係)**

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、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、および利用者に係る個人情報の取扱いに関する事項を含む。）

**運用基準の改正の骨子**（組織管理と運用）　**(3.7.1関係)**

人的資源は規則第６条第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*

# 付録： 改正骨子の内容

**運用基準の改正の骨子**（組織管理と運用）　**(3.7.1関係)**

人的資源は規則第６条第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

*「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。*

# 付録： 改正骨子の内容

**時刻同期の改正の骨子　(3.7.2関係)**

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

| |
|---|
| 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。 |

# 付録： 改正骨子の内容

**リモート署名対応の改正の骨子　(3.7.3関係)**

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を追加する。

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。

# 付録： 改正骨子の内容

**リモート署名対応の改正の骨子　(3.7.3関係)**

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２に追加する。

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、第三号のニイ又はロの方法。

# 付録： 改正骨子の内容

**リモート署名対応の改正の骨子　(3.7.3関係)**

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第第６条３の４として追加する

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（利用者鍵認可用詞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。

# 付録： 改正骨子の内容

**リモート署名対応の改正の骨子　(3.7.3関係)**

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。さらに、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

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。