資料１－５

本検討会における議論の方向性（案）

令和５年９月６日

総務省　サイバーセキュリティ統括官室

本検討会における議論のスコープ（案）

- ✓ 本検討会においては、eシールについて、実際に提供されている（又は提供されることが具体的に見込まれている）サービスの**ユースケース**を念頭に、**国によるeシールに係る認定制度創設の要否**を含めて、望ましい制度整備の在り方を検討することとしたい。
- ✓ なお、諸外国との相互承認を始めとした長期的なトラストサービスの在り方に関する検討については、本検討会でのメインテーマとはしないものの、目指すべき将来像として留意しながら議論を進める。

現在

指針のみ存在

・技術や運用等に関する一定の基準のみが存在

eシールに係る指針

各認証局が指針を参考に認証業務を実施

認証局a　認証局b　認証局c

※国による適合性評価の枠組みは存在せず

本検討会のスコープ

認定制度あり

・国による適合性評価の枠組みを創設

認証業務によって認証を受けたeシール　（例）

認証局 A

国が定めた基準に適合する認証業務によって認証を受けたeシール

認証局 B

国に認定された認証業務によって認証を受けたeシール

認証局 C

将来像

国際相互承認

・国際相互承認を実現するための適合性評価の枠組みを拡充

EU　eIDAS規則に基づくQualifiedのeシール

認証局①　認証局②　……　認証局n

国際相互承認

日本　国に認定された認証業務によって認証を受けたeシール

認証局①　認証局②　……　認証局n

eシールに係る適合性評価の実現について

- ✓ eシールについては、大量発行される電子文書の信頼性を一括して検証することが可能なことから、**契約関係書類**（領収書、請求書等）や**組織が発行する証明書**（各種証明書等）の分野を中心に活用が期待されるが、現状としてeシールに係る適合性評価の仕組みは存在しておらず、**国による信頼性の裏付けがないことを理由にeシールの導入を躊躇する企業も多い**。
- ✓ 企業におけるDX化が加速する中、eシールに対するニーズが高まっていることから、政府方針においても、「**eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現**」に取り組むこととされており、**総務大臣によるeシールに係る認定制度**を創設することも視野に入れて、検討を進めていく必要がある。

政府戦略におけるeシールの位置付け

◆ **デジタル社会の実現に向けた重点計画**（令和5年6月9日閣議決定）

データの利活用による経済発展と社会的課題の解決を図るためには、信頼のあるデータ流通の基盤となるトラストの確保が重要であり、デジタル化の進展に伴いその必要性は一層高まっている。（中略）今後、オンライン取引・手続等において、発行元に関する証明のニーズが高まることが想定されるため、eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現にも取り組む。

認定制度創設に当たって検討が必要な事項

- ✓ トラストサービスについて、総務大臣による認定制度の例としては、2021年４月に総務省告示によって創設した**タイムスタンプに係る認定制度**があり、仮にeシールに係る認定制度を創設する場合には、同告示も参考に論点を整理することが考えられる。
- ✓ 総務大臣によるeシールに係る認定制度を創設するに当たっては、**タイムスタンプに係る認定制度の告示（及び実施要項）と同等の枠組み**の検討に加えて、次ページ以降に掲載する**eシールの制度化を検討する上でのeシール固有の論点**について議論する必要がある。

総務省告示によるタイムスタンプの認定制度

- 認定（第３条）
- 認定の更新（第４条）
- 変更の認定等（第５条）
- 運用規程（第６条）
- 個人情報等の取扱い（第７条）
- 実施状況の報告等（第８条）
- 認定の取消し（第９条）
- 承継（第10条）
- 報告義務等（第11条）
- 指定調査機関等（第12条～第24条）

細則を規定

時刻認証業務の認定に関する実施要項（一部抜粋）

【告示】	【実施要項】
・第３条第１項第１号 デジタル署名方式（中略）を用いるものとすること。	**・第４条（タイムスタンプ）** －タイムスタンプの規格 **・第５条（電子証明書）** －電子証明書の記載事項 －信頼できる認証事業者の要件　等
・第３条第１項第２号 日本標準時通報機関である（中略）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。	**・第６条（時刻源）** －時刻源の要件 **・第７条（時刻の品質管理及び証明）** －時刻の品質管理及び証明方法
・第３条第１項第３号 認定業務であるかどうかを一意に特定できる情報を含み、自らが改ざんされた際にこれを検知する手段を有するタイムスタンプを、当該タイムスタンプが有効である間十分な安全性を有する暗号技術や装置等を用いて堅実に生成すること。	**・第８条（認定業務の特定）** －タイムスタンプに包含すべき情報 **・第９条（タイムスタンプの生成に関わる暗号技術）** －生成に関わる暗号技術の要件 **・第10条（秘密鍵の保護装置）** －秘密鍵の保護装置の要件 **・第11条（タイムスタンプの生成処理）** －生成処理方法の要件 **・第12条（秘密鍵の管理）** －秘密鍵の管理方法の要件 **・第13条（タイムスタンプの有効期間）**

認定制度創設に当たっての論点（案）

1．eシールの定義

- 「eシールに係る指針」における定義からの変更の要否　等

2．eシールのレベル分け

- eシールのレベル分けと認定制度との関係の整理　等

3．電子証明書の発行対象となる組織等の範囲

- 法人以外に対象に含める組織等の範囲　等

4．電子証明書の発行に関する事項

- 発行元の組織等を一意に特定可能な識別子、OID　等

5．リモートeシールの位置付け

- 利用者の秘密鍵を管理するRSSPの認定制度における位置付け　等

6．認定制度の在り方

- タイムスタンプの告示等を参考に必要事項を検討

論点①　eシールの定義

1．eシールの定義

◆ 議論が必要な事項

- 「eシールに係る指針」に示されている定義を基に、告示での規定をイメージすると以下の形か。他に追加すべき要素はあるか。
- 「eシール」に和名での正式名称を設けるか。

告示における「eシール」の定義のイメージ（案）

第●条　この規程において「eシール」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った組織等の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

（参考１）「eシールに係る指針」における「eシール」の定義

電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み

（参考２）電子署名法における「電子署名」の定義

第二条　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

２・３　（略）

論点②　eシールのレベル分け

2. eシールのレベル分け

◆ 議論が必要な事項

- 「eシールに係る指針」では「eシールのレベル分け」が示されているが、電子署名法のように「認証業務のレベル分け」を行うよう整理するか。
- 仮に認定認証業務に係るeシールをレベル３とすると、それぞれのレベルに求められる要件をどのように整理するか。
- 具体的なユースケースを踏まえ、各レベルの認証業務に係るeシールが必要とされる場面をどのように整理するか。

（参考１）「eシールに係る指針」における「eシール」のレベル分け

レベル３： レベル２に加えて、十分な水準を満たしたトラストアンカーによって信頼性が担保されたeシール（発行元証明として機能することに関し、第三者によるお墨付き（将来的には国による認定制度等の要否を検討）があるものを想定）

レベル２： 一定の技術基準を満たすeシール（技術的には発行元証明として十分機能することが確認できるもの）

レベル１： 裸のeシール（eシールの定義には合致するが、レベル２の要件を満たす保証がないもの）

（参考２）電子署名法における「認証業務」、「特定認証業務」、「認定認証業務」の定義

第二条（略）

２　この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

３　この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

第四条　特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

２・３（略）

論点③　電子証明書の発行対象となる組織等の範囲

3. 電子証明書の発行対象となる組織等の範囲

◆ 議論が必要な事項

- 「法人　、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等」を発行対象とした「eシールに係る指針」の整理を維持するか。
  - ➢ 認定に係るeシールとそれ以外のeシールで、電子証明書の発行対象となる組織等の範囲に差を設けるか。
- 組織内における事業所・営業所・支店・部門単位や、担当者（意思表示を伴わない個人）、機器についても、「eシールに係る指針」の整理を維持するか。
- 後述の論点と重複するが、電子証明書の発行対象となる組織等には、当該組織等を一意に識別できる識別子が必要となるため、その識別子をどのように設定するか。

（参考）「eシールに係る指針」における「組織等の範囲」に関する整理（抜粋）

eシール用電子証明書の発行対象すなわちeシールが示す発行元となり得る組織等の対象は、eシールの普及・拡大の観点から、幅広い対象を含めることとし、法人、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等とする。

他方、それよりも粒度の細かい、組織内における事業所・営業所・支店・部門単位や、担当者（意思表示を伴わない個人）、機器については、eシール用電子証明書の発行対象としてのニーズが一定程度あるものの、その実在性を認証局において正確に確認することは困難であること等に鑑みて、eシール用電子証明書の任意のフィールドである拡張領域に記載できることとし、それらの確認方法や記載方法については2.3に記載する。

論点④　電子証明書の発行に関する事項

4. 電子証明書の発行に関する事項

◆ 議論が必要な事項

- 組織等の実在性・申請意思の確認の方法については、「eシールに係る指針」の整理を維持するか。
- 認定に係るeシールの電子証明書のフォーマットは、ITU-T X.509を使用することで良いか。また、従来のレベル２相当のeシールについても同様で良いか。
- 認証局における秘密鍵の管理については、「eシールに係る指針」の整理を維持するか。
- eシール用証明書やeシール署名鍵を物理的に受け渡す場合やオンラインで受け渡す場合の要件を定めるか。
- ①組織を一意に特定するための識別子（組織識別子）、②トラストサービスの種類を識別するためのOID（Object Identifier：オブジェクト識別子）について、どのように整理するか。 ⇒ 次ページ以降に案を掲載

（参考１）「eシールに係る指針」における「組織等の実在性・申請意思の確認の方法」に関する整理（抜粋）

組織等の実在性の確認の具体的な方法については、登記事項証明書や第三者機関データベース等を用いることが想定される。また、組織等の申請意思の確認の具体的な方法については、電子署名、押印、署名等で行うことが想定される。

（参考２）「eシールに係る指針」における「電子証明書のフォーマット」に関する整理（抜粋）

国内外の類似制度との整合性に鑑みて、レベル３及びレベル２のeシール用電子証明書のフォーマットは、ITU-T X.509を使用することとする。

（参考３）「eシールに係る指針」における「認証局の秘密鍵の管理」に関する整理（抜粋）

認証局のHSM自体の基準及びHSM自体の管理に係る基準について、レベル３のeシールではそのセキュリティ要件等において十分な水準を満たす必要があり、同じトラストサービスの１つである電子署名の認定認証業務における認証局の秘密鍵の管理と同等の水準が求められると想定されることから、基本的には電子署名法の規定（FIPS140-１ レベル３相当）を準用することとする。

ただし、HSM自体の技術基準は現行化（FIPS140-2 レベル３相当）することを前提とし、念頭に置くレベルはFIPS140-2 レベル３相当もしくは、ISO/IEC 15408のEAL4+相当（プロテクションプロファイルは別途検討が必要）とする。

論点④　電子証明書の発行に関する事項

組織識別子の仕様案

■ **国際的に決まったプレフィクス（NTR, VAT）を使用した場合の組織識別子案**

※NTR；National Trade Register
※VAT；Value Added Tax

- 国が管理する番号体系を使用する。

プレフィクス	組織識別子案	使用する既存の番号体系案 （ZZZZZZに使用する既存番号体系案）
NTRJP	NTRJP-ZZZZZZ	**法人番号**
		会社法人等番号
VATJP	VATJP-ZZZZZZ	**適格請求書発行事業者登録番号**
		法人番号（NTRJPで使用しない場合）

■ **我が国独自のプレフィクスを設けて使用する組織識別子案**

- 上記以外の既存番号体系と我が国独自のプレフィクスを使用する。
- EDINETコードや民間が管理する番号体系を複数使用して、我が国においてeシールを利用する組織等を網羅する。

＜使用イメージ（EDINETコード（※1）の場合）＞　※1：開示書類等提出者ごとに発番される一意のコード

既存の番号体系名	プレフィクス案	組織識別子案
EDINETコード	ED:JP	（例）ED:JP-E12345

既存の番号体系を複数用いてeシールを利用する組織等を網羅する

主な論点

- ✓ NTRJP、VATJP及び我が国独自のプレフィクスを使用した組織識別子を使用する方向性で問題ないか。また、それぞれどの番号体系を用いるか。
- ✓ 認定に係るeシールの電子証明書には国が管理する番号を組織識別子として用いることとし、それ以外の電子証明書には民間コードを用いることも可能と整理するか。

論点④　電子証明書の発行に関する事項

オブジェクト識別子の仕様案

■ オブジェクト識別子（OID）の仕様案

- eシール用OIDはレベルごとに区分し、リモートeシールとローカルeシールも識別可能とする。

（例）総務省管理の番号体系を使用する場合

0.2.440.100145.○.1.1.1 → 日本の認定認証業務に係るeシール用証明書ポリシ
0.2.440.100145.○.1.1.2 → 日本の特定認証業務に係るeシール用証明書ポリシ
0.2.440.100145.○.1.1.3 → 日本のeシール用証明書ポリシ
0.2.440.100145.○.1.1.4 → 日本の認定認証業務に係るリモートeシール用証明書ポリシ
⋮　⋮

■ オブジェクト識別子の例

- EU eIDASにおけるOID体系

（EU eIDASにおける共通の証明書ポリシ 具体例）
0.4.0.194112　ETSI適格証明書ポリシ
0.4.0.194112.1　ETSI適格証明書ポリシ識別子
0.4.0.194112.1.0　自然人用適格証明書ポリシ（=EU適格署名用ポリシ）
0.4.0.194112.1.1　法人用適格証明書ポリシ（=EU適格eシール用ポリシ）
0.4.0.194112.1.2　QSCDを用いた自然人用適格証明書ポリシ（=EU適格署名用ポリシ）
0.4.0.194112.1.3　QSCDを用いた法人用適格証明書ポリシ（=EU適格eシール用ポリシ）
0.4.0.194112.1.4　EU適格ウェブサーバー用証明書ポリシ

- 日本における具体例

（日本における具体例）
0.2.440.100145 総務省
BCA 相互認証証明書ポリシ
0.2.440.100145.8.1.1.1.110　SHA256withRSAの官職証明書用
0.2.440.100145.8.1.1.21.130　SHA256withRSAの利用者証明書用
BCA 相互認証テスト用証明書ポリシ
0.2.440.100145.8.1.1.1.100　SHA256withRSAの官職証明書用
0.2.440.100145.8.1.1.21.100　SHA256withRSAの利用者証明書用

主な論点

- ✓ オブジェクト識別子を使用するトラストサービスの範囲はeシールに限定してOID番号を決定するか。その他のトラストサービスにも適用するか。
- ✓ OIDが必要な全てのトラストサービスに対してOIDを割り振る場合、トラストサービス用のOIDアークを設けるべきか。
- ✓ eシール用証明書向けのOIDの中で番号が必要なものは何か。

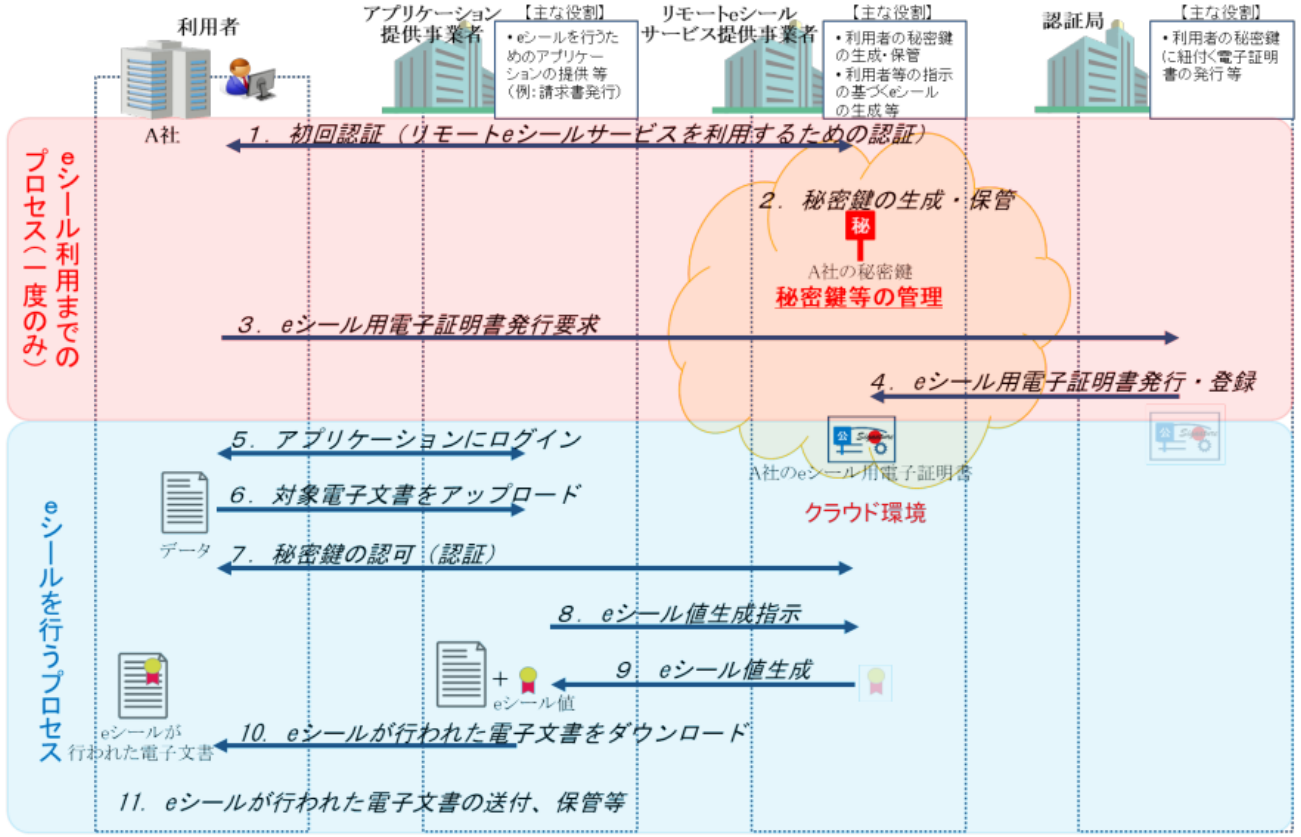
論点⑤　リモートeシールの位置付け

5. リモートeシールの位置付け

◆ 議論が必要な事項

- 認証業務を対象とする認定制度を創設する場合、利用者の秘密鍵を管理するリモートeシールサービス提供事業者に対しては認定制度上どのような規律を課すことが適当であるか。
- 認定制度とは別に、リモートeシールサービス提供事業者が遵守すべき事項をガイドライン等で示す必要があるか。
- 電子証明書において、ローカル/リモートのいずれの方法で付されたeシールであるかを判別できるようにすべきか。

<リモートeシールの一例>　eシールに係る指針（令和３年６月25日総務省策定）より抜粋



注）認証局、リモートeシールサービス提供事業者のそれぞれを同一の事業者が行う場合もあり得る

論点⑥　認定制度の在り方

6. 認定制度の在り方

◆ 議論が必要な事項

タイムスタンプの告示等を基にすると、以下の事項等について議論する必要がある。

① 認定の対象
- 認証業務を認定の対象とすることで良いか。

② 認定の更新
- ２年ごとに更新を求めることで良いか。

③ 変更の認定
- 認定業務の変更に当たっては、原則として、総務大臣の認定を受けることとするか。

④ 運用規程

⑤ 個人情報等の取扱い

⑥ 実施状況の報告等
- 認定事業者は年一回以上の監査（内部監査も可）を行い、監査の結果を審査期間に報告することで良いか。

⑦ 認定の取消し
- 認定事業者が一定の要件に該当した場合、認定を取り消すことを可能とするか。

⑧ 承継

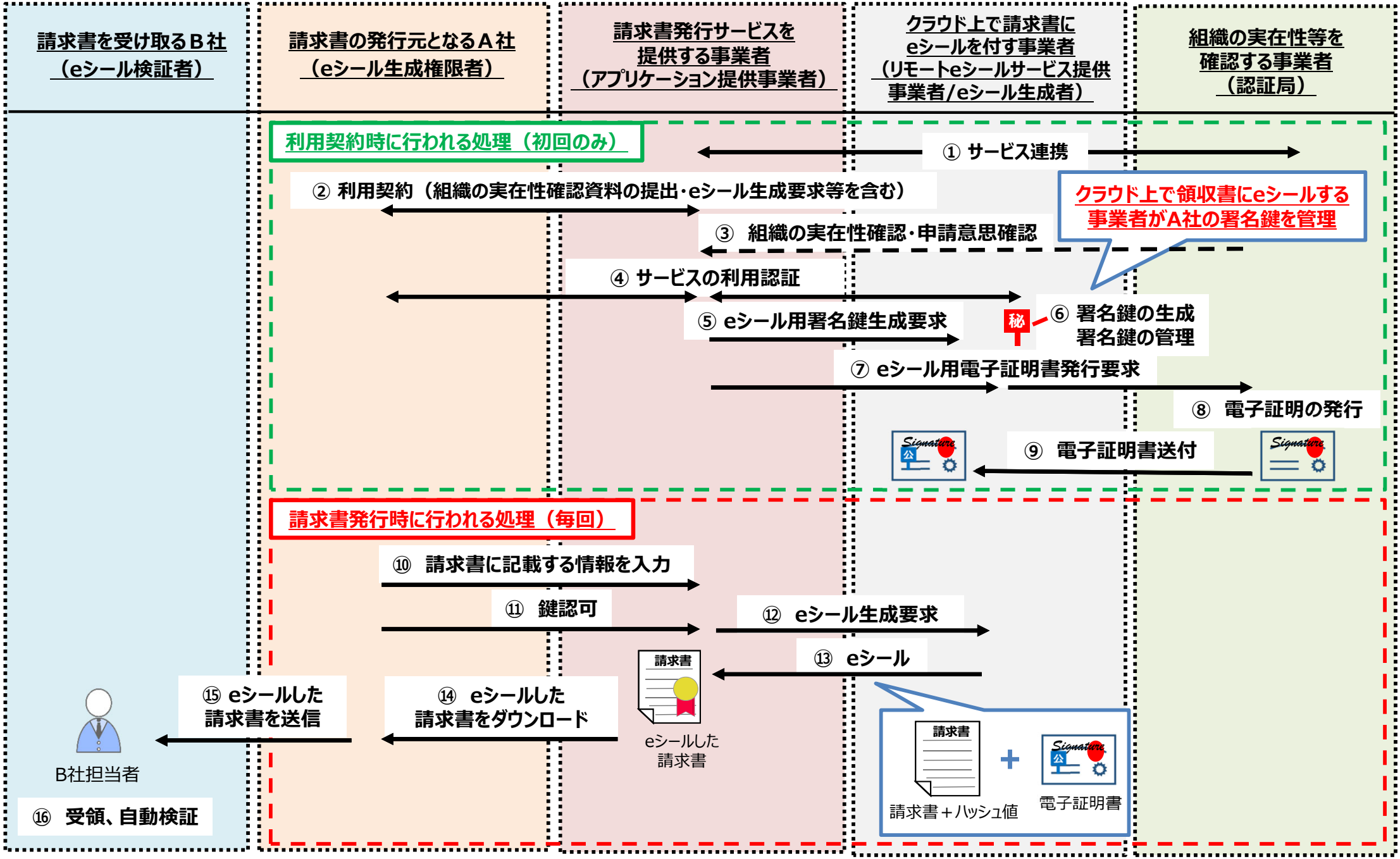
⑨ 報告義務
- 緊急事態発生時に総務大臣に報告することで良いか。

⑩ 指定調査機関
- 総務大臣による実施状況の調査等の一部を指定調査機関に行わせることを可能とするか。

⑪ 指定調査機関の指定等に係る手続

（参考１）eシール活用のイメージ①（請求書）

クラウドでの請求書発行サービス等を利用して、請求書に対してリモートでeシールする事例



（参考２）eシール活用のイメージ②（資格証明書）

資格証明書発行機関が自身で秘密鍵を管理し、資格証明書に対してローカルでeシールする事例

資格証明書を発行要求する資格取得者（eシール検証者）

資格証明書を発行する機関（eシール生成権限者）

組織の実在性等を確認する事業者（認証局）

利用契約時に行われる処理（初回のみ）

① 利用契約（組織の実在性確認資料の提出・eシール生成要求等を含む）

② 組織の実在性確認・申請意思確認

③ eシール用署名鍵生成・電子証明書発行要求

④ 署名鍵の生成・電子証明書の発行

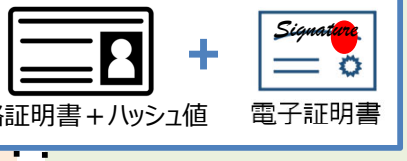
⑤ 署名鍵、電子証明書を送付

資格証明書を発行する機関が自身の署名鍵を管理

資格証発行の裏側で行われる処理

⑥ 資格証明書発行要求

⑦ 自身でeシール



eシールした資格証明書

⑧ eシールした資格証明書を送付

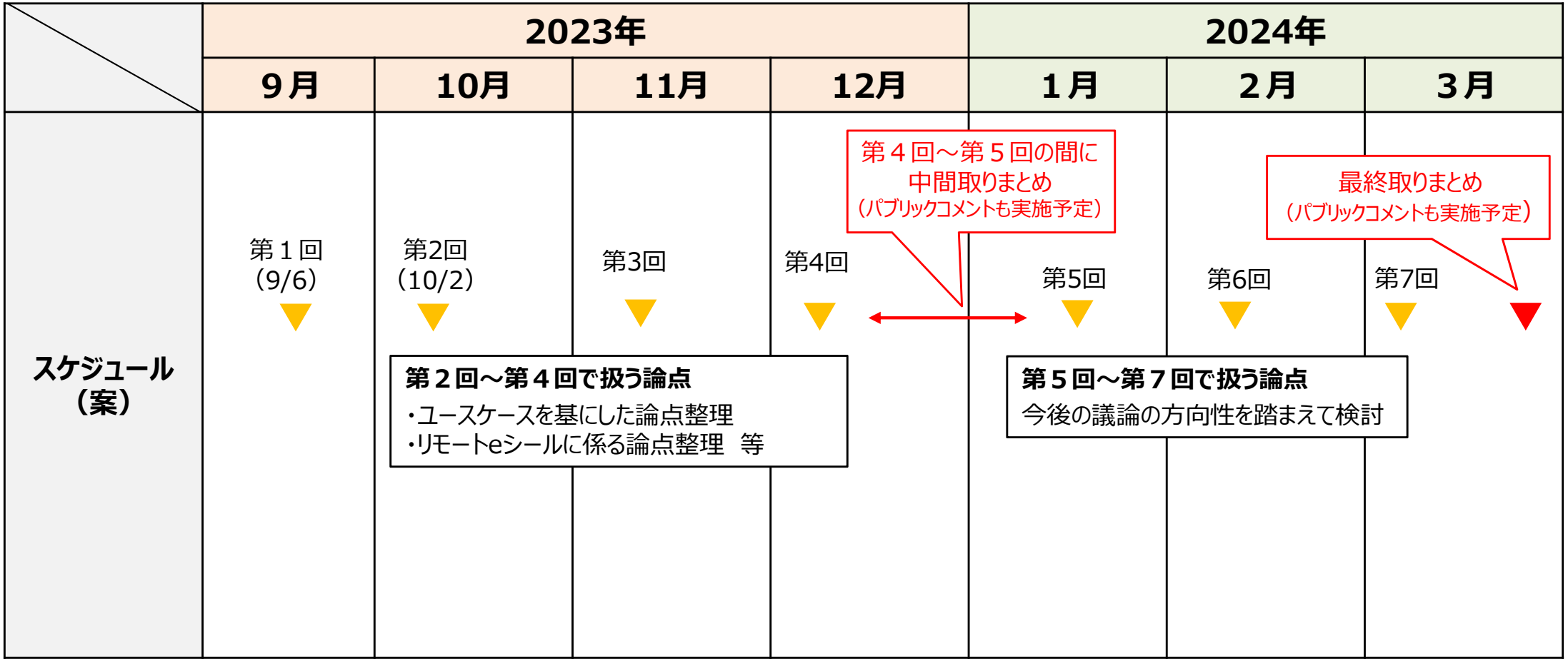
⑨ 受領、自動検証

⑩ eシールした資格証明書を送付

資格証明書の提出を求める第三者（eシール検証者）

⑪ 受領、自動検証

今後の検討スケジュール（案）



※スケジュール及び検討内容は変更の可能性あり