資料７－２

eシールについて検討すべき主な事項

令 和 ２ 年 １ ２ 月 ２ ３ 日

サイバーセキュリティ統括官室

eシールの目的

- 新型コロナウイルス感染拡大に伴って、テレワークの推進が一層求められており、インターネット上で官民のあらゆるやり取りを完結する要請が高まるなか、トラストサービスの１つであるeシール（電子文書の発信元の組織を示す目的で行われる暗号化等の措置）がその重要な役割の一端を担うことが期待されている。
- eシールの活用によって、データ発行元の組織を簡便に確認できるようになり、これまで紙で行われていた書類等の企業間のやり取りを電子的に安全に行えるようになる。また、意思表示を伴わないことから、機械的に迅速・大量にeシールを付すことができるため、業務効率化や生産性向上が期待される。
- これまで本検討会では、eシールが有効だと考えられるユースケースについて、ヒアリングや提案募集等を通じて深掘りを行ってきた。
- デジタル・ガバメント閣僚会議 データ戦略タスクフォース※においても、我が国におけるeシールを含む包括的なトラストサービスの在り方の検討の必要性が議論されている。

※　内閣官房情報通信技術（IT）総合戦略室及び内閣府政策統括官（科学技術・イノベーション担当）にて庶務を処理。主査は内閣総理大臣補佐官。

主なユースケースの例

- 見積もりから請求・支払プロセスまでの経理関係業務や契約に紐づいて発生する書類
- 組織が公開する情報（決算短信、ニュースリリース 等）
- 組織が発出する証明書（レポート、在職証明書、保証書 等）
- 監査手続において、外部証跡を入手及び確認する必要のある資料
- 行政と民間との間でやり取りされる証明書・報告書

データ戦略タスクフォースでの議論

- **「事実・情報」：発行元証明**
  自然人、**法人や事業所などの「組織」**、さらには IoT 時代において爆発的に増大する「機器」が存在するという事実と、当該機器**が発行する情報等の信頼性を担保するためには、発行した自然人・組織・機器が信頼できるか、その発行方法が信頼できるのか、当該事実・情報が作成しようとした通りのものかなどの証明（発行元証明）が必要**である。（データ戦略一次取りまとめ（案）12月8日時点）

本検討会で取り上げられたユースケース及び内閣官房に検討が進められているデータ戦略タスクフォースでの議論を踏まえた上で、我が国におけるeシールの在り方について検討が必要。

検討に当たっての主な観点

１．国内の類似制度との整合性

- 同じトラストサービスの1つである電子署名法上の電子署名との関係性
- 商業登記に基づく電子認証制度上の電子署名との関係性　等

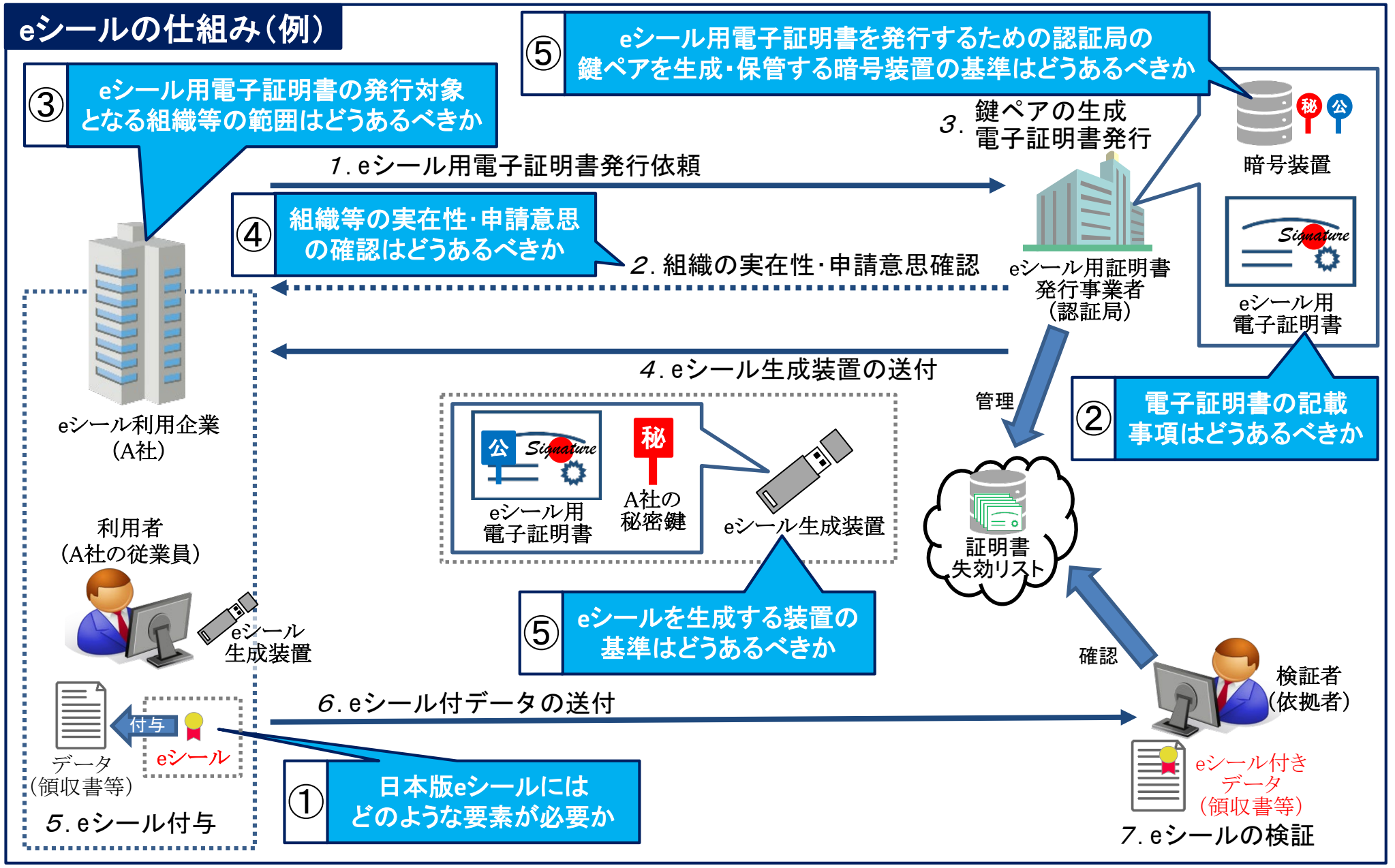
２．国際的な整合性

- EU等の諸外国の仕組み・制度との整合性
- ISO等国際標準との整合性　等

３．eシールの普及・利用促進

- eシールの利用者視点で、わかりやすいeシールの目的・用途
- eシール用電子証明書発行事業者視点で、参考となるeシールの仕組みや技術基準　等

eシールの仕組みの全体像（例）



我が国におけるeシールの検討事項の全体像（案）

我が国におけるeシールの在り方について、主に検討すべき事項は以下のとおり。

① eシールに求められる要素

② eシール用電子証明書の記載事項

③ eシール用電子証明書の発行対象となる組織の範囲

④ 組織等の実在性・申請意思の確認の方法

⑤ 設備（認証局側の暗号装置、ユーザー側のeシール生成装置等）の基準

⑥ その他

検討事項案①

① eシールに求められる要素

- 我が国におけるeシールはどのような要素を備えるべきか。
- eシールの用途等にあわせて、レベル感を分けて検討することが必要か。

＜例＞

レベル1：eシールの定義（データの起源と完全性を保証 等）

レベル2：一定の技術基準を満たすeシール（eシール生成者に一意にリンクしている、eシールの生成者を識別できる、十分な強度の暗号の活用、改ざん検知が可能 等）

レベル3：レベル2に加えて、トラストアンカーとして十分な水準を満たすeシール（適切な組織等の実在性・申請意思の確認、国際標準との整合性（設備、電子証明書等） 等）

（参考となる制度）

✓ 電子署名法：第2条第1項の電子署名、特定認証業務、認定認証業務

✓ EUのeIDAS：（裸の）eシール、先進eシール、適格eシール

② eシール用電子証明書の記載事項

- eシール用の電子証明書に記載すべき事項として、どのような項目が考えられるか。
- 電子証明書のフォーマットはどうあるべきか。

＜例＞

記載事項：発行者、有効期間、公開鍵、署名アルゴリズム 等

フォーマット：ITU-T X.509 等

（参考となる制度）

✓ 電子署名法の電子署名の証明書の記載事項、フォーマット

✓ 商業登記電子証明書の記載事項、フォーマット

✓ EUのeIDAS等で定めるeシールの電子証明書の記載事項、フォーマット

検討事項案②

③ eシール用電子証明書の発行対象となる組織の範囲

- eシール用電子証明書の発行対象となる組織の範囲（法人、それ以外等）はどうあるべきか。
- 組織内の発行対象の範囲（部門等）はどうあるべきか。
- eシール用電子証明書の発行対象を特定する識別子の付与の仕方はどうあるべきか。

＜例＞

組織の範囲：法人、個人事業主、権利能力なき社団・財団、それに満たない任意団体、個人（意思表明なし） 等

組織内の範囲：会社、部門、営業所・事業所 等

発行対象の識別子：電子署名ではOID

（参考となる制度）

✓ 商業登記電子証明書の発行対象範囲、識別子

✓ EUのeIDASで定めるeシールの発行対象範囲、識別子

④ 組織等の実在性・申請意思の確認の方法

- ③で検討した組織等の実在性確認の方法はどうあるべきか。
- eシール用電子証明書の発行を受ける組織等の申請意思の確認の方法はどうあるべきか。

＜例＞

実在性確認：手段（対面、オンライン）、手続のフロー、確認に用いる書類（商業登記等）やデータ 等

申請意思の確認：確認レベルの高いものの例として、電子署名（マイナンバーカード、商業登記電子証明書、電子署名法認定認証業務に係る電子証明書 等）、署名、押印（登録したものに限る）
確認レベルの低いものの例として、押印（認印）、メール、電話 等

（参考となる制度）

✓ 商業登記電子証明書発行の手続

✓ EUのeIDAS等で定めるeシール用電子証明書発行の手続

✓ 電子署名法認定認証業務に係る電子証明書発行の手続（申請意思の確認）

✓ マイナンバーカード発行の手続（申請意思の確認）

検討事項案③

⑤ 設備（認証局側の暗号装置、ユーザー側のeシール生成装置 等）の基準

- eシール用電子証明書を発行するための鍵ペア（秘密鍵、公開鍵）を生成・保管する暗号装置である認証局側の設備（Hardware Security Module：HSM）の基準はどうあるべきか。
- eシールを生成する装置であるユーザー側の設備（USB、ICカード等のデバイス（HSM））の基準はどうあるべきか。

＜例＞

ISO/IEC 15408（コモンクライテリア）のEAL4+ 等

FIPS140-2 レベル3以上

（参考となる制度）

✓ 電子署名法の認定認証業務で求める設備の基準

✓ EUのeIDAS等で定める設備の基準

「組織が発行するデータの信頼性を確保する制度に関する検討会」のスケジュール（案）

- これまで7回検討会を開催し、eシールのユースケースについて深掘りを実施。
- 今後は、国内の制度（電子署名法、商業登記電子証明書）やEUの制度等も踏まえながら、我が国におけるeシールの在り方について、検討を実施予定。
- 本検討会での議論を踏まえ、2021年度春頃目途にeシールに係る指針（案）策定を目指す。

全体スケジュール（案）