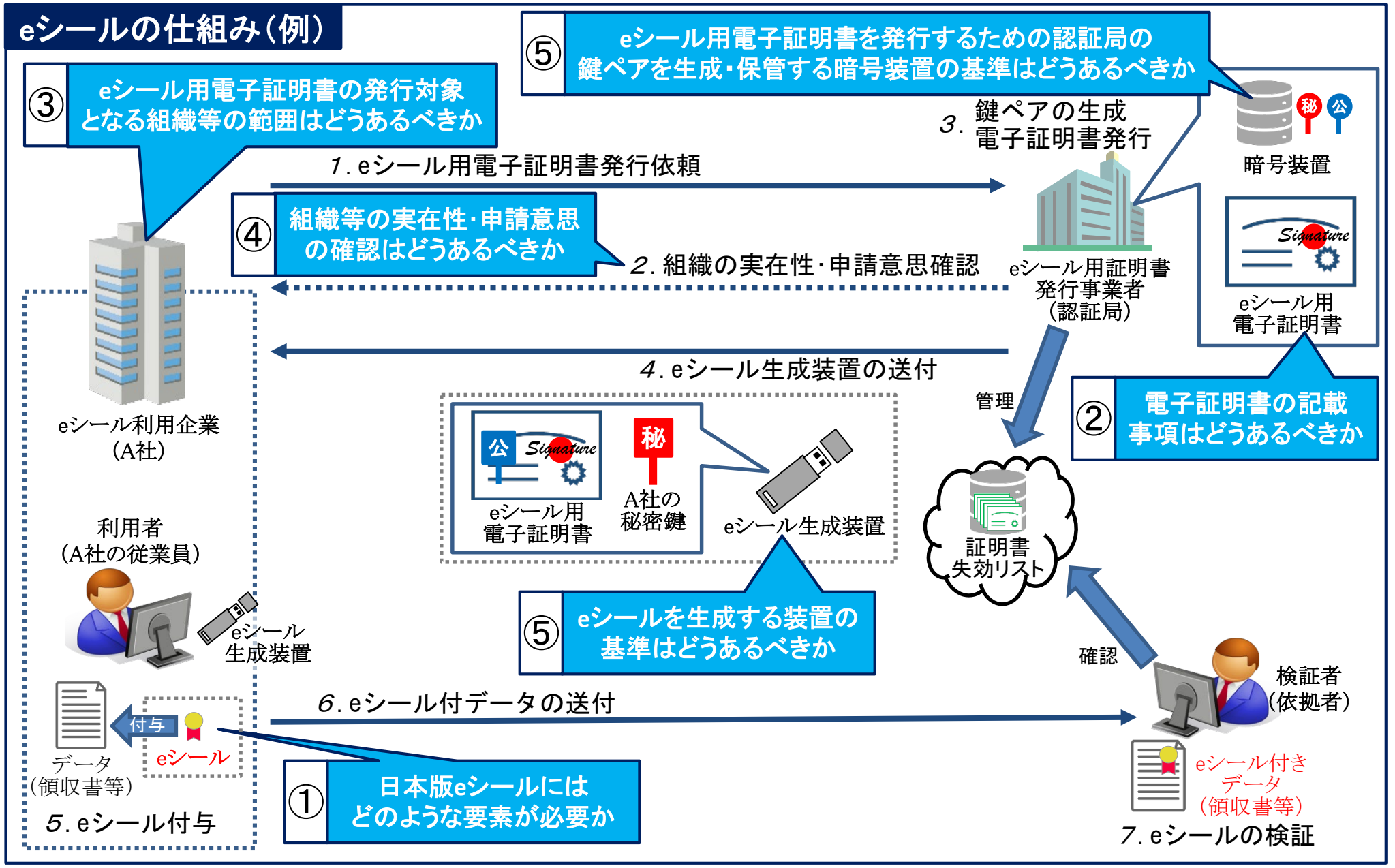
資料８－１

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（第８回）
事務局資料

令 和 ３ 年 １ 月 ２ ９ 日

サイバーセキュリティ統括官室

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

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。

既に検討された項目　今回検討する項目　今後検討する予定の項目　検討継続中の項目

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等の範囲

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（一定の技術基準（CRL（失効リスト）等）等）

前回検討会（第７回）の振返り

議論であがった主な意見

① eシールに求められる要素
- まずはeシールの定義付けをする必要があるのではないか。
- レベル毎のeシールで、それぞれどのような用途で使えて何が異なるのかを検討すべきではないか。

② eシール用電子証明書の記載事項
- 発行元の組織の情報だけでなく、eシールを付すデバイスや場所等についても検討する必要があるのではないか。

③ eシール用電子証明書の発行対象となる組織等の範囲
- 特になし

④ 組織等の実在性・申請意思の確認の方法
- サーバ証明書（EV、OV証明書）の発行手順が参考になるのではないか。
- WebTrustの監査制度の基準やガイドラインが参考になるのではないか。

⑤ 設備の基準
- １つのeシールを複数人で使用可能とするのであれば、eシールを付す際の秘密鍵の管理の在り方（レベル毎に分けて考えるか、一律一定の水準を設けるのか）について検討する必要があるのではないか。
- リモート署名方式によるeシールも検討する必要があるのではないか。

⑥ その他
- eシールの電子証明書の失効（CRL）についても検討する必要があるのではないか。
- eシールをプログラムが自動的に付すことを考慮すると、eシールを付すプログラム側の要件も検討する必要があるのではないか。
- （eシールを発行する事業者を管理監督する機関についても検討することが必要ではないか。）
- （タイムスタンプとeシールが併用されることも考慮して、eシールの有効期間を検討する必要があるのではないか。）

確認事項

① eシールに求められる要素（その１）

【確認事項】

- 我が国におけるeシールの定義について。
  - **発行元証明**： 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（または発行されて以降）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】

デジタル・ガバメント閣僚会議（第10回）（令和2年12月21日）「データ戦略タスクフォース第一次とりまとめ」（P29）から抜粋

c)eシール

eシールとは、**電子文書等の発行元の組織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**であって、発行元が個人に限らず組織となることもある。我が国においては、eシールに関する公的な仕組みは現状存在していないものの、一部の企業において、組織名の電子証明書としてe シールの導入が進んでいる。

同とりまとめ（P31）から抜粋

b)「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。

同とりまとめ（P33）から抜粋

b)発行元証明

組織や機器に係る真正性の担保に係る検討課題の例としては下記のとおり。（「自然人」については意思表示の証明※の項目参照）組織に係る証明については、法人などの組織をどこまで細分化するか、その際の発行元証明の有効性のバランスをどう確保するか、権限関係が存することをどのように裏付けるか（電子委任状で十分か）、頻繁に権限関係が変わる際に要するコストの評価が論点となる。

機器に係る証明については、個々の機械を弁別するためのID の発行・管理（証明の基点がハードウェア化された堅牢なデバイスかどうか、など）及び自動化された処理の堅牢性に係る認証の論点、その機器の較正基準やセキュリティなどの論点がある。特にIoT 時代においては、幅広い多様な機器についても真正性が確認できる簡便な手段が提供されることが重要である。

改ざん防止（完全性の担保）については、a)意思表示の証明※と同様。

※ a)意思表示の証明 対面での確認、公的書類での確認、自己宣言など、サービスレベルに応じた本人確認レベルの区別や認証レベル（例：任意のID・PW、二要素認証、二段階認証、その中間）についての考え方の整理を行っていく必要がある（真正性の担保）。当該意思表示が改ざんされていないことも証明する必要（完全性の担保）があり、そのためには改ざんを検知し、それを公開する仕組みに関するルールを策定する必要がある。（同とりまとめ（P33）から抜粋）

eIDAS規則 Article3

‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;（「eシール」とは、データの起源と完全性を保証する為に電子データに添付又は論理的に関係している電子形式のデータをいう；）

検討事項

① eシールに求められる要素（その２）

【検討事項】

- 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※1を満たす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）

※1　組織等の実在性確認の方法、電子証明書のフォーマット、eシール生成装置の基準等の一定の水準

主な用途例：国際取引等における証憑類、法的に保存義務が課されているデータ、排他的独占業務とされている士業の証明書等

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）

主な用途例：行政手続における提出書類※2、民民の契約に関連する書類、IR関連資料等の公開情報等

※2　用途によっては、レベル3が必要となるケースも考えられる

レベル1：裸のeシール（eシールの定義（P4参照）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）

主な用途例：民民における企業間で日常的にやり取りされる電子データ全般、発行元を担保したい情報等

- 上記のレベル分けに加えて、さらに細かいレベル分けの検討は必要か。

【参考】

✓ 電子署名法：認定認証業務、特定認証業務、第2条第１項の電子署名（定義）

✓ EUのeIDAS：適格eシール、先進eシール、（裸の）eシール（定義）

提案募集から見られるユースケースのレベル分け（例）

	分類① 契約関係	分類② 組織が公開する情報	分類③ 組織が発出する証明書	分類④ 官民間のやりとり	分類⑤ 監査関係	分類⑥ その他
高 発出元証明による信頼性担保の必要性 レベル3		• 気象データ	• 資格証明書（排他的独占業務とされている士業等）等 • 商工会議所が発行する貿易関係書類	• 法令上保存義務のある書類（国税関係等）		
	• 領収書	• IR関連資料	• 健康診断結果証明書	• 国への各種申請書類等	• 監査の合格証明書	
レベル2	• 請求書 • 見積書 • 納品書 • 受領書 • 【契約書】	• 広報資料 • 【会社法に定める議事録】	• 生産者証明書 • 在学、卒業証明書 • 機器の保証書、ライセンス証書 • 加工証明書	• 請負、委託業務の成果物	• 残高証明書	
		• デジタル名刺	• 機器測定データ		• 企業文書	• 情報連携基盤・クラウド環境等でやり取りされるデータ
レベル1 低		• 企業間でやりとりされる一般的なデータ				

【 】内は、本来、意思表示を目的とする“電子署名”が馴染むと考えられるユースケース

主に機械的に大量に発行するものにeシールの活用が期待

次回の検討事項（予定）

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等の範囲

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（一定の技術基準（CRL（失効リスト）等）等）

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