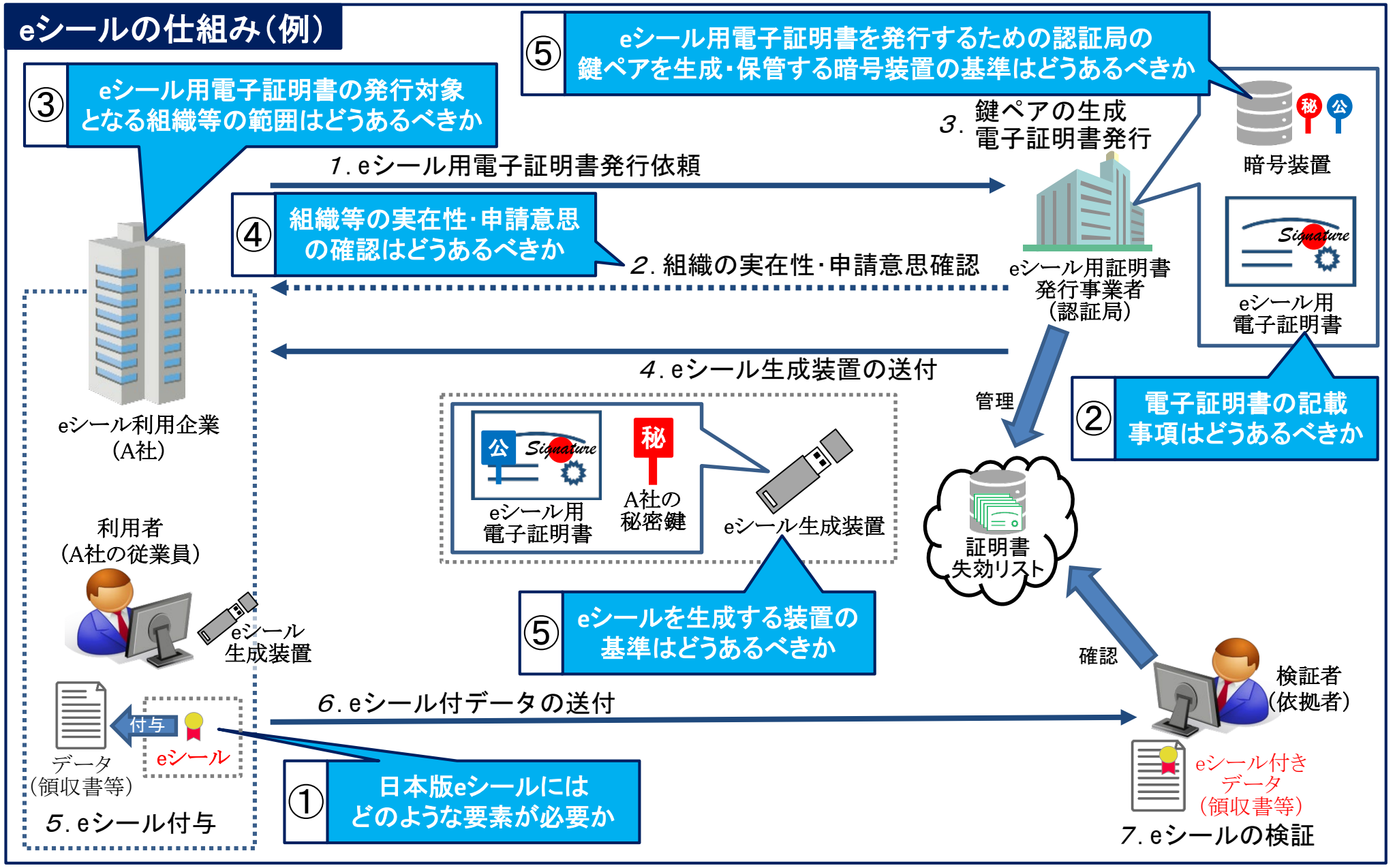
資料11－１

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11回）事務局資料

令 和 ３ 年 ３ 月 ２ ６ 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（リモート方式、CRL（失効リスト）等）等）

前回検討会（第10回）の振返り

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備自体の基準～認証局側の設備～

【検討事項】

- レベル3のeシールにおける、認証局側の設備であるHardware Security Module（HSM※1）の基準はどうあるべきか。

※1 耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置

【議論であがった主な意見】

- 国内の類似制度や国際的な通用性も鑑みて、ISO/IEC 15408（コモンクライテリア）のEAL4+又はFIPS140-2 レベル3を求めることが適当ではないか。
- 現状の日本の認証局の数を考えると、HSMの基準として日本独自のプロテクションプロファイルを作成するのはコストがかかり過ぎるので、望ましくない。ISO/IEC 15408は国際相互認証されており、プロテクションプロファイルはそのためにあるので、それを適用するのがよいのではないか。
- 電子署名法と同等の基準を設けるということでよいと思う。現状の電子署名法の規定では、特定の認証取得製品に限定しておらず、FIPSでもISO/IEC 15408でも使用できるような記載になっているため、同じような記載でいいのではないか。その上で、実際にどのような製品（FIPS認証製品なのか、ISO/IEC 15408認証製品なのか、その他の認証製品なのか等）を使っていくかは別の議論。

【方向性】

- **<u>レベル3のeシールにおける認証局側のHSMの基準は、</u>**基本的には**<u>電子署名法を準用</u>**することとする。ただし、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+相当とする。

注）電子署名法の現行の基準はFIPS140-1 レベル3相当

前回検討会（第10回）の振返り

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備自体の基準～ユーザー側のeシール生成装置～

【検討事項】

- レベル3のeシールにおける、ユーザー側のeシール生成装置の基準を求めることが適切か。
  求める場合、その基準はどうあるべきか。

【議論であがった主な意見】

- 日本でも少なくともQSCD相当のものを使用して耐タンパ性能が確保されたところで秘密鍵が管理されるよう規程の整備が必要ではないか。Society5.0やDFFTを実現していく上で、データを自動で検証して処理し、更にそのデータが自動処理されていくということを想定していくと、検証時に秘密鍵が適切な環境で保護されているかどうかを確認できる必要がある。レベル3のeシールでQSCDを求めるかどうかは別の議論になるが、EUのQCステートメントのように、少なくとも検証時において、QSCDを使用していることがわかるような制度にした方がいい。
- 電子署名法とのバランスが重要である一方、EUとの相互運用の関係もあるので非常に難しい問題。商業登記や法的効力のある電子署名法でも署名生成装置は規定されておらず、また、実世界でも実印の管理については規定がないため、QSCDの規定は設けないという考え方が1つある。電子署名には推定効というものがあるが、eシールがそれ以上の効力を持つことは考えられないのでeシールにのみQSCDを求めるというのは全体のバランスを欠くのではないか。
- QSCDの規定を設ける場合、QSCDの使用/未使用によってeシールの効力にどれだけ違いが出るのかについては、レベル2、3問わずeシールには現段階では法的効力がないことを考えると、EUの適格として通用するかどうかではないか。
- 選択肢としては、電子署名法でもeシールでも両方QSCDを求めるか、あるいは両方求めないか、という2択になるのではないか。両方求める場合は、現状規定のない電子署名法は規制強化になってしまうことが懸念される。他方、両方求めない場合はEUと相互運用を目指す際に課題となる。従来の我が国の法制度の中での秘密鍵等の管理は本人に任されていて本人の責任であるという考え方を維持するのであれば、QSCDは必須にしないが、秘密鍵等の管理の方法として、QSCDを使用する方法もあるということやEUとやりとりする際のオプションとして使用することをガイドライン等に記載するのはどうか。
- eシールの普及という観点では、国内での申告や申請等に利用するということでレベル2の世界で考え、レベル3については欧州等の諸外国との相互運用に値する他国に恥じない基準にすることが適切ではないか。
- EU等の諸外国との相互運用の観点も重要であるが、QSCDの規定を設ける場合は実際の企業側の運用と基準がどうフィットするのかについても検討が必要ではないか。

前回検討会（第10回）の振返り

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備自体の基準～ユーザー側のeシール生成装置～（続き）

【方向性】

- 国内の法的効力をもつ電子署名でも署名生成装置に関する規定がない現状とのバランスを考慮し、当面は、**eシールにおいても一定の基準を満たしたeシール生成装置を用いることを認定の要件とはしない**ことが適当。
- ただし、**第三者機関による認証を受けたeシール生成装置**（例えばEUのQSCDやコモンクライテリアの認証を受けたICチップ等を搭載したICカード等）**を用いてもよい**。
- なお、国際的なやりとりにおいて、諸外国がQSCD等の生成装置を求める場合は、我が国におけるQSCD等の生成装置で秘密鍵を管理して付されたeシールが、海外でも認められるための仕組み（工夫）について今後検討が必要。
- 例えば、QSCDのような第三者機関による認証を受けたeシール生成装置（以下、「認証eシール生成装置」という。）を使用していないにも関わらず、認証eシール生成装置を使用しているように誤認させる表示は禁じる。一方、認証eシール生成装置が用いられている際に、当該eシールが認証eシール生成装置を用いて付されていることを検証者が判断可能な仕組みとすることが適切。
- なお、電子署名法含め、将来的にユーザー側の生成装置に関してセキュリティ上の問題が生じた場合には、改めてQSCDの要否について検討が必要。（例えば、トラストサービスの包括的な枠組の検討を機に生成装置に係る規定を設ける場合は、現状の電子署名法の規制強化（今まで可としていたものが不可となってしまう）につながる点を留意した上で検討が必要。）

前回検討会（第10回）の振返り

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備の管理に係る基準～認証局側の設備～

【検討事項】

- レベル3のeシールにおける、認証局側のHSMの管理に係る基準はどうあるべきか。

【議論であがった主な意見】

- 電子署名法の認定認証業務で要求している基準と同等の基準を求めることが適切ではないか。

【方向性】

- **レベル3のeシールにおける認証局側のHSMの管理に係る基準は、**基本的には**電子署名法を準用**することとする。

前回検討会（第10回）の振返り

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備の管理に係る基準～ユーザー側のeシール生成装置～

【検討事項】

- レベル3のeシールにおける、ユーザー側のeシール生成装置の管理に係る基準はどうあるべきか。
  - １つのeシール生成装置を複数人で共同で使用することを認めるか。
  - 又は、同一の秘密鍵を複数のeシール生成装置に格納し、複数人がそれぞれ管理して使用することを認めるか。
  - 又は、同一の組織等に対して複数のeシール用電子証明書を発行することを認めるか。
- 単にeシールを機械で自動的に付すことを認めるか。認める場合、特段の要件を求める必要があるか。

【議論であがった主な意見】

- eシール生成装置の管理については、①複数人での共同使用、②秘密鍵自体の複製、③同一組織等への複数のeシール発行のいずれかを認めなければ、利便性が低下して実質的に制度としての効果が限定される可能性があるという事務局の懸念に賛同。
- EUでは法人の管理下にあることが求められており、電子署名法でも実質的には同じルールになっているため、特段の要件は不要ではないか。
- EU等の諸外国との相互運用の観点も重要であるが、QSCDの規定を設ける場合は実際の企業側の運用と基準がどうフィットするのかについても検討が必要ではないか。（再掲： 設備自体の基準～ユーザー側のeシール生成装置～）

【方向性】

- 電子署名法でも規程がなく、EUでも法人の管理に委ねられていることに鑑み、**eシール生成装置の管理は発行対象である組織等の管理に委ねる**こととし、**特段の規定は設けない**ことが適切ではないか。

検討事項

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

〇eシールの大量発行に係る検討

【検討事項】

- レベル3のeシールにおいて、eシールを大量発行処理をする場合、複数の対象文書に一括でeシール付与の認証（指示）を行うことを認めるか。

➡ 実世界における決裁・押印等の手続を鑑みると、一度の認証で大量の付与対象データにeシールを付すことを認めることは適当ではないか。
ただし、その場合は利用者が認知・意図しない部分、すなわち利用者が対象文書に対するeシール付与の指示を行って以降、他のデータが紛れ込むことがないことをeシールサービス側で担保する必要があるのではないか。

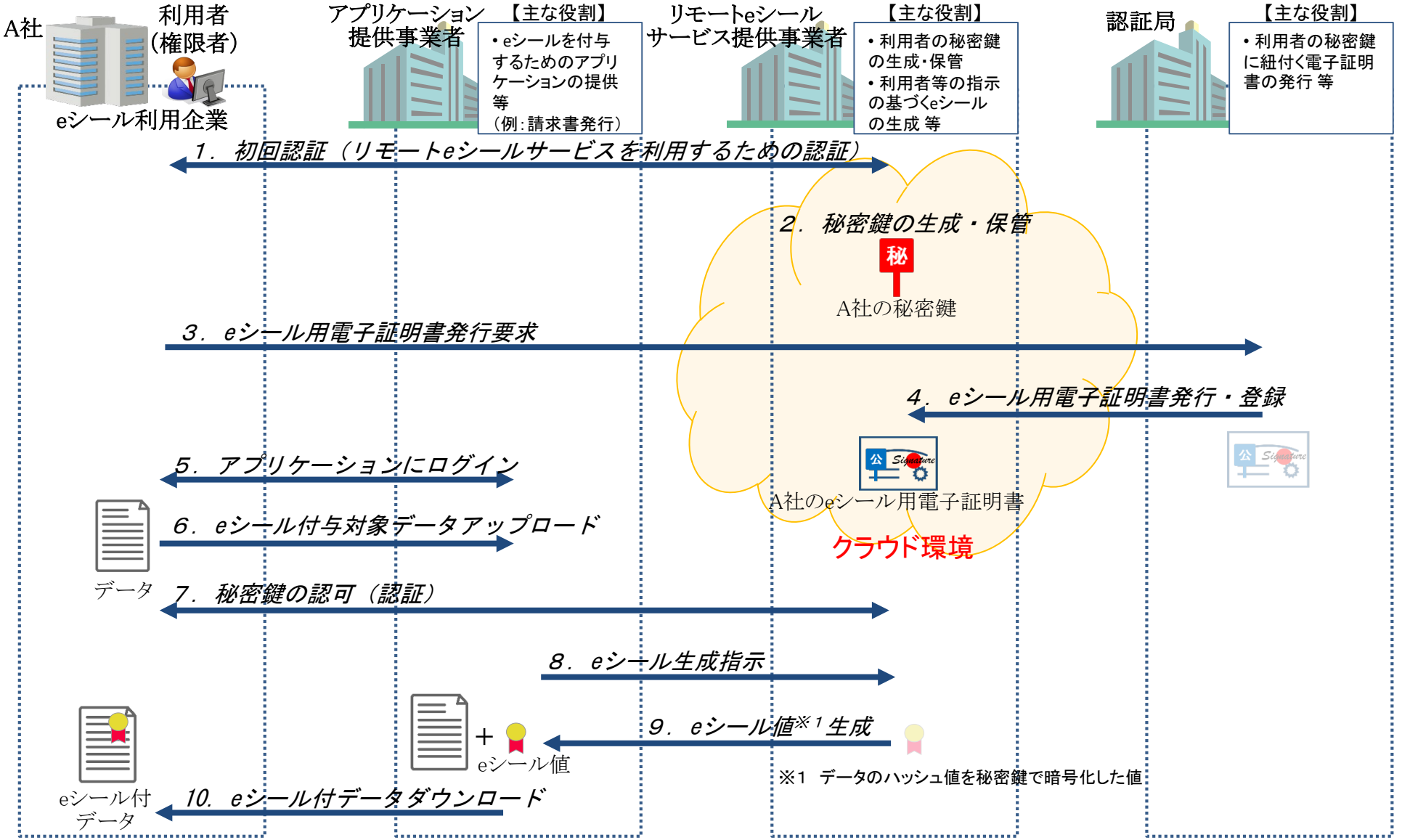
＜参考＞

✓ EU：ローカルeシールの場合は、署名対象及び秘密鍵共に署名者の管理下にあり、その際の一括署名に関する特段の規定はない。
リモートeシールの場合は、一括署名方式について加盟国によって対応が分かれているが、技術基準は存在する。（資料11-2参照）

検討事項

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

○ リモートeシール方式の一例（リモートeシール利用申込及び認証局による組織の確認後）

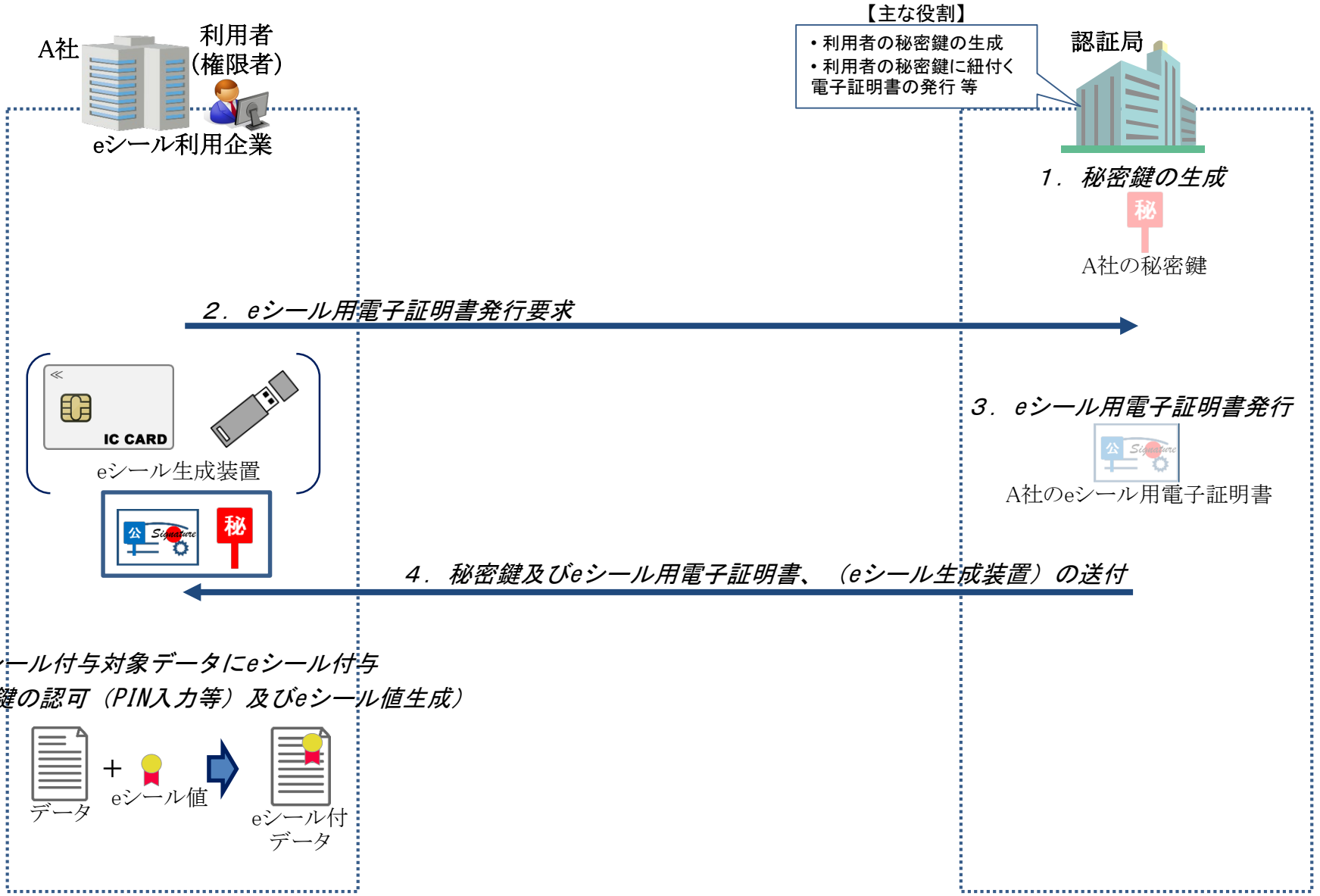


注） 認証局、リモートeシールサービス提供事業者のそれぞれを同一の事業者が行う場合もあり得る

検討事項

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

○（参考）ローカルeシール方式の一例（eシール利用申込及び認証局による組織の確認後）



検討事項

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

○eシールのリモート方式※1に係る検討

【検討事項】

※1 利用者がリモート環境にある秘密鍵にアクセスしてeシール等の措置を行う方式

※2 日本トラストテクノロジー協議会（JT2A）が作成したリモート署名に関する技術的な基準を示したガイドライン

- リモートeシールサービス提供事業者が利用者の秘密鍵を管理し、利用者がそのリモート環境にある秘密鍵にアクセスしてeシールを付す方式であるリモートeシールについて、レベル3のリモートeシールを付す際にはどのような認証が必要か。
- なお、ローカルeシールでは、利用者自ら秘密鍵を管理していることに留意。

＜参考＞

✓ リモート署名ガイドライン※2：レベル2（電子署名法における認定認証業務と同等の信頼性を想定）では、サービス提供を受けるための利用者の認証（以下、「利用認証」という。）と秘密鍵（署名鍵）を利用するための鍵認可を分けて行うこと、また、鍵認可は複数要素認証を行うことを要求。

- 利用認証
  - リモートeシールサービスへのログインの際のID/PW認証等
- 鍵認可
  - 知識要素：PINコード等
  - 所持要素：ワンタイムパスワード等
  - 生体要素：指紋等

（これらの2つ以上の組合せを要求。）

✓ EU：SCAL2（適格レベル）では、利用認証と鍵認可を分けて行うこと、また、鍵認可はコモンクライテリアの認証を取得した署名活性化モジュールにて行い、複数要素認証を行うことを要求。

➡ リモートeシールの場合は、リモート署名と同様に少なくともeシールを付すことができる権限者（リモートeシールサービスへの登録者）であることを認証するための利用認証と実際にeシールを付すために必要な認証である鍵認可、すなわち2段階認証が必然的に求められるのではないか。

ただし、電子署名には推定規定があるが、eシールには現段階では推定規定がないことを鑑みると、鍵認可については、複数要素認証まで求める必要はないのではないか。

検討事項

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

〇eシールのリモート方式に係る検討（続き）

【検討事項】

- レベル3のリモートeシールにおいて、eシールを付す際の鍵認可で使用する知識要素（PINコード等）や生体要素（指紋等）等の認証要素の管理はどうあるべきか。
  - ➢ 利用者のみが管理することを求めるか。
  - ➢ リモートeシールサービス提供事業者やアプリケーション提供事業者が管理することも認めるか。

＜参考＞

✓ リモート署名ガイドライン： レベルを問わず、利用者本人のみが秘密鍵（署名鍵）を活性化（鍵認可）できることを要求。

✓ EU： 認証要素の管理は法人に委ねられ、アプリケーション提供事業者が管理することも否定されていない。

リモートeシールにおいて、リモートeシールサービス提供事業者が利用者に断りなくeシールを付すことができる可能性がある場合は、そもそも認証要素としての意義が失われ、eシールを付した利用者、すなわち発行元が誰であるかの判断ができなくなる可能性がある。

加えて、eシールの場合には、eシールが付されたデータを受け取る者には、リモートeシールサービスの利用について協議を受けられない蓋然性が高い（電子署名の場合には、文書の名義人間で、どのような方式を取るかの合意があるため、リモート署名サービスの利用について、双方の合意があるとみなす余地がある）。

このため、レベル3の電子証明書を用いたリモートeシールにおいて、eシールを付す際の鍵認可で使用する認証要素の管理が適切に行われない可能性がある場合には、信頼性のないレベル3のeシールが存在することなるため、制度の安定性そのものに影響を与えかねない。

これらを勘案し、eシールとしての用をなさないレベル3のeシールの生成、流通を防止するため、レベル3のeシールをリモートで付与する事業者については、一定の基準（認定制度？）が必要か。

検討事項

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

〇失効に係る検討

【検討事項】

- eシール特有の問題（電子証明書と自然人の紐付けが1対1である電子署名とは異なり、eシールは1つのeシールを複数人で使用することが想定される）として、失効要求ができる者の範囲はどこまでとすることが適切か。
  - ➢ 電子証明書の発行を求めることができる者に限定する。
  - ➢ 上記に加えて、当該eシールを付す権限を有する者でも可とする。
  - ➢ 当該eシールの発行を受けた組織等に属する者であれば誰でも可とする。
- その他、失効に係る事項でeシール特有の検討すべき事項はあるか。

➡ 失効要求についても、eシール用電子証明書の発行申請と同様に意思表示が必要であると考えられることから、失効要求できる者は電子証明書の発行を要求できる者（法人であれば代表者又は代表者から委任を受けた者）に限定することが適当か。

＜参考＞

✓ EU：誰が失効要求を行うことができるのかについて、法人と認証局間で予め取り決めをしておくことが求められている。
なお一例として、失効要求時にパスワード認証等を行うこととし、そのパスワードを知っている者を失効できる者としている等がある。

検討事項

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

○失効に係る検討

【参考】

～電子署名及び認証業務に関する法律施行規則～（抜粋）

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。

[一～九　略]

十　電子証明書の有効期間内において、**利用者から電子証明書の失効の請求**があったとき又は電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該電子証明書の失効の年月日その他の失効に関する情報を電磁的方法（電子的方法、磁気的方法その他の人の知覚によっては認識することができない方法をいう。以下同じ。）により記録すること。

十一　電子証明書の有効期間内において、署名検証者からの求めに応じ自動的に送信する方法その他の方法により、署名検証者が前号の失効に関する情報を容易に確認することができるようにすること。

十二　第十号の規定により電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該電子証明書の利用者にその旨を通知すること。

～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～（抜粋）

第八条　規則第六条第一号に規定する利用申込者に対して説明を行うべき事項とは、次の各号に掲げる事項を内容として含むものとする。

[一・二　略]

三 利用者署名符号が危殆化（盗難、漏えい等により他人によって使用され得る状態になることをいう。以下同じ。）し、又は危殆化したおそれがある場合、電子証明書に記録されている事項に変更が生じた場合又は電子証明書の利用を中止する場合においては、遅滞なく電子証明書の失効の請求を行わなければならないこと。

第十二条 規則第六条第十三号に規定する認証業務の実施に関する規程は、次の各号に掲げる事項に関する規定を含むことを要するものとする。

[一～四　略]

五　電子証明書の失効の請求に関する事項

六　電子証明書の失効に関する情報の確認の方法及び確認することができる期間に関する事項

[七～十二　略]

2　前項第十号に掲げる事項には、認定に係る業務を廃止する日（認定の更新を受けない場合においては、認定期間の満了の日。以下同じ。）の六十日前までにその旨を利用者に通知すること（法第十四条第一項の規定により認定を取り消された場合等、やむを得ない場合はこの限りでない。）及び認定に係る業務を廃止する日までに利用者に対して発行した電子証明書について失効の手続を行うことが含まれるものとする。

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

第8回の振返り①

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

【議論であがった主な意見】

- eシールの定義を発行元証明とすることに賛同。
- eシールと電子署名の違いを明確にし、使う側がどちらを使えばいいのかを明確にわかるようにした方がいい。
- 出口戦略として、法令上の整理をすることが必要。（→個別の保存義務付け制度で措置すべきか）

【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。

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；）

第8回の振返り②

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。

【議論であがった主な意見】

- 用途等にあわせてレベル分けすることに賛同。
- eシールは必ずしも完璧なものである必要はなく、例えば印鑑では印鑑登録しているものに限定していることもあれば、緩いものが使われることもあり、レベル分けされたeシールがあるのはいいこと。
- 中小企業等がレベル2，3のeシールを扱う場合も考慮し、事業者視点で利用しやすいように設計することが必要。
- 証明書の発行に関するレベル分けだけではなく、署名鍵の管理に関するレベル分け（１つのeシールをごく少数でしか扱えないのか、多人数で扱えるのか、機械的に扱えるのか）の観点も重要ではないか。
- eシールの法的効果として、「組織から発出されたことが推定できる」といったことを規定できるといいのではないか。
  →我が国では、民事訴訟法第247条の規定により、自由心証で裁判官の判断がなされる。推定効のようなものがなかったとしても、eシールが仮に国の認定制度になった場合に、国のお墨付きを受けたeシールを裁判官が無下にすることは考えにくいのではないか。

【方向性】

- 我が国におけるeシールは以下のようにレベル分けを行う。

※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
※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）

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

レベル1：裸のeシール（eシールの定義（P3参照）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

第9回の振返り①

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

【検討事項】

- eシール用電子証明書の発行対象となる組織等の範囲は以下のどこまでを含めることが適切か。
  - 法人、個人事業主、権利能力なき社団・財団、その他の団体等の組織
  - 事業所・営業所・支店・部門等の組織内の細かい単位
  - その他（組織に所属する個人、機器等）
- eシール用電子証明書の発行対象を特定するための識別子はどうあるべきか。

【議論であがった主な意見】

- eシールは発出元の証明であるということを考慮すると、発行対象は法人（組織）とするのがいいのではないか。
- 発行対象として、事業所等まで含めることが望ましいが、組織の体制とeシールの紐付きが強固になってしまうと、組織の体制の変更等に伴って電子証明書の更新が頻繁に発生し、eシールの利便性の低下に繋がる可能性がある。
- 認証局で事業所等の実在性確認まで行わず、事業所等の情報を代表者の責任で電子証明書に記載するのであれば、当該情報はeシール付与対象のデータに直接記載されていることで十分という考え方もできるのではないか。
- 今後、インボイスでeシールが活用されることを考慮すると、公的なデータベース（識別子）として適格請求書発行事業者登録番号も検討の余地があるのではないか。

【方向性】

- **eシール用電子証明書の発行対象**（認証局の責任の及ぶ範囲）**は、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の組織**とする。（※）
- それよりも粒度の細かい、**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、**eIDASとの整合性を図るため、**電子証明書の任意のフィールドである拡張領域に記載**することができることとする。（事業所等の記載に係る責任は「組織等の実在性・申請意思の確認の方法」に記載）
- eシール用電子証明書の発行対象を特定するための**識別子については、**上記の発行対象（※）を前提とした場合、幅広いID・番号体系が併存し発行対象を網羅的に管理可能な識別子が現状存在しないことに鑑み、**既存のID・番号を包括的に表現可能な方式**（OID：Object Identifier（オブジェクト識別子）等）**を軸として今後検討**することが必要。

第9回の振返り②

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

【参考】

（ヒアリング等の結果に基づき、事務局にて一例として整理）

			法人番号	会社法人等番号	企業コード				その他
					TDB企業コード	TSR企業コード	D-U-N-S® Number	LEI	
eシール用電子証明書を発行する対象	組織・団体等	法人	○	○	○	○	○	○	—
		権利能力なき社団・財団	○	—	○	○	○	—	—
		その他任意の団体	—	—	○	○	○	—	—
		個人事業主	—	—	○	○	○	○	—
		その他の個人	—	—	—	—	—	—	マイナンバー、運転免許証、旅券番号 等
拡張領域に記載する対象	その他	事業所・営業所・支店・部門等	—	—	—※1	—※2	△※3	—	—
		担当者	—	—	—	—	—	—	社員番号 等
		機器	—	—	—	—	—	—	型番、シリアルナンバーの組合せ 等

※1　別体系で保持

※2　日本国内に存在する事業所には TSR 企業コードは付与せず、事業所コードを付与。
なお、事業所コードは単独では発番せず、TSR 企業コードに必ず付随する。

※3　事業所単位で付番。日本企業の場合、同一ビル内や事業所内にビジネスユニットが複数存在する場合、D-U-N-S®Numberを発番できるのは 1 箇所のみとなる。

第9回の振返り③

④ 組織等の実在性・申請意思の確認の方法

【検討事項】

- レベル3のeシール用電子証明書の発行に当たり、どのような手続・手段で確認することが必要か。
- 登記よりも小さい単位（事業所・営業所・支店・部門等）については、当該組織の代表者による宣言の結果を尊重することが適切か、または認証局が事業所等の実在性を直接確認することが適切か。
- 機器は事業所・営業所・支店・部門等と同様に扱うか。

【議論であがった主な意見】

- 組織の確認として、事業等の細かい単位まで網羅的に認証局が確認することは、多大な負担となり、困難ではないか。
- 組織の確認に際しては、確認コストも見据えて優先順位付けが必要。公的な書類やデータベースで確認することは認証局にとって手間のかからない方法になる一方、実地調査はコストが高くなってしまう。
- 認証局が組織のどこまで確認するかという問題よりも、その記載した情報に誰が責任を持つかが重要。代表者が宣言していることを認証局が確認するという方法と、認証局においても何らか一定の事業所等の確認をするという方法がある。前者であれば、その事業所等の情報をeシールの証明書に記載することに果たしてどれだけの意味があるのかということについて検討が必要。後者であれば、一定の責任が認証局に出てくるが、それにどれだけ意味が出てくるのかは検討が必要。
- 第三者機関データベースは、それがしっかり管理・構築されているかを確認しその扱いについてランク付けが必要ではないか。
- 組織の確認については、認証局側ですべき確認と第三者機関（TDBやTSR等）で行っている確認との切り分けを明確に整理すべきではないか。

【方向性】

- 組織等の**実在性の確認については、登記事項証明書や第三者機関データベース等で行い、申請意思については、電子署名、押印、署名等で行うことが必要**。ただし、当該申請者（電子署名、押印、署名等をした者）が間違いなく当該組織の代表者であることを確認できることが必要。
- **レベル3のeシール**の電子証明書の発行にあっては、**組織等の実在性の確認に用いるエビデンスが公的な情報に裏付けられたもの**であることが必要。
- 組織等よりも細かい粒度である、**事業所・営業所・支店・部門等や担当者、機器の実在性の確認については、組織の代表者の宣言の結果を尊重**することとし、**認証局の責任の範囲外**であることが適当。

第9回の振返り④

④ 組織等の実在性・申請意思の確認の方法

- eシールに係る電子証明書の発行の手続きの整理は主に以下の表のとおり。
  - 第三者機関データベースにて組織等の実在性確認を行う場合、レベル3にあっては商業登記情報等の公的な機関が管理する情報と照合されたものであることが求められる。

（★）はデジタルで行える手続

	組織等の実在性の確認	組織（代表者）の意思の確認	組織の代表者の在籍の確認
レベル3	• 商業登記電子証明書による電子署名が行われた利用申込 (★)		
	• 登記事項証明書	• 申込書への押印（代表印に係る印鑑証明書が添付されている場合に限る）	
	• 第三者機関が管理するデータベース*（商業登記情報等の公的な機関が管理する情報と照合されたものに限る。）*(★)	• 代表者のマイナンバーカードの署名用電子証明書又は認定認証業務に係る電子証明書等による電子署名が行われた利用申込 (★)…① • 申込書への代表者の署名又は押印…②	【甲： 意思の確認が①の場合】 • 第三者機関が管理するデータベース*（商業登記情報等の公的な機関が管理する情報と照合されたものに限る。）*に登録されている代表者の住所と電子証明書に記載されている代表者の住所の一致の確認（★） 【乙： 意思の確認が②、又は甲で確認できない場合】 • 第三者機関が管理するデータベース*（商業登記情報等の公的な機関が管理する情報と照合されたものに限る。）*に登録されている電話番号等を通じた代表者本人に対する当該申請の有無の確認
レベル2	• 第三者機関が管理するデータベース※(★)		【丙： 意思の確認が①の場合】 • 第三者機関が管理するデータベース※に登録されている代表者の住所と電子証明書に記載されている代表者の住所の一致の確認（★） 【丁： 意思の確認が②、又は丙で確認できない場合】 • 第三者機関が管理するデータベース※に登録されている電話番号等を通じた代表者本人に対する当該申請の有無の確認

※ 定期的に更新され、信頼できるデータソースとしてみなされるデータベース

第9回の振返り⑤

② eシール用電子証明書の記載事項等

【検討事項】

- eシール用電子証明書に記載すべき事項として何が考えられるか。

＜例＞**公式名称（eシール用電子証明書の発行対象の組織等）**、有効期間、公開鍵、署名アルゴリズム、発行者、eシールのレベルを判別可能な情報、その他属性情報（営業所、事業所、機器等）等

- eシール用電子証明書のフォーマットはどうあるべきか。

＜例＞ITU-T X.509

- eシールのレベルに応じて記載事項を検討する必要があるか。

【議論であがった主な意見】

- eシール用電子証明書のフォーマットとして、X.509を採用することには異論なし。
- 発行対象を一意に特定可能な識別子は記載する必要がある。

【方向性】

- **レベル2及びレベル3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。
- 電子証明書には、**発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子、有効期間、公開鍵、署名アルゴリズム、発行者、eシールのレベルを判別可能な情報、その他属性情報（営業所、事業所、機器等）等を記載**することとする。なお、レベル2で第三者による評価を受けている場合は、評価を行った第三者機関を拡張領域に記載することを認める（レベル3の場合は、制度上明確化された認定主体であるため記載は自由）。レベル3、レベル2に関わらず、記載項目は変わらない。
- eシールのレベルを判別するための呼称（eIDASの例：適格（Qualified）、先進（Advanced）、裸のeシール）については将来決定することが必要。

第9回の振返り⑤

② eシール用電子証明書の記載事項等

【参考】

- eシール用電子証明書（ITU-T X.509）の記載の一例

	フィールド名	値（サンプル）
基本領域	バージョン	V3
	シリアルナンバー	WWWWWWWWW
	署名アルゴリズム	sha256RSA/sha512RSA
	署名ハッシュアルゴリズム	sha256/sha512
	発行者	発行者を識別する情報
	有効期限の開始時刻	Monday, January 5, 2020 5:00:00 PM
	有効期限の終了時刻	Thursday, January 5, 2022 5:00:00 PM
	サブジェクト	発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子等
	公開鍵	RSA (2048bit)
	公開鍵パラメータ	05 00 …
拡張領域	認証機関アクセス情報	[1]CA証明書のURL [2]OCSPのURL
	サブジェクト鍵識別子	YYYYYYYYYY
	QCステートメント	eシールのレベルを判別可能な情報等
	証明書ポリシー	[1]0.4.0.194112.1.1/0.4.0.194112.1.3 [2] http://xxxxxxxxxxxxxx
	CRL配布ポイント	http://xxxxxxxxxxxxxxxCA.crl
	基本制約	Subject Type = End Entity
	鍵使用目的	Non-Repudiation (40)

注） 赤字は具体的な記載方法について、今後検討が必要な項目