EUにおけるeシールの基準

株式会社コスモス・コーポレイション
濱口　総志

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

eシールとSociety5.0、DFFT

eシールの特徴

- デジタル署名
  eIDAS規則は技術的中立性の観点からデジタル署名方式に限定していないが…

- 適格eシールであればデータの起源（origin)と完全性が推定される
  データの発出元の信頼性と、そのデータが改ざんされていないことの保証

- 自動処理可能
  自然人の意志に基づく電子署名と異なり、
  eシール生成の都度自然人の意志確認を必要としない。
  ➡法人の管理下にあるシステムや装置が自動でeシールを生成できる。

オープンバンキングやX-Road等でeシールが利用されており、異なる組織間のデータ連携時のリクエストやレスポンスの信頼性を自動で保証/検証する仕組みとして利用できる

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

*eIDAS reg. Art. 3 定義 (27)

適格eシール ＝ 先進eシール ＋ 適格証明書 ＋ 適格eシール生成装置

先進eシール

eIDAS reg. Art. 36 先進eシールの要件

eIDAS reg. Art. 37 公的セクターにおけるeシール

委員会実施決定 2015/1506
AdESフォーマット
- ETSI TS 103171(XAdESベースラインプロファイル),
- ETSI TS 103173(CAdESベースラインプロファイル),
- ETSI TS 103172(PAdESベースラインプロファイル),
- ETSI TS 103174(ASiCベースラインプロファイル)

電子データと組織の紐づけと電子データの完全性を保証

＊証明書で保証される組織と電子データの紐づけを保証する仕組み

適格証明書

eIDAS reg. Art. 38 eシールの為の適格証明書

eIDAS reg. Annex III eシールの為の適格証明書に対する要件

ETSI EN 319412 適格証明書プロファイル

法人の身元と実在性を保証

＊実在の組織情報をサイバー空間で保証する仕組み

適格トラストサービスプロバイダが適格証明書を発行する（eIDAS Reg. Art.3）

適格トラストサービスプロバイダ

eIDAS reg. Art. 19 トラストサービスプロバイダに適用されるセキュリティ要件

監督（eIDAS Reg. Art. 20）

適合性評価機関が適格トラストサービスプロバイダを監査(eIDAS reg. Art. 20)
- ETSI EN 319 401 (一般ポリシー要件)
- ETSI EN 319 411-1 (認証局のポリシー要件)
- ETSI EN 319 411-2 (適格証明書を発行する認証局のポリシー要件)

監督機関

eIDAS reg. Art. 17 監督機関

適合性評価機関

Reg. (EC) No 765 /2008 Art. 2

認定機関が適合性評価機関を認定する (Reg. (EC) No765/2008 Art. 3)
- ETSI EN 319 403
- ISO/IEC 17065

認定機関

Reg. (EC) No 765 /2008 Art. 4

適格eシール生成装置

eIDAS reg. Art. 39 適格eシール生成

eIDAS reg. Annex II 適格eシール生成の要件

法人のみがeシールを生成できることを保証

＊証明書に対応する秘密鍵が法人の管理下にあることを保証する仕組み

適切な機関が適格電子署名生成装置を認証する(eIDAS reg. Art. 30)
委員会実施決定 2016/650
- ISO/IEC 15408
- EN 419 211 (Protection Profiles)

適切な機関

eIDAS reg. Art. 30 適格電子署名生成装置の認証

加盟国は適切な機関を指定する（eIDAS reg. Art. 30）

加盟国

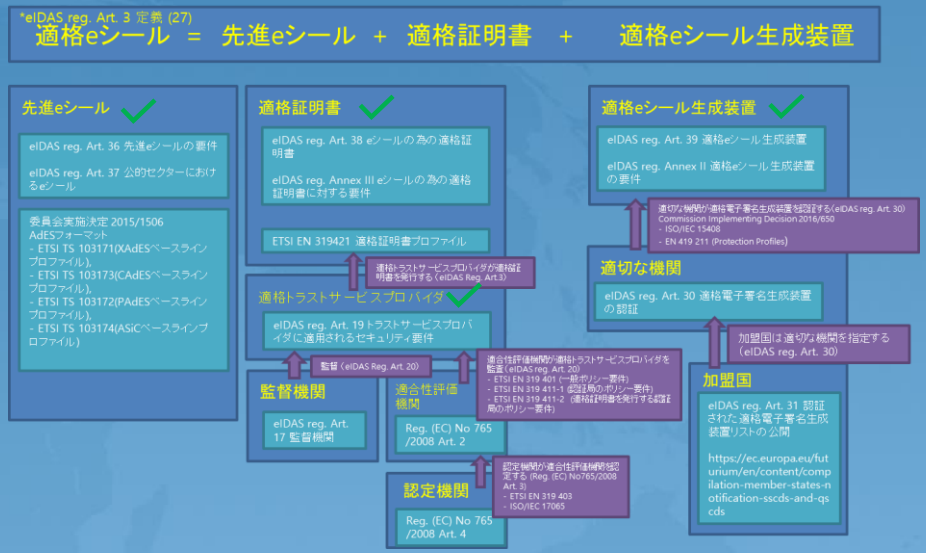
eIDAS reg. Art. 31 認証された適格電子署名生成装置リストの公開

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

eシールの検証

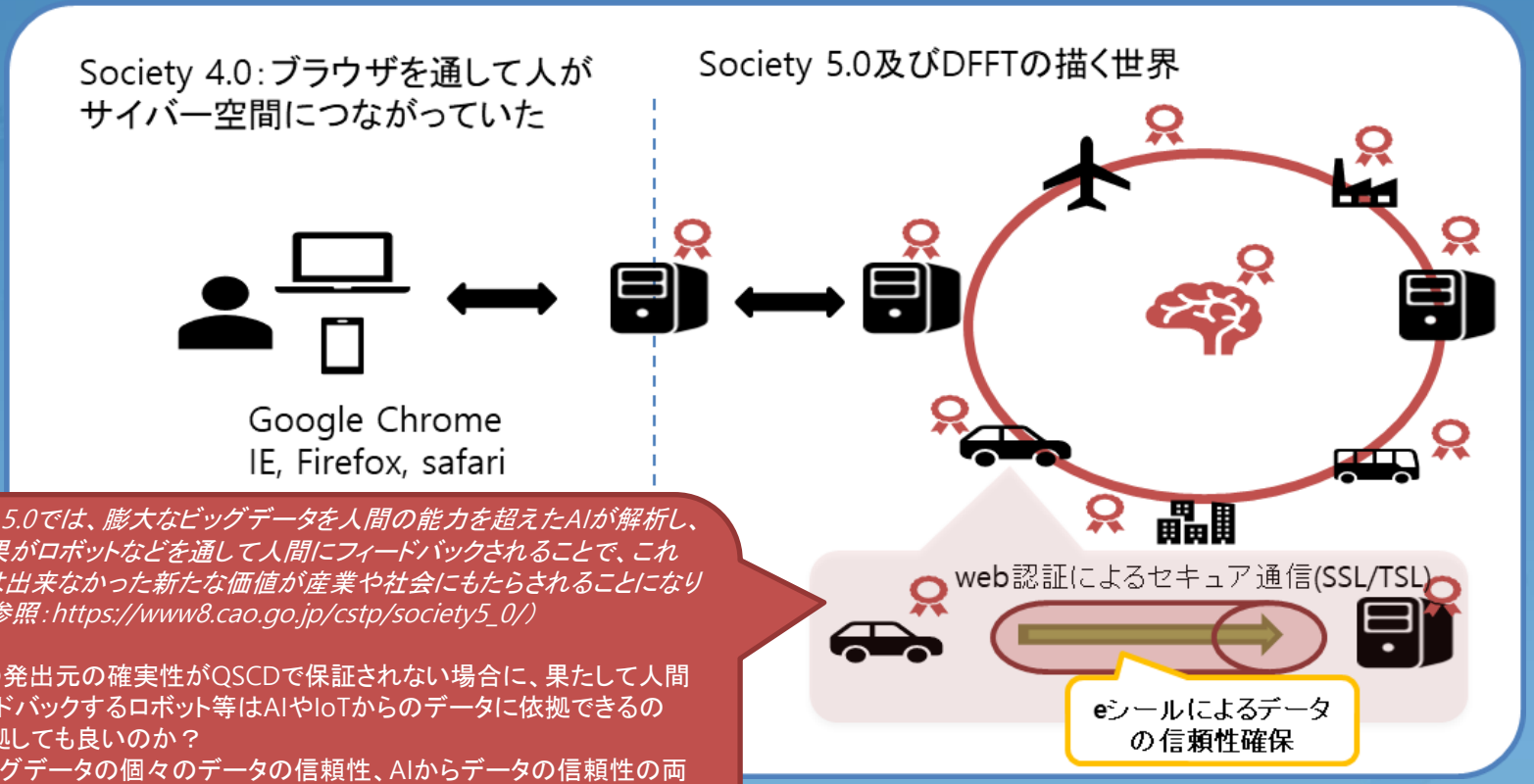
eシール付きデータの受信者はeシールをトラステッドリストと合わせて検証することで、eシールが適格eシールの条件を満たしていることが自動的に判別できる。

- 先進eシールであるか ➡ デジタル署名の検証 ✓
- eシール用の適格証明書であるか ➡ id-etsi-qcs-QcCompliance / id-etsi-qct-eseal ✓
- 適格証明書が適格トラストサービスプロバイダから発行されているか
  ➡ 発行者をトラステッドリストで検証 ✓
- 適格eシール生成装置が利用されているか ➡ id-etsi-qcs-QcSSCD ✓



Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

問1. QSCDは必要か？

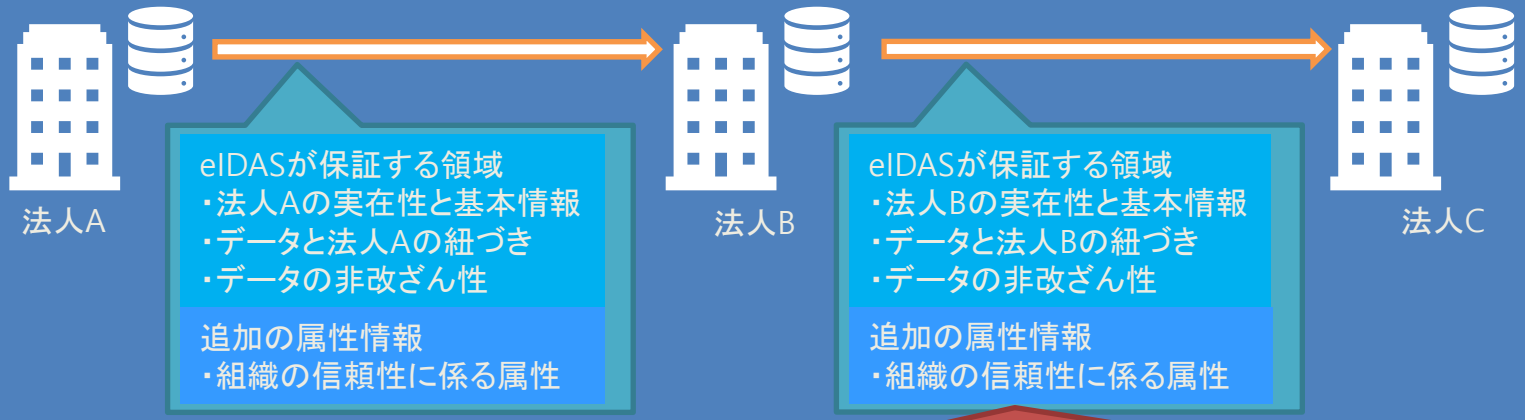


Society 5.0では、膨大なビッグデータを人間の能力を超えたAIが解析し、その結果がロボットなどを通して人間にフィードバックされることで、これまでには出来なかった新たな価値が産業や社会にもたらされることになります。（参照：https://www8.cao.go.jp/cstp/society5_0/）

データの発出元の確実性がQSCDで保証されない場合に、果たして人間へフィードバックするロボット等はAIやIoTからのデータに依拠できるのか？依拠しても良いのか？
e.g. ビッグデータの個々のデータの信頼性、AIからデータの信頼性の両方について制度として秘密鍵の保護環境を保証しない場合…事故発生時の責任の所在は明確化できるのだろうか…

問2. eシールの保証する信頼性とは？

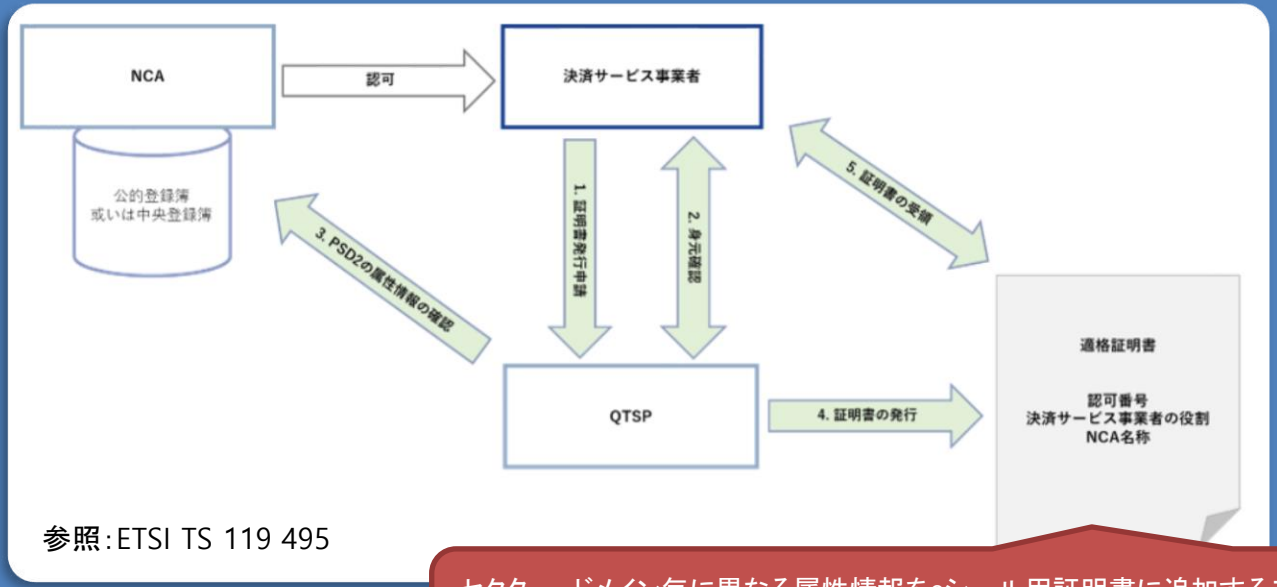
eIDAS規則におけるeシールはデータと組織の紐づけを保証する仕組み
➡組織が信頼できる組織であるか否かは制度の対象外であるが…



セクター、ドメイン毎に異なる属性情報をeシール用証明書に追加することで、組織の実在性とデータとの紐づき以上の信頼性を保証することが可能となっている。

PSD2における属性情報の追加例

認証局が決済サービス事業者の属性情報をNCA（金融当局）に確認することで、証明書に追記することで、eシールのフレームワークにPSD2の属性情報を載せることができる。



参照：ETSI TS 119 495

セクター、ドメイン毎に異なる属性情報をeシール用証明書に追加することで、eシールのフレームワークを**拡張し**、より詳細な組織の信頼性に関する情報を載せることが可能になっている。

*eIDAS reg. Art. 3 定義 (27)

適格eシール ＝ 先進eシール ＋ 適格証明書 ＋ 適格eシール生成装置

先進eシール

eIDAS reg. Art. 36 先進eシールの要件

eIDAS reg. Art. 37 公的セクターにおけるeシール

委員会実施決定 2015/1506
AdESフォーマット
- ETSI TS 103171(XAdESベースラインプロファイル),
- ETSI TS 103173(CAdESベースラインプロファイル),
- ETSI TS 103172(PAdESベースラインプロファイル),
- ETSI TS 103174(ASiCベースラインプロファイル)

電子データと組織の紐づけと電子データの完全性を保証

＊証明書で保証される組織と電子データの紐づけを保証する仕組み

適格証明書

eIDAS reg. Art. 38 eシールの為の適格証明書

eIDAS reg. Annex III eシールの為の適格証明書に対する要件

ETSI EN 319412 適格証明書プロファイル

法人の身元と実在性を保証

＊実在の組織情報をサイバー空間で保証する仕組み

適格トラストサービスプロバイダが適格証明書を発行する（eIDAS Reg. Art.3）

適格トラストサービスプロバイダ

eIDAS reg. Art. 19 トラストサービスプロバイダに適用されるセキュリティ要件

監督（eIDAS Reg. Art. 20）

適合性評価機関が適格トラストサービスプロバイダを監査(eIDAS reg. Art. 20)

適格eシール生成装置

eIDAS reg. Art. 39 適格eシール生成

eIDAS reg. Annex II 適格eシール生成の要件

法人のみがeシールを生成できることを保証

＊証明書に対応する秘密鍵が法人の管理下にあることを保証する仕組み

適切な機関が適格電子署名生成装置を認証する(eIDAS reg. Art. 30)
委員会実施決定 2016/650
- ISO/IEC 15408
- EN 419 211 (Protection Profiles)

適切な機関

eIDAS reg. Art. 30 適格電子署名生成装置の認証

加盟国は適切な機関を指定する（eIDAS reg. Art. 30）

このフレームワークが色んなセクター、ドメインにおけるデータ連携を支える技術として利用可能になる

➡根幹となるeシールのフレームワークの制度、技術基準を適切に整備/維持することが**重要！！！！！！なんです！！！！**

ご清聴ありがとうございました

株式会社コスモス・コーポレイション
ITセキュリティ部
濱口 総志
E-Mail：s.hamaguchi@cosmos-corp.com
http://www.safetyweb.co.jp/

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING