デジタル時代、トラストサービスの信頼基盤となるHSMとは？
～電子データの信頼性を支えるHSMについて～

東京エレクトロン デバイス株式会社

CN BU　CN技術本部
プロダクト第三技術部 第四グループ
小林　俊一

会社概要

会社名	**東京エレクトロン デバイス株式会社**
設立年月日	1986年3月3日
代表者	代表取締役社長　徳重　敦之
上場証券取引所	東京証券取引所 プライム市場 （証券コード：2760）
資本金	24億9千5百万円（2024年3月31日現在）
売上高	242,888百万円（2024年3月期）
従業員数	連結: 1,357名（2024年3月31日現在）
本社所在地	神奈川県横浜市神奈川区金港町1-4 横浜イーストスクエア

TOKYO ELECTRON DEVICE

取扱い製品

Connect Beyond

Security Cloud

マルチクラウド

クラウド

aws

Microsoft Azure

App配信＆Sec

Distributed Cloud Services

CNAPP

WIZ

IaC

HashiCorp Terraform

シークレット管理

HashiCorp Vault

セキュリティ診断

ASV

PENTERA

クラウドアクセス/ゼロトラストソリューション

エンドポイント

SentinelOne

SSE／SASE

netskope

CASB／SWG

IDaaS

okta

HSM

ENTRUST

THALES

SIEM

DEVO

社内アクセス/多層防御ネットワークソリューション

Wi-Fi

ARISTA

Extreme networks

VPN

WAF

NGINX Part of F5

NDR

ARISTA

DNS/DHCP

infoblox

Firewall

paloalto NETWORKS

FORTINET

Infrastructure

仮想化基盤ソリューション

HCI

NUTANIX

3Tier

PURESTORAGE

ネットワークソリューション

IP Clos

JUNIPER NETWORKS

L2/L3スイッチ

ARISTA

NVIDIA

Extreme networks

ADC

NGINX Part of F5

AI/DLソリューション

GPU

NVIDIA

GPU System

AIRI AI-READY INFRASTRUCTURE

Accelerator

cerebras

ファイルストレージソリューション

Scale Out

Power Scale

DELL Technologies

PURESTORAGE

Scale Up

Unity XT

DELL Technologies

バックアップソリューション

クラウドバックアップ・リカバリ

rubrik

VEEAM

その他取扱い製品

その他の取り扱い製品については以下のWebよりご覧ください。

https://cn.teldevice.co.jp/

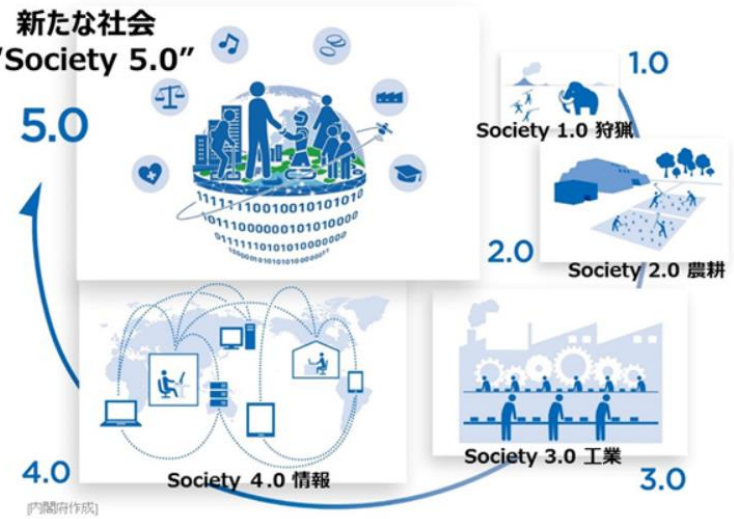
東京エレクトロン デバイス

自己紹介

- 名前：小林　俊一　（こばやし　しゅんいち）
- 出身地：東京
- 職歴：2015年に東京エレクトロンデバイスに中途入社し現在に至る
  - HSM（ハードウェア・セキュリティ・モジュール）と呼ばれるセキュリティ製品のエンジニアとして従事
  - HSM製品に関してプリ・ポストセールス、構築、保守まで一貫した業務経験を積む
  - 最近3か月間育児休暇を取得し、6月から仕事復帰　ようやく勘を取り戻してきた今日この頃

トラストサービスとは？

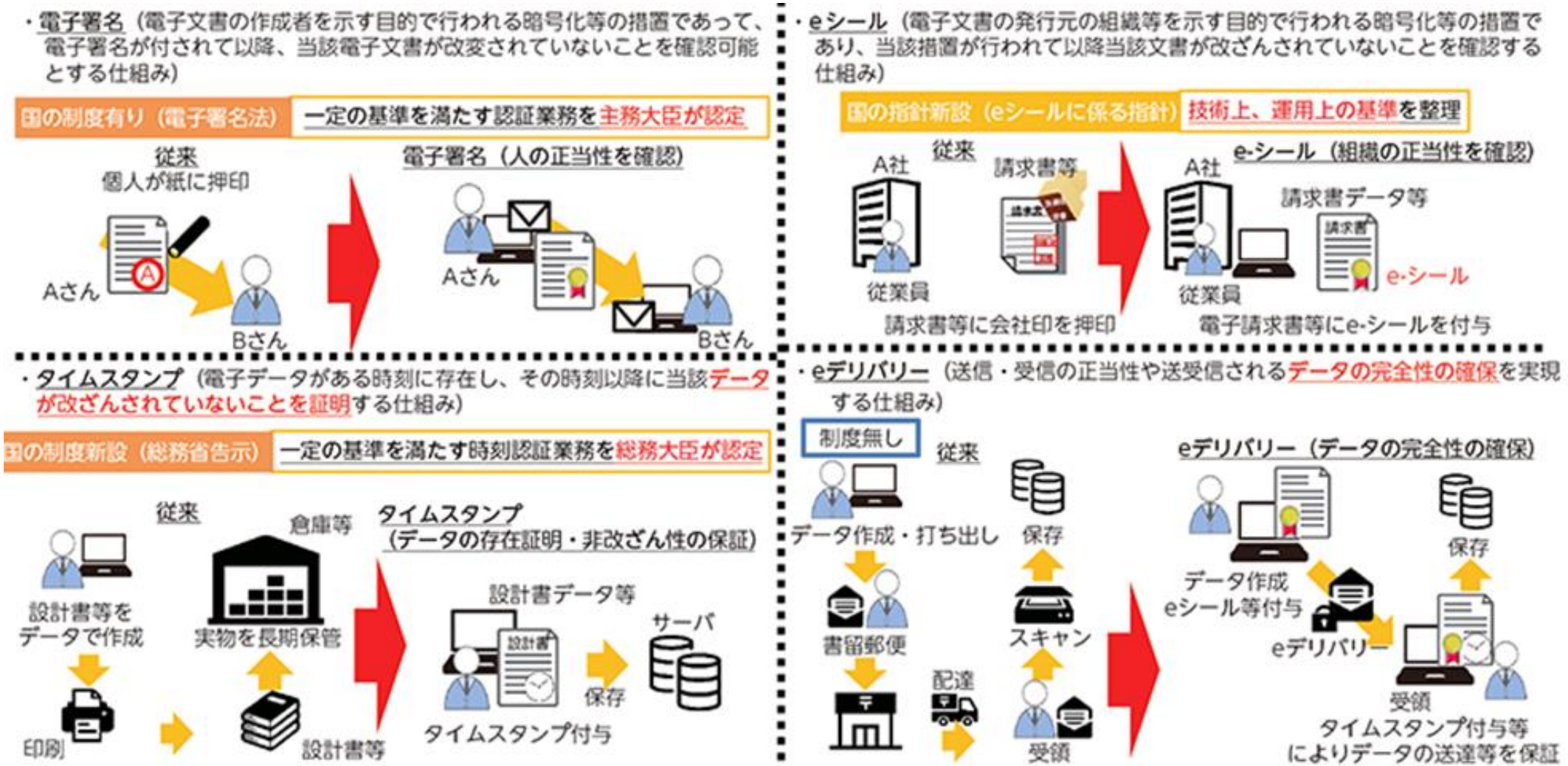
インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み



- トラストサービスの普及が求められる背景
  - デジタル化の進展（オンライン取引の増加、リモートワークの普及）
  - 効率化とコスト削減（業務プロセスの自動化、ペーパーレス化の促進）
  - セキュリティの確保（サイバー攻撃やデータ漏えい等に対するデータ保護の重要性）
  - グローバル化（国際取引増により信頼性のある認証・仕組みが求められている）

☞ 安全で効率的なデジタル社会の創造にはトラストな基盤がもとめられる
☞ トラストサービスは信頼のある自由なデータ流通（DFFT：Data Free Flow with Trust）の基盤の要！

トラストサービスの代表例　～総務省：トラストサービスの取り組み抜粋～



引用：総務省　令和5年 トラストサービスに関する取組
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd255240.html

トラストサービス：諸外国の動向

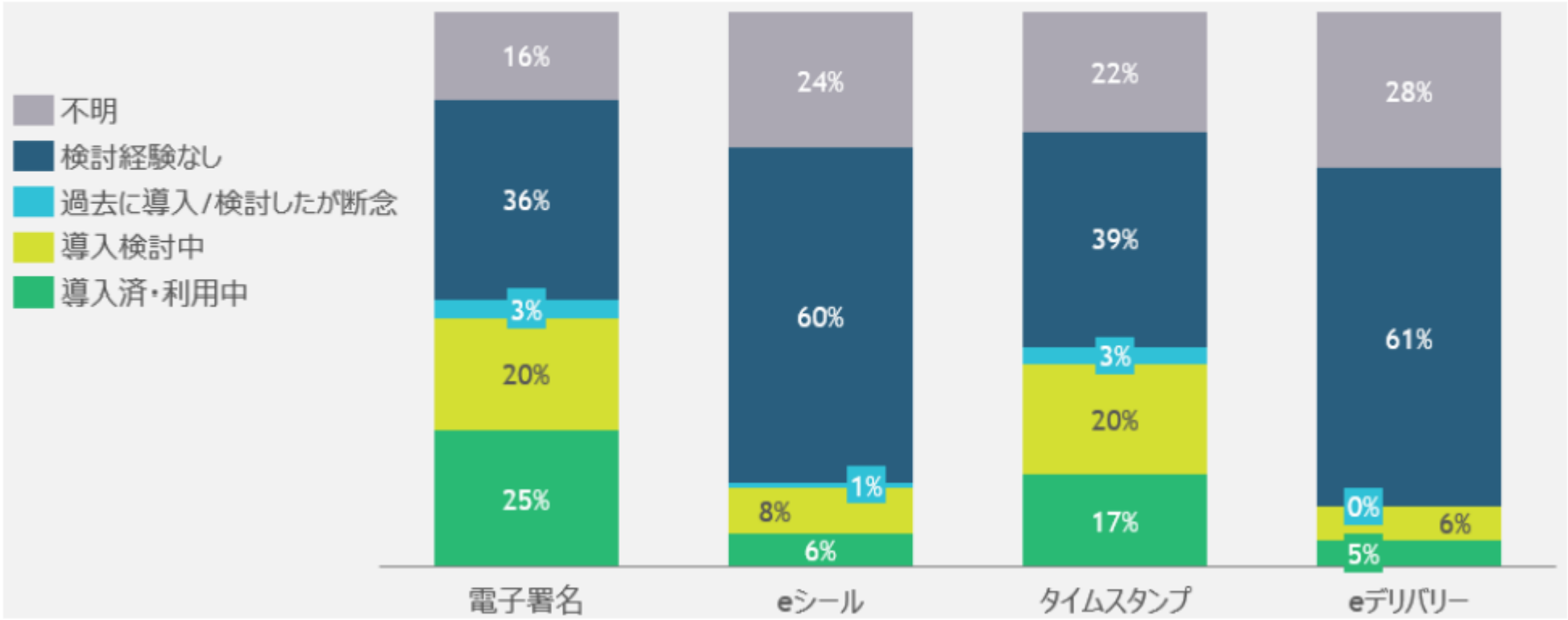
- EU：eIDAS規則　2014年施行
  - 電子署名、タイムスタンプ、eシール、eデリバリー等の包括的な枠組み
  - エストニア：X-road
    - データ交換のプラットフォーム。住民登録、健康保険、金融関連情報の共有等に活用
    - データ送信時にeシール、データ受信時にタイムスタンプを付与することで信頼性を確保（＝eデリバリー）
    - 多様な電子サービス（行政サービス、e-Prescription:電子処方箋サービス）を提供
- 米国：ESIGN法　2000年施行
  - 電子署名に関する法律はあるが、他トラストサービスはeIDASの様に包括的な法律はない
  - 州レベルでの法制度（統一電子取引法（UETA））も存在
  - 日本やEUとは異なり、国のTSPの認定・認証制度は存在しない
    - TSP（トラストサービスプロバイダ）：電子署名やeシールなどトラストサービスに関する証明書発行機関
- 中国：中華人民共和国電子署名法　2005年施行
  - 電子署名に関して法律があるが、米国と同様に包括的な法律はない

☞ 日本はEUのeIDASの様に包括的な枠組みとしての法制度が進められている

【参考】トラストサービスの利用率（2022年）

企業におけるトラスト基盤の現状と課題

一方で、企業ではトラストサービスの利用率は、電子署名 25%、e シール 6%、タイムスタンプ 17%、e デリバリー 5%であり、いずれも限定的な利用率に留まっている。



引用：デジタル庁　日本におけるトラスト基盤の整備に係る調査研究最終報告書概要
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/82a1ea56-128f-4cf6-bbd5-9ef6d4b7bafc/4b9531e7/20231206_policies_budget_entrustment_deliverables_report_04.pdf

民間企業では、トラストサービス自体が全体的に認知されていない現状

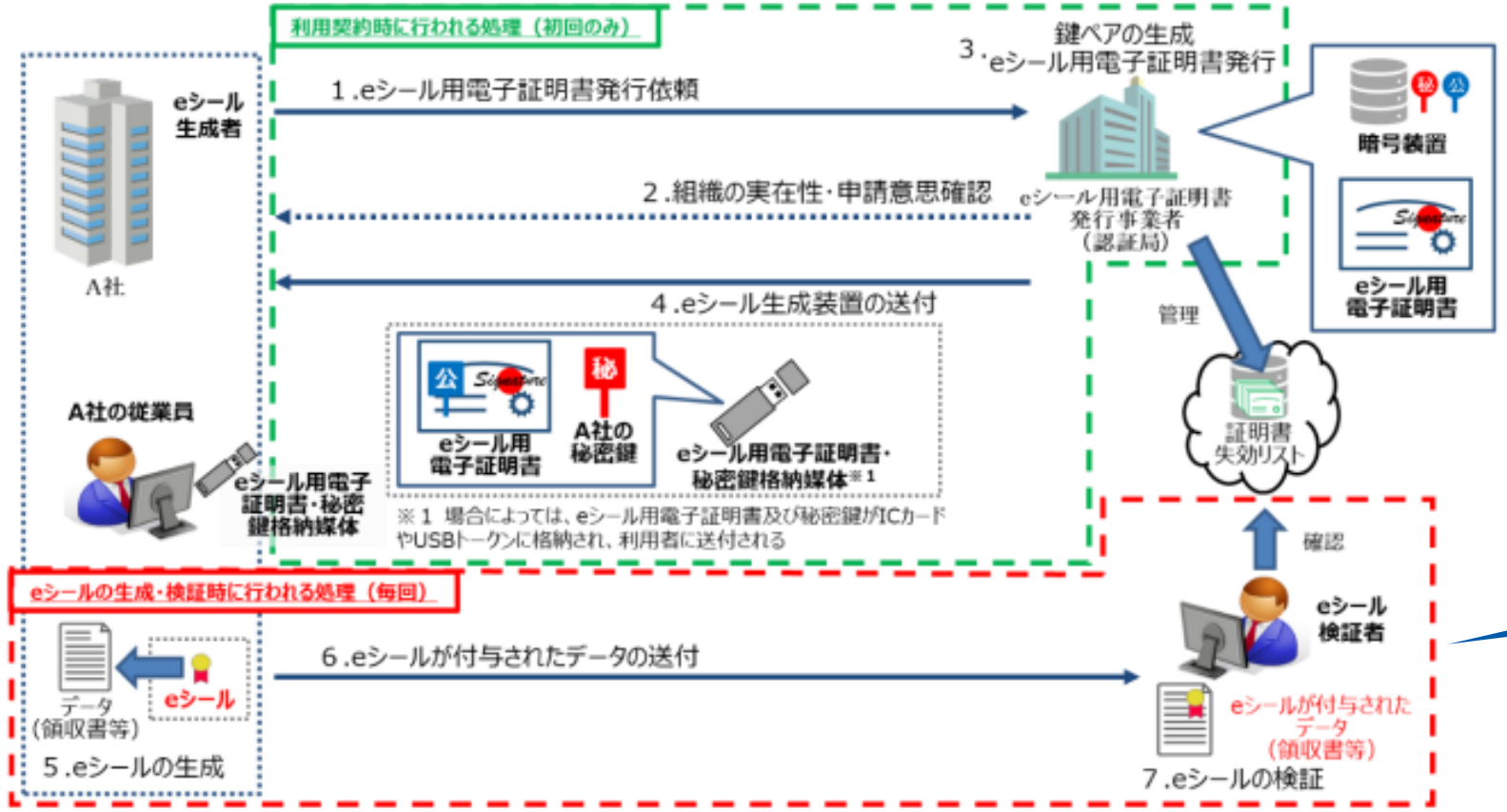
日本のトラストサービス普及が遅れている理由の考察

- 法規制とコストの課題
  - トラストサービスに関連する法整備が海外諸国に比べて遅れている。（電子署名法の改正やeシールの運用に必要な法的な枠組み整備が必要）そのため、民間企業や自治体は導入に踏み切れない
  - 電子署名やeシールの導入には初期投資が必要であり、特に中小企業にとってはコストが負担となる
- 技術的なインフラ整備の課題
  - トラストサービスを提供するための技術的なインフラ（認証局、デジタル証明書発行システムなど）にはハイレベルなセキュリティが求められるが、法規制と同様に十分に整備がされていないでない
- 文化的な要因
  - 伝統的な紙の書類やハンコ文化が根強く残っており、新しい技術への移行に抵抗感がある
  - トラストサービスの重要性や利便性についての認知が不足しているため、利用意欲が低い

早期に法制度を整備し、インフラ構築や啓蒙活動を進めていくべき

トラストサービスの基盤を支えるPKI

- eシールを用いてトラストを確保する仕組みの一例



■請求書等にe-シールを付与することで請求書の発行元を証明
=なりすましの証明書を排除
■紙のコストや紛失リスクも減

引用：総務省　eシールに係わる指針(第二版)　https://www.soumu.go.jp/main_content/000942602.pdf

図5 PKIを用いたeシールの仕組みの例

eシール、電子署名、タイムスタンプいずれのトラストサービスもPKIが信頼の基盤

特に、2023年10月施行のインボイス制度が起因し、eシール認定制度の検討が活発化

PKIに必要不可欠なHSM（Hardware Security Module）

2．4　認証局の秘密鍵の管理に係る基準

認証局の秘密鍵は、認証局が発行する電子証明書及び証明書失効リストに署名する際に使用され、e シールを生成する際に使用する秘密鍵とは用途が異なるものである[14]。このため、例えば悪意のある第三者に盗まれて悪用された場合、当該認証局の発行する e シール用電子証明書の信頼性が著しく損なわれてしまい、当該認証局から e シール用電子証明書の発行を受けた全ての組織等に影響が及ぶため、認証局の秘密鍵はHSM[15]等で厳格に管理されることが必要となる。また、当該 HSM が配置される部屋のセキュリティ対策や不正アクセスに対する対策等も当然必要となる。

認証局の HSM 自体の基準及び管理に係る基準について、認定 e シール用認証業務における e シール用電子証明書に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[16]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を準用することとする。ただし、HSM 自体の技術基準は、別に定める基準のとおり、現行化することを前提とする。

引用：総務省　eシールに係わる指針(第二版)　https://www.soumu.go.jp/main_content/000942602.pdf

（タイムスタンプの生成に関わる暗号技術）

第９条　タイムスタンプの付与対象となる電子データのハッシュ値（以下「ハッシュ値」とする。）を得るためのハッシュ関数及び告示第３条第１項第１号のデジタル署名に用いる署名アルゴリズムは CRYPTREC 暗号リスト（注）のうち、「電子政府推奨暗号リスト」に記載された暗号技術を用いることとする。

（注）CRYPTREC 暗号リストについては、最終更新版を参照することとする。

（秘密鍵の保護装置）

第 10 条　秘密鍵は、ハードウェア・セキュリティ・モジュール（FIPS 140-2 のレベル３以上又は ISO/IEC 15408 EAL4＋以上（EN 419 221-5 に対応するもの）の認証を受けた製品とし、以下「HSM」という。）を用いて保護することとする。

引用：総務省　時刻認証業務の認定に関する実施要項　https://www.soumu.go.jp/main_content/000743330.pdf

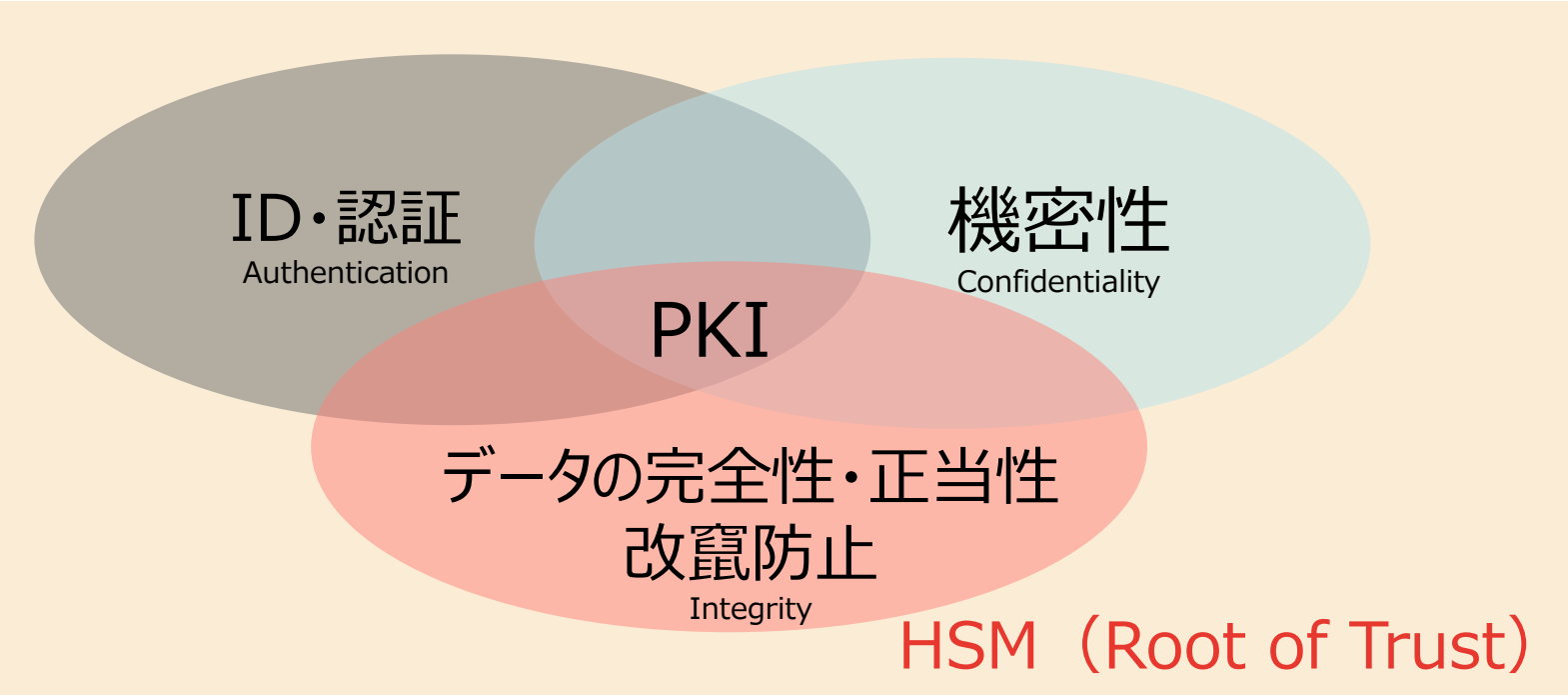
👉 認証局で使われる秘密鍵はHSMで保護することが求められている

HSMの特徴

- 安全な暗号鍵の保護
  - HSM（ハードウェアセキュリティモジュール）は暗号鍵の生成/管理/利用を安全に行う専用のハードウェア装置
  - 耐タンパーの性質を持つ（不正アクセスや改ざんから保護する機能）
- 高速な暗号演算
  - 高速演算チップ（RSA,ECC）を搭載
  - ハードウェア乱数生成器を搭載
- セキュリティ規格への準拠
  - FIPS140-2、FIPS140-3のレベル2 or 3
  - Common Criteria規格　EAL4+ AVA_VAN.5/ALC_FLR.2
- 様々なAPIに対応
  - PKCS#11、JCE、MSCAPI、CNG等

まとめ

- 社会全体のデジタル化にはトラストな基盤の構築が必要
- トラストサービスにおいてPKI（公開鍵暗号）記述は必須
- PKIを支える徹底した「鍵管理」が重要　→　HSMは不可欠
- HSMはRoot of Trustのコア



ご清聴ありがとうございました

デジタル認証の新標準：eシールの可能性と展望

東京エレクトロン デバイス株式会社

CN BU　CN技術本部
プロダクト第三技術部 第四グループ
内野　優輝

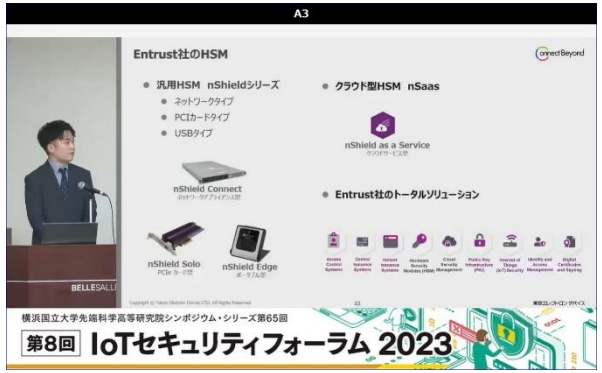
自己紹介

氏名	内野　優輝（うちの　ゆうき）
所属	CN技術本部　プロダクト第三技術部 第4グループ　　（2021年入社）
担当	HSM製品のポスト・プリセールスエンジニア

- サポート業務（ヘルプデスク、自前保守）
- お客様先での構築作業
- 製品拡販に向けたプリセールス活動

  →主に金融、製造、トラストサービス業界のお客様に啓蒙活動

HSM：暗号鍵を守る金庫



フォーラムへの登壇

ベンダーのブートキャンプ in プーケット

eシール概要

- eシールとは

  総務省 eシールに係る指針 （第２版）より、eシールは、企業等が発行する
  電子データの発行元を証明し、また、**電子データに改ざんがないことを証明**できるようにするために用いられる。

- 日本での検討状況　~総務省 eシールに係る検討会~

  電子署名はデジタル庁、タイムスタンプ・eシールに関しては総務省が取りまとめ。

  - 認定eシール用認証業務による保証有無で2つの保証レベルを規定

    レベル1：総務大臣の認定なし　　レベル2：総務大臣の認定あり

  - eシールの生成方式
    - ローカルeシール方式：USBトークンなどで、eシール生成者が署名用秘密鍵を管理
    - リモートeシール方式：eシール生成者はあくまでサービス利用のみ。eシールサービス事業者が鍵管理

参考: https://www.soumu.go.jp/main_content/000942602.pdf

考察①
EU事例にみる、国際間取引でのeシール

EU事例①：VAT免税証明書電子化

- 2024年7月8日、EUにてVAT（Value Added Tax, 付加価値税）免税証明書の電子化に関するDIRECTIVEが公表（以下、和訳抜粋）

加盟国がデジタル時代の高まる需要に対応し、企業の管理負担を軽減できるようにするため、
現在の紙のバージョンを新しい電子証明書に置き換える必要があります。
~省略~
電子署名された文書の電子処理を可能にするために必要な、技術的手段を導入することを要求する**EU 法令**によって課せられた義務を遵守できるようになります。

- EU法令 ＝ 電子識別規則 (EU) No 910/2014 ＝ **eIDAS規則**

(58) 法人からの適格eシールを要するやりとりの場合、法人の権限のある代表者からの適格電子署名が均等に承認されなければならない。
(59) eシールは、電子文書が法人から発行されたことの証拠として、その文書の原本性及び完全性の確実性の確保を提供するものでなければならない。
(60) eシールの適格証明書を発行する信頼サービスプロバイダは、司法手続または行政手続の過程において国内レベルでそのような同一性識別が必要となる場合、電子シールの適格証明書が提供される法人を代表する自然人の同一性を確認できるようにするために必要となる措置を実装しなければならない。

参考: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024PC0278&qid=1721033139136

EU事例②：EUDIウォレットとeシールの相互作用

- EUDIウォレットとは
  - EUDI（European Union Digital Identity）
    →EUDIを利用したモバイルアプリ＝EUDIウォレット。EWCと呼ばれるコンソーシアムで情報提供
  - 市民が安全にデジタルIDを管理し、オンラインでの認証や署名に利用可能
  - 主な機能：デジタルID管理、デジタル署名、認証、個人データの保護

- eシールとの相互作用
  - 安全な認証プロセス：EUDIウォレットを使ったeシールの発行と確認
    ユーザーはEUDIウォレットを通じて自身のデジタルIDを確認し、eシールを取得
  - 信頼性の向上：EUDIウォレットとeシールの連携により、オンライン取引の信頼性が向上
    デジタル署名の正当性と改ざん防止の確立
  - 国際取引の促進：EU内および他国との安全な電子取引の推進
    EUDIウォレットとeシールの共通基盤により、国際的な電子商取引の円滑化

参考: https://eudiwalletconsortium.org/

国際間取引でのeシール展望

- 総務省 eシールに係る検討会では、**国際間取引でのeシール活用は検討段階**

> 上記の議論に加え、欧米等における状況も参考にしながら、我が国における包括的なトラスト基盤の構築の要否や認定に係る公表方法等を含めて、戦略的に制度設計等を検討していく必要があることが指摘された。国際間のデータ流通におけるトラストサービスの活用は、上記の国際データ連携基盤以外も含め我が国が提唱する DFFT 等とも整合的であり、デジタル庁及び総務省においては、国際的な基準・規格等も踏まえながら戦略的に検討を進める必要がある。

- 前述の事例にもあるように、諸外国では国際間データ流通を想定したeシール導入が本格化

以下2パターンいずれか、もしくは両方により、**日本でもeシール導入の加速化**

①国際間相互認証と信頼の促進のため、eIDAS規制によるeシール利用がスタンダード化
②eシールの受容性向上、利便性周知により、各社での利用拡大
⇒以降のスライドで技術観点でのeシールについて解説します。

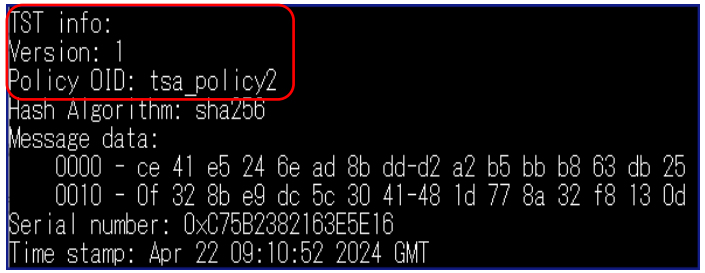
参考: https://www.soumu.go.jp/main_content/000932048.pdf

考察②
日本市場でのeシールビジネス展開に向けた技術観点での考察

eシールビジネス化に向けて技術観点での考察　システム実装は容易？

- eシール実装は現時点で**PKIを前提**としており、既に認定制度が策定されている
  電子署名・タイムスタンプと同様であり、システム実装は容易と想定される
  - 共通証明書ポリシーOID

    国際相互運用性を考慮したOID体系を認定制度で策定されると想定。OID設定における技術的ハードルは低い



TSA証明書のポリシーOID例

（4）共通証明書ポリシーOID 体系の整備

本検討会での議論においては、認証局における運営コスト削減等の観点から、共通証明書ポリシーOID を用いて 1 つの認証局の秘密鍵から「電子署名用」の電子証明書と「e シール用」の電子証明書を発行することを許容する方向で検討すべき等の議論がなされた。

  - eシールを大量に生成する際の処理

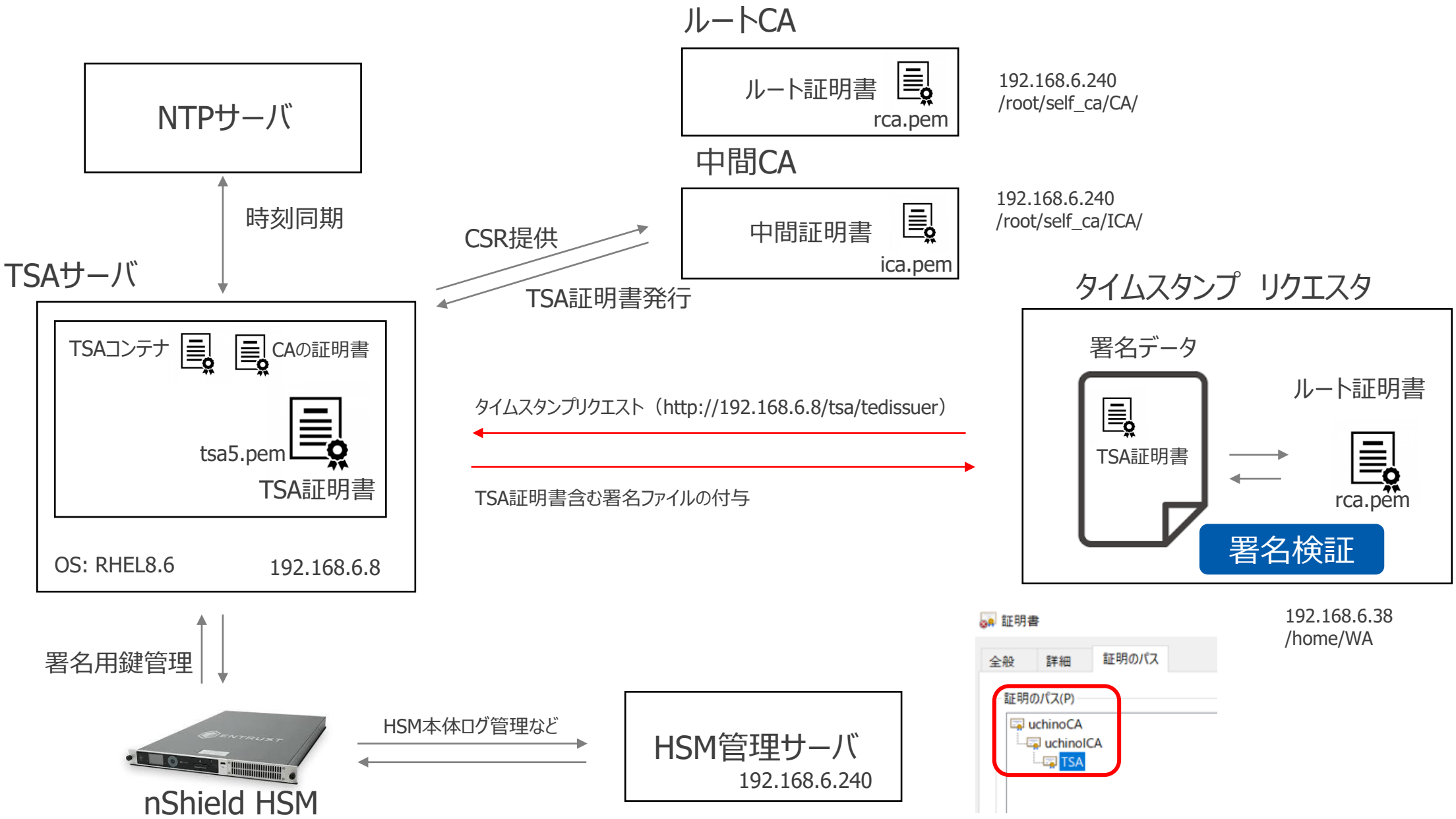
    PKIにおける署名処理ではRSA, ECDSAなどの
    公開鍵を利用。HSM等のアクセラレータに
    性能依存するが、高速処理が可能。

（2）方向性

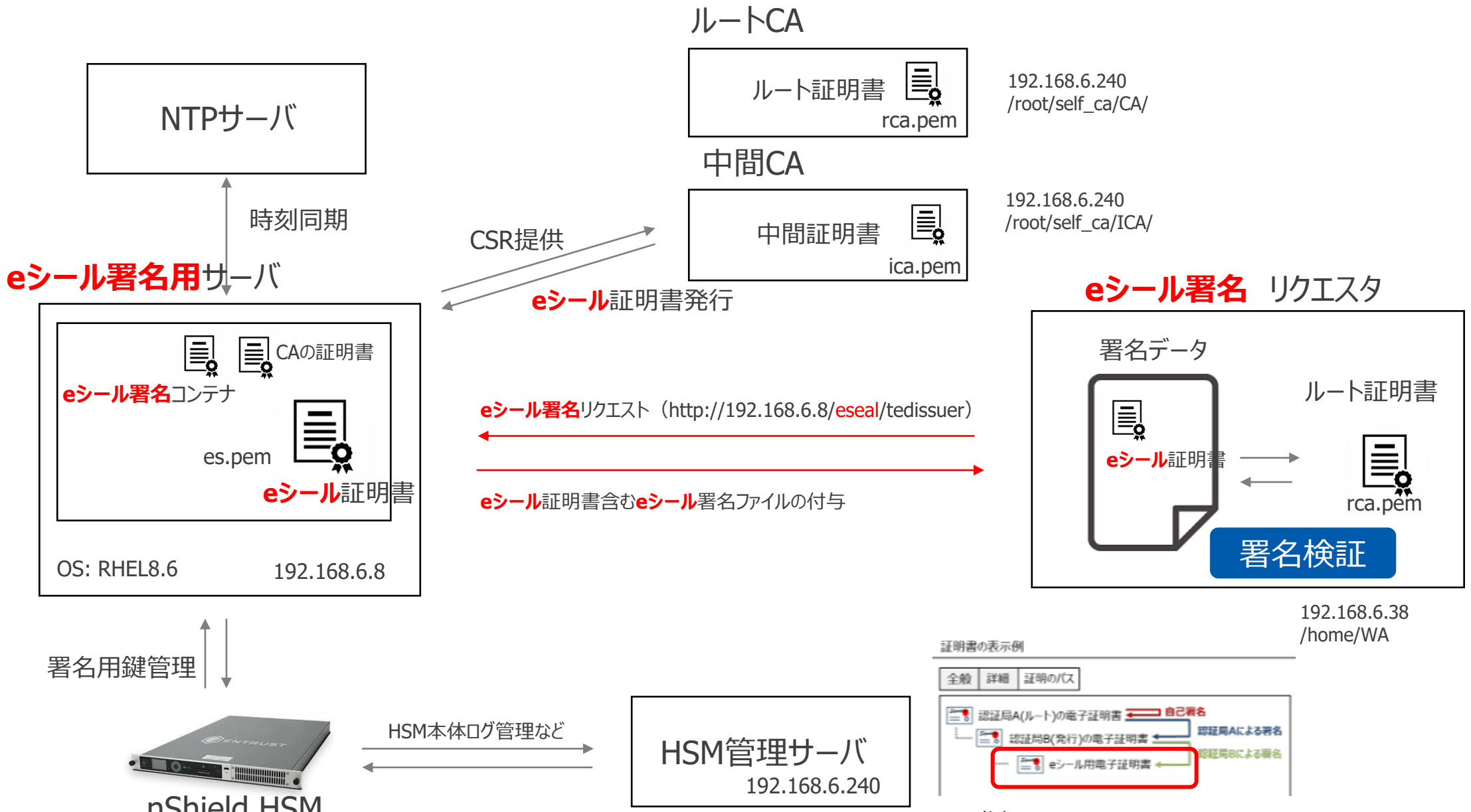
機械的・自動的に複数の対象電子文書等に対して一括で e シールを付与するニーズが想定されるため、「e シールに係る指針」で示している方向性に基づき、総務大臣認定に係るeシールについても、複数の対象データに一括でeシールを付すことを認めることとする。

参考: https://www.soumu.go.jp/main_content/000932048.pdf

弊社タイムスタンプ認証局（TSA）検証環境



弊社タイムスタンプ認証局（TSA）検証環境　eシール置き換えの際の相違点



参考: https://www.soumu.go.jp/main_content/000932048.pdf

東京エレクトロン デバイス

考察③
eシールに求められるセキュリティ要素

PKIにおけるセキュリティ　eシール認証局の秘密鍵保護

弊社取り扱い　Entrust社　nShield HSM

- 認証局での秘密鍵管理

  タイムスタンプ等と同様、以下いずれか認定のHSMが必須

  - FIPS 140-2 Level3
  - CC (ISO/IEC 15408)　EAL4+

- 技術進展による運用変更

  - FIPS 140-3 Level3　への移行
  - SHA1等アルゴリズムの危殆化
  - 量子暗号技術の進歩

    ➡耐量子暗号アルゴリズムの採用

    （ポスト量子暗号対応SDKでの開発）

その上で、HSM の技術基準として満たすべき FIPS の規格を始め、技術・設備・運用基準については、技術の進展等に応じて変化していくため、国際動向等も踏まえて機動的に見直しができるよう、「e シールに係る指針」とは別に定め、「e シールに係る指針」はそれを参照する形で規定することが適当である。

参考: https://www.soumu.go.jp/main_content/000932048.pdf

リモートeシール方式における利用認証・鍵認可

すなわち、リモート e シール方式で認定 e シール用認証業務を行う場合は、少なくとも利用認証と鍵認可を別に行うことが求められる。なお、意思表示を伴う電子署名は推定規定[20]が法定されていることもあり、リモート署名に関する「リモート署名ガイドライン」において、利用認証と別に鍵認可を行うことに加え、鍵認可は複数要素認証を要求しているが、リモート e シール方式の鍵認可においては、e シールが意思表示を伴わない発行元証明にとどまることに鑑み、単要素認証でも可とする。

- リモートeシール方式においては、サービス提供事業者が鍵を管理

  ➡利用者側の鍵認可に関しては

  単要素認証OKのため制限は低い。

Entrust社 鍵/シークレット管理ソリューション KeyControl

- 一方で、認可で使用するPINコード等の認証要素は、サービス提供事業者で適切な管理が必要と規定

  ➡シークレット管理ソリューションなどを用いて管理し、

  不正なeシール生成を防ぐことが重要！

参考: https://www.soumu.go.jp/main_content/000932049.pdf

まとめ

- お伝えしたかった3ポイント

eIDASで規定されたeシールは既に海外でも
受容性が高まっている

日本においても、**法規制や利便性周知**により
急激に**eシール導入が加速化されると予想！**

トラストサービス事業者によるサービス実装において
PKIを前提としたeシールの技術障壁は低い

eシールシステムのセキュリティにおいて2点が重要
①認証局の**秘密鍵保護はHSM必須**
②eシールサービス事業者の**認証要素管理**

東京エレクトロン デバイス

onnect Beyond