

# シンポジウム「情報通信アーキテクチャの今とこれから ～標準化活動の観点から～」

## 電子署名関連に関する標準化活動（ETSIの活動等）

セコム株式会社 IS研究所  
主任研究員  
佐藤 雅史

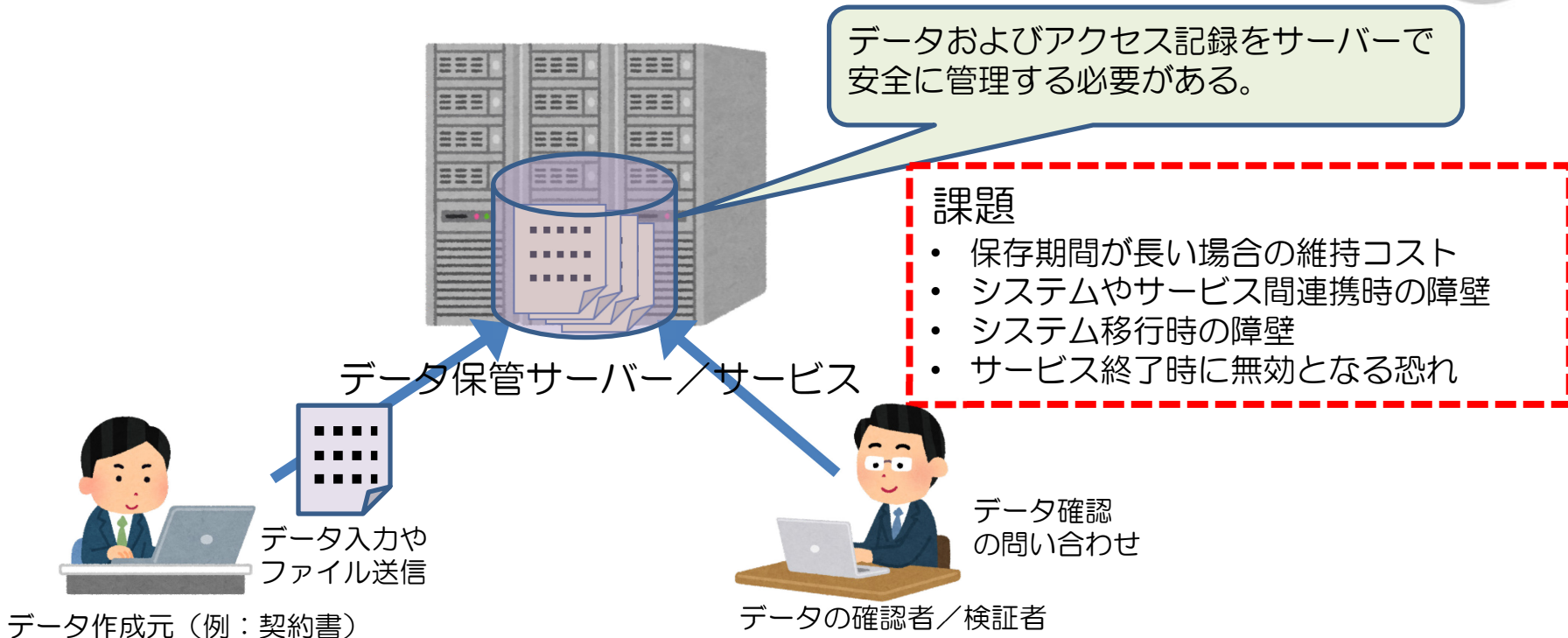
# 自己紹介



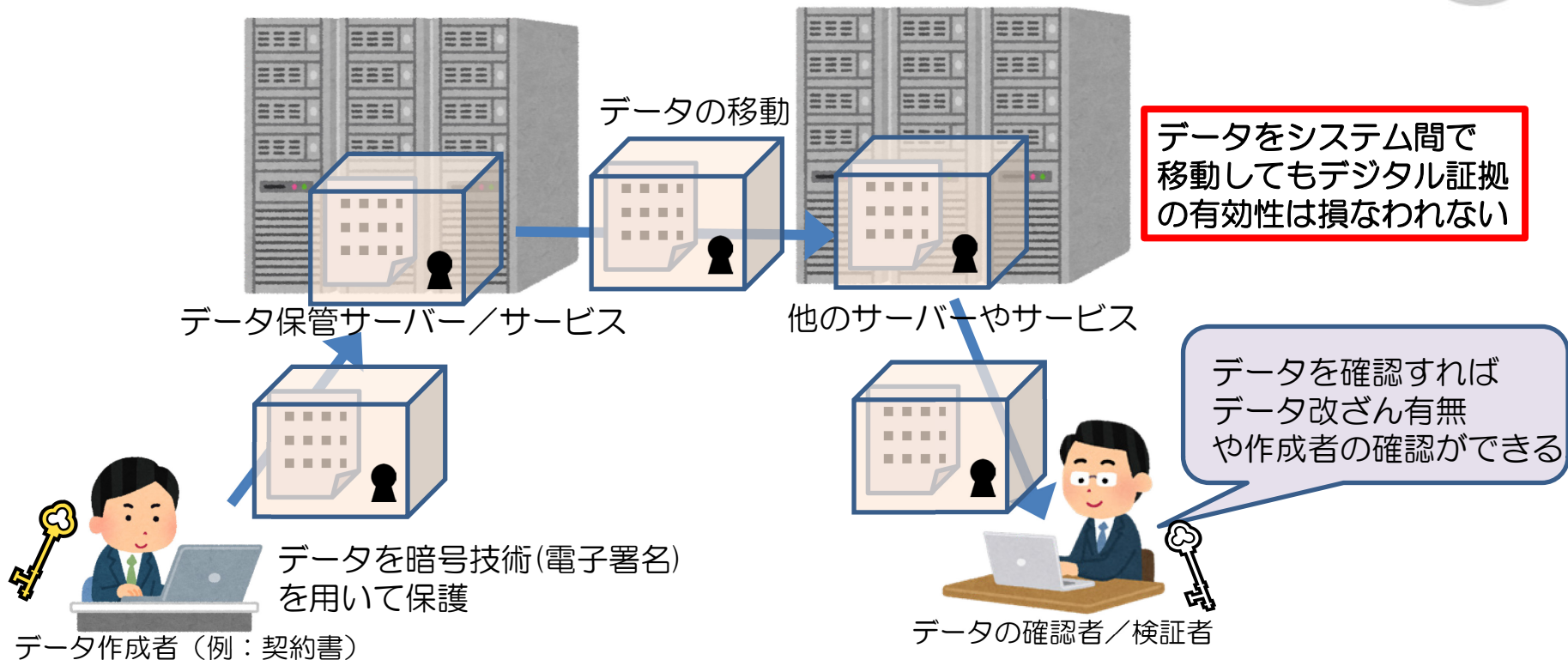
## 佐藤 雅史

- 情報セキュリティ、暗号を応用した電子認証や電子署名、ブロックチェーンなどが専門
- 日本ネットワークセキュリティ協会、日本トラストサービスフォーラムなど、様々な業界団体で活動
- ISO/TC 154 (Processes, data elements and documents in commerce, industry and administration) WG6
- ISO/TC 307 (Blockchain and distributed ledger technologies), 国内審議委員会, WG2/JWG4国内主査

# デジタル証拠(デジタルデータによる証明) における課題



# デジタル証拠とデータポータビリティ



# 電子署名に関する標準化の考え方

使える標準規格をめざす！  
相互運用性の確保が重要課題！

- JNSA Challenge PKI Project (2001-2004頃)
- ECOM 電子署名プラグテスト (2005)
- 日欧 電子署名プラグテスト (2007)
- ETSI 電子署名プラグテスト (2008年～)

# ETSI ESIについて

- ETSI (European Telecommunications Standards Institute)

欧州の電気通信に関する様々な技術仕様を定める標準化団体

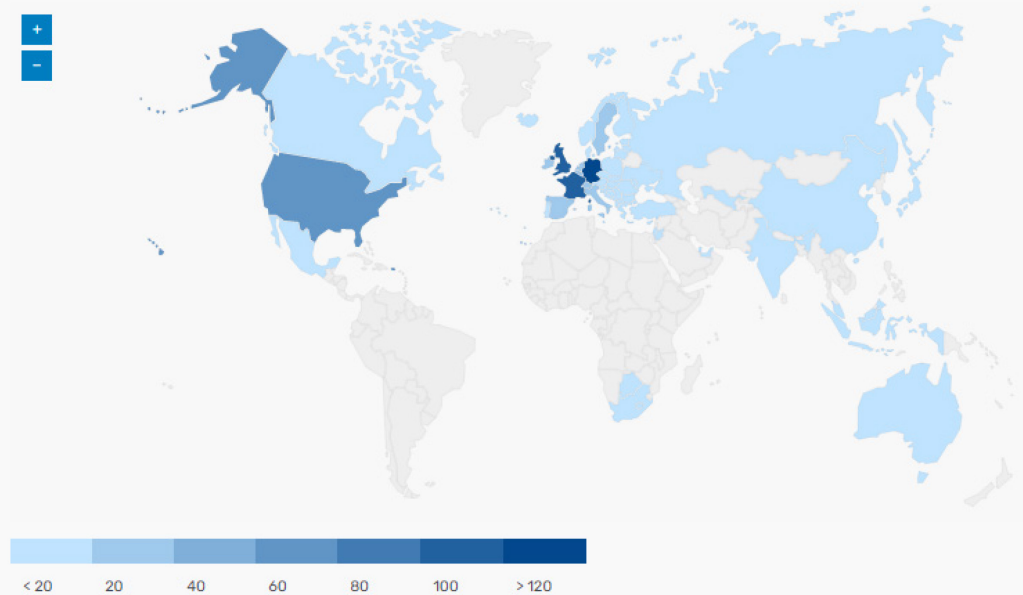
- ESI (Electronic Signatures and Infrastructures)

ETSI内に設置された技術委員会(Technical Committee)の一つ。認証局や電子署名を中心とした技術や運用に関する仕様を策定する。

JNSA(日本ネットワークセキュリティ協会)はETSIのassociate memberとして参加

## ETSI members around the world

ETSI counts more than 900 member organizations worldwide, drawn from 65 countries and five continents. Members comprise a diversified pool of large and small private companies, research entities, academia, government and public organizations. Browse the map to find our members.



<https://www.etsi.org/membership>

# 欧州における規格と制度の関係

- EU 電子署名指令 (1999-2016)
  - EUが示す指針に従いEU加盟国が電子署名法を制定
  - ETSIやCENが定める技術仕様(TS: Technical Specification)や技術レポート(TR: Technical Report)が存在
- EU eIDAS 規則 (2016~)
  - EUが定める規則が各国の電子署名法を上書き。
  - 電子署名以外のeID(認証)などの対象の拡大。
  - より強制力のある標準化へシフト。ETSIとCENの仕様をベースに、EN (欧州規格: European Norm)の制定。

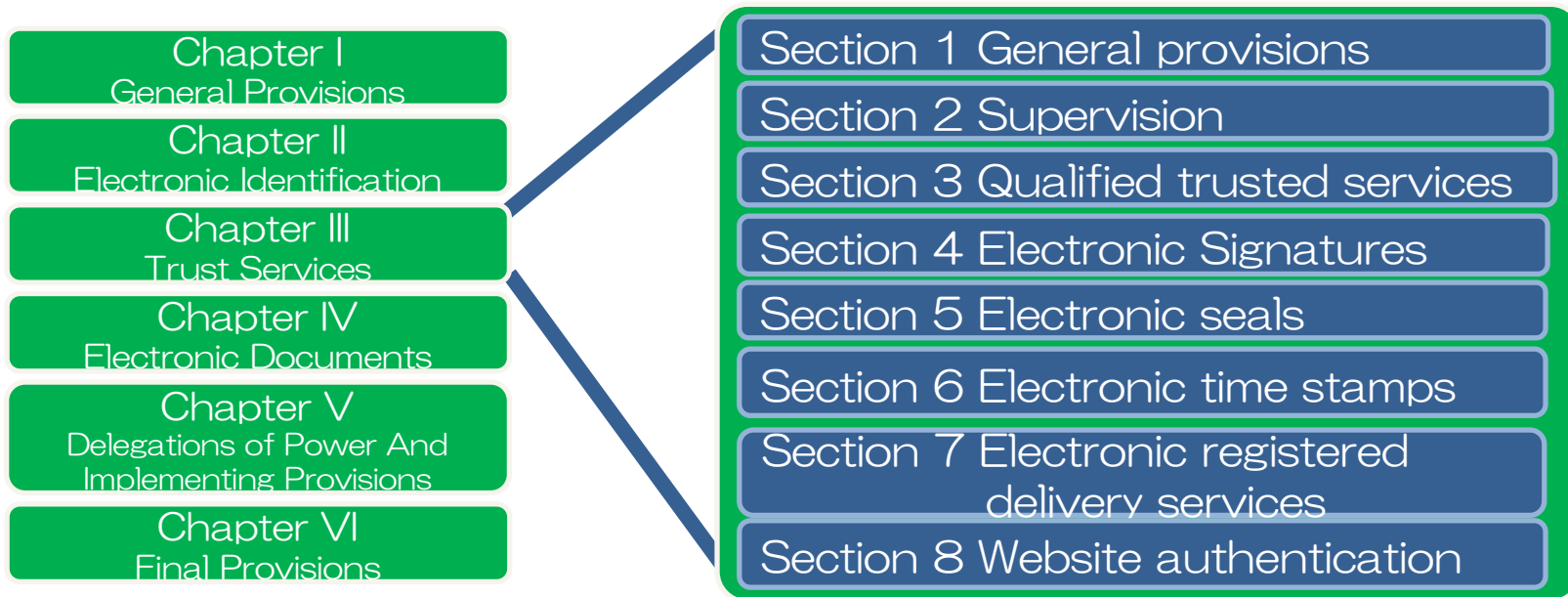


# eIDASとは？

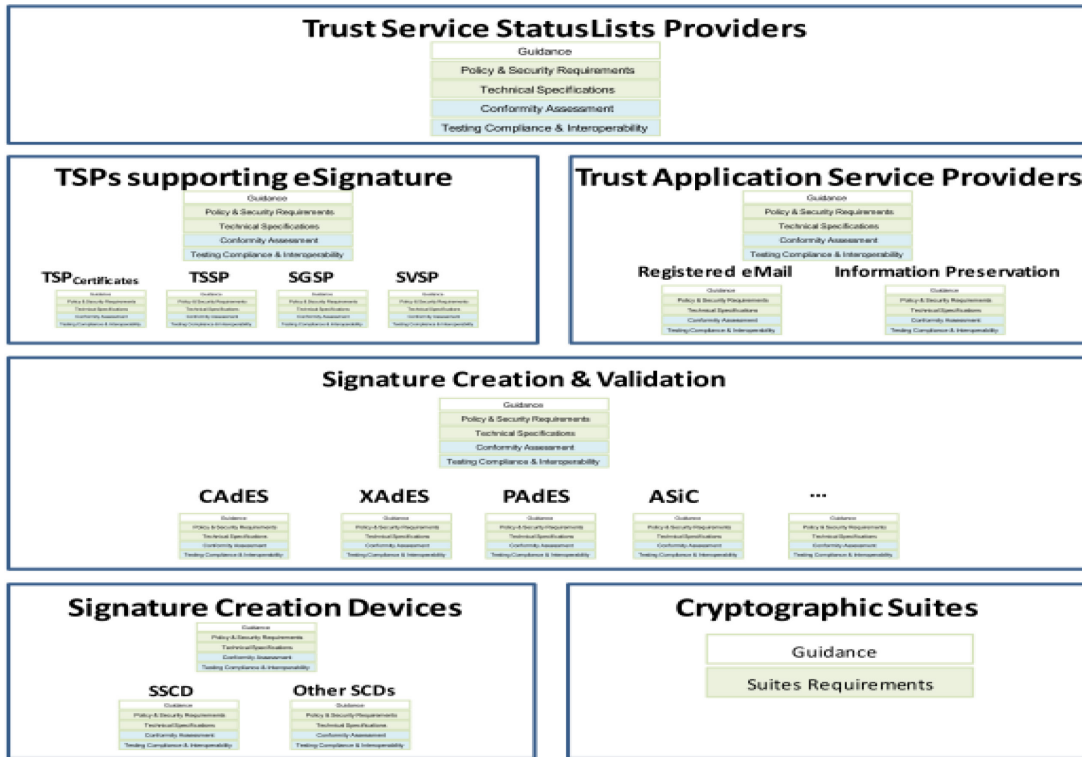
- eIDAS: Electronic identification and trust services
- EUで定めた電子認証や電子署名を含めたトラストサービスに関する規則。
- 電子認証やトラストサービスを普及させることで、国境を越えた電子取引を安全かつシームレスに実現させる（デジタル単一市場の形成）ことが目的。

# EU-Regulation eIDASの構成

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

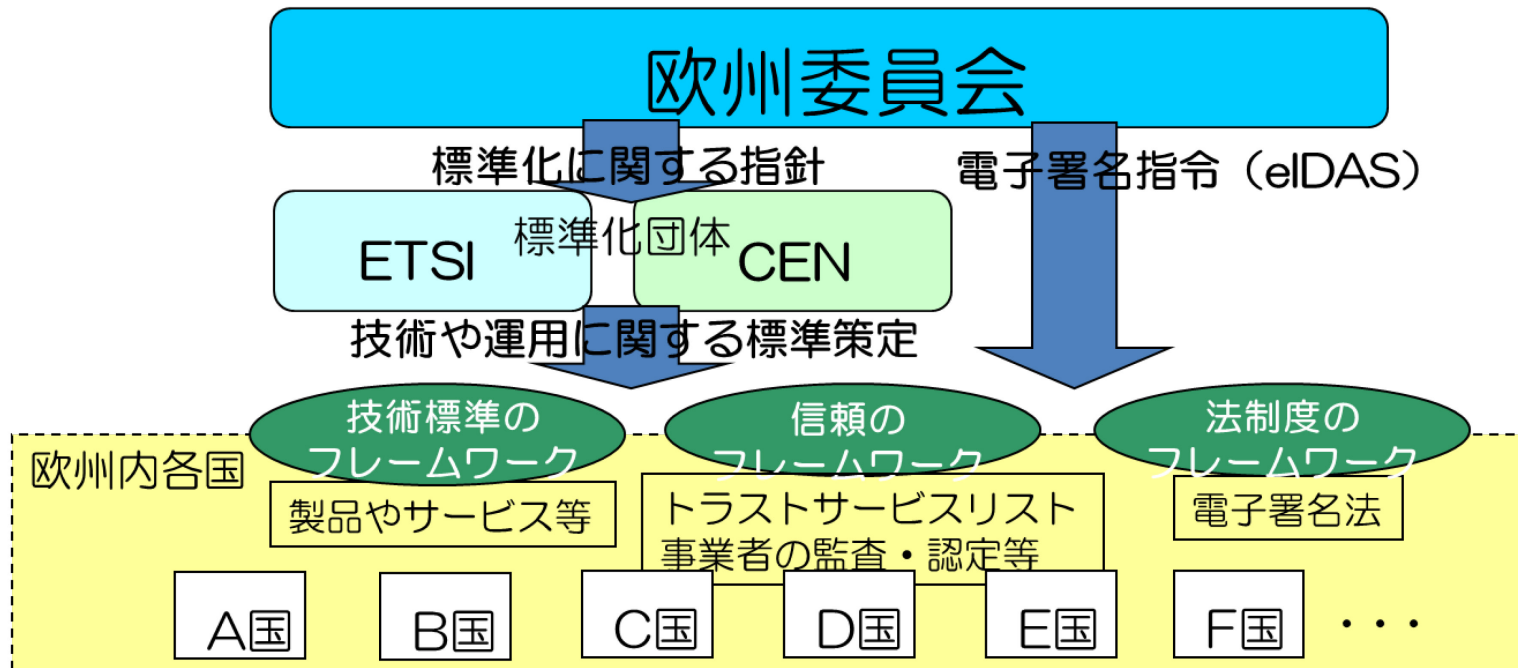


# 欧州電子署名標準フレームワーク



ETSI SR 001 604より

# 欧州(EU)の電子署名の体系



欧州委員会のトップダウンによる体系化されたアプローチ。  
制度と技術が結びついた整合性のあるフレームワークを目指している。

# CEF (Connecting Europe Facility)

- 欧州における重要インフラへの投資を促進
- デジタルサービスインフラは重点項目の一つ
- 電子署名の生成や検証を行うオープンソースソフトウェアライブラリや、データの標準準拠性を確認するテストツールが提供されている

# 欧州の今後の動向

- eIDAS規則の見直し
- サイバーセキュリティAct.

# 電子署名関連ISO規格

- ISO/TC 154
  - ISO 14533-1 Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
  - ISO 14533-2 Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
  - ISO 14533-3 Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)
- ISO/TC 215
  - ISO 17090-4 Health informatics — Public key infrastructure — Part 4: Digital Signatures for healthcare documents

# 電子署名に関する、日本の標準化 活動の課題

- 日本からの発信の必要性
  - 規格改定や新規規格策定において、日本で実運用中の実装やユースケースの観点での意見を積極的にできるとよい
- 継続的な活動の必要性
  - 規格のメンテナンス
  - 標準化動向の継続的なウォッチ（複数の標準化団体の横断的な視点も必要）
  - 標準化団体やメンバーとの継続的な関係の維持
- 技術的/標準化的視点での専門家の育成
- 標準化への貢献に対する評価の難しさ



ご清聴ありがとうございました