NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA電子署名WG春祭り
「電子署名の世界(SIGN WORLD)」

電子署名法視点で技術の棚卸をしてみよう

2018年5月23日

JNSA電子署名WGサブリーダー
セコム株式会社　IS研究所
佐藤　雅史

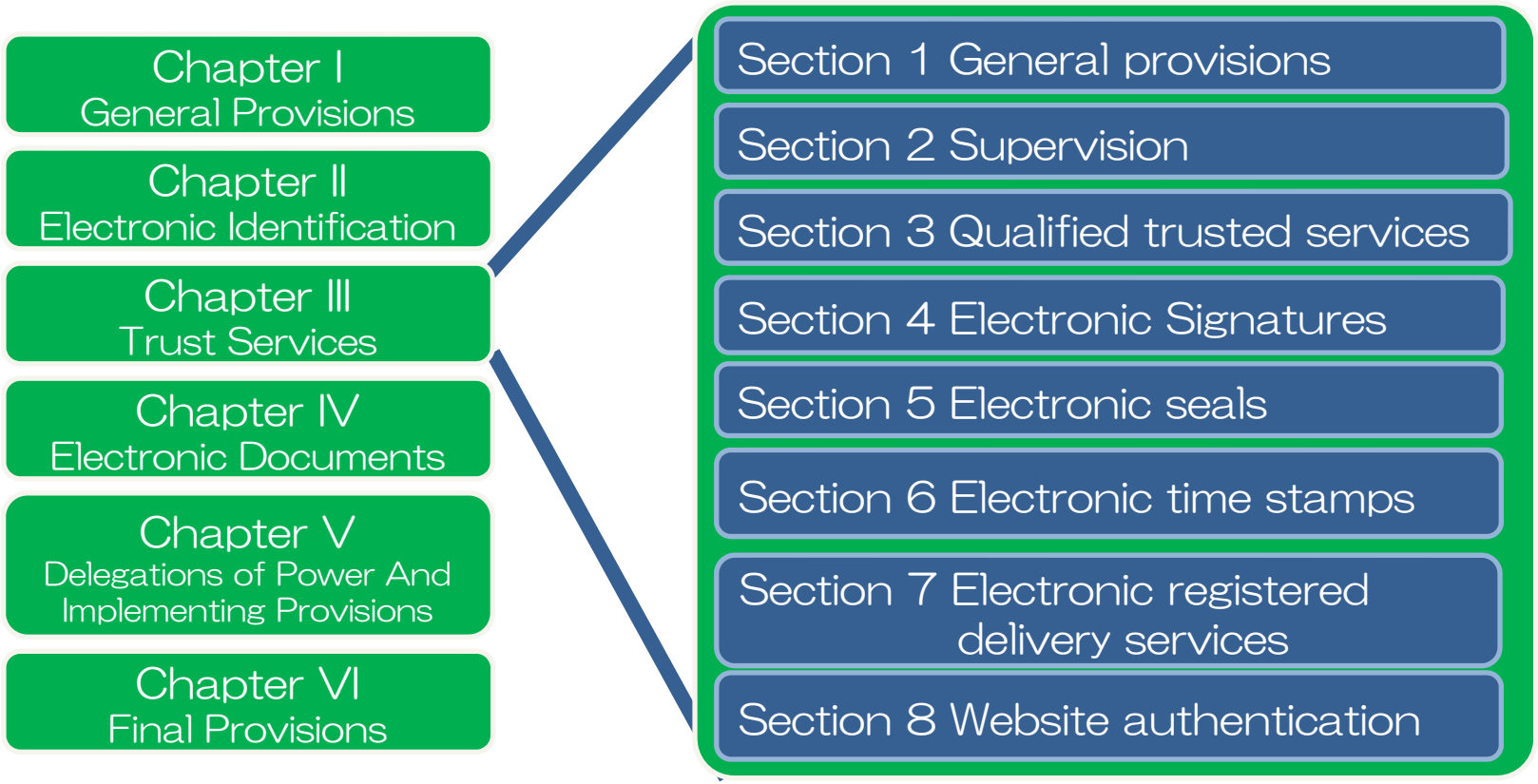
日本の話の前にEUの話を…

JNSA

- 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

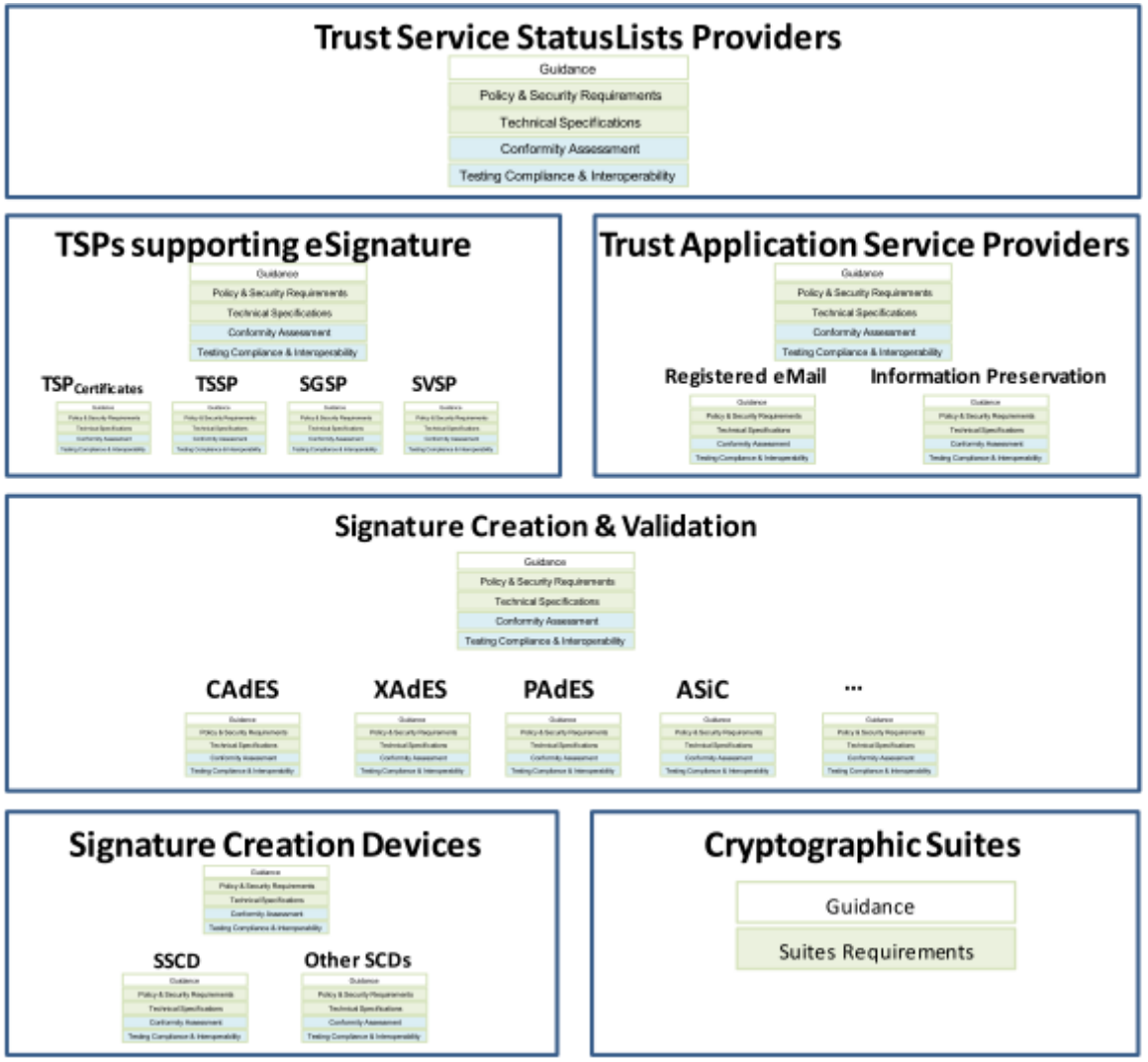


EC指令460(mandate460:2009/12

M/460 STANDARDISATION MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO ELECTRONIC SIGNATURES

- 欧州の電子署名規格の軽量化と再編成
  - 期限切れの規格の更新や廃棄
  - 規格の統合、再構成
  - 理解と利用を促進するための規格の簡素化
- ETSI技術仕様(TS)の生成から欧州規格(EN)やISOへの進化が定義されたライフサイクル
- 4年スパンの行動計画
- TS普及とプレゼンテーションインフラ維持のための恒久的な予算措置

欧州電子署名標準フレームワーク



ETSI SR 001 604より

eIDAS Regulationに関するImplemented Acts (署名関連を抜粋。赤字は佐藤が変更)

- COMMISSION IMPLEMENTING REGULATION (EU) 2015/806
  - 22 May 2015
  - laying down specifications relating to the form of the EU trust mark for qualified trust services
- COMMISSION IMPLEMENTING DECISION (EU) 2015/1505
  - 8 September 2015
  - laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- COMMISSION IMPLEMENTING DECISION (EU) 2015/1506
  - 8 September 2015
  - laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- COMMISSION IMPLEMENTING DECISION (EU) 2016/650
  - 25 April 2016
  - laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

eIDAS Regulationに関するImplemented Acts (署名関連を抜粋。赤字は佐藤が変更)

JNSA

- COMMISSION IMPLEMENTING REGULATION (EU) 2015/806
  - 22 May 2015
  - laying down specifications relating to the form of the EU trust mark for qualified trust services
- COMMISSION IMPLEMENTING DECISION (EU) 2015/1505
  - 8 September 2015
  - laying
    pursua
    Council on electronic identification and trust services for electronic transactions in the internal market

トラステッドリストに関する要件

trusted lists

Parliament and of the

法律×標準技術

COMMISSION IMPLEMENTING DECISION (EU) 2015/1506

- 8 Sept
- laying
  signa
  Article
  Counc
  market

電子署名フォーマットの要件。
CAdES, XAdES, PAdES, ASiCへのリファー（旧TS版ですが）。

the

COMMISSION IMPLEMENTING DECISION (EU) 2016/650

- 25 Apr
- laying
  seal
  of the
  electro

署名生成デバイスに関する要件。
ISO/IEC 15408シリーズや、EN 419 211シリーズ（署名生成デバイスのPP）へのリファー。

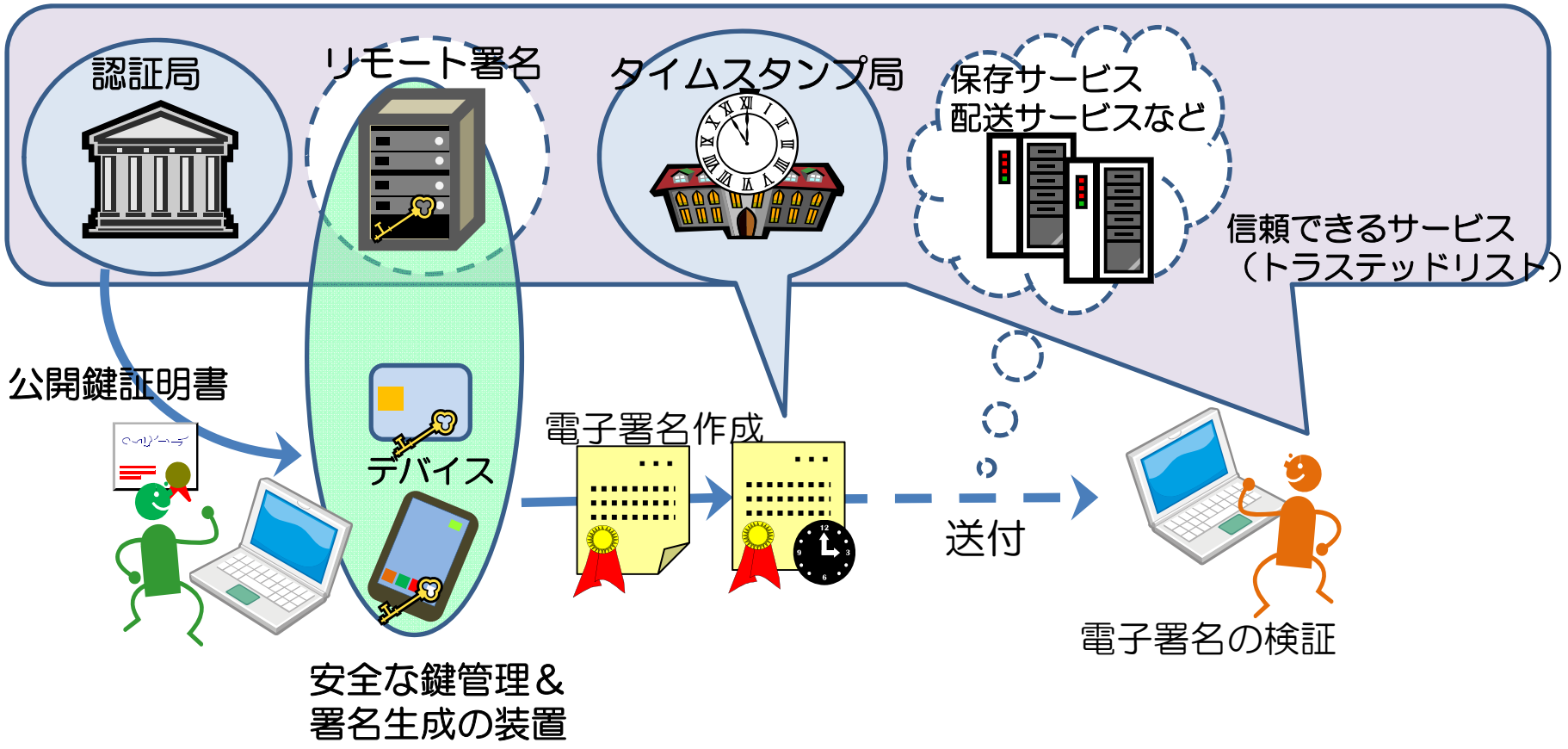
nd

014

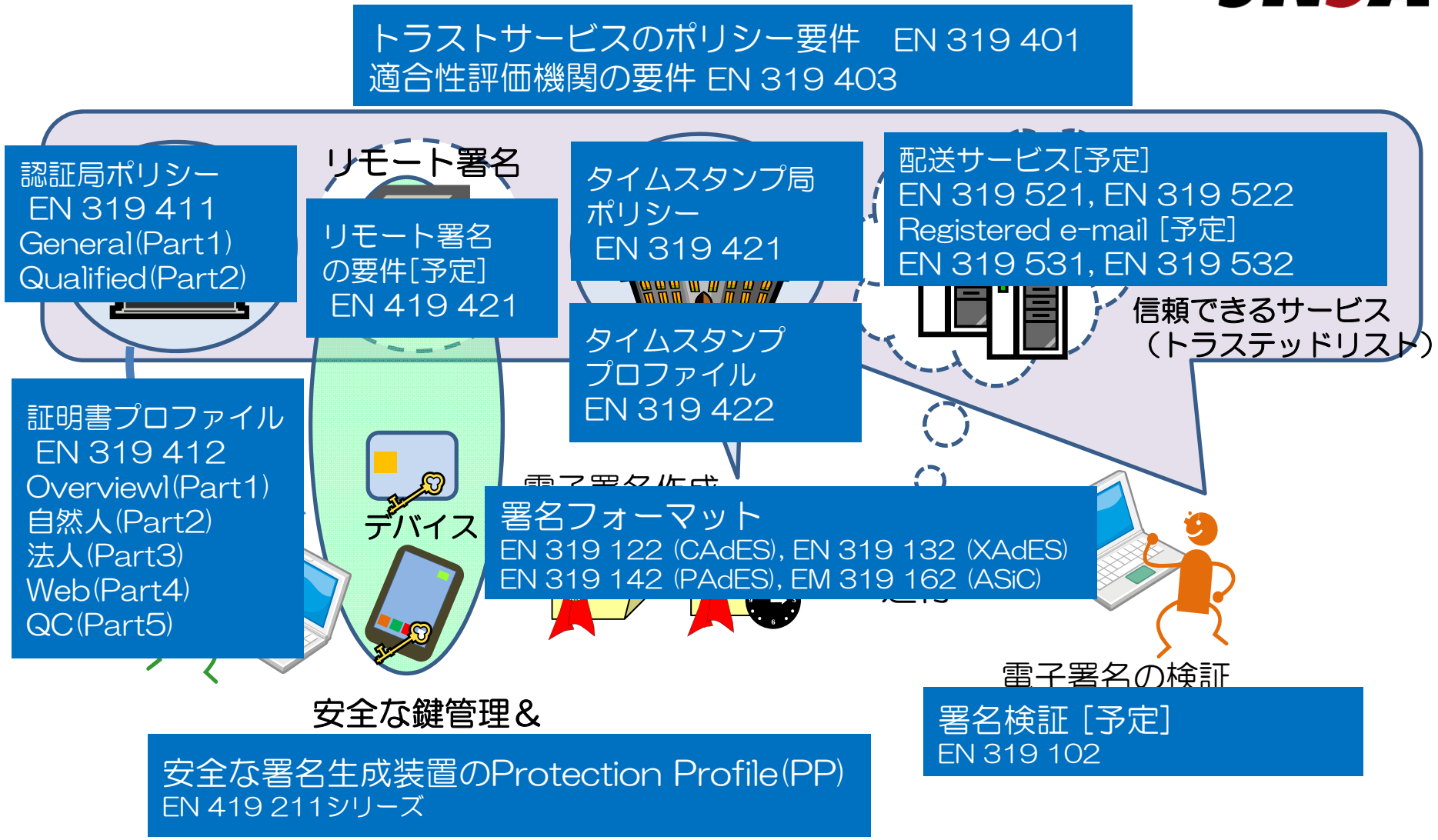
EUのeIDAS Regulationの動き

- 法制度と技術標準（ENやISO等）のリンク
- 1999年からのDirective時代よりも強制力UP
- 一気通貫的に体系化された技術標準を目指した動き
  - トラステッドリスト
  - トラストサービス(CA, TSA, Delivery Service, etc.)に関するポリシーや運用
  - 証明書プロファイル
  - 署名フォーマット
  - デバイスやリモート署名サーバー

再構築作業真っ只中のEN標準



再構築作業真っ只中のEN標準



さて、日本は？
電子署名法の周辺だけ覗いてみます

日本の電子署名法

JNSA

電子署名及び認証業務に関する法律（2000年制定）

- 電磁的記録の真正な成立の推定
  電子署名の付された電磁的記録が手書きの署名や押印の付された文書と同等に通様する法的基盤の確立（真正に成立したとの推定がなされる。）
- 任意的な認定認証制度
  電子署名が本人のものであることを確認する認証業務に関し、任意的な認定制度の導入（認証業務の利用者に対し、信頼性の目安を提供）

http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/law-index_e.htmlより引用

電子署名法と認証局

電子署名法 第二条一項　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。
一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
二　当該情報について改変が行われていないかどうかを確認することができるものであること。

認証業務：当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務（二項）
特定認証業務：主務省令で定める基準に適合するもの（三項）
特定認証業務の認定：特定認証業務を行おうとする者は、主務大臣の認定を受けることができる（第四条）

- 電子署名及び認証業務に関する法律施行規則
  証明書とそれを発行する認証局の要件、認定認証局の要件
- 電子署名及び認証業務に関する認定に係る指針
  より詳細な認定の指針

電子署名法と電子署名技術

電子署名法 第二条一項　（略）
一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
二　当該情報について改変が行われていないかどうかを確認することができるものであること。

電子署名法 第三条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

「電子署名及び認証業務に関する法律施行規則」では
- 電子署名の暗号（署名）アルゴリズムへの要件が示されている
- 認定される特定認証業務の基準が示されている

それ以外の、利用者側の適正な署名鍵の管理や署名データフォーマット等の要件は？？？

e文書法

- 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律(2005年施行)
- 平たく言うと、民間事業者に対して紙での作成/交付/保存が求められていた文書を電子データでも認めるようにした。
  - 個別の法改正なく容認だが例外もある（個別の法律で規定）。
- 電子データの作成/交付/保存の要件は文書の種類により各省庁が定める。
  - これらの要件はあくまでも民側が保存義務等を守るために必要なもの。その文書が民事訴訟など他の係争に備えるためにも必要であれば、別の要件（証明力を備えるためのセキュリティ対策など）も考える必要があるだろう。

e文書法に関わる省令やガイドラインの例

- 財務省・国税庁
  - 「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」(1998年)
    - e文書法を受け2005年に改正（スキャナ保存の容認）
    - 保存方法の要件緩和で施行規則が2015年と2016年に改正
- 厚生労働省
  - 「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」(2005年)
  - 「医療情報システムの安全管理に関するガイドライン」 第5版
- 国土交通省
  - 「国土交通省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則 」（2015年）
  - 関連：「建築確認手続き等における電子申請の取扱いについて（技術的助言）」(2014年)
  - 関連：「建築確認検査電子申請等ガイドライン」（2014年,一般財団法人建築行政情報センター）
- 法務省
  - 会社法施行規則（2006年）
  - 関連：商業登記法

e文書法に関わる省令やガイドラインの例と電子署名技術との関係

※タイムスタンプはいずれも日本データ通信協会認定のもの

- 財務省・国税庁
  - 「 関 列に

電子帳簿保存法の施行規則と通達で規定
- 電子取引：タイムスタンプ or 不当な訂正削除を防止する規定と運用
- 国税関係書類のスキャナ保存： タイムスタンプ

- 厚生労働省
  -

医療情報システムの安全管理に関するガイドラインで紹介
- 電子署名の標準規格としてJIS X 5092(CAdES), JIS X 5093(XAdES)

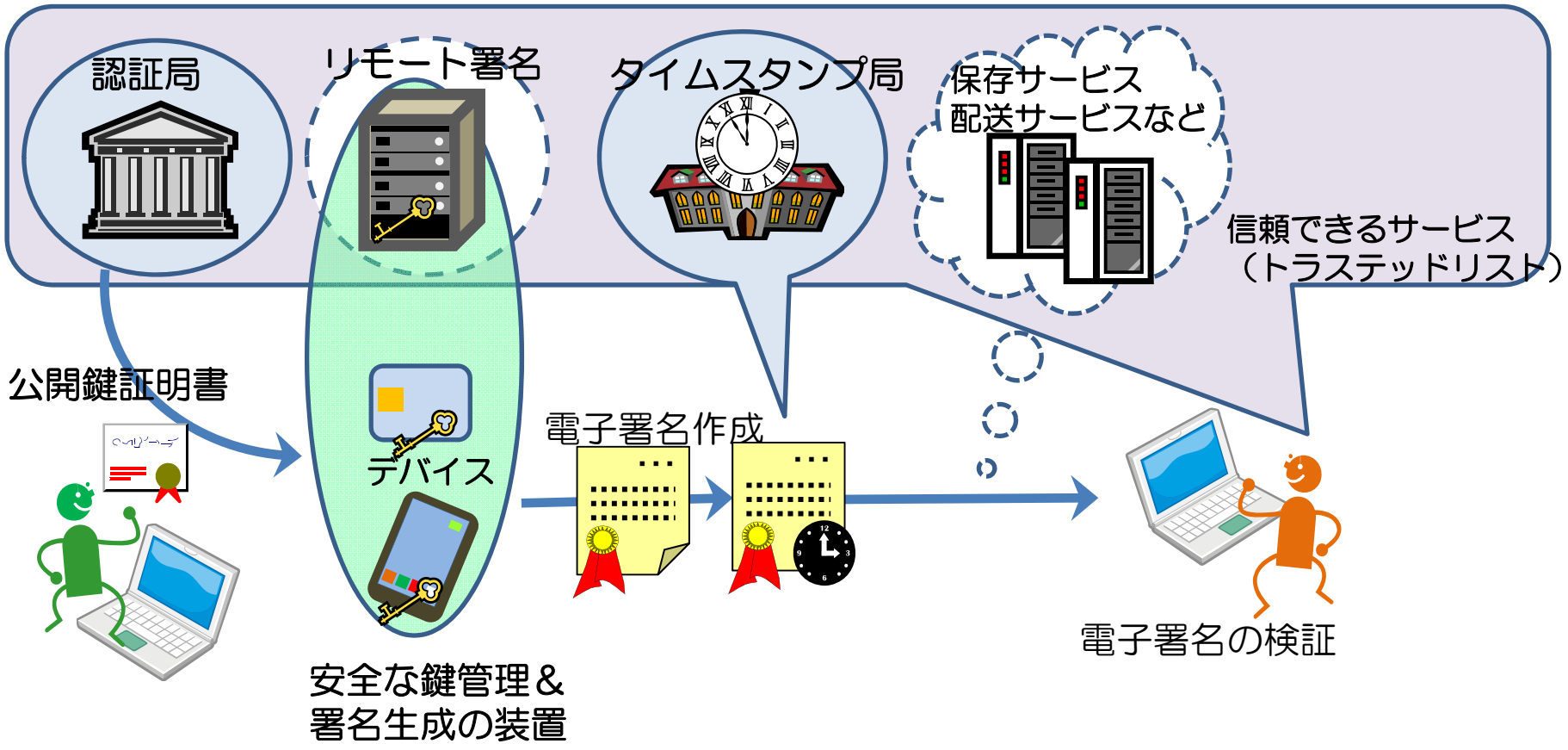
  -
- 国土交通省
  - 「国土交通省の所管する法令に係る民間事業者等が行う書面の保存等に
  - 術的
  - 関連：「建築確認検査電子申請等ガイドライン」（2014年,一般財団法人建築行政情報センター）

建築確認検査電子申請等ガイドラインで記述
- 電子署名形式としてPAdESを推奨。
- 証明書は、商業登記認証局、公的個人認証、認定認証局

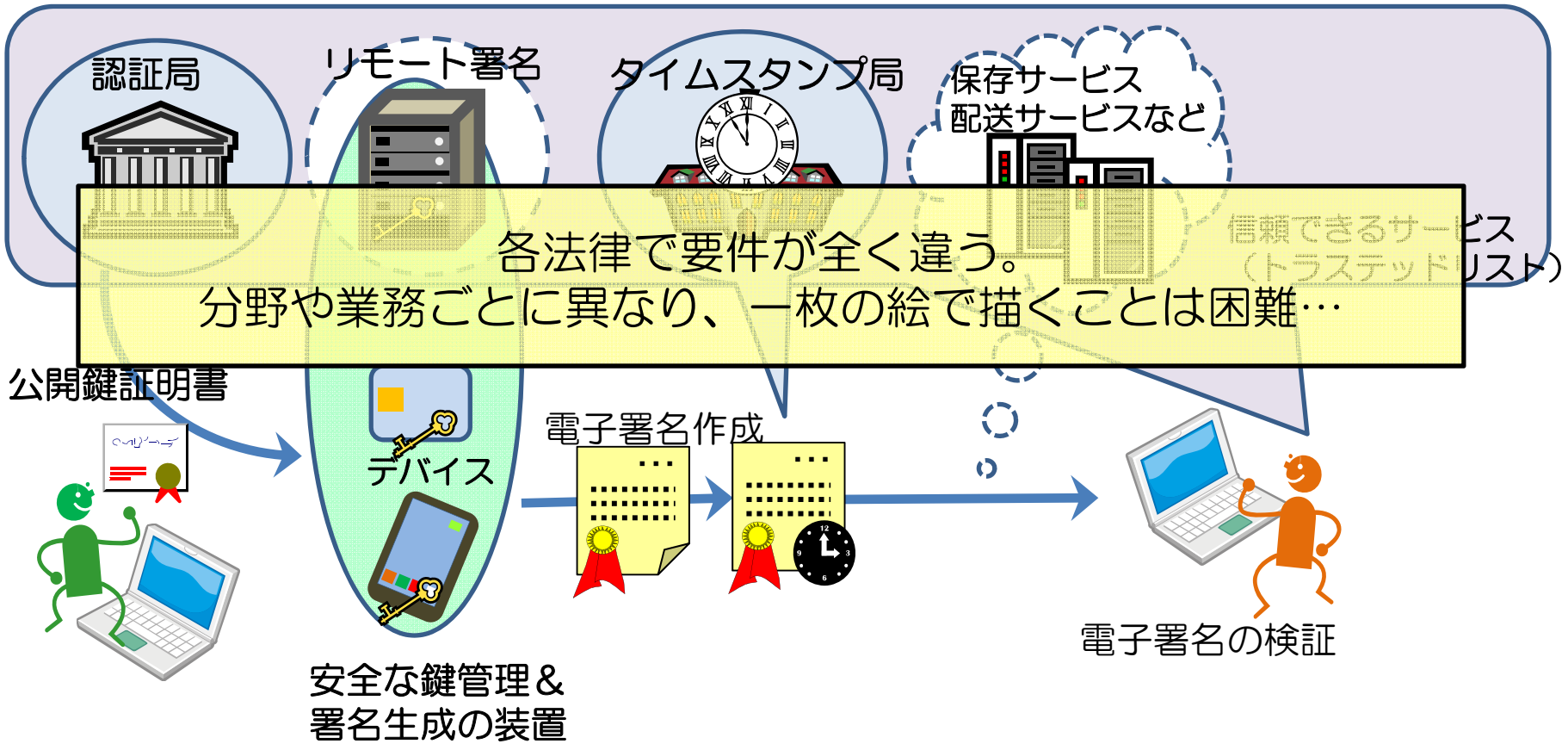
- 法務省
  -
  -

会社法：署名または記名押印に代わる措置として電子署名（標準技術は特に言及なし）。ただし、商業・法人登記のオンライン申請をする場合は商業登記法施行規則に従った証明書が必要（商業登記認証局, 公的個人, 認定認証局）。

日本の法制度と電子署名技術の関係とは？

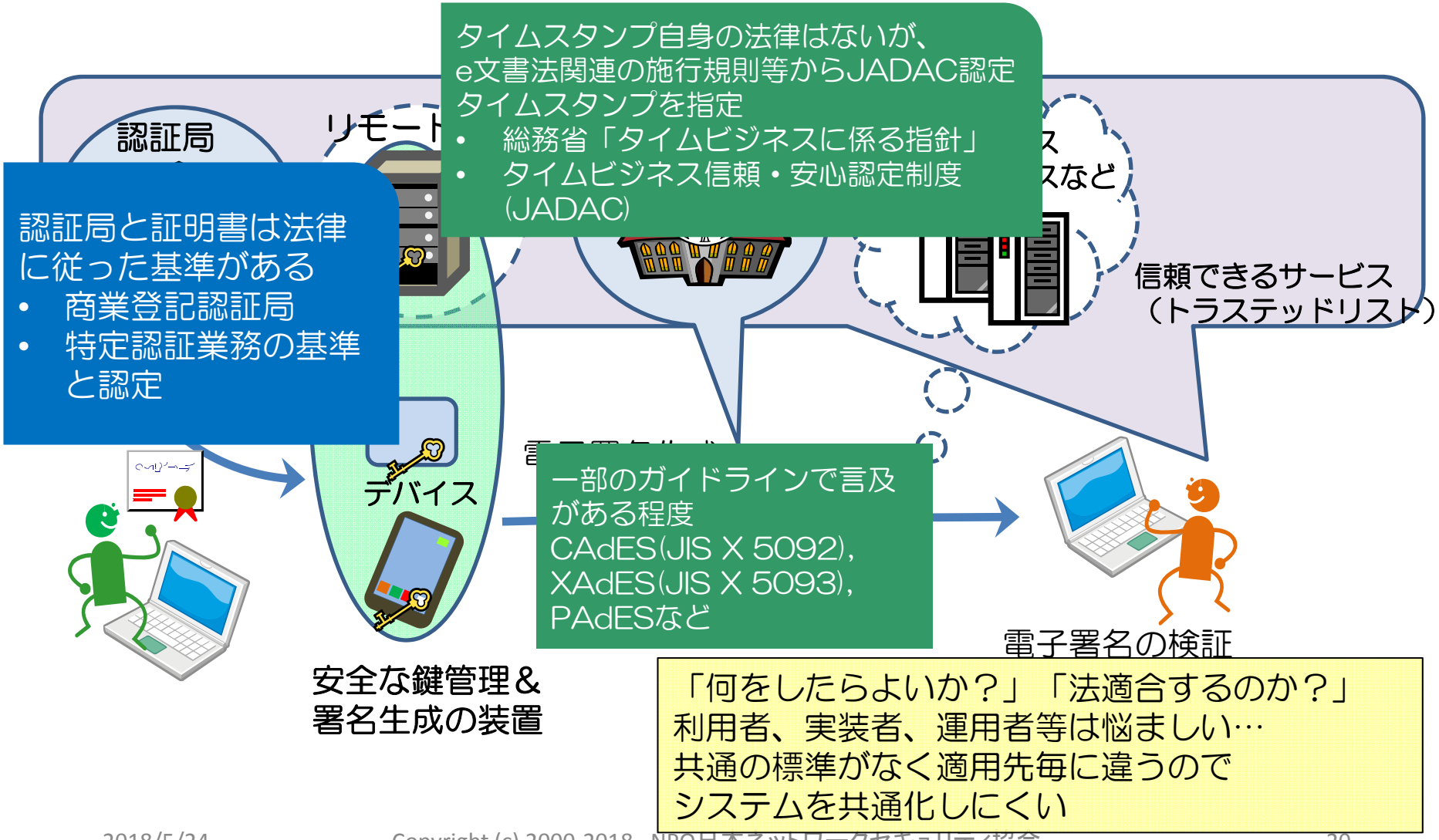


日本の法制度と電子署名技術の関係とは？



日本の法制度と電子署名技術の関係とは？

あえて書いてみるなら…これくらいか



まだまだ議論は続く

JNSA

- 個別議論だけでなく横断的で整合性のあるフレームワークは作れないものか…
- 電子署名だけでもやるべきことが多い
  - 電子署名フォーマット
  - 電子署名検証処理、検証レポートの標準
  - 鍵管理（リモート署名ガイドなど）
  - トラストサービス基準、トラステッドリスト
- 周辺技術との整合性
  - ユーザー認証を含めた真正性の証明
  - 電子データの活用・連携基盤

まだまだ議論は続く

- 個別議論だけでなく横断的で整合性の
  レームワークは作れないものか…
  - 子署名だけでもやるべきことが多い
  - 電子署名フォーマット
  - 電子署名検証処理、検証レポートの標
  - 鍵管理（リモート署名ガイドなど）
  - トラストサービス基準、トラステッドリスト
  - 辺技術との整合性
  - ユーザー認証を含めた真正性の証明
  - 電子データの活用・連携基盤

宮地さんの発表

村尾さんの発表

山中さんの発表

濱口さんの発表

JNSAで議論

JNSAで議論

JT2Aで議論

TSFで議論
（トラストサービス推進フォーラム）

JT2Aで議論