JNSA

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

Network Security Forum 2014
ミニパネル：
電子署名をめぐる国内外の最新動向

宮崎　一哉

電子署名WGリーダー

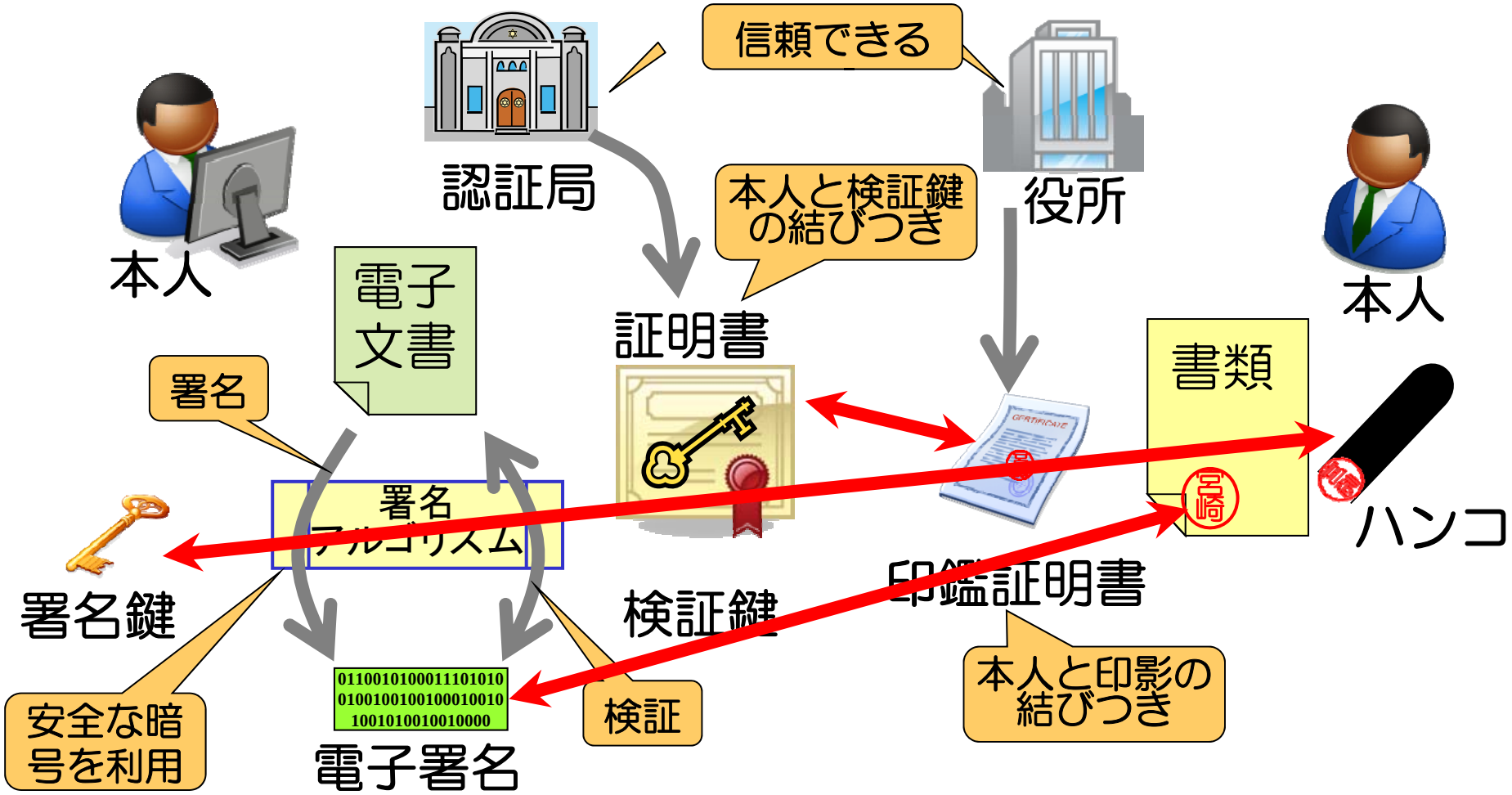
（三菱電機株式会社）

2014 年1月29日

このセッションの進め方

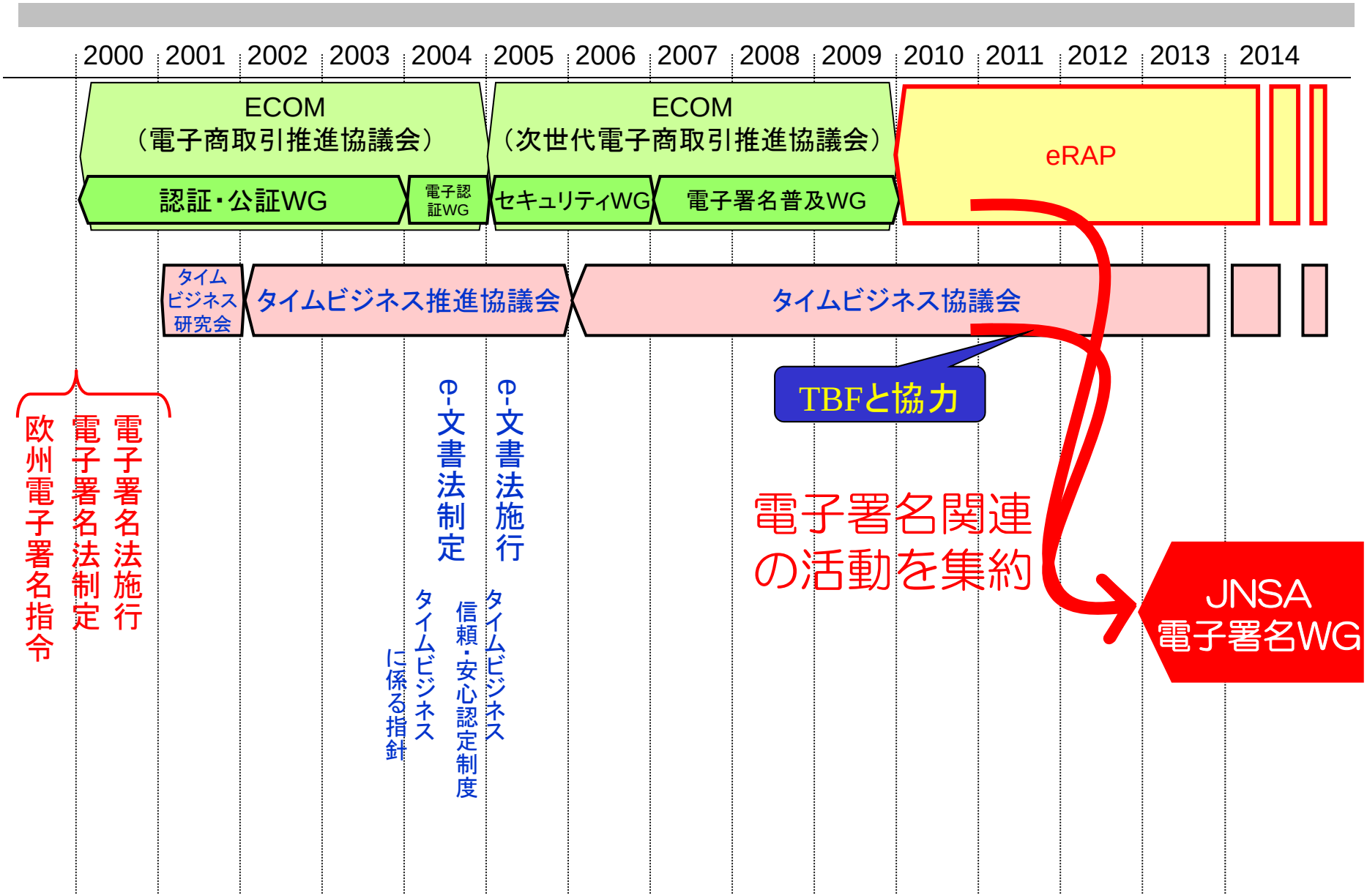
- まえおき
  - 電子署名とは？
  - 電子署名WGについて
  - 電子署名をめぐる国内外の情勢
- パネリストによるミニプレゼン
  - サブリーダ：佐藤雅史さん
  - TBF：村尾進一さん
  - サブリーダ：宮地直人さん
- 今後に向けて
  - パネリストからのコメント

電子署名とは

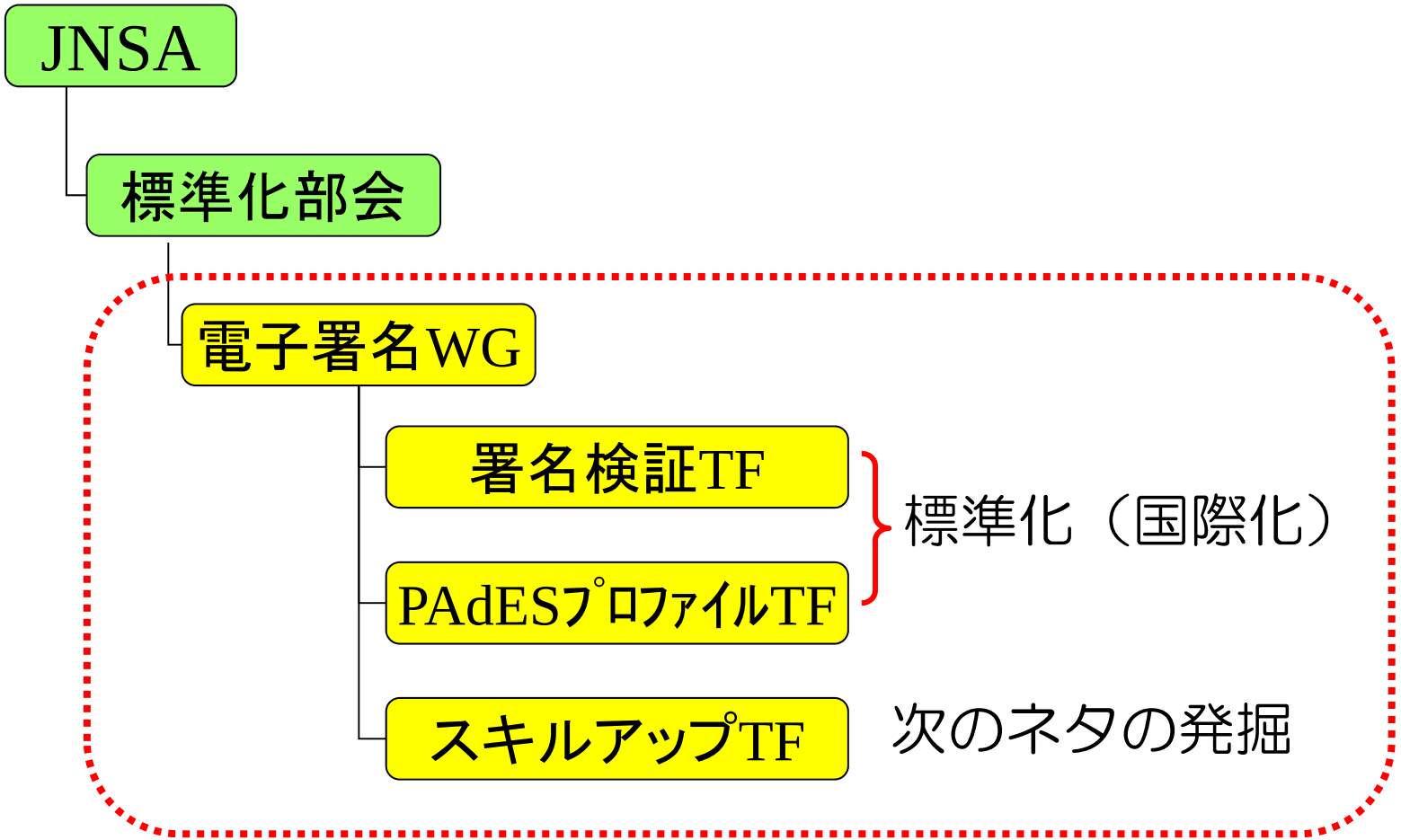


電子署名は、署名者が誰であるかに加え、電子文書が改ざんされていないことも確認できる技術。

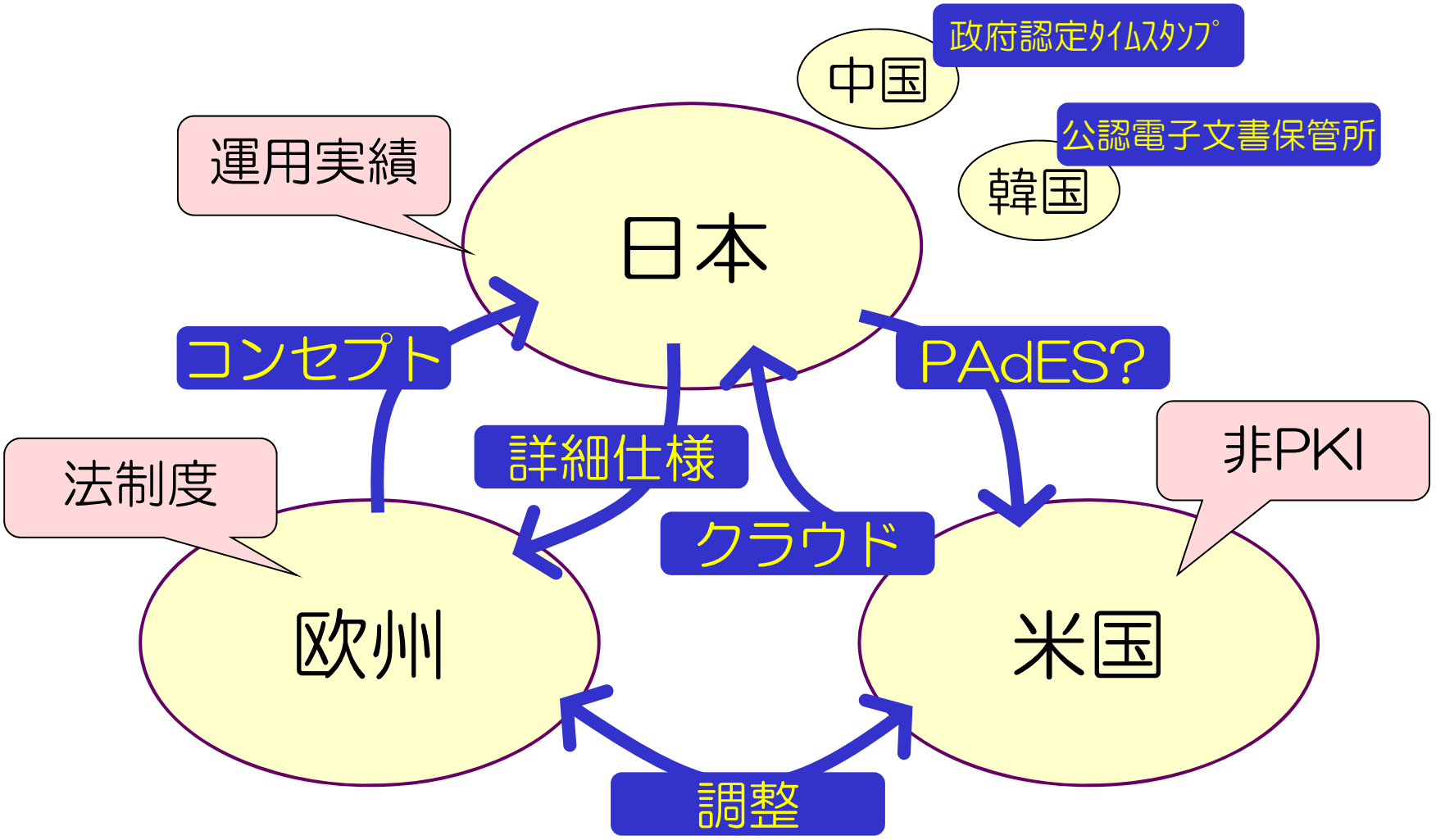
電子署名WGについて：設立経緯



電子署名WGについて：活動内容



電子署名をめぐる国内外の情勢



パネリスト

- サブリーダ：佐藤雅史さん
  （セコム）
  『電子署名標準化の動向』
- TBF：村尾進一さん
  （セイコーソリューションズ）
  『タイムスタンプ活用の動向』
- サブリーダ：宮地直人さん
  （ラングエッジ）
  『電子署名の今後に向けて』

最後に

- PKI Day 2014で本日の話題の詳細を報告します。
  - 日時：3月13日（木）10：00～18：00
  - 場所：IIJグループ本社
- 電子署名WGのFaceBookページを開設。
  https://www.facebook.com/eswg.jnsa.org
- 電子署名WGは電子署名のポータル、よろず相談窓口、交流拠点、発信基地、メッカ、、、、を目指します。
- 皆さんのご参加をお待ちしております。

JNSA

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

Network Security Forum 2014
電子署名をめぐる国内外の最新動向
～電子署名標準化の動向～

佐藤雅史

セコム株式会社　IS研究所

2014 年1月29日

欧州と米国の電子署名

JNSA

欧州

- 規制型のモデル
- PKIに基づく電子署名
- 技術や運用の標準
- 各国との相互運用テスト
- 信頼基盤の構築

米国

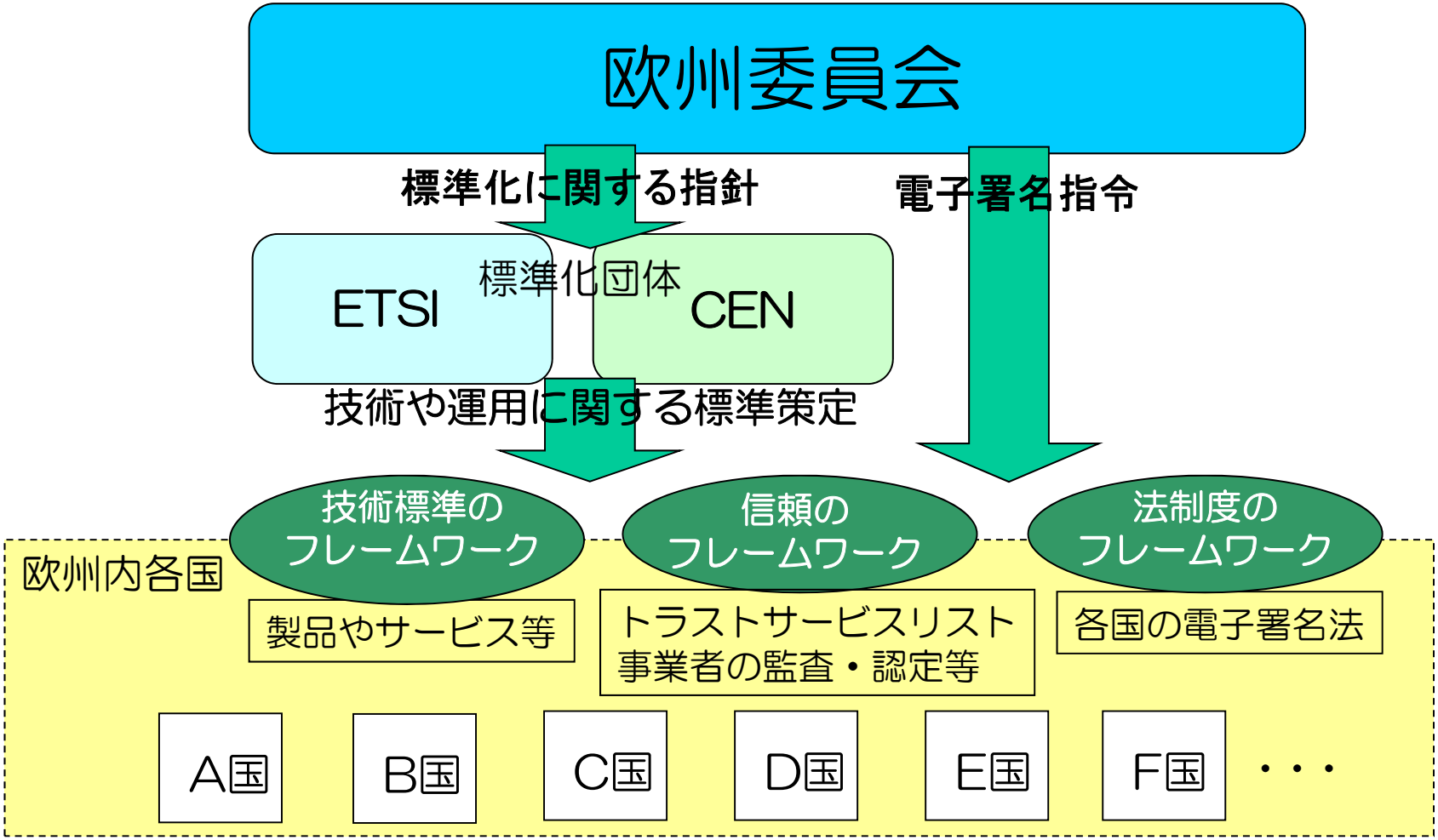
- 市場型のモデル
- 特定の技術に依存しない
- クラウド型の電子署名(契約)サービス

欧州・米国共同による電子署名ワークショップ開催

・クラウド/モバイルのための標準策定
・EU電子署名法の見直し（法人署名）

・クラウド電子署名サービスによる欧州型電子署名のサポート

欧州の電子署名の体系



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。

欧州の電子署名の動向

- より安全な電子署名のための基盤構築
  - 欧州内の横断的なトラストサービスリストの構築：信頼できるサービス（認証局、タイムスタンプ局など）の認定など。
- より使いやすい電子署名を目指した標準策定
  - 技術標準体系のたな卸し
  - 新しい技術標準の策定
    - ASiC
    - クラウド型サービスのための技術標準
    - CAdES新バージョン
    - 電子署名検証手順
  - 相互運用性テストの実施
    - 2013年12月のCAdES相互運用テストでは60社を超える参加者！（日本、ブラジルも参加）
      →（参考）2009年に行った初テストでは17社が参加
- 電子署名法の見直し
  - 自然人の電子署名だけでなく法人の電子署名も対象に（e-Seal）

日本の電子署名

- 法制度と技術が整合性のある形で体系化されていない問題がある。
  - 各省庁や各業界団体でビジョンが共有されておらず、別個の要件が提示されうる。分かりにくさの原因にもなっている。
  - 欧州のように法制度も技術標準も見直しのサイクルが必要。
- 電子署名の運用経験は世界をリードしているかもしれない。
  - 電子帳簿保存や医療分野など電子署名の文書量では、実は世界的に見てもかなり多いのでは？
  - 電子署名の運用経験も豊富で、解決すべき課題も見えてきている（その解決策を日本から世界に発信できる可能性がある！）
- これまでの日本の貢献も意外と（？）と大きい。
  - オンライン相互運用テストの開始と欧州への提案。
  - 欧州規格改定の提言。
  - PDF長期署名（PAdES）策定の元となる問題提起。
  - 日本からの国際標準化 (ISO 14533)。JIS規格化(JIS X 5092/5093)。

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

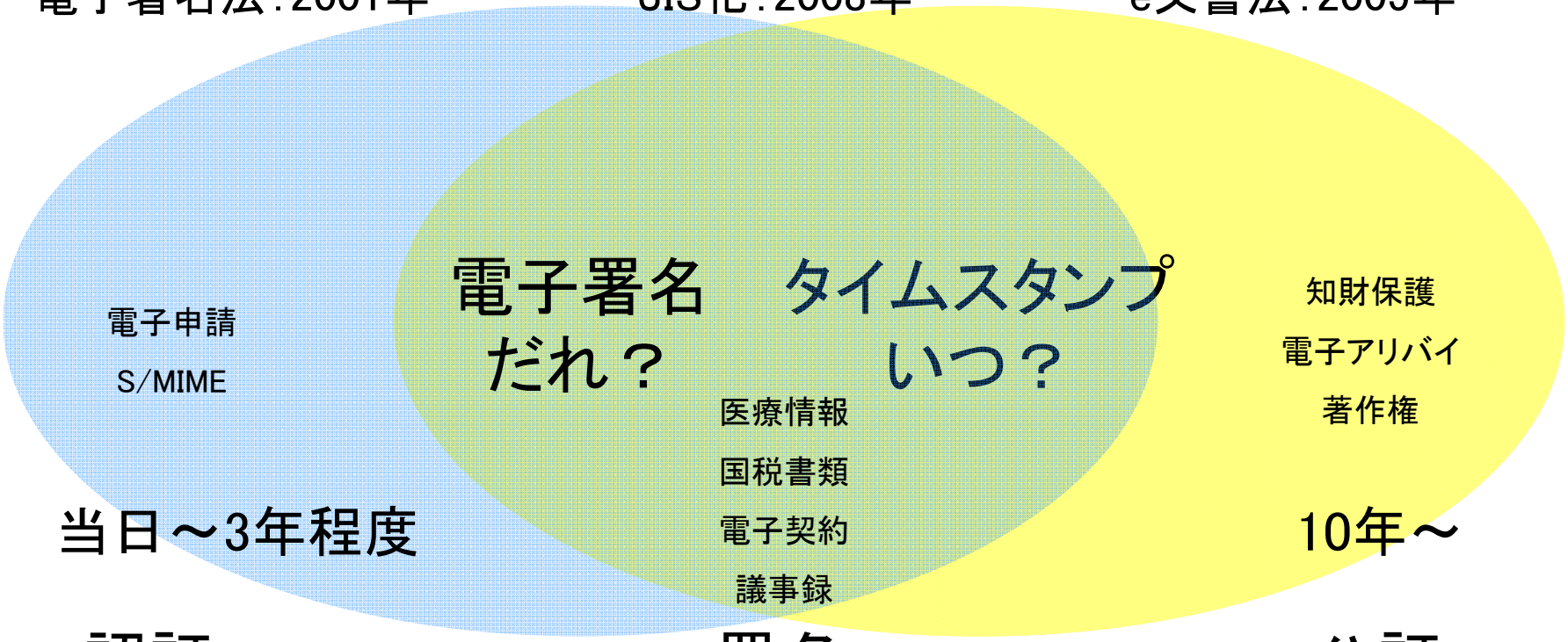
Network Security Forum 2014
タイムスタンプ活用の動向

村尾　進一

セイコーソリューションズ株式会社
クロノトラスト部

2014 年1月29日

電子認証、タイムスタンプ、そして電子署名



長期署名プロファイルの規格
（JIS：2008年3月、ISO：2012年9月）

JIS-X5092，ISO14533-1　CMS利用電子署名（CAdES）の長期署名プロファイル

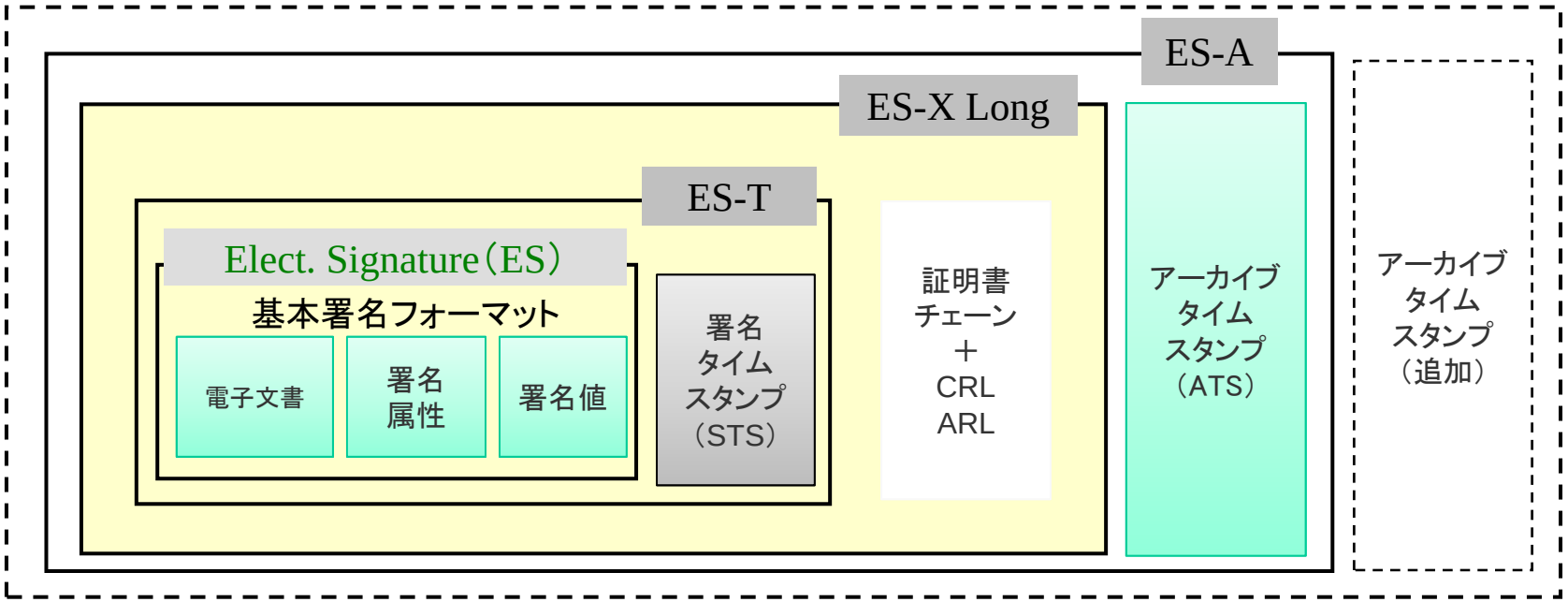
JIS-X5093，ISO14533-2　XML署名利用電子署名（XAdES）の長期署名プロファイル

【ポイント】

・署名タイムスタンプ（STS）により署名時刻の証拠性を確保

・失効情報や証明書を署名データ内に格納し、証明書検証の継続性を確保

・アーカイブタイムスタンプ（ATS）の暗号アルゴリズムにより、署名データや失効情報等を保護



ES：
Electronic Signature

ES-T：
Electronic Signature with Time stamp

ES-X Long：
Electronic Signature eXtended

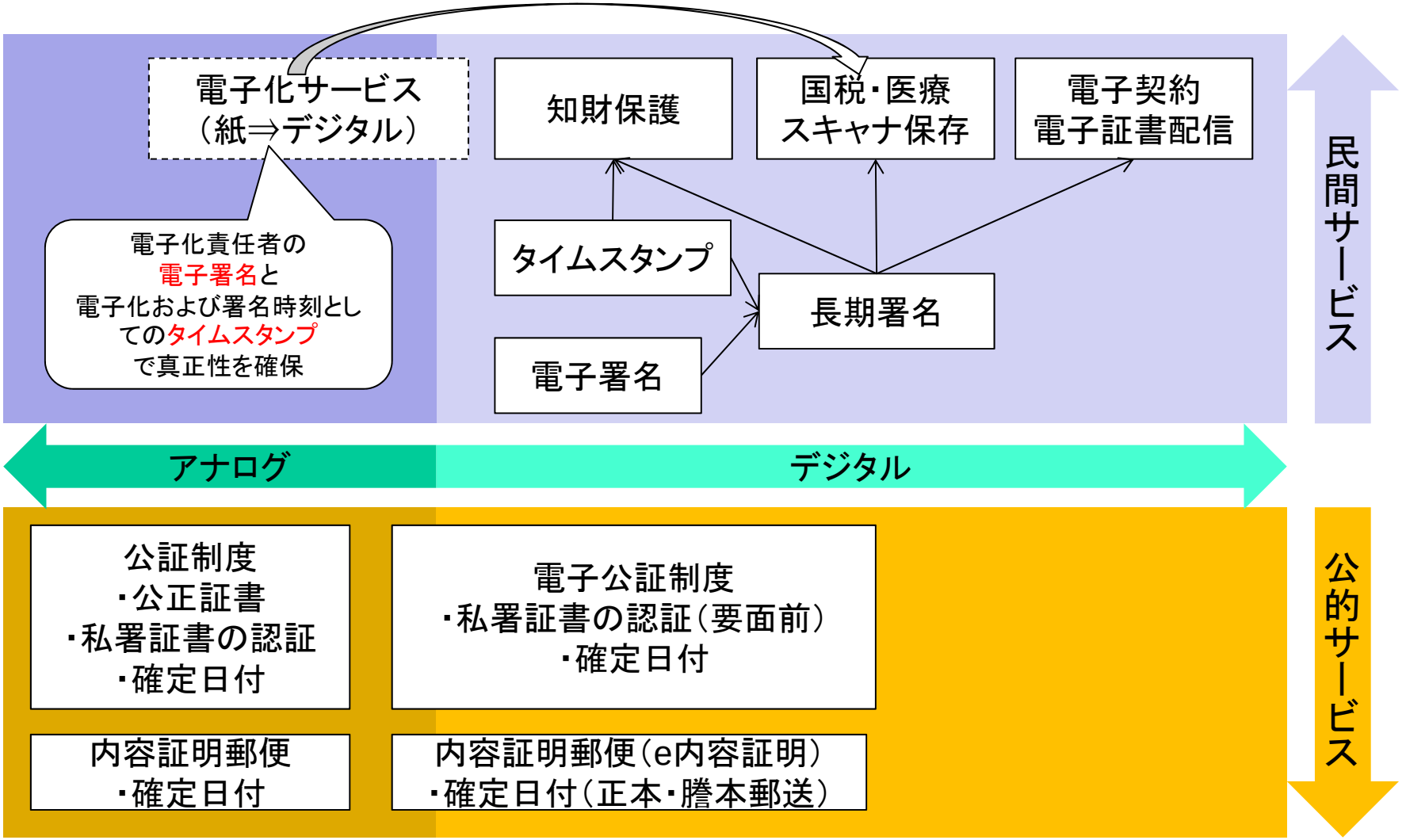
ES-A：
Electronic Signature Archive

タイムスタンプ利活用の拡大に向けて

- 従来から一般的であった公証制度および内容証明郵便に対して電子署名やタイムスタンプを代用したり併用する際の妥当な適用範囲と運用要件を検討し課題をとりまとめました。
  - 「公証制度の電子化適用に関するガイドライン検討報告書」

- 上記報告書はhttp://www.dekyo.or.jp/tbf/seika/index.htmlよりダウンロードいただけます。

証明サービスマップ

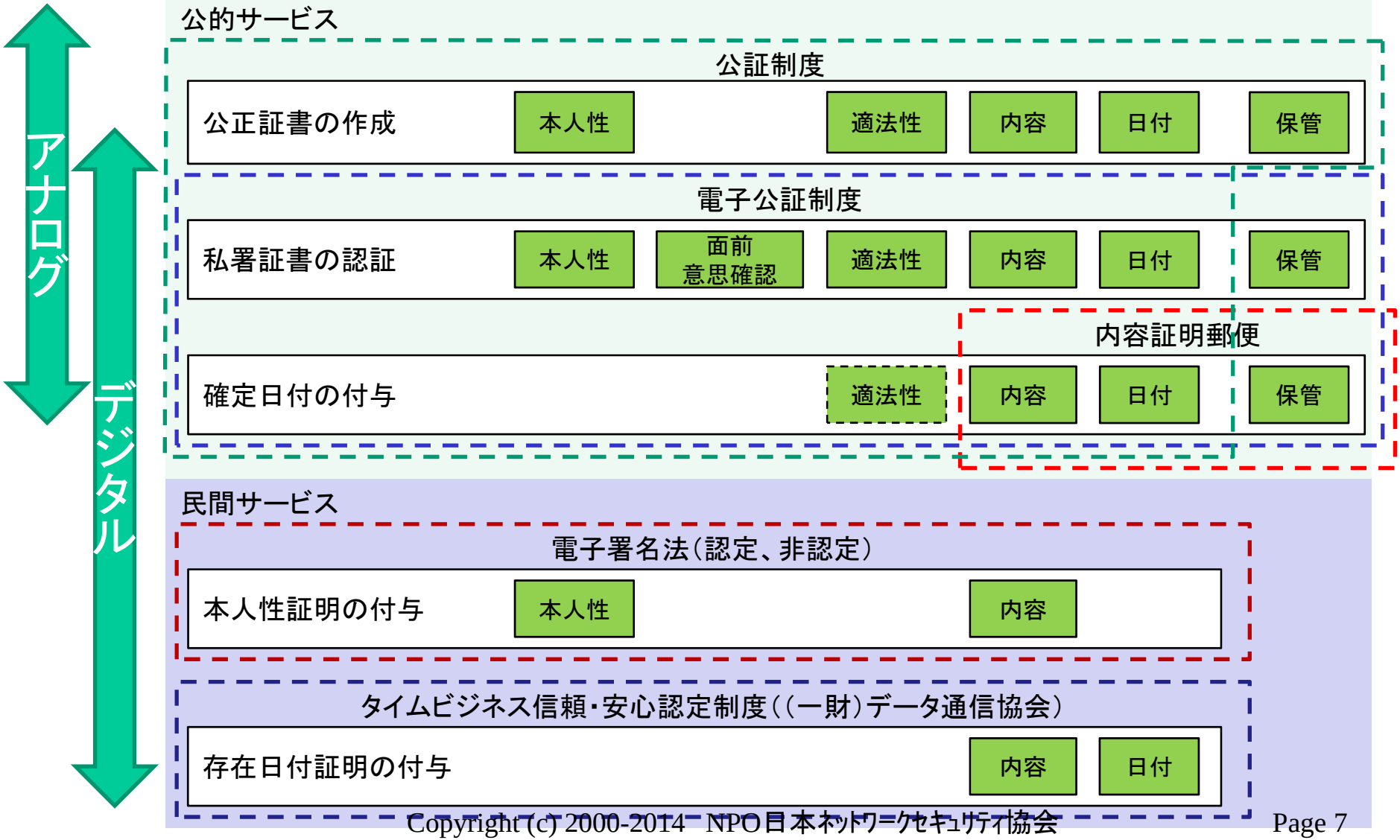


証明サービス選択の要件

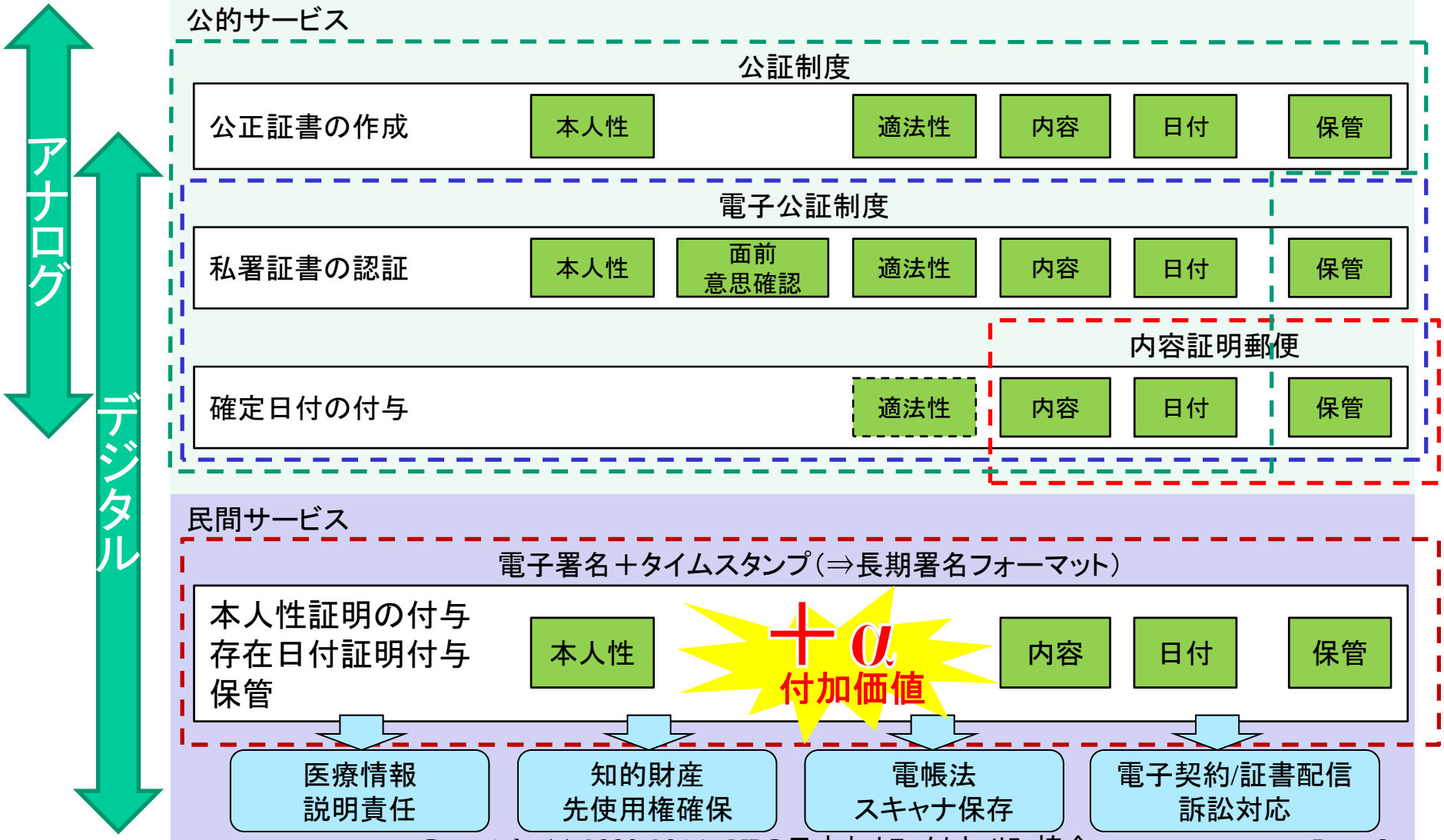
証明サービスを利用するに当たっての主な実施要件

No.	要件	主なチェックポイント
1	証明対象文書の特定	ファイル形式 ファイルサイズ 数量
2	証明対象文書の必要な証明期間の特定	短期：1~3年 長期：~10年 超長期：10年以上 参考： 電子公証サービス：保管期間20年 e 内容証明：保管期間5年 電子証明書：1年～5年 タイムスタンプ：～10年
3	証明対象文書の証明方式の特定	公的サービス：公証制度、電子公証制度、内容証明郵便 民間サービス：電子署名、タイムスタンプ、･･･
4	その他の確認	公知な方法？：国際規格？独自仕様？ 安全性は？：暗号アルゴリズム？ 汎用性・互換性は？：データ移行可？ 利便性は？：使い易さ？アクセス方法？

公的／民間証明サービスの整理（1）



公的／民間証明サービスの整理（2）



海外タイムスタンプ動向

国名	トピック	備考
中国	知的財産保護目的でのタイムスタンプ利用が急速に拡大している。 既に判例2件あり。	RFC3161タイムスタンプ準拠 タイムスタンプ局の認定制度あり
韓国	韓国特許庁で「営業秘密原本証明サービス」を開始（2010年10月）。証明手段としてタイムスタンプを利用。	日本でも日本版「営業秘密保護センター」の創設を検討中。
タイ	タイムスタンプ局（TSA）および時刻配信局（TAA）の制度創設を検討。	
ヨーロッパ	EU指令460にて、適格タイムスタンプ要件（法的推定効要件）が規定された。 ・正確な方法で、協定世界時（UTC）に紐付いていること ・正確なタイムソースに基づいていること ・適格信頼サービス提供者によって発行されること ・高度な電子署名または適格信頼サービスプロバイダの高度な電子シールを使用して、またはいくつかの同等の方法によって署名されていること。	2012年6月4日に欧州議会で採択

国内動向（電子署名・タイムスタンプ利活用可能領域）

IT利活用の裾野拡大のための規制制度改革集中アクションプラン

（平成25年12月20日高度情報通信ネットワーク社会推進戦略本部）

	項目名		項目名
1	高等学校での遠隔授業の正規授業化	15	政府のオンライン行政手続きにおける本人確認手続きの見直し
2	不動産取引における重要事項説明に際しての対面原則の見直し	16	ID連携による制度間の本人確認の合理化
3	国家資格の取得更新時におけるｅ－ラーニングの活用	17	個人番号カードを活用した公的個人認証サービスの利用場面拡大
4	株式会社の事業報告等のウェブ開示	18	登記情報の共有化、添付書類省略
5	電子的な手法による労働条件の明示	19	自動車保有関係手続きのワンストップサービスの拡充
6	国税関係帳簿書類の電子化保存に関する規制の見直し	20	道路占用手続きの簡素化・統一化
7	教科書の電子化	21	航空機登録申請の添付書類を削減した上での電子化
8	保険契約の解約返戻金がないことを記載した書面の交付義務の緩和	22	旅館における宿泊者名簿の電磁的作成・保存の推進
9	ｅ－文書法の再徹底	23	クラウドメディアサービスの実現のための規制の見直し
10	ハローワークにおける「在宅勤務」の取り扱いの見直し	24	金融機関による外部委託先の監督についての明確化
11	「くるみん」制度認定基準へのテレワークの組み込み	25	現況地形及び施工図の3D化・配信の推進
12	労働者が希望する場合に所定労働時間内の深夜労働割増の柔軟化	26	建築確認申請の電子化
13	在宅勤務と育児休業を両立させるための給付金支給規定の改定	27	公的機関からの電子的手段による通知の促進
14	遠隔雇用をする場合の最低賃金基準の見直し	28	地下街等の閉空間における電波申請書（工事設計書）の簡素化

JNSA

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

Network Security Forum 2014

ミニパネル

電子署名をめぐる国内外の最新動向

「電子署名の今後に向けて」
～スキルアップTFの活動から～

宮地 (miyachi@langedge.jp)

電子署名WGサブリーダー/スキルアップTFリーダー

（有限会社ラング・エッジ）

2014 年 1 月 29 日

話の前にスキルアップTF

電子署名の今後の動向を調査・勉強・開拓する
未来志向のタスクフォースです。

1. 勉強会でWG/TFメンバーのスキルアップ
2. 新しいトレンドや情報をキャッチアップ
3. 電子署名プログラマへの情報や環境提供

2013年度は既に6回勉強会を開催。
興味があれば外部からも講演者を招へい。
新しい事に挑戦します！

スキルアップTF勉強会テーマ

JNSA

第1回：7月：長期署名入門

講師＞電子署名WGオールスター 宮崎氏、佐藤氏、石本氏、西山氏、宮地

第2回：8月：クラウド署名とHSM

講師＞タレス・ジャパン 住田氏、セーフネット/JIPDEC客員研究員 亀田氏、他

第3回：9月： jsrsasign / jsjws 勉強会

講師＞富士ゼロックス 漆嶌氏

補足＞JavaScriptによるRSA/PKIモジュールとJSON署名

第4回：10月： PDF電子署名仕様入門

講師＞ラング・エッジ 宮地

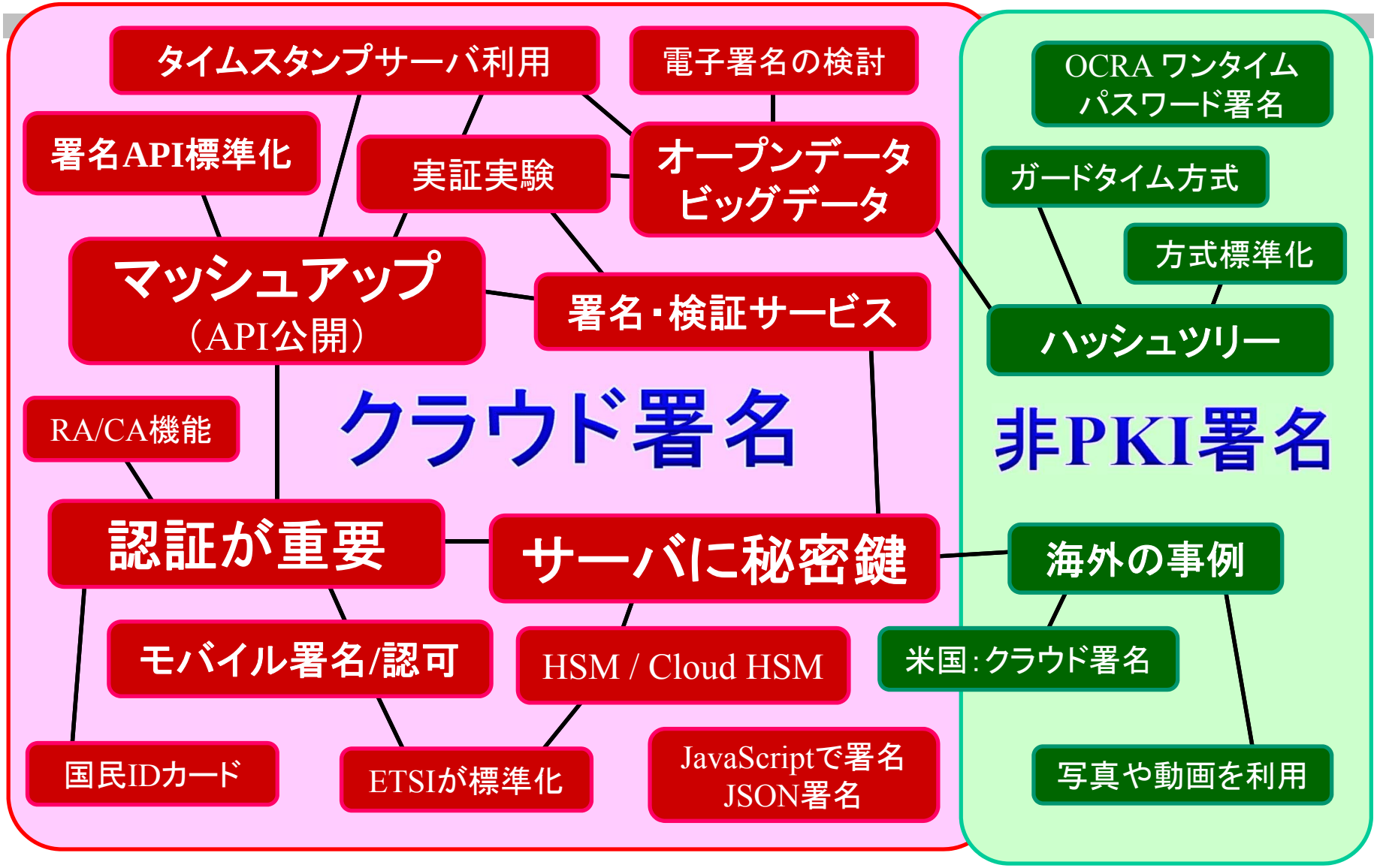
第5回：11月：クラウド時代のデータセキュリティ

講師＞ガードタイム 柳原氏

補足＞ガードタイム社による非PKI署名他

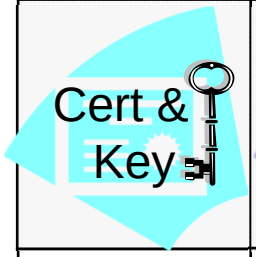
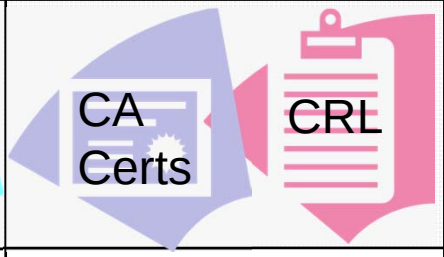
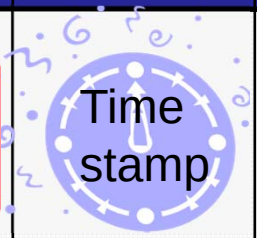
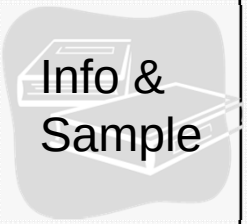
第6回：1月：電子署名WG合宿ダイジェスト

今後のキーワードを俯瞰



遊び場プロジェクト
～プログラマの為のお試し環境構築～

JNSA

CA機能			TSA機能	情報公開	署名機能	検証機能
						
証明書・鍵サービス	リポジトリ公開 HTTP / LDAP	OCSP発行	タイムスタンプ発行	ソース他公開	サービス提供	サービス提供
対話画面による発行	CA証明書は公開 CRLは定期的に更新 出来ればCSP/CP等も	証明書DBまたはCRL連動し発行	CA機能でTSA証明書を準備	各機能実装情報やサンプルを公開	APIや対話画面を用意してクラウド的にモバイル署名も考慮して検討する	
OpenSSLのCA機能認証連携	OpenSSLの簡易CA機能を利用 画面は作成が必要	OpenSSLで可能？ ocspオプション利用	 準備完了 FreeTSA	Wiki, Blog GitHub 等	Ruby on Rails 等か CA機能と連携？ FreeXAdES, jsrsasign 等の利用	
証明書・秘密鍵は登録制等にして完全フリーは難しいかも。一応本人確認くらいはする？ OCSPは最初は無くても良いかもしれない。			認定TSAからの提供も歓迎	長期署名サンプル等ノウハウも	クラウド署名の実証実験的にできるとベスト HSM等使えると面白い	
JNSAではかつて「チャレンジPKI http://www.jnsa.org/mpki/index_j.html 」があった。今は使えない。						

興味を持った技術者がフリーで使えてプラグテストにも使える！

参考：FreeTSA（本日は説明無し）

OpenSSLコマンドによる簡単タイムスタンプ（RFC3161）サービス

- タイムスタンプって面白そうだから使ってみたい！
- タイムスタンプ クライアントの試験って使えるサーバは？

と言うような要望に応える為にOpenSSL 1.0.0のコマンドを利用して簡易タイムスタンプサービス（サーバ）の構築手順をまとめた。ラング・エッジのサーバで稼働させて手軽に使えるタイムスタンプサービスを提供中。プロジェクトとしては以下の2つ。なお作るには**別途TSA証明書は用意が必要**。

作る：FreeTSA Project：10分でできるタイムスタンプ局
使う：FreeTSA Service：自由に使えるタイムスタンプ局

- 参考 LangEdge Weblog: フリータイムスタンプ局（FreeTSA）のすゝめ
  http://www.langedge.jp/blog/index.php?itemid=665

電子署名の今後に向けて

JNSA

- 引き続き、新しいテーマを調査・勉強・開拓
  → 将来性があれば新しいTFの立ち上げ
- 勉強会を利用して実装や開発を（手を動かす）
  → 遊び場プロジェクトの推進
  → フリーソフトやプロジェクトの開発（FreeXAdES等）
- 他WGや他団体との連携（特にクラウド方面）
- 一般のプログラマ・技術者向け勉強会の開催
  → できれば若い電子署名技術者でコミュニティ形成を
- 足りない仕様の検討と標準化
  → 仕様の後追いでは無く先行したい
- 実証実験やプラグテストの実施
- 報告書や資料の作成と公開

若い世代の
活性化を！

FaceBookページやってます

最新情報やイベント情報等を公開しています。

https://www.facebook.com/eswg.jnsa.org

最後に

ご清聴ありがとうございました。

宣伝

クラウド/モバイル署名＆非PKI電子署名
詳しくは3月13日の PKI Day 2014 にて！

電子署名WGへの参加者募集中です！