



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

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

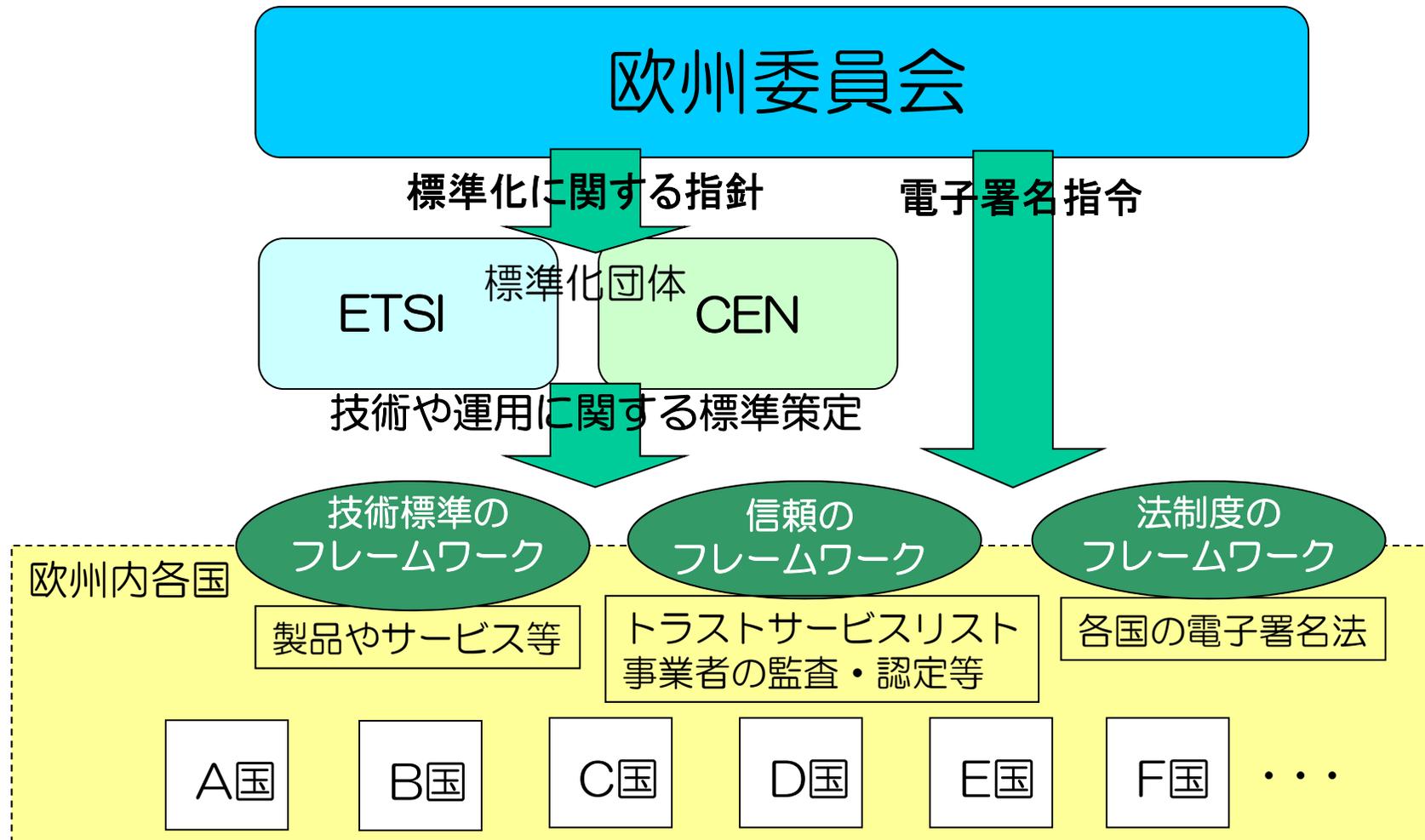
- 市場型のモデル
- 特定の技術に依存しない
- クラウド型の電子署名(契約)サービス

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)。

