セコムIS研究所
Intelligent Systems Laboratory

eRAP活動成果と今後の展開
～電子署名に関する活動について～

2013年3月19日

技術検討WG 副主査
セコム株式会社　佐藤雅史

News

Long-term authenticity of electronic signatures with ISO standard

by *Roger Frost* on 20 February 2013

A new ISO standard will help business and governments guarantee the long-term authenticity of electronic signatures, increasingly used in e-commerce and e-government.

Following the requirements of ISO 14533 will also ensure the interoperability of electronic signatures when the documents they authenticate are transferred and processed through different information technology systems. The new standard is in two parts:

- ISO 14533-1:2012, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles* – Part 1: *Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)*
- ISO 14533-2:2012, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles* – Part 2: *Long term*

organizations and governments who wish to preserve, or are mandated to preserve, electronic documents for a long period of time. These include organizations who wish to store electronic messages (such as EDI and XML based), agreements, contracts, or other documents for a period longer than possible up to now.

Klaus-Dieter Naujok, Chair of ISO technical committee ISO/TC 154 who developed the standard, comments: "ISO 14533-1:2012 and ISO 14533-2:2012 provide a new framework complying with the European Commission Mandate M/460, as well as helping the work by UN/CEFACT on its current revision on Recommendation 14 (Authentication of Trade

http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1706

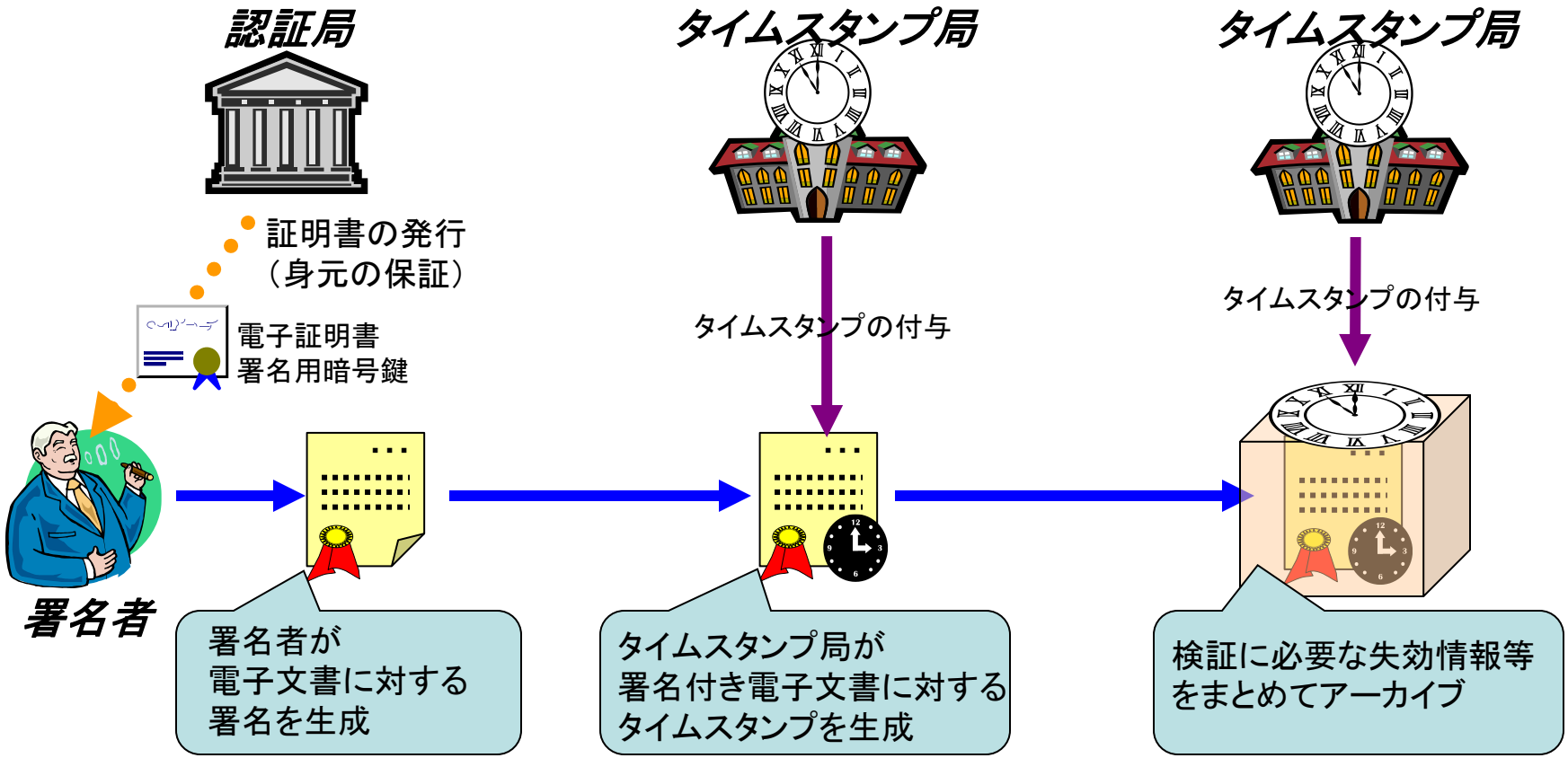
セコムIS研究所
Intelligent Systems Laboratory

発表内容

- 電子署名の仕組みと特徴
- これまでの取り組み
- 欧州の標準化団体ETSIとの関係
  - 日本と欧州における電子署名の体系の違い
- 電子署名の動向と課題
- 今後の活動

セコム IS研究所
Intelligent Systems Laboratory

電子署名（長期署名）の仕組み



電子文書の真正性担保
- 電子文書の改ざん検知
- 署名者の身元の保証

署名付き電子文書の時刻証明
(第三者による存在証明)

暗号脆弱化等への対策
（長期保存への対応）

セコムIS研究所
Intelligent Systems Laboratory

真正性を担保した電子文書の長期保管

文書保管システム/サービスで担保する場合

- システムごと保護する必要がある。
  - アクセスログの厳格な管理など。
- システムやサービスへの依存性大。
  - システムやサービスを移行しにくい。
  - ベンダーがサポートを停止した際の影響。

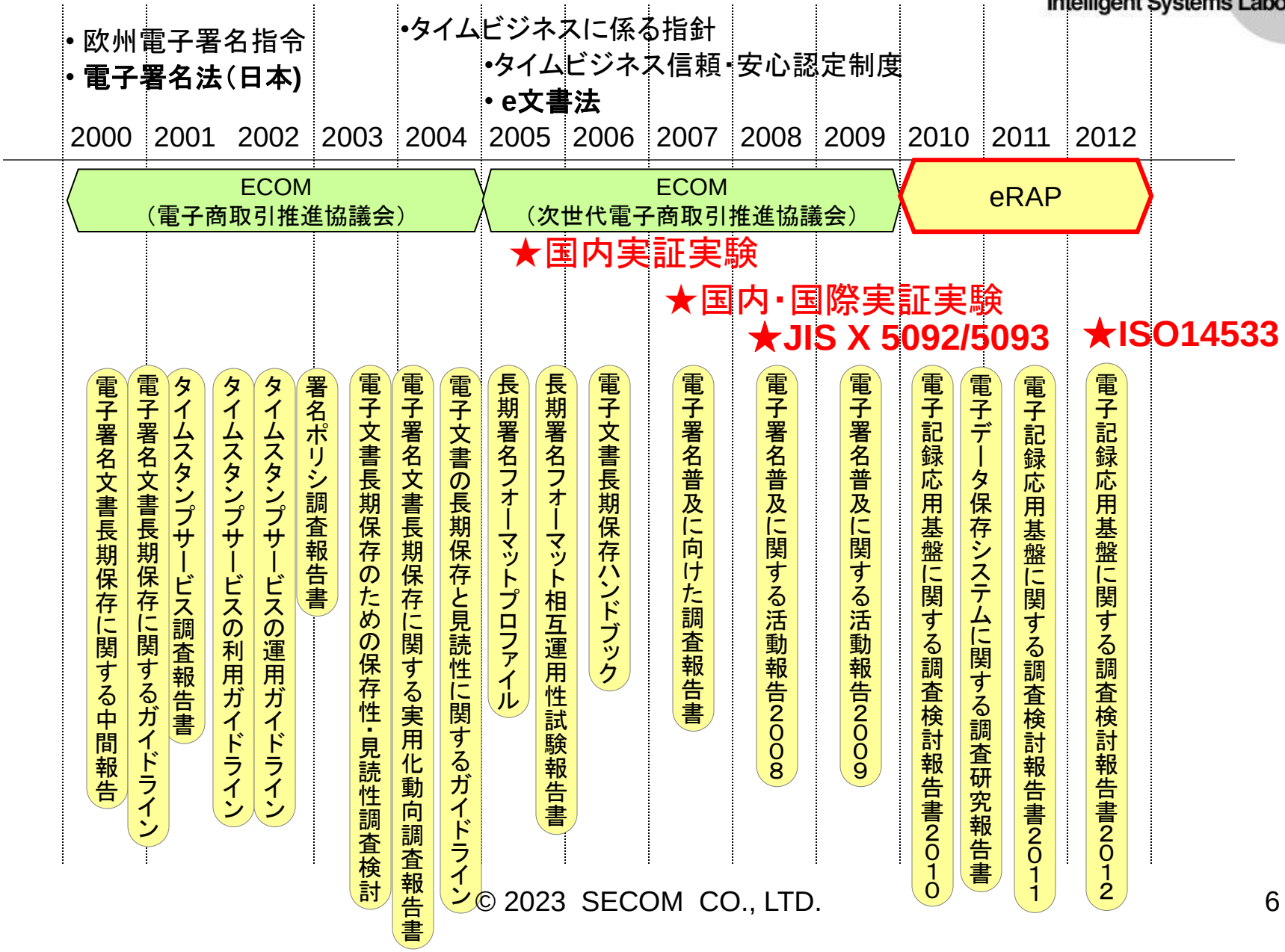
電子署名で担保する場合

- 電子データのみで検証可能。
- オープンな標準規格。
  - システムやサービスに依存しない。
  - 相互運用可能なデータフォーマット。
  - 第三者的に検証が可能である。

システムに依存しない仕組みを構築するためには相互運用性の確保が重要！

電子署名に関する主な成果

セコムIS研究所
Intelligent Systems Laboratory



eRAP成果報告会

電子署名に関する主な成果

セコムIS研究所
Intelligent Systems Laboratory

- 欧州電子署名指令
- **電子署名法(日本)**
- タイムビジネスに係る指針
- タイムビジネス信頼・安心認定制度
- **e文書法**

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012

ECOM（電子商取引推進協議会）

ECOM（次世代電子商取引推進協議会）

eRAP

★国内実証実験

★国内・国際実証実験

★JIS X 5092/5093 ★ISO14533

調査研究の時代（2000-2004頃)
・紙から電子への期待
・電子署名法
【主な成果】
・署名/タイムスタンプ調査
・長期保存ガイドライン

事業立ち上がりの時代（2004-2008頃)
・e文書法
・タイムスタンプ事業、署名製品市場の活性化
【主な成果】
・電子署名実証実験
・ECOMプロファイル

実用化の時代（2008～)
・電子保存の広がり
【主な成果】
・欧州との実証実験
・JIS規格策定
JIS X 5092/5093
・ISO規格策定
ISO 14533 Part1/Part2

電子署名普及に関
電子記録応用基盤
電子データ保存シ
電子記録応用基盤
電子記録応用基盤
に関する中間報告
に関するガイドライン
調査報告書
の利用ガイドライン
の運用ガイドライン
めの保存性・見読性調査検討
に関する実用化動向調査報告書
に関するガイドライン
ル
性試験報告書
告書

電子署名の規格

セコムIS研究所
Intelligent Systems Laboratory

CAdES
(CMS Advanced Electronic Signature)

バイナリデータ形式(ASN.1)のフォーマット

関連する代表的な規格

- ETSI TS 101 733
- RFC 5126 (IETF)

XAdES
(XML Advanced Electronic Signature)

XML形式のフォーマット

関連する代表的な規格

- ETSI TS 101 903

PAdES
(PDF Advanced Electronic Signature)

PDF形式のフォーマット

関連する代表的な規格

- ETSI TS 102 778
- ISO 32000-2(ドラフト)

ECOM/eRAPが原案作成

- JIS X 5092:2008
- ISO 14533-1
- JIS X 5093:2008
- ISO 14533-2

相互運用性を確保した
長期保存のためのプロファイル

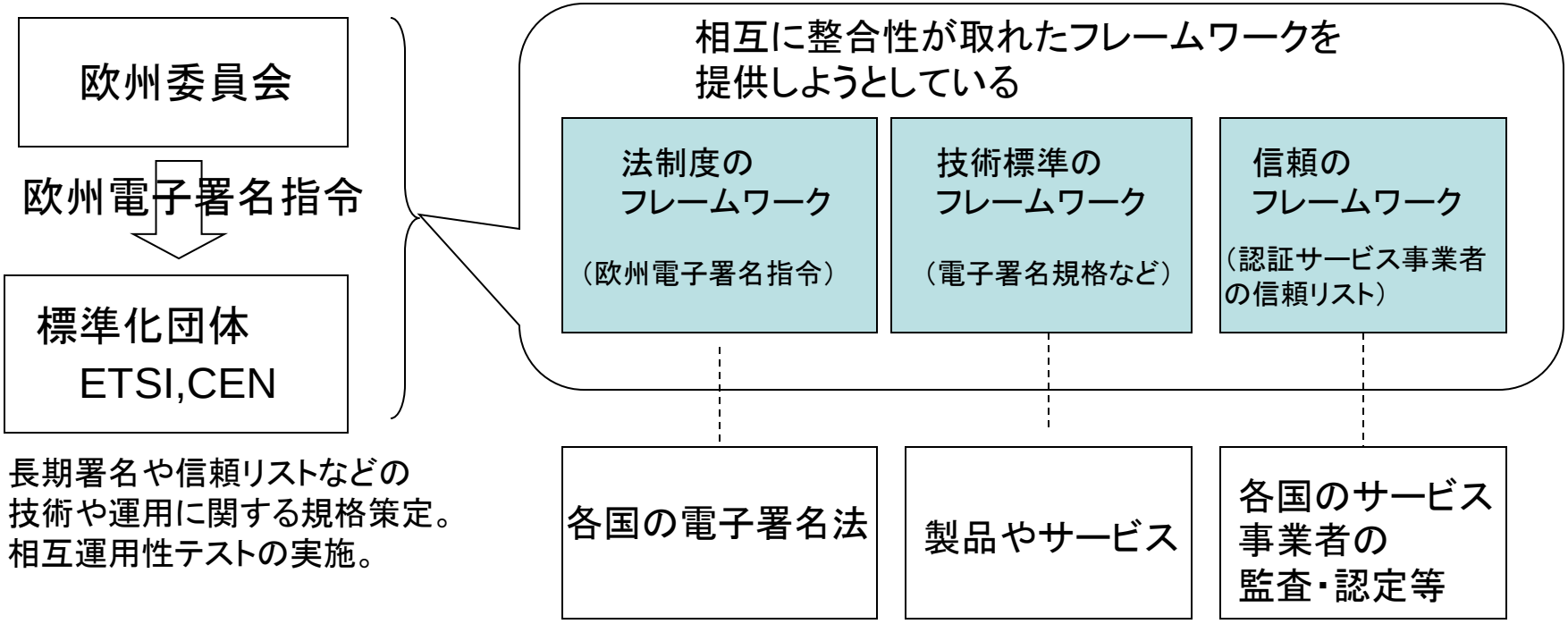
セコムIS研究所
Intelligent Systems Laboratory

ETSI（欧州電気通信標準化機構）との関係

- 実証実験や規格策定においてETSI ESI (technical committee Electronic Signatures and Infrastructures)のメンバーと協力関係を築いてきた。
- ETSIでは初となるインターネット経由による非対面の実証実験(リモートプラグテスト）を提案。現在も実施されているETSIプラグテストはECOM実証実験がモデルになっている。
- ETSI規格の問題点を指摘し修正。
- PDF規格における長期署名の問題を指摘し、後のPAdES規格策定の動きへとつながった。

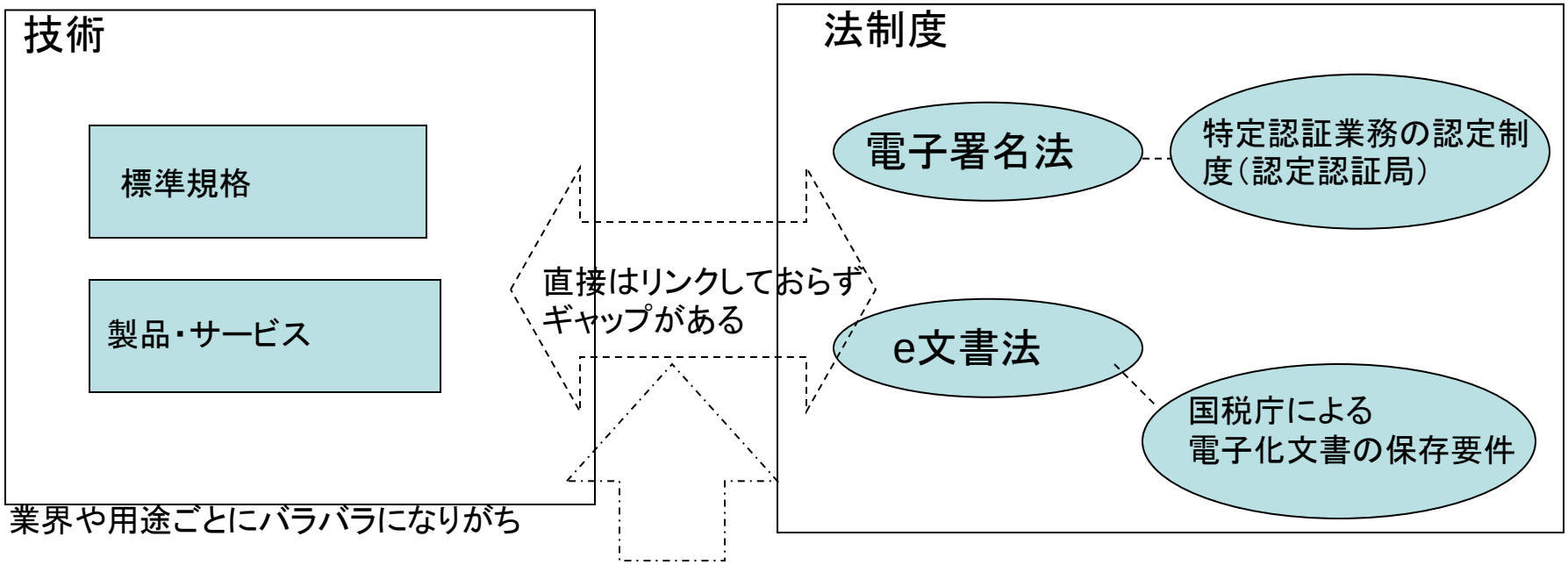
欧州の電子署名の体系

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。
制度と技術が相互に結びついている。



セコムIS研究所
Intelligent Systems Laboratory

日本の電子署名のイメージ



信頼構築のための枠組みは無い…

電子署名の動向

電子署名の分野は終わったわけではありません！
欧州でも電子署名の分野は常に変化しています。

- 新たな署名形式
  - PAdES (PDF Advanced Electronic Signature)
  - ASiC (Associated Signature Container)
- 署名のプロファイル規定
  - ETSIベースラインプロファイル
    EU指令に基づくプロファイル規定。このプロファイルに合わせてベース規格であるCAdESも改訂された。
- 電子署名の検証手順
  - 電子署名の検証手順の詳細を規定。ETSIベースラインプロファイルをベースにしているため、日本（やその他の国）には適合しにくい問題がある。
- 既存のベース規格の改訂
- 信頼構築のためのフレームワーク
  - Trust Service status List(TSL)
    信頼できるサービス事業者（認証局など）のリスト

電子署名の欧州規格は国際的な影響力をもつ一方で、
欧州向けの仕様が入り込む可能性もある。
黙っていると日本国内で適用しにくい規格に変貌してしまう恐れもある。

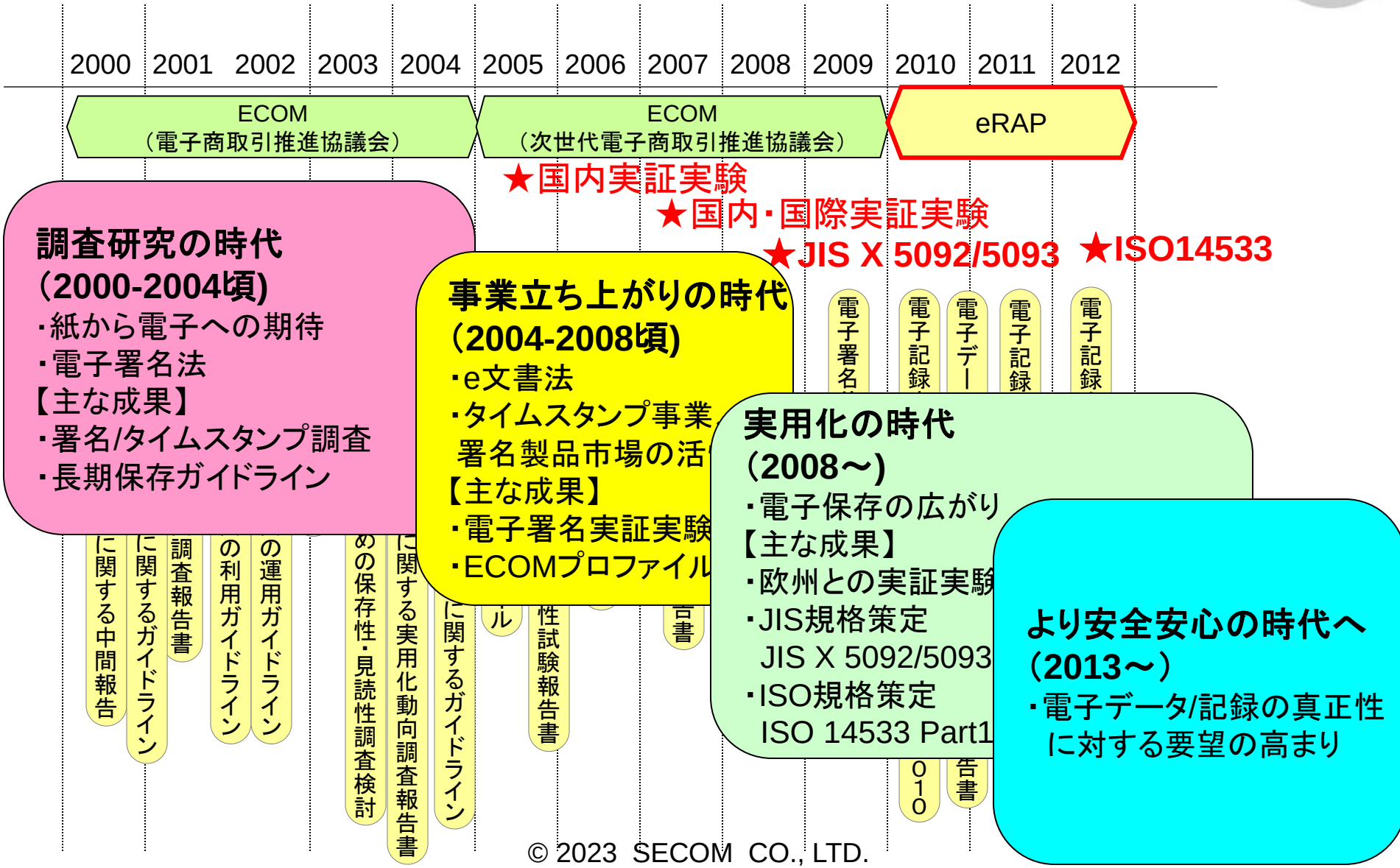
セコムIS研究所
Intelligent Systems Laboratory

電子署名の課題

- 長期保管も可能な電子署名は相互運用性を確保していくことが特に重要な分野である。
  - 新しい規格や規格改訂には注意が必要である。
  - 規格改訂の提案や補完する規格の策定を行う必要もある。
  - 現状では主に以下の課題が明らかになっている。
    - CAdES改訂による相互運用性の影響を把握すること（JIS規格などへの影響）。
    - PAdESの相互運用性を確保するためのプロファイル規格の策定が必要。
    - 日本の電子署名でも適用可能な電子署名の検証手順の提案が必要。
- 日本においても信頼構築のための仕組みを検討する必要がある。
  - 現状は信頼モデルが混沌としつつあるように思われる。
  - 日本版トラストサービスリストが必要か？
  - 信頼点となる証明書の長期保管や、廃業する認証局等の移管などの検討も必要。
- などなど

電子署名に関する主な成果

セコムIS研究所
Intelligent Systems Laboratory



セコムIS研究所
Intelligent Systems Laboratory

電子署名に関する今後の活動

- 電子記録応用基盤研究会
  - 記録管理における電子署名の応用を検討。
- 今後の電子署名技術に関する調査研究は JNSA（日本ネットワークセキュリティ協会）にて
  - JNSA 電子署名WG（仮称）
  - 近日、キックオフミーティング開催
  - ご興味のある方ぜひご参加ください！

セコムIS研究所
Intelligent Systems Laboratory

ご清聴ありがとうございました