セコムIS研究所
Intelligent Systems Laboratory

パネルディスカッションのお題目
PKIの過去、現在、未来

2007 年 6月25日

セコム株式会社 IS研究所

松本　泰

PKI day 2007パネルディスカッション
PKIの過去、現在、未来

セコムIS研究所
Intelligent Systems Laboratory

- IT技術、ネットワーク技術が深く社会に浸透し行くなか、IT社会、ネットワーク社会における信頼関係を確立するための基盤が求められています。
- PKIは、こうしたことに対応する技術ですが、広くIT社会の基盤となるためには、まだ、多くの課題があります。「広くIT社会の基盤」の課題の解決のたには、組織や業界を超えて、PKI技術や相互運用に関する共通の課題などを共有する必要があるのではないでしょうか。
- PKI day 2007では、PKIの過去から現在までの状況、標準化などの最新状況などを踏まえた上で、共通課題の認識とその解決策、そして将来の方向性を議論します。

パネルディスカッション
PKIの過去、現在、未来

- パネリスト
  - 日本電気株式会社　　小松 文子 氏
  - 富士ゼロックス株式会社　稲田　龍 氏
  - 東京大学　　佐藤 周行 氏
  - セコム株式会社IS研究所　松本　泰

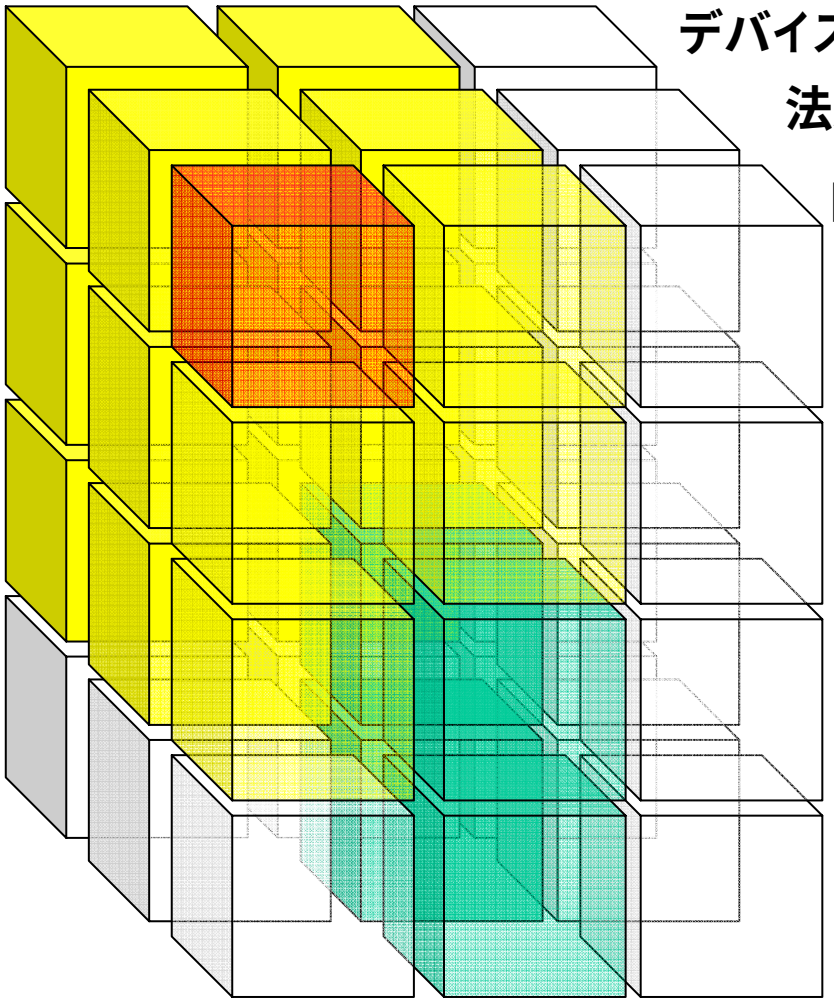
セコムIS研究所
Intelligent Systems Laboratory

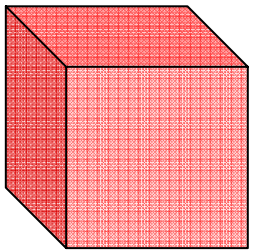
パネルディスカッションのお題目

- 電子署名法の功罪
- PKIが利用されるべき領域
- 複雑さの克服

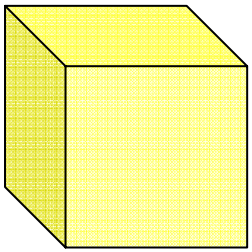
松本キューブ？

セコムIS研究所
Intelligent Systems Laboratory

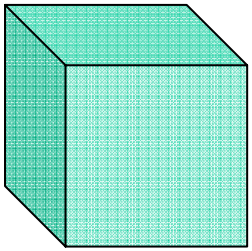




電子署名法の
カバー範囲



基準などを
整備すべき領域

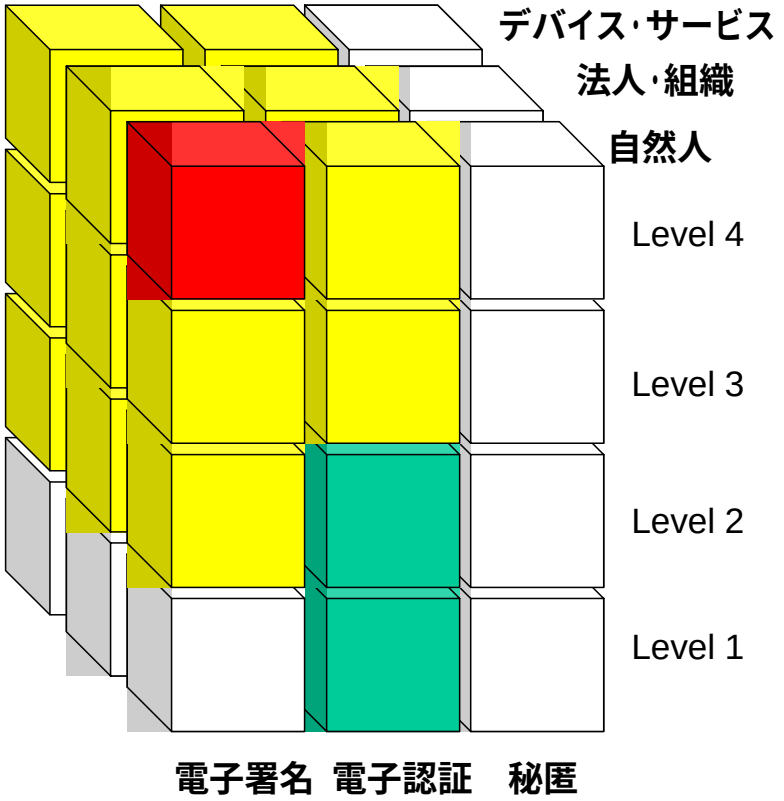


電子署名　電子認証　　秘匿

電子署名法の功罪

セコムIS研究所
Intelligent Systems Laboratory

- 「電子署名法」は、リスクを許容しない非常に厳しい基準を課している。そのため、電子署名法の認定基準自体は、世の中で署名が使われるべき全ての領域に対してベストプラクティスを提供している訳ではない。
- 現状の電子署名法のカバーしている領域は、非常にニッチであり、このニッチな電子署名法の各種の厳しい基準が、電子署名は使いにくい、高価、運用が難しいというイメージを与えている面がある。
- 電子署名法にある「誤認防止」の弊害
  - 様々な信頼モデルを構築できない。



IT社会に追従できない
IT技術に関連した法制度

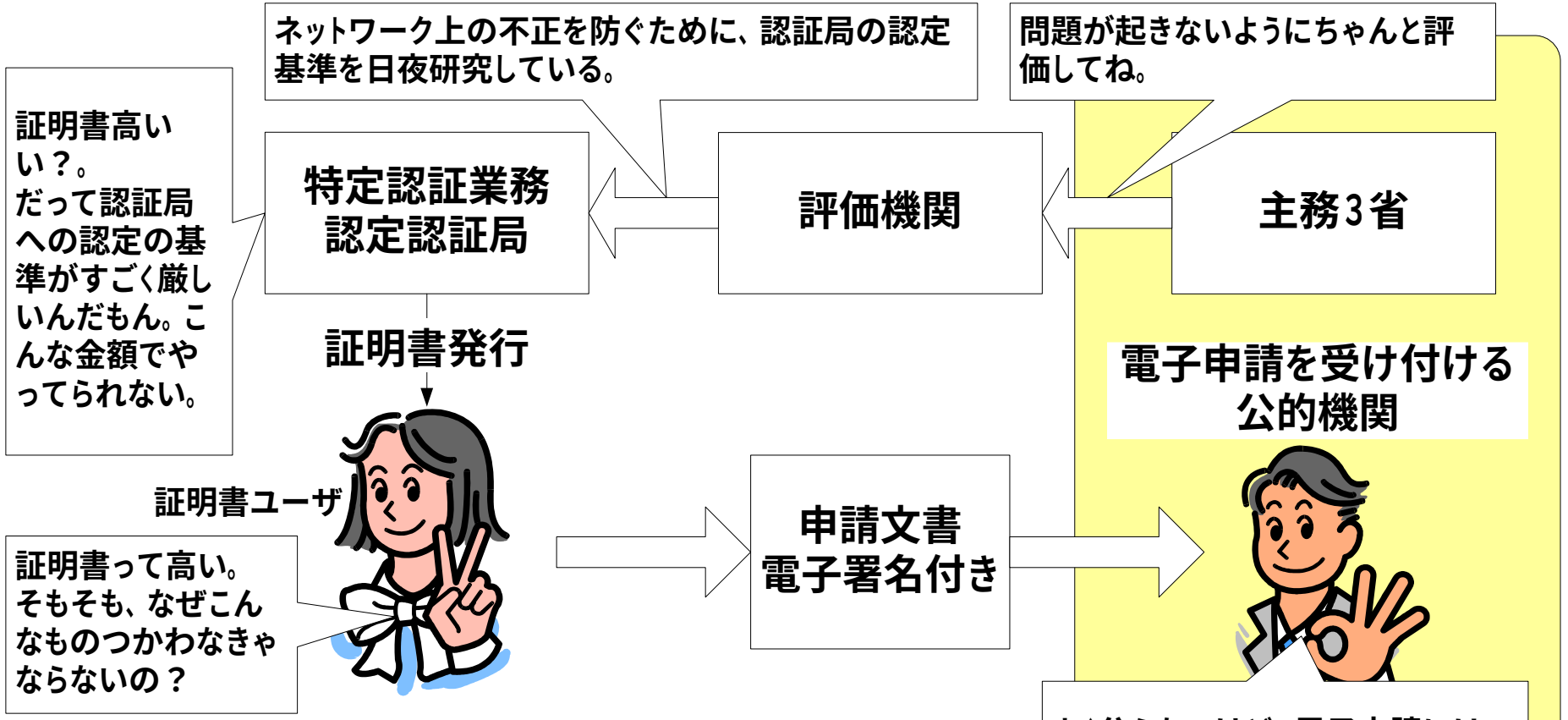
セコム IS 研究所
Intelligent Systems Laboratory

- 強制力が働く法制度　->　「官民」とも過剰に反応する
  - 個人情報保護法、SOX法関係など。。。
  - 「コンプライアンスがセキュリティ技術者をダメにするかも??」系典型的な法制度
- してもよい系の法制度　ー>　まったく効力を発揮しない
  - 「してもよい」に対して「官」過剰に反応して省令などで、高い敷居を設けてしまう。結果、機能しない。。。。
  - 電子署名法
    - 技術の不理解からのくる様々な制約等
  - e文書法
    - スキャン文書　　領収書は3万円以下まで
- 「強制力が働く法律」「してもよい系の法律」双方ともベストプラクティスでないセキュリティを生み出してしまっている。

IT社会に追従できないIT技術に関連した法制度

電子署名法改正の議論　非常に認定基準が厳しい　- 結果、高コスト

セコム IS 研究所
Intelligent Systems Laboratory

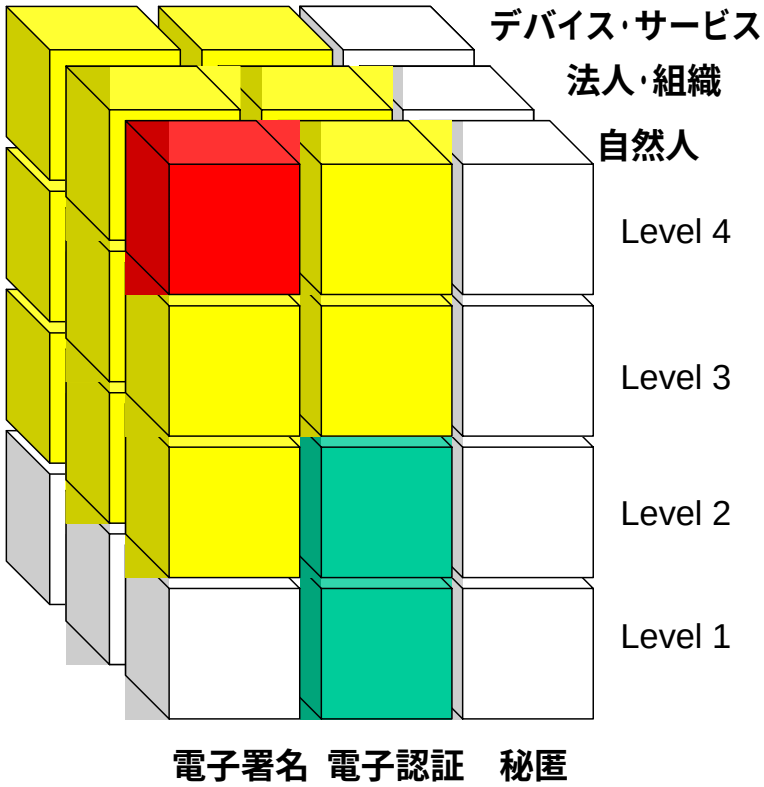


- ***セキュリティとコストがバランスする構造になってない***
- ***セキュリティ基準が高くてうれしいのは、本来電子申請を受け付ける府省などであるはず。ところが、府省からは料金を徴収できない。***

**公的個人認証サービスは、証明書検証者からお金を取ってる！！

PKIが利用されるべき領域

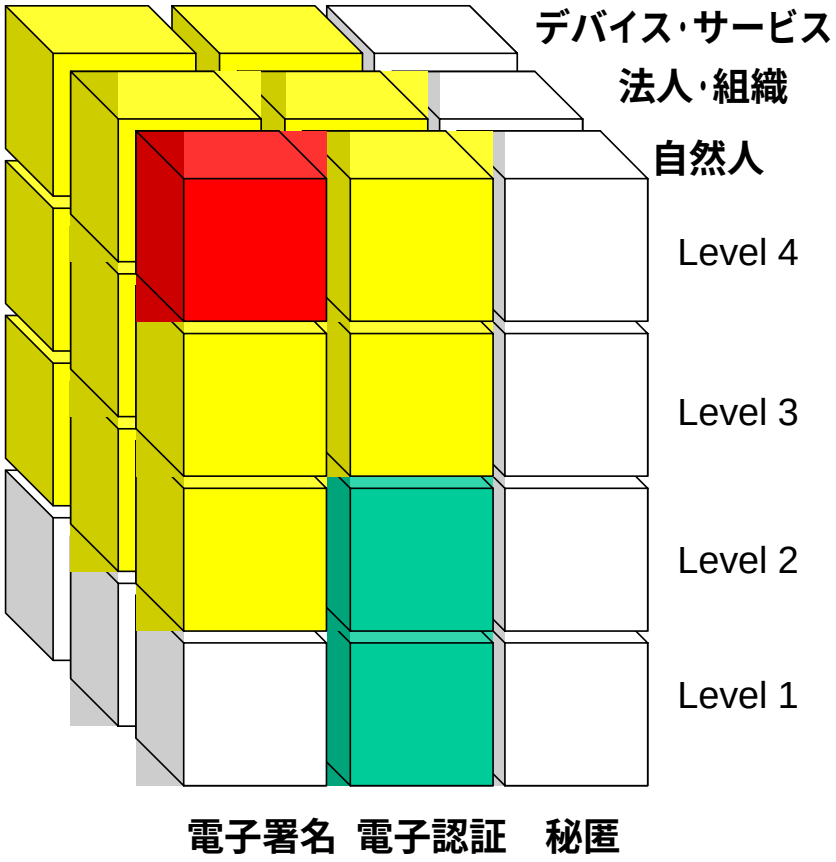
- PKIの適応されるべき領域は、現状のニッチな電子署名法の領域よりもはるかに広い。
- 様々な証明書
  - デバイス証明書、リソース証明書、etc….
- Levels of Assurance
  - Lightweight PKI の重要性
  - Lightweightであっても基準が必要
    - #電子署名法の (認定でない) 特定認証業務は、これ (基準) がない。。。。



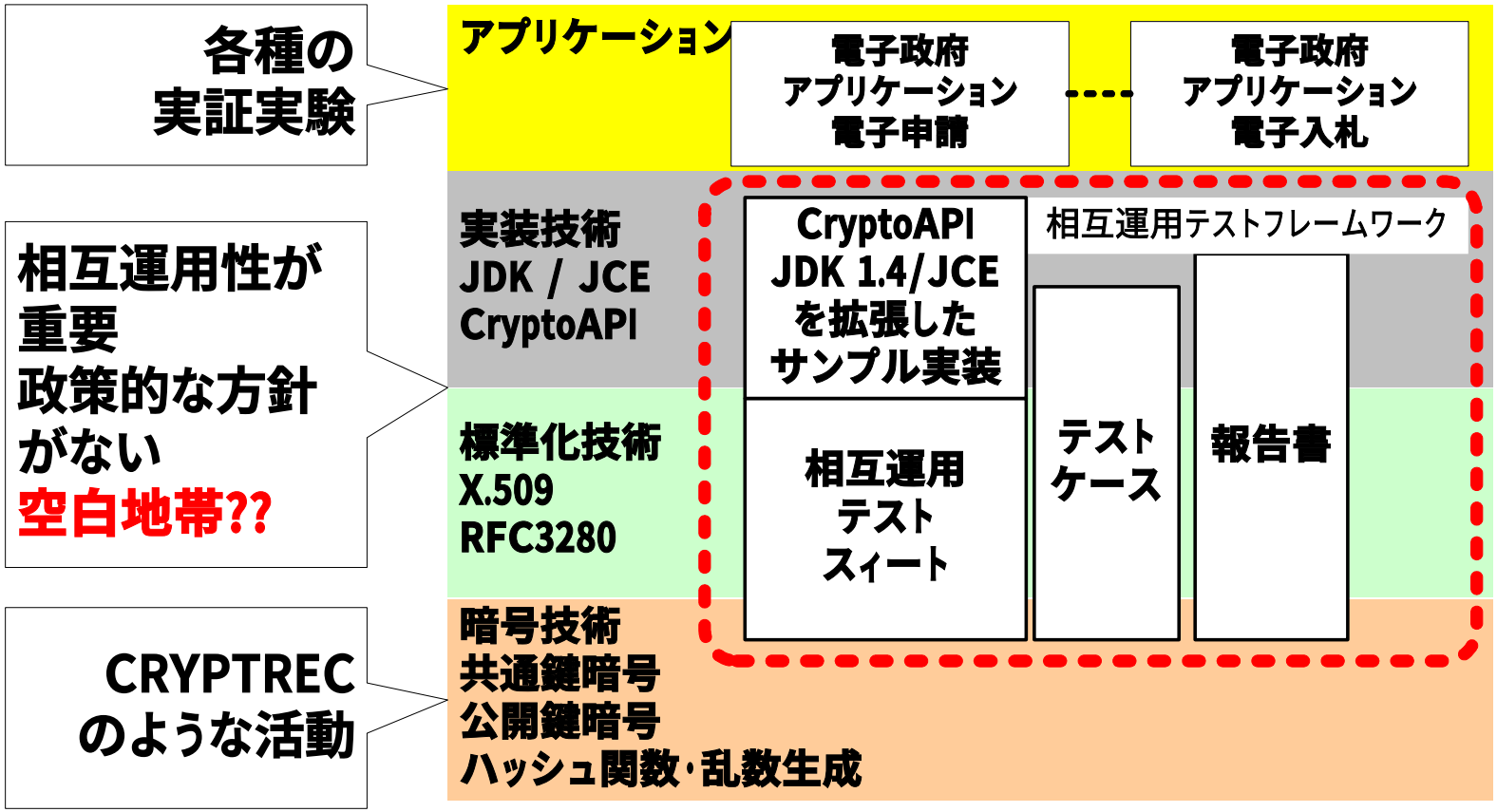
複雑さの克服

セコムIS研究所
Intelligent Systems Laboratory

- 複雑さ（技術だけでなく、運用、マネージメント、さらに制度との関係）を克服できていない。
- 複合技術としてのPKIの困難さ、基盤として様々なステークホルダーが関与することに起因する困難さ。。。
- この大きな課題の解決には、要素技術におけるブレークスルーとはまったく異なる、複合技術の複雑さの課題をブレークするためのアプローチの確立が必要??



複雑さの克服
Challenge PKIプロジェクトの活動
プロジェクトの目標と課題 – *Challenge PKI 2002*



複雑さを隠蔽するためどんどん階層化されていく。。
このことが、問題の本質を分かり辛くしている！！

複雑さの克服
Challenge PKIプロジェクトの活動
セキュリティフレームワークやミドルウェア重要性 *Challenge PKI 2003*

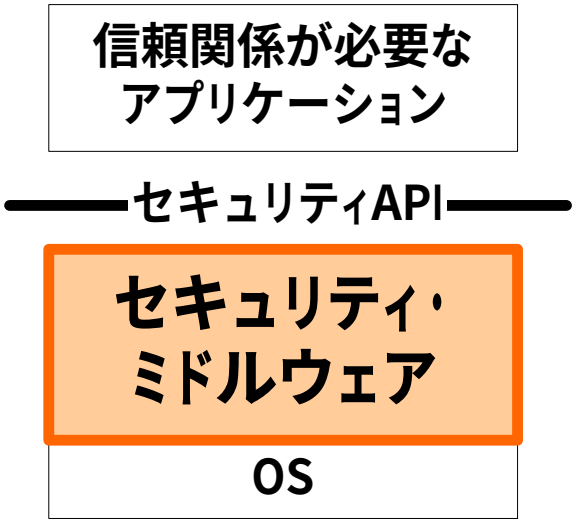
セコム IS 研究所
Intelligent Systems Laboratory

標準化、相互運用の課題

非常に複雑なセキュリティプロトコルの要求

セキュリティに対応し切れていない標準化＆標準化組織

テスト環境、テストケース、相互運用テストが非常に重要だが、整備ができていない



実装上の課題

暗号技術等、基礎技術が、セキュリティ・フレームワーク＆ミドルウェアに組み込まれていかない
（日本の話し。。。。）

多くのバグが内在する可能性
(OpenSSLなどは典型的)

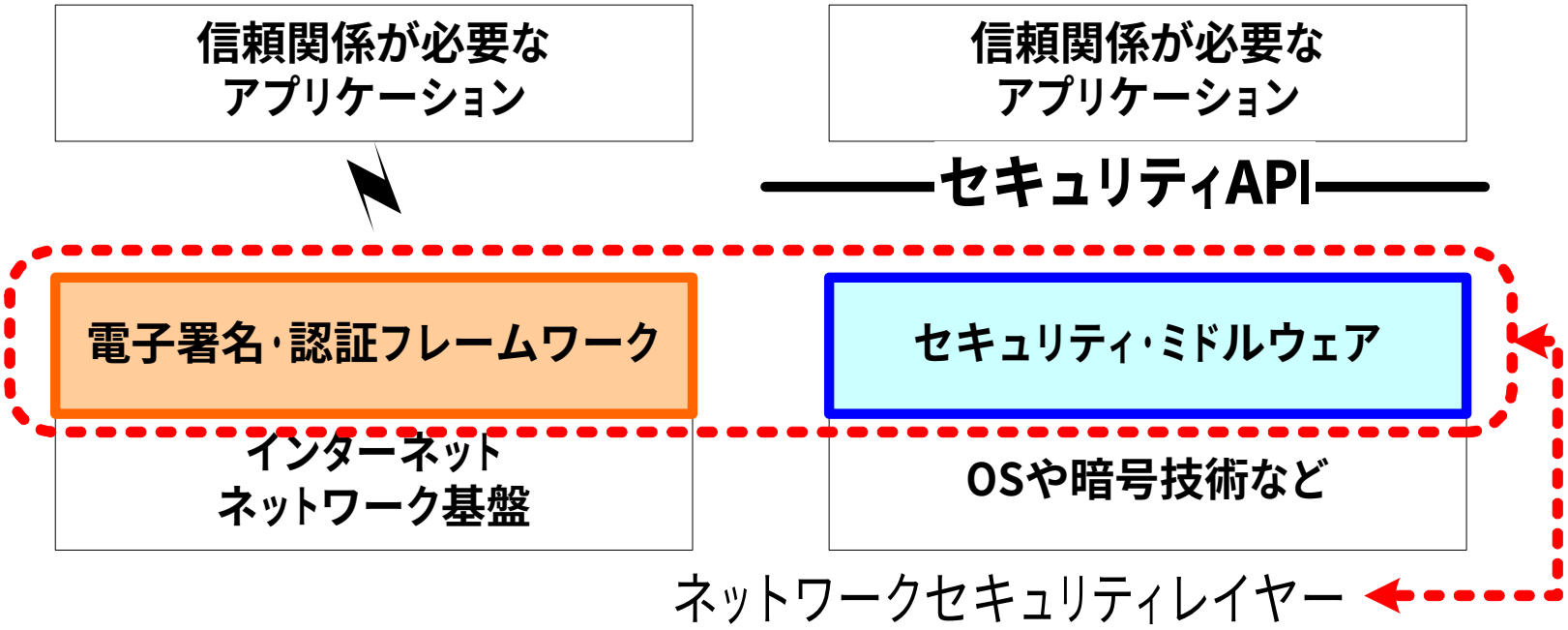
標準と実装のギャップ。何がどこまで正しく実装されているのか分からない。

複雑さを隠蔽するために、どんどん階層化されていく。そのことにより本質的な問題点も隠蔽されていく??

複雑さと問題点が集約されていく

複雑さの克服
Challenge PKIプロジェクトの活動

セキュリティフレームワークやミドルウェア重要性 *Challenge PKI 2003*



- 何処でも、何時でも、誰にでもつながるユビキタスネットワークにおいて信頼の拠りどころが求められる。。。。
- ネットワーク上の信頼を実現するセキュリティ・レイヤーの必然性
  - これらは、古典的なOSI参照モデルなどでは説明がつかない。。。

複雑さの克服
IC・ID カードの相互運用可能性の向上に係る基礎調査
IC・IDカードに限らず課題と思うこと。。。。

セコム IS 研究所
Intelligent Systems Laboratory

- 情報セキュリティ技術、特に情報セキュリティに関連した（相互運用）技術は、進歩しておらず停滞している。
- 情報セキュリティへの関心が高まるほどに、逆に情報セキュリティに関連する相互運用の問題の解決へのインセンティブは下がっている。
  - 情報の非公開、囲い込みなど、相互運用性を確保とは反対の方向へ向かっている。
- 複雑さ（技術だけでなく、運用、マネージメント、さらに制度との関係）を克服できていない。
- #放って置くと、技術の形骸化を生む。既に、優秀な技術者が情報セキュリティ分野から逃げ出しているように感じられる。
- 結果。。 PKI相互運用技術WG。。終われない。。