セコムIS研究所
Intelligent Systems Laboratory

PKI の展開と最新技術動向

セコム株式会社 IS研究所/
JNSA PKI相互運用技術WGリーダー
松本　泰

2006 年 6月 7日

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

PKI の展開と最新技術動向

セコム IS 研究所
Intelligent Systems Laboratory

- PKIは、情報社会の様々なインフラとなるべき技術ですが、その技術は非常に幅広く、また、奥深いものがあります。
- 今回は、医療PKI、学術系PKI、全世界的な連携が検討されているGridコンピュータのPKIなど、今後展開が期待されている分野の紹介を中心に、PKIの標準化とその実装に非常に影響力の大きい、オープンソースのPKIの実装とマイクロソフトのPKIなど、今後の動向を占う意味で重要な最新の情報をお届けします。

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

PKIの展開と最新技術動向

セコム IS 研究所
Intelligent Systems Laboratory

- 「PKI の展開と最新技術動向」
  - セコム株式会社 IS研究所／PKI相互運用技術WGリーダー　松本 泰
- 「わが国の保健医療福祉分野PKIの動向」
  - 東京大学大学院 情報学環・学際情報学府　山本 隆一 氏
- 「大学間連携のための全国共同電子認証基盤UPKI構想と米国学術PKIの動向」
  - 国立情報学研究所　島岡 政基 氏
- 「グリッドにおけるセキュリティの概要と動向」
  - 産業技術総合研究所　田中 良夫 氏
- 「長期署名フォーマットとECOMにおける相互運用実証実験について」
  - ＥＣＯＭ長期署名保存フォーマット普及SWGリーダ
  - 三菱電機株式会社　情報技術総合研究所　チームリーダ　宮崎 一哉 氏
- 「標準はどうのように実装されているのか？-- OpenSSLにおけるSSL/TLSの実装に関して」
  - 富士ゼロックス株式会社　稲田 龍 氏
- 「Windows VistaのPKIとIE7」
  - マイクロソフト株式会社　渡辺 清 氏

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

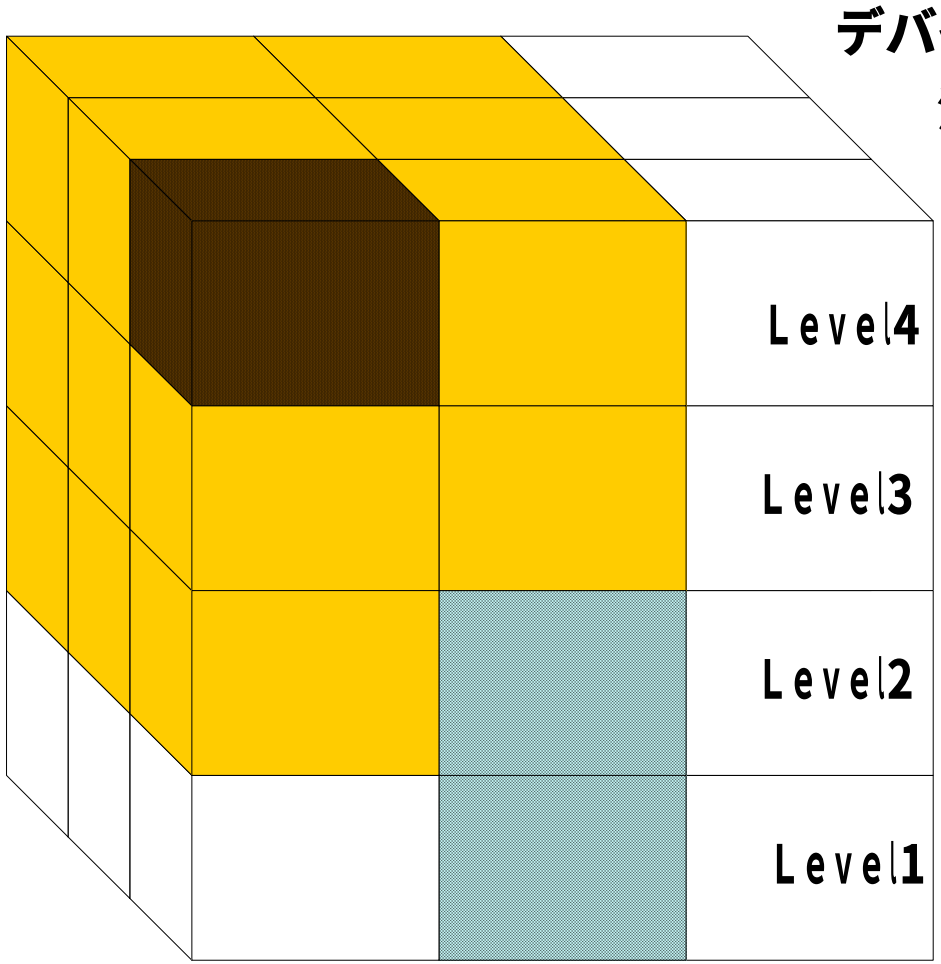
PKI の展開と最新技術動向

- NPO JNSAのChallenge PKIプロジェクトの活動
- 電子署名法の改正の議論
- 電子署名の展開
- 組織を超えた連携のための基盤
- #PKI相互運用技術からみたSHA-1問題(おまけ)

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

PKI の展開と最新技術動向
松本キューブ？？？（PKIが適用されるべき領域）

セコム IS 研究所
Intelligent Systems Laboratory



Copyright © 2006 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

NPO JNSAの Challenge PKIプロジェクトの活動

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

Challenge PKIプロジェクトの活動
プロジェクトの目標と課題

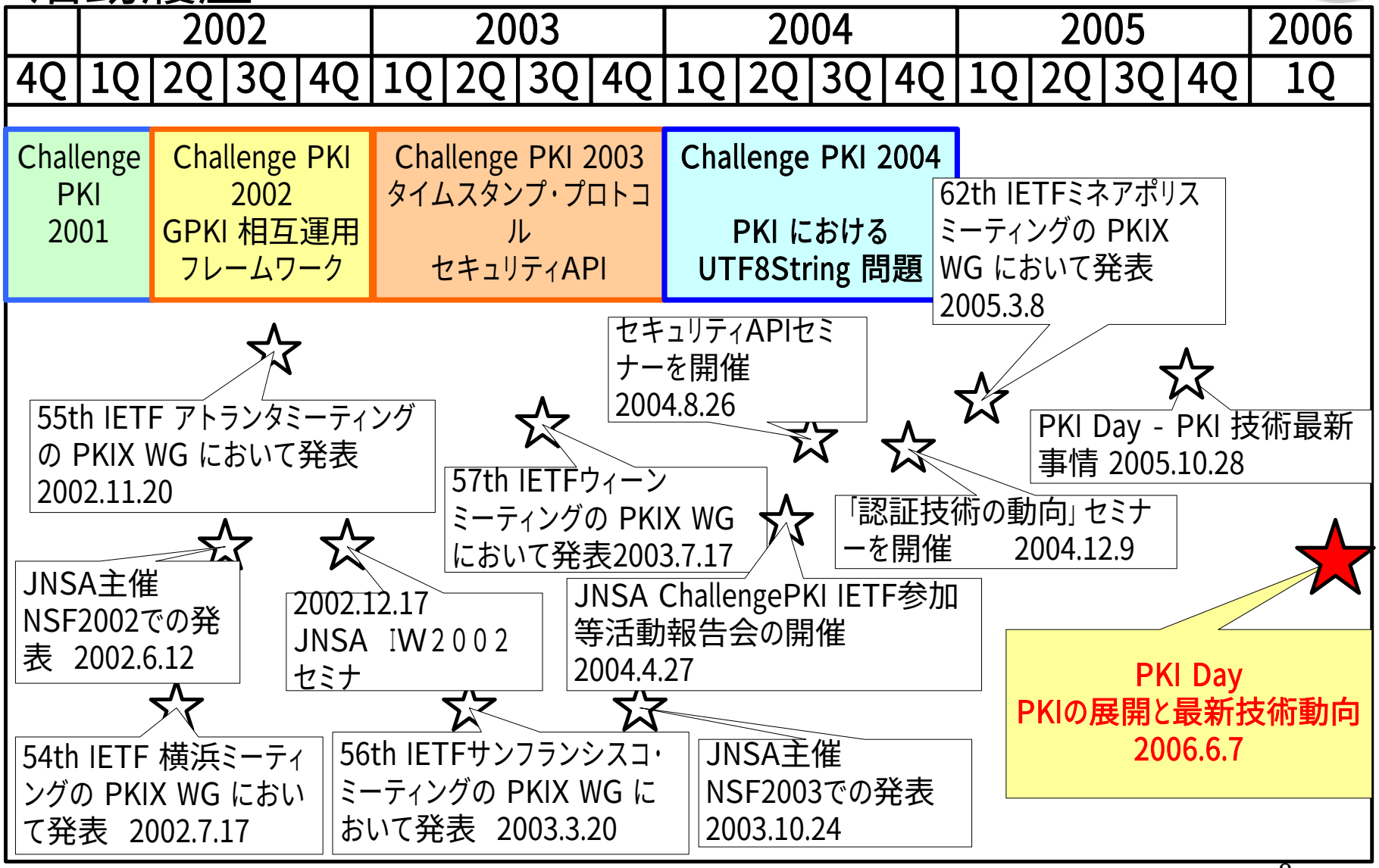
セコム IS 研究所
Intelligent Systems Laboratory

- プロジェクトの今後の目標
  - 実際に幅広く展開可能なセキュリティインフラの構築(= 幅広く相互運用可能なPKIの展開)
- 標準化の課題 (標準・実装から展開)
  - アイディアから仕様へ　　-> 多くの研究者が行っている
  - 仕様から標準、標準から実装　-> 学術系＆ベンダーなど
  - 標準・実装から展開 (相互運用)　-> 誰が担うか
    - 標準と呼ばれる文書は山のようにある。しかし相互運用可能なものは極わずか…. これを解決して行かなければならない。
    - -> ベストプラクティスが重要。。。。ここに注力する。
- セキュリティフレームワークやミドルウェア重要性
  - 実際のアプリケーションにおいて、セキュリティ・ミドルウェアが、実行時のネットワーク上の信頼と複雑な相互運用の問題を吸収する

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

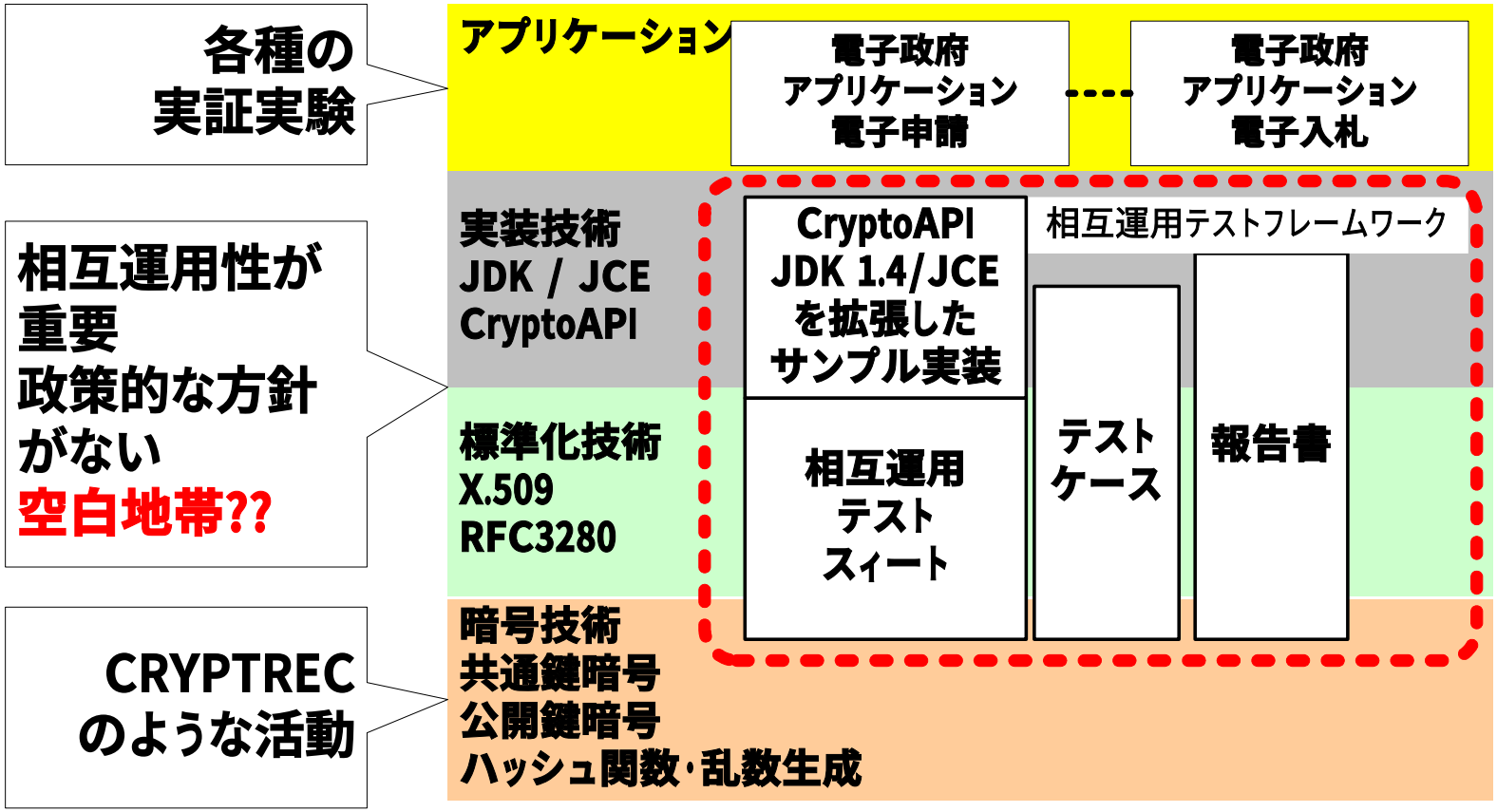
Challenge PKIプロジェクトの活動
活動履歴

セコム IS 研究所
Intelligent Systems Laboratory



Copyright © 2006 SECOM Co., Ltd. All rights reserved.

Challenge PKIプロジェクトの活動
プロジェクトの目標と課題(2) – *Challenge PKI 2002*



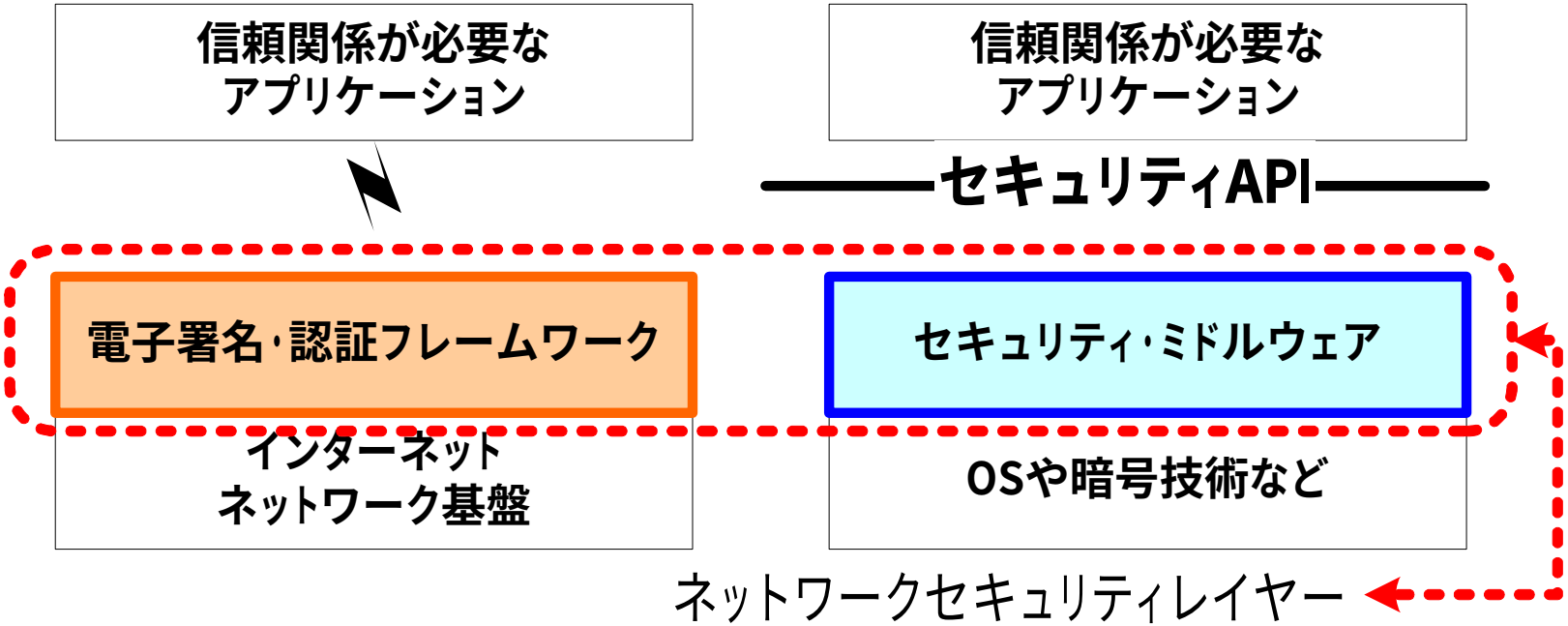
複雑さを隠蔽するためどんどん階層化されていく。。
このことが、問題の本質を分かり辛くしている！！
「PKI相互運用技術からみたSHA-1問題」も同様！！

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

Challenge PKIプロジェクトの活動

セコムIS研究所 Intelligent Systems Laboratory

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。。。

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

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*

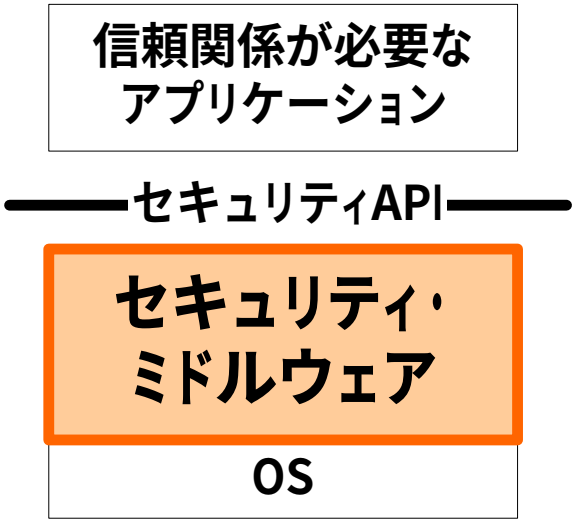
セコム IS 研究所
Intelligent Systems Laboratory

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

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

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

セコムIS研究所
Intelligent Systems Laboratory

- 【講演】「標準はどうのように実装されているのか？」
  - 「OpenSSLにおけるSSL/TLSの実装に関して」
  - 富士ゼロックス株式会社　稲田 龍 氏
- 【講演】「Windows VistaのPKIとIE7」
  - マイクロソフト株式会社　渡辺 清 氏

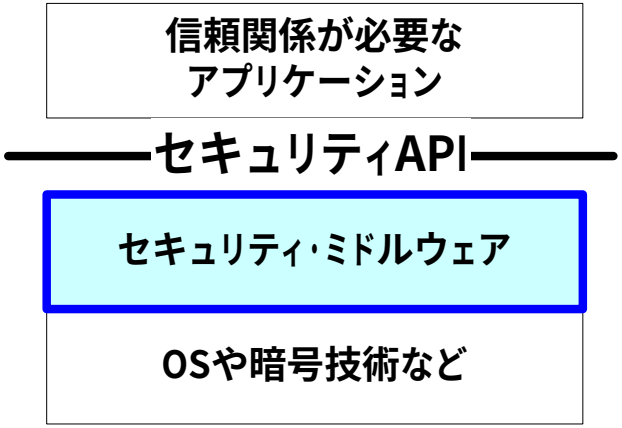
Copyright © 2006 SECOM Co., Ltd. All rights reserved.

Challenge PKIプロジェクトの活動
セキュアジャパン2006

セコムIS研究所
Intelligent Systems Laboratory

- イ) 政府機関における安全な暗号利用の推進体制等の検討（内閣官房、総務省及び経済産業省）
  - 電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進めるとともに、電子政府推奨暗号のあり方の見直し等を含めた暗号利用に関する政府内の推進体制について、２００６年度に検討を開始する。
- b) 高セキュリティ機能を実現する次世代ＯＳ環境の開発（内閣官房、内閣府、総務省及び経済産業省）
  - ２００６年度において、ＩＴの信頼性確保のための喫緊な取組みとして、ＯＳにおいてアプリケーションに依存しない形でセキュリティを確保し、かつ、電子政府で直近に求められる基盤機能に絞り込んだ技術基盤の開発を推進する。

ありがたいことに「セキュアジャパン2006」では、セキュリティプロトコルなどの標準化やセキュリティ・ミドルウェアの実装などに関連した相互運用性に関しての記述は全くなく、政策的な方針がない空白地帯は継続しそうなので、我々の活動の意義はまだありそうです。



Copyright © 2006 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

電子署名法の改正の議論

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

電子署名法の改正の議論
電子署名法 -「電子署名及び認証業務に関する法律」

セコム IS 研究所
Intelligent Systems Laboratory

- 正式名称
  - 「電子署名及び認証業務に関する法律」
- 主な内容
  - 電磁的記録の真正な成立の推定
  - 認証業務に関する任意的認定制度の導入
    - 「特定認証業務」の認定 – 2006年5月時点で19件の認定
- 対象
  - **自然人**の電子署名が対象
- 対象外
  - 法人、サーバ、エージェント。。。。の署名
  - PKIの機能である電子認証(Authentication)や暗号。。
- 電子署名法の施行　2001年4月1日に施行　（来年で5年)
  - 政府は、この法律の**施行後五年**を経過した場合において、この**法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずる**ものとする」(附 則　第三条)
    - ###5年前、当初目指していた社会との齟齬はたくさんあるはず。

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

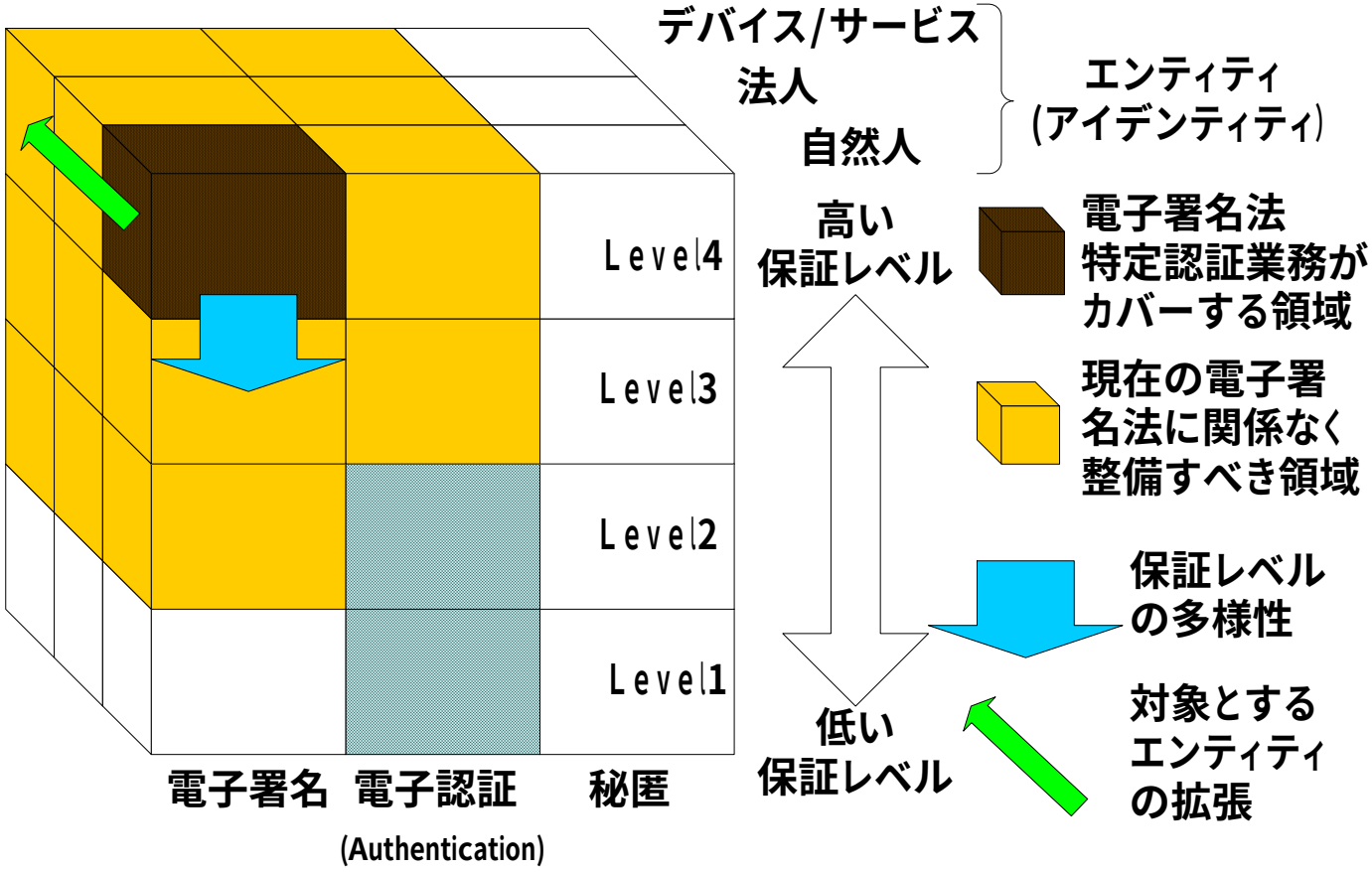
電子署名法の改正の議論
主な論点

セコムIS研究所
Intelligent Systems Laboratory

- 総論としての意見
  - **普及の観点**が必要(現在の電子署名法は完璧を求めすぎていないか？)
  - #「民事訴訟法の推定項」が「働く」「働かない」の0/1の議論
  - #リスクを許容しない完璧が求められている?? -> 2001年の施行という施行の時期にも関係している？？
- **証明するエンティティ**
  - 自然人以外の法人、サービスなどを対象にすべきでないか？
- **証明のレベル**
  - 現在の「特定認証業務」の認定のレベルは高すぎないか？
  - #「高いレベルが必要ない」という議論はあまりない。別レベルが必要という議論
- 暗号の危殆化に関する対応
  - 現在の話題は、SHA-1問題 ->「PKI相互運用技術からみたSHA-1問題」
- その他(松本の私見)
  - そもそも5年毎の見直しは、「ドッグイヤー時代」にふさわしくない？
  - 「認定認証業務と他の業務との誤認を防止」が問題??
    - 結果、様々な信頼関係を築くことができない？（人とサービスとか）

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

電子署名法改正の議論
電子署名法の範囲の拡大??



- 「特定認証業務」の非常に厳しい認定基準は、電子署名のビジネス領域をニッチなものにしている。また、電子証明書はコストが高いものというイメージを植えつけている。こうしたことを解決するため保証レベル(Assurance level)の概念が導入されるべき？？

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

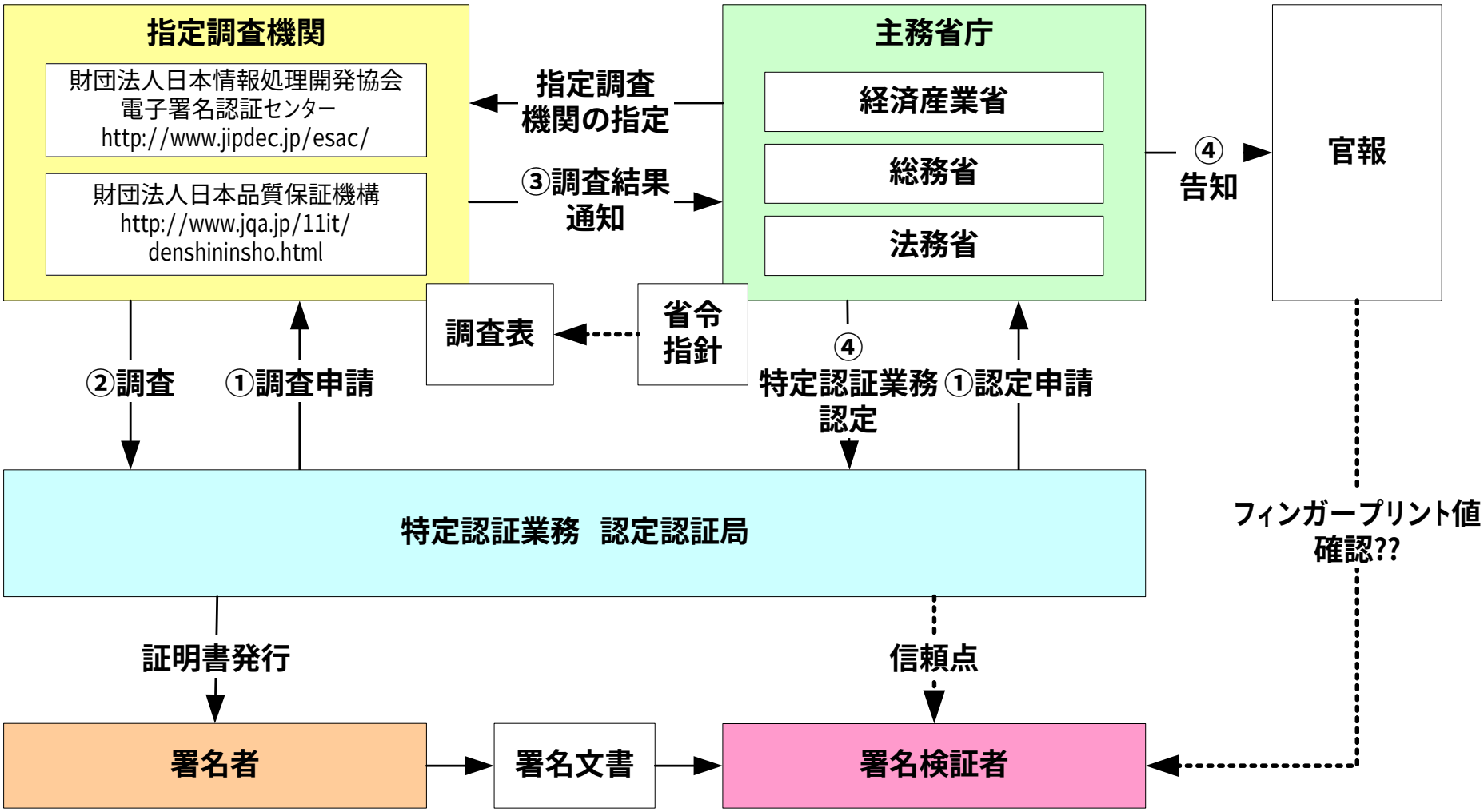
電子署名法改正の議論
電子署名法特定認証業務認定制度の問題

セコムIS研究所
Intelligent Systems Laboratory

- 「非常に**認定基準が厳しい**」
  - 結果、高コスト
  - 「認定基準が厳しい」ことは悪いことではない。問題は「認証事業者」以外がこのことを知らないこと。- ISO15408の状況に多少似ている（「開発者」以外..)
- 「非常に**制約が厳しい**」　#技術の不理解が融通の利かない制度を作っている??
  - 「認定認証業務と他の業務との誤認を防止」による制約と「自然人にしか証明書が発行できない」という制約
  - 結果、柔軟なPKIが構築できない
  - 「電子署名法」の範疇は、人と人の関係だけで、人とサービス、サービスとサービスの信頼関係を築けない。もしくは、人とサービス、サービスとサービスの信頼関係を分断しているかもしれな
- 民間における電子署名法特定認証業務認定認証局の問題
  - 「非常に認定基準が厳しい」+「非常に制約が厳しい」=民間におけるビジネスの創造を阻害している可能性がある。
  - 現実に**純粋に民間のサービス向け**の認証局は少ないし減少傾向にある。これは本来の制度の目的を満たしていない。また、普及しないのであれば「制度」自体の意味をなさない??

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

電子署名法改正の議論
電子署名法特定認証業務認定のスキーム



Copyright © 2006 SECOM Co., Ltd. All rights reserved.

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

ネットワーク上の不正を防ぐために、認証局の認定基準を日夜研究している。

問題が起きないようにちゃんと評価してね。

証明書高いい？。
だって認証局への認定の基準がすごく厳しいんだもん。こんな金額でやってられない。

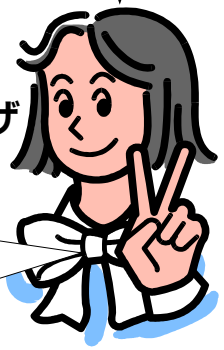
特定認証業務
認定認証局

評価機関

主務３省

証明書発行

電子申請を受け付ける公的機関



証明書ユーザ

証明書って高い。
そもそも、なぜこんなものつかわなきゃならないの？

申請文書
電子署名付き

よく分らないけど、電子申請には、電子署名が必要と言われている。
でも、オンライン利用促進、50%達成のため、電子署名を省略するかもしれない。。。。。

- ***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！！

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

電子署名の展開

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

電子署名の展開
電子認証(Auth.)と電子署名の違い

セコムIS研究所
Intelligent Systems Laboratory

	電子認証(Authentication)	(否認防止の) 電子署名(Signature)
手段	現状は色々な認証のメカニズムが乱立しておりユーザからは差が分らない (クライテリアが未整備)	電子署名はPKI以外の現実的な手段はない
法制度	現状、法制度との結び付きはなく、 認証の (保証) レベルもバラバラ	そもそも (電子でない) 署名も法制度と関係が深い。電子署名法、e文書法など法制度との結び付きが深い
マーケット	ネットワークを利用した様々なサービス。 今後のユビキタスネットワーク時代のユーザ認証、機器認証などの需要は測り知れない	紙に依存した比較的レガシーな業界に需要が多い。効率化するために電子化、IT化を推進したいが電子署名などの敷居の高さが壁になっている。
PKIの適用	SSL/TLS、IPsecVPN、802.1X..etc Lightweightから厳密な認証まで。	何らかの法的な強制力が働く領域。 e文書法対応、電子データ保存、電子契約。
普及の鍵	認証(Auth.)のベストプラクティスとしてのPKI	普及には業務知識、そして効率化のためのＢＰＲが伴うことを理解する必要がある。

電子署名は、法制度との関係が深く、署名文書は、長期の保存が必要な場合が多い。つまりLong-Term Security的な検討が必要。適応先はレガシでも技術は難しい。

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

電子署名の展開
なぜ医療情報分野での電子署名が重要か？

セコム IS 研究所
Intelligent Systems Laboratory

- 医療情報の電子化、ネットワーク化とセキュリティ基盤の整備の要求
  - IT化による医療情報の有効利用促進をはかり患者へのサービス向上
- セキュリティ基盤の整備の要求
  - 病診**連携**、病病**連携**など、連携、情報共有+「患者の視点」を行なうためには、セキュリティ基盤が重要　-> 単なるIT化ではない。
  - セキュリティ基盤のひとつに**医師による電子署名**を行うための**保健医療福祉分野PKI(HPKI)**がある
- 医療情報分野における電子署名の必然性
  - 医療は、様々な法制度に沿って行なわれており、医療で作成される文書には作成者・責任者の署名または記名・押印が求められるものが存在する。
    - 例えば、診療録、処方箋、放射線記録、紹介状。。。。
  - 医師という資格を持った人間が、その責任において文書に（電子）署名を施す。法令遵守などを示すためには、この**（電子）署名文書が保存**される必要がある。
  - 法的な問題をクリアするために電子署名が必要になる。
  - 電子署名は、社会的な責任の所在を明確にする手段でもある。
    - #なので、利用者に利便性を提供すると言うだけではない。
- 【講演】「わが国の保健医療福祉分野PKIの動向」
  - 講師：東京大学大学院 情報学環・学際情報学府　山本 隆一 氏

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

電子署名の展開
電子署名された文書は長期に保存される。。。
ECOMの「長期署名フォーマットのプロファイルの相互運用性テスト」

セコム IS 研究所
Intelligent Systems Laboratory

- 長期保存が要求される電子文書の**長期保存**
  - 法律で保存期間が定められた文書が多数存在する
  - (完全性を保った)「電子文書」のデータとしての独立性が要求される
  - 基本的には、暗号技術、タイムスタンプ等の(暗号) 技術等によりシステムから独立した電子文書のデータとしての独立性が実現可能
- 長期署名フォーマットの標準化
  - 理論的or技術的に長期保存が可能だとしても、保存されるデータがばらばらのフォーマットで**Long-Term Security**が実現できたと言えるだろうか？
  - 長期に保存されるデータだからこそ特定のシステムからの依存性を脱し標準化されたフォーマットで電子署名技術を用いて保存されるべき。つまり**Long-Term Security**の実現には、こうした**標準化**、そして広く利用されるための**相互運用**、**展開**の努力が欠かせない　->　Challenge PKIプロジェクト的観点
- 【講演】「長期署名フォーマットとECOMにおける相互運用実証実験について」
  - ＥＣＯＭ長期署名保存フォーマット普及SWGリーダ
  - 三菱電機株式会社　情報技術総合研究所　チームリーダ　宮崎 一哉 氏

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

電子署名の展開
不正に強く、透明性の高い電子社会

セコムIS研究所
Intelligent Systems Laboratory

現在の社会

紙と押印の世界

AsIs（現状）モデル

ITや電子署名が存在しなかった時代の法制度等による制約や、慣習の壁により、電子化、IT化が阻まれている。

BPR&改革が必要
紙前提の業務との大きなギャップ

改革には痛みも伴う、この手当ても必要

電子社会

電子データと電子署名の世界

ToBe（理想）モデル

効率的で、不正に強く、透明性の高い社会(を目指すべき)
電子署名の普及がカギ

効率、コスト削減のための改革とIT化、同時にIT化の中で適切なセキュリティを保つために電子署名が重要な意味を持つ

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

セコムIS研究所
Intelligent Systems Laboratory

組織を超えた連携のための基盤

Multi-domain PKI Interoperability Framework

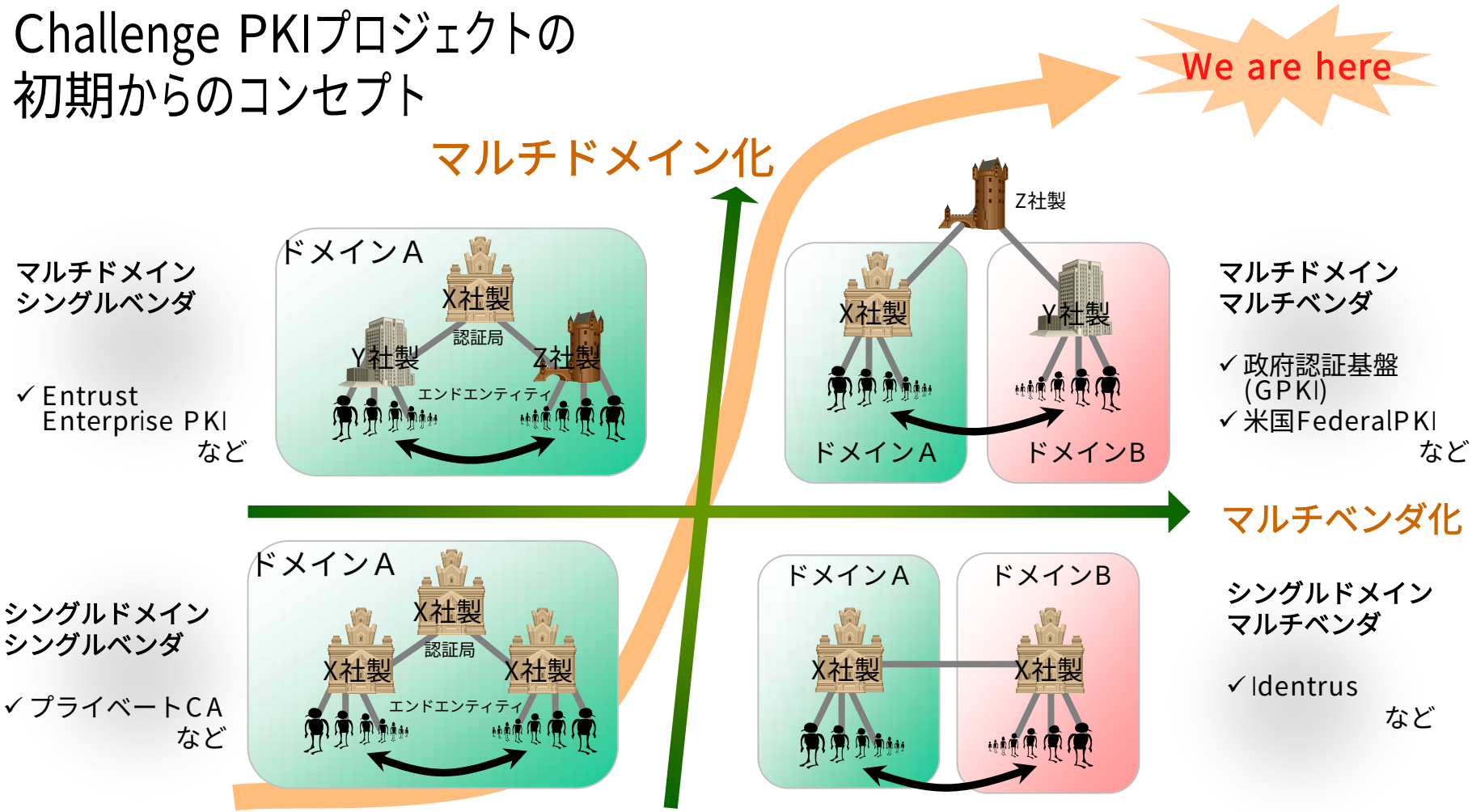
Copyright © 2006 SECOM Co., Ltd. All rights reserved.

組織を超えた連携のための基盤
Multi-domain PKI Interoperability Framework.

http://www.jnsa.org/mpki/index_j.html

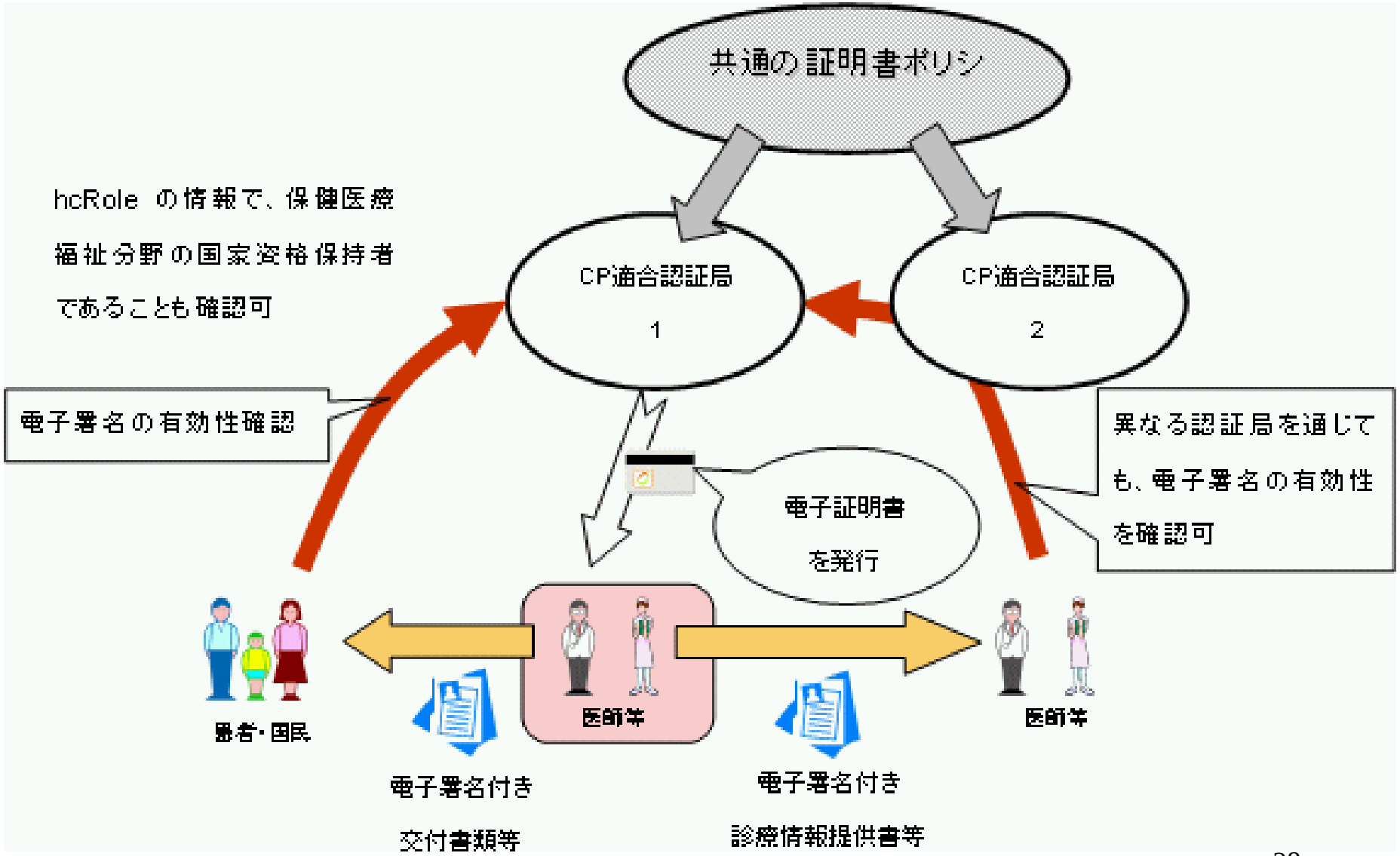
セコム IS 研究所
Intelligent Systems Laboratory

Challenge PKIプロジェクトの初期からのコンセプト



Copyright © 2006 SECOM Co., Ltd. All rights reserved.

組織を超えた連携のための基盤
保健医療福祉分野PKI



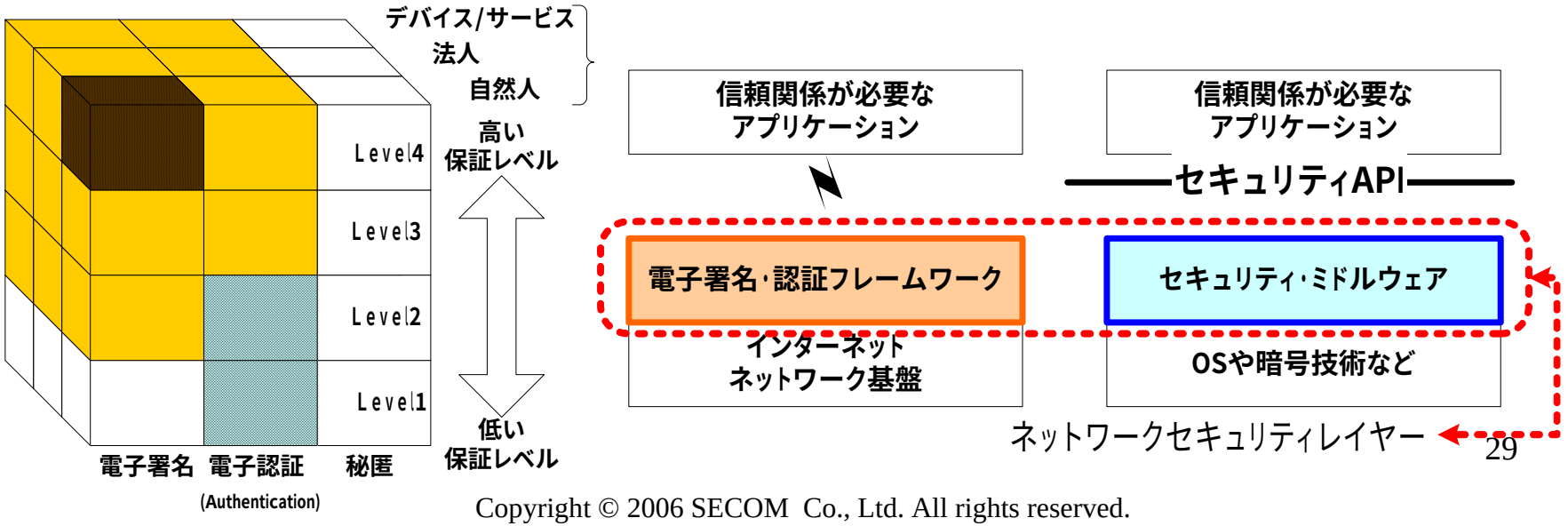
http://www.mhlw.go.jp/shingi/2005/07/s0725-10c.html

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

組織を超えた連携のための基盤
連携のための基盤の課題

セコム IS 研究所
Intelligent Systems Laboratory

- 相互運用技術
  - 企業内等においてオープンシステムを実現するための相互運用技術の必要性はよく理解されている。しかし、**連携**のための基盤には、組織を超えた「Trust」を実現するアーキテクチャと相互運用技術が必要になる。ここが重要
- ポリシーの整合　– 保証レベルに応じたレファレンスとなるポリシーが必要
- 信頼関係モデル(Trust Model)
  - 現実社会と現実のITで実現できるモデルとのギャップ
- #ステークホルダー間の調整　– 技術の不理解が調整を難しくしている？

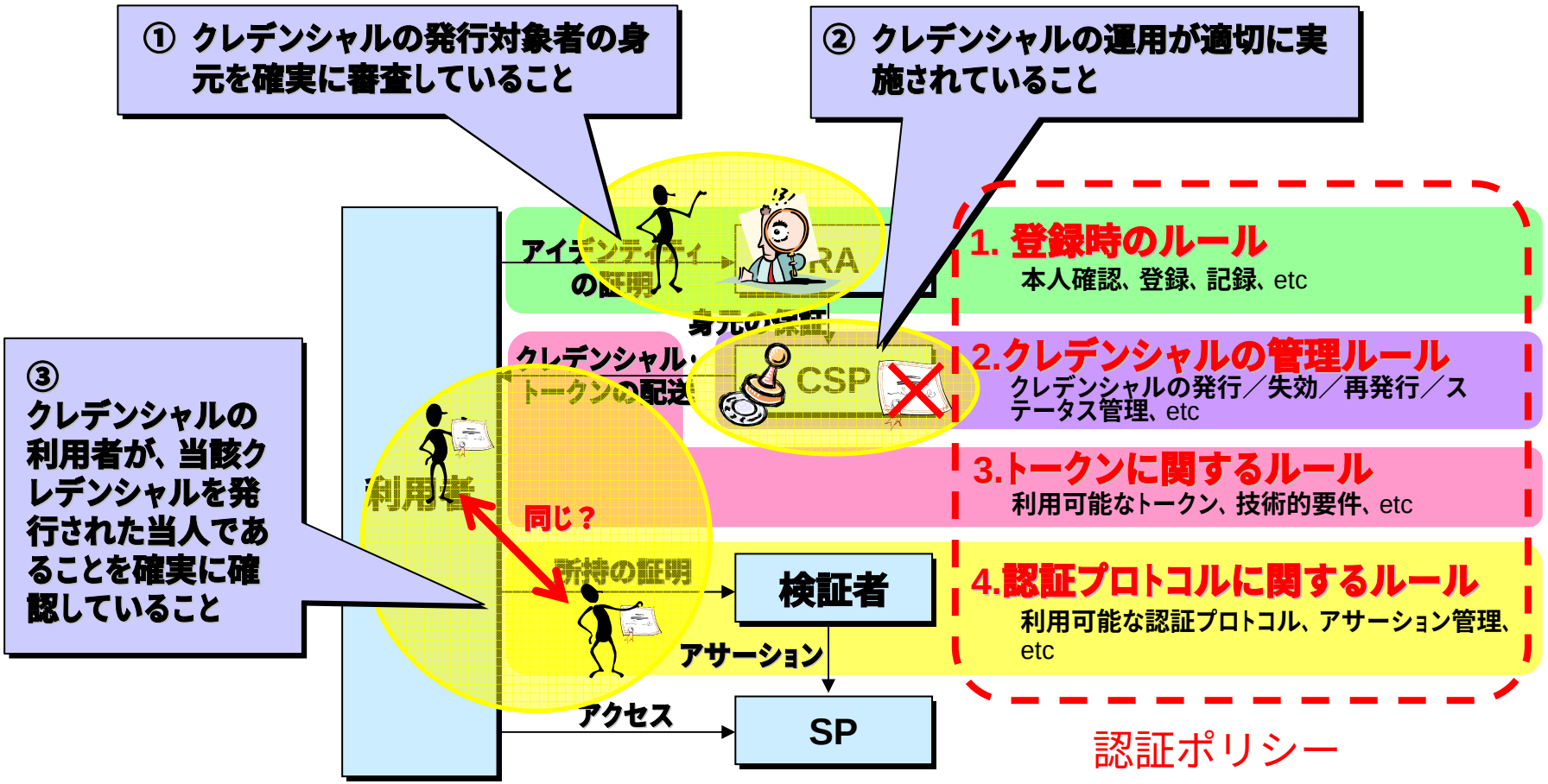


Copyright © 2006 SECOM Co., Ltd. All rights reserved.

組織を超えた連携のための基盤
次世代認証基盤プロジェクトの電子認証ポリシガイドライン

セコム IS 研究所 Intelligent Systems Laboratory

認証ポリシー(Authentication Policy)とは？

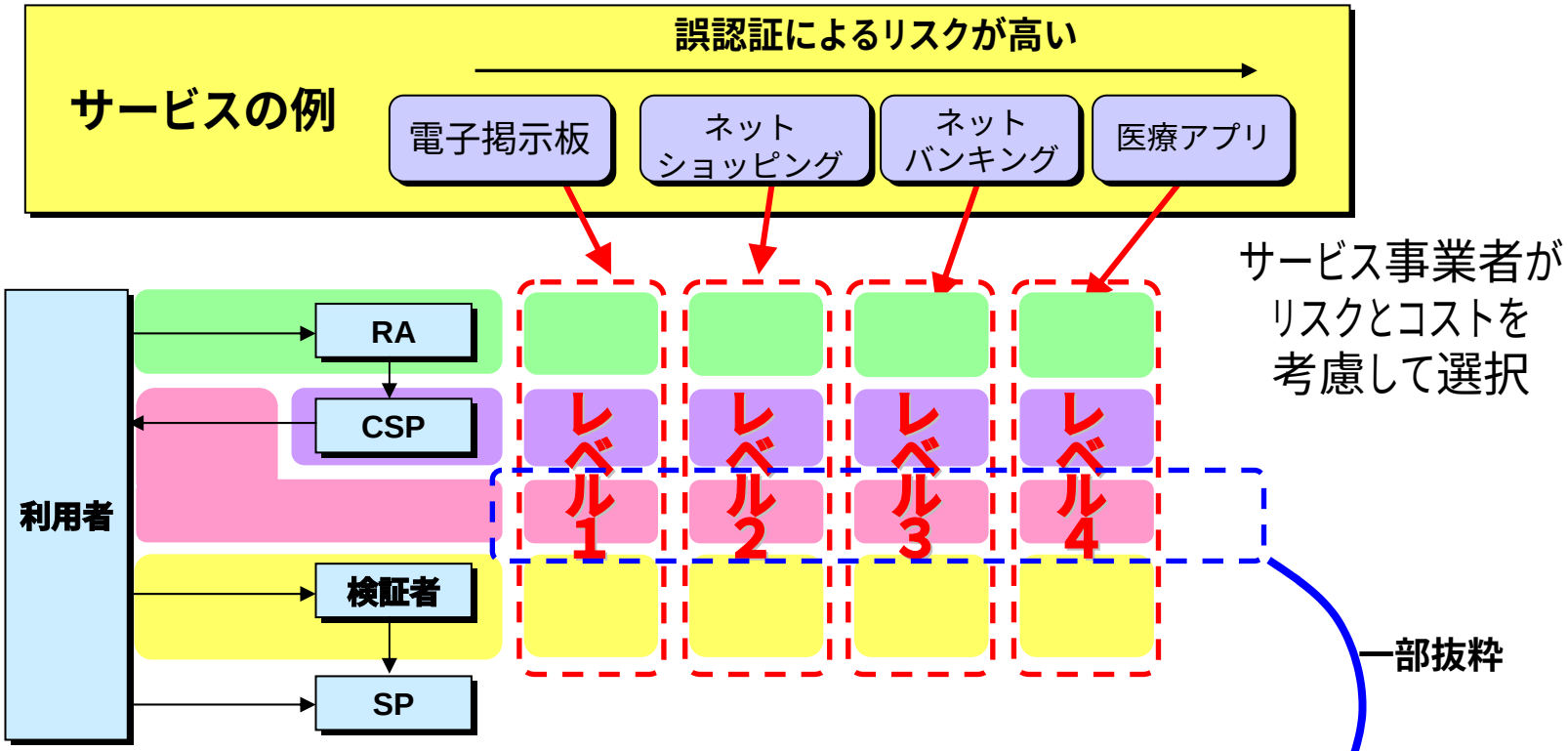


これらの要件を満たした技術の実装、および運用を行うことにより、クレデンシャルの信用を得ることができる

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

組織を超えた連携のための基盤
次世代認証基盤プロジェクトの電子認証ポリシガイドライン
保証レベル(Assurance level)のイメージ

セコム IS 研究所
Intelligent Systems Laboratory



基準の例

		レベル1	レベル2	レベル3	レベル4
利用可能なトークン	パスワードトークン	○	○	×	×
	OTPデバイストークン	○	○	○	×
	ソフトウェアトークン	○	○	○	×
	ハードウェアトークン	○	○	○	○

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

組織を超えた連携のための基盤

セコムIS研究所
Intelligent Systems Laboratory

- 【講演】「わが国の保健医療福祉分野PKIの動向」
  - 東京大学大学院 情報学環・学際情報学府　山本 隆一 氏
- 【講演】「大学間連携のための全国共同電子認証基盤UPKI構想と米国学術PKIの動向」
  - 国立情報学研究所　島岡 政基 氏
- 【講演】「グリッドにおけるセキュリティの概要と動向」
  - 産業技術総合研究所　田中 良夫 氏

例えば、医療の場合、非常にセンシティブな個人情報を扱う。ITによる医療の質の向上や効率化が望まれるが、これたは、単に情報を金庫にしまって置くだけでは実現できない。情報の活用が望まれる。そのためには、Trustを実現した組織を超えた**連携**のための基盤が重要になる。

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

PKI相互運用技術からみたSHA-1問題(おまけ)
#結論のみ。。。

- SHA-1脆弱性問題に限らず、暗号アルゴリスムの危殆化問題は、Long-termセキュリティの観点が必要
  - ハッシュアルゴリズムで一番多く利用されているのはたぶんMD5。これらがすべて問題がある訳ではない。
  - 移行には、ロードマップを示すことが重要。移行には長い時間がかかる。
- 暗号アルゴリズムの移行には、相互運用技術の観点からの検討が必須
  - 鍵更新、Hash Agility、Algorithm Agility、 Downgrade protection、etc….

Copyright © 2006 SECOM Co., Ltd. All rights reserved.

PKI の展開と最新技術動向
参考

セコム IS 研究所
Intelligent Systems Laboratory

- NPO JNSA Challenge PKIプロジェクトのホームページ
  - http://www.jnsa.org/mpki/index_j.html
- これまでのNPO JNSA&PKI相互運用技術WG主催セミナー
  - PKI Day PKI技術最新事情
    - http://www.jnsa.org/seminar/2005/seminar_20051028.html
    - 2005年10月28日 (金)
  - セキュリティAPIセミナー
    - http://www.jnsa.org/seminar/2004/seminar_20040826.html
    - 2004年8月26日(木)
  - 「認証技術の動向」セミナー
    - http://www.jnsa.org/seminar/2004/seminar_20041209.html
    - 2004年12月9日(木)
- 次世代認証基盤プロジェクト
  - http://www.japanpkiforum.jp/hojo/index.htm
  - 電子認証ポリシガイドライン
  - http://www.japanpkiforum.jp/hojo/index.htm

Copyright © 2006 SECOM Co., Ltd. All rights reserved.