WG 成果報告会
PKI相互運用技術WG/ Challenge PKIプロジェクト

セコム株式会社IS研究所
松本　泰

2004 年 5月 18日

WG 成果報告会　PKI相互運用技術WG

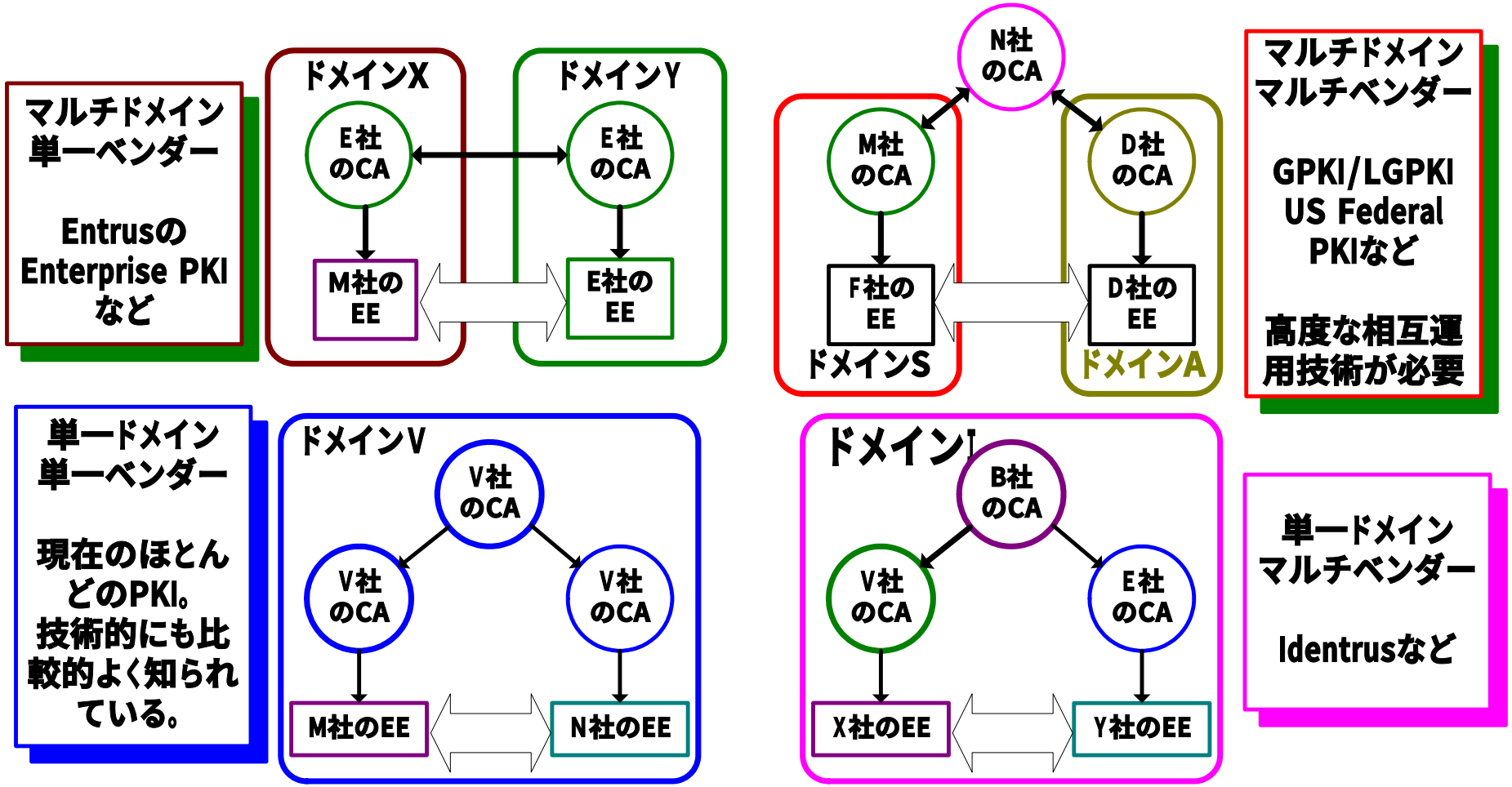
- PKI相互運用技術WGでは、年3回行なわれたIETFの参加、Challenge PKIプロジェクトの としてIPAの公募に応募し採択されたプロジェクトへの参加、そして、それらの成果物の WG内での発表などを行ってきました。 今回は、IETFでの活動報告と、ＩＰＡから公開されている、ふたつの調査報告書（「タイムスタンプ・プロトコルに関する技術調査」、「セキュリティAPIに関する技術調査」）ついて報告します。

Challenge PKI活動概要

Challenge PKI 2001	- ９つのCAが参加を得て行ったマルチドメイン、マルチベンダーのPKI相互運用実験 - 課題はCA間の相互接続	マルチドメイン、マルチベンダー環境下でのPKI相互運用フレームワークの確立
Challenge PKI 2002	- 相互運用テストスィートの開発など - よりPKIアプリケーションよりのPKI相互運用の課題に挑戦 - GPKIのようなマルチドメイン、マルチベンダーのPKI開発を容易にする	
Challenge PKI 2003	-「セキュリティAPI」「タイムスタンプ」etc. - ＩＥＴＦ　RFCの提案	**標準技術の調査、フィードバック**

- JNSAのモチベーション
  - PKIのインフラとしての必要性を社会にアピール
  - ネックとなるPKI相互運用性の問題などを自ら解決していく
- 独立行政法人 情報処理推進機構（IPA）の委託を受けて実施

Challenge PKI 2001
マルチベンダーPKI、マルチドメインPKI



Challenge PKIの活動履歴

2001	2002				2003				2004
4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q

Challenge PKI 2001 プロジェクト

Challenge PKI 2002 プロジェクト

Challenge PKI 2003 プロジェクト

PKI関連相互運用性に関する調査報告を公開 (2002.5.16)

2002.11.20 55th IETF アトランタミーティングの PKIX WG において発表

2003.7.17 57th IETFウィーンミーティングの PKIX WG において発表

JNSA主催 NSF2002での発表 2002.6.12

2002.12.17 JNSA IW2002セミナ

JNSA主催 NSF2003での発表 2003.10.24

54th IETF 横浜ミーティングの PKIX WG において発表した。 2002.7.17

2003.3.20 56th IETFサンフランシスコミーティングの PKIX WG において発表

JNSA主催 ChallengePKI IETF参加等活動報告会 2004.4.27

IETFでの活動 (2002年度)

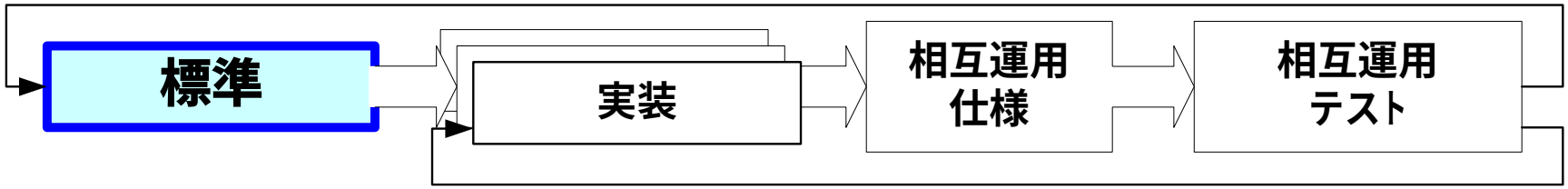
- 54th IETF 横浜での発表　-　2002年7月17日
  - ChallengePKI2001の成果の発表
  - http://www.jnsa.org/mpki/ChallengPKI2001-IETF-PKIX.pdf
  - http://www.jnsa.org/mpki/Interoperability_mPKI.pdf
- 55th IETF アトランタでの発表　2002年11月17日
  - Challenge PKI 2001で明らかになった問題点など報告
  - ChallengePKI2002の紹介
  - http://www.ietf.org/proceedings/02nov/slides/pkix-5.pdf
- 56th IETF サンフランシスコでの発表　2003年3月20日
  - ChallengePKI2002の成果の発表
  - 開発した相互運用テストスィートのデモ
  - http://www.ietf.org/proceedings/03mar/slides/pkix-2.pdf

2003年度のChallenge PKI の活動方針

- 標準化活動への参加
  - IETFでの活動
    - 標準自体へのフィードバック
  - 標準・仕様作成と相互運用仕様作成は同時進行であるべき
- PKI相互運用イニシアチブの活動
  - 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。
  - 海外との連携
- 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

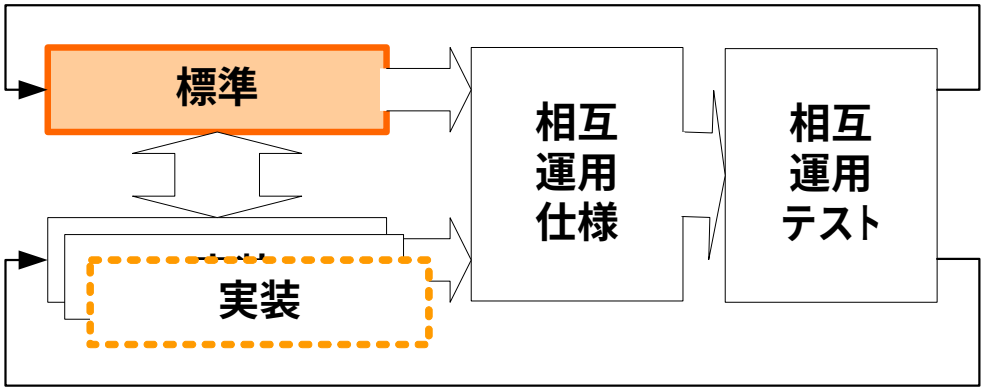
Challenge PKI プロジェクトの展開
標準化から実装、そして相互運用

- **ISO／IEC、ITUなどの標準化から実装、相互運用**



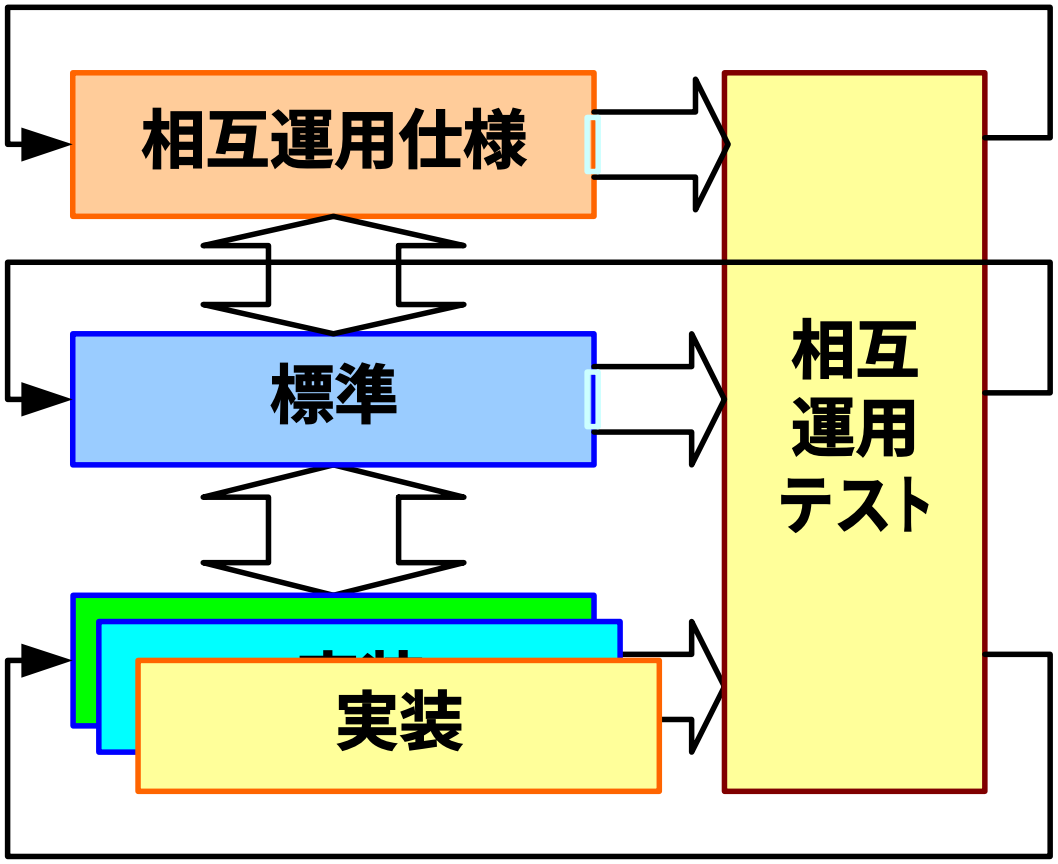
  - **実装を伴わない現実味のない標準ができる可能性**
  - **長い標準化期間、そして、長いターンアラウンド**

- **IETFの標準化から実装、相互運用**



- IETFの標準化の基本コンセプトは、ラフコンセンサス アンド ランニングコード
- 複雑なセキュリティプロトコルに対していい加減な実装が蔓延してしまう….

Challenge PKI プロジェクトの展開
標準化から実装、そして相互運用の統合



- 標準の作成と相互運用仕様の作成を同時に行う。
- 相互運用テスト（準拠性テスト）を早期に行う
- 相互運用テストスィートなどの開発も考慮する

57th IETF@Vienna

- PKIX WG
  - 初めてmPKI I-Dについて発表を行った。(セコムトラストネット 島岡)
    - 幅広い認証ドメインにおけるPKIのベストカレントプラクティスを示す「マルチドメインPKIの相互運用性に関するメモ」
    - http://www.ietf.org/proceedings/03jul/slides/pkix-9/index.html
    - 直前に初版(-00)をリリース。
  - 文書構成、各章の概要、今後の作業などについて説明。
  - WG ChairのTim PolkはじめInternet2のBob Morgan(ワシントン大)や、認証パス構築に関するI-Dの著者の一人であるMatt Cooper(Orion Security)らから支持を受けた。
- その他
  - PKIX WG中で担当ADのRuss Housleyから、PKIX WGはおおよそのミッションを達成したので、現在抱えているI-DをRFC化して終息方向へ向かう、という事実上のクローズ宣言がなされた。

57th IETF@Vienna

57 th IETFにおいて、チャレンジPKIプロジェクトの中心メンバーの一人であるセコムトラストネットの島岡氏の発表

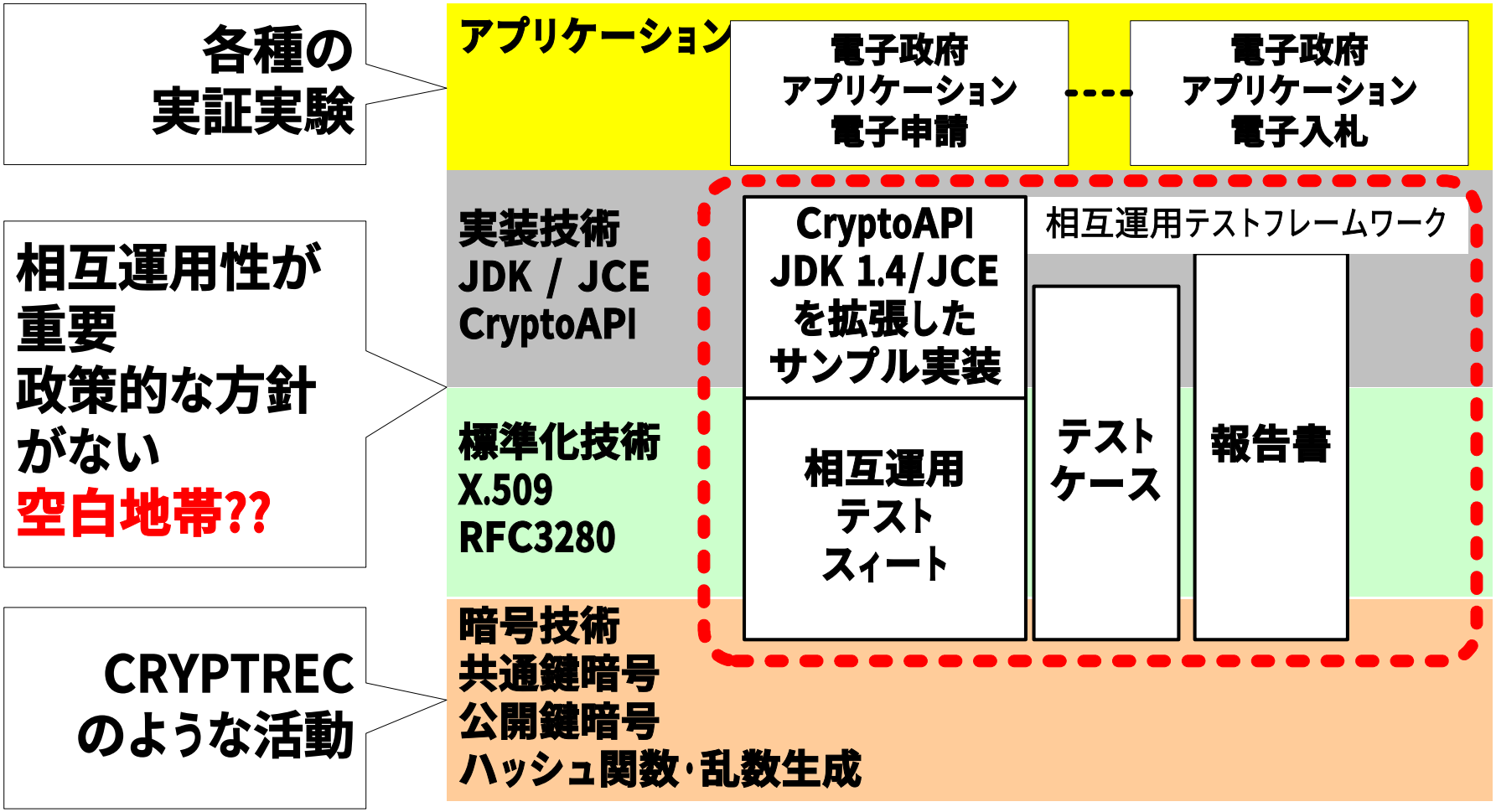
新WGの検討@59th Seoul

- Before 59th IETF@Seoul
  - mPKI I-D **第3版**(-02)**をリリース**
  - PKIX WG**へエキスパートレビュを依頼**
    - WG Chair**他数名から、**PKIX**とは**Scope**が異なる(広すぎる)ので別**WG**を新設して検討すべきでは、とのコメント。**
    - D.Pinkas, P.Hesse**ら実質的な**WG**主要メンバからのコメントがいくつか寄せられた。**
- At 59th IETF@Seoul
  - WG**新設のニーズ、可能性等について**AD/WG Chair**らと検討**

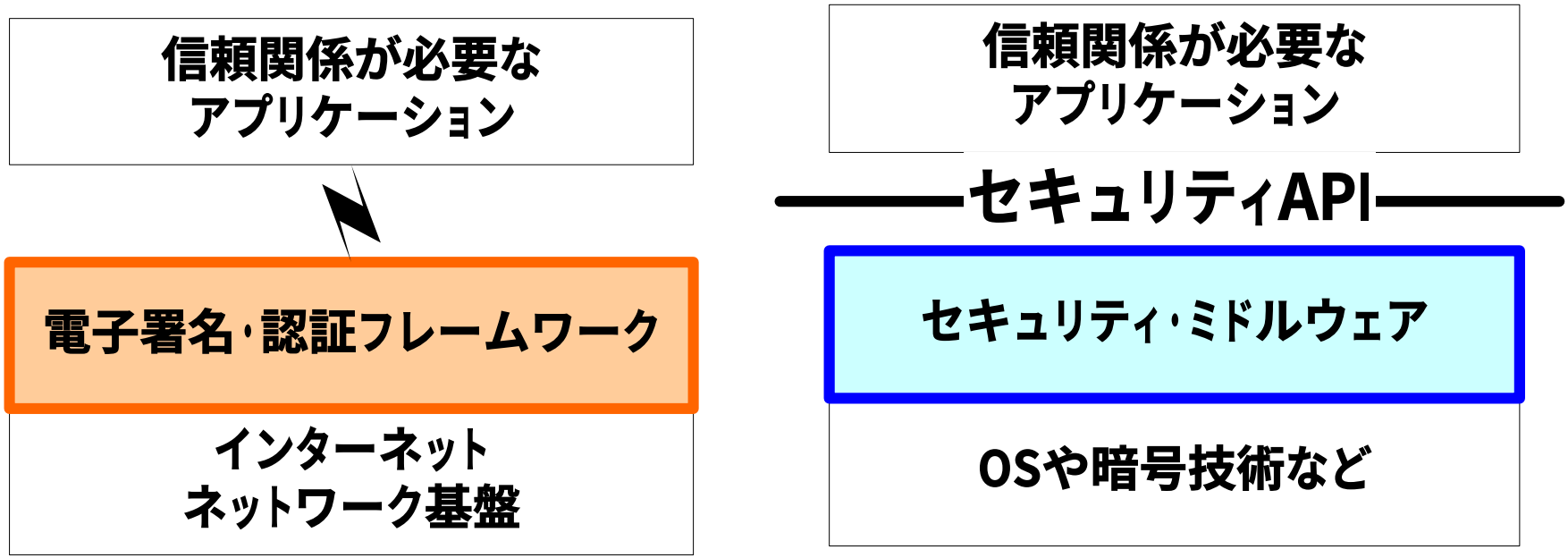
Power Dinner @ 59thSeoul (2)

- **議題**
  1. WG**新設のニーズ**
  2. **新**WG**運営のフィージビリティ**
  3. mPKI I-D**の**RFC**化**
- **結論**
  1. **新**WG**運営には非技術面での問題解決も不可欠**
     - **こと**PKI**は国によっては政策的側面もあるため、エンジニアだけでは調整が困難。**
  2. WG**設立を望む同志がいれば協力は可能。**
  3. IESG**レビュの前に**PKIX**以外の関連**WG(S/MIME, TLS, pki4ipsec**など)のエキスパートレビュも不可欠**

Challenge PKI プロジェクトの展開
セキュリティフレームワークやミドルウェア重要性

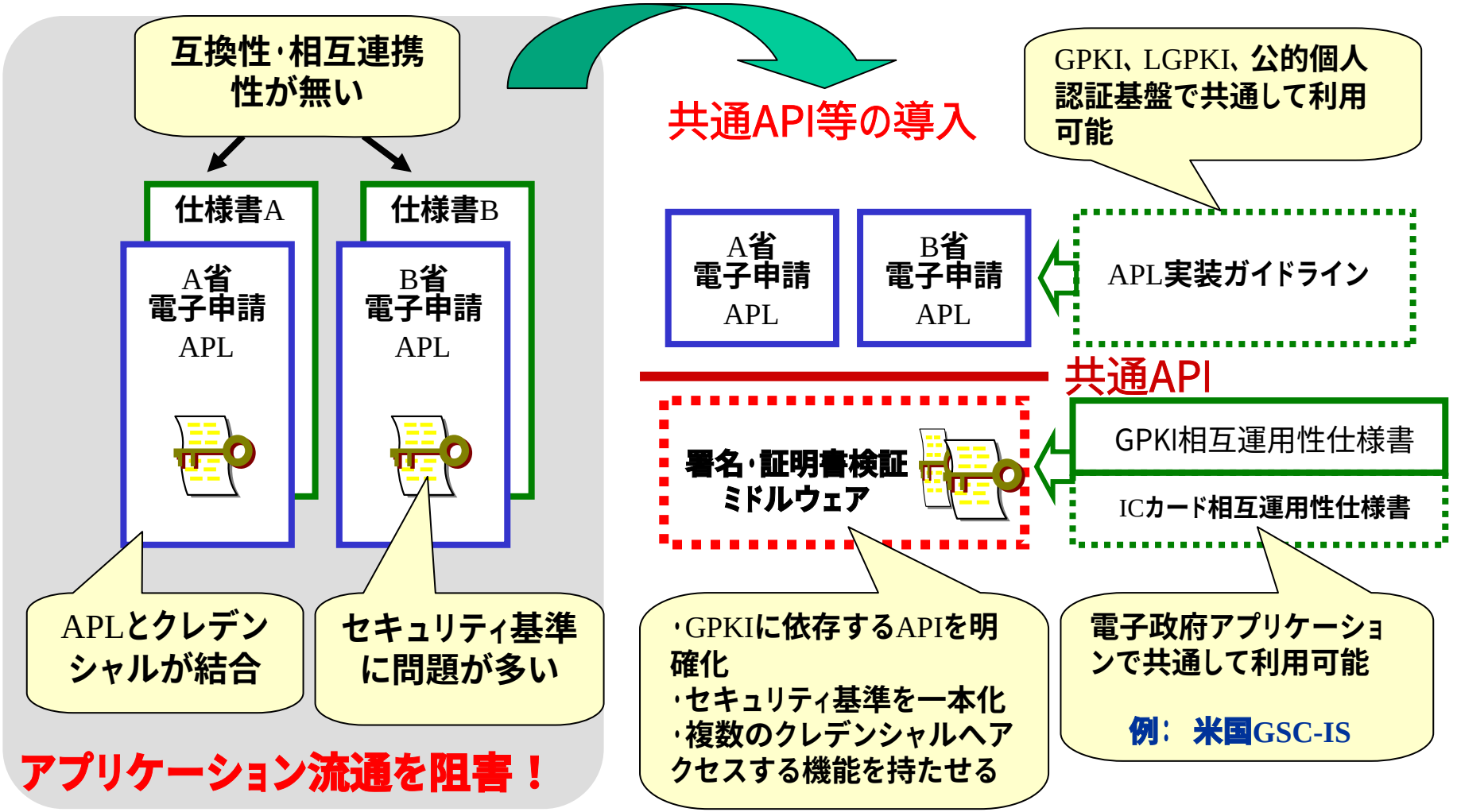


Challenge PKI プロジェクトの展開
セキュリティフレームワークやミドルウェア重要性



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

Challenge PKI プロジェクトの展開
セキュリティフレームワークやミドルウェア重要性



IPAのプロジェクト

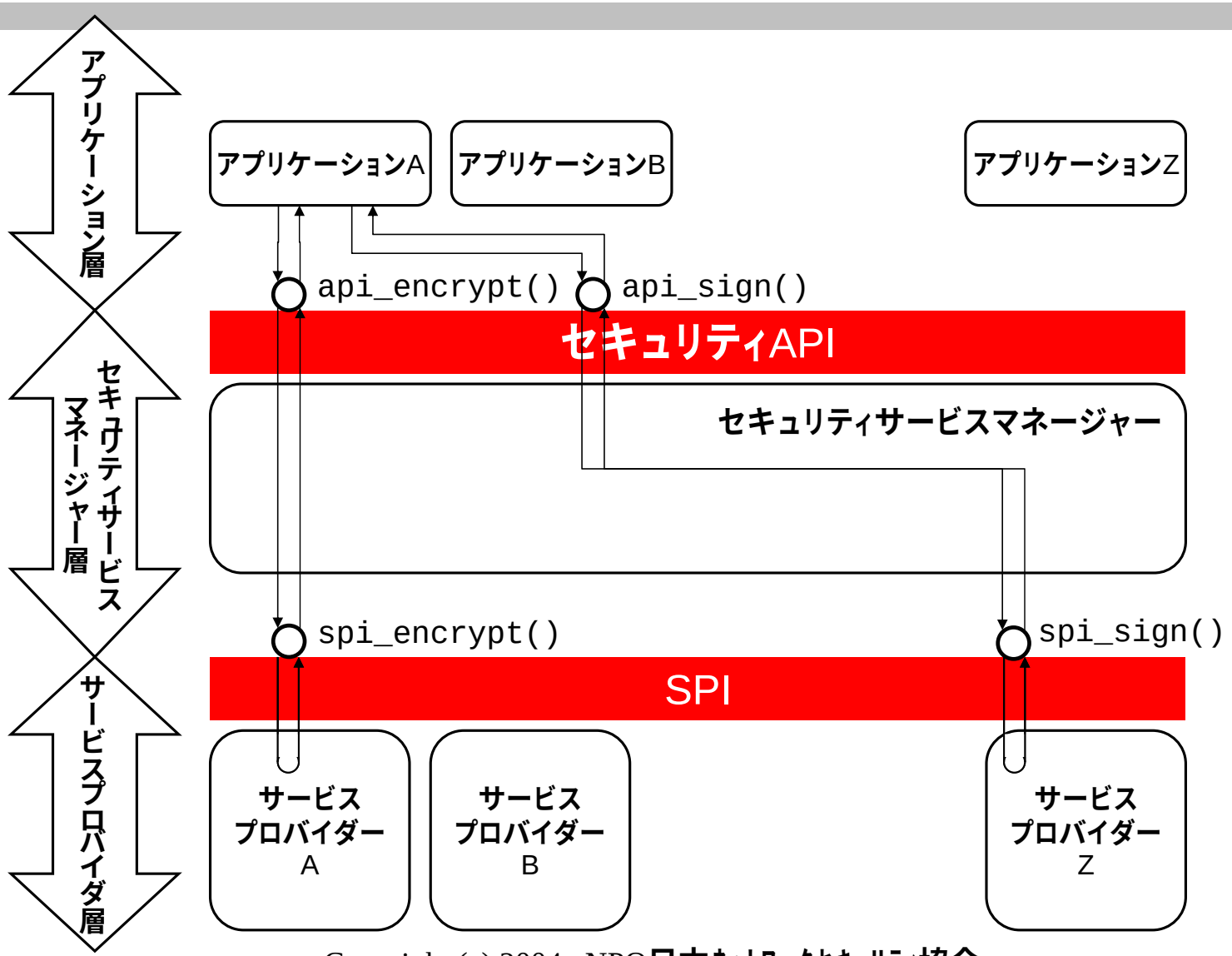
- **セキュリティAPIに関する技術調査**
  - 設計者、開発者向けの報告書
  - セキュリティフレームワークやミドルウェア重要性に着目
  - セキュリティAPIのアーキテクチャ
  - セキュリティAPIが共通に提供する重要な機能
  - 普及しているプラットフォーム上で提供されているセキュリティAPIの利用法
  - 近年の技術動向の中で重要性が増している新しいセキュリティAPI
- **タイムスタンプ・プロトコルに関する技術調査**
  - 設計者、開発者向けの報告書
  - RFC 3161の相互運用性を中心テーマにして、タイムスタンプに関連した最新技術動向
- **PKI 相互運用テストスィートへの機能追加開発および関連調査**
  - 日本国内のタイムスタンプの利用検討状況をヒアリングした報告書
  - RFC 3161のテストスィート

セキュリティAPIに関する技術調査

- Part 0. 報告書の構成、セキュリティ API の利用に関する提言
  - 13 page 全体のオーバビュー
- Part 1. セキュリティ API の概要、アーキテクチャ、機能、暗号技術とアルゴリズム
  - 121page
- Part 2. Java JCE (Java Cryptographic Extensions) ： 機能と利用法
  - 65page サンプルコード付き
- Part 3. .NET Crypto API ： 機能と利用法
  - 67 page サンプルコード付き (Part 2. Java JCE と似た構成)
- Part 4. IC カードなどのハードウェアトークンAPI
  - 58 page ICカードのAPI。.NET Crypto API 、PKCS#11、米国のGSC-IS
- Part 5. バイオメトリック認証の API
  - 69 page BioAPI。ICカード+PKI+BioAPIのアーキテクチャ

セキュリティAPIの層アーキテクチャ

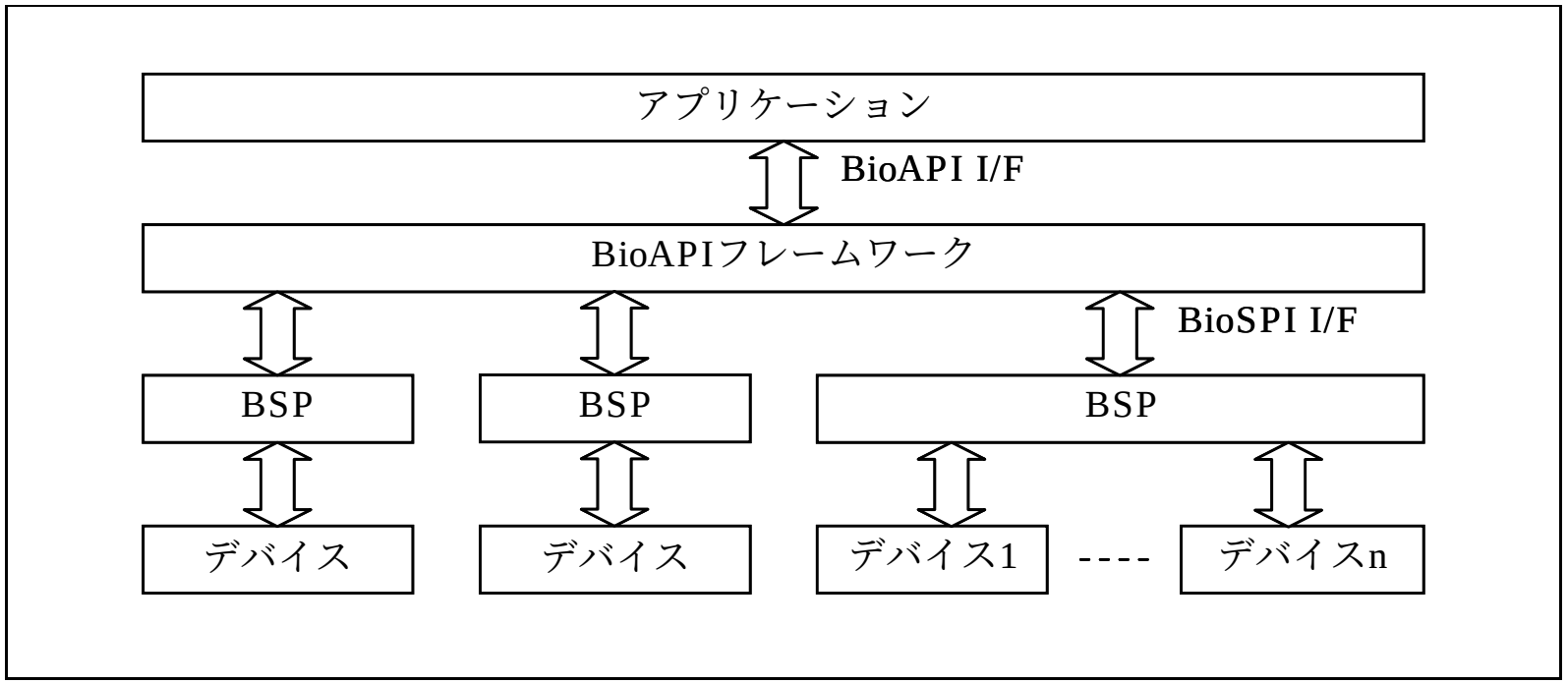
Part 1. セキュリティ API の概要、アーキテクチャ、機能、暗号技術とアルゴリズムより



セキュリティAPIの層アーキテクチャ

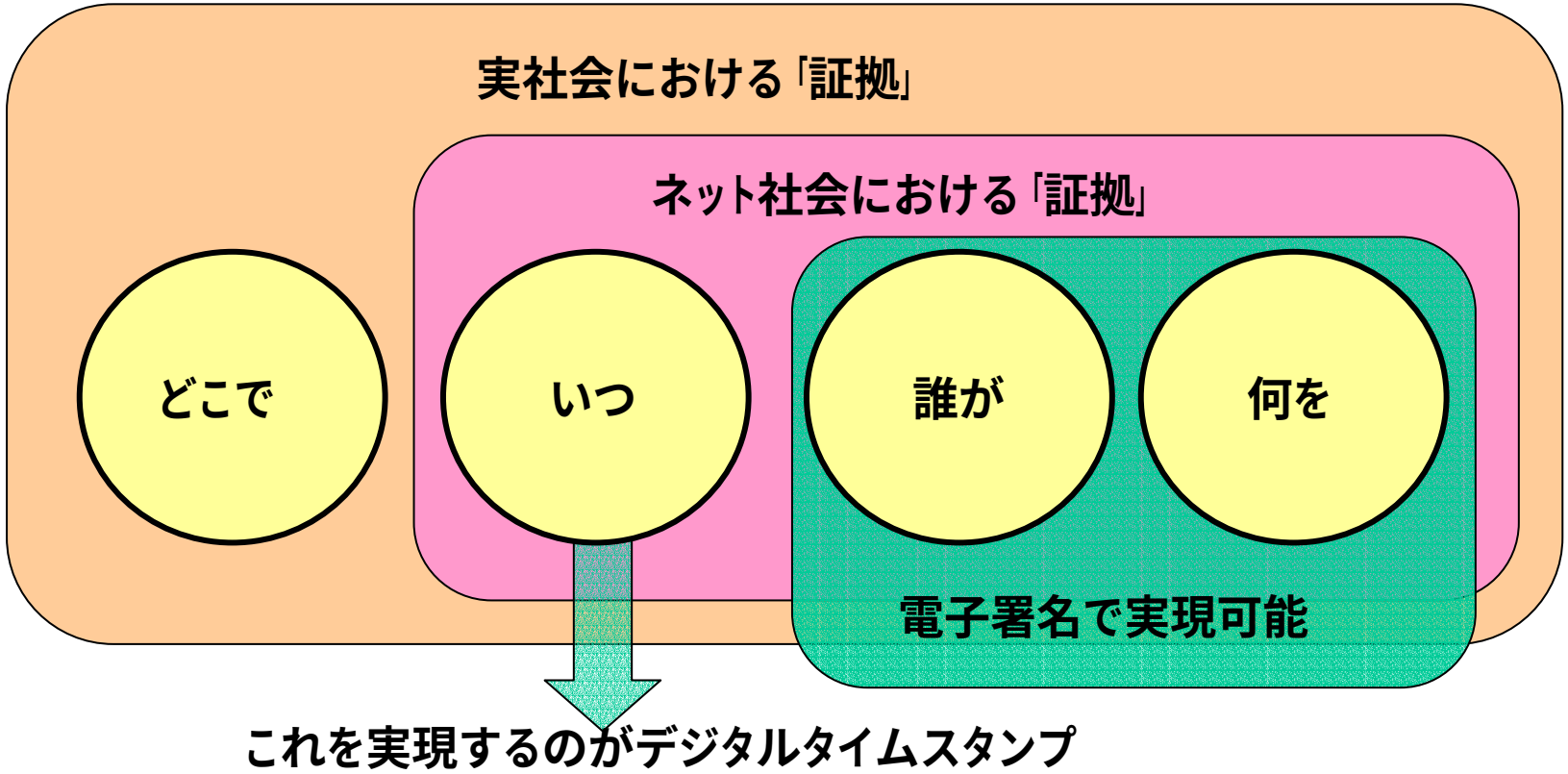
Part 2. Java JCE、Part 3. .NET Crypto API 、Part 4. IC カードなどのハードウェアトークンAPI、Part 5. バイオメトリック認証の APIで、それぞれのセキュリティAPIの層アーキテクチャを解説。

BioAPIの層アーキテクチャ (Part5)



タイムスタンプとは？

PKI 相互運用テストスィートへの機能追加開発および関連調査より



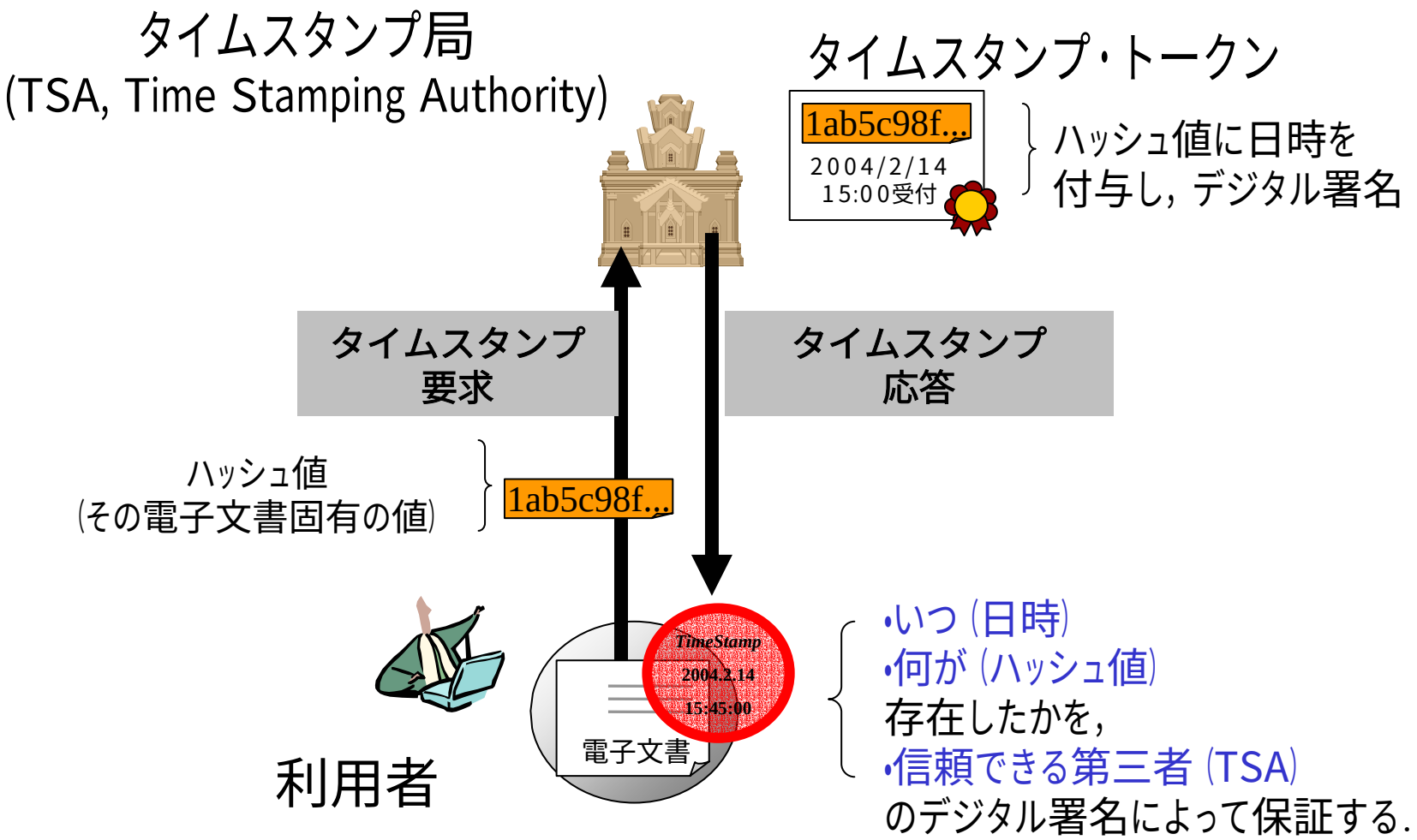
電子文書の時刻を証明＆存在証明

紙文書から電子文書への移行には必須の技術

ログデータの保存などコンピュータフォレンジックなどにおいても有望な技術

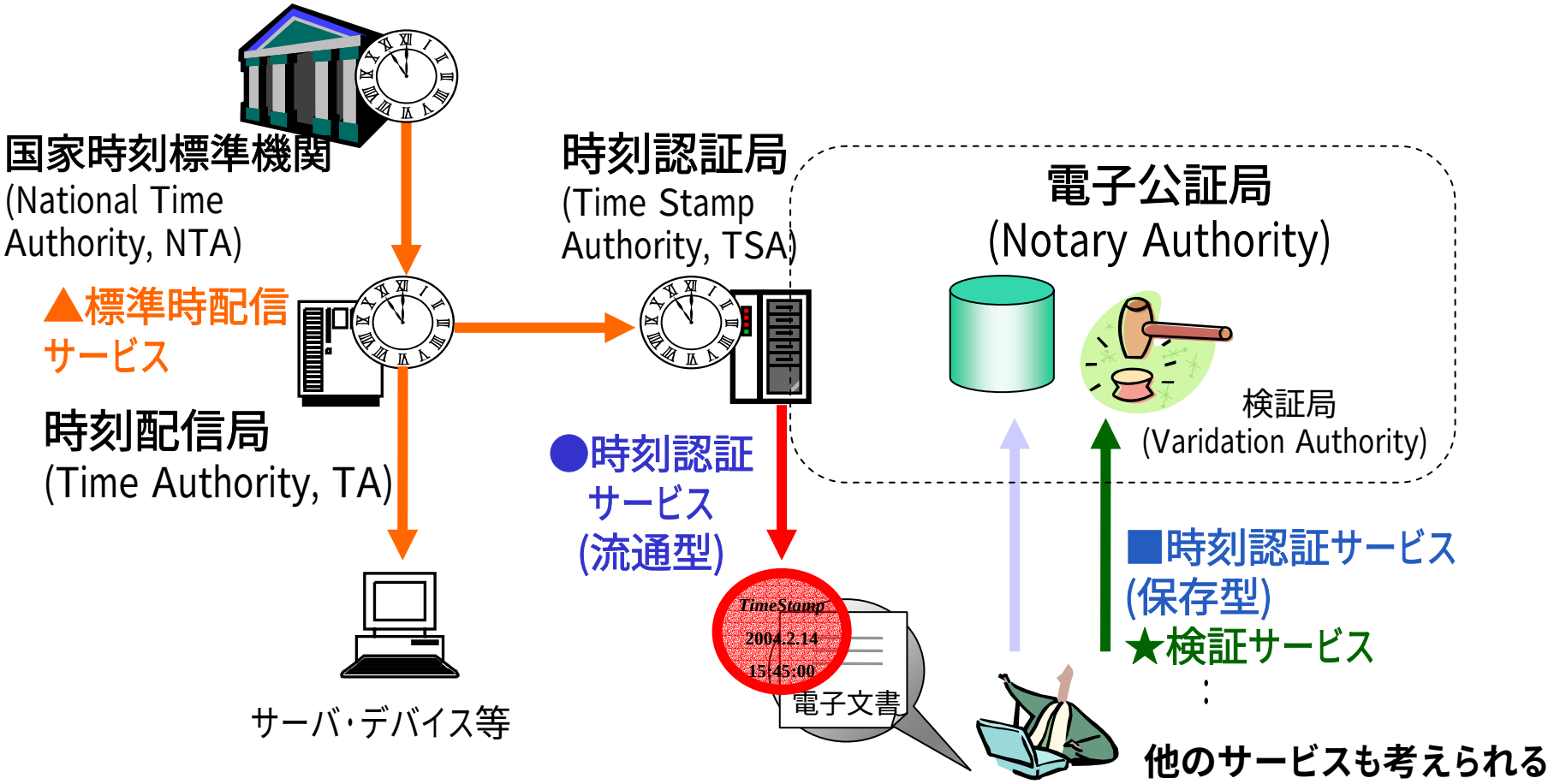
RFC 3161 X.509インターネット PKI タイムスタンププロトコル (TSP)

PKI 相互運用テストスィートへの機能追加開発および関連調査より



タイムビジネス

PKI 相互運用テストスィートへの機能追加開発および関連調査より

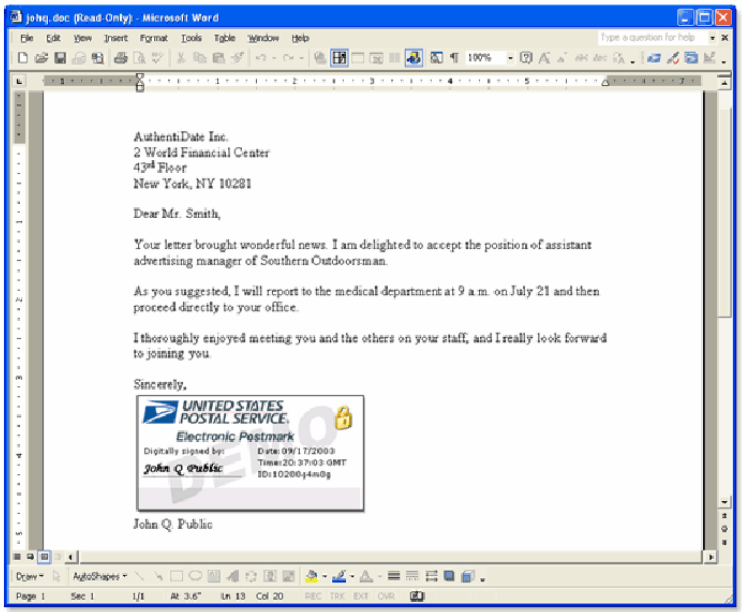


米国郵政公社(USPS)の電子消印サービス(EPM)

タイムスタンプ・プロトコルに関する技術調査より

●時刻認証サービス(流通型)

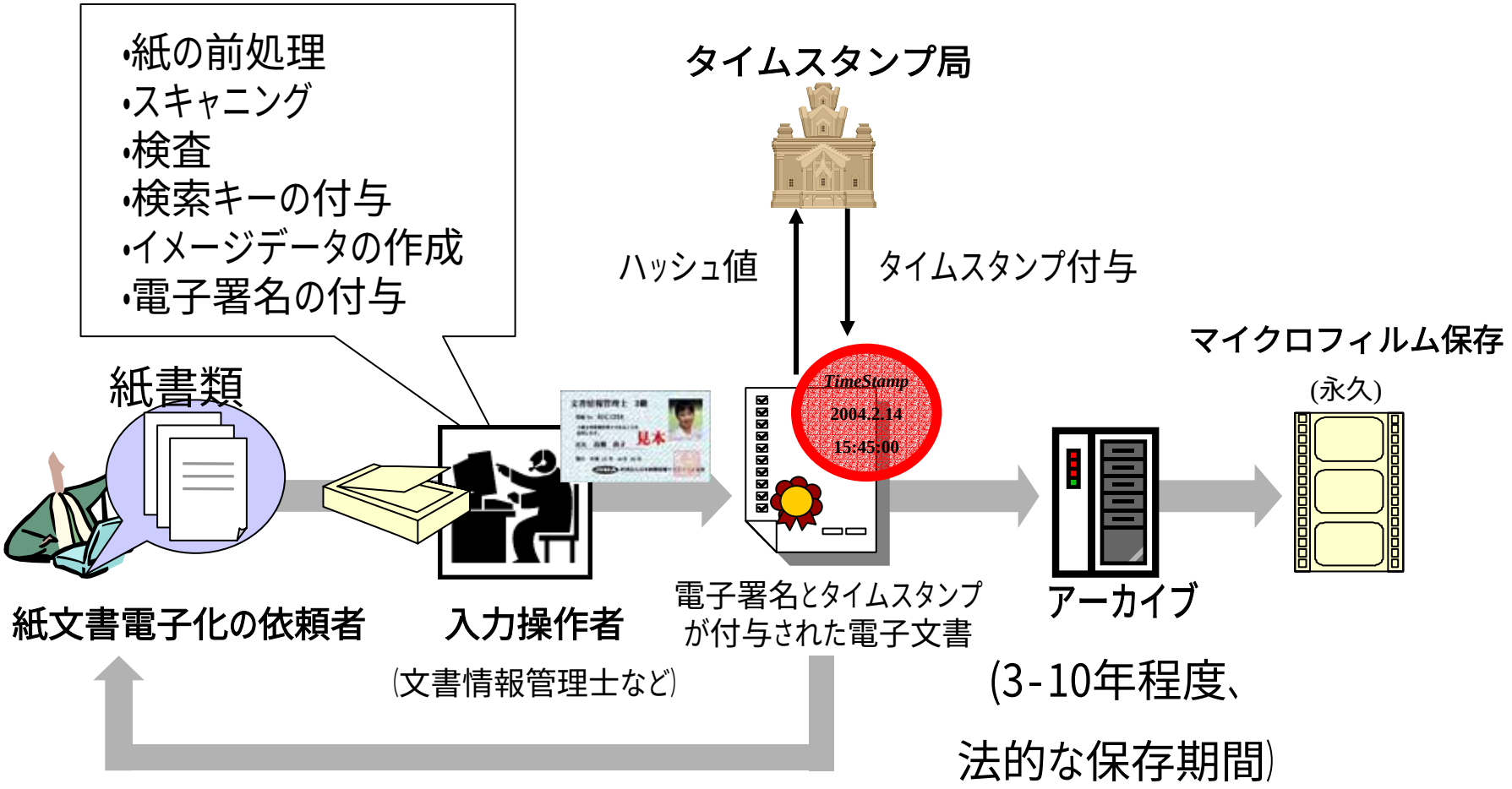
- 利用者拡大の戦略
  - MicrosoftOfficeの専用プラグインを無料配布
  - 世界中から誰でも利用できる
  - １スタンプ$0.1～$0.8※
- サービスの提供者
  - 米国郵政公社 (USPS)
  - 米Authentidate社
    (サービス・技術の提供)
  - マイクロソフト



※　25EPMを購入する場合：1EPM当たり0.8米ドル
1,000,000EPMを購入する場合：1EPM当たり0.1米ドル

文書電子化に関わる動向

PKI 相互運用テストスィートへの機能追加開発および関連調査より



スキャナなどで取り込んだ紙データの電子化においても電子保存を容認の方向へ

文書電子化に関わる動向
参考：e-文書保存法の検討内容

現状

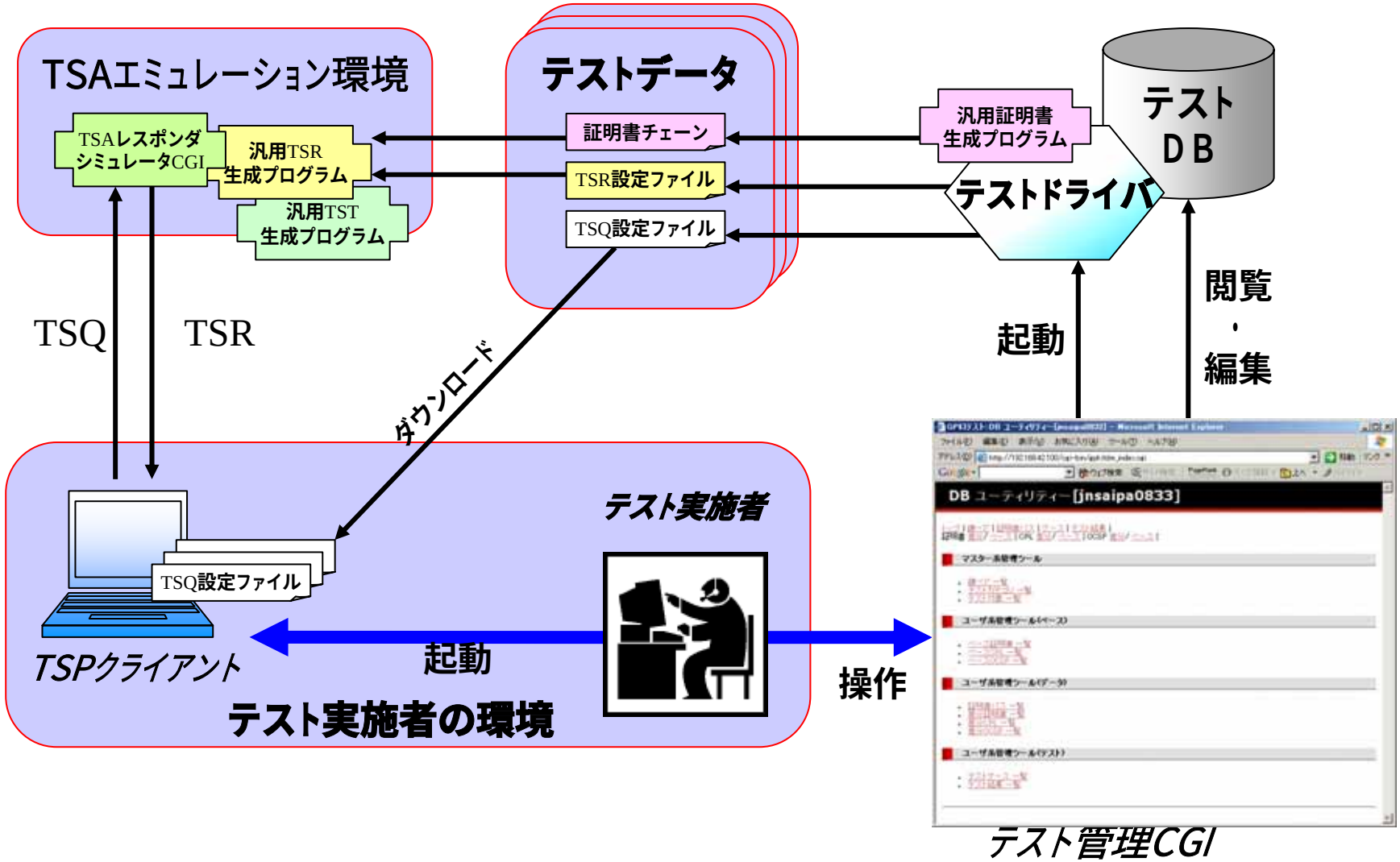
電子的保存に関する対応の段階	法律（本）
①電子保存容認 （当初紙で作成したものや他人から紙で受け取ったものでも電子保存を容認）	４８
②一部容認 （当初から電子的に作成したものに限り電子保存を容認）	５８ 例）財務関係書類 税務関係書類
③書面に限定 （電子保存を容認せず）	１２２
計	２０３

各省庁の検討状況

法律（本）
１８８ 例）*財務関係書類* *税務関係書類*
９
１４
２０３

※内閣官房IT担当室：民間保存文書の電子的保存に関する対応の方向性について,平成16年4月5日より

RFC 3161 タイムスタンププロトコルテストスィート



Challenge PKI　プロジェクトの今後の案

- Memorandum for multi-domain PKI InteroperabilityのRFC化
  - BCP ベストカレントプラクティスの確立に力を注ぐ
- Son of RFC 3280のテストケースの設計
  - UTF8Stringの扱いなど….
- 公的個人認証サービスも含めた電子政府全体のテスト環境
  - テストケースも含め配布できる形態で提供
  - テストサイトの立ち上げ
- デジタルタイムスタンプなどPKIをベースとしてプロトコル類のテストスィートへ
  - #近日中にタイムスタンプのテストサイトを公開予定….
- 米国、EU、アジアでのPKIテストスィート、及び、テストケースの共有
  - 日韓台湾等の国際間相互接続実証実験でも利用している..

参考

- JNSA Challenge PKI IETF参加等活動報告会
  - http://www.jnsa.org/seminar_20040427IETF.html
  - 島岡、稲田、松本
- 第59 回IETF ミーティング参加報告書
  - http://www.jnsa.org/houkoku2003/59th-IETF-JNSA.pdf
- 第57 回IETF ミーティング参加報告書
  - http://www.jnsa.org/houkoku2003/57th-IETF0724.pdf
- NSF2003 springでのWG活動発表資料
  - 「PKIアプリケーションの相互運用を促進するChallenge PKI 2002」
  - http://www.jnsa.org/nsf2003spring/pdf/b4.pdf

参考　(続き)

- タイムスタンプ・プロトコルに関する技術調査
  - http://www.ipa.go.jp/security/fy15/reports/tsp/index.html
- セキュリティAPIに関する技術調査
  - http://www.ipa.go.jp/security/fy15/reports/sec_api/index.html
- PKI 相互運用テストスィートへの機能追加開発および関連調査
  - http://www.ipa.go.jp/security/fy15/development/pki_interop/index.html
- JNSA Press No.10 セキュリティAPIに関する技術調査
  - http://www.jnsa.org/active/press/vol10/2_2tokusyuu.pdf
- Challenge PKI
  - http://www.jnsa.org/mpki/index_j.html
- Challenge PKI 2003 (Time Stamp)
  - http://www.jnsa.org/mpki/2003/index.html