NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セキュリティAPIの重要性

セコム株式会社IS研究所/
JNSA PKI相互運用技術WGリーダ

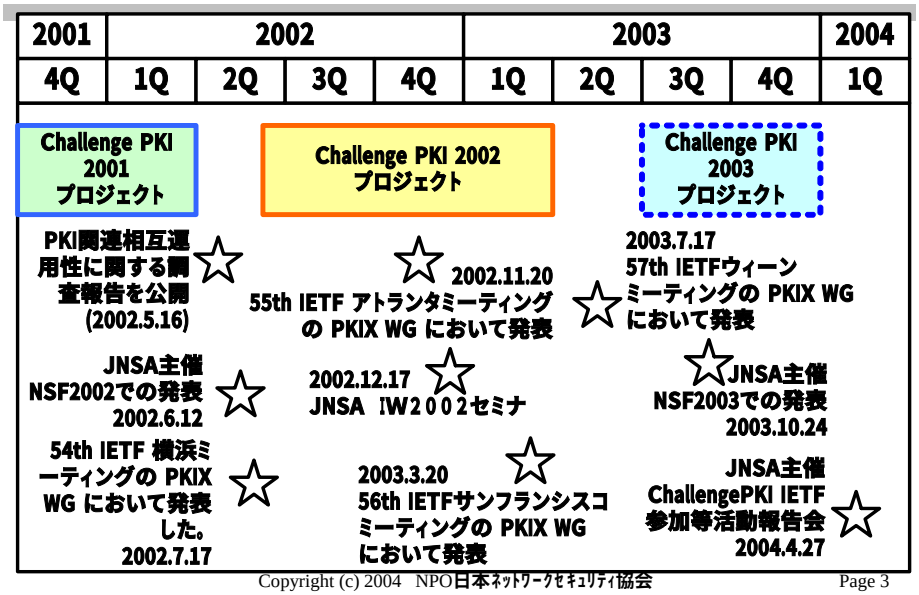
松本　泰

2004 年 8月 26日

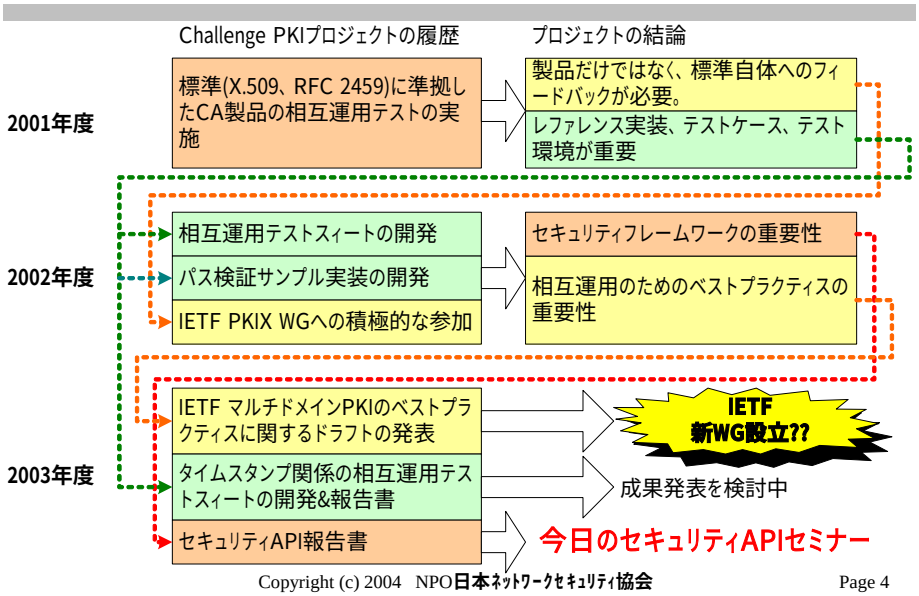
プロローグ

- 古きよき時代のネットワークプログラミング
  - RFC 1939　pop3の実装をやってみよー。
  - 分からなかったらRFC見てね。RFC 1939 たった 23 page 。
  - Socketが基本だよーん
  - #昔は新たなプロトコルの「ラフコンセンサス アンド ランニングコード」の「ランニングコード」も簡単だった。。。
- 現在のネットワークプログラミング
  - クリアーテキストのパスワードなんて認証じゃない。暗号技術などを駆使するのは常識。複雑に関連したRFCなど標準ドキュメント沢山あるけどみんな読破して作ってね。
  - #しかし多くの場合、APIを呼ぶだけ。こうしたことは、誰かがやってくれていると思われている。。。。

Challenge PKIプロジェクトの活動履歴



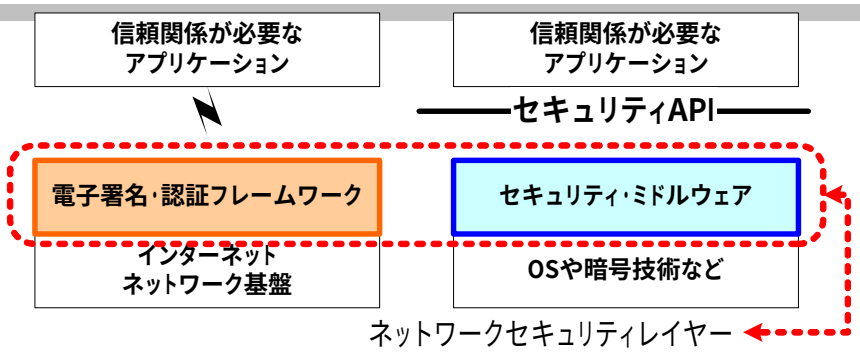
Challenge PKIプロジェクトの活動履歴(2)



Challenge PKIプロジェクトの目標と課題

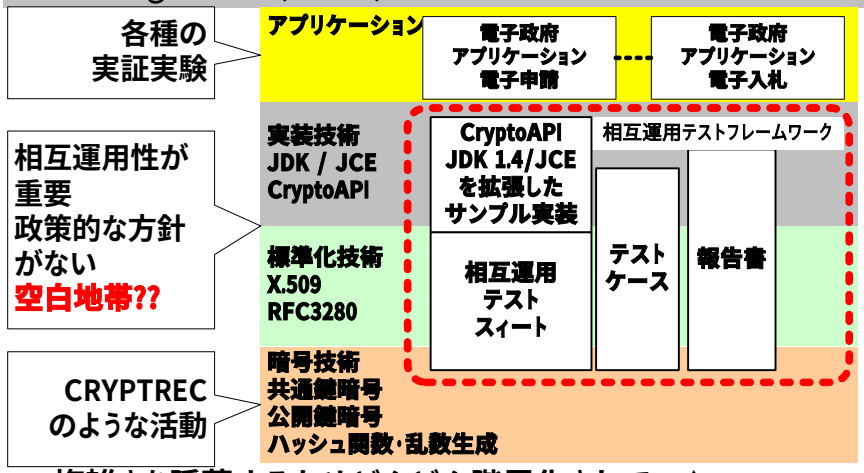
- プロジェクトの今後の目標
  - 実際に幅広く展開可能なセキュリティインフラの構築(= 幅広く相互運用可能なPKIの展開)
- 標準化の課題 (標準・実装から展開)
  - アイディアから仕様へ -> 多くの研究者が行っている
  - 仕様から標準、標準から実装 -> 学術系＆ベンダーなど
  - 標準・実装から展開 (相互運用) -> 誰が担うか
    - 標準と呼ばれる文書は山のようにある。しかし相互運用可能なものは極わずか…. これを解決して行かなければならない。
    - -> **ベストプラクティス**が重要。。。。ここに注力する。
- セキュリティフレームワークやミドルウェ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

セキュリティフレームワークやミドルウェア重要性



- 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。。。

セキュリテ・ミドルウェアの課題　その1
Challenge PKI (2002)のプロジェクトの範囲

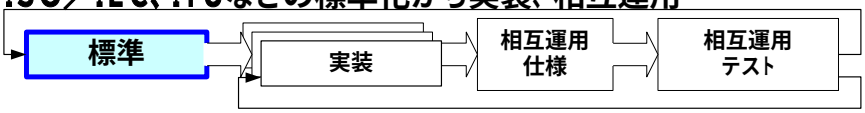


複雑さを隠蔽するためどんどん階層化されていく。。

このことが、問題の本質を分かり辛くしている！！

セキュリテ・ミドルウェアの課題　その2
標準化の課題（標準・実装から展開）

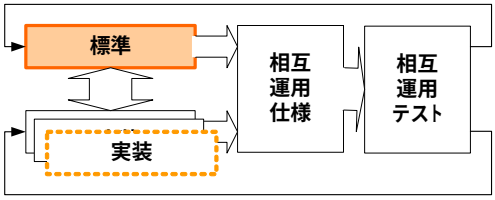
・ISO／IEC、ITUなどの標準化から実装、相互運用



・実装を伴わない現実味のない標準ができる可能性（OSIプロトコル ….）

・長い標準化期間&長いターンアラウンド（ドッグイヤー時代の標準化にそぐわない）

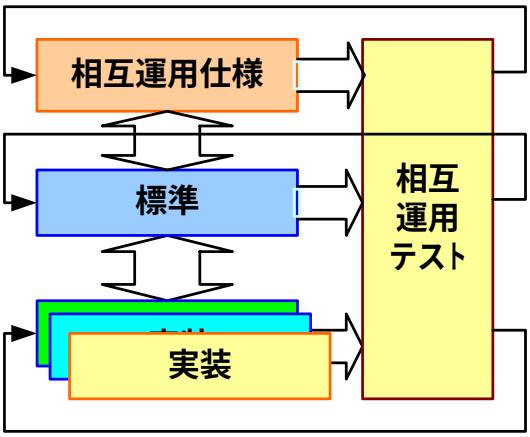
・IETFの標準化から実装、相互運用



・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….

セキュリテ・ミドルウェアの課題　その２
標準化の課題（標準・実装から展開）続き



- 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

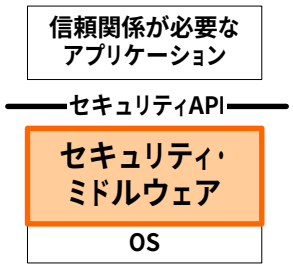
ユビキタスネットワーク時代には必須の
セキュリティ・ミドルウェアの課題

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

「セキュリティAPIセミナー」のメニュー

- 「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」
  - 東京大学先端科学技術研究センター　申吉浩
- 「Java JCE（Java Cryptographic Extensions）：機能と利用法」
  - 富士ゼロックス株式会社 稲田　龍
- 「.NET Crypto API：機能と利用法」
  - 株式会社オレンジソフト　澤野 弘幸
- 「IC カードなどのハードウェアトークンAPI」
  - 大日本印刷株式会社　半田　富己男
- 「バイオメトリクス認証の API」
  - セコム株式会社　松本　泰

エピローグ

- **よ〜くかんがえよぉ〜**
- 「セキュリティAPI」**は大事だよぉ〜**
- **るーるるーるるるー**