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

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

2005 年 6月 13日

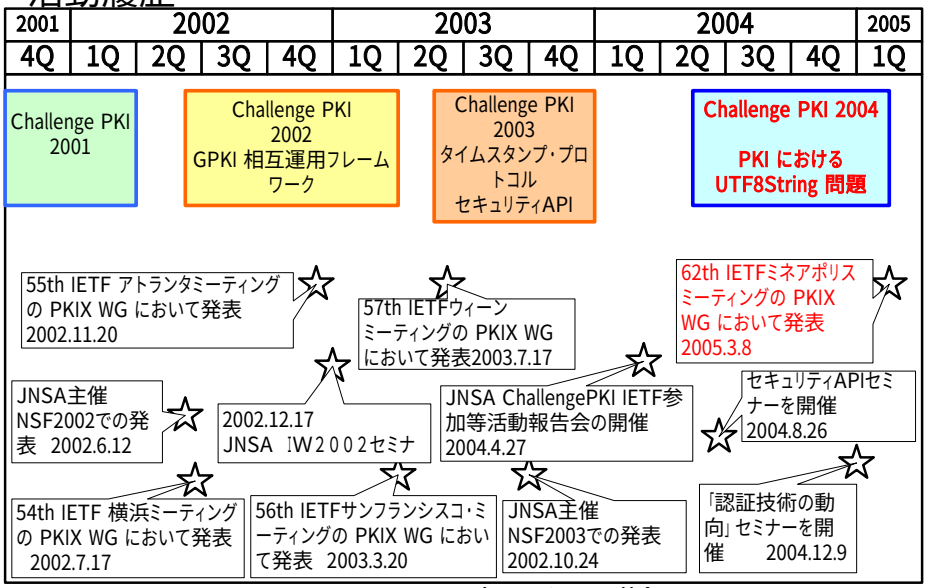
WG 成果報告会　PKI相互運用技術WG

- **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での活動等のChallenge PKIプロジェクトの活動概要と、IPAから公開されている、調査報告書（「PKI における UTF8String 問題に関する調査」）ついて報告します。**

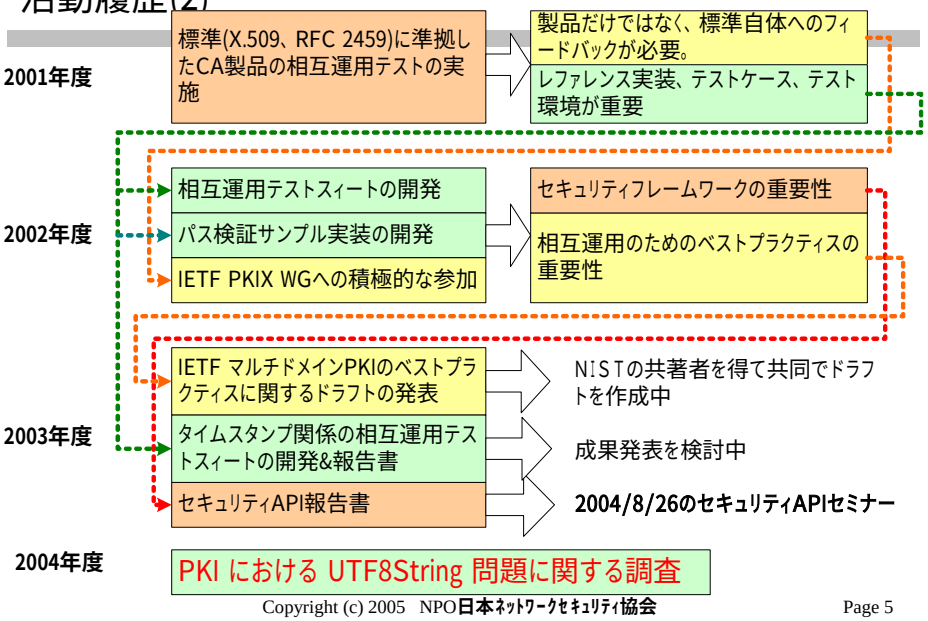
WG 成果報告会　PKI相互運用技WG

- Challenge PKIプロジェクトの活動
- PKI における UTF8String 問題
- 今後の課題

Challenge PKIプロジェクトの活動
活動履歴



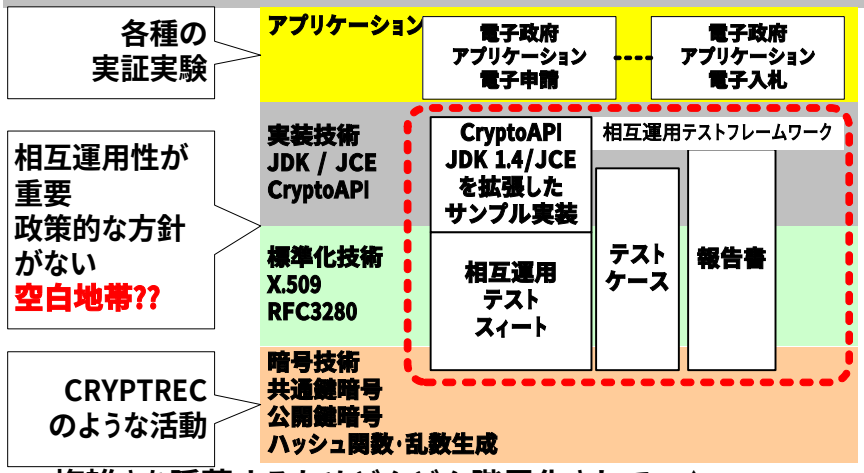
Challenge PKIプロジェクトの活動
活動履歴(2)



Challenge PKIプロジェクトの活動
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

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

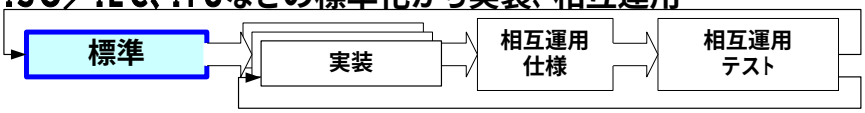


複雑さを隠蔽するためどんどん階層化されていく。。

このことが、問題の本質を分かり辛くしている！！

Challenge PKIプロジェクトの活動
標準化の課題（標準・実装から展開） Challenge PKI 2002

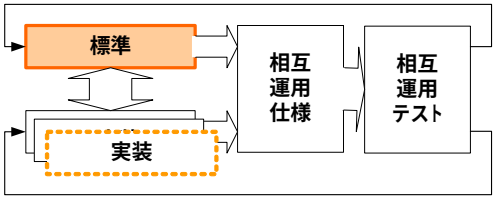
・ISO／IEC、ITUなどの標準化から実装、相互運用



・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)

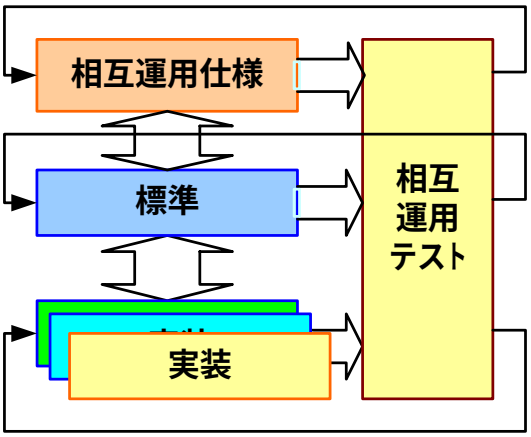
・IETFの標準化から実装、相互運用



・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

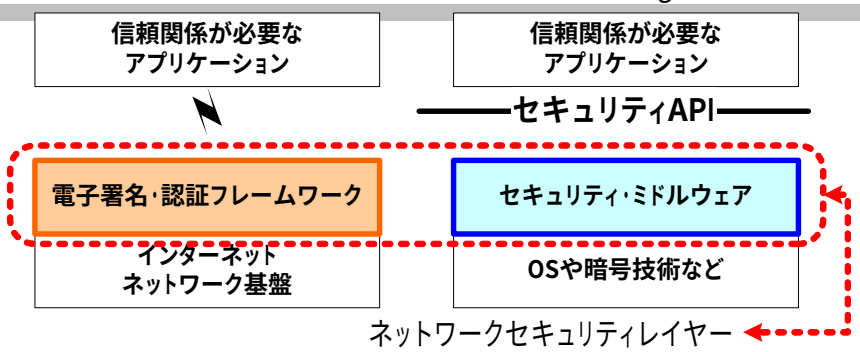
・複雑なセキュリティプロトコルに対していい加減な実装が蔓延してしまう….

Challenge PKIプロジェクトの活動
標準化の課題（標準・実装から展開） Challenge PKI 2002



- 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

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。。。

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

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

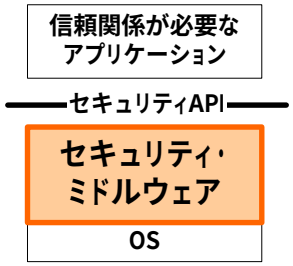
セキュリティに対応し切れていない標準化＆標準化組織

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。

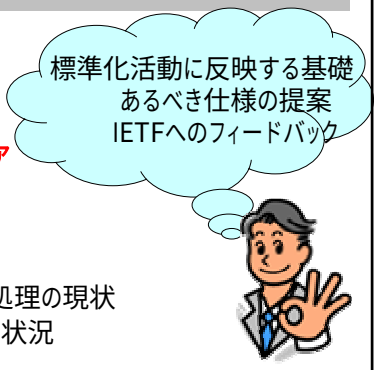
複雑さを隠蔽するために、どんどん階層化されていく。そのことにより本質的な問題点も隠蔽されていく??

複雑さと問題点が集約されていく

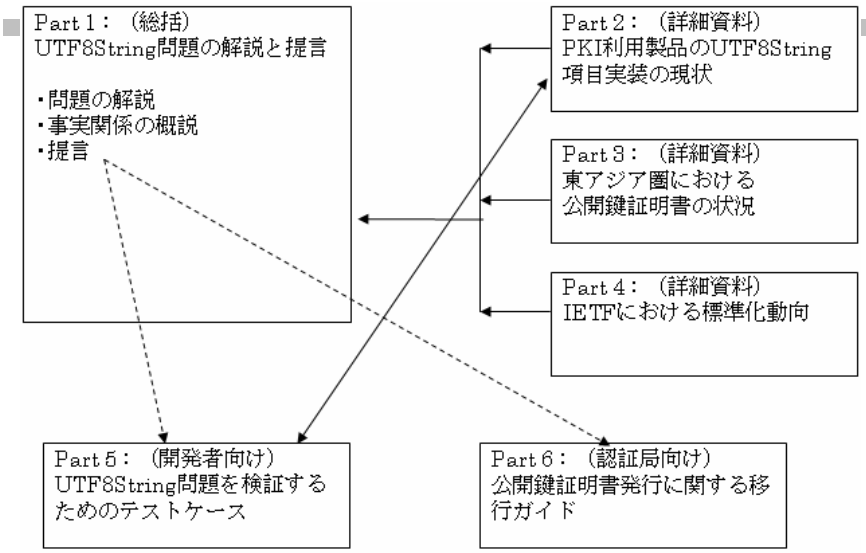
PKI における UTF8String 問題

PKI における UTF8String 問題に関する調査報告書

- 調査報告書の概要
  - 問題の公知化と論点の整理
    - 対象とする読者
      - **標準化団体に参画しているエンジニア**
      - **PKI 利用ソフトウェア開発者**
      - **認証局を運用管理している主体**
      - **政策当局**
  - PKI利用S/W製品におけるUTF8String項目処理の現状
  - 東アジア圏で発行されている証明書の項目の状況
  - IETFにおける標準化動向
  - 開発者向けのテスト仕様設計
  - 認証局向け移行指針の提言
- **調査報告書**URL
  - http://www.ipa.go.jp/security/fy16/reports/pki-utf8string/pki-utf8string.html



PKI における UTF8String 問題
報告書の構成



PKI における UTF8String 問題
UTF8Stringとは

- UTF8String
  - UTF-8でエンコードされた文字列を示すASN.1型。
  - 意味論的にはUTF-8と同義。
- UTF-8
  - UCS (Unicode Character Set) Transformation Format 8
  - Unicodeコンソーシアムが定義する文字セット(UCS-2やUCS-4) に対するエンコード方式のひとつ。
  - UCSは、世界中の全ての文字を一意なコードで表す文字セット。
  - RFC 3629としてIETFの文字コード標準のひとつとして採用されている。

PKI における UTF8String 問題
標準の問題 - RFC 3280

JNSA

RFC 3280

UTF8String への移行

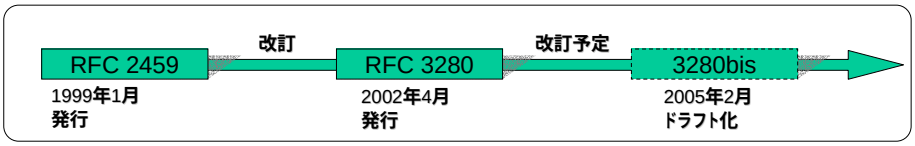
2003年12月31日以降に発行する証明書は全てUTF8Stringで エンコードされなければならない(とされていた。。。しかし現実には 移行されなかった。。)

*RFC 2459の遺産
*3280bisでは削除

要件定義

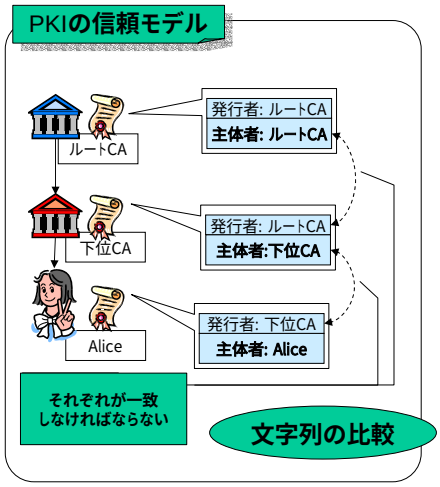
曖昧な記述、あるいは記述の欠如

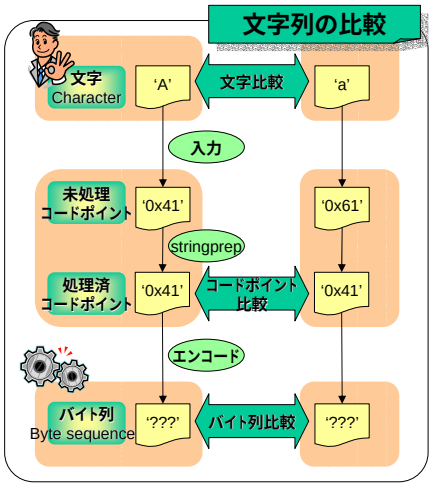
文字列比較、移行、証明書発行、アプリケーション



PKI における UTF8String 問題
PKIの信頼モデルとDNの比較

JNSA





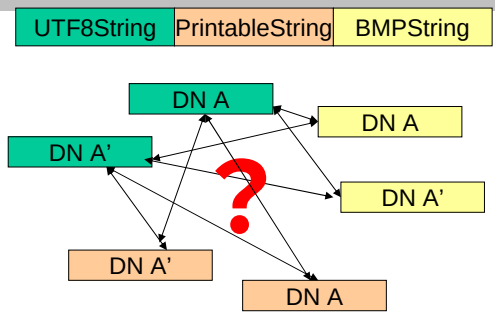
PKI における UTF8String 問題
様々な関係者 - 様々な悩み

- **標準仕様の策定者**の悩み
  - 「PKIの信頼モデルとDNの比較」の仕様の曖昧さを解消できていない
  - マイグレーションに対する指針を示せていない – 意見が集約できない。。。
- **CA (認証局) 運営者**の悩み
  - CAは、アプリケーションが対応しない限り、 UTF8Stringに対応した証明書を発行できない。。。移行できない。
- **PKIミドルウェア開発者**の悩み
  - 標準が曖昧で、マイグレーションを考えると複雑な実装になってしまう。
  - テストケースの不在
- **アプリケーションベンダー**の悩み
  - **PKIミドルウェア**頼み。悩みがないわけでもないが分からない。。。
- (電子政府などの)??の悩み
  - #理解していないので悩みはない。。。。???

PKI における UTF8String 問題
実装の問題 - UTF8String実装調査

- **対象**
  - Windows Application
  - Java API
  - OpenSSL Application
- **範囲**
  - DirectoryName

  の比較部分
- **内容**
  - **エンコードが異なるものを比較**
  - **微妙にデータが異なるものを比較**
- **方法**
  - **さまざまなDNを持つ証明書を用意**
  - **アプリケーションで検証**
  - **成功？失敗？**



同じ「文字」なのに、エンコードが違うだけで検証失敗するのはおかしい???

微妙に違う形の文字を同一視してしまうのはまずい???

PKI における UTF8String 問題
実装の問題 - UTF8String実装調査結果

	Windows・CryptoAPI	Java	OpenSSL
エンコード方式が違うと	一致しない	UTF8Stringと PrintableStringの比較では一致する。	一致しない
形が似ている文字を	一切同一視しない	いわゆる全角、半角を同一視する	一切同一視しない
ASCIIの大文字、小文字を	区別しない	区別しない	区別しない
アプリケーションごとの実装の差異	MS製のアプリではなし。OS バージョンによる差異もなし非MS製アプリでは差異あり		なし

単一の環境で完結していれば問題はない。しかし…

Javaアプリケーションで正しいとされた証明書が、Windowsアプリケーションではじかれてしまう？！

Windowsアプリケーションで異なる組織向けに発行された証明書なのにJavaアプリで同じ組織と思われてしまう？？？

PKI における UTF8String 問題
62nd IETF Meeting, ミネアポリス 2005.3.8

発表シーン

Tim Polk（NIST）：**NISTの電子認証ガイドラインの著者の1人**

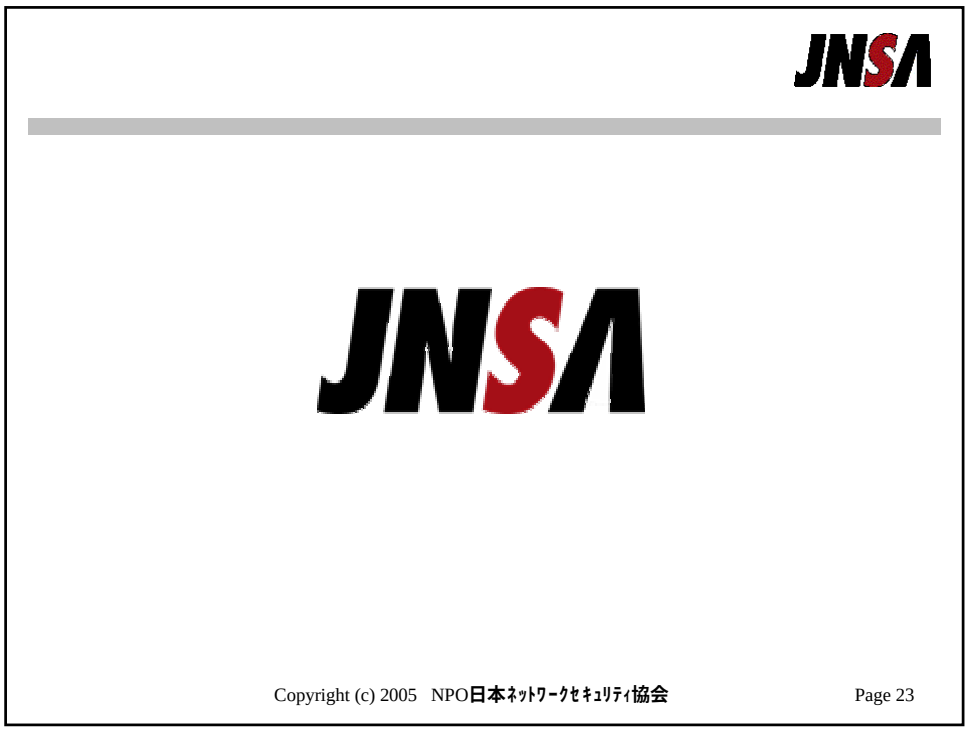
Steve Kent（BBN Tech.）

PKI における UTF8String 問題 62nd IETF Meeting, ミネアポリス (2)

- 内容
  - 問題概説、これまで、プロジェクトの説明
  - 東アジアでの状況
  - 進行中：移行プラン、テストケース
- 質問 from Stefan Santesson (Microsoft)
  - 3280bisではUTF8StringとPrintableStringの共存を認めた。
  - Q) にも関わらずPrintableStringからUTF8Stringへ移行する必要があるのであれば、教えてほしい。--Stefan
  - A) 名前比較規則を正しく設計し、実装がサポートするなら必要ない(No)。そうでなければ移行する必要がある(Yes)だろう。--Shimaoka

今後の課題

- 「PKI における UTF8String 問題」の解決はこれから
  - 標準へのフィードバック - 3280bisへのフィードバック
  - 政策(電子政府など)、実装、テスト、認証局、これらへの反映
- 似た問題 - SHA-1からの移行
  - CRYPTRECの見解 平成16年9月8日
    - ハッシュ関数SHA-1及びRIPEMD-160の安全性について
      - 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。
  - 現実の世界
    - IEの証明書リストにある107個の自己署名証明書
      - MD5(46個)、MD2(11個)、SHA1(50個)
    - 自己署名証明書の有効期間は、10年から20年
- どうやって移行するのか??誰が全体を取りまとめるか??
  - 政策担当者(電子政府など)、暗号関係者、アプリケーション開発ベンダー、認証局、PKI標準化関係者。。。これらの2者以上で会話することは極めて稀


JNSA
JNSA
Copyright (c) 2005 NPO日本ネットワークセキュリティ協会
Page 23