マルチドメインPKIと相互運用性のBCP (Best Current Practice)

2005/10/28 “PKI day”

Challenge PKI Project
セコム IS研究所
島岡 政基 shimaoka@secom.ne.jp

本日の概要

- イントロ
- マルチドメインPKIとは
- マルチドメインPKIの相互運用性
- Best Current Practiceへ向けてのコンセンサス作り

マルチドメインPKIイントロ

駆け足で。ちょっと乱暴に。

これまでのPKI相互運用の流れ

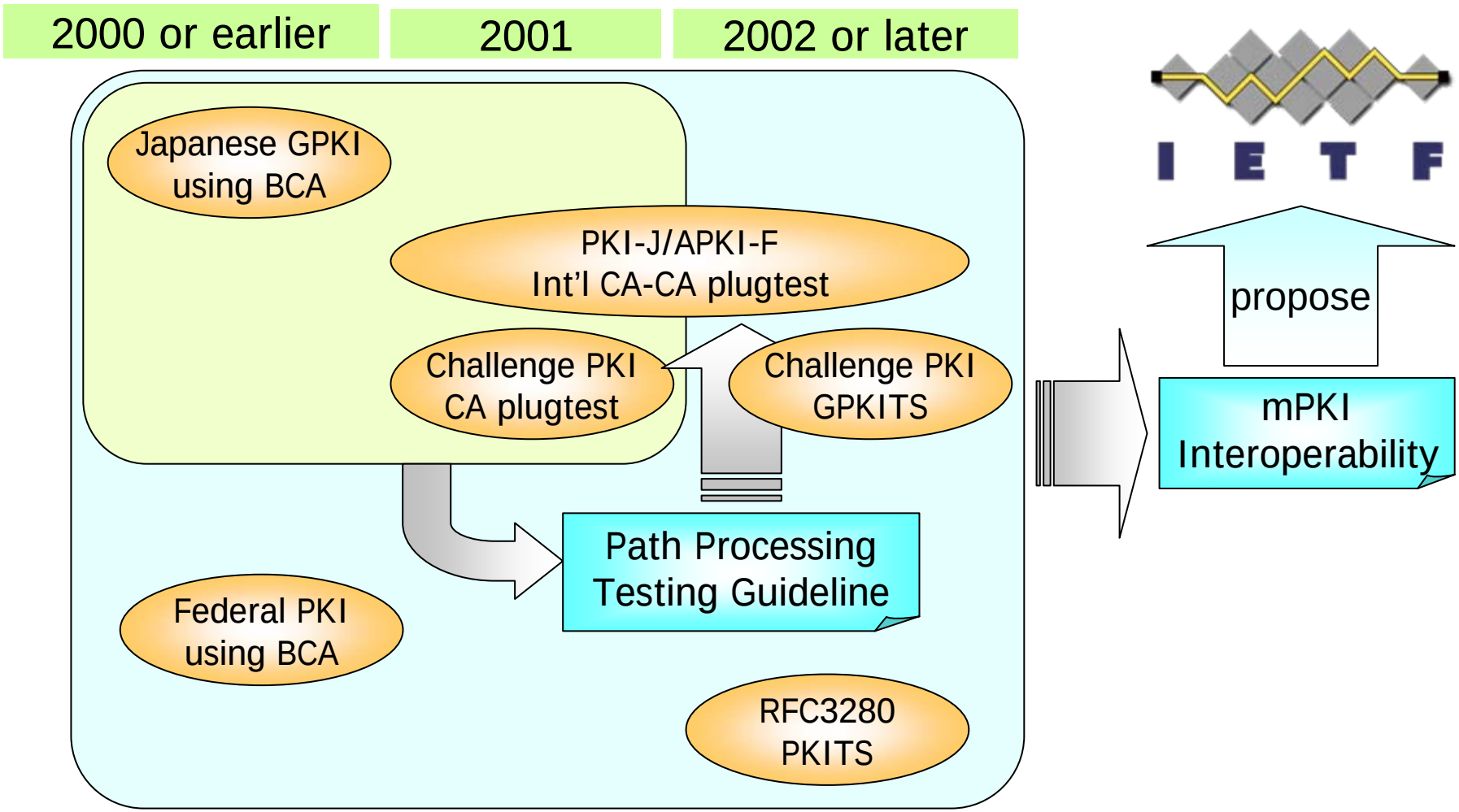
- 私の経歴とPKI相互運用イニシアチブ
  - 2000年～ 政府認証基盤(GPKI)
  - 2001年～ 日本PKIフォーラム 国際間相互接続実証実験
  - 2001年～ JNSA チャレンジPKIプロジェクト
  - 2004年～ NISTとの協働
  - 2005年～ 全国共同大学間連携認証基盤(UPKI)
    - 国立情報学研究所 特任助教授として従事
- これらの相互運用ノウハウを文書化し、Best Current Practiceとするべくietfへ提案中
  - ”Memorandum for multi-domain PKI interoperability”
  - 米NISTとの共同提案

なぜBest Current Practiceが必要なの?

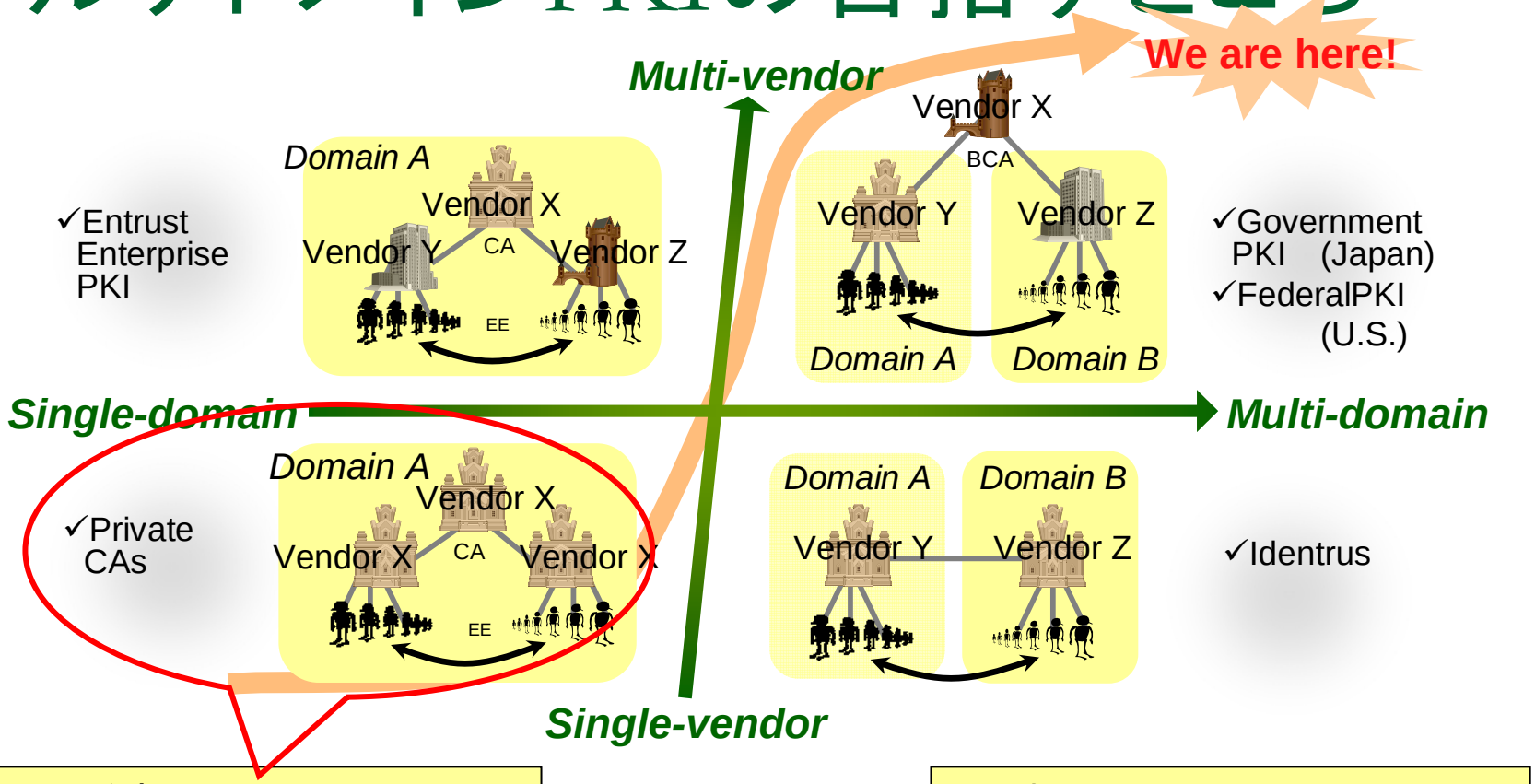
- Best Current Practiceって?
  - 現時点における最良の実践
  - 技術仕様だけでなく、相互運用性確保のために実績すべきことを示す文書が必要。

- 現状、PKIのBCPを発信する世界的な組織がない。
  - 以前はPKI Forumがあった。
  - IETFにおいてもPKIのBCPはまだ、ない。
- 世界的に(マルチドメインに)共有すべき問題。
  - 日本だけ、業界だけ、という閉じた問題ではない。
  - マルチドメイン問題を解決しようというのだから…
- まだほとんど誰も着手してない問題。
  - まず、できる人たちが少しずつ、ボトムアップで。
  - #トップダウンはそれから。

各PKI相互運用イニシアチブの関係



マルチドメインPKIの目指すところ



従来のInhouse PKI	技術的な相互接続性	これからのmulti-domain PKI
単一ベンダ、単一実装		複数ベンダ、複数実装
単一ドメイン、単一ポリシ	ポリシも含めた相互運用性	複数ドメイン、複数ポリシ

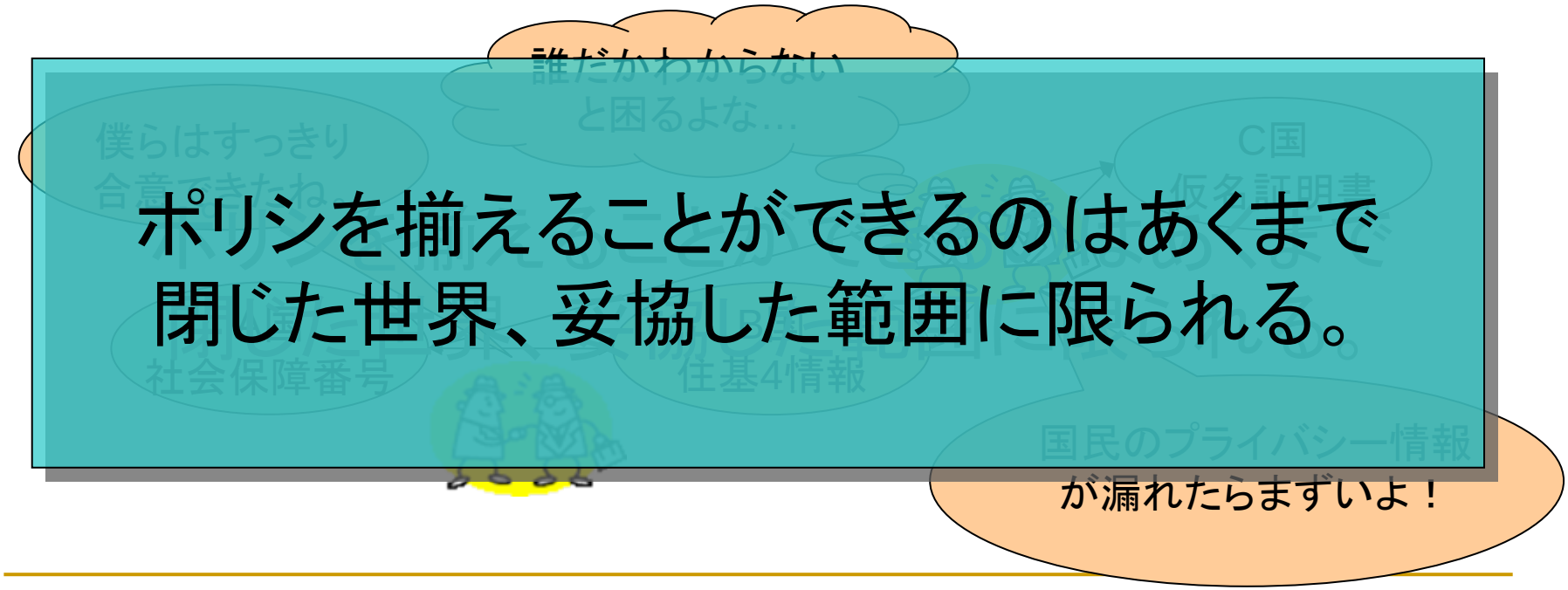
マルチドメインPKIとは?

PKIドメインとマルチドメインPKI

- マルチドメインPKIとは、
  - 読んで字の如く「PKIドメインの集合」。
  - PKIドメインをまたぐ信頼関係を築くこと。
- では「PKIドメイン」とは?
  - あるポリシの管理下で運用されるPKIの単位
  - 典型例としてInhouse PKI。
    - 一定のポリシ下で設計・運用管理されるPKI。
    - かみ合わないポリシが入り乱れることはない。
    - # マルチドメインではこれが難しい。

マルチドメインPKIの課題

- PKIドメインをまたぐ信頼関係を必要とする。
- PKIドメイン毎の様々なポリシを評価する必要がある。
  - ドメインが異なれば、当然ポリシも異なる。



ポリシを揃えることができるのはあくまで
閉じた世界、妥協した範囲に限られる。

PKIに限らないマルチドメイン問題

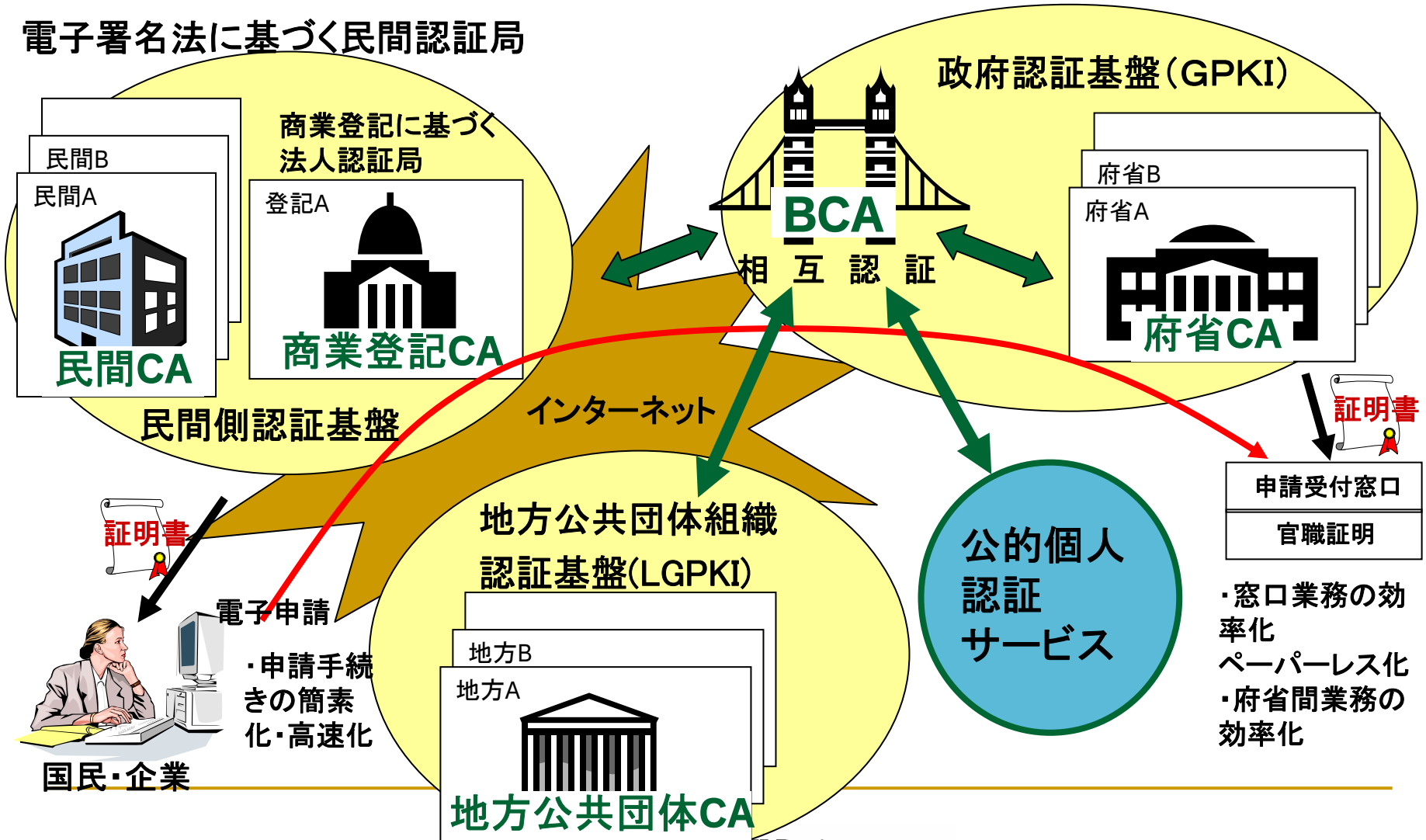
- 国際化ドメイン名とUnicode問題
  - http://日本語.jp/など。
  - アラビア語などbi-directionalな表記もある。
  - Unicodeの正規化問題も解決しないといけない。
  - 日本語だけ解釈できるブラウザでも…じゃダメ!!
- 複数企業が係わる大規模プロジェクトの管理
  - 横断的なスケジュール管理、データのやり取り
  - 個々の企業の異なるセキュリティポリシ
  - どこのリソースを使って情報共有するか?

マルチドメインとは、異なるポリシを持つ組織を連携させること。

事例(1) 政府認証基盤(GPKI)

- 国内で最初の本格的なマルチドメインPKI
  - 府省(各府省認証局)
    - 異なるポリシに柔軟に対応できるよう設計
    - 実際には、ブリッジ認証局とマッピングする共通ポリシのみ
  - 民間(特定認証局)
    - 電子署名法の厳格な認定基準
    - 事業者毎のポリシは、利用者からみればわずかな違い
- その他、地方自治体認証基盤(LGPKI)、公的個人認証サービスとも相互接続
- 海外との相互接続?
  - 米:Federal PKI、カナダ:GoC PKI、欧州:Bridge-CA(?)
  - アジア:韓国、シンガポール、台湾、タイ

GPKIを軸に展開されるマルチドメインPKI



マルチドメインPKIと相互運用性

他とのポリシの違いを明確に示せること

典型的な信頼モデルが確立されること

ポリシの違いを具現するには…

	要件	提案
信頼モデルの整理	●信頼関係を築く主な手法 トラストリスト、相互認証など	● PKIにおける信頼関係を整理 ● PKIドメインの定義
	●PKIの典型的信頼モデル 階層モデル、ブリッジモデルなど	●シングルドメインPKIのモデル定義 ● マルチドメインPKIのモデル定義
認証パスの要件	● ポリシの違いを正しく表現 ● 他ドメインからの認証パス構築 リポジトリの運用、CRLDP/AIA拡張など	● 認証パスをデザインする時の注意点 ● 認証パスを検証する時の注意点

提案中のInternet-Draftの目次

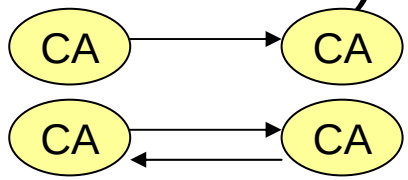
- 1 Introduction
- 2 Requirements and Assumptions
- **3 Trust Relationship**
  - 3.1 Operation based Trust Relationship
  - 3.2 Certificate based Trust Relationship
- **4 PKI Domain**
- **5 Single-domain PKI**
  - 5.1 Single CA PKI model
  - 5.2 Hierarchy PKI model
  - 5.3 Mesh PKI model
- **6 multi-domain PKI**
  - 6.1 Multi Trust point model
  - 6.2 Single Trust Point model
- 7 Operational Considerations
- 8 Security Considerations
- 9 References
- 10 Acknowledgements
- 11 Author's Address
- 12 Full Copyright Statement

信頼モデルの整理

- **PKIにおける信頼関係**
  - 運用ベースのトラストリストモデル
    - User Trust List
    - Authority Trust List
  - 証明書ベースの相互認証モデル
    - 片側相互認証、双方向相互認証
  - 最も典型的な従属(階層)モデル
- **PKIドメインの定義**
  - PKIドメインとしての要件
  - 相互運用性の高いPKIドメイン

PKIにおける信頼関係

- 運用ベースのトラストリストモデル
  - User Trust Listモデル
    - EE自身がトラストポイントのリストを管理する
    - 柔軟だが野放図な信頼関係
  - Authority Trust Listモデル
    - 第三者がトラストポイントのリストを管理する
    - 厳格な信頼関係
- 証明書ベースの相互認証(Cross-certification)モデル
  - 片方向(unilateral)相互認証モデル
  - 双方向(mutual)相互認証モデル



- 従属モデル
  - トポロジとしては階層だが、下位CAは自己署名証明書を持たない。

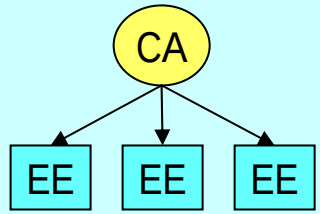
PKIドメインの定義

- PKIドメインの要件
  - ドメインポリシを持っていること
    - ドメイン内で共有する一つ以上のポリシ
  - ドメインを代表するPrincipal CAがいること
    - 他のドメインと相互接続するためには明確であるべき
- 相互運用性を確保するために…
  - ネームスペースの管理
  - 明示的なドメインポリシ
  - パス検証パラメータの明確化
  - 証明書情報の公開・配布

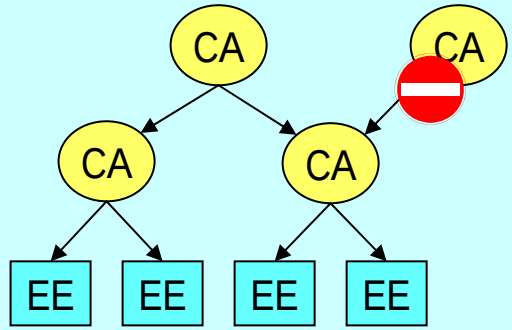
これらが曖昧だと、他ドメインとの違い(ポリシの違い)を明確にできない。
つまりPKIドメインとしては信頼してもらえない。

シングルドメインPKIのモデル定義

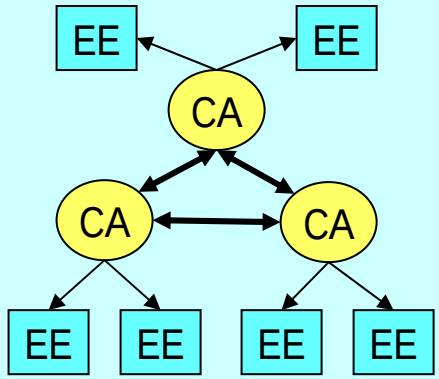
- シングルPKI
  - 単一CAモデル



- 階層PKI(Subordination)
  - いわゆる階層モデル
  - 唯一のTopCAと複数の下位CA
  - 下位CAは、複数の上位CAを持ってはいけない(厳密階層)。

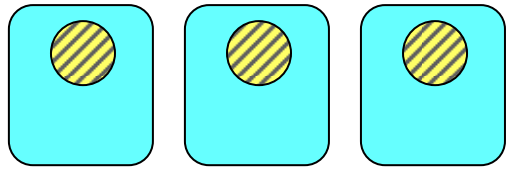


- メッシュPKI(Cross-Certification)
  - 複数のCAが相互に相互認証している。

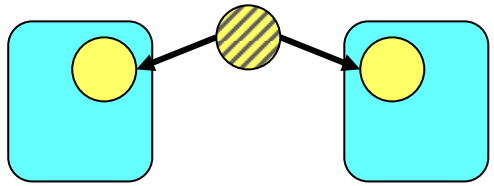


マルチドメインPKIのモデル定義

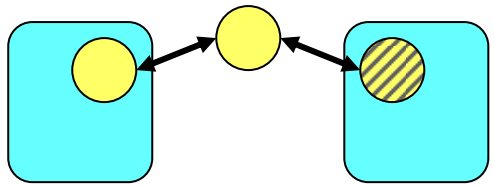
- マルチトラストポイントモデル
  - User Trust List
  - Authority Trust List



- シングルトラストポイントモデル
  - Unified Domain Model



  - Bridge Model



認証パスにおける要件

- 認証パスをデザインする時の注意点
  - ポリシを明確にするための証明書プロファイル
    - 証明書ポリシ: certificatePolicies, policyMappings
    - 制約拡張: nameConstraints, policyConstraints, etc.
  - 証明書情報を明示的に公開･配布するための証明書プロファイル
    - AuthorityInformationAccess, cRLDistributionPoints, issuingDistrubutionPoint
- 認証パスを検証する時の注意点
  - トラストポイント
  - 認証パス検証パラメータ

マルチドメインPKIの相互運用性

- マルチドメインPKIを確立するために
  - 他ドメインとのポリシの違いを明確に示せること
    - ドメインXとドメインYのポリシが違うことが明確にわからなければならない。
- マルチドメインPKIを普及させるために
  - 典型的な信頼モデルが確立されること
    - 柔軟すぎるアーキテクチャを使いこなすのは難しい。
    - マルチドメインPKIを構築する上でのユースケース、お手本が必要。

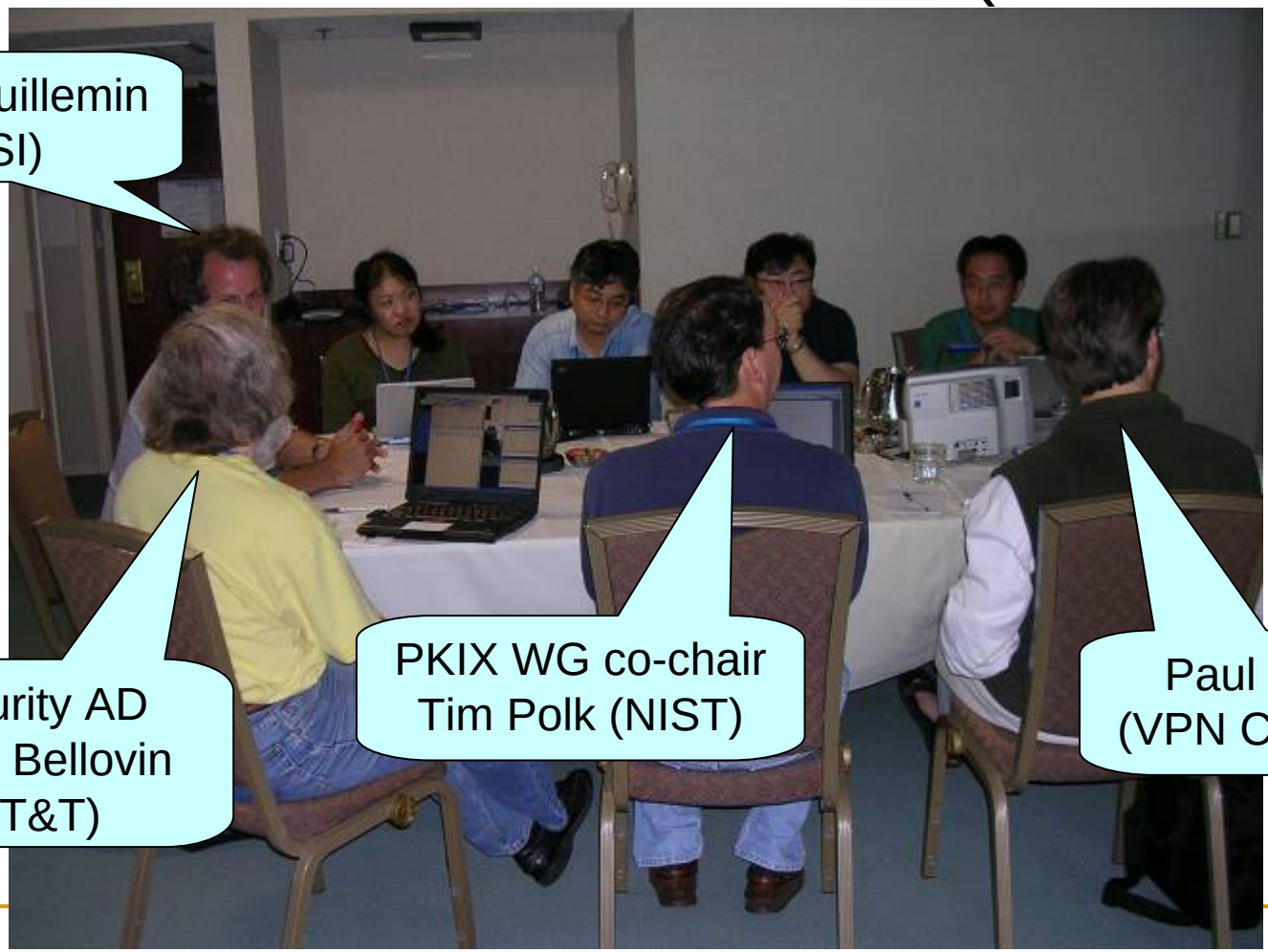
Best Current Practiceの
コンセンサス作り

IETFへのInternet-Draft提案

- 2003/07 PKIX WG in 57th IETF(ウィーン)

IETFでのコンセンサス作り

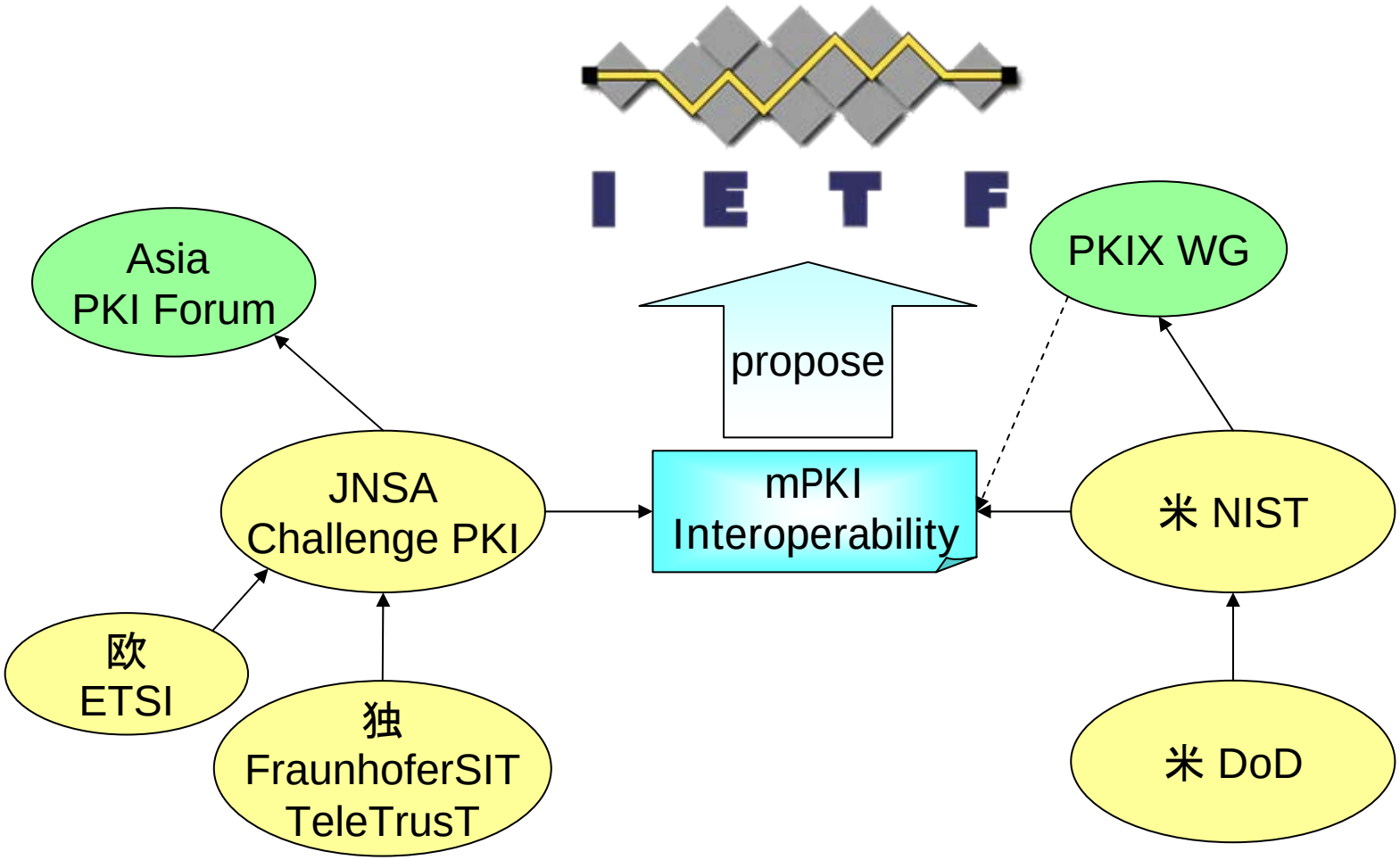
- 2004/08 有識者レビュ60th IETF(サンディエゴ)



米NISTから共著者をリクルート

- 2004/09 Nelson Hastingsを共著者に。

コンセンサス作りのプレイヤー



これからの展開

- Internet-Draft: IETFへの提案
  - 米DoD(国防省)からのレビュコメント
    - Federal PKIの中でもう一つのブリッジCAを運用している。
- その他PKIに関連するマルチドメイン問題
  - UTF8String移行問題
    - 文字コード屋さん、アプリ屋さん、CA屋さん、の三つ巴…?
  - SHA-1危殆化問題
    - 本質的には違うが、移行運用については該当する。
    - PKIの中ではUTF8String問題に限りなく近い話。
- 新たなマルチドメインPKIの事案
  - 大学間連携のための全国共同電子認証基盤(UPKI)

参考情報

UPKIの紹介

関連URI

大学間連携のための全国共同電子認証基盤（UPKI）構築事業

- 目的
  - 大学が有する教育研究用計算機，電子コンテンツ，ネットワークを安全・安心に有効活用するための電子認証基盤の構築
- 7大学とNIIの連携
  - 大学内・大学間認証基盤の国家的なモデル作り
    7大学：大学内認証基盤 ＋（地域）
    NII　：大学内認証基盤の相互接続
- 効果
  - 大学間の相互認証
    → 教育・研究資源、コンテンツの有効活用（単位互換、e-learning応用）
  - メール内容などの暗号化 → 情報漏洩の防止
  - 電子認証・電子署名
    → 電子決済・電子回覧による効率化，
    フィッシング対策などセキュリティ強化
  - ネットワークローミング → 無線LAN，公衆Web端末
  - グリッドコンピューティング
    → 7大学スパコンリソースをCSI上に統合

関連URL(1)

- JNSA Challenge PKI プロジェクト
  - http://www.jnsa.org/mpki/
- Internet-Draft
  - http://www.ietf.org/internet-drafts/draft-shimaoka-multidomain-pki-05.txt
- PKIX WG発表資料(57th IETF@Vienna)
  - http://www.ietf.org/proceedings/03jul/slides/pkix-9/index.html
- PKI 関連相互運用性に関する調査報告
  - Challenge PKI 2001成果物
  - http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.html
- GPKI相互運用テストスィートの開発
  - Challenge PKI 2002～2003成果物
  - http://www.ipa.go.jp/security/fy14/development/pki/interop.html
  - http://www.ipa.go.jp/security/fy15/development/pki_interop/index.html

関連URL(2)

- 政府認証基盤(GPKI)
  - http://www.gpki.go.jp/
- 米NIST PKI Home
  - I-Dの共著者であるNelson Hastingsが担当者
  - http://www.csrc.nist.gov/pki/publickey.html
- 大学間連携の全国共同電子認証基盤(UPKI)
  - TBD
- セコムIS研究所 サイバーセキュリティ読本
  - http://www.secom.co.jp/isl/j/cs_reader/

ご意見･ご質問

Challenge PKI プロジェクト

セコム IS研究所

島岡 政基 shimaoka@secom.ne.jp