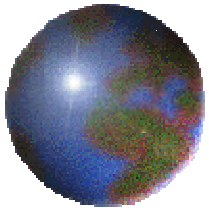


マルチドメインPKI - 日本発のPKI相互運用性標準
～なぜ我々が標準化を主導したのか?～

島岡　政基
セコムIS研究所
Challenge PKIプロジェクト

Challenge PKI Project
The Multidomain PKI Interoperability Framework

Challenge PKI プロジェクト

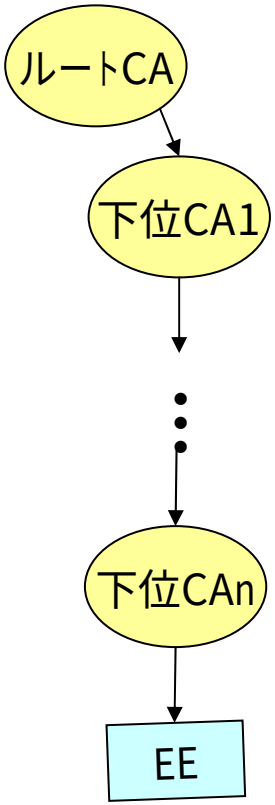
- PKIの相互運用実験(2001)
  - PKI相互運用性の問題点を明らかにする
  - 複数CA間の信頼確立
  - アプリケーション間の相互運用

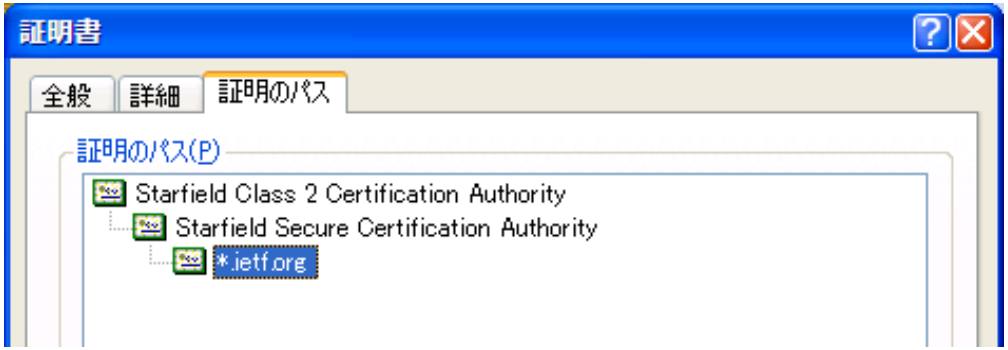
9つのCA製品
階層、相互認証、ブリッジ
SSL/TLS, S/MIME, IPsec

- PKI相互運用テストスィートの開発(2002～2003)
  - PKIアプリ開発に必要な様々なテストデータをWebベースで生成･管理
  - 認証パス構築･検証環境の生成
  - LDAP、OCSP、CVS(GPKI)、タイムスタンプをサポート
- 各種PKI技術の調査研究
  - タイムスタンプ
  - UTF8String問題
- マルチドメインPKIの相互運用に関する標準化
  - RFC 5217: Memorandum for multi-domain PKI interoperability

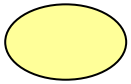
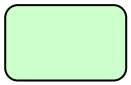
古典的なPKI: 階層型PKI

- 自己署名証明書を持つルートCA　(トラストアンカ)
- 上位CA(ルートCA)から発行された証明書を持つ下位CA
- 非常に理解しやすい ＝ 疑念が生じにくい
  - SSL/TLSでもお馴染み!?



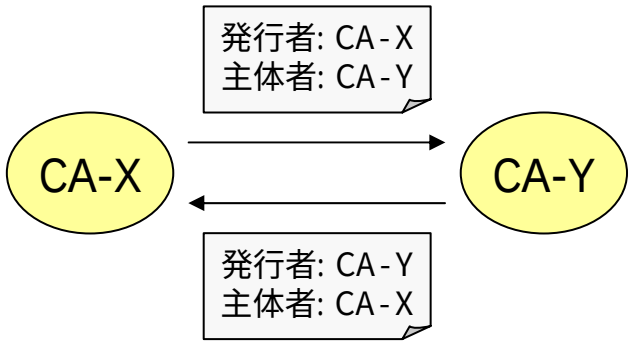


凡例

記号	解説
	認証局(CA)
	エンドエンティティ
	PKIドメイン
A→B	AからBに証明書を発行
A⇢B	AがBをトラストアンカとして信頼

横断(相互)認証: Cross-Certification

- CAが、別のCAと相互に信頼しあう
  - 相互に横断証明書(Cross-Certificate)を発行

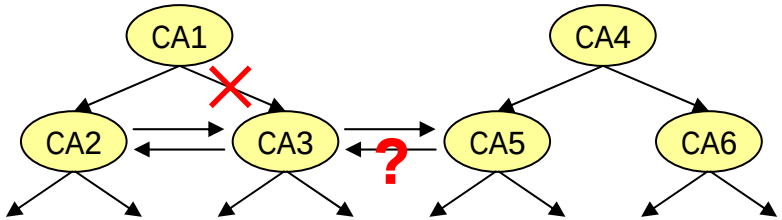


- これ自体はごくごく単純な定義。

横断認証が複雑さを加速。。。

- 双方向(Mutual-)横断認証と片方向(Unilateral-)横断認証
  - 下位CA証明書も片方向横断証明書の一種
- CAトポロジはツリーからグラフへ
  - メッシュ型PKIやブリッジ型PKIなど
- 信頼モデルも複雑に
  - 下位CA同士の横断認証?
  - 横断認証先のCAが上位CAから失効されたら?

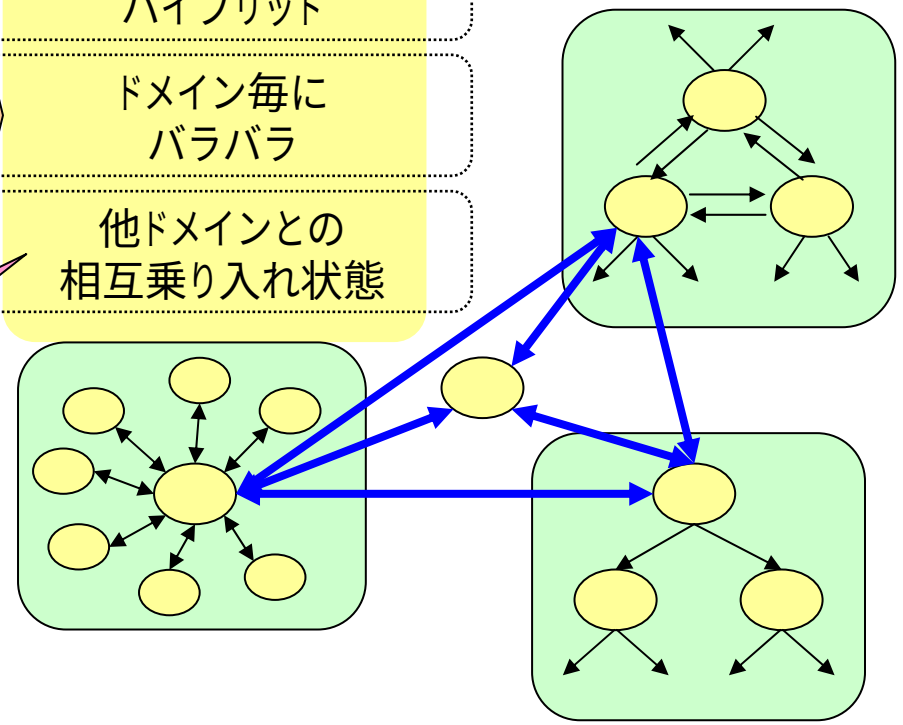
実装(認証パスの構築・検証)もいっそう複雑に。。。



PKIのマルチドメイン化

	典型的なシングルドメインPKI	マルチドメインPKI化が進むと…
アーキテクチャ:	階層型または単層型	ブリッジ型や階層型のハイブリッド
CP/CPS:	全CA共通または上位のサブセット	ドメイン毎にバラバラ
利用者:	ルートCAを直接信頼する利用者のみ	他ドメインとの相互乗り入れ状態

「オレオレ運用」では通用しなくなることを意味する



PKIにおけるマルチドメイン問題

- マルチドメイン問題: (セキュリティ)ポリシの多様性によって生じる組織間連携の障壁
  - CP/CPSはセキュリティポリシの一種
  - ポリシは組織によって様々 → CP/CPSも様々

多様なCP/CPSをアセスメント/マッピングすることさえできれば解決するのか?

- アセスメント/マッピングガイドライン作りは文脈に大きく依存する。
  - 業界の種類によって準拠法が異なるなど
- アセスメント/マッピング以前に解決しておくべき課題がいくつかある。
  - そもそもドメインを識別する属性情報(識別子)がない
  - どのような信頼モデルを構築すればよいのか、リファレンスがない

ドメイン内では自明だったことも、バックグラウンドの異なる他人同士が相互接続する際には明文化しておく必要がある

相互運用実現へ向けての課題

- 設計上の課題(認証局)
  - 複雑化する信頼モデルの整理
- 実装上の課題(アプリケーション)
  - 複雑化した認証パスの構築・検証
- 運用上の課題(認証局)
  - 異なるドメインを信頼する要件の確立

基本的な
考え方のみ

RFC 5217
マルチドメインPKI相互運用性に関するメモ

1. はじめに
2. PKIの基礎
3. PKIドメイン
4. PKI外部の信頼関係
5. 用語
6. セキュリティ考察
7. リファレンス

1. はじめに

1. 文書の目的
2. 文書の構成

1.1. 文書の目的

- マルチドメインPKIに関連する用語の概念の確立と相互運用要件を定義
  - 信頼モデルの整理
  - PKIドメインという概念の導入
  - 設計と実装上の考察
  - 信頼関係を確立する上での考察

2. PKIの基礎

1. 基本用語
2. CA間の関係
3. PKIアーキテクチャ
4. PKIとリライングパーティの関係

2.1. 基本用語

- 証明書ポリシ文書
  - 証明書の発行･管理に関する規程
  - 規程に紐付くポリシOIDを定義する(複数可)
- ポリシOID
  - 証明書の発行管理に関する規程を示す識別子
  - 証明書ポリシ文書の中で定義される
- リライングパーティ
  - 証明書を信頼するエンティティ(利用者)

「証明書ポリシ」は、文書とOIDいずれを指すのか文脈によって異なるため、個別の語句として定義

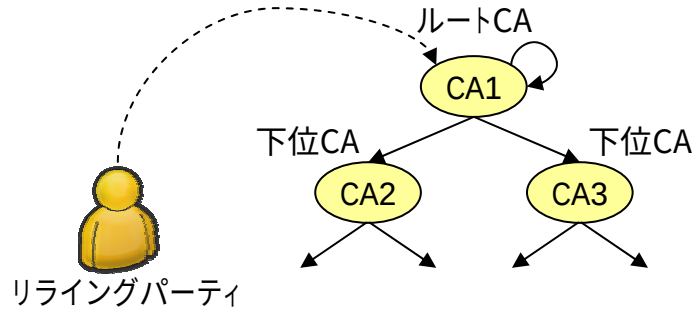
「○○認証局　証明書ポリシ」

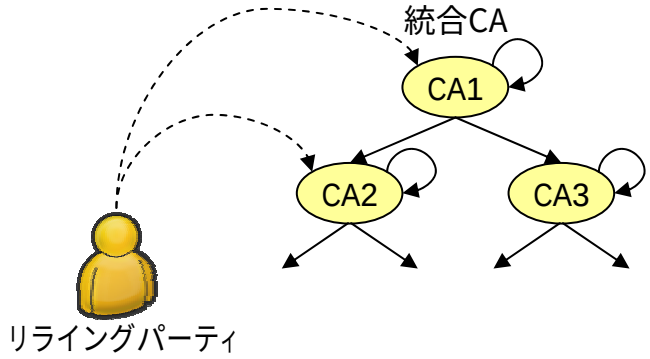
- 1.2. 文書の名前と識別
  - 本CPの正式名称は、「○○認証局　証明書ポリシ」という。
  - 本CPでは、○○認証局が扱う二種類のポリシ(○○ポリシXと○○ポリシY)について規定する。各ポリシのOIDは以下の通りである。

ポリシ名	ポリシOID
○○ポリシ-X	1.2.392.xxx.1
○○ポリシ-Y	1.2.392.xxx.2

2.2. CA間の関係

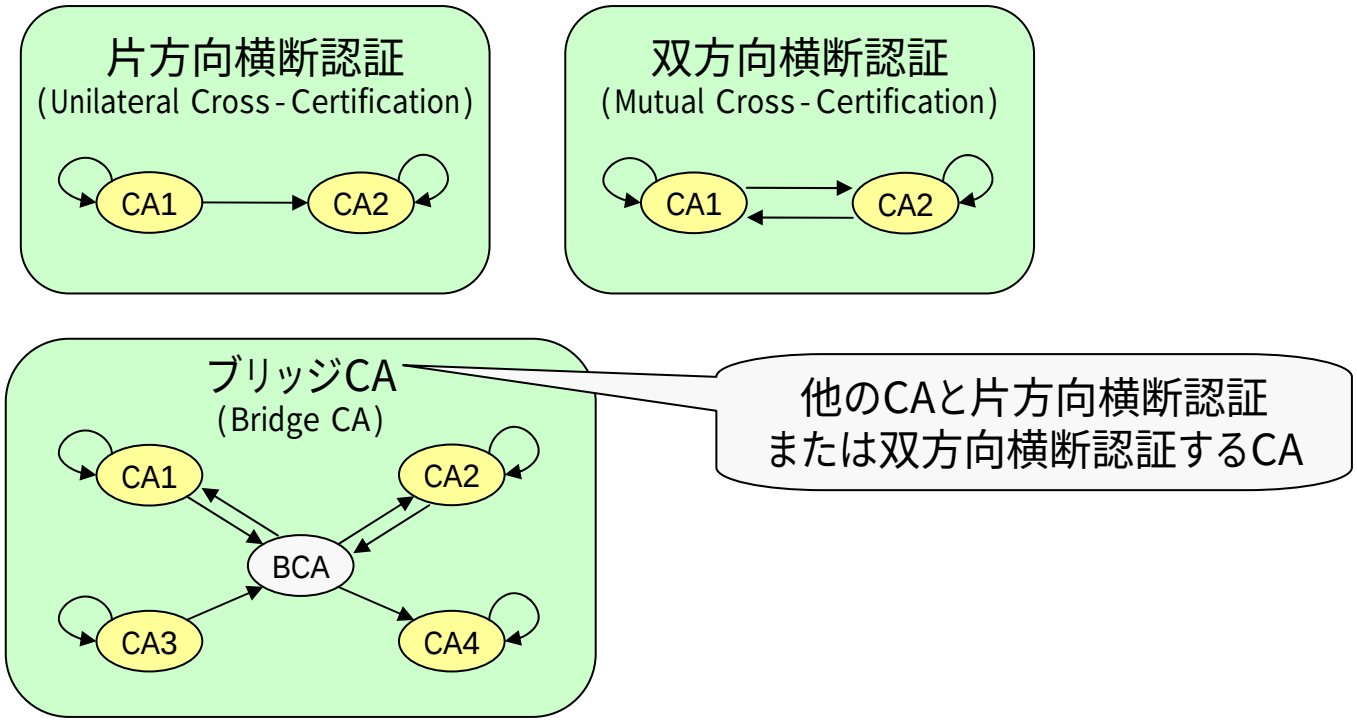
- 階層型CA関係
  - 下位CA: トラストアンカとして用いることを明確に禁止
  - トラストアンカになり得るCAは下位CAと呼ばない。
  - 自己署名証明書を持つCAに対する上位CAは、ルートCAではなく「統合CA(Unifying CA)」と呼ぶこととする。





2.2. CA間の関係（続き）

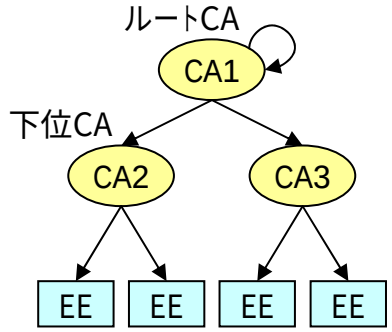
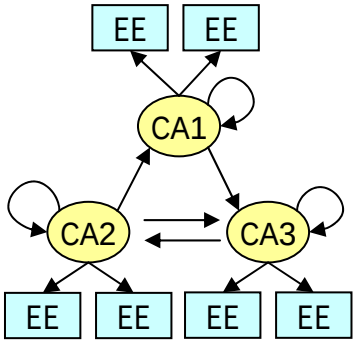
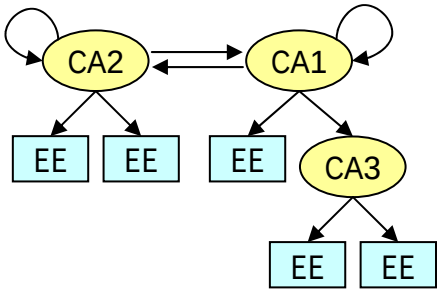
- ピアツーピアCA関係



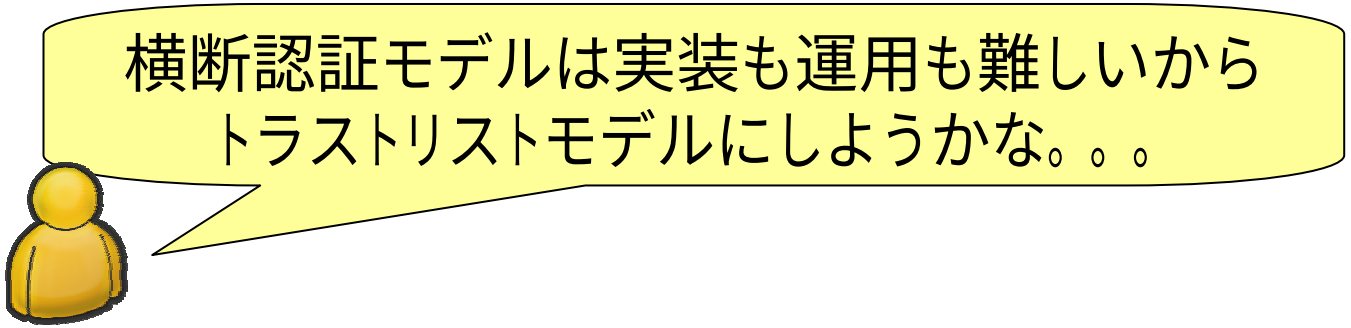
2.3. PKIアーキテクチャ

- 用語の定義
  - PKI
    - 同じ証明書ポリシ文書に基づいて運用されるCAシステム
  - Principal CA(PCA)
    - 他のPKIのPCAに、横断証明書を発行するCAとして指定される、自己署名証明書を持つCA
    - 他のPKIのPCAから、横断証明書を発行されるCAとして指定される場合がある

2.3. PKIアーキテクチャ（続き）

	階層型	メッシュ型	ハイブリッド型
			
定義	唯一のルートCAと、複数の下位CAで構成される。 下位CAは複数の下位CAを持つことができる。	相互に横断証明書を発行する複数のCAで構成される。いずれも自己署名証明書が必要。	階層型とメッシュ型の混合で構成される。
トラストアンカ	ルートCA	加入者: 発行者CA 利用者: 任意	自己署名証明書を持つ任意のCA
PCA	ルートCA	任意、ただし複数不可	任意、ただし複数不可

2.4. PKIとリライングパーティの関係



- アプローチとしては近いがアーキテクチャは全く異なる
  - 横断認証はCA-CA間の信頼モデル
  - トラストリストはリライングパーティ-CA間の信頼モデル
- トラストリストはPKI間の信頼関係に何ら影響しない
  - リライングパーティが勝手に複数のドメインを信頼するだけ

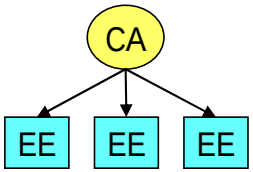
→2章・3章の範囲外として4章に記述。

補足: 信頼関係の違い

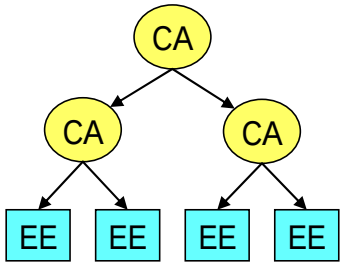
CA - CA間の信頼関係

CA - EE間の信頼関係

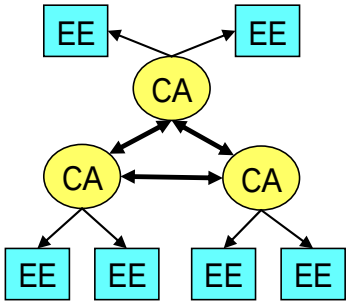
シングルPKI



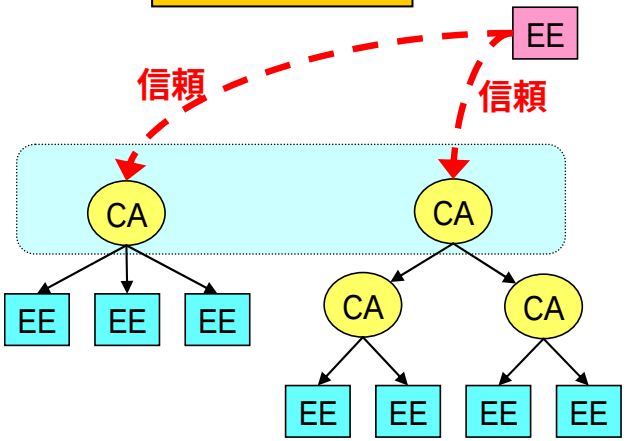
階層PKI



メッシュPKI



トラストリスト



CA同士は他に誰が
信頼されているのか
把握していない

3. PKIドメイン

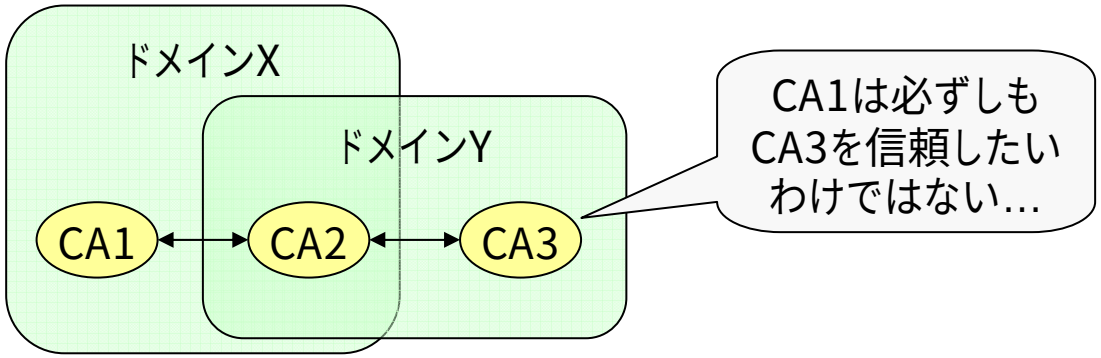
1. PKIドメインの属性
2. PKIドメイン要件
3. PKIドメインモデル
4. 運用考察

3. PKIドメイン

- PKIドメイン
  - 横断証明書によって信頼関係を持つ複数のPKIの集合。
- ドメインポリシOID
  - PKIドメイン全体で共有されるポリシのOIDであり、ドメインを識別するために用いられる。
  - ドメイン内の各CAは、このドメインポリシに準拠する。
  - 各CAはドメインポリシOIDに加えて独自のポリシOIDを持ってもよいが、双方に準拠する必要がある。

3.1. PKIドメインの属性

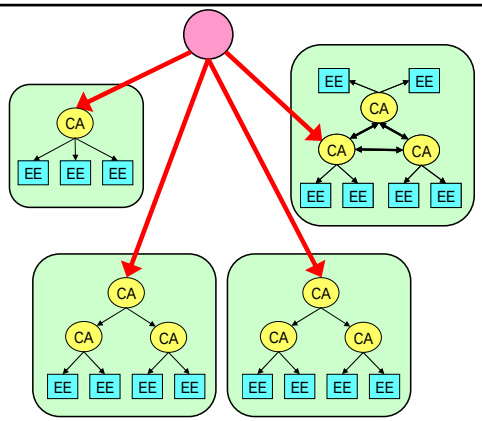
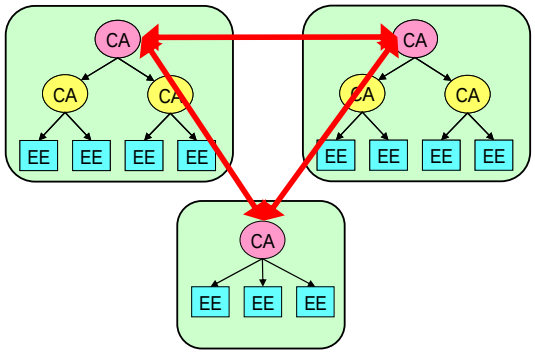
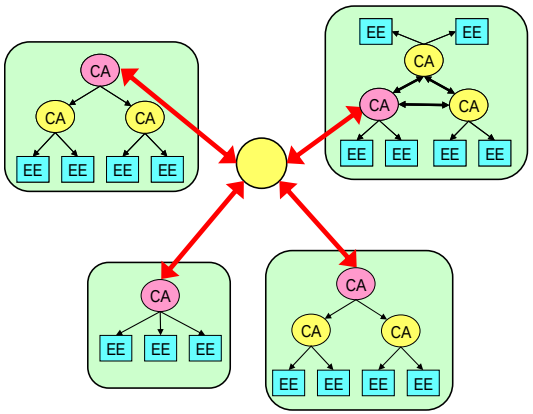
- 一つのPKIは複数のPKIドメインに所属することができる。
- PKIドメインは、別のPKIドメインを含むことができる。
- 複数のPKIドメインが信頼関係を確立して、新たなPKIドメインを確立することができる。
  - 旧ドメインとの併存、移行いずれも可。
- PKIは、同じドメイン内のPKIに対して信頼を制限・禁止することができる。



3.2. PKIドメインの確立・参加要件

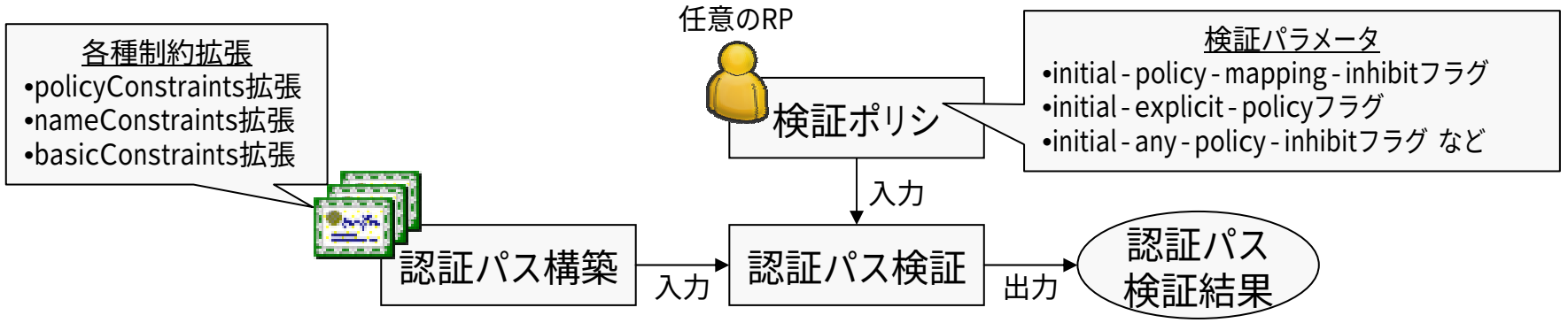
- PKIに対する要件
  - RFC 3647準拠の証明書ポリシ文書
  - 証明書ポリシ文書に対する一つ以上のポリシOID
  - 既定のプリンシパルCA
- PKIドメインに必要な文書
  - PKIドメインの存在を明文化
  - PKIドメインを管理するオーソリティを規定
  - PKIドメインの管理方法を規定
  - PKIドメインへの参加手続きと要件を記述
- PKIドメインメンバへの通達
  - 新規追加メンバ、脱退メンバの通知
  - メンバの変更に合わせたパス制約の見直し
- 複数ポリシを持つPKIやPKIドメインに関する考察
  - 明確に1対1、多対1、1対多いずれかの関係であることを横断証明書で定義する必要がある。

3.3. PKIドメインモデル

	トラストポイント統合型	トラストポイント独立型	
		直接横断認証モデル	ブリッジモデル
			
定義	各PKIドメインのPCAの上位として統合CA(Unifying CA)を提供する	各PKIドメイン(のPCA)が直接相互に(あるいは片方向で)横断認証する	ブリッジCAを介して相互に(あるいは片方向で)横断認証する
トラストアンカ	全ドメインのRPともに、自ドメインPCAから統合CAに切替	それぞれ自ドメインPCAのまま	

3.4. 運用考察

- PKIドメイン間で認証パスに制約を加えたい場合、リライングパーティの検証ポリシに委ねるのではなく、明示的に横断証明書に明示的に制約を含めるべき。

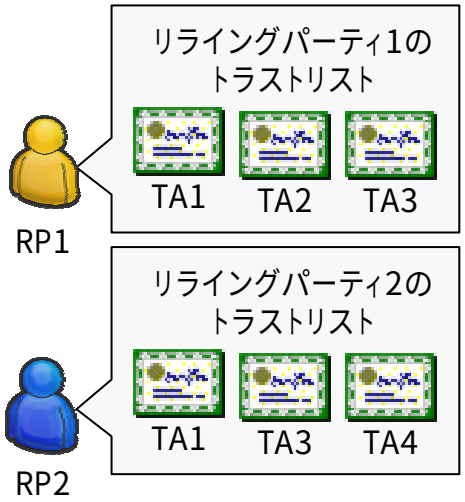
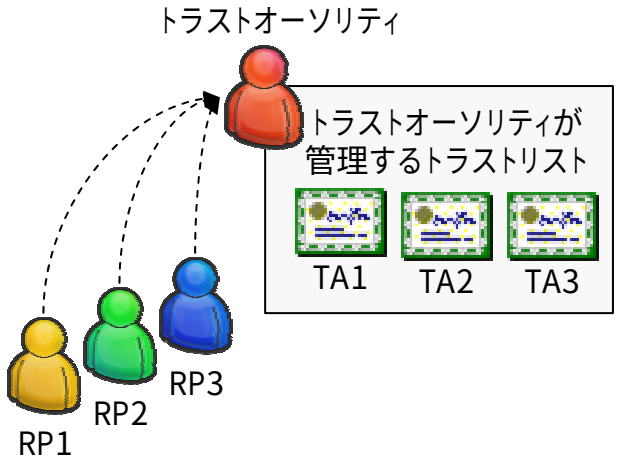


4. PKI外部との信頼モデル

1. トラストリストモデル
2. トラストリスト考察

- トラストリスト
  - 一つ以上のPKIを明示的に信頼するために、リライングパーティが使う一つ以上のトラストアンカの集合

4.1. トラストリストモデル

ローカルトラストリストモデル	トラストオーソリティモデル
	
リライングパーティが自身のために インストール・管理するトラストリスト	複数のリライングパーティのために 使用されるトラストリストを管理する エンティティ

4.2. トラストリスト考察

- PKI(認証局):
  - リライングパーティやトラストオーソリティに対して以下の情報を公開すること
    - 証明書ポリシ文書
    - (EE証明書の)失効情報
    - トラストアンカやプリンシパルCAが危殆化した場合の広報
- リライングパーティおよびトラストオーソリティ:
  - トラストリストに認証局を登録するにあたり、以下の責任を負うこと
    - 保証レベルなどリライングパーティの要件を満たしていることを、証明書ポリシ文書で確認すること。
    - 定期的にリポジトリなどにアクセスして、証明書ポリシ文書の改訂や危殆化に関する通知などを確認すること。
- トラストオーソリティに関する特記事項
  - 以下の項目を含む「トラストオーソリティポリシ」を規定すべき
    - リライングパーティの範囲
    - トラストリストへのトラストアンカの追加･削除手続き
    - トラストアンカによって提供される保証
    - トラストリストの完全性(integrity)を実現する方法
    - トラストオーソリティから証明書検証のために必要な情報を取得する方法

6. セキュリティ考察

1. PKIドメインモデル
2. トラストリストモデル

6.1. PKIドメインモデル

- リポジトリに対するDoS攻撃
  - 認証パス情報のキャッシュで回避可能
- 不必要な信頼関係
  - ドメインメンバへの通知によって回避可能

6.2. トラストリストモデル

- トラストリストの不正操作
  - トラストリストに対するアクセス保護
- トラストアンカのリポジトリに対するDoS攻撃 (トラストオーソリティモデルのみ)
  - トラストオーソリティのSLA
  - トラストリストのキャッシュ活用

RFC 5217のまとめ

- PKIをマルチドメイン環境で運用するために必要な情報を整理した
  - 単位となるPKIドメインを定義
  - PKIドメイン同士の信頼モデルを整理

オレオレ運用にならないこと
客観的に評価可能な運用設計

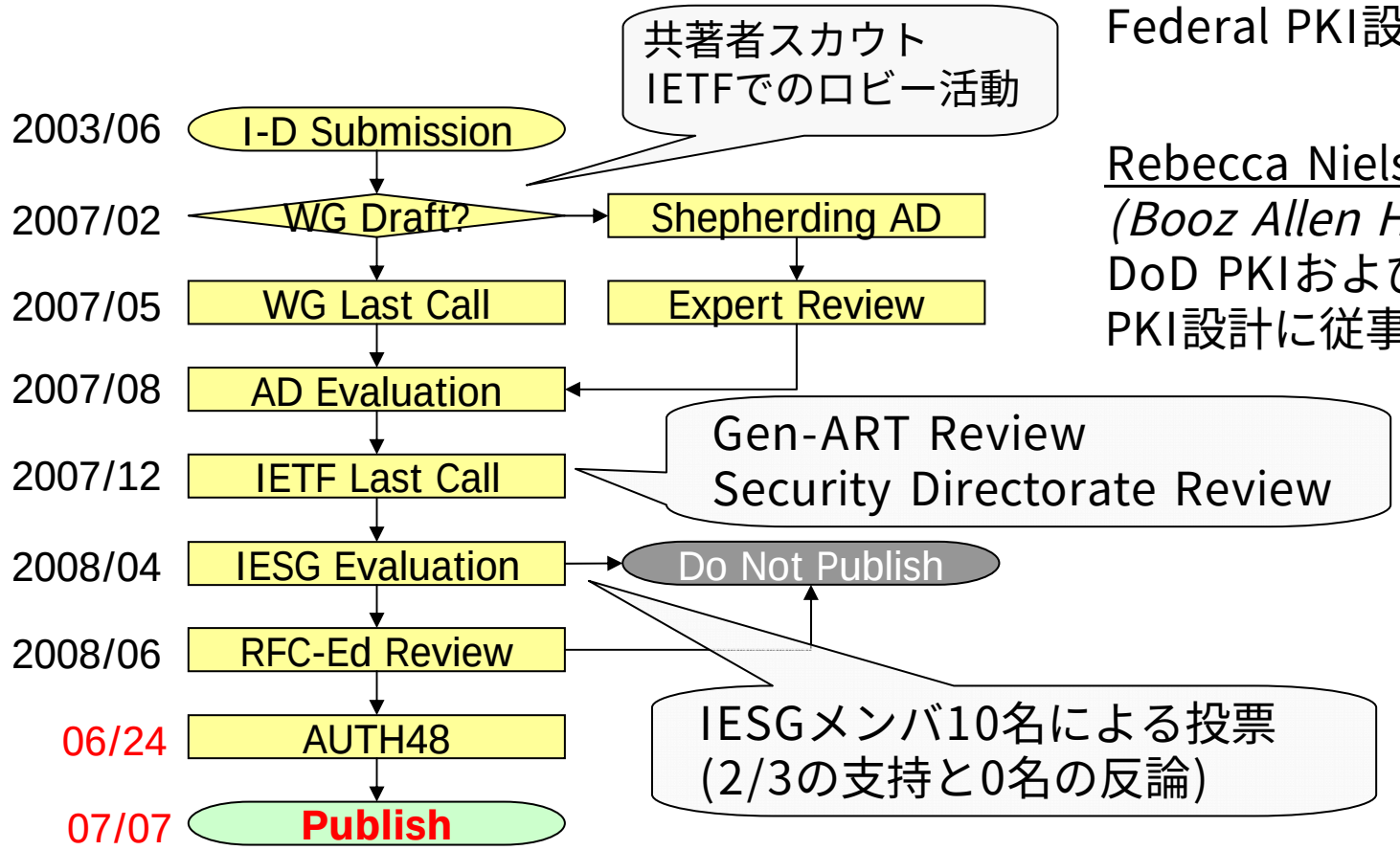
マルチドメイン環境を
構築する手法

バックグラウンドが異なる他人同士が相互接続する際に
必要な暗黙知を明確化した

標準化までの道のり

Nelson Hastings
(NIST)
Federal PKI設計に従事

Rebecca Nielsen
(Booz Allen Hamilton)
DoD PKIおよびFederal PKI設計に従事



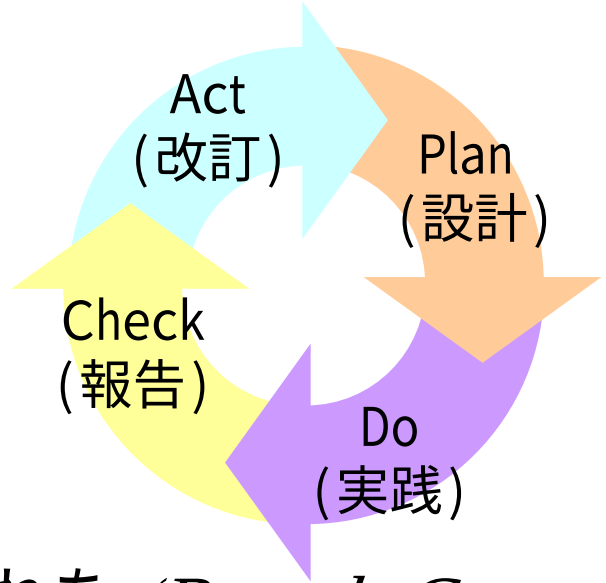
IETF(特にPKIX WG)のジレンマ

- 技術仕様の策定に終始しがち
  - 技術者のコミュニティなのでやむを得ないが、、、
- Best Current Practiceとのギャップ
  - 仕様が複雑化、机上検討だけで精一杯
  - 実装を作って、相互運用性を確認して…という取り組みが少ない
- 「標準」のジレンマ
  - 標準である以上、汎用性の高い仕様が求められる
  - 特定の文脈に依存した仕様は好まれない

ポリシなど個々のドメインに
依存する話はなおさら??

標準技術のPDCAサイクル

- 「枯れた技術」にするために不可欠な作業



- IETFは、これを *'Rough Consensus & Running Code'* で実践してきた

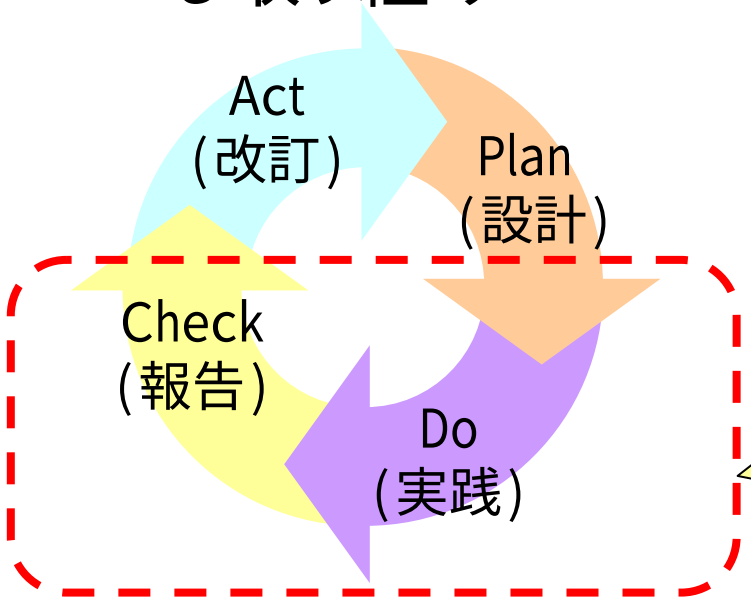
'Rough Consensus & Running Code' の限界?

- 仕様が複雑化
  - RFC 5280の認証パス検証アルゴリズムに完全に準拠したPKIアプリケーションは、世界中でも数えるほどしかないのでは。
- 検証するシステムの構築も複雑化
  - LDAPサーバ、認証局、署名プログラム、署名検証プログラム、場合によってはOCSPレスポンダ、SCVPサーバなどなど。。。
- マルチドメイン問題
  - ポリシの問題を棚上げして、実装だけで評価できる問題ではない。。。
  - 実際にポリシの異なるドメイン同士を相互運用してみる「実践(Practice)」がなければ、問題は見えて来ない。

一人のハッカーがプロトコルを設計して、コーディングして、、、
というレベルではなくなっている。
組織的な活動・支援などが必要。

相互運用の重要性

- これからの標準技術を支えるのは、相互運用に対する取り組み

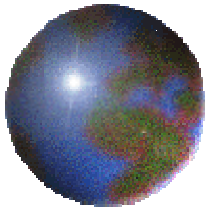


Challenge PKIの成果

- PKI相互運用実験
- PKI相互運用テストスィート
- RFC 5217

参考情報

- RFC 5217
  - http://www.ietf.org/rfc/rfc5217.txt
  - http://www.jnsa.org/mpki/rfc5217.html
- Challenge PKI プロジェクト
  - http://www.jnsa.org/mpki/
- JNSA PKI相互運用技術WG関連情報
  - http://www.jnsa.org/result/pki/index.html



謝辞

RFC 5217発行に至るまで、長期間に渡ってご支援ご協力いただいた方々に心から感謝の意を表します。