Challenge PKI Project
The Multidomain PKI Interoperability Framework

PKIドメインを確立するには

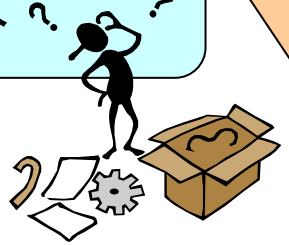
セコム(株) IS研究所
島岡 政基

PKIが展開していくと今後どうなる？

- GPKIのような大規模PKIの展開
- 組織同士の統合･合併
- 組織を超えたPKI同士の相互接続

→ PKIの
マルチドメイン化

併存するポリシの
整合



←
- 大規模PKIにおける個々のポリシ
- 個々のPKIが持つ既存のポリシ
- 統合･合併などで新たに作られるポリシ

ポリシに柔軟なドメイン構造が求められる

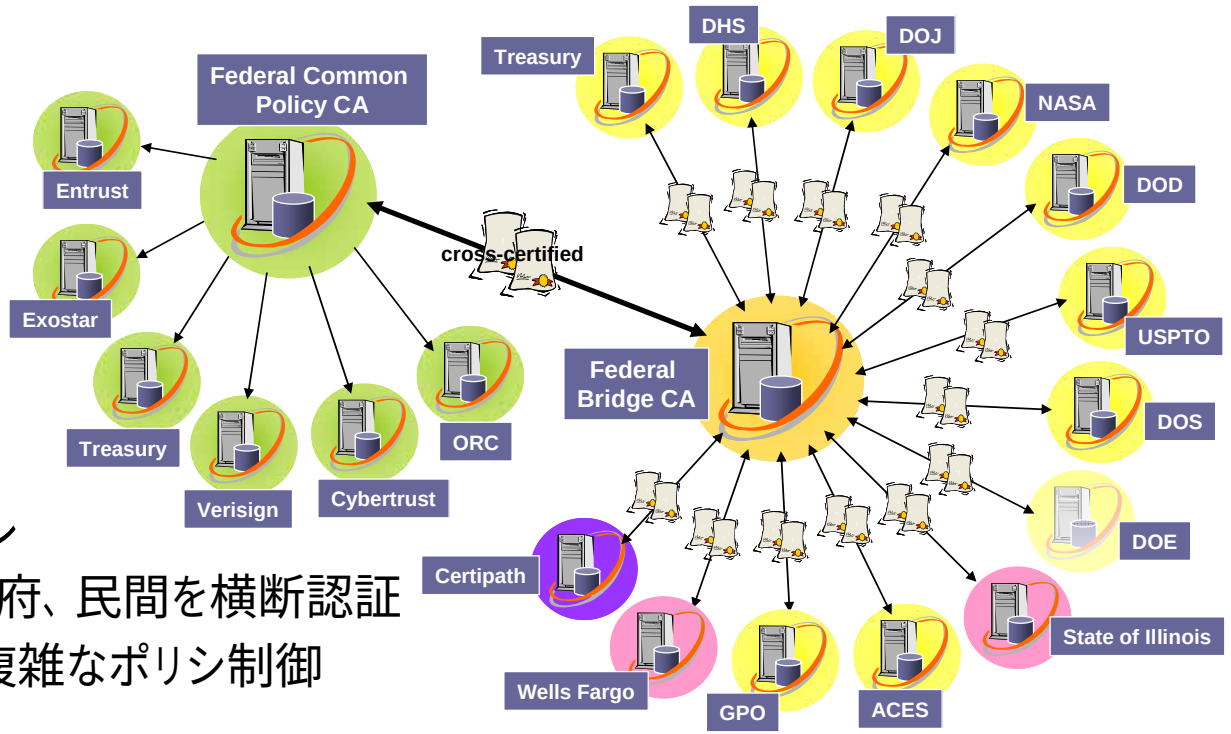
本日の内容

- 1. マルチドメインPKIの事例
- 2. 何故PKIドメインが必要なのか?
- 3. PKIの信頼モデルとPKIドメイン
- 4. 相互運用確立へ向けての標準化

1. マルチドメインPKIの事例

どんなところで使われているの？

Federal PKI

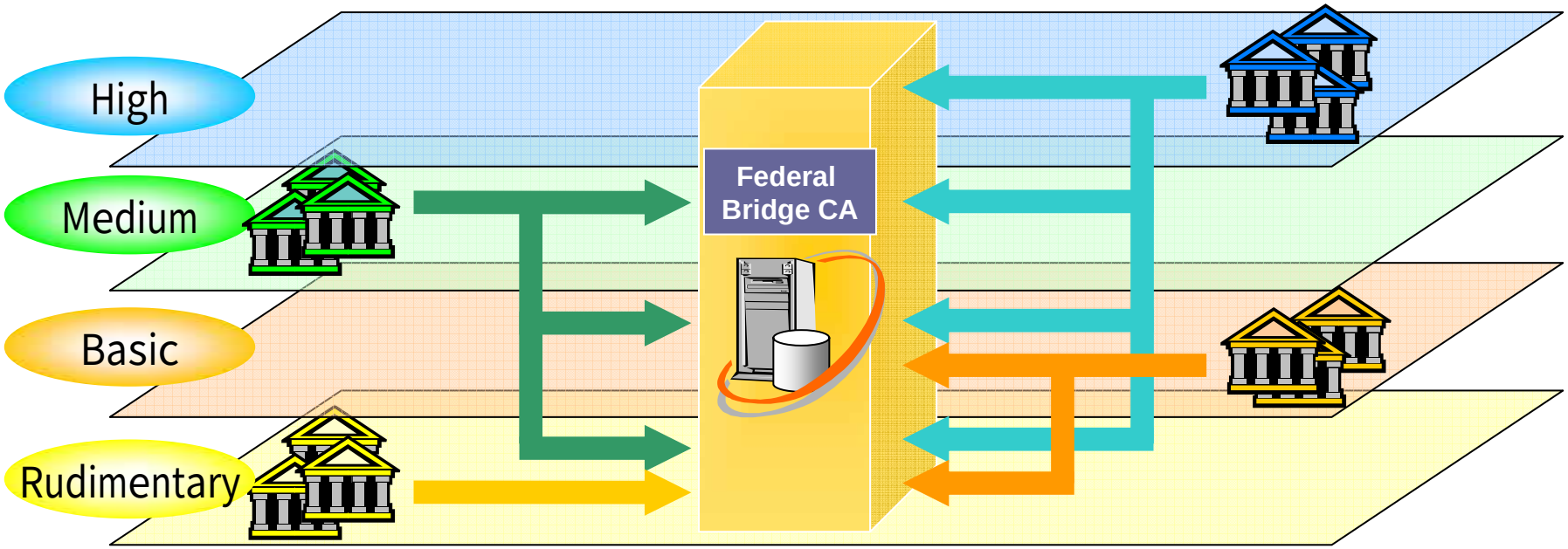


"Federal Identity Credentialing", 6th PKI R&D Workshop より
http://middleware.internet2.edu/pki07/proceedings/

- 米連邦政府のPKI
- 大規模なブリッジモデル
  - 連邦政府省庁、州政府、民間を横断認証
  - 複雑な認証パスと、複雑なポリシ制御
- コモンポリシの整備
  - 4レベルのポリシクライテリア
    - High, Medium, Basic, Rudimentary
  - 各CAのポリシをいずれかにマッピング
- コモンポリシにもとづく共用CAサービスの提供
  - Shared Service Provider
  - C4CA(Citizen and Commerce Class Common CA)

Federal PKIのドメイン構成

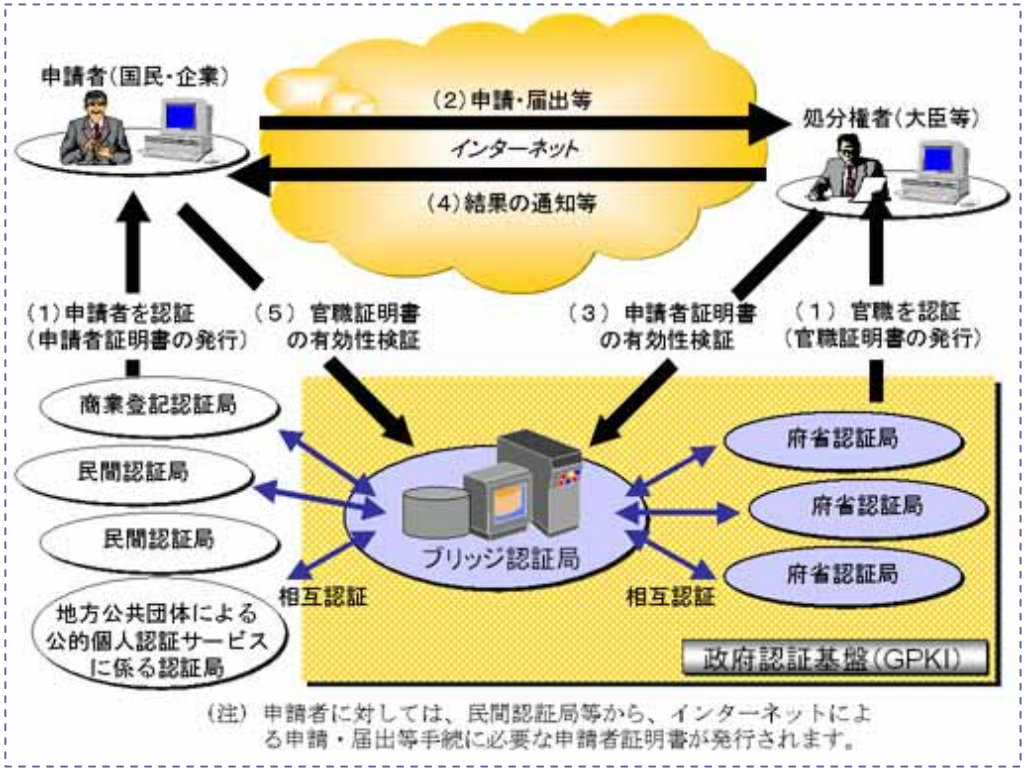
- レベルに応じた4つのポリシドメイン
  - 同じレベルであれば省庁、民間も混在?
  - レベルの上下関係をマッピングに反映



GPKI: 政府認証基盤

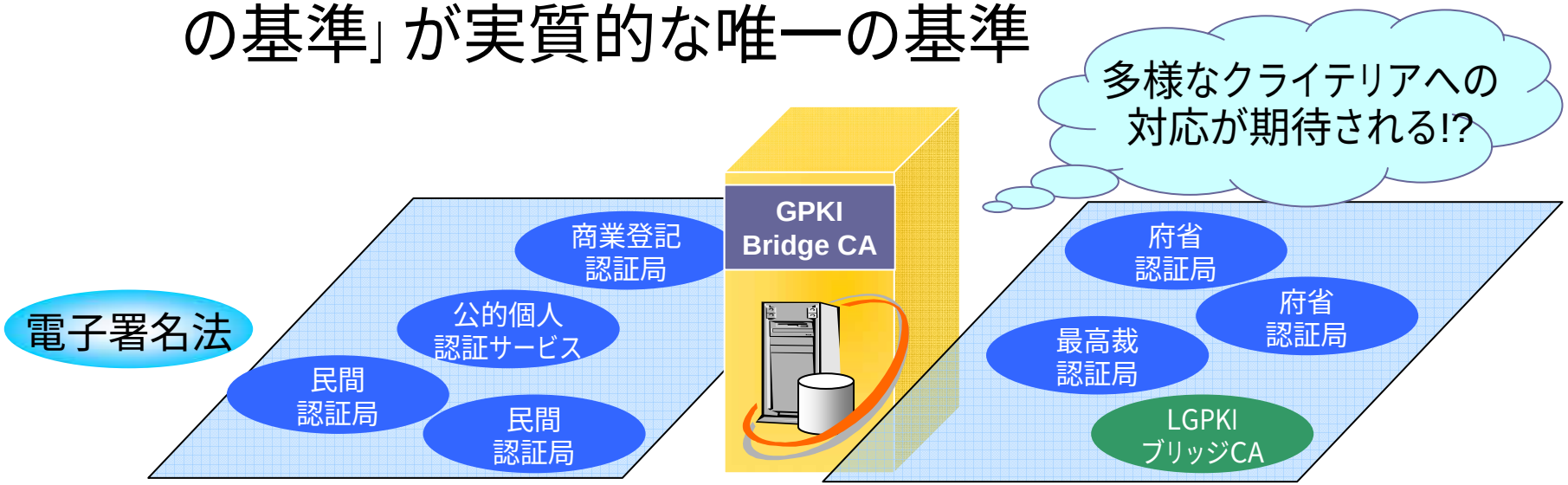
- 国民から行政機関への電子申請に利用
  - 本人確認、改ざん検知
- ブリッジCAで府省と民間を横断認証
  - 官職ドメイン
    - 府省認証局(14府省)
    - 最高裁認証局
    - LGPKI ブリッジ認証局
  - 申請者ドメイン
    - 電子署名法認定認証局(16)
    - 公的個人認証サービス
    - 商業登記認証局

http://www.gpki.go.jp/documents/gpki.htmlより



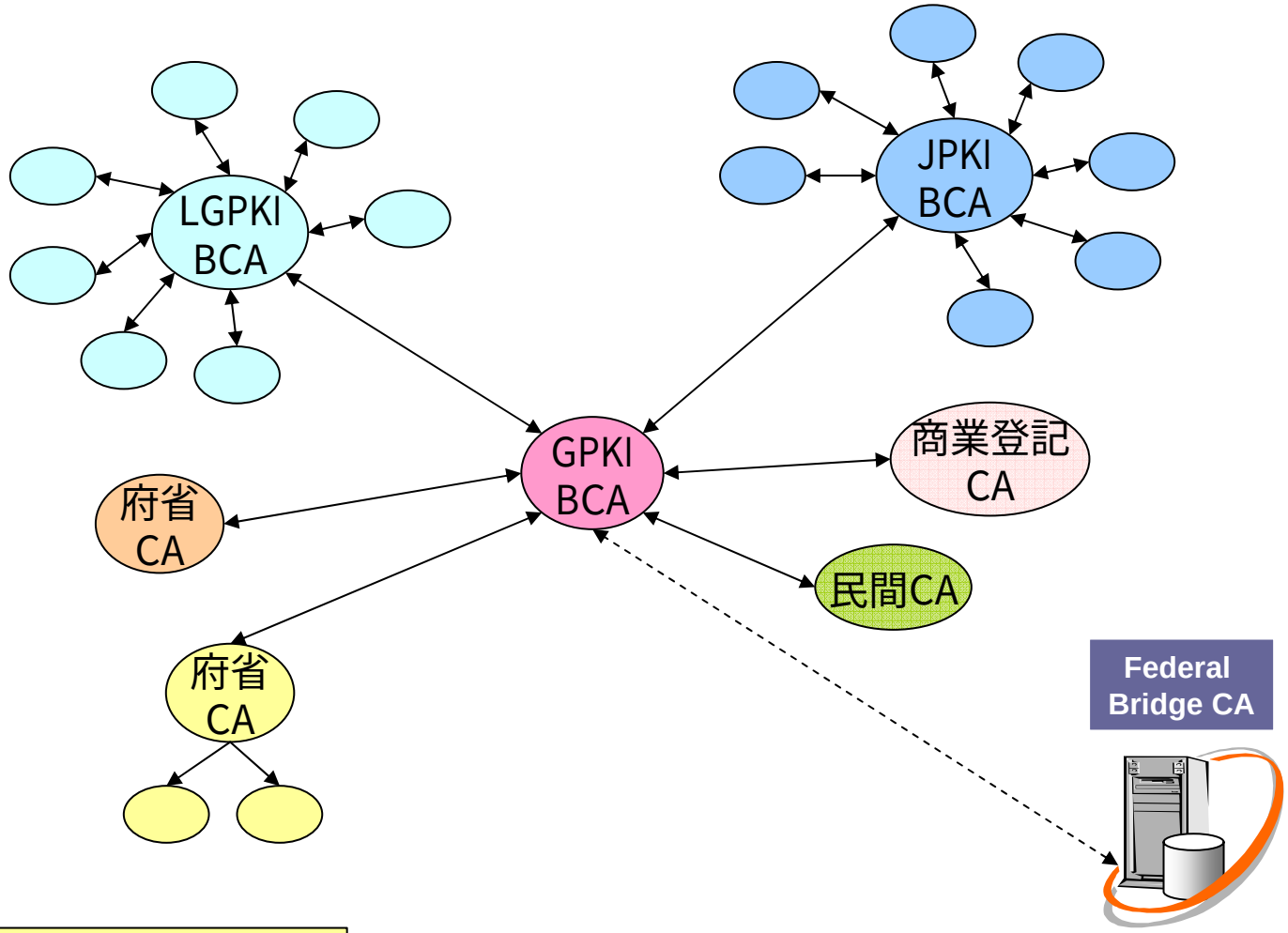
GPKIのドメイン構造

- 単一レベルでのポリシマッピング
  - 官職ドメインと申請者ドメインを相互接続
  - 電子署名法の「特定認証業務に係る電子署名の基準」が実質的な唯一の基準



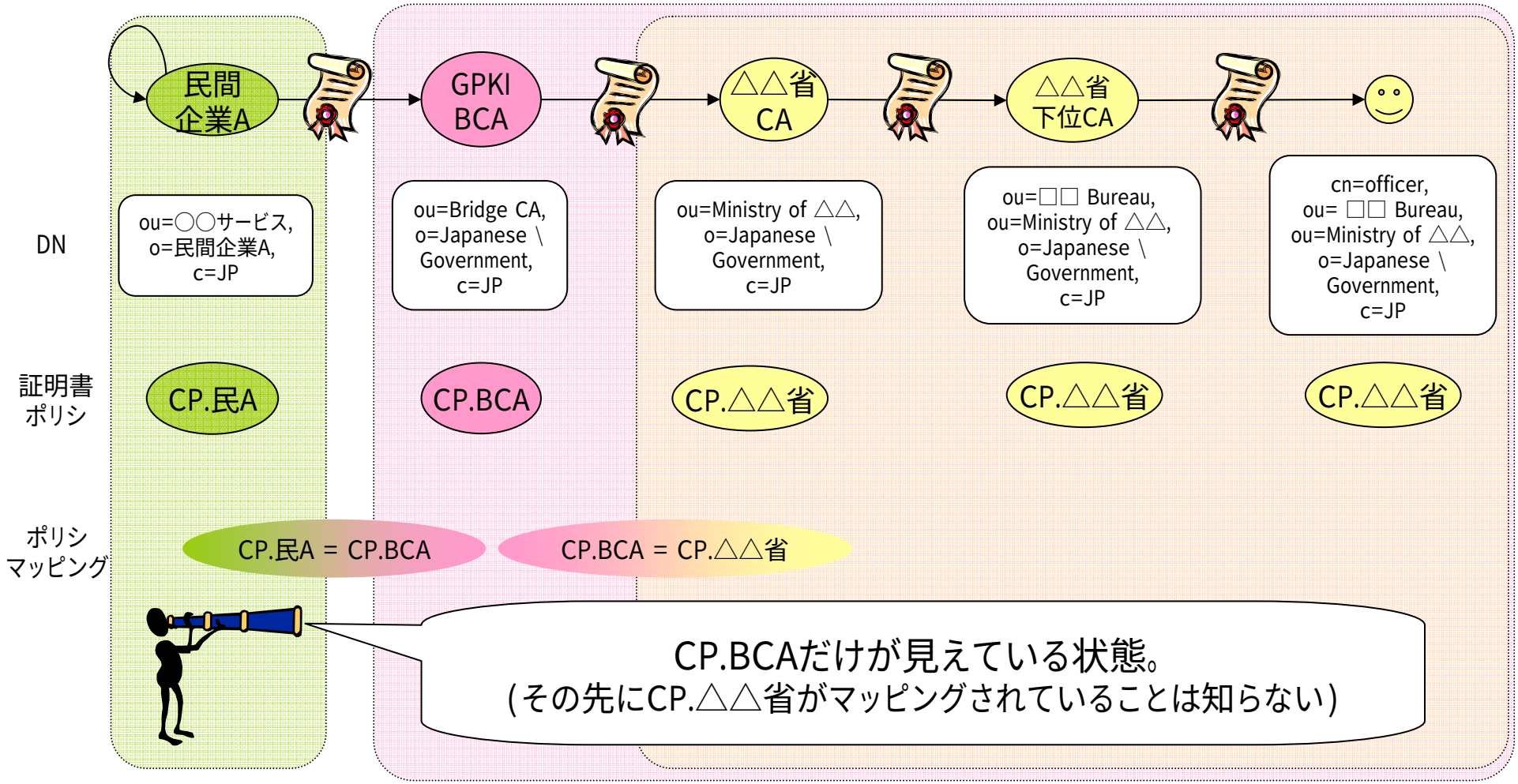
2. なぜPKIドメインが必要になるのか?

1つの巨大なPKI?

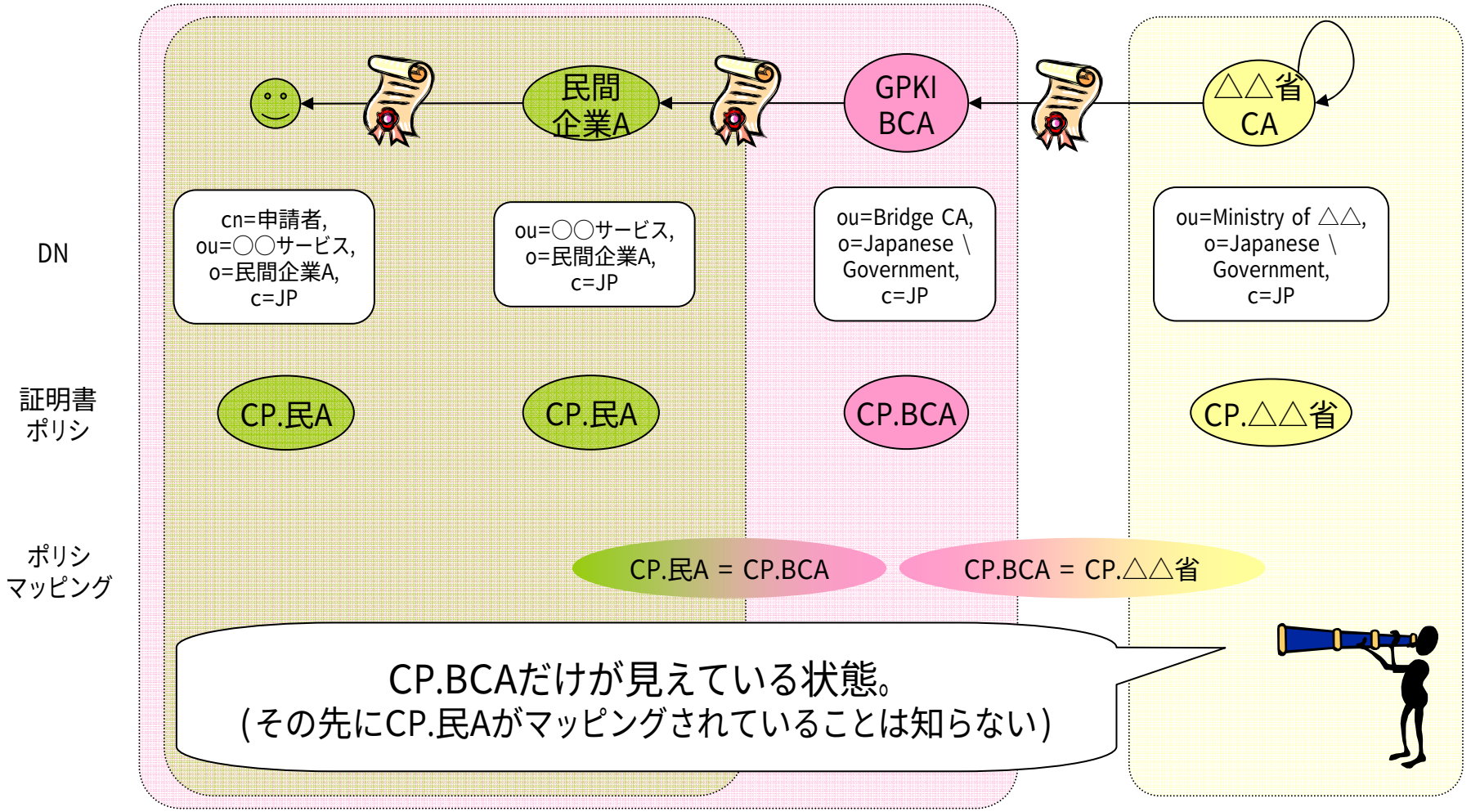


注)あくまで例です！
事実と異なる場合がありますのでご了承ください。

民間企業Aから見ると…

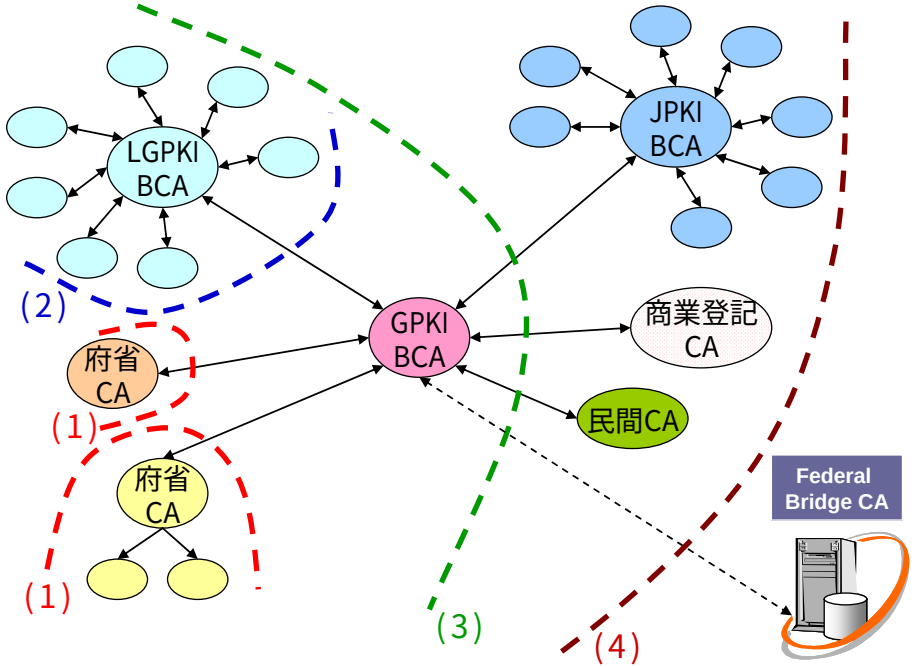

民間企業A
GPKI BCA
△△省 CA
△△省 下位CA
DN
ou=○○サービス, o=民間企業A, c=JP
ou=Bridge CA, o=Japanese \ Government, c=JP
ou=Ministry of △△, o=Japanese \ Government, c=JP
ou=□□ Bureau, ou=Ministry of △△, o=Japanese \ Government, c=JP
cn=officer, ou= □□ Bureau, ou=Ministry of △△, o=Japanese \ Government, c=JP
証明書ポリシ
CP.民A
CP.BCA
CP.△△省
CP.△△省
CP.△△省
ポリシマッピング
CP.民A = CP.BCA
CP.BCA = CP.△△省
CP.BCAだけが見えている状態。
(その先にCP.△△省がマッピングされていることは知らない)

△△省から見ると…


民間
企業A
GPKI
BCA
△△省
CA
DN
cn=申請者,
ou=○○サービス,
o=民間企業A,
c=JP
ou=○○サービス,
o=民間企業A,
c=JP
ou=Bridge CA,
o=Japanese \
Government,
c=JP
ou=Ministry of △△,
o=Japanese \
Government,
c=JP
証明書
ポリシ
CP.民A
CP.民A
CP.BCA
CP.△△省
ポリシ
マッピング
CP.民A = CP.BCA
CP.BCA = CP.△△省
CP.BCAだけが見えている状態。
(その先にCP.民Aがマッピングされていることは知らない)

PKIドメインとは

- 同じポリシを持つPKIと、異なるポリシを持つPKIとの境界を示すためのもの。
- 異なるポリシを持つPKIと相互運用して初めて必要となる。
  - だからなかなか認識されない…



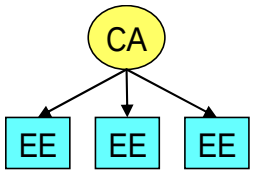
(1) 府省ドメイン同士の境界
(2) LGPKIとGPKIの境界
(3) 官職ドメインと申請者ドメインの境界
(4) 日米PKIの境界??

3. PKIの信頼モデルとPKIドメイン

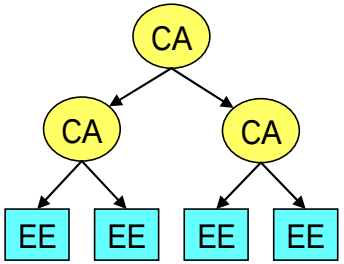
PKIの信頼モデル

CA - CA間の信頼関係

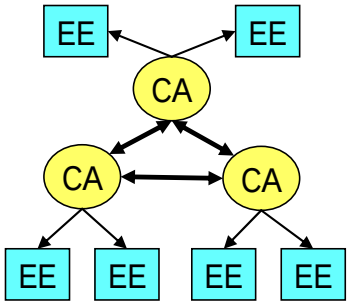
シングルPKI



階層PKI



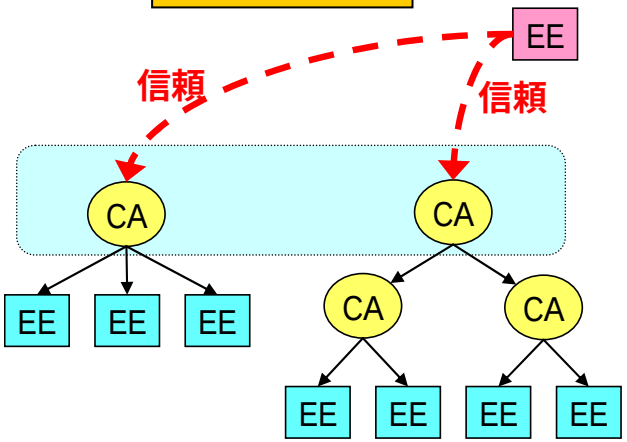
メッシュPKI



それぞれのCA間に境界があったら？
各モデルのつなぎ目が境界になったら？

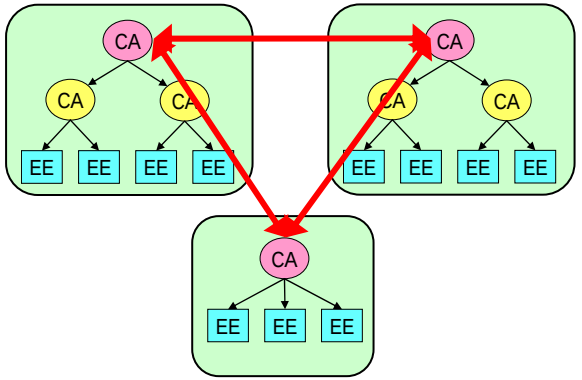
CA - EE間の信頼関係

トラストリスト



CA同士はお互いの
関係を認識できない!

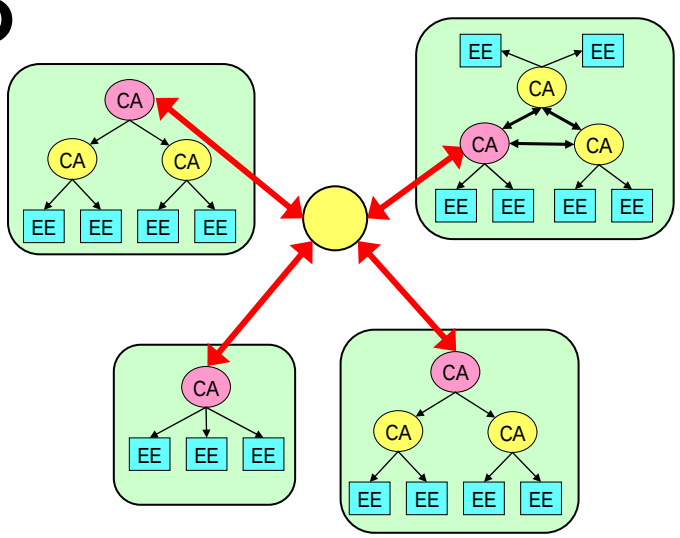
PKIドメインモデル 1/3



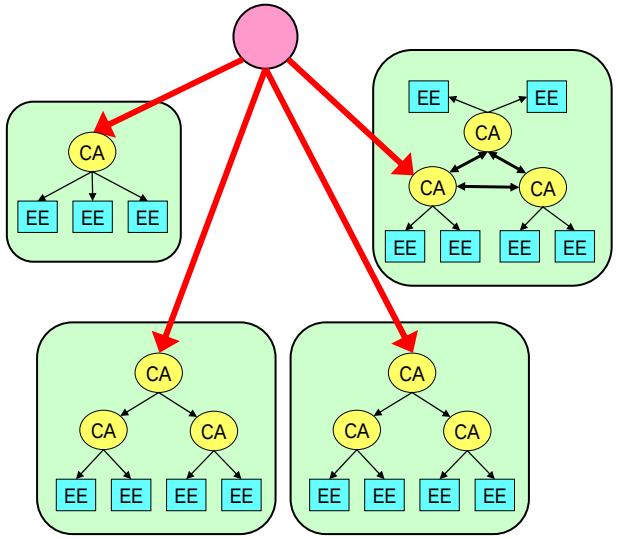
- 直接横断認証モデル
  - 各PKIドメインのPrincipal CAが直接相互に横断認証
  - 最もプリミティブなモデル
  - 認証パスが長くならない
  - 参加ドメインが増えればメッシュ型に…
  - トラストポイントは、各PKIドメインのPrincipal CA
    - CA-EE間の信頼関係が変わるわけではない。

PKIドメインモデル 2/3

- ブリッジモデル
  - 全てのPKIドメインがブリッジCAを介して横断認証
  - PKIドメインが増えても認証パスが複雑にならない
  - GPKIによって広く知られたモデル
  - 中立的第三者としてのブリッジCA
    - 全PKIドメインに共通したクライテリアに基づくポリシマッピング
  - トラストポイントは、各PKIドメインのPrincipal CA
    - CA-EE間の信頼関係が変わるわけではない



PKIドメインモデル 3/3



- 統合ドメインモデル
  - 各PKIドメインのPrincipal CAが、「統合CA」の下位CAとなる
  - 複数のPKIドメインをあたかも一つの階層PKIのように統合することができる
  - トラストポイントは、各PKIドメインのPrincipal CAではなく「統合CA」になる
    - 他のPKIドメインモデルと異なり、CA-EE間の信頼関係が変わる

4. 相互運用確立へ向けての標準化

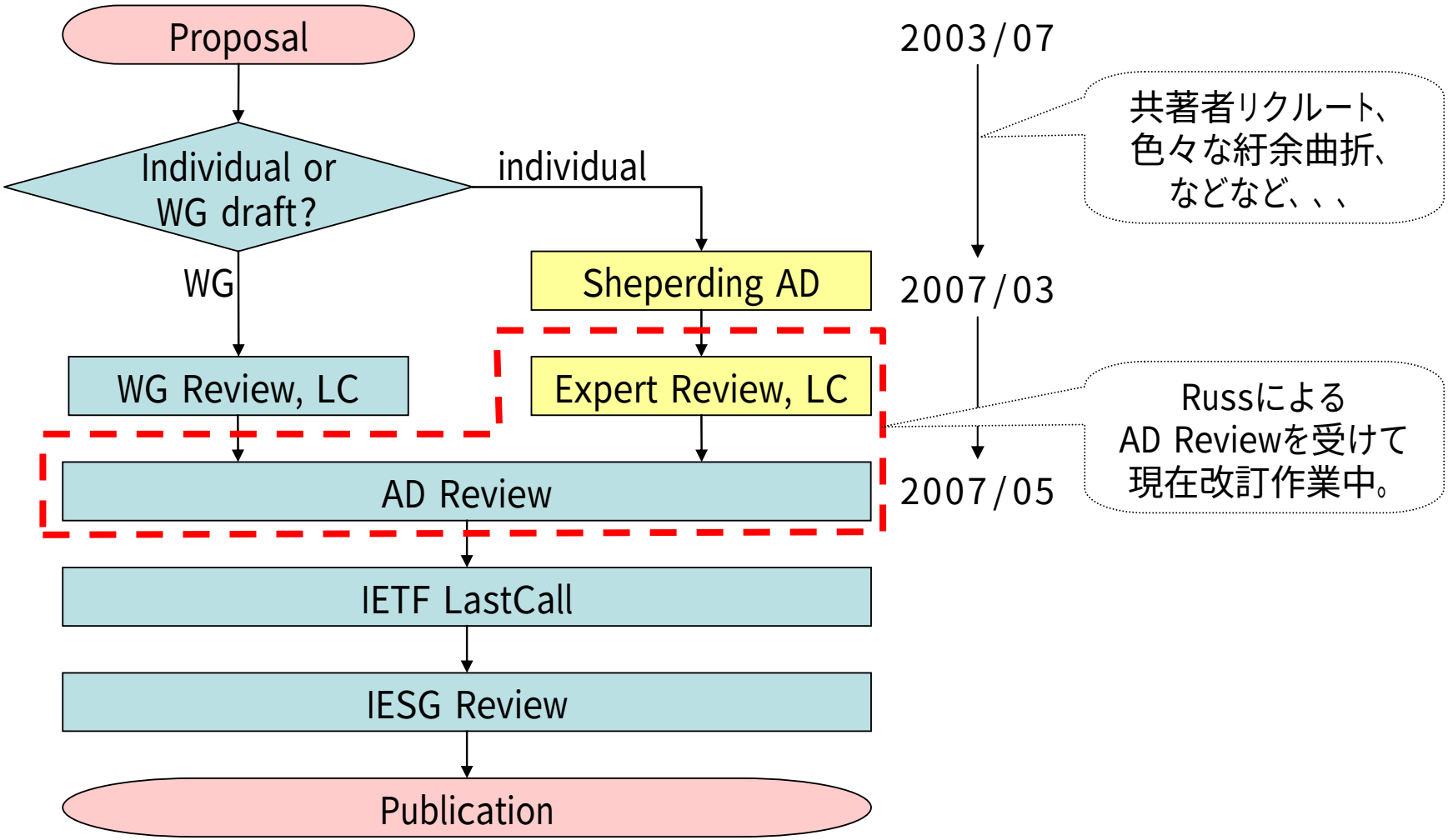
マルチドメインPKIの相互運用

- PKIドメインという概念
  - ローカルなPKIにはあまり縁のない話だが…
  - 長期運用を求められるPKIに統合・拡張は不可避の問題
- 概念を固める⇒世界的な合意形成が必要
  - 時間がかかる作業
  - 統合・拡張に直面する前に整理しておくべき
- 更に、業界を超えた合意形成…

IETFでの標準化

- Internet-Draftを提案中
  - Memorandum for multi-domain PKI interioerability
  - 「PKIの信頼モデルとPKIドメイン」の合意形成を目指す
- 共著者
  - Rebecca Nielsen(Booz Allen Hamilton), 米国防総省PKIに従事
  - Nelson Hastings(NIST), Federal PKIに従事
  - いずれもブリッジモデルのマルチドメインPKIでの運用実績がある
  - 主にメールで意見交換、相互レビューなどを実施
- IETFのキーパーソン
  - Russ Housley(現IETF Chair←前Security Area Director)
    - 本I-Dの担当AD
    - PKIX WGを中心に数多くのPKI関連RFCを執筆
  - Tim Polk(現Security Area Director←前PKIX WG co-chair)
    - 提案当初からのマルチドメインPKI相互運用の理解者
    - '00/08～'06/03まで非常に長期間PKIXを支えた功労者

標準化までの(長〜い)道のり



まとめ

- いずれ既存PKIの相互接続が必要に
  ⇒PKIドメインという考え方が不可欠
- GPKIなどの大規模PKIによるケーススタディ
  - 稀少な事例に学ぶ
- PKIドメインのモデル化
  - PKIの信頼モデルを正しく理解しておく
- IETFでの標準化
  - 業界を超えた合意形成

参考資料

- JNSA Challenge PKI Project
  - http://www.jnsa.org/mpki/
- Internet-Draft: Memorandum for multi-domain PKI Interoperability
  - http://www.ietf.org/internet-drafts/draft-shimaoka-multidomain-pki-09.txt
- 政府認証基盤(GPKI)
  - http://www.gpki.go.jp/
- Federal PKI Policy Authority
  - http://www.cio.gov/fpkipa/
- NIST PKI
  - http://www.csrc.nist.gov/pki/publickey.html
- セコムIS研: マルチドメイン環境におけるPKI相互運用性の標準化
  - http://www.secom.co.jp/isl/theme/cs04/report01/index.html
- IPA: PKI関連技術情報
  - http://www.ipa.go.jp/security/pki/pki.html