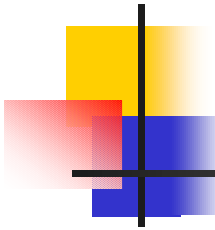
PKIの相互運用実験
Challenge PKI 2001

JNSA/セコムトラストネット株式会社
松本　泰
yas-matsumoto@secomtrust.net



PKIの相互運用実験Challenge PKI 2001

- Challenge PKI 2001とは？
  - Challenge PKI 2001の概要
  - Challenge PKI 2001のコンセプトなど
- PKIの相互運用とChallenge PKI 2001の実験の内容
  - PKIの基本的な信頼モデル
  - マルチPKIドメインの説明
  - 実験で使用する信頼モデル
  - 実験で使用するPKIアプリケーション
  - 実験で使用する証明書プロファイル
- Challenge PKI 2001の参考
  - 参考にすべき相互運用実験の事例
  - PKI相互運用性の参考

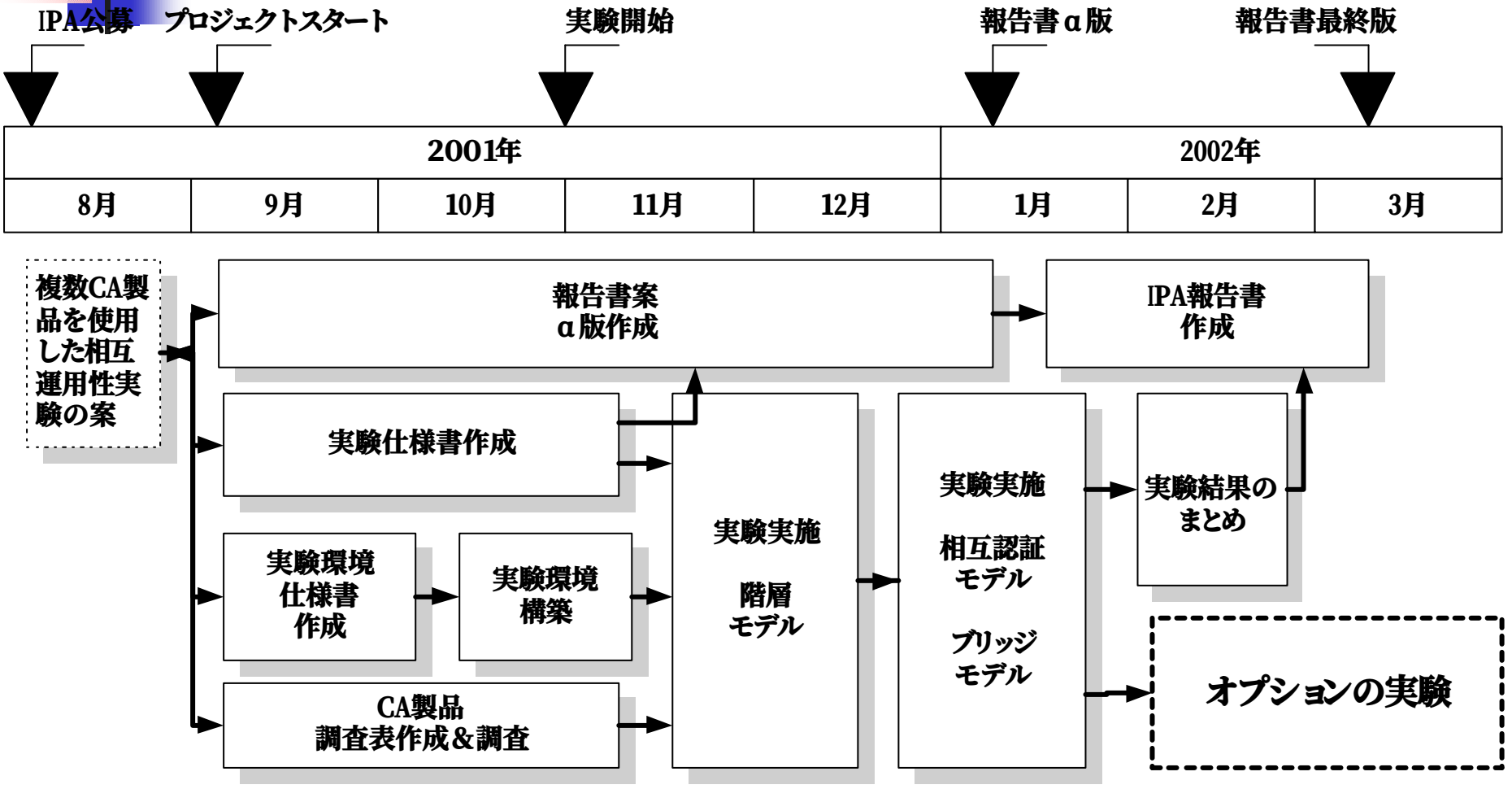
Challenge PKI 2001とは？

- 複数CAを使用したPKI相互運用実験」
  - JNSAが、IPAの 情報セキュリティ関連の調査・開発に関する公募」の「PKI関連相互運用性に関する調査」にIPsec相互接続実験などを合わせて応募し、採択されたもの
- 9団体の9CA(サービスを含む)で構成
  - マルチベンダーのPKI相互運用実験として、9つもの異なるCAを使用する実験は世界的にも例がない。
  - 各参加団体から、多彩なメンバーが参加
  - 工学院大学などの協力
- マルチPKI ドメイン
  - 実験では、GPKIなどで採用されている異なるPKI ドメイン間の相互運用性を取り上げる。

Challenge PKI 2001の参加団体

実験参加企業（団体）	実験参加CA
セコムトラストネット/エントラストジャパン	Entrut PKI 6.0
SSH	SSH Certificate 2.0
NECソフト	Carassuit電子政府版Ver1.1
RSAデータセキュリティ	Keon 6.0
富士ゼロックス/富士ゼロックス情報システム	未発表製品
マイクロソフト プロダクトディベロップメント リミテッド	MicroSoft Windows Server
日本ベリサイン	非公開)
名古屋工業大学	Easy Cert(開発 奥野琢人氏)
W DEプロジェクト	ICAP v2.51 (CAT)

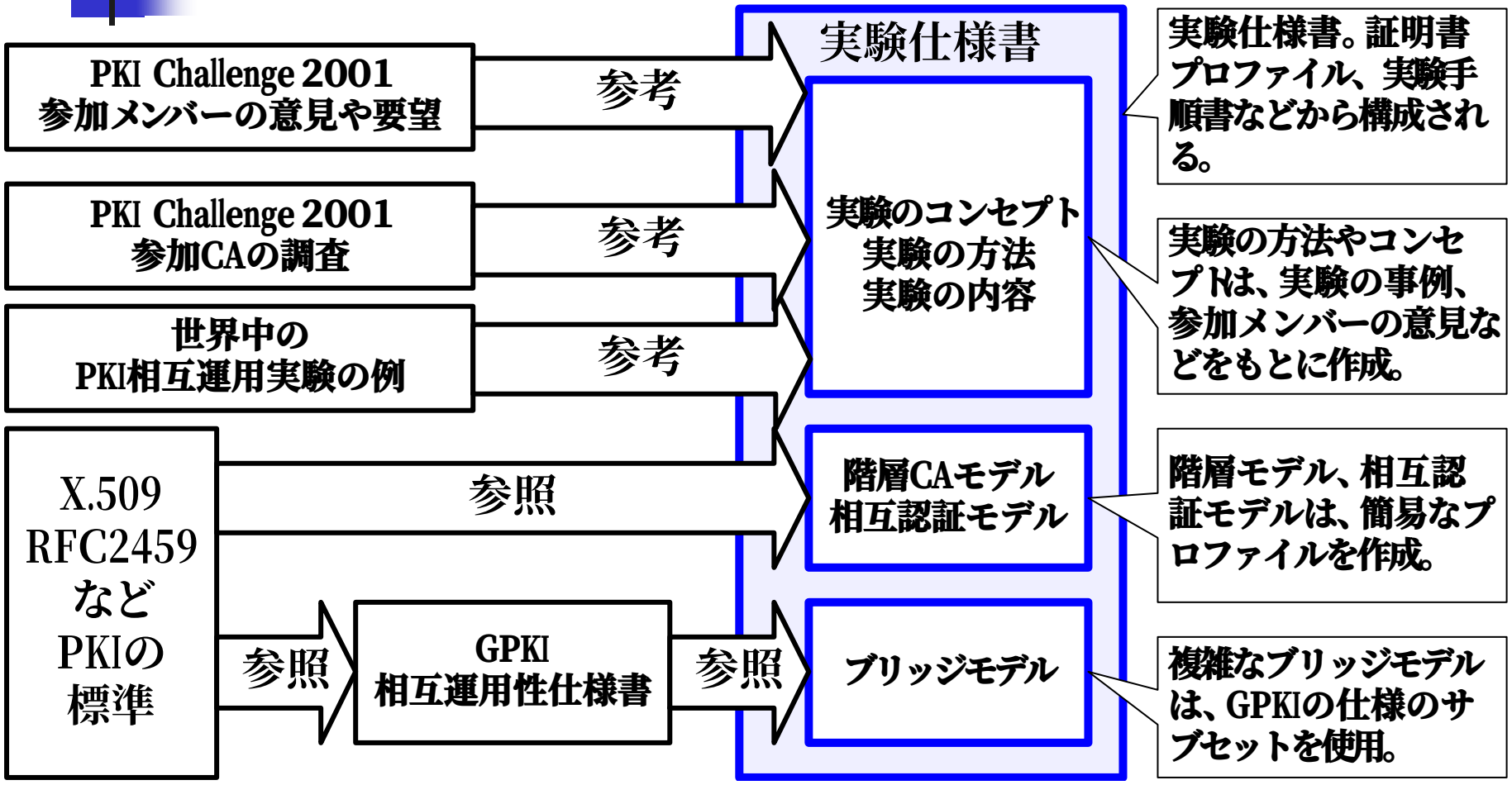
Challenge PKI 2001のスケジュール



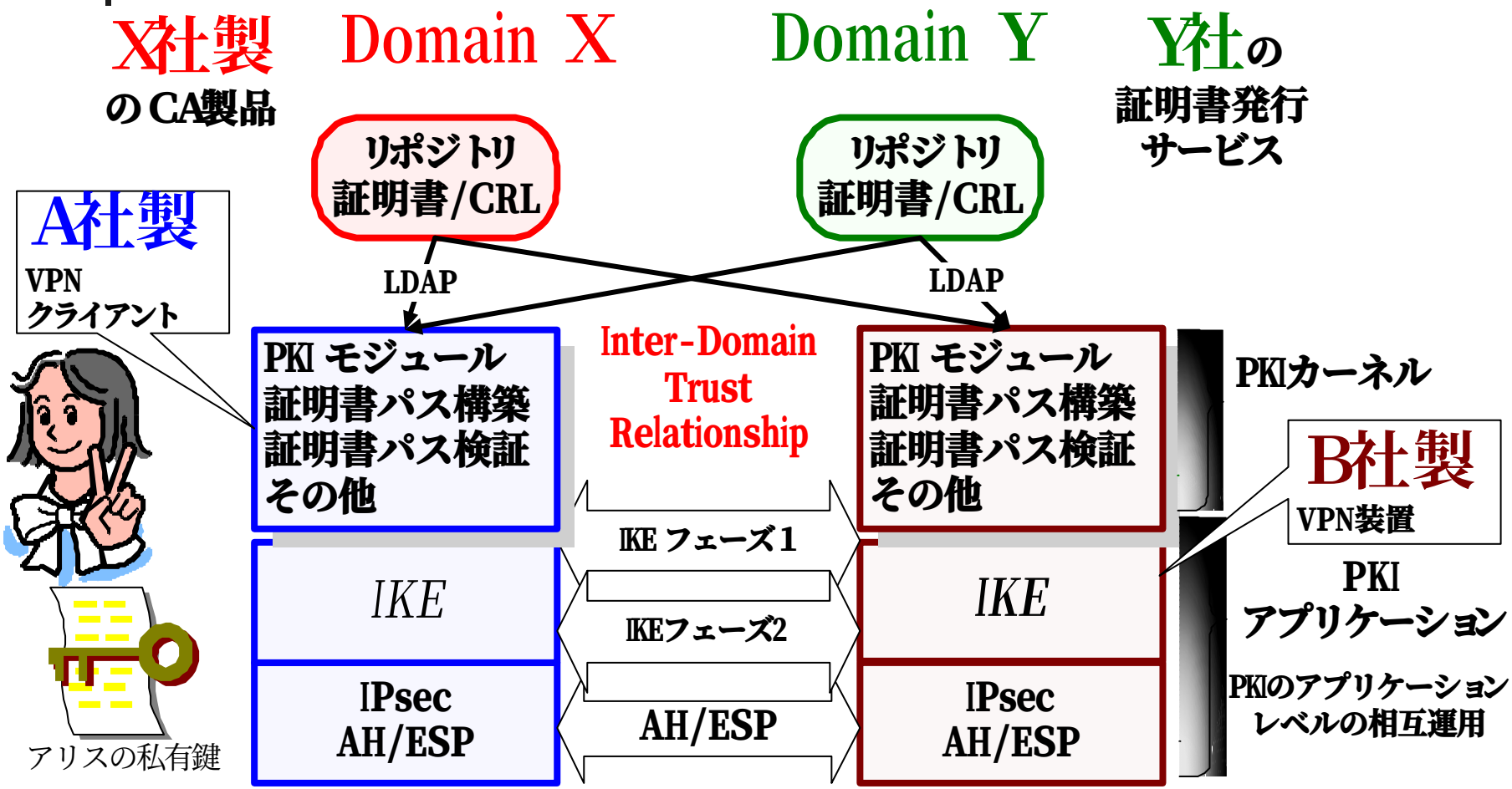
Challenge PKI 2001
実験内容のコンセプト

- PKIの相互運用性の問題点を明らかにする
  - オープンなPKIでは、幅広い相互運用性が要求される。標準同士の不整合、実装の標準に対する解釈のずれなど、相互運用性を阻害する要因は多々ある。これらを実験を通じて明らかにする。　複数CA製品を使用した相互運用実験」では、PKIの相互運用の中で以下をフォーカスした実験を行う。
- マルチベンダーPKI対応（複数のCA製品）
  - 単一ベンダーの製品を使ったPKIから、マルチベンダーの製品を使ったPKIへ流れがある。これは、PKIが真のインフラになるためには当然の流れだと考えられる。しかし、まだ事例が少なく問題点が明確になっていない。今回は、PKIのアプリケーションではなく、複数のCA製品を使った実験にフォーカスする。
- マルチPKIドメインの対応
  - 相互認証モデル、ブリッジモデルのような複数のPKIドメインをつなぐモデルが登場してしている。PKIが真の広域認証の基盤になるためには、マルチドメインの認証が必要だと考えられる。しかし、これも同じく、事例が少なく、問題点が明確になっていない。

Challenge PKI 2001実験のバックグランド

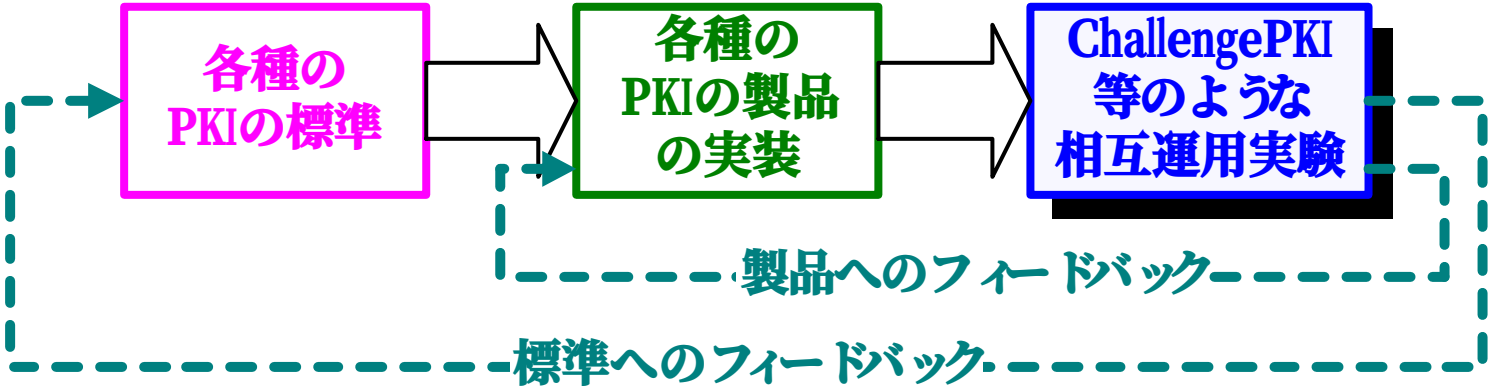


Challenge PKI 2001実験の目標イメージ
マルチベンダー&マルチPKIドメイン下の相互運用

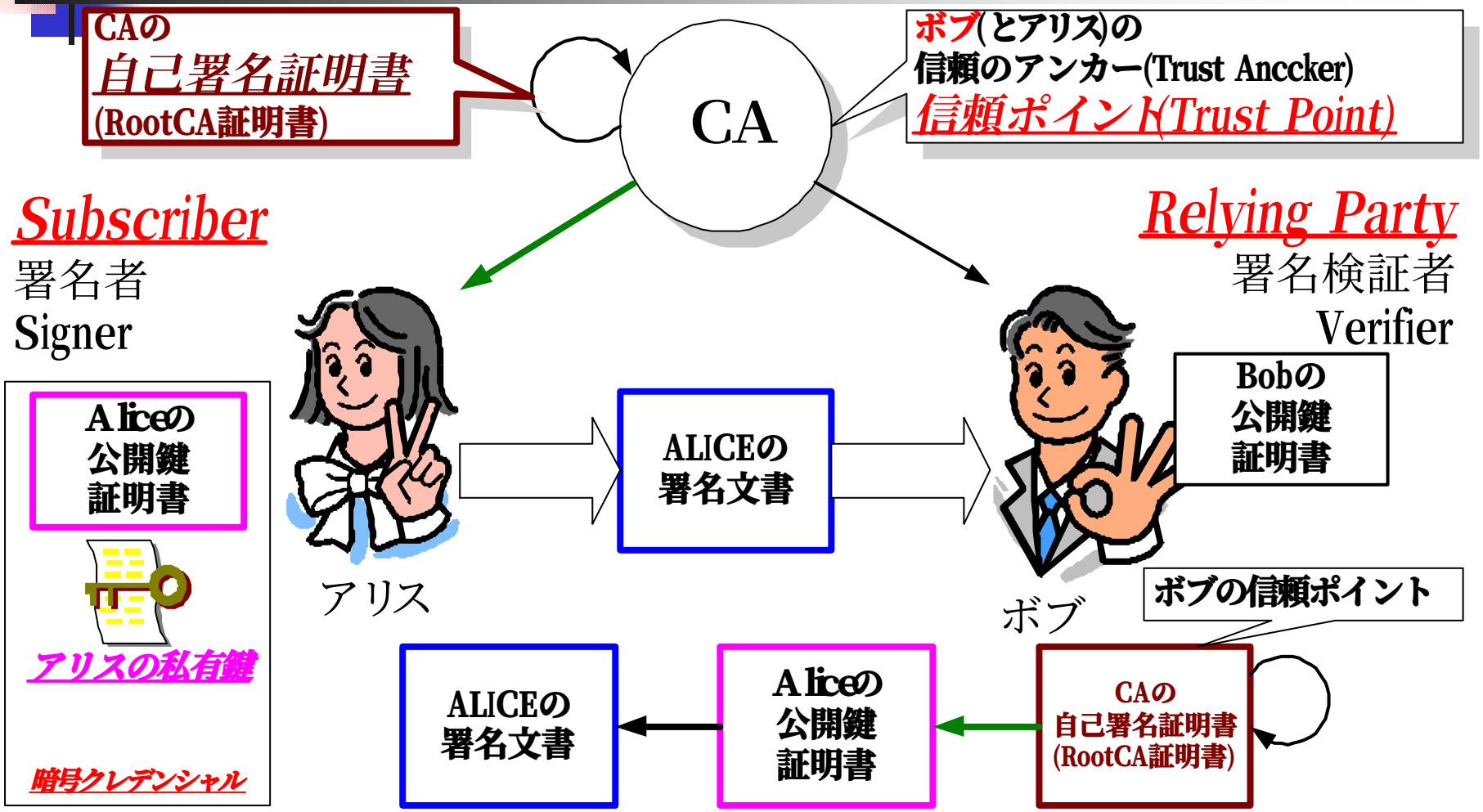


Challenge PKI 2001実験の目標

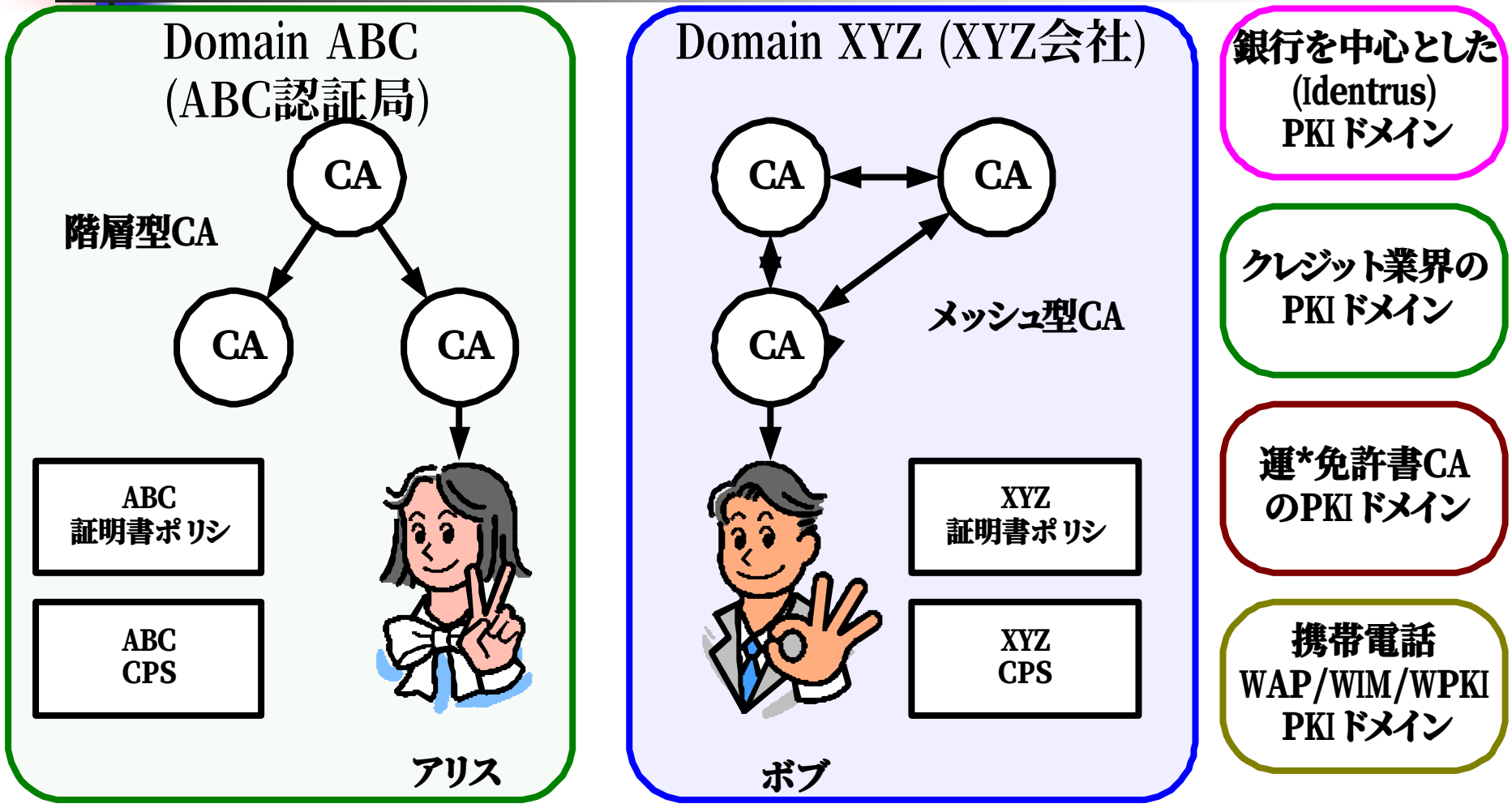
- 実験参加のモチベーション
  - マルチベンダーPKI, マルチPKIドメインなどで要求されるPKIを実際に構築することで技術を共有する。
- 実験の目標
  - 実験を行うことにより、マルチベンダーPKI, マルチPKIドメインの相互運用性の問題点を明らかにする。
  - 将来的に更に広範囲なPKIの相互運用実験を行うための方法論やスキームを確立する。



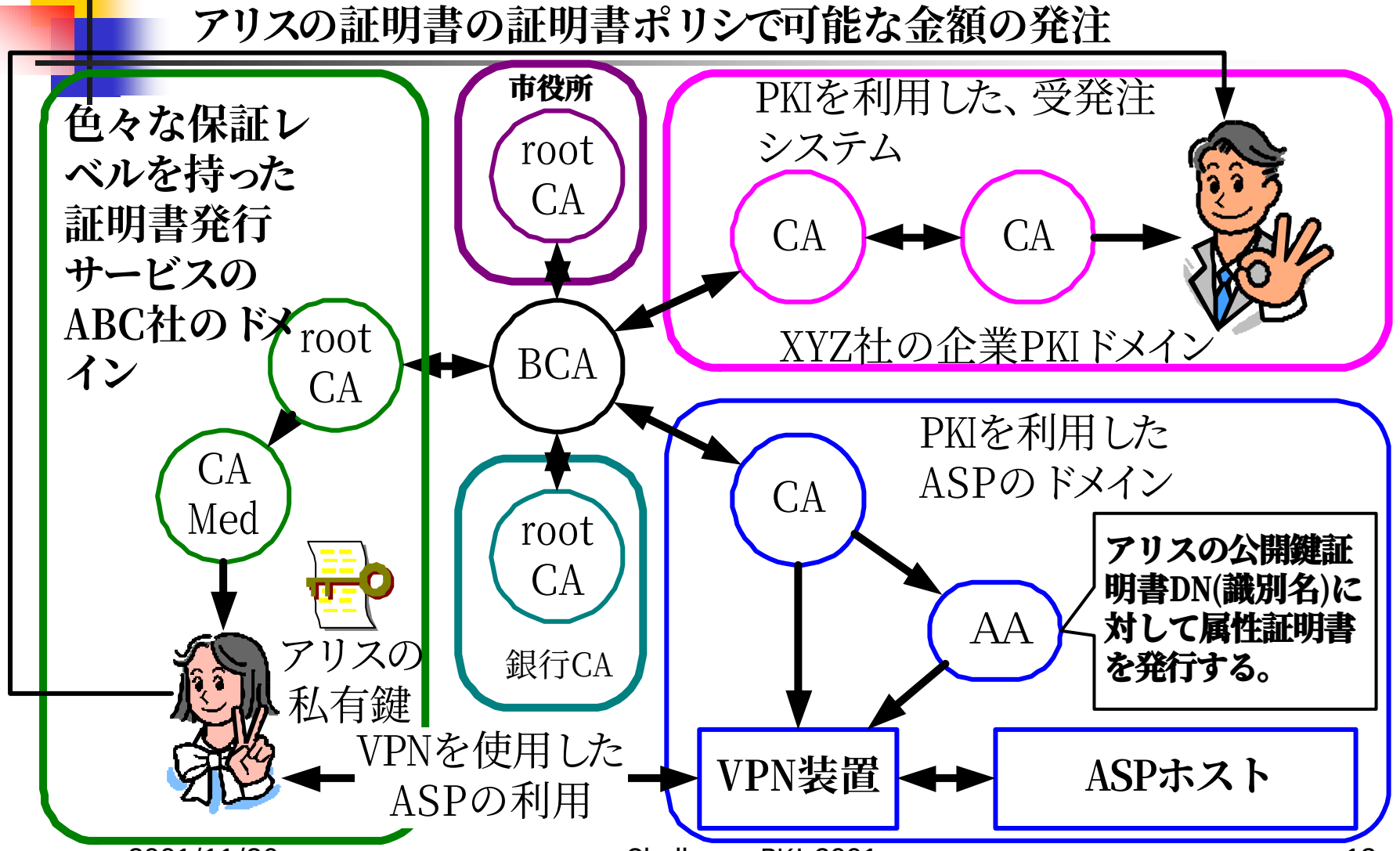
PKIの基本的な信頼モデル



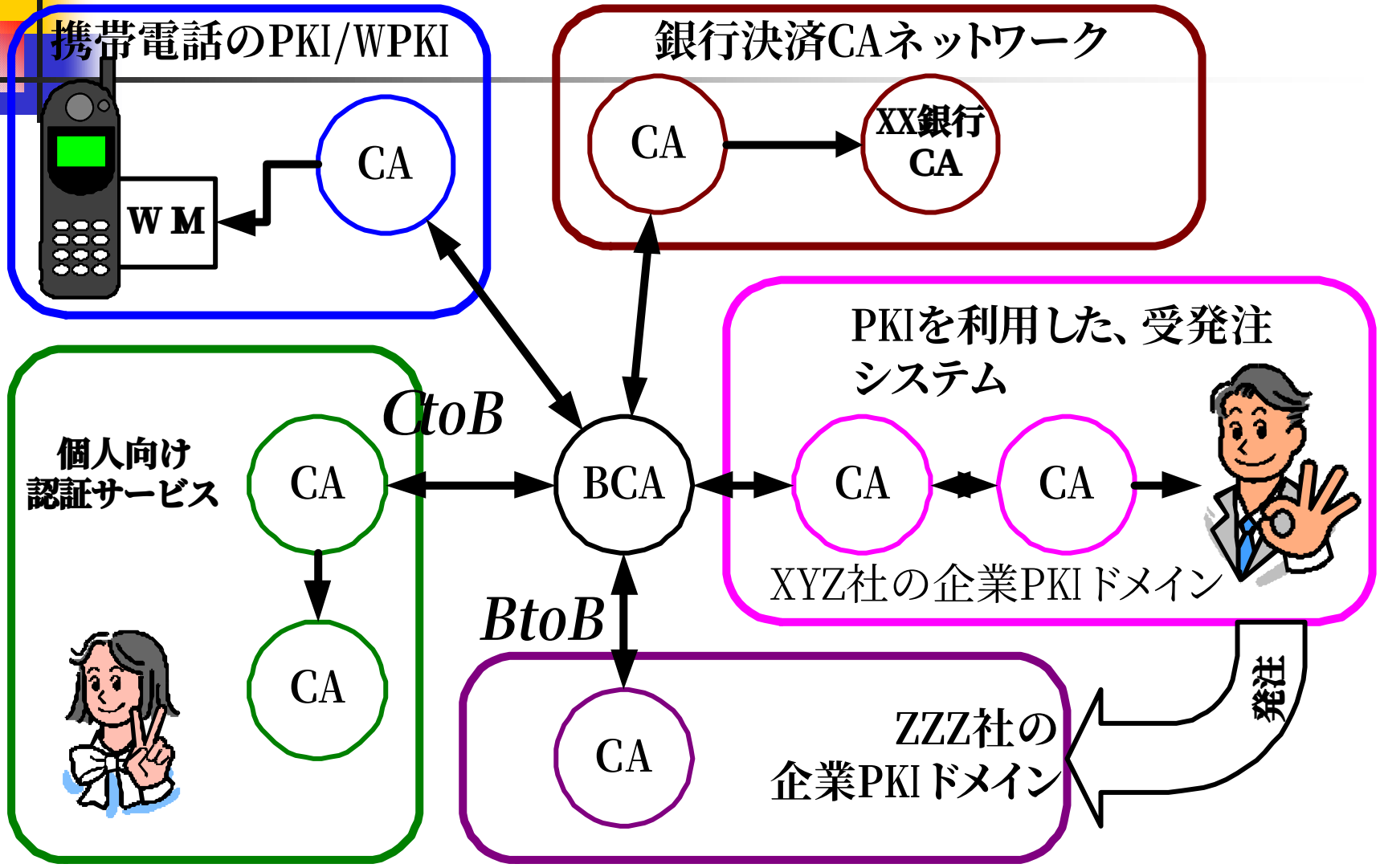
マルチPKIドメインの説明
色々な信頼ドメイン（PKIドメイン）



マルチPKIドメインの説明
マルチPKIドメインの目標(Subscriber側のメリット)



マルチPKIドメインの説明
マルチPKIドメインの目標(Relying Party側のメリット)



Challenge PKI 2001の実験の内容

- 3つの信頼モデルを実験する
  - 複数のCAを扱う上で、実験で採用する信頼モデルは、重要な選択になる。
  - 階層CA、相互認証モデル、ブリッジモデルの3つの信頼モデルで実験を行う。
  - 比較的、その技術が知られた階層CAモデルから、技術的に複雑なブリッジモデルまで実験を行う。
- 3つのPKIアプリケーションを使って実験する
  - 現在、PKIで比較的使用されているアプリリケーションである、SSLクライアント/サーバ認証、IPsec 、S/MIMEの 3つを使用して実験を行う。

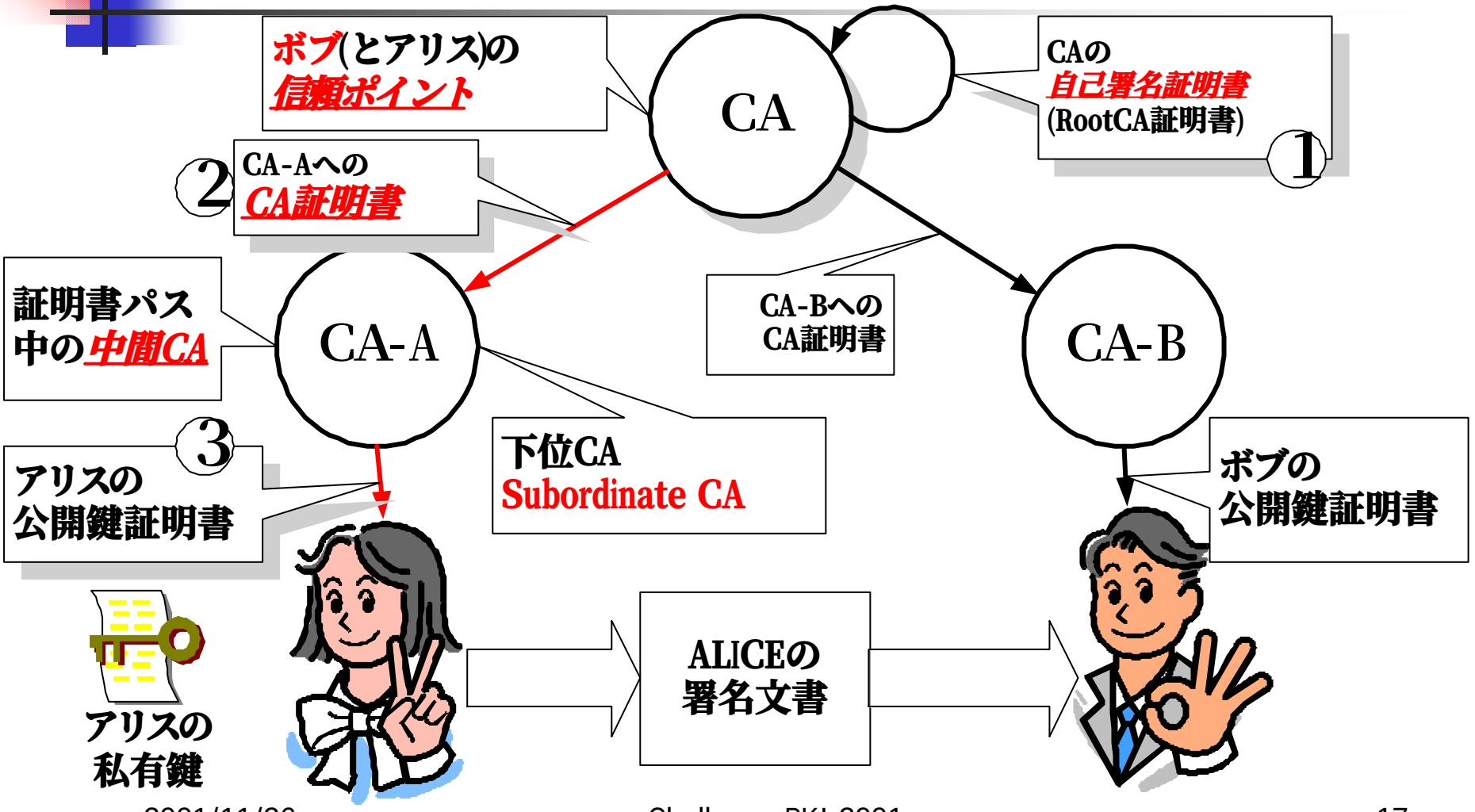
実験で使用する信頼モデル

- 階層CAモデル
  - 2レベルの単純な階層CA
  - 単純な証明書プロファイル
  - アプリケーション中心の実験
- 相互認証モデル
  - 単純な相互認証
  - 単純な証明書プロファイル
  - ブリッジモデルへのつなぎの実験
- ブリッジモデル
  - 政府認証基盤（GPKI）に準拠したブリッジモデルでの実験
  - 最低限のアプリケーションで実験
  - GPKIに近い環境を構築することがひとつの目標

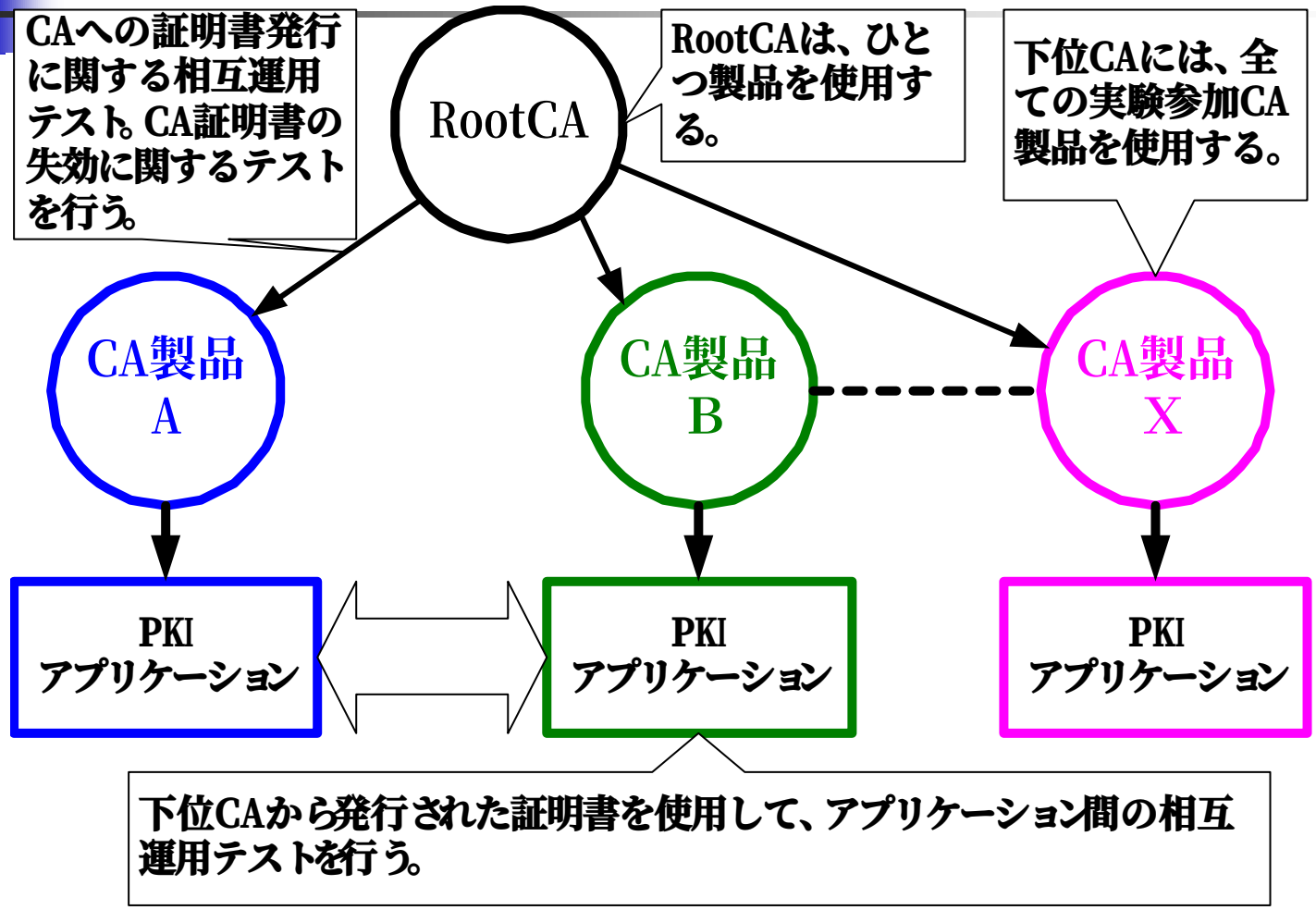
実験で使用する信頼モデル
階層CAモデルでの実験

- 実験の意義
  - 階層CAモデルは、技術的に広く知られており、マルチベンダーPKIの検証、色々なアプリケーションの実験が行い易い。
- 階層CAモデルでの実験
  - 2レベルの階層CA
  - 単純な証明書プロファイル
    - 最低限の実験のための証明書プロファイルを定義
  - レファレンスCAと下位CAから発行された証明書を使用したアプリケーション間
    - なるべく多くのアプリケーションで実験
  - 全下位CAから発行された証明書を使用したアプリケーション間
    - S/MIMEのみ行う
- 実験のポイント
  - CA間の証明書交換。
  - 主なPKIアプリケーションの動作検証。

実験で使用する信頼モデル
階層CAモデルの説明



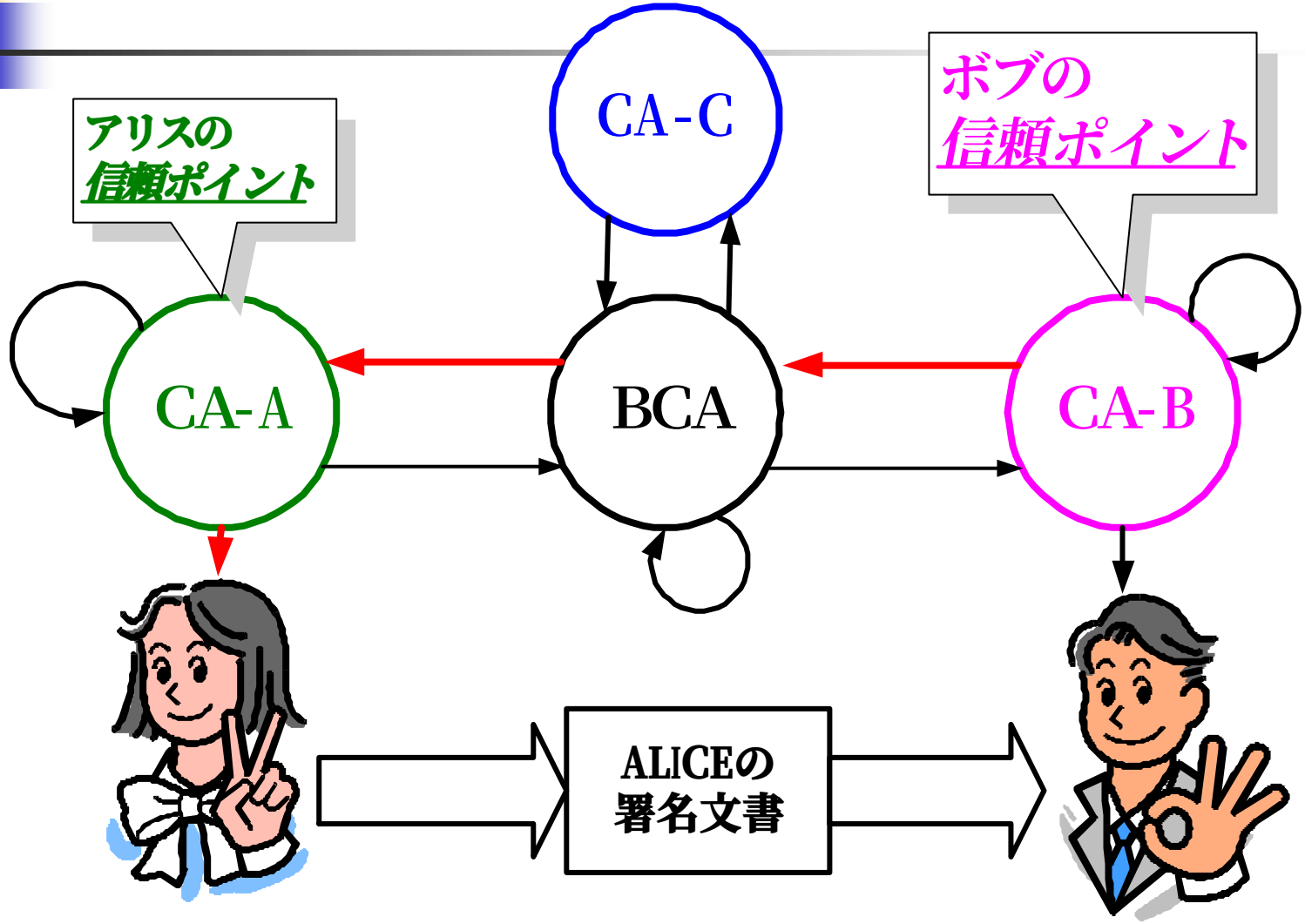
実験で使用する信頼モデル
階層CAモデルと参加CAの関係



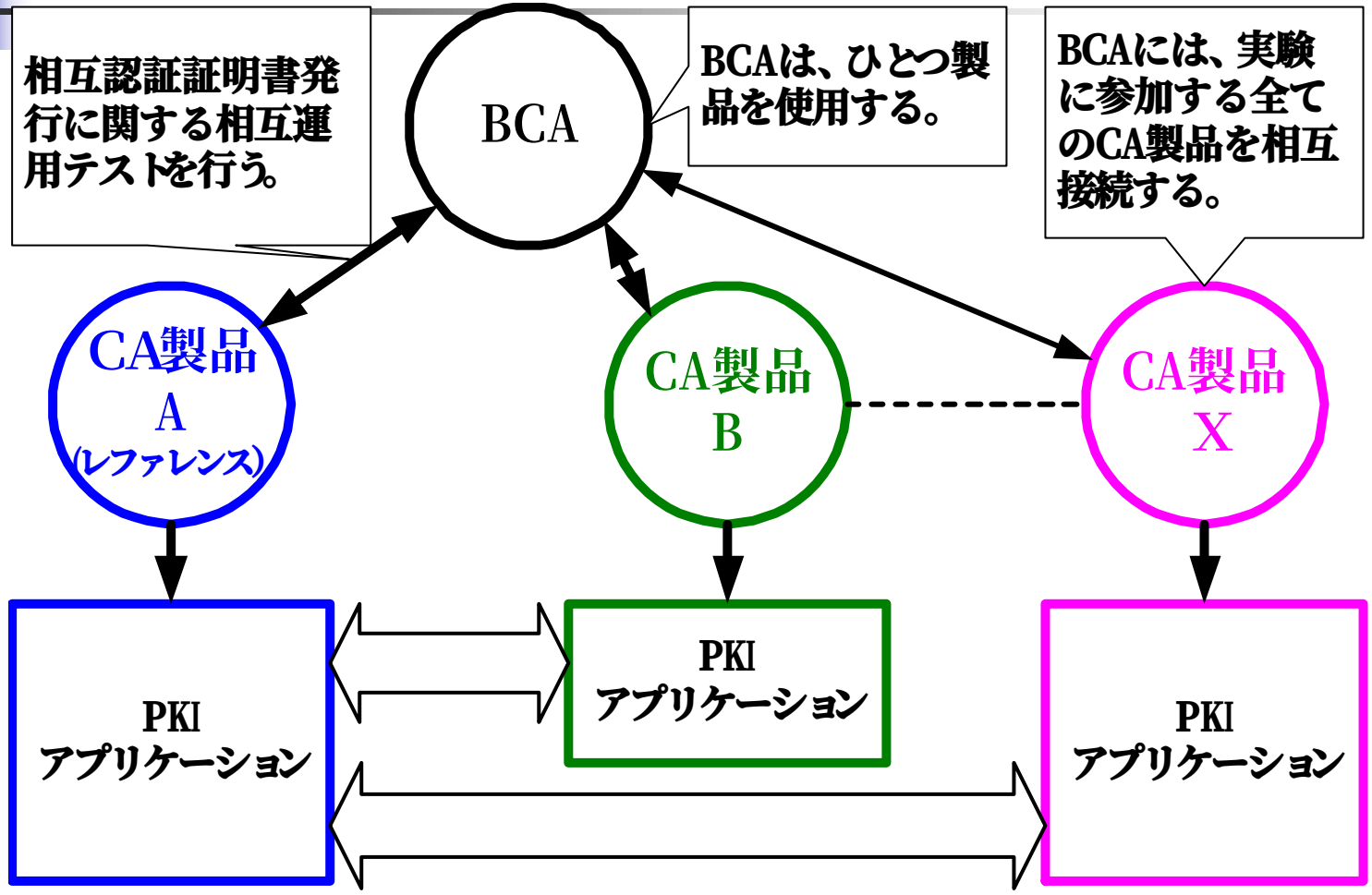
実験で使用する信頼モデル
ブリッジモデルでの実験

- **実験の意義**
  - **マルチPKIドメインの実現手段のひとつとしてブリッジモデルがある。ブリッジモデルを実現するには、多くの最新の標準を検証する必要がある。ブリッジモデルを構築することで、よりチャレンジャブルな実験を行う。**
- **ブリッジモデルでの実験**
  - **GPKI相互運用性仕様書に基づいた実験**
    - **GPK準拠、または、近い証明書プロファイルを使用**
    - **GPKIの仕様書を使うことで、実験のバックグランドとなる仕様書の作成の手間を省く。**
- **最低限のアプリケーションで実験**
  - ブリッジモデルで動作するEntrustのクライアント(S/MIMEが使用できるOutlookのプラグイン)をRelying Party側のレファレンスとして使用。
- **実験のポイント**
  - **GPKIで要求されるCAとしての証明書発行**
  - **ブリッジ環境及び、GPKI環境で、アプリケーションの仕様として何が要求されるか検証する**

実験で使用する信頼モデル
ブリッジモデルの説明



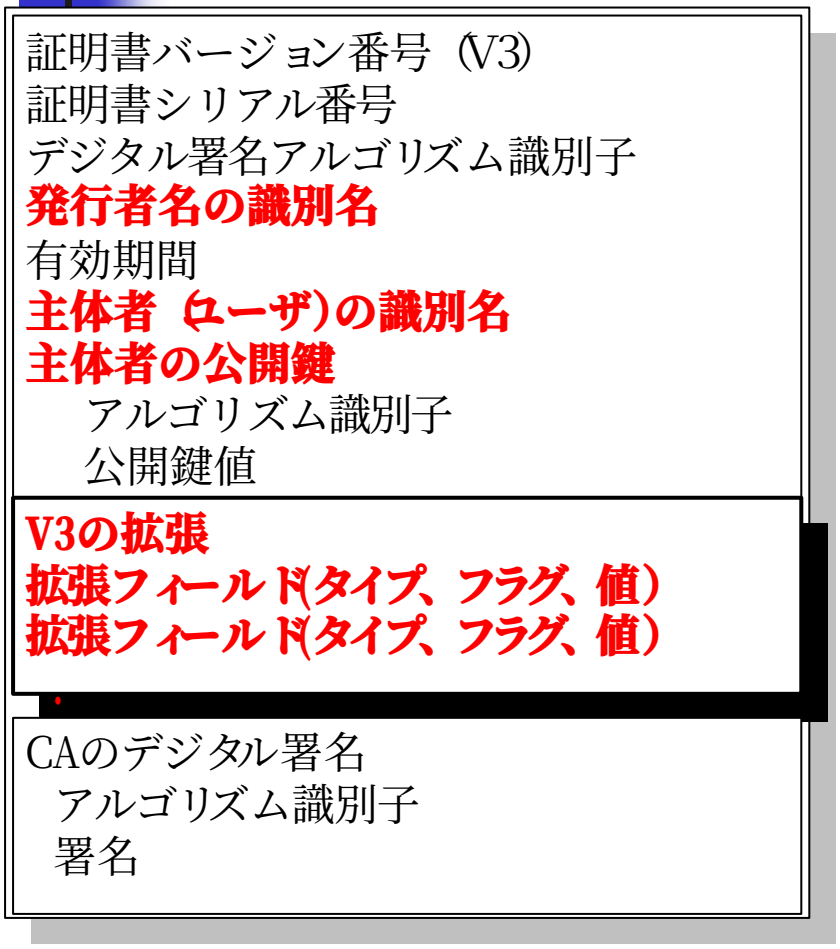
実験で使用する信頼モデル
ブリッジモデルと参加CAの関係



実験で使用するアプリケーション

- 実験で使用するアプリケーションの選択のポリシ
  - なるべく一般的に使用されているPKIアプリケーションを使用するということで、
- SSLクライアント/サーバ認証
  - Webブラウザ（IE、Netscapeなど）
  - Webサーバ（Apache、IISなど）
- IPsec/IKE
  - SSHコミュニケーション社IPsec製品など
- S/MIME
  - OutlookExpressなど
  - 実験参加団体提供のメーラ&プラグインなど
- その他のPKIアプリケーション
  - その他は、参加会社の希望など

実験で使用する証明書プロファイル X.509証明書について



- 代表的な公開鍵証明書
  - 主体者(アリス)と、主体者(アリス)の公開鍵や、その他の属性をCA鍵(アリスの証明書を発行したCAの署名鍵)の署名でバインドする。
  - この時、主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- 1997年版 X.509 3rd Edition
  - X.509v3証明書フォーマット
    - X.509v3拡張
  - 14の標準拡張フィールド
- *Challenge PKI 2001の実験で使用するのはX.509v3証明書フォーマット*

実験で使用する証明書プロファイル
X.509証明書拡張(v3拡張)

No	標準拡張(X.509v3)	説明
1	発行者鍵識別子	発行者の鍵の識別に使用されCA鍵の更新に必要
2	主体者鍵識別子	主体者の鍵の識別に使用されCA鍵の更新に必要
3	鍵使用方法	私有鍵の使用方法。例えば署名用鍵で、暗号化を禁止する
4	私有鍵有効期間	証明書の有効期間に対して、私有鍵の有効期間。
5	証明書ポリシ	証明書ポリシIDなどが格納される。ポリシによる制御などに使用
6	ポリシマッピング	信頼ドメイン間のポリシのマッピングを行う
7	主体者別名	主体者の別名が格納される。例えばVPN装置の場合のIPaddress
8	発行者別名	発行者の別名が格納される。
9	主体者ディレクトリ属性	証明書の主体者のためのディレクトリ属性
10	基本制約	証明書の種類(CAorEE)。CAだった場合パス数の制限
11	名前制約	CA証明書で、相手のCAが発行する名前による制約
12	ポリシ制約	CA証明書で、相手のCAが発行するポリシ関係制約
13	拡張鍵使用方法	"鍵使用方法"以外の鍵使用方法のOIDが格納される。
14	CRL配布点	失効情報リストの配布点のDNやURLが格納される。

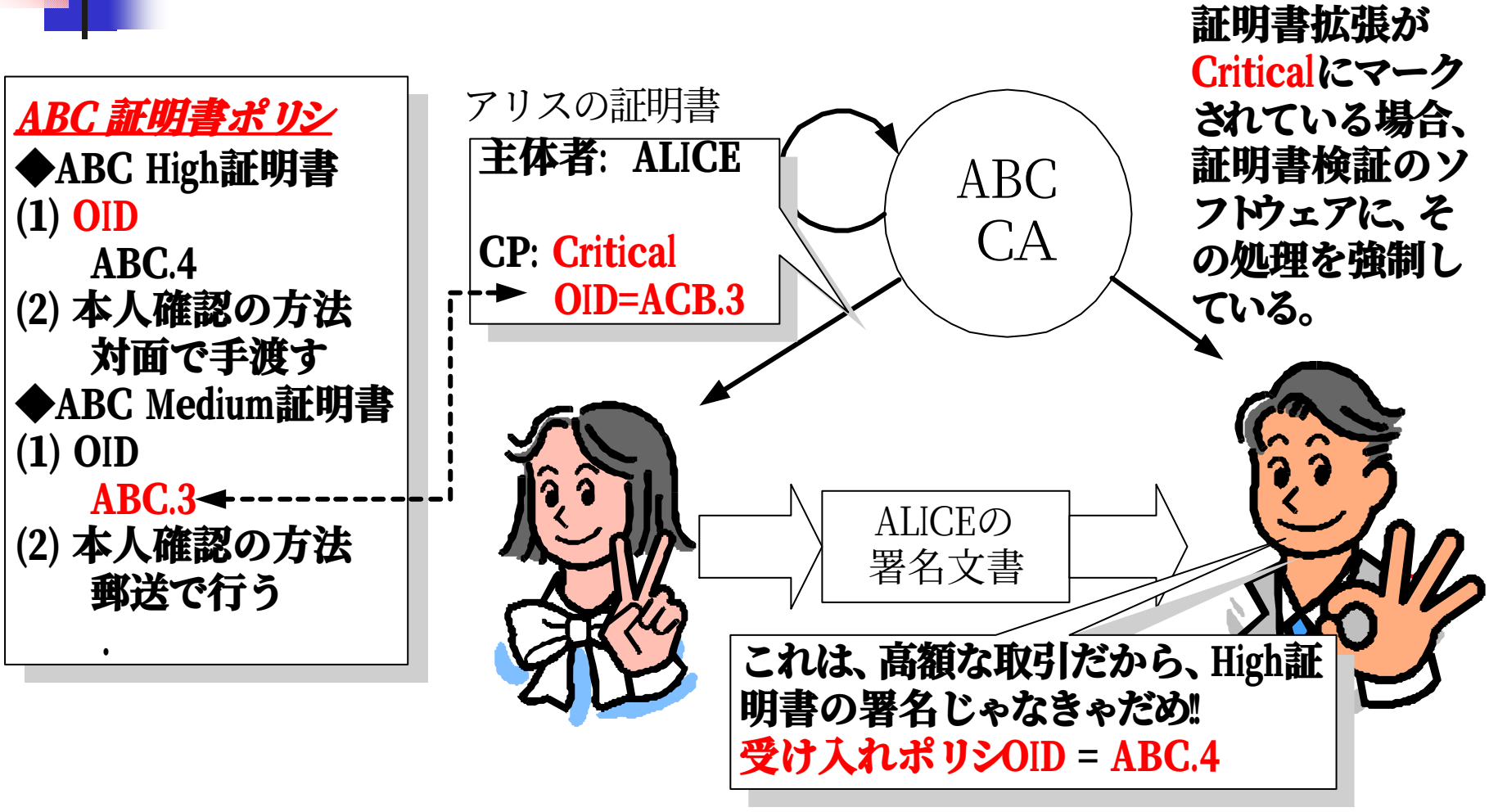
実験で使用する証明書プロファイル 証明書プロファイルの関係

- RFC2459準拠の意味するもの
  - 証明書発行そのものよりも、そのプロファイルを解釈するアプリケーションの実装が格段に難しい。アプリケーションにおいて、100% RFC2459サポートは、まずない。

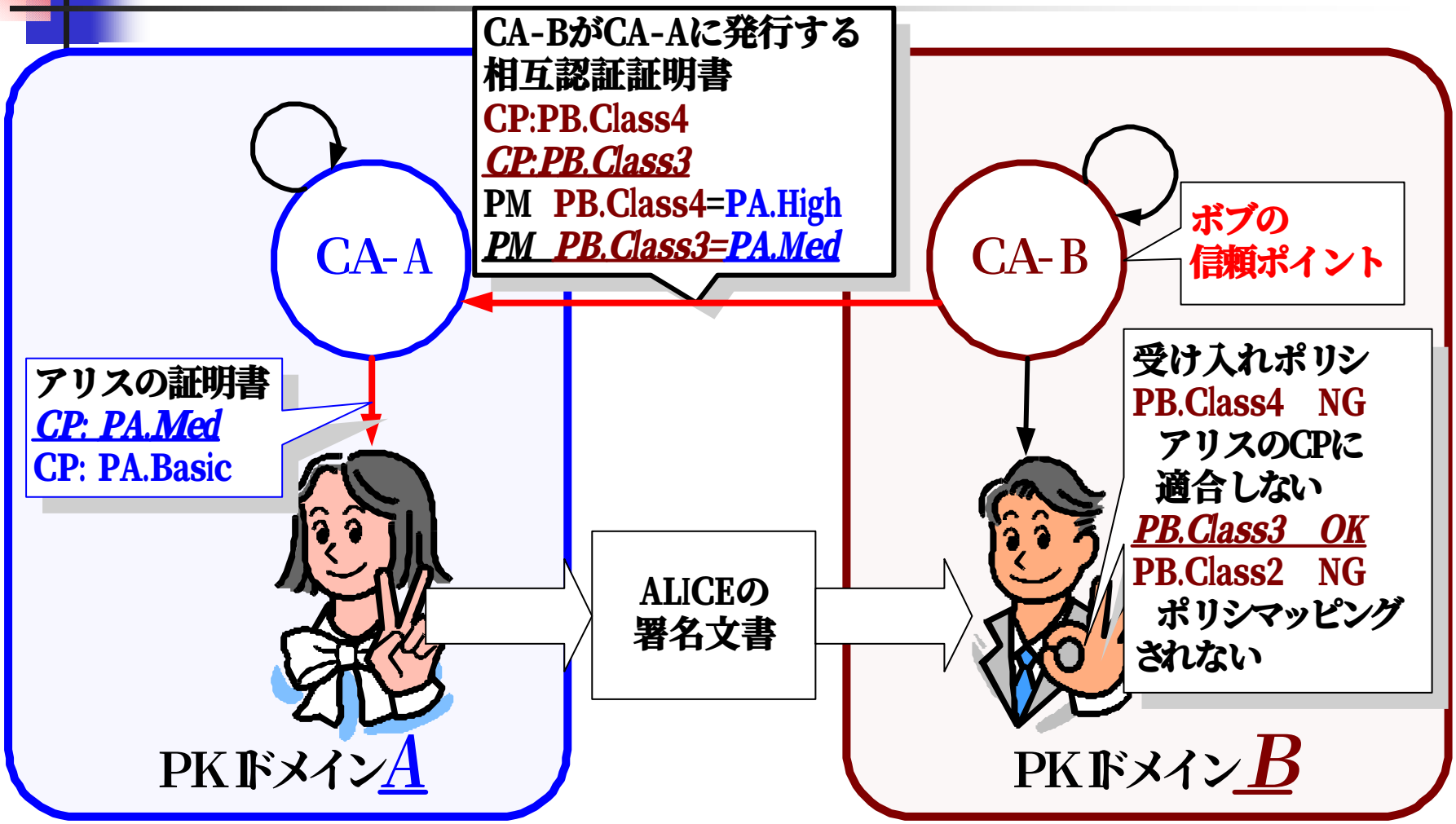
実験で使用する証明書プロファイル
各信頼モデルでの証明書プロファイル

- 実験に使用するX.509証明書・CRLフォーマット
  - 全てX.509v3証明書フォマーット
  - 全てCRLv2フォーマットとする
- 階層CAモデル
  - 基本制約拡張など
- 相互認証モデル
  - 階層CAモデルと同様
- ブリッジモデル
  - 基本的にGPKI証明書プロファイル準拠
  - 証明書ポリシ拡張、ポリシマッピング拡張などを使用する
  - CRLの拡張も重要

実験で使用する証明書プロファイル
（ブリッジモデルで使用する証明書ポリシ拡張）



実験で使用する証明書プロファイル
（ブリッジモデルで使用するポリシマッピング拡張）



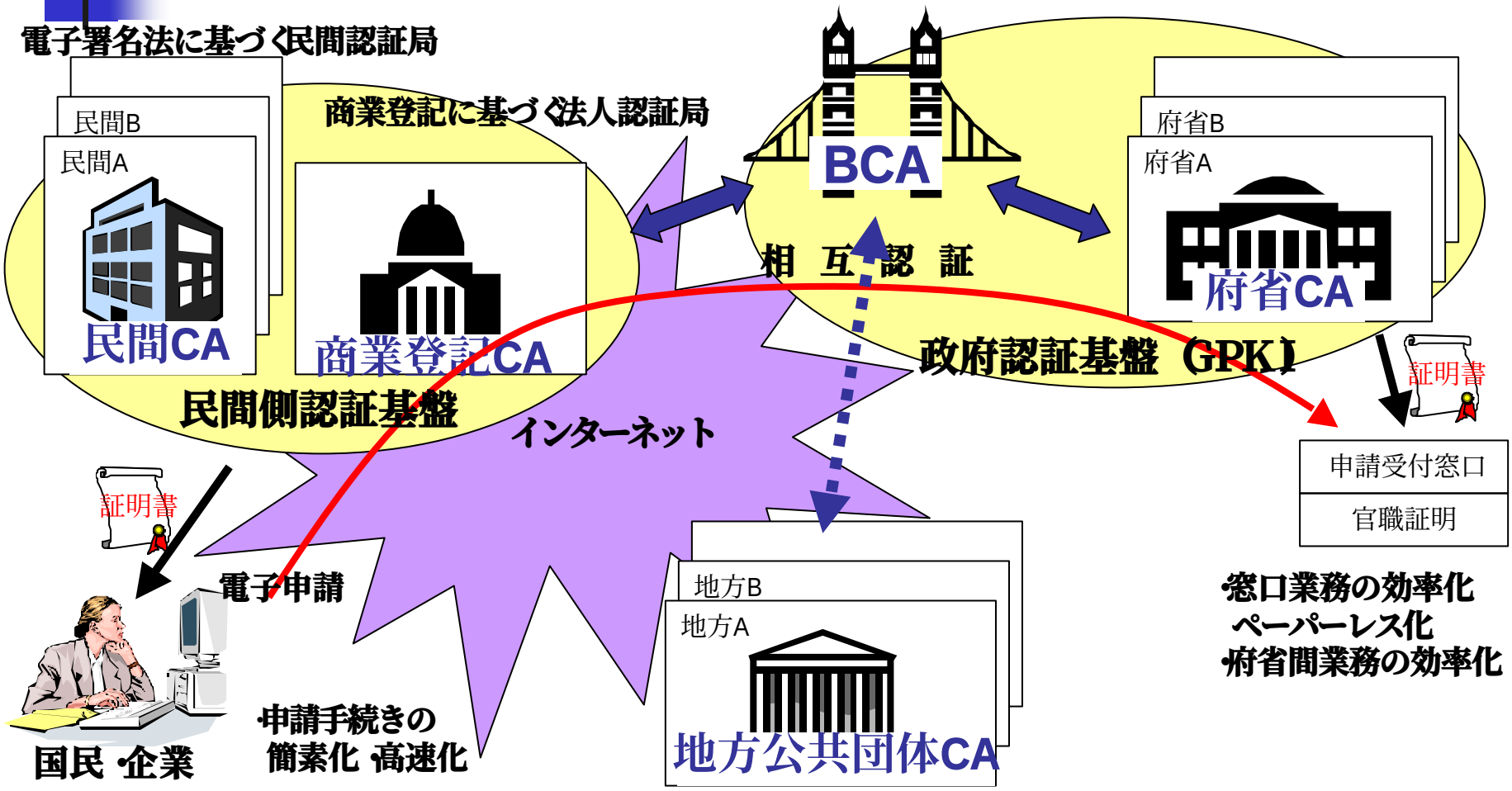
Challenge PKI 2001の参考
参考にすべき相互運用実験の事例

- 相互運用実験の例
  - 複数ベンダー、複数CAから構成されるPKIの相互運用実験は、その必然性から世界各国で行われている。実験には、広範囲で、高度な技術を要することが認識されている。Challenge PKI 2001 でもこれらを参考にして実験を進める。
- 参考にすべき例
  - GPKIの実証実験
  - PKIフォーラムの各種相互運用プロジェクト
  - EMA Challenge 2000
  - BCA Technology Demonstration　Phase 2
  - CESG　PKI相互運用テスト(イギリス)
  - EEMA Pki Challenge (EU)
  - ３国間相互運用性実証実験（日本、韓国、シンガポール）

政府認証基盤(GPKI)の実証実験

- 政府認証基盤(GPKI)ホームページ
  - http://www.gpki.go.jp/
  - 政府認証基盤(GPKI)相互運用性仕様書、接続基準、CP/CPSなどGPKIのブリッジ認証局へ接続するための要件や、実際に接続されている認証局などが公開されている。
- 政府認証基盤相互運用性仕様書
  - http://www.gpki.go.jp/session/010514_2.pdf
  - ブリッジ認証局へ接続するための技術的な要件、GPKI証明書プロファイル、GPKIで動作させるアプリケーションの要件などが記述されている
  - *Challenge PKI 2001のレファレンスの仕様書のひとつ*
- 実証実験の内容
  - http://www.gpki.go.jp/documents/arch.html
  - 2000年 1月から3月にかけて、GPKIブリッジCA、先行府省CA、商業登記CAなどが参加して、ブリッジCAを介した相互運用テストが行われた。ポリシマッピング、CA鍵更新、OCSP、証明書検証サーバなどを含んだ、高度な相互運用テストを行っている。

GPKIの概要


電子署名法に基づく民間認証局
民間B
民間A
民間CA
商業登記に基づく法人認証局
商業登記CA
民間側認証基盤
BCA
相 互 認 証
府省B
府省A
府省CA
政府認証基盤（GPKI）
インターネット
証明書
申請受付窓口
官職証明
電子申請
国民・企業
・申請手続きの
簡素化・高速化
地方B
地方A
地方公共団体CA
・窓口業務の効率化
ペーパーレス化
・府省間業務の効率化

GPKI証明書プロファイルの特徴

(Challenge PKI 2001の実験でも使用するプロファイル)

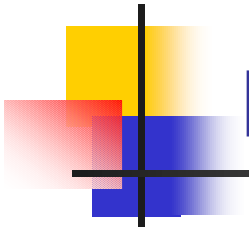
フィールド	critical	相互認証証明書	自己署名証明書	リンク証明書	官職証明書	申請者証明書	クライアント	補足
keyUsage	TRUE	○	△	○	○	○	サポート	※1
certificatePolicies	TRUE	○	×	○ non-critical	○	○	サポート	※2
policyMappings	FALSE	○	×	×	×	×	サポート	
basicConstraints	TRUE	○	○	○	△ non-critical	△ non-critical	サポート	※3
nameConstraints	TRUE	△	×	×	×	×	サポート	※4
policyConstraints	TRUE	△	×	×	×	×	サポート	

【補足】
※1:自己署名証明書とリンク証明書のcriticalはTRUE/FALSEどちらでも可。
※2:少なくとも1つ以上のCertPolicyIDを含む。リンク証明書ではanyPolicyを入れる。
※3:cAはTRUE（官職証明書、申請者証明書はFALSE）。自己署名証明書のcriticalはTRUE/FALSEどちらでも可。
※4:少なくともpermittedSubtreeを含む。

○ :含めることは必須 △ :含めることはオプション × :含めることは禁止

PKIフォーラムの各種相互運用プロジェクト

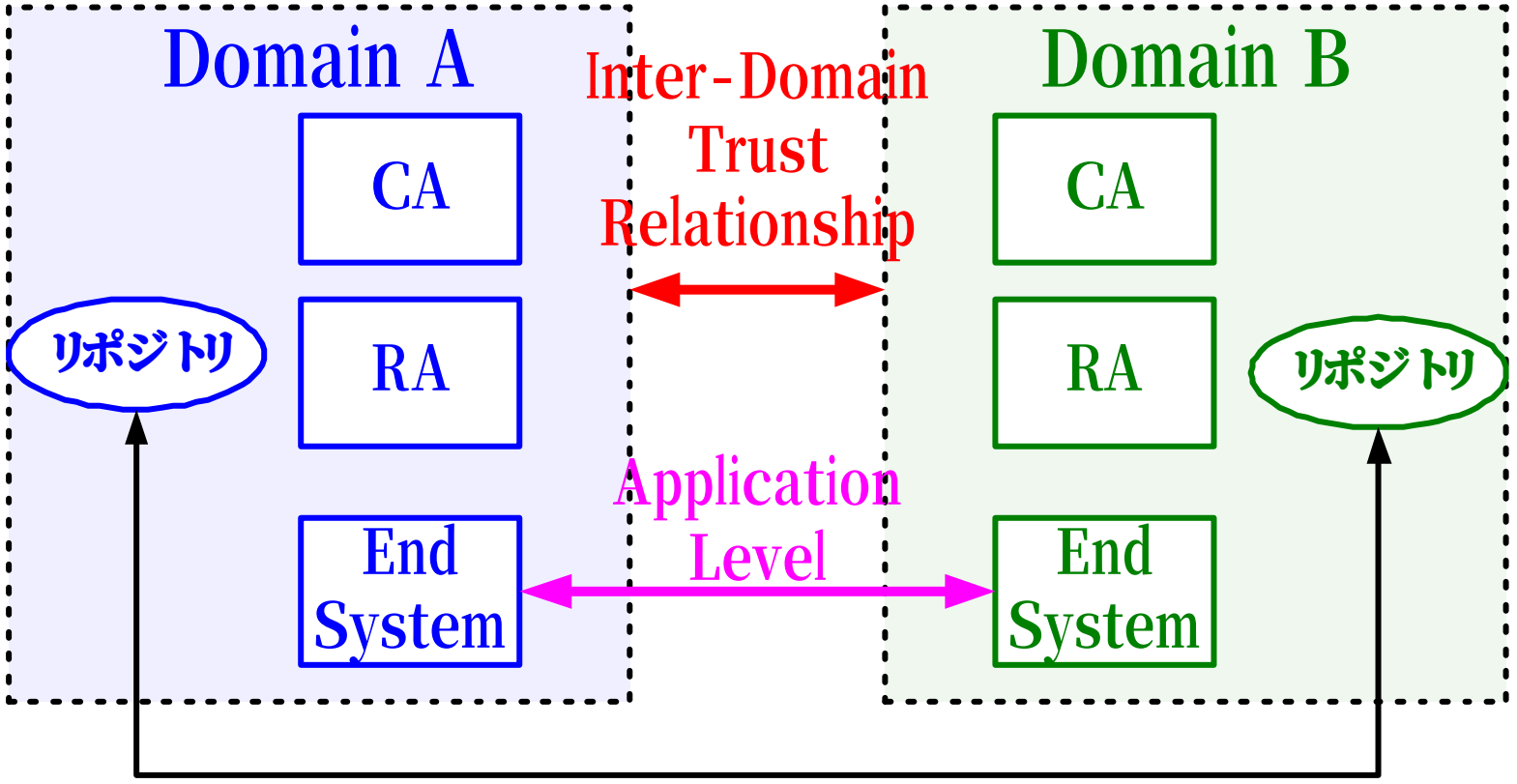
- PKIフォーラムの各種相互運用プロジェクト
  - CMPv2 interoperability、Application Certificate interoperability、CA-CA interoperability、Token Portability and interoperability、OCSP interoperability、CMC interoperabilityなどが行われている。詳細な結果は公表されていないが、その成果はWhitePaperなどに反映されている。
- PKIフォーラムのWhitePaper
  - 「複数CA製品を使用した相互運用実験」にも非常に関係あるWhitePaperがある。
    - http://www.pkiforum.org/resources.html
  - PKI Interoperability Framework White Paper
    - PKIフォーラムの相互運用モデル
      - *PKI相互運用とは何かを知る上で非常に重要*
  - CA-CA Interoperability White Paper
    - CAの信頼モデルなど

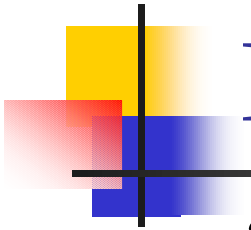


PKIフォーラムの相互運用モデル

- Interoperability Framework
  - Component-Level Interoperability
    - LDAP,OCSP,PKIX-CMP,SCEP　etc…
    - CA-CA、CA-RA、クライアント-CA、クライアント-RA
  - Application-Level Interoperability
    - S/MIME,IPsec/IKE,TLS/SSL,etc…
  - Inter-Domain Interoperability
    - *Challenge PKI 2001でも実験で取り上げるブリッジモデルでは重要なテーマ*

PKIフォーラムの相互運用モデル（ドメイン間の相互運用）

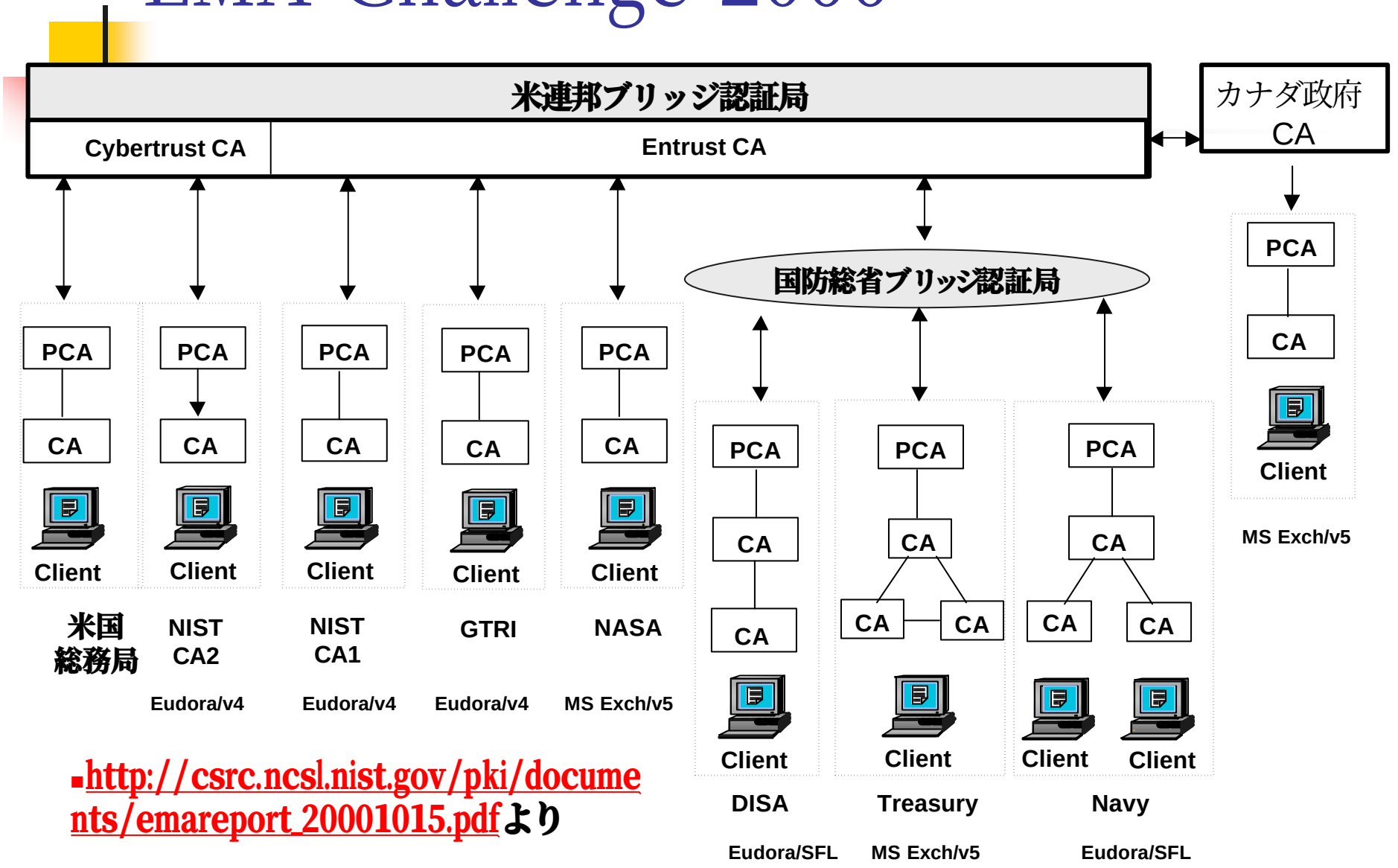




EMA Challenge 2000

- 2000年4月に行われた、米連邦ブリッジ認証局(FBCA)を利用した公開鍵インフラストラクチャ(PKI)相互運用のデモンストレーション
- 実験に参加した規模や内容の概要
  - 5つのCA製品
    - Entrust、Cybertrust、モトローラ、Spyrus、CygnaCom
  - 4つのディレクトリ製品
  - 階層モデル、メッシュモデルなどのPKIをブリッジで相互認証
  - 最大で7つの証明書パス
  - PKIアプリケーションとしてS/MIMEを使用
- 報告書
  - http://csrc.ncsl.nist.gov/pki/documents/emareport_20001015.pdf

EMA Challenge 2000



- http://csrc.ncsl.nist.gov/pki/documents/emareport_20001015.pdf より

Bridge Certification Authority Technology Demonstration Phase 2

- 概要
  - Phase 1(EMA Challenge 2000同様)に対して以下を追加している
    - ポリシマッピング、証明書ポリシ、名前制約などの証明書拡張
    - 属性証明書によるWebのアクセス制御
    - S/MIMEv3での暗号化メール(Phase1では署名のみ)
    - 複数署名アルゴリズム＆複数ハッシュアルゴリズムの混在
      - RSA/DSA or DSA/SHA-1
- 参加ベンダー
  - 政府 (NSA)
  - CA
    - Cygnacom(BCA)、Entrust、Baltimore、SETECS、Spyrus、Motorola
  - その他
    - Entgrity、Getronics、A&N Associates

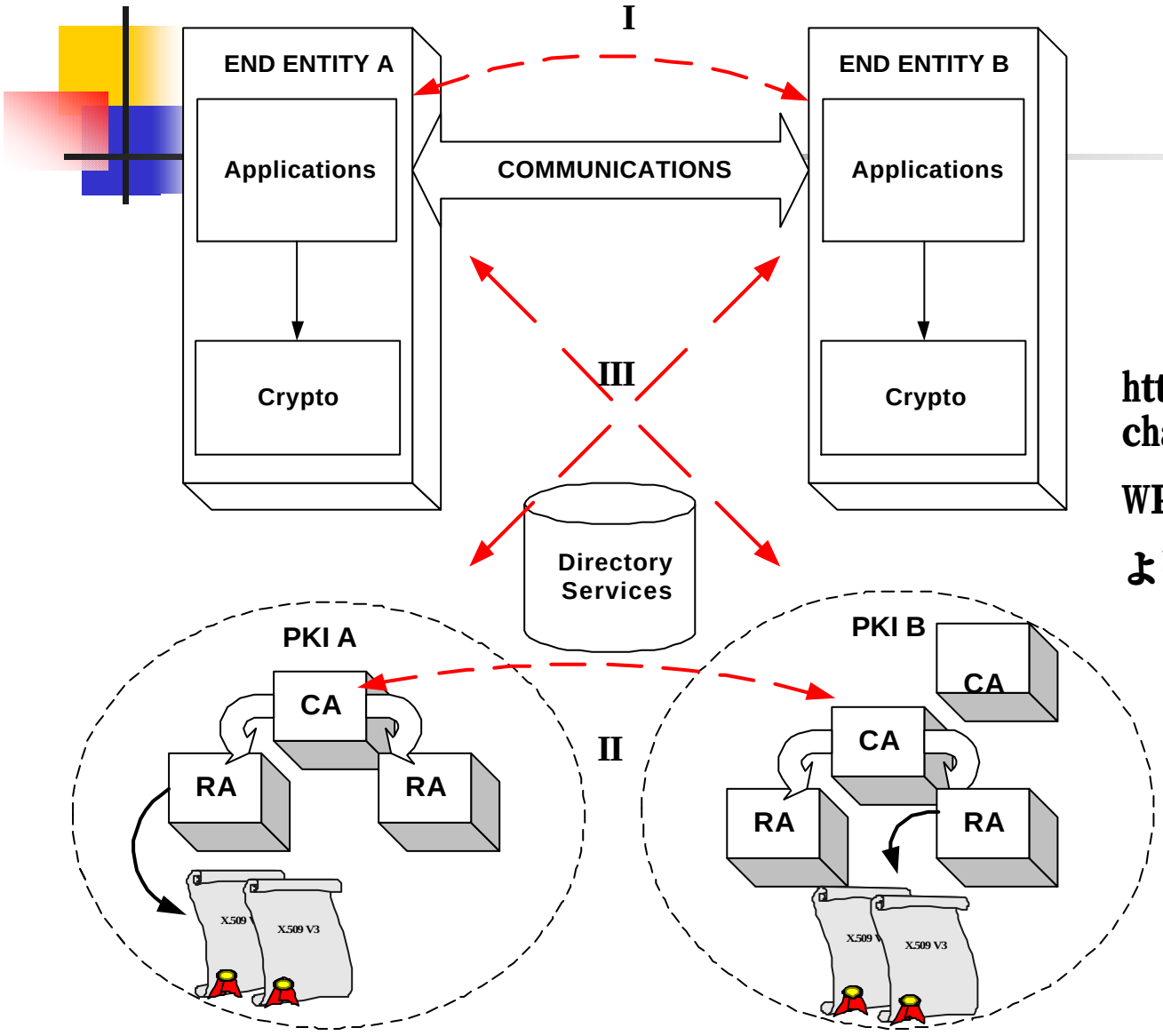
CESG PKI相互運用テスト (英国通信電子セキュリティ・グループ)

- 概要
  - 昨年、CESGで行われた、階層CA、マルチベンダー下でのS/MIMEの相互運用テストが中心のPKI相互運用テスト
  - Baltimore TechnologiesのRootCA下に7社のCA製品を下位CAに配置した階層CAモデルでの実験
- 参加企業
  - Baltimore Technologies、Compaq、Entegrity Solutions、Entrust、Novell、Reflex Magnetics、Shym、Spyrus、SSE、XCert (now RSA Security)
- 今後
  - PKIフォラームや、EEMAのPki Challengeと協調??
- 報告書
  - http://www.cesg.gov.uk/cloudcover/PKIdemonstrator.htm
  - Secure Messaging And PKI Interoperability Demonstrator Final Report
    - 2001年3月1日

Pki Challenge

- Pki Challengeの概要
  - PKIの相互運用を目指したプロジェクト
    - 資金は、ヨーロッパ委員会が提供。実施はEEMA
  - EEMA(European Forum for Electronic Business)
    - EEMAは、32ヶ国、273団体から構成される業界団体
  - 2001年Q1から2年間のプロジェクト
  - 参加メンベーの中で実験の内容自体を計画中。非常に幅広い実験を計画しており非常に参考になる。
  - http://www.eema.org/pki-challenge/
- 参加組織
  - Entrust, BaltimoreのようなPKIベンダー、Globalsignのような認証プロバイダ、UK Postのようなユーザ、KPMGのような監査コンサルタント、その他大学など幅広い組織が参加している。

Pki Challengeの相互運用モデル



http://www.eema.org/pki-challenge/files/WP2N006v2.

WP2 N006–相互運用テストの提案

より

Pki Challengeの相互運用モデル

- インタフェース[Ⅰ]
  - アプリケーションへ間
  - S/MIME、IPsec、SSL
- インタフェース[Ⅱ]
  - PKIサービス
  - PKIX CMP/CMC
- インタフェース[Ⅲ]
  - ディレクトリ&有効性検証サービス
  - LDAPディレクトリインタフェース
  - ディレクトリスキーマ
  - CDPs &デルタCRLsへのディレクトリサポート
  - OCSP

Pki Challengeの計画

WP No.	Work pakege名	工数 人月	2001				2002			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	プロジェクト管理	16								
2	技術の範囲と定義 相互運用の基準	9								
3	参加者の契約と確認	2.5								
4	テストプランの詳細	6								
5	テスト環境の構築	5								
6	相互運用性テスト	10.5								
7	デモと普及	4								
8	最終報告	2.5								
全体		55.5								

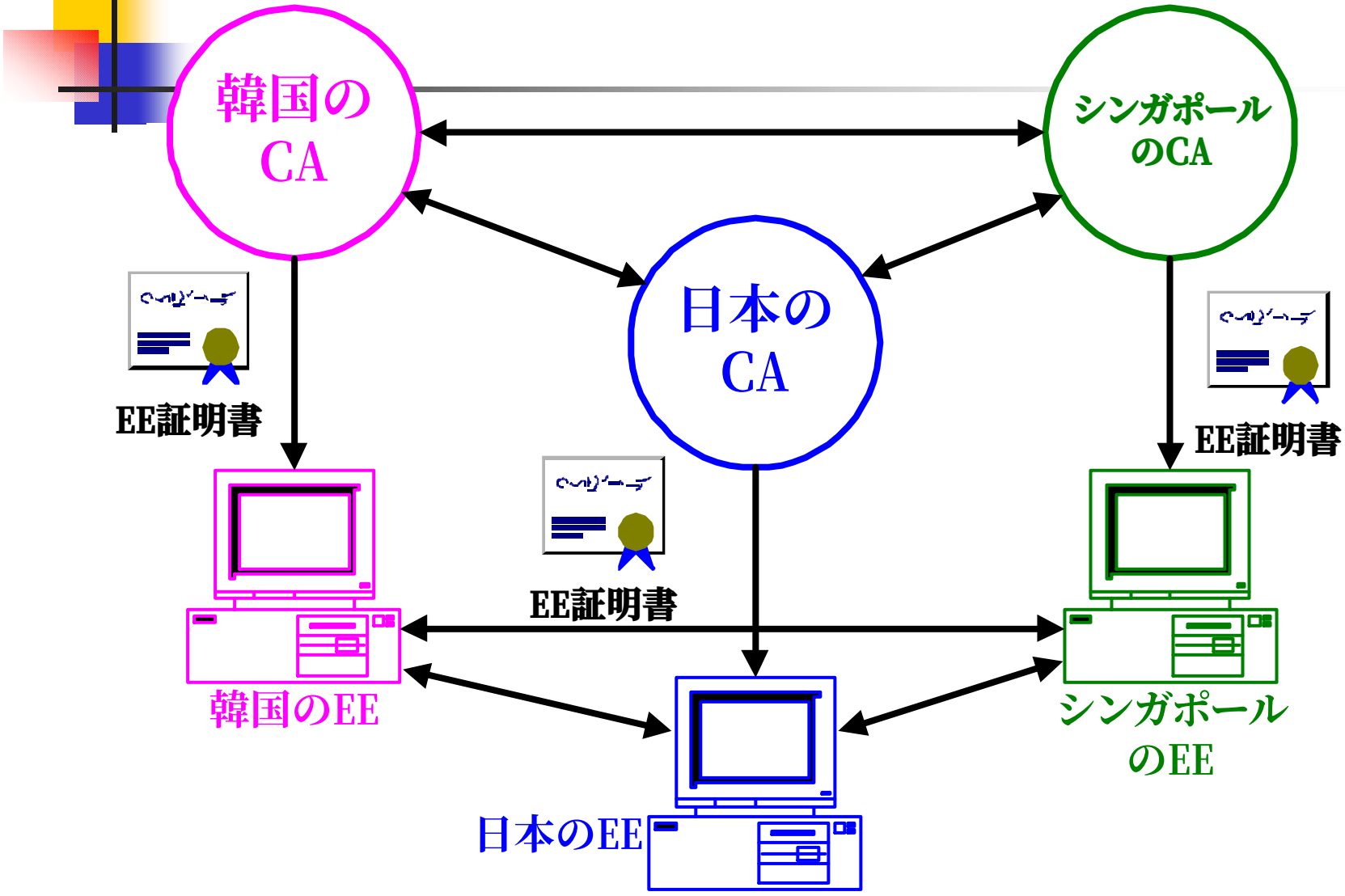
ＷＰ2の成果物であるWP2NO13- Interoperability Test Criteriaが非常に参考になる

http://www.eema.org/pki-challenge/files/WP2-N013.pdf

アジアPKIフォーラム推進会議と３国間相互運用性実証実験

- アジアPKIフォーラム推進会議(APKI-J)
  - http://www.apki-j.gr.jp/
  - アジア諸国と協力しながらアジア共通の電子認証基盤（アジアPKI）を構築するための活動
  - 日立、NEC、富士通など中心になって立ち上げた。メーカ、商社、銀行などの参加メンバーが多い。
- ３国間相互運用性実証実験
  - http://www.apki-j.gr.jp/suishin/suishin_index.htm
  - 日本、韓国、シンガポールの3国間での相互認証の実証実験
  - 日立、NEC、富士通、三菱、セコム、大日本印刷、NTTコミニュケーションズの7社が参加（国際間相互認証実証実験推進会議）
  - アジアPKIフォーラム推進会議の相互認証WGとの連携

３国間相互運用性実証実験



各実験のとの比較

実験名	地域・主催	信頼モデル	実験アプリケーション	その他
GPKIの 実証実験	日本 総務省ほか	比較的単純なブリッジモデル	GPKIテストプログラム	BCA、3府省CA、商業登記CA、テストCA
EMA Challenge 2000	米国 EMA	階層、メッシュが混在したブリッジモデル	S/MIME	5つのCA製品。最大７つの証明書パス
BCA Technology Demonstration Phase 2	米国 NSA他	階層、メッシュが混在したブリッジモデル	S/MIME、属性証明書などの使用	6つのCA製品。複数署名アルゴリズムなど
CESG PKI相互運用テスト	英国 CESG	階層モデル	S/MIME	7つのCA製品。
EEMA Pki Challenge	EU	3レベルの階層モデル 相互認証モデル	各種のPKIアプリケーションを検討中	-
3国間相互運用性 実証実験	日本、韓国 シンガポール	2001年11現在未発表	-	-
JNSA Challenge PKI 2001	*日本 JNSA/IPA*	*階層モデル、相互認証モデル、ブリッジモデル*	*SSLクライアント認証、IPsec、S/MIME*	*9つのCA製品 サービスを含む)*

Challenge PKI 2001の参考 PKI相互運用性関係の参考情報

- GPKI勉強会
  - GPKIの相互運用等に関する提言を行っている
  - *主催者の宮川祥子氏は、Challege PKI2001のプロジェクトメンバー*
  - http://siren.sfc.keio.ac.jp/GPKI/
- 松本が講師を務めたセミナの資料
  - 「PKIの相互運用とOpen PKIの流れ」
    - 主に主にドメイン間の相互運用をテーマにしたセミナの資料
    - http://www.iaj.or.jp/bukai/isec/forum/20001207report.html
    - http://www.iaj.or.jp/bukai/isec/forum/20001207.pdf
  - 「PKIのアプリケーション環境」
    - ハードウェアトークンの相互運用などを取り上げている
    - http://www.iajapan.org/bukai/isec/forum/2001/20010510report.html
    - http://www.iajapan.org/bukai/isec/forum/2001/pki.pdf

Challenge PKI 2001の参考
PKI相互運用性関係の参考情報（書籍）

- PKI 公開鍵インフラストラクチャの概念、標準、展開
  - C・アダムズ、S・ロイド著、鈴木 優一 訳
  - 2000年7月15日 初版第1刷発行
    出版社 ピアソン・エデュケーション
    （SBN4-89471-248-2)
  - *訳者の鈴木優一氏はChallege PKI2001のプロジェクトメンバー*

- PKI と電子社会のセキュリティ
  - (ISBN4-320-12028-0)
  - 青木隆一・稲田 龍 著
  - 村井 純 監修
  - 菊判, 248頁, 3300円
  - *著者の一人、稲田 龍氏はChallege PKI2001のプロジェクトメンバー*