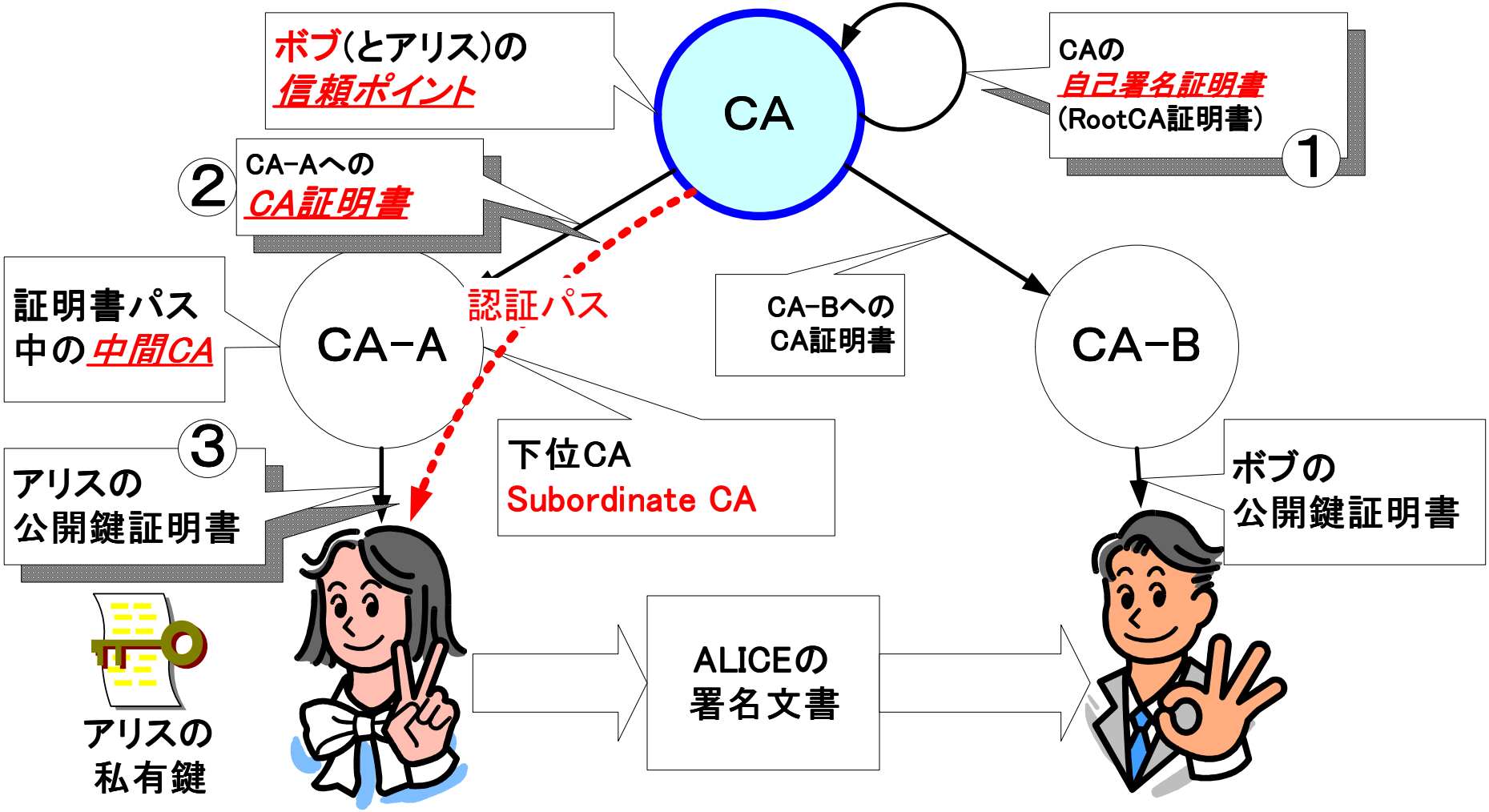
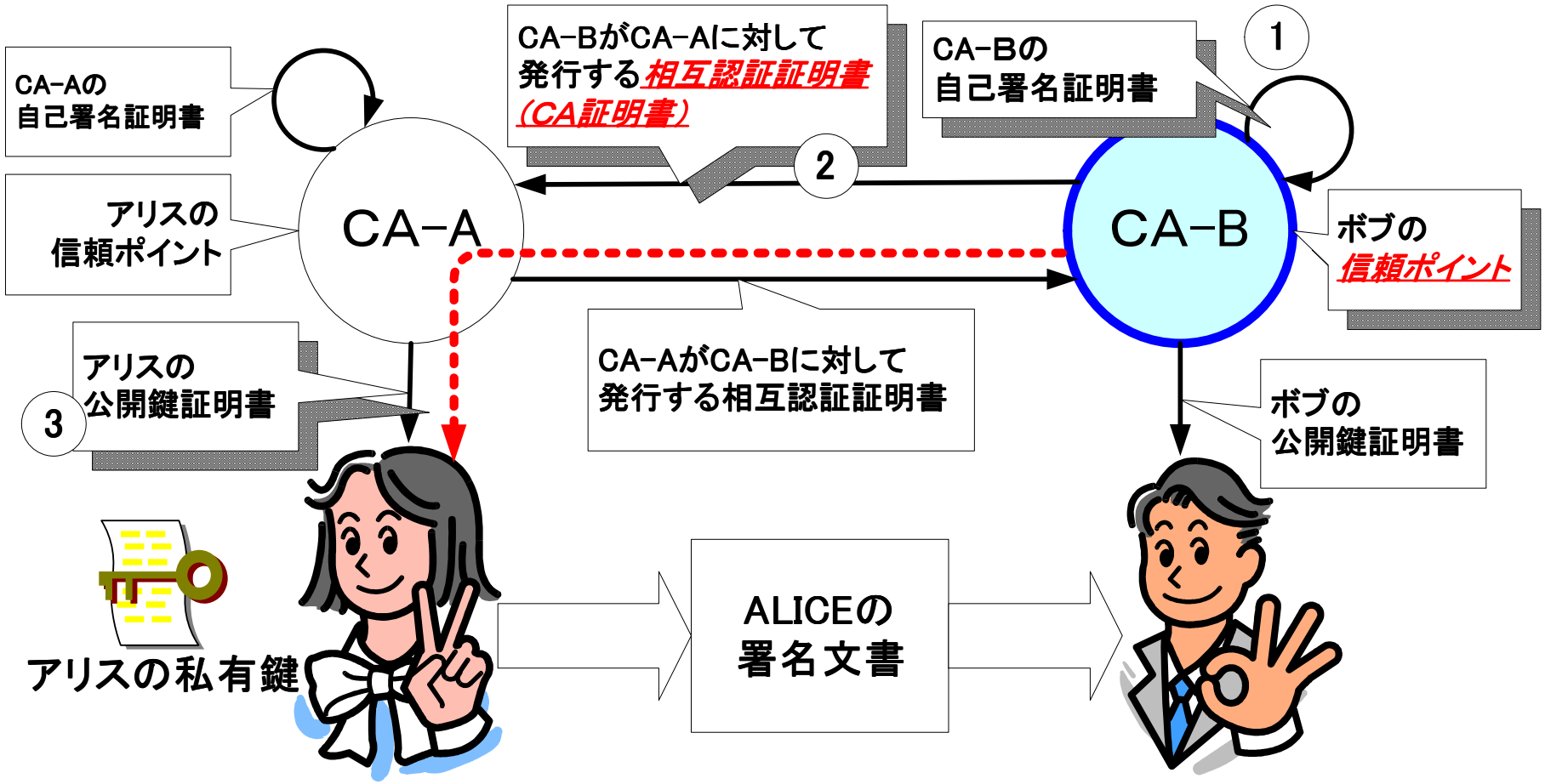
セコムIS研究所
Intelligent Systems Laboratory

リライングパーティ/検証者

リライングパーティ/検証者
階層型CAモデル

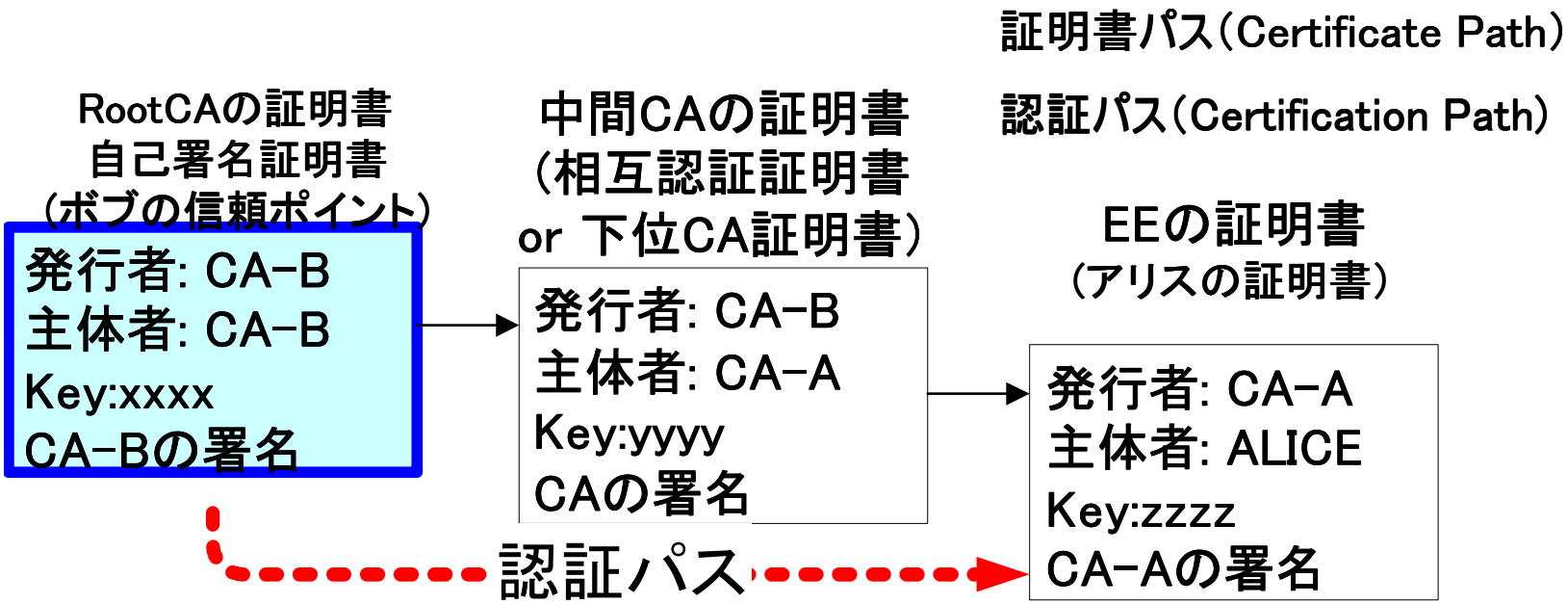


リライングパーティ/検証者
相互認証モデル(Cross certificate)

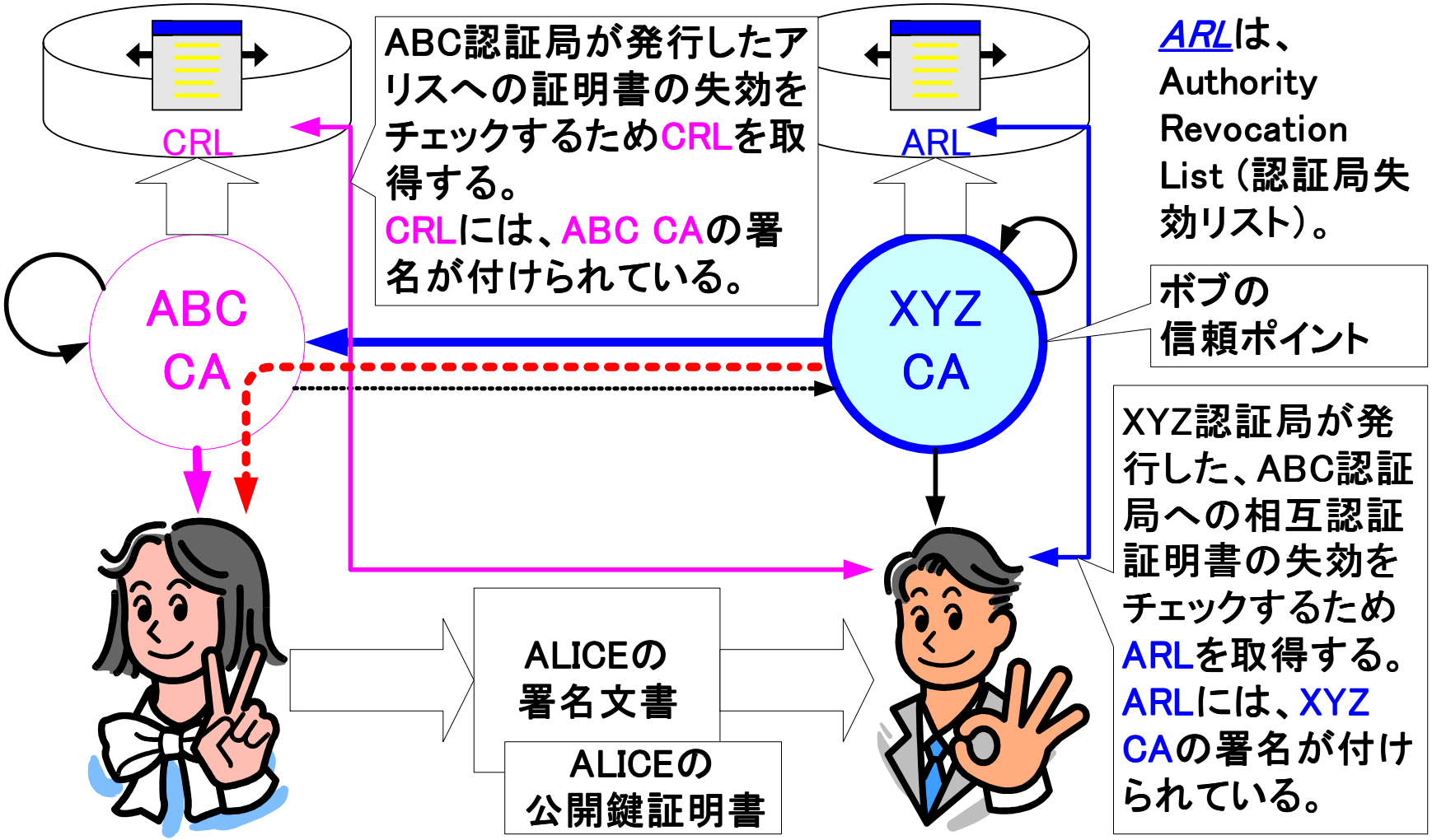


リライングパーティ/検証者
認証パスとは何か？

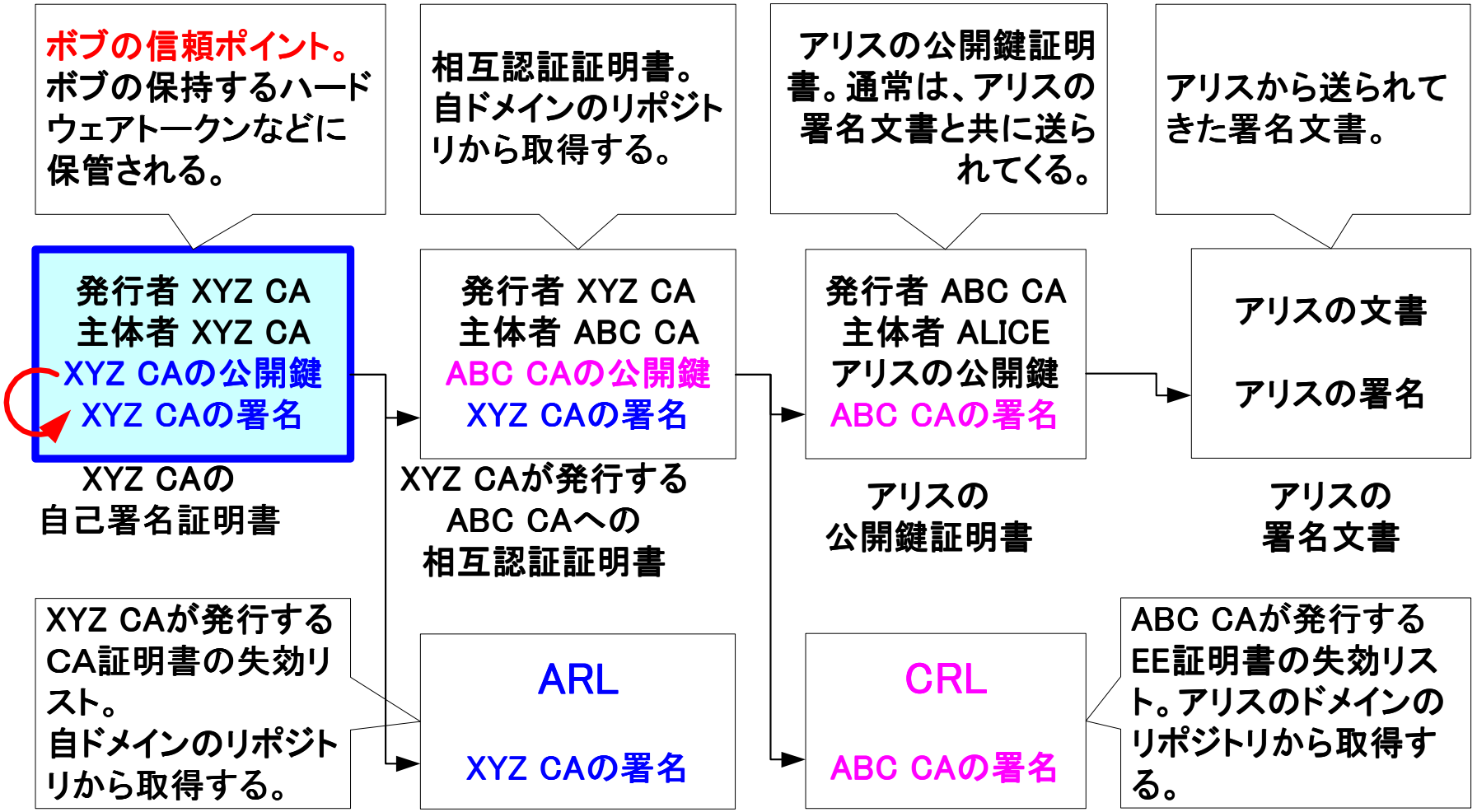
- ボブ(RP)はアリス(SC)からのメッセージを受け取った。
- ボブは、アリスからのメッセージの署名を検証したい
- 自分(ボブ)の“*信頼のポイント*”(ボブのRootCA)からの*認証パス*を検証する
- 検証は署名のチェーンの検証だけでなく、各証明書の失効チェック、そしてX.509証明書拡張に関する検証が行われる。



リライングパーティ/検証者
4コーナモデルでのCRL/ARLによる失効情報の取得



リライングパーティ/検証者
CRL/ARLと証明書検証

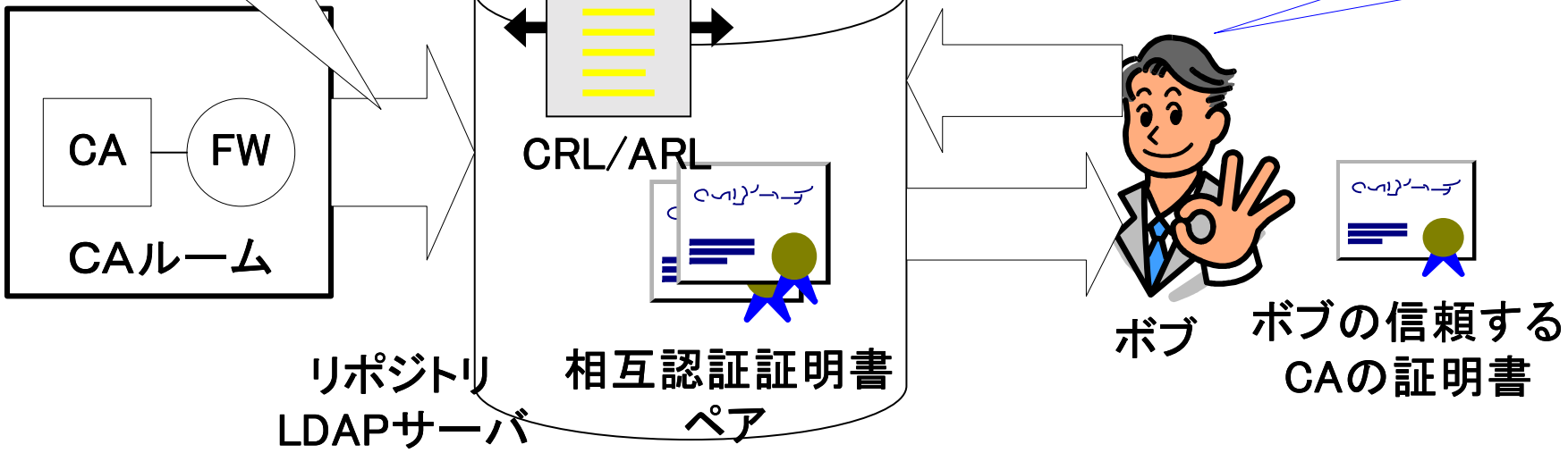


リライングパーティ/検証者
PKIにおけるリポジトリ

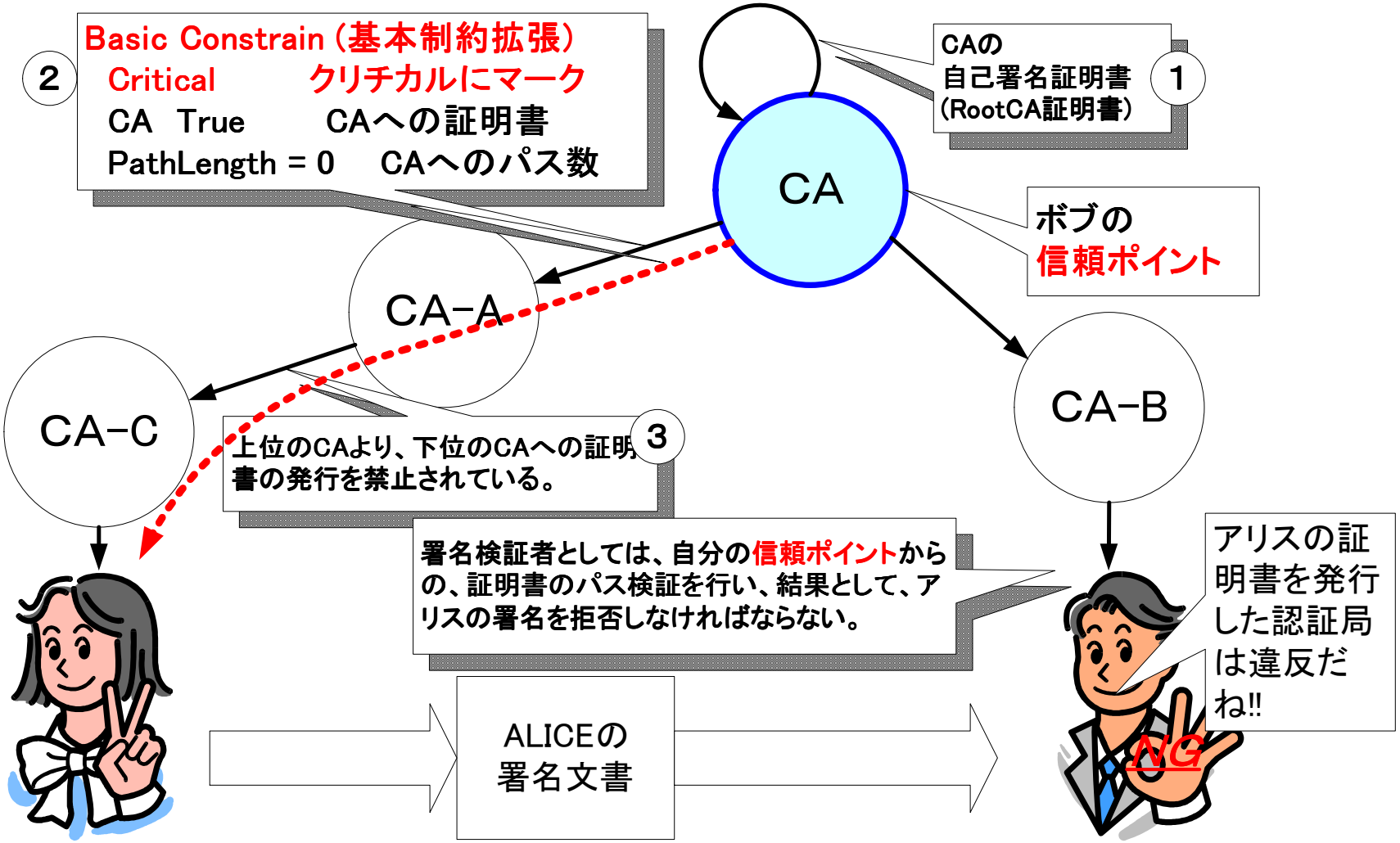
CAからは、定期的、非定期的にCRL/ARLがリポジトリに登録される。また、証明書も必要に応じて登録される。PKI的に重要なことは、登録されるものは、CAの署名がなされること

リポジトリは、証明書ユーザからアクセス可能な場所に置かれる。PKIを利用するアプリケーションから常にアクセスされるため、一般に耐障害性が要求される。

(Relying Partyの)ボブは、証明書検証のため、リポジトリ(LDAPサーバ)をアクセスする。ボブは、リポジトリに格納されたデータの内容を無条件に信用するわけではなく、自分が信頼するCAの証明書の公開鍵からの署名チェーンをチェックする。



リライングパーティ/検証者
X.509v3証明書の基本拡張基本制約拡張



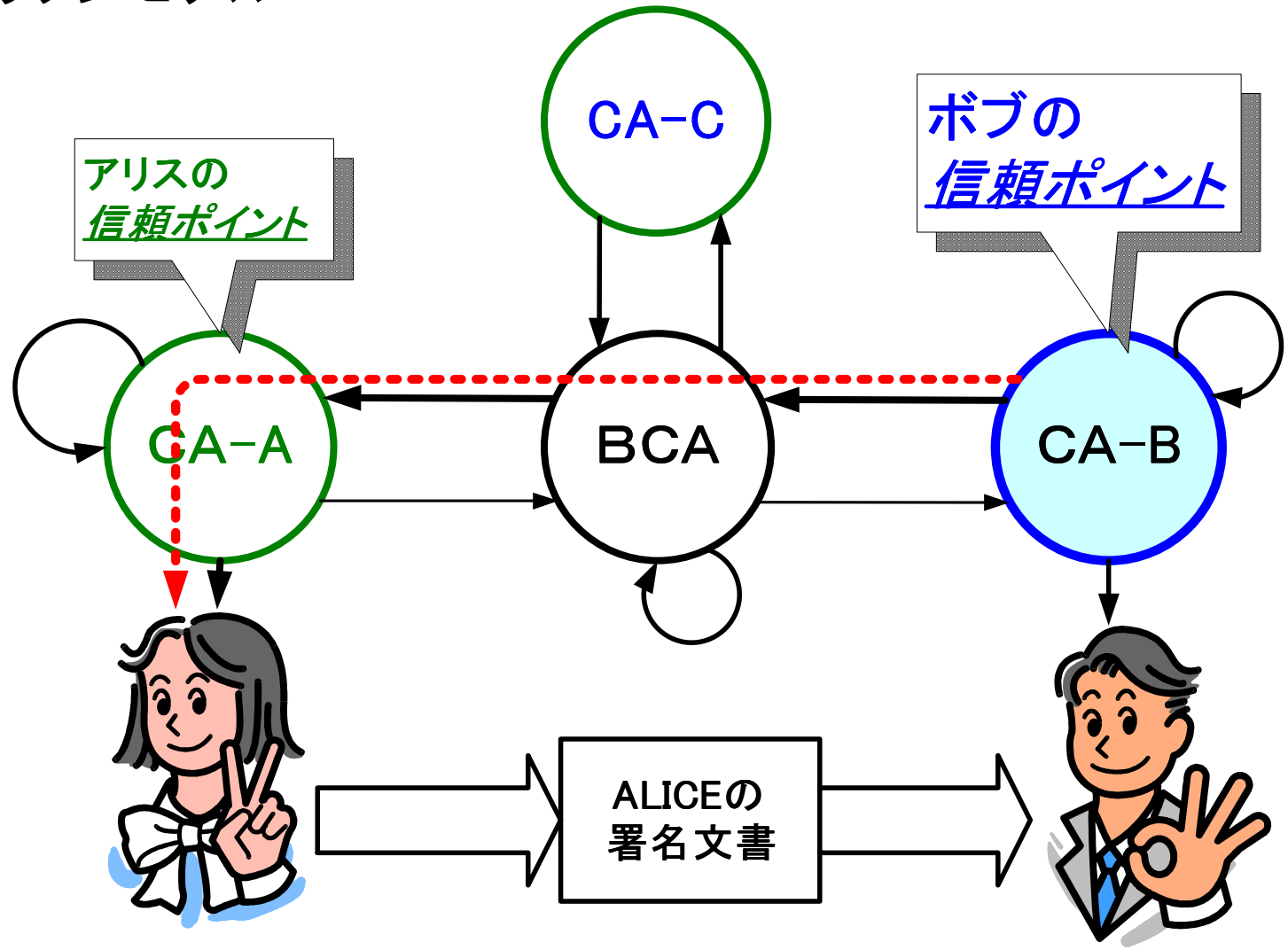
** GPKIでは、CA証明書でクリチカルな基本制約拡張を必須としている。

リライングパーティ/検証者
基本制約拡張の実装のバグ

セコム IS 研究所
Intelligent Systems Laboratory

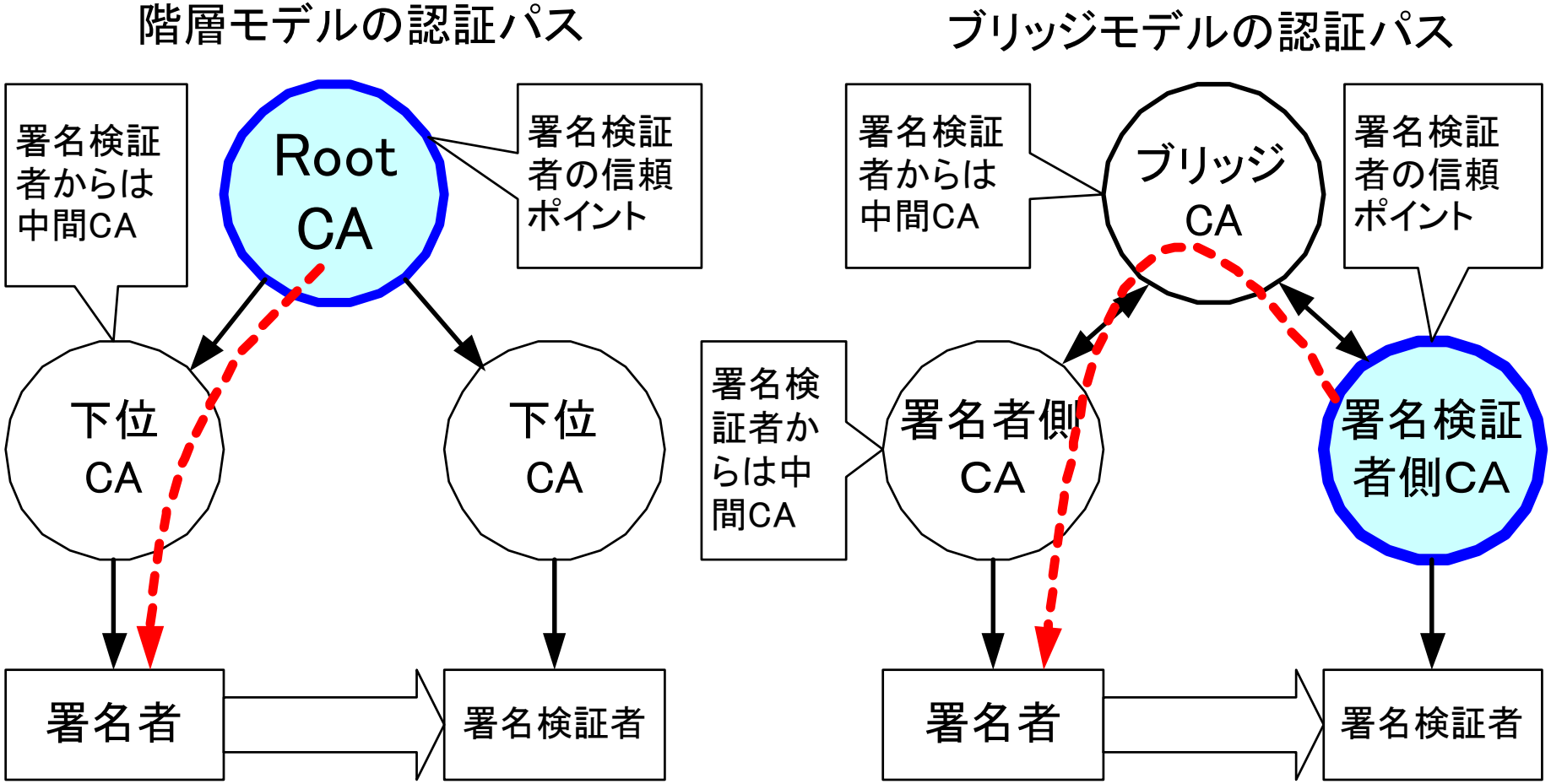
- 「デジタル証明書関連の脆弱性」
  - 「MS02-050：証明書確認の問題により、IDが偽装される(Q328145)」について　- 登録日：2002/09/05
  - 基本制約拡張は、最も基本的な制約拡張
- 制約拡張の意味
  - 制約拡張は、検証を制約する方向の働く
    - 証明書の検証は、署名のチェーンだけで検証するのではない
- それでは、他の制約拡張必要なのか、検証しているのか？
  - 広い認証ドメインにおいて、色々なポリシの証明書が発行される中、必要なポリシの検証を行うため必要になる。
  - GPKI/LGPKI/公的個人認証サービスの証明書プロファイルは、多くの制約拡張を使用している。

リライングパーティ/検証者
ブリッジモデル



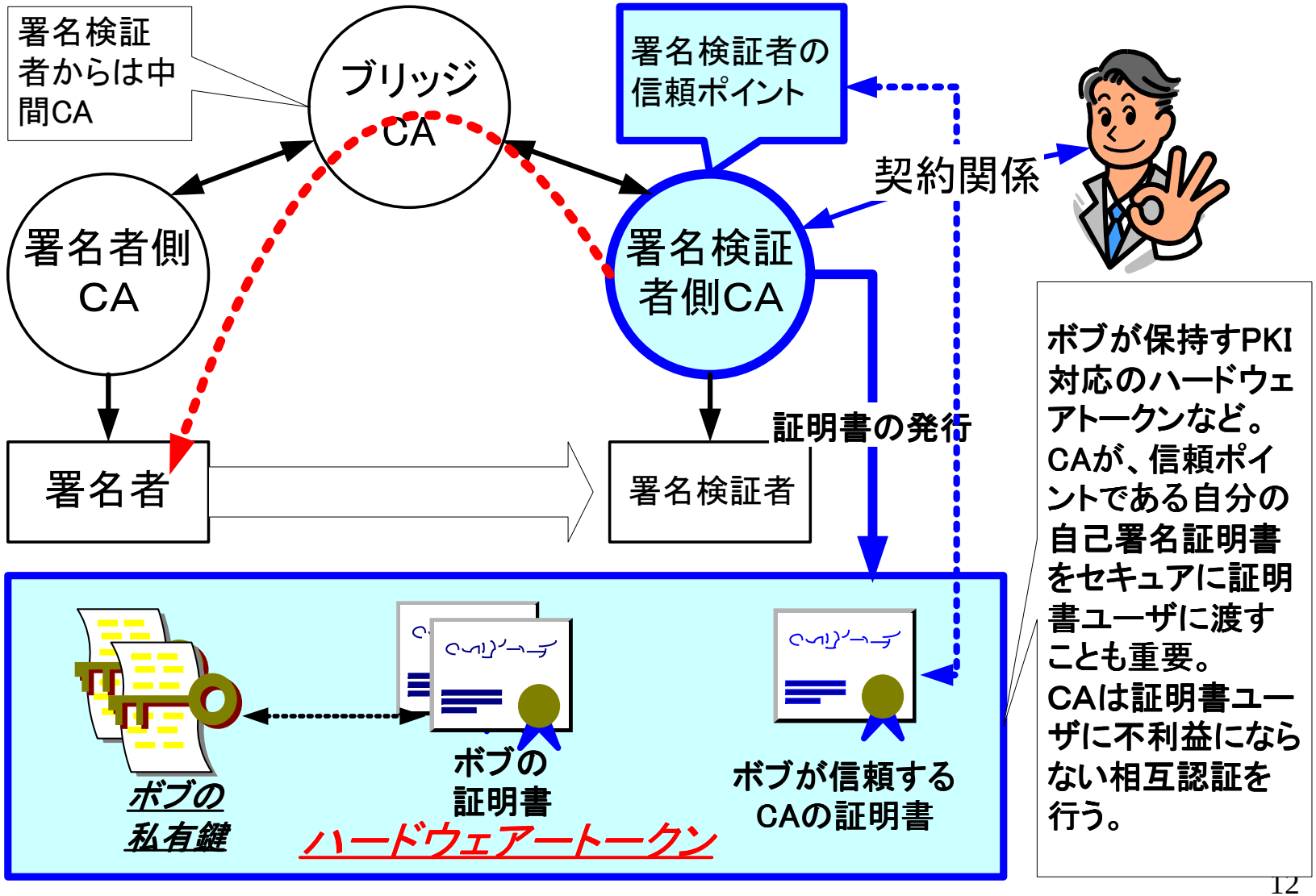
リライングパーティ/検証者
階層モデルとブリッジモデルの認証パス

セコムIS研究所
Intelligent Systems Laboratory

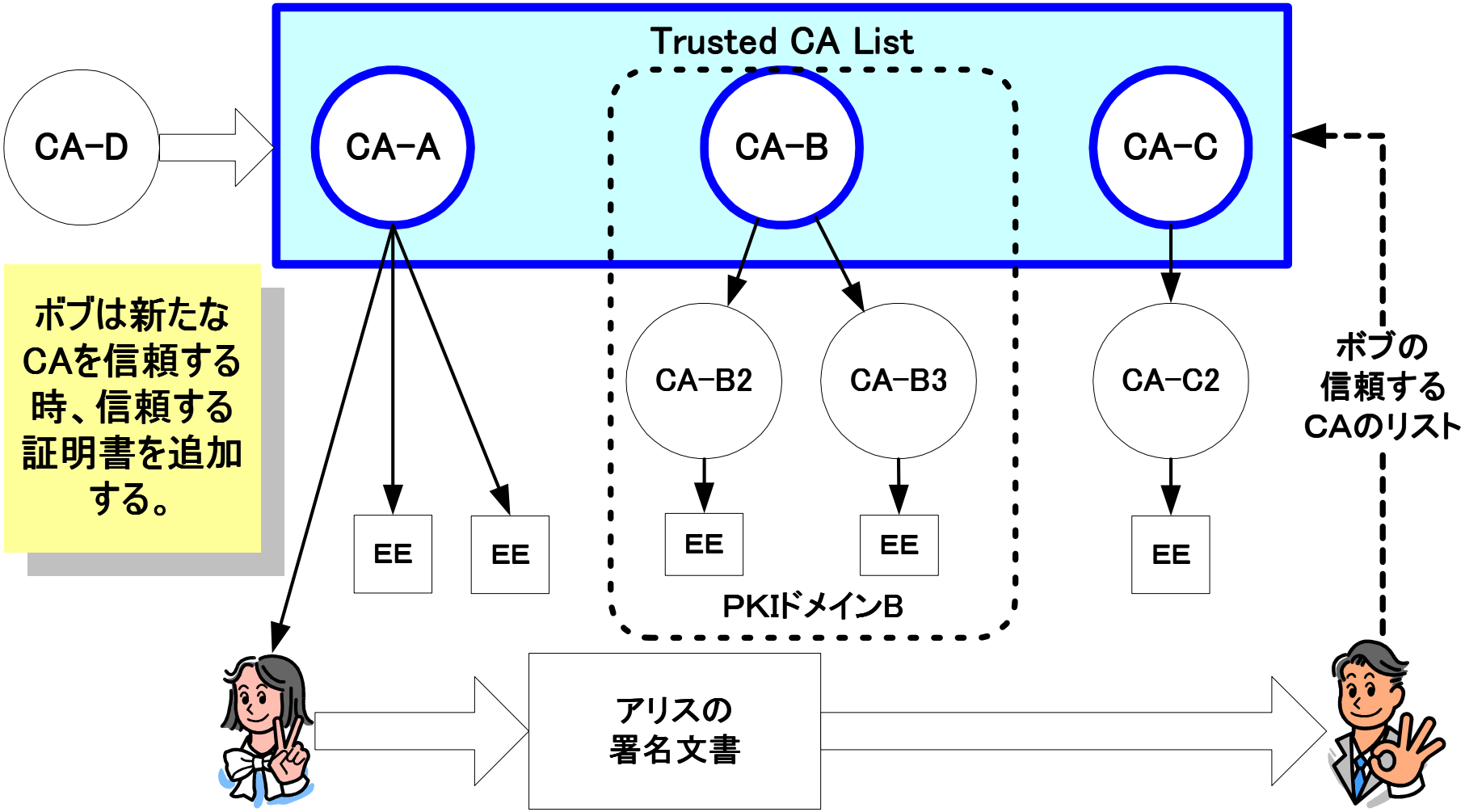


RFC3280などに記述されている認証パス検証は、信頼モデルに依存しない。しかし、ブリッジモデルでは、その性格から、RFC3280の仕様の多くの部分の実装が要求され、高度なPKI相互運用技術が要求される。

リライングパーティ/検証者
ブリッジモデルにおける信頼ポイントの扱い



リライングパーティ/検証者
証明書信頼リストによる方法（Webモデル）



リライングパーティ/検証者
証明書検証(サーバ)の動向

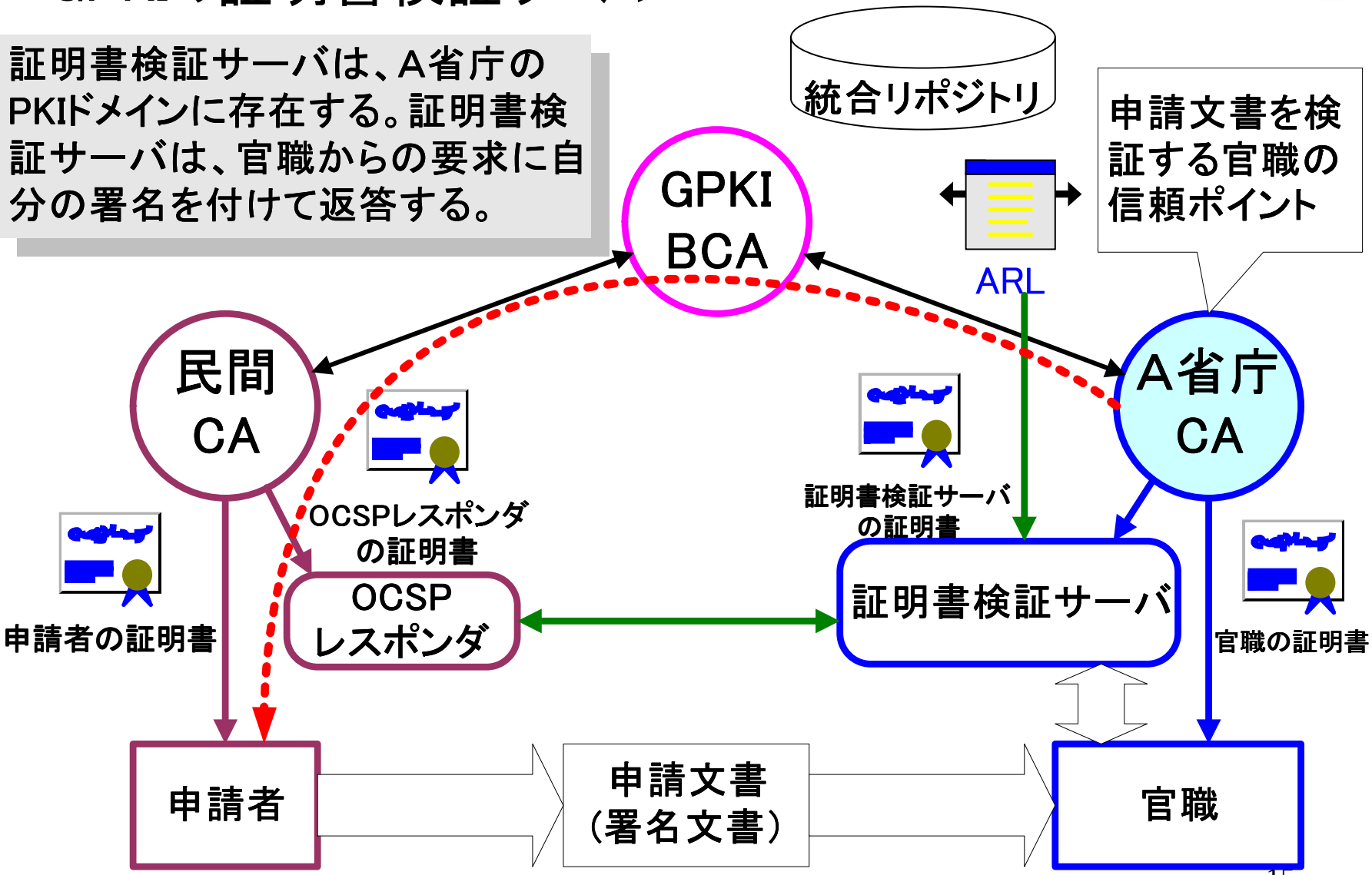
セコムIS研究所
Intelligent Systems Laboratory

- GPKI政府認証基盤の証明書検証サーバ
  - ブリッジモデル -> 証明書パス構築、パス検証が非常に難しい
  - 府省側に証明書検証サーバがある
  - 証明書検証サーバのプロトコルは独自プロトコル OCSP v1の独自拡張
- SCVP (Simple Certificate Validation Protocol)
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-13.txt
  - 証明書検証サーバとの標準プロトコル(になりそう)。
  - GPKIも独自プロトコルからSCVPへ変更すべき
- XKMS　　XML鍵管理サービス
  - X-KISS(XML Key Information Service Specification)
  - 鍵情報の有効性検証サービス
  - XML署名の<ds:KeyInfo>要素の処理を、クライアントアプリケーションから信頼できるサービス(Trust Service)に委託する
- サーバとの信頼 - SCVPの応答メッセージ、XML署名の検証…
  - これらは、信頼ポイントからの認証パスの検証が必要なことには変わりない。
  - 複雑さ(技術的な問題やポリシ上の問題)が隠蔽できるかもしれないが、複雑さがなくなるわけではない。誰かがやらなければならない…

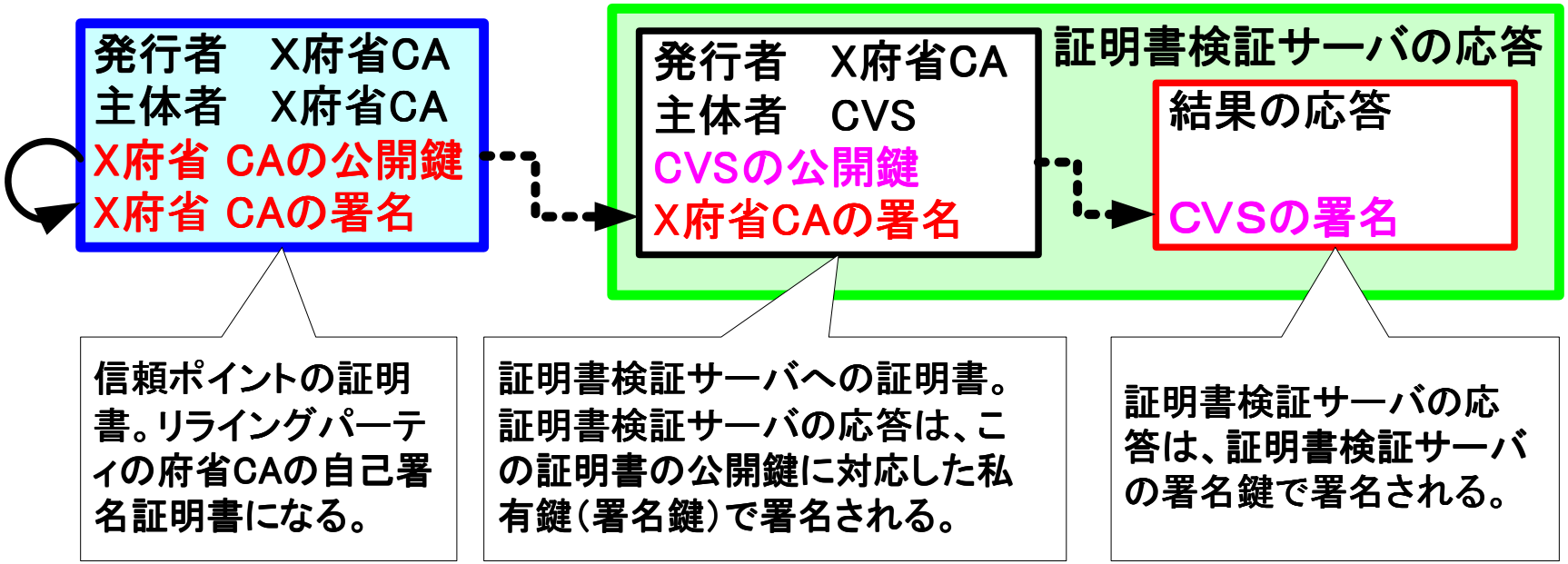
リライングパーティ/検証者
GPKIの証明書検証サーバ

セコム IS 研究所
Intelligent Systems Laboratory

証明書検証サーバは、A省庁のPKIドメインに存在する。証明書検証サーバは、官職からの要求に自分の署名を付けて返答する。



リライングパーティ/検証者
証明書検証サーバの応答



リライングパーティ/検証者
PKIとXML