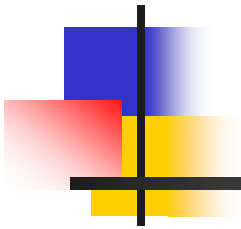


CSIの構築に向けた全国大学共同電子認証基盤(UPKI)に関する研究開発と調査

国立情報学研究所

1．グリッドミドルウェアを利用したCSI向け認証局の開発

- NAREGI　CAソフトウェアを，学内認証局として利用可能となるよう，ソフトウェアの改造を実施
- 今年度，オープンソースとして公開
- 主な改造点は次のとおり

(1) RA機能の権限分離

大学等で証明書を発行する場合，学部・学科等へ権限委譲が行われることが考えられる。そのため，登録局の権限をICカードにより委譲できる機能を追加し，RA管理者権限とRA・LRA運用者権限を分離した。（RAオペレータを認証するための証明書）

(2) チャレンジPIN対応

RA・LRAが許可した後，証明書の発行・更新・失効の申請を本人が可能とする機能を付加し，業務の効率化を実現した。

2. 学術機関向け証明書発行スキームと証明書ポリシーに関するガイドラインの設計開発

- 学術機関に特化した身元確認レベルの設定

身元確認レベル		レベル1（学術機関関連の Web サイトである）	レベル2（特定の学術機関の Web サイト）	レベル3（特定の学術機関の Web サイト）
ドメイン確認		×	△	○
申請者確認	実在性確認	×	△	○
	本人性確認	×	△	○
組織の存在確認		○	○	○

- パブリック証明書の身元確認レベル毎の必要性

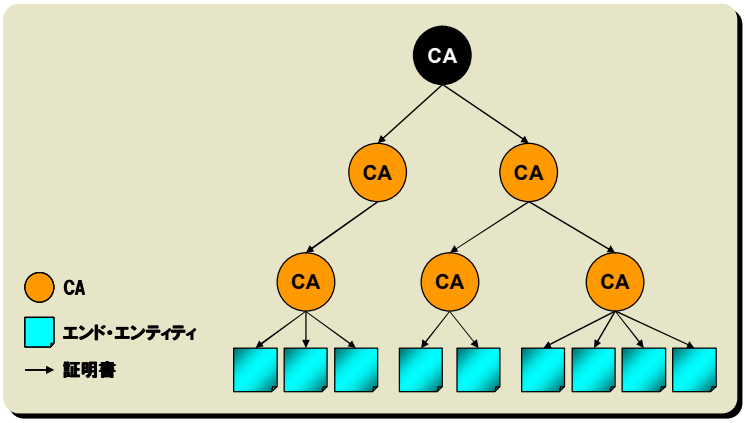
発行対象者	証明書	身元確認レベル		
		レベル1（実在証明なし）	レベル2（承認者の実在証明のみ）	レベル3（本人の実在証明あり）
サーバ	SSL サーバ証明書	○	○	○
自然人	S/MIME 用証明書	△	△	○
	電子署名用証明書	×	△	○
	認証用証明書	×	△	○

３．大学におけるセキュリティコンプライアンスの調査・分析

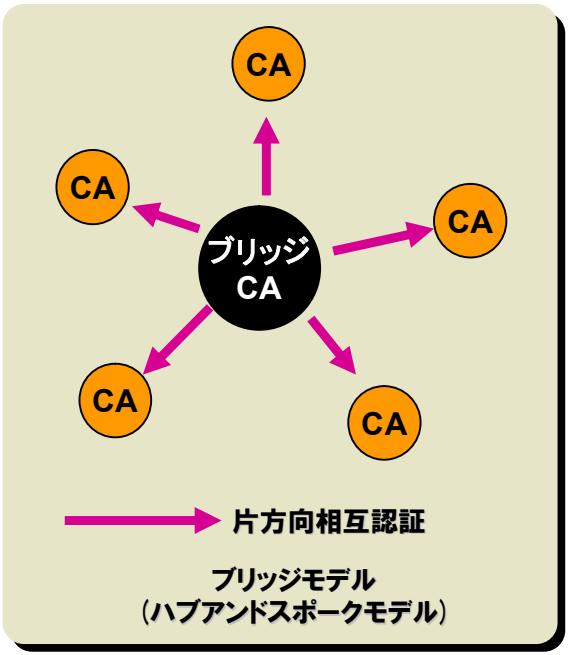
- 大学毎に，セキュリティポリシーは異なっている
- 異なるポリシー間で連携するためには，技術面のみならず，運用面での検討も必要
- 「政府機関の情報セキュリティのための統一基準」から主要な項目を抽出し，３大学について実態調査を実施
- 調査結果については，各大学にフィードバック済
- 今後，運用面から見た連携方式を検討していく
- 連携する大学間相互での，セキュリティポリシーの客観的評価方式も検討していく

4. プライベート認証局間連携方式の調査・分析

- 認証局間の連携方式は，複数のモデルが存在している。
  大学間連携に最適な方式を調査



階層（ルート）モデル



ブリッジモデル

4. プライベート認証局間連携方式の調査・分析（続き）

- 認証局間の信頼モデルの比較・分析を実施

	評価項目	単一	階層	Web	CTL	相互認証	メッシュ	ブリッジ
技術	PKI 対応状況	○	○	○	○	○	×	△
	動的な信頼関係の定義	×	×	×	×	○	○	○
	セキュリティ	○	○	×	○	○	○	○
	国際標準の不足	○	○	○	×	○	○	○
政策	大規模ドメイン展開時のリスク	N/A	×	×	×	×	×	○
運用	ドメインの保守	○	○	○	△	○	×	○
	証明書ポリシの独立性	○	×	×	○	○	○	○
	相互認証の手続き	N/A	○	N/A	○	○	×	○
	モデル管理組織の有無	○	○	×	○	○	○	×
価格	検証コスト	○	○	○	○	○	×	△
	監査コスト(1CA あたり)	○	○	○	○	○	△	○
性能	証明書有効性確認の応答時間	○	○	○	○	○	×	○
	ドメインの拡張又は縮小	N/A	○	○	○	○	×	○

5. S/MIME証明書パイロット発行実験

- パブリック証明書の発行実験という位置づけでS/MIMEのパイロット実験を実施
- WTCA認定ベンダーのホスティングサーバを利用し，パブリック証明書の申請・発行を実現
- S/MIMEそのものの普及も狙いとしている
- 今後は，パブリック証明書発行業務を，WTCA認定ベンダーに委託することにより，安価にパブリック証明書を発行するモデル作成を実施する

6. UPKIシンポジウムの開催

- 平成18年2月15日(水) に一ツ橋記念講堂でUPKIシンポジウムを開催
- 当日の出席者は400名以上であった
- 参加者からは，学内認証基盤を構築する際の情報が不足しているとの声が多かった
- 今後は，先行している大学等の事例紹介や，仕様書作成に有効な情報の公開，UPKI相互運用フレームワークの公開の実施を検討する