ネットワークの高度化に伴うセキュリティの強化としての認証基盤構築

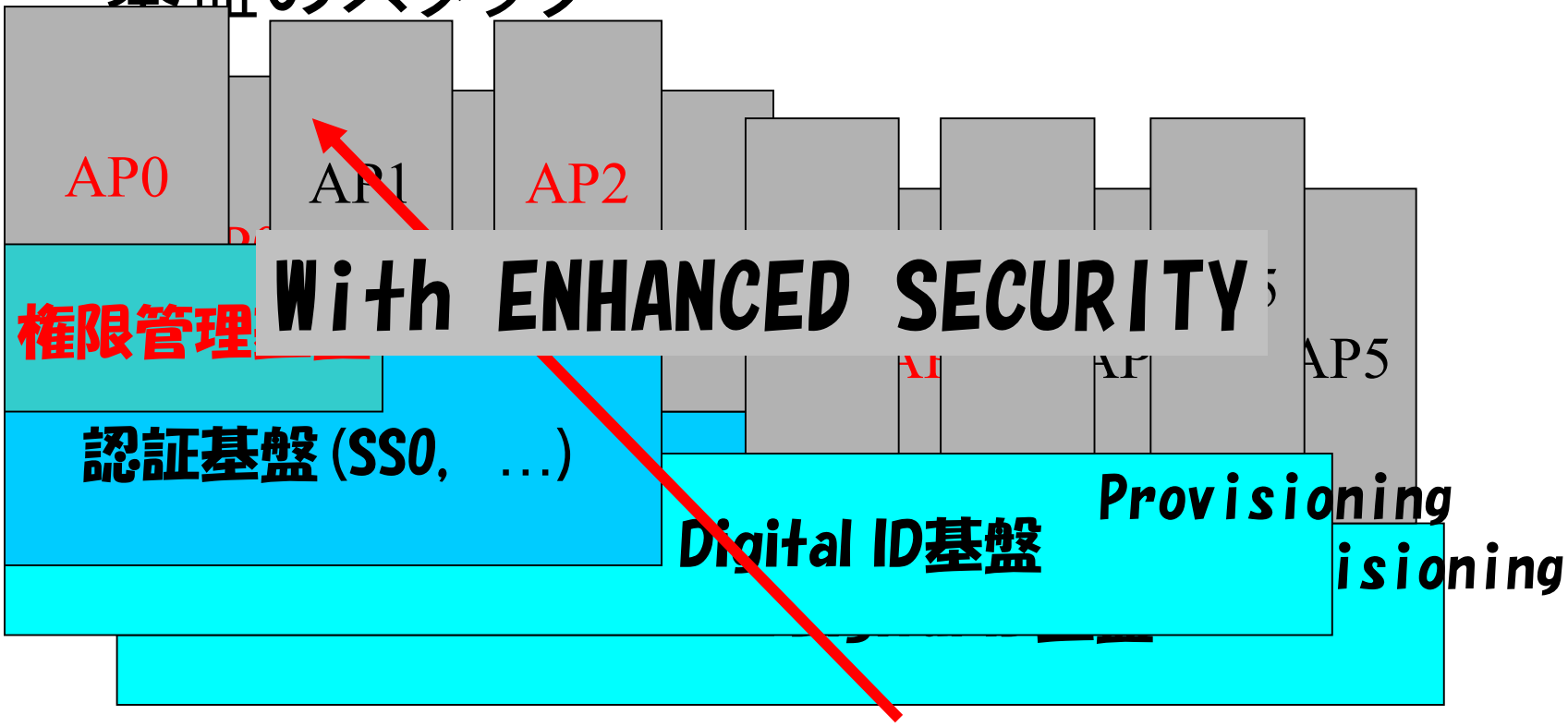
東京大学

佐藤周行

西村健

Goal of PROJECT

- 基盤のスタック



Goal of PROJECT (cont'd)

- 信頼するに足る認証基盤の構築
  - 信頼するに足るPKIの構築
- 「信頼するに足る」ことのコストの評価
  - 内部運用が可能か？
- 可用性をたかめるための、PKI＋αの研究開発
  - 権限とプライバシー
- 認証基盤上のアプリケーションの普及と開発

Procured Material

- 信頼するに足るPKIの構築
  - In-house CAの構築
- 権限とプライバシー
  - 属性管理機能付きCA
- アプリケーション
  - PKI対応SSL-VPN

「信頼するに足る」とは

- あまり深く考えると自家中毒になる。
- Sloppyなやりかたでは、構築した認証基盤は「ちょっとだけセキュリティが強化された」以上の意味は持たない。
  - アプリケーションを特定したものならOKだが、全学的な認証基盤を提供するときに問題になる。
- 格納メディアも重要

→

どうせなら、徹底したものを作る。

信頼のコスト

- 「どこまで内製、どこから外注」の線引きは重要な検討対象
  - （注）アプリケーションを限定すれば、「えいや」で決めても大事には至らない
- 検討項目（調達＆コンサルティング）
  - IA自身の信頼性
  - 運用体制の構築にかかるコスト
    - 物理的セキュリティ
    - 組織の構築

信頼するに足るPKIの構築(1/3)

- IA/RAの物理的要件
  - サーバ室への入退室管理
  - ラック鍵の管理
  - HSM(Hardware Security Module)利用
    私有鍵漏洩を防ぐ
  - 複数人による作業の強制
    権限者の不正を防ぐ
  - 等々

信頼するに足るPKIの構築(2/3)

- 人的要件
  - IA管理要員　…　14名
  - その他申請の確認・受理のために各部局2名ずつ
    - 管理単位は部局の事情によって変化する
    - 詳細は実地試験によって詰めなければならない

信頼するに足るPKIの構築(3/3)

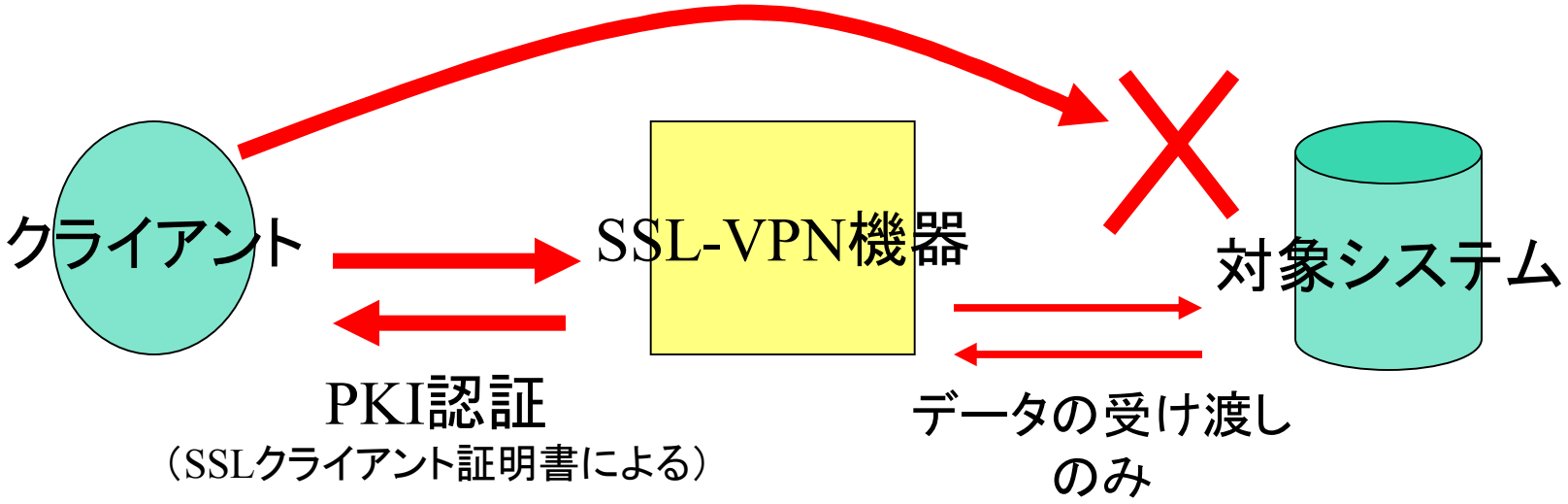
- 私有鍵は職員証／学生証に格納
  - 既存物利用による携帯性への配慮
  - 学生の意識を向上する必要性あり？

PKI対応SSL-VPNの導入

- F5 NetworksのFirePassを導入し情報基盤センター内で運用している
- PKIを認証に用いる直接的な応用例
- ID管理と提供機能の完全な分離
  - IDは事務で発行
  - 失効はCRLで管理、SSL-VPN側で自動的に取り込む

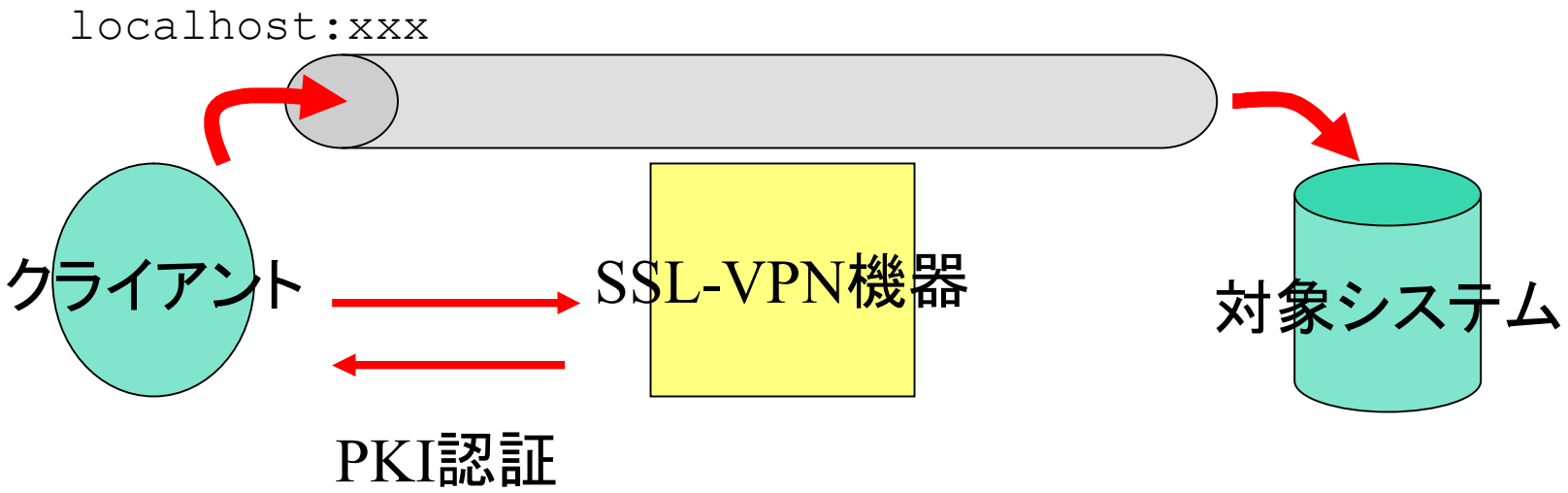
PKI対応SSL-VPNの問題点

- PKI対応のためにSSLクライアント証明書が使用されるため、対象システムが本来持っているSSL機能が利用できない。



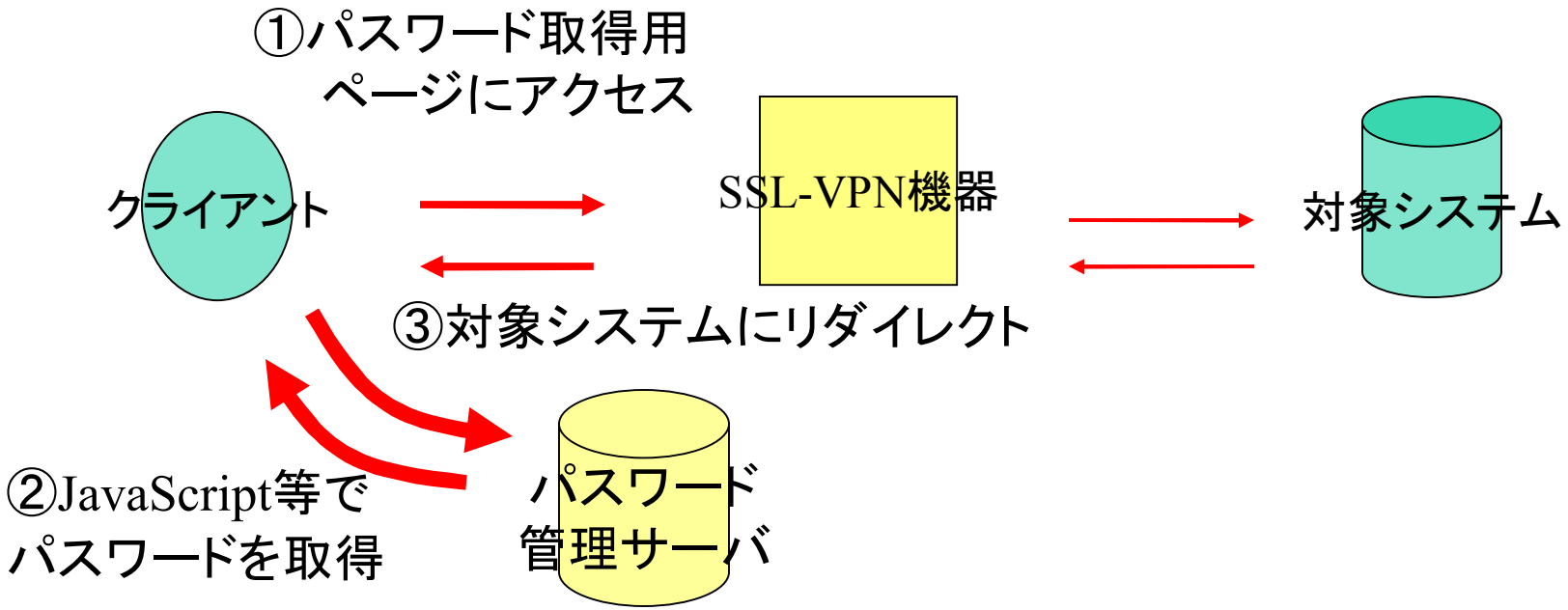
PKI対応SSL-VPNの発展(1)

- 前記の問題点の解消
  → トンネリング（ポート転送）の利用
    → FirePassのオプション機能



PKI対応SSL-VPNの発展(2)

- 簡易なSSO(Single Sign-On)の実現
  - パスワード管理サーバを介して



まとめ

- 「信頼するに足る」PKIを構築した
  - 実地で更に検討を行なう
- その応用としてPKI対応SSL-VPNを導入した
  - 簡易SSO等への発展の可能性