東京大学の学術認証基盤運用に関する研究開発

情報基盤センター
佐藤周行

ID管理について（まとめ）

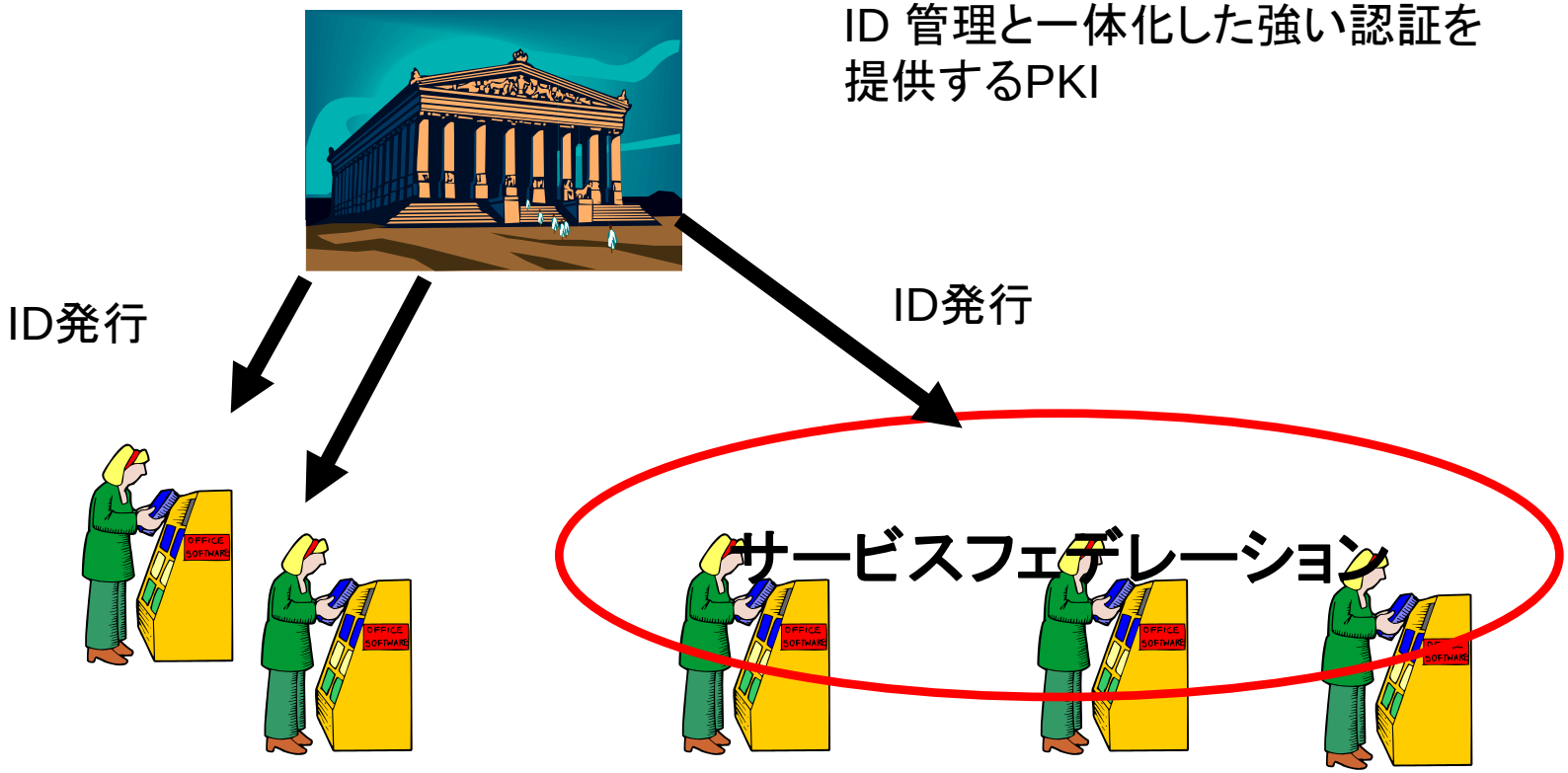
- PKIについての見解
  - 対費用効果で厳しい判断も
  - 証明書認証が必要な場面は学内にどれくらいあるのか？
- ID Federationへの参加検討
  - 全学的な規模での参加は少し時間がかかるかもしれない
  - 努力中

ID管理の適正化

- 中央管理すべきID・ロールの管理をどうするかは今後の課題
  - 部署ごとの分散管理を束ねる東大モデルは適正だったのか（今までは効果的であっても、今後とも効果が期待できるか）？
- アプリケーションごとに管理できるIDをどう適正に管理するか
  - 特にS/MIME

- セルフサービス型のID発行・保守システムの提案と検討
  - S/MIMEについては、PKI本体から切り離し、独自に管理できるサーバの運用準備（現在停止中）
  - セルフサービスのqualityを担保するための強い認証の準備（現在停止中）
    - 大学では、特殊なケース（バイオ、原子力その他）を除いて認証にそれほどの強さを求めないことは雰囲気として強く感じた。
    - IDを発行するところだけは守る必要がある。ここまで「適当でよい」とされるとちょっと困るだろう

- 将来図



サーバ証明書プロジェクト（まとめ）

- 運用上の経験の蓄積
  - 累計300枚以上の処理
  - 分散管理によるコストの最適化
  - 監査の経験（3回目）
- サーバ証明書の「書き換え」への対応
  - 短期間での対応ができた
  - ユーザを急かすことはほとんどなかった
- EV証明書の導入
  - テストケースとして導入
  - 今までのスキームが有効に機能

運用上の経験の蓄積

- 運用上の経験の蓄積
  - NIIのCP/CPSに対する付属文書として東大版CP/CPSを公開。それに基づいてRAを運用
  - 学内ネット基盤の上に付加サービスとして運用
  - 現在、8部局と協同して（分散管理で）RAでの審査を行なっている
  - サーバ証明書についての理解が深まっている
  - 年1度の監査を分散管理先に実施。3回の経験を積む

EV証明書

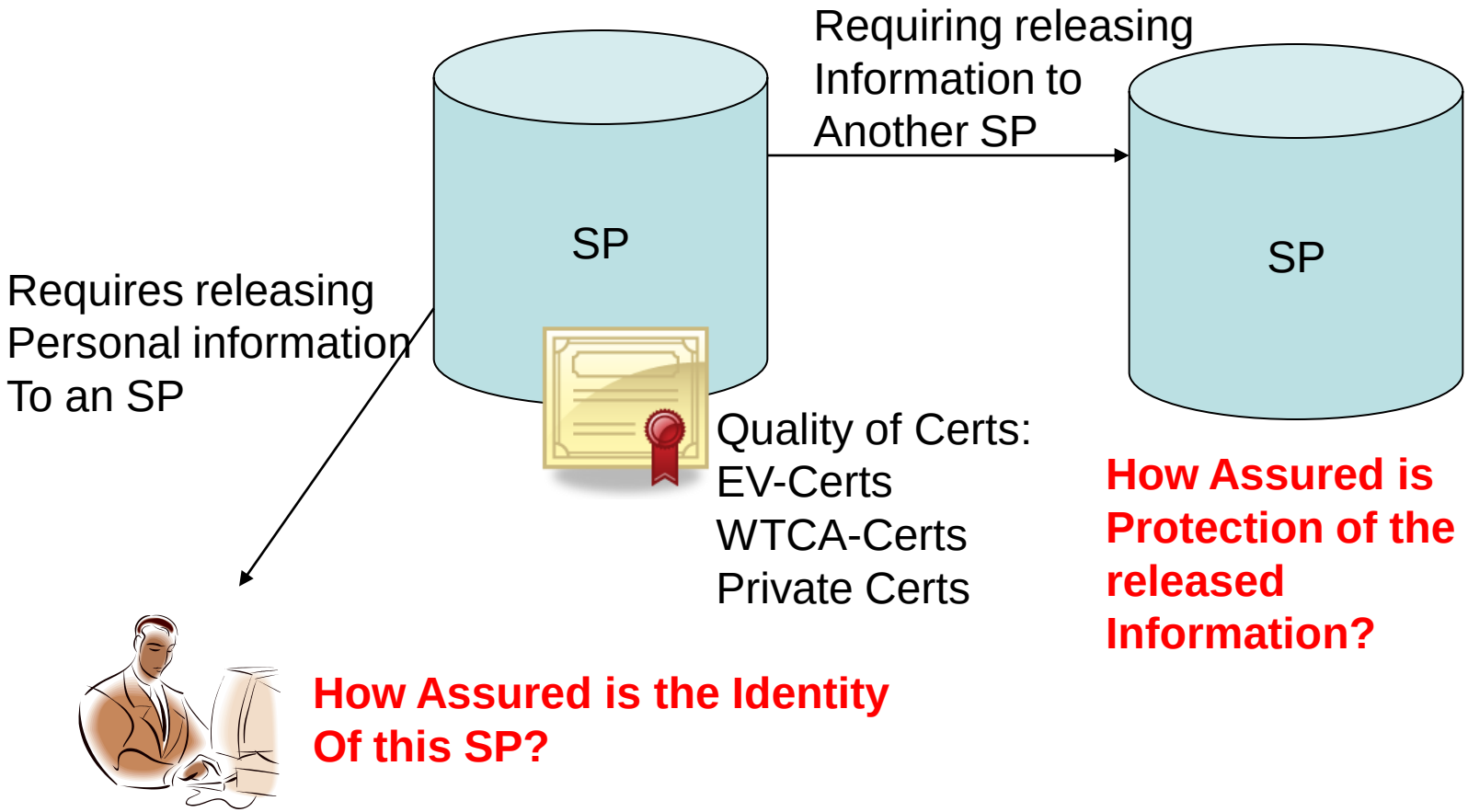
- Entrust社のEV証明書をキャンペーン期間中に購入
  - グレードの高い証明書を扱うことによるメリットは？
  - 今まで作ってきたRA機能が有効に働くことの（あたらな）テスト。ただし、EV証明書では、東大は審査はできない。申請するときの「安心」感を求める
  - 9末までの期限で20枚（2年もの）の権利

技術的なことども（まとめ）

- LoAとサービスレベル
  - PKIとサーバ証明書、フェデレーションへの参加を経て、各々がサービスに対して何らかの格付けを持つことが今後必要になるという結論になった。
- 2008DebianでのOpenSSLのバグへの対応と解析
  - 2009年度に対外発表（by 西村）

Scenario of Grades

- LoA for SPs



2008Debian OpenSSL BUGS

- 2008年５月に発覚したDebian系でのOpenSSLの誤った改変（鍵生成においてエントロピーを極端に減じる改変だった）
- 当初は管理対象にある証明書のチェック等に追われた。
- 一段落したところで解析が始まった
  - どのくらいCriticalなバグ入れだったのか？

- 情報基盤センターのスーパーコンピュータを利用して、鍵生成のほとんど全部のリプレイを行なった。
  - 2ヶ月程度あれば十分な計算量だった。ただし、やり直しを含めて最終的には2009年はじめまで断続的に計算
  - 結論として「深刻な問題ではなかった」
  - 西村がNIIに移ってからは、NIIの証明書も対象にして解析、発表。
  - 証明書界の超新星爆発
    - 多くの知見が手に入った。
    - 証明書のライフサイクル管理の実態が一部明らかに…

全体としてのまとめ

- ID管理について
  - ID管理の適正化の必要性
- サーバ証明書プロジェクト
  - 運用上の経験の蓄積
  - EV証明書
- 技術的なことども
  - サーバのグレードの重要さ
  - Debian系のOpenSSLのバグの解析