Simple SSO on SSL-VPN

西村　健
PKIプロジェクト
情報基盤センター
東京大学

東京大学情報基盤センター PKIプロジェクトについて

- 目標：東京大学にPKIを普及させる
  - PKIがID管理の中核となることを目指す
  - 約40,000人の大学構成員
  - **普及のためにはPKIアプリケーションの充実も必要**
    - **全学レベルから研究室レベルまで多岐にわたるサーバ**

サイボウズ問題　ー
既存のサーバとの連携問題

- 大学には既に様々なサービスが存在する
  - 全学レベル、学部レベル、研究室レベル…
- IDおよびパスワードのみで認証を行なっているレガシーWebアプリケーションとの連携が重要
  - PKI対応が難しい

この問題を「サイボウズ問題」と呼ぶ

- 大学で人気の高いグループウェアの名を取って

サイボウズ問題　－　合理的なコスト

- 「サイボウズ問題」はコンテンツサーバ側に手を加えれば解決することは明らか
  - ただし様々な要因で困難なことも多い
    - ライセンスの問題、ソフトの複雑さの問題、…
    - 特に小規模な組織においてや多数のサーバを扱う場合

合理的なコストで解決するには、コンテンツサーバに手を加えず実現しなければならない

あらためて問題設定

- サイボウズ問題の解決
  - PKI認証の導入コスト
- Single Sign-Onの実現
  - 複数のID、複数のパスワード
- 高度なセキュリティ
  - PKIによる厳密な認証、他
- ID/パスワードをformで入力し、cookieによりセッションを管理するコンテンツを対象とする
  - 実際的な要求として

従来の方式の検討

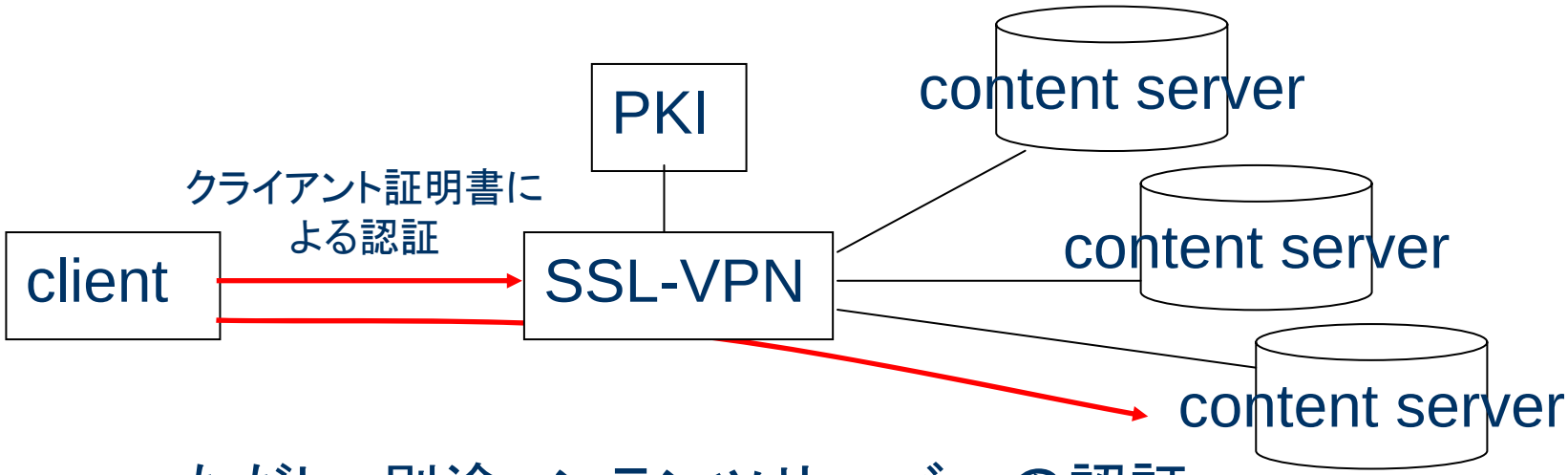
- 大きく分けて2種類
  - SAMLベースSSO
    - コンテンツサーバの認証部分の改変が不可欠であり、サイボウズ問題によりコスト増
  - パスワードサーバ
    - 各人のID/パスワードを保管するサーバを導入し、プロキシとして代理で送信する
    - コンテンツサーバとの通信が常にプロキシを介するため効率が低下
    - パスワードサーバ自身のセキュリティ問題

いかなる者からもパスワードを保護する

- 盗聴者に対して通信の暗号化
- クライアントの防御としてキーロガー対策
- パスワードサーバのクラッキング対策、パスワードサーバ管理者の不正防止
  - 機密性の高いものが集中しているため重要
  - 対策として、ある程度の処理をクライアント側で行なう必要

SSL-VPNとは

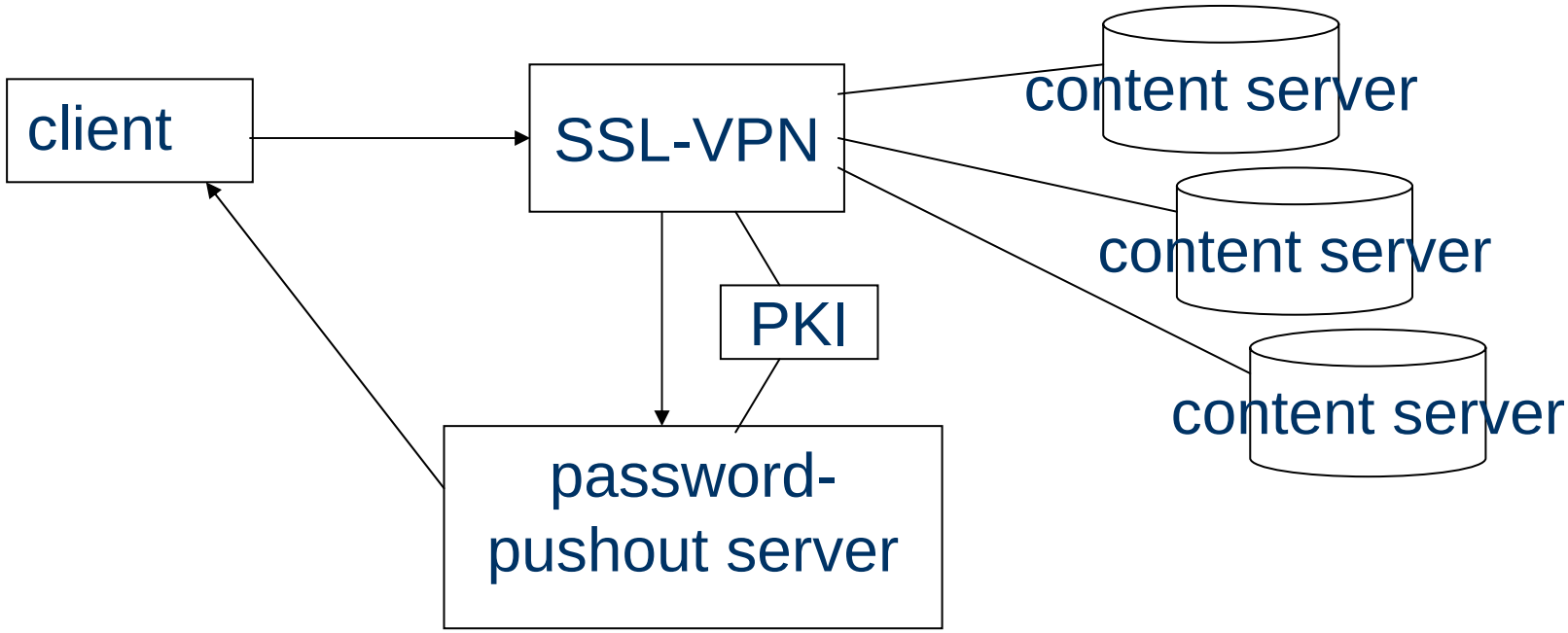
- SSL-VPNは認証パスを統一する



ただし、別途コンテンツサーバへの認証が必要

提案するシステムの構成

- SSL-VPNアプライアンス（リバースプロキシ型）にpassword-pushout serverを追加する



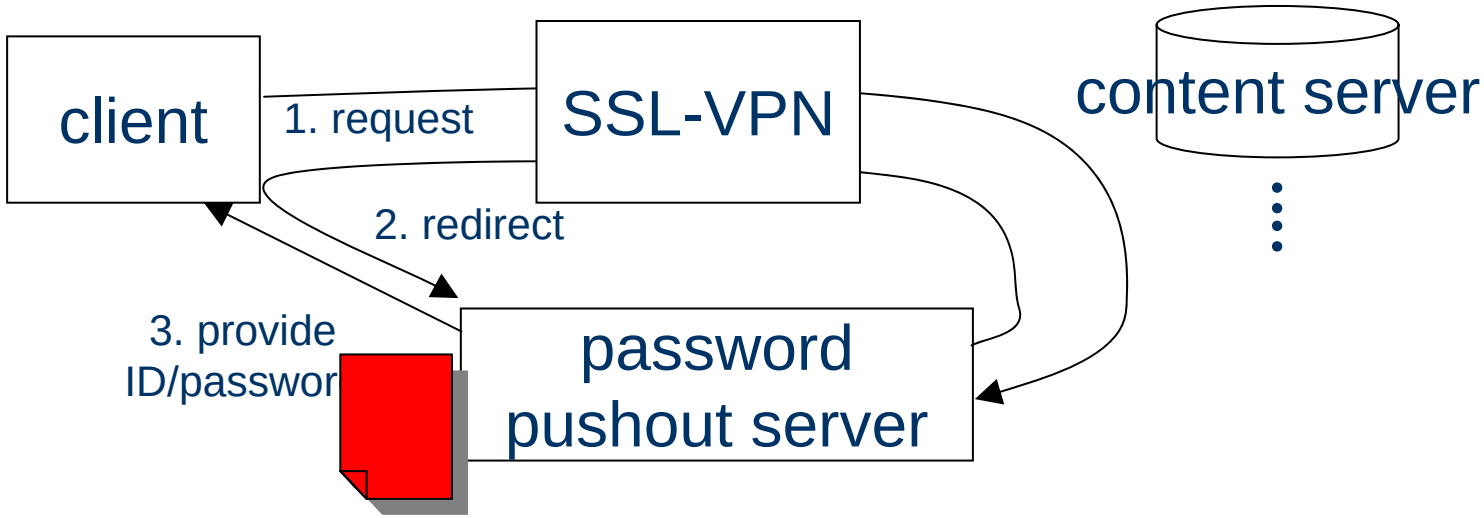
Password-pushout server

各利用者のIDおよびパスワードを保管する

- クライアント証明書による認証
  - SSL-VPNを介さずに直接アクセスする
- 保管されるパスワードは利用者の公開鍵により暗号化される

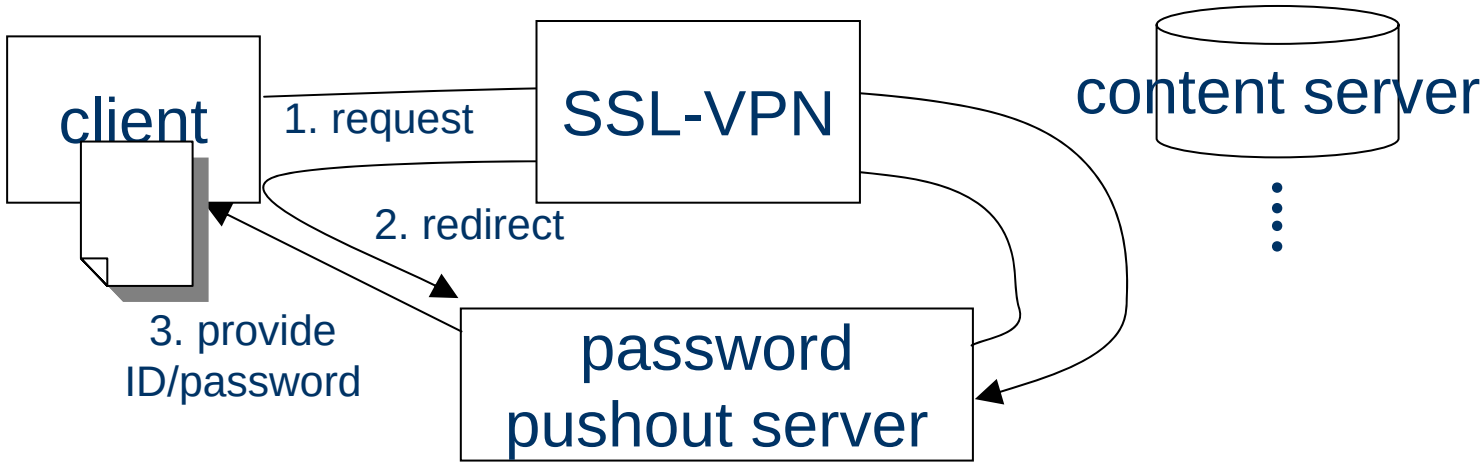
認証の流れ

1. コンテンツサーバへの接続要求
2. Password-pushout serverへリダイレクト （ダミーページ経由）
3. PKI認証、ID/暗号化パスワードの提供 （ログイン用formの形で）
4. パスワードを復号し、認証情報を送信



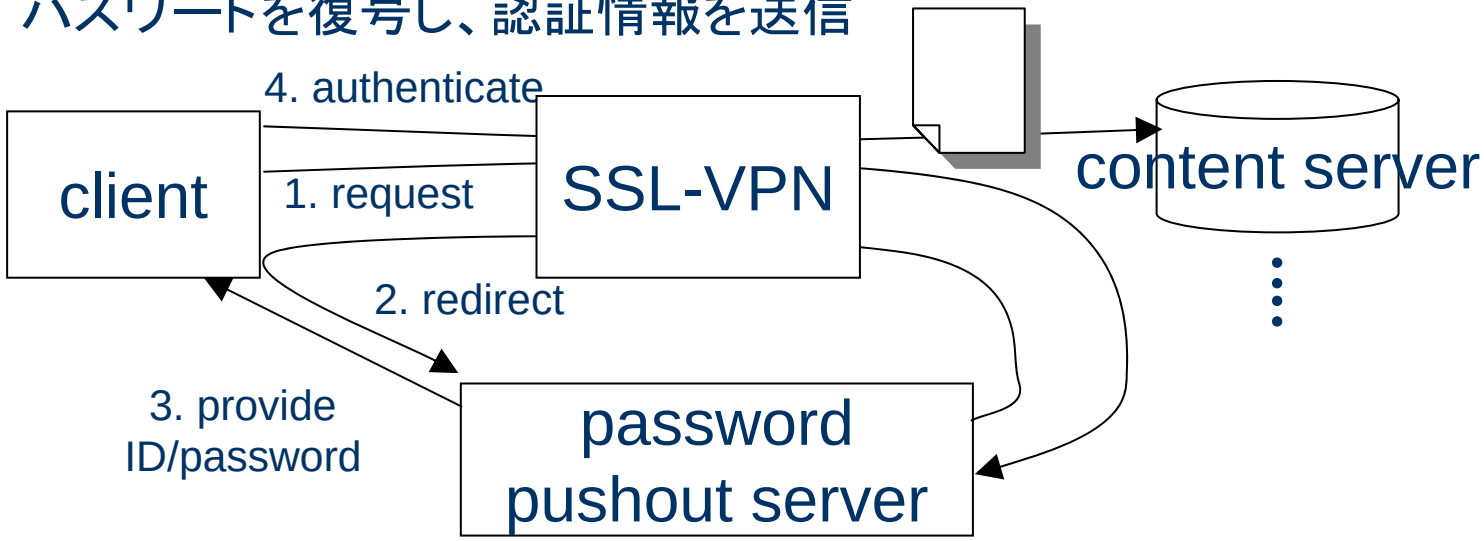
認証の流れ

1. コンテンツサーバへの接続要求
2. Password-pushout serverへリダイレクト （ダミーページ経由）
3. PKI認証、ID/暗号化パスワードの提供 （ログイン用formの形で）
4. パスワードを復号し、認証情報を送信



認証の流れ

1. コンテンツサーバへの接続要求
2. Password-pushout serverへリダイレクト （ダミーページ経由）
3. PKI認証、ID/暗号化パスワードの提供 （ログイン用formの形で）
4. パスワードを復号し、認証情報を送信



password-pushout serverに保管される情報

利用者 Subject DN	Server ID	サーバ上の User ID	暗号化されたパスワード
A DN	Server 1	User ID A	XXXXX…
B DN	Server 1	User ID B	YYYYY…
…	…	…	…

パスワードは利用者の公開鍵により暗号化される

パスワード保護の実現

- 通信経路上での盗聴はSSL-VPNでブロック
- パスワードを入力しないためキーロガーによる窃盗も起こりえない
- **パスワードが暗号化されているためpassword-pushout server管理者であっても不正にパスワードを取得することはできない！**

「簡易SSO」と呼ばれる仕組み

- パスワード等ユーザからの介入が一回のみで以降の認証が行なわれる、という意味で「SSO」
  - サーバ間で認証を行なっているわけではないので「簡易」
- クライアント認証のPIN確認は最初の一回だけ
  - 厳密にはブラウザの実装依存

プロトタイプの実装環境

使用機器:

- SSL-VPN:FirePass 1010
- password pushout server:Mac mini 1.83GHz
- client:Windowsマシン Firefox 2

暗号化／復号処理の実装

- Firefoxでは証明書による暗号化／復号を行なうJavaScriptインターフェースが用意されている
  - 署名されたスクリプト or 拡張機能（アドオン）の形で
- CMS形式で保存されている

関連研究

- サーバ側の解
  - SAMLベースのSSO
    - コンテンツサーバ改変に伴うコスト増
    - ID管理に主眼
- クライアント側の解
  - ブラウザのサポート
    - いくつかのブラウザは入力されたパスワードを記憶しておくことが可能
  - TPMを利用したパスワードの保管
  - クライアント依存、全ての管理等の負担が利用者へ

まとめと今後の課題

- 合理的なコストでの簡易SSOの実現
  - Password-pushout serverを中継する
  - コンテンツサーバに一切の変更を加えない
- 実利用で必要になる追加コストの洗い出しと既存の手法との性能面での比較を行ないたい
- 特に初期登録時の方式検討