

弊社のWeb認証ソフト技術

2009年度

(株)システムサイエンス研究所

1. 経験したプロジェクト概要

官公庁や大企業における例えば電子入札や公共サービス、ビデオオンデマンドサービスなどに使うWeb認証のソフト(認証サーバ側、クライアント側、認証局CA局側)を担当しました。1999年から現在まで常に5～6人のメンバが従事しております。

経験環境

OS: Linux、Unix、Windows、

言語: Java、C等、

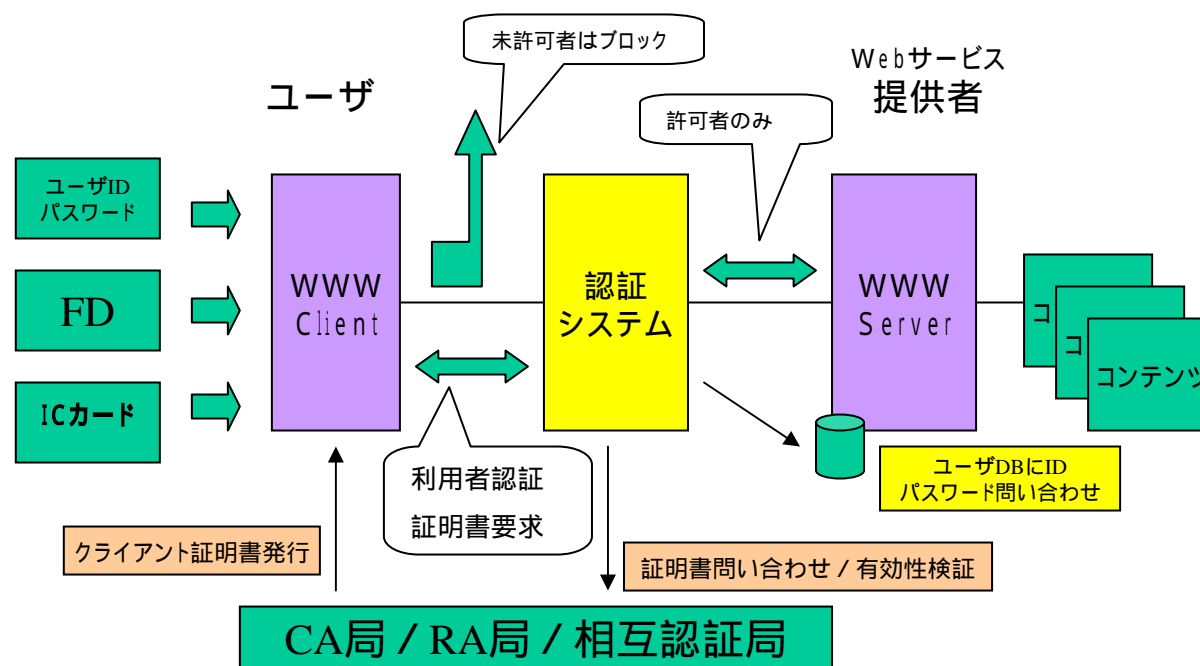
データベース: Oracle、SQL Server、Postgres等

Webサーバ: IIS、Apache、

関連技術: Jrun、Tomcat、認証のためのICカード制御

2. 全体像

- 1) ユーザがクライアント側からWebサーバにアクセスするときの認証を行う。
 - ・ユーザのID / パスワード管理
 - ・アクセス制御管理(各コンテンツ毎のアクセス条件等)、課金処理
 - ・様々な種類の認証処理対応(ICカード、FD、ID / パスワード入力等)
- 2) シングルサインオン(複数Web認証システム間の連携)サポート(独自形式、LibertyAlliance仕様)
- 3) 文書(XML, バイナリ)へのPKI署名生成と署名検証(証明書有効性検証)部分をサービスAPに提供。
- 4) CA局システムでの登録等の受付処理部分のシステム。



ポイント

- ・XML署名生成ライブラリ
- ・XML署名検証ライブラリ
- ・証明書有効性検証ライブラリ
LDAP/OCSP(GPKI準拠)
- ・属性証明書付加
- ・属性証明書検証
- ・アクセス制限機能
属性 (Role/Group)
コンテンツグループ
ユーザーグループ
日時/時間帯/曜日/休日
課金カウント
- ・RealVideoServerとの
連動認証プロキシ
- ・Javaによる非プラットフォーム依存
Unix, Linux, Windows

3. 関連技術

- 1) Java servlet / applet マルチプラットフォーム
- 2) PKI (Public Key Infrastructure)、GPKI (政府認証基盤)
 TripleDES、RSA (暗号)
 PKIの規格: PKCS#1 (RSAによる暗号化・デジタル署名の方法)
 PKCS#12 (秘密鍵・証明書の転送・保存構文定義)
 PKCS#11 (カード等暗号デバイス向けAPI定義)
- 3) XML署名・検証 (XML文書での署名及びその検証)
- 4) 複数認証局パス構築、ブリッジ認証局 (民・官の相互認証)
- 5) シングルサインオン (複数Webサイト認証の一括管理)
 Liberty Alliance (シングルサインオンの仕様の1つ)
- 6) CA局 (認証局)・RA局 (登録局)
- 7) SSL (Secure Socket Layer: 一般的なブラウザ等における暗号化及び認証)
 LDAP (ネットワークでのディレクトリサービスへのアクセスプロトコル)
 OCSP (インターネットPKIオンライン証明書状態 (有効性等) プロトコル)
 RTP (Real Time Transport Protocol) / RTSP (Real Time Streaming Protocol)
- 8) OSS (Open Source Software) 導入 (Linux, Apache, PostgreSQL)
 Jakartaプロジェクトのソフトの利用: Apache, Tomcat, Struts等
- 9) DBシステム構築
 Unix (Solaris) Oracle
 Windows 2000 Server SQL 2000 Server
 Linux Postgres

4. 開発規模

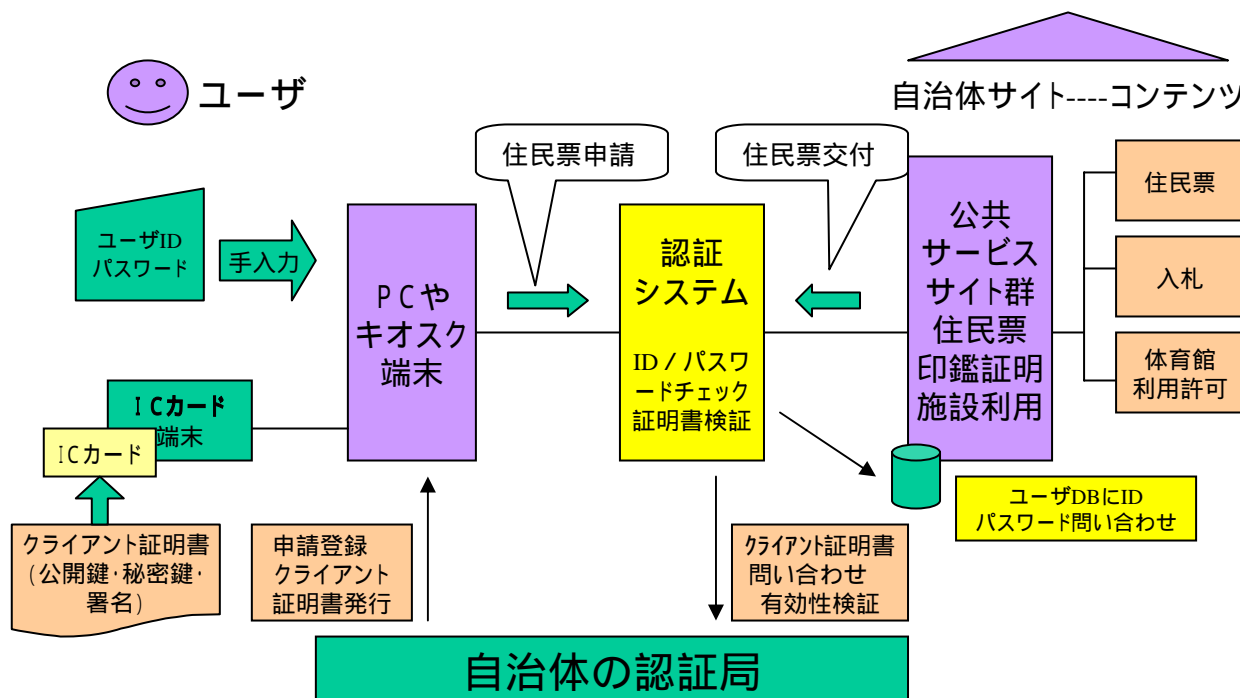
開発ソフト	規模
Web認証ソフト XML文書署名検証ライブラリ	35 Kline 11 Kline
公開鍵証明書登録局システム 運用構築システム	17 Kline 10 Kline

5. 実際の認証ソフトの応用先

- 1) 公共機関等での電子的な申請における認証
- 2) ビデオオンデマンドのサイトでの認証
- 3) 公共等のサービスで
ICカードへインターネットを使ってAPソフトをダウンロードする時の認証
- 4) 認証に必要な電子的証明書の登録や発行
- 5) 住基端末システムの開発(ノウハウ応用)

6. 例: 電子申請

ユーザは身元を示すクライアント証明書が入ったICカードを認証局に申請・取得する。
 ICカードをPCやキオスク端末に差し込んで住民票等を電子申請する。
 その際はID・パスワードを要求される。
 さらにクライアント証明書の有効性が検証される。
 その結果住民票を取得する。



7. 例:ビデオオンデマンド

ユーザはクライアント証明書を認証局に申請・取得しPCに保持する。
 見たいビデオを要求する。
 その際はID・パスワードを要求される。
 さらにクライアント証明書の有効性が検証される。
 ID / パスワード / 証明書の内容から課金・コンテンツ閲覧制限(時間・曜日、性別、年齢、履歴)。

