

Webアプリケーションにおける、低コスト機器を用いたセキュアなログイン方法の提案

株式会社東芝

橋本 賢

satoshi7.hashimoto@toshiba.co.jp

開発における問題点

サーバのパスワード保存＝流出リスク
 →指紋認証器等を用いて、クライアント側で本人確認する手法が増加

- ・Windows Hello (Windows10)
- ・Sign in with Apple (iOS)

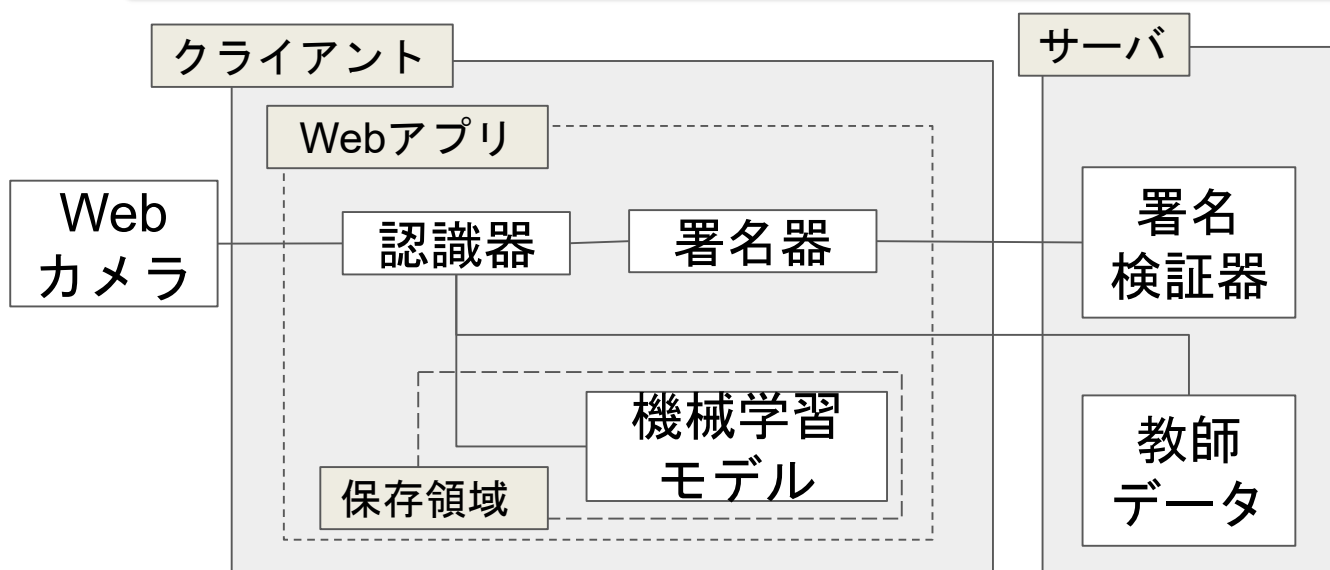
より効率的+低コストな開発には、OSに依存しないクロスプラットフォーム+低価格な機器が必要

提案手法の適用による解決

- ・クロスプラットフォーム環境
 →Webアプリケーション
- ・低価格な本人確認機器
 →Webカメラ(を用いた顔認証)

OS依存のアプリケーションと比較して制約が強いWebアプリケーションでも、検証により実現可能性が高い事を確認した。

システム構成



提案手法の効果

- ・Webアプリ上の領域に学習モデルを保存
 - ・保存するにはフォーマット、容量に強い制約
 - ・軽量な学習モデル(MobileNet)の採用
 - ・情報量を抑えた教師データの採用
 - 上記2点によりこれをクリア
 - リアルタイム性を損なう事なく本人確認を実現
- ・オープンソースの活用
 - ・顔認識器(機械学習モジュール)
 - ・機械学習モデル
 - ・署名の作成/検証(暗号化ライブラリ)
 - ・Webサーバ

上記技術は全てオープンソースがベース
 →低コストでシステムの試作を実現

課題

- ・採用学習モデルの精度
 - 判定が荒く、より多人数を対象とした際は要検証
- ・WebアプリのログインAPI(WebAuthn)に準拠する通信
 - 自作の認証器では専用プロトコル(CTAP)が要実装
- ・なりすましログイン
 - スマホの画面で、他人の顔からログインできてしまう



→対象者を限定したユースケースでの運用や、ジェスチャーなど別の顔の特徴を利用して本人確認