セキュリティ総論 D レポート No.1

セキュアな受講者認証システムの提案

慶應義塾大学 61908697 佐々木良輔

要件定義

受講者の識別システムの検討にあたり機能要求 (FR) として以下を定義した.

FR 1. 受講者そのものを識別できる (別のユーザーや bot による操作を判定できる)
FR 2. IC カードリーダーなどの追加の機器を必要としない
FR 3. セキュリティ確保のためユーザーのカメラ画像をサーバーに送信しない
FR 4. クライアントサイドのアプリケーションはクロスプラットフォームである

ログイン認証や学生証による認証では他のユーザーにパスワードを教えたり学生証を渡すことによりなりすましが行われる可能性がある. したがってこういったなりすましが困難なシステムとすべく FR 1. を設定した. また大学の授業の受講人数は膨大であり, また各学生の金銭事情もバラバラであるため新たなデバイスを購入せずにシステムを利用できる必要があることから FR 2. を設定した. また 2. に関連してユーザーが既存のデバイスを利用し続けられる必要性があること, また利便性の面から FR 4. を定義した. また今回のシステムの目的はカメラを用いないことではなく, ユーザーのプライバシーを保護することである. したがってカメラを用いたとしてもそのデータがローカルでのみ利用され外部に送信されることが無いのであればセキュリティ上のリスクは低いと考えられることから FR 3. を設定した. 以上の要求に基づき大学における受講者識別システムとして以下を提案する.

- 受講者の顔の特徴量による識別システム

1. 受講者の顔の特徴量による識別システム

このシステムは以下の要素で構成される.

- 受講者識別サーバー並びに付随するネットワーク (サーバー)
- 特徴量抽出機能を持ったクライアントサイドアプリケーション (授業支援システム)

このシステムの概要は以下の通りである. サーバーの機能は以下の通りである.

- サーバーは各学生の顔写真から抽出された特徴量 (1) を保管する
- 授業支援システムから特徴量 (2) を受信する
- 以上のデータを比較し受講者の出席を判定する
- 講師に判定結果を通知する

特徴量 (1) は入学手続きなどの際に大学に提出される顔写真を元に生成され, 大学側は必要に応じて明るさの違う場合やメガネの有無などのバリエーションを用いてより良いデータを抽出する. 特徴量 (2) は授業支援システムで生成される, 詳細は後述.

授業支援システムは受講者のブラウザ上またはネイティブで動作するアプリケーションである. 授業支援システムには以下の機能がある.

- デバイスのカメラから受講者の顔写真を取得する
- 上記の写真からクライアントサイドで特徴量 (2) を計算する
- サーバーへ特徴量 (2) を送信する
- 必要に応じてまばたき検出などの生体認証を行う

特徴量 (2) は受講者のデバイスのカメラを元に授業支援システムによって計算され, サーバーに送信される. サーバーはそのデータと既知の特徴量 (1) を比較することで受講者を認証する. またまばたき検出などの生体認証を行うことで, 顔写真などを用いたなりすましが行われていないことをサーバーに通知する.

このシステムの要は顔写真そのものではなく, 顔写真から得た特徴量をある種のハッシュとして用いて受講者の識別を行うことである. これにより受講者の顔写真やカメラのデータそのものがネットワーク上に流れることがなく, またサーバー側にも顔写真を保持しないことから安全に受講者を識別できる. また必要なハードウェアはカメラのみであり, スマートフォンや PC の Web カメラなど既存のデバイスのみで利用が可能である. 一方で懸念点としては, クライアントサイドのソフトウェアで常に画像処理を行う必要があることから, 電力消費の増加や CPU の占有などが懸念される. これについては常に受講者の識別を行い続けるのではなく, 一定またはランダムな間隔で識別を行うなどで対応する必要がある. またこのシステムでは顔写真が直接ネットワーク上に流れることはないが, それに由来する特徴量のデータが通信されるため, 伝送路やデータそのものの暗号化など扱いには十分注意するべきである. 更にクライアントサイドで完結するとはいえ一時的に受講者のカメラにアクセスし画像を取得していることからシステムへの改ざんが行われないように十分注意する必要がある. また授業支援システムはクロスプラットホームであることや, インストールの手間を減らすという点から javascript などで記述されブラウザ上で動作することが好ましい.