キャンパス情報システムにおける クラウド型指静脈認証とPBIを用いたPKI基盤

今井 勉 Imai Tsutomu
高橋 健太 Takahashi Kenta
菊地 健史 Kikuchi Takeshi
齋藤 訓 Saito Satoshi
近野 雅樹 Konno Masaki

大学，企業などへの不正ログインなどの攻撃で個人情報の漏えい事故が増加傾向であり，大きな社会問題となっている。しかし，生体認証をオンプレミスで導入する場合には，専用サーバの構築・運用，既存システムの改修など多額のコストが課題となる。
日立グループは，京都産業大学の協力の下，現場立脚で既存のキャンパス情報システムとクラウド型指静脈認証を連携し，導入ならびに運用に関する課題抽出と横展開に向けた共同実証実験に取り組んでいる。その結果により，安全・安心・便利な学術システム，および社会インフラを実現することが可能となる。

1. はじめに

日本では日立製作所を含め，産学協同あるいは産学連携に積極的に取り組んでいる。昨今，大学などの研究成果と企業のニーズを融合し，持続可能なイノベーションを創出するため，実用化に向けた取り組みが求められている。

国立研究開発法人科学技術振興機構と国立研究開発法人新エネルギー・産業技術総合開発機構では，わが国の産学連携を強力に推進するために，国内最大規模の産学マッチングの場であるイノベーション・ジャパンを主催している。日立は，イノベーション・ジャパン2013に出展していた京都産業大学 秋山豊和准教授に安全・安心・便利な本人認証を実現するクラウド型指静脈認証を提案した。インターネットサービスの普及に伴い，パスワードリスト攻撃をはじめとする不正ログインの脅威が急速に増加しており，大学の情報システムにおいても，ユーザー認証の強度を今後より担保する必要性を秋山准教授は感じていたことから，事業化を前提として社会的な課題解決をめざす共同研究の合意に至った。

本稿では，キャンパス情報システムにおいて，クラウド型指静脈認証，および新技術のテンプレート公開型生体認証基盤（PBI：Public Biometric Infrastructure）を用いたPKI（Public Key Infrastructure：公開鍵暗号基盤）を活用した共同実証実験の取り組みについて述べる。

2. キャンパス情報システム連携

2.1 背景と目的

インターネットサービスの普及に伴い，パスワードリスト攻撃をはじめとするユーザー認証情報への攻撃が急速に増加しており，インターネットにおけるサービス提供者にとって，認証情報の保護が大きな課題の一つとなっている。

大学の情報システムにおいても，情報システム上で個人情報を扱うため，ユーザー認証の安全性強化が課題となっている。しかし，生体認証などのより安全な認証方式の導入には，専用サーバの構築・運用，既存システムの改修など高いコストがかかると考えられている。

そこで，京都産業大学と日立グループの共同研究として，大学における新たな生体認証技術を用いた認証強化の可能性について調査するため，クラウド型指静脈認証プロトタイプシステムと京都産業大学側で構築しているPKIの利用を簡易化する機構のプロトタイプシステムを用いて，クラウド型指静脈認証の導入ならびに運用に関する課題抽出のための共同実証実験を行った。

2.2 研究目標

この研究テーマでは，京都産業大学のキャンパス情報システムと日立グループのクラウド型指静脈認証サービスとを連携し，効率性，利便性，および課題を導出する。

具体的には，SSO（Single Sign On）認証製品SHIELD

および指静脈認証製品AUthentiGateによるクラウド型指静脈認証プロトタイプと，学術認証フェデレーション（以下,「学認※1)」と記す。）で標準的に利用されているSSOミドルウェアShibboleth※2)を用いて京都産業大学に構築した認証サーバを連携させ，学認Shibboleth環境から日立グループのクラウド型指静脈認証への上位認証技術を確立させる。

また，学認Shibboleth側の変更箇所を明確にし，モデルとして確立することによって大学側導入時の負担軽減を図る。さらに，利用者側の使用感について調査を行い，導入・ユーザー操作における留意・検討事項を提示することを目標とした。

2.3 研究成果

この研究の成果は次の3点である。

(1) SHIELDとShibbolethをSAML（Security Assertion Markup Language）2.0で連携させることに成功し，その際に必要な設定項目を洗いだすことができた。

(2) 認証サーバ（IdP：Identity Provider）側の設定自体はShibbolethに標準で備わっている設定項目の追加によって実現できることが確認できた。

(3) Shibboleth IdPとSHIELD IdPの連携はShibboleth IdP上のRemoteUser認証のURL（Uniform Resource Locator）をShibbolethのSP（Service Provider）モジュールで保護し，ShibbolethのSPモジュールとSHIELDのIdPを連携させることで実現できた。

以上により，学認Shibboleth側の変更箇所を明確にし，モデルとして確立することができた。このことにより，学認参加大学が日立グループのクラウド型指静脈認証を導入する場合，これらの研究成果を適用でき，大学側のサーバ設定変更の負担を軽減することが可能となると考える。

今回の結果から，現状の「ID・パスワード」によるログイン認証に対し，体感速度・使用感・認証精度ともユーザー利用シーンにおいて劣っていることがなく，十分に日常の利用に耐えることが分かった。このことから「ID・パスワード」のキー入力によるセキュリティリスク（盗聴・なりすましなど）の低減といった観点から十分に導入の意義はあると考えられる。

一方で，すべてのユーザーの抵抗感を導入時から拭うのは難しいと考えられる。クラウド型指静脈認証導入は，学生を含めた全構成員を当初からの対象にするのではなく，特定の業務にあたる教職員など，特定範囲から順次導入していき，生体認証利用シーンが徐々に大学内に広がっていくといった環境の醸成が望ましいと考えられる。

3. PBIを用いたPKI基盤

3.1 背景と目的

Webブラウザはインターネットにアクセスするインタフェースとして広く普及しており，WebRTC（Web Real-Time Communication）のようにローカルなデバイスとの連携が強化されるに従い，P2P（Peer to Peer）型の通信も含め，これまでにない新たな形態での通信の必要性が高まっている。

一方で，WebSSOの技術が広まり，SSOサーバによってエンドユーザーの真正性が確認できる環境が整いつつある。しかし，SSOではアプリケーションに対してエンドユーザーの真正性を示す手段しか提供しておらず，エンドユーザー間で直接他のユーザーを認証する手段を提供していない。

3.2 研究目標

この研究テーマでは，SSOの適用領域をP2P通信やコンテンツ署名が必要な領域へと拡大し，学認の有用性を高めることをめざす。

京都産業大学ではWebSSOとPKIを連携させることで，Webブラウザ上でエンドユーザー間が直接相手を検証する手段を提供する方法を検討し，そのセキュリティ上の課題について明らかにする研究開発を行っている。

本共同研究において，京都産業大学の研究開発とクラウド型指静脈認証を組み合わせることで，Webアプリケーションにおいてより安全に簡易なPKI認証を実現できる可能性がある。

3.3 研究概要

京都産業大学ではWebSSOによってエンドユーザーが認証できるという前提の下，Webブラウザ上でオンラインでの証明書要求，発行，利用が可能な簡易PKI環境の構築をめざしている。その際，次の項目に着目している。

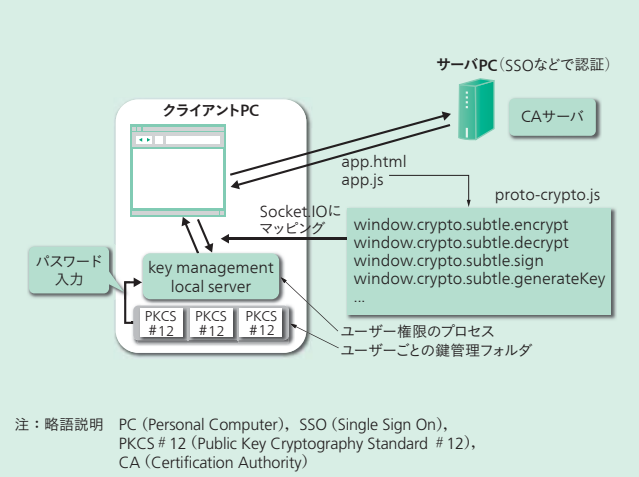
(1) 悪意のあるWebサイトに対する安全性の確立

(2) ユーザーの複雑な鍵管理操作からの解放

(3) WebRTCなどの新たなアプリケーションへの適用

ブラウザ上で暗号処理を実現するためのJavaScript※3) API（Application Programming Interface）として，Web Cryptography APIの標準化ならびに各ブラウザでの実装が進められている。標準化文書上ではJavaScriptから隔離さ

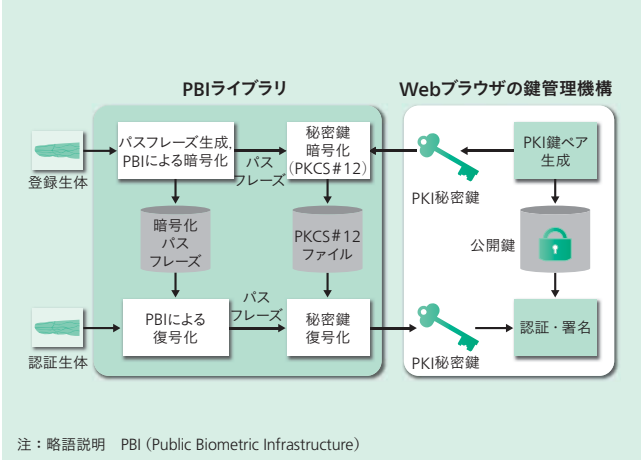
※1) 学認は，大学共同利用機関法人情報・システム研究機構国立情報学研究所の登録商標である。
※2) Shibbolethは，Internet2の登録商標である。
※3) JavaScriptは，Oracle Corporationおよびその子会社，関連会社の米国およびその他の国における商標または登録商標である。



注：略語説明　PC（Personal Computer），SSO（Single Sign On），PKCS＃12（Public Key Cryptography Standard ＃12），CA（Certification Authority）

図1｜簡易PKI機能検証用フレームワーク

京都産業大学において，クライアントPC上のブラウザ外部に暗号機能を実装し，PKI（Public Key Infrastructure）の鍵管理を容易化するプロトタイプを開発した。



注：略語説明　PBI（Public Biometric Infrastructure）

図2｜PBIの連携モデルとWebブラウザの鍵管理機構

PBIの暗号化／復号化機能を応用することで，パスフレーズを入力することなく，クライアント認証を実現可能とする。

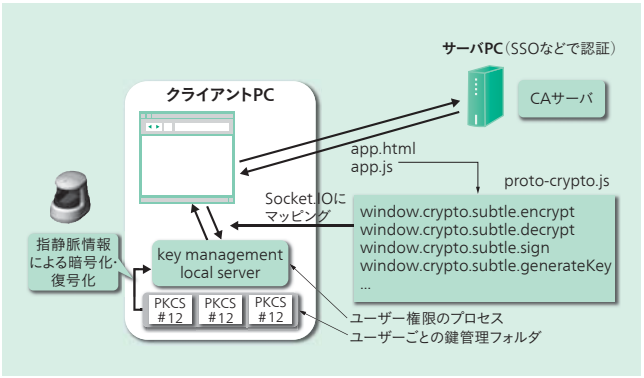


図3｜簡易PKI検証用フレームワーク上でのPBI連携モデルの検証

鍵管理サーバを拡張し，指静脈認証装置を活用して，パスフレーズの入力を省くことを実現した。

れた鍵管理に関する言及があるが，調査を行った段階ではブラウザ上には機能が実装されていなかった。すべてのWebブラウザに暗号機能を実装するのは困難であるが，Web Cryptography APIの実装を待たずに上述のような検討を進めるためには，検証環境が必要となる。

そこで，ブラウザ外部に暗号機能を実装し，機能検証を行うフレームワークを構築した（図1参照）。

ローカルPC（Personal Computer）上にNode.jsで実装した鍵管理サーバを配置し，Webブラウザ上のJavaScriptからSocket.IOにより鍵ペア生成，CSR（Certificate Signing Request）送付，証明書受領，PKCS#12（Public Key Cryptography Standard #12）格納などの操作を依頼する。鍵管理サーバのAPIで鍵の取り出しを禁止すれば，JavaScriptからの不正な鍵操作を防ぐことができる。

これまでに，構築したフレームワークを用いて，Webアプリケーションと鍵を自動マッピングし，鍵管理を容易化する機構のプロトタイプを実装している。

この研究では，これまでに構築した鍵管理サーバの機能を拡張し，PBIへの対応を検討した。PBIは「生体情報を秘密鍵とする暗号化／復号化および電子署名機能」を有している。本研究の鍵管理サーバでは，鍵管理サーバ上ではパスフレーズによってPKCS#12形式で鍵を暗号化して保存しているため，鍵の利用時にはパスフレーズを入力する必要がある。

ここで，PBIの「生体情報を秘密鍵とする暗号化／復号化機能」を用いてPKCS#12の暗号化に用いるパスフレーズを暗号化して保存しておき，認証時に再び生体情報を用いて復号化することで「手ぶら，パスワードレスでPKIに基づくユーザー（クライアント）認証」が実現できる。PBIライブラリとWebブラウザの鍵管理機構の連携モデルを図2に示す。

同図の連携モデルに基づいて鍵管理サーバを拡張し，PBIに対応した検証フレームワークを図3に示す。

検証環境のPKCS#12で暗号化された鍵はソフトウェアトークンであるため，実質的に偽装の難易度は変わらないが，指静脈認証の機能面での検証に用いることができる。一方，該当システムの構築中に，Web Cryptography APIにおいてトークンの実装については仕様の範疇（ちゅう）外であり，API上では明示的にトークンが利用できないことが確認できた。

実際にはPBIのような偽装の難易度が高いトークンを利用する場合，LoA（Level of Assurance）としてより高いレベルを想定していると考えられ，アプリケーション側で明示的に一定以上の偽装の難易度を持つトークンの利用を強制したいケースがあると考えられる。例えば，金沢大学で開発しているAuthentication EngineやShibboleth 3における保証レベル指定などを活用する場合には，このようなトークン指定ができることが望ましいと考えられる。今後Web Cryptography APIの拡張も視野に入れて検討していく必要がある。

3.4　研究成果

この研究成果は次の3点である。

(1) Web Cryptography APIでは，暗号処理プロバイダの実装はベンダ依存となるため，仕様の範疇外である一方，保証レベルに沿った安全な認証方式を選択するという点において，Webアプリケーション側からの要求をWebブラウザに伝え，適切なプロバイダを選択するという仕組みが必要となる。

(2) 本研究で用いるフレームワークでは，ソフトウェアトークンをベースに実装しており，その利用時にパスワードで認証する方式と指静脈で認証する方式を選択して利用可能な形としたが，これらのプロバイダ側の認証方式を指定するAPIの追加が必要になると推考する。

(3) 本研究開発においては，PBIとWebブラウザの鍵管理機構の連携モデルを検討し，簡易PKI検証用フレームワーク上に適用した。具体的にはPKCS#12の暗号化に用いるパスフレーズを暗号化して保存しておき，認証時に再び生体情報を用いて復号化することで「手ぶら，パスワードレスでPKIに基づくユーザー(クライアント)認証」を実現できることが確認できた。

以上により，現状ではPKI検証用フレームワークを用いた具体的なWebアプリケーション構築が完了していないため，今後アプリケーションを構築し，その動作検証を行うことで，Web Cryptography APIの標準化が進んで仕様が明確になった際の課題を抽出していく必要がある。Web Cryptography APIで利用されるハードウェアトークンについては，W3C (World Wide Web Consortium) が開催したワークショップ「W3C Workshop on Authentication, Hardware Tokens and Beyond」において議論が進められているが，ハードウェアベンダ間の調整なども含めてしばらく時間を要すると考えられる。その間は構築したフレームワークによって先行して検証を進めていくことになる。

4.　おわりに

ここでは，京都産業大学の研究開発と日立グループのクラウド型指静脈認証，およびPBI技術を応用した認証基盤の確立に関する取り組みを述べた。

顧客と共に現場で課題を共有し，双方が保有する研究成果を融合することによって，実用的かつ革新的なソリューションの創出が可能となることが分かった。

今後も京都産業大学と連携して「学認」への適用を実現し，電子決済，宅配業，政府機関，レジャー産業などの分野で活用できる社会インフラサービスを提供していく所存である。

謝辞

本稿で述べた共同実証実験，および検証結果にあたっては，京都産業大学の関係各位に多大なるご支援を頂いた。深く感謝の意を表する次第である。

参考文献など

1) 秋山，外：キャンパス情報システムにおけるキャンセラブル生体認証ならびにPBIを用いたPKI基盤の導入ならびに運用課題の調査研究，京都産業大学 研究者データベースシステム (2014)
2) 秋山：より安全・確実な新しい生体認証技術の可能性，J-LIS，地方公共団体情報システム機構 (2015.3)
3) 加賀，外：安全・安心・便利な社会を実現する生体認証基盤―Public Biometric Infrastructure―，日立評論，97，6-7，362～367 (2015.6)
4) 京都産業大学ニュースリリース，テンプレート公開型生体認証基盤 (PBI) を活用し、安全に大学システムを利用できる認証方式を実現，http://www.kyoto-su.ac.jp/more/2014/305/20141022_cloud.html
5) 株式会社日立システムズニュースリリース，テンプレート公開型生体認証基盤 (PBI) を活用し、安全に大学システムを利用できる認証方式を実現 (2014.10)，http://www.hitachi-systems.com/news/2014/20141022.html
6) 日立ニュースリリース，指静脈情報を用いた電子決済向け生体署名システムの試作に成功 (2014.6)，http://www.hitachi.co.jp/New/cnews/month/2014/06/0609.html
7) イノベーション・ジャパン―大学見本市，http://www.jst.go.jp/tt/fair/
8) 学術認証フェデレーション，https://www.gakunin.jp/
9) セキュリティソリューション「SHIELD」(シールド)，株式会社日立システムズ，http://www.hitachi-systems.com/solution/t01/shield/
10) 認証管理システムAUthentiGate，株式会社日立ソリューションズ，http://www.hitachi-solutions.co.jp/AUthentiGate/sp/product/feature.html

執筆者紹介

今井 勉
日立製作所 情報・通信システム社 クラウドサービス事業部
エンジニアリングサービス本部 認証ソリューション部 所属
現在，指静脈認証装置のシステム設計に従事

高橋 健太
日立製作所 研究開発グループ システムイノベーションセンタ
セキュリティ研究部 所属
現在，生体認証の研究開発に従事
博士 (情報理工学)
電子情報通信学会会員，情報処理学会会員

菊地 健史
株式会社日立ソリューションズ
クロスインダストリソリューション事業部
セキュリティソリューション本部 セキュリティプロダクト第1部
所属
現在，指静脈認証関連ソフトウェアの開発に従事

齋藤 訓
株式会社日立システムズ サービス・ソリューション事業統括本部
ビジネスサービス開発推進部 所属
現在，PBIクラウド型指静脈認証サービスの事業化に従事

近野 雅樹
株式会社日立システムズ 研究開発本部 事業開発センタ 所属
現在，流通・小売業向け最新デバイス活用，生体認証サービスの事業開発に従事