5W-3

公的個人認証を用いた統合認証方式の実装

田島祥太† 佐々木淳† 田中充† 山田敬三† 船生豊†
†岩手県立大学大学院ソフトウェア情報学研究科

1 はじめに

ユーザ認証技術は，セキュリティを確保する上で重要な役割を担っている．しかし，従来多用されてきたパスワードでのユーザ認証には，セキュリティの確保が困難になりつつあるという安全性の問題に加え，多すぎるパスワードをユーザが覚えきれないという利便性の問題が発生している．

本研究では安全性を確保しつつ利便性の高い認証を妥当なコストで達成することを目標とし，実現手段として公的個人認証を用いた統合的なユーザ認証手法を提案する．

本稿では，提案手法の概要と岩手県紫波町における実装および運用について報告する．

2 公的個人認証を用いた統合認証方式

安全性の確保を実現するための認証属性と PKI（Public Key Infrastructure），高い利便性を実現するための統合認証の実現に向けた考え方を述べる．

認証属性 ユーザを認証するための属性は知識・所有物・生体の三つに分類される．現在は知識であるパスワードを用いた単属性認証が主流であるが，安全性の観点からは複数の手段を併用した多要素認証が望ましい [1]．三属性のうち，生体属性の利用は所有物属性に比べ認証用機器が高額になり，また生体情報の登録に抵抗を感じる利用者も存在するという課題がある [2]．そのため，本提案手法では知識と所有物による二要素認証を行うことが現実的であると考えた．

PKI ユーザ認証だけでは対策出来ない MITM（Man-In-The-Middle）型フィッシングや事後否認にはデジタル署名が有効である [3]．デジタル署名利用時における，署名の正当性を保障する基盤として PKI がある．政府が提供する PKI である公的個人認証サービス（以下，JPKI とする）は運用が法律に制限される側面があるものの，民間の PKI に比べ利用料が格段に安いというメリットがある．また，住基カード内に格納された電子証明書を有効利用することが研究課題として挙げられる．このため，本研究では PKI としての安全性に加え，IC カードと PIN コード，言い換えれば所有物と知識による二要素認証を安価に行うことが出来ることと，住基カードの利用範囲拡大に向けた研究を行うため JPKI を実装し，評価することとした．

統合認証 本稿では，統合認証を，単一の手続きで複数のシステム認証が可能であるという意味で用いる．統合認証を用いることで，ユーザ側からは複数システム利用時における認証方法が単純になるため利便性が増す．また，サーバ側からは個別アプリケーションにおける認証機能の作りこみが不要になるため実装コストが削減される点や権限の統合管理による運用コスト削減といったメリットがある．統合認証は実装方法によりリバースプロキシ型やエージェント型，サービスチケット型に大別される [4]．サービスチケット型統合認証は他の２つに比べ機能が軽量であるため実装コストを抑えることが出来るというメリットがある．

以上の検討結果より，本研究では，公的個人認証を用いたサービスチケット型統合認証を実装し，実験評価を行うこととした．

3 実装

岩手県紫波町にて行われている住基カードを用いた実証実験「結いネット」での認証機構として

An Implementation of an Integrated Authentication Method by Utilizing Japanese Public Key Infrastructure

Shota TAJIMA†, Jun SASAKI†, Michiru TANAKA†, Keizo YAMADA†, and Yutaka FUNYU†
†Graduate School of Software and Information Science, Iwate Prefectural University

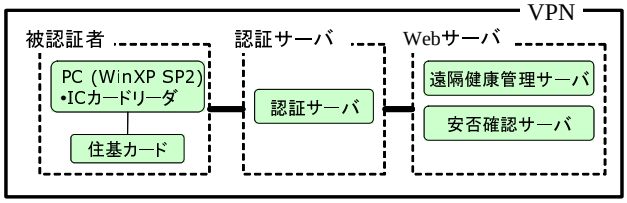

図 1 結いネットの構成概要

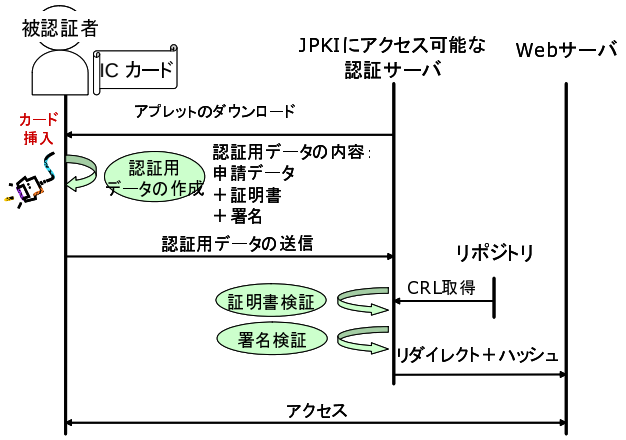

図 2 実装した認証のフロー

提案手法を実装した.「結いネット」の構成概要を**図 1** に示す．遠隔健康管理サービスにて測定した健康データを送信・閲覧する際や，安否確認システムや遠隔健康管理システムの管理者機能を利用する際に本提案の認証方式が用いられる．

実装した認証のフローを**図 2** に示す．認証用データの内容は，公的個人認証に係るサービスの利用申請書類データ（以下，申請データ）および電子証明書，申請データへの署名である．ここで申請データを作成する理由は，公的個人認証法によりサービス利用の申請を電子的な書類として送信しなければならないためである．証明書検証では，証明書の有効期限確認と CRL（Certificate Revocation List）による失効確認を行う．署名検証では，申請データから生成されたハッシュと証明書により署名を復号して得たハッシュを比較し，申請データに改ざんが無いことを確認する．証明書検証と署名検証に成功した場合，サービスを提供する Web サーバへチケットとなるハッシュと共にリダイレクトする．以降は認証されたユーザと Web サーバ間で直接アクセスを行う．

4 運用と考察

平成 18 年 12 月より，提案手法の有効性を確認するため，遠隔健康管理サービスを受ける 23 名，管理者である紫波町役場の職員 11 名による運用を行っている．

利用者一人あたりに必要となるコスト要素は，次式の通りである．

$$\begin{aligned}\text{コスト要素} \quad = \quad & \text{住基カード取得費} + \\ & \text{電子証明書取得費} + \\ & \text{IC カードリーダ購入費}\end{aligned}$$

JPKI において電子証明書取得が極めて安価であるため，コスト上の問題は発生していない．

しかし，1)JPKI の法規制により申請データの作成が必要となる，2) ダイアログメッセージが固定である，3)JPKI の利用を明示しなければならないため利用者への表示が堅苦しく難解である，などの課題が指摘されている．

5 まとめ

公的個人認証を用いたサービスチケット型統合認証方式を提案し，岩手県紫波町における「結いネット」での認証として実装を行った．今後は，提案手法の有効性を確認するために，数ヶ月間運用を継続し評価を行う予定である．

謝辞

本研究は,（財）自治体衛星通信機構および岩手県紫波町の助成および協力に基づいて研究したものであり，ここに感謝の意を表します．

参考文献

[1] L. O'Gorman. "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proceedings of the IEEE, vol.91, pp. 2021-2040, 2003.

[2] 松本勉. "バイオメトリック認証の脆弱性 -身体的特徴の偽装問題-," 情報処理, vol.47, no.6, pp. 589-594, 2006.

[3] 警視庁. "情報セキュリティ調査研究報告書," http://www.npa.go.jp/cyber/research/h9/secrepo/title.htm, 1997.

[4] 次世代電子商取引推進協議会. "認証属性ハンドブック," http://www.ecom.jp/en/results/results2004/2004_08.pdf, 2004.