4E-2

フィッシング詐欺対策のための，〉ICカードを用いた個人情報送信判定方式〉

橋本〉英明†〉　桜井〉鐘治†〉　撫中〉達司†〉
三菱電機株式会社†〉

〉

１．〉はじめに

近年，インターネット利用者の増加に伴い，フィッシング詐欺による個人情報漏洩が社会問題となっている．フィッシング詐欺は，詐称メールにリンクされた偽装サイトを使用して個人情報を盗む新たな詐欺で，被害者の多くは個人情報を盗まれたことに気づかない．〉

本稿では，被害が増加中の本詐欺への対策として，IC カードを用いた個人情報送信判定方式を提案する．本方式は，予め IC カードに個人情報とその個人情報の送信を許可するサイトを登録し，サイトへデータを送信する際に登録情報を基に送信の可否を IC カード内で判定し，ユーザが気づかない場合でも注意を促すことで偽装サイトへの個人情報漏洩を防止することに特徴がある．〉

２．〉研究の背景

〉近年，電子商取引のようなオンラインサービスの普及により，ユーザの利便性が向上する一方，電子的に送受信される個人情報の不正取得を目的とした犯罪が多発している．

このような犯罪の一つとしてフィッシング詐欺がある．文献[1]によると，報告されたフィッシングサイトの件数は１ヶ月で 15820 件(2005 年 10 月)であり，増加の一途を辿っている．本詐欺の手法は巧妙で，ポップアップウィンドウを用いたアドレスバー詐欺などさまざまなものがある[2]．本詐欺被害の増加に伴い，さまざまな対策手法が提案されている．文献[3]では，正規の web サイト情報が登録された証明サーバとカメラ付き携帯電話を用いて個人情報の送信先が正当なサイトであるかどうかを検証している．ユーザに使いやすい手法である一方，サーバを使用するため，迅速な更新が必須で管理負荷が大きいことや，サーバが停止してしまうとサービスを提供できないといった問題がある．〉

〉本稿では大きな管理負荷や高い信頼性を必要とするサーバを使用しないフィッシング対策として，IC カードを用いた個人情報送信判定方式〉を提案する．〉

３．提案する個人情報送信判定方式

３．１．概要

〉本方式では，IC カードに個人情報とその個人情報の送信を許可するサイト(以降，これらをあわせたものを本稿での個人情報とする)を登録し，この登録された情報を基に IC カード内で個人情報の送信可否を判定し，フィッシング詐欺による個人情報の漏洩を防止する．〉

３．２．特徴

〉本方式は，以下の特徴を持つ．〉

1. 個人情報を IC カード内で保持〉
2. 判定機構を IC カード内に持つ〉
3. 未登録サイトへの送信を警告〉

〉これらの特徴について以降説明する．〉

３．２．１．個人情報を IC カード内で保持〉

〉本方式では，ユーザから入力された個人情報を IC カード内に登録，保持する．このため，端末上に個人情報を保持する場合に比べて安全に個人情報を扱うことができる．〉

３．２．２．判定機構を IC カード内に持つ〉

〉本方式では，IC カード内に判定機構(判定プログラム)があり，個人情報の送信可否の判定は判定機構が IC カード内で行う．端末上で個人情報の送信可否の判定をする場合に比べて，端末上のウイルスの影響を受けずに済み，判定プログラムの改ざんを防止することができる．また，IC カードに格納された個人情報を IC カード内から端末上にコピーする必要がなくなり，登録した個人情報の漏洩を防止することができる．〉

３．２．３．未登録サイトへの送信を警告〉

〉本方式では，ユーザが偽装サイトへの送信に気づかない場合でも注意を促すことで個人情報の漏洩を防止する．具体的には，個人情報をサイトに送信する際に，登録された個人情報と一致しない場合は，登録されていないサイトに送信しようとしていることを通知し，ユーザに注意を促す．その後，登録されていないサイトに個人情報を送信するか否かはユーザ自身が判断し決定する．注意を促し，最終的な判断をユーザに委ねることでセキュリティに対する意識を高めてもらい，個人情報の漏洩を防止することができる．〉

A Method of Checking Transmission of Private Information with IC Card to Prevent Phishing Attacks
† Hideaki Hashimoto, Shoji Sakurai and Tatsuji Munaka
Mitsubishi Electric Corporation

3．3．システム構成

提案方式を実現するためのシステム構成を図1に示す．HW は，IC カードとそれが着脱可能なユーザ端末のみで構成される．SW は，IC カード内の判定機構（判定プログラム）と個人情報登録機構(登録プログラム)およびローカルプロキシと，ユーザ端末上の設定アプリと web ブラウザとから構成される．なお，個人情報登録機構とローカルプロキシは IC カード内からユーザ端末上にロード，実行される．

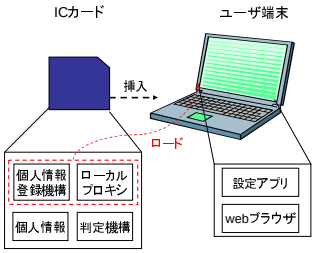

図1） システム構成

3．4．処理フロー

本方式の処理フローを図2に示す．なお，初期設定では，IC カードには個人情報が登録されていないものと仮定する．

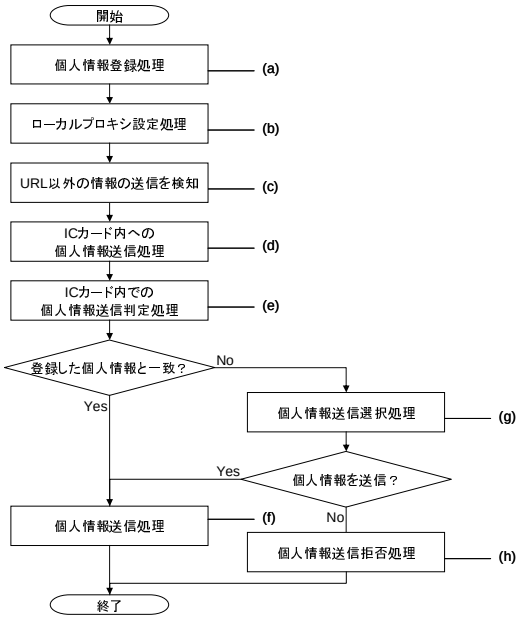

図2） 個人情報送信判定処理フロー

IC カードがユーザ端末に挿入されると，設定アプリが個人情報登録機構(登録プログラム)をユーザ端末のメモリにロードする．ロードされた個人情報登録機構は，個人情報登録用の画面を立ち上げ，ユーザがその画面を用いて個人情報の入力を行う．入力が終わると，個人情報登録機構はその情報を IC カード内に登録する((a))．(a)の処理が終わると設定アプリが IC カードに格納されていたローカルプロキシをユーザ端末のメモリにロードする((b))．その後，ロードされたローカルプロキシは，URL 以外の情報の送信を検知すると((c))，ユーザが Web ブラウザから入力した個人情報や送信先サイトの URL 情報の送信をブロックし，ブロックした情報を IC カード内の判定機構に送信する((d))．判定機構では，(a)で登録した個人情報と，(d)でブロックした情報を比較し，一致するものがあるかどうかを判定する((e))．一致する場合，ローカルプロキシはブロックした情報をサイトへ送信する((f))．一致しない場合，その旨を通知し，送信を許可するか拒否するかの判断をユーザに指定させる画面を表示する((g))．ユーザが個人情報の送信を許可した場合，ローカルプロキシはブロックした情報をサイトへ送信する((f))．ユーザが個人情報の送信を拒否した場合，その旨を通知する画面を表示し，ローカルプロキシはブロックした情報を破棄する((h))．

4．おわりに

本稿では，フィッシング詐欺対策のための IC カードを用いた個人情報送信判定方式について述べた．この方式によって個人情報を IC カードで安全に保護し，送信可否の判定をユーザに委ねることでセキュリティ意識の向上を図ることができる．また，個人情報の送信判定処理はサーバを使わず IC カード内で行うため，サーバの維持管理が不要であり，また，ユーザ端末にウイルスが存在してもその影響を低くできる．

今後の課題として，プロトタイプを作成してその有効性を実証するとともに，ユーザ端末にロードされたローカルプロキシをユーザ端末に存在するウイルスから守るための方式を検討する．

参考文献

[1] Anti-Phishing Working Group: Phishing Activity Trends Report – October 2005, http://antiphishing.org/apwg_phishing_activity_report_oct_05.pdf, 2005.

[2] 荒金陽助，柴田賢介，金井敦“フィッシング詐欺に対策に向けた一考察”, DICOMO 2005, pp.481-484, July, 2005.

[3] 柴田賢介，荒金陽助，金井敦“フィッシング詐欺対策のための URL 検証方式の提案”, DICOMO 2005, pp.485-488, July, 2005.