M-011

フィッシング対策としてのPKIの適用と課題
Issue of PKI based countermeasures against Phishing

榊原裕之†　藤井誠司†
Hiroyuki Sakakibara　Seiji Fujii

1．はじめに

近年，インターネット上の詐欺行為であるフィッシングが横行しており，個人情報が奪取される被害が報告されている．対策として接続先サイトを確認するためにSSL/TLS[1]或いはS/MIME[2]等の署名メールなどのPKI(Public Key Infrastructure)技術の適用が奨励されることがあるが，PKIを適用すれば安全であるという風潮を逆手にとり，PKIに対応した一見安全に見えるフィッシングWebサイト／メールの出現が予想される．

そこで本稿では，フィッシング対策の観点でのPKIの実装・運用の課題と改善策について論ずる．

2．フィッシングについて

フィッシングとは，悪意のある人物/組織（以下，フィッシャー）が，正規の金融機関等に成りすまし，一般ユーザ（以下，ターゲット）から個人情報を搾取するインターネット上の詐欺行為である．

代表的な手口を以下に説明する．フィッシャーは金融機関を偽装するフィッシングメールをターゲットに送付する．フィッシングメールをHTMLで表現することで，個人情報をメール上で直接入力させ，フィッシャーのサーバに情報を送信させる.また，メールに指定されたURLへ接続すると，フィッシングWebサイトに誘導され，尤もらしい口実でログイン情報等の個人情報を入力させる方法がある[3].

3．フィッシング対策としてのPKIの適用と課題

3.1　PKIの適用

フィッシングの手段に利用されるメールとWebサイトに対し，通信相手の認証を強化するため，以下のようなPKI技術の適用を確認することが推奨されている[3].

○　SSL/TLS（以下SSL）の利用

SSLを適用したWebサイト(以下SSL-Webサイト)にアクセスする場合は，ユーザはWebサイトをサーバ認証により認証する．サーバが保持する証明書には，ドメイン名が記載される．ブラウザは当ドメイン名とアクセス先URLのドメイン名の一致をチェックすることで，接続先のWebサイトがCA(Certification Authority)より証明書の発行を受けたことを確認できる．

○　S/MIMEの利用

S/MIME署名メールを使用している場合は，電子署名により送付者が認証される．メールの送信者がCAより証明書の発行を受けたことを確認できる．

3.2　PKIが推奨される理由

PKIの推奨理由に「犯罪集団が公的なCAから証明書の発行を受けることは無い」という仮定が推測される．例えばサーバ証明書の発行を受ける場合はCAの審査が必要であり，発行を受けたとしても，フィッシング行為が発覚した場合は審査時の情報に基づき追跡調査される可能性があるためである．つまり，正常に通信可能なSSL-WebサイトやS/MIME署名メールであればフィッシャーの様な犯罪集団が運営しているリスクは低いという仮定がある．

一方，普及しているWebサーバ，ブラウザ，メーラは既にPKIに対応しているものが多いため，導入し易い対策であることも理由であると考えられる．

3.3　PKIを悪用したフィッシング

PKIの適用がフィッシング対策として推奨されているため「SSL-Webサイト/署名メール＝安全」と漫然と誤解するターゲットも多いと考えられる．よって，今後フィッシャーは偽装のSSL-Webサイトや署名メールを悪用することで，ターゲットに安心感を与えた上でフィッシングを行う可能性がある．

その場合，フィッシャーは証明書を保持する必要があるが，公的なCAから証明書の発行を受けることはリスクがあり困難である．従って，フィッシャーは，自作のCAで証明書を発行し，フィッシングSSL-Webサイト／S/MIME署名メールを使用する必要がある．

3.4　PKIアプリケーションの課題

自作のCAの証明書はブラウザ／S/MIMEメーラにはインストールされていないため，そのままでは証明書のチェック時に警告画面が表示される．フィッシャーは当表示を回避するためにターゲットに対して以下を準備として行う必要がある．

(A)　警告画面における証明書の受入の指示を出す．

(B)　自作のCAの証明書を偽装Webサイトからダウンロードさせるかメールに添付し，予め信用する証明書のストア（トラストストア）へインストールする指示を出す．

これらの指示はフィッシングSSL-Webサイトへの接続やS/MIMEメール受信に先立ち，金融機関を偽装するメール等で行う．いかにも尤もらしい理由を示すことでターゲットを錯覚させることが必要である．特に（B）の指示に成功した場合は，その後は，自作CAの発行する証明書は全てチェックに成功するため，警告画面が表示されること無く任意の企業になりすますことが可能となり危険である．証明書の受入／トラストストアへのインストールの妥当性を適切に判断できるターゲットは少ないため，当準備が成功する可能性がある．

4．PKIアプリケーションの課題の解決

そこで，ユーザが不審な証明書の受入やインストールを行う可能性を低減する方法として，SSL／S/MIMEなどのPKIアプリケーションの通信メッセージのスキャン機能を備えた装置（本稿ではPKIスキャナと呼ぶ）を提案する．PKIスキャナでは以下の証明書に関する監視処理を行う。

4.1　SSL-Webサイトとの通信の監視

・許諾されない証明書の監視

† 三菱電機株式会社　情報技術総合研究所，
MITSUBISHI ELECTRIC CORPORATION
INFORMATION TECHNOLOGY R & D CENTER

SSL ハンドシェイクを監視し，通信に利用されている証明書が許容されるものか否かをチェックする．企業等の組織においては図１の様に監視対象の組織のネットワーク上に PKI スキャナを設置し，ServerCertificate[1]内に運用ポリシー上許諾されない証明書を含む SSL ハンドシェイクメッセージを検知した場合は受信者にメールで警告を発行する．サーバ証明書の許諾条件は以下である．

(a) サーバ証明書のパスが許諾される CA 証明書下に構築されかつ署名の検証に成功すること
(b) 証明書のパスが有効期限内であること
(c) https で接続する URL 内のドメイン名がサーバ証明書内に含まれること

処理(c)については，Proxy を使用する環境では https でのリクエスト(CONNECT)[1]を捕捉し，接続先のドメイン名・IP アドレスを記録する．当 IP アドレスから ServerCeritificate が返信された場合にチェックを行う．Proxy を使用しない環境では，ClientHello を捕捉し，送信先の IP アドレスから DNS を逆引きしドメイン名を記録，以降は同様のチェックを行う．

・証明書の一時受け入れの監視

ブラウザにおいてチェックに失敗した証明書をユーザが GUI で一時受入したことを検知する方法である．ブラウザは ServerHelloDone[1]を受信してからサーバ証明書のチェックを処理し，警告画面を表示する．サーバ証明書を一時受入した場合は ClientKeyExchange が送出される．証明書のチェックが成功した場合に比べ，警告画面の表示と一時受入ボタンを押す操作の分 ClientKeyExchange の送出が遅くなるため遅延時間を捕捉することで一時受入を行ったか否かを判定する（図２）．図２の実装例とは異なり，ハンドシェイクを確立した後で証明書のチェックを処理する実装も存在する．この場合においても，チェックに失敗した場合は警告画面を表示する実装となるので，ハンドシェイク終了後の通信の開始の遅延時間を捕捉することで一時受入を判定する．

4.2 S/MIME メールの監視

・許諾されない証明書の監視

S/MIME 署名メールでは，署名者の証明書がメッセージに含まれるため，4.1 の SSL 通信の監視と同様に署名者の証明書が許諾可能かを監視する．

・証明書の一時受け入れの監視

証明書の受入に関しては，SSL の様に通信データの特徴から判定することはできない。そこで，署名者の証明書が許諾されない場合に，メール差出人/本文に記載のメールアドレス・URL を保持し，一定期間，これらのアドレスに対する同受信者からのアクセスを監視する。アクセスがあった場合は，証明書を受入れメールを閲覧した結果アクセスを行っていると判断できる（図３）．

また，フィッシャーは，3. 4 の（B）に示す自作 CA の証明書を添付したメールを S/MIME 署名メールとして送信する可能性がある．よって，S/MIME 署名メールにおいて署名対象のデータをスキャンし証明書が添付されている場合は許諾されるものか否かチェックする．

4.3 非 PKI メッセージにおける証明書の監視

証明書を含んだ HTML コンテンツ/証明書が添付された（S/MIME ではない）通常のメールを監視し，許諾される証明書か否かチェックすることで，3.4 の(B)の準備行為の検知が可能となる．

○ PKI スキャナの適用箇所

4.1～4.3 では図１の様にネットワークスキャナの適用形態を想定しているが，ゲートウェイに適応した場合では，不審な証明書を捕捉した時に，警告メッセージの発行に加え通信／メッセージの遮断が可能となる．

また，PKI スキャナを ISP(Internet Service Provider)に設置することで，一般のインターネットのユーザへのフィッシング防止サービスとしても適用可能である．

5．おわりに

フィッシング対策として PKI の適用が推奨されているが，PKI アプリケーションの証明書の取り扱いの柔軟さが逆にフィッシングに悪用される課題を示し，対策として PKI スキャナを提案した．PKI スキャナで許諾されない証明書を監視することにより，ユーザが許諾されない証明書を受入れることによるフィッシングの被害を低減することが可能である．同時に，許諾されない証明書を利用した許諾されない暗号化通信を捕捉することになるため，企業等の組織に適用した場合では，情報漏洩防止の観点での暗号化通信の監視にも適用可能である．

今後は，実装を通し実用性の確認を予定している．

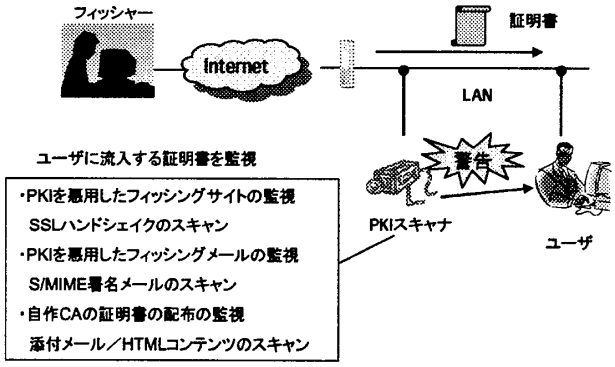

図１ PKI を適用したフィッシングへの対策例

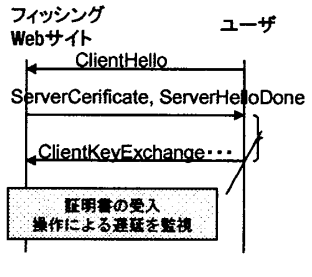

図２ SSL 通信の監視

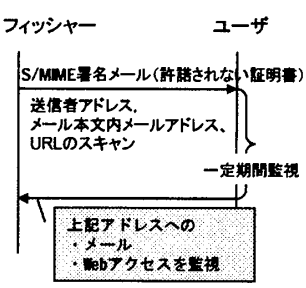

図３ S/MIME 署名メールの監視

[参考文献]
[1] SSL and TLS Designing and Building Secure Systems, Rescorla, Addison Wesley, 2001
[2] RFC2311 S/MIME Version 2 Message Specification
[3]Anti-Phishing Working Group,Consumer Advice
http://www.antiphishing.org/consumer_recs.html