COLUMN

電　子　認　証　い　ま　む　か　し

第3回　電子認証の苦悩（1）

櫻井 三子　mine@ax.jp.nec.com
日本電気（株）

木村 泰司　taiji-k@is.naist.jp
奈良先端科学技術大学院大学

回 WWWにおける電子認証

WWW（World Wide Web）はインターネットを使うネットワークサービスの中で最も多く利用されているシステムであろう．ニュースやブログ等の情報伝達手段であると同時に，政府の電子申請や通信販売などにも使われている．電子認証の技術はWWWが作られる前から存在していたが，その重要性はインターネット，特にWWWの利用分野の拡大とともに増してきていると思われる．今回は，電子認証の仕組みが利用されていながらも確からしさを疑い出すときりがないという「苦悩」を，WWWで使われているSSL（Secure Sockets Layer）を例に紹介する．

回 鍵マークとSSLと認証局

ある日あなたのところに，金融機関の何らかの手続きを促す電子メールが届いたとする．メールにはその金融機関らしきURLが書いてある．Webブラウザでアクセスしてみると見たことのある金融機関のロゴマークが入ったWebページが表示される．果たしてこれは自分のパスワードなどを入力してもよい状態なのだろうか．Webブラウザの設定を含めて，疑いをかけられる点を見ていこう．

Webページの見た目

はじめに，URLを元にWebブラウザでアクセスしたときにその金融機関のWebページが表示されなかったら，そもそもの「手続きを促す電子メール」がおかしい．フィッシング詐欺のメールだとしても手際が悪い．

このコラムを読まれている方であればお分かりのことと信じたいが，たとえそこで金融機関らしき見た目のWebページが表示されたとしても安心はできない．表示されたWebページをいったん保存してそれをWebブラウザで開いてみれば，本物とまったく同じWebページが表示される．つまり偽者のWebサーバが，あらかじめオリジナルのWebページ（htmlファイルなど）を入手しておき，あなたがアクセスしたときに本物のWebサーバの如くに送ってくることは十分にあり得ることである．

メールに書かれたURLの信憑性

Webページの見た目が信じられないのならそのURLを疑う方がいるかもしれない．金融機関だと分かっているドメイン名がURLに入っていれば，アクセスしているWebサーバがその金融機関だと見なすことができるかもしれない．しかしそもそも金融機関のドメイン名をいちいち覚えていられないのが実情だろう．Webサーバの運営が業務委託されていてまったく想像がつかないドメイン名が使われている場合もある．

一方，通知してきたメールの信憑性は確認のしようがない．送信者（From）が書き換えられているかもしれないし，メールのヘッダから送信元が金融機関かどうかを判断することは難しい．そこで次に述べるSSLの認証が必要になる．

SSLかどうか

多くのWebブラウザで表示される鍵マーク（Internet ExplorerやMozillaならステータスバーの近くにある）は，もはやお馴染みであろう．鍵マークはSSLのコネクションが確立したことを示しており，この時にやりとりされたデータは暗号化され，Webサーバが認証されている状態である．SSLでWebサーバの認証ができていないと，そのサーバは見た目が同じようなWebページを送ってきた偽者である可能性がある．そこでパスワードなどを入力すると，そのデータは盗聴されたり入力したデータが偽者のWebサーバに送られる可能性があり，危険である．

それでは鍵マークが表示されていれば安全なのだろうか．

回 Webサーバの電子証明書を発行した認証局

ここではSSLで行われた認証の結果を左右する要素について考えてみる．SSLで行われるサーバ認証にはPKI（公開鍵基盤）が使われている．Webサーバの電子証明書を，発行元であるCA（Certification Authority：認証

局）の電子証明書（以下，証明書と呼ぶ）を使って検証し，成功すれば認証できたことになる．この仕組みのおかげで CA の証明書が手元にありさえすれば，初めてアクセスする Web サーバでも認証できる．

そこで問題となるのは，ユーザはどの CA の証明書を持っておくか，ということである．本来であれば**図 -1** にあるような，CA の証明書のフィンガープリントを「本物」と比べることで確認し，確認された CA の電子証明書のみを持っておく方法が考えられる．しかし，もしユーザが 1 つ 1 つのフィンガープリントを確認する必要があったら，その手間を考えると，今日のように多くのユーザに SSL が使われることはなかっただろう．

Web ブラウザの「信頼された認証局のリスト」はこの確認の手間を省くために使われている．このリストは，信頼された CA の証明書を Web ブラウザに設定しておくことで，サーバ認証のたびに CA の証明書を検査する手間を省くことができる．リストに入っている CA のどれかから Web サーバ証明書が発行されていれば，警告なしに Web ページが表示される．

ちなみに Microsoft 社は「Microsoft ルート証明書プログラム」[☆1] と呼ばれる承認プログラムを実施しており，Windows 製品に証明書が組み込まれるルート CA の条件を設けている．このプログラムでは米国公認会計士協会（AICPA）の定めた「WebTrust for CA」[☆2] と呼ばれる認証局監査の基準を主に利用している．

しかし「信頼された認証局のリスト」はユーザ自身による追加や削除ができるようになっている．組織内部で利用するようなプライベートな CA を導入しようとする際に，ユーザがその CA の証明書を追加することがある．

回 鍵マークが出ていても疑わしいケース

ここで鍵マークが表示され，警告が出ていなくても疑わしいケースを 2 つ紹介する．1 つは有効な証明書を使ったフィッシング詐欺である．これまでは SSL を使わずに単に似たような Web ページを用意するだけのフィッシング詐欺しか報告されていない．しかし，金融機関の Web サーバであるかのようなホスト名を使って，証明書の検証に成功するようなサーバ証明書が発行されていた場合にはどうなるのだろうか．ユーザはその URL が金融機関の提供しているサーバのものかどうかを容易には確かめられない．もう 1 つは他の CA が同じホスト名の証明書を発行した場合である．「信頼された認証局のリスト」にある他の CA が，金融機関の Web サーバと同じホスト名が載っている証明書を発行したとする．偽者のサーバ管理者が DNS を悪用するなどして，ユーザのアクセスを誘導したらどうなるのか．先ほど書いたように Web ページのコピーを活用すると，この 2 つのどちらの場合も本物のような Web ページと SSL の鍵マークが表示されてしまう．

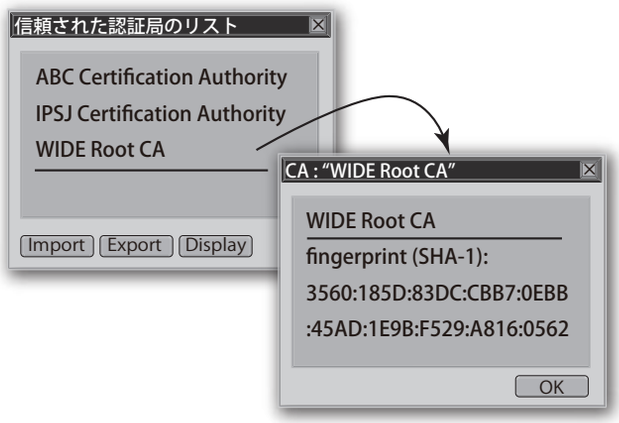

図 -1　CA の証明書のフィンガープリント

そこで Web ページでパスワードや個人の情報を入力する前に 1 つのチェックをお勧めしたい．それは，その認証にどの CA の証明書が用いられたのかを見ることである（Internet Explorer ならば，鍵マークをダブルクリック）．まず自分が Web ブラウザに登録した CA であるかどうかである．アクセスしている Web サーバに対して，自分が登録したことのある CA が証明書を発行しているのであれば，認証の信憑性を確かめやすい．一方，あらかじめ Web ブラウザに組み込まれていた CA の証明書の場合は，Web ブラウザに組み込まれる条件とその CA の運用状況を調べて判断するしかない．そのためには CA から公表された認証業務規程（CPS：Certification Practice Statement）を読む方法があるが，それはサービスの契約書を読むような作業で，最終的には各個人の判断となる．

回 携帯電話に思うこと

携帯電話に CA の証明書が組み込まれる時代になった．SSL の通信機能が搭載されているので，PKI を使ったサーバ認証ができるということになる．

しかし私（木村）が持っている携帯電話では，フィンガープリントを表示できないし，また自分の好きな CA の証明書を組み込むこともできない．組み込みの操作ができなければ，おかしな CA の証明書が使われることがなく安全だという考え方はあるかもしれない．しかし CA の証明書はユーザの信頼の基点である．ユーザ自身が安心できるような仕組みをとっておいていただけるとありがたいのだが …

次回は，PKI をユーザへどう見せるかといった普及に関係する議論を紹介したい．

（平成 17 年 4 月 28 日受付）

☆1 Microsoft ルート証明書プログラム：http://www.microsoft.com/japan/technet/security/news/rootcert.asp
☆2 WEBTRUST：http://www.webtrust.net/