COLUMN

電　子　認　証　い　ま　む　か　し

第 6 回　電子認証の未来

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 認証いまむかし

先日知人と会うために職場の近くにある珈琲屋に入ることがあった．いわゆるシアトル系コーヒーショップではなく，むかしながらの地元の珈琲屋さんである．店内はやや薄暗く，ソファーが並んでいて，全席喫煙が可能．ホットコーヒーの注文は「ホット 1 つ」で通じる．

休憩時間らしき OL が文庫本を読む傍ら，サラリーマン風の男性 2 人がしきりと話し込んでいた．それが筆者（木村）らのすぐ隣りの席であるので，聞かずとも話が聞こえてしまう．どうやら，ある人物からもたらされた商品の情報が本当なのか，そしてその人物は本物だったのか，という話のようである．

店内の雰囲気に影響されて若干探偵の気分になっている筆者（木村）としては，まずその人物の所属から裏を取る必要があるように思われた．その人物が語った会社にこちらから連絡をかけてみて，その人物が実在するかを確かめる．

それでは，これが Web ページや，流行の RSS（Rich Site Summary）の話であったらどうだろうか．もちろん同じ方法で裏を取ることはできるかもしれない．しかし見た情報のすべてをこの方法で確かめていたらきりがない．情報の発信源となる人も問合せに対応しきれないだろう．

インターネットでは，人の認証と同様にホストを認証することが重要なのかもしれない．電子署名などを使って情報を発信した人を認証する代わりに，情報を送信するホストを認証すれば，情報の信憑性を効率よく確認できると考えられる．

回 人の認証とホストの認証

人の認証といえば，指紋などの身体的特徴を登録しておいて確認する技術がある．本コラムでは特に触れてこなかったが，今後の電子認証の強化に一役買うことは間違いないと思う．ただし，本人が一度は直接サービス提供者に出向いて身体的特徴を登録する必要があり，世界中にあるオンライン上のサービスへの応用を考えるとまだまだ工夫が必要であろう．

PKI の実験開始当初，筆者（櫻井）は人にストレスを感じさせない強固なユーザ認証の実現と継続的な運用に関心を持っていた．しかし，数々の指摘や本コラムを通じての再考により，サービスを提供するホストの認証はユーザ認証よりもさらにチャレンジングと改めて感じている．サービスを提供するための設備であるホストの運用は，インターネットの発展とともに役割分担が細分化されてきた．つまり，多くの人や組織が介在している．オンラインのサービスでは，サービスの信頼をある程度ホストの運用の健全さに委ねなければならない．しかし，それを PKI のサーバ証明書と CA 証明書の確認で納得しきれるかが問題となりつつあるように思う．

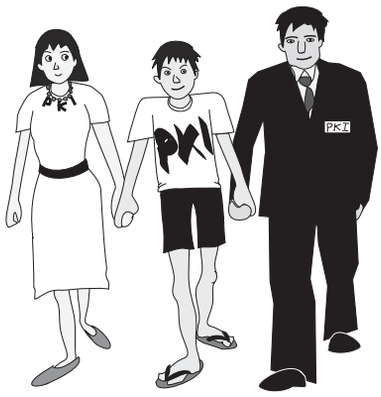
そこで，今回はホストの認証をとりまく最近の話題や方向性について筆者らの思うところをお送りする．

回 Web ブラウザに組み込まれていない CA の証明書について

本コラム第 3 回では，Web ブラウザに CA の証明書を追加できると書いた．また，Web ブラウザに CA の証明書を追加するときには，フィンガープリントと呼ばれる値を確認する必要があること，しかしながら，そのような確認は敷居が高くすべてのユーザがやりきれることではないことを書いた．

ここ 1 年，これを逆手にとって，ユーザの Web ブラウザにニセの CA の証明書を登録させてしまう「オレオレ証明書」が掲示板等で話題になっており，WIDE プロジェクトでも議論になった．なかには「限られたグループ内で使われるサーバ証明書であっても，自社 CA で発行するのではなく，商用 CA から取るのが適切だ」という意見が出た．これは Web ブラウザに証明書があらかじめ組み込まれている CA からサーバ証明書を発行してもらって利用すれば，自社 CA を立ち上げるよりも信頼性が高く，またその CA がリスクを負ってくれるのでよい，という理由である．

しかしこれには議論の余地が残されているように思われる．商用 CA は自社 CA よりも信頼性を高めやすいという点は正論だと思う．これは第 5 回のリスク #7 のところで述べた強固な設備の共同利用によって，サービス提供の原



価を下げ，自社 CA よりもコスト対効果を得やすいと考えられるためである．しかし内部利用を前提としたサーバの認証は，ユーザにとっての信頼がどこにおかれるか，という点で自社 CA の方がふさわしいことがあるように思える．これは，証明書を使った認証のユーザインタフェースの問題ではないのだろうか．

回 ホスト認証の今後

ホスト認証は，ユーザがサーバを認証したり，ホスト同士が認証する場面で行われる．「SSL のサーバ認証」はこれにあたる．ユーザが認証する側なので，認証の結果の分かりやすい表示は重要である．

SSL のサーバ認証のとき，これまでは CA の証明書が正しいかどうかなどを疑うことは少なかったのではないだろうか．見方を変えると，Web ブラウザにデフォルトで証明書がついている CA のすべてを，ユーザが暗黙的に信頼してきたと言える．

これは筆者（木村）の想像であるが，今後のホスト認証は状況が変わっていくように思われる．

まず，デフォルトで Web ブラウザについてくる CA 証明書と，ユーザが後から加えた CA 証明書は区別されるようになるのではないだろうか．現状のように CA の証明書がありさえすればなんでも鍵マークが表示されるのではなく，ユーザによって信頼する設定がなされた認証が行われたときだけ鍵マークが表示される，という具合である．これまで「人は悪いことはしないだろうから安全だろう」と思わざるを得なかったことが「自分が設定した通りの動作だから安全だろう」という認識になれば，ユーザは本当の安心感を得られるはずだ．デフォルトにはない「ユーザによって信頼された CA のリスト」は，自社の CA や取引先の CA など，ユーザにとって身近で，自らが信頼できる CA のリストになるはずである．

さらに細分化が進むかもしれない．ユーザ自身は信頼する設定をしていないが，認定基準をクリアしていて社会的に安全と認められる CA 証明書が使われる場合である．この場合は鍵マークに加えて注釈が表示されればよいかもしれない．詳細を知りたいユーザは注釈をクリックすればいいし，気にしたくないユーザは，あらかじめ鍵マークの表示の条件を厳しくしておいて，鍵マークが表示されたときには安全だと覚えておけばよい．

認定基準をクリアした CA のほかに，マイクロソフト社の CA のようにソフトウェアの配布のために必要となる CA のリストができるかもしれない．メールサーバの認証や IP 電話におけるサーバの認証など，インターネットを使う上で必要な CA のリストも必要だろう．これは ISP と契約するときにこのリストに CA が追加されるような利用のイメージである．

この細分化のためには，Web ブラウザ等に変更を加える必要がある．しかし，いずれの方法でもユーザが本当に安心できる仕組みが必要だ．

回 もっとつながって

ホストの認証はいろいろ工夫の余地がある中で，インターネットには情報家電など細かい機器がつながってくる．PC ほどの性能がなく，負荷の大きい認証の処理ができない機器も続々とつながってくるだろう．そのような機器に PKI が導入されるには，性能面，コスト面，そして，機器の寿命と証明書の有効期限とのバランス面といった条件をクリアする必要がある．なかなか厳しい条件だ（余談になるが，実際，ソフトウェアの寿命と証明書の有効期限とのアンバランスは，JAVA JCE 1.2.1 問題 [1] として露見している）．

しかし，隅から隅まで（単一の仕組みとしての）PKI である必要はないかもしれない．通信パケットがいくつかの中継点を経て最終地点に到達するように，認証の結果が引き継がれていって使われることがあってもよいはずだ．たとえば，認証されたユーザが自宅の情報家電を登録すると，その情報家電をリモートから認証できるようになり，安全に使える状態になるといった，認証の連携はあり得る．

インターネットの運用技術の分野では，DNS での名前管理に適った認証の仕組みや，ルーティングの経路情報の正しさを認証する仕組みが，IETF（Internet Engineering Task Force）で活発に議論されている．インターネットの IP アドレスを管理している“レジストリ”でも認証局が構築されつつある☆1．インターネットの仕組みと電子認証はもっとつながっていくだろう．

これからの探偵さんは，喫茶店の公衆電話 1 本で身元調査というわけにはいかないかもしれない．その代わり街中の公衆無線 LAN を暗号で武装して使いながら，PKI 技術を駆使して，「その情報は臭いぜ」と手元の PC で証明書を見ながら言うような時代になるかもしれない．

本コラムは，今回が最終回となった．この分野への誘いにつながれば幸いである．

参考文献，URL:
1) http://www.ipa.go.jp/security/vuln/20050708_jce.html

（平成 17 年 7 月 26 日受付）

☆1 筆者（木村）は，日本国内のレジストリである JPNIC で認証局の構築に取り組んでいる．