COLUMN

電　子　認　証　い　ま　む　か　し

第 5 回　苦悩と魅力はウラハラ !?

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 普及を進める原動力とは

WIDE プロジェクトに初めて参加したときの筆者（櫻井）の感想は，「インターネットとはなんと略語の類が多い世界だろう」だった．ちんぷんかんぷんながらも，研究室の先輩が徹夜をするとネットワークが伸びていて，手を動かせば実感できた．筆者らが WIDE プロジェクトで行っている PKI の実験の説明では，セキュリティ用語の略語を使うわけだが，自分たちと同じようには面白いと感じてもらえていないことに気づいた．認証に関して手を動かす環境を作っているのだから，きっと用語の説明が下手なだけだと最近まで思い込んでいた．

また筆者（木村）は「認証の分野には，身近にない概念がたくさん登場するなぁ」という印象を持っていた．権限を与えることを示す「認可」や証明書の効力がなくなる「失効」という概念は，当時の私には格式ばった世界のものだった．そのため，それらが電子的に実現することの良さがピンとこなかった．

電子認証技術の普及を進める原動力は，もしかしたら技術発展だけでなく「電子認証が実現された世界の魅力の表現」にあるかもしれない．今回は "Ten Risks of PKI" の残りのリスク #6-10 を取り上げるが，回答に苦悩するばかりでなく，逆に魅力となるポイントを見直したい．

回 Risk #6: Is the user part of the security design?

[概要] SSL サーバ証明書の内容と，表示される Web ページの内容との関係を確認する手段がなく，だまされた場合に証明書の検証者であるユーザがリスクを負う．

[回答] 今のところ，コンテンツを提供する会社とサーバ証明書に記載された会社情報がかけ離れた例をあまり見たことがない．しかしこのリスクに対して，根本的な回避策を SSL のみで出すことは難しいと思われる．

まず SSL のサーバ認証では，コンテンツ作成者を認証することはできない．コンテンツ作成者を認証するためには，電子署名のような仕組みが必要になるが，WWW で電子署名をどのように確認すべきかが標準化されていない．また認証対象をだれにするか，という運用上の問題もある．コンテンツ作成者が個人レベルで分かるようになっても，店との関係を確認することは難しい．

現実的には，運用面で対応する方法が考えられる．いわば「オンライン買い物保険」をかけ，SSL のサーバ認証でだまされた場合の補償をしてくれるというものだ．技術的にすぐに解決が図れなくても，リスクが具体的になれば運用次第でなんとかなるかもしれない．

回 Risk #7: Was it one CA or a CA plus a Registration Authority?

[概要] ビジネス上典型的な PKI のシステムに，CA ベンダとユーザ企業で役割分担をして，ユーザ企業が許可すると CA ベンダが証明書を発行する仕組みがある．しかし，CA ベンダがユーザ企業に知られずに偽った内容の証明書を発行する可能性がある．

[回答] このリスクは PKI に特有のものではなく，ユーザ企業の鍵をセキュリティベンダが預かる場合に共通するものである．これは回避が難しい．むしろ役割分担をせずにユーザ企業がすべてを抱えることの方が現実的でないように思われる．

確かにリスクはあるが，役割分担によって運用の安全レベルが高くなることはあると思う．CA ベンダが鍵を預かって不正が発覚した場合，CA ベンダは存続の危機にさらされる．CA ベンダの方が厳しい条件で人材を探したり安全な設備を整えるはずである．CA ベンダに任せる選択肢もあるはずだ．

証明書に発行元である CA ベンダの名前を入れるだけではリスクの低減は難しいかもしれない．不正の疑いが CA ベンダにあっても，被害者は CA ベンダの都合で取り決められがちな約款に従わざるを得ないためだ．これは筆者（木村）の考えに過ぎないが，運用面での新たな対策が必要ではないかと思う．たとえば，証明書に発行を許可したユーザ企業の情報を入れ，ユーザ企業が連絡の受付窓口を行う．するとユーザ企業は主体的に CA ベンダの業務をチェックする立場になり，CA ベンダの不正を抑止できるかもしれない．これと同じ効果のためか，

NPO 法人 CACAnet Fukuoka で使われている証明書の中には発行を許可した人の名前が入っているものがあるようだ．

回 Risk #8: How did the CA identify the certificate holder?

[概要] CA が証明書の所有者の本人性確認をオンラインで行う適切な手段がなく，商用 CA がリスクを負っている．

[回答] インターネット上でグローバルに利用することを想定した電子認証共通のリスク．まだ解決していない．電子メールの到達確認をもって本人性確認とする妥協点があるが，電子メールアドレスの詐称のリスクは商用 CA が負う．逆にいうと，電子メールの到達性確認程度で発行された証明書を使って受けられるサービスは限られる．一方，携帯電話や IC カードを使う方法も妥協点の 1 つと言える．肌身離さず持つようになった携帯電話への期待は今後も高まるだろう．

回 Risk #9: How secure are the certificate practices?

[概要] CA の安全性が他の認証と比べて高いとしても，CA の運用が適切でなければ，セキュアな認証基盤を実現できず，アプリケーションを含めたシステム全体にセキュリティリスクが出てくる．

[回答] 電子認証共通のリスク．文献 1）の著者は，「CA を入れるととりあえず安全」といった口調の宣伝をまずはたしなめたかったのだろう．どんな運用にすればどんな問題をつぶせるかの解決にはまだまだ時間がかかりそうだ．失効情報の伝達は徐々に工夫がされているようだが，証明書のライフサイクルや鍵長については，決め手となる基準のようなものはない．それらは「決めの問題」と言われることがあるが，それですべてを片付けるわけにもいかない．類似した話として思い出すのは，ファイアウォール装置が出回り始めた頃の宣伝だ．「右に倣え」でファイアウォール装置を買っても，適切に設定しなければ安全にはならない．今では常識だが，セキュリティをとりまく社会の変化を経てようやく浸透したのだ．時間がかかるのはしかたがない．

回 Risk #10: Why are we using the CA process, anyway?

[概要] CA 導入の目的をしっかり持っていないと，期待したシステムを構築できない．シングルサインオンは CA 導入だけでは実現できない上に，一度認証が実行された後，他の人がアクセスできる状態になってしまうことが，業務の設計次第であり得る点に注意が必要だ．

[回答] システム導入に共通のリスク．解決には，CA ベンダに限らずいろいろな立場のベンダと「実際に実現すること」を確認する以外にはないと思う．シングルサインオンで一度認証した後に他の人でもシステムにアクセスできる危険性は，情報漏えいの危険性とも通じるため，離席時の画面のロックといった運用による解決の兆しが感じられる．

回 電子認証の魅力のありか

"Ten Risks of PKI" の指摘は，電子認証の運用に共通する問題が多い．そしてたとえ証明書をパスワードに置き換えてみても，同様の問題が存在するように思われる．つまり PKI の登場によって初めて露呈しただけで，もともとの電子認証を始める環境に問題があったとも言える．そのためか電子認証の導入を検討するときに「あの場合はどうか」「この場合はどうか」といった課題の想定から始めると，きりがなくなってしまう．

逆に電子認証の技術を「どんな運用を実現するのか」という，目指す姿の想定に使えばよいかもしれない．なにもなければ安全かどうかが分からない電子的な認証に，気をつけるべきポイントを整理して示せることが電子認証の魅力であるように思われる．

何しろ，WIDE プロジェクトでの実験を通じて得られた数々の指摘と "Ten Risks of PKI" を突き合わせてみて，限りないと思われた課題を数えたら 10 個と分かってきたことは励みになった．

また，電子認証の運用は，究極には誰でもが簡単かつ安全に扱えるシステムを目指してはいるものの，システムを扱う人間の適性や能力もまだまだ重要な分野である．性善説だけでもなく性悪説だけでもない，システムと人間の関係のあり方の模索．色々な工夫が求められるという意味で苦悩であり，かつ魅力であると思う．

次回は，サーバ認証とホスト認証に関する最近の話題をお送りする．

参考文献

1）Ellison, C. and Schneier, B.: Ten Risks of PKI: What you're not Being Told about Public Key Infrastructure, Computer Security Journal, Vol. XVI, No.1 (2000).

（平成 17 年 6 月 29 日受付）