COLUMN

電　子　認　証　い　ま　む　か　し

第 2 回　PKI と電子認証のツールたち

櫻井 三子　mine@ax.jp.nec.com
日本電気（株）

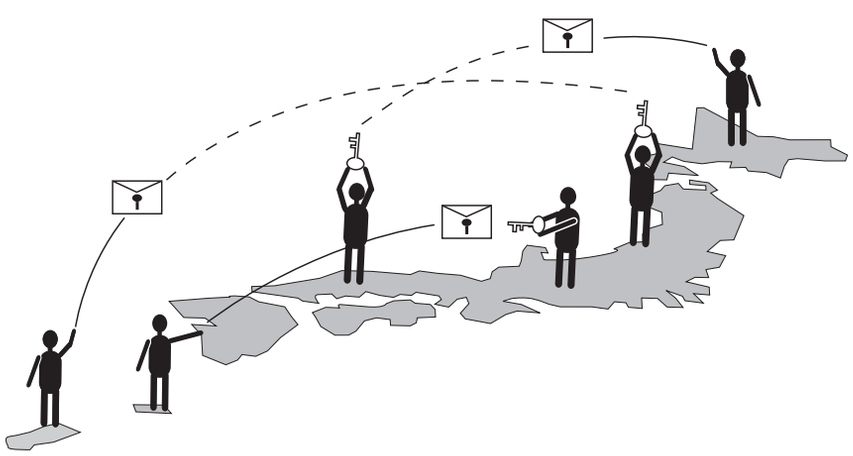
木村 泰司　taiji-k@is.naist.jp
奈良先端科学技術大学院大学

回 本当に相手と分かるまでにひっかかること

多くの人と知り合いになればなるほど，相手の認証は難しくなる．電子認証の方式を語るとき，なぜかよく登場する人が Alice と Bob だ．やはり，Alice と Bob から始めよう．

Alice: こんにちは．
Bob: こんにちは，どちらさまですか？
Alice: Alice です．
Bob: どちらの Alice さんですか？
Alice: 私です．Alice です．
Bob: Alice って人を何人も知ってるんです．
Alice: そう言われても，「私」が Alice ですから．
Bob: どういうお知り合いでしたっけ？
Alice:「私」です．昨日会ったじゃないですか．
Bob:（何人にも会ったんですけど ...）

オンラインで本人かどうかを確認するには，嘘を名乗っていないか，自分の知っている Alice かどうか，確かめる方法は確かかなど引っかかることはいろいろある．しかも，何人もの Alice と知り合いになると，「誰」かを確認するだけでは足りなくて，「どこの誰」まで知る必要がある．今までに電子認証の方式が次々と開発されてきたが，適用範囲の想定が違うと，名乗るときに使う ID の決め方が違ってくるし，認証の途中でなりすましをされないかどうかの脅威想定と対策も違ってくる．今回は，電子認証の進化をたどることで「むかし」を振り返り，PKI がどのように影響を受けたかを見て行こう．



回 電子認証のツールたち

1990 年代は電子認証のツールが流行と議論を巻き起こした時代である．1990 年代に登場したツールたちは，多くのものが現在も使われているし，考え方としてはすべて残っているといってよい．PKI もここから始まった．

1990 年代は，インターネットの普及が進むにつれて，電子認証の技術も急速に進んでいた感があった．電子認証の技術の発展には，おおまかには下記の方向がある．

1. 本人確認確度の向上（所有物，記憶，身体的特徴のうちどれを使った認証か）
2. オンライン上のやりとりの安全性向上
3. サーバ側の本人確認情報管理の安全性向上

NIS，Kerberos，ワンタイムパスワード，SSH，PGP，PEM，S/MIME，そして，https．これらのツールは，認証技術の全方向での発展を促してきた．まずは，エンドユーザがオンライン上のサービスを利用する（ログイン）時に使われるログインツールから見てみよう．

NIS（Network Information System）は，認証方式ではないが，ユーザ管理情報やホスト管理情報を複数のワークステーションで情報共有する仕組みで，パスワード情報の共有にも使われた．3. の方向だ．NIS のような考え方は，ユーザ管理情報をディレクトリで一括

管理し参照する，という世界で根付いている．

Kerberos は，一度認証を受けたらその結果をチケットとしてとっておき，サービス利用時にチケットを再提示することにより，認証をシステム間で統合する仕組みである．チケットの所持で本人確認する点が 1. の方向，チケットを得るまでのプロトコル上の工夫が 2. の方向である．認証した結果をとっておいて再提示という考え方は PKI も同様である．また，認証を一度受けるだけで，複数のサービスにアクセスできるという意味では，シングルサインオンのあけぼのといってもよい．北米の大学ではキャンパスワイドの認証方式として定着した．現在，Kerberos は，Windows サーバで採用されており，身近に使われるようになってきている．ちなみに，Kerberos とはギリシャ神話に登場する，冥府の番犬ケルベロスのことである．呼び名が略語でない認証方式は珍しい．

ワンタイムパスワードは，パスワードを使い捨てにすることによってネットワーク上でのパスワード盗聴に対抗する仕組みで，2. の方向である．時刻同期やチャレンジレスポンスといったさまざまな方式が生まれ，商用化も進んだ．今でも新しい製品が出てくる．PKI を使った認証プロトコルも，大雑把に言えば認証情報がワンタイムになるように設計される．

ログインツールは，電子認証の強化が進むと，通信コンテンツ保護の方向へ発展した．そして，認証と通信の暗号化の両方に対応できる技術として公開鍵暗号が使われるようになった．たとえば，SSH（Secure SHell）もその 1 つで，主に機器の管理者が遠隔からのメンテナンスに利用している．

ここから先は，公開鍵暗号の利用がアプリケーションツールへと広がっていった．PGP（Pretty Good Privacy）は，データ保護やメッセージ認証の観点で 1 つの完成形を示した．爆発的な発展はないが，商用化までは進んでいる．公開鍵とユーザ名の対応づけは，友達（知っている人）が証明する．友達の輪が大きければ大きいほど自分の鍵が多くの人に信頼される点が特徴だ．PKI では，鍵と名前の対応を友達ではなく CA が証明する．

PKI 応用の第 1 弾となった暗号メール PEM（Privacy Enhanced Mail）も同時期に登場した．世界中でいくつかの実装があり，相互接続実験も行われた．PEM は，電子メールの発展の影響を受け，やがて S/MIME（Secure MIME）へと移行した．いわゆる添付メールの暗号化ができるようになったのは S/MIME からである．Outlook Express や Netscape Messenger など，S/MIME 対応の電子メールツールは増えている．ただし，電子メールは身近であるがゆえに一度気に入ったツールを手放しづらく，暗号メールを目的にツールを替える人は少ない．普及とまではいえない状況である．

1990 年代後半になると，WWW が登場した．PKI 応用の代表例となる，SSL（Secure Sockets Layer）が Web ブラウザに実装されると，オンラインショッピングのようなサービスが急速に発展した．https としておなじみであろう．ユーザが店のサーバを認証する立場での PKI 利用は広まり，ベリサインなどの商用 CA ベンダが出現した．今や https なしではインターネット上のサービスを語れないほどよく使われている．

いずれのツールも，片端から試すことはできた．サーバにアクセスするためのツールは，少人数でも評価を進められた．しかし，暗号メールはメールを読む相手が必要で，多人数で試す運用実験が特に重要になる．

回 PKI とユーザ認証と FJPEM

FJPEM も 1990 年代を駆け抜けたツールの 1 つであり，日本発の PEM 実装であった．筆者らは，運用実験を通じ PKI の奥深さを肌で知った．

FJPEM は，大学や企業などの分散した組織間で運用実験を行ったという意味で特別であった．当時は，暗号メールとしてのユーザインタフェースや，PKI の証明書の発行手続きに関する議論で夢中だった．今振り返ると，ID に関する人間のこだわりを初めて実感した時期であったように思う．PKI が他の電子認証の仕組みと大きく異なる点として，ID の表現の自由度が大きいことがある．ID を電子メールアドレスにしてもよいし，「どこの誰」かを日本語で表現してもよいし，これらを組み合わせてもよい．PKI では，名刺のように，実社会で通用している ID をインターネット上で使える可能性がある．実験では，電子メールアドレスに加え，所属や氏名を証明書に記載した．

すると，たとえば同姓同名問題．証明書に記載する ID がぶつかったら，どうするのか？ N 大学の Alice と K 会社の Alice を取り違えてしまわないか？同じ人の古い証明書，新しい証明書の 2 枚が同時に存在したら混同しないか？など，PKI を広く利用するときの課題が次々と湧いてきた．

FJPEM では，N 大学の Alice と K 会社の Alice を最初に確認する機関（CA）は 1 つであった．しかし，現実の世界では，CA は複数あり，「どこの誰」の確認は今も解決していないやっかいな問題だ．

次回は，オンラインショッピングでよく利用される https は安全か，携帯電話で PKI，認証基盤の運用は誰がすればよいのか，といった「いま」の話題に移る．

（平成 17 年 3 月 28 日受付）