PKI の利用例 ～ 情報基盤センター内向け PKI 対応 SSL-VPN の紹介

PKI(Public Key Infrastructure, 公開鍵基盤)と聞いてあなたは何を連想するだろうか。それはメールあるいは通信の暗号化であったり電子署名であったり、はたまた否認防止であったりするかもしれない。今回この稿で取り上げるのは上記用途とは若干趣を異にするが、認証機能についての応用例である。とはいえ PKI の主要用途の一つであり、PKI の利用用途を大きく広げ、またコンピュータシステムの安全性向上に大きく貢献するものである。

PKI の認証機能とは

認証とは、広義にはある行為の主体が誰であるか特定することであるが、ここでは狭義の意味で何らかのサービスを利用するときに行なう利用者認証（クライアント認証）を指すものとする。

PKI において認証がどのように実現されるのか、公開鍵暗号と関連付けて概念的に説明する。各利用者は個別の鍵ペアを持つ。認証を行ないたい側（サーバ）はランダムな文章を生成し利用者に渡す。利用者はその文章に署名しサーバに返す。サーバは返された署名が正しいことを検証することで、相手が鍵ペアに結び付けられた証明書に記載されている本人であると確認できるのである。このような手順を踏むことで、PKI の認証機能は公開鍵暗号が破られないという条件のもとで安全である。つまり高々十数桁のパスワードと比較して（文字通り）桁違いの安全性がある。もちろん単純なパスワードのように秘密情報がそのまま外に出ることはないので盗聴に対しても安全である。

SSL-VPN【Secure Socket(s) Layer Virtual Private Network】とは

現在の一般的なネットワーク構成において、サービスが特定のネットワーク（研究室内、学部内など）からしか利用できないという状況はありふれたものであろう。特に機密情報を扱うシステムでは外部の悪意ある第三者の侵入を防ぐためにファイアウォール等導入しているかもしれない。このような対策は有効であるが、利便性を著しく損なう可能性がある。例えば普段は問題なくとも、出張等で自分が「外部」になった途端に何もできなくなったという経験をお持ちの方は多いのではないだろうか。

安全性と利便性はトレードオフの関係にあるが、インターネット上の特定のクライアントマシンを、あたかもそれが内部ネットワーク上にあるかのように見せ、内部システムにアクセスできるようにする技術を VPN(Virtual Private Network)という。SSL-VPN はクライアントとの通信において WWW で一般的に用いられている SSL 暗号化を用いたものである。他方 IPSec と呼ばれる VPN 技術もあるが、IPSec による VPN と比較して、SSL-VPN はクライアント側で設定の必要がないことや経路上のファイアウォール等の制限を受けにくいことから、不特定多数の端末から特定少数のサーバを利用する「リモートアクセス」型の利用形態の場合に、VPN の簡便な実現方法として有効であると言われている。

PKI 対応 SSL-VPN - 情報基盤センターでの運用例

ここまで述べてきたように、SSL-VPN は内部向けシステムを外部から利用できる利便性を与える一方、そこが内部システムへの抜け道になりうるという安全面での不安をもたらすものにもなる。安全を確保するには、特定の利用者にのみ機能を提供するだけでなく、利用者の特定を行なう認証の強度が高いことが重要である。そこで認証の強度を高めるために、SSL-VPN での認証部分に PKI の認証機能を組み込んだものが PKI 対応 SSL-VPN である。PKI

を用いることで、高いレベルの認証強度を持ち、それにより安全面を補強した SSL-VPN システムが構築できるのである。
実際に情報基盤センターで運用している PKI 対応 SSL-VPN システムの構成を図 1 に示す。

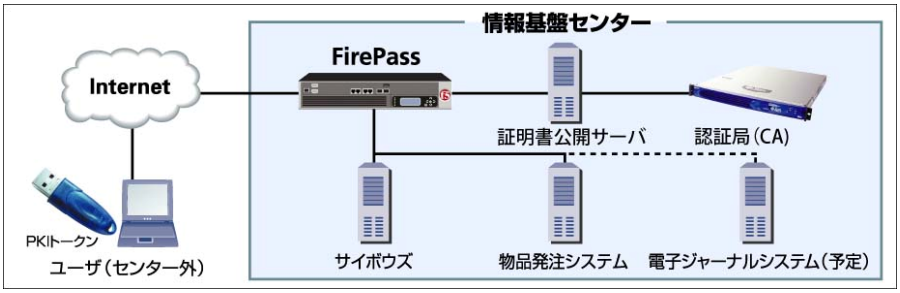

図 1　PKI 対応 SSL-VPN のネットワーク構成[12]

まず図中の「認証局(CA)」が PKI の中核である。ここで鍵ペアと証明書が発行され、それらは PKI トークン(USB トークン，図 2)または IC カード(図 3)に格納される。(注：現在 PKI プロジェクトでは本格的な認証基盤として使えるシステムを構築しているところであるが、ここで使用しているのは既に稼動している研究目的のプロトタイプシステムである。)

図 2　USB トークン

外部からアクセスする対象となるシステムは、情報基盤センター教職員のスケジュール管理や施設予約管理、文書管理などを行なっている「サイボウズ」や、同じく教職員から研究に必要な設備・備品の発注を用度係との間で仲介する「物品発注システム」などである。本部の財務会計システムについても、先方からの了解を得た上で SSL-VPN 経由の接続を許可している。

図 3　IC カード

実際に外部からの接続を受け付けるのが図中で「FirePass」と書かれている SSL-VPN 機器である。サイボウズや物品発注システムでは情報基盤センター内および SSL-VPN からのアクセスのみ許可しており、それ以外からのアクセスは遮断している。SSL-VPN での認証は PKI のみに限定し、認証時にはユーザから提示された証明書が正しく上述の認証局から発行されたものであることを確認しアクセスを許可している。SSL-VPN からのアクセス先は先に述べた対象システムに限定し、他のセンター内システムには一切アクセスできない。今回の場合対象システムが全て Web アプリケーションであるため、SSL-VPN 経由のアクセスにリバースプロキシ型のアクセスを採用することでより簡潔で安全な運用を行なっている。

なお、IC カードを利用する場合は、IC カードリーダが必要となるので、情報基盤センタ

12 この構成図は若干古い。電子ジャーナルシステムにアクセスするための VPN は別システムとして既に稼動している。また PKI トークン(USB トークン)だけでなく IC カードにも対応している。

ーでは、IC カードとともに、IC カードリーダを配付している。
　ここで挙げた SSL-VPN の使用例で情報基盤センター特有の事情を考慮したものは一切なく、各部局でもシステムさえ用意すれば同様の運用が可能である。各部局において外部からの接続を許可していない部局内システムがあり、同様の悩みを抱えているのであれば、PKI 対応 SSL-VPN を解決策の一つして考えてはいかがだろうか。

まとめ

　今回はPKI の応用例の一つとして、SSL-VPN の認証部分にPKI を利用したものを紹介した。これは実際に情報基盤センターで運用しているものである。アプライアンス(特定の利用(この場合は SSL-VPN)に特化し、簡単な設定で利用できるシステム)を利用することで特に知識・労力を必要とすることなく、PKI の強固なセキュリティを持つ認証機能を提供することができる。全学的な PKI が提供されれば、個別に IC カードやカードリーダを配布する手間も省けて、更に簡単になることが期待できる。

(西村　健)