インターネット A Scene of Internet History

歴史の一幕

ソフトウェア・コンサルタント
鈴木裕信

pgp.nic.ad.jp開設の経緯 ~The Untold Story of PKS~

「スター型のトポロジのネットワークがある。すべての通信は中心を通過するものとする。末端にはアリスとボブがおり、中心にはマロリーがいる。この時、アリスとボブがマロリーに情報を盗まれることなく安全に通信するにはどうしたらよいか」

ありきたりのセキュリティ教科書の例題のように見えるが、90年代初期に自分とJUNET上でメールをやりとりしていた仲間は現実の問題として解決しなければいけなかった。

まず共通鍵暗号を使うことを考えた。これもまた教科書的問題で、まず鍵配送をどうするか、次に多人数で使う時の鍵管理をどうするかに頭を悩ませることになる。全員で一つの鍵（パスワード）を共有し、直接会うか、もしくはFAXで鍵を送るということを実際に（嘘のようだが本当!）行った。なんとも原始的である。どうにかできないものかとしばらく考えていたが、ボンクラな筆者の頭では当然ながら解決はできない。

ある時、中野秀男先生から（暗号の話ではなく、たぶんP≠NP予想みたいな話の中でだろうと思う）「公開鍵暗号法RSAを解読するには素因数分解をしなければならないが……」といった話を聞いた。そこに答えはあった。

今はGoogleで簡単に検索することができるが、これは1991年とか92年当時のことである。当たり前であるがWikipediaもない。しかし集合知は既にあった。Usenet*である。当時、筆者はSRAという会社のソフトウェア工学研究所という部門にいた。SRAは国内におけるUNIXの先駆者的な会社で、当時VAX780ファミリにBSDを入れて開発に使っていた数少ない会社だ。この会社のコンピュータの中にはUsenetで流れていた「comp.*」がアーカイブされていた。それっぽいグループを片っ端から読んでみた。ごくごく最近に流れてきたソースコードが話題になっていた。そのソフトウェアの名前はPGP（Pretty Good Privacy）だった。

PGPを使えば、少なくともこれまでの問題は解決する。しばらくは満足したが、次の段階としてPKI問題が出てくる。すべてをいきなり解決はできない。そもそも2015年の今であってもPKIが有効かどうかは疑問の残るところである。まずはN対Nにおける鍵交換である。メールでPGPの公開鍵を送り公開鍵プールを作る。メールでPGP公開鍵のリクエストを送りメールで返送される。素朴ではあるがN対Nの公開鍵交換には十分であった。

MIT、UCSD、ハンブルグ、オックスフォードといった名だたる大学では、メールでのPGP公開鍵交換サービスの提供を開始した。全世界で4台とか5台とかしか存在していないPGPの公開鍵交換サービスの頃であったが、筆者もその交換サービスに日本から加わることにした。これらのサーバはお互いに公開鍵を同期していて、どこかに公開鍵をおけば、全世界の鍵サーバに配送された。筆者は1994年4月11日からサービスを始めた。95年当時、世界で14台のPGP鍵サーバがあった。当時のドキュメントがネットで手に入る。

http://www.enet.umn.edu/docs/software/pgp/keyserv.txt

実は使っていたマシン、筆者の会社の机の上にあるSun SPARCstation 10である。筆者の所属していたソフトウェア工学研究所は、当時、四谷三丁目の丸正スーパー総本店の5階にあった。日本UNIXユーザ会（jus）やソフトウェア技術者協会（SEA）も同じフロアにあったので、古くからのインターネット業界関係者は知っている人も多いかと思う。筆者のいた環境は割と自由で何でもできたが、それであっても、振り返って考えると、ずいぶん無茶である。

しばらくすると、新しくスタートする研究プロジェクトのメンバーとして、情報処理推進機構（IPA）に出向することになった。まだ神谷町にIPAがあった頃である。ちなみに、このプロジェクトは認知科学のアプローチからUIを研究するプロジェクトでセキュリティとは無関係である。同じ頃、菊池浩明氏、村山優子氏といったセキュリティの専門家もIPAに関係していた。研究とか関係なくずいぶん仲良くしてもらった。くどいようだが当時の筆者の研究プロジェクトは認知科学である。

その後、筆者は1996年7月にSRAを退職する。さて、PGP公開鍵サーバをどうしようかと考えていたら、菊池浩明氏が認証実用化実験協議会（ICAT）で実験として動かしてはどうかと誘ってくれた。

ICATとは、「暗号技術を応用した相互運用性のある認証技術の確立と、実サービスへの応用を目指して、大規模かつオープンなネットワーク環境下でさまざまな企業、団体等が実施する認証技術開発と実験を円滑に進めるため、この分野における各種課題について、産学協同で研究を推進する」ために作られた組織である。次のURLで過去の記録を参照できる。ちなみにこのWebサイトの最初のバージョンは筆者が作ったもので、この文章があるページは今から20年前に筆者が書いたHTMLファイルである。まさか20年後に自分で引用するとは思わなかった。

* https://www.nic.ad.jp/timeline/#usenet

http://www.wide.ad.jp/document/historical-projects/icat/

さて、実際にサーバのハードウェアとネットワークが設置されたのはICAT事務局とJIPDEC（当時の名称は財団法人日本情報処理開発協会）があった機械振興会館の地下のコンピュータルームだった。これはJIPDEC職員であった大林正英氏が手配してくれた。当時JIPDECは情報処理技術者試験の指定試験機関であった。情報処理技術者試験を管理するシステムがこのコンピュータルームにあり、当然ながら入退室は大変厳しかった。

これまでオフィスの仕事で使っていたワークステーションで動いていたものから、大変セキュアな環境におかれることになった。用意してもらったプラットフォームはSunのサーバだったので移行はまったく問題なかった。大変ありがたかった。

同時期にMITのMarc Horwitz氏が開発したPKS keyserverが現れた。このPGP鍵サーバは、メールだけではなくTCP/IP接続可能であった。hkpというプロトコルで直接PGP公開鍵をやりとりする。ICATサーバは直接インターネットに接続しているので、このHorwitz版鍵サーバを動かすには最高の環境であった。しかし、MITは（たぶんVAX環境で）うまく動くのに、Sun OS環境でコンパイルして動かしてもなかなか安定しなかった。あっちこっちにパッチを当てずいぶん苦労した記憶がある。パッチは鍵サーバ管理者コミュニティにフィードバックした。

当時ICATに提出した報告書を読み返してみると、「オックスフォード大のサーバは負荷が高く、できれば切り離したい旨のオファーを受けて、96年8月以降から97年4月まで同期を行っていなかった」といったことが書かれている。

当時国内でも大阪大学でPGP公開鍵サーバが立ち上がっていて、ICATから同期をしていた。また広島市立大学の村山（優子）研究室の学生らによってPGP公開鍵サーバの運用実験が行われており、筆者も立ち上げに協力した。

97年の暮れになると「ICATでやっているサーバよりもっといい環境が必要ではないか」と提案してくれる人が現れた。JPNICの運営委員長であった佐野晋氏である。当時、佐野氏とはJPCERT/CCの立ち上げで一緒に活動していた。佐野氏の勧めもありJPNIC向けに提案書を書いた。これはJPNICの公開資料「1997/12/22運営委員会 資料 4-2」として現在もネット上で次のように公開されている。

> 国内のPGPキーサーバの運用取りまとめを行っている，鈴木氏より，運営委員長に対して以下のような提案がありましたので，審議をお願いいたします．
>
> Subject：JPNICでのPGP Public Key Server 実験運用の提案
> AUTHOR：鈴木裕信（ソフトウェア・コンサルタント）
> E-Mail：hironobu@h2np.suginami.tokyo.jp
>
> 「日本国内におけるPGPユーザの公開鍵交換をスムーズに行なう支援を行ないインターネットでのセキュリティ，特に日本におけるインターネットでのセキュリティに寄与するために，JPNICにてPGP Public Key Server実験運用を行なうことを提案する。」

かくしてICATからJPNICに移行する。98年に入ってからまもなくのことである。ICAT時代もネットワークのトラブルを起こしたことはないし、トラフィックもハードウェアも十分であった。

ではあるが、JPNICが提供してくれた環境は日本のインターネットの中心的なデータセンターで、さらにハードウェアはデータセンター向けの最新のハードウェアであった。日本国内で考えられる最良のネットワーク環境を提供してもらえた。

日本のインターネットの中心ともいえるネットワーク環境であり、日本国内でも最もセキュアな環境の一つである。当然、もはや筆者のような怪しい人物は近づくこともできず、pgp.nic.ad.jpの実際のハードウェアが稼働している姿を筆者は一度も拝んだことがない。

JPNICのスタッフによりお守りをされているハードウェアやネットワークは日本で最も恵まれた環境にいるといえよう。筆者は何の不安もなくPGP鍵サーバを管理すればよいのだから本当に幸せである。

さて、それ以外でPGP鍵サーバ関連で記録しておきたいトピックスは、2000年のPGP Public Keyserver Admin Meetingだろう。もしかするとちょっと名前は違ったかもしれない。世界中からPGP鍵サーバを作ったり管理している者がオランダはユトレヒトにあるSurfnetの会議室に集まり2日間ミーティングをするというものだ。といっても全世界から集めても20名前後なのだが。声がかかったので、筆者も自分の財布を叩いて飛んでいった。

今振り返るとPGP鍵サーバだけではなくPGP/GPG（GNU Privacy Guard）に関係する人間がすべて集まったという後にも先にもないミーティングになった。PGP作者Philip Zimmermann 氏、最近話題になったGPG作者Werner Koch氏、MITでサーバを書いたMarc Horwitz氏、別実装サーバの作者、ヨーロッパやアメリカの鍵管理者などが集まった。鍵管理者は大学でセキュリティを専門にしている方々で、後にアカデミックでのインターネット・セキュリティの中心的存在として活躍することになる人物が何人もいた。この時の人脈が後に筆者と佐野氏が関わっている初期のJPCERT/CCをヨーロッパで認知してもらう際に大きな役割を果たした。なお、このミーティングは色々な意味でかみ合わず、2度目は開かれなかった。

最後になるが、少し技術的なことを書き残そう。現在pgp.nic.ad.jpで動いている実装は、初期のHorowitz実装からかなりコツコツと手を入れており、特にDBまわりは分割して動かすなど、以前のコードとはがらりと変わっている。ちなみにBerkeley DB由来のSleepycat（今やOracleに買われBerkeley DBと元に名前が戻っているようだが）を使っているので大変高速である。また、Sun OS、FreeBSD、Linuxと乗り換える度に書き換えている。自分でゼロから書いた別実装のOpenPKSDのノウハウがあり、中身がわかっていて手を入れる理由もあるのだが、もうほとんど別物になっているレベルといえるかもしれない。

考えてみればPGPに関わってもう24年、PGP鍵サーバは20年経つのであるが、つい最近のような気がするのは不思議なものである。これまで本当に多くの人に支えられてここまでやってこれたのは、これまでの話でもおわかりいただけたかと思う。紙面の都合で名前をあげることができなかった方々も含め多くの支えてくれた方々に感謝する次第である。