pgp.nic.ad.jpサービスを振り返って

はじめに

OpenPGP公開鍵情報の登録・検索サービスを、2022年9月30日（金）で終了した。

PGPの公開鍵サーバーは、1998年9月中旬に認証実用化実験協議会（ICAT）の管理していたサーバーからJPNICの管理するサーバーpgp.nic.ad.jpに移行したので、かれこれ約24年間にわたりOpenPGP公開鍵情報の登録・検索サービスを提供していた。

pgp.nic.ad.jpのサービスを終了するにあたって、振り返りとして少し書き留めておきたい。

pgp.nic.ad.jpに至るまでの経過

1993年に開始されたPGP公開鍵交換のためのサーバーは、メールで登録・検索・要求を行う実装であった。1993年の年末にようやくNCSA HTTPdが現れたという時代で、Webを介しての動的なコンテンツサービスというものは存在していなかった。当時、MIT、UCSD、ハンブルグ、オックスフォードといった四つか五つぐらいの大学にあるサーバーでPGP公開鍵交換サービスが開始され、どこかに登録すると、相互に共有するという仕組みになっていた。

筆者は1994年4月11日からPGP公開鍵サーバーのサービスを開始し、世界に散らばるPGP公開鍵サーバーと相互に公開鍵を交換し共有した。運用していたサーバーは、当時筆者が所属していた株式会社SRAの研究部門の一つであった、ソフトウェア工学研究所内にあった。当時のメールでPGP公開鍵を登録したり取得したりする方法に関しては、MITのサーバーの上にテキストファイル※が残っている。1994年6月時点で筆者のサイトも含めて、世界中で14サイトがサービスしていることがわかる。

1997年当時MIT大学院生だったMarc Horowitz氏によって、TCP/IPで接続可能なPGP鍵サーバーpksd（PGP Public Keyserver）が実装された。この時に、hkp（Horowitz Keyserver Protocol）プロトコルが考案された。これによって、いわゆるインターネット接続可能なPGP公開鍵サーバーの運用が開始されるようになった。hkpプロトコルは現在も、The GNU Privacy Guardで提供されているOpenPGP仕様の暗号ツールgpgで利用可能である。

1996年7月に、PGP公開鍵サーバーをICATに移行した。このバージョンは、それまでと同様にメールによるインタフェースである。MITがHorowitz版PGP鍵サーバーpksdに移行して、しばらくしてICATもpksdに移行した。しかし、当時のpksdは、まだ初期段階で、品質は高くなく、Sunのマシン上ではコンパイルも通らないような不安定なものであった。筆者は、かなりソースコードに手を入れ、パッチを鍵サーバーのコミュニティに還元していった。

ちなみに1998年にpgp.nic.ad.jpに移行した後も、かなりソースコードに手を入れている。その結果、pgp.nic.ad.jp上で動いているpksdは、筆者が長年にわたりコードに手を入れ続けたので、オリジナルのコードからずいぶんと違うものになっている。

Web of Trust

PGPやGnuPGといった、OpenPGP仕様（rfc4880）の公開鍵暗号・電子署名ツール（以降 pgp/gpg/OpenPGP）は中心となる認証局は持たず、相互の信頼によって相手を認証する。最もプリミティブな方法は、お互いが対面で相手を確認し、その際に、相手の鍵に自分の署名を付けるというものである。

ここで一つ、非デジタル的な問題がある。ここにアリスとボブがいて、アリスであることを保証し、ボブであることを保証して、相互認証を行おうとした場合は、公的証明書を確認するなどが必要となる。1対1では行うには効率が良くない。

そこで、鍵署名パーティー（Keysigning Party）が行われるようになる。実際行われる鍵署名パーティーは、本来のセキュリティ的な価値より、集まって自己紹介する一種の親睦を深めるイベントのようなものである。初期の頃は、参加者が、お互いに身分証明書を見せ合い、自分の公開鍵のfingerprintの印刷物を渡す、あるいは読み上げるという素朴なものだった。あちこちでやり方がバラバラだったので、元々効率が悪かったものが、さらに効率が悪くなった。

そこで現れたのが、Zimmermann-Sassaman key-signing protocolである。これが生まれるきっかけとなったのが、the First PGP Keyserver Manager Symposiumでの鍵署名パーティーであった。従来の方法があまりにも効率が悪いので、PGPオリジナル作者である Philip Zimmermannが、Zimmermannとともに参加していた当時PGP社のレン・サスマンに、もっと効率の良い方法を考えるようにと指示を出した。そして、完成したのがEfficient Group Key Signing Methodであり、現在、Zimmermann-Sassaman key-signing protocolと呼ばれるものである。

なぜ、そのようなことを知っているかと言うと、そのシンポジウムに筆者も参加していたからである。各国の鍵サーバー管理者やPGPおよ

※ http://web.mit.edu/Tcl/src/exmh-1.6.1/misc/pgp-keyservers.txt

びGnuPGの関係者が、オランダはユトレヒトにあるSurfnetの会議室に集まり2日間行われた。その中で行われた鍵署名パーティーだったが、20名前後の小さな集まりで行われたにもかかわらず、Zimmermannは最後、ウンザリした顔をしていたのを今でも思い出す。さて、このようにして生まれた鍵署名パーティーであるが、今年の7月(July 24, 2022)にコソボで行われたDebConf22でも行われている。

お互い対面で確認し署名をするという方法ができない場合、「自分が既に署名している信頼のおける公開鍵から署名されている公開鍵は信頼することとする」という方式を使う。これがWeb of Trust(信頼の輪)である。この考え方は既に、1992年のPGP version 2.0に現れる。一元化された(集中型)信頼モデル(centralized trust model)としてのPKI(Public Key Infrastructure)と対比される形で、分散型信頼モデルとしてWeb of Trustは存在している。

しかし、シンプルに考えると今も昔もWeb of Trustは、「友達の友達は友達だ」というレベルである。筆者も初期の頃は、Web of Trustという方法も意味があるのではないかと考えていたが、現在では欺瞞(deception)に対して脆弱な極めて危険な方法論と考えている。1992年から2022年の現在まで使われ続けており、それによってWeb of Trustという方法が安全であるような幻想が、独り歩きしているとすら筆者は考えている。

pksd公開鍵サーバーの問題点

pgp.nic.ad.jpで可動していたpksdが作られた頃は、インターネットは性善説を前提としていていた。誰でも登録可能な公開鍵サーバーであった。今から考えれば牧歌的な時代であったと感じる。勝手に他人の公開鍵を登録することも可能である。自分の公開鍵であるにもかかわらず、一度誰かによって登録されてしまうと、たとえ一つの公開鍵サーバーから消しても、他の運用ポリシーの違う公開鍵サーバーに自動的に登録されるため、すべての公開鍵サーバーから消し去ることは実質的に不可能であった。後にいくつかのOpenPGP仕様に対応した公開鍵サーバーでは、鍵の中に有効なメールアドレスを加えていることを登録条件としているものが出てきた。

2016年に作られたGDPR(General Data Protection Regulation; EU一般データ保護規則)には、当然のこととして対応していない。公開鍵に付けられているメールアドレスや名前などは、そのままむき出しである。自らの意思で登録したならばともかく、第三者が登録しているような公開鍵に付いている個人情報に対して何もプロテクションできないし、オプトアウトも実質できないので、明らかにGDPRに抵触する。これまでの長い歴史的な経緯があり、現在も運用してるという理屈も限界であろうと筆者は考える。

理想と現実のギャップ

1992年当時に筆者が考えていたインターネットの世界は、end-to-endでデータが暗号化され、データが保護される時代が来るというものだった。確かに現在では、TLSで通信路が守られていてend-to-endで保護されているが、データそのものを暗号化するというトレンドは現れなかった。また日本においてはいわゆるPPAP問題のように、ファイルを共通鍵暗号で暗号化し、メールで送り、その後に暗号化に使った鍵をメールで送るという、誤った暗号技術の利用方法が広く使われるといった、残念な状況にまでなっている。

pgp.nic.ad.jpのトラフィックを見ても、日本国内からのアクセスは最初から最後まで低調だった。1990年代の終わり頃は、「インターネットのセキュリティは発展途上なので現状では利用はほとんどないが、あと10年もすれば個人で利用する電子メールやファイルはすべて電子署名付きでやり取りされるようになる」と考えていた。しかし、残念ながらそうはならなかったし、今後もそうはならないだろう。これはPGP/GnuPG/OpenPGPだけではなく、TLS(SSL)もそうであると言える。httpsが急激に普及したのは無料の“Let's Encrypt”が普及したためであり、それまでのように高価な“SSL証明書”を販売していたのではそうはならなかった。では有料と無料の価値がどれだけ違うかと言えば、米国防総省の情報機関NSAの公式WebサイトはLet's Encryptの証明書を利用していると言えばわかってもらえるだろうか。少なくとも、PGP/GnuPG/OpenPGPに限らず公開鍵暗号の個人利用に関しては、現状のアプローチでは利用は広まらないであろう。

現在、PGP/GnuPG/OpenPGPで利用可能な公開鍵サーバーをいくつか挙げておく。

```
keys.openpgp.org
keyserver.ubuntu.com
pgpkeys.eu
```

公開鍵サーバーの代替案として

Web of Trustは信頼するのに十分ではないと説明したが、信頼できるツリー方式というのは十分に考えられる。例えば組織のCA局(Certificate Authorityという言い方は不適切かもしれないが、他に思い付く言葉がないのでここではCAと呼ぶ)にあたるOpenPGP署名用公開鍵をDNSの専用領域に用意しておき、それを使うという方法である。RFC4398ではThe CERT resource record(RR)という形で規定されており、またgpgでは、RRの公開鍵を利用できるようになっている。組織の中で利用する公開鍵は、そのCA(マスター鍵)によって署名を付けてもらう。これで公開鍵の信頼度は、その組織のDNS管理の信頼度に近似できる。組織内のメンバーで利用する際は、同じ信頼度である。pgp/gpg/OpenPGPでは、複数のCA局からの一つの公開鍵に署名を付けることができる。信頼できるCA局(一つまたは複数)の署名が付けられている時、そのCA局が保証している範囲の信頼度で利用することが可能となる。

近年では、個人のブログやgithubでリポジトリを利用している場合も多い。Webページはもちろんのこと、例えばgithubのリポジトリにAscii Armorフォーマットの公開鍵のファイルを置いておくなどが

個人でもできる。例えば、筆者がpublickeysというリポジトリを作成し、その下にpublic.ascというOpenPGPフォーマットの公開鍵ファイルを置いておくとする。この場合、次のようにしてダウンロードしてインポートすることが可能である。このように、リポジトリに公開鍵（署名）を含めておくと、以降、作者からのメッセージとして署名を使うことができる。

```
curl -s https://raw.githubusercontent.com/
SUZUKI-HIRONOBU/publickeys/main/public.asc |
gpg --import
```

この場合、信頼の起点はgithubである。最初に得たものを信じて使うというTOFU（Trust on First Use）の亜流ではあるが、既に活動実績のあるリポジトリで、githubのセキュリティレベルで管理されている点が大きく違う。しかし、これも、これまでyumやaptといったGNU/Linuxのシステムメンテナンスのツール群も、ダウンロードサーバー上に置かれている公開鍵をcurlによってダウンロードし、システムに設定するという方法を使っているので、それを個人ベースに置き換えていると言っても差し支えないであろう。

まとめ

pgp.nic.ad.jpを終了するにあたり、公開鍵サーバーとは何だったのかを振り返ってみた。システムの安全性を確保するためにpgp/gpg/OpenPGPの技術はシステムに組み込まれ広く使われたが、個人ベースの利用は過去も現在も極めて限られている。公開鍵サーバーを経由して個々のユーザーが公開鍵を交換するというモデルは、この30年近い運用をしたものの、現実のニーズに即してはいなかったと言える。システムに組み込まれたpgp/gpg/OpenPGPは広く使われるようになり、一部でPPAP問題のような状況が出てきたにしろ、暗号技術による安全性の確保というのは必須の技術となった。その点は大変良かったと感じる。筆者の目から見たざっくりとした振り返りであるが、何かの役に立てば幸いである。

（元pgp.nic.ad.jp管理者 鈴木裕信）

INFORMATION　国際会議開催のお知らせ

IETFミーティングが7年ぶりに日本にやってきます！

IETF Meetings 2023 3.25 SAT → 31 FRI

第116回IETFミーティングが2023年3月25日（土）～31日（金）の日程で、WIDEプロジェクトのホストにより横浜で開催されることになりました。日本でのIETFミーティング開催は、第54回（2002年、横浜）、第76回（2009年、広島）、第94回（2015年、横浜）に続いて4回目となります。

IETFとは？

IETFは、インターネット技術の標準化を推進するグループで、メーリングリストと年に3回行われるミーティングを通じて、インターネットに関わる標準の文書であるRFC（Request For Comments）を策定しています。IETFにおける技術標準化の議論はワーキンググループ（WG）を単位にして推進されていて、ミーティングやメーリングリストでの議論には誰でも自由に参加することができます。

IETFにおける技術仕様の策定は、ラフコンセンサス（Rough Consensus）とランニングコード（Running Code）を重視しているのが特徴で、まずラフな仕様を作成し、それから相互接続実験や実運用を通じて、工夫、改善を加えながら詳細な仕様を実装していくという、非常に柔軟な仕様策定プロセスとなっています。

最近ではリモート参加という方法もありますが、今回の日本開催は技術標準を議論する場に直接入っていき、多くの技術者と直接話しができる貴重な機会です。会場など詳細が決まりましたらJPNICのWebなどであらためてお知らせしますので、ぜひ多くの皆さまのご参加をお待ちしています。

IETF 116 Yokohama
https://www.ietf.org/how/meetings/116/