

次世代 OpenPGP Public Keyserver (OpenPKSD)

OpenPKSD プロジェクト

鈴木裕信

本ドキュメントは平成 13 年度年次総括報告書として IPA に提出したものです

概要

インターネット上で最も利用されている暗号技術は OpenPGP(RFC2440[RFC2440])である。OpenPGP の公開鍵インフラ(PKI)に使われているサーバソフトが PGP Public Keyserver である。運用は世界各地の鍵管理者コミュニティのボランティアによって支えられており、インターネットセキュリティの向上に貢献している。現状で稼働中の PGP Public Keyserver は最新の OpenPGP 規格をサポートできていない。また超大規模な公開鍵データベースとしては処理効率や管理運用面では大きな問題をもっている。新たな PGP Public Keyserver の開発は鍵管理者コミュニティにおいての緊急の課題となっている。そこで根本から設計を見直した上で次世代 OpenPGP Public Keyserver を作成する。最終的には現在世界各地で運用している PGP Public Keyserver を置き換えることを目標・目的とする。

1. はじめに

1.1 PGP Public Keyserver とは

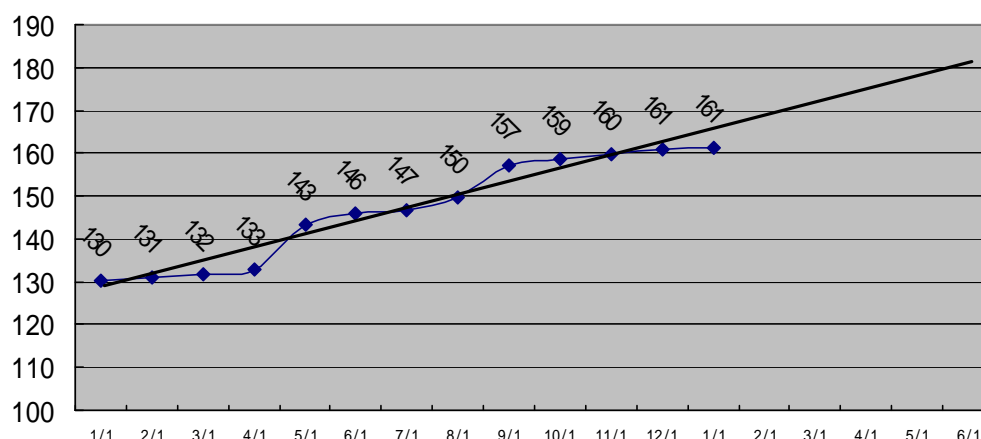
PGP Public Keyserver とはインターネット上で広く公開されている OpenPGP 仕様の公開鍵パケットの登録および検索サービスのことである。現在、PGP Public Keyserver として広く使われているソフトウェアは Marc Horowitz が作成した pksd[MARC]である。

1.2 背景

日本で最初の PGP Public Keyserver のサービスは 1994 年 4 月 11 日に筆者が開始した [ICAT]。ここでの開始とは世界中に分散する PGP Public Keyserver と公開鍵の同期を開始した日である。同期先は MIT の鍵サーバであった。ここから現在の pgp.nic.ad.jp までの 8 年間、日本においてサービスを提供してきた。登録されている公開鍵数であるが、1997 年 12 月 26 日時点では約 5 万 5000 鍵 (pgp.icat.or.jp) であったものが 2002 年 1 月 7 日では約 159 万 5300 鍵 (pgp.nic.ad.jp) へと飛躍的に伸びている。

PGP Public Keyserver は過去 8 年間のあいだボランティアの手により支えられ続けている。世界各地に散らばる鍵サーバ管理者数名からなるコミュニティが中心となり各々の持つ鍵サーバ同士を同期させる形でシステムの冗長性を持たせている。また同時にどこでも同じサービスを提供できるようにしている。

登録鍵数は日々増加している。pki.surfnet.nl の鍵サーバ管理者 Teun Nijssen からのメール[TEUN]によれば昨年 1 年間で約 31 万鍵増えた。この増加率だと 2002 年 6 月には 180 万鍵程度になると思われる。



pki.surfnet.nl の 1 年間の増加推移：単位は万

現在、多くのサイトで運用しているのは Marc 版 pksd であるが、この鍵サーバは数百万という単位の公開鍵をサポートすることは考慮していなかった。非常に良いデザインのため現在はまだ登録、検索に関しては破綻していない。DB として Berkeley DB [SLEEPYCAT] をプログラム内に組み込み利用しているので検索に関しては現在でも十分に高速である。

一方で大規模データベース運用としてのメンテナンス性は、あまり良くはない。最も困るのはデータベースを運用しながら、並行してバックアップを取るといった機能がない点である。これはデータベースシステムと鍵を検索/登録するサーバプログラムが独立していないためである。

また Marc 版 pksd には、このプログラムがリリースされて以降に OpenPGP (PGP) に加わったパケットフォーマットはサポートしていないという問題があった。

本格的な DB エンジンを利用し大量の鍵を扱い、普通の DB ベース運用のような管理でき、最新の OpenPGP のパケットフォーマット

をサポートするようなプログラムが必要とされていた。

1.3 期待される効果

期待される効果以下の通りである。

- (1) OpenPGP(GnuPG や PGP)を用いた安全な通信のための公開鍵インフラの再構築と世界規模でのサポート
- (2) それによる一般ユーザのインターネットセキュリティの健全な発展を促進
- (3) 大規模、高負荷、高信頼性ソフトウェアを完全に公開することによるテクノロジー転スファアとその波及効果
- (4) 緩やかに結びついている広域分散データベースでのコンテンツ同期のメカニズムの開発とその技術の公開によるテクノロジー転スファアと波及効果
- (5) 全世界のフリーソフトウェア・コミュニティへのエンカレッジとコントリビューション

2. 開発の目標と内容

本テーマにおける開発の目標と内容は以下の項目である。

- 大規模、高負荷耐性、高信頼性に優れた鍵データベース
- OpenPGP(RFC2440)仕様の鍵パケットのサポート
- 世界各地に分散するサーバ間で鍵データベースのコンテンツの同期
- GPL ライセンスの下で公開・配布
- 現在の PGP Public Keyserver の置き換え

2.1 大規模、高負荷耐性、高信頼性に優れた鍵データベース

現時点では運用が面倒だとはいえ Marc 版 pksd でも十分に利用できている。しかし、既に Marc 版 pksd がデザインされた時とは規模が違っている。このままでは日々増え続ける鍵を管理しきれなくなる日がくるだろう。ここで必要なのは、そのような事態が現実になるのか、あるいはいつなのかという議論ではない。ユーザの観点から何が重要かという議論である。ユーザから見れば将来へのロードマップを示せないシステムなど信頼はしないであろう。その上で技術面からも実用的な「大規模でも大丈夫」「高負荷でも大丈夫」「高い信頼性」を示さなければならない。

PGP Public Keyserver はネットワークでアクセスされるデータベースの一種である。ソフトウェアの面から大規模化、高負荷耐性、高信頼性を考えた場合、以下のテクニックがあげられる。

(1) クラスタ化されたデータベース

(2) アクセス負荷分散

(3) データベースのノンストップ運用 / 高速なリストア

本年度は(1)を実現するためにデータベースクラスタ化の調査[WANG]を行なった。来年度はその調査を元にクラスタ化を行なう。目標は1億鍵の登録とその状態での頻繁な検索である。もちろん通常はクラスタ化した形で PGP Public Keyserver が利用されるとは考えていない。しかし柔軟なクラスタ化が可能であることを示すことは重要である。将来、想像を超える増加があっても対応できるという潜在的能力を示すことができるからである。(2)は PGP Public Keyserver が PGP や GPG といった暗号ツールとやり取りする時の hkp (Horowitz Key Protocol)は HTML ベースである点に着目した。この特徴を活かし http ロードバランサー[JSERV] と同じアプローチでの負荷分散が可能であると思われる。来年度はロードバランサー機能をサーバに加える予定である。(3)を実現するためにデータベース PostgreSQL[POST] を採用した。PostgreSQL は使いやすく、PC サーバ上では商用 DB 以上の性能を持ち、商用 DB が持つような機能のほとんどを備えている。またデータベースを止めることなく、データ - のバックアップが可能である。Vaccum と呼ばれるデータベース内容の“掃除”もできる。商用 DB には見られない PostgreSQL 独自の高速リストア機能はハードウェアをリプレースする時に有用である。

2.2 OpenPGP(RFC2440)仕様の鍵パケットのサポート

過去の pksd のコードを流用することなく

openpkgsd プログラムを Ruby[RUBY]で書くので、OpenPGP(RFC2440)仕様の鍵パケットのサポートではなく、OpenPGP(RFC2440)仕様の鍵パケットをターゲットに作成したと表現するのが正しいかと思われる。Ruby はオブジェクト指向なので、プログラム内部では個々の鍵のパケットをインスタンスとして表現している。そのインスタンス自分自身の振舞(メソッド)を知っている。オブジェクト指向言語を使ったことでプログラム中での鍵の扱いが扱いが楽であった。

2.3 世界各地に分散するサーバ間で鍵データベースのコンテンツの同期

登録数が 150 万鍵を超える鍵サーバが、各々自立的に稼働しており、1 つのサイト上で鍵が更新されると同期している他のサイトの鍵サーバが更新される。pgp.nic.ad.jp では 2001 年 1 月 7 日 ~ 2002 年 1 月 7 日までの間に鍵の更新同期が 826321 回発生し、新たに約 31 万の公開鍵が追加された[NIC]。

現在の方法は一方向へ鍵が送られる方法である。実際の運用では相手の鍵サーバが止まっていて更新する鍵が送れない、逆に自分の鍵サーバが止まっていて受け取れないなどがある。しかし、下記データを見る限り、特に鍵サーバが停止していないのにも関わらず多くの鍵の違いが発生しているようである(原因不明)。

各鍵サーバの保持している公開鍵		
鍵数	サーバ名	計測日
1595374	pgp.nic.ad.jp	(2002/1/23)
1605783	pgp.rediris.es	(2002/1/25) [FRAN]
1614164	pki.surfnet.nl	(2002/1/02) [TEUN]
1623342	cc.gatech.edu	(2002/2/01) [PETER]

そこで同期する相手サイトと自分が何を持っていて、何を持っていないのかを知り、必要な鍵を相手から取り寄せる ihave/sendme [RFC850]のような機能が必要になってくる。本年度はネットワーク上の 2 つのサイトにあるデータベースから違いを見つけるアルゴリズムには、どのようなものを使うのがよいかを検討した。

1 つは計算量、もう 1 つはデータ転送量という観点から見た場合、常に有利なアルゴリズムは見つからなかった。大量にデータが違う場合極めて少量のデータが違う場合の 2 つのアルゴリズムを検討した[KNUTH]。ハードウェア故障などにより数日停止した場合と、毎日定期的にチェックする場合を想定し、条件に応じて使い分けを行なう方針である。予備的な実験では Linux 2.4、Althron 1GHz[ATHLON]、Mem 1GB 上で 100 万鍵分の鍵 ID を扱った場合、前者は最良約 70 秒/最悪約 90 秒、後者は内容にまったく違いがない場合は約 0.2 秒異なる鍵の数対し平均 2 乗のオーダー程度の速度低下となった。来年度はもう少しアルゴリズムの検討を詰めてみながら openpkgsd に組み込む予定である。

3. 本年度の活動状況

本年度の活動は OpenPGP(RFC2440)パケットが扱える Marc 版 pkgsd コンパチブルなサーバを作り Web サーバで公開すること、それに関連した OpenPGP の利用方法などの情報を公開すること、来年度にむけてクラスタ化のための調査を行なうこと、正しく同期するためのアルゴリズムの調査を行なうことであった。

これらの成果を公開するためにドメイン

openpkd.org [OPENPKSD] を取得しサーバを運用し始めた。一般の公開は 2001 年 12 月からである。関連するドキュメントやソースコードは GPL ライセンスの形で、hkp プロトコルでアクセスできる鍵サーバのサービス、および Webサーバ経由でのアクセスサービスを openpkd.org でサービスしている。

openpkd 上のな公開物(2002/02)

内容	作者	書類
About development	H. SUZUKI	pdf
Loadmap of this project	H. SUZUKI	pdf
Overview of this project	H. SUZUKI	pdf
What is OpenPGP	H. SUZUKI	pdf
Compatibikity between OpenPGP tools	Iwate-pu Univ.	html pdf
About OpenPGP and PKI	Iwate-pu Univ.	html pdf
How to Use OpenPGP Plug-in	Iwate-pu Univ.	html
Applied OpenPGP	Iwate-pu Univ.	html
PostgreSQL and Cluster	Iwate-pu Univ.	pdf
Sync algorithm between two keyserver	Osaka-city Univ. H. SUZUKI	html
Keyserver link list	H. SUZUKI	html
Keyserver Web Interface	H. SUZUKI	html cgi-bin
Openpkd dist package	H. SUZUKI	tar.gz
Openpkd Aux package	H. SUZUKI	tar.gz

4. 成果物

IPA に対する本年度の納品物件は以下の通り。

開発成果報告書	1 式
ソースプログラム	1 式
ロードモジュール	1 式
調査報告書	1 式

本ソフトウェアはフリーソフトウェアとして GNU General Public License を取り入れているためにソースコードとバイナリ実行形式を区別せずアーカイブしている。形式上ソースプログラムとロードモジュールの 2 つを用意して納品としているが、両方に同じものを入れている。尚、ソースコードは頻繁に更

新が行なわれているので、もし、利用したい場合は、直接 <http://openpkd.org> から最新版をダウンロードすることを勧める。

5. 今後の課題

鍵サーバがたとえ Yahoo や eBay のような人気サイトになってアクセスが激増したとしても処理できる見通しはついた。

今後は故意の利用妨害(DoS)に対する耐性を高めなければいけないだろう。尋常ではない頻度で繰り返しアクセスしてくるアドレスを規制したり、流量をチョークしたりといった対応などが考えられる。現在の鍵サーバにはアクセスコントロールは存在しない。あるいは Trust ユーザのみが鍵を更新/参照できるといったサービス。大量の公開鍵がデータベース化しているので、ある公開鍵がどの程度信頼できるものかといった評価などのサービスも考えられる。

6. まとめ

インターネット上での暗号セキュリティツールの主役は PGP であり GNUPG である。openpkd はあくまでも裏方のインフラを受け持つ。今回のプロジェクトは長年使われているインフラの改良と整備というブラクティカルな活動だと位置付けることができるだろう。

pkd の後継としての地位を築いたとしても、openpkd のソフトウェアをインストールするサイトは全世界で 100 サイト以下であろう。ただし openpkd のサービスを利用する者は登録鍵のオーダー、つまり 100 万単位の利用者ということになる。運用側としては、やはり長期に安定して使えるプラットフォームをユーザにいか提供するかが課題となる。

それを提供するの openpkd の役目である。

openpkd の本来の全体像を完成するまで達してはいないが、このまま順調に開発が進めば Marc 版 pksd と世代交替できる可能性は高まるだろう。

7. 関連資料

[RFC2440]

<http://www.ietf.org/rfc/rfc2440.txt>

[MARC]

<http://www.mit.edu/people/marc/pks/>

[ICAT]

http://pgp.nic.ad.jp/docs/icat_rep_1.txt

[TEUN] Teun Nijssen Teun.Nijssen@kub.nl

との私的メール交換 (2002/1/27)

[SLEEPYCAT]

<http://www.sleepycat.com/>

[WAN]

<http://openpkd.org/docs/report2001/PGP-005/PostgreSQLandCluster.pdf>

[JSERV]

<http://www.clab.kwansei.ac.jp/manual/jserv/howto.load-balancing.html>

[POST]

<http://www.postgresql.org/>

[RUBY]

<http://www.ruby-lang.org/en/index.html>

[NIC]

<http://pgp.nic.ad.jp/docs/2001.txt>

[FRAN] Francisco Jesus Monserrat Coll

francisco.monserrat@rediris.es との私的メール交換 (2002/1/29)

[PETER] Peter N. Wan

Peter.Wan@cc.gatech.edu との私的メール交換 (2002/2/3)

[RFC850]

<http://www.ietf.org/rfc/rfc850.txt>

[KNUTH] Donald, E. Knuth, "The Art of Computer Programming", 2nd ed, vol 3, 1997.

[ATHLON]

http://www.amd.com/us-en/Corporate/VirtualPressRoom/0,,51_104_572_863^2003~10639,00.html

[OPENPKSD]

<http://openpkd.org>

Acknowledgement

OpenPGP 及び関連ツール等に関する調査およびドキュメント等は岩手県立大学ソフトウェア情報学部村山優子を中心とした PGP-folk のメンバーである山根信二、王家宏、権藤広海、間宮章彦、荒川健介、市川快らによって行われた。加えて秋山和隆、手塚一郎の協力があった。同期アルゴリズム等は大阪市立大学学術情報総合センター中野秀男を中心とした大西克実、石橋勇人らとのメーリングリストでのディスカッションをベースにまとめたものである。PGP Public Keyserver の情報を調べるに当たり Peter N. Wan (ジョージア州工科大学)、Francisco Jesus Monserrat Coll (RedIRIS)、Teun Nijssen (Surfnet) の協力があった。OpenPKSD プロジェクトには SRA-KTL 馬場尚子、榎田義一が参加した。(文中敬称略)