JPNIC PGP公開鍵サーバー実験タスクフォース：すずきひろのぶ hironobu@h2np.suginami.tokyo.jp

JPNIC通信

26

PGP公開鍵サーバーの実験運用開始について

JPNICでは1998年6月1日より、PGP公開鍵サーバーであるPGP PUBLIC KEYSERVERの運用実験を開始しました。今回はPGPの概要および公開鍵サーバーの現状について解説します。

PGP PUBLIC KEYSERVER

PGP.NIC.AD.JP[❷]でサービスを開始したPGP PUBLIC KEYSERVERは、暗号ツールであるPGPの公開鍵をユーザー間で交換するためのサーバーです。

PGPはPhilip Zimmermann氏が作成した汎用の暗号ツールです。暗号機能として、公開鍵暗号、秘密鍵暗号、電子署名などの便利な機能を用意しています。そのため、PGPはインターネット上で安全な情報交換を行うツールとしてすでに多くの人に使われています。

PGPに関係するRFCとしては、RFC1991やRFC2015などがあります。現在は、PGPの仕様をRFC化するためにIETFの分科会で活動が行われています。これはOpenPGPという名称で呼ばれ、細かい仕様の規格化作業が行われています。

PGPには現在、ネットワークアソシエイツ社（旧PGP社）から商用の製品として出荷されている米国版および国際版、また、フリーソフトウェアとして配布されている米国版および国際版の合計4つのバージョンがあります。これらは配布元が異なるだけで、使用しているソースコードは同一のものとなっています。

PGP PUBLIC KEYSERVERの位置付け

PGP PUBLIC KEYSERVERの目的は、ユーザーが公開鍵を交換する中継点として利用することであり、その公開鍵が本当に正しい公開鍵であることを保証しているわけではありません。公開鍵をプールしているだけなので、相手の公開鍵が正しいかどうかは自分で判断する必要があります。

PGP PUBLIC KEYSERVERは、世界各地でボランティアによって運営されていて、主要なサーバーは10か所程度あり、全体の総数は、現在20から30サイト程度と考えられています。

サーバーは同期メカニズムを持っており、世界各地に散らばるサーバー間で同期をとっています。したがって、ユーザーが世界中のどこかの公開鍵サーバーに新規に公開鍵を登録すれば、その公開鍵は自動的に世界中のすべての公開鍵サーバーに反映されます。

JPNICのサーバーは、運用実験という形で世界中のボランティアと協力し、世界中を網羅するPGPの鍵交換インフラの一部として存在しています。

サービス内容

PGP.NIC.AD.JPはMITのMarc Horowiz氏が開発中の公開鍵サーバーシステムpks（7月1日現在、バージョンはpks-0.9.3db2test）を使用し、以下のサービスを提供しています。

●WWWページからの登録と検索

URL http://pgp.nic.ad.jp/

●hkp[❷]でのアクセス

URL http://pgp.nic.ad.jp:11371

PGP PUBLIC KEYSERVERの規模

PGP.NIC.AD.JPが保持している公開鍵数は約8万から9万です。規模としては中規模なサーバーにあたります。

海外のサーバーとの間で行われるトランザクションは、平均して毎日2000から8000トランザクション程度発生しています。多い時は、1日に10000トランザクションを超えることがあります。

現在、同期を取っている海外のサーバーは以下のとおりです。

●オランダ SURFnet：国際フリー版デフォルト参照サイト

●ドイツ PCA-DFN：ドイツ学術ネットワーク認証実験プロジェクト

●アメリカ MIT：米国フリー版デフォルト参照サイト

●ポーランド ICM：大学

●アメリカ FRB：連邦準備制度理事会

参考資料

【❶】PGP公開鍵サーバの実験運用開始について
http://www.nic.ad.jp/topics/archive/1998060101.html

【❷】APNIC-063
hkpはPGP 5.0以上で実装されているプロトコルで、直接PGPのプログラムがサーバーに鍵を問い合わせる機能。

PGP公開鍵サーバーに関する問い合わせ先
E-mail：pgp-query@nic.ad.jp

JPNICダイジェスト　JPNICで公開する文書を告知いたします。
1998年6月 http://www.nic.ad.jp/topics/old/199806.html

公開日	タイトル	公開日	タイトル
1998/6/1	PGP公開鍵サーバの実験運用について	1998/6/2	Internet Week 97の資料販売・レクチャーノート公開について
1998/6/12	「学校ドメイン名」の御意見募集の結果について	1998/6/15	ED.JPドメイン名新設の提案