

A Short History of the GNU Privacy Guard (日本語翻訳版)

最初のバージョンの GNU Privacy Guard¹ がリリースされてから 10 年たちました。この最初のバージョンは GnuPG とは呼ばれず、g10 と呼ばれ、これはドイツの憲法の通信の自由を定義する第十項 (Grundgesetz Artikel 10) 及び、シークレットサービスがこの憲法をすり抜けることができる、G-10 法に対する語呂合わせとして命名しました。最初のバージョン 0.0.0 は 1997 年 12 月 20 日² に公開され、これはぎりぎり RSA や IDEA の特許で保護されたアルゴリズムを使用せず、Elgamal 及び Blowfish を使用した PGP との互換性を持ったぎりぎり動作するものでした。これはテスト版としてマークされており、現在 GnuPG で見られるほとんどの機能を含んでいませんでした。データのフォーマットは OpenPGP と互換性を持っておらず、より PGP 2 のフォーマットに近く、いくつかの拡張 (データのストリームを可能にするなど) を含んでいました。OpenPGP 作業会は 1997 年の秋に設立されており、その存在を知ったのは私が g10 を作成するにあたり、当時すでに存在していたドラフトを参考にするには遅すぎました。著作権の問題から、PGP-5 が使用するフォーマットをリバースエンジニアすることができなかつたので、OpenPGP 作業会は必要とされていたものが必要なタイミングに設立されたものでした。

GnuPG について語る前に数年、時間を遡ってみましょう。1991 年に政治活動家であった Phil Zimmermann が Pretty Good Privacy (PGP) と呼ばれるソフトウェアを公開しました。PGP は簡単に使え、さらにバックドアが存在せず、ソースコード公開された暗号化ツールでした。PGP は暗号手法的に強力であり、pretty good (訳注: 「けっこう優れた」) 以上のものでしたが、初期的にはいくつかのバグがあり、自家製の暗号化アルゴリズムでした。ソースコードが公開されていたことで、コミュニティーのハッカー (Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, 他) などがこれらを修正し、信頼できるバージョン 2 をリリースしました。

この直後に問題が発生しました。ほとんどの国で暗号化のデバイスやソフトウェアの使用や輸出が強力に制限されていたように、米国においても例外ではありませんでした。一般的には弱い暗号しか認められていませんでした。PGP は非常に強力であり、また Usenet や FTP、BBS などで公開されたために、他国でも事故的に漏れることとなり、Phil はライセンスなしの軍需品輸出のため、起訴されました。これらの輸出管理はソフトウェアの時代に追従したのではなく、印刷したソフトウェア形態は規制がないという滑稽な効果を生み出しました。MIT Press は PGP のソースコードを本で出版し、米国外でこれをスキャンし、PGP-2i (i は international の意) のベースとなりました。これは広く使われることになりました。

1996 年に Phil に対する犯罪捜査は終了し、彼は PGP-5 を書くため、PGP Inc を設立しました。最初の公開版は 1997 年の春にリリースされました。同年の 8 月に、Munich で開かれた第 39 回 IETF 会議において Phil Zimmermann と Jon Callas が IETF に対して PGP-5 で使用されているプロトコルを標準として発行する作業会の設立を要請しました。この大きな目的は、強力な暗号を広めるとともに、新しい会社が PGP の販売、サポートを停止した場合においてもそれを保てる

1 <http://www.gnupg.org>

2 <ftp://ftp.gnupg.org/gcrypt/historic/g10-0.0.0.tar.gz>

ように、ということでした。現にその数ヶ月後に、PGP Inc は Network Associate により買収され、2002 年に PGP のサポートと開発が停止されました。(ただし、その後、PGP の製品は PGP Corporation により継続されることになります。)

PGP はフリーソフトウェアとは言われていましたが、それはそのために要求される項目を満たしたものではありませんでした。PGP-5 はれっきとした私有のソフトウェアでした。ソースコードが公開されていることだけではフリーとは呼べません。PGP-2 は商用利用に一定の制限があり³、これによってもフリーではありませんでした。他の問題として、PGP-2 は特許が存在する RSA と IDEA アルゴリズムの使用を強制するものでした。RSA の特許は米国内でのみ有効でしたが、IDEA は多くの国でまだ有効⁴なものとなっています。

GNU プロジェクトでは PGP の互換実装の必要性が数年に渡ってリストされていましたが、全ての公開鍵暗号のアルゴリズムが有効である限り、それを実装開始することは不可能でした。これは、基本的な公開鍵暗号の特許 (Diffie-Hellman 米国特許 4200770) が 1997 年 4 月に、そしてさらに広義な Hellman-Merkle 特許 (4218582) が期限切れになった時に変わりました。

その次の月に Aachen で開催された Individual-Network Betriebstagung (訳注: 独立ネットワーク年次会)⁵において BoF セッションにおいて、Richard Stallman がヨーロッパのハッカーに公開鍵ソフトウェアを実装して欲しいと要請しました。米国の武器売買法において GNU プロジェクトがそのようなソフトウェアを米国民が他国で行ったとしても実装することができませんでした。そのため、ユニークな立場にいる、ヨーロッパのハッカーに対し GNU が暗号ソフトウェアを取りそろえるのを手伝って欲しいと頼んだわけです。

SMGL の変換ソフトウェアを書くのにつかれ、おもしろいプロジェクトがなかった私は、PGP-2 のパースングコードを RFC-1991 と pgformat.txt ファイルを参考にしてハックしていました。これは簡単なものでしたので、私はさらに続け、PGP-2 のデータを復号し、作成するコードを仕上げることに成功しました。GNU に PGP の互換実装を行うことを伝えた後、私はその年の残りを IDEA を Blowfish、RSA を Elgamal に変更した上、ストリーム暗号やその他の鍵管理を加え、コードを整理するのに費やしました。

当時、PSST と呼ばれる、Secure Shell のフリーなバージョン(その後 LSH として知られる)の計画があり、それなりの人数がいるメーリングリストがあり、これは Martin Hamilton により管理されていました。Martin は寛大に g10 のためのメーリングリストを設置してくれ、その旨をその (PSST の) リストでアナウンスしてくれました。これにより最初のメンバーが加入しました。その後、私は最初の tarball を作成し、ドイツの UNIX ユーザーグループの FTP サーバである ftp.guug.de にいれ、その旨をアナウンスしました。⁶

3 pgpdoc2.txt より: 「PGP を商業製品に変え、お金を儲けたい場合、私も儲ける方法に合意しないといけません。[...] PGP はこの PGP ユーザーガイドを含む、PGP のドキュメンテーションなしに配布することができません。

4 「有効」は特許保持者がそれを行行使することであり、私はソフトウェア特許が有効なコンセプトであるとは考えていません。詳しくは <http://www.fsfeurope.org/projects/swpat/background.en.html>

5 <http://www.dascon.de/IN-BT97/programm.html>

6 <http://lists.gnupg.org/pipermail/gnupg-devel/1997-December/014131.html> 12 月に特許に関するいくつかのメールがあります。

その次の日に Peter Gutmann は /dev/random が存在しないシステム向けに、乱数コードを提供することを申し入れてきました。これにより GnuPG を多数のプラットフォームに提供することを可能とすることになりました。その後、二ヶ月間はコードの更新及び、名称をどうするべきかということについて長い議論が交わされ、最終的には Anand Kumria の提案による GnuPG に決定し、2月24日⁷にその名称 (gnupg-0.2.8) が使用されることになりました。その数日後に、Windows における試験的なバージョンが公開されました。(このリリースは、Alpha システムにおけるアライメントの問題によりログが蓄積大量に蓄積し、管理者に本当にこれをバックアップする必要があるのか、と聞かれる問題もまた解消しました。;-)

1998年7月にある程度の OpenPGP の準拠した草案がリリースされました。Matthew Skala は新規にクリーンに仕上げた Twofish コードを提供しました。(当時、Twofish は AES の有力な候補であり、Schneier により Blowfish の代わりとしての実装を推奨されましたが、リフェレンスコードに関して著作権の懸念がありました。) Michael Roth は Triple-DES 実装を提供し、その年の後半に、OpenPGP アルゴリズムの要件を満たしたものになりました。その次の年には一般的な問題が解消され、機能について議論され、それぞれの作者により他のソフトウェアよりの gpg のサポートや互換性が発表されました。

最終的に、1999年の9月7日、1.0.0 が公開され、これには Mike Ashley による GNU Privacy Handbook⁸ が含まれていました。その一年後の9月20日に RSA 特許が切れる予定でしたが、その3週間前に特許保持者はそれをパブリックドメインとしたため、9月18日には RSA サポートを含んだ 1.0.3 を公開することができました。暗号使用の大きな障害がまた一つ解消されたのです。(それは、かなり遅すぎました、もちろん)

また、同1999年にドイツの政府は強力な暗号は規制されず、誰でも使うことを推奨する判断を下します。これを公的にサポートするために、財務省は GnuPG を Microsoft Windows に移植するための資金提供⁹を行いました。米国はそれに対して良く思わなく、規制なしに暗号のソフトウェアが配布されることに関してドイツ政府に考え直す働きかけ¹⁰を試行しました。これはうまくいかず、やがて米国もその輸出ルールを緩和するしかありませんでした。

GnuPG は現在もヨーロッパにあるサーバ上で開発されていますが、この新しい米国の輸出規制により、米国内のハッカーが GnuPG の開発に寄与できるようになりました。2001年に David Shaw がプロジェクトに参加し、それから現在に至るまでもっともアクティブな GnuPG ハッカー及び共同管理者となっています。

GnuPG が楽しいプロジェクトとして管理できる時は遠い過去のこととなり、私は現在、ほとんどのプロフェッショナルとして、GnuPG の管理や拡張を生業としています。2001年に私は GnuPG やその関連ソフトウェアの開発やサポート業務を行うフリーソフトウェア会社、g10 Code を設立しました。そのもっともよく知られたプロジェクトは恐らく、GnuPG-2 で、NewPG として Aegypten プロ

7 <http://lists.gnupg.org/pipermail/gnupg-devel/1998-February/014208.html>

8 <http://lists.gnupg.org/pipermail/gnupg-announce/1999q3/000037.html>

9 <http://partners.nytimes.com/library/tech/99/11/cyber/articles/19encrypt.html>

10 <http://www.heise.de/tp/r4/artikel/5/5124/1.html>

プロジェクトの広義としてスタートしました。Aegypten のメインの目標として、よく知られた中では KMail などの他のメールクライアントにクリーンに統合できる、S/MIME の GNU/Linux 上での実装でした。2004 年よりアクティブに使用されていましたが、2.0.0 のリリースはわずか一年前でした。

X.509/CMS (一般的には S/MIME として知られる) ソフトウェアを書くのはエレガントで相互互換性のある OpenPGP を書くのに比べてあまりおもしろいものではありませんでした。これをマスターした後、他の S/MIME 実装とうまく機能するソフトウェアを書くのに成功しました。また私は、最近の POSIX プラットフォームが必要であるとの意見とは違い、GnuPG-2 を Windows に移植することも可能であることがわかりました。この開発によりフリーソフトウェアをビジネスとして開発するのは実行可能であるを見せるものとなりました。

新しいツールにより、またユーザの目から見ると S/MIME と OpenPGP はそんなに差がないように見えるようになります。ただ、今日 RSA のヨーロッパカンファレンスにおける簡単な人気投票により、OpenPGP は世界でもっとも広く使われている暗号プロトコルということが公表された時にはスマイルせずにはいらませんでした。

GnuPG は一つのツールにしか過ぎないということを思い出してください。他にもプライバシーの問題を解決するためのツールが多数公開されています。長年プライバシーツールを書き、公開している皆さんに賛辞を述べたいと思います。ハッピーハッキング!

Werner