OpenPGP と PKI

COMM Internal Note 007 / PGP–001

山根 信二
岩手県立大学ソフトウェア情報学部

村山 優子
岩手県立大学ソフトウェア情報学部*

平成 14 年 2 月 13 日

全体の構成

本章とそれに続く章では，以下の調査報告を行なう．

PGP–001 OpenPGP と PKI

PGP–002 Windows, Macintosh での PGP/OpenPGP メール

PGP–003 OpenPGP とその応用 (ネットワーク篇)

PGP–004 OpenPGP 準拠ツールの互換性

付録 PGP/GnuPG のインストール方法とコマンドライン版の使用上の注意

*本レポートは OpenPKSD プロジェクトの一環として作成された．

1 はじめに

1.1 本章の目的: OpenPGP と PKI

本章では，OpenPGP をインターネットの認証基盤としての視点から考察する．まず最初に PGP および GnuPG それぞれについての説明を行なった後，X.509 に代表される従来の PKI との比較検討を加え，最後に OpenPGP 鍵サーバの役割について論じる．

なお，本文では一般的仕様に関しては OpenPGP と呼び，個々の実装を PGP あるいは GnuPG と呼んで区別する．

1.2 OpenPGP とは

1.2.1 Pretty Good Privacy

OpenPGP の原型となった PGP (Pretty Good Privacy) はデータを暗号化するアプリケーションである．1991 年に Philip Zimmamman が最初の PGP version 1.0 を作成し，その後世界各地の有志によって改良に改良が加えられた．1998 年には OpenPGP として規格化され，その内容は RFC2440[4] として公開されている．

ソフトウェアとしての PGP は，Pretty Good Privay, Inc. 社が販売，開発，そして無料ソフトウェアとしての配付を行なっていたが，後に同社を買収した Network Associates, Inc が作業を引き継いだ．しかしながら，PGP は今後のバージョンアップが困難な状態にある．2001 年 10 月に Network Associates,Inc は PGP 事業部門を再統合することを発表し，PGP および関連製品ラインはそれ以降メンテナンスモード (開発停止) になっている (NAI の発表は http://www.nai.com/other/jump/pgp-integrated.asp, 日本法人の発表は http://www.nai.com/japan/pgp/ を参照)．売却先が見つかるまでは，PGP の保守やサポートは続けられるが開発が継続される予定はない．

2002 年 2 月の時点で PGP 製品版の最新バージョンは PGP Desktop Security 7.1.1 である．無料配付版である PGP Freeware はバージョン 7.1 の Windows 版および Mac 版が公開されている．UNIX 用コマンドライン版の最新版としては PGP 6.5.8 がバイナリ/ソースコードともに無料で公開されている．これらの無料公開版は非商用という条件下で無料で利用できる．無料版の詳しい利用条件は LISENCE ファイルに入っている PGP Network Associates Freeware End User License Agreement に記述されている．

1.2.2 GNU Pairvacy Guard

OpenPGP を実装した GnuPG(GNU Privacy Guard) は，German Unix Users Group (GUUG) のメンバーである Werner Koch によって開発された．Version 0.0.0 は 1997 年 12 月にリリースされ，2001 年現在の最新版は Version 1.0.6 である．特徴として，商用非商用を問わず GNU Public License に従って自由に改良再配布ができることが挙げられる．また特許で制限されたアルゴリズムを全く使っていないために，特許上の利用制限もないという特徴を持っている．たとえば当初は RSA 暗号は特許制限があるために標準パッケージには含まれなかったが，2000 年 9 月の RSA アルゴリズムの Public domain 化にともない，バージョン 1.0.4 からは RSA が標準で使えるようになった．

1.2.3 メールの暗号化だけではない OpenPGP

PGP/GnuPGは，一言で説明すれば汎用のデータ暗号ツールである．公開鍵暗号，共有鍵暗号，電子署名などの基本的な機能をもち，広域ネットワーク上での鍵交換を容易にするために鍵サーバへネットワーク経由でアクセスする機能などの周辺機能を持つ.「PGPはメールのセキュリティを高めるツールである」と説明する文を多く見受けるが，これはOpenPGPの機能の一面を示しているに過ぎない．(ただしインターネットを利用するユーザが最も多く利用するサービスはメールであるので，結果的にOpenPGPが多く利用される場面はメールであることは事実である．OpenPGPは出力フォーマットをバイナリもしくはアスキー (Radix-64形式) で出力できるため，アスキー出力された結果をメールその他のメッセージに張りつけてアスキー形式のテキストファイルとして送ることはインターネットでは広く行われてきた．)

本章では，このOpenPGPの広い用途の中でも，特にインターネットの認証基盤としての役割に注目する．

2 PKIの標準化動向

公開鍵暗号を使ってファイルの署名や検証を行なう仕組みである電子署名は，インターネット社会において重要な役割を担っている．しかしながらインターネット上の公開鍵暗号利用には,「通信したい相手の公開鍵をどうやって手に入れるか」「公開鍵が本物であるかどうかを誰が確認するのか」という根本的な問題が存在する．そして現在，その問題を解決する共通鍵のインフラ (Public-Key Infrastructure)，すなわちPKIの整備が必要とされる．

PKIの主な機能には以下の3点がある [13].

- 利用者を登録し，公開鍵証明書を発行する
- 公開鍵が失効した場合には公開鍵証明書を破棄する
- 検証のために公開鍵証明書を保管する

大規模分散ネットワークであるインターネット上でこれらの機能を実現するインターネットPKIの仕組みは，現在も開発途上である．その中でも活発な活動が進められているプロジェクトとして，X.509とOpenPGPをあげることができる．X.509とOpenPGPの両者はまったく異なる思想にもとづいたシステムであり，現在のところ相互運用性はない．そしてしばしばX.509とPKIとは同一視されているために,「PKIとPGPは両極の方式である」[2]と紹介されることもあるが，この表現は正確ではない．正しくは「PKIを実現する技術標準としてX.509とOpenPGPの標準化活動が活発に進められており，その両者はまったく異なる考え方に基づいてつくられている」と言い直すことができる．

本章では，これらの異なるモデルの比較検討という点からPKIを考察する．また，その他のPKIのモデルや今後のPKIの将来像についても報告する．

2.1 X.509 の PKI

2.1.1 X.509 Public Key Infrastructure

X.509[8] は ITU(国際通信連合) の下部組織である ITU-T(International Telecommunication Union-Telecommunication sector) によって提案された技術標準で，国際標準規格 ISO 9594-8 としても登録されている．

X.509 の認証においては，認証局すなわち CA(Certificate Authority) と呼ばれる発行機関が管理機能を与えられている．CA は電子署名の証明書を利用者に発行する．さらにそれぞれの CA は階層構造をなしており，CA 同士が相互認証することによって証明書の連鎖を形成している．CA の機能には登録機能も含まれるが，その機能は登録機関 (RA) に委託される場合もあり，必ずしも CA 自らが登録を行なう必要はないとされる．

X.509 は OSI の X.500 ディレクトリシステムを前提としたオンライン認証全般についての規格だったが，柔軟な運用を行なうための改訂が行なわれている．X.509v3(Version 3) では，公開鍵証明書に任意の情報を埋め込むための拡張項目が追加された (表 1 参照)．後述するインターネット公開鍵インフラストラクチャおいても，X.509 は X.500 ディレクトリを前提せずに標準化する議論が進められている．

1. version
2. serialNumber
3. signature
4. issuer
5. validity
6. subject
7. subjectPublicKeyInfo
8. issuerUniqueIdentifier (v2 または v3 のオプション)
9. subjectUniqueIdentifier (v2 または v3 のオプション)
10. extensions (v3 のみのオプション)

表 1: X.509 の公開鍵証明書

2.1.2 X.509 とインターネット標準化

インターネット技術の標準化を推進する IETF では，X.509 のインターネットでの利用についても討議が行なわれてきた．当初，X.509 の実装は WWW やメールといったアプリケーションごとに議論されてきたが，今日では総合的な PKI についての議論が進められている．

Netscape 社のブラウザに採用され，インターネットで爆発的に普及した RSA 社 (RSA Data Security, Inc.) の SSL は，公開鍵証明書のための規格として X.509v3 に準拠した方式を採用している [11]．RSA 社は電子メールにおいても同様のデータフォーマットを

S/MIME(Secure/Multipurpose Internet Mail Extensions)として提案した．このS/MIMEはIETFのS/MIME Working Group (http://www.ietf.org/html.charters/smime-charter.html)にて検討されている．

さらに，インターネットの総合的なPKIとしてX.509を採用する議論がIETFのPublic-Key Infrastructure (X.509) (pkix) Working Group (http://www.ietf.org/html.charters/pkix-charter.html)にて行なわれている．S/MIMEの認証機構はPKIX Working Groupの作業に基づいて行なわれることになっており，両グループは密接な関係にある．

インターネットでのX.509についてはRFC 2459に，S/MIMEについてはRFC 2311, 2312にて規格化されている．それらはIPA(情報処理振興事業協会)セキュリティセンターにて日本語訳も公開されている (http://www.ipa.go.jp/security/pki/pki.html)．

2.2 OpenPGPのPKI

2.2.1 OpenPGPの Web of Trust

OpenPGPは，X.509で提案されたモデルとは異なる独自のPKIによって電子署名の認証を行なう．OpenPGPでは公開鍵暗号が本人のものであるかどうかを末端利用者同士が個人レベルで認証するモデルを採用している．つまり，どの証明書を信頼してどの証明書を排除するかはCAではなく各利用者が責任を負う．このモデルは，PGPのドキュメントで “Web of Trust”(信頼の輪)と表現されている．

2.2.2 OpenPGPとインターネット標準化

OpenPGPのインターネットにおける標準化は，IETFのOpenPGP Working Group (http://www.ietf.org/html.charters/openpgp-charter.html)にて推進されている．2002年までにRFC化されたもので，有効なものは以下のものである．

RFC2440, “OpenPGP Message Format” OpenPGPを定めた規格．RFC 1991, “PGP Message Exchange Formats”はPGPバージョン2をもとに作られた規格だが，RFC 2440はPGPバージョン5以降をもとにして作られた新しい規格である．1998年発行．
2002年1月現在，利用できる暗号アルゴリズムの見直しなどを行なった改訂版 [5] を策定中である．

RFC3156, “MIME Security with OpenPGP” RFC2015, “MIME Security with Pretty Good Privacy(PGP)”を改訂したもの．別名OpenPGP/MIMEとも呼ばれる．2001年発行．

2.3 X.509とOpenPGPの比較

X.509とOpenPGPの特徴について述べた．

X.509およびとOpenPGPはたとえ同じ暗号アルゴリズムを採用していても，これまでまったく別々に標準化を進めており，相互接続性はない．たとえば，S/MIME準拠の電子署名メールとOpenPGP準拠の電子署名メールとは別々のアプリケーションによって処理される．これは両者のPKIのモデルが異なっているためである．

特徴	X.509	OpenPGP
PKIの形態:	hierarchical PKI	trust-file PKI
公開鍵の認証者:	専門機関 (CA)	各ユーザ
信頼点:	ルート CA	利用者自身 (面識)
認証の連鎖構造:	ツリー型	ユーザ中心型
認証者を認証する根拠:	利用者による選択	利用者自身
証明書の破棄の管理:	あり	不完全
コスト:	高い	低い

表 2: X.509 と OpenPGP の相違点

2.3.1 相違点

表 2 に PKI としての OpenPGP と X.509 とを比較する．

先に OpenPGP の認証システムを “Web of Trust” と呼んだが，別の呼び方としては，利用者が CA に問い合わせず自分で認証を行ない，手元の認証ファイルを元にして相手を信頼するために trust-file PKI とも呼ばれ，それに対して階層化された CA によって認証を行なう X.509 は hierarchical PKI とも呼ばれる [13].

このために，OpenPGP は通信したい相手の公開鍵を CA から入手するのではなく，末端利用者が自力で入手しなければならない．これは認証システム構築において問題となる可能性がある．これでは大規模な認証システムの運営には不向きだと言えるかもしれない．しかしながら，PGP/GnuPGP は全世界規模のインターネットコミュニティにおいて利用されてきた．

たとえば，ニュースグループで配信されるコントロールメッセージへの PGP 署名は 1990 年代からすでに実用化されている [9]. これは，メッセージを中継する世界各地の無数のニュースサーバがコントロールメッセージ (ニュースグループ管理に関わる特定のメッセージ) への署名を自動的に検証する仕組みである．ニュースグループへの配信受信には第三者機関の登録は必要なく，ニュースサーバと PGP/GnuPG を導入してコントロールメッセージ用の公開鍵情報を設定すれば誰もがこの電子署名システムを利用可能である．このシステムが実用化された理由として，ソースコードおよびドキュメントがすべて無料で公開されている点もあげられる．INN, C News, DNews, ANU News といった主要ニュースサーバが速やかにこの機構を実装できたのも，このオープンソースの利点を生かしたためだと考えられる．

このように見ると，OpenPGP に適しているのは，(ニュースグループのように) 利用に際して第三者機関の登録認証を必要としないシステムであり，末端同士が随時メッセージを交換し認証を行なうアドホックなシステムである．このようなシステムは，近年 peer-to-peer システムとして注目を集めている [12]．今後さらなる開発および実用化が見込まれる peer-to-peer システムでは，セキュリティやアカウンタビリティを保証するために OpenPGP の “Web of Trust” の利用が進むと考えられる．

また，低コストで PKI を構築する場合にも OpenPGP および関連するオープンソースソフトウェアの利用は有効だと考えられる．

それに対して，X.509 の PKI は，アドホックな登録/認証作業には適していないが，継続的つ安定した認証サービスに適している．

2.3.2 OpenPGP の問題

OpenPGP を X.509 と比較した際に，末端利用者が通信相手の鍵をどのように入手し信頼するのかという問題を先に述べた．そしてさらに深刻な問題点も存在する．それは，公開鍵の失効の処理である．公開鍵の有効期間中に内容変更・秘密鍵の盗難・紛失・破壊などが生じたために公開鍵証明書が失効した場合，利用者に通知する必要が生じる．この場合，X.509 では CA がそれぞれの運営方針に応じて証明書失効リスト (CRL) を作成し連携する CA へと配布する．それに対して OpenPGP では，利用者自身が破棄証明書を作成し，各利用者へ配布する．その際の問題点として，利用者への通知が困難なこと，さらに利用者自身が秘密鍵を紛失した際には破棄証明書すら作成できなくなる．したがって，今後 OpenPGP は通知システム関連の改善が必要とされる．(この問題について鍵サーバが果たす役割については後で述べる．)

2.3.3 今後の展望

X.509/OpenPGP の実用化が進んでいるが，両者のモデルは本質的に異なり，それぞれの特性に適した用途が考えられる．すなわち，両者は相互排除の関係にあるのではなく，併存可能である．今後は，必要とされる状況に応じて双方の利点を生かしたインターネット PKI の構築を目指すべきである．

2.4 SPKI

X.509 や OpenPGP の他に注目されるインターネット PKI の標準化動向としては，SPKI(Simple Public Key Infrastructure) がある．SPKI は，IETF SPKI Working Group (http://www.ietf.org/html.charters/spki-charter.html) において標準化作業が行なわれており，現在は検討段階を終えて実装と相互運用性実験の段階に入っている．

SPKI Working Group での議論は Rivest と Lampson による SDSI(Simple Distributed Security Infrastructure) の研究 (http://theory.lcs.mit.edu/~cis/sdsi.html) をベースとしている．このため，研究分野では SPKI/SDSI と呼ばれる場合が多い．技術標準としては，1999 年に出された RFC 2692[7] において背景の概念が述べられ，RFC 2693 では証明書フォーマットや実装に必要な処理規則が規定されている．

現在のところ，SPKI は X.509 や OpenPGP のようには普及していないため，今後の普及の見通しの見込みは立っていない [1]．

最後に，X.509, OpenPGP, SPKI/SDSI の技術的な比較を表 3 に示す．

2.5 OpenPGP の今後の展望と鍵サーバの意義

OpenPGP の問題点として，「通信したい相手の公開鍵をどうやって手にいれるか」そして「公開鍵の破棄証明をどうやって通知するか」という鍵情報の入手の問題を挙げた．この問題に対して有効だと考えられるのがインターネット上の OpenPGP 公開鍵サーバである．この鍵サーバは OpenPGP 標準化以前の PGP バージョン 2 の頃から運用されており，現在も世界各地の鍵サーバが分散データベースを構築している．鍵サーバは電子メールや WWW 経由

X.509	ネームスペース:	グローバル
	証明タイプ	本人性の証明
	識別名と鍵との結合:	単一値関数: グローバルな識別名はそれぞれ唯一の 鍵ペアと一対一対応している． (ユーザはただひとつの公開鍵秘密鍵ペアを持っていると仮定する)
	CA の特徴:	グローバルな階層．コマーシャルの X.509 CA も存在する X.509 のコミュニティはトップダウンによって構築される．
	信用モデル:	階層型の信用モデル．信用は「信用できる」CA がつくる．
	電子署名:	それぞれの証明書は証明書発行者によって電子署名されている．
	証明書の失効:	CA が CRL(Certificate Revocation List) を配布する．
PGP	ネームスペース:	グローバル
	認証タイプ:	本人性の認証
	識別名と鍵との結合:	単一値関数: グローバルな識別名はそれぞれ唯一の 鍵ペアと一対一対応している． (ユーザはただひとつの公開鍵秘密鍵ペアを持っていると仮定する)
	CA の特徴:	平等主義的なデザイン．それぞれの鍵で証明書を発行できる． PGP のコミュニティは分散構造のボトムアップによって構築される．
	信用モデル:	*Web of Trust*(信用の輪)
	電子署名:	それぞれの証明書は複数の署名を含むことができる．最初の署名は証明書発行者による署名である．
	証明書の失効	利用者が破棄証明書を PGP 公開鍵サーバに登録することで， 無効になった公開鍵を手元に持っている相手に配布する．
SPKI/ SDSI	ネームスペース:	ローカル
	証明タイプ:	本人性の証明または認証の証明
	識別名と鍵との結合:	多値関数: ローカルな名前はゼロ，1，それ以上の鍵と結合される． (ユーザはただひとつの公開鍵秘密鍵ペアを持っていると仮定する)
	CA の特徴:	平等主義的なデザイン．それぞれの鍵は証明書を発行できる． SPKI/SDSI のコミュニティは分散構造のボトムアップによって構築される．
	信用モデル:	*chain of authorization* の提供 グループを定義し認証を委任するためにインフラストラクチャは 明快でスケーラブルなモデルを持つ．
	電子署名:	それぞれの証明書は証明書の発行者による署名を一つ含んでいる．
	証明書の失効:	短い有効期限と生存証明書を用いる

表 3: 技術的な観点からの X.509, OpenPGP, SPKI/SDSI の比較．Clarke[6] の表を参考にした．

で利用可能であり，自由に公開鍵の登録を行ない，さらにはメールアドレス，ニックネーム，鍵 ID で公開鍵を検索できる．さらに，公開鍵の破棄証明を送れば登録されている公開鍵に破棄証明が加えられる．

利用者個人が認証に責任を持つ OpenPGP の PKI は，鍵サーバの機能を組み合わせることによってさらに有効な PKI となると言える．

3 本章のまとめ

本章では，PKI の視点から X.509 および OpenPGP をとりあげ，両者が異なるモデルの実現を目指していること，および両者の特長を示した．また，それ以外の PKI の提案として SPKI/SDSI についても紹介した．PKI には唯一のモデルは存在しない．したがって PKI を構築するにあたってどのモデルを採用するのかという視点が必要となる．

PKI としての OpenPGP は，認証局及び登録機関を介することなく peer-to-peer の認証を行なえるという特長がある．しかしながら,「通信したい相手の公開鍵をどうやって手にいれるか」そして「公開鍵の破棄証明をどうやって通知するか」という点が不十分である．この問題点への取り組みとして，鍵サーバの役割をあげた．

4 備考: ドイツ政府の GnuPG への取り組み

1999 年以降，ドイツ政府は GnuPG プロジェクトを支援し，政府機関に採用する動きを見せている．まず 1999 年 11 月にドイツの連邦経済技術省 (BMWi, Bundesministerium für Wirtschaft und Technologie) が GnuPG プロジェクトに 318,000 マルク (およそ 17 万 US ドル) の資金援助を行なうことを発表した [3, 14]．このプロジェクトリーダーはドイツ在住の Werner Koch である (GnuPG は世界各地から開発者が参加しているが，プロジェクトリーダーは Werner Koch が担当している)．

GnuPG の初期バージョンのリリースと前後してドイツ政府はソースコードを公開にすることでシステムの安全性を確保するために，暗号の配布/輸出に対して制限を設けない方針を発表しているが，GnuPG の支援はその延長として考えられる．

さらに，GnuPG およびソースコード公開の暗号システムを政府の情報基盤として位置づける方針も打ち出されている．2001 年 10 月 1 日に，ドイツ内務省の情報技術保安局 (BSI, Bundesamt für Sicherheit in der Informationstechnik)[10] は政府標準メーラ Sphinx(スフィンクス) プロジェクトを発表した．この Sphinx メーラの仕様には X.509v3 に準拠した S/MIME の実装が含まれているが，注目されるのはこの計画に採用された Ägypten(エジプテン) プロジェクトである．

Ägypten プロジェクトでは，Sphinx メーラをフリーソフトウェアで作成し，その成果を GNU Public License のもとに公開することが計画されている．そして，さらに注目すべきことに，GnuPG の Werner Koch も参画しているこのプロジェクトは Sphinx の仕様に OpenPGP を追加し，S/MIME と OpenPGP の両者を併存させる予定である (http://www.gnupg.org/-aegypten/)．

このように，政府向け PKI とソースコード公開の重要性，そして OpenPGP の関わりを考える上でドイツ政府は斬新な試みを行なっており，2002 年に予定されている Sphinx メーラ

の発表が注目される.

参考文献

[1] Carlisle Adams and Steve Lloyd. *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations.* Macmillan Technical Publishing, 1999. 邦訳『PKI: 公開鍵インフラストラクチャの概念、標準、展開』(ピアソン・エデュケーション, 2000.7).

[2] 青木隆一, 稲田龍. PKI と電子社会のセキュリティ. 共立出版, October 2001.

[3] BMWi. Press release on the promotion of "Open Source and IT-Securit Enhancement and Marketing of the GNU Privacy Guards (GnuPG) project". *Sicherheit im Internet*, November 22 1999. Online press release in English, available at http://www.sicherheit-im-internet.de/-themes/themes.phtml?ttid=20&tsid=196&tdid=337.

[4] Jon Callas, Lutz Donnerhacke, Hal Finney, and Rodney Thayer. OpenPGP Message Format. *Request For Comments*, November 1998. RFC 2440 (Category: Standards Track) replaces RFC 1991, "PGP Message Exchange Formats".

[5] Jon Callas, Lutz Donnerhacke, Hal Finney, and Rodney Thayer. OpenPGP Message Format. *Internet Draft*, August 2001. draft-ietf-openpgp-rfc2440bis-03.txt. Revision of RFC 2440[4]. http://www.ietf.org/internet-drafts/draft-ietf-openpgp-rfc2440bis-03.txt.

[6] Dwaine E. Clarke. SPKI/SDSI HTTP Server / Certificate Chain Discovery in SPKI/SDSI. Master's thesis, Department of Electrical Engineering and Computer Science at Massachusetts Institute of Technology, September 2001. http://theory.lcs.mit.edu/~cis/theses/clarke-masters-.pdf.

[7] Carl M. Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian Thomas, and Tatu Ylönen. SPKI Certificate Theory. *Request For Comments*, September 1999. RFC 2693 (Status: Experimental).

[8] International Telecommunications Union-Telecommunication Standardization Sector (formerly "CCITT"). Recommendation X.509, "Information Technology–Open Systems Interconnection–The Directory: Authentication Framework". (Equivalent to ISO 9594-8.), June 1997.

[9] David C Lawrence. Authentication of Usenet Group Changes. Online document, 1999. ftp://-ftp.isc.org/pub/pgpcontrol/README.html.

[10] KMail and mutt as Sphinx-clients for German authorities. *NewsForge*, October 05 2001. Online article available at http://www.newsforge.com/article.pl?sid=01/10/05/162238.

[11] Magnus Nystrom and Burt Kaliski. PKCS #10: Certification Request Syntax Version 1.7. *Request For Comments*, November 2000. RFC 2986 (Status: Informational).

[12] Andy Oram, editor. *Peer-to-Peer: Harnessing the Power of Disruptive Technologies.* O'Reilly & Associates, March 2001.
Some chapter is available at http://www.oreilly.com/catalog/peertopeer/.

[13] Robert W. Shirey. Internet Security Glossary. *Request For Comments*, May 2000. RFC 2828 (Also FYI 36) (Status: Informational).

[14] Peter Wayner. Germany awards grant for encryption. *New York Times*, November 19 1999. Also available at http://www.nytimes.com/library/tech/99/11/cyber/articles/19encrypt.html.

[0]参考文献中のオンライン情報の最終アクセス日は 2001 年 12 月 29 日である.