



【セミナー】

暗号メール標準化の行方を探る

PGP/MIMEとS/MIME

山本 和彦 IJ技術研究所

電子メールでの通信においてプライバシーを守る手段として何度も本誌で取り上げている暗号メール。この暗号メールの主流としてPGP/MIMEとS/MIMEという2つの方式がある。現在両者ともインターネットでの標準化が活発化している。今回は、暗号メールが持つ機能に触れ、両者の違いを解説しながら、暗号メールの標準化の動きについて解説する。

PGP/MIME & S/MIME

現実社会よりも安全なインターネット

「悪者がはびこるインターネットは現実社会よりも危険である」という誤った報道が心ないマスコミによって繰り返されている。確かに、遠隔から姿を見せずに侵入できることやデータの電子的なコピーは証拠が残らないことなどはクラッカーに有利に働くように思える。通信技術を深く理解していない人にとって、インターネットがよくわからない危険な世界に映るのもいたしかたないだろう。

しかし、そう悲観になることはない。危害を加える者にとって武器となる技術が存在

する一方で、プライバシーを保護する技術も洗練されている。現実社会の安全性にはなんら客観的な根拠がないのに対し、電子的なプライバシーのそれは数学的に保証されている。この意味では、現実社会よりもインターネットのほうが安全といえるだろう。ユーザーが正しく技術を理解し適切に利用すれば、インターネットは快適で安心できる世界である。

暗号が可能にする 4つのプライバシー保護

インターネットユーザーにとってもっとも馴染みの深いサービスの1つが電子メールである。

ここでは電子メールのプライバシーを保護するための技術について解説していく。これは一般的に「暗号メール」という名で知られているが、この言葉から連想されるイメージはプライバシー保護機能の一面しか捉えていない。

インターネットに普及しているプライバシー保護の技術では、以下の4つの項目を保証できる。もちろん、暗号メールも例外ではない。

- ①機密性：意図した相手だけが内容を理解できること。第三者には内容が知られないこと。
- ②認証：ある名前を名乗る人が、本当にその

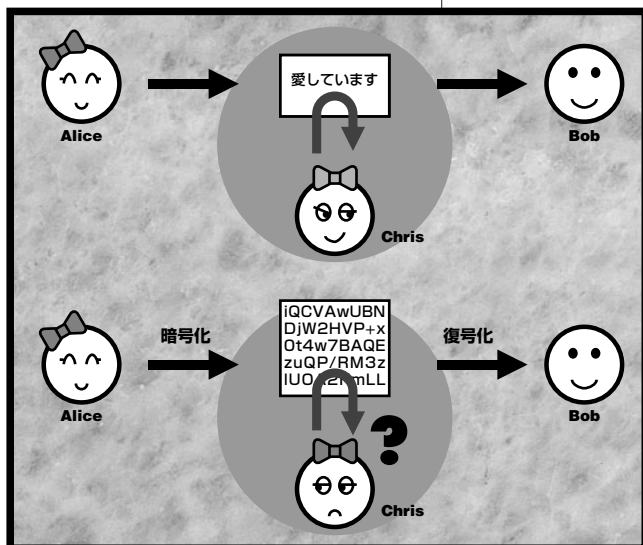


図1 電子メールの機密性

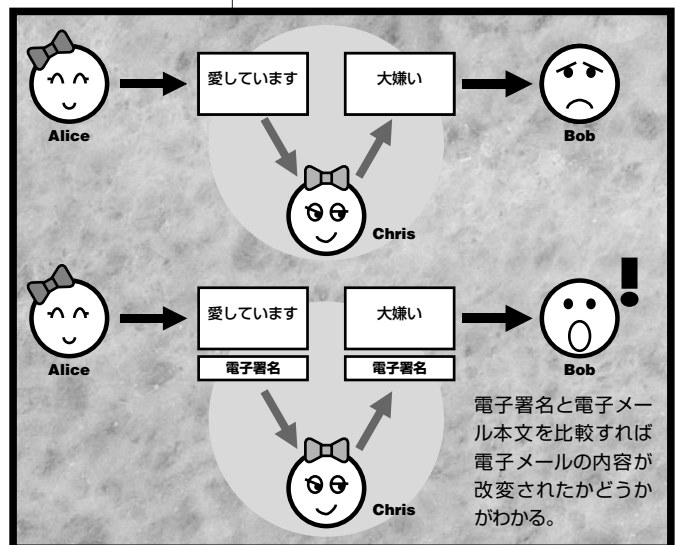


図2 電子メールの内容の完全性

人だと確認すること。

- ③**完全性**：送信者が書いた内容がそのまま受信者に伝わること。第三者によって内容が変更された場合は、それを検知できること。
- ④**否認防止**：通信内容をあとから否定できないこと。

一般的によく使われる機密性と認証

機密性は、まさに暗号メールという言葉から連想される機能である。たとえば、AliceがBobに電子メールで愛をささやく場合、当然内容をほかの人には知られたくない。電子メールの機密性を守るためには、Bobだけが読めるようにする暗号技術が利用できる。以前は政府や軍隊の独占物であった解読に数千年以上もかかる強力な暗号は、もう我々市民の手の中にある。封筒で覆うことで中身を保護している郵便と比較すれば、暗号メールがいかに安全であるかが理解できるだろう (図1)。

認証という機能自体はわかりやすく、その必要性もすぐに察しがつくだろう。再び封筒を例に挙げるなら、差出人に自分以外の名前

を書くのは簡単である。たとえば、嫉妬に狂ったChrisがAliceの名をかたってBobに絶交文を書くかもしれない。郵便では、筆跡だけが相手を見極める手段である。筆跡という手がかりがない電子メールでは、「From:」フィールドにAliceと書くだけで、十中八九Bobをだませる。しかし、「電子署名」を利用して認証すれば、電子メールの差し出し人を確実に確認できる。

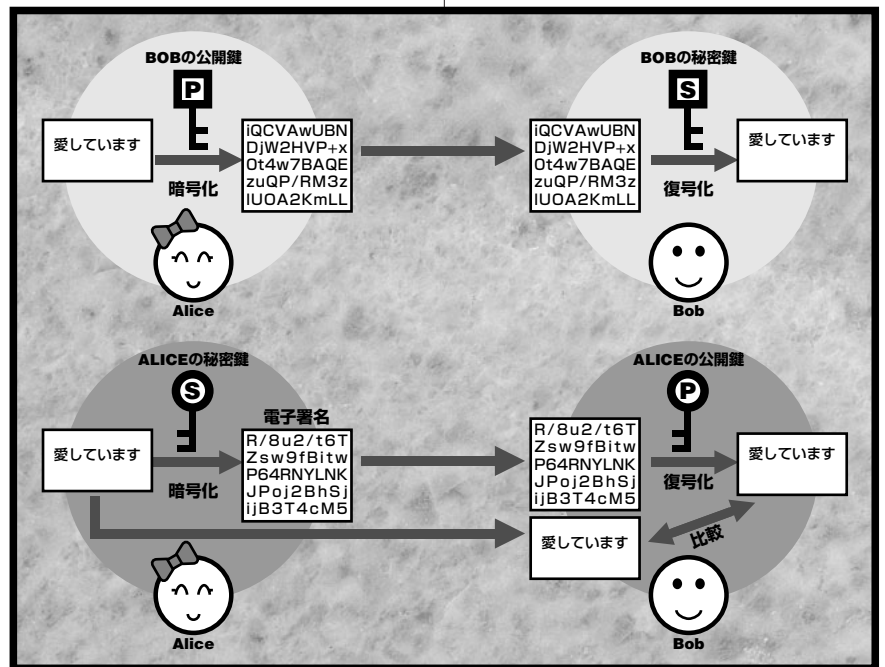
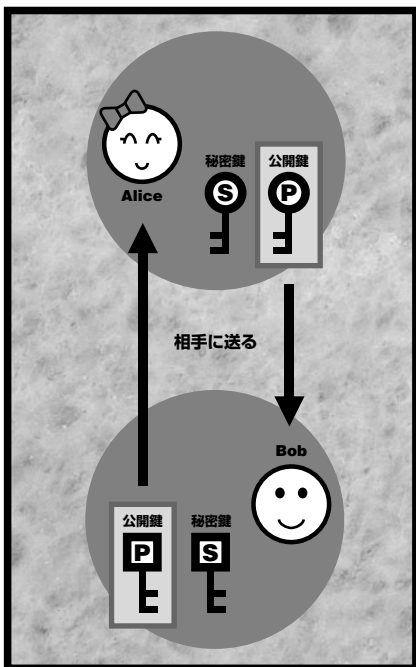
内容の完全性の保証や否認の防止もできる

完全性も直観的に理解できる機能だろう。Aliceが書いた「愛しています」というセリフをChrisが「大嫌い」と変更してBobに送り付けるのは、筆跡のない電子メールなら造作もないことである。しかし、電子署名を利用すれば電子メールの完全性も保証できる。ただし、暗号メールでは、変更が加えられた事実は検知できるが、どこが変更されたかまではわからない方式が使われていることが多い (図2)。

否認防止は見落としがちなプライバシー保護機能である。たとえば、BobからのプロポーズをAliceは了承したのに、あとからそんなことは言っていないと言われても困る。またインターネットで商売をする際には、商品の発送後に「こんな発注はかけていません」と言われると大打撃だ。このようにあとから通信の内容を否定できない機能は、インターネット上でのプライバシー保護にとって重要である。否認防止は認証と完全性から保証できる。つまり、ある文章の内容が変更されていないことを証明でき、さらに、それを書いた人を確実に特定できるなら、否定のしようがない。このように、否認防止も電子署名によって実現できる。

暗号メールには公開鍵暗号が使われる

暗号メールには、公開鍵暗号という近代的な暗号が必要となる。この公開鍵暗号のおかげで、上記の4つの機能が実現可能となった。以下では機密性と認証を実現する方法を簡略



化して解説する。実際の方法はこれよりも複雑であるが、詳しいことは今回は触れない。

公開鍵暗号では2つの鍵を生成する。一方を秘密に保持し、他方を公開するので、それぞれ秘密鍵と公開鍵と呼ばれている。これらの鍵は互いに鍵と錠前の関係にある。一方で暗号化すれば、他方で復号化できる。ほかの鍵で暗号文を復号化することはできない。また、公開鍵から秘密鍵を推測することは大変困難である。さらに、秘密鍵と公開鍵の組みはほかの誰のものとも違うように生成される(図3)。

4つの機能を同時に満たす暗号メール

AliceがBobに暗号文を送ることを考えよう。AliceはBobの公開鍵を、BobはAliceの公開鍵をあらかじめ手に入れているとする。Aliceはラブレターを書いた後、Bobの公開鍵を使ってその内容を暗号化する。この暗号文は、Bobの秘密鍵でしか復号化できない。Bobの秘密鍵はBobしか持っていないのだから、Bobしかラブレターの内容を読めず、機密性を保てる。

次は、BobがAliceを認証する方法に移ろう。機密性の場合とは違い、今度は公開鍵と

秘密鍵の立場を逆転させる。Aliceはメッセージのコピーを取り、それを自分の秘密鍵で暗号化する。これが電子署名である。この電子署名とメッセージと一緒にBobに送る。Bobはまず、電子署名をAliceの公開鍵で復号化し、メッセージの内容と比較する。まったく同じであれば、このメッセージはAliceが書いたに違いない。なぜなら、この電子署名を生成できるのは、Aliceの秘密鍵を持っているAliceだけなのだから(図4)。

完全性もこの電子署名で確かめられることが容易にわかるだろう。ただし、実際にはメッセージ全体を暗号化することは非効率なので、メッセージを特徴づける値を抽出し、これを暗号化する。このため改変の可能性は検出できても、どこが改変されたのかわからないのである。

暗号メールでは、内容の暗号化と電子署名を同時に組み合わせて使用できる。よって、1つのメッセージを送る際に、前述の4つの機能を同時に実現できる(図5)。

秘密鍵と公開鍵

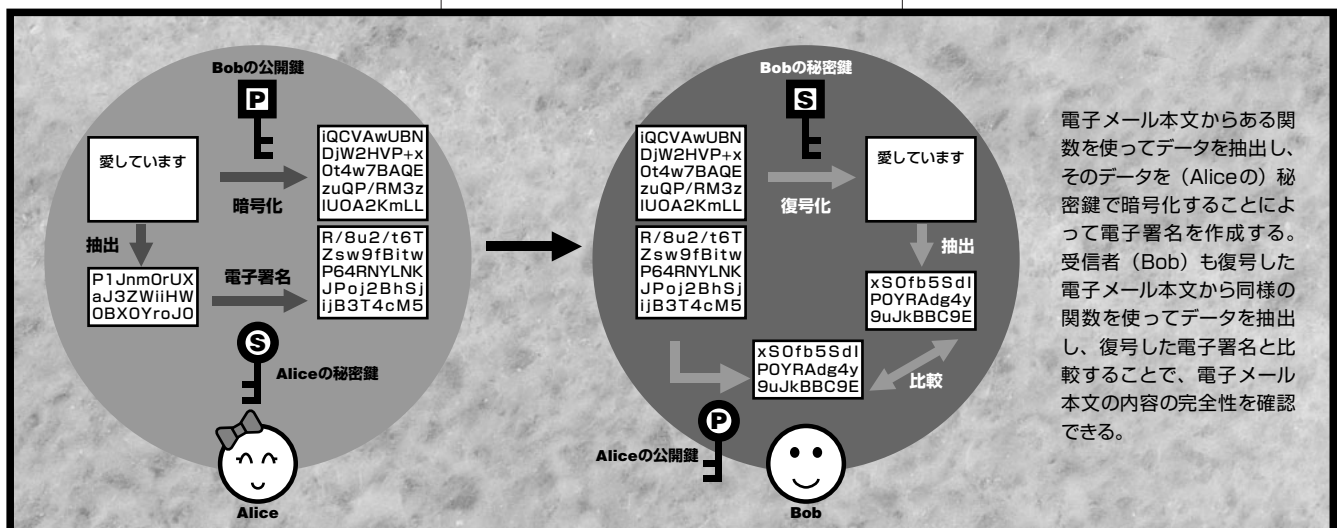
暗号メールの利用で重要なのは、秘密鍵を秘密に保持すること、そして、公開鍵を安全に相手に届けることである。秘密鍵は通常パ

スワードで暗号化されて保存されている。必要になったらパスワードを入力し、秘密鍵を取り出すのである。電子署名が改変されないようにするのは、信用できる誰かに電子署名自体に署名してもらえばよい。この「誰か」を誰にするのかということ、信用モデルという。信用モデルについては、後述する。

各国で異なる暗号の規制

どんな道具も諸刃の剣である。適切に利用すれば作業を効率化できるし、また生活を豊かにしてくれる。しかし、悪用されると武器や凶器になりかねない。暗号もそうだ。市民のプライバシーを保護する一方で、警察がマフィアの悪事の相談を盗聴することを困難にする。

政府によっては危機感を覚え、市民の暗号利用を制限したり輸出を規制したりしている。米国に暗号の輸出規制があることはよく知られている。一説には米国政府が解読できる暗号のみに輸出の許可がおりるそうだ。フランスには、市民が暗号を使用してはいけないという規制がある。また、米国は通信相手に加えて政府も暗号を解読できるような仕組みをもつ暗号を利用するように圧力をかけ始めている。幸いなことに日本国内での暗号の利用は自



電子メール本文からある関数を使ってデータを抽出し、そのデータを(Aliceの)秘密鍵で暗号化することによって電子署名を作成する。受信者(Bob)も復号した電子メール本文から同様の関数を使ってデータを抽出し、復号した電子署名と比較することで、電子メール本文の内容の完全性を確認できる。

図5 電子署名付き暗号メール

PGP/MIME & S/MIME

由である。しかし、米国の政策になびく通産省は、暗号関連製品の輸出規制に乗り出した。

このような規制はソフトウェアの発展やビジネスの展開を著しく抑制する。インターネットの発展を願うなら、このような規制はナンセンスである。

一企業の利益につながらない技術

また、暗号は特許やロイヤリティーの問題にも悩まされてきた。一企業の利益につながるような技術を、インターネットの標準化組織IETFが標準として採用するわけにはいかない。しかし、特許はいつかは切れる。1997年4月、多くの人が待ちに待った2つの強力な公開鍵暗号の特許が消滅した。Diffie-Hellman暗号とElGamal暗号である。ちなみに、有名なRSA暗号の特許は2000年9月まで有効である。IETFで標準化されるインターネットのあらゆるセキュリティ技術は、このような束縛のない暗号を採用し始めている。

このような背景のある現在、我々が安心して利用できる暗号メールは2つ存在する。それは、PGP/MIMEとS/MIMEである。

PGP/MIMEとS/MIMEが出現するまでには、時代時代の背景を反映した方式の提案が繰り返されてきた。ここでは、その長い歴史を簡単に振り返ってみよう。

電子メール拡張のための2つの流れ

長い間利用されて来た電子メールは、本文にASCII文字列のみが許されていた。このため、初期の電子メールは、テキストメールと呼ばれている。日本で本文に日本語を入れているのは厳密にはルール違反であった。また、画像を送るためには、手作業でファイルをいったんASCII文字列に符号化して本文に挿入していた。

インターネットが裾野を広げ、ユーザーの要望が多様化するに従い、テキストメールを拡張するための大きな流れが2つ生まれた。一方が国際化を含むマルチメディア化、他方がプライバシーの強化である。これらの議論の場はIETFである。

PEMから始まる暗号メールの歴史

プライバシーの強化としては、PEM (Privacy Enhanced Mail) が開発された。暗号メールの歴史からみれば、前述の4つの機能を持つ仕様が公開されて知識が普及したことはまさに画期的な事件だったといえる。しかし、PEMはテキストしか扱えなかったこと、利用を始めるにはまず誰かに公開鍵を認証してもらって「証明書」を手に入れる必要があることなどが足かせとなり、潮流に乗れなかった。

PEMの仕様策定とからみ合うように、マ

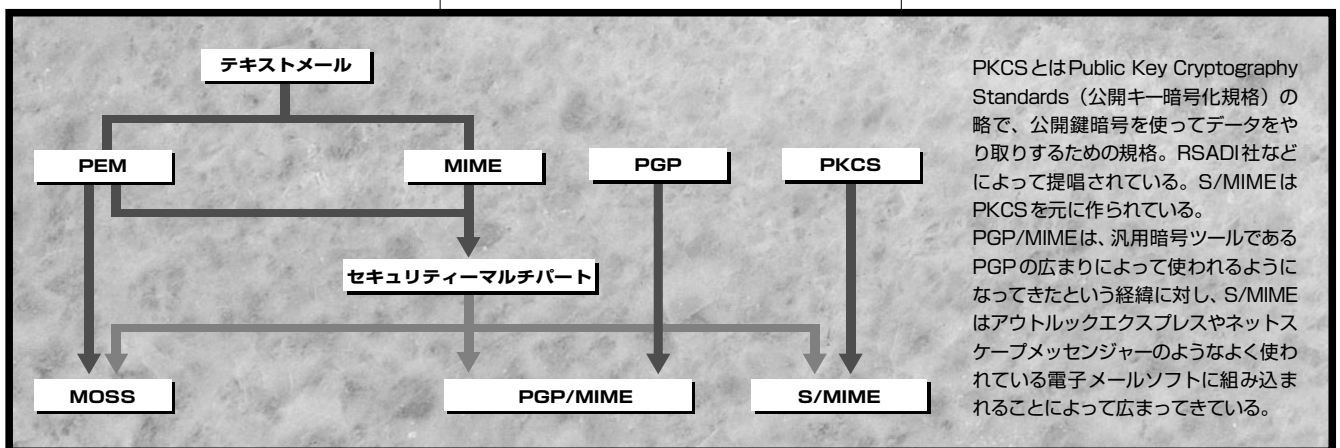
ルチメディアメールMIME (Multipurpose Internet Mail Extensions) が標準化された。MIMEでは、データ型を指定するためのラベルが導入されたのでさまざまなデータを添付できる。テキストデータには文字コードを指定できる。また、複数のデータを格納するためのマルチパートや電子メール自体を格納するためのメッセージというデータ型が定義されたので、本文の構造を柔軟に作成できる。さらに、配送する際に安全となるような符号化方式も採択された。

MIMEはさまざまなベンダーから支持されて急速に広まった。MIMEのおかげで本文に日本語を入れることはもはや違反ではないし、さまざまなデータを簡単に添付できる。

PEMのMIMEへの統合により生まれたMOSS

MIMEの登場以来、テキストしか扱えないPEMが時代遅れであることは誰の目にも明らかだった。そうはいってもPEMが果たした役割が色あせるわけではない。事実PEMで開発された符号化方式は、そのままMIMEに利用されている。

このような時代背景の中で、MIMEという汎用的な電子メールの枠組を使ってプライバシーを保護する方式を開発する必要があった。つまり、PEMのMIMEへの統合である。



PKCSとはPublic Key Cryptography Standards (公開鍵暗号化規格) の略で、公開鍵暗号を使ってデータをやり取りするための規格。RSAD社などによって提唱されている。S/MIMEはPKCSを元に作られている。PGP/MIMEは、汎用暗号ツールであるPGPの広まりによって使われるようになってきたという経緯に対し、S/MIMEはアウトLOOKエクスプレスやネットスケープメッセンジャーのようなよく使われている電子メールソフトに組み込まれることによって広まってきている。

図6 暗号メールの歴史

PGP / MIME & S / MIME

この統合作業の結果、暗号メールの枠組と
 その中で実現される具体的なサービスが分離
 された。前者は、マルチパートを利用するの
 で「セキュリティーマルチパート」と呼ばれ
 ている。この枠組の中で実現したPEMが、
 MOSS (MIME Objects Security Service)
 である。MOSSはPEMの後継であるが互換
 性はない。MOSSではPEMの場合と同じよ
 うに「証明書」を発行してもらう必要がある
 が、このことが再び足かせとなった。

結局MOSSはベンダーの支持を受けること
 ができず、現在では歴史的な産物の地位に甘
 んじている。

PGPのMIMEへの統合

IETFの活動とは関係なく、インターネッ
 トで暗号ツールの実質的な標準の地位を得て
 いたのがPGPである。PGPは証明書の発行
 というお役所的な制約を持たず、知り合い同
 士が互いに認証し合うことで信用を保証す
 るので、使い始めるのが容易である。暗号や署
 名を施したファイルをテキストメールで配送
 するために、PGPは独自の書式を生成でき
 た。しかし、MIMEの中での利用方法は定義
 されていなかったため、自動的な署名の検証
 や暗号文の復号化などは実現できなかった。

そこで、PGPをMIMEへ統合するために、
 セキュリティーマルチパートにPGPの書式を

埋め込む方式が提案された。この方式は
 IETFで承認され、現在ではPGP/MIMEと
 呼ばれている。PGPの普及度に合わせる形で、
 PGP/MIMEを実装した電子メールソフトは
 数多い。

標準を目指すS/MIME

S/MIMEは、暗号の老舗RSADSI社が提
 供する暗号に関する書式PKCSをMIMEに当
 てはめた暗号メールである。セキュリティー
 マルチパートに強く依存してはいないが、署
 名の一方式としてそれを利用する。S/MIME
 バージョン1はIETFとは関係なく規定され
 た。しかし、IETFで承認されない規約は廃れてい
 く傾向にある。

そこで、S/MIMEの開発者たちはバージ
 ョン2を開発する際にIETFに参加した。

その際S/MIMEはIETFにはふさわしくな
 い問題を2つ抱えていた。1つはS/MIMEが
 RSADSI社の登録商標であること。IETFが
 ある会社の宣伝となるような名前を利用す
 るわけにはいかない。もう1つは、S/MIMEが
 基づいているRSA暗号の特許である。商標と
 同様に、特定の企業が所有する特許を採用
 することはできない。

S/MIMEの開発者たちは、登録商標は
 RSADSIが保持するものの宣伝目的には利用
 しないという約束をIETFに取り付け、バージ

ョン2を「情報提供」という形で発行した。
 現在バージョン3の策定が進んでいる。Diffie-
 Hellman暗号を採用することで、真の標準と
 なることを目指す予定である。

OpenPGPによって標準化が進められるPGP

実は、PGPバージョン2もRSA暗号を利用
 している。PGPバージョン2に基づいた
 PGP/MIMEが標準化のプロセスに乗れたの
 は、まだIETFの採択ポリシーが緩かったから
 である。

現在、PGP/MIMEはS/MIMEと同様に、
 「情報提供」の位に格下げされている。

現在のPGPのバージョンは5であり、この
 書式を広めるためにIETFでOpenPGPとい
 う分科会が結成された。PGPバージョン5は、
 公開暗号としてRSA暗号をオプションに、
 ElGamal/DSSを必須にしている。このPGP
 の書式自体は、真の標準として採択されるだ
 ろう。今後は、PGPバージョン5に基づいた
 PGP/MIMEを開発する必要がある。

決定的な違いは『信用モデル』

PGP/MIMEとS/MIMEのどちらを使え
 よいのか迷ってしまう方も多だろう。それ
 ぞれ長所と短所を持ち合わせているので、特



IETF

URL: <http://www.ietf.org/>

OpenPGP,S/MIMEともにIETFで標準化作業が進めら
 れている。このサイトからドラフトをダウンロードできる。

決定事項	S/MIME v3	OpenPGP
メッセージフォーマット に基づくバイナリー	CMS (Cryptographic Message Syntax)	PGP方式
認証フォーマット	X.509v3	PGP方式
共有鍵暗号アルゴリズム	トリプルDES (DES EDE3 CBC)	トリプルDES (DES EDE3 Eccentric CFB)
公開鍵暗号アルゴリズム	Diffie-Hellman/DSS	ElGamal/DSS
ハッシュ関数アルゴリズム	SHA-1	SHA-1
署名付きデータの MIME フォーマット	multipart/signedまたは application/pkcs7-mime	multipart/signed
暗号データの MIME フォーマット	application/pkcs7-mime	multipart/encrypted

出展：インターネットメールコンソーシアムのウェブページより

URL: <http://www.imc.org/smime-pgpmime.html>

S/MIMEバージョン3とOpenPGPの違いと共通部分

PGP/MIME & S/MIME

微をみきわめて自分の目的に合ったほうを利用すべきである。

まず機能の差として、信用モデルの違いが挙げられる(図7)。

PGPは知り合いに自分の公開鍵に署名してもらふことによって、自分の公開鍵の信用度を保証してもらふ。つまり、通信相手をよく知っているなら、PGP/MIMEは導入の敷居も低く現実的な方法といえる。

S/MIMEでは、どこかの認証局に自分の公開鍵を保証する証明書を発行してもらふ必要がある。

つまり、導入の際に利用できる認証局を探さなければならないというPEMやMOSSと同じ問題を抱えている(自分自身で証明書に署名する自己署名という方法を使えば、すぐにも使い始められるが、そんなことをするぐらいならPGP/MIMEを用いたほうがよい)。

PEMやMOSSの時代とは違って、認証局のサービスを行う会社が現れている。たとえば、ベリサイン社やサイバートラスト社である。また、会社でプライベートな認証局を立ち上げる方法も考えられる。

面倒という感の拭えない認証局であるが、知らない人たちが通信する際には、必ず両者を保証する第三者が必要になる。真剣にインターネットでの商売を考えるなら、認証局は

避けては通れない問題である。

実装の点では両者とも互角

実装と普及の面に目を向けてみよう。PGPバージョン2はフリーソフトとして普及したことを反映してか、それに基づいたPGP/MIMEを実装している電子メールソフトにはフリーソフトウェアが多い。日本からもMewやSEMIといった優れた実装が提供されている。

PGPバージョン2の実装は世の中に1つしかなかったのに対し、PGPバージョン5の実装は少なくとも3つあるようである。そのうちの1つは本家のPGPであり、もう1つはGNUのGNUPGである。

そこで、今まで悩まなくてよかった相互接続性という問題に直面することになるだろう。また、多くの人が利用しているPGPバージョン2から最新のバージョン5への移行という問題も抱えている。

S/MIMEは、当初から複数のベンダーが実装していた。たとえば、ネットスケープメッセージャー、マイクロソフトのアウトルックエクスプレス、オレンジソフトのWinbiffなどで利用できる。当然相互接続性を検証していく必要がある。また、これらがサポートしている

のはバージョン2であるため、バージョン3への移行も課題に挙げられる。さらに、S/MIMEには認証局との相互接続性の問題もある。

こう考えてみると、実装状況では優位な差はないように思える。最後にこれからの技術的な話題について触れておこう。

統合が進めば加速度的な普及が見込める

日本人なら公開鍵や証明書の中の自分の名前に日本語を使いたいだろう。OpenPGPとS/MIMEの両方とも、国際化の方式としてUTF-8という文字コードを採用した。これは、Unicode 2.0にある変換を施して1~6バイトにしたコード体系である。Unicodeがどれくらい日本で受け入れられるか疑問であるが、多言語性を要求されない署名の国際化としては現実的な解かもしれない。

また、OpenPGPとS/MIMEで互いの証明書を利用できるようにしようという試みもある。これが実現すれば、加速度的に暗号メールが普及するのではないかと思う。

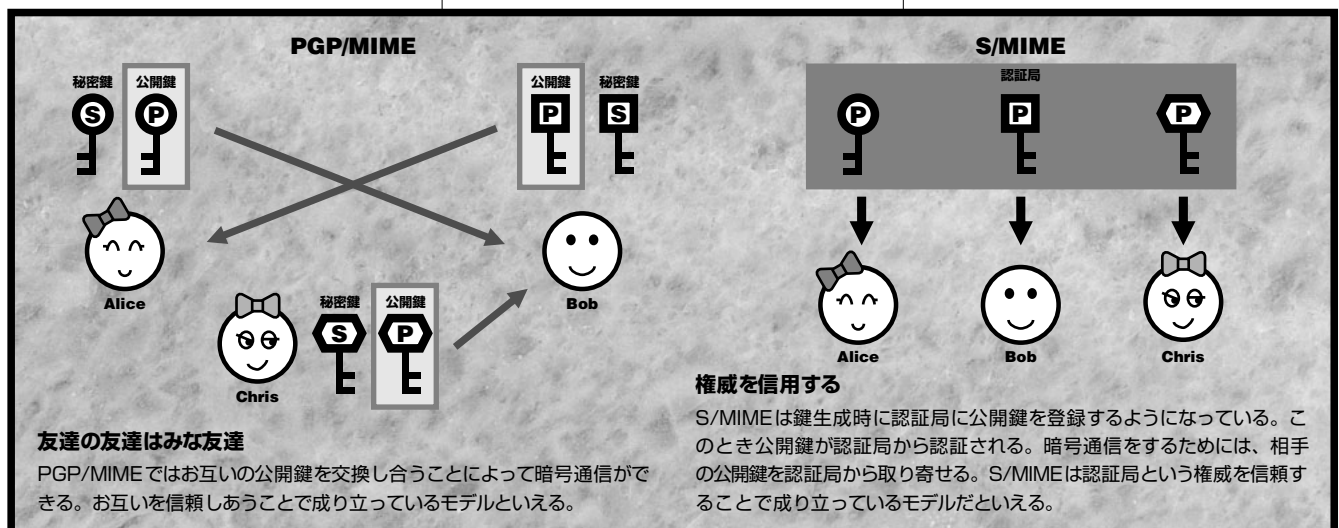


図7 両者の信用モデルの違い



[インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

株式会社インプレスR&D

All-in-One INTERNET magazine 編集部

im-info@impress.co.jp