電子メール最新技術動向

渡部 直明

((株)オレンジソフト)

1999年12月15日

Internet Week 99**パシフィコ横浜**

（社）日本ネットワークインフォメーションセンター編

目次

1 概要

この講演では、「電子メールの最新技術動向」について説明します。電子メールは気軽に利用されていますが、そのシステムを安定した運用を実現するため、様々な技術が組み合わせて適用されれています。ここでは、電子メールに関する今年のキーワードから始め、携帯電話の普及による電子メールの利用方法の広がり、即ち、個人同士の気軽なメールのやり取りから企業内での重要な情報伝達手段としてのメールの利用法を紹介します。本来、インターネットの電子メールは信頼性が保証されていなかったものですが、利用範囲が広がるにつれ信頼性を求められてきています。このような背景から、電子メールの危険性、メール管理 IMAP4 の新機能、暗号などを説明します。

2 今年のキーワード

以下に、今年のキーワードを挙げ紹介します。

● 通信傍受法の成立

今年になって通信傍受法案が成立し、電子メールも傍受の対象になりました。ところが、実際に電子メールを傍受する時、どんな技術で実現するのか、どういう方法でメールを特定するのかなどの具体的なことは不明のまま法律が成立してしまいました。傍受されることを前提とした時、電子メールを防御するための方法として暗号化という手法も有力であり今後の普及が予想されます。

● 電子メール感染型ウィルスの流行

メリッサ、Happy99 など多くのウイルスが出現しました。実際、当社に来るサポート依頼のメールの中にウイルスを持ったメールが混じっており、発信者への対応に苦慮した経験があります。最近は特に、OutLook、Exchange などの Windows の MAPI を使ったメールにウィルス感染されているのが目立ちます。それに伴い、アンチウイルス（ワクチン）ソフトも電子メールを防御する形で対応してきています。

● 携帯電話の登場

今年の一番大きな話題として携帯電話の登場を挙げることができます。携帯電話の登場で、手軽に電子メールを見ることができるようになったので、今まで電子メールに縁がなかった人も電子メールを使用し始め、利用者が急増しました。電車の中やその他の場所で、i モードや WAP を利用して電子メールをやり取りしている姿を見かけます。

● 電子メール転送の問題

携帯電話、PDA など電子メールを扱えるデバイスでインターネットの電子メールを読むには、転送先をキャリアに切り替える必要のある場合がありました。そして、これらを統合するサービスも出現しつつありますが、電子メールを転送してもセキュリティは大丈夫かという不安があります。

● 政府が電子認証制度の導入を発表

1999 年 8 月、政府は 2001 年 4 月に電子認証制度を導入するという発表をを行いました。昨年も同じ話題があり PKI(Public Key Infrastructure) 元年だと噂していたのですが、実際はそこまでの普及に至りませんでした。1999 年 11 月に、政府が電子署名法案(仮称)の骨格を固め、電子認証局の資格を民間に与え、そこに認証業務を委託するという話が出てきています。現在、日本で商用の認証局がきちんと機能しているとは言い難いのですが、公的に電子認証、電子署名を利用するという動きになってきています。これが実現されますと、電子メールでの商取引が現実性を帯びてきます。

3 電子メールの技術動向

前のキーワードで説明した状況を背景に、次に、電子メールの技術動向を説明します。

3.1 従来からの技術

従来から使われている電子メールの技術には、以下のものがあります。

・SMTP(Simple Mail Transfer Protocol)
・POP3(Post Office Protocol) & APOP
・MIME　- RFC2045-RFC2049
・POP before SMTP
・S/MIME、PGP(PGP/MIME)
・IMAP4rev1 (Internet Message Access Protocol)- RFC2060
・LDAPv3(Lightweight Directory Access Protocol) - RFC2251-2256

SMTP など、MTA-MTA 間の通信手段としての基本的な技術はほとんど枯れており、ESMTP、AUTH-SMTP という技術の発展はありますが、今後 SMTP 単体での急激な発展はないと思われます。

POP before SMTP は、明確なプロトコルではなく暫定的な SPAM 対策の手段です。いずれ破綻し、SMTP AUTH に移っていくと予想されます。

MIME は、メッセージのフォーマットとしては確立されており、拡張が続いていますが、新しい技術というよりは、問題点を解決している段階にあるという理由で、従来の技術に入れています。

LDAP はメールと直接の関係はありませんが、証明書を LDAP で管理したり、LDAP でユーザ管理を行うなどが考えられ、電子メールの様々な技術と関連してきています。SMTP、POP、IMAP、LDAP のセッションをそれぞれ SSL で暗号化するという動きも出てきています。

3.2 今年も継続している技術

従来の技術の中で現在も使われている、そして今後も使われるであろうと予想される技術です。現在注目を集めている技術ということになります。

・IMAP4rev1
・S/MIME,PGP(PGP/MIME)
・LDAPv[2 | 3]

IMAP4 は、今まで大手 ISP がサービスしていなかったものですが、今年から NTT ドコモのモペラで IMAP を採用し、IMAP メールという形で IMAP メールサービスを開始しています。各 ISP が従来のフリーのメールソフトから商用のメールサーバに切り替えを進めていますので、それら商用メールソフトが IMAP4 に対応していることもあり、他の ISP もサービスを始めるのではないかと予想しています。

LDAP を、電子メールと連携して使用するという方法はまだ普及していません。しかし、Netscape Communicator のローミング機能は実際に LDAP を利用していますし、ユーザ管理や S/MIME および PGP の公開鍵管理を LDAP で実現しようという動きが出てきていますので、今後、新しい技術が出てくると思われます。現在 LDAP のスキーマについて統一された方向性は出ていませんが、今後統一の動きが出てくると思われます。

3.3 今年のトピックス

今年のトピックスは以下のものです。

(1) SMTP AUTH(RFC2554)- SMTP Service Extention forAuthentication

メール送信については、従来の方法では、一切認証のない形で行われていました。そのため、SPAM から MTA を不正中継に使われていたわけです。その防止策として、SMTP AUTH はメールを送る時に事前に認証しようというものです。

SMTP は従来 MTA-MTA 間で使われ、この間は UNIX システムが使用されていますので、ここにログインする人は限られており、認証がなくても大丈夫な世界でした。しかし、インターネットが普及し、PC クライアントの POP3 が出現すると、MUA から MTA を直接アクセスすることも可能になり、MTA 側での認証が必要になってきました。

MTA に SMTP での認証が実装されると、送られるメールに関しては確実に認証されることになります。将来的には、認証部分に X.509 証明書ベースの認証が得られれば、認証自体にセキュリティがかかるようになります。

(2) MDNs(RFC2298)- Message Disposition Notifications

MDN は、相手がそのメールを開いたかどうか、開封確認をするものです。MUA 側に実装します。MDN を実装しているところはまだ少ないのですが、Netscape には実装されています。

(3) DSNs(RFC1894)- An Extensible Message Format for Delivery Status Notifications

DSN はメールの到着確認機能で、実際にメールが相手のメールボックスに正しく届けられたことを通知するものです。MTA 側に実装します。

送信者から出されたメールは、MUA から MTA に送られ、そこからさらに次の MTA、次の MTA という具合にリレーされ、最後に受信者の MUA に到達します。DSN が、最後のメールボックスに到達したことを通知し、MDN が、到達したメールを相手が開封したことを通知します。従来、Return-Received-To があり、これは送られた MTA 全てから確認が返ってきましたが、DSN は最終的に到達したメールボックスから返ってきます。

DSN、MDN の実装に関しては、MUA が MDN を返そうとした時に、既に送り返してしまったメールに対して応答を返したり、メーリングリストに MDN 付のメールを出した時にメーリングリスト参加者全員から MDN が帰って来たり、また MDN を送るとそれに対して MDN が帰ってきてループが発生したり、という問題の発生が考えられます。その問題を解決するためにも互換性テストが必要になります。1999 年 3 月米国サンノゼで開催された Internet Mail Consortium 主催の「Mail Connect 5」では互換性テストも行われていましたので、次回は我々も参加する予定です。

移動しながら利用することのできる、携帯電話のメールは便利なはずですが、無線のため不安もあります。DSN と MDN を組み合わせて確認が取れるようにすると、面白いサービスができると予想しています。

4 携帯電話がやってきた

今年の一番大きな話題に携帯電話があります。CDA や WAP の数は 20-30 万台の規模ですが、携帯電話は 500 万（来年 3 月の予想）という爆発的な数の広がりを見せていますので、「i モードメール」の利用者数の膨大な増加が予想されます。つまり、今までの利用者とは違った人達が電子メールを使うようになり、遊びの要素が強い電子メールが広がってきています。インターネットのメールとキャリアのメール相互間でメールの転送が生じる環境では、セキュリティがますます重要になってきます。

4.1 電子メールにひとつの切り分け

携帯電話電子メールの出現によって電子メールの利用形態が、
「ビジネスでの電子メール」と、「遊びの電子メール」とに分かれてきました。

ビジネスで電子メールを利用するユーザはセキュアな運用管理を求めていますが、遊びの電子メールを利用するユーザはそうではありません。例えば、企業の人事関係のメールが携帯電話会社（キャリア）に転送されたら大変です。特に、携帯電話会社のサーバにトラブルがあり、エラーでどこかに送信されてしまうという状況が発生すると、怖いことが起こると思います。

企業内では、電子署名や暗号の対応を既に実施中の会社もあるでしょうし、検討中の会社もあると思います。ところが、電子署名をしたり暗号化をしたりして作成したメールを携帯電話に送っても電子署名を認証できないとか復号できないということでは、意味がなくなってしまいます。

企業側は、電子メールを重要な通信手段としてよりセキュアな環境で利用する動きをしているのに対し、携帯電話は手軽な故にそれらが無視されてきています。

携帯電話同士がメールのやり取りをしている内はまだ良いのですが、携帯電話には、「文字数の制限」があったり「添付ファイルが使えない」ということがありますので、携帯電話のメールと従来のメールとの間でやりとりすると互換性がとれないことになります。

従来のメールの互換性に関して、各クライアント間のトラブルが最近やっと少なくなってきましたが、膨大な数の携帯電話の登場によって、メール互換性の問題がもう一度出てくると思います。電子メールの標準を見直す必要が生じてきたと思います。

4.2 電子メール転送の恐怖

電子メール転送の恐怖というのがあります。社内の電子メール、あるいは ISP 経由の電子メールを携帯電話に送った時、電子メールを携帯電話で読もうとすると、発信元のメールボックスを全てキャリア側のメールボックスに転送しなければなりません。キャリアのメールシステムで配送の遅延が発生しても利用者はなかなか気付きません。電子メールを送ったのに相手には、届いていないという現象になります。ビジネスの世界ではこのようなことは許されません。

携帯電話でメールが使えるのは、外出中でもメールが読め便利なわけですが、この便利さに頼りすぎるとトラブル時に大変なことになってしまいます。

4.3 電子メールを安全に読む方法

携帯電話を使って電子メールを安全に見る方法を考えてみました。電子メールのメールボックスを転送する時にコピーを送る方法があります。同じメールを２ヶ所に持つわけです。そうすると２ケ所の電子メールの内どちらでも見ることができるので安全です。しかし、同じメールが 2 ヶ所にあるので混乱しそうです。そこで、WebMail のような形式でセキュリティを考慮した上で、企業側およびキャリア側が相互に相手を見れるような方法を取れば、安全を確保しながらメールを読むことができるので良い方法ではないかと考えています。

4.4 次なるサービス大胆予想

携帯電話の電子メールは可能性が大きいので、次なるサービスを大胆予測してみました。

携帯電話会社（キャリア）による電子メールサービスは出揃いました。競っているのは受信可能文字数、保存日数だけですが、これは電子メールの本質とは違います。インターネットで誰とでもメール交換ができると謳うのなら、これらの制限があるのはおかしいと思いますし、MIME は処理して欲しいと思っています。競って欲しいのは、電子メールのサービスあるいは管理面です。

現在携帯電話各社のサービスは、完全に横並び状態ですが、次なるサービスは何だろうかと期待しているところです。特に、携帯電話の電子メール利用者層は従来のパソコンでの電子メール利用者層と違い、携帯電話を買ったらメールが付いてきた、インターネットに触れてみたいので使おうという利用者が多いのではないかと思います。また、圧倒的な数

の利用者なので、これらの人達からどんな要求が出てきてどんなサービスを提供することになるのか興味のあるところです。当然これらの要求、提供サービス対して、従来のメ－ルソフトおよびメールサーバのメール管理方法などにも影響があるのではないかと考えています。

5 電子メールの危険性

従来の電子メールに加えて携帯電話の電子メールが広がる中で、「プッシュ型広告」としての電子メールの利用など、ビジネスに電子メールが使われてきていますが、電子メールには危険性も含まれています。

電子メールにおける危険性には、以下のものがあります。

- 盗聴(経路上での盗聴)
- 盗聴(コンピュータ内ファイルの盗聴)
- メール爆弾
- 不正中継
- なりますし
- なりすましスパムメール
- 改ざん

● 盗聴(経路上での盗聴)

経路上での盗聴ですが、技術的には十分可能です。インターネット経路上の盗聴よりは社内での盗聴の方が危険です。近くのハブに PC や UNIX マシンを接続してパケットをキャプチャするようなソフトは沢山あるので、社内での盗聴の方が技術的には簡単です。実際には経路に流れている大量データの中から自分の必要なデータを選択することの方が大変で、経路上の盗聴は言われる程には怖くないと思っています。通信傍受法も１つの盗聴ですが、同じ悩みを持つと思います。

● 盗聴(ファイルの盗聴)

ファイルの盗聴、ファイルの覗き見です。メールの場合、メールサーバのスプールが対象になりますが、見られたくないメールは暗号化してしまえばとりあえず対応できます。従来の SendMail など UNIX の標準のファイル形式を利用したスプールですとファイルの位置は一目瞭然なので、サーバにログインさえできればスプール内のメールを簡単に覗くことができます。しかし、商用のメールソフトは専用あるいは商用のデータベースを利用しているのでファイル構造が複雑になり覗くのは困難になります。

それから中継途中でのメールサーバのファイルですが、中継する全てのサーバが安全とは限らないので、DNS のセキュリティホールを狙われて

MX を書き換えられ、メールを別のところに転送され盗聴されるようなこともありえます。

PC に保存されているデータも簡単に狙われるので注意が必要です。

● メール爆弾

最近はあまり聞かなくなりましたが、大量のメールを送りつけたり、サイズが大きなメールを送りつけたり、沢山のメールを一斉に送りつけ大量のセッションを張り、相手のメールサーバを使用不能にするのがメール爆弾です。

POP を使用してメールを全て PC に取り込む方法では、受信する PC 側も使用不能になる可能性があります。

● 不正中継

メールサーバを SPAM の不正中継に利用されてしまうと、サーバの負荷が高くなり、本来の業務に支障がでることもあります。他社から苦情が来て、企業の信用を落とすことも大きな問題です。最近ではほとんどのサーバは「不正中継対策」を行なっているので SPAM は少なくなりました。ほとんどの商用製品は不正中継対策機能を装備しているので、設定さえ正しければ不正中継に利用されることはありません。

● なりすまし

なりすましという問題があります。発信人を他人になりすまして電子メールを送信することで、なりすまされた側と受け取った側の信頼感が損なわれるので、なりすましは電子メールにとって一番怖い存在です。

まず、特定個人になりすますことがあります。「会社の役員を名乗って広告メールが数千通送信され、その役員の元に 3 日程苦情メールが殺到した」という事例があります。そして、企業などの代表アドレス（例えば webmaster@会社名.co.jp）になりすますことです。商用メール(メール新聞、メールマガジン)になりすまして、嘘の号外を流すことも可能になります。

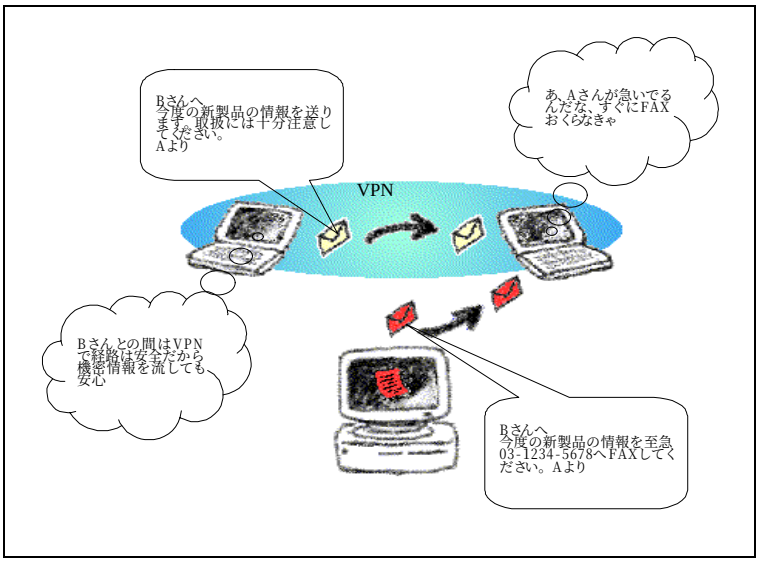

図 1：なりすましの例

企業のなりすましでは、EC (電子商取引)向けのものが大きな課題になります。電子メールで商取引をする際に、なりすまされると大変なことになります。これに対しては「電子署名」が解決のキーポイントになります。主要なメールソフトには、既に電子署名のしくみが組み込まれていますが、それにも関わらず、これは実際にはほとんどの企業で使用されていません。電子メールには、電子署名を使ういう運用ルールにすると良いと思います。

なりすましでスパムメールが送信されることもありますが、これには対処のしようがありません。しかし、会社の運用ルールとして電子署名を義務付けていると、電子署名のないメールは自分の会社から発信した電子メールではないと主張することができます。

● なりすましスパムメール

なりすましのスパムメールが怖いのは、いつ被害に会うかわからないこと、実際に送信されていてもなりすまされた自分達は気づかないことにあります。急にエラーメールが沢山送られてきて、最初は何が起きたのかわからなくて驚くのですが、後で実はなりすまされたスパムメールが発信されていたと気付くことになります。

自分が出したのではないと証明する方法はありますが、直接防止する対策はありません。

● 改ざん

改ざんは、送信されたメール内容を変更するものです。電子商取引で注文数量や金額が改ざんされたら大変なことになります。改ざんされる場所としては、「送信時のメールサーバ」、「相手先のメールサーバ」、「中継中のサーバ」、「受信後の自分の PC」が考えられます。

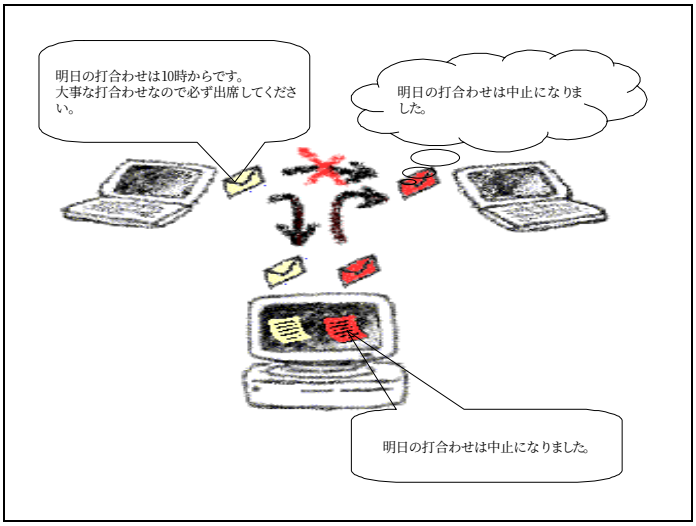

図 2：改ざんの例

これら電子メールの危険性の根本原因は現在のインターネットによるメールシステムの脆弱さにあると思います。

6 IMAP4

メールの一元管理として、IMAP4rev1(Internet Mail Access Protocol)の説明をします。従来、グループウェア(Domino、Exchange など)ではメールの一元管理を行っていましたが、インターネットの場合は POP を使ってメールサーバから個々の PC にメールを取り出し、後は PC 側で個々にメールの管理をするという方法を採用していました。IMAP はインターネットの標準的なプロトコルでメールをサーバ側で一元管理するものです。

今まで IMAP は ISP がサポートしていませんでしたが、今年から大手キャリアを含めてサービスが始まりましたので、これから本格的に普及すると予想されます。

● IMAP4

IMAP という場合は、IMAP4 rev1 RFC 2060 を指します。

商用メールサーバ製品では IMAP のサポートは当たり前の状態になってきましたが、その実装に関しては様々なものがありサポートレベルの差があります。

IMAP では、メールの保存管理はサーバ側で行い、未読/既読の管理、フォルダの管理の機能を持っています。メールのバックアップはサーバ側で行うので、各自が PC 側でそれぞれバックアップを行う必要がなくなりました。個人 PC 側の負担を軽くしたり、見積書など個人のみでなく企業でも管理したいものをサーバ側で管理できるので便利な機能です。

● MailConnect 5 – イベント

今年 3 月、米国サンノゼで MailConnect 5 というイベントが開催され、IMAP4 以外に DSN、MDN のテストも行われました。3 日間開催されたイベントの初日に MDN と DSN のテストが行われましたが、MDN と DSN のサポートは広がってきているようです。

IMAP4 に参加しましたが、ここでは日本語の検索について皆興味を持っていました。私は、IMAP4 の Language Extension のテストをしました。Language Extension のドラフトは draft-gahrns-imap-language-00.txt に書かれたのですが、実際の実装としてはこれが始めてです。

このテストに参加している人達は、商用メール製品の開発段階の新機能をテストしており、実際に販売されている商用製品の性能試験をやっているものではありません。

● Language Extension 機能

Language Extension とは、サーバからの応答メッセージを各国の言語(例：英語「Password Error」、日本語「パスワードが間違っています」)で返すよう、言語指定できる機能です。

当初は、このような機能を加えなくてもサーバからコードを返せば良いのではないかと考えていましたが、サーバの実際のエラー状況を詳細にコード化するのは困難だとわかり、このような機能も必要であると感じています。

これを実装すると、相手が日本人の初心者でも、「パスワードが違います」とメッセージを日本語で出したり、「○○なので管理者に連絡して下さい」、「○○なので内線 XXX に電話して下さい」という具合に、日本語で詳細な指示が出せ、ヘルプデスクではエンドユーザへのサポート対応が軽減されると思います。

● Messaging Interoperability Japan – イベント

MailConnect 5 は米国で開催されたものですが、米国まで行ってテストをしたりするのは大変ですので、日本で Messaging Interoperability Japan というイベントが開催されました。業界内部のイベントで、開発者同士が集まりメールの互換性テストを行いました。

1999 年 4 月 7-8 日に IRI(インターネット総合研究所)で開催されました(10 社が参加)。

Messaging Interoperability Japan の参加社とプロダクトです(順不同)。

・日本電気株式会社 (ExpressMail)
・日本電気テレコムシステム株式会社 (WeMail32)
・カスタム・テクノロジー株式会社 (N-PLEX)
・日本ネットスケープ・コミュニケーションズ株式会社
(Netscape MessagingServer、Netscape Communicator)
・アライドテレシス株式会社 (AT-Mail Server、AT-承認メール)
・ロータス株式会社 (Domino、Notes)
・株式会社オレンジソフト (Winbiff)
・株式会社クニリサーチインターナショナル (Eudora)
・株式会社ケイ・ジー・ティー (IMail Server for Windows NT)
・コンパックコンピュータ株式会社 (Software.com 社製 InterMail)

ここには開発者が集まり、製品出荷前に相互接続テストを行うことによってバグを潰したり、RFC の読み違いがないかを確認しました。

電子メールシステム運用中にトラブルがあっても製品のエラーなのか設定のエラーなのか原因がわからないケースが多いので、このように開発元の技術者同士が集まって事前に確認するのは非常に有意義なことです。

この時のテスト結果を踏まえて、Interop の Message Solution コーナーで、メールの接続展示を行いました。

● Messaging Interoperability Japan 2nd – イベント

さらに、1999 年 11 月 8-9 日第２回イベント(Messaging Interoperability Japan 2nd)が電通国際サービスで開催されました。

そこで確認した内容は次のとおりです。

- ◆ 検索機能の実装明確化
  - ・サポート文字コードの確認
  - ・Encode、Contents-type での検索可否
  - ・Line Break(行にまたがる文字)の検索可否
- ◆ 共有フォルダの実装明確化
  - ・ネームスペースの実装可否
  - ・未読／既読管理はホルダー単位か個人単位か

また、意見が一致した内容は次のとおりです。

- ◆ IMAP サーバでの日本語対応時の実装ガイドライン
  (文字セットは ISO-2022-jp)
- ◆ 添付ファイルのファイル名長(RFC2231)
- ◆ Accept Language への対応(ドラフトはこれから)

詳細は、日本インターネット協会からリンクが張られるはずです。

● IMAP4 だけなぜいじめられるの？

IMAP に関して次のようなことが噂されています。

・IMAP にはセキュリティホールがある？
・サーバに HDD が無限に必要？
・IMAP はスケールしない？

IMAP はプロトコルなので、スケールするかしないかはファイルやデータベースの実装次第です。このような噂は、基本的に情報の不足が原因です。

● IMAP4 は重い？

メールが多くなるとファイルが大きくなり開くのが重くなる、と言う人がいますが、これはメールボックスが UNIX の mbox 形式でのことを言っています。同じフリーソフトでも cyrus ではかなり改善されています。IMAP はプロトコルですが、プロトコルとデータの操作は分けて考える必要があります。ファイル(メール)へのアクセス速度は実装に依存します。検索などの速度も実装依存です。製品(ソフト)をしっかり吟味する必要があります。

「cyrus imapd」のファイルの実装例を以下に示します。

```
-rw-----        1 cyrus  mail   6662756  May 21  21:09  cyrus.cache
-rw-----        1 cyrus  mail       136  Feb  8  20:27  cyrus.header
-rw-----        1 cyrus  mail    426444  May 21  21:09  cyrus.index
-rw-----        1 cyrus  mail        53  Feb  8  20:36  cyrus.seen

-rw-----        1 cyrus  mail       402  May 21  21:09  8200.
-rw-----        1 cyrus  mail    438674  Mar 30  08:28  8199.
-rw-------      1 cyrus  mail    179410  Mar 30  08:28  8198.
-rw-------      1 cyrus  mail     66076  Mar 30  08:28  8197.
-rw-------      1 cyrus  mail     66319  Mar 30  08:28  8196.
-rw-------      1 cyrus  mail    152660  Mar 30  08:28  8195.
-rw-------      1 cyrus  mail     43279  Mar 30  08:27  8194.
-
```

7 S/MIME・PGP

電子メールを守る技術ということで、S/MIME、PGP という暗号技術を紹介します。

● 暗号メールの基本

なぜ、電子メールに暗号が必要かといいますと、理由は明確です。盗聴に対し暗号で防御できるからです。

ファイアウォールでは守れないのか、と聞かれることがあります。しかし、電子メールはファイアウォールを通過してやって来ますので、電子メールの安全はファイアウォールでは守れません。SMTP、POP、IMAP4 はファイアウォールを通過して通信します。

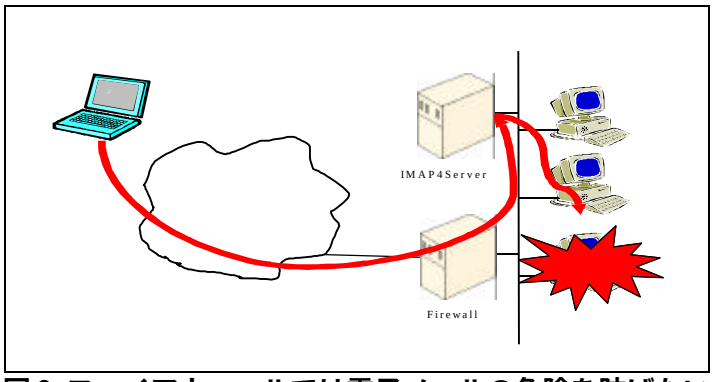

図 3:ファイアウォールでは電子メールの危険を防げない

・暗号化すれば安全か？
・暗号は破られないのか ？

という質問には、何もしないよりは安全だと言う答えになります。

暗号を使用することで、自分が出したメールでないことを証明、つまり他人が自分のアドレスを勝手に使用してなりすまされることの防止もできます。

● 暗号に必要な技術

暗号技術には次のものがあります。

① 共通鍵暗号
　　DES、3DES、RC2、RC4、IDEA、MISTY、FEAL
② 公開鍵暗号
　　RSA、Diffie-Hellman、ElGamal
③ ハッシュ関数
　　SHA-1、MD5

● 共通鍵暗号と公開鍵暗号

「共通鍵暗号」は、お互いが同じ鍵(共通鍵)を使用する方式で、平文を共通鍵で暗号化して相手に送り、相手は共通鍵で暗号文を平文にします。共通鍵の受け渡しや鍵の保管が問題になりますが、処理速度が速いという特徴があります。

「公開鍵暗号」は、秘密鍵と公開鍵の 2 つを使用する方式で、公開鍵は公開しますが、秘密鍵は個人が管理します。まず、送信者は受信者の公開鍵で平文を暗号化して相手に送り、メールを受け取った相手(受信者)は受信者の秘密鍵で暗号文を平文に復号します。処理速度は遅くなります。

● 暗号化

実際の暗号化は処理速度の違いを考慮して公開鍵暗号と共有鍵暗号を組み合わせて次のように行っています。

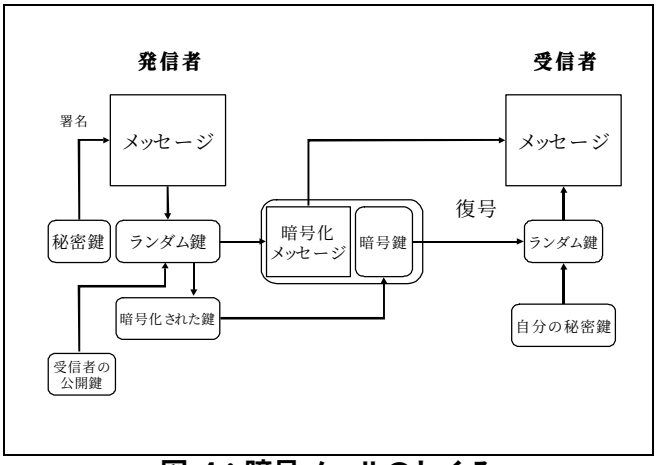

図 4：暗号メールのしくみ

発信者は、メッセージをランダム鍵で暗号化すると共に受信者の公開鍵を使ってランダム鍵を暗号化し、暗号化されたメッセージと鍵を送りま

す。受信者は、自分の秘密鍵で暗号化された鍵を復号してランダム鍵を作り、そのランダム鍵を使ってメッセージを復号します。

● 電子署名のしくみ

電子署名は、発信者が間違いなくメールを書いた当人であることを証明するためのものです。送信者が自分の秘密鍵で暗号化し、受信者が送信者の公開鍵で復号する方法を取り、もし間違いなく復号できたら送信者を確認できる原理を使用しています。

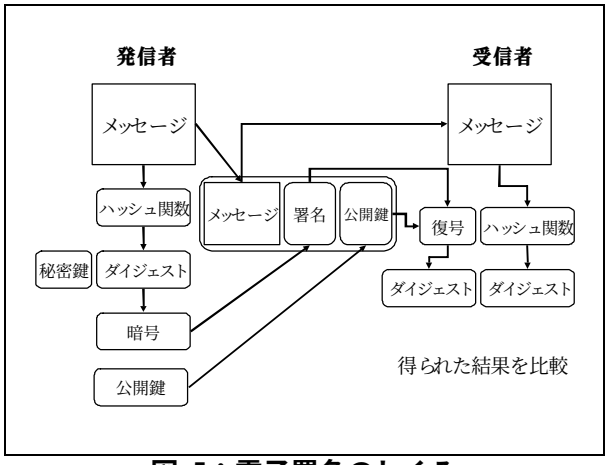

図 5：電子署名のしくみ

発信者は、メッセージのハッシュ関数からのダイジェストを発信者の秘密鍵で暗号化しメールに署名として添付ます。受信者は署名を発信者の公開鍵で暗号化されたダイジェストを復号したものと、メッセージのハッシュ関数からのダイジェストを比較し、これが一致すれば同一人であることが確認されます。

● S/MIME と PGP の認証の違い

認証の仕方の違いを、S/MIME、PGP を例に取り示します。

PGP は、お互いが信用に基づく"信頼の輪"でもって、公開鍵に対する認証を行う方式を取ります。つまり、私(A)が信用できる人(B)が信用している人(C)なら、私(A)もその人(C)を信頼しましょうというものです。

S/MIME は、信頼できる機関(CA 局)に認証を依頼するもので、CA 局の発行した証明書で公開鍵を認証します。Netscape Communicator、Outlook Express、Winbiff などには既にこの機能が具わっています。

● 認証局をどうやって信用するか

S/MIME を使っていて問題になるのは、認証局をどうやって信用するかということです。現在メーカーは認証局の公開鍵をプログラムに組み込んで出荷しています。メーカーは認証局と契約してプログラムに公開鍵

を入れているわけですが、問題なのはその公開鍵の認証期限が切れた時更新する方法があるかどうかということです。

認証局の証明書が切れた時にどうなるかというのが、S/MIME の一番の問題です。A という認証局と B という認証局を経て C さんが認証されたとします。その時、A の期限は切れていないが C の期限は切れている、C の期限は残っているが A の期限は切れている、という具合に認証チェーンの期間が切れた時どう対応するかということです。

S/MIME の実装としては自分のすぐ上の認証局の証明書はそのメッセージに添付して送るのですが、さらにその上の階層でトラブルが起こった際に、認証局の証明書の期限が切れた時、あるいは、秘密鍵が交換された後にトラブルが起きた時、どういう具合に運用するかが問題になると思われます。

● 秘密鍵の管理

秘密鍵の管理については、次のような課題があります。

- 各クライアントで生成するか？
- 管理者がまとめて生成するか？
- 秘密鍵の管理はユーザまかせか？
- 鍵を紛失した時の対応は？
- システム管理者が全員の鍵を管理するか？
- 誰の権限で管理するか？

これらを防止するために、キーリカバリ、キーエスクロという方法があり、一個の鍵でどんなメッセージでも開くようにしておく対策です。

S/MIME で秘密鍵の管理を実現する場合、今一番確実なのはキーエスクロで、各個人の秘密鍵を管理者が全部保管しておき、いざ内容を見なければならない時には誰かの権限でメッセージを復号することができるようにする方法です。

● CRL の運用

公開鍵は、認証局の証明期限切れとは別に、次のような場合無効にする必要があります。

- 秘密鍵の紛失
- 証明書の期限切れ（認証局証明書の期限切れ）
- 退職など
- 秘密鍵を盗まれる

その無効になった証明書のリストがCRL(Certification Revocation List)です。

CRL の扱いについては次のような課題が存在します。

・どのように配布するのか？
・いつ配布(取得)するのか？
・オフラインの時はどうするのか？
・すべての CRL を公開しても良いのか？
・個人情報をどこまで開示可能か？

● 日本語での問題

日本語の文字セットの扱いについては当初トラブルがありましたが、電子署名は ISO-2022-JP を使用し、MTA による文字セットなどの書き換えは行わないことになって、最近はトラブルがほとんどなくなりました。

8 まとめ

● 今後の普及に期待

メールの開封確認（MDNs：RFC2298)、配送確認（DSNs：RFC1894)の機能が実装できる段階にきました。今後の普及に期待しています。また、これらにも電子署名が必要になると思います。

● 配達通知,開封確認は必要か?

配達確認、開封確認は、従来グループウェアでは可能でしだが、インターネットメールではできないと言われてきました。しかし、インターネットメールにも MDN、DSN の機能が実装されることになり利用可能になっています。

実装に際して、開封確認を取られたくない場合もあります。クライアント側で開封確認を出すか否かを選択できる必要があります。

● SMTP での認証の必要性

SMTP は、本来は MTA-MTA 間の転送が目的でしたが、POP3 の出現などにより MUA も SMTP を使い始めました。しかし、認証がないので誰でも利用でき、スパムに利用されてしまうような事態が生じています。POP before SMTP が登場しましたが、間に合わせの方法のため、SMTP AUTH を実装すべきです。

インターネットの脆弱さをなくすためにも、まず SMTP での認証が不可欠だと思います。

● 電子メールは相互接続が重要

電子メールで一番重要なことは、相互接続性です。サーバ、クライアント間の接続として SMTP、IMAP、LDAP を、End To End の接続として MIME、S/MIME を使っており、接続性の検証がされてきました。今後携帯電話のメールが加わることにより、電子メールの利用者は増える一方で、しかも利用者のほとんどが一般ユーザになっています。

それら全てを含めて、相互接続ができるよう互換性を取っていかなければ電子メールは破綻してしまいます。 今後も様々な接続テストなどを継続して実施していきたいと思います。

9 Q&A

Q : 携帯電話で電子メールを使っていたらメッセージ ID が閉じていなかった。RFC ではそのことについて何か規定されているのかどうか？ メッセージ ID が不正なまま使用されている中で何かトラブルが生じることがあるのか？

A : メッセージ ID はきちんと閉じるように RFC では規定されています（RFC822 のメッセージスペシフィケーション）。メッセージ ID が不正な時のトラブルは、同じメッセージが判断できなくなることと、メールのリファレンスが狂うことが考えられます。

Q : MDN に関して、Peer-to-Peer では有効ですが、メーリングリストのように 1 対 N の場合には有効ではないと考えますがいかがでしょうか？

A : その通りだと思います。

Q : 学校関係者ですが、学校では PC を不特定多数が使うという状況の中、POP だとトラフィックが二重化するという理由で、IMAP を使用しています。 最近 WebMail を学内で使用した方がより良いのではないかという話が出てきています。先程の説明の中に、会社のメールを携帯電話に送ると複数のメールができ一元化できないという話がありましたが、社内に WebMail サーバを置いて利用すれば先程の問題は一部解決するのではないかと思いました。今後 WebMail はどの位普及するでしょうか？

A: 今、クライアントがありサーバは IMAP でメールを一元管理している状況を考えた時に、WebMail になるということではなくて、IMAP のメールを WebMail として読むことになるのです。ですから、WebMail で見るか、普通のクライアントから見るかは利用する人の自由になります。私の会社としては、クライアントから見る時は IMAP で見るし、携帯から見る時は WebMail 形式で見るという解決策をとっています。そしてキャリアのゲートウェイと WebMail の間は SSL を張るということもやっています。

Q : IMAP での日本語検索について、良いサーバに良いクライアントを選べば大体普通の人ができて欲しいと思う検索ができるのか？、あるいは、そういう状況を作るには設定など様々な要件を考える必要があり、まだ現状では難しいのか？どちらでしょうか？

A : 個人的な意見として、良いサーバと良いクライアントを選べば大丈夫です。

Q : IMAP のプロトコル上で検索文字列が送られる時は UTF8 になって送られるのでしょうか？

A: いいえ、検索文字列を送る時はサーチで任意に文字セットを指定できます。