平成一一年一月一日発行（毎月一日一回発行）

經濟論叢

第163巻　第1号

定道　宏教授記念號

平成11年1月

京都大學經濟學會

経済論叢（京都大学）第163巻第1号，1999年1月

インターネット時代における グループウェア・メール

高　井　才　明

I　は　じ　め　に

グループで分業・協業を行う場合，グループメンバー間でさまざまなコミュニケーションやスケジュール調整，ワークフロー管理などを行う必要がある。そのようなグループ協業を支援するコンピュータ・システムあるいはソフトウェアをグループウェアと呼ぶ。グループウェアには支援するグループの形態などによってさまざまな支援ツールが必要となるが，なかでも電子メールは，グループメンバー間のコミュニケーションを支援する基本的ツールとしてグループウェアに必須のツールである。

我国における電子メール環境は，インターネットの普及により大きく変化してきた。初期のインターネット・メールでは，異なるメール・システムを採用したネットワークが混在した環境にあり，ネットワーク間でメールを使用する際にはユーザ側で注意が必要であった。定道［1993］は，当時の国内のインターネットとその相互接続関係を概観し，BITNET などの異なるメールシステムを採用したネットワークが混在しているためにインターネット・メールを利用する際にはユーザ側でネットワークの接続関係を意識して利用しなければならないという問題があることを指摘している[1]。その後インターネットは急速に普及し，商用パソコン通信や各組織の LAN などのさまざまなネットワークと相互接続されてきたが，現在ではほぼ全てのネットワークで SMTP を前

1）定道宏［1993］，1-10ページ。

提とした環境が整いつつあり，ユーザはネットワーク間の相違を意識することなくインターネット・メールを送受信できる環境となってきた。個々の組織においても，インターネットが普及するにつれ，ローカルなネットワークとインターネットとの接続性を確保するために，従来のLAN環境からインターネット技術を利用したイントラネットおよびエクストラネットが主流となりつつあることから，インターネット・メールを指向した電子メール・システムの構築が主流となっている。

他方では，WWW技術の発展によって，インターネット・メールの機能そのものも拡張されてきた。インターネットにおいては，1995年頃よりWWWをはじめとするマルチメディア情報処理技術が急速に発達した。これに刺激されて電子メールにおいてもマルチメディア情報に対応すべく拡張がなされてきた。また，インターネット・メールのユーザの増加により，セキュリティが重要な問題となってきている。これを受けてインターネット・メールにおけるさまざまなセキュリティ技術が提案されている。

本稿では，まずインターネット・メールの変遷およびセキュリティの現状を展望したうえで，インターネット時代におけるグループウェア・メールとしてWebメールを提案し，その役割と有用性について検討する。

II　グループウェアにおける電子メール

グループウェアとは，「共有化環境へのインターフェースを提供し，共通の作業（または目標）に従事しているグループのメンバーを支援するコンピュータベースのシステムである」[2]。すなわち，なにか共通の目標に向けて協業作業を行っているグループのメンバー間で情報を共有するための環境を提供し，グループ協業を支援するようなハードウェアおよびソフトウェアからなるシステムである。

DeSanctis & Gallupe [1985] によるとグループ支援の形態は，そのグルー

2) Ellis, A., Gibbs, S. J. and, G. L. Rein [1991], p. 38.

図1　グループウェア時間／空間マトリックス

空間＼時間	同じ（リアルタイム）	異なる（非同期）
同じ（同一地域）	会議のサポート	（LAN を前提とした） 電子メール 電子掲示板
異なる（遠隔地）	遠隔会議 ＴＶ会議	（WAN を前提とした） 電子メール・電子掲示板 共同執筆 ワークフロー管理

プが置かれている空間的時間的環境によって，図1のような4つのカテゴリに分類できる[3]。

グループで分業・協業を行う場合，グループのメンバーが同時に作業を行う場合と各メンバーがそれぞれ都合の良い時間に作業を行う場合がある。またメンバーが同じ場所に集合して作業する場合と各々が複数の離れた場所に分散した状態で作業を行う場合がある。これらの組合せによって，グループ協業環境は，リアルタイム・同一地域型，リアルタイム・遠隔地型，非同期・同一地域型，非同期・遠隔地型に分類できる。この分類によれば，電子メールを利用したコミュニケーション支援は，非同期型のグループ支援に適していると言える。

ところで，電子メールは，使用されるネットワークのスコープ（範囲）によって(1)ホスト型メール，(2)イントラネット型メール，(3)エクストラネット型メール，(4)インターネット型メールに分類できる。ホスト型メールは，Bitnet やパソコン通信に見られるような，ホストコンピュータに接続された端末間で用いられるメッセージ交換システムである。イントラネット型メールは，イントラネット環境，つまりファイアーウォールで守られた組織内ネットワーク上のユーザ間でのメッセージ交換を意図したメール・システムである。エクス

3）DeSanctis, C. G. and B. Gallupe [1985], pp. 195-197. また，Johansen はグループウェアによるグループ支援の17のケースをこのカテゴリに分類している。Johansen, R. [1988], pp. 12-44.

トラネット型メールは，エクストラネット環境，つまりイントラネット内およびインターネットを介した特定のイントラネット間でのメッセージ交換を意図したメール・システムである。インターネット型メールは，TCP/IP (Transmission Control Protocol / Internet Protocol ; RFC 793, RFC 791) に準拠したインターネット環境で用いられるメッセージ交換システムであり，RFC 821 (1982) に提案されている SMTP (Simple Mail Transfer Protocol) によるメールである[4]。

従来は，同一地域型に属するグループウェア・メールとして組織独自の LAN を前提としたメール・システムが，また遠隔地型に属するグループウェアには，専用線を用いた組織独自の WAN を前提としたメール・システムが用いられてきた。これらは通常その組織が採用しているネットワーク環境および OS あるいはグループウェア製品が前提としているプロトコルに準拠したメール・システムを利用するのが一般的であった。

ところが，近年，企業においてインターネット環境が普及し，組織内ではイントラネット環境が，特定範囲の組織間ではエクストラネット環境が主流となりつつあることから，OS やグループウェア製品独自のプロトコルによるメール以外に TCP/IP および SMTP に準拠した電子メールの利用要求が増してきた。これを受けて従来独自のプロトコルによるメール・システムを提供していた OS やグループウェア製品などでは，サーバにゲートウェイ機能を付加したり SMTP サーバ自体を具備することによって従来のメールに加え SMTP によるメールにも対応したメール・システムを提供するようになってきた。

4) Postel, J., (RFC 821, 1982) インターネット上で用いられる標準プロトコルや規格，情報などは，RFC (Requests For Comments) と呼ばれる文書に記述される。RFCには，登録された順に番号が付され，一旦登録された文書は直接変更せず，改訂されたものがあらたに番号が付されて登録される。RFCには，標準化の行程レベルによって，Standard, Draft Standard, Proposed Standard, Informational, Experimental, Historicのようにレベルわけされ，その標準が要求されるレベルによってRequired, Recommended, Elective, Limited Use, Not Recommended に分類される。RFC の詳細および原文は，http://www.rfc-editor.org/rfc.html を参照。

たとえば，Microsoft 社の Exchange では，Exchange Server に SMTP ゲートウェイである Internet Mail Connector を標準で装備し，自社独自の NetBEUI プロトコルに準拠したメール・システムである Microsoft Mail や Microsoft Fax，The Microsoft Network による通信に加えインターネット・メールも統合的に利用できる環境を提供している。Exchange では，Windows 上のアプリケーションが1つのインターフェースを通してさまざまなメッセージサービスと通信を行うために，サーバ—クライアント間の通信に MAPI (Messaging Application Programming Interface) インフォメーションサービスが用いられる。MAPI は，API (Application Programming Interface) 機能と OLE (Object Linking and Embeded) インターフェースのセットで，サーバ - クライアント間のゲートウェイの役割を果たす。

また，インターネット・メールにおいては，WWW をはじめマルチメディア情報処理技術が急速に発展しており，これに刺激され電子メールにおいてもマルチメディア情報に対応したより高度なコミュニケーション環境が整いつつある。このような変化に刺激され，グループウェアにおけるメールとしてインターネット・メールを指向する傾向が増してきた。

III　インターネット・メールの変遷

1　テキスト・メール

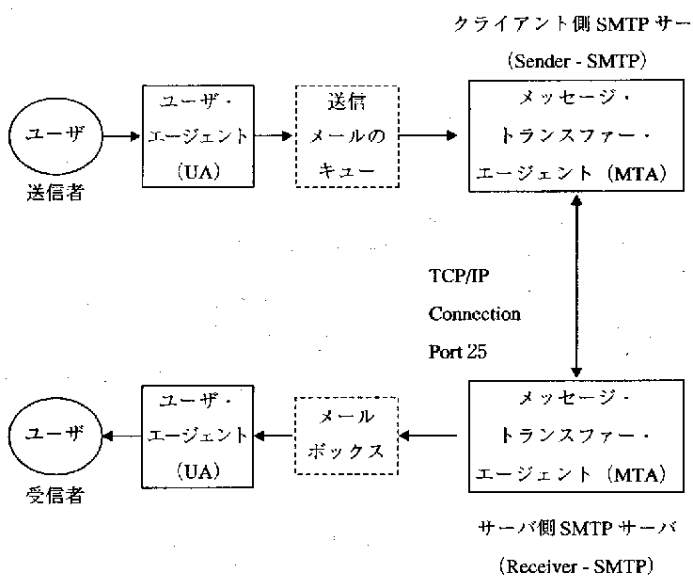
インターネット・メールは，RFC 821 で提案された SMTP と RFC 822 に定義されたフォーマットにもとづいた，わずか14個のコマンドからなるコマンド／応答型のプロトコルによるメールである。

SMTP は，TCP/IP 上で用いられるメール交換プロトコルである。SMTP によるメール交換の概要は，図2のように表すことができる[5]。

ユーザは，端末上でメッセージの作成と送信を支援するユーザ・エージェント（UA）を用いて，メッセージを作成する。メッセージは，サーバ上で一旦

5)　Stevens, W. R. [1994], p. 441.

図2　TCP/IP 上でのメール交換（Stevens, p. 441）



送信待ち行列に蓄えられ，メッセージ・トランスファー・エージェント（MTA）にひきわたされる。SMTP の場合 MTA は SMTP サーバであるが，SMTP サーバは，メッセージの送信・受信の両方を行い，送信する側（クライアントの役割をする）を Sender-SMTP，受信する側（サーバの役割をする）を Receiver-SMTP と呼ぶ。MTA 間の通信には，TCP/IP が用いられる。メール交換用の TCP ポートは，通常25番が用いられる。このサーバ間の TCP/IP による通信上で，SMTP を用いてメッセージが交換される。Receiver-SMTP は，メッセージを受信すると，宛て先のユーザのメールボックスにメッセージを格納する。受信側のユーザは，UA を用いてメールボックス内のメッセージを端末上に読み出し，メッセージを閲覧する。メールボックスからユーザの端末へは，RFC 1081（1988）で提案されている POP 3（Post-Office Protocol Version 3）あるいは RFC 1730（1994）で提案されて

いる IMAP 4（Internet Message Access Protocol 4）とよばれるメール配布プロトコルを用いて転送する[6]。

SMTP によって送受信されるメッセージのフォーマットは，RFC 822（1982）に示されている。SMTP メールは，大別して送受信のための情報が記述されているヘッダとメッセージの本文であるボディの 2 つのパートから構成されている。ヘッダとボディは，一連のテキストデータであるが，ヘッダ部とボディ部との間は，空行によって区分されている。

ところで，インターネットに接続されているローカルなネットワークでは，独自のメールシステムを用いている場合がある。そうしたローカルなメールシステムとのメッセージ交換は，メール・ゲートウェイを経由させることによって行われる。たとえば，RFC 1168（1993）では，インターネットと他の商用ネットワークとの間のメールリレーサービスについて記述されている。また，現在では多くの LAN 製品やグループウェア製品に，インターネット・メールや他のメール・システムとの互換性を提供するためのメール・ゲートウェイが実装されている。

SMTPが提案された当初におけるインターネットの標準化思想では，インターネット上に接続されるであろうさまざまハードウェアおよびソフトウェアにおいて最大限の互換性を確保する方針であったため，RFC 821 および RFC 822 による SMTP メールでは，ほとんどすべての機器で最低限サポートしているであろう 7 bitUS-ASCII コードを用いたテキストメッセージが前提となっていた。このため，日本語をはじめ非 ASCII コードである各国独自のコード体系を使用したメッセージあるいは 8 bit コードやバイナリデータによるメッセージは，SMTP の規格外でありインターネット上では用いるべきではないとされていた。

ところが，現実にはそれぞれのローカルなネットワーク内ではさまざまな

6) POP 3 のRFC最新版は，RFC 1939（1996）であり，RFC 1957（1996）で若干の修正が行われている。また，IMAP 4 の RFC 最新版は，RFC 2060（1996）の IMAP 4 Revision 1 である。

データ形式でメッセージ交換をしたいという要求がある。たとえば，日本国内では，2バイト漢字コードを用いた日本語のメッセージ交換の方が現実的である[7]。そうした要求が高まるにつれ，7 bitUS-ASCII コード以外のデータをメッセージとして用いるための方策が検討されることになった。

2 マルチメディア電子メール

1980年代後半からインターネットが世界中に拡大したこと，そして1989年に開発された WWW（World Wide Web）および1993年に開発された Web ブラウザ（Mosaic）をきっかけとしてインターネット上においてマルチメディア情報を扱う技術が発達してきたことから，各国独自の言語コードやマルチメディア情報などの非 ASCII コードによるデータでもってメッセージ交換を行いたいという要求がますます高まった。そこで，その要求に対処するために RFC 822 の SMTP メールフォーマットの拡張として RFC 1341（Multipurpose Internet Mail Extensions : MIME, 1992）が提案された[8]。

MIME では，RFC 822 で定義されたヘッダ・フィールドに加えて，MIME-Version，Content-Type，Content-Transfer-Encoding，Content-ID，Content-Description の5つのヘッダ・フィールドが定義され，ボディ部のデータを個別にカプセル化するための仕組みが提案されている。メッセージ・データをカプセル化することにより，SMTP の制限を受けずに 7 bitUS-ASCII コード以外のデータによるメッセージや複数のデータ・パートからなるメッセージを送受信することが可能となった。カプセル化されたボディ部は，UA が MIME ヘッダ・フィールドの情報を解釈することにより復元され，それぞれのユーザ端末にあわせて表示される。

MIME-Version には，使用する MIME のバージョンを記述する。現在の

7） 日本国内においては，それまでも 7 bitJIS コードを用いることによって，日本語によるメッセージ交換を行っていた。

8） MIME は，以後何度か改訂されており，現在の最新版は RFC 2045（Part 1）から RFC 2049（Part 5）のシリーズである。

MIME のバージョンは，1.0である。

Content-Type には，メッセージのデータの種類を記述する。メッセージのデータの種類は，タイプとサブタイプとに分けて記述される。RFC 1341 で指定されている標準タイプとサブタイプは，表1のとおりである。

Content-Transfer-Encoding には，メッセージデータの転送／符号化形式を記述する。RFC 1341 によるこのフィールドに記述できるタイプには，7 bit, 8 bit, Binary, Base 64, Quoted-Printable がある。このヘッダが省略された場合は，RFC 821 で前提とされている 7 bit コードであるとみなされる。

7 bit コード以外のコードやイメージ，オーディオ，ビデオなどのバイナリデータ，アプリケーションデータなどは，SMTP で配送可能な 7 bit US-ASCII コードに符号化する。符号化の方式にはいくつかのものがあるが，MIME によって標準とされているものとしては，Base 64 と Quoted-printable とがある。Base 64 は，8 bit コードやバイナリデータなどの SMTP がサポートしていないデータ形式を 7 bitUS-ASCII コードに符号化するのに適した変換方式である。Quoted-printable は，US-ASCII コードの一部に非 US-ASCII データが混在するような場合の符号化に適した方式である。データを符号化するための他の方式としては，UNIX などで用いられる uuencode や Apple 社の MacOS 上で用いられる BinHex などがあるが，これらの方式は，特定のゲートウェイでは取り扱うことが出来ないことや，UNIX の種類によって変換方式に方言があることなどから，MIME 標準からは除外されている[9]。

Content-ID と Content-Description は，複数のメッセージデータをボディ部にカプセル化する際に，各パートごとの情報を記述するのに用いられる。Content-ID には，各パートに個別に割り付けられた ID が記述され，それぞ

9) ただし，UNIX ユーザ間では，以前から UUENCODE と tar によるデータ交換が行われてきた。また，Macintosh のファイル転送のためのフォーマットに関する規定は RFC 1740（1994）で，BinHexデータの送信のためのContent-Typeに関する規定は RFC 1741（1994）で提案されている。

表1　Content-Typeヘッダフィールドの標準タイプ/サブタイプ

タイプ	サブタイプ
text	plain richext enriched tab-separated-values
multipart	mixed alternative digest parallel appledouble header-set
message	rfc 822 partial external-body news
application	octet-stream postscript oda atomicmail andrew-inset slate wita dec-dx dca-rft activemessage rtf applefile mac-vinhex 40 news-message-id news-transmission wordperfect 5.1 pdf zip macwriteii msword remote-printing mathematica
image	jpeg gif ief tiff
audio	basic
video	mpeg quicktime

れのパートを識別するために用いられる。Content-Description には，各々のパートにカプセル化されたメッセージに関するコメントを記述することができる。

RFC 1341 による MIME では，これらのヘッダ・フィールドを追加することによりボディ部の柔軟性を高めたが，ヘッダ部のデータ形式に関しては，依然 SMTP の制約を受けることになる。しかも，インターネット上で SMTP サーバを経由してメールが転送される際には，途中経由するメールシステム（サーバやクライアント）によって，ヘッダ・フィールドの追加や再構成が自

動的に行われる場合がある。このため，ヘッダ部には，7 bitUS-ASCII コードはもちろんエスケープ・コードも使用することができないという制約があった。これを解決するために，RFC 1522（1993）で MIME 拡張メッセージ・ヘッダの仕様が提案され，ヘッダ部においても非 US-ASCII コードを符号化したものを用いることが可能となった。

MIME を用いることによって，データ形式の異なる複数のメッセージをひとつのメール内に梱包して送受信することが可能となる。たとえば，日本語も含めたテキストデータと画像データなどのバイナリデータを一緒に送ったり，他のアプリケーションソフトで作成したデータをテキストメッセージに添付して送ったりすることが可能となる。

ところで，MIME によってマルチメディア電子メールを送受信することが可能となったが，それによってつぎのようなあらたな問題も明らかとなった。第一に，マルチメディア・データは，一般的にデータの容量が大きいためこれまでの SMTP サーバでは十分な対応が出来ないという問題である。第二に，MIME のヘッダ・フィールドでは，ボディ部にカプセル化された複数のメッセージの関係付けを自由に定義できないという問題である。

第一の問題については，SMTP の拡張として ESMTP（Extended SMTP）が提案されている。ESMTP の仕様は，SMTP サービス拡張（SMTP Service Extensions）と題された一連の RFC で定義されており，MIME を使用したメールのための拡張やエラー処理などの改善がなされている。たとえば RFC 1425（1993）では，まず EHLO コマンドが定義された。EHLO コマンドは，SMTP の HELO コマンドを拡張したもので，送信先のサーバが SMTP サービス拡張に対応しているか否かを確認する。それにつづく RFC 1426（1993）では，MIME で標準データ形式のひとつとなっている 8 bit コードのデータを転送する際のサービスの拡張が示されている。8 bit コードのデータは，MIME では標準データ形式として定義されたが，従来の SMTP では完全なサポートがなされていなかった。一般的にマルチメディ

ア・データは，テキストデータと比較してデータの容量が大きい。MIME を用いて大容量のマルチメディア・データの送信した場合，Receiver-SMTP が必ずしもそうした大容量データを処理しきれる環境であるとは限らないが，従来の SMTP では，事前にサーバ同士の環境を確認するための機能が具備されていなかったため，とりあえずデータを送信し，応答コードでもって判断するという無駄が生じることになる。そこでつづく RFC 1427 (1993) では，MIME による大容量のマルチメディアメッセージデータを送受信するためのサーバ側からの対応として，メッセージを送受信する前に送信されるデータの容量を前もってサーバ間で確認し合うための手順が定義された。

SMTP サービス拡張では，その他にもバイナリデータを送信するための BDAT コマンド (RFC 1830, 1995)，送信チェックと再送信に関するサービス拡張 (RFC 1854, 1995)，配信状況の警告を知らせるサービス (RFC 1891, 1996)，メッセージ待ち行列を遠隔操作するための拡張 (RFC 1985, 1996)，エラーコードの拡張 (RFC 2034, 1996) などが提案されている。

第二の問題については，Web で用いられる HTML によるリンク機能を応用することによって解決できる。

3 Web メール

メールに梱包した複数のマルチメディア・データを関連付ける方法のひとつとして，Web で使用されている HTML を応用する方法がある。すなわち，メッセージを HTML 形式で記述し，HTML のリンク機能や埋め込み機能を利用してメッセージデータ間の関連を指定する方法である。HTML データをメッセージにカプセル化するための仕組みを MIME-HTML (MHTML) と呼ぶ。HTML の解釈は，各 UA で行い，Web をブラウズする要領でメッセージを表示する。

MHTML は，いくつかの MIME ヘッダ・フィールドの拡張によって実現される。MHTML のための拡張フィールドは，RFC 2110 (1997)，RFC

2111 (1997), RFC 2112 (1997) で提案されている。RFC 2110 では, Content-Location および Content-Base の 2 つの MIME ヘッダ・フィールドの提案, RFC 2111 では Content-ID と Message-ID の利用について, RFC 2112では Content-Type のサブタイプとして Multipart/Related の提案, がそれぞれ記述されている。メールのメッセージとして HTML を用いるだけであれば, 従来の SMTP および MIME でも可能であったが, これらの RFC では, ヘッダ・フィールドの拡張により(1)メール内にカプセル化された複数のデータを HTML でもって構造化しメッセージとして送受信すること, (2)メールの外部にあるデータをリンクすることによってメッセージとして送受信すること, (3)複数の HTML データを一つのメール内にカプセル化すること, などが可能となる。この MHTML を用いることによって, Web ページとほぼ同等の表現力を備えた「Web メール」が利用可能となる[10]。

現在, Microsoft 社の Outlook Express や Netscape Communications 社の Messenger をはじめとして多くのパソコン用メール・クライアントが MHTML に対応している[11]。これらのメール・クライアントでメールを作成する場合, HTML 形式でメッセージを作成するか通常のテキスト形式でメッセージを作成するかを選択することができる。HTML 形式を選択した場合には, WYSIWIG 形式の HTML メッセージ作成ウィンドウが表示され, HTML の文法を意識することなく Web メールを作成することが可能である。これらのメール・クライアントでは, HTML だけではなく JavaScript などの Script 言語にも対応しており, メッセージ・コンテンツに Script を記述することによって, クライアント側で何らかの処理を行うようなメッセージも作成することができる。また Outlook Express では, Web ブラウザで表示して

10) Web メールについては, 定道宏教授（京都大学）を中心に行ったグループウェアに関する研究プロジェクトにおいて議論され命名された。その研究成果の一部は, 中原・高井・細井・北室 [1997] において発表された。なお, 最近, ポータルサイトなどのサービスでウェブページ上からメールの送受信を行うサービスをウェブ・メールと呼ぶ場合があるが, ここで言う Web メールとは異なり単にウェブページでもってメールの送受信のサービスを提供するものに過ぎない。

11) ただし, 現在のところ複数の HTML データをメール内に含める機能は対応していない。

いるWebページをそのままメッセージ・コンテンツとして送信することも可能である。

IV Webメールのセキュリティ

ビジネス環境においてだけではなく，個人利用においても，電子メールのセキュリティは重要である。とくに，オープンなインターネット環境においては，ホスト型メールやイントラネット型メールのようなクローズドな環境におけるメールと比較して，悪意のあるなしに関わらず第三者によるなんらかの干渉を受けやすい。

電子メールにおけるセキュリティに要求される機能には，大別すると(1)データの秘匿性（confidentiality）と(2)ユーザの認証性（authenticity）とがある。データの秘匿性は，正当な受信者のみがメッセージを読めることを示し，ユーザの認証性は，送られてきたメールが発信者からのものであることの保証を示す。前者は，メッセージの暗号化処理でもって行い，後者は，ハッシュ関数を利用した電子署名でもって行う。

暗号化とは，なんらかのパターンのもとに元のデータをある写像へとデータを変換することを意味する。暗号化されたデータは，正当な閲覧者のもとで復号化可能でなければならない。暗号化および復号化にどのようなパターンを用いるかを決定する情報を「鍵」と呼ぶ。送信者側と受信者側でそれぞれ暗号化と復号化のための鍵を用意しておき，鍵情報をもとに送信者側で暗号化，受信者側で復号化を行う。

鍵の方式は，暗号化と復号化に同じ鍵が使用されるか否かによって，(1)対称鍵暗号系（秘密鍵方式）と(2)非対称鍵暗号系（公開鍵方式）とに分けることができる。

対称鍵暗号系では，暗号化と復号化に同じ鍵を用いるが，この方式ではメッセージの送信者と受信者との間であらかじめどの鍵を用いるかを決めておかなければならないという不便さが生じる。受信者と送信者の間で鍵を秘密にして

用いるために，秘密鍵方式とも呼ばれる。

非対称鍵暗号系では，暗号化と復号化に別の鍵を用いる。つまり暗号化には相手の公開鍵を，復号化には自分の秘密鍵を用いることにより，受信者と送信者の間であらかじめ鍵の申し合わせをする必要がない。受信者が秘密にして用いる秘密鍵と送信者がメールを暗号化するための公開鍵を用いることから，公開鍵方式とも呼ばれる。

公開鍵方式による暗号化は比較的大きな計算になるため，一般的にはデータの暗号化は秘密鍵方式で行い，使用した秘密鍵を公開鍵方式で暗号化する方法が用いられる（図3）。対象鍵暗号系の主なものとしては，DES，RC シリーズなどがあり，非対称鍵暗号系の主なものとしては，DSS，RSA がある。

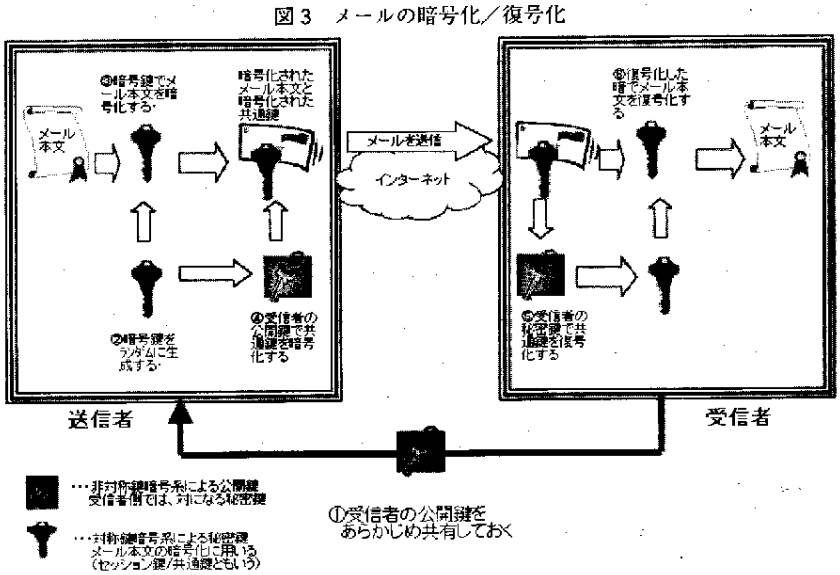
メッセージの認証には，ハッシュ関数が用いられる。まず，認証のためにメッセージからハッシュ関数を用いて，ハッシュ・コード（メッセージ・ダイジェスト）が求められる。このメッセージ・ダイジェストは，いわばメッセージのディジタル指紋であり，これを送信者が暗号化し，メッセージに添付する。受信者は，送信者の公開鍵でメッセージ・ダイジェストを復号化することによって，確かに送信者本人からのメッセージであることを確認する。

インターネット・メールのセキュリティ方式には，これまでいくつかのものが提案されてきた。代表的なものには，MSP，PEM（RFC 1421-RFC 1424, 1993），MOSS（RFC 1848, 1995），PGP（RFC 1991, 1991），PGP/MIME（RFC 2015, 1996），S/MIME（RFC 2311, 1998 ; RFC 2312, 1998）などがあるが，MIME に対応しており，現在代表的なメール・クライアントによって支持されているものとしては，PGP/MIMEとS/MIME があり，この2つが事実上のインターネット標準となっている。

MIME におけるセキュリティに関しては，RFC 1847（1995）によってセキュリティのための MIME における Multipart フィールドの拡張が行われている[12]。RFC 1847では，あらたに Multipart/Signedと Multipart/Encrypted

12）RFC 1847 は，MOSS を利用するために提案された MIME 拡張であるが，他の方式にお/

図3　メールの暗号化／復号化



の2つのMultipartサブタイプが定義されており，認証情報に関してはMultipart/Signedフィールドを利用して，暗号化情報に関してはMultipart/Encryptedフィールドを利用して，追加パラメータでもって認証方式および暗号化方式に関する情報を記述することになっている。

S/MIME（Secure/MIME）は，（米）RSA Data Security社[13]が提唱するMIMEを用いて暗号化メールを実現する規格である。S/MIMEでは，同社の研究所が提唱する非対称鍵暗号方式の暗号規格であるPKCS（Public-Key Cryptography Standard）を用いてMIMEメッセージを暗号化する[14]。PKCSは，＃1から＃10（ただし，＃2と＃4は他の規格に統合された）からなる暗号化規格群である（表2）。

いてもこの拡張が利用されている。

13）RSAウェブ・ページ http://www.rsa.com/。

14）S/MIMEおよびPKCSの詳細についてはRSAウェブ・ページを参照。

表2　PKCS 規格

PKCS#1	RSA Encryption
PKCS#3	Diffie-Hellman Key Agreement
PKCS#5	Password-Based Encryption
PKCS#6	Extended Certificate Syntax
PKCS#7	Cryptographic Message Sysax
PKCS#8	Private-Key Information Syntax
PKCS#9	Selected Attribute Type
PKCS#10	Certification Request Syntax

S/MIME では，MIME に application/x-pkcs 7-mime と application/x-pkcs 10 の 2 つのデータタイプを導入することにより，メールの暗号化方式に関する情報をメッセージに記述する。

application/x-pkcs 7-mime は，pkcs＃7 によって当該メッセージ・パートが暗号化されていることを示す。暗号化の手順としては，まず MIME のボディ・パートとしてデータを準備した後，PKCS＃7 によって暗号化処理を行う。PKCS＃7 で定義されているデータ形式では，(1)電子署名処理を施されたデータ（SignedData），(2)暗号化処理を施されたデータ（EnvelopedData），(3)電子署名と暗号化処理を施されたデータ（SignedAndEnvelopedData）のいずれかを用いることができる。

application/x-pkcs 10 は，PKCS＃10にもとづいた証明書の発行を要求するのに必要な情報を記述したメッセージ・パートであることを示す。このメッセージ・パートには，バージョン番号，証明書の発行を希望するユーザ名，公開鍵情報，ユーザの属性情報が記述され，PKCS＃10にもとづいたデータ形式に変換される。

主流となっている S/MIME のバージョンは，RFC 2311 および RFC 2312 で RFC 化された Version 2.0 であるが，現在 Version 3.0 が開発中である。データ暗号化のための対応する共通鍵暗号方式としては，トリプル DES (168 bit)，RC 2 (40 bit)，また共通鍵の暗号化方式として対応する主な公開

鍵暗号方式は，DSS と RSA である。鍵の管理方式およびユーザの身元証明には，認証局（Certificate Authority : CA）によって行われる。

PGP（Prety Good Privacy）は，P. Zimmerman によって開発され，フリーソフトウェアとして流通している暗号化パッケージである。また，サポートも含めたパッケージが，（米）ネットワーク・アソシエイツ社から販売されている。PGP は，当初テキスト・メールの暗号化ソフトウェアとして開発されたが，現在では，MIME に対応した PGP/MIME が開発されている。PGP に関しては，RFC 1991（1991）で，PGP/MIME に関しては RFC 2015（1996）で RFC 化されている。PGP/MIME では，PGP を用いるための新しい Content-Type として，application/pgp-encrypted, application/pgp-signature, application/pgp-key の 3 つのタイプが定義されている。

application/pgp-encrypted は，メッセージが PGP によって暗号化されていることを示す。PGP によって暗号化されたメッセージは，ボディ部にバージョンを示すパートと実際に暗号化されたメッセージを含むパートの 2 パートからなる。バージョンを示すパートには，PGP/MIME 標準を満たすことを示す "Version : 1" フィールドを記述する。暗号化メッセージを含むパートには，オクテットストリームからなる暗号化されたメッセージ本文を記述する。

application/pgp-signature は，PGP によって署名されていることを示すタイプである。PGP によって署名されたメッセージは，ボディ部に署名されたデータを含むパートと PGP デジタル署名を含むパートの 2 つのパートからなる。

application/pgp-key は，PGP の公開鍵の配布に関する情報を示すタイプである。

現在主流となっている PGP のバージョンは，2.6.3 i である。RFC 2015 による PGP/MIME は，このバージョンを MIME に対応させたものである。PGP は，現在，次期バージョンの 5.5 i が開発中であり，PGP/MIME の次期バージョンとしては OpenPGP が既に Internet-Draft に公開されている[15]。

データ暗号化のための対応する共通鍵暗号方式としては，トリプル DES (168 bit)，CAST5 (128 bit)，IDEA (128 bit)，また共通鍵の暗号化方式として対応する主な公開鍵暗号方式は，DSS と RSA である。鍵の管理方式は，ユーザが個々に管理する方式を採っており，ユーザの身元証明はユーザ間の相互認証によって行われる。

現在，Netscape Communications 社の Netscape Messenger や Microsoft 社の Outlook Express などのメール・ソフトでは，S/MIME による暗号化機能が標準でサポートされており，事実上の業界標準となりつつある。また，公開鍵の管理方式として CA を通した認証方式を採用していることから，S/MIME は，鍵の集中管理が必要となる企業での利用に向いた暗号方式であるといえる。それに対して，PGP は主にフリーソフトウェアとして流通していること，公開鍵の管理方式として個人管理による認証方式を採用していること，などから手軽に利用できる暗号化パッケージであり，むしろ個人利用に向いた暗号化方式であるといえる[16]。

V　グループウェア・メールとしての Web メール

グループウェア・メールを Web メールでもって実現しようとした場合，従来の LAN 型メールと比較して，つぎのような利点があげられよう。

第1に，MIME によるマルチメディア電子メールを拡張したものであり，アプリケーション・データや画像，音声，動画を添付ファイルとしてだけではなく，Web のコンテンツのように表現力豊かにデザインし，表示できる。これによって，細かいニュアンスや具体的なイメージをメッセージとして送信することが可能となり，グループメンバー間のより高度なコミュニケーションを

15) Internet-Draft は，IETF (Internet Engineering Task Force) で現在作業中のインターネット関連の技術を文書化した「作業中文書」である。文書の有効期間は，発行後6ヶ月であり，その後作業の進歩状況に応じて破棄，改訂，RFC 化，などされる。Internet-Draft の詳細および文書に関しては，IETF ウェブ・ページを参照。(http://www.ietf.org/home.html)

16) ただし，パッケージによっては，CA 不要な S/MIME を利用したものや CA を利用できる PGP パッケージなどもある。

支援することができよう。

第2に，Script処理を行えることによって，動的なメッセージを送ることが可能となる。従来の電子メールは，データを表示するだけのビューアであったが，Webメールでは，メッセージ内にScriptを埋め込んでおくことによって，受信側でScriptを実行しなんらかの処理を行うようなメッセージが可能である。たとえば，受信側でメールを開くと，自動的に対話形式で質問や処理をおこない，あらかじめ決められていたあて先に自動的に返信するような電子メールも可能である。

Webメールあるいはインターネット・メールでもって，以上のようなグループ支援が可能となる反面，グループウェアメールとしてより有効に活用するためには，つぎのような課題も残されている。

第一に，グループ支援のための他のツールとの連携である。グループによる分業・協業支援においては，メールによる一対一のコミュニケーションの他に，電子掲示板などによる一対多あるいは多対多のコミュニケーションも重要である。Webメールでもってグループコミュニケーションを支援する場合，このような一対多，多対多のコミュニケーションをいかに支援するかという問題がある。ひとつの解決策としては，メーリング・リストやNNTP (Network News Transfer Protocol)，HTTP (Hyper Text Transfer Protocol) などの他のインターネット標準技術を導入し，連携させて用いる方法が考えられる。たとえば，MIMEによるアプリケーション・データの添付やWebメールによって特定の相手に高度に構造化されたデータを配布することが容易となるが，これをメーリング・リストや同報送信などと組合せて活用することにより，遠隔会議の資料をHTML形式あるいはワープロなどのアプリケーションでもって作成し，まえもってメンバーに配布するなどの利用が考えられるであろう。このような活用をユーザがさらに容易に行うためには，UAにおける他のサービスとの連携機能やグループ単位のアドレス管理機能などの向上が求められる。

第二に，マルチメディア・データの容量と伝送媒体の問題である。画像・音

声・動画などのマルチメディア・データは，テキストデータと比較して大容量のデータとなる。ところが，インターネットは，10 Base から ATM (Asynchronous Transfer Mode)，ギガビット Ethernet などまでさまざまな帯域の伝送媒体が混在しているネットワークであり，マルチメディア情報を送受信するための均一な伝送帯域を確保することが困難である。マルチメディア・データは，そのデータ容量によってそれぞれ異なった QoS (Quality of Service) をもつが，伝送媒体によっては十分に QoS を維持することができない。ITU-T（国際電気通信連合―電気通信標準化部門）では，各伝送媒体に応じてそれぞれのマルチメディア・データが要求する QoS を維持するためのマルチメディア標準プロトコルを勧告しているが，現在のインターネット上では，必ずしもこれを保証することはできない。この問題に関しては，インターネット伝送媒体の均一化はもちろん，高速な伝送容量を持つネットワーク上で作成された大きなメッセージを低速な伝送容量のネットワーク利用者に送信する場合の対策やマルチメディア・データの圧縮技術の改良による解決が必要であろう。

VI おわりに

非同期型のグループ協業支援を行う場合，グループメンバー間のコミュニケーションを支援するために電子メールは，必須である。とくにネットワーク環境やマルチメディア情報処理環境が整備されつつある企業では，インターネット／イントラネット環境およびより高度なコミュニケーションに対応した電子メールが求められよう。本稿では，インターネット・メールの変遷とセキュリティ技術について展望し，グループウェア・メールとして Web と同等の表現力を持つ Web メールを適用することについて考察した。

Web メールは，表現力豊かなコンテンツをメッセージとして送受信できること，インターネット／イントラネット環境で社内外へとシームレスにメッセージを送受信できること，セキュリティ技術の強化および標準化が積極的に

行われていることなどから，インターネット時代におけるグループウェア・メールとして有効であるといえる。しかし，目的が明確で比較的閉じた環境で用いられるLAN型グループウェア製品と比較して，Webメールは多目的でオープンなインターネット環境で用いられることから，グループ協業支援を指向した機能向上やインフラストラクチャの整備などの課題も残されている。

参考文献

DeSanctis, G. and B. Gallupe [1985] "Group Decision Support Systems : A New Frontier," in *Decision Support Systems* 2nd ed, ed. by Sprague, R.H.jr. and H. J. Watson, New Jersey, Prentice Hall.

Ellis, C. A., S. J. Gibbs and G. L. Rein [1991] "Groupware : Some Issues and Experiences," *Communications of the ACM*, Vol. 34, No. 1, Jun. 1991, p. 38.

Johansen, R., [1988] *Groupware : Computer Support for Business Teams*, New York, The Free Press.

Marca D., and G. Bock [1992] *Groupware : Software for Computer Supported Cooperative Work*, IEEE Computer Society Press.

Migliarese, P. and E. Paolucci [1995] "Improved Communications and Collaborations among Tasks Induced by Groupware," *Decision Support Systems*, Vol. 14 No. 3, Jul. 1995.

Stevens, W. R. [1994] *TCP/IP Illustrated* Vol. 1, ADDISON-WESLEY.

笠野英松監修 [1998] 『インターネットRFC事典』アスキー出版。

定道　宏[1993] 「インターネットにおける電子メールの利用」『経済経営研究』第43号，1-10ページ。

中原昭宏・高井才明・細井貞人・北室康一 [1997] 「WWW時代におけるマルチメディア電子メール―グループウェアとWebメール―」『オフィス・オートメーション』Vol. 18, No. 4-2, 116-119ページ。

ヒューズ, L. J., Jr.（長原宏治監訳）[1997] 『インターネットセキュリティ』インプレス。

藤原　洋・大久保　栄[1996] 『インターネット時代の画像圧縮技術―MPEGからケーブルモデムまで―』アスキー出版。

参照ウェブ・ページ

RFC ウェブ・ページ, http://www.rfc-editor.org/rfc.html

The Internet Engineering Task Force ウェブ・ページ，
http://www.ietf.org/home.html
(米) RSA社ウェブ・ページ，http://www.rsa.com/
(米) ネットワーク・アソシエイツ社，http://www.nai.com/

メールに関する主要な RFC

Postel, J., "Simple Mail Transfer Protocol," RFC 821, 1982.

Crocker, D. H., "Standard for The Format of ARPA Internet Text Messages," RFC 822, 1982

Freed, N., & N. Borenstein., "Multipurpose Internet Mail Extensions (MIME) : Mechanisms for Specifying and Describing the Format of Internet Message Bodies.", RFC 1341, Nov. 1996.

Klensin, N. Freed, M. Rose, E. Stefferud & D. Crocker. "SMTP Service Extensions.", RFC1425, Feb.1993 / RFC1651, July 1994 / RFC1869, Nov. 1995.

Klensin, J., N. Freed, M. Rose, E. Stefferud & D. Crocker., "SMTP Service Extension for 8bit-MIME transport.", RFC 1426, Feb. 1993 / RFC 1652, July 1994.

Klensin, J., N. Freed & K. Moore., "SMTP Service Extension for Message Size Declaration", RFC 1427, Feb. 1993/RFC 1653, July 1994/RFC 1870, Nov. 1996.

Crocker, D., N.Freed & A. Cargille., "SMTP Service Extension for Checkpoint/Restart.", RFC 1845, September 1995.

Freed, N., "SMTP Service Extension for Command Pipelining.", RFC1854, October 1995.

Vaudreuil, G., "SMTP Service Extensions for Transmission of Large and Binary MIME Messages.", RFC 1830, August 1995.

Moore, K., "SMTP Service Extension for Delivery Status Notifications.", RFC 1891, January 1996.

Winter, J., "SMTP Service Extension for Remote Message Queue Starting.", RFC 1985, August 1996.

Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes.", RFC 2034, October 1996.

Freed, N., & N. Borenstein., "Multipurpose Internet Mail Extensions (MIME) Part One : Format of Internet Message Bodies.", RFC 1521, Sep. 1993 / RFC 2045, Nov. 1996.

Freed, N. & N. Borenstein., "Multipurpose Internet Mail Extensions (MIME) Part

Two : Media Types.", RFC 1522, Sep. 1993 / RFC 2046, November 1996.

Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three : Message Header Extensions for Non-ASCII Text.", RFC 2047, November 1996.

Freed, N., J. Klensin & J. Postel., "Multipurpose Internet Mail Extension (MIME) Part Four : Registration Procedures.", RFC 2048, November 1996.

Freed, N., & N. Borenstein., "Multipurpose Internet Mail Extensions (MIME) Part Five : Conformance Criteria and Examples.", RFC 2049, November 1996.

Palme, J. & A.Hopmann, "MIME E-mail Encapsulation of Aggregate Documents, such as HTML (MHTML)," RFC 2110, March 1997.

Levinson, E., "Content-ID and Message-ID Uniform Resource Locators," RFC 2111, March 1997.

Levinson, E., "The MIME Multipart/Related Content-type," RFC 2112, March 1997.