ビジネスにおける電子メールの活用と最近の法制の関係その2
―ビジネス場面別活用事例―

Current Status of E-mail Usage in Business and Related Laws, Part2―Examples for Individual Business Scene

奥山　徹
Tohru Okuyama

前回の報告[1]においてビジネスにおける電子メールの有効性と危険性について議論し、2003年までに制定された電子メールに関連する法律との関係を明らかにした。今回は、その議論をさらに深化させ、ビジネスにおける個々の活用場面を想定して、電子メールをビジネスに応用することを考える。さらに、2004年以降に制定された電子文書法[2]などとの関係についても議論する。

1．はじめに

電子メールは既に多くのビジネスの場面において活用されている。しかしながら、電子メールには技術的な面での各種の危険性があることを前回の報告[1]で示し、一応の解決策を示した。その後、電子メールによるウイルスの媒介、SPAMメールなどの横行はさらに加速され、最近では Phishig と呼ばれる電子メールを使った詐欺行為が頻発している。本報告では、これらの新しい危険性を含めて、ビジネスのそれぞれの場面ごとの電子メールの活用と危険性について議論する。

ビジネスにおける電子メールの用途を大別すると次の4つとなる[3]。

（1） 業務連絡・周知
（2） 各種データの共有
（3） 決済・稟議
（4） 電子取引

また、利用者を想定すると社員間での利用と社員と顧客との間での利用が考えられる。したがって、これらの関係を整理すると表1のような電子メールの利用形態が想定できる。

表1．ビジネスにおける電子メールの利用形態と頻度

	社員間	社員－顧客間
業務連絡・周知	◎	◎
各種データの共有	◎	○
決済・稟議	○	△
電子取引	△	○

（◎多用される、○しばしば利用される、△たまに利用される）

今回は、これらの利用形態について、それぞれの活用場合を想定し、電子メールの利用の際に起きると考えられるトラブルについて述べ、その解決策を探る。

2．利用形態別活用事例

最初に、利用形態別の活用事例を示し、それぞれの事例が抱える問題点について議論する。

2．1．「業務連絡・周知」の場合

現在の電子メール利用の大半を占めていると考えられる。社内の人間同士だけではなく、広く顧客との間でも利用されている。したがって、利用頻度が高いだけにトラブルに結びつくことが多い。ここでは、いくつかの事例について、実際に起きたトラブルを題材にして、トラブル回避の手段を考える。

【事例1：社内業務連絡とトラッキング処理】

A 社の営業部営業一課は通常の業務連絡用として電子メールを利用していた。連絡網として電子メールを利用する場合のルールとして、必ず上司である、課長あるいは係長にも Cc（カーボンコピー）を送ることを義務付けていたが、それが徹底して守られていない。そのため、重要な会議や商談の経過が、しばしば課長や係長に届くのが遅れ、重要な判断の遅れを招くことがある。そのため、何らかの改善策を必要としている。

[キーワード] Cc（カーボンコピー）：あるあて先（To）へ送るメールのコピーを他者に送るための手段であり、あて先（To）にコピーを送ったことが明示的に示される通常の Cc と、送ったことを隠匿する Bcc がある。

さて、Cc を使っていると、ついうっかり Cc を入れることを忘れることがある。それが重要な情報のメールであればあるほど、情報伝達の遅れはビジネスにとり致命傷となりかねない。また、Cc と Bcc の利用方法を間違えると、不必要な誤解を招く恐れもある。ここでは、情報伝達を確実にするために、次のような改善を考える。

【改善案】

（1） メーラをカスタマイズして、いつでも Cc が入るようにする。

（2） Cc をやめてメーリングリストを使う。

2 つの改善案のなかで、（1）はメーラをカスタマイズできる技術的スキルを持つ必要があり、また、逆に全てのメールが Cc されるため、Cc を送られる人のメールの取り扱いが不可能となる場合が想定される。一般的に、一人が一日に取り扱えるメールの数は、**最大 100 通**と言われている[4]。ただし、最大 100 通とは、電子メールの処理に専念した場合である。しかしながら、著者の経験によると、個人差もあるが通常は 40～60 通程度が、通常業務を行いながら処理できる量と考えられる。したがって、Cc を受ける人にとって、未処理のメールをためる危険性があり、必ずしも解決策とはなりえない。そこで、（2）のメーリングリストを使う方法を考える。なお、メーリングリストの詳細は、次節で述べる。

【トラッキング処理】

電子メールを使う場合（特に電子メールを使う場合に限らないのだが)、もう一つ重要な問題がある。それは、リクエストに対するトラッキング処理である。電子メールでは書面を介さないので、多くの依頼事項が発生する場合がある。そこで、どのような依頼が発生して、それがどのような状態になっているかを追跡することが重要となる。Ccやメーリングリストにより、部下からのメールを収集して整理することが可能な上司は、このようなリクエストトラッキングを管理することが重要な仕事の一つである。なお、トラッキングのためのツールとしては、例えばサブジェクト（表題）ごとに、電子メールを管理することが可能なメーラを利用することで、ある程度は管理できる。なお、トラッキング処理の重要性については、次の事例2で詳しく述べる。

［キーワード］　メーリングリスト（ML)：メーリングリストは、あるグループの代表メールアドレスを決めておき、そのアドレスにメールを送ると、グループの全てのメンバーにメールが届く仕組みである。詳しくは、次の節で述べる。

【事例2：顧客からの問い合わせ処理】

あなたは製品のサポート担当として顧客からの各種の苦情を受け付ける立場にあるとする。現在、サポート担当は2名おり、その2名が交代で電話と電子メールによる苦情を処理している。ある日、新製品の欠陥を指摘する苦情メールが飛び込んできた。先月発売した場合の新製品のことなので、サポート側もはっきりとした情報をつかんでいなかったとする。さて、社内処理をするためにあなたは駆けずり回り、ようやく回答を送ろうとし直前、対応の遅さを理由に、顧客から取引の停止をにおわせるメールが入り、上司とその処理に忙殺される結果となってしまった。

［キーワード］サブジェクト（表題、Subject)：メールの要約として付けられる短い文である。通常、メーラは電子メールのリストを提示するとき、サブジェクトを同時に表示することが多い。また、多くのユーザはサブジェクトを見て、すぐに読むべきメールかどうかを決めている。したがって、サブジェクトは電子メールにおける重要な情報であると認識すべきである。リクエストトラッキングを行う場合も、サブジェクトが重要な手がかりとなる場合が多い。また、後に述べるSPAMフィルタの設定などにもサブジェクトが使われる場合が多い。したがって、不用意なサブジェクトはSPAMフィルタに引っかかり、相手にメールを見てもらいない場合も生じる。

以下に、SPAMフィルタに引っかかるサブジェクトの典型的な例を示す。

- No Subject（サブジェクトがない）
- Hello（あるいは、Hello!, Hello!!なども同様）

この事例において、事態を悪化させ

た原因はなんであろうか。現実には、顧客を待たせた時間が問題となる。2,3 日ならばこのような結果にならなかったのかもしれないが、それは結果論である。正しい対応の手順をマニュアル化しておく必要がある。

【解決策】

このような問い合わせの例の場合、基本は**即時対応**と**情報提供**である。

即時対応は、電話のような即時系の通信サービス（相手とリアルタイムで通信を行うサービス）ではサービスの特性上確保されている。例えば、電話を受けて、受話器をはずしたまま長時間放置しておくことはない。また、返事に時間がかかる場合は、その旨を相手にきちんと伝えて、対応のための時間を稼ぐことができる。しかしながら、メールのような待時系の通信サービス（一度スプールに蓄積し利用するため、送信者と受信者の間で情報共有の時差が生じるような通信サービス）の場合、即時系で可能であった基本的な対応を忘れてしまう場合がある。電子メールを受けた時点で、何らかの応対をするのが基本である。もちろん、社内での情報収集などで時間がかかる可能性がある場合は、それを相手に伝えておく必要がある。

情報提供も基本的事項であり、特に解説する必要もないと思われる。しかしながら、情報提供を怠るとか、逆に過度の情報提供を行うことはビジネスでは避けなければならない。電話の場合、頻繁な情報提供（＝頻繁に電話して相手の貴重な時間を奪う）はかえって迷惑となる場合もあるが、電子メールの場合、適切な頻度であれば情報提供は電話よりも容易である。したがって、適切な時期における的確な情報提供を心がけることが必要である。このような情報提供に関しては、上司のトラッキング処理が重要であり、どこまで相手の要求に迅速に答えているかを把握するとともに、自社に不利となるような情報の提供を止める処置なども必要である。

【事例 3 ：SPAM メールの処理問題】

B さんはこのところ、SPAM メールに悩まされていた。ある日、そのことを ISP の担当者に相談すると、早速、SPAM フィルタを設ければよいと言われ、いくつかのフリーウェアを紹介された。B さんは、SPAM フィルタのデータベースをメンテナンスしながら、これまで悩まされていた SPAM の数が減ってきて、快適なメール処理を行うことができるようになった。ところが、ある日、電話での苦情受付を担当している C さんから得意先の方が怒っているというメールを受け取った。内容は次のようなものである。

得意先の X 商事の S さんは、長年当社とつきあいがあった。最近、X 商事も電子メールを導入し、特に重要な問題以外は電子メールを使って情報の交換や簡単な受注を行っていた。ところが、数日前から B さん宛てにメールを出しているが、いっこうに返事がないとのことである。メール内容は新しい受注が決まりそうなので、部品の在庫

状況をチェックして、不足分の購入計画を立てるための納期の問い合わせであった。さほど切迫した話でもなかったので、電子メールで気軽に問い合わせをしたとのことである。

B さんは、自分の電子メールのアーカイブを検索したが、S さんからのメールは見当たらない。もしやと思い、SPAM リストにより振り分けられた SPAM メールのアーカイブを検索すると、S さんからのメールが見つかった。SPAM として認識された原因は、S さんからのメールのサブジェクトと以前来た SPAM メールのサブジェクトが類似しており、サブジェクトのファジイ検索を ON にしていたため、S さんのメールをメーラが SPAM メールと解釈してしまったためである。幸いにして、X 商事は具体的な被害にあったわけではないので商取引上の問題はなかった。しかしながら、このような個人の裁量による SPAM フィルタの導入は、今後の商取引に影響を与える可能性がある。

[キーワード] SPAM メール：一般的に受け取るいわれのない電子メールを総称して SPAM メールと称している。（実際には、もう少し詳細な定義があるが省略する。）SPAM メールは種々の形で送られてくる。例えば、広告メールだったり、あるいは不幸の手紙のようなチェーンメールだったりする。SPAM メール対策は、現在、電子メールをビジネスで利用することを考えている多くのユーザを悩ませている事項である。

【解決策】

この事例に関してはいくつかの複雑な要因が存在する。それらを解きほぐして、具体的な対応を取る必要がある。まず、問題の本質を考える。

[キーワード] SPAM フィルタ：SPAM メール対策のための手段の一つである。メーラ（ユーザ）側に設定するものと、サーバ側に設定するものの両者がある。基本的に、過去の SPAM メールのアーカイブをデータベース化しておき、差出人（From）、サブジェクト（Subject）や場合によってはコンテンツを見て、SPAM かどうかを判断し、通常のメールボックスに入れるか、SPAM ボックスに入れるかを振り分ける。サーが側への設置には、電子メールサーバの知識が必要である。また、不用意な SPAM フィルタの設定は、重要なメールを欠落させてしまう可能性があるので、慎重に行う必要がある。

[キーワード] ファジイ検索：文字列などのパターン検索における一つの方法で、類似したパターンを見つけるための方法を提供する。例えば、「Hello」というキーワードを登録することで、「Hello!」や「Hello？」のような似たキーワードを同時に検索してくれる。便利な反面、種々のトラブルの原因となることがある。

（1） SPAM 対策の問題：全社的な取り組みあったか？

（2） キーワード選定の問題：既に議論したとおりであるが、S さんからのメールにも問題があったかもしれない。

（3） 複数での対応：電子メールの場合は、単独で担当者が受けてしまうと、担当者が出張中などで対応できない場合などの問題が生じる。主担当を決めておくのは良いことであるが、得意先からのメールなどはMLを使って部署全体で責任を持って受ける体制を確立すべきである。

以上の 3 点が議論の出発点である。これらの主要な問題を一つずつ解決してやる必要がある。全社的な取り組みに対しては、セキュリティポリシーや運用規程などを整備して、全社員に対する意識付けをしなければならない。

また、実際にSPAMフィルタを設ける場合は、可能ならばサーバ側で設定すべきであり、システム担当者による定期的なSPAMボックスのチェックも実施すべきである。また、電子メールを活用するための一つの方策として、MLを使った複数の担当者によるメール対応を示している。しかし、このような方法も問題が存在する。例えば、重複対応が起きることや、主担当に遠慮して迅速な対応ができない、などである。これを是正するためには、社内における電子メールへの対応規程の整備や、上司によるトラッキング処理が重要となる。せっかく電子メールを使って、ビジネスチャンスを拡大しようと考えているなら、このようなことをきちんと考えておく必要がある。

2．2．「各種データの共有」の場合

電子メールを使ってデータを共有する場合、添付ファイルを使ってデータを相手に送るという手段をとる場合が多い。そして、これは今日では電子メールの重要な使い方の一つとなっている。添付ファイルとして送ることができるファイルの種類は、MIME[5]と呼ばれる技術により、あらゆるものが可能となった。その反面、巨大なファイルを添付して送るとか、必要ないファイルまで添付して送るなど、ネットワークやディスク資源の無駄遣いとしか思えないことも起きている。また、添付ファイルにはウイルスを媒介するという、別の側面もある。いずれにしても、電子メールにファイルを添付する場合は、十分注意する必要がある。

【事例４：添付ファイルが届かない】

設計課の電気配線係に属するDさんは、得意先から大至急、新しく購入する新社屋のネットワークの構成図と系統図を送ってほしいと連絡を受けた。その際、電子メールで送っても良いかと尋ねたところ、OKとのことだったので、教えられたISP 上の得意先のメールアドレスに電子メールを使って図面を送った。この際、できるだけコンパクトになるようにPDF化して送った。しかしながら、先方からは届かないという苦情が来た。メールの送信ログには間違いなく送ったことが示されていた。

【解決策】

この問題の解決のためには、なぜメールが届かなかったかを探る必要がある。この場合、考えられることは、『ISPの電子メールの使用ポリシーに反している』可能性である。例えば、メールスプールの容量が決められていて、それ以上のファイルは送れない、などの制約がISPによっては設定されている。そこで、そのような制約に引っかかっていないかを確かめる必要がある。

もし、そのような制約によって送れないのであれば、ISPから何らかのエラーメッセージなどが返っている可能性があるので、それを詳細に検討する必要がある。いずれにしても、電子メールでは巨大なファイルを添付して送ることは避けるべきである。

ここで、添付ファイルに関する簡単な実験を行ってみる。2〜3行のテキストファイルを作成し、それを添付ファイルとして送った場合のメールの大きさを計測してみる。例えば、添付するテキストファイルとしてつぎのようものを考える。

〔添付ファイルの内容〕

これは実験用の小規模なテキストファイルです。

〔MIMEエンコードされた内容〕

```
----------5f4UaYIcEeIxEF7eowFBdZ
Content-Type: text/plain; name="test.txt"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="test.txt"

grGC6oLNjsCMsZdwgsyPrItLls2CyINlg0y
DWINng3SDQINDg4uCxYK3gUI=
----------5f4UaYIcEeIxEF7eowFBdZ--
```

この場合は、テキストファイルであるため、それほど急激なサイズの変化はないが、ファイルの形式によっては元のファイルに比べ巨大なファイルサイズとなる場合がある。

【事例5：添付ファイルを開けない】

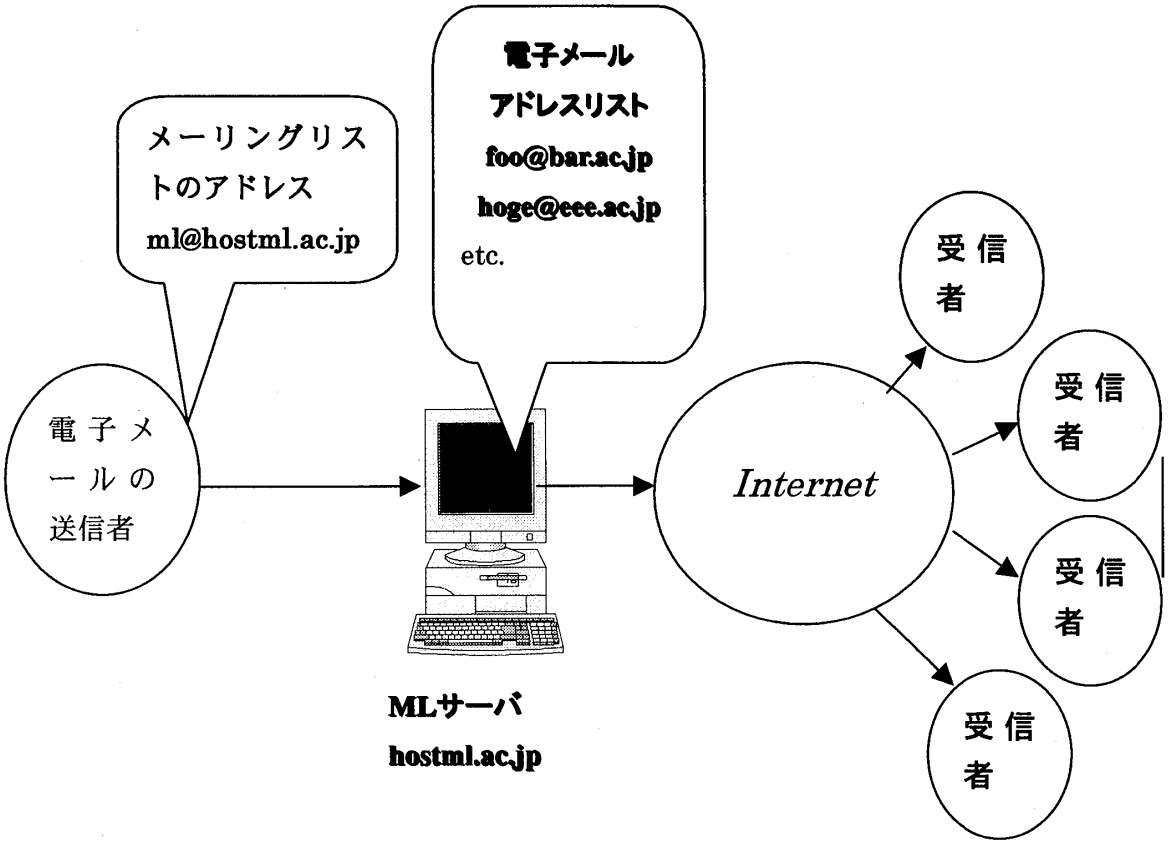
Pパソコンショップに勤めるKさんは、顧客からの見積もり依頼に対して、電子メールでPDF化した見積書を添付して送付していた。しかしながら、あるとき顧客から添付したファイルが開けないという苦情が寄せられた。症状的には、添付ファイルが途中で途切れており、アプリケーションから開くことができないとのことである。この場合は、ファイルを再送することで問題は解決したが、その後も添付ファイルが開けなくなる症状にしばしば悩まされることとなる。

【解決策】

添付ファイルが開けなくなる症状はしばしば観測されるが、原因としては次のようなことが考えられる。

（1） 送信側のエンコードの失敗
（2） 受信側のデコードの失敗
（3） 受信側でのダウンロードの失敗

その他に、まれではあるがオリジナルファイルが壊れている場合や利用しているアプリケーションのバージョンが合わない場合がある。しかしながら、多くの場合は上記の（1）〜（3）の場合が多い。また、MIMEのマルチパートを解釈でき



ないメーラを使っている場合には、当然ながら添付ファイルを処理できない。あるいは、MIME のマルチパートを展開できない場合もある。これらの場合は、メールそのものをファイルに保存して、手動でデコードすることも可能であるが、base64[6]などのエンコード／デコードのためのツールの知識などが必要になる。

ファイルの破損による場合は、ファイルを再送してもらう必要がある。

2．3．「決済・稟議」および「電子取引」の場

この場合重要となるのは前回の報告[1]に示したとおり、電子メールの安定性と安全性である。電子メールの安定性はネットワークやサーバの安定性に関連し、安全性に関しては現状では電子メールを利用する者が自ら確保しなければならない。これらのことについては、既にいくつかの報告[1,7]をしているので、今回は省略する。

3．メーリングリストの活用

前節の議論の中で、電子メールをビジネスに利用する場合、必ず複数の人間が関与する方がよいと述べた。そのためには、電子メールの Cc（カーボンコピー）機能を使い、必要と思われる人もメールのコピーを送ることを義務付けるなどが重要である。しかしながら、時として Cc を忘れたり、操作の過程で Cc に入っていた人のアドレスがロストしたりする可能性があることを指摘した。

また、自分宛てのメールには、

（1） 自分があて先となっている（To にアドレスが入っている）

（2） 明示的にコピーが送られてきて

いる（Ccにアドレスが入っている）

（3）送信者に知られないようにコピーが送られてきている（Bccにアドレスが入っている）

の3種類があり、どの形態でメールを受け取ったかにより、対処の方法が異なる。また、Bccの場合は、利用しているメーラによりBccであることを告知する方法が異なるので、注意深くメールを見て、Bccかどうかを判断する必要がある。

さて、複数の人が同じメールを受け取る方法として、メーリングリストと呼ばれるものがある。メーリングリストは、図1に示したように、1つの電子メールアドレス（図の場合はml@hostml.ac.jp）を登録しておき、そのアドレスにメールが届くと、あらかじめ指定されている複数のメールアドレスに同じメールを再配送する。

図1では、ml@hostmal.ac.jpなるメールアドレスにメールを送ると、hostml.ac.jp上のメーリングリスト（以下、「ML」と略記する）のデータベースに蓄積されているメールアドレスのリスト（図1の例では、foo@bar.ac.jpやhoge@eee.ac.jpなど）宛てにメールが再配送される。したがって、MLでは、あらかじめMLの代表メールアドレスとそれと関連付けられる電子メールアドレスのデータベースを用意し、電子メールを送受信するソフトウェア（これをメール転送エージェント（MTA）と呼ぶ）にMLのアドレスエントリを作成し、そのアドレスと処理方法を関連付ければよい。

では、MLを使い、どのようなサービスを展開できるのであろうか。ビジネスシーンから見た場合、次のようないくつかの使用例が想定される。

【事例6：社内業務連絡とトラッキング処理】

事例1として紹介したものと同じである。社内業務連絡を電子メールベースで行う場合、必要に応じてMLを作成すると良い。例えば、営業1課用MLとか、総務課用MLのような必要な部署ごとのML、新製品販促グループMLのような特定グループ用のもの、あるいはプロジェクトチームのためのMLなど、様々なものが考えられる。MLは常設されるものと、アドホックに作成されるものがある。したがって、MLの作成は機動的に行えるようにしておくとよいが、ISPにメールサーバを委託して運用している場合は、MLの設定をISPにて行う必要がある。このような方法では、機動性は失われるがISP側のサービスさえ良ければ、大きな問題とならない。もし、独自ドメイン名サービスと電子メールのサービスをISPに委託するなら、MLの設定についてのサービス内容も確認しておくと良い。

独自ドメイン名を使用する場合、ドメイン名を登録する必要がある。また、その前に、利用したいドメイン名が既に使われていないかどうか確かめなければならない。ドメイン名は.jpの場合、一組織一ドメイン名しか登録できない属性型／地域型ドメイン名と呼ばれるものと、自由に登録できる汎用ドメイン名とに分か

れる。

ドメイン名の登録状況を調査する方法は、JPRS の Web ページ[8]にアクセスして、whois サービスを使うと良い。

[キーワード] 独自ドメイン名サービス：電子メールアドレスの「@」マークから右側をドメイン名と呼ぶ。例えば、foo@bar.ac.jp の「bar.ac.jp」の部分である。通常、ISP との接続契約を結ぶと、電子メールアドレスは、その ISP の持つドメイン名を利用したものが割り当てられる。例えば、豊橋市の CATV 会社である豊橋ケーブルネットワークと契約すると、zzz@xxx.tees.ne.jp なるメールアドレスが割り当てられる。ここで、zzz はユーザが指定したメールアカウント、xxx は豊橋ケーブルテレビ側が指定した電子メールサーバの名前（ホスト名）である。このように、電子メールアドレスとして ISP のものを使っていれば、メールサーバや名前解決のための DNS サーバなどを独自で持つ必要がなく便利であるが、例えば自社独自の名前を使って電子メールサービスを受けることはできない。そこで、独自ドメイン名を取得して、自社名での電子メールサービスを受けることが可能となる。

ドメイン名の登録は最終的にドメインレジストリである JPRS（.jp の場合）に登録しなければならない。しかしながら、一般の組織や人がドメイン名を登録する場合、ドメインレジストリから委託を受けたレジストラに申し込むことで独自ドメイン名を取得できる。JPRS のレジストラの一覧は、JPRS の Web ページに掲載されている。

[キーワード] DNS（ドメイン名システム）：インターネットのサービスプログラムが IP アドレスを利用して、接続先を識別することは既に述べた。しかしながら、我々は、例えば電子メールアドレスのように、ドメイン名を使い相手を指定する。したがって、ドメイン名と IP アドレスを相互に変換するサービス必要となる。そのようなサービスは DNS と呼ばれる。DNS のサービスは、ドメイン名と IP アドレスの相互変換のためのデータベースを持ち、問い合わせに答えるネームサーバと、問い合わせのためのクライアントであるリゾルバと呼ばれるプログラムが相互により変換を行う。リゾルバは、通常 OS に附属しており、ドメイン名から IP アドレスを得る、あるいはその逆のリクエストが来ると、自動的にその問い合わせを指定されたネームサーバに転送する。一方、ネームサーバは届いたリクエストに対して、全世界に散らばる他のネームサーバと協調して、リクエストの答えを見つけ出し、リゾルバに返す

ドメイン名を登録するには登録費用や年間での維持費用（データベースの維持費用）がかかる。これらの費用は登録を依頼するレジストラごとに異なるので、それぞれのレジストラの Web ページであらかじめ確かめる必要がある。

ドメイン名を登録しただけではインターネット上ですぐに利用できるようにならない。実際に利用する場合は、DNS と呼ばれるサービスのためのサーバ（ネームサーバ）

を構築し、自分のドメインのためのデータベースをきちんと管理しなければならない。ネームサーバの設定が終わったなら、ドメインレジストリに申請して、ネームサーバを登録しなければならない。登録が完了し、自分のドメイン名がインターネット上からアクセス可能となり、ようやく独自ドメイン名を利用したサービスが可能となる。

このような一連の作業は技術的なスキルを要求されるので、可能ならばISPやネットワークの納入業者に依頼するとよいが、自分自身でも最低限の知識を身につけ、特にDNSのデータベースが正しく保たれているかどうかチェックを怠らないようにすべきである。

3．1．MLの実現方法

MLの実現方法には次の2つのがある。

（1） メールの別名機構を使い設定する

（2） ML サーバソフトウェアを使い設定する（なお、この場合もメールの別名機構への代表メールアドレスの登録は必要）

（1）の方法はMTAが持っているメールの別名機構[9]を使って、MLの代表アドレスと登録すべきメールアドレスを関連付けする。例えば、MTAとしてpostfix[10]と呼ばれるソフトウェアを使っているなら、そのaliases（メールの別名を登録するデータベース）に代表メールアドレス（この場合、fooとする）を次のように登録することでMLを実現できる。ここで、addr1以降が個別のメールアドレスとなる。（2）の方法については、次節で解説する。

```
# ML Setting example in aliases database

foo: addr1,addr2,addrs,...
```

【ML作成のためのガイドラインの例】

MLを使っても、実際にはそれを運用する規程がなければ問題の発生に対処できない。そのため、ここでは社内連絡用ML作成のための指針を考える。MLは基本的に、常設MLとアドホックMLがあることを示した。常設MLは固定された部署などのためのものであり、通常は、会社の組織と一致したものとなる。一方、アドホックMLは、必要に応じてその都度作成されるMLである。したがって、作成や消去のためのガイドラインを作成しておく必要がある。以下、常設ML及びアドホックMLのための作成と消去のガイドラインの一例を示す。

常設ML作成及び消去のためのガイドライン（例）：

（1） 社内の部・課・係りに対して、それぞれ部、課、係りのMLを設置する。部、課、係りにはそれぞれに属する全員のメールアドレスが登録されるので、利用する場合、情報を伝達する必要がある範囲を十分考えて、メールを出すこと。

（2） 社内の常設委員会のためのMLを設置する。例えば、営業部課長会議など、常に設置されている委員

会には、それぞれの委員の電子メールアドレスを含めたMLを用意するので、委員会の連絡事項や資料の回覧にはそれを使い、通常の部や課のMLと有効に使い分けること。

（3） その他必要と思われる場合（課内のグループや作業部会など）は常設のMLを設置するが、必要がなくなった場合は、直ちに届け出て、消去の手続きを取ること。

（4） MLの消去は必要時に行う。必要時とは、社内の機構改革等により組織改変が行われた場合や、明示的にMLの消去の手続きが取られたときである。

アドホックML作成及び消去のためのガイドライン（例）：

（1） 社内おいて必要とされる場合は、アドホックなMLを設定することができる。

（2） アドホックなMLは主任以上のMLの責任者が、MLの利用目的と必要性、登録電子メールアドレス、必要な期間を明示して（様式××を使うこと）、システム課に申請すること。システム課では、申請に基づき、当該部課の長に確認後、必要性が認められればすみやかにMLを作成する。

（3） アドホックMLについては、その利用目的を逸脱しないように、十分に中止すること。

（4） アドホックMLが必要なくなった場合は、直ちにシステム課に届けること（様式○○を使うこと）。システム課は当該部課の長の確認が取れ次第、MLを消去する。

なお、MLはそのままトラッキング処理の単位として利用することができる。そのためには、MLサーバを使い、どのMLからのメールかを明示できるようにしておくことと、表題によるメールのグループ化の機能を持つメーラソフトを組み合わせて利用する。

3．2．MLの活用事例

【事例7：顧客からの問い合わせ処理】

前述の事例2の場合と同様のケースである。顧客からの問い合わせ処理は、たとえ主に担当する者が一人であっても、問い合わせ内容や応対に対する周知やスムーズな引継ぎのためにはMLとして運用することが望ましい。例えば、info@foo.co.jpのような問い合わせアドレスを用意して、それをMLとして、複数のメンバーを登録しておくことは、今日ではよく行われている。

ただし、複数のメンバーの役割分担を明確にし、メンバーに支障がある場合は、それをスムーズに代行できる体制を取っておくことが大切である。

【事例8：情報提供ツールとしての利用】

情報提供ツールとしてMLを利用することができる。例えばメールマガジンなどはその代表例である。メールマガジンは定期刊行物として、購読者に各種の情報を提供することができる媒体として、

急速に浸透しつつある。

ところで、メールマガジンなどを送付する場合の注意として、どのようにして顧客の電子メールアドレスを集めるかという問題と、顧客の電子メールアドレスなどの情報漏洩を起こさないことがあげられる。

メールマガジンは電子メールを使った定期あるいは不定期刊行物の総称である。メールマガジンは顧客への情報提供の一つの手段として、ビジネスの世界で定着しつつある。また、ビジネスのみならず、例えば小泉内閣のメールマガジンなどのように、あらゆる分野で利用されつつある。

メールマガジンなどで顧客のメールアドレスを取得する方法として、**オプトイン**と**オプトアウト**という手段がある。これらは、顧客の電子メールアドレスの取得とその後の処理に関する 2 つの考え方である。前回の報告[1]にオプトインとオプトアウトの考え方について説明してあるが、簡単に記すと次のようなことである。オプトインは電子メール配信以前に合意を取る方法であり、Web ページなどを使い電子メールアドレスを事前収集すると共に、メールマガジンや広告メール配信の合意を取っておく方法である。一方、オプトアウトはメール送信後に合意を取る方法であり、電子メール中にメールが不要な場合の対処法を明示しておき、メールが不要とされた場合には、迅速にそれに対処することが義務付けられている。メールマガジンの場合は、オプトインにより事前に合意を取っておくほうが安全である。ただし、オプトインの場合でも、メールが不要となった場合の対処法を明示しておかなければならない。

次に**情報漏洩問題**について簡単に述べる。電子メールアドレスは個人情報である。そのため、情報の取り扱いには十分注意し、決して情報漏洩を起こさないようにしなければならない。個人情報の取り扱いに関しては 2005 年 4 月より「個人情報の取り扱いに関する法律」[11]、いわゆる個人情報保護法が完全施行され、個人情報の取り扱いに対する注意義務が法的な拘束力を持つに至っている。

以下では、その他の ML に関する問題をいくつか指摘しておく。ISP や各種インターネットサービス会社によっては、無料の ML サービスを実施しているところがある。これらの多くは、無料サービスを実施する見返りとして、各種の広告を配布する電子メールに付加することを条件としている。このような ML のサービスを利用する場合、登録者に事情を説明し、広告付きメールが送付されることをあらかじめ知っておいてもらう必要がある。もし、このようなことを怠ると、新たなトラブルの原因となるので注意する必要がある。

「メールマガジンとメーリングリストは異なるのか」という問いを受けることがままある。厳密に言えば、この 2 つは異なる。なぜなら、メールマガジンは特定アドレスから届くだけであり、その特定のアドレスはメールを出すことは一般的に許されず、メールマガジンを購読し

ている読者に対して、何か共有情報を発信することはできない。それに対して、MLは、特定のメールアドレスを使い、登録者間で自由に双方向にメールの授受ができ、共有情報を提供することができる。ただし、事象的には異なるが、実際に利用されるソフトウェアはMLのためのソフトウェアを使っている場合が多い。そのため、この2つは親戚関係にあると言ってよい。

3．3．ML管理ソフトウェアの設定と運用

ML管理ソフトウェア（これを便宜上「MLサーバ」と呼ぶ）の設定とその運用方法について、fml[12]と呼ばれるソフトウェアを例として紹介する。その前に、MLサーバとしてどのようなものがあるかを表2に示しておく。

表2．MLサーバソフトウェア[13]

ソフトウェアの名称	使用料金など	使用システム
Majordomo	無料	UNIX
fml	無料	UNIX, Windows NT, MacOS X
CML	無料	UNIX
Distribute	無料	UNIX
Mojo Mail	GPL	UNIX
Post Office	有料	UNIX, Windows2000/NT, MacOS X

fmlは日本で作られたMLサーバソフトウェアであり、そのため日本語による解説も豊富である。fmlはhttp://www.fml.org/から容易に入手できる。ただし、現在のfmlにはPerlと呼ばれるインタープリタ言語が同時にインストールされている必要がある。UNIXの場合はほぼデフォルトでPerlがインストールされているが、Windowsの場合は、別途Perlをインストールする必要がある。fmlのインストールはPerlがインストールされていれば簡単である。

fmlの設定は、makefmlコマンドで新しいMLを作成後に、そのMLに対する種々の設定値を設定ファイル上で作成することで行われる。実際のMLの作成と設定に関しては、既に示したfmlのWebページを参照してほしい。

fmlを使ったMLの運用は2つの段階に分けて考えなければならない。最初の段階は、fmlによるMLの初期立ち上げの段階であり、この場合には次のような作業を必要とする。なお、実際のコマンドの使用例において、下線の部分は、設定すべきMLのために必要な文字列を入れるものとする。

（1） makefmlコマンドを使った新しいMLの作成：次のコマンドの入力例のようにMLの名称を指定してMLを新規に作成する。

```
# makefml newml ML の名称
```

（2） config.phの編集によるMLの設定：config.phはMLを作成したディレクトリ内にデフォルト状態で作成される。MLの管理者は必要に応じてconfig.phを編集し、MLが希望通りの動作をするようにしなければならない。

（3） guide や help ファイルの作成：ML の使用法を記した help ファイルや ML の目的などを記した guide ファイルを適宜編集する必要がある。

（4） 初期ユーザの登録：ML の初期ユーザ名を登録する。fml の場合、ユーザの登録は members と actives の 2 つのファイルに行わなければならない。members は ML に対してメールを出すことができるアドレス（config.ph においてメールの受け付けを members_only とした場合）となる。ただし、メールの受け付けを any（全て OK）とした場合は、このファイルは意味をなさない。一方、actives はメールが再配送される電子メールアドレスを記入する。例えば、複数のメールアドレスを使ってメールを出す可能性のある場合は、members にあらかじめそれら全てのアドレスを登録しておく必要がある。また、受け取りに関しては1つのアドレスだけにしたい場合は、actives に利用するアドレスを1つだけ記入すれば良い。

（5） MTA の別名ファイルへの登録と MTA の再起動：全てのファイルの準備が終わったなら、MTA の別名ファイルに ML のためのアドレス登録を行い、MTA を再起動する。

以上で、fml を用いた ML の作成が完了する。ML の運用の第二段階は、ML の運用が始まった後の処理について発生する。例えば、新しいメンバーの追加やメールアドレスの変更、削除、メールの配送の確認などである。また、必要に応じて ML 内での議論をチェックし、誹謗中傷メールなどが発生しないように監視する必要がある。

fml 以外の ML サーバに関しては、それぞれの設定方法があるので、各 ML サーバに付属するマニュアルや Web ページを参照してほしい。

3．4．ML における情報共有時の問題

ML を運用する他の目的は、顧客を交えた情報共有の場を形成することである。これは、いわゆる BBS（掲示板機能）の電子メール版である。このような情報提供と共有は、単に顧客と企業の関係だけでなく、顧客間の関係が生じるので注意を要する。ここでは、顧客間の情報共有を含む ML の運営において注意しなければならないことを、事例を中心として紹介する。

【事例9：誹謗中傷問題】

A さんは、会社がある製品のモニタのために立ち上げた ML の運営を任されていた。あるとき、ML に登録されている hoge@aaa.jp さんから、同じく ML に登録されている foo@bar.jp さんのメールに対するクレームメールが舞い込んできた。このクレームは foo@bar.jp さんの些細な

発言から生まれたものであり、それを自分に向けられた誹謗中傷発言として受け取った hoge@aaa.jp さんが反応してしまったのである。A さんは、この問題を解決するために、両者に冷静な対応を望むメールを個人的に送ったが、双方のクレームメールはエスカレートしていくばかりであった。やむなく、A さんは、二人のメールアドレスから ML へのメール発信を一時的に停止して、沈静化を図った。ところが、今度は両者の矛先が A さんに向けられ、A さんに対する嫌がらせメールへと発展してしまった。

この ML には、ML 登録時の契約規程がなく、A さんは独自の判断に基づき対処せざるを得なかったために、騒ぎが大きくなってしまった。

【解決策】

このような誹謗中傷問題は ML や掲示板など、インターネット上の情報交換における多くの場面で見受けられる。実は、この問題はインターネットの初期から観察された問題であり、当時から多くの打開策が検討されたが、完全な解決策は見出せていない。現在では、ネチケットと呼ばれるエチケット問題や情報倫理と呼ばれる倫理観に訴えてこの問題を解決することが主流であるが、実際には誹謗中傷問題は後を絶たない。

しかも、この例のように対処した人に矛先が向くこともしばしばある。企業の運営する ML の場合、他者に不快な思いをさせるよりも企業内の責任者が対応を一任される場合が多い。しかしながら、本来、この問題は ML 全体の問題として取り上げ、参加者全員で解決すべきである。そのでなければ、同じ問題が繰り返されることになる。

この問題を解決する方法は、参加者に対するルールを明確化した憲章と規範を示しておくことであり、これらを守らない場合は、全員の合意の元にしかるべき処置を取れば良い。もしも、憲章や規範が明示されていない場合は、そのような問題が起きた時に、全員で議論して、早急に作成すべきである。

なお、議論するときには必ず議長役を置き、議長が議論の流れをコントロールすると、スムーズな展開が得られる。議長役は、できれば可能な限り中立的な立場にある人を選ぶと良い。

【事例１０：著作権法違反】

B さんは、自分が ML に送った画像がそのままある Web ページで使われていることを見つけて、ML に対してクレームのメールと事実調査の照会を行った。ML を管理していた C さんは、直ちに事実関係を調べ、ML に注意喚起のメールを送ると共に、当該 Web ページの管理者と連絡を取り、当該画像を使用した経緯を入手した。その結果、D さんが B さんに無断で画像を利用したことが判明した。

【解決策】

電子媒体により交換される情報であっても、著作権はそのまま適用されることが、現在の著作権法[14]では明示されている。したがって、ML に流れた個人の画像

などの著作権はあくまでもその個人に帰属する。MLでは、その憲章や規範の中でこのような著作権に対する条項を示す必要がある。また、MLに流れたデータを再利用する場合は、必ず著作権者の許諾を得るようにしなければならない。

【事例１１：リテンションマーケティング的な観点】

ビジネスにおけるMLの運営において、コンクェスト（新規顧客）を優先するのかリテンション（既にいる顧客）を優先するかは議論の分かれるところである。しかしながら、現在ではリテンションマーケティングを優先し、それとコンクェストマーケティングを融合させる方策を採ることが良いとされている。したがって、リテンションマーケティング的な観点を持ってMLを運用する必要がある。そのための観点を以下にまとめておく。

（1）情報発信時の内容チェック：不要な情報の発信を抑えると共に、ウイルス付きメールやSPAMメールとなるような内容をMLに流さないための処置を講じておく必要がある。その他、MLに対するサービス妨害攻撃（「空の電子メールを多数送る」とか「不必要に大きな添付ファイルを送る」）なども想定する必要がある。

（2）違法行為に関するチェック：誹謗中傷問題とか著作権法に関する問題点は、既に述べたとおりである。

（3）顧客のプライバシー管理：顧客情報の漏洩に注意するとともに、登録者間での情報のやり取りについても注意を喚起する必要がある。

これらのことは基本的に当然のことである。MLに参加している顧客に対して、当然のことを要求するのだから、という安易な発送で簡単な説明だけで済ませてしまってはいけないのである。あくまでも、憲章と規範をきちんと制定し、それを守ってもらう方策をめぐらさなければ、せっかく獲得した顧客を逃がすことになる。

４．電子メールに対する最近の脅威

この節では、電子メールの安定性や安全性を脅かす最近の脅威について解説する。

電子メールのセキュリティに関して最大の脅威となるのはウイルスであり、ウイルスは電子メールを使うすべての局面で問題となるために、その対策を怠ることはできない。今日、ウイルス対策に対しては、クライアント側だけでなくサーバ側でも対策が進み、ウイルスに対する耐性は上がってきている。しかしながら、いつ新種のウイルスが猛威を振るうかわからないため、電子メールの添付ファイルの取り扱いには最新の注意を払う必要がある。

一方、電子メールをビジネスで利用する観点から考える場合、別の脅威が存在することは前回の報告[1]の中でも述べた。ビジネスの内容伝達や受注そのものが電子メールで行われることを前提とした場合、次のような問題点として、次の４つについて指摘した。

- 電子メールで受注を受けたが、そのメールは確かに発注者から送信されたものか（**送信者の認証**）
- 電子メールで顧客リストを本店－支店間で交換したいが、顧客リストが外部に漏洩することはないか（**電子メールの秘匿性**）
- 電子メールで受注した受注伝票の内容が正しいかどうか（**電子メールの完全性**）
- 電子メールで受注したが、発注者がそのようなメールを送っていないと主張したらどうなるか（**電子メールの送信否認防止**）

これらのことは、公開鍵暗号[15]を用いることで、安全性を確保できる。そのために使われる技術的基盤は、PGP[16]のようなプライベートな公開鍵暗号システムや、PKI（Public Key Infrastructure）[17]と呼ばれ、社会基盤として整備されつつある公開鍵暗号システムをまで多くのものが存在する。

これらの技術基盤は全て公開鍵暗号と呼ばれる非対称の暗号鍵システムを利用している。公開鍵暗号では、**秘密鍵**と呼ばれる利用者が秘匿している鍵と**公開鍵**と呼ばれる公開されている鍵を利用する。そして、秘密鍵で暗号化したものは公開鍵でのみ復号化でき、逆に、公開鍵で暗号化されたものは秘密鍵でのみ復号化できる。したがって、秘密鍵で署名することで認証と完全性及び否認防止を行い、公開鍵で暗号化して送ることで秘匿性を確保する。

このようにして、電子メールに対する一定の安全性を保証する仕組みが整えられつつある。

しかしながら、今日ではスパイウェアであるとか Phising といった、電子メールの関連する新たな脅威が登場しつつある。本節では、既に PGP を使った電子メールの暗号化と署名の問題は報告[1]しているので、PKI の利用について最初に概観し、その後、新しい脅威について述べる。

4．1．PKI による電子メールの安全性の確保

PKI（Public Key Infrastructure）とは、公開鍵暗号システムを用いた本人認証と暗号化の仕組みであり、公開鍵暗号基盤と訳される。

PKI についての詳細は、他の文献[18]に詳しく紹介したので、ここでは、電子メールとの関連についてのみ述べる。基本的に現在の PKI は X.509[19]と呼ばれる国際標準の公開鍵に対する証明書システムに基礎を置いている。つまり、PGP が「信用の和」と呼ばれる自己署名を含めた、自己責任による安全性の確保を行うのに対して、PKI では登録局と認証局と呼ばれる公的な機関、あるいは公的な機関の代行機関により発行された公開鍵に対する証明書（X.509 証明書）を使って安全性を確保する。

X.509 証明書の構造を図 2 に示す。図 2 の構造の署名部分以外に対して、ハッシ

ュ関数を用いて「メッセージダイジェスト」を作成し、それを証明書発行機関（認証局）の秘密鍵で暗号化し、署名を作成する。作成された書名は、図 2 の署名部分に入れられる。証明書の検証は、署名部分以外のメッセージダイジェストを作成し、署名を複合化して得られるメッセージダイジェストと比較することで、行われる。

このようにして、証明対象ユーザの公開鍵が正しいものであることを証明する。したがって、検証された公開鍵を使うことで、通信相手に対して安全な電子メールの送信が可能となる。

バージョン
シリアル番号
証明書発行者
発行者ユニーク識別子（ｖ２）
証明書対象ユーザ
ユーザユニーク識別子（ｖ２）
証明対象公開鍵アルゴリズム
証明対象公開鍵
証明書有効期限
証明書拡張（ｖ３）
署名アルゴリズム
署名

図２．X.509 証明書の構造

ただし、実際に PKI を利用した公開鍵の利用を行うには、あらかじめ自分の鍵に対する証明書を発行してもらうひつようがある。その際の本人確認をおこなうのが登録局であり、登録局の本人確認が厳密に行わなければ、その後の認証局における証明書発行が正しいものであるという保証はなくなる。

PGP の場合[7]の場合においても指摘したが、X.509 証明書を用いる場合でも、あらかじめ鍵ペアの生成と証明書の取得を行い、それを電子メールシステムに組み込む必要がある。X.509 を使った電子メールに対する公開鍵を利用するには、S/MIME[20]などを利用する必要がある。

４．２．電子メールに関する新しい問題

最後に別の観点からの引き起こされる、新しい電子メールに関する問題を指摘する。それは、スパイウェアの横行による情報漏洩と Phising に見られる電子メールを使った詐欺行為である。

スパイウェアとはコンピュータに寄生する小さなプログラムである。基本的にはウイルスの一種であるが、ウイルスのような積極的な活動はせずに、寄生したコンピュータの種々の情報（ユーザ情報、電子メールアドレスの収集、特定のファイルの盗聴や通信状態の監視等）を収集し、特定の電子メールアドレスに送ったりする。また、最近ではWebページに監視システムが設置されており、特定の情報を要求し、それに答えないとページが表示されないようなものもある。あるいは、キーロガーと呼ばれるプログラムはユーザが入力したキーストロークを全て記録し、そこから各種の情報の取得を目論むものもある。

これらのプログラムの目的は、基本的に情報の収集であり、収集された情報は時として、電子メールシステムを使った Phising のための基本情報として使われる。この場合、電子メールアドレスを詐称するのでは

なく、正規ユーザとしてそのメールアドレスを利用したりするため、被害者側からは把握しにくい。

Phising は fishing からのアナロジーによる造語である。Phising とは、釣り人があたかも餌を付けた針をたらして釣りをするように、各種の情報を、電子メールなどを使いばら撒いて詐欺行為に及ぶことである。例えば、インターネットを介さなくても通常の郵便による利用料金の振り込み詐欺などと同列に扱って良い。

ただし、インターネットを使った Phising 詐欺は、通常の郵便よりも短時間で数多くのターゲットに対して餌をばら撒くことができ、しかも、犯罪者の秘匿性は格段に高くなる。また、スパイウェアなどから得た実在する電子メールアドレスなどを使うことで、相手により信憑性のある餌をばら撒くことができるようになる。

いずれにしても、スパイウェアの横行や Phising 詐欺は、電子メールの利用を含めた新しいインターネット上の脅威となっており、電子商取引などを阻害する要因となると考えられる。

PKI による認証は Phising などを防ぐためにも有効と考えられるが、実際に普及するにはまだ時間がかかると思われる。

5．最近の法制との関係

2002 年に施行された「特定電子メールの送信の適正化等に関する法律」[21]において、迷惑メールの防止に対する法律ができあがり、電子メールの利用などにも一定の法律の枠組みが示された。その後、IT 関連の法律の中で、今回は次の 2 つについて考える。1 つは 2004 年に公布され 2005 年度 4 月 1 日より完全施行された、「個人情報の保護に関する法律」[11]であり、他の 1 つは「電子文書法」あるいは「e-文書法」と呼ばれる、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」[2]である。

個人情報の保護に関する法律は、その名のとおり、個人情報と保護することを意図して制定された。官公庁が保有する個人情報の保護に関しては早くから法令が整備されていたが、今回の法律の施行により、官民問わず個人情報の保護について留意しなければならなくなった。もっとも、先進的な企業はインターネットなどのコンピュータネットワークの普及とともに、個人情報の保護に対する対策を打ち出しており、今回、駆け込み的にあわてたのは、むしろそのような保護対策をなおざりにしてきた特定の行政機関や教育機関、あるいは企業などであろうと推測される。

個人情報の保護に関する法律の解説は数多く存在[22]するので、ここでは深く触れることはしない。ただし、第一条の「高度情報通信社会の進展に伴い個人情報の利用が著しく拡大→個人情報の有用性に配慮しつつ、個人の権利利益を保護」という目的と第三条の「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであり、その適正な取扱いが図られなければならない。」という理念は、ネットワーク社会を迎えて今日、当たり前のこととして認識されなければならい。著者は、JPNIC[23]において長

年インターネットのディレクトリサービスを担当する立場にあったが、1994年以降、急激に拡大するインターネットに関連した各種の情報を公開すべきか隠蔽すべきかの議論に巻き込まれたことがある。その際、個人情報の保護と公益とのバランスを図ることの重要性を学んだ。このようなバランス感覚は、実際の環境に遭遇しないとわからない部分が多く、明確な指針を与えられらいのが残念であるが、必要なことは、先の目的と理念を見失わないことであると考えている。

さて、電子文書法であるが、これは、正式な法律名から明らかなように電子的なメディアによる文書が紙媒体の書面と法律的には同じ取扱いを受けることを保証するものである。しかも、紙媒体の書面をスキャンしたものについても、一部その効力は及ぶと考えられている。これにより、大量の文書を電子的な記憶として処理することが可能となり、ネットワークを介した電子商取引は大きな飛躍を遂げることが期待される。

その反面、電子的な書面に対する保護と認証の問題がますます重要視されることになる。今回は、紙面の都合上、この法律の全体像を明らかにすることはできないが、近い機会に、電子文書法に関する整理を行いたいと考えている。

さて、電子文書法によれば正しく署名された電子メールは書面と同じ効力が発揮できると思われる。したがって、今後は、これまで曖昧であった電子メールによる受発注などの商取引行為がきちんとした法律に裏付けられることが期待される。

6．終わりに

今回、電子メールの利用に関連する種々の問題点を、ビジネスシーンごとに整理した。また、電子メールをビジネスに利用するための裏付けとなる電子文書法の制定についても注意した。このような流れはこれからさらに加速するもとと考えられ、電子メールはビジネスにおけるさらに重要なツールをなると思われる。しかしながら、そのためには、電子メールに対する安全性と安定性をより高める努力が必要である。

7．文献など

[1] 奥山徹、種田智哲、「ビジネスにおける電子メールの活用と最近の法制との関係」、 情報学研究（朝日大学情報教育研究センター紀要)、Vol.13、pp.1-25、2004.

[2]「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」、2004.
http://www.mhlw.go.jp/shingi/2004/06/s0624-5a.html

[3] E ジャパン協議会、「企業における電子メールの利用、及びインターネットのビジネス利用に関する動向調査」、2001.
http://www.ejf.gr.jp/report/daikigyo.htm

[4] 人が一日に処理できる能力についての詳しいデータはないが、例えば、浜嶋鉱一郎、「ＩＴ(情報技術)を身近

に感じるために－２」、2002.（http://www.oakis.co.jp/soft/oje/infotech_2.html）によれば、人は一日数十通の電子メールの処理に辟易するであろうと指摘している.

[5] N.Freed and N.Bornstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC2045, IETF, 1996.

[6] Chapter 6 in Reference [5].

[7] 奥山徹、「PGP(Pretty Good Privacy)－あなたの電子メールは安全ですか？－」、情報学研究（朝日大学情報教育研究センター紀要)、Vol.13、pp.41-60、2004.

[8] http://www.jprs.jp/参照.

[9] 秋丸春夫、奥山徹、「情報通信プロトコル－LAN とインターネット」、pp.163-164、2001.

[10] http://www.postfix.org/参照.

[11] 「個人情報の保護に関する法律」、2004. http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

[12] http://www.fml.org/参照.

[13] http://www.kt.rim.or.jp/~atsato/ml/basic/software.html 参照.

[14] 「著作権法」、1970. http://www.cric.or.jp/db/article/a1.html

[15]例えば、メル、他、「暗号技術のはなし－シーザー暗号から公開鍵暗号まで」、日経 BP 企画、2001、などを参照.

[16] http://www.pgpi.org/参照.

[17] 例えば、http://www.pki-page.org/など参照.

[18] 郭崢、奥山徹、「中国における PKI の利用の現状と問題点」、朝日大学大学院経営学研究科紀要、Vol.5、pp.1-18、2003.

[19] 大山実、他、「X.500 ディレクトリ入門—LDAP/X.509 公開鍵証明書/ディジタル署名」、東京電機大学出版局、2001.

[20] B. Ramsdell, ed. "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC3851, IETF, 2004.

[21] 「特定電子メールの送信の適正化等に関する法律」、2003. http://law.e-gov.go.jp/htmldata/H14/H14HO026.html

[22] 例えば、個人情報保護法研究プロジェクト、「実践! 個人情報保護～弁護士による核心的 Q&A」、毎日コミュニケーションズ、2005、などを参照.

[23] http://www.nic.ad.jp/参照.

奥山　徹　（経営学部情報管理学科教授）