電子メール技術動向とシステム構築

熊谷 誠治（(株) 電通国際情報サービス ディジタルキャンパス）
渡部 直明（(株) オレンジソフト）

１９９９年12月16日

InternetWeek 98　**国立京都国際会館**

(社)日本ネットワークインフォメーションセンター編

目的

電通国際情報サービスの熊谷は、今2,000人ぐらいのユーザを抱えたシステムを運用しており、オレンジソフトの渡部はＰＧＰやＳ/ＭＩＭＥに対応しているメールソフトを開発しています。２人共、コンサルティングの仕事もやっておりますので、お互いのエリアは重なっている部分もあり、異なる部分もあります。作成者側と利用者側、サーバとクライアントのような立場になり、２人で説明を進めていきます。全体のテーマは「電子メール技術動向とシステム構築」ですが、大きく２つのパートに分け、前半を熊谷がメールサーバの運用や安全なメール・システムについて説明させて戴き、後半は渡部が暗号メールを中心に説明していきます。

目次

1. メールサーバの運用

メールはビジネスインフラ

・これまでは…
  - 「電話が止まると仕事にならない」
    重要なビジネス・インフラだった
・今は…
  - 「メールが止まると仕事にならない」
    メールがビジネス・インフラに成長した
・あなたの会社のメール・システムは大丈夫?
  - トラブル発生時に何時間以内に回復しますか ?
  - どのようなトラブルを想定していますか ?
  - 利用者はどのようなことに気をつけるべきですか ?

皆さん多くの方が既に電子メールを使われていて、メールがないと生活ができないようになりつつあるのではないかと想像しております。昔は全部電話を使っていたのですが、最近は電子メールに変わってきました。トラブルが起こるとどうなるでしょうか？電話の場合ですと、社内に専門の人がいなくても電話工事屋さんがいて、総務部の人が連絡すると修理に来てくれます。通常の場合、企業の中の電話が長時間止まるということはありません。ところが電子メールの場合ですと、十分に考えられていないケースが多いのです。利用者の中には、なんとなく電子メールは動いているが、誰が運用している知らなかったり、電子メールというのは消えるものだという事を信じている方も世の中にはいらっしゃいます。電子メールを利用していて、届かなくても仕方がないという事が前提ですと、通信インフラとして電話の代役を果たすことができないことになります。

トラブルが起こるとどうなる?

電子メールにトラブルが起きると、ただ単に通信ができなくなるだけでなく、機会損失を含めて考えると被害はかなり大きくなる可能性があります。この事をしっかり踏まえて、メールシステム全体を考えておかなければならないという事を、これから説明したいと思います。

トラブルはいつ復旧しますか?

トラブルが起こって、システム運用者と利用者の一番重要な課題は「いつ復旧するか？」ということです。復旧までに、 ３日かかるのと30分かかるのとでは、その対応の仕方、仕事の進め方が変わってきます。メールが届かない場合、電話をすべきなのか、それとも復旧を待てば良いのか判断する必要があるのです。
一方、運用している側にとっては、何かトラブルが発生して止まったことは事実なのですが、「原因をどこからどういう具合に追及していくか？」、原因が分かっても、「復旧させるための手段はどうするか？」を考えなければなりません。メールサーバのマシンが壊れた。エラーを吐いているから、ハードウェアの故障らしい。しかし、ハードウェアの故障のときに、どういう手順で回復させるのかが明確でないと、右往左往するだけで時間だけが経過するということが起こってきます。そうならないために、対応の手順書をつくることが非常に重要になるのです。
トラブルが起こったら最悪何時間以内に復旧させるのかという目標は、電子メールシステムの作成時点から十分検討をしておく必要があります。これは導入するハードウェア構成や運用にも関係してきます。ノンストップから運任せまで、目標を決める事が必要です。

どのように復旧しますか?

壊れたシステムは、復旧させないといけませんが、一般的には次の手順をふみます。
・トラブル発見 - ユーザに任せる ?
・トラブルの内容特定 - 状況から本当のトラブルを見極める
・トラブル原因究明 - トラブルの様子から原因を探す
・トラブル原因排除 - 原因を排除する
・トラブル復旧 - 関連する影響を調べて、問題点をすべて直す
・

トラブルを避けるために

トラブルを避けるのと、トラブルによる影響を抑えるという事を、考えておく事は非常に重要です。明らかなのは、準備がないと対応が遅れるということです。メールが重要なものになればなるほど準備が大切になってきます。よくあるトラブルの原因としては停電、ハードウェアの故障、ソフトウェアのバグ、設定ミスや操作ミス、があげられます。実際に対応策を考えている企業は少なく、対応をしっかり考えておかないと、安定してメールを運用できないことになります。

目標復旧時間を決めてますか？
・トラブルによって復旧時間は違う
  - ハードウェアトラブル → 修理 + リストア
  - 停電 → 停電復旧時間 + [ハードウェアトラブル]
  - 設定ミス → リストア
  - インターネット接続 → プロバイダ次第
・復旧時間の想定によってコストが違う
  - 冗長性の高いシステムはコストも高い
  - 万全な体制は金がかかる
    24時間オンサイトメンテナンス契約
    要員を配置すれば人件費がかさむ
・金イトの世界
トラブルにより復旧時間はことなりますが、メール・システムの目標復旧時間を決めるのは重要です。逆に、復旧時間を保証するからお金をかけられるとも言えるのです。しっかり準備をすればするほどお金がかかってくる。「金イト」といって、金に糸目をつけないという意味なのですが、金に糸目をつけなければ目標の復旧時間を縮められるけれども、そうでなければ目標の復旧時間というのは長くなってくるということです。

停電
停電の原因は次の事が考えられます。
・工事や検査に伴う停電
・事故による停電(突然襲ってくる、機器の故障やデータの破損につながることも、回復時間が分からない)
・事故停電は避けられない(UPSで守る)
停電事故に対しては、ＵＰＳで守るという手があります。、ＵＰＳは非常に重要だと思います。
熊谷 ＵＰＳは入れられていますか？
渡部 勿論です。二重にしています。
熊谷 ＵＰＳのテストはしていますか。
渡部 ＵＰＳのテストは停電になる時にします（笑）。ビルが停電になる時に、ＵＰＳで何分もつかというテストをしています。
熊谷 停電して、初めてＵＰＳが機能していなかったことがわかるケースが多くありますね。

ハードウェアの故障
・機械は必ず壊れる
・データの破損を防ぐ
この２点が、当然であり重要です。
ハードウェアの故障によってディスクが壊れてしまえば、中のデータは消えてしまう可能性が高くなります。そうなると、データのバックアップを取る方法を考えるのですが、電子メールは常時送られてくるので、ほとんど有効ではありません。それ以外の方法でデータを守るには、ディスクを二重化したり、レイドディスクを使うという方法があります。

ソフトウェアのバグ
ソフトウェアにはバグがつきものです。 それが原因でトラブルを生じることもあります。バグの少ないソフトを使うことが重要なのですが、ソフトウェアが製品としてきちんと機能を果たすか、実績として使われてきちんと動いているかという処で選択する事になります。

設定ミス・操作ミス
設定ミスや操作ミスは、人間がやる事なので発生するのですが、いかに影響を大きくしないかということが重要です。利用者の教育というのも重要になると思います。

トラブル対応マニュアル
・トラブル発生時の連絡先
  - トラブルの受付体制と関係者との連絡方法
  - メンテナンス会社の連絡電話番号
・トラブル検出のしくみ
  - 第一報はユーザから届くことが多い
    「メールが送れない」、「メールが届かない」
  - ユーザが検知できないトラブルもある
    管理者が検出しないとトラブルが続く

- 検出するしくみが重要に
・過去のトラブルをデータ・ベースに
- 同じトラブルでは時間をとられない

トラブル対応マニュアルを作りましょう。トラブル発生時の連絡先や、どういうふうに連絡するのかを書いておくと、システム運用者はすごく楽になります。又、過去のトラブルを記録に残しておくと、同じトラブルが起こったときに発見が早くなるので有効です。

耐障害性の高いメールサーバ

障害に強いサーバを作成するには次のようにします。

・予備マシンや部品を用意する
- 故障すればマシンを交換
- 故障した部品を交換

・システムを２重化する
- ミラー・ディスク、RAID5、ホット・スタンバイ、フェイル・オーバー

・停まらないコンピュータを用意する
- 銀行システムなどで使われている
- 非常に高価
- サーバが停まらないだけでは運用は続けられない

金をいくらかけるかということが、対障害性につながってくると思います。

メールシステムの安定運用

・壊れにくい機器と安定したOS
- 世の中には1か月連続運転できないようなOSもある
  負荷が高まれば早くトラブルが出る

・迅速なメンテナンスの受けられる機器
- “普通の” PCのオンサイト契約じゃだめ

・集中メールシステム(サーバが1台)
- 集中方式にすれば停まるときはすべて停まる
- 分散方式は利用者が構成を意識する必要あり
- 離れた場所のサーバは対応が遅れる
- 機器が増えればトラブルも増える

メールシステムの安定運用という面で考えてみると、ハードウェアが壊れにく、なおかつ安定したＯＳであるということが重要です。私の会社ではメールの集中運用をやっていまして、メールサーバを１台にしていいます。それを社員全部(メールの利用者が2,000人ぐらい)が１台のメールサーバを使っています。集中運用なので、止まればすべて止まり余計なアナウンスが必要ないのです。止まりましたと言えば良いのです。分散にすると、１つが壊れても別が使えて大丈夫という考え方もあります。どちらにするかは、どんな運用体制をとるかを考えたうえでシステムを設計するというところにかかってくると思います。

SPAMメール問題

・SPAM(スパム)とはハムの缶詰
- 勝手に送られてくる電子メールの広告を意味
- うるさい

・捨てるだけだが読むのにもコストがかかる
- これまでのダイレクトメールは発信者のコストが大
- ダイレクト電子メールは読む側のコストが大

・悪質なものと単なる無知と
- 「1000万人に広告を送ってあげます」
- そのような業者に広告を依頼しないことが一番

・中継に使われることも

ＳＰＡＭメールは大量に使われると、安定運用に差し支えるとようなケースもあります。先日実際にあったことですが、あるサーバが中継に使われ、そこからＳＰＡＭメールという宣伝メールがあちこちに送られました。そのメールが全部エラーで返ってきたために、メールサーバのログファイルがあふれてしまい、メールサーバが止まってしまいました。大量のメールは、サーバに負荷をかけます。私の勤めている会社では、年末年始、年賀メールは禁止になっています。

サーバのチューニング

・同じ機器でも設定次第でパワーを発揮できない
- ボトルネックを探すことが重要
  CPU、ネットワーク、メモリ、ディスクアクセスなど

ボトルネックを順々に解消していく → 努力が重要
- 「タコ」な設定はマシンの能力を殺す
・利用方針に合わせた設定が必要
- 受け取られなかったメールの戻し方
- 受発信ログの残し方
・「これ」という解決策はない
- システムに合わせて調整する
- 経験がものをいう
大量のメールをさばくためには、サーバのチューニングが非常に重要になってきます。同じ機械でも、設定次第でパワーを発揮できないことが起こってきます。メールが集中してくると、遅配というんですか、メールのレスポンスが遅くなってきます。いろいろ調べてみると、ボトルネックがどこかにあるので、それをどういうふうに探していくかというのが問題です。いろんなツールを使って、ＣＰＵが問題なのか、ネットワークが問題なのか、メモリなのか、ディスクなのか、を解決していく。３つ位の原因が重なって遅いこともあるので、順々に解決しながら解消していかないとだめです。努力は面倒だから、金で速いマシンを買えば良いという方もいらっしゃるかもしれません。それはそれでひとつの解決策だとは思いますが、早いマシンを買って直らないものもありますので、注意と努力が重要だと思います。
実例ですが、設計的には１日10万通ぐらいのメールはこなせるメールサーバだったのが、１万５千通ぐらいでメールが送れなくなったのです。ディスクのアクセスがすごく混んでいるので、調べてみると、メールを受け取るスプールと、その次に書き込むユーザのスプールと、さらにユーザが保存するエリアが同じディスクに取ってあり、書きに行くたびにディスクが一生懸命働くのですが、なかなか追いつかない。結局、ディスクを増やして、それぞれのスプールを、添付ファイル、スプール……というふうに、全部分けていくと、突然、よく動くようになりました。原因を、努力して探すということが重要だと思います。
それから、メールは相手のメールサーバが受け取れる状態になかったら、自分のところに保存して置きます。インターネットの中をメールが１週間さまよって、１週間目に返ってきたという話がよくあります。ほとんどのケースは、相手のメールサーバが応えてくれなかったので自分のメールサーバの中に残っており、自分のサーバの設定が、たまたま１週間送れなかったら戻すという設定になっており、１週間目に戻ってきたというケースが多いのです。設定を２日にしておけば、２日目に分かります。
熊谷 エラーメールは、どれぐらいで戻されているんですか。
渡部 うちは24時間か48sendmaiです。sendmaiの標準は、１週間で、24時間でアラームを出すという設定もあります。
企業で使っているメールであれば、誰がいつ、どこに送ったかという、ログを全部残す事も必要です。その残し方も、どの程度のログを、どんな形で残すかをルールとして決めておく。１年たてばテープに落とすという具合に。

安全なメールシステムとは
安全なメールシステムとは次のようなシステムだと考えています。
・届いてなんぼのシステム - 届かないメールをメールとは呼ばない
・いつもちゃんと動いている - たびたび止まると安心して使えない
・メールがなくならない
・メールが届いてない事を教えてくれる- 6時間送れないのなら教えてほしい
・不正なメールを送らない - メールループをよく起こすシステムもある
・よく考えてシステムを選ぼう

HTML, Riched Text
・メールの表現力をアップする
- 強調文字、色文字、アンダーライン、フォント
- 絵、音、動画で伝える
・これらの機能を売り物にするツールも登場
- マルティメディアメール
-MIME(Multimedia Internet Mail Extensions)を利用
-NetscapeもOutLookも対応
・こんなメールが必要なのか?
- 読めないメーラもある
- トラフィックが増える
-知らず知らずに送っていませんか ?
最近、プレーンな普通のテキストではないＨＴＭＬやRiched Textのメールがたくさん来始めており、表現力がアップするのは確かに良いのですが、トラフィックが増えるし、読

めないメーラもありま。
社内的に使うべきか使うべきでないのか、又相手側が使えないということもありますので、運用側でしっかり押さえておかないと社員が社外の人に迷惑をかけるようなことが起こり得ます。

2．モバイル環境での電子メール

モバイル環境での電子メール

・メールが重要な通信手段なら…
  - いつでも読み書きできなければならない
  - どこででも読み書きできなければならない
・移動中や移動先ではEthernetは使えない
  - 接続方法が問題
  - 無線電話(携帯、PHS)、公衆電話、ホテルの電話
・無線は高くて遅い
  - PHSでさえ29.2kbps
・有線も高くて遅い
  - ISDNでさえ最高128kbps
・どうすりゃいいの?

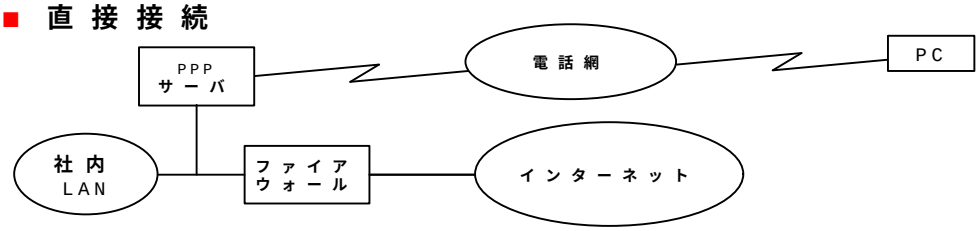
電子メールがかなり普及してきて、移動中でも読みたいという要求が増えてきているのですが、移動中とか移動先ではネットワークがなかなか使えないという接続方法の問題があります。

モバイルでの接続方法

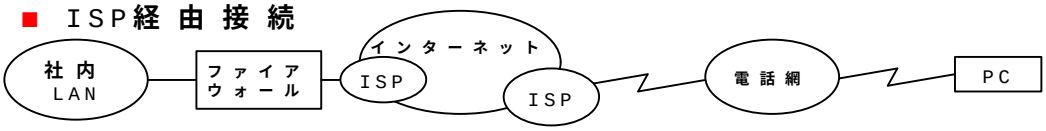
・インターネット経由で接続
  - インターネットは盗聴される
    パスワードが盗まれる
    メール自体を読まれてしまう
  - やっぱりインターネット経由は危ない
・社内ネットワークにダイアルアップ接続
  - PPPサーバを社内に設置
  - 出張先からは長距離電話や国際電話…非常に高価
  - 社員が接続できればクラッカーも接続できる
・セキュリティをどうしようか?

外 部 か ら の 接 続 例

■ 直 接 接 続

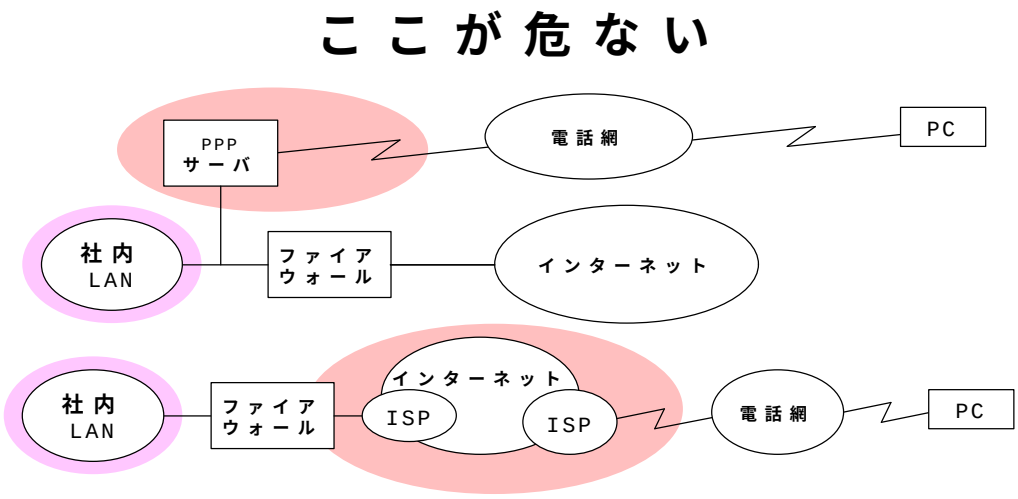


■ ISP経 由 接 続



上図は、直接接続など外部からの接続方法を図示したものです。このように外部から接続するようになると、パスワードが盗聴される、メールが盗聴される、というセキュリティの問題が出てきます。

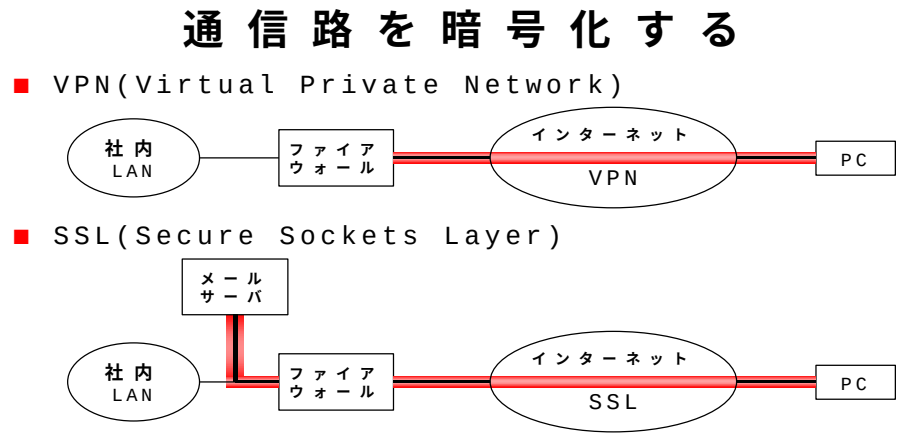
安全にネットワーク接続したい
安全なネットワークとは次の事です。
・侵入されない　　→　接続パスワードを守る
・なりすまされない →　接続パスワードを守る
・盗み読みされない →　通信路の暗号化
・パスワードだけの接続は危ない
　- 玄関にダイアル錠をつけておくようなもの
　　何度かトライすれば「偶然」入れる
　　鍵を開けるところを盗み見する
　- これではセキュリティを確保できない
・インターネットは盗聴されている
　- メールが流れれば中身を読まれる
　- パスワードを送ればパスワードが盗まれる
たとえば社内のネットワークに侵入されてしまうと、すごく困ることになります。そのためには接続のパスワードを守らないといけないわけです。なりすましというのも起こりますので、それも接続パスワードを守るとか、盗聴されないとかというのが必要になります。こういうことを考えると、パスワードだけでつなぐというのは非常に危ないわけです。これは玄関にダイアル錠をつけておくと、偶然、入れてしまう可能性があるわけで、これではセキュリティとは言えないわけです。また、たとえば端末ルームからつないでいるのにしても、誰かがネットワークを監視するソフトを動かしていると、それでパスワードを取られているかもしれないわけです。そういうことを考えると、やはり、非常に危険なわけです。



上図はネットワークの危ない場所を示しています。
ＰＰＰサーバから入られたり、インターネット経由ファイアウォールから入られたり、社内ＬＡＮの中でも盗聴されている可能性があります。

外部からの接続は許さない?
一方で、「外部からの接続は許さない」という企業が非常に増えています。これはセキュリティの守り方というのを考えると、ひとつの重要な解決策ではあるわけです。ただ、そうするとすごく不便なので、やはり物理的に相手を認証しようという使い方が出ています。たとえばコールバックと呼ばれる、呼んできたところに対して呼び返すという仕組みです。これですと、相手を特定できるからいいんですが、なかなか、どこででも使えるかというと、そうでもないわけです。たとえばホテルの部屋からだと使えないわけです。ただ、そうすると、つながる相手がすごく制限されてきますので、今度はパスワードを使い捨てにしようというものです。同じパスワードをずっと使っているから、１回パスワードを盗聴されると次も使われてしまうので、使い捨てにする方法を使っていこうというわけです。それには、「ワンタイムパスワード」と呼ばれるソフトウェアでやる方法とか、」ワンタイムパッド」と呼ばれるハードウェアでやる方法があります。

安全にネットワーク接続する
・接続が安全なだけでは不十分
  - 経路によっては盗聴対策が必須
  - インターネットを経由すると盗聴が大問題
・通信路を暗号化する
  - VPN (Virtual Private Network)
  - SSL (Secure Sockets Layer)
  - SSH (Secure SHell)
・安全につないで安全に使う
  - 接続時の安全確保と接続中の安全確保
  - 両方考えないといけない



安全にネットワークを接続する為に、通信路を暗号化する方法があります。ＶＰＮとかＳＳＬとかＳＳＨと呼ばれるものです。ＶＰＮは、日本語に訳すと「実質的な専用線」です。「Virtual 」を「仮想」と言うのはどうも好きではないので、「実質的な」という言い方をしますが、「実質的な専用線」ということになるわけです。これはインターネットの中を暗号化することによって、あたかも専用線のように使おうということです。通信路の中での盗聴を防ぐために、こういう方法を使い始めているところが、どんどん増えてきていると思います。

具体的な接続方法
モバイルの接続方法には次の方法があります。
・日本国内なら
  - 自宅の電話(直接接続、ISP経由)
  - ISDN公衆電話(直接接続、ISP経由)
  - 携帯電話、PHS(直接接続、ISP経由)
  - ホテルの部屋の電話(直接接続、ISP経由)
・海外から
  - 国際電話(直接接続、ISP経由接続)
    空港のラウンジ、ホテルの部屋、飛行機の中
  - 市内電話(ISP経由)
    空港のラウンジ、ホテルの部屋、飛行機の中
  - 携帯電話

３．メーラを考える

モバイル時代のクライアント
最近は様々なクライアントが出ておりますので、特徴に応じて使い分ける必要があります。
・多彩なクライアントが登場
　- PDA、サブノートPC、ノートPC、携帯電話、CE
・機能が違う
　- 入力装置、表示装置、記憶装置
・用途に合わせてクライアントを選ぶ
　- メール、メモ、住所録、電話帳、Web、FAX
・使い分けの例
　- PalmPilot　　スケジュール、カレンダー
　- サブノートPC メール、Web、プレゼンテーション
　- 携帯電話　　電話帳、ライト、時計
　- メモ帳　　メモ

リモート環境からメールを使う
リモート環境からメールを使う場合に、ＰＯＰ(Post Office Protocol)が主流になっていますが、最近IMAP4(Internet Mail Access Protocol Version 4)が注目されています。

POP3(Post Office Protocol Ver.3)
ＰＯＰ３は、今、広く普及していています。プロトコルがとても簡単で、実装も簡単です。サーバ側は、メールを貯めておいて、クライアントのパソコンに渡してしまったら終わりという感じです。
メールの管理は基本的にクライアント側が行うので、デスクトップとノートパソコンといった複数の環境でメールを読もうとすると読めない事があります。また、メールサーバにメールを残したままにすると、スプールがいっぱいになって思いもよらぬトラブルが発生する事もあります。

ＰＯＰのコマンドは下表の通りです。パスワードを暗号化するＡＰＯＰがあり、ＭＤ５で一時的な使い捨てのパスワードで認証できます。ＰＯＰでメールを取るときも非常に簡単で、ユーザ名を言ってパスワードを入れて、あとはリトリーグといって、「１番目のメールをちょうだい」と言うとメールが落ちてくるという具合です。

ＰＯＰ３のコマンド

POP3(RFC1939)	
STAT	メールボックスのメール数とサイズの所得
LIST	ここのメールのサイズの所得
RETR	指定したメールの取出し
DELE	指定したメールの削除
NOOP	何もしない
RSET	操作の取消し
QUIT	接続の終了
TOP	指定したメッセージのヘッダと本文を指定した行数所得する
UIDL	ここのメールのサーバ内でのIDを所得する
USER	ユーザ認証時のユーザ名の送信
PASS	ユーザ認
APOP	MD5で暗号化されたユーザ認証

ＰＯＰ３でのメールの取得

```
+OK POP3 beer.orangesoft.co.jp v5.49 server ready
USER kitarou
+OK User name accepted, password please
PASS nazonazo
+OK Mailbox open, 1230 messages
RTET 1
+OK 3360 octets
```

メール本文

```
.
DELE 1230
+OK Message deleted
```

IMAP4(Internet Mail Access Protocol Ver.4)
POPの問題は、ほとんどＩＭＡＰで解決できます。ＩＭＡＰが最近注目されている理由として、Internet Mail Access Protocolと、頭にInternet(昔はInteractiveと読んでいた)がついているからです。最近、ＩＭＡＰを採用しているベンダーも非常に多く、Sun Microsystems、Netscape、Microsoft、NECなどが対応製品を出してきています。クライアント製品も、Netscape、Microsoft、Orangesoftなどが対応製品を出しています。

ＩＭＡＰは次の特徴をもっています。
・メールの管理はサーバ側
　- 未読/既読の管理
　- フォルダの管理
　^ メールの保存は基本的にサーバ側
・各自のメールのバックアップはサーバで
・複数の端末から同じようにメールが読める
　- 自席のデスクトップと外出先のノートPC
・多彩なメール取得手段
・クライアントの実装次第
　- ヘッダ(From:, Subject等)を指定して取得できる
　- MIMEのパート単位の取得
・必要なメールだけダウンロード
　- Subjectをみて選べる
　- メモリが少ないマシンでも使える
　　PDAやインターネットTVなど
ＩＭＡＰ４のコマンドは表のように一杯あり、さらにこのコマンドの使い方の中に様々な種類があるので、とてもこの表だけでは書ききれません。実装は面倒だと思います。しかし、ＩＭＡＰを使ってＰＯＰ Likeな使い方をすると事もできるので、実装をどこまでやるかで難しさが変わります。

IMAP4rev1のコマンド

IMAP4(RFC2060)	
CAPABILITY	サーバのIMAP4のバージョンや認証機能等のサーバの機能の所得
NOOP	何もしない
LOGOUT	接続の終了
AUTHENTICATE	LOGIN以外の認証方式によるユーザ認証
LOGIN	サーバへのLOGIN
SELECT	メールボックスの選択(メールボックスのオープン)
EXAMINE	読み込み専用でメールボックスを選択(メールボックスのオープン)
CREATE	メールボックスの作成
DELETE	メールボックスの削除
RENAME	メールボックスのリネーム
SUBSCRIBE	ニュースグループの購読
UNSUBSCRIBE	ニュースグループの購読中止
LIST	メールボックスリストの所得
LSUB	指定したニュースグループの階層のリストの所得
STATUS	指定したメールボックスのメール数とUIDの所得
APPEND	指定したメールボックスへのメッセージの書き込み
CHECK	SELECTしたメールボックスの新着チェック
CLOSE	SELECTしたメールボックスのクローズ
EXPUNGE	DELETEフラグがセットされたメッセージの削除
SEARCH	メッセージの検索
FETCH	メッセージ、フラグ等の取出し
STORE	メッセージへのフラグのセット
COPY	メッセージのコピー
UID	UIDを指定してコマンドの実行

IMAP4でのメールの取得(1)

```
* OK beer.orangesoft.co.jp IMAP4rev1 v11.241 server ready
A1 LOGIN kitarou nazonazo
A1 OK LOGIN completed
A2 SELECT INBOX
* 1229 EXISTS
* 10 RECENT

 省略

A2 OK [READ-WRITE] SELECT completed
A3 FETCH 1235 BODYSTRUCTURE
* 1235 FETCH (BODYSTRUCTURE (("TEXT" "PLAIN" ("CHARSET" "iso-2022-jp") NIL NIL "
7BIT" 113 10 NIL NIL NIL)("APPLICATION" "X-PKCS7-SIGNATURE" ("NAME" "smime.p7s")
 NIL NIL "BASE64" 3630 NIL ("ATTACHMENT" ("FILENAME" "smime.p7s")) NIL) "SIGNED"
 ("PROTOCOL" "application/x-pkcs7-signature" "MICALG" "rsa-sha1" "BOUNDARY" "---
------911557871-23039209") NIL NIL))
* 1236 EXISTS
* 2 RECENT
A3 OK FETCH completed
```

IMAP4でのメールの取得(2)

```
A4 FETCH 1235 BODY[HEADER.FIELDS (DATE FROM SUBJECT)]
* 1235 FETCH (BODY[HEADER.FIELDS ("DATE" "FROM" "SUBJECT")] {144}
Subject: =?ISO-2022-JP?B?GyRCJDMkcyRLJEEkTxsoQg==?=
From: Watanabe Naoaki <kitarou@orangesoft.co.jp>
Date: Fri, 20 Nov 1998 19:31:12 +0900

)
* 1240 EXISTS
* 6 RECENT
A4 OK FETCH completed
A4 FETCH 1235 BODY[1]
* 1235 FETCH (BODY[1] {113}
 これは、テストです。

 省略
)
* 1241 EXISTS
* 7 RECENT
A4 OK FETCH completed
```

実際にＩＭＡＰでメールを取得する方法は上図の通りです。ログインは一緒なのですが、SELECTでメールボックスを選ぶと、「もう、何通ある」とか、「新着が10通ある」、等が出てきます。左上のよに「1235番目のメールをちょうだい」、「BODYの構造は？」と尋ねると、１番目の構造は"TEXT" "PLAIN"で"CHARASET"は"iso-2022-jp"で、次に"APPLICATION"で"X-PKCS"で、電子署名がついているというような情報が全部見える。取ろうと思うと、HEADER FIELDSの"DATE"と"FROM"と"SUBJECT"だけ欲しいと言える。サーバとのやりとりで、必要な情報だけが落とせるのでかなり楽です。

それぞれのメリット

POP3、IMAPの各々のメリットは次の通りです。

・POP3
- 接続すれば全てのメールがクライアントに届く
- 全部が自分のマシンで管理できる

・IMAP4
- 必要なメールを自分で選択してダウンロードできる
- 通信時間が見積もれる
- ^ 自分のマシンが壊れてもメールは安心
- 過去のメールも参照できる
- ネットワークのトラフィックの軽減

それぞれのデメリット

POP3、IMAPの各々のデメリットは次の通りです。

・POP3
- 通信時間がわからない
  どれだけメールがあるか事前にわからない
- 自分のPCが壊れると保存してあるメールが消滅
  バックアップは自分の責任
- 別のマシンに保存してあるメールは読み出せない

・IMAP4
- サーバにそれなりのディスクが必要
- サーバソフトの選択に注意が必要
- サーバのバグやクライアントとの互換性
- サーバ側でバックアップが必要
- サーバが停まると過去のメールも読めない

IMAP4は膨大な資源が必要？

ＩＭＡＰは、各自のメールを全部ＩＭＡＰサーバに保存するので、かなり大きな資源が必要です。仮に１人あたり１日50通来て、１通のサイズが平均50KB、10人いると考えると、500通×10ｋ、365日で1.82GBあれば間に合うので、４GBのハードディスクを買っておけば大丈夫です。

今後の主流はIMAP4か？

今後の主流はＩＭＡＰだと思います。ハードディスクは、どんどん安くなってきているので買い足せば済みます。ＩＭＡＰ４対応のサーバ製品は確実に増えてきています。ＩＭＡＰ対応のメーラ、メールソフトも増えてきています。サーバとそのメールソフトの互換性、接続性テストは、アメリカのＩＭＣというところでメールコネクトというイベントが行われており、ベンダーのMicrosoftとか Netscapeなどが互換性テストをやっていますので大丈夫だと思います。

IMAP4サーバの選び方

ＩＭＡＰサーバの選び方を示します。

・カタログや比較表の ○ の数はあてにならない
  - 陥りやすい過ち
  - 本当に必要なのは安定性

・価格にだまされてはいけない
  - 高価だからいいとは限らない
  - フリーだからいいとも限らない

・操作画面の日本語化にだまされてはいけない
  - 本当の日本語化はサーバのSEARCH機能など

・どれだけのクライアントと接続実績があるか
  - クライアントのバージョンも重要
  - バージョンが上がるとコマンドの使い方が変わることも

４．暗号電子メール

電子メールの弱点

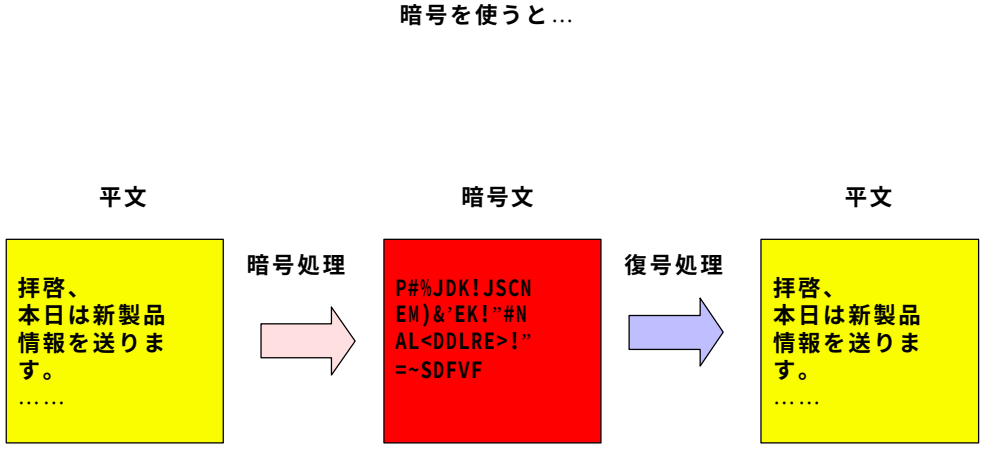
電子メールはこれだけ普及してきていますが、やはり弱点があります。インターネットでは盗聴ができてしまうのです。盗聴できてしまうため、電子メールの内容も盗聴される危険性があります。したがって、重要な情報、人事情報とかは今危ないですね。インターネットで受け取ったメールは、相手を確認する手段が全然ないのです。他人になりすますのは、すごく簡単です。仮に本人であったとしても、もらった電子メールの内容を書き換えられても分からない。

こういう問題があって、「Ｓ/ＭＩME(Secure/Multipurpose Internet Mail Extensions)」が誕生しました。S/MIMEを使うと、電子メールを暗号化して、送った相手以外には読めないようにできる。それから、電子署名をして、自分自身が書いたんだということを特定して、改ざんやなりすましができないようにできるようになります。

暗号メールの基本

最近の企業はFirewallを入れて外からの侵入は守っており、Firewallがあるから電子メールも守れるように思われますが、Firewallでは電子メールを守ることはできません。FirewallやＶＰＮを使用して安全にしても、外からなりすまし、改ざんされたメールが来て、一般利用者がだまされてしまうと、ほとんど意味がありません。暗号の安全性は、暗号が破られるか破られないかで決まります。そして、自分が出した電子メールを証明することが必要になります。

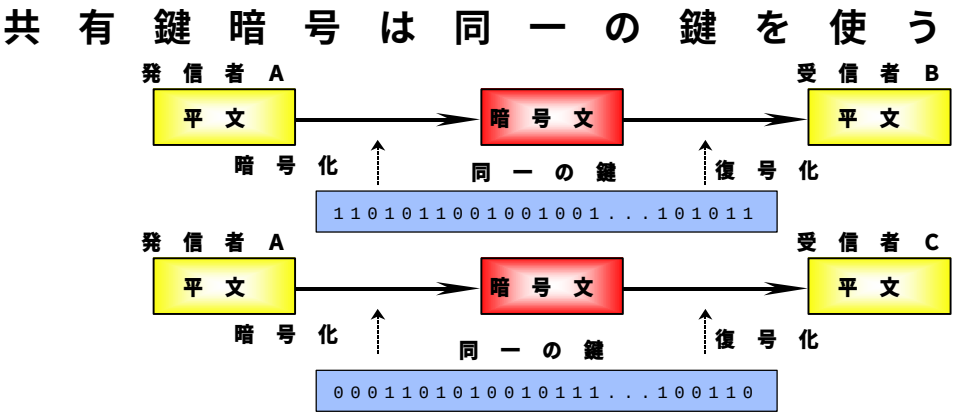
暗号を使うと



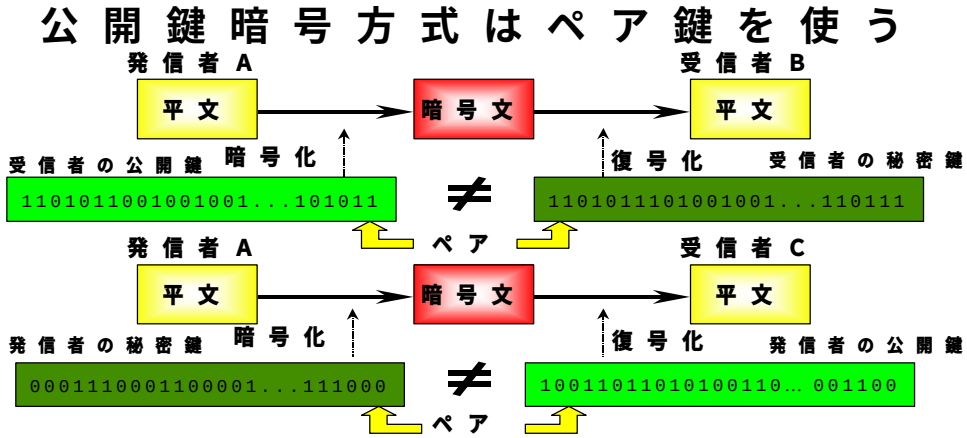
盗聴などの問題は、暗号技術で解決できます(できるはずです)。

重要な暗号技術
暗号は米国の技術が中心で、次のようなものが有名です。
・公開鍵暗号方式(RSA、Diffie-Hellman)
・共有鍵暗号方式(DES、RC-2、RC-4)
・メッセージ・ダイジェスト(MD5、SHA-1)
共有鍵暗号方式には、最近は、ＲＣ-６とかもあります。それから、メッセージ・ダイジェスト。これは文書の署名、電子メールの証明をとるようなときに使いますが、ＭＤ５とかＳＨＡ-１とかがあります。こういった暗号技術は、もう、携帯電話とかでも使っていると思いますし、あとはスマートカードというＩＣカードなどに、これから広く使われてくるでしょう。暗号には、強度、アメリカの輸出規制、日本からの輸出規制等の問題を含んでいます。公開鍵暗号方式は、公開鍵(Public Key)と秘密鍵(Private Key)の鍵ペアで、公開鍵をみんなに公開し、秘密鍵は誰にも教えないというものです。そして、公開鍵で暗号化し、秘密鍵でのみ復号可能という仕組みになっています。

共有鍵暗号方式
共有鍵暗号方式について下に示します。
・送信者と受信者は暗号、復号に同じ鍵を使う
　- 同じ鍵を共有するから「共有鍵暗号」
・送信者と受信者の間での鍵の受渡しが問題
　- 定期的に鍵は交換したい
　　通信ごとに変える方が安全
　- 安全な鍵交換の方法
　　メールで送ると盗聴される
　　鍵が盗まれては意味がない
　- 複数人に鍵を配布するのが面倒
　　相手ごとに違う鍵が必要
　- 処理速度は速い



公開鍵暗号方式
公開有鍵暗号方式については以下のとおりです。



・暗号化鍵と復号化鍵が異なる
  - ふたつの鍵がペアになっている
  - 片方を公開(公開鍵)、片方を秘密(秘密鍵)
・公開鍵から秘密鍵を求めるのが困難
  - 復号化鍵(公開鍵)は誰にでも配布できる
  - 公開鍵を安全(確実)に相手に渡す
    公開鍵のすり替えに注意
・処理速度は遅い
  - メッセージ全体の暗号には不向き
  - 共有鍵暗号の鍵を暗号化する

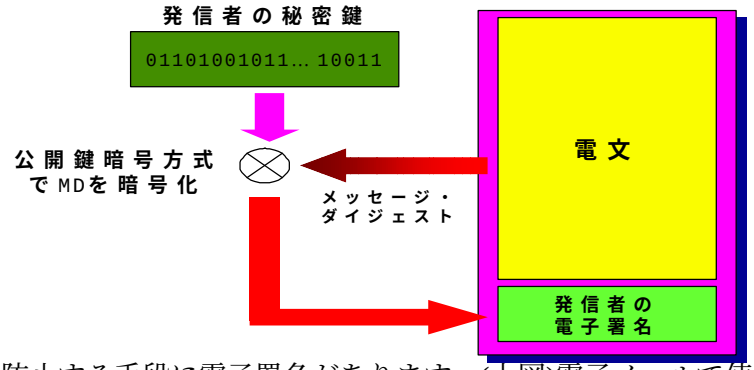
公開鍵暗号方式は、暗号化鍵と複号化鍵が異なります。秘密鍵と公開鍵はペアになって使用されます。これらを鍵ペアと呼んでいます。

Certification Authority
公開鍵を相手に正しく渡すために、公開鍵の持ち主を証明する機関が、Certification Authority(ＣＡ局、認証局)です。証明書を出して、この公開鍵の持ち主を証明する組織です。
市役所での印鑑証明に相当します。ベリサインとか、サイバートラストとか、こういうところが認証してくれます。

暗号化メールと個人認証
暗号メールをやりとりする際、差出人が間違いなく本人であるという確認が必要になってきます。
本人である事を誰が証明してくれるのかを考えなければなりません。社員の場合は会社が証明してくれたり、あとは地方自治体とかボランティア組織が証明してくれたり、CA局が証明してくれたりが必要です。ＣＡ局を使うとき。証明書発行機関から証明書をもらって使うのですが、ブラウザとかメールソフトとか、いろんなものを使うたびに証明書が必要になってくるのか不明です。

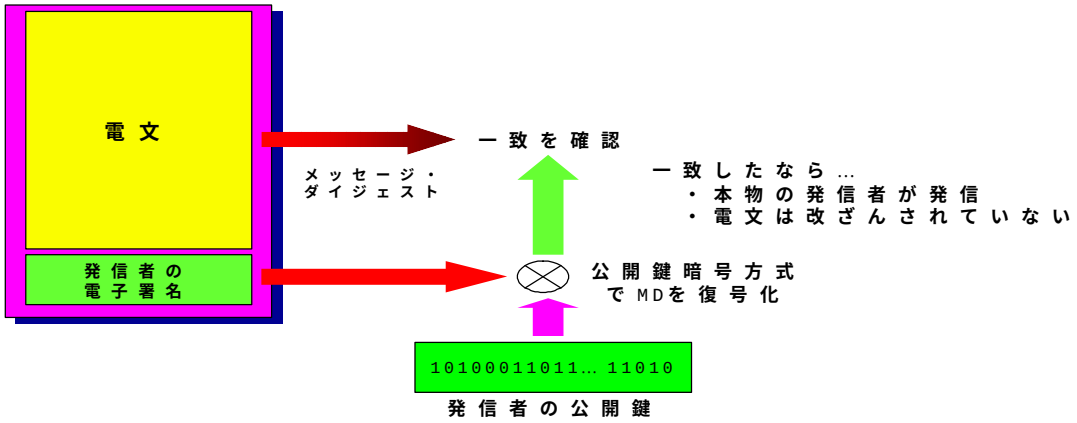
改ざん
電子メール内容の改ざんが本当にできるのですか、という質問を受けます。これはできます。どこでやれるかというと、メールを受け取ったときの最初のＳＭＴＰサーバ、途中のメールサーバ、自社のメールサーバ等、しようと思えば何でもできます。

電子署名で改ざんを防ぐ



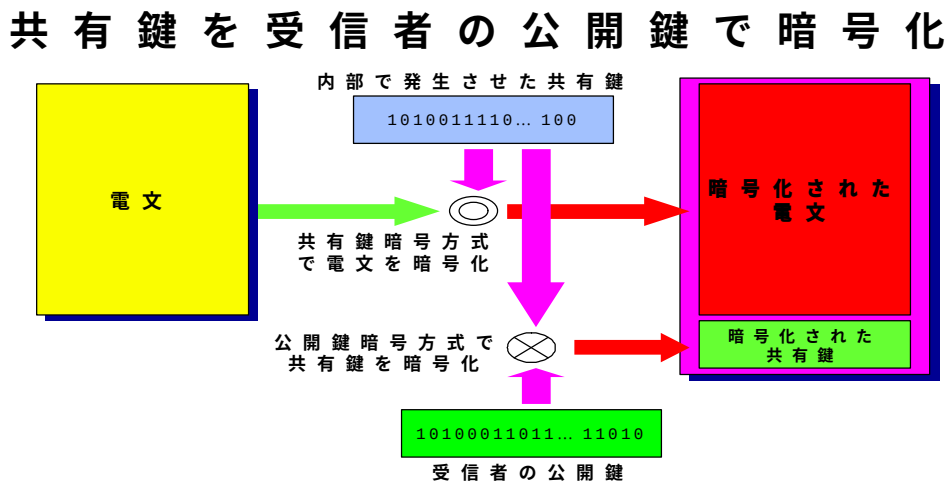
改ざんを防止する手段に電子署名があります。(上図)電子メールで使われている電子署名は、送るときに電子メールとして送るメッセージ自体のメッセージ・ダイジェスト(ある特定の数値)を得ます。これに、ＭＤ５やＳＨＡ-１を使ったハッシュ関数を使ってダイジェストをつくり、それを発信者の秘密鍵で暗号化して添付して送ります。

電子署名で改ざんを確認する



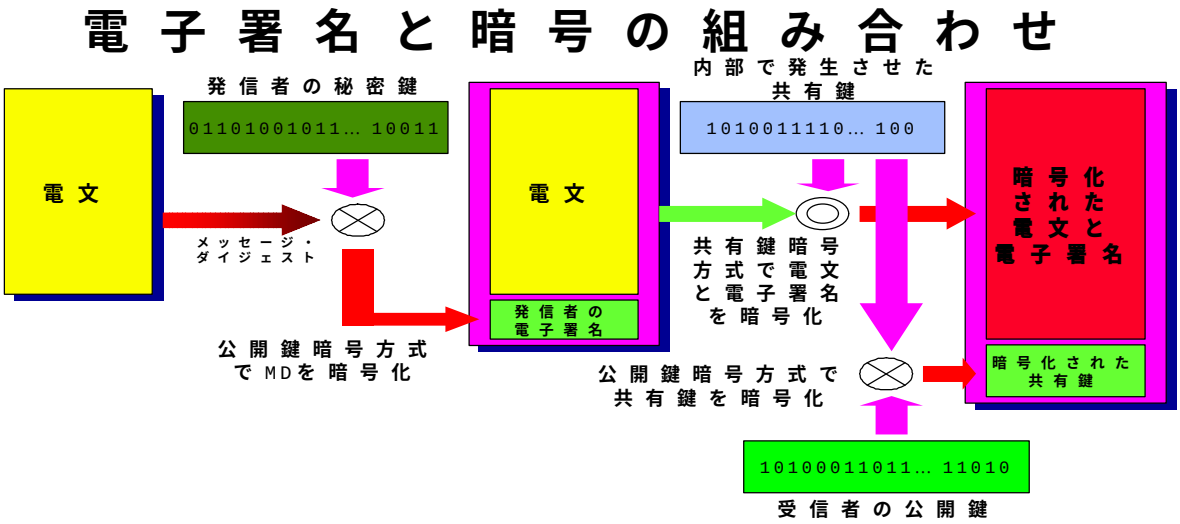
（上図）改ざんを確認するには、受け取ったメッセージから自分自身で同じハッシュ関数を使ってメッセージ・ダイジェストを作成し、あとは発信者の電子署名（この発信者が計算したメッセージ・ダイジェスト）を発信者の公開鍵で複号します。（発信者の秘密鍵で暗号化されているので、発信者の公開鍵を持っていれば、誰でも複号できます。） この結果を照合して、同じだったら、そのメールは改ざんされていないということになります。

電文の暗号化



公開鍵暗号というのは、処理速度が遅いので、メール等の場合、メール全体の暗号化を共有鍵で暗号化し、共有鍵を受信者の公開鍵で暗号化するような方法をとります。

複数の相手に暗号メールを同報



複数の人に暗号化されたメールを送る場合には、まず、発信者の秘密鍵でメッセージ・ダイジェストをとり、電子署名を付けます。署名を付けて、それに対して内部で発生したランダム鍵で暗号化し、それを各自の公開鍵でランダム鍵を暗号化して添付します。そうすると、Ａさんもこの共有鍵を見られるし、Ｂさんもこの共有鍵が解けるので、メッセージ本文を複号することができるようになります。

電子署名時の漢字コード

電子署名をするときに、漢字コードが問題になってきます。電子署名はクリアテキストなので、相手が署名を検証出来なくても、誰でも読めるので良いわけです。しかし、中を検証しようと思ったら、相手が署名をしたときの状態の漢字コードでないと署名が検証できないません。途中の配送経路で、漢字コードを変換されてもだめです。まだ世の中には、途中でShift_JisやＥＵＣに変換する人もいますので、そういう配送経路を通ったら絶対に電子署名は使えません。

PGPとS/MIME

PGP

・公開鍵に対する認証はお互いが信用に基づく
  - 信頼の輪
      信用できる証明者
  - PGP2.6.3i
  - PGP5.5

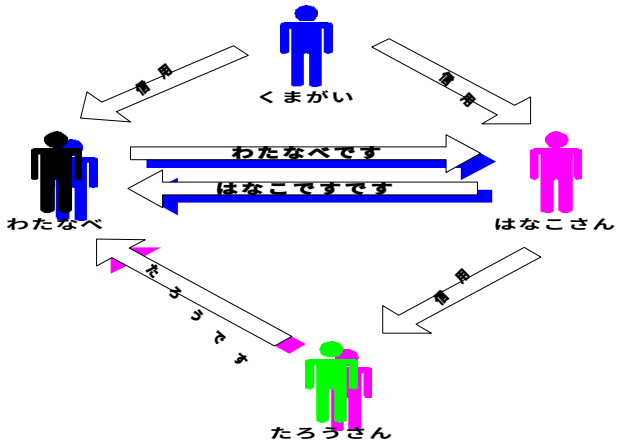
・S/MIME
  - 公開鍵に信頼できる機関による認証が行われる
      認証局による証明書の発行
  - Netscape Communicator, Outlook Express, Winbiff等々

ＰＧＰとS/ＭＩＭＥは認証方式が違います。ＰＧＰでの公開鍵に対する認証は、お互いの信用に基づく信頼の輪で行い、S/ＭＩＭＥでは、公開鍵に対して信頼できる機関がその公開鍵を証明する事です。

信頼の輪(web of trust)

ＰＧＰとかの信頼の輪は、下図で説明すると、熊谷さんが私(渡部)を信用するとします。そして花子さんも熊谷さんは知っていて信用している。そうすると、私は熊谷さんの信用をつけて花子さんにメールを送ると、花子さんは熊谷さんを知っているので、「ああ、よしよし、分かった分かった、この渡部というのは、熊谷さんが信用しているから大丈夫なのね」となります。

信頼の輪(web of trust)



私が花子さんを信用すれば、花子さんが信用している太郎さんも信用できるというふうに、信頼の輪ができることになります。

PGPにおける鍵の管理

ＰＧＰにおける鍵の管理は、公開鍵を鍵サーバに登録します。そして、実際に暗号でメールをやりとりする人皆に自分の公開鍵を配布する。このとき、安全に配布しなければいけないのが面倒です。相手の公開鍵も随時、どんどん入手して、自分の中に持って管理しなければなりません。

S/MIMEにおける鍵の管理

Ｓ/ＭＩＭＥは、秘密鍵に関してはほとんど同じですが、公開鍵を認証局に１度送って、認証局がこれが正しいと署名して証明書を返してくれる。そうすると、自分の公開鍵は、認証局の証明書もついた状態の証明書になります。ですから、受け取った人がこの証明書を信用すればその公開鍵が正しいことが証明されます。

認証局

認証局は、公開鍵が正しいことを証明します。印鑑証明みたいなものです。商用で日本だと日本ベリサインやサイバートラスト等々、たくさんあります。最近、自社でプライベートな認証局を運用しようとしているところもあるようです。

暗号メール運用上の問題点

暗号メールの運用の問題を次に示します。

・使おうとすると簡単ではない
  - 使えるメーラが少ない
  - メーラがこなれていない
  - 互換性に疑問が残る
・証明書が高くつく
  - 商用認証局は高すぎる
  - 自社で認証局を開設しても運用が必要
・その他の問題点
  - LDAP(Lightweight Directory Access Protocol)
  - CRL(Certification Revocation List)
  - メーリングリスト

キーリカバリとキーエスクロウ

・キーリカバリ
  - 共有鍵、秘密鍵がなくても復号可能
  - 安全性とプライバシーは？
  - しかし、どうしても復号したい場合もあるのでは？
・キーエスクロウ(鍵寄託)
  - 第三者に復号可能な鍵を預ける
    部分的な預託もありうる
    使うときのルールが重要
  - 会社等では必要？
    社員が退職した時
    鍵を紛失してしまった
    検閲

LDAPとは
・Lightweight Directory Access Protocol
  - X.500から無駄な機能を取り除いて簡素化
・インターネット上のアドレス帳
  - bigfoot,YahooPepleSerach等
・電子メールアドレスの検索
  - もちろん証明書やCRLの検索にも
  - Webで公開すると組織構成がばれる
・登録される情報
  - 氏名、メールアドレス、証明書、公開鍵、電話番号
  - 証明書、公開鍵の有効、無効

CRLとは
・Certification Revocation List
  - 無効になった証明書の一覧表
・クレジットカードのブラックリストと同じ
  - 証明書を受け取ったたびに確認しなければならない
  - どうやってリストを配布するか
  - 公開していいとは限らない
・退職者はCRLに載る
  - 証明書が無効になるから
  - 公開すると問題にならないか

メーリングリストの運営
・メールを暗号化してみんなに送る
  - 誰の鍵で暗号化するのか ？
  - 送信時に全員の公開鍵で個別に暗号化する ？
    発信者にとっては大きな負荷
  - メーリングリスト用の秘密鍵を全員に配布
    メンバーが変ったときにどうするか
・暗号化メーリングリストサーバが必要 ？
  - 参加者の公開鍵をメーリングリストサーバに登録
  - 利用者はサーバの公開鍵で暗号化してサーバへ送る
  - サーバは自分の秘密鍵で復号化
  - サーバでメンバー個々の公開鍵で暗号化して配送

５．Q&A

Ｑ１ ある人が10MBの貼付ファイルを送ったのですが、添付ファイルのサイズをどの位の大きさまで許していいのか、何か経験則があったら教えていただきたいんですが。
Ａ１ (熊谷・渡部) 経験則は特にありません。

Ｑ２ 送ったメールが相手の社内サーバで３日間止まっていて、当社内で問題になった事があります。 何か対処法あるんでしょうか。
Ａ２ (熊谷)相手のメールサーバが悪いのですから、相手の企業に教えてあげるのが解決手段になると思います。そして、社内の人には、電子メールは相手の都合によって届かないことがあるこを教育するしかありません。

Ｑ３ ＣＡを使われた経験はおありですか。
Ａ３ (渡部)私はまだないです。
（熊谷）私は今、いくつか証明書を持っていまして、VeriSignに10ドルほど払うと１年間有効のもの、S/Gomaを買うと１年間使えるものを実際にやっています。

Ｑ４ ＩＭＡＰについてですが、ステーブルに使えて運用できるというサーバというのが現在、製品として存在しますでしょうか？ それとも、もう１～２年待ったほうが良いのでしょうか？
Ａ４ （渡部） すぐに大丈夫な製もあります。

< 以上 >