【集中企画】
電子メール
応用編

情報セキュリティー時代がやってきた

ビジネス分野で電子メールを使う場面が増えてきた。取り引きや商談などが電子メールでやり取りされているのだ。でもちょっと考えてみよう。インターネットでの通信は本当に安全なのだろうか。暗号の使用といったセキュリティーに対しての関心は高まっているようだが、実際はその利用はまだまだ少ないようだ。そんな中、RSAデータセキュリティー社が提唱するS/MIMEという規格にのっとったセキュアメールソフトが、ネットスケープ社やマイクロソフト社を含む多くのメーカーから次々と発表、発売されている。そこでこのセキュアメールシステムに注目し、そのしくみとネットスケープメッセンジャーでの使い方を紹介しよう。

暗号メール
そのしくみと実践

井上尚司＋インターネットマガジン編集部編
取材協力：日本ベリサイン株式会社

プライバシーを侵す3つの危険

インターネットでのコミュニケーションツールとして、電子メールはなくてはならないものになってきている。特に最近では、企業のインターネット利用によって、ビジネスシーンで電子メールを使用する機会が増えてきているようだ。ビジネス分野では企業間の情報交換やある種の契約のような内容のメールといったものから、個人のプライバシーに関わるような人事通達や給与明細といったものが、必然的に電子メールを使ってやり取りされていくだろう。もし、こういった電子メールの内容が第三者によってのぞかれていたらどうだろう。運が悪ければ、自分の社会的地位や企業を脅威に陥れるような事態になりかねない。インターネットで情報のやり取りをするにはこんな危険が待ちかまえていることも事実だ。

では、いったいどんな種類の危険があるのか、一般に考えられているものを挙げてみることにする（図1）。

まず最初に「盗聴」がある。これは通信内容を第三者が盗み見る行為である。秘密にしておかなければならない情報を盗聴されることは絶対に避けなければならないことである。

次に考えられるのが「なりすまし」である。これは悪意ある第三者が特定の人物になりすますことである。通信している相手が、誰かになりすましていたり、自分の名前を使って別の誰かと通信していたりする可能性がある。

ほかに「改ざん」が考えられる。これは悪意ある第三者がなんらかの形でメールの内容を書き換えてしまうことだ。自分の書いたメールが誰かに書き換えられたり、手元に届いたメールが誰かに書き換えられていたりということが起こりうる。

以上は特に電子メールの交換に限ったことではない。インターネットの通信には、いつでもつきまとうことである。

では、どのようにこれらの危険を回避すればよいのだろうか。一般的な暗号のしくみを解説しながら、それが電子メールでどのように使われるかを説明していこう。

図1 通信の3つの危険

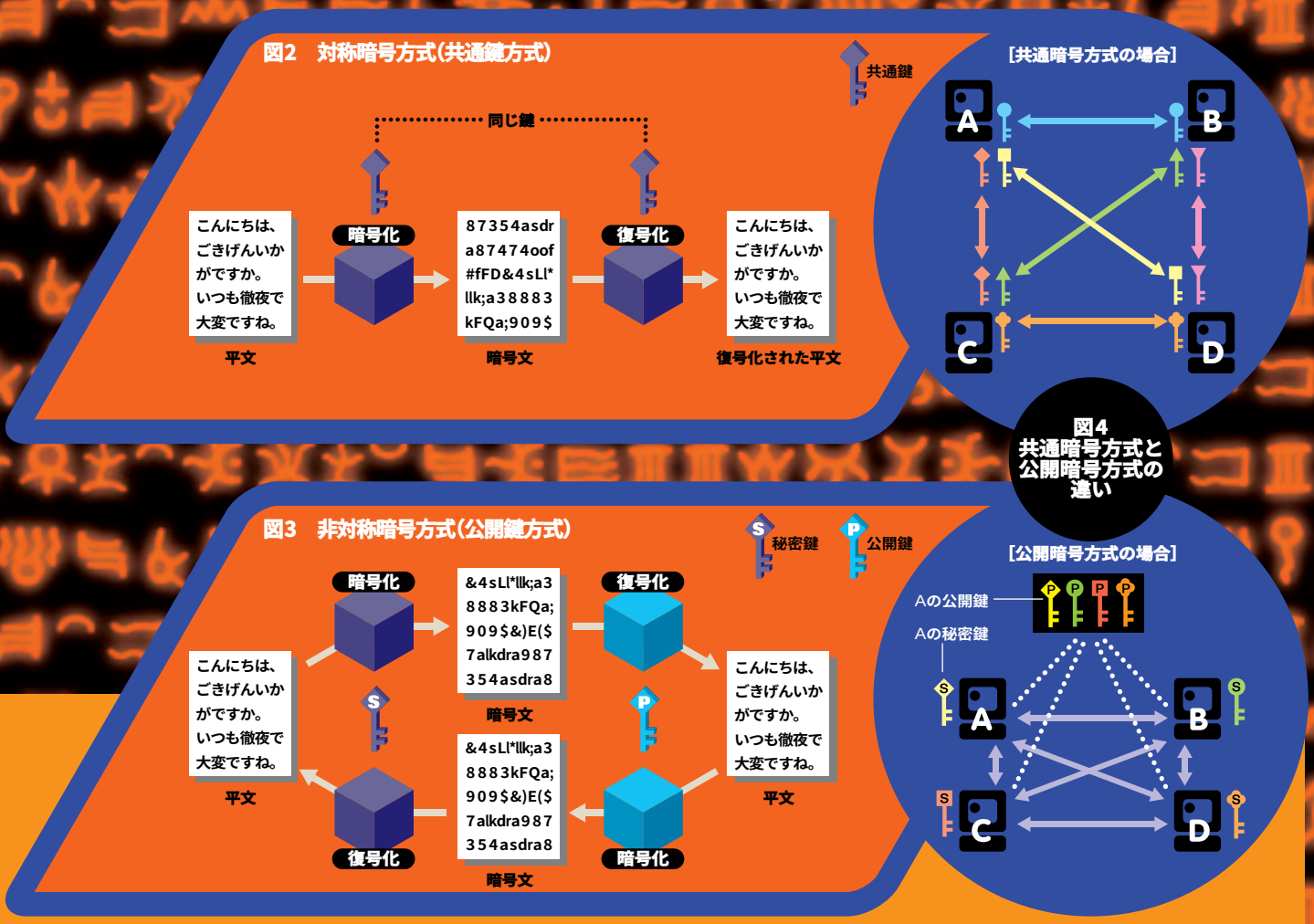


図4
共通暗号方式と公開暗号方式の違い

インターネットで使われる暗号の基礎知識

セキュアメールについて説明する前に、その中で使われている暗号について説明する必要があるだろう。セキュアメールツールを使ってしまえばユーザー側からは何も見えないが、いったいそこで何が行われているかの知識を持っていれば安心感も増すに違いない。

ひとことで暗号といっても、その方法やどのようにそれが使われているかはさまざまである。ここでは、一般にインターネット上の通信で使われている「対称暗号方式」と「非対称暗号方式」を中心に解説しよう。

対称暗号方式

対称暗号方式は、暗号化と暗号化したものを元にもどす復号化に同じ鍵を用いる方式だ。そのため、「共通鍵暗号方式」とも呼ばれる（図2）。この方式は、暗号化と復号化にかかる時間が短く、暗号化された文の大きさも極端に大きくはならないという長所を持つ。

対称暗号方式を用いたメールの送受信は、送信者と受信者が同一の共通鍵を保持して行うことになる。

ここで、4人で暗号化メールを相互に送受信することを考えてみよう。この場合、送信者と受信者の組み合わせが全部で6通りあるので、その組み合わせごとに共通鍵を用意する必要がある。すなわち、各自が受信者3人分の鍵を保持するわけだ（図4上）。メールの相手が増えるにつれて保持する鍵も増えていくので、この方式は現実的ではない。

また暗号を行う前に送信者は受信者に鍵を送らなければならないが、ネットワーク上で鍵を送信すると誰かに盗まれる恐れがある。また無事に届いたとしても、相手の管理によっては、鍵をなくしたり盗まれたりすることもあるだろう。共通鍵方式ではこのような問題点もある。

非対称暗号方式

非対称暗号方式は公開鍵暗号方式とも呼ばれる。この方式では、2つの対になった鍵（キーペアー）を用いる。通常、一方を秘密鍵と呼びもう一方を公開鍵と呼ぶ。公開鍵を使って暗号化したものは、その公開鍵と対になっている秘密鍵でしか復号化できない。逆に秘密鍵を使って暗号化したものは、その秘密鍵と対になっている公開鍵でしか復号化できない（図3）。当然秘密鍵で暗号化した暗号文と公開鍵で暗号化した暗号文では結果が異なる。この方式の暗号化と復号化にかかる時間は共通鍵暗号方式にくらべて長く、また暗号化された文も長くなるという短所がある。

暗号メール そのしくみと実践

公開鍵暗号方式を用いたメールの送受信では、まずメールを受信する各自が、自分の秘密鍵と公開鍵を用意し、自分の公開鍵を他の人が見られるようにどこかに「公開」する、つまり知られるようにすることが必要である。そしてメールの送信者は、受信者の公開鍵を使ってメールの本文を暗号化する。暗号化メールの受信者は、自分の秘密鍵を使って復号化する。秘密鍵を持つのは受信者のみなので、メールを他人に復号化される心配はない。公開鍵と秘密鍵の間には数学的な関係はあるが、公開鍵から秘密鍵を求めるには、天文学的な時間がかかることから安全といえるだろう。

対称暗号方式と同様に、4人のメールのやり取りを考えてみる。4人それぞれが自分自身の秘密鍵と公開鍵を用意し、公開鍵を他の3人に知らせるだけで、暗号化メールを相互にやり取りできる（図4下）。

公開鍵自体は誰に知られても問題はないので、各自が安全に保持しなければならないのは、自分自身の秘密鍵だけでよい。

対称暗号方式より、鍵の保管や配送の点で勝っている方式といえる。

公開鍵暗号方式は、こういった特性を活かして次に述べる「電子署名（Digital Signature）」でも大きな効力を発揮する。

電子署名

暗号化の方法について述べてきたが、いったい、なりすましや改ざんを防ぐ手だてがあるのだろうか。その解決策が電子署名である。普通の（手で紙に書く）署名が自分が書いたことを証明し、さらにその内容にうそ偽りがないことを証明するために用いるのと同じように、電子メールでは電子署名が使われる。いったいどのように「署名」するのかを図5を見ながら説明していこう。

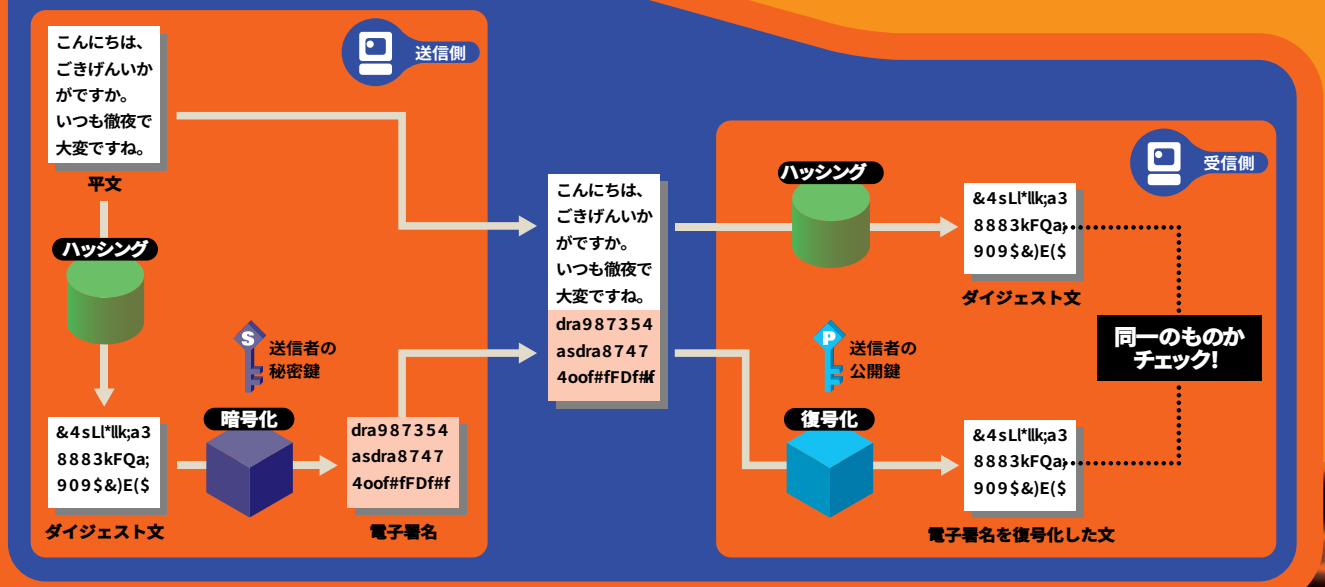
電子メールとして書かれた本文すなわち平文がある。これを「ハッシング」という方法で「ダイジェスト」と呼ばれる特殊な文に変換する。このハッシングとはハッシュ関数という決まった手順によって文を変換する方法で、まったく同じ平文であればハッシングされた結果からは同じダイジェスト文が得られる。ハッシングによって作られたダイジェスト文は、どんな長い文でもまったく同じサイズの小さな文に変換される。このため、2つの長い文はハッシングしてから比較したほうが効率的だ。

このダイジェスト文を電子メールの送信者の秘密鍵で暗号化する。この暗号化されたダイジェスト文が電子署名である。送信者はメールの本文とこの電子署名を一緒に送信するのである。

受信者はメールを受け取ると、メール本文と電子署名に分ける。次にメール本文をハッシングしてダイジェスト文を作り、電子署名を送信者の公開鍵を使って復号化する。この両者を比較してまったく同じであるか否かを確認する。同じであればメールそのものが改ざんされていないことが証明されるとともに、公開鍵で復号化できたということは送信相手の特定もされたことになる。

ここで重要なことは、公開鍵暗号方式での鍵の扱いである。電子署名で公開鍵を使う目的の1つは、相手を特定するということだが、公開鍵自体には人物を本当に特定するものは何1つない。対になった秘密鍵で暗号化されているということを証明しているにすぎない。公開鍵によって本当の人物を特定するのは困難である。

図5 電子署名



これを解決するための「鍵管理」の方法として、2者間で使用する公開鍵の正当性を証明する第三者としての機関が必要になる。これが「認証局（Certificate Authority）」である。

認証局の役割

公開鍵暗号方式での鍵の正当性の検証が難しいことは述べた。そのために認証局が必要であることも前述のとおりだ。ここでは認証局の大手であるベリサイン社を取り上げてその役割について説明する。

認証局の仕事は、大きく分けて2つある。1つは、「デジタルID」という公開鍵とその公開鍵が誰のものであるかを証明する証明書を発行することである。図を使って説明しよう。

図6を見てほしい。Aさんは認証局に公開鍵の登録を行おうとしている。まず最初にキーペアー（秘密鍵と公開鍵）を生成する。通常この生成はセキュアメールソフトやWWWブラウザー内部で行われる。次に認証局に公開鍵とその公開鍵の正当性を証明するような自分の属性（Aさんの名前、メールアドレスなど）を一緒に送る。認証局では受け取った情報をもとにデジタルIDを発行する。これで公開鍵の登録は完了である。

認証局のもう1つの仕事は、登録されている公開鍵の問い合わせが第三者からあった場合に、それを証明書付きで送付することである。Aさんと暗号通信したい相手（この場合Bさん）がAさんの公開鍵を認証局に要求した場合、その公開鍵を証明書付きで送付する。

このように認証局は公開鍵に関する管理を厳重に行っている。では、認証局であるベリサイン社が発行するデジタルIDとはいったいどのようなものなのかをみてみよう。

デジタルIDは図7のような内容になっている。有効期限、認証番号、発行した認証局名に加え、登録者の属性（名前、メールアドレスなど）、登録者の公開鍵がその中に含まれている。これらを組み合わせたものをハッシングして認証局としてのベリサイン社の秘密鍵で暗号化した電子署名を作る（これもデジタルIDの中に含まれている）。これがデジタルIDとして発行される。

しかし、ここで疑問が生じる。ベリサイン社の電子署名を検証するために使う公開鍵はどこにあるのだろう。これに関しては心配は無用だ。RSAデータセキュリティー社の提唱するS/MIMEという暗号通信方法を使ったセキュアメールソフトウェアには、標準でベリサイン社の公開鍵が添付されているのだ。例えば、ネットスケープコミュニケーター（ネットスケープメッセンジャー）やマイクロソフトインターネットエクスプローラー（アウトルックエクスプレス）、また最近ではEudora Proなどのメールソフトに暗号化機能をもたせるようなソフトウェアがあり、これのソフトウェアにはベリサイン社の公開鍵がすでに配布されたかたちで組み込まれているのである。

図6 認証局の仕事

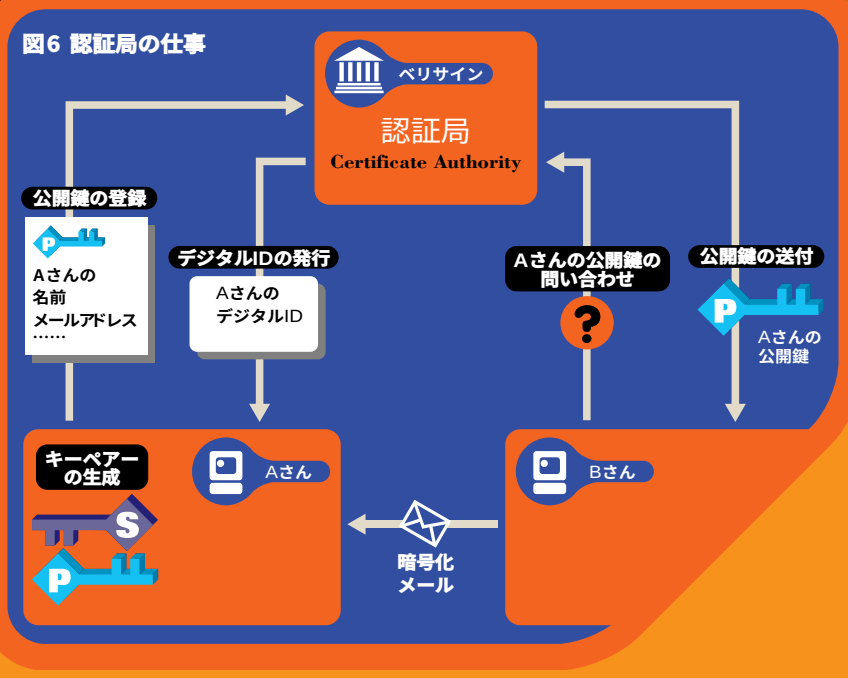
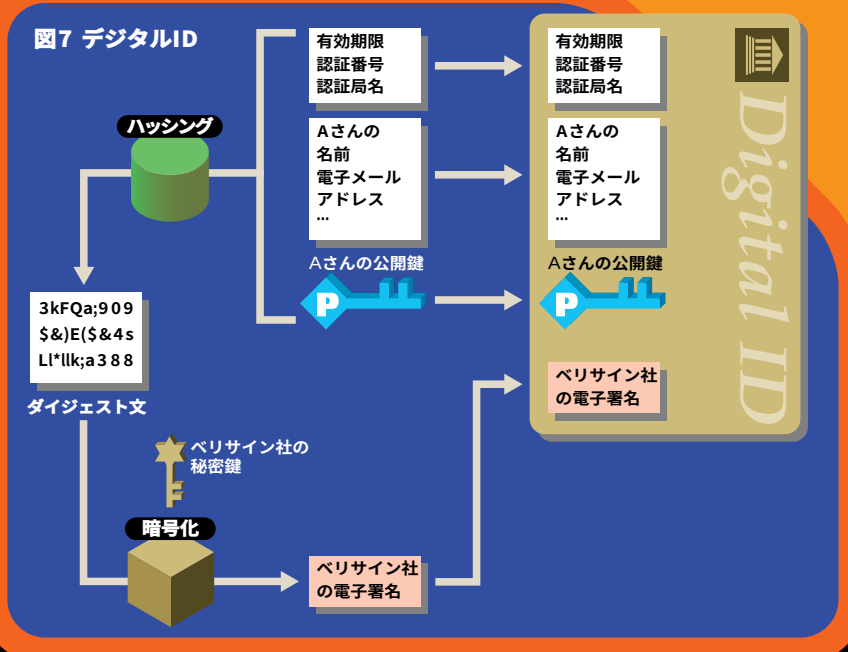


図7 デジタルID



図解　セキュアメールの送信から受信まで

暗号化のしくみは分かった。ではいったいどうやってセキュアメールはやり取りされているのか。ここでは電子署名付き暗号化メールが送信者から受信者へ届けられる様子を図を使って説明しよう。

1 公開鍵を手に入れる

暗号化メールを送る相手（この場合Bさん）の公開鍵を手に入れる

Aさん

あらかじめキーペアーを作成し、認証局に公開鍵の証明書であるデジタルIDを発行してもらう。

Aさんの秘密鍵

Aさんのデジタル ID

Bさんの公開鍵

認証局
Certificate Authority

公開鍵

2 メール本文から電子署名をつくる

メール本文をハッシングして
Aさんの秘密鍵で暗号化する。

このメールは暗号化されて送信しています。 → ハッシング → Ll*llk;a38883kFQa;9Ll*llk;a38883 → 暗号化（Aさんの秘密鍵） → 電子署名

本文
このメールは暗号化されて送信しています。

本文
電子署名
Aさんのデジタル ID

暗号文
38883kFQa;9Ll*llk;a38883kFQa;909$&)E38883kFQa;9Ll*
暗号化された共通鍵

5 メールを送信する

3 メール全体を暗号化する

メール本文と電子署名、AさんのデジタルIDを共通鍵で暗号化する。
共通鍵はメールソフトが自動的に生成する

本文
電子署名
Aさんのデジタル ID

共通鍵 → 暗号化 → 暗号文
38883kFQa;9Ll*llk;a38883kFQa;909$&)E38883kFQa;9Ll*

4 共通鍵を暗号化する

③で使った共通鍵をBさんの公開鍵で暗号化する。

共通鍵 → 暗号化（Bさんの公開鍵） → 暗号化された共通鍵

暗号を組み合わせよりスピーディーに

この図で説明した電子署名付き暗号化メールの送受信では「盗聴」、「改ざん」、「なりすまし」のすべての危険を回避することができる。ここで注目してほしいのは、③でなぜ共通鍵暗号を使ってメール全体を暗号化しているかということである。

共通鍵暗号方式は公開鍵暗号方式に比べて、暗号化と復号化処理が圧倒的に高速である。また暗号化で生成された文の大きさも小さくてすむ。そのため、メール全体を受信者の公開鍵で暗号化するより、メール全体を共通鍵で暗号化し、共通鍵だけを受信者の公開鍵で暗号化するほうが効率がよい。これはメール本文の大きさが大きくなるほど顕著となる。

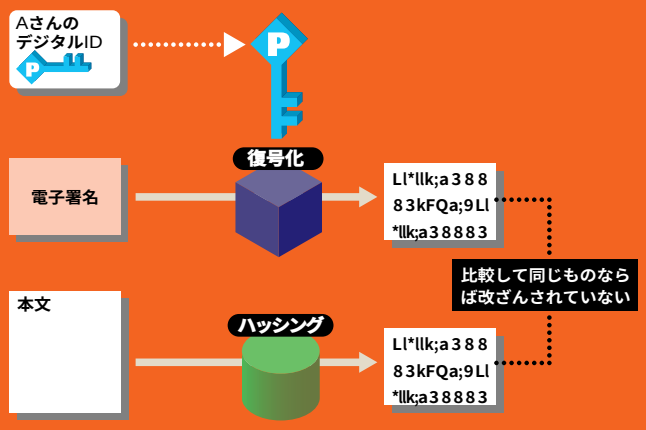
また、同じメールを複数の人に送るときも、メール全体を受信者ごとに各自の公開鍵で暗号化するよりも、1つの共通鍵で暗号化し、共通鍵だけを各自の公開鍵で暗号化したほうが効率的である。

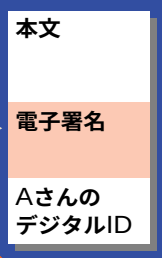
このように2つの暗号方式の利点を活かすことによって安全で高速な処理が実現されているのだ。

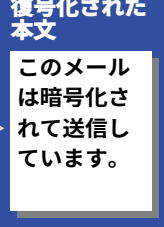
なお、共通鍵は送信のたびにまったく新しいものが生成されるので、管理については考えなくてもよい。

⑧ 電子署名をチェックする

⑦で得られたものを使い、メール本文をハッシングし、電子署名をAさんの公開鍵で復号化する。両方の結果を比較し、同一であればメール全体が改ざんされていないことが確認される

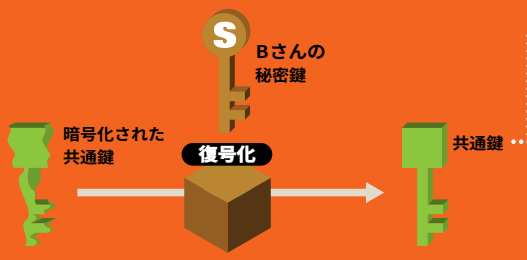






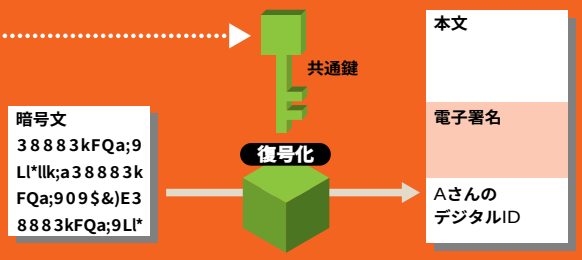
⑥ 共通鍵を復号化する

受信したメールから、暗号化された共通鍵を取り出しBさんの秘密鍵で復号化する。



⑦ 暗号文を復号化する

暗号文を⑥で得られた共通鍵を使って復号化する。

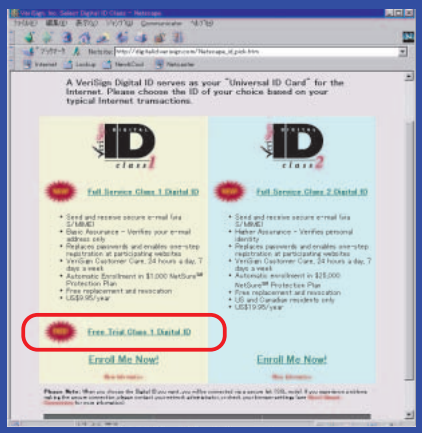


ネットスケープメッセンジャーを使った セキュアメールの使い方

Step 1 ベリサイン社から自分のデジタルIDを手に入れよう

電子署名を付けたり、メールを暗号化したりするには、なにはなくともデジタルIDが必要だ。現在、ベリサイン社がWWWブラウザー用に6か月間無料で使えるトライアル用のデジタルIDを提供している。ここではこのデジタルIDの入手方法をネットスケープコミュニケーターを使って解説しよう。

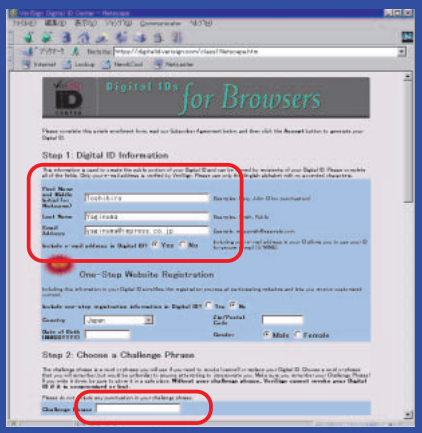
1 ベリサイン社のデジタルIDセンターへ



下記のURLのベリサイン社デジタルIDセンターから「エンドユーザー」→「ブラウザ用デジタルID」→「Netscape Navigater」を選ぶと図の画面が表示される。ここから「Free Trial Class 1 Digital ID」を選ぶ。

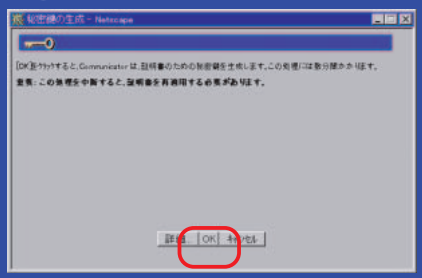
URL：http://digitalid.verisign.co.jp/

2 必要事項を記入



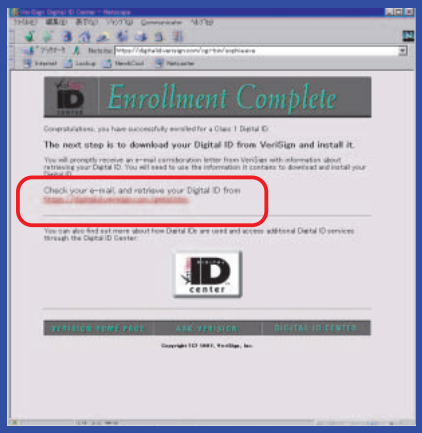
デジタルID登録画面が表示されるので必要事項を入力する。また「Challenge Phrase」は、手に入れたデジタルIDをあとで破棄する際に必要なので忘れないようにしよう。

3 鍵の生成



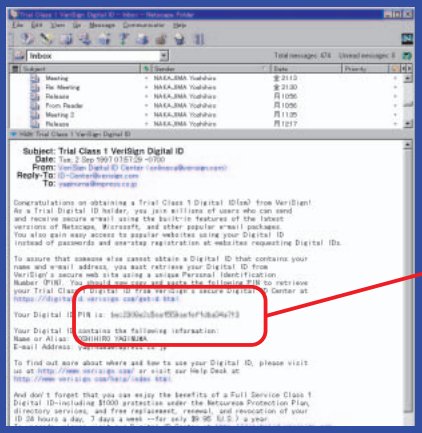
②で記入を終えて「Accept」ボタンをクリックすると図のウィンドウが表示され、コミュニケーターがキーペアー生成の準備に入る。OKボタンを押すと生成が始まる。

4 ベリサインへ鍵を登録



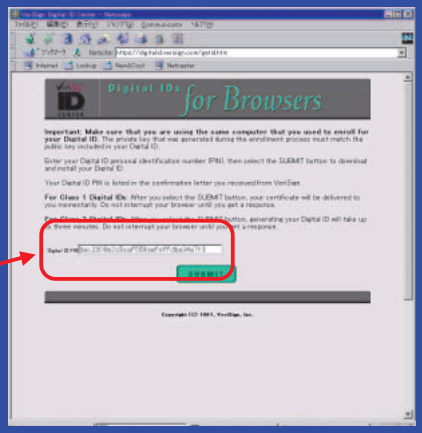
キーペアーの生成が終わると、自動的に公開鍵がベリサインに登録される。

5 登録確認メールの受信



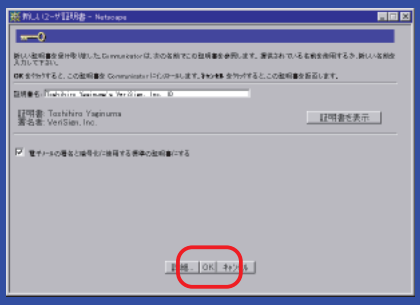
登録が完了すると、②で入力したメールアドレス宛てにベリサインよりメールが届く。このメールには、登録の確認とデジタルIDをダウンロードするための「PIN」という名前の登録番号が書かれている。

6 デジタルIDをダウンロード



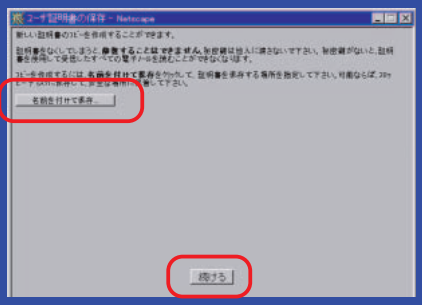
④の登録完了ページからデジタルIDのダウンロードページに行き、⑤のメールに記述されているPINを入力して「SUBMIT」ボタンをクリックする。

7 デジタルIDの確認



⑥が終わると自動的にデジタルIDがダウンロードされ、その確認画面が表示される。確認できたらOKボタンをクリックする。

8 デジタルIDの保存

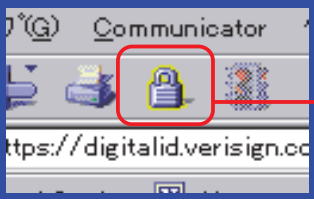


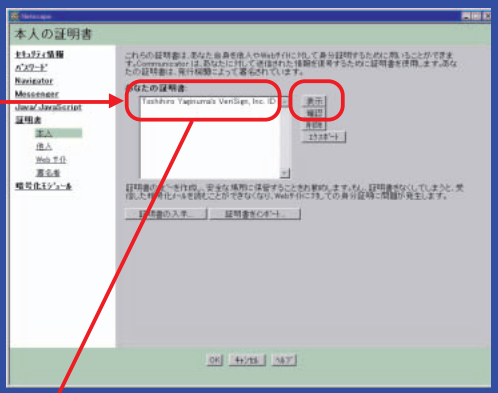
必要であれば秘密鍵（の証明書）のコピーを作成しておく。秘密鍵が壊れると修復は不可能なので、バックアップを作っておくことは大切だ。コピーはフロッピーディスクなど他人の手に届かない安全なところに保存して置こう。

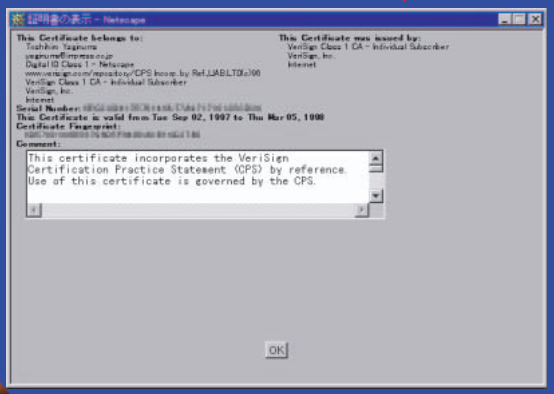
9 デジタルIDのインストール完了

これですべてが完了だ。最後に自分のデジタルIDを確認してみよう。

10 手に入れたデジタルIDの確認







発行されたデジタルIDを確認するには、コミュニケーターの「セキュリティ」ボタンをクリックし、表示されたウィンドウの「証明書」の「本人」をクリックする。ここでインストールされたデジタルIDが確認できる。デジタルIDには、自分の名前、メールアドレス、発行認証局名、有効期限などが記載されていることが分かる。

コミュニケーターの例を取り上げて、デジタルIDの入手方法を解説してみた。ここで入手したデジタルIDは無料トライアル用のもので6か月間しか使えない。もしその後も利用したいときは、1年につき9.95ドルが必要だ。また手に入れたのはベリサイン社の発行するクラス1というレベルのデジタルIDである。ベリサイン社ではそのレベルに応じて、3つのデジタルIDを発行している。

[クラス1]…個人情報として名前と電子メールアドレスのみで登録できるWWWブラウザーやメールソフト向けのデジタルIDだ。これは厳密には個人を特定することはできない。
[クラス2]…デジタルIDの取得の際にクラス1よりも高いレベルで個人を特定できるように社会保障番号などの入力を求められる。これは現在北米でのみ取得できる。より重要な情報をやり取りする電子メールやオンラインショッピングで効力を発揮するだろう。
[クラス3]…一般的には企業向けのものであり、主にWWWサーバーの認証用に使われている。料金も高額だ。

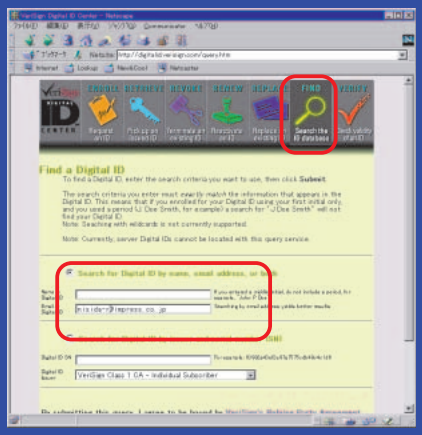
今回のデジタルIDの取得は米国ベリサイン社より行った。現在のところWWWブラウザー用のデジタルIDは日本ベリサインでは発行していないが、特定のS/MIME対応メールソフトウェアを使用した場合のみ日本でデジタルIDが発行されるようだ。これらのソフトウェアには1年間のデジタルID使用料が含まれている。日本ベリサインではさらに継続してS/MIME用クラス1のデジタルIDを使用するのに年間1,500円の価格を予定している。

暗号メール
そのしくみと実践

Step 2 受信者の公開鍵(デジタルID)を手に入れよう

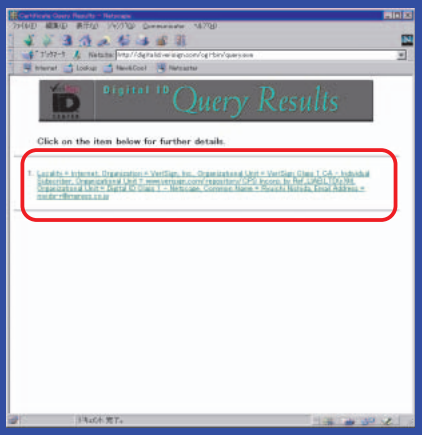
自分のデジタルIDは手に入れた。やっと暗号化メールを送ることができる。と思ったら送信相手の公開鍵がないことに気が付いた。どうすればいいのだろう。そんなときのためにここではベリサイン社に登録されている公開鍵の入手方法を解説しよう。

1 受信者のデジタルIDを検索



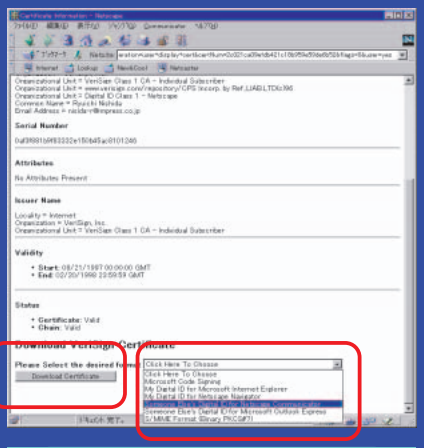
ベリサイン社の発行するデジタルIDを管理するのがデジタルIDセンター(http://digitalid.verisign.com/)だ。登録されているデジタルIDを検索するには、「FIND」をクリックして図の検索画面に行く。ここで相手の名前もしくは電子メールアドレスを正確に入力する。

2 検索結果の表示



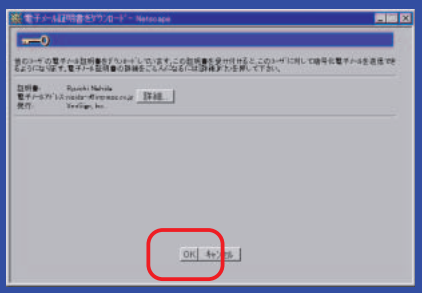
①で入力を完了し「SUBMIT」ボタンをクリックすると、図の検索結果が表示される。相手によっては複数結果が表示される場合もある。送信相手にどれを使うかを確認する必要がある。

3 必要なデジタルIDの選択



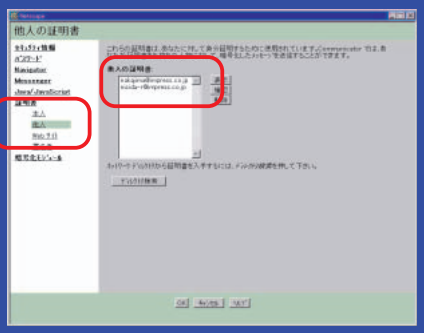
②で表示された結果をクリックし、詳細ページにすすむ。ページ下部より必要なデジタルIDの種類を選ぶ。リストから「Someone Else's Digital ID for Netscape Communicator」を選択し、「Download Certificate」ボタンを押す。

4 デジタルIDのダウンロード



自動的にデジタルIDのダウンロードが始まる。図のウィンドウが開いたらOKボタンを押すだけでデジタルIDがWWWブラウザーのデジタルIDデータベースに登録される。

5 デジタルIDの確認



入手したデジタルIDを確認してみよう。WWWブラウザーの「セキュリティ」ボタンをクリックし、「証明書」の「他人」をクリックする。今ダウンロードしたものが表示されている。さらに詳細を見たい場合は、表示ボタンをクリックしよう。

ベリサインに登録されているデジタルIDを探すためには、デジタルIDセンターにアクセスする必要がある。このデジタルIDセンターには米国(http://digitalid.verisign.com)のものと日本(http://digitalid.verisign.co.jp)のものがある。日本で発売されているいくつかのS / MIME対応ソフトウェアは日本のベリサインにデジタルIDを登録するようになっている。しかし残念ながら日本で登録されたIDは米国デジタルIDセンターでは検索できない。同様に、今回のように米国ベリサインで登録した場合、日本のベリサインのデジタルIDセンターで検索できない。これに関しては今後の対応を待ちたい。

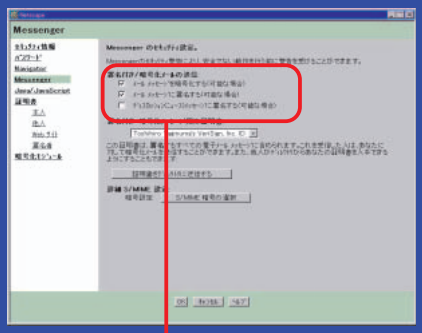
ほかの方法として、公開鍵は相手から署名付きのメールを送ってもらうことで手に入れられるということを覚えておくと便利だ。

暗号メール そのしくみと実践

Step 3 電子署名付き暗号化メールを送信しよう

すべて準備はととのった。操作はいたって簡単で、設定さえすれば普通のメールと同じように送信できる。では、電子署名付き暗号化メールを送ってみよう。

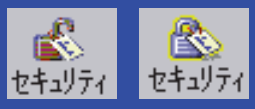
1 セキュリティーボタンで設定

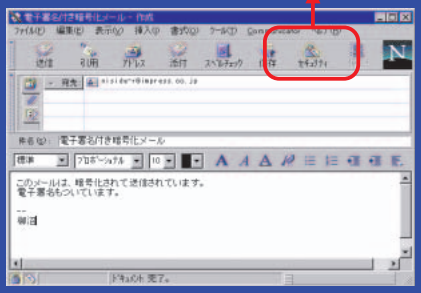


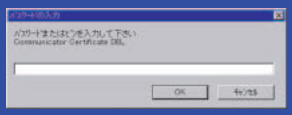
署名付き/暗号化メールの送信:
- [x] メール メッセージを暗号化する(可能な場合)
- [x] メール メッセージに署名する(可能な場合)
- [ ] ディスカッション(ニュース)メッセージに署名する(可能な場合)

署名付きや暗号化といった設定は、コミュニケーターの「セキュリティ」ボタンをクリックし、「Messenger」を選択して設定できる。図のチェックボックスで好みの設定をすればよい。公開鍵は一度手に入れればよいが、暗号化するにはメールを送信する前に手に入れておく必要がある。

2 メールを書く





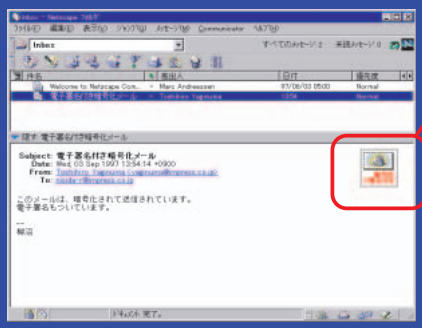


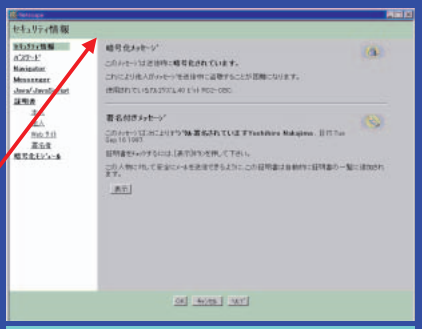
ここで注目して欲しいのはメッセンジャーの「セキュリティ」ボタンだ。署名付きのみを設定していればアイコンに名札が付き、署名付きと暗号化を両方設定していれば、名札が付き、鍵がしまる。送信ボタンを押すと、秘密鍵使用のためのパスワードが要求される。これは他のユーザーに秘密鍵を乱用されないようにするためだ。

Step 4 受信メールを確認しよう

受信者側は特に何もすることがなくマークがあるかどうかを確認するだけだ。

1 メールの受信





相手に送信したメールはどのように見えるのだろう。 メッセンジャーで受け取った場合、図のように表示画面の上に署名付きか暗号化かが表示される。このマークをクリックすると詳細を見ることができる。

スタンダードの有力候補「S/MIME」

インターネットでの通信に多くの危険が伴うことは冒頭で述べた。電子メールは特にその標的にされやすいことをいつも念頭に置いておくべきだ。それを防ぐためのS/MIMEに対応したセキュアメールは、しくみこそ難しいもののその操作は非常に簡単であることが分かっていただけただろう。

今回取り上げたS/MIME以外にもインターネットで普及しているセキュアメールとしてPGP（Pretty Good Privacy）がある。PGPは利用者は多いが、その操作方法の難しさから初心者などには敬遠されがちだ。インターネットの標準にS/MIMEとPGPのどちらが採用されるかで揺れ動いているようだが、多くの主要メーカーがサポートしている現時点ではS/MIMEに軍配があがることも予想される。

S/MIMEではこれに対応したソフトウェアを送受信双方で使わなければならない。現在S/MIMEに対応したソフトウェアはRSAデータセキュリティー社のInteroperability Center（http://www.rsa.com/smime/html/interop_center.html）で確認することができる。最後に、日本で発売されているS/MIME対応ソフトウェアを紹介しておく。

S/MIMEに対応したおもな日本語製品

【電子メールソフト】

●ネットスケープメッセンジャー
日本ネットスケープコミュニケーションズ株式会社
価格…… オープン価格

●アウトルックエキスプレス
マイクロソフト株式会社
価格……無料配布

【アドインソフト】

●セキュアメッセンジャ 1.0 J
株式アスキーサムシンググッド
価格 ……14,800円（1ユーザー）

●魔法便
NTTエレクトロニクス株式会社
価格 ……15,200円（1ユーザー）

アドインソフトは、既存のメールソフトウェアにS/MIMEの機能を追加するものだ。対応ソフトウェアはマイクロソフトエクスチェンジ、マイクロソフトWindows Messaging、マイクロソフトアウトルック97、Eudora Proである。これらのソフトは基礎編（250ページ）で取り上げているので参考にして欲しい。

［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的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

Copyright © 1994-2007 Impress R&D, an Impress Group company. All rights reserved.