

電子メールのセキュリティ

S/MIMEを利用した暗号化と電子署名

目次

1	電子メール利用上の脅威.....	1
1.1	盗聴が可能.....	1
1.2	なりすましが可能.....	2
1.3	暗号を使って安全な通信を確保する.....	2
2	暗号技術について.....	3
2.1	共通鍵暗号方式.....	3
2.2	公開鍵暗号方式.....	4
2.3	メッセージダイジェスト関数.....	4
3	公開鍵暗号方式を使ってできること.....	5
3.1	公開鍵暗号方式の使い方.....	5
3.2	メッセ - ジの暗号化.....	6
3.3	電子署名.....	8
3.4	電子署名と暗号化.....	10
4	公開鍵を信頼するために.....	12
4.1	PGP 的信頼の輪.....	12
4.2	認証機関(CA)を導入.....	13
5	認証機関が発行する公開鍵証明書と CRL(失効リスト).....	15
5.1	証明書(公開鍵証明書、デジタル ID®).....	15
5.2	CRL(Certificate Revocation List).....	17
6	電子メールソフト Microsoft Outlook Express で S/MIME を使う.....	18
6.1	電子メールで S/MIME を使うための準備.....	18
6.2	他人の証明書の収集.....	26
6.3	電子署名を付けて電子メールを送る。.....	27
6.4	暗号化して電子メールを送る。.....	28
6.5	電子署名と暗号化を組み合わせる.....	28
6.6	電子署名付きメールを受ける.....	28
6.7	暗号化されたメールを受ける.....	29
6.8	電子署名と暗号化されたメールを受ける.....	29
6.9	不正なメールを受けると.....	30
6.10	証明書の管理.....	31
6.11	CRL(証明書失効リスト).....	32
7	電子メールソフト Netscape Messenger で S/MIME を使う.....	33
7.1	電子メールで S/MIME を使うための準備.....	33
7.2	他人の証明書の収集.....	34

7.3	電子署名を付けたり、暗号化をして電子メールを送る。	35
7.4	電子署名付きメールを受ける	35
7.5	暗号化されたメールを受ける	35
7.6	電子署名と暗号化されたメールを受ける	36
7.7	不正なメールを受けると	37
7.8	証明書の管理	37
8	電子メールソフト Winbiff で S/MIME を使う	38
8.1	電子メールで S/MIME を使うための準備	38
8.2	他人の証明書の収集	41
8.3	電子署名を付けたり、暗号化をして電子メールを送る。	42
8.4	電子署名付きメールを受ける	43
8.5	暗号化されたメールを受ける	43
8.6	電子署名と暗号化されたメールを受ける	43
8.7	不正なメールを受けると	44
8.8	証明書の管理	44
9	S/MIME のメールメッセージ	45
9.1	標準仕様	45
9.2	MIME ヘッダ	45
9.3	電子署名の例	47
9.4	暗号化	47
9.5	電子署名+暗号化	48
9.6	証明書署名要求	48
9.7	証明書の添付	49
10	証明書の実例	51
11	認証パスの実例	53
12	ルート認証局の証明書について	54
13	参考文献	55

1 電子メール利用上の脅威

電子メールの通信というのは、郵便葉書を使った、メッセージのやりとりと似ています。電子メールのメッセージは、葉書の裏に書かれた文章が、まったく隠されずに運ばれているのと、同じように、いくつものコンピュータを経由して運ばれて相手に運ばれていきます。そこでは、通信の経路上に関わっている人たちが良心を持ちあえて、他人のメッセージの内容に関与するようなことはせず、仲介してくれることによってなりたちます。

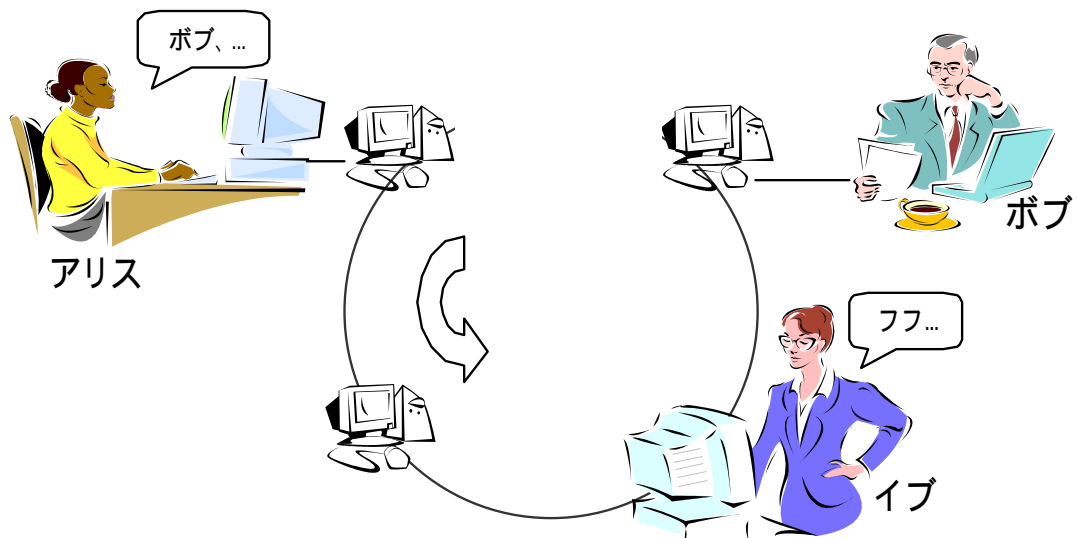
また、送り手は、どのような経路で相手に届くのかを選択することができません。

そのような、協調的な分散型のシステムでは、盗聴やなりすましなどの危険が潜んでいます。

1.1 盗聴が可能

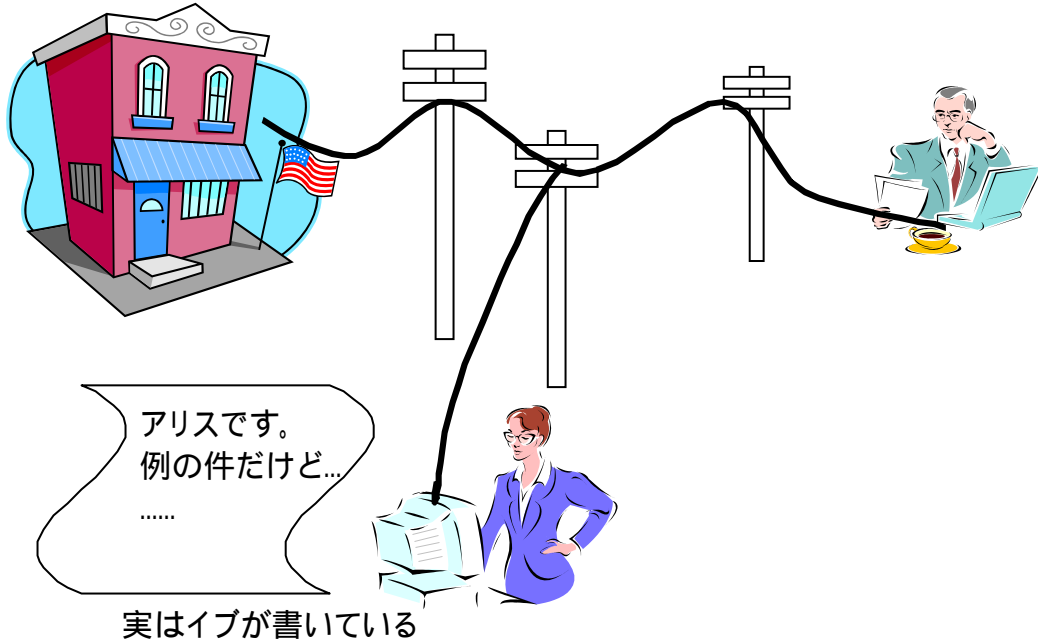
「アリス」が「ボブ」に電子メールでメッセージを送る場合、メッセージの先頭に宛名として、ボブのアドレスを付けて、送信します。このメッセージがボブに届くまでに、いくつものコンピュータを経由しています。

この途中に経由しているコンピュータの操作者は、簡単にアリスの電子メールのメッセージをみることができます。



1.2 なりすましが可能

「アリス」と「ボブ」の電子メールを知っている「イブ」は、送り元アドレスに「アリス」のメールアドレスを記入することによって、「アリス」と偽って「ボブ」に電子メールを送ることが簡単にできます。



その他の悪意ある行為として、「イブ」は、メーリングやニュースグループなど、不特定多数の相手の目に触れる場に対して、「アリス」と偽って発言することも可能です。

盗聴が可能であれば、盗聴したメッセージを変更して(改ざん)「アリス」になりすまして、「アリス」と「ボブ」のコミュニケーションを惑わすことも可能です。

1.3 改ざんが可能

「イブ」は盗聴した電子メールの中身を変えて、「アリス」になりますまして「ボブ」に送ることもできます。これを「改ざん」と呼びます。

1.4 暗号を使って安全な通信を確保する

このような環境にある、電子メールによるコミュニケーションにセキュリティを確保するために、私たちにできることは、メッセージを暗号化して意図しない他人に読まれることを防ぐこと、メッセージに電子署名を付けて、自分が書いた文章であることを保証することです。

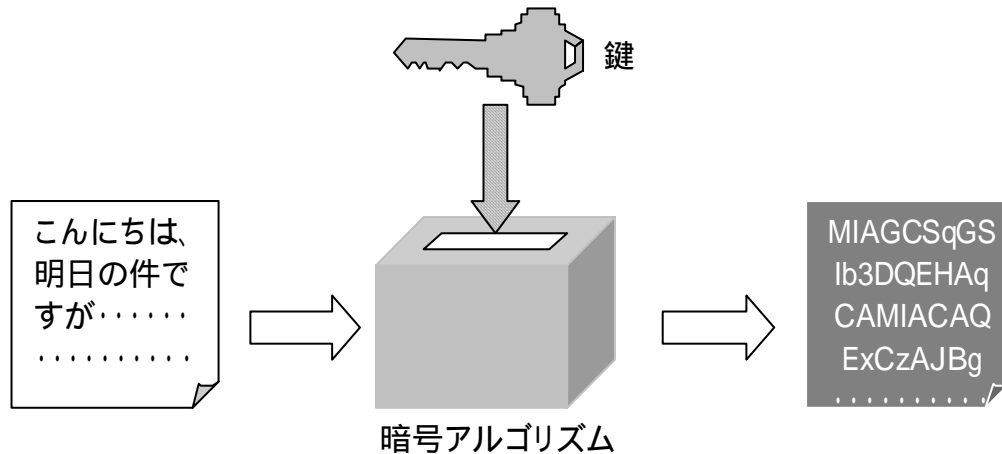
電子署名を付けることを条件に通信をおこなえば、電子署名がなければ、あるいは、電子署名が正しいものでなければ、偽造されたメッセージであることがわかるわけです。

次章以降では、これらの暗号と電子署名の仕組みについて、説明します。

2 暗号技術について

暗号化とは、特定の決まりにしたがって、文章やファイルのデータの並び替えを行うことです。

この特定の決まりとして、数学的な処理(暗号アルゴリズム)や、鍵とよばれる特別なパスワードを使います。もとのメッセージ(平文と呼びます)を、並び替えて、別のメッセージ(暗号文)に変換することを暗号化といいます。暗号文をもとの平文に戻すことを復号といいます。

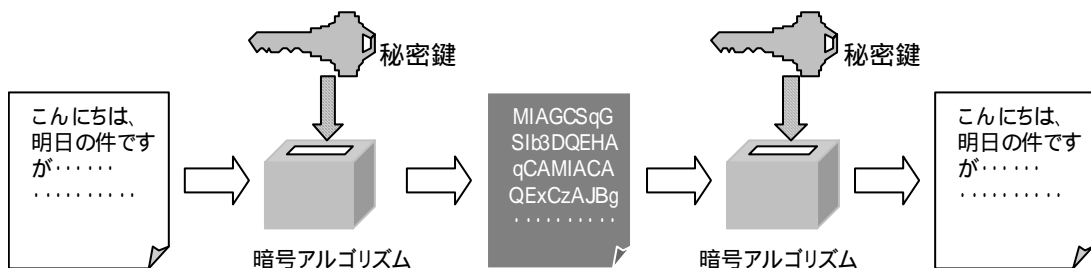


電子メールに適応される暗号技術は、鍵の使い方や処理方式によって、大きく次の3つに分類することができます。

2.1 共通鍵暗号方式

メッセージを暗号化するときと、復号するとき同一鍵を使う暗号アルゴリズムです。秘密鍵暗号方式または、対称暗号方式などとも呼ばれます。

この方式を基にしたものに RC2、RC5、DES、Triple-DES、IDEA などがあります。

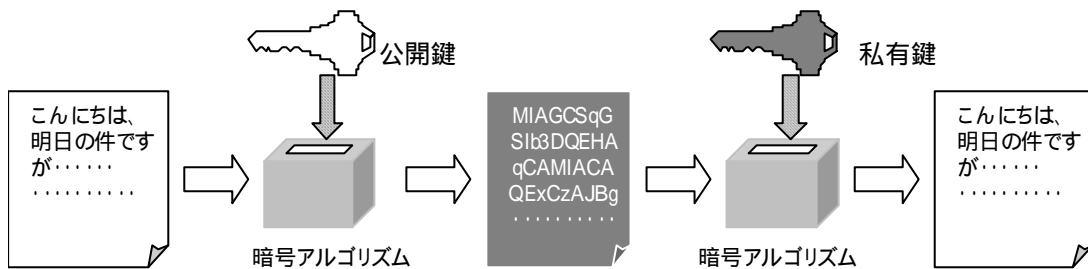


2.2 公開鍵暗号方式

メッセージを暗号化するときと、復号するときで、異なる鍵を使う暗号アルゴリズムです。この方式では、暗号化用の鍵を公開し、復号用の鍵を自分だけが秘密に保持します。そのため、暗号化用の鍵を公開鍵(public key)、復号用の鍵を私有鍵(private key)と呼びます。

また、この方式は、非対称暗号方式とも呼ばれます。

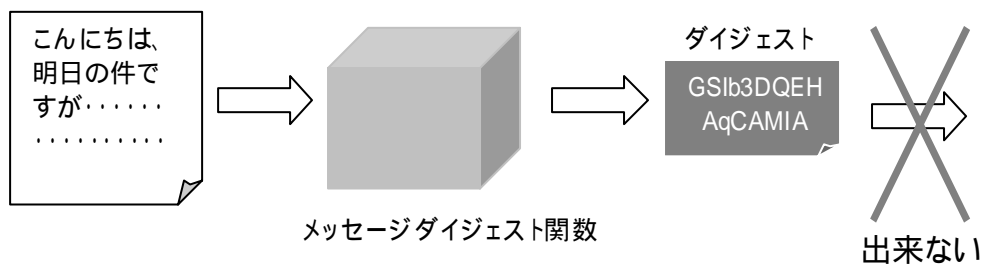
この方式を基にしたものに RSA、Diffie-Hellman などがこの方式です。



2.3 メッセージダイジェスト関数

不定長のデータを固定長のデータに変換する関数です。変換結果の固定長のデータをハッシュ値と言います。生成したハッシュ値から、もとのデータを逆算しにくいものを、特にメッセージダイジェスト関数と呼びます。メッセージダイジェスト関数の結果のハッシュ値をダイジェスト(または、メッセージダイジェスト)と呼びます。

メッセージダイジェスト関数としては、MD2(ハッシュ値は 16 バイト)、MD5(16 バイト)、SHA1(20 バイト)などがあります。



3 公開鍵暗号方式を使ってできること

前章で説明した3つ暗号方式を組み合わせ、電子メールに応用することによって、以下の3つのセキュリティを確保します。

- メッセージの秘匿性
- 認証
- メッセージの完全性

メッセージの秘匿性とは、メッセージを暗号化することによって、意図しない相手に盗み見られることを防ぐことです。共通鍵暗号、公開鍵暗号方式と組み合わせることによって共通鍵暗号における秘密鍵の共有の困難さを解決し、メッセージの暗号化を実現します。

認証とメッセージの完全性はメッセージに電子署名を付け加えることによって実現されます。そなわち、電子署名の正しさを確認することによって、送信元に偽りのないことと、メッセージに改ざんのないことが確かめられます。電子署名は、メッセージダイジェスト関数と公開鍵暗号方式を組み合わせることによって実現します。

そのための手順には S/MIME や PGP があります。次節以降では、どのような手順でこれら3つのセキュリティが可能となるのかを見ていきます。

3.1 公開鍵暗号方式の使い方

まず、あなたは、公開鍵暗号方式を使うために、公開鍵と私有鍵のペアを作成します。その公開鍵は暗号メールをやり取りする相手に渡します。

あなたの公開鍵を持っている通信相手は、あなたが、私有鍵をキーとして暗号化したデータを復号することができます。この方式を電子署名で用います。

また、通信相手があなたの公開鍵を用いて暗号化したデータを、あなたは、あなたの私有鍵で復号できます。この方式を暗号化で用います。

したがって、受け取った、公開鍵が正しく相手のものであることが、前提となります。どのようにすれば、受け取った公開鍵が間違いなく相手のものであると信用できるのかについては次章で説明します。

一方、私有鍵は、作成した本人だけが保持し、あなただけが使えるように、パスワードを使って暗号化しておくなど安全に保管しておきます。そして、電子署名をするとき、または、暗号化されたメッセージを復号するために、私有鍵を使う場合、パスワードを入力してから使うようにします。私有鍵のパスワードは他人に明かさずにしておき、あなただけが使えるようにしておきます。ただし、私有鍵のパスワードの扱いは、製品によって、様々です。OS と統合する、起動後の初回のみ確認するなどのバリエーションがあります。

3.2 メッセージの暗号化

1) 送信側と受信側の処理は以下のようになります。

送信側(アリス)

メッセージを共通鍵暗号方式で、暗号化し暗号文を作成します。

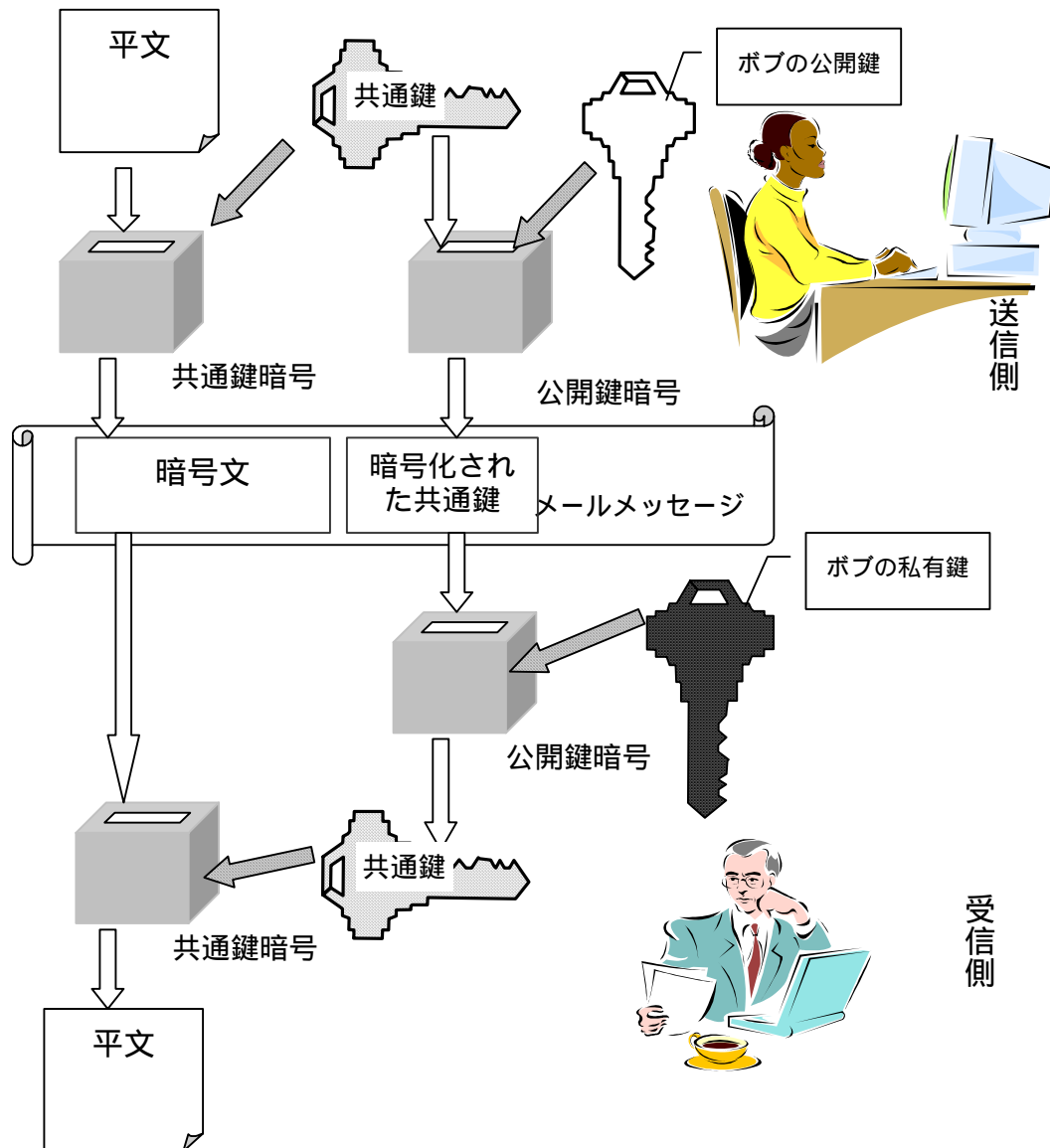
で用いた秘密鍵を、受信者の公開鍵を鍵として使って公開鍵暗号方式で暗号化します。 受信者の数だけ、同様の操作をします。

の暗号化の結果のデータと の結果のデータをメールで送ります。

受信側(ボブ)

送られて来たデータの中から、自分宛のパートの暗号文を自分の私有鍵を鍵として使って公開鍵暗号方式で復号します。その結果、共通鍵暗号方式の秘密鍵を獲得します。

で得た、秘密鍵を使って暗号文を復号し元のメッセージを得ます。



2) 暗号化されたメールメッセージの中身

暗号化されたメールメッセージは下表のような形式になっています。

受信者ごとのデータのうち、識別データが、自分宛のものを探し出し、そこについている、秘密鍵を暗号化したデータが与えられるので、私有鍵を鍵として、復号し、秘密鍵を得ます。

暗号文
受信者 A の識別データ (証明書発行者名+シリアル番号)
暗号文の作成に用いた、暗号キーを受信者 A の公開鍵をキーとして公開鍵暗号で暗号化したデータ
受信者 B の識別データ (証明書発行者名+シリアル番号)
暗号文の作成に用いた、暗号キーを受信者 B の公開鍵をキーとして公開鍵暗号で暗号化したデータ
(受信者分)

3.3 電子署名

1) 送信側と受信側の処理は以下のようになります。

送信側(アリス)

メッセージダイジェスト関数を使って本文のダイジェストを作成します。

秘密鍵をキーとしてダイジェストを公開鍵暗号化方式で暗号化します。 署名データの作成

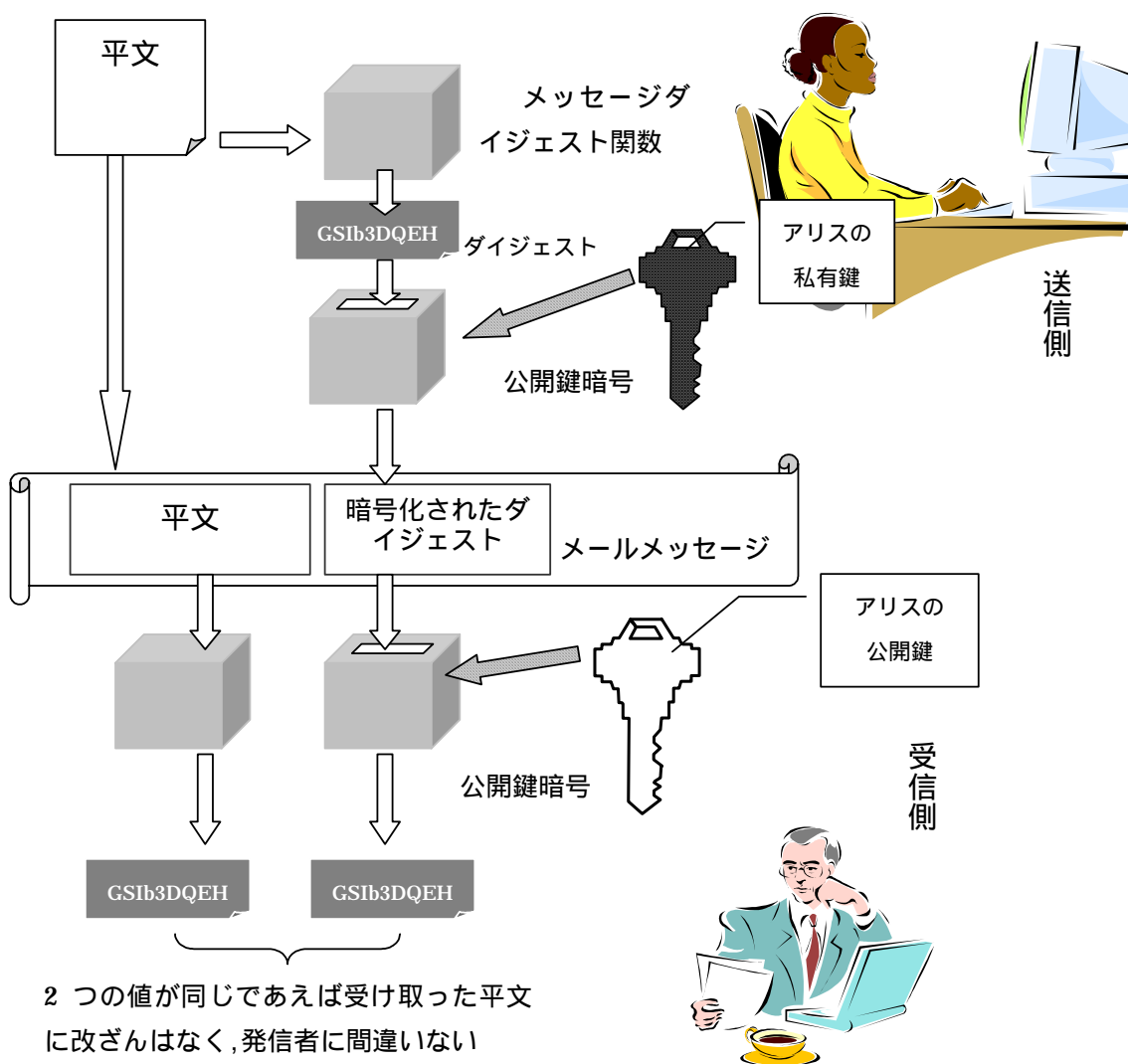
本文と署名データ(の結果)をメールで送ります。

受信側(ボブ)

発信者と同様に、メッセージダイジェスト関数を使って本文のダイジェストを作成します。

署名データを発信者の公開鍵をキーとして公開鍵暗号化方式で復号します。 その結果、発信者の作った、ダイジェストを獲得します。

との結果を比較して、同一であれば、発信が作成したメッセージであることが保証されます。



2) 電子署名のついたメールメッセージの中身

電子署名をつけた、メッセージは下表のような形式になっています。

署名者を識別するデータがあるので、そこにしめされた証明書発行者名とシリアル番号から、署名者の証明書が明らかになり、その証明書に含まれる、公開鍵によって、署名を検証します。

メッセージ(平文)	
署名 データ	署名者の識別データ (証明書発行者名+シリアル番号)
	ダイジェストを署名者の私有鍵を鍵として公開鍵暗号方式で暗号化したデータ (署名データ)
署名者の証明書 (オプション)	

3) 証明書の添付

署名者の証明書は、受信した側で既に持っていることも考えられるので、通信量を減らすなどの目的で証明書が添付されていない場合もあります。

Microsoft Outlook Express では、「署名付きメッセージにデジタル ID を追加する」をチェックすると証明書を添付し、チェックをはずすと証明書を添付しません。

Netscape Messenger では、常に証明書を添付しています。

Oangesoft Winbiff+S/Goma では、「証明書を添付する」をチェックすると証明書を添付し、チェックをはずすと証明書を添付しません。

4) 平文のエンコード

電子署名には、上表のようなメッセージ本文を平文のまま送る形式と BASE64 とよばれる、コード化をする形式があります。BASE64 でコード化された場合、平文は一目では明らかになりませんが、元に戻すための決まった方法があるので、ユーザが意識することなく、メールソフトなどが自動的に元に戻して、平文が確認できます。

Microsoft Outlook Express では「署名する前にメッセージをエンコードする」をチェックするとこの形式になります。

Netscape Messenger では、この形式は選択できません。

Oangesoft Winbiff+S/Goma では「分離署名(クリア電子署名)」のチェックを外すとこの形式になります。

3.4 電子署名と暗号化を組み合わせる

1) 送信側と受信側の処理は以下のようになります。

送信側

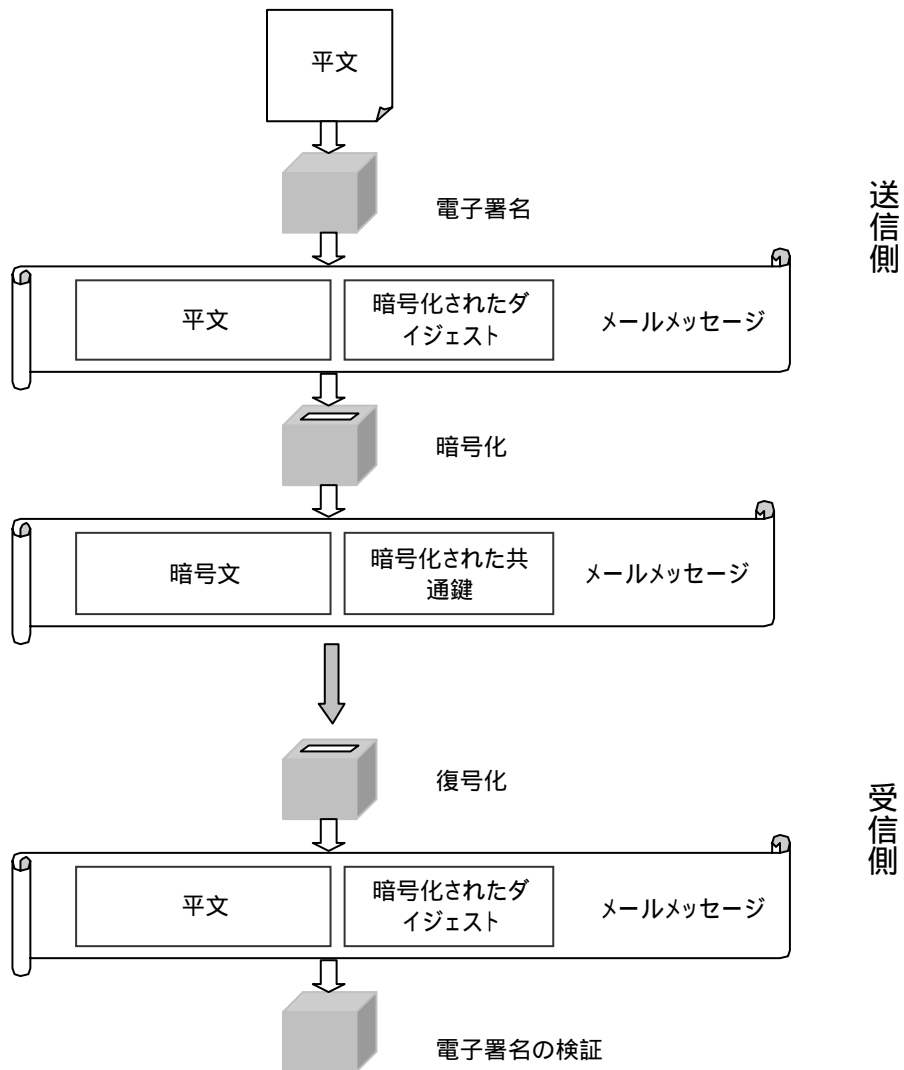
電子署名をします。

電子署名のついたメッセージを入力として暗号化します。

受信側

受信したメッセージを復号して、電子署名されたメッセージを得ます。

電子署名を検証します。



2) 電子署名と暗号化を組み合わせる 2 つの方法

暗号化と電子署名を 1 つのメッセージに対して行う場合、2通りの方法が考えられます。

電子署名したデータを入力として暗号化をする (Sign-Then-Envelop)

受信側では、暗号文を復号し、電子署名されたデータを得る。その後、電子署名の検証を行います。

1)ではこの方法について説明しています。S/MIME ではこの方法が使われます。

電子署名したデータと暗号化したデータをくっつける。(Sign-And-Envelop)

受信側では、暗号文を復号し、平文を得ます。

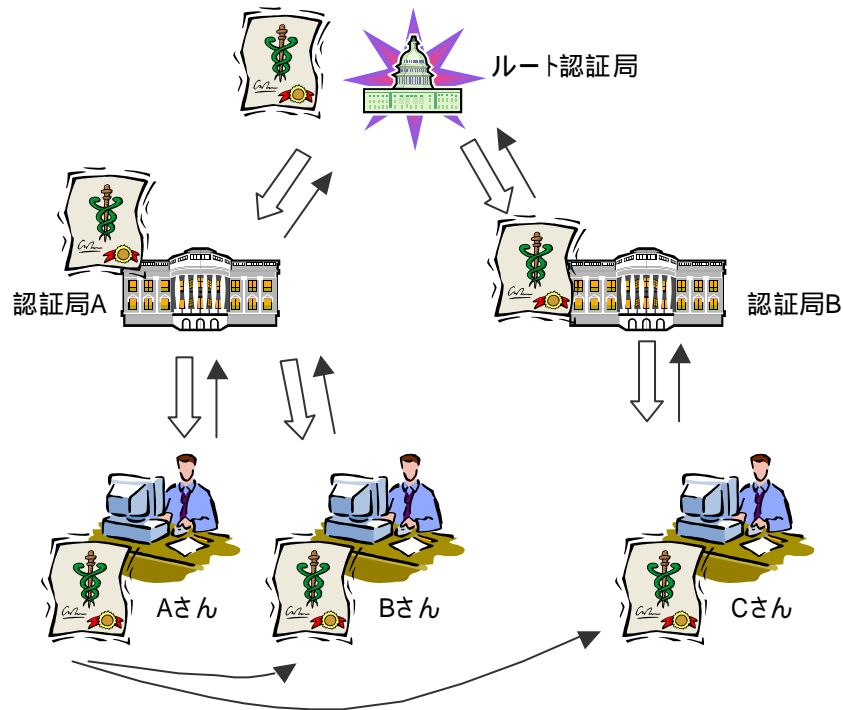
平文のダイジェストと、電子署名中の暗号化されたダイジェストを復号し、比較、検証します。

PEM と呼ばれる、S/MIME に似た古い仕様では、この方式になっており、S/MIME では PEM との互換のためにのみ用いられます。

署名者の識別データ (証明書発行者名+シリアル番号)
ダイジェストを署名者の秘密鍵をキーとして公開鍵暗号で暗号化したデータ (署名データ)
(署名者の証明書)
暗号文
受信者 A の識別データ (証明書発行者名+シリアル番号)
暗号データの作成に用いた、暗号キーを受信者 A の公開鍵をキーとして公開鍵暗号で暗号化したデータ
受信者 B の識別データ (証明書発行者名+シリアル番号)
暗号データの作成に用いた、暗号キーを受信者 B の公開鍵をキーとして公開鍵暗号で暗号化したデータ

(受信者分)

4.2 認証機関(CA)を導入



ユーザはルート認証局(最上位の署名者)の公開鍵を予め持っている、信頼しています。
 ルート認証局は、下位の認証局の公開鍵に署名を付けた公開鍵証明書を発行します。
 Aさんは、認証局Aに公開鍵を提出します。認証局Aは署名を付けてAさんの公開鍵証明書を発行します。
 Aさんの公開鍵証明書を受け取ったBさんやCさんは、まず認証局Aの公開鍵証明書の署名を手元にあるルート認証局の公開鍵を使って検証します。認証局Aの公開鍵として正しいことがわかったなら、次にAさんの公開鍵証明書の署名を認証局Aの公開鍵を使って検証します。
 S/MIMEでは、以上のような手順で、入手した公開鍵を信頼します。

4.3 拇印、指紋

公開鍵証明書を SHA.1 や MD5 などのメッセージダイジェスト関数の入力にして、得られたダイジェスト値を「拇印(Thumbprint)」または「指紋(fingerprint)」と呼びます。利用したメッセージダイジェスト関数を特に「拇印アルゴリズム」などとも呼びます。

SHA1 を使った場合、ダイジェスト値は 20 バイトなので、数字として表示すると、40 文字になります。初めて受け取った公開鍵証明書は、その拇印の 40 文字を、公開鍵の持ち主に問い合わせるなどして、公開鍵証明書の正しさを確認することができます。

ルート認証局の公開鍵証明書を受け取ったときなどは、この方法で確認することが有効です。

5 認証機関が発行する公開鍵証明書と CRL(証明書失効リスト)

5.1 証明書(公開鍵証明書、デジタル ID®)

暗号メールの利用者はお互いの公開鍵が必要ですが、その公開鍵は本人のものであることが保証されなければなりません。この問題を解決するために証明書と呼ばれるものが利用されます。

証明書のシリアル番号
認証局の名前
証明書の有効期間
公開鍵の所有者の名前、メールアドレス等
公開鍵
X.509 拡張項目
～ までのダイジェストに認証局の秘密鍵をキーとして公開鍵暗号で暗号化したデータ

公開鍵証明書とは、公開鍵とその所有者の名前、所属、メールアドレス等の情報を組み合わせたデータに第三者である認証局が電子署名したものです。認証局はその証明書データが本人のものであることを確認し、証明書の正しさを保証します。

認証局が電子署名をつけることを、証明書を発行すると言います。

利用者は、証明書データを認証局に提出し、自分の証明書を取得、公開することにより、初めて、暗号メールの送受信が可能となります。

認証局へ認証データを送ることを、証明書署名要求(Certificate Signing Request)と呼びます。

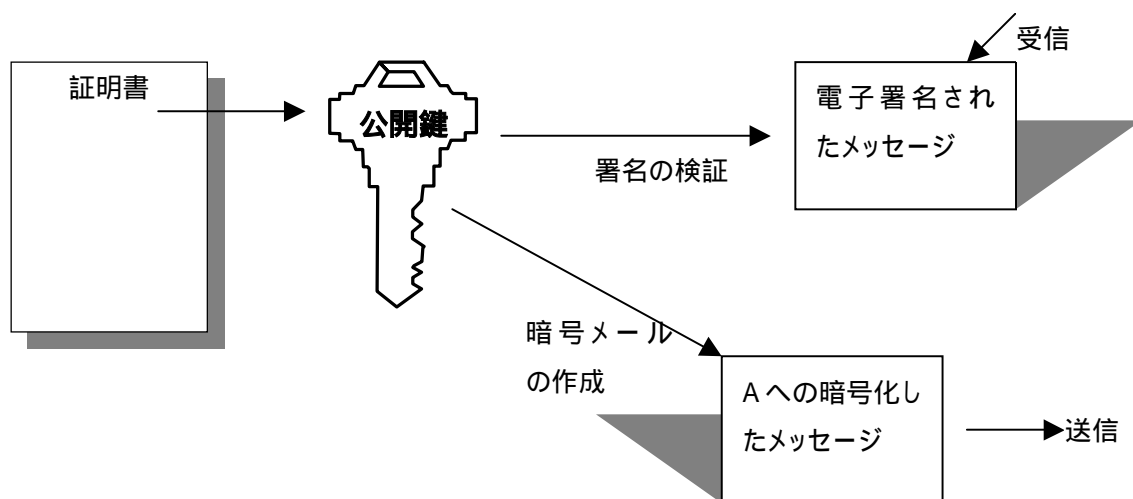
この方式は、階層構造になるので、最上位の認証局をルート認証局と言います。

ルート認証局 - 認証局 - ユーザ のような、階層を持った信頼関係を構築するので、これを認証パスあるいは証明パス(Certificate Chain)といいます。

ルート認証局は自身の私有鍵によって電子署名することによって、公開鍵証明書を作成します。このような証明書を自己署名の証明書などとも言います。

利用者はルート認証局の証明書を絶対的に信用することにより、この信頼関係は成り立ちます。ユーザはルート認証局の証明書には慎重にならなければなりません。

電子メールや Web ブラウザなどのアプリケーションソフトウェアでは下の図のように、証明書から公開鍵を取り出し、電子署名の検証や暗号化に使っているわけです。



なお、公開鍵証明書は ISO/IEC で規定されている X.509 仕様に基づいています。

X.509 V3 拡張項目は、以下のような構造になっていて、証明書には複数の項目を入れることができます。

項目 ID	
重要性	(重要または非重要) 重要となっていた場合、この項目の意味に応じた処理が要求されていることを示します。
値	

拡張項目では、公開鍵の用途を規定したり、次節でのべる CRL がどこから入手できるのかなどが示されています。

5.2 CRL(Certificate Revocation List、証明書失効リスト)

CRLとは無効になった証明書のシリアル番号の一覧に、認証局が電子署名をしたデータです。一つのエントリは、認証局が証明書ごとに割り振ったシリアル番号とそのシリアル番号の証明書が無効になった日付の組み合わせによりなります。

CRLの発行者の名前
CRLの発行日
次回CRL発行日
証明書のシリアル番号

無効になった日付
と の組み合わせが無効になった証明書の数だけ続く
電子署名 上のデータのダイジェストに認証局の秘密鍵を鍵として公開鍵暗号で暗号化したデータ

と に示されている日付が、CRLの有効期間を示します。 の示す時点で新しい、CRLが発行されます。したがって、ユーザは常に有効なCRLを入手する必要があります。

ただし、現在、CRLの配送に関して、明確な仕様はなく、S/MIMEをサポートしたメーラの場合、ほとんどが、証明書に同封されているCRLのみをあてにしています。

現実的な解決方法としては、ディレクトリサービスにユーザの個人情報とともに、証明書を登録しておき、CRLが発生した都度、サーバ側で、同期をとり、常に最新の証明書のステータスを保持しておくことが考えられています。

その場合、ユーザは、署名付きのメールを受け取るごとに、署名をした人の証明書が有効であるか、ディレクトリサーバに問い合わせることになります。

あるいは、電子署名をしたメールを送ってくる人たちの証明書の有効性を、 の時点で、ディレクトリサーバに問い合わせ確認しておくことになります。

S/MIMEで用いられるCRLはX.509に基づいています。

6 電子メールソフト Microsoft Outlook Express で S/MIME を使う

電子署名や暗号を利用するためには公開鍵証明書が必要になります。次節では、認証機関から公開鍵証明書を取得する手順について説明します。

公開鍵証明書はデジタルIDなどともよばれ、認証サービスを行っている会社などから取得することが可能です。

日本でも日本ベリサイン株式会社 <http://www.verisign.co.jp> などが、個人ユーザ向けに認証サービスを行っています。それ以外でも、電子署名法の施行を受け、今後は自社で運営する認証局や地域コミュニティや行政機関などからも公開鍵証明書が発行されるようになると考えられます。

6.1 電子メールで S/MIME を使うための準備

1) 公開鍵証明書の取得

日本ベリサインの Web サイト

<https://digitalid.verisign.co.jp/browser/client/index.html>

にアクセスします。「米国ベリサイン」を選んで、案内にしたがって、

<http://digitalid.verisign.co.jp/client/browser/>

に移ります。

そのページで"Enroll Now"をクリックします。

次のページでブラウザの種類を選択し、下の図のようなページに移ります。

The screenshot shows a web browser window displaying the VeriSign enrollment page. The page title is 'VeriSign™ Class 1 Digital ID™ for Microsoft Outlook and Outlook Express'. The main heading is 'Step 1 of 4: Complete Enrollment Form'. Below this, there are several sections with input fields:

- Contents of Your Digital ID™:** A section with two input fields: 'Name in Digital ID:' (with a placeholder 'John Stevens') and 'Your E-mail Address:' (with a placeholder 'john@stevens.com').
- Easy Web Site Registration:** A section with a radio button for 'Include Additional Information?' (set to 'Yes'), a 'Country:' dropdown menu (set to 'Japan'), a 'Zip/Postal Code:' input field (with '154-0504'), a 'Date of Birth:' input field (with a placeholder 'mm-dd-yyyy'), and radio buttons for 'male' and 'female'.
- Challenge Phrase:** A section with an input field for 'Enter Challenge Phrase:' (with a placeholder 'John').

入力は、すべて半角英数字で行います。

Contents of Your Digital ID の
入力

First Name: 「名」を入力します。

Last Name: 「姓」を入力します。

E-mail Address: 「電子メールアドレス」を入力します。

Easy Web site Registration の
入力

Include Additional Information?: で Yes を
選択された場合:

Country: 「Japan」を選択します。

Zip/Postal Code: 「郵便番号」を入力します。

Date of Birth: 「誕生日」を入力します。

male(男性)/female(女性)のいずれかを選
択します。

Challenge Phrase の入力

ここで指定した、Challenge Phrase は証明書
を無効にしたいときなどに、確認されること
になります。

Choose a Full-service Class1 Digital ID, or a 60-day Trial Digital ID の選択

I'd like a one-year, full-service Digital ID for only US\$14.95 per year.:

- ・ 一年間有効のフルサービスになります。
- ・ US\$14.95 のクレジットカード決済となります。
に進みます。

I'd like to test drive a 60-day trial Digital ID for free.:

- ・ 60 日間無料のお試し版になります。
- ・ 破棄、再取得、更新のサービスがありません。
- ・ ネットシュアSM・プロテクション・プランという保証制度の対象外

になります。

に進みます。

Billing Information の入力 (フルサービスを選択の方のみ)

クレジットカードの情報を入力します。

Card Type: 「カードの種類」を選択します。

Card Number: 「カード番号」を入力します。

Expiration Date: 「カードの有効期限」を選択します。

Name on Card: 「カードに登録の名前」を入力します。

- 〒154-0004 東京都世田谷区太子堂 1-4-14 萩籐ビル3階 の場合 -

Street Address: 1-4-24 Taishido

Apartment/Unit Number: Hagitou Bldg 3F

City: Setagaya-Ku Tokyo

State/Province: JP

ZIP/Postal Code: 154-0004

Country: Japan

Option の選択

Internet Explorer の場合

「Microsoft Base Cryptographic Provide v1.0」を選択します。

Netscape Communicator の場合

「512」を選択します。

Additional Security for Your Private Key の選択 (Internet Explorer の場合のみ)

Check this Box to Protect Your Private Key:

チェックボックスをチェックすることにより、秘密鍵にパスワードを設定することができます。

Digital ID Subscriber Agreement の確認

読んで、同意できたら、「Accept」を押します。「Accept」をしなければ、先に進みません。

電子メールアドレスの確認

電子メールアドレスを確認し、「OK」を押します。

秘密鍵へのパスワード設定 (Netscape Communicator の場合のみ)

秘密鍵が生成されます。

Communicator Certificate DB にパスワードを設定します。

申請の終了

下の図のようなページが表示されれば申請終了です。



電子メールを確認します

一時間以内には電子メールが届きます。

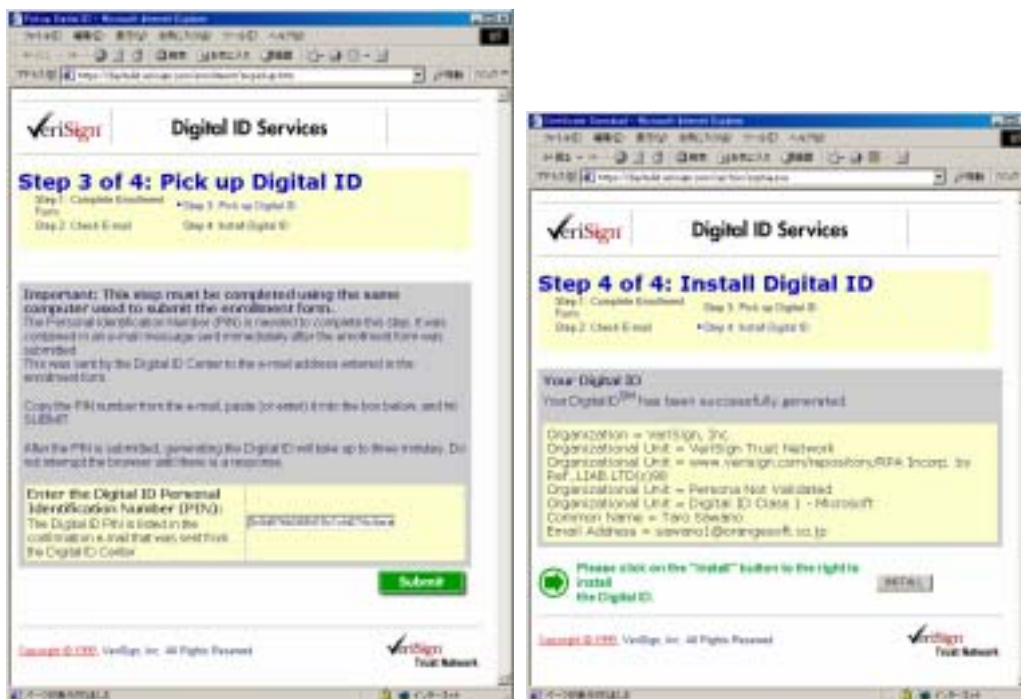


電子メールの内容を確認します。

メールに、以下の2点の記載を確認します。

- ・「https://・・・」と記述された URL
- ・「Your Digital ID PIN IS: …」と記述された PIN 番号

再度、ブラウザを使い Web サイトにアクセスし、デジタル ID をインストールします
で確認した URL にアクセスし、PIN 番号を入力します。「Submit」ボタンを押します。



「INSTALL」ボタンを押すと、あなたのパソコンにデジタル ID が取り込まれます。

[補足]

ここでは、米国ベリサイン社の CA が発行するデジタル ID を取得する手順を説明しましたが、日本ベリサイン発行のデジタル ID を取得するには、デジタル ID の販売代理店

(株)ピーイング

(株)日立情報ネットワーク デジタル ID センター

から購入することができます。その手順については、日本ベリサインの Web サイト

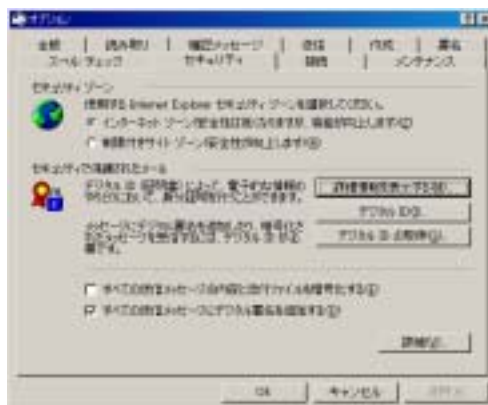
<https://digitalid.verisign.co.jp/browser/client/index.html>

に案内があります。

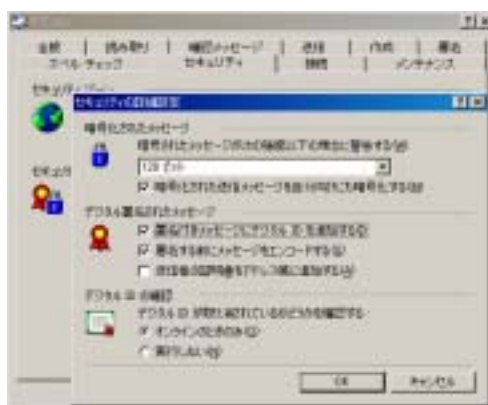
また、Outlook Express のツール / オプションのセキュリティの「デジタル ID の取得」をクリックして表示されるホームページにも、海外の個人ユーザ向けに認証サービスを行っている会社の Web サイトへのリンクが用意されています。

2) S/MIME の設定

下の図のような Outlook Express の「ツール」メニュー / 「オプション」の「セキュリティ」のページで、「デジタル ID」ボタンをクリックすると証明書の一覧が表示され「個人」のページであなたの証明書が確認できます。



「詳細」ボタンをクリックすると表示される下の図のような画面で、S/MIME に関する詳細な指定ができます。



「暗号化されたメッセージが以下の強度以下の場合に警告する」とは、相手によって暗号化の際に利用する共通鍵暗号方式の鍵長が制限されることがあるので、ここで、意図する鍵長以下になってしまうときに、警告を発するようにします。あるいは、受信した暗号メールにつかわれた鍵の長さについても、同様に警告します。

「証明付きメッセージにデジタル ID を追加する」をチェックしておく、電子署名の際に証明書を添付します。送り先の方があなたの証明書を、持っていない場合もあるので、通常はチェックしておいたほうが便利です。

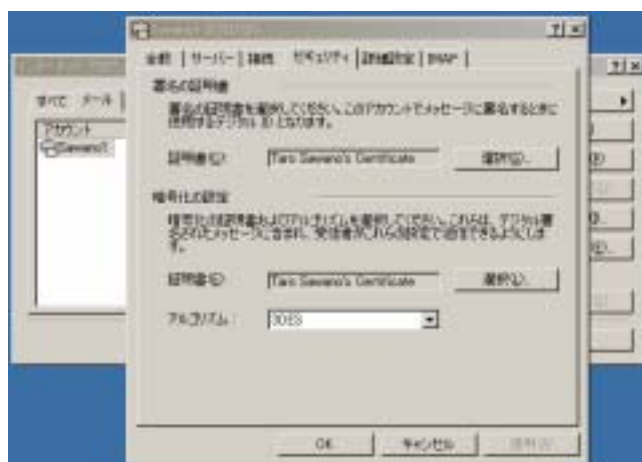
「署名する前にメッセージをエンコードする」は電子署名の際に平文を付けた multipart/signed 形式にせず、平文と署名データ、全てを PKCS#7 のバイナリデータにして、添付ファイルとして送信します。

「送信者の証明書をアドレス帳に追加する」をチェックしておく、他人の証明書が増えていくので、暗号化する際に、新たに証明書を入手する手間がかからないので便利です。

証明書に記載されている有効期限内でも、無効になる場合があるので、「デジタル ID が取り消されているかどうかを確認する」を「オンラインのときのみ」としておけば、リアルタイムな確認ができるの

で安全です。

「ツール」メニュー / 「アカウント」の「プロパティ」ボタンをクリックすると、下の図のような画面が表示されます。この「セキュリティ」のページでも S/MIME の設定があります。



「署名の証明書」では、あなたが、電子署名をする際に使う証明書を選びます。

電子署名のデータの中に、相手が暗号化の際に使ってほしいあなたの証明書と、使ってほしい共通鍵暗号のアルゴリズムを指定できますが、「暗号化の設定」では、その証明書とアルゴリズムを選択します。署名の証明書と暗号化の証明書は同じでもかまいません。

6.2 他人の証明書の収集

1) 電子署名付きのメールを受信する。

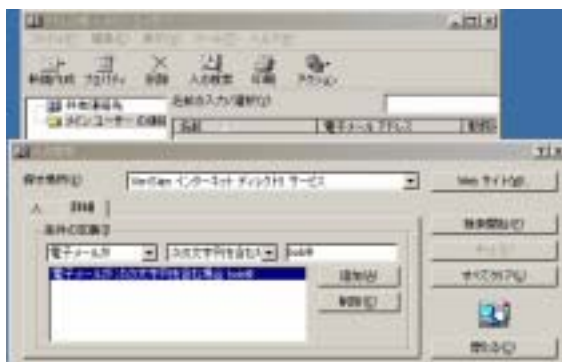
他人の証明書を入手するためのもっとも簡単な方法は、暗号メールを送りたい相手に、電子署名したメールを送ってもらうことです。オプションの指定にもよりますが、通常は電子署名には署名者(すなわち通信相手)の証明書が添付されています。アプリケーションは証明書を自動的に保管しておき、あなたが、必要なときに使うことができます。

2) ディレクトリサーバから検索する

Outlook Express には高性能なアドレス帳が付属しています。このアドレス帳はディレクトリサーバと呼ばれる、インターネット上にあるアドレス帳のようなものにアクセスして、個人の情報を取り出してくることができます。

認証局によっては、このディレクトリサーバに証明書も一緒に保管してサービスしている場合があります。以下では、ディレクトリサーバから証明書を取り出してくる操作について説明します。

- 電子メールアドレスなど、探し出すヒントを指定します、ここでは、電子メールアドレスが、bob@で始まることを指定しています。



- ヒントに従って、見つかった情報が一覧で表示されます。



- 通信相手の証明書を選んで、内容を表示します。

間違いがなければ、「概要」や「全般」のページで「アドレス帳に追加」を実行します。



3) Web サーバで検索する

認証局によっては、この Web サーバ上で証明書の検索を可能にしている場合があります。

例えば、ベリサン社の場合、

<https://onsite.verisign.com/services/VeriSignJapanKKVeriSignClass1CAIndividualSubscriber/client/search.htm>

に、アクセスして、電子メールアドレスか名前を指定して探します。

証明書の内容を確認して、「Download」を指定すると、アプリケーションに応じたダウンロードするデータフォーマットが指定できるので、選択します。「S/MIME Format (Binary PKCS # 7)」を選択してインポートすることも可能です。

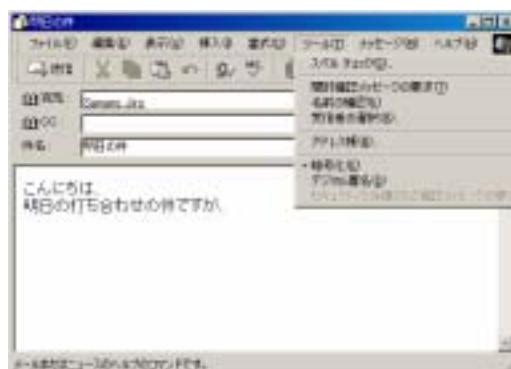
6.3 電子署名を付けて電子メールを送る。

「メッセージの作成」ウィンドウで「ツール」メニュー / 「デジタル署名」を選択します。



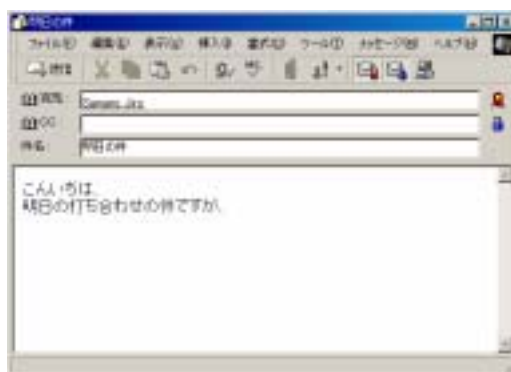
6.4 暗号化して電子メールを送る。

「メッセージの作成」ウィンドウで「ツール」メニュー / 「暗号化」を選択します。



6.5 電子署名と暗号化を組み合わせる

前節の2つを選択しておく、電子署名と暗号化を組み合わせる行えます。

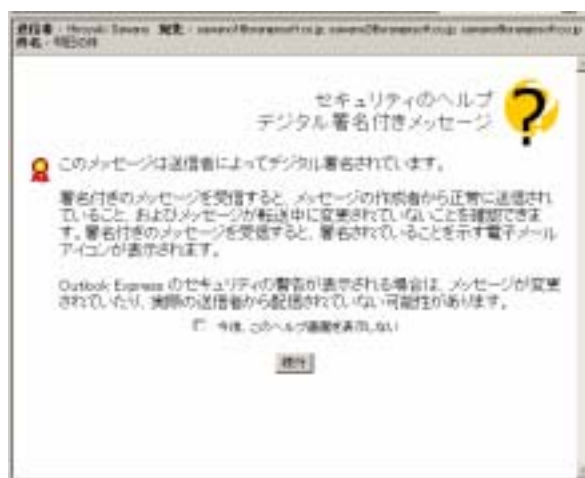


宛先:の横のほうには電子署名、CC:の横のほうには暗号化のアイコンが表示されています。

6.6 電子署名付きメールを受ける

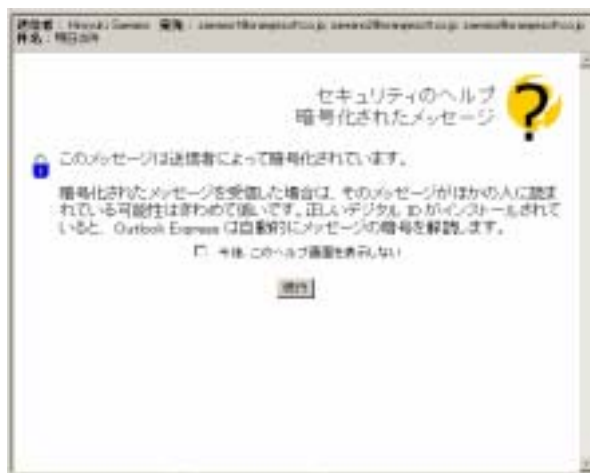
電子署名付きメールを受けると、下の画面のように、電子署名が付いていることがわかります。

「続行」をクリックすると、署名が検証されて、メッセージが表示されます。



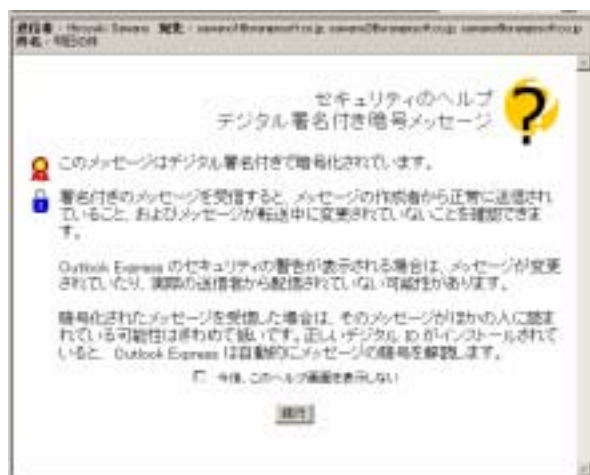
6.7 暗号化されたメールを受ける

暗号化されたメールを受け取ると、下の画面のように、電子署名が付いていることがわかります。「続行」をクリックすると、復号されてメッセージが表示されます。



6.8 電子署名と暗号化されたメールを受ける

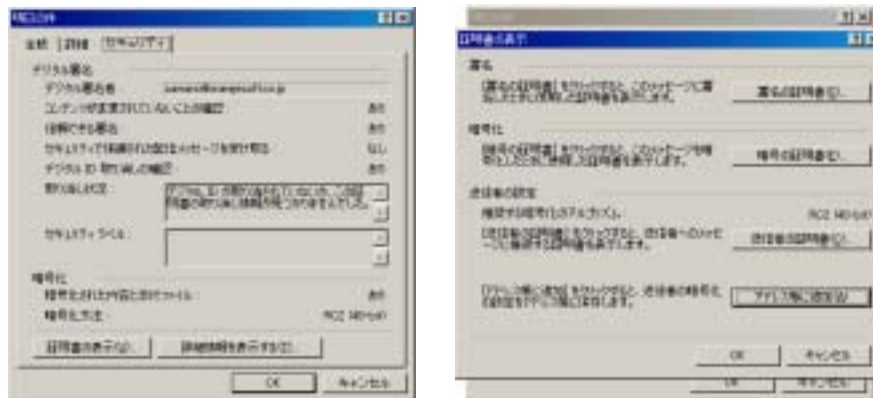
電子署名と暗号化されたメールを受け取ると、下の画面のように、電子署名と暗号化がなされていることがわかります。



「続行」をクリックすると、復号と署名の検証が行われ、メッセージが表示されます。



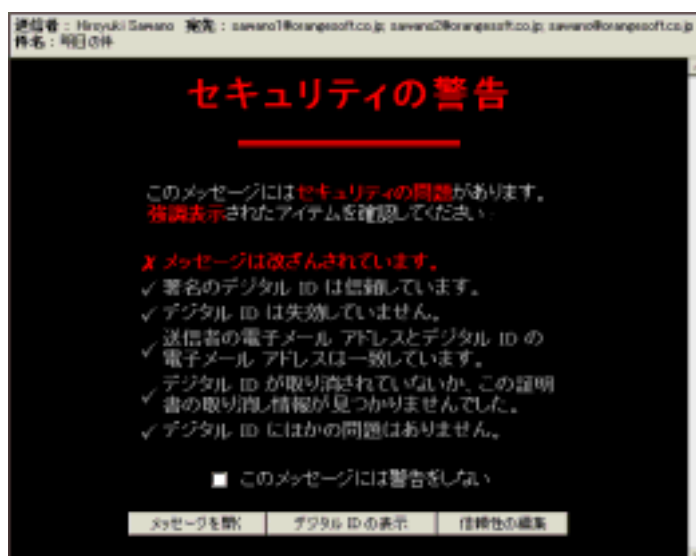
送信者、件名のところに表示されている電子署名または暗号化のアイコンをクリックすると、セキュリティに関する情報が表示されます。利用された暗号のアルゴリズムなどが確認できます。下の図では RC2(40 ビット)となっています。



「証明書の表示...」をクリックすると表示される右の画面では、送信者の証明書を確認したり、証明書を「アドレス帳」に追加したりすることができます。

6.9 不正なメールを受けると

不正なメールを受けた場合、「続行」ボタンを押した後などに、下の図のような画面になります。この例では、メッセージに改ざんがあったことが告げられています。



6.10 証明書の管理

Outlook Express で使われる、証明書は、「ツール」メニュー / 「オプション」の「セキュリティ」ページの「デジタル ID」をクリックして表示される、下のような画面で確認できます。

「個人」のページで表示されるの証明書が、あなたの証明書です。

「ほかの人」のページには、通信相手の証明書が表示されます。

「中間証明機関」のページには、認証パスが 2 階層以上の場合、ルートの下に位置する認証局の証明書が表示されます。

「信頼されたルート証明機関」のページには、ルート認証局の証明書が表示されます。



個々の証明書について、以下のような情報が確認できます。

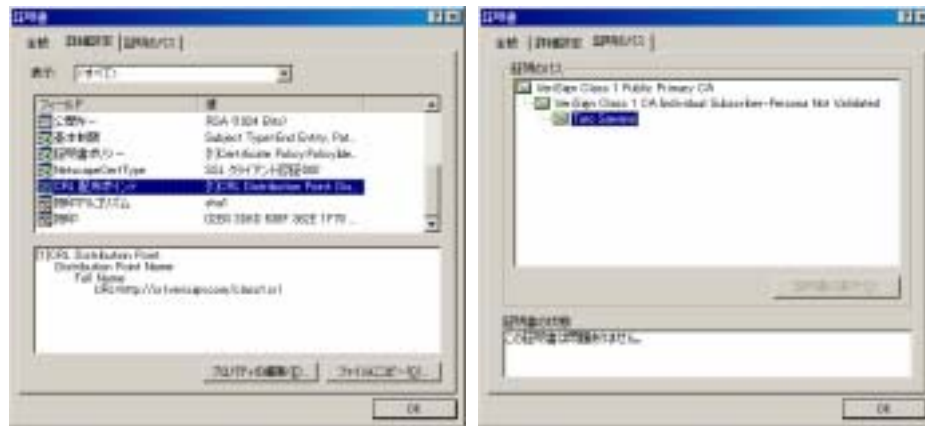
「全般」のページでは、証明書の有効性などが表示されています。

「詳細設定」のページでは証明書の各項目が、項目(フィールド)名とその値とを対応付けて表示されています。



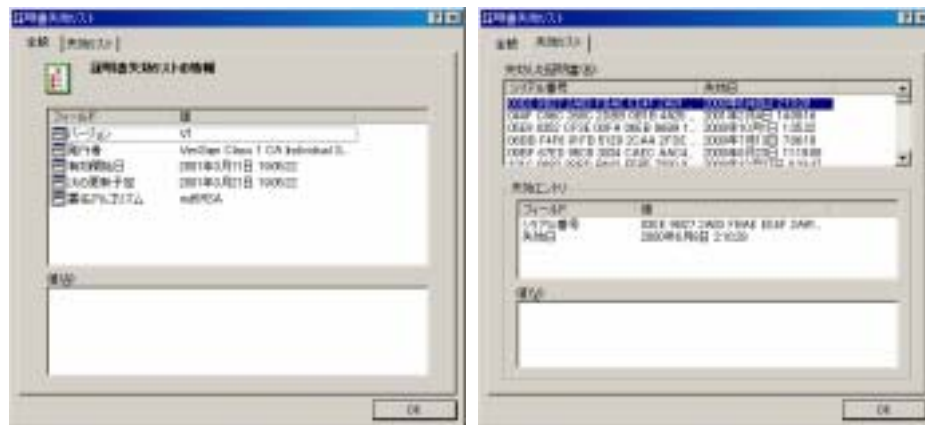
X.509V3 拡張については、アイコンで重要であるか非需要であるかがわかるようになっています。

「証明のパス」のページでは、認証のパスの階層構造が確認できます。



6.11 CRL (証明書失効リスト)

ダウンロードしたCRLのファイルを表示すると、下の図のように発行した日付や、失効した証明書のシリアル番号などが表示されます。



CRLはエクスプローラの右コンテキストメニューの「CRLのインストール」を選択することで、インポートされます。

7 電子メールソフト Netscape Messenger で S/MIME を使う

7.1 電子メールで S/MIME を使うための準備

4) 公開鍵証明書の取得

Microsoft Outlook Express の場合と同様の操作であなたの証明書を用意します。

あなた自身の証明書はメニューの「セキュリティ」の「証明書 / 本人」のページで確認できます。



「表示」ボタンをクリックすると、下の図のように証明書の詳細情報が確認できます。

「確認」ボタンをクリックすると、証明書の有効性が確認できます。



5) S/MIME の設定

S/MIME に関する設定は「セキュリティ」の「Messenger」のページで行います。



「S/MIME 暗号の選択」をクリックして表示される画面では、暗号化の際に使う共通鍵暗号方式を選択できます。

7.2 他人の証明書の収集

1) 電子署名付きのメールを受信する。

Microsoft Outlook Express と同様です。

2) ディレクトリサーバから検索する

「セキュリティ」の「証明書 / 他人」のページで行います。「ディレクトリ検索」ボタンをクリックして表示される画面でディレクトリサーバを選択し、通信相手のメールアドレスを指定します。ディレクトリサーバに相手の証明書が存在すれば、自動的にインポートされ、一覧に追加されます。

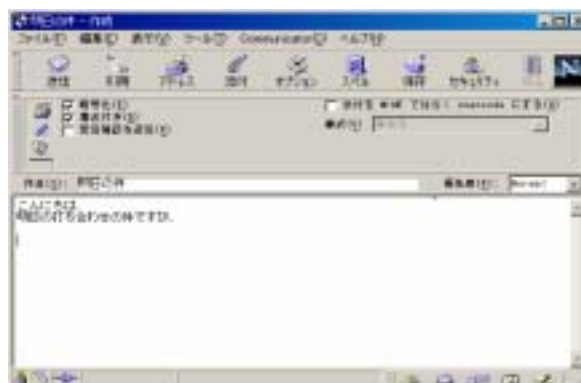


3) Web サーバで検索する

Microsoft Outlook Express と同様です。

7.3 電子署名を付けたり、暗号化をして電子メールを送る。

メッセージの作成ウィンドウで「暗号化」や「署名付き」をチェクします。



7.4 電子署名付きメールを受ける

メッセージ本文を表示するウィンドウの右上に「署名付き」のマークが表示されます。



7.5 暗号化されたメールを受ける

メッセージ本文を表示するウィンドウの右上に「暗号化」のマークが表示されます。



7.6 電子署名と暗号化されたメールを受ける

メッセージ本文を表示するウィンドウの右上に「暗号化と署名付き」のマークが表示されます。



マークをクリックすると、セキュリティに関する情報が表示されます。利用された暗号のアルゴリズムなどが確認できます。下の図では RC2(40 ビット) となっています。

「表示 / 編集」ボタンをクリックすると、証明書の詳細が確認できます。



7.7 不正なメールを受けると

セキュリティ上の問題があるようなメールを受けると、下の図のような画面になります。



セキュリティ・マークをクリックすると、どこに問題があるのかがわかります。

この場合では、メッセージが改ざんされたようなメールだったようです。



7.8 証明書の管理

前述の「ディレクトリサーバから検索する」で説明したように、「セキュリティ」の「証明書 / 他人」のページで、証明書が確認できます。

また、認証局の証明書は「セキュリティ」の「証明書 / 署名者」で確認できます。



8 電子メールソフト Winbiff で S/MIME を使う

(株)オレンジソフトの電子メールソフト「Winbiff」は、アドインソフト「S/Goma」と合わせて使うことで、S/MIME のメールメッセージを扱えるようになります。

(株)オレンジソフト <http://www.orangesoft.co.jp>

(株)オレンジソフトの製品情報のページ <http://www.orangesoft.co.jp/products.html>

8.1 電子メールで S/MIME を使うための準備

1) 公開鍵証明書の取得

Winbiff での証明書の取得は、他の 2 つのように、Web サーバにアクセスリアルタイムにサービスを受けるのではなく、電子メールを用いて、要求と応答と言う形となります。

くりかえしますが、利用者は公開鍵を認証局に提出して、認証局によって電子署名された証明書を発行してもらう必要があります。

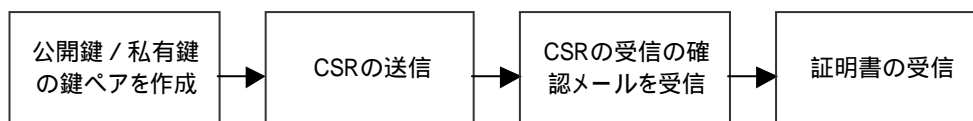
証明書発行を依頼することを (Certificate)Signing Request といいます。Signing Request のためのデータフォーマットは PKCS#10 と呼ばれるものです。PKCS#10 は公開鍵や、電子メールアドレスや名前等の個人の情報などからなります。

認証局では、CSR を受け取ったら、その CSR がそこに示されている個人のものであることを確認したのち、公開鍵と個人の情報を含むデータに、認証局の秘密鍵で電子署名をします。これが証明書です。

暗号文を送る場合は、送り先の公開鍵が必要となりますが、送り先の相手の証明書を入手することで、相手の公開鍵を得ることが出来ます。

証明書の信頼、つまり、公開鍵が確かにその持ち主とされている人のものであることは、その証明書についての認証局の電子署名を検証することにより確認できます。

この節では、Winbiff を用いて CSR を作成し、証明書を取得するまでの流れを説明します。



鍵ペアの作成と CSR の送信

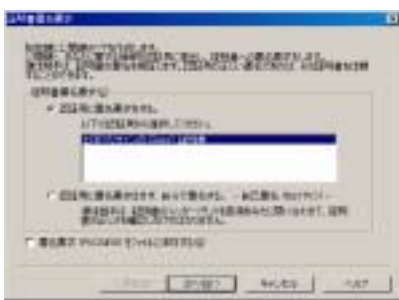
「環境設定 / 暗号」画面で「鍵ペアの作成」を選んで、操作を進めます。



「パスワードの入力」画面

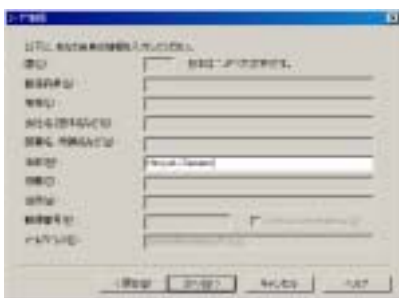


「認証局の選択」画面

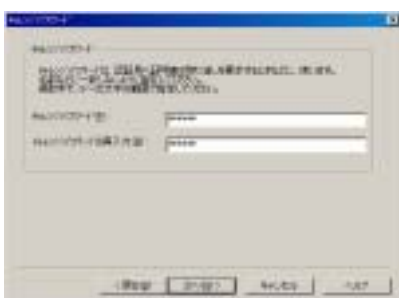


「ユーザ情報の入力」画面

認証局に送る CSR の一部である、個人情報を入力します。



「チャレンジパスワードの入力」画面



「ユーザ情報の確認」画面

「ユーザ情報の入力」画面での入力内容を確認します。

「乱数の種の生成」画面

鍵ペアを作成するために必要な、乱数の種をキーの任意な押下によって得ます。



[CSR の送信]

以上の操作が完了すると、選択した認証局のメールアドレスに対し、メールを送信します。オフラインの場合は Outgoing に保管されます。



CSR 受信確認のメッセージ



証明書受信

認証局からのメールで証明書を受信したら、メニュー「暗号」/「復号」を実行します。証明書 DB にインポートされ、私有鍵と対応付けて管理されます。



2) S/MIME の設定

「環境設定 / 暗号」画面で「セキュリティ設定」を選んで、操作を進めます。



8.2 他人の証明書の収集

1) 電子署名付きのメールを受信する。

Microsoft Outlook Express や Netscape Messenger と同様です。

2) ディレクトリサーバから検索する

現行の S/Goma V1.01 ではディレクトリサーバへのアクセスはサポートされていません。

3) Web サーバで検索する

Web ブラウザを使って検索。ダウンロードした証明書ファイルをインポートします。

インポートするためには、「環境設定 / 暗号」画面で「証明書一覧」をクリックして表示される画面で、「インポート」をクリックしてファイルを指定します。



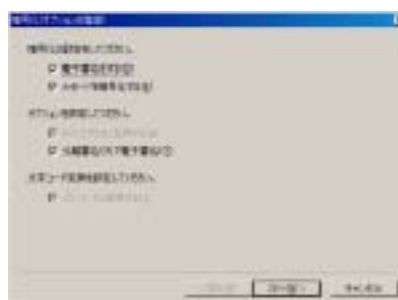
8.3 電子署名を付けたり、暗号化をして電子メールを送る。

メッセージの作成ウィンドウで「暗号」メニューの「暗号化 + 電子署名」や「電子署名」をチェックします。

また、「送信の確認」ウィンドウで「暗号化 + 電子署名」や「電子署名」をチェックすることも可能です。



オプションを再度確認します。



暗号化に使う証明書を確認します。



電子署名をするために、私有鍵のパスフレーズを入力します。

あなたの証明書が複数ある場合、ここで、署名に使う証明書

を変更することも可能です。



送信する前に、送信するメールの内容を確認します。



8.4 電子署名付きメールを受ける

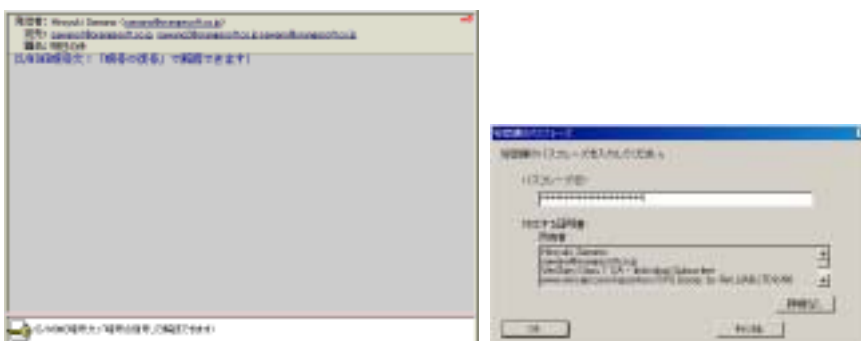
下の図のように添付ファイルのウィンドウのところで電子署名があることがわかります。「暗号」メニューの「復号」を選ぶがアイコンをクリックすると、署名の検証が行われます。



8.5 暗号化されたメールを受ける

下の図のように添付ファイルのウィンドウのところでメッセージが暗号化されておりことがわかります。

「暗号」メニューの「復号」を選ぶがアイコンをクリックすると、パスワードを入力して復号されます。



8.6 電子署名と暗号化されたメールを受ける

暗号化されたメールを受けたときと同じようにアイコンが表示されます。「復号」をすると、下の図のような画面が表示され、セキュリティ情報を確認できます。



9 S/MIME のメールメッセージ

9.1 標準仕様

1) 基本となる仕様

「RFC2311 "S/MIME Version 2 Message Specification"」

「RFC2312 "S/MIME Version 2 Certificate Handling"」

2) RSA 暗号アルゴリズム

「RFC2313 "PKCS #1 : RSA Encryption Version 1.5"」

3) 証明書署名要求

「RFC2314 "PKCS #10 : Certification Request Syntax Version 1.5"」

認証局への証明書署名要求データのフォーマットについて記述しています。

4) 暗号メッセージ

「RFC2315 "PKCS #7 : Cryptographic Message Syntax Version 1.5"」

暗号データのフォーマット。電子署名、暗号化、電子署名+暗号化、証明書、CRL(若干)のデータフォーマットについて記述されています。

5) クリア電子署名の MIME ヘッダについて

「RFC 1847 "Security Multiparts for MIME"」

6) CRL

「RFC1422 "Privacy Enhancement for Internet Electronic Mail : Part II: Certificate-Based Key Management"」

7) PKCS

もともと、S/MIME は米国の RSA Data Security Inc.が中心なって開発された、電子メールの暗号プロトコルです。そのため、S/MIME で用いられる暗号文のデータフォーマットは PKCS(Public Key Crypt System)と呼ばれる RSA Data Security Inc.が開発して仕様を基本にしているのです。

9.2 MIME ヘッダ

S/MIME のメールメッセージは

電子封書、電子署名のデータを PKCS#7 に規定されたフォーマットにします。

のデータを Base64 にエンコードして、RFC2311 に規定されている、MIME ヘッダをつけた添付ファイルにします。ただし、現在、流通しているアプリケーションでは、ほとんどが、Internet Draft の段階で定義されていた MIME ヘッダを使っています。

1) 電子封書または、電子署名を含む電子封書

RFC

Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

Internet Draft

Content-Type: application/x-pkcs7-mime; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

2) 電子署名

RFC

Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

Internet Draft

Content-Type: application/x-pkcs7-mime; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

3) クリア電子署名

RFC

Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

Internet Draft

Content-Type: application/x-pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

4) 証明書署名要求

RFC

Content-Type: application/pkcs10; name=smime.p10
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p10

Internet Draft

Content-Type: application/x-pkcs10; name=smime.p10
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p10

5) 証明書

RFC

Content-Type: application/pkcs7-mime; smime-type=cert-only; name=smime.p7c
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7c

Internet Draft

Content-Type: application/x-pkcs7-mime; name=smime.p7c
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7c

9.3 電子署名の例

1) クリア電子署名 multipart/signed の場合

To: Hiroyuki Sawano <sawano@orangesoft.co.jp >
 From: Taro Sawano <sawano1@orangesoft.co.jp >
 Subject: Digital Sign
 MIME-Version: 1.0
 Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1;
 boundary="-----ms8B7876C5A4971B52E1D24E61"

This is a cryptographically signed message in MIME format.

-----ms8B7876C5A4971B52E1D24E61
 Content-Type: text/plain; charset=iso-2022-jp
 Content-Transfer-Encoding: 7bit

こんにちは、
 明日の打ち合わせの件ですが、(JIS コード)

-----ms8B7876C5A4971B52E1D24E61
 Content-Type: application/x-pkcs7-signature; name="smime.p7s"
 Content-Transfer-Encoding: base64
 Content-Disposition: attachment; filename="smime.p7s"
 Content-Description: S/MIME Cryptographic Signature

MIIOQDwYJKoZihvcNAQcCoiIQADCCD/wCAQExCzAJBgUrDgMCGGUAMAsGCSqGSIb3DQEHAaCC
 Dn0wggnHMIIJMKADAgECAhA4kcRP4QGC7RTq2FZKZF0TMA0GCSqGSIb3DQEBAUAMGixETAP

(中略)

MjQ2MzRaMB4GCSqGSIb3DQEJDzERMA8wDQYIKoZihvcNAwICASgwDQYJKoZihvcNAQEBOAE
 QBOPytJm3nmFp6lYXCZHIDyG9VULK8hhgyU0vAHELLV/9Grx4+5fvbeerP/YXSmox8G6CTw
 J7/hi+ooJvN4cuM=

-----ms8B7876C5A4971B52E1D24E61--

2) PKCS#7 signedData の場合

To: Hiroyuki Sawano <sawano@orangesoft.co.jp >
 From: Taro Sawano <sawano1@orangesoft.co.jp >
 Subject: Digital Sign
 MIME-Version: 1.0
 Content-Type: application/x-pkcs7-mime; name="smime.p7m"
 Content-Transfer-Encoding: base64
 Content-Disposition: attachment; filename="smime.p7s"

MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhkiG9w0CBQUAMIAAGCSqGSIb3DQEHAaCAJIAEbkNv
 bnRlbnQlVHlwZTogdGV4dC9wbGFpbG0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluc2VudGVudGVk

(中略)

hvcNAQkEMRIEFE6IM/MZQmTGdlaAG17hE4wDQYIKoZihvcNAQEBOAEQC+f4FYqZiV4QgzS3BAB
 YpazDyMF61HtuVOU5rZ9IguQzFB/nH6K+G0cF1+hAmaGdpFkC3lCVh0Py2XnMPg5TvoAAAAAAAAAA
 AA==

9.4 暗号化

To: Hiroyuki Sawano <sawano@orangesoft.co.jp >
 From: Taro Sawano <sawano1@orangesoft.co.jp >
 Subject: Digital Envelop
 MIME-Version: 1.0
 Content-Type: application/x-pkcs7-mime; name="smime.p7m"
 Content-Transfer-Encoding: base64
 Content-Disposition: attachment; filename="smime.p7m"
 Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxgc8wgcwCAQAwDjBiMREwDwYDVOQHEwhJbnRlcm5ldDEX
 MBUGA1UEChMOVmVyaVNpZ24slEluYy4xNDAYBgNVBAsTK1ZlcmItaWduENsYXNzIDEGQ0Eg

(中略)

Bh0SaWCqCd9p0OpbNnHyi2G3tvMEuC74u+nvWjZT8fXeBAGgdXGjYOOBzQQUiUHE0vqb2InIA
 AAAAAAAAAAAAA

9.7 証明書の添付

1) 署名要求の応答として、認証局から送られてきたメール

From: smime-info@verisign.co.jp
 To: sawano@orangesoft.co.jp
 Subject: Your VeriSign Class 1 S/MIME Digital ID
 Errors-to: errors@verisign.co.jp
 MIME-Version: 1.0
 Content-Type: multipart/mixed;
 boundary="=====
 X-winbiff-flags: Seen

-----VeriSignOnlineCA_926060059_
 Content-Type: application/x-pkcs7-mime; name="verisign.p7c"
 Content-Transfer-Encoding: base64
 Content-Disposition: attachment; filename="verisign.p7c"

MIIH4gYJKoZlHvcNAQcColIH0zCAAgEBMQAwCwYJKoZlHvcNAQcBoIAwggRzMIID
 3KADAgECAhBSHxudA47yQAkoRWHwCk0MA0GCSqGSIb3DQEBAUAMIG1MRwwGgYD
 (中略)
 nBBRt38GgTb5UzC1d3ltwRuluUEWzTYSgqFzdIPGMNwLiHsVRQ+8lCnL0Hzjk4b
 htMvd1ekbp84WuohKzi2m7b9OchVlVJ0rJJxfqjgi2D/bjCCgfyZg4lpzaZ1GwBz
 AAAXAAAA

-----VeriSignOnlineCA_926060059_
 Content-Type: text/plain; charset=iso-2022-jp
 Content-Transfer-Encoding: 7bit

この度は、ベリサインの S/MIME 用デジタル ID をお申し込み頂きありがとう
 ございました。(JIS コード)

(中略)

VeriSign Digital ID Center
 id-center@verisign.co.jp

-----VeriSignOnlineCA_926060059_
 Content-Type: text/plain; charset=iso-2022-jp
 Content-Transfer-Encoding: 7bit

デジタルID加入契約
 デジタルID (証明書)を申請し、承認し、または使用する前にこの加入契約を必
 ずお読み下さい。もし、この 加入契約の規定に同意しない場合は、デジタルID
 (証明書)の申請、承認または使用をしないで下さい。

(後略)

-----VeriSignOnlineCA_926060059_--

2) PKCS#7 証明書 複数の証明書を 1 つのファイルにいれることが可能です。

From: Taro Sawano <sawano1@orangesoft.co.jp>
 Mime-Version: 1.0
 Content-Type: MultiPart/Mixed; Boundary="-----971840212-66036305"
 X-winbiff-flags: Seen

-----971840212-66036305
 Content-Type: text/plain; charset=iso-2022-jp

こんにちは、私の証明書です。(JIS コード)

-----971840212-66036305
 Content-Transfer-Encoding: Base64
 Content-Type: application/pkcs7-mime; name="sawano1.p7c"
 Content-Disposition: attachment; filename="sawano1.p7c"

MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCBHQwggPdoAMCAQICED8
 IXamPnts5jp/o62cvbMwDQYJKoZlHvcNAQEEBQAwbUxHDAaBgNVBAoTE1ZlcmliTtaWdulEph
 (中略)
 ZdIPGMNwLiHsVRQ+8lCnL0Hzjk4bhtMvd1ekbp84WuohKzi2m7b9OchVlVJ0rJJxfqjgi2D/
 bjCCgfyZg4lpzaZ1GwBzAAAXAAAAAAAAA==

-----971840212-66036305—

3) DER エンコードされた X.509 証明書 の形式

From: Taro Sawano <sawano1@orangesoft.co.jp>
Mime-Version: 1.0
Content-Type: MultiPart/Mixed; Boundary="-----971840212-66036305"
X-winbiff-flags: Seen

-----971840212-66036305
Content-Type: text/plain; charset=iso-2022-jp

こんにちは、私の証明書です。(JIS コード)

-----971840212-66036305
Content-Transfer-Encoding: Base64
Content-Type: application/ pkix-cert; name="sawano1.cer"
Content-Disposition: attachment; filename=" sawano1.cer"

MIAGCSqGSib3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCBHQwggPdoAMCAQICED8
IXamPnts5jp/o62cvbMwDQYJKoZIhvcNAQEEBQAwgbUxHDAaBgNVBAoTE1Zlcm1TaWdulEph

(中略)

ZdIPGMNWLiHsVRQ+8ICnL0Hzjk4bhtMvd1ekbp84WuohKzi2m7b9OchVlVJ0rJJxfqjgi2D/
bjCCgfyZg4lpzaZ1GwBzAAAxAAAAAAAAAA==

-----971840212-66036305—

10 証明書の実例

米国 VeriSign 社が発行したエンドユーザ向けの証明書の中身を下の表に示します。

項目	値(例)または説明
証明書フォーマットのバージョン	2
証明書のシリアル番号	25 F3 74 4F 14 10 11 C6 0A 36 51 1A AC 48 19 F7
デジタル署名のアルゴリズム	md5withRSAEncryption
証明書発行者(認証局)名 DN	CN = VeriSign Class 1 CA Individual Subscriber-Persona Not Validated OU = www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98 OU = VeriSign Trust Network O = VeriSign, Inc.
有効期限	開始 2001 年 3 月 9 日 9:00:00 終了 2001 年 5 月 9 日 8:59:59
証明書所有者名 DN	E = sawano1@orangesoft.co.jp CN = Taro Sawano OU = Digital ID Class 1 - Microsoft OU = Persona Not Validated OU = www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98 OU = VeriSign Trust Network O = VeriSign, Inc.
証明書所有者名の公開鍵情報	
アルゴリズムの ID	RSA(1024 ビット)
公開鍵	30 81 89 02 81 81 00 B4 B6 30 57 A5 57 C9 40 9C B4 DA 47 50 5B D3 13 6F 30 E4 1E 6F 36 97 5D 59 73 1A 05 67 D5 AC FF F1 06 86 4D EB 63 2F 57 70
X.509 V3 拡張	
基本制限	Subject Type=End Entity Path Length Constraint=None
証明書ポリシー	PolicyIdentifier=2.16.840.1.113733.1.7.1.1 [1,1]Policy Qualifier Info: Policy QualifierInternet Draft=CPS Qualifier: https://www.verisign.com/CPS [1,2]Policy Qualifier Info: Policy QualifierInternet Draft=ユーザ通知 Qualifier:

	<p>Notice Reference: Organization=VeriSign, Inc. Notice Number=1 Notice Text=VeriSign's CPS incorp. by reference liab. ltd. (c)97 VeriSign</p>
キー使用法	Digital Signature , Key Encipherment(A0)
Netscape Cert Type	SSL クライアント認証(80)
CRL 配布ポイント	Distribution Point Name: Full Name: URL=http://crl.verisign.com/class1.crl
署名	
アルゴリズムの ID	md5withRSAEncryption
署名データ	49 AB 1D AC 7A BF 6D 54 09 E0 53 0C DB CF 53 8E 32 7D 0E 1E EB 17 F9 A6 BC 5B 12 D2 8A 6D C3 DE CC 7C 4B 47 A9 20 DA 31 3F B9 C6 50 46 26 31 36

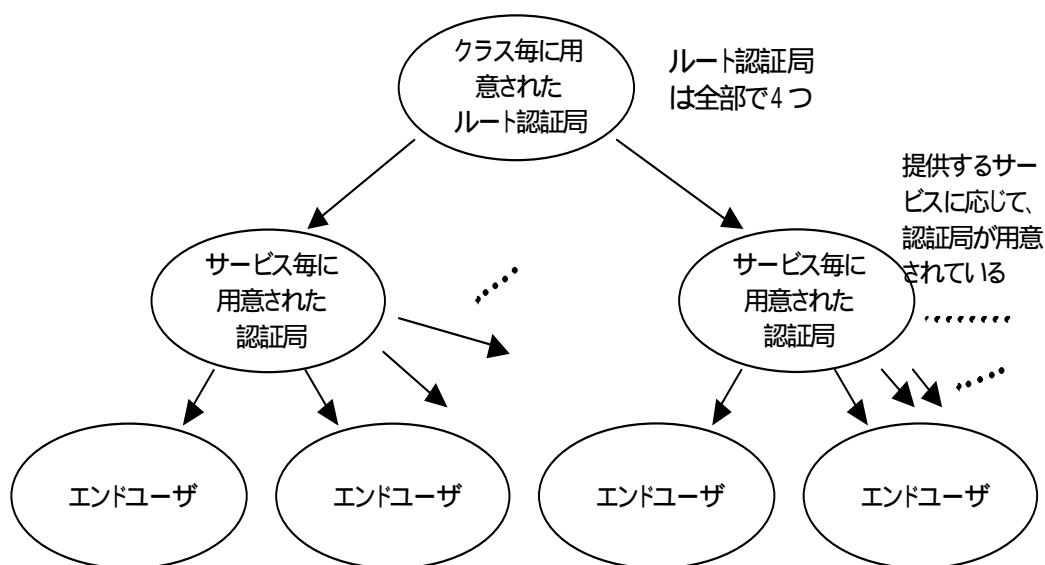
11 認証パスの実例

階層形モデルのCAの構造をもつ認証パスの例として、ベリサイン社の構造を以下に示します。

ベリサイン社では、セキュリティのレベルの応じて、クラス1～4の4つのルート認証局が存在します。

それぞれのルート認証局を根として以下のような階層構造が実現されています。

証明書を発行する際の本人確認の仕方などによって、Class1(軽い)～4(重い)に分れています。例えば、Class1では受信したメール中の送信元メールアドレスと認証データ中のメールアドレスが一致していれば、OKとなります。



ルート証明書の所持者の X.500 名前

OU = Class 1 Public Primary Certification Authority
 O = VeriSign, Inc.
 C = US
 OU = Class 1 Public Primary Certification Authority
 O = VeriSign, Inc.
 C = US

中間の CA の証明書の所持者の X.500 名前

CN = VeriSign Class 1 CA - Individual Subscriber
 OU = Terms of use at <https://www.verisign.co.jp/RPA> (c) 98
 OU = VeriSign Trust Network
 O = VeriSign Japan K.K.

エンドユーザの証明書の所持者の X.500 名前

E = sawano@orangesoft.co.jp
 CN = Hiroyuki Sawano
 OU = Digital ID Class 1 - SMIME Orangesoft Inc./Winbiff/2.1
 OU = www.verisign.com/repository/CPS Incorpor. by Ref., LIAB.LTD(c)96
 OU = VeriSign Class 1 CA - Individual Subscriber
 O = VeriSign Japan K.K.
 C = JP

VeriSign 社の 認証パスの階層の詳細は VeriSign 社の Web サイト「Repository / VeriSign PKI Hierarchy」

<http://www.verisign.com/repository/hierarchy/hierarchy.pdf>

を参照してください。

12 ルート認証局の証明書について

1) 信頼の基本

利用者は、まず、第一にルート認証局の証明書を絶対的に信用することにより、信頼関係が成り立ちます。すなわち、またがった証明書をルート認証局のものであると判断した場合、信頼関係が台無しになってしまいます。

2) バンドルされて出荷

ルート認証局の証明書は Web ブラウザや電子メールのソフトウェアなどに予めバンドルされた形で提供されることが多いです。

例えば、Microsoft Outlook Express では Internet Explorer と一体となって、以下のようにたくさん



3) インポートの際、注意すること

新たなルート認証局の証明書をアプリケーションで利用する場合、インポートと呼ばれる操作を行います。前述のように、ルート認証局の証明書は慎重に扱わなければなりません。インポートの際には、証明書の拇印を別の手段で入手しておき、インポートされる証明書と照らし合わせて、一致することを確認しましょう。

拇印には SHA.1 による 20 バイトのものと MD5 による 16 バイトのものがあるので注意しましょう。



13 参考文献

「デジタル署名と暗号技術」

ウォーウィック・フォード+マイケル・バウム 著、山田慎一郎 訳、日本ペリサイン(株) 監修
出版社 (株)ピアソン・エデュケーション

「PKI 公開鍵インフラストラクチャの概念、標準、展開」

カーライル・アダムス+スティーブ・ロイド 著、鈴木優一 訳
出版社 (株)ピアソン・エデュケーション

「PGP 暗号メールと電子署名」

Simon Garfinkel 著、山本和彦 監訳、(株)ユニテック 訳
出版社 (株)オライリー・ジャパン

「UNIX & インターネットセキュリティ」

Simon Garfinkel + Gene Spafford 著、山口英 監訳、谷口功 訳
出版社 (株)オライリー・ジャパン

「E-Mail セキュリティ」

Bruce Schneier 著、力武健次 監訳、道下亘博 訳
出版社 (株)オーム社

月刊 ドクター・ドブス・ジャーナル 1998.2 月号

特集 「暗号化技術が拓くインターネット新時代」

出版社 (株)翔泳社

IPA インターネット・セキュリティ関連の RFC <http://www.ipa.go.jp/security/rfc/RFC.html>

セコム情報システム(株) ネットワーク・セキュリティ読本

<http://www.sisnet.or.jp/sis/dokuhon/index.html>

電子商取引推進協議会 (ECOM) 暗号利用技術ハンドブック

http://www.ecom.or.jp/qecom/about_wg/wg05/cr-swg/code-index.html

PKIX Working Group <http://www.imc.org/ietf-pkix/>

S/MIME Working Group <http://www.imc.org/ietf-smime/>

電子メールのセキュリティ
S/MIME を利用した暗号化と電子署名

情報処理振興事業協会
セキュリティセンター

〒113-6591 東京都文京区本駒込 2-28-8
文京グリーンコート
センターオフィス 16F
FAX:03-5978-7518
e-mail: isec-info@ipa.go.jp