インターネットセキュリティ

最近では ADSL や CATV インターネットの利用など、学校内外においてもインターネットに常時接続される環境が一般的になってきた。このため、外部から自分のパソコンにアクセスされてしまう例も珍しくなくなってきている。個人のパソコンに侵入されることも困るが、学校のパソコンにアクセスされ、生徒の個人データが外部に漏れるようなことはあってはならない。そのためには、セキュリティに関する知識を十分に身に付け、インターネットからの脅威に対応するための手段を整えておく必要がある。そこでインターネットセキュリティに関して詳しく述べていく。

Ⅰ　攻撃パターンを知る

セキュリティ対策の第一歩は「敵を知る」ことである。クラッカーと呼ばれる攻撃者がどのようにネットワークセキュリティを侵害し、それによってどのような被害を与えるのか。セキュリティ対策とは、クラッカーの侵害行為に対して予防線を張ることといえる。侵害の手法はパターン化しており、そのパターンを理解し、ターゲットにされないようにすることが大切である。

インターネットに接続している限り、クラッキング（クラッカーによる侵害行為）の対象になるのは仕方がない。クラッカーはインターネットに接続するホストを無差別にターゲットにしている。つまり、インターネットに接続するホストから幅広く調査して、適当なものがあればそれを攻撃対象にする。自分のＰＣをそのまま使ってクラッキングするクラッカーはおらず、第３者のホストを「踏み台」にして最終ターゲットを攻撃する。踏み台とは、クラッカーに操られて攻撃に加担するホストのことで、ターゲットとは、こうした踏み台に使うホストのことである。

１　ＩＰアドレスを収集

インターネットで通信するためにはグローバル IP アドレス（以下 IP アドレス）が必要となる。クラッキングのほとんどは、インターネットを介した通信として行われるため、IP アドレスはクラッカーにとって非常に重要な情報である。約４３億個の IP アドレスのうち、日常的に稼動している IP アドレスを収集することがクラッキングの最初の段階となる。

有効な IP アドレスは、様々な方法で収集される。最も頻繁に採られるのは、ICMP エコーを使った方法である。ICMP（Internet Control Message Protocol）とは、パケット配送を担当する IP と同じネットワーク層に属するプロトコルであり、IP レベルで通信が可能かどうか、可能でなければどんな状況なのかを報告する働きをする。そのうち ICMP エコーは、通信先のホストが稼動しているかどうか、稼動している場合どのくらい応答時間がかかるかを調べるものである。これは、「ping」コマンドで送ることができる。あるホストに対して ping を発行すると、IP レベルでホストが稼動しているかどうかを識別できる。稼動していれば応答時間とともに ICMP エコー応答のパケットが戻ってくるし、稼動していなければエラーメッセージが表示される。

ping は基本的に１台のホストに対して発行されるが、専用ツールを使えば連続したアドレス範囲で ping を送ることもできる。さらに、掲示板サイトなどに不用意に表示された IP アドレスも収集の対象になる。掲示板の書き込みから、ユーザが常時接続していることや、あまりネットワークに詳しくなさそうだということがわかれば「踏み台にしてやろう」と考えるクラッカーがいるのである。

２　ポートスキャン

ICMP エコーを使ってホストの稼働状況がわかっても、まだ IP レベルで接続できることが判明しただ

けである。ある住所を入手して行ってみたら、そこに家が建っていることがわかったのと同じ程度である。次に必要な作業は、そのホスト（家）へ侵入する入口を探すことである。ネットワーク通信では、すべて「ポート」にパケットを受け渡すことで実現している。ポートにパケットを受け渡すのは TCP と UDP（トランスポート層）であり、ポートには 0～65,535 番までの番号が振られている。Web やメールサーバは、このうち 1023 番以下の特定ポート（ウェルノウンポート）を使って、パケットを待ち受けしている。つまり、サーバプログラムは通常、クライアントからの接続要求を受け付けてサービスを提供するため、いつでもポートを開けてパケットの到達を待っていなければならない。そのため公開サーバなど、ネットワーク上の他のホストに対して何らかのサービスを提供するホストは、必ずいくつかのポートを開けていなければならない。この開いているポートを探す行為が「ポートスキャン」である。

ポートスキャンは、ホストの各ポートに順番に接続要求（SYN パケット）を送ることで可能になる。特定のポートでサーバが待ち受けしていれば、その確認（ACK）と、クライアントに対するサーバからの接続要求（SYN）がセットになった「SYN+ACK」パケットが送られてくる。これが戻ってきたら、ポートが開いていることが判断できる。

ポートスキャンは、TCP が通信路であるコネクションを確立する「３ウェイハンドシェイク」を利用している。したがって、ポートスキャンを防御することは、TCP の仕組み上できない。では、コネクションを使わない UDP ではポートスキャンされないかといえば、そうでもない。UDP の通信には３ウェイハンドシェイクはないが、サービスが稼動していなければ即座に ICMP エラーが返される。そこから UDP を使うサーバの待ち受け状態がわかる。

＜ポート番号＞
ビルでイメージする。→　ＩＰアドレスはビルの住所、ポート番号は各部屋番号
ビルの 25 号室（ポート番号 **25**＝SMTP）では手紙を１通ずつ受けたり出したりするサービスを行っている。
ビルの 110 号室（ポート番号 **110**＝POP3）では、誰からの要求によってその人物あてに届いた手紙を一括して送り出すサービスを実施している。

ポート番号は、ネットワーク経由で任意のサービスを受ける際に、そのサービスを識別するために用いられる。
ＩＰアドレスはＩＰが対応するレイヤ３（ネットワーク層）で、ポート番号はＴＣＰ／ＵＤＰが対応するレイヤ４（トランスポート層）で機能する。

＜パケットフィルタリング＞
ビルの部屋なら鍵をかけておかなければ不審者が部屋に入り込んで何か悪さをするかもしれない。
ポートも同様、使用／不使用に関わらず、鍵をかける必要がある。
パケットフィルタリングには、２種類のポリシーベースがある。
「初期状態では全てのパケットを通しておき、必要に応じてパケットをフィルタリングするための規則を設定するという」ポリシーと、「初期状態ではすべてのパケットを通さずに（リジェクトし）、必要なものだけ通すように設定する」というポリシー。現在は後者のポリシーを採用している場合が多い。（デフォルトとなっている）

３　アプリケーションバナーを調査

どんなプログラムにも「バグ」と呼ばれる実装上の不具合がある。そのバグが悪用され、ホストへの侵入を許してしまうことがある。バグがセキュリティホールとなる可能性はきわめて高い。そこでクラッカーは、ポートスキャンで得られた待ち受けポートで稼動するサーバプログラムの種類やバージョン（アプ

リケーションバナーという)を調べる。ここからセキュリティホールがあるかどうかがわかるからである。アプリケーションバナーを見てセキュリティパッチ（バグの修正プログラム）を適用していないプログラムが動作していることがわかれば、そのホストを手中に収めたのも同然である。バッファオーバーフロー攻撃を使って、実際にホストに侵入することができる。

アプリケーションバナーの取得には、リモートログインプロトコルの「Telnet」を使う。Telnet は通常、Telnet サーバ（TCP23 番ポートで待ち受け）に接続して、遠隔のホストからコマンドを送るのに使われる。しかし、Telnet 接続時に別のポート番号を指定すれば、Telnet サーバ以外のサーバにコマンドを送ることができる。

4　バッファオーバーフロー攻撃

ここまでのプロセスは、クラッキングまでの前調査である。実際に何か被害を被るわけではないが、通常の通信にはまったく不要の行為で、明らかにクラッキングの予兆と見ることができる。もし、この段階でセキュリティホールが発見されたら、攻撃を受ける可能性がきわめて高いといえる。

セキュリティホールに対する実際の攻撃には、「バッファオーバーフロー攻撃」がよく使われる。バッファオーバーフロー攻撃とは、プログラムの不具合を利用して OS のメモリをあふれさせたうえ、任意のプログラムを実行することをいう。

バッファオーバーフロー攻撃は、手法としては古典的ともいえる。そのため多くの場合、セキュリティパッチをまめに適用し、セキュリティホールを作らないことで防ぐことができる。

5　踏み台を使った DoS 攻撃

クラッカーが最終的に被害をもたらそうとしているホストは、個人的な思惑によって決められている。（ニュースになるのを期待して世界的に著名なサーバなど）しかし、こうした著名なサーバはきちんとした運用がなされているため、バッファオーバーフロー攻撃が通用しないことが多い。そこで、管理の甘いホストを探しそれを踏み台にして「防ぎようのない」方法で攻撃する。その一つが「DoS 攻撃」である。

DoS とは「Denial of Service」を意味し、「サービス不能」攻撃などと訳される。特定のホストに大量のパケットを送りつけることで、本来のサービス（通信機能）を妨げ、それによって被害をもたらす攻撃である。

DoS 攻撃にはいくつかの種類があるが、「スマーフ攻撃」や「SYN フラッド攻撃」が有名である。スマーフ攻撃は、ICMP エコー（ping）を悪用してホストの接続回線の帯域を食い潰す DoS 攻撃である。方法としては、あるネットワークに対して ICMP エコー要求をブロードキャストし、要求を受け取ったホストは送信元へ ICMP エコー応答を返すが、要求はブロードキャストで行われているため、何十、何百というホストから同時に応答が戻される。ICMP エコー要求の送信元 IP アドレスを別の IP アドレスに書き替えておけば、膨大な量の応答を別のホストへ向けられるという仕組みである。

もう一つの SYN フラッド攻撃は、TCP の３ウェイハンドシェイクを悪用してホストを応答不能に陥れる DoS 攻撃である。方法としては、ターゲットに対して端時間に膨大な量の接続要求（SYN）パケットを送りつける。SYN を受け取ったホスト（ターゲット）は SYN+ACK を返して、通信相手（クラッカー）から最後の ACK が戻ってくるのを一定時間待機するが、その間ホストのリソース（メモリ）は消費される。もしこのとき、最後の ACK を送り返さないまま、次々に大量の SYN を送ればホストはいずれリソースを使い果たして、応答不能に陥ってしまう。

こうした攻撃はいわば物量攻撃なので、たくさんのホストから一斉に仕掛けたほうが効果的である。しかし、1 箇所から連続して大量のパケットを送ると、相手のファイアウォールが遮断することもある。そこで多くの場合、DoS 攻撃は複数の踏み台から同時に行う。

6　なりすまし

バッファオーバーフローやDoS攻撃のように「力ずく」でホストを攻撃する以外にも、「こっそり」と情報を盗み出すクラッキングもある。代表的なものが「なりすまし」で、これは文字通り、本来の通信先ホスト（サーバ）になりすまして、あるホストを騙すことである。

実際の方法としては、DNS サーバの情報を書き替える「DNS スプーフィング」が有名である。DNS サーバはドメイン名に対応する IP アドレスを回答するサーバであり、同時に自分が保持していない情報は、別のサーバに尋ねるという機能を持っている。そこで、ある DNS サーバが別の DNS サーバに問い合わせをしたときに、その通信を途中で横取りし（セッションハイジャック）、嘘の IP アドレスを答える。嘘の IP アドレスを教えられた DNS サーバは、それを元の問い合わせ先（クライアント）に回答する。その結果、クライアントは図らずも別のサーバに接続し、そのまま通信してしまうというわけである。

Ⅱ　ファイアウォール

インターネットからの脅威に対応するための手段、そして防衛のための一般的な手段として利用されるのがファイアウォールである。クラッカー（攻撃者）の攻撃にはいくつかのパターンがあり、前準備の段階ではホストへ侵入する入り口を探している。その入り口よりも前に設置し、不正な侵入を前もって防御するための機能がファイアウォールである。ファイアウォールは、「安全でないネットワーク」であるインターネットと、社内ネットワークなどの「安全を確保したいネットワーク」との境界に唯一の出入口として設置する、文字通り「壁」のような存在である。

インターネットの脅威として、以下の表のようなことがあげられる。

脅　威	意　　味	現実に例えた場合
乗っ取り	外部からの侵入者（クラッカー）がシステムの最高の利用権限を得てしまう状態。	泥棒に自宅に侵入された状態。自宅にあるすべてのものが危険にさらされる。
ポートスキャン	システムの弱点を探し出す。情報収集であり、直接的な被害に直結するものではない。	泥棒が侵入口を探してドアや窓を丹念に調べている状態。
物量作戦	無意味なデータを大量に送りつけることで通信を阻害する。	暴走族が深夜に自宅の周りを走り回るとか、街宣車に乗り付けられるという状態。
一撃必殺	あるポートに特定のデータを送りつけるとシステムがダウンするといった類のもの。	現実の家屋にたとえると放火に近い。
メールウイルス	メールに添付したマクロなどにウイルスを仕込むメールウイルスによる攻撃。	剃刀入り封筒や爆弾が自宅に送られてくるというイメージ。

インターネットの脅威

現実の家屋に対してはそうそう簡単に生じるものではないが、コンピュータネットワークの世界では、現実世界よりも罪悪感が薄くなりがちである。こうした行為を犯した場合のクラッカー側が負うリスクも、現実世界の犯罪に比べれば少ないので、被害に遭う可能性も高い。そのため何らかの防御手段を考えておくことが必要である。そのためにまず利用される一般的な方法が、ファイアウォールである。

外部からの脅威の侵入を食い止めるための防御手段一般を指す。ファイアウォールの実装手段には何種類もあり、実装方法によって防御できるもの、向き不向きがある。

Ⅲ　パケットフィルタリング

ファイアウォールを実現する技術で基本となるのが、「パケットフィルタリング」である。パケットフィルタリングとは、パケットに含まれるさまざまなヘッダ情報を参照し、あらかじめ設定したルールに照らしてそのパケットを通すか通さないかを判断する。

1　パケットフィルタ

パケットをフィルタリングする機能。パケットを一つずつチェックして、事前に設定された条件に従って通過させたり遮断したりする機能。ただし、一般的にはIPおよびTCP/UDPのヘッダまでしかチェックしない。パケットフィルタの判断材料には、送信元／受信先それぞれのIPアドレス、ポート番号やプロトコル、そして最初のパケットか、既存のセッションに属する応答かなどがある。これを適宜組み合わせることで、内部から外部への通信は許可するが、外部から内部への通信は、内部から開始された通信の応答以外は遮断するといった機能が実現できる。また、ポートを条件として利用すれば、通信に必要なポート以外への着信をすべて遮断することが可能となる。そういった場合、NATが非常に有効である。

一方、通信自体は正当だが、データに不都合があるというケースにメールウイルスがある。メール自体がそのユーザに送られてきたものであり、ユーザ自信がPOPなどを利用してメールをサーバから転送してくる場合、そのパケットのヘッダなどに不正な点がないし、当然ＮＡＴによる隠蔽も意味をなさない。こうした「正当な通信に混入される不正な情報」を遮断するのはパケットフィルタでは困難である。また、物量作戦に関してもパケットフィルタに限らず有効な対策はない。

2　アプリケーションゲートウェイ（最近ではプロキシサーバと呼ばれる）

アプリケーションレベルで中継を行い、その過程で詳細なチェックを行うことができる。単純に言えば、クライアントの代わりに、まずファイアウォールが全データを受信し、チェックしたあとクライアントに渡すという手順になる。Ｗｅｂアクセスの際に使われるHTTPプロキシなどがその例である。ただし、プロキシサーバには様々な用途があり、必ずしもファイアウォールとしてのみ利用されるとは限らない。HTTPプロキシの場合も、実際キャッシュサーバとして利用される例が目立つ。メールに添付されてくるウイルスをチェックするウイルスチェックなどでは、一度ファイアウォールがメールを受け取ってウイルスチェックをかけたあと、本来のメールクライアントに再度データを渡すという処理をするものが多いが、これもアプリケーションゲートウェイの実装だといえる。

ファイアウォールの実装場所にも様々な例が考えられる。最近目立つのは、ＰＣ以外のハードウェアに組み込まれる例である。ＩＳＤＮダイアルアップルータや、ケーブルモデムに接続することを想定した「ブロードバンドルータ」のほとんどすべてには、パケットフィルタの機能やアドレス変換の機能が組み込まれている。こうした組み込み型のファイアウォールでは、機能面では拡張性に欠ける面があるが手軽に利用でき、ＰＣよりも安定して動作することが期待できる。一般家庭や小規模な組織では、こうしたパケットフィルタ内蔵のデバイスを利用するのが簡単でよい。

ソフトウェア製品として実装されているファイアウォールでは、高価なものからＯＳ標準の機能として提供されるものまで様々なものがある。高機能なものでは、アプリケーションゲートウェイとパケットフィルタを組み合わせて利用できるほか、ＬＤＡＰ（Lightweight Directory Access Protocol）などのディレクトリサービスや認証メカニズムと連携して高度なセキュリティ機能を提供するのが一般的である。

ファイアウォールを組み込んだＯＳとしてはLinuxがよく知られているが、Windows2000にも簡単なパケットフィルタ機能は提供されている。したがって、外部ネットワークとの接続点にこうしたＯＳが稼

動するマシンを設置しておくだけでも小規模環境では有用である。さらに、Windows95 以降では、クライアント上で直接動作する「パーソナルファイアウォール」があり、１台しかＰＣを所有していないホームユーザには有用である。

３　パケットフィルタリング

ビルの部屋なら鍵をかけておかなければ不審者が部屋に入り込んで何か悪さをするかもしれない。ポートも同様、使用／不使用に関わらず、鍵をかける必要がある。

パケットフィルタリングには、２種類のポリシーベースがある。「初期状態では全てのパケットを通しておき、必要に応じてパケットをフィルタリングするための規則を設定するという」ポリシーと、「初期状態ではすべてのパケットを通さずに（リジェクトし）、必要なものだけ通すように設定する」というポリシー。現在は後者のポリシーを採用している場合が多い。（デフォルトとなっている）

Ⅳ　アドレス変換の必要性

最近では、LAN 内部などではプライベートアドレスを利用する方が一般的である。個々のマシンにグローバルアドレスを割り当てるのは、例外的なケースになってきている。プライベートアドレスを利用するには、NAT（Network Address Translation）または IP マスカレードと呼ばれる機能を利用してアドレスを変換する。NAT は１対１の対応で、IP マスカレードは１対多の対応となる。最近では、ＮＡＴと単純に呼びつつも、実体としては１対多の IP マスカレードであるという例が多い。NAT / IP マスカレードの機能は、最近では ISDN ダイアルアップルータやブロードバンドルータ、そして一般的な OS に実装されている。クライアント OS でも、Windows98 Second Edition 以降で実装されている「インターネット接続共有」という機能は、実体としては IP マスカレードである。

NAT と IP マスカレードは「単一のグローバルアドレスを複数のマシンで共有できる」という点に関しては共通だが、セキュリティ面からは重要な違いがある。単純な NAT の場合、グローバルアドレスとプライベートアドレスが単純に変換されるだけなので、LAN 内に複数の PC がある場合「グローバルアドレスがどのプライベートアドレスにマッピングされているか」はわからないが、その PC に対して外部からアクセスすることは可能である。この場合、グローバルアドレスを指定してポートスキャンをかけると、実際にはプライベートアドレスを利用している PC のポートが走査される。マッピングが変更されれば状況が変化するとはいえ、セキュリティが強化されることはない。

一方 IP マスカレードでは、グローバルアドレス+ポートがプライベートアドレス+ポートに変換される。このように、ポート番号も含めて変換されるため、ポートスキャンは実質上意味をなさなくなる。つまり、IP マスカレードを利用するだけでポートスキャン対策になる。

セキュリティを考えた場合、ＩＰマスカレードを利用するだけで簡易ファイアウォールと見なせるレベルのセキュリティが実現できる。特に、ブロードバンドルータなど、デバイスのみグローバルアドレスが割り当てられている状態であれば、乗っ取りやポートスキャン、一撃必殺型攻撃に関してはほぼ保護される。

さて、このようにセキュリティ面での効果も期待できる IP マスカレードだが、一方ではセキュリティを強化するためには利用が必須というわけではない。ファイアウォールを適切に設定すれば、グローバルアドレスを利用していたとしても外部からのアクセスを個々の PC ごとに制御することは可能である。また、プロキシサーバを経由して接続することで個々の PC に外部から直接接続できないような環境を構築することもできる。

Ⅴ　NAT と NAPT

NAT（Network Address Translation）と NAPT（Network Address Port Translation：ＩＰマスカレード）の違いについて、NAT も NAPT も、企業などの組織内で使用できるアドレス（ローカルアドレス）と、インターネット上のアドレス（グローバルアドレス）を透過的に相互変換し、１つのグローバルアドレスを複数のコンピュータで共有する技術である。相違点は、ＮＡＰＴではアドレスだけでなく TCP / UDP のポート番号も動的に変換されるので、１つのグローバルアドレスで複数のコンピュータからの同時接続を実現できる。NAT は「１：１のアドレス変換」で、NAPT は「１：多のアドレス変換」である。

ＩＰマスカレード	→	NAT による IP アドレスの変換だけでなく、その上位プロトコルである TCP／UDP のポート番号も識別することで、異なる通信ポートを利用するものについては、1 つのグローバル IP アドレスを利用して、複数のローカルノードが外部と通信できるようにしたソフトウェア。UNIX システムの 1 つである Linux 上で最初に開発された。「masquerade」は「仮面舞踏会」という意味。

Ⅵ　ウイルス感染の仕組み

ウイルスといっても様々なパターンがあり、当然その仕組みや目的も異なるし対策も変わってくる。そこで、ウイルスとは何かというところから記述していく。

国内のウイルス届出窓口となっている政府機関の IPA（Informaion-technology Promotion Agency：情報処理振興事業協会）によると、コンピュータウイルスは「①プログラムに寄生する極めて小さなプログラムであり、②自分自身を他のプログラムファイルにコピーすることで増殖し、③コンピュータウイルス自身に組み込まれたユーザの予期しない動作を起こすことを目的とした特異なプログラム」とされている。

現状では、③の特徴をもつプログラムをひとくくりにして「ウイルス」と呼ぶ場合が多い。しかし、厳密な意味でのウイルスは不正プログラムの１つの形態なので、他の不正プログラムである「ワーム」や「トロイの木馬」とは別ものである。ワームやトロイの木馬は、それ自身が１つの独立したプログラムとして動作する点で①の特徴を持つウイルスとは異なる。ワームは自分自身の増殖が主目的であり、作成者はどれだけ広範囲に広がるかに焦点を当てて作成している。一方トロイの木馬は、ターゲットになる PC に潜ませておいて、あとからクラッキングするために利用する仕掛けである。この２つのウイルスはユーザの知らないところで勝手に動作して被害をおよぼすという点は共通している。また、現在はメールが普及したことで、以前に比べて短時間で広範囲に不正プログラムが行き渡りやすくなっている。また、「Code Red（コードレッド）」のような、ウイルス、ワーム、トロイの木馬が連携するタイプの不正プログラムが増加している状況もある。

ウイルスの正体はプログラムであり、ウイルスを実行することで他のプログラムにウイルスが埋め込まれたりする。一般にウイルスが埋め込まれているプログラムを「ウイルスに感染しているプログラム」と呼ぶ。ウイルスがいつ活動を始めてもおかしくない状況を「感染」というのである。このことから、ウイルスに感染するのは「ウイルス作成者が送り込んできたウイルスプログラムを実行する」ことが前提となる。裏を返せば、ウイルスを実行しなければ感染しないということである。

以前は、ウイルスはフロッピーなどの物理的な媒体を経由して運ばれることが多かった。メールを介して次々にウイルスが広まる現状では、悪循環に陥る可能性が高い。誰かがどこかで止めなければ、永久にループしてウイルスの被害はなくならない。

また最終的な目的はどうであれ、ウイルス作成者はウイルスが広範囲に広がることを期待し、自分の能力

を誇示したい場合もあるだろうし、DoS 攻撃の攻撃元に利用する場合は、攻撃元が多ければ多いほど効果的である。現在のようにこれだけメールが普及していれば、それを使わない手はない。つまり、狙った相手にウイルスプログラムを実行させれば、後はメールに乗って広範囲に広がることは明らかなのである。

先に「ウイルスプログラムを実行しなければウイルスには感染しない」と述べたが、よくクラッカーに狙われる Outlook Express では、プレビューする際に Internet Explorer のプログラムモジュールを呼び出すようになっている。このため、ActiveX や JavaScript などで書かれたプログラムを Outlook Express でプレビューすると、Internet Explorer が実行環境（シェル）として呼び出されてしまう。「Nimda（ニムダ）」や「Klez（クレズ）」などは、この方法を利用して爆発的に広がった。

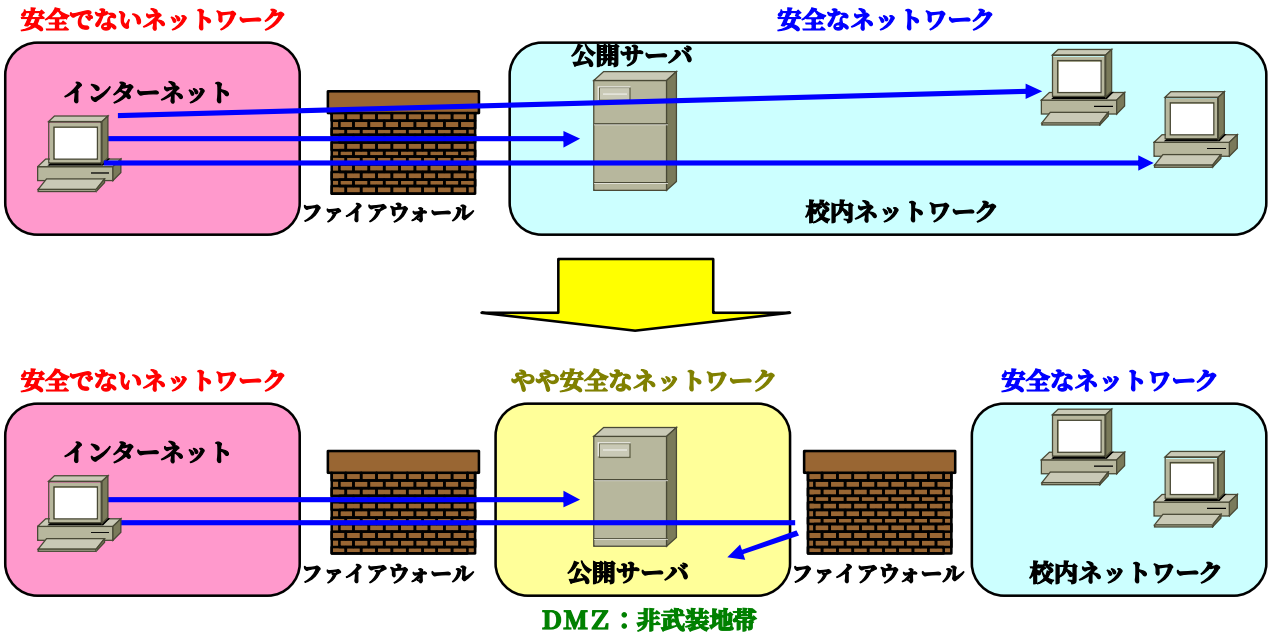
具体的には、セキュリティホールを利用するため、バッファオーバーフローを起こすような特定のコマンドやスクリプトをメールの本文に記入し、最後に添付ファイルを実行するようにしておく。すると、メールをプレビューした時点でスクリプトが実行され、そのまま添付ファイルも実行されてしまう。

これらの対策として、Outlook Express や Internet Explorer を使わなければいいという意見もあるが、一番の対策は、セキュリティパッチをこまめに当てたうえでメールクライアントの「自動的にプレビューを表示する」機能をオフにすることである。

Ⅶ　DMZ とホストの要塞化

1　外部にサーバを安全に公開する

外部にサーバを公開するということは、安全でないインターネットにサーバを公開するということである。そのためにはそれなりの工夫が必要となる。ファイアウォールの内側（校内ネットワーク内）に公開サーバを設置すると、インターネットからの通信をすべて遮断してしまい、サーバを公開できない。かといってサーバへの通信を許可すれば、外部からの接続を校内に入れてしまうことになる。つまり、他のホストの安全性が公開サーバと同じレベルまで下がってしまう。そこで、もう一つ別のネットワークでサーバを公開する。１台のファイアウォールでは、ルールが一つしか決められないため、「安全な校内ネットワーク」と「そうでないインターネット」の２つにしか切り分けられない。しかしファイアウォールを２台設置すれば、ルールは２つ決められる。そうすると３つのセグメントができ、１つ目は安全でないネットワーク、２つ目はやや安全なネットワーク、３つ目が安全なネットワークとなる。この３つ目のセグメ



ントに、校内ネットワークと異なるセキュリティポリシー（パケット通過のルール）を適用すれば公開サーバを安全に運用できる。この３つ目のセグメントのことを DMZ（DeMilitarized Zone：非武装地帯）という。DMZ は、２台のファイアウォールにはさまれた中間のセグメントのことを指す。インターネットと DMZ 間は「やや安全」に、DMZ と校内ネットワーク間を「絶対安全」にというポリシーを作れば、校内ネットワークのセキュリティを下げずにサーバを公開できるようになる。

２　DMZを介したパケットの流れ

３つのセグメント間でのパケットの流れにおいて、基本的にパケットは「否定」「必要なポートのみ許可」「問い合わせに対する応答のみ許可」の３種類のルールに基づいてネットワーク内を流れる。

ファイアウォールの設定			
接続元		あて先	動　作
インターネット	→	DMZ	必要な通信のみ許可
	→	校内ネットワーク	拒否
DMZ	→	インターネット	問い合わせに対する応答のみ許可
	→	校内ネットワーク	問い合わせに対する応答のみ許可
校内ネットワーク	→	インターネット	拒否
	→	DMZ	必要な通信のみ許可

① インターネットと校内ネットワークの間は、パケットを通さない「拒否」になっており、双方とも直接通信できない。つまり、インターネットから直接校内ネットワークにアクセスできず、逆に校内ネットワークからインターネットにも直接出られない。これで校内ネットワークは「絶対安全なネットワーク」として守られる。

② 「必要なポートのみ許可」は、インターネットと校内ネットワークが、DMZ にアクセスする際のルールである。DMZ にメールサーバ、Web サーバ、DNS サーバの３台を設置すると、プロトコルとしては、SMTP（25 番）、HTTP（80 番）、DNS（53 番）の３つのみが DMZ に出入りする。つまり、DMZ に設置した公開サーバにアクセスさせるためには、この３つの宛先のルールポートに対する通信を許可すればよいことになる。逆に、これ以外はアクセス拒否にしておけば、ファイアウォールに必要最低限のポートを開けることになるので、一定レベルのセキュリティが保たれる。

③ 「問い合わせに対する応答のみ許可」は、先のルールとは逆に DMZ から他の２つのセグメントに向けた通信用に適用される。公開されたメールや Web、DNS サーバへの問い合わせに対する応答のみ許可される。具体的には、それぞれの送信元ポートが 25、80、53 番だった場合は通信を許可し、それ以外は拒否されるということになる。

３　ファイアウォールの機器

ファイアウォールを構築する機器として最も原始的なものは、ルータである。ルータはパケットフィルタリングを使ったファイアウォールである。あるいは、１台の PC サーバに NIC を２枚挿してインターネットと校内ネットワークを接続し、OS のパケットフィルタリング機能やプロキシソフト、ファイアウォール専用ソフトを使って構築することもある。DMZ は２台のルータで構築したり、PC サーバにもう１枚の NIC を取り付けることで作ることができる。しかし、いずれの方法でも、複数のルータ

を適切に設定したり、ゼロからマシンを構築するなどの手間がかかる。

そこで最近主流なのが、ファイアウォール専用機（アプライアンス）を利用するケースが多くなってきている。

4　サーバの要塞化

公開サーバを設置するための DMZ は、インターネットからの接続を直接受け付けるための「やや安全なネットワーク」にすぎず、校内ネットワークよりも危険度が高いといえる。少なからず、攻撃される危険性がある。そこで公開サーバには、サーバ自体を強固なものにする「サーバの要塞化」というセキュリティ対策も欠かせない。サーバの要塞化は、複数の手法を組み合わせて行う。

① セキュリティパッチの適用

サーバで稼動している OS やアプリケーションを、常に最新のものにしておくという方法がある。インターネットでは、日々新しいセキュリティホールが発見され、それに追随する形で各ベンダーから最新のセキュリティパッチ（修正プログラム）が提供される。

② 不要なサービスの停止

サーバで動作している不要なサービスを止める。Windows や UNIX 系 OS に限らず、OS はインストール直後の状態で、何らかの機能を提供するための「サービス」と呼ばれるプログラムが動作している。不要なサービスとして、外部からホストにリモートログインするための Telnet が挙げられる。Telnet では、ユーザ名とパスワードが判明してしまえば、そのマシンにログインできる。また、通信は平文で行われるため、盗聴されてしまえばパスワードの情報が漏れてしまう。そこで現在では、暗号化通信が可能な SSH（Secure SHell）を使われることが多い。

③ 強固なパスワードの設定

管理者用のパスワードを強固なものにする。クラッカーがサーバに侵入しようとする際は、とりあえず考えられる文字の組み合わせをすべて試したりするからである。

④ ログの管理

最後に、サーバのログをきちんと管理することも要塞化につながる。もちろんログを収集するだけでは意味がないので、きちんとした解析が必要となる。ログの解析ツールを使えば、システムの状態だけではなく、攻撃を受けた形跡をビジュアル的に調査できる。また、ログを数ヶ月保存しておく必要がある。これは攻撃を受けたら、その痕跡を数ヶ月に遡って調べる場合もあるからである。さらにログは、安全な場所に保管し、syslog を使って他のマシンにログを定期的に転送しておくことも要塞化の有効な方法である。

Ⅷ　盗聴を防ぐための通信

1　暗号化通信

インターネットで送られるデータは、郵便の「はがき」に書かれた文字と同じで、データはホストが作成したままの状態で配送される。テキストデータであれば、生のテキストがネットワークに流れ、相手に届くまでのルートもあらかじめ決められていないため、どこをどう通るのかわからない。つまりインターネットは、データの中身が誰の目に触れてもおかしくない状態で通信されている。はがきが大事な用件の伝達に不向きなように、インターネットでも機密性の高い情報のやり取りには向いていない。しかし現在では、インターネットが生活や仕事の一部になっているため、平文で送らないようにする方法を取る必要がある。それを行うのが暗号化通信である。

暗号化通信は、送信元で平文のデータを加工する「暗号化」を行い、受信先で元のデータに戻す「復号化」をすることで実現される。

2　暗号鍵の共有方法

暗号鍵の共有には２通りの方法がある。１つ目は、送信ホストと宛先ホストで同一の暗号鍵を共有する方法である。この方法は「共通鍵暗号方式」と呼ばれ、暗号化通信するホスト同士で共通の鍵を共有する。暗号化通信したい相手に自分の鍵を渡すことにより実現できる非常にシンプルな方法である。しかし、共通鍵暗号方式の課題として、暗号鍵の受け渡しをどのように行うかである。離れている相手に鍵を渡すために、メールの添付ファイルとして送れば、その鍵自体が盗聴される恐れがある。安全を期すためには、暗号鍵をフロッピーディスクに入れて手渡しするしかない。そこで、もっと手軽にかつ安全に暗号鍵を受け渡せる方法が考え出された。それが２つ目の「公開鍵暗号方式」である。公開鍵暗号方式では、暗号鍵を２つに分けて、１つを一般に公開する（公開鍵）。そして、もう１つの鍵は自分だけで管理する（秘密鍵）。暗号化はどちらの鍵を用いても行えるが、復号化できるのは他方の鍵だけとなる。つまり、公開鍵を使って暗号化してもらえば、それを復号化できるのは秘密鍵を持つ「自分だけ」ということになる。

公開鍵暗号方式なら、共通鍵暗号方式の課題である鍵の受け渡しの問題はなくなる。しかし、公開鍵暗号方式にも問題がある。それは、公開鍵を配布している人が「本当に通信しようとしている相手」かどうか何の保証もないことである。もし、公開鍵の持ち主が他人になりすました悪意の第三者であれば大変なことになってしまう。そのため公開鍵暗号方式では、公開鍵の所有者の身元を確認したうえで通信できる仕組みが不可欠である。これは現在、PKI という技術によって実現されている。

また公開鍵暗号方式は、身元の確認や、512 ビットや 1024 ビットの長い鍵長のため重く、処理に時間がかかるという問題がある。そこで実際の暗号化通信では、最初に公開鍵暗号方式を使って共通鍵を送受信し、そのあとは処理の軽い共通鍵方式を使うという「２つの方式の組み合わせ」で行う場合がほとんどである。

3　さまざまな暗号化技術

暗号化技術とは、暗号アルゴリズムを機能として使えるようにするものである。これは通信のレイヤ（層）ごとにいくつか開発されている。

TCP/IP での通信は、４つの階層に分かれて機能している。下から順番に、ホストの物理的な接続を提供する「データリンク層」、IP アドレスに基づいてデータ（パケット）を送受信する「ネットワーク層」、パケットをアプリケーションに受け渡す「トランスポート層」、アプリケーション同士でデータを解釈する「アプリケーション層」である。暗号化技術はこの各層ごとにあり、中でも上位３層のものは馴染み深い。

最上層のアプリケーション層には、メールの暗号化を行う「PGP（Pretty Good Privacy）」や「S／MIME（Secure MIME）」、ホストの遠隔操作を暗号化する「SSH（Secure SHell）」がある。

その下のトランスポート層の暗号化では、Web 通信でよく利用される「SSL/TSL（Secure Sockets Layer / Transport Security Layer）」がある。

ネットワーク層で暗号化する「IPsec（IP security）」では、IP レベルで暗号化するため、すべてのアプリケーションの通信を丸ごと保護する。実際にパケットを暗号化／復号化するのは、ルータなどネットワーク層で動作する機器である。つまり IPsec を使うと、アプリケーションは暗号化のことを考えなくても暗号化通信できる。またホストやネットワーク全体を暗号化の対象にするため、インターネットを介し

たリモート接続や LAN 間接続にも利用しやすい。

4　SSL の仕組み

現在最も普及している暗号化技術では SSL（Secure Sockets Layer）である。これは、一般に利用されるほとんどの Web ブラウザで使用することができる。SSL では、共通鍵暗号方式と公開鍵暗号方式の組み合わせで暗号化通信を行う。

SSL ではまず、公開鍵暗号方式を使ってクライアントとサーバ間で安全な通信路を確立する。この通信路を使ってやり取りされるのは、実際のデータ通信の暗号化に使う共通鍵の「元データ」である。この元データは、「プレマスターシークレット」と呼ばれる 48 バイトのランダムな数値である。

公開鍵暗号方式による通信は、具体的に次のようになる。クライアントがサーバへ接続要求を送ると、それに対する応答が戻ってくる。応答には、サーバの公開鍵が含まれている。クライアントは公開鍵の所有者を確認したあと、プレマスターシークレットを生成する。これをサーバの公開鍵で暗号化して送り返す。サーバがプレマスターシークレットの暗号文を受け取ったら、自分の秘密鍵で複合化する。この時点でクライアントとサーバは「同じデータ」を共有できたことになる。しかし、このデータから直接共通鍵が作られるわけではない。クライアントとサーバ間のセッションが途中で横取りされていないとも限らないので、共通鍵の生成には２つのランダムデータ（最初の要求－応答時に送られている）を加える。これによって、クライアント－サーバごとに固有で、セッションごとに固有な共通鍵を共有できる。共通鍵の共有ができれば、あとはその鍵を使った共通鍵暗号方式で暗号化通信を行う。

5　IPsec とは

SSL 以外にも、最近は IPsec（IP security）も徐々に普及の兆しを見せている。ネットワーク層で暗号化をする IPsec はネットワーク自体を対応させる必要があるため、他の暗号化技術に比べて導入の敷居が高い。具体的には、パケットの出入口にあたる２点間を IPsec の暗・複合化する「VPN ゲートウェイ」で接続しなければならない（LAN 間接続の場合）。しかも、IPsec の実装は VPN ゲートウェイベンダーによってばらつきがあり、相互接続性が乏しいのが現状である。

IPsec はもともと、IP レベルで広くセキュリティを確保するために開発されて技術である。IPsec でできることは、暗号化通信に限らず、あるプロトコルのネットワークに別のプロトコルパケットを通す「トンネリング」や、パケットの改ざんを防止する「パケット認証」、通信先の正当性を確認する「サーバ認証」といった、安全な通信に欠かせない機能が盛り込まれている。そのため、IPsec の構造はとても複雑である。

Ⅸ　PKI と電子署名

現在のインターネットでは、公開鍵暗号方式と共通鍵暗号方式の組み合わせによって暗号化通信が行われている。ただし公開鍵暗号方式では、公開鍵の所有者が「本当に通信する相手」であることが保証されなければ、安全な通信はできない。例えば、あるショッピングサイトで買い物をし、買い物時に入力する氏名や住所、クレジットカード番号といった情報は、SSL を使った暗号化通信によって保護されている。しかし、暗号化に利用した公開鍵は、本当にショッピングサイトのものかどうかわからない。そしかするとショッピングサイトになりすました悪意の第三者かもしれない。そうなると、送信した個人情報は別の誰かに知られてしまう。そこで、公開鍵暗号方式を利用した通信を行う場合、クライアントが公開鍵の所有者を確認できるようにするのが「PKI」である。

1　PKI（公開鍵暗号基盤）で身元証明

PKI は公開鍵暗号方式を利用して、ネットワーク上のセキュリティを確保するために考えられた仕組みである。PKI はインターネットがビジネスや生活にすっかり浸透した現在、これまで「紙ベース」で進めていた様々な処理をオンラインで安全に行うために必要になる。具体的には、顔が見えないネットワークで、①相手の身元を確認し（なりすまし防止）、②データが途中で書き替えられていないかを調べ（改ざん防止）、③内容の食い違いをなくす（否認防止）ための技術が盛り込まれている。

前に挙げたショッピングサイトの例で考えれば、ショッピングサイトで安心して買い物するためには、ネットワーク上で配布された公開鍵の所有者の身元を証明しなければならない。加えて、その証明が正当なものであることの保証も必要となる。これを実現するために、PKI では「電子証明書」（公開鍵証明書）と、「電子署名」という２つの技術を使う。

Web ブラウザからショッピングサイトと SSL 通信する際、実はサーバから公開鍵といっしょに電子証明書も送られてきている。サーバから送られてきた電子証明書は、SSL のページにアクセスしている Web ブラウザ（Internet Explorer）の右下にある「鍵」のアイコンをダブルクリックすれば表示される。これを見れば、暗号化に使う公開鍵の所有者を確認できる。

実際に電子証明書を見てみると、「発行先」としてショッピングサイトの名前、「発行者」として何らかの組織名が記されていることがわかる。発行先は、公開鍵の所有者である。また発行者は、この証明書を作成した組織を示す。つまり、発行先の名前がサイトの名前と同じであれば、発行者によって公開鍵は発行先のサイトのものであることが証明されている。

発行先は何らかの組織名が記されていると前述したが、この組織は「認証局（CA：Certificate Authority）」と呼ばれる。もし、この認証局が怪しい組織であれば、確かにその証明書は疑わしいが、認証局がユーザにとって「信頼できる組織」であれば、送られてきた証明書は信頼できることになる。しかし、認証局を信頼できるかどうかはユーザ自身の問題であるため、PKI では一般に「著名な組織」か、「自分に関連する組織」であれば信頼できることを前提にしている。それは、電子署名という仕組みによって、証明書を改ざんすることや偽造することが非常に困難になっているからである。

認証局には、２つの種類がある。１つは第三者的な立場で、様々なサイトに電子証明書を発行する専業の認証局（パブリック CA）。もう１つは、特定の関係者だけで利用するネットワーク用に専用の構築ソフトを使って自前で運営する認証局（プライベート CA）である。パブリック CA は、ベリサインなどいくつかの有名なセキュリティ事業者によって運営されている。こうした名の知れた認証局であれば信頼できる。

①　PKI の用途

PKI では以下のような幅広い用途が考えられる。

ア　電子商取引のインフラ構築

安全な電子商取引を行うためには、企業間あるいは事業者内で専用線を使ってセキュリティを保つことが考えられるが、将来の本格的な企業間の取引ではインターネットを介したセキュアな取引が必須となる。また、オンライン販売のような販売事業者対消費者の場合では、インターネットでクレジットカードを使ったオンライン決済が必要となる。ここに PKI を適用すれば、相手が誰であるかを確実に確認でき、しかも情報が漏洩する不安のない電子商取引が円滑に行えるようになる。

イ　イントラネットのアクセスコントロール

企業や組織でイントラネットを構築し情報の提供や共有を行なう場合、部署や役職等に応じてアク

セスできる情報に制限を設けたい場合がある。PKI を使えば、このような情報のアクセス制御が容易になる。PKI が提供するセキュリティの特徴は、外敵の侵入を防ぐのではなく、対象物（エンティティ）を守るセキュリティを提供するところにある。イントラネット上の重要な文書は意図したユーザだけに閲覧（復号化）を可能にし、かつ、その文書が正しい人物によって作成されたことを証明するため、文書の改ざんの危険からも回避できる。

② 高等学校で PKI の活用

PKI は、電子商取引等のアプリケーションを構築するためのインフラであるため、高等学校での活用については考えていない。しかし、将来的には校内ネットワークのアクセスコントロールという方向で検討し、導入する価値があるようにも感じられる。

2 電子証明書の記載内容

電子証明書に記載されている情報は、発行先（公開鍵の所有者）と発行者（認証局）だけではない。Web ブラウザでどこかの電子証明書を開けるなら、ウィンドウのタブを「全般」から「詳細設定」に切り替えるとその中身を見ることができる。

あるショッピングサイトの電子証明書の詳細設定を開いて確認すると様々なことが記述されている。PKI で使われる電子証明書は、「X.509（バージョン３）」という形式に基づいて記述される。この形式では、発行先や発行者情報の他にも、証明書の有効期限など様々な情報が記載されている。ここで注目すべき点は、証明書に公開鍵が埋め込まれていることである。

PKI では、公開鍵は電子証明書の一部として送られている。これは、証明書で単に公開鍵の「所有者の身元」を示しているのではなく、「公開鍵と所有者の結び付き」を証明しているためである。つまり、証明書が発行されたあとに、勝手に鍵を変更できないようになっている。また、証明書の最後に付けられた認証局の電子署名にも注目しておく。電子署名はよく、デジタルの印鑑などと言われるが、単なる「確認印」ではない。実はもっと重要な役割を担っており、公開鍵を含めた電子証明書のデータが 1 ビットでも改変されると、証明書を受け取った側ですぐにわかるようにしている。これによって、証明書の改ざんを防止している。

3 メッセージダイジェストと電子署名

電子署名で改ざん防止が実現するのは、署名データが証明書の「メッセージダイジェスト」から生成されているからである。メッセージダイジェストとは、「ハッシュ関数」という特殊な関数（SHA1 や MD5）を使って生成された文字列である。ハッシュ関数は「不可逆的な一方向の関数」ともいわれ、生成したメッセージダイジェストから元のデータを取り出せないようになっている。また、同一のメッセージダイジェストを持つ、２つの異なるデータを作ることもできない。

このメッセージダイジェストの性質を利用すると、２つのデータの同一性を確認できる。例えば２つのデータが①「ネットワークに送信する前のデータ」と、②「送信後、相手が受け取ったデータとする。データ①を送るとき、あらかじめ生成しておいたメッセージダイジェストを添付すれば、受け取った側はデータ②から生成したメッセージダイジェストと比較できる。比較した結果、２つのメッセージダイジェストが一致すれば、データ②が送信中に改ざんされていないこと（①と②の同一性）が保証される。

電子署名を使った改ざん防止は、このような仕組みを利用する。送信側（認証局）で、証明書全体のデータを元データとしたメッセージダイジェストを生成し、証明書に添付しておけば、受信側で証明書の内

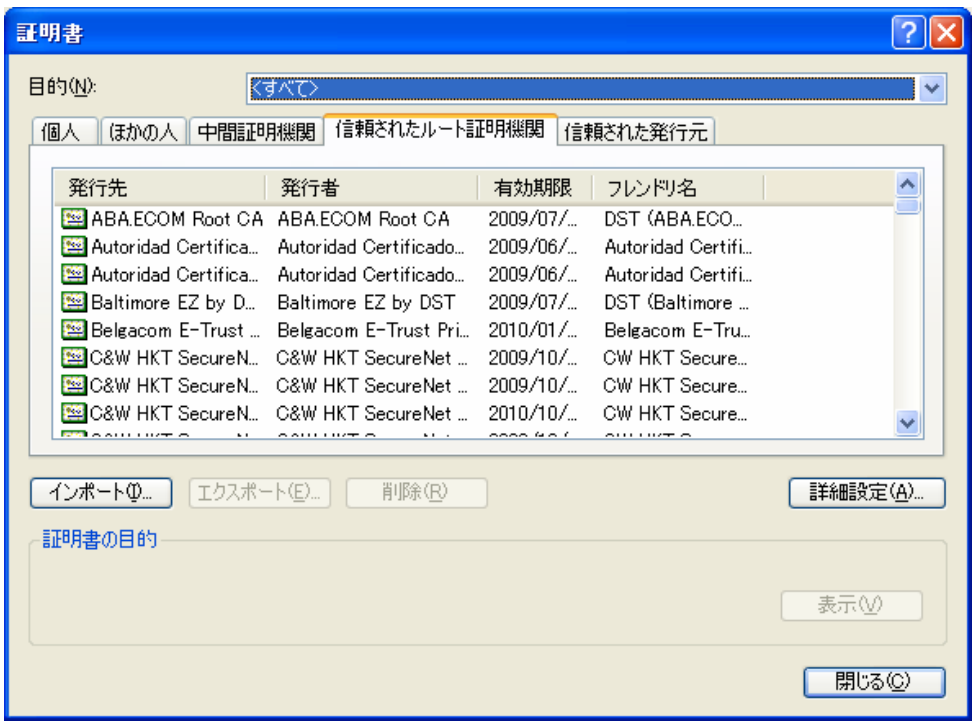
容を検証できる。加えて、メッセージダイジェストを認証局の秘密鍵で暗号化すれば、これを生成したのはその認証局であることを証明することにもなる。これを「本人認証」という。

ネットワークを介して電子証明書を受け取った側（ユーザ）は、次の手順で正当性を検証する。まず、証明書全体のデータを元データとしてメッセージダイジェストを生成する。同時に、電子署名の部分だけを「認証局の公開鍵」（サイトの公開鍵ではない）で復号化し、認証局が生成したメッセージダイジェストを取り出す。この２つのメッセージダイジェストが一致すれば、証明書全体は改ざんされていないことがわかる。認証局が証明書を発行したあとに、もしその一部でも改変されていれば、２つのメッセージダイジェストは一致しないからである。

4　認証局の公開鍵

電子署名を使った改ざん防止のプロセスでは、認証局の公開鍵が必要である。証明書にはサイトの公開鍵が含まれているが、認証局の公開鍵は含まれていない。多くのパブリック CA の公開鍵は、証明書という形で Web ブラウザにあらかじめ登録されている。例えば Internet Explorer では、「ツール」「インターネットオプション」「コンテンツ」「証明書」から登録されている認証局の証明書を見ることができる。また、登録されていない認証局（特にプライベート CA）の証明書を別途登録することも可能である。こうして Web ブラウザにあらかじめ認証局の公開鍵を持たせておくことで、証明書に付けられた電子署名を復号化できるようになっている。上記の Internet Explorer に登録してある証明書の認証局には、「中間証明機関」と「信頼されたルート証明機関」の２種類がある。

認証局に２種類あるのは、PKI では認証局自体の身元を別の認証局によって階層的に証明しているためである。これにより、「信頼の連鎖」を構築することができる。前で、認証局を信頼できるかどうかはユーザ自身の問題で、著名なパブリック CA や自分と関連するプライベート CA であれば信頼できると述べた。認証局の信頼が階層構造になっていれば、ユーザは間接的に多くの認証局を信頼できるようになる。



階層の頂点に立つのがルート認証局である。これは、別の認証局に電子証明書を発行する（＝署名する）役割を担う。また、ルート認証局から署名され、各サイトに証明書を発行するのが中間認証局である。例えば、あるサイトの証明書がどこかの中間認証局Ａから発行されているとする。この場合、ユーザが認証局Ａを信頼できなくても、その認証局がベリサインといった信頼できるルート認証局から署名されていれば、必然的にＡを信頼できる。この理屈から、ルート認証局を信頼すれば、大半の認証局を信頼できることになる。すなわち、PKI は「ルート認証局を信頼する」という前提で成り立っているのである。