# セキュリティ入門

熊谷 誠治（(株）電通国際情報サービス）

1999 年 12 月 15 日

Internet Week 99　パシフィコ横浜

（社）日本ネットワークインフォメーションセンター編

# 目次

# 1 概要

この講演では、次の事柄を中心にセキュリティの概要を説明します。

- なぜセキュリティが重要なのか。
- インターネットにはどのような危険が存在しているのか。
- インターネットを利用するときには、どのような点に注意すべきなのか。

# 2 セキュリティとは何か

まず、セキュリティという語の意味を考えてみます。英和辞典で「security」という語を引くと、安全や安心という訳語が得られます。また、コンピュータ用語としては、無断でデータにアクセスできないようにする「安全保護」という訳語が示されています。このようなことから、セキュリティとは安全を守ることのように思えます。

では、何から何を守るのでしょうか。一般には、人命・企業・財産・名誉・情報・人権などを、天災・事故・犯罪者・一般人・運命などから守ることになると思います。このとき、これらの守るべき対象を、どのようにして守るかが課題となります。

たとえば、守るべき対象にどの程度までコストをかけることができるのでしょうか。また、そのコストを本当にかける必要があり、それによって何が得られるのでしょうか。このような検討の際には、守れなかったときに失われるものを知ることが重要です。たとえば、会社の存続にかかわる情報や回復が難しい信用などは守るべきものとなりますが、失ってしまってもよいものであれば守る必要はないはずです。

では、どのような事件がインターネット上で発生しているのでしょうか。インターネットに関連した事件には、次のようなものがあります。

- 盗聴
- 侵入
- なりすまし
- 情報の改ざん
- 情報の破壊
- 情報の盗み出し

- ウィルス*
- ワーム*
- SPAM*

このような事件によって、次のような不正行為が多発しています。

- 誹謗や中傷
- 不法品の売買
- 猥褻画像の陳列
- クレジットカードの盗用
- 脅迫
- アクセス妨害
- 業務妨害
- 詐欺
- プライバシ侵害
- 著作権侵害
- いたずら

次に、このような被害の具体例を示します。

- 私の名前で掲示板に第三者の悪口を投稿された。
- 私のメールアドレスで宣伝メールを送られた。
- プロバイダの請求額が予想よりも多い。
- 掲示板に自宅の住所と電話番号が掲載された。
- 宣伝メールがどんどん送られてくる。
- 身に覚えのないクレジットカードの請求がきた。

| | |
|---|---|
| **ウィルス** | 感染した後、一定の潜伏期間が経過すると、自己増殖しながらコンピュータシステムを破壊し始めるプログラムです。 |
| **ワーム** | 感染した後、ネットワーク上のコンピュータ間で自己複製しながらコンピュータシステムを破壊していくプログラムです。 |
| SPAM | 不特定多数への宣伝広告のために、インターネットを利用して同時に同一のメッセージを送信することです。 |

- 私が送ったメールを第三者が知っているようだ。
- パソコンに変な表示が出た後、動かなくなった。
- NASA からアタックはやめろと抗議メールがきた。
- Web ページを勝手に書き替えられた。

このような不正行為はインターネット上でのみ発生しているのでしょうか。たとえば、怪文書による誹謗・中傷、注文していない商品の配達、クレジットカードの偽造、キャッチセールスなどは、実社会でも発生している事件です。ただし、インターネットの登場によって、このような犯罪がより手軽に実行されるようになってしまっているようです。また、「顔」が見えないため、罪悪感にさいなまれることなく実行されている可能性もあります。

## 2.1 インターネットの安全性

たとえば、先ほども示したクレジットカードの盗用は、実社会でもインターネット上でも発生しています。クレジットカードは、発行元のカード会社によって信用限度額が保証されているためサインのみで利用できます。ただし、インターネット上ではサインを送れないため、カード会社に登録している電話番号を確認する程度でクレジットカードによる決済が実行されています。ここで注意しなければならないことは、電話番号は他人が簡単に調べることができるため容易に悪用できてしまうことです。また、クレジットカードでは 4 桁の暗証番号によってキャッシングも可能ですが、暗証番号の盗用による不正利用には保険がきかないため、暗証番号の管理には細心の注意が必要です。このようにクレジットカードにはさまざまな問題が存在していますが、多くの人々がクレジットカードを利用し続けています。

つまり、クレジットカードは、その利用者がどのように意識して利用しているかが重要となります。たとえば、他人が思い付きにくい番号を暗証番号とすることで不正に利用される危険性は少なくなりますが、自らも暗証番号を忘れてしまう可能性が高くなります。そして、すべてのクレジットカードの暗証番号を同じものにしたときには、同時にすべてのクレジットカードが不正利用されてしまう危険性が高くなります。このようなことから、クレジットカードを利用するときには、利用控を保存し、毎月送付されてくる利用明細の内容を確認するだけでなく、誤請求されたときの処理手順やクレジットカード会社の責任範囲を確認したり、商品購入先の安全性を確認したりすることが重要となります。

では、インターネットの安全性はどうなのでしょうか。現実にインターネットに関連した事件がマスコミによって報道されていますし、次の被害者となってしまうかもしれません。また、技術の進歩が早すぎ、社内にインターネット技術を理解している人がいなかったり、勉強してもなかなか追いつくことができなかったりします。さらに、専門家が少なすぎるため、自分自身より少しでも多くの知識を持っている人の意見を信じるしかないのですが、その人の意見が一般的な常識であるかどうかは

判断できません。このようなことからインターネットは危険なものと考える人がいます。

これに対して、現実に多くの人たちが利用しているためインターネットは危険なものではなく、犯罪に巻き込まれる確率も低く、安全のためのしくみも多数販売されているので、専門家に任せておけば安全であると考えている人もいます。また、インターネットでは、常に最新情報が受け渡されているため、それをきちんと参照しておくことで危険な状況を事前に把握できると考えている人や、インターネットを使わなければビジネスが成り立たない状況になってきているのだから、インターネットを安全なものであると考えている人もいます。

真実はどちらなのでしょうか。実際には、インターネットが安全なものだと考えている人たちには「インターネットを安全だと思って利用することが危険である」ことを示し、潜在する危険を説明する必要があります。また、インターネットが危険だと考えている人たちには「インターネットは対応さえしっかりすれば安全に利用できるものであり、ビジネスに利用すべきである」ことを説明します。インターネットは、先ほど示したクレジットカードと同様に、その危険性を理解し、十分な対策を実施して、常に危険性を意識しながら利用すべきものなのです。

現在の日本では、情報を盗んでも罪に問われることがありません。たとえば、企業の顧客情報などを社員が盗んだときには、顧客情報を盗んだことが罪に問われるのではなく、情報を盗むために使用したプリンタ用紙やフロッピーディスクなどの物品を盗んだことのみが罪となります。また、日本では、偽造クレジットカードを保有しているだけでは罪に問われず、そのカードを利用したときに初めて犯罪となります。さらに、最近、法制化され「盗聴法」などと呼ばれている通信傍受法では、その手続きや対象範囲にあいまいな部分が残ったままだとも言われています。

このため、現状では、ユーザ自身の情報はユーザ自らが守る必要があります。また、システムへの外部からの侵入を阻止したり、侵入自体を検知したりすることも必要です。さらに、セキュリティホール* や CGI* によって外部からプログラムを送り込み、不正なコマンドを実行できてしまうことも認識しておくべきです。

---

**セキュリティホール**　プログラムのバグなどによって、本来許されていない方法で利用できてしまうプログラムの弱点です。

CGI　「Common Gateway Interface」の略。データベースサーバなどのバックエンドプログラムと Web サーバが情報を受け渡すためのインタフェースです。

---

# 3 個人に対するセキュリティ

ここでは、個人のセキュリティに関係する次の事柄を説明します。

- プライバシの保護（3.1 を参照）
- ウィルスへの注意（3.2 を参照）
- Unsolicited Commercial Email（3.3 を参照）
- パスワードの安全性（3.4 を参照）

## 3.1 プライバシの保護

現在、個人のプライバシが狙われ始めています。たとえば、顧客サービスを提供する Web システムでは、サーバにアクセスしてきたクライアントを特定するために cookie というしくみが利用されています。cookie によって、Web サーバの所有者は、特定のコンピュータからのアクセス状況を把握できます。また、Web ページ上のアンケートなどで氏名を明かしていたときには、cookie と関連づけられることで個人のアクセス状況までが把握されることになります。Web ブラウザでは、cookie の利用を拒否することもできますが、デフォルトでは受け付けるように設定されています。このため、プライバシを保護するために cookie の利用方法を検討しておく必要があります。

また、単に電話会社の電話帳に自分の電話番号を載せただけで、電話番号から氏名や住所を検索するサービスに自分の情報が利用されてしまうことがあります。同様に、同窓会名簿などに氏名や電話番号を掲載したことで、勧誘サービスの対象となってしまうこともあります。情報は必要な人々には伝えなければならないのですが、その情報がどこまで広がっていくのかも注意する必要があります。

さらに、最近では、相手のメールアドレスを入力するだけで無料で年賀状やクリスマスカードを送付できる Web サイトが増えてきています。ただし、このようなサイトは、メールアドレスを収集するために運営されていることが多いため、送り先となった相手に迷惑をかけてしまう可能性があります。同様に、プレゼントやアンケートを実施している Web サイトも増えていますが、これらもメールアドレスなどを収集するための手段として運営されています。このように、現在では、これまでに比べて個人情報が流出しやすくなっていると思えます。

## 3.2 ウィルスへの注意

ウィルスとは、システムを破壊するプログラムです。ウィルスは、メールに添付されたプログラムやデータに寄生して伝染し、データの転送などによって感染範囲を広げていきます。最近では、部門で利用しているサーバにウィルスが感染してしまい、部門内のすべてのコンピュータが被害にあったという例も増えてきています。

ウィルスの感染チェックや除去は、ウィルスチェック用プログラムで実行できます。ただし、ウィルスを特定するためのパターンファイルは、ウィルスが蔓延し始めてから提供されるため処置が遅れてしまうことがあります。このため、不明なプログラムなどを受け取ったときには、すぐに起動せずに、問題がないことが明らかになった後に利用するようにします。つまり、できるかぎり他人を信用せずに、自分の安全は自分自身で守るようにする必要があります。

## 3.3 Unsolicited Commercial Email

Unsolicited Commercial Email は、SPAM とも呼ばれる宣伝や広告のためのメールです。このようなメールでは、発信者のコストはごくわずかなものですが、ファクシミリによるダイレクトメールの配信と同様に大量のメールを受け取る受信者にとっては通信コストだけでなく処理の手間などを強いる迷惑なものとなります。また、インターネット上でメールアドレス自体が売買され、Unsolicited Commercial Email の利用は販売促進に効果があると勘違いされているようです。

Unsolicited Commercial Email は、このようなメールに記載されている企業から商品を購入しないようにすることで、効果がないことを分からせれば、多少なりとも数を減らせると思えますし、ある程度はシステムによって防ぐこともできます。

## 3.4 パスワードの安全性

パスワードとして使用する文字列には、辞書に記載されていたり、人名・製品名・グループ名などの容易に想像できたりするものは避けるべきだと言われています。現在利用されているパスワードシステムの多くは、システム上に暗号化したパスワードを保存しておき、ユーザが入力した文字列を暗号化した後、保存してあるものと照合しています。このため、辞書などに記載されている文字列を利用していると、簡単にパスワードが見つけ出されてしまいます。また、想像しづらい文字列をパスワードとしていたとしても、その文字列が短かったときには総当たりで処理することで短時間に解読されてしまいます。

このようにパスワードは比較的容易に解読されてしまうため、同一の文字列を複数のシステムのパスワードに利用しないようにします。同一のパスワードを複数のシステムで使用していると、そのパスワードが解読されてしまったときに複数のシステムが不正にアクセスされることになり、被害が広がる恐れがあります。また、保護しなければならない対象の利用目的や重要度に合わせて、パスワードを使い分ける必要があります。

さらに、複数のメンバーで同一のパスワードを共有しないようにもします。たとえば、サポートのための管理者用パスワードを使ってシステムに直接ログインするのではなく、各個人が個別にシステムにログインした後にスーパーユーザとなって作業を実施し、その内容を記録として残すようにします。

ワンタイムパスワードなどと呼ばれる使い捨てパスワードを利用することで、毎回異なる文字列をパスワードとして利用できるようになります。使い捨てパスワードを利用すれば、パスワードが盗聴され解読されたとしても、そのパスワードによって不正アクセスされることはありません。具体的には、S/Key というフリーウェアや SecurID というトークンカードによって、使い捨てパスワードを利用できます。ただし、S/Key ではパスワードのための文字列が毎回計算され、SecurID では PIN（Personal Identification Number）の入力が必要となるなど、実際の利用には手間がかかります。しかし、セキュリティのためには必要だと考えるべきだと思います。

# 4 情報に対するセキュリティ

ここでは、情報のセキュリティに関係する次の事柄を説明します。

- 情報の改ざん（4.1 を参照）
- 踏み台（4.2 を参照）
- ハッカー（4.3 を参照）
- 盗聴（4.4 を参照）
- メール（4.5 を参照）
- オンラインショッピングの安全性（4.6 を参照）

## 4.1 情報の改ざん

ハッカーに侵入され Web ページの内容が改ざんされても問題はないと言う人がいます。このような人たちは、Web ページの内容が重要なものでなかったり、手元のコピーを使って簡単に内容を復元できたり、誰も読んでいないなどの理由から安心しているようです。ただし、改ざんされた内容が競合企業の悪口だったり、ウィルスを仕掛けられたり、新聞などに取り上げられてしまったりしたときには、Web ページの内容が改ざんされたという問題だけではなくなってしまいます。このため、情報が改ざんされたときの影響を考えてサーバを管理していく必要があります。

## 4.2 踏み台

踏み台とは、他のシステムに侵入するために利用されることです。ハッカーは、いくつかのシステムを踏み台として利用することで、アクセス経路を追跡しづらくしています。踏み台にされただけでは、システム自体に被害は発生しません。ただし、侵入先のシステムからは侵入者のシステムのように見え、犯人扱いされてしまうことがあります。

## 4.3 ハッカー

世の中には、ハッカーは尊敬に値する研究者のことであり、システムの破壊者はクラッカーだという意見があります。ただし、マスコミなどが破壊者を表すために「ハッカー」という語を使い、現在では多くの人々がハッカーをシステムの破壊者と認識してしまっています。このため、この講演では、システムの破壊者をハッカーと呼んでいます。

ハッカーは、次の 3 種類に分かれます。

- 産業スパイなどのプロフェッショナル
- 自らの技術を試したくなった研究者
- 犯罪であることの認識がなく、手に入れた情報を試したくなった模倣犯

## 4.4 盗聴

インターネット上での盗聴に関しては、次のようなウワサがあります。

- ハッカーが多数存在している。
- インターネットはバケツリレー方式である。
- 国家レベルで監視されている。
- 社内 LAN では容易に盗聴できる。

このようなウワサのいくつかは真実ですが、残りは誤りです。それは、インターネットの利用が商用化され、ネットワークの構成や管理体制が従来とは異なるものとなったためです。

このようなウワサでは、メールやクレジットカード番号などのあらゆる通信の内容がインターネット上で盗聴されていると言われています。そして、このような情報の盗聴は、次のようなさまざまな場所で実行される可能性があります。

- 社内 LAN
- 接続している ISP*
- 経路の ISP
- 相手の社内 LAN
- 通信会社
- サーバ

---

ISP　「Internet Service Provider」の略で、インターネットへの接続サービスを提供する事業者です。

---

前述のウワサのうち、「インターネットはバケツリレー方式である」というものは、現在では誤りです。現在のインターネットでの通信は、図 1 に示すように、通信する 2 台のコンピュータがエンドツーエンドで直接通信するため、一時的にでも、どこかに通信内容が保存されることはありません。そして、ネットワーク上で通信を盗聴するのは技術的にかなり難しいのです。また、メールも、途中にサーバが介在せずに送信側のサーバと受信側のサーバが通信するので、盗聴のためにはメールの内容が保存されているメールサーバが狙われることになります。

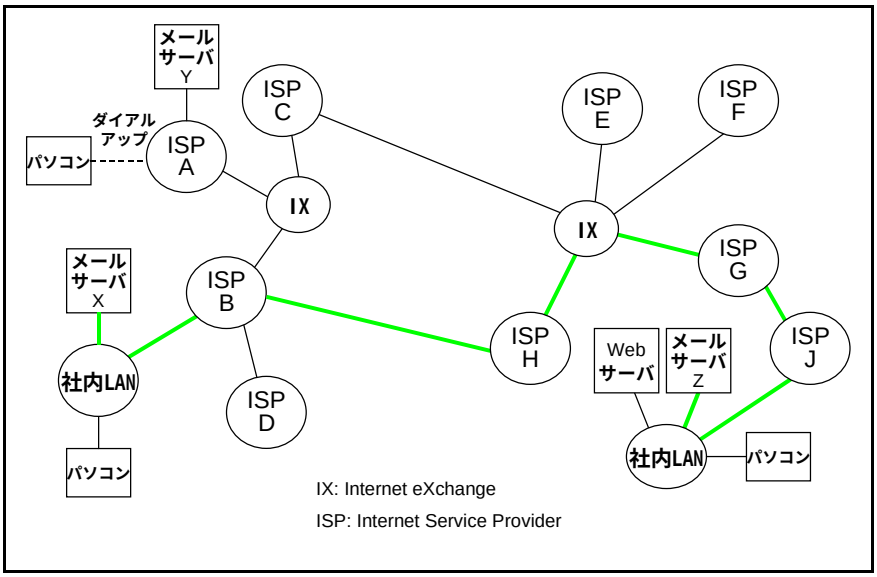


**図 1：インターネットのしくみ**

これに対して、もう 1 つの「社内 LAN では容易に盗聴できる」というウワサは真実です。社内では 1 つの Ethernet ケーブル上にあらゆるデータが流されているため、簡単に盗聴することができます。また、盗聴したデータを解析するソフトウェアさえも存在しています。

この問題は、スイッチングハブ * を利用して不要なポートにデータを流さないようにしたり、ルータ * によってネットワークを分割することで、ある程度防ぐことができます。それでも、ネットワーク上を流れるメールやパスワードなどの生データが盗聴される可能性は残ります。

---

**スイッチングハブ**　スイッチング機能を持つ集線装置です。スイッチングハブでは、データは送信先の端末が接続されているポートに対してのみ送られます。

**ルータ**　異なるネットワークアドレスを持つ LAN 間を接続する装置です。ルータでは、IP アドレスによってデータの中継経路が制御されます。

---

これまでにも示してきたようにインターネット通信路上での盗聴は、国家や通信会社の職員が荷担しないかぎり容易には実行できません。ただし、絶対に盗聴されないという保証はないため、データを守るようにはすべきです。このために重要なデータはインターネット経由では送らないという方法も考えられますが、電話回線による通信はより危険な方法です。実際には、通信路や電文を暗号化することで、盗聴からデータを守るようにします。

実際にインターネットを介した通信路に暗号化技術を利用したものが、図 2 に示す「VPN（Virtual Private Network）」です。

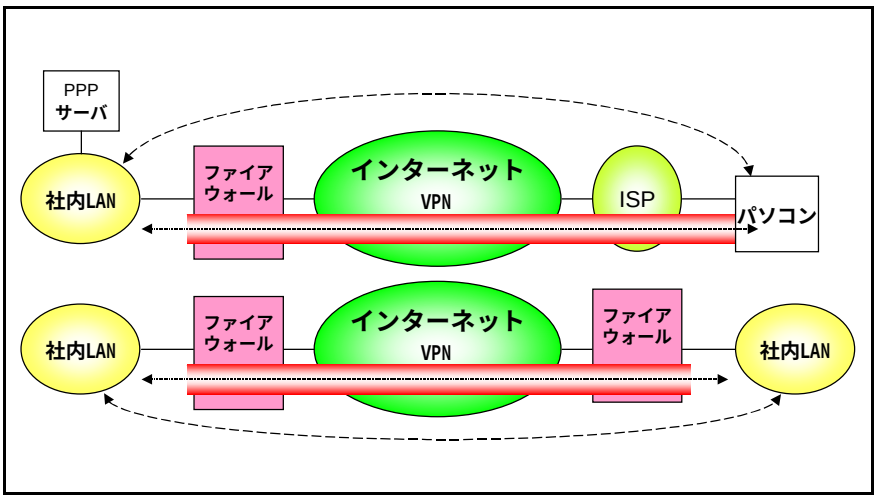


**図 2：VPN の構成例**

VPN は、あたかも専用線のように利用され、ネットワークとネットワーク、ネットワークとコンピュータ、コンピュータとコンピュータといったさまざまなパターンで接続されています。VPN を利用することで、次のようなメリットが得られます。

- 専用線に比べて通信費が削減される。
- 社外から安全に通信できる。

ただし、VPN を利用することで、接続相手側の危険性がそのまま社内のネットワークにまで及ぶ可能性もあります。たとえば、接続相手先のパソコンのセキュリティが社内 LAN よりも低かったときには、VPN を利用したことでシステム全体のセキュリティが低下してしまいます。また、エクストラネットとして他社の社内 LAN と VPN によって接続したときには、あらゆる社内情報が相手先企業によって参照されてしまう可能性があるため、公開する情報を適切に管理しなければなりません。

## 4.5 メール

現在、多くの企業でメールが利用されてきていますが、メールには次のような問題があります。

- 電文が暗号化されていないため、盗聴しやすい。
- 発信者を確認できないため、なりすましやすい。
- 書き替え可能なため、改ざんしやすい。

このような問題を回避するために、PGP（Pretty Good Privacy）や S/MIME（Secure Multipurpose Internet Mail Extensions）による暗号化メールが提供されています。このような暗号化メールでは、共通鍵暗号方式（後述）によって図 3 のように電文を暗号化し、盗聴の危険性を回避しています。

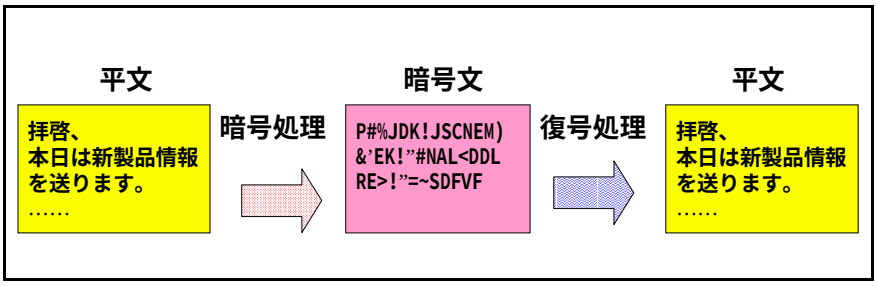


**図 3：電文の暗号化による盗聴の防止**

また、公開鍵暗号方式（後述）とメッセージダイジェストによる電子署名を図 4 のように利用することで、発信者の確認と改ざんの検出を実現しています。

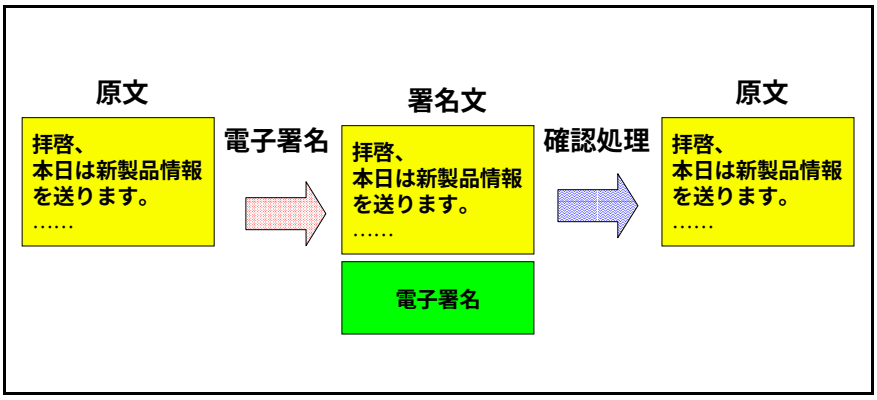


**図 4：電子署名による発信者の確認と改ざんの検出**

次に、暗号化メールで電文を暗号化するために利用される「共通鍵暗号方式」について説明します。

共通鍵暗号方式では、図 5 に示すように、発信者による暗号化と受信者による復号に同一の鍵が使用されます。

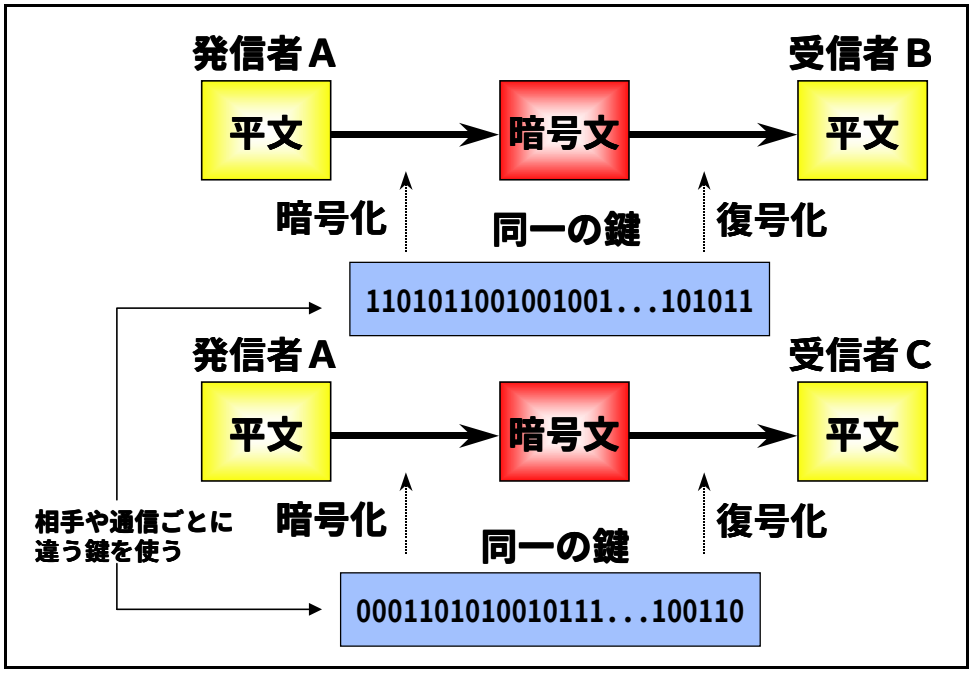


**図 5：共通鍵暗号方式**

共通鍵暗号方式は、処理速度が速いため大量データを短時間で処理できます。ただし、発信者と受信者で同一の鍵が使用されるため、相手ごとに異なる鍵を用意したり、ネットワーク上で安全に鍵を交換したりする方法が必要となります。

また、現在の技術では 40 ビット鍵長の暗号を総当たり方式によって 5 ～ 6 秒で解読できてしまうため、暗号鍵の長さや強度が問題となります。このような共通鍵暗号方式の代表的なものには、DES、TripleDES、ISEA、RC2、RC4、MISTY、FEAL、CAST などがあります。

引き続き、「公開鍵暗号方式」について説明します。

認証と共通鍵の暗号化のために利用される公開鍵暗号方式では、図 6 に示すように、暗号化と復号に異なる鍵が使用されます。

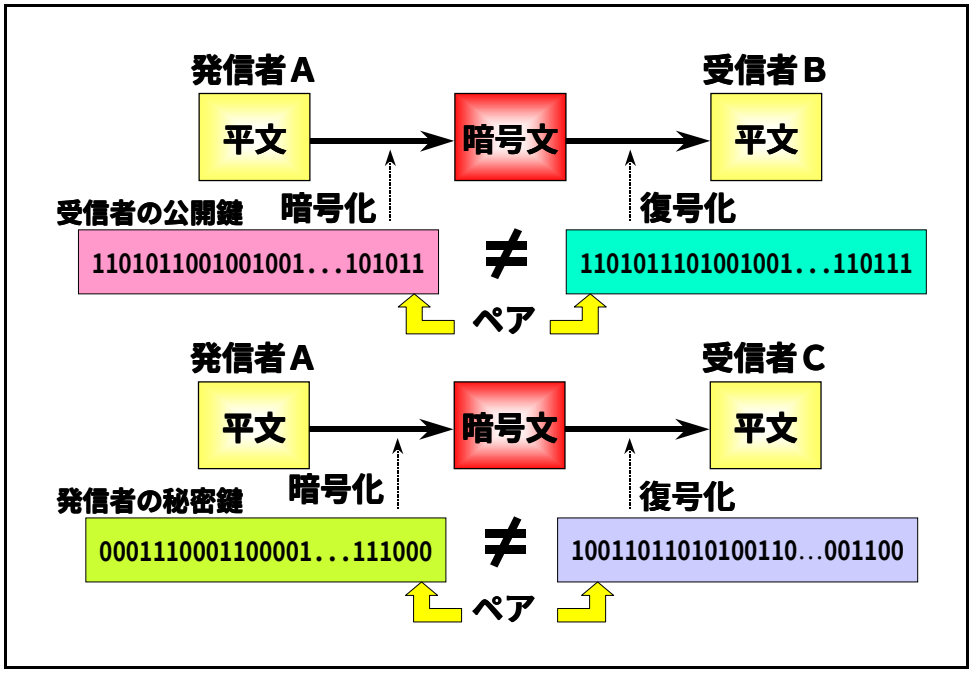


**図 6：公開鍵暗号方式**

公開鍵暗号方式では、公開鍵と暗号鍵という 1 対の鍵が利用されます。そして、公開鍵で暗号化されたものは秘密鍵でのみ復号でき、暗号鍵で暗号化されたものは公開鍵でのみ復号できます。たとえば、上図のように受信者の公開鍵で暗号化した文は、秘密鍵を持つ受信者しか復号できないため受信者を特定できます。また、発信者の秘密鍵で暗号化された文は、発信者の公開鍵でのみ復号できるため発信者を特定することができます。

このような公開鍵暗号方式は、共通鍵暗号方式に比べ処理速度が遅いため、メッセージ全体を暗号化するには不向きです。また、公開鍵暗号方式でも鍵の強度が問題となります。現在、公開鍵暗号方式での強度を保つためには、704 ビット以上の鍵長が必要だと言われ、米国内では 1024 ビットのものが利用されていますが、米国から日本に輸出できるものは 512 ビットまでとなっています。このような公開鍵暗号方式の代表的なものには、RSA、Diffie-Hellman、EIGamal などがあります。

電子メールに対する改ざんを検出するために利用される「メッセージダイジェスト」は、原文に対して特定の計算処理を実施することで得られた 128 ビットや 160 ビットの文字列です。メッセージダイジェストは、原文の内容がわずかでも変化すると異なる結果となります。また、同一のメッセージダイジェストを得るように原文を変更することは非常に困難なものとなっています。このようなメッセージダイジェストを生成する代表的な方法には、SHA-1 や MD5 があります。

ここまでに示してきた共通鍵暗号方式、公開鍵暗号方式、メッセージダイジェストを次のように利用することで、暗号化メールが実現されています。

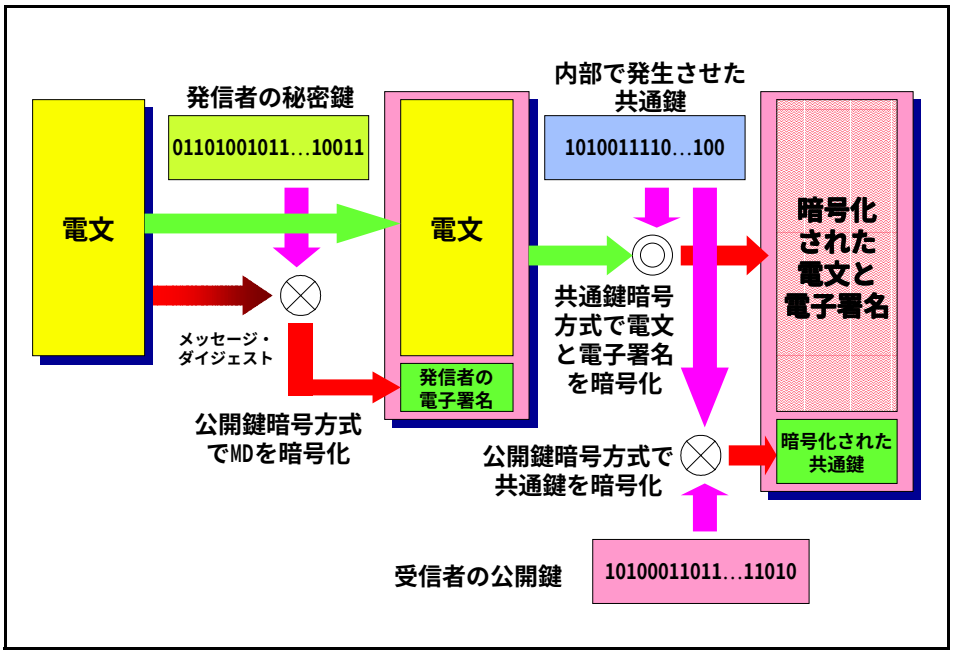


**図 7：暗号化メールのしくみ**

まず、発信者は、電文のメッセージダイジェストを生成し、発信者の秘密鍵によって暗号化することで電子署名を作成します。そして、電文と電子署名を一時的に生成した共通鍵で暗号化した後、その共通鍵自体を受信者の公開鍵で暗号化します。このような手順で暗号化した電文、電子署名、共通鍵を受信者に送ることで、秘密鍵を持つ受信者のみが共通鍵を復号し、電文と電子署名を取り出せるようになります。また、受信者は、受け取った電文からメッセージダイジェストを生成した後、添付されていた電子署名を発信者の公開鍵で復号したものと照合することで、電文の発信者や改ざんの有無を確認できます。

このような暗号化メールでは、公開鍵をどのように配布するかが課題となります。たとえば、公開鍵自体をメールで送ると改ざんされる可能性がありますし、直接対面して手渡ししたときには配布できる範囲が限られてしまいます。この問題は、CA（Certification Authority）や認証局と呼ばれる証明書発行機関が、第三者として公開鍵に対して電子署名を実施し、その正当性を証明することで解決されます。

これまでに示してきた暗号化は、犯罪者やテロリストの情報さえも守ることができ、国家や軍事に対する影響も大きなものであるため、暗号化技術の国外持ち出しや利用にはさまざまな制限が設けられています。このため、一般ユーザが高強度な暗号化技術を利用できないこともありますが、インターネットビジネスの普及を阻害してしまうため、その制限は徐々に緩められています。

## 4.6 オンラインショッピングの安全性

オンラインショッピングを提供する Web サイトによっては「当サイトは SSL 対応なので安心してショッピングしていただけます」などというメッセージを表示しているものがあります。この SSL とは、Secure Sockets Layer の略で、Netscape Comminications 社によって開発され、共通鍵暗号方式と公開鍵暗号方式を利用した技術です。オンラインショッピングなどでは、SSL を利用することでクレジットカード情報などを暗号化して受け渡しています。

オンラインショッピングでは、SSL によって通信路中での盗聴はかなり困難なものになりますが、ショッピングサイトに情報が届いてからが問題となります。たとえば、ショッピングサイトのサーバが侵入され情報が盗まれたり、従業員が顧客データを持ち出したりしてしまう可能性があります。実際に Web サーバ上に直接クレジットカード情報を保存している企業もあるようです。このため、オンラインショッピングでは、信用があり技術力を持った企業のショッピングサイトのみを利用すべきだと思います。

先ほど示したように、図 8 のような構成では、不正アクセスによってデータベースの情報が盗まれてしまう可能性があります。

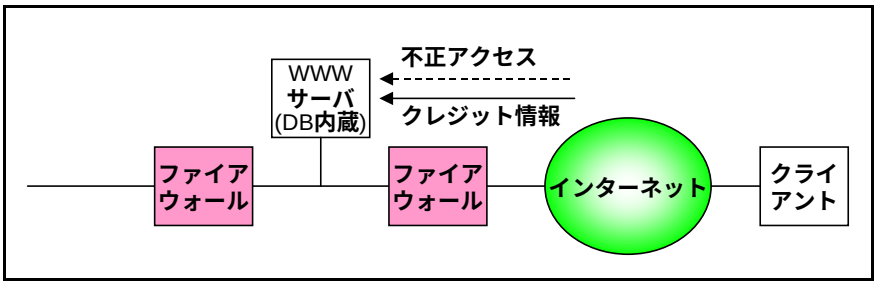


**図 8：危険な構成例**

これに対して、図 9 のようにデータベースサーバをファイアウォールの内側に設置することで、不正アクセスを防止できます。

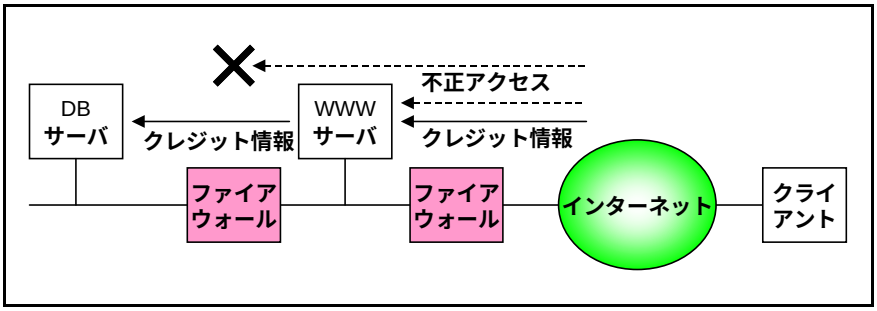


**図 9：一般的な構成例**

SSL やショッピングサイトの適切な構成によってクレジットカード情報は保護されます。ただし、クレジットカードによる買い物では、購入した商品の内容がカード会社に通知されユーザの嗜好が収集されます。さらに、収集したユーザの嗜好を販売している会社も存在しています。同様に同一サイトで買い物を続けていると、個人情報が収集されていきます。このような情報の収集によって、個々のユーザの好みに合わせたサービスを受けることもできますが、その危険性も意識しておく必要があると思います。

# 5 サーバに対するセキュリティ

ここでは、サーバのセキュリティに関係する次の事柄を説明します。

- ファイアウォール（5.1 を参照）
- システム運用（5.2 を参照）
- セキュリティホール（5.3 を参照）
- ログ管理（5.4 を参照）

## 5.1 ファイアウォール

先ほど示したように、外部からアクセスできるサーバは、不正アクセスの対象となる可能性があります。このときには、セキュリティホール、設定ミス、不適切な CGI の利用などによって不正アクセスが実行されます。また、ファイアウォールによって特定のポートのみを有効としていても、不正アクセスの対象となり攻撃される可能性があります。このため、ファイアウォールに対する適切な知識を得て、正しい設定を行い、確実に監視しておくことが必要です。

火災発生時にのみ機能して延焼を食い止める防火壁と同様に、ファイアウォールは、インターネットに安全に接続するための解決策となっています。ファイアウォールの利用は、大きく次の 2 つに分けられます。

- 必要な通信のみを通す。
- 危険な通信を止める。

ファイアウォールをどこに設置し、何を通過させたり拒否したりするかは、ネットワークの使い勝手と安全性を考慮して管理者が適切に設定する必要があります。また、社内 LAN をインターネットに接続するときには、次のような要求を満たす必要があります。

- 各種サーバはインターネットとの通信が必要。
- 社内からもインターネットにアクセスしたい。
- メンテナンスのために社外からもアクセスしたい。

このような要求のうち、1 番目の「各種サーバはインターネットとの通信が必要」という要求には、SMTP*、DNS*、HTTP* などの必要最低限の通信のみを許可し、telnet* や ftp* などの不要と思える通信は許可しないようにします。

また、2 番目の「社内からもインターネットにアクセスしたい」という要求に対しては、インターネットへの直接通信は許可せずに必ず Proxy サーバ * を経由するようにし、ログを残して問題の発生に備えるようにします。さらに、「メンテナンスのために社外からもアクセスしたい」という要求に対しては、次のような処置によって不正アクセスの発生を防ぐようにします。

- 通信路の暗号化
- 接続時のワンタイムパスワードの利用
- IP アドレスによるフィルタリング *

| | |
|---|---|
| SMTP | 「Simple Mail Transfer Protocol」の略で、電子メールを他のマシンに転送するためのプロトコルです。 |
| DNS | 「Domain Name System」の略で、ネットワーク上でホスト名と IP アドレスの対応関係を提供するサービスです。 |
| HTTP | 「HyperText Transfer Protocol」の略で、Web サーバと Web ブラウザが情報を受け渡すために使用するプロトコルです。 |
| telnet | 「telecommunication network」の略で、リモートで仮想端末機能を実現するためのプロトコルです。 |
| ftp | 「file taransfer protocol」の略で、ネットワーク上でファイルを転送するためのプロトコルです。 |
| Proxy **サーバ** | インターネット上のサービスへのアクセスを中継するソフトウェアやサーバマシンです。 |
| **フィルタリング** | 特定の条件に合ったものだけを通過させる処理です。 |

また、ファイアウォールの設置にも、図 10 のようにさまざまな方法が考えられます。

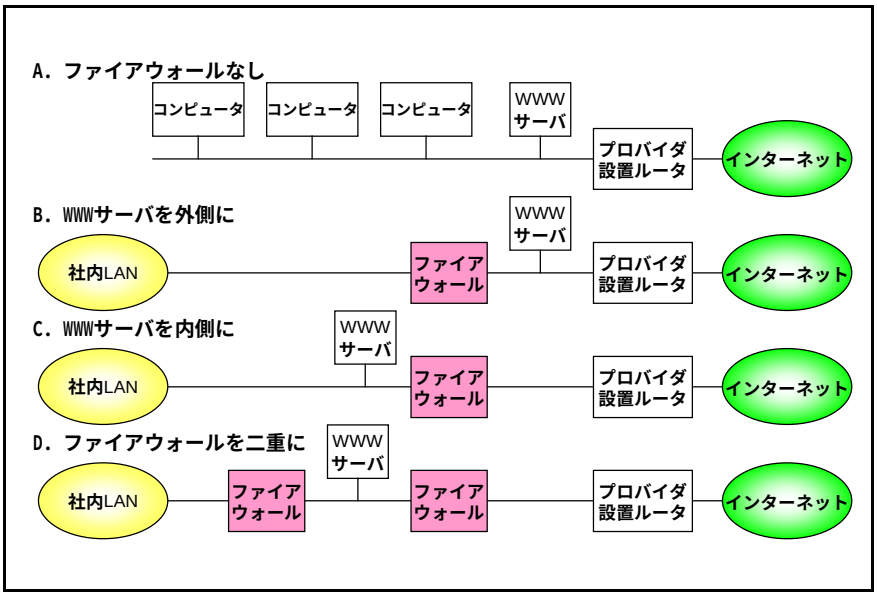


**図 10：ファイアウォールの設置例**

設置例のうち 1 番目のもの（A）は、ファイアウォールを設置せずにプロバイダが設置したルータでフィルタリングしています。このような利用は、設置したルータの管理者権限がユーザに提供されているときにのみ利用できます。

また、2 番目の例（B）はファイアウォールの外側に外部アクセス用サーバを設置し、3 番目の例（C）はファイアウォールの内側に外部アクセス用サーバを設置しています。さらに、最後の設置例（D）では、二重化したファイアウォールの間に外部アクセス用サーバを設置しています。

一般には、このようなファイアウォールの設定のうち最後に示した「二重化したファイアウォールの間に外部アクセス用サーバを設置する」方法が利用されています。この方法によって設定される中間部分は、非武装地帯を表す DMZ（De-Militalized Zone）と呼ばれています。

DMZ では、図 11 に示すように DMZ 内に設置されたサーバを経由するアクセスのみが許可され、社内 LAN とインターネットの双方の直接アクセスはファイアウォールによって禁止されます。

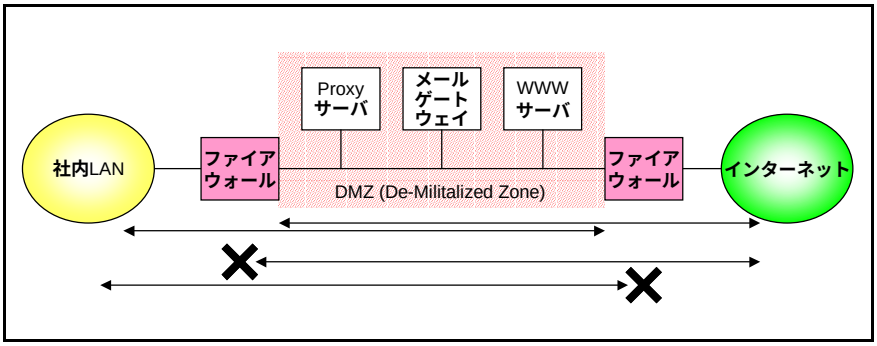


**図 11：DMZ によるアクセス例**

また、DMZ は、図 12 のように 1 つのファイアウォールによって設定することもできます。

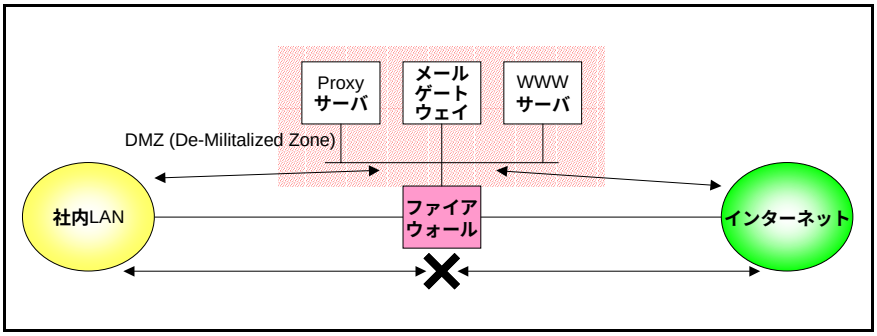


**図 12：1 つのファイアウォールによる DMZ の設定**

ただし、ファイアウォールを設置しただけでは安全は守れません。不正アクセスのための手段は日々進化しているため、ファイアウォールによる守り方も進化させる必要があります。また、セキュリティホールがあるファイアウォール製品も存在しているため、機能、性能、使い勝手、信頼性などから適切なファイアウォール製品を選択する必要があります。さらに、常にセキュリティ情報に注意し、ログを確認して不正アクセスが発生していないことを確認し続ける必要もあります。そして、このような作業が困難であるときには、専門家に任せるようにすべきです。

また、このようなファイアウォールに対する作業とともに、フェイルセーフという考えに基づいて、ファイアウォール自体が機能しなくなっても安全を保てるようにします。たとえば、tcpwrapper というソフトウェアをファイアウォールと併用することで、telnet や ftp などのプロトコルに対する処置を二重化することができます。

実際に社内 LAN とインターネットを接続すると、RealPlayer*、IRC*、telnet、NetMeeting* などの利用をユーザから要求されるようになります。ただし、このようなさまざまな通信を許可することは、ファイアウォールの弱点となる「穴」を開けることになり、不正アクセスの対象となる可能性を増やします。また、これらのソフトウェアによる通信では広帯域が要求されるため、ネットワークを圧迫し業務に支障をきたすことも考えられます。

通信のためにファイアウォールに開けられた「穴」は、ポートスキャンによって探され、不正アクセスの対象となることがあります。ポートスキャンでは、DNS によって見つ出したサーバのポートを順番にアクセスしていき、応答するサーバを探し出そうとします。現在、ポートスキャンを実行するフリーウェアなどが配布されてるため、誰でも簡単にポートスキャンを実行できてしまいます。このため、常にログを参照して、ポートスキャンされたかどうかを確認しておく必要があります。

また、実際の運用では、次のような危険な社内 LAN がインターネットに多数接続されています。

- ファイアウォールが、予算がないために購入されていなかったり、購入したときのままでいっさい設定されていなかったりする。
- 複数のメンバーで管理しているため、同一のパスワードを使ってリモートログインしている。
- 内容がわからないのでログファイルは見ていない。

---

| | |
|---|---|
| RealPlayer | インターネット上で音声や動画をオンライン再生するためにリアルネットワークス社が提供しているソフトウェアです。 |
| IRC | 「Internet Relay Chat」の略で、インターネット上で文字による会話をリアルタイムに実現するためのソフトウェアです。 |
| NetMeeting | インターネット上でビデオ会議などを実施するためにマイクロソフト社が提供しているソフトウェアです。 |

---

## 5.2 システム運用

不正アクセスによる侵入や破壊からシステムを守ることだけがセキュリティではありません。ディスク障害や停電によってシステムが停止してしまうと業務に支障をきたすため、常にシステムを安定して利用できるようにすることもセキュリティ上の重要な課題です。このためには、システム維持のための適切な予算を確保し、故障しにくい機器と故障しても停止しないしくみを作り上げる必要があります。また、万が一システムが停止したときのために、短時間で復旧するしくみ、手順、体制をあらかじめ作成しておくようにします。

さらに、インターネットは、その開発動機の 1 つに核攻撃によって一部が破壊されても全体の運用に支障が生じないようにするというものがあったようです。ただし、現在の商用インターネットは複数の ISP によって運営されている状態ですので、核攻撃だけでなく地震や広域に渡る停電が発生したときには、その運用が難しくなると思えます。

したがって、システムを安定して利用し続けられるようにするためには、故障しやすそうな部分を二重化しておくようにします。すべてを二重化すると費用も 2 倍になってしまうため、故障の発生する確率と費用対効果から適切な箇所のみを二重化するようにします。

## 5.3 セキュリティホール

セキュリティホールは、本来存在しないはずのプログラムのバグです。このようなバグでは、特定のデータなどを受け取ると、予期しない動作が発生してしまいます。ハッカーは、このような不測の動作を利用してシステムに侵入したり特定の命令を実行したりします。セキュリティホールは、安全設計が不十分であったときに開発時からプログラム内に存在してしまいます。また、プログラムの規模が大きくなるほど、その発見は難しくなっていきます。

現在、セキュリティホールは、発見されたときではなく、対策方法が確立した後に公表されています。これは、対策方法が確立する以前に公表してしまうと、そのセキュリティホールを悪用した不正アクセスが多発する可能性があるためです。このようなことからも、セキュリティホールが公表されたときには、できるかぎり速やかに対策を講ずる必要があります。セキュリティホールに関する情報は次の場所から入手できます。

- CERT/Coordination Center（*http://www.cert.org/*）
- JPCERT/CC（*http://www.jpcert.or.jp/*）

## 5.4 ログ管理

すでに示したように、システムを運用していくときにはログへの記録が重要となります。また、どの情報を記録することでどのようなことが可能となるかを検討しながら、ログを記録するようにします。

たとえば、次のようなアクセス状況をログとして記録しておくようにします。

- PPP アクセス
- メール送受信
- Web アクセス
- 機密情報アクセス
- 管理権限アクセス

このようなログ情報によって、次のような状況を把握できます。

- 利用状況の確認
- 混雑状況の把握
- 不達メールの確認
- 不正利用の犯人特定

# 6 まとめ

次のような項目によって、安全を守ることができます。

- パスワードを守る。
- パスワードを共有しない。
- 必須な利用に留める。
- 危険な使い方を避ける。
- 外部からのアクセスは最低限しか許さない。
- セキュリティホールをふさぐ。
- アクセスログを残す。
- セキュリティ情報を常時把握しておく。
- 危険を発見したらすぐに対応する。

このような項目を実現するための具体的な方法は、システムの構成、運用ポリシー、予算などによって異なってくるため、個別に検討していく必要があります。