情報処理演習

情報倫理とセキュリティ

目次

- インターネットの危険性
- メール利用時の注意
- WWW利用時の注意
- 暗号化技術
- ファイルの保存方法

情報セキュリティ

- インターネットの危険性
  - 直接攻撃によるもの
  - 電子メールを媒体とするもの
  - Webのページを使うもの
- セキュリティホールとポートスキャン
  - セキュリティホールを自動的にスキャン
  - もしあれば自動的に攻撃して、コンピュータを乗っ取る

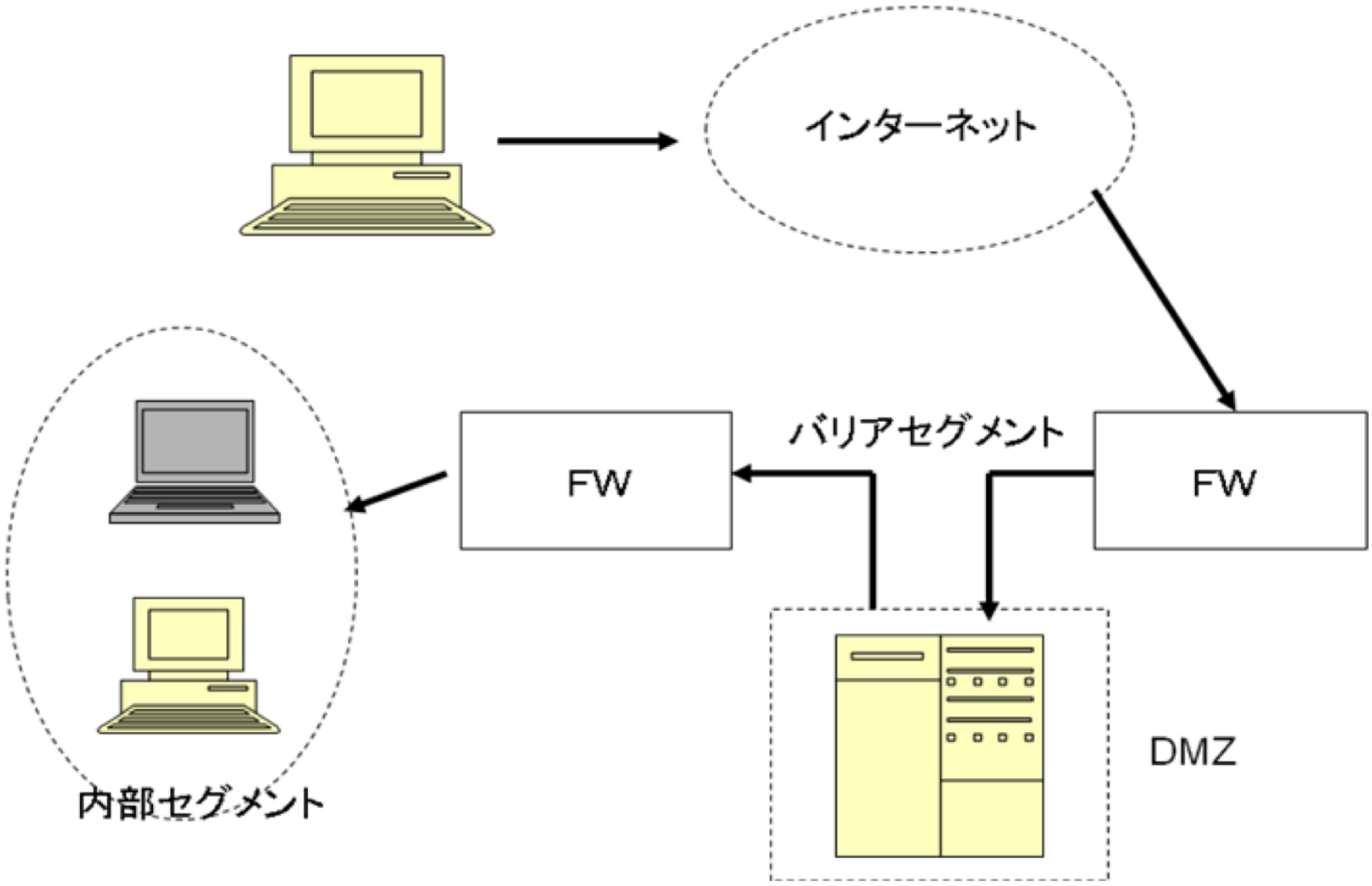
ファイヤウォール

- 目的
  - インターネットの外部から内部への不正なアクセスを防止
  - 内部から外部への不正なデータ漏洩を防止
- 組織レベル
  - 対外接続のところで外部との通信を規制
  - IPアドレスやポート番号で通信を制御
- 個人レベル
  - 家庭用のブロードバンドルータの設定
  - パーソナルファイヤウォールの使用

DMZ

- 外部と内部の間の緩衝地帯
- 外部と内部の両方からアクセスできるが、外部から内部へは直接アクセスできない
- 外部向けのサーバなどを設置

DMZの概念図



IDS

- セキュリティホールを利用した一連の攻撃シーケンスを検出
- 人間が気がつかないようなコマンドとコマンドの間が長期間に渡る攻撃シークエンスも検出可能
- ログが多量にでる

パスワード

- コンピュータの正当な利用者であることを証明する情報
- 他人に漏れると、
  - ファイルを改ざんされたり、
  - 情報漏洩が起こったり、
  - 他のコンピュータの攻撃の踏み台に使われる
- 絶対に人には教えてはいけない
  - メモしたり、張り紙をしては駄目

パスワードの推測方法

- 個人レベルでは
  - 紙に書かれている利用者IDとパスワードを見る、盗む、拾う
  - 名前、誕生日、趣味などをベースに推測
- 組織的には
  - 暗号化されているパスワードファイルを入手し、パスワードを破る

組織的なパスワードの破り方

- 不正アクセスなどでパスワードファイルを入手
- 英単語の辞書、パスワードに使用しそうな単語類を暗号化し、パスワードファイルの暗号化された文字列と比較
- もし同じ文字列になっているものがあれば、元の文字列がパスワード

- 専用のプログラムがあり、結構、簡単に破れる

スパイウェア

- ユーザのキーボードやマウスからの入力情報、あるいはブラウザで見て回ったサイトの閲覧情報など、ユーザの使い方に関する情報を収集して、漏洩
- キーボードロガー
  - オンラインバンキングなどの情報
  - ソフトウェアキーボードで対抗
- ウイルス対策ソフトウェアなどで検出・排除

ウイルス

- 利用者の意図とは無関係に望ましくないことを行うプログラム
- ウイルスの侵入を「感染」、活動開始までを「潜伏」、活動開始すると「発病」
- 感染経路
  - メールの添付ファイル
  - Webの利用
  - 外部記憶装置を経由して感染
- デマメールもある
  - 無視すれば実害はないが、素人はだまされる

ウイルス感染の症状

- 余計な文字を表示
- 画面上の文字が崩壊
- アイコンが変わる
- ハードディスク内のデータを破壊
- システムの動作を不安定にする
- 動作が遅くなる
- メモリが足りなくなる
- メールを勝手に送信し、ファイルを添付して、情報漏洩がを生
- 外部からコンピュータを操作できるようにし、他のコンピュータを攻撃する踏み台にする
- ログイン名やパスワードを密かに記録しメールで外部に送信し、情報漏洩を起こす

ウイルス対策ソフトウェア

- PCには必ずウイルス対策ソフトウェアを導入
- 定期的にパターンファイルを更新
- 外部から持ち込んだ外部記憶装置（CD、DVD、USBメモリ、SDメモリなど）は必ずウイルスチェックを行ってから使用
- 外部記憶装置を接続した時にプログラムを自動的に実行する機能はoffに設定

SPAMメール

- 不要なメール（ゴミメール）
  - 世界中の9割のメールがゴミ！
  - 宣伝、アダルトサイトへの勧誘、フィッシング詐欺
- SPAMフィルターで排除
  - 組織としてのSPAMフィルター
  - ウイルス対策ソフトについているSPAMフィルター
- Webページなどに不用意にメールアドレスを書くと届くようになる

システムソフトウェアの更新

- Windows XPやVistaではWindows Update
- Mac OS Xでは、リンゴマークの中に「ソフトウェア・アップデート」
- Linuxではシステムアップデート
- 自動的に更新にしておくと良い
- いずれにしてもこまめに実行することが必要

メールの作法

- 依存しすぎないこと（電話、FAX、郵便）
- メールは100%確実な通信手段ではない
- 送信相手を間違えないこと
- 文章に十分注意して書くこと
- 添付ファイルの大きさに注意
- 添付ファイルを不用意に開かないこと

Web利用時の注意

- 重要な通信には暗号化通信（SSL=HTTPS）
- ブラウザの鍵マークに注意
- アドレス部分のURLに注意
- フィッシング詐欺に注意
  「本物」
- オンラインショッピング、オンラインバンキング
  - 暗唱番号、クレジット、支払い方法、個人情報

掲示板、ブログ

- 情報発信のコストが劇的に低下
- 誰でも気軽に情報発信可能
- ネットワーク上では誰でも１人前
- 「してはいけないことは、してはいけない」
- 通信は記録されている

著作権関連

- Webページのイメージや文章を情報をそのまま使うと著作権法違反
- 「五年以下の懲役若しくは五百万円以下の罰金に処し、又はこれを併科する。」
- WinMX、Winny、Napstere、Donkey2000、Gnutella、KaZaAなどのP2Pファイル
  - 知らない間に著作権法違反を幇助
- 文章は引用であることを明記、出所を明示

暗号化

- 必要性
  - インターネットでは平文で通信するので、情報は漏れる
  - 発信人や受信人を保証する必要がある
  - 内容が改ざんされていないことを保証する必要がある
- 暗号化には2種類
  - 秘密鍵暗号（共通鍵暗号、配布が難しい）
  - 公開鍵暗号（暗号化と複合化の鍵が異なる、配布の問題なし）

公開鍵暗号

- 暗号化と複合化とで異なる鍵を使用
- 公開鍵（public key）と秘密鍵（private key）
- RSA暗号が有名で広く使用
- AからB宛の時には
  - AはBの公開鍵で暗号化
  - Bは自分の秘密鍵で複合化
- 計算に時間がかかる

電子署名

- 送信人と受信人を保証（A→B）
  - Aさんは、Aさんの秘密鍵とBさんの公開鍵で暗号化
  - Bさんは、Aさんの公開鍵とBさんの秘密鍵で複合化
- 内容を保証
  - 本文をMD5などのハッシュ関数で計算
  - この値をメールに添付
  - 復号化した後で再度計算して、値を比較

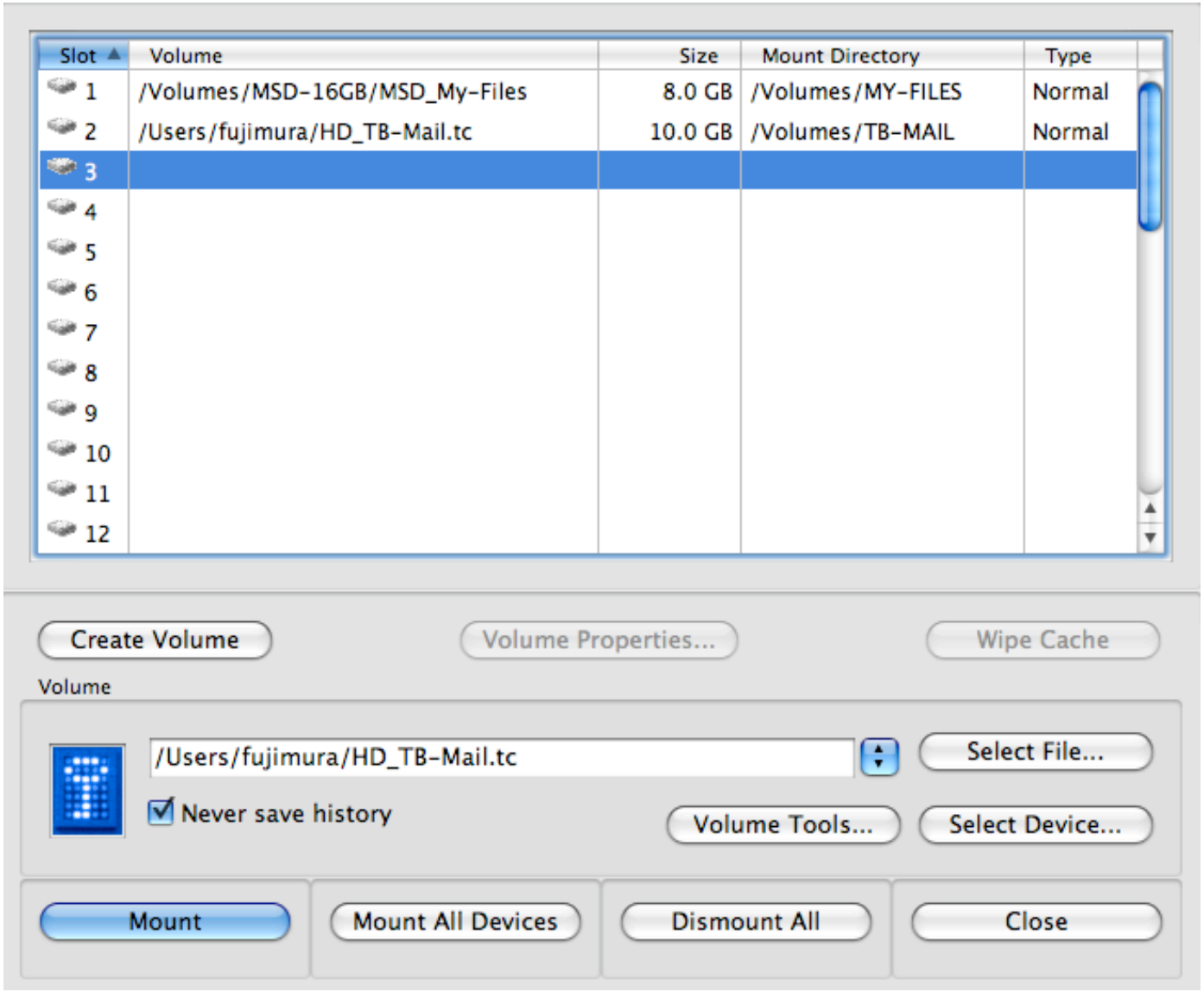
ファイルの安全な保存

- パソコンの内蔵ハードディスクにファイルを保存すると、故障した時に困る
- 取り外し可能な記憶装置に保存すると、故障したら取り外すだけで済む
- ただし紛失、盗難に備えて、暗号化ボリュームを活用する
  - 正しいソフトウェアとパスワードがないと読み書きできない
- こまめにバックアップを取る

TrueCrypt

- http://www.truecrypt.org/
- Windows、Mac OS X、Linuxで使える
- オープンソース
- 大きなファイルを作成し、一つの仮想的なボリュームとして扱える
- パスワードを指定して、マウントしない限りただの巨大ファイルにしか見えない

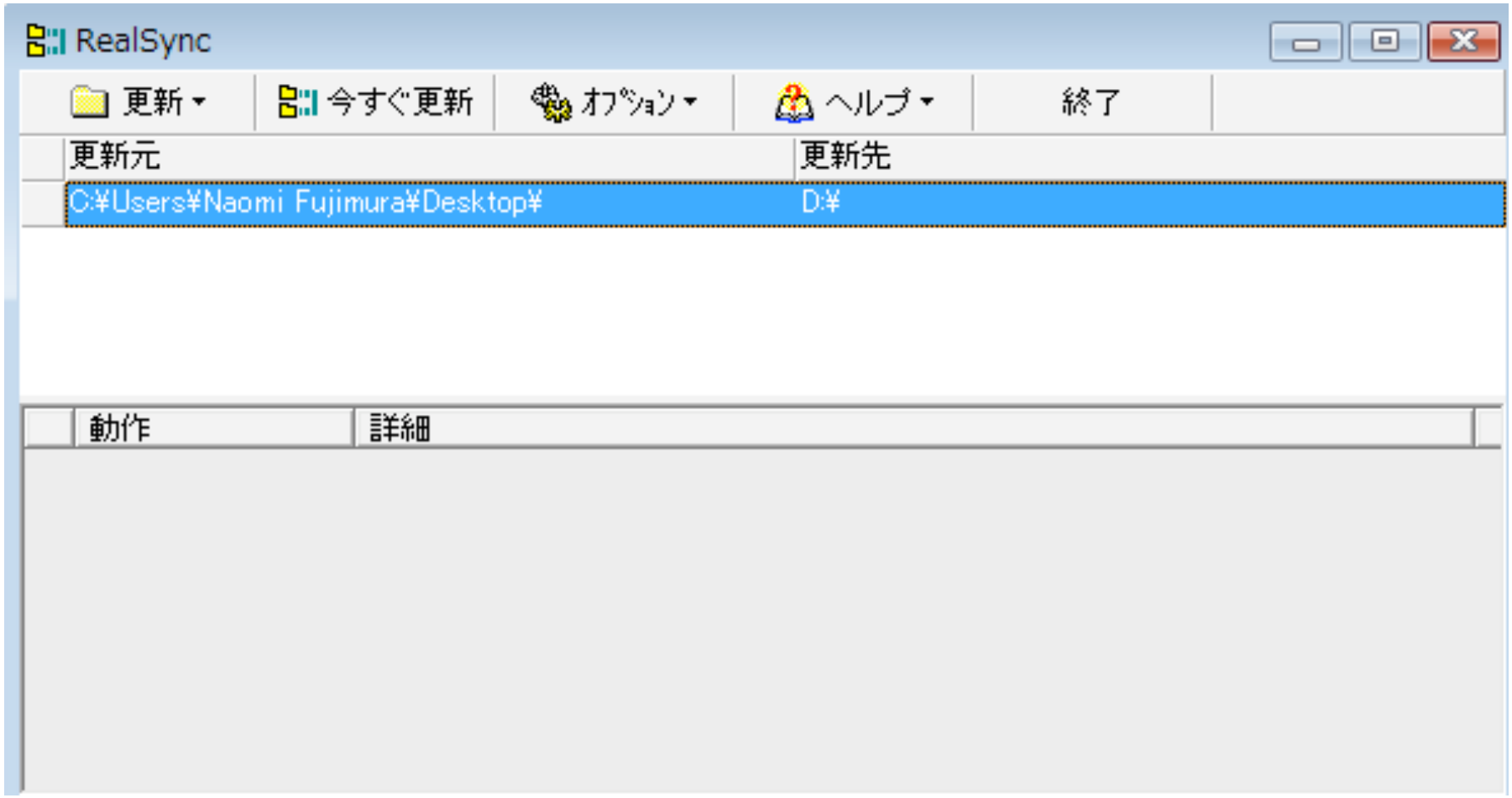
TrueCrypt画面例



バックアップ

- MacとLinux
  - rsync
  - http://rsync.samba.org/
- Windows
  - realsync
  - http://www.takenet.or.jp/~ryuuji/realsync/

Realsync画面例



1. 情報セキュリティ、情報倫理

1.1. インターネットの危険性について

インターネットを利用する上で、快適さや使い易さと安全性は基本的に相反する関係にあります。例えば、ブラウザなどを使いやすくすると安全性が低下し、安全性を高くすると使い勝手は悪くなります。日常的にはこれらのバランスをどうするかが大事です。そうは言っても守るべきものは守らないといけません。ただその場合にも、何を、何から、どれだけコストをかけて守るかという判断が必要です。まずは問題点とその対策を理解し、適切なバランスで使いこなしてください。

外部からの攻撃について見ると、次のような攻撃形態があります。

- 直接攻撃するもの
- 電子メールを媒体とするもの
- WWW のアクセスを利用するもの

直接攻撃によるものは、ポートスキャンでセキュリティホールを利用して不正に侵入するもの、ログイン名とパスワードを不正に入手して不正に利用するものなどがあります。不正にログインする場合には、単にファイルを改ざんするだけでなく、パスワードを記録するためのスパイウェアなどの何かを仕掛ける、あるいはさらに他のコンピュータを攻撃するための踏み台にすることなどを目的にしています。

1.2. セキュリティホールとポートスキャン

セキュリティホールとは、プログラムの書き方が不適切で、ある種の特殊な操作によってプログラムに本来の目的とは異なる動作を強制し、コンピュータのアクセス権限を不正に得るなど、安全性の問題点になるものです。コンピュータでこうした脆弱性に関連するセキュリティホールが見つかると、全世界の関係者に連絡が届きます。しかしながらそれに対する対策が行き渡る前、あるいは対策を講じないコンピュータのセキュリティホールを利用して、先述したような不正アクセスが行われます。

従来は攻撃する人が知っているドメイン名のコンピュータが中心に狙われていた時代もありましたが、現在ではポートスキャンによる攻撃は自動化され、すべての IP アドレスに対して自動的にセキュリティホールがあるかどうかの確認が行われ、脆弱性があると判断されたら即座にシステム破りに利用されます。これがポートスキャンと呼ばれる方法です。

1.3. ファイヤウオール

不正アクセスでコンピュータが乗っ取られるのを守るために様々な対応策が取られます。個人の場合にはパソコンに入れているパーソナルファイヤウオールと呼ばれる機能の利用や家庭に設置されているブロードバンドルータで、こちらから依頼していない、外部からの一方的な通信要求を無視するなどといった方法が有効です。大学などの組織では、外部との接続点にファイヤウオールを設置する、あるいは IDS（Intruder Detection System）を設置し、外部からの不正アクセスを検出・遮断するなどの方法が行われます。

ファイヤウオールとは、インターネットの外部から内部への不正なアクセスを防止する、内部から外部への不正なデータ漏洩を防止するなどの機能を果たす仕組みです。ファイヤウオールでは、IP アドレスやポート番号を元に、通信を許可するか、許可しないかという判断を行い、安全性を確保します。ファイヤウオールを整備していても、外部向けのサービスを行うためにファイヤウオールを通れるように“穴をあけて”あると、外部からの攻撃に直接さらされることになります。したがってできるだけ外部にサービスを行っているサーバ群は DMZ と呼ばれる緩衝地帯におき、外部と内部の両方

からアクセス可能であるが、外部から内部へは直接アクセスできないようにする運用形態が一般的です。

1.4. IDS

IDS は組織の内部と外部の通信を監視し、セキュリティホールを利用した一連の攻撃シーケンスを検出し、もし該当するものを見つけたら警告すると同時に通信を遮断します。人間が目で監視することは困難な、攻撃シーケンスの間に長い時間をおいて管理者が気づきにくくしているような長時間に渡る攻撃も検出することができます。ただし監視すべき回線の速度が上がると監視対象になる通信量が増え、性能の問題やログの出力量が問題になります。ログというのはこの場合には問題がありそうな通信がある時に出力される警告の記録などですが、通信量が増えると、それに比例して警告も増えるので、攻撃の発見が困難になるなどの問題が起こるということです。

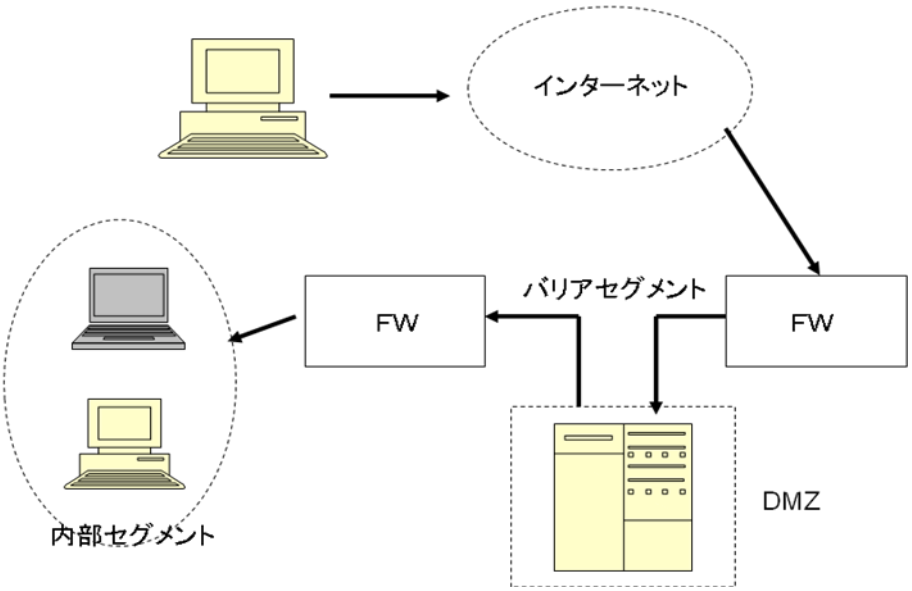


図 1-1 DMZ の例

1.5. パスワード

利用者 ID とパスワードはそのコンピュータの正当な利用者であることを証明するための情報です。これが他人に漏れると、ファイルを改ざんされたり、情報漏洩が起こったり、他のコンピュータの攻撃の踏み台に使われたりします。どんなに仲が良くても他の人に利用者 ID とパスワードを教えてはいけません。これらを紙に書いてパソコンの近くに貼っておくというのも問題外です。

悪意のある人がどのようにして利用者 ID とパスワードを入手しているかを説明します。

- 紙に書かれている利用者 ID とパスワードを見る、盗む、拾う。
- 名前、誕生日、趣味などをベースに推測する。
- 暗号化されているパスファードファイルを入手し、パスワードを破る。

利用者 ID は学生番号や社員番号などのように別の用途の ID を使う場合も多く、自分で選択できない場合にはどうしようもありません。選択できる場合には、できるだけ自分の名前などをそのまま使わないという工夫は必要かもしれません。いずれにしてもパスワードを破られないものにすることが重要です。

パスワードを破ろうとする人は、個人的な攻撃の場合にはその人の個人情報、姓、名、誕生日、住所、趣味、好きなタレントなど、日頃から聞いて知っている情報を駆使して、推測します。パスワードを入力する時に人に手元を見られないようにする、あるいは画面に●●などと表示されているのを見られて、何文字であるかを知られないようにするという注意が必要です。パスワードが何文字であるかはパスワードを破る側から見ると、とても役に立つ重要な情報です。

パスワードファイルを不正に入手してパスワードを破ろうとしている場合など、組織的な攻撃の場合には次のような手順で行います。

1. パスワードファイルを入手する。
2. 英単語の辞書、パスワードに使用しそうな単語類を暗号化する。
3. パスワードファイルの暗号化された文字列と比較する。
4. もし同じ文字列になっているものがあれば、元の文字列がパスワードである。

パスワードファイルの中の暗号化されている文字列を元に戻すことはできません。通常は単語を暗号化して､その結果の文字列とパスワードファイルの中の暗号化されたパスワードの情報を比較します。暗号化のアルゴリズムは広く知られており、英単語の辞書も公開されたものがあります。またパスワードを破るためのプログラムそのものがネットワーク上で公開されています。したがって、姓、名、住所、年月日、アイドルの名前、１語の英単語、それらの前後に数字を数桁付加するなどといったパターンは間違いなく解読されます。解読されにくいパスワードは、２語以上の英単語を特殊文字でつなぐ、できればさらに母音を抜く、綴りを故意に間違えるなどが有効と考えられます。

1.6. スパイウェア

スパイウェアとは、例えばユーザのキーボードやマウスからの入力情報、あるいはブラウザで見て回ったサイトの閲覧情報など、ユーザの使い方に関する情報を、スパイウェアを仕掛けた人に送信するソフトウェアを指します。スパイウェアは、大抵の場合にユーザが気づかないうちにパソコに組み込まれ、バックグランドで様々な活動をします。

例えば、キーロッガーと呼ばれるスパイウェアはユーザがキーボードを使う時にどのキーをどの順番で入力しているかを記録し、適当なタイミングでスパイウェアを仕掛けた人に送る機能を持っています。これはログイン名やパスワードを盗むための常套手段です。これに対抗するために最近のオンラインバンキングなどではキーボードから直接文字を入力するのではなく、マウスで文字をクリックして入力するソフトウェアキーボードを使用するようになりました。この方法では仮にマウスでクリックした座標を記録しても、ソフトウェアキーボードが画面の何処にあるかがわからない限り、どの文字を入力したかを推測することが困難であることを利用したものです。

ウイルス対策ソフトウェアにはたいていスパイウェアを検出する機能がついているので、定期的にスパイウェアが組み込まれていないかどうかを確認し、問題が起こらないように排除することが大事です。パソコンの使い方、氏名、住所、ログイン名、パスワードなど、ユーザの個人的な情報が外部に漏れると大抵は後で困った事態に遭遇することになるので、十分な注意が必要です。

2. メール利用時の注意、作法

2.1 ウイルスについて

コンピュータウイルスは利用者の意図とは無関係に望ましくないことを行うプログラムです。ウイルスはパソコン内のファイルに自分自身のコピーを追加していくことで増えて行きます。ウイルスが侵入することを「感染」、活動を開始するまでを「潜伏」、実際に活動している状態を「発病」していると呼ぶことがあります。他のプログラムに感染せずに、プログラム自身が利用者の意図しない動作をする不正プログラムを「ワーム」と呼びます。コンピュータウイルスはメールの添付ファイル、Web の閲覧、ネットワーク経由で直接攻撃されるなど、様々な経路で感染します。最近では毎日のように新型のコンピュータウイルスが作られ、世界中に伝搬しています。個々のコンピュータにウイルス検出ソフトウェアを導入するなどの対策が必須です。

インターネットが普及し始めていた 1988 年に世界で最初のコンピュータウイルスが出現しました。その後、1999 年に電子メールの添付ファイルを通じて感染するウイルス Melissa が出現、2001 年にサーバ上のセキュリティホールを悪用する Code Red が出現、Web ページを閲覧することで感染するワームの Nimda が出現して以来、続々と新種のウイルスやワームが出現しています。

これらのウイルスやワームに感染すると、次のような症状が発生します。

- 余計なメッセージを表示する。画面上の文字が崩れる。アイコンが変わる。
- ハードディスク内のデータを破壊する。
- システムの動作を不安定にする。動作が遅くなる、メモリが足りなくなるなど。
- メールを勝手に送信する。その際にファイルを添付することで、情報漏洩が発生する。
- 外部からコンピュータを操作できるようにし、他のコンピュータを攻撃する踏み台にする。
- ログイン名やパスワードを密かに記録しメールで外部に送信し、情報漏洩を起こす。

コンピュータウイルスそのものではありませんが、デマメールというものがあります。「これこれのファイルはコンピュータウイルスなので削除するように」といった嘘の情報を流すものです。しかしながら問題のファイルが実はシステムに必須のファイルだったりして、削除するとシステムが正常に動作しなくなるというたちの悪いものです。

また不幸の手紙のようなチェインメールもあります。電子メールでは手軽にかつ迅速にメールを配布することができるので、こうした不幸の手紙が始まると猛烈な勢いでメールが飛び交うことになり、影響が大きいので、こうしたメールの転送には注意して下さい。

2.2 ウイルス対策ソフトウェア

現在ではウイルス対策ソフトウェアなしにウイルスを確実に検出し、対応することはできません。したがって、日常的にパソコンを使う際には次のような注意が必要です。

- パソコンには必ずウイルス対策ソフトウェアを入れる。
- 定期的にウイルス検出用のパターンファイルを更新する。
- 外部から持ち込んだ外部記憶装置（CD、DVD、USB メモリ、SD メモリなど）をパソコンに接続する時は必ずウイルスチェックを行ってから中身を使う。
- こうした外部記憶装置を接続した時にプログラムを自動的に実行する機能は off にしておく。

最近のウイルス対策ソフトウェアは、メールに添付されてくるウイルス対策だけでなく、外部との通信のリアルタイム監視、ファイルをダウンロードする時の監視、危険な URL をアクセスしようとする時に警告を表示、定期的にボリュームを検査して、ウイルスやワーム、スパイウェアなど

が含まれていないかを確認するといった機能があるので、これらを有効に使うことが望まれます。

2.3　SPAM について

みなさんがメールを使いはじめてしばらくすると、まるで心当たりがないアドレスからメールが届くようになります。宣伝だったり、アダルトサイトへの勧誘だったり、フィッシング詐欺のメールだったりします。こうしたメー ルを SPAM メール（ごみメール）と呼びます。これらを排除するために一般的には SPAM フィルターという機能が使われます。世界中を飛び交っているメールの大部分（約９割）が実はごみメールだと言われています。これはインターネットにおける壮大な資源の無駄遣いだと言えます。みなさんが Web ページなどにメールアドレスなどを記述すると SPAM メールの送信先として記録され、SPAM メールの宛先として追加されることが多いので、十分に注意しましょう。最近のウイルス対策ソフトウェアには SPAM フィルターの機能がついているものもあり、これらを活用するのも良いと思います。

2.4　メールの差出人

電子メールの差出人は簡単に詐称することができます。したがって、知っている人から届いたメールだからと油断すると、トラブルに巻き込まれることがあり得ます。メールの差出人は簡単にごまかせるということを知っておくだけでもトラブルに巻き込まれないために役に立つと思います。

2.5　システムソフトウェアのアップデート

Windows や Mac OS、UNIX などのシステムには必ずセキュリティホールと呼ばれる、外部からの攻撃に使われる抜け道があります。これらが発見されると、改善のための新しいソフトウェアが提供されますので、こまめにこれらの修正プログラムを適用する必要があります。

1）Windows XP や Vista では Windows Update という機能があります。これは色々なところから起動することができますが、例えば Internet Explorer のツールの中に Windows Update というメニューがあるので、これを選択すると、パソコンのシステムを調べて、修正すべきソフトウェアがあれば、その修正を適用する作業を自動的に行ってくれます。
2）Mac OS X では、画面左上のリンゴマークの中に「ソフトウェア・アップデート」というメニューがあるので、これを選択すると、パソコンのシステムを調べて、新しく修正すべきソフトウェアがあれば、その修正を適用する作業を自動的に行ってくれます。

2.5　メールの作法について

メールは使いこなせると便利ですが、利用する上での注意も必要です。

- 電子メールに依存しすぎずに、それぞれの特徴を考えて、電話、手紙、 FAX などとの使い分けてください。
- 電子メールは必ず届くという保証はありません。インターネットは「ベストエフォート」といって、「できるだけ頑張るけど、駄目なときはごめん」という方針で動いています。その上のアプリケーションである電子メールは当然この方針の影響を受けます。インターネットの途中のコンピュータのトラブルで中継が遅れる、紛失する可能性もあります。最近では、SPAM フィルターで SPAM メールと判断されて捨てられる場合も増えています。特に大事な通信を行う時にメールだけを頼りにするのは危険です。電子メールは届かないことがあるという前提で使用してください。
- 送信する相手を必ず確認してから送信してください。送る必要がない人に送信してしまったら取消しはできません。

- 相手のアドレスを間違えないようにしてください。特にたくさんの人が登録されている情報処理センターなどで、単純な通し番号になっているアドレスではメールアドレスの一部を間違えると他の人に届いてしまいます。
- 知らない人に送信するときはくれぐれも文章の書き方に注意してください。良く知っている相手だと、この言い方（表現）はたぶんこういう雰囲気だろうと察してもらえることもありますが、知らない相手では自分の言いたいことが正しく伝わるとは限りません。感情的にこじれることが多々ありますから正確な日本語で、誤解の起こらないような書き方を心がけて下さい。
- 電子メールに大きなファイルを添付しないでください。九州大学はネットワークやメールサーバの性能が良いので、あまり問題になりませんが、相手によっては大きなファイルを添付すると迷惑をかけることがあります。一定以上の大きさのメールの受信に制限をもうけている場合もあります。携帯電話や PHS でメールを受信している人がいることも考えてください。教育情報システムで提供しているメールは受け取るメールの総量の上限が 30MB です。写真や大きな原稿などを添付するとすぐにこの上限に到達して、受け取れなくなります。
- 知らない人から届いたメールは慎重に扱って下さい。特に添付ファイルがあるものは細心の注意が必要です。知っている人からのメールでもウイルスに感染している「危ない」ファイルが添付されていることがあるので、こころ当りがない場合には本人に確認してから開くぐらいの慎重さが必要です。開く前にウイルス対策ソフトなどを使ってウイルスに感染していないことを確認する心構えが必要です。また「表示」から「メッセージのソース」を選択すると、メールの中がどうなっているかを見ることができますので、ある程度の経験を積んでくると、安全かどうかを判断できる可能性があります。

3. Web 利用時の注意

3.1　サイトの正当性と暗号通信

インターネットを利用することで、様々な情報を手軽に入手でき、オンラインショッピングやオンライントレーディングなどの商取引も容易になり、とても便利になりました。しかしながら便利であるということは反面で危険であるということでもあります。インターネットを使った通信は通常は暗号化されていません。したがって回線を盗聴されるとすべての情報が漏洩する可能性があります。重要な情報を盗聴されないためには暗号化通信を積極的に使用する必要があります。ブラウザなどでは SSL (Secure Socket Layer)と呼ばれる通信方式を使用すると、サーバ（情報を提供しているコンピュータ）とクライアント（ブラウザが動いているパソコン）の間の通信を暗号化することができます。https で始まっている URL が SSL 通信を行うことを意味しています。SSL を使用していると、ブラウザの画面に鍵マークが表示されます。Safari では右上()、Internet Explorer ではアドレスバーの右()に表示されます。

3.2　フィッシング詐欺

SSL 通信を利用していると、相手が正しいサイトであること、途中で盗聴される心配がないことから、個人情報（名前、住所、電話番号、写真、クレジット情報）を送信しても良いと考えられます。ただし、最近ではフィッシング詐欺という新しい手口の犯罪が発生しており、注意が必要です。フィッシング詐欺というのは、オンラインバンキングやオンラインショッピング事業者などを装い、不特定多数のインターネットユーザから個人情報を盗む詐欺行為のことで、ユーザに偽りの情報を記載した電子メールを送りつけ、本物と酷似した Web サイトへ誘導し、ユーザの ID やパスワード、カード番号や、口座番号などの個人情報を入力させるものです。そうして入手した個人情報は、金融機関から現金を引き出したり、ショッピングサイトで物品を購入後、転売したりすることに悪用される、あるいは偽造カードを作って悪用されます。画面上で

「本物」

と表示されていても、その定義は

「本物」

となっている可能性があります。つまり「本物」をクリックすると「偽物」に誘導される訳です。以前、サーバの URL を知られたくない銀行は URL を表示しないようにしていましたが、最近では偽物ではないことを確認できるように積極的に URL がアドレスバーに表示されるようにしています。ここを確認して、現在アクセスしているサイトが本物かどうかを確認する習慣をつけてください。

3.3　オンライン取引

オンラインで買い物、銀行の利用などが可能になっています。オンラインショッピングでは支払い方法に注意が必要です。クレジットカードで支払うようにすると簡便ですが、クレジットカードによる支払い方法は、基本的には名前、カード番号、有効期限の３つの情報が揃うと他人でも使用できるという特徴があります。SSL を使って暗号通信を行い、途中でクレジット方法が漏洩しないようにすることはもちろんですが、情報を受け取った取引先の企業から漏洩する、クレジット会社との決済手続きの途中で漏洩するなど、様々なリスクがあります。2005 年 6 月にアメリカの会社で発生した情報漏洩では 4000 万件のクレジット情報が漏洩し、多額の被害が発生しています。あるいは商品を注文してお金を支払ったにも関わらず商品が配送されない、配送はされたが劣悪な商品だったとかいったこともあり得ます。もし可能であれば支払いは運送業者が配送した時に、現物を確認した上で「代

金引換」で受け取る方法が安全ではないかと思います。

3.4　掲示板、ブログ、SNS

インターネットの普及に伴って、個人で簡単に情報発信ができるようになりました。そうした場合に公序良俗に違反するような内容を書いてはいけません。インターネットの世界では、年齢、性別、社会的な身分などに関わりなく、一人の人間として扱われます。したがって「若気の至り」といったような言い訳はできません。もし他人を誹謗中傷したりして告発されると、裁判で有罪なることもあります。「自分がされたくないことは他人にもしない」というごく基本的なマナーを守るようにしましょう。

インターネットで何かをした際に、一見、匿名性が保たれていて、誰が情報発信したか追跡できないと思っている人もいるかも知れませんが、実体が誰であるかを追跡することは、個人では困難でも、しかるべき権限があれば可能です。サーバにはアクセスの記録が残りますし、途中の通信も記録されています。したがってもし本当に必要になったら、誰がその情報を発信したかは、あるいは誰が閲覧したかは確実に明らかになります。発覚しなければ何をやっても良いということではなく、インターネットの世界も普通の社会と同じで、「してはいけないことは、してはいけない」のです。

3.5　著作権について

Web ページを作成する時に、気に入った Web ページのイメージや文章を使いたくなることがあると思います。しかしながら、これらには著作権があり、無断で使用すると著作権法に違反することになります。ネットワーク上で、無償で公開されているフリーソフトウェアやオープンソースのソフトウェアを利用することは問題ありませんが、他人が購入した市販ソフトウェアをコピーして利用することもしてはいけないことの一つです。現在の著作権法ではこうした場合には「五年以下の懲役若しくは五百万円以下の罰金に処し、又はこれを併科する。」となっています。

P2P と呼ばれる技術を使って、音楽や写真などを流通することが世間では広く行われていますが、九州大学では、WinMX, Winny、Napstere、Donkey2000、Gnutella、KaZaA などの P2P ファイル交換ソフトウェアを利用することが禁止されています。これを利用して自分自身が本来入手してはいけない情報を手に入れることはもちろん駄目ですが、これらのソフトウェアを利用していると、本人が知らない間に他人が不法にファイル交換することに貢献し、著作権法に違反することを手助けすることになるからです。これが原因で大学生が逮捕された例もありますので、十分に注意してください。

4. 暗号化技術

暗号は、もともとは軍で使用されていた技術です。戦闘時には作戦行動に関する情報を敵に知られることなく、味方に確実に知らせなければなりません。また、その情報が確かに味方から送られたものであること、敵に変更されていないことが確認できなければなりません。これらは、機密性、正確性、真正性を意味しています。インターネットの普及に伴い、インターネット上の通信で同様の性質が要求され、暗号化技術が利用されています。

4.1 暗号と鍵

暗号化する前の原文を平文（plaintext）と呼びます。これを暗号化の手法で暗号文（ciphertext）に変えます。この暗号文はだれにも理解できないデータになっています。受信者が暗号文を受け取ると復号化を行って元の平文に戻します。復号できなければ暗号文は意味をなしません。

例えば「シーザー暗号」という暗号があります。これは、文字をアルファベット順に何文字かずらすことで暗号文を作ります。平文の例として「jouhou」があるとすると、1 文字ずらした暗号文は「kpvipv」となります。2 文字ずらすと「lqwjqw」になります。何文字ずらすかを決めれば、暗号化と復号化が可能です。シーザー暗号の場合、ずらす文字数が鍵となります。このように鍵は暗号化と復号化で必要となります。映画「2001 年宇宙の旅」に出てくる超コンピュータ「HAL」は「IBM」のシーザー暗号と言われています。

4.2 共通鍵暗号

暗号化と複合化とで同じ鍵を使用する暗号のことを共通鍵暗号（common key cryptography）と呼びます。共通鍵暗号には暗号化と復号化の処理を高速に行えるというメリットがあります。そのため、標準化された暗号がいくつかあります。米国商務省標準局（ANSI）は AES（Advanced Encryption Standard）を標準暗号方式にしています。

共通鍵暗号は、送信者と解読者で同じ鍵を共有する必要があります。先のシーザー暗号は、ずらす文字数という同じ鍵を暗号化と複合化で使用する共通鍵暗号です。そのため、暗号文を送る前に「1 文字ずらして送るからね」という鍵を仲間に渡しておくことになります。しかし、仲間内で鍵を共有する方法には問題があります。暗号化を行った人は、暗号文を復号して読んで欲しい人だけに、暗号化のときに使用した鍵を渡しておく必要があります。しかし、インターネットの環境では、通信相手にあらかじめ鍵を渡しておくことは困難です。インターネット上で鍵をそのまま送ると誰かに傍受される可能性があります。傍受されたらそれ以降は暗号文が解読されてしまいます。そのため、初めて交信する相手には鍵さえも送ることができません。

4.3 公開鍵暗号

公開鍵暗号（public key cryptography）は、暗号化と複合化とで異なる鍵を使用する暗号方式のことです。2 つの鍵は公開鍵（public key）と秘密鍵（private key）と呼ばれ、片方の鍵で暗号化した暗号文は他方の鍵でないと復号化できません。また、公開鍵と秘密鍵のペアは、公開鍵から秘密鍵を推測することができないようになっています。公開鍵暗号としては、RSA 暗号が有名で広く使用されています。

公開鍵は一般に公開し、だれでも入手できるようにしておきます。一方、秘密鍵は他人に知られないように大切に保管しておきます。重要な平文を A さんに送りたいときは、A さんの公開鍵で暗号化した暗号文を送ります。この暗号文は A さんの秘密鍵がなければ復号化できないので、秘密鍵を持つ A さんは復号化して平文を取り出すことができますが、A さん以外の人は復号化できません。このように共通鍵暗号で問題であった鍵の共有はこの方法では問題になりません。

公開鍵暗号は、暗号化と復号化に時間がかかります。そのため、長い（大きな）平文を暗号化する際には、弱点となります。その問題を回避するために、公開鍵暗号と共通鍵暗号を組み合わせて暗号化通信を行うことがあります。これは、平文を暗号化するときに一時的に使用する共通鍵を使って暗号化し、暗号文を相手に送ります。この暗号化で使った共通鍵を最初に送る時に相手の公開鍵で暗号化し、相手に送ります。この共通鍵の情報を転送中には、共通鍵は暗号化されているので読解不可能です。通信相手は自分の秘密鍵で共通鍵を取り出し、以後はその共通鍵を使って暗号化と複合化を行います。

4.4　電子署名

どんな重要なドキュメントも偽造の可能性があっては無意味なものになってしまいます。そのため、メッセージを作成したのが本人であるか、内容が改竄されていないかを検証する技術が必要になってきます。これを電子署名といいます。

電子署名は公開鍵暗号を利用して行われます。例えば、A さんが署名したい文を自分の秘密鍵で暗号化して送ったとします。受け取った人は、A さんの公開鍵を使って復号化できるので、この暗号文は A さんが送ったものであることを検証できます。受取人を確認するには、送信分を B さんの公開鍵で暗号化して送ります。B さんは自分の秘密鍵で内容を取り出すことができますが、他の人は複合化をすることができないので、受信人を確実にすることができます。

内容の改竄がないことを検証するには公開鍵暗号だけではできませんが、ハッシュ関数という技術と組み合わせることで可能となります。そのために本文をハッシュ関数（MD５がよく使われる）で処理した結果を一緒に送ります。受信した人は受け取った本文から同様にハッシュ関数で計算して、同じ値になれば改ざんされていないことを確認することができます。

上に示したやり方は、公開されている A さんの公開鍵が、確かに A さんが生成したもので、そのペアである秘密鍵を A さんだけが持っていることが条件になります。そのため、公開鍵の証明書が必要になります。それを行う機関が公開鍵証明機関で、VeriSign などが有名です。

4.5　SSL

SSL（Secure Sockets Layer）は暗号技術を使用してクライアントとサーバ間で安全な通信環境を提供するプロトコルです。SSL は OSI の基本参照モデルのトランスポート層で機能するプロトコルで、柔軟性が高いという特長があります。上位の階層で機能する HTTP や SMTP、POP3 などに変更を加えずに SSL を使った暗号通信を行うことができます。

SSL は公開鍵暗号と共通鍵暗号を組み合わせて通信内容の暗号化を行います。また、公開鍵の証明書を使用することにより、サーバ、クライアント間で相手を認証できます。その他、いろいろな技術を組み合わせて、「通信内容が盗聴されない」「通信相手が本人に間違いない」「通信内容が改ざんされていない」通信を可能にしています。

5. 安全・安心なパソコンなファイル保存

5.1 ファイル保存に関連する問題

パソコンで作業を行って、標準的な場所にファイルを保存すると、通常は内蔵のハードディスクに保存されます。この状態でパソコンが故障すると、保存しているファイルを使うことができなくなります。修理に出すと、戻ってくるまで使えないだけでなく、修理中にファイルの中身を見られる可能性もあります。パソコンの内蔵ディスクなどに、人に見られては困る重要な情報を含むファイルなどを保存していると、そうした場合にパソコンを修理に出せなくなります。

九州大学では研究費で購入したパソコンを学外に持ち出す時には事前に許可を得ることになっていますが、持ち出しの許可の有無にかかわらず、内蔵ディスクに重要な情報を保存したパソコンを紛失、あるいは盗難に遭うと、それらのファイルを利用できなくなるだけでなく、情報漏洩という問題が発生します。問題はパソコンではなく、格納している情報の方が大切だということです。それは個人で購入したパソコンでも同様です。

5.2 外部記憶装置への保存

パソコンへのファイルの保存に際しては、利便性と情報の保護のために、次のような手順を採用することを勧めます。

1) パソコンの電源投入時などには必ずパスワードを使ってログインする設定にする。
2) しばらく使わない場合にはスクリーンセーバが起動するように設定し、スクリーンセーバを解除するにはパスワードが必要な設定にする。
3) パソコンの内蔵ハードディスクなどに情報を保存しない。必ず取り外し可能な外部記憶媒体（外付けのハードディスク、USB メモリ、SD カード、CF カードなど）に情報を保存する。
4) 外部記憶媒体に保存する情報は、暗号化ボリュームなどの技術を使って、仮にその記憶媒体が他人の手に渡っても、使用している暗号化ボリュームソフトウェアと正しいパスワードが分からない限り、中身を見られる心配がないようにする。
5) 日々の作業が一段落した時に、こまめにファイルのバックアップを取り、仮に外部記憶媒体が紛失、盗難などにあっても仕事に必要な情報がないために困るという事態を避ける。

5.3 暗号化ボリュームについて

暗号化ボリュームとは、USB メモリなどの取り外し可能な記憶媒体の中に大きなファイルを作成し、そのファイルに保存する情報をすべて暗号化し、一つの仮想的なボリュームに見せかける技術です。正しいソフトウェアと正しいパスワードを使ってパソコンにボリュームとしてマウントしない限り、中身を見られる心配はありません。

広く使用されている暗号化ボリュームソフトウェアに TrueCrypt があります。これは Windows XP/2000/VISTA、Mac OS X、Linux で使え、オープンソースであることから、安心して使用することができます。詳細は次の URL を参照してください。

http://www.truecrypt.org/

使い方は次の通りです。

1) ソフトウェアをダウンロードします。最新版は 2009 年 5 月現在で 6.2 です。
2) インストールします。基本的にはダウンロードしたファイルをダブルクリックし、メッセージに従って作業すれば容易にインストールできます。

3) TrueCrypt を起動します。
4) 最初に暗号化ボリュームを作成します。暗号化ボリューム用にパスワードを設定します。
Mac OS X で大きなボリュームを作成する場合にはNTFS を処理できるソフトウェアが必要になるので（これがないと NTFS のファイルを読めるが、書けない)、別途ソフトウェア（NTFS-3G など）が必要になります。
5) 暗号化ボリュームとして設定したファイルを選択して、マウントします。ここで、ボリュームを作成する時に設定したパスワードが必要です。何処にマウントするかを一覧から選択しておかないと失敗します。
6) マウントすれば後は通常のボリュームとして使用できます。
7) 使い終わったらアンマウントします。アンマウントせずにサスペンドやスリープ、休止などをする場合には、パソコンの起動時やスクリーンセーバ解除時にパスワードが必要な設定にしておくことが肝要です。

5.4　バックアップについて

外部記憶媒体に情報を保存する場合には、当然、紛失や盗難に備える必要があります。暗号化ボリュームを使えば盗難に遭っても中身を見られる心配はありませんが、手元に必要な情報がないというのは困ります。したがって、作業が一段落したら、こまめにバックアップを取る必要があります。ここではバックアップしたいディレクトリとバックアップ先のディレクトリの下に存在するすべてのファイルとディレクトリを同期できるソフトウェアを紹介します。これらは変更があったファイルだけを検出して更新するため、高速にディレクトリ間の同期を取ることができます。また特殊な形でバックアップするのではなく、通常のファイルやディレクトリとしてコピーするので、必要ならバックアップしているファイルをそのまま使うことができます。なお、パソコンとバックアップ用の外部記憶媒体を一緒に持ち歩いて、両方とも同時に紛失や盗難に遭うと、意味がありませんから、同時には持ち歩かないようにしましょう。

○ Windows XP の場合
realsync
http://www.takenet.or.jp/~ryuuji/realsync/

○ Mac OS X、Linux の場合
rsync
http://rsync.samba.org/