情報セキュリティとは

- 災害による情報の消失、情報通信機能の停止
- 情報の盗難・紛失
- クラッカによるコンピュータへの侵入
  →なりすまし、情報詐取、改ざん、機能停止
- コンピュータウィルス
  →ファイルの破壊、機能停止、増殖

「情報セキュリティとはこれらの脅威から大切な情報を守ること」

パソコンと情報の管理

- ログインには個人のパスワードを設定する
- USBキーやICカードなどによる、よりセキュリティの高いログイン方法を使う
- パソコンの万一の紛失等に備えて、重要なファイルは暗号化する
- 重要なファイルは外部の記憶装置にバックアップをとる

テレワークとパソコンの管理

テレワーカはパソコンの管理に十分気をつける必要がある。ノート型のパソコンの機能が飛躍的に向上し、どこでも、いつでも仕事ができるという、テレワーカの強い味方ですが、外出時に携帯した場合、電車の棚に置き忘れたり、盗難の心配があります。自宅で盗難に会うことも想定しなければならない。個人使用、あるいは家族と共用している場合でも、必ずパスワードによるログインを行うことが必要である。また、より安全なログイン方法として、個人のIDやパスワードが記録されたUSBキーやICカードを利用したログイン方法もある。USBキーには、ファイルを暗号化して保存できるものもあります。万一パソコンが盗難にあったり、紛失した場合に備えて、特に重要なファイルは暗号化して保存するのが安全である。パソコンの不測の障害により重要なファイルが消去されたり、読み出しができなくなってしまうこともあるので、定期的にFDDやCDDに保存しておきます。パソコンのOS自体が起動不能になると、作業が全くできなくなってしまうので、OSのリカバリーには慣れておいたほうがよい。重要なファイルはOSとは別のドライブ（Dドライブなど）に保存しておくとリカバリーの際には便利である。情報の漏洩ということでは家庭でも普及している無線LANの使い方にも注意が必要である。

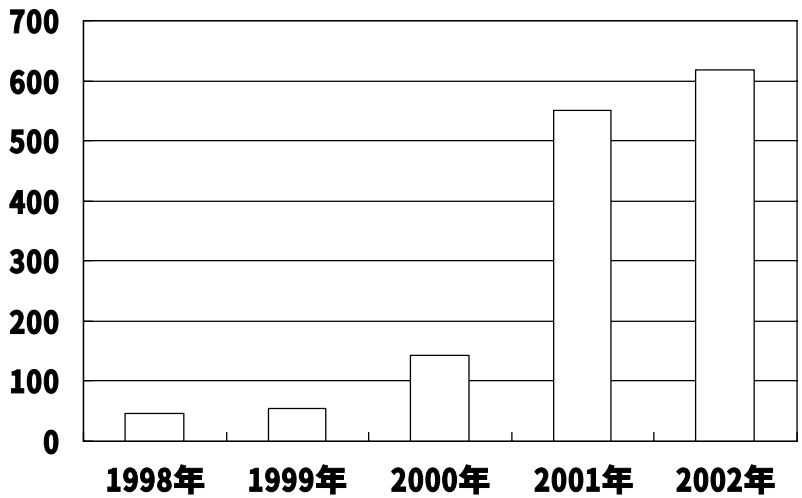
無線ＬＡＮの脅威と対策
（自宅で無線LANを利用するときの留意点）

- 無線ＬＡＮは電波の性質上セキュリティ上の課題が多い
- ＥＳＳ－IDには認証機能はない
- 暗号機能としてＷＥＰがあるが、解読される危険性がある
- 認証機能と暗号機能の両方を強化できるＩＥＥＥ８０２．１ｘ という新規格はユーザ毎の認証ができるので、セキュリティの強化が期待できる
  （ＩＥＥＥ８０２．１ｘ の機能は Windows XP に標準装備）
- 小規模のネットワークではＭＡＣアドレスによるフィルタリングで不正アクセスは防げる

ＥＳＳ－ID：Extended service set ID
ＷＥＰ：Wired equivalent privacy

クラッカーによる不正侵入

- IPA／ISECへの被害届出数は表のとおり2001年に急増している。これはブロードバンドの普及とは無縁ではないだろう。回線の高速化と常時接続が一般化したため、クラッカーの進入の機会が増えたといえる。
- 2002年の619件の不正アクセスの申告のうち、侵入は106件、不正アクセスの形跡は356件、アドレス詐称は49件、Dos攻撃は16件、メールの不正中継は16件となっている。
- しかしこれらの数字は氷山の一角と思われる。あえて申告しない、気がつかないケースもあろう。



クラッカーによる被害届出数

(IPA・ISEC資料より)

クラッキングの手口1 (不正侵入の前調査)

- **アドレス・スキャン**

  稼動しているサーバのIPアドレスを取得する。インターネットで自由に手に入るツールをつかってスキャンし、効率的に調べることができる。

- **ポート・スキャン**

  稼動しているサーバマシンで動作しているサービスを調べる。

- **バナー・チェック**

  サーバマシンで動いているサーバソフトの名称やバージョンを調べる。

  公開されているセキュリティ情報よりセキュリティホールがわかる。

クラッキングの手口2 (不正侵入の実犯行)

- パスワード・クラック (表から侵入)
  - ID/パスワード解析ツールを使う。
  - ネットワーク管理者などから聞き出す。
  - パスワードファイルを入手して解析する。
- バッファ・オーバーフロー (裏から侵入)
  - ソフトウエアのバグ (セキュリティホール) をついてバッファーをオーバーフローさせサービスを停止させる。(サービス妨害 DoS)
  - バッファオーバーフローを利用して別の命令を実行させることで、管理者の権限を奪うこともできる。

Webサーバをクラッカーから守る

- ファイアウオールではサーバのセキュリティ・ホールは守れない
- Windows は初期設定のまま使うのは危険
- HFNetChkを使うと適用しいていないパッチをリストアップしてくれる

  http://www.microsoft.com/japan/technet/security/tools/tools/hfnetchk.asp

- IIS Lockdown Wizard を使えば通常使わない機能を止める設定ができる

  http://www.microsoft.com/japan/technet/security/tools/tools/locktool.asp

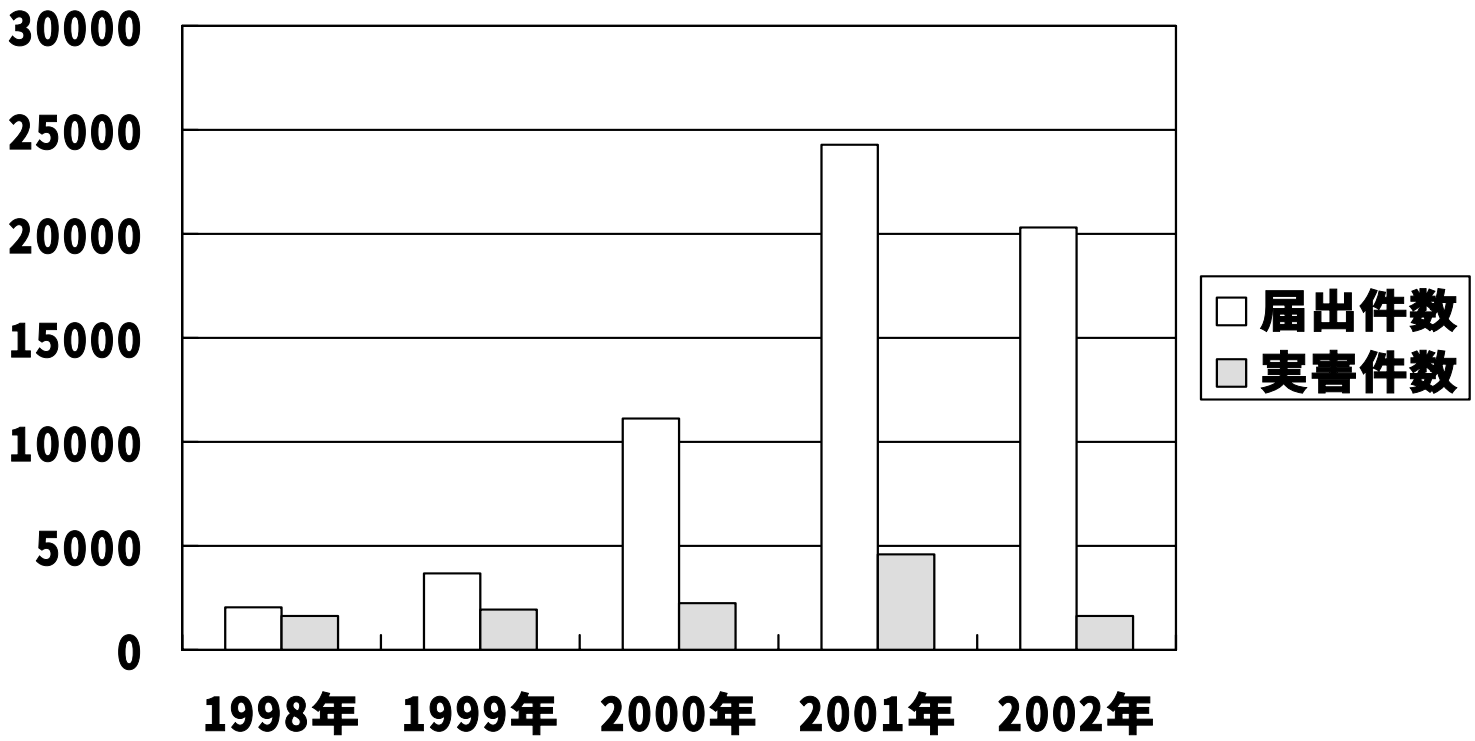
- URLScanでIISが受け付けるHTTPアクセスを制限できる
  (Lock Down Wizard を実行すると自動的にインストールされる)

コンピュータ･ウィルスとは

不正プログラムの総称であり、次のように分類される

- ウィルス(本来の定義)
  - ほかのプログラムに感染するプログラム
- ワーム
  - ネットワークを介して自己増殖するプログラム
- トロイの木馬
  - 正規ソフトを装った単体で動作するプログラム

ウイルス届出の件数(IPA/ISEC発表)



ウイルスによる具体的な症状

ハードディスクのフォーマット

ファイルの削除

BIOSの破壊

ファイルの改ざん

メールの大量送信

ユーザー情報の盗難

メッセージの表示

いたずらプログラムの実行

メモリーやネットワーク資源の浪費

パソコンのウイルス対策

ウイルス対策ソフトをパソコンに常駐させるとともに、最新のウイルス定義ファイルに更新すること。ウイルス定義ファイルの更新がネットワーク上で自動的に行われるものを利用するとよい。定期的に最新のバージョンを確認することも重要である。以下にテレワーカに必要なウイルス対策を列挙する。

1. 最新のウイルス定義ファイルに更新した対策ソフトをパソコンに常駐させる

2. メールの添付ファイルは、開く前にウイルス検査を行う

3. ダウンロードしたファイルは、使用する前にウイルス検査を行う

4. アプリケーションのセキュリティ機能を活用する

5. セキュリティパッチをあてる

6. ウイルス感染の兆候を見逃さない

7. ウイルス感染被害からの復旧のためデータのバックアップを行う

セキュリティ情報の収集

セキュリティ情報の収集がセキュリティ対策の第一歩
下表の各組織のホームページなどで最新の情報が得られる

組織名		セキュリティ情報のあるホームページ
IRT系	CERT／CC	http://www.cert.org/
	CIAC	http://www.ciac.org/ciac
	IPA	http://www.ipa.go.jp/security/isg/ciadr.html
	JPCERT	http://www.jpcert.or.jp
ベンダー系	マイクロソフト	http://www.microsoft.com/japan/security
	サンマイクロシステムズ	http://sunsolve.sun.co.jp/pub-cgi/secBulletin.pl
	米シスコシステムズ	http://www.cisco.com/warp/public/707/sec_incident_response.shtml
	シマンテック	http://symantec.co.jp/region/jp/sarcj/index.html
	トレンドマイクロ	http://www.trendmicro.co.jp/virusinfo/index.asp
	日本ネットワークアソシエイツ	http://www.nai.com/japan/virusinfo/vlatest.asp
	米レッドハット	http://www.redhat.com/apps/support/errata/index.html