８．ネットワーク接続時の対処

ウィルス対策の基本(1)

１．ソフトウェアのセキュリティホールはふさぐ

ソフトウェアのセキュリティホールを突いて、プログラムを送り込み、実行させる場合がある

↳ Windowsマシンであれば、Microsoft Update（Windows Update ）を活用

２．ウィルス対策ソフトやウィルスチェックサービスを利用する

(1) ウィルス対策ソフト

・ウィルス対策ソフトを常に起動状態とする（リアルタイムチェック）
・メールやファイルを開く前にウィルスチェックを行うように、設定する
・ウィルス定義ファイルを更新し、常に最新の状態に保つ
・ライセンスの更新を行う

(2) ISPによるウィルスチェックサービス

・メールのチェックであり、Web経由やCD-ROMなどには対応していない

ウィルス対策の基本(2)

３．無闇にファイルをダウンロードしない

・知らないサイトからファイルをダウンロードしない
・ファイルをダウンロードしたら、ウィルス検査を行う

４．怪しいファイルは開かない（実行させない）

・不正プログラムが存在しても、実行しない限り、危険はない
・自分で実行しなくても、パソコン内のプログラム（ブラウザなど）にセキュリティホールがあれば、それを突いて、実行される場合もある
・ファイルの拡張子を表示させる設定にする

５．アプリケーションのセキュリティを適切に設定する

・WordやExcelのマクロ自動実行をオフにする
・メールソフトやブラウザのセキュリティレベルは中以上にする

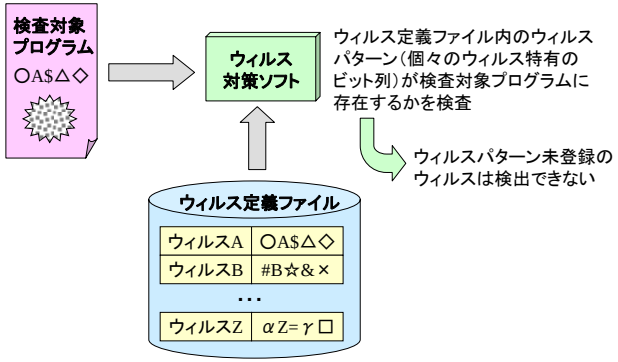
６．万一に備え、データのバックアップを行う

・ウィルス等に感染すると、データの復元ができない場合がある
・データのバックアップを頻繁に行う

ウィルス対策ソフト

ウィルス対策ソフト（ワクチンソフト）

コンピュータウィルスなどの検出、駆除などを行うソフトウェア



ウィルス感染時の処置

1. ネットワークへの接続を遮断する

・被害の拡大を防ぐため、ネットワークを遮断する

2. ウィルス対策ソフトで検査する

・ウィルス対策ソフトを使用して、ウィルス検査を行う

3. ウィルス対策ソフトで駆除する

・見つかったウィルスをウィルス対策ソフトで駆除または隔離する

4. ウィルス対策ソフトで再度検査する

・最新のウィルス定義ファイルを使用して、ウィルス検査を行う

5. データを復旧する

・データが破壊されている恐れがあるので、バックアップデータに基づき、データを復旧する

6. 再発防止策を講じる

・感染原因を究明し、対策を講じる

スパイウェアの対策

(1)ブラウザのセキュリティやプライバシーの設定を調整する

・ブラウザ(Internet Explorerなど)のセキュリティレベル、プライバシー設定は中以上にする
・低くすると、利用者の確認を経ず、プログラムがダウンロードされる

(2)ファイルのダウンロードに気を付ける

・知らないサイトからファイルをダウンロードしない
・プログラムの使用許諾書の細部を確認する
・無料の音楽、映画ファイル共有プログラムのインストールに注意する

(3)スパイウェアの検出、削除ツールを利用する

・定期的に検出、削除ツールでチェックする
・検出、削除ツールのチェック用データを更新する

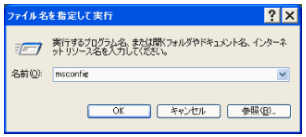
(4)アンインストール又は自動起動設定ファイルをチェックする

・レジストリなどが書き換えられているので、アンインストールを行う
・Windowsであれば、システム構成ユーティリティを使用し、スタートアッププログラム一覧から怪しいファイルの自動起動を削除する

(5)パソコンのソフトウェアを最新の状態に保つ

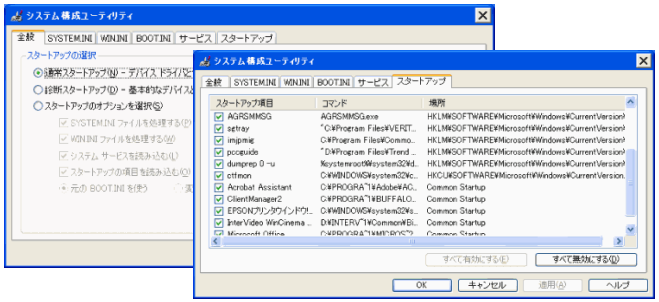
・Windowsであれば、定期的にMicrosoft Update(Windows Update)を実行する

付. システム構成ユーティリティ(XP)



怪しいファイルの自動起動の削除

①「ファイル名を指定して実行」ダイアログで名前にmsconfig と入力
②「システム構成ユーティリティ」の「スタートアップ項目」のチェックを外す



WebサイトのURLの確認

IEのアドレスバーが偽装されている恐れがあるので、以下の方法で本当のURLを確認する。

1. Webサイトへの通信がhttpsであれば、公開鍵証明書(デジタル証明書)の発行先の名前で確認する。

2. 以下の何れかのJscript コマンドをアドレスバーに入力して、現在の Web サイトの本当のURL を表示する。

javascript:alert("実際のURL アドレス : " + location.protocol + "//" + location.hostname + "/");

javascript:alert("実際のURL は次のとおりです :¥t¥t" + location.protocol + "//" + location.hostname + "/" + "¥nアドレスのURL は次のとおりです :¥t¥t" + location.href + "¥n" + "¥nサーバ名が異なる場合は、成りすましたサイトの可能性があります。");

3. 「履歴」ウィンドウを使用して、現在の Web サイトの本当のURL を確認する。

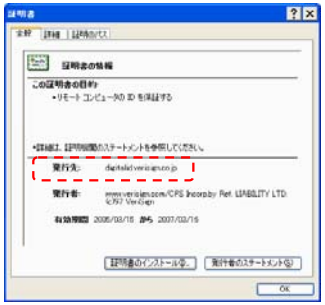
4. アドレス バーのURL をコピーして、新たに立ち上げたIEのアドレスバーに貼り付け、実際に使用されたURLを確認する。

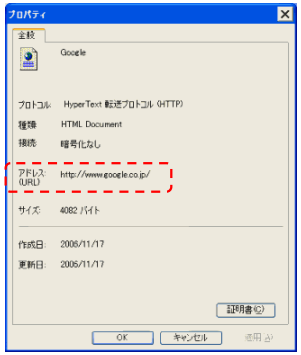
5. 「ファイル」メニューのプロパティの「アドレス(URL)」欄で本当のURL を確認する。

付. WebサイトのURLの確認

公開鍵証明書（デジタル証明書）の発行先の名前の確認

プロパティの「アドレス（URL）」欄で本当のURL を確認

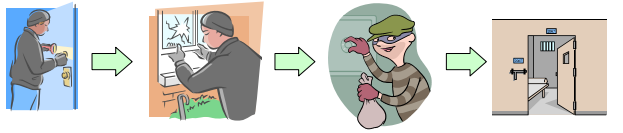




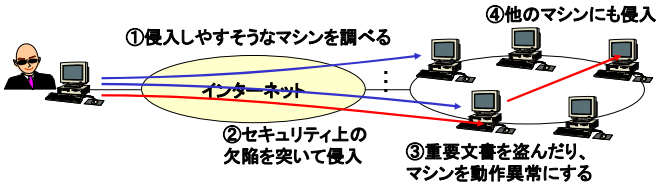
攻撃の手順

泥棒の手順

①侵入しやすそうな部屋を探す → **②窓や鍵を壊して侵入** → **③貴重品を盗んだり、物を壊す** → **④他の部屋にも侵入**



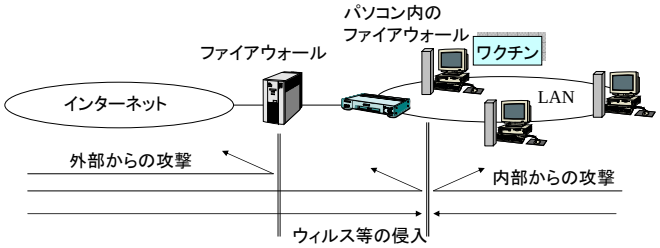
マシン攻撃の手順



攻撃と防御

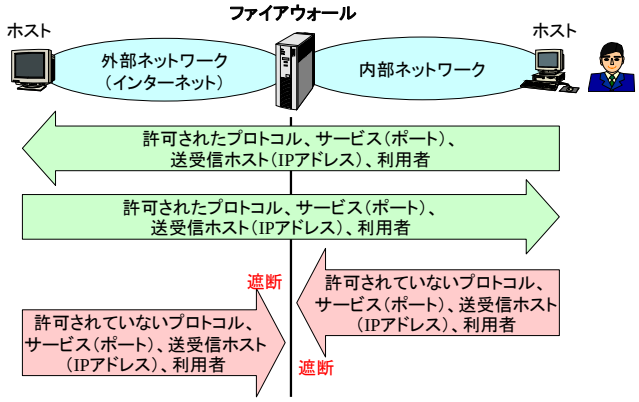
攻撃の種類		攻撃、侵入の契機	防御策	
攻撃*	外部	Webアクセス、ネットワーク接続（セキュリティホールを突く攻撃）	ファイアウォール	セキュリティホールをなくす（Windows Update）
	内部		パソコン内のファイアウォール	
ウィルス等の侵入		メールの添付ファイル、ファイルのダウンロード	ワクチンソフト（ウィルス対策ソフト）	

＊攻撃の一環としてウィルス等を送り込む場合がある



ファイアウォール

内部ネットワークの保護を目的として、外部ネットワークとの間に設置され、パケットの通過制御を行うシステム



アクセス制御

1. システムアクセス制御

システムの使用を正規ユーザに限定するための機能

識別(identification)と認証(authentication)

識別:アクセスしてきたユーザが誰であるかを認識すること(IDによる認識)

認証:名乗ったユーザの本人性を検証すること(パスワードによる検証)

2. リソースアクセス制御

リソース(データ、サービス等)へアクセスするユーザ、アクセス方法を限定するための機能

○ファイルパミッション(File permission)

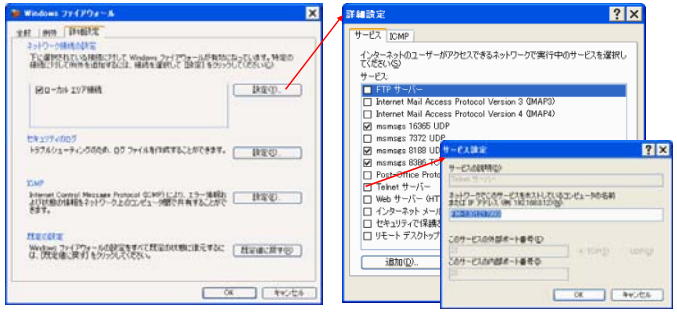
・対象の所有者、グループ、その他に分けて、対象に対するアクセス権を設定 (UNIXのuser/group/other制御)

(例)-rw-rw-r-- 1 owner group 81904 Nov 7 13:25 FILE1

13

付. Windowsファイアウォールでのサービス選択

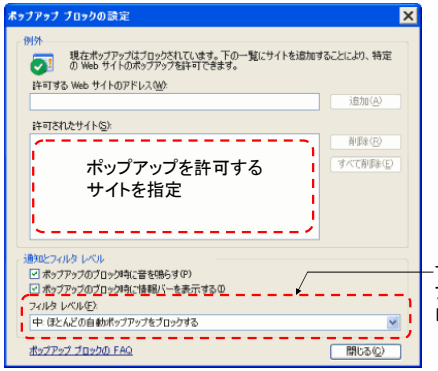
[セキュリティセンター]で[Windowsファイアウォール]をクリックし、[Windows ファイアウォール]プロパティの[詳細設定]タブで、[ネットワーク接続の設定]欄の設定ボタンをクリックする。その後、[詳細設定]ダイアログの[サービス]タブで、許可したいサービスの先頭のチェックボックスをクリックする。[サービス設定]ダイアログが開くので、確認し、OKボタンをクリックする。



14

付. IEでのポップアップブロック

ポップアップウィンドウにはJavaScriptなどによる不正スクリプトが存在する恐れがあるため、Windows XP SP2では初期設定でブロックされている。その制御を行う場合は、[ツール]メニューから[ポップアップブロックの設定]を選択する。

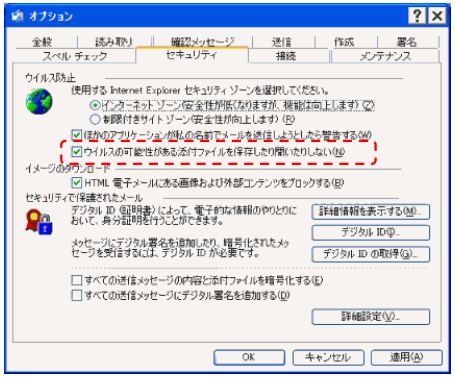


すべてのポップアップをブロックするにはフィルタレベルを高にする

15

付. Outlook Expressでの添付ファイル

Outlook Expressの[ツール]ー[オプション]で表示されるダイアログの[セキュリティ]タブでの「ウィルスの可能性がある添付ファイルを保存したり開いたりしない(N)」にチェックを付けておく(初期設定ではチェックが付いている)。



16