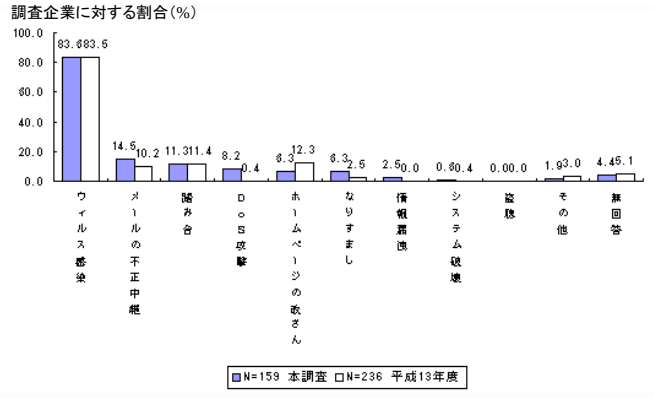
7. ネットワーク接続時の脅威

1

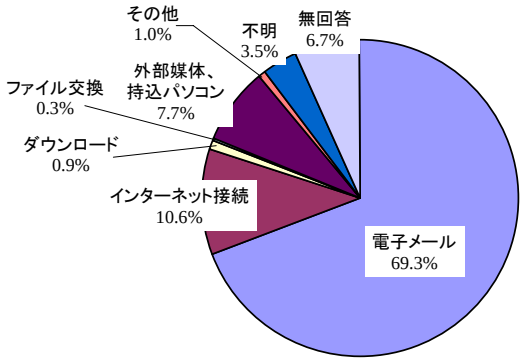
不正アクセスの被害



警察庁「不正アクセス行為対策の実態調査」2002年度(2003年5月12日)
http://www.npa.go.jp/hightech/cyberterror/nsresearch07/09.htm

2

付. ウィルスの感染・発見経路

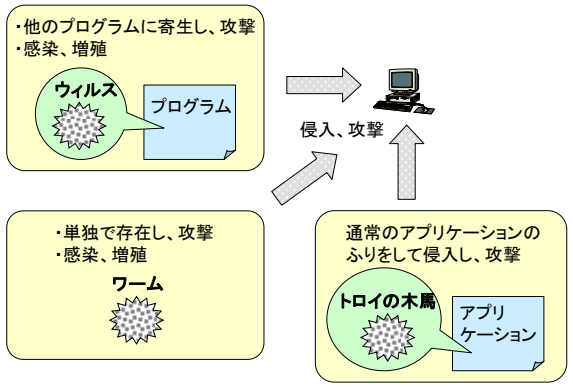


出典:IPAの「国内におけるコンピュータウイルス被害状況調査報告書(2005年4月)」

3

不正プログラム

コンピュータに侵入し、攻撃を行うプログラムには、**ウィルス**、**ワーム**、**トロイの木馬**などがある(総称して**ウィルス**と呼ぶこともある)



4

付．ウィルスの定義

通商産業省（現経済産業省）の定義

通商産業省告示 第952号（コンピュータウイルス対策基準）平成12年12月28日

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

(1)自己伝染機能
　自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2)潜伏機能
　発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3)発病機能
　プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

ウィルス感染の影響(1)

（1）情報漏洩

・コンピュータ内のファイルがメールの添付ファイルとして送信され、機密情報の漏洩に繋がる。
・キーボード入力を記録（**キーロガー**）して外部に送信され、機密情報の漏洩に繋がる。
・コンピュータの使用ユーザ名、組織名、デスクトップ画面、デスクトップのファイルなどがファイル交換ソフトの提供フォルダに置かれ、内部情報の流通に繋がる。

（2）情報の改ざん、消去

・ファイルやフォルダが削除される。
・Webページが改ざんされる。

（3）なりすまし

・メールソフトのアドレス帳にあるアドレス宛に、差出人を詐称したウィルス付きのメールが送信される。
・偽のアイコンが表示される。

ウィルス感染の影響(2)

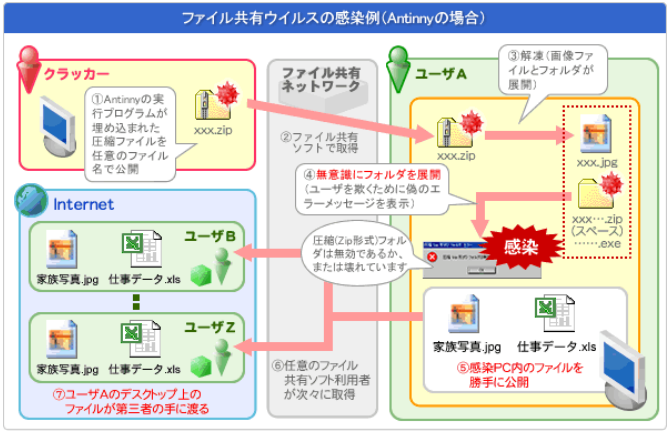
（4）不正使用

・画像が表示されたり、音楽が演奏されたりする。
・攻撃の踏み台にされ、自分が加害者になる。
・バックドアを設置し、再侵入を容易にする。

（5）サービス妨害

・コンピュータが不安定になり、再起動を繰り返す。
・アプリケーションソフト（ウィルス対策ソフトも）やコンピュータが起動できなくなる。
・コンピュータが乗っ取られる。
・特定のサーバに大量のパケットが送信され、ネットワークが混雑すると共に、そのサーバがサービス停止に追い込まれる（DoS攻撃）。

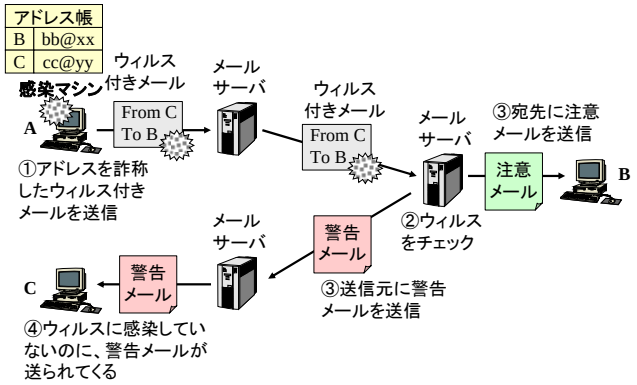
付．Antinny



http://www.security.ocn.ne.jp/guideline/virus/t_file.html

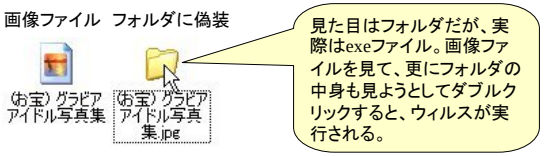
メールアドレスの詐称

メールソフトのアドレス帳や受信トレイにあるアドレス宛に、差出人を詐称したウィルス付きのメールが送信される。差出人もアドレス帳等にあるアドレスから選択される。

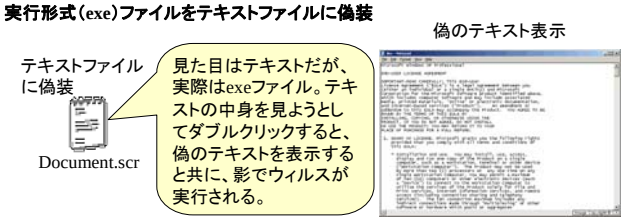


アイコンの偽装

実行形式(exe)ファイルをフォルダに偽装

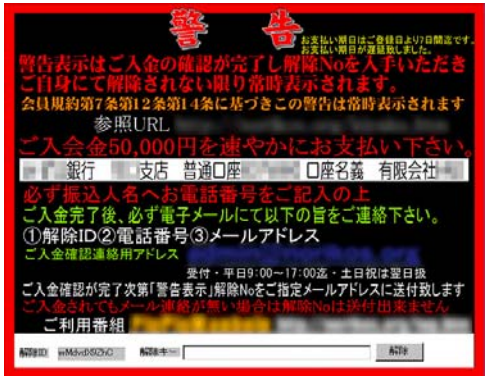


実行形式(exe)ファイルをテキストファイルに偽装



なりすましによる登録

・特定のWebサイトにアクセスするとウィルスがダウンロードされて感染
・感染したPCからメールアドレスを盗み、特定のアダルトサイトに登録
・入会金を支払って解除キーを受け取るまで、以下のメッセージを30秒ごとに表示

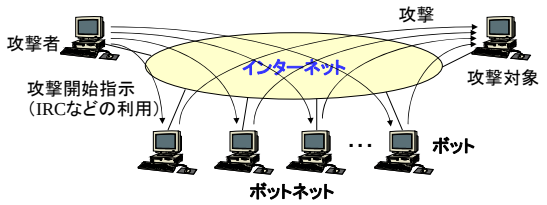


ボット

外部からの指示に応じた動作を行うプログラム
(ボットに感染したマシンは外部から操られる)

特徴
- ○ソースコードが出回り、ツールの整備もあり、作成が容易
  →変種が多く、ウィルス対策ソフトでの検出が困難
- ○感染マシンには障害を起こさないため、感染に気付きにくい
- ○詐欺、恐喝などの犯罪に使われることが多い

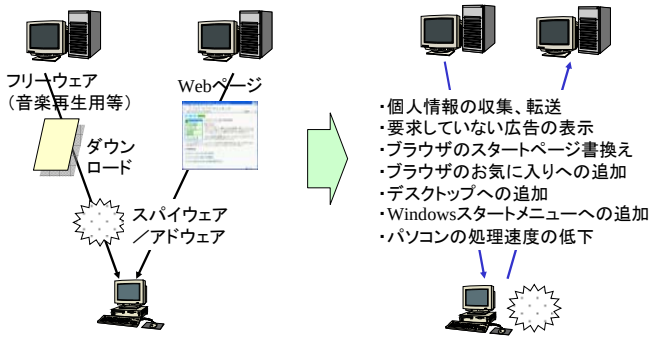
ボットによる攻撃例(DDoS)



スパイウェア

スパイウェア：利用者に気付かれずに、又は承認を得ずに、個人情報（利用者のWebアクセス履歴、パスワードなど）を収集し、転送するソフトウェア

アドウェア：強制的に広告を表示する代わりに、無料で使用できるソフトウェア



13

付．スパイウェアによる犯罪事例

2005年8月、米国でスパイウェアを使った大規模な個人情報盗難が発覚した。攻撃者はPC上のキーボード入力を記録して外部に送信するスパイウェア（キーロガー）を使って多数のパソコンからクレジットカード番号、社会保障番号、ユーザ名、暗証番号、インスタントメッセージのチャット内容、検索のために入力したキーワードなどの個人情報を収集した。関係した銀行は50にもおよび、連邦捜査局（FBI）による調査が行われた。

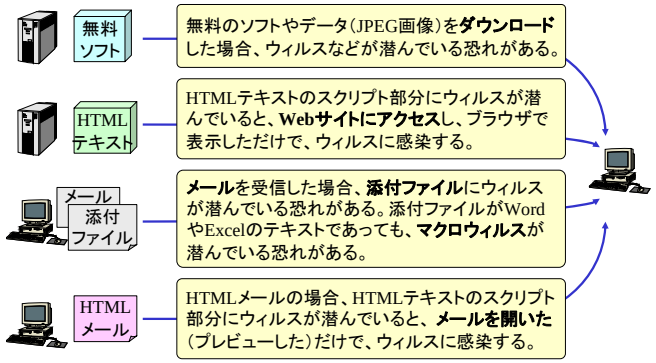
2005年7月4日、国内のネット銀行でパソコンの情報が盗まれ預金が引き出される事件が起こった。攻撃者はPC上のキーボード入力を外部に送信するスパイウェア（キーロガー）を使ってインターネットバンキングの利用者のPCから口座の支店名や口座番号、暗証番号を盗み、預金13万円を無断で引き出していた。

2005年7月9日、国内のネット銀行でパソコンの情報が盗まれ貯金が別の口座に転送される事件が2件起こった。攻撃者はPC上のキーボード入力を記録して外部に送信するスパイウェア（キーロガー）を使って利用者のPCからネットバンキング用のIDや暗証番号を盗み、利用者の口座から、別の口座に総額500万円を無断で転送した。

14

ネットワークからの取り込み(1)

ネットワークからのプログラムやデータの取り込みには危険が潜んでいる

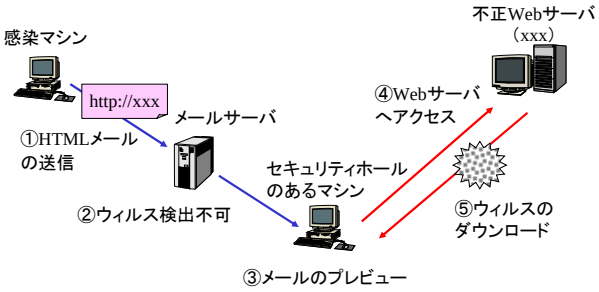


スクリプト：機械語に変換することなく実行できる簡易プログラム（JavaScript、VBScript）
HTMLメール：HTMLテキスト形式のメール

15

ネットワークからの取り込み(2)

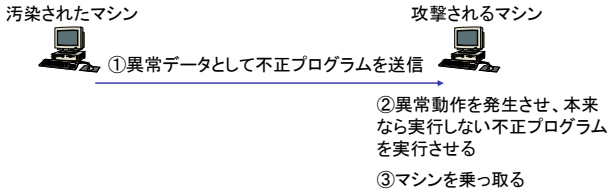
メールサーバのウィルスチェックで検出されないメールウィルス



16

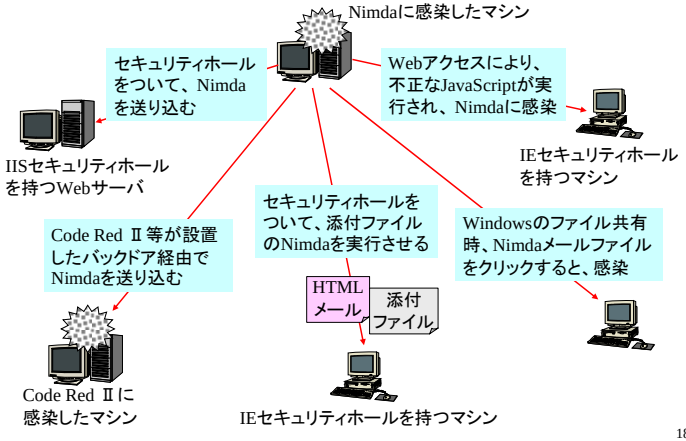
ネットワークへの接続

セキュリティホールがあると、ネットワークに接続しただけで、ウィルスやワームなどに感染する恐れがある



無線LANで、暗号通信などの設定を怠ると、情報漏洩や不正侵入に繋がる恐れがある。

付．Nimdaの例



媒体経由の感染

USBメモリや携帯音楽プレーヤの普及で、媒体経由のウィルス感染が増える傾向にある。

これまでの感染事例

- 1998年4月：通商産業省（現経済産業省）が入札説明会で配布したフロッピーディスクにウィルス（Laroux）が感染していた。
- 2001年：IBM 32MB USBメモリー・キーのブート・セクターが感染していた。
- 2006年9月：米アップルコンピュータのビデオiPodの80ギガバイト型と30ギガバイト型の2製品の一部がウイルスが感染していた。
- 2006年9月：日本マクドナルドが景品として配布した携帯音楽（MP3）プレーヤにウイルスが感染していた。

迷惑メール(1)

不要なメール、大量のメールなど、受信者にとって迷惑なメール

（1）スパムメール

- 広告メールなどのように、毎日何通も送られてくる不要なメール

（2）メール爆弾

- 圧縮率が非常に高い（例えば、1000倍）ファイルを添付ファイルとして、送信する。これを受信者側で解凍すると、ハードディスクの容量が圧迫され、パソコンの動作が不安定になる。
- 大容量の添付ファイルを持つメールを何通も送信し、メールボックスの容量を圧迫し、他のメールを受信できないようにさせる。

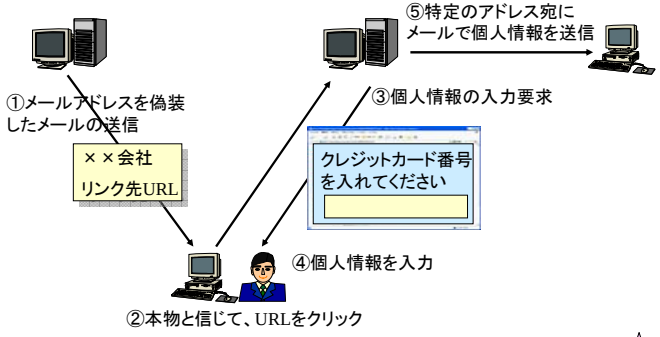
（3）チェーンメール

- 車の当たり屋の車両番号を知らせるメールなどのように、有用なメール、重要なメールに見せかけ、転送を促すメール

迷惑メール(2)

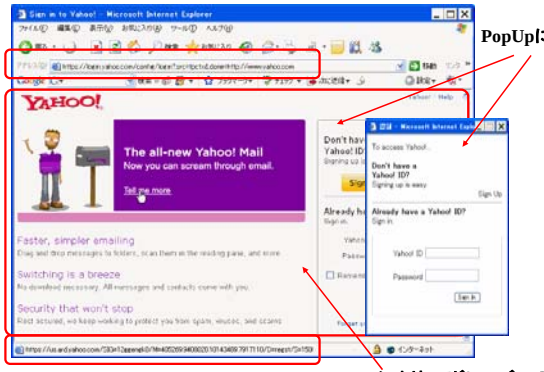
(4)フィッシングメール(phishing mail)

・本当の企業から送信したように見せかけたメールにより、偽のWebサイトへ誘導し、個人情報(クレジットカード情報など)を搾取するメール



Webページ表示時の偽装

アドレスバーの偽装



ステータスバーの偽装

IFRAMEにより、アドレスバーのWebページとは異なるWebページを表示

スピア型攻撃

特定の相手を狙った攻撃(フィッシング、スパイウェア等)。スピア(spear)とは槍。

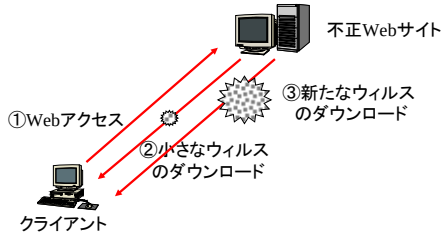
事例
・労働組合をかたるフィッシングメールが組合員に送られた。
・顧客を装った添付ファイル付きメールを送り、スパイウェアを送り込む。
・上司になりすまし、業務上の機密情報を搾取した。

http://www.trendmicro.com/jp/security/general/sclass/backnumber/sclass0603.htm

モジュラー攻撃

ウィルスがモジュール化されており、Webアクセス時などに最初は小さなウィルスがダウンロードされ、その後次々と新たなウィルスをダウンロードさせる攻撃

・最初のダウンロードは短時間で終了するため気付かれにくい。
・最初にダウンロードされるウィルスがウィルス対策ソフトで発見されないようにしている場合もある。



ブラウザクラッシャー

HTMLやJavaScriptの機能を悪用し、パソコンの動作を不安定にさせること

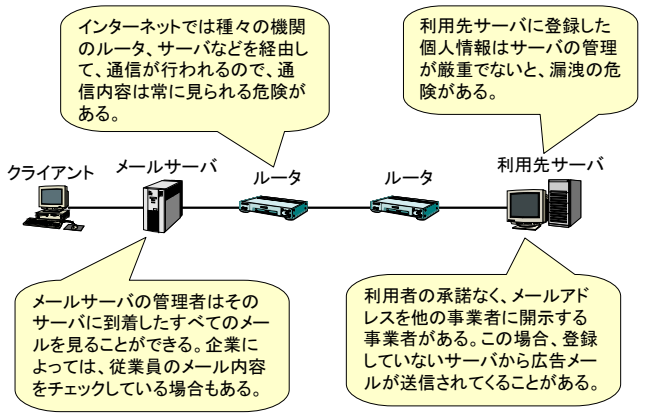
・JavaScriptを使用し、ブラウザを別画面で多数起動し、パソコンの動作を不安定にする。

・ HTMLテキストに、Outlook Expressなどのメールソフトへのリンクを多数埋め込むなどして、そのテキスト（Webページ）表示時に、メール送信ウィンドウを多数起動し、パソコンの動作を不安定にする。（mailtoストーム）

・HTMLテキストに、フロッピーディスクやCD-ROMへのリンクを多数埋め込むなどして、そのテキスト（Webページ）表示時に、フロッピーディスクやCD-ROMへのアクセスを頻発させ、パソコンの動作を不安定にする。

情報の漏洩

通信路や利用先サーバなどで、情報の漏洩が起こりうる



パスワードの盗難(1)

パスワードや暗証番号が盗まれると大きな被害に繋がる場合がある

・生年月日、電話番号、名前など、意味のある数字、文字列をパスワードや暗証番号に使用すると推測されやすい。

・パソコンやATMなどの使用時に、パスワードや暗証番号を肩越しに見られる恐れがある（**ショルダハッキング**）。

・ネットカフェなどのように不特定多数の人が利用するパソコンでは、**キーロガー**を仕掛け、パスワードなどを盗む場合がある。

・古いキャッシュカードの場合、カード内に利用者ID、暗証番号が格納されており、スキミングツールにより、これらが盗まれる危険がある。複数のカードで暗証番号を同一にしている人が多く、預金を引き出される恐れがある。

・電話や電子メールで、言葉巧みに、本人を騙し、ID、パスワードを入手する場合がある（**ソーシャルエンジニアリング**）。

パスワードの盗難(2)

・パスワードを忘れた場合に備え、個人的な質問と解答を登録しておき、パスワード問合せ時に、その質問に正解すると、パスワードを通知してくれる（**リマインダ**）。リマインダ機能は親しい友人などによって悪用される危険がある。

・利用者の操作性向上を目的として、メールソフトやWebブラウザでは、IDやパスワードをハードディスクに保存しており、利用者がこれらの一部を入力した段階で、自動で補う機能（**オートコンプリート**）を備えている。しかし、保存されている情報を抽出するツールがあり、パソコンを他人が使用できれば、これらの情報が盗まれる。

ホームページの開設

ホームページに掲載する情報には注意が必要

電話番号やメールアドレスを掲載していると、いたずら電話の対象となったり、広告メールが送られてくる場合がある。

独自のWebサーバには厳重な管理が必要

各種プログラムを最新の状態に保たないと、バグを突いた攻撃を受け、Webページの改ざん、サーバ内の情報の盗難、攻撃の踏み台にされるなどの危険を招く。

ドメイン名を登録すると、個人情報が公開される

ドメイン名を登録する時には、氏名、住所、電話番号などの情報を登録する必要がある。ネットワークに障害が生じた時などに、ドメイン名の責任者に連絡を取れるようにするため、これらの情報は公開される。しかし、これが悪用される危険がある。

29