ネットワークとセキュリティ

2002/2/18

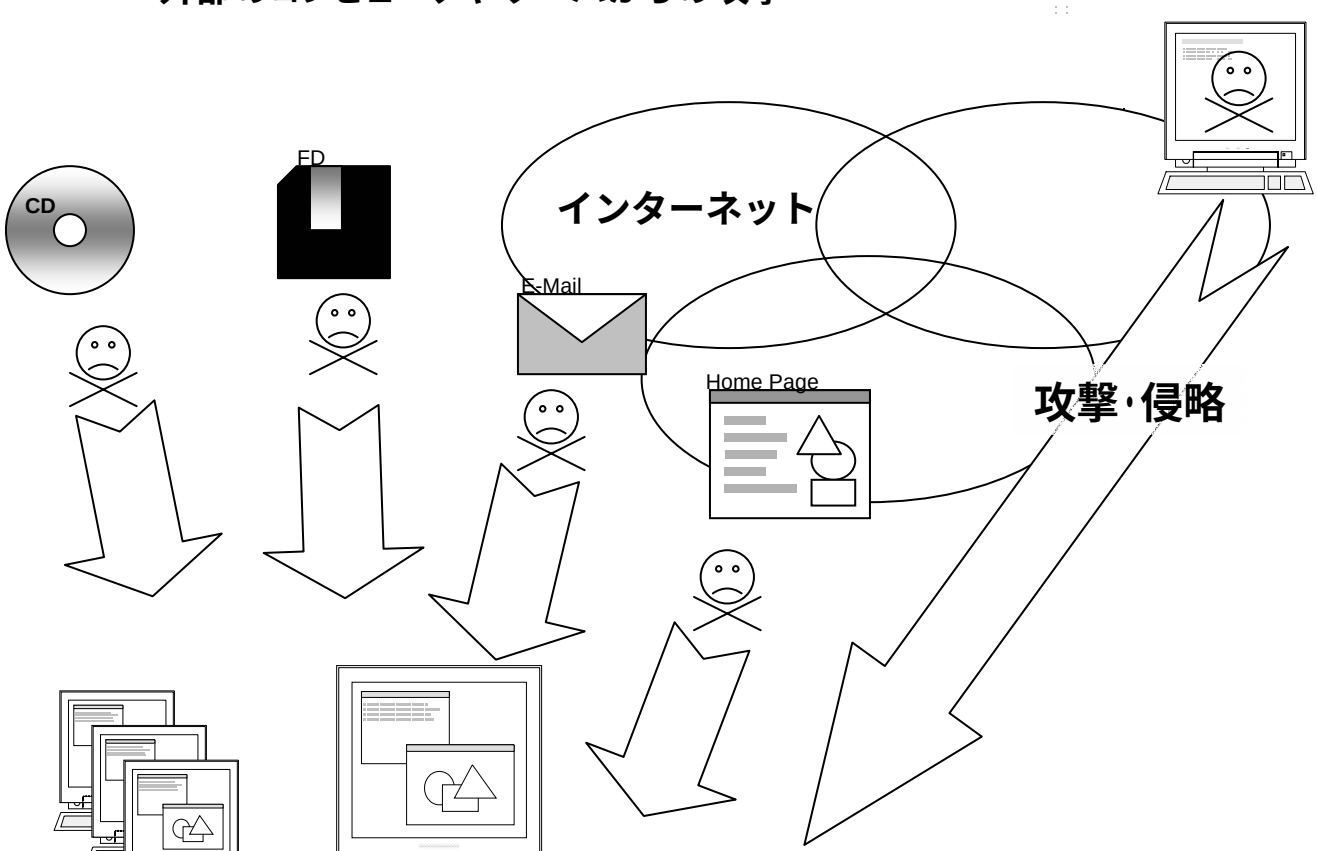
株式会社インフォランド
中田 隆

Microsoft Certified Professional

1. 脅かされるセキュリティ

1.1 外部から受ける攻撃

- ウィルスやワームなどを取り込み
- 外部のコンピュータやサーバからの攻撃



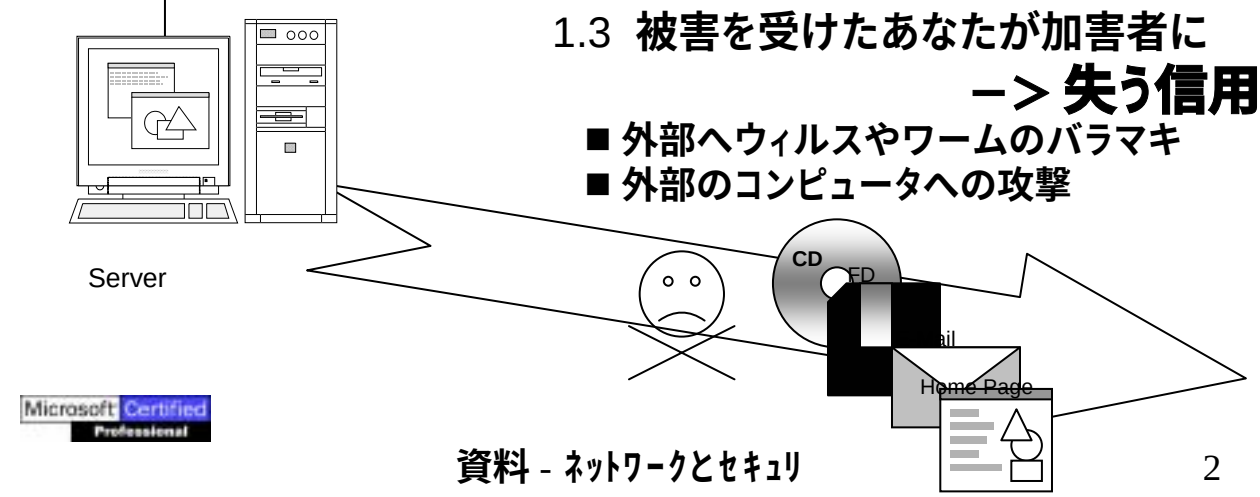
1.2 被害

- 動作しなくなるコンピュータ
- 各種データの破壊

1.3 被害を受けたあなたが加害者に

－＞失う信用

- 外部へウィルスやワームのバラマキ
- 外部のコンピュータへの攻撃



2. 外部から受ける攻撃の種類 (攻撃の概要を知ることが大切)

2.1 ウィルスやワームなど

ウィルス

- パソコンに一度感染すると、パソコン内のすべてのファイルやプログラムに自分をコピーする
- ある日付・時刻になるとファイルを消す、パソコンを起動できなくするなど障害発生

ワーム

- メールに添付された悪意のあるプログラムやスクリプト(Javaやその他のコマンドライン)。
- 発病するとアドレス帳にあるあて先に、自分自身を自動発信 －＞ 自分が加害者に

トロイの木馬

- 役立つプログラムを装い進入。
- 発病するとネットワークのセキュリティを解除したり、外部からの侵略を許す裏口を作成。
- 気のついたときには自社のコンピュータは外部から自由に覗かれたり改ざんされたり。

2.2 外部から受ける攻撃・侵略

データの改ざん (例: ホームページの改ざん)

- OSやネットワークのセキュリティの脆弱性をついて外部からコンピュータを自由に操作
- ホームページの改ざんを受けたときは、他のホームページを改ざんする攻撃を行うことが多い

データの流出

- OSやネットワークのセキュリティの脆弱性をついて外部からコンピュータを自由に操作。
- 悪意のある人間が特定のコンピュータを狙いハッキングする。

サービス不能攻撃

- OSやネットワークのセキュリティの脆弱性をついて外部からOSやネットワークを停止させる

大量データによるネットワークやサーバの性能低下

- 大量・大容量のメールを送りつけるなどの手段で過重な負荷を与える。

踏み台攻撃

- メールサーバなどデータをリレーする機能のあるサーバが、悪意のある他人から悪用される。
- メールサーバを踏み台にされると「外部からリレーされたメール」があたかも「自社のネットワークから送信されたように見える」ために、あたかも自社に悪意のある人間がいることに。

SPAMメール

- 価値のないメールを大量に送信。踏み台攻撃とセットで悪用されることが多い。

デマウィルス

- 「○○ウィルス情報。以下の対応を… この情報を知人に知らせてあげてください。」

3. ネットワークの保護

3.1 5つの基本

既知のセキュリティの脆弱性を改善

- 現在大流行のウィルスやワームおよび攻撃は殆んど既知のセキュリティーホールの悪用。
- セキュリティの脆弱性を改善すれば、保菌しにくい、発病しない、攻撃されない。
- マイクロソフトセキュリティーアップデートの活用。(Windows、BackOffice、Office)
- トレンドマイクロ、シマンテック、IPAセキュリティセンターには充実した情報が。

ワクチンソフトやファイヤウォールなど攻撃と侵略に対する防護壁を築く

- 対外部へのWebサーバやメールサーバはイントラネットと独立にする。
- インターネットとイントラネットの接続点にファイヤウォールを導入。
- サーバにはサーバ対応のワクチンソフトの導入。
- 各パソコンにワクチンソフトの導入。

利用実績の高いネットワーク構成の導入、ネットワーク機器とソフトウェアの利用

- 利用実績の多いシステム(Windows)は攻撃される事例も他と比較し突出して多い。
- それは悪意を持った人間から見れば、たくさんの人に迷惑をかけられることから当然のこと。
- 一方、攻撃の検出のスピードと、それへの対応法の開発と広報の迅速性と確かさかつ対応の解りやすさも優れている。
- 実績が高いので、理解している人口が多く、Webや書籍などの情報源も豊富。
- 反例としてサーバとファイヤウォールを両方ともLinuxで構成した場合、問題が発生するか否か？ 解決方法は如何に？ など苦労することになる。
- セキュリティのあるサーバとパソコンはWindows NT、Windows 2000、Windows XP Professionalのみ。(Windows 9x、Windows Me、Windows XP Home Editionでは不可能)

システム担当者はセキュリティに対し高度なスタディを (コンサルタントの導入も)

- いまやウィルスやワームは誕生後25時間で世界を席捲。 (CodeRedの場合)
- その対策法や対策ワクチンは発見後24時間以内にインターネットで配布。
- 攻撃に使われるメカニズムは多岐にわたり、新たな概念の攻撃も多数。
  －＞ 伝播スピードの把握と攻撃メカニズムの概要の理解が防御の第一歩。

利用ルールを作成。かつ利用者に厳格に守らせるための十分なセキュリティ教育

- 社外と自由にフロッピーでデータのやり取りを許している ？？？
- 雑誌のCDのプログラムが役立ちそうなので入れました ？？？
- 会社のパソコンを家に持ち帰り、家でインターネットをしています ？？？
- パスワードは付けていません ？？？
- みんながシステム管理の権限があります？？？
  －＞ ほとんどの会社が完璧には守れていない。
  －＞ ただし重要なシステムについては実施している会社も多い。

3.2 セキュリティで保護されたネットワークの実例