2002/05/08 担当 :岩見

3級 技術編 A09

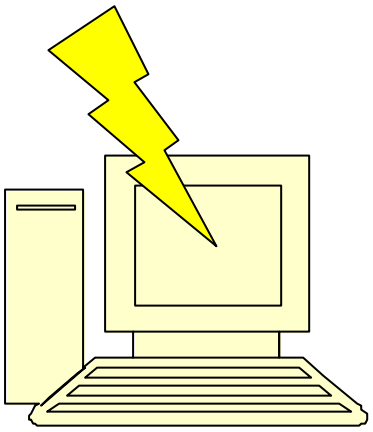
コンピュータへの攻撃とその対策

目的

・データを破壊・改変するため
・データを盗むため
・更なる攻撃対象への踏み台にするため

侵入経路

・無防備な設定を悪用
・セキュリティホール（セキュリティ上の弱点）からの攻撃
・バックドア（侵入しやすいように設けられた「裏口」）からの侵入
・ウィルス（トロイの木馬・ワーム等も含む）による攻撃
・パスワードクラック（辞書アタック・総当りアタック等）での侵入
・ソーシャルエンジニアリング



活動

（データの破壊・盗難）
- 機密データ・システム上重要なファイルの消去
- 機密データを侵入者の手元にコピー

（踏み台として利用）
- 侵入マシンからウィルスメールの送信、第３者への不正アクセス等をおこなう

（活動を隠すために）
- アクセスログ（接続記録）を、侵入者に関する部分、または一定期間分を消去
- 新しいユーザ ID を製作し、その ID で活動を行う（再侵入も容易に）

（活動・再侵入を容易にするために）
- ネットワーク接続設定を変更（入りやすい設定にする）
- アクセス権を書き換える（どのファイルにもアクセスできるように）

対策

（被害にあった？と思ったら）
- 被害にあったらまずマシンをネットワークから物理的に隔離（ケーブルを抜く等）
- 「活動」で示されているような変化が起きてないか確認
- それ以外でもいつもと何か違う点（設定・ログ）が無いか一通り点検してみる。

（被害にあったら）
- 必要なファイルをバックアップし、１度ディスクを初期化してしまうのが望ましい

（予防策）
- リリースされたセキュリティパッチ（修正プログラム）を当てておく
- 必要以上の外部からのアクセスを許可しない（不必要なサービスは停止しておく）
- ワクチンソフトを導入してウイルス感染を予防する
- ファイヤーウォール（不正アクセスを防ぐための機器やソフト）の構築
- 内部ユーザに対し、セキュリティ意識を高めるような指導を行なう