不正プログラム調査 WG

WG リーダー
株式会社アークン　渡部　章

■ 活動目的

トロイの木馬、スパイウェア、リモートアクセスツールなど、不正アクセスを目的にしたハッキングツールが増加しています。また、ウイルス、ワームも同様に 近年では不正アクセスを目的としたものも少なくありません。実際の不正アクセス技術ではこれらのツールを組み合わせて利用するケースが多く、不正プログラムとその対策の調査研究を実施し、その成果を普及させます。

■ 活動内容

様々な不正プログラムを分類化し、その利用目的を明らかにし、各分類における代表的な不正プログラムと、昨今話題となっている不正プログラムのメカニズムを説明できるような資料を作成公開します。合わせて具体的な対策方法も示して、この種の技術に関する正しい知識を広めていきます。また、既存のセキュリティ技術のこれら不正プログラムによる侵入、攻撃に対する有効性を検証します。

■ 年間活動予定

- 月1回程度の会合
- 年1回の合宿
- 成果物の取りまとめ

2006 年 3 月　合宿風景

■ 過去の成果物

「メモリ感染型ネットワーク・ワームの脅威とその対策」（2002年度）

当WGが発足した2002年度は、今後の方向性を見極めるために将来的成果物のインデックスを作成しました。その中から、年度中にまとめられる内容として、一連のワーム事件を特に取り上げ､「メモリ感染型ネットワーク･ワームの脅威とその対策」について報告書を作成しました。他の組織からの報告書と差別化するために、既存対策で検出できなかった理由、事件後の対応状況や、今後の対策への考察を中心にまとめました。

「不正プログラム対策ガイドライン」（2003年度）

不正プログラムの定義、分類、構造、対策についてまとめました。対策としては、セキュリティルールの策定方法について、また、対策ツールの導入については、スタンドアロン、LAN、インターネット接続、グループウェアなど環境別に取りまとめました。

「絵で見るネットワークのぜい弱性と脅威」（2004年度）

近年、不正プログラムがセキュリティ問題の中核を成していることを鑑み、特に注意を要するネットワーク上の脆弱性と脅威について、わかりやすく取りまとめました。その骨組みとして攻撃頻度の高い脆弱性を技術的に取りまとめた「SANSインターネットセキュリティ脆弱性トップ20」を利用し、特筆すべき近年の脅威について追加しました。

■ 本年度の活動

本年度は、不正プログラムを分類化し、タイプ別、レイア別に、その対策ソリューションを調査、整理し、マッピング化することにしました。予定している成果物としては、「不正プログラム対策ガイドライン ver.2」です。本ガイドラインは、「ユーザ企業の視点でセキュリティソリューション購入のガイドとなる」および「セキュリティソリューションの販売者がユーザ企業への説明用に使用できる」ことを目的としています。

■ 今後の展開について

ウイルスによる被害は、他のセキュリティ被害に比べて圧倒的なもので、これは今後も継続するに間違いないと思われます。ただし、ウイルス対策ソフトウェアなどの既存セキュリティ技術では対策が十分ではないワームや、キーロガーなどのトロイの木馬、そしてスパイウェアなどによる情報漏えいは、新しい脅威として既に多大な被害が出てきています。これらの背景から当WGは、不正プログラムをウイルスだけに留めず、広範囲にその現況と対策について調査研究を実施していきます。