2006 年 9 月 22 日

ネットワーク解析とインターネット犯罪者との戦い（概要）

弊社では「通信パケットログ」をベースに通信解析システム「Ｃｕｓｔ．ＦＡＩシステム」の開発・製造・販売・監視代行サポートを行っています。

現在、通信を使った情報システムへの攻撃・侵入・情報漏洩が問題になっており被害も多く出ています。この被害の事実や範囲を証明するため、近年「ネットワーク・フォレンジック」が脚光を浴びています。弊社通信解析システムは「通信パケットログ」をベースにしているため、被害の事実や範囲の証明は他社製品よりはるかに簡単に行え、また状況を確認することができます。

弊社通信解析システムでは、送信元・送信先がＩＰアドレスだけでなく「企業名・団体名」で表示されるなど一目見て状況がわかる工夫がされています。これに加えＰ２Ｐ通信検知機能はＷｉｎｎｙやＳｈａｒｅなどの Ｐ２Ｐ通信に関連する通信データを表示しますが、接続先が一目でわかりますので通信データを復号する必要がありません。実際に実験した結果、海外に多くの接続先があることが判明。防衛庁や公務員の情報漏洩が単に国内だけでなく海外に漏れていたという驚愕の事実がわかりました。

最近ではＩＴに詳しくない人たちのパソコンにボット型ウィルスが入り込み、ここを踏み台にして政府機関が攻撃される事件が発生しています。このボット型ウィルスは送信元のＩＰアドレスに他のＩＰアドレスを使うため、実際に攻撃を受けた場合、送信元がわからないという問題がありました。弊社通信解析システムでは不正な通信に対する送信元の通信経路探査とその通信記録を不正な通信の記録と結びつける機能があり、これによりボット型ウィルスが存在するネットワーク（ボットネット）が特定できるようになりました。

弊社では通信解析システムを弊社の情報システムに接続し、現在までインターネットからの様様な攻撃・侵入行為を解明、成果をホームページに公開しています。

本展示におきましては上記成果の説明に加え、弊社通信解析システムを使用し「ネットワーク・フォレンジック」の紹介、通信解析の手順などを実演していきます。

有限会社　日本ネット技術研究所　森田富治男
http://www.netpub.tsuzuki.yokohama.jp/index.html