2005 年 10 月 24 日

報道関係各位

東海大学

インターネットに接続されているサーバの約１万５千台に１台は不正
～不正パケットの分散観測により推定に成功～

東海大学(神奈川県平塚市北金目 1117、学長：髙野二郎)の電子情報学部 菊池浩明研究室では、中央大学理工学部情報工学科の土居研究室及び日立製作所 HIRT(Hitachi Incident Response Team)との共同研究で、不正パケットの分散観測技術を開発し、サーバやパソコン、ルータなど、インターネットに接続されている全ての機器のうち、他のコンピュータへ侵入を試みる、いわゆる「不正ホスト」の総数と密度を明らかにすることに成功いたしました。

今回、不正ホスト数を明らかにするために用いた技術は、「ポートスキャン*1 の独立一様分布の仮定に基づく数学的モデル*2」で、2005 年 5 月 31 日から 8 月 31 日までの間、計 5 台の観測装置で測定した不正パケット（不正侵入や攻撃を目的とするアクセス）の累計データを適用して算出いたしました。

従来の定点観測*3 実験がアクセス先やポートごとの平均パケット数の推移だけに留まっていたのに対して、今回の技術開発はインターネットに接続されている不正ホストの密度が初めて明らかになり、1 万 5 千台に 1 台は不正であると判明いたしました。

また、脆弱性のあるホストをインターネットに接続した場合、20 分後には全体の 70%が感染し、60 分後には全体の 95%が感染するという結果が出ております。加えて、不正ホストは、1 秒あたり平均 78.27 回の攻撃、コンピュータウイルスなどのスクリプトの実行を実行していると判断できます。

この技術により、不正ホストからの平均的な影響を考慮して、ネットワークの安全な運用や設計が可能になると期待しております。

なお、本実験の詳細は 10 月 26 日（水）より、愛媛県松山市の「メルパルク松山」で開催される、情報処理学会主催の「コンピュータセキュリティシンポジウム 2005（CSS2005)」にて発表予定です。

この件に関するお問合せ
東海大学　学長室広報課　担当：関野
Tel：0463-50-2402（直通）

実験環境

	観測装置（S1）	観測装置（S2）	観測装置（S3）	観測装置（S4～S6）
観測期間	2005 年 5 月 29 日～8 月 31 日			8 月 1 日～31 日
ﾕﾆｰｸﾎｽﾄ数 (異なる攻撃者数)	1326	3938	4754	各々1100
接続するﾈｯﾄﾜｰｸ	大学 A 構内	大学 B 構内	ｲﾝﾀｰﾈｯﾄ直結	大学 B 構内（設置場所は別々）
ﾈｯﾄﾜｰｸｸﾗｽ	B	B	C	B
ﾌｨﾙﾀﾘﾝｸﾞ	あり	あり	なし	あり

*1 サーバやパソコン、ルータなど、インターネットに接続された端末のネットワークポートにアクセスし、各ポート上のセキュリティの弱点を探し出すという不正アクセス手法。

*2 攻撃対象をランダムに選択すること。選択はステートレス（過去の履歴を考慮しない）に行うこと、単位時間当たり一定の割合で攻撃すること、攻撃者の IP アドレスは静的であることを仮定している。

*3 インターネット上に設置した複数のセンサーから得られる情報を解析して、脆弱性情報などを提供するシステム。警視庁や有限責任中間法人 JPCERT コーディネーションセンターで運用されている。