

- 大規模なサービス不能攻撃などを再現可能な「不正パケット模倣装置」を開発
 - 平成14年11月12日
-

独立行政法人通信総合研究所(理事長:飯田尚志)は、不正アクセスに強いネットワークおよびサーバの設計・開発に役立つ、不正パケット模倣装置を開発しました。本装置を使うことで、大規模なサービス不能攻撃などが再現可能です。

<背景>

インターネットの電子商取引などに使用されるサーバは、大勢のユーザによるアクセスに耐える頑丈なものである必要があります。そのようなサーバの開発のためには、大量のパケットを模擬的に発生させる装置を使って、耐久性能を検証することが不可欠です。また、インターネットからの大規模な不正アクセスでは、パケットのヘッダー(発信元などの情報が書かれている冒頭部分)の内容を偽の情報と置き換えて発信元などを詐称した「不正パケット」が多く用いられますが、このような不正パケットを模擬的に大量に発生させる装置については、これまで実用化はされていませんでした。

<概要>

このほど通信総合研究所は、大量のアクセスによりコンピュータのサービスを不能にするDoS(Denial of Service)攻撃などに使われる不正パケットを模擬的に発生させる装置を開発しました。不正アクセスに強いネットワークやサーバを設計・開発するためには、このような装置による検証が役立ちます。今回開発した装置は、あらかじめ取得した不正パケットのパターンデータを編集することや、構成方法の分かっている不正パケットパターンを専用の言語を用いて記述し、生成することなどが可能です。これらの不正パケットのパターンデータに基づき、指定した時間間隔や発生量で不正パケットを発生させることができます。ギガビット級ネットワークを埋め尽くすほどの大量の不正パケットを発生させ、DDoS(Distributed Denial of Service: 分散型サービス不能)攻撃などの大規模な攻撃を再現することが可能です。

本装置は、11月14日にホテルJALシティ広島で開催される、「第12回ITRC(インターネット技術研究委員会)研究会」のデモ解説セッションにおいて公開されます。

<連絡先>

通信総合研究所
情報通信部門 非常時通信グループ
滝澤 修
Tel. 042-327-5542

不正パケット模倣装置の構成と外観

