報道発表

- **情報通信危機管理研究開発施設による研究開発に着手**
- **平成13年5月23日**

独立行政法人通信総合研究所（本所：東京都小金井市貫井北町4-2-1　理事長：飯田尚志）は、不正アクセス行為やサイバーテロなどの不正行為を未然に防止する技術を確立するための「情報通信危機管理研究開発施設」を整備し、本格的な研究開発に着手しました。

＜背景＞

今後極めて大きな発展が見込める電子商取引などのIT市場において、不正アクセス行為やサイバーテロは、発展の大きな阻害要因となります。それらの不正行為を未然に防止する技術を確立するために、通信総合研究所は平成12年度公共事業等予備費により、情報通信危機管理研究開発施設を本所内に整備しました。

＜施設の概要＞

情報通信危機管理研究開発施設は、不正アクセス行為を検証・再現し、分析するための模擬実験システム（テストフィールド）を備えています。同模擬実験システムは、実際のインターネット環境を模擬したもので、その中で模擬的に不正アクセス行為を再現し、攻撃側の振る舞いと被害システム側の状況を詳細に解析することができます。（補足資料2）

また、実際に行われた不正アクセス行為の事例を蓄積するための記憶システムも備えています。同記憶システムには、不正アクセスの手法やシステムの脆弱性に関する情報が格納され、実際に不正アクセス行為が発生した場合に、この情報との照合を行い、上記模擬実験システムを使って解析することで、いち早く対策を講じることができます。（補足資料3）

これらの不正アクセス模擬実験システムおよび不正アクセス事例記憶システムは、通信総合研究所が横河電機株式会社（本社：東京都武蔵野市中町2-9-32　社長：内田　勲）と共同で開発しました。
同システムのモデルは、6月4日～8日に幕張メッセにおいて開催される"Networld ＋ Interop2001 TOKYO"において横河電機のブースにて展示される予定です。

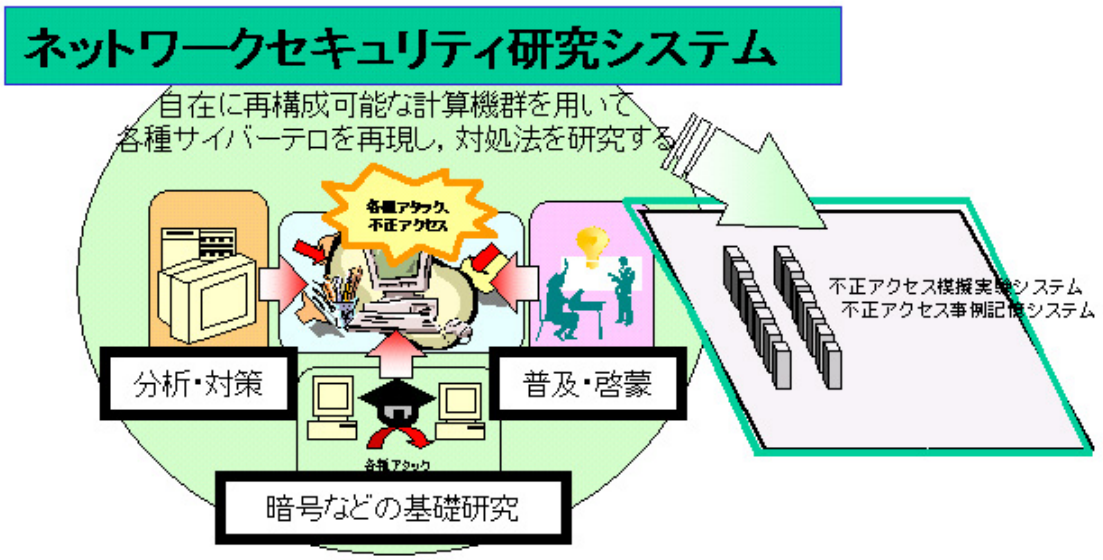
＜今後＞

通信総合研究所では、同施設を用いた研究開発に着手し、不正アクセス行為やサイバーテロへの対策法の開発を行います。また実際のシステムの脆弱性評価に資するため、本施設を用いた共同研究や受託研究の実施も進める考えです。

（お問い合わせ先）
独立行政法人通信総合研究所
情報通信部門　非常時通信グループ
担当：大野浩之、滝澤修
Tel: TEL：042-327-5542　　FAX：042-327-7941

[補足資料1]

情報通信危機管理研究開発施設



システムの概念図

システムの外観

[補足資料2]

＜不正アクセス模擬実験システム＞

- インターネット上のウェブサイトの利用形態をモデルとして、以下からなる実験環境を構成し、この模擬環境上で実際の不正アクセス状況の再現を可能としている。
    - サービス不能攻撃模擬サブシステム
    - 模擬インターネットサブシステム
    - 測定サブシステム外部ネットワーク
    - 測定サブシステム公開用ネットワーク
    - 測定サブシステム内部ネットワーク
- 特にサービス不能攻撃模擬サブシステムにおいては、複数の仮想ネットワークの構築などをグラフィカル・ユーザ・インタフェースを使い簡単に実インターネット環境に即して構成することが可能となっている。
- 不正アクセスを受けるサーバ、ネットワークから、負荷率やリソース消費状況など各種データの収集を、一元的に行うことが可能となっている。
- 不正アクセス状況をリアルタイムに把握することが可能となっている。
- 実験システムを管理するアプリケーションはJAVAを用いて作成されているため、プラットホーム非依存で使用することができる。
- この装置を用いて、不正アクセスツールの動作とアタックを受けるシステムの被害の詳細解析を行うことができる。
- また、不正アクセスを受けた際のネットワークセキュリティ機器（ファイアウォール等）の動作の検証を行い、脆弱性の改善、対抗手段の検討を行うことができる。

[補足資料3]

＜不正アクセス事例記憶システム＞

- 不正アクセスに関する技術、およびその影響と対策、その他の情報を脆弱性情報として格納している。
- 海外より収集した脆弱性情報については、日本語翻訳の上データベース化しており、参照及び活用が容易となっている。
- 脆弱性データは、他の脆弱性データベースとの互換性を考慮したフォーマットになっているため、データの増強が容易になっている。
- 具体的な脆弱性攻撃手順を脆弱性情報の重要項目として扱い、攻撃の検出方法の検討、再現、対策の実証に利用することが可能になっている。
- 脆弱性情報のライフサイクルを考慮して情報の追加、更新、破棄を行うことができ、更新履歴が残るようになっている。
- 脆弱性情報の項目ごとの検索、および全文検索を行うことができる。
- 脆弱性情報の一次データストアとしては、信頼性を重視してリレーショナルデータベースを利用している。
- 検索結果や編集結果の脆弱性情報の入出力はXMLで行い、情報の二次利用、およびオフラインでの利用が可能になっている。