3.6.1　情報通信セキュリティ研究センター　インシデント対策グループ

グループリーダー　　中尾康二　ほか 8 名

広域ネットワーク（サイバー空間）で発生するセキュリティインシデントを的確・迅速に把握し、実時間の原因特定、対策導出の実現に向けた研究開発

【概　要】

インターネットに代表されるサイバー空間の安全性及び信頼性を確保するためのセキュリティインシデント対策を中心としたネットワークセキュリティにかかわる基盤技術、応用技術の研究開発を行う。

(1)　サイバー空間上で発生する各種攻撃の分析を目指し、攻撃の各収集点で効率的･効果的に攻撃イベントを収集管理する技術の研究開発を行う。

(2)　サイバー空間上で発生する（又は蓄積された）各種イベントの挙動傾向、挙動原因、他挙動との因果関係等を実時間で解析するイベント分析技術の研究開発を行う。

(3)　イベント分析の結果とその結果情報から得られた蓄積ノウハウに基づき、各種攻撃に対する事前対策、インシデント対応（現状対応）、事後対策に係る総合技術の研究開発を行う。

(4)　各種データ収集法の研究開発と、サイバー空間上でのイベントの効果的収集と、以後の分析のための管理･運用技術に関する研究開発を行う。

(5)　各種イベントに対して複数の単体分析を実時間で並行的に実施し、それぞれの分析結果間の相関分析･統合分析により、イベント挙動傾向・原因・他イベントとの関連を導出する。

(6)　過去のイベント分析結果等に基づき、各種イベントに起因する攻撃の予兆を洞察し、予知されるインシデントに対する事前対応及び緊急対応に関する研究開発を行う。

(7)　上記の技術を総合的に関連･連携させ、統合型分析システム（nicter）を柔軟性高く構築することにより、今後のネットワーク系研究開発基盤システムを実現する。

【平成 22 年度の成果】

(1)　イベント収集管理技術の研究開発

①　トラフィック収集

委託研究「インシデント分析の広域化･高速化技術に関する研究開発」との連携の下、国内複数組織に新たに nicter センサを展開し、ダークネット（未使用 IP アドレス）トラフィックの情報源の拡大を図るとともに、地域･組織間のインシデントの差異などを把握することを可能とした。

図 1　変化点検出システムの Web インターフェイス

②　スパムメール収集

ダブルバウンスメール（送信元 / 宛先不達メール）だけではなく、実ユーザに届くスパムメールの収集を開始した。これにより、スパムメールを大量送信する大規模なボットネットの特定やより広範囲なリンク先分析が可能となった。

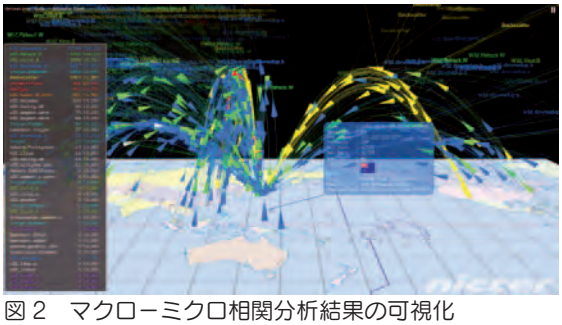

図 2　マクロ－ミクロ相関分析結果の可視化
（ロケット上部にマルウェア名を表示するとともに、マルウェア種別ごとに色分け）

(2)　イベント分析技術の研究開発

①　変化点検出システムの高度化

変化点検出システム用データベースの高速化を行いトラフィック量増加への追随を可能とした。また、同システムにドリルダウン機能を追加し、統計データを詳細に分析することが可能になった。

②　マクロ－ミクロ相関分析の実現

ダークネットで観測したトラフィック（現象）から、送信元のホストに感染しているマルウェア（原因）の特定を可能にするマクロ－ミクロ相関分析エンジンの開発に世界で初めて成功した。また、相関分

析の結果を準リアルタイムに可視化表示する可視化エンジンを開発した。

③　スパムメール解析システムの構築

スパムメールの送信元や、メール本文に含まれる URL のリンク先などの情報を基にクラスタリングを行い、スパムメールとボットネットとの相関関係を明らかにするスパムメール解析システムの構築を行った。

④　ミクロ解析システムの高度化

マルウェア感染ホスト（犠牲ホスト）の OS の自動切り替え機能を持ったマルウェア動的解析システムを開発し、マルウェアの動作環境に合致した解析が可能となった。また、バイナリコードの良悪性判定機能を開発し、入力されたバイナリコードがマルウェアか否かを、その挙動を基に判定可能となった。

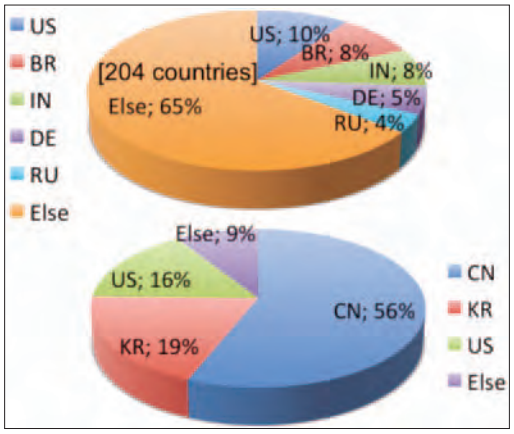

図 3　スパムメール送信元（上）とリンク先（下）の国別分析結果

⑤　マルウェアの分類アルゴリズムの開発

マルウェアの API シーケンスをスレッドごとに分割して、そのシーケンスを基にクラスタリングを行うアルゴリズムを開発し、マルウェアの挙動ベースの分類を可能とした。

(3)　サイバー攻撃対策導出技術の研究開発

①　ダークネット観測に基づくアラートシステム DAEDALUS（Direct Alert Environment for Darknet And Livenet Unified Security）のアラート集約方法やユーザインターフェイスの高度化を行うとともに、機構内ネットワークへの導入を行い、実インシデントの検出のための運用試験を実施した。

②　委託研究「マルウェア対策ユーザサポートシステム」との連携の下、nicter のミクロ解析システムを応用し、マルウェアの簡易駆除ツール（Stopper）の自動生成・自動配布を実現するシステムの構築を進めた。

(4)　IPv6 ネットワークにおけるセキュリティ検証

①　産学官が連携し IPv6 ネットワークにおけるセキュリティ検証を行う IPv6 技術検証協議会を設立し、IPv6 セキュリティテストベッド設計・構築を行うとともに、IPv6 模擬攻撃システムを導入し、各種のセキュリティ検証を行った。

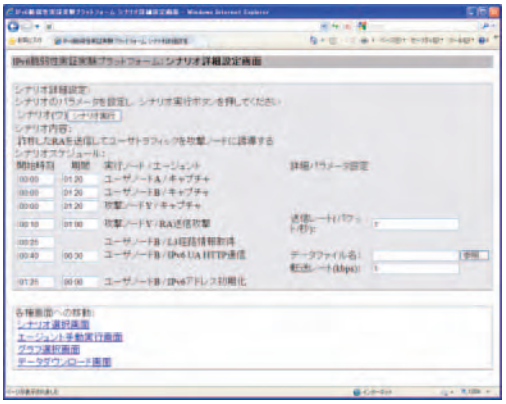
図 4　IPv6 模擬攻撃システム操作画面

(5)　新世代ネットワークセキュリティアーキテクチャ検討

①　ネットワークアーキテクチャグループと連携し、新世代ネットワークにおける脅威分析と、セキュリティアーキテクチャの基礎検討を行った。

(6)　外部組織との連携、技術移転

①　外部の共同研究者に nicter の蓄積データを安全に提供するためのプラットフォーム NONSTOP（Nicter Open Network Security Test-Out Platform）のフィルタ機能等の高度化を進めるとともに、国内 3 大学と連携し実証実験を開始した。

②　nicter の可視化技術を応用したトラフィックリアルタイム可視化ツール NIRVANA（NIcter Real-network Visual ANAlyzer）にフィルタ機能やフロー表示機能を追加し、国内企業への導入を行った。また、機構内ネットワークにも導入し、ネットワーク管理の高度化・効率化に貢献した。

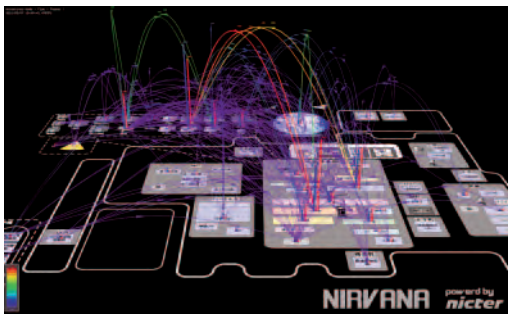

図 5　NIRVANA による機構内ネットワークの可視化