3.7.1　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 12 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っている。

(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 21 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

国内組織からのダークネットトラフィックの受信範囲の拡大及びセンサ拡充への取組として、国内の複数の大学組織と連携し、幅広いダークネットトラフィックの提供を受けるべく環境構築をすすめ、現在 14 万以上のダークネット（未使用）IP アドレスの観測を実施した。

②マルウェア検体収集

マルウェアの侵入経路の多様化に対応するため、平成 20 年度に開発した高対話型ハニーポットによる検体収集を実施した。また、スパムメールによる感染経路の解析等対策を行うためにスパムメールの収集を開始し、1 日 あたり 30,000 通以上のスパムメールを収集し、解析を実施した（図 1）。

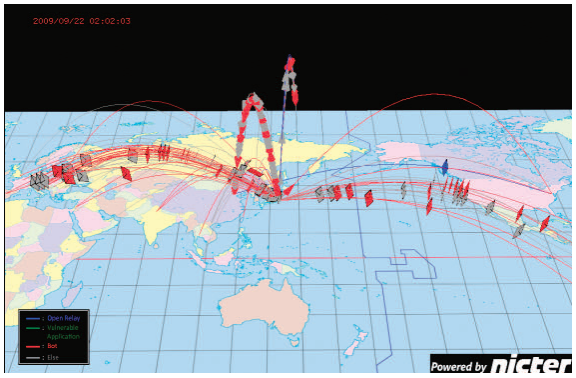

図 1　収集を開始したスパムメールの可視化

(2)イベント分析技術の研究開発

①マクロ解析システムの高度化及び拡充

マクロ解析システムの機能拡充として、マルウェア挙動のスペクトラム解析エンジン SPADE（SPectrum Analysis for Distinction and Extraction of malware features）の開発、変化点検出エンジン CPD（Change Point Detector）の高度化、及びパケットヘッダの特徴に基づいたダークネットトラフィック分類手法の提案を行い、高度化を続けるサイバー攻撃の検知が可能となった。

②可視化・分析システムの拡充

実際にユーザが利用するネットワークにおけるリアルトラフィックの観測・可視化システム Atlas X を開発し、Interop Tokyo 2009 の基幹ネットワークである ShowNet において実運用に供され、障害把握・ボ

トルネック調査等に貢献した（図 2）。同時に、nicter における各種可視化エンジンを Web アプリケーションとして実装することで、外部組織との連携体制を強化した。

③ミクロ解析システムの高度化

近年、高度化の一途を辿るマルウェアに追随するため、ミクロ解析システムの機能拡張として、ハーダ模擬機能付き動的解析システム、半開環境型サンドボックス（マルウェアの実インターネットへの接続を限定的・段階的に開放することができる解析環境）、及び汎用マルウェア難読化解除ツールの研究開発を行った。

④マクロ－ミクロ相関分析の実運用に向けた、nicter 保有情報の高速データベース化

ダークネット観測による膨大なトラフィックを高速に処理するため、データベースの分散管理、冗長化及びロードバランシング機能を駆使し、高速な新規登録・検索システム（MacS DB）を開発した。また、ミクロ解析システムにおいては、解析結果をより効率的に管理するためのミクロ解析結果データベース（MicS DB）を構築した。さらに、nicter の要であるマクロ－ミクロ相関分析を実現するためのデータベースであるマルウェア情報プール MNOP（ Malware kNOwledge Pool）の開発を行った。

⑶サイバー攻撃対策導出技術の研究開発

①外部組織との連携強化のためのプラットフォーム開発

外部の共同研究者に nicter の分析システム及び蓄積データを安全に提供するためのオープンプラットフォーム NONSTOP（Nicter Open Network Security Test-Out Platform）の試験運用を開始した。

②スパムメール分析フレームワークの構築

スパムメールの 90%以上がマルウェアによって送信されているという実態をより詳細に把握し、その背後にいるボットネットの全貌を解明するため、スパムメール送信分析システム、スパムメールリンク先分析システム、及びそれらの分析結果に基づくスパムメールを媒介したマルウェアの活動を視覚化する可視化エンジンを開発した。

⑷ IPv6 環境における脅威分析と対策手法の導出

①IPv6 におけるセキュリティ脅威分析

IPv6 におけるプロトコル上あるいは実装に依存する 60 項目以上の脅威・脆弱性を明らかにした。また、そのうち特に重要性の高い 15 項目について、模擬攻撃環境を構築し、それらの脆弱性を悪用した攻撃が成立することを実証した。

②ホームネットワークを対象とした IPv6 セキュリティ対策技術の開発

ホームネットワークの出入り口で家庭内部を守る IPv6 セキュアホームゲートウェイ（SHG）のプロトタイプ開発を行った。

⑸ nicter を応用した研究開発

①リアルトラフィックの可視化ツールの開発

nicter の可視化ツールを応用して、ネットワークトラフィックの可視化ツール（AtlasX）を開発し Interop Tokyo 2009 の基幹ネットワーク ShowNet で障害把握等の実運用実験を実施した。実験での成果を NIRVANA（NIcter Real-network Visual ANAlyzer）としてパッケージ化し、一部企業へ販売・納入を実施した（図 2）。

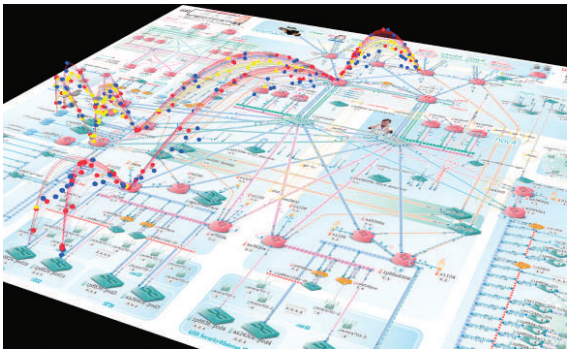

図 2　Interop Tokyo 2009 ShowNet において実施したリアルトラフィック可視化実験の模様