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11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。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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20年度の成果

⑴　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

平成19年度に引き続き、学術研究機関より幅広いサブネット長のネットワークの提供を受け、当該ネットワークに到達するトラフィックをNICT小金井本部へ転送する環境を維持し、トラフィックの収集を継続した。上述のトラフィックを収集するセンサ群に加えて、現在幅広いダークネットトラフィックの提供を受けるべく大学等と各種交渉や環境構築を進めた。

②　マルウエア検体収集

ア　オープンソースのマルウエア検体収集システムによるマルウエア検体収集

インシデント対策グループが本収集活動のために確保したインターネットアドレスにおいて、オープンソースのマルウエア検体収集システムの最新版の稼働を継続して運用し検体収集を実施した。

イ　複数の機関からのマルウエア検体提供体制確立

マルウエア検体の提供収集体制を確立し、大手アンチウイルスベンダ等、複数の機関からマルウエア検体の提供を受け１日あたり約2,000検体以上の送受信を開始した。これにより、*nicter*が保有するマルウエア検体の網羅性の向上が期待できる。

ウ　高対話型ハニーポット開発

最新のマルウエアを捕獲するため、実機Windowsの高速自動復元機構と二次感染防止機構を持つ、高対話型ハニーポットを開発し、試験運用を開始した。この開発により、最新のマルウエアを収集することが可能になる。

③　*nicter*アクセス制御機構

*nicter*ではダークネットトラフィックやマルウエア検体など機密性の高い情報を扱う一方で、企業研究所や大学等、複数の研究協力者が必要となり、遠隔からの*nicter*へのセキュアアクセス機能の構築が必須となる。そのため、外部の研究協力者が*nicter*にアクセスする場合のアクセス制御方式を具体化し、その実現に向けた階層的アクセス制御機構の研究及びそのプロトタイプ化を進めた。

⑵　イベント分析技術の研究開発

①　マクロ解析

広域ネットワークモニタリングを行うマクロ解析では、分析フレームワークの整備と各種分析エンジンについて機能強化を行った。

ア　変化点検出エンジン（CPD）の高度化

時系列データの変化を迅速に検出する変化点検出エンジンCPD（Change Point Detector）を高度化し、これまでの入力データであったポート番号ごとのパケット数だけでなく、全ポート番号の観測を可能にした。また、ポート番号ごとのホスト数やポート番号、スキャンパターンごとのホスト数など、多種多様な時系列データの変化点検出を可能にした。

イ　マルウエア挙動のスペクトラム解析エンジンSPADE開発

マルウエアのスキャンパターンに対し離散フーリエ変換によるスペクトラム解析を行うことで、マルウエアの挙動ベースの相関性を導出する分析エンジンSPADE（SPectrum Analysis for Distinction and Extraction of malware features）を提案し、プロトタイプ実装と評価を実施した。

ウ　ダークネット観測に基づくアラートシステムDAEDALUS開発

組織内部からの不正なトラフィックを分散展開したダークネットセンサで検出し、アラートを発行するという、従来とは逆転したダークネットの活用法によって、ダークネット観測を実ネットワークのインシデント対応に直結させる新しい観測アーキテクチャDAEDALUS（Direct Alert Environment for Darknet And Livenet Unified Security）を提案し、試験運用を開始した。

エ　長期振舞分析エンジンCHRONOS開発

マルウエアに感染したホスト群の、数か月から数年単位に渡る長期的な挙動を蓄積・分析する、長期振舞分析エンジンCHRONOSを開発し試験運用を開始した。

②　ミクロ解析

マルウエア検体の分析を行うミクロ解析では、完全に自動化されたミクロ解析システムの機能強化及び規模拡張を行った。

ア　大規模ミクロ解析システム環境構築

マルウエア自動解析（ミクロ解析）システムの解析エンジンを拡充し、並列処理による大規模解析環境の構築を行った。これにより、１日あたり最大2,000検体の自動解析性能を可能にした。

イ　ハーダ模擬機能付き動的解析システム開発

ボットを遠隔操作する攻撃者であるハーダの模擬機能付き動的解析システムを構築し、サンドボックス内でのボットの制御・詳細解析環境を実現した。

ウ　Webクローラ型ハニーポットの開発

Web経由で感染するマルウエアの出現を受け、Webを自動巡回しマルウエアの検体を収集するWebクローラ型ハニーポットシステムを開発し、実運用を開始した。

③　マクロ－ミクロ相関分析

ア　*nicter*オープンプラットフォーム計画NONSTOP始動

*nicter*にはトラフィックデータやマルウエア検体など、ネットワークセキュリティの研究に不可欠となる膨大な実データ群が蓄積されている。それらのデータ群を外部の共同研究者が安全に利用可能なオープンプラットフォームNONSTOP（Nicter Open Network Security Test-Out Platform）の構築を開始した。NONSTOPの実現により、*nicter*がネットワークセキュリティ研究の中心地となることが期待できる。

⑶　サイバー攻撃対策導出技術の研究開発

①　マルウエア駆除ツール自動生成・配布システム

*nicter*のマルウエア自動解析（ミクロ解析）システムを応用し、マルウエア駆除ツールの自動生成及びユーザへの自動配布システムのプロトタイプ開発を行った。このシステムは、*nicter*の分析オペレーションのユーザへの提供を目指すものである。

②　エクスプロイトコード検出エンジンの高度化

感染対象ホストの制御を奪取するための攻撃コードであるエクスプロイトコードの検出エンジンを高度化し、エクスプロイトコード検出をトリガにしたTCPストリームからのEXEファイル抽出や、エクスプロ

イトコード前後のTCPストリームの保存・分析を可能とした。

③　*nicter*インシデントレポート

*nicter*の各種分析エンジンから得られた分析結果により毎月インシデントレポートを作成し、継続的なレビューを行ってレポートの品質向上を図った。本インシデントレポートは、*nicter*の関連機関に対し情報展開する予定である。