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19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

ア　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

これまで観測していたダークネットトラフィックに加えて、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構築した。また、上記と異なる学術研究機関からもネットワークの提供を受け、こちらはインターネット上でIPsecを用いたセキュアチャネルを確立してトラフィックの転送する環境を構築した。これにより、nicterの観測アドレス数が倍増し、情報収集能力が大幅に向上した。

イ　センサ拡充への取組

上述のトラフィックを収集するセンサ群に加えて、現在、九州地区の大学及び欧州の電気通信事業者からのダークネットトラフィックの提供を、Telecom-ISAC Japanからはダークネットトラフィック及びISPのアドレスに設置したハニーポットが送受する高インタラクションなトラフィックの提供を受けるべく、各種交渉や環境構築を進めている。

②　マルウェア検体収集

ア　オープンソースのマルウェア検体収集システムによるマルウェア検体収集

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ェア検体収集システムの最新版を稼働させ、平成19年8月～平成20年1月にかけて新たに約1000検体の取得に成功した。

イ　Cyber Clean Center（CCC）からの検体提供体制確立

総務省・経産省連携のボット対策プロジェクトである CCC が捕獲したマルウェア検体の提供を受けるべく、検体送受のための光専用回線敷設等の環境構築や、マルウェア検体の安全な取扱ポリシに関する規程を整備した。平成19年度中の検体提供開始を目指し各種作業を進めた。

ウ　アンチウイルスベンダからの検体提供体制確立

大手アンチウィルスベンダから、毎週新規マルウェア検体の提供を受ける体制を確立し、平成19年

度後半より検体の取得を開始。これにより、nicterが保有するマルウェア検体の網羅性の向上が期待できる。

③　センサハイディング技術

nicter のトラフィック収集装置であるセンサは国内の複数箇所に設置されており、設置数は今後も増加していくことが見込まれる。センサのネットワーク的位置を攻撃者に知られないよう、センサとnicterセンタの間の通信は通信内容のみならず通信の存在自体を秘匿する必要がある。そのため情報ハイディング技術に基づくセンサ－センタ間通信秘匿技術の研究を進め、具体的な方式提案を行った。

④　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ェ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開始した。

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　nicter のセンサ群が収集したイベントを Information Bus と呼ぶ nicter 内部のマルチキャストチャネル上に流し、各種分析エンジンが Information Bus に join し分析を実行するという形態の、スケーラブルな分析フレームワークを整備した。

イ　トラフィック3D表示、世界地図表示、振舞分析表示の機能を拡張し、視点変更や拡大縮小、スナップショット機能、リプレイ機能など、オペレーションの柔軟性を格段に向上させた。また、統合的なユーザインターフェイスを構築しユーザビリティを向上させた。

ウ　時系列データの急激な変化を検出する変化点検出エンジンを用い、ダークネットトラフィックの全ポート番号を網羅的に観測し、変化点が検出されたポート番号に関してはより詳細な観測プロセスを開始する全ポート観測のアーキテクチャを提案し、nicterへの導入を行った。

エ　マルウェアの感染活動のうち、感染対象の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検出エンジンのnicterへの導入を行い、定常的観測を開始した。

②　ミクロ解析

マルウェ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　動的解析システムの箱庭環境にダークネット、低インタラクションセンサ及び実インターネットからのダウンロード機能を導入し、マルウェア解析能力の強化を行った。

イ　リモート制御型のマルウェアであるボットをホスト上で動作させ、コード解析技術の応用によりボットを制御するためのパスワードや命令群を自動抽出可能なボット動的解析システムを構築した。

ウ　ボットを感染ホストのメモリ上に展開した上で逆アセンブルし、アセンブリコードの中からボットの有する各種情報を自動抽出可能なボット静的解析システムを構築した。

エ　共同研究機関から提供される予定の大量のマルウェア検体の定常的な解析を実施するため、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を実現するための環境構築を行った。

③　マクロ－ミクロ相関分析

上記マクロ解析で観測されたインターネット上のスキャンの挙動と、ミクロ解析で抽出されたマルウェアのスキャンの挙動をプロファイルしてマクロ(現象)とミクロ(原因)の突合を行う相関分析システムのアイデアを更に拡張し、マルウェアの感染活動の第1ステップであるスキャンのみならず、第2ステップであるエクスプロイトコード、第3ステップのマルウェア本体のダウンロードを分析対象に取り入れることで、更に高精度の相関分析を実現する新しいコンセプトを提案した(JWIS2007 Best Paper Award受賞)。これはnicterNXT (次世代nicter)の核となるコンセプトである。

⑶　サイバー攻撃対策導出技術の研究開発

①　インシデント予測

ネットワークトラフィックから得られる時系列データ(単位時間当たりの特定ポートのへアクセス数

等)に対し、ウェーブレット解析を用いて予測を行う方式を提案し、nicterのダークネットトラフィックに適用した。

その結果、インシデントが発生する直前の兆候をとらえて、数時間後の予測が成功するケースが見られ、インシデント予測の実現可能性を示せた。

② 駆除ツール自動生成エンジン

ミクロ解析システムの動的解析の結果を応用・拡張して、マルウェアの駆除ツールを自動生成するエンジンをnicterに導入した。

③ 駆除ツール自動配布システム

ユーザの要求に従って、ユーザのマシンにマルウェア自動抽出エージェントを送り込み、抽出されたマルウェアをnicterのミクロ解析システムに送信してそれを動的解析し、その結果得られる駆除ツールをユーザに返送する駆除ツール自動配布システムのプロトタイプを実装中である。

④ 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から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。