主 論 文 要 旨

No. 1

報告番号	甲 ~~乙~~ 第　　号	氏 名	竹 森　敬 祐

主 論 文 題 目

ネットワークシステムにおける
サイバーテロ監視技術に関する研究

（内容の要旨）

近年、世界的な規模で広がりをみせるサイバーテロの脅威が高まっている。2001年7月にはCodeRedと呼ばれるコンピュータウィルスが、2003年1月にはSlammerウィルスが、同年8月にはBlasterウィルスが現れ、多数のホストがこれらに感染していまい、インターネットが一時的にサービス停止状態に陥るなどの影響が出た。このようなサイバーテロの脅威を最小限に抑え、安心・安全なネットワークシステムを提供するためには、各地のネットワークシステムの状態を的確に監視し、セキュリティログ等による未知の攻撃情報の収集を行い、これらの攻撃情報から、いちはやく脅威を分析して対策を促すセキュリティ監視センタ(SOC: Security Operation Center)の構築が重要な課題となっている。

本論文では、ネットワーク上で発生するコンピュータへの侵入攻撃やサービス不能攻撃等のサイバーテロを即座に発見し、その挙動の把握を可能とするSOCの運用に必須となる要素技術として、上記のシステムリモート監視、攻撃情報収集、セキュリティログ分析についてそれぞれ新たな手法を提案している。提案方式のシステム実装および評価実験を通じて、これまで検知できなかった攻撃やその被害を迅速に把握できることを明らかにし、提案方式の有効性を提示する。攻撃を的確に把握することは、ネットワークシステムの安定稼動に寄与できる。以下に具体的内容を示す。

第1章では、本研究の背景となるサイバーテロの検知手法に関する従来研究を概観し、本研究の目的と位置付けを明確にしている。

第2章では、Webサーバが管理するホームページ用のファイルをリモートから監視することで、改竄攻撃やネットワークサービス停止攻撃による異常を検知できるWebサーバリモート監視システムを提案している。本提案システムでは、リンクペ

主 論 文 要 旨

ージを辿ることにより監視対象となるファイルを自動的に抽出する機能と、ファイルのヘッダ情報やハッシュ値の変化に注目して改竄を判定する機能を有しているため、運用者の負担がほとんど無い状態において高い確率で Web サーバに対する攻撃を検知できる。大規模監視の実現性検証のために、インターネット上での監視処理速度に関する実験を行い、ネットワークへ与える負荷を軽減しつつ、局所的な輻輳に影響を受けない安定したリモート監視システムであることを定量的に明らかにしている。

第 3 章では、未知の攻撃情報を収集するためのシステムとして、侵入検知システム（IDS: Intrusion Detection System）と連携して、不審な通信コネクションを本来のシステムからおとりシステムへと切替えて行動ログを収集するトラップ型おとりシステムの切替え手法を提案している．本切替え手法は，本来のシステムとおとりシステムの通信状態の同期をとっておくことで, 切替え処理の高速性と通信シナリオの継続性を確保でき，侵入者におとりシステムの存在を気付かれない方式となっている。そして FTP サービスならびに Web サービスへの実装を行い, 実験用ネットワークを用いて評価を行った結果、侵入者に気付かれないレベルの高速な切替えを実現していることを確認している．このシステムにより、本来のサービスを提供しつつも侵入者の挙動・攻撃手法を容易に収集することが可能となる。

第 4 章では、広域ネットワークの各地に設置された IDS から出力される攻撃検知ログを統合管理して，異常なイベントを客観的に抽出する IDS ログ分析支援システムを提案している．本システムでは、ログに含まれる各種イベントの異常性について順位付けし、長期間のイベント傾向を比較対象として短期間のイベントの発生状況から、異常性を客観的な数値で評価する分析手法を提案している。各地で運用されている IDS の攻撃検知ログを用いて評価を行った結果，多量のイベント情報の中から、従来では発見が困難であった異常なイベントを特定できること、検証不要なイベントを排除できることを確認している。これにより、広域ネットワークを監視する運用者の作業負担を大幅に軽減すると共に、ネットワーク上で発生している攻撃の挙動を容易に把握することが可能となった。

第 5 章は結論であり、本論文の内容を総括している。