主　論　文　要　旨

報告番号	㊙ 乙　　第2557号	氏　名	寺　田　真　敏

主 論 文 題 目：

ネットワークワームに対処するためのインシデントオペレーションに関する研究

（内容の要旨）

2001 年以降の Code Red、Slammer、Blaster ワームの流布により、イントラネットならびにインターネットに接続する多数のシステムが感染し、ネットワークが一時的に停止状態に陥るなどした。このような大規模なネットワークワーム流布に対して以前は、被害が発生した後の対応であるインシデントレスポンスが中心であった。しかし、インターネットが社会インフラとしての地盤を固めたこともあわせ、インシデントに伴う被害を予測・予防し、インシデント発生後は被害の拡大を低減するために実施する一連のセキュリティ対策の総称であるインシデントオペレーションという対処の考え方が求められてきている。ネットワークワームを対象としたインシデントオペレーション実現には、脆弱性公開からネットワークワーム出現までの「脆弱性対策活動」とネットワークワーム出現以降の「インシデント対応活動」を通して流布の局所化や被害低減を図ることが重要となる。しかし、現在の情報システムにおけるネットワークワームの対処は、(1)ネットワークワーム出現に至るまでの状況を共有する仕組みがなく、また、(2)脆弱性から重要インシデントへの発展を可能な限り早期に弁別し事前対応する手順、ならびに(3)ネットワークワームの被害発生を想定したシステム構築の対応が不足している。

本研究では、1 つ目の課題に対して脆弱性ならびに修正プログラムの公開から「いつ攻略コードが公開されたのか？」「脆弱性を悪用したインシデントは何があったのか？」「インシデントに伴いどのような対策がとられたのか？」という脆弱性に関わる状況変化を共有するシステム JVN(JP Vendor Status Notes)を提案する。また、2 つ目の課題である脆弱性から重要インシデントへの発展を可能な限り早期に弁別し事前対応する手順に関しては、特に、各組織単独で実現可能なネットワークワーム挙動解析の検証環境が未整備であることに着目しネットワークワーム動作検証システムを提案する。3 つ目の課題である被害発生を想定したシステム構築では、ネットワークサービスを退避するという考え方に基づき被害を回避するイントラネット向けネットワークワーム流布対策システムである Web マッパを用いて解決を図る。

1 つ目の課題を解決する脆弱性に関わる状況変化を共有するシステム JVN は、システム管理者やシステムエンジニア向けに対策情報を広く告知することを目的とした公開型データベースであり、CERT Advisory ならびに CIAC Bulletin などの対策勧告に対する製品開発ベンダの対策情報を提供する Vendor Status Notes (VN)と、勧告で取り上げられた脆弱性に関わる経過を時系列イベント情報として提供する Status Tracking Notes (Trnotes)から構成している。本提案システムを用いることにより、システム管理者やシステムエンジニアの情報収集の作業軽減を図り、かつ、インシデントオペレーションに有効な情報共有が可能となる。また、2 つ目の課題を解決するネットワークワーム動作検証システムは、ネットワークワームがイントラネットのシステムに感染した場合、深刻な被害に直結するかいなかを予測するための重要な要因のひとつである探索特性と感染動作に伴い使用するポート番号に関する情報を収集する。提案システムは特殊な装置を使用する必要がなく、小規模な機器構成となっており、ネットワークワーム出現フェーズにおいて各組織単独でネットワークワーム挙動解析の検証が可能となる。3 つ目の課題を解決する Web マッパでは、イントラネットにおける HTTP サービスポートを攻略するネットワームワーム流布を回避するために、Web サーバの HTTP サービスのポート番号を代替ポート番号に移動させることでネットワークワームの流布を抑止する。次に、中継装置上で Web サーバの HTTP サービスが代替ポート番号に移動したことを利用者に意識させない機能を用いて Web サーバの稼動継続性を確保する。これにより、本来の Web サーバのサービスを提供しつつ、ネットワークワームの流布抑止が実現可能となる。

提案した各システムについて、試行運用、検証システムを用いた実験ならびに、提案方式に基づき実装したシステムの実環境での評価を通じて，ネットワークワーム出現に伴うインシデントオペレーション支援に有効であることを確認した。