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

平 成 17 年 度

寺田　真敏

あらまし

2001 年 8 月の Code Red，9 月の Nimda の流布，2003 年 1 月の Slammer，8 月の Blaster の流布によって, 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, ネットワークサービスが一時的に停止状態に陥るなどの影響がでた. このような大規模なネットワークワーム流布に対して今までは，インシデント (incident：人為的な事象により発生した事件) 発生後の事後処理を中心とした対処であるインシデントレスポンス (incident response) が進められてきた．しかし，インターネットが社会インフラとして普及するにつれ, インシデントに伴う被害を予測ならびに予防し, 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．そして，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 (incident operation) の実現には, 脆弱性ならびに修正プログラムの公開からネットワークワームが出現するまでの“脆弱性対策活動 (vulnerability handling)”とネットワークワームが出現した後の“インシデント対応活動 (incident handling)”の全体を通して, 被害を如何に予測ならびに予防するかという対策を実施することにより，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 つ目の課題を解決するために，脆弱性ならびに修正プログラムの公開から，いつ攻撃検証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処がとられたのか？，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，各組織単独で実施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 (Web mapper) を提案する.

本論文の構成は次の通りである.

第 1 章では, 本研究の背景とこれまでのインシデント対処の移り変わりを概観した後, 本研究の目的と位置付けを示す.

第 2 章では, 時代と共に様相を変えているセキュリティ侵害技術とそれに伴うインシデント対処の歴史について概説した後, 本研究に関連する従来研究とその課題について示す.

第 3 章では, 1 つ目の課題を解決するために, 国内で利用されているソフトウェアや装置の脆弱性を対象とした対策情報を提供する脆弱性／インシデント対処情報共有システム JVN を提案している. JVN は, セキュリティに関わるシステム管理者やシステムエンジニア向けに脆弱性対策ならびにインシデント対応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る. 脆弱性対策活動支援として CERT Advisory ならびに CIAC Bulletin など主要な対策勧告に対する製品開発ベンダの脆弱性対策情報を整理した後に提供する. また, インシデント対応活動支援として対策勧告で取り上げられた脆弱性に関わる時系列イベント情報の提供を特徴としている. 提案システムを用いることにより, セキュリティに関わる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支援に有効な情報共有が可能となる.

第 4 章では, 2 つ目の課題を解決するために, ネットワークワームの感染動作に関する情報収集を目的とした動作検証システムを提案している. ネットワークワームの感染先探索範囲は, 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否かを左右する要因のひとつであり, 感染拡大を予測する判断情報のひとつとなっている. また, ネットワークワームの感染拡大を防ぐにあたっては, 組織外部の情報に頼りきってしまうのではなく, 各組織単独で対策立案のための情報収集手段, たとえば, 感染動作を検証する実機環境などを保有することは早期対応ならびに情報収集のバックアップという点からも重要である. 提案システムはネットワークワーム流布時の対策立案への利用を踏まえ, 感染先探索範囲に関する動作情報の収集を目的としたネットワークワーム感染先探索特性の検証システムと, 感染動作に伴い使用するポート番号に関する動作情報の収集を目的としたネットワークワーム感染動作の検証システムから構成している. そして, 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していることから, 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.

第 5 章では, 3 つ目の課題を解決するために, HTTP (Hyper Text Transfer Protocol) ポート (80/TCP) を攻略するネットワークワーム流布時を想定したイントラネット向けの回避システム Web マッパを提案している. 情報システムが Web 主体に構成され

ているイントラネットにおいて，HTTP ポートを攻略するネットワークワーム流布に伴う影響は甚大である．HTTP ポートを攻略するネットワークワーム流布時の課題としては，ネットワークワームの流布抑止と Web サーバの稼動継続性確保の二面性を兼ね備えた対策が必要とされる．この課題を解決するために，Web マッパでは，Web サーバにおける HTTP ポートを任意の代替ポート番号に切り替え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 ポートを代替ポート番号に切り替えたことをユーザ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．

第 6 章は，インシデント対処の今後の展開であり，インターネットにおける新たな脅威とその対処体制の考え方である組織相互連携オペレーションについて示す．

第 7 章は結論であり，本論文の内容を総括している．

目次

あらまし

第 1 章 緒論 **1**
1.1 研究の背景 1
1.2 本研究の目的 3
1.3 本研究の位置付け 4
1.4 本論文の構成 4

第 2 章 インシデント対処の歴史と既存技術の課題 **7**
2.1 セキュリティ侵害技術の変遷 7
2.2 インシデント対処の変遷 13
2.2.1 インシデントレスポンス 13
2.2.2 インシデントレスポンスチーム 13
2.2.3 インシデントオペレーション 14
2.3 既存技術の課題 19
2.3.1 脆弱性公開以降の各種イベントの発生把握 19
2.3.2 ネットワークワームの挙動解析 23
2.3.3 被害発生を想定したシステム構築 27

第 3 章 脆弱性／インシデント対処情報共有システム **31**
3.1 まえがき 31
3.2 脆弱性／インシデント対処情報共有システム JVN 33
3.2.1 脆弱性／インシデント対処のための情報共有方式 33
3.2.2 試行サイトでの実現方式 39
3.3 試行サイトの有効性検証 43
3.3.1 利用実績ならびに利用状況 43
3.3.2 ネットワークワーム出現と時系列イベントの関連性 48
3.4 まとめ 50

第 4 章 ネットワークワーム動作検証システム **51**
4.1 まえがき 51
4.2 動作検証を実現する 2 つの検証システム 52
4.2.1 システム要件 53

4.2.2 ネットワークワーム感染先探索特性の検証システム 53
4.2.3 ネットワークワーム感染動作の検証システム 56
4.3 検証システムを用いた実験 60
4.3.1 既知ネットワークワームの感染先探索特性 61
4.3.2 既知ネットワークワームの探索動作における TCP 再送処理 68
4.3.3 既知ネットワークワームの感染動作 72
4.4 まとめ 78

第 5 章 ネットワークワーム流布対策システム 79
5.1 まえがき 79
5.2 Web マッパ 80
5.2.1 Web ポート／ホストマッピング方式 80
5.2.2 Web マッパのコンポーネント 81
5.2.3 実現方式 84
5.3 評価と考察 89
5.3.1 トラフィックの抑止効果 89
5.3.2 コンポーネントの機能動作確認 89
5.3.3 実イントラネット環境での実験的な利用 93
5.4 まとめ 96

第 6 章 インシデント対処の今後の展開 97
6.1 インシデントの変化 97
6.1.1 受動型攻撃 98
6.1.2 ネットワークワームの変化 100
6.2 組織相互連携オペレーション 106
6.3 まとめ 108

第 7 章 結論 109

謝辞 112
発表論文リスト 113
参考文献 115

図目次

図 1.1：既存技術に対する本研究の位置づけ 4
図 1.2：本論文の構成 6
図 2.1：インシデントの変遷 8
図 2.2：CERT/CC から報告された Code Red への感染状況 11
図 2.3：2001 年から 2005 年までのネットワークワーム流布履歴 12
図 2.4：Sasser ワーム出現までの経過 15
図 2.5：Blaster, Welchia ワーム出現までの経過 21
図 2.6：Code Red II 累積アクセス数と累積感染ホスト数 28
図 2.7：Nimda 累積アクセス数と累積感染ホスト数 28
図 3.1：JVN 試行サイトの構築ならびに運用の経過 32
図 3.2：脆弱性対策とインシデント対応 33
図 3.3：VN での情報提供事例 (JVNCA-2003-04) 44
図 3.4：JVN 試行サイトのアクセス数状況 44
図 3.5：TRnotes での提供情報事例 (TRCA-2003-22) 45
図 3.6：VN エントリ毎のアクセス数の推移 45
図 3.7：Sasser に関連する VN, TRnotes のアクセス状況 47
図 3.8：Netsky に関連する TRnotes のアクセス状況 48
図 4.1：ネットワークワーム感染先探索特性の検証システム構成 54
図 4.2：感染先探索特性の検証システムの Web インタフェース 55
図 4.3：ネットワークワーム感染動作の検証システム構成 56
図 4.4：DNAT を用いた送信先 IP アドレスの変換 58
図 4.5：感染動作検証システムにおけるフロー分析手順の概要 58
図 4.6：フロー分析に基づく送信先ポート番号の発生系列とその頻度の例 59
図 4.7：経過時間毎の探索 IP アドレス (Code Red 3) 62
図 4.8：経過時間毎の探索 IP アドレス (Nimda.E) 63
図 4.9：経過時間毎の探索 IP アドレス (Blaster) 64
図 4.10：経過時間毎の探索 IP アドレス (Sasser.B) 65
図 4.11：経過時間毎の探索 IP アドレス (Sasser.C) 66
図 4.12：経過時間毎の探索 IP アドレス(Slammer) 67
図 4.13：経過時間毎の TCP パケット送信数 (Blaster) 69
図 4.14：経過時間毎の TCP パケット送信数 (Code Red 3) 69
図 4.15：経過時間毎の TCP パケット送信数 (Nimda.E) 69
図 4.16：日本語版 Windows XP 環境での TCP パケット送信数 (Sasser.B) 70
図 4.17：日本語版 Windows XP 環境での TCP パケット送信数 (Sasser.C) 70

図 4.18：日本語版 Windows 2000 環境での TCP パケット送信数 (Sasser.B) 71
図 4.19：日本語版 Windows 2000 環境での TCP パケット送信数 (Sasser.C) 71
図 4.20：感染先探索特性の分類 77
図 5.1：Web ポート／ホストマッピングシステム 82
図 5.2：Web マッパ適用時のアクセス経路 84
図 5.3：ポート切り替え用 Apache サーバの定義ファイル (一部) 85
図 5.4：Microsoft IIS Web サーバ用のポート切り替え指示スクリプト 85
図 5.5：ポート／ホスト名称変換処理 87
図 5.6：Web ベースの管理インタフェース 88
図 5.7：hsc/hsd を用いたコンポーネント間連連携 88
図 5.8：hwmapd を介した環境変数表示用 CGI へのアクセス結果 91
図 5.9：異なるホスト名称に書き換えた場合の警告ダイアログ 91
図 5.10：IDS 連携機能指示による切り替えの完了報告 92
図 5.11：Web マッパ評価環境の構成概要 93
図 6.1：インシデントの変遷 98
図 6.2：MS03-026, MS04-011, MS05-039 を悪用するマルウェア発生状況 100
図 6.3：捕食関係にあったネットワークワームの感染報告数 102
図 6.4：感染先探索特性の分類 104

表目次

表 1.1：インシデント対処の比較 2
表 1.2：既存技術の課題と本研究の効果 5
表 2.1：警戒段階において調査対象となる情報 16
表 2.2：インシデントオペレーションにおける 6 つの段階 18
表 2.3：Doomjuice DDoS 機能活性化に関する情報 26
表 3.1：Vendor Status Notes における情報提供項目 34
表 3.2：Cisco IOS のサービス運用妨害の脆弱性に関連するイベント 36
表 3.3：OpenSSH のバッファ管理機構の脆弱性に関連するイベント 37
表 3.4：電子メール型ワーム Sobig.F の流布に関連するイベント 38
表 3.5：Status Tracking Notes における情報提供項目 39
表 3.6：Vendor Status Notes の構築フェーズ 40
表 3.7：通知手順で使用する電子メール通知フォーマット 41
表 3.8：TRnotes におけるイベントの特徴項目 42
表 3.9：Sasser に関連して発行した VN，TRnotes の概要 47
表 3.10：Netsky に関連して発行した TRnotes の概要 48
表 3.11：Windows 環境の脆弱性を悪用した代表的なマルウェア 49
表 3.12：Blaster，Sasser ワーム出現までの代表的な時系列イベント 49
表 4.1：Sasser ワームが選択する探索 IP アドレスの生成割合 52
表 4.2：アドレスブロック探査比率 (Code Red 3) 62
表 4.3：アドレスブロック探索比率 (Nimda.E) 63
表 4.4：アドレスブロック探索比率 (Sasser.B) 65
表 4.5：アドレスブロック探索比率 (Sasser.C) 66
表 4.6：フロー分析に基づく送信先ポート番号の発生系列 (Blaster) 73
表 4.7：フロー分析に基づく送信先ポート番号の発生系列 (Welchia) 74
表 4.8：フロー分析に基づく送信先ポート番号の発生系列 (Sasser.B) 75
表 5.1：ポート／ホスト変換コンポーネント hwmapd の定義ファイル 86
表 5.2：ネットワークワームが送出する TCP パケット数の比較 90
表 5.3：Web マッパ評価環境の Web サーバ台数 93
表 5.4：Web マッパ評価における確認項目 94
表 5.5：HTTP 要求／応答の 1 トランザクション毎の応答性能 95
表 5.6：コンポーネント切り替えの所要時間 95
表 6.1：Blaster，Sasser，Zotob の感染活動の比較 103
表 6.2：インシデント対処の今後の展開 107

第1章　緒論

1.1　研究の背景

1988 年 11 月に出現したインターネットワームは，最終的に何千というコンピュータシステムにまで感染を広げ，正常な活動とインターネットを何日間も混乱させた．それから 10 年後の 1999 年には電子メール型ワームである Melissa ウイルス，2000 年には Love Letter ウイルスが流布した．そして，2001 年にはネットワークワームである Code Red，Nimda，2003 年には Slammer，Blaster が流布し，インターネットの正常な稼動を阻害した．

このような電子メール型ワームやネットワークワームが利用するセキュリティ侵害技術は，基本的に人間やコンピュータシステムを騙すことにより重要な情報を引き出したり，正規のユーザとしてアクセスしたり，あるいは，サービスを提供できない状態に陥れるための技術であり，その本質は今も昔も変わってはいない．しかしながら，セキュリティ侵害技術は時代と共にその形態を変え，発生するインシデントも様相を変えてきている．すなわち，インシデントへの対処方法もインシデントにあわせて変えていく必要がある．

インターネットがビジネスの使い始めであった 2000 年前後と，社会インフラとして利用され始めた 2003 年以降の代表的なインシデントとインシデント発生に伴う影響の比較を表 1.1に示す．2000 年前後は，サイトへの不正侵入や Web ページの書き換えなど局所的な被害に留まっていたために，単独組織での対処かつ事後処理を中心とした対応で収まっていた．しかし，社会インフラとしても利用され始めた 2003 年以降のインシデントは，“ Slammer, Blaster などのネットワークワームの流布 ”, “ Blaster, Sobig.F，MyDoom 感染システムから特定サイトへの DDoS (Distributed Denial of Service) 攻撃 ” など，急速，大規模かつ広域に影響を与えるものとなり，単独かつ事後処理だけではインシデントに伴う被害拡大を低減することができなくなってきた．

表 1.1：インシデント対処の比較

項目	2000 年前後 インシデントレスポンス	2003 年以降 インシデントオペレーション
インターネットの利用度 (依存度)	ビジネスでの使い始め	社会インフラ
代表的な インシデント	サイトへの不正侵入 Web ページの書き換え	電子メール型ワーム ネットワークワーム DDoS 攻撃 悪性スパム フィッシングなど
インシデント発生に 伴う影響	局所的な被害 経済活動等への影響小	広範囲に渡る被害 各種業務等全般に関わるため 経済活動への影響大
インシデントの 対処体制	単独組織での対応	複数組織での共同対応
インシデント対処の 考え方	事後処理を中心とした対応	インシデントに伴う被害を予測 ならびに予防し，インシデント発 生後は被害の拡大を低減する 対応

インシデントの移り変わりを踏まえ，2003 年，経済産業省は 3 つの戦略と 42 の具体的施策項目から成る情報セキュリティ総合戦略を発表した．この戦略の中でしなやかな事故前提社会システムの構築を提示している [経産省 03].

戦略 1：しなやかな事故前提社会システムの構築
(高回復力／被害局限化の確保)

第一に，事前に事故を予防することや，起きた事故に対症療法的に対応することばかりではなく，情報セキュリティに絶対はなく，事故は起こりうるものとの前提で，事故／事件からの迅速な回復力の確保を図ったしなやかな社会システムを構築する．すなわち，全体として事故の回避(予防), 被害の最小化／局限化及び回復力の確保が達成されるよう，官民が連携して総合的な視点から対応を強化する．

このように，インターネットが社会インフラとして定着するに従い，インシデント発生後の事後処理を中心とした対処ではなく，インシデントに伴う被害を予測ならびに予防し，インシデント発生後は被害の拡大を低減するという対処の考え方が求められてきている．

1.2　本研究の目的

本論文は, インシデントオペレーションという考え方からネットワークワームを対象としたインシデント対処について，次の 3 つの研究をとりまとめたものである．

- 脆弱性ならびに修正プログラムの公開からネットワークワームの流布収束までの活動を支援する脆弱性／インシデント対処情報共有システムの研究
- ネットワークワーム出現フェーズの活動を支援するネットワークワーム動作検証システムの研究
- ネットワークワームの流布フェーズの活動を支援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の研究

ここで述べるインシデントオペレーションとは, インシデントに伴う被害を予測ならびに予防し, 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り，“ 被害が発生した後の対処 ”を中心としたインシデントレスポンスに，“ 被害を如何にして予防するか ”という活動を取り入れたインシデント対処の考え方である．

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には，インシデントに伴う被害を予測ならびに予防し, インシデント発生後は被害の拡大を低減するというセキュリティ対策の取り込みが不足している．そこで，本論文で述べる研究は，(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, 特に，各組織単独で実施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, 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という課題に着目する．そして，これらの課題の解決を通して，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を具現化していくことを目的とする．

本論文で示すインシデントオペレーションという考え方に基づいたインシデント対処は, 情報システムのシステム管理者やシステム構築に関わるシステムエンジニアにとって，安全で安心なインターネット環境の維持に役立つものと期待される．

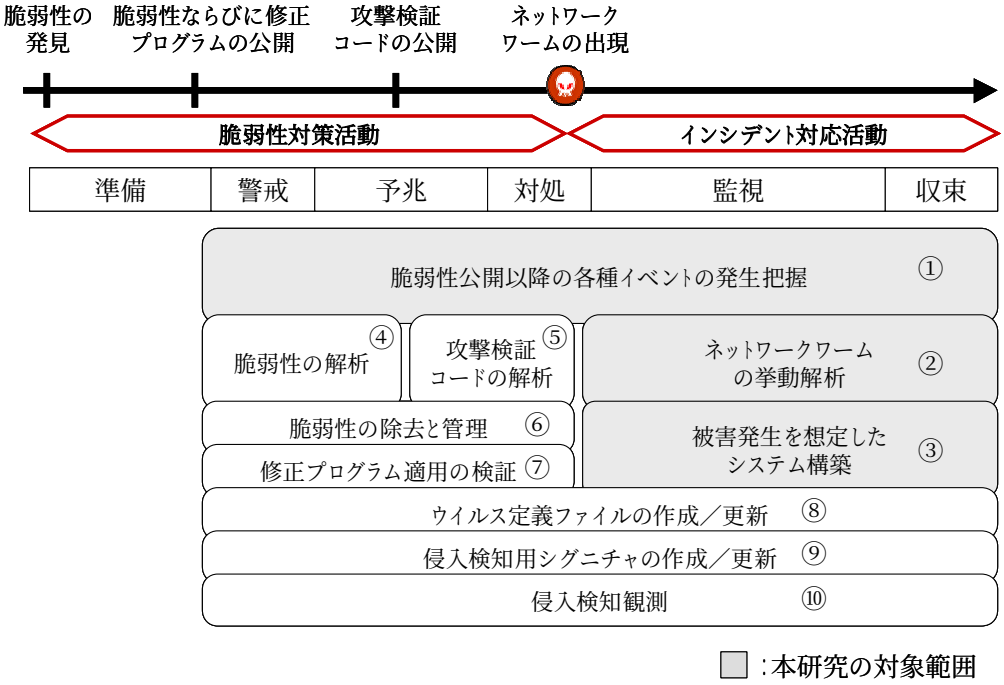


図 1.1：既存技術に対する本研究の位置づけ

1.3 本研究の位置付け

インシデントオペレーションは, 脆弱性ならびに修正プログラムの公開からネットワークワームの流布収束までを対象に対応活動をおこなう必要がある. それぞれのフェーズでインシデントオペレーションに必要とされる対応活動を図 1.1に示す. 本研究では, これら対応活動のうち, 脆弱性公開以降の各種イベントの発生把握 (図 1.1の①), ネットワークワームの挙動解析 (図 1.1の②), 被害発生を想定したシステム構築 (図 1.1の③)を対象としている. 表 1.2に既存技術の課題と本研究の効果を示す.

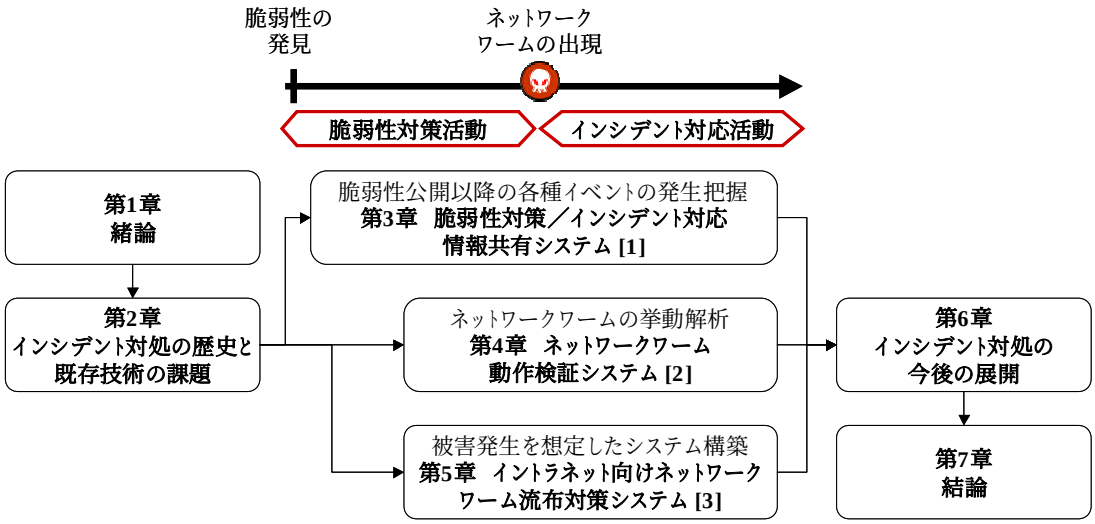
1.4 本論文の構成

本論文は, 緒言と結言を含め, 図 1.2に示す 7 章からなっている.

まず, 第 2 章は, 時代と共に様相を変えているセキュリティ侵害技術とそれに伴うインシデント対処の歴史について概説した後, 本研究に関連する従来研究とその課題について示す.

表 1.2：既存技術の課題と本研究の効果

章	項目	説明
第 2 章	対応活動	脆弱性公開以降の各種イベントの発生把握
	目的	ネットワークワーム出現ならびに収束に至るまでの状況を共有する仕組みを提供する.
	既存技術の課題	ネットワークワームが攻略対象とする脆弱性を対策するために必要となる国内製品に関する脆弱性対策ならびにインシデント対応情報については, 情報が散々しており, 影響範囲などを把握する手段が実現されていない.
	提案方式	主要な対策勧告に対する製品開発ベンダの脆弱性対策情報を整理した後に提供する, 対策勧告で取り上げられた脆弱性に関わる時系列イベント情報の提供することを特徴とした, 脆弱性／インシデント対処情報共有システム JVN を提案する.
	効果	提案システムを用いることにより, セキュリティに関わる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支援に有効な情報共有が可能となる.
第 3 章	対応活動	ネットワークワームの挙動解析
	目的	各組織単独で実施可能なネットワークワーム挙動解析の検証環境を提供する.
	既存技術の課題	ネットワークワームに関する公知となった情報を確認する, ネットワークワームに関する解析情報が公知になっていない時点で感染動作の情報を収集するなど各組織単独で実施可能な検証手段が実現されていない.
	提案方式	感染先探索範囲に関する動作情報の収集を目的としたネットワークワーム感染先探索特性の検証システムと, 感染動作に伴い使用するポート番号に関する動作情報の収集を目的としたネットワークワーム感染動作の検証システムを提案する.
	効果	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.
第 4 章	対応活動	被害発生を想定したシステム構築
	目的	HTTP ポートを攻略するネットワークワーム流布時のイントラネット向けの回避システムを提供する.
	既存技術の課題	ネットワークワーム流布時に, 稼動しているネットワークサービスを縮退あるいは退避させる考え方に基づいたシステム構築は実現されていない.
	提案方式	Web サーバの HTTP ポートを任意の代替ポート番号に切り替えることでネットワークワームの流布を抑止し, 中継装置上に Web サーバの HTTP ポートが代替ポート番号に切り替わったことをユーザに意識させない機能を備えた回避システム Web マッパを提案する.
	効果	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可能となる.



[ ]は，発表論文リスト(p.113)に掲載した論文の番号であり，
各章はその論文をもとに執筆したことを示す．

図 1.2：本論文の構成

第 3 章から第 5 章は，インシデントオペレーションという考え方に基づいたインシデント対処に関する具体的な研究を述べたものである．

第 3 章では，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いという 1 つ目の課題を解決するために，セキュリティに関わるシステム管理者やシステムエンジニア向けに脆弱性対策ならびにインシデント対応情報を広く告知することを目的とした脆弱性／インシデント対処情報共有システム JVN を提案している．第 4 章では，各組織単独で実施可能なネットワークワーム挙動解析の検証環境が整備されていないという 2 つ目の課題を解決するために，ネットワークワームの挙動に関する情報収集を目的とした動作検証システムとして，感染先探索特性の検証システムと感染動作の検証システムを提案している．第 5 章では，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という 3 つ目の課題を解決するために，HTTP ポートを攻略するネットワークワーム流布時のイントラネット向け回避システムとして，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ネットワークワーム流布対策システム Web マッパを提案している．

第 6 章は，インシデント対処の今後の展開であり，インターネットにおける新たな脅威とその対処体制の考え方である組織相互連携オペレーションについて概説する．

最後に，第 7 章では結言として，本研究で得られた研究成果を総括的に述べ，今後の課題について示す．

第2章　インシデント対処の歴史と既存技術の課題

本章では, 時代と共に様相を変えているセキュリティ侵害技術とそれに伴うインシデント対処の歴史について概説した後, ならびに, 本研究に関連する従来研究とその課題について示す.

2.1　セキュリティ侵害技術の変遷

本節では, 時代と共に様相を変えているセキュリティ侵害技術とそれに伴うインシデントについて, 図 2.1に示すインシデントの変遷に沿い概説する.

(1) Web ページの書き換え

1993 年, WWW (World Wide Web) をより簡単に使えるようにしたブラウザ NCSA (National Center for Supercomputing Applications) Mosaic の登場と共に, インターネットのセキュリティ侵害技術は, Web, Java を攻略対象としはじめた. この背景には, Web, Java の普及と共に, 1996 年に入り Web, Java に関連する脆弱性が顕在化したことにある. 特に, NCSA httpd, Apache httpd に付属している CGI (Common Gateway Interface) サンプルプログラムの脆弱性はシステム侵入のために悪用された [CERT96b]. このころから, 侵入した痕跡, すなわちインシデントは Web サイトのページ書き換えという新たな形として表現されるようになり, 1996 年 8 月に米国司法省 (http://www.doj.gov/), 1996 年 11 月に米国 CIA (http://ww.cia.gov/), 1997 年 3 月には米国 NASA (http://www.hq.nasa.gov/) などこれまでに数多くの Web ページが書き換えられている. そして, 2000 年 1 月には科学技術庁 (http://www.sta.go.jp/) の Web ページの書き換えを皮切りに, 国内官公庁系の Web サイトにおいて多数の被害が発生した.

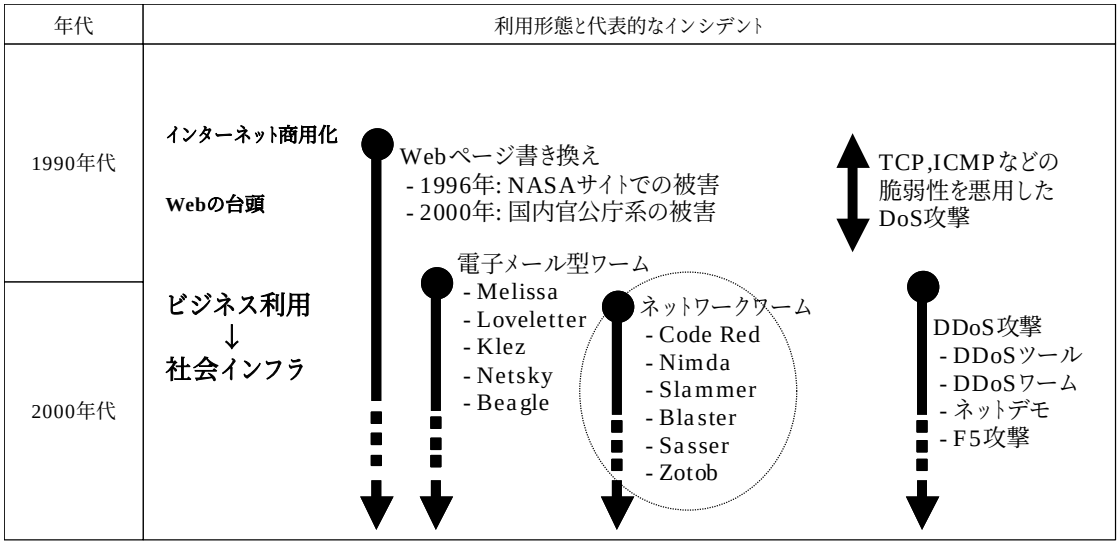


図 2.1：インシデントの変遷

また，Web ページの書き換え情報をアーカイブしている Zone-H には，2005 年現在も Web ページ書き換えに関する世界中のインシデント報告が寄せられている．そして，書き換えの多くは，既知の脆弱性を用いた侵害とシステム設定の不整合を用いた侵害に起因しており，特定の OS や Web サーバプログラムに依存したものではないことを報告している [Zoneh04].

(2) パケットレベルの DoS 攻撃の出現

1990 年代中盤の攻撃手法として，TCP (Transmission Control Protocol), ICMP (Internet Control Management Protocol) などのプロトコル実装上の脆弱性を攻略する数多くのパケットレベルの DoS (Denial of Service) 攻撃が公開された．これら攻撃手法のひとつである TCP SYN Flood 攻撃により，1996 年 9 月には PANIX (http://www.panix.com/) のシステムがダウンし，同年 12 月には Web コミュニケーションズ (http://www.webcom.com/) のサイトがダウンしたという事件も報告されている．この時期発見されたパケットレベルの代表的な DoS 攻撃手法は次の 6 種類であった．しかし，それ以降，攻略パケットの組合せ方やデータサイズを変更するなどの既知 DoS 攻撃手法の変形型がツールと共に多数流布した．

- UDP (User Datagram Protocol) パケットのパケットループを用いた DoS 攻撃 (UDP Echo Flooding 攻撃) [CERT96a]
- TCP SYN パケットを大量に送信する DoS 攻撃 (TCP SYN Flood 攻撃) [CERT96c]
- 正規のパケットサイズを超過した ICMP Echo request パケットを用いた DoS 攻撃 (ping of death 攻撃) [CERT96d]
- 不正な分割パケットを用いた DoS 攻撃 (Teardrop 攻撃) [CERT97]
- 同一送受信先のパケットを用いた DoS 攻撃 (Land 攻撃) [CERT97]
- ICMP ブロードキャストパケットを用いた DoS 攻撃 (smurf 攻撃) [CERT98]

(3) 電子メール型ワームの出現

1998 年末からウイルスと共に，電子メールを介して次の特徴を持つマルウェア (malware：ウイルス，ワーム，トロイの木馬などの有害な機能を持ったプログラムの総称) [IPA99] が流布し始めた.

- 感染したシステムから取得した情報 (パスワード情報など) を電子メールや FTP (File Transfer Protocol) などの配送経路を用いて，特定の電子メールアドレスやサイトに送出してしまう情報収集型
- 感染したシステムに対してリモートからの無制限アクセスを可能とし, 無防備状態にしてしまうリモートコントロール型
- マルウェア自身が備えている電子メール送信あるいは，SMTP (Simple Mail Transfer Protocol) 機能を利用して，電子メールに自分自身を添付し送信し，他のシステムにコピーを伝播させていく自己伝播型

特に，1999 年に入るとマルウェアの数は激増し，ユーザ名やパスワード情報を横取りする Picture.exe，K2PS.exe，Y2Kcount.exe，電子メールに自分自身を添付し送信してしまう Ska (Happy99)，Melissa，PrettyPark，ExploreZip など，トロイの木馬，電子メール型ワームに該当する数十種以上のマルウェアが発見されている. 特徴としては, 著名なサポートセンタを騙ってトロイの木馬を添付した電子メールを送付するという, いわゆるソーシャルエンジニアリング攻撃の利用や, 配布経路として電子メール以外のコミニュケーションチャネル，たとえば，IRC (Internet Relay Chat) などの利用が挙げられる.

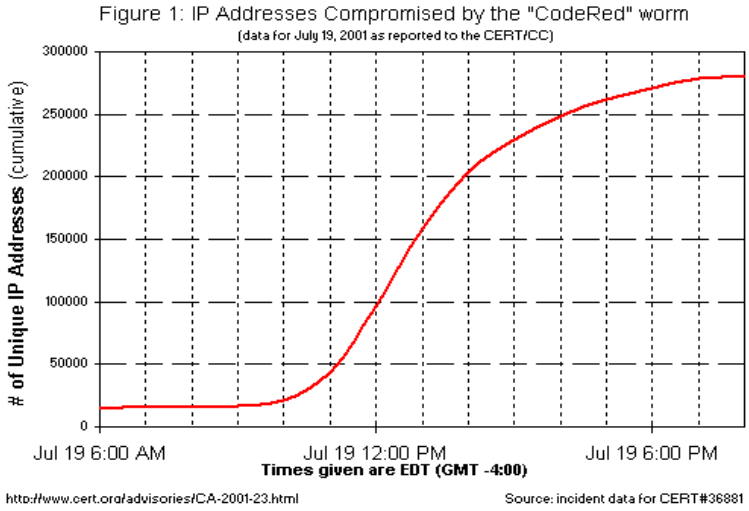
(4) DDoS 攻撃の出現

1999 年の後半に入ると，1990 年代中盤の攻撃手法として注目を集めたパケットレベルの DoS 攻撃は，DDoS 攻撃へと形を変えている．DDoS 攻撃とは，不正侵入した多数のシステムにパケットレベルの DoS 攻撃用エージェントなどを分散配置し, さらにそれらのエージェントを制御しながら, 特定のサイトに攻撃を仕掛ける手法である．この DDoS 攻撃は，2000 年に入ってから，米国の著名 Web サイト (2000 年 2 月 7 日に Yahoo!!，Buy.com，eBay，Amazon.com，CNN.com，2 月 8 日に MSN, 2 月 9 日に E*TRADE, ZDNet など) に向けられた. また, Trin00, TFN (Tribe Flood Network)，TFN2K (Tribe FloodNet 2K)，Stacheldraht などの DDoS ツールの出現 [CERT01b] は，DDoS 攻撃に伴う被害として，既知の脆弱性を利用してシステムに不正侵入され DDoS ツールをインストールされてしまう，DDoS ツールの攻撃対象となりサービス不能状態に陥れられてしまうという 2 種類の被害形態を引き起こすこととなった.

(5) ネットワークワームの出現と流布

2000 年に入ると, 次の特徴を持つマルウェアの活動が活発化し始めた. この中で, 人手の介入を必要としない自己伝播の方法として Windows ネットワークファイル共用が利用され始めたことは, マルウェアの急速な拡散と共に被害の拡大を予期させるものとなった.

- 電子メール型ワームの台頭
  LoveLetter，Stages，SirCam，MTX，Hybris，Navidad，Nimda など，電子メールを介して自己伝播する数十種類の電子メール型ワームが発見された.
- Windows ネットワークファイル共用の利用
  Network 911.Worm, QAZ, Magistr, Nimda などの電子メール型ワームは, 人手の介入を必要としない自己伝播の方法として，Windows ネットワークファイル共用を利用し始めた.
- 自己伝播機能を備え始めたトロイの木馬
  リモートから操作可能なバックドア機能を持つトロイの木馬に, 電子メールやバックドアを介した自己伝播機能が組み込まされ始めた(たとえば，QAZ)．これに伴い，セキュリティ侵害の直接的な被害を受けたり，侵害活動の踏み台として間接的な被害をもたらしたりする可能性が高まってきた.



出典：CERT Advisory CA-2001-23 [CERT01a]

図 2.2：CERT/CC から報告された Code Red への感染状況

さらに，2001 年に入ってからは，電子メールを介して自己伝播する電子メール型ワームに加え, サーバプログラムの脆弱性を直接攻略するネットワークワームが台頭し，人手の介入を必要としない自己伝播の方法が主流となり始めた．特に，sadmind/IIS，Code Red，Nimda など，Microsoft Internet Information Server (Microsoft IIS と略す) サーバの脆弱性を攻略対象とするネットワークワームの流布が際立っている．2001 年 5 月の sadmind/IIS では 10,000 台近くのサーバが被害にあい，2001 年 7～8 月の Code Red に至ってはネットワークの帯域を枯渇させるサービス不能状態を引き起こすと共に，少なくとも 300,000 台以上のコンピュータシステムに影響を与えたと言われている．

これらネットワークワームによる被害波及は, 短期間のうちに脆弱なシステムを探し出し，その結果として指数関数的な自己伝播を実現した (図 2.2) [CERT01a] [Stuart02]．これまでのセキュリティ侵害活動は，単発的な攻撃であり，セキュリティ侵害の実現に数週間あるいは数か月かかったが, ネットワークワームの場合には数分あるいは数時間の間に何万ものシステムのセキュリティ侵害が可能となってしまっている．また，Code Red の流布後には，Code Red が攻略対象とする脆弱性を修復するネットワークワーム Code Green がインターネット上に放たれ, Code Red による攻撃を受けた際にその発信元の Code Red を駆除する CRClean の公開や他の既知脆弱性を攻略対象とするネットワークワームが新たに作成公開されるなど，Code Red が呼び水となり様々な活動がインターネット上で行われた．

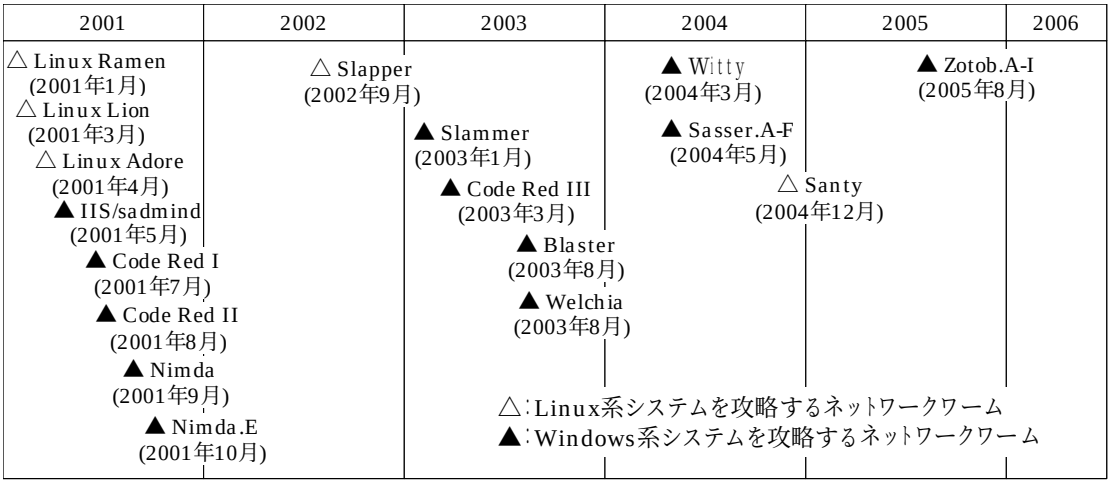


図 2.3：2001 年から 2005 年までのネットワークワーム流布履歴

2001 年 9 月の Nimda の流布にいたっては，脆弱な Microsoft IIS サーバを探して感染する，大量に電子メールを送信して感染する，ネットワーク共有ドライブを探して感染する，そして，悪質な Web ページコンテンツを作成し，そのコンテンツを介して感染するという何通りもの方法で感染拡大できることを示したと言える．

このようなネットワークワームの流布は，Microsoft IIS サーバに限られたものではなく，UNIX サーバの脆弱性を攻略対象とするネットワークワームも発生している．Linux システムを攻略対象とするネットワークワームとしては，Linux Ramen (2001 年 1 月)，Lion (2001 年 3 月)，Adore (2001 年 4 月) が知られている．

また，図 2.3に示す通り，2002 年以降も Windows 系システムを攻略するネットワークワームを中心に毎年のように出現し，“ ネットワークワームの流布＝大規模インシデントの代表格 ” として要警戒対象として取り扱われるに至っている．

2.2　インシデント対処の変遷

本節では, インシデントの変遷に伴い新たに生まれてきたインシデント対応の考え方である“インシデントオペレーション”について述べる.

2.2.1　インシデントレスポンス

インシデントレスポンスとは, 事業継続に大きな影響を及ぼすような事象に, あらかじめ決めておいた計画に沿って対処する事後対策を意味する. 特に, 情報システムのセキュリティに関連するインシデントの場合には, セキュリティインシデントとも呼ばれ, JPCERT/CC の FAQ [JPCERTb] では, 次のように説明している.

> コンピュータセキュリティに関係する人為的事象で, 意図的および偶発的なもの (その疑いがある場合) を含む. たとえば, リソースの不正使用, サービス妨害行為, データの破壊, 意図しない情報の開示や, さらにそれらに至るための行為 (事象) などがある.

具体的には, 各サイトは, サイトのセキュリティポリシーに応じたセキュリティ技術や製品を導入して, それらを適切に運用するとともに, 近い将来発生し得るセキュリティインシデントに備えて, 事前に対応手順を明確にする. インシデント発生時には, その対応手順に従った運用をおこない, その被害の拡大を最小限にするための行動がインシデントレスポンスとなる.

また, インターネットで発生するセキュリティインシデントは, ネットワークワームのように急速に被害拡大する可能性があるため, 適切なインシデントレスポンスを実現する必要がある. その実現には, インシデントの原因や対応方法などの情報を共有することが重要であることから, 次節のインシデントレスポンスチームと呼ばれる組織体が構成されるようになった.

2.2.2　インシデントレスポンスチーム

米国では, 1988 年のインターネットワームの出現を契機に, コンピュータコミュニティでの脆弱性に対する脅威の認識を高め, インシデントの原因や対応方法などの情報を共有することの重要性が認識された. そして, このようなワームがインターネット上に放たれてしまった場合, その被害は甚大なものとなることから, 米国国防総省高等研究計画局 (DARPA: Defense Advanced Research Projects Agency) が中心となり, CERT/CC (Computer Emergency Response Team/Coordination Center) [CERTa] を設立した. CERT/CC は, インターネットにおいて発生した不正侵入やサービス運用妨害等に関する脆弱性情報やインシデント情報を広く収集し, その対策活動

を支援するセンターとして活動している．日本では 1996 年に JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center) が活動を開始した [JPCERTa][大林 98].

また, このようなインシデントレスポンスチームの組織間ならびに国際間連携については，1990 年，大学，研究機関，企業，政府，軍などの CSIRT (Computer Security Incident Response Team) コミュニティから構成される FIRST (Forum of Incident Response and Security Teams) [FIRST90] が組織された．これは，1989 年 10 月に SPAN VAX/VMS システムを攻略する Wank ワーム [CERT89] が出現した際に，国境，組織をまたがった CSIRT 間のコミュニケーションの欠落が適切なインシデントレスポンスの推進を妨げたことに起因する．近年，フィッシングなどのインシデントに対処するために，国際間での CSIRT 連携を積極的に図るなど，所在国の地域性とインターネットの持つ広域性の両輪によるインシデントレスポンスが推進されている．

2.2.3 インシデントオペレーション

2001 年以降の Code Red，Slammer，Blaster の流布によって，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今までは, 被害が発生した後の対処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普及するにつれ, インシデントに伴う被害を予測ならびに予防し, 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いる.

インシデントオペレーションにおいては, 脆弱性から重大な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ことが, インシデント発生後の被害拡大の低減につながるというアプローチをとる．このために，インシデント発生以降から対応活動が始まるのではなく，脆弱性の発見あるいは，脆弱性ならびに修正プログラムの公開以降から対応活動が始まる．ここでは，インシデントオペレーションの担当者が，脆弱性から重大なインシデントへの発展を可能な限り早期に弁別するために実施する 6 つの段階である準備，警戒，予兆，対処，監視，収束について，関連するセキュリティ対策技術 (図 1.1) と Sasser の出現までの過程 (図 2.4) とを用いて概説する．また，インシデントオペレーションの各段階の具体的な対応状況の事例として，Sasser の事例を表 2.2に示す.

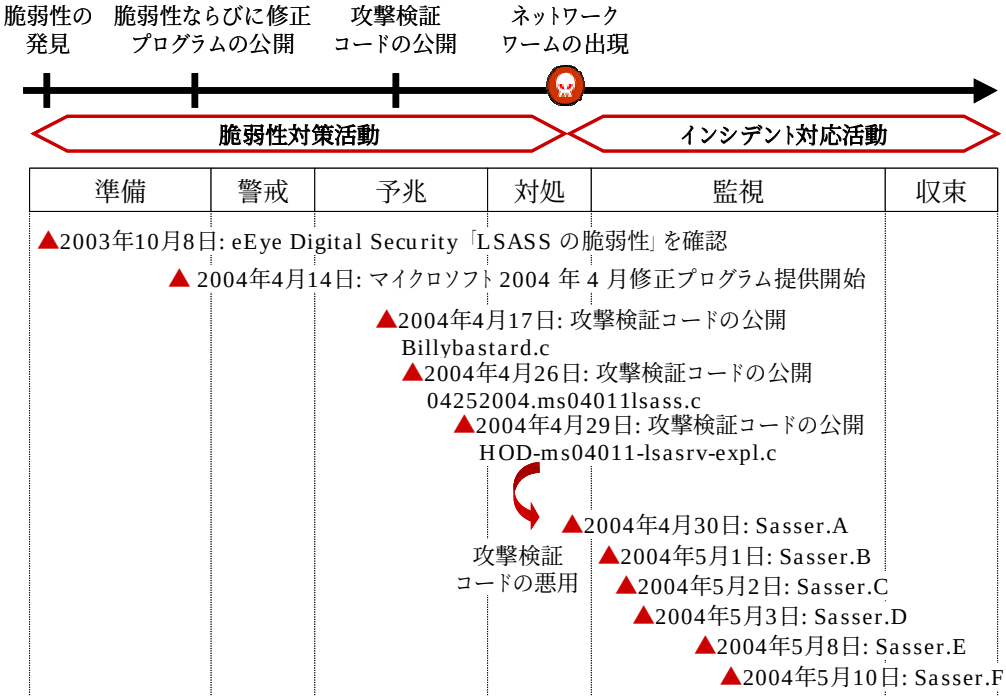


図 2.4：Sasser ワーム出現までの経過

(1) 準備段階

インシデントオペレーションの担当者は, 発見された脆弱性の解析をおこなうことにより, 脆弱性が与える影響, 脆弱性への攻撃容易性を検討すると共に, 脆弱性を悪用された場合のインシデントシナリオを想定作成する. 脆弱性の解析とインシデントシナリオの作成における実施事項は, 次の通りである. なお, 準備段階の実施事項は, 脆弱性ならびに修正プログラムの公開以降に開始しなければならない場合もある.

- 脆弱性の解析 (図 1.1の④)

  脆弱性が与える影響 (DoS, 任意のコード実行, 権限昇格など), 脆弱性への攻撃容易性 (攻撃に必要な権限, 攻撃に利用できるネットワークサービスポート, 攻撃コードへの制約有無, 攻撃コードの作成難易度など) を検討することにより, 攻撃検証コードの公開や脆弱性の亜種公開を警戒すべきかを判断する.
- インシデントシナリオの作成

  脆弱性の解析結果から, 考えうる攻撃コードを想定すると共に, 攻撃検証コードの公開可能性と脆弱性を悪用した最悪シナリオ (ワーム化の可能性など) を想定する.

表 2.1：警戒段階において調査対象となる情報

分類	情報源
脅威レベル情報	AlertCON [ISSb] ThreatCON [symantec] など
脆弱性情報	US-CERT Vulnerability Notes Database [USCERT] SecurityFocus Vulnerability Database [SF] X-Force Database [ISSa] BugTraq [SF] Full-Disclosure [Disclosure] など
脆弱性検査ツール情報	マイクロソフト eEye Digital Security [eEye] ISS [ISSc] Foundstone [Foundstone] など
定点観測情報	@police [police] ISDAS [JPCERTc] Dshield [Dshield] など
アラート情報	JPCERT/CC, IPA, 官公庁, セキュリティベンダなどが発行する注意喚起など
メディア情報	ニュース記事, 解説など

(2) 警戒段階

修正プログラムの実機検証をおこなうと共に, 脆弱性公開に伴う各組織の対応を把握することにより, 現時点でとりうる脆弱性の対策を判断する. 修正プログラムの実機検証と各組織の対応の把握における実施事項は, 次の通りである.

- 修正プログラムの実機検証 (図 1.1の⑦)

  修正プログラムによる脆弱性除去の実機検証, 修正プログラムに伴う不具合状況確認を通して, 現時点でとりうる脆弱性の修正あるいは脆弱性の回避策を再確認する.
- 修正プログラムの適用とその適用状況把握 (図 1.1の⑥)

  修正プログラムの適用による脆弱性除去の推進と共に, 修正プログラムの適用状況を把握する.
- 各組織の対応の把握 (図 1.1の①⑩)

  表 2.1に示す情報を幅広く調査し, 動向を把握する.

(3) 予兆段階

攻撃検証コードの公開を監視する期間である. 攻撃検証コードが公開された場合には，攻撃検証コードの解析により，実際に発生する影響 (DoS，任意のコード実行，権限昇格など)，動作適用範囲 (OS，言語，バージョンやサービスパック依存性など) と転用の可能性 (インシデントシナリオの修正) を検討すると共に，脆弱性への攻撃容易性を再検討する (図 1.1の⑤).

さらに，攻撃検証コードを利用したセキュリティ侵害を検出するために，攻撃検証コードを検出可能なウイルス定義ファイルの作成／更新ならびに，侵入検知用シグニチャの作成／更新をおこなう (図 1.1の⑧⑨). これにより，対処段階において，侵害活動の影響範囲などを判断する際の材料となる観測データの収集を実施する.

(4) 対処段階

攻撃検証コードから派生した侵害活動ならびにネットワークワームなどの出現期間である. 侵害活動痕跡の調査ならびにネットワークワームの挙動解析により，これら侵害活動が与える影響，動作適用範囲 (言語依存性，サービスパックやバージョン依存性など) の確認をおこなうと共に，侵害活動発生に伴う観測データを分析する.

ネットワークワームの挙動解析と観測データの分析に関する具体的な実施事項は，次の通りである.

- ネットワークワームの挙動解析 (図 1.1の②)

  ネットワークワームの挙動解析に関する公開情報については，提供側 (ウイルス対策ベンダ，IDS (Intrusion Detection System) 製品ベンダ，侵害活動の影響を受ける製品開発ベンダなど) の立場によって提供される情報の有効範囲が異なり，また，対策側 (インターネットユーザ，イントラネット管理者，インターネットサイト管理者，ISP など) の立場によって対策検討に必要とする情報が異なる. このため，ネットワークワームの挙動解析にあたっては，公開情報，コード解析結果と実機検証結果とを組合せて影響，動作適用範囲を確認することが情報の確度ならびに範囲を広げる意味で有効となる.

  ネットワークワームの挙動解析のポイントとしては，次の通りである.

  - ネットワークワームの探索 IP アドレスの選択方法
  - ネットワークワームが悪用する脆弱性の特徴 (OS，言語，バージョンやサービスパック依存性など)
  - ネットワークワームが攻略に使用するネットワークサービスポート
  - DNS への問合せ頻度や通信トラフィック量など，ルータ，スイッチ，DNS サーバなどネットワークインフラに与える影響

表 2.2：インシデントオペレーションにおける 6 つの段階

段階	Sasser の場合の対応状況
準備段階	Sasser の攻略対象とした MS04-011 の LSASS (Local Security Authority Subsystem Service) の脆弱性 [MS04] は，リモートから任意のコードを実行可能な脆弱性であり，マイクロソフトが MS04-011 で提示した深刻度は“緊急”であった.
警戒段階	Sasser の場合，MS04-011 の公開に伴い，CERT/CC ，IPA，@police からWindows システム脆弱性対策に関する注意喚起がなされた.
予兆段階	予兆段階において，MS04-011 の PCT (Private Communications Transport) の脆弱性に関する攻撃検証コードが先に公開されたために，LSASS の脆弱性への注目度が少し低下した. また，PCT の脆弱性の攻撃検証コードが公開されたことと，大型連休を控えていたことから，経産省，総務省，警察庁合同で Windows システム脆弱性対策に関する注意喚起を発行した.
対処段階	Sasser は，2004 年 4 月 29 日(米国時間)に“houseofdabus”によって公開された攻撃検証コードを利用していた. この攻撃検証コードは英語版とロシア語版 Windows 2000 Professional と Windows 2000 Server，そして Windows XP Professional に対して攻撃を成功させることが確認された. 一方，日本語版 Windows 2000 に対しては攻撃が失敗することと，他言語版の Windows 2000 においても同様に攻撃は失敗する可能性があることが確認された [eEye04]. これにより，Sasser が日本語版 Windows 2000 を介して感染拡大する可能性がないと判断するに至った.
監視段階	2004 年 4 月 30 日の Sasser.A に続き，Sasser.B (5 月 1 日)，Sasser.C (5 月 2 日)，Sasser.D (5 月 3 日)，Sasser.E (5 月 8 日)，Sasser.F (5 月 10 日) と亜種の出現が続いた. いずれも，“houseofdabus”によって公開された攻撃検証コードをベースとしていた.
収束段階	2004 年 5 月 8 日に Sasser 作成の容疑者が逮捕された. Sasser に関する一連の活動は，Sasser.F (5 月 10 日) の亜種の出現後にほぼ収束した.

- 観測データの分析(図 1.1の⑩)

  SOC (Security Operation Center)，ISP，定点観測などでのネットワークワーム検知状況に基づき，影響範囲の確認，感染拡大の危険性を検討する．なお，観測データを分析する際には，国内とワールドワイドでの検知数の弁別，観測データの観測箇所 (観測 IP アドレス範囲，観測箇所数) と観測方法 (ファイアウォール，IDS など) による依存性を加味し，複数の状況を確認して局所的な現象か全体的な現象か，パケットや検体解析と関連付けた検知推移の判断をおこなう必要がある．

(5) 監視段階

ネットワークワームの亜種出現の兆候に関する監視強化，観測データの状況推移に関する監視強化をおこなう．また，急速な被害拡大を防止するための機能やシステム (図 1.1の③) の稼動確認をおこない，緊急時に備えた体制を準備する．特に，ネットワークワームの亜種は，動作不良の解決，動作適用範囲の拡大，機能拡張などがおこなわれている場合もあるため，亜種出現時には対処段階と同様，ネットワークワームの挙動解析をおこなう必要がある．

(6) 収束段階

ネットワークワームの出現に伴い実施した一連の活動内容を関連組織間で整理し，課題を確認し，その結果を次回以降のインシデントオペレーションにフィードバックする．

2.3　既存技術の課題

本節では，本論文で対象とする，脆弱性ならびに修正プログラムの公開以降のインシデントオペレーション (図 1.1の①②③) を構成するセキュリティ対策技術と関連研究について概説した後，その課題について示す．

2.3.1　脆弱性公開以降の各種イベントの発生把握

脆弱性公開以降の各種イベントの発生把握とは，脆弱性対策活動ならびにインシデント対応活動において，脆弱性やインシデントに関わる情報を収集し，状況整理する活動である (図 1.1の①)．

インターネットをとりまくセキュリティ侵害の対策環境は日々改善しており，脆弱性対策活動に必要となる脆弱性対策情報の共有については，米国あるいは，英語圏を中心に，US-CERT Vulnerability Notes Database [USCERT]，NIST - NVD (National

Institute of Standards and Technology - National Vulnerability Database) [NVD], OSVDB (Open Source Vulnerability Database) [OSVDB] など数多くの脆弱性情報 (脆弱性対策情報) データベースが構築されている．また，これら脆弱性情報データベースに登録されている脆弱性情報ならびにセキュリティ情報同士の関連付けを実現する識別子として CVE (Common Vulnerabilities and Exposures) [CVE] も開発されており，脆弱性自身の記述を目的とした仕様 AVDL (Application Vulnerability Description Language)[AVDL] や脆弱性の存在有無確認を目的とした仕様 OVAL (Open Vulnerability Assessment Language) [OVAL] などの検討も進められている．

インシデントに関わる情報の共有については，米国を中心に観測システム Dshield が構築されており，国内においてはインターネット定点観測システム [JPCERTc] [police] が観測データの公開提供を開始している．さらに，インシデント自身の記述，アーカイブ，交換をおこなうことを目的とした共通データフォーマット IODEF (Incident Object Description and Exchange Format) [Arvidsson01][Danlyliw05] の策定が進められている．この IODEF は，侵入検知観測データを他組織に通知するフォーマットとして JPCERT/CC のインシデント情報交換システム [JPCERT04] や，侵入検知観測データを取り込む際のフォーマットとしてインシデント発生時の対応案件管理を支援するシステム [梅澤 05] において利用され始めており，脆弱性対策ならびにインシデント対応のための情報を早期に入手できるようになってきた．

しかしながら，国内マーケットを対象とする製品の脆弱性対策情報が US-CERT Vulnerability Notes Database などの米国あるいは，英語圏の脆弱性情報データベースに掲載されていることはほとんどない．また，IODEF は発生したセキュリティインシデントを処理，追跡ならびに調査することに主眼をおいたフォーマットであるために，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考慮されているわけではない．すなわち，日本という地域性を考慮した脆弱性情報 (脆弱性対策情報) データベースは整備されるに至っておらず，“ いつ攻撃検証コードが公開されたのか？ ”，“ インシデントに伴い各組織でどのような対応がとられたのか？ ”など，ネットワークワームの早期対応ならびに被害拡大を低減するために必要となる関連イベントを共有する環境が整備されていないことが，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に不足している 1 つ目の課題として挙げられる[i]．次に，解決すべき具体的な事例を示す．

---

i) 2004 年 7 月 7 日経済産業省 “ソフトウエア等脆弱性関連情報取扱基準”が公示され，以降，日本国内の製品開発ベンダの脆弱性対応状況については対策ポータルサイトである http://jvn.jp/ サイトから公開されている．

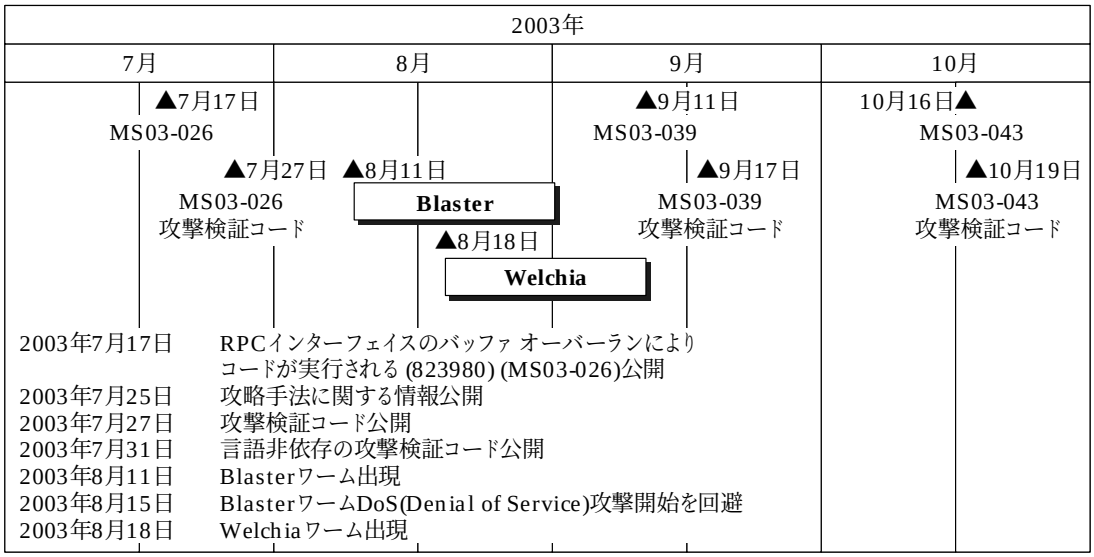


図 2.5：Blaster，Welchia ワーム出現までの経過

(1) 脆弱性公開以降の関連イベントの共有

2003 年は, 1 月末の Slammer の流布, 8 月の Blaster, Welchia (Nachi) の流布, 9 月の Sobig.F の流布だけではなく, 7 月には Cisco IOS のサービス運用妨害に関わる脆弱性 [CERT03a] の攻略活動など，インターネットインフラに多大な影響を与えるインシデントが数多く発生した．これらインシデントの発生を通して, 国内においても“脆弱性はどのようなものなのか？”，“脆弱性の影響を受ける製品は？”，“製品開発ベンダの脆弱性対策情報は？”という脆弱性対策情報に関する提供環境は整備され始めた.

しかし，“いつ攻撃検証コード (exploit code とも呼ばれている) が公開されたのか？”，“脆弱性を悪用したインシデントとして何が発生したのか？”，“インシデントに伴い各組織でどのような対処がとられたのか？”など，インシデントの早期対応ならびに被害拡大を低減するために必要となる関連イベントを共有情報として提供する環境は整備されるに至ってはいない．たとえば，ネットワークワームによるインシデント発生は，脆弱性の発見，脆弱性ならびに修正プログラムの公開，攻撃検証コードの公開，ネットワークワームの出現という段階を経ることが多く，2003 年 8 月に流布した Blaster, Welchia ワームについても図 2.5に示すように同様な段階を経ている.

ネットワークワーム出現までの過程において, 攻撃検証コードの公開は, 脆弱性未対策システムへの対策促進ならびに, ネットワークワーム出現に備えた監視ならびに対応体制の強化を図るトリガとなる．このように, 現在どのような段階にあるのかと

いう経過を情報として共有することは, 次に実施すべきインシデント対応対策を検討する上で必要とされてきている.

(2) 国内で利用されているソフトウェアや装置を対象とする脆弱性対策情報の収集

セキュリティインシデントに対する活動を早期から進めている CERT/CC では, 脆弱性対策を喚起する対策勧告である CERT Advisory と, 脆弱性に関連する情報をまとめた Vulnerability Notes Database の 2 種類を脆弱性対策情報として提供している[ii]. これら CERT/CC から提供される情報は, 国内のセキュリティ教育において脆弱性対策の参照情報として紹介されることも多い. 特に, 後者の Vulnerability Note Database は, 脆弱性に関連する製品開発ベンダの対応状況が一覧としてまとめられており, 脆弱性対策を推進するにあたっては有用なポインタとなる.

ところが, 国内マーケットを対象とする製品の脆弱性対策情報が CERT Advisory や Vulnerability Notes Database に掲載されていることはほとんどない. これは掲載可能な国内の製品開発ベンダが少ないだけではなく, 国内の製品開発ベンダにとって, 海外展開していない製品の脆弱性対策情報を掲載する利点は少ないという製品マーケットにも一部起因している. また, 国内の商用サービスによる脆弱性対策情報の多くは, 英語圏の情報が翻訳され提供されているのが実情である. たとえば, 国内製品の脆弱性対策情報を英語版として公開すると, 英語圏のセキュリティ情報収集ベンダが拾い上げ, 商用サービスが英語を日本語に再翻訳して提供しているという事例もある.

このように, CERT Advisory や Vulnerability Note Database は国内のセキュリティ教育で紹介されていながらも, 実際には国内で利用されているソフトウェアや装置を対象とする製品開発ベンダの脆弱性対策情報は掲載されていない. また, 商用サービスについても同様な状況となっている. このため, セキュリティに関わるシステム管理者やシステムエンジニアは必要にあわせてインターネット上に散在している脆弱性対策情報を探し回らなければならないというのが実情である.

(3) 脆弱性の影響範囲の把握

項番(2)の情報散在とも関係するが, 現状の脆弱性対策情報の提供環境は, 報告された脆弱性が国内で利用されているソフトウェアや装置にどの程度影響を与えているのかを把握しにくい. たとえば, 2002 年に報告された SNMP についてはインターネット全体で 90 社近くの製品開発ベンダに影響を与える脆弱性であった [CERT02a]. その他にも Apache [CERT02b], OpenSSH [CERT02c], DNS リゾルバ [CERT02d], OpenSSL [CERT02e] の脆弱性は, 国内で利用されているソフ

ii) 2004 年 1 月末以降, CERT/CC の情報提供活動は US-CERT に統合されている.

トウェアや装置にも広く影響を与えているはずであるが, その実態すらも把握することができない状況にある.

このような状況を引き起こしてしまっている要因のひとつとして, 国内マーケットを対象とする製品にオープンソフトウェアがいろいろな形態で取り込まれ, 販売されていることが挙げられる. また, この課題は, 国内での脆弱性対策情報の提供が海外で報告された脆弱性にシステム管理者が対処するというレベルに留まってしまっており, 国内の製品開発ベンダの対応状況を収集し, 整理するための手順など, 国内で利用されているソフトウェアや装置という地域に即した脆弱性対策情報の提供環境が整備されていないことにも起因していると思われる.

事例に示した課題を解決し, 脆弱性公開以降の各種イベントの発生把握を実現するための技術的な課題をまとめると, 次の通りとなる.

- 各種イベントデータの交換フォーマットの作成や提供情報の分類整理をおこなう際の基盤となる情報提供項目の選定ならびに提供情報への識別子付与方法
- 情報提供項目や提供情報の識別子に基づき, 脆弱性やインシデントに関わる情報を効率的に収集し, 関連項目毎に分類整理する方法

本研究では, 提供項目の選定ならびに提供情報への識別子付与方法について試行を通して検討をおこなった. なお, 関連イベントの収集と分類整理する方法については, 今後の課題である.

2.3.2　ネットワークワームの挙動解析

ネットワークワームの挙動解析は, インシデントオペレーションの対処段階において, ネットワークワームによる侵害活動が与える影響, 動作適用範囲の確認をおこなう活動である (図 1.1の②).

マルウェアは 1998 年末頃から電子メールを介して流布するようになり, 2001 年に入ってからは電子メールを介して自己伝播するワームに加え, サーバプログラムの脆弱性を直接攻撃するワーム (Code Red, Nimda など), クライアントの脆弱性を悪用したダイレクトアクション型ワーム (Nimda, Aliz, Klez など) も現れ, 人手の介入を必要としない自己伝播の方法が主流となり始めた.

本研究が対象とするマルウェアはネットワークワームであり, 代表例として Code Red I/II, Nimda, Slammer, Blaster, Sasser がある. これらのネットワークワームは, ランダムに選んだ IP アドレスの特定ポート番号に対して TCP あるいは UDP 通信を開始する. 送信先との通信に成功した場合には, 特別なメッセージを送付すること

で脆弱性を攻略し感染を試みる．たとえば，Slammer の場合には，ランダムに選んだ IP アドレスのポート番号 1434/UDP に Microsoft SQL Server Resolution Service の脆弱性(MS02-039) [MS02] を攻略する UDP パケットを送信して感染を試みる．Sasser の場合には，ランダムに選んだ IP アドレスのポート番号 445/TCP に TCP コネクションを確立して, Local Security Authority Subsystem Service (LSASS) の脆弱性 (MS04-011) [MS04] を攻略し感染を試みる．

このようなネットワークワームの挙動解析にあたっては, ネットワークワームが与える影響を調査する場合にはシミュレーションが用いられ [高橋 04][広岡 04][関 04]，ネットワークワームの動作自身を調査する場合には, 主にリバースエンジニアリングによるコード解析が利用されている [Mihai03]. ここで目的とするネットワークワームの挙動解析とは後者であり，たとえば，eEye Digital Security は逆アセンブラツールである IDA を用いて Blaster のコード解析をおこない, その結果を公開している [eEye03]. また，難読化が施されたプログラムの解読にあたっては，逆アセンブラツールと，エミュレータを組合せて利用することにより解析する手法 [Chris04] などが提案されている．これに対して，実機での動作検証を用いた挙動解析としては，電子メールサーバ内の仮想マシン上でウイルスの可能性がある添付ファイルを受信し, その挙動を監視することで電子メールを利用して感染活動を拡大する未知ウイルス検知をおこなうシステム [三宅 02][神薗 03] がある．この他にも，コード解析と実機での動作検証とを組合せることによりウイルス解析を自動化するシステム [伊沢 05] が検討され, ハニーポットなどを用いた侵入者の行動やシステムへの攻撃手法の調査がおこなわれている [Honeynet][小泉 04][澁谷 04][Niels04][片岡 05].

また, 多くの組織において，ネットワークワームの動作に関する情報収集は組織外部に頼っているのが現状である．このため，組織内でネットワークワームが出現した場合にも，組織外部の情報が公開されるまでの間は感染動作がわからず，実施した対策も局所的な対処に留まってしまう可能性がある．この課題を解決する最も有効な手法は，コード解析によりネットワークワームの動作を解析するアプローチである．しかし，各組織に必ずしもコード解析のできる技術者が在籍しているとは限らず，さらには，マルウェア自身のコード難読化が進んでいることを踏まえると，このアプローチは，必ずしも現実的な解ではない．ハニーポットやハニーネットなどを用いて，侵入者の行動やシステムへの攻撃手法の調査, あるいはウイルス捕獲システムを構築し調査解析するといった研究 [小山 05] もおこなわれている．しかし，発生したインシデントを収束させることを主眼におく各組織が, このようなハニーポットやハニーネットなどの仕組みを必ずしも保有できる環境があるとは限らない．さらに，挙動に関する情報が公知となった以降も，コード解析に伴う結果報告が提供者により異なっている場合や，結果報告そのものが適切ではないことも見受けられることがあり, 公知となった挙動に関する情報を確

認し，情報の確度を上げることも対策を検討する上で必要不可欠となっている．次に解決すべき具体的な事例を示す．

(1) 公表される情報が必ずしも正確ではないことがある．

2004 年 5 月に流布した Sasser ワームに関して，下記のような動作情報が報告された．

> W32.Sasser.Worm が実行されると，次のことを行います．
> 中略
> すべてのホスト IP アドレスを繰返しスキャンし，次の IP アドレス
> を除く IP アドレスを探します．
> * 127.0.0.1
> * 10.x.x.x
> * 172.16.x.x - 172.31.x.x
> * 192.168.x.x
> * 169.254.x.x

また，ウイルス対策ベンダやセキュリティによっては，上記 IP アドレスはインターネットへの可達性確認のためにを使用すると報告され, セキュリティのメーリングリスト Full-Disclosure [Disclosure04] では，Sasser ワームの 10.x.x.x へのスキャンは発生しないのではないかという投稿に関して, 動作確認の情報交換がおこなわれた．

(2) 各ベンダが提供する情報が必ずしも同一ではない．

DDoS 攻撃の活性化の日時は, 対策側としてはより正確な情報の入手が必要となるが，2004 年 1 月に流布した Mydoom の DDoS 攻撃に関して，各ベンダの動作情報の報告は微妙に異なっている (表 2.3).

いずれの事例も，コード解析結果を確認する，情報の確度をあげるという視点からの検証手段の確立が必要となる. 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，各組織単独で実施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が, 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に不足している 2 つ目の課題として挙げられる．

表 2.3：Doomjuice DDoS 機能活性化に関する情報

ベンダ, 名称		活動概要
アンラボ Win32/Doomjuice.worm.36864	感染対象	MyDoom に感染しているシステム
	活性化	毎年 2 月 9 日 (9 日を含む) 以後:DoS 攻撃
	攻撃対象	microsoft.com
日本エフセキュア Doomjuice	感染対象	MyDoom.A に感染しているシステム
	活性化	2004 年 2 月 8 日以降:DDoS 攻撃 2004 年 2 月 12 日以降:すぐに DDoS 攻撃 After the 8th of February the starts a DDoS attack against www.microsoft.com. Between 8th and 12th of February the worm will wait for up to 365 seconds. After the 12th it will start the attack right away.
	攻撃対象	www.microsoft.com
日本ネットワークアソシエイツ W32/Doomjuice.worm.a	感染対象	MyDoom.A, MyDoom.B に感染しているシステム
	活性化	―
	攻撃対象	www.microsoft.com
ソフォス W32/Doomjuice-A	感染対象	MyDoom.A に感染しているシステム
	活性化	2 月 9 日以降:2 分から 6 分の間待機した後 DDoS 攻撃 On 9th February and any date thereafter the worm will wait for between 2 and 6 minutes and then attempt a distributed denial of service (DDoS) attack.
	攻撃対象	www.microsoft.com
シマンテック W32.HLLW.Doomjuice	感染対象	MyDoom.A, MyDoom.B に感染しているシステム
	活性化	February 8th and 11th, the worm launches a DoS attack against www.microsoft.com, after delaying for a random amount of time. February 11th, but before the end of this month, the worm immediately launches a DoS attack against www.microsoft.com.
	攻撃対象	www.microsoft.com
トレンドマイクロ WORM_DOOMJUICE.A	感染対象	MyDoom.A, MyDoom.B に感染しているシステム
	活性化	2 月 9 日～12 日:一定期間スリープした後 DoS 攻撃 2 月 13 日以降:スリープ期間なしで DoS 攻撃 Between February 9 and 12, this malware creates a denial of service (DoS) attack thread. It sleeps for a period of time before performing a DoS attack. Above February 13, it continually creates DoS threads with no delay.
	攻撃対象	microsoft.com

2.3.3　被害発生を想定したシステム構築

被害発生を想定したシステム構築は, インシデントオペレーションの監視段階においては, 矢継ぎ早やの亜種発生への対応など, インシデント発生後の被害拡大を低減するための活動である (図 1.1の③).

2001年は, sadmind/IIS (2001年5月), Code Red (2001年7〜8月), Nimda (2001年 9 月) など, Microsoft IIS サーバの脆弱性を攻略対象とするネットワークワームの流布が際立った. 本研究で対象とするマルウェアは, ポート番号 80 に対して直接 TCP コネクションを確立した後, Web サーバの脆弱性を攻略するネットワークワームである. 代表例として Code Red I/II, Nimda がある. Code Red I/II は, ランダムに選んだ IP アドレスのポート番号 80/TCP に対して TCP コネクションを確立する. 確立に成功した場合には, 特別な HTTP GET 要求を送信して, Microsoft IIS の idq.dll の脆弱性 [MS01] を攻略し感染を試みる. 感染後はワームの自己伝播型の特性により, 4.3 節に示す感染先の探索特性に従い, 他のシステムに対して同様な感染活動をおこなう.

Nimda は, 電子メール, 共用ファイル, Web サーバ経由など複数の感染手法を持つ. このうち, Web サーバ経由の場合には, 4.3節に示す感染先の探索特性に従い選択した IP アドレスのポート番号 80/TCP に対して TCP コネクションを確立し, Microsoft IIS の脆弱性 “ Web サーバーフォルダへの侵入 ” [MS00] の攻略を試みる.

次に, 対象とするネットワークワームとなる Code Red II と Nimda のイントラネットでの流布状況を, イントラネット Web サイトから回収したアクセスログに基づき例示する.

(1) Code Red II

2001年8月6日の Code Red II 流布開始当初からの累積アクセス数と累積感染ホスト数を図 2.6に示す. このグラフは, 5 箇所のイントラネット Web サイトに記録された Code Red II の HTTP GET 要求のアクセス件数と発信元 IP アドレス件数の平均値から作図している. 流布状況は, 流布開始直後から 2 時間で累積アクセス数が約 100 件となっていることから, 10 分あたりに換算すると約 8 件のアクセスが発生していたことになる.

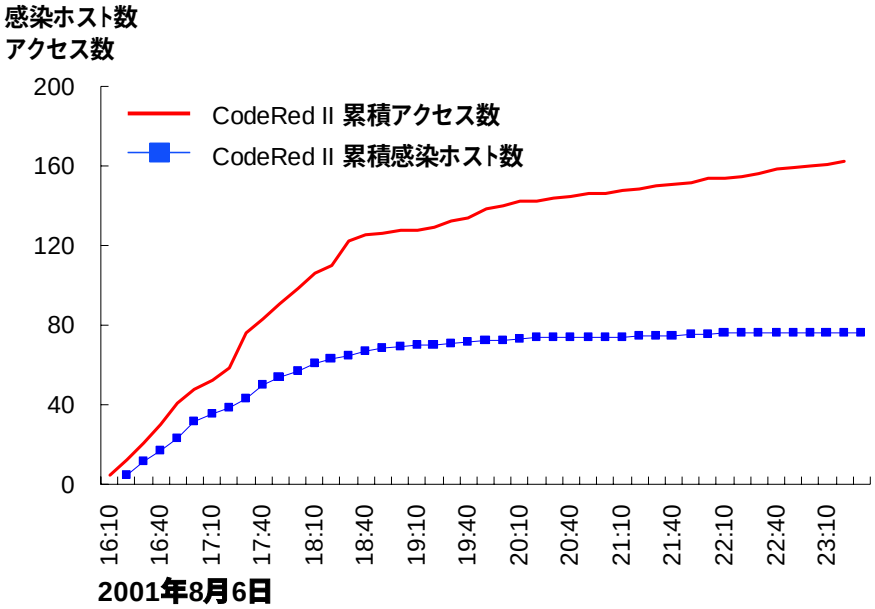


図 2.6：Code Red II 累積アクセス数と累積感染ホスト数

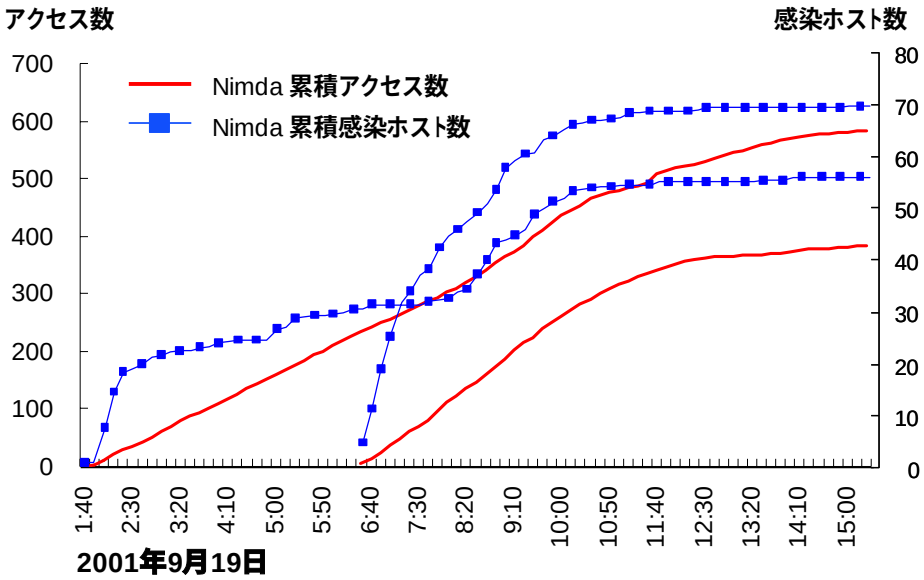


図 2.7：Nimda 累積アクセス数と累積感染ホスト数

(2) Nimda

2001 年 9 月 19 日の Nimda 流布開始当初からの累積アクセス数と累積感染ホスト数を図 2.7に示す．Nimda の場合には，夜間から流布活動の痕跡を記録していたアクセスログと早朝から流布活動の痕跡を記録しはじめたアクセスログがあり, 痕跡形態が夜間型と早朝型の 2 つにはっきりとわかれている．このため，Nimda の累積アクセス数と累積感染ホスト数については，6 箇所のイントラネット Web サイトのアクセスログを痕跡の記録開始時刻を用いて分類した後，記録された Nimda の HTTP GET 要求のアクセス件数と発信元 IP アドレス件数の平均値を算出して作図している．夜間型の流布状況は，Code Red II と同じく流布開始直後から 2 時間で累積アクセス数が約 100 件となっていることから, 10 分あたりに換算すると約 8 件のアクセスが発生していたことになる．

Code Red II，Nimda いずれの事例も，数時間のうちに 50 台以上のシステムに感染していることから, 感染したシステムがイントラネットに送出したトラフィックはかなり高かったものと想像される．

ネットワークワームが流布した際の基本的な対策手段は, ウイルス対策ベンダの提供するアンチウイルスソフトウェアのウイルス定義ファイルを更新すると共に, 脆弱なネットワークサービスが稼動している場合には，セキュリティ修正プログラム (patch program) による脆弱性の除去をおこなうか, ネットワークサービス自身を無効化することである．また, システムがこれらのネットワークワームに感染してしまった場合には除去ツールを適用するか，初期からシステムを再構築することになる．ところが，現状のイントラネットにおける情報システムの多くが Web 主体に構成されているために, HTTP ポートを攻略対象とするネットワークワームが流布した場合, 対策が完全に完了するまでの間，次に示す対策上の課題を伴ってしまい，この影響は甚大となる．

- Web サーバが HTTP ポートを用いてサービスを提供していること自体がネットワークワームの流布ならびに，流布に伴うトラフィック増加を助長してしまう．
- ネットワークワームが HTTP ポートを攻略対象としているために，Web によるインシデント対応情報の発信や，既存 Web サーバの正常稼動が阻害されてしまう．

現在，このようなネットワークワームが流布した際の検知方式としては，シグニチャを用いた検知方式やネットワークワームが感染活動により送出するトラフィックパターンを用いて検知する方式 [面 03][Dan04][東角 05] などがある．

また，ネットワークワームによる被害発生を想定したシステム構築については，事前

にネットワークワームに感染する可能性のある機器を排除あるいは, 脅威から保護するアプローチと, 事後にネットワークワームに感染した機器あるいは, 感染に関与するトラフィックを排除するアプローチがある. 事前にネットワークワームに感染する可能性のある機器を排除するアプローチとしては, 持ち込み機器からワームやウイルス感染が発生しやすいという点に着目して, 持ち込み機器を接続前に検査する検疫機構を提案している [三輪 04][横山 05]. 感染する可能性のある機器を脅威から保護するアプローチとしては, 脆弱なサービスへのアクセスを遮断した接続環境が提案されている [角 04]. 事後にネットワークワームに感染した機器あるいは, 感染に関与するトラフィックを排除するアプローチとしては, 検知機構とフィルタリング機構とを組合せた手法の研究や [角 05], シグニチャに合致する不正なアクセスのみを止める IPS (Intrusion Prevention/Protection System) が実用化されている.

この他に, 感染に関与するトラフィックを抑止することでネットワークワームの拡散を遅延させる方法も提案されている [Williamson02][大宅 05][岡本 04]. そして, これらのアプローチの共通的な特徴は, 問題となりうる機器ならびにトラフィックを取り除くというブラックリスト (black list) の考え方にたっていることである.

しかし, 上記課題を解決するためには, ネットワークワームの流布を抑止することと, サービスの稼動継続性を確保することの二面性を兼ね備えた対策が必要となる. このような対策を実現するためには, ある条件を満たしているシステムのみを存続させるアプローチ, すなわち, ホワイトリスト (white list) の考え方に基づいたシステム構築が有効である. たとえば, 電子メールサービスの場合には, 通常状態は電子メール送信に際して特に制約事項はないが, 電子メール型ワームの流布で電子メールサービスに対する脅威レベルが上がるに従い, “電子メール送信時にユーザ認証をおこなう”, “電子メールの件名に特定のキーワードが記載された場合のみ転送する”, “インフラを運用するシステム管理者向けの電子メールサービスのみを有効とし, 一般ユーザのサービスを停止する”というネットワークサービスを縮退させる方法である. また, Web サービスの場合には, Web サーバにおける HTTP ポートを任意の代替ポート番号に切り替えることでネットワークワームの流布を抑止する. 同じく Web サーバにおける HTTP ポートを代替ポート番号に切り替えることで Web サーバの稼動継続性を確保するというネットワークサービスを退避させる方法である. このように, 稼動しているネットワークサービスを縮退あるいは退避させるというホワイトリストの考え方に基づいたシステム構築の検討が不足していることが, 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に不足している 3 つ目の課題として挙げられる.

第3章　脆弱性／インシデント対処情報共有システム

本章では, 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いという1つ目の課題を解決するために, セキュリティに関わるシステム管理者やシステムエンジニア向けに脆弱性対策ならびにインシデント対応情報を広く告知することを目的とした脆弱性／インシデント対処情報共有システム JVN を提案する.

3.1　まえがき

JVN は，セキュリティに関わるシステム管理者ならびにシステムエンジニア向けに脆弱性対策ならびにインシデント対応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る. CERT Advisory [CERTb] ならびに CIAC Bulletin [CIAC] など主要な対策勧告に対する製品開発ベンダの脆弱性対策情報を整理して提供すると共に, 対策勧告で取り上げられた脆弱性攻略に伴うインシデント対応に備え, 関連するイベントを時系列情報として提供することを特徴としている.

また，JVN を公開型データベースとして具体化するために，2002 年 6 月に JPCERT/CC の支援を受け慶應義塾大学に試行サイト構築ワーキンググループを立ち上げた後，JPCERT/CC と共にいくつかの製品開発ベンダを訪問し，JVN の趣旨説明と共に試行サイトへの情報掲載協力を依頼した. そして, 2003 年 2 月に JPCERT/CC の試行サイト (http://jvn.doi.ics.keio.ac.jp/) として運用を開始した [寺田 02].

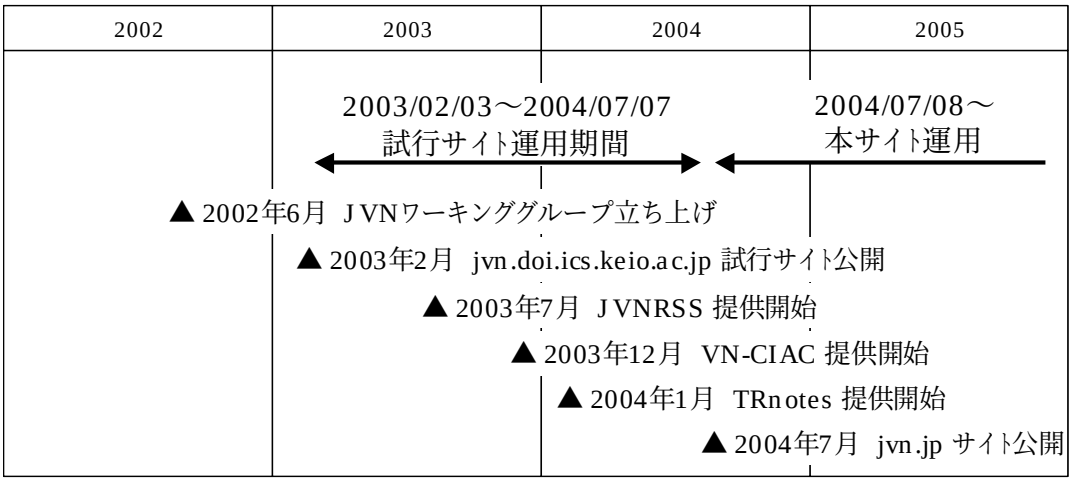
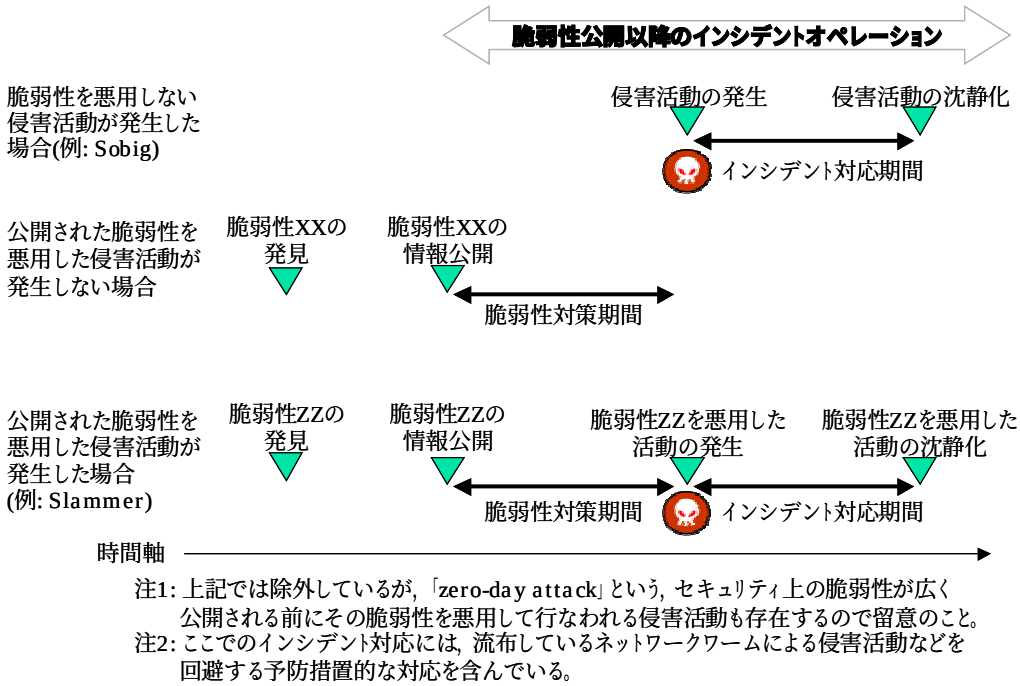


図 3.1：JVN 試行サイトの構築ならびに運用の経過

以降, 2003 年 7 月に XML (eXtensible Markup Language) フォーマットに共通の書式でドキュメントの見出しや要約などをリスト化する JVNRSS (JVN RDF Site Summary) を用いた情報提供 [寺田 03] [JVNRSS], 2003 年 12 月に CIAC Bulletin に対応した VN-CIAC (Vendor Status Notes - CIAC) の情報提供, 2004 年 1 月には関連するイベントを時系列情報として共有する TRnotes (Status Tracking Notes) の情報提供を実施し [寺田 04], 試行サイトでの情報提供の有効性についての検証をおこなった (図 3.1). その結果, 提案システムを用いることにより, セキュリティに関わる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支援に有効な情報共有が可能となることを確認した.

本章の構成について述べる. 3.2節で情報提供のフレームワークと Web 試行サイトでの実現方式を示す. 3.3節では試行サイトでの提供実績と利用状況を示す. 3.4節はまとめである.



注1: 上記では除外しているが,「zero-day attack」という, セキュリティ上の脆弱性が広く公開される前にその脆弱性を悪用して行なわれる侵害活動も存在するので留意のこと。
注2: ここでのインシデント対応には, 流布しているネットワークワームによる侵害活動などを回避する予防措置的な対応を含んでいる。

図 3.2：脆弱性対策とインシデント対応

3.2　脆弱性／インシデント対処情報共有システム JVN

本節では，2.3.1節で述べた課題を解決するための脆弱性／インシデント対処情報共有システム JVN について述べる.

3.2.1　脆弱性／インシデント対処のための情報共有方式

ネットワークワームなどのセキュリティ侵害に対処するためには, セキュリティ上なんらかの問題を引き起こす脆弱性を除去するための脆弱性対策活動と, 実際に発生している侵害活動の回避やセキュリティに関する問題事象を解決するためのインシデント対応活動があり，これらの活動は図 3.2に示すような時間軸上でのつながりがある.

脆弱性対策情報の提供にあたっては, 脆弱性対策活動とインシデント対応活動のつながりを考慮しなければ, ネットワークワームのように“ 脆弱性ならびに修正プログラムの公開 ”から“ ネットワークワームの出現 ”のように一連の段階を経るインシデントに対して後手の対応を踏むことになってしまう．そこで，JVN では国内での脆弱性対策ならびにインシデント対応を支援するために, 国内で利用されているソフトウェアや装置の脆弱性を対象として対策情報を提供する VN (Vendor Status Notes) と，脆弱性に関わる関連イベントを時系列情報として提供する TRnotes (Status Tracking Notes) から構成する方式を提案する.

表 3.1：Vendor Status Notes における情報提供項目

項目	説明
識別子	脆弱性対策情報 VN を一意に識別するための識別子
タイトル	脆弱性対策情報の題名
概要	脆弱性に関する情報ならびに脆弱性により影響を受けるバージョン, システムに関する情報
想定される影響	脆弱性により発生しうる影響
ベンダ情報	製品開発ベンダの脆弱性対策情報
参考情報	官公庁系の注意喚起やインターネットで公開されている脆弱性対策情報などの参考情報と該当する Status Tracking Notes の情報

(1) Vendor Status Notes (VN)

Vendor Status Notes の目的は脆弱性対策活動を支援するための情報提供である．国内製品や国内向けにポーティングされたオープンソフトウェアなど, 国内で利用されているソフトウェアや装置の脆弱性を対象として製品開発ベンダの対策情報を整理し提供することで2.3.1節の課題(2)(3)の解決を図る．

Vendor Status Notes で提供する情報としては，表 3.1に示すように，脆弱性の概要, 想定される影響, 脆弱性対策に必要となる製品開発ベンダの情報ならびに参考情報がある．

(2) Status Tracking Notes (TRnotes)

Status Tracking Notes の目的は, 実際に発生しているセキュリティ侵害活動の回避や関連する問題事象を解決するインシデント対応活動のための情報提供である．具体的には，図 2.5に示した Blaster ならびに Welchia 出現までの経過情報以外にも次のような事例がある．

事例 1： 各脆弱性の公開ならびに脆弱性を攻略する活動の経過を共有する．

2003 年 7 月に報告された Cisco IOS のサービス運用妨害に関わる脆弱性(CA-2003-15) [CERT03a] については，“ 脆弱性ならびに修正プログラムの公開 ” から “ 攻撃検証コードの公開 ” までの時間が約 1 日強と極めて短時間であった (表 3.2)．さらに，2004 年 3 月に報告された ISS Protocol Analysis Module (PAM) コンポーネントの ICQ 向け解析ルーチンに関わる脆弱性 [ISS04] に至っては, 脆弱性の公開翌日に脆弱性を悪用するネットワークワーム Witty が出現している．

脆弱性公開後の活動経過，すなわち，現在どのような段階にあるのかという状況情報を共有することは大規模インシデントの発生を未然に防ぐという観点からも有効かつ重要となる．

事例 2：　短期間に発生する対策の更新を共有する．

脆弱性対策活動に含まれる部分ではあるが，2003 年 9 月に報告された OpenSSH のバッファ管理機構の脆弱性 (CA-2003-24) [CERT03b] では，初版の対策版 openssh-3.7.tgz リリースからわずか 12 時間後に，影響を受けるバージョンが“ OpenSSH 3.7 未満 ”から“ OpenSSH 3.7.1 未満 ”となり改訂版 openssh-3.7.1.tgz がリリースされた．さらに 1 週間後に新たな脆弱性が確認され，openssh-3.7.1p2.tgz がリリースされている (表 3.3).

製品開発ベンダの迅速な対応は，脆弱性を早期に除去する対策を推進することができる反面，脆弱性対策状況を短期間に変更する可能性を高め，スナップショットとして発行される注意喚起だけでは状況を把握しきれなくなる場合もある．

事例 3：　インシデント発生に伴う各組織の対応を共有する．

2003 年 8 月に出現した電子メール型ワーム Sobig.F [CERT03c] は，8 月末になるとトロイの木馬機能が活性化し，DoS 攻撃活動を開始するというコード解析結果が報告されていた．国内の ISP によっては“ トロイの木馬機能の活性化に関与する特定 IP アドレスへのパケット遮断 ”を実施するなどの予防措置を取っている (表 3.4)．また，Blaster 以降，関連省庁が合同で注意喚起を促す機会も増えてきており，このような各組織の動きをトリガとした脆弱性対策の強化推進は，インシデントを予防するという観点では重要となる．

特に, ネットワークワームや電子メール型ワームのように広範囲に渡る被害を伴うインシデント対応にあたっては，1.1節のインシデント対処で述べている通り，他の組織と連携した共同対処を必要とする場合もあり, 状況把握のための情報共有は連携のための前提条件となる．

表 3.2：Cisco IOS のサービス運用妨害の脆弱性に関連するイベント

[JVN03b]

日時 (JST)	内容
2003-07-17 09:00	Cisco Systems, Inc.“Cisco IOS Interface Blocked by IPv4 Packets”の初版 (Revision 1.0) を Web 公開
2003-07-17 11:40	Full-Disclosure に“Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packet”が投稿される
2003-07-17 AM	ISS AlertCON レベル①から②へ SecurityFocus ThreatCON レベル①から②へ
2003-07-17 13:58	CERT/CC メーリングリストで“CA-2003-15”を配信
2003-07-17 16:10	ISSKK“Cisco IOS におけるリモートからのサービス不能攻撃の脆弱点”を Web 公開
2003-07-18 23:35	@police“Cisco 社製ネットワーク機器の脆弱性について”を Web 公開
2003-07-18 08:00	Cisco Systems, Inc. 影響を受けるプロトコルフィールドを提示した“Cisco IOS Interface Blocked by IPv4 Packets”の第 3 版 (Revision 1.3) を Web 公開
2003-07-18 10:29	Foundstone, Inc. SNScan v1.05 をリリース
2003-07-18 13:42	Full-Disclosure に攻撃検証コードが投稿される #Cid: shadowchode.tar.gz #Cid: 07.18.shadowchode.c
2003-07-18 19:00	Cisco Systems, Inc. 攻撃検証コードが公開されたことに伴い,“Cisco IOS Interface Blocked by IPv4 Packets”の第 4 版 (Revision 1.4) を Web 公開
2003-07-18 PM	ISS AlertCON レベル②から③へ
2003-07-18	OCN“Cisco 社製ルータの脆弱性に対するＯＣＮの対応について (該当パケットを遮断)”を Web 公開 NTT 西日本“Cisco 社製ルータにおける脆弱性に対する NTT 西日本の対応について (該当パケットを遮断)”を Web 公開
2003-07-19 00:29	CERT/CC メーリングリストで“CA-2003-17”を配信
2003-07-19 AM	SecurityFocus ThreatCON レベル②から③へ
2003-07-21 07:54	Full-Disclosure に“FW: Cisco Vulnerability forensic protocol analysis results.”が投稿される
2003-07-22 AM	ISS AlertCON レベル③から②へ SecurityFocus ThreatCON レベル③から②へ

表 3.3：OpenSSH のバッファ管理機構の脆弱性に関連するイベント

[JVN03c]

日時 (JST)	内容
2003-09-16 01:02	Full-Disclosure に“new ssh exploit? (ssh の新たな脆弱性の存在有無に関する問合せ)”が投稿される
2003-09-16 08:31	Full-Disclosure に“openssh remote exploit (openssh の脆弱性に関する指摘)”が投稿される
2003-09-16 13:56	OpenSSH openssh-3.7.tgz, openssh-3.7p1.tgz をﾘﾘｰｽ
2003-09-16 21:32	OpenSSH“OpenSSH Security Advisory: buffer.adv 第 1 版 (RCS file: buffer.c,v)”を openbsd-announce に投稿ならびにWeb公開 #Affected-Version: OpenSSH 3.7 未満
2003-09-17 01:25	OpenSSH openssh-3.7.1.tgz, openssh-3.7.1p1.tgz をﾘﾘｰｽ
2003-09-17 08:06	CERT/CC ﾒｰﾘﾝｸﾞﾘｽﾄで“CA-2003-24”を配信 #Affected-Version: OpenSSH 3.7 未満
2003-09-17 08:13	OpenSSH“OpenSSH Security Advisory: buffer.adv 第 2 版 (RCS file: buffer.c,v channels.c,v)”を openbsd-announce に投稿ならびにWeb公開 #Affected-Version: OpenSSH 3.7.1 未満
2003-09-17 13:37	ISSKK“OpenSSH ﾒﾓﾘ破損の脆弱性”を Web 公開
2003-09-17	CERT/CC“CA-2003-24 第 2 版”を Web 公開 #Affected-Version: OpenSSH 3.7.1 未満
2003-09-19 07:11	Full-Disclosure に“new openssh exploit in the wild! (remote openssh buffer management sploit を装ったﾄﾛｲの木馬 theosshucksass.c)”に関する情報が投稿される
2003-09-23 14:49	OpenSSH openssh-3.7.1p2.tgz をﾘﾘｰｽ
2003-09-23 (米国日付)	CERT/CC OpenSSH の“Pluggable Authentication Modules (PAM)”の脆弱性に関する Vulnerability Note VU#209807, VU#602204を Web 公開
2003-09-23 21:39	OpenSSH Portable OpenSSH 3.7.1p2 released を openbsd-announce に投稿ならびにWeb公開
2003-09-30 08:08	CERT/CC ﾒｰﾘﾝｸﾞﾘｽﾄ“CERT Advisory Notice: Clarifications regarding recent vulnerabilities in OpenSSH (OpenSSH に 3 つの脆弱性 VU#333628, VU#209807, VU#602204 が報告されていることに関する注意喚起)”を配信

表 3.4：電子メール型ワーム Sobig.F の流布に関連するイベント

[JVN03a]

日時 (JST)	内容
2003-08-19 08:46	W32.Sobig.F がネットワークニュースグループに投稿される
2003-08-18 (米国日付)	シマンテック W32.Sobig.F@mm を確認
2003-08-19 (米国日付)	ネットワークアソシエイツ W32/Sobig.f@MM を確認 トレンドマイクロ WORM_SOBIG.F を確認
2003-08-20 08:29	@police“Sobig.F ウィルスの蔓延について”を Web 公開
2003-08-22	IPA/ISEC“W32/Sobig の亜種 (Sobig.F) に関する情報”を Web 公開
2003-08-22 (米国日付)	CERT/CC“CERT Incident Note IN-2003-03 W32/Sobig.F Worm”を Web 公開
2003-08-23 02:38	OCN SOBIG.F 対策における特定 IP アドレスへのパケット遮断を実施
2003-08-23 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-08-25 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-08-25 11:37	ISSKK“大量に電子メールを配信する Sobig.F ワームトロイの木馬機能”を Web 公開
2003-08-25	OCN“SOBIG.F 対策における特定 IP アドレスへのパケット遮断について”を Web 公開
2003-08-29 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-08-31 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-09-05 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-09-07 04:00-07:00	W32.Sobig.F トロイの木馬機能の活性化 (活動は不発)
2003-09-10	W32.Sobig.F 活動停止
2003-09-18	OCN“SOBIG.F 対策における特定 IP アドレスへのパケット遮断の解除について”を Web 公開

そこで, Status Tracking Notes で提供する情報としては, 表 3.5に示す通り脆弱性またはインシデントに関する概要に加えて, 攻撃検証コードの公開, インターネット定点観測システムの兆候変動, 官公庁系の注意喚起発行など監視ならびに対応体制のエスカレーションのトリガとなりえるイベント, 特定パケットの遮断や DNS の設定変更などを用意した. これらインシデントの拡大防止のために実施された対処に関するイベントをインシデント対応に求められる時系列イベントとして加味することで, 2.3.1節の課題(1)の解決を図っている.

表 3.5：Status Tracking Notes における情報提供項目

項目	説明
識別子	脆弱性に関して共有すべき状況情報 TRnotes を一意に識別するための識別子
タイトル	脆弱性に関して共有すべき状況情報の題名
概要	脆弱性やインシデントに関する情報
時系列イベント	脆弱性の発見日, 各種勧告の発行日, 攻撃検証コードの公開日, ワームやウイルスの出現日, 官公庁系の注意喚起発行日などのイベント情報
参考情報	該当する Vendor Status Notes の情報

3.2.2　試行サイトでの実現方式

脆弱性／インシデント対処情報共有システムとして JVN を具体化するためには，情報提供に必要となる情報識別子の付与方法や時系列イベントの表記方法などを規定すると共に，国内で脆弱性対策ならびにインシデント対応をおこなっている既存 CSIRT が推進する活動との協調が必要となる．本節では，JPCERT/CC の試行サイトとして実施した情報提供について述べる．

(1) VN - Vendor Status Notes 試行サイトの構築のアプローチ

Vendor Status Notes 試行サイト構築にあたっては，JPCERT/CC が実施している情報提供との関連を保つことに主眼を置き，次に示す方針を設定した．

(a) 主要な対策勧告に追従した Vendor Status Notes の提供

試行サイトの構築にあたっては表 3.6に示す通り，構築フェーズを 3 つに分けることとし，本研究を構築フェーズのステップ 1 に位置付ける．また，ステップ 1 の実施事項は，次の通りとする．

- 広く知られている対策勧告である CERT Advisory ならびに CIAC Bulletin に追従することにより，インターネット全体に影響を及ぼす可能性の高い脆弱性ならびにインシデントに関する情報を提供すること．
- CERT Advisory については，国内のシステム管理者やシステムエンジニアの注目度も高いことから，製品開発ベンダの脆弱性対策情報を収集後，整理し同日公開すること．

表 3.6：Vendor Status Notes の構築フェーズ

構築フェーズ	説明
ステップ 1 (本研究の対象)	主要な対策勧告に関する製品開発ベンダの脆弱性対策情報を整理し提供
ステップ 2	国内で報告された脆弱性に関する製品開発ベンダの脆弱性対策情報を整理し提供
ステップ 3	製品開発ベンダが対策勧告発行と同時に脆弱性対策情報を提示できる早期状況提供体制の整備

(b) 対策勧告の文書番号に基づく識別子の付与

脆弱性を一意に識別する識別子して, 脆弱性情報ならびにセキュリティ情報の関連付けのために開発された CVE がある．しかし，Vendor Status Notes の場合には, システム管理者やシステムエンジニアに対策勧告との関連性を明示的に示すことがより重要であると考え，CERT Advisory あるいは CIAC Bulletin の文書番号に JVN の文書であるプレフィックスを付与した形式を使用する.

(c) 既存情報提供活動との関連性の確保

JPCERT/CC ではインシデント報告などに基づき同種のインシデント発生の防止を目的とした緊急報告，最新のセキュリティ関連情報などを週刊でまとめた JPCERT/CC レポートを発行している. 試行サイトでは, 緊急報告, JPCERT/CC レポートで取り上げる製品開発ベンダの脆弱性対策情報との整合性をとり公開型データベースを作成する．これにより，スナップショットとして発行される緊急報告，JPCERT/CC レポートと，これら情報の計時的な集積となる Vendor Status Notes との連携を図る.

(d) 製品開発ベンダからの脆弱性対策情報通知手順の確立

国内の製品開発ベンダの脆弱性対策情報を整理するにあたっては, 試行サイト側で一方的に脆弱性対策情報を収集し開示するのではなく, 製品開発ベンダの協力を得た推進を実施する．すなわち，製品開発ベンダからの脆弱性対策情報通知手順を整備することで2.3.1節の課題(3)で示した整理手順の改善を図っていく．表 3.6のステップ 1 では，製品開発ベンダ側の業務形態と作業工数を考慮し，表 3.7に示す電子メールフォーマットと試行サイト更新に必要な情報を電子メールにより通知する手順を準備することとした.

表 3.7：通知手順で使用する電子メール通知フォーマット

タグ	説明
X-JVN-cano:	CERT Advisory No (必須)
X-JVN-vendor:	製品開発ベンダ名称 (必須)
X-JVN-id:	脆弱性対策情報の ID (オプション)
X-JVN-title:	脆弱性対策情報のタイトル (必須)
X-JVN-url:	脆弱性対策情報の掲載された URL (必須)
X-JVN-update:	脆弱性対策情報の更新日 (オプション)

(2) TRnotes - Status Tracking Notes 試行サイトの構築のアプローチ

脆弱性ならびに修正プログラムの公開直後からの経過を共有することは大規模インシデントの発生を未然に防ぐという観点からも有効かつ重要となる．たとえば，3.2.1節の事例 1 に示した Cisco IOS のサービス運用妨害に関わる脆弱性(表 3.2)については，“脆弱性ならびに修正プログラムの公開”から“攻撃検証コードの公開”までの時間が約 1 日強であった．さらに，ISS PAM コンポーネントの ICQ 向け解析ルーチンに関わる脆弱性に至っては，脆弱性対策情報の公開翌日に脆弱性を悪用するネットワークワーム Witty が出現している．

このような実情を踏まえ，Status Tracking Notes 試行サイト構築にあたっては関連するイベントを時系列情報として共有することに主眼を置き，次に示す方針を設定した．

(a) 時間単位での時系列イベント表示

脆弱性対策ならびにインシデント対応に関連する状況変化は日単位というよりは時間単位になりつつある．さらに，時差を加味したイベントの時系列化は，インターネット全体として状況変化を追いかけやすくなる．この 2 点を考慮し，時差を加味すると共に，可能な限り時間単位レベルでのイベント表示をおこなう．現時点の時刻情報の収集方法として，メーリングリストの場合には投稿時間，Web サイトの場合には HTTP プロトコルのヘッダ情報として提供される Last-Modified を利用する．

表 3.8：TRnotes におけるイベントの特徴項目

項目	内容
Affected-Port	脆弱性により影響を受けるポート番号
Affected-Version	脆弱性により影響を受けるバージョン情報
Severity-Rating	脆弱性の深刻さ
Cid	攻撃検証コードに付与されていると思われるファイル名
Tested	攻撃検証コードの動作環境に関する情報
Binding-Port	攻撃検証コードが使用すると思われるポート番号

例:攻撃検証コードの公開

日付 (JST)	**内容**
2003-11-12 21:40	Full-Disclosure **に** "Proof of concept for Windows Workstation Service overflow" **が投稿される** #Cid: 11.12.MS03-049PoC.c #Tested: Windows 2000 [EN] + SP4 #Binding-Port: 5555 #Post-Date: Wed, 12 Nov 2003 15:40:38 +0300

(b) 公開情報に基づくイベントの時系列化

組織にまたがって経過を共有することを想定し, 公開されている情報に基づき状況変化, すなわち時系列イベントをまとめる. これにより, 組織間の情報共有でしばしば問題となる情報に対する守秘義務などの制約が発生せず, より多くのシステム管理者やシステムエンジニアとの間で関連するイベントを時系列情報として共有することが可能となる.

(c) イベントの特徴項目の抽出

脆弱性に関わる経過記述にあたっては, 表 3.8に示すイベントを特徴付ける項目として抽出し併記する. これらは, 類似するイベント同士の差分の明確化, 対応体制のエスカレーションのトリガ, 監視項目の対象となりえる項目となる. たとえば, 脆弱性が発見された場合には, 脆弱性の深刻さや脆弱性により影響を受けるバージョン情報をイベントの特徴付け項目とした. 攻撃検証コードの公開の場合には, 攻撃検証コードの名前, 動作確認のおこなわれた環境, 攻撃検証コードの動作として使用すると思われるポート番号を特徴付け項目とした. 特に, 攻撃検証コードの名前は, 攻撃検証コードを掲載するサイトによって名前が異なることも多いことから, 同一の攻撃検証コードを異なる名前で参照している場合などに利用することができる. また, 使用すると思われるポート番号については, 公開型のインターネット定点観測システム [Dshield] のモニタリング情報を参照する形態をとることで簡易的な機能連携を実現する.

(d) Vendor Status Notes との連携

脆弱性対策活動とインシデント対応活動のつながりを考慮し, 脆弱性に関する対策情報が整理されている Vendor Status Notes と脆弱性に関する経過情報 Status Tracking Notes を相互参照可能とする.

3.3　試行サイトの有効性検証

本節では, 試行サイトにおける利用実績ならびに利用状況と, 時系列イベントからの特徴抽出を通して JVN の有効性を検証する.

3.3.1　利用実績ならびに利用状況

(1) 試行サイトでのサービス提供実績

2003 年 2 月から開始した試行サイトでの Vendor Status Notes 提供事例を図 3.3に示す. 試行サイトでは, 対策勧告である CERT Advisory ならびに CIAC Bulletin に追従した脆弱性対策情報として約 210 件を提供すると共に, 国内製品開発ベンダの協力を得て脆弱性対策情報通知手順を用いた製品開発ベンダ情報の更新を実施した. また, 概要, 想定される影響, 製品開発ベンダ情報に加え, 脆弱性対策情報の Web ページ毎に PGP (Pretty Good Privacy) による電子署名情報を準備することにより, 脆弱性対策情報の発信元を確認できる手段を提供した.

2004 年 1 月から開始した試行サイトでの Status Tracking Notes 提供事例を図 3.5に示す. 試行サイトでは, CERT Advisory, CERT Vulnerability Notes Database ならびに CIAC Bulletin のうち約 40 件を対象に経過情報を提供すると共に, 国内 CSIRT 組織の協力を得てイベント情報の更新を実施した.

(2) サービスの利用状況と情報提供の有効性

試行サイト全体の利用状況を HTTP GET アクセスと HEAD アクセスの面グラフとして示す (図 3.4). 試行サイト運用開始から半年が経過した以降は, 立ち上げ当初の倍近くの利用頻度となっており, 少しづつではあるが活用されていることを確認した. また, 図 3.6に 2004 年 9 月から 2005 年 2 月に掲載した 5 件の VN エントリのアクセス数推移を面グラフとして示す. 図 3.6の VN エントリ毎のアクセス数が山となっている部分は, 新たな脆弱性対策情報が公開されたときとほぼ合致していることと, 1 日あたりのアクセス数は公開後おおよそ約 2 週間から 1 ヶ月までの間がそれ以降に比べ多くなっているという結果が得られた. この結果は, 製品開発ベンダが脆弱性対策情報を JVN に掲載する際の期間的な目安として利用できる.

図 3.3：VN での情報提供事例 (JVNCA-2003-04)

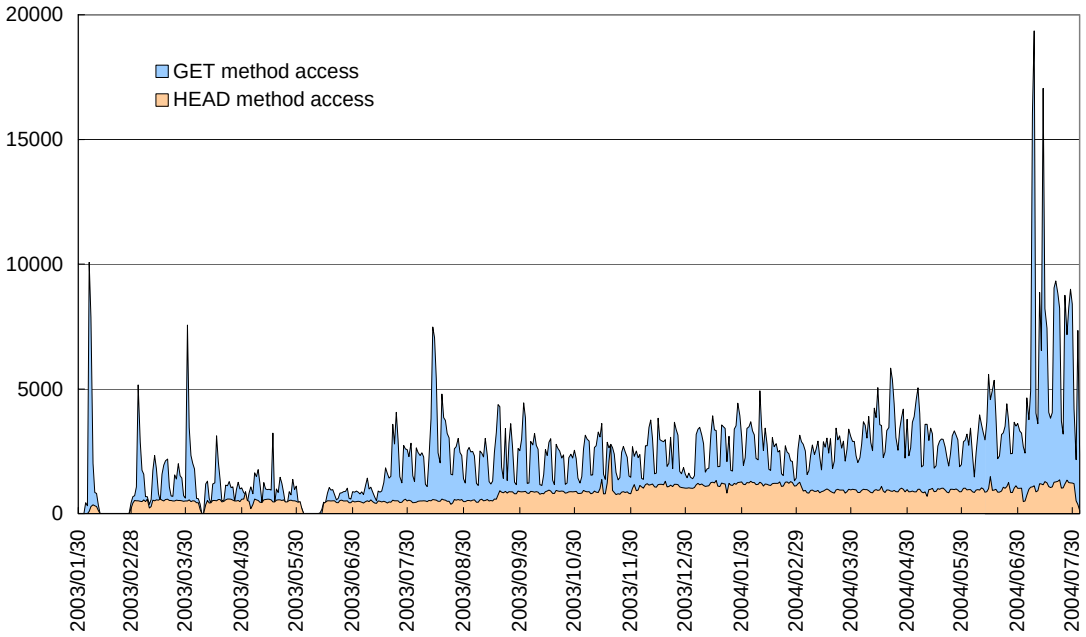


図 3.4：JVN 試行サイトのアクセス数状況

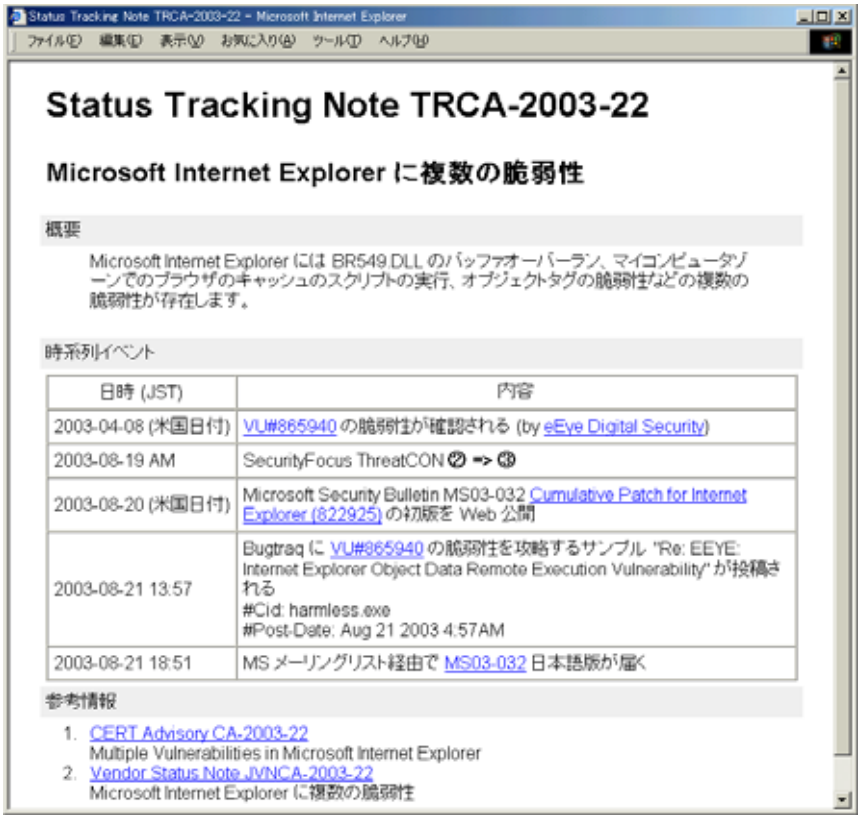


図 3.5：TRnotes での提供情報事例 (TRCA-2003-22)

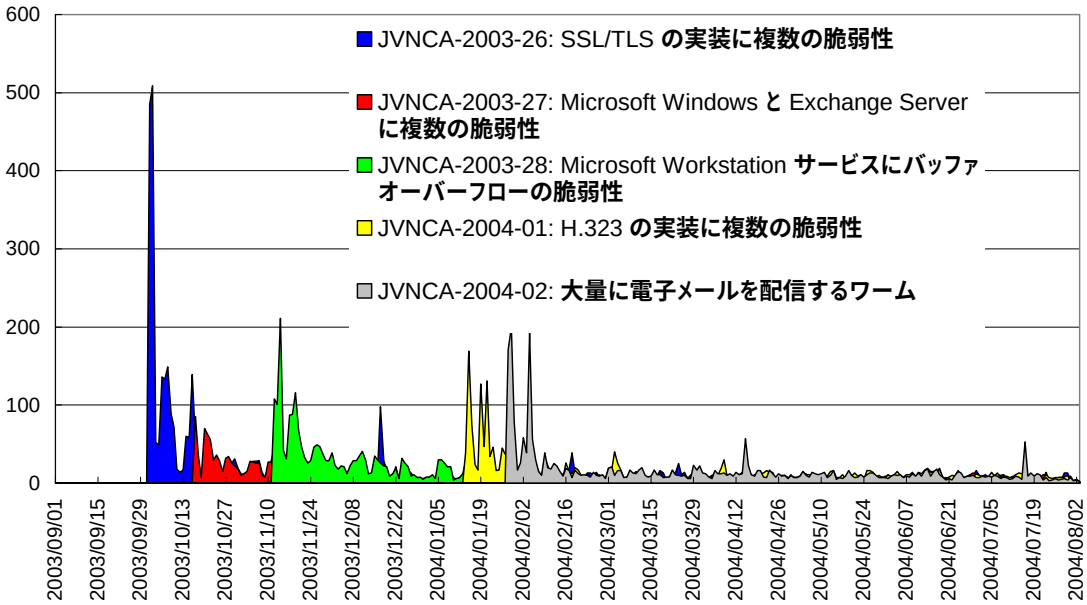


図 3.6：VN エントリ毎のアクセス数の推移

次に, 脆弱性対策情報の提供にあたって考慮した脆弱性対策とインシデント対応活動支援の観点から利用状況について述べる.

(a) 脆弱性が公開されてから，その脆弱性を悪用したインシデントが発生した事例

脆弱性が公開されてから, その脆弱性を悪用したインシデントが発生した事例として Microsoft Windows 環境の脆弱性 [MS04] を悪用し流布した Sasser を取り上げる.

Sasser に関しては表 3.9に示す 3 件の Vendor Status Notes と Status Tracking Notes を提供している．これら情報の利用状況である図 3.7を見ると，当初は脆弱性対策情報である JVNTA04-104A に比べ，経過情報を示す TRTA04-104A へのアクセスは少ないものの，Sasser の出現にあわせアクセス数が増加している．また Sasser に絞った経過情報のリリースに伴い TRJVN04-2004-02 にアクセスが集まり，収束すると全体の経過情報である TRTA04-104A にアクセスが戻っている．この事例の場合, 脆弱性対策とインシデント対応活動のつながりを対象とした情報提供が活用されたと判断できる.

(b) 脆弱性の公開を伴わずにインシデントが発生した事例

脆弱性の公開を伴わずにインシデントが発生した事例として Netsky を取り上げる.

Netsky に関しては表 3.10に示す 2 件の Status Tracking Notes を提供している．これら情報の利用状況である図 3.8を見ると，当初は Netsky とその亜種の出現に関する経過情報を示す TRIN-2004-02 へのアクセスは少ないものの，DDoS 機能を具備した亜種 Netsky.Q の出現にあわせアクセス数が増加している．また Netsky.Q に絞った経過情報の公開に伴い TRJVN-2004-01 にアクセスが集まり，収束すると Netsky 全体の経過情報である TRIN-2004-02 にアクセスが戻っている．この事例の場合，インシデント全体の情報とその中の特定のインシデントを対象とした情報提供の組合せが活用されたと判断できる.

いずれの事例においても，脆弱性対策情報である Vendor Status Notes とインシデント対応のための経過情報である Status Tracking Notes の双方が活用されているという利用状況を確認した.

表 3.9：Sasser に関連して発行した VN，TRnotes の概要

名称	種別	提供情報の概要
JVNTA04-104A	VN	2004 年 4 月に Microsoft Windows 環境において確認された複数の脆弱性(MS04-011～MS04-014)に関する脆弱性対策情報である.
TRTA04-104A	TRnotes	上記 Microsoft Windows 環境において確認された複数の脆弱性に関する経過情報である. 2004 年 4 月～7 月の期間で約 130 件の経過記録があり, うち, 攻撃検証コードの公開に関する記録が 12 件, ウイルスの出現に関する記録が約 30 件となっている.
TRJVN04-2004-02	TRnotes	Sasser に絞った経過情報である. 2004 年 4 月～5 月の期間で約 30 件の経過記録がある.

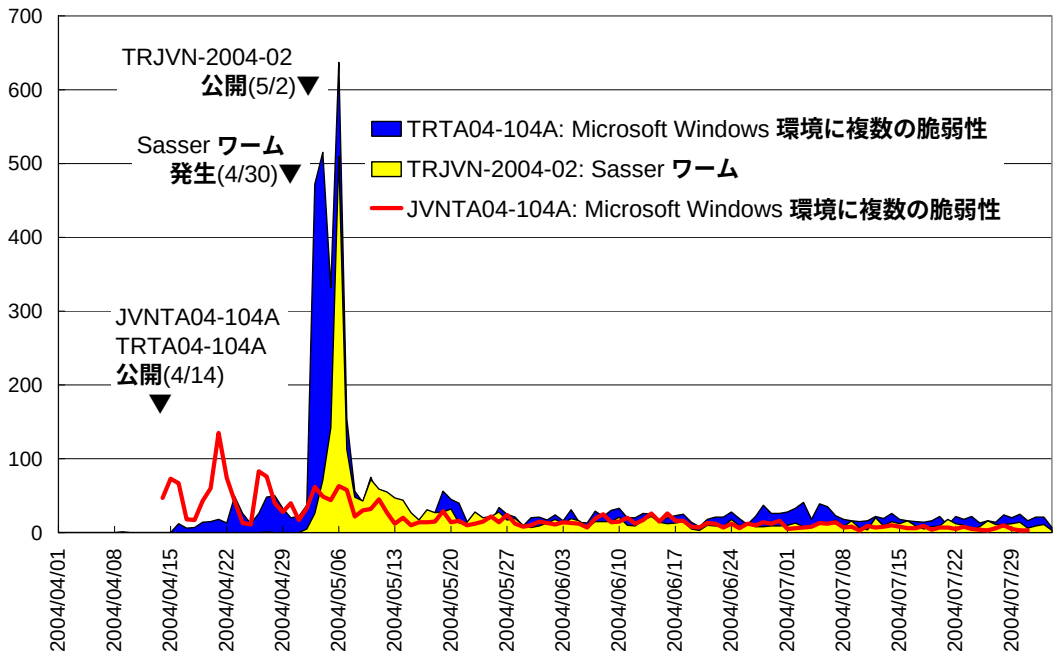


図 3.7：Sasser に関連する VN，TRnotes のアクセス状況

表 3.10：Netsky に関連して発行した TRnotes の概要

名称	種別	提供情報の概要
TRIN-2004-02	TRnotes	Netsky とその亜種の出現に関する経過情報であり，Netsky.Q 以外の DDoS 機能を具備した亜種 Netsky.S～Netsky.Z など，2004 年 3 月～7 月の期間で約 110 件の経過記録がある.
TRJVN-2004-01	TRnotes	DDoS 機能を具備した亜種 Netsky.Q に絞った経過情報である. 2004 年 3 月～4 月の期間で約 14 件の経過記録がある.

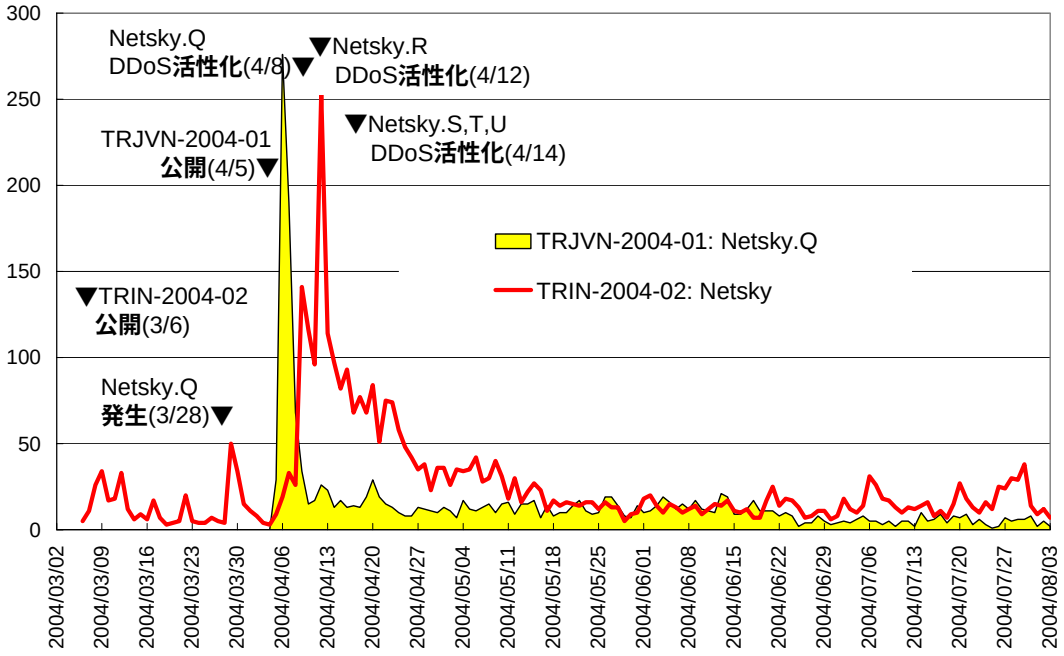


図 3.8：Netsky に関連する TRnotes のアクセス状況

3.3.2 ネットワークワーム出現と時系列イベントの関連性

本節では，ネットワークワーム出現に関する時系列イベントの特徴抽出を通して，提案方式が脆弱性対策とインシデント対応活動支援に有効であることを示す.

表 3.11：Windows 環境の脆弱性を悪用した代表的なマルウェア

脆弱性	出現した代表的なマルウェア
MS03-001	Nachi.F
MS03-007	Nachi～Nachi.F
MS03-014	Mimail
MS03-026	Blaster, Nachi～Nachi.F, Raleka, Cirebot
MS03-049	Nachi.B～Nachi.F
MS04-011	Sasser, Gaobot

表 3.12：Blaster，Sasser ワーム出現までの代表的な時系列イベント

項目	MS03-026	MS04-011
発生したネットワークワーム名	Blaster	Sasser
脆弱性公開日	2003 年 7 月 17 日	2004 年 4 月 14 日
公開された攻撃検証コードの数	4 種類以上	4 種類以上
攻撃検証コードの初出日	2003 年 7 月 21 日	2004 年 4 月 17 日
ネットワークワームに利用された攻撃検証コードの公開日	2003 年 8 月 11 日	2004 年 4 月 30 日
脆弱性を悪用するトロイの木馬の出現日	2003 年 8 月 2 日 Cirebot	2004 年 4 月 27 日 Gaobot
脆弱性を悪用するトラフィックの兆候発生日	2003 年 8 月 5 日	2004 年 4 月 30 日
攻撃検証コードが使用するポート番号に関するトラフィックの兆候発生日	2003 年 8 月 11 日	－

2003 年～2004 年にかけて報告された Windows 環境の脆弱性 [MSa] のうち, その脆弱性を悪用して流布した代表的なマルウェアは表 3.11の通りである．このうち，ネットワークワームの出現につながった“MS03-026 (CA-2003-16): Microsoft Windows RPC にバッファオーバーフローの脆弱性 [MS03]”，“MS04-011 (TA04-104A): Microsoft Windows 環境に複数の脆弱性 [MS04]”の脆弱性について, マニュアル作業で時系列イベントの抽出をおこなったところ表 3.12に示す結果が得られた．この時系列イベントの抽出からは次の特徴を導き出すことができる．特に，前者の脆弱性を悪用するトロイの木馬の出現は, 脆弱性の攻略しやすさ，すなわち脆弱性を攻略するネットワークワームへの発展可能性のひとつの指標となり, 監視や対応体制の強化を図るトリガのひとつになると言える．

- ネットワークワームの出現につながった脆弱性は，ネットワークワームの出現前に脆弱性を悪用するトロイの木馬が発見されている．
- 脆弱性の悪用に使用するポート番号あるいは攻撃検証コードが使用するポート番号のトラフィックには，攻略活動の兆候が現れる．

このように脆弱性公開後の時系列イベントの提供は，インシデントの予兆に関する情報共有にもつながり，脆弱性対策とインシデント対応活動支援の観点からも有効であると判断できる．

3.4 まとめ

本章では，国内でのインシデントオペレーションを支援するために，脆弱性／インシデント対処情報共有システム JVN (JP Vendor Status Notes) を提案した．

まず，課題解決にあたっては，脆弱性対策活動とインシデント対応活動を考慮し，国内で利用されているソフトウェアや装置の脆弱性を対象として脆弱性対策情報を提供する Vendor Status Notes と，対策勧告で取り上げられた脆弱性攻略に伴うインシデント対応に備え，脆弱性に関わる経過を時系列情報として提供する Status Tracking Notes から構成する方式を提示した．

次に，提案に基づき Web 試行サイトを構築し運用した．利用状況は立ち上げ当初の倍近くの利用頻度となっており，少しづつではあるが活用されている．また，“ 脆弱性が報告されてから，その脆弱性を悪用したインシデントが発生した事例 ”，“ 脆弱性の公開を伴わずにインシデントが発生した事例 ”のいずれにおいても，脆弱性対策情報である Vendor Status Notes とインシデント対応の経過情報である Status Tracking Notes の双方が活用されていることを確認した．さらに，時系列イベントの抽出から，ネットワークワーム出現までの過程において，脆弱性を悪用するトロイの木馬の出現は，監視や対応体制の強化を図るトリガのひとつになることを提示した．以上の試行活動を通して，提案システムを用いることにより，セキュリティに関わる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支援に有効な情報共有が可能となることを確認した．

現在，JVN 試行サイトは，2004 年 7 月 7 日，経済産業省告示 “ ソフトウェア等脆弱性関連情報取扱基準 ”を受けて，日本国内の製品開発ベンダの脆弱性対応状況を公開する対策ポータルサイト (http://jvn.jp/) としてリニューアルされ発展的に活用されている．

第4章　ネットワークワーム動作検証システム

本章では, 各組織単独で実施可能なネットワークワーム挙動解析の検証環境が整備されていないという 2 つ目の課題を解決するために, ネットワークワームの挙動に関する情報収集を目的とした動作検証システムとして, 感染先探索特性の検証システムと感染動作の検証システムを提案する.

4.1　まえがき

2004 年 4 月 30 日の Sasser の出現を皮切りに，5 月 1 日には Sasser.B，5 月 2 日には Sasser.C とその亜種が連日にわたり出現した．Sasser は Code Red，Nimda，Blaster と同様にネットワーク上の感染先システムを探索し流布する．これらネットワークワームの特徴は，感染のための探索 IP アドレスをランダムに生成し，その IP アドレスの特定ポート番号に対して直接 TCP コネクションを確立する．確立に成功した場合には，特別なメッセージを送付することで脆弱性を攻略し感染を試みる．

ネットワークワームが感染のために選択する探索 IP アドレスの特性は，同一ネットワーク内での感染流布やインターネットからイントラネットへの感染橋渡しの可能性に影響を与える．Sasser の選択する探索 IP アドレスの特性については，いくつかのウイルス対策ベンダやセキュリティベンダから提供されており，そのコード解析結果 [eEye04] によれば感染のために選択する探索 IP アドレスの生成は表 4.1の通りである．表 4.1において，上位 2 オクテットが同一 (同.同.異.異) とは，感染したシステムの IP アドレスを 131.113.1.1 とした場合，その感染したシステムが感染先として IP アドレス 131.113.x.x を 25%の割合で選択することを意味している．コード解析やシミュレーションによりネットワークワーム流布の傾向を検討しやすくなってきてはいる．しかし，探索 IP アドレスの生成アルゴリズムにバグがあった場合や実際に使用する乱数生成ルーチンによって発生しうる感染特性の偏りまでを考慮するまでには至っていない.

表 4.1：Sasser ワームが選択する探索 IP アドレスの生成割合

感染先となる探索 IP アドレス	割合
上位 2 オクテットが同一(同.同.異.異)	25%
上位 1 オクテットが同一(同.異.異.異)	23%
上記以外(異.異.異.異)	52%

たとえば，偏りにより上位 2 オクテットが同一 (同.同.異.異) を選択する割合が高くなったとすると，イントラネットに感染した場合には，感染活動がイントラネットに留まる確率が高くなり，結果としてイントラネットへの流布拡大の可能性が高くなる．すなわち，感染先の探索範囲は，ネットワークワームがイントラネットに感染した場合，深刻な被害に直結するか否かを左右する要因であり，インシデントオペレーションの対処段階において感染拡大を予測する判断情報のひとつとなっている．このため，実測データに基づく感染先の探索範囲の検証は，コード解析結果を確認する情報として重要であると考えられているが，公開された実測データはないのが実情である．

また，ネットワークワームの感染拡大を防ぐにあたっては，組織外部の情報に頼りきってしまうのではなく，各組織単独で対策立案のための情報収集手段，たとえば感染動作を検証する実機環境などを保有することは早期対応ならびに情報収集のバックアップという点からも重要である．特に，ネットワークワームが発生してから，組織外部のコード解析情報が公開されるまでの間の対策立案については検討の余地がある．

本章では，ネットワークワーム流布時の対策立案への利用を踏まえ，感染先の探索範囲に関する動作情報の収集を目的としたネットワークワーム感染先探索特性の検証システムと，感染動作に伴い使用するポート番号情報の収集を目的としたネットワークワーム感染動作の検証システムを提案する．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．

本章の構成について述べる．4.2節で検証システムについて述べ，4.3節で検証システムを用いた実験による効果を示す．4.4節はまとめである．

4.2 動作検証を実現する 2 つの検証システム

本節では，2.3.2節で述べた課題を解決するためにネットワークワームの挙動に関する情報収集を目的とした動作検証システムとして，ネットワークワーム感染先探索特性の検証システムとネットワークワーム感染動作の検証システムについて述べる．

4.2.1　システム要件

提案する 2 つの検証システムは, ネットワークワームの検体が存在するか, あるいは, 感染したと思われるシステムが存在することを前提としている．ここでは，2.3.2節で述べた課題を踏まえ，提案するシステムに必要とされる要件をまとめる．

要件 1：　各組織単独で実施可能な情報収集手段であること．すなわち，特殊な装置を使用する必要がないこと，小規模な機器構成であること．

要件 2：　ネットワークワームの感染拡大を防ぐために必要となる情報を収集できること．ただし，本節では，感染拡大を防ぐために必要となる情報として感染のひろがりに関わる情報，感染の通信動作に関わる情報を対象とし，具体的には次の 2 つの情報収集を可能とすること．

(a) ネットワークワームが生成する感染先となる探索 IP アドレスを収集できること．

(b) ネットワークワームが感染動作に伴い使用する送信先ポート番号の情報を収集できること．

要件 3：　効率的な検証を可能とすること．すなわち，ネットワークワームの特徴でもあるランダムに生成される探索 IP アドレスを被感染システムに収束させ，効率的に感染動作につなげること．

4.2.2　ネットワークワーム感染先探索特性の検証システム

ネットワークワーム感染先探索特性の検証システムは, ネットワークワームが感染のために選択する探索 IP アドレスの特性，特に，IP アドレスの発生分布に関する情報を収集することを目的とする(要件 2 の(a))．また，本検証システムで収集した情報は，ネットワークワームの探索動作安定性に関する情報にも利用できることを4.3.2節で示す．本検証システムの構成は図 4.1の通りである．

感染 PC は仮想マシン環境を備えており，この仮想マシン環境上でネットワークワームの検体を実行する. モニタ装置はパケットモニタ機能で感染動作の通信履歴をファイルに記録し，トラフィック集計機能では記録されたファイル中の通信履歴を集計する．最終的に，経過時間毎やアドレスブロック毎の探索 IP アドレスの発生分布などを Web インタフェースにより表示する. なお, 検証システムのプロトタイプ開発にあたっては, パケットモニタ機能としてコマンドライン型 ethereal [Ethereal] を使用し，トラフィック集計機能と Web インタフェース向けの表示整形をスクリプト言語 perl で実装した．

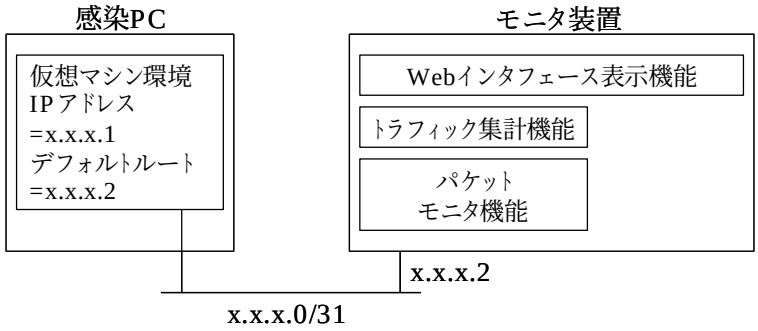


図 4.1：ネットワークワーム感染先探索特性の検証システム構成

(1) トラフィック集計機能

トラフィック集計機能では, 要件 2(a)を満たすために, パケットモニタ機能の記録したファイル中の通信履歴から次の 4 項目のデータ抽出をおこなう.

- 経過時間毎の探索 IP アドレスの発生分布 (図 4.2の左上)
- 上位 1 オクテットが同一 (同.異.異.異) となる探索 IP アドレスの発生分布 (図 4.2の左下)
- 上位 2 オクテットが同一 (同.同.異.異) となる探索 IP アドレスの発生分布 (図 4.2の右下)
- 上位 2 オクテットが同一，上位 1 オクテットが同一，その他についての探索 IP アドレスの生成割合 (図 4.2の右上)

また, パケットの抽出にあたっては, ブロードキャストアドレスを除外すると共に, ネットワークワームが感染のために送出するパケットが同一である点に着目して, 最も発生頻度の高い送信先ポート番号のパケットのみを抽出する (ICMP の発生頻度が高い場合には ICMP パケットのみを自動抽出する). これにより，感染 PC あるいは仮想環境自体が正常稼動のために送出するパケットを除外している.

(2) Web インタフェース表示機能

Web インタフェース表示機能は，トラフィック集計機能の抽出したデータファイルを利用して，項番(1)の該当項目のグラフ用の画像ファイルと図 4.2を表示するための HTML ファイルを出力する.

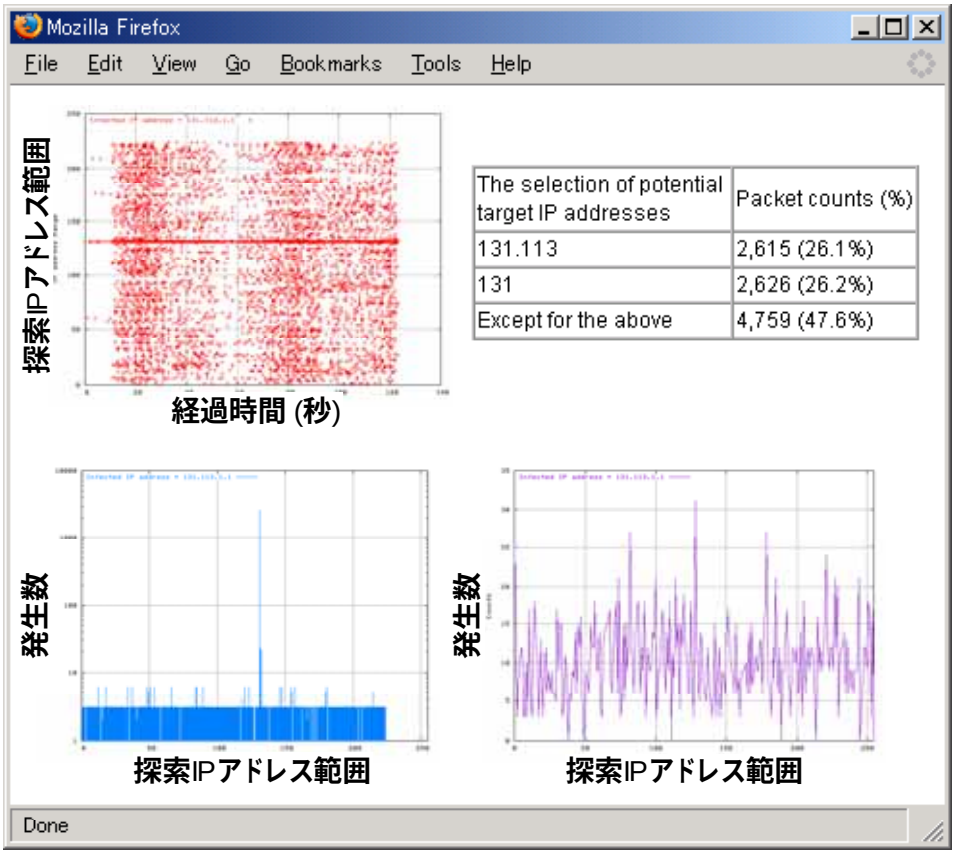


図 4.2：感染先探索特性の検証システムの Web インタフェース

本検証システムの構成上の特徴は次の通りである.

- 2 台の PC で検証環境を構築できる (要件 1).
- サブネットワークに属する IP アドレスが感染先として選択された場合にも, トラフィック集計に利用できない通信履歴は最大 3 個に抑えることができる[iii].

iii) 感染先として，感染 PC の IP アドレスならびにサブネットワークのブロードキャストアドレスが選択された場合には，トラフィック集計に利用可能な通信履歴として収集できない可能性がある.

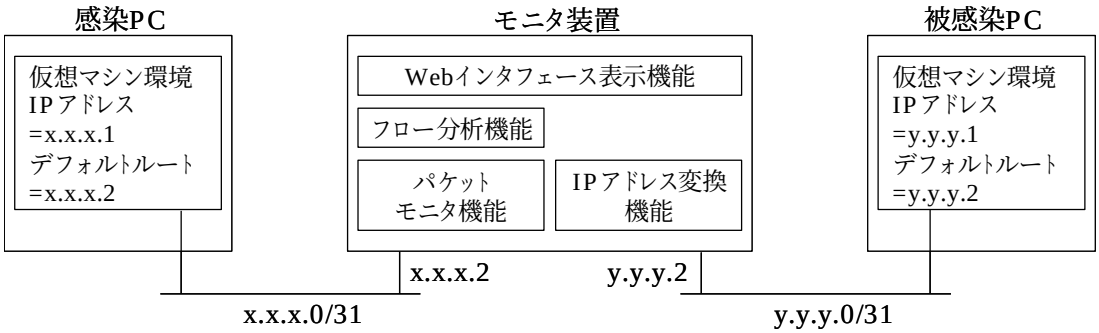


図 4.3：ネットワークワーム感染動作の検証システム構成

ただし, 感染のために選択された IP アドレスとしてモニタ装置以外の IP アドレスが選択された場合にはパケットを廃棄する．このため，TCP を用いて感染活動をおこなうネットワークワームの場合, 感染 PC からの TCP の SYN パケットのみの送信に留まり，TCP コネクションを確立することはできない．また，感染 PC として感染したと思われるシステムを本検証システムに接続する場合には，ネットワーク環境設定を感染 PC に合わせる必要があるため，必ずしもトラフィック集計に利用可能な通信履歴を収集できない場合がある．

4.2.3 ネットワークワーム感染動作の検証システム

ネットワークワーム感染動作の検証システムは，ネットワークワームの感染動作，特に感染動作に伴い使用するポート番号の情報収集を目的とする (要件 2 の(b))．ここで得られたポート番号のトラフィックを止めることにより, 流布拡大を阻止することができる．本検証システムの構成を図 4.3に示す.

感染 PC ならびに被感染 PC は仮想マシン環境を備えており，これらの仮想マシン環境上でネットワークワームの感染を試行させる．モニタ装置は，パケットモニタ機能で感染動作の通信履歴をファイルに記録する．フロー分析機能で記録されたファイル中の通信履歴のフローを分類した後に，Web インタフェース表示機能で HTML ファイルを出力する．また，IP アドレス変換機能は，ネットワークワームがランダムに生成する IP アドレスを感染先として用意したシステムに振り向けることにより効率的な検証を実現する．なお，検証システムのプロトタイプ開発にあたっては，パケットモニタ機能としてコマンドライン型 ethereal, IP アドレス変換機能として Linux の iptables を使用し，フロー分析機能と Web インタフェース向けの表示整形をスクリプト言語 perl で実装した.

(1) IP アドレス変換機能

インターネットにおける IP v4 アドレス空間は 2^{32} = 4,294,967,296 である．このため，ネットワークワームが感染のための探索 IP アドレスをランダムに生成する場合, ネットワークワーム自体がスレッド化などにより同時探索の稼働率をあげたとしても被感染 PC の IP アドレスが選択される確率はきわめて低く，結果として短時間での感染動作検証ができないことは容易に類推できる．被感染 PC のネットワークインタフェースに複数 IP アドレスを割り当てることで選択される確率を上げる方法もあるが，必ずしも被感染 PC に複数 IP アドレスを割り当てる機能があるとは限らない．そこで，中継装置としても機能するモニタ装置に送信先 IP アドレスを被感染 PC の IP アドレスに変換する IP アドレス変換機能を持たせる．また，本機能の実現にあたっては要件 1 を満たすために，Linux の iptables が提供する DNAT (Destination Network Address Translation) [NAT] を使用することとした．

DNAT は送信先 NAT とも呼ばれ，送信先 IP アドレスを特定の IP アドレスに変換する機能である. 主にファイアウォールの内側にあるネットワークサービスをインターネット側から利用できるようにする機能として提供されており, ファイアウォールのローカルサーバ機能あるいは, バーチャルコンピュータ機能とも呼ばれている．プロトタイプシステムでは，図 4.4のように iptables の DNAT を用いた送信先 IP アドレス変換を設定しており，モニタ装置はインタフェース eth0 に届いたすべての感染 PC からのパケットの送信先 IP アドレスを y.y.y.1 に変換した後, 被感染 PC に転送する．

(2) フロー分析機能

フロー分析機能では, 要件 2(b)を満たすために, パケットモニタ機能の記録した通信履歴から次の 2 項目のデータ抽出をおこなう．

- ネットワークワームが感染動作に伴い使用する送信先ポート番号
- 送信先ポート番号の発生系列とその頻度

本検証システムにおいて発生するトラフィックはネットワークワーム感染動作によるトラフィックのみと仮定できる．したがって，先頭パケットの抽出，送信先ポート番号に基づく発生系列の抽出の 2 ステップからフロー分析をおこなうことにより，ネットワークワームが使用する送信先ポート番号の発生系列とその頻度，すなわち，感染動作を概観できることになる．

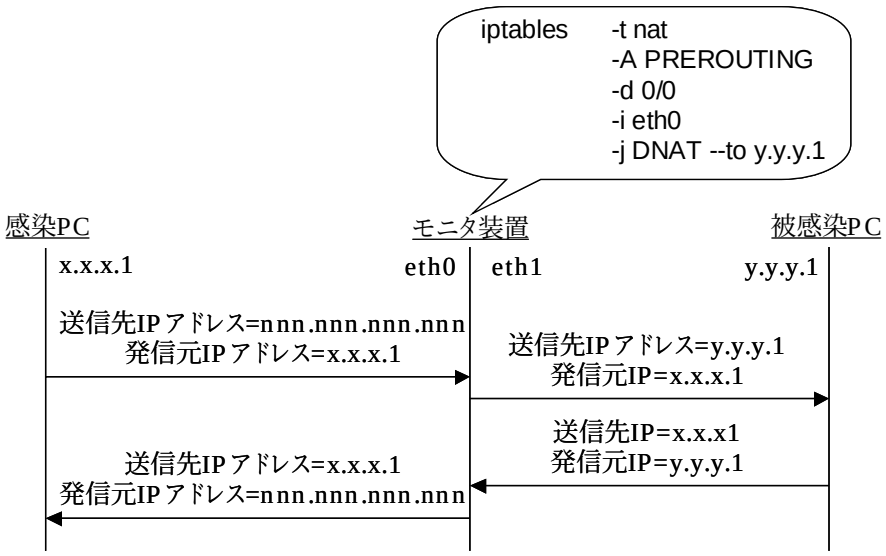


図 4.4：DNAT を用いた送信先 IP アドレスの変換

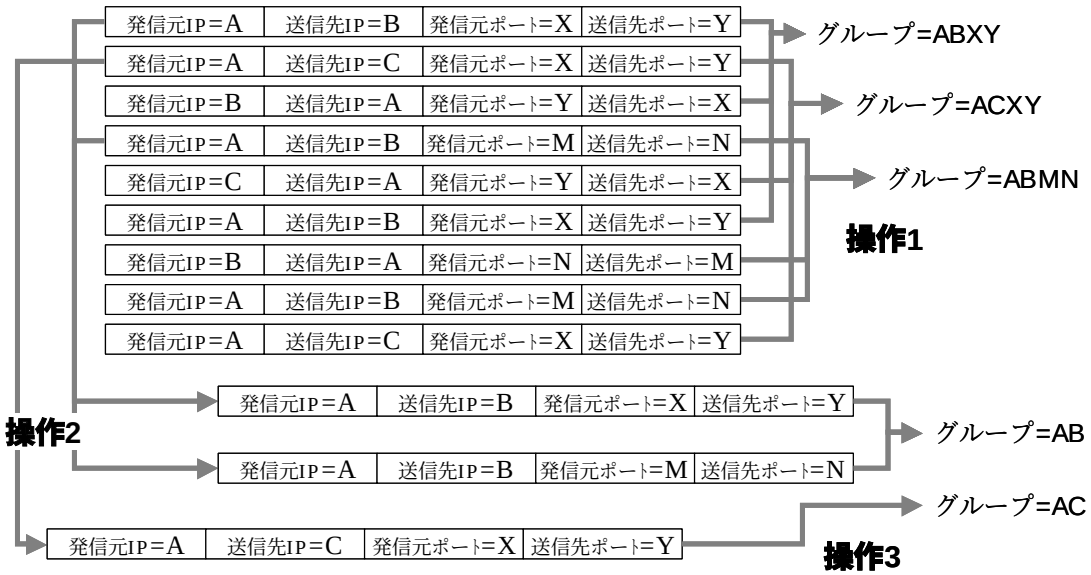
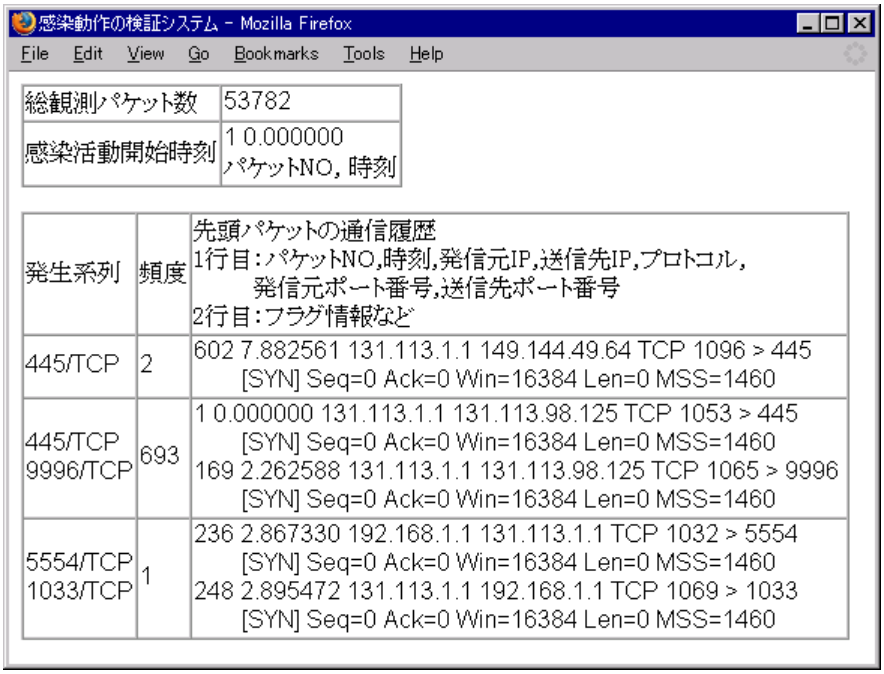


図 4.5：感染動作検証システムにおけるフロー分析手順の概要


感染動作の検証システム - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

総観測パケット数	53782
感染活動開始時刻	1 0.000000 パケットNO, 時刻

発生系列	頻度	先頭パケットの通信履歴 1行目:パケットNO,時刻,発信元IP,送信先IP,プロトコル, 発信元ポート番号,送信先ポート番号 2行目:フラグ情報など
445/TCP	2	602 7.882561 131.113.1.1 149.144.49.64 TCP 1096 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
445/TCP 9996/TCP	693	1 0.000000 131.113.1.1 131.113.98.125 TCP 1053 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 169 2.262588 131.113.1.1 131.113.98.125 TCP 1065 > 9996 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
5554/TCP 1033/TCP	1	236 2.867330 192.168.1.1 131.113.1.1 TCP 1032 > 5554 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 248 2.895472 131.113.1.1 192.168.1.1 TCP 1069 > 1033 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460

図 4.6：フロー分析に基づく送信先ポート番号の発生系列とその頻度の例

(a) 先頭パケットの抽出

通信履歴から発信元／送信先 IP アドレスのペアと発信元／送信先ポート番号のペアの組み合わせによるグループ化をおこなった後 (図 4.5 操作 1)，グループ内での先頭パケットを抽出することで (図 4.5 操作 2)，ネットワークワームが感染動作に使用する送信先ポート番号を特定する．TCP 通信の場合には，通常 SYN フラグの設定されたパケットが抽出対象となる．

(b) 送信先ポート番号の発生系列の抽出

抽出した先頭パケットを発信元／送信先 IP アドレスのペアで再グループ化した後 (図 4.5 操作 3)，グループ内での送信先ポート番号の発生系列を抽出する．たとえば，図 4.5の場合には，発信元 IP アドレス=A，送信先 IP アドレス=B において，送信先ポート番号の発生系列={Y,N}となる．これにより，ある発信元／送信先 IP アドレスのペアにおける送信先ポート番号の発生系列を導き出すことができる．その後，全グループを対象とした送信先ポート番号の発生系列の頻度を算出する．

感染 PC の IP アドレス 131.113.1.1，被感染 PC の IP アドレス 192.168.1.1 として構成した検証システムで確認をおこなった Sasser.C の送信先ポート番号の発生系列と頻度の結果を図 4.6に例示する．

総観測パケット数は，パケットモニタ機能が記録した全通信履歴のエントリ数である．感染活動開始時刻は，最も頻度の高い発生系列で観測された先頭パケットの時刻であり，感染動作に利用するパケットが送出されはじめた時刻に相当する．そして，発生系列は，フロー分析によってグループ化した結果であり，発生頻度と共に先頭パケットの通信履歴を表示する．

この事例では，53,782 件の通信履歴を取得している．そして，Sasser.C の感染動作は，ポート番号 {445/TCP}{445/TCP，9996/TCP}{5554/TCP，1033/TCP} の 3 つの発生系列があり，観測開始から 1 パケット目で感染動作に利用するパケットが 445/TCP 宛に送出されていることになる．さらに，先頭パケットの通信履歴に記載された IP アドレスの発生形態を見ることにより，発生系列の動作の違いを読み取ることができる．この場合，ポート番号 {5554/TCP，1033/TCP} には被感染 PC に付与された IP アドレス 192.168.1.1 が発信元／送信先 IP アドレスとして利用されていることが，ポート番号 {445/TCP}{445/TCP，9996/TCP} の動作とは大きく異なる点となっている．

本検証システムの構成上の特徴は次の通りである．

- 3 台の PC で検証環境を構築できる (要件 1).
- 感染のためにランダムに生成された探索 IP アドレスを効率的に被感染 PC に振り向けることができる (要件 3). 図 4.6の事例では，248 パケット目，約 3 秒で感染動作の最終段階に入っている．なお，IP アドレス変換機能の効果については，4.3節の実験においても示す．

4.3 検証システムを用いた実験

本節では，4.2節にて提示した検証システムを用いて確認した既知のネットワークワームの感染先探索特性と感染動作について述べる．また，ネットワークワーム感染先探索特性の検証システムの通信履歴から得られる探索動作に伴う TCP 再送処理状況を参照することにより，ネットワークワームの探索動作安定性に関する情報を収集できることを示す．

4.3.1　既知ネットワークワームの感染先探索特性

提案するネットワークワーム感染先探索特性の検証システムを用いて, 既知のネットワークワームの感染先探索特性について調査した結果を示す.

(1) 実験環境

実験に使用した環境は次の通りであり, 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いる.

- 感染 PC：Dell PowerEdge1400 (Pentium III, メモリ 256MB) に日本語版 Microsoft Windows 2000 Server Service Pack 4 をインストールした.
- モニタ装置：IBM ThinkPad 2609-93J (Pentium III, メモリ 192MB) に Redhat Linux 7.3 をインストールした.
- ネットワーク：100Mbps の Ethernet スイッチングハブを用意した.
- 感染 PC の仮想マシン環境：メモリゲストサイズ 160MB, 全仮想マシンの総メモリ 176MB を設定した VMware Workstation 上に日本語版 Windows (修正プログラムとサービスパック適用なし) 環境を準備し, Windows 2000 環境で Code Red 3, Nimda.E, Blaster, Slammer, Windows XP Professional 環境で Sasser.B, Sasser.C を確認した.

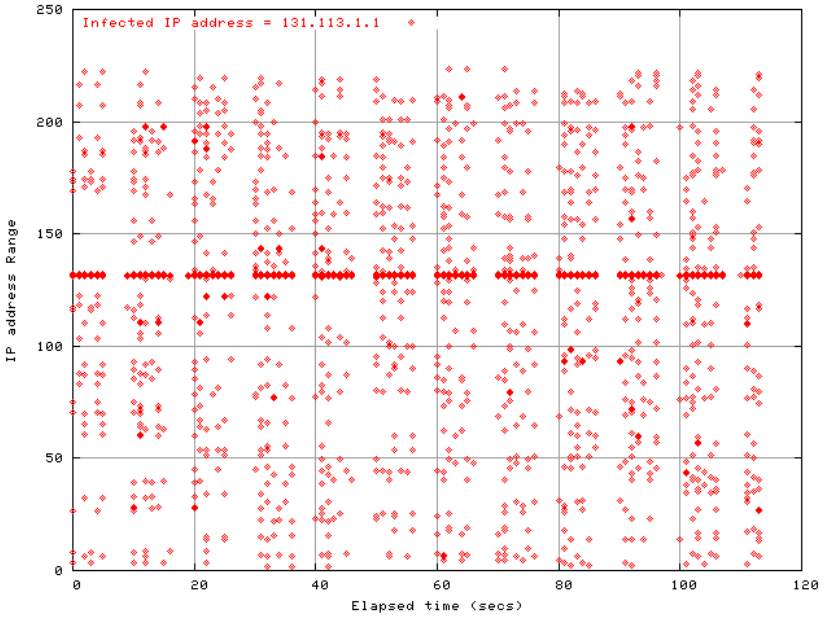
(2) 感染先探索特性

構築した実験環境を用いて調査した Code Red 3, Nimda.E, Blaster, Slammer, Sasser.B, Sasser.C の感染先探索特性の結果を示す.

(a) Code Red 3

Code Red 3 [police03c] は 2003 年 3 月に出現したネットワークワームであり, アドレスブロック探索比率を加味して常に探索 IP アドレスをランダムに選択するタイプ (アドレスブロック探索比率加味型兼ランダム探索型を略す) に属する.

Code Red 3 のコードはそのオリジナルである Code Red II と 2 バイトしか異ならない. この 2 バイトの違いは Code Red II に設定されていた稼動期限 2001 年 9 月末が, 34,952 年 9 月末まで動作するよう変更されたことによる. したがって, Code Red II と Code Red 3 の感染探索特性は同一であり, 本節で確認した特性は Code Red II にも当てはまる.



観測開始から 10,000 パケットを対象にプロット

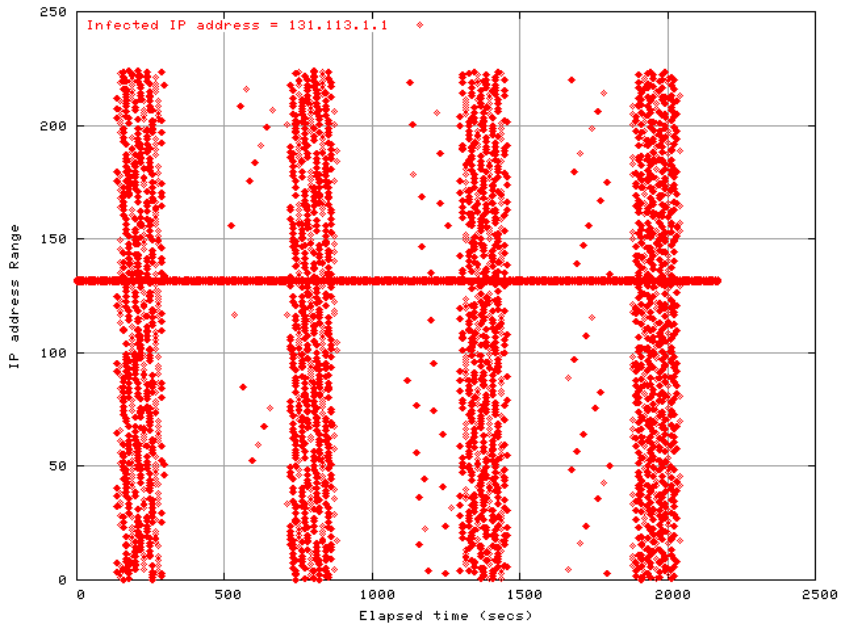
図 4.7：経過時間毎の探索 IP アドレス (Code Red 3)

表 4.2：アドレスブロック探査比率 (Code Red 3)

感染先となる探索 IP アドレス	実験結果	コード解析
上位 2 オクテット同一(同.同.異.異)	37.7%	37.5%
上位 1 オクテット同一(同.異.異.異)	50.8%	50.0%
上記以外(異.異.異.異)	11.5%	12.5%

試行 3 回, 観測開始から 10,000 パケットを対象とした平均値

経過時間毎の探索 IP アドレスの分布を図 4.7に示す．横軸は Code Red 3 感染以降の経過時間，縦軸は送出されたパケットの送信先 IP アドレス範囲 (0.0.0.0～255.255.255.255) である．また，Code Red 3 のアドレスブロック探索比率は表 4.2に示す通りコード解析 [police03c] の結果に沿っていると言える．



観測開始から 51,261 パケットを対象にプロット

図 4.8：経過時間毎の探索 IP アドレス (Nimda.E)

表 4.3：アドレスブロック探索比率 (Nimda.E)

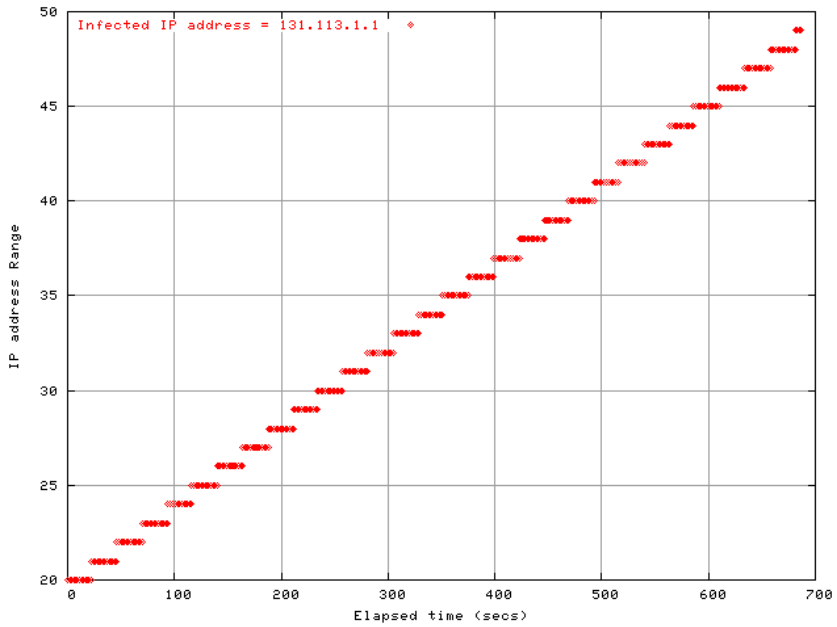
感染先となる探索 IP アドレス	実験結果	コード解析
上位 2 オクテット同一(同.同.異.異)	50.9%	50%
上位 1 オクテット同一(同.異.異.異)	38.8%	25%
上記以外(異.異.異.異)	10.3%	25%

試行 9 回, 観測開始から 10,000 パケットを対象とした平均値

(b) Nimda.E

Nimda.E [IPA01] は 2001 年 10 月に出現したネットワークワームであり，同年 9 月に流布した Nimda の亜種である．Nimda.E も Code Red 3 と同様にアドレスブロック探索比率加味型兼ランダム探索型に属する．

経過時間毎の探索 IP アドレスの分布を図 4.8に示す．縦軸は送出されたパケットの送信先 IP アドレス範囲 (0.0.0.0～255.255.255.255) である．Nimda.E の場合には探索動作に周期性が見られ, サンプリングによっては探索比率に偏りを伴ってしまう．結果として“ 上記以外(異.異.異.異) ”の比率がコード解析 [CERT01c] よりも低い実測値となっていることがわかる(表 4.3).



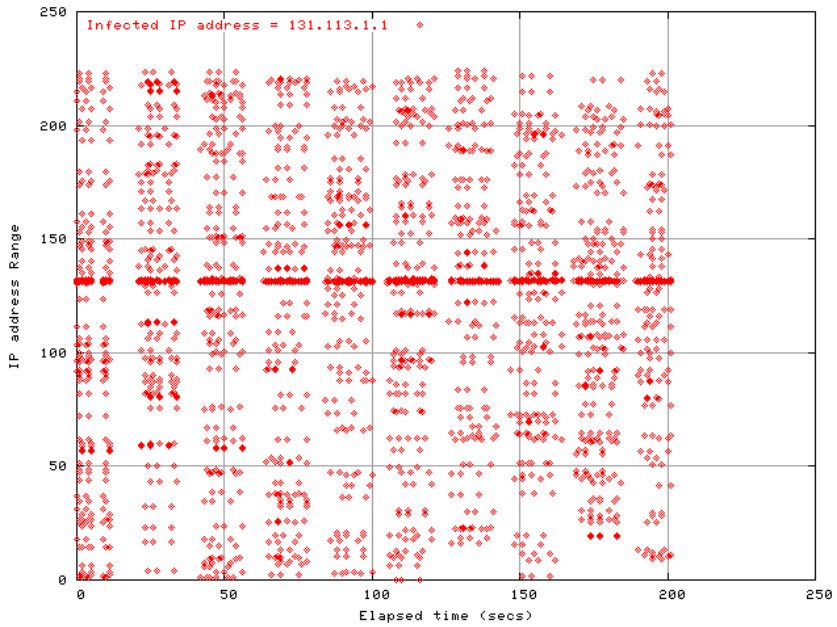
観測開始から 7,500 パケットを対象にプロット

図 4.9：経過時間毎の探索 IP アドレス (Blaster)

(c) Blaster

Blaster [police03b] は，2003 年 8 月に出現したネットワークワームである．アドレスブロック探索比率を加味して探索開始 IP アドレスを決定した後，順次 IP アドレスを加算し探索する方式 (アドレスブロック探索比率加味型兼スイープ型と略す) を使用している．感染先探索特性上，この点が Code Red，Sasser との大きな違いとなっている．

探索範囲に絞った経過時間毎の探索 IP アドレスの分布を図 4.9に示す．縦軸は送出されたパケットの送信先 IP アドレス範囲 153.75.20～153.75.50 を示している．図 4.9の場合，探索開始 IP アドレスとして 153.75.20.1 が選択されており，以降 4 オクテット目が 1 つずつカウントアップしながら感染先を探索していることを示している．なお，探索範囲を絞ったグラフ作成については，実験毎にプログラムのカスタマイズで対処した．



観測開始から 3,757 パケットを対象にプロット

図 4.10：経過時間毎の探索 IP アドレス (Sasser.B)

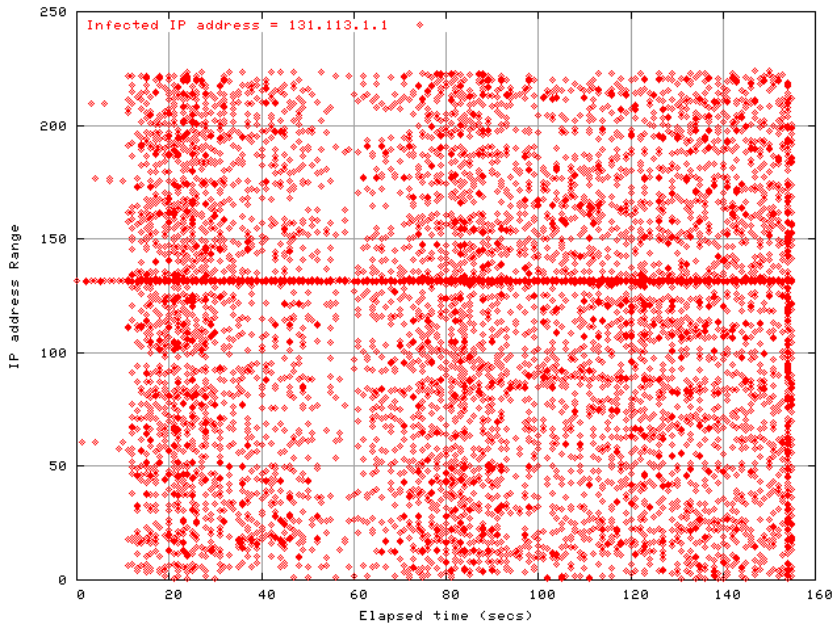
表 4.4：アドレスブロック探索比率 (Sasser.B)

感染先となる探索 IP アドレス	実験結果	コード解析
上位 2 オクテット同一(同.同.異.異)	27.2%	25%
上位 1 オクテット同一(同.異.異.異)	24.6%	23%
上記以外(異.異.異.異)	48.2%	52%

試行 5 回, 観測開始から 3,000 パケットを対象とした平均値

(d) Sasser.B

Sasser.B [IPA05] は 2004 年 5 月に出現したネットワークワームであり，アドレスブロック探索比率加味型兼ランダム探索型に属する．経過時間毎の探索 IP アドレスの分布を図 4.10に示す. 縦軸は送出されたパケットの送信先 IP アドレス範囲 (0.0.0.0～255.255.255.255) である．Sasser.B の場合 “ 上記以外 (異.異.異.異) ” の比率がコード解析結果よりも低い実測値となっている(表 4.4).



観測開始から 13,602 パケットを対象にプロット

図 4.11：経過時間毎の探索 IP アドレス (Sasser.C)

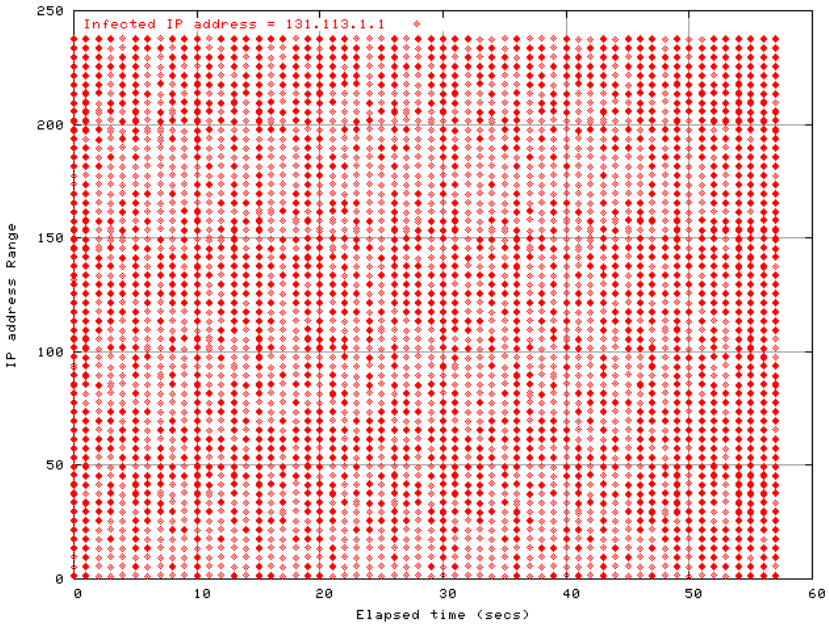
表 4.5：アドレスブロック探索比率 (Sasser.C)

感染先となる探索 IP アドレス	実験結果	コード解析
上位 2 オクテット同一(同.同.異.異)	27.1%	25%
上位 1 オクテット同一(同.異.異.異)	24.8%	23%
上記以外(異.異.異.異)	48.1%	52%

試行 5 回, 観測開始から 10,000 パケットを対象とした平均値

(e) Sasser.C

Sasser.C は 2004 年 5 月に出現したネットワークワームであり, Sasser.B の感染動作で使用するスレッド数 128 に対し, スレッド数 1024 へと拡張されている. 経過時間毎の探索 IP アドレスの分布を図 4.11に示す. 縦軸は送出されたパケットの送信先 IP アドレス範囲 (0.0.0.0〜255.255.255.255) である. Sasser.B と同様に“ 上記以外 (異.異.異.異) ”の比率がコード解析結果よりも低い実測値となっている(表 4.5).



観測開始から 10,000 パケットを対象にプロット

図 4.12：経過時間毎の探索 IP アドレス(Slammer)

(f) Slammer

Slammer [police03a] は，2003 年 1 月末に流布したネットワークワームである．コード解析 [police03a] によれば，GetTickCount 関数の結果をシードとして探索 IP アドレスを生成し，アドレスブロック探索比率を加味せず常に探索 IP アドレスをランダムに選択するタイプ (ランダム探索型と略す) に属する．また，UDP を利用した流布が特徴であり，この点が TCP を利用して流布した Code Red，Nimda，Sasser と大きく異なる．

経過時間毎の探索 IP アドレスの分布を図 4.12に示す．縦軸は送出されたパケットの送信先 IP アドレス範囲 (0.0.0.0〜255.255.255.255) である．確認の範囲において探索 IP アドレス生成に規則性は見られないが，探索対象となる IP アドレスブロックと外れてしまうブロックがある．すなわち，単一の感染 PC だけをみると，探索対象となる IP アドレスブロックには偏りが発生している．

4.3.2 既知ネットワークワームの探索動作における TCP 再送処理

ネットワークワーム感染先探索特性の検証システムで収集した通信履歴からは, ネットワークワームの感染先探索範囲に関する動作情報だけではなく, ネットワークワームの探索動作安定性に関する情報を収集できる．本節では，ネットワークワーム感染先探索特性の検証システムで取得した4.3.1節の通信履歴を用いて，既知ネットワークワームの探索動作における TCP 再送処理状況を示す．次に，TCP 再送処理状況から推定できる探索動作安定性について述べる．

(1) 実験環境

Code Red 3，Nimda.E，Blaster については4.3.1節で述べた Windows 2000 環境下で取得した通信履歴を使用した．また，Sasser.B，Sasser.C については4.3.1節で述べた Windows XP Professional 環境下で取得した通信履歴と，日本語版 Windows 2000 環境で新たに取得した通信履歴を使用した．

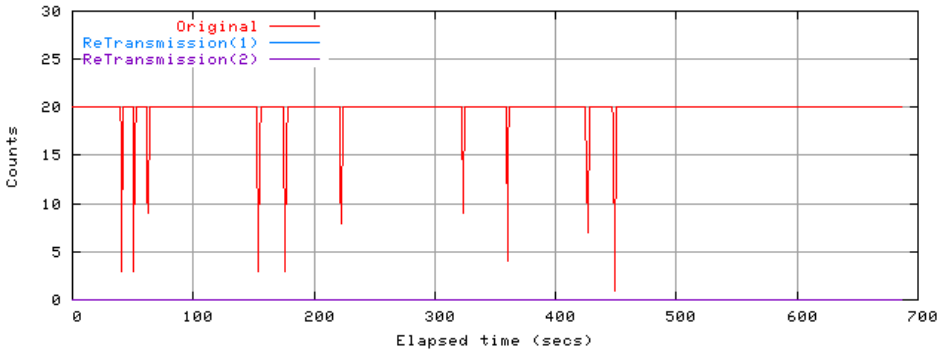
(2) 探索動作における TCP 再送処理

ネットワークワーム感染先探索特性の検証システムにおいて，感染先 IP アドレスとしてモニタ装置以外の IP アドレスが選択された場合，感染 PC から送出されたパケットはすべて廃棄される．このため，TCP を用いて感染活動をおこなうネットワークワームである Code Red，Nimda.E，Blaster，Sasser.B，Sasser.C の場合には，TCP SYN パケットの再送処理が発生することになる[iv]．そこで，ネットワークワーム感染先探索特性の検証システムで収集した通信履歴から経過時間毎の TCP SYN パケットの送信数を抽出し，探索動作に伴う TCP 再送処理状況を把握する．

図 4.13から図 4.17からに，通信履歴から TCP SYN パケットの送信数を抽出して経過時間毎にプロットしたグラフを示す．Blaster のコード解析 [eEye03] によれば，Blaster は 20 個の TCP コネクションの確立操作後，1.8 秒間スリープした時点でソケットの状態確認をおこない，TCP コネクションが利用できない場合には解放操作に入る．図 4.13の TCP パケット送信数からも Blaster が TCP SYN パケット再送抑止をおこない，安定したパケット送信動作をおこなっていることがわかる．

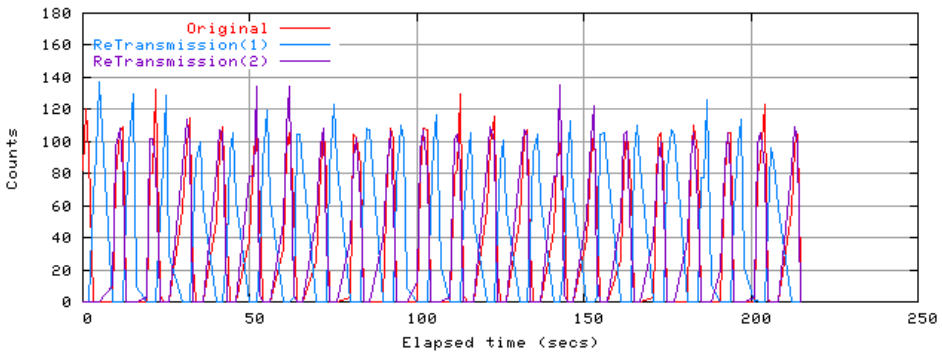
---

iv) Windows 2000 ならびに Windows XP の場合，通常，再送タイムアウトの 1 回目が約 3 秒，2 回目はその倍の約 6 秒となっている．



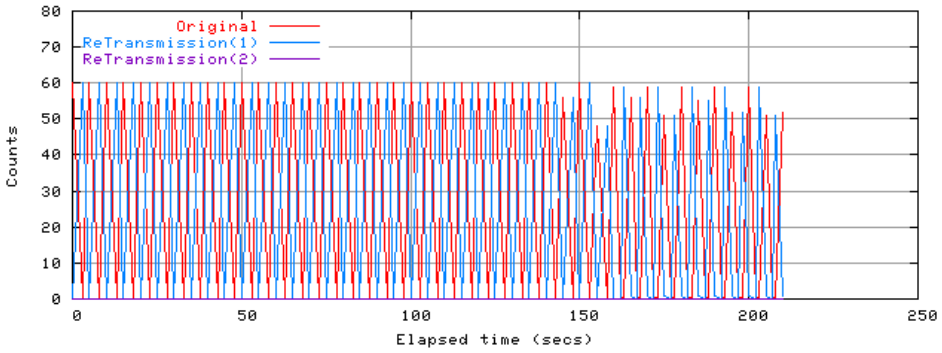
観測開始から 7,500 パケットを対象にプロット

図 4.13：経過時間毎の TCP パケット送信数 (Blaster)



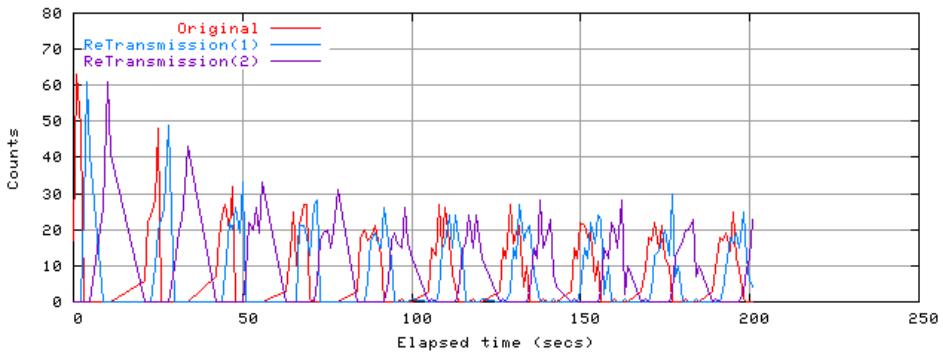
観測開始から 10,000 パケットを対象にプロット

図 4.14：経過時間毎の TCP パケット送信数 (Code Red 3)



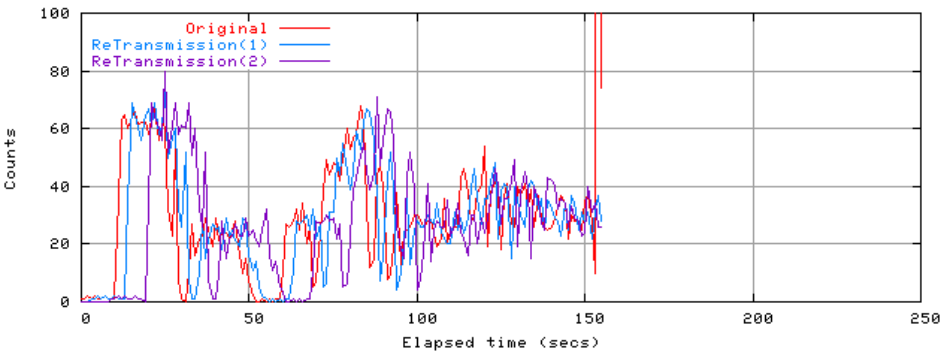
観測開始から 10,000 パケットを対象にプロット

図 4.15：経過時間毎の TCP パケット送信数 (Nimda.E)



観測開始から 3,757 パケットを対象にプロット

図 4.16：日本語版 Windows XP 環境での TCP パケット送信数 (Sasser.B)

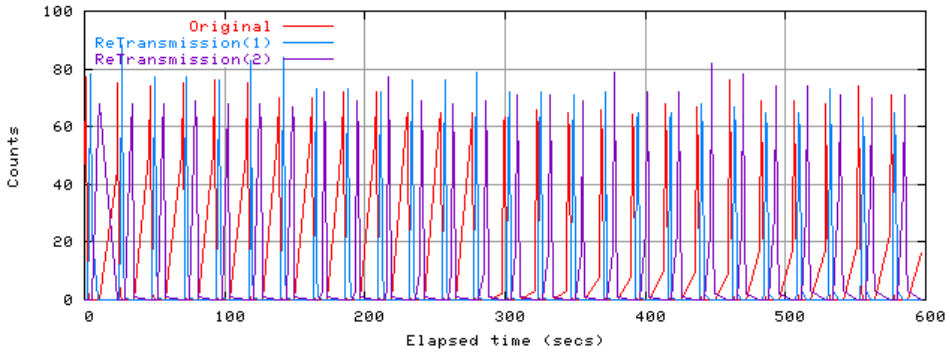


観測開始から 13,602 パケットを対象にプロット

図 4.17：日本語版 Windows XP 環境での TCP パケット送信数 (Sasser.C)

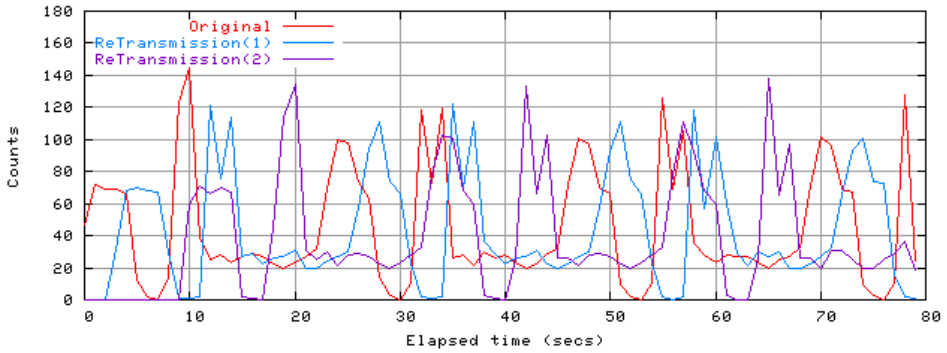
また，Code Red 3 (図 4.14)，Nimda.E (図 4.15) の場合，Sasser (図 4.16，図 4.17) に比べ探索に伴う TCP SYN パケット送信数の変動が安定しており，同じ Sasser でも感染動作で使用するスレッド数 128 の Sasser.B (図 4.16) の方がスレッド数 1028 の Sasser.C (図 4.17) よりもパケット送信が安定性していると判断できる．

コード解析によれば，日本語環境において Sasser がネットワーク経由で再感染対象とする OS は日本語版 Windows XP のみであった．図 4.18 と図 4.19 に Sasser.B，Sasser.C を日本語版 Windows 2000 上で実行した場合の経過時間毎の TCP パケット送信数を示す．日本語版 Windows 2000 環境では，Sasser 実行時も“システムのシャットダウン”を示す警告ダイアログが挙がることはなく，特に，Sasser.B の場合には探索に伴うパケット送信数の変動が安定していることがわかる．



観測開始から 10,000 パケットを対象にプロット

図 4.18：日本語版 Windows 2000 環境での TCP パケット送信数 (Sasser.B)



観測開始から 10,000 パケットを対象にプロット

図 4.19：日本語版 Windows 2000 環境での TCP パケット送信数 (Sasser.C)

さらに，Sasser のスレッド数の拡張は，日本語版 Windows XP 環境と同様にパケット送信の安定性を欠く要因となっていると言える．再感染対象ではない環境での動作確認は，感染拡大の可能性を予測する上で有益な情報を得ることができると考えられる．

4.3.3 既知ネットワークワームの感染動作

提案するネットワークワーム感染動作の検証システムを用いて, 既知のネットワークワームの感染動作について調査した結果を示す.

(1) 実験環境

実験に使用した感染 PC，モニタ装置とネットワーク環境は4.3.1節と同一であり, ネットワークワーム感染動作の検証システムで新たに用いた機器は, 次の通りである.

- 被感染 PC：HITACHI FLORA (Pentium 4，メモリ 1GB) に Microsoft Windows XP Professional Service Pack 1 をインストールした.
- 被感染 PC の仮想マシン環境：メモリゲストサイズ 512MB，全仮想マシンの総メモリ 528MB を設定した VMware Workstation 上に日本語版 Windows (修正プログラムとサービスパック適用なし) 環境を準備し，Windows XP Professional 環境で Blaster，Welchia，Sasser.B を確認した.

なお，本検証システムにおいて，感染 PC の IP アドレスは 131.113.1.1，被感染 PC の IP アドレスは 192.168.1.1 として構成した.

(2) 感染動作

(a) Blaster

Blaster の送信先ポート番号の発生系列と頻度の結果を表 4.6に例示する．この事例では，総観測パケット数は 3,317 件である．Blaster の感染動作は，ポート番号 135/TCP，4444/TCP の順に発生する通信と，ポート番号 69/UDP に対する通信の 2 段階に分かれている．125 パケット目の発信元 IP アドレスが被感染 PC に付与された IP アドレス＝192.168.1.1 であることから，感染を実行するために送出されたパケットであると想定でき, 約 4.5 秒で感染動作の最終段階に入っていることがわかる．なお，この感染動作シーケンスはコード解析の結果に合致している.

表 4.6：フロー分析に基づく送信先ポート番号の発生系列 (Blaster)

発生系列	頻度	先頭パケットの通信履歴
135/TCP	540	パケット No 3 観測時刻 0.000000 131.113.1.1 > 115.11.58.1 TCP 1032 > 135 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
135/TCP 4444/TCP	2	パケット No 7 観測時刻 0.005741 131.113.1.1 > 115.11.58.5 TCP 1036 > 135 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 パケット No 103 観測時刻 2.276719 131.113.1.1 > 115.11.58.5 TCP 1052 > 4444 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
69/UDP	1	パケット No 125 観測時刻 4.517823 192.168.1.1 > 131.113.1.1 UDP Source port: 1031 Destination port: 69

(b) Welchia

Welchia (Nachi) の場合, 今回実装したプロトタイプシステムのデフォルト設定では感染動作を検証することはできなかった．これは，感染 PC に DNS の設定がされていない場合には感染動作を継続しないことと，感染開始の際に DNS を利用して microsoft.com ドメインの存在を確認し，同ドメインの存在を確認できない場合には感染動作を継続しないことに起因している．このため，個別に検証環境を調整することで動作確認を実施した．

表 4.7：フロー分析に基づく送信先ポート番号の発生系列 (Welchia)

発生系列	頻度	先頭パケットの通信履歴
53/UDP	1	パケット No 1 観測時刻 -4.080282 131.113.1.1 > 144.144.144.144 UDP Source port: 1031 Destination port: 53
ICMP 135/TCP	4434	パケット No 3 観測時刻 0.000000 131.113.1.1 > 131.113.0.0 ICMP Echo (ping) request
		パケット No 5 観測時刻 0.007983 131.113.1.1 > 131.113.0.0 TCP 1032 > 135 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
707/TCP 69/UDP	1	パケット No 29 観測時刻 0.050722 192.168.1.1 > 131.113.1.1 TCP 3011 > 707 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
		パケット No 2618 観測時刻 3.345150 192.168.1.1 > 131.113.1.1 UDP Source port: 3060 Destination port: 69

Welchia の送信先ポート番号の発生系列と頻度を表 4.7に例示する. この事例では，総観測パケット数は 77,448 件である．Welchia の感染動作は，ポート番号 53/UDP への通信にはじまり，ICMP，ポート番号 135/TCP の順に発生する通信と，ポート番号 707/TCP，69/UDP に対する通信の 3 段階に分かれている．29 ならびに 2618 パケット目の発信元 IP アドレスが被感染 PC に付与された IP アドレス 192.168.1.1 であることから，感染を実行するために送出されたパケットであると想定でき，2618 パケット目，約 3.3 秒で感染動作の最終段階に入っていることがわかる. なお, この感染動作シーケンスはコード解析の結果に合致している.

表 4.8：フロー分析に基づく送信先ポート番号の発生系列 (Sasser.B)

発生系列	頻度	先頭パケットの通信履歴
445/TCP	1254	パケット No 9 観測時刻 0.000000 131.113.1.1 > 131.113.202.138 TCP 1054 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
445/TCP 9996/TCP	586	パケット No 10 観測時刻 0.003998 131.113.1.1 > 131.225.169.253 TCP 1055 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 パケット No 231 観測時刻 2.748501 131.113.1.1 > 131.225.169.253 TCP 1075 > 9996 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
5554/TCP 1033/TCP	1	パケット No 353 観測時刻 4.024249 192.168.1.1 > 131.113.1.1 TCP 1032 > 5554 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 パケット No 367 観測時刻 4.135242 131.113.1.1 > 192.168.1.1 TCP 1084 > 1033 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460

(c) Sasser.B

Sasser.B の送信先ポート番号の発生系列と頻度を表 4.8に例示する．この事例では，総観測パケット数は 44,509 件である．Sasser.B の感染動作は，ポート番号 445/TCP，9996/TCP の順に発生する通信と，ポート番号 5554/TCP, 1033/TCP の順に発生する通信の 2 段階に分かれており, 367 パケット目, 約 4.1 秒で感染動作の最終段階に入っている．後者のポート番号系列では，発信元／送信先 IP アドレスとして被感染 PC に付与された IP アドレス 192.168.1.1 が使用されていることから，Sasser.C の結果同様 (図 4.6)，感染を実行するために送出されたパケットであると想定できる．なお，この感染動作シーケンスはコード解析の結果に合致している．ただし，367 パケット目のポート番号 1033/TCP へのアク

セスは, 感染 PC から被感染 PC への FTP のデータコネクションであり, ポート番号は固定した値を取るわけではないことがコード解析結果として報告されている.

(3) 実験結果のまとめ

(a) IP アドレスの発生分布に関する実験成果

要件 2(a)の感染のひろがりに関わる情報の収集に関して, 本検証システムを用いた実験の成果を示す.

- アドレスブロックの探索比率の偏り

  Sasser.B，Sasser.C については，“上記以外 (異.異.異.異)”の IP アドレス発生比率がコード解析よりも 4%ほど低い実測値となっており，アドレスブロックの探索比率に偏りがみられることを示した．この結果は，Sasser に感染した PC は, 上位 1 オクテットならびに上位 2 オクテットが同一のネットワークを探索する比率がコード解析結果よりも高くなるために, イントラネットへの流布拡大の影響が多少なりとも増加する可能性があることを意味している.

- 探索動作の周期性

  Nimda.E については，アドレスブロックの探索比率だけでは表現することのできない探索動作として周期性のあることを示した.

- 探索動作の視覚化

  今回実験をおこなったネットワークワームについては，探索 IP アドレスの発生分布を経過時間毎の視点から視覚化することにより, 探索動作の差異を示した．また，対象としたネットワークワームの感染先の探索動作は，アドレスブロック探索比率の加味と探索形態を用いて分類できる (図 4.20)．この分類は，探索動作の差異を明確化にするだけではなく，新たにネットワークワームが発生した場合に, 既存種との対応付けによる影響想定を検討する上で有効であると考える.

- TCP 再送処理と探索動作の安定性

  ネットワークワーム感染先探索特性の検証システムで収集した通信履歴から経過時間毎の TCP SYN パケットの送信数を抽出することにより，探索動作の安定性に関する情報を得ることができることを示した．また，探索動作に伴う TCP SYN パケット送信数の変動は，ネットワークワームの探索動作安定性の実装レベルを判断する指標のひとつになることを示した.

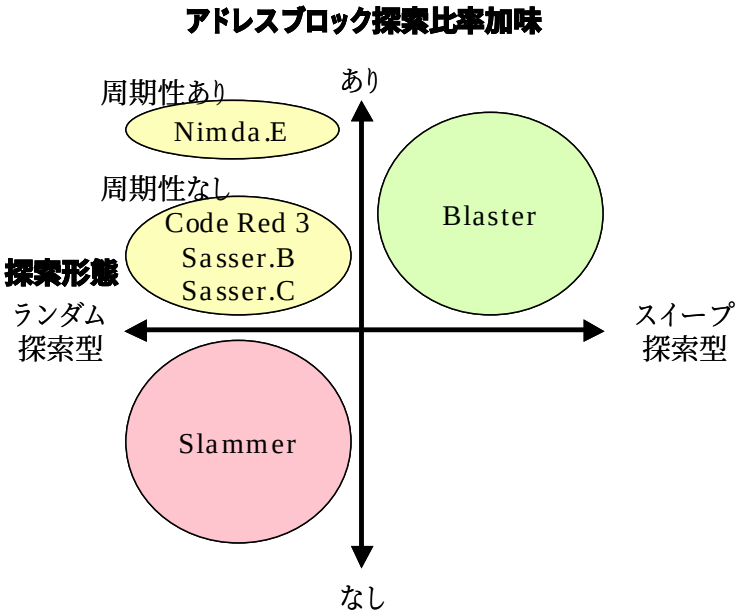


図 4.20：感染先探索特性の分類

(b) 感染動作に関する実験成果

要件 2(b)の感染の通信動作に関わる情報の収集に関して, 検証システムを用いた実験の成果を示す.

- 送信先ポート番号の発生系列と頻度に基づくフロー分析

  送信先ポート番号の発生系列と頻度により, コード解析の結果に合致した感染動作シーケンスを抽出できることを示した. また, 抽出した送信先ポート番号の発生系列を用いて, ネットワークワームが感染に使用するポート番号のトラフィックを止めることにより, 流布拡大を抑止できる.
- IP アドレス変換機能による効率的な検証

  IP アドレス変換機能を利用することにより, 数秒で感染動作の最終段階まで検証可能であることを示した.
- 本検証システムの限界と可能性

  Slammer のように別途 SQL サーバプログラムをインストールし稼動させる必要のあるネットワークワームの場合, 今回実装したプロトタイプシステムでは部分的な感染動作の確認だけに留まってしまう. また, Welchia のような複雑な感染動作をとるネットワークワームの場合には, プロトタイプシステムのデフォルト設定では感染動作を検証することはできなかった. ただし, すでに Welchia に感染した PC を本検証システムに接続した検証形態の場合には,

個別に感染動作環境を調整したのと同様な結果が得られた．このことから，検証の形態によっては感染動作の確認可能な対象を広げることができる．

4.4 まとめ

本章では, 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，特に，各組織単独で実施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した. 提案システムは，ネットワークワームが生成する感染先となる探索 IP アドレスに関する情報の収集を目的としたネットワークワーム感染先探索特性の検証システムと, 感染動作に伴い使用する送信先ポート番号に関する情報の収集を目的としたネットワークワーム感染動作の検証システムから構成される.

次に, 提案方式に基づき実装したプロトタイプシステムを用いて代表的なネットワークワームの感染先探索特性と感染動作を確認した. ネットワークワーム感染先探索特性の検証システムでは，ネットワークワームが生成する感染先となる探索 IP アドレスに関する情報だけではなく，TCP 再送処理状況から探索動作安定性についての情報が得られることを示した．また，ネットワークワーム感染動作の検証システムでは，IP アドレス変換機能により数秒で感染動作の最終段階まで検証可能であること, フロー分析機能による送信先ポート番号の発生系列と頻度の抽出からコード解析の結果に合致した感染動作シーケンスを導くことができることを示した.

検証システムを用いて感染動作を確認するためには，被感染 PC がネットワークワームの感染動作に呼応する必要があるため, 必ずしも動作全体をトレースできない場合もある．このような利用上の制限はあるものの，実装したプロトタイプシステムを用いた実験を通して，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に利用できることを確認した.

第5章　ネットワークワーム流布対策システム

本章では, 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という 3 つ目の課題を解決するために, HTTP (80/TCP) ポートを攻略するネットワークワーム流布時のイントラネット向け回避システムとして, 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ネットワークワーム流布対策システム Web マッパを提案する.

5.1　まえがき

イントラネットでの HTTP ポートを攻略するネットワークワーム流布時の対策に対象を絞り，ネットワークワームの流布を抑止する対策と Web サーバの稼動継続性を確保する対策とを合わせて提供することを目的とした機構 Web マッパ (Web mapper：Web ポート／ホストマッピングシステム) を提案する.

提案方式は, Web サーバ上のポート切替コンポーネントが Web サーバの HTTP ポートを任意の代替ポート番号に切り替えることでネットワークワームの流布を抑止する. 次に，プロキシサーバ上のポート／ホスト変換コンポーネントが Web サーバの HTTP ポートを代替ポート番号へ切り替えたことによる URL 変更を隠蔽することで Web サーバの稼動継続性を確保する HTTP ポート対応の Web ポート／ホストマッピング方式である．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.

本章の構成について述べる．5.2節では HTTP ポート対応の Web ポート／ホストマッピングの実現方式を記述した後, 5.3節で実装したシステムの評価を示す．5.4節はまとめである.

5.2 Web マッパ

本節では，Code Red, Nimda などの HTTP ポートを攻略するネットワークワーム流布時に，ネットワークワームによるトラフィック増加の抑止と Web サーバの継続性を確保するための HTTP ポート対応の Web ポート／ホストマッピングシステム (Web マッパと略す) について述べる．

5.2.1 Web ポート／ホストマッピング方式

(1) 課題解決のアプローチ

2.3.3節の課題を解決するために，対象とするネットワークワームが，“ポート番号 80/TCP に対して直接 TCP コネクションを確立した後，Web サーバの脆弱性を攻略する”という特徴に着目し，次に示す方法で解決を図る．

- ネットワークワームの流布を抑止する．

  ネットワークワームが攻略対象としている Web サーバの HTTP ポート (80/TCP) へのトラフィックをルータやファイアウォールで遮断するか，Web サーバの HTTP ポートを TCP ポート番号 80 以外の任意の代替ポート番号 (たとえば，9999/TCP) に切り替える．この対策により，ネットワークワームは Web サーバの TCP ポート番号 80 に対して TCP コネクションを確立することができず，結果として感染活動を阻止できることになる．
- Web サーバの稼動継続性を確保する．

  ネットワークワームが攻略対象としている Web サーバの HTTP ポート (80/TCP) を代替ポート番号 (9999/TCP) を用いて稼動させることで，ネットワークワームの攻撃を回避しながら Web サーバがサービスを継続して提供できることになる．

  さらに，Web サーバの HTTP ポートが代替ポート番号に切り替わったことに伴う影響を最小限に留めるために，中継経路上にあるプロキシサーバにおいて，HTTP 標準ポート番号 (80/TCP) へのアクセスを代替ポート番号 (9999/TCP) へのアクセスに振り替える URL マッピング操作を実施する．この URL マッピング操作は，Web サーバの稼動継続性を提供する上で，ポート番号の変更をユーザに意識させないようにするための対策となる．

(2) Web マッパ適用にあたっての前提条件

課題解決のアプローチを情報システムに適用するにあたっては, いくつかの前提条件を想定する必要がある．そこで，本提案方式では，次に示す条件を前提とする．

- Web マッパの適用にあたってはネットワーク構成変更を伴うため，イントラネットなどの組織内ネットワークを対象とする．
- HTTP ポートを攻略するネットワークワームは，Web サーバの HTTP 標準ポート番号 80/TCP に直接 TCP コネクションを確立して攻撃を仕掛ける Code Red, Nimda タイプのネットワークワームを想定する．
- Web ブラウザからの Web アクセスは, すべてプロキシサーバ経由とする. なお, プロキシサーバを攻略するネットワークワームについては, 本提案方式の適用対象外とする．
- HTTP ポートを任意のポート番号に切り替えることを想定する．イントラネットの場合には，HTTP ポートとして非標準ポート番号 (たとえば，7777/TCP) を用いた Web サーバを事前に構成することで，HTTP 標準ポート番号 80/TCP に直接 TCP コネクションを確立して攻撃を仕掛けるネットワークワームを回避できる．しかし，この場合には，ポート番号が固定されてしまうために，HTTP ポートに割り当てたポート番号 (7777/TCP) に対して新たな攻撃が発生した場合には回避できないことになり, 被害発生を想定したシステム構築の実現としては十分な機能を備えているとは言えない．

5.2.2　Web マッパのコンポーネント

Web マッパは，課題解決のアプローチで示した方法を組み合わせることにより，HTTP ポートを攻略するネットワークワーム流布を回避するためのシステムであり, 次の 4 つのコンポーネントから構成する (図 5.1).

(1) ポートフィルタリングコンポーネント

HTTP ポートを攻略するネットワークワームが流布した際に，Web サーバのネットワークサービスを提供しているポート番号 (80/TCP) へのトラフィックをフィルタリングする．フィルタリングにあたっては，既存ネットワーク機器であるルータ，ファイアウォールを用いることを想定している．

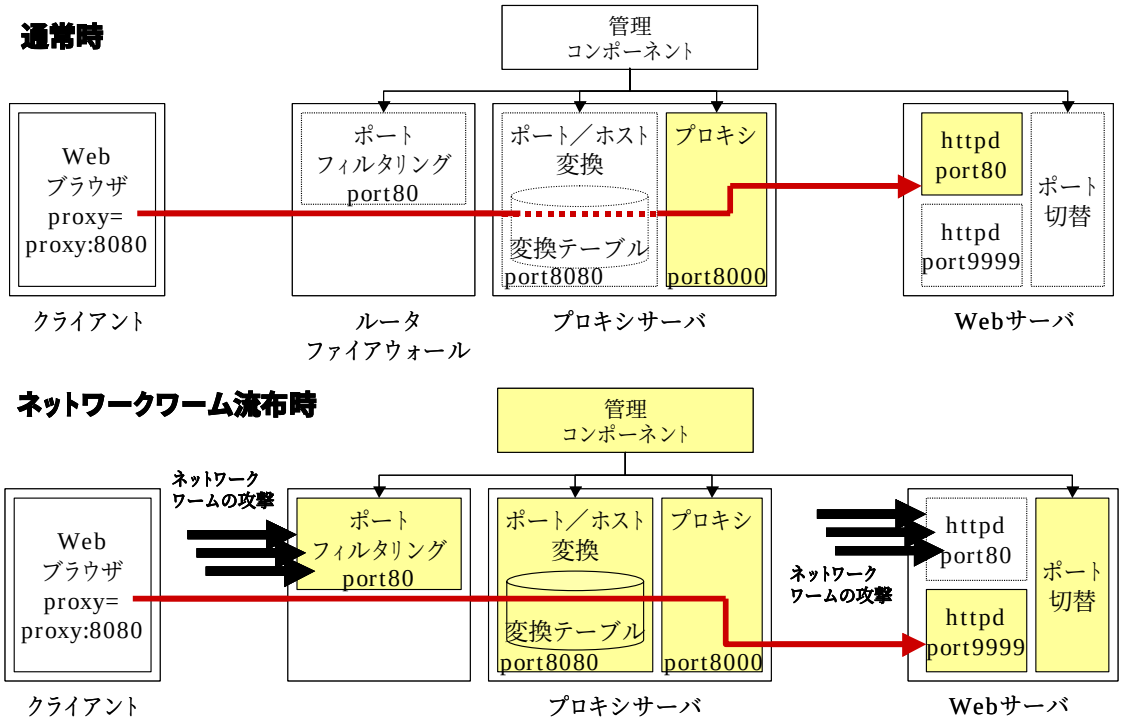


図 5.1：Web ポート／ホストマッピングシステム

(2) ポート切替コンポーネント

ネットワークワームが攻略対象としている Web サーバを任意の代替ポート番号 (たとえば，9999/TCP) を用いて提供するためにポート番号切り替えをおこなう．Web サーバのネットワークサービスを代替ポート番号に切り替える方法は，ネットワークワームが攻略しようとしているポート番号 (80/TCP) でのネットワークサービスを停止し，さらに代替ポート番号 (9999/TCP) でネットワークサービスを提供することになるため，ワームの流布の抑止と Web サーバの稼動継続性確保の双方に有効である．

(3) ポート／ホスト変換コンポーネント

Web サーバが任意の代替ポート番号に切り替わったことをユーザに意識させないようにするために，既存ポート番号 (80/TCP) へのアクセスを代替ポート番号 (9999/TCP) へのアクセスに振り替える URL マッピング操作をおこなう．

(4) 管理コンポーネント

上記 3 コンポーネントに対して，フィルタリング，ポート切替，URL マッピングの変更指示を出す．管理者によるマニュアル操作や IDS との連動を想定している．次に，Web マッパを介した場合の Web ブラウザから Web サーバまでのアクセス経路概要を図 5.2に示す．

(a) Web ブラウザ ⇒ プロキシサーバ

Web ブラウザからのアクセスは，すべてプロキシサーバ経由である．そして，プロキシサーバのポート番号 8080/TCP に対して，ユーザの入力した URL を HTTP 要求 (例：GET http://AAA/index.html) として送信する．

(b) プロキシサーバ

プロキシサーバ上のポート／ホスト変換コンポーネントでは，HTTP 要求を定義ファイル (ポート／ホスト変換テーブル) に従い URL 書き換え操作 (URL マッピング操作) をおこなった後，プロキシコンポーネントに HTTP 要求 (例：GET http://AAA:9999/index.html) を転送する．図 5.2の場合には，“LABEL-fromto AAA　AAA:9999”により，ホスト名称＝AAA がホスト名称：ポート番号＝AAA:9999 に書き換えがおこなわれる．

(c) プロキシサーバ ⇒ Web サーバ

プロキシコンポーネントでは，書き換えのおこなわれた後の HTTP 要求 (例：GET http://AAA:9999/index.html) に従い，Web サーバのポート番号 9999/TCP に対して HTTP 要求を送信する．

このように，Web マッパの基本的な仕組みは，プロキシサーバ上のポート／ホスト変換コンポーネントと Web サーバ上のポート切替コンポーネントが連動して HTTP のポート番号 (80/TCP) を任意の代替ポート番号 (9999/TCP) に切り替えることにより，ネットワークワームの流布を抑止し，Web サーバの稼動継続性を確保する．さらに，プロキシサーバ上のポート／ホスト変換コンポーネントを利用して，代替ポート番号 (9999/TCP) への切り替えに伴う URL 変更の隠蔽をおこない，ユーザに対して既存 Web サーバの稼動環境の提供を維持する．

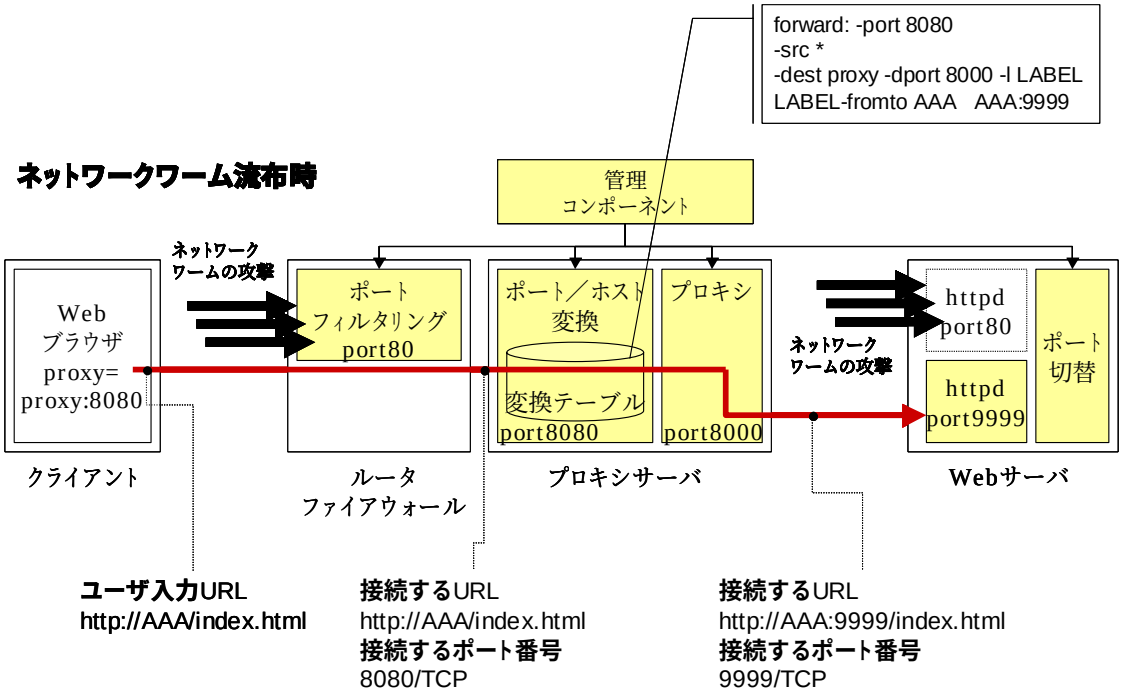


図 5.2：Web マッパ適用時のアクセス経路

5.2.3 実現方式

Web マッパを構成する 4 つのコンポーネントのうち，新たに実装が必要となるポート切替コンポーネント，ポート／ホスト変換コンポーネントならびに，管理コンポーネントの実現方式について述べる．

(1) ポート切替コンポーネント

ポート切替コンポーネントについては, Microsoft IIS [MSb] Web サーバ用としてポート番号を設定する VB (Visual Basic) スクリプト (図 5.4) を作成し，Apache [Apache] Web サーバ用として通常時とワーム流布時の 2 種類のポート定義ファイル (図 5.3) とこれら定義ファイルを切り替えるためのスクリプトを作成した．

(2) ポート／ホスト変換コンポーネント

ポート／ホスト変換コンポーネントは URL の書き換え機能であり，次に示す機能を持つネットワークデーモン hwmapd として開発をおこなった．

```
# Listen: Allows you to bind Apache to specific IP addresses
# and/or ports, in addition to the default. See also the
# <VirtualHost> directive. Change this to Listen on specific IP
# addresses as shown below to prevent Apache from glomming
# onto all bound IP addresses (0.0.0.0)
Listen 80


# Listen: Allows you to bind Apache to specific IP addresses
# and/or ports, in addition to the default. See also the
# <VirtualHost> directive. Change this to Listen on specific IP
# addresses as shown below to prevent Apache from glomming
# onto all bound IP addresses (0.0.0.0)
Listen 9999
```

上段：通常時　下段：ワーム流布時

図 5.3：ポート切り替え用 Apache サーバの定義ファイル (一部)

```
' Move IIS Server PORT from 80 to 9999
Dim IIsServerNum
Dim IIsObjectPath
Dim IIsObject
Dim IIsSchemaObject
Dim IIsPort
IIsServerNum      = 2
IIsPort           = ":9999:"
IIsObjectPath = "IIS://LocalHost/W3SVC/" & IIsServerNum
Set IIsObject = GetObject(IIsObjectPath)
Set IIsSchemaObject ¥
        = GetObject("IIS://LocalHost/Schema/ServerBindings")
IIsObject.Put "ServerBindings", IIsPort
IIsObject.Setinfol
```

図 5.4：Microsoft IIS Web サーバ用のポート切り替え指示スクリプト

(a) ポート／ホストマッピング機能

Web ブラウザから受信した HTTP／HTTPS 要求については，表 5.1に示す定義ファイルに従いポート番号ならびに，ホスト名称の書き換えをおこなう．具体的には，HTTP 要求ヘッダのメソッド行と Host 行が定義ファイルに指定された“変換前ホスト名称：変換前ポート番号”に合致する場合，“変換後ホスト名称：変換後ポート番号”に変換した後，転送をおこなう (図 5.5上段).

表 5.1：ポート／ホスト変換コンポーネント hwmapd の定義ファイル

# 書き換えをおこなうホスト名称とポート番号を指定		
forward:	転送ラベル	
-port	待ちポート番号	
-src	HTTP 用の定義	発信元 IP アドレス(アクセス制御用)
-dest		転送先サーバ IP アドレス
-dport		転送先サーバのポート番号
-ssrc	HTTPS 用の定義	発信元 IP アドレス(アクセス制御用)
-sdest		転送先サーバ IP アドレス
-sdport		転送先サーバのポート番号
-l	マッピングルールラベル	
#マッピングルールラベル		
-fromto	変換前 IP アドレス／ホスト名称:ポート番号	
-sfromto	変換後 IP アドレス／ホスト名称:ポート番号	
# 定義ファイル例		
forward: -port 8080 -src * -dest proxy -dport 8080 -ssrc * -sdest proxy -sdport 8080 -l LBL LBL-fromto tomato.hitachi.jp kiwi.hitachi.jp:9999 LBL-sfromto tomato.hitachi.jp kiwi.hitachi.jp:8443		

また，HTTPS (CONNECT) 要求については，HTTPS (CONNECT) 要求ヘッダのメソッド行が定義ファイルに指定された“変換前ホスト名称：変換前ポート番号”に合致する場合，“変換後ホスト名称：変換後ポート番号”に変換した後，転送をおこなう (図 5.5下段).

(b) 送信元に対するアクセス制御機能

許可されたクライアントからの HTTP／HTTPS 要求に対してのみ，ポート／ホストマッピングならびに，HTTP／HTTPS 要求の転送をおこなう.

(c) アクセスログ機能

ポート／ホストマッピング機能の処理ログとして，発信元 IP アドレス／ホスト名称，転送先 IP アドレス／ホスト名称，時刻，HTTP／HTTPS 要求ヘッダのメソッド行を取得する.

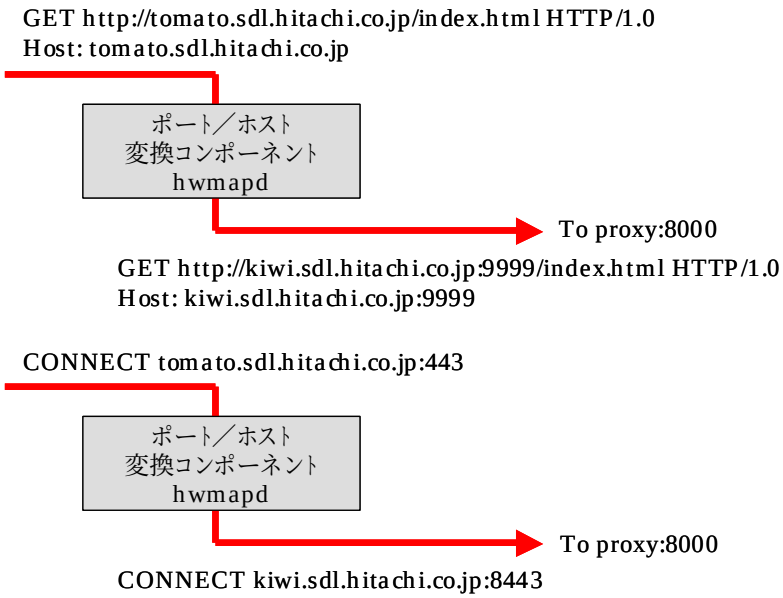


図 5.5：ポート／ホスト名称変換処理

(3) 管理コンポーネント

管理コンポーネントでは，各コンポーネントに対して，フィルタリング，ポート切替，URL マッピングの変更指示を出すためのマネジャ／エージェント機能と，夜間などのネットワークワーム流布時に自動的な切り替えを実現するための IDS 連携機能を開発した．

- マネジャ／エージェント機能

  マネジャ／エージェント機能は，図 5.6に示す通常時／緊急時 (ネットワークワーム流布時) のポート切り替え可能な Web ベースの管理インタフェース，あるいは，IDS 連携機能の検知状態をトリガとして，ポート切替とポート／ホスト変換コンポーネントに対して設定変更の指示を出す．

  また，マネジャ／エージェント間の通信ならびにコンポーネント間連携については，分散ネットワークサービス管理のためのセキュア通信基盤として開発された hsc/hsd (Hitachi Secure Socket Client/Daemon) を使用している (図 5.7) [中野 99]．hsc/hsd は HTTP プロトコルを使用した軽量通信モジュールであり，hsc から hsd に対して CGI スクリプト指定形式でプログラム起動をおこなうことができ，通信内容も独自モジュールにより認証／暗号化している．

図 5.6：Web ベースの管理インタフェース

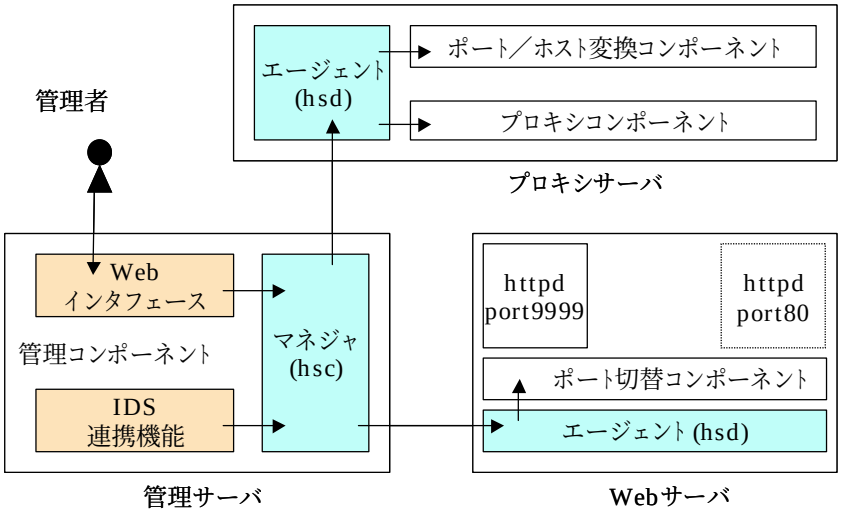


図 5.7：hsc/hsd を用いたコンポーネント間連連携

- IDS 連携機能

  IDS と連携して HTTP ポートを攻略するネットワークワーム流布時に Web マッパの変更をおこなう．本システムでは，管理サーバ上のポート番号 80/TCP に立ち上げた HTTP サーバを簡易的なホスト IDS とした．

  イントラネットにおいては，明示的に Web サーバの公開を宣言していない限

り，その Web サーバにアクセスが発生することはない．言い換えれば，管理サーバ上のポート番号 80/TCP にアクセスが発生すること自体が異常であると判断できる．なお，IDS 連携機能では，HTTP サーバへの単位時間内のアクセスがしきい値を超過した場合，上記のマネジャ／エージェント機能経由で，各コンポーネントに対してワーム流布時の切り替え指示を出す仕様とした．

5.3　評価と考察

評価については，Web サーバの HTTP ポートを任意の代替ポート番号に切り替えたことによるトラフィックの抑止効果，URL 変更の隠蔽ならびに管理コンポーネントとの連動に関する機能動作確認に加え，実イントラネット環境での実験的な利用という項目を対象とした．

5.3.1　トラフィックの抑止効果

Code Red I/II，Nimda の送出する TCP パケット数を実測すると，ポート切り替えの前後で表 5.2の通りとなる．この結果から，提案方式は，ネットワークワームの流布に伴うトラフィック抑止において効果があることを確認した．

5.3.2　コンポーネントの機能動作確認

コンポーネントの機能動作確認では，URL 変更の隠蔽と管理コンポーネントとの連動による切り替え動作の機能確認をおこなった．

(1) HTTP アクセスにおける URL 変更の隠蔽について

代替ポート番号 (9999/TCP) でサービスを提供している Web サーバに対し，ポート／ホスト変換コンポーネント hwmapd を介して，次の 5 つの形態でのアクセスをおこなった．その結果，図 5.8に示す通り，標準ポート番号 (80/TCP) の URL 指定で代替ポート番号 (9999/TCP) にアクセスしていることと，代替ポート番号への切り替えによる URL 変更を，ポート／ホスト変換コンポーネント hwmapd が隠蔽していることを確認した．

表 5.2：ネットワークワームが送出する TCP パケット数の比較

	ポート切り替え前 Web サーバをポート番号 (80/TCP) で稼動している場合	**ポート切り替え後** ポート番号 (80/TCP) を閉じ, Web サーバをポート番号 (9999/TCP) で稼動している場合
Code Red I	**13 パケット** SYN, SYN+ACK, ACK, HTTP 要求(1), ACK, HTTP 要求(2), ACK, HTTP 要求(3), ACK, HTTP 応答, FIN+ACK, RST, RST	**6 パケット** SYN, RST (3 回再送されるため, 2 x 3 パケットとなる)
Code Red II	**13 パケット** 同上	**6 パケット** 同上
Nimda	**128 パケット** SYN, SYN+ACK, RST, ACK, HTTP 要求, HTTP 応答, FIN+ACK, RST (16 個の HTTP 要求が送信されるため 8 x 16 パケットとなる)	**96 パケット** 同上 (16 個の HTTP 要求の送信が 3 回再送されるため 2 x 16 x 3 パケットとなる)

注) 実測条件：TCP セグメントの最大サイズ=1,460 バイト

- 環境変数表示用 CGI プログラムへのアクセス
- 相対パス記述の URL へのアクセス
- 絶対パス記述の URL へのアクセス
- ホスト名称＋ポート番号記述の URL へのアクセス
- JavaScript によるホスト名称記述の URL へのアクセス

また，今回，今後の機能拡張を考慮し，ポート／ホスト変換コンポーネントとして hwmapd の開発をおこなったが，HTTP アクセスについては，同等の機能を Apache の既存機能 (rewrite, proxy 機能) の組み合わせにより実現できることを確認した[v].

v) HTTP アクセス用のポート／ホスト変換コンポーネントの代用については，Apache 2.0.43 の rewrite, proxy 機能により確認をおこなった.

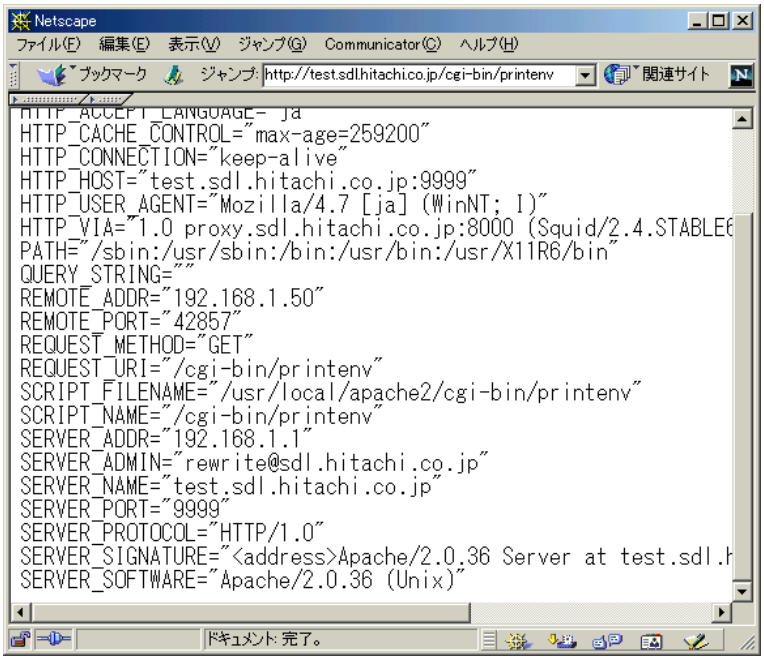


図 5.8：hwmapd を介した環境変数表示用 CGI へのアクセス結果

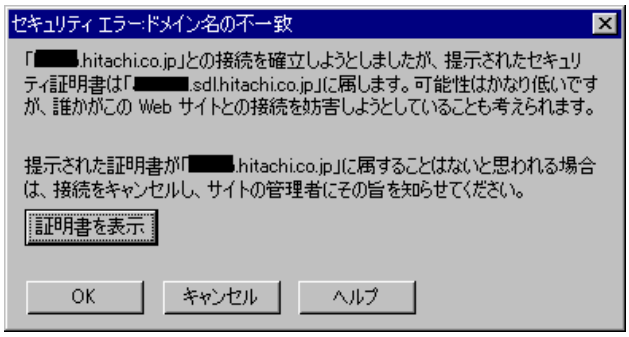


図 5.9：異なるホスト名称に書き換えた場合の警告ダイアログ

(2) HTTPS アクセスにおける URL 変更の隠蔽について

HTTP アクセスと同様に 5 つの形態でのアクセスをおこなった結果, 標準ポート番号 (443/TCP) の URL 指定で代替ポート番号 (8443/TCP) にアクセスしていることと，代替ポート番号への切り替えよる URL 変更を隠蔽していることを確認した. さらに, ポート／ホスト名称変換の対象範囲をドメイン名部分にまで適用した場合には，図 5.9に示す警告ダイアログ“ セキュリティエラー：ドメイン名の不一致 ”を表示するが，ディレクトリパスは Web サーバに格納されているディレクトリパスに従いアクセスできることを確認した.

図 5.10：IDS 連携機能指示による切り替えの完了報告

(3) 管理コンポーネントとの連動について

(a) 手動による設定変更

Web ベースの管理インタフェースから hsc/hsd 経由でポート切り替えスクリプトを起動することにより, 対象となるすべてのコンポーネントの通常時／緊急時の相互切り替えを確認した.

(b) IDS 連携機能からの設定変更

マネジャ機能は，定期的に簡易的なホスト IDS へのアクセス数をカウントし, 単位時間内のアクセスがしきい値を超過した場合, エージェント経由でポート切替コンポーネントとポート／ホスト変換コンポーネントの設定変更を指示する. この IDS 連携機能からの設定変更についても, すべての設定変更が終了した時点で Web ベースの管理インタフェースに完了報告を上げることを確認した(図 5.10). なお, 単位時間内のしきい値は，2.3.3節での調査事例を参考に 10 分間あたり 8 アクセスとしたが, 流布の規模を踏まえたしきい値の設定については, 今後の課題である.

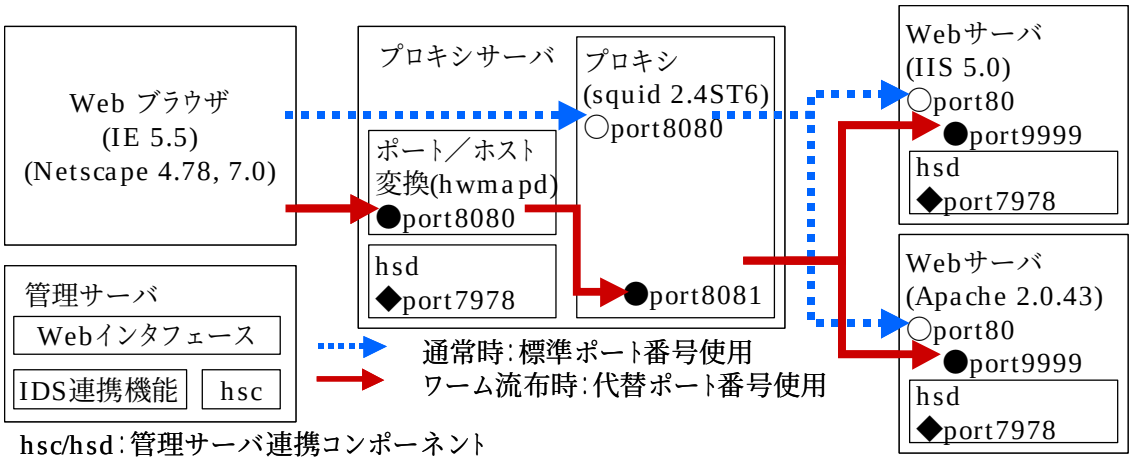


図 5.11：Web マッパ評価環境の構成概要

表 5.3：Web マッパ評価環境の Web サーバ台数

項目	内容
ユーザ利用テストで確認した Web サーバ台数	イントラネットに接続する 10 サイト (注)
セッション制御動作テストで確認した Web サーバ台数	同上
切り替えテストで確認した Web サーバ台数	イントラネットに接続する 3 サイト

注) 10 サイトのうち，代替ポートを準備して確認をおこなったサイトは 3 サイトであり，残りの 7 サイトについては Web ブラウザの URL で代替ポート番号 (http://host:9999) を指定する形態で確認をおこなった．

5.3.3　実イントラネット環境での実験的な利用

図 5.11，表 5.3に示す実イントラネット環境下において，実装システムの適用可能性を検討した．適用評価のシステム構成では，管理コンポーネント用としてポート番号 7978/TCP，プロキシサーバ用としてポート番号 8080/TCP を固定的に割り当てている．また，プロキシサーバ内部では，通常時にはプロキシコンポーネントとして使用した Squid のポート番号 8080 経由で，緊急時には Squid のポート番号 8081 経由で代替ポート番号 (9999/TCP) にアクセスする形態を用いて，次に示す項目についての確認をおこなった．

表 5.4：Web マッパ評価における確認項目

分類	確認内容
(a) ユーザ利用テスト	ポート／ホスト変換コンポーネントを有効としたプロキシサーバを介して Web サーバにアクセスした場合に, ページが表示されないなどの問題がない.
	ポート／ホスト変換コンポーネントの定義対象外となる Web サーバ, たとえば, インターネットならびに, 他サイトのページについては, これまで通りアクセスすることができ, ページが表示されないなどの問題がない.
(b) セッション制御 動作テスト	Web サーバのポート切り替え後 (80/TCP⇒9999/TCP) も, ユーザの追加操作なく, Web サーバ (Apache, Microsoft IIS) を継続して利用可能である.
	Web サーバのポート切り替え後 (80/TCP⇒9999/TCP) も, ユーザの追加操作なく, Cookie を用いてセッション制御をおこなっているアプリケーション, URL を用いてセッション制御をおこなっているアプリケーションを継続して利用可能である.
(c) 切り替えテスト	Web ベースの管理インタフェース (http://admin:20021/) からの指示に従い, Web サーバのポート番号の切り替え, ポート／ホスト変換コンポーネントの有効化が可能である.
	IDS 連携機能からの指示に従い, Web サーバのポート番号の切り替え, ポート／ホスト変換コンポーネントの有効化が可能である.

- ポート番号の切り替えによる Web サーバの継続利用
  実環境下において，ポート番号切り替えに伴う Web サーバアクセスへの影響有無を確認する(表 5.4：(a) ユーザ利用テスト, (b) セッション制御動作テスト).
- IDS 検知機能と連動したポートの自動切換え
  深夜の運用支援を想定し, IDS などの検知機構と連動したポート切り替えを対象に動作確認をおこなう(表 5.4：(c) 切り替えテスト).

結果として，ユーザ利用，セッション制御動作のいずれのテストにおいてもページが表示されないなど，Web サーバの継続利用を妨げる問題はなかった．また，Web マッパのポート／ホスト変換コンポーネントと同等の機能を持つ Apache の既存機能 (rewrite, proxy 機能) についても確認項目に関して hwmapd と同様の結果が得られた.

表 5.5：HTTP 要求／応答の 1 トランザクション毎の応答性能

実測環境	hwmapd 経由	hwmapd 経由なし
応答値が最小の Web サイト	36 ミリ秒	33 ミリ秒
応答値が最大の Web サイト	3.2 秒	2.2 秒

注) ユーザ利用テストで使用した Web サイトにアクセスし, その応答時間を
測定した. 測定値は 20 回おこなって平均をとった.

表 5.6：コンポーネント切り替えの所要時間

実測環境	Web ベースの管理インタフェース経由
切り替え時間	15.7 秒

注) Web ベースの管理インタフェースを用いて対象とする 3 サイトの切り替えが
完了するまでの総時間を測定した. 測定値は 20 回おこなって平均をとった.

次に，実装システムを用いた HTTP アクセスの応答性能について述べる．性能評価に利用した機器のうち, Web サーバについては実イントラネットに設置された Web サーバを, プロキシサーバについても同じく実イントラネットに設置されたプロキシサーバを利用している．HTTP 要求／応答の 1 トランザクションの応答性能測定は，Web サーバに対する HTTP GET 要求データを発行してから HTTP 応答データを受信完了するまでの時間をスクリプト言語 perl で作成したツールを HITACHI FLORA (Pentium II, Microsoft Windows 2000) 上で実行し測定した．HTTP 要求／応答の 1 トランザクション毎に測定をおこなった場合，ポート／ホスト変換コンポーネント hwmapd 経由の性能は表 5.5の通りである．ただし，Web ブラウザにおいて画像が多数リンクされた Web ページを表示する際に 1 分近く要する場合もあり，hwmapd への同時アクセスに伴う性能改善を検討していく必要がある.

また, 切り替えテストについても動作自身にトラブルはなく, 管理コンポーネントによる設定変更指示から完了報告までの時間にばらつきはあるが，1 サイトあたり約 15 秒前後での切り替えができている(表 5.6). ただし，約 1 分／サイトを要する場合もあり，イントラネット全体への適用を想定した場合には，設定変更指示方法の改良，並行処理ならびにサイト単位での分散処理を検討していく必要のあることがわかった.

5.4 まとめ

本章では，イントラネットにおいて HTTP ポートを攻略するネットワークワーム流布時の対策として，ネットワークサービスを退避させる Web ポート／ホストマッピング方式を提案した．

まず, 課題を解決するために, 対象とするネットワークワームが“ ポート番号 80/TCP に対して直接 TCP コネクションを確立した後，Web サーバの脆弱性を攻略する ”という特徴に着目し，ネットワークワームの流布を抑止することと，Web サーバの稼動継続性を確保することの二面性を兼ね備えた対策を提示した．具体的には，Web サーバ上のポート切替コンポーネントが Web サーバの HTTP ポートを任意の代替ポート番号に切り替えることでネットワークワームの流布を抑止する．次に，プロキシサーバ上のポート／ホスト変換コンポーネントが Web サーバの HTTP ポートを代替ポート番号に切り替えたことによる URL 変更を隠蔽することで, Web サーバの稼動継続性を確保する HTTP ポート対応の Web ポート／ホストマッピング方式である．

また, 提案方式に基づき実装したシステム Web マッパを用いて, Web サーバの HTTP ポートを代替ポート番号に切り替えたことによるトラフィックの抑止効果，URL 変更の隠蔽ならびに管理コンポーネントとの連動に関する機能動作確認に加え, 実イントラネット環境での実験的な利用について評価をおこなった．これらの評価を通じて，提案方式が本来の 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ことを確認した．

このような対策方法を開示することにより, その対策方法を回避するネットワークワームの出現は予想しうることである．しかし，セキュリティにおいて，万能な対策方法はなく，多層防御に代表される，対策の多重化を実現する部品ならびに環境作りが重要であると考えている．

第6章　インシデント対処の今後の展開

本章では，インシデント対処の今後の展開として，インターネットにおける新たな脅威とその脅威に対処するための体制である組織相互連携オペレーションについて概説する．

6.1　インシデントの変化

2005 年 8 月 10 日，マイクロソフトから“ Windows プラグ アンド プレイ サービスに関するバッファオーバーフローの脆弱性 (MS05-039) ”が報告された．この脆弱性はリモートからのコード実行ならびに特権昇格に悪用することができ，2005 年 8 月 13 日にネットワークワーム Zotob ならびにその亜種が流布する際に利用された．脆弱性の公開，攻撃検証コードの公開，そして，ネットワークワームの出現という流れについては, PRC DCOM (MS03-026) の脆弱性を悪用し 2003 年 8 月に流布した Blaster, LSASS (MS04-011) の脆弱性を悪用し 2004 年 5 月に流布した Sasser と同様である．しかし, Zotob は, これまでのネットワークワームとは異なる特徴を持ちあわせており，昨今の脆弱性を取り巻く脅威にも新たな変化が見られはじめている．

本節では, セキュリティ侵害の新たな活動として, 図 6.1に示す悪性スパムならびに, フィッシングで使用される受動型攻撃と，ネットワークワームの変化について述べる．

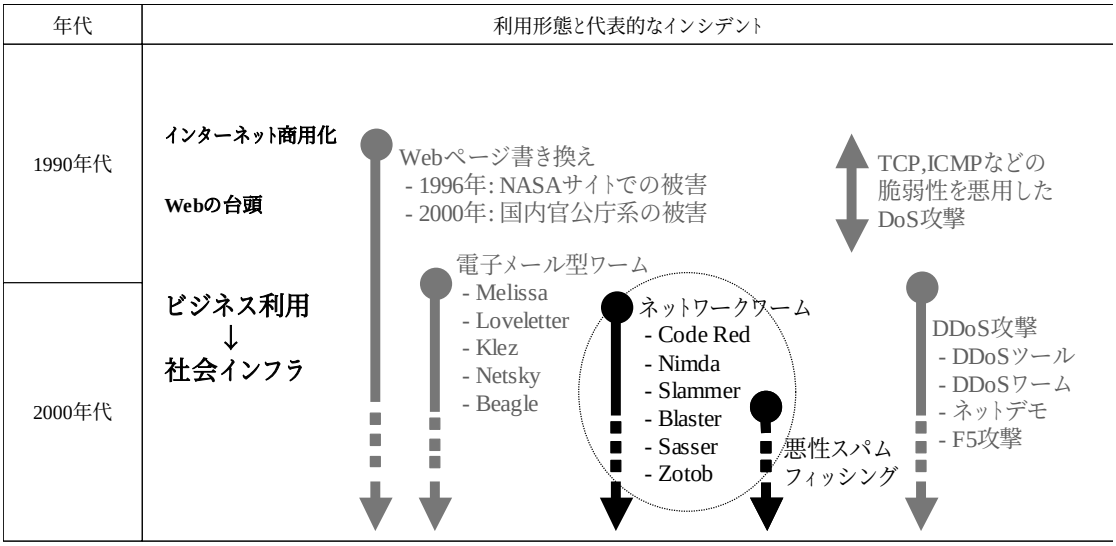


図 6.1：インシデントの変遷

6.1.1 受動型攻撃

2003 年以降，金融機関などからの正規の電子メールや Web サイトを装い，暗証番号やクレジットカード番号などを搾取する詐欺，いわゆるフィッシング (phishing) による被害が報告されはじめた．このセキュリティ侵害活動は，主に，ボット (bot) と受動型攻撃という新たな組み合わせにより構成されている．

ボットとは，外部からの命令を待ち，その命令に従って何らかの動作をするプログラムである．ボットをインストールされてしまったシステムは，悪意ある第三者により外部から自由に操作できるようになってしまい [police05]，システムに関する不正な情報取得，正規の電子メールを装ったフィッシングメールを送出する中継システムならびに，DDoS 攻撃を仕掛けるエージェントとして利用されている [総務省 05]．そして，このようなボットをユーザにインストールさせたり，フィッシングサイトに誘導させたりするために利用されている手法のひとつが，ソーシャルエンジニアリング攻撃に代表される“ 受動型攻撃 ” [Yoshida01][共立 03] である．

ソーシャルエンジニアリング攻撃とは, 社会工学的な観点から発生する脆弱性を利用した攻撃方法である．たとえば，管理者を装ってパスワードや機密情報を聞き出す行為や, ゴミ箱の中身やパソコンの周辺に貼られたメモからパスワードを推測したりする行為がある．1991 年には，CERT Advisory CA-1991-04: Social Engineering [CERT91] としてソーシャルエンジニアリング攻撃に関するセキュリティ侵害報告が発行されている．ここで報告された攻撃方法は，管理者を装ってパスワードの変更を促す電子メールを送りつけるという手法である．さらに，ソーシャルエンジニアリング攻撃は，管理者を装ったパスワード変更依頼だけではなく，Melissa，LoveLetter など電子メールを介したウイルスの流布にも利用されている．いずれの場合も，攻略対象は電子メール受信者となるユーザであり，そのユーザを騙すために，電子メールの内容は，電子メール受信者が興味を引く内容となっている．

受動型攻撃とは，ソーシャルエンジニアリング攻撃などを利用して，攻略対象となるコンピュータシステムのユーザに攻撃活動の引き金を引かせてしまう形態のことを指している．これに対して，攻撃活動の引き金を攻撃者自身が引く形態，すなわち，攻撃者自身が電子メールサーバ, Web サーバや DNS サーバなどのサーバプログラムの脆弱性を悪用して攻略対象となるシステムに不正侵入する形態は“ 能動型攻撃 ”と呼ばれている．Web ページの書き換えやネットワークワームによるセキュリティ侵害は，主に能動型攻撃であり，ファイアウォールなどのネットワークの防火壁が有効に働いた．しかし，受動型攻撃の場合には，攻撃者はマルウェアを電子メールに添付するか，Web サイトに掲載するだけでよい．そして，送信されたマルウェアが電子メールを経て攻略対象となるクライアントシステムに届いたり，あるいは，掲載されたマルウェアをユーザ自身がインターネット上からダウンロードしたりすることでクライアントシステムに持ち込んでしまう．これは，能動型攻撃に比べファイアウォールによる防火壁を越えるのが容易であり，イントラネットへも潜り込み易いことを意味する．

さらに，攻撃者は，フィッシングやこれまでのトロイの木馬を流布させる方法として利用されてきたランダムに配布するという手法ではなく, 特定の個人ならびに組織を対象にカスタマイズ化したセキュリティ侵害活動 (スピアフィッシングと呼ばれている) [USCERT05b] を進めている．このような侵害形態の場合，マルウェアの添付された電子メールの流通量も少なくなり, ウイルス定義ファイルの元となる検体そのものの流通量が減る．その結果，攻撃者にとっては，アンチウイルスソフトウェアを回避し，かつ検出されにくい環境を作り出すことができてしまうことになる．

このように今後のインシデントの発生形態ならびに被害形態は, 気がつかない間にシステムが侵害され，被害が進行することが予想される．

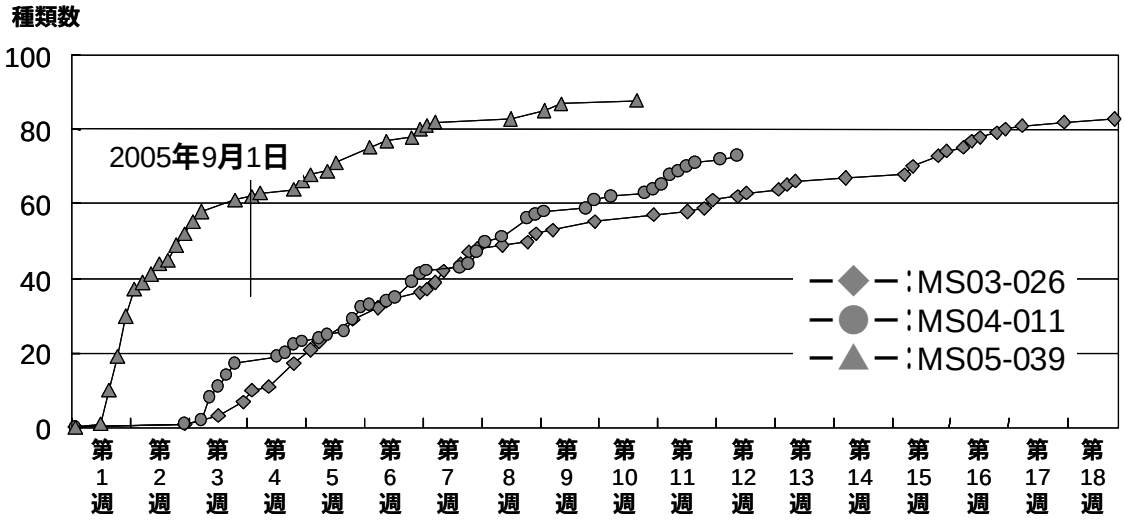


図 6.2：MS03-026, MS04-011, MS05-039 を悪用するマルウェア発生状況

6.1.2 ネットワークワームの変化

プラグ アンド プレイ サービスの脆弱性 (MS05-039) の公開，攻撃検証コードの公開，そして，ネットワークワーム Zotob の出現という経過は，Blaster に悪用された PRC DCOM (MS03-026) の脆弱性，Sasser に悪用された LSASS (MS04-011) の脆弱性と同じ経過を辿っている．しかし，Zotob は，Blaster，Sasser とは異なる特徴を持ちあわせており, 昨今の脆弱性を取り巻く脅威にも新たな変化が見られはじめている．ここでは，脆弱性の悪用に関する変化と，ネットワークワームにおける変化についてまとめる．

(1) 脆弱性の悪用に関する変化

2003 年以降ネットワークワームに悪用された代表的な脆弱性として，2003 年 7 月に報告され Blaster に利用された MS03-026，2004 年 4 月に報告され Sasser に利用された MS04-011, 2005 年 8 月に報告され Zotob に利用された MS05-039 がある．これら MS03-026，MS04-011，MS05-039 を悪用するマルウェアの発生状況は図 6.2の通りである [寺田 05]．MS03-026 と MS04-011 のマルウェア発生状況は，ほぼ類似した推移をたどっているのに対して Zotob に利用された MS05-039 については次の点で推移形態が異なっている．

- Zotob とその亜種との争いにより, 初期段階におけるマルウェア種類数の報告件数が MS03-026，MS04-011 に比べて多い.
  脆弱性の公開から第 4 週までに報告されたマルウェア種類数が, MS05-039 では約 60 件であるのに対し，MS03-026，MS04-011 ではその 1/3 の 20 件以下に留まっている.
- 2005 年 9 月以降，マルウェア種類数の報告件数が同時期の MS03-026, MS04-011 の推移に比べて少ない.
  第 4 週から第 8 週までに報告されたマルウェア種類数が，MS03-026, MS04-011 では約 40 件であるのに対し, MS05-039 ではその半分の 20 件前後に留まっている.

このうち，Zotob とその亜種との争いについては，F-Secure から報告されており [Fsecure05b]，IRCBOT (Esbot.A，Esbot.B，Esbot.C，Zotob.D) と BOZORI (Zotob.E，Zotob.F) 系のボット (捕食者) が，Zotob，RBOT，SDBOT などの競合相手であるボット (被食者) をシステムから削除すると報告している．ここで, MS05-039 に関連して捕食関係にあったネットワークワームの感染報告数とその関係を図 6.3に示す. 図 6.3では捕食者として活動するボットから被食者となるボットに向けて矢印を記載している．また，図 6.3に記載したトレンドマイクロ ウイルスストラッキングセンターの感染件数の報告 [TrendMicro] から，次のことが言える.

- 被食者の感染報告数は，捕食者の感染報告数増加と共に激減している．この様子は，捕食者の感染報告数が増加しはじめた 2005 年 8 月 16 日前後に現れている.
- 捕食者は, ネットワークワーム (Zotob.A, Zotob.B, RBOT.YN, SDBOT.ADB) を攻撃対象としている. すなわち, ネットワークワームを競合相手としている.
- 捕食者は, 電子メール型ワーム Zotob.C を攻撃対象としていない. このため, Zotob.C の感染報告数は，捕食者の感染報告数変動に影響を受けていない.

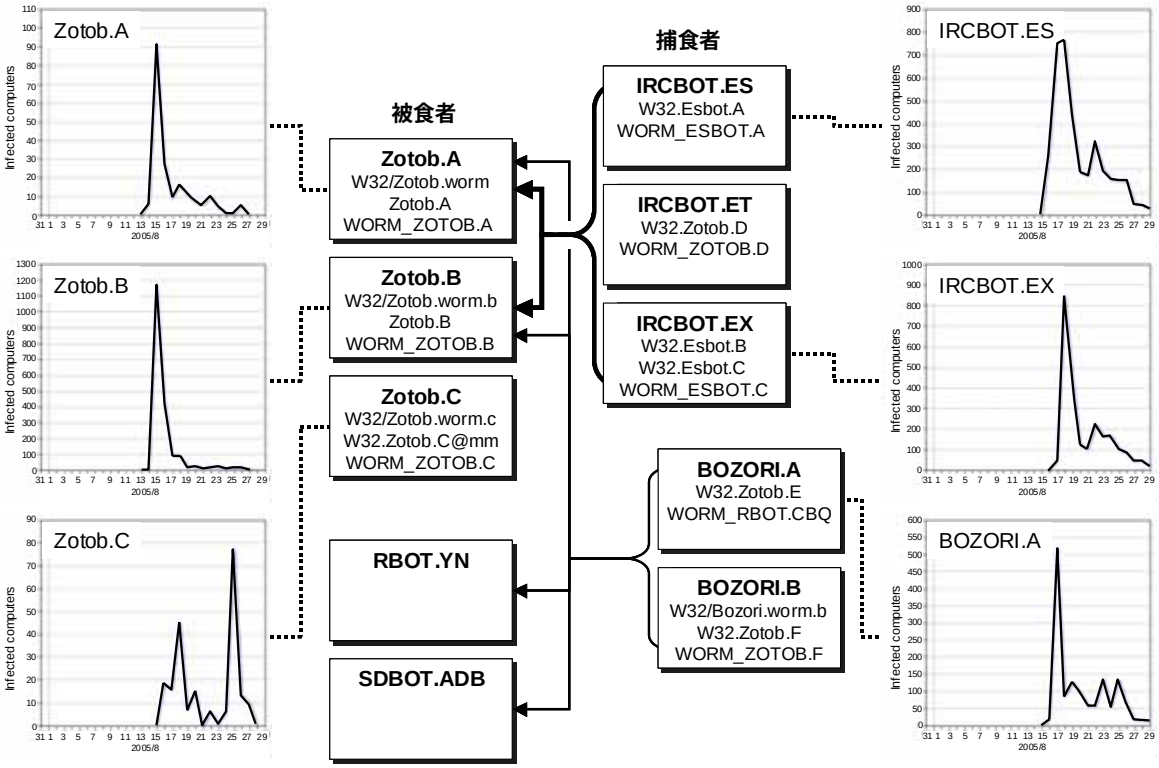


図 6.3：捕食関係にあったネットワークワームの感染報告数

代表的な捕食活動としては，Netsky と Beagle の争いはあるが，表立って報告された活動はあまり多くはない．今回の捕食活動は，ネットワークワームのみを攻撃対象としていることから，侵害活動のインフラ構築，すなわち，ボットネット (botnet：ボットのインストールされたシステムの集合体) 構築など活動エリアの確保とも関係していると考えられる．

(2) 感染活動の変化

Blaster，Sasser(.A)，Zotob(.A)の感染活動の比較を表 6.1に示す．Zotob は，Mytob を元に作成されたと報告 [Fsecure05a] されており，バックドア活動も Blaster，Sasser に比べボット系機能の色合いが強い．X-Force の分析によれば，Zotob，Esbot，Rbot の複数の亜種が，ボットネットの所有者により適切に制御されていることも，今までのネットワークワームとは異なる点であると指摘している [ISS05].

表 6.1：Blaster，Sasser，Zotob の感染活動の比較

項目	Blaster	Sasser.A	Zotob.A
悪用する 脆弱性 (公開日)	MS03-026 2003 年 7 月 17 日	MS04-011 2004 年 4 月 14 日	MS05-039 2005 年 8 月 10 日
利用された 攻撃検証コード (公開日)	dcom.c 2003 年 7 月 27 日 [eEye03]	HOD-ms04011-lsasrv-expl.c 2004 年 4 月 29 日 [eEye04]	HOD-ms05039-pnp-expl.c 2005 年 8 月 12 日 [Fsecure05a]
元となった マルウェア	―	―	Mytob [Fsecure05a]
ネットワーク ワーム出現日	2003 年 8 月 11 日	2004 年 4 月 30 日	2005 年 8 月 14 日
探査方法: 探索比率加味	アドレスブロック 探索比率加味型	アドレスブロック 探索比率加味型	アドレスブロック 探索比率加味型
探査方法: 探索形態	スイープ探索型	ランダム探索型	ランダム探索型
探査方法: 探索範囲	限定なし (グローバル)	限定なし (グローバル)	同一ネット
バックドア活動	・DoS 攻撃 特定の日付条件で, windowsupdate.com に対して DoS 攻撃開始	―	・プロセスの終了 ・DoS 攻撃 ・特定の IRC サーバに 接続 ・インターネットから ファイルのダウンロード ・特定の Web サイトに アクセス ・自身のコピーのアン インストール ・システム情報の収集 (CPU 速度, メモリ容量) ・自身のアップデート ファイルのダウンロード ・ポート 8888 番を介して リモートコマンドシェルを 作成

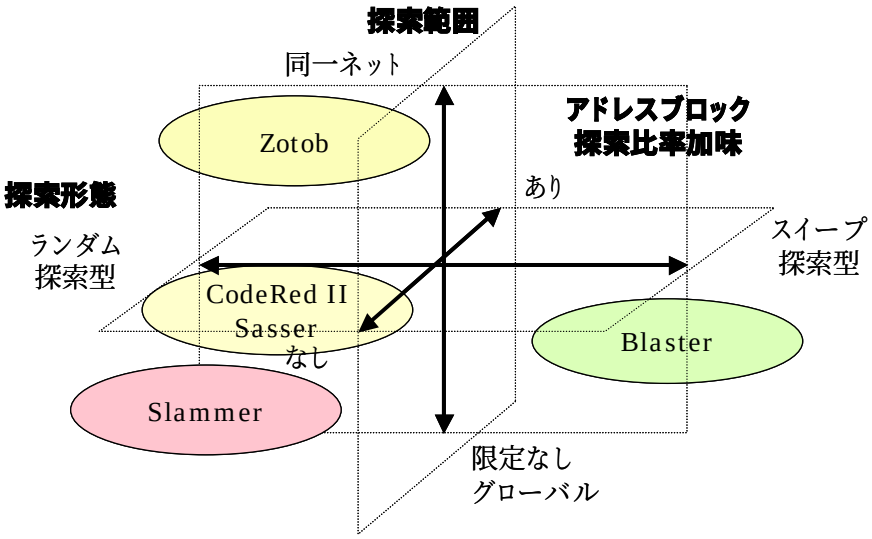


図 6.4：感染先探索特性の分類

次に，感染先探索特性の分類の視点から比較を図 6.4に示す．Zotob の感染活動に伴う探索範囲は，同一ネット (上位 2 オクテットが同一) に限定されており，このような動作は探索範囲に制限を設けずに流布する既存ネットワークワーム Code Red, Slammer, MS Blaster, Sasser との大きな違いとなっている．X-Force によれば，Zotob，Esbot，Rbot の複数の亜種は，同一ネット (上位 2 オクテットの IP アドレスが同一) に限定した探索動作をおこなうために，大きな組織では，感染活動に伴うすべての通信がそのイントラネットにとどまってしまうことを指摘している [ISS05]．これは“個々の組織を狙っているようだ”との感染被害の報告内容と合致している．

Zotob の流布形態ならびに被害形態の調査から，脆弱性を取り巻く脅威は，次のような流れにあると考えられる．

- バックドア活動

  ネットワークワームのバックドア活動の主目的が，DDoS 攻撃ではなく，侵害活動のインフラ構築，すなわち，ボットネット構築に移行している．

- 感染先探索活動

  ネットワークワームの感染活動は，探索範囲に制限を設けずに流布する形態ではなく，探索範囲を限定して流布する形態が主流となり，侵害活動がより見えにくくなっていくことが予想される．探索範囲を限定して流布する形態については，US-CERT の報告 Targeted Trojan Email Attacks [USCERT05a] や米 IBM Global Security Intelligence チームのセキュリティトレンドの報告 [IBM05] も同様な傾向を提示している．

> 無差別に送りつけられるスパムや単純なウイルスに代わり，重要な情報やアイデンティティ情報の詐取，恐喝といった明確な目的を持って特定の組織や業種を狙い撃ちにする，標的を絞った攻撃が増加している．また，フィッシング詐欺でも特定の組織や個人を標的にした狙い撃ち手法が増加している．
>
> 出典：IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005 から抜粋 [IBM05]

また，侵害活動がより見えにくくなっていくという傾向は，図 6.2の MS05-039 を悪用するマルウェア種類数の報告件数が 9 月以降あまり増加していないことと合致している．

- マルウェアへの攻撃検証コード組み込み期間

  Sasser と Zotob のいずれも，攻撃検証コードが公開されてからマルウェアに組み込まれるまでの期間は 2 日間ほどである．このことから，マルウェアの作成が手順化ならびにモジュール化されていると類推され，今後も，短期間のうちに，脆弱性を悪用する機能がマルウェアに組み込まれることが予想される．

6.2 組織相互連携オペレーション

これまでの電子メール型ワーム，ネットワークワームならびに，DDoS 攻撃によるセキュリティ侵害は，予兆ならびに被害を誰もが把握できる事象であった．ところが，ボットと受動型攻撃という新たな組合せによるセキュリティ侵害活動は，特定の組織，業種や個人に標的を絞った攻撃をおこなうことで，予兆や被害を隠蔽化する傾向にある．インシデント対処の今後の展開においては，このような新たな脅威に対抗するインシデントオペレーションの確立が必要となる．本節では，新たな脅威に対抗するための組織相互連携オペレーション (Coalition Operation) という考え方について述べる．

ネットワークワーム出現の予兆は，脆弱性ならびに修正プログラムの公開，攻撃検証コードの公開，脆弱性を悪用するトロイの木馬の出現という過程として現れてきた．また，電子メール型ワームやネットワークワームの被害は，均一的かつ広範囲において，システムがワームに感染するという形で現れた．そして，DDoS 攻撃の被害は，攻撃対象となる Web サイトがサービス不能状態に陥り，DDoS 攻撃パケットが通過する ISP においてトラフィック増大という形で現れた．このように，予兆に関しては単独組織での観測することが可能であり，また，被害収束に関しては広範囲で均一的な事象が発生しているので，複数組織の協力による問題事象の解決が容易であった．ところが，ボットと受動型攻撃という新たな組合せによるセキュリティ侵害活動は，特定の組織，業種や個人に標的を絞った攻撃をおこなうことで，予兆や被害を隠蔽化する傾向にある．このため，たとえ予兆や被害が表面化したとしても局所的な問題事象としてしか現れず，結果として重要インシデントへの発展を見過ごしてしまう可能性が高くなる．

このような新たなセキュリティ侵害活動に対しては，局所的な問題事象を大局的な問題事象として捉えることで，インシデントに伴う被害を予測ならびに予防し，インシデント発生後は被害の拡大を低減することが重要となる．また，問題事象の大局化をおこなうためには，分野の枠を越えた複数組織の連携として，次に示すような連携が必要となる．

- 各組織が保有する観測機能を連携させることによる局所的な予兆や被害に関する状況把握の実施
- 把握した予兆や被害の状況分析とその分析に基づく問題事象の大局化
- 各組織が保有する対処機能を連携させることによる問題事象の解決

表 6.2：インシデント対処の今後の展開

項目	2003 年～2005 年 インシデントオペレーション	2006 年以降 組織相互連携オペレーション
インターネットの利用度 (依存度)	社会インフラ	同左
代表的な インシデント	電子メール型ワーム ネットワークワーム DDoS 攻撃	悪性スパム フィッシング
インシデント発生に 伴う影響	均一的かつ広範囲に渡る被害 各種業務等全般に関わるため 経済活動への影響大	類似した局所的な被害 各種業務等全般に関わるため 経済活動への影響大 (予兆や 被害が見えにくくなる傾向大)
インシデントの予測 ならびに 予防の対処体制 (警戒, 予兆, 対処)	予兆に基づく 単独組織での対応	複数組織で局所的な予兆を 共有しながら対応
インシデント発生後の 対処体制 (対処, 監視, 収束)	複数組織の協力により均一的 かつ広範囲に渡る被害に対応	複数組織の協力により類似 した局所的な被害を大局的な 被害として捕らえ対応
インシデント対処の 考え方	インシデントに伴う被害を予測 ならびに予防し, インシデント発 生後は被害の拡大を低減する 対応	組織相互連携を用いたインシ デントに伴う被害を予測ならび に予防し, インシデント発生後 は被害の拡大を低減する対応

これまでのインシデントオペレーションと新たな脅威に対抗するために必要となるインシデントオペレーションの違いは表 6.2の通り, 複数組織の連携を通して, 分析と対処判断を繰り返しながら大局的な問題事象として捉えていく組織相互連携型のインシデントオペレーション (組織相互連携オペレーション) を確立していく必要があろう.

6.3 まとめ

昨今の脆弱性を取り巻く脅威の変化は，侵害活動インフラの構築と，構築したインフラ活用という面において，顕著に現れてきている．

- ボットを用いた侵害活動インフラの構築
  攻撃者は，侵害したシステムにボットをインストールすると共に，ボットの集合体 (ボットネットと呼ばれている) を構成することで侵害活動のインフラを構築している．
- 攻略対象を絞った受動型攻撃の実施
  攻撃者は，フィッシングやこれまでのトロイの木馬を流布させる方法として利用されてきたランダムに配布するという手法ではなく，特定の個人や組織を対象としたセキュリティ侵害活動を進めている．

これら新たな脅威に対しても，インシデントに伴う被害を予測ならびに予防し，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，特に，“ 重大な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 ”というインシデントオペレーションの考え方は有効である．そして，予兆や被害が表面化しないという事象については，予兆ならびに被害を複数組織で共有しながら対処する組織相互連携型のインシデントオペレーションにより解決することができるであろう．

今後は，これら新たな脅威に関する現状の状況ならびに脅威分析をおこない，対応の段階分けと共に，各段階での実施事項の明確化を検討していきたいと考えている．

第7章　結論

本研究では，インシデントオペレーションという考え方に基づき，ネットワークワームを対象としたインシデント対応について研究をおこなった.

- 脆弱性ならびに修正プログラムの公開からネットワークワームの流布収束までの活動を支援する脆弱性／インシデント対処情報共有システムの研究
- ネットワークワーム出現フェーズの活動を支援するネットワークワーム動作検証システムの研究
- ネットワークワームの流布フェーズの活動を支援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の研究

脆弱性／インシデント対処情報共有システムの研究では, 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いことから, 脆弱性ならびに修正プログラムの公開から“いつ攻撃検証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処がとられたのか？”という脆弱性に関わる状況変化を共有するシステム JVN を提案した．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 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 から構成している．提案に基づき構築した Web 試行サイトの運用を通して，脆弱性対策情報である Vendor Status Notes とインシデント対応の経過情報である Status Tracking Notes の双方が活用されていること，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ことを確認した.

ネットワークワーム動作検証システムの研究では, 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，特に，各組織単独で実施可能なネッ

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の感染動作に関する情報収集を目的とした検証システムを提案した. 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の感染先探索範囲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. 実装したプロトタイプシステムを用いた実験を通して, 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に利用できることを確認した.

ネットワークワーム流布対策システムの研究では, 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ことから, 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 マッパを提案した. Web マッパは, イントラネットにおける HTTP ポートを攻略するネットワークワーム流布を回避するために, Web サーバの HTTP ポートを任意の代替ポート番号に切り替え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 ポートを代替ポート番号に切り替えたことをユーザ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. 提案方式に基づき実装したシステム Web マッパを用いて, トラフィックの抑止効果, 機能動作確認ならびに, 実イントラネット環境での実験的な利用について評価をおこなった結果, 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ことを確認した.

本論文では, インシデントオペレーションの一部を具現化するシステムの提案に留まってはいるが, インシデントオペレーションという考え方に基づいたインシデント対応は, 情報システムのシステム管理者やシステム構築に関わるシステムエンジニアにとって, 安全で安心なインターネット環境の維持に役立つものと期待される.

インシデントオペレーションについては, まだまだ多くの研究の余地と運用実績の積み上げが必要となる. 提案したシステムに関連する今後の課題は次の通りである.

第 3 章の脆弱性／インシデント対処情報共有システムについては, 脆弱性対策情報ならびにインシデント対応のための経過情報を収集し, 再配信するための情報流通機構の検討や, インターネット定点観測システムなどの各種ネットワークモニタリングと連携したインシデント検出などが挙げられる. 現在, 情報流通機構については, 関連情報の収集と整理の自動化を実現するために, “ RDF Site Summary を用いたセキュリティ情報流通に関する検討 ”[寺田 03] に基づき, JVNRSS による実現を検討推進中である.

第 4 章のネットワークワーム動作検証システムについては, DNS サーバの模擬機能などを検証システムに組み込むことにより, Welchia のような複雑な感染動作をとるネ

ットワークワームに対応すること，すなわち，デフォルト設定で感染動作の確認可能な対象を広げていくこと．さらには，ネットワークワームの感染動作だけではなく，各種マルウェアの動作確認を支援するために，電子メールサーバや Web サーバなどの各種模擬機能を備えた小規模な仮想インターネット環境機能の構築や, 送信先ポート番号の発生系列とプロトコルアナライザとを連携させることにより, 各ポート番号で使用されているプロトコルを明らかにしていくことで, より効果的な対策につなげる機能連携などが挙げられる．

第 5 章の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については, 評価で得られた結果をもとに機能ならびに性能改善を図ること．また，本提案方式だけでは回避することのできない HTTP ポートを攻略するネットワークワーム，たとえば，プロキシサーバ自身を攻略対象としたネットワークワームやプロキシサーバを乗り越えて HTTP ポートを攻略するネットワークワームへの対処方法を検討していくことが挙げられる．さらに，HTTP ポート以外についてもネットワークサービスを縮退あるいは退避するという考え方に基づき被害を回避する方法の検討していきたいと考えている．

謝辞

本研究を遂行するにあたり，大変多くの方々からのご協力，ご支援を頂き，ここに深く感謝の意を表します．

本稿の執筆にあたり，ご懇切なご指導，ご鞭撻，ならびに様々なご配慮を賜った慶應義塾大学 土居範久名誉教授 (現中央大学 理工学部教授), 慶應義塾大学 理工学部 高田眞吾専任講師に深謝致します．また，有益なご助言，ご示唆を賜った慶應義塾大学 理工学部 河野健二助教授，山本喜一助教授，笹瀬 巌教授に深く感謝の意を表します．

本研究の推進にあたり終始ご指導，ご助言を頂きました株式会社日立製作所 システム開発研究所の舩橋誠壽博士，宝木和夫博士，辻 洋博士 (現大阪府立大学教授)，岩手県立大学の村山優子教授，筑波大学の岡本栄司教授，東京電機大学の佐々木良一教授，そして，研究活動を後押ししてくれた株式会社日立製作所 Hitachi Incident Response Team の田中和雄氏，梅木久志氏に深く感謝致します．

本研究は，大学内外の方々のご指導，ご助力を得て進められたものである．第 3 章に関しては，JPCERT コーディネーションセンターの大林正英氏，山賀正人氏，鎌田敬介氏，伊藤友里恵氏，株式会社インターネットイニシアティブ (IIJ) の齋藤衛氏，インターネットセキュリティシステムズ株式会社の菊地完人氏，高橋正和氏，徳田敏文氏，情報処理推進機構の福澤淳二氏 (現日立製作所) に研究活動の具体的な推進をご支援頂いた．第 4 章に関しては，防衛庁の岡谷 貢氏，富士通研究所の鳥居 悟氏，インターネットセキュリティシステムズ株式会社の高橋正和氏らとの有益な議論が研究の推進力となった．第 5 章に関しては，同僚の礒川弘実氏にプログラム開発を含め一翼を担って頂いた．また，JVN 試行サイト活動を本サイト活動につなげることができたのは，JVN 試行サイトの運用にあたりご協力を頂いた慶応義塾大学高田研究室の皆様，そして，JVN に関わる多くの皆様のご支援ならびに，ご協力によるものです．深く感謝致します．

上記以外にも，多くの方々のご指導，ご協力を頂いた．活発な討論をして頂き，かつ，建設的な批判により著者を激励してくれた友人とのめぐりあいは幸運でした．

最後に，本研究を終始あたたかく見守り励ましてくれた妻 美穂子に感謝します．

発表論文リスト

論文誌論文

[1] 寺田真敏，礒川弘実，永井康彦，倉田盛彦，土居範久．“Webサービスを対象とするワーム流布対策方式の提案”．情報処理学会論文誌 Vol.45 No.12, pp.2815-2823 (2004)

[2] 寺田真敏，高田眞吾，土居範久．“脆弱性対策情報データベースJVNの提案”．情報処理学会論文誌 Vol.46 No.5, pp. 1256-1265 (2005)

[3] 寺田真敏，高田眞吾，土居範久．“ネットワークワーム動作検証システムの提案”．情報処理学会論文誌 Vol.46 No.8, pp.2014-2024 (2005)

[4] 寺田真敏，萱島信，倉田盛彦，佐々木良一．“企業内不正アクセス対策情報サービスシステムの構築”．情報処理学会論文誌 Vol.41 No.08, pp.2246-2254 (2000)

国際会議論文

[1] Masato Terada, Yasuhiko Nagai, Morihiko Kurata. “Proposal of the counter measure for the Web service based worm propagation”. The 7th World Multi-Conference on Systemics, Cybernetics and Informatics Vol III, pp.387-392 (Jul.27-30, 2003)

[2] Masato Terada, Norihisa Doi. “Proposal of the Security Information Sharing System with RDF Site Summary”. The 8th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol.X, pp.40-46 (Jul.18-21, 2004)

[3] Masato Terada, Shingo Takada, Norihisa Doi. “Proposal for the experimental environment for Network Worm infection”. 17th Annual FIRST Conference on Computer Security Incident Handling (2005)

講演

[1] 寺田真敏，永井康彦，倉田盛彦．“ Webサービスを対象とするワーム流布対策方式の検討 ”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2002 No.068 , pp.89-96 (Jul.18-19, 2002)

[2] 寺田真敏，礒川弘実，永井康彦，中原亮．“ Webマッパ(Webサービスポート/ホストマッピングシステム)の機能拡張と適用評価 ”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2003 No.045 , pp.41-46 (May.15-16, 2003)

[3] 寺田真敏，土居範久．“ JPCERT/CC Vendor Status Notes DB構築に関する検討 ”．情報処理学会 コンピュータセキュリティ シンポジウム 2002 , pp.173-177 (Oct.30-Nov.1, 2002)

[4] 寺田真敏，土居範久．“ RDF Site Summaryを用いたセキュリティ情報流通に関する検討 ”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2003 No.074 , pp.273-278 (Jul.17-18, 2003)

[5] 寺田真敏，城戸博行，菊地大輔，高田眞吾，土居範久．“ Status Tracking Notes；時系列イベント情報の共有 ”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2004 No.54 , pp.37-42 (May.21, 2004)

[6] 寺田真敏，高田眞吾，土居範久．“ ネットワークワームの感染先探索特性の検討 ”．情報処理学会 コンピュータセキュリティ シンポジウム 2004 , pp.487-492 (Oct.20-22, 2004)

その他

[1] 菊地大輔，寺田真敏，千葉雄司，矢田健一，土居範久．“ バージョン情報をもちいた脆弱性ソフトウェア検査システムの検討 ”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2004 No.54 (May. 2004)

[2] 菊地大輔，寺田真敏，福澤淳二，土居範久．“ マルチベンダ環境の情報システムを対象とした脆弱性管理システムの検討 ”．情報処理学会 コンピュータセキュリティ シンポジウム 2005, pp.667-672 (Oct. 2005)

参考文献

[Apache] The Apache Software Foundation,
http://www.apache.org/

[Arvidsson01] J. Arvidsson, A. Cormack, Y. Demchenko and J. Meijer. "TERENA's Incident Object Description and Exchange Format Requirements". RFC3067 (Feb. 2001)
http://www.ietf.org/rfc/rfc3067.txt

[AVDL] Application Vulnerability Description Language (AVDL)
http://www.avdl.org/

[CERTa] Computer Emergency Response Team/Coordination Center (CERT/CC)
http://www.cert.org/

[CERTb] CERT/CC. "CERT/CC Advisories"
http://www.cert.org/advisories/

[CERT89] CERT/CC. "CA-1989-04: WANK Worm On SPAN Network". CERT Advisory CA-1989-04 (Oct. 1989)
http://www.cert.org/advisories/CA-1989-04.html

[CERT91] CERT/CC. "CA-1991-03: Unauthorized Password Change Requests Via Mail Messages". CERT Advisory CA-1991-03 (Apr. 1991)
http://www.cert.org/advisories/CA-1991-03.html

[CERT96a] CERT/CC. "CA-1996-01: UDP Port Denial-of-Service Attack". CERT Advisory CA-1996-01 (Feb. 1996)
http://www.cert.org/advisories/CA-1996-01.html

[CERT96b] CERT/CC. "CA-1996-06: CA-1996-06 Vulnerability in NCSA/Apache CGI example code". CERT Advisory CA-1996-06 (Mar. 1996)
http://www.cert.org/advisories/CA-1996-06.html

[CERT96c] CERT/CC. "CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks". CERT Advisory CA-1996-21 (Sep. 1996)
http://www.cert.org/advisories/CA-1996-21.html

[CERT96d] CERT/CC. "CA-1996-26: Denial-of-Service Attack via ping". CERT Advisory CA-1996-26 (Dec. 1996)
http://www.cert.org/advisories/CA-1996-26.html

[CERT97] CERT/CC. "CA-1997-28: IP Denial-of-Service Attacks". CERT Advisory CA-1997-28 (Dec. 1997)
http://www.cert.org/advisories/CA-1997-28.html

[CERT98] CERT/CC. "CA-1998-01: "smurf" IP Denial of Service Attacks". CERT Advisory CA-1998-01 (Jan. 1998)
http://www.cert.org/advisories/CA-1998-01.html

[CERT01a] CERT/CC. "CA-2001-23: Continued Threat of the "Code Red" Worm". CERT Advisory CA-2001-23 (Jul. 2001)
http://www.cert.org/advisories/CA-2001-23.html

[CERT01b] CERT/CC. "Trends in Denial of Service Attack Technology". (Oct. 2001)
http://www.cert.org/archive/pdf/DoS_trends.pdf

[CERT01c] CERT/CC. "CA-2001-26: Nimda Worm". CERT Advisory CA-2001-26 (Aug. 2001)
http://www.cert.org/advisories/CA-2001-26.html

[CERT02a] CERT/CC. "CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)". CERT Advisory CA-2002-03 (Feb. 2002)
http://www.cert.org/advisories/CA-2002-03.html

[CERT02b] CERT/CC. "CA-2002-17: Apache Web Server Chunk Handling Vulnerability". CERT Advisory CA-2002-17 (Jun. 2002)
http://www.cert.org/advisories/CA-2002-17.html

[CERT02c] CERT/CC. "CA-2002-18: OpenSSH Vulnerabilities in Challenge Response Handling". CERT Advisory CA-2002-18 (Jun. 2002)
http://www.cert.org/advisories/CA-2002-18.html

[CERT02d] CERT/CC. "CA-2002-19: Buffer Overflows in Multiple DNS Resolver Libraries". CERT Advisory CA-2002-19 (Jun. 2002)
http://www.cert.org/advisories/CA-2002-19.html

[CERT02e] CERT/CC. "CA-2002-23: Multiple Vulnerabilities In OpenSSL". CERT Advisory CA-2002-23 (Jul. 2002)
http://www.cert.org/advisories/CA-2002-23.html

[CERT03a] CERT/CC. "CA-2003-15: Cisco IOS Interface Blocked by IPv4 Packet". CERT Advisory CA-2003-15 (Jul. 2003)
http://www.cert.org/advisories/CA-2003-15.html

[CERT03b] CERT/CC. "CA-2003-24: Buffer Management Vulnerability in OpenSSH". CERT Advisory CA-2003-24 (Sep. 2004)
http://www.cert.org/advisories/CA-2003-24.html

[CERT03c] CERT/CC. "IN-2003-03: W32/Sobig.F Worm". CERT Incident Note IN-2003-03 (Sep. 2003)
http://www.cert.org/incident_notes/IN-2003-03.html

[Chris04] Chris Eagle. "Attacking Obfuscated Code with IDA Pro". Black Hat 2004 (Oct. 2004)

[CIAC] U.S. DOE-CIAC (Computer Incident Advisory Capability). "CIAC Bulletins"
http://www.ciac.org/cgi-bin/index/bulletins

[CVE] Common Vulnerabilities and Exposures (CVE)
http://cve.mitre.org/

[Dan04] Dan Ellis, Jack Aiken, Kira Attwood and Scott Tenaglia. "A Behavioral Approach to Worm Detection", ACM Workshop on Rapid Malcode (WORM 2004) (Oct. 2004)
http://www.icir.org/vern/worm04/worm04-program.html

[Danlyliw05] R. Danyliw, J. Meijer and Y. Demchenko. "The Incident Object Description Exchange Format Data Model and XML Implementation". draft-ietf-inch-iodef-04.txt (Aug. 2005)
http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-04.txt

[Disclosure] [Full-Disclosure] Mailing List Charter
http://lists.grok.org.uk/full-disclosure-charter.html

[Disclosure04] [Full-Disclosure] Sasser skips 10.x.x.x Why?
http://archives.neohapsis.com/archives/fulldisclosure/2004-05/0091.html

[Dshield] Distributed Intrusion Detection System,
http://www.dshield.org/

[eEye] eEye Digital Security. “Retina Single Audit Scanners”.
http://www.eeye.com/html/resources/downloads/index.html

[eEye03] eEye Digital Security. "MSBlaster worm disassembly by eEye Digital Security, Inc.". (Aug. 2003)
http://www.eeye.com/html/Research/Advisories/Blaster_Analysis.txt

[eEye04] eEye Digital Security. "ANALYSIS: Sasser Worm" (May. 2004)
http://www.eeye.com/html/research/advisories/AD20040501.html

[Ethereal] Ethereal. "A Network Protocol Analyzer".
http://www.ethereal.com/

[FIRST90] Forum of Incident Response and Security Teams (FIRST)
http://www.first.org/

[Foundstone] Foundstone, Inc. “Free Tools".
http://www.foundstone.com/resources/freetools.htm

[Fsecure05a] F-Secure. "New worm using a fresh exploit found" (Aug. 2005)
http://www.f-secure.com/weblog/archives/archive-082005.html#00000624

[Fsecure05b] F-Secure. "This is not a viruswar, this is a botwar!" (Aug. 2005)
http://www.f-secure.com/weblog/archives/archive-082005.html#00000631

[Honeynet] The Honeynet Project.
http://project.honeynet.org/

[IBM05] IBM. "IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005" (Aug. 2005)
http://www-1.ibm.com/press/PressServletForm.wss?MenuChoice=pressreleases&TemplateName=ShowPressReleaseTemplate&SelectString=t1.docunid=7815&TableName=DataheadApplicationClass&SESSIONKEY=any&WindowTitle=Press+Release&STATUS=publish

[IPA99] 情報処理推進機構. “Malwareに関する見通し：EICAR99 (European Institute for Computer Anti- Virus Research ”(1999)
http://www.ipa.go.jp/security/fy10/contents/virus/3_1_3.html

[IPA01] 情報処理推進機構. “新種ウイルス W32/Nimda に関する情報”
http://www.ipa.go.jp/security/topics/newvirus/nimda.html

[IPA05] 情報処理推進機構. “新種ワーム「W32/Sasser」に関する情報”
http://www.ipa.go.jp/security/topics/newvirus/sasser.html

[ISSa] Internet Security Systems. "X-Force Database"
http://xforce.iss.net/xforce/search.php

[ISSb] Internet Security Systems. “AlertCon Status”
http://www.isskk.co.jp/MSS/gtoc.html

[ISSc] Internet Security Systems. "Product Utilities"
http://www.iss.net/support/product_utilities/

[ISS04] Internet Security Systems. “Internet Security Systems セキュリティ アラート: ISS 製品における ICQ 解析の脆弱点”(Mar. 2004)
http://www.isskk.co.jp/support/techinfo/general/ICQ_ISS_166.html

[ISS05] Internet Security Systems. “Internet Security Systems セキュリティ アラート: Windows プラグ アンド プレイによるリモートからのセキュリティ侵害”(Aug. 2005)
http://www.isskk.co.jp/support/techinfo/general/win_plugandplay_202.html

[JPCERTa] Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC)
http://www.jpcert.or.jp/

[JPCERTb] JPCERT/CC. “JPCERT/CC に関してよくある質問と答え”
http://www.jpcert.or.jp/faq.txt

[JPCERTc] JPCERT/CC. “Internet Scan Data Acquisition System (ISDAS)”
http://www.jpcert.or.jp/isdas/

[JPCERT04] JPCERT/CC. “JPCERT/CC インシデント情報交換システムの稼動を開始”
http://www.jpcert.or.jp/press/2004/0317.txt

[JVNRSS] JVN.“JVNJS/RSSとは”.
http://jvn.jp/rss/

[JVN03a] JVN. “TRIN-2003-03: W32/Sobig.F ワーム”(Dec. 2003)
http://jvn.jp/tr/TRIN-2003-03/index.html

[JVN03b] JVN. “TRCA-2003-17: Cisco IOS サービス運用妨害に関する脆弱性の攻略”(Jul. 2003)
http://jvn.jp/tr/TRCA-2003-17/index.html

[JVN03c] JVN. “TRCA-2003-24: OpenSSH のバッファ管理機構に脆弱性”(Sep. 2003)
http://jvn.jp/tr/TRCA-2003-24/index.html

[Mihai03] Mihai Christodorescu and Somesh Jha. "Static Analysis of Executables to Detect Malicious Patterns", 12th USENIX Security Symposium (2003)
http://www.usenix.org/events/sec03/tech/christodorescu.html

[MSa] マイクロソフト. “Microsoft TechNet: セキュリティ センター”
http://www.microsoft.com/japan/technet/security/

[MSb] マイクロソフト. “Microsoft Internet Information Server”.
http://www.microsoft.com/japan/products/iis/

[MS00] マイクロソフト. “Web サーバー フォルダへの侵入の脆弱性に対する対策 (MS00-078)”(Oct. 2000)
http://www.microsoft.com/japan/technet/security/bulletin/MS00-078.mspx

[MS01] マイクロソフト. “Index Server ISAPI エクステンションの未チェックのバッファにより Web サーバーが攻撃される (MS01-033)”(Jan. 2001)
http://www.microsoft.com/japan/technet/security/bulletin/MS01-033.mspx

[MS02] マイクロソフト. “SQL Server 2000 解決サービスのバッファのオーバーランにより, コードが実行される(323875) (MS02-039)”(2002)
http://www.microsoft.com/japan/technet/security/bulletin/MS02-039.mspx

[MS03] マイクロソフト. “RPC インターフェイスのバッファ オーバーランによりコードが実行される (823980) (MS03-026)”(Jul. 2003)
http://www.microsoft.com/japan/technet/security/bulletin/MS03-026.mspx

[MS04] マイクロソフト. “Microsoft Windows のセキュリティ修正プログラム (835732) (MS04-011)”(Apr. 2004)
http://www.microsoft.com/japan/technet/security/bulletin/MS04-011.mspx

[NAT] Guide to IP Layer Network Administration with Linux, Destination NAT with netfilter (DNAT)
http://linux-ip.net/html/nat-dnat.html

[Niels04] Niels Provos. "A Virtual Honeypot Framework", 13th USENIX Security Symposium (2004)
http://www.usenix.org/events/sec04/tech/provos.html

[NVD] NIST. "National Vulnerability Database"
http://nvd.nist.gov/

[OSVDB] Open Source Vulnerability Database (OSVDB)
http://www.osvdb.org/

[OVAL] Open Vulnerability Assessment Language (OVAL)
http://oval.mitre.org/

[police] 警察庁セキュリティポータルサイト@police. “インターネット定点観測”
http://www.cyberpolice.go.jp/detect/observation.html

[police03a] 警察庁セキュリティポータルサイト@police. “W32/SQLSlammer” (Jan. 2003)
http://www.cyberpolice.go.jp/server/virus/pdf/Slammer_jp_20030104_report.pdf

[police03b] 警察庁セキュリティポータルサイト@police. “W32.Blaster.Worm”(Aug. 2003)
http://www.cyberpolice.go.jp/server/virus/pdf/W32_Blaster_Worm_Mix.pdf

[police03c] 警察庁セキュリティポータルサイト@police. “W32/CodeRed.F” (Oct. 2003)
http://www.cyberpolice.go.jp/server/virus/pdf/W32CodeRed_F_jp_20030302.pdf

[police05] 警察庁セキュリティポータルサイト@police.“複数の脆弱性を悪用するGaobot ワームについて”. (Jul. 2005)
http://www.cyberpolice.go.jp/detect/pdf/report_gaobot.pdf

[SF] SecurityFocus
http://www.securityfocus.com/

[symantec] symantec. "ThreatCon Definitions"
https://tms.symantec.com/threatCon_Def.asp

[Stuart02] Stuart Staniford, Vern Paxson and Nicholas Weaver. "How to 0wn the Internet in Your Spare Time", 11th USENIX Security Symposium (2002)
http://www.icir.org/vern/papers/cdc-usenix-sec02/

[TrendMicro] トレンドマイクロウイルストラッキングセンター
http://www.trendmicro.com/jp/security/map/overview.htm

[USCERT] US-CERT. "US-CERT Vulnerability Notes Database"
http://www.kb.cert.org/vuls

[USCERT05a] US-CERT. "Targeted Trojan Email Attacks". US-CERT Technical Cyber Security Alert TA05-189A (Jul. 2005)
http://www.us-cert.gov/cas/techalerts/TA05-189A.html

[USCERT05b] US-CERT. “Summary of Security Items from May 4 through May 10, 2005”. US-CERT Cyber Security Bulletin SB05-131 (May. 2005)
http://www.us-cert.gov/cas/bulletins/SB05-131.html

[Williamson02] M.M. Williamson. "Throttling Viruses: Restricting propagation to defeat malicious mobile code". 18th Annual Computer Security Applications Conference (ACSAC) (Dec. 2002)

[Yoshida01] Eiji James Yoshida. “受動的攻撃検証サイト”. (2001)
http://isweb27.infoseek.co.jp/computer/zaddik/index.html

[Zoneh04] Zone-H. "Zone-H 2004 statistics are ready to be downloaded". (2005)
http://www.zone-h.org/en/news/read/id=4457/

[伊沢05] 伊沢亮一，市川幸宏，白石善明，毛利公美，森井昌克．“ウイルス解析支援システムの開発 --- コード解析結果からのウイルス活動把握の自動化 ---”．情報処理学会，コンピュータセキュリティシンポジウム2005 (2005)

[梅澤05] 梅澤昭生，横地裕，田中貴志，門脇正．“コンピュータセキュリティインシデントとその対応支援システム”．FIT2005 (Sep. 2005)

[大宅05] 大宅裕史，櫨山寛章，門林雄基．“ワームの拡散遅延を目的とした検知・遮断機構の提案”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2005 No.33 (2005)

[大林98] 大林正英，石田晴久．“インターネットにおける不正アクセス対応とJPCERT/CC”．電子情報通信学会 FACE98-24, pp.23-27 (Dec. 1998)

[岡本04] 岡本剛．“DNSの正引き応答を利用したパケットフィルタリングによるコンピュータワームの増殖抑制”．情報処理学会論文誌 Vol.45 No.10 (2004)

[面03] 面和成，鳥居悟．“ワームによるランダムスキャンの検知方式の検討”．情報処理学会 コンピュータセキュリティシンポジウム2003 (Oct. 2003)

[角04] 角将高，馬場達也，稲田勉．“動的VLAN制御による脆弱ホスト保護方式の提案”．情報処理学会 コンピュータセキュリティシンポジウム2004 (Oct. 2004)

[角05] 角将高，馬場達也，稲田勉．“動的VLAN制御による統合ワーム対策システムの提案”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2005 No.33 (Mar. 2005)

[片岡05] 片岡真紀，石毛由美子，葛谷暢崇，大橋史治．“囮サーバで送受信されたパケット系列を統計分析することによるワーム検知システムの提案”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2005 No.70 (2005)

[神薗03] 神薗雅紀，白石善明，森井昌克．“仮想ネットワークを使った未知ウイルス検知システム”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2003 No.022-016 (Jul. 2003)

[共立03] “情報セキュリティ事典”．共立出版 (2003)

[経産省03] 経済産業省．“情報セキュリティ総合戦略”
http://www.meti.go.jp/policy/netsecurity/strategy.htm

[小泉04] 小泉芳，小池英樹，安村通晃．“行動制限型ハニーポットの改良方法の提案・実装・運用”．情報処理学会 コンピュータセキュリティ 研究報告Vol.2004 No.129 (Dec. 2004)

[小山05] 小山覚. “ボットネット実態調査結果”. Black Hat Japan 2005 (Oct. 2005)

[澁谷04] 澁谷芳洋，小池英樹，高田哲司，安村通晃，石井威望. “高対話型おとりシステムの運用経験に関する考察”. 情報処理学会論文誌 Vol.45 No.8 (Aug. 2004)

[関04] 関聡司，佐々木良一，岩村充. “コンピュータ・ウイルス対策における疫学的アプローチに関する研究（その１） ～ウイルス拡散・制御シミュレータの開発～”. 情報処理学会 コンピュータセキュリティ 研究報告 Vol.2004 No.54 (2004)

[総務省05] 総務省. “次世代IPインフラ研究会 報告書（案） 情報セキュリティ政策2005の提言”. (2005)
http://www.soumu.go.jp/s-news/2005/pdf/050525_2_02.pdf

[高橋04] 高橋正和，佐々木良一. “ワームの特性に基づく拡散モデルの提案と適用”. 情報処理学会 コンピュータセキュリティシンポジウム 2004 (Oct. 2004)

[寺田02] 寺田真敏，土居範久. “JPCERT/CC Vendor Status Notes DB 構築に関する検討”，情報処理学会 コンピュータセキュリティシンポジウム 2002 (Oct. 2002)

[寺田03] 寺田真敏，土居範久. “RDF Site Summaryを用いたセキュリティ情報流通に関する検討”. 情報処理学会 コンピュータセキュリティ 研究報告 Vol.2003 No.021 (Jul. 2003)

[寺田04] 寺田真敏, 城戸博之, 菊池大輔, 高田眞吾, 土居範久. “Status Tracking Notes；時系列イベント情報の共有”. 情報処理学会 コンピュータセキュリティ 研究報告Vol.2004 No.025 (May. 2004)

[寺田05] 寺田真敏. “マイクロソフトの脆弱性を悪用するワームやボットの発生度合い”.
http://www.doi.ics.keio.ac.jp/%7Eterada/fdin/TA05-221A.htm

[中野99] 中野喜之，礒川弘実，萱島信，寺田真敏，山崎隆行. “分散ネットワークサービス管理のためのセキュア通信基盤の開発”. 情報処理学会 コンピュータセキュリティ 研究報告 Vol.1999 No.007 (Jan. 1999)

[東角05] 東角芳樹，面和成，鳥居悟. “ワームのランダムスキャンによる検知の高速化方式の提案”. 情報処理学会，コンピュータセキュリティシンポジウム2005 (Oct. 2005)

[広岡04] 広岡俊彦，市川幸宏，白石善明，森井昌克，中尾康二. “ウイルスの挙動を解析するための実ネットワークを使った仮想感染ネットワークの設計”. 情報処理学会 コンピュータセキュリティシンポジウム2004 (Oct. 2004)

[三宅02] 三宅崇之，白石善明，森井晶克．“仮想サーバを使った未知ウイルス検知システムの提案”．情報処理学会 コンピュータセキュリティ 研究報告 Vol.2002 No.018-008 (Jul. 2002)

[三輪04] 三輪信介，大野浩之．“持ち込みPC検疫機構の設計と実装”．情報処理学会 コンピュータセキュリティシンポジウム2004 (Oct. 2004)

[横山05] 横山恵一，田中英彦．“イントラネットにおけるIPv6検疫ネットワークシステムの提案”．情報処理学会 コンピュータセキュリティシンポジウム2005 (Oct. 2005)