



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

15 情経第 1675 号

未知ウイルス検出技術に関する調査

実験報告書

2004 年 4 月
独立行政法人 情報処理推進機構

(空白ページ)

目次

1	はじめに.....	1
2	背景と目的.....	2
2.1	背景.....	2
2.2	目的.....	2
2.3	用語の定義.....	2
3	調査・検討結果.....	4
3.1	未知ウイルス検出手法に関する検討.....	4
3.1.1	未知ウイルス検出手法の検討.....	4
3.1.2	未知ウイルス検出手法プロトタイプの概要.....	6
4	評価実験.....	8
4.1	実験環境.....	9
4.2	実験準備.....	10
4.3	実験結果.....	11
4.3.1	W32/Lovsan.worm.gen.....	13
4.3.2	W32/Lovsan.worm.a.....	17
4.3.3	W32/Lovsan.worm.e.....	20
4.3.4	W32/Nachi.worm.....	23
4.3.5	W32/Hybris.gen@MM.....	28
4.3.6	W32/Magistr.a@MM.....	29
4.3.7	W32/Magistr.b@MM.....	31
4.3.8	W32/CodeRed.worm.c.....	33
4.3.9	W32/CodeRed.worm.f.....	37
4.3.10	W32/CodeGreen.dr.....	41
4.3.11	W32/Klez.gen@MM.....	44
4.3.12	W32/Klez.h@MM.....	47
4.3.13	W32/Klez.e@MM.....	49
4.3.14	W32/Nimda.gen@MM.....	51
4.3.15	W32/Nimda@MM.....	53
4.3.16	W32/Nimda.s@MM.....	55
4.3.17	W32/SirCam@MM.....	60
4.3.18	W32/Sobig.a@MM.....	62
4.3.19	W32/Sobig.f@MM.....	64
4.3.20	W32/Rous.a.....	65
5	まとめ.....	67

1 はじめに

本報告書は、コンピュータウイルスの検出技術の調査結果より未知ウイルスを検出するための新しい手法を検討、模擬実装し、その結果を報告するものである。

実験に用いたウイルスは下記の 11 ファミリー 20 検体である。なお、ウイルス名称は Network Associates 社の McAfee VirusScan で表示されたものを用いている。

ウイルス名	検体ファイル名
W32/Lovsan.worm.gen	W32BLASTER_C.EXE
W32/Lovsan.worm.a	msblaster.exe
W32/Lovsan.worm.e	W32BLASTER_E.EXE
W32/Nachi.worm	welchia.exe
W32/Hybris.gen@MM	i-worm.hybris.c.exe
W32/Magistr.a@MM	vs000021.exe
W32/Magistr.b@MM	W32MAGIC.EXE
W32/CodeRed.worm.c	W32CDRX.BIN
W32/CodeRed.worm.f	W32CDRFX.BIN
W32/CodeGreen.dr	W32CDGR.EXE
W32/Klez.gen@MM	W32KLEZ.EXE
W32/Klez.h@MM	setup.exe
W32/Klez.e@MM	value.bat
W32/Nimda.gen@MM	nimda.exe
W32/Nimda@MM	read.exe
W32/Nimda.s@MM	sample.exe
W32/SirCam@MM	SCam32.exe
W32/Sobig.a@MM	W32SOBIG.EXE
W32/Sobig.f@MM	sobig-f/sobig.f.pif
W32/Rous.a	i-worm.rous.a.exe

2 背景と目的

2.1 背景

インターネットの急速な普及に伴い、電子メールや Web サイトの閲覧を通じてコンピュータウイルス(以下ウイルスと呼ぶ)に感染する被害が増えている。オリジナルを一部改変した多くの亜種ウイルス、自らのプログラムの一部を自ら変更するウイルス等があり、これらについては、従来のワクチンソフトが採用している単純な定義ファイルとの比較を主としたパターンマッチングによる手法では即時の対応・発見が困難である。そのため、定義ファイルが作成されていないウイルスの感染が瞬時に拡大する危険性がある。

2.2 目的

本調査では、従来の手法とは異なるアプローチによる未知ウイルスの検出技術について、技術開発の現状を把握するとともに、有効な検出手法の分析・検討を行う。

発表された論文や技術情報を元に技術開発の現状を調査し、手法について分類比較等に基づいた分析を行う。さらに、この分析を基に未実現のウイルス検出技術についても検討を行い、プロトタイプ方式の提案と評価実験を行う。

本調査は、調査および実験の結果を、ウイルス対策技術の開発のための参考資料として、またウイルス解析業務の基礎資料として活用可能な報告とすることを目的とする。新たなウイルス検出手法の有効性の確認により、これらの実用化と普及、社会のウイルス対策の一層の進展へ貢献することを目指すものである。

なお、本報告書では、新しい未知ウイルス検出手法の検討とそのプロトタイプの提案、評価実験について記載しており、これの元になる従来のウイルス検出技術に関する調査結果とその分析等は別紙にて報告する。

2.3 用語の定義

本報告書で使用する用語を以下の通り定義する。

ウイルス

通商産業省(現経済産業省)告示第 952 号「コンピュータウイルス対策基準」¹のコンピュータウイルスの定義に準ずる。

コンピュータウイルス (以下「ウイルス」とする。)

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

(1) 自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2) 潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3) 発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

要するに、他のファイルやシステムに感染して拡散するものや単独で拡散するもので、他に悪影響を与える不正なプログラムを総じてウイルスと呼ぶ。これは広義のウイルスであり、不正プログラムとも呼ばれる。

感染

ウイルスが他のファイルやシステムに自分自身をコピーすること。通常、それらのファイルやシステムが実行される際にウイルスのコピーが動作するよう対象を改変する。この感染機能を持つ不正プログラムが狭義のウイルスであり、感染動作を行わず、単独で伝搬、拡散するものをワームとも呼ぶ。

ウイルス検出

あるファイルやシステムがウイルスに感染しているか、あるいはウイルスファイルそのものかどうかを判断すること。

ウイルス対策

ウイルスの検出・駆除や、ウイルスの感染を防止するための方策。一般的にはワクチンを用いる。

駆除

ウイルスに感染しているファイルやシステムから、ウイルスのみをきれいに取り除くこと。

ウイルスによっては感染の際に対象のファイルに上書きするなど、元のファイルを壊してしまうことがあるが、その場合はウイルス部分のみを安全に取り除くことはできないため、ファイル全体を削除したり、原本のファイルを再インストールするなどして復旧する必要がある。

ワクチン

ウイルスを検出・駆除するためのソフトウェア。ウイルススキャナ、アンチウイルスなどとも呼ばれる。

未知ウイルス

新種、または既存のウイルスを改変した亜種または変種と呼ばれるウイルスで、その機能が未分析のもの。機能が分析済みで、命名され、検出方法が確立されたウイルスは既知ウイルスと呼ばれる。

3 調査・検討結果

3.1 未知ウイルス検出手法に関する検討

ここでは、既存のウイルス検出手法の調査結果(別紙、調査報告書参照)から未知ウイルスの検出手法について検討を行い、プロトタイプ的设计を行う。

3.1.1 未知ウイルス検出手法の検討

ウイルス検出手法および侵入検出手法に関する調査・分析の結果に基づき、未知ウイルス検出手法について検討を行った結果を以下に示す。また、ウイルス検出の核となるコア技術やその具体的な実装技術について実現可能な新しい手法の検討も行っている。

(1) 未知ウイルス検出手法として有望な手法

未知ウイルスを検出することが可能なコア技術としては、インテグリティチェック法、ヒューリスティック法、ビヘイビア法が挙げられる。

インテグリティチェック法

手法: ハッシュとデジタル署名を利用して、プログラムの内容が変化したことを検出する。

利点: 主に感染行動型のウイルスに対応。チェック対象をプログラムファイルだけでなく、ディレクトリエントリやシステムレジストリの重要な部分などに広げることで、ファイル感染を行わないワームなどによる改変にも対応できる可能性がある。検査対象を実行しないで検査できる。検査に要する時間は比較的短い。

欠点: 事前に、ウイルスに感染していない状態のプログラムすべてにデジタル署名を施しておく必要がある(署名のない未知のプログラムは実行できない)。ウイルスの種類は判別できない(そもそも変化の原因がウイルスかどうかもわからない)。システム領域感染型でコンピュータの起動時にメモリに常駐するステルス型ウイルスの場合は、チェック自体が欺かれる恐れがある(メモリ常駐プログラムをチェックする他の手法と併用することが望ましい)。

ヒューリスティック法

手法: プログラムの挙動をルールベースで静的に解析する。

利点: 感染行動型のウイルスにも拡散行動型のワームにも対応。検査対象を実行しないで検査できる。検査に要する時間は比較的短い。

欠点: あらかじめ良質のルールを定義しておく必要がある。コードの読み込みを妨害するステルス型や、静的な解析の困難な暗号化型、多形態型等のウイルスには向かない。

ビヘイビア法

手法: プログラムの挙動をルールベースで動的に解析する。

利点: 危険な動作そのものを検出して阻止できるため、被害を防ぐ可能性が高い。暗号化型や多形態型、自己改変型やネットワーク型など、ほとんどのウイルスに有効。

欠点: モニタリングやエミュレーション等の高度な技術が必要になる。プログラムを実行して検査するため、ウイルスの活動条件によっては危険な動作を起こさず、検出できない恐れがある。仮想環境での実行の場合は、実環境との違いをチェックして活動を起こさないウイルスもあり得る。プログラムを一通り実行する必要があるため、検査に要する時間は比較的長い。

以上の通り、その利点から、未知ウイルスを検出するための新しい手法を検討するには、まずビヘイビア法の実装技術に注目することが重要であると考ええる。

(2) 新たな未知ウイルス検出手法の検討

ここでは、ビヘイビア法の実装技術を中心に、未知ウイルスを検出可能な手法を考案し、その可能性および有効性について検討した結果を示す。

なお、今回は運用技術に関するもの(パターンの更新方法やネットワーク経由の管理方法など)や検出処理の効率化に関するもの(データベース検索の高速化手法)など、検出手法に直接関係しないものは対象外とした。

ファイル構造のチェック(案)

手法: アセンブラ、コンパイラ、リンカなどのプログラム開発ツールが出力するオブジェクトコードや実行可能コードにはそれぞれ特徴的な部分がある。これらのツールで素直に作成されたプログラムファイルは、その特徴を残した綺麗な構造をしていると考えられる。これに対し、感染行動型ウイルスによって内容が改変されると、EXE ヘッド、コードセグメント、データセグメントなどのファイル内部の構造が乱れてしまう可能性がある。この乱れをうまく判断することができれば、ファイルの改変(ウイルスの感染)を検出することも可能である。

利点: プログラムコードを分析しないため、非常に高速にチェックできる可能性がある。

欠点: 構造の乱れが判断できない(検出率が低い)恐れがある。感染しないワームなどには対応できない。

ファイルシステムの監視によるワーム検出(案)

手法: 単体ファイルのチェックではなく、OS を構成するシステムファイル群やレジストリ等をチェックする。具体的には、不正な実行ファイルの設置などを、ディレクトリエントリやファイルアロケーションテーブルの監視により検出する。そのファイルを自動実行させるようにレジストリを書き換えたならば、それはワームであると判断する。

利点: 実装が容易。受動的検出による処理負荷の軽減。ワームに対応。

欠点: 検査項目が単純なため、誤認の恐れがある。

セキュリティホール攻撃のチェック(案)

手法: セキュリティホールを狙うワームに注目し、その攻撃に特徴的な活動からルールベースによって検出する。

利点: ワームに対応。

欠点: ワーム以外には非対応。

新しいルール生成法を用いたビヘイビア検出手法(案)

手法: ビヘイビア法のルールをより高精度なものにするための学習アルゴリズムを検討する。例えばニューラルネットの利用や、隠れマルコフモデルなどウイルスの行動事象の統計的な予測モデルの応用などは、更なる検討の余地がある。

利点: ビヘイビア法の検出精度が向上する可能性がある。

欠点: 採用するモデルの選択には実験を重ねる必要があり、短期間の実装は困難。

3.1.2 未知ウイルス検出手法プロトタイプ概要

以下、前項のリストから本調査期間において実験可能なものを選択し、その検出手法を実装した評価実験用のプロトタイプを設計・作成する。

ここでは、セキュリティホールを狙って単体でネットワーク内を徘徊するワームの動作に注目し、それに対応する検出手法を設計案として提示する。

現在、セキュリティホールを突いたウイルスが問題視されている。2003年8月のBlasterウイルス(ワーム)の被害は甚大なものであった²。市販のワクチンを導入していたにもかかわらず被害に遭ったというホームユーザが多かったのみならず、ワームの拡散行動がネットワークを麻痺させた。

このようなウイルスは、セキュリティホールを突く exploit と呼ばれるコードを悪用し、作成される。通常、セキュリティホールの情報は、それを発見した研究者などによって公開され、それを修正するためのパッチがオペレーティングシステムやアプリケーションソフトウェアのベンダなどから提供される。しかし、前述のように、パッチを適用していないユーザがセキュリティホールを悪用したウイルスの被害に遭う事例が多数報告されている。

一般に、セキュリティホールの情報が公開されてから、それを悪用するウイルスが出現するまでには多少の時間がかかるだろう。もしその情報をいち早く入手し、対策を取ることができれば、ウイルスが作成される前に対策できることになり、理想的な未知ウイルス検出手法といえるだろう。

すなわち、セキュリティホールが見つかった特定のポートを監視し、それを悪用して侵入してシステムに常駐するようなファイルをウイルスとして検出する。

なお、ファイアウォールでポートを完全に塞ぐのではなく、サービス可能な状態のままウイルスが侵入した場合はそれを検出できるため、本手法の有用性は高いと考える。

完成予想図としては、セキュリティホールの情報を収集し提供するサーバと、それを入手し対応するクライアント側のウイルス検出プログラムで構成されるシステムになるであろうが、本調査ではウイルス検出部の動作を検証するためのプロトタイプの作成と、その有効性の検証を行うこととする。

以下、クライアント側のウイルス検出プログラムについて説明する。

ここでは、セキュリティホールの情報はあらかじめ入手しているものとし、ウイルス検出プログラムはこの情報をもとに特定のポートを監視する。そして、そのポートに何らかのデータが送られてきた場合には特定のディレクトリ(OSのシステムディレクトリなど)の監視を開始し、ディレクトリ下のファイル追加/変更/削除/リネームといった変化を危険な兆候と判

断してユーザに変化の内容を報告するものである。

今回、実験用に作成したウイルス検出プログラムの動作フローを図 3-1に示す。

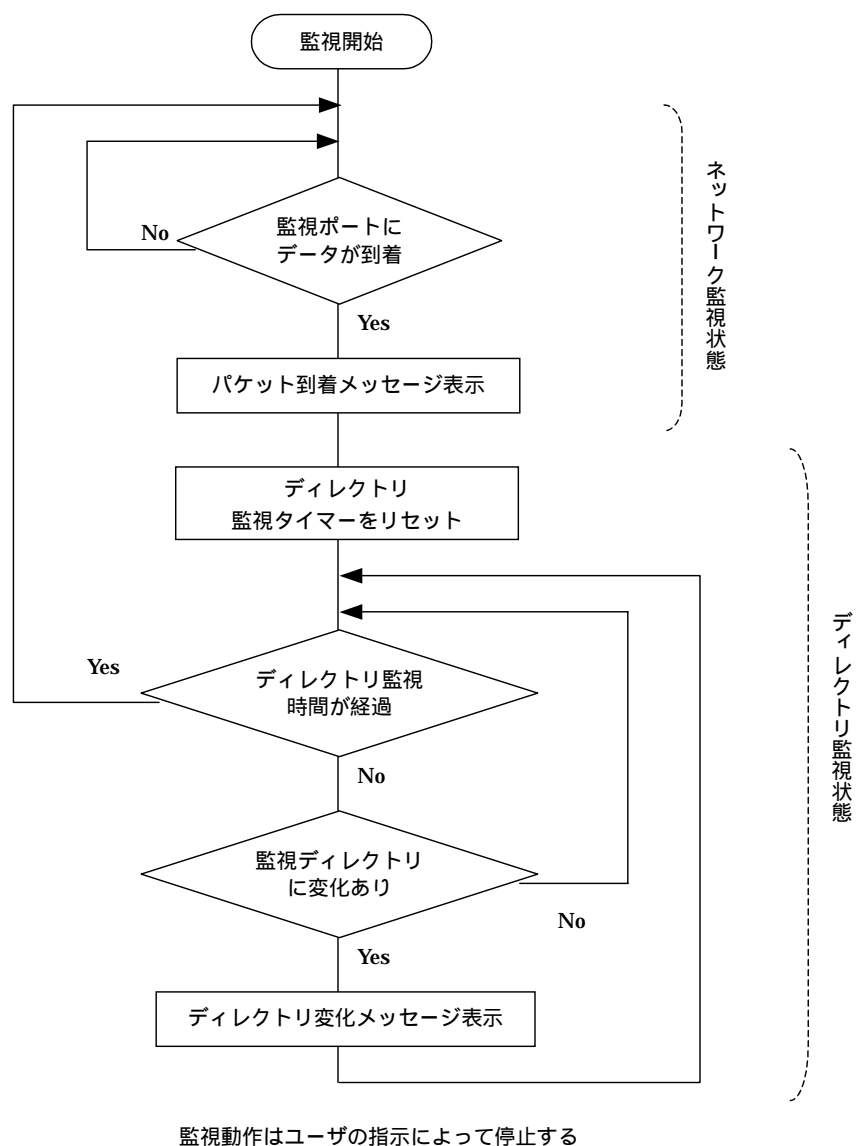


図 3-1 動作フロー

この図からも明らかなように、このウイルス検出プログラムはネットワーク上の他のマシンから自マシンに接続して侵入・感染を試みるタイプのウイルスを対象としている。メールサーバに接続して受信メールを取り込む、受信メールや Web のブラウズを行う、受信メールの添付ファイルを実行するなどの人為的な操作を伴うケースは検出動作の契機としていないため、メール添付で拡散するようなウイルスについては検出対象としない。

4 評価実験

実験用に作成したプロトタイプを使い、新たな未知ウイルス検出手法の可能性・有効性に関する評価実験を行う。Windows 環境で動作する実際のウイルス検体を用いた検出実験を、ネットワークから隔離された実験環境を構築して行う。

ウイルス検体としては以下の 11 ファミリー 20 検体を用いる。

ウイルス名	検体ファイル名
W32/Lovsan.worm.gen	W32BLASTER_C.EXE
W32/Lovsan.worm.a	msblaster.exe
W32/Lovsan.worm.e	W32BLASTER_E.EXE
W32/Nachi.worm	welchia.exe
W32/Hybris.gen@MM	i-worm.hybris.c.exe
W32/Magistr.a@MM	vs000021.exe
W32/Magistr.b@MM	W32MAGIC.EXE
W32/CodeRed.worm.c	W32CDRX.BIN
W32/CodeRed.worm.f	W32CDRFX.BIN
W32/CodeGreen.dr	W32CDGR.EXE
W32/Klez.gen@MM	W32KLEZ.EXE
W32/Klez.h@MM	setup.exe
W32/Klez.e@MM	value.bat
W32/Nimda.gen@MM	nimda.exe
W32/Nimda@MM	read.exe
W32/Nimda.s@MM	sample.exe
W32/SirCam@MM	SCam32.exe
W32/Sobig.a@MM	W32SOBIG.EXE
W32/Sobig.f@MM	sobig-f/sobig.f.pif
W32/Rous.a	i-worm.rous.a.exe

主に、検出率、誤検出率について測定を行う。

提案手法が検出の主対象とするウイルスとそれ以外のウイルスについて、それぞれ検出率、誤検出率を測定し、その有効性の評価を行う。

4.1 実験環境

今回、実験で使用する動作環境は、ウイルス検出プログラムが動作するマシン（以降感染先マシンと記述する）と、ウイルスを拡散するマシン（以降攻撃マシンと記述する）とで構成する。使用した機器はネットワーク環境の構築及び、繰り返して実験を行うためにマシン初期設定を容易に行えるようパソコン（以降実マシンと記述する）上の仮想マシンにて構築することとした。仮想マシンはVMware Workstation 4.0を使用した。表 4-1に実マシンのスペックを、図 4-1に実験環境イメージを示す。

表 4-1 実マシンスペック

CPU	OS	メモリ
Pentium 800MHz	Windows XP Professional	640MB

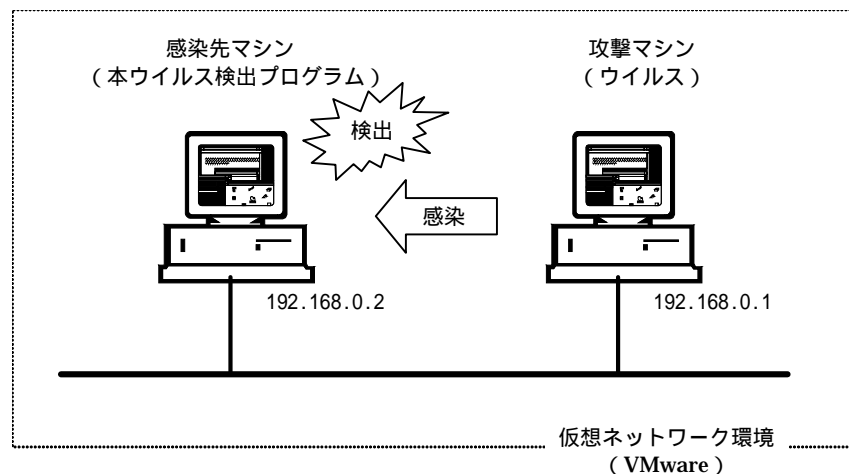


図 4-1 実験環境イメージ

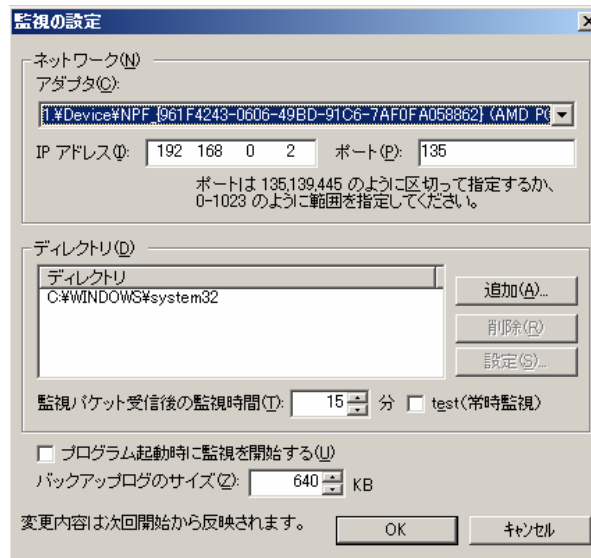
実験は次の手順に従って実施した。

感染先マシンでウイルス検出プログラムを起動し、監視を開始する。
攻撃マシンでウイルスを動作させ、感染先コンピュータへの感染を誘発する。
感染先コンピュータでウイルス検出プログラムが感染を検出するかどうか（ディレクトリの変化を検出するかどうか）を確認する。

なお、実験ウイルスにより仮想マシンの環境は異なるため、仮想マシン環境の詳細は実験結果の各ウイルスの説明にて記載する。

4.2 実験準備

攻撃マシン、感染先マシンを起動し、感染先マシンにてウイルス検出プログラムを起動した。ウイルス検出プログラムは、特定サービスポートへのアクセスを契機として指定するディレクトリを監視する。設定画面イメージを図 4-2に、ウイルス検出プログラムで監視を開始したときの開始画面イメージを図 4-3に示す。



IP アドレス	: 感染先マシン IP アドレス
ポート	: 実験ウイルスが攻撃の際使用する脆弱性に関するポートを指定
監視対象ディレクトリ	: 実験ウイルス毎に監視ディレクトリを指定
監視時間	: 15 分
ログサイズ	: 640KB

図 4-2 設定画面

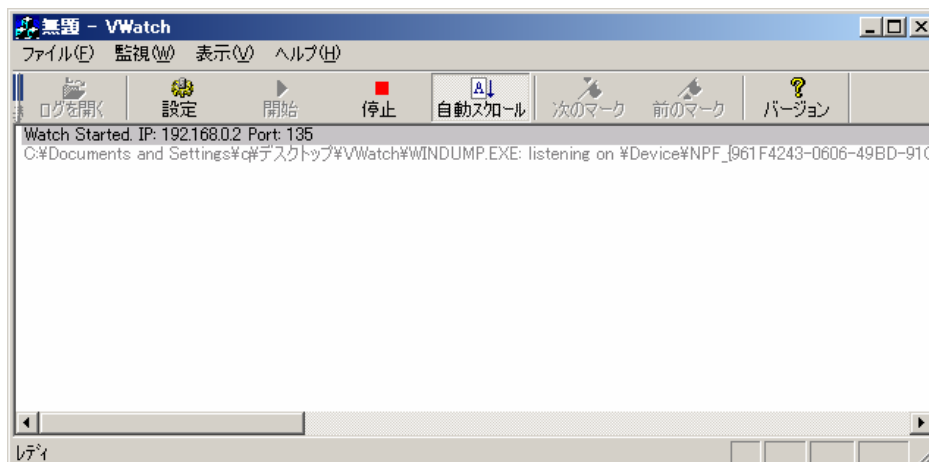


図 4-3 開始画面

4.3 実験結果

実験の結果、本ウイルス検出プログラムによって、11 ファミリー中 5 ファミリー（20 検体中 8 検体）のウイルスを検出した。検出した 8 検体での検出率はどれも 100%だった。また、検出しなかった 12 検体の内訳は、感染先マシンへの侵入動作が認められなかったものが 10 検体、予備調査により今回のウイルス検出プログラムでは検出不可能と判断してデータ採取に至らなかったものが 2 検体である。侵入動作が認められたもので検出できなかった検体は無い。

表 4-2にウイルス検体についてウイルスが使用する主な侵入方法、本ウイルス検出プログラムでの検出可能性の有無、および実験結果を示す。

表 4-2 ウイルスの感染方法、検知可能性、実験結果

No.	ウイルス名	主な侵入方法	検出可能性	実験結果
1	W32/Lovsan.worm.gen	ポート		100%検出 (2回検出/2回侵入)
2	W32/Lovsan.worm.a	ポート		100%検出 (2回検出/2回侵入)
3	W32/Lovsan.worm.e	ポート		100%検出 (2回検出/2回侵入)
4	W32/Nachi.worm	ポート		100%検出 (2回検出/2回侵入)
5	W32/Hybris.gen@MM	メール添付	×	予備調査のみ実施
6	W32/Magistr.a@MM	メール添付/ネットワーク		侵入動作確認できず
7	W32/Magistr.b@MM	メール添付/共有フォルダ		侵入動作確認できず
8	W32/CodeRed.worm.c	HTTP リクエスト		100%検出 (3回検出/3回侵入)
9	W32/CodeRed.worm.f	HTTP リクエスト		100%検出 (3回検出/3回侵入)
10	W32/CodeGreen.dr	HTTP リクエスト		侵入動作確認できず
11	W32/Klez.gen@MM	メール添付/共有フォルダ		100%検出 (2回検出/2回侵入)
12	W32/Klez.h@MM	メール添付/共有フォルダ		侵入動作確認できず
13	W32/Klez.e@MM	メール添付/共有フォルダ		侵入動作確認できず
14	W32/Nimda.gen@MM	バックドア/ポート/メール添付/共有フォルダ		侵入動作確認できず
15	W32/Nimda@MM	バックドア/ポート/メール添付/共有フォルダ		侵入動作確認できず
16	W32/Nimda.s@MM	バックドア/ポート/メール添付/共有フォルダ		100%検出 (2回検出/2回侵入)
17	W32/SirCam@MM	メール添付/共有フォルダ		侵入動作確認できず
18	W32/Sobig.a@MM	メール添付/共有フォルダ		侵入動作確認できず
19	W32/Sobig.f@MM	メール添付	×	予備調査のみ実施
20	W32/Rous.a	(不明)	(不明)	侵入動作確認できず

ウイルス検出プログラムは他のマシン（攻撃マシン）から脆弱性ポートを攻撃して侵入するウイルスを想定し、自マシン（感染先マシン）へのポートアクセスをチェックの開始契機としている。従って、侵入方法がメール添付のみであるようなウイルスについては検出可能性が無いものと判断した。

以下に、各ウイルスの実験結果の詳細をウイルス別に示す。

4.3.1 W32/Lovsan.worm.gen

(1) ウイルスの概要

W32/Lovsan.worm.gen の概要を表 4-3に示す。^{3, 4}

表 4-3 W32/Lovsan.worm.gen の概要

種別	ワーム
特徴	MS03-026「DCOM RPC の脆弱性」を悪用し、可能な限りのマシンに繁殖しようとする。ウィンドウズのセキュリティホールを利用することで、ユーザ側のアクションがなくてもワームの実行を可能とする。また、リモートアクセスポイントを作成し、アタッカーがシステムコマンドを実行する事を許可する。
プラットフォーム	Windows 2000, Windows XP
動作概要	IP アドレスをランダムに生成し、そのアドレスのコンピュータに感染を試みる。 DCOM RPC の脆弱性を悪用することのできる TCP ポート 135 にデータを送信する。 感染先に TCP ポート 4444 で待機するリモートシェルを作成する。 感染先の 4444 番ポートに接続し、TFTP.EXE を使用してウイルスのダウンロードを実行するよう命令する。 感染先でダウンロードしたウイルスを実行する。

なお、Network Associates 社の Web サイトで公開されているウイルス検索では W32/Lovsan.worm.gen という名称に一致するものは見当たらなかった。表 4-3は W32/Lovsan.worm.a の名称で公開されている情報をもとにまとめたものである。

(2) 実験環境の設定

OS の脆弱性情報⁵より、ポート 135、139、445、593 または、その他 RPC 用に設定されたポートが悪用される。

実験環境の設定を表 4-4に示す。

表 4-4 W32/Lovsan.worm.gen 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	135	-

設定項目	感染先マシン	攻撃マシン
監視対象ディレクトリ	C:\WINDOWS\system32 (サブディレクトリ含む)	-

本ウイルスが悪用するポートは 135 のみ、変更ディレクトリも Windows システムディレクトリのみであるため、上記の設定でも実験的には特に問題はなかったが、「セキュリティホールを悪用して侵入する未知ウイルス検出」という観点からは、脆弱性情報で示されるポート番号 135、139、445、593 および RPC 用に設定されたポートのすべてを監視対象とすべきである。また、監視ディレクトリについても、Windows システムディレクトリ以外に、標準的に存在するディレクトリをも監視対象に含める必要があるだろう。

(3) 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの Windows システムディレクトリ内にウイルスのファイルが作成されたかどうかで判別することができる。

ウイルスが感染を試みる IP アドレスはランダム的に生成される。そこで、感染先 IP アドレスからはずれた IP アドレスを攻撃している兆候が見られた場合は実験を中断し、攻撃マシン、感染先マシンを再起動して実験を再開した。本ウイルスが生成する IP アドレスは、ランダム的とはいえ、同一セグメント内の IP アドレスを生成する確率が高くなるように設定されているようであり、数回～数十回の試行で感染先マシンへの攻撃兆候が確認された。

また、ウイルスが送信する攻撃用データには Windows XP 用と Windows 2000 用の 2 通りがあり、これもランダム的に選択される。感染先の OS とは異なる攻撃用データが送信された場合も侵入に失敗する。そこで、感染先マシンにウイルスのファイルが作成されなかった場合も実験を中断し、攻撃マシン、感染先マシンを再起動して実験を再開した。

結果：実験期間中に 2 回の侵入が認められ、2 回ともウイルスを検出することができた。

図 4-4に W32/Lovsan.worm.gen ウイルス検出の一例を示す。

でポート番号 135 へのアクセスを検出、その後のディレクトリ監視により、でウイルスの侵入（監視対象ディレクトリにファイル TFTP1584 が作成された）を検出している。

さらに、図 4-4のデータからは、表 4-3に記載したウイルス動作の様子までうかがい知ることができる。以下に、その様子を説明する。なお、ネットワーク監視データとディレクトリ監視データは非同期にログ出力を行っているため、図 4-4では と の順序が時系列的に逆になっている。

攻撃マシンから感染先マシンへの脆弱性ポート番号 135 へのアクセス。
 感染先マシンの 4444 番ポートを利用したりリモートコマンド指示。
 攻撃マシンの 69 番ポート（TFTP 用ポート）を利用した TFTP コマンド実行。
 ダウンロードが開始され、一時ファイルが作成された。

(C:\WINDOWS\system32\TFTP1584)

ダウンロードが完了し、一時ファイルが要求されたファイル名に変更された。

(C:\WINDOWS\system32\penis32.exe)

```
11:11:44.390226 IP 192.168.0.1.1062 > 192.168.0.2.135: S 515958102:515958102(0) win 16384 <mss 1460,nop,n
11:11:44.398788 IP 192.168.0.2.135 > 192.168.0.1.1062: S 3268001129:3268001129(0) ack 515958103 win 17520
11:11:44.404410 IP 192.168.0.1.1062 > 192.168.0.2.135: . ack 1 win 17520 (DF)
11:11:45.215378 IP 192.168.0.2.137 > 192.168.0.1.137: udp 50
11:11:45.218720 IP 192.168.0.1.137 > 192.168.0.2.137: udp 193
11:11:45.229256 arp who-has 192.168.0.3 tell 192.168.0.2
11:11:48.230689 arp who-has 192.168.0.3 tell 192.168.0.2
11:11:51.203526 arp who-has 192.168.0.3 tell 192.168.0.2
11:11:54.231782 arp who-has 192.168.0.4 tell 192.168.0.2
11:11:57.194265 arp who-has 192.168.0.4 tell 192.168.0.2
11:12:00.186833 arp who-has 192.168.0.4 tell 192.168.0.2
11:12:03.194498 arp who-has 192.168.0.5 tell 192.168.0.2
11:12:06.171706 arp who-has 192.168.0.5 tell 192.168.0.2
11:12:09.178405 arp who-has 192.168.0.5 tell 192.168.0.2
11:12:11.817289 IP 192.168.0.1.1062 > 192.168.0.2.135: P 1:73(72) ack 1 win 17520 (DF)
11:12:11.826312 IP 192.168.0.2.135 > 192.168.0.1.1062: P 1:61(60) ack 73 win 17448 (DF)
11:12:11.831641 IP 192.168.0.1.1062 > 192.168.0.2.135: . 73:1533(1460) ack 61 win 17460 (DF)
11:12:11.838632 IP 192.168.0.1.1062 > 192.168.0.2.135: P 1533:1777(244) ack 61 win 17460 (DF)
11:12:11.842546 IP 192.168.0.2.135 > 192.168.0.1.1062: . ack 1777 win 17520 (DF)
11:12:11.848450 IP 192.168.0.1.1062 > 192.168.0.2.135: R 515959879:515959879(0) win 0 (DF)
11:12:12.198402 arp who-has 192.168.0.6 tell 192.168.0.2
11:12:12.206369 IP 192.168.0.1.1083 > 192.168.0.2.4444: S 523306442:523306442(0) win 16384 <mss 1460,nop,n
11:12:12.207298 IP 192.168.0.2.4444 > 192.168.0.1.1083: S 3274430265:3274430265(0) ack 523306443 win 17520
11:12:12.211932 IP 192.168.0.1.1083 > 192.168.0.2.4444: . ack 1 win 17520 (DF)
11:12:12.335617 IP 192.168.0.1.1083 > 192.168.0.2.4444: P 1:37(36) ack 1 win 17520 (DF)
11:12:12.429509 IP 192.168.0.2.4444 > 192.168.0.1.1083: . ack 37 win 17484 (DF)
11:12:13.378402 IP 192.168.0.2.4444 > 192.168.0.1.1083: P 1:40(39) ack 37 win 17484 (DF)
11:12:13.471132 IP 192.168.0.1.1083 > 192.168.0.2.4444: . ack 40 win 17481 (DF)
11:12:13.471896 IP 192.168.0.2.4444 > 192.168.0.1.1083: P 40:141(101) ack 37 win 17484 (DF)
11:12:13.654217 IP 192.168.0.1.1083 > 192.168.0.2.4444: . ack 141 win 17380 (DF)
11:12:14.266 File Added: C:\WINDOWS\system32\TFTP1584
11:12:14.184885 IP 192.168.0.2.1050 > 192.168.0.1.69: 20 RRQ "penis32.exe"
11:12:14.196549 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 1
11:12:14.366488 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 1
11:12:15.829 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:15.027482 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 2
11:12:15.028397 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 2
11:12:15.199004 arp who-has 192.168.0.6 tell 192.168.0.2
11:12:15.964237 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 3
11:12:15.964933 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 3
11:12:16.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:16.864431 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 4
11:12:16.865171 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 4
11:12:17.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:17.773191 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 5
11:12:17.774350 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 5
11:12:18.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:18.201852 arp who-has 192.168.0.6 tell 192.168.0.2
11:12:18.678243 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 6
11:12:18.683921 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 6
11:12:19.542453 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 7
11:12:19.543273 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 7
11:12:20.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:20.535718 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 8
11:12:20.536414 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 8
11:12:21.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:21.289481 arp who-has 192.168.0.7 tell 192.168.0.2
11:12:21.421032 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 9
11:12:21.421617 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 9
```

```

11:12:22.454 File Modified: C:\WINDOWS\system32
11:12:22.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:22.321002 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 10
11:12:22.321695 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 10
11:12:23.641 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:23.223402 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 11
11:12:23.223910 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 11
11:12:24.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:24.162619 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 12
11:12:24.163360 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 12
11:12:24.288567 arp who-has 192.168.0.7 tell 192.168.0.2
11:12:25.031621 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 13
11:12:25.032276 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 13
11:12:25.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:25.946565 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 14
11:12:25.947296 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 14
11:12:26.798 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:26.824658 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 15
11:12:26.825324 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 15
11:12:27.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:27.296057 arp who-has 192.168.0.7 tell 192.168.0.2
11:12:27.759255 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 16
11:12:27.760290 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 16
11:12:28.829 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:28.658084 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 17
11:12:28.658744 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 17
11:12:29.798 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:29.562029 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 18
11:12:29.563068 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 18
11:12:30.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:30.309036 arp who-has 192.168.0.8 tell 192.168.0.2
11:12:30.456490 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 19
11:12:30.457413 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 19
11:12:31.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:31.374472 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 20
11:12:31.375199 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 20
11:12:32.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:32.298729 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 21
11:12:32.299372 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 21
11:12:33.782 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:33.231849 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 22
11:12:33.232511 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 22
11:12:33.311234 arp who-has 192.168.0.8 tell 192.168.0.2
11:12:33.435306 IP 192.168.0.1.1083 > 192.168.0.2.4444: P 37:55(18) ack 141 win 17380 (DF)
11:12:33.653478 IP 192.168.0.2.4444 > 192.168.0.1.1083: . ack 55 win 17466 (DF)
11:12:34.266 File Modified: C:\WINDOWS\system32\TFTP1584
11:12:34.329 File Modified: C:\WINDOWS\system32
11:12:34.360 File name changed from: C:\WINDOWS\system32\TFTP1584 to: C:\WINDOWS\system32\penis32.exe ←
11:12:34.407 File Modified: C:\WINDOWS\system32\penis32.exe
11:12:34.766 File Modified: C:\WINDOWS\system32\config\software.LOG
11:12:34.813 File Modified: C:\WINDOWS\system32\config\software.LOG
11:12:34.829 File Modified: C:\WINDOWS\system32\config\software.LOG

```

図 4-4 W32/Lovsan.worm.gen ウイルス検出例

4.3.2 W32/Lovsan.worm.a

(1) ウイルスの概要

W32/Lovsan.worm.a の概要を表 4-5に示す。^{3, 4}

表 4-5 W32/Lovsan.worm.a の概要

種別	ワーム
特徴	MS03-026「DCOM RPC の脆弱性」を悪用し、可能な限りのマシンに繁殖しようとする。ウィンドウズのセキュリティホールを利用することで、ユーザ側のアクションがなくてもワームの実行を可能とする。また、リモートアクセスポイントを作成し、アタッカーがシステムコマンドを実行する事を許可する。
プラットフォーム	Windows 2000, Windows XP
動作概要	IP アドレスをランダムに生成し、そのアドレスのコンピュータに感染を試みる。 DCOM RPC の脆弱性を悪用することのできる TCP ポート 135 にデータを送信する。 感染先に TCP ポート 4444 で待機するリモートシェルを作成する。 感染先の 4444 番ポートに接続し、TFTP.EXE を使用してウイルスのダウンロードを実行するよう命令する。 感染先でダウンロードしたウイルスを実行する。

(2) 実験環境の設定

OS の脆弱性情報⁵ より、ポート 135、139、445、593 または、その他 RPC 用に設定されたポートが悪用される。

実験環境の設定を表 4-6に示す。

表 4-6 W32/Lovsan.worm.a 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	135	-
監視対象 ディレクトリ	C:\WINDOWS\system32 (サブディレクトリ含む)	-

本ウイルスが悪用するポートは 135 のみ、変更ディレクトリも Windows システムディレ

クトリのみであるため、上記の設定でも実験的には特に問題はなかったが、「セキュリティホールを悪用して侵入する未知ウイルス検出」という観点からは、脆弱性情報で示されるポート番号 135、139、445、593 および RPC 用に設定されたポートのすべてを監視対象とすべきである。また、監視ディレクトリについても、Windows システムディレクトリ以外に、標準的に存在するディレクトリをも監視対象に含める必要があるだろう。

(3) 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの Windows システムディレクトリ内にウイルスのファイルが作成されたかどうかで判別することができる。

ウイルスが感染を試みる IP アドレスはランダム的に生成される。そこで、感染先 IP アドレスからはずれた IP アドレスを攻撃している兆候が見られた場合は実験を中断し、攻撃マシン、感染先マシンを再起動して実験を再開した。本ウイルスが生成する IP アドレスは、ランダム的とはいえ、同一セグメント内の IP アドレスを生成する確率が高くなるように設定されているようであり、数回～数十回の試行で感染先マシンへの攻撃兆候が確認された。

また、ウイルスが送信する攻撃用データには Windows XP 用と Windows 2000 用の 2 通りがあり、これもランダム的に選択される。感染先の OS とは異なる攻撃用データが送信された場合も侵入に失敗する。そこで、感染先マシンにウイルスのファイルが作成されなかった場合も実験を中断し、攻撃マシン、感染先マシンを再起動して実験を再開した。

結果：実験期間中に 2 回の侵入が認められ、2 回ともウイルスを検出することができた。

図 4-5 に W32/Lovsan.worm.a ウイルス検出の一例を示す。

でポート番号 135 へのアクセスを検出、その後のディレクトリ監視により、でウイルスの侵入（監視対象ディレクトリにファイル TFTP1284 が作成された）を検出している。

さらに、図 4-5 のデータからは、表 4-5 に記載したウイルス動作の様子までうかがい知ることができる。以下に、その様子を説明する。なお、ネットワーク監視データとディレクトリ監視データは非同期にログ出力を行っているため、図 4-5 では と の順序が時系列的に逆になっている。

攻撃マシンから感染先マシンへの脆弱性ポート番号 135 へのアクセス .

感染先マシンの 4444 番ポートを利用したリモートコマンド指示 .

攻撃マシンの 69 番ポート (TFTP 用ポート) を利用した TFTP コマンド実行 .

ダウンロードが開始され、一時ファイルが作成された .

(C:¥WINDOWS¥system32¥TFTP1284)

ダウンロードが完了し、一時ファイルがダウンロード要求ファイル名に変更された .

(C:¥WINDOWS¥system32¥msblast.exe)

```

Watch Started. IP: 192.168.0.2 Port: 135
C:¥Documents and Settings¥q¥デスクトップ¥Watch¥WINDUMP.EXE: listening on ¥Device¥NPF_{961F4243-0606-49B
11:34:18.059994 IP 192.168.0.1.3117 > 192.168.0.2.135: S 511649468:511649468(0) win 16384 <mss 1460,nop,n ←
11:34:18.062716 IP 192.168.0.2.135 > 192.168.0.1.3117: S 3197155047:3197155047(0) ack 511649469 win 17520
11:34:18.064960 IP 192.168.0.1.3117 > 192.168.0.2.135: . ack 1 win 17520 (DF)
11:34:37.719280 IP 192.168.0.1.3117 > 192.168.0.2.135: P 1:73(72) ack 1 win 17520 (DF)
11:34:37.724013 IP 192.168.0.2.135 > 192.168.0.1.3117: P 1:61(60) ack 73 win 17448 (DF)
11:34:37.727715 IP 192.168.0.1.3117 > 192.168.0.2.135: . 73:1533(1460) ack 61 win 17460 (DF)
11:34:37.729915 IP 192.168.0.1.3117 > 192.168.0.2.135: P 1533:1777(244) ack 61 win 17460 (DF)
11:34:37.732347 IP 192.168.0.2.135 > 192.168.0.1.3117: . ack 1777 win 17520 (DF)
11:34:37.748818 IP 192.168.0.1.3117 > 192.168.0.2.135: R 511651245:511651245(0) win 0 (DF)
11:34:38.077677 IP 192.168.0.1.3138 > 192.168.0.2.4444: S 517243114:517243114(0) win 16384 <mss 1460,nop, ←
11:34:38.078634 IP 192.168.0.2.4444 > 192.168.0.1.3138: S 3201776129:3201776129(0) ack 517243115 win 1752
11:34:38.085264 IP 192.168.0.1.3138 > 192.168.0.2.4444: . ack 1 win 17520 (DF)
11:34:38.208447 IP 192.168.0.1.3138 > 192.168.0.2.4444: P 1:37(36) ack 1 win 17520 (DF)
11:34:38.355772 IP 192.168.0.2.4444 > 192.168.0.1.3138: . ack 37 win 17484 (DF)
11:34:38.955109 IP 192.168.0.2.4444 > 192.168.0.1.3138: P 1:40(39) ack 37 win 17484 (DF)
11:34:39.058954 IP 192.168.0.1.3138 > 192.168.0.2.4444: . ack 40 win 17481 (DF)
11:34:39.060217 IP 192.168.0.2.4444 > 192.168.0.1.3138: P 40:141(101) ack 37 win 17484 (DF)
11:34:39.335402 IP 192.168.0.1.3138 > 192.168.0.2.4444: . ack 141 win 17380 (DF)
11:34:40.314 File Added: C:¥WINDOWS¥system32¥TFTP1284 ←
11:34:39.917798 IP 192.168.0.2.1050 > 192.168.0.1.69: 20 RRQ "msblast.exe" ←
11:34:39.925698 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 1
11:34:40.025784 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 1
11:34:41.377 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:40.818908 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 2
11:34:40.819822 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 2
11:34:42.330 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:41.771672 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 3
11:34:41.772914 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 3
11:34:43.330 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:42.617220 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 4
11:34:42.634111 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 4
11:34:44.361 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:43.583051 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 5
11:34:43.583900 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 5
11:34:44.472564 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 6
11:34:44.473298 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 6
11:34:45.330 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:45.384603 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 7
11:34:45.385196 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 7
11:34:46.392 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:46.254414 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 8
11:34:46.255776 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 8
11:34:47.330 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:47.234118 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 9
11:34:47.236024 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 9
11:34:48.345 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:48.091335 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 10
11:34:48.092022 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 10
11:34:49.392 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:49.013140 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 11
11:34:49.013804 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 11
11:34:50.330 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:49.867593 IP 192.168.0.1.69 > 192.168.0.2.1050: 516 DATA block 12
11:34:49.868433 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 12
11:34:51.205 File Modified: C:¥WINDOWS¥system32¥TFTP1284
11:34:51.377 File name changed from: C:¥WINDOWS¥system32¥TFTP1284 to: C:¥WINDOWS¥system32¥msblast.exe ←
11:34:51.408 File Modified: C:¥WINDOWS¥system32¥msblast.exe
11:34:50.833934 IP 192.168.0.1.69 > 192.168.0.2.1050: 36 DATA block 13
11:34:50.834444 IP 192.168.0.2.1050 > 192.168.0.1.69: 4 ACK block 13
11:34:50.939883 IP 192.168.0.2.4444 > 192.168.0.1.3138: P 141:202(61) ack 37 win 17484 (DF)
11:34:51.134758 IP 192.168.0.1.3138 > 192.168.0.2.4444: . ack 202 win 17319 (DF)

```

図 4-5 W32/Lovsan.worm.a ウイルス検出例

4.3.3 W32/Lovsan.worm.e

(1) ウイルスの概要

W32/Lovsan.worm.e の概要を表 4-7に示す。^{6, 7}

表 4-7 W32/Lovsan.worm.e の概要

種別	ワーム
特徴	MS03-026「DCOM RPC の脆弱性」を悪用し、可能な限りのマシンに繁殖しようとする。ウィンドウズのセキュリティホールを利用することで、ユーザ側のアクションがなくてもワームの実行を可能とする。また、リモートアクセスポイントを作成し、アタッカーがシステムコマンドを実行する事を許可する。
プラットフォーム	Windows 2000, Windows XP
動作概要	IP アドレスをランダムに生成し、そのアドレスのコンピュータに感染を試みる。 DCOM RPC の脆弱性を悪用することのできる TCP ポート 135 にデータを送信する。 感染先に TCP ポート 4444 で待機するリモートシェルを作成する。 感染先の 4444 番ポートに接続し、TFTP.EXE を使用してウイルスのダウンロードを実行するよう命令する。 感染先でダウンロードしたウイルスを実行する。

(2) 実験環境の設定

OS の脆弱性情報⁵より、ポート 135、139、445、593 または、その他 RPC 用に設定されたポートが悪用される。

実験環境の設定を表 4-8に示す。

表 4-8 W32/Lovsan.worm.e 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象ポート番号	135	-
監視対象ディレクトリ	C:\WINDOWS\system32 (サブディレクトリ含む)	-

本ウイルスが悪用するポートは 135 のみ、変更ディレクトリも Windows システムディレ

クトリのみであるため、上記の設定でも実験的には特に問題はなかったが、「セキュリティホールを悪用して侵入する未知ウイルス検出」という観点からは、脆弱性情報で示されるポート番号 135、139、445、593 および RPC 用に設定されたポートのすべてを監視対象とすべきである。また、監視ディレクトリについても、Windows システムディレクトリ以外に、標準的に存在するディレクトリをも監視対象に含める必要があるだろう。

(3) 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの Windows システムディレクトリ内にウイルスのファイルが作成されたかどうかで判別することができる。

ウイルスが感染を試みる IP アドレスはランダム的に生成される。そこで、感染先 IP アドレスからはずれた IP アドレスを攻撃している兆候が見られた場合は実験を中断し、攻撃マシン、感染先マシンを再起動して実験を再開した。本ウイルスが生成する IP アドレスは、ランダム的とはいえ、同一セグメント内の IP アドレスを生成する確率が高くなるように設定されているようであり、数回～数十回の試行で感染先マシンへの攻撃兆候が確認された。

また、ウイルスが送信する攻撃用データには Windows XP 用と Windows 2000 用の 2 通りがあり、これもランダム的に選択される。感染先の OS とは異なる攻撃用データが送信された場合も侵入に失敗する。そこで、感染先マシンにウイルスのファイルが作成されなかった場合も実験を中断し、攻撃マシン、感染先マシンを再起動して実験を再開した。

結果：実験期間中に 2 回の侵入が認められ、2 回ともウイルスを検出することができた。

図 4-6 に W32/Lovsan.worm.e ウイルス検出の一例を示す。

でポート番号 135 へのアクセスを検出、その後のディレクトリ監視により、でウイルスの侵入（監視対象ディレクトリにファイル TFTP1756 が作成された）を検出している。

さらに、図 4-6 のデータからは、表 4-7 に記載したウイルス動作の様子までうかがい知ることができる。以下に、その様子を説明する。なお、ネットワーク監視データとディレクトリ監視データは非同期にログ出力を行っているため、図 4-6 では と の順序が時系列的に逆になっている。

攻撃マシンから感染先マシンへの脆弱性ポート番号 135 へのアクセス .

感染先マシンの 4444 番ポートを利用したリモートコマンド指示 .

攻撃マシンの 69 番ポート (TFTP 用ポート) を利用した TFTP コマンド実行 .

ダウンロードが開始され、一時ファイルが作成された .

(C:¥WINDOWS¥system32¥TFTP1756)

ダウンロードが完了し、一時ファイルが要求されたファイル名に変更された .

(C:¥WINDOWS¥system32¥mslaugh.exe)

```

Watch Started. IP: 192.168.0.2 Port: 135
C:¥Documents and Settings¥q¥デスクトップ¥Watch¥WINDUMP.EXE: listening on ¥Device¥NPF_{961F4243-0606-49BD-91C6
13:18:46.973858 IP 192.168.0.1.1035 > 192.168.0.2.135: S 2308535098:2308535098(0) win 16384 <mss 1460,nop,n ←
13:18:46.988466 IP 192.168.0.2.135 > 192.168.0.1.1035: S 3778426670:3778426670(0) ack 2308535099 win 17520
13:18:47.001458 IP 192.168.0.1.1035 > 192.168.0.2.135: . ack 1 win 17520 (DF)
13:19:06.664336 IP 192.168.0.1.1035 > 192.168.0.2.135: P 1:73(72) ack 1 win 17520 (DF)
13:19:06.665915 IP 192.168.0.1.1035 > 192.168.0.2.135: . 73:1533(1460) ack 1 win 17520 (DF)
13:19:06.668640 IP 192.168.0.2.135 > 192.168.0.1.1035: . ack 1533 win 17520 (DF)
13:19:06.669119 IP 192.168.0.1.1035 > 192.168.0.2.135: P 1533:1777(244) ack 1 win 17520 (DF)
13:19:06.670348 IP 192.168.0.1.1035 > 192.168.0.2.135: F 1777:1777(0) ack 1 win 17520 (DF)
13:19:06.671844 IP 192.168.0.2.135 > 192.168.0.1.1035: . ack 1778 win 17276 (DF)
13:19:06.676231 IP 192.168.0.2.135 > 192.168.0.1.1035: P 1:61(60) ack 1778 win 17276 (DF)
13:19:06.682679 IP 192.168.0.2.135 > 192.168.0.1.1035: F 61:61(0) ack 1778 win 17276 (DF)
13:19:06.695490 IP 192.168.0.1.1035 > 192.168.0.2.135: R 2308536876:2308536876(0) win 0 (DF)
13:19:06.701572 IP 192.168.0.1.1035 > 192.168.0.2.135: R 2308536876:2308536876(0) win 0
13:19:07.183443 IP 192.168.0.1.1056 > 192.168.0.2.4444: S 2314181056:2314181056(0) win 16384 <mss 1460,nop,n ←
13:19:07.184405 IP 192.168.0.2.4444 > 192.168.0.1.1056: S 3783108181:3783108181(0) ack 2314181057 win 17520 <mss 1460,n
13:19:07.186429 IP 192.168.0.1.1056 > 192.168.0.2.4444: . ack 1 win 17520 (DF)
13:19:07.304871 IP 192.168.0.1.1056 > 192.168.0.2.4444: P 1:37(36) ack 1 win 17520 (DF)
13:19:07.488946 IP 192.168.0.2.4444 > 192.168.0.1.1056: . ack 37 win 17484 (DF)
13:19:07.610337 IP 192.168.0.2.4444 > 192.168.0.1.1056: P 1:40(39) ack 37 win 17484 (DF)
13:19:08.296 File Added: C:¥WINDOWS¥system32¥TFTP1756 ←
13:19:07.850316 IP 192.168.0.1.1056 > 192.168.0.2.4444: . ack 40 win 17481 (DF)
13:19:07.852392 IP 192.168.0.2.4444 > 192.168.0.1.1056: P 40:141(101) ack 37 win 17484 (DF) ←
13:19:08.128364 IP 192.168.0.2.1034 > 192.168.0.1.69: 20 RRQ "mslaugh.exe" ←
13:19:08.145084 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 1
13:19:08.156113 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 1
13:19:08.162308 IP 192.168.0.1.1056 > 192.168.0.2.4444: . ack 141 win 17380 (DF)
13:19:09.359 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:08.968536 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 2
13:19:08.969745 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 2
13:19:10.343 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:09.863385 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 3
13:19:09.864610 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 3
13:19:10.753000 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 4
13:19:10.753769 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 4
13:19:11.343 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:11.674758 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 5
13:19:11.675953 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 5
13:19:12.343 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:12.594265 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 6
13:19:12.595173 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 6
13:19:13.343 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:13.446823 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 7
13:19:13.447560 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 7
13:19:14.359 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:14.372317 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 8
13:19:14.373327 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 8
13:19:15.343 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:15.325974 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 9
13:19:15.326710 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 9
13:19:16.343 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:16.170632 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 10
13:19:16.207641 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 10
13:19:17.343 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:17.593 File Modified: C:¥WINDOWS¥system32
13:19:17.094573 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 11
13:19:17.095326 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 11
13:19:18.003376 IP 192.168.0.1.69 > 192.168.0.2.1034: 516 DATA block 12
13:19:18.004156 IP 192.168.0.2.1034 > 192.168.0.1.69: 4 ACK block 12
13:19:19.109 File Modified: C:¥WINDOWS¥system32¥TFTP1756
13:19:19.156 File name changed from: C:¥WINDOWS¥system32¥TFTP1756 to: C:¥WINDOWS¥system32¥mslaugh.exe ←
13:19:19.187 File Modified: C:¥WINDOWS¥system32
13:19:19.296 File Modified: C:¥WINDOWS¥system32¥mslaugh.exe

```

図 4-6 W32/Lovsan.worm.e ウイルス検出例

4.3.4 W32/Nachi.worm

(1) ウイルスの概要

W32/Nachi.worm の概要を表 4-9に示す。^{8, 9}

表 4-9 W32/Nachi.worm の概要

種別	ワーム
特徴	MS03-026「DCOM RPC の脆弱性」または MS03-007「未チェックのバッファによりサーバーが侵害される脆弱性」のいずれかを悪用し、可能な限りのマシンに繁殖しようとする。W32/Lovsan が動作しているときは、終了させる。またシステムディレクトリにある msblast.exe を削除する。ウィンドウズのセキュリティホールを利用することで、ユーザ側のアクションがなくてもワームの実行を可能とする。また、リモートアクセスポイントを作成し、アタッカーがシステムコマンドを実行する事を許可する。
プラットフォーム	Windows 2000, Windows XP
動作概要	IP アドレスを攻撃元の IP アドレス(A.B.C.D)から A.B.0.0 より順に、またはランダムに IP アドレス(E.F.0.0 から順に)そのアドレスのコンピュータに感染を試みる。 DCOM RPC の脆弱性を悪用することのできる TCP ポート 135 にデータを送信する。または「未チェックのバッファによりサーバーが侵害される」脆弱性を悪用することのできる TCP ポート 80 にデータを送信する。 感染先から攻撃マシンの TCP ポート 666 ~ 765 のいずれかに接続する。接続すると TFTP.EXE を使用してウイルスのダウンロードを実行するよう命令する。 感染先でダウンロードしたウイルスを実行する。 msblast.exe を削除するよう命令する。 meblast.exe を削除する。

(2) 実験環境の設定

OS の脆弱性情報^{5, 10}より、ポート 80、135、139、445、593 または、その他 RPC 用に設定されたポートが悪用される。

実験環境の設定を表 4-10に示す。

表 4-10 W32/Nachi.worm 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1

設定項目	感染先マシン	攻撃マシン
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	135	-
監視対象 ディレクトリ	C:¥WINDOWS¥system32 (サブディレクトリ含む)	-

本ウイルスが悪用するポートは 80, 135 のいずれかで、変更ディレクトリも Windows システムディレクトリのみであるが、監視するポートを 135 のみに設定しても実験的には特に問題はなかった。しかしながら、「セキュリティホールを悪用して侵入する未知ウイルス検出」という観点からは、脆弱性情報で示されるポート番号 80、135、139、445、593 および RPC 用に設定されたポートのすべてを監視対象とすべきである。また、監視ディレクトリについても、Windows システムディレクトリ以外に、標準的に存在するディレクトリをも監視対象に含める必要があるだろう。

(3) 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの Windows システムディレクトリ内にウイルスのファイルが作成されたかどうかで判別することができる。

結果：実験期間中に 2 回の侵入が認められ、2 回ともウイルスを検出することができた。

なお、上記 2 回の侵入はいずれもポート番号 135 への攻撃であり、ポート番号 80 への攻撃兆候は観測されなかった。

図 4-7に W32/Nachi.worm ウイルス検出の一例を示す。

でポート番号 135 へのアクセスを検出、その後のディレクトリ監視により、で感染先マシンへの TFTP.EXE (SVCHOST.EXE) の送信 (監視対象ディレクトリにファイル TFTP1036 が作成された) を検出し、でウイルスの侵入 (監視対象ディレクトリにファイル TFTP1468 が作成された) を検出している。

さらに、図 4-7のデータからは、表 4-9に記載したウイルス動作の様子までうかがい知ることができる。以下に、その様子を説明する。なお、ネットワーク監視データとディレクトリ監視データは非同期にログ出力を行っているため、図 4-7では / の順序が時系列的に逆になっている。

攻撃マシンから感染先マシンへの脆弱性ポート番号 135 へのアクセス .
 感染先マシンから攻撃マシンの 707 番ポートへの接続およびコマンド指示 .
 攻撃マシンの 69 番ポート (TFTP 用ポート) を利用した TFTP コマンド実行 .
 ダウンロードが開始され、一時ファイルが作成された .
 (C:¥WINDOWS¥system32¥TFTP1036)

ダウンロードが完了し、一時ファイルが要求されたファイル名に変更された。

(C:¥WINDOWS¥system32¥wins¥SVCHOST.EXE)

攻撃マシン 707 番ポートからのコマンド指示。

攻撃マシンの 69 番ポート (TFTP 用ポート) を利用した TFTP コマンド実行。

ダウンロードが開始され、一時ファイルが作成された。

(C:¥WINDOWS¥system32¥TFTP1468)

ダウンロードが完了し、一時ファイルが要求されたファイル名に変更された。

(C:¥WINDOWS¥system32¥wins¥DLLHOST.EXE)

攻撃マシン 707 番ポートからのコマンド指示。

ファイルが削除された。

(C:¥WINDOWS¥system32¥msblast.exe)

```

Watch Started. IP: 192.168.0.2 Port: 135
C:\Documents and Settings\¥q¥デスクトップ¥¥Wwatch¥¥WINDUMP.EXE: listening on ¥Device¥¥NPF_{961F4243-0606-49B
11:53:50.197640 IP 192.168.0.1.3414 > 192.168.0.2.135: S 506626105:506626105(0) win 16384 <mss 1460,nop,n
11:53:50.205155 IP 192.168.0.2.135 > 192.168.0.1.3414: S 825838943:825838943(0) ack 506626106 win 17520 <
11:53:50.216364 IP 192.168.0.1.3414 > 192.168.0.2.135: . ack 1 win 17520 (DF)
11:53:50.219466 IP 192.168.0.1.3414 > 192.168.0.2.135: P 1:73(72) ack 1 win 17520 (DF)
11:53:50.256680 IP 192.168.0.2.135 > 192.168.0.1.3414: P 1:61(60) ack 73 win 17448 (DF)
11:53:50.263699 IP 192.168.0.1.3414 > 192.168.0.2.135: . 73:1533(1460) ack 61 win 17460 (DF)
11:53:50.267928 IP 192.168.0.1.3414 > 192.168.0.2.135: P 1533:1777(244) ack 61 win 17460 (DF)
11:53:50.271281 IP 192.168.0.2.135 > 192.168.0.1.3414: . ack 1777 win 17520 (DF)
11:53:50.708141 IP 192.168.0.2.2994 > 192.168.0.1.707: S 826028925:826028925(0) win 16384 <mss 1460,nop,n
11:53:50.723411 IP 192.168.0.1.707 > 192.168.0.2.2994: S 506886055:506886055(0) ack 826028926 win 17520 <
11:53:50.724248 IP 192.168.0.2.2994 > 192.168.0.1.707: . ack 1 win 17520 (DF)
11:53:50.728381 IP 192.168.0.2.135 > 192.168.0.1.3414: F 61:61(0) ack 1777 win 17520 (DF)
11:53:50.730541 IP 192.168.0.1.3414 > 192.168.0.2.135: . ack 62 win 17460 (DF)
11:53:50.762857 IP 192.168.0.1.3414 > 192.168.0.2.135: F 1777:1777(0) ack 62 win 17460 (DF)
11:53:50.763097 IP 192.168.0.2.135 > 192.168.0.1.3414: . ack 1778 win 17520 (DF)
11:53:51.164783 IP 192.168.0.2.2994 > 192.168.0.1.707: P 1:40(39) ack 1 win 17520 (DF)
11:53:51.309899 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 40 win 17481 (DF)
11:53:51.310610 IP 192.168.0.2.2994 > 192.168.0.1.707: P 40:105(65) ack 1 win 17520 (DF)
11:53:51.340503 IP 192.168.0.1.707 > 192.168.0.2.2994: P 1:23(22) ack 105 win 17416 (DF)
11:53:51.342417 IP 192.168.0.2.2994 > 192.168.0.1.707: P 105:126(21) ack 23 win 17498 (DF)
11:53:51.481467 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 126 win 17395 (DF)
11:53:51.481772 IP 192.168.0.2.2994 > 192.168.0.1.707: P 126:310(184) ack 23 win 17498 (DF)
11:53:51.483109 IP 192.168.0.1.707 > 192.168.0.2.2994: P 23:47(24) ack 310 win 17211 (DF)
11:53:51.484011 IP 192.168.0.2.2994 > 192.168.0.1.707: P 310:334(24) ack 47 win 17474 (DF)
11:53:51.680563 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 334 win 17187 (DF)
11:53:51.680816 IP 192.168.0.2.2994 > 192.168.0.1.707: P 334:522(188) ack 47 win 17474 (DF)
11:53:51.681911 IP 192.168.0.1.707 > 192.168.0.2.2994: P 47:101(54) ack 522 win 16999 (DF)
11:53:51.683057 IP 192.168.0.2.2994 > 192.168.0.1.707: P 522:576(54) ack 101 win 17420 (DF)
11:53:52.593 File Added: C:\WINDOWS\system32\TFTP1036
11:53:52.843 File Modified: C:\WINDOWS\system32\TFTP1036
11:53:52.905 File Removed: C:\WINDOWS\system32\TFTP1036
11:53:52.921 File Added: C:\WINDOWS\system32\wins\SVCHOST.EXE
11:53:52.983 File Modified: C:\WINDOWS\system32\wins
11:53:53.046 File Modified: C:\WINDOWS\system32\wins\SVCHOST.EXE
11:53:51.798154 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 576 win 16945 (DF)
11:53:52.513471 IP 192.168.0.2.3015 > 192.168.0.1.69: 20 RRQ "svchost.exe"
11:53:52.565284 IP 192.168.0.1.3416 > 192.168.0.2.3015: udp 516
11:53:52.591145 IP 192.168.0.2.3015 > 192.168.0.1.3416: udp 4
11:53:52.600583 IP 192.168.0.1.3416 > 192.168.0.2.3015: udp 516
11:53:52.602311 IP 192.168.0.2.3015 > 192.168.0.1.3416: udp 4
: : :
: : :
11:53:52.786816 IP 192.168.0.1.3416 > 192.168.0.2.3015: udp 516
11:53:52.787249 IP 192.168.0.2.3015 > 192.168.0.1.3416: udp 4
11:53:52.791047 IP 192.168.0.1.3416 > 192.168.0.2.3015: udp 276
11:53:52.791240 IP 192.168.0.2.3015 > 192.168.0.1.3416: udp 4
11:53:52.844104 IP 192.168.0.2.2994 > 192.168.0.1.707: P 576:638(62) ack 101 win 17420 (DF)
11:53:52.853783 IP 192.168.0.1.707 > 192.168.0.2.2994: P 101:155(54) ack 638 win 16883 (DF)
11:53:52.887016 IP 192.168.0.2.2994 > 192.168.0.1.707: . ack 155 win 17366 (DF)
11:53:52.959621 IP 192.168.0.2.2994 > 192.168.0.1.707: P 638:640(2) ack 155 win 17366 (DF)
11:53:53.024493 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 640 win 16881 (DF)
11:53:53.024816 IP 192.168.0.2.2994 > 192.168.0.1.707: P 640:714(74) ack 155 win 17366 (DF)
11:53:53.208908 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 714 win 16807 (DF)
11:53:55.093 File Added: C:\WINDOWS\system32\TFTP1468
11:53:55.139 File Modified: C:\WINDOWS\system32\TFTP1468
11:53:55.218 File Removed: C:\WINDOWS\system32\TFTP1468
11:53:55.249 File Added: C:\WINDOWS\system32\wins\DLLHOST.EXE
11:53:55.264 File Modified: C:\WINDOWS\system32\wins
11:53:55.296 File Modified: C:\WINDOWS\system32\wins\DLLHOST.EXE
11:53:54.674580 IP 192.168.0.2.3036 > 192.168.0.1.69: 20 RRQ "dllhost.exe"
11:53:54.722653 IP 192.168.0.1.3417 > 192.168.0.2.3036: udp 516
11:53:54.738451 IP 192.168.0.2.3036 > 192.168.0.1.3417: udp 4
11:53:55.780 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:55.936 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:56.014 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:56.046 File Modified: C:\WINDOWS\system32\config\system.LOG

```

```

11:53:56.186 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:56.280 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:56.374 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:56.421 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:56.593 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:54.751068 IP 192.168.0.1.3417 > 192.168.0.2.3036: udp 516
11:53:54.751631 IP 192.168.0.2.3036 > 192.168.0.1.3417: udp 4
11:53:54.753033 IP 192.168.0.1.3417 > 192.168.0.2.3036: udp 516
11:53:54.754975 IP 192.168.0.2.3036 > 192.168.0.1.3417: udp 4
      :      :      :
      :      :      :
11:53:54.799600 IP 192.168.0.1.3417 > 192.168.0.2.3036: udp 516
11:53:54.800043 IP 192.168.0.2.3036 > 192.168.0.1.3417: udp 4
11:53:54.803950 IP 192.168.0.1.3417 > 192.168.0.2.3036: udp 4
11:53:54.804459 IP 192.168.0.2.3036 > 192.168.0.1.3417: udp 4
11:53:54.826968 IP 192.168.0.2.2994 > 192.168.0.1.707: P 714:776(62) ack 155 win 17366 (DF)
11:53:55.007008 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 776 win 16745 (DF)
11:53:55.007240 IP 192.168.0.2.2994 > 192.168.0.1.707: P 776:798(22) ack 155 win 17366 (DF)
11:53:55.238632 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 798 win 16723 (DF)
11:53:55.339978 IP 192.168.0.1.707 > 192.168.0.2.2994: P 155:173(18) ack 798 win 16723 (DF)
11:53:55.341005 IP 192.168.0.2.2994 > 192.168.0.1.707: P 798:816(18) ack 173 win 17348 (DF)
11:53:55.511241 IP 192.168.0.1.707 > 192.168.0.2.2994: . ack 816 win 16705 (DF)
11:53:57.796 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:57.827 File Modified: C:\WINDOWS\system32\config\system.LOG
      :      :      :
      :      :      :
11:53:58.452 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.468 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.499 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.514 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.561 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:56.409528 IP 192.168.0.1.707 > 192.168.0.2.2994: R 506886228:506886228(0) win 0 (DF)
11:53:58.624 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.671 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.686 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.780 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:58.936 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:59.139 File Modified: C:\WINDOWS\system32\config\system.LOG
11:53:59.233 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:02.468 File Modified: C:\WINDOWS\system32\msblast.exe
11:54:02.499 File Removed: C:\WINDOWS\system32\msblast.exe
11:54:02.796 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:02.858 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:02.952 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:02.968 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:03.014 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:03.046 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:03.124 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:03.155 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:03.171 File Modified: C:\WINDOWS\system32\config\system.LOG
11:54:03.780 File Modified: C:\WINDOWS\system32\wbem\Logs\wbemess.log
11:54:05.577331 IP 192.168.0.2 > 192.168.0.1: icmp 72: echo request seq 256

```

図 4-7 W32/Nachi.worm ウイルス検出例

4.3.5 W32/Hybris.gen@MM

(1) ウイルスの概要

W32/Hybris.gen@MM の概要を表 4-11に示す。^{11, 12}

表 4-11 W32/Hybris.gen@MM の概要

種別	ワーム
特徴	メールに添付して拡散する。
プラットフォーム	Windows 全般
動作概要	メール添付されたこのワームの実行により WSOCK32.DLL ファイルが変更もしくは置き換えられる。これによりすべての送信メールにワームを添付するようになる。

本ウイルスの拡散手段はメール添付のみである。このタイプのウイルスは本ウイルス検出プログラムでは検出の見込みがないため、今回の実験では上記ウイルス調査に止め、データ採取までは行わなかった。

4.3.6 W32/Magistr.a@MM

(1) ウイルスの概要

W32/Magistr.a@MM の概要を表 4-12に示す。^{13, 14}

表 4-12 W32/Magistr.a@MM の概要

種別	ウイルス、ワーム
特徴	メールに添付して拡散する。またネットワークを経由して拡散する。
プラットフォーム	Windows 95、Windows98、WindowsNT、Windows2000、WindowsMe、WindowsXP
動作概要	.dll ファイルを除く Windows Portable Executable ファイルに感染する。 メール添付されたこのワームの実行により Explorer.exe の使用しているメモリ空間にある読み込み可能、書き込み可能、初期化済の領域を探し、見つかった場合は 110 バイトのプログラムルーチンを挿入し活動する。 感染可能ファイルを最大 20 個探し、そのうちの一つに感染し、最大 100 件のメールアドレスに送信する。 ローカルのハードディスクや共有されているネットワーク上の全てのドライブから感染対象となるファイルを検索し、その場所に Windows ディレクトリがあれば run=行を追加する。

(2) 実験環境の設定

本ウイルスはネットワーク共有の機能を悪用する。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-13に示す。

表 4-13 W32/Magistr.a@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む)	-

設定項目	感染先マシン	攻撃マシン
	共有ディレクトリ (サブディレクトリ含む)	

本実験では、感染先マシンの C:\Documents and Settings\All Users\Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ（Eドライブ）として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 139 だけの指定でもネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

（ 3 ） 実験結果

結果：実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.7 W32/Magistr.b@MM

(1) ウイルスの概要

W32/Magistr.b@MM の概要を表 4-14に示す。^{15, 16}

表 4-14 W32/Magistr.b@MM の概要

種別	ウイルス
特徴	メールに添付して拡散する。またネットワークを経由して拡散する。
プラットフォーム	Windows 95、Windows98、WindowsNT、Windows2000、WindowsMe、WindowsXP
動作概要	.dll ファイルを除く Windows Portable Executable ファイルに感染する。 メール添付されたこのワームの実行により system.ini ファイルの Boot セクション内にある Shell=explorer.exe に W32.Magistr.Trojan を呼び出す命令項目を追加する。 Windows および Eudora のアドレス帳、Outlook Express の送信済みアイテム、Netscape の送信済みアイテムのファイルから取得したメールアドレス全てに送信する。 ローカルのハードディスクや共有されているネットワーク上の全てのドライブから感染対象となるファイルを検索し、感染する。

(2) 実験環境の設定

本ウイルスはネットワーク共有の機能を悪用する。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-15に示す。

表 4-15 W32/Magistr.b@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ	-

設定項目	感染先マシン	攻撃マシン
	(サブディレクトリ含む)	

本実験では、感染先マシンの C:\Documents and Settings\All Users\Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ（Eドライブ）として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 139 だけの指定でもネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

（ 3 ）実験結果

結果：実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.8 W32/CodeRed.worm.c

(1) ウイルスの概要

W32/CodeRed.worm.c の概要を表 4-16に示す。^{17, 18, 19}

表 4-16 W32/CodeRed.worm.c の概要

種別	ワーム
特徴	バッファ・オーバーフローと呼ばれる脆弱点を悪用して自分を繁殖させる。この脆弱点は、「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)」ものである。
プラットフォーム	Windows 2000, Windows NT4.0
動作概要	子スレッドを 300 ないし 600 個作成する。作成された子スレッドはワーム活動を繰り返し行う。 各スレッドはそれぞれランダムな IP アドレスを作成し、セキュリティホールを狙った HTTP アクセス (TCP/IP 転送のポート 80 番) でワームのコードを送信する。 C:ドライブおよび D:ドライブのルートディレクトリに"explorer.exe"というファイルを作成する。このファイルは Web サーバーのローカルドライブに外部からアクセスできるように設定するためのハッキングツール (トロイの木馬) である。 また、Windows のシステムファイルである"cmd.exe"を以下のパスにコピーする C:¥inetpub¥scripts¥root.exe D:¥inetpub¥scripts¥root.exe C:¥Program Files¥common files¥system¥MSADC¥root.exe D:¥Program Files¥common files¥system¥MSADC¥root.exe レジストリの改ざんを行う。

なお、Network Associates 社の Web サイトで公開されているウイルス検索では W32/CodeRed.worm.c という名称に一致するものは見当たらなかった。W32/CodeRed.c.worm として公開されているものがこれに該当すると思われる。表 4-16は W32/CodeRed.c.worm の名称からまとめたものである。

(2) 実験環境の設定

OS の脆弱性情報²⁰より、Web セッションの確立に使用されるポートが悪用される。通常、Web サーバーが提供するサービス (http サービス) のポート番号は 80 である。

実験環境の設定を表 4-17に示す。

表 4-17 W32/CodeRed.worm.c 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows 2000 Professional	Windows 2000 Professional
メモリ	96MB	64MB
IP アドレス	192.168.0.1	192.168.0.2
監視対象 IP アドレス	192.168.0.1	-
監視対象 ポート番号	80	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥Inetpub (サブディレクトリ含む) C:¥Program Files¥Common Files (サブディレクトリ含む) C:¥WINNT (サブディレクトリ含まず) C:¥WINNT¥system32 (サブディレクトリ含む)	-

本実験では、Web サーバーである IIS (Internet Information Services) の稼動環境を想定しているため、IIS 関連のディレクトリを監視対象に含めている。

また、Windows システムディレクトリはサブディレクトリも含めて監視ディレクトリに指定している。この設定だと、config サブディレクトリに置かれている Windows のレジストリ情報関連ファイルの変更まで検出することになる。これによってウイルス動作によるレジストリの書き換えを検出することも可能であるが、他の正常な動作によるレジストリ書き換えも考慮するならばレジストリ情報関連ファイルを除外する設定でも検出可能でなければならないと考えられる。

なお、ウイルスは D:ドライブにも変更を加えるようであるが、実験システムの D:ドライブは CD-ROM であるため除外した。複数のドライブに Windows をインストールしているような場合には、これも監視に含めるべきであろう。

(3) 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの C:ドライブのルートディレクトリにファイル explorer.exe が作成されたかどうかで判別することができる。

ウイルス本体が感染を試みる IP アドレスはランダム的に生成されるが、入手した検体はウイルスが送信するデータをファイル化したものであったため、感染先 IP アドレスの 80 番ポートに TCP/IP 接続を確立し、このデータファイルの内容を送信するプログラムを用意して実験を行った。

結果：実験期間中に 3 回の侵入が認められ、3 回ともウイルスを検出することができた。

図 4-8に W32/CodeRed.worm.c ウイルス検出の一例を示す。

でポート番号 80 へのアクセスを検出、その後のディレクトリ監視により、でウイルスの動作（レジストリ情報関連のファイルが変更された）を検出している。レジストリ情報関連の変更を無視することにしても、でウイルスの侵入（C:\Inetpub\Scripts ディレクトリに root.exe ファイルが作成された）を検出することができる。

さらに、図 4-8のデータからは、表 4-16に記載したウイルス動作の様子までうかがい知ることができる。以下に、その様子を説明する。

攻撃マシンから感染先マシンへの脆弱性ポート番号 80 へのアクセス。

レジストリ情報関連のファイルが変更された。

C:\Inetpub\Scripts ディレクトリにファイル root.exe が作成された。

C:ドライブのルートディレクトリにファイル explorer.exe が作成された。

```
Watch Started. IP: 192.168.0.1 Port: 80
C:\Program Files\Watch\WINDUMP.EXE: listening on %Device%\NPF_{79A1D903-846C-405F-A513-83EE9459122F}
18:10:03.894562 IP 192.168.0.2.1033 > 192.168.0.1.80: S 3172163467:3172163467(0) win 16384 <mss 1460,nop,n
18:10:03.962471 IP 192.168.0.1.80 > 192.168.0.2.1033: S 4023193903:4023193903(0) ack 3172163468 win 17520
18:10:03.988583 IP 192.168.0.2.1033 > 192.168.0.1.80: . ack 1 win 17520 (DF)
18:10:04.015702 IP 192.168.0.2.1033 > 192.168.0.1.80: . 1:1461(1460) ack 1 win 17520 (DF)
18:10:04.056056 IP 192.168.0.2.1033 > 192.168.0.1.80: . 1461:2921(1460) ack 1 win 17520 (DF)
18:10:04.078631 IP 192.168.0.1.80 > 192.168.0.2.1033: . ack 2921 win 17520 (DF)
18:10:04.106059 IP 192.168.0.2.1033 > 192.168.0.1.80: P 2921:3819(898) ack 1 win 17520 (DF)
18:10:04.289147 IP 192.168.0.1.80 > 192.168.0.2.1033: . ack 3819 win 16622 (DF)
18:10:05.777 File Modified: C:\WINNT\system32\config\SAM.LOG
18:10:05.808 File Modified: C:\WINNT\system32\config\SAM.LOG
18:10:05.808 File Modified: C:\WINNT\system32\config\SAM.LOG
18:10:09.511 File Modified: C:\WINNT\system32\config\software.LOG
18:10:09.542 File Modified: C:\WINNT\system32\config\software.LOG
18:10:09.558 File Modified: C:\WINNT\system32\config\software.LOG
18:10:16.199 File Modified: C:\WINNT\system32\config\software.LOG
18:10:16.511 File Modified: C:\WINNT\system32\config\software.LOG
18:10:16.871 File Modified: C:\WINNT\system32\config\software.LOG
18:10:17.042 File Modified: C:\WINNT\system32\config\software
18:10:17.074 File Modified: C:\WINNT\system32\config\software
18:10:17.121 File Modified: C:\WINNT\system32\config\software
18:10:17.136 File Modified: C:\WINNT\system32\config\software.LOG
18:10:18.780482 IP 192.168.0.1.80 > 192.168.0.2.1033: P 1:2(1) ack 3819 win 16622 (DF)
18:10:19.078996 IP 192.168.0.2.1033 > 192.168.0.1.80: . ack 2 win 17519 (DF)
18:10:26.980 File Added: C:\Inetpub\Scripts\root.exe
18:10:27.214 File Modified: C:\Inetpub\Scripts\root.exe
18:10:27.683 File Modified: C:\Inetpub\Scripts\root.exe
18:10:27.839 File Added: C:\explorer.exe
18:10:28.042 File Modified: C:\explorer.exe
18:11:05.808 File Modified: C:\WINNT\system32\config\SAM.LOG
18:11:05.855 File Modified: C:\WINNT\system32\config\SAM.LOG
18:11:05.902 File Modified: C:\WINNT\system32\config\SAM.LOG
18:11:06.402 File Modified: C:\WINNT\system32\config\SAM
18:11:06.542 File Modified: C:\WINNT\system32\config\SAM
18:11:06.605 File Modified: C:\WINNT\system32\config\SAM
18:11:06.683 File Modified: C:\WINNT\system32\config\SAM.LOG
```

図 4-8 W32/CodeRed.worm.c ウイルス検出例

なお、図 4-8 のデータでは、表 4-16 に示されるウイルス動作のうち、C:\Program Files\common files\system\MSADC ディレクトリへの root.exe ファイルの作成は検出されていない。しかし、後で当該ディレクトリを調べてみても root.exe ファイルは存在せず、検出漏れではないことを確認している。

4.3.9 W32/CodeRed.worm.f

(1) ウイルスの概要

W32/CodeRed.worm.f の概要を表 4-18に示す。^{21, 22, 23}

表 4-18 W32/CodeRed.worm.f の概要

種別	ワーム
特徴	バッファ・オーバーフローと呼ばれる脆弱点を悪用して自分を繁殖させる。この脆弱点は、「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)」ものである。
プラットフォーム	Windows 2000, Windows NT4.0
動作概要	子スレッドを 300 ないし 600 個作成する。作成された子スレッドはワーム活動を繰り返し行う。 各スレッドはそれぞれランダムな IP アドレスを作成し、セキュリティホールを狙った HTTP アクセス (TCP/IP 転送のポート 80 番) でワームのコードを送信する。 C:ドライブおよび D:ドライブのルートディレクトリに"explorer.exe"というファイルを作成する。このファイルは Web サーバーのローカルドライブに外部からアクセスできるように設定するためのハッキングツール (トロイの木馬) である。 また、Windows のシステムファイルである "cmd.exe" を以下のパスにコピーする C:¥inetpub¥scripts¥root.exe D:¥inetpub¥scripts¥root.exe C:¥Program Files¥common files¥system¥MSADC¥root.exe D:¥Program Files¥common files¥system¥MSADC¥root.exe レジストリの改ざんを行う。

なお、Network Associates 社の Web サイトで公開されているウイルス検索では W32/CodeRed.worm.f という名称に一致するものは見当たらなかった。W32/CodeRed.f.worm として公開されているものがこれに該当すると思われる。表 4-18は W32/CodeRed.f.worm の名称からまとめたものである。このウイルスは亜種 F となっているが、亜種 C (W32/CodeRed.c.worm) とほとんど同一である。

(2) 実験環境の設定

OS の脆弱性情報²⁰より、Web セッションの確立に使用されるポートが悪用される。通常、Web サーバーが提供するサービス (http サービス) のポート番号は 80 である。

実験環境の設定を表 4-19に示す。

表 4-19 W32/CodeRed.worm.f 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows 2000 Professional	Windows 2000 Professional
メモリ	96MB	64MB
IP アドレス	192.168.0.1	192.168.0.2
監視対象 IP アドレス	192.168.0.1	-
監視対象 ポート番号	80	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥Inetpub (サブディレクトリ含む) C:¥Program Files¥Common Files (サブディレクトリ含む) C:¥WINNT (サブディレクトリ含まず) C:¥WINNT¥system32 (サブディレクトリ含む)	-

本実験では、Web サーバーである IIS (Internet Information Services) の稼動環境を想定しているため、IIS 関連のディレクトリを監視対象に含めている。

また、Windows システムディレクトリはサブディレクトリも含めて監視ディレクトリに指定している。この設定だと、config サブディレクトリに置かれている Windows のレジストリ情報関連ファイルの変更まで検出することになる。これによってウイルス動作によるレジストリの書き換えを検出することも可能であるが、他の正常な動作によるレジストリ書き換えも考慮するならばレジストリ情報関連ファイルを除外する設定でも検出可能でなければならぬと考えられる。

なお、ウイルスは D:ドライブにも変更を加えるようであるが、実験システムの D:ドライブは CD-ROM であるため除外した。複数のドライブに Windows をインストールしているような場合には、これも監視に含めるべきであろう。

(3) 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの C:ドライブのルートディレクトリにファイル explorer.exe が作成されたかどうかで判別することができる。

ウイルス本体が感染を試みる IP アドレスはランダム的に生成されるが、入手した検体はウイルスが送信するデータをファイル化したものであったため、感染先 IP アドレスの 80 番ポートに TCP/IP 接続を確立し、このデータファイルの内容を送信するプログラムを用意して実験を行った。

結果：実験期間中に 3 回の侵入が認められ、3 回ともウイルスを検出することができた。

図 4-9に W32/CodeRed.worm.f ウイルス検出の一例を示す。

でポート番号 80 へのアクセスを検出、その後のディレクトリ監視により、でウイルスの動作（レジストリ情報関連のファイルが変更された）を検出している。レジストリ情報関連の変更を無視することにしても、でウイルスの侵入（C:\Inetpub\Scripts ディレクトリに root.exe ファイルが作成された）を検出することができる。

さらに、図 4-9のデータからは、表 4-18に記載したウイルス動作の様子までうかがい知ることができる。以下に、その様子を説明する。

- 攻撃マシンから感染先マシンへの脆弱性ポート番号 80 へのアクセス。
- レジストリ情報関連のファイルが変更された。
- C:\Inetpub\Scripts ディレクトリにファイル root.exe が作成された。
- C:\ドライブのルートディレクトリにファイル explorer.exe が作成された。

```
Watch Started. IP: 192.168.0.1 Port: 80
C:\Program Files\Watch\WINDUMP.EXE: listening on %Device%\NPF_{79A1D903-846C-405F-A513-83EE9459122F}
14:21:26.826205 IP 192.168.0.2.1033 > 192.168.0.1.80: S 3126388467:3126388467(0) win 16384 <mss 1460,nop,n
14:21:26.970788 IP 192.168.0.1.80 > 192.168.0.2.1033: S 4015793903:4015793903(0) ack 3126388468 win 17520
14:21:27.004074 IP 192.168.0.2.1033 > 192.168.0.1.80: . ack 1 win 17520 (DF)
14:21:27.006207 IP 192.168.0.2.1033 > 192.168.0.1.80: . 1:1461(1460) ack 1 win 17520 (DF)
14:21:27.052678 IP 192.168.0.2.1033 > 192.168.0.1.80: . 1461:2921(1460) ack 1 win 17520 (DF)
14:21:27.062041 IP 192.168.0.1.80 > 192.168.0.2.1033: . ack 2921 win 17520 (DF)
14:21:27.085854 IP 192.168.0.2.1033 > 192.168.0.1.80: P 2921:3819(898) ack 1 win 17520 (DF)
14:21:27.118974 IP 192.168.0.1.80 > 192.168.0.2.1033: . ack 3819 win 16622 (DF)
14:21:29.459 File Modified: C:\WINNT\system32\config\SAM.LOG
14:21:29.538 File Modified: C:\WINNT\system32\config\SAM.LOG
14:21:29.584 File Modified: C:\WINNT\system32\config\SAM.LOG
14:21:35.163 File Modified: C:\WINNT\system32\config\software.LOG
14:21:35.194 File Modified: C:\WINNT\system32\config\software.LOG
14:21:35.194 File Modified: C:\WINNT\system32\config\software.LOG
14:21:44.428 File Modified: C:\WINNT\system32\config\software.LOG
14:21:44.522 File Modified: C:\WINNT\system32\config\software.LOG
14:21:44.584 File Modified: C:\WINNT\system32\config\software.LOG
14:21:44.600 File Modified: C:\WINNT\system32\config\software
14:21:44.616 File Modified: C:\WINNT\system32\config\software
14:21:44.616 File Modified: C:\WINNT\system32\config\software
14:21:44.631 File Modified: C:\WINNT\system32\config\software.LOG
14:21:53.811006 IP 192.168.0.1.80 > 192.168.0.2.1033: P 1:2(1) ack 3819 win 16622 (DF)
14:21:54.012180 IP 192.168.0.2.1033 > 192.168.0.1.80: . ack 2 win 17519 (DF)
14:22:12.350 File Added: C:\Inetpub\Scripts\root.exe
14:22:12.475 File Modified: C:\Inetpub\Scripts\root.exe
14:22:14.694 File Modified: C:\Inetpub\Scripts\root.exe
14:22:15.006 File Added: C:\explorer.exe
14:22:15.413 File Modified: C:\explorer.exe
14:22:30.131 File Modified: C:\WINNT\system32\config\SAM.LOG
14:22:30.319 File Modified: C:\WINNT\system32\config\SAM.LOG
14:22:30.381 File Modified: C:\WINNT\system32\config\SAM.LOG
14:22:30.522 File Modified: C:\WINNT\system32\config\SAM
14:22:31.397 File Modified: C:\WINNT\system32\config\SAM
14:22:31.881 File Modified: C:\WINNT\system32\config\SAM
14:22:31.928 File Modified: C:\WINNT\system32\config\SAM.LOG
```

図 4-9 W32/CodeRed.worm.f ウイルス検出例

なお、図 4-9 のデータでは、表 4-18 に示されるウイルス動作のうち、C:\Program Files\common files\system\MSADC ディレクトリへの root.exe ファイルの作成は検出されていない。しかし、後で当該ディレクトリを調べてみても root.exe ファイルは存在せず、検出漏れではないことを確認している。

4.3.10 W32/CodeGreen.dr

(1) ウイルスの概要

W32/CodeGreen.dr の概要を表 4-20に示す。^{24, 25, 26}

表 4-20 W32/CodeGreen.dr の概要

種別	ワーム
特徴	Code Red と同様に MS01-033 のセキュリティホールを利用しワーム活動を行い、Code Red の活動を停止させる。(“ワーム駆除”ワーム)
プラットフォーム	Windows NT
動作概要	ランダムに IP アドレスを作成し、セキュリティホールを狙った HTTP リクエストで自身のコードを送信する。 セキュリティホールを持った IIS サーバーがこの HTTP リクエストを受信すると、送信されてきたワームのプログラムコードがメモリ上で直接実行される。 MS サイトからパッチをダウンロードして適用する。 C:ドライブと D:ドライブのルートディレクトリに"EXPLORER.EXE"というファイル名のファイルがあった場合、"ex_Xer_X_"というファイル名にリネームする。

なお、Network Associates 社の Web サイトで公開されているウイルス検索では W32/CodeGreen.dr という名称に一致するものは見当たらなかった。表 4-20は"Code Green"という一般的な名称から情報を収集してまとめたものである。

(2) 実験環境の設定

OS の脆弱性情報²⁰より、Web セッションの確立に使用されるポートが悪用される。通常、Web サーバーが提供するサービス (http サービス) のポート番号は 80 である。

実験環境の設定を表 4-21に示す。

表 4-21 W32/CodeGreen.dr 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows NT Server 4.0	Windows NT Server 4.0
メモリ	64MB	64MB
IP アドレス	192.168.0.3	192.168.0.4
監視対象 IP アドレス	192.168.0.3	-
監視対象 ポート番号	80	-

設定項目	感染先マシン	攻撃マシン
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥InetPub (サブディレクトリ含む) C:¥Program Files¥Common Files (サブディレクトリ含む) C:¥WINNT (サブディレクトリ含まず) C:¥WINNT¥system32 (サブディレクトリ含む)	-

ウイルス情報では、プラットフォームは Windows NT となっている。また、ウイルスが利用する脆弱性情報より、Windows NT 4.0 のサービスパック 3 以上で利用可能な IIS 4.0、Index Server 2.0 が必要である。攻撃マシン・感染先マシンとも、実験環境の Windows NT には、ウイルス発生の 2001 年 9 月当時にごく一般的に利用されていたサービスパック 4 (西暦 2000 年問題の改善版)、IIS 4.0、Index Server 2.0 を適用した。

本実験では、Web サーバーである IIS (Internet Information Services) の稼動環境を想定しているため、IIS 関連のディレクトリを監視対象に含めている。

なお、ウイルスは D:ドライブにも変更を加えるようであるが、実験システムの D:ドライブは CD-ROM であるため除外した。複数のドライブに Windows をインストールしているような場合には、これも監視に含めるべきであろう。

注) 今回試作したウイルス検出プログラムは本ウイルスのプラットフォーム (Windows NT) には正式には対応していない。しかし、Microsoft Visual C++ 6.0 の MFC dll をインストールする追加作業により、本環境での動作には問題なく利用できることを事前に確認した。

(3) 実験結果

ウイルス本体が感染を試みる IP アドレスはランダム的に生成されるが、入手した検体を攻撃マシンで実行しても IP アドレスをスキャンするような兆候は観測されなかった。また、攻撃マシンや感染先マシンの C:ドライブのルートディレクトリにダミーの EXPLORER.EXE ファイルを作成しておいてもリネームされることはなかった。システム日付をウイルス発生当時に変更する、Windows 2000 環境で実行する (本ウイルスが駆除対象としている Code Red は Windows 2000 にも感染する) などしても、やはりウイルスが活動する兆候は見られなかった。

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

ウイルスが活動しなかった原因としては、ウイルス内部の動作アルゴリズムや動作環境によるものが考えられる。例えば、今回の実験はウイルスが外部に流出しないよう、VMware の仮想環境上で行っており、Microsoft 社のダウンロードサイトへの接続環境は整っていない。

ウイルスはパッチを適用しようとするはずであるが、上記のような環境では活動を停止してしまうのかもしれない。

仮に、Microsoft 社のダウンロードサイトへの接続環境を整え、ウイルスが侵入活動を開始したとすれば、パッチをダウンロードする際のディレクトリ変更によりウイルス検出は可能と考えられる。

ただし、攻撃対象として選択する IP アドレスの生成が完全にランダムだったなら、IP アドレスを固定した感染先マシンが選択されるような偶然是期待薄であり、実験時、感染先マシンにウイルスを誘導するための工夫が必要になると思われる。

4.3.11 W32/Klez.gen@MM

(1) ウイルスの概要

W32/Klez.gen@MM の概要を表 4-22に示す。^{27, 28}

表 4-22 W32/Klez.gen@MM の概要

種別	ウイルス、ワーム
特徴	Windows のアドレス帳で発見したメールアドレス全てに自分自身を送信する。その際スプーフィングを行うことがある。メールを開封あるいはプレビューするだけで添付ファイルが自動的に実行されるように Microsoft Outlook または Outlook Express の脆弱性 MS01-020 を利用する。
プラットフォーム	Windows95 , Windows98 , WindowsNT , WindowsMeWindows 2000, Windows XP
動作概要	Windows のアドレス帳を探し、発見した全メールアドレス宛てに.bat、.exe、.pif、.scr のうちいずれかの拡張子がついたファイルを添付して送信する。 ネットワーク共有ドライブすべてに自分自身をコピーするよう試みる。

(2) 実験環境の設定

本ウイルスはネットワーク共有の機能を悪用する。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-23に示す。

表 4-23 W32/Klez.gen@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:\Documents and Settings\All Users\Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ (E ドライブ) として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 139 だけの指定でもネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

(3) 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの共有ディレクトリ (C:\Documents and Settings\All Users\Documents) にウイルスのファイルが作成されたかどうかで判別することができる。

結果：実験期間中に 2 回の侵入が認められ、2 回ともウイルスを検出することができた。

図 4-10 に W32/Klez.gen@MM ウイルス検出の一例を示す。

でポート番号 139 へのアクセスを検出、その後のディレクトリ監視により、 でウイルスの侵入 (監視対象ディレクトリにファイル Sq.htm.exe が作成された) を検出している。

```

Watch Started. IP: 192.168.0.2 Port: 0-1023
C:\Documents and Settings\q\Desktop\Watch\WINDUMP.EXE: listening on Device\NPF_{961F4243-0606-49BD-91C6-7A
17:04:13.629726 IP 192.168.0.1.1061 > 192.168.0.2.139: S 518486481:518486481(0) win 16384 <mss 1460,nop,n ←
17:04:13.636129 IP 192.168.0.2.139 > 192.168.0.1.1061: S 3562451129:3562451129(0) ack 518486482 win 17520
17:04:13.645862 IP 192.168.0.1.1061 > 192.168.0.2.139: P 1:73(72) ack 1 win 17520 (DF)
17:04:13.654366 IP 192.168.0.2.139 > 192.168.0.1.1061: P 1:5(4) ack 73 win 17448 (DF)
:
:
:
17:04:37.625339 IP 192.168.0.2.139 > 192.168.0.1.1061: P 5481:5541(60) ack 5067 win 17186 (DF)
17:04:37.647808 IP 192.168.0.1.1071 > 192.168.0.2.80: S 524045349:524045349(0) win 16384 <mss 1460,nop,n
17:04:37.649609 IP 192.168.0.2.80 > 192.168.0.1.1071: S 3568005265:3568005265(0) ack 524045350 win 17520
17:04:37.674709 IP 192.168.0.1.1071 > 192.168.0.2.80: . ack 1 win 17520 (DF)
17:04:37.676798 IP 192.168.0.1.1071 > 192.168.0.2.80: P 1:152(151) ack 1 win 17520 (DF)
17:04:37.774602 IP 192.168.0.1.1061 > 192.168.0.2.139: . ack 5541 win 16545 (DF)
17:04:37.865114 IP 192.168.0.2.80 > 192.168.0.1.1071: . ack 152 win 17369 (DF)
17:04:42.097 File Modified: C:\WINDOWS\system32\config\software.LOG
17:04:42.129 File Modified: C:\WINDOWS\system32\config\software.LOG
17:04:42.222 File Modified: C:\WINDOWS\system32\config\system.LOG
17:04:42.254 File Modified: C:\WINDOWS\system32\config\system.LOG
17:04:42.582 File Modified: C:\WINDOWS\system32\wbem\Logs\wmprov.log
17:04:42.707 File Modified: C:\WINDOWS\system32\wbem\Logs\wmprov.log
17:04:42.754 File Modified: C:\WINDOWS\system32\wbem\Logs\wmiadap.log
17:04:42.785 File Modified: C:\WINDOWS\system32\config\software.LOG
17:04:42.847 File Modified: C:\WINDOWS\system32\wbem\Logs\wbemess.log
17:04:43.457 File Modified: C:\WINDOWS\Registration
17:04:43.957 File Modified: C:\WINDOWS\Registration
17:04:43.491822 IP 192.168.0.2.138 > 192.168.0.255.138: udp 179
17:04:45.519 File Modified: C:\WINDOWS\system32\config\software.LOG
17:04:48.082 File Added: C:\WINDOWS\system32\Logfiles\W3SVC1
17:04:48.238 File Added: C:\WINDOWS\system32\Logfiles\W3SVC1\ex031203.log
17:04:48.300 File Modified: C:\WINDOWS\system32\Logfiles\W3SVC1\ex031203.log
17:04:47.943581 IP 192.168.0.2.80 > 192.168.0.1.1071: P 1:394(393) ack 152 win 17369 (DF)
17:04:47.972046 IP 192.168.0.1.1071 > 192.168.0.2.80: P 152:324(172) ack 394 win 17127 (DF)
17:04:48.171854 IP 192.168.0.2.80 > 192.168.0.1.1071: . ack 324 win 17197 (DF)
17:04:48.754 File Added: C:\Documents and Settings\All Users\Documents\Sq.htm.exe ←
17:04:48.894 File Modified: C:\Documents and Settings\All Users\Documents\Sq.htm.exe
17:04:49.004 File Modified: C:\Documents and Settings\All Users\Documents\Sq.htm.exe

```

図 4-10 W32/Klez.gen@MM ウイルス検出例

4.3.12 W32/Klez.h@MM

(1) ウイルスの概要

W32/Klez.h@MM の概要を表 4-24 に示す。^{29, 30}

表 4-24 W32/Klez.h@MM の概要

種別	ウイルス、ワーム
特徴	Windows のアドレス帳で発見したメールアドレス全てに自分自身を送信する。その際スプーフィングを行うことがある。メールを開封あるいはプレビューするだけで添付ファイルが自動的に実行されるように Microsoft Outlook または Outlook Express の脆弱性 MS01-020 を利用する。
プラットフォーム	Windows95 , Windows98 , WindowsNT , WindowsMeWindows 2000, Windows XP
動作概要	Windows のアドレス帳を探し、発見した全メールアドレス宛てに.bat、.exe、.pif、.scr のうちいずれかの拡張子がついたファイルを添付して送信する。 ネットワーク共有ドライブすべてに自分自身をコピーするよう試みる。

(2) 実験環境の設定

本ウイルスはネットワーク共有の機能を悪用する。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-25 に示す。

表 4-25 W32/Klez.h@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:\Documents and Settings\All Users\Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ (E ドライブ) として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 139 だけの指定でもネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

(3) 実験結果

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.13 W32/Klez.e@MM

(1) ウイルスの概要

W32/Klez.e@MM の概要を表 4-26に示す。^{31, 32}

表 4-26 W32/Klez.e@MM の概要

種別	ウイルス、ワーム
特徴	Windows のアドレス帳で発見したメールアドレス全てに自分自身を送信する。その際スプーフィングを行うことがある。メールを開封あるいはプレビューするだけで添付ファイルが自動的に実行されるように Microsoft Outlook または Outlook Express の脆弱性 MS01-020 を利用する。
プラットフォーム	Windows95 , Windows98 , WindowsNT , WindowsMeWindows 2000, Windows XP
動作概要	Windows のアドレス帳を探し、発見した全メールアドレス宛てに.bat、.exe、.pif、.scr のうちいずれかの拡張子がついたファイルを添付して送信する。 ネットワーク共有ドライブすべてに自分自身をコピーするよう試みる。

(2) 実験環境の設定

本ウイルスはネットワーク共有の機能を悪用する。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-27に示す。

表 4-27 W32/Klez.e@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象ポート番号	0-1023	-
監視対象ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:\Documents and Settings\All Users\Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ (E ドライブ) として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 139 だけの指定でもネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

(3) 実験結果

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.14 W32/Nimda.gen@MM

(1) ウイルスの概要

W32/Nimda.gen@MM の概要を表 4-28に示す。^{33, 34}

表 4-28 W32/Nimda.gen@MM の概要

種別	ワーム
特徴	さまざまなウイルスの感染方法を取り入れた複合型のウイルス。自身を添付したメール送信による感染、共有ネットワークに接続したパソコンへの感染、Microsoft Internet Explorer のセキュリティホールからの感染等がある。
プラットフォーム	Windows 95、Windows98、WindowsNT、Windows2000、WindowsMe
動作概要	Microsoft IIS 4.0 および 5.0 の Web サーバーに感染を試みる マイネットワーク全体を調べ、また、ランダムに作成した IP アドレスで検索することによって、ネットワーク上で開いている共有をすべて探し出し、そこにあるすべてのファイルをチェックして、感染対象となるファイルを探す。 .EML、.NWS ファイルを開いているネットワーク共有にコピーし、.DOC ファイルを含むフォルダすべてに自分自身を Riched20.dll としてコピーする。 ローカルシステム上に存在する .htm、.html ファイルに含まれる電子メールアドレスを探す。また、MAPI を使って、電子メールクライアントの受信トレイ内にあるメールを調べる。入手したメールアドレスを、差出人と宛先のアドレスとして使用し送信する。

なお、Network Associates 社の Web サイトで公開されているウイルス検索では、W32/Nimda.gen@MM は W32/Nimda.a@MM の亜種としか記載されていなかった。表 4-28 は W32/Nimda.a@MM の名称で公開されている情報をもとにまとめたものである。

(2) 実験環境の設定

OS の脆弱性情報³⁵より、Web セッションの確立に使用されるポートが悪用される。通常、Web サーバーが提供するサービス (http サービス) のポート番号は 80 である。また、ネットワーク共有の機能も悪用される。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-29に示す。

表 4-29 W32/Nimda.gen@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows 2000 Professional
メモリ	128MB	80MB
IP アドレス	192.168.0.2	192.168.0.128
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:¥Documents and Settings¥All Users¥Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ（Eドライブ）として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 80 と 139 だけの指定でも Web サービスやネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

(3) 実験結果

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.15 W32/Nimda@MM

(1) ウイルスの概要

W32/Nimda@MM の概要を表 4-30に示す。^{33, 36}

表 4-30 W32/Nimda@MM の概要

種別	ワーム
特徴	さまざまなウイルスの感染方法を取り入れた複合型のウイルス。自身を添付したメール送信による感染、共有ネットワークに接続したパソコンへの感染、Microsoft Internet Explorer のセキュリティホールからの感染等がある。
プラットフォーム	Windows 95、Windows98、WindowsNT、Windows2000、WindowsMe
動作概要	Microsoft IIS 4.0 および 5.0 の Web サーバーに感染を試みる マイネットワーク全体を調べ、また、ランダムに作成した IP アドレスで検索することによって、ネットワーク上で開いている共有をすべて探し出し、そこにあるすべてのファイルをチェックして、感染対象となるファイルを探す。 .EML、.NWS ファイルを開いているネットワーク共有にコピーし、.DOC ファイルを含むフォルダすべてに自分自身を Riched20.dll としてコピーする。 ローカルシステム上に存在する .htm、.html ファイルに含まれる電子メールアドレスを探す。また、MAPI を使って、電子メールクライアントの受信トレイ内にあるメールを調べる。入手したメールアドレスを、差出人と宛先のアドレスとして使用し送信する。

なお、Network Associates 社の McAfee VirusScan で W32/Nimda@MM と表示されるものはベンダーにより Nimda.G と呼ばれるもので、亜種 D・E とほとんど同じものである。

(2) 実験環境の設定

OS の脆弱性情報³⁵より、Web セッションの確立に使用されるポートが悪用される。通常、Web サーバーが提供するサービス (http サービス) のポート番号は 80 である。また、ネットワーク共有の機能も悪用される。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-31に示す。

表 4-31 W32/Nimda@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows 2000 Professional
メモリ	128MB	80MB
IP アドレス	192.168.0.2	192.168.0.128
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:¥Documents and Settings¥All Users¥Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ（Eドライブ）として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 80 と 139 だけの指定でも Web サービスやネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

(3) 実験結果

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.16 W32/Nimda.s@MM

(1) ウイルスの概要

W32/Nimda.s@MM の概要を表 4-32に示す。^{33, 34}

表 4-32 W32/Nimda.s@MM の概要

種別	ワーム
特徴	さまざまなウイルスの感染方法を取り入れた複合型のウイルス。自身を添付したメール送信による感染、共有ネットワークに接続したパソコンへの感染、Microsoft Internet Explorer のセキュリティホールからの感染等がある。
プラットフォーム	Windows 95、Windows98、WindowsNT、Windows2000、WindowsMe
動作概要	Microsoft IIS 4.0 および 5.0 の Web サーバーに感染を試みる マイネットワーク全体を調べ、また、ランダムに作成した IP アドレスで検索することによって、ネットワーク上で開いている共有をすべて探し出し、そこにあるすべてのファイルをチェックして、感染対象となるファイルを探す。 .EML、.NWS ファイルを開いているネットワーク共有にコピーし、.DOC ファイルを含むフォルダすべてに自分自身を Riched20.dll としてコピーする。 ローカルシステム上に存在する .htm、.html ファイルに含まれる電子メールアドレスを探す。また、MAPI を使って、電子メールクライアントの受信トレイ内にあるメールを調べる。入手したメールアドレスを、差出人と宛先のアドレスとして使用し送信する。

なお、Network Associates 社の Web サイトで公開されているウイルス検索では W32/Nimda.s@MM という名称に一致するものは見当たらなかった。詳細は不明だが、W32/Nimda.a@MM と同様のものと考えられる。表 4-28は W32/Nimda.a@MM の名称で公開されている情報をもとにまとめたものである。

(2) 実験環境の設定

OS の脆弱性情報³⁵より、Web セッションの確立に使用されるポートが悪用される。通常、Web サーバーが提供するサービス (http サービス) のポート番号は 80 である。また、ネットワーク共有の機能も悪用される。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-33に示す。

表 4-33 W32/Nimda.s@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows 2000 Professional
メモリ	128MB	80MB
IP アドレス	192.168.0.2	192.168.0.128
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:¥Documents and Settings¥All Users¥Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ（Eドライブ）として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 80 と 139 だけの指定でも Web サービスやネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

（ 3 ） 実験結果

本ウイルスの感染先マシンへの侵入は、感染先マシンの共有ディレクトリ（ C:¥Documents and Settings¥All Users¥Documents ）にウイルスのファイルが作成されたかどうかで判別することができる。

結果：実験期間中に 2 回の侵入が認められ、2 回ともウイルスを検出することができた。

図 4-11に W32/Nimda.s@MM ウイルス検出の一例を示す。

でポート番号 139 へのアクセスを検出、その後のディレクトリ監視により、でウイルスの侵入（監視対象ディレクトリにファイル desktop.eml が作成された）を検出している。以下 ~ まで、拡張子が.eml または.nws のファイルや riched20.dll ファイルの作成を検出している。

```

Watch Started. IP: 192.168.0.2 Port: 0-1023
C:\Documents and Settings¥q¥デスクトップ¥¥Wwatch¥¥WINDUMP.EXE: listening on ¥Device¥NPF_{961F4243-0606-49B
15:57:47.957736 IP 192.168.0.128.1053 > 192.168.0.2.139: S 1434162503:1434162503(0) win 16384 <mss 1460,n
15:57:47.968477 IP 192.168.0.2.139 > 192.168.0.128.1053: S 3243755047:3243755047(0) ack 1434162504 win 1
15:57:47.980181 IP 192.168.0.128.1053 > 192.168.0.2.139: . ack 1 win 17520 (DF)
15:57:47.982764 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1:73(72) ack 1 win 17520 (DF)
15:57:47.995390 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1:5(4) ack 73 win 17448 (DF)
15:57:48.041316 IP 192.168.0.128.1053 > 192.168.0.2.139: P 73:210(137) ack 5 win 17516 (DF)
15:57:48.063994 IP 192.168.0.2.139 > 192.168.0.128.1053: P 5:94(89) ack 210 win 17311 (DF)
15:57:48.086074 IP 192.168.0.128.1053 > 192.168.0.2.139: P 210:394(184) ack 94 win 17427 (DF)
15:57:48.098333 IP 192.168.0.2.139 > 192.168.0.128.1053: P 94:441(347) ack 394 win 17127 (DF)
15:57:48.129640 IP 192.168.0.128.1053 > 192.168.0.2.139: P 394:728(334) ack 441 win 17080 (DF)
15:57:48.185881 IP 192.168.0.2.139 > 192.168.0.128.1053: P 441:562(121) ack 728 win 16793 (DF)
15:57:48.199552 IP 192.168.0.128.1053 > 192.168.0.2.139: P 728:840(112) ack 562 win 16959 (DF)
15:57:48.209800 IP 192.168.0.2.139 > 192.168.0.128.1053: P 562:628(66) ack 840 win 16681 (DF)
15:57:48.219457 IP 192.168.0.128.1053 > 192.168.0.2.139: P 840:980(140) ack 628 win 16893 (DF)
15:57:48.221406 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 980 win 16541 (DF)
15:57:48.230475 IP 192.168.0.2.139 > 192.168.0.128.1053: P 628:667(39) ack 980 win 16541 (DF)
15:57:48.260040 IP 192.168.0.128 > 192.168.0.2: icmp 40: echo request seq 2304
15:57:48.262350 IP 192.168.0.2 > 192.168.0.128: icmp 40: echo reply seq 2304
15:57:48.386882 IP 192.168.0.128.1053 > 192.168.0.2.139: . ack 667 win 16854 (DF)
15:58:18.288 File Modified: C:\¥WINDOWS¥system32¥config¥SAM.LOG
15:58:18.475 File Modified: C:\¥WINDOWS¥system32¥config¥SAM.LOG
15:58:18.522 File Modified: C:\¥WINDOWS¥system32¥config¥SAM.LOG
15:58:18.694 File Modified: C:\¥WINDOWS¥system32¥config¥SAM.LOG
15:58:34.069 File Modified: C:\¥WINDOWS¥system32¥config¥software.LOG
15:58:34.100 File Modified: C:\¥WINDOWS¥system32¥config¥software.LOG
15:58:39.522 File Modified: C:\¥WINDOWS¥system32¥config¥software.LOG
15:58:39.569 File Modified: C:\¥WINDOWS¥system32¥config¥software.LOG
15:58:39.632 File Modified: C:\¥WINDOWS¥system32¥config¥software.LOG
15:58:39.710 File Modified: C:\¥WINDOWS¥system32¥config¥software.LOG
15:58:54.230611 IP 192.168.0.128.1053 > 192.168.0.2.139: P 980:1164(184) ack 667 win 16854 (DF)
15:58:54.234243 IP 192.168.0.2.139 > 192.168.0.128.1053: P 667:1014(347) ack 1164 win 16357 (DF)
15:58:54.239509 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1164:1402(238) ack 1014 win 16507 (DF)
15:58:54.244854 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1014:1135(121) ack 1402 win 16119 (DF)
15:58:54.249979 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1402:1502(100) ack 1135 win 16386 (DF)
15:58:54.251809 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1135:1195(60) ack 1502 win 17520 (DF)
15:58:54.280840 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1502:1620(118) ack 1195 win 16326 (DF)
15:58:54.307465 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1195:1279(84) ack 1620 win 17402 (DF)
15:58:54.346685 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1620:1749(129) ack 1279 win 16242 (DF)
15:58:54.350178 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1279:1428(149) ack 1749 win 17273 (DF)
15:58:54.370245 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1749:1849(100) ack 1428 win 16093 (DF)
15:58:54.371327 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1428:1488(60) ack 1849 win 17173 (DF)
15:58:54.380807 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1849:1953(104) ack 1488 win 17520 (DF)
15:58:54.399325 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1488:1627(139) ack 1953 win 17069 (DF)
15:58:54.422737 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1953:2093(140) ack 1627 win 17381 (DF)
15:58:54.425257 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1627:1678(51) ack 2093 win 16929 (DF)
15:58:54.434755 IP 192.168.0.128.1053 > 192.168.0.2.139: P 2093:2156(63) ack 1678 win 17330 (DF)
15:58:54.436707 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1678:1810(132) ack 2156 win 16866 (DF)
15:58:54.455227 IP 192.168.0.128.1053 > 192.168.0.2.139: P 2156:2348(192) ack 1810 win 17198 (DF)
15:58:54.459633 IP 192.168.0.2.139 > 192.168.0.128.1053: P 1810:2218(408) ack 2348 win 16674 (DF)
15:58:54.465952 IP 192.168.0.128.1053 > 192.168.0.2.139: P 2348:2393(45) ack 2218 win 16790 (DF)
15:58:54.468490 IP 192.168.0.2.139 > 192.168.0.128.1053: P 2218:2257(39) ack 2393 win 16629 (DF)
15:58:54.485477 IP 192.168.0.128.1053 > 192.168.0.2.139: P 2393:2577(184) ack 2257 win 16751 (DF)
15:58:54.486848 IP 192.168.0.2.139 > 192.168.0.128.1053: P 2257:2604(347) ack 2577 win 16445 (DF)
15:58:54.489621 IP 192.168.0.128.1053 > 192.168.0.2.139: P 2577:2815(238) ack 2604 win 16404 (DF)
15:58:54.492278 IP 192.168.0.2.139 > 192.168.0.128.1053: P 2604:2725(121) ack 2815 win 16207 (DF)
15:58:54.494412 IP 192.168.0.128.1053 > 192.168.0.2.139: P 2815:2915(100) ack 2725 win 16283 (DF)
15:58:54.494807 IP 192.168.0.2.139 > 192.168.0.128.1053: P 2725:2785(60) ack 2915 win 16107 (DF)
15:58:54.507046 IP 192.168.0.128.1053 > 192.168.0.2.139: P 2915:3027(112) ack 2785 win 16223 (DF)
15:58:54.508067 IP 192.168.0.2.139 > 192.168.0.128.1053: P 2785:2851(66) ack 3027 win 17520 (DF)
15:58:54.519748 IP 192.168.0.128.1053 > 192.168.0.2.139: P 3027:3117(90) ack 2851 win 16157 (DF)
15:58:54.530959 IP 192.168.0.2.139 > 192.168.0.128.1053: P 2851:3587(736) ack 3117 win 17430 (DF)
15:58:54.537977 IP 192.168.0.128.1053 > 192.168.0.2.139: P 3117:3215(98) ack 3587 win 17520 (DF)
15:58:54.540926 IP 192.168.0.2.139 > 192.168.0.128.1053: P 3587:3691(104) ack 3215 win 17332 (DF)
15:58:54.544419 IP 192.168.0.128.1053 > 192.168.0.2.139: P 3215:3323(108) ack 3691 win 17416 (DF)
15:58:54.548400 IP 192.168.0.2.139 > 192.168.0.128.1053: P 3691:4539(848) ack 3323 win 17224 (DF)
15:58:54.551326 IP 192.168.0.128.1053 > 192.168.0.2.139: P 3323:3447(124) ack 4539 win 16568 (DF)

```

```

15:58:54.552191 IP 192.168.0.2.139 > 192.168.0.128.1053: P 4539:4643(104) ack 3447 win 17100 (DF)
15:58:54.555377 IP 192.168.0.128.1053 > 192.168.0.2.139: P 3447:3581(134) ack 4643 win 16464 (DF)
15:58:54.557051 IP 192.168.0.2.139 > 192.168.0.128.1053: P 4643:5375(732) ack 3581 win 16966 (DF)
15:58:54.574120 IP 192.168.0.128.1053 > 192.168.0.2.139: P 3581:3739(158) ack 5375 win 17520 (DF)
15:58:54.661907 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 3739 win 16808 (DF)
15:58:54.747382 IP 192.168.0.2.139 > 192.168.0.128.1053: P 5375:5514(139) ack 3739 win 16808 (DF)
15:58:54.759019 IP 192.168.0.128.1053 > 192.168.0.2.139: P 3739:3827(88) ack 5514 win 17381 (DF)
15:58:54.788 File Added: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\desktop.eml ←
15:58:54.879223 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 3827 win 16720 (DF)
15:58:54.961704 IP 192.168.0.2.139 > 192.168.0.128.1053: P 5514:5578(64) ack 3827 win 16720 (DF)
15:58:54.970135 IP 192.168.0.128.1053 > 192.168.0.2.139: . 3827:5287(1460) ack 5578 win 17317 (DF)
:
:
:
15:58:55.101322 IP 192.168.0.2.139 > 192.168.0.128.1053: P 6088:6127(39) ack 195921 win 17032 (DF)
15:58:55.308925 IP 192.168.0.128.1053 > 192.168.0.2.139: . ack 6127 win 16768 (DF)
15:58:55.913 File Modified: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\desktop.eml
15:58:56.314968 IP 192.168.0.128.1053 > 192.168.0.2.139: P 195921:196047(126) ack 6127 win 16768 (DF)
15:58:56.365463 IP 192.168.0.2.139 > 192.168.0.128.1053: P 6127:6266(139) ack 196047 win 16906 (DF)
15:58:56.381209 IP 192.168.0.128.1053 > 192.168.0.2.139: P 196047:196135(88) ack 6266 win 16629 (DF)
15:58:56.471253 IP 192.168.0.2.139 > 192.168.0.128.1053: P 6266:6330(64) ack 196135 win 16818 (DF)
15:58:56.482700 IP 192.168.0.128.1053 > 192.168.0.2.139: . 196135:197595(1460) ack 6330 win 16565 (DF)
15:58:56.482959 IP 192.168.0.128.1053 > 192.168.0.2.139: . 197595:199055(1460) ack 6330 win 16565 (DF)
15:58:56.483121 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 199055 win 17520 (DF)
15:58:56.483934 IP 192.168.0.128.1053 > 192.168.0.2.139: . 199055:200515(1460) ack 6330 win 16565 (DF)
15:58:56.483976 IP 192.168.0.128.1053 > 192.168.0.2.139: . 200515:201975(1460) ack 6330 win 16565 (DF)
15:58:56.484119 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 201975 win 16100 (DF)
15:58:56.484542 IP 192.168.0.128.1053 > 192.168.0.2.139: . 201975:203435(1460) ack 6330 win 16565 (DF)
15:58:56.484578 IP 192.168.0.128.1053 > 192.168.0.2.139: . 203435:204895(1460) ack 6330 win 16565 (DF)
15:58:56.484614 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 204895 win 13180 (DF)
15:58:56.484837 IP 192.168.0.128.1053 > 192.168.0.2.139: . 204895:206355(1460) ack 6330 win 16565 (DF)
15:58:56.484866 IP 192.168.0.128.1053 > 192.168.0.2.139: . 206355:207815(1460) ack 6330 win 16565 (DF)
15:58:56.484897 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 207815 win 10260 (DF)
15:58:56.485106 IP 192.168.0.128.1053 > 192.168.0.2.139: . 207815:209275(1460) ack 6330 win 16565 (DF)
15:58:56.485135 IP 192.168.0.128.1053 > 192.168.0.2.139: . 209275:210735(1460) ack 6330 win 16565 (DF)
15:58:56.485166 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 210735 win 7340 (DF)
15:58:56.485429 IP 192.168.0.128.1053 > 192.168.0.2.139: . 210735:212195(1460) ack 6330 win 16565 (DF)
15:58:56.485540 IP 192.168.0.128.1053 > 192.168.0.2.139: . 212195:213655(1460) ack 6330 win 16565 (DF)
15:58:56.485579 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 213655 win 4420 (DF)
15:58:56.485804 IP 192.168.0.128.1053 > 192.168.0.2.139: . 213655:215115(1460) ack 6330 win 16565 (DF)
15:58:56.485833 IP 192.168.0.128.1053 > 192.168.0.2.139: . 215115:216575(1460) ack 6330 win 16565 (DF)
15:58:56.485867 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 216575 win 1500 (DF)
15:58:56.486070 IP 192.168.0.128.1053 > 192.168.0.2.139: . 216575:218035(1460) ack 6330 win 16565 (DF)
15:58:56.487841 IP 192.168.0.2.139 > 192.168.0.128.1053: . ack 218035 win 17520 (DF)
15:58:56.489890 IP 192.168.0.128.1053 > 192.168.0.2.139: . 218035:219495(1460) ack 6330 win 16565 (DF)
15:58:56.489987 IP 192.168.0.128.1053 > 192.168.0.2.139: . 219495:220955(1460) ack 6330 win 16565 (DF)
15:58:56.490008 IP 192.168.0.128.1053 > 192.168.0.2.139: . 220955:222415(1460) ack 6330 win 16565 (DF)
:
:
:
15:58:57.589552 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1490433:1490478(45) ack 13671 win 16768 (DF)
15:58:57.589908 IP 192.168.0.2.139 > 192.168.0.128.1053: P 13671:13710(39) ack 1490478 win 17355 (DF)
15:58:57.591795 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1490478:1490586(108) ack 13710 win 16729 (DF)
15:58:57.601694 IP 192.168.0.2.139 > 192.168.0.128.1053: P 13710:13849(139) ack 1490586 win 17247 (DF)
15:58:57.603794 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1490586:1490706(120) ack 13849 win 16590 (DF)
15:58:57.605642 IP 192.168.0.2.139 > 192.168.0.128.1053: P 13849:13913(64) ack 1490706 win 17127 (DF)
15:58:57.607327 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1490706:1490751(45) ack 13913 win 16526 (DF)
15:58:57.607677 IP 192.168.0.2.139 > 192.168.0.128.1053: P 13913:13952(39) ack 1490751 win 17082 (DF)
15:58:57.615253 IP 192.168.0.128.1053 > 192.168.0.2.139: P 1490751:1490790(39) ack 13952 win 16487 (DF)
15:58:57.616460 IP 192.168.0.2.139 > 192.168.0.128.1053: P 13952:13991(39) ack 1490790 win 17043 (DF)
15:58:57.854059 IP 192.168.0.128.1053 > 192.168.0.2.139: . ack 13991 win 16448 (DF)
15:59:00.491 File Added: C:\Documents and Settings\All Users\Documents\My Music\サンプル.eml ←
15:59:01.132 File Modified: C:\Documents and Settings\All Users\Documents\My Music\サンプル.eml
15:59:01.194 File Modified: C:\Documents and Settings\All Users\Documents\My Music\サンプル.eml
15:59:02.163 File Modified: C:\Documents and Settings\All Users\Documents\My Music\サンプル.eml
15:59:02.225 File Added: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\desktop.eml ←
15:59:02.272 File Modified: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\desktop.eml
15:59:02.366 File Modified: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\desktop.eml
15:59:02.866 File Modified: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\desktop.eml
15:59:02.882 File Added: C:\Documents and Settings\All Users\Documents\My Pictures\desktop.eml ←

```

```

15:59:02.944 File Modified: C:\Documents and Settings\All Users\Documents\My Pictures\desktop.eml
15:59:10.038 File Modified: C:\Documents and Settings\All Users\Documents\My Pictures\desktop.eml
15:59:10.100 File Modified: C:\Documents and Settings\All Users\Documents\My Pictures\desktop.eml
15:59:10.210 File Added: C:\Documents and Settings\All Users\Documents\共有w o r k\test\riched20.dll ←
15:59:13.319 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\test\riched20.dll
15:59:13.647 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\test\riched20.dll
15:59:13.772 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\test\riched20.dll
15:59:16.397 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\test
15:59:16.866 File Added: C:\Documents and Settings\All Users\Documents\共有w o r k\test\サンプル.eml ←
15:59:17.007 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\test\サンプル.eml
15:59:17.913 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\test\サンプル.eml
15:59:20.178 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\test\サンプル.eml
15:59:20.225 File Added: C:\Documents and Settings\All Users\Documents\共有w o r k\win2000.eml ←
15:59:20.272 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\win2000.eml
15:59:22.194 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\win2000.eml
15:59:22.914264 IP 192.168.0.2.137 > 192.168.0.255.137: udp 50
15:59:23.669997 IP 192.168.0.2.137 > 192.168.0.255.137: udp 50
15:59:23.647 File Modified: C:\Documents and Settings\All Users\Documents\共有w o r k\win2000.eml
15:59:23.725 File Added: C:\Documents and Settings\All Users\Documents\サンプル.nws ←
15:59:23.772 File Modified: C:\Documents and Settings\All Users\Documents\サンプル.nws
15:59:24.412181 IP 192.168.0.2.137 > 192.168.0.255.137: udp 50
15:59:24.866 File Modified: C:\Documents and Settings\All Users\Documents\サンプル.nws
15:59:25.132 File Modified: C:\Documents and Settings\All Users\Documents\サンプル.nws
15:59:25.330202 IP 192.168.0.2.137 > 192.168.0.255.137: udp 50

```

図 4-11 W32/Nimda.s@MM ウイルス検出例

4.3.17 W32/SirCam@MM

(1) ウイルスの概要

W32/SirCam@MM の概要を表 4-34に示す。^{37, 38}

表 4-34 W32/SirCam@MM の概要

種別	ウイルス
特徴	メールに添付して拡散する。
プラットフォーム	Windows95、Windows98、WindowsMe
動作概要	マイドキュメントディレクトリの中の任意のファイルとウイルス自身を Windows アドレス帳の全てのユーザーに送信する。 ネットワーク共有のパソコンやハードディスクへ感染を試みる。

WindowsXP、Windows2000 ではウイルスのバグにより動作しないようである。

(2) 実験環境の設定

ウイルス検出プログラムは本ウイルスの動作プラットフォーム(Windows95、Windows98、WindowsMe)に対応していないが、念のため WindowsXP 環境での実験を試行した。

本ウイルスはネットワーク共有の機能を悪用する。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-35に示す。

表 4-35 W32/SirCam@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:\Documents and Settings\All Users\Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ (E ドライブ) として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 139 だけの指定でもネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

(3) 実験結果

攻撃マシン内にて WINDOWS SYSTEM ディレクトリに自分自身をファイル名 : SCam32.exe でコピーするのを確認できたが、感染先マシンへウイルスファイルをコピーする活動はみられなかった。

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.18 W32/Sobig.a@MM

(1) ウイルスの概要

W32/Sobig.a@MM の概要を表 4-36に示す。^{39, 40}

表 4-36 W32/Sobig.a@MM の概要

種別	ワーム
特徴	.txt、.eml、.html、.htm、.dbx、.wab ファイルで発見したメールアドレスに自分自身を添付してメール送信する。
プラットフォーム	Windows95、Windows98、WindowsNT、Windows2000、WindowsXP、WindowsMe
動作概要	.txt、.eml、.html、.htm、.dbx、.wab ファイルで発見したメールアドレスに自分自身を添付してメール送信する。 ネットワーク共有のディレクトリに自分自身をコピーしようと試みる。

(2) 実験環境の設定

本ウイルスはネットワーク共有の機能を悪用する。通常、ネットワーク共有サービスのポート番号は 139 である。

実験環境の設定を表 4-37に示す。

表 4-37 W32/Sobig.a@MM 実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:¥Documents and Settings¥All Users¥Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワー

クドライブ (Eドライブ) として設定している。

ポート番号は 0 - 1023 を監視対象としているが、ポート番号 139 だけの指定でもネットワーク共有を悪用した侵入の検出には十分であろうと思われる。

(3) 実験結果

本ウイルスを攻撃マシンにて実行すると、まず自分自身を Windows のインストールディレクトリにファイル名 : winmgm32.exe としてコピーするはずだが、入手した検体では攻撃マシンにて当該ファイルが生成されなかった。

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

4.3.19 W32/Sobig.f@MM

(1) ウイルスの概要

W32/Sobig.f@MM の概要を表 4-38に示す。^{41, 42}

表 4-38 W32/Sobig.f@MM の概要

種別	ワーム
特徴	.txt、.eml、.html、.htm、.dbx、.wab、.hlp、.mht ファイルで発見したメールアドレスに自分自身を添付してメール送信する。
プラットフォーム	Windows95、Windows98、WindowsNT、Windows2000、WindowsXP、WindowsMe
動作概要	.txt、.eml、.html、.htm、.dbx、.wab、.hlp、.mht ファイルで発見したメールアドレスに自分自身を添付してメール送信する。 ネットワーク共有のディレクトリに自分自身をコピーしようと試みる。

ウイルスはネットワーク共有のディレクトリに自らをコピーしようとするが、ウイルスコード内のバグのため失敗する。

ネットワーク共有ドライブへのコピーが失敗することから、本ウイルスの拡散手段はメール添付のみとなる。このタイプのウイルスは本ウイルス検出プログラムでは検出の見込みがないため、今回の実験では上記ウイルス調査に止め、データ採取までは行わなかった。

4.3.20 W32/Rous.a

(1) ウイルスの概要

W32/Rous.a の概要を表 4-38に示す。^{43, 44}

表 4-39 W32/Rous.a の概要

種別	ワーム
特徴	詳細不明
プラットフォーム	Windows
動作概要	詳細不明

Network Associates 社の Web サイトで公開されているウイルス検索では W32/Rous.a という名称に一致するものは見当たらなかった。検体ファイル名 i-worm.rous.a.exe で調査したところ、Win32 実行形式のワームであること以外、特徴や動作に関する情報は得られなかった。検体ファイル名からの逆引きで I-Worm.Rous.a や BAT.Rous.worm という名称もたどることができたが、それでも検体と同じと判断できるような情報は得られなかった。

なお、詳細を解析したわけではないが、ウイルスファイル (Win32 実行形式) の内容をバイナリダンプすると、以下のように、メール添付送信を連想させるスクリプトのようなテキストデータが含まれていた。

```
Set RS=CreateObject("Outlook.Application")
```

```
:  
:
```

```
Mail.Attachments.Add("C:¥RousSarc.EXE")
```

```
Mail.Send
```

メール添付型ウイルスと思われるが、複合型ネットワーク感染の可能性も否定できないため、実験を実施することにした。

(2) 実験環境の設定

実験環境の設定を表 4-40に示す。

表 4-40 W32/Rous.a の実験環境の設定

設定項目	感染先マシン	攻撃マシン
OS	Windows XP Professional	Windows XP Professional
メモリ	128MB	128MB
IP アドレス	192.168.0.2	192.168.0.1

設定項目	感染先マシン	攻撃マシン
監視対象 IP アドレス	192.168.0.2	-
監視対象 ポート番号	0-1023	-
監視対象 ディレクトリ	C:¥ (サブディレクトリ含まず) C:¥WINDOWS (サブディレクトリ含まず) C:¥WINDOWS¥system32 (サブディレクトリ含む) 共有ディレクトリ (サブディレクトリ含む)	-

本実験では、感染先マシンの C:¥Documents and Settings¥All Users¥Documents ディレクトリを共有ディレクトリに設定し、攻撃マシンにおいては左記ディレクトリをネットワークドライブ (E ドライブ) として設定している。

本実験では、ウイルスの動作が不明のため、ポート番号 0 - 1023 (Well Known Ports すべて) を監視対象としている。

(3) 実験結果

本ウイルスを攻撃マシンにて実行すると、直ちにアプリケーションエラー (メモリアクセス違反の例外) が発生し、強制終了となった。その際、攻撃マシン自身のファイル変化も調べたが、活動の形跡は見られなかった。Windows 2000、Windows NT4.0 環境も用意して実験を試みたが、いずれも同様の症状だった。

結果: 実験期間中に侵入の兆候が認められず、ウイルス検出のデータ採取はできなかった。

ウイルスが動作しなかった原因としては、ウイルス内部の動作アルゴリズムや動作環境によるもの、あるいはウイルスコード内のバグが考えられる。今回は、本ウイルスに関する情報が不足しており、環境や活動契機、他コンピュータへの感染頻度も不明で実験データは得られなかった。

5 まとめ

本報告書では、別紙で報告したウイルス対策技術に関する調査結果の検討と、現在のウイルス被害届出状況から、特にワームを対象に、その特徴に注目した適応的かつ効率的なウイルス検出手法を一例として提案した。

提案システムは、入手したセキュリティホール情報をもとに脆弱性に関わるポートを監視し、当該ポートに何らかのデータが送られてきたことを検出する。次に、そのデータ受信を契機として特定のディレクトリ(OSのシステムディレクトリなど)の監視を開始し、当該ディレクトリ下のファイル変化(追加/変更/削除/リネーム)を検出する。そして、そのファイル変化を危険な兆候とみなしてユーザに通知するものである。

本システムはネットワーク上の他のマシンから自マシンに接続して侵入・感染を試みるタイプの未知ウイルスに対して有効と考えられる。OSやサービスに脆弱性が発見されパッチが提供されるまでの期間、未知ウイルスに対して無防備なサービスを継続することは大きなリスクを伴うのが現状である。提案システムはサービスを提供しつつ、未知ウイルス検出が可能なものであり、その意義は大きいと考えられる。

ウイルス検体を用いた実験の結果、今回試作したウイルス検出プログラムでは、11ファミリー中5ファミリー(20検体中8検体)のウイルスが検出できた。また、検出した8検体での検出率はどれも100%だった。検出できなかった12検体のうち10検体は、感染先マシンへの侵入動作が認められなかったためである(ウイルスとしての活動が行われなかった、感染先マシンが感染先として選択されなかった、等)。

今後の課題として下記を挙げる。

(1) 自マシンへのポートアクセスを伴わないウイルスの検出には向かない

現状では、自マシンの特定ポートへのアクセスを監視契機にしているため、メール添付により拡散を行うウイルスは検出できない。しかし、例えばクライアントマシンからメールサーバ側へのPOP3通信(サーバ側ポート番号110)のアクセスを監視するよう改善すればクライアントマシンでもウイルスを検出できる可能性はある。ただし、この場合、アクセス検出後のファイルシステムの変更監視期間をどの程度の長さにするべきか、などの問題も解決しなければならない。これは、添付ファイルを実行するタイミングは、ユーザのアクション(添付ファイルをいつ開くか)に依存するためである。

(2) 監視対象とするディレクトリの設定が検出精度に影響する

指定が狭いとウイルスを検出できず(false negative)、指定が広いとウイルスでないものを

誤検出(false positive)する恐れがある。今回の実験でも監視ディレクトリの設定は試行錯誤の状態だった。また、レジストリの変化についてはレジストリ関連情報を格納するファイル単位ではなく、特定のレジストリキーごとに監視できることが望ましい。

(3) メモリ内でのみ活動するウイルスには対応していない

侵入した時点でファイルを生成せず、マシンのメモリ内でのみ活動し、ネットワーク経由で別のマシンに感染を広げるウイルスもある。SQL Slammer⁴⁵などがこのタイプに属する。このタイプのウイルスは、感染したマシンを再起動するだけで、そのマシン単体では完全復旧が可能である。しかし、ウイルスの動作中は盛んに拡散活動を起こすため、感染マシンやネットワークの負荷を著しく増大させる原因になる。これに対処するには、自マシンへの脆弱性ポートへのアクセス検出後に自マシンから他マシンへの脆弱性ポートへのアクセス頻度を監視するなど、別の検出手段が有効だろう。

なお、今回のウイルス検出プログラムではウイルスを検出することに重点を置き、検出後のウイルス駆除に関する検討および実装は行っていないが、ウイルスの侵入を阻止する、侵入したら検出し、駆除するといった一連の流れがウイルス対策の基本であることを忘れてはならない。

未知ウイルスを検出することが可能な手法について、今回提案した手法の他にも着手すべき点はあるだろうが、今後の検討の指標として本報告書が活用されることを期待している。

参考文献

本文中に脚注として示した文献(Web 情報)を以下に示す。なお、URL は 2003 年 11 月現在のものである。

- 1 通商産業省(現経済産業省)告示第 952 号
「コンピュータウイルス対策基準」
<http://www.ipa.go.jp/security/antivirus/kijun952.html>
- 2 情報処理振興事業協会(現:情報処理推進機構)
「W32/MSBlaster」ワームに関する情報
<http://www.ipa.go.jp/security/topics/newvirus/msblaster.html>
- 3 ネットワークアソシエーツ
W32/Lovsan.worm.a
<http://www.nai.com/japan/security/virL.asp?v=W32/Lovsan.worm.a>
- 4 シマンテック
w32.blaster.worm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.worm.html>
- 5 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)
<http://www.microsoft.com/japan/technet/security/bulletin/MS03-026.asp>
- 6 ネットワークアソシエーツ
W32/Lovsan.worm.e
<http://www.nai.com/japan/security/virL.asp?v=W32/Lovsan.worm.e>
- 7 シマンテック
w32.blaster.e.worm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.e.worm.html>
- 8 ネットワークアソシエーツ
W32/Nachi.worm
<http://www.nai.com/japan/security/virN.asp?v=W32/Nachi.worm>
- 9 シマンテック
w32.welchia.worm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.welchia.worm.html>
- 10 マイクロソフト
Windows コンポーネントの未チェックのバッファにより サーバーが侵害される
(815021) (MS03-007)
<http://www.microsoft.com/japan/technet/security/bulletin/MS03-007.asp>
- 11 ネットワークアソシエーツ
W32/Hybris.gen@M
<http://www.nai.com/japan/security/virH2000.asp?v=W32/Hybris.gen@M>

-
- 12 シマンテック
w32.hybris.gen
<http://www.symantec.com/region/jp/sarcj/data/w/w32.hybris.gen.html>
- 13 ネットワークアソシエーツ
W32/Magistr.a@MM
<http://www.nai.com/japan/security/virM2001.asp?v=W32/Magistr.a@MM>
- 14 シマンテック
w32.magistr.24876@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.magistr.24876@mm.html>
- 15 ネットワークアソシエーツ
W32/Magistr.b@MM
<http://www.nai.com/japan/security/virM2001.asp?v=W32/Magistr.b@MM>
- 16 シマンテック
w32.magistr.39921@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.magistr.39921@mm.html>
- 17 ネットワークアソシエーツ
W32/Lovsan.worm.a
<http://www.nai.com/japan/security/virL.asp?v=W32/Lovsan.worm.a>
- 18 シマンテック
W32.Blaster.Worm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.worm.html>
- 19 トレンドマイクロ
WORM_MSBLAST.A
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A
- 20 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)
<http://www.microsoft.com/japan/technet/security/bulletin/MS01-033.asp>
- 21 ネットワークアソシエーツ
W32/CodeRed.f.worm
<http://www.nai.com/japan/security/virC.asp?v=W32/CodeRed.f.worm>
- 22 シマンテック
CodeRed.F
<http://www.symantec.com/region/jp/sarcj/data/c/codered.f.html>
- 23 トレンドマイクロ
CODERED.F
<http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=CODERED.F>
- 24 トレンドマイクロ

-
- WORM_CODEGREEN.A
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_CODEGREEN.A
- 25 ZDNet JAPAN
ネットを舞台にした赤と緑の対決 Code Red
<http://www.zdnet.co.jp/broadband/0109/07/codegreen.html>
- 26 ネット・セキュリティ
Code RedII を駆除するプログラムをリリース(2001.9.13)
<https://www.netsecurity.ne.jp/article/2/2824.html>
- 27 ネットワークアソシエーツ
W32/Klez@MM
<http://www.nai.com/japan/security/virK.asp?v=W32/Klez@MM>
- 28 シマンテック
w32.klez.gen@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.klez.gen@mm.html>
- 29 ネットワークアソシエーツ
W32/Klez.h@MM
<http://www.nai.com/japan/security/virK2002.asp?v=W32/Klez.h@MM>
- 30 シマンテック
w32.klez.h@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.klez.h@mm.html>
- 31 ネットワークアソシエーツ
W32/Klez.e@MM
<http://www.nai.com/japan/security/virK2002.asp?v=W32/Klez.e@MM>
- 32 シマンテック
w32.klez.e@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.klez.e@mm.html>
- 33 ネットワークアソシエーツ
W32/Nimda.a@MM
<http://www.nai.com/japan/security/virN2001.asp?v=W32/Nimda.a@MM>
- 34 シマンテック
w32.nimda.a@mm.html
<http://www.symantec.com/region/jp/sarcj/data/w/w32.nimda.a@mm.html>
- 35 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)
<http://www.microsoft.com/japan/technet/security/bulletin/ms00-078.asp>
- 36 シマンテック
W32.Nimda.E@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.nimda.e%40mm.html>

-
- 37 ネットワークアソシエーツ
W32/SirCam@MM
<http://www.nai.com/japan/security/virS2001.asp?v=W32/SirCam@MM>
- 38 シマンテック
w32.sircam.worm@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sircam.worm@mm.html>
- 39 ネットワークアソシエーツ
W32/Sobig@MM
<http://www.nai.com/japan/security/virS.asp?v=W32/Sobig@MM>
- 40 シマンテック
w32.sobig.a@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sobig.a@mm.html>
- 41 ネットワークアソシエーツ
W32/Sobig.f@MM
<http://www.nai.com/japan/security/virS.asp?v=W32/Sobig.f@MM>
- 42 シマンテック
w32.sobig.f@mm
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sobig.f@mm.html>
- 43 PestPatrol
i-worm_rous_a
http://www.pestpatrol.com/PestInfo/i/i-worm_rous_a.asp
- 44 シマンテック
BAT.Rous.worm
<http://www.symantec.com/region/jp/sarcj/data/b/bat.rous.worm.html>
- 45 情報処理振興事業協会（現：情報処理推進機構）
「W32/SQLSlammer ワーム」に関する情報
<http://www.ipa.go.jp/security/ciadr/vul/20030126ms-sql-worm.html>