



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

---

## 調査報告書

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	調査の背景と目的.....	2
2.1	背景.....	2
2.2	目的.....	2
2.3	用語の定義.....	2
3	調査結果.....	5
3.1	ウイルスの分類に関する調査.....	5
3.1.1	行動による分類.....	5
3.1.2	感染のタイミングによる分類.....	6
3.1.3	感染対象による分類.....	6
3.1.4	感染エンジンの機能による分類.....	6
3.1.5	実装言語環境(ファイルタイプ)による分類.....	7
3.1.6	対象プロセッサによる分類.....	8
3.1.7	ネットワーク上で観測可能な挙動による分類.....	9
3.1.8	ウイルスの分類に関するまとめ.....	9
3.2	ウイルス検出手法に関する調査.....	10
3.2.1	検出手法の分析.....	11
3.2.2	コンペア法/チェックサム法/インテグリティチェック法.....	16
3.2.3	パターンマッチング法.....	20
3.2.4	ヒューリスティック法.....	23
3.2.5	ビヘイビア法.....	27
3.2.6	ウイルス検出手法に関するまとめ.....	34
3.3	侵入検知手法によるウイルス検出に関する調査.....	35
3.3.1	侵入検知手法の分類.....	35
3.3.2	ホスト型 IDS.....	37
3.3.3	ネットワーク型 IDS.....	37
3.3.4	最近の商用 IDS の特徴.....	38
3.3.5	最近の研究.....	39
3.3.6	侵入検知手法に関するまとめ.....	39
4	まとめ.....	41
付録 A	ウイルスの分類に関する文献.....	42
付録 B	ウイルス検出手法に関する文献(特許情報).....	49
付録 C	ウイルス検出手法に関する文献(論文 Web).....	69
付録 D	侵入検出手法に関する文献.....	90

# 1 はじめに

本報告書は、未知ウイルスを検出することが可能な新しい手法を検討・模擬実装するために、既存のコンピュータウイルスの検出技術を調査・分析し、その結果を報告するものである。

調査は、下記の3項目について、現在入手可能な公開されている文献をもとに行っている。

- ・ウイルスの分類
- ・ウイルス検出手法
- ・侵入検知手法によるウイルス検出

なお、この調査を元にした新しい検出手法の検討および模擬実装に関しては別途報告する。

## 2 調査の背景と目的

### 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。

全体像としては、初めに、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、従来のウイルス検出技術に関する調査結果とその分析について記載しており、それを元にした新しい技術の検討とそのプロトタイプの提案、評価実験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」<sup>1</sup>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

---

<sup>1</sup> <http://www.ipa.go.jp/security/antivirus/kijun952.html>

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 調査結果

### 3.1 ウイルスの分類に関する調査

本調査における前提としてウイルスの分類について調査を行い、検出・対策の対象となる機能・性質等を明確化する。調査は、公開され入手可能な文献(書籍および Web ページ)について行った(付録 A 参照)。

ウイルスの分類方法は文献によって様々であるが、主な分類基準として、感染対象別、オペレーティングシステム別、活動機能別、利用技術別などがあった。

この結果に独自の視点を加え、ウイルスを以下の基準で分類し、それらの概要について順に説明する。

- (1) 行動: 感染行動型、拡散行動型、単体行動型
- (2) 感染のタイミング: 直接感染型、メモリ常駐型
- (3) 感染対象: システム領域感染型、ファイル感染型、複合感染型
- (4) 感染エンジンの機能: 追加感染型、上書き感染型、挿入感染型、圧縮型、ステルス型、暗号化型、多形態型、自己改変型
- (5) 実装言語: 機械語型、中間言語型、スクリプト型、マクロ型
- (6) 対象プロセッサ: Intel 86 系 16 ビット型、32 ビット型、Motorola 68 系型、ARM 系型、MIPS 系型、SH 系型
- (7) ネットワーク上で観測可能な挙動: ファイル共有型、パケット送信型、メール送信型

#### 3.1.1 行動による分類

ウイルスは感染型と拡散型に大別できる。これは、狭義のウイルスか、広義のウイルスか、という分類でもある。文献[A21][A35][A43]他。

##### 感染行動型(ウイルス)

宿主を必要とし、感染活動を行って増殖するウイルス。感染対象によってさらに分類できる。

##### 拡散行動型(ワーム)

宿主が不要のワームであり、電子メール、ファイル共有、その他ソケット通信等によって拡散する。

##### 単体行動型(トロイの木馬)

自身では感染も拡散もしないトロイの木馬、論理爆弾、時限爆弾等であり、単体で不正な処理を行う。これらのウイルスファイルはユーザの行動、すなわち電子メールに添付して送信したりフロッピーディスク等に入れて渡すなど、人的行為により拡散する。

### 3.1.2 感染のタイミングによる分類

ウイルスは、感染がいつ行われるかで直接感染型ウイルスとメモリ常駐型ウイルスに大別できる。文献[A18][A34][A37]他。

#### 直接感染型

ウイルスプログラムを起動した時に感染活動を実行し、メモリに常駐しないもの。ダイレクトアクション型、非メモリ常駐型とも呼ばれる。

#### メモリ常駐型

ウイルスがメモリに常駐し、それ以降にアクセスしたディスクやファイルに感染を広げるもの。MS-DOSではDOSファンクションコールを乗っ取って常駐終了(TSR: Terminate and Stay Resident)を行い、WindowsではWindows APIを乗っ取ったバックグラウンド実行による。

### 3.1.3 感染対象による分類

感染型ウイルスはその感染対象によって下記のように分類できる。文献[A3][A12][A42]他。

#### システム領域感染型

ディスクのブートセクタやパーティション領域に感染し、コンピュータシステムの起動時に活動を開始するもの。ブートセクタ/パーティション領域感染型、あるいは単にブート感染型とも呼ぶ。例えば、感染したフロッピーディスクをセットしたままコンピュータを再起動し、フロッピーディスクのブートセクタを読み込んでしまうと、ウイルスが実行され、そのコンピュータのハードディスクに感染してしまう。

システム領域感染型でかつメモリ常駐型ウイルスの場合、システム起動時からコンピュータのすべての機能がウイルスの制御下に置かれることとなり、大変危険である。

#### ファイル感染型

アプリケーションプログラムのファイルや、オペレーティングシステムを構成するシステムファイル、データファイル(マクロ)など、ファイルを感染対象とするウイルスの総称。どんなファイルを狙うかによって、実行ファイル型やマクロ型などに細分化できる。

#### 複合感染型

上記2つの機能を併せ持つウイルス。主にファイル感染によって増殖・拡散し、システム領域への感染によってシステム起動時から活動を開始する。

### 3.1.4 感染エンジンの機能による分類

感染行動型ウイルスの感染エンジン(感染処理の中核部分)は、単に自分自身を対象にコピーするだけのものから、検出を避けるための工夫を凝らしたものまで様々であるが、その感染の方法や補助的な機能によってウイルスを下記のように分類できる。文献[A4][A11][A16]他。

#### 追加感染型/上書き感染型/挿入感染型

これらは感染方法による分類で、追加感染型は感染対象ファイルの末尾にウイルスコード

を追加し、ウイルス部分が実行されるようプログラムのエントリポイント(実行開始アドレスまたは実行開始地点の命令)を書き換えるもので、通常は感染後のプログラムサイズはおよそウイルスサイズだけ大きくなる。

上書き感染型は対象プログラムの先頭からウイルスファイルの内容を上書きするため、十分大きな対象プログラムであれば感染後のファイルサイズを変えないことが可能である。

挿入感染型は単純な追加や上書きではなく、プログラムファイルの中間部にウイルスコードを挿入したり、ファイルに未使用領域が十分あれば、そこにウイルスコードの断片を埋め込むように感染したりする。

#### 圧縮型/ステルス型

これらは主に感染の事実を隠すための技術であり、圧縮型は、感染後のプログラムサイズの変化を起こさないように宿主プログラムを圧縮するものである。これにより、ウイルス自身や圧縮部分の展開ルーチンを付加しても元のサイズを超えないように感染することができる。

ステルス型はより積極的に感染の事実を隠す機能を持つものである。例えば、メモリに常駐してファイルに関する情報を未感染の状態として報告することにより、ファイルサイズを得ようとしても元のファイルサイズが返されたり、ファイルのダンプを取っても元の内容が返され、ユーザの目を欺こうとする。なお、検出を免れるという意味で、次の暗号技術を用いたウイルスもステルス型に含めて扱う場合がある。

#### 暗号化型/多形態型/自己改変型

これらは静的なウイルス解析を困難にする目的でウイルス自身を判読困難化するものであり、暗号化型は単にウイルス自身が暗号化されているものを指す。しかし、暗号化/復号アルゴリズムが一定であることが多く、復号ルーチンをそのままパターンマッチングすることで検出できることがある。

多形態型はミューテーション型やポリモーフィック型とも呼ばれ、パターンマッチングによる検出を免れるため、感染のたびに異なる暗号化/復号ルーチンを生成し、ウイルスコードを暗号化するものである。しかし、感染後のファイルには復号ルーチンが含まれているため、エミュレーションによって容易に復号できる。復号されたウイルスコードは一定であるため、この時点でパターンマッチング方式で検出できる。

自己改変型はメタモーフィック型とも呼ばれ、感染のたびに異なる命令パターンを用いて自分自身を変更する、非常に複雑なウイルスである。この場合、プログラムを仮想実行するなどし、その挙動を監視してウイルスかどうかを判断しなければならないだろう。

### 3.1.5 実装言語環境(ファイルタイプ)による分類

ウイルスといってもプログラムには違いなく、各種プログラミング言語によって記述されており、ほとんどの場合、その言語環境がそのまま感染対象の環境になっている。ウイルスを記述する言語には、プロセッサやオペレーティングシステムに依存する機械語、仮想マシン上で動作する中間言語やスクリプト言語、アプリケーションソフトウェア上で動作するマクロ言語などが使われている。文献[A6][A7][A9]他。

## 機械語型

アセンブラや各種コンパイラで作成された拡張子が COM や EXE などのウイルスを指す。単に実行ファイル型ともいう。中身はプロセッサ依存の機械語で構成されるが、実際にはウイルスもオペレーティングシステムの機能を利用せざるを得ないため、オペレーティングシステム依存のウイルスであるともいえる。MS-DOS 型、Windows 16 ビット型、Windows 32 ビット型、Macintosh 型、Linux 型、PalmOS 型などに細分類される。

## 中間言語型

プログラムが中間言語で構成されていて、実行するために特定の実行環境が必要なものを指す。例えば、Java 型ウイルスは Java バイトコードで構成される拡張子が class のファイルであり、Java 仮想マシン上で動作する。なお、Visual Basic で作成・コンパイルしたのも Visual Basic の実行環境(ランタイムライブラリ)を必要とするが、ファイル形式が EXE であるため、機械語型に分類されることもある。

## スクリプト型

スクリプトとはインタプリタ言語で記述されたプログラムであり、実行環境(インタプリタ)があればソースプログラムファイルをそのままの状態で行うことができる。MS-DOS のシェル上で動作するバッチファイル型、UNIX のシェル上で動作するシェルスクリプト型や、Windows 環境でも WSH(Windows Scripting Host)上で動作する JavaScript 型、JScript 型、VBScript 型などがある。

## マクロ型

アプリケーションソフトウェアの機能を自動実行するためのマクロ機能を悪用して作成されたウイルス。アプリケーションソフトウェアで作成・保存するデータファイル内にマクロを含めることができる場合、データファイルを開いただけで動作し、感染してしまう場合がある。有名なものは Microsoft Office 系のマクロウイルスであるが、アプリケーションソフトウェアがマクロの保護やデジタル署名機能を持つに至り、その活動が抑制されつつある。

### 3.1.6 対象プロセッサによる分類

オペレーティングシステムによる分類と大差ないが、機械語型ウイルスは、対象プロセッサの種類やそのバージョンによって分類することも可能である。例えば、最新のプロセッサの機能を用いたウイルスは旧型のプロセッサでは動作しない可能性がある。Intel 86 系 16 ビット型、32 ビット型、Motorola 68 系型(、未確認ではあるが ARM 系型、MIPS 系型、SH 系型もあり得る)などに分類できる。

なお、WindowsCE を搭載する携帯コンピュータでは PXA250(XScale)、StrongARM、MIPS、SH3 等のプロセッサが採用されており、特定のプロセッサ向けにコンパイルされたウイルスプログラムは別のプロセッサでは動作しない。これはウイルスの広がりを抑制する良い環境だったのだが、Microsoft は PocketPC のプロセッサを ARM 系(StrongARM、XScale)に統一したようで、今後の PocketPC 環境でのウイルスの拡散が懸念される。

### 3.1.7 ネットワーク上で観測可能な挙動による分類

ネットワーク環境が発展・整備されつつある現在、ウイルスもネットワーク環境を悪用するようになってきたが、ネットワーク上でどのような行動を起こすかでその対処も変わってくるため、その観点での分類も必要であろう。文献[A17][A40]他。

#### ファイル共有型

ネットワークコンピュータのファイル共有機能を利用して他のコンピュータへ感染するもの。パスワードなしで書き込み可能な共有フォルダがあると、自分自身を送り込み、LAN内に拡散していく。ファイル共有に利用するポートのデータの流れを監視することで検出可能であろう。

#### パケット送信型

主にオペレーティングシステムのセキュリティホールを狙い、特定のポートへパケットを送りつけて侵入・感染するウイルス。これが大量に動作するとネットワークに輻輳が発生する。このウイルスは、パケットモニタリングによって検出し、パケットフィルタリングによって拡散を防止することが可能であるが、適切なパッチを当てるなどしてセキュリティホールを閉じることが必要である。

#### 大量メール送信型

単純に、ウイルス自身を電子メール(以下単にメールと呼ぶ)に添付して送信するものから、メールソフトのセキュリティホールを狙って特殊なメールメッセージを構成し、自分自身をばらまくものなど、メールを悪用して拡散するウイルス。このウイルスはメールサーバに大きな負担をかけるが、メールサーバで適切に検出・駆除することで集中的に対策できる利点もある。

なお、メールの添付ファイルは不用意に開かないことが大切だが、セキュリティホールを狙ったものの場合、メール本文を開いたり、メール本文をプレビューしたり、あるいはそのメッセージをリストの中から選択しただけでも、添付されたウイルスが活動を開始することがあるので、セキュリティホールを確実に閉じることが重要である。

### 3.1.8 ウイルスの分類に関するまとめ

ウイルスの種類、働き等を知ることは、効果的なウイルス対策技術やそれをういた製品を開発するために必要である。特に、新しい自己改変型ウイルスは、従来の単純なコードパターンの比較では検出不可能であり、検出手法の根本的な改革が必要となる。

なお、本報告書は未知ウイルスの検出技術を広く捉えて考察するために、主に(1)行動による分類、(2)感染のタイミングによる分類、(3)感染対象による分類、(4)感染エンジンの機能による分類、(7)ネットワーク上で観測可能な挙動による分類、に注目している。

## 3.2 ウイルス検出手法に関する調査

現状における代表的なウイルス検出手法および現在研究開発途上にあるウイルス検出手法についての調査を、公開され入手可能な特許情報、論文、技術情報等の文献および Web ページ(付録 B、付録 C参照)に基づいて行った。

特許情報に関しては、平成 2 年以降平成 15 年 10 月 10 日現在までの国内特許公報を対象に、キーワードによって検索した。キーワードは「コンピュータウイルス」「コンピュータウイルス」「コンピュータ・ウイルス」「コンピュータ・ウイルス」「新種ウイルス」である。これにより得られた情報の中には他の関連特許を引用しているものもあったため、その調査も加えた。これらは、検出手法に関わっていない特許と関わりのある特許に大別される。検出手法に関わっていない特許とは、ウイルス検出を目的とせず、ウイルス感染から保護したい対象を守るための方法やシステムの構築を目的とするものである。検出手法に関わりのある特許とは、検出手法が特許の特徴(もしくはその一つ)となっているものやウイルスへの対処方法およびシステムを特許の特徴として提案する中に検出過程を含むもの等である。

論文や Web 情報に関しては、ウイルス検出手法の詳細まで解説しているものが少なかったため、ここではウイルス対策に関する文献を広く収集し、総合的に分析することとした。

以上の調査対象文献の概要は文献リスト(付録 B、付録 C)にも記載したので参照されたい。なお、後の分析のために、本報告書ではウイルス対策技術を以下の 3 つに分類している。

### コア技術

ウイルス検出の核となる技術。これにより、パターンマッチング法、インテグリティチェック法など、検出手法を大まかに分類できる。

### 実装技術

各検出手法の具体的な実装方法。1 つのコア技術に複数の実装技術があり、例えば、ビヘイビア法にどのようなルールを用いるか、などは、ワクチンベンダーごとに異なる手法を用いていることだろう。

### 運用技術

各検出手法の効果的な運用環境の構成。パターンマッチング法のウイルスパターンデータをいかに早く確実に更新するか、など、実装技術をサポートするシステムレベルの技術。

調査した文献の「検出手法の分類」はこのコア技術について述べており、「検出手法の特徴」に(もしあれば)実装技術の概要を述べている。

以下、ウイルス検出のための技術的な情報を含むものに注目し、検出手法を分類し、その分類ごとに特徴的な技術を文献から取り上げて解説する。

### 3.2.1 検出手法の分析

#### (1) 検出手法の分類

表 1はウイルス検出に関して調査した文献をコア技術(検出手法)ごとに分類したものである。なお、検出に無関係の文献は除き、複数の手法を用いている文献は番号に重複がある。

表1: 検出手法による分類

検出手法	文献番号
コンペア法	B26, B32, B67, B75, B82
チェックサム法	B74, B84, B92, B93, C19, C43, C69, C78, C80
インテグリティチェック法	B38, C4, C82, C83
パターンマッチング法	B4, B5, B6, B7, B9, B10, B11, B12, B13, B14, B20, B21, B22, B23, B25, B27, B29, B35, B39, B40, B42, B43, B44, B45, B48, B50, B52, B53, B60, B63, B64, B65, B69, B70, B71, B79, B83, B87, B88, B89, B90, C6, C9, C22, C23, C24, C25, C27, C39, C41, C44, C49, C57, C67, C70, C76
ヒューリスティック法	B2, C3, C7, C10, C11, C12, C21, C37, C42, C46, C52, C55, C56, C58, C60, C79, C81
ビヘイビア法	B3, B34, B49, B61, B62, B72, B75, B76, B85, B86, C5, C8, C10, C12, C14, C20, C26, C28, C29, C31, C32, C33, C35, C36, C38, C42, C45, C46, C47, C48, C50, C53, C54, C59, C63, C66, C68, C71, C74, C81, C84, C85

各検出手法の分類基準(特徴)は以下の通り。なお、各手法の具体的な説明は3.2.2項以降で述べる。

#### コンペア法

ウイルスの感染が疑わしい対象(検査対象)と安全な場所に保管してあるその対象の原本を比較し、異なっていれば感染を検出する場合をこの手法に分類する。

#### パターンマッチング法

文献中の用語でいう「パターンデータ」「ウイルスパターン」「パターンファイル」「ウイルス定義ファイル」等を用いて、何らかの特徴的なコードをパターンとしてウイルス検査対象と比較することで検出する場合をこの手法に分類する。また、特徴的なコードの定義には、ファイル名、メール送受信者の名前やアドレス、送信経路情報、メールメッセージの表題、テキスト文章、バイナリ情報等も含めて考え、それらの登録情報(パターン)と検査対象の情報との比較による検出についても同手法によるものとする。

### チェックサム法/インテグリティチェック法

検査対象に対して別途ウイルスではないことを保証する情報を付加し、保証がないか無効であることで検出する場合をこの手法に分類する。代表的な保証方法には「チェックサム」「デジタル署名」等がある。

### ヒューリスティック法

ウイルスのとりでであろう動作を事前に登録しておき、検査対象コードに含まれる一連の動作と比較して検出する場合をこの手法に分類する。「動作の特徴コード」を検出に用いているかどうか分類の大きな尺度となる。

### ビヘイビア法

ウイルスの実際の感染・発病動作を監視して検出する場合をこの手法に分類する。感染・発病動作として「書込み動作」「複製動作」「破壊動作」等の動作そのものの異常を検知する場合だけでなく、感染・発病動作によって起こる環境の様々な変化を検知することによる場合もこの手法に分類する。例えば、「例外ポート通信・不完パケット・通信量の異常増加・エラー量の異常増加」「送信時データと受信時データの量的変化・質的变化」等がそれにあたる。

ウイルス検出技術の発展は、単純なコンペア法から、その弱点を改善するチェックサム法、インテグリティチェック法への流れと、パターンマッチング法からヒューリスティック法、ビヘイビア法への流れがある。

初期のウイルス対策の技術を含む特許情報(付録 B)ではパターンマッチング法が多く見受けられたが、比較的新しい論文や Web 情報(付録 C)ではより高度なヒューリスティック法やビヘイビア法が多く取り上げられていた。今後も後者の分野が活発に研究されていくことと思われる。

## (2) 検出のタイミング

各文献のウイルス検出手法について、ウイルスを検出できるのはそのウイルスプログラムの実行前か、実行中か、実行後か、という観点で分析を行った。これは、検出技術の安全性や検出後の対応方法に影響する項目である。

### コンペア法/チェックサム法/インテグリティチェック法

検査対象プログラムがウイルスに感染しているかどうかを、そのプログラムを実行しないでチェックできる。しかしながら、あらかじめ原本、チェックサム、デジタル署名などを計算・保存済みの既知のプログラムであればよいが、そうでない未知のプログラムの場合は検査のしようがなく、基本的に安全ではないと判断する。また、検査対象プログラムが未感染の状態から感染状態に変化したことを検出するということは、そのプログラムに感染させたウイルスがどこかで活動している、すなわち既に侵入しているかもしれない、ということの意味する。検査対象プログラムの変化を検出するという点では、これらの手法は「既知の検査対象ファイルがウイルスに感染後、検査対象ファイルの実行前」に検出するということになる(感染元ウイルスファイル A の実行後、それによって感染した検査対象ファイル B の

実行前)。

#### パターンマッチング法

この検査は、検査対象プログラムを実行しないで行う。正しいプログラムの情報を検査するコンペア法等とは逆に、既知ウイルスの情報を検査するパターンマッチング法は、検査対象プログラムが既知のものでも未知のものでも検査可能である。外部から入手したプログラムをしっかりとチェックすることにより、例えば、メールの添付ファイルやネットワークからダウンロードしたファイルなどは実行前のチェックによって既知ウイルスの自システムへの感染を防ぐことが可能となるが、もし、元からシステム内にある既知プログラムからウイルスを検出した場合は、それに感染させたウイルスが既に活動しているということになる。理想的な状態での検出のタイミングは「ウイルス実行前」であるが、新種や亜種などの未知ウイルスには対処できない問題がある。

#### ヒューリスティック法

この検査も、検査対象プログラムを実行せず、ウイルスらしい行動を起こすかどうかをプログラムコードの静的な解析によって判断する。したがって、検出のタイミングは「ウイルス実行前」である。この場合、未知ウイルスであっても、既存のウイルスと同様の動作を行うのであれば検出の可能性があるが、ウイルスが暗号化されていると静的な解析ができなくなるという問題がある。

#### ビヘイビア法

ウイルスの振る舞いを監視するビヘイビア法では、検査対象プログラムを実行する必要がある。ただし、直接実行して危険な行動を検出した時点でその動作を停止させる手法と、仮想環境を利用し、仮想的に動作させて危険な行動を検出する手法がある。したがって、検出のタイミングは「ウイルス実行中」である。これは暗号化されているウイルスでも復号しながら検査できるため、検出力の高い強力な検査法といえる。なお、直接実行する手法はウイルスプログラムを実行してしまう危険性があり、一方、仮想環境を用いる手法はウイルスが仮想環境であることを識別して機能しなくなる(検出できない)可能性があり、どちらも研究課題となっている。

### (3) 対応ウイルス

各文献のウイルス検出手法が対応するウイルスの種類について、検査手法の特徴から可能と思われるものについて分析したが、ほとんどの場合、ウイルス検出手法の得手不得手の通りであった。

#### コンペア法/チェックサム法/インテグリティチェック法

未感染のプログラムの情報を安全に保存していれば、ほとんどの感染行動型ウイルス(狭義のウイルス)に有効。ただし、特別の注意を払わない限りステルス型ウイルスには無効である。

未知のプログラム、すなわち感染しない拡散行動型のワームや単体行動型のトロイの木馬には無効であるが、オンラインソフトなどで提供者のデジタル署名付きのファイルが入手

経路のどこかで改ざんされていないことを確認することは可能である(インテグリティチェック法)。

なお、アプリケーションソフトウェアのデータファイル内のマクロ部分に感染するマクロ型ウイルスの場合は、頻繁に変化するであろうデータファイル全体のコンペア、チェックサム、デジタル署名などは現実的ではなく、マクロ部分のみを抽出してコンペア等を行うような手間が必要である。

#### パターンマッチング法

ほとんどの既知のウイルスに有効。ただし、特別の注意を払わない限りステルス型には無効であり、感染のたびにコードが変化する多形態型や自己改変型にも無効である。

#### ヒューリスティック法

ほとんどのウイルスに有効。ただし、特別の注意を払わない限りステルス型には無効であり、コードの静的な解析が困難な暗号化型や多形態型にも無効である。

#### ビヘイビア法

ほとんどのウイルスに有効。プログラムの挙動だけでなく、ネットワーク的な影響を監視することで、ファイル共有型、パケット送信型、大量メール送信型などのネットワーク型ウイルスにも効果が期待できる。

#### (4) 検出のために必要とする環境

検出を主とする手法において、クライアントマシン、メールサーバ、ゲートウェイなどの既存の機器以外に必要なものがある場合は、その旨文献リストに記載した。例えば、ネットワーク環境でなければ検出できない手法や、他のサーバと連携して働くものなどがある。

なお、ウイルスの挙動を監視するモニタリングシステムや、プログラムを仮想実行するエミュレータなどについては、クライアントマシンやメールサーバなどの内部で動作してウイルス検出を行う場合は、特別な環境は不要とした。

#### (5) 未知ウイルスに対する検出の可能性

未知ウイルスへの対応に関しては、以下の通りほとんど検出手法の特徴そのままである。

#### コンペア法/チェックサム法/インテグリティチェック法

基本的に監視対象プログラムの変化を検出するため、感染行動型のウイルスであれば未知のものであっても検出可能である。しかし、単純なチェックサム法では、ウイルスが感染処理後にチェックサムを再計算して偽装することが可能である。

なお、デジタル署名等の偽造・改ざんが不可能な技術を用いるインテグリティチェック法の場合は、ウイルスの感染によって署名が壊れたり、署名の付いていないプログラムは実行されないが、フリーソフトなどのプログラム開発者が皆デジタル署名等を実施しなければならず、有能なエンジニアがバグのあるプログラムを個人的に修正することもできなくな

る。また、ウイルス作者が不正に入手したデジタル ID<sup>2</sup>で署名したり、自爆テロ的に自らのデジタル ID を用いて署名した場合はすぐには対応できないという問題がある。

#### パターンマッチング法

ウイルス作者は既存のパターンにマッチしないようなプログラムを書けばよく、未知ウイルスを検出することは不可能といえる。

#### ヒューリスティック法

プログラムの挙動をルールベースで静的に解析するため、未知ウイルスも検出の可能性がある。ただし、静的な解析の困難な暗号化型や多形態型ウイルスを除く。

#### ビヘイビア法

モニタリングやエミュレーション等により、プログラムの挙動をルールベースで動的に解析するため、未知ウイルスであっても検出の可能性はある。

以下、表 1 で分類した各手法を、主要な文献を抜粋しながら解説する。

なお、手法の理解を助けるため、下記のデモウイルスを例に挙げる。

#### デモウイルス DemoVir.com の 16 進ダンプ

```
ADDRESS  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F   0123456789ABCDEF
-----
00000000  BA 09 01 B4 09 CD 21 CD 20 44 45 4D 4F 20 56 49   .....!. DEMO VI
00000010  52 55 53 21 24                                         RUS!$
```

この 21 バイトのコードで構成される COM 型プログラムは、実際にはウイルスと呼ぶべきものではなく、実行すると単に「DEMO VIRUS!」の 1 行を表示するだけだが、これは非常に短く無害なプログラムであるため、以後、ウイルス検出手法を説明する際のウイルス例として用いることとする。

---

<sup>2</sup> デジタル ID の発行には十分な身元確認がなされているはずであるが、残念なことに、過去に Microsoft の名を騙って不正にデジタル ID を入手した者がいた。  
<https://www.netsecurity.ne.jp/article/1/1870.html>

### 3.2.2 コンペア法/チェックサム法/インテグリティチェック法

これらの手法は、プログラムの内容(コンペア法)またはそこから算出した情報を記録しておき、後にそれが異なった値になれば改ざんされたと判断する。ウイルスが感染した場合はプログラムの内容が変化するため、たとえそれが未知のウイルスであっても、これらの手法で感染を検出できるのである。

算出手法としては、プログラムを構成する各バイトの総和、重み付けした和、CRC(Cyclic Redundancy Code)、一方向性ハッシュ関数である MD5(Message Digest 5)などが用いられている(チェックサム法)。

算出値は別に保存したり、プログラムファイル末尾に付加される場合もあるが、算出アルゴリズムは通常公開されており、ウイルス作者はこれを利用して、感染処理後に再計算を行うウイルスを作成することができる。

したがって、算出値の検証はできても改ざんはできないように、公開鍵暗号技術で保護する必要がある。すなわち、ファイルに対するデジタル署名であり、ファイルの作者は自分のデジタル ID の秘密鍵を用いて署名を施し、ファイルの利用者はその作者の公開鍵で署名を検証する(インテグリティチェック法)。署名が正しければ、プログラムの作者が特定され、かつ、プログラムの内容が改ざんされていないことが確認できたことになる。

逆に、署名が不正なものであれば、そのプログラムは完全ではない(壊れている)証拠であるので、利用者はそのプログラムを破棄すればよい。プログラムが壊れるのはウイルスの感染だけが理由ではないが、壊れたプログラムを実行することが危険であることには変わりはない。

なお、欠点としては、プログラムの変化のみの確認のため、ウイルス名の特定はできず、駆除も不可能であり、感染しないウイルスにも対応できないことが挙げられる。

#### コンペア法による検出の例

デモウイルス DemoVir.com を例に挙げると、このファイルの正しい内容が

```
"BA0901B409CD21CD2044454D4F2D56495255532124"
```

であったとする。これと現在の内容

```
"BA0901B409CD21CD2044454D4F2056495255532124"
```

を先頭から 1 バイトごとに比較していくと、14 個目のバイトが変化していることがわかり、内容の改変が行われたと判断できる。もちろん、正しい内容が安全に保管されている必要がある。

#### チェックサム法による検出の例

同じくデモウイルス DemoVir.com を例に挙げると、このファイル

```
"BA0901B409CD21CD2044454D4F2056495255532124"
```

の MD5 によるハッシュ値は

```
"A3FE0E0BE827CD9F7C71BE59DE301536"
```

となるが、もしこれが他のウイルスに感染し、内容が 1 ビットでも変更されると、ハッシュ値は大幅に異なる値となり、完全性が失われていることが判断できる。例えば、内容が

"BA0901B409CD21CD2044454D4F2D56495255532124"

に改ざんされると、MD5 のハッシュ値は

"EDE7F31590392433D90D6F5109456487"

となり、改ざんが検出できる。

もちろん、正しいハッシュ値が安全に保管されていてこそ正しい判断ができるので、ハッシュ値を公開鍵暗号などで保護することが望ましい(このインテグリティチェック法の例は割愛する)。ただし、ウイルスの作者が自分のデジタル ID で正しいデジタル署名を付加することもできるため、署名者の身元の検証も必要であることはいうまでもない。

以下、本検出手法に分類できる文献の事例を紹介する。

#### (1) 特開 2001-216173 [B38]

「ウイルス・フリー・ファイル証明書を作成し使用するための方法及びシステム」

インターナショナル・ビジネス・マシーンス・コーポレーション / ジェーン・フランソワーズルペネック

##### 検出方法

ファイルがウイルスに感染していないことを証明する署名付きの証明書を、信頼のおけるアンチ・ウイルス認証局サーバを使って作成することによって、ファイルに認証を与え、ウイルス感染を防止する。すなわち、認証がないか無効であることでウイルス検知が可能となる方法が提案されている。

##### 検出方法の特徴

信頼のおける認証方法及びシステムを構築することによって、認証の有無、認証効力の有無などでウイルスを防止、検出できると考えられている。

##### 検出に関わる一連動作の概略

まず、認証サーバに対して、ファイルの証明書を要求する。その後、認証サーバにファイルが送付され、認証サーバでファイルがチェックされる。ここでウイルスが検出されると、検出されたウイルスに関する情報と応答が要求元に返される。そして、最終的には、修正済みファイルも要求元に送り返される。ウイルスが検出されなければ、ファイルの署名が作成され、その署名の付いた証明書が作成され、要求元に送られる流れである。

##### ウイルスへのその他の対処

認証サーバの作成する証明書には、主体者名・発行者名・公開鍵値・有効期間・通し番号・署名等の要素を持たせ、その信頼性を確かなものにするように考えられている。

#### (2) 特開 2002-342106 [B26]

「既知や未知のコンピュータウイルスの検索・駆除方法」

ベイジンライジングテクノロジーコーポレーションリミテッド / タンハオミョウ

## 検出方法

ウイルス感染を誘発するための仮想のコンピュータ環境を作成し、疑いのある対象を仮想環境内でロードする。ロード前後での環境の変化があれば、その対象はウイルスを含んでいたとする検出方法である。

## 検出方法の特徴

この方法では、ウイルスの感染性を主として利用し、仮想環境内で感染を誘発することにより、感染性のある未知ウイルスを効果的に検索することができると考えられている。

## 検出に関わる一連動作の概略

まず、ウイルス感染を誘発するための仮想のコンピュータ環境を確立し、そこに検査対象(ファイルやマクロ等)を置く。仮想環境内では、感染を誘引するための様々な動作がとられる。例えば、マクロの実行、時間や日付の任意設定等による感染誘引がそれにあたる。そして、仮想環境内を感染された状態にする。その際に、感染前後の仮想環境内を比較し、変化の有無を調査する。変化があれば、検査対象のウイルス含有を判定する流れである。

## ウイルスへのその他の対処

仮想環境内の感染状態をデータとしてサンプル化する。それを元に当該ウイルスの情報を収集し、ウイルス駆除に役立てることも考えられている。

## (3) 特開平 8-16387 [B73]

「プログラム実行装置」

エイ・ティ・アンド・ティ・コーポ / グレググイー・ブロンダー

## 検出方法

個人携帯端末(PDA)固有の装置識別子に結び付けられて暗号化されたプログラムのみが PDA において実行され、暗号化されていないプログラムの実行を防止する方法が提案されている。ウイルスに感染したプログラムは、暗号化されていないプログラムとして検出される。

## 検出方法の特徴

固有の装置識別子に結び付けられた暗号を用いることにより、暗号化されているか否かによってウイルスプログラムを検出できると考えられている。

## 検出に関わる一連動作の概略

まず、PDA で新しいプログラムを入手しようとする時、ベンダーのサーバで PDA 識別子に基づく暗号キーでそのプログラムを暗号化する。その暗号化されたプログラムを PDA が受信し、PDA 内の検索エンジンで暗号は解読されプログラムの入手が完了する。PDA で受信したプログラムが暗号化されていない時、そのプログラムの実行を拒絶する。また、暗号化されていないプログラムは、安全であると識別されたワードを読み出すことができるようになっている。さらに、ワードが安全であると識別されている場合、プログラムの安全を確かめることができる。そして、そのプログラムが書込みアクセスを求めるものであれば、その

アクセスを拒絶する。読み出しアクセスの場合は、アクセスを許可する。このような一連の動作により、ウイルス感染プログラムを検出し、ウイルス感染を防止する流れである。

ウイルスへのその他の対処

PDA のユーザが PDA に取り付けられているボタンを押すことにより、暗号化されていないプログラムのすべての実行を停止することができるように考えられている。

#### (4) IPAINCS [C82]

情報処理振興事業協会（現：情報処理推進機構）

検出手法

デジタル署名技術を用い、新種ウイルスにも強く、偽造などのウイルスの攻撃にも強い感染検知方法。

検出方法の特徴

あらかじめプログラムに対する署名データ(プログラムをハッシュ関数で圧縮し秘密鍵で暗号化したもの)を生成しておく。感染の有無を検査する場合には、署名生成時と同じハッシュ関数でプログラムを圧縮し、添付された署名を復号した値と比較する。プログラムが改ざんされて(感染して)いればこの値は一致せず、検知できる。

### 3.2.3 パターンマッチング法

パターンマッチング法とは、ウイルスの特徴的なコード列(パターン)が検査対象プログラム内に存在するかどうかを調べる方式である。存在すれば、それはウイルス(またはウイルスに感染している)プログラムであると判断する。単にスキャン法とも呼ばれる。

パターンの定義やマッチングの手法などの具体的な部分については、ワクチンベンダーごとに独自の技術を持っていると思われるが、以下では、調査結果と一般的な情報から考察する。

まず、ウイルスの特徴パターンを定義しなければならない。これはウイルスのプログラムを解析し、どの部分に特徴があるかを判断して決定する。例えば、ウイルスとして独特のアルゴリズムを持つものであればそのコードを、あるいはウイルスが表示するメッセージによって判別可能であるならそのメッセージ文字列などをパターンデータベースに格納することになる。

次に、パターンの長さについて考えると、単純計算では、ランダムバイナリデータと偶然一致する確率は  $1 \div (256^{\text{長さ}})$  なので、検査パターンが長いほど誤認は減るが、データベースが大きくなって検査速度が落ちるだろう。また、プログラムコードはランダムデータではなく、プログラムにありがちな定石コードも用いられているだろうから、実際には偶然に一致する確率ももっと大きくなる。検査対象ファイルのサイズが大きい場合はなおのこと、誤検出の問題が大きくなるだろう。したがって、短いパターンを複数ピックアップする場合、単にすべてのパターンを含むだけで検出と判断するのではなく、パターンの順序やパターン間の距離などの位置関係も考慮しなければならない。また、短いパターンの組み合わせで判断するとなれば、これはもう実質はヒューリスティック法に相当するといえる。文献[C7]によれば、現在のワクチンは、パターンマッチング法にヒューリスティックな手法を併用し、パターンデータベースの爆発的な増大を防いでいるという。

処理効率に関連して、検査対象のどこに注目するかも検討しなければならない。例えば、ファイル全体を見るのか、エントリポイント(実行開始地点)から限られた範囲のみか、コードセグメントのみか、データセグメントも含めるのか、などである。

検査のタイミングとしては、ワクチンをオンデマンドに起動してスキャンする場合と、ワクチンがメモリに常駐し、それ以降に実行されるプログラムをその都度スキャンする場合がある。

なお、パターンの質が良ければウイルスが特定できる可能性も高く、また、構造的に駆除可能なウイルスであれば、ワクチンはスキャンと同時に駆除処理を行うことも可能であるが、検出はパターンに依存するため、未知のウイルスは検出できず、多形態型や自己改変型にも対応できないという欠点もある。

#### パターンマッチング法による検出の例

デモウイルス DemoVir.com を例に挙げると、特徴的なコードはメッセージを表示する MS-DOS ファンクションコールの呼び出し部とメッセージ本体であり、これを検出するためのパターンを 16 進数で表すと、例えば

"CD21"

"44454D4F2056495255532124"

の2つになるだろう。あるいは、このプログラムは通常の利用では変化しないため、21バイトのコード全体

"BA0901B409CD21CD2044454D4F2056495255532124"

をパターンとして利用してもよい。しかしそれだけでは、偶然このコードを含むファイルがすべて警告されてしまうので、対象をCOM型プログラムのみ限定したり、スキャン開始位置を指定することも必要になるだろう。例えば、

拡張子が".COM"であり、

アドレス"0005"に"CD21"、かつ

アドレス"0009"に"44454D4F2056495255532124"

あるいは

アドレス"0000"に"BA0901B409CD21CD2044454D4F2056495255532124"

があればウイルス検出とする、などである。

以下、本検出手法に分類できる文献の事例を紹介する。

#### (1) 特開平 6-337781 [B90]

「情報処理装置」

日本電気ホームエレクトロニクス株式会社 / 内田浩一

検出方法

ウイルスのパターンデータと入力データを比較して検出する方法が提案されている。

検出方法の特徴

パターンとして、ウイルスがシリアル転送された場合とパラレル転送された場合、圧縮をかけた場合が記憶されている。

検出に関わる一連動作の概略

まず、データはバッファ手段によってバッファされる。そして、その入力データとウイルスパターンデータを比較する。そこに一致を見ることによってウイルスを検出するという流れである。

ウイルスへのその他の対処

ウイルスが検出された時、CPUに対して警告信号を送り、ウイルスが検出された入力データの送出手を停止することができるように考えられている。

#### (2) 特開平 11-119991 [B53]

「フック方式を用いたコンピュータウイルス自動検出システム」

日本電気株式会社 / 梅田久一

## 検出方法

ネットワークから受信したデータを代理関数に送る。そのデータとウイルスのデータ列との比較を代理関数で行い、ウイルスを検出する方法が提案されている。

## 検出方法の特徴

フック手段を用いて代理関数に処理を渡すことにより、ユーザが特別な操作をすることなく、かつファイル転送プログラムを改造する必要もなくウイルスを検出することができると考えられている。

## 検出に関わる一連動作の概略

まず、フック手段によって、ファイル転送プログラムからソケットモジュールへの受信命令を横取りして代理関数に処理を渡す。代理関数は受信命令をソケットモジュールに対して送り、ソケットモジュールからの受信データが代理関数に送られる。代理関数は、ソケットモジュールからの受信データとウイルスのデータ列とを比較してウイルスの有無を判定するという流れである。

## ウイルスへのその他の対処

ウイルスが検出された場合には、ユーザに検出を通知し、受信処理を続行するかどうかを確認する。受信処理の続行を指示した場合は、データをファイル転送プログラムに送り、中止を指示した場合は、受信データを破棄し、ファイル転送プログラムに受信エラーを返す処理がなされるように考えられている。

### (3) Behavior Blocking: The Next Step in Anti-Virus Protection / 指紋採取 [C39] SecurityFocus / シマンテック Carey Nachenberg

## 検出手法

すべてのスキャンされたファイル、ディスクおよびネットワーク送信中の何万ものデジタル指紋を探索することにより、悪意のあるコードを検知する。各指紋は、特定のウイルス検体から抽出された短いバイト列である。与えられた指紋が見つかった場合、その内容が感染していることが報告される。

### (4) ウイルス検出技術についての解説 / スキャン方式 [C67] TrendMicro

## 検出方法

ウイルスの特徴をデータベース(パターンファイル)に登録しておき、検索ファイルをパターンファイルの情報とマッチングさせることでウイルスを発見する。

### 3.2.4 ヒューリスティック法

ヒューリスティック法とは、エンジニアがプログラムの挙動に疑問を抱き、そのプログラムを解析して、それがウイルスであると判断する、という場合の判断基準や一連の手続きを明確化し、自動化したものである。

あるプログラムがウイルスかどうかは、そのプログラムが行う動作と「ウイルスの定義」を照合して判断することになるが、具体的には、既存のウイルスの動作を統計的に分析した結果得られるルールをもとに、それにどれだけ該当するかで判断することが一般的である。エンジニアの場合は、プログラムを逆アセンブルしたり、デバッガなどでトレース実行してその動作を確認するが、ここでは、ワクチンが行う静的な解析について説明する。後述の動的ヒューリスティック法(ビヘイビア法)に対して、静的なものは特にスタティックヒューリスティック法とも呼ぶ。

まず、検査対象プログラムのコードを、命令コードとオペランドや、命令コード群などに分類していき、それらが呼び出しているシステムコール(MS-DOS ファンクションコールや Windows API)の働きをもとに、そのプログラムが行う動作をリストアップしていく。

そうして得られた行動のリストが、既存のウイルスの行動リストとよく似ていれば、それはウイルスである可能性が高いと判断できる。

似ているかどうかの判断にはさまざまな手法が用いられるが、文献[B2]では、各ルールには経験的に数値化された重み(ウイルスらしさの程度)が与えられており、複数のルールの重みの総和がしきい値を超えていればウイルスと見なしている。

しかしながら、プログラム作成者の悪意や、プログラムに込められた悪意を定量的にルール化することは容易ではない。例えば、下記のどれをウイルスとして検出するべきだろうか。

- (a) ディスクをフォーマットするプログラム
- (b) 自分自身を他のファイルへコピーするプログラム
- (c) 他の実行ファイルの内容を書き換えるプログラム
- (d) メールを大量に送信するプログラム
- (e) 利用者の意図しない動作を行うプログラム

もしかしたら、(a)は `format.com`、(b)は `xcopy.exe`、(c)は `bupdate.exe` (バイナリファイルの差分パッチ当てプログラム)、(d)は `outlook.exe`、(e)は単にバグのあるプログラム、かもしれない。

全く同じ動作でも、善意のもの、悪意のもの、意図しないバグ、の3通りがあり得る。となれば、悪意の判断基準は(A)利用者やその周囲への悪影響が、(B)非通知で実行されるよう、(C)明確にプログラミングされていること、といえるだろう。

これらはどれもルールベースで判断せざるを得ないだろうが、正確な判断のためには十分なルールの検討が必要である。

なお、(B)の非通知かどうかは、プログラマ、利用者、ワクチンベンダーが誤検出の可能性のあるプログラムに関する共通の情報を持ち、有名なフォーマットプログラム等をウイルスと判断することを避ける必要があるだろう。

ヒューリスティック法は、特定のパターンに依存せず、プログラムの挙動をルールベース

で静的に解析するため、未知ウイルスを検出できる可能性がある。しかしながら、静的な解析の困難な暗号化型、多形態型、自己改変型ウイルスなどの検出には適さないという問題がある。

#### ヒューリスティック法による検出の例

デモウイルス DemoVir.com は危険な行動は一切行わないが、仮にメッセージの表示やプログラムの終了に MS-DOS ファンクションコールを利用している点をルールとして診断すれば、それらのどちらも行う DemoVir.com は確実に検出できるだろう。もちろん、もっと複雑な処理を行うウイルスも、ルールの定義やその重み付けが適切であれば、高い確率で検出が可能となる。

DemoVir.com の逆アセンブルリストを以下に示す。

```
0100 BA0901      MOV    DX,0109
0103 B409        MOV    AH,09
0105 CD21        INT    21
0107 CD20        INT    20
0109 44454D4F    DB     'DEMO VIRUS!$'
010D 20564952
0111 55532124
```

ここで、先頭の 0100 はアドレスであり、COM 型プログラムのエントリポイントである。1 行目で表示するメッセージ(5 行目以降のデータ)の先頭アドレスを DX レジスタにセットし、2 行目で MS-DOS ファンクションコールのファンクション番号 9 を AH レジスタにセットしている。このファンクションは DX レジスタの内容のアドレスから '\$' 文字の直前までの文字列を画面に表示するものである。3 行目がそのファンクションを呼び出すソフトウェア割り込みであり、4 行目はプログラムを終了するシステムコールである。

仮のルールを

ルール 1: AH レジスタが 09 で INT 21 を行う、ウイルスらしさ 80

ルール 2: INT 20 を行う、ウイルスらしさ 40

ウイルスらしさが 100 以上でウイルスと見なす

とすると、この場合、DemoVir.com はルール 1 とルール 2 にマッチし、ウイルスらしさの合計は 120 で、ウイルスとして検出することになる。

これはあくまでも例であり、具体的なルールは文献[B2][C12]等を参照されたい。

以下、本検出手法に分類できる文献の事例を紹介する。

#### (1) 特開 2003-186687 [B2]

「ウイルス検出方法および装置」

学校法人金沢工業大学 / 服部進実

## 検出方法

文書ファイル内のマクロ情報から再構築したソースコードをトレースして、ウイルスの特徴コードが含まれていないかどうかを検査し、特徴コードの重みに基づいてマクロの危険度を算出してマクロがウイルスであるかどうかを判定する検出方法が提案されている。特徴コードとは、マクロウイルスが特有の動作(自己伝染・発病・潜伏機能)をとるために必要なコードである。

## 検出方法の特徴

この方法は、新種のウイルスまたは変種ウイルスを効果的に検出することを目的としており、固有のコードとのパターンマッチングに依存しないものである。

## 検出に関わる一連動作の概略

ウイルス特有の動作をとるために必要なコードとそのコードがウイルスとして使用された場合の危険性を示す値(重み)等を 1 レコードとしてデータベースに登録する。マクロを 1 行ずつトレースし、登録された特徴コードと一致するものがあるかどうかを検査し、一致した特徴コードとその重みを収集する。収集した特徴コードの組み合わせから、各重みを基にしてウイルスであるかどうかの判断値となる危険度を算出する。危険度が所定の基準値を超えた時、そのマクロをウイルスであると判断する流れである。

## ウイルスへのその他の対処

ウイルスを検出した場合、収集したコードや過去の検出状態を基に重みを増減させてデータベースを更新するように設定されている。

また、このシステムが、マクロ機能を持つアプリケーションに組み込まれる形態で提供された場合、アプリケーションがマクロファイルをオープンして実行する前に、その危険度をユーザに通知して警告を与えることも可能であることも挙げられている。

## (2) HEURISTIC ANTI-VIRUS TECHNOLOGY [C12]

Frans Veldman

## 検出手法

ワクチンソフト TbScan はウイルスとして疑わしい命令コードを認識するため、それらに下記のようなフラグを割り当てている。

- F: ファイルを感染させるための疑わしいファイルアクセス。
- R: プログラムコードが怪しい方法で再配置される。
- A: 疑わしいメモリ割付け。プログラムは探索やメモリ割付けに非標準の方法を使用する。
- N: 間違っている拡張子。拡張子がプログラム構造と矛盾する。
- S: 実行可能ファイル(.COM または .EXE)を探索するルーチンを含んでいる。
- #: 命令復号ルーチンを発見。これは、ウイルスには一般的であるが、保護されたソフトウェアにも一般的である。

- E: 柔軟なエントリポイント。コードは、実行可能なファイル内の任意の位置上でリンクされるように見える。ウイルスにはよくある。
- L: プログラムがソフトウェアのロード時をねらってトラップする。ソフトウェアを感染させるためにプログラムのロードを遮るウイルスかもしれない。
- D: ディスク書き込みアクセス。プログラムが DOS を使用せずにディスクに書き込む。
- M: メモリ常駐コード。このプログラムは、メモリに常駐することを試みる。
- !: 無効な命令コード(非 8088 命令)あるいは範囲外に分岐する命令。
- T: 正しくないタイムスタンプ。いくつかのウイルスは、感染したファイルをマークするためにこれを使用する。
- J: 疑わしいジャンプ命令を構築している。連続的なあるいは不正なジャンプ経由のエントリポイント。これは正常なソフトウェアには見られないが、ウイルスには一般的である。
- ?: 一貫しない EXE ヘッダ。ウイルスかもしれないが、バグでもありうる。
- G: ゴミ命令。暗号化以外に目的を持たないように見えるコードあるいはウイルススキャナによる認識を回避するコードを含んでいる。
- U: 非公開の割り込み/DOS 呼び出し。プログラムはそれ自体を検知する非標準の方法を使用するという巧妙な動作をするため、ウイルスである可能性が高い。
- Z: EXE/COM 判定。プログラムは、ファイルが COM または EXE のファイルかどうかチェックしようとする。ウイルスは、プログラムを感染させるためにこの動作を行う必要がある。
- O: メモリ中のプログラムを上書きまたは移動させるために使用できるコードが見つかった。
- B: エントリポイントに戻る。エントリポイントの修正がなされた後、再度プログラムを開始するためのコードを含んでいる。ウイルスには普通の事である。
- K: 異常なスタック。プログラムは疑わしいスタックを持っている。

これにより、下記のウイルスは次のフラグで検出できる。

ウイルス名:	ヒューリスティックフラグ
Jerusalem/PLO:	FRLMUZ
Backfont:	FRALDMUZK
Minsk_Ghost:	FELDTGUZB
Murphy:	FSLDMTUZO
Ninja:	FEDMTUZOBK
Tolbuhin:	ASEDMUOB
Yankee_Doodle:	FN#ELMUZB

### 3.2.5 ビヘイビア法

ビヘイビア法はヒューリスティックな手法の一種であるが、これは動的な解析をもとに判断するもので、ダイナミックヒューリスティック法とも呼ぶ。すなわち、プログラムを動作させ、その挙動を監視して、ヒューリスティック法と同様のルール(ウイルスによく見られる行動)に該当する行動を基準値以上に起こした場合にウイルスと判断する。動的な解析であるため、複雑な多形態型ウイルスや自己改変型ウイルスにも対応可能である。

プログラムの実行は、これを実マシン環境で行う場合と、仮想マシン環境で行う場合がある。

実マシン環境では、あらかじめシステムコールや Windows API をフックしておき、それらが呼び出された時点で動作の記録をとり、ある程度ルールに該当した時点で検出し阻止する。

仮想マシン環境を利用する場合は、ウイルスにとって実環境と同じ状態を提供する必要がある。研究レベルでは市販の仮想マシンソフトウェアを利用している場合が多いが、単体のワクチンとして構成する場合は、オペレーティングシステムの機能やネットワーク環境などすべてを自前で持っている必要があり、実装が非常に困難である。

また、ネットワーク環境における挙動を監視することで、ネットワークベースのウイルスを検出することも可能である。ただし、例えば、特定のサーバに接続し、その反応を元に活動内容を変えるウイルスの場合、サーバに接続できなければウイルスとしての動作を行わず、検出できないかもしれない。しかし、現実の外部ホストとの通信を許してしまうと、ウイルスが外部に流出する危険性も生まれる、という課題もある。

#### ビヘイビア法による検出の例

デモウイルス DemoVir.com の場合、前述のヒューリスティック法での例示の通り、仮にメッセージの表示やプログラムの終了の MS-DOS ファンクションコールをルールとして診断することで検出可能である。

前述のルールを用いると、DemoVir.com はルール 1 の動作(AH=9 で INT 21)を実行し、続けてルール 2 の動作(INT 20)も実行する。これらの割り込みをワクチンがあらかじめフックしておき、これらが呼び出された時点で挙動を記録・監視することで、これをウイルスとして検出することになる。

以下、本検出手法に分類できる文献の事例を紹介する。

#### (1) 特許第 002621799 号 [B72]

「コンピュータウイルス感染監視・防止方式」

日本電気株式会社 / 愛場豊和

#### 検出方法

ウイルスの中には、感染する際に一時的にオペレーティングシステム内の書き込み禁止命令プログラムの内容を書き換えて、その命令を無効にした後に感染し、感染後は書き換えた内容を元に戻す動作を行うものがある。そのようなウイルスへの対抗手段として、書き込み

禁止命令プログラムの内容が「正当な内容」であるかどうかを監視し、正当な内容ではないと判定した時、プログラムの書き換えが行われたと判断し、ウイルスの感染を認識するという方法が提案されている。ここでいう「正当な内容」とは、「予め固定的に記憶されている書き込み禁止命令プログラムの内容」や「過去に参照し取得した書き込み禁止命令プログラムの内容」を指す。

#### 検出方法の特徴

この方法では、ウイルスの「書き込み禁止命令プログラムの内容への書き換えを行う動作」に注目し、その動作を監視することにより検出することができると考えられている。

#### 検出に関わる一連動作の概略

まず、システム内で書き換えを監視する際に、書き込み禁止命令プログラムを実現する領域を示すアドレスを保持させ、一定時間間隔でアドレスによって特定される領域の内容(その時点での書き込み禁止命令プログラムの内容)を参照する。その参照内容が正当な内容であるかどうかを判定し、正当な内容ではないと判定した時、ウイルスの感染を認識するという流れである。なお、この一定時間間隔については、プログラム実行システムのハードウェアやオペレーティングシステムの能力によって可能な限り最短の時間で行うことが好ましいことが付記されている。

#### ウイルスへのその他の対処

ウイルスの感染を認識した場合、警告メッセージの表示、システム内で行われている処理の強制終了、入力制御等を行うことができるように考えられている。

### (2) 特開 2003-241989 [B3]

「コンピュータウイルス発生検出装置、方法、およびプログラム」

株式会社東芝 / 高橋俊成

#### 検出方法

ウイルス発生の可能性を示す特異データを収集し、それらのデータに基づいてウイルス発生の有無を判定する検出方法が提案されている。ここでいう特異データとは、通常使用されない例外ポートを使用した TCP/IP 通信が行われたことによる不完全なパケットの発生、通信量の異常な増加、エラー量の異常な増加等である。

#### 検出方法の特徴

この方法では、ウイルスを不特定のままに検出することができ、感染被害を未然に防止することができると考えられている。

#### 検出に関わる一連動作の概略

まず、インターネット接続後、エラー量の測定、例外ポート通信の検出、不完パケットの検出、通信量の測定が、並行して、もしくはは任意の順番で逐次行われる。それぞれから特異データが得られた場合に、総合的なウイルス判定処理を行うという流れである。その際の処

理は、所定のしきい値との比較処理や統計学的な処理などを含んでいる。

#### ウイルスへのその他の対処

ウイルス発生を判定した場合、異常発生通知を出し、インターネットとの接続を遮断する。また、パターンファイルやセキュリティホール修正プログラム等をイントラネット内のクライアントマシンに配布する方法も例示されている。

### (3) 特開 2002-314614 [B34]

「電子メールの中継システム及び電子メール中継方法」

東日本電信電話株式会社 / 鈴木晃

#### 検出方法

ユーザ端末が電子メールを受信する前に、受信メールを試験サーバに中継させ、所定の異常動作を引き起こすか否かをチェックし、ウイルスを検出する方法が提案されている。ここでチェックする異常動作には、オペレーティングシステムの書き換え動作やメールの送受信に関係のないファイルの書き換え動作、ファイルの破壊動作、メモリの浪費等が挙げられている。

#### 検出方法の特徴

検出専用のサーバを設定し、受信メールをチェックすることにより、ユーザ端末のウイルス感染を未然に防止できると考えられている。

#### 検出に関わる一連動作の概略

まず、受信メールは試験サーバで受信される。そこで、メールは開封・実行され、所定の異常動作が起こるか否かを監視する。異常動作が発生しなかった場合のみ、ユーザ端末でのメール受信が可能となる。異常動作が発生した場合、そのメールをユーザに中継するか破棄するかを判断し、ウイルスの有無を判定する。

#### ウイルスへのその他の対処

メールを破棄した場合、メールの管理者や送信ユーザ端末に対して警告メールを送信することもできるように考えられている。

### (4) 特表平 10-501354 [B62]

「コンピュータ・ウィルス・トラップ装置」

クワンタム・リープ・イノベーションズ・インコーポレーテッド / シュヌラー、ジョン

#### 検出方法

エミュレーションである外部オペレーティングシステムにデータが挿入され、環境内の変化を監視することによってウイルスを検出する方法が提案されている。環境内の変化とは、割込み要求テーブルが修正されたか否か、別のプログラムが書き込まれたか否か等である。

## 検出方法の特徴

この方法では、エミュレーションを用いて検出するように考えられている。また、そのためのオペレーティングシステムを外部に設定し、データ取り込みの際に中継させることで、ウイルスを隔離した状態で検出できるように考えられている。

## 検出に関わる一連動作の概略

まず、外部から入ってくるすべてのデータがエミュレーションボックスに入力される。ここで、ウイルスのすべての動作を起こさせる。そこでの環境の変化をチェックし、単純にデータが書き込まれたか、または実行可能なコードが書き込まれたかがチェックされる。実行可能な命令が入ると、巡回冗長検査が、エミュレーションボックス内に配置されたすべてのファイルで行われる。そして、実行可能命令の強制実行がなされる。そこで、割込み要求テーブルが修正されたか否か、別のプログラムが書き込まれたか否か等、環境の変化をチェックすることでウイルスを検出する流れである。

## ウイルスへのその他の対処

ウイルスを検出した場合に、システム管理者への通知、ファイル送受信者への通知、ファイルの削除、フロッピードライブへの書き込み、ページャ呼び出し、シャットダウン等の指令を任意に実行することができるように考えられている。

## (5) Behavior Blocking: The Next Step in Anti-Virus Protection [C35] [C36] [C38]

SecurityFocus / シマンテック Carey Nachenberg

## 検出方法

ビヘイビアブロッキングソフトウェアについて述べている。これは、ホストコンピュータのオペレーティングシステムと統合し、プログラムの悪意のある振る舞いをリアルタイムにモニタする。そして、システムに影響する前にそのアクションを阻む。モニタされる振る舞いは次のとおりである。

- ファイルオープン、削除または修正する試み
- ディスクドライブのフォーマットや復旧不可能なディスク操作
- 実行可能ファイル、マクロ、スクリプトのロジックの修正
- スタートアップ設定のような重大なシステム設定の修正
- 実行可能ファイルを送るための電子メールとインスタントメッセージクライアントのスクリプト記述
- ネットワーク通信の開始時

既存のビヘイビアブロッキングシステムは2つのカテゴリに分割できる。それは、ポリシーベースのブロッキングシステムとエキスパートベースのブロッキングシステムである。

ポリシーベースのシステムは、管理者がどの振る舞いを許可するかを指定する。そして、それ以外の振る舞いを閉鎖する。プログラムがオペレーティングシステムに要求するごとにビヘイビアブロッカーはリクエストを遮る。ポリシーデータベースを調べ、リクエストを許可するか、完全に遮断するかを決める。例えば、Javaのためのポリシーベースのビヘイビア

ブロッキングシステムは下記のオプションを提供する。

ビヘイビアブロッキングシステムの持つオプション

オペレーション記述: ブロックリクエスト

アプレットがファイルを開くことを許可する: Yes

アプレットがファイルを削除することを許可する: Yes

アプレットがネットワーク接続を始めることを許可する: Yes

アプレットがシステムディレクトリ中のファイルにアクセスすることを許可する: No

ポリシーベースシステムとは対照的に、エキスパートベースのシステムは、オペレーションのより不明瞭な方法を使用する。これらのシステムでは、人間のエキスパートが、悪意のあるコードの全クラスを分析しており、次に疑わしい振る舞いを認識し阻止するためにビヘイビアブロッキングシステムを設計した。

ポリシーに基づいたシステムは、例えば「システムファイルへのアクセスを閉鎖するオプション」を持つだろうし、エキスパートに基づいたシステムは「ウイルスの振る舞いを阻むオプション」を持つことになるだろう。

## (6) Immune System for Virus Detection and Elimination [C53]

Technical University of Denmark / Rune Schmidt Jensen

### 検出方法

隠れマルコフモデルを用いて、プログラムコードの静的な学習とプログラム実行時のシステムコールの利用をトレースして学習することにより、「正常な振る舞い」を意味する統計的なデータを得る。後に、プログラムをモニタリングし、これと異なる振る舞いを行うものをウイルスとして検知する。

コードベースとシステムコールベースの統計的なビヘイビア法であり、未知のウイルスも検出可能である。しかしながら、未感染のプログラムを用いてある程度の時間をかけて学習させなければならない。

### 検出方法の特徴

隠れマルコフモデル(HMM)フレームワークを Java で実装し、ウイルスに感染しているプログラムと HMM の実験を行っている。HMM は無感染のプログラムから静的コードを学習し、無感染のプログラムの実行によって生成されたシステムコールをトレースする。そのプログラムがウイルスに感染したときに HMM がその感染を検知する能力をテストしている。HMM が静的コードやプログラムの実行によって生成されたシステムコールのトレースからプログラムのウイルス感染を成功裡に発見することができることを示している。

自分以外を定義してそれを検出することは困難だが、自分を定義し、それと異なるものを検出することは可能である。ここでは、ウイルスの振る舞いパターンからウイルスを検知する。これは、自己が有害でない正常な振る舞いを表わし、非自己が有害な異常な振る舞いを

表わすことを意味する。

異常な振る舞いを検出するために HMM を採用している。根本概念は、すべての正常で感染していないプログラムの正常な振る舞いプロフィールを構築し、後で、いずれかのプログラムがこのプロフィールに反するかどうか確かめるためにモニタすることである。

静態分析は、ウイルス感染によりプログラムの異常な振る舞いを発見することを目指している。ここでは、コードとデータのセグメントを扱っている。なお、この方式はブートセクタウイルスや、Word および Excel ドキュメントで見つかったマクロウイルスを検知するために容易に拡張することができたという。

動態分析では、異常な振る舞いを検知するためにシステムコールのトレースをスキャンしている。根本概念はシステムコールの正常な作用するトレースからの偏差を検知することである。

#### (7) 仮想ネットワークを使った未知ウイルス検知システム [C85]

徳島大学 神園 雅紀、白石 善明、森井 昌克

##### 検出手法

仮想マシンとその閉じたネットワークを利用してウイルスの自己増殖活動の検知を行うことを目的に、未知ウイルスにも対応できるシステムについて述べている。特徴は、複数の検査対象の添付ファイルを同時に検査することで、実環境に適した処理時間で検査できることである。検査方法としては、二分探索法の要領で検査対象メールを分割していく。ウイルス活動を検知した場合はさらに分割して検査を続け、検知しなければそのファイルは検査対象外とし、残りの検査対象ファイルを検査する。このような処理を繰り返すことによりウイルスファイルを特定する。

提案されている手法において、未知ウイルスの検知は仮想ネットワーク監視、監視サーバでのウイルスメール取得、そして整合性検査の3つにより実現すると述べている。

仮想ネットワーク監視によるウイルス検知では、仮想マシンソフトウェアである VMware の仮想ネットワーク (VMnet) を監視し、ウイルスの自己増殖において、ウイルス実行ホストからのネットワークアクセスを検知することによりウイルスか否かを判断する。ここでは、仮想ネットワークを監視するために、ホスト OS にパケットフィルタリングツールである iptables を導入している。Iptables を導入することにより、SMTP ポート以外のポートへ攻撃をするウイルスも検知できる。

#### (8) 仮想サーバを使った未知ウイルス検知システムの提案 [C84]

徳島大学 三宅 崇之、白石 善明、森井 昌克

##### 検出手法

ユーザが電子メールを受信する前にメールサーバ内の仮想マシン上でウイルスの可能性のある添付ファイルを受信し、その挙動を監視することで未知ウイルス検知を行うシステムについて述べている。

提案手法で用いられているウイルス検知手法は、パターンマッチング方式、スタティックヒューリスティック方式、そしてダイナミックヒューリスティック方式である。ホストエミュレータを用いて完全な仮想ホストマシンを構築し、メールに添付されているファイルを実行・検査する手段が提供されている。

#### 検知手順

##### 第一段階: メールヘッダ、添付ファイルの検査

メールヘッダ内のパターンマッチングを行って過去のウイルスを判断する。添付ファイルが以前にウイルスとして検知されていないかどうか確認する。検査対象ファイルのハッシュ値を以前取得したウイルスファイルのハッシュ値と比較することによって検査を行うことができる。新たにウイルスを検出した場合、次回の検知に用いる。

##### 第二段階: プログラムコードの検査

添付ファイルを検査対象とし、ウイルスがとる可能性の高い行動パターンを表すプログラムコードの存在の確認を行う。第二段階でも第一段階と同様の学習機能を持つ。

##### 第三段階: 仮想実行後の行動パターンの検査

仮想マシンを用いて添付ファイルを仮想的に実行し、行動パターンの収集を行う。そしてその行動パターンがウイルスのものであるか検査を行う。検査方法は2つあり、ワーム対策として自動的にウイルス付きメールを送信する動作の検出、ファイルの改ざん対策としてファイルのハッシュ値を取得し、以前取得したハッシュ値との比較を行い、改ざん等の検出を行う。また、第三段階も第一、第二と同様の学習機能を持つ。なお、ここで述べている仮想マシンとは市販の仮想マシンソフトウェア VMware を指している。

#### ワームの検知手法

プログラムを実行した際にメールを送信するかどうかという点に着目している。手順を以下に示す。

1. VMware にゲスト OS としてインストールした Windows の標準アドレス帳に宛て先の存在しないダミーのメールアドレスを登録する。また、メールソフトである Outlook Express にはウイルス検知に用いる SMTP サーバへのアドレスを設定する。

2. 仮想マシン上でメールの添付ファイルを実行する。

3. 実行した添付ファイルがワームの場合、アドレス帳を参照しリストに存在するアドレスに対してウイルス付きメールの送信を行う。

4. 3.で送信されたメールはもう一つのゲスト OS である Linux 上の自作 SMTP サーバへと渡される。

5. 自作 SMTP サーバはメールを受信した段階でこのプログラムをウイルスであると判断する。

6. ウイルスと判断された場合、SMTP サーバでは受領したメールを解析し、ウイルスの特徴を抽出する。

7. 抽出した特徴を検知用データとして学習する。

### 3.2.6 ウイルス検出手法に関するまとめ

3.2.1項の表 1の通り、今回の調査で最も多く用いられていた手法はパターンマッチング法だった。この手法では、既知コードさえあれば、それをスキャンすることによって高い確率でウイルスを特定し検出することができる。しかし、一方で新種や亜種のウイルスには無力である。そのため、この手法では、いかにして迅速に最新のパターンデータを作成、入手、配布するかが重要になってくる。この手法に関わる文献が多かったのは、その迅速な対応を目指した方法やシステムの構築が多く提案されていた結果であるともいえる。

次に多く用いられていた手法はビヘイビア法である。ウイルスを確実に検出するための最も本質的な方法はこれであろう。ウイルス作者がプログラムに込めた悪意は、結局はそのプログラムの挙動によって判断せざるを得ない。

特許情報を見ると、特開平 06-149681「コンピュータウイルスからハードとフロッピーディスクを保護する回路」[B85]がビヘイビア法に分類できる最初のものだった。ここでは、保護プログラムが動作されないまま、もしくは微動作状態で、ハード及びフロッピーディスクコントローラが動作することによって検知する手法が提案されている。最近では、特開 2003-241989「コンピュータウイルス発生検出装置、方法、およびプログラム」[B3]で、例外ポート通信や不完パケット、通信量、エラー量等を調べる手法が提案されている。論文でもビヘイビア法の実装技術が論じられており、今後も注目していく必要があるだろう。

年々多様化し巧妙化するコンピュータウイルスであるが、そこには感染、発病、潜伏等の何らかの動作があることには違いない。この手法を時系列でみると、その時々ウイルス動作の特徴を捉え、システム内で起こる変化の調査観点や調査場所を変えながら検出してきていることがわかる。

現在のウイルスは、処理効率や検出率の問題はあるが、ビヘイビア法でほぼ対応できると考えられる。しかし、ウイルスといえどプログラムであり、根本的な排除が困難である以上、今後もコンピュータの高度化や環境の変化によって新しい概念のウイルスが出現する恐れがあり、それに対応する検出技術を常に開発し続けていく必要があるだろう。

### 3.3 侵入検知手法によるウイルス検出に関する調査

ウイルス検出に類似・関連する技術手法として侵入検知手法が挙げられる。

ネットワークシステムにおいて、ファイアウォールだけでは防げない Web ページ改ざん、DoS (Denial of Service: サービス不能) 攻撃、DDoS(Distributed DoS: 分散 DoS) 攻撃や、システムへの不正侵入を最初のステップにした攻撃は増加の一途をたどっている。侵入口を探る偵察行動や実際の侵入の試みは日常茶飯事となり、組織内部からの侵入行為も増加している。

不正侵入手法には、自動スキャン、トロイの木馬攻撃、パスワードクラッキング、セキュリティホール攻撃、DoS 攻撃などがあり、次々に新しい手口が開発されている。不正アクセスが内部犯行であるケースは約 7 割ともいわれており、その対策が重要な課題となっている。

そこで、現状における侵入検知手法について、公開されている特許情報、論文、技術情報等の文献および Web ページ(付録 D)に基づき、ウイルス検出への応用の可能性に関する調査を行った。

#### 3.3.1 侵入検知手法の分類

IDS (Intrusion Detection System) は上述のような不正侵入を検出するためのツールであり、侵入検知システムと呼ばれている。これは、ネットワークまたはホスト上で発生したイベントを監視および分析し、侵入の試み(秘匿性、完全性、アベイラビリティの侵害を試みるイベント)を検知する。

IDS は分析対象により一般にホスト型とネットワーク型の 2 種類に分類される。

##### ホスト型

監視対象に直接インストールして使用される。監視対象は自ホストに流れてきたパケット、システムファイルやログのサイズ、パーミッション、ユーザ操作情報などのアクティビティで正常運用時の情報をプロファイルとして保存し、左記情報と定期的またはリアルタイムに比較・確認する。

##### ネットワーク型

ネットワーク上を流れるパケットを収集し、シグネチャと呼ばれる不正パケットの兆候を示すデータとマッチングすることによりチェックする。

日本ではネットワーク型が主流になっている。上記に加えてファイアウォールの拡張版のように機能することも可能なインライン型と呼ばれるものもある。

表 2 に、インライン型も加えた各タイプの特徴をまとめる。

表2: ホスト型、ネットワーク型、インライン型の特徴

	長所	短所
ホスト型	<ul style="list-style-type: none"> <li>・ 既知の侵入を確実に検知可能</li> </ul>	<ul style="list-style-type: none"> <li>・ 監視対象が複数ある場合、全てにインストールする必要がある</li> <li>・ 定期メンテナンスが大変</li> </ul>
ネットワーク型	<ul style="list-style-type: none"> <li>・ 監視対象ホストに負荷をかけるけない</li> </ul>	<ul style="list-style-type: none"> <li>・ ネットワークトラフィックが増加するとパケットの取りこぼしが発生する可能性がある</li> <li>・ 暗号化されたパケットは解析できない</li> <li>・ 一般的に、直接コンピュータにログインしているユーザの不正行為は検出できない</li> </ul>
インライン型	<ul style="list-style-type: none"> <li>・ パケットの取りこぼしがない</li> <li>・ 監視対象ホストに負荷をかけるけない</li> </ul>	<ul style="list-style-type: none"> <li>・ 本機能が停止するとネットワークが停止する危険がある</li> </ul>

また、分析手法により不正検出型(misuse detection)と異常検出型(anormary detection)に分類される。

#### 不正検出型

攻撃を特定するパターンをデータベースとして持ち、収集したパケットと照合して不正パケットを検出する。ネットワーク型 IDS で多く採用されている検出方法。

#### 異常検出型

普段のネットワークを流れるパケットパターンやトラフィック量、ユーザのログイン時刻、アプリケーションの種類、使用コマンド、RFC で規定されるプロトコルなど、正常時の状態をプロファイルとして記憶しておき、実際のシステム上での振る舞いが左記情報からはずれる場合に異常と判断する。

例えば、ping コマンドを使ってネットワーク機器の状態を確認することは通常の管理行動の一つだが、コマンド送出は大抵 1 秒に 1 回ぐらいである。それが 1 秒間に 100 回送られたとすれば、それは異常行動といえる。

表 3に、不正検出型、異常検出型の特徴をまとめる。

表3: 不正検出型、異常検出型の特徴

	長所	短所
不正検出型	<ul style="list-style-type: none"> <li>・ 既知攻撃を確実に検知する</li> <li>・ 具体的なインシデント名称で表示可能</li> </ul>	<ul style="list-style-type: none"> <li>・ 未知の攻撃が検知できない</li> <li>・ シグネチャデータベースの更新が必要である</li> <li>・ トラフィック量増加への追従が困難</li> </ul>
異常検出型	<ul style="list-style-type: none"> <li>・ 未知の攻撃を検知する可能性がある</li> </ul>	<ul style="list-style-type: none"> <li>・ 導入前に学習期間が必要、また学習期間中の攻撃に対応不可能</li> <li>・ ログがそのまま報告されるので、管理者はログの解析に手間がかかる</li> <li>・ 正規のユーザでも普段と異なる行動をとった場合に検出する可能性がある</li> </ul>

### 3.3.2 ホスト型 IDS

ホスト型 IDS は監視対象にインストールされ、攻撃者の行動またはファイル等の状態を通常状態と比較することにより攻撃を検出する。以下、機能の概要を Tripwire [D1]を例に説明する。

初めに、指定されたファイルやディレクトリについて、システムの最良状態にてチェック情報をハッシュ計算し基準データベースとして保存する。Tripwire for Servers では、基準データベースは 1024 ビットの署名付き El Gamal(エルガマル)非対称暗号方式を利用して署名される。ハッシュ方式には CRC32(32 ビット)、MD5(128 ビット)、SHA(160 ビット)、HAVAL(128 ビット)がある。ホスト型 IDS ではこの基準データベースを元に変化を検出するため、導入初期での基準データベース作成が非常に重要になってくる。

運用時は、設定された時間間隔で整合性をチェックし、不整合を検出した場合はレポートとして保存するほか、指定したアドレスにメール送信することも可能である。

### 3.3.3 ネットワーク型 IDS

ネットワーク型 IDS は、ネットワークを流れるパケットをシグネチャと比較することで攻撃を検出する。以下、機能の概要を Snort [D2]を例に説明する。

ネットワーク型 IDS ではシグネチャと呼ばれる攻撃の兆候を表すデータと比較を行う。Snort ではシグネチャ(ルール)をルールヘッダと括弧でくくられたルールオプションの形式でデータベース化する。

Snort の導入やシグネチャについては文献[D3]にも詳しく説明してあるが、以下に概要を記述する。

### ルールヘッダ (ルールオプション)

ルールヘッダには検知する攻撃のアクションやプロトコル、IP アドレス、ポート番号とデータの流れる方向を以下のように記述する。

アクション プロトコル 元 IP アドレス 元ポート番号 -> 先 IP アドレス 先ポート番号

上記例では元から先へデータが流れる。"<"(先から元へ) や "<>"(双方向)も指定可能。ルールオプションは詳細な条件(チェックするデータ、検出時出力する文字列など)を以下のように指定する。

オプション:値

複数のオプションを記述する場合は";"で区切る。

ルールはルールセットと呼ばれるサービスなどに分かれたファイルが多数ある。これらの各ルールと採取したパケットを比較しルールにマッチするものを検出する。

### 3.3.4 最近の商用 IDS の特徴

商用 IDS はネットワーク型全盛時に比べ、ホスト型・ネットワーク型の両方の機能を兼ね備え、不正検出型と異常検出型の両方の機能を有するものがでてきた。シグネチャは日々作成され、定期的または自動的な更新を可能とするものもある。また、パケット単体の比較から、同じ接続セッションの前後のパケットの関係をチェックするステートフルインスペクションや RFC プロトコル違反をチェックするなどのプロトコル異常検出技術などにより検知機能がより高精度になってきている。

以下にいくつかの製品について、上述の機能に加えての固有の特徴(他製品に同様機能がある場合もある)を記述する。

なお記述する特徴は記載する Web ページおよびキーワード検索("侵入検知"および各製品名)にてヒットした Web ページを参照した。

#### Realsecure [D4]

ホストベース、ネットワークベースのセンサーと管理コンソールで構成される。不正を検知すると可能な限りバックトレースを行い、侵入者を特定しアドレスをフィルタリングすることができる。

#### Dragon [D5]

ホスト型機能、ネットワーク型機能、管理機能から構成される。仮想サーバを構築して攻撃者を誘い込み、行動を記録するハニーポットモジュールがある。

#### NFR NID [D6]

N-Code と呼ばれる通信解析用のプログラミング言語で記述されたロジックシグネチャにより通信内容を検査する。

### ManHunt [D7]

イベントの分析や関連付けをリアルタイムで行う相関分析エンジンを搭載し、攻撃元の IP アドレスやポート番号、攻撃タイプなどを元に似たイベント同士をグループ化し、管理を容易にしている。

### IntruShield [D8]

既知攻撃(シグネチャ使用)、新規/未知攻撃(アノマリ技術使用)、DoS 攻撃(統計的なヒューリスティック技術を採用する複合的なアルゴリズムを使用)の検知を可能にする、現在適用可能な IDS 技術を統合している。

### Sniper [D9]

メールの本文や添付ファイルを保管・管理し、メールの全文検索機能を有する。

## 3.3.5 最近の研究

最近の侵入検知に関する研究では、以下のような分野についての取り組みが盛んである。

### 検知手法に関する技術研究

複数の検出手法の融合や収集情報の共有・統合・標準化を行う研究[D10][D11][D12][D13]や、仮想環境に関して誘導・試行・調査を行う研究[D14][D15][D16][D17][D18][D19]、異常検出のプロファイルに関する研究[D20][D21]やエージェントを用いた検出手法に関する研究[D22]など。

### 管理者の判断材料の補助を行う技術研究

収集・検出したログの扱いに関する研究[D23][D24][D25][D26]など。

### 被害予測に関する技術研究

攻撃を受けた場合の被害を予測する研究[D27][D28][D29]など。

### 攻撃者の特定に関する技術研究

能動的な情報付与を利用して攻撃者を特定する研究[D30]など。

## 3.3.6 侵入検知手法に関するまとめ

コンピュータウイルス、特にワームは、不正アクセス手法の中でも最も頻繁に新しいパターンが現れている。その検知手法は、既知のものは侵入検知における不正検出型と同様、ルールパターンとの比較によるものである。

未知ウイルスの検出を考えると、未知のものは不正検出型の手法では検知することはできないため、ウイルスに感染したコンピュータが次の対象を探すためのスキャン行動や、増殖のためメールを使用することによるトラフィック増加などを検知する異常検出型の侵入検知手法に効果がある。これはウイルス検出手法におけるビヘイビア法に相当する。

すなわち、ワームのようにネットワーク上での挙動が顕著なウイルスに関しては、ネット

ワーク機器や回線の状況を監視することで未知ウイルスの検出が可能であるといえる。ビヘイビア法にネットワークの監視も含めることにより、有用性の高いウイルス対策システムとなるだろう。

## 4 まとめ

ウイルス検出手法に関する、公開され入手可能な論文、書籍、特許情報、Web ページ等の文献により、ウイルスの分類とウイルス検出の中心となる技術(コア技術)について調査し、それを利用したウイルス検出システムの情報を分類、分析した。

その結果、コア技術については、従来からあるパターンマッチング法はもちろん、より高度な新しい技術であるビヘイビア法も多数公開されていた。最近の文献の大半がビヘイビア法に関するものであり、これは、この技術が現在もっとも注目されていることを表している。

ビヘイビア法は、検査対象プログラムを動作させ、その挙動を監視することにより、そのプログラムが実際に行う危険な行為を検出し阻止することのできる、最も本質的な検出手法であるといえる。これに、既知ウイルスの検出技術として歴史的蓄積のあるパターンマッチング法を併用することが、ウイルス対策システムの主流であることは間違いないだろう。

また、侵入検知手法の調査により、ネットワークを徘徊するワームに関しても、ネットワークベースのビヘイビア法が有効であることを確認した。ワクチンとファイアウォールは連係して動作するようになっていても実体は別々の製品であることが多いが、これらの機能をより密に連係・統合することでより効果的なシステムが実現できる可能性がある。

なお、本報告書ではコア技術を大まかに分類したため、これら以外の手法は簡単には開拓できないように見える。新しいコア技術を開発するには大きな環境の変化が必要となるだろう。

しかしながら、コア技術を実装するための詳細設計の部分について、例えば、ヒューリスティックな検出技術の精度を高めるためのルールの生成方法に別の統計分析モデルを用いたり、人工知能的な学習アルゴリズムを採用するなど、実装技術に関してはまだまだ研究の余地がある。また、コア技術を効果的に利用する運用技術に関しても、新しいアイデアが生まれる可能性はまだ十分にあると考えられる。

ただし、現状の対策はあくまでも現状のウイルスを元に検討されており、今後コンピュータを取り巻く環境が変わったり、コンピュータの新しい問題を悪用する新しいウイルスが出現した場合は、その特徴に合わせた新しい対策を検討していかなければならないだろう。

今回注目した技術はあくまでも全体の一部であり、これら以外にも着目すべき部分があると考えられる。今後のさらなる検討の指標として、本報告書が活用されることを期待している。

## 付録A ウイルスの分類に関する文献

ウイルスの分類に関して調査した文献を、その分類の概要とともに以下に示す。

下記のリストは、[文献番号] 著者名, 「文献名」, 分類の概要, 文献の所在, 発表年、の順に記載している。ただし、Web ページに発表年が明記されていないものに関しては、そのページデータの最終更新年を記載している。また、URL は 2003 年 10 月現在のものである。

書式

[文献番号] 著者名,  
「文献名」,  
分類の概要,  
文献の所在, 発表年

- [A1] Ahnlab,  
「ウイルスデータベース / ウイルスの種類」,  
ブートウイルス、ファイルウイルス、ブート/ファイルウイルス、ウィンドウズウイルス、Linux、OS/2、MAC、マクロウイルス、スクリプト、JAVA(スクリプトでない)、トロイの木馬(バックドア)、Dropper、ワーム(WORM),  
[http://www.ahnlab.co.jp/virusinfo/sec\\_vir\\_search.asp](http://www.ahnlab.co.jp/virusinfo/sec_vir_search.asp), 2003
- [A2] David Harley, Robert Slade and Urs E. Gattiker,  
「ウイルス対策マニュアル」,  
ウイルス、ワーム、ドロPPER、ジェネレータ、トロイの木馬、パスワード窃盗型、バックドア、リモートアクセスツール、DDoS エージェント、ルートキット等に分類している,  
SOFTBANK, 2003
- [A3] IBM,  
「コンピュータウイルスの症状による分類」,  
マクロ感染型、システム感染型、ファイル感染型,  
<http://www-6.ibm.com/jp/domino04/pc/support/beginner.nsf/btechinfo/SYB0-005A160>, 2001
- [A4] INTERNET Watch,  
「現在のコンピューター・ウイルスの全貌とその解説」,  
プログラムファイル感染型、上書き感染型、添付感染型、メモリ非常駐型(直接感染型)、メモリ常駐型、ブートセクタ感染型、マクロウイルス、スクリプトウイルス、Java ウイルス、Batch ウイルス、ステルス型、ポリモフィズム機能を備えたウイルス、メタモフィズム機能を備えたウイルス,  
<http://internet.watch.impress.co.jp/www/column/security/0822.htm>, 2002
- [A5] Panda Software,  
「Virus, worms, trojans and backdoors」,

- Worms、Trojans、Backdoors,  
[http://www.pandasoftware.com/virus\\_info/about\\_virus/keys2.htm](http://www.pandasoftware.com/virus_info/about_virus/keys2.htm), 2003
- [A6] Sophos,  
「コンピュータウイルス用語集 (OS 別)」,  
DOS 実行ファイル感染型ウイルス、DOS ブートセクタ感染型ウイルス、DOS ワーム、Linux 実行ファイル感染型ウイルス、Linux ワーム、Macintosh ファイル感染型ウイルス、Macintosh ワーム、PalmOS 実行ファイル感染型ウイルス、Unix ワーム、Win16 実行ファイル感染型ウイルス、Win32 実行ファイル感染型ウイルス、Win32 ワーム、Windows 95 実行ファイル感染型ウイルス、Windows 98 実行ファイル感染型ウイルス、Windows NT 実行ファイル感染型ウイルス、Windows 2000 実行ファイル感染型ウイルス,  
<http://www.sophos.co.jp/virusinfo/articles/glossary.html>, 2001
- [A7] Sophos,  
「コンピュータウイルス用語集 (スクリプト系)」,  
AppleScript ワーム、Corel Script ウイルス、JavaScript ウイルス、JavaScript ワーム、mIRC、pIRCH スクリプトワーム、Visual Basic Script ウイルス、Visual Basic Script ワーム、バッチファイル感染型ワーム,  
<http://www.sophos.co.jp/virusinfo/articles/glossary.html>, 2001
- [A8] Sophos,  
「コンピュータウイルス用語集 (その他)」,  
コンパニオンウイルス、トロイの木馬、ドロッパー、ドロップ(作成された)ファイル、マスターブートセクタ感染型ウイルス、レジストリ感染型ウイルス、Macromedia Flash 感染型ウイルス,  
<http://www.sophos.co.jp/virusinfo/articles/glossary.html>, 2001
- [A9] Sophos,  
「コンピュータウイルス用語集 (マクロ系)」,  
Access 97 マクロウイルス、Excel 97 マクロウイルス、Excel フォーマットウイルス、Excel マクロウイルス、Office 97 マクロウイルス、PowerPoint 97 マクロウイルス、Word マクロウイルス、Word 97 マクロウイルス、Word 97 マクロトロイの木馬、Word 97 マクロワーム、Word 2001 マクロウイルス,  
<http://www.sophos.co.jp/virusinfo/articles/glossary.html>, 2001
- [A10] Symantec,  
「3 種類に大別できるコンピュータ・ウイルス」,  
プログラム感染型、ブート感染型、マクロ感染型(マクロ・ウイルス),  
<http://www.symantec.com/region/jp/sarcj/reference/column/column991117.html>, 1999
- [A11] Symantec,  
「次々に誕生する複合型や新型ウイルス」,

- ステルス型、ステルス型、ポリモフィック型、メモリ常駐型、ダイレクト・アクション型、複合感染型、マルチ・プラットフォーム型(Java、VBS),  
<http://www.symantec.com/region/jp/sarcj/reference/column/column991117.html>,  
1999
- [A12] Symantec,  
「ウイルスの影響による分類」,  
ブートセクタ、プログラム,  
<http://www.symantec.com/region/jp/sarcj/reference/vfaq.html>, 1998
- [A13] Symantec,  
「ウイルスの種類による分類」,  
プログラム感染型、ブート感染型、複合感染型,  
<http://www.symantec.com/region/jp/sarcj/reference/vfaq.html>, 1998
- [A14] Symantec,  
「ウイルスの特徴による分類」,  
メモリ常駐、非メモリ常駐、ステルス、暗号化、多形態、トリガーイベント、自然界ウイルス、動物園ウイルス,  
<http://www.symantec.com/region/jp/sarcj/reference/vfaq.html>, 1998
- [A15] Symantec,  
「コンピュータウイルスの要約 / コンピュータウイルスとその動作形態」,  
ファイル型、ブートセクタ/パーティションテーブル型、複合感染型、トロイの木馬、  
ファイルオーバーライター(上書き感染型)、多形態型、ステルス型,  
<http://www.symantec.com/region/jp/sarcj/reference/corpst.html>, 1998
- [A16] Trend Micro,  
「ウイルスが利用する技術による分類」,  
VB スクリプト型、Java スクリプト型、Java アプレット型、ActiveX コントロール  
型、ステルス型、 ミューテーション型(ポリモフィック型),  
<http://www.trendmicro.com/jp/security/general/type/overview.htm>, 2003
- [A17] Trend Micro,  
「ウイルスの活動による分類」,  
ワーム型、ダイレクトアクション型、ウイルスドロPPER、ネットワーク型、バック  
ドア型,  
<http://www.trendmicro.com/jp/security/general/type/overview.htm>, 2003
- [A18] Trend Micro,  
「メモリに常駐するかどうかによる分類」,  
メモリ常駐型、直接感染型(非メモリ常駐型),  
<http://www.trendmicro.com/jp/security/general/type/overview.htm>, 2003
- [A19] Trend Micro,  
「感染する場所による分類方法」,

ファイル感染型、システム領域感染型、複合感染型、マクロ型、トロイの木馬型、携帯端末型、

<http://www.trendmicro.com/jp/security/general/type/overview.htm>, 2003

[A20] Vector,

「コンピュータウイルスの分類」,

ブートセクタ感染型、ファイル感染型、ポリモフィック型、ステルス型、複合感染型、

[http://www.vector.co.jp/for\\_users/study/virus.html#top\\_of\\_bunrui](http://www.vector.co.jp/for_users/study/virus.html#top_of_bunrui), 2000

[A21] アイ・オー・エス,

「コンピュータウイルスとは」,

ブートセクタ型、ファイル感染型、マクロ型、ワーム、トロイの木馬、

<http://www2.ios-corp.co.jp/index.asp>, 2003

[A22] アトミックドロップ,

「最新 コンピュータウイルスがわかる」,

ファイル感染型、システム感染型、複合感染型、マクロ型、Java/ActiveX 型、ワーム、トロイの木馬、VBS ウィルスに分類し、追記感染型と上書き感染型、直接感染型とメモリ常駐型、としても分類している、

技術評論社, 2000

[A23] アラジンジャパン,

「ウイルスの種類による分類」,

ファイル感染型、ファイルシステムウィルス、マクロウィルス、システム/ブートレコード感染型、

<http://www.aladdin.co.jp/esafe/viruses.html>, 2002

[A24] インターネット株式会社 / テクノロジーボックス,

「ウイルスが利用する技術による分類」,

VB スクリプト型、Java スクリプト型、Java アプレット型、ActiveX コントロール型、ステルス型、 ミューテーション型、

<http://www.technologybox.co.jp/virus/main/kind.htm>, 2002

[A25] インターネット株式会社 / テクノロジーボックス,

「ウイルスの活動による分類」,

ワーム、ダイレクトアクション型、ネットワーク型、バックドア型、ウィルストロッパー、

<http://www.technologybox.co.jp/virus/main/kind.htm>, 2002

[A26] インターネット株式会社 / テクノロジーボックス,

「メモリに常駐するかどうかによる分類」,

メモリ常駐型、直接感染型、

<http://www.technologybox.co.jp/virus/main/kind.htm>, 2002

[A27] インターネット株式会社 / テクノロジーボックス,

- 「感染する場所による分類」,  
システム領域感染型、ファイル感染型、複合感染型、マクロウイルス、トロイの木馬型、携帯端末型,  
<http://www.technologybox.co.jp/virus/main/kind.htm>, 2002
- [A28] ジェイエムシー ,  
「ウイルスが利用する技術による分類」,  
VB スクリプト型、Java スクリプト型、Java アプレット型、ActiveX コントロール型、ステルス型、 ミューテーション型(ポリモフィック型),  
月刊情報セキュリティ NO.2 <http://www.monthlysec.net/mail/samplemail2sec.htm>、月刊情報セキュリティ NO.3 <http://www.monthlysec.net/mail/samplemail3sec.htm>, 2003
- [A29] ジェイエムシー ,  
「ウイルスの活動による分類」,  
ワーム型、ダイレクトアクション型、ウイルスドロッパー、ネットワーク型、バックドア型,  
月刊情報セキュリティ NO.2 <http://www.monthlysec.net/mail/samplemail2sec.htm>、月刊情報セキュリティ NO.3 <http://www.monthlysec.net/mail/samplemail3sec.htm>, 2003
- [A30] ジェイエムシー ,  
「メモリに常駐するかどうかによる分類」,  
メモリ常駐型、直接感染型(非メモリ常駐型),  
月刊情報セキュリティ NO.2 <http://www.monthlysec.net/mail/samplemail2sec.htm>、月刊情報セキュリティ NO.3 <http://www.monthlysec.net/mail/samplemail3sec.htm>, 2003
- [A31] ジェイエムシー ,  
「感染する場所による分類方法」,  
ファイル感染型、システム領域感染型、複合感染型、マクロ型、トロイの木馬型,  
月刊情報セキュリティ NO.2 <http://www.monthlysec.net/mail/samplemail2sec.htm>、月刊情報セキュリティ NO.3 <http://www.monthlysec.net/mail/samplemail3sec.htm>, 2003
- [A32] 富士通 / AzbyClub,  
「活動の仕方による分類」,  
ワーム型、ダイレクトアクション型、ネットワーク型、バックドア型,  
[http://azby.fmworld.net/support/security/virus/virus01\\_01.html](http://azby.fmworld.net/support/security/virus/virus01_01.html), 2003
- [A33] 富士通 / AzbyClub,  
「感染する対象による分類」,  
ファイル感染型、システム領域感染型、複合感染型、マクロ型、トロイの木馬型、携帯端末型,  
[http://azby.fmworld.net/support/security/virus/virus01\\_01.html](http://azby.fmworld.net/support/security/virus/virus01_01.html), 2003

- [A34] 吉田宣也,  
「コンピュータウイルス図鑑'98」,  
種別としてファイル感染型、システム領域感染型、複合感染型、マクロ型に分類し、  
性質としてメモリ常駐型と非メモリ常駐型、ステルス型、ミューテーション型にも  
分類している,  
日経 BP 販売, 1998
- [A35] 渡部 章,  
「コンピュータウイルス事典」,  
不正プログラムを、ウイルス、バクテリア、ワーム、トロイの木馬、ロジック爆弾、  
時限爆弾に分類し、ファイル感染型、システム領域感染型、ステルス型などにも分  
類している,  
オーム社, 1993
- [A36] 韓国情報保護振興院 CERTCC-KR,  
「Computer Virus FAQ」,  
トロイの木馬(Trojan)、ワーム(Worm)、Dropper として分類し、また、感染する領  
域によって、ブートウイルス、ファイルウイルス、ブート/ファイルウイルスにも分  
類,  
<http://www.certcc-kr.jp/cvirc/bank/FAQ/virus-faq.html#??%201-3>, 2000
- [A37] 京栄社,  
「ウイルスの種類」,  
ファイル感染型、複合感染型、トロイの木馬型、多形態ウイルス、ステルス型ウイ  
ルス、メモリ常駐型、非メモリ常駐型、ブートセクタ/パーティションテーブル型、  
ファイルオーバーライター,  
[http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki\\_2.html](http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki_2.html), 2002
- [A38] 厚木市 / 森の里ホームズ,  
「コンピュータウイルスの種類」,  
マクロ型、システム領域感染型、ファイル感染型、トロイの木馬型、ワーム型、複  
合感染型、ミューテーション型(ポリモフィック型),  
<http://mh.at-g.net/memo/mn0011.htm>, 2001
- [A39] 総務省,  
「ウイルスの活動方法による分類」,  
自己増殖、コンピュータシステムの破壊、メッセージや画像の表示、トロイの木馬  
型,  
[http://www.soumu.go.jp/joho\\_tsusin/security/kiso/k04\\_dousa02.htm](http://www.soumu.go.jp/joho_tsusin/security/kiso/k04_dousa02.htm), 2003
- [A40] 総務省,  
「ウイルスの感染経路による分類」,  
電子メールの添付ファイル、電子メールのHTMLスクリプト、ホームページの閲覧、  
ネットワークのファイル共有、マクロプログラムの実行,  
[http://www.soumu.go.jp/joho\\_tsusin/security/kiso/k04\\_dousa01.htm](http://www.soumu.go.jp/joho_tsusin/security/kiso/k04_dousa01.htm), 2003

- [A41] 日本データ通信協会,  
「コンピュータワームの種類」,  
スクリプト型、添付型、ネットワーク型,  
<http://www.vcon.dekyo.or.jp/virus/kind/index.html>, 2003
- [A42] 日本データ通信協会,  
「狭義のウイルスの種類」,  
プログラムファイル感染型、ブートセクタ感染型、複合感染型、マクロ感染型,  
<http://www.vcon.dekyo.or.jp/virus/kind/index.html>, 2003
- [A43] 日本データ通信協会,  
「広義のウイルスの種類」,  
狭義のウイルス、トロイの木馬、コンピュータワーム,  
<http://www.vcon.dekyo.or.jp/virus/kind/index.html>, 2003

## 付録B ウイルス検出手法に関する文献(特許情報)

ウイルスの検出手法に関して調査した文献(特許情報)を、その概要とともに以下に示す。

下記のリストは、[文献番号] 出願人/発明者、「発明・考案の名称」、発明・考案の内容、対処、検出手法の特徴、検出手法の分類、検出のタイミング、検出対象となるウイルス、検出に必要な特別な環境、未知ウイルスに対する検出の可能性、出願番号 特許番号、発表年、の順に記載している。

ただし、対処、検出手法の特徴、検出手法の分類、検出のタイミング、検出対象となるウイルス、検出に必要な特別な環境、未知ウイルスに対する検出の可能性、の各項目に関しては、公表されている文献から読み取れたものを簡潔に記載したものである。文献中に明記されていない項目は - または推測可能な範囲で記述した。特に、検出対象となるウイルスは文献に明記していない場合が多く、一般的なウイルスに対応している場合は - で記し、特定の種類のウイルスを対象としている場合にはそれを明記した。

### 書式

[文献番号] 出願人 / 発明者,  
「発明・考案の名称」,  
発明・考案の内容,  
対処(検出、防止、復旧など), 検出手法の特徴,  
検出手法の分類, 検出のタイミング, 検出対象となるウイルス (文献に明記していない場合、一般的なウイルスの場合は - ), 検出に必要な特別な環境, 未知ウイルスに対する検出の可能性 高い(+), 低い(-), 出願番号 特許番号, 発表年

[B1] 科学技術振興事業団 / 厚井裕司,  
「コンピュータウイルスの駆除方法及びコンピュータウイルスの検出表示方法」,  
コンピュータウイルス対策用のプログラムにコンピュータウイルスと同様の感染能力を持たせることで、コンピュータウイルスの感染先に自動的にワクチンを送り込む方法を提供する,  
駆除, ワクチンに感染能力を持たせ、感染先に送り込むことを目的にしており、検出方法については「公知の技術を用いる」として、ウイルスパターンやシグネチャをもとにスキャンすることが例示されているに留まっている,  
-, -, ワームやトロイの木馬等も含む不利益をもたらす不正プログラム, -, -, 特開  
2003-288227, 2003

[B2] 学校法人金沢工業大学 / 服部進実,  
「ウイルス検出方法および装置」,  
特徴コードの重みによってマクロの危険度を算出し、マクロがウイルスであるかどうかを判定する,  
検出, 特徴コードの重みによってマクロの危険度を算出し、マクロがウイルスであるかどうかを判定、検出する,

- ヒューリスティック法, 特徴コードが所定の基準値を超えた時, マクロウイルス, -, (+), 特開 2003-186687, 2003
- [B3] 株式会社東芝 / 高橋俊成,  
「コンピュータウイルス発生検出装置、方法、およびプログラム」,  
特異データを収集し、未知ウイルスの状態での発生を検出する,  
検出 通知, 例外ポート通信、不完パケット、通信量、エラー量等のデータからウイルス判定、検出する,  
ビヘイビア法, 侵入時または感染後、特異データ検出時, 想定外の振る舞いが起こる全てのウイルス。ワームも含む。-, -, (+), 特開 2003-241989, 2003
- [B4] 株式会社日立製作所 / 片岸誠,  
「電子メールシステム、メールサーバ及びメール端末」,  
小型のメール端末に負担を発生させることなく、メールサーバでウイルスの感染判定を行う,  
検出 通知, 携帯電話事業主が設置するメールサーバで、ウイルスパターンに基づいて感染を判定する,  
パターンマッチング法, メール送受信時, 消去、書換え、外部転送等の悪影響を起こすプログラム, -, (-), 特開 2003-143230, 2003
- [B5] 株式会社日立製作所 / 高橋政慶,  
「コンピュータウイルスのチェック方法」,  
コンピュータウイルスのデータベースを用いてウイルスチェックを管理し、ハードの負担を軽減する,  
検出, ワクチンプログラムによって検出する,  
パターンマッチング法, 定期的なウイルスチェック時, -, -, (-), 特開 2003-216445, 2003
- [B6] 株式会社日立製作所 / 寺田真敏,  
「システム稼働保証支援方法」,  
ウイルスの駆除ツールが配布されていなくてもウイルスの拡散を抑止し、ネットワークシステムの通信稼働性を保証するために異常トラフィックの検知、宛先サービス番号・通過サービスのアクセス制御の切替え等を行う,  
検出 拡散防止, 不正パケットパターンデータに類似する不正パケットを一定時間内に閾値以上検出した時にウイルスの拡散を判断する,  
パターンマッチング法, 不正パケットパターンデータに類似する不正パケットを一定時間内に閾値以上検出した時, ワームも含む, ネットワーク, (-), 特開 2003-281002, 2003
- [B7] 株式会社リコー / 上原敏生,  
「ネットワークファクシミリ装置」,  
インターネットファクシミリ装置に進入するコンピュータウイルスの感染の拡大を防止する,

- 検出 感染防止, 電子メール添付された TIFF ファイルを展開したとき、所定のウイルス対策ソフトにより、TIFF ファイルから検出する,  
パターンマッチング法, メール受信時, -, -, (-), 特開 2003-259066, 2003
- [B8] コグニティブリサーチラボ株式会社 / 津田和彦,  
「高速データ通信対応の分散処理型ファイアウォールシステム」,  
ウイルスの検出をサーバで行い、フィルタリング処理をクライアントで行うことで、超高速データ受信の実現を図る,  
分散処理, ウイルスの検出をサーバで行い、フィルタリング処理をクライアントで行うというシステム提供を目的としたものであり、検出手法には関わらない,  
-, -, -, ウイルス検出サーバ, -, 特開 2003-141077, 2003
- [B9] ザクソン・アールアンディ株式会社 / 吉井清敏,  
「コンピュータウイルス検査システムの一斉管理システム」,  
ネットワーク内で検出されたウイルス情報を他のユーザに対し、注意を喚起したり、監視システムの状態を遠隔監視する手段を提供したりする,  
検出 通知, ネットワーク内のある 1 台で、ワクチンデータとの照合等によって検出する,  
パターンマッチング法, ワクチンデータ照合時, 改ざん、破壊等の望ましくない動作をするように作成したプログラム, ネットワーク, (-), 特開 2003-005989, 2003
- [B10] さくら情報システム株式会社 / 松永善充,  
「コンピュータウイルス対策システム及びコンピュータウイルス対策方法」,  
アンチウイルスソフトによりウイルスの攻撃を受けたファイルを含む検疫情報、それに基づく機器情報を一元的に管理しながら、情報としてポータルサイトにて提供する,  
情報提供, アンチウイルスソフトによって検出する,  
パターンマッチング法, アンチウイルスソフト実行時, -, -, (-), 特許第 003404032 号, 2003
- [B11] ソニー株式会社 / 栗原高明,  
「通信システム、通信装置およびその方法」,  
ウイルス検知パターンデータファイルをユーザが自動的かつ効率的に更新できる通信システムを提供する,  
検出, ウィルス検知パターンデータファイルによって検出する,  
パターンマッチング法, パターンデータによる検証時, -, -, (-), 特開 2003-241987, 2003
- [B12] 米澤明憲,  
「ネットワーク免疫システムおよびネットワーク免疫プログラム」,  
ネットワーク上のコンピュータウイルスの検査・治療作業を安全かつ自動で行うことによって管理運営の効率化を図る,  
検出 修復, 第三者の不正介入からネットワーク内の安全を確保しつつワクチンソフ

トを配布するための認証システム及び方法が提案されている。この認証はウイルス対策としては用いられていない。ウイルス検出はワクチンソフトによるものである。、パターンマッチング法、検査ソフト実行時、-, -, (-), 特開 2003-208325, 2003

- [B13] 株式会社エヌ・ティ・ティ・ドコモ / 茂呂田聡,  
「移動通信端末、情報処理装置、中継サーバ装置、情報処理システム及び情報処理方法」,  
移動端末で使用されるデータについてウィルスの検出を効率よく行うために、ウィルス検査装置へのデータ送信をし、検出結果を受信する,  
検出、中継サーバ装置で、パターンデータによって検出する,  
パターンマッチング法、中継サーバ装置でのデータ受信時、-, ウィルス検査装置、中継サーバ装置、(-), 特開 2003-256229, 2003
- [B14] 株式会社エヌ・ティ・ティ・ドコモ / 茂呂田聡,  
「サーバ装置、移動通信端末、情報送信システム及び情報送信方法」,  
携帯電話におけるウイルス検出を効率よく行うためのサーバ装置を提供する,  
検出、パターンデータによって検出する,  
パターンマッチング法、パターンデータによる検証時、-, サーバ装置、(-), 特開 2003-216447, 2003
- [B15] 株式会社フリード / 稲垣靖彦,  
「電子メール配信システム」,  
メールの送受信の管理システムを構築し、職務責任者による自動閲覧を可能とすることにより、適正かつ効率的な送受信が遂行する,  
送受制限、メールの送受信に関する管理システムであり、検知、検出手法とは関わっていない,  
-, -, -, -, -, 特開 2003-016004, 2003
- [B16] 株式会社日立情報システムズ / 阿部秀晴,  
「コンピュータウィルスの侵入防止方法」,  
ウィルスチェック処理の実施日時、ファイル作成日時の情報をもとに、ウィルス感染の恐れのある場合はファイルへの要求をすべて拒否するなど、感染を防止する,  
防止、ウィルスチェックを確実にを行うための方法であり、検出手法には関わらない,  
-, -, -, -, -, 特許第 003392283 号, 2003
- [B17] 株式会社日立情報システムズ / 吉澤満,  
「コンピュータウィルス検出時対処支援装置とその方法およびその処理プログラム」,  
ウィルス検出時に、その対処方法のデータベース、対処方法検索手段、対処方法送信手段を有する対処支援装置を提供する,  
対処支援、検出後の対処支援を目的としており、検知・検出手法には関わらない,  
-, -, -, -, -, 特開 2003-015899, 2003
- [B18] 大阪瓦斯株式会社 / 内堀保治,

「コンピュータウイルス拡散防止方法」,  
新種のコンピュータウイルスに対し、拡散を抑制して被害を最小限に留めるために、  
ウイルス情報確認工程、プロファイル工程、情報通信端末起動工程を実施する、  
拡散防止, OS 実行前にウイルス情報サーバからウイルス情報を確認し、より素早い  
対応方法で拡散を防ぐことを目的としており、検出手法には関わらない、  
-, -, -, -, 特開 2003-256230, 2003

[B19] 翼システム株式会社 / 春山裕彦,  
「端末稼働監視システムおよび端末稼働監視方法」,  
稼働状態に影響を与える異常やウイルス感染を早期に発見するためのネットワーク  
内の PC の集中監視システムを提供する、  
監視 通知, ネットワーク内のウイルス感染に対する素早い対応を目的とするもので  
あり、検知・検出の手法には関わっていない、  
-, ネットワーク内で異常発生後, -, ネットワーク集中監視システム, -, 特開  
2003-186702, 2003

[B20] 青山相現,  
「不審な電子メールからの保護システム」,  
不審な電子メール、添付ファイルを、検出及び除去可能な処理センターに送り、処  
理を依頼する、  
検出 除去, 処理センターで、最新のウイルス検出・除去プログラム、最新ワクチン  
ソフトを使って検出、除去する、  
パターンマッチング法, 不審メール受信後、メール開封前・添付ファイル実行前に処  
理センターへ送信して検出, トロイの木馬、ワーム、マクロウイルス、ファイル感  
染型ウイルス等, ウイルス処理センター, (-), 特開 2002-366487, 2002

[B21] 株式会社セクイ・コム / 金男俊,  
「ネットワークを通じた遠隔コンピュータウイルス防疫システム及びその方法」,  
ウイルス診断、治療手段、ウイルス監視及びワクチン配布、アップデート等の防疫  
システムを提供する、  
検出 修復 監視, ウイルス感染後のウイルスの早期分析・アップデートワクチンのネ  
ットワーク内での早期配布等を目的にしており・検出の方法としては、右記の分類  
手法を用いていると言える、  
パターンマッチング法, ワクチンソフト実行時, -, -, (-), 特開 2002-259149, 2002

[B22] 株式会社富士通プライムソフトテクノロジ / 南部雅也,  
「ワクチンソフト提供方法及びプログラム」,  
新種ウイルスの感染拡大を防いで障害の発生を早期に防止するためのワクチンソフ  
トの提供方法、  
情報提供, 情報提供を目的としたものである。提供する情報にはワクチンソフト及び  
パターンファイルが含まれており、検出手法は右記の分類手法と言える。、  
パターンマッチング法, ワクチンソフト実行時, -, -, (-), 特開 2002-259150, 2002

- [B23] コグニティブリサーチラボ株式会社 / 苜米地英人,  
「抗体接種型動的アンチウイルスシステム」,  
実行プログラムとセキュリティ監査手段を一体化したセキュリティ監査機能付実行プログラムを生成することでセキュリティ監査を時間的遅延なく実行する,  
検出, パターンファイルによって検出する,  
パターンマッチング法, アプリケーションソフト実行時, -, -, (-), 特開 2002-196944, 2002
- [B24] トレンドマイクロ株式会社 / リー、フランク,  
「データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体」,  
情報通信装置から受信したデータをセキュリティサーバに転送し、ウイルスチェックをした後にデータを宛先へ送信する,  
検出, ユーザの利便性を損ねることなくチェックすることを目的としているものであり、検出手法には関わらない,  
-, -, -, セキュリティサーバ, -, 特開 2002-358253, 2002
- [B25] パイオニア株式会社 / 野崎隆志,  
「電子メールのウイルスチェックシステム」,  
電子メール配信システムにおいて、メールサーバがウイルスパターンデータに基づいてウイルスチェックを行う,  
検出, ウィルスパターンデータに基づいて検出する,  
パターンマッチング法, 電子メール配信システムでの配信前, -, -, (-), 特開 2002-368820, 2002
- [B26] ベイジンライジングテクノロジーコーポレーションリミテッド / タンハオミョウ,  
「既知や未知のコンピュータウイルスの検索・駆除方法」,  
ウイルス感染を誘発するための仮想環境を作成し、疑いのある対象をロードさせ、そこでの感染による環境の変化を監視することによって、ウイルスを検出する方法を提供する,  
検出 駆除, この方法では、ウイルスの感染性を主として利用し、仮想環境内で感染を誘発することにより、感染性のある未知ウイルスを検索する,  
コンペア法(感染前後のバイト比較), 仮想環境内でウイルスを実行し、感染を誘発した時, 感染性のあるウイルス, 仮想マシン環境, (+), 特開 2002-342106, 2002
- [B27] 沖電情報サービス株式会社 / 平良英一,  
「パターンファイル更新システム」,  
動画・音声・静止画データ等を含むコンテンツ情報をウイルスパターンファイル更新時に同時にダウンロードさせることにより、ユーザに更新への関心を持たせる,  
情報提供, パターンファイル更新を意識付けることを目的としたものであり、検出手法には関わらない,  
パターンマッチング法, -, -, -, (-), 特開 2002-196942, 2002

- [B28] 株式会社エヌ・ティ・ティエムイー / 岩水堅治,  
「電子メール送信装置及び方法、電子メール送信プログラムを記録したコンピュータ読み取り可能な記録媒体」,  
大容量の添付ファイルを有する電子メールを圧縮・分割等の処理を施すことにより、受信処理が容易で且つウイルス感染していない情報を送信することのできる送信装置を提供する,  
-, 大容量の添付ファイルを有する電子メールの送信処理方法であり、検出手法には関わらない,  
-, -, -, -, 特開 2002-123473, 2002
- [B29] 株式会社ソフトサイエンス / 沖野秀信,  
「ネットワーク集中監視方法」,  
ウイルス対策、不正アクセス対策、不接続対策のため、ワクチン投入・最新ワクチンダウンロード・各情報機器の接続状況の監視等を一括して行うネットワーク監視方法を提供する,  
監視, ワクチンプログラムを用いて検出する,  
パターンマッチング法, ウイルスチェックプログラム実行時, -, ネットワーク, (-),  
特開 2002-149435, 2002
- [B30] 三菱電機株式会社 / 白井昭宏,  
「情報処理装置および BIOS の復帰方法」,  
BIOS 復帰プログラムを実行することにより、ウイルス被害を受け破壊された BIOS データを復帰させる,  
修復, データの復帰を目的とするものであり、検出には手法には関わらない,  
-, -, -, -, 特開 2002-023875, 2002
- [B31] 森田壽郎,  
「内容証明電子メール」,  
電子メールの内容をネットワーク中のサーバに保管し、発信者受信者または第三者の要求により内容、日時等の証明書を発行する また、複数サーバへの保管によってハッカー・ウイルス・天災等からデータを保護する,  
保護, サーバ管理による内容証明は電子メールの内容の保護を目的とし、内容証明をウイルス検出手法としては用いていない,  
-, -, -, サーバ, -, 特開 2002-064535, 2002
- [B32] 船井電機株式会社 / 田中秀樹,  
「情報伝送システム、及び、情報伝送方式」,  
ネットワーク内で送受信されたデータを送信データと受信データを照合することでウイルス混入・不正アクセス行為の痕跡を検出する,  
検出, 送信装置から受信装置へ送信されたデータを送信装置へ返信、照合し、データの不一致によって検出する,  
コンペア法(送受信間のバイト比較), 送信装置へのデータ返信、照合時, -, -, (+), 特開 2002-073501, 2002

- [B33] 東京工業大学長 / 大山永昭,  
「耐ウィルスコンピュータシステム」,  
ウィルスによるファイル更新の履歴退避処理に対する攻撃を防止し、ファイル更新に関する退避領域の使用を抑制してできる限りに任意時点のファイルのデータ内容に復元するためのシステムを提供する,  
防止 修復, ウィルスによるファイル更新の履歴退避処理に対する攻撃を防止、ファイルのデータ内容の復元を目的としており、検出手法には関わらない,  
-, -, -, -, 特開 2002-351723, 2002
- [B34] 東日本電信電話株式会社 / 鈴木晃,  
「電子メール中継システム及び電子メール中継方法」,  
電子メールを中継する試験用サーバを設置し、異常動作を引き起こすか否かの試験を行う,  
検出, 試験用サーバで、異常動作を引き起こさせることによって検出する,  
ビヘイビア法, 試験用サーバでのメール受信時, -, 試験用サーバ, (+), 特開 2002-314614, 2002
- [B35] 東日本電信電話株式会社 / 東裕司,  
「コンピュータウィルスの検知パターンデータ保守方法」,  
ウィルス検知パターンデータと広告データを同時に配信し、広告データの広告費を用いてウィルス検知パターンデータを無償配布することで広く最新のパターンデータを提供する,  
情報提供, 最新のウィルスパターンデータで検出する,  
パターンマッチング法, ウィルスチェックプログラム実行時, -, -, (-), 特開 2002-091786, 2002
- [B36] 富士通株式会社 / 近藤久基,  
「パスワード変更方法及びコンピュータシステム並びにプログラムを格納したコンピュータ読取可能な記録媒体」,  
ウィルス等によるパスワードの変更、設定等を防止し、パスワード変更の際してオペレータが使い慣れた GUI 等の使用環境で変更できるようにしたシステム、記録媒体を提供する,  
防止, パスワードの変更、設定等を防止することを目的としたものであり、検出手法には関わらない,  
-, -, -, -, 再特 WO02 / 005073, 2002
- [B37] 富士通株式会社 / 内藤久生,  
「コンピュータウィルス感染情報提供方法及びコンピュータウィルス感染情報提供システム」,  
ユーザ端末の通信履歴を監視し、感染時期、感染経路等の感染情報を精度よくユーザに提供する,  
情報提供, 情報提供を目的としたものであり、検出手法には関わらない,

- , -, -, -, 特開 2002-287991, 2002
- [B38] インターナショナル・ビジネス・マシーンズ・コーポレーション / ジエーン・フランソワズルペネック,  
「ウィルス・フリー・ファイル証明書を作成し使用するための方法及びシステム」,  
ファイル署名を含むウィルス・フリー証明を作成することでウィルス感染を防止する認証システムを提供する,  
防止, ウィルス・フリー証明書による認証が無い、もしくは認証が無効である場合を、  
ウィルスが存在する場合と捉えて検出する,  
インテグリティチェック法, 証明書が無い時もしくは無効の時, -, -, (-), 特開  
2001-216173, 2001
- [B39] エヌイーシーフィールドディング株式会社 / 藤井崇司,  
「ソフトウェア管理方法、コンピュータウイルス駆除システム、および記録媒体」,  
最新ウイルス駆除ソフトウェアの早期適用、適正運用を管理する,  
検出 駆除 管理, 最新のウイルス駆除ソフトで検出する,  
パターンマッチング法, ウィルス駆除ソフト実行時, -, -, (-), 特開 2001-159975,  
2001
- [B40] エブリゾーン株式会社 / 申東潤,  
「電子メールを用いてコンピュータウイルスを警報、検索及び治療するシステム及び方法」,  
ワクチンサービスサーバからクライアントに対して、電子メールを用いて、ウィルスの警告をしたり、ワクチンを送信したりする,  
検出 通知 修復, ワクチンサービスサーバでワクチンプログラムを使って検出する,  
パターンマッチング法, ワクチンプログラム実行時, -, ワクチンサービスサーバ, (-),  
特開 2001-154970, 2001
- [B41] 株式会社セブナーイレブン・ジャパン / 鈴木敏文,  
「統一形式に変換して一時的にデータ貯溜するオンラインデータプリントの代行実現方式」,  
通信機能を利用してコンピュータウイルスや印刷データ形式に対して、統一的に対処し、  
経済的な印刷代行サービスを実現する,  
-, 通信機能を利用してウィルス等に対処する印刷代行サービス方法の提供を目的とする  
ものであり、検出手法には関わらない,  
-, -, -, -, 特開 2001-243383, 2001
- [B42] ザクソンアールアンドディ株式会社 / 吉井清敏,  
「コンピュータウイルス検査機能を備えたファイルおよび電子メールのダウンロード装置」,  
インターネット、イントラネットからファイルまたは電子メールをダウンロードする装置に  
ウィルス検査機能を組み合わせ、ダウンロードと同時にウィルス検査を行う,

検出, ウィルスパターンとの照合によって検出する,  
パターンマッチング法, データのダウンロード中または直後, -, -, (-), 特開  
2001-034554, 2001

- [B43] チェイニーソフトウェアインターナ / チェン.チアーホアン,  
「データベース及びメールサーバーと共に使用するための抗ウィルスエージェント」,  
電子メールメッセージに対して、サーバーコンピュータに位置づけられた抗ウィルス  
モジュールがウィルスを走査する,  
検出, 抗ウィルスモジュールがウィルスについてファイルを検査して検出する,  
パターンマッチング法, データ受信時, 許可無くコンピュータの動作方法を変える  
プログラム, -, (-), 特表 2001-500295, 2001

- [B44] 中部日本電気ソフトウェア株式会社 / 奥村尚,  
「電子メール受信システム」,  
ウィルス侵入の恐れのあるファイル名を登録しておき、電子メール受信の際に、登  
録されているものかどうかによって、検出、排除する,  
検出, ウィルス侵入の恐れのあるファイル名を登録しておき、登録の有無によって検  
出する,  
パターンマッチング法 (ファイル名), データ受信時, -, -, (-), 特開 2001-134433,  
2001

- [B45] 東日本電信電話株式会社 / 佐藤和彦,  
「コンピュータウイルスチェック方法及び装置」,  
インターネットでのパケットデータを IP アドレスと地域 IP アドレスに対応させて  
ファイルデータに組み立て、ウイルスチェックし、感染していないデータを加入者  
端末に転送する,  
検出, ウィルス定義ファイルを使って検出する,  
パターンマッチング法, ウィルス対策用ゲートウェイヘデータ転送時, -, -, (-), 特開  
2001-256045, 2001

- [B46] 吉田博,  
「コンピュータ・ウイルス防衛除去の為の論理方式及び同システム」,  
外部電子情報を電子情報体系とは異なる別の情報体系に次元変換を行い、ウィルス  
の防衛除去を図る,  
-, ウィルスを防衛するためのシステムの提案であり、検出手法には関わらない,  
-, -, -, -, -, 特開 2001-067216, 2001

- [B47] 株式会社東芝 / 田中博明,  
「情報再生装置の命令実行方法、情報再生装置に対して命令を実行させるためのプ  
ログラムを記録した記録媒体、ディスク再生装置」,  
ディスク再生装置の操作内容をホストコンピュータの命令発行装置から発行し、ユ  
ーザの人為的操作も加わって命令の実行の可否を決定するため、ウィルスによるデ

ディスク再生装置への命令を防止する、  
命令防止、ウイルス侵入後、ウイルスによるディスク再生装置への命令を防止するものであり、検知手法には関わらない、  
-, -, -, -, 特開 2000-222201, 2000

[B48] 日本電信電話株式会社 / 吉川研一,  
「ウイルス検出付ライセンス管理方法及びシステム及びワクチンセンタ及びウイルス検出付ライセンス管理プログラムを格納した記録媒体」,  
最新のウイルス検出・除去ソフトを有するワクチンセンタからソフトを呼出して判定・除去するためのシステム・管理プログラムを提供する、  
検出 管理, 最新のウイルス検出・除去ソフトを用いて検出する、  
パターンマッチング法, ウィルス検出・除去ソフト実行時, -, ワクチンセンタ, (-), 特開 2000-039994, 2000

[B49] 株式会社明電舎 / 山本厚史,  
「遠方監視システム」,  
ウイルス感染及び不具合の発症を自動的に検知及び対処処理できる遠方監視システムを提供する、  
監視 検出, アプリケーションのファイルサイズ、OS の管理資源についての監視データからウイルス感染を判定する、  
ビヘイビア法, 監視データから異常判断した時, -, 監視システム, (+), 特開平 11-161517, 1999

[B50] 株式会社リンク・コンセプト / 南誠,  
「コンピュータウイルス自動検出装置」,  
多数のフレキシブルディスクを一度の作業で連続的かつ自動的に処理してウイルス感染の有無を検査する（ワクチンプログラム使用）,  
検出, ワクチンプログラムの実行によって検出する、  
パターンマッチング法, ワクチンプログラムの実行時, -, -, (-), 特開平 11-066669, 1999

[B51] 呉ゆい徳,  
「ハードディスクドライブを有するコンピュータのメモリ管理方法」,  
システムディスクドライブ内のシステムファイルを初期状態に維持し、ウイルスからハードディスクを保護する、  
初期形態維持, ウィルスからハードディスクを保護するものであり、検知手法には関わらない、  
-, -, -, -, 特開平 11-194938, 1999

[B52] セイコーエプソン株式会社 / 水谷憲司,  
「電子メール情報管理方法及び装置並びに電子メール情報管理処理プログラムを記録した記録媒体」,  
電子メール情報をデータベース化したものにウイルスチェックを施し、ウイルスを

検出し、削除する、

検出 駆除, 送受信者の名前やアドレス、送信経路情報、表題、テキスト文章、バイナリ情報などの内容から判断し検出する、

パターンマッチング法 (メールメッセージ), 電子メールサーバ送受信時, メールで拡散するウイルスを含む, -, (-), 特開平 11-252158, 1999

[B53] 日本電気株式会社 / 梅田久一,

「フック方式を用いたコンピュータウイルス自動検出システム」,

ソケットモジュールへの通信命令から代理関数に渡すフック手段を使って、ウイルスの有無を検査し、検出されればユーザに通知する、

検出 通知, 受信したデータとウイルスデータ列の比較を代理関数で行い、検出する、パターンマッチング法, データを記憶装置に格納する前, -, -, (-), 特開平 11-119991, 1999

[B54] 日本電気株式会社 / 山平拓也,

「ネットワーク警備方式」,

コンピュータウイルスの種類に対応して、障害発生を予防するプログラムをユーザ端末に送信し、防止処置、原因確認、障害の有無、被害の程度確認等を実行する、障害予防, 障害を予防するためのネットワーク構築を目的にしており、検出手法には関わらない、

-, -, -, -, 特開平 11-017776, 1999

[B55] ブラザー工業株式会社 / 藤井則久,

「コンピュータシステム及びコンピュータウイルス対抗方法並びにコンピュータウイルス対抗プログラムが記録された記録媒体」,

電子メール及び添付ファイルの送信元の検出、ウイルスの検出、駆除、駆除ソフトの添付等、ウイルスへの対抗策をシステム化して提供する、

情報提供, 既知ウイルスデータベースに基づき検索する手法、実行ファイルやシステム領域の変更など一定の動作を監視することで検出する手法などが取り上げられているが、その具体は明記されていない、

-, -, -, -, 特開平 11-110211, 1999

[B56] 三菱電機株式会社 / 岡賢一郎,

「プリンタ装置」,

アプレットをウイルスが混入していないことを確認してからプリンタ自身の CPU に合うように機械語に翻訳して PDL データの処理に用いるようにする、

-, プリンタ装置内部でのウイルス検出を具現化することを目的にしており、検出手法には関わらない、

-, -, -, -, 特開平 11-119927, 1999

[B57] 株式会社東芝 / 櫻修,

「コンピュータウイルスの感染経路検出方法とその方法に用いるトレースウイルスを記録する記録媒体」,

トレースウィルスを調査領域内に蔓延させウィルス感染した際に、トレースウィルスの感染履歴を順次調べていくことで、感染ルートを特定し、そのルートに基づいて侵入箇所を検出する、

経路検出 防止, 感染経路の早期検出を目的にしており、検出手法には関わらない、  
-, -, 自己複製し、感染するウィルス, -, -, 特開平 11-282673, 1999

- [B58] 日本電気株式会社 / 池村和行,  
「ウィルス対応ネットワーク接続コンピュータ」,  
ネットワーク分離プログラムによってウィルスチェック処理の実行中は情報処理装置をスタンドアローン状態にして処理中のウィルス拡散を防止する,  
拡散防止, ネットワーク拡散防止を目的にしており、検出手法には関わらない、  
-, -, -, -, -, 特開平 11-073384, 1999

- [B59] 日本電信電話株式会社 / 吉川研一,  
「ウィルス検出履歴管理装置及び方法、並びに、ウィルス検出履歴管理プログラムを記録した記録媒体」,  
ウィルスの検出状況データと除去状況データとを組み合わせることでウィルス検出履歴データとしてライセンス使用条件書に格納し、ユーザに表示できるようにし、ウィルスの検出、除去に関する冗長な作業等を減少させる、  
-, ウィルス検出履歴データをライセンス使用条件書に格納することによる検出、除去作業の効率化を目的とするものであり、検出手法には関わらない、  
-, -, -, -, -, 特開平 11-296367, 1999

- [B60] 富士通株式会社 / 石寺紳高,  
「端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体」,  
ネットワーク上の情報処理装置のウィルスチェックを確実に実行、管理できる端末管理方法及び管理装置及び端末装置等のシステム、記録媒体を提供する、  
検出, ウィルスパターンによって検出する、  
パターンマッチング法, チェックプログラム起動時, -, -, (-), 特開平 11-102333, 1999

- [B61] 武田英夫,  
「コンピュータ・ウィルスによる不正アクセス検出方法」,  
管理プログラムは被管理プログラムに対してアクセス可能アドレス領域を与え、不正アクセスを防止し、処置する、  
検出 防止, アドレスと CPU の動作を示す状態信号（書き込み信号、プログラム・フェッチ信号、スタック操作命令による実行を示す信号）から不正アクセスを検出する、  
ビヘイビア法, アクセス可能アドレス領域とそれに付随する許可条件に当てはまらないアクセスがあった時, -, -, (+), 特開平 11-073372, 1999

- [B62] クワンタム・リープ・イノベーションズ・インコーポレーテッド / シュヌラー、

ジョン,  
「コンピュータ・ウィルス・トラップ装置」,  
保護されるコンピュータから隔離された仮想環境を提供し、ウィルスにその意図する行動を行わせるエミュレーション、その行動を監視するウィルス・トラッピング装置を提供する,  
監視 検出, 仮想環境内で、割込み要求テーブルが修正されたか否か、別のプログラムが書き込まれたか否か等の変化をチェックすることで検出する,  
ビヘイビア法, トラップ装置内でのウィルス実行時、異常な挙動が検知された時, -, 仮想マシン環境, (+), 特表平 10-501354, 1998

[B63] 株式会社東芝 / 荒川豊,  
「ウィルス検査機能を有する磁気ディスク装置」,  
ホストコンピュータに負担をかけずにソフトウェアのウィルス検出・修復処理を自立的に適宜実行する磁気ディスク装置を提供する,  
検出 修復, 予め記憶されているウィルスの特徴データとのマッチング処理によって検出する,  
パターンマッチング法, 磁気ディスクのアイドル状態が一定時間以上継続した時, -, 専用機器, (-), 特開平 10-011283, 1998

[B64] 株式会社東芝 / 久田永子,  
「ウィルスチェック機能付計算機」,  
検出及び駆除のウィルスチェックを定期的に行う,  
検出 駆除, ウィルスチェックプログラムによって検出する,  
パターンマッチング法, ウィルスチェックプログラム実行時, -, -, (-), 特開平 10-040097, 1998

[B65] 新潟日本電気株式会社 / 横山正敏,  
「コンピュータウイルス受信監視装置及びそのシステム」,  
ウイルス受信監視装置をコンピュータ回線網と受信側装置との間に介在させる,  
監視 検出, ウィルスパターンによって検出する,  
パターンマッチング法, 受信監視装置でのデータ受信時, -, 監視装置, (-), 特開平 10-307776, 1998

[B66] 富士通株式会社 / 岩月孝憲,  
「情報処理装置」,  
ハードウェア構成の比較回路によってウイルス感染後に情報処理装置を停止させる, 装置停止, ウィルス感染後に情報処理装置を停止させることを目的としており、検出手法には関わらない,  
-, -, -, -, -, 特開平 10-027035, 1998

[B67] アレン、ローレンススィー、ザサード,  
「デジタル信号集合体に対する改変検出方法」,  
試験的な複数の隣接デジタル信号とスクリーニングされているコンピュータファイ

- ルとの一致不一致によってウィルスを検出する方法を提供する，  
 検出，試験的な複数の隣接デジタル信号とスクリーニングされているコンピュータ  
 ファイルとの不一致によってウィルスを検出する，  
 コンペア法，ファイルスクリーニング時，-, -, (+)，特表平 09-502550, 1997
- [B68] 株式会社日立情報システムズ / 阿部秀晴，  
 「コンピュータウィルスの侵入防止方法」，  
 2003 年の特許第 003392283 号に同じ，  
 -, -,  
 -, -, -, -, -, 特開平 09-231067, 1997
- [B69] 株式会社日立製作所 / 近藤毅，  
 「ネットワークシステムの防疫方法及びその装置」，  
 フレーム中継装置による警告機能をネットワーク上に位置づけ、ウィルスの侵入、  
 拡散、被害を最小限にとどめる，  
 検出 防止，ウィルスコードとの比較によって検出する，  
 パターンマッチング法，ウィルスフィルタ機能を備えたデータ中継装置でのデータ  
 受信時，-, データ中継装置，(-)，特開平 09-269930, 1997
- [B70] 新潟日本電気株式会社 / 横山正敏，  
 「コンピュータウィルスチェックシステム」，  
 flashROM とウィルスチェック専用のワークメモリを用いてウィルス検索を行うこ  
 とにより、ウィルスの感染、常駐を防ぐ，  
 検出 防止，flashROM とウィルスチェック専用のワークメモリを用いてウィルス検  
 索を行う（パターン検索），  
 パターンマッチング法，ウィルス検索プログラム実行時，-, 専用機器，(-)，特開平  
 09-319574, 1997
- [B71] 静岡日本電気株式会社 / 石神肇，  
 「コンピュータウィルス感染監視方法および装置」，  
 ウィルス感染監視プログラムと既存ウィルス情報によって、システム立ち上げ時に  
 感染状態のチェックをする，  
 検出 監視，パターンデータによって検出する，  
 パターンマッチング法，起動時にかかる時間が前回の処理時の時間よりも一定時間  
 以上余計に経過している時や立ち上げ回数が一定回数以上の時，-, -, (-)，特開平  
 09-288577, 1997
- [B72] 日本電気株式会社 / 愛場豊和，  
 「コンピュータウィルス感染監視・防止方式」，  
 プログラム実行システム上の実行可能プログラムに対するコンピュータウィルスの  
 感染を監視し、その感染による影響の発生を防ぐため、書き込み防止機能の内容の  
 書換えの有無を判定し、書込みありの判定によりウィルス感染を認識する，  
 監視 検出，書き込み防止機能の内容の書換えの有無によって検知する，

- ビヘイビア法, ウィルス実行時、書き込み防止機能の内容の書換え行為があった時、書き込み防止機能の内容を書き換えるウィルス, -, (+), 特許第 002621799 号, 1997
- [B73] エイ・ティ・アンド・ティ・コーポ / グレググイー・ブロンダー,  
「プログラム実行装置」,  
個人携帯端末(PDA)固有の装置識別子に結び付けてプログラムを暗号化する 安全であると推定されるプログラムの実行のみ継続を許可する,  
-, 個人携帯端末へのウィルス侵入を防止するためのプログラムの暗号化に関するものであり、検出手法には関わらない,  
-, -, -, -, (-), 特開平 08-016387, 1996
- [B74] 日立ソフトウエアエンジニアリング株式会社 / 多胡滋,  
「ウィルスチェックシステム」,  
予め複製保存した末端システムのウィルスチェックプログラムを一方向性関数によって変換したものと末端システムから転送された一方向性関数計算手段の変換結果の不一致によって、チェックプログラム内のウィルスを検出する,  
検出, ウィルスチェックプログラムを一方向性関数によって変換し、ウィルスチェックプログラム自身の感染を検出する,  
チェックサム法, 一方向性関数変換結果の不一致時, -, -, (+), 特許第 002989487 号, 1996
- [B75] 正岡孝一,  
「電子計算機におけるセキュリティ、システム保護を行うソフトウェアの構造及び仕組み」,  
正常なプログラムと不正プログラムに感染した時の差分を得て、ウィルスの侵入、感染、潜伏、発病を検知し、除去、防御するソフトウェアを使用する,  
検出 駆除, 記憶媒体、メモリーにおけるプログラムの増量、内容の比較、書き込み動作等、様々な差分情報を用いて監視、検知する,  
コンペア法 / ビヘイビア法, ウィルスチェック実行時, 侵入、感染、潜伏、発病するプログラム, -, (+), 特開平 08-044556, 1996
- [B76] 村上清治,  
「コンピュータウィルス侵入防止装置」,  
ファイル書込可能オープン要求の直前にファイルの属性変更要求があるか否かによってウィルスの可能性を判別し、ウィルスの場合は要求を禁止し、その旨を表示する,  
検出 防止, ファイル書込可能オープン要求の直前にファイルの属性変更要求があるか否かによってウィルスの可能性を判別する,  
ビヘイビア法, ウィルス実行時、ファイル書込可能オープン要求の直前, 自己増殖能力、感染能力を持つ悪性のプログラム, -, (+), 特公平 08-023846, 1996
- [B77] 富士通株式会社 / 外川好房,  
「ウィルス対応型記憶装置」,

ウイルス感染を積極的に防止しつつ、ウイルス感染したファイルについては、その使用を禁止していくと共に自動的に復旧させていく記憶装置を提供する、  
検出、修復、最新のウイルス差分情報を得ることが目的であり、検出手法には関わらない、

特開平 08-328846, 1996

- [B78] 株式会社日立製作所 / 今井厚祐,  
「ウイルス感染プロテクト法」,  
ネットワーク接続の際、ウイルス検査を行ったかどうかの情報を一元管理し、検査後のコンピュータのみの接続を許可することで、ウイルス感染を防ぐ、  
、ウイルス感染を防止するためのネットワーク構築の方法の提供であり、検出手法には関わらない、

特開平 07-281980, 1995

- [B79] シャープ株式会社 / 木村満秀,  
「コンピュータ・ウイルス検索装置」,  
ウイルス検索プログラム及びウイルス検索補助データを格納した EPROM を用いてメモリやファイル等の資源内のウイルスを検索し、不用意に書換えできないようにする装置を提供する、  
検出、ウイルスの存在データを認識するバイト列のデータを見つけることで検出する、  
パターンマッチング法、ウイルス検索プログラム実行時、特開平 07-295804, 1995

- [B80] 株式会社日立製作所 / 小川仁,  
「ディスク装置」,  
ディスク装置に関し、書き込み許可、禁止、1 回のみ 3 種類のデータ書き込み属性を含ませ、ウイルスによるデータ破壊を未然に防ぐ、  
防止、ウイルスによるデータ破壊を未然に防ぐためにデータ書き込み禁止措置をとることも可能にするものであり、検出手法には関わらない、

特開平 07-013705, 1995

- [B81] 日本電気株式会社 / 愛場豊和,  
「コンピュータウイルス感染監視・防止方式」,  
1997 年の特許第 002621799 号に同じ、

、

特開平 07-319690, 1995

- [B82] 日本電信電話株式会社 / 森啓,  
「コンピュータウイルス診断方法」,  
診断対象プログラムのデータ長を診断前後で比較することによりウイルス感染の判断をする、  
検出、診断対象プログラムのデータ長を診断前後で比較することによって検出する、

- コンペア法(データ長), 診断対象プログラム読込時, 自己複製し、感染するプログラム, -, (+), 特開平 07-175647, 1995
- [B83] インターナショナル・ビジネス・マシーンズ・コーポレーション / ジェフリー・オーウェン・ケバート,  
「コンピュータ・ウィルスおよび他の望ましくないソフトウェア実在物のシグネチャを評価し、抽出するための方法および装置」,  
ウィルスの機械コードからシグネチャを自動的に抽出し評価するための、コンピュータで実施される自動手順を提供する,  
検出, 所与のシグネチャにほぼ一致するバイト列の認識によって検出する,  
パターンマッチング法, 抽出・評価実行時, プログラムに付加する機能を有しコンピュータ命令またはコードの実行可能な組み合わせを含むもの, -, (-), 特開平 06-250860, 1994
- [B84] エイサー・インコーポレイテッド / ベイカー・リン,  
「コンピュータウィルスからコンピュータシステムを保護するための方法及びシステム」,  
ブート処理前にシステムの格納デバイスの修正を不可能にし、システムの割り込みベクタの健全性を検査することにより、ウィルスの攻撃からシステムを保護するためのシステム及び方法を提供する,  
保護 検出, 感染されていないシステムモジュールのチェックサムの計算値と対応するチェックサムの計算値を比較し、検出する,  
チェックサム法, オペレーティングシステムモジュール実行前, ブート時攻撃、ハードウェア、BIOS 直接動作、オペレーティングシステムモジュール常駐, -, (+), 特開平 06-348486, 1994
- [B85] クニックスコンピュータカンパニー / ソンキュキム,  
「コンピュータウィルスからハードとフロッピーディスクを保護する回路」,  
動作感知手段によって、ウィルスにデータを破壊されないように保護プログラムを使用する,  
保護, 保護プログラムが動作されないまま、もしくは微動作状態で、ハード及びフロッピーディスクコントローラが動作することによって検知する,  
ビヘイビア法, 保護プログラムが動作されないまま、もしくは微動作状態でのハード及びフロッピーディスクコントローラ動作時, -, -, (+), 特開平 06-149681, 1994
- [B86] 株式会社オーテック / 大原誠夫,  
「コンピュータウィルス防止制御方法及び装置」,  
拡張 BIOS により DOS に、非正常操作を監視し、必要に応じて保護する,  
監視 保護, ブートセクタ特有のデータと書き込むデータが異なる場合、デバイス・ドライバ・プログラムのエントリーポイントが修正されている場合、ファイルの修正が常駐インタラプタを利用せずに修正された場合、COMMAND.COM の場合に警告を発する,

- ビヘイビア法, 監視中に異常が発生した時, ブート型、ファイル型ウイルス, -, (+),  
特開平 06-230959, 1994
- [B87] 株式会社リコー / 大瀬戸太,  
「ファクシミリ装置」,  
ローカルエリアネットワークにおいて、受信するデータが感染しているものかどうかを調べ、感染している場合は、データ消去、通知をするファクシミリ装置を提供する,  
検出 駆除 通知, ウィルス検査ソフトによって検出する,  
パターンマッチング法, 送信対象ファイル受信時, -, -, (-), 特開平 06-350784, 1994
- [B88] 株式会社日本システムプロジェクト / 土屋達彦,  
「コンピュータウイルス防御装置」,  
着脱可能な外部記憶手段を用いて、ファイルを読み込む前にウイルスチェックと処理をし、ファイルを書き戻す,  
検出, ウィルスコード列、ファイル長、ファイルスタンプ、ファイル属性等の予め準備されて情報によって検出する,  
パターンマッチング法, スキャンワクチンプログラム実行時, -, -, (-), 特開平 06-168114, 1994
- [B89] 三菱化成株式会社 / 厚木晋,  
「情報記録媒体及びそのデータの記録方法」,  
情報記録媒体に、ウイルスチェックプログラムの記録された読み出し専用記憶領域を設け、外部データを書き込む指令が発生したとき、ウイルスをチェックする,  
検出 防止, プログラムパターンをチェックすることによって検出する,  
パターンマッチング法, データ書換え指令時, -, -, (-), 特開平 06-274419, 1994
- [B90] 日本電気ホームエレクトロニクス株式会社 / 内田浩一,  
「情報処理装置」,  
バッファされた入力データとパターンデータとを比較しウイルスを検出すると、警報信号を発生し、インターフェイスの動作を停止し、入力データの送出を停止する情報処理装置を提供する,  
検出 通知 停止, バッファされた入力データとパターンデータとを比較しウイルスを検出する,  
パターンマッチング法, 入力データバッファ時, -, -, (-), 特開平 06-337781, 1994
- [B91] 村上清治,  
「コンピュータウイルス侵入防止装置と侵入防止方式」,  
1996 年の特公平 08-023846 に同じ,  
-, -, -, -, 特開平 05-108487, 1993
- [B92] レンツステファンエイ,  
「コンピュ - タデ - タおよびソフトウェアの完全性保護装置および方法」,

アプリケーションプログラム等への CPU 制御の移送を連続して阻止し、アプリケーションプログラム等のウイルスを検出し、存在していたならば、警告信号を発生させ、拡散を防止する、

検出、ファイルサイズの確認、チェックサム、ファイルサインによる検出が例示されている、

チェックサム法、ファイルチェック時、指示コードの中にそれ自体の完全なコピーを行うための方法を有するプログラム、-, (+), 特表平 03-502263, 1991

[B93] 日本電気株式会社 / 矢津義之、

「実行形式ファイルの被破壊チェック方式」、

実行形式ファイル名、ファイル長、ファイルチェックサム等を調べることによってウイルスを検出する、

検出、実行形式ファイル名、ファイル長、ファイルチェックサム等を調べることによってウイルスを検出する、

チェックサム法、実行形式ファイルチェック時、自己複製機能及びシステム損傷機能を持つプログラム、-, (+), 特開平 03-233629, 1991

[B94] 茨城日本電気株式会社 / 星野裕之、

「記憶保護回路」、

データの上書きを許可するか否かをチェックビットでチェックしながらデータの書き込みを行うことでウイルスから保護する、

保護、書き込みを禁止するによってウイルスからデータを保護することを目的にしており、検出手法には関わらない、

-, -, -, -, -, 特開平 02-238536, 1990

## 付録C ウイルス検出手法に関する文献(論文 Web)

ウイルスの検出手法に関して調査した文献(論文、Web 情報)を、その概要とともに以下に示す。

下記のリストは、[文献番号] 発表元名称、「製品名称 / 技術名称」、概要、対処、検出手法の特徴、検出手法の分類、検出のタイミング、検出対象となるウイルス、検出に必要な特別な環境、未知ウイルスに対する検出の可能性、文献所在、発表年、の順に記載している。

ただし、対処、検出手法の特徴、検出手法の分類、検出のタイミング、検出対象となるウイルス、検出に必要な特別な環境、未知ウイルスに対する検出の可能性、の各項目に関しては、公表されている文献から読み取れたものを簡潔に記載したものである。文献中に明記されていない項目は - または推測可能な範囲で記述した。特に、検出対象となるウイルスは文献に明記していない場合が多く、一般的なウイルスに対応している場合は - で記し、特定の種類のウイルスを対象としている場合にはそれを明記した。また、Web ページに発表年が明記されていないものに関しては、そのページデータの最終更新年を記載している。URL は 2003 年 10 月現在のものである。

### 書式

[文献番号] 発表元名称,  
「製品名称 / 技術名称」,  
概要,  
対処(検出、防止、復旧など), 検出手法の特徴,  
検出手法の分類, 検出のタイミング, 検出対象となるウイルス (文献に明記していない場合、一般的なウイルスの場合は - ), 検出に必要な特別な環境, 未知ウイルスに対する検出の可能性 高い(+)、低い(-),  
文献所在, 発表年

[C1] AVET / Aleksander Czarnowski,  
「Polymorphic shellcode: advances in recent years」,  
多形態シェルコードの危険性を訴えている。エクスプロイトを利用するワームが多形態シェルコードをも利用するのは時間の問題である。 ,  
 , ,  
 , , ワーム, , ,  
<http://www.virusbtn.com/conference/vb2003/abstracts/aczarnowski03.xml>, 2003

[C2] CacheFlow,  
「Integrating Virus Scanning with CacheFlow」,  
ウェブリクエストのための、ウェブプロトコルをスキャンするツール。スキャン済みのコンテンツをキャッシュして効率化する。 ,  
検出, Web サービスのための効率的な検査システムの提案。 ,  
 , Web コンテンツのリクエスト時, , Web サーバ, ,

- [http://www.cacheflow.com/files/datasheets/an\\_virusscanning\\_sg.pdf](http://www.cacheflow.com/files/datasheets/an_virusscanning_sg.pdf), 2002
- [C3] Computer Associates / Taras Malivanchuk,  
「The Win32 worms: classification and possibility of heuristic detection」,  
新種のワームが、既存のものと同様の複製方法を使用するような再開発されたもの  
ならば、ヒューリスティックな検知は可能である。検知はワームが使用するファイ  
ル構造およびウイルスの特徴(使用コンパイラや複製方法)による。、  
検出、ワームの構造や機能を分析し、既存のものに似ていれば検出する。、  
ヒューリスティック法、チェックプログラム起動時、ワーム、-, (+),  
<http://www.virusbtn.com/conference/vb2002/abstracts/heuristic.xml>, 2002
- [C4] David Harley, Robert Slade and Urs E. Gattiker,  
「ウイルス対策マニュアル / ジェネリック方式、完全性チェック」,  
完全性チェッカ(変更検出型)は基準となる情報と現状を比較して、改ざんを検出す  
る。、  
検出、同左。、  
インテグリティチェック法、チェックプログラム起動時、-, -, (+),  
SOFTBANK, 2003
- [C5] David Harley, Robert Slade and Urs E. Gattiker,  
「ウイルス対策マニュアル / ジェネリック方式、活動モニタリング」,  
活動(振る舞い)モニタは、プログラムが何をしようとしているかを探り、疑わしいも  
のを警告する。、  
検出、同左。、  
ビヘイビア法、実行時、疑わしい動作を行ったとき、-, -, (+),  
SOFTBANK, 2003
- [C6] David Harley, Robert Slade and Urs E. Gattiker,  
「ウイルス対策マニュアル / パターンマッチング方式」,  
既知ウイルスの特徴コード列をパターンとしてマッチングする。、  
検出、同左。、  
パターンマッチング法、チェックプログラム起動時、-, -, (-),  
SOFTBANK, 2003
- [C7] David Harley, Robert Slade and Urs E. Gattiker,  
「ウイルス対策マニュアル / ヒューリスティック法」,  
現在は、スキャン方式のワクチンであっても検査するパターンは最小限にしており、  
実質は疑わしい複数のコードを広くチェックしてウイルスかどうかを推論している。  
すなわち、現在のパターンマッチング法は本質的にヒューリスティック法である、  
と述べている。、  
検出、同左。、  
ヒューリスティック法、チェックプログラム起動時、-, -, (-),  
SOFTBANK, 2003
- [C8] e-frontier,

「ウイルスキラー / RisingVirusInfectionSimulationScan (R-VISS)」 ,  
未知のウイルスを強力に検出。仮想コンピュータ上でウイルスを実際に感染させ、その感染性を確認する。その際、ウイルスの駆除に必要な情報も読み出すことによって、単に、誤認を減少させるだけでなく、駆除に生かす。 ,  
検出 駆除, 仮想コンピュータ上でウイルスを実際に感染させ、その感染性を確認する。 ,  
ビヘイビア法, チェックプログラム起動時, -, -, (+),  
<http://www.e-frontier.co.jp/products/utility/vk2003n/>,  
<http://www.g-wise.co.jp/software/vk2003/index1.html>, 2003

[C9] ESET,

「NOD32 / スマート CRC」 ,  
既知ウイルスのデータベース情報を用いた検索を行う技術。対数的アプローチとも呼ばれる高速検索を実現している。 ,  
検出, パターンマッチング法で高速に検索する技術。 ,  
パターンマッチング法, チェックプログラム起動時, -, -, (-),  
<http://www.mediaselect.co.jp/magazine/its/0302/0302210071.html>, 2003

[C10] ESET,

「NOD32 / ヒューリスティックスキャンエンジン」 ,  
検査対象のファイル内部を直接解析し、ウイルスの振る舞いをするプログラムコードが含まれるファイルを検出する。また、コードエミュレータを用いて、メモリ内に作成した仮想マシン上でファイルを実行する。 ,  
検出, スタティックなコード分析と、仮想マシンを用いたダイナミックなコードシミュレーションによって検査する。 ,  
ヒューリスティック法 / ビヘイビア法, チェックプログラム起動時, -, -, (+),  
[http://canon-sol.jp/update/nd/nd\\_catalog.pdf](http://canon-sol.jp/update/nd/nd_catalog.pdf),  
<http://www.mediaselect.co.jp/magazine/its/0302/0302210071.html>, 2003

[C11] ESET Software / Richard Marko,

「Heuristics: retrospective and future」 ,  
ESET 社の製品 NOD32 が採用しているヒューリスティック法に関する説明。 ,  
情報, -,  
ヒューリスティック法, チェックプログラム起動時, -, -, (+),  
[http://www.virusbtn.com/conference/vb2002/abstracts/heuristics\\_retrospective.xml](http://www.virusbtn.com/conference/vb2002/abstracts/heuristics_retrospective.xml), 2002

[C12] Frans Veldman,

「HEURISTIC ANTI-VIRUS TECHNOLOGY / ヒューリスティック技術のフラグについて」 ,  
ワクチンソフト TbScan が行う判断基準。疑わしい指示シーケンスを認識するため、それらの指示シーケンスごとにフラグを割り当て、プログラムから検出したフラグ

- 群によって総合的に判断する。 ,  
 検出, ヒューリスティック法で用いる判断基準 (フラグ方式) の説明。 ,  
 ヒューリスティック法 / ビヘイビア法, チェックプログラム起動時, -, -, (+),  
<http://www.rootmode.com.ar/Secciones/Virii/Archivos/heuris.zip>, 1995
- [C13] H+BEDV / John Ogness,  
 「Dazuko: an open solution to facilitate 'on-access' scanning」 ,  
 ファイルアクセス・コントロールのための標準インターフェース(Dazuko)を提供する。 ,  
 検出補助, Dazuko はファイルアクセスを監視するためのオープンな共通インターフェースであり、これを利用することで高信頼かつ広範囲のマシン環境をサポートするウイルス対策システムが実現できる。 ,  
 -, -, ファイルアクセスを行うウイルス, -, -,  
<http://www.virusbtn.com/conference/vb2003/abstracts/jogness03.xml>, 2003
- [C14] IBM Research / Ian Whalley, Bill Arnold, Dave Chess, John Morar and Alla Segal,  
 「An Environment for Controlled Worm Replication and Analysis or: Internet-inna-Box」 ,  
 仮想インターネットに接続された仮想 SOHO ネットワークおよび仮想マシンによる環境を構築する。仮想マシンは複数の VxD(仮想デバイスドライバ)から構成され、ファイルシステム活動およびレジストリ活動を監視する。 ,  
 検出, ワームの疑いのあるプログラムは、この仮想インターネット環境へ導入され、実行され、監視される。 ,  
 ビヘイビア法, データ送受信時, ワーム, 仮想インターネット、仮想 SOHO、仮想マシン, (+),  
<http://www.research.ibm.com/antivirus/SciPapers/VB2000INW.htm>, 2000
- [C15] IBM Research / Jeff Kephart, Dave Chess and Steve White,  
 「Blueprint for a Computer Immune System」 ,  
 未知のウイルス病原体の存在を感じてから、数分以内にそれを検知し削除するための手段を自動的に引き出し、展開させるコンピュータ用の免疫系を開発した。 ,  
 通知 情報入手 管理, ウイルスの疑いがあるときにその対処情報を素早く入手して対応するためのシステム。検出手法ではない。 ,  
 -, -, -, -, -,  
<http://www.research.ibm.com/antivirus/SciPapers/Kephart/VB97/index.html>, 1997
- [C16] IBM Research / Jeffrey Kephart and Steve White,  
 「Directed-Graph Epidemiological Models of Computer Viruses」 ,  
 疫学モデルを用いた、ウイルス感染の振る舞いの分析、シミュレーション方法について述べている。 ,

分析, 疫学的な分析。検出手法ではない。 ,

〒〒〒〒〒

<http://www.research.ibm.com/antivirus/SciPapers/Kephart/VIRIEEE/virieeee.gopher.html>, 1994

[C17] IBM Research / Jeffrey Kephart and Steve White,

「Measuring and Modeling Computer Virus Prevalence」 ,

ウイルスの働きの統計分析により、ウイルス拡散についての新しい疫学モデルを開発している。あるマシンが感染していると分かれば、近隣のマシンがウイルスの有無をチェックする、という方法により、組織のためのコスト効率の良いアンチウイルス技術が実現されている。 ,

通知, 疫学的な分析により、ウイルスを発見したときの通知方法の効率化を提案している。 ,

〒〒〒〒〒

<http://www.research.ibm.com/antivirus/SciPapers/Kephart/PREV/prevalence.gopher.html>, 1994

[C18] IBM Research / John Morar and David Chess,

「Can Cryptography Prevent Computer Viruses?」 ,

ウイルスに感染しているファイルが送受信の際に、あるいはサーバ上に保存される際に暗号化されている場合、従来のウイルス対策システムでは検出不可能であることの問題提起。 ,

-, 暗号化通信がウイルス検出の妨げになることを警告している。検出手法ではない。 ,

〒〒〒〒〒

<http://www.research.ibm.com/antivirus/SciPapers/VB2000JFM.htm>, 2000

[C19] ISS (Internet Security Systems),

「RealSecure Desktop Protector」 ,

パーソナルファイアウォール機能と侵入検知機能を持つ製品。未知のアプリケーションの起動を阻止するアプリケーション制御機能を搭載。MD5 チェックサムにより正当なプログラムを装うトロイの木馬プログラムも認識し、その活動を阻止する。 , 検出, チェックサム(MD5)による不正プログラムの識別。MD5 ハッシュ値が既知のもののみ対応か。 ,

チェックサム法, チェックプログラム起動時, トロイの木馬, -, (-),

[http://www.isskk.co.jp/company/press\\_office/press02/DesktopProtector\\_091002.html](http://www.isskk.co.jp/company/press_office/press02/DesktopProtector_091002.html), 2002

[C20] ISS (Internet Security Systems),

「プリエンティブ・ビヘイビア・インスペクション技術」 ,

ビヘイビア解析技術。これはネットワークから集まってくる膨大なパケット/ログを統計的なパターンと比較し、正常時のパターンと異なるものを検出する手法。未知ワームの検出にも理論上有効。 ,

- 検出, ネットワークトラフィックの統計的パターンが異常なときに検出する。 ,  
ビハイビア法, データ送受信時, ワーム, -, (+),  
[https://www.isskk.co.jp/company/press\\_office/press02/vCIS\\_091002.html](https://www.isskk.co.jp/company/press_office/press02/vCIS_091002.html), 2002
- [C21] McAfee,  
「SpamAssassin エンジン」 ,  
スパム検知ルールを利用し、それぞれのルールに加重スコアを割り当てることによ  
って、スキャン対象の電子メールを累積的に評価する。 ,  
検出, スパムの検出であり、ウイルス検出手法ではないが、ルールベースの手法の実  
装方法としては参考になる。 ,  
ヒューリスティック法, -, -, -, ,  
[http://www.nai.com/Japan/products/mcafee/spamkiller\\_ws.asp?menu=tokucho](http://www.nai.com/Japan/products/mcafee/spamkiller_ws.asp?menu=tokucho),  
2003
- [C22] McAfee,  
「VirusScan Enterprise / E-Mail スキャン」 ,  
Microsoft Outlook の MAPI 電子メールクライアントに対応。電子メールのメッセー  
ジ本文と添付ファイルをスキャンし、ウイルスや悪性コードを検出して、感染を未  
然に防ぐ。 ,  
検出, 電子メールを検査する。 ,  
パターンマッチング法, メール送受信時, 電子メール型, -, (-),  
<http://www.nai.com/Japan/products/mcafee/vse.asp?menu=tokucho>, 2003
- [C23] McAfee,  
「VirusScan Enterprise / オンアクセススキャン」 ,  
常時監視機能により、フロッピーディスク、ネットワークやインターネット上のさ  
まざまなソースを感染源とするウイルスを防御する。 ,  
検出 防止, 常駐して監視する。 ,  
パターンマッチング法, ディスク等のアクセス時, -, -, (-),  
<http://www.nai.com/Japan/products/mcafee/vse.asp?menu=tokucho>, 2003
- [C24] McAfee,  
「VirusScan Enterprise / メモリスキャン」 ,  
メモリ内プロセスのスキャンにより、ウイルス、ワーム、トロイの木馬を検出でき  
る。プロセスをメモリから削除することによって、ディスクにコードを書き込まな  
いウイルスも検出し、駆除する。 ,  
検出 駆除, メモリ内をスキャンする。 ,  
パターンマッチング法, チェックプログラム起動時, ワーム、トロイの木馬を含む, -,  
(-),  
<http://www.nai.com/Japan/products/mcafee/vse.asp?menu=tokucho>, 2003
- [C25] McAfee,  
「WebShield Appliance / 透過スキャン」 ,

透過型ブリッジ構成と透過型ルータ構成の 2 種類の透過スキャンモードを備えており、SMTP、HTTP、FTP および POP3 トラフィックをスキャンしてウイルスとワームを削除する。、

検出 駆除, ネットワークに追加して透過的にスキャンする。、

パターンマッチング法, データ送受信時, -, ネットワーク, (-),

<http://www.nai.com/japan/products/mcafee/ws.asp?menu=tokucho>, 2003

[C26] McAfee,

「WebShield SMTP / アウトブレイクマネージャ」,

アウトブレイクマネージャは、ウイルスの感染を予見かつ自動的に防止する、未知ウイルスの感染の典型的な兆候を検出する。、

検出, 全く同一のファイルが添付されたメールが数百通届く場合など、ウイルスの感染拡大時に発生しがちなケースを「ウイルスの発生」とみなす。、

ビヘイビア法, 異常動作検出時, 電子メール型, -, (+),

[http://www.nai.com/japan/products/mcafee/ws\\_sntp.asp?menu=tokucho](http://www.nai.com/japan/products/mcafee/ws_sntp.asp?menu=tokucho), 2003

[C27] McAfee,

「WebShield SMTP / コンテンツスキャン」,

ネットワーク内外を通過するトラフィックを正確に把握し、件名、メッセージ本文、添付ファイル名などのコンテンツをフィルタリングする。、

検出 防止, メールコンテンツ内をスキャンする。、

パターンマッチング法, メール送受信時, 電子メール型, -, (-),

[http://www.nai.com/japan/products/mcafee/ws\\_sntp.asp?menu=tokucho](http://www.nai.com/japan/products/mcafee/ws_sntp.asp?menu=tokucho), 2003

[C28] McAfee,

「McAfee Virex / ビヘイビabloッキング」,

未知の悪意のあるコードからのリアルタイム保護を行う。ビヘイビabloッカーは ActiveX、Java アプレット、様々なスクリプト言語、および電子メール、インターネットあるいは他のネットワーク接続によってホストに到着する移動コードを調べる。、

検出 防止, OS 資源やアプリケーションへのアクセスを制限するサンドボックスの中で対象コードを実行し、監視する。コードがあらかじめ定められたポリシーを破ろうと試みた場合、ビヘイビabloッカーはその機能を停止させる。、

ビヘイビア法, 実行時, ポリシーを破る行動を起こしたとき, -, -, (+),

[http://www.carleton.edu/campus/ITS/software/antivirus/ds\\_virex.pdf](http://www.carleton.edu/campus/ITS/software/antivirus/ds_virex.pdf), 2000

[C29] Norman / Kurt Natvig,

「SANDBOX TECHNOLOGY INSIDE AV SCANNERS」,

ウイルスの振る舞いによる検知。仮想マシンを用いた技術。ウイルス活動として、その他のコンピュータ・ファイルにコードおよびデータを転送することや、コンピュータのファイルコントロールを奪ってファイル感染を試みるなどの動作を重点的に監視している。、

検出, サンドボックスを用いたエミュレーション。VM(仮想マシン)を使用し、仮想空間でウイルスを実行させ、異変がみられた場合に分析を実行する。 ,  
ビヘイビア法, チェックプログラム起動時, -, -, (+),  
[http://www.norman.com/documents/nvc5\\_sandbox\\_technology.pdf](http://www.norman.com/documents/nvc5_sandbox_technology.pdf), 2002

- [C30] Norman ASA / Kurt Natvig,  
「How do advanced Win32 worms really work?」 ,  
ワームがどのように動作するかの説明。また、ウイルス解析の問題点の提起。例えば、いくつかのウイルスは特定の DNS サーバと通信を行うが、多くの場合閉じた環境で解析するため実際のインターネットに接続できない。 ,  
-, ワームの動作を検証するためには実際のネットワークが必要な場合があることを問題にしている。 ,  
-, -, ワーム, -, -,  
<http://www.virusbtn.com/conference/vb2003/abstracts/knatvig03.xml>, 2003

- [C31] Norman ASA / Kurt Natvig,  
「Sandbox II: Internet」 ,  
ワクチン内部でのシミュレータでワームを検出する方法に関する説明。ワームに対してコンピュータやネットワークがあるように見せかける。 ,  
検出, ワームに対してコンピュータやネットワークがあるように見せかけ、活動させてその行動を監視する。 ,  
ビヘイビア法, チェックプログラム起動時, ワーム, -, (+),  
<http://www.virusbtn.com/conference/vb2002/abstracts/sandbox.xml>, 2002

- [C32] SecureVM,  
「Anti-Virus SecureVM / AISP (AI ServerProtection)」 ,  
サーバプロセスの振る舞いを数日から数週間カタログ化(DB)する。カタログにない動作に対し、リクエストを失敗させる、または停止が可能。セキュリティホールから進入し、サーバサービスや、インターネットにダメージを与える脅威を検出する。 ,  
検出 防止, サーバプロセスの振る舞いの異常を検出。 ,  
ビヘイビア法, サービス提供時、異常な振る舞いを検出したとき, -, -, -,  
[http://www.securevm.com/japan/whitepaper/aisp\\_product.htm](http://www.securevm.com/japan/whitepaper/aisp_product.htm), 2003

- [C33] SecureVM,  
「Anti-Virus SecureVM / Behavior Detection」 ,  
コンピュータに重要な変更を加えることができるシステムコール(API)を監視。プロセスの振る舞いと、過去のコンピュータウイルスの特徴的な振る舞いを比較。 ,  
検出, プログラム実行時の振る舞い検出。 ,  
ビヘイビア法, 実行時、異常な振る舞いを検出したとき, スパイウェアを含む, -, (+),  
[http://www.securevm.com/japan/product/svm\\_product.html](http://www.securevm.com/japan/product/svm_product.html),  
[http://www.securevm.com/japan/whitepaper/svm\\_wp.html](http://www.securevm.com/japan/whitepaper/svm_wp.html), 2003

- [C34] SecureVM,

「Anti-Virus SecureVM / PDS (ProactiveDefenseSystem)」,  
バックドア型ウイルスを検出すると、サーバポートを FireWall に通知。FireWall  
は、該当ポートを閉じるか、該当ポートに対し、外部から接続を試みたエンドポ  
イントを追跡する。、  
通知 防止, ウイルス検出時の通知技術。、

、 、 、 、 、

[http://www.securevm.com/japan/whitepaper/pds\\_product.htm](http://www.securevm.com/japan/whitepaper/pds_product.htm), 2003

- [C35] SecurityFocus /シマンテック Carey Nachenberg,  
「Behavior Blocking: The Next Step in Anti-Virus Protection / エキスパートベ  
ース」,  
人間のエキスパートが悪意のあるコードを分析しており、そのようなウイルスの疑  
わしい振る舞いを検出し、阻止する。、  
検出 防止, エキスパートベースのビヘイビア法の実装方法の説明。、  
ビヘイビア法, チェックプログラム起動時, -, -, (+),  
<http://www.securityfocus.com/infocus/1557>, 2002

- [C36] SecurityFocus /シマンテック Carey Nachenberg,  
「Behavior Blocking: The Next Step in Anti-Virus Protection / ビヘイビアプロ  
ッキング」,  
モニタは悪意のある振る舞いをリアルタイムに検出し、それらがシステムに影響す  
る前に、ビヘイビアプロッキング・ソフトウェアがそのアクションを阻む。、  
検出, ビヘイビア法の説明。、  
ビヘイビア法, チェックプログラム起動時, -, -, (+),  
<http://www.securityfocus.com/infocus/1557>, 2002

- [C37] SecurityFocus /シマンテック Carey Nachenberg,  
「Behavior Blocking: The Next Step in Anti-Virus Protection / ヒューリスティ  
ック」,  
プログラムの全面的な構造を検査し、ロジック上明白な意図に基づいて悪意がある  
という可能性の評価を行う。暗号化ウイルスに対しては CPU エミュレーションある  
いはサンドボックス技術を使用する。、  
検出, ヒューリスティック法の説明。、  
ヒューリスティック法, チェックプログラム起動時, -, -, (+),  
<http://www.securityfocus.com/infocus/1557>, 2002

- [C38] SecurityFocus /シマンテック Carey Nachenberg,  
「Behavior Blocking: The Next Step in Anti-Virus Protection / ポリシーベース」,  
管理者がどの振る舞いを許可するかを指定する。それ以外の振る舞いは阻止する。、  
検出 防止, ポリシーベースのビヘイビア法の実装方法の説明。、  
ビヘイビア法, チェックプログラム起動時, -, -, (+),  
<http://www.securityfocus.com/infocus/1557>, 2002

- [C39] SecurityFocus /シマンテック Carey Nachenberg,  
「Behavior Blocking: The Next Step in Anti-Virus Protection / 指紋採取」,  
指紋(ウイルスの特徴的なコード列)に基づいてファイル、ディスクおよびネットワーク送信中の悪意のあるコードを検知する。 ,  
検出, パターンマッチング法の説明。 ,  
パターンマッチング法, チェックプログラム起動時, -, -, (-),  
<http://www.securityfocus.com/infocus/1557>, 2002
- [C40] Sophos,  
「Sophos Anti-Virus / InterCheck」 ,  
ファイルアクセスが行われるたびに、ファイルのウイルス検索が必要かどうかを判断する。 ,  
-, 検査の必要性を判断する技術。 ,  
-, -, -, -, -,  
<http://www.sophos.co.jp/sophos/docs/jpn/papers/sav-overview.pdf>, 2002
- [C41] Sophos,  
「Sophos Anti-Virus / ウイルス検出エンジン」 ,  
ウイルス、トロイの木馬、ワームに対して、ファイルを検索して検出する。ポリモルフィック型ウイルス検出用の完全なコードエミュレータ、圧縮ファイル内のウイルスを検出するためのオンライン解凍機能、マクロウイルスを検出・駆除するためのOLE2 エンジンを持つ。 ,  
検出, ウイルスパターンによる検出のようだが、多形態型ウイルスのためのエミュレータも持っている。 ,  
パターンマッチング法, チェックプログラム起動時, -, -, (-),  
<http://www.sophos.co.jp/sophos/docs/jpn/papers/sav-overview.pdf>, 2002
- [C42] Sophos,  
「ヒューリスティック検査法」 ,  
ウイルスの亜種を検知することが可能。エミュレーションと結合した総括的な検知技術を利用。 ,  
検出, ヒューリスティックな手法とエミュレーションによる検出らしい。 ,  
ヒューリスティック法 / ビヘイビア法, チェックプログラム起動時, -, -, (+),  
[http://www.ostamerica.com/Gartner\\_Sophos.htm](http://www.ostamerica.com/Gartner_Sophos.htm),  
[http://www.phangnaughton.com/sophos\\_clippings/may03/region1/050103CMP.pdf](http://www.phangnaughton.com/sophos_clippings/may03/region1/050103CMP.pdf), 2002
- [C43] Sophos,  
「Computer virus prevention: a primer / Checksummers」 ,  
ウイルスがファイルに感染する時はそのファイルが変化する。この変化をスキャナによって検出する。 ,  
検出, チェックサムによりファイルの変更を検出する。 ,

- チェックサム法, チェックプログラム起動時, 感染を行うウイルス, -, (+),  
<http://www.securitymap.net/sdm/docs/virus/prevention.html>, 2000
- [C44] Sophos,  
「F-PROT」,  
ウイルスおよび疑わしいファイルを検知するスキャナ。WinWord ドキュメントおよびエクセル・ワークブックと同様に圧縮ファイルの中でも検知する。 ,  
検出, ファイルをスキャンする。 ,  
パターンマッチング法, チェックプログラム起動時, -, -, (-),  
<http://www.ima.com/pdf/ienews/vol2no12.pdf>, 1999
- [C45] SSIJ (Security Systems Integration Japan),  
「NETSCREEN-IDP / バックドア検知」,  
侵入検知システムの一機能。攻撃者がネットワークの脆弱性を利用してトロイの木馬を仕掛け、そのシステムを乗っ取るようにするインタラクティブなセッションを検知する。サーバの乗っ取りや攻撃の踏み台とされることを防ぐ。 ,  
検出 防止, 侵入検知の一手法。ウイルス検出への応用の可能性あり。 ,  
ビヘイビア法, データ送受信時, セキュリティホールを狙ったウイルス, -, (+),  
<http://www.telcn.jp/~cn/product/syo92.html>,  
<http://www.ssi.co.jp/products/idp.html>, [http://www.ssi.co.jp/pdf/idp\\_02.pdf](http://www.ssi.co.jp/pdf/idp_02.pdf), 2003
- [C46] Symantec,  
「Norton AntiVirus / Bloodhound」 ,  
人工知能技術を使ってプログラムの様々な論理領域を特定し、その論理領域一つ一つに含まれるプログラムロジックを分析して、ウイルスらしき動作を探す。スタティックとダイナミックの両方の技術を使用している。 ,  
検出, 人工知能によるウイルスらしさの判定。 ,  
ヒューリスティック法 / ビヘイビア法, チェックプログラム起動時, -, -, (+),  
<http://www.symantec.com/region/jp/sarcj/reference/heuristc.pdf>, 2002
- [C47] Symantec,  
「Norton AntiVirus / Striker」 ,  
多形態ウイルスを識別するための技術で、プログラムファイルをスキャンするたびに専用の仮想コンピュータの中で実際のコンピュータ上であるかのように動作する。多形態ウイルスが自己解読動作を終えた後、Striker が作動しウイルス感染を検出して修復する。 ,  
検出 修復, 仮想実行による暗号化プログラムの復号後、ウイルスを検出する。 ,  
ビヘイビア法, チェックプログラム起動時, 多形態型ウイルス, -, (-),  
<http://www.symantec.com/region/jp/sarcj/reference/heuristc.pdf>, 2002
- [C48] Symantec,  
「NetProwler」 ,  
企業ネットワークの誤用・濫用傾向を常時かつ透過的に監視するネットワークベ-

スの侵入検知ツール。ネットワーク上で動作中の ワームを検知し、攻撃を受けたシステムを特定し、ログに記録する。 ,  
検出, ネットワークの異常を検出。 ,  
ビヘイビア法, 異常検出時, ワーム, ネットワーク, (+),  
[http://www.symantec.com/region/jp/enterprise/resource/whitepaper/ses\\_btcsac\\_wp\\_j.pdf](http://www.symantec.com/region/jp/enterprise/resource/whitepaper/ses_btcsac_wp_j.pdf), 2001

[C49] Symantec,  
「Symantec Enterprise Firewall、VelociRaptor / フルインスペクション」 ,  
アプリケーション層で完全検査を行うフルインスペクション・アーキテクチャにより、Nimda や CodeRed による Web サーバのスキャンを阻止。特定の Web サーバ攻撃を識別し、それらの脅威を遮断する URL パターン・マッチング・リスト機能も持つ。 ,  
防止, 通信状態を監視して攻撃を検出する。また、URL のパターンマッチングも行う。 ,  
パターンマッチング法, データ送受信時, ワーム, -, (-),  
[http://www.symantec.com/region/jp/enterprise/resource/whitepaper/ses\\_btcsac\\_wp\\_j.pdf](http://www.symantec.com/region/jp/enterprise/resource/whitepaper/ses_btcsac_wp_j.pdf), 2001

[C50] Symantec,  
「Symantec Intruder Alert / FileWatch」 ,  
ホストベースの侵入検知ツール。ワームなどによるネットワーク上の不正あるいは悪質な動作を検知し、重要なファイルへの変更、削除、移動を検知、復元する。 ,  
検出 修復, ワームなどの不正・悪質な動作を検出。 ,  
ビヘイビア法, 異常検出時, ワーム, -, (+),  
[http://www.symantec.com/region/jp/enterprise/resource/whitepaper/ses\\_btcsac\\_wp\\_j.pdf](http://www.symantec.com/region/jp/enterprise/resource/whitepaper/ses_btcsac_wp_j.pdf), 2001

[C51] Symantec / Frederic Perriot,  
「Defeating polymorphism through code optimization」 ,  
多形態ウイルスを検出するために、最適化コンパイラに使われるコード単純化技術を利用する方法を提案している。 ,  
検出補助, 多形態ウイルスや変形ウイルスの検出のために、コード単純化技術を使用する。 ,  
-, -, 多形態型、変形型, -, -,  
<http://www.virusbtn.com/conference/vb2003/abstracts/fperriot03.xml>, 2003

[C52] TASC,  
「eDNA」 ,  
プログラムコードの振る舞いパターンの分析により、既知と未知のトロイの木馬を検出する。 ,  
検出, プログラムの特徴的なコードを認識し、微妙な違い(亜種)を判別する。単純な

パターンマッチングではなく、実行を伴う検査でもない。 ,  
ヒューリスティック法, チェックプログラム起動時, トロイの木馬(亜種にも対応), -,  
(+),  
<http://www.tasc.com/brochures/D-00199.pdf>,  
<http://www.tasc.com/solutions/edna.html>, 2001

- [C53] Technical University of Denmark / Rune Schmidt Jensen,  
「Immune System for Virus Detection and Elimination」 ,  
隠れマルコフモデルを用いて、プログラムコードの静的な学習とプログラム実行時のシステムコールの利用をトレース学習することにより、正常な振る舞いを意味する統計的なデータを得る。後に、プログラムをモニタリングし、これと異なる振る舞いを行うものをウイルスとして検知する。 ,  
検出, ハミング距離、R-隣接シンボルおよび隠れマルコフモデルを用いた、コードベースとシステムコールベースの統計的なビヘイビア法。ある程度の時間をかけて学習させなければならない。 ,  
ビヘイビア法, チェックプログラム起動時, -, -, (+),  
[http://www.imm.dtu.dk/pubdb/views/edoc\\_download.php/959/pdf/imm959.pdf](http://www.imm.dtu.dk/pubdb/views/edoc_download.php/959/pdf/imm959.pdf),  
2002

- [C54] Tiny,  
「TPF」 ,  
パーソナルファイアウォール。特に、サンドボックス機能を備えており、アプリケーションをサンドボックス内で機能させ、実行しようとするシステムリソースやレジストリの書き込みなどに関する行動を全て監視する。 ,  
検出 隔離, プログラムの危険な行動を検出。 ,  
ビヘイビア法, チェックプログラム起動時, -, -, (+),  
<http://www.watch.impress.co.jp/internet/www/article/2002/1120/nod32.htm>, 2002

- [C55] TrendMicro,  
「BootTrap」 ,  
ヒューリスティック検知。ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。ブートセクタなどに感染するタイプのウイルスを検出する。 ,  
検出, ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。 ,  
ヒューリスティック法, チェックプログラム起動時, ブートセクタウイルス, -, (-),  
<http://pcweb.mycom.co.jp/news/2003/01/30/08.html>, 2003

- [C56] TrendMicro,  
「MacroTrap」 ,  
ヒューリスティック検知。ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。VBA や Word Basic で記述されたマクロウイルス

- を検出する。 ,  
検出, ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。 ,  
ヒューリスティック法, チェックプログラム起動時, マクロウイルス, -, (-),  
<http://pcweb.mycom.co.jp/news/2003/01/30/08.html>, 2003
- [C57] TrendMicro,  
「Scan String、Exact Identification」 ,  
ウイルスコードの中から特徴的な部分を抜き出してウイルスかどうかを判断する。 ,  
検出, ファイルからパターンをスキャンする。 ,  
パターンマッチング法, チェックプログラム起動時, -, -, (-),  
<http://pcweb.mycom.co.jp/news/2003/01/30/08.html>, 2003
- [C58] TrendMicro,  
「ScriptTrap」 ,  
ヒューリスティック検知。ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。VBS や JS、ASP、HTML で記述されたスクリプトウイルスを検出する。 ,  
検出, ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。 ,  
ヒューリスティック法, チェックプログラム起動時, スクリプトウイルス, -, (-),  
<http://pcweb.mycom.co.jp/news/2003/01/30/08.html>, 2003
- [C59] TrendMicro,  
「SoftMice III」 ,  
ウイルスを仮想メモリ上で活動させるためのエミュレータで、システム上に仮想メモリ空間を確保し、その上でウイルスを実行させてその動作を調べる。 ,  
検出, ウイルスを実行させてその動作を調べる。 ,  
ビヘイビア法, チェックプログラム起動時, 多形態型ウイルスなど, -, (+),  
<http://pcweb.mycom.co.jp/news/2003/01/30/08.html>, 2003
- [C60] TrendMicro,  
「WinTrap」 ,  
ヒューリスティック検知。ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。Win32 形式のファイルに感染するウイルスを検出する。 ,  
検出, ウイルスの活動を分析して、その行動をルール化した上でウイルスかどうかを判断する。 ,  
ヒューリスティック法, チェックプログラム起動時, Win32 ウイルス, -, (-),  
<http://pcweb.mycom.co.jp/news/2003/01/30/08.html>, 2003
- [C61] TrendMicro,  
「パターンマッチング方式、ルールベース方式」 ,

ウイルス対策ソフト全般に使われている技術として、パターンマッチング方式とルールベース方式が用いられている。ルールベース方式では主に MacroTrap・スクリプトトラップ・ブートトラップ・ファイルトラップ・メモリトラップがある。、  
、方式の名称のみ。、

、 、 、 、 、

<http://www.trendmicro.com/jp/security/general/tech/overview.htm>, 2003

[C62] TrendMicro,

「ウイルス検出技術についての解説 / ActivePS (プロキシフィルタ技術)」, Java や ActiveX によるインターネットウイルスを検出する技術。インターネット上のパケットをプロキシ上でファイルに組み立てて実行し、検査する方式。、  
検出補助, 直接的な検出手法ではない。、

、 、 、 、 ネットワーク、 、

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C63] TrendMicro,

「ウイルス検出技術についての解説 / AI 型ウイルス解析プログラム」, 従来のウイルス分析は、技術者がさまざまな方法でファイルを検査してウイルスかどうか判断していた。この手順を組み入れて、コンピュータに自動的にウイルスを発見させるために開発されたプログラム。、

検出, 同左。、

ビヘイビア法, チェックプログラム起動時、 、 、 (+),

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C64] TrendMicro,

「ウイルス検出技術についての解説 / VSAPI」,

トレンドマイクロが開発した VSAPI は、ウイルス検索時に発生するボトルネックを解消した最新のウイルス検索エンジン。ウイルスの検索時間を従来比で 200% 向上させることができる。、

検出補助, ウイルス検査時の高速化技術。直接的な検出手法ではない。、

、 、 、 、 、

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C65] TrendMicro,

「ウイルス検出技術についての解説 / Web トラップ方式」,

Web トラップ方式は、プロキシフィルタ技術を応用したウイルス検索技術。インターネットからダウンロードされた Java アプレットや ActiveX コントロールをプロキシ上で解析しウイルスのソースコードが含まれていればリアルタイムに設定された処置をすることができる。、

検出補助, 直接的な検出手法ではない。、

、 、 、 、 Web サーバ、 、

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C66] TrendMicro,

「ウイルス検出技術についての解説 / インテリジェントトラップ」,  
ウイルスは、システムの主要部分への書き込みや、自分自身のコピーを作るなど通常のファイルが行わない不審な動きをする。このような不審な動きをするファイルを見つけるための新しい技術がインテリジェントトラップである。、

検出, 同左。、

ビヘイビア法, チェックプログラム起動時, -, -, (+),

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C67] TrendMicro,

「ウイルス検出技術についての解説 / スキャン方式」,

ウイルスの特徴をデータベース(パターンファイル)に登録しておき、検索ファイルをパターンファイルの情報とマッチングさせることでウイルスを発見する。欠点は、新種のウイルスを発見することができないこと。、

検出, 同左。、

パターンマッチング法, チェックプログラム起動時, -, -, (-),

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C68] TrendMicro,

「ウイルス検出技術についての解説 / ソフトマイス技術」,

ポリモフィック型(ミューテーション型)のウイルスを発見するための技術。メモリ内に確保した専用の領域で検索ファイルを実行し、その動きを分析してウイルスを発見する。パターンマッチング技術と組み合わせることでより効果的なウイルス検索が可能となる。、

検出, 同左。、

ビヘイビア法, チェックプログラム起動時, -, -, (+),

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C69] TrendMicro,

「ウイルス検出技術についての解説 / チェックサム方式」,

ウイルスに感染していない状態で特定の値を計算し、その値をデータベースに格納する。次回、計算したファイルの値が変わっていればウイルスに感染したおそれがあると判断する。弱点は、チェックサムの方式がばれたときにそれをすり抜けるウイルスが作成できること。、

検出, 同左。、

チェックサム法, チェックプログラム起動時, -, -, (+),

<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

[C70] TrendMicro,

「ウイルス検出技術についての解説 / ファジーパターン技術」,

新種ウイルスの多くは既存のソースコードの一部を変更したものとされている。そこで、改変されたソースコードを解析する機能を搭載したのがファジーパターン技術である。、

検出, 同左。 ,  
ヒューリスティック法に近いパターンマッチング法, チェックプログラム起動時, -, (+),  
<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

- [C71] TrendMicro,  
「ウイルス検出技術についての解説 / マクロトラップ方式」,  
マクロウイルスの新種を発見する技術。メモリ上の専用領域でマクロを稼働させ不審な動きをするファイルを検知する。 ,  
検出, 同左。 ,  
ビヘイビア法, チェックプログラム起動時, マクロウイルス, -, (+),  
<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

- [C72] TrendMicro,  
「ウイルス検出技術についての解説 / 圧縮ファイル、エンコードファイル検索」,  
インターネットの普及により、電子メールでのコミュニケーションが一般的になってきた現在、メールに添付された圧縮ファイルにウイルスが潜んでいることがある。また、UUEncode や MIME などに変換されたファイルの検索も必要となる。 ,  
検出補助, 直接的な検出手法ではない。 ,  
,,, ,  
<http://www.zdnet.co.jp/pcweek/archives/980821/980821p1701.html>, 1998

- [C73] Yinrong Huang,  
「Stemming the (Over)flow」 ,  
jmp/call esp 技術によるスタック・バッファ・オーバーフローの悪意ある行いを x86 PC 上で不可能にするため、ret の前のスタック上にブレークポイント(0xCC)を挿入する手法を説明している。 ,  
防止, ワームの侵入後、バッファオーバーフローによる活動の開始をブレークポイント命令で阻止する。検出手法ではないが、応用できるかもしれない。 ,  
,,, ,  
<http://www.phsecurity.com/pdf/BreakpointMechanism.pdf>, 2003

- [C74] アラジンジャパン,  
「eSafe / XploitStopper」 ,  
電子メールに潜む脆弱性を利用する攻撃プログラムを検知する技術。攻撃パターンを予めインプリメントしておくことで新種、未知ウイルスからの脅威を軽減する。 ,  
検出, 脆弱性への攻撃パターンをルール化して、未知ウイルスにも対応している。 ,  
ビヘイビア法, メール送受信時, 電子メール型, -, (+),  
[ftp://ftp.aladdin.co.jp/pub/eSafe/Gateway/4.0/eSafe\\_whitepaperJ.pdf](ftp://ftp.aladdin.co.jp/pub/eSafe/Gateway/4.0/eSafe_whitepaperJ.pdf), 2003

- [C75] ネットセキュリティ / アラジンジャパン,  
「eSafe Gateway for Nitroinspection BridgeMode / 完全透過型リアルタイムウイルス検査(Plug&Play)」 ,

既存のネットワーク構成を全く変更する必要なくスムーズに HTTP のウイルスチェックを導入するアーキテクチャを採用。NIC 自身に独自のドライバをインプリメントする。サーバ側、クライアント側双方の設定をいじる必要がないので導入が比較的容易に実施できる。、

検出, 透過型検査システム。具体的な検出手法は不明。、

-, データ送受信時, -, ネットワーク, -,

<https://www.netsecurity.ne.jp/article/3/9756.html>, 2003

[C76] 京栄社 (技術提供シマンテック),

「ウイルスガードマン / シグネチャベーススキャナ」,、

ブートセクタ、システムメモリ、パーティションテーブル、ファイルなど、感染の可能性のあるあらゆる場所を調べ、スキャナのメモリに蓄えられたウイルスのシグネチャと一致するコード列がないかどうかチェックする。、

検出, ファイルからパターンをスキャンする。、

パターンマッチング法, チェックプログラム起動時, -, -, (-),

[http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki\\_6.html](http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki_6.html), 2002

[C77] 京栄社 / シマンテック,

「ウイルスガードマン / TSR モニタ」,、

バックグラウンドで稼働するウイルス検出用の TSR プログラム。、

検出, 常駐して監視するという技術で、ウイルス検出技術とは直接関係しない。、

-, -, -, -,

[http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki\\_6.html](http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki_6.html), 2002

[C78] 京栄社 / シマンテック,

「ウイルスガードマン / インテリジェントなチェックサム分析と消去技法」,、

デバイスドライバの更新など、ファイルへの書き込みを認識できるアルゴリズムが追加されている。ジェネリック検出に加え、ジェネリック消去機能が含まれている。

ウイルス検出ソフトウェアを特に狙ったウイルスからのセキュリティが向上。、

検出, 改善されたチェックサム法。、

チェックサム法, チェックプログラム起動時, -, -, (+),

[http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki\\_7.html](http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki_7.html), 2002

[C79] 京栄社 / シマンテック,

「ウイルスガードマン / エキスパートシステムによるウイルス分析」,、

システムのソフトウェアに対し数百万回の検査を実行し、コードの流れやコール、実行、およびその他のソフトウェア機能を調べる。これらの各検査の結果に基づいてソフトウェアにいくつかのポイントを割り当て、これらのポイントの得点を基準にウイルスを識別する。、

検出, 対象プログラムを実行せずに検査を行う。、

ヒューリスティック法, チェックプログラム起動時, -, -, (+),

[http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki\\_7.html](http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki_7.html), 2002

- [C80] 京栄社 / シマンテック,  
「ウイルスガードマン / チェックサム比較」,  
システムに感染がないことが分かっているときに記録されたチェックサムと、疑わしいファイルやディスクの現在のチェックサムを比較することで検出する。 ,  
検出, チェックサムによりファイルの変更を検出する。 ,  
チェックサム法, チェックプログラム起動時, 感染を行うウイルス, -, (+),  
[http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki\\_7.html](http://www.kyouei.co.jp/hosting/option/virus/tisiki/tisiki_7.html), 2002
- [C81] 芝浦工業大学 松浦 佐江子、加藤 道子、小島 量,  
「未知のコンピュータ・ウイルス検出プログラムの開発」,  
悪意のある振る舞いパターンを実装したコードを検出する。プログラムが発生するイベントを抽象化したプログラム動作状態の抽象モデルを定義し、その上でウイルスの振る舞いパターンとその検出方法を定義している。 ,  
検出, 構造解析部で検査対象プログラムを逆アセンブルし、構造を静的に解析。シミュレータ部でプログラムの振る舞いを動的に検査。これらのデータから検出モデル生成部で抽象モデルを生成し、検出部がウイルスの振る舞いパターンを検出する。各パターンの組み合わせにより判定を行う。 ,  
ヒューリスティック法 / ビヘイビア法, チェックプログラム起動時, -, -, (+),  
情報処理学会 研究報告「コンピュータセキュリティ」 No.020 - 016, 2002
- [C82] 情報処理振興事業協会, (現：情報処理推進機構)  
「IPAINCS (IPA Integrity Check System)」,  
デジタル署名といわれる暗号技術を用い、新種ウイルスにも強く、偽造などのウイルスの攻撃にも強い感染検知方法。 ,  
検出, あらかじめプログラムに対する署名データ(プログラムをハッシュ関数で圧縮し秘密鍵で暗号化したもの)を生成しておく。感染の有無を検査する場合には、署名生成時と同じハッシュ関数でプログラムを圧縮し、添付された署名を復号した値と比較する。プログラムが改ざんされて(感染して)いればこの値は一致せず、検知できる。 ,  
インテグリティチェック法, チェックプログラム起動時, 感染を行うウイルス, -, (+),  
<http://www.ipa.go.jp/security/integ/ipaincs/aboutipaincs.html>, 1999
- [C83] 東京工業大学 / 脇田建,  
「悪性ソフトウェアとアンチウイルスに関するサーベイ / 一貫性検査システム」,  
インテグリティチェック法は、ファイルに対して過去に保存された特徴量と現在の特徴量を比較することによって変更を検知する。主な特徴量はCRCと暗号化したチェックサム。 ,  
検出, インテグリティチェック法に関する説明。 ,  
インテグリティチェック法, チェックプログラム起動時, -, -, (+),  
<http://www.is.titech.ac.jp/~wakita/surveys/security/virus-survey.pdf>, 2001

- [C84] 徳島大学 三宅 崇之、白石 善明、森井 昌克、  
「仮想サーバを使った未知ウイルス検知システムの提案」、  
ユーザが電子メールを受信する前にメールサーバ内の仮想マシン上でウイルスの可能性のある添付ファイルを受信し、その挙動を監視することで未知ウイルス検知を行う。、  
検出、具体的にはパターンマッチング方式、スタティックヒューリスティック方式、ダイナミックヒューリスティック方式を用いている。、  
主にビヘイビア法、メール送受信時、電子メール型、-, (+),  
情報処理学会 研究報告「コンピュータセキュリティ」 No.018 - 008, 2002
- [C85] 徳島大学 神園 雅紀、白石 善明、森井 昌克、  
「仮想ネットワークを使った未知ウイルス検知システム」、  
仮想マシンと閉じたネットワークを利用して、電子メール型ウイルスの自己増殖活動の検知を行う。、  
検出、仮想ネットワーク監視、監視サーバでのウイルスメール取得、整合性検査の3つにより実現。ウイルスの自己増殖において、ウイルス実行ホストからのネットワークアクセスを検知することによりウイルスか否かを判断する。、  
ビヘイビア法、メール送受信時、電子メール型、仮想マシン環境 / 仮想ネットワーク環境、(+),  
情報処理学会 研究報告「コンピュータセキュリティ」 No.022 - 016, 2003
- [C86] 徳島大学 神園 雅紀、白石 善明、森井 昌克、  
「仮想ネットワークを使った未知ウイルス検知システムの考察 / メモリ常駐型ウイルスへの対応」、  
メモリ常駐型ウイルスを検出するための補助的な技術を提案している。、  
検出補助、メモリ常駐型ウイルスの動作のトリガーとなる部分を強制的に発動させる技術。これにより、仮想実行の際にウイルス部を動作させる。検出には直接関係しない。、  
、  
情報処理学会 コンピュータセキュリティシンポジウム 2003 論文集 pp.109-114, 2003
- [C87] 福島県ハイテクプラザ試験研究報告、  
「未知の攻撃に対応できるウイルス除去ファイアウォールの開発」、  
Linux を搭載した PC 上で Ruby 言語によるプログラム作成を行い、既存のメールサーバの設定を変更することなく設置が可能で、ウイルスの有無の自動判定、新種のウイルスの侵入防止、ウイルスパターンの自己学習といった機能を持つ次世代型ファイアウォール。、  
検出、単純なパターンマッチングではないようだが、詳細は不明。、  
-, メール送受信時、電子メール型、-, (+),  
<http://www.s-iri.pref.shizuoka.jp/tech/elect/el141224.htm>、  
[http://www.fukushima-iri.go.jp/Portable\\_Document\\_Format\\_files/randd/rep\\_rd1](http://www.fukushima-iri.go.jp/Portable_Document_Format_files/randd/rep_rd1)

3.pdf, 2001

## 付録D 侵入検出手法に関する文献

侵入検出手法に関して調査した文献(論文、Web 情報)を以下に示す。

下記のリストは、[文献番号] 発表元名称, 「文献名称」, 文献所在, 発表年、の順に記載している。なお、Web ページに発表年が明記されていないものに関しては、そのページデータの最終更新年を記載している。URL は 2003 年 10 月現在のものである。

書式

[文献番号] 発表元名称,  
「文献名称」,  
文献所在, 発表年

- [D1] Tripwire, <http://www.tripwire.co.jp>
- [D2] Snort, <http://www.snort.org>
- [D3] ラック / 大貫大輔,  
「ネットワーク型 IDS 「Snort」の導入」,  
<http://www.atmarkit.co.jp/flinux/rensai/security10/security10.html>, 2002  
「ネットワーク型 IDS 「Snort」のシグネチャ作成法」,  
<http://www.atmarkit.co.jp/flinux/rensai/security11/security11.html>, 2002
- [D4] Realsecure, <http://www.isskk.co.jp>
- [D5] Dragon, <http://www.enterasys.co.jp>
- [D6] NFR NID, <http://www.nclc.co.jp>
- [D7] ManHunt, <http://www.symantec.com>
- [D8] IntruShield, <http://www.nai.com>
- [D9] Sniper, <http://www.wins21.com>
- [D10] 金岡晃、岡本栄司,  
「IDS 標準化:実装と評価」,  
コンピュータセキュリティシンポジウム 2002(CSS2002)論文集, pp.449-454, 2002
- [D11] 野田健治、勅使河原可海,  
「分散型侵入検知システムにおける相関分析手法の提案」,  
コンピュータセキュリティシンポジウム 2002(CSS2002)論文集, pp.455-460, 2002
- [D12] 山田明、三宅優、田中俊昭,  
「亜種攻撃を検知できる侵入検知システムの提案」,  
コンピュータセキュリティシンポジウム 2003(CSS2003)論文集, pp.659-664, 2003
- [D13] 安藤類央、武藤佳恭,  
「二段階直交定量検出法とネットワーク動的防御システムへの適用」,  
コンピュータセキュリティシンポジウム 2003(CSS2003)論文集, pp.575-580, 2003
- [D14] 加藤岳久、清水歩、池田竜朗、才所敏明,  
「出所不明の packets 流出を許さないセキュアなネットワークの研究開発」,

- コンピュータセキュリティシンポジウム 2002(CSS2002)論文集, pp.239-244, 2002
- [D15] 竹内大輔、千石靖、服部進実,  
「仮想マシンを用いた実行形式型ウィルスの検出」,  
コンピュータセキュリティシンポジウム 2001(CSS2001)論文集, pp.179-184, 2001
- [D16] 伊吹賢一、千石靖、服部進実,  
「ウィルスコードの自動解析を行う学習型ウィルス検出システムの構築」,  
コンピュータセキュリティシンポジウム 2001(CSS2001)論文集, pp.185-190, 2001
- [D17] 竹森敬祐、力武健次、清本晋作、田中俊昭、中尾康二,  
「Intrusion Trap System の実装および評価」,  
コンピュータセキュリティシンポジウム 2001(CSS2001)論文集, pp.415-420, 2001
- [D18] 宮本大輔、久保聡之、大江将史、門林雄基,  
「侵入監視のための Honeypot の実装と評価」,  
コンピュータセキュリティシンポジウム 2001(CSS2001)論文集, pp.421-427, 2001
- [D19] 金岡晃、岡本栄司,  
「ニューラルネットワークを用いたデータマイニングによるリアルタイムネットワーク異常検出について」,  
暗号と情報セキュリティシンポジウム 2002(SCIS2002)予稿集 Vol.II, pp.645-649, 2002
- [D20] 馬場達也、鴨田浩明、小久保勝敏、松田栄之,  
「プロトコル仕様及びポリシー情報を利用した不正アクセス検知システムの実装と評価」,  
コンピュータセキュリティシンポジウム 2001(CSS2001)論文集, pp.173-178, 2001
- [D21] 大山恵弘、王維、加藤和彦,  
「静的解析に基づく侵入検知システムの最適化」,  
第 6 回プログラミングおよび応用のシステムに関するワークショップ(SPA2003),  
ソフトウェアシステム研究会, 2003
- [D22] 井上直、女部田武史、浅香緑,  
「ネットワーク侵入検出システム IDA の研究開発」,  
第 19 回 IPA 技術発表会, 2000
- [D23] 大塚丈司、白石善明、森井昌克,  
「不正アクセスのセンター集中管理方式」,  
コンピュータセキュリティシンポジウム 2002(CSS2002)論文集, pp.143-148, 2002
- [D24] 平石広典、溝口文雄,  
「不正侵入トレース用ブラウザの設計」,  
コンピュータセキュリティシンポジウム 2001(CSS2001)論文集, pp.161-165, 2001
- [D25] 高田哲司、小池英樹,  
「見えログ:情報視覚化とテキストマイニングを用いたログ情報ブラウザ」,  
情報処理学会論文誌, Vol.41, No.12, 2000

- [D26] 小泉芳、小池英樹、高田哲司、安村通晃、石井威望,  
「情報エントロピーを用いたネットワーク侵入検知システムログ解析手法の提案」,  
コンピュータセキュリティシンポジウム 2003(CSS2003)論文集, pp.653-658, 2003
- [D27] 内山一雄,  
「自律型セキュリティ管理システムによる不正アクセス対処の効果について」,  
コンピュータセキュリティシンポジウム 2003(CSS2003)論文集, pp.647-652, 2003
- [D28] 鴨田浩明、馬場達也、小久保勝敏、松田栄之、矢口博之,  
「ニューラルネットワークを利用した不正アクセス被害予測方式」,  
コンピュータセキュリティシンポジウム 2002(CSS2002)論文集, pp.131-136, 2002
- [D29] 栗林利光、白石善明、森井昌克,  
「不正アクセスに対する被害予測システム」,  
コンピュータセキュリティシンポジウム 2002(CSS2002)論文集, pp.137-142, 2002
- [D30] 鈴木雅貴、榎本圭、赤井健一郎、井上大介、松本勉,  
「目印付きレスポンスによる侵入者追跡」,  
暗号と情報セキュリティシンポジウム 2001(SCIS2001)予稿集 Vol.I, pp183-188,  
2001