



ユーザーズマニュアル



Intego VirusBarrier X for Macintosh

(c) 2000 – 2002 Intego, Inc. All Rights Reserved

Intego, Inc.

www.intego.com

本書は、Intego VirusBarrier X for Macintosh のユーザを対象に作成されています。本書および本書で説明している Intego VirusBarrier X ソフトウェアは著作権法により保護されており、無断転載は禁止されています。また、ソフトウェアライセンスで許可されている場合、または Intego, Inc. の書面による許可がある場合を除き、本書および Intego VirusBarrier X の複製は禁じられています。

本ソフトウェアは、Intego およびそのサプライヤの所有物であり、その構造、機構、およびコードは Intego およびそのサプライヤの貴重な企業秘密です。本ソフトウェアは、米国著作権法および国際条約の規定により保護されています。

Intego VirusBarrier X では、Erik Dörnenburg により記述された EDCCommon および EDInternet フレームワークが使用されています。



目次

1 - Intego VirusBarrier X について.....	6
Intego VirusBarrier X とは	7
Intego VirusBarrier X の機能.....	9
本書の利用について	11
2 - コンピュータウイルスとは	12
なぜコンピュータの保護が必要なのか.....	13
コンピュータウイルスとは	14
誰がウイルスを作るのか	15
コンピュータウイルスはどのように働くのか	16
ウイルスの種類.....	18
システムウイルス.....	19
ファイルウイルス.....	21
デマウイルス.....	25
ウイルスはどのように流行するのか	26
ウイルスからコンピュータを保護するには	27
3 - インストール.....	30
システム要件.....	31
Intego VirusBarrier X をインストールする.....	31
Intego VirusBarrier X を登録する.....	36
試用版として Intego VirusBarrier X を使用する.....	37



4 - クイックスタート	38
Intego VirusBarrier X の既定モード.....	39
Intego VirusBarrier X のインターフェース.....	40
手動スキャンを実行する	41
NetUpdate の設定	44
ドラッグ・アンド・ドロップ操作でスキャンを実行する.....	47
Intego VirusBarrier X を Dock で使用する	47
5 - Intego VirusBarrier X の機能	49
ウイルススキャン	50
手動スキャン	50
ドラッグ・アンド・ドロップ操作でスキャンを実行する	59
スキャン結果	59
警告	64
6 - Intego VirusBarrier X の設定	65
環境設定	66
警告オプション	72
NetUpdate.....	74
ウイルス事典	75
Intego VirusBarrier X について	76



7 - 診断.....	78
ウイルスに感染したと思ったら.....	79
基本的な予防策.....	80
8 - テクニカルサポート.....	82
9 - 付録.....	84
用語集.....	85
ウイルス事典.....	88



1 - Intego VirusBarrier X について



Intego VirusBarrier X とは

Intego VirusBarrier X は、Macintosh コンピュータ用のシンプルかつ高速で、手間いらずなアンチウイルスセキュリティソリューションです。販売元は、NetBarrier パーソナルセキュリティソフトが好評の Intego です。このソフトでは、フロッピーディスクや CD-ROM、リムーバブルメディアを通じて、またインターネットやその他のネットワークからのダウンロードなど、ウイルスに感染したファイルやアプリケーションから入ってくるすべての種類のウイルスを徹底的に排除します。

Intego VirusBarrier X は、お使いのコンピュータで読み取りおよび書き込みしたすべてのファイルを常にチェックし、アプリケーションや他のファイルにおけるウイルスの活動を示す疑わしい兆候がないかどうかを監視して、コンピュータをウイルスから守ります。Intego VirusBarrier X をインストールすることで、コンピュータがどのようなウイルスからも守られているという安心感を得ることができます。

Intego VirusBarrier X は、バックグラウンドで動作し、ウイルスを検索しながらコンピュータの活動をすべてチェックするソフトウェアです。このソフトは、既知のすべての Macintosh ウイルスの特性を把握しています。新種のウイルスが発見されると、Intego のアンチウイルス SWAT チームは最新のウイルス定義ファイルを用意します。ユーザは、Intego VirusBarrier X の NetUpdate 機能を使って自動的にそのファイルをダウンロードすることができます。

Intego VirusBarrier X を購入されたお客様は、購入日より 1 年間、これらのウイルス定義ファイルを無償でご利用いただけます。それ以降は、新たに Intego と契約することをご利用いただけるようになります。契約は、Intego Web サイト (www.intego.com) または NetUpdate から行うことができます。



第 1 章- Intego VirusBarrier X について

Intego VirusBarrier X は、いくつかのコンセプトに基づいて設計されました。第一のコンセプトは、アンチウイルスソフトとは、インストールと設定を行った後、ウイルスが検出されない限りユーザの手間を取らせてはいけないものであるという考えです。Intego VirusBarrier X の哲学は、“シンプル”、“高速”、“手間いらず” の 3 つの言葉で表すことができます。

シンプル

Intego VirusBarrier X は、もっとも単純で使いやすいアンチウイルスプログラムです。インストール後、バックグラウンドで動作し、コンピュータを監視し、コンピュータ上のファイルを効率的かつ静かにチェックします。

高速

Intego VirusBarrier X は、高速かつ効率的に動作します。このソフトウェアによってコンピュータの処理速度が遅くなることはありません。また、ユーザの手を煩わせることもありません。Intego VirusBarrier X は、ユーザが書き込んだり、使ったり、開いたりしたファイルをその都度チェックし、ウイルスに感染していないかどうかを確かめます。

手間いらず

Intego VirusBarrier X は、ユーザの手を煩わせません。ユーザが何らかのプログラムをインストールする度に“疑わしい”活動について一つ一つ確認メッセージを表示することも、また際限なく“誤認アラーム”を鳴らすこともありません。VirusBarrier X のインストール後、ウイルスを検出して警告が発生しない限り、ユーザはこのプログラムの存在にすら気付かないでしょう。また、新しいソフトウェアをインストールする際、そのソフトのインストーラやマニュアルにどのような指示があろうと、



Intego VirusBarrier X の機能を停止する必要はありません。Intego VirusBarrier X がバックグラウンドで絶えず動作し、コンピュータをウイルスから守っているので何も心配はいりません。

Intego VirusBarrier X の機能

ウイルススキャン

Intego VirusBarrier X の動作方法は複数あります。コンピュータへのウイルスの侵入を常時監視させることもできますが、マニュアルモードで使用して、特定のディスクやボリューム、ネットワークをスキャンするようにユーザが指示することもできます。

自動修復

Intego VirusBarrier X を自動モードで実行している場合、感染ファイルが検出されると、可能な限りウイルスを駆除してファイルを修復します。修復できない場合は、ファイルが破損している旨をユーザに知らせます。自動モードでは、ユーザは Intego VirusBarrier X の存在を忘れてしまっても構いません。ウイルスや感染の疑いのあるファイルが報告されたときに思い出してください。

手動スキャン

Intego VirusBarrier X では、ファイルのスキャンを手作業で行うこともできます。インストール直後に実行して、コンピュータが安全なことを確認してください。また、ユーザは、ディスクやボリュームに対していつでも手動スキャンを実行し、ウイルスに感染していないことを確かめることができます。



ターボモード

ターボモードを使うと、スキャンを短時間で実行することができます。Intego VirusBarrier X では、初回スキャン時にチェックしたファイルがすべて記憶されます。Intego VirusBarrier X は、それらのファイルに対して、更新されたときだけ再びスキャンを実行します。これにより、スキャン速度が 5 ～ 40 倍速くなります。

スキャンログ

Intego VirusBarrier X には、検出したウイルスと感染の疑いのあるファイルの記録がすべて表示されます。このログを使って、感染、修復または破損したファイルやアプリケーションを特定することができます。

Dock

Intego VirusBarrier X を Dock に置いておくと、アプリケーションを開かなくても、ファイルやフォルダを Intego VirusBarrier X アイコンにドラッグするだけで、そのファイルやフォルダのウイルスチェックを行うことができます。

NetUpdate

Intego VirusBarrier X には、Intego 独自の NetUpdate プログラムが搭載されています。NetUpdate を使うと、プログラムの更新状況や新しいウイルス定義ファイルを自動または手動で確認することができます。自動アップデート機能を使用すると、アップデートの頻度を設定することができます。この場合、NetUpdate は、設定した曜日と時間に毎週アップデート状況をチェックします。プログラムを手動で更新する場合、クリック操作一つで Intego サーバに接続し、アップデート状況を確認することができます。



ウイルス警告

Intego VirusBarrier X では、バックグラウンドでウイルスチェックを実行している間に、ウイルスが検出されたことを知らせる警告の方法も指定できます。警告画面を表示することも、警告音を鳴らすことも、または指定の e-mail アドレスにメールで知らせることもできます。この機能は、Intego VirusBarrier X をネットワークとつながっているコンピュータで使用している場合、およびネットワーク管理者や、コンピュータから離れた場所にいるコンピュータ所有者に知らせる場合に便利です。

本書の利用について

本書では、Intego VirusBarrier X をインストール、使用および更新する方法について説明し、また Macintosh ウイルスに関する情報を提供します。さらに本書には、ウイルス関連の用語集もあります。

まず、第 2 章を読み、コンピュータウイルスについて理解してください。次に、第 3 章の「インストール」に進みます。その後、第 5 章「Intego VirusBarrier X の機能」をお読みください。ウイルスについてさらに詳しい情報が必要な方は、第 9 章の「ウイルス事典」と「用語集」をご覧ください。

コンピュータに異常があり、ウイルスに感染している可能性がある場合は、第 7 章「診断」をお読みください。この章では、コンピュータの問題に関するトラブルシューティングと、本当にウイルスに感染しているかどうかを確かめる方法が紹介されています。また、感染した可能性のあるファイルを Intego のウイルスモニタリングセンターに送って、検査する方法も記載されています。



2 - コンピュータウイルスとは



なぜコンピュータの保護が必要なのか

皆様のコンピュータには、大切な情報やファイルが含まれています。仕事で使用する情報やファイルを失った場合、どれほどの時間とコストがかかるのかご存知でしょう。コンピュータを家庭だけで使っている場合でも、失うと困るファイルがあります。その上、大切なファイルを失っただけでなく、ウイルスによってすべてのファイルが消されてしまうと、システムやソフトウェアをすべて再インストールするのに膨大な時間がかかる可能性があります。

アンチウイルスプログラムは、保険契約のようなものです。ご自分のコンピュータがウイルスに感染することはないと思われるかもしれませんが、しかし、感染してしまった場合は最悪です。Intego VirusBarrier X は、すべての種類のウイルスに対応する保険です。コンピュータを監視し、安心を提供します。

ウイルスの脅威は現実のものになっています。毎日発見されるウイルスの数は増加の一途を辿っています。Macintosh が、Windows よりも比較的ウイルスを受けにくいのは事実です。それでもなお、既存のウイルスや新種のウイルスがコンピュータに侵入し、ファイルが壊される危険性があります。



コンピュータウイルスとは

コンピュータユーザにとって、自分のコンピュータがウイルスに感染しているかもしれないと言われることほど怖いものはありません。病気が判明したときと同じくらいのショックがあります。コンピュータユーザなら誰でも、ウイルスが引き起こす悲惨な話を耳にしたことがあるでしょう。中には喜ぶ人もいますが、自分のコンピュータでウイルスが見つかったときに無関心でいられるユーザはいません。

毎日 e-mail でファイルをやりとりするデータ通信の時代において、これはとても深刻な問題です。コンピュータウイルスは、インフルエンザウイルスと同じくらい速く蔓延します。ところで、実際にコンピュータウイルスとは何でしょうか。どのように活動するのでしょうか。また、なぜそんなにも危険なのでしょう。

“ウイルス”という言葉が初めて使われたのは、自己繁殖コンピュータプログラムが“ユーザ環境”に出回った 1980 年代初頭です。

ウイルスとは単に、ファイルやアプリケーションに加えられたわずかな実行可能コードのことです。ウイルスは空気感染しません。フロッピーディスクや CD-ROM、インターネットを通じて送られたファイルなど、ウイルスを運ぶ媒体が必要です。人間の体を蝕むウイルスと同じように、コンピュータウイルスも宿主に感染した後、他のファイルやアプリケーションに自らをコピーして繁殖を試みます。その後、ウイルスは自分のコピーを作って、新たな宿主を攻撃します。これが繰り返されるのです。

基本的にウイルスは、小さなコンピュータプログラムです。小さいほど都合がよく、ファイルやアプリケーションに容易に侵入して、監視の目から逃れます。ウイルスが作られる目的は一つです。それは、



第 2 章 - コンピュータウイルスとは

自己繁殖して他のコンピュータに転移することです。ウイルスの中には危害を与えないものや、画面に特定の文字を表示するだけのものもありますが、ウイルスの多くはコンピュータやファイルに実害をもたらします。また、悪意を持たずに作られた有名なウイルスもありますが、ほとんどの場合、ファイルの破壊や、他のコンピュータへの繁殖という目的を持って作られています。

家庭用コンピュータから会社のネットワークまで、ウイルス対策を行わない限り、どのようなコンピュータにもウイルスが感染する可能性があります。講じられる最善のウイルス対策は、Intego VirusBarrier X を使用すること、そして常に最新の状態で使用することです。

誰がウイルスを作るのか

噂はあるにしても、コンピュータウイルスはアンチウイルスソフトウェアを売るために企業が作っているわけではありません。アンチウイルスソフトウェア会社には、確かにウイルスの進歩に遅れずについていけるほどの技術がありますが、自らウイルスを増やすようなことはありません。

ウイルスを誰が作っているのか、まだ正確にはわかっていません。ストレスの溜まった少年・少女かもしれませんし、ベテランのハッカーかもしれません。ウイルスを作って逮捕された人もいますが、それは氷山の一角です。逮捕されたウイルス作成者は、自ら作ったウイルスを受け取った人から注目されたかたのかもしれません。なぜなら発見された多くのウイルスの中から、作成者の名前が見つかったのです。そうでなければ、自分で作った単純なプログラムでパニックが起きるのを見て楽しんでる野蛮な人が作っているのかもしれません。さらに、自分のウイルスがどこまで繁殖し、どれ程多くのコンピュータに広まるのか実験したがっている人もいます。それとも、ウイルスは、あるウイルス作成者の言葉どおり“電子版落書き”にすぎないのでしょうか。



第 2 章 - コンピュータウイルスとは

中には、“悪意”のないウイルスもありますが、それでもやはり結果的に数多くの問題を引き起こします。その一例が MacMag ウイルスです。このウイルスは、世界平和に関するメッセージを広めようとしたものです。詳しくは、第 9 章で説明します。

インターネットの登場以来、ウイルスに対する現実的な恐怖は、孤独な一人の人間が単に関心を集めるために広めたものでは済まされなくなりました。明らかに悪意のある人がウイルスを使って、経済に大ダメージを与えようとする場合もあります。ウイルスの大流行により、企業が攻撃にあつと、生産性の大幅低下やダウンタイムでどれほどのコストがかかるのかが明らかになりました。LoveBug ウイルスの流行はその例です。このような事態を回避するために、可能な限りの対策を取って自分を保護しなければなりません。

コンピュータウイルスはどのように働くのか

ほとんどのコンピュータユーザは、“コンピュータウイルス”という言葉で、あらゆる種類の“マルウェア（悪意のこもったソフト）”を意味するものと捉えています。ただし、すべてが実際のウイルスであるとは限りません。たとえば、トロイの木馬とワームの動作方法は異なり、ウイルスのように必ずコピー活動を行うわけではありません。しかし、ほとんどのユーザはそれらをウイルスの一つと捉える傾向にあります。これらのプログラムも悪質で、コンピュータやファイルに深刻な被害をもたらす可能性はありますが、ウイルスとは機能面で異なります。

厳密に言うと、ウイルスとは小さなコンピュータコード群か、またはターゲットにしているコンピュータ上で実行するプログラミング命令を指します。したがって、DOS や Windows への攻撃を目的に作成されたウイルスは、Macintosh コンピュータには無害です。またその逆も同様です。（ただし、



第 2 章 - コンピュータウイルスとは

いずれかのオペレーティングシステムを Macintosh 上のエミュレータで実行している場合、エミュレートしたシステムのウイルスへの脆弱性を考慮する必要があります。)

ウイルスは、コンピュータ上で 2 つの活動を行います。まず、プログラムどおりの破壊活動を行うためにコードを実行しようとしています。次に、コードをファイルやアプリケーション、ディスクまたはネットワーク上のボリュームにウイルス自らコピーして繁殖しようとしています。ここで、架空のウイルスを例に挙げて、Macintosh での活動を見てみましょう。(実際に、この例では、わかりやすくするためにトロイの木馬の活動を取り上げます。)

あなたはインターネットを通じて、友人や顧客からウイルスに感染したプログラムを受け取りました。知らない人から来た e-mail の添付ファイルは開かないように用心していましたが、このメールは信頼している人から来たため、あなたは添付ファイルを開いてしまいます。仮に、そのプログラムを動画カードとしましょう。ファイルをダブルクリックすると、プログラムが実行し始めます。動画を見させている間に、そのプログラムはウイルスコードを実行し、システムファイルを書き換えています。悪質なコードをあなたのシステムにコピーするだけでなく、あなたの会社のローカルネットワークを探して、他のシステムファイルにも繁殖します。動画が終わると、あなたはプログラムを閉じます。この時点では何も起こりません。しかし、ウイルスコードは、コンピュータを再起動したときに実行するようにプログラミングされているのです。

翌朝、あなたが会社に行き、コンピュータの電源を入れると、いつもより起動に時間がかかることに気付きます。コンピュータが起動すると、いつもよりも動作のスピードが遅いように感じます。さらに、昼までに終わらせなければならない急ぎの報告書を開こうとすると、



第 2 章 - コンピュータウイルスとは

そのファイルがなくなっています。ハードディスクを調べると、数十、数百ものファイルがなくなっています。昨日コンピュータのバックアップを取り忘れたため、ファイルのコピーはありません。

一方で、あなたは昨日の動画カードを他の友人に送っていました。しかし、ファイルがなくなったことと動画カードが関係しているとは思っていません。数時間後、友人の一人から電話が入ります。その友人も動画カードが原因でコンピュータが壊れてしまったのです。

ご覧のとおり、事態は非常に深刻です。被害は、自分だけでなく知人にも及びます。今日、ウイルスの最大の問題は、ファイルの交換をインターネットを通じて行っており、ファイルをフロッピーディスクで送っていたときよりも感染速度が高まっていることにあります。Intego VirusBarrier X で自分を保護することで、友人を保護することもできるのです。

コンピュータウイルスは 24 時間以内に世界中を駆け巡ります。特定のソフトウェアを使用している Windows コンピュータを攻撃する Melissa や LoveBug ウイルスが話題になりましたが、同じようなウイルスが Macintosh コンピュータを標的することも十分に考えられるのです。

ウイルスの種類

ウイルスの攻撃対象によって、ウイルスを 2 つの種類に分類することができます。1 つ目の種類は“システムウイルス”と呼ばれ、システムファイルや機能拡張ファイル、デスクトップファイルなどを攻撃します。もう 1 つは“ファイルウイルス”と呼ばれ、アプリケーションやデータファイル、コントロールパネル、機能拡張ファイルに感染します。



システムウイルス

システムウイルスは危険度のもっとも高いウイルスで、オペレーティングシステム自体を破壊する可能性があります。本書では、トロイの木馬とワームも システムウイルスに分類します。これら 2 つは、システムウイルスと技術的には異なりますが、ファイルウイルスよりも世界レベルで広まる傾向にあります。

ウイルス

コンピュータウイルスは、寄生虫のように活動する小さなプログラムです。ホストファイルやプログラムに住み着き、ファイルやアプリケーションに自己再生して他のコンピュータに繁殖します。元々病気に使われていた言葉をそのままコンピュータの“ウイルス”に使っているのは興味深いことです。どちらのウイルスも同じような働きを持っています。

システムを攻撃するウイルスは、もっとも破壊的です。システムウイルスの被害を受けると、システムをすべてインストールし直さなければならない場合があります。また、場合によっては、ハードドライブを再フォーマットしたり、バックアップが感染されていないかどうか、すべてチェックしなければなりません。

CDEF や WDEF ウイルスなど、一部のウイルスは Macintosh のデスクトップファイル (Mac OS 9 以前) のみに感染します。これらのファイルは不可視で、アイコンと、ファイルやアプリケーションの種類を関連付けています。Macintosh では、ディスクやボリュームをマウントしたときに、まずそれらの



第 2 章 - コンピュータウイルスとは

デスクトップファイルを読み取ります。したがって、他のファイルに感染しないこのようなウイルスは極めて速く広がります。

SevenDust ウイルスなど、その他のシステムウイルスは、特定の日にシステムファイルやコントロールパネル、アプリケーションに感染し、起動ディスク上の非アプリケーションファイルをすべて削除します。

このように、すぐに感染するウイルスもあれば、特定の時間に活動を始めるように設定されているウイルスもあります。中には、単独では他のディスクやボリュームに繁殖できないものもありますが、システムウイルスは一様に破壊力を持っています。

トロイの木馬

“トロイの木馬”という名前は、数百年前、ギリシャ軍とトロイ軍が戦った戦争中のエピソードに由来します。トロイの木馬は、木をくり抜いて作った巨大な木馬で、ギリシャ軍からトロイ軍にプレゼントされたものでした。その後ギリシャ軍は撤退し、終戦したと言われています。トロイ軍の中には懐疑的な者もいましたが、木馬はトロイの要塞の中に運ばれました。その夜、ギリシャ兵士が木馬の中から現われ、トロイの街の門を開き、大勢のギリシャ兵士たちが街の中に突入してきたのです。

トロイ人は、贈り物を決して開けないように忠告されてなかったのです。私たちが心配しているトロイの木馬は、悪意のない、特定の動作を実行するためのプログラムのように見えます。しかし、実際は悪質なコードやウイルスが含まれています。多くの場合、トロイの木馬は他のウイルスよりも



第 2 章 - コンピュータウイルスとは

高い危険性をはらんでいます。たとえば、ChinaTalk はシステム機能拡張ファイルのように見えますが、フォルダを削除します。また、有名な MacMag Trojan は、システムファイルに感染します。

ワーム

ワームは、コンピュータのウイルスプログラムの中でもっとも古いものの一つです。また、ファイルやアプリケーションに入り込まずに繁殖するため、見つけるのが非常に困難です。最近深刻化している Macintosh のワームは AutoStart ワームと呼ばれるもので、不可視ファイルを作成してデータやファイルを破壊します。

ワームはシステムの機能を使って広がります。たとえば、AutoStart ワームは Mac OS の Autoplay 機能を利用し、感染した CD-ROM から繁殖します。このワームは、不可視の機能拡張ファイルを作成し、コンピュータを再起動するたびに実行します。

ファイルウイルス

ファイルウイルスは、アプリケーションではなくデータファイルに自己繁殖する点でシステムウイルスと異なります。また、侵入したウイルスは、特定のプログラムを使ってコンピュータを破壊します。ファイルウイルスの最近の例として、Windows をターゲットにした Melissa や LoveBug ウイルスなどが挙げられます。これらのウイルスは添付ファイルに侵入し、添付ファイルを開くと、Windows に搭載されている Microsoft アプリケーション用に作られた特定の機能を実行します。一見トロイの木



馬のように見えます。しかし、トロイの木馬は特定の動作を実行するのに対し、これらのファイルウイルスはファイルに埋め込まれるコードであるという点で異なります。

マクロウイルス

通常、ファイルウイルスはマクロウイルスです。今日、この種のウイルスは、Macintosh ユーザに多大な脅威をもたらしています。

最初に発見された Concept マクロウイルスは、Microsoft Word ファイルを攻撃するものでした。その後、あるウイルス作成者が Word の普及率に強力な破壊力を見出し、変種を作りました。後に、Microsoft Excel を利用したマクロウイルスも作られるようになりました。初めてマクロウイルスが発見されてからたったの 5 年間で、数千のマクロウイルスが見つかっています。

マクロウイルスの真の危険性は、初のクロスプラットフォームウイルスである点にあります。長年、Macintosh コンピュータを狙ったウイルスは数十しか見つかっていなかったため、何千ものウイルスに狙われている Windows よりも比較的安全だと言われてきました。しかし現在、マクロウイルスが普及したことで、危険性は高まっています。

多くのプログラムには、マクロコマンドを作成する機能が搭載されています。それらの単純なプログラムでは、AppleWorks などのアプリケーションの内部機能を使って、よく使われるコマンドシーケンスを“記録”および“再生”します。また、Nisus Writer などのアプリケーションには、メニューコマンドとプログラミング言語の両方を備えた、もっと強力なマクロ言語が含まれています。Microsoft



第 2 章 - コンピュータウイルスとは

Word や Excel などのプログラムは、Basic プログラミング言語に似た、Visual Basic のマクロ機能を基礎としています。

マクロウイルス作成者が Microsoft のプログラムを狙う理由の一つは、それらのアプリケーションでは、マクロをデータファイルに組み込むことができるためです。かつて、ウイルスはアプリケーションを通じて入ってくるものでした。ウイルスが活動するにはアプリケーションを実行する必要があり、アプリケーションだけがウイルスを活動させることができたのです。しかし、Microsoft Visual Basic の登場で状況は変わりました。マクロをテンプレートから実行するか、またはマクロをデータファイルに追加して実行することができるのです。当初、ユーザはこの技術に驚きました。ワープロや計算ソフトのファイルを開く際、“実行” するものは何もないと思ったからです。しかし実際は、これらのファイルには“プログラム” が含まれており、ユーザが予想もしてない動作を行うのです。

マクロ言語にファイルを書き換える能力があれば、マクロウイルスは、同じアプリケーションで使用する別のファイルに自己再生できるようになります。つまり、他のファイルを開いたり、ファイルを新規作成したり、ファイルを他者に渡すとき、ウイルスが広まってしまうのです。

Microsoft Word を狙ったほとんどのマクロウイルスでは、AutoOpen、AutoClose、AutoExec および AutoExit などのコマンドを使用します。これらのコマンドは、ファイルに特定のイベントが発生したときに実行され、ファイルで作業を行うとこれら 4 つのイベントが必ず実行されます。たとえば、特定のメニューコマンドを選択したときに自己再生するようにマクロがプログラミングされている場合、繁殖の可能性はそれほど高くありません。

マクロウイルスの多くは、ユーザがファイルを開いたときに実行し、開いているテンプレートに自己繁殖します。このテンプレートはユーザ自身が開くものではありません。バックグラウンドでいつも開い



第 2 章 - コンピュータウイルスとは

ています。このテンプレートには、ツールバーや後から追加した正式なマクロなど、ユーザ独自の情報が含まれています。

Microsoft Word を攻撃するもっとも一般的なマクロウイルスは、使用中のテンプレートに自らをコピーし、特定のメニューアイテムを変更するものです。したがって、ユーザはテンプレートを編集することも、ファイルの種類を変更する（テンプレート自体に見せかけるためにアイコンを変更する）こともできなくなります。その後、マクロウイルスは、破壊したテンプレートからユーザが作成または開いた新しいファイルに自己繁殖します。このウイルスをすぐに発見できれば、使用中のテンプレートファイルと感染ファイルを削除して、ウイルスを取り除くことができます。

他にも、もっと危険なマクロウイルスがあります。それらのマクロウイルスは、ファイルを破壊または削除したり、特定のアプリケーション機能を隠したりします。その上、それらはクロスプラットフォームウイルスのため、Macintosh コンピュータと Windows 搭載コンピュータの両方に被害をもたらす可能性があります。

マクロ言語は、非常に便利で強力なツールです。マクロがすべてウイルスなわけではありません。Microsoft Word には、開こうとしている文書にマクロが含まれている場合に警告を表示する機能があります。しかし、これによってマクロ機能の利便性が損なわれています。問題なのは、マクロが、単独のマクロファイル（Nisus Writer などの一部のアプリケーションではこれを採用しています）ではなく、データファイルに格納される点です。ユーザは、簡単にマクロをやり取りすることができます。また、ファイルにデータのみを使用すれば確実です。残念なことに、このような対策は、マクロに対する過剰な不安をユーザに与え、機能拡張のためにマクロを使用する機会をユーザから奪っています。



第 2 章 - コンピュータウイルスとは

Intego VirusBarrier X は、既知の Word および Excel マクロウイルスをすべて検出し、新しいマクロウイルスが発見されると常にアップデートされます。

デマウイルス

e-mail やニュースグループで、存在しないコンピュータウイルスを警告するデマウイルスが問題になっています。それ自体はウイルスではありませんが、ウイルスのように増殖します。つまり、心配したユーザがそのメッセージを信じて、友人や同僚に転送してしまい、架空のウイルスに対する不安が広がってしまうのです。

もっとも流行したデマウイルスは Good Times です。e-mail に Good Times という件名を使用し、ウイルスが含まれているように装います。それがデマウイルスだと気付けばそれ以上広まらないのですが、Good Times “ウイルス” は 1994 年に初めて発見されて以来、今でも姿を消しません。これを真似したデマウイルスメッセージは、インターネット中を駆け巡っています。誰でも一度は目にしたことがあるでしょう。

このようなデマウイルスは、インターネットユーザのコンピュータ知識の欠如につけこんだものです。実際、デマウイルスの内容は、とても深刻に見え、大手コンピュータ会社からのメッセージのように装っている場合もあります。しかし、それらはすべて冗談です。無論、まったくおもしろくありませんが。



第 2 章 - コンピュータウイルスとは

このようなメッセージを受け取って、本当のウイルス情報ではないかと心配になったら、会社であればまずシステム管理者に相談して、それが本物の情報であるかどうかを確認してもらいましょう。自宅であれば、Intego のホームページ (www.intego.com) で確認することができます。注意が必要な新しいウイルスが見つかったら、Intego はホームページにできるだけ早く情報を公開するようにしています。Intego のウイルスモニタリングセンターは年中無休 24 時間体制で待機し、新しいウイルスの一次兆候が見つかったらすぐに対応しています。

新しいウイルスに感染した疑いがある場合は、第 7 章「診断」をお読みください。ここには、コンピュータの診断方法や、Intego のウイルスモニタリングセンターへの連絡先があります。

ウイルスはどのように流行するのか

ウイルスは、いくつかの単純な手段で蔓延します。ウイルスは、ファイルまたはリムーバブルメディアを通じて広がります。Macintosh 用の CD-ROM、Zip カートリッジなどのメディアには、デスクトップファイルという不可視ファイルが含まれています。これらのファイルには、システム関連のファイルアイコンやアプリケーションに関する情報があります。デスクトップファイルに感染するウイルスは、コンピュータでそれらのリムーバブルメディアを読み取ったときに広まります。それは、Macintosh では、ディスクやボリュームをマウントしたときに、まずそれらのデスクトップファイルを読み取るためです。Intego VirusBarrier X を使うと、リムーバブルメディア内のすべてのデスクトップファイルをスキャンして、ウイルスの侵入を防ぐことができます。また、Intego VirusBarrier X によってデスクトップファイルでウイルスが見つかったら、コンピュータがファイルを読み込む前にウイルスを駆除します。



第 2 章 - コンピュータウイルスとは

ウイルスは、感染ファイルを通じて広がることもあります。ファイルは、CD-ROM やその他のリムーバブルメディアで渡す場合も、またインターネットからダウンロードする場合もあるでしょう。また、e-mail の添付ファイルとして送られることもあります。感染ファイルを開いたり、読み込んだりしなければウイルスが活動することはありません。また、単にアプリケーションをコピーしただけではウイルスに感染することはありませんが、アプリケーションを起動すると感染する可能性があります。データファイルの場合も同様です。マクロウイルスを含んだファイルを受信した場合、そのファイルを開かなければ心配はいりません。Intego VirusBarrier X は、ユーザがコンピュータ上のファイルを編集したり、使用したり、開いたりした場合、そのファイルをスキャンしてコンピュータをウイルスから守ります。ユーザがファイルを操作するとすぐに、そのファイルはスキャンされます。そして、Intego VirusBarrier X によってウイルスが検出された場合、ウイルスを駆除するか、またウイルスを駆除できない場合はユーザに通知します。

ウイルスからコンピュータを保護するには

コンピュータウイルスからコンピュータを守る方法はいくつかあります。1 つ目は、もっとも重要なことですが、Intego VirusBarrier X を使って常にコンピュータを監視し、ウイルスチェックを自動的に行う方法です。Intego VirusBarrier X には、Macintosh 用の最高の保護機能が搭載されており、バックグラウンドで動作して、コンピュータの安全を確保します。

Intego VirusBarrier X にすべてのウイルスを確実に監視させるには、プログラムを定期的にアップデートする必要があります。Intego VirusBarrier X の NetUpdate 機能を使うと、プログラムのアップデート作業が簡単になります。また、アップデートを自動的に行うように設定することもできます。ユーザはアップデート状況を毎月 1 回は確認してください。また、Intego のホームページ



第 2 章 - コンピュータウイルスとは

(www.intego.com) で、プログラムのアップデートがすぐに必要な新しいウイルスが見つかっていないかどうかを確認することもできます。

もう 1 つの重要な点は、評判の良い発売元が出しているソフトウェアを使用することです。違法コピーソフトには、ウイルスが含まれている可能性があります。また、ソフト自体がトロイの木馬かもしれません。コンピュータには、提供元の確かなソフトウェアのみをインストールしてください。Intego VirusBarrier X では、インストール後、ファイルの一つずつチェックし、それらのファイルが安全であることを確かめます。

さらに、添付ファイルや、e-mail またはインターネットを通じて送られたファイルには用心してください。何気なく開いた贈り物が悲惨な結果をもたらした、記録に残るもっとも古い例を取り上げました（ギリシャ軍から贈られた木馬をトロイ軍が“開いた”とき）。かつては、知らない人から届いた添付ファイルを決して開いてはいけないと言われていました。しかし、Windows コンピュータを狙った近ごろのウイルスは、友人や同僚から送られた添付ファイルを通じて広まっているのです。いかなる場合も、知らない人から送られた添付ファイルは絶対に開かないでください。しかし、この方法だけでは知人が無意識のうちに送ったウイルスを防ぐことができません。Intego VirusBarrier X は、ユーザがファイルを開くと、ファイルをすべてスキャンし、既知のウイルスをすべて自動的に排除します。コンピュータがネットワークにつながっていて、Intego VirusBarrier X によって添付ファイル内のウイルスが検出された場合、ただちにネットワーク管理者に連絡して、会社のメールサーバから感染ファイルを削除してもらってください。

Intego VirusBarrier X にはすべてのアンチウイルス保護機能が搭載されていますが、データの保護だけはユーザ自身で必ず行ってください。つまり、定期的にファイルのバックアップを取ってください。重要なファイルのバックアップを毎日取ることはもちろん、バックアップを複数作っておくことをお



第 2 章 - コンピュータウイルスとは

勧めします。バックアップに使用するメディアは、破損していることがあります。その場合、そのバックアップは役に立ちません。Intego Personal Backup X は、完全なバックアップソリューションを提供します。バックアップを自動的に実行して、お使いの Mac がウイルスに感染した場合でも安全なコピーを確保できるよう支援します。

次のようなバックアップ方法を取るとよいでしょう。たとえば、Zip ドライブを使ってファイルのバックアップを取ります。バックアップ用に、2 つ以上の Zip カートリッジを用意し、毎日カートリッジを交換します。バックアップを保険だと考えてください。これによって、コンピュータでウイルスが見つかった場合に、安全なファイルのコピーを確保できるだけでなく、ハードディスクの故障など、ウイルス以外の問題からもデータを保護することができます。書き込み可能な CD-ROM や外付けのハードディスクなどは、比較的安価なリムーバブルディスクです。また、それほど必要でないとしても、システムやアプリケーションのバックアップを取ることも必要です。何らかの理由でコンピュータが故障した場合、システムやアプリケーションを再インストールするのに相当の時間がかかります。コンピュータ全体のバックアップを取っておけば、復旧作業は数分で終わります。



3 - インストール



システム要件

- 公式にサポートされている Mac OS X 互換コンピュータ
- Mac OS X 10.1.1 以降、または Mac OS X Server 10.1.1 以降
- 20 MB の空きハードディスク容量
- 画面解像度 800 x 600 以上

Intego VirusBarrier X をインストールする

Intego VirusBarrier X のインストールはとても簡単です。Intego VirusBarrier X の CD-ROM を、コンピュータの CD-ROM ドライブに挿入します。Intego VirusBarrier X インストーラ、Read me ファイル、Intego VirusBarrier X マニュアル(本書)、および Acrobat Reader インストーラを含むウィンドウが開きます。Intego VirusBarrier X をダウンロードして入手した場合は、VirusBarrier X.dmg というディスクイメージファイルがあります。このファイルをダブルクリックすると、ディスクイメージが開いてデスクトップにマウントされます。

まず、Read me ファイルを読み、最新の変更内容を確認してください。

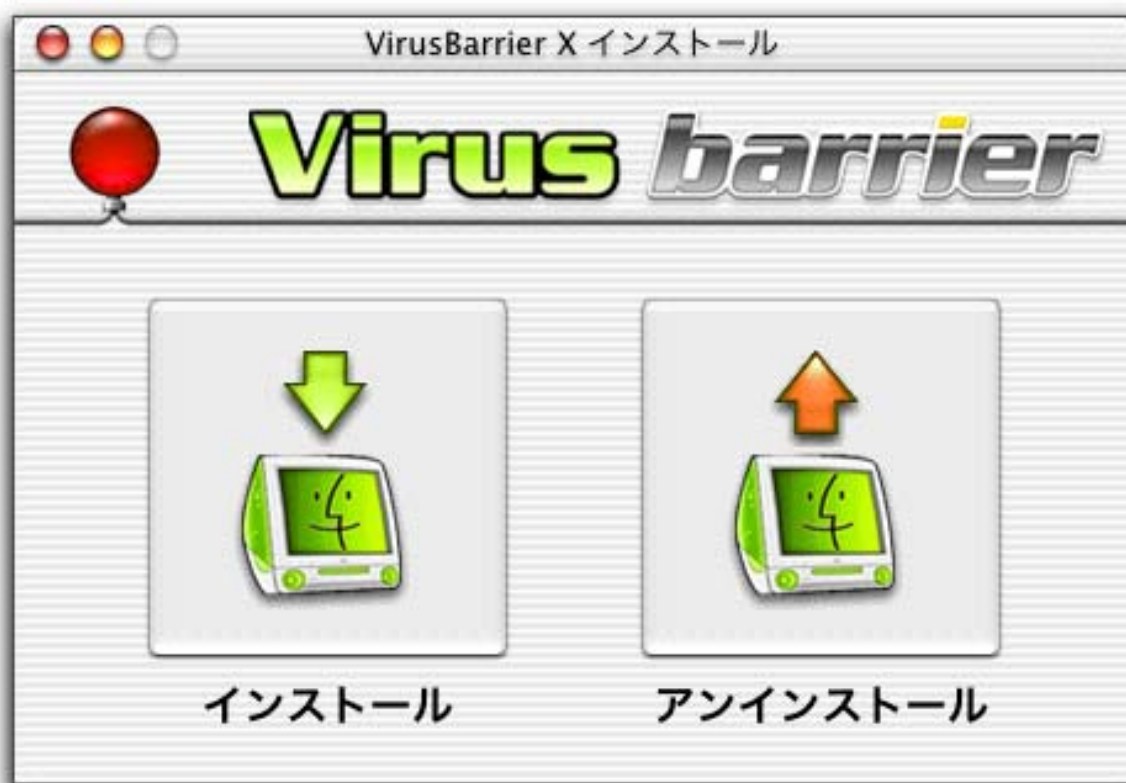
次に、Intego VirusBarrier X インストーラをダブルクリックします。





VirusBarrier X Install

このインストーラには、「インストール」と「アンインストール」という 2 つのオプションがあります。



Intego VirusBarrier X をインストールする場合は「インストール」をクリックします。Intego VirusBarrier X をアンインストールする場合は「アンインストール」をクリックします。



第 3 章 - インストール

ウインドウが開き、Intego VirusBarrier X をインストールするには管理者用パスワードを入力しなければならないという旨のメッセージが表示されます。ロックをクリックして自分のパスワードを入力するか、表示されたダイアログに自分のパスワードを入力します (OS X 10.2 以降)。パスワードを入力し、「OK」をクリックします。次のウインドウが表示されます。



「続ける」をクリックしてインストールを続行します。Intego ソフトウェアの使用許諾契約が表示されます。「続ける」をクリックし、この使用許諾契約に同意する場合は「同意します」をクリックします。同意しない場合は、「同意しません」をクリックしてインストーラを終了します。

第 3 章 - インストール

次のウインドウには、コンピュータ内にある使用可能なディスクまたはボリュームが表示されます。Intego VirusBarrier X をインストールするディスクまたはボリュームを選択し、「続ける」をクリックします。

Intego VirusBarrier X をインストールするには「インストール」をクリックします。このオプションを選択すると、基本インストールが実行されます。カスタムインストールを実行したい場合は、「カスタマイズ」をクリックします。次のウインドウが表示されます。



第 3 章 - インストール

このウインドウで、インストールする項目を選択します。「Common Intego Services」チェックボックスは淡色表示になっています。これは、この項目を必ずインストールしなければならないことを意味します。Intego VirusBarrier X と NetUpdate については、どちらか一方または両方ともインストールするように選択できます。お使いのコンピュータに他の Intego プログラムがインストールされている場合は、アップグレードのオプションが表示されます。つまり、すべての Intego プログラムで使用される特定のコンポーネントは再びインストールされないようになっています。

インストールが完了したら、コンピュータを再起動する必要があります。



Intego VirusBarrier X を登録する

コンピュータを再起動すると、Intego VirusBarrier X が起動します（このアプリケーションは「アプリケーション」フォルダ内にあります）。登録用のプログラムが起動し、次のウインドウが表示されます。



The image shows a registration dialog box for Intego VirusBarrier X. The title bar reads "登録番号を入力してください" (Please enter the registration number). On the left is the VirusBarrier logo, a red sphere with the text "Virus barrier". To the right are three input fields: "名前:" (Name), "所属:" (Affiliation), and "シリアル番号:" (Serial number). Below the serial number field is an example: "例: XXXX-XXXX-XXXX-XXXX-1234". At the bottom right are two buttons: "キャンセル" (Cancel) and "OK".

Mac OS X はマルチユーザオペレーティングシステムであるため、すべてのユーザが同じ権限を持っているわけではありません。Intego VirusBarrier X の初回起動時に、いずれのユーザでもシリアル番号を入力できますが、プログラムの設定を行えるのは管理者権限を持つユーザのみです。

自分の名前、会社に所属している場合はその会社名、およびシリアル番号を入力します。シリアル番号は、Intego VirusBarrier X CD のシールに記載されています。登録が完了すると、Intego VirusBarrier X が開きます。管理者の場合は、ここでプログラムを設定できます。

試用版として Intego VirusBarrier X を使用する

Intego VirusBarrier X には試用版があり、製品を購入する前にその機能や使い心地などを試すことができます。Intego VirusBarrier X を試用版として使用するには、登録画面が表示されたときに「キャンセル」をクリックします。そうすると、プログラムを試用版で実行するかどうかを尋ねるメッセージが表示されます。試用版として実行する場合は「試用する」をクリックします。それ以外の場合は「キャンセル」をクリックします。



4 – クイックスタート



Intego VirusBarrier X の既定モード

Intego VirusBarrier X をインストールして Macintosh コンピュータを再起動すると、プログラムは自動的に起動します。Intego VirusBarrier X は、シンプルで、ユーザの手間を省いた設計になっています。また、何も操作しなくても、コンピュータは完全に保護されます。

プログラムをインストールしたら、あとは何もしなくてもプログラムが自動的に実行します。ただし、NetUpdate を設定して、プログラムのアップデートがあるかどうかを自動的にチェックさせることを推奨します。そうしない場合は、最低でも月に一度は自分で確認してください。

Intego VirusBarrier X を開いて、設定を変更したり、手動スキャンを実行したりするには、「アプリケーション」フォルダにある「Intego VirusBarrier X」アイコンをダブルクリックします。



Intego VirusBarrier X のインターフェース

次の図は、Intego VirusBarrier X アプリケーションのインターフェースです。インターフェースには Orb があり、コンテキスト制御ボタンや、設定を選択したり、スキャンを実行したりするためのボタンが表示されます。それらの機能を使用するには、インターフェース上の該当するボタンをクリックして引き出しを開きます。



Intego VirusBarrier X ORB

現在の処理に関する情報が表示されます。

「コンテキストコントロール」ボタン

このボタンは、スキャン、一時停止、中止など、機能に応じて変化します。

「選択」ボタン

このボタンを使って、ウイルススキャンを実行するボリューム、フォルダまたはファイルを指定することができます。

「ログ」ボタン

ログの一覧を開いて、手動スキャンを実行した日時と、感染または破損が検出されたファイルを表示します。

「NetUpdate」ボタン

このボタンを使って、Intego VirusBarrier X をアップデートできます。

「環境設定」ボタン

Intego VirusBarrier X のその他の設定を選択できます。

「バージョン情報」ボタン

Intego VirusBarrier X に関する情報が表示されます。

引き出しを閉じるには、同じボタンをクリックするか、または引き出しの右側にある三角形をクリックします。また、他のボタンをクリックすると、現在開いている引き出しが閉じて、他の引き出しが開きます。

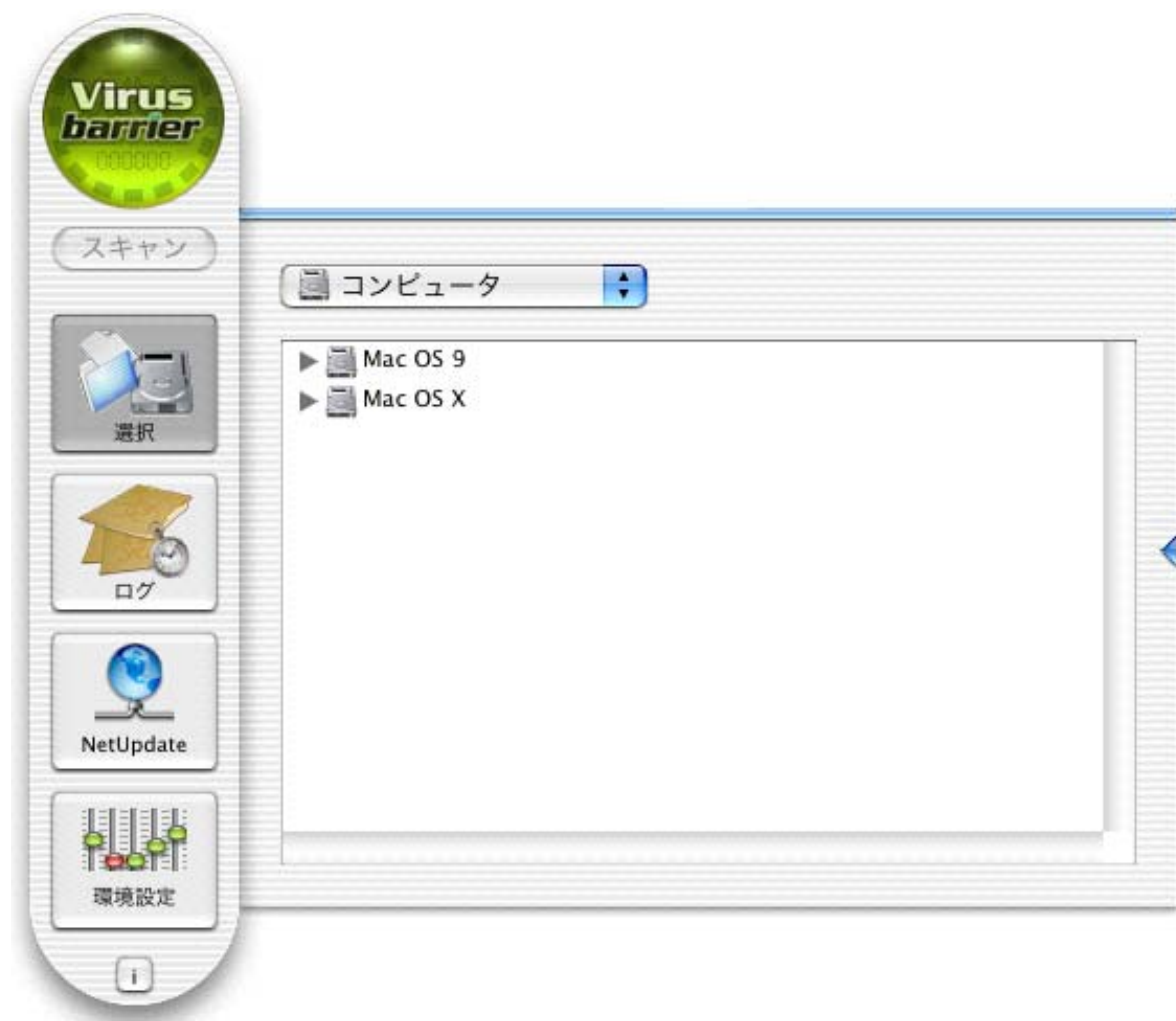
手動スキャンを実行する

Intego VirusBarrier X をインストールすると、ファイルを監視して、ウイルス感染からファイルを保護します。ただし、Intego VirusBarrier X がウイルスチェックを行うのは、ファイルを読み込んだり、使用したり、書き込んだりする場合です。プログラムのインストール時に、インストール直後にすべてのファイルを手動でスキャンして、コンピュータ全体が感染していないことを確認するためのオプションが用意されています。感染ファイルが一つもないことを確認するために、手動スキャンを実行してください。その後追加した新しいファイルのウイルスチェックは、Intego VirusBarrier X が行います。

インストール直後に手動スキャンを実行するように指定しなかった場合、または好きなときに実行するように指定した場合、「アプリケーション」フォルダの Intego VirusBarrier X アイコンをダブルクリックしてプログラムを開きます。

「選択」ボタンをクリックして引き出しを開き、現在コンピュータにマウントされているすべてのボリュームを表示します。このビューは、Finder リストビューに似ており、ボリュームやフォルダ、ファイルが階層形式で表示されます。ボリュームやフォルダを展開して内容を表示するには、左側の三角形をクリックします。その下にあるファイルやフォルダがすべて表示されます。展開したボリュームまたはフォルダを閉じる場合も三角形をクリックします。





いずれかのボリューム、フォルダまたはファイルで手動スキャンを実行するには、スキャンを行うアイテムをダブルクリックするか、またはアイテムを一度クリックして、「スキャン」ボタンをクリックします。スキャンが始まると、Orb に処理状況が表示されます。最初に Orb に表示されるのは、スキャンが終わったファイルの数です。

第 4 章- クイックスタート

「環境設定」で「残りファイル数」を選択している場合は、これからスキャンを行うファイルの数が計算され、その残り数とパーセンテージが表示されます。Orb をクリックすると、表示はスキャンが終わったファイルの数とパーセンテージに変わります。



「中止」ボタンをクリックすると、いつでもスキャンを中止することができます。スキャンを一時停止する場合は、キーボードの Shift キーを押します。「中止」ボタンが「一時停止」ボタンに変わります。このボタンをクリックすると、スキャンが一時停止します。



第 4 章- クイックスタート

スキャンを再開する場合、このボタンをクリックします。このとき、このボタンは「レジューム」ボタンになっています。



NetUpdate の設定

「NetUpdate」ボタンをクリックすると、「NetUpdate」引き出しが開きます。この引き出しを使ってアップデート情報を確認することができ、前回確認したときの情報や Intego VirusBarrier X のバージョン番号、登録有効期限が表示されます。Intego VirusBarrier X を購入されたお客様は、購入日より 1 年間、アップデートと最新のウイルス定義ファイルをご利用いただけます。



重要なのは、Intego VirusBarrier X を定期的にアップデートして、最新のウイルスから保護されるようにすることです。Intego VirusBarrier X には、Intego の NetUpdate が含まれており、プログラムが更新されているかどうかを自動的に確認し、アップデートファイルをダウンロードすることができます。

第 4 章- クイックスタート

アップデートファイルがあるかどうかを確認するには、「今すぐ確認...」をクリックします。Intego NetUpdate が開き、Intego のサーバに接続してプログラムやウイルス定義ファイルが更新されているかどうかを確認します。Intego VirusBarrier X を購入されたお客様は、購入日より 1 年間、アップデートと最新のウイルス定義ファイルをご利用いただけます。

システム環境設定の「NetUpdate 環境設定」パネルで、自動アップデートの日時の指定など、NetUpdate の設定を行うことができます。

NetUpdate の詳細については、第 6 章「Intego VirusBarrier X の設定」および NetUpdate のマニュアルを参照してください。



ドラッグ・アンド・ドロップ操作でスキャンを実行する

ボリュームやフォルダ、ファイルを VirusBarrier X インタフェース内にドラッグしてスキャンを行うこともできます。ドラッグしたアイテムを放すと、他の手動スキャンの場合と同じようにスキャンが開始します。

Intego VirusBarrier X を Dock で使用する

Intego VirusBarrier X を起動すると、Dock にプログラムのアイコンが表示されます。



このアイコンをクリックし、表示されたメニューから「Dock に保存する」を選択すると、アプリケーションを終了した後も Dock にアイコンが表示されたままになります。



第 4 章- クイックスタート

Intego VirusBarrier X アプリケーションを開いている間はアイコンが緑色に、開いていないときは赤色になります。



必要に応じて、ファイルやフォルダ、ボリュームを Dock の Intego VirusBarrier X アイコンにドラッグします。そうすると、Intego VirusBarrier X アプリケーションが開き、ファイルのウイルスチェックが開始されます。Dock の Orb に、現在のチェック状況が表示されます。



「環境設定」で、起動時にアプリケーションを表示しないように設定すると、Intego VirusBarrier X アプリケーションは開かず、Dock の Orb にすべての活動が表示されます。環境設定の詳細については、第 6 章「Intego VirusBarrier X の設定」を参照してください。



5 - Intego VirusBarrier X の機能



Intego VirusBarrier X は、すべての種類のウイルスからコンピュータを保護するためのパワフルで使いやすいプログラムです。このプログラムは、バックグラウンドで動作し、静かで効果的な保護機能を絶えず提供します。

ウイルススキャン

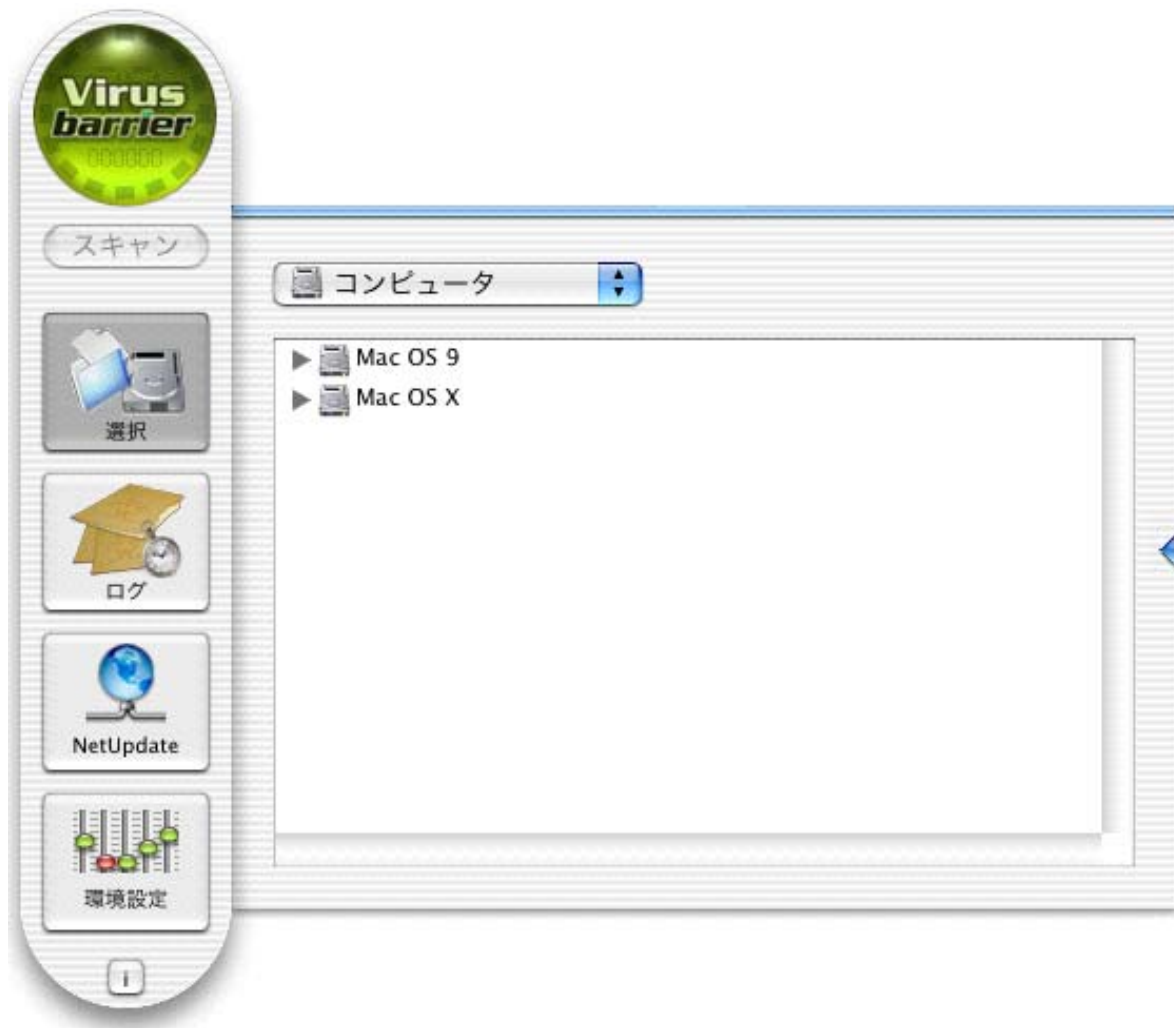
Intego VirusBarrier X の実行方法はいくつかあります。ウイルスからお使いのコンピュータを守るために、常にコンピュータを監視し、CD-ROM、ZIP カートリッジなどのリムーバブルメディアをドライブに挿入するとすぐに、それらのメディアのウイルスチェックを自動的に実行させることができます。また、プログラムを手動モードで使用して、コンピュータ、ディスク、またはコンピュータやネットワーク上のボリュームをスキャンすることもできます。

手動スキャン

Intego VirusBarrier X を初めて使用する際、コンピュータのハードディスクやボリュームをすべて手動でスキャンする必要があります。これにより、コンピュータにウイルスがないことが保証されます。手動スキャンは、プログラムのインストール直後に行ってください。

また、ボリュームやフォルダ、ファイルでいつでも手動スキャンを実行することができます。手動スキャンを実行するには、Intego VirusBarrier X を開いて「選択」ボタンをクリックします。





引き出しが開いて、コンピュータ内にある使用可能なすべてのボリュームが表示されます。このビューは、Finder リストビューに似ており、ボリュームやフォルダ、ファイルが階層形式で表示されます。ボリュームやフォルダを展開して内容を表示するには、左側の三角形をクリックします。その下にあるファイルやフォルダがすべて表示されます。展開したボリュームまたはフォルダを閉じる場合も三角形をクリックします。



ボリュームをスキャンする



ボリュームをスキャンするには、そのボリュームをダブルクリックするか、またはボリュームを一度クリックして「スキャン」ボタンをクリックします。スキャンが始まると、Orb に処理状況が表示されます。最初に Orb に表示されるのは、スキャンが終わったファイルの数です。

「環境設定」で「残りファイル数」を選択している場合は、これからスキャンを行うファイルの数が計算され、その残り数とパーセンテージが表示されます。Orb をクリックすると、表示はスキャンが終わったファイルの数とパーセンテージに変わります。



「中止」ボタンをクリックすると、いつでもスキャンを中止することができます。

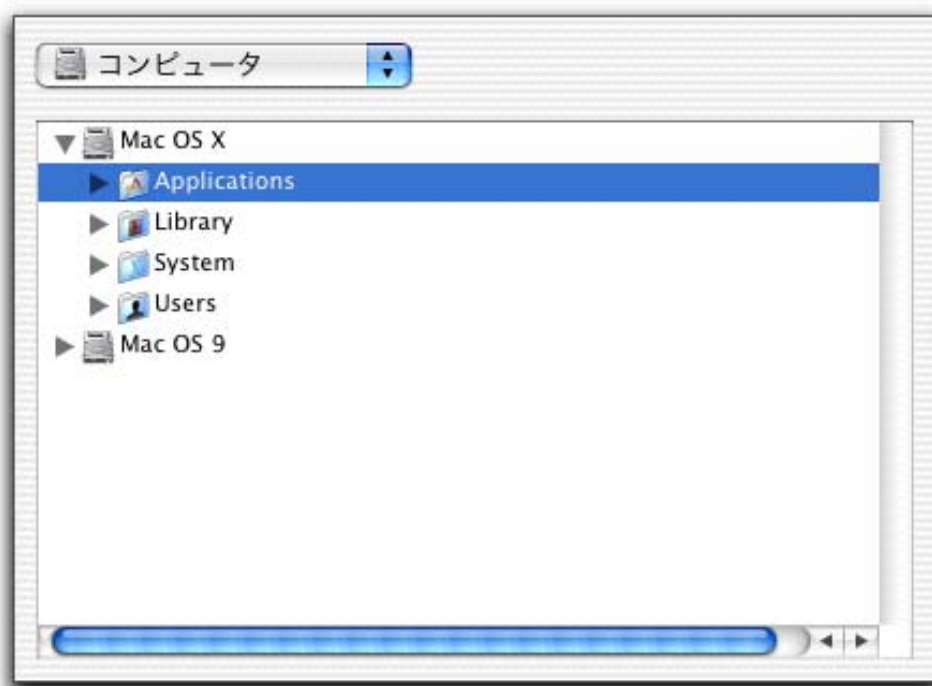


スキャンを一時停止する場合は、キーボードの Shift キーを押します。「中止」ボタンが「一時停止」に変わります。このボタンをクリックすると、スキャンが一時停止します。



スキャンを再開する場合、このボタンをクリックします。このとき、このボタンは「レジューム」ボタンになっています。

フォルダをスキャンする



コンピュータ内のフォルダをスキャンするには、ボリュームの左側にある三角形をクリックして展開し、スキャンを実行するフォルダを表示します。フォルダをダブルクリックするか、またはフォルダを一度クリックして選択し、「スキャン」ボタンをクリックします。スキャンが始まると、Orb に処理状況が表示されます。最初に Orb に表示されるのは、スキャンが終わったファイルの数です。

「環境設定」で「残りファイル数」を選択している場合は、これからスキャンを行うファイルの数が計算され、その残り数とパーセンテージが表示されます。Orb をクリックすると、表示はスキャンが終わったファイルの数とパーセンテージに変わります。



「中止」ボタンをクリックすると、いつでもスキャンを中止することができます。



スキャンを一時停止する場合は、キーボードの Shift キーを押します。「中止」ボタンが「一時停止」に変わります。このボタンをクリックすると、スキャンが一時停止します。





スキャンを再開する場合、このボタンをクリックします。このとき、このボタンは「レジューム」ボタンになっています。

ファイルをスキャンする



コンピュータ内のファイルをスキャンするには、ボリュームの左側にある三角形をクリックして展開し、スキャンを実行するファイルを表示します。ファイルをダブルクリックするか、またはファイルを一度クリックして選択し、「スキャン」ボタンをクリックします。スキャンが開始すると、Orb に処理状況が表示されます。しかし、たいていの場合、スキャンを実行するファイルが一つのため、スキャン処理はすぐに完了します。



ドラッグ・アンド・ドロップ操作でスキャンを実行する

ボリュームやフォルダ、ファイルを VirusBarrier X インタフェース内にドラッグしてスキャンを行うこともできます。ドラッグしたアイテムを放すと、他の手動スキャンの場合と同じようにスキャンが開始します。

スキャン結果

Intego VirusBarrier X で感染ファイルが発見されると、「ログ」ウインドウが開き、感染ファイルの名前と感染したウイルスの種類が表示されます。Intego VirusBarrier X にスキャンのみを実行するように指示し、修復を指示しなかった場合、ここに感染ファイルとウイルスの種類が表示されます。Intego VirusBarrier X を、感染ファイルの自動修復を実行するように設定した場合、修復したファイルの名前と感染していたウイルスの種類が表示されます。



スキャン結果の内容

Intego VirusBarrier X では、既知のウイルスに感染したファイルを検出するとユーザに通知が出されます。また、破損したファイルが見つかった場合も通知されます。

感染ファイル



感染ファイルが見つかり、Intego VirusBarrier X Orb が赤色に変わり、「ログ」引き出しが開きます。この引き出しは、感染ファイルが見つかり、すぐに開きます。したがって、引き出しが開いている間は、まだスキャンが進行中である可能性があります。また、Intego VirusBarrier X では、「環境設定」で設定した警告オプションに従って警告を表示します。警告オプションの詳細については、第 6 章「Intego VirusBarrier X の設定」を参照してください。

「ログ」引き出しの表示は、「環境設定」で選択したスキャンモードによって異なります。感染または破損したファイルが見つかったときに、Intego VirusBarrier X に自動修復させる（修復モード）ことも、警告のみを表示させることもできます（スキャンモード）。修復モードを選択すると、修復で

きる場合はただちに修復を実行します。スキャンモードを選択した場合は、自分で修復を行う必要があります。修復モードの詳細については、第 6 章「Intego VirusBarrier X の設定」を参照してください。



スキャンモードを選択している場合、「ログ」引き出しに感染したファイルの名前が表示されます。ファイルを修復するには、修復を行うファイルを選択し、ウインドウの一番下にある「修復」ボタンをクリックします。ファイルが修復され、「ログ」引き出しに変更内容が表示されます。表示されたファイルを Finder に表示する場合は、ファイルをクリックして選択し、「Finder に表示」をクリックします。



破損ファイル

破損したファイルが見つかったら、Intego VirusBarrier X に「ログ」引き出しが表示されます。この引き出しは、破損ファイルが見つかったらすぐに開きます。したがって、引き出しが開いている間は、まだスキャンが進行中である可能性があります。また、Intego VirusBarrier X では、「環境設定」で設定した警告オプションに従って警告を表示します。警告オプションの詳細については、第 6 章「Intego VirusBarrier X の設定」を参照してください。

破損ファイルにはウイルスが含まれていない場合もあります。しかし、それらのファイルにウイルスが感染していなくても、多くのウイルスはファイルに悪影響を及ぼすことがあります。それらのファイルは、ファイルを開いたときに生じたディスクエラーやクラッシュが原因で破損した可能性もあります。破損ファイルが見つかった場合、そのファイルをできるだけ早く交換してください。



警告

先述のとおり、Intego VirusBarrier X では手動でスキャンを実行できますが、通常このプログラムはバックグラウンドで動作します。感染ファイルが見つかった場合の警告には、いくつかの方法があります。

警告が表示されるのは、VirusBarrier X で感染ファイルが検出され、VirusBarrier X をスキャンのみを実行し、感染ファイルの自動修復を行わないように設定している場合です。



ファイルの修復を行う場合は「修復」をクリックします。修復しない場合は、「この警告を無視」をクリックします。この場合、ファイルは修復されません。注意：警告を無視するのは危険です。特別な理由がない限り、「修復」を選択してください。

警告の設定方法については、第 6 章「Intego VirusBarrier X の設定」を参照してください。

6 - Intego VirusBarrier X の設定



環境設定

Intego VirusBarrier X インタフェースの「環境設定」ボタンを押すか、または Intego VirusBarrier X メニューの「環境設定...」を選択してオプションを設定することができます。左側のタブではスキャンモードオプションを、右側のタブでは警告オプションをそれぞれ設定できます。

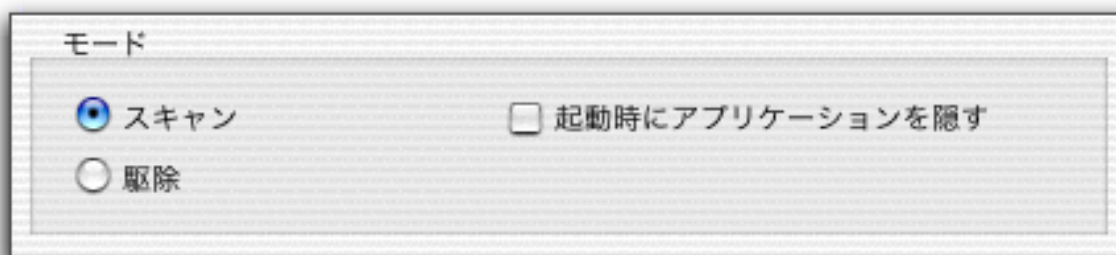


スキャンモード

このタブを使って、Intego VirusBarrier X のウイルススキャンの方法、および Orb に表示される情報に関するオプションを設定できます。

モード

ここでは、スキャンの実行モードと、起動時にアプリケーションを開くかどうかを指定します。



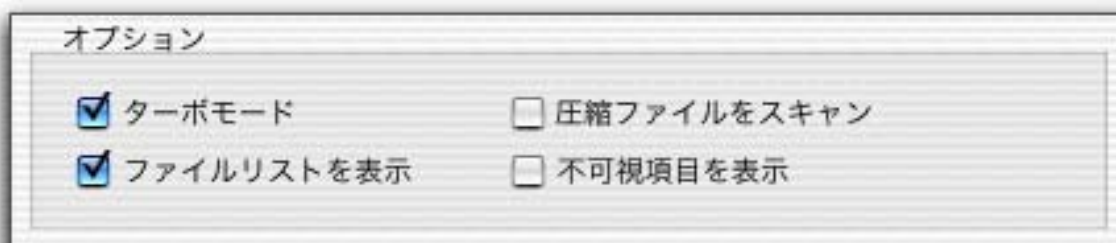
Intego VirusBarrier X では、ウイルススキャンの実行モードを「スキャン」モードと「駆除」モードのいずれかから選択できます。スキャンモードを選択すると、感染ファイルが検出された際に警告が表示されますが、ウイルスは駆除されません。スキャン時に感染ファイルが見つかった場合は警告が表示され、手動スキャンを実行している場合はログに感染ファイルが表示されます。ただし、ファイルの修復はユーザ自身で行う必要があります。この機能は、コンピュータがネットワークにつながっている場合や、ネットワーク管理者が検出したファイルを調査する必要がある場合に便利です。

スキャンモードを使用するには、「スキャン」ラジオボタンをオンにします。

「起動時にアプリケーションを隠す」をオンにすると、アプリケーションを起動したときに Intego VirusBarrier X は Dock に表示され、アプリケーション自体は表示されません。この場合、ファイル、フォルダまたはボリュームを Dock 上の Intego VirusBarrier X アイコンにドラッグしてスキャンを実行することができます。スキャン中にウイルスが検出されると、「警告」タブの設定に従って警告が表示されます。

オプション

他にも、Intego VirusBarrier X の動作方法を設定するためのオプションが用意されています。



ターボモード

「ターボモード」チェックボックスをオンにすると、ファイルのスキャンが高速化されます。Intego VirusBarrier X では、初回スキャン時にチェックしたファイルがすべて記憶されます。Intego VirusBarrier X は、それらのファイルが更新されない限り、それらのファイルのスキャンは実行しません。これにより、スキャン速度が 5 ~ 40 倍速くなります。ただし、後から変更が加えられたファイルに対しては、スキャンを実行します。また、Intego VirusBarrier

X のウイルス定義を更新した場合は、既知のウイルスがないことを確認するために、すべてのファイルにスキャンが実行されます。

ファイルリストを表示

このオプションをオンにすると、ファイルのスキャン中、Intego VirusBarrier X Orb にスキャン済みのファイル数ではなく、残りのファイル数が表示されます。

圧縮ファイルのスキャン

「圧縮ファイルのスキャン」チェックボックスをオンにすると、Stuffit アーカイブに含まれる圧縮ファイルに対してスキャンが実行されます。Stuffit アーカイブにある圧縮ファイルのスキャン実行中、アーカイブのウイルスチェック中であり、アーカイブに感染ファイルや破損ファイルが見つかった場合に通知される旨のメッセージが数秒間表示されます。それらのファイルの修復またはウイルス駆除を行う場合は、アーカイブを解凍し、ファイルまたはフォルダを Intego VirusBarrier X Orb にドラッグして修復またはウイルス駆除を実行します。その後、感染または破損した元のアーカイブを削除します。

不可視項目を表示

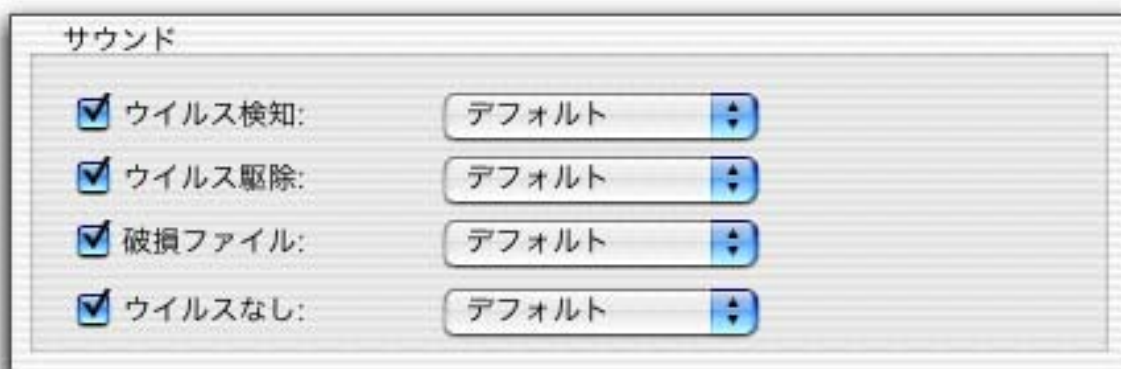
このチェックボックスをオンにすると、ブラウザの引き出しに不可視ファイルが表示されます。



サウンド

Intego VirusBarrier X では、次の 4 つのイベントを音で通知することができます。

- ウイルス検知
- ウイルス駆除
- 破損ファイル
- ウイルスなし



デフォルトのサウンドを指定して合成音でイベントを通知することも、また、コンピュータ上にある他のサウンドを使用することもできます。ポップアップメニューから使用するサウンドを指定してください。

警告

「警告」タブには、警告がある場合の Intego VirusBarrier X の動作方法を指定するためのオプションがあります。



警告オプション

Intego VirusBarrier X がバックグラウンドで動作している場合、ファイル内でウイルスが見つかったことを通知するには 3 通りの方法があります。



駆除し警告ダイアログを表示

このオプションをオンにすると、感染ファイルのウイルス駆除を自動的に実行し、感染ファイルの名前と見つかったウイルスの種類が表示されます。

駆除しログに残す

このオプションをオンにすると、感染ファイルのウイルス駆除を自動的に実行し、感染ファイルの名前と見つかったウイルスの種類をログに記録します。この場合、ユーザへの通知は行われません。したがって、ユーザは感染ファイルが検出されたかどうかをログで確認する必要があります。

警告ダイアログを表示

このオプションをオンにすると、感染ファイルの名前と見つかったウイルスの種類を通知してユーザに警告を促します。その際、感染ファイルを修復するかどうかを確認するメッセージが表示されます。

オプション

オプション

e-mail 送信

宛先: john.doe@mac.com

受信アドレス: jane.doe@mac.com

送信 (SMTP) サーバ: smtp.mac.com

入力例

e-mail 送信

このチェックボックスをオンにすると、テキストフィールドに入力したアドレスに 30 秒以内に e-mail メッセージが送信されます。送信メールサーバだけでなく、差出人と受取人の e-mail アドレスを入力する必要があります。この e-mail メッセージは、複数の受取人に送ることができます。その場合は、e-mail アドレスをカンマで区切って入力します。

NetUpdate

「NetUpdate」ボタンをクリックすると、「NetUpdate」引き出しが開きます。この引き出しを使ってアップデート情報を確認することができ、前回確認したときの情報や Intego VirusBarrier X のバージョン番号、登録有効期限が表示されます。Intego VirusBarrier X を購入されたお客様は、購入日より 1 年間、アップデートと最新のウイルス定義ファイルをご利用いただけます。



アップデートファイルがあるかどうかを確認するには、「今すぐ確認...」をクリックします。Intego NetUpdate が開き、Intego のサーバに接続してプログラムやウイルス定義ファイルが更新されているかどうかを確認します。Intego VirusBarrier X を購入されたお客様は、購入日より 1 年間、これらのウイルス定義ファイルを無償でご利用いただけます。

システム環境設定の「NetUpdate 環境設定」パネルで、自動アップデートの日時の指定など、NetUpdate の設定を行うことができます。

NetUpdate および NetUpdate の設定に関する詳細は、NetUpdate のマニュアルを参照してください。

ウイルス事典

この引き出しの右側のタブ「ウイルス定義」には、VirusBarrier X がブロックするさまざまな Macintosh ウイルスの歴史が紹介されている「ウイルス事典」があります。



Intego VirusBarrier X について



この引き出しには、VirusBarrier X のバージョン番号、サポート番号（テクニカルサポートを受ける際に必要となる番号）、Intego の Web サイトや e-mail アドレスへのリンク、および Intego 社の所在地や電話番号など、Intego VirusBarrier X に関する情報が表示されます。

第 6 章 – Intego VirusBarrier X の設定

質問があり、Intego に問い合わせる場合は「問い合わせ」リンクをクリックしてください。お使いの e-mail ソフトが起動し、「お客様番号 # からのメッセージ」という件名で Intego にメッセージを送ることができます。“#”にはお客様番号が入力されます。本文欄に問い合わせの内容を入力し、Intego にただちに送信してください。

Intego のテクニカルサポートを受けられる方は「サポート」リンクをクリックしてください。お使いの e-mail プログラムが起動し、「お客様番号 # からのサポート依頼」という件名で Intego にメッセージを送ることができます。“#”にはお客様番号が入力されます。本文欄に問い合わせの内容を入力し、Intego にただちに送信してください。

「オンライン登録...」ボタンをクリックすると、Intego Web サイトの Intego VirusBarrier X ユーザ登録ページが開きます。ユーザ登録は必ず行ってください。ユーザ登録することで、Intego より VirusBarrier X の最新情報や、その他の製品情報をお送りすることができます。

「製品情報」リンクをクリックすると、Intego Web サイトに移動します。



7 - 診断



ウイルスに感染したと思ったら

感染の症状

次のような症状がある場合でも、必ずしもウイルスに感染しているとは限りません。以下は、あくまでもウイルス攻撃によって生じる可能性がある症状の例です。

- 予期しないエラーメッセージが表示される
- Macintosh が不可解な“クラッシュ”を起こす
- 操作していないにも関わらず、ハードディスクまたはフロッピーディスクの読み込みが始まる
- システムの動作が非常に遅い
- 大量のファイルを保存したわけでもないのに、ディスクの空き容量が著しく減少した

上記のような症状が現れた場合、ウイルスが原因で問題が起きたのか、他のソフトウェアに問題があるのかを確認する方法があります。

まず、Apple の Disk Utility プログラムを実行します。このプログラムは、コンピュータのハードディスクにある問題を診断し、修復するためのものです。Disk Utility プログラムは、デフォルトで「Applications」フォルダの「Utilities」フォルダにインストールされます。このプログラムによって修復不可能な問題が見つかった場合は、市販のディスクメンテナンスプログラムが必要になります。

Disk Utility で問題が解決できない場合は、最近インストールしたソフトウェアが原因である可能性があります。コンピュータで生じるほとんどの問題は、ソフトウェアとの互換性に原因がありま



第 7 章 - 診断

す。最近ソフトウェアをインストールしたことがある場合は、そのソフトウェアをアンインストールし、問題が解決するかどうかを確認してください。

また、コンピュータに接続した外付けドライブや USB ハードウェア、プリンタドライバなど、他のハードウェアが原因で問題が生じることもあります。それらのデバイスやドライバを起動して、問題が生じるかどうかを確認します。

それでも問題が解決されない場合は、Apple Web サイト (www.apple.com) の「サポート」で、問題の解決方法があるかどうかを確認することができます。

それでも解決せず、ファイルがウイルスに感染している可能性がある場合は、ファイルのコピーを Intego ウイルスモニタリングセンターに送ってください。詳細については、第 8 章「テクニカルサポート」を参照してください。

基本的な予防策

お使いの Macintosh には Intego VirusBarrier X の監視の目が光っていますが、コンピュータ上のファイルを確実に保護するために、次のような基本的な予防策を講じる必要があります。

- ファイルのバックアップを定期的に取り。Intego Personal Backup X で自動的にバックアップを取るようにすると便利です。
- もっとも重要なファイルは何部かコピーを作っておく。



第 7 章 - 診断

- リムーバブルメディアを他のコンピュータに“一時的に移す”場合や、それらのメディアを他者に貸す場合は、(可能であれば)メディアのライトプロテクトタブをスライドさせて「ライトプロテクト」にしておく。
- よほどの理由がない限り、Intego VirusBarrier X の機能を停止しない。ほとんどのインストールプログラムでは他のアプリケーションをすべて閉じるように指示されますが、新しいプログラムをインストールする際に、Intego VirusBarrier X を終了する必要はありません。
- 海賊版のソフトウェアを使用しない。これは違法というだけでなく、複数のコンピュータで使用されてきたため、ウイルスが含まれていることが多くあります。
- したがって、手を加えられていないことが確実なプログラムのみをインストールするようにしてください。
- 必要に応じて NetUpdate を使用し、Intego VirusBarrier X の最新版があるかどうかをチェックする。また、定期的にチェックして、Intego VirusBarrier X を常に最新の状態に保ってください。
- ウイルス対策には Intego VirusBarrier X のみを使用する。他のソフトウェアを併用すると、互換性の問題が生じる可能性があります。



8 – テクニカルサポート



第 8 章- テクニカルサポート

Intego VirusBarrier X のユーザ登録を済ますと、テクニカルサポートを受けられるようになります。

e-mail によるお問い合わせ

support@intego.com

Intego 社の Web サイト

www.intego.com

Intego ウイルスモニタリングセンターにファイルを送る場合は、sendvirus@intego.com 宛にお問い合わせください。



9 - 付録



用語集

INIT - 機能拡張ファイルの別名。この用語は、コンピュータのブート時にそれらのファイルが initialized (初期化) されることに由来しています。

アーカイブ - 複数のファイルが含まれるファイル。通常、ディスクスペースを節約するために圧縮されています。Macintosh で使用される一般的な圧縮方法は Stuffit です。

アンチウイルス - スキャンの実行やウイルスの駆除、感染ファイルの修復を行って、ウイルスからコンピュータを保護するためのプログラム。アンチウイルスでは、ファイルやアプリケーションの特定の場所で、ウイルスの“特性”を構成する小さなコード群を探します。

ウイルス - 自己再生して増殖するコンピュータプログラム、またはわずかなコンピュータコード。ほとんどのウイルスは悪質で、ファイルに入り込んで感染します。また、ウイルスは寄生先のファイルを利用し、ユーザがそのファイルを開いたり、実行したりしたときに繁殖します。

感染 - 「ファイルが感染した」とは、ウイルスがファイルに自己繁殖したことを意味します。それはワープロファイルに繁殖するマクロの場合もあれば、アプリケーションに繁殖する他の種類のコードの場合もあります。

機能拡張 - 機能拡張 (init とも言う) は、コントロールパネルのようなもので、Macintosh オペレーティングシステムの一部です。基本システムに機能を追加し、特定のハードウェア用のドライバとして使用されます。機能拡張には、コンピュータをブートしたときにシステムと一緒にロードされるものと、必要によってシステムに呼び出されるものの 2 種類があります。

コード - コンピュータプログラムはコード、またはプログラミング言語で書かれています。ウイルスもコンピュータプログラムで、やはりコードで書かれています。



トロイの木馬 - トロイの木馬（略して“トロイ”）は、実際には、ある悪質なコードを隠しているプログラムです。これは、繁殖しないため本質的にウイルスではありません。しかし、トロイの木馬を実行したときに、他のファイルに自己再生するウイルスコードが含まれている可能性があります。「トロイの木馬」という名前は、ギリシャ軍からトロイ軍にプレゼントされた、中が空洞の巨大な木馬に由来します。この木馬はトロイ軍の要塞に持ち込まれました。しかし、その夜、ギリシャ兵士が木馬の中から現われ、トロイの街の門を開き、大勢のギリシャ兵士たちが街の中に突入してきたのです。

デスクトップファイル - アイコンと、ファイルやアプリケーションの種類を関連付けるための不可視ファイル。MacOS 9、Desktop DB および Desktop DF では、コンピュータ上のボリュームやディスクはすべて不可視なデスクトップファイルとして扱われます。リムーバブルディスクをドライブに挿入すると、必ずそれらのデスクトップファイルが読み込まれるため、古いウイルスの中にはデスクトップファイルを狙ったものがあります。

デマウイルス - 嘘のウイルス警告。現在、数多くのデマウイルスが e-mail で広まっています。このようなデマメールは、e-mail を読んだだけでウイルスに感染するという情報を流しています。

パーティション - ボリューム、ハードディスクの論理部分。ハードディスクには、各パーティションがそれぞれ小さなハードドライブのように働く、数多くのパーティションを作ることができます。オペレーティングシステムは、パーティションを個別のボリュームとみなします。

ブート - コンピュータのブートとは、コンピュータを再起動することです。ブートという言葉は“ブートストラップ”に由来し、“独力でやり遂げる”という意味があります。

変種 - ウイルスの変種とは、特定のウイルスの変化型を言います。この用語は、医学で生物ウイルスに用いられるように、コンピュータウイルスに対しても使われます。また、突然変異により、新しい変種が作られることもあります。



ボリューム - 本質的にハードドライブ、またはその他のリムーバブルメディアユニット。ハードディスク全体、ハードディスク上のパーティション、ネットワーク上のリモートコンピュータ、またはフロッピーディスクを指します。ボリュームの特徴は、ボリューム上に格納されているファイルの場所を表すディレクトリファイルが含まれている点です。

マクロ - 特定のアプリケーションのマクロ言語が持つ組み込み機能を使用する、ショートプログラム。マクロ機能は数多くのアプリケーションに搭載されており、頻繁に使う機能をより簡単に実行するために設計されています。残念なことに、マクロもシステムを破壊する可能性があります。ユーザ環境には数多くのマクロウイルスが存在し、Microsoft Word や Excel で動作します。

マクロウイルス - アプリケーションに組み込まれているマクロ言語を利用するウイルス。現在、Macintosh ユーザにとって、マクロウイルスはもっとも危険なウイルスです。特に、マクロウイルスは Macintosh コンピュータから Windows コンピュータに移行できるため、Microsoft Word や Excel を使用しているユーザには脅威です。

マクロコマンド - マクロで使用可能な小さなプログラミングコマンド。マクロコマンドでは、アプリケーション特有のマクロ言語を使用します。

リソース - Macintosh のファイルには、リソースフォークとデータフォークの 2 つがあります。リソースフォークには、アイコン、コード、その他のアプリケーションの命令を含むことができます。ウイルスの中には、リソースに隠れたり、リソースを破壊したり、変更したりするものもあります。

リムーバブルメディア - ドライブに挿入して使用する、CD-ROM、Zip カートリッジ、フロッピーディスクなどのデータ保存メディア。

ワーム - 自己再生を繰り返して、ネットワーク上で広がるプログラム。ワームは悪質な活動を実行する能力があるため、ウイルスの一種としてみなされがちですが、動作方法が異なります。ワームは、自己再生するための寄生先のファイルを必要としません。



ウイルス事典

ANTI

ANTI ウイルスは、1989 年にフランスで発見されました。最初に見つかったものを“ANTI-A”と呼びます。1990 年に見つかった 2 つ目の変種は“ANTI-B”です。このウイルスは、アプリケーションに感染しますが、システムやデータファイルには感染しません。System 6 でのみ増殖します。

ANTI という名前は、ウイルスから“ANTI”という文字列が見つかったために付けられました。このウイルスは、アプリケーションを破損し、クラッシュさせるため、比較的危険なウイルスです。ANTI によって破損したアプリケーションは修復不可能なため、インストールし直さなければなりません。しかし、このウイルスは再生するだけで他の活動は行わないため、アプリケーションの破損原因は一見偶発的な故障のように見えます。

ANTI-B は、ANTI-A より前に作られたものであると考えられています。それは、ANTI-A には ANTI-B の機能を無効にするコードが含まれているためです。その他にも、これら 2 つには相違点があります。

AUTOSTART ワーム

1985 年 5 月、Macintosh コンピュータで初めて感染したワームが発見されました。東南アジアにすぐに広まり、世界中で流行しました。このワームには、AutoStart 9805-A、B、C、D、E、F などの変種があります。



このワームは、感染した CD-ROM をコンピュータで読み込むと、QuickTime の “CD-ROM AutoPlay” 機能を持つ Macintosh コンピュータに簡単に感染します。ワームはホストコンピュータに自己再生し、「Desktop Print Spooler」、「Desktop Printer Spooler」または「DELDesktop Print Spooler」という機能拡張フォルダに不可視ファイルを作成します。

このワームは、ファイルを削除したり、データを破壊したりするなど、コンピュータに深刻な問題をもたらす可能性があります。また、他の種類のファイルを攻撃する変種もあり、破損したファイルはゴミデータに書き換えられ、修復することも元に戻すこともできません。感染したコンピュータでは、3分、6分、10分 または 30分ごとにディスクが多くの異常な動作を行います。「Applications」メニューに「Desktop Print Spooler」が表示されることもあります。

CDEF

CDEF ウイルスは、1990年にニューヨーク州イサカで初めて発見されました。このウイルスの作成者は、ウイルスの発見直後に逮捕されました。この作成者は、WDEF の作成者でもあります。CDEF という名前は、Macintosh デスクトップファイルの CDEF リソースを使って繁殖することに由来します。通常、CDEF リソースは、特定のアプリケーションとシステムファイルにあります。したがって、CDEF ファイルがあるからといって、そのファイルが必ずしも感染しているわけではありません。しかし、このリソースは通常デスクトップファイルにはありません。

CDEF ウイルスは、デスクトップファイルのみに感染し、ディスクからディスクへすぐに広まります。これは、Macintosh ではマウントしたディスクのデスクトップファイルをすべて読み込むためです。このウイルスは、悪質な損害を与えません。しかし、他のウイルスと同様に、危険であることには変わりません。



第 9 章- 付録

1993 年、最初の CDEF とほとんど変わらない変種が発見されました。

CODE 1

CODE-1 は、1993 年に米国で発見されました。このウイルスは、それほど破壊的ではありませんが、システムファイルやアプリケーションに感染します。このウイルスは、毎年 10 月 31 日にコンピュータを起動すると、起動ボリュームの名前を「Trent Saburo」に変更します。このウイルスも他のコンピュータに感染し、システムと特定のアプリケーションのクラッシュを引き起こします。

CODE 252

CODE 252 ウイルスは、1992 年に米国で発見されました。このウイルスは、システムファイルとアプリケーションの両方に感染し、6 月 6 日～ 12 月 31 日の間に感染したコンピュータを起動すると、次のメッセージを表示します。

```
You have a virus.  
Ha Ha Ha Ha Ha Ha Ha  
Now erasing all disks...  
Ha Ha Ha Ha Ha Ha Ha  
P.S. Have a nice day  
Ha Ha Ha Ha Ha Ha Ha  
(Click to continue...)
```

このメッセージが表示されても、ファイルは削除されません。6 月 5 日以前は、ウイルスはアプリケーションからシステムファイル、システムファイルから他のアプリケーションへと自己繁殖を繰り返すだけです。System 7 では、クラッシュやファイルの破損といった現象が見られますが、他のアプリケー



第 9 章- 付録

ションには繁殖しません。ただし、この未完成なウイルスは、コードに複数のエラーがあるため、他のクラッシュや損害を引き起こす可能性があります。

CODE 9811

CODE 9811 ウイルスは、1998 年 11 月にスウェーデンで発見されました。このウイルスはアプリケーションのファイルを不可視に変え、ランダムな文字列で構成される名前を付けて、それらのファイルをゴミファイルに置き換えます。毎週月曜日に、このウイルスは 25% の確率で「You have been hacked by the Praetorians」というメッセージを表示します。また、感染したコンピュータのデスクトップを虫の絵柄に変えてしまいます。また、このウイルスは、起動ボリュームにあるアンチウイルスソフトウェアを削除しようとします。

CODE 32767

このウイルスは 1997 年に発見されましたが、今ではほとんど見られなくなりました。このウイルスは、毎月 1 度ドキュメントを削除しようとします。

Flag

Flag ウイルス (WDEF-C ウイルスとも呼ぶ) は、システムファイルに感染します。大きな損害は与えませんが、WDEF リソースを ID 0 に変更します。これにより、コンピュータが破損する可能性があります。このウイルスは、今ではほとんど見られなくなりました。



Frankie

Frankie ウイルスはドイツで発見され、Atari または Amiga コンピュータなどの特定の Macintosh エミュレータのみを攻撃する珍しいウイルスです。海賊版のエミュレータソフトウェアを狙っているような振りをし、「Frankie says:No more piracy!」というメッセージを表示して、Atari をクラッシュさせます。Macintosh コンピュータには影響ありませんが、アプリケーションに感染します。このウイルスは、感染したアプリケーションから他のエミュレータのコピーに広がる可能性があります。

Graphics Accelerator

SevenDust を参照。

INIT-M

INIT-M は、1993 年に米国で発見されました。これは非常に危険なウイルスで、13 日の金曜日に動作するようにプログラミングされています。このウイルスは、さまざまなフォルダやファイルの名前をランダムな文字列で構成される名前に変更します。また、ファイルのクリエータや種類をランダムな 4 つの文字列に変更します。これにより、ファイルのアイコンが変更され、この情報を元に戻さない限り、ファイルを開けなくなる可能性があります。さらに、ファイルの作成日と更新日を 1904 年 1 月 1 日に変えてしまいます。場合によっては、ファイルを削除したり、ウインドウを意味不明な表示に変えてしまうこともあります。

このウイルスは、すべての種類のファイルに感染し、「環境設定」フォルダに「FSV Prefs」というファイルを作成します。



INIT 17

INIT 17 は、1993 年にカナダで発見されました。このウイルスは、システムファイルやアプリケーションに感染します。感染したコンピュータを 1993 年 10 月 31 日午前 6:06:06 以降に初めて起動したとき、「From the depths of Cyberspace」というメッセージを表示します。一度このメッセージが表示されると、二度と表示されません。

このウイルスには数多くのエラーが含まれているため、一部の 68000 Macintosh コンピュータでクラッシュを引き起こす可能性があります。このクラッシュは、意図したものではなく、どちらかと言うと偶発的なものです。

INIT 29

このウイルスは、1988 年に初めて発見され、1994 年には変種が見つかっています。これらは、それぞれ INIT 29 A、INIT 29 B と呼ばれます。

これは極めて危険なウイルスで、システムファイル、アプリケーションファイル、ドキュメントに感染します。ただし、感染したドキュメントから他のファイルには感染しません。

このウイルスは、感染以外の損害を引き起こしませんが、ロックしたフロッピーディスクをコンピュータに挿入すると、次のようなメッセージを表示します。

The Disk “xxxx” needs minor repairs.

Do you want to repair it?



第 9 章- 付録

さらに、感染したコンピュータでは、クラッシュやさまざまなエラー、印刷上の問題など、あらゆる問題が見つかっています。

INIT 1984

INIT 1984 ウイルスは、1992 年にオランダと英国で発見されました。他の多くのウイルスと同様、13 日の金曜日に感染したコンピュータを起動するとウイルスが動作します。このウイルスは、INIT-M ウイルスのように、さまざまなフォルダやファイルの名前をランダムな文字列で構成される名前に変更します。また、ファイルのクリエイターや種類をランダムな 4 つの文字列に変更します。これにより、ファイルのアイコンが変更され、この情報を元に戻さない限り、ファイルを開けなくなる可能性があります。そして、ファイルの作成日と更新日を 1904 年 1 月 1 日に変更します。

このウイルスは、INIT (または機能拡張) のみに感染し、他の種類のファイルには一切感染しません。INIT は、コンピュータ間に広まることはほとんどないため、アプリケーションに損害を与える他のウイルスほど速く広まりません。

INIT 9403

このウイルスは、SysX ウイルスとしても知られ、1994 年にイタリアで発見されました。現在は、イタリア版のシステムソフトウェアを搭載した Macintosh のみに感染します。このウイルスは非常に危険で、ファイルを削除して、現在マウントされているディスクを消去しようとします。また、このウイルスは海賊版のソフトウェアに感染するようで、Finder に感染します。そして、特定の圧縮およびアーカイブプログラムにも感染します。



マクロウイルス

今日、マクロウイルスは、Macintosh ユーザに多大な脅威をもたらしています。

最初に発見された Concept マクロウイルスは、Microsoft Word ファイルを攻撃するものでした。その直後、あるウイルス作成者が Word の普及率に強力な破壊力を見出し、変種を作りました。後に、Microsoft Excel を利用したマクロウイルスも作られるようになりました。初めてマクロウイルスが発見されてからたったの 5 年間で、数千のマクロウイルスが見つかっています。

マクロウイルスの真の危険性は、初のクロスプラットフォームウイルスである点にあります。長年、Macintosh コンピュータを狙ったウイルスは数十しか見つかっていなかったため、何千ものウイルスに狙われている Windows よりも比較的安全だと言われてきました。しかし現在、マクロウイルスが普及したことで、危険性は高まっています。

Microsoft Word を狙ったほとんどのマクロウイルスでは、AutoOpen、AutoClose、AutoExec および AutoExit などのコマンドを使用します。これらのコマンドは、ファイルに特定のイベントが発生したときに実行され、ファイルで作業を行うとこれら 4 つのイベントが必ず実行されます。たとえば、特定のメニューコマンドを選択したときに自己再生するようにマクロがプログラミングされている場合、繁殖の可能性はそれほど高くありません。

マクロウイルスの多くは、ユーザがファイルを開いたときに実行し、開いているテンプレートに自己繁殖します。このテンプレートはユーザ自身が開くものではありません。バックグラウンドでいつも開いています。このテンプレートには、ツールバーや後から追加した正式なマクロなど、ユーザ独自の情報が含まれています。



第 9 章- 付録

Microsoft Word を攻撃するもっとも一般的なマクロウイルスは、使用中のテンプレートに自らをコピーし、特定のメニューアイテムを変更するものです。したがって、ユーザはテンプレートを編集することも、ファイルの種類を変更する（テンプレート自体に見せかけるためにアイコンを変更する）こともできなくなります。その後、マクロウイルスは、破壊したテンプレートからユーザが作成または開いた新しいファイルに自己繁殖します。このウイルスをすぐに発見できれば、使用中のテンプレートファイルと感染ファイルを削除して、ウイルスを取り除くことができます。

他にも、もっと危険なマクロウイルスがあります。それらのマクロウイルスは、ファイルを破壊または削除したり、特定のアプリケーション機能を隠したりします。その上、それらはクロスプラットフォームウイルスのため、Macintosh コンピュータと Windows 搭載コンピュータの両方に被害をもたらす可能性があります。

MacMag

MacMag ウイルスは、意図が失敗に終わったよい例です。MacMag は、MacMag マガジンから発生しました。1988 年 3 月 2 日に、感染したコンピュータを起動すると、平和のメッセージを表示し、その後自らを削除します。これは元々、New Apple Products と呼ばれる HyperCard スタック（トロイの木馬）で、システムファイルに感染して広まります。現在ではほとんど見られなくなりましたが、古いディスクや CD-ROM に残っている可能性があります。

MBDF

このウイルスは、1992 年にウェールズで、Claris アプリケーションに搭載されているウイルスチェック機能によって発見されました。このウイルスは元々、10 Tile Puzzle や Obnoxious Tetris という



第 9 章- 付録

ゲーム、および Tetricycle というトロイの木馬から広まりました。ほとんどのウイルスとは異なり、MBDF ウイルスの作成者として米国の 2 人の学生が逮捕され、有罪判決を受けました。

このウイルスは、MBDF リソースを ID 0 でコピーして、アプリケーションとシステムファイルの両方に感染します。しかし、システムファイルにはすでにこの名前のリソースがあるため、リソースは変更されません。

このウイルスは悪質ではありませんが、システムファイルに損害を与えます。その場合、システムファイルをインストールし直さなければなりません。また、特定のメニューに損害を引き起こすこともあります。このウイルスには、MBDF A と MBDF B という 2 つの変種があります。これら 2 つは本質的に同じです。

MDEF

MDEF ウイルスには、A、B、C、D の 4 つの変種があります。A は Garfield ウイルスとも呼ばれ、また B は Top Cat ウイルスとも呼ばれます。これらのウイルスは、1990 年と 1991 年にニューヨーク州のイサカで発見されました。このウイルスの作成者は、ウイルスの発見直後に逮捕されました。この作成者は CDEF の作成者でもあります。

MDEF という名前は、MDEF リソースを使って繁殖することに由来します。通常、MDEF リソースは、特定のアプリケーションとシステムファイルにあります。したがって、MDEF ファイルがあるからといって、そのファイルが必ずしも感染しているわけではありません。



第9章- 付録

このウイルスは、アプリケーションとシステムファイルの両方を攻撃します。また、ドキュメントやデスクトップファイルにも感染します。特に悪質な損害を及ぼすように作成されていませんが、無害ではありません。アプリケーションやファイルの中には、このウイルスが原因で破損するものもあります。

MDEF 666

SevenDust を参照。

MDEF 9806

SevenDust を参照。

MDEF 999

SevenDust を参照。

nVIR

nVIR ウイルスは、1987年にヨーロッパで発見されました。主に、nVIR A と nVIR B という2つの変種があります。また、このウイルスは AIDS、Fuck、Hpat、Jude、MEV#、nFlu という名前でも知られています。

このウイルスは、悪質な損害を引き起こしませんが、システムファイルやアプリケーションに感染して自己繁殖します。このウイルスは、ビープ音を鳴らすか、または MacinTalk がインストールされて



第 9 章- 付録

いるコンピュータでは「Don't panic」という音声を鳴らすことがあります。これらのイベントは、コンピュータを起動したときに不意に発生します。

Scores

Scores は、Eric、Vult、NASA、San Jose Flu ウイルスとしても知られ、1988 年に米国で初めて発見されました。このウイルスの作成者は、ウイルスの動作を学ぶためにこのウイルスを作りましたが、このウイルスはすぐに広まりました。このウイルスは、Scores と Desktop という 2 つの不可視ファイルを作成し、システムファイルに感染します。また、NotePad や Scrapbook ファイルのアイコンを変更して、これらのファイルを破壊します。このウイルスは、コンピュータ上で実行している他のアプリケーションにも感染しますが、すべてのアプリケーションに感染するとは限りません。また、コンピュータを不意にクラッシュさせたり、印刷上の問題を引き起こしたりすることもあります。

SevenDust

SevenDust ウイルスには、A から G まで複数の変種があります。また、MDEF 9806 や MDEF 666 という名前でも知られています。これらのウイルスは、MDEF、MENU、WIND リソース、およびその機能拡張に感染します。SevenDust E は、Graphics Accelerator と呼ばれ、元々 1998 年に見つかったトロイの木馬でした。

このウイルスのファミリーは、アプリケーション、システムファイル、コントロールパネルに感染します。これらのウイルスは、毎月 6 日と 12 日の午前 6~7 時にコンピュータを実行していると、起動ボリュームにあるアプリケーション以外のファイルをすべて削除しようとします。



第 9 章- 付録

SevenDust F は、ExtensionConflict と呼ばれるトロイの木馬として広まりました。また、このウイルスには、5 つの亜種があり、他の機能拡張を通じて広まります。

SysX

INIT 9403 を参照。

T4

T4 ウイルスは、1992 年に発見されました。GoMoku バージョン 2.0 および 2.1 の一部として、7 つの FTP サイトにアップロードされました。このウイルスは、アプリケーションと Finder に感染し、システムファイルを改ざんしようとします。また、「Disenfectant」というフリーウェアのアンチウイルスプログラムを装って、他のアンチウイルスプログラムを欺きます。

このウイルスは、システムファイルに修復不可能な危害を加える可能性があり、コンピュータを不意にクラッシュさせます。また、このウイルスに感染すると、コンピュータをブートできなくなることがあります。

1997 年、T4-D という変種が見つかりました。このウイルスは、システムフォルダにあるファイルやドキュメントを削除しますが、システムファイルは削除しません。T4-D は、アプリケーションの CODE リソースに自己再生して、アプリケーション間で繁殖します。



WDEF

WDEF ウイルスは、1989 年にベルギーで発見されました。WDEF という名前は、デスクトップファイルにある WDEF リソースに由来します。WDEF A と B という 2 つの変種があり、WDEF ファイルに感染して広まります。システムは、マウントしたすべてのディスクのデスクトップファイルを読み込むため、アプリケーションを実行しなくても、すぐに広まります。

このウイルスは、コンピュータに悪質な損害を引き起こしませんが、プログラミング上のエラーがあるため、クラッシュやフォントの表示エラーといった問題が発生する可能性があります。

ZUC

ZUC ウイルスは、1990 年に発見されました。その名前は、発見者の Don Ernesto Zucchini に由来します。このウイルスには、ZUC A、B、C という 3 つの変種があります。いずれもアプリケーションのみに感染し、アプリケーションを実行しなくても広まる可能性があります。これらのウイルスによって、カーソルの動作が不安定になる場合がありますが、他には損害を引き起こしません。

