V3 Pro 2000 Deluxe

for Windows 9x / NT (Workstation) / 2000 (Professional)

Version 4.02 SP2

ユーザーズガイド

안철수컴퓨터바이러스연구소
DR.AHN'S ANTI-VIRUS LABORATORIES, INC.

2000年4月10日　第二版　発行
開発元：Dr. Ahn's Anti-Virus Laboratories, Inc.

テクニカル・カスタマーサポート／ウイルス届出・お問い合わせ

住所:　Dr. Ahn's Anti-Virus Laboratories, Inc.
10th Fl., SamHwa Bldg.,
144-17, Samsung-dong, Kangnam-gu,
Seoul, 135-745, Republic of Korea

インターネット:　http://www.ahnlab.com

電話:　82-2-2186-6000（代表）
82-2-558-7400（カスタマーサポート センター）
82-2-558-7566（ウイルス届け出センター）

Fax:　82-2-2186-6100（代表）
82-2-558-7567（カスタマーサポート センター専用）

前置き

注

このガイドはV3Pro 2000 Deluxeご購入のお客様のために作られた本です。最初から最後までお読みください。V3Pro 2000 Deluxeに関する使い方だけではなくコンピュータウイルスに対する対処能力も一層高まります。

ガイド構成

ユーザーズガイドは本文5章で構成されています。1章にはカスタマーサポート及びプログラムのお使いになる前に知っておくべき内容が入っています。2章にはV3Pro 2000 Deluxeの特徴とインストール方法が、3章には概要が、4章では使い方が、5章では便利なツールとWebリンクについて説明されております。

ガイドの表記及び規則

このガイドは日本語専用を原則にしましたが、ただし必要な場合はアルファベットで表記します。

本文での「Dr. Ahn’s Anti-Virus Laboratories」は「Dr. 安研究所」または「安研究所」に、「コンピュータウイルス」は「ウイルス」に、「NTワークステーション」は「NT」に、「Windows 2000 Professional」は「2000」に略して表記します。また、V3製品シリーズはV3シリーズに略して表記します。

規則

表記	内容
NT/2000	Windows NT (Workstation) / 2000 (Professional) に当たる内容です。
参照	説明またはヒント、例外、ショットカット方法などを説明します。
注意	予想できない状況や大きな損失を被るかもしれない状況に対する警告項目です。

アルファベット大文字	ディレクトリ、パス、ファイル名などを表します。
太字	メニュー、ダイアログ窓、オプションなどを表します。
<Key1>+<Key2>	<Key1>を押している状態で<Key2>を同時に押します。
<Key1>→<Key2>	<Key1>を押した後<Key2>を押します。
太字1 → 太字2	太字1をクリックした後太字2をクリックします。

目次

第1章

はじめる前に

- ユーザー登録及びサポートサービス
- お問い合わせとテクニカルサポート
  - 新種ウイルスを発見した場合
- V3Pro 2000 Deluxeご利用の注意点

ユーザー登録及びサポートサービス

Dr.安研究所はV3シリーズのテクニカルサポートを始めカスタマーサポート、ウイルスのお問い合わせまで登録ユーザーのために様々なサービスを提供いたします。

ユーザー登録は必ず行ってください

V3Pro2000Deluxeご購入の方は必ずユーザー登録を行ってください。新しいウイルスが続いて発見されているのでDr.安研究所のV3シリーズは一般プログラムとは違って、持続的なアップデートが必要です。そこで、毎週1回アップデートされ、登録ユーザーのために別途のサービスを提供しつづけています。しかし、ユーザー登録が確認できないと製品ご購入のお客様でもカスタマーサポートサービスを受けることができません。ご購入後、必ずユーザー登録を行ってください。

インターネットを通じてオンライン ユーザー登録をなさると便利です

V3シリーズの中に含まれているユーザー登録カードを送ってくださるとカスタマーサポート担当に受け付けされるまで時間が掛かりますので、その間お客様はサービスを受けられません。それで、インターネットご利用のお客様はインターネットWebサイトを通じてオンライン加入なさるとより早くサービスを受けられます。

Dr.安研究所のwebサイト(http://www.ahnlab.com)でお客様専用フォーラム--オンラインユーザー登録メニューを利用なさるとご加入できます。ただし、インターネットが利用できないお客様は製品パッケージに含まれているユーザー登録カードにお名前、郵便番号、住所、電話番号、現在ご利用のパソコン通信IDなどユーザー情報を正確に記入し、郵便またはファクス(82-2-558-7567)にてお送りください。

カスタマーサポート期間は登録から1年間です

V3シリーズのカスタマーサポート期間は登録から1年間です。登録から1年が過ぎると週一回の定期エンジンアップデートサービスを含めて登録ユーザーに提供されるサービスが中止されます。

登録ユーザーには様々なサービスが提供されます

登録ユーザーには登録期間中次のような様々なサービスが提供されます。

- 週一回の最新アップデートサービス
- e-mail／インターネット／パソコン通信／郵便／電話による相談サービス
- 登録期間中アップグレードすると、同じ製品は無料アップグレードサービス

- Webマガジン "Dr. Ahn's Anti-Virus News"
- 年一回、ウイルスカレンダー提供サービス
- e-mailによる様々なニュース提供サービス
- Anti-Virusセミナー、教育プログラム開催時、無料参加サービス

登録更新方法

ワクチンプログラムは何より迅速なアップデートが重要です。そこで、V3シリーズは一週間間隔の迅速なアップデート周期を持っており、持続的な研究、開発に投資しています。その為に他のプログラムとは違って1年という登録有効期限があります。

カスタマーサポートサービスは登録後1年が過ぎると、それ以上サポートを受けられませんので、システムが新種ウイルスの危険にさらされる恐れがあります。従って登録期限を過ぎているお客様は必ず登録更新をなさってウイルスからコンピュータを安全に保護してください。

登録更新が近付いているお客様にはe-mailで登録更新案内メールをお送りします。もし受け取っていないとか、登録更新手続きに関してより詳しい内容をお求めの方はDr.安研究所インターネットWebサイトのカスタマーサポート メニューを参考なさってください。

V3Pro 2000 Deluxeエンジンアップデート方法

V3Pro 2000 Deluxe登録ユーザーには、一週間間隔で(毎週水曜日前後)最新のエンジンアップデートファイルをカスタマーフォーラムからダウンロードできる権限をお送りします。

登録ユーザーにはアップデート案内メールを一週間間隔で定期的にお送り致します。アップデート案内メールを受け取った後、インターネットご利用の方はインターネットWebサイト (http://www.ahnlab.com)の中のカスタマーフォーラムを。インターネットご利用のお客様はV3Pro 2000 Deluxeプログラムに入っているスマートアップデート機能をご利用なさって、[アップデート]ファイルを直ちにダウンロードできます。

> **参考**: 登録更新とは既にV3シリーズを購入して、登録済みのお客様に提供されるサービスとして、エンジンアップデートサービスをまた1年間受ける場合、新規ユーザーより50%引きの値段で製品がご利用できる[登録ユーザー割引制度]です

お問い合わせとテクニカルサポート

V3Pro 2000 Deluxeご使用中、知らないことがあれば、まずこのユーザーズガイドをお読みください。その他、お問い合わせは次のe-mail、インターネットホームページ、パソコン通信フォーラム、電話、ファクス、郵便をご利用ください。

インターネット

Ahn’s Lab Web Site: www.ahnlab.com

カスタマーサポート担当　E-mail住所及びID

インターネット: customer@ahnlab.co.kr

郵便、電話、Fax

Customer Support Representative
Dr. Ahn’s Anti-Virus Laboratories, Inc.
10th Fl., SamHwa Bldg.,
144-17, Samsung-dong, Kangnam-gu,
Seoul, 135-745, Republic of Korea

電話 : 82-2-558-7400 (カスタマーサポートセンター)
Fax : 82-2-558-7567

新種ウイルスを発見した場合

新種ウイルスだと疑われるとDr.安研究所にお問い合わせください。

新種ウイルスに感染した場合、また感染が疑われるとき、V3シリーズではなく別のワクチンプログラムでウイルスを発見した場合はDr.安研究所のウイルス届け出センターまたはカスタマーセンターに問い合わせてそのデータを送ってください。頂いたファイルは迅速に分析してウイルス感染有無を確認して新種ウイルスとして確認された場合は、一番早いワクチンアップデートサポートで被害を最小限度に収まるように致します。

ファイル(マクロウイルスを含めて)ウイルスとブートウイルスを採取する方法は次の通りです。 (付録「DOS用V3+Neoについて) 参照)

- **ファイル(マクロ)ウイルス採取方法** - ファイル(マクロ)ウイルスは実行するファイルに感染するので感染が疑われるファイル(マクロウイルスの場合MS-office関連ファイル)などを送ってください。
- **ブートウイルス採取方法** - V3Pro 2000 Deluxeが提供するブート領域バックアップ機能を利用するか、または DOS用 V3+ Neoに入っているブートウイルス採取ユーティリティであるV3BACKUP.EXEを使えば、(例　C:¥V3BACKUP <drive name>)簡単にブートウイルスを採取できます。

ただし、DOS用プログラムV3BACKUP.EXEを使う場合は新しいDOSディスクで起動した後、実行してください。実行した後作成されるMBS.V3とDBS.V3ファイル(フロッピディスクの場合はFBS.V3ファイル作成)をウイルス届け出センター担当に送ってください。

インターネット

Ahn's Lab Web Site: www.ahnlab.com

ウイルス届け出センター担当e-mail、ID

インターネット: webmaster@ahnlab.co.kr

郵便、電話、Fax

Virus Reporting Center Representative

Dr. Ahn's Anti-Virus Laboratories, Inc.
10th Fl., SamHwa Bldg.,
144-17, Samsung-dong, Kangnam-gu,
Seoul, 135-745, Republic of Korea

電話 : 82-2-558-7400 (ウイルス届出／お問い合わせ)
Fax : 82-2-558-7567

ユーザー登録とアップデート

1. 必ずユーザー登録を行ってください。

または 2 の方法でユーザー登録を行ってください。

1. オンライン ユーザー登録

   http://www.ahnlab.comに接続→"Online Registration"選択

2. ユーザー登録カードで登録
   製品に含まれているユーザー登録カードに記入し、FAX(82-2-558-7567)または郵便で送る。

参照: パソコン通信ではユーザー登録を受け付けていません。

2. ユーザー登録をしなければならない重要な理由

－新種ウイルスが続いて発見されているのでワクチンは短い周期でアップデートしなければなりません。V3Pro 2000 Deluxeのエンジンアップデートファイルは製品ご購入のお客様だけが利用できるファイルなので、ユーザー登録をしてからワクチンをアップデートできます。最新バージョンこそ新たに発見されるウイルスを診断・治療できます。

3. 必ずアップデートなさってください。

－ユーザー登録を済ませた方だけがエンジンアップデートファイルを次の方法でダウンロードできます。 (1.2.3.の中でお好みの方法を選んでください。)

1. Dr.安研究所 web サイトからアップデートファイルをダウンロード

   a. http://www.ahnlab.comに接続してカスタマーフォーラムの「会員」メニューを選択します。
   b. usernameとpasswordを入力します。
   c. 統合エンジンを選択してファイルをダウンロードします。
   d. ダウンロードしたファイルをエクスプローラでダブルクリックします。
   e. V3Pro 2000 Deluxeを実行してエンジン日付が最新のものに変更されているか確認します。

2. スマートアップデート機能を使う

   a. V3Pro 2000 Deluxeを実行します。
   b. スマートアップデート ユーティリティを実行してスマートアップデート開始ボタンを選択します。
   c. V3Pro 2000 Deluxeを終了して再起動するとアップデートが完了します。

参照: スマートアップデートはインターネットに繋がっている状態で実行してください。

V3Pro 2000 Deluxeご利用の注意点

情報が含まれていない新種ウイルスは検査できません。

V3Pro 2000 Deluxeは今まで韓国で発見されているコンピュータウイルスと他の国で発見されている破壊力の強い外国ウイルスが検査・治療できます。しかし、新種ウイルスはV3Pro 2000 Deluxeにその情報が含まれるまでには検査できません。(他のワクチンプログラムも同様です。)また、それによって被ったウイルス感染と被害についてはDr.安研究所では責任を負いません。従って、コンピュータウイルス感染に完璧に対処するためにはワクチンプログラムに頼るだけではなく大事な資料は予めバックアップ（コピ）しておくなど他の予防方法を併用するのが望ましいです。

治療不可能ファイルもあります。

V3Pro 2000 Deluxeでコンピュータウイルスに感染したファイルを治療するとほとんど感染する以前の状態に戻ります。しかし新種変形ウイルス、上書きウイルス、複合感染、感染したマクロファイルを実行した場合は正常に治療できないこともあります。即ち一個のファイルが複数のウイルスに同時に感染して壊れているか、ファイル感染と共にファイルを壊す上書き型ウイルスに感染した場合、また感染したマクロファイルが実行されて（または開いている）いる場合も治療できません。従って、治療する前にウイルスに感染したファイルは必ずバックアップまたは終了した後、治療してください

必ず毎週提供されるアップデートサービスを受けてください。

Dr.安研究所のV3シリーズは現在まで販売されているワクチンの中で一番短いアップデート周期を保っています。(一週間間隔)その理由は一週間の間にも新しいウイルスが続けて登場する現実を考慮したもので、新種ウイルスに素早く対処することでコンピュータウイルスから被害を最小限度にします。登録ユーザーはDr.安研究所が週一回提供するアップデートサービスを受けると登場し続けている新種ウイルスに迅速に対処できます。また、悪性ウイルスが登場すると緊急アップデートサービスが随時提供されるので緊急な場合も素早く対処できます。

参照：ワクチンは一度組み込んだ後も最新バージョンにアップデートしてからこそ新種ウイルスの侵入からお客様のシステムを安全に保護することができます。

参照：悪性新種ウイルスが出現すると、Dr.安研究所では24時間以内に緊急アップデート サービスを随時提供いたします。

第2章

V3Pro 2000 Deluxeの特徴とインストール

- 特徴
- 必要システム環境及び構成
- インストール
- V3Pro 2000 Deluxeの削除

特徴

V3Pro 2000 DeluxeはDr.安研究所が開発したWindows 9x/NT (Workstation) / 2000 (Professional)のコンピュータウイルスワクチンプログラム(Anti-Virus Program)です。V3Pro 2000 Deluxeは海外の数多くのワクチン製品の中で一番早くて強力なAnti-Virus機能を提供するだけではなく、インターネットから受信する各種データ及びファイルのウイルス感染有無を監視・診断・治療する強力なワクチンプログラムです。V3Pro 2000 Deluxeは世界的なワープエンジン(WARP engine)を持っていて誤診する可能性はほとんどなく、感染したファイルの治療に当たっては優れたファイル復元能力を誇りにしています。

V3Pro 2000 Deluxeの特徴は次の通りです。

インターネットを通じて流れ込むウイルスを完全に遮断

インターネット監視機能はシステム監視機能と統合されてインターネットを通じて入ってくるデータのウイルスの感染有無を監視、ウイルスを発見した場合は完璧な診断・治療機能を提供しています。

ウイルス監視・自動治療機能

知能的なウイルス監視(予防)システムを採用、作業中ウイルスを発見するとシステム次元でウイルスの活動を阻止した後、すぐ自動的に感染ファイルを治療します。システム監視機能は特にウイルスを完全封鎖するのにとても優れている性能を持っています。その上システムのスピードにはほとんど影響を与えないのがV3Pro 2000 Deluxeの重要な機能です。

強力なワープエンジン(WARP Engine®)

Dr.安研究所によって独自的に開発された優れもののワープエンジンを採用して、Windows 9x / NT (Workstation) / 2000 (Professional) のシステム領域だけではなくDOSメモリ領域まで徹底的に検査することでシステムを安心してご使用なれます。また、韓国及び海外のワクチンの中で検査スピードが一番速くて完璧な治療成功率を持っており、感染したファイルの治療に当たって優れたファイル復元能力を誇りにしています。

Dr.安研究所独自の技術で開発されたワープエンジン(WARP Engine®)はウイルス診断と治療、予防技術が統合されたワクチンソフトの核として次のような長所を持っています。

- **ウイルスに即時対応するAnti-Virus機能** - 最近まで発見されている韓国製ウイルスについて100%診断・治療機能を提供するだけではなく、韓国及び海外に広範囲に広がっているウイルス、そして海外から最近流れ込んだ悪性ウイルス (特にCHI及びMelissa、ExploreZip、Back Orifice等) までも完璧に診断・治療します。

韓国特許及びKTマーク獲得でその高品質が公認された WARP Engine®の意味と由来

WARP Engine®の“WARP”は映画“STAR TREK”から取ったもので、主人公たちが乗る連邦宇宙船に搭載されている超光速推進エンジンをいいます。映画に因れば、いわばワープドライブシステムは光より速いスピードで旅行したり空間移動をする威力的なパワーを持っているといいますが、Alpha Centauri(太陽系から一番近い惑星)から来た Zefram Cochraneという科学者が2061年に発明したそうです。

Dr.安研究所のV3シリーズに搭載しているAnti-Virusエンジンは「世界的に一番早くて正確な治療(復元)率を提供する」という意味で「ワープ」(WARP: World-class Accelerated Recovery Processor)という名前になりました。Dr.安研究所はWARP Engine® のこのような特性をより強化して、他のワクチンとは異なる独自の技術でワクチンソリューションを提供してきました。

- **感染ファイル治療に当たって、優れたファイル復元能力** – ウイルスに感染したファイルの治療に当たって、優れたファイル復元能力を誇りにしています。従って、元のファイルが壊れる被害を最小限度に止めます。
- **一番早い診断・治療速度** – Dr.安研究所独自のワクチンアルゴリズム（特定位置検査技術：ウイルス感染可能性のある領域だけを選んで検査する追跡アルゴリズム）設計として現在出されているワクチン製品の中で一番早い診断・治療性能を提供しています。
- **韓国内、未発見ウイルス診断機能** – 韓国では現在発見されていない外国製ウイルス一万種余りについても診断機能を提供することで新種ウイルスの流れ込みにも徹底的に対処しています。

迅速なアップデートで新種ウイルスを撃退

V3Pro 2000 Deluxeを含めてDr.安研究所のV3シリーズは今まで出された韓国と海外のワクチンの中で一番短いアップデート周期（週一回）を持っています。またユーザーが自分でアップデートする不便を無くすためにプログラム内部に自動アップデートシステムであるスマートアップデート(Smart Update)サービスが入っています。スマートアップデートを実行するとDr.安研究所のインターネット アップデートサービスホストを通じてエンジンアップデートファイルを自動的にダウンロードしてご利用いただけます。

ウイルスを発見した際、確実で安心できる治療オプション

検査結果、ウイルスに感染しているのが確認されると、すぐ自動治療は勿論治療によって安全な対処法を提供します。即ち、ユーザーの選択オプションによって、治療を試みる前に万が一起こるかも知れないファイル破壊に備えて元のファイルを別のバックアップフォルダに保存します。治療不可能ファイルの場合は、自動削除してウイルスの拡散に備えます。

これもまた削除する前にバックアップフォルダに保存して万が一の場合に備えます。

一方、フロッピディスクにアクセスするとかWindowsが終了するときブートウイルス感染有無を予めチェックできるのでヴーとウイルスの流れ込みを完全に塞げます。

効率的な防疫・管理のための様々な付加機能

信頼度の高いウイルス分析、研究結果に基づいたウイルス関連情報を集めたウイルス情報データベースとさらにウイルスカレンダーも入っていて年中、特定日に発病するウイルスに前もって備えることができます。

また、ユーザーがウイルス感染に対処できるように検査記録情報、また各種便利なツールメニュー、お客様の便宜を図った多彩な環境設定オプション、インターネットを通じてのオンラインユーザー登録機能を提供することで状況に合わせてより柔軟な防疫管理ができます。

Windows NT Workstation 及び Windows 2000 使用の注意事項！

1. マニュアルの中でブート領域と関連する部分は NT(Workstation)と Windows 2000 には当てはまりません。
2. マニュアルの中でSOSディスク作成機能は NT(Workstation) 及び Windows 2000 には当てはまりません。
3. マニュアルの中でスマートアップデート機能は NT(Workstation) 及び Windows 2000 (プロフェショナール)に管理者権限のお持ちのユーザーがログインした状態の上でだけ実行できます。

必要システム環境及び構成

必要システム環境

V3Pro 2000 DeluxeはWindows 9x / NT (Workstation) / 2000 (Professional)用のワクチンプログラムです。V3Pro 2000 Deluxeを実行するために必要なシステム環境は次の通りです。

- Intel Pentium 133MHz以上のIBM PC互換機種
- 64MB メモリ以上
- VGA以上のグラフィックカードとモニター
- 10MB以上のハードディスクの空きスペース
- Windows 9x / NT (Workstation) / 2000 (Professional)
- CD-ROMドライブ(24倍速以上推薦)
- マウス

プログラム構成

プログラムを構成するフォルダの技能は次の通りです。

フォルダ名	説明
UPDATE	アップデートファイル
BACKUP	感染したファイルをバックアップするフォルダ
TEMP	V3Pro 2000 Deluxeが一時的に使うフォルダ
TXT	Dr.安研究所から受け取ったメッセージ
SYSTEM	V3Pro 2000 Deluxeで使われるシステムファイル
LOGWIN	検査記録保存フォルダ

製品構成

V3Pro 2000 Deluxeパッケージの中にはCD-ROM1枚、ユーザーズガイド、ユーザー登録カード、ライセンス証書が入っています。CD-ROMの中にはWindows 9x / NT (Workstation) / 2000 (Professional)用のV3Pro 2000 DeluxeとDOSバージョンのV3+Neoが含まれています。DOS用のV3+NeoはOSを新しくインストールするとか、または再起動できない場合安全にウイルス検査をする為に入っています。

V3Pro 98とV3Webより新しくなった機能

1. 早くなった検査速度

検査過程をより効率的に改善して検査するときより早くなったスピードを感じられます。

2. V3Webの統合でインターネット監視機能安定化

V3Pro 98とV3Webが完全に統合されてシステム監視機能と共にインターネットからのウイルスの流れ込みを徹底的に監視します

3. スマートアップデート機能強化

複数のアップデートサーバーを準備してより早くアップデートサービスを受けられます。

4. ブートウイルス完全封鎖のためにフロッピドライブアクセスのとき自動検査

もしブートウイルスに感染したフロッピディスクを入れてシステムを終了した後、システムを再起動するとまずフロッピディスクにアクセスします。その過程でブートウイルスはハードドライブを感染させます。その後、フロッピディスクを取り除いても既にハードドライブに入ったブートウイルスによる被害は防げません。このようなウイルスの接近を完全に統制するために、フロッピドライブアクセスのとき検査機能を付け加えた上に、Windowsが終了するときもフロッピディスクが入っていれば、ウイルス検査をしてより安全なAnti-Virus環境が保てます。

5. 「快速検査バー」を取り入れて検査方法の多様化

ユーザーが自分で検査対象を直接入力して検査できる機能です。それで、様々な検査方法によってより柔軟な防疫管理ができます。

6. システムが使用中であるファイルも治療可能

Windowsシステムが使用中であるファイルを治療できます。V3Pro 2000 Deluxeが感染ファイルを強制に終了した後、治療を試みます。強制終了した場合は自動的に実行しないし、終了しなかった場合も実行中であるファイルを別にコピして治療した後、再起動するとき治されたファイルで交替するのでWindowsシステムが使用中であるファイルも安全に治療できます。

7. バックアップ管理及び自動送信機能強化

感染したファイルを別のバックアップフォルダに保存してファイル損傷など万が一の場合に備えます。もし新種ウイルスの場合にはDr.Ahn’s 研究所のウイルス届け出センターにすぐ送信し、直ちにワクチンアップデート サポートを受けられるようにします。

8. ワクチンの全活動追跡可能

イベント記録及びメッセージメモではシステム／インターネット監視、アップデート実行、ウイルス検査、Dr.安研究所からのメッセージなどの情報が記録されており、ワクチンの全活動が追跡できるのでより安全にシステムが管理できます

9. Neo Scan機能

現在実行中であるWindowsシステムを強制に終了し、DOSで起動してwindowsがまた実行される前にV3+ Neoですべてのハードディスクを検査する機能です。特にWindowsシステムが使用中であるファイルの場合、確実な防疫管理を保証します。

10. Web LinkとOffice Protector機能

Dr.安研究所に直接繋げるWeb Link機能とMicrosoft Office 2000、Microsoft Internet Explorer 5.0に対するプラグイン機能が追加されました。

11. インターネット ポート検査機能追加

インターネット御利用の際、使われているポートなどを検索してBack Doorプログラムが実行中であるかを検索します。ウイルスが使っているようなポートを発見すると警告メッセージを出力する機能です。

12. レジストリ治療エンジン追加

PrettyParkのようにレジストリ値を改ざんするなどWindowsシステムを任意に変更するウイルスの場合、その治療のために別個のバッチファイルを実行しなくてもV3エンジンだけで直ちに治療できます。

13. 実行中であるプログラム検査機能追加

Back Doorプログラムが実行されながら動作するウイルスが増えていることに対応してファイル検査をする前に現在システムで実行されているプログラムを常に検査する機能です。

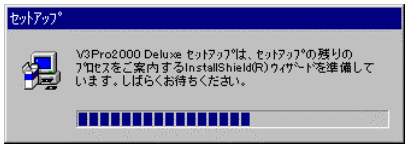
14. 完璧なWindows 2000支援

システム監視機能を強化してWindows 2000シリーズをより完璧に支援しています。

インストール

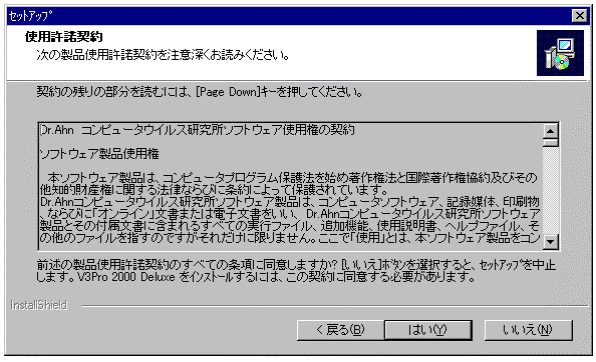
Windows 9x / NT (Workstation) / 2000 (Professional)の「スタート」ボタンをクリックして「ファイル名を指定して実行」を選択します。 名前(O)にCD-ROMドライブ名とインストールプログラム名を入力します。(普通、V3Pro 2000 Deluxeは自動的にインストールが実行されます。自動的に立ち上がらないようにするためには<Shift>キーを押してCD-ROMを入れれば自動実行しません。)

即ち、「D:¥setup.exe」を入力した後、「OK」をクリックすれば,V3Pro 2000 Deluxeのインストール プログラムが実行され、その過程が次々と表示されます。



V3Pro 2000 Deluxeインストール手順

1. V3Pro 2000 Deluxeの著作権を確認するダイアログ ボックスが表示されます。使用許諾契約書の内容に同意し、インストールを続けるためには「はい(Y)」を押してください。



2. V3Pro Deluxeをインストールする前に、システムにウイルスがあるか検査することを先に訪ねます。まずシステム内の「すべてのフォルダ」または「システムフォルダ」、それとも「検査しない」を選択しま

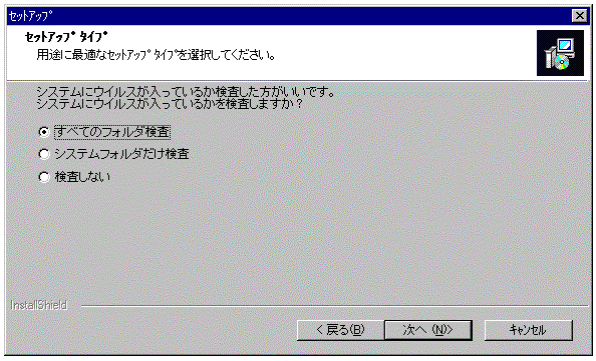
旧バージョンの製品または他社のワクチンソフトが組み込まれている場合

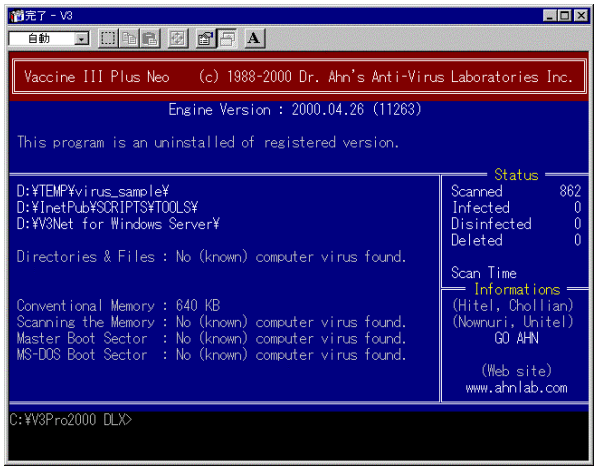
V3Pro 2000 Deluxeをインストールするためにはシステムに入っているV3シリーズを削除しなければなりません。もし以前のバージョンが組み込まれていれば、「削除しますか」と尋ねる画面が現れます。（他のワクチンも同じ手順でインストールするかを確認します。）

はい(Y)をクリックして、以前のバージョンを削除した後インストールしてください。

参考: 既に入っている他社のワクチン含めてワクチンプログラムを削除しなければ、V3Pro 2000 Deluxeは正常にインストールできません。

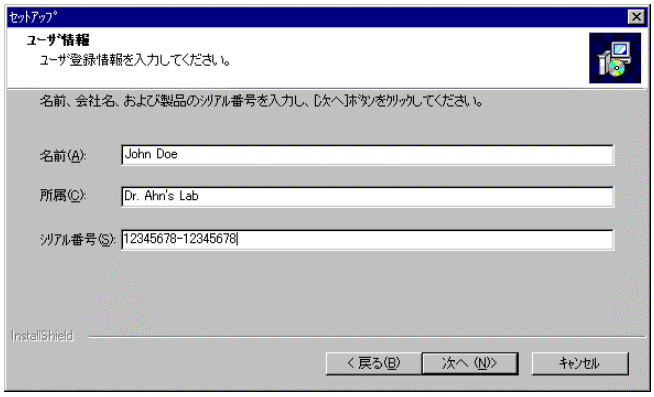
す。システムにウイルスがあるかを検査するためには検査対象を選択した後「はい(Y)」をクリックします。すると、V3Pro 2000 Deluxeに含まれているV3+Neoが実行され、システムにウイルスがあるか否かを検査した後、DOSプロンプトを閉じるとWindowsに戻って続けてインストールを行います。



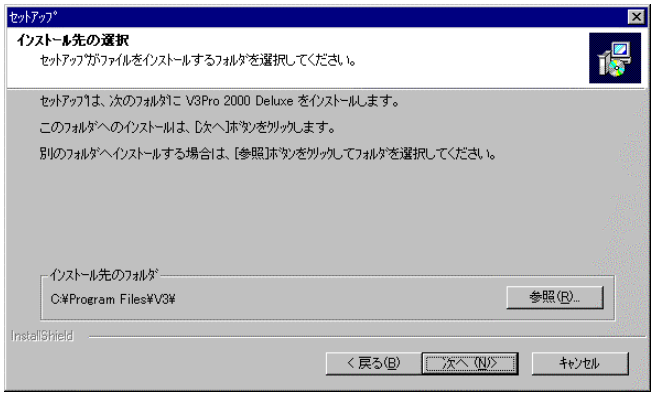


3. V3Pro 2000 Deluxeの著作権を確認するダイアログ ボックスが表示されます。それに、「インストールを実行する前にすべてのWindowsアプリケージョンを終了してください。」というメッセージも出ます。「次へ(N)」をクリックすると次の段階に移ります。もし他のWindowsアプリケーションが開いてあれば、そのプログラムを終了してからインストールを始めなければなりません。

4. ユーザー情報を入力します。お名前、所属団体、会社、シリアル番号(製品番号)を記入します。シリアル番号はユーザー登録カードのステッカに書いてある番号を入力してください。



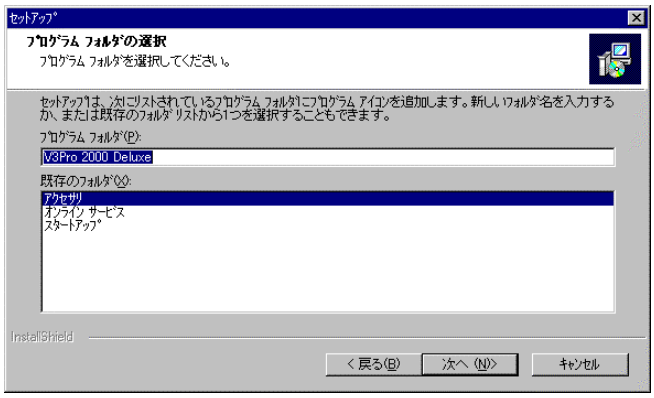
5. V3Pro 2000 Deluxeをインストールするフォルダを選択します。インストール先は「C:¥Program Files¥V3」になっています。もし他のフォルダにインストールする場合には、「参照(R)」をクリックして他のフォルダを選択します。インストール先を「C:¥Program Files¥V3」にする場合は6)から進めます。



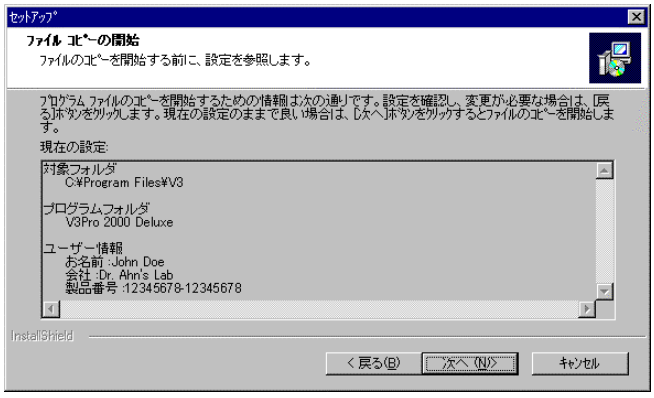
6. 上の4.で「参照(R)」をクッリクすると、フォルダを指定できます。

7. インストール先を選択したらプログラムフォルダを選択します。プログラムフォルダはV3Pro 2000 Deluxeになっています。新しいフォルダ名

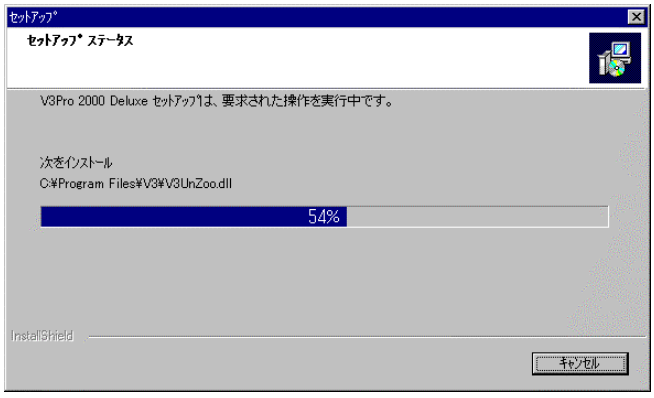
を入力するか、既存のフォルダの中で一つを選択した後、「次へ(N)」を押せば、インストールが続きます。



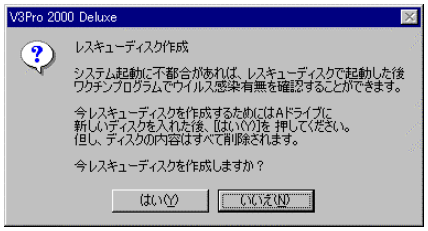
8. V3Pro 2000 Deluxeをインストールする前に現在設定されている内容を確認します。もし設定内容をやり直すか、変更する場合には「戻る(B)」をクッリクする。そのままでよければ、「次へ(N)」をクリックして続けます。



9. V3Pro 2000 Deluxeのインストールを始めます。

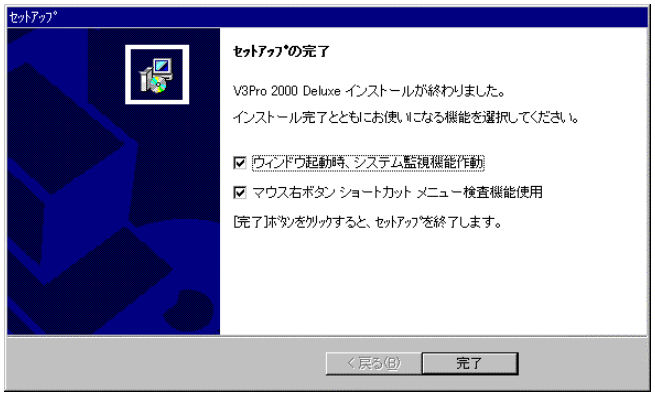


10. インストールが終わる前にSOSディスクの作成を尋ねます。



SOSディスクを作成するにはAドライブにフロッピディスクを入れて、「はい(Y)」をクリックするとフォーマットウィンドウが表示されます。フォーマット形式とオプションを指定した後、「スタート(S)」をクリックすると、フォーマットを始めます。フォーマットが終わると「閉じる(C)」を選択してSOSディスクを作成します。この時フロッピディスクの既存のデータはすべて削除されるのでフォーマットする前に中身を必ず確認してください。(Windows NTではSOSディスク作成を尋ねません。)

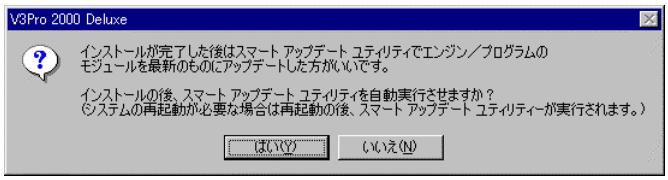
11. これで、V3Pro 2000 Deluxeの組み込みが終わります。「Windows起動時システム監視開始」「マウス右ボタン、ショットカットキー メニュー検査機能の使用」の機能をすぐ使うなら、「完了」をクリックしてください。 すぐ使用しない場合はそのオプションのチェックをオフにしてから「完了」を押してください。



12. 「完了」をクリックするとインストールが終わります。

> **参照**：「Windows起動時システム監視機能開始」をオンにすれば Windows98/95/NTのシステム監視機能が作動してウイルスの侵入を監視・予防中であることを表示するアイコンが現れます。

13. インストール過程が終わるとスマートアップデート ユーティリティを実行するかを尋ね、最新バージョンにアップデートします。

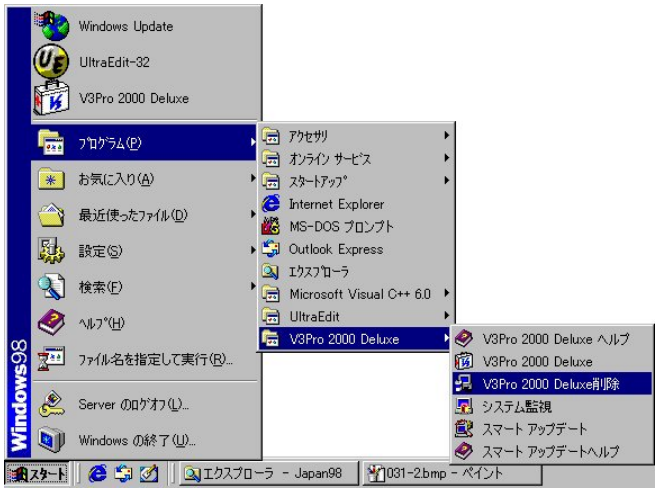


V3Pro 2000 Deluxeの削除

既にV3Pro 2000 Deluxeが組み込まれているフォルダに再びV3Pro 2000 Deluxeをインストールする場合、既存の組み込まれているプログラムを削除してからプログラムをインストールするのが安全です。V3Pro 2000 Deluxeにはアンインストール ユーティリティが含まれているのでこれを使えば、簡単に削除できます。

V3Pro 2000 Deluxeの削除手順

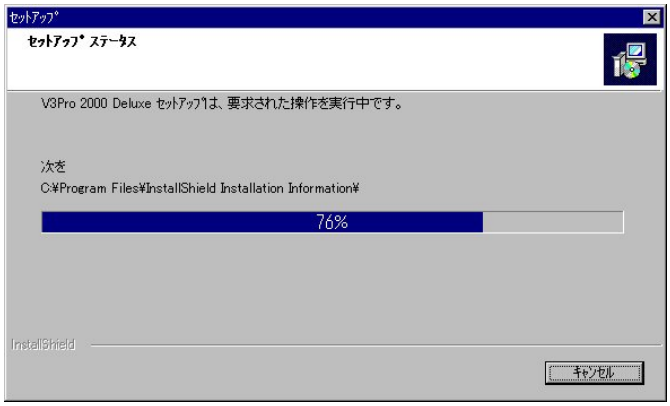
1. まず、V3Pro 2000 Deluxeプログラムフォルダで「V3Pro 2000 Deluxe削除」をクリックします。



マウスで「スタート」を押した後、「プログラム」－「V3Pro 2000 Deluxe」－「V3Pro 2000 Deluxe削除」の順でマウスポインタを移動します。

2. 次のような質問に「はい(Y)」をクリックして削除を始めます。

3. 次のような手続きを表示して、V3Pro 2000 Deluxeの構成要素を削除します。



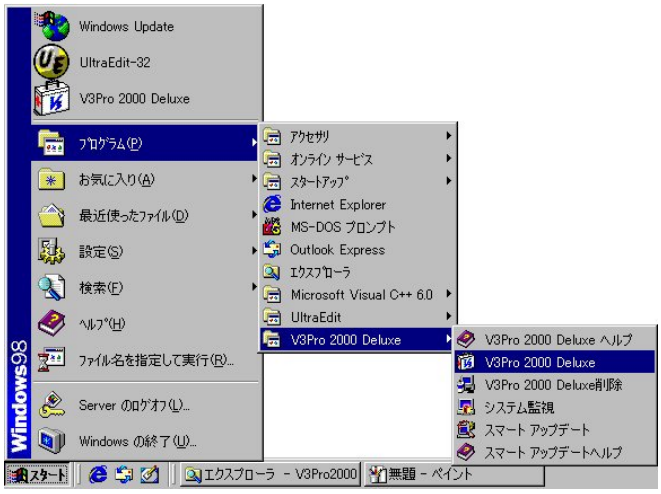
第3章

V3Pro 2000 Deluxe概要

- V3Pro 2000 Deluxe実行
- 基本画面構成
- 検査・治療機能

V3Pro 2000 Deluxe実行

V3Pro 2000 Deluxeを実行するにはWindows 9x / NT (Workstation) / 2000 (Professional)のタスクバーの「スタート」をクリックして、「プログラム」にマウスポインタを移動します。すると、フォルダの中にプログラムグループが表示されます。その中でV3Pro 2000 Deluxeのフォルダに移って「V3Pro 2000 Deluxe」をクリックすれば、実行されます。また、インストールすると、スタートメニューにアイコンが自動的に登録されるのでこのアイコンをクリックしても実行できます。

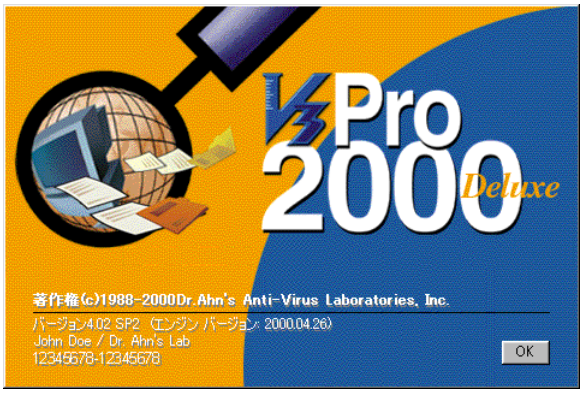


マウスで「スタート」－「プログラム」－「V3Pro 2000 Deluxe」－「V3Pro 2000 Deluxe」の順でマウスポインタを移動します。

V3Pro 2000 Deluxeはインストールされると、自動的に「スタートアップ」のフォルダに実行アイコンを作成するのでここを押して直ちに実行させることができます。

基本画面構成

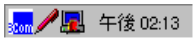
V3Pro 2000 Deluxeを始めると、情報画面が現れてすぐV3Pro 2000 Deluxeの初期画面、即ち手動検査画面が表示されます。



V3Pro 2000 Deluxeのメニューウィンドウは手動検査、検査状態、情報表示、記録表示、バックアップ管理及び届出センター転送、ツール、Webリンクで構成されています。

システム監視機能

V3Pro 2000 Deluxeのシステム監視機能はシステム起動時OS次元で24時間動作しながら外からのウイルスの流れ込みを完全に封鎖するだけではなく、ウイルスに感染したファイルを発見すると自動的に治療、削除、バックアップなどします。それによって、どんな状況の下でもウイルスの侵入からシステムを安全に保護します



作動中OS次元でウイルス検査

Windows NTのシステム監視はサービスプログラムから提供しています。

基本的な構成及び選択項目とその機能は次の通りです。

- **ツール バー** - V3Pro 2000 Deluxeで頻繁に使われる機能を集めてあるツール バーです。
- **快速検査バー** - 検査したい対象を直接入力して検査する機能です。
- **メニュー バー** - V3Pro 2000 Deluxeの様々な機能メニューがあります。
- **メニューウィンドウ** - V3Pro 2000 Deluxeのコマンダーニューウィンドウです。
- **作業ウィンドウ** - 各メニューによる作業内容を表示します。
- **記録表示ウィンドウ** - 作業について様々な記録を表示します。

メニューウィンドウの中のメニュー説明

- **手動検査** - V3Pro 2000 Deluxeが実行されて始めて現れる初期画面として検査する対象をドライブまたはフォルダ単位で指定できます。検査対象を設定した後、「検査」をクリックして検査したい対象の検査を行います。
- **検査状態** - システム監視、インターネット監視、予約検査、スクリーン セーバー実行中検査、マウス右ボタン検査などの環境設定状態を見ることができます。
- **情報表示** - ウイルス カレンダー、ウイルス情報、メッセージメモメニューがあり、様々な有益な情報を得ることができます。
- **記録表示** - システム／インターネット監視作動、ウイルスを発見した時の検査記録、エンジン
アップデート成功／失敗記録などを表すイベント記録と検査結果記録内容を見ることができます。
- **バックアップ管理及び届出センター転送** - ウイルスを発見したとき感染したファイルを別のフォルダに復旧したり、新種ウイルスの場合そのファイルを添付して素早くウイルス届出センターに送られる機能です。
- **ツール** - スマート アップデート、Neo Scan、ブート領域バックアップ、SOSディスク作成、OfficeプロテクターツールがあるからこそV

3Pro 2000 Deluxeはより強力なワクチンプログラムになりました。これらを適切にご活用なさるとお客様のシステムはより強力なAnti-Virus環境になります。Windows NTはツールの中にブート領域バックアップとSOSディスク作成機能がありません。

- **Webリンク** - Dr.安研究所Webサイト(Ahn’s Lab Home Page、研究所ニュース、新種ウイルス、ウイルスFAQ、Webマガジン「ウイルスニュース」、 オンライン登録)にリンクする機能です。

検査・治療機能

V3Pro 2000 Deluxeの詳細な機能を習う前にウイルスを発見したとき検査・治療する方法を簡単に説明します。

ウイルス検査

V3Pro 2000 Deluxeを始めた後、手動検査画面で検査したいドライブを選択すると、そのドライブのアイコンが濃い色に変わります。検査対象を選択したら、「検査開始」ボタンを押してそのドライブについて検査を始めます。（もし検査したいドライブが一つだけである場合は、そのドライブのアイコンをダブルクリックすることでウイルス検査を始めることができます）もし二個以上のトライブを選択する場合は、マウスのドラッグ＆ドロップ機能を利用して、複数のドライブを一緒に指定できます。

ドラッグ＆ドロップ機能を使って選択対象を指定する

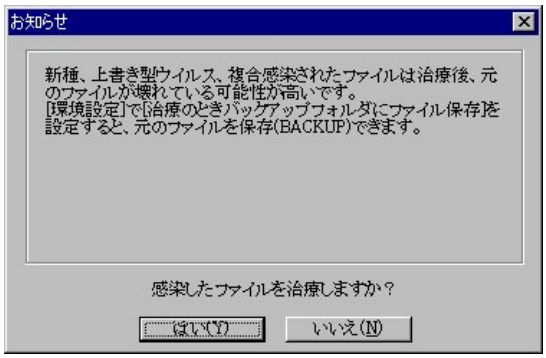
ウイルス発見・治療

もし検査途中ウイルスを発見すると、警告音（ピー）が鳴ってウイルスに感染したファイル、フォルダ名、検査日付、ウイルス名、状態、検査方法などの情報を表示します。その後すぐ、ユーザーが選択した(環境設定の「一般」設定)に従って治療を始めます。

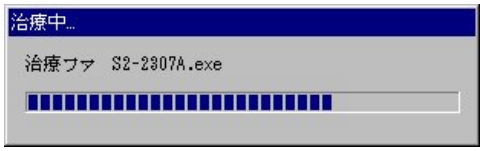
- **すべての目録治療** – ウイルスを発見して治療ウィンドウに登録されたウイルスを全部治療しようとするとき選択します。
- **選択した目録だけ治療** –ユーザーが指定した目録のファイルだけを治療します。

ここで、すべての目録を治療するなら「すべての目録(A)」を、選択した目録だけを治療するには「選択した目録だけ治療(C)」を選択して治療します。

もし次のようなメッセージが出たとき「はい(Y)」を押せば、感染したファイルを治療します。



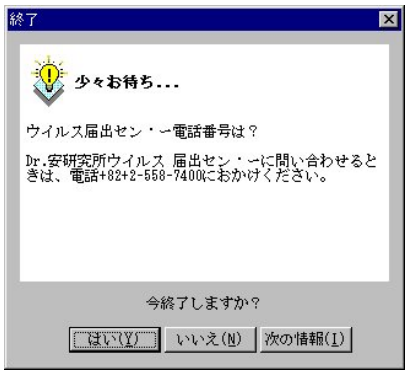
「はい(Y)」をクリックすると感染したファイルを治療を始めます。



治療が終わると次のようなメッセージが現われ、治療が終わったのを知らせます。

終了

V3Pro 2000 Deluxeを終了するためには「ファイル」－「終了」を選択するか、画面右端の一番上の「閉じる」ボタンを押せばプログラムは終了します。プログラムが終わる度に「少々お待ち... 」のダイアログボックスが表示されます。



このダイアログボックスには様々なウイルスに関する情報を短いヒント形式で紹介されます。この内容を参考した後、終了ウィンドウの「はい(Y)」をクリックするとV3Pro 2000 Deluxeが終了します。

参考: V3Pro 2000 Deluxeは終了しても、システム監視機能は作動を続けています。プログラムとは別にシステム監視機能を終了しなければなりません。

V3Pro 2000 Deluxeの基本検査対象

V3Pro 2000 Deluxeではいかなる方法でウイルス検査をしても次の対象は基本検査対象に含めて検査します。検査ウィンドウのレポート結果でワクチン自身は検査に含まれませんが、ブート領域検査は含まれるので検査ファイル数が異なる場合があります。

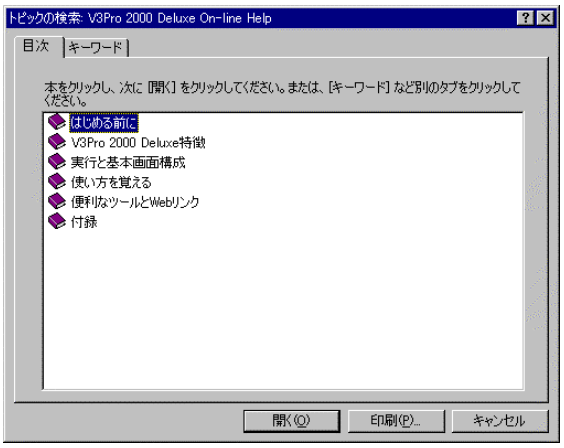
(1) ワクチンソフト自身の検査

(2) C：ドライブの主ブートセクター

(3) C：ドライブのDOS1番ブートセクター

ヘルプについて

V3Pro 2000 Deluxeを使うとき調べたい項目があれば、「ヘルプ」－「ヘルプ項目」をクリックするか、標準ボタンの「ヘルプ」を選択するとすべての機能が表示されます。



ウイルス治療ウィンドウの中の状態情報による措置事項

ウイルス検査をするとウイルス治療ウィンドウでは次のような状態情報を見ることができます。状態情報は治療完了、治療可能、新種ウイルス、実行圧縮ファイル、圧縮ファイル、治療不可能として表示されます。

◆ 治療可能

V3Pro 2000 Deluxeが完璧に治療できるファイルとして、自動的に治療します。治療できるファイルの中で次のようなメッセージが出る場合にはその手順に従って行ってください。

- ウイルスによってファイルが壊れたので設定されているオプションに従って処理します。
- Wordファイルのパスワードを解除して治療してください。
- Excelファイルのパスワードを解除して治療してください。
- PowerPointファイルのパスワードを解除して治療してください。
- ファイルが壊れているか、悪性コードなので削除します。
- wormファイルを取り除いた後、WindowsのSYSTEMフォルダのWSOCK32.DLLファイルを削除してWSOCK32.SKAをWSOCK32.DLLにファイル名を変更してください。

◆ 新種ウイルス（感染したファイルをDr.安研究所に送ってください。）

診断はできますが、現在のバージョンでは治療不可能なファイルです。この場合には感染したファイルを採取して安研究所のウイルス届出センターに送ってください。

◆ 実行圧縮ファイル(圧縮を解凍した後、再検査してください。）
圧縮ファイル（圧縮を解凍した後、再検査してください。）

環境設定で実行圧縮ファイルまたは圧縮ファイル検査オプションを選択して検査すると圧縮されているファイルに入っているウイルスを検査できます。しかし、治療はしないのでそのファイルの圧縮を解凍した後、治療してください。

◆ 治療不可能(複合感染、上書き型ウイルスに感染)

ウイルスが正常に治療できないファイルを発見した場合に表示されます。即ち、一個のファイルに複数のウイルスが同時に感染してファイルが壊れている場合とかファイル感染と共にファイルを損傷する上書き型ウイルスに感染した場合、治療後0バイトになった場合、マクロウイルス治療のときそのファイルにパスワードが掛かっているか、他のプログラムでそのファイルを開いている(OPEN)場合、書込み禁止になっているディスクを治療しようとしたときなどに表示される状態情報です。

第4章

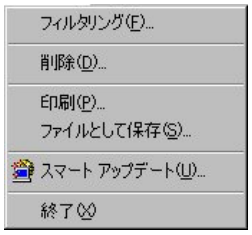
使い方を覚える

- メニューバー
- 快速検査バーで手動検査
- システム監視実行
  - 手動検査
  - 検査状態
  - 情報表示
  - 記録表示
  - 環境設定
- バックアップ管理及び届出センター転送

メニューバー

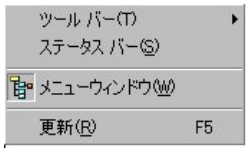
メニューバーで利用できる機能を説明します。「ファイル」はメニューウィンドウの内容によってメニューが少し異なります。基本的に手動検査画面の場合に表示されるメニューバーの内容です。

ファイル



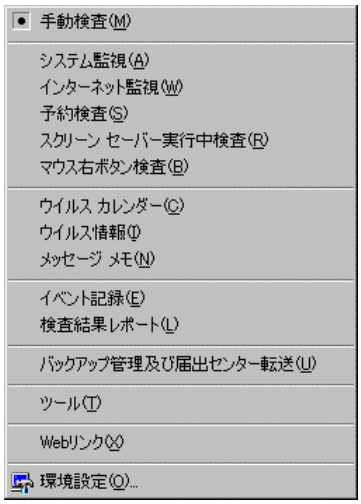
- **検査** – 手動検査で設定した検査対象を検査します。
- **削除** – 選択したリストまたは対象を削除します。
- **新規リスト作成** – ユーザー指定検査対象を作ります。
- **プロパティ** – 対象リストとして指定されたフォルダなどの情報を表示します。
- **スマートアップデート** – インターネットに接続してアップデートサービスを受けます。
- **終了** – V3Pro 2000 Deluxeを終了します。

表示



- **ツール バー** – ツールを表示したり隠したりします。
- **ステータス バー** – ステータス バーを表示します。
- **メニューウィンドウ** – メニューウィンドウを表示します。
- **記録表示ウィンドウ** – 記録表示ウィンドウを表示します。
- **ドライブ単位検査** – ドライブ単位で検査します。
- **フォルダ単位検査** – フォルダ単位で検査します。

作業



- **手動検査** – 手動検査を設定します。
- **システム監視** – システム監視を設定します。
- **インターネット監視** – インターネット監視を設定します。
- **予約検査** – 予約検査を設定します。
- **スクリーンセーバー実行中検査** –スクリーンセーバー実行中検査のオプションを設定します。
- **マウス右ボタン検査** – マウス右ボタン検査のオプションを設定します。
- **ウイルスカレンダー** – 特定日に発病するウイルスを表示したウイルス感染注意知らせのカレンダーです。
- **ウイルス情報** – ウイルスに関する分析情報を集めたデータベースです。
- **メッセージメモ** – Dr.安研究所から受信したメッセージの内容です。
- **イベント記録** – システム／インターネット監視、検査記録、エンジン アップデート成功／失敗の記録を表示します。
- **検査結果レポート**– 検査した結果を表示します。
- **バックアップ管理及び届出センター** – 発見したウイルスをバックアップフォルダに保存したり、安研究所のウイルス届出センターに転送します。
- **ツール** – スマート アップデート、Neo Scan、ブート領域バックアップ、SOSディスク作成、Officeプロテクターなど様々な有益なツールを集めてあります。
- **Webリンク** – 安研究所のwebサイトにリンクする機能です。
- **環境設定** – 個々の検査機能に適したオプションに設定します。

ヘルプ

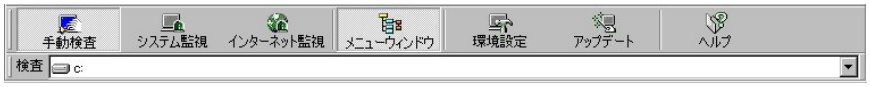
- **ヘルプ項目** - ヘルプを表示します。
- **V3Pro 2000 Deluxe情報** - ユーザー名、製品番号、エンジン日付などが確認できます。

知っておくと便利なショット カットメニュー

ショットカットキー	説明
F1	ヘルプ
F2	「手動検査」ウィンドウで「検査開始」
F3	「快速検査バー」に切り替え
F5	「メッセージメモ」「イベント記録」「検査結果レポート」で「更新」
F6	次のウィンドウに切り替え
Shift + F6	以前のウィンドウに切り替え

快速検査バーで手動検査

快速検査バーは次の場所に存在します。



快速検査バー：ここに検査対象を直接入力して指定できます。

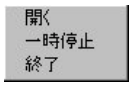
快速検査バーに入力するとき、フォルダを区別する記号は空白（スペース）です。複数のフォルダを入力する場合も空白で区別し、長いフォルダ名とか空白が含まれているフォルダ名は“　”で区別します。（参照：対象フォルダはサブフォルダまで検査しないので、サブフォルダまで含ませるためには「/s）オプションを指定して検査してください。）

項目	説明
オプション設定値	/?
ドライブ単位検査	C:
フォルダ単位検査	c:¥windows
複数のフォルダ検査	C:¥windows,“ c:¥program files” d: /s
サブフォルダ検査	C:¥windows /s
すべてのファイル検査	C:¥windows /a
圧縮ファイル検査	C:¥windows /c /s
ファイル単位検査	C:¥windows¥win.com
ネットワーク共有フォルダ検査	¥¥ahn4¥t¥（¥¥で区分して入力します。）

システム監視実行

システム監視機能はOS次元でウイルスの侵入からシステムを守るプログラムとして、ユーザーが V3Pro 2000 Deluxeをインストールする際、または環境設定で指定されているのを解除しない限りWindows 9x / NT (Workstation) / 2000 (Professional)が動作するとき一緒に作動します。

この機能が実行されるとWindowsタスク バーの右側にシステム監視アイコンが表示されます。このアイコンの上にマウスを持っていって右ボタンを押せば、次のように三つの機能が現れます。



- **開く** - V3Pro 2000 Deluxeのメインプログラムを開きます。
- **一時停止** - システム監視機能が一時的に停止します。この時アイコンの絵柄も変わって、また実行させるためにはこの機能を選択し、解除すればいいです。
- **終了** - システム監視プログラムを終了します。

システム監視機能をWindowsで直接実行するためには[スタート]－[プログラム]－[V3Pro 2000 Deluxe]－[システム監視]を選択すると直ちに作動します。

手動検査

手動で検査するためには

検査する対象を設定してウイルスを検査するメニューです。また、記録表示ウィンドウではエンジン日付と選択されているオプションなどを知らせてくれるのでユーザーが設定した内容を一目でわかります。

作業ウィンドウ

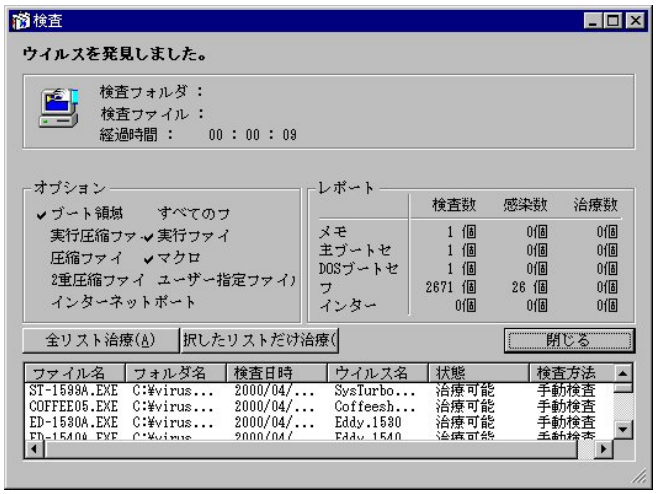
エンジン日付と選択されているオプションが分かる記録表示ウィンドウ

作業ウィンドウは現在システムに繋がっているすべてのディスクドライブの状況をV3Pro 2000 Deluxeが自動的に認識し、アイコンとして表示する所です。また、各アイコンは検査対象を直ちに指定または解除できるように検査対象設定／解除ウィンドウも兼ねています。

マウスで各アイコンを押せば、そのアイコンが濃い色に表示され、そのアイコンが表す領域をウイルス検査対象として指定します。返って検査対象指定を取消したいなら、選択した検査対象ドライブをマウスでもう一度押して指定を取消せます。

検査対象設定ウィンドウから検査したい対象を設定した後、「検査開始」をクリックすると設定した検査対象に対して検査を始めます。または検査対象設定ウィンドウで検査したいドライブをダブルクリックすると直ちに検査が行われます。

検査結果、ウイルスを発見しなかったら、ウイルスがないというメッセージを表示します。ウイルスを発見すると、検査を完了した後自動的に治療ウィンドウが現れて治療を始めます。



新規対象リスト

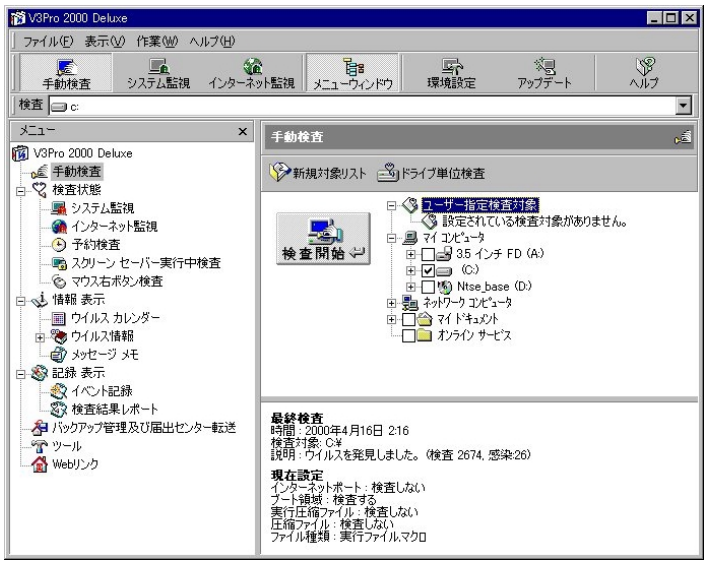
ユーザーが指定して新しい対象リストを作ることができます。

ユーザーが指定したフォルダまたはドライブだけを検査できる機能として、ユーザーの環境によって特に頻繁に検査する必要がある領域を別に設定できます。この機能はドライブ全体を検査する非効率性を省き、検査時間も節約できます。特に大容量ハードディスクお使いのユーザーには便利な機能です。

手動検査作業ウィンドウの「新規対象リスト」を選択すると、「ユーザー指定検査対象設定」ウィンドウが開きます。左ウィンドウには選択対象リストが、右ウィンドウには検査対象リストが現れます。検査したい項目を選択して指定してください。

フォルダ単位で検査／ドライブ単位で検査

V3Pro 2000 Deluxeを初めて実行すると、検査ウィンドウにドライブ単位で検査する画面が初期値として現れます。もしフォルダ単位に変えたいなら、「フォルダ単位検査」を選択してフォルダ単位に変更できます。

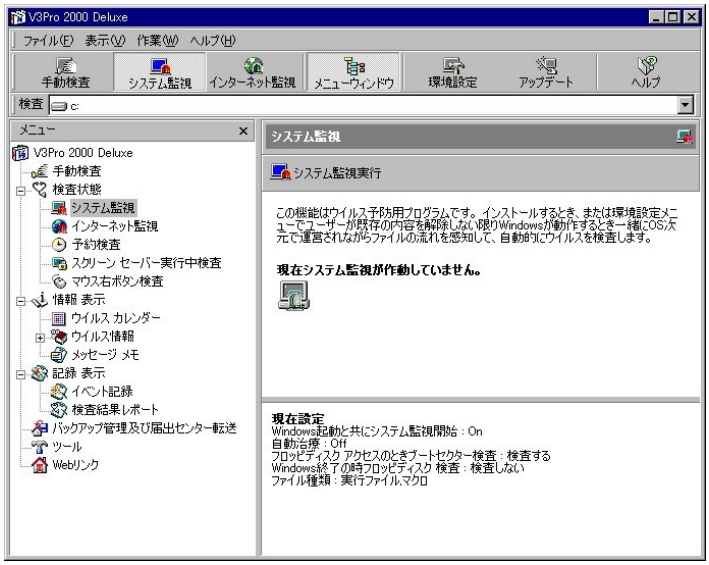


またドライブ単位に設定を変えたいときには「ドライブ単位で検査」を選択します。

検査状態

システム監視

現在システム監視が作動中であるか、一時停止状態であるかが分かります。システム監視はインストールする時または環境設定メニューでユーザーが既存の内容を解除しない限り、Windowsが作動するときOS次元で一緒に運営されながらファイルの流れを感知して、自動的にウイルスを検査します。



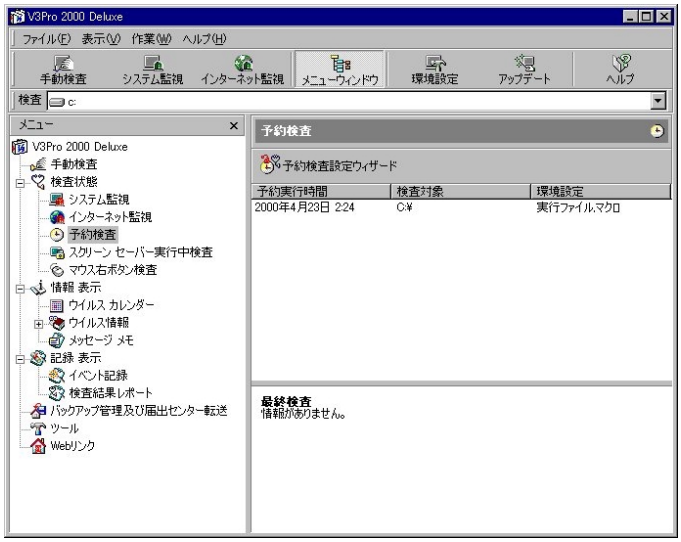
ここを押せば**システム監視**が終了します。

インターネット監視

インターネットで送受信されるデータの状態がグラフ画面を通して一目で把握できる機能です。もしTCP/IP基盤のすべてのプロトコルを検査する場合にはすべてのプロトコルを選択し、特定のプロトコルだけを検査したいときにはそのプロトコルを環境設定メニューで指定します。

予約検査

現在待機中である予約検査状態を見ることができます。もし予約検査を追加するなら、「予約検査設定ウィザード」をクリックして希望する予約時間を設定できます。

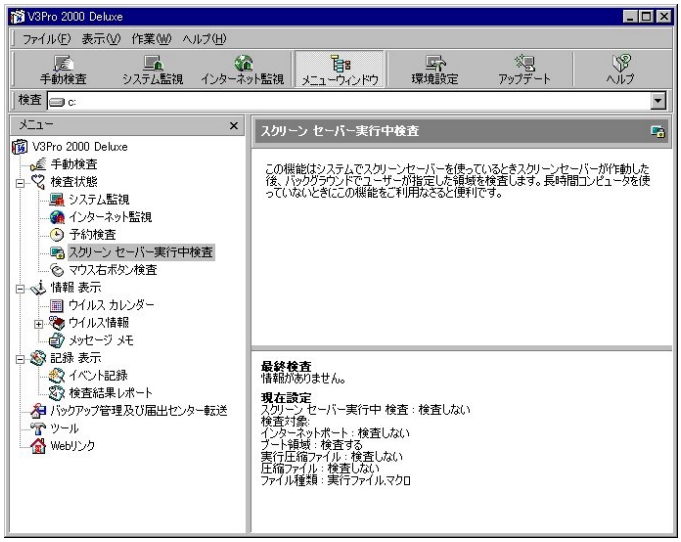


ここを押せばシステム監視が終了します。

スクリーン セーバー 実行中検査

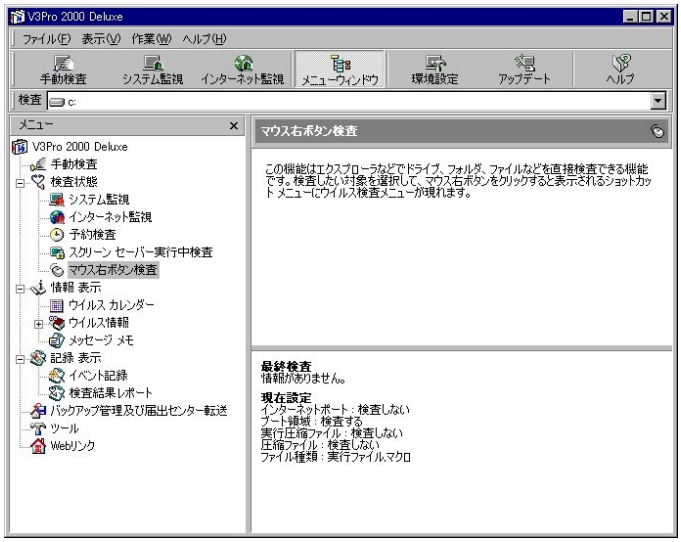
スクリーンセーバー実行中の設定状態を表示します。スクリーンセーバー実行中検査オプションを指定するとスクリーンセーバーが作動した後、バックグラウンドでユーザーが指定した領域を検査します。長時間コン

ピュータを使っていないときに「スクリーン セーバー実行中検査」をご利用なさると便利です。



マウス右ボタン検査

マウス右ボタン検査の設定状態及び検査状態を表示します。

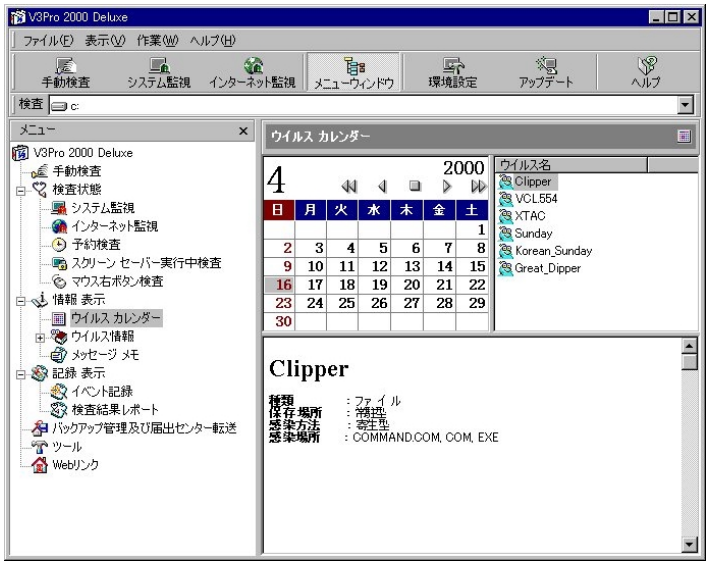


「マウス右ボタン検査」はエクスプローラなどでドライブ、フォルダ、ファイル等を直接検査できる機能です。検査したい対象を選択し、マウス右ボタンをクリックすると表示されるショットカット メニューにウイルス検査メニューが現れます。ここを押せば、エクスプローラなどで検査対象を直接検査できます。ショットカット メニューに現れる**「V3でウイルス検査」**をクリックすれば、選択した検査対象を直接検査できます。

情報表示

ウイルス カレンダー

ウイルスカレンダーでは特定日に発病するウイルスの情報を見ることができます。



コンピュータウイルスの中ではシステムの「時計(日付と時刻)」をチェックして特定日に発病を開始することでユーザーに被害を与えるウイルスがあります。Michelangeloの誕生日である3月6日に発病するMichelangeloウイルスをはじめ、13日と金曜日が重なる日に発病するエルサレム ウイルス(JERUSALEM)、12月25日に発病するクリスマス挨拶ウイルス(CHRISTMAS)などが代表的な特定日発病ウイルスです。ウイルス全体の中で特定日に発病するウイルスが占める割合は高くありませんが、ウイルスカレンダーは特定日発病ウイルスに対して備えられるだけではなく、ウイルスに対する注意を呼び起こすのに有益な道具になります。

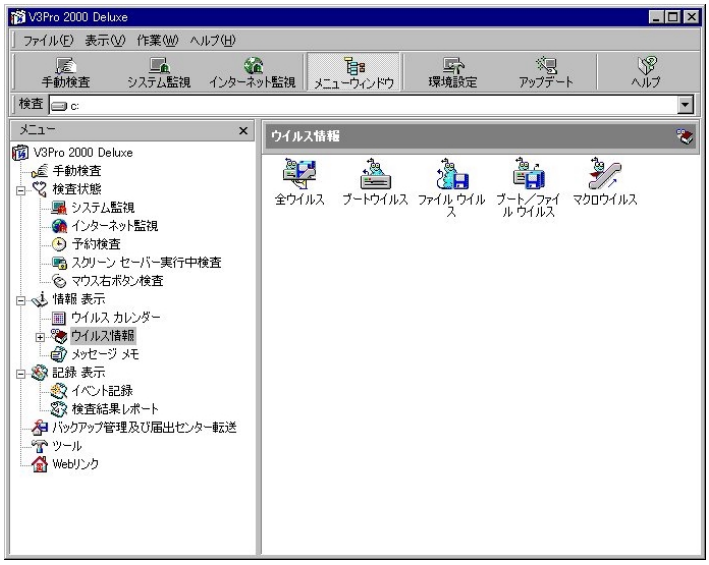
ウイルスカレンダーのウイルス情報ウィンドウには今月のカレンダーと当日に発病するウイルスのリストが表示されます。また、下のウィンドウではそのウイルスについての情報を見ることができます。例えば、November_17th.855ウイルス名を選択するとそのウイルスに関する特徴（種類、感染方法、感染位置、症状）についての情報が表示されます。

その上、カレンダーを捲って見たい年度の月を表示させて、日付を選択すると、その日に発病するウイルス情報を見ることもできます。カレンダーの上にある方向を表すボタンを押せば、一ヶ月または一年単位でカレンダーを捲って特定日に発病するウイルスの発病日を見ることができます。

上のボタンを押してカレンダーを捲ると該当年度、月のカレンダーが現れ、日付はいつも現在状態として表示されます。もし特定日に発病するウイルスを見たいなら、カレンダーを見たいところに捲って、その日にマウスを持って行ってクリックすると指定できます。

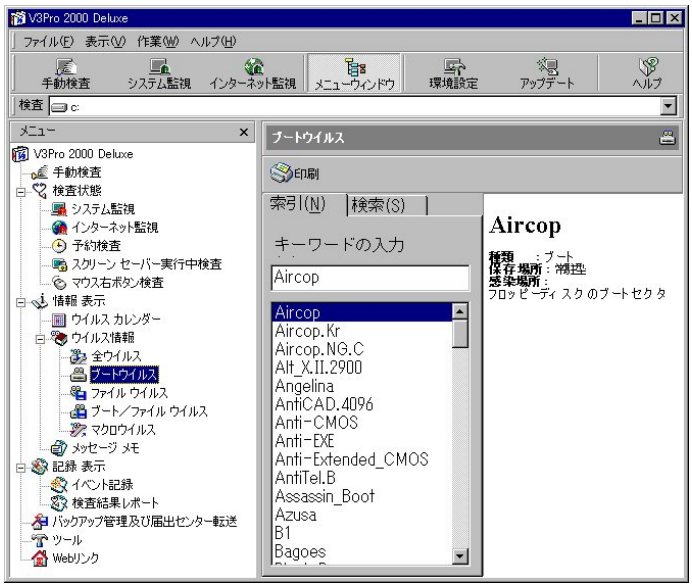
ウイルス情報

診断・治療できるウイルスに対する分析情報を項目別に詳細に見ることができます。全ウイルス、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、マクロウイルスに関する情報を得ることができます。



- **全ウイルス** – すべてのウイルス
- **ブート** – ブート領域に感染するウイルス
- **ファイル** – ファイルに感染するウイルス
- **ブート／ファイル** – ブートセクターと実行ファイル両方に感染するウイルス
- **マクロ** – マクロ機能を利用して製作されたウイルス

この中でユーザーの知りたいウイルスに関する情報を選択すると、ウイルス情報ウィンドウが表示されます。ウイルス情報ウィンドウは七つのメニューで構成され、マウスで選択すると個々のウイルスについての情報を見ることができます。



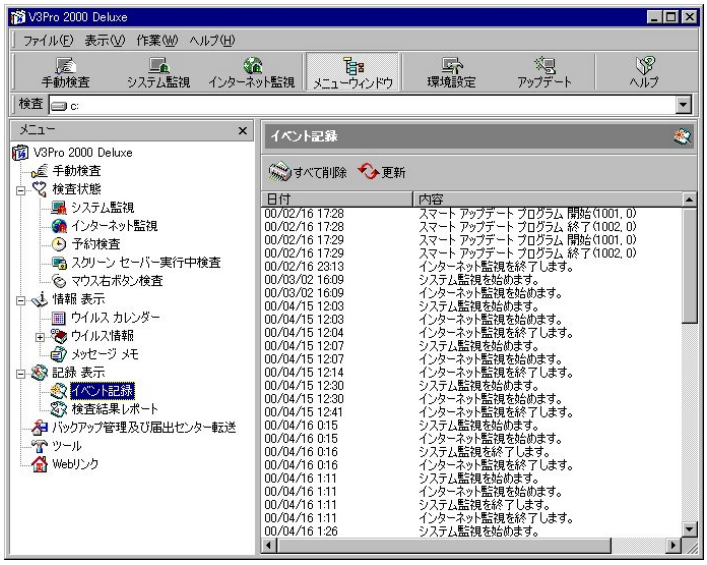
メッセージ メモ

Dr.安研究所からアップデートするとき配布されるテキスト文書を表示します。この文書ファイルには追加されたウイルス、新種ウイルス、その他ウイルスに関する情報が含まれています。

記録表示

イベント記録

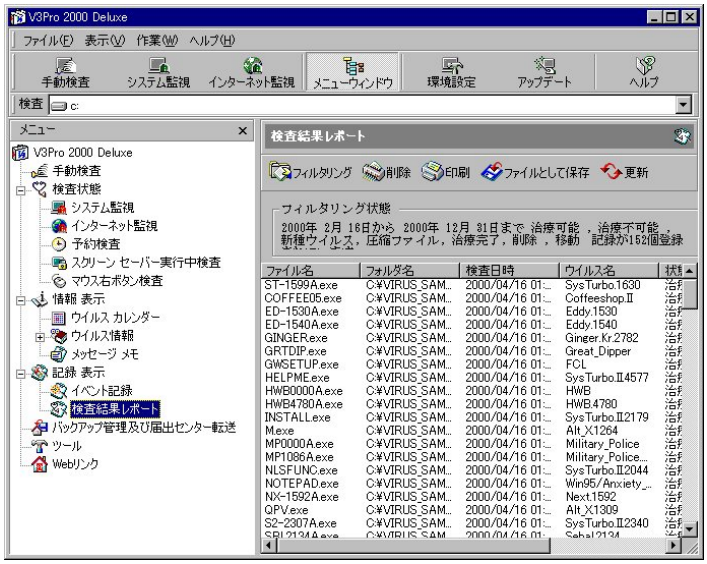
システム／インターネット監視、ウイルスを発見した時の検査記録、エンジン アップデート成功／失敗記録を表示します。 (Windows NTの場合、イベント記録が記録されません。この記録はV3Pro 2000 Deluxeのイベント記録／検査レポートにあります。)



- **すべて削除** – 現在保存されている記録をすべて削除します。
- **更新** – 新しい内容が追加されたとき変更された内容を表示します。

検査結果レポート

V3Pro 2000 Deluxeはウイルスを検査した後、ウイルスを発見すると検査記録を保存してその内容をユーザーが参照できるようにします。検査結果メニューがこの機能を担当するもので、検査結果レポートを選択すると最近まで検査したすべてのウイルスの記録を見ることができます。「ファイル名」と「フォルダ名」では検査結果、感染したのが確認されたファイル名とそのファイルが存在するフォルダのパスを表します。「ウイルス名」では感染したウイルス名を表示します。「状態」では治療が完了されたか否かについての結果記録を表します。



環境設定

V3Pro 2000 Deluxeの環境設定では様々なオプション設定ができます。V3Pro 2000 Deluxeが提供する環境設定メニューを活用すれば、より強力なAnti-Virus環境を整えることができます。標準ボタンの「環境設定」をクリックするか、「作業」－「環境設定」を選択すれば次のような六つのメニューが現れます。一般、手動検査、システム／インターネット監視、予約検査、スクリーン セーバー実行中検査、マウス右ボタン検査などの設定ができます。これらは次のような選択事項が含まれています。

治療設定

「環境設定」－「一般」を実行して一般的な検査オプションを設定できます。

- 治療の時、バックアップフォルダにファイル保存
- 治療不可能ファイル処理
- ウイルスを発見すると音を鳴らす
- ウイルス発見した時だけ検査結果表示
- 検査記録保存／非検査領域設定

検査設定

検査する領域と対象を設定します。

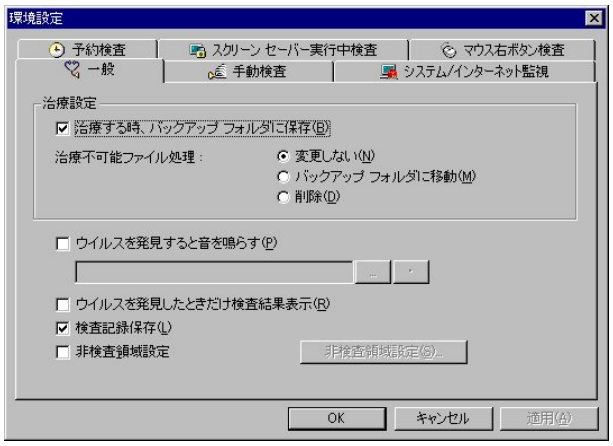
- **ブート領域検査** - システムのブート領域を検査します。
- **実行圧縮ファイル検査** - DIET, LZEXE, PKLITEなどの実行圧縮ファイルを検査します。
- **圧縮ファイル検査** - 拡張子がZIP, ARJ, RAR, JAR, CAB, LHA, UUEN/DECODE, ZOO, MIMEである圧縮ファイルを検査します。
- **二重圧縮ファイル検査** - 二重に圧縮されているファイルを検査します。

検査するファイルの種類

- **すべてのファイル検査**-マクロ、実行ファイル、圧縮ファイル、一般文書ファイルなど全種類のフィルを検査します。
- **実行ファイル検査** - 拡張子がCOM, EXE, OVL, DLL, BINなど実行可能なフィルを検査します。
- **マクロ検査** - マクロウイルスに感染し得るファイルを検査します。
- **ユーザー指定ファイル種類検査** - ユーザーが指定した拡張子のファイルを検査します。

一般設定

「環境設定」－「一般」を選択すると各検査方法のオプション設定画面が表示されます。



各検査のとき検査対象について指定するオプションです。治療のときバックアップフォルダにファイルを保存、治療不可能ファイル処理などファイルの処理方法を指定できます。また、「ウイルスを発見すると音を鳴らす」、「ウイルスを発見した時だけ検査結果表示」、「検査記録保存」及び「非検査領域設定」のオプションがあります。(非検査領域は「検査しない領域)を表します。

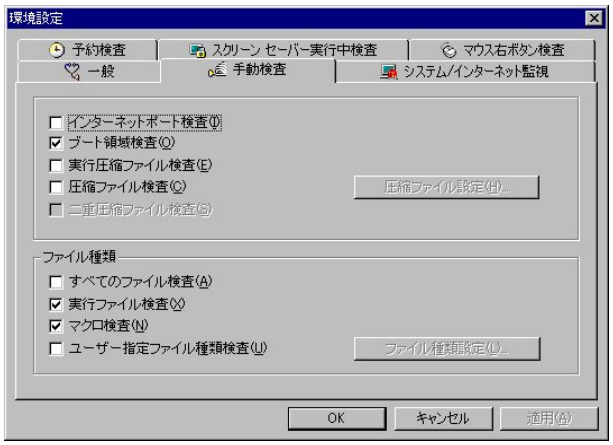
- **治療のときバックアップフォルダにファイル保存** – 元のファイルが壊れる場合に備えた機能として、ウイルスを発見して治療する前に現在ウイルスに感染したファイルをバックアップしておいてから治療します。例えばDATA.COMファイルにウイルスが感染した場合、バックアップフォルダに拡張子がV3Bに変わったDATA.V3Bファイルが生成されます。
- **治療不可能ファイル** – 正常に治療できないウイルスに感染した場合、そのファイルをユーザーが指定したフォルダに移動・保存しておくか、削除する機能です。初期値は「変更しない」に設定され、ユーザーが変えたいときには治療不可能ファイルをバックアップフォルダに移動したり、直ちに削除することもできます。
  - **「変更しない」**：ファイルを元の状態でそのままにしておきます。
  - **「バックアップフォルダに移動」**：バックアップフォルダに移動します。
  - **「削除」**：感染したファイルを削除します。
- **ウイルスを発見すると音を鳴らす**–ウイルスを発見した時、音が鳴ってウイルスを発見したのを知らせてくれる機能を指定できるオプションです。WAVファイルを変更してお好みの音に替えることもできます。
- **検査記録保存** –「検査記録保存」を選択するとウイルスを検査

した後、作成されるレポート記録が1日1個のLOGフィルとして保存されます。(**参照**：イベント記録は常に保存されます。)

- **非検査領域設定** – 「検査しない領域設定」を意味して、大容量ハードディスクご使用のユーザーには便利な機能です。ユーザーの判断でウイルスが全然存在しないフォルダであり、そのフォルダを検査するのは時間の無駄である場合、そのフォルダを検査しない機能です。この機能で設定された領域はV3Pro 2000 Deluxeのいかなる検査方法を使っても検査しないので設定するときにはお気をつけてください。**参照**：ビギナーの方はできるだけ「非検査領域設定」を指定しないことをお勧めします。

手動検査

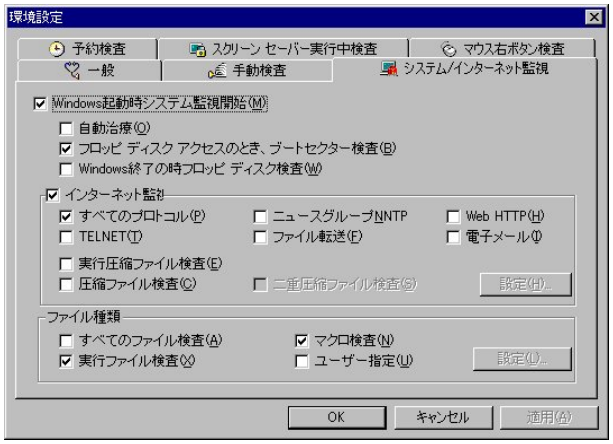
V3Pro 2000 Deluxeを実行したとき最初に表示される初期画面でドライブまたはフォルダを選択して「検査開始」をクリックする方法として、ウイルス検査をするとき使われるオプションです。初期値ではブート領域検査と実行ファイル、マクロファイルだけ検査します。



システム／インターネット監視

システム／インターネット監視プログラムはWindowsシステム次元でウイルスに感染したファイルが実行されるのを予防するのに使われます。V3Pro 2000 Deluxeはインストールする際システム／インターネット監視機能を一緒に組み込むように勧めます。それによって、V3Pro 2000 Deluxeをインストールすると、Windows作動と共にシステム監視プログラムがいつもバックグラウンドで遂行されながらウイルスからシステムを安全に保護してくれます。

Windows 9x / NT (Workstation) / 2000 (Professional)のタスク バー右端を見るとシステム監視設定アイコンが常住しているのが見られます。これはWindows 9x / NT (Workstation) / 2000 (Professional)と共にシステム監視プログラムが作動中であることをユーザーに知らせてくれるアイコンです。



参照: システム監視にはインターネット機能が含まれて制御されているので、システム監視を中止するとインターネット監視機能も中止されます。

システム監視オプション

- **Windows起動時システム監視開始** – インストールする時、システム監視機能はWindows起動と共に始まるように指定されています。このオプションのチェックをオフにすれば、設定を変更できます。
- **自動治療** –ウイルスに感染したファイルを実行したり開いたりするとき、そのファイルを自動的に治療して正常なファイルだけを実行する（開く）強力なAnti-Virus機能です。ファイルウイルスとマクロウイルスによる被害を根本的に防げる機能です。
- **フロッピディスク アクセスの時ブートセクター検査**–フロッピディスクによって感染するブートウイルスを阻むために、フロッピディスクを使うときブートセクターを検査するようにしたオプションです。
- **Windows終了時、フロッピディスク検査**–Windows終了時、フロッピディスクを検査するようにして、フロッピディスクによるウイルスの侵入を完全に阻みます。

ファイル種類

- **すべてのファイル検査** – すべてのファイル種類を検査します。
- **マクロ検査** – マクロウイルスに感染し得るファイルを検査します。
- **実行ファイル検査** – 拡張子がCOM, EXE, OVL, DLL, BINなど実行可能なファイルを検査します。
- **ユーザー指定** –
  ユーザーが指定した拡張子のファイルを検査します。

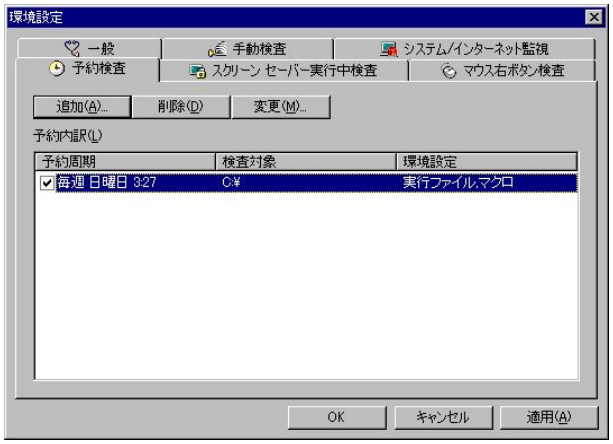
安全性を考えると検査データ設定は「すべてのファイル検査」を選択するのが望ましいですが、ほとんどのウイルスが実行ファイルとマクロウイルスに感染し得るファイルを優先的に感染させるので、検査対象を実行ファイルとマクロデータに設定すると検査する時間の節約になります。

インターネット監視

- **すべてのプロトコル** - すべてのプロトコルを監視します。
- **ニュースグループNNTP** - ニュースグループNNTPを監視します。
- **Web HTTP** - web HTTPを監視します。
- **Telnet** - telnetを監視します。
- **ファイル転送** - FTPを監視します。
- **電子メール** - POP3とSMTPを監視します。
- **実行圧縮ファイル検査** - DIET, LZEXE, PKLITEなどの実行圧縮ファイルを検査します。
- **圧縮ファイル検査** - ZIP, ARJ, RAR, CAB, LHA, UUENCODE/UUDECODE, ZOOなど圧縮ファイルを検査します。
- **二重圧縮ファイル** - 二重に圧縮されているファイルを検査します。

予約検査設定

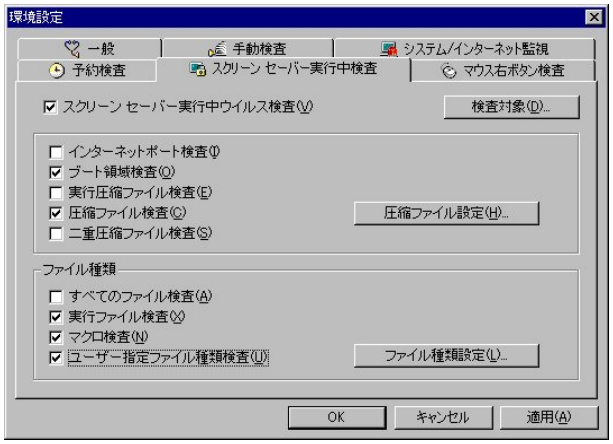
「スクリーン セーバー実行中検査」機能と併用できる機能として、システムを付けたまま長時間お使いになる場合、ユーザーが指定した時間に指定した領域を検査するように設定できます。予約検査は初期値が設定されていなくて、ユーザーが検査日程を設定できます。それによって、システムを起動すると毎日、毎週、毎月一回単位で特定時間に検査対象ドライブまたはフォルダを検査する機能です。



「追加」を押せば「予約検査設定ウィザード」が実行され、検査日程を設定できる画面が表示されます。これを設定した後にはその予約検査で使う検査方法及びファイル種類を指定します。

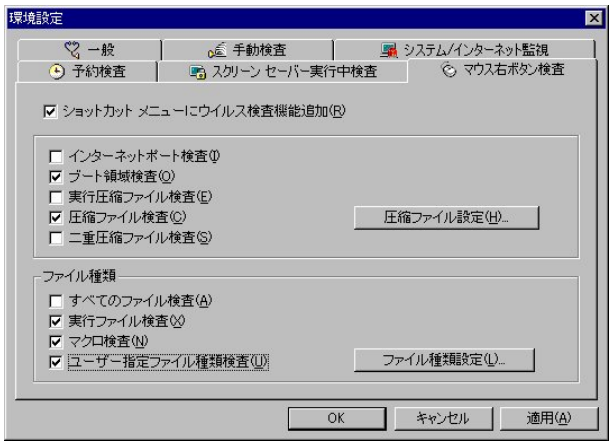
スクリーン セーバー実行中検査

スクリーン セーバーが実行されているとき、ユーザーが設定した領域をバックグラウンドで検査します。これは初期値として選択されていません。



マウス右ボタン検査

マウス右ボタン ショットカット メニューを利用して特定領域（ドライブ／ファイル／フォルダ）に対する検査機能を実行するかを設定します。V3Pro 2000 Deluxeはインストールのときこの機能を設定するように勧めますが、環境設定メニューで「ショットカット メニューにウイルス検査機能追加」項目をオフにすれば、この機能は使えなくなります。



検査記録ウィンドウから覗けるウイルス情報

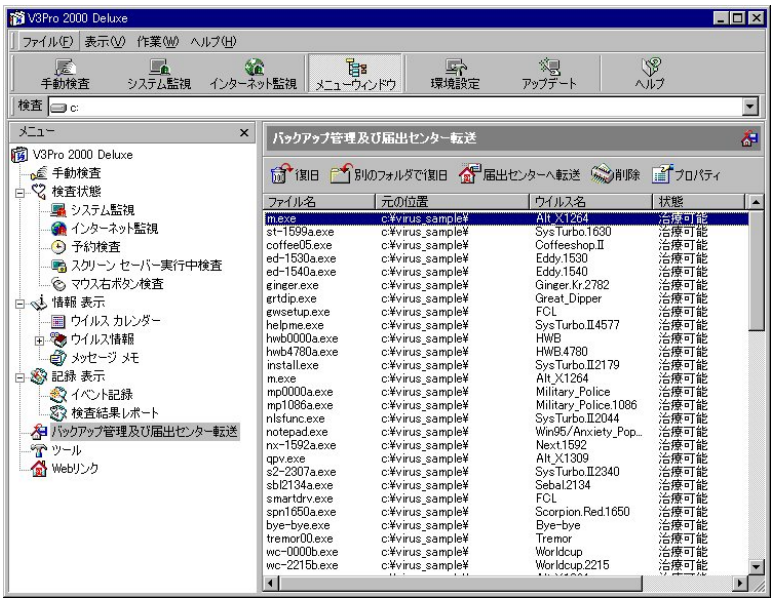
検査記録ウィンドウに現れるウイルス名にマウスポインタを持っていくと、ウイルスに関する情報がポップアップ トピックで現れます。

上の画面のようにマウスポインタをWin-Trojan/Back-Orificeの上に持っていくと、このウイルスに関する簡単な特徴がポップアップトピックの形で現れます。そのウイルスに対する詳細な内容はウイルス情報メニューをご覧になってください。

バックアップ管理及び届出センター転送

コンピュータウイルスに関するお問い合わせとか新種ウイルスを届け出るためにはユーザーがインターネットに繋がっていれば、研究所が営んでいるインターネットwebサイト(www.ahnlab.com)に接続し、電子メールを送ったり、疑われるファイルを添付して届け出ることができます。研究所のインターネットホームページに接続し、ウイルス届出センターに入って、ウイルス届出様式を選択すると問合せ様式が現れます。この様式に合わせて問い合わせていただけば、折返しご返答いたします。

V3Pro 2000 Deluxeではメニューウィンドウからバックアップ管理及び届出センター転送をクリックすると、直ちに研究所のインターネットwebサイトのウイルス届出センターに繋がります。



- **復旧** – 元のフォルダに復旧します。感染したファイルなので注意してください。
- **別のフォルダで復旧** – 別のフォルダに移します。
- **届出センターへ転送** –研究所のウイルス届出センターに転送します。治療不可能と新種ウイルスだけ転送できます。
- **削除**–指定した対象を削除します。
- **プロパティ**–バックアップ前の状態に関するファイル情報を見ることができます。

第5章

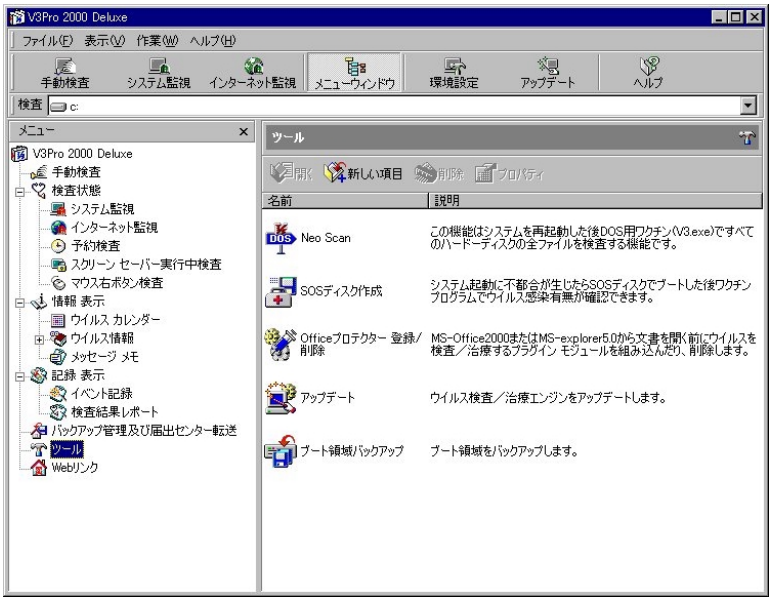
便利なツールとWebリンク

- スマートアップデート
- Neo Scan
- ブート領域バックアップ
- SOSディスク作成
- Office Protector
- Webリンク

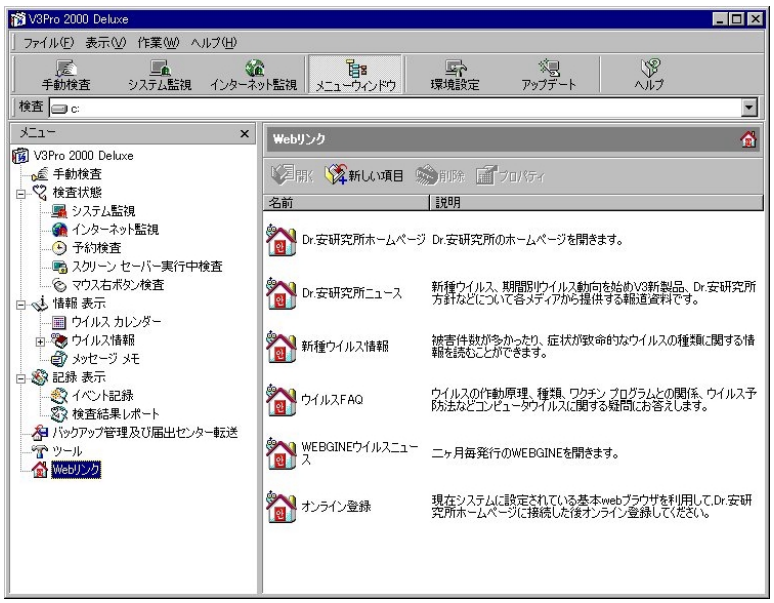
V3Pro 2000 Deluxeのツール及びWebリンクにはスマートアップデート、Neo Scan、ブート領域バックアップ、SOSディスク作成、Dr.安研究所ホームページにリンクする機能（安研究所ホームページ、安研究所ニュース、新種ウイルス、ウイルスFAQ、Webマガジン「ウイルスニュース」、オンライン登録）などV3Pro 2000 Deluxeをより強力なワクチンプログラムにしてくれる便利なツールが入っています。これら機能を適切に活用すれば、お客様のシステムをより強力なAnti-Virus環境に調えることができます。

ツール及びWebリンクメニューの各機能は追加/削除できます。もし使わない機能なので削除したいときには「削除」ボタンをクリックして削除できます。（各機能にマウスを持っていき、右ボタンを押して現れるメニューの中で削除を選択しても削除できます。）

ツール



Webリンク


V3Pro 2000 Deluxe
ファイル(F) 表示(V) 作業(W) ヘルプ(H)
手動検査
システム監視
インターネット監視
メニューウィンドウ
環境設定
アップデート
ヘルプ
検査
c:
メニュー
V3Pro 2000 Deluxe
手動検査
検査状態
システム監視
インターネット監視
予約検査
スクリーン セーバー実行中検査
マウス右ボタン検査
情報 表示
ウイルス カレンダー
ウイルス情報
メッセージ メモ
記録 表示
イベント記録
検査結果レポート
バックアップ管理及び届出センター転送
ツール
Webリンク
Webリンク
開く
新しい項目
削除
プロパティ
名前
説明
Dr.安研究所ホームページ
Dr.安研究所のホームページを開きます。
Dr.安研究所ニュース
新種ウイルス、期間別ウイルス動向を始めV3新製品、Dr.安研究所方針などについて各メディアから提供する報道資料です。
新種ウイルス情報
被害件数が多かったり、症状が致命的なウイルスの種類に関する情報を読むことができます。
ウイルスFAQ
ウイルスの作動原理、種類、ワクチン プログラムとの関係、ウイルス予防法などコンピュータウイルスに関する疑問にお答えします。
WEBGINEウイルスニュース
二ヶ月毎発行のWEBGINEを開きます。
オンライン登録
現在システムに設定されている基本webブラウザを利用して,Dr.安研究所ホームページに接続した後オンライン登録してください。

スマート アップデート

スマートアップデートとは？

スマートアップデート(Smart Update)™は安研究所が開発した独自のサービスとして、ユーザーが安研究所のパワーサービス インターネットホストを通じて、エンジンアップデートファイル及びユーザーに送るメッセージなどを自動的にダウンロードしてユーザーのサーバーシステムに組み込む一連の機能を指します。

その上、スマートアップデート™ サービスは自動または手動モードの様々な設定を支援しているのでユーザーの要求に合わせていつでもユーザーのサーバーに最新バージョンのワクチンをダウンロードし、アップデートしてくれます。

自動モードに設定すると、リアルタイム サーバー監視や予約検査が実行されたとき、リアルタイム サーバー監視や予約検査が作動中である状態のまま日付が変わる度にスマートアップデート™が自動実行されます。スマートアップデート™™が行われた後は既に作動中であったリアルタイムサーバー監視や予約検査プログラムが再開されます。

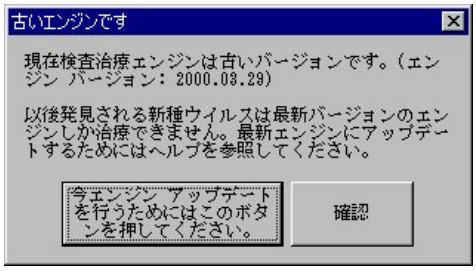
最新エンジン アップデート方法

1. 作業ウィンドウの**ツール－スマートアップデート**を選択するとスマートアップデート ユーティリティが実行されます。

2. 自分のシステム環境に合わせてアップデート経路とダウンロートファイルの種類を選択した後、**アップデート開始**ボタンを押せば最新エンジンアップデートファイルに簡単にアップデートできます。

3. エンジンアップデートフォルダのデフォルトは ’C:¥Progam files¥V3¥UPDATE’ です。もし現在組み込まれているV3Pro 2000 Deluxe

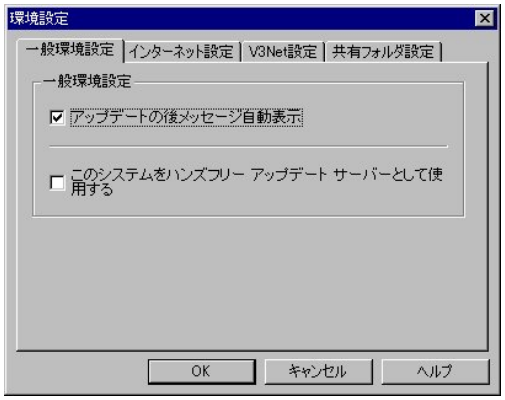
のエンジンが一ヶ月以上過ぎていればV3Pro 2000 Deluxe実行後、
初期画面にスマートアップデート ユーティリティアイコンが現れ、
アップデートするように自動的に知らせてくれます。



環境設定

一般環境設定

アップデート実行後、アップデートされた後のメッセージを自動的に表示するかを、またシステムをアップデートサーバーとして使用するかどうかを指定できます。



- **アップデート後メッセージ自動表示** - 項目を指定しておくとエンジンと共に提供される文書ファイルを自動的に読むことが出来ます。
- **このシステムをアップデートサーバーとして使用する** - 項目を指定しておくとそのシステムをアップデートサーバーとして使うことが出来ます。

インターネット設定

次のアップデートサーバーを通じてアップデートサービスを受けられます。

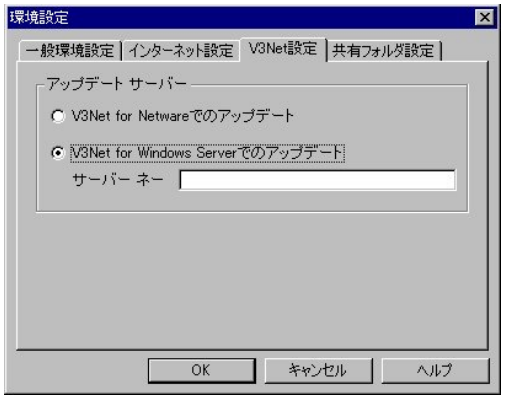
- Kornet server
- Shinbiro server
- Boranet server
- I-Net server

このようなサーバーの中で速いインターネットサーバーを選択してご使用ください。この機能はインターネットに繋がっているときだけお使いになれます。

プロキシサーバーを使う場合**プロキシサーバー使用**を選択してプロキシサーバーのアドレスとポート番号を入力してください。

V3Net設定

ネットワークの同一セグメントに組み込まれているサーバー用V3シリーズであるV3Netを通じてアップデートを行う機能です。従ってこのアップデート方法はV3Netが無かったり、ネットワークを通じて繋がっていなければ行われません。



共有フォルダ設定

共有するフォルダ名を入力して設定します。

エンジンアップデートファイルのあるネットワークドライブの共有フォルダから直接アップデートを行ったり、ローカルドライブ(A:, C:など)のドライブやフォルダを指定してアップデートを行える機能です。

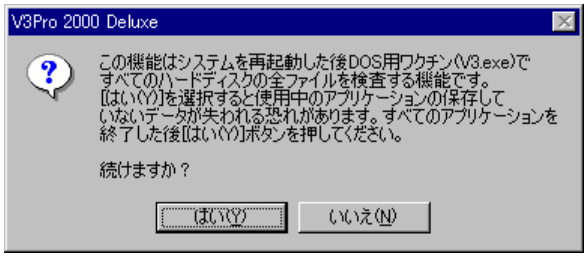
予約設定

アップデート方法と予約日時が指定できます。

- **追加** – スマートアップデートを予約するためには**予約追加**ボタンを選択して予約を登録します。アップデート経路はインターネット、V3Net、共有フォルダの方法で指定できます。予約日時は毎日、毎週、毎月、ユーザー指定オプションとして指定できます。
- 修正 – 修正したい予約検査を選択した後、**予約修正**ボタンを押せば予約検査設定画面が現れます。修正したい項目を修正した後、**確認**ボタンを押します。
- 削除 – 削除したい予約検査を選択した後、**予約削除**ボタンを押します。

Neo Scan

Neo Scan機能はウイルスを完全封鎖するために現在実行中であるWindowsシステムを強制に終了します。そしてDOSで起動した後、Windowsが再起動する前にワクチンであるV3+ Neoですべてのハードディスクを検査する機能です。特にWindowsシステムが使用中であるファイルが感染した場合、確かな防疫管理になります。まず「ツール」－「Neo Scan」を選択すると次のような画面が現れ、Neo Scanを実行するかを尋ねます。



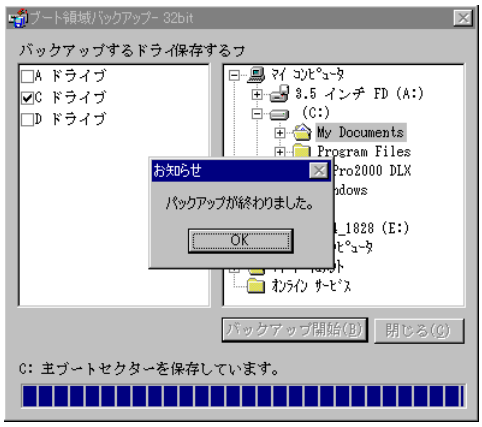
「はい（Y）」を選択すると、Neo Scan機能が実行されます。

ブート領域バックアップ

ブート領域バックアッププログラムは新しいブートウイルスと疑われる時とか、ブート領域データについての分析作業が必要な場合に備えてブート領域データをバックアップ（保存）する機能です。

ブート領域パックアッププログラムは新種ブートウイルスに感染した場合、簡単にサンプルが採取でき、正常なシステムのブート領域をバックアップしてそのデータを別の場所に保存します。それで、ブート領域が破壊された時、システムを復旧するのにそれを参考資料として使うこともできます。V3Pro 2000の「ツール」－「ブート領域バックアップ」をクリックするとブート領域バックアップ ウィンドウが開きます。

ブート領域バックアップ ウィンドウは二つのウィンドウで構成され、左のウィンドウではバックアップするドライブを、右のウィンドウでは保存するフォルダを選択します。バックアップするドライブはC:が初期値として設定されてあり、保存するフォルダとしては基本的にはフロッピディスク ドライブであるA:に設定されています。もしフロッピディスクのブート領域をバックアップするなら、フロッピドライブ アイコンの左側にチェックを入れてください。逆にハートディスクのブート領域をバックアップしないなら、ハードディスクドライブ アイコンの左側のチェックを取消してください。上と同様に保存するフォルダ設定も同じ方法で指定したり、指定を取消したりします。ブート領域を保存するドライブとフォルダを設定した後ブート領域バックアップ ウィンドウの下にある「バックアップ開始(B)」ボタンをクリックするとバックアップが行われ、結果確認ボックスが現れます。



このとき、「OK」ボタンをクリックしてブート領域バックアップ ウィンドウの「閉じる(C)」ボタンを押せば、前の画面に戻ります。

ブート領域バックアップはメインメニューから「作業」－「ツール」－「ブート領域バックアップ」を選択します。

SOSディスク作成

「ツール」－「SOSディスク作成」メニューを選択すると非常の場合に使える起動用ディスクを作成します。但し、このときA:ドライブにはフォーマットしてもいいディスクを挿入してください。フォーマットウィンドウで「開始(S)」ボタンを押してフォーマットが完了したら、「閉じる(C)」ボタンをクリックしてください。これで、システムの情報がフロッピディスクにコピされます。

また、SOSディスクを作成するとそのディスクにV3RESCUE.EXEというプログラムをコピします。

これはSOSディスクに含まれているシステムのハードディスクのブート領域をハードディスクに自動的にコピしてくれるユーティリティです。またハードディスクブート領域のデータが壊れたとき起動できるように助けてくれます。（参照：Windows NTではSOSディスク作成ツールがありません。）

注意: SOSディスクを作成した後、ハードディスク フォーマットなどの作業でシステムのブート領域データが変更された場合、ブート領域のデータはSOSディスク作成時のシステム(変更前の)ブート領域データとは異なります。この点を無視して、SOSディスクに含まれている古いブートデータを上書きさせると、システムに致命的な問題が発生することもあります。従って、V3RESCUE.EXEプログラムをお使いになるときには注意してください。

Office Protector（Officeプロテクター）

MS-Office 2000またはMS-Internet Explorer 5.0で文書を開く、ダウンロード、OLEファイルを開くなどの作業中、ウイルス感染を診断・治療する機能です。

MS-Office 2000またはMS-Internet Explorer 5.0のプラグインを組み込む・削除するためには「ツール」－「Office Protector」を選択します。この機能にマウスポインタを持っていってダブルクリックすると、登録または削除を尋ねる次のような内容が表示されます。

プラグインを組み込むためには「登録」を、削除するには「削除」のボタンをクリックします。

Webリンク

メニューウィンドウからWebリンクを選択すると、Dr.安研究所のwebサイトにリンクできるツールがあります。Dr.安研究所ホームページ、安研究所ニュース、新種ウイルス情報、ウイルスFAQ、Webマガジン「ウイルスニュース」、オンライン登録などのメニューがあります。

- **安研究所ホームページ** - Dr.安研究所のホームページを開きます。
- **案研究所ニュース** - 新種ウイルスを始め、期間別ウイルス動向、V3新製品、Dr.安研究所方針などについて各メディアが提供する報道資料を読むことができます。
- **新種ウイルス** - 新種ウイルス警告に登録されているウイルスに関する情報です。被害件数が多かったり、症状が致命的なウイルスの種類とそれに関する情報を読むことができます。
- **FAQ** -コンピュータウイルスに関する疑問にお答えする所です。ウイルスの作動原理から種類、ワクチンソフトとの関係、ウイルス予防法などがわかりやすく説明されています。
- **Webマガジン「ウイルスニュース」** - 案研究所から発行する隔月刊行物「安コンピュータウイルス ニュース」を読むことができます。
- **オンライン登録** - カスタマーサポートを正常に受けるためのオンラインユーザー登録ができます。

付録

- ウイルス予防するための五原則
- 用語説明
- FAQ
- DOS用のV3+ Neoについて

ウイルス予防するための五原則

年々増えつつある新種コンピュータウイルスはワクチンソフトだけでは完全に退治するのが難しいです。一番重要なことは感染した後の退治ではなく、ウイルスに感染しないように予め予防することです。次のことを守れば、コンピュータウイルスによる被害はほとんど防げます。

1. 不正コピをしないで、正規の商品だけを使います。
2. 大事なプログラム、データは更新する度にパックアップします。
3. 新しいプログラムを使うときにはいつも最新バージョンのワクチンソフトで検査するし、定期的にすべてのハードディスクを検査します。
4. シェアウェアとかフリーウェアを使う場合、パソコンに詳しい人が長い間使っていたものをコピして使います。
5. 感染していないのが確認されたDOSディスクに書込み禁止をして非常時に使えるように前もって準備します。

用語説明

ウイルスと関連して様々な用語について述べます。

Back Door

システム設計者または管理者によって意図的に残されているシステム セキュリティの盲点として、アプリケーションとかOSに挿入されたプログラムコードです。即ち、Back Doorはシステムアクセスに対するユーザー認証など正常な手続きを取らなくてもアプリケーションまたはシステムにアクセスできるようにします。このようなセキュリティの盲点を残しておく理由は悪意的なものだけではありません。場合によっては現場サービスエンジニアとかシステム供給者の維持補修プログラマが使う目的として、特殊アカウントを許可するコードをOSまたはアプリケーションに入れることがあります。このようなBack Doorはデバッグするとき、開発者に認証及びセットアップ時間を節約するための裏門として使われます。しかしこのようなBack Doorはハッカーなどによって不法的なアクセスが試みられたり、開発が完了した後、削除されなかったBack Doorが他のユーザーによって発見された場合、侵入される恐れが高いです。

Back Orifice

略称BOとして、アメリカのハッカー集団「Cult of the Dead Cow」が開発・配布しているクラッキングツールです。他人のWindowsマシンを乗っ取り、インターネット(TCP/IP)などを通じて、遠隔地からデータの破壊を含むあらゆる操作を自由に行うことができるようになります。乗っ取りを行うためのプログラムは電子メールの添付ファイルの形で送られてきます。ユーザーが誤ってそのファイルを実行すると、乗っ取りプログラムがこっそりシステムの内部にコピされます。ハッカーは「管理者用」ツールを使って、遠隔地からインターネットなどを通じて、ユーザーに気づかれることなく、あらゆる操作（ファイル削除・コピ・移動、またフォルダ検索・作成・削除、ファイル圧縮・圧縮解凍など）を行うことができるようになります。またシステム情報を得る程度を越えてユーザーが入力する内容、パスワードを密かにキャプチァーしたり、それをファイルに保存してハッカーのパソコンに洩らすこともできます。システムを再起動することもできます。ユーザーよりも多くの権限をもって操作できるので特に注意する必要があります。Back Orificeはウイルスのように自分を複製する機能はないが、油断すると大きな被害を被る恐れがあるものをV3シリーズではトロイの木馬に分類して"Back Orifice Trojan"として診断・削除します。

Encryption Virus

ワクチンソフトで診断できないようにウイルスプログラムまたはその一部を暗号化して保存したウイルスです。暗号型ウイルスにはCascade Virus、Slow Virusなどがあります。

Excel Macro Virus

スプレドシートの世界標準といえるExcelのマクロ機能を利用して感染するもので、Excel文書に感染させます。代表的なものとしてはLaroux、ExcelMacro.Extras、ExcelMacro.VCX、ExcelMacro.Compatなどがあります。

Hacking Version

ハッキングバージョン(Hacking Version)とは製作者(社)が作ったことのないプログラムです。それで、ハッキングバージョンを実行すると、プログラムの削除、ハードディスクフォーマットなどの異常な作動でユーザーに被害を与える場合があります。V3シリーズのハッキングバージョンによる被害を受けないためには次のことを必ず確認してください。

各パソコン通信(Hitel, Chollian, Nownuri, Unitel)にある研究所フォーラムの資料室だけからダウンロードしてお使いください。もし、フォーラムの公開資料室に乗っている非登録版より最新バージョンがあれば、それは当然ハッキングバージョンになるでしょう。

PKZIPではなくRARまたはARJなどの圧縮ユーティリティで圧縮されたV3+は使用しないでください。

PKZIPファイルの圧縮を解凍したとき-AV検査と共に最後に次のようなメッセージが表示されるかを確認して、もし表示されなかったらご使用にならないでください。それに、そのファイルの出所を案研究所に届け出て下さい。(但し、WINZIPで解凍すると表示されません。)

″Authentic files Verified! # SUR710

Dr. Ahn's Anti-Virus Laboratories, Inc.″

Linking Virus

プログラムに直接感染させないでディレクトリ領域に保存されているプログラムの「開始」位置をウイルスプログラムの「開始」位置に変更します。従って、プログラムを実行すると元のプログラムの代わりにウイルスプログラムが先に実行されるし、プログラムを閉じると元のプログラムを終了させてユーザーが気づかないようにします。その体表的な例がByway Virusです。

Logic Bomb

正常なプログラムに隠されたルーチンを挿入して、そのルーチンが不法行為の対象になるシステムでルーチンが決まった論理条件が合うと、ルーチンに挿入された命令を実行するようにします。例えば、決まった時間になると、システムが利子を計算する方式または利子率を変えて計算して残りの金額を、それを意図した他人の預金口座に送金するようにさせることがこれに属します。また、決まった条件に合ったらシステム運営に必要な基本ファイルを削除してシステムの作動を中断させたり、パソコン通信で自分と敵対関係にいるユーザーがパソコンを使うとそのユーザーのディレクトリにあるファイルを全部削除する破壊的なやり方にも使えます。

Overwriting Virus

これらのウイルスはプログラムにリンクし、元のコードはそのままにして、できるだけ多くのファイルに付着することでファイルに感染します。従って、感染したファイルを実行すると元のプログラムの代わりにウイルスプログラムが実行され、元のプログラムが破壊されます。その為ワクチンプログラムでも復旧不可能になる確率が高いです。但し、上書きウイルスがプログラムで未使用領域に入った場合は、元のプログラムを実行するに影響を及ぼさないのでワクチンプログラムで復旧できます。

Parasitic Virus

これらのウイルスはプログラムを破壊しないで、元のコードはそのままにしておいてファイルの前後に付着することでファイルに感染します。寄生型ウイルスに感染したファイルは元のプログラムとウイルスプログラムが共存して増殖する以外は何もしません。ユーザーはウイルスプログラムが実行された後、元のプログラムが実行されるのでウイルスに感染していることに気づかないことが多いです。殆どのファイルウイルスがこのタイプに属します。

Possible Virus

一部のメインボードで、low-level formatとかハードディスク セッティングをしようとすると"possible virus"というメッセージが現れる場合があります。このようなメッセージが現れる理由はCMOSセットアップ で"Boot Record virus protection"関連オプション（このようなオプションはボードによって異なりますが、）をenableに設定したからです。このオプションはブートセクターにウイルスが入るとユーザーに警告をするオプションとして外からブートセクターを変更しようとすると、ユーザーに知らせてくれる役割をします。このオプションを"Disable"または"Normal"に変更した後、作業をすればそのメッセージは現れません。

Primitive Virus

初めて、現れた第1世代コンピュータウイルスとも言えます。プログラムの構造が単純なもので、Stoned Virus,Jerusalem Virusなどがあります。

Spawning Virus

EXEファイルに直接感染させないで、同じファイル名のCOMファイルを作成してウイルスプログラムを入れておきます。同じファイル名のCOMファイルとEXEファイルが同一ディレクトリに存在するとき、ファイル名を入力して実行させると、COMファイルが先に実行されるのでファイルウイルスに直接感染したときと同じ現象が起こります。代表的なものとしてはAIDS II Virusがあります。

Stealth Virus

ウイルス自身がユーザーやワクチンに発見されないよう、さまざまな工夫を凝らしたタイプ。ステルス型ウイルスは、従来のウイルス検出ツールの目を逃れられる特殊な技法を使っています。即ちステルス型ウイルスは、実行されたときにメモリに潜むことでこのようなトリックを行い

ます。ステルス型ウイルスはファイルやブートセクターに付着しますが、ホストソフトウェアを調べても、普通と変わらず変化がないようにみえます。スキャナが検索のためにファイルを開くと、ウイルスが一時的にファイルから離れ、正常であるように偽装するのでワクチンやユーザーは騙されます。この種類にはBrain Virus、Joshi Virus、512 Virus、4096 Virusなどがあります。

Worm

ファイルやシステム領域に直接感染するものではありませんが、ネットワークを通じてほかのマシンに拡散することを目的とした不正プログラムです。代表的なワームにはHLLC.AIDS_II、HLLC.Even_Beeper、HLLC.Laufwerkなどがあります。インターネットが普及した現代のワームの特徴は、メールを最大限に利用することにあります。インターネット ワームプログラムを実行すると、従来のワームとかウイルスのように他のフォルダ、ファイルに感染増殖するのではなく、ワームプログラム自身を添付して自動的にメールを送信する機能を持っています。インターネット時代にふさわしく、近年のワーム型の隆盛はすさまじいものがあります。今後もっとも注意が必要なタイプと言えます。

Word Macro Virus

MS-Word文書に感染するウイルスです。例えば、Word97Macro.CLASSウイルスは多形態と隠蔽技法を使っていて、Word作業終了時メッセージを表示します。

Windows Virus

Windows OSを基盤としてウイルスです。1992年に発見された最初のWindowsウイルスであるWinVirを始め、Boza、Tentacle、Marburg、CIH Virusなどがここに属します。

WindowsウイルスはDOSウイルスに比べ治療し難い面があり、 ビギナーを悩ませるものです。Windows環境では感染したファイルが実行中であると、治療できないのでプログラムを閉じてから治療しなければ安定的に治療できません。

コンピュータウイルス (Computer Virus)

「ユーザーが知らないうちに他のプログラムにウイルス自身を複製するプログラム」と定義できます。より正確には「すでにホストシステムにあるコンピュータコード（プログラムまたは実行可能なファイル）を変形して、そこに自身または自己の変形を増殖しながら蔓延するように設計されたプログラム」です。

ウイルスという名前がついた理由は生物ウイルスが自己を複製する遺伝因子を持っているのと同じく、この悪質プログラムも自己を複製するコマンダーを持っていて生物ウイルスに似ているため、コンピュータウイルスと呼ばれるようになったのです。従って、「コンピュータウイル

ス」というより「コンピュータウイルス プログラム(Computer Virus Program)」と言った方がより正確な表現です。

システム領域感染型 (Boot Virus)

ハードディスクのシステム領域（ブートセクター、パーティションテーブル）に感染するウイルスです。DOSの仕組みにより、システムファイルよりも先にウイルスがメモリにロードされるので、ウイルスはDOSの割り込み命令の制御を完全に奪うことになります。このため、通常の起動プロセスの前にウイルスが呼び出されることになります。世界で初めて発見されたウイルスであるBrain VirusとMichelangelo Virusなどがブートウイルスに属します。

デマウイルス (Hoax Virus)

実際には存在しないウイルスに対して脅威を呼びかけるデマ情報をデマウイルスと呼びます。警告でもない警告をしながらチェーンメール的に転送させることを促し、混乱の拡大を狙っています。内容は主に特定の題目のメールを受けると「メールを読むだけで感染する」 といった、ウイルスの活動としては考えにくいことが記述されています。"Returned or Unable to Deliver" or "Penpal Greetings!"という題目の手紙を読んではいけないというのも同じ症状を見せます。これらのメールは技術的な用語をまさに本物のように見せかけていますが、いたずらメールに過ぎないのでこのようなメールは直ちに削除してください。

トロイの木馬型 (Trojan Horse)

「自己伝染機能はなく、発病を意図して作られたプログラム」のことです。より正確に「システムに中にユーザーが意図しない動作をするもので、ほかのファイルやシステムに感染活動を行わない、つまり増殖を目的としない不正プログラム」のことを指します。

トロイの木馬プログラムは意図的である点から、プログラマの過ちであるバグ(Bug)とは異なります。また、他のファイルに自己複製しない点からコンピュータウイルスとも区別されます。例えば、あるプログラムを実行したときハードディスクのファイルを削除するだけで他のプログラムに複製しなければ、これはコンピュータウイルスではなくトロイの木馬プログラムです。

ハッカー(Hacker)

元々はコンピュータ技術に精通したマニアのことを言い、コンピュータ及び通信に優れた実力の所有者を指しますが、９０年代初めには、コンピュータ技術を悪用して他人のコンピュータに侵入・無断閲覧・変造・破壊を行う者を「ハッカー」と呼んでいます。最近になってはインターネットを中心としたサイバー空間での犯罪行為をする恐れの高い人々を指す用語としても使われています。本来ハッカーには悪い意味はなく、これらの人々は「クラッカー」と呼んで区別すべきであります。

ブート/ファイル感染方(Boot/File Virus)

ブートセクターとファイル両方に感染するウイルスとして、Natas Virus、One_Half Virus Tequila Virusなどがある。

ファイル感染型(File Virus)

これらはファイルに付着することで感染しますが、付着するのは一般に、アプリケーションやプログラムを制御する.EXEや.COMファイルなどの実行可能ファイルです。その他 Overlay File、デバイスドライバ(Device Driver)などに感染します。

マクロウイルス(Macro Virus)

現在、もっとも遭遇しやすいウイルス。マクロウイルスとは、MS-Officeのマクロ機能を利用して感染するもので、機種・OS等にも依存しないで感染することからマルチプラットホーム型ウイルスと呼ばれることもあります。開発の容易さ、電子メールの普及などさまざまな要素が絡み合って全世界的に被害件数を急激に伸ばしたウイルスです。

ミューテーション型(Polymorphous Virus)

ミューテーション型ウイルスは、自身を複製する度にウイルス自体の暗号化コードをランダムに改変するので、感染する度に暗号化ルーチンが変化します。このため、既存のウイルスパターンを検索する大半のワクチンソフトでは発見が極めて困難です。多形態コンピュータウイルスの中には一つのウイルスから派生された多形態ウイルスが、100万という形態のどれにでもなれるので識別が困難になります。

メモリ常駐型(TSR Virus)

感染プログラムが実行される際にメモリに常駐します。常駐後、未感染ファイルが実行される度に感染します。Jerusalem Virus, Dark_Avenger Virusなどがこれに属します。

メモリ非常駐型(Non-TSR Virus)

感染プログラムが起動されるとき、ウイルスがメモリに常駐しなくて消えてしまうウイルスとして、Taiwan Virus、Vienna Virusなどがあります。

FAQ

Q **1. V3Pro 2000 Deluxeで「治療不可能ファイルは削除」のオプションを指定するとその削除されたファイルは「ごみ箱」に残りますか。**

A 「治療不可能ファイルは削除」のオプションを指定して削除されたファイルは、「ごみ箱」に入らなくて永久に削除されます。たまにこのオプションを使って削除されてからもファイル名がそのまま残っていますが、ファイルのサイズは0バイトである場合があります。これは使用中であるファイルなのか、パスワードが掛けられていたファイルなので現れる現象として、復旧できる方法はありません。もしバックアップファイルが残っていればそのファイルを使って治療した後、使ってみてください。

Q **2. V3Pro 2000 Deluxeの快速検査バーで直接フォルダ名を入力して検査しようとしますが、うまくいきません。**

A 入力方法に問題はないか確かめてください。快速検査バーでの検査対象入力時フォルダを区分する記号はスペースです。また複数のフォルダ入力もスペースで区分するし、長いフォルダ名とか空白のあるフォルダ名は“ ” で区分します。50ページを参照してください。(参照：対象フォルダはサブフォルダまでは検査しないのでサブフォルダまで含ませるためには /s オプションを指定してください。)

Q **3. 現在V3Pro 2000 Deluxeの正規製品を使用中です。あるインターネットプロバイダーに加入後、ただで貰ったV3+Neoがあります。これらをどのように使えばよろしいですか。**

A V3+ NeoはDOS用のワクチンです。お客様がV3Pro 2000 Deluxeの正規製品をご使用中なら、そのプログラムの中に既にDOS用のワクチンV3+Neo登録版が含まれているのでそれをお使いください。

インターネットプロバイダーから貰ったV3+ Neoはシェアウェアとして正規製品とは異なり、ネットワークドライブ診断機能とか、マクロウイルス治療機能など一部の機能が使えません。

Q **4. V3Pro 2000 Deluxe CD-ROMをドライブに入れましたが、自動インストールができません。CDの中にAUTORUN.INFファイルも存在するのに自動インストールできない理由は何ですか。**

A V3Pro 2000 Deluxeは自動インストール機能、即ちAUTORUNが実行されます。もしAUTORUNが実行されなかったら、次の事項を確かめてください。Windowsの「マイ コンピュータ」をクリックしてからマウス右ボタンを押します。この時「プロパティ」－「デバイス マネージャ」－「CD-

ROM」をクリックすると、組み込まれているドライブ名が表示されます。そのドライブ名をダブルクリックして、「プロパティ」－「設定」メニューをクリックした後、「挿入の自動通知」機能がチェックされているかを確かめてください。もしチェックされていなければ、V3Pro 2000 Deluxeだけではなくいかなる CD-ROMのAUTORUNも実行されません。

とりあえず、「挿入の自動通知」機能にチェックを入れてから、再起動するとAUTORUNが実行できます。

(参照：AUTORUNが実行されないようにするためには<Shift>キーを押して、CD-ROMを入れれば、自動実行されません。)

Q 5. 「ツール」－「Neo Scan」を実行してウイルスを検査した後、Windowsに戻りません。

A Neo Scan機能を使うために一時的に使用するファイルであるautoexec.batとautoold.batがお互い繰り返し実行され、起こる現象です。起動後、Neo Scanが実行される前に<Ctrl-C>または<Ctrl-Break>キーを押してbachファイルが実行されないようにしてから、autoexec.batとautoold.batファイルのファイル名を変更するか、別のフォルダに移動した後削除すると正常な起動ができます。

Q 6. エンジンアップデートのとき「組み込まれているV3製品がありません。」というメッセージが現れます。

A エンジンアップデートを行ったとき、V3エンジンアップデート ウィンドウに「組み込まれているV3製品がありません。」というメッセージが現れる場合があります。このメッセージはユーザー情報、ワクチンの組み込みパスなどの情報が保存されているC:¥V3AHN.CFGファイルが削除されたかファイル内部が壊れてエンジンアップデートを行えないとき現れます。確認方法はV3Pro 2000 Deluxeを実行して「ヘルプ」－「V3Pro 2000 Deluxe 情報(A)」を選択するとユーザー名と製品番号が表示される位置に損傷されていることを知らせるメッセージが表示されます。この場合には組み込まれているワクチンをWindowsのアンインストール機能を使っては削除できない場合もあるので組み込まれているワクチンのフォルダを手動で削除してから再インストールしてください。

Q 7. V3+ Neoでウイルスを治療しようとしましたが、「ディスクに書き込みができません」というエラーメッセージが現れ、治療できません。

A Windows 98／95のシステムがブートウイルスに感染したとき、DOSプロンプトを開いてV3+のように治療しようとすると、このようなエラーメッセージが表示されます。このようなエラーメッセージが現れるのはWindows 98/95自体がブート領域のデータを管理するためであり、このために正常な治療ができません。この場合にはブートウイルスに感染していないDOSバージョン6.2以下の起動用のディスクで再起動した後、また

治療してください。

Q A 8. システムの基本メモリが640 Kbyteではなければ、ブートウイルスに感染したことになりますか？

一般的にコンピュータの基本メモリは640 Kbyteの大きさを持っています。ブートウイルスに感染すると基本メモリの大きさが大体減りますが、ブートウイルスに感染しなくても基本メモリが640 Kbyteではない場合が多くあります。一部 AMI BIOSを使っているコンピュータの場合には639 Kbyteである場合もあるし、Pentium PCI機種は基本メモリが637 Kbyteである場合も多いです。その他にもWindows環境によって、基本メモリの大きさは変わることがあります。

Q A 9. V3BACKUP.EXEはどこに使いますか？

V3BACKUP.EXEファイルはブート領域のサンプルを簡単に採取できるユーティリティです。一般的に多くの方が「基本メモリが640 Kbyteではないと、まずブートウイルスに感染したのではないか」と疑う場合が多いですが、取り敢えずウイルスに感染していない起動ディスクを使って、A:ドライブで起動してから基本メモリの大きさを比較したとき同じだったら安心してもいいです。もし違う場合にはウイルスに感染した恐れがあるのでV3BACKUP.EXEを使って、ブート領域のデータをファイルとして送ってください。V3BACKUP.EXEを実行する時、ドライブを指定して実行すると、（例えば：V3BACKUP.EXE C:）V3BACKUP.EXEを実行させたフォルダに次のようなファイルが生成されます。：

ファイル	説明
MBS.V3	ハードディスクの主ブートセクター
DBS.VS	ハートディスクのDOSブートセクター
FBS.V3	フロッピディスクのブートセクター

即ち、ハードディスクのブートセクターが疑われる場合はMBS.V3とDBS.V3Ifを、フロッピディスクのブートセクターが疑われる場合にはFBS.V3を研究所に送ってください

Q A 10. マクロウイルスを治療するには？

MS-Officeにあるマクロ機能を利用したマクロウイルスが全世界的に発見され続けています。現在全世界的に既に2000種類以上のマクロウイルスが発見されており、これからもこのような増加傾向は続くでしょう。今まで発見されたマクロウイルスの殆どはMS-Word/Excelのデータファイルに感染する2種類として、これからも多くの変形ウイルスが続けて発見されるだろうと思われます。

Q 11. ウイルス名が数字で表示されますが...

A V3シリーズでウイルスを診断したとき、ウイルス名が数字で表示される場合があります。このような症状はV3シリーズが組み込まれているフォルダまたはV3.EXEファイルが実行されたディスクにV3WARPN.V3Dファイルが無いとき起こります。ディスクにDOS用プログラムであるV3.EXEファイルだけコピしてお使いになっている方が多いですが、V3WARPN.V3D, V3WARPD.V3D, V3WARPA.V3Dファイルも必ず一緒にコピしてお使いください。

Q 12. V3Pro 2000 Deluxeインストール時SOSディスクを作成しました。自分のパソコンで作成したディスクを友達のパソコンで起動したとき,トラブルが起こりました。

A SOSディスクはSOSディスクを作成したパソコンのハードディスク情報を持っており、ハードディスクが認識できない緊急な事態に備えて、起動できるようにする為に作っておくディスクです。従って、必ず書込み禁止にして保管しなければなりません。起動するだけなら大丈夫ですがV3RESCUE.EXEを実行させると元のシステムにあるハードディスクのブート領域データを他のハードディスクに自動コピするので、お友達のパソコンのブート領域データが変わってしまって、起動できなくなることもあります。

Q 134. Back Orifice Trojanというウイルスに感染しましたが、治療できません。

A Back Orifice Trojanのようにウイルス名の中に“Trojan”が含まれているのは他のファイルに感染するウイルスではなくユーザーの作業を妨げるなどのトラブルを起こすトロイの木馬プログラムです。このプログラムによる損害を防止するためにはV3シリーズで診断、削除しなければなりません。その他HLLCで始まるspawningウイルスも他のファイルに直接感染しないのでこのようなファイルも発見したら、直ちに削除してください。

DOS用のV3+ Neoについて

構成

V3+ NeoにはV3.EXE, V3BACKUP.EXEプログラムが含まれています。V3.EXEは今まで韓国で発見されたコンピュータウイルスを診断・治療するプログラムで、V3BACKUP.EXEはブートウイルスに感染したブート領域のサンプルを簡単に採取できるユーティリティです。

V3.EXE(診断・治療用)の使い方

基本的な使い方

V3.EXEは韓国内外のコンピュータウイルスを診断して治療してくれるプログラムです。例えばC:ドライブを検査するためにはDOSプロンプトで次のように入力します。:

```
C:¥>V3
```

オプション指定

V3.EXEを実行するとき使えるオプションは次の通りです。:

V3 [ドライブ名][パス][ファイル][オプション]

オプション	説明
/L	使用言語
/L:E	英語
/L:K1	組合せ型　韓国語
/L:K2	KS完成型　韓国語
/F	複数のフロッピディスク検査
/S	サブディレクトリ検査
/A	すべてのファイル検査
/U	ウイルス自動治療
/?	使い方印刷

どんなオプションも使わないか、"/?"オプションを使った場合には基本的にメモリを検査・治療した後、使い方を表示します。

ドライブだけ指定した場合にはまずメモリと自己検査をするし、フロッピディスクの場合にはブートセクターを、ハードディスクの場合には主

ブートセクターとDOSブートセクターを検査した後すべてのディレクトリの実行ファイルを検査します。

パス名を指定した場合にはそのディレクトリの実行ファイルを検査します。パス名はメインディレクトリを含めて完全なパス名を使うことも、現在のディレクトリを基準にした相対的なパス名を使うこともできます。

ファイル名を指定した場合はそのファイルだけ検査します。

ファイル名、拡張子(extension)にはワイルドカード(wild card, ？ または*)が使えます。

V3BACKUP.EXEの使い方

ブートウイルス採取について

V3BACKUP.EXEはユーザーが簡単にディスク情報のバックアップ及びブートウイルスを採取できるユーティリティです。新しいブートウイルスに感染した場合、感染していない新しいフロッピディスクで起動した後V3BACKUP.EXEユーティリティを使って感染したブートセクターをファイルにして案研究所に送ってください。

感染していない場合でもV3BACKUP.EXEを使って、ブートセクターをバックアップしておくと、ブートセクター復旧の際有用な資料として使えます。

使い方

DOSプロンプト状態で次のように入力すると、指定したドライブ（A: または C:)の主ブートセクター及びDOSブートセクターをファイルに換えて現在のディレクトリに保存します。

C:¥>V3BACKUP C:

V3BACKUP.EXEを実行するとき使えるオプションは“ /?” オプションだけです。ドライブを指定しないか、“ /?” オプビョンを使った場合には使い方を表示します。ブートセクター採取のためにはドライブ名を必ず指定しなければなりません。指定したドライブのブートセクターを採取すると次のようなファイル名で保存されます。

ブートセクター	ファイル名
フロッピディスクのブートセクター	FBS.V3
ハードディスクの主ブートセクター	MBS.V3
ハードディスクのMS-DOSブートセクター	DBS.V3

また、RAMドライブ、CD-ROMドライブ、ネットワーク ドライブなどブーティング不可能なドライブを指定した場合はエラーメッセージが現れて、ファイルを生成しません。

付録

안철수컴퓨터바이러스연구소
DR.AHN'S ANTI-VIRUS LABORATORIES, INC.

Dr.安コンピュータウイルス研究所はウイルスワクチン、コンピュータセキュリティと有害情報遮断に関する製品を開発・販売しています。またコンピュータ関連犯罪の予防・退治とセキュリティ関連広報・啓蒙活動を行っています。