

Preface

導入の前に

この度はNOD32 アンチウイルス（以降NOD32）をお買い上げいただきありがとうございます。このユーザーズガイドには、本製品のインストールから実際の使用方法までが記載されています。本製品を正しくご利用いただくために、必ずこのユーザーズガイドを一読されておくことをお勧めします。

また、このパートでは本製品を使用するうえで知っておくと役に立つ基礎的な知識も紹介しています。

ソフトウェアライセンス契約書

本契約書（以下「本契約」とします。）は米国カリフォルニア州法人 ESET, LLC.（以下「ライセンサー」とします。）と以下の条件について、本契約の締結者（以下「お客様」とします。）との間で締結されます。

1. **製品** 本契約は、お客様とライセンサーとの間の NOO32 アプリケーションシステム（以下「本製品」とします。）に関するライセンス契約書です。本製品には、付随文書およびお客様に配布される可能性があります。全ての修正、リリース、アップグレード、ウイルスステータアップデート、新バージョン、強化バージョンを含むこととなります。

2. 初期使用

本製品は、お客様に電子的なダウンロード版として、もしくは、自動インストール機能付きのメディアで提供されます。お客様は、本製品を付随文書に規定された適切なコンピュータにインストールすることが必要です。お客様は当該コンピュータに、本製品の存在に対して反対の動作を要するソフトウェアや機器が設定されていないことを確認する必要があります。

3. 使用許諾環境

(a) 使用環境 お客様が本契約に合意し、第 2 条（初期使用）で規定されたインストールを行い、第 7 条（価格及び支払）で規定されたライセンス費用を支払ったことを条件として、ライセンサーはお客様に本製品のライセンスの非独占的な使用権（インストール・保存・ロード・実行および表示することを総称して使用とします。）を許諾します。なお、お客様の、発注書に明示され、お支払いを行った数のコンピュータ並びにプラットフォームについても、同様に使用権を許諾します。本製品は機械翻訳のオブジェクトコード形式でのみ提供されます。

(b) 使用者 本製品はお客様およびお客様の法人の従業員のみ使用可能です。当該使用者は、第 4 条（使用目的）で述べたため、前項の使用環境において本製品を使用することができます。

(c) 災害復旧用例外条項 火災・水害・地震・暴動等のお客様に責がなない災害の場合、お客様は、60日間に限り、前(a)項の使用環境と実質的に同様の環境のバックアップコンピュータ上へ本製品を移行し当該環境で使用する可能性があります。お客様は、当該期間の範囲内では、非常事態が続いている間に限り、独立した復旧センターの職員を使用者が指定することができます。非常事態が解消された場合、お客様は本製品を元の環境に戻し、バックアップ機器から全ての複製物を消去して下さい。

4. 使用目的

お客様は、本製品を使用環境において、お客様自身の業務の処理に、また、ソフトウェアライセンスが購入されたコンピュータ上に保管されたお客様自身の情報を物理的に保護し、使用することとなります。

5. 権利の留保

(a) 本製品に関する権利 本製品に関する知的財産権はライセンサーおよび付随文書に記載されたそのほかの所有者の財産です。本契約に合意し適切なライセンス料を支払う限りにおいて、お客様は、オブジェクトコード形式で本製品を使用するに限定した許可を与您えられたこととなります。お客様は、本製品を逆アセンブル、デコンパイル、リバースエンジニアリング等によって解析しないことに合意することとなります。お客様は、また、本条項の制限を侵害したことがより詳細な情報は、本製品の知的財産権者に自動的に移管され、当該権利者の独占的所有物となる秘密情報であることを合意することとなります。お客様は、本製品に際する秘密情報について、常に通常の管理の注意を払い、保管ならびに保護することとなります。お客様は、本製品に關して出所・品名・権利所有者が判別される、全てのマーク・注意書き・表示を取り除かず、また可読状態に保つておくこととなります。

(b) 権利留保 本契約中の他の条項によつてお客様に明示的に許諾されたものを除き、ライセンサーは以下の権利を留保し、お客様は、直接か間接を問わずまたは一部か全体かを問わず貸与・賃貸・リース・再許諾もしくはそのほかの方法により複製すること、第三者の利益のために本製品を使用すること、および、本製品を変更・改訂・翻訳およびそのほかの派生的な製品を作成することを禁止されています。但し、ここでいう改訂は、使用者が、保管の目的でおよび、使用環境での本製品を使用する目的のために欠かさない行為として、本製品の複製を行うことを禁止していません。

6. 製品サポート

お客様は、ライセンサーおよび認定販売代理店が通常提供する範囲で、公衆回線による電話サポート並びに本製品のアップデートサービスを受けられます。

(a) 電話サポート お客様は、本製品の修正版に関する変更、ならびに、最新バージョンに関する使用・操作方法についてライセンサーまたは販売代理店の通常の営業時間内に電話または、その他の手段によるサポートサービスを受けられます。お客様は、連絡した問題点が再現できるような、十分な情報を提供する必要があります。必要な場合には、お客様の許諾並びに通常のセキュリティ手段を通じて、本製品にリモートアクセスが可能な手段を提供して頂く場合がございます。

(b) アップデート お客様は、本製品および付随文書のアップデートならびに改訂版を受領することができます。当該情報が、新バージョンもしくは機能向上版であるアップデートであるかというライセンサーの表示は、明らかな誤りの場合を除き、決定的なものとなります。アップデートはライセンサーまたは販売代理店のオンラインシステムを通じてダウンロードすることができ、ライセンサー及び販売代理店は、全てのそれ以前のアップデートが適用された最新バージョンのみを製品サポートの対象としておきますので、お客様は全てのアップデートを適切に適用する必要があります。

(c) サポート条件 ライセンサーは、以下の各号の場合に製品サポートを提供する義務を負いません。

- (i) 当該問題点が、本製品のソースコード・プログラムのパラメータそのほかのお客様が変更可能な点を、許可を得ずに変更したことによる場合、
- (ii) 当該問題点が使用者のミスによるか、ライセンサーが提供した以外のデータもしくはソフトウェアによる障害や使用目的外の使用や、付随文書に記された使用の場合、
- (iii) 当該問題点が、以前のバージョンで発生し、お客様が未適用のアップデートで既に修正されている場合。

7. 価格および支払

(a) 価格 お客様は、本製品が発注された時点のライセンサー（または販売代理店）の公表価格表に定められたライセンス料、をライセンサーもしくは販売代理店およびその代理人に対して支払うこととなります。ライセンス料の支払によって、お客様は本契約の期間中、本契約の規定に従い本製品を使用する権利を賦与されます。製品サポートの費用については別途とします。

(b) 支払 ライセンサーまたは販売代理店の請求書により、お客様はライセンス料金および出荷費用を、納品後しかるべく支払うこととなります。お客様は、ライセンサーの所得および収益に付加される税金を除き、全ての販売・使用・付加価値・一般消費税・資産税およびそのほかの税と、当該税金を対して付加される全ての手数料等を負担することとなります。もし、支払期限までににお支払いが行われなかった場合、お客様の本製品に関する使用権は自動的に停止され、お客様は、しかるべき法的な手続を含み、使用権に関わる費用を負担することとなります。

(c) ライセンサーが明示した場合、試用期間中にライセンス料が適用されません。

8. 譲渡

お客様は本契約に基づき本製品に関する権利を第三者に譲渡することはできません。

9. 保証

以下の各項の規定は第 1 条（損害賠償制限）の規定に従うこととなります。全ての保証はお客様自身に関するもののみとし、誤差不能であり、いかなる第三者にも適用されません。

(a) 権利侵害に関する保証 ライセンサーは、本契約を締結する権限を有し、その知りうる限りにおいて、お客様による本製品の使用環境における使用目的を著し、第三者の請求における著作権・商標権・特許権または営業秘密を侵害しないことを保証します。これに反する全ての国法が、適切にライセンサーに通知される限り、ライセンサーは、以下の各号のいずれかの措置を執ることをします。

- (i) お客様が本製品を使用し続けられるよう、法的手段により防衛するか交渉により権利取得する。
- (ii) 本製品を変更し、もとの機能を持ったまま当該侵害が無くなるようにする。
- (iii) 本製品を同様の機能のあるものに置換する。
- (b) ソフトウェア媒体 ライセンサーは、本製品が記録された磁気・光学媒体および付随文書が、物理的な障害がなく、マスター媒体から正確に複製されたものであることを保証します。ライセンサーまたは販売代理店は、当該障害がある媒体ならびに付随文書を交換しますので、ご購入の証拠書を添えてお申し込み下さい。
- (c) 動作に関する非保証 本条に記載されている以外では、お客様は、本製品ならびに関連するサービスが「そのまま」の状態で、明示されたあるいは暗示的な品質、仕様への適合、信頼性もしくは機能性に對して保証および他の証明無しに提供されるものであることに、合意することとなります。お客様は、本製品の適合性、動作および不動作に關して、全てのリスクを負担することとなります。ライセンサーは、本製品について明示的・暗示的に拘わらず、一切保証せず、商品性・権利・特定目的への適応について、全ての暗示的な保証を行わないこととなります。お客様の居住する地域により、暗示的な保証の範囲を制限することが認められていない場合があり、その場合には、上記保証制限も適用されないものとします。本契約はお客様に特定の法的権利を賦与するものとして、お客様にお住みの地域の法律により異なる権利が賦与されます。2000年法廷に關する記載に關しては、米州連邦法の規定による「Year 2000 Readiness Disclosure」として連邦法の規定による保証の対象となります。

10. ソフトウェアロックおよび非開示機能

ライセンサーは、本製品には、付随文書に記載されたセキュリティ機能を除いて、付随文書に記載された操作を制限するあるいは機能を停止せよ。計時機能、カウンター、使用メーター・錠および類似の機能を機能を持たないことに保証します。

11. 損害賠償制限

以下の各項目は、本契約の実質的な条件を記載しており、リスクの適正な配分を反映したものです。救済 お客様は、ライセンサーが保証事項ならびにその他の本契約条項に違反し、ライセンサーが修復またはそのほかの修正が経済的・技術的に可能であると判断した場合に、お客様が支払ったライセンス料の返金を受けることができ、最大限の救済措置とあることに合意することとなります。お客様は、また、本製品中のライセンサーの知的財産権の保護について、法的救済が不十分ものか否かという場合、そのほかの救済措置に加えて、ライセンサーが特に約定無しにそうした権利を一時・恒久的に法廷の命令を得ることとするに合意することとなります。

(b) 損害賠償 お客様はライセンサーがお客様が本契約に基づき支払ったライセンス費用を超える損害賠償義務を負わないことに合意することとなります。いかなる場合においても、ライセンサーは、それら契約上の救済による損失を含む不法行為によるものも、いかなる間接的、偶発的、経済的損害（利益またはデータの喪失、データの消滅、業務の中断を含む、そうした損害の可能性が事前にライセンサーに告知された場合をふくみます）に對して損害賠償義務を負いません。この対象は、お客様、お客様の顧客、および、全ての第三者の損害を含みます。この対象はライセンサーならびに販売代理店・販売店を本製品を購入了お客様が保護するためのものです。地域によっては、経済的・偶発的損害に対する損害賠償制限が禁止されている場合には、ここでいう損害賠償限定はお客様には適用されません。

12. 期間および契約

(a) 一箇条項 本契約は、本条項または他の条項に従い締結されない限り 1 年間有効とし、ライセンス費用の支払により更新可能とします。本契約は、お客様がいずれかの条項に違反した場合自動的に解約されます。また、お客様は、お客様の判断によりいつでも本契約を解約することができます。

(b) 解約の効力 本契約の解除により、お客様は本製品を保有する権利を喪失します。いかなる理由による解約の場合も、お客様は本製品および付随文書のオリジナルおよび全ての複製物を廃棄し、契約後の使用を中止することに同意することとなります。本契約の解除後第 5 条(a)（本製品に関する権利）第 9 条（保証）第 1 条（損害賠償）第 1 4 条（輸出規制）の各条項については、有効に存続するものとします。

13. 紛争の解決・管轄法

第 1 条（損害賠償）で認められた特定の法廷の命令による場合を除き、ライセンサーおよびお客様は、本契約に関する全ての紛争は、アメリカ仲裁協会の商事仲裁規則に従って、一人の仲裁人に提出されるものとする。仲裁人の書面による決定内容の明示がある決定は、法廷による決定と同様、両者を拘束し、法廷においても有効性を維持することとなります。本契約の管轄法は、アメリカ合衆国連邦ならびにカリフォルニア州法とし、裁判によって解決される場合は当該国の裁判所を第一審管轄裁判所とします。お客様は、紛争の発生から 1 年以内に訴訟を提起しなかった場合、当該訴訟は無効とします。

14. 輸出規制

技術的環境を超えての移転は、米国政府および各国政府により規制されています。お客様は、必要な政府の許可を事前にて得ること無しに、本製品を間接的・直接的に輸出しないことに合意することとなります。お客様は、米国商務省輸出管理局の許可が必要な場合には、書面による許可無しに、規制対象の技術や、米国の政府の規制対象となつている国へ、直接的または間接的に輸出しないこととします。本条は、本契約の解除後も有効とします。

15. 米国政府機関権利留保

本製品および付随文書は、権利留保事項に基づき提供されます。政府機関による使用・複製・開示は、DFARS 227.7202-3 の商用コンピューターソフトウェア条項または、48 CFR 52.227-19 のサブ(グラフィック)(c)および(2)の商用コンピューターソフトウェア権利留保事項の適用可能な方の制限に従います。Contractor は ESET, LLC. です。

16. その他の条項

本書面はライセンサーとお客様との間のここに記載された事項に関する全ての合意事項であり、全ての書面もしくは口頭による伝達事項に優先します。本書面、並びにお客様に電子的なサイン（もしくは合意）を通じて印刷されたハードコピーは、本契約の有効性に疑義が生じた場合に、証拠能力がある署名がある書面として、オリジナルなものと認められます。お客様は、当該税金を対して付加される本製品は、本契約の効力に影響を与えません。本契約はライセンサーの承認された代表者の署名のある書面によるのみ改訂または修正されます。本製品の販売者または販売代理店は、本契約を変更する権限を有しておりません。もし、本契約の一部の条項が法廷により違法もしくは無効と判断された場合には、本契約は、法的に必要な最低限まで変更され、本契約のその他の条項は全て有効とします。特定の条項に関して、一方が請求を行わなかったとしても、以後の当該条項に関する請求を妨げるものではありません。見出しは参考のためであり、重要性がないこととなります。

本書の表記について / お断り

NOD32をインストール後、設定の変更を全く加えていない状態を「既定値」と表記しています。

アイコンやボタンなどに \leftarrow ポインタを合わせ、マウスの左ボタンを1度押すことを「クリック」、すばやく2回押すことを「ダブルクリック」、マウスの右ボタンを1度押すことを「右クリック」と表記しています。

ダイアログなどのチェックボックス、及びラジオボタンをクリックし、 \square \square の状態にすることを「チェックする」「チェックボックスをオン/オフにする」と表記しています。

Windows XPにおける「通知領域」のことを本書では「システムトレイ」と表記しています。



- 本書は、本書作成時のソフト及びハードウェアの情報に基づき作成されています。その後のソフトウェアのバージョンアップ等により、記載内容とソフトに搭載されている機能が異なっている場合があります。また、本書の内容は、将来予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複写、複製、改変することはその形態を問わず、禁じます。
- Microsoft、Windows、Windows Vistaは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。NOD32はスロバキア共和国ESET s.r.o.の登録商標です。本プログラムの著作権は、ESET s.r.o.に帰属します。本プログラムの著作権は、Esetに帰属します。本ユーザーズガイドの著作権は、キャノンシステムソリューションズ株式会社に帰属します。その他の製品名および社名などは、各社の商標または登録商標です。

CONTENTS

| | | |
|------------------|--|-----------|
| Preface | 導入の前に | 1 |
| | ソフトウェアライセンス契約書 ----- | 2 |
| | 本書の表記について / お断り ----- | 3 |
| | NOD32の主な機能と動作環境 ----- | 6 |
| | 主な機能 | 6 |
| | 動作環境 | 7 |
| | ウイルスに関する基礎知識 ----- | 8 |
| | ウイルスとは | 8 |
| | ウイルスに侵入されるとコンピュータはどうなるか | 8 |
| | ウイルスに感染しないためには | 9 |
| | 用語解説 ----- | 10 |
| | パソコン関連 | 10 |
| | インターネット関連一般 | 11 |
| | NOD32に固有の用語(ウイルス対策ソフト全般) | 12 |
| | 悪意を持つプログラム(マルウェア)の種類 | 13 |
| Chapter 1 | NOD32の導入 | 15 |
| | NOD32のユーザー登録について ----- | 16 |
| | ユーザー登録手続きの手順 | 16 |
| | NOD32をインストールする ----- | 19 |
| | NOD32をアンインストールする ----- | 23 |
| | スタートメニューからアンインストールを行なう | 23 |
| | コントロールパネルからアンインストールを行なう | 24 |
| Chapter 2 | NOD32の仕様と基本操作 | 25 |
| | NOD32がウイルスをシャットアウトする仕組み ----- | 26 |
| | NOD32コントロールセンターとNOD32オンデマンドスキャナの詳細 ----- | 27 |
| | コントロールセンターについて | 27 |
| | コントロールセンターの表示方法 | 28 |
| | コントロールセンターを自由に扱うには | 29 |
| | オンデマンドスキャナの起動方法 | 30 |
| | NOD32の更新を手動で行なう ----- | 31 |
| | Step 1 更新画面を表示する | 31 |
| | Step 2 更新を開始する | 31 |
| | 手動でウイルスを検査・駆除する NOD32 オンデマンドスキャナを利用する ----- | 32 |
| | Step 1 コントロールセンターを表示する | 32 |
| | Step 2 オンデマンドスキャナを起動する | 32 |
| | Step 3 ウイルス検査を行なう | 33 |
| | Step 4 駆除を行なう(ウイルス検出の際の対処法) | 34 |
| | 警告ウィンドウの見方と対処方法について ----- | 35 |
| | 警告ウィンドウその | 35 |
| | 警告ウィンドウその | 36 |
| Chapter 3 | NOD32の機能詳細 | 39 |
| | ファイル操作時にウイルスを検査・駆除する AMON (Access MONitor) を設定する ----- | 40 |
| | Step 1 AMONの操作画面を表示する | 40 |
| | Step 2 AMONの検査対象や検査のタイミングなどを設定する | 41 |
| | Step 3 AMONのウイルス検査の方法を設定する | 43 |

| | |
|---|-----|
| Step 4 AMONのアクション(ウイルス発見時の対処方法)を設定する | 44 |
| Microsoft Office 文書のチェックを行なう DMON(Document MONitor)を設定する ----- | 48 |
| Step 1 DMONの操作画面を表示する | 48 |
| Step 2 DMONの設定を行なう | 49 |
| Microsoft Exchangeメールのウイルスを検査・駆除する EMON (E-mail MONitor)を設定する ----- | 53 |
| Step 1 操作画面の表示について | 53 |
| Step 2 EMONの設定を行なう | 54 |
| 電子メール、Webの検査を行なう IMON (Internet MONitor)を設定する ----- | 61 |
| Step 1 IMONの操作画面を表示する | 61 |
| Step 2 IMONの設定を行なう | 62 |
| 検査するディスクやフォルダ・ファイルを設定する NOD32 オンデマンドスキャナ ----- | 70 |
| アンチウイルスの設定 | 70 |
| 検査ログで詳細を知る NOD32 オンデマンドスキャナ ----- | 73 |
| 検査ログの見方 | 73 |
| ウイルス検出時の処置を設定する NOD32 オンデマンドスキャナ ----- | 74 |
| アクション設定の詳細 | 74 |
| 検査時の設定 NOD32 オンデマンドスキャナ ----- | 76 |
| 検査時のさまざまな設定の詳細 | 76 |
| プロファイルで“設定”を保存する NOD32 オンデマンドスキャナ ----- | 80 |
| 設定の保存と読み出し | 80 |
| 自動更新機能の詳細と設定 NOD32 コントロールセンター ----- | 82 |
| 更新とは？ | 82 |
| Step 1 [設定]ボタンをクリックする | 83 |
| Step 2 プロファイルを選択する | 83 |
| Step 3 サーバを設定する | 84 |
| Step 4 更新の種類を設定する | 85 |
| Step 5 自動更新の設定を行なう | 86 |
| Step 6 ネットワークに関する設定を行なう | 90 |
| ログの詳細と設定 NOD32 コントロールセンター ----- | 91 |
| ログの表示方法と項目 | 91 |
| Column 「ログ」の便利な利用方法 ----- | 94 |
| 「システムツール」の詳細 NOD32 コントロールセンター ----- | 96 |
| 隔離情報について | 96 |
| スケジュールについて | 98 |
| システム情報について | 99 |
| システム設定について ----- | 100 |
| システム設定の表示方法と項目 | 100 |
| 一般 | 101 |
| 通知 | 103 |
| ログの保守 | 105 |
| 詳細 | 106 |
| リモートコントロール | 107 |
| ライセンスキー | 107 |
| ThreatSense.Net | 108 |

Chapter 4 よくある質問 111

Chapter 5 サポートについて 119

| | |
|----------------|-----|
| サポートについて ----- | 120 |
|----------------|-----|

NOD32の主な機能と動作環境

NOD32は高いウイルス検出・駆除能力を持ち、高速な検査を可能としたウイルス対策ソフトです。パソコンへの負荷も極力軽減していますので、軽快に利用することができます。

ここでは、その主な特長と動作環境を解説します。

≡≡≡ 主な機能

業界最高水準の検出率

NOD32は従来のウイルス定義ファイルによるウイルス検出はもちろん、独自技術である「ヒューリスティック手法」によるウイルス検出を可能としました。

これは、問題のあるファイル内のプログラムコードを解析し、その挙動を分析、さらにNOD32の仮想マシン内でプログラムを動作・監視し、ウイルス検出を行なうというもので、ウイルス定義ファイルに依存しない画期的なウイルス検出法です。このヒューリスティック手法を利用すれば、新種のウイルスに対しても高い検出率を実現できます。NOD32の作成する仮想マシンはディスプレイやフロッピーディスクといったデバイスもシミュレートできるので、非常に精度の高いものとなっています。

アンチステルス技術を搭載

新種のウイルスを検出するThreatSense（スレットセンス）テクノロジーの強化を図り、アンチステルス技術を搭載すること（1）によって、ルートキットの検出/駆除が強化されました。これまでルートキットは、侵入したことを隠蔽する（侵入痕跡を消す）という特性から、検出/駆除には専門の対策ツールが必要とされてきましたが、「NOD32 アンチウイルス V2.7」は、高度なルートキット対策を実現し、ユーザーに高いレベルの保護を提供します。

1 Microsoft Windows 98 / 98SE / Meは除く

軽快なモジュール

NOD32は最高の検出率を誇りながらも、そのシステムリソースの使用率は低く抑えられています。したがって、システム内のウイルス検査もいたって軽快です。

常駐保護

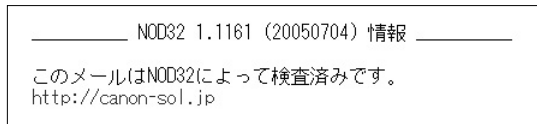
NOD32の常駐モジュールである「AMON（アクセスモニター）」は、バックグラウンドで常駐・動作し、常にコンピュータを監視、ウイルスの脅威から大切なシステムを守ります。

自動アップデート

NOD32はインターネット経由でエンジンおよび、ウイルス定義ファイルを自動更新します。したがって常に最新のウイルス情報をもとにしたウイルスの検出・駆除を行なうことができます。また更新スケジュールも設定可能です。

メール検査

NOD32は、受信するメールのウイルス検査も確実に行ないます。Outlook ExpressをはじめとするPOP3に対応した多数のメールソフトにおいて、受信したメールメッセージの中に、ウイルス検査の結果を挿入することが可能です。NOD32で安心してメールをプレビューすることができます。



結果を挿入することが可能です。NOD32で安心してメールをプレビューすることができます。

受信例

スケーラビリティ

プロキシサーバ経由のネットワークや、ダイヤルアップによるインターネット接続でも、NOD32であれば問題ありません。

動作環境

[32ビット環境]

対応OS

日本語 Microsoft Windows 98 / 98SE / Me /
NT Workstation 4.0 (Service Pack6以降)
2000 Professional / XP Home Edition /
XP Professional / 2000 Server /
2000 Advanced Server /
Server 2003, Standard Edition /
Server 2003 R2, Standard Edition /
Vista Ultimate / Vista Enterprise / Vista Business /
Vista Home Premium / Vista Home Basic

CPU/メモリ

次のOSごとに必要なIntel Pentium及び互換プロセッサを搭載したPC/AT互換機、またはNEC PC98-NXシリーズのコンピュータ (その他のNEC PC98シリーズはサポートしません)

| OS | CPU | メモリ |
|-----------------|----------|---------|
| Windows 98/98SE | 133MHz以上 | 32MB以上 |
| Windows Me | 150MHz以上 | 32MB以上 |
| Windows NT 4.0 | 133MHz以上 | 32MB以上 |
| Windows 2000 | 133MHz以上 | 64MB以上 |
| Windows XP | 300MHz以上 | 128MB以上 |

[64ビット環境]

対応OS

日本語 Microsoft Windows XP Professional x64 Edition /
Server 2003, Standard x64 Edition /
Server 2003 R2, Standard x64 Edition /
Vista Ultimate / Vista Enterprise / Vista Business /
Vista Home Premium

CPU/メモリ

Intel 64アーキテクチャー (旧称EM64) もしくはAMD64に対応した製品
Intel Itaniumベースのコンピュータではご使用いただけません。

| OS | CPU | メモリ |
|------------|----------|---------|
| Windows XP | 300MHz以上 | 128MB以上 |

[共通]

HDD

50MB以上の空き容量

グラフィックカード

VGA以上

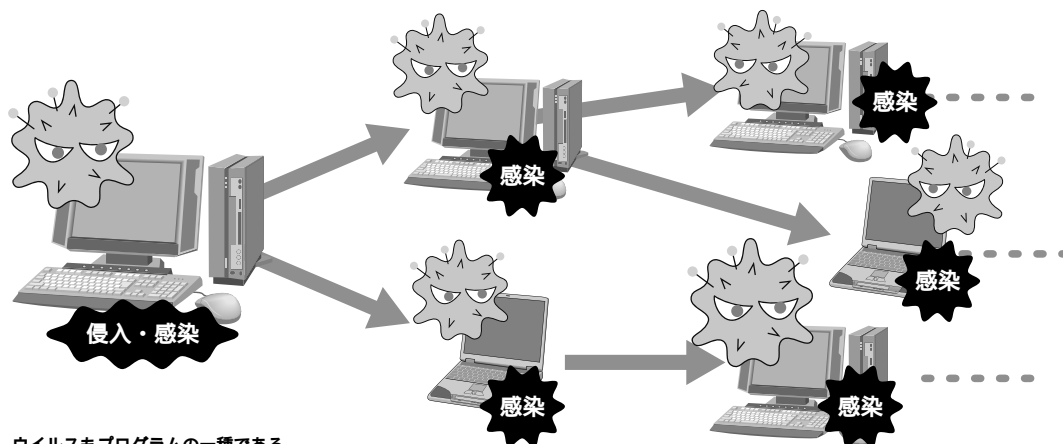
その他の必要条件

インターネット接続環境必須、Internet Explorer 5.5 (Service Pack 2以降)、メールアドレスと電子メールを送受信できる環境も必要となります。

ウイルスに関する基礎知識

ウイルスとは

ウイルスとは、正式にはコンピュータ・ウイルスと呼ばれ、悪意を持って作られたプログラムのことを指します。コンピュータに害を及ぼすことが目的で、しかも風邪のように感染し拡大していくことから、私たちにとって身近な風邪（ウイルス）に見立てて、コンピュータ・ウイルス（以下、ウイルスとします）と呼ばれているのです。主にメールの受信時、インターネットの閲覧時、ファイル交換時に侵入します。



ウイルスもプログラム的一种である

ウイルスに侵入されるとコンピュータはどうか

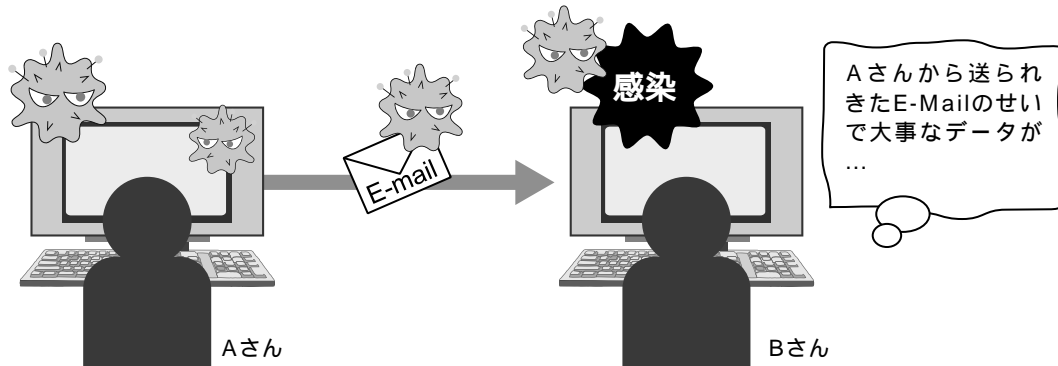
ウイルスに侵入されたコンピュータの症状はさまざまです。感染だけして、何も症状が出ないウイルスもありますが、大抵のウイルスは何かしら症状があります。

ウイルスに感染した際の主な症状

- ・コンピュータ（またはプログラム）の実行速度が著しく遅くなる。
- ・特定アプリケーションの実行時エラーが発生する。
- ・コンピュータが理由なく頻繁にダウンする。
- ・パスワードなどの情報を収集し、外部に送信する。
- ・奇異なエラーメッセージや画像が表示されたり、音がする。
- ・コンピュータに仕掛けをし、データを盗み取ったり、外部からの自由なコントロールを可能にする。

感染例

感染したウイルス(ワーム)が、コンピュータ内に保存されているメールアドレス宛に、自分自身を添付ファイルとして送信することで、さらに感染を広げます。



ウイルスが感染すると貴方の信用が失われる

この場合、BさんはAさんがウイルスをばらまいていると誤ってしまいます。本当は、ウイルスに感染しているAさんも被害者なのですが、加害者だと勘違いされてしまいます。このようにウイルスに感染したパソコンだけではなく、そこから感染が拡大し、人物の信用も落とすことになってしまいます。

ウイルスに感染しないためには

本製品 (NOD32 アンチウイルス) を使用し、最新バージョンへの更新をすることでウイルスの脅威からご使用のコンピュータを守ることができます。しかし、十分に予防するには以下の点にも注意をしてください。

出所の怪しいソフトウェアは絶対に実行しない

ソフトウェアのプログラムなどの中にウイルスが存在している場合があります。

知り合いから送信されたメールに添付されたプログラム (.exe など) でも、不用意に実行しない

上記の感染例で書いてるような場合もありますので、ご注意ください。

使用している Web ブラウザ (例: Internet Explorer) やメールソフト (例: Outlook Express) は、常に最新バージョンに保つ

ウイルスは Web ブラウザやメールソフトのセキュリティホールを狙って襲撃する確率が高いため、日ごろのアップデートは重要です。

用語解説

ここでは、本書に登場する基本的な用語を解説しています。

パソコン関連

| | |
|--|--|
| API (Application Program Interface) | Windows上のプログラムが、Windowsの機能を簡単に使用できるようにする仕組みです。 |
| OS | コンピュータの基本的な部分を操作するための基礎プログラム。ワープロや表計算ソフトなどの一般的なプログラムはOS上で動作します。WindowsはOSの1つです。 |
| 圧縮された実行形式 | ファイルサイズを節約するために圧縮された状態でありながら、起動されると自分自身を解凍して動作する実行ファイルです。通常は圧縮された状態なので、ウイルスパターンで検出するのが難しくなります。 |
| 拡張子 | ファイル名の「.(ドット)」以下を拡張子といいます。Windowsでは、この拡張子を判別してファイルの種類を判断します。このことを関連づけといいます。コンピュータのファイルは大きく分けて実行形式(プログラム)と非実行形式(データ)がありますが、ウイルスによっては、自分自身を非実行形式の拡張子に見せかけるものがあります。 <ul style="list-style-type: none"> ・ AABBC.C.DAT (DATが拡張子) ・ readme.exe (exeが拡張子) |
| コンテキストメニュー | Windowsにおいては、ファイルやフォルダを選択してマウスを右クリックすることで表示されるメニューのことを指します。 |
| システムリソース | 各種メモリやオーディオ装置、記憶装置など、コンピュータ上におけるいろいろな資産のことです。また狭義では、Windowsの管理上設けられている特殊なメモリ領域を指します。プログラムが起動すると、システムリソースを消費しつつ動作することになります。システムリソースは有限であるため、たくさんのプログラムを同時に動作させるとシステムリソースが足りなくなることがあります。 |
| 実行ファイル | コンピュータが実行することのできるプログラムファイルのことです。 |
| 常駐(プログラム) | 起動されたプログラムがメモリ上にとどまり、他のプログラムと同時に動作する状態を「常駐」といいます。一般的に常駐するタイプのプログラムは、操作ウィンドウを持ちません。またタスクバーなどに、小さくアイコン表示されることが多くあります。 |
| ブートセクタ | ブートセクタとは、HDD / FD / CD-ROMにあるコンピュータを起動するためのプログラムが書き込まれた領域です。コンピュータがブートする |

際、まずこのブートセクタのプログラムが起動しその後、WindowsなどのOSに制御が移ります。

| | |
|------|--|
| メモリ | コンピュータがデータを記憶するための場所で、プログラム自体もメモリに読み込まれ、実行されます。HDDなどより遙かに高速な読み書きが可能です。ほとんどのウイルスはファイルを介してコンピュータに感染しますが、そのときメモリに常駐することもあります。 |
| リブート | コンピュータを再起動させることです。 |

インターネット関連一般

| | |
|-------------------------|---|
| MAPI (Messaging API) | マイクロソフトが提唱する、メールに関するAPIのことです。OutlookやOutlook Expressは、このMAPIを利用しています。 |
| POP3 | POP3はメールを受信する手続き（プロトコル）の一種です。POP3を監視することにより、メールに添付されたウイルスの発見がし易くなります。またメールの送信手続き（プロトコル）は、SMTPと呼びます。 |
| アーカイブ (アーカイブ・ファイル) | 複数のファイルを1つのファイルにまとめて管理することです。多くは、ファイルサイズを節約するために圧縮されたデータファイルです。実行形式でなく、圧縮されているのでこのままではウイルスは活動できませんが、ウイルスのパターン検出は難しくなります。解凍されると、通常のファイルに復元されるのでウイルスも活動可能となります。 |
| ウイルス | 悪意を持って作られたプログラムをウイルスと呼びます。ウイルスの特徴としては、メールやファイル交換によって、他のコンピュータへと感染を広げていくことがあります。 |
| サーバ | 各種のサービスを提供するコンピュータのことです。Web サービスを提供するコンピュータをWebサーバ、メールサービスを提供するサーバをメールサーバなどと呼びます。 |
| セキュリティホール | ソフトウェアにおけるバグ（欠陥）の一種です。特にネットワーク系のソフトウェアにおいて、バグを内包しているプログラム以外にも広く被害を与えるようなプログラムの欠陥をセキュリティホールと呼びます。 |
| ダイヤルアップ（接続） | ダイヤルアップモデムを使って、電話回線を介してインターネットに接続することです。 |
| 添付ファイル | メールメッセージに付いてくるファイル。近年のウイルスは自分自身を添付ファイルとして送信し、感染を拡大するケースが増えています。メールに添付されたファイルを、安易にクリックすることは非常に危険なので、注意してください。 |
| バックドア | コンピュータに感染したウイルスは、侵入者のための入り口を設けることがあります。これが「バックドア（裏口）」です。バックドアは「トロ |

イの木馬」とも呼ばれています。通常パスワードなどで守られているコンピュータですが、バックドアを使えば簡単にコンピュータに進入することができますようになります。

| | |
|-----------|---|
| プロキシ | 英語で"proxy"。「代理」という意味があります。 |
| プロキシサーバ | プロキシサーバは代理サーバとも呼ばれます。プロキシサーバはLANとインターネットの間に設置され、LANからインターネットへの接続を代行します。トラフィックを制御することで安全性の確保やその他の負荷価値を持ちます。 |
| ポート | ネットワークにおいてデータを交換するとき使用するコンピュータ上の窓口のことです。インターネット上のデータを監視する際には、どのポートを使用するかを定めなければなりません。メールやWebなど、広く普及したサービスにはそのサービスで使用するポートが決められています。 |
| メッセージサービス | Windowsには、LAN内において簡易的にメッセージを交換する手段があり、それをメッセージサービスと呼びます。NOD32の機能で「メッセージサービス」がありますが、これはあくまでも“自動的に通知するサービス”のことであり、MSNメッセージなどのことではありません。インターネットを使ったチャット的なメッセージサービスとは異なるものです。 |

NOD32に固有の用語(ウイルス対策ソフト全般)

| | |
|-----|--|
| 隔離 | NOD32において隔離とは、後にウイルスを解析・研究するために特定のフォルダ(設定可能)にウイルスを保存する処理です。NOD32はウイルスを検出すると駆除や削除を行いますが、隔離の設定を有効にすることで駆除や削除を行なうと同時に、そのウイルスを隔離します。なお、隔離されたウイルスはNOD32が無力化処理を施しますので、心配は不要です。 |
| 既定値 | あらかじめ設定されている値のこと。NOD32では、標準でインストールされた値ということになります。各設定を施すことによって、よりきめ細かい動作を指定することができますが、的確にウイルスを検出・駆除する設定はすでになされています。設定内容がよくわからないときは既定値のままお使いください。 |
| 駆除 | 各ウイルス対策ソフトによって「駆除」の定義は微妙に違いますが、ここではウイルスに感染したファイルからウイルスを取り除き、正常なファイルに戻すことを「駆除」と表現しています。しかし全てのウイルスを駆除することは不可能です。マクロウイルスなどであれば比較的、駆除の成功率が高くなります。しかしファイルそのものがウイルスだったり、実行ファイルがウイルスに感染していたりすると駆除することができず、削除する必要性が生じます。 |

| | |
|-------------|---|
| 更新 | 新種のウイルスや既存ウイルスを改造したものなど、ウイルスは刻々と変化します。したがってウイルスの検出法もその都度、最新の情報によって行なわなければなりません。このウイルスの変化・発達に対して、NOD32も変化・対応する必要があります。ウイルス定義ファイルを最新の状態に保ったり、NOD32のプログラムコンポーネントをバージョンアップすることを「更新」といいます。NOD32はプログラムコンポーネントやウイルス定義ファイルをインターネット経由で自動更新することが可能です。 |
| 削除 | 各ウイルス対策ソフトによって「削除」の定義は微妙に違いますが、ここではウイルスに感染したファイルを消去することを「削除」と表現しています。駆除できないウイルスは、削除する必要があります。 |
| ウイルス定義ファイル | ウイルスに感染したファイルや、ワーム(下記参照)などの特徴を収録したファイルのことです。ウイルスのデータベースで、「パターンファイル」と呼ばれることもあります。 |
| シグネチャ | ここでいうシグネチャとは、各ウイルスを判別するための特徴です。NOD32の持つウイルス定義ファイルには、今まで発見されたウイルスのシグネチャ(特徴)が記録されており、その情報からウイルスの検出を行ないます。 |
| ヒューリスティック | ウイルス定義ファイルとウイルスのパターンを比較する従来の検出方法では、解析の終わった既知のウイルスしか発見することができません。ヒューリスティックは、ウイルスらしきコードを実際に仮想コンピュータの中で動作させ、その挙動を観察することによってウイルスを検出します。このヒューリスティックにより、新種のウイルスを検出することが可能になります。 |
| ログ(ログ・ファイル) | さまざまな過程を詳細に記録したファイルのことです。NOD32ではウイルス検査を行った日時や検査したファイル名など、きめ細かいログを記録・保持・表示します。 |

悪意を持つプログラム(マルウェア)の種類

| | |
|---------|--|
| マルウェア | ウイルスやワームをはじめ、スパイウェアやリスクウェアなど、ユーザーの意図しない動作によって、ユーザーに迷惑を掛けるプログラム全般を指す用語です。日本語では「悪意のあるソフトウェア」と訳されます。 |
| マクロウイルス | ExcelやWordなど、広く普及したプログラムの中で動作するマクロ(スクリプト)言語で記述されたウイルスです。データファイルと見分けが付かないことが多いです。 |
| ワーム | インターネットを使って、独自に感染を繰り返すプログラムです。ウイルスがメールやWebアクセスなど、人のオペレーションを介して感染を広げるのに対し、ワームは独自にコンピュータを探してセキュリティーホールから感染を繰り返します。 |

| | |
|----------|--|
| トロイ(の木馬) | 悪意を持ったプログラムの一種です。ユーザーが興味をひくプログラムや画像、音楽を装ってダウンロードさせ、実行すると同時に悪意的なプログラムが動作し、ユーザーの意図しない動作を行ないます。ウイルスとは異なり、他のファイルへの寄生や、自分自身の増殖活動は行ないません。プログラムや画像は正常に動作する(開く)ように見えるため、ユーザーが検知しにくいのが特徴です。 |
| ルートキット | 自らの存在を隠蔽し、アンチウイルスソフトウェアによる検出を免れようとする特殊なタイプのマルウェアです。攻撃者の狙いは、ルートキットを利用してシステムのアクセス権を乗っ取ることにあります。 |
| スパイウェア | ユーザーが気づかぬうちに個人情報のデータを収集し、インターネット上の特定のサーバーなどに送信を行なうプログラムのことです。データとしてはメールアドレスや閲覧したホームページの履歴などが多く、収集した個人情報は主に広告の配信などに使われます。 |
| アドウェア | 広告を表示する仕掛けがなされたプログラムのことです。仕組み的には、トロイの木馬の一種です。Webブラウザのスタートページを勝手に書き換え、広告表示のページに変更したり、特定のWebサイトアクセス時に、勝手に別ウィンドウで広告を表示するものなどがあります。 |
| リスクウェア | ユーザーが意図しない形で、危険な働きをするソフトウェアのことです。ウイルスとは異なり繁殖活動は行ないませんが、Windowsの脆弱性をつき、また、他のソフトの脆弱性を利用してユーザーの操作を受け付けられない状態にしたり、ファイルを削除してWindowsの動作を阻害するなどの動作を行ないます。 |
| ボット | コンピューターを外部から操作することを目的として作られたプログラムのことです。ボットがコンピューターに侵入すると、外部からの操作によって、「スパムメールの大量送信」「特定サイトの攻撃・不正アクセス」「パソコン内の情報を外部に送信」などが行なわれます。感染しても特別な症状が現れないことが多いため、被害者になるばかりではなく、加害者にもなってしまいます。 |

Chapter 1

NOD32の導入

ここでは、NOD32をお使いいただくために必要なユーザー登録方法と、インストールおよびアンインストール方法について解説しています。

Chapter 1
NOD32の
導入

NOD32 のユーザー登録について

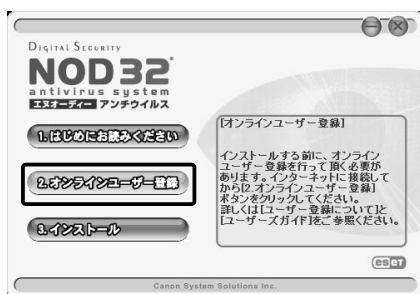
導入前に必ずお読みください

NOD32をご利用いただくには、予めインターネット経由でユーザー登録を行ない、NOD32を更新するための「ユーザ名」と「パスワード」を取得していただく必要がございます。

以下の手続き手順をご参照いただき、ユーザー登録を行なってください。

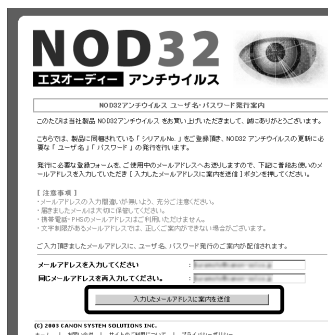
ユーザー登録手続きの手順

Step 1



NOD32のインストールCDをCD-ROMドライブに挿入してください。ランチャーが起動します。[オンラインユーザー登録]をクリックします。

Step 2



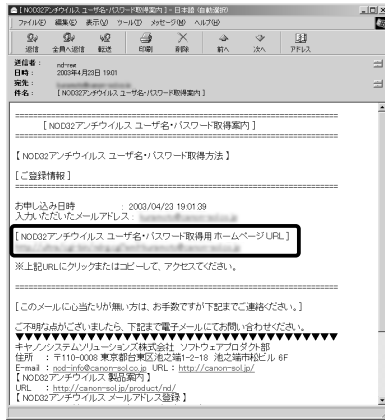
ユーザー登録のページが開きますので、メールアドレスを入力した後、[入力したメールアドレスに案内を送信]をクリックします。

Step 3



メール送信の確認画面が表示されますので、確認してください。

Step 4



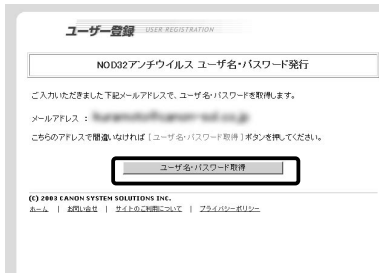
メールを受信いただいたら、[NOD32アンチウイルス ユーザー名・パスワード取得用ホームページURL] をクリック、あるいはURLをコピーしてブラウザで表示します。



URLを示す文字列中に改行が入っている場合は、URL文字列をコピーしてください。

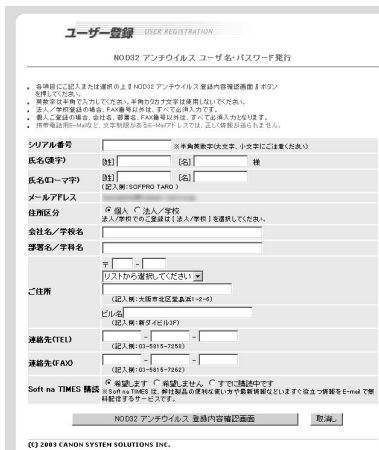
Chapter 1
NOD32の
導入

Step 5



ユーザー登録のページが表示されますので、間違っていなければ[ユーザー名・パスワード取得]をクリックします。

Step 6



ユーザー情報の入力ページが表示されます。必要事項を記入し、画面下部にある[NOD32 アンチウイルス 登録内容確認画面]ボタンをクリックします。



シリアル番号は、「ユーザー登録について」に記載されていますので、そちらをご覧ください。また、個人で登録される場合、会社名、部署名、FAX番号以外は、すべて入力が必要となります。

Step 7

ユーザー登録 USER REGISTRATION

「NOD32 アンチウイルス ユーザー名・パスワード発行」確認画面

| | |
|----------|--|
| シリアル番号 | |
| 会社名/学校名 | |
| 部署名/学科名 | |
| 住所 | |
| 氏名(漢字) | |
| 氏名(ローマ字) | |
| 連絡先(TEL) | |
| 連絡先(FAX) | |
| E-mail | |

赤字で表示されているメールアドレスの、最終確認をお願いします。

記入事項をもう一度ご確認の上、次の「登録する」ボタンを押してください。
修正する場合は、ブラウザの「戻る」ボタンを押してください。

(C) 2003 CANON SYSTEM SOLUTIONS INC.
ホーム | お問い合わせ | サイトの仕組みについて | プライバシーポリシー

ユーザー登録の確認画面が表示されます。内容を確認し、問題がなければ[登録する]ボタンをクリックします。



point

修正する場合はブラウザの[戻る]ボタンをクリックし、内容を修正してください。

Step 8

ユーザー登録 USER REGISTRATION

「NOD32 アンチウイルス ユーザー名・パスワード発行」が完了しました。

NOD32 アンチウイルス ユーザー名・パスワード発行が完了しました。
数分後に、登録しましたメールアドレスに、ユーザー名とパスワードが自動送信されます。

【メールが届いたお客様】
メールに送附されているユーザー名とパスワードを NOD32 アンチウイルス に入力してください。
NOD32 アンチウイルスの「更新」メニューより最新プログラムのダウンロードください。

【メールが未着のお客様】
ご入力されたメールアドレス に登録済みかどうかご確認ください。

ご入力されたメールアドレスの間違い、もしくは重複登録が考えられます。
大変申し訳ございませんが、この段階から再登録はできませんので、お手数ですが
サポートセンターまでご連絡をお願いします。サポートセンターの連絡先は、お手持のマニュアル
もしくは下記お問い合わせをご覧ください。

(C) 2003 CANON SYSTEM SOLUTIONS INC.
ホーム | お問い合わせ | サイトの仕組みについて | プライバシーポリシー

ユーザー登録の完了画面が表示されます。ご確認ください。何か問題が生じたときのためにプリントアウトをしておくことをお勧めします。

Step 9

数分後にユーザー名とパスワードが書かれたメールが、登録フォームに記入したメールアドレス宛に送信されてきます。

以上で、NOD32 アンチウイルスのユーザー登録は完了です。

NOD32をインストールする

NOD32のインストール(標準インストール)を開始します。

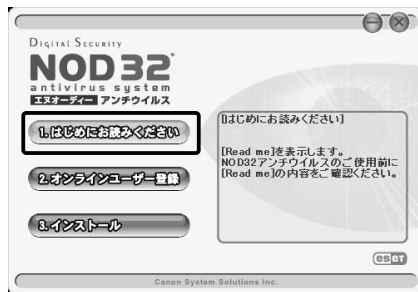


他のアンチウイルスソフトがインストールされている場合は、必ずこれらのソフトをアンインストールしてからNOD32をインストールしてください。他のアンチウイルスソフトが共存している環境で起こった不具合に関しましては、サポート対象外となります。

1

NOD32のインストールCD、「ユーザ名」、「パスワード」を用意し、使用中のプログラム等をすべて終了します。

2

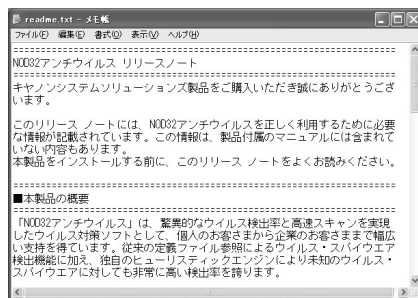


NOD32のインストールCDをCD-ROMドライブに挿入してください。ランチャーが起動します。[はじめにお読みください]をクリックします。



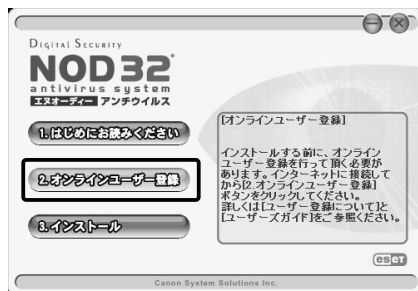
ランチャーが起動しない場合は、[マイコンピュータ]をダブルクリックし、NOD32のアイコンに変わっているCD-ROMドライブをダブルクリックします。

3



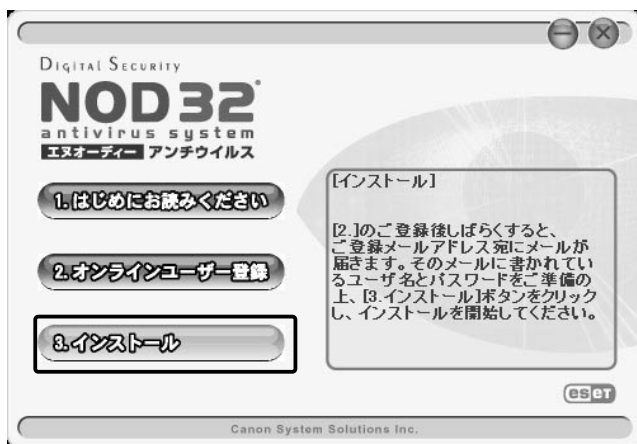
リリースノートをお読みください。ここでは、本製品の制限事項や動作環境などを説明しています。読み終わったら[閉じる]ボタンをクリックします。

4



まだオンラインユーザー登録を行っていない場合は、[オンラインユーザー登録]をクリックし、オンラインユーザー登録を行なっていただきます。登録方法の詳細については、16～18ページを参照してください。すでに登録が終了している方はこの作業は必要ありません。

5

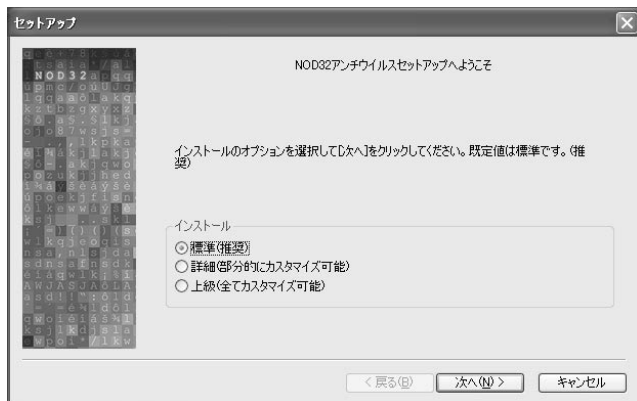


[インストール]をクリックします。



インストールはユーザ名とパスワードを取得してから開始してください。

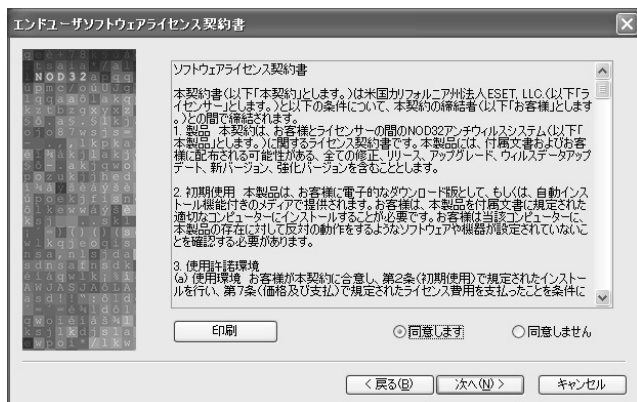
6



NOD32のセットアップ・プログラムのウィザード画面が起動します。「標準(推奨)」が指定されていることを確認し、[次へ]ボタンをクリックします。

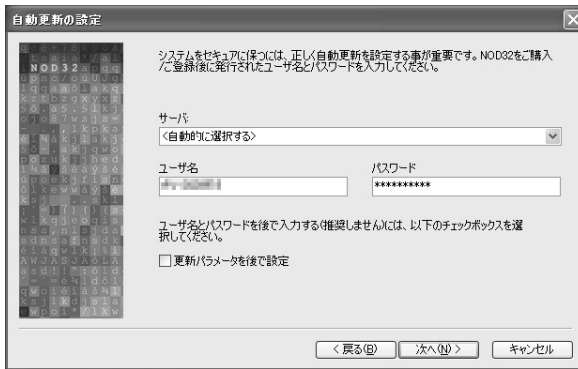
[キャンセル]ボタンをクリックした場合は、インストール作業は行われずにセットアップ・プログラムが終了します。

7



ソフトウェアライセンス契約書に同意いただける場合は[同意します]をクリックし、[次へ]ボタンをクリックします。

8



サーバ欄は、既定値の「<自動的に選択する>」の状態にします。

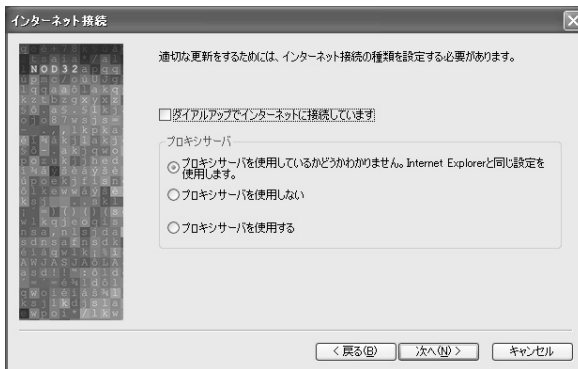
オンラインユーザー登録によって取得した「ユーザー名」と「パスワード」を入力し、[次へ]ボタンをクリックします。



caution

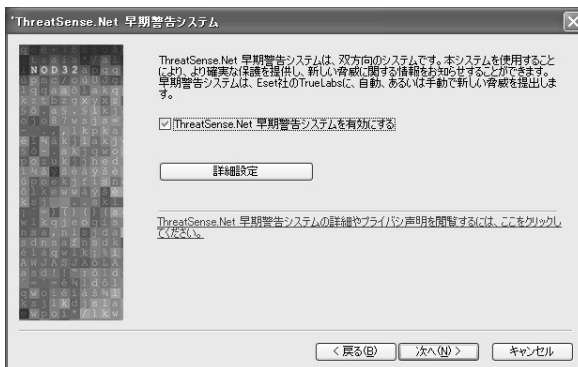
ユーザー名等を後から入力する場合には「更新パラメータを後で設定」のチェックボックスをオンにします。ただし推奨ではありませんので、このボックスにチェックを入れる際にはご注意ください。

9



ご使用のインターネット接続環境を指定し、[次へ]ボタンをクリックします。

10



Threatsense.Net 早期警告システムを設定し、[次へ]ボタンをクリックします。



point

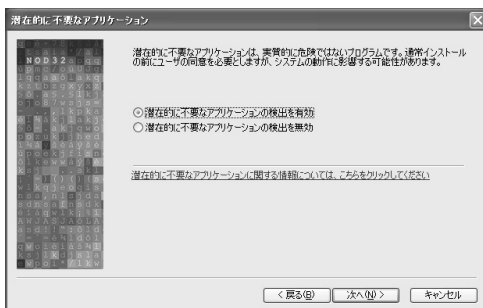
この機能を有効にすると、ウイルスが発見された場合にEset社に提出することができます。



caution

早期警告システムを利用したEset社へのファイル提出は、早期対応をお約束するものではありません。

11



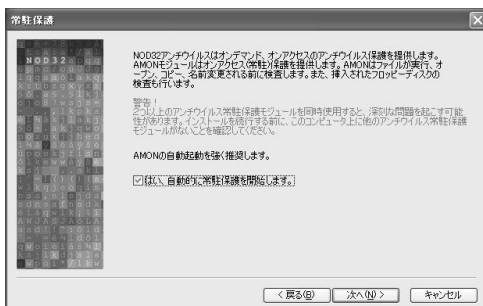
「潜在的に不要なアプリケーションの検出」を有効にするか無効にするかは任意です。どちらかをチェックし、[次へ]ボタンをクリックします。



point

「潜在的に不要なアプリケーション」はよくある質問(117ページ)にて解説していますのでご参照ください。

12



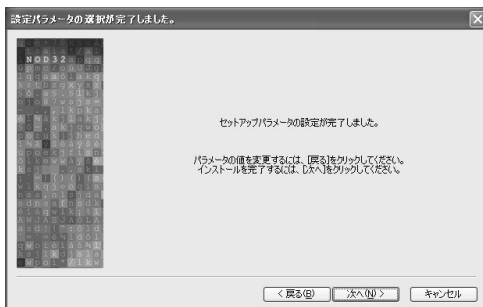
常駐保護機能の設定を行いません。通常は既定値のまま[次へ]ボタンをクリックします。



point

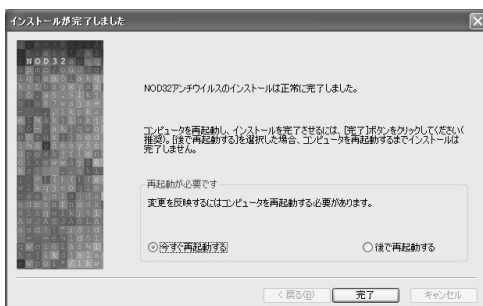
EMONの設定ダイアログが表示された場合は、53ページをご参照ください。

13



左の画面を確認したら、NOD32の最小限の設定の完了です。[次へ]ボタンをクリックしてください。

14



インストールは完了しました。「今すぐ再起動する」「後で再起動する」のいずれかをチェックして[完了]ボタンをクリックしてください。



caution

NOD32を正しくご利用いただくためには再起動が必要です。

NOD32 をアンインストールする

NOD32は以下の2種類の方法でアンインストールすることができます。

スタートメニューからアンインストールを行なう

1



スタートメニューから、[すべてのプログラム] [Eset] [アンインストール]をクリックします。

Windows XP/Vista以外のOSでは「プログラム」を選択します。

2



確認画面が表示されますので、[はい]をクリックしてください。アンインストールを中止する場合は、[いいえ]をクリックします。



caution

Windows Vistaの場合は、この画面表示の前に「ユーザー アカウント制御」画面が表示されます。[続行]をクリックしてください。

3

アンインストールを完全に実行するには、コンピュータを再起動する必要があります。アンインストールが終了すると確認の画面が表示されます。「今すぐ再起動する」のチェックをオンにして[完了]をクリックすると、コンピュータが再起動します。

「後で再起動する」のチェックをオンにして[完了]をクリックすると、コンピュータはそのまま、アンインストールが終了します。



caution

「後で再起動する」のチェックをオンにして[完了]をクリックした場合、アンインストール画面は終了しますが、NOD32は完全にアンインストールされていません。できるだけ早く、コンピュータを再起動するようにしてください。

コントロールパネルからアンインストールを行なう

1



スタートメニューから、[コントロールパネル]をクリックします。

2



[プログラムの追加と削除]をクリックします。



point

Windows Vista の場合は、[プログラムのアンインストール] (または [プログラムと機能]) になります。それ以外の OS では [アプリケーションの追加と削除] になります。

3



[NOD32 アンチウイルス] をマウスで選んで反転させ、[変更と削除] をクリックしてください。

4

この後は「スタートメニューからアンインストールを行なう」の手順②と同様です。



point

NOD32 のアンインストール手順は、XP 以外の Windows でも同様となります。

Chapter 2

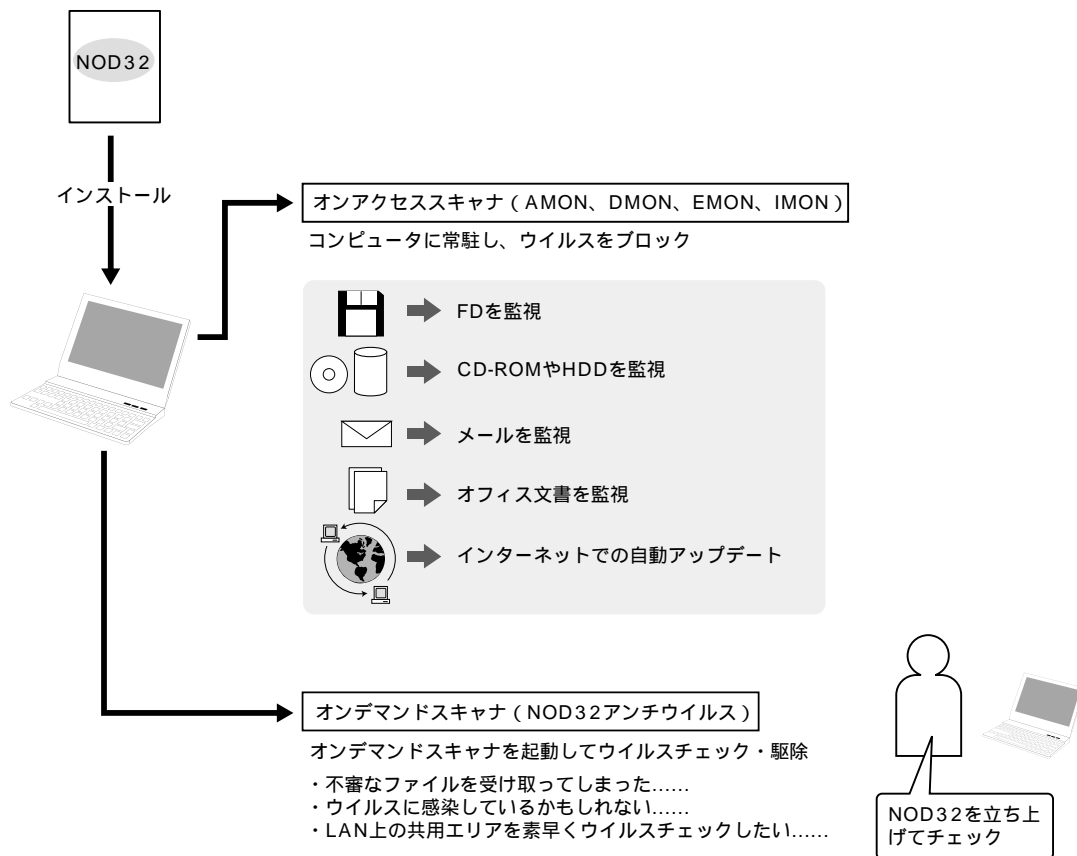
NOD32 の仕様と 基本操作

ここでは、NOD32の基本操作について解説しています。

Chapter 2
NOD32
の仕様と
基本操作

NOD32 がウイルスをシャットアウトする仕組み

NOD32をインストールすると、オンアクセススキャナ(AMON、DMON、EMON、IMON)がコンピュータに常駐し、ファイル操作やメールを常時監視します。また、ユーザのオペレーション等によってオンデマンドスキャナ(NOD32)が起動し、コンピュータ内のファイルに対してウイルス検査を行いません。



NOD32 コントロールセンターと NOD32 オンデマンドスキャナの詳細

☰ コントロールセンターについて

コントロールセンターは、以下のモジュールから構成されています。



| | |
|------------------------------|--|
| ① AMON (Access MONitor) | ファイルの操作時等に、ウイルス検査を行ないません。 |
| ② DMON (Document MONitor) | Microsoft Office (WordやExcelなど) 文書のウイルス検査を行ないません。 |
| ③ EMON (E-mail MONitor) | Microsoft Office OutlookのExchangeメール(Microsoft Exchangeをホストとするメール)のウイルス検査が行なえます(インターネットを経由するメールはIMONで検査されません)。 |
| ④ IMON (Internet MONitor) | メールなどインターネットからのデータを監視し、ウイルス検査を行ないません。 |
| ⑤ NOD32 | オンデマンドスキャナを起動します。 |
| ⑥ 更新 | NOD32の更新や、ウイルス定義ファイルを更新します。 |
| ⑦ ログ | 各種ログを参照します。 |
| ⑧ システムツール | システムの設定などを行ないません。 |

Chapter 2

NOD32
の仕様と
基本操作

☰ コントロールセンターの表示方法

コントロールセンターは、「プログラムメニュー」と「システムトレイ」から起動することができます。通常の方法でNOD32をインストールした場合、コントロールセンターはコンピュータに常駐しますので、ここでいう「起動」とは「コントロールセンターを呼び出す（表示する）」ということになります。

表示方法

表示手順その 「プログラムメニュー」を利用する



[スタート] [すべてのプログラム]
[Eset] [NOD32 コントロールセンター]を
クリックします。

Windows XP/Vista以外のOSでは「プ
ログラム」を選択します。

表示手順その 「システムトレイ」を利用する



デスクトップ右下のシステムトレイの中にあるNOD32のアイコンをク
リックします。



コントロールセンターを終了し、その後起動させた場合は、コントロールセンター画面は表示されず、システムトレイの中に格納されます。

☰ コントロールセンターを自由に扱うには

システムトレイに格納されているコントロールセンター画面は、**1** デスクトップに画面を表示させたり、**2** システムトレイへ退避させたり、また、**3** 終了させたりすることができます。

1 表示方法



2 システムトレイへの退避方法

2 の「隠す」ボタン(どちらでもよい)をクリックすると、システムトレイに格納されます。



3 終了方法

3 の「終了」ボタンをクリックすると、コントロールセンターを終了します。



caution

コントロールセンターを終了するとウイルス警告が表示されなくなり、適切な処置が選択できなくなりますので、ご注意ください。

オンデマンドスキャナの起動方法



オンデマンドスキャナはユーザーのオペレーションによってウイルス検査とウイルスの駆除・削除を行なうプログラムです。AMONを常駐させていればウイルスに感染することはありませんが、適切なタイミングでオンデマンドスキャナを実行することによって、より完璧なウイルス検査を行なうことができます。また出所不明なプログラムを実行してしまったなど、ウイルスに感染した可能性が否定できない場合にも、オンデマンドスキャナを実行してください。

オンデマンドスキャナの起動方法

起動手順その「プログラムメニュー」を利用する



オンデマンドスキャナを起動するには、[スタート] [すべてのプログラム] [Eset] [NOD32]をクリックします。

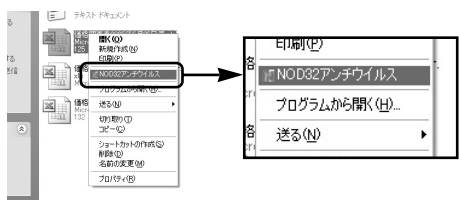
Windows XP/Vista以外のOSでは「プログラム」を選択します。



point

[オンデマンドスキャナ]は[コントロールセンター]からも起動することができます。起動方法は「NOD32」を選択し、「スキャナの起動」をクリックします。

起動手順その「マウス右クリック」を利用する



ファイルやフォルダを選んでマウスを右クリックすると、そのファイルをオンデマンドスキャナでチェックすることができます。

NOD32の更新を手動で行なう

NOD32は、新種のウイルスやワームなどに対処するため、ウイルス定義ファイルやプログラム本体を最新のバージョンに保つ「更新」機能を搭載しています。基本的に更新作業は自動で行なわれますが、自動更新が何らかの原因で行なわれなかった場合などでは、手動で更新を行なえます。

更新に関する詳細な設定については、82ページを参照してください。

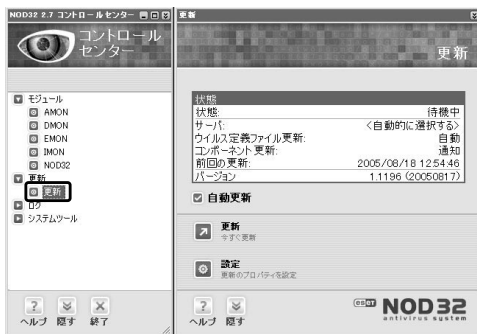


caution

更新を行なうには、ユーザー登録後に発行される「ユーザ名」と「パスワード」が必要です。ユーザー登録に関しては、16ページを参照してください。

Step 1

更新画面を表示する

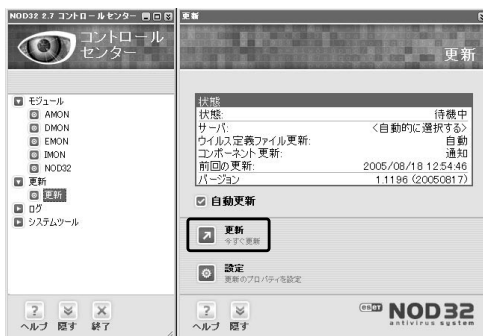


コントロールセンターを起動し、[更新]をクリックします。

コントロールセンターの表示方法は28ページをご覧ください。

Step 2

更新を開始する

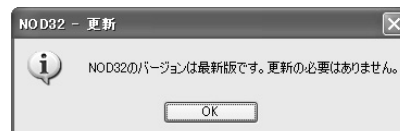


表示された更新画面より、[更新]をクリックします。更新画面の「状態」に通信状態や進行状況が表示された後、更新作業が自動的に終了します。



point

NOD32が最新の状態に保たれており、更新の必要がなかった場合は、次のダイアログ画面が表示されます。[OK]をクリックすると、更新画面に戻ります。



手動でウイルスを検査・駆除する

NOD32 オンデマンドスキャナを利用する

ここでは、手動によってウイルスの検査・駆除を行なう方法を紹介しています。

Step 1

コントロールセンターを表示する

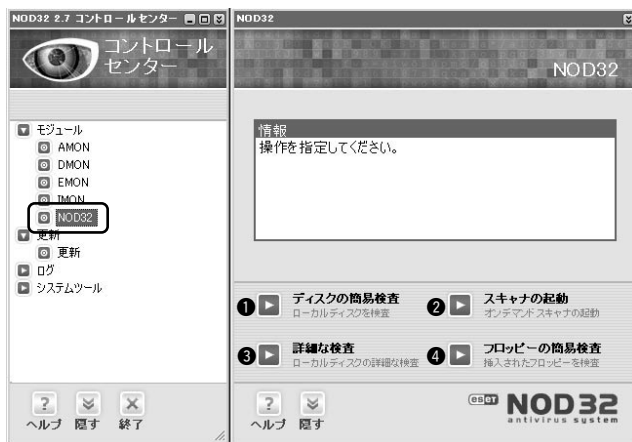
システムトレイに格納されたNOD32アイコンをクリックします。ここでは、一度コントロールセンターを表示してから、オンデマンドスキャナを起動します。

そのほかの起動方法については30ページを参照してください。

Step 2

オンデマンドスキャナを起動する

[モジュール] [NOD32]と選択し、右側にNOD32を表示します。①～④の各ボタンをクリックすることによって、オンデマンドスキャナを呼び出すことができます。メモリ上のウイルス検査を行なった後、指定したモードでオンデマンドスキャナが起動します。ここでは、[スキャナの起動]をクリックします。



| | |
|--------------|-----------------------------------|
| ① ディスクの簡易検査 | オンデマンドスキャナがローカルディスク簡易検査モードで起動します。 |
| ② スキャナの起動 | オンデマンドスキャナが通常モードで起動します。 |
| ③ 詳細な検査 | オンデマンドスキャナがローカルディスク詳細モードで起動します。 |
| ④ フロッピーの簡易検査 | オンデマンドスキャナがフロッピー簡易検査モードで起動します。 |



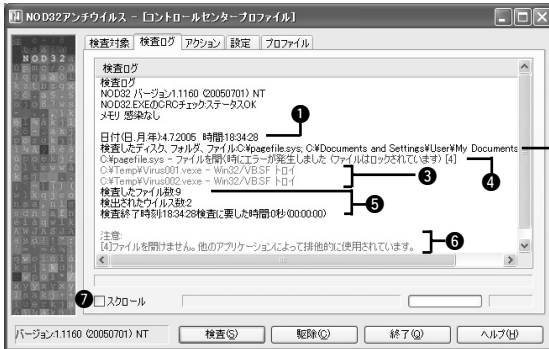
point

簡易検査モードとは、クリックした時点ですぐに検査が開始されることを示しています。ただし、既定値の設定で検査が行なわれますので、ご注意ください。

Step 3

ウイルス検査を行なう

検査ボタンをクリックするとウイルス検査が行なわれ、その経過及び結果が検査ログに表示されます。



- ① ウイルス検査を行なった日時です。
- ② ウイルス検査を行なう対象ドライブや、パス、ファイルが表示されます。
- ③ ウイルスが発見されると、ウイルスの情報が赤文字で表示されます。
- ④ ウイルス検査の時に発生したエラーなどが、青文字で表示されます。
- ⑤ ウイルス検査を行なったファイル数、検出ウイルス数、終了時間、所要時間が表示されます。
- ⑥ 注意などがあったら、表示されます。
- ⑦ 検査ログを自動的にスクロールします。



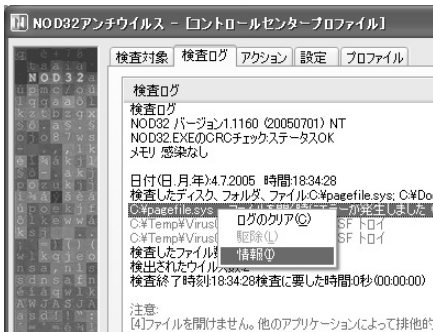
caution

[検査]では、ウイルス検査のみが行なわれ、ウイルスの駆除や削除は行なわれません。ウイルスの駆除や削除を行なう場合は、[駆除]をクリックします。また他のアプリケーションで使用されているファイルはウイルス検査ができないことがあります。ウイルス検査の際には、できるだけ他のソフトウェアを終了させてください。



point

検査ログの内容を右クリックすると、[ログのクリア]、[駆除]、[情報]などのメニューが表示されます。



| | |
|--------|---------------------------|
| ログのクリア | 検査ログをクリアします。 |
| 駆除 | ウイルスの場合は、ウイルスを駆除します。 |
| 情報 | クリックしたログの情報のみをウィンドウ表示します。 |

情報

C:\pagefile.sys - ファイルを開く時にエラーが発生しました (ファイルはロックされています) (4)

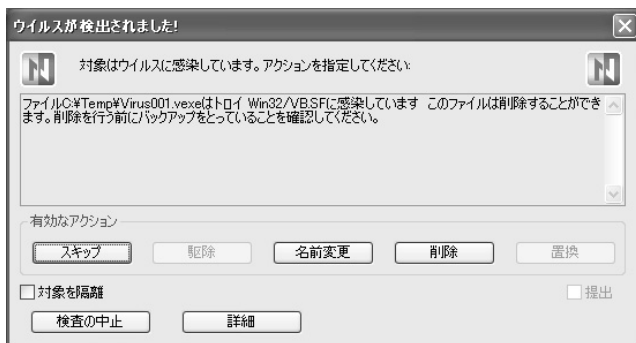
閉じる

Step 4

駆除を行なう(ウイルス検出の際の対処法)

[駆除]ボタンをクリックすると、ウイルス検査が行なわれ、ウイルスが発見された場合は、[アクション]タブで設定しているアクションが適用されます。

駆除できない場合



検出された感染ファイルがウイルス本体であった場合、駆除はできません。このような場合は[隔離]にチェックを入れて、[削除]を行なうと良いでしょう。

ファイルC:\Temp\Virus001.vexeはトロイ Win32/VB.SFに感染しています このファイルは削除することができません。削除を行う前にバックアップをとっていることを確認してください。

警告ウィンドウの見方と対処方法について

NOD32のウイルス検出時のアクションは、既定値では警告ウィンドウを表示し、ユーザに処理をうながすように設定されています。

警告ウィンドウが表示された場合は、通常は「駆除」か「削除」を選択して、コンピュータをウイルスの感染から防いでください。

| | |
|----------|--|
| 駆除 | ウイルスに感染したファイルからウイルスのみを取り除き、正常なファイルに戻します。 |
| 名前変更 | ウイルスに感染したファイルの名前（拡張子）を非実行ファイル形式に変更して、無力化します。 |
| 削除 | ウイルスに感染したファイルを削除します。 |
| (対象を) 隔離 | ウイルスに感染したファイルを安全な形式に変換し、隔離フォルダにコピーします。 |
| 提出 | 検出されたファイルを、ThreatSense.Net 早期警告システムを利用して提出します。 |

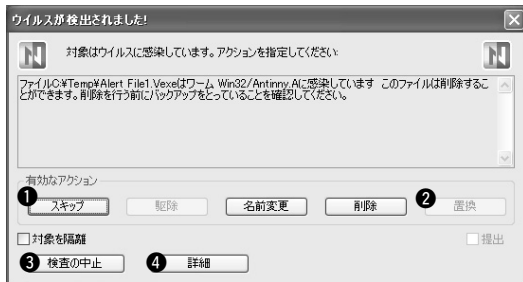


早期警告システムを利用したEset社へのファイル送信は、早期対応をお約束するものではありません。



「提出」のチェックボックスが有効になるのは、以下の条件を満たしている場合です。
 早期警告システムを有効に設定している
 定義ファイルに登録されていない、ウイルスの疑いのあるファイルが検出された

警告ウィンドウその



オンデマンドスキャナが発する警告ウィンドウです。通常は「駆除」か「削除」を選択して、コンピュータをウイルスの感染から防いでください。



感染場所等によっては、「駆除」および「削除」を選択できず、手動処理が必要となる場合があります。

| | |
|---------|---|
| ① スキップ | このウイルスに対しては何も処理を行わず、ウイルス検査を続行します。 |
| ② 置換 | ブートセクタ上に存在するウイルスの場合、ウイルスを正常なモジュールに入れ替えます。 |
| ③ 検査の中止 | ウイルス検査を中止します。 |
| ④ 詳細 | 詳細な情報を表示します。 |

警告ウィンドウその



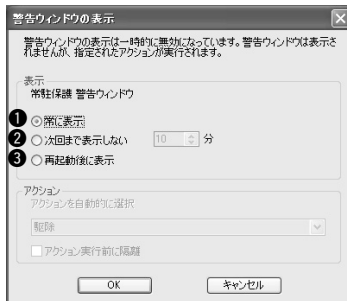
オンアクセススキャナ(AMON、DMON、EMON、IMON)が発する警告ウィンドウです。通常は「駆除」か「削除」を選択して、コンピュータをウイルスの感染から防いでください。

① ウイルス情報

ファイル：ウイルスを検出したファイル名を表示します。
 ウイルス：既知のウイルスであれば、そのウイルスの名前を表示します。
 コメント：駆除の可能性や検出時の状態など、ウイルスに関する情報を表示します。

② 警告ウィンドウを表示

この警告ウィンドウを、今後也表示するかどうかを設定します。このエリアをクリックすると以下の画面が表示されます。



- | | |
|-------------|--|
| ① 常に表示 | 常に警告ウィンドウを表示します。 |
| ② 次回まで表示しない | 警告ウィンドウを表示しない時間を設定できます。 |
| ③ 再起動後に表示 | コンピュータを再度立ち上げるか再起動するまで、警告ウィンドウが表示されなくなります。 |

Chapter 3

NOD32の機能詳細

ここでは、NOD32の機能詳細について解説しています。

Chapter 3
NOD32の
機能詳細

ファイル操作時にウイルスを検査・駆除する

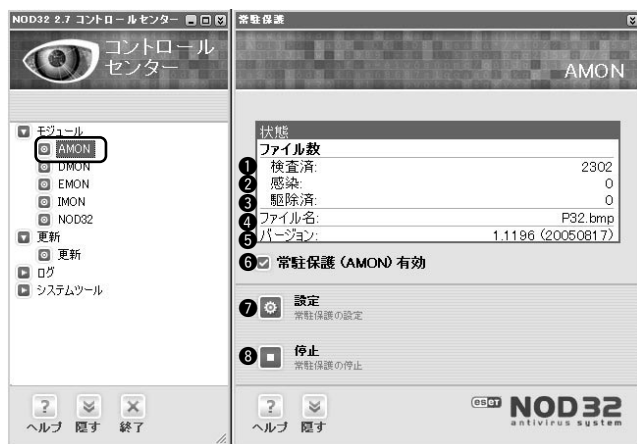
AMON (Access MONitor) を設定する

AMONは、ファイルに対してオープン/作成/実行といった操作が行なわれるたびに、自動的にウイルス検査を行ないます。細かな検査方法やアクション(ウイルスが検出された際にどのような処置を実行するのか)などを設定することができます。


Step 1


AMON の操作画面を表示する

AMONの操作画面を表示するには、コントロールセンターから、[AMON]をクリックします。



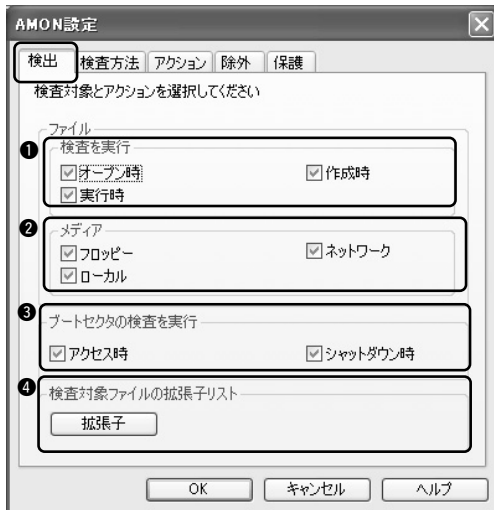
コントロールセンターの表示方法は28ページをご覧ください。

| | |
|--------------------|--|
| ① 検査済 | AMONを起動してから現在まで、ウイルス検査を行なったファイル数を表示しています。 |
| ② 感染 | 感染ファイルを検出した回数を表示しています。 |
| ③ 駆除済 | 感染したファイルを発見した場合、そのウイルスを駆除することに成功したファイル数を表示しています。 |
| ④ ファイル名 | 最後にウイルス検査を行なったファイル名を表示しています。  これらの①～④はリアルタイムで更新されるので、コンピュータを操作すると、表示内容が刻々と変化します。 |
| ⑤ バージョン | ウイルス定義ファイルのバージョン情報を表示しています。 |
| ⑥ 常駐保護 (AMON)有効 | この部分をクリックすると、AMONの機能を一時的にオン/オフすることができます(チェックマークが付いている状態がオンです)。ただし、AMONの機能をオフにするとウイルスに対して無防備になりますので、常時オンでご使用ください。 |

| | |
|------------------|---|
| <p>⑦ 設定</p> | <p>この部分をクリックすると、AMONの設定画面が表示されます。詳細は「AMONの検査対象や検査のタイミングなどを設定する」を参照してください。</p> |
| <p>⑧ 停止 / 開始</p> | <p>この部分をクリックすると、AMONを停止 / 開始することができます。[停止]と表示されているときにクリックするとAMONを停止し、[開始]と表示されているときにクリックするとAMONを開始します。しかしAMONを停止するとウイルスに対して無防備になりますので常時、[停止]と表示されている状態（AMON有効状態）でご使用ください。</p> <div style="display: flex; align-items: center;">  <p>システムによって、いったんAMONを停止してからAMONを再開しようとするときに「常駐保護をロードできません」と表示され、AMONを再開できない場合があります。このような場合、コンピュータを再起動してください。</p> </div> |

Step 2 AMONの検査対象や検査のタイミングなどを設定する

⑦[設定]ボタンをクリックすると、AMONの動作設定が行なえます。タブ部分ををクリックすることで、各設定画面（検出 / 検査方法 / アクション / 除外 / 保護）を表示します。各設定画面には[OK]・[キャンセル]・[適用]・[ヘルプ]ボタンがあり、設定項目をオン / オフした後、[適用]ボタンをクリックするか、[OK]ボタンをクリックすることで設定が有効になります。



① 検査を実行
ウイルスを検出するファイルに対する操作を設定します。

| | |
|-------|---------------------------|
| オープン時 | ファイルを開くときにウイルス検査を実施します。 |
| 作成時 | ファイルを作成するときにウイルス検査を実施します。 |
| 実行時 | ファイルを実行するときにウイルス検査を実施します。 |

② メディア
ウイルス検査を行なうメディアを設定します。

| | |
|--------|----------------------------|
| フロッピー | フロッピー上のファイルに対して、検査を実施します。 |
| ネットワーク | ネットワーク上のファイルに対して、検査を実施します。 |
| ローカル | ローカルなファイルに対して、検査を実施します。 |

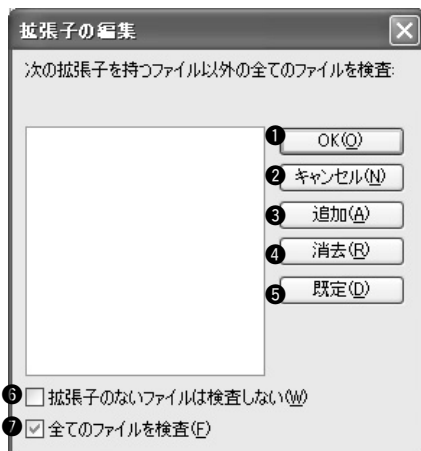
③ ブートセクタの検査を実行

ブートセクタをチェックするタイミングを設定します。

| | |
|----------|----------------------------------|
| アクセス時 | FDやCD-ROMにアクセスしたときにブートセクタを検査します。 |
| シャットダウン時 | コンピュータをシャットダウンするときにブートセクタを検査します。 |

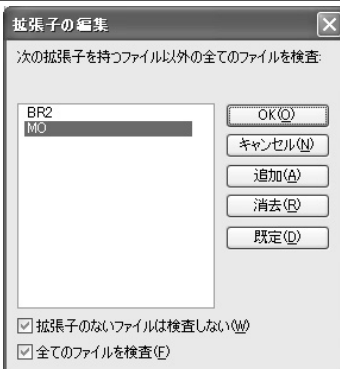
④ 検査対象ファイルの拡張子リスト

ウイルス検査を実施するファイルの拡張子を設定します。設定する拡張子は“.”(ドット)以降を設定してください。通常は既定値のままお使いください。



| | |
|-----------------|--|
| ① OK | 変更を決定します。 |
| ② キャンセル | 何もせずに、処理を終了します。 |
| ③ 追加 | 拡張子を追加します。表示されたテキストボックスに拡張子を入力して、[OK]ボタンをクリックしてください。 |
| ④ 消去 | 拡張子を削除します。拡張子を表示しているリストウィンドウから、消去する拡張子をマウスで選んで反転させた状態で、[消去]ボタンをクリックしてください。 |
| ⑤ 既定 | 登録された拡張子を既定状態に戻します。 |
| ⑥ 拡張子のないファイルを検査 | 拡張子を持たないファイルもウイルス検査の対象にします。 |

⑦ 全てのファイルを検査



全てのファイルをウイルス検査の対象にします。同時にこの画面で設定された拡張子のファイルをウイルス検査の対象外とします(設定が反転することになります)。追加された拡張子のファイルがウイルス検査の対象外となり、[拡張子のないファイルは検査しない]と変更されます。

Step 3

AMONのウイルス検査の方法を設定する

検査方法

ウイルス検査の方法を設定します。



caution

安全のため、少なくとも「シグネチャ検査」と「ヒューリスティック検査」の2項目はオンにしてください。

① オプション

シグネチャ検査

ウイルス定義ファイルとウイルスのパターンを照らし合わせ、ウイルスを検出する方法です。ウイルス定義ファイルに記録された既知のウイルスなら、この方法で検出可能です。ただし「コントロールセンター」の「更新」で、絶えずウイルス定義ファイルを最新の状態にしておく必要があります。

ヒューリスティック検査

ウイルスを仮想コンピュータで実際に動作させ、その挙動を観察することにより、ウイルスを検出する方法です。ウイルス定義ファイルに記録されてない、新種のウイルスに対して有効です。

アドウェア/スパイウェア/リスクウェア

定義ファイルに記録されたパターンを基準に、アドウェアやスパイウェアなどの検出を行いません。

潜在的に不要なアプリケーション

定義ファイルに記録されたパターンを基準に、潜在的に不要なアプリケーションの検出を行いません。

潜在的に安全ではないアプリケーション

定義ファイルに記録されたパターンを基準に、潜在的に安全ではないアプリケーションの検出を行いません。

② ファイル作成

新規作成時や変更時に検査対象とするファイルの形式や検査方法を設定します。

圧縮された実行形式

通常は圧縮されていて、実行時に解凍される形式のファイルを検査対象に含めます。

自己解凍形式

自己解凍形式(解凍プログラムを含む形で圧縮されたファイル)を検査対象に含めます。

アドバンスドヒューリスティック

ファイル内部を直接解析してウイルスのコードを検査した後、仮想コンピュータで動作させてウイルスの有無を確認します。

③ 検査の最適化

検査方法の設定やパターン情報に合わせて検査手法を変更し、速度を向上させます。



この機能は、Windows 98/Meでは動作しません。

Step 4

AMONのアクション(ウイルス発見時の対処方法)を設定する

アクション

ウイルスを検出した際の対処方法を設定します。



ウイルス検出時

| | |
|-----------------------|---|
| ① アクセスを禁止し、アクションを選択する | ウイルスに感染したファイルに対するアクセスを禁止し、警告ウィンドウを表示して対応をオペレーションで決定します。 |
| ② アクセスを禁止する | ウイルスに感染したファイルに対するアクセスを禁止します。 |
| ③ 自動的に駆除する | 感染したファイルからウイルスを駆除します。 |

除外

特定のフォルダやファイルを、ウイルス検査の対象から除外する設定です。

A 追加

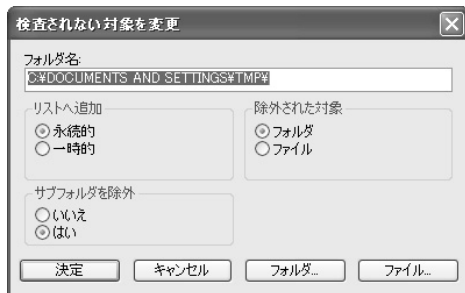
特定のフォルダやファイルを除外の対象にするときに、クリックします。



| | |
|-----------------|--|
| ① フォルダ名 | 除外するフォルダやファイルを入力します。フォルダを指定するときには、[フォルダ]をクリックしてディレクトリツリー画面から選択することができます。ファイルを指定するときには、[ファイル]をクリックして、ファイル選択画面から選択することができます。 |
| ② リストへ追加・永続的 | 除外の設定をこのまま使用する場合は、この項目をオンにします。 |
| ③ リストへ追加・一時的 | 除外の設定を一時的に使用する場合は、この項目をオンにします。この項目をオンにした場合、除外の設定は操作の終了から有効となりますが、次にコンピュータを再起動したときには無効になります。 |
| ④ 除外された対象・フォルダ | 除外するフォルダを指定するときにはオンにします。 |
| ⑤ 除外された対象・ファイル | 除外するファイルを指定するときにはオンにします。 |
| ⑥ サブフォルダを除外・いいえ | 検査対象外にフォルダを指定した場合、そのサブフォルダを除外の対象にしません。 |
| ⑦ サブフォルダを除外・はい | 検査対象外にフォルダを指定した場合、そのサブフォルダを除外の対象にします。 |

**B 変更**

表示されたフォルダやファイルを選んで、このボタンをクリックすると、その内容を変更することができます。

**C 削除**

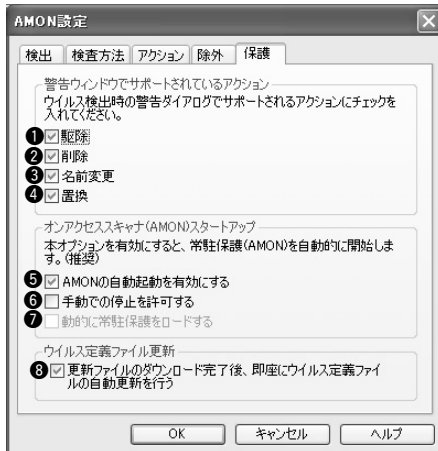
表示されたフォルダやファイルを選んで、このボタンをクリックすると、その内容を削除することができます。

D 既定

除外の対象を、既定状態に戻します。

保護

ウイルスが検出されたときに現れる警告ウィンドウで、選択することのできる対処方法を設定します。



| | |
|--------|------------------------------------|
| ① 駆除 | ウイルスを駆除します。 |
| ② 削除 | ウイルスに感染したファイルを削除します。 |
| ③ 名前変更 | ウイルスに感染したファイルの名前を変更して、ウイルスを無力化します。 |
| ④ 置換 | ブートセクタ上のウイルスを、正常なコードに置換します。 |



[駆除]はウイルスのみを削除し、感染されたファイルなどを正常に戻す措置です。[削除]は感染されたファイル自体を削除し、ウイルスを撃退します。よって[削除]では感染されたファイルを復元することはできません。ウイルスのタイプによって駆除できるものと、駆除できずに削除しなければならないものがあります。

| | |
|---|--|
| ⑤ AMONの自動起動を有効にする | [コントロールセンター]のロードと同時にAMONを自動起動するとき、オンにします。この項目をオフにするとウイルスに対して無力となる場合がありますので、必ず自動起動を有効にしてください。 |
| ⑥ 手動での停止を許可する | 起動しているAMONを手動で停止させる必要がある時、この項目をオンにします。[コントロールセンター]に[停止]ボタンが表示されます。 |
| ⑦ 動的に常驻保護をロードする | コンピュータを再起動せずにAMONの停止と開始が可能になります。Windows 9x系のOSでのみ、この項目の指定が可能になります。 |
| ⑧ 更新ファイルのダウンロード完了後、即座にウイルス定義ファイルの自動更新を行なう | 更新ファイルをダウンロードした後、すぐにウイルス定義ファイルを更新する時、オンにします。ウイルス定義ファイルの自動更新で問題が生じる場合はオフにしてください。 |

Microsoft Office 文書のチェックを行なう

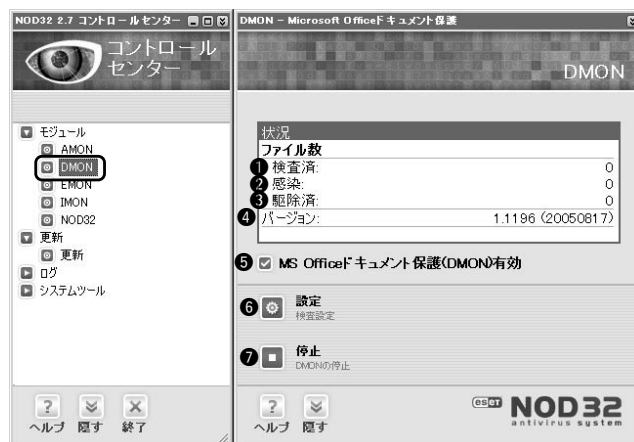
DMON(Document MONitor)を設定する

DMONは、Microsoft Office 文書ファイルおよびInternet Explorer(IE)が自動的にダウンロードするファイルのウイルス検査を行ないます。Office 文書に埋め込まれたマクロウイルスなどの感染を発見し、処理を施すことが可能です。また、ActiveXのようにIEが自動的にダウンロードするファイルの検査も行ないます。

Step 1

DMON の操作画面を表示する

DMONの操作画面を表示するには、コントロールセンターから、[DMON]をクリックします。



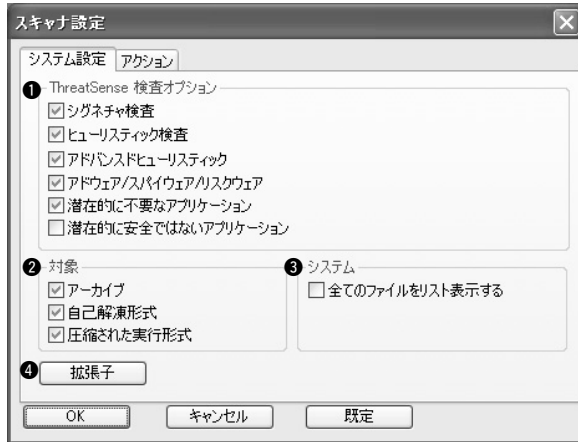
コントロールセンターの表示方法は28ページをご覧ください。

| | |
|-----------------------------|--|
| ① 検査済 | DMONを起動してから現在まで、ウイルス検査を行なったファイル数を表示しています。 |
| ② 感染 | 感染ファイルを検出した回数を表示しています。 |
| ③ 駆除済 | 感染したファイルを発見した場合、そのウイルスを駆除することに成功したファイル数を表示しています。 |
| ④ バージョン | ウイルス定義ファイルのバージョン情報を表示しています。 |
| ⑤ MS Officeドキュメント保護(DMON)有効 | この部分をクリックすると、DMONの機能を一時的にオン/オフすることができます(チェックマークがついている状態がオンです)。ただし、DMONの機能をオフにするとウイルスに対して無防備になりますので、常時オンでご使用ください。 |
| ⑥ 設定 | この部分をクリックすると、DMONの設定画面が表示されます。詳細は「DMONの設定を行なう」を参照してください。 |
| ⑦ 停止/開始 | この部分をクリックすると、DMONを停止/開始することができます。DMONを停止するとウイルスに対して無防備になりますので、常時[停止]と表示される状態(DMON有効状態)でご使用ください。 |

Step 2

DMON の設定を行なう

システム設定



① ThreatSense 検査オプション

| | |
|---------------------|--|
| シグネチャ検査 | ウイルス定義ファイルとウイルスのパターンと照らし合わせ、ウイルスを検出する方法です。ウイルス定義ファイルに記録された既知のウイルスなら、この方法で検出可能です。ただし[コントロールセンター]の[更新]で、絶えずウイルス定義ファイルを最新の状態にしておく必要があります。 |
| ヒューリスティック検査 | ウイルスを仮想コンピュータ上で実際に動作させ、その挙動を観察することにより、ウイルスを検出する方法です。ウイルス定義ファイルに記録されていない、新種のウイルスに対して有効です。 |
| アドバンスドヒューリスティック | より高度なヒューリスティック検査を行ないます。通常はオンの状態でお使いください。 |
| アドウェア/スパイウェア/リスクウェア | 定義ファイルに記録されたパターンを基準に、アドウェアやスパイウェアなどの検出を行ないます。 |
| 潜在的に不要なアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に不要なアプリケーションの検出を行ないます。 |
| 潜在的に安全ではないアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に安全ではないアプリケーションの検出を行ないます。 |



安全のため、少なくとも「シグネチャ検査」と「ヒューリスティック検査」の2項目はオンにしてください。

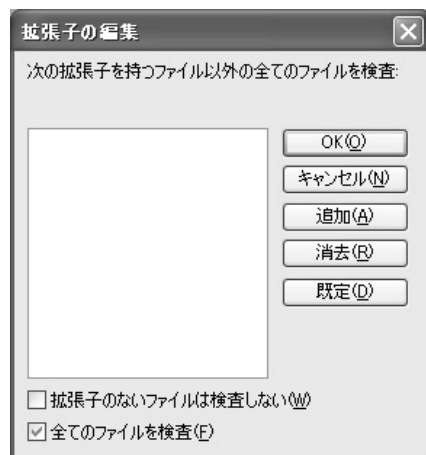
② 対象

| | |
|-----------|---|
| アーカイブ | 実行形式でない書庫形式のファイルを、ウイルス検査の対象にします。 |
| 自己解凍形式 | 自己解凍形式(解凍プログラムを含む形で圧縮されたファイル)もウイルス検査の対象に含めます。 |
| 圧縮された実行形式 | 通常は圧縮されていて、実行時に解凍される形式のファイルをウイルス検査の対象にします。 |

③ システム

この項目をオンにすると、ウイルス検査の際に、感染していないファイルも含めてログファイルを表示します。

④ 拡張子

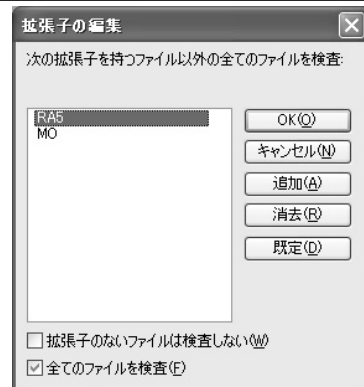


このボタンをクリックすると、ウイルス検査の対象となるファイルの拡張子を設定することができます。設定する拡張子は“.”(ドット)以降を設定してください。通常は既定値のままお使いください。

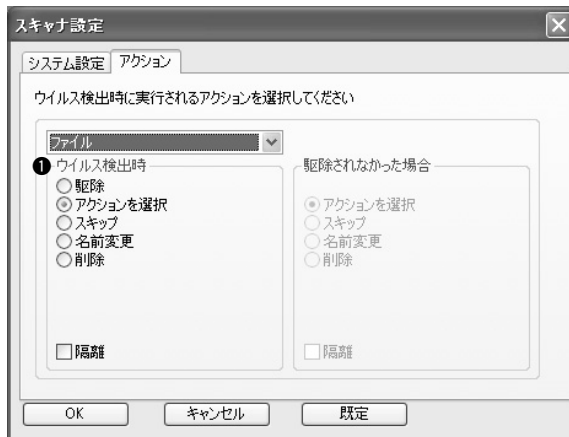
| | |
|------------------|--|
| OK | 変更を決定します。 |
| キャンセル | 何もせずに、処理を終了します。 |
| 追加 | 拡張子を追加します。表示されたテキストボックスに拡張子を入力して、[OK]ボタンをクリックしてください。 |
| 消去 | 拡張子を削除します。拡張子を表示しているリストウィンドウから、消去する拡張子をマウスで選んで反転させた状態で、[消去]ボタンをクリックしてください。 |
| 既定 | 登録された拡張子を既定状態に戻します。 |
| 拡張子のないファイルは検査しない | 拡張子を持たないファイルはウイルス検査の対象から外します。 |

全てのファイルを検査

全てのファイルをウイルス検査の対象にします。同時にこの画面で設定された拡張子のファイルをウイルス検査の対象外とします（設定が反転する事になります）。[追加]された拡張子のファイルがウイルス検査の対象外となり、[拡張子のないファイルを検査]は[拡張子のないファイルは検査しない]に変更されます。

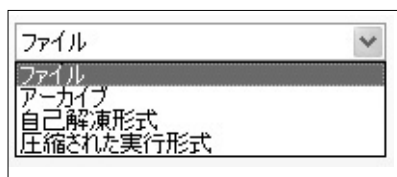


アクション



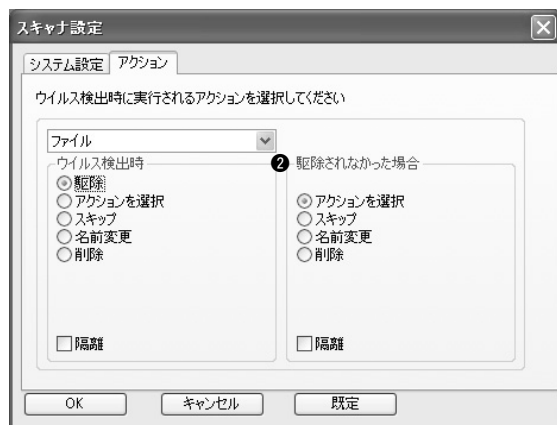
① ウイルス検出時

ウイルスが検出された時、どのような対処方法を実施するかを設定します。アクションはファイル/アーカイブ/自己解凍形式/圧縮された実行形式のそれぞれに対して設定します。形式の選択は▼をクリックして行ないます。



| | |
|----------|---------------------------------------|
| 駆除 | 感染したファイルからウイルスを駆除します。 |
| アクションを選択 | 警告ウィンドウを表示して対応をオペレーションで決定します。 |
| スキップ | ウイルスに対する措置は行ないません。 |
| 名前変更 | ウイルスに感染したファイルの名前を変更して、無力化します。 |
| 削除 | ウイルスに感染したファイルを削除します。 |
| 隔離 | ウイルスに対して決められた措置を行なう前に、感染したファイルを隔離します。 |

② 駆除されなかった場合



[ウイルス検出時]の設定で「駆除」を選択した場合、駆除に失敗したときの処置を設定する必要があります。

| | |
|----------|---------------------------------------|
| アクションを選択 | 警告ウィンドウを表示して対応をオペレーションで決定します。 |
| スキップ | ウイルスに対する措置は行ないません。 |
| 名前変更 | ウイルスに感染したファイルの名前を変更して、無力化します。 |
| 削除 | ウイルスに感染したファイルを削除します。 |
| 隔離 | ウイルスに対して決められた措置を行なう前に、感染したファイルを隔離します。 |

Microsoft Exchange メール の ウィルス を 検査 ・ 駆除 する

EMON(E-mail MONitor)を 設定 する

EMON は、Microsoft Outlook 95 以降 で、MAPI を 利用 した メール サーバ と の 接続 時 に ウィルス 検査 を 行 な い ます。Microsoft Outlook 2000 以降 で は、POP3 や IMAP など の プロトコル を 利用 した メール の 検査 も 行 な う こ と が で き ます。



caution

Microsoft Outlook Express を は じ め と す る インターネットメール(POP3 メール)のウィルス検査はIMONが行ないます。

Step 1

操作画面の表示について

EMON の 操作 画面 を 表示 す る に は、コントロールセンターから[EMON]をクリックします。



コントロールセンターの表示方法は28ページをご覧ください。

| | |
|-------------------------------------|---|
| ① 検査済 | メール送受信時に検査したファイル数を表示します。 |
| ② 感染 | 感染ファイルを検出した回数を表示しています。 |
| ③ 駆除済 | ウィルスの駆除に成功したファイル数を表示します。 |
| ④ バージョン | ウイルス定義ファイルのバージョンを表示します。 |
| ⑤ MS Outlook用 メールモニタ (EMON)有効 | EMONの機能を一時的にオン/オフすることができます(チェックマークが付いている状態がオンです)。 |

| | |
|-----------|---|
| ⑥ システム設定 | EMONの機能設定画面が表示されます。詳細は「EMONの設定を行なう」を参照してください。 |
| ⑦ 終了 / 開始 | EMONを停止 / 開始する事ができます。[終了]と表示されている状態でクリックするとEMONの動作を一時停止し、[開始]と表示されている状態でクリックするとEMONの動作を再開します。 |

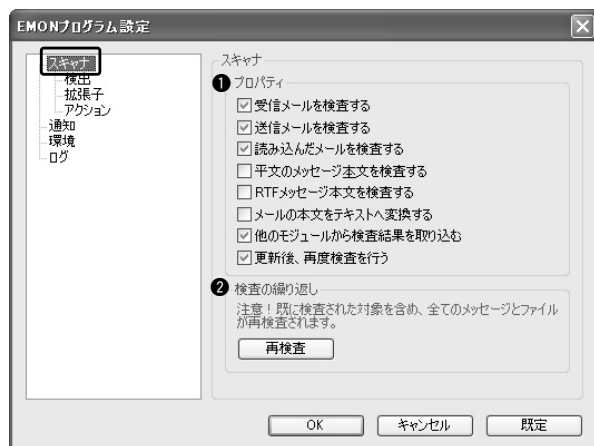
Step 2

EMON の設定を行なう

コントロールセンターの[システム設定]をクリックすると、EMONの各種設定を行なうことができます。

スキャナ

ウイルス検査の対象やタイミングに対する設定を行ないます。



① プロパティ

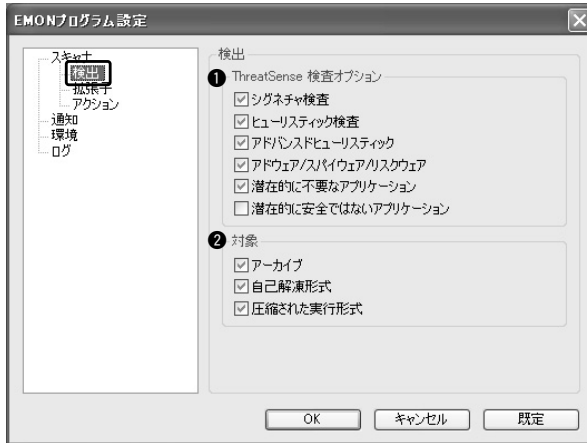
| | |
|--------------------|---|
| 受信メールを検査する | メール受信時にウイルス検査を行ないます。 |
| 送信メールを検査する | メール送信時にウイルス検査を行ないます。 |
| 読み込んだメールを検査する | メールの読み込み時にウイルス検査を行ないます。 |
| 平文のメッセージ本文を検査する | テキスト(平文)で作成されたメール本文を検査します。 |
| RTFメッセージ本文を検査する | RTF(リッチテキストフォーマット)で作成されたメール本文を検査します。 |
| メールの本文をテキストへ変換する | ウイルス検査時にHTMLやRTF形式で作成されたメール本文をテキストに変換します。 |
| 他のモジュールから検査結果を取り込む | NOD32やIMONなどから検査結果をEMONに取り込み、ウイルス検査精度を高めます。 |
| 更新後、再度検査を行う | EMONのウイルス定義ファイル更新後、自動的にウイルス検査を再度実行します。 |

② 検査の繰り返し

再検査 | すべてのExchangeメールと添付ファイルに対し、強制的に再検査を行ないます。

検出

ウィルス検査方法や対象ファイルに対する設定を行ないます。



① ThreatSense 検査オプション

| | |
|---------------------|---|
| シグネチャ検査 | ウィルス定義ファイルを基準とするパターン検査を行ないます。定義ファイルに記録された既知ウィルスなら、この検査で検出が可能です。ただし[コントロールセンター]の[更新]で、絶えずウィルス定義ファイルを最新の状態にしておく必要があります。 |
| ヒューリスティック検査 | ウィルスを仮想コンピュータ上で実際に動作させ、その挙動を観察することによりウィルスを検出します。ウィルス定義ファイルに記録されていない、新種のウィルスに対して有効です。 |
| アドバンスドヒューリスティック | ファイル内部を直接解析してウィルスのコードを検査した後、仮想コンピュータで動作させてウィルスの有無を確認します。ヒューリスティックよりさらに高度な検査です。 |
| アドウェア/スパイウェア/リスクウェア | 定義ファイルに記録されたパターンを基準に、アドウェアやスパイウェアなどの検出を行ないます。 |
| 潜在的に不要なアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に不要なアプリケーションの検出を行ないます。 |
| 潜在的に安全ではないアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に安全ではないアプリケーションの検出を行ないます。 |



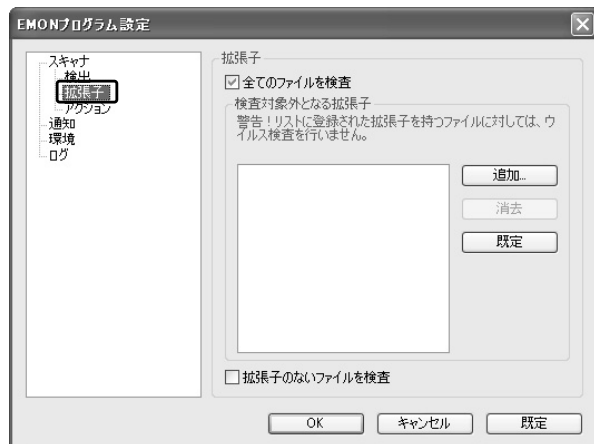
安全のため、少なくとも「シグネチャ検査」と「ヒューリスティック検査」の2項目はオンにしてください。


② 対象

| | |
|-----------|---|
| アーカイブ | 実行形式でない書庫形式のファイルをウイルス検査の対象に含めます。 |
| 自己解凍形式 | 自己解凍形式(解凍プログラムを含む形で圧縮されたファイル)をウイルス検査の対象に含めます。 |
| 圧縮された実行形式 | 通常は圧縮されていて、実行時に解凍される形式のファイルをウイルス検査の対象に含めます。 |

拡張子

ウイルス検査の対象となるファイルを、拡張子を基準に設定します。



| | |
|---------------|--|
| 全てのファイルを検査 | 拡張子のないファイル以外、検査が可能なすべてのファイルを検査対象に設定します(拡張子設定は無効になります)。 |
| 追加 | 検査対象から外される拡張子を入力する画面を表示します。検査対象から外したい拡張子を“.”(ドット)を付けずに入力してください。  |
| 消去 | 選択した除外拡張子設定を消去します。 |
| 既定 | 除外拡張子設定を既定値に戻します。 |
| 拡張子のないファイルを検査 | 拡張子を持たないファイルもウイルス検査の対象に含めます。 |

アクション

ウィルス検査の対象となるファイル拡張子の設定を行います。



アクション対象
ファイル

ファイル / アーカイブ / 自己解凍形式 / 圧縮された実行形式 の項目毎に、ウィルス検出時のアクション設定が可能です。

① ウィルス検出時

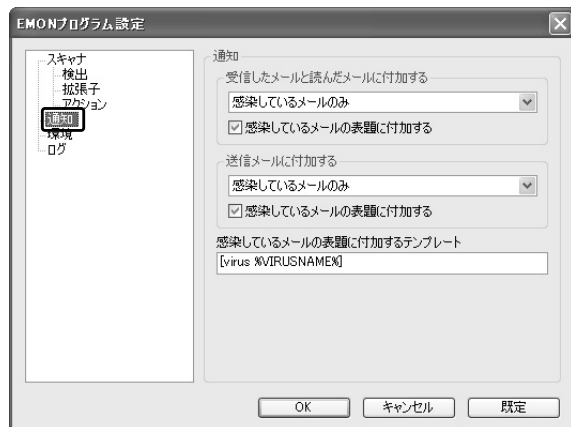
| | |
|----------|--|
| 駆除 | 感染したファイルからウィルスを駆除します。 |
| アクションを選択 | 警告画面を表示し、ユーザーの処理選択を待ちます。 |
| スキップ | ウィルスに対する処置を行いません。 |
| 名前変更 | ウィルスに感染したファイルの名前を変更し、無力化します。 |
| 削除 | ウィルスに感染したファイルを削除します。 |
| 隔離 | 設定したアクション処理を行なう前に、感染したファイルを隔離し、安全性を高めます。 |

② 駆除されなかった場合

| | |
|----------|--|
| アクションを選択 | 警告画面を表示し、ユーザーの処理選択を待ちます。 |
| スキップ | ウィルスに対する処置を行いません。 |
| 名前変更 | ウィルスに感染したファイルの名前を変更し、無力化します。 |
| 削除 | ウィルスに感染したファイルを削除します。 |
| 隔離 | 設定したアクション処理を行なう前に、感染したファイルを隔離し、安全性を高めます。 |

通知

NOD32は、受信・送信したメールのウイルス検査を行なった際、メール本文に対するウイルス検査済みのコメントの付加や、ウイルスに感染したメールの表題の変更が可能です。ここでは、この通知機能に関する設定を行ないます。



受信したメールと読んだメールに付加する
受信した(または開封した)Exchangeメールに
対するコメント付加の設定を行ないます。

| | |
|-------------|--|
| しない | メールにウイルス検査のコメントを付加しません。 |
| 感染しているメールのみ | ウイルスに感染したメールのみにウイルス検査のコメントを付加し、感染していないメールには付加しません。 |
| 全てのメール | ウイルスの感染・非感染に関わらず、ウイルス検査のコメントを付加します。 |

感染しているメールの表題に付加する

ウイルスに感染したメールの表題に、指定した文字列が自動的に付加されます。

送信メールに付加する

送信したExchangeメールに対するコメント付加の設定を行ないます。

| | |
|-------------|--|
| しない | メールにウイルス検査のコメントを付加しません。 |
| 感染しているメールのみ | ウイルスに感染したメールのみにウイルス検査のコメントを付加し、感染していないメールには付加しません。 |
| 全てのメール | ウイルスの感染・非感染に関わらず、ウイルス検査のコメントを付加します。 |

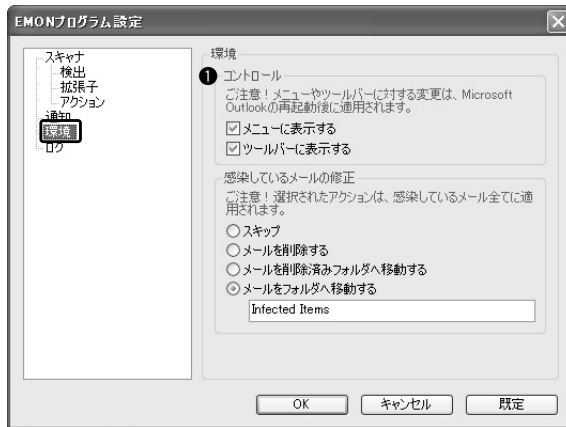
感染しているメールの表題に付加する

ウイルスに感染したメールの表題に、指定した文字列が自動的に付加されます。

感染しているメールの表題に付加するテンプレート

と のチェックがオンになっている際にウイルスに感染したメールの表題に付加する、文字列の設定を行ないます。既定値では、本来の表題の前にウイルスの名称を付加する設定です。

環境



① コントロール

NOD32は、Outlookのメニューバーやツールバーに、NOD32の操作を行うメニュー/ボタンを付加できます。ここでは、それらの設定を行ないます。

| | |
|------------|--------------------------------------|
| メニューに表示する | OutlookのメニューにNOD32のウイルス検査メニューを追加します。 |
| ツールバーに表示する | OutlookのツールバーにNOD32の操作ボタンを追加します。 |

② 感染しているメールの修正

NOD32は、ウイルス感染が発見されたメールを、特定のフォルダへ自動的に移動する機能があります。ここでは、この機能に関する設定を行ないます。

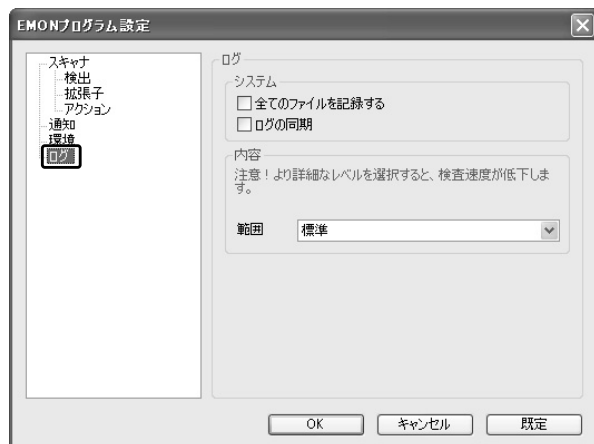


ここで設定する設定は「アクション」で設定するウイルス対処方法とは関係がありません。また、感染が確認されたメール全てに適用されます。とくにメールを削除する設定には注意してください。

| | |
|-------------------|--|
| スキップ | ウイルス感染したメールに対する移動作業を行ないません。 |
| メールを削除する | ウイルス感染したメールを、自動的に削除します。 |
| メールを削除済みフォルダに移動する | ウイルス感染したメールを、Outlookの「削除済み」フォルダへ移動します。 |
| メールをフォルダへ移動する | 設定した名称のフォルダを作成し、ウイルスに感染したメールを移動します。 |

ログ

ここでは、EMONのウイルス検査ログの記録に関する設定を行います。



| | |
|--------------|--|
| 全てのファイルを記録する | ウイルス検査ログに、ウイルスに感染していないメールに関する内容も含めません。 |
| ログの同期 | NOD32全体のシステムログに、EMONのウイルス検査ログを含めます。 |
| 内容 | ウイルス検査ログに含めるデータ量の詳細度を、最小 / 標準 / 詳細の3段階から選択します。 |



「内容」で詳細度を高めると、記録されるデータの詳細度が高まる代わりに、ウイルス検査速度が低下します。

電子メール、Webの検査を行なう

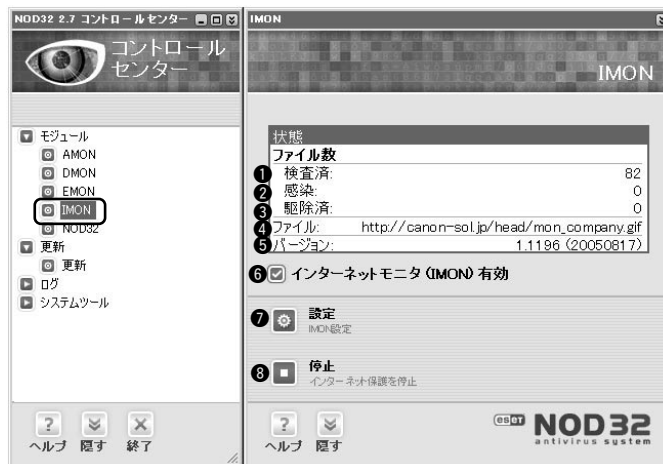
IMON (Internet MONitor) を設定する

IMONは、Webページ上のデータをはじめとするHTTPで転送されるファイルや、POP3メールに対するウイルス検査を行ないます。Webサイト上のファイルやメールに添付されたファイルを受信時に検査し、感染していたファイルの場合は即座に対処を行ないます。

IMONに関する設定は、コントロールセンターのIMON操作画面から行なえます。ここでは、設定項目の詳細について解説します。

Step 1

IMONの操作画面を表示する



IMONの操作画面を表示するには、コントロールセンターから、[IMON]をクリックします。

コントロールセンターの表示方法は28ページをご覧ください。

| | |
|------------------------|---|
| ① 検査済 | IMONが検査したファイル数を表示します。 |
| ② 感染 | 感染ファイルを検出した回数を表示しています。 |
| ③ 駆除済 | 感染したファイルから、駆除に成功したファイル数を表示します。 |
| ④ ファイル | 最後にウイルス検査を行なったファイル名を表示します。 |
| ⑤ バージョン | ウイルス定義ファイルのバージョン情報を表示します。 |
| ⑥ インターネットモニタ (IMON) 有効 | この部分をクリックすると、IMONの機能を一時的にオン/オフすることができます (チェックマークが付いている状態がオンです)。ただし、IMONの機能をオフにするとウイルスに対して無防備になりますので、常時オンでご使用ください。 |
| ⑦ 設定 | この部分をクリックすると、IMONの設定画面が表示されます。詳細は「IMONの設定」を参照してください。 |

| | |
|-----------|---|
| ⑧ 停止 / 開始 | この部分をクリックすると、IMONを停止 / 開始する事ができます。[停止]と表示されているときにクリックするとIMONを終了し、[開始]と表示されているときにクリックするとIMONを開始します。しかしIMONを終了するとウイルスに対して無防備になりますので、常時[停止]と表示されている状態（IMON有効状態）でご使用ください。 |
|-----------|---|

Step 2

IMON の設定を行なう

POP3

POP3を使ったメールのウイルス検査に関する設定を行ないます。

① 設定

メール検査を有効にする

この項目がオンになっていれば、メールに対するウイルス検査を行ないます。安全性を保つためにも、いつもオンにしておきましょう。

POP3が使用するポート番号

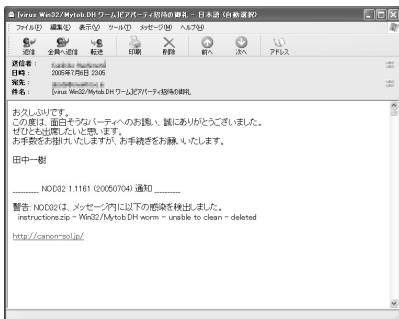
この項目にはPOP3でメールを受信するとき使用するポート番号を設定してください。通常POP3のポートには“110”が使われますので、変更する必要はありません。

② 検査済みメール

検査したメールに対する処理を設定します。

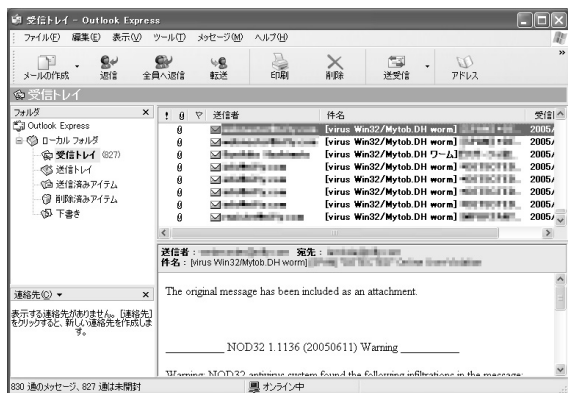
・メールに検査通知を付加する

| | |
|-----------------|---|
| 付加しない | メールにウイルス検査のコメントを付加しません。 |
| 感染しているメールのみ付加する | ウイルスに感染したメールのみ、ウイルス検査のコメントを付加し、ウイルスの感染していないメールには付加しません。 |
| 全てのメールに付加する | ウイルスに感染・非感染に関わらず、メールにウイルス検査のコメントを付加します。 |



ウイルス検査のコメントを付加したメール（Outlook Expressの例）

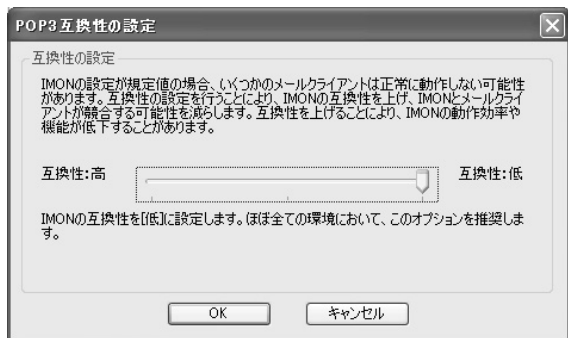
感染したメールの表題を次の文字列に修正する



ウイルスに感染したメールの表題に、指定した文字列が自動的に付加されます。既定値では、本来の表題の前にウイルスの名称を付加する設定となっています。

③ 互換性の設定

IMONとメールクライアントの互換性を設定したり、ネットワーク設定の変更を自動的に反映させるかどうかの設定が行なえます。通常は既定値で問題ありませんが、メールクライアントが正常に動作しない場合は、「設定」ボタンをクリックし、互換性を上げてください。



HTTP



HTTPを使った通信に関するウイルス検査の設定を行いません。

① 設定

| | |
|----------------------------|--|
| HTTP 検査を有効にする | HTTPを使用した通信に対してウイルス検査を行いません。 |
| HTTP が使用するポート番号 | HTTP が使用するポート番号を指定します。ポート番号はカンマで区切れば複数指定できます。 |
| 他ポートにおける HTTP 通信の検査を自動的に行う | 指定したポート以外のポートで通信が行なわれた場合、ウイルス検査を行なうかどうかを指定します。 |

② アクション

ウイルスの感染が検出された時、どのような対処方法を実施するかを設定します。

| | |
|--------------------------------|---|
| 警告ウィンドウを表示し、アクションを選択する | 警告ウィンドウを表示します。処理方法を選択してください。 |
| ウイルス感染しているファイルのダウンロードを自動的に拒否する | ウイルスに感染したファイルは、自動的にファイルのダウンロードを拒否し、警告ウィンドウを表示します。 |

③ 交換性の設定

IMONとHTTPクライアントの交換性を設定します。通常は既定値で問題ありませんが、特定のHTTPクライアントが動作しない場合は、IMONの動作を弱くし、交換性を高く設定できます。

「サーバとの交換性」ボタンをクリックして表示されるウィンドウで、高い交換性に設定するプログラムを選択してください。「設定」ボタンをクリックすると、交換性が高く設定されているHTTPクライアントの名称を確認できます。

④ 自動バッシュモード

大容量(または長時間)のダウンロードを必要とするファイルに対して、自動的にIMONの動作を交換性の高いモードに切り換える設定です。通常は既定値で問題ありません。ファイルのダウンロードに関して動作の異常が発生する場合のみ、設定を変更してください。

詳細



① インターネットフィルタ

外部から侵入しようとした形跡があれば、その情報をログに記録します。

② ネットワーク設定の変更

ネットワークの設定が変更されたことを自動的に検出し元の設定に戻します。他人によるネットワーク設定の改ざんを防ぐことができます。また、[修正]をクリックすることで、いつでもネットワーク設定の修正ができます。

③ 除外



IMONの検査から除外するアプリケーションを設定します。[編集]をクリックして検査から除外するアプリケーションを追加します。

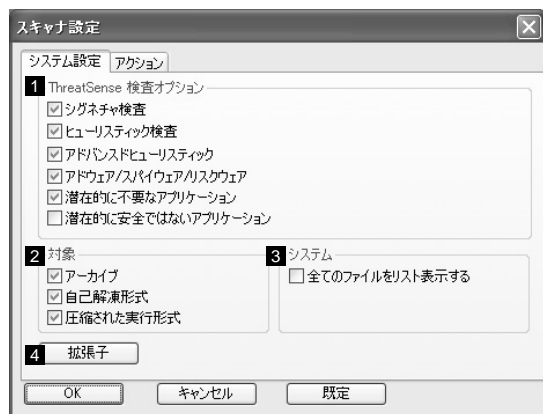
④ 表示

サイズの大きいファイルをダウンロードする際に、システムトレイ付近にその進行状況を表示します。表示画面の透明度は、スライダーで設定できます。



この機能は、Windows 98/Meでは動作しません。

⑤ スキャナ



[設定]ボタンをクリックすると、ウイルス検査の詳細やウイルスを検出したときの措置を設定する画面が表示されます。[システム設定]タブと[アクション]タブをクリックすることで、各設定画面を表示します。

[システム設定]と[アクション]画面で設定を行なったあと、[OK]をクリックするとその設定が有効になります。[キャンセル]をクリックすると、設定を行わず終了します。[既定]は、設定内容を既定値に戻します。

システム設定

ウイルス検査の方法を設定します。

① ThreatSense 検査オプション

| | |
|---------------------|--|
| シグネチャ検査 | ウイルス定義ファイルとウイルスのパターンと照らし合わせ、ウイルスを検出する方法です。ウイルス定義ファイルに記録された既知のウイルスなら、この方法で検出可能です。ただし[コントロールセンター]の[更新]で、絶えずウイルス定義ファイルを最新の状態にしておく必要があります。 |
| ヒューリスティック検査 | ウイルスを仮想コンピュータ上で実際に動作させ、その挙動を観察することにより、ウイルスを検出する方法です。ウイルス定義ファイルに記録されてない、新種のウイルスに対して有効です。 |
| アドバンスドヒューリスティック | より高度なヒューリスティック検査を行ないます。通常はオンの状態でお使いください。 |
| アドウェア/スパイウェア/リスクウェア | 定義ファイルに記録されたパターンを基準に、アドウェアやスパイウェアなどの検出を行ないます。 |
| 潜在的に不要なアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に不要なアプリケーションの検出を行ないます。 |
| 潜在的に安全ではないアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に安全ではないアプリケーションの検出を行ないます。 |



安全のため、少なくとも「シグネチャ検査」と「ヒューリスティック検査」の2項目はオンにしてください。

2 対象

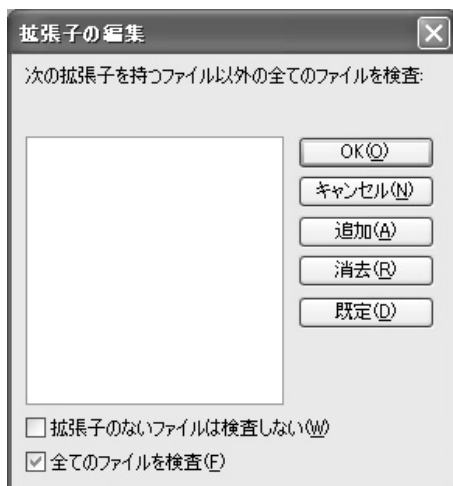
| | |
|-----------|---|
| アーカイブ | 実行形式でない書庫形式のファイルを、ウイルス検査の対象にします。 |
| 自己解凍形式 | 自己解凍形式(解凍プログラムを含む形で圧縮されたファイル)をウイルス検査の対象に含めます。 |
| 圧縮された実行形式 | 通常は圧縮されていて、実行時に解凍される形式のファイルをウイルス検査の対象にします。 |

3 システム

添付ファイルごとにウイルス検査の結果をメールに表示します。

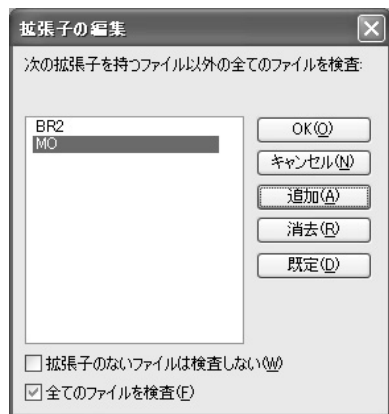
4 拡張子

ウイルス検査の対象となるファイルの拡張子を設定することができます。設定する拡張子は“.”(ドット)以降を設定してください。通常は既定値のままお使いください。

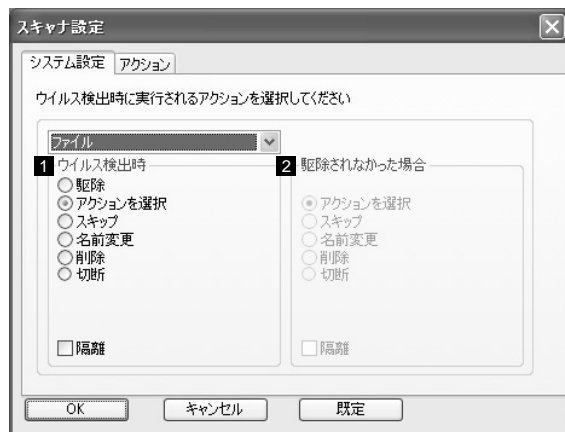


| | |
|-------|--|
| OK | 変更を決定します。 |
| キャンセル | 何もせずに、処理を終了します。 |
| 追加 | 拡張子を追加します。表示されたテキストボックスに拡張子を入力して、[OK]ボタンをクリックしてください。 |
| 消去 | 拡張子を削除します。拡張子を表示しているリストウインドウから、消去する拡張子をマウスで選んで反転させた状態で、[消去]ボタンをクリックしてください。 |
| 既定 | 登録された拡張子を既定状態に戻します。 |

| | |
|------------------|--|
| 拡張子のないファイルは検査しない | 拡張子を持たないファイルをウイルス検査の対象から外します。 |
| 全てのファイルを検査 | 全てのファイルをウイルス検査の対象にします。同時にこの画面で設定された拡張子のファイルをウイルス検査の対象外とします(設定が反転する事になります)。[追加]された拡張子のファイルがウイルス検査の対象外となり、[拡張子のないファイルを検査]は[拡張子のないファイルは検査しない]に変更されます。 |



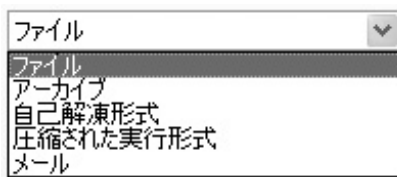
アクション



1 ウイルス検出時

ウイルスが検出された時、どのような対処方法を実施するかを設定します。アクションはファイル/アーカイブ/自己解凍形式/圧縮された実行形式/メール、それぞれのファイル形式に対して設定します。

ファイル/アーカイブ/自己解凍形式/圧縮された実行形式/メールの選択は、▼をクリックして行ないます。



| | |
|----------|---------------------------------------|
| 駆除 | 感染したファイルからウイルスを駆除します。 |
| アクションを選択 | 警告ウィンドウを表示して対応をオペレーションで決定します。 |
| スキップ | ウイルスに対する措置は行ないません。 |
| 名前変更 | ウイルスに感染したファイルの名前を変更して、無力化します。 |
| 削除 | ウイルスに感染したファイルを削除します。 |
| 切断 | 当該通信を切断します。 |
| 隔離 | ウイルスに対して決められた措置を行なう前に、感染したファイルを隔離します。 |

2 駆除されなかった場合

[ウイルス検出時]の設定で駆除を選択した場合、駆除に失敗したときの処置を設定する必要があります。

| | |
|----------|---------------------------------------|
| アクションを選択 | 警告ウィンドウを表示して対応をオペレーションで決定します。 |
| スキップ | ウイルスに対する措置は行ないません。 |
| 名前変更 | ウイルスに感染したファイルの名前を変更して、無力化します。 |
| 削除 | ウイルスに感染したファイルを削除します。 |
| 切断 | 当該通信を切断します。 |
| 隔離 | ウイルスに対して決められた措置を行なう前に、感染したファイルを隔離します。 |

⑥ ウェブサイト アクセス ブロッキング

あらかじめ定義されたブロッキングリスト(アクセス禁止リスト)に従い、悪意のあるファイルが存在するウェブサイトへのアクセスが検知された際、自動的にアクセスを遮断します。アクセスと同時にスパイウェアなどを自動的にダウンロードさせようとするサイトなどに対して有効です。

検査するディスクやフォルダ・ファイルを 設定する

NOD32 オンデマンドスキャナ

オンデマンドスキャナの設定

オンデマンドスキャナの起動画面です。ここでポイントとなるのは、**A** 上部に配置された5つのタブと**B** 検査対象となる「ディスク」の設定欄、そして、**C** 検査対象となる「フォルダとファイル」の設定欄です。



オンデマンドスキャナが起動すると、いったん検査ログ表示を行ない基本事項のチェックの後、この検査対象画面を表示します。

A 設定画面切り替えタブ

各タブをクリックすることによって、オンデマンドスキャナの設定を行ないます。

| | |
|----------|---|
| ① 検査対象 | ウイルス検査を行なうドライブやCD-ROMドライブ、ファイルやフォルダを設定する画面を表示します。 |
| ② 検査ログ | ウイルス検査を行なったログ(記録)を表示します。 |
| ③ アクション | ウイルスを検出したとき、ウイルスに対してどのような処置を行なうか設定できます。 |
| ④ 設定 | ウイルス検査の対象、検出方法などNOD32の詳細な設定を行ないます。 |
| ⑤ プロファイル | 色々な設定内容に名前を付けて保存し、必要に応じて読み出すことができます。 |

B 検査対象となる「ディスク」の設定欄について

ウイルス検査を行なうドライブを表示・設定します。表示されているドライブをマウスでダブルクリックすると、赤いチェックマークがオンになり、ウイルス検査の対象になります。

既にチェックされているドライブを、もう一度ダブルクリックすると、チェックマークをオフにすることができます(ウイルス検査の対象から外れます)。



チェックマークが入っている

Cドライブは赤いチェックマークがオンでウイルス検査の対象となっているが、Dドライブはウイルス検査の対象となっていない状態



caution

この設定でウイルス検査の対象から外したドライブは、ウイルス検査が行なわれませんので注意が必要です。大容量ディスクなどで、ウイルス検査に時間がかかりすぎる等以外では、既定値の設定を使用するか、全てのディスクをチェックするようにしてください。

| | |
|-----------|--|
| ⑥ ローカル | この項目をオンにすると、ローカルのHDD全てがウイルス検査の対象になります。 |
| ⑦ ネットワーク | この項目をオンにすると、ドライブ名 (C:やD:など) が割り当てられているネットワークドライブが全てウイルス検査の対象になります。この項目はネットワークドライブをドライブ名に置き換えている場合のみ有効です。 |
| ⑧ 全て選択 | ディスクとして認識・表示されているドライブを、全てウイルス検査の対象とします。 |
| ⑨ 選択を全て解除 | 現在、ウイルス検査の対象とされているディスクを、全てウイルス検査の対象から解除します。 |

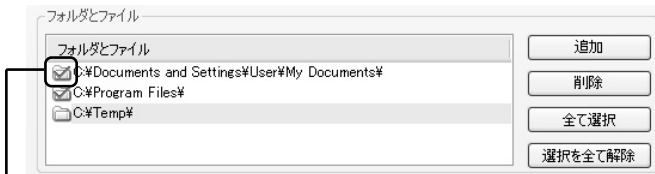
④ 検査対象となる「フォルダとファイル」の設定欄について

この設定によりドライブ単位ではなく、より詳細なフォルダやファイルをウイルス検査の対象とすることができます。共有フォルダや共通のファイルなど、特に危険性の高いエリアを指定することによって、迅速なウイルス検査を行なうことができます。

指定のチェックと追加について

表示されているフォルダやファイルをマウスでダブルクリックすると、赤いチェックマークがオンになり、ウイルス検査の対象になります。

既にチェックされているフォルダ名やファイル名を、もう一度ダブルクリックすると、チェックマークをオフにすることができます (ウイルス検査の対象から外れます)。

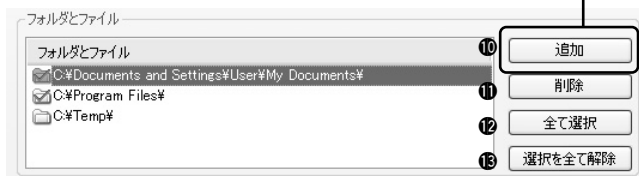


チェックマーク

"C:\Documents and Settings\User\My Documents" は赤いチェックマークが付きウイルス検査の対象となっているが、"C:\Temp" は対象となっていない状態

⑩追加

フォルダとファイルのリストに、対象フォルダやファイルを追加します。またこのボタンで追加されたフォルダやファイルは赤いチェックマークがオンになり、ウイルス検査の対象になります。このボタンをクリックするとフォルダ及びファイルの選択画面になります。



caution

この設定でウイルス検査の対象から外したフォルダ・ファイルは、ウイルス検査が行われませんので注意が必要です。大容量ディスクなどで、ウイルス検査に時間がかかりすぎる等以外では、既定値の設定を使用するか、全てのディスクをチェックするようにしてください。

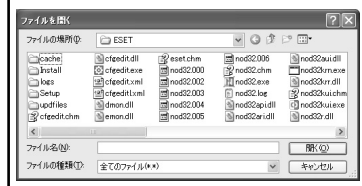
フォルダやファイルを選んだら、最後に[OK]ボタンをクリックします



[フォルダ]ボタンをクリックすると、フォルダツリー選択画面が表示されるので、対象フォルダをクリックしてください。



[ファイル]ボタンをクリックすると、ファイル選択画面が表示されるので、対象ファイルをクリックしてください。



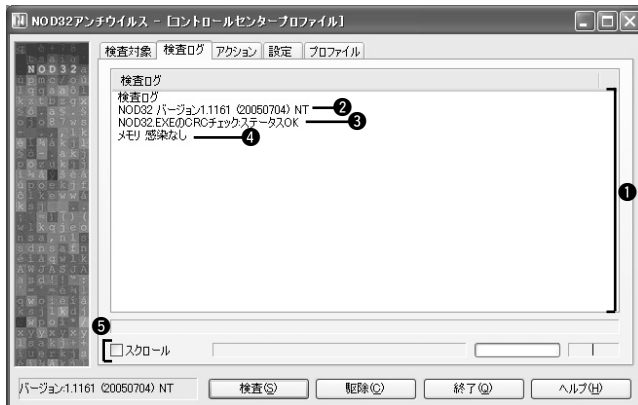
| | |
|----------|---|
| ⑪削除 | 表示されているフォルダやファイルを選択した状態で、このボタンをクリックすると、ファイルとフォルダ表示から削除されます。 |
| ⑫全て選択 | 表示されているフォルダやファイルを、全てウイルス検査の対象にします。 |
| ⑬選択を全て解除 | 表示されているフォルダやファイルを、全てウイルス検査の対象外にします。 |

検査ログで詳細を知る

NOD32 オンデマンドスキャナ

検査ログの見方

ここでは検査ログ画面について説明しています。検査ログ画面は、オンデマンドスキャナを起動し、[検査ログ]タブをクリックすることで表示できます。



① ウイルス検査の過程（ログ）を順次、表示するエリアです。



上記画面は、NOD32 が起動した直後のものです。お使いのコンピュータがウイルスに感染することなく、NOD32 が正常起動するとこのような画面になります。

② NOD32のバージョン情報を表示します。

③ 自分自身（NOD32）が改ざんされていないかをチェックし、その結果を表示します。ウイルスにはワクチンソフトに改ざんを加え、無力化してしまうものがあります。NOD32は自分自身が書き換えられていないかを、起動時にチェックします。

④ メモリにウイルスが常駐していないかをチェックし、その結果を表示します。

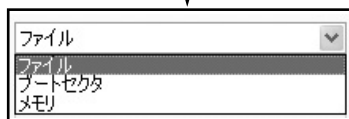
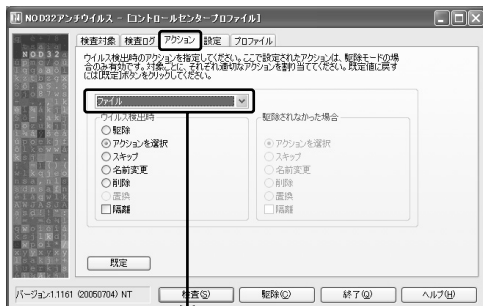
⑤ ウイルス検査中のファイルなどを表示するエリアです。[スクロール]がオンになっていると、自動的にログ表示がスクロールされ、現在実行中の作業を表示し続けることができます。

ウイルス検出時の処置を設定する

NOD32 オンデマンドスキャナ

アクション設定の詳細

ここではアクション設定について説明しています。アクション画面は、オンデマンドスキャナを起動し、[アクション]タブをクリックすることで表示できます。



アクションでは、ウイルスが検出された際に、どのような処置を行なうかを設定します。まず最初にアクションを設定する対象（ファイル/ブートセクタ(OS起動時に必ず実行されるプログラムが格納されている、ハードディスクやフロッピーディスクの場所)/メモリなど）を選択します。

対象を選択後、「ウイルス検出時」における設定と「駆除されなかった場合」における設定を行ないます。各項目をマウスで選んでクリックすると、チェックマークがオンになります。

ウイルス検出時



| | |
|----------|---|
| 駆除 | 感染したファイルからウイルスを駆除します。 |
| アクションを選択 | 警告ウィンドウを表示して対応をオペレーションで決定します。 |
| スキップ | ウイルスに対する措置は行ないません。 |
| 名前変更 | ウイルスに感染したファイルの名前を変更して、無力化します。 |
| 削除 | ウイルスに感染したファイルを削除します。 |
| 置換 | ウイルスを安全なコードに置換します（この措置はブートセクタのみに対して有効です）。 |
| 隔離 | ウイルスに対して決められた措置を行なう前に、感染したファイルを隔離します。 |



[駆除]はウイルスのみを削除し、感染されたファイルなどを正常に戻す措置です。[削除]は感染されたファイル自体を削除し、ウイルスを撃退します。したがって、[削除]では感染されたファイルを復元することはできません。ウイルスのタイプによって駆除できるものと、駆除できずに削除しなければならないものがあります。

駆除されなかった場合

駆除されなかった場合

- アクションを選択
- スキップ
- 名前変更
- 削除
- 置換
- 隔離

| | |
|--------------|---|
| アクション を選択 | 警告ウィンドウを表示して対応をオペレーションで決定します。 |
| スキップ | ウイルスに対する措置は行ないません。 |
| 名前変更 | ウイルスに感染したファイルの名前を変更して、無効化します。 |
| 削除 | ウイルスに感染したファイルを削除します。 |
| 置換 | ウイルスを安全なコードに置換します(この措置はブートセクタのみに対して有効です)。 |
| 隔離 | ウイルスに対して決められた措置を行なう前に、感染したファイルを隔離します。 |



caution

設定内容によっては、ウイルス検査が無効化することがありますので、注意してください。

検査時の設定

NOD32 オンデマンドスキャナ

検査時のさまざまな設定の詳細

ここでは検査時の設定について説明しています。設定画面は、オンデマンドスキャナを起動し、[設定]タブをクリックすることで表示できます。



ウイルス検査の方法や、ログファイル表示・扱いなど、オンデマンドスキャナの重要な項目を設定します。

① 検査対象

ウイルス検査を行なう対象を設定します。

| | |
|-------------|---|
| ファイル | HDDやCD-ROM上のファイルをウイルス検査の対象にします。多くのウイルスはファイルに寄生します。 |
| ブートセクタ | OS起動時に必ず実行されるプログラムが格納されている、ハードディスクやCD-ROM、フロッピーディスクのブートセクタを、ウイルス検査の対象にします。ウイルスによってはこのエリアに寄生することがあります。 |
| メモリ | メモリをウイルス検査の対象にします。メモリに常駐するウイルスも存在します。 |
| アーカイブ | チェックをオンに設定すると、実行形式でない書庫形式のファイルをウイルス検査の対象に含めます。 |
| 自己解凍形式 | チェックをオンに設定すると、自己解凍形式(解凍プログラムを含む形で圧縮されたファイル)をウイルス検査の対象に含めます。 |
| 圧縮された実行形式 | チェックをオンに設定すると、通常は圧縮されていて、実行時に解凍される形式のファイルをウイルス検査の対象に含めます。 |
| メール | メールや添付ファイルをウイルス検査の対象に含めます。 |
| NTFSサブストリーム | NTFSでフォーマットしたHDDにおいて、ファイル管理用に使われる特殊領域(サブストリーム)をウイルス検査の対象に含めます。 |

②ThreatSense 検査オプション

ウイルスのチェック方法を設定します。

| | |
|---------------------|--|
| シグネチャ検査 | ウイルス定義ファイルのウイルスパターンと照らし合わせ、ウイルスを検出する方法です。ウイルス定義ファイルに記録された既知のウイルスなら、この方法で検出可能です。ただし、[コントロールセンター]の[更新]で、絶えずウイルス定義ファイルを最新の状態にしておく必要があります。 |
| ヒューリスティック検査 | ウイルスを仮想的なコンピュータ内で実際に動作させ、その挙動を観察することにより、ウイルスを検出する方法です。ウイルス定義ファイルに記録されていない、新種のウイルスに対して有効です。 |
| アドバンスドヒューリスティック | ファイル内部を直接解析してウイルスのコードが含まれていないかを検査し、仮想コンピュータで実際に動作させてウイルスの有無を確認します。ウイルス定義ファイルに記録されていない、新種のウイルスに対して有効です。 |
| アドウェア/スパイウェア/リスクウェア | 定義ファイルに記録されたパターンを基準に、アドウェアやスパイウェアなどの検出を行ないます。 |
| 潜在的に不要なアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に不要なアプリケーションの検出を行ないます。 |
| 潜在的に安全ではないアプリケーション | 定義ファイルに記録されたパターンを基準に、潜在的に安全ではないアプリケーションの検出を行ないます。 |



安全のため、少なくとも「シグネチャ検査」と「ヒューリスティック検査」の2項目はオンにしてください。

③システム

ログの表示方法や警告音の有無、メールのチェック方法について設定します。

| | |
|-------------------|---|
| 全てのファイルをリスト表示する | ウイルス検査の際に、ウイルスに感染していないファイルもログファイルに表示します。この設定をオンにするとログファイルが増大するので、特に理由がない限り、オフにしておきます。 |
| 警告音 | ウイルスを検出すると、警告音を鳴らします。 |
| MAPIインターフェースを利用する | メールをウイルス検査する場合、MAPIインターフェースを利用するようにします。MAPI (Messaging API) とは、マイクロソフト社が提唱するメール操作のための仕組みです。OutlookなどMAPIを採用したメーラーをご利用の場合は、このチェックをオンにしておきます。 |
| アンチステルス技術を有効 | ステルス技術を使ってコンピュータに身を潜めるルートキットの検出を行ないます。この機能は、Windows 98/Meでは動作しません。 |

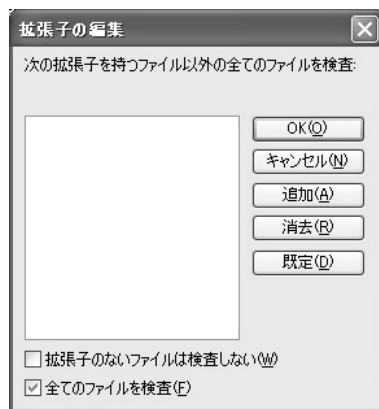
④ 検査ログ

検査ログに対する設定を行いません。

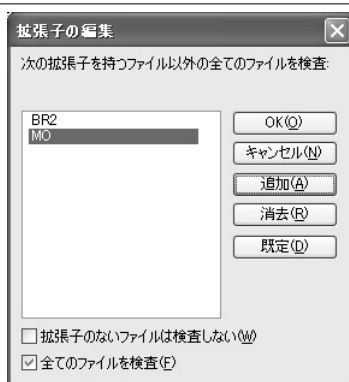
| | |
|----------|--------------------------------|
| 有効 | 検査ログを有効にします。通常はこの項目をオンにしてください。 |
| 整形 | 検査ログを整形します。 |
| 追記 / 上書き | 検査ログをその都度上書きするか、追記するかを設定します。 |
| 最大サイズ | 検査ログの最大サイズを設定します。 |
| 名前 | 検査ログの名前を設定します。 |

⑤ 拡張子

ウイルス検査を実施するファイルの拡張子を設定します。設定する拡張子は“.”(ドット)以降を設定してください。通常は既定値のままお使いください。[拡張子]をクリックすると次の画面が表示されます。



全てのファイルを検査

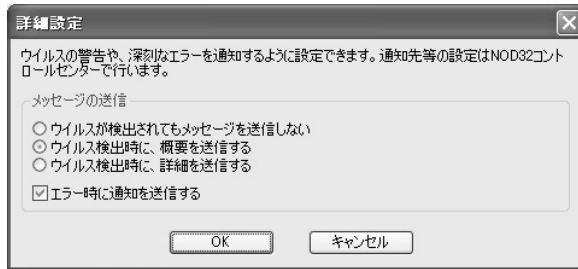


| | |
|------------------|--|
| OK | 変更を決定します。 |
| キャンセル | 何もせずに、処理を終了します。 |
| 追加 | 拡張子を追加します。表示されたテキストボックスに拡張子を入力して、[OK]ボタンをクリックしてください。 |
| 消去 | 拡張子を削除します。拡張子を表示しているリストウィンドウから、消去する拡張子をマウスで選んで反転させた状態で、[消去]ボタンをクリックしてください。 |
| 既定 | 登録された拡張子を既定状態に戻します。 |
| 拡張子のないファイルは検査しない | この項目をオンにすると、拡張子を持たないファイルはウイルス検査の対象から外します。 |

この項目をオンにすると、全てのファイルをウイルス検査の対象にします。同時にこの画面で設定された拡張子のファイルをウイルス検査の対象外とします（設定が反転する事になります）。追加された拡張子のファイルがウイルス検査の対象外となり、[拡張子のないファイルは検査しない]に変更されます。

⑥ 詳細

ウイルスの検出時に、システム管理者にその旨の通知を出すことができます。



point

通知先や通知方法などの設定は、NOD32 コントロールセンターの[システムツール] [システム設定]を選択し、[設定]ボタンをクリックして表示される画面の[通知]タブで行ないます(103 ページ参照)。

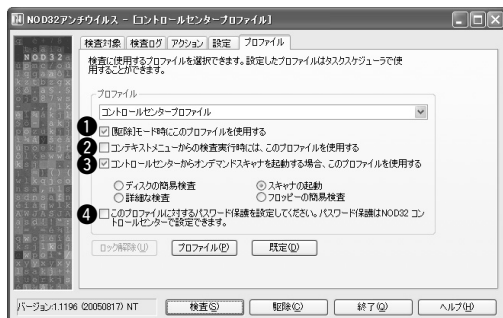
プロファイルで “ 設定 ” を保存する

NOD32 オンデマンドスキャナ

設定の保存と読み出し

ここではプロファイルの設定について説明しています。設定画面は、オンデマンドスキャナを起動し、[プロファイル]タブをクリックすることで表示できます。

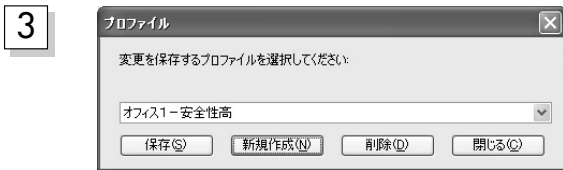
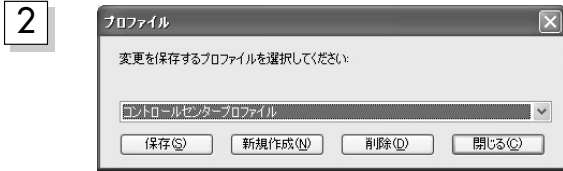
プロファイルでは、各設定を保存し再度、読み出すことができます。複雑な設定でも、プロファイルに登録しておけば、使用状況や目的に合わせて設定を容易に切り替えることができます。



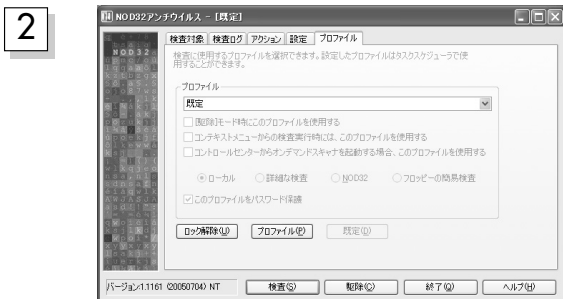
保存方法

1 [プロファイル]タブをクリックします。

- ①の[[駆除]モード時に~]は、検査スケジュールに登録しているプロファイルにのみ有効で、このチェックをオンにする事で、駆除モードでスケジュールを作成する事ができます。
- ②の[コンテキストメニューからの~]をオンにすると、現在選択されているプロファイルを、ファイルやフォルダに対してマウスの右クリックでNOD32を起動した場合の既定値とすることができます ([コンテキストメニュー]とは、ファイル等を右クリックした際に表示される、ポップアップメニューのことです)。
- ③の[コントロールセンターから~]をオンにし、下のパターンより検査対象となるドライブ (または検査の詳細さ)を選択すると、現在選択されているプロファイルを、コントロールセンターからNOD32を起動した場合の既定値とすることができます。
- ④のチェックをオンにして[プロファイル]ボタンをクリックすると、プロファイルはパスワード保護された状態で保存されます。次回起動時には[ロック解除]ボタンをクリックしてパスワードロックの解除を行なわない限り、他の設定を行うことはできなくなります。[既定]をクリックすると、選択中のプロファイルの設定変更を破棄し、NOD32の既定値に戻します。



設定の読み出し方法



[プロファイル]ボタンをクリックすると、「プロファイル」画面が表示されます。既定値の「コントロールセンタープロファイル」でよろしければ、[保存]ボタンをクリックします。

新しいプロファイル名で保存したい場合は、[新規作成]ボタンをクリックします。「新しいプロファイル名」入力画面が表示されますので、名前を入力後、[OK]ボタンをクリックします。

入力した名前が「プロファイル」画面に表示されます。よろしければ、[保存]ボタンをクリックします。

▼ をクリックして過去に保存したプロファイルを選択すると、その設定が復元されます。

プロファイル（設定状態）にパスワードが施されていれば、[ロック解除]のボタンがアクティブになります。[ロック解除]のボタンをクリックするとパスワードの入力が求められますのでパスワードを入力し、ロックを解除します。



point

パスワードの設定は、NOD32 コントロールセンターの[システムツール] [システム設定]を選択し、[設定]ボタンをクリックして「一般」タブの「パラメータ設定の保護」内の[設定]ボタンをクリックすることで行ないます（102 ページ参照）。

自動更新機能の詳細と設定

NOD32 コントロールセンター

更新とは？

「更新」は、ウイルスの特徴を記述したウイルス定義ファイルやNOD32自身を最新の状態へと更新します。この「更新」によって、新種のウイルスや亜種へと変化したウイルスが検出可能となります。またNOD32自身もバージョンアップされるので、機能の追加や充実も併せて行なうことができます。

また「更新」の設定によっては、決められた時間やイベント時に、ウイルス検査やプログラムを実行することもできます。

ここでは、「更新」画面について説明します。

「更新」画面の表示方法と内容について

「更新」の操作画面を表示するには、NOD32 コントロールセンターから、[更新]をクリックします。



NOD32 コントロールセンターの表示方法は28ページを参照してください。

| | |
|----------------|--|
| ① 状態 | 現在更新が行なわれているのか、待機中なのか、その状態を表示しています。 |
| ② サーバ | 接続するサーバを表示しています。 |
| ③ ウイルス定義ファイル更新 | ウイルス定義ファイルが自動更新されるのか、通知更新されるのかを表示しています。 |
| ④ コンポーネント更新 | NOD32のコンポーネントが自動更新されるのか、通知更新されるのかを表示しています。 |
| ⑤ 前回の更新 | 前回更新された日時を表示しています。 |
| ⑥ バージョン | ウイルス定義ファイルのバージョンを表示しています。 |
| ⑦ 自動更新 | この部分をオンにすると自動更新や設定された更新スケジュールが有効になります。オフにすると無効になります。 |

| | |
|-----|--|
| ⑧更新 | このエリアをクリックすると、今すぐ更新作業を開始し、新しいウイルス定義ファイルやモジュールがあればダウンロード・更新します。 |
| ⑨設定 | 更新作業の詳細を設定します。詳しい内容は[更新の設定]を参照してください。 |



自動更新と通知更新については、「更新の種類」を参照してください。



「更新」を行なうには、ユーザーIDとパスワードが必要です。ユーザーIDとパスワード取得に関しては16ページを参照してください。

更新の設定方法

Step 1

[設定]ボタンをクリックする

[設定]ボタンをクリックします。



セキュリティ保護のパスワードを設定している場合は、そのパスワード入力画面が表示され、パスワードの入力を求められます。

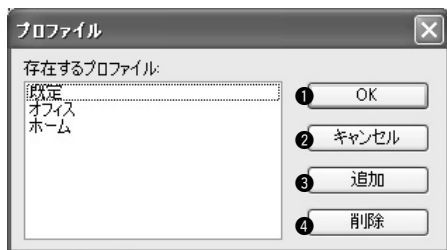
Chapter 3
NOD32の
機能詳細

Step 2

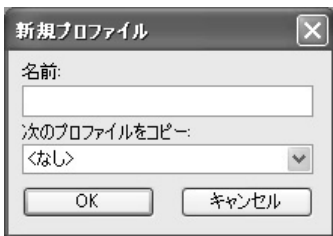
プロファイルを選択する

▼をクリックして保存されたプロファイルを選択します。選択されたプロファイルによって設定が切り替わります。

プロファイルの追加・削除について



新規にプロファイルを追加したり、削除することができます。

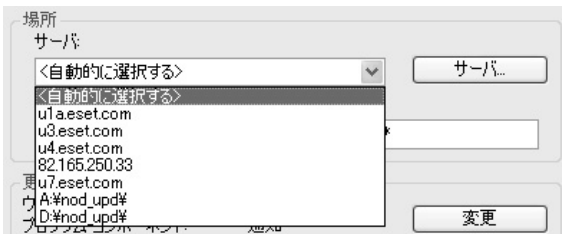
| | |
|---------|---|
| ① OK | プロファイルを追加・削除した場合、[OK]をクリックすることで追加・削除が有効になります。 |
| ② キャンセル | 何もせずに処理を終了します。 |
| ③ 追加 | 新しいプロファイルを追加します。  |
| ④ 削除 | マウスでプロファイルを選んで反転させ、[削除]をクリックすると、そのプロファイルを削除します。 |

名前に新しいプロファイル名を入力して、[OK]をクリックすると新規のプロファイルが作成されます。新しく作成するプロファイルに従来のプロファイルの内容をコピーするときは、▼をクリックしてコピーするプロファイルを選んでください。[キャンセル]をクリックすると、処理を中断します。

Step 3

サーバを設定する

更新を実行するために接続するサーバを設定します。▼をクリックして、接続するサーバを選択してください。



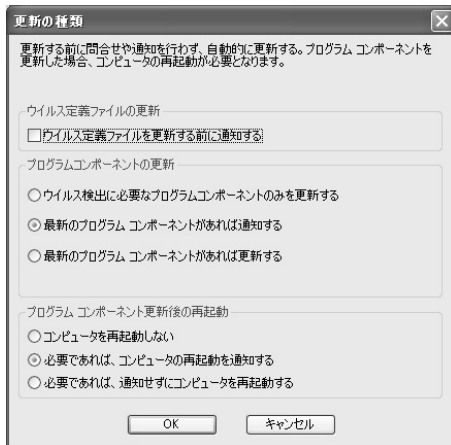
[サーバ]ボタンをクリックすると、新しいサーバを追加することができます。通常は、既定値の状態でお使いください。

Step 4

更新の種類を設定する

この欄には、現在のウイルス定義ファイルとプログラムコンポーネントの更新方法が表示されています。通常はなにも行わず、次のステップへ進みます。

変更を行なう場合は……



変更する場合は、83ページの「更新の設定」画面で[変更]ボタンをクリックします。「更新の種類」が表示され、どのような変更を加えるかの詳細な設定ができます。

ウイルス定義ファイルの更新

[ウイルス定義ファイルを更新する前に通知する]のチェックをオンにすると、ウイルス定義ファイルを更新するときに、その旨の通知を表示します。



[ウイルス定義ファイルを更新する前に通知する]のチェックをオンにすると、ウイルス定義ファイルを更新するときにこのような確認画面が表示されます

プログラムコンポーネントの更新

ウイルス定義ファイルが更新されるタイミングで、プログラムコンポーネントも更新するか、あるいは、更新前に通知するのか、などの設定を行ないます。[最新のプログラムコンポーネントがあれば更新する]のチェックをオンにすると、新しいプログラムコンポーネントがあると自動的に更新されます。

プログラム コンポーネント更新後の再起動

プログラムコンポーネント更新後の設定を行いません。プログラムコンポーネントの種類によっては、コンピュータの再起動が必要になることがありますので、通常は既定値のままお使いください。

Step 5

自動更新の設定を行なう

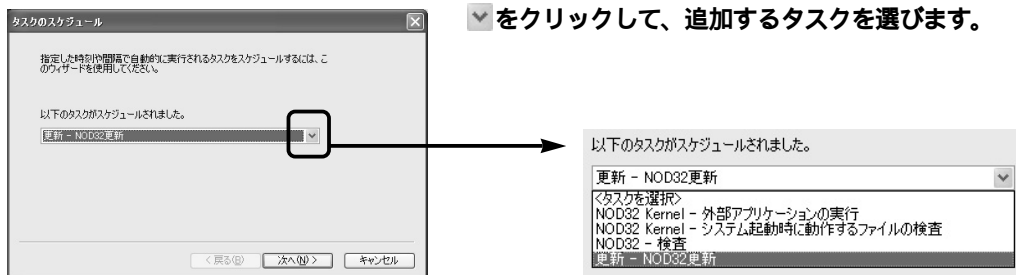
プログラムコンポーネントやウイルス定義ファイルの更新スケジュール、ウイルス検査実施スケジュール、NOD32から起動する外部プログラムのスケジュールを設定します。スケジュールを設定することによって、更新やウイルス検査を自動的に実行できるようになります。

すでにスケジュールが設定されている場合は、「自動更新がスケジュールされています」と表示されます。追加のスケジュールを設定する場合は、[スケジュール]をクリックしてください。なお、すでに設定されたスケジュールは、NOD32コントロールセンターの[システムツール] [スケジュール]で確認及び、変更等が可能です。既定値では1時間毎に設定されています。NOD32コントロールセンターの[システムツール] [スケジュール]の説明も併せてご参照ください(98ページ参照)。

スケジュールを設定するには

- 1 [スケジュール]ボタンをクリックします。

- 2  をクリックして、追加するタスクを選びます。



point

[NOD32 Kernel - 外部アプリケーションの実行]では、NOD32から外部プログラムを起動するスケジュールを設定します。

[NOD32 - 検査]では、オンデマンドスキャナを起動して、ウイルス検査を行うスケジュールを設定します。[NOD32 Kernel - システム起動時に動作するファイルの検査]では、オンデマンドスキャナを起動し、システム(OS)起動時に必要なファイルのウイルス検査を行うスケジュールを設定します。

[更新 - NOD32更新]では、NOD32におけるウイルス定義ファイルやプログラムコンポーネントの更新スケジュールを設定します。

追加するタスクを選んだら、[次へ]をクリックします。

3



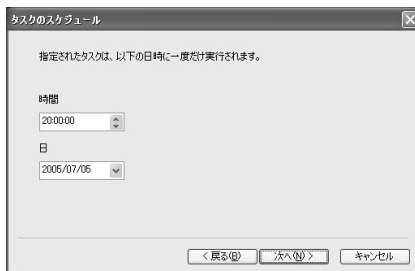
実行するタスク名と、実行タイミングを設定します。実行するタスク名を入力し、実行タイミングを選択したら、[次へ]をクリックします。



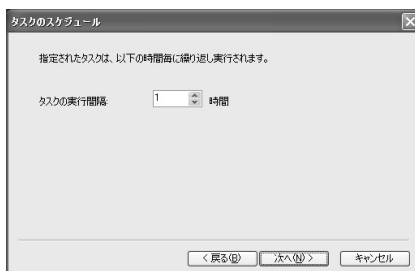
タスク名と実行タイミングを入力しないと、[次へ]をクリックできません。

4

3で選択した実行タイミングに応じた設定画面が表示されます。[戻る]をクリックすると、一つ前の画面に戻ります。実行タイミングを選択したら、[次へ]をクリックします。[キャンセル]をクリックすると、処理を終了します。

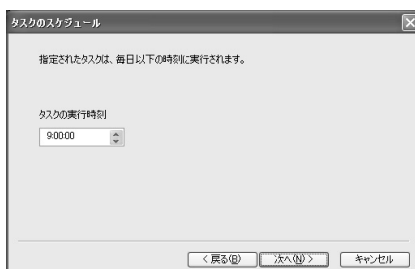


3で[一回]を設定した場合、時間はそれぞれ時間/分/秒をマウスで選んで、上下矢印をクリックすると値が増減します。直接キーボードから値を入力することもできます。日付は▼をクリックすると、カレンダーが表示されますので、日付を選んでください。直接キーボードから値を入力することもできます。

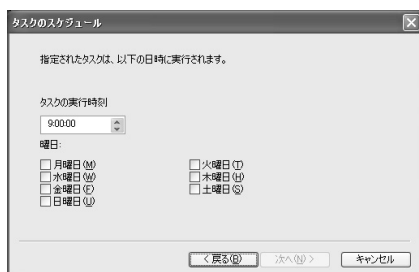


3で[繰り返し]を設定した場合、時間は上下矢印をクリックすると値が増減します。直接キーボードから値を入力することもできます。

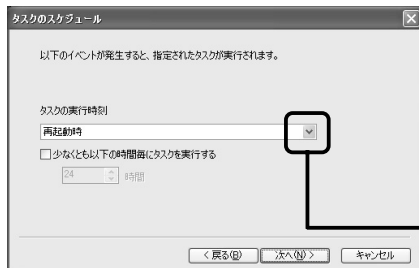
既定値では1時間毎に設定されています。



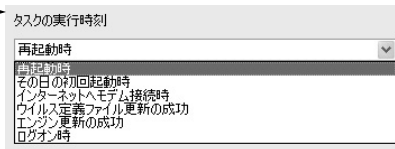
3で[毎日]を設定した場合、時間は上下矢印をクリックすると値が増減します。直接キーボードから値を入力することもできます。



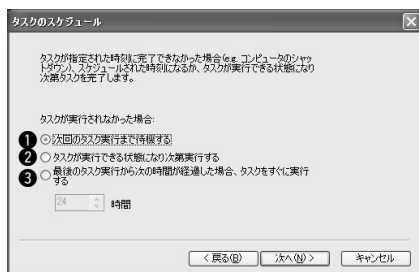
3で[毎週]を設定した場合、時間は $\uparrow\downarrow$ をクリックすると値が増減します。直接キーボードから値を入力することもできます。実行する曜日をマウスで選んで、チェックマークを付けてください。



3で[イベント毎]を設定した場合、 \downarrow をクリックして、イベントを選択します。イベント以外にも、時間でタスクを実行することも可能です。その場合には、[少なくとも以下の時間毎にタスクを実行]をオンにし、時間を入力します。



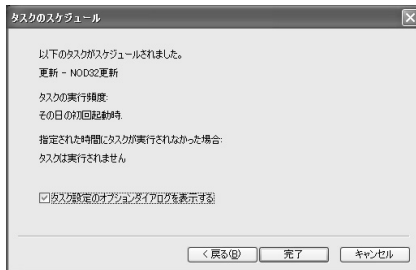
5



設定したタスクが完了できなかった時の措置を設定します。次の項目内容を参考にチェックをオンにした後、[次へ]をクリックします。

| | |
|-------------------------------------|---|
| ① 次回のタスク実行まで待機する | 次に設定した条件を満たすまで、タスクを実行しません。 |
| ② タスクが実行できる状態になり次第実行する | 設定した条件に関わらず可能になり次第、タスクを実行します。 |
| ③ 最後のタスク実行から次の時間が経過した場合、タスクをすぐに実行する | 一定の時間を経過したら、タスクを実行します。このとき、その時間を更に設定してください。 |

6



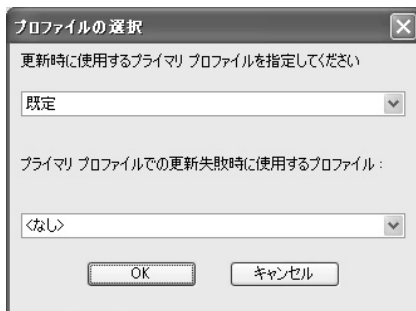
設定の内容が表示されますので、その内容を確認します。設定を確認したら、[完了]をクリックします。



[タスク設定のオプションダイアログを表示する]の項目は、NOD32の更新タスクを設定した場合のみ有効になります。

7

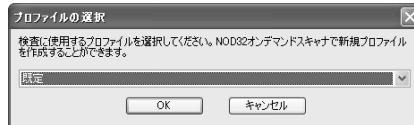
設定したタスクに応じて、最終的な項目を設定します。



NOD32の更新タスクを追加した場合、更新設定で使用するプライマリ プロファイル(優先プロファイル)名と、プライマリ プロファイルでの更新が不可能だった際に使用するプロファイル名を選択します。それぞれの▼をクリックし、選択してください。



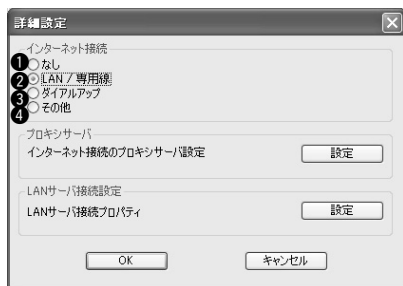
外部プログラムの起動タスクを追加した場合、実行ファイルとその作業フォルダ、コマンドラインを入力します。ファイル横の[参照]をクリックすると、ファイル選択画面が表示されます。作業フォルダ横の[参照]をクリックすると、選択画面が表示されます。



ウイルス検査タスクを追加した場合、ウイルス検査で使用するプロファイル名を選択します。▼をクリックして選択してください。

Step 6

ネットワークに関する設定を行なう



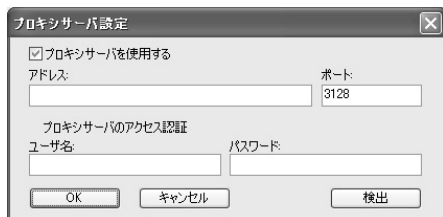
[詳細]ボタンをクリックすると、インターネット接続、プロキシサーバ、LANサーバの設定画面になります。

インターネット接続

お使いのインターネット接続方法を設定します。

| | |
|-------------|--|
| ① なし | インターネットに接続していないときに選択します。 |
| ② LAN / 専用線 | LAN経由または、専用線でインターネットに接続しているときに選択します。 |
| ③ ダイアルアップ | モデムを使ってダイアルアップ接続を使用しているときに選択します。 |
| ④ その他 | 公共の無線LANサービスなど、そのほかの方法でインターネットに接続しているときに選択します。 |

インターネット接続のプロキシサーバ設定

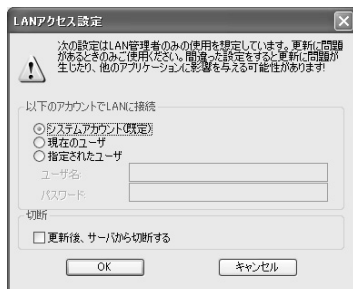


インターネットを利用する際、プロキシサーバを経由しての場合は、[設定]をクリックしてください。プロキシサーバに関する設定を行なう画面が表示されます。[検出]をクリックすると、プロキシサーバの検出を行ないます。

[プロキシサーバを使用]のチェックをオンにすると、各内容が設定可能になります。

LANサーバ接続設定

LAN内のサーバに接続する場合、[設定]をクリックしてください。

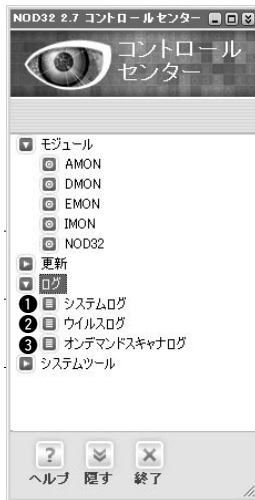


[設定]をクリックすると、左記の画面が表示されます。この設定はLAN管理者向けのもので、通常は設定する必要はありません。間違った設定を行なうと更新に問題が発生することがありますので、ご注意ください。

ログの詳細と設定

NOD32 コントロールセンター

ログの表示方法と項目



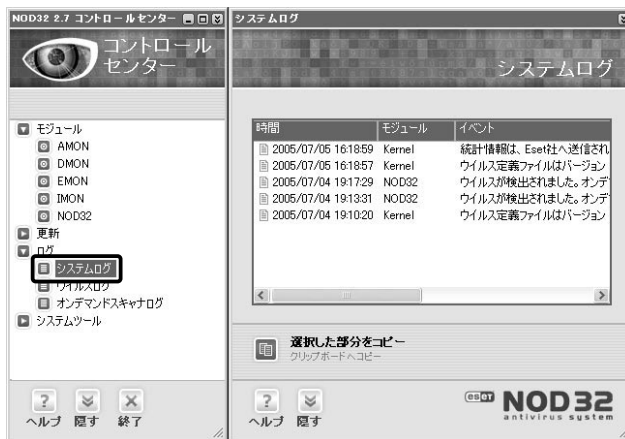
「ログ」の操作画面を表示するには、NOD32 コントロールセンターの [ログ] から、[システムログ]、[ウイルスログ]、[オンデマンドスキャナログ] をクリックしてください。

| | |
|----------------|--|
| ① システムログ | ウイルス定義ファイルの更新状況や、発生したエラーの記録を閲覧表示します。 |
| ② ウイルスログ | AMON、DMON、EMON、IMON におけるウイルス検査の記録を閲覧表示します。 |
| ③ オンデマンドスキャナログ | オンデマンドスキャナの動作記録を閲覧表示します。 |

Chapter 3
NOD32 の
機能詳細

システムログについて

ウイルス定義ファイルの更新状況や、発生したエラーの記録を閲覧表示します。



[選択した部分をコピー] をクリックすると、選択されたログ全体をクリップボードにコピーします。クリップボードにコピーされたログは、エディタなどに貼り付けることができます。



| 時間 | モジュール | イベント |
|---------------------|--------|------------------|
| 2005/07/05 16:18:59 | Kernel | 統計情報は、Eset社へ送信され |
| 2005/07/05 16:18:57 | Kernel | ウイルス定義ファイルはバージョン |
| 2005/07/04 19:17:29 | NOD32 | ウイルスが検出されました。オンデ |
| 2005/07/04 19:13:31 | NOD32 | ウイルスが検出されました。オンデ |
| 2005/07/04 19:10:20 | Kernel | ウイルス定義ファイルはバージョン |

ログをマウスで選ぶと、反転します。複数行を選択する場合は、[Ctrl]キーを押しながらクリックします。[Shift]キーを押しながら矢印キーを押しても複数行のログを選択できます。

ログをマウスで選択し、右クリックするとメニューが表示されます。

| 時間 | モジュール | イベント |
|---------------------|--------|------------------|
| 2005/07/05 16:18:59 | Kernel | 統計情報は、Eset社へ送信され |
| 2005/07/05 16:18:57 | Kernel | ウイルス定義ファイルはバージョン |
| 2005/07/04 19:17:29 | NOD32 | ウイルスが検出されました。オンデ |
| 2005/07/04 19:13:31 | NOD32 | ウイルスが検出されました。オンデ |
| 2005/07/04 19:10:20 | Kernel | ウイルス定義ファイルはバージョン |

[選択した部分をコピー]を選択すると、選択されたログをクリップボードにコピーします。[全てコピー]を選択すると、ログ全体をクリップボードにコピーします。[選択した部分を削除]を選択すると、選択した部分のログを削除します。[ログのクリア]を選択すると、ログ全体をクリアします。

ウイルスログについて

AMON、DMON、EMON、IMONにおけるウイルス検査の記録を閲覧表示します。


| 時間 | モジュール | 対象 | 名前 |
|---------------------|-------|------|--------------|
| 2005/07/04 19:54:18 | AMON | ファイル | C:\#Document |
| 2005/07/04 19:54:10 | IMON | ファイル | http://www0 |
| 2005/07/04 19:17:22 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:17:14 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:17:12 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:17:04 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:58 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:52 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:40 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:37 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:34 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:31 | AMON | ファイル | C:\Temp#\Vir |

[選択した部分をコピー]をクリックすると、選択した部分をクリップボードにコピーします。クリップボードにコピーされたログは、エディタなどに貼り付けることができます。



| 時間 | モジュール | 対象 | 名前 |
|---------------------|-------|------|--------------|
| 2005/07/04 19:54:18 | AMON | ファイル | C:\#Document |
| 2005/07/04 19:54:10 | IMON | ファイル | http://www0 |
| 2005/07/04 19:17:22 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:17:14 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:17:12 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:17:04 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:58 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:52 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:40 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:37 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:34 | AMON | ファイル | C:\Temp#\Vir |
| 2005/07/04 19:16:31 | AMON | ファイル | C:\Temp#\Vir |

ログをマウスで選択し、右クリックするとメニューが表示されます。

| | | |
|----------------------------|---|----------------------------|
| <p>① 詳細</p> |  | <p>選択した行のウイルス情報を表示します。</p> |
| <p>② 選択した部分をコピー</p> | <p>選択して反転した行をクリップボードにコピーします。クリップボードにコピーされたログは、エディタなどに貼り付ける事が可能です。</p> | |
| <p>③ 全てコピー</p> | <p>ログ全体をクリップボードにコピーします。クリップボードにコピーされたログは、エディタなどに貼り付ける事が可能です。</p> | |
| <p>④ 選択した部分を削除</p> | <p>選択した部分のログを削除します。</p> | |
| <p>⑤ ログのクリア</p> | <p>ログ全体をクリアします。</p> | |

Chapter 3
NOD32の
機能詳細

オンデマンドスキャナログについて

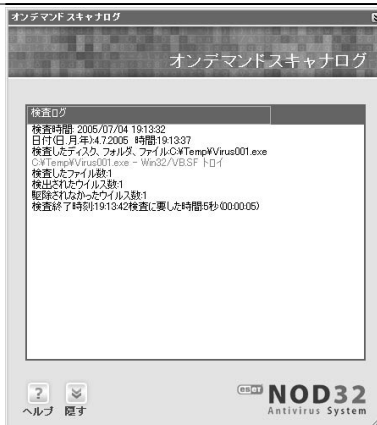


オンデマンドスキャナの動作記録を閲覧表示します。



ログをマウスで選択し、右クリックするとメニューが表示されます。

① 詳細



選択した行のオンデマンドスキャナの詳細ログを表示します。

② 選択した部分を削除

選択した部分のログを削除します。

Column

「ログ」の便利な利用方法

ログに記録されたNOD32の各動作記録は、クリップボードを経由することによりワープロソフトなどで再利用することができます。

1



ログをマウスで選択し、クリップボードにコピーします。

2



スタートメニューから、[すべてのプログラム] [アクセサリ] [メモ帳]でメモ帳を起動します。

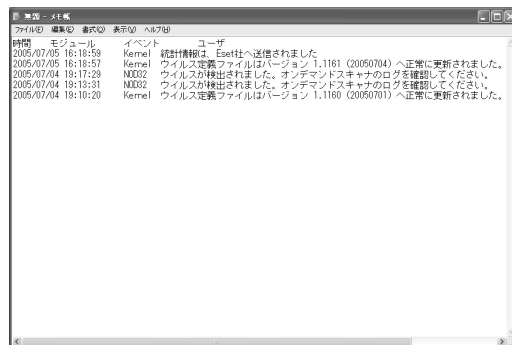
Windows XP/Vista以外のOSでは「プログラム」を選択します。

3



メモ帳のメニューから、[編集] [貼り付け]で、クリップボード上のログを貼り付けます。

4



NOD32のログがメモ帳で編集可能になります。

いったんクリップボードにコピーされたNOD32のログデータは、Wordなどにも同様の手順で貼り付けることができます。

「システムツール」の詳細

NOD32 コントロールセンター

隔離情報について



「隔離情報」はウイルスを隔離した記録を表示します。またすでに隔離したウイルスを削除したり、復元させることも可能です。

「隔離情報」の操作画面を表示するには、NOD32コントロールセンターの[システムツール]から、[隔離情報]をクリックしてください。



隔離されたウイルスをマウスで選択し、右クリックするとメニューが表示されます。

① 追加



任意のファイルを隔離フォルダに追加します。クリックするとファイルを選択するダイアログ画面が表示されるので、追加したいファイルを指定してください。

② 提出

ウイルスに感染したファイルをEset社の早期警告システムに提出します。

早期警告システムについては、108ページの「ThreatSense.NET」を参照してください。

③ 復元

隔離されたウイルスを、ウイルスの検出場所に復元します。ただし、IMONによってメールから隔離されたウイルスの復元はできません。

④ 復元場所

隔離されたウイルスを、任意の場所に復元します。このメニューをクリックすると復元フォルダを指定するダイアログ画面表示されますので、フォルダを指定してください。

⑤ 削除

隔離されたウイルスを削除します。

スケジュールについて

プログラムコンポーネントやウイルス定義ファイルの更新スケジュール、ウイルス検査の実施スケジュール、NOD32から起動する外部プログラムのスケジュールなどを表示・設定します。スケジュールを設定することによって、更新やウイルス検査を自動的に実行できるようになります。

スケジュールの追加は、NOD32コントロールセンターの[更新] [更新]でも設定することが可能です(86ページも併せて参照してください)。

スケジュールの表示方法と設定項目

「スケジュール」を表示するには、NOD32コントロールセンターの[システムツール]から、[スケジュール]をクリックしてください。

②
このチェックボックスをクリックしてオン/オフすることで、一時的にそのスケジュールを有効/無効にすることができます。チェックが付いた状態が有効です。

| 名前 | タスク | モジュール | スケジュール | |
|-------------------------------------|------------|--------------|--------------|--------------|
| <input checked="" type="checkbox"/> | 定期更新... | NOD32更新 | 更新 | 1時間毎に繰り返す |
| <input type="checkbox"/> | ダイヤルアップ... | NOD32更新 | 更新 | インターネットへの接続時 |
| <input type="checkbox"/> | ユーザの... | NOD32更新 | 更新 | その日の初回起動時 |
| <input checked="" type="checkbox"/> | システム... | システム起動時に動... | NOD32 Ker... | その日の初回起動時 |
| <input checked="" type="checkbox"/> | 更新 - N... | NOD32更新 | 更新 | その日の初回起動時 |
| <input checked="" type="checkbox"/> | システム... | システム起動時に動... | NOD32 Ker... | ウイルス定義ファイル |

①
設定されたスケジュールが表示されています。

③ 追加
スケジュールを追加します。スケジュールの追加については、86ページを参照してください。

タスクのスケジュール

指定した時刻や間隔で自動的に実行されるタスクをスケジュールするには、このウィザードを使用してください。

以下のタスクがスケジュールされました。

タスクを選択

< 戻る (B) 次へ (N) > キャンセル

④ 削除
マウスで選んで反転されたスケジュールを削除します。削除確認の画面が表示されますので、[はい]をクリックします。処理を中断する場合は、[いいえ]をクリックします。

nod32kui

本当にこの項目“ダイヤルアップ接続確立後に自動更新”を削除しますか?

はい (Y) いいえ (N)

システム情報について

NOD32のプログラムコンポーネントやウイルス定義ファイルのバージョンを表示します。またコンピュータにインストールされたWindowsやメモリなどの情報も併せて表示します。

情報の表示と設定

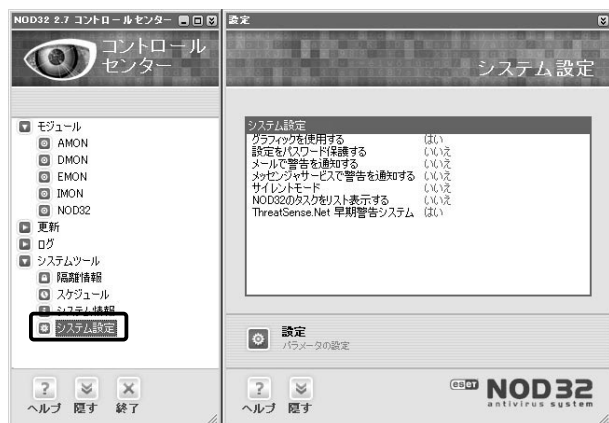


「システム情報」を表示するには、NOD32コントロールセンターの[システムツール]から、[システム情報]をクリックしてください。

システム設定について

NOD32におけるシステム状態表示・設定を行ないます。

システム設定の表示方法と項目



「システム設定」を表示するには、NOD32コントロールセンターの[システムツール]から、[システム設定]をクリックしてください。

[設定]をクリックするとシステム設定画面を表示します。



タブ部（一般 / 通知 / ログの保守 / 詳細 / リモートコントロール / ライセンスキー / ThreatSense.Net）をクリックすると、各設定画面を表示します。各画面で設定を行ない[OK]をクリックすると、設定が有効になり設定画面を終了します。

一般



グラフィック

表示画面に関する設定を行ないます。

[グラフィックモードを有効にする]のチェックをオフにするとNOD32コントロールセンターをノングラフィックモードにします。NOD32の設定値は、グラフィックモードになります。



ノングラフィックモードのNOD32コントロールセンター



[起動時にスプラッシュウィンドウを表示しない]のチェックをオンにするとシステムの起動時に、左の表示をさせらる。

サイレントモード

警告ウィンドウに関する設定を行ないます。

[サイレントモードを有効にする]のチェックをオンにするとNOD32からのメッセージを表示しないようにします。しかしオペレーションが必要なウィンドウや重要なメッセージは表示されます。

パラメータ設定の保護

NOD32コントロールセンターにおける各設定をパスワードで保護します。

[設定]ボタンをクリックすると、パスワード設定画面が表示されます。パスワードを設定する場合は、新規パスワードを入力後、確認のためにもう一度パスワードを入力します。

すでに設定されているパスワードを変更する場合は、以前のパスワードを入力してから新規パスワードを入力し、確認のためにもう一度パスワードを入力します。新規パスワードを入力すると [パスワードなし]が[OK]に変化します。[OK]をクリックすればパスワードが設定されます。すでに設定されているパスワードを無効(パスワードの保護無し)にする場合は、以前のパスワードを入力し、[パスワードなし]をクリックしてください。[キャンセル]で処理を終了します。



caution

ここで設定したパスワードを忘れると、NOD32のアンインストールもできなくなります。

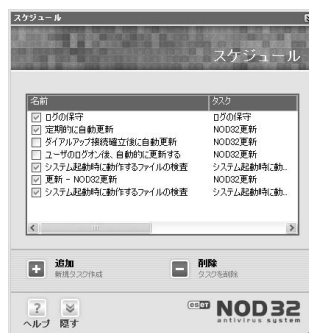
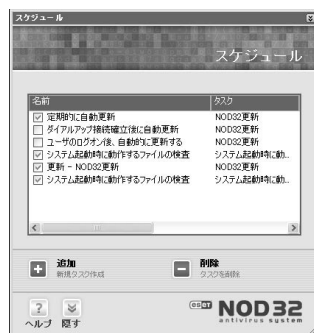
既定のタスク

[既定のタスクの表示を有効にする]のチェックをオンにすると、スケジュール設定画面で、NOD32の動作に必須となっている既定のタスクを表示し、既定のタスクに対して設定変更を行えます。



caution

既定のタスクは、不用意に設定変更を行うと、NOD32の動作に深刻な影響を及ぼします。そのため、既定値ではチェックはオフになっています。ネットワーク管理者などが特別な設定を行う場合などを除き、既定値のままお使いください。



通知


ウイルスを検出した時に電子メールやメッセンジャサービスで、システム管理者にウイルス検出の事実を自動的に通知することができます。



ここで明記している「メッセンジャサービス」とは、“自動的に通知するサービス”のことであり、MSN メッセンジャーのことではありません。用語解説の「メッセンジャサービス」(12 ページ)と併せてご確認ください。

メール

メールでウイルスの検出を通知するときに設定します。
[メールで通知する]のチェックをオンにすると、他の項目を入力できるようになります。

| | |
|-----------------------------------|--|
| SMTPサーバ | <p>メール送信を行なうSMTPサーバを入力します (例 smtp.aaabbb.co.jp)</p> <p> 「POP After send」形式のSMTPサーバは指定できません。 「Outbound Port 25 Blocking」には対応しておりません。</p> |
| 送信元アドレス | 警告メッセージを送信する元のメールアドレスを入力します。 |
| ウイルス警告送信先 | ウイルスを検出した際に送信される警告メールの送信先メールアドレスを入力します。 |
| 他の警告送信先 | エラー等、ウイルス検出警告以外の警告メールの送信先、メールアドレスを入力します。 |
| SMTPサーバーへアクセスする際のユーザ名、パスワード (必要時) | SMTPサーバが認証を必要とする場合、ユーザ名とパスワードを入力します。(SMTP AUTH LOGIN にのみ対応しております) |

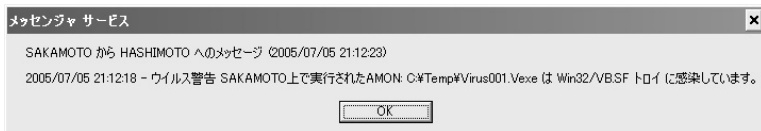
メッセンジャサービス

メッセンジャサービス

 LAN内のコンピュータに警告を通知する
 次のコンピュータに通知する

Windowsのメッセンジャサービスでウイルスの検出を通知するときに設定します。[LAN内のコンピュータに警告を通知する]のチェックをオンにする

と、他の項目を入力できるようになります。「次のコンピュータに通知する」の欄には、Windowsのメッセンジャサービスでメッセージを送信するコンピュータ名を入力します。コンピュータ名は、マイクロソフトネットワークで使用される名前です。



ウイルスを検出すると、左のようなメッセージがLAN内の他のコンピュータ上で表示されるようになります。



メッセンジャの通知は、Messengerサービスが利用可能なOSでのみ使用できます。

詳細

詳細

メールまたはメッセンジャサービスでの通知設定

設定

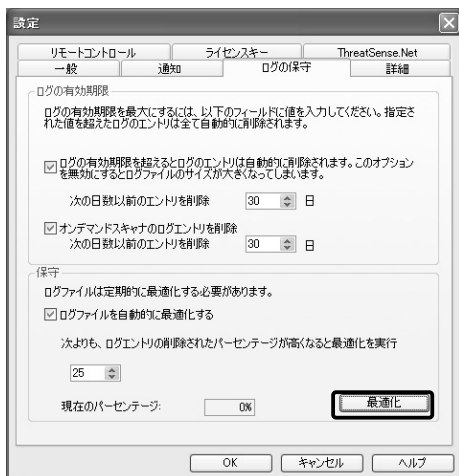


[設定]をクリックすると、メールやメッセンジャサービスの詳しい内容を設定する画面が表示されます。[メールでの言語サポート]は日本語でお使いの場合、[iso-2022-jpでエンコードする]をオンにしてください。[OK]をクリックすると、設定が有効になります。[キャンセル]は処理を中断します。[既定]をクリックすると、設定内容を既定値に戻します。



「%」で囲まれた文字列は予約語ですので、この部分は編集しないことを推奨します。

ログの保守



ログファイルのサイズを調節するなど、ログファイルの自動メンテナンスに関する設定を行ないます。

この画面から最適化を行なうこともできます。その際は各種設定を施してから[最適化]をクリックします。[最適化]をクリックすると、手動でログの最適化を行なうことができます。

ログの有効期限

[ログの有効期限を越えると~]のチェックをオンにすると、「次の日数以前のエンTRIESを削除」に設定した日数以前のログを自動的に削除し、ログファイルの大きさを一定に保つことができます。



caution

この項目をオフにすると、ログファイルが削除されないためファイル容量が増大し、HDDを圧迫することがあります。

「次の日数以前のエンTRIESを削除」では、ログエンTRIESを削除する日数を設定してください。

[オンデマンドスキャナのログエンTRIESを削除]のチェックをオンにすると、[次の日数以前のエンTRIESを削除]に設定した日数以前のオンデマンドスキャナのログを自動的に削除し、ログファイルの大きさを一定の状態に保つことができます。

「次の日数以前のエンTRIESを削除」では、オンデマンドスキャナのログエンTRIESを削除する日数を設定してください。

保守

ログファイルは定期的に最適化する必要があります。最適化とは、削除されたエンTRIESを持つログファイルを整形する処理です。最適化することで、ログファイルのサイズをより小さくすることができます。

[ログファイルを自動的に最適化する]のチェックをオンにすると、ログファイルを自動的に最適化します。この項目はオンでお使いください。この項目がオンの時、「次よりも、ログエントリの削除されたパーセンテージが高くなると最適化を実行」で最適化するタイミングを設定してください。

「次よりも、ログエントリの削除されたパーセンテージが高くなると最適化を実行」では、削除されたログエントリが、この設定以上のパーセンテージを占めるようになると、最適化を行いません。

「現在のパーセンテージ」では、削除されたログエントリが、ログファイル上に占めるパーセンテージを表示しています。

詳細



その他の項目を設定します。

自動的にウィンドウを閉じる

[自動的にメッセージウィンドウを閉じる]のチェックをオンにすると、NOD32からのメッセージウィンドウ（オペレーションを必要としないメッセージウィンドウ）が、[自動的にウィンドウを閉じる]で設定した秒数の間表示された後、自動的に閉じます。

ターミナルサーバ / XP ユーザ切り替え

ターミナルサーバとして動作している場合、システムレポートをユーザー権限で表示します（Windows 98 / Me では利用できません）。

隔離情報

ウイルス警告ウィンドウなどで「隔離」するときの、隔離先フォルダを設定します。[参照]をクリックすると、フォルダツリー表示画面になりますので、フォルダを選択する事ができます。

アンチステルス技術を有効

ステルス技術を使ってコンピュータに身を潜めるルートキットの検出を行いません。



この機能は、Windows 98 / Me では動作しません。

リモートコントロール

NOD32をリモートコントロールサーバ経由で使用するときを設定します。通常、この設定を変更する必要はありません。



リモートコントロールサーバに接続する場合は、[リモートコントロールサーバへ接続する]のチェックをオンにします。

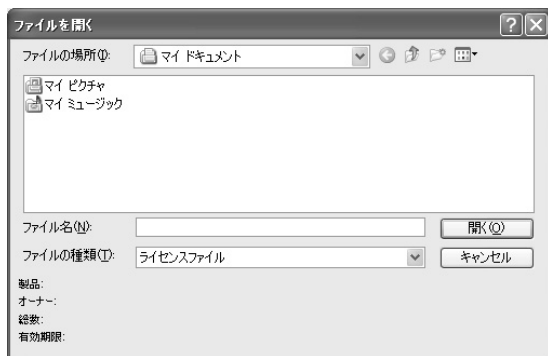
オンにすると、[サーバアドレス]、[ポート]、[サーバへの接続間隔(分)]が入力可能になりますので、設定してください。

ライセンスキー



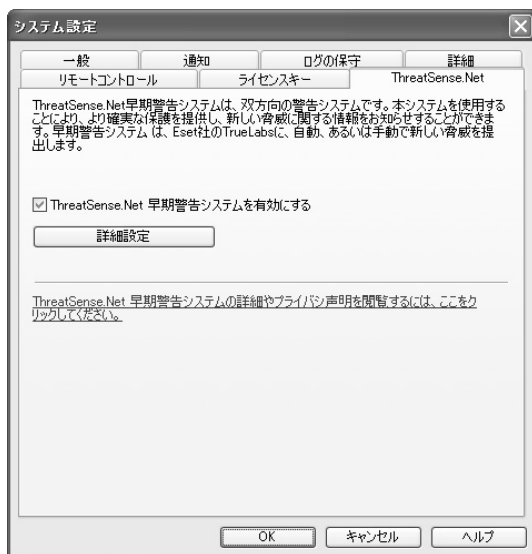
NOD32のライセンスキーを記録したファイルの管理を行いません。

なお、ライセンスキーファイルが提供されないライセンス形態の場合は、この画面での操作を行なう必要はありません。



[追加]ボタンをクリックすると、ライセンスファイルの追加を行うダイアログ画面が表示されるので、適切なファイルを選択してください。ダイアログ画面では、ライセンスファイルに記録された製品やオーナー、有効期限などの情報が確認できます。

ThreatSense.Net



Eset社の「ThreatSense.Net」(早期警告システム)へのファイル提出に関する設定を行いません。

早期警告システムとは、ユーザーのNOD32で新種のウイルス(定義ファイルにデータの無いウイルス)として疑わしいファイルが発見された際に、ファイルを自動的にEset社に提出する機能です。

早期警告システムの機能を使うには、「ThreatSense.Net 早期警告システムを有効にする」のチェックをオンにし、[OK]ボタンをクリックします。

[詳細設定]ボタンをクリックすると、早期警告システムの詳細設定画面が表示されます。

詳細設定画面は、3つのタブシートから構成されています。

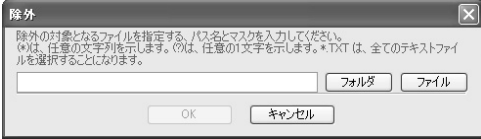



早期警告システムを利用したEset社へのファイル提出は、早期対応をお約束するものではありません。

疑わしいファイル



疑わしいファイルが発見された際の動作と、早期警告システムに送信する際の設定を行ないます。

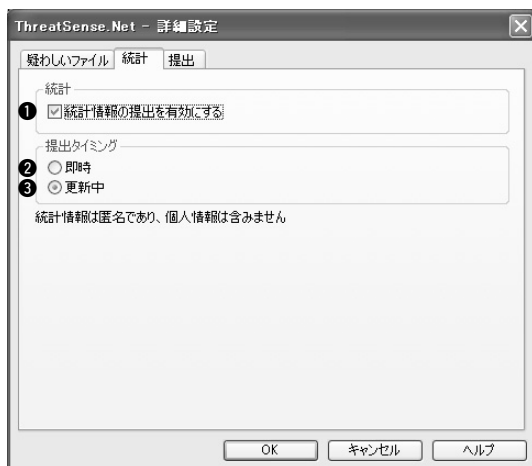
| | |
|-------------|--|
| ① 提出しない | 疑わしいファイルが発見されても、提出を行いません。 |
| ② 提出前に通知する | 疑わしいファイルが発見された時点で、ユーザーに提出の可否を求めるダイアログ画面を表示します。 |
| ③ 提出前に通知しない | 疑わしいファイルが発見されたら、ユーザーに問い合わせを行わず、自動的に提出を行ないます。 |
| ④ 即時 | 疑わしいファイルが発見された時点で、すぐに提出を行ないます。 |
| ⑤ 更新中 | 疑わしいファイルが発見された時点では提出せず、NOD32の更新に合わせて提出を行ないます。 |
| ⑥ 除外フィルタ | <p>感染が疑わしい場合でも、提出を行なわない(提出条件より除外する)ファイルの条件を設定します。各種の文書ファイルやユーザーの作成したデータファイルを除外することにより、データの漏洩を防ぐための機能です。既定値では、代表的なデータファイルの拡張子が設定されています。</p>  <p>[追加]をクリックすると、除外対象となるフォルダパスやファイル名を追加できます。</p> |
| ⑦ メール | <p>ファイルと同時に送信元のメールアドレスを送る場合に、入力します。</p>  <p>メールアドレスの入力は任意です。入力しない場合も、正常に動作します。また、このメールアドレスは、解析情報の連絡を約束するものではありません。</p> |

統計

ウイルス感染の統計情報の提出に関する設定を行ないます。



統計情報は匿名で送信され、個人情報に含まれません。



| | |
|-----------------|-------------------------------------|
| ① 統計情報の提出を有効にする | チェックをオンにすると、早期警告システムへ統計情報の提出を行ないます。 |
| ② 即時 | 統計情報が収集された時点で、すぐに提出を行ないます。 |
| ③ 更新中 | 収集時点では提出せず、NOD32の更新に合わせて提出を行ないます。 |

提出

早期警告システムへの提出を行ないます。



| | |
|---------------|--|
| ① 今すぐ提出 | このボタンをクリックすると、早期警告システムへの疑わしいファイルや統計情報の提出を即時に実行します。 |
| ② データの送信を記録する | チェックをオンにすると、データの提出をログファイルに記録します。 |

Chapter 4

よくある質問

ここでは、想定される質問に対してお答えしています。サポートセンターなどへ連絡される際は、まずこちらの章をチェックしてみてください。

Chapter 4
よくある
質問

ウイルス定義ファイルの更新について

Q
A

ウイルス定義ファイルとはなんですか？

ウイルスの特徴を記録したデータベースです。ウイルスが発見されると、そのウイルスがNOD32の開発チームにより解析され、特徴や検出方法がウイルス定義ファイルに登録されます。ウイルス定義ファイルに登録されたウイルスは、後のウイルス検査で使用されます。NOD32はインターネットを利用して更新し、ウイルス定義ファイルを最新のものに保つことができます。既知のウイルスに対して有効で、ウイルス名の定義に必要です。

Q
A

更新を行うと、ユーザ名とパスワードを求めるダイアログが表示されます。

設定されているユーザ名やパスワードが違う場合に、このダイアログが表示されます。ダイアログで正しいユーザ名とパスワードを入力しますと更新は可能ですが、入力した情報は保存されません。下記のように設定を変更してください。

「更新設定」画面を表示します。

この画面の表示方法は、82ページをご参照ください。

「ユーザ名」「パスワード」欄に現在入力されている内容を削除し、正しいユーザ名とパスワードを入力しなおします。

「OK」ボタンをクリックしてください。

Q
A

更新を行うと「サーバ接続に失敗しました。」と表示されます。

このエラーは、お客様のPCがNOD32アンチウイルスの更新サーバに接続できないときに表示されます。接続できない主な理由として、下記が考えられますのでご確認ください。

- ・ NOD32の更新はインターネット経由で行われます。WEBブラウザでホームページの閲覧や電子メールの送受信が可能かご確認ください。
- ・ ファイアウォールソフトの設定でNOD32アンチウイルスの通信を許可されていないことが考えられます。

ファイアウォールソフトがインストールされている場合は、ファイアウォールソフトの遮断した履歴にNOD32 アンチウイルスが含まれていないかご確認ください。

- ・更新サーバへの接続がプロキシ設定の有無によって失敗する場合があります。プロキシサーバの設定方法につきましては、90ページをご参照ください。

検査について

Q

NOD32の「駆除」と「削除」はどちらがうのですか？

A

「駆除」とは、ウイルスに感染したファイルからウイルスを除去して、正常な状態（ファイル）へ戻す処置です。「削除」とは、ウイルスやウイルスに感染したファイル自体を削除します。ウイルスの種類によって、「駆除」が可能なものと不可能なものが存在し、ウイルスを「駆除」できないケースでは「削除」を行なう必要があります。

Q

「隔離」とは、どういうことですか？

A

ウイルス検出の警告ウィンドウなどで表示される「隔離」とは、ウイルスに対して「削除」や「駆除」を行なうことと並行し、そのウイルスを隔離フォルダにコピーする処理です。後にウイルスを解析するなど、何らかの理由でウイルスを保存する必要があるときに実施してください。

Q

ヒューリスティックとは何ですか？

A

ウイルスと思われるモジュールを仮想的なコンピュータの中で動作させる仕組みです。これは新種のウイルスに対して有効な手法で、NOD32独自のエンジンを採用しています。その動作を監視することにより、ウイルスであるかどうかを判断します。このヒューリスティック解析により、ウイルス定義ファイルに記録されていない新種のウイルスを検出する事ができるようになります。

Q

オンデマンドスキャナでの検査時に「pagefile.sys - ファイルを開く時にエラーが発生しました」と表示されます。

A

この表示は、NOD32の異常な動作を示すものではありません。「pagefile.sys」は仮想メモリ技法を実現するためのスワップファイルです。Windowsのシステムが排他的に利用しているファイルですので、他のアプリケーションから開くことができず、このようなエラーメッセージが表示されます。

Q

「デフォルトのメールクライアントが設定されていないか、現在のメール・・・」と表示されます。

A

このメッセージは、Microsoft Outlookがインストールされている環境で、デフォルトのメールクライアントにMicrosoft Outlook以外をご使用の場合に表示されます。下記のように設定を変更してください。

表示されたダイアログは「OK」を選択し、ウィンドウを閉じます。

「オンデマンドスキャナ」を起動します。

オンデマンドスキャナの起動方法は、30ページをご参照ください。

「設定」タブを選択し、「MAPIインターフェイスを使用する」のチェックを外します。

「プロファイル」タブをクリックし、別のプロファイルを選択し、同様に設定を行ないます。

別のプロファイルを選択した際、保存するかどうかの確認ダイアログが表示されますので、「はい」を選択します。

全プロファイルの設定後、「終了」を選択します。



- ・「MAPIインターフェイスを使用する」のチェックボックスは、オンデマンドスキャナでの検査に対してのみ有効です。このチェックボックスを外しても、POP3メール受信時のウイルス検査は行なわれず。
- ・NOD32メニュー内の「フロッピーの簡易検査」、「ディスクの簡易検査」については、上記設定を行なった後も、ダイアログが表示されます。

Q

オンデマンドスキャナ起動時に、下記のエラーが表示されます。

物理ディスク 1. の有効なブートセクタを検査中にエラーが発生しました。セクタ読み込みエラー

物理ディスク 2. のMBRを検査中にエラーが発生しました。セクタ読み込みエラー

A

このエラーは、物理ディスクのセクタにエラーが発生している場合だけでなく、以下の環境においても出力されることがあります。

メモリスティック、スマートメディアなど、メディアを読み書きするためのインターフェイス（リーダ/ライター）がPCに接続されており、このインターフェイスにメディアが挿入されていない。

この場合、当該メッセージが表示されても、お客様のPCに問題が発生しているということではありません。

Q

「C:¥System Volume Information¥_restore{xxx}¥RPxxx」内に検出されたウイルスの駆除・削除ができない。

A

「C:¥System Volume Information¥_restore{xxx}¥RPxxx」は、Windows の「システムの復元」機能がバックアップしたファイルです。一時的に「システムの復元」を無効にして、ウイルスが検出される復元ポイントを破棄してください。

「マイコンピュータ」を右クリックし、「プロパティ」を選択します。

「システム復元」タブを選択します。

「システムの復元を無効にする」にチェックを入れます。

「適用」をクリックし、「OK」をクリックします。

念のため、復元ポイント破棄後に、ローカルドライブのウイルス検査を行なうことをお勧めします。

Q

「Temporary Internet Files」内に検出されたウイルスの駆除・削除ができない。

A

「Temporary Internet Files」は、Microsoft Internet Explorer の一時ファイル(キャッシュ)が保存されています。お手数ですが下記の手順を参考に、一時ファイルを削除してください。

Microsoft Internet Explorer（以下、IE）を開き、「ツール」「インターネットオプション」と選択します。

IE6の場合は「全般」タブの[インターネット一時ファイル]内にある「ファイルの削除」をクリックします。

IE7の場合は「全般」タブの[閲覧の履歴]内にある「削除」をクリックします。「閲覧の履歴の削除」画面が表示されますので、「ファイルの削除」をクリックします。

IE6の場合は「[Temporary Internet Files]フォルダのすべてのファイルを削除しますか?」と表示されますので、「すべてのオフラインコンテンツを削除する」にチェックを入れて「OK」をクリックします。

IE7の場合は「ファイルの削除」確認画面が表示されますので、「はい」をクリックします。IE7の場合は以上で終了です。

IE6の場合は「適用」をクリックし、「OK」をクリックします。

Q
A

メール受信時に、ウイルスを自動的に駆除もしくは削除するには？

下記のように設定を変更してください。

「IMON設定」画面を表示します。

この画面の表示方法は、61ページをご参照ください。

[詳細]タブをクリックし、「設定」ボタンをクリックします。

[アクション]タブをクリックします。

プルダウンメニュー内の全ての項目について、以下のように設定します。

ウイルス検出時：駆除

駆除されなかった場合：削除、隔離

各項目にチェックを入れ、「OK」ボタンをクリックします。

「OK」ボタンをクリックし、表示されているダイアログを順に閉じます。

Q
A

検査スケジュールを駆除モードで実行するには？

検査スケジュールに使用するプロファイルを以下のように設定する事で、駆除モードで実行可能です。

「オンデマンドスキャナ」を起動し、[プロファイル]タブをクリックします。

オンデマンドスキャナの起動方法は、30ページをご参照ください。

プルダウンメニューより、検査スケジュールに使用するプロファイルを選択します。

選択したプロファイルの[駆除]モード時にこのプロファイルを使用する]にチェックを

入れます。

プロファイルを保存します。

81ページの [2] ~ [3] をご参照ください。

その他

Q
A

Q NOD32は他のウイルス対策ソフトと併用できますか？

A できません。ウイルス対策ソフトはウイルスを検出するために、Windowsと非常に密接な状態を作り出します。このような状態で複数のウイルス対策ソフトが動作していると、コンピュータが正常に動作しないことがあります。NOD32だけをインストールして、お使いください。

Q
A

Q 「潜在的に不要なアプリケーションの検出」は有効にする必要がありますか？

A 「潜在的に不要なアプリケーションの検出」の、検出対象となるプログラムは、実質的に危険ではないプログラムです。この機能は次の方法でシステムの動作に影響を与える可能性があるものに対して検出します。また、これらのプログラムはインストールする前にユーザーの同意を必要とします。

- a) 通常では開かないウィンドウを表示する
- b) ユーザーには見えないプロセスを起動して実行する
- c) システムリソースの消費を拡大する
- d) 検索結果を変更する
- e) アプリケーション プロバイダサーバーと通信する

これらの該当するアプリケーションに対して、「安全である」と判断または利用規約などで「同意した」上でご利用を続ける場合は、無効に設定してください。

Chapter 5

サポートについて

ここでは、キヤノンシステムソリューションズ サポートセンターについて紹介しています。

サポートについて

お問い合わせ

本ユーザーズガイド、ヘルプ、ホームページ等をご覧いただいても問題が解決しなかった場合は、キヤノンシステムソリューションズサポートセンターまでご相談ください。ご相談は、電話やFAX、電子メールにて受け付けております。

なお、下記につきましてはサポートをいたしかねる場合がございますので予めご了承ください。

- ・ユーザー登録をお済ませでない方
- ・動作保証外、サポート対象外の環境でご使用のお問い合わせ
- ・お客様の故意や改造等による紛失、不具合の発生、破壊等によるサポート
- ・訪問、出張が伴うサポート
- ・弊社休業日、受付時間外でのサポート
- ・FAXまたは電子メールでお問い合わせいただいた際、必要な内容が書かれていない場合
- ・法的な不正やライセンス契約内容に違反する事実が判明した場合

ホームページURL <http://canon-sol.jp/>

電話でのお問い合わせ先：キヤノンシステムソリューションズ サポートセンター

TEL：03 - 5730-7197 受付時間：月曜日～金曜日（祝祭日、夏季・年末年始等の休業日を除く）
10：00～12：00、13：00～17：00

日時によっては混み合っている場合がございます。その際は、誠に恐れ入りますが時間を改めてお掛け直しいただけますようお願いいたします。

FAXでのお問い合わせ先：キヤノンシステムソリューションズ サポートセンター

FAX：03 - 5730-7122

電子メールでのお問い合わせ先：キヤノンシステムソリューションズ サポートセンター

NOD32係 電子メールアドレス：nod-info@canon-sol.co.jp

お問い合わせにはできるだけ迅速に対応いたしますが、お問い合わせの内容によっては、弊社または開発元での動作検証が必要になる場合がございます。このような場合には、返信にかなりのお時間をいただく場合がございます。予めご了承くださいませようお願い申し上げます。

ユーザー登録のお願い

サポートや今後の最新情報をお受けいただくには、ユーザー登録が必要です。

同梱の「ユーザー登録について」をご参照の上、お早めに弊社ホームページからオンラインにてご登録ください。

お問い合わせシート

NOD32インストールCD内に、「techsupp.txt」というファイルがあります。電子メールやFAXでお問い合わせする際、ご利用ください。

製品情報シート

製品ご利用の際に必要な、シリアル番号、ユーザ名、パスワードは大切な情報ですので、取得後はこちらに記載して保管することをお勧めします。

製品名

NOD32 アンチウイルス

シリアル番号

[例：JP99-ab1cd2ef3]

シリアル番号はパッケージに同梱の「シリアル番号のご案内」用紙に記載されています。
更新パック、5ライセンス専用更新パックをご購入のお客様はお持ちのシリアル番号を記入してください。

ユーザ名

[例：AV-1234567]

ユーザ名とパスワードは、ユーザー登録後にメールにて配信されます。

パスワード

[例：abcde2f3g4]

更新有効期限

年 月 日

備考