ESET NOD32アンチウイルス
Mac OS X/Linux 用
ユーザーズマニュアル

目次

■本書について

○本書は、ESETセキュリティ ソフトウェア シリーズ ライセンス製品の共通ガイドとしてまとめています。

○文中に設けているアイコンは、該当するプログラムを示しています。「ESET Endpoint Security」は  アイコン、「ESET Endpoint アンチウイルス」はアイコン、「ESET File Security for Microsoft Windows Server」はアイコン、「ESET NOD32アンチウイルス」はアイコンです。

■お断り

○本書は、本書作成時のソフトウェアおよびハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェア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、改訂などにより予告なく変更することがあります。

[Chapter 1]
ESET NOD32 アンチウイルス

1.1 ESET NOD32アンチウイルスとは

Unixベースのオペレーティングシステムを使用するユーザーが増えた結果、悪意のある人間によってMac/Linuxユーザーをターゲットにした脅威が開発され続けています。ESET NOD32アンチウイルスは脅威に対して強力かつ効率的な保護機能を提供します。ESET NOD32アンチウイルスにはWindowsの脅威を回避する機能が搭載されており、Windowsユーザーとやり取りする際にMac/Linuxユーザーを保護します(逆の場合も同様です)。WindowsのマルウェアはMac/Linuxに対する直接的な脅威にはなりませんが、Mac/Linuxに感染したマルウェアを無効にすることで、ローカルネットワークまたはインターネットを介してWindowsベースのコンピューターに脅威が拡散する問題を回避できます。

[Chapter 2]
インストール

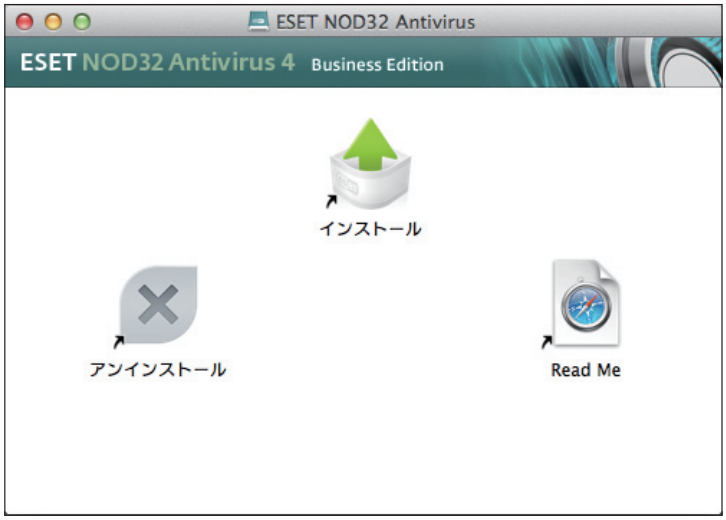
2.1 インストールについて

インストール処理を開始する前に、コンピューター上に開いているすべてのプログラムを閉じてください。ESET NOD32アンチウイルスには、すでにコンピューターにインストールされている他のウイルス対策プログラムと競合する可能性のあるコンポーネントが含まれています。ESETは、問題の生じる可能性をなくすため、他のウイルス対策プログラムを削除することを強く推奨します。Mac/Linux用のESET NOD32アンチウイルスは、インストールCDまたはWebページで入手できるファイルを使用してインストールできます。

2.1.1 Macにインストールするには

インストールウィザードを実行するには、次のいずれかを実行します。

●インストールCDを使用してインストールする場合、CD-ROMドライブにインストールCDを挿入すると、メニュー画面が表示されます。ESET NOD32アンチウイルスインストールアイコンをダブルクリックして、インストーラを起動します。
●ダウンロードしたファイルを使用してインストールする場合は、そのファイルをダブルクリックすると、インストーラーが起動します。



インストーラーを起動すると、インストールウィザードが表示されるので、その案内に従って基本設定を行ってください。使用許諾契約書に同意した後、インストールの種類を以下から選択することができます。

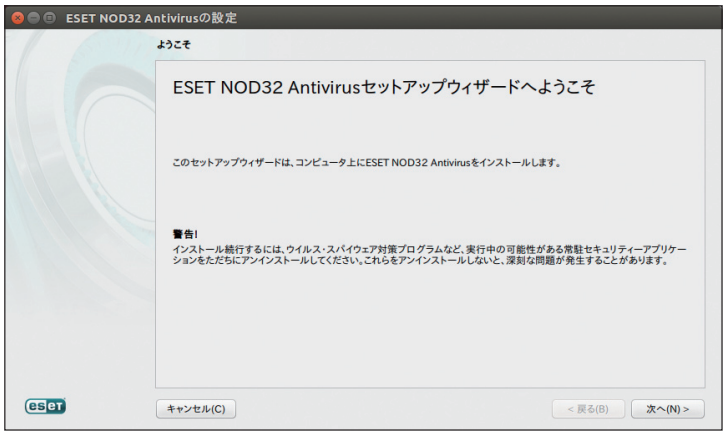
●標準インストール　12ページ
●カスタムインストール　14ページ
●リモートインストール　17ページ

2.1.2 Linuxにインストールするには

Linuxでインストールウィザードを実行するには、次のいずれかを実行します。また、ESET NOD32アンチウイルスのインストールには、root権限（スーパーユーザー）で作業する必要があります。

●インストールCDを使用してインストールする場合は、ESET NOD32アンチウイルスインストールアイコンをダブルクリックしてインストーラーを起動します。

●ダウンロードしたファイルを使用してインストールする場合は、そのファイルをダブルクリックすると、インストーラーが起動します。



インストールCDを使用した場合、またダウンロードをしたファイルを使用した場合ともに、インストーラー起動時にRootパスワードの入力画面が表示される場合があります。この画面が表示されたときは、rootパスワードを入力し、[OK] をクリックすると、インストーラーが起動します。

正しいパスワードを入力してもrootパスワードの認証に失敗するときは、ターミナル（端末）を開き、コマンドラインを使ってroot権限を取得してインストーラーを起動してください。たとえば、Ubuntuを使用している場合は、以下のように入力します。

```
$sudo / インストーラーの保存フォルダ名 / ファイル名
```

実行例

インストーラーが「/tmp」に保存されており、ファイル名が「ueavbe.x86_64.ja.linux」である場合は、以下のように入力します。

```
$sudo /tmp/ueavbe.x86_64.ja.linux
```

また、ダウンロードしたファイルをダブルクリックしてもインストーラーが起動しなかったときは、ファイルのアクセス権を変更してください。アクセス権の変更は、インストーラーを右クリックし、表示されるメニューから［プロパティ］をクリックして、プロパティ画面を表示します。［アクセス権］をクリックし、［プログラムとして実行可能］のチェックをオンにして、［閉じる］をクリックすることで行えます。

インストーラーが起動すると、インストールウィザードが表示されます。［次へ］をクリックすると、インストールのタイプを「ESET NOD32 Antivirusのインストール」と「ESET NOD32 Antivirusのリモートインストールを用意する（詳細は18ページを参照）の中から選択できます。

また、インストールの種類を選択した後、インストールウィザードの案内に従って作業を行い、使用許諾契約書に同意すると、インストールの種類を以下から選択できます。

●標準インストール　　13ページ
●カスタムインストール　15ページ
●リモートインストール　18ページ
※インストール後に、権限の設定をする必要があるため、インストール時に権限の設定ができるカスタムインストールを行うことを推奨します。

2.1.3　64bit版のLinuxにインストールする場合の注意点

64bit版LinuxにESET NOD32アンチウイルスをインストールする場合、以下のような依存性の欠如エラーが表示され、インストールできないことがあります。このエラーは32bitのglibcがインストールされていない場合に表示されます。この画面が表示されたときは、必要なパッケージをインストールしてから再度インストールを実行してください。なお、Linuxのインストール時に「互換性ライブラリ」のパッケージを選択することでも、32bitのglibcがインストールされます。

2.2 標準インストール

標準インストールには、ほとんどのユーザーが利用できる構成オプションが用意されています。この設定は最大限のセキュリティと共に優れたシステムパフォーマンスを実現します。標準インストールは既定のオプションで、固有の設定に対して特定の要件を必要としない限り推奨されます。

2.2.1 Macの場合

[一般(推奨する最適な設定)]インストールモードを選択すると、プログラムの自動アップデートを有効にするためにユーザー名とパスワードの入力を求められます。プログラムの自動アップデートは、継続してシステムを保護する上で重要な役割を果たします。[ユーザー名]および[パスワード]フィールドに、製品の購入後または登録後に受け取った認証データーを入力します。現在、使用可能なユーザー名とパスワードがない場合は、[アップデートパラメーターを後から設定する]オプションを選択し、インストールを続行します。ユーザー名とパスワードは、インストール完了後に設定することもできます。

ThreatSense.Net早期警告システムによって、ESETは新しいマルウェアを迅速かつ継続的に把握し、コンピューターをすばやく保護することができます。ESETのウイルスラボに新しい脅威が提出されると、これらが解析および処理され、ウイルス定義データベースに追加されます。既定では、[ThreatSense.Net早期警告システムを有効にする]オプションが選択されています。疑わしいファイルの提出に関する詳細設定を変更するには、[設定...]をクリックします。(詳細については、「ThreatSense.Net」を参照してください)。

インストールプロセスの次のステップでは、望ましくない可能性があるアプリケーションの検出を設定します。潜在的に望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。これらのアプリケーションは、その他のプログラムに同梱されていることが多く、インストールプロセス時に気が付きにくいことがあります。これらのアプリケーションはインストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。ESET NOD32アンチウイルスでこのような脅威を検出できるようにする(推奨)には、[望ましくない可能性があるアプリケーションの検出を有効にする]オプションを選択します。このオプションを有効にしない場合は、[望ましくない可能性があるアプリケーションの検出を無効にする]オプションを選択します。
標準インストールの最後のステップでは、[インストール]ボタンをクリックしてインストールを確認します。

2.2.1 Linuxの場合

[一般(推奨する最適な設定)]インストールモードを選択すると、プログラムの自動アップデートを有効にするためにユーザー名とパスワードの入力を求められます。プログラムの自動アップデートは、継続してシステムを保護する上で重要な役割を果たします。[ユーザー名]および[パスワード]フィールドに、製品の購入後または登録後に受け取った認証データーを入力します。現在、使用可能なユーザー名とパスワードがない場合は、[次へ]をクリックし、インストールを続行します。ユーザー名とパスワードは、インストール完了後に設定することもできます。

ThreatSense.Net早期警告システムによって、ESETは新しいマルウェアを迅速かつ継続的に把握し、コンピューターをすばやく保護することができます。ESETのウイルスラボに新しい脅威が提出されると、これらが解析および処理され、ウイルス定義データベースに追加されます。既定では、[ThreatSense.Net早期警告システムを有効にする]オプションが選択されています。疑わしいファイルの提出に関する詳細設定を変更するには、[設定...]をクリックします。(詳細については、「ThreatSense.Net」を参照してください)。

インストールプロセスの次のステップでは、望ましくない可能性があるアプリケーションの検出を設定します。潜在的に望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。これらのアプリケーションは、その他のプログラムに同梱されていることが多く、インストールプロセス時に気が付きにくいことがあります。これらのアプリケーションはインストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。ESET NOD32アンチウイルスでこのような脅威を検出できるようにする(推奨)には、[望ましくない可能性があるアプリケーションの検出を有効にする]オプションを選択します。このオプションを有効にしない場合は、[望ましくない可能性があるアプリケーションの検出を無効にする]オプションを選択します。
標準インストールの最後のステップでは、[インストール]をクリックしてインストールを確認します。

2.3 カスタムインストール

カスタムインストールは、経験豊富なユーザーがインストールプロセス時に詳細な設定を変更できるように用意されています。

2.3.1 Macの場合

[カスタム] インストールモードを選択した後は、[ユーザー名] と [パスワード] (製品の購入または登録後に受け取った認証データ) を入力する必要があります。現在、使用可能なユーザー名とパスワードがない場合は、[アップデートパラメーターを後から設定する] オプションを選択し、インストールを続行します。ユーザー名とパスワードは、インストール完了後に設定することもできます。

プロキシサーバーを使用している場合は、[プロキシサーバーを使用する] オプションを選択することによって、パラメーターを定義できます。[アドレス] フィールドにプロキシサーバーのIPアドレスまたはURLを入力します。[ポート] フィールドには、プロキシサーバーが接続を受け付けるポートを指定します (既定では3128です)。プロキシサーバーで認証が要求される場合は、有効な [ユーザー名] と [パスワード] を入力して、プロキシサーバーへのアクセスを可能にする必要があります。プロキシサーバーを使用していないことがわかっている場合は、[プロキシサーバーを使用しない] オプションを選択します。不明な場合は、[システム設定と同じ設定を使用する (推奨)] を選択すると、現在のシステム設定を使用できます。

ESET NOD32アンチウイルスをESET Remote Administrator (ERA) で管理する場合は、ERA Serverパラメーター (サーバー名、ポート、およびパスワード) を設定すると、インストール後にESET NOD32アンチウイルスはERA Serverに自動的に接続されます。

次のステップでは、プログラム設定を編集できる [権限ユーザーの定義] を設定します。左側のユーザー一覧からユーザーを選択し、[追加] をクリックして [権限ユーザー] の一覧に追加します。全てのシステムユーザーを表示するには、[全ユーザーを表示] オプションを選択します。

ThreatSense.Net早期警告システムによって、ESETは新しいマルウェアを迅速かつ継続的に把握し、コンピューターをすばやく保護することができます。ESETのウイルスラボに新しい脅威が提出されると、これらが解析および処理され、ウイルス定義データベースに追加されます。既定では、[ThreatSense.Net早期警告システムを有効にする] オプションが選択されています。疑わしいファイルの提出に関する詳細設定を変更するには、[設定...] をクリックします。詳細については、「ThreatSense.Net」を参照してください。

インストールプロセスの次のステップでは、望ましくない可能性があるアプリケーションの検出を設定します。潜在的に望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。これらのアプリケーションは、その他のプログラムに同梱されていることが多く、インストールプロセス時に気付きにくいことがあります。これらのアプリケーションはインストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。

ESET NOD32アンチウイルスでこのような脅威を検出できるようにする（推奨）には、[望ましくない可能性があるアプリケーションの検出を有効にする] オプションを選択します。

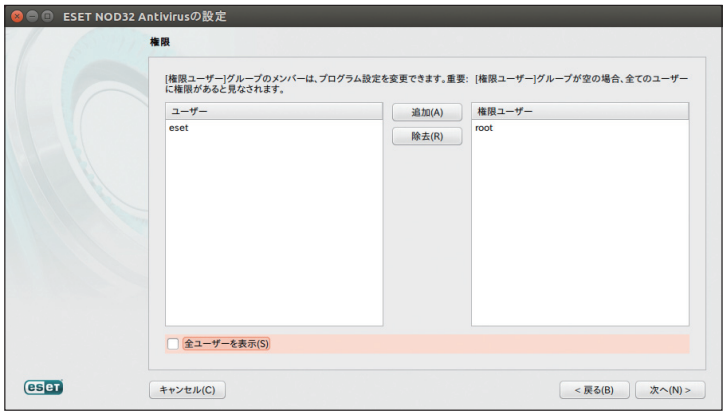
2.3.2 Linuxの場合

[カスタム] インストールモードを選択した後は、[ユーザー名] と [パスワード]（製品の購入または登録後に受け取った認証データ）を入力する必要があります。現在、使用可能なユーザー名とパスワードがない場合は、[次へ] をクリックし、インストールを続行します。ユーザー名とパスワードは、インストール完了後に設定することもできます。

プロキシサーバーを使用している場合は、[プロキシサーバーを使用する] オプションを選択することによって、パラメーターを定義できます。[アドレス] フィールドにプロキシサーバーのIPアドレスまたはURLを入力します。[ポート] フィールドには、プロキシサーバーが接続を受け付けるポートを指定します（既定では3128です）。プロキシサーバーで認証が要求される場合は、有効な [ユーザー名] と [パスワード] を入力して、プロキシサーバーへのアクセスを可能にする必要があります。プロキシサーバーを使用していないことがわかっている場合は、[プロキシサーバーを使用しない] オプションを選択します。

次のステップでは、リモート管理の設定を行います。ESET NOD32アンチウイルスをESET Remote Administrator（ERA）で管理する場合は、ERA Serverパラメーター（サーバー名、ポート、およびパスワード）を設定すると、インストール後にESET NOD32アンチウイルスはERA Serverに自動的に接続されます。

次のステップでは、プログラム設定を編集できる [権限ユーザーの定義] を設定します。権限ユーザーを追加するには、左側のユーザー一覧からユーザーを選択し、[追加] をクリックして [権限ユーザー] の一覧に追加します。全てのシステムユーザーを表示するには、[全ユーザーを表示] オプションを選択します。既定値では、「root」のみが権限ユーザーに設定されており、他のユーザーは、root権限を取得しない限り、ESET NOD32アンチウイルスの各種設定を行うことはできません。一般のユーザーが、ESET NOD32アンチウイルスの各種設定を変更できるようにするには、ここで設定を行ってください。



ThreatSense.Net早期警告システムによって、ESETは新しいマルウェアを迅速かつ継続的に把握し、コンピューターをすばやく保護することができます。ESETのウイルスラボに新しい脅威が提出されると、これらが解析および処理され、ウイルス定義データベースに追加されます。既定では、[ThreatSense.Net早期警告システムを有効にする] オプションが選択されています。疑わしいファイルの提出に関する詳細設定を変更するには、[設定...] をクリックします。詳細については、「ThreatSense.Net」を参照してください。

インストールプロセスの次のステップでは、望ましくない可能性があるアプリケーションの検出を設定します。潜在的に望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォー

マンスに悪影響を及ぼす可能性があります。これらのアプリケーションは、その他のプログラムに同梱されていることが多く、インストールプロセス時に気付きにくいことがあります。これらのアプリケーションはインストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。ESET NOD32アンチウイルスでこのような脅威を検出できるようにする（推奨）には、[望ましくない可能性があるアプリケーションの検出を有効にする] オプションを選択し、[次へ] をクリックします。

すべての設定を終えると、最終ステップの画面が表示されます。[インストール] をクリックすると、ESET NOD32アンチウイルスのインストールが実行されます。

2.4 リモートインストール

Mac/Linuxともに [リモート] インストールモードを使用すると、ターゲットコンピューターにリモートインストールできるインストールパッケージを作成できます。

リモートインストールは次の2つの段階で実行されます。

1. ESETインストーラーによるリモートインストールパッケージの作成　17ページ
2. ターゲットコンピューターへのリモートインストール　19ページ

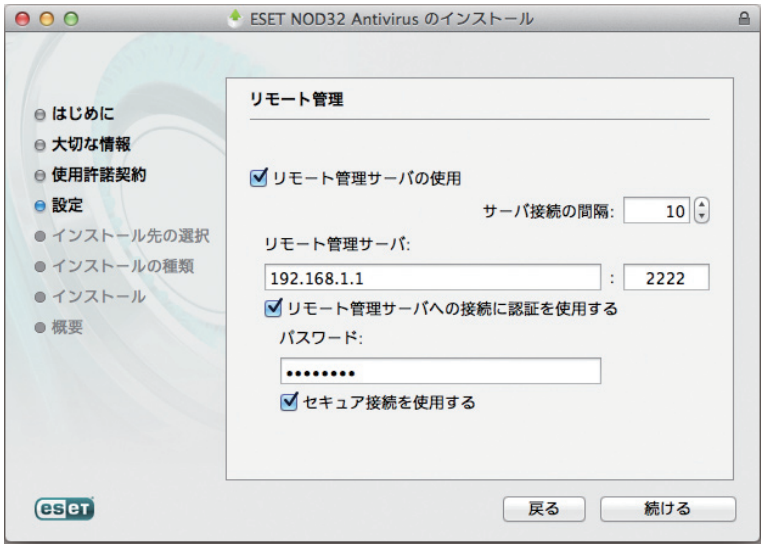
2.4.1 リモートインストールパッケージの作成

ESETインストーラーを利用したリモートインストールパッケージの作成は、以下の手順で行えます。

2.4.1.1 Macの場合

[リモート] インストールモードを選択すると、ESET NOD32アンチウイルスのウイルス定義データベースアップデートを有効にするためにユーザー名とパスワードの入力を求められます。[ユーザー名] および [パスワード] フィールドに、製品の購入後または登録後に受け取った認証データを入力します。現在、使用可能なユーザー名とパスワードがない場合は、[アップデートパラメーターを後から設定する] オプションを選択し、インストールを続行します。ユーザー名とパスワードは、インストール完了後に設定することもできます。

次のステップでは、インターネット接続を設定します。プロキシサーバーを使用している場合は、[プロキシサーバーを使用する] オプションを選択することによって、パラメーターを定義できます。プロキシサーバーを使用していないことがわかっている場合は、[プロキシサーバーを使用しない] オプションを選択できます。不明な場合は、[システム設定を使用] を選択して、現在のシステム設定を使用できます。



リモート管理サーバーのパラメーター(サーバー名、ポート、およびパスワード) を設定すると、インストール後にESET NOD32アンチウイルスはESET Remote Administrator Serverに自動的に接続されます。

次のステップでは、プログラム設定を編集できる[権限ユーザーの定義]を設定します。左側のユーザー一覧からユーザーを選択し、[追加]をクリックして[権限ユーザー]の一覧に追加します。全てのシステムユーザーを表示するには、[全ユーザーを表示]オプションを選択します。

ThreatSense.Net早期警告システムによって、ESETは新しいウイルスを迅速かつ継続的に把握し、コンピューターをすばやく保護することができます。ESETのウイルスラボに新しい脅威が提出されると、これらが解析および処理され、ウイルス定義データベースに追加されます。既定では、[ThreatSense.Net早期警告システムを有効にする]オプションが選択されています。疑わしいファイルの提出に関する詳細設定を変更するには、[設定...]をクリックします。詳細については、「ThreatSense.Net」を参照してください。

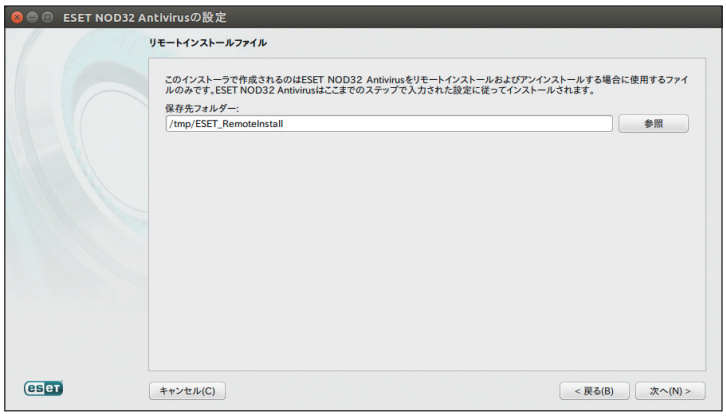
インストールプロセスの次のステップでは、望ましくない可能性があるアプリケーションの検出を設定します。潜在的に望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。これらのアプリケーションは、その他のプログラムに同梱されていることが多く、インストールプロセス時に気付きにくいことがあります。これらのアプリケーションはインストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。ESET NOD32アンチウイルスでこのような脅威を検出できるようにする(推奨)には、[望ましくない可能性があるアプリケーションの検出を有効にする]オプションを選択します。

インストールウィザードの最後の手順では、保存フォルダーを選択し、[保存]をクリックします。ESETインストーラーによってインストールパッケージ(EAV4_Remote_Install.pkg)とアンインストールシェルスクリプト(EAV4_Remote_UnInstall.sh)が作成されます。

2.4.1.2 Linuxの場合

[リモート]インストールモードを選択した後、インストールウィザードの案内に従って作業を行い、使用許諾契約書に同意すると、「標準インストール」または「カスタムインストール」の中からインストールの種類を選択できます。

標準インストールを選択したときは、13ページを参考に各種設定を行います。カスタムインストールを選択したときは、15ページを参考に各種設定を行います。いずれの場合もインストールウィザードの案内に従ってすべての設定を終えると、インストールパッケージの保存先を選択する画面が表示されます。保存先フォルダーを選択し、[保存]します。次の画面で[作成]をクリックすると、ESETインストーラーによってrpmパッケージ(32bit版の場合は、「lsb-esets.i386.rpm」、64bit版の場合は「lsb-eset.x86_64.rpm)と.linuxファイル(32bit版の場合は、「lsb-esets.i386.linux」、64bit版の場合は「lsb-eset.x86_64.linux)の2種類のファイルが作成されます。



2.4.2 ターゲットコンピューターへのリモートインストール

ターゲットコンピューターへのリモートインストールは、以下の方法で行います。

2.4.2.1 Macの場合

ESET NOD32アンチウイルスは、Apple Remote Desktopまたは標準のMacパッケージ(.pkg)のインストールをサポートする他のツールを使用して、ターゲットコンピューターにインストールすることができます。ターゲットコンピューターにファイルがコピーされ、シェルスクリプトが実行されます。

Apple Remote Desktopを使用してESET NOD32アンチウイルスをインストールするには、[パッケージのインストール...] コマンドを実行し、EAV4_Remote_Install.pkgファイルを選択し、[インストール] をクリックします。

ESET Remote Administratorを使用してクライアントコンピューターを管理する詳細な手順については、「ESET Remote Administrator ユーザーズマニュアル」を参照してください。

2.4.2.2 Linuxの場合

ESET NOD32アンチウイルスのリモートインストールは、ターミナルウィンドウを開き、コマンドラインで「Secure Copy(SCP)」または「Secure Shell(SSH)」を利用して行います。ESET NOD32アンチウイルスのリモートインストールを行うターゲットコンピューターは、sshによるリモート接続が行えるように設定されている必要があります。インストールパッケージのターゲットコンピューターへのコピーは、SCPを利用します。ターミナルから以下のように入力することでインストールパッケージをコピーできます。インストールパッケージをターゲットコンピューターにコピーしたら、ESET NOD32アンチウイルスのインストールを行ってください。

```
$scp インストールパッケージ名 user@host:/ コピー先フォルダー名
```

実行例

インストールパッケージ名が「lsb-eset.x86_64.linux」、ターゲットコンピューターのユーザー名が「user」、IPアドレスが「192.168.1.11」、コピー先フォルダー名が「/tmp」である場合は、以下のように入力します。

```
$scp lsb-eset.x86_64.linux user@192.168.1.11:/tmp
```

2.4.3 リモートアンインストール

クライアントコンピューターからMac用のESET NOD32アンチウイルスをアンインストールするには、

1. Apple Remote Desktopで [アイテムのコピー...] を使用して、インストールパッケージと共に作成されアンインストールシェルスクリプト(EAV4_Remote_UnInstall.sh)を選択し、シェルスクリプトをターゲットコンピューターにコピーします。
2. Apple Remote Desktopで [Unixコマンドの送信...] を実行します。アンインストールが完了すると、コンソールログが表示されます。

2.4.4 リモートアップグレード

Mac用のESET NOD32アンチウイルスのリモートアップグレードは、Apple Remote Desktopで [パッケージのインストール...] コマンドで実行します。

NOTE

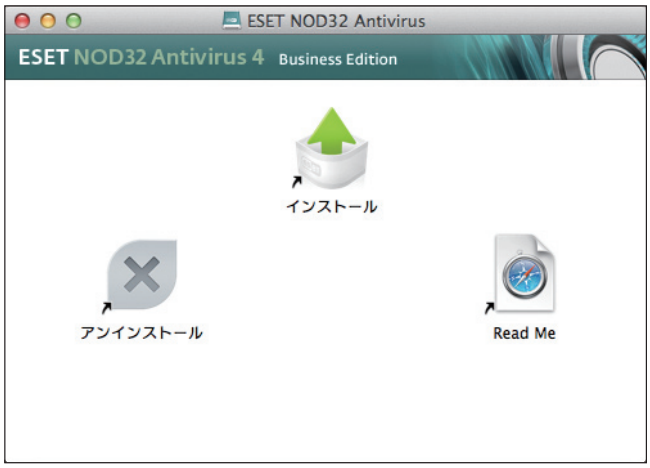
Mac用のESETリモートインストールパッケージに保存されている設定は、アップグレードプロセス時にターゲットコンピューターには適用されません。アップグレード後に、ESET Remote Administratorを使用してESET NOD32アンチウイルスをリモートで設定する必要があります。

2.5 アンインストール

ESET NOD32アンチウイルスのアンインストールは、以下の方法で行います。

2.5.1 Macの場合

Mac版のESET NOD32アンチウイルスは、インストーラーとアンインストーラーは同じファイルです。インストーラーを起動し、「アンインストール」をダブルクリックするとインストールウィザードが起動します。インストールウィザードの案内に従って作業を行います。



2.5.2 Linuxの場合

Linux版のESET NOD32アンチウイルスは、インストーラーとアンインストーラーが同じファイルです。ESET NOD32アンチウイルスがインストールされたコンピューターでインストーラーを起動すると、アンインストールウィザードが起動します。アンインストールウィザードの案内に従って作業を行います。なお、アンインストールは、root権限（スーパーユーザー）で作業する必要があります。

Linux版のESET NOD32アンチウイルスは、以下のファイルをroot権限（スーパーユーザー）で実行することでもアンインストールを行えます。たとえば、Ubuntuを使用している場合は、ターミナルを開き、コマンドラインで以下のように入力します。

実行ファイル

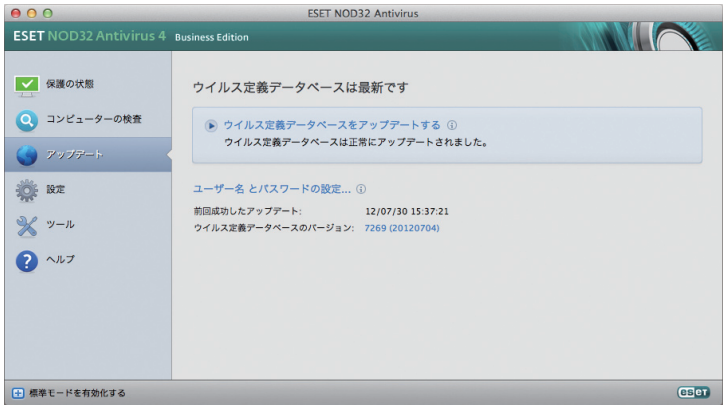
```
/opt/eset/esets/bin/esets_gil
```

実行例

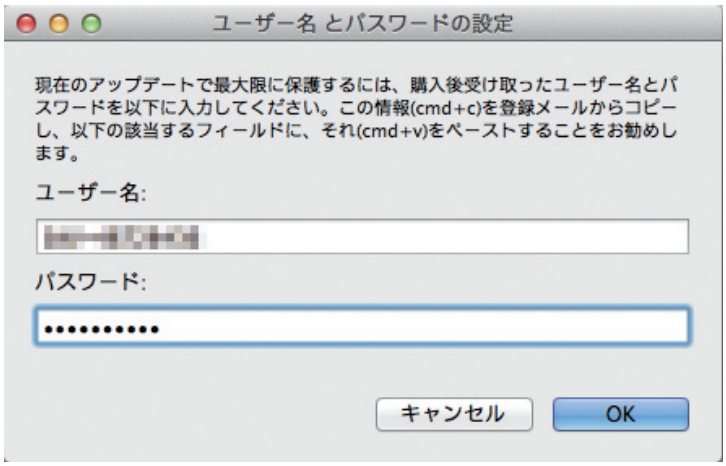
```
$sudo /opt/eset/esets/bin/esets_gil
```

2.6 ユーザー名とパスワードの入力

最適な動作を確保するには、ウイルス定義データベースのアップデートが自動的に行われるように設定することが重要です。
ウイルス定義データベースのアップデートには、認証データ（ユーザー名とパスワード）を登録するアップデートの設定を行う必要があります。アップデートの設定は、基本画面を開き、メインメニューの［アップデート］>［ユーザー名とパスワードの設定］をクリックします。



「ユーザー名とパスワードの設定」ダイアログが表示されたら、ユーザー名とパスワードを入力します。設定を行ったら、［ウイルス定義データベースをアップデートする］をクリックしてアップデートが完了することを必ず確認してください。
なお、ユーザー名とパスワードは、弊社ユーザーズサイトで確認できます。詳細は、「ESETライセンス製品 ご利用の手引」をご参照ください。

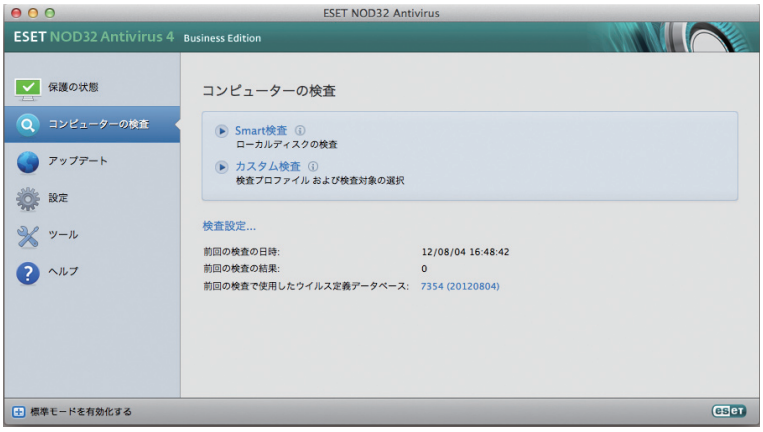


NOTE

ESET NOD32アンチウイルスは、権限ユーザー（51ページ参照）に登録されたユーザーのみがユーザー名とパスワードの入力を行えます。Linux版の既定値では、「root（スーパーユーザー」）のみが権限ユーザーに登録されており、他のユーザーは、登録されていません。ユーザー名とパスワードの登録画面が開けないときは、基本画面をroot権限（スーパーユーザー）で起動し、各種設定を行ってください。詳細については、28ページをご参照ください。

2.7 コンピューターの検査

ESET NOD32アンチウイルスのインストール後は、悪意のあるコードを見つけるためにコンピューターの検査を実行する必要があります。そのために、基本画面から［コンピュータの検査］をクリックし、［Smart検査］をクリックします。コンピューターの検査の詳細については、「コンピューターの検査」を参照してください。



[Chapter 3]
初心者向けガイド

3.1 ユーザーインターフェースのデザインの概要 - モード

ESET NOD32アンチウイルスの基本画面は、2つのセクションに分かれています。右のプライマリウィンドウには、左のメインメニューで選択したオプションに対応する情報が表示されます。
次に、メインメニューにあるオプションについて説明します。

保護の状態	ESET NOD32アンチウイルスの保護の状態に関する情報が表示されます。[詳細モード]を有効にすると、[統計]サブメニューが表示されます。
コンピュータの検査	このオプションを使用すると、[コンピュータの検査]の設定や起動を行うことができます。
更新(アップデート)	ウイルス定義データベースのアップデートに関する情報が表示されます。
設定	このオプションを選択すると、コンピューターのセキュリティレベルを調整することができます。[詳細モード]を有効にすると、[ウイルス・スパイウェア対策]サブメニューが表示されます。
ツール	[ログファイル] [隔離]および[スケジューラ]にアクセスできます。このオプションは[詳細モード]の場合にのみ表示されます。
ヘルプ	プログラム情報が表示され、ヘルプファイル、インターネットのナレッジベース、および製品Webサイトにアクセスできます。

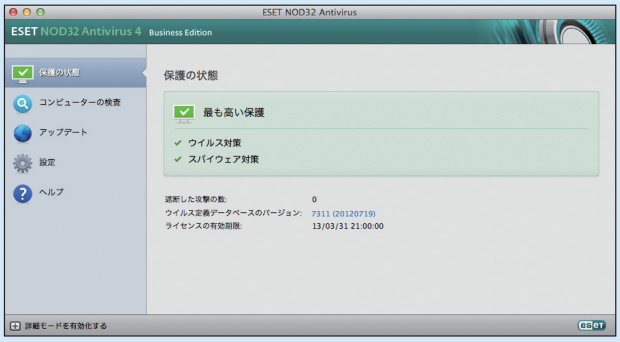
ESET NOD32アンチウイルスのユーザーインタフェースでは、標準モードと詳細モードを切り替えることができます。標準モードでは、一般的な操作に必要な機能にアクセスすることができます。詳細オプションは表示されません。モードを切り替えるには、基本画面の左下にある [詳細モードを有効にする] / [標準モードを有効にする] の横のプラスアイコンをクリックします。

標準モードでは、一般的な操作に必要な機能にアクセスすることができます。詳細オプションは表示されません。

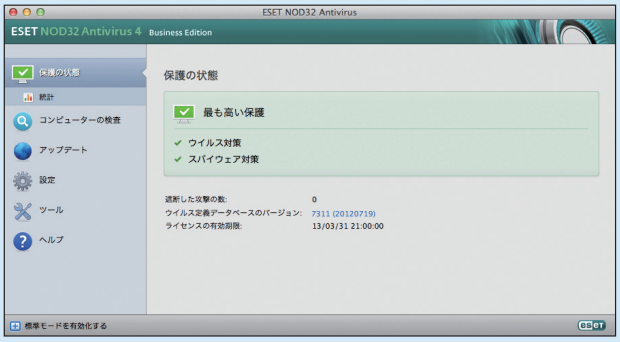
詳細モードに切り替えると、[ツール] オプションがメインメニューに追加されます。[ツール] オプションを使用すると、[ログファイル] [隔離]、および [スケジューラ] のサブメニューにアクセスできます。

▸▸▸ NOTE

このガイドの残りの説明は、[詳細モード] を用いています。



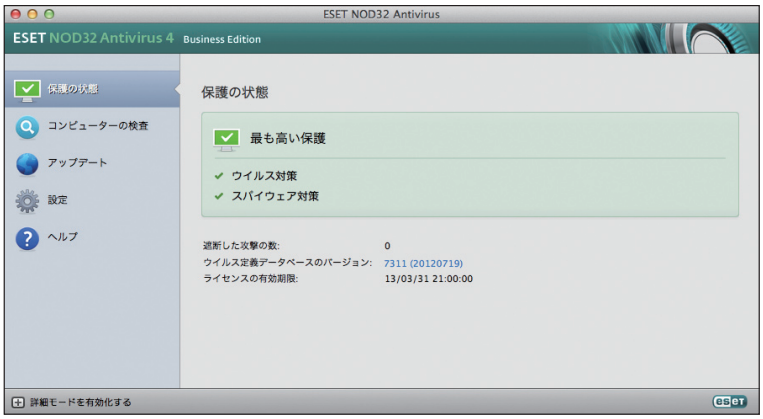
標準モード



詳細モード

3.1.1 システムの動作の確認

[保護の状態] を表示するには、メインメニューの一番上のオプションをクリックします。プライマリウィンドウにはESET NOD32アンチウイルスの動作状態の概要と [統計] などのサブメニューが表示されます。[統計] を選択すると、システムで実行されたコンピューターの検査に関する詳細な情報と統計が表示されます。[統計] ウィンドウは詳細モードの場合にのみ使用できます。



3.1.2 プログラムが正しく動作しない場合の解決方法

有効なモジュールが正しく動作している場合は、緑のチェックアイコンが表示されます。正しく動作していない場合は、赤またはオレンジの通知アイコンが表示され、詳細情報がウィンドウの上部に表示されます。モジュールを修正するための推奨される解決策も表示されます。各モジュールのステータスを変更するには、メインメニューの [設定] をクリックし、必要なモジュールをクリックします。

解決策を使用して問題を解決できない場合は、[ヘルプ] をクリックしてヘルプファイルにアクセスするか、ナレッジベースを検索してください。

サポートが必要な場合は、サポートセンターにお問い合わせください。お客様のご質問に迅速に回答し、解決のお手伝いをいたします。

NOTE

サポートセンターへの問い合わせ窓口は「ESETライセンス製品 ご利用の手引」をご参照ください。

3.1.3 Linux版利用時の注意点

ESET NOD32アンチウイルスは、権限ユーザー（51ページ参照）に登録されたユーザーのみが基本画面から各種設定を行えます。権限ユーザー以外のユーザーは、一部の設定を変更できません。Linux版の規定値では、「root（スーパーユーザー」）のみが権限ユーザーに登録されており、他のユーザーは登録されていません。
他のユーザーを権限ユーザーに登録するには、次の２つの方法があります。

●基本画面から設定を行う方法
●コマンドラインから権限を追加する方法

基本画面から設定を行う場合

51ページの手順を参照してください。
また、基本画面をroot権限（スーパーユーザー）で起動したいときは、以下のファイルを実行します。例えば、Ubuntuを使用している場合は、ターミナルを開き、コマンドラインで以下のように入力します。

実行ファイル

```
/opt/eset/esets/bin/esets_gui
```

実行例

```
$sudo /opt/eset/esets/bin/esets_gui
```

コマンドプロンプトから権限を追加する方法

下記のコマンドを実行後、OSを再起動してください。

実行例

```
$sudo /opt/eset/esets/sbin/esets_set --set 'privileged_users ="username:root"'
```

実行例（複数のユーザを追加する場合）

```
$sudo /opt/eset/esets/sbin/esets_set --set 'privileged_users ="username1:username2:root"'
```

username, username1,2の部分はお使いの環境に合わせて変更してください。
複数追加する場合は、":"で区切り追加することが可能です。

[Chapter 4]
使用方法：ESET NOD32 アンチウイルス

4.1 ウイルス・スパイウェア対策

ウイルス·スパイウェア対策は、潜在的な脅威を与えるファイルを修正することによって、悪意のあるシステム攻撃を防御する機能です。悪意のあるコードを含むウイルスが検出されると、ウイルス対策機能がブロックし、次に駆除、削除、または移動して隔離することにより、ウイルスを排除できます。

4.1.1 リアルタイムファイルシステム保護

リアルタイムファイルシステム保護では、システムで発生する、ウイルスが関係するイベントを全て検査します。リアルタイムファイルシステム保護はファイルがコンピューター上で開かれるとき、作成されるとき、または実行されるときに、悪意のあるコードがないか検査します。リアルタイムファイルシステム保護は、システム起動時に開始されます。

4.1.1.1 リアルタイム保護の設定

リアルタイムファイルシステム保護では、あらゆる種類のメディアを調べます。検査はさまざまなイベントで実行されます。ThreatSenseテクノロジーの検出方法（詳細は「ThreatSenseエンジンのパラメーターの設定」のセクションを参照）を使用するリアルタイムファイルシステム保護は、新規作成ファイルと既存ファイルで動作が異なることがあります。新規作成ファイルの場合、よりレベルの高い検査を行います。

既定では、リアルタイム保護はシステム起動時に起動し、中断されることなく検査が行われます。他製品と競合する場合など特殊な場合は、メニューバー（画面最上部）のESET NOD32アンチウイルスアイコンをクリックし、[リアルタイムファイルシステム保護を無効にする] オプションを選択して、リアルタイム保護を終了することができます（Mac版のみ）。リアルタイム保護はメインウィンドウから終了することもできます（[設定] > [ウイルス·スパイウェア対策] > [無効]）。

リアルタイム保護の詳細設定を変更するには、[設定] > [詳細設定を表示する...] > [保護] > [リアルタイム保護] に移動して、[詳細設定オプション] の横にある [設定...] ボタンをクリックします（「詳細検査オプション」セクションを参照）。

検査のタイミング（イベント発生時の検査）

既定では、ファイルを開くときファイルを作成するとき、またはファイルを実行するときに検査されます。既定の設定によりコンピューターが最大限のレベルでリアルタイムに保護されるので、既定の設定を変更しないことをお勧めします。

詳細検査オプション

このウィンドウでは、ThreatSenseエンジンによる検査の対象にするオブジェクトの種類を定義し、アドバンスドヒューリスティックを有効化/無効化できます。アーカイブおよびファイルキャッシュの設定を変更することもできます。

アーカイブネストの値を大きくするとシステムのパフォーマンスが低下する場合があるため、特定の問題を解決するために必要でない場合を除き、[既定のアーカイブ設定] セクションの既定値を変更しないことをお勧めします。

作成したファイルおよび変更したファイルだけでなく、実行したファイルに対してもThreatSenseアドバンスドヒューリスティック検査のオンとオフを切り替えることができます。この切り替えを行うには、個々のThreatSenseパラメーターセクションで [アドバンスドヒューリスティック] チェックボックスをクリックします。

リアルタイム保護を使用する際に、最適化キャッシュのサイズを定義し、システムフットプリントを最小化することができます。この動作は、[未感染ファイルをキャッシュ] オプションが有効の場合にアクティブになります。このオプションが無効の場合、全てのファイルがアクセスのたびに検査されます。定義したキャッシュのサイズに達するまで、キャッシュされたファイルが繰り返し検査されることはありません(ファイルが変更されている場合は除く)。ウイルス定義データベースがアップデートされると、直ちにファイルが再検査されます。

このオプションを有効化/無効化するには、[未感染ファイルをキャッシュ] をクリックします。キャッシュされるファイルの容量を設定するには、[キャッシュサイズ] の横の入力フィールドに値を入力します。

[ThreatSenseエンジンの設定] ウィンドウでその他の検査パラメーターを設定できます。リアルタイムのファイルシステム保護に関しては、検査対象のオブジェクトの種類をオプションと駆除レベルの組み合わせで定義できます。また、検査対象に課す制限を拡張子とファイルサイズで定義することもできます。ThreatSenseエンジンの設定ウィンドウを表示するには、[詳細設定] ウィンドウで [ThreatSenseエンジン] の横にある [設定...] ボタンをクリックします。

検査からの除外

このセクションでは、特定のファイルやフォルダーを検査から除外することができます。

パス	除外されるファイルやフォルダーのパスです。
脅威	除外されるファイルの横に脅威の名前がある場合、ファイルは特定の脅威に対してのみ除外され、完全には除外されません。したがって、このファイルが後で他のマルウェアに感染した場合は、ウイルス対策機能によって検出されます。
追加...	オブジェクトを検出対象外にします。対象のパスを入力するか(ワイルドカード*および?を使用できます)、ツリー構造でフォルダーまたはファイルを選択します。
編集...	選択したエントリーを編集します。
削除	選択したエントリーを削除します。
既定	全ての除外対象を取り消します。

4.1.1.2 リアルタイム保護の設定の変更

リアルタイム保護は、安全なシステムを維持するために最も必要不可欠な要素です。リアルタイム保護パラメーターを変更する場合は、注意が必要です。特定の状況に限ってパラメーターを変更することをお勧めします。たとえば、特定のアプリケーションとの競合がある場合などです。

ESET NOD32アンチウイルスのインストール後は、最大レベルのシステムセキュリティをユーザーに提供するように全ての設定が最適化されています。既定の設定に戻すには、[リアルタイム保護] ウィンドウ ([設定] > [アプリケーションの設定を入力する...] > [保護] > [リアルタイム保護]) の左下にある [既定] ボタンをクリックします。

4.1.1.3 リアルタイム保護の確認

リアルタイム保護が機能しており、ウイルスを検出することを確認するため、eicar.comのテストファイルを使用します。このテストファイルは、あらゆるウイルス対策プログラムで検出できる特殊な無害のファイルです。このファイルは、EICAR（European Institute for Computer Antivirus Research）が、ウイルス対策プログラムの機能をテストする目的で作成しました。ファイルeicar.comは、http://www.eicar.org/anti_virus_test_file.htmからダウンロードできます。

4.1.1.4 リアルタイム保護が機能しない場合の解決方法

この章では、リアルタイム保護使用時に発生することがあるトラブル、およびその解決方法について説明します。

リアルタイム保護が無効である

ユーザーが不注意にリアルタイム保護を無効にしてしまった場合は、再開する必要があります。リアルタイム保護を再開するには、[設定] > [ウイルス・スパイウェア対策] に移動し、基本画面の [リアルタイムファイルシステム保護を有効にする] リンク（右側）をクリックします。リアルタイムファイルシステム保護を有効にする別の方法として、[詳細設定] ウィンドウの [保護] > [リアルタイム保護] で、[リアルタイムファイルシステム保護を有効にする] オプションを選択する方法もあります。

リアルタイム保護がマルウェアの検出と駆除を行わない

コンピューターに他のウイルス対策プログラムがインストールされていないことを確認します。2つのリアルタイム保護シールドが同時に有効になっていると、互いに競合することがあります。システムから他のウイルス対策プログラム（インストールされている場合）をアンインストールすることをお勧めします。

リアルタイム保護が開始されない

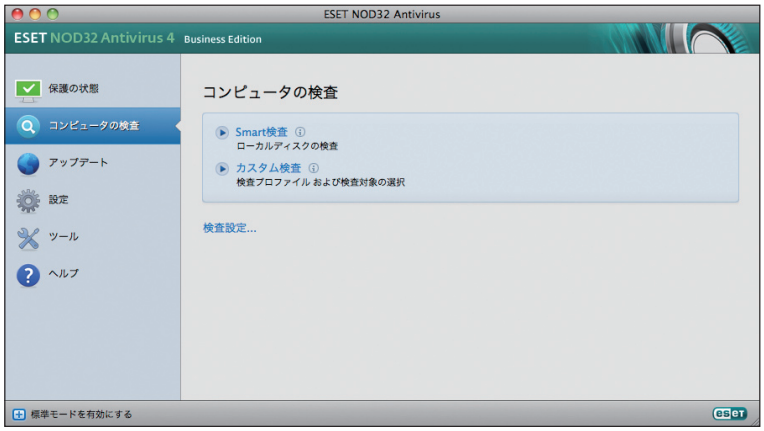
リアルタイム保護がシステム起動時に開始されない場合、他のプログラムとの競合が原因であることがあります。この場合には、サポートセンターまでご相談ください。

▸▸▸ NOTE

サポートセンターへの問い合わせ窓口は「ESETライセンス製品 ご利用の手引」をご参照ください。

4.1.2 コンピューターの検査

コンピューターが感染していると思われる場合には、[コンピュータの検査] > [Smart検査] を実行して、コンピューターに感染していないかどうかを調べます。保護機能の効果を最大化するため、感染が疑われるときだけコンピューターの検査を実行するのではなく、通常のセキュリティ手段の一環として定期的に実行する必要があります。検査を定期的に行うと、ディスクに保存されたときにリアルタイムスキャナーで検出されなかったマルウェアでも、検出できる場合があります。リアルタイムスキャナーで検出できないケースとは、感染時にリアルタイムスキャナーが無効に設定されていた場合や、ウイルス定義データベースが最新でない場合などです。



コンピューターの検査を最低でも月に1回は実行することをお勧めします。[ツール] > [スケジューラ] で、検査をスケジュールされたタスクとして設定できます。

4.1.2.1 検査の種類

コンピューターの検査には次の2種類があります。[Smart検査] では、検査パラメーターを追加で設定することなく、簡単にシステムを検査します。[カスタム検査] では、あらかじめ定義した検査プロファイルを選択することや、特定の検査対象を選択することができます。

Smart検査

Smart検査を使用すると、コンピューターの検査が開始され、ユーザーの操作無しに感染しているファイルからウイルスを駆除できます。主な利点は、簡単に操作でき、スキャンを詳細に設定しなくても済むことです。Smart検査では、全てのフォルダーにある全てのファイルが検査されます。検出されたウイルスがあれば、自動的に駆除または削除されます。駆除のレベルは自動的に既定値に設定されます。駆除の種類の詳細については、「駆除」を参照してください。

カスタム検査

カスタム検査は、検査の対象やスキャン方法などの検査パラメーターを自分で指定したい場合に最適です。カスタム検査を実行する利点は、パラメーターを詳細に設定できることです。さまざまな設定をユーザー定義の検査プロファイルとして保存できます。これは、同じパラメーターで検査を繰り返し実行する場合に便利です。

検査の対象を選択するには、[コンピュータの検査] > [カスタム検査] を選択し、ツリー構造から特定の検査の対象を選択します。検査対象をさらに細かく指定するには、対象にするフォルダーまたはファイルのパスを入力します。システムの検査で追加の駆除アクションを実行する必要がない場合は、[駆除せずに検査する] オプションを選択します。さらに、[設定...] > [駆除] をクリックして、3種類の駆除レベルから選択できます。

カスタム検査でコンピューターの検査を実行するのは、ウイルス対策プログラムを以前に使用した経験のある上級者にお勧めします。

4.1.2.2 検査の対象

[検査の対象] ツリー構造を使用すると、ウイルスを検査するファイルおよびフォルダーを選択できます。フォルダーはプロファイルの設定に従って選択することもできます。

検査の対象をさらに細かく設定するためには、検査の対象に含めるフォルダーまたはファイルのパスを入力します。コンピューター上で使用できる全てのフォルダーを表示しているツリー構造から対象を選択します。

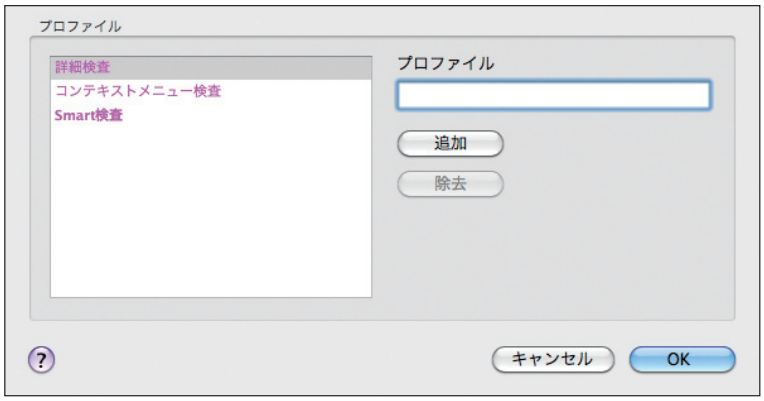
4.1.2.3 検査プロファイル

検査について目的の基本設定を保存して、後で検査を行う際に使用できます。さまざまな検査対象、検査方法、およびその他のパラメーターについて、定期的に行う検査ごとにプロファイルを作成することをお勧めします。

新しいプロファイルを作成するには、[設定（検査設定）] > [アプリケーションの設定を入力する...] > [保護] > [コンピュータの検査] をクリックし、現在のプロファイルの一覧の横にある [編集...] をクリックします。

ニーズに合った検査プロファイルを作成するための参考情報として、「ThreatSenseエンジンのパラメーターの設定」セクションにある検査設定の各パラメーターの説明を参照してください。

例



既にあるSmart検査の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があるとします。例えば、ランタイム圧縮形式と安全でない可能性があるアプリケーションは、検査しないように設定します。また、厳密な駆除を適用することもできます。検査プロファイルの作成は、[オンデマンドスキャナープロファイルリスト] ウィンドウで、プロファイル名を入力して [追加] ボタンをクリックし、[OK] をクリックして確認します。次に、ThreatSenseエンジンおよび検査の対象を設定してパラメーターを調整し、自分のニーズに合わせます。

4.1.3 ThreatSenseエンジンのパラメーターの設定

ThreatSenseは、複雑なウイルス検出方法で構成される技術の名前です。この技術は事前対応型なので、新しいウイルスが広がる初期の段階でも保護することができます。この技術では、システムのセキュリティを大幅に強化するために連携して動作するさまざまな方法（コード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャ）の組み合わせが使用されます。検査エンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。また、ThreatSense技術によってルートキットを除去することもできます。

ThreatSense技術の設定オプションを使用すると、ユーザーはさまざまな検査パラメーターを指定することができます。

●検査するファイルの種類および拡張子
●さまざまな検出方法の組み合わせ
●駆除のレベルなど

設定ウィンドウにアクセスするには、[設定] > [ウイルス・スパイウェア対策] > [ウイルス・スパイウェア対策の詳細設定] をクリックし、次に [システム保護] [リアルタイム保護] および [コンピュータの検査] の各タブの [設定...] ボタンをクリックします。これらのタブはいずれも、ThreatSense技術を使用します。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

● [システム保護] > [自動起動ファイルの検査]
● [リアルタイム保護] > [リアルタイムファイルシステム保護]
● [コンピュータの検査] > [コンピュータの検査]

ThreatSenseのパラメーターは機能ごとに固有の最適化がされているので、パラメーターを変更すると、システムの動作に大きく影響することがあります。たとえば、常にランタイム圧縮形式を検査するようにパラメーターを変更したり、リアルタイムファイルシステム保護モジュールでアドバンスドヒューリスティックを有効にしたりすると、システムの処理速度が低下することがあります。そのため、コンピュータの検査を除く全ての機能について、ThreatSenseの既定のパラメーターを変更しないことをお勧めします。

4.1.3.1 検査対象

[検査対象] セクションでは、マルウェアを検査するファイルを指定できます。

ファイル	一般的なファイルの種類（プログラム、画像、音声、動画、データベースファイルなど）を全て検査します。
シンボリックリンク	（オンデマンド検査のみ）オペレーティングシステムによって別のファイルまたはディレクトリーへのパスとして解釈され、たどることができるテキスト文字列を含む特殊な種類のファイルを検査します。
電子メールファイル	（リアルタイム保護では使用できません）電子メールメッセージが含まれている特殊なファイルを検査します。
メールボックス	（リアルタイム保護では使用できません）システム内のユーザーのメールボックスを検査します。このオプションを正しく使用しない場合、電子メールクライアントとの競合が発生することがあります。
アーカイブ	（リアルタイム保護では使用できません）アーカイブ内の圧縮されたファイル（.rar、.zip、.arj、.tarなど）を検査します。
自己解凍形式	（リアルタイム保護では使用できません）自己解凍形式のアーカイブファイルに含まれているファイルを検査します。
圧縮された実行形式	メモリーに展開されるランタイム圧縮形式（標準のアーカイブ形式とは異なります）、および標準的な静的圧縮形式（UPX、yoda、ASPack、FGSなど）を検査します。

4.1.3.2 オプション

[オプション] セクションでは、ウイルス検査の方法を指定することができます。使用可能なオプションは、以下のとおりです。

ウイルス定義データベース	ウイルス定義データベースを使用して、シグネチャにより正確かつ確実にマルウェアの検出と特定を行えます。この項目は、Linux版でのみ選択できます。
ヒューリスティック	ヒューリスティックは、悪意のあるプログラムの活動を解析するアルゴリズムを使用します。ヒューリスティック検出法の主な利点は、存在しなかった、またはこれまでのウイルス定義データベースで特定されていなかった、悪意のある新しいソフトウェアを検出できる能力です。
アドバンスドヒューリスティック	アドバンスドヒューリスティックは、ESETが開発した独自のヒューリスティックアルゴリズムで構成されます。このアルゴリズムは、コンピューターワームやトロイの木馬を検出するために最適化されています。アドバンスドヒューリスティックによって、プログラムの検出能力が大幅に向上します。
望ましくない可能性があるアプリケーション	望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピューターにインストールすると、アプリケーションをインストールする前とは異なる状態でシステムが動作します。最も大きな変化としては、不要なポップアップウィンドウ、隠しプロセスの開始と実行、システムリソースの使用率の増加、検索結果の変更、アプリケーションがリモートサーバーと通信することなどがあります。
潜在的に危険性のあるアプリケーション	潜在的に危険性のあるアプリケーションとは、そのアプリケーションがインストールされたことをユーザーが知らない場合、アタッカーが悪用する可能性のある、市販のソフトウェアのことを指します。これには、リモートアクセスツールなどのプログラムが含まれます。そのため、既定ではこのオプションは無効に設定されています。

4.1.3.3 駆除

駆除設定により、感染ファイルからウイルスを駆除するときのスキャナーの動作が決まります。駆除には、3つのレベルがあります。

駆除なし	感染しているファイルが自動的に駆除されることはありません。警告ウィンドウが表示され、アクションを選択することができます。
標準的な駆除	感染ファイルが自動的に駆除または削除されます。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択します。その後のアクションとして選択した内容は、あらかじめ指定したアクションを完了できなかった場合にも表示されます。
厳密な駆除	全ての感染ファイルが駆除または削除されます(アーカイブも対象)。ただし、システムファイルは除きます。感染ファイルを駆除できなかった場合は、警告ウィンドウでアクションを選択することができます。

CAUTION

既定の標準的な駆除モードで、アーカイブファイル全体が削除されるのは、アーカイブ内の全てのファイルが感染している場合のみです。問題のないファイルが含まれている場合には、アーカイブファイルは削除されません。厳密な駆除モードでは、感染しているアーカイブファイルが検出された場合、感染していないファイルがあっても、アーカイブ全体が削除されます。

4.1.3.4 拡張子

拡張子は、ファイル名の一部であり、ピリオドで区切られています。拡張子は、ファイルの種類を示します。ThreatSenseパラメーター設定のこのセクションでは、検査から除外するファイルの種類を指定できます。

既定では、拡張子に関係なく、全てのファイルが検査されます。検査から除外するファイルの一覧に任意の拡張子を追加できます。[追加] および [削除] のボタンを使用することで、目的の拡張子の検査を有効または無効にできます。

特定のファイルの種類を検査すると、その拡張子を使用しているプログラムが正常に動作できなくなる場合には、その拡張子を検査対象から除外することが必要になります。たとえば、.log　.cfg、および.tmp拡張子は除外することをお勧めします。

4.1.3.5 制限

[制限] セクションでは、検査対象のオブジェクトの最大サイズおよびネストされたアーカイブのレベルを指定できます。

最大サイズ	検査対象のオブジェクトの最大サイズを定義します。これにより、ウイルス対策機能では、指定した値より小さいサイズのオブジェクトのみが検査されます。既定値から変更しないことをお勧めします。大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。
最長検査タイム	オブジェクトの検査に割り当てられた最長時間を定義します。ここでユーザー定義の値が入力されていると、検査が終わっているかどうかにかかわらず、その時間が経過するとウイルス対策機能はそのオブジェクトのウイルス検査を停止し、次のオブジェクトの検査を行います。
最大のネストレベル	アーカイブの検査の最大レベルを指定します。既定値から変更しないことをお勧めします。ネストされたアーカイブ数が原因で検査が途中で終了した場合、アーカイブは未チェックのままになります。
最大のファイルサイズ	このオプションを使用すると、アーカイブ(抽出された場合)に含まれているファイルの最大ファイルサイズを指定できます。この制限により検査が途中で終了した場合、アーカイブは未チェックのままになります。

NOTE

Linux版でシステム (/procおよび/sys) によって制御されるフォルダーの検査を無効にするには、[システム制御フォルダーを検査から除外する] オプションを選択します。なお、このオプションは、スタートアップ検査では使用できません。

4.1.3.6 その他

スマート最適化を有効にすると、スキャンの速度を最高に保ちながら最も効率的なスキャンレベルが確保されるように、最適な設定が使用されます。さまざまな保護モジュールで高度にスキャンを行い、異なるスキャン方法を使用して、それらを特定のファイルタイプに適用されます。SMART最適化は製品内で厳密に定義されているものではありません。ESET開発チームは新しい変更点を継続的に実装し、通常のアップデートでお使いのESET NOD32アンチウイルスに組み込みます。SMART最適化を無効にすると、特定のモジュールのThreatSenseコアのユーザー定義設定のみがスキャンの実行時に適用されます。

[代替データストリームを検査する] (オンデマンドスキャナーのみ)

代替データストリーム (リソース/データフォーク) は、ファイルシステムによって使用され、通常のスキャン技術では検出できないファイルおよびフォルダーの関連付けです。多くのマルウェアが、自らを代替データストリームに見せかけることによって、検出を逃れようとします。

[最終アクセスのタイムスタンプを保持] (オンデマンドスキャナーのみ)

データバックアップシステムでの利用などを考慮して、検査済みファイルへのアクセス日時を更新せずに元のまま保持するには、このオプションを選択します。この設定は、Linux版でのみ行えます。

4.1.4 マルウェアが検出された場合

マルウェアがシステムに侵入する経路は、Webページ、共有フォルダー、電子メールや、コンピューターのリムーバブルデバイス（USB、外付けハードディスク、CD、DVD、フロッピーディスクなど）など、さまざまです。

使用しているコンピューターが、マルウェアに感染している兆候（処理速度が遅くなる、頻繁にフリーズするなど）を示している場合、次の処置を取ることをお勧めします。

1.ESET NOD32アンチウイルスを開き、[コンピュータの検査] をクリックします。
2.[Smart検査] をクリックします（詳細については、「Smart検査」を参照してください）。
3.検査終了後、ログで検査済みファイル、感染ファイル、および駆除済みファイルの件数をそれぞれ確認します。

ディスクの特定の部分だけを検査するには、[カスタム検査] をクリックし、ウイルスを検査する対象を選択します。

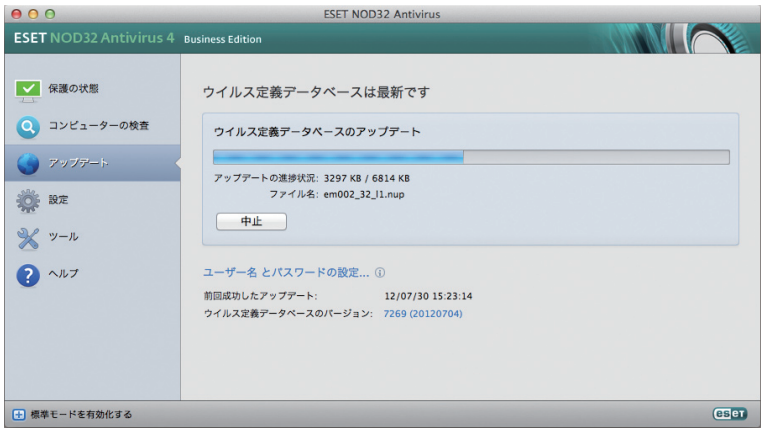
ESET NOD32アンチウイルスでのマルウェアの一般的な処理例として、リアルタイムファイルシステム保護（駆除レベルは既定値）によりマルウェアが検出されたものとして、説明します。リアルタイム保護機能は、ファイルからウイルスを駆除するか、ファイル自体を削除しようとします。リアルタイム保護モジュールにあらかじめ指定されたアクションがない場合は、警告ウィンドウが表示され、オプションを選択するよう求められます。選択できるオプションは通常、[駆除] [削除]、および [何もしない] のいずれかです。[何もしない] はお勧めできません。感染しているファイルが、そのままにされるためです。唯一の例外は、そのファイルが「無害なのに誤って感染が検出された」と確信できる場合です。

[駆除と削除] -ウイルスが悪意のあるコードをファイルに添付して攻撃している場合に、駆除を行います。この場合、ファイルを元の状態に戻すため、まず感染しているファイルからウイルスの駆除を試みます。ファイルが悪意のあるコードのみで構成されている場合には、ファイル全体が削除されます。

[アーカイブのファイルの削除] -既定の駆除モードでは、アーカイブファイルに感染ファイルしか含まれていない場合にのみ、アーカイブファイル全体が削除されます。つまり、感染していない無害なファイルも含まれている場合には、アーカイブは削除されません。ただし、厳密な駆除スキャンを実行する際には注意が必要です。厳密な駆除では、アーカイブに感染ファイルが1つでも含まれていれば、アーカイブ内の他のファイルのステータスに関係なく、アーカイブが削除されます。

4.2 アップデート

最大レベルのセキュリティを確保するためには、ESET NOD32アンチウイルスの定期的アップデートが必要です。アップデート機能により、ウイルス定義データベースがアップデートされ、プログラムは常に最新の状態に維持されます。

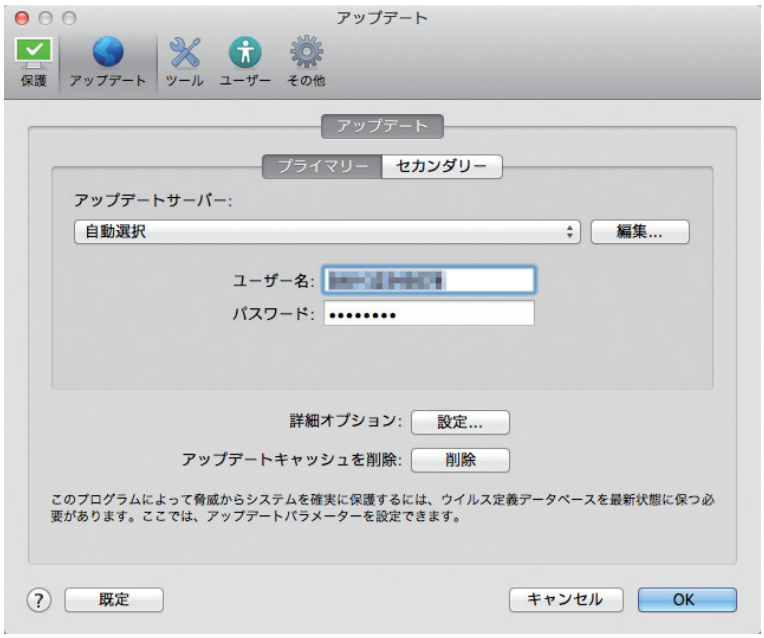


メインメニューの［アップデート］をクリックすると、前回成功したアップデートの日時、アップデートが必要かどうかなど、現在のアップデートの状態を確認できます。アップデートプロセスを手動で開始するには、［ウイルス定義データベースをアップデートする］をクリックします。

通常の状況では、アップデートファイルが正常にダウンロードされると、［アップデート］ウィンドウに［ウイルス定義データベースは最新です］というメッセージが表示されます。ウイルス定義データベースをアップデートできない場合は、アップデートの設定を確認することをお勧めします。このエラーの最も多い原因に、認証データ（ユーザ名とパスワード）の入力が正しくない、または接続設定の誤りがあります。

［アップデート］ウィンドウには、ウイルス定義データベースのバージョンに関する情報も表示されます。ウイルス定義データベースの番号はWebサイトへのリンクになっており、このリンクをクリックすると、そのアップデートで追加されたウイルス情報一覧が表示されます。

4.2.1 アップデートの設定



アップデート設定セクションでは、アップデートサーバーやそれらのサーバーの認証データなど、アップデートファイルの送信元の情報を指定します。既定では、[アップデートサーバ] ドロップダウンメニューは自動的に [自動選択] に設定され、最もネットワークトラフィックが少ないESETサーバーからアップデートファイルが自動的にダウンロードされます。

使用可能なアップデートサーバーのリストにアクセスするには、[アップデートサーバ] ドロップダウンメニューを使用します。新しいアップデートサーバーを追加するには、[編集...] をクリックします。[アップデートサーバー] 入力フィールドに新しいサーバーのアドレスを入力し、[追加] ボタンをクリックします。アップデートサーバーの認証は、購入後に提供されるユーザー名とパスワードを利用します。

テストモードの使用を有効にするには、[詳細オプション] の横にある [設定...] ボタンをクリックし、[テストモードを有効にする] チェックボックスをチェックします。アップデートに成功するごとに表示されるシステムトレイの通知を無効にするには、[成功したアップデートについての通知を表示しない] チェックボックスをチェックします。

一時的に保存されたアップデートファイルを全て削除するには、[アップデートキャッシュを削除] の横にある [削除] ボタンをクリックします。アップデート中に問題が発生した場合はこのオプションを使用してください。

NOTE

アップデートの設定を変更できるのは、権限ユーザーに登録されたユーザーのみです。権限ユーザーの詳細については、51ページをご参照ください。

4.2.2　アップデートタスクの作成方法

アップデートを手動で開始するには、メインメニューの［アップデート］をクリックした後に表示されるプライマリウィンドウで、［ウイルス定義データベースをアップデートする］をクリックします。

アップデートはスケジュールされたタスクとしても実行できます。スケジュールされたタスクを設定するには、［ツール］＞［スケジューラ］をクリックします。ESET NOD32アンチウイルスでは、次のタスクが既定で有効になっています。

●定期的に自動アップデート
●ユーザーログオン後に自動アップデート

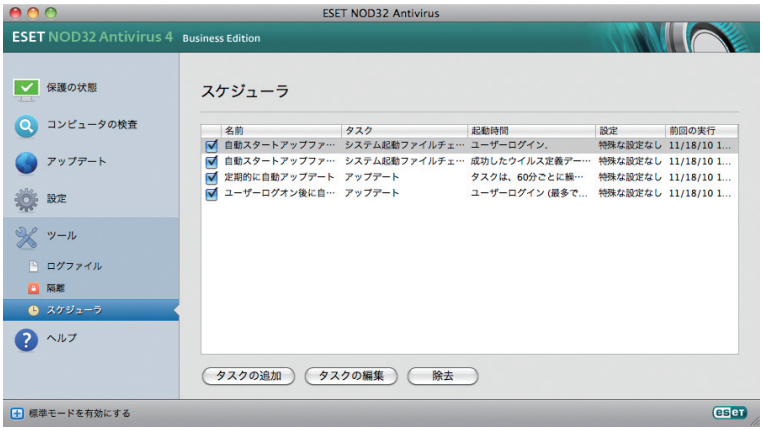
上記のアップデートタスクはそれぞれ、ユーザーのニーズに合わせて変更することができます。ユーザーは、既定のアップデートタスクとは別に、ユーザー定義の設定で新しいアップデートタスクを作成することができます。アップデートタスクの作成と設定の詳細については、「スケジューラー」セクションを参照してください。

▸▸▸ NOTE

アップデートタスクの作成が行えるのは、権限ユーザーに登録されたユーザーのみです。権限ユーザーの詳細については、51ページをご参照ください。

4.3 スケジューラー

ESET NOD32アンチウイルスの詳細モードが有効になっている場合、スケジューラーを設定することができます。スケジューラーは、ESET NOD32アンチウイルスのメインメニューの [ツール] にあります。スケジューラーには、スケジュール済みの全てのタスクと設定プロパティ（あらかじめ定義した日付、時刻、使用する検査プロファイルなど）の一覧が表示されます。



既定では、次のスケジュールされたタスクがスケジューラに表示されます。

●定期的に自動アップデート
●ユーザーログオン後に自動アップデート
●自動起動ファイルの検査（ユーザーのログオン後）
●自動起動ファイルの検査（ウイルス定義データベースの正常なアップデート後）
●ログの保守（スケジューラーの設定で [システムタスクを表示する] オプションを有効にした後）

既存のスケジュールされたタスク（既定のタスクおよびユーザー定義のタスク）の設定を編集するには、タスクを右クリックして [編集...] をクリックするか、変更するタスクを選択して [編集...] ボタンをクリックします。

NOTE

スケジューラーの設定が行えるのは、権限ユーザーに登録されたユーザーのみです。権限ユーザーの詳細については、51ページをご参照ください。

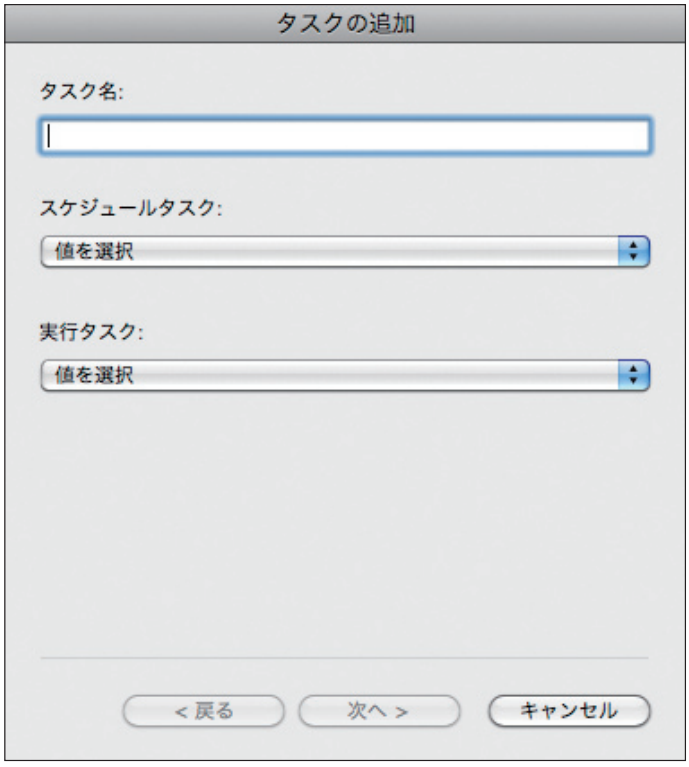
4.3.1　スケジューラー

スケジューラーでは、スケジュールされたタスクが、あらかじめ定義された設定やプロパティと共に管理され、開始されます。設定およびプロパティには、日時のほか、タスクの実行時に使用される所定のプロファイルなどの情報が含まれます。

4.3.2　新しいタスクの作成

スケジューラーで新しいタスクを作成するには、[タスクの追加...] ボタンをクリックするか、右クリックしてコンテキストメニューから [追加...] を選択します。次の5種類のスケジュールされたタスクが使用可能です。

●アプリケーションの実行
●アップデート
●ログの保守
●コンピュータの検査
●システムのスタートアップファイルのチェック



スケジュールされたタスクの中でアップデートが最もよく使用されるので、新しいアップデートタスクを追加する方法を説明します。

[スケジュールタスク] ドロップダウンメニューから [アップデート] を選択します。[タスク名] フィールドにタスクの名前を入力します。[実行タスク] ドロップダウンメニューからタスクの頻度を選択します。使用可能なオプションは、[ユーザー定義] [1回] [繰り返し] [毎日] [毎週]、および [イベントの発生時] です。選択された頻度に基づいて、さまざまな更新パラメーターが提示されます。次に、スケジュールされた時刻にタスクを実行できない場合や完了できない場合に実行するアクションを定義することができます。次の3つのオプションが使用可能です。

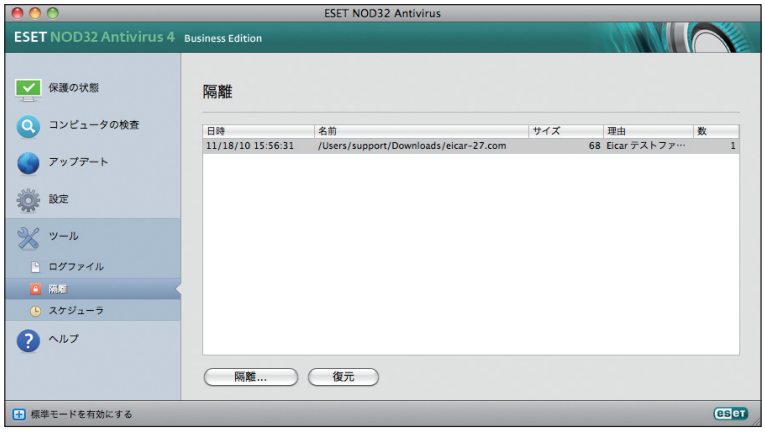
●次のスケジュール設定日時まで待機
●実行可能になりしだい実行する
●前回実行されてから次の時間が経過した場合は直ちに実行する（[タスクの実行間隔] スクロールボックスで、間隔を定義することができます）。

次のステップでは、現在のスケジュールされたタスクに関する情報の概要のウィンドウが表示されます。[終了] ボタンをクリックします。

新しくスケジュールされたタスクが、現在スケジュールされているタスクのリストに追加されます。
システムには、製品を正常に機能させるため、いくつかの重要なタスクがあらかじめスケジュール設定されています。これらのタスクは、不用意に変更されないように既定では非表示にされています。このオプションを変更し、これらのタスクを表示するには、[設定] > [詳細設定を表示する...] > [ツール] > [スケジューラ] をクリックし、[システムタスクを表示する] オプションを選択します。

4.4 隔離

隔離の主な役割は、検出したファイルを安全に保存することです。ファイルを駆除できない場合、ファイルの削除が安全でないまたは推奨されない場合、あるいはESET NOD32アンチウイルスで誤って検出された場合、ファイルを隔離する必要があります。



なお、任意のファイルを選択して隔離することもできます。これは、ファイルの動作が疑わしいにもかかわらず、ウイルス対策スキャナーによって検出されない場合にお勧めします。隔離したファイルは、ESETのウイルスラボに提出して分析を受けることができます。

隔離フォルダーに保存されているファイルは、隔離の日時、感染ファイルの元の場所のパス、ファイルサイズ（バイト単位）、理由（"ユーザーによって追加されました"など）、およびウイルスの数（複数のマルウェアを含むアーカイブの場合など）を表示するテーブルで参照することができます。ファイルが隔離された隔離フォルダーはESET NOD32アンチウイルスのアンインストール後もシステムに残ります。隔離されたファイルは暗号化された安全な形式で格納されており、ESET NOD32アンチウイルスにより再度復元することもできます。隔離フォルダーは、以下にパスに設定されています。

●Macの場合
/Library/ApplicationSupport/Eset/cache/esets/quarantine

●Linuxの場合
/var/opt/eset/esets/cache/quarantine

▸▸▸ NOTE

Linux版では、隔離されたファイルをウイルス定義データベースのアップデート後に自動的に検査するように設定できます。この設定は、[設定]>[詳細設定を表示する]とクリックし、保護画面が表示されたら[ツール]>[隔離]とクリックして、[アップデート後は毎回隔離ファイルを再検査する]オプションを選択します。

4.4.1 ファイルの隔離

削除されたファイルは、ESET NOD32アンチウイルスにより自動的に隔離されます（警告ウィンドウでユーザーがこのオプションをキャンセルしなかった場合）。必要に応じて、[隔離...] ボタンをクリックして不審なファイルを手動で隔離することができます。この操作にもコンテキストメニューを使用することができます。[隔離] ウィンドウ内で右クリックし、隔離するファイルを選択し、[開く] ボタンをクリックします。

4.4.2 隔離フォルダーからの復元

隔離されているファイルは、元の場所に復元することができます。そのためには、[復元] ボタンを使用します。復元はコンテキストメニューから選択することもできます。それには、[隔離] ウィンドウで特定のファイルを右クリックし [復元] をクリックします。コンテキストメニューには、[復元先を指定...] オプションもあります。このオプションを使用すると、隔離される前の場所とは異なる場所にファイルを復元することができます。

4.4.3 隔離フォルダーからのファイルの提出

プログラムによって検出されなかった疑わしいファイルを隔離した場合、またはファイルが（ヒューリスティック分析などによって）感染していると誤って評価されて隔離された場合は、そのファイルをESETのウイルスラボに送信してください。隔離フォルダからファイルを提出するには、ファイルを右クリックし、コンテキストメニューから [分析のためにファイルを提出] を選択します。

4.5 ログファイル

ログファイルには、発生した全ての重要なプログラムイベントに関する情報が格納され、検出されたウイルスの概要が表示されます。ログは、システムの分析、ウイルスの検出、およびトラブルシューティングで重要なツールとして使用されます。ログへの記録はバックグラウンドでアクティブに実行され、ユーザーの操作を必要としません。情報は、ログの詳細レベルに関する現在の設定に基づいて記録されます。また、ログをアーカイブするだけでなく、ESET NOD32アンチウイルス環境から直接ログを表示することができます。

ログファイルにアクセスするには、ESET NOD32アンチウイルスのメインメニューで［ツール］［ログファイル］の順にクリックします。ウィンドウの最上部にある［ログ］ドロップダウンメニューを使用して、目的のログの種類を選択します。使用可能なログは次のとおりです。

1. 検出された脅威-このオプションを選択すると、マルウェアの検出に関連するイベントに関する全ての情報が表示されます。
2. イベント-このオプションは、システム管理者およびユーザーが問題を解決するために使用します。イベントログには、ESET NOD32アンチウイルスによって実行された全ての重要なアクションが記録されます。
3. コンピュータの検査-このウィンドウには、完了した全ての検査結果が表示されます。エントリーをダブルクリックすると、コンピューターの検査結果の詳細がそれぞれ表示されます。

各セクションで、エントリーを選択し、［コピー］ボタンをクリックすると、表示されている情報をクリップボードに直接コピーすることができます。

4.5.1 ログの保守

ESET NOD32アンチウイルスのログの設定には、プログラムのメインウィンドウからアクセスすることができます。[設定] > [詳細設定を表示する...] > [ツール] > [ログファイル] の順にクリックします。ログファイルの次のオプションを指定することができます。

古いログレコードを自動的に削除する	指定した日数より古いログエントリーが自動的に削除されます。
ログファイルを自動的に最適化する	未使用のレコードが指定した割合を超えると、ログファイルが自動的に最適化されます。

[ログレコードの既定フィルター] を設定するには、[編集...] ボタンをクリックし、必要に応じてログの種類を選択または選択解除します。

4.5.2 ログのフィルター

ログには、重要なシステムイベントに関する情報が保存されます。ログのフィルター機能では、特定の種類のイベントに関するレコードを表示することができます。

最もよく使用されるログの種類を次に示します。

重大な警告	致命的なシステムエラー(ウイルス・スパイウェア対策の起動に失敗したなど)。
エラー	"ファイルのダウンロードエラー "などのエラーメッセージと致命的なエラー。
警告	警告メッセージ。
情報レコード	アップデートの正常完了、警告などの情報。
診断レコード	プログラムの微調整に必要な情報および上記の全てのレコード。

[全てのフィルター] では、上記の全てのログタイプを選択または選択解除します。

4.6 ユーザーインタフェース

ESET NOD32アンチウイルスのユーザーインタフェースの設定オプションを使用すると、各自のニーズに合わせて作業環境を調整することができます。これらの設定オプションには、[設定] > [詳細設定を表示する...] > [ユーザー] > [インタフェース] からアクセスします。

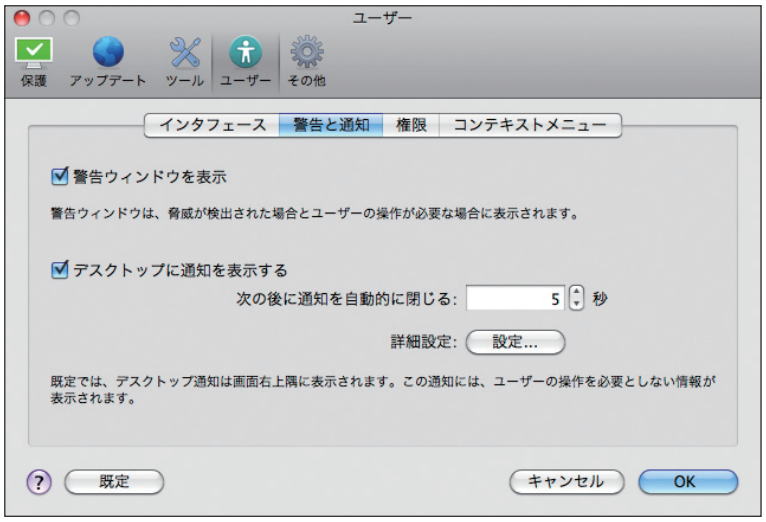
このセクションの詳細モードオプションを使用して、詳細モードに切り替えることができます。詳細モードでは、ESET NOD32アンチウイルスのより詳細な設定が表示されます。

スプラッシュウィンドウ機能を有効にするには、[起動時にスプラッシュウィンドウを表示する] オプションを選択します。

[標準メニューを使用する] セクションで、[標準モードで] または [詳細モードで] オプションを選択すると、それぞれの表示モードでプログラムの基本画面の標準メニューを使用できます。

ツールヒントの使用を有効にするには、[ツールヒントを表示] オプションを選択します。[隠しファイルを表示する] オプションを選択すると、[コンピュータの検査] の [検査の対象] 設定で隠しファイルを表示して選択することができます。

4.6.1 警告と通知



[警告と通知] セクションでは、ウイルス警告やシステム通知をESET NOD32アンチウイルスでどのように処理するかを設定することができます。

[警告ウィンドウを表示] オプションを無効にすると、全ての警告ウィンドウが表示されなくなります。この設定が適しているのは、特定の限られた状況のみです。ほとんどのユーザーには、既定の設定のままにすることをお勧めします（チェックボックスをオンにします）。

[デスクトップに通知を表示する] オプションを選択すると、ユーザーの操作が不要な警告ウィンドウをデスクトップに表示できます（既定では画面の右上角）。通知の表示時間を定義するには、[次の後に通知を自動的に閉じる] X [秒] の値を調整します。

4.6.1.1 警告と通知の詳細設定

ユーザーの操作が必要な通知のみ表示する

このオプションを使用すると、ユーザーに操作を要求するメッセージの表示をオンまたはオフにすることができます。

全画面モードでアプリケーションを実行中にユーザーの操作が必要な通知のみ表示する

プレゼンテーション、ゲームなど、画面全体が必要な操作を行う場合、このオプションを選択すると便利です。

4.6.2 権限

ESET NOD32アンチウイルスの設定は組織のセキュリティポリシーにとって非常に重要です。許可なく変更が行われた場合は、システムの安定性と保護が危険にさらされる可能性があります。このような問題に備えて、プログラム設定を編集する権限を持つユーザーを選択できます。

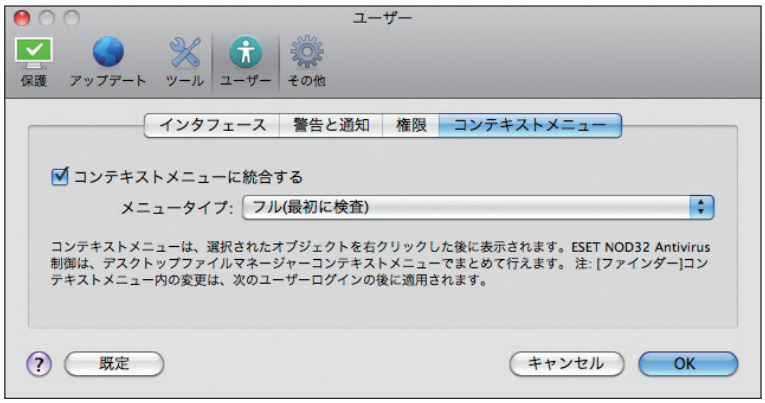
権限ユーザーを指定するには、[設定] > [詳細設定を表示する...] > [ユーザー] > [権限] に入力します。

システムの最大限のセキュリティを確保するには、プログラムを正しく設定することが重要です。許可なく変更が行われた場合、重要なデータが失われることがあります。権限ユーザーの一覧を設定するには、左側の[ユーザー]一覧からユーザーを選択し、[追加] ボタンをクリックします。ユーザーを削除するには、右側の [権限ユーザー] 一覧でユーザー名を選択し、[除去] をクリックします。

NOTE

権限ユーザーの一覧が空の場合、システムの全てのユーザーにプログラムの編集権限があります。また、権限ユーザーの登録が行えるのは、権限ユーザーとして登録されているユーザーのみです。Linux版をご利用の場合で、はじめて権限ユーザーの設定を行う場合は、基本画面をroot権限(スーパーユーザー)で起動して設定を行うか、コマンドラインから設定を追加する必要があります。コマンドラインから追加する方法は、28ページを参照してください。

4.6.3 コンテキストメニュー



コンテキストメニューの統合を有効にするには、[設定] > [詳細設定を表示する...] > [ユーザー] > [コンテキストメニュー] セクションで [コンテキストメニューに統合する] チェックボックスをオンにします。

4.7 ThreatSense.Net

ThreatSense.Net早期警告システムにより、ESETは新しいマルウェアを迅速かつ継続的に把握することができます。

ThreatSense.Net早期警告システムは、検出した疑しいファイルのサンプルファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、およびコンピューターのオペレーティングシステムについての情報を収集します。そしてその情報を元に解析を行い新しいマルウェアかどうか判定します。

収集した情報は、新しいウイルスに迅速に対応する目的以外で使用されることはありません。

ThreatSense.Netの設定にアクセスするには、[詳細設定] ウィンドウで [ツール] [ThreatSense.Net] の順に選択します。[ThreatSense.Net早期警告システムを有効にする] オプションを選択して有効にし、[詳細設定オプション] 見出しの横にある [設定...] ボタンをクリックします。

4.7.1 不審なファイル

[不審なファイル] オプションでは、分析を受けるためにESETのウイルスラボにウイルスを提出する方法を設定することができます。

不審なファイルがある場合は、ESETのウイルスラボに提出して分析を受けることができます。そのファイルが悪意のあるアプリケーションであることが判明すると、次のウイルス定義データベースのアップデートにその検出が追加されます。

不審なファイルの提出-[アップデート時] に不審なファイルを送信することができます。つまり、通常のウイルス定義データベースのアップデート時にESETのウイルスラボに提出します。また、[即時] に送信することもできます。この設定は、永続的なインターネット接続が利用可能な場合に適しています。

ファイルを提出しない場合は、[提出しない] オプションを選択します。分析を受けるためにファイルを提出しなくても、統計情報の提出には影響しません。これは別の領域で設定されます。

ThreatSense.Net早期警告システムでは、新しく検出されたウイルスに関連するコンピューターについての匿名の情報が収集されます。この情報には、マルウェアの名前、マルウェアが検出された日時、ESETセキュリティ製品のバージョン、オペレーティングシステムのバージョン、およびローカル設定が含まれます。統計は通常、1日1回または2回、ESETのサーバーに配信されます。

提出される統計パッケージの例は次のとおりです。

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

匿名情報と統計情報の提出-統計情報を提出する時期を定義することができます。[即時] の提出を選択した場合、統計情報が作成され次第、送信されます。この設定は、永続的なインターネット接続が利用可能な場合に適しています。[アップデート時] オプションを選択した場合は、全ての統計情報が収集後のアップデート時に提出されます。

匿名の統計情報を送信しない場合は、[提出しない] オプションを選択できます。

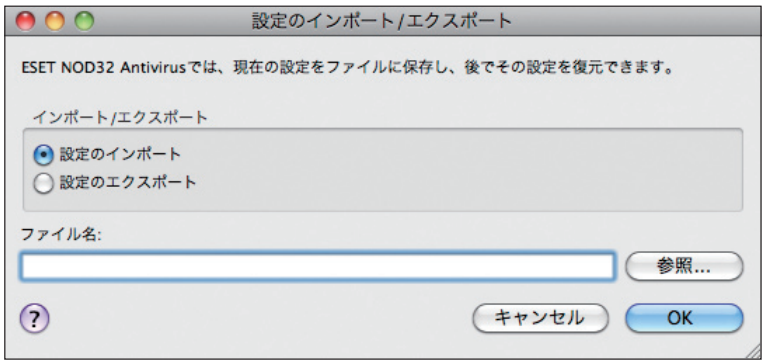
提出方法	ファイルと統計情報をESETに提出する方法を選択できます。[リモート管理サーバまたはESET] オプションを選択した場合、使用可能なあらゆる方法によって、ファイルおよび統計情報が提出されます。[リモート管理サーバー] オプションを選択した場合、ファイルおよび統計情報がリモート管理サーバーに送信された後、ESETのウイルスラボに提出されます。[ESET] オプションを選択した場合は、全ての不審なファイルおよび統計情報がプログラムから直接、ESETのウイルスラボに送信されます。
除外フィルタ	このオプションを使用すると、特定のファイルやフォルダーを提出から除外することができます。たとえば、ドキュメントやスプレッドシートなど、機密情報が含まれている可能性があるファイルを除外すると便利です。なお、最も一般的なファイルの種類(.docなど)は、既定で除外されます。除外するファイルの一覧にファイルの種類を追加できます。
連絡先の電子メールアドレス(任意)	不審なファイルと共に電子メールアドレスを送信できます。この電子メールアドレスは、分析のために詳しい情報が必要な場合の連絡先として使用されます。詳しい情報が必要でない限り、ESETから連絡することはありません。

[Chapter 5]
上級者向けガイド

5.1 設定のインポート /エクスポート

ESET NOD32アンチウイルスの設定のインポートとエクスポートは、詳細モード時に [設定] から行うことができます。

インポートとエクスポートのいずれの場合もアーカイブファイルを使用して設定を保存します。インポートとエクスポートは、後で使用するためにESET NOD32アンチウイルスの現在の設定をバックアップする必要がある場合に便利です。エクスポート設定オプションは、ESET NOD32アンチウイルスの好みの基本設定を複数のシステムに対して使用する場合にも便利です。設定ファイルを簡単にインポートして、目的の設定を転送できます。



NOTE

設定のインポート／エクスポートを行えるのは、権限ユーザーに登録されたユーザーのみです。権限ユーザーの詳細については、51ページをご参照ください。

5.1.1 設定のインポート

メインメニューで [設定] > [設定のインポート /エクスポート...] をクリックし、[設定のインポート] オプションを選択します。設定ファイルの名前を入力するか、[参照...] ボタンをクリックして、インポートする設定ファイルを参照します。

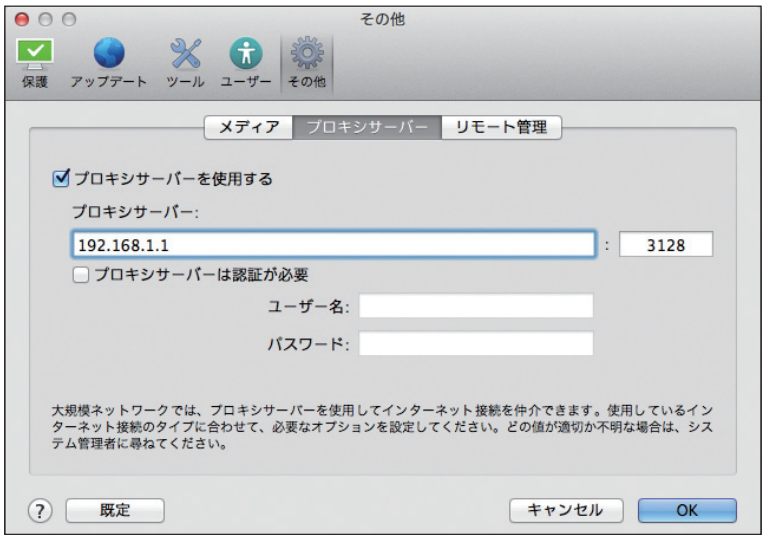
5.1.2 設定のエクスポート

メインメニューで [設定] > [設定のインポート /エクスポート...] をクリックし、[設定のエクスポート] オプションを選択します。設定ファイルの名前を入力するか [参照] ボタンをクリックしてエクスポート先を選択します。

5.2 プロキシサーバーの設定

プロキシサーバーの設定は、[その他] > [プロキシサーバー] で行うことができます。プロキシサーバーをこのレベルで指定すると、ESET NOD32アンチウイルス全体のプロキシサーバー設定が指定されることになります。ここで設定するパラメーターは、インターネットへの接続を必要とする全てのモジュールで使用されます。

プロキシサーバー設定をこのレベルで指定するには、[プロキシサーバーを使用する] チェックボックスをオンにし、プロキシサーバーのアドレスを [プロキシサーバー] フィールドに入力し、プロキシサーバーのポート番号を指定します。プロキシサーバーとの通信に認証が必要な場合、[プロキシサーバーは認証が必要] チェックボックスをオンにし、有効なユーザー名とパスワードをそれぞれのフィールドに入力します。



NOTE

プロキシサーバーの設定が行えるのは、権限ユーザーに登録されたユーザーのみです。権限ユーザーの詳細については、51ページをご参照ください。

5.3 リムーバブルメディアのブロック

リムーバブルメディア（CD、USBなど）に悪意のあるコードが含まれ、コンピューターを危険にさらす可能性があります。リムーバブルメディアをブロックするには、[リムーバブルメディアの遮断を有効にする]オプションをオンにします。特定のタイプのメディアへのアクセスを許可するには、必要なメディアボリュームの選択を解除します。

NOTE

リムーバブルメディアのブロック設定が行えるのは、権限ユーザーに登録されたユーザーのみです。権限ユーザーの詳細については、51ページをご参照ください。

5.4 リモート管理

ESET Remote Administrator (ERA) は、セキュリティポリシーを管理するため、およびネットワーク内の全体的なセキュリティの概要を取得するために使用するツールです。大規模なネットワークで使用すると、特に効果的です。ERAによってセキュリティレベルが向上するだけでなく、クライアントワークステーションにおけるESET NOD32アンチウイルスの管理が容易になります。

リモート管理の設定オプションには、ESET NOD32アンチウイルスのメインウィンドウからアクセスすることができます。[設定] > [詳細設定を表示する...] > [その他] > [リモート管理] をクリックします。

リモート管理を有効にするには、[リモート管理サーバーに接続する] オプションを選択します。この操作で、下記のオプションへのアクセスが可能になります。

サーバー接続の間隔 - ESET NOD32アンチウイルスがERA Serverに接続する頻度を指定します。0に設定されている場合、数十秒ごとに情報が送信されます。
リモート管理サーバー - ERA Serverがインストールされているサーバーのネットワークアドレスとポート番号です。このフィールドには、ネットワーク接続に使用される、あらかじめ定義されたサーバーポートが表示されます。既定のポート設定である2222をそのまま使用することをお勧めします。

一般的には、プライマリーサーバーのみを設定する必要があります。複数のERA Serverがネットワーク上で稼働している場合、別のセカンダリーERA Server接続を追加することもできます。それはフォールバックソリューションとして機能します。プライマリサーバーにアクセスできなくなると、ESET NOD32アンチウイルスは自動的にセカンダリーERA Serverに問い合わせます。同時に、ESET NOD32アンチウイルスはプライマリーサーバーへの接続の再確立を試行します。この接続が再度有効になると、ESET NOD32アンチウイルスは元のプライマリーサーバーに切り替えられます。ローカルネットワークおよびネットワーク外部から接続するノートパソコンを使用したモバイルクライアントでは、2つのリモート管理サーバープロファイルの設定がよく使用されます。

NOTE

リモート管理の設定が行えるのは、権限ユーザーに登録されたユーザーのみです。権限ユーザーの詳細については、51ページをご参照ください。

[Chapter 6]
用語集

6.1 マルウェアの種類

マルウェアとは、ユーザーのコンピューターに入り込み、損害を与えようとする悪意があるソフトウェアのことです。

6.1.1 ウイルス

コンピューターウイルスとは、コンピューター上の既存のファイルを破損させるマルウェアの一種です。ウイルスは生物学上のウイルスにちなんで名付けられました。

コンピューターウイルスの目的と重大度は、さまざまです。ハードディスクからファイルを意図的に削除できるウイルスもあり、このようなウイルスは大変危険です。一方、実質的には被害を及ぼさないウイルスもあります。作成者が単にユーザーを困らせ、自分の技術上の技量を誇示するに過ぎないものもあります。

トロイの木馬やスパイウェアと比較するとウイルスは少なくなっています。悪意のあるソフトウェア開発者にとって金銭的に魅力的ではないためです。また、"ウイルス"という用語は、あらゆる種類のマルウェアを意味する用語として誤用されることがよくあります。この用法は、新しくより正確な用語"マルウェア"（悪意のあるソフトウェア）へと次第に言い換えられています。

お使いのコンピューターがウイルスに感染した場合は、感染したファイルを元の状態に復元する、つまりウイルス対策プログラムでファイルからウイルスを駆除する必要があります。

●ウイルスの例

OneHalf Tenga、およびYankee Doodle。

6.1.2 ワーム

コンピューターワームとは、感染先のコンピューターを攻撃しネットワークを介して蔓延する、悪意のあるコードを含むプログラムを指します。ウイルスとワームの基本的な違いは、ワームは自己を複製し、自ら移動できることです。ワームは宿主ファイル（またはブートセクター）に依存しません。ワームはアドレス帳の電子メールアドレスを介して広がるか、ネットワークアプリケーションのセキュリティ上の脆弱性を悪用します。

したがって、ワームはコンピューターウイルスよりはるかに実行可能性が高いプログラムです。インターネットを至る所から利用できるので、リリースしてから数時間以内に世界中に蔓延できます。場合によっては、数分で広まることもあります。自己を単独で急速に複製できる能力があるので、他の種類のマルウェアよりはるかに危険です。

システム内でワームが活性化すると、深刻な事態が引き起こされることがあります。ファイルの削除、システムパフォーマンスの低下だけでなく、プログラムが動かなくなることすらあります。コンピューターワームはその本来の性質ゆえに、他の種類のマルウェアの"輸送手段"に利用されることもあります。

コンピューターがワームに感染した場合は、感染ファイルを削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

●ワームの例

Lovsan/Blaster Stration/ Warezov Bagle、およびNetsky。

6.1.3 トロイの木馬

従来、コンピューター分野でのトロイの木馬は、自己を有益なプログラムに見せかけ、ユーザーを騙して実行させようとするマルウェアの1つのクラスとして定義されてきました。今やトロイの木馬は偽装する必要がなくなりました。トロイの木馬の唯一の目的は、できるだけ簡単に侵入し、悪意のある目標を達成することです。"トロイの木馬"は、極めて一般的な用語になりました。今日ではマルウェアのどの特定のクラスにも分類されないマルウェアなら、全て該当します。

このカテゴリーの範囲は非常に広いので、多くのサブカテゴリーに分類されることもよくあります。

ダウンローダー	インターネットから他のマルウェアをダウンロードする機能を備えた悪意のあるプログラム。
ドロッパー	他の種類のマルウェアを弱体化されたコンピューターに落とす(ドロップする)トロイの木馬の一種。
バックドア	リモートの攻撃者と通信して、システムにアクセスし制御できるようにするアプリケーション。
キーロガー	(キーストロークロガー)-ユーザーが入力した各キーストロークを記録し、リモートの攻撃者にその情報を送信するプログラム。
ダイアラー	情報料代理徴収番号に接続するよう設計されたプログラム。新しい接続が作成されたことにユーザーが気づくのは、ほとんど不可能です。ダイアラーで被害を被るのは、ダイヤルアップモデムを使用するユーザーのみです。このモデムは今日ではあまり使用されていません。

通常、トロイの木馬は実行可能ファイルの形式です。トロイの木馬として検出されるファイルがコンピューターにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

●トロイの木馬の例

NetBus Trojandownloader.Small.ZL Slapper。

6.1.4 アドウェア

アドウェアは、広告機能をサポートしているソフトウェアを省略した用語です。広告を表示するプログラムが、このカテゴリに分類されます。アドウェアアプリケーションは、広告が表示される新しいポップアップウィンドウをインターネットブラウザー内に自動的に開いたり、ブラウザーのホームページを変更することがあります。アドウェアは、フリーウェアプログラムに同梱されていることが多いです。

アドウェア自体は危険ではありません。ユーザーは広告に悩まされるだけです。危険は、アドウェアが（スパイウェアと同様に）追跡機能を発揮することがある、という事実にあります。

フリーウェアプログラムを使用することにした場合には、インストールプログラムに特に注意してください。大半のインストールプログラム（インストーラー）は、アドウェアプログラムを追加でインストールすることをユーザーに通知します。アドウェアのインストールをキャンセルし、アドウェアなしで目的のプログラムをインストールできることが一般的です。

場合によっては、アドウェアをインストールしないと目的のプログラムをインストールできなかったり、機能が制限されてしまうこともあります。これは、そのアドウェアが頻繁にシステムに"合法的に"アクセスする可能性があることを意味します。アドウェアとして検出されるファイルがコンピューターにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

6.1.5 スパイウェア

このカテゴリーは、個人情報を当人の同意を得ず、当人が知らないうちに送信する全てのアプリケーションが該当します。スパイウェアは、追跡機能を使用して、アクセスしたWebサイトの一覧、ユーザーの連絡先リストにあるメールアドレスや、記録されたキーストロークなどのさまざまな統計データを送信します。

スパイウェアの作成者は、こうした手法はユーザーのニーズと関心に関するデータをさらに見つけ、的を絞った広告を出せるようにすることが目的であると主張します。問題は、有益なアプリケーションと悪意のあるアプリケーションとの間に明確な境界線がなく、しかも、引き出された情報が悪用されることはない、とだれも断言できないことです。スパイウェアが収集したデータには、セキュリティコード、PIN、銀行の口座番号などが含まれていることがあります。スパイウェアはフリーウェアプログラムの作成者が、プログラムに同梱していることがよくあります。これは、収益を上げたり、そのプログラムを購入するよう動機を与えるためです。プログラムのインストール中に、スパイウェアが含まれていることをユーザーに知らせることもよくあります。これは、スパイウェアが含まれない有料バージョンにアップグレードするよう促すためです。

スパイウェアが同梱されている、よく知られているフリーウェア製品の例としては、P2P（ピアツーピア）ネットワークのクライアントアプリケーションがあります。SpyfalconやSpy Sheriffを始めとする多数のプログラムは、スパイウェアの特定のサブカテゴリーに属します。これらは一見、スパイウェア対策プログラムに見えますが、実はそれ自体がスパイウェアプログラムなのです。

スパイウェアとして検出されるファイルがコンピューターにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

6.1.6　安全でない可能性があるアプリケーション

ネットワークに接続されたコンピューターの管理を容易にする機能を持つ適正なプログラムは、少なくありません。ただし、悪意のあるユーザーの手に渡ると、不正な目的で使用または悪用される可能性があります。ESET NOD32アンチウイルスにはこのような脅威を検出するオプションがあります。

「潜在的に危険性のあるアプリケーション」は、市販のソフトウェアに使用される分類です。これには、リモートアクセスツール、パスワード解析アプリケーション、キーロガー（ユーザーが入力した各キーストロークを記録するプログラム）などのプログラムが含まれます。

コンピューターに潜在的に危険性のあるアプリケーションが存在して実行されている（しかも、自分ではインストールしていない）ことに気づいた場合には、ネットワーク管理者に連絡するか、そのアプリケーションを削除してください。

6.1.7 望ましくない可能性があるアプリケーション

望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピューターにインストールすると、インストール前とは異なる方法でシステムが動作します。最も大きな違いは次のとおりです。

●これまでに表示されたことがない新しいウィンドウが開く。
●隠しプロセスがアクティブになり、実行される。
●システムリソースの使用率が高くなる。
●検索結果が異なる。
●アプリケーションがリモートサーバーと通信する。