ESET ライセンス製品

Mac OS X用
ユーザーズガイド

本書はWindows用のユーザーズガイドの補足資料です。
章番号はWindows用のユーザーズガイドに対応しています。そのため、一部の番号が抜けて記載されていますので、ご注意ください。
本書をお読みの際は、必要に応じてWindows用のユーザーズガイドと併用してご利用ください。

目次

■導入編

■本書の表記について

○本書は、Windows用のユーザーズガイドの補足資料として作成されており、章番号は、Windows用のユーザーズガイドと対応しています。

○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マウスポインタ を合わせ、マウスの左ボタンを１度押すこと（または副ボタンのクリック）を「クリック」、素早く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、およびラジオボタンをクリックし、☑ ◉の状態にすることを「チェックを入れる」と表記しています。

○本書では、クライアントソフト「ESET Smart Security」と「ESET NOD32アンチウイルス」を総称して、「クライアントPC用ソフトウェア」と呼んでいます。

■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および名称が異なっている場合があります。また本書の内容は、予告なく変更することがあります。

導入編

導入編

[Chapter 1]
ESET ライセンス製品の概要

01-01 ESETライセンス製品の商品構成

ESETライセンス製品は、提供されるソフトウェアやユーザー（ライセンスの対象者）によって、いくつかの種類があります。本節では、ESETライセンス製品の種類と構成について説明します。

ESETライセンス製品とは？

「ESETライセンス製品」とは、ライセンス契約にもとづいて企業や団体向けに提供される、セキュリティソフトウェアおよびサービスの総称です。
下記2つのライセンス製品がシリーズの中核を成し、それぞれ「企業向け」「官公庁向け」「教育機関向け」に提供しています。

●ESET Smart Security V4.2 ライセンス
●ESET NOD32アンチウイルス V4.2 ライセンス

ESETライセンス製品のベースとなるセキュリティソフトウェア（クライアントPC用ソフトウェア）は、ESET Smart Security V4.2 Windows用プログラムとESET NOD32アンチウイルス V4.2 Windows用プログラム、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの3種類があります。

ESET Smart Security V4.2 ライセンスでは、ESET Smart Security V4.2 Windows用プログラムおよびESET NOD32アンチウイルス V4.2 Windows用プログラムとESET NOD32アンチウイルス V4.0 Mac OS X用プログラムが提供されます。ESET NOD32アンチウイルス V4.2 ライセンスでは、ESET NOD32アンチウイルス V4.2 Windows用プログラムおよびESET NOD32アンチウイルス V4.0 Mac OS X用プログラムが提供されます。

また、両ライセンス製品ともに、クライアントPCを管理するためのESET Remote Administrator V4.0 Windows用プログラムが付属しています。

なお、ESETライセンス製品として上記のほか、教育機関向けの「ESET NOD32アンチウイルス V4.2 スクールパック」、Windowsサーバー向けに個人ユーザー様もご利用いただける「ESET NOD32アンチウイルス V4.2 サーバー」もございます。

ご購入のライセンスの種類については、「ライセンス通知書」または「お手続き完了のメール」に記載されていますので、ご確認ください。

● ESET ライセンス製品の商品構成

製品名		対象ユーザー	備考
ESET Smart Security V4.2 ライセンス	企業向け	企業	・対象ユーザーが異なっても、提供されるソフトウェアの機能や性能に違いはありません。
	官公庁向け	官公庁	
	教育機関向け	教育機関	
ESET NOD32アンチウイルス V4.2 ライセンス	企業向け	企業	・対象ユーザーが異なっても、提供されるソフトウェアの機能や性能に違いはありません。
	官公庁向け	官公庁	
	教育機関向け	教育機関	
ESET NOD32アンチウイルス V4.2 スクールパック		教育機関	・ESET NOD32アンチウイルス V4.2 ライセンスと機能は同じですが、ライセンスの対象が文部科学省認可の幼稚園、小学校、中学校、高等学校、高等専門学校、養護学校、盲学校、聾学校、看護学校などの教育機関となっています。 ・ライセンス数は無制限です。 ・同一学校内(敷地内)でのご利用、およびウイルス定義データベース更新用のミラーサーバー構築が必須となります。
ESET NOD32アンチウイルス V4.2 サーバー		企業・団体および個人	・Windowsサーバー向けのライセンス製品です。 ・1ライセンスから購入可能です。 ・個人利用も可能です。 ※クライアント管理機能、ミラーサーバー機能はご利用いただけません。

提供されるソフトウェア

ESETライセンス製品は、以下のソフトウェアで構成されています。同じライセンス製品でも企業向け／官公庁向け／教育機関向けと、ライセンスの形態が異なりますが、提供されるソフトウェアの機能や性能に違いはありません。

ライセンス形態		ESET Smart Security V4.2 Windows 用プログラム	ESET NOD32 アンチウイルス (Windows 用プログラム / Mac OS X 用プログラム)	ESET Remote Administrator V4.0 Windows 用プログラム		
				ESET Remote Administrator Server (ERAS)	ESET Remote Administrator Console (ERAC)	ESET コンフィグレーションエディタ
ESET Smart Security V4.2 ライセンス	企業向け	○	○	○	○	○
	官公庁向け					
	教育機関向け					
ESET NOD32 アンチウイルス V4.2 ライセンス	企業向け	–	○	○	○	○
	官公庁向け					
	教育機関向け					
ESET NOD32アンチウイルス V4.2 スクールパック		–	○	○	○	○
ESET NOD32アンチウイルス V4.2 サーバー		–	○	–	–	–
概要		総合セキュリティソフト	ウイルス・スパイウェア対策ソフト	クライアントPCの情報収集や管理を行うためのサーバー用モジュール	ERASで収集した情報の閲覧やクライアントPCの操作を行うための管理者PC用モジュール	ESETセキュリティソフトウェアの設定を作成するためのソフトウェア

※ESET NOD32アンチウイルス V4.2 サーバーは、Windows用プログラムのみの提供となります。

※ESET Smart Security V4.2 ライセンスは、OSや用途に応じてクライアントPC用のプログラムをESET Smart Security V4.2 Windows用プログラムおよびESET NOD32アンチウイルス V4.2 Windows用プログラム、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムから選択して利用できます。

※ESET NOD32アンチウイルス V4.2 スクールパックの提供条件として、ミラーサーバーの構築が必須となります。

※ESET コンフィグレーションエディタは、ERACと一緒にインストールされます。

※ESET Remote AdministratorはWindows用プログラムのみの提供となります。

CAUTION

上記ソフトウェアは、提供されるCD-ROMからインストールできます。また、各ソフトウェアの最新版は、弊社ユーザーズサイトからダウンロードできます。

弊社ユーザーズサイト
→　http://canon-its.jp/product/eset/users/

01-02 ESETライセンス製品の機能と動作環境

ESETライセンス製品は、大きく分けて以下の3つの機能を提供します。

●クライアント用セキュリティ対策機能
●アップデート用ミラー機能
●クライアント管理機能

必要とする機能を検討し、ソフトウェアを導入します。

クライアントPC用ソフトウェアについて

対象ソフトウェア	対応 OS	概要
ESET Smart Security S	Windows	ウイルス・スパイウェア対策をはじめ、不正侵入対策、迷惑メール対策、フィッシング対策などの機能を搭載した総合セキュリティソフトウェア。
ESET NOD32アンチウイルス NW NM	Windows Mac OS X	ウイルス・スパイウェア対策などの機能を搭載したセキュリティソフトウェア。

クライアントPCにESET Smart SecurityまたはESET NOD32アンチウイルスを導入することで、ウイルスなどの脅威からコンピューターを守ります。ESET Smart Security V4.2 ライセンスにはESET NOD32アンチウイルス V4.2 Windows用プログラムおよびESET NOD32アンチウイルス V4.0 Mac OS X用プログラムが含まれていますので、ESET Smart Security V4.2 ライセンスをご契約の場合は、OSや用途に応じてESET Smart Security V4.2 Windows用プログラムとESET NOD32アンチウイルス V4.2 Windows用プログラムおよびESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのどちらでも導入することができます。

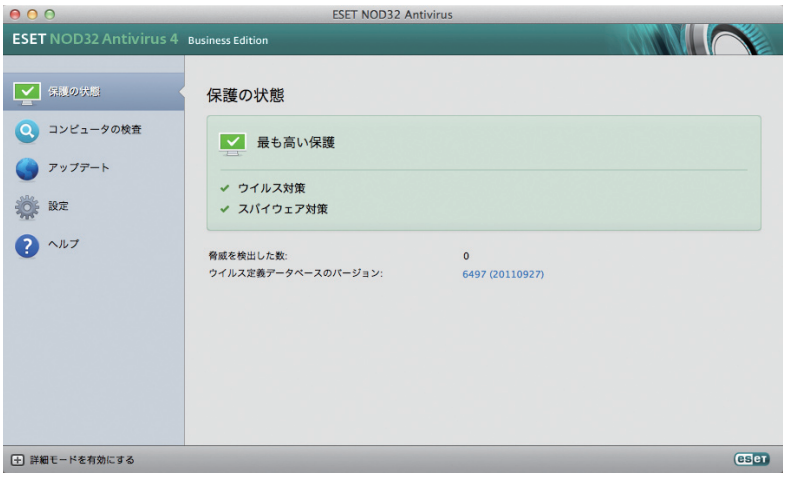
●ライセンス製品別利用可能クライアント PC 用プログラム一覧

製品名	ESET Smart Security	ESET NOD32アンチウイルス	
	Windows 用	Windows 用	Mac OS X 用
ESET Smart Security V4.2 ライセンス	○	○	○
ESET NOD32 アンチウイルス V4.2 ライセンス	–	○	○

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの機能

独自技術でウイルス対策を強化

高性能なヒューリスティック機能を持つThreatSenseテクノロジーを搭載しています。新種や亜種のウイルスに対しては遺伝子技術を応用したヒューリスティック機能を用い、既知のウイルスに対してはウイルス定義データにて防御します。ルートキットはもちろん、マクロウイルス、ワーム、アドウェア、トロイの木馬など、あらゆるマルウェアを検出します。

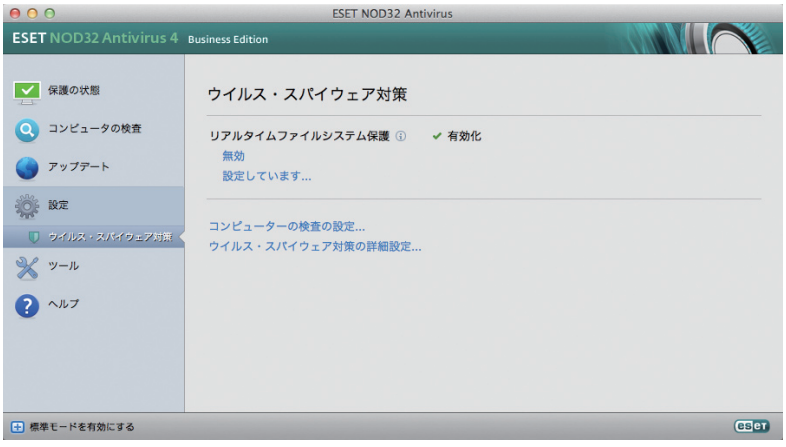


POINT

「ヒューリスティック手法」とは、ファイル内のプログラムコードを解析し、プログラムの挙動分析と動作検証を行って、ウイルス検出を行う手法です。ウイルス定義データベースを使用した検出方法だけでは、新種のウイルスは防げません。本プログラムは、これらの機能を搭載して、ウイルス対策を強化しています。

ウイルス・スパイウェア対策

ファイルやプログラムのアクセス時および実行時などにリアルタイムに検査を行う「リアルタイムファイルシステム保護」によりウイルスの侵入を防ぎます。



ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの動作環境

対応OS

Mac OS X v10.5.6 Leopard以降

Mac OS X v10.6 Snow Leopard

Mac OS X v10.7 Lion

※サーバーOSは対象外です

CPU

インテルプロセッサ（32bitまたは64bit）

※Power PCは対象外です。

メモリー

512MB 以上

ハードディスク

100MB以上の空き容量（推奨：1GB以上の空き容量）

[注意事項]
- オペレーティングシステムがあるドライブにインストールする場合は，できる限り 1GB 以上の空き容量を確保した上でインストール作業を実施してください。また，特別な理由がない限りインストール先は標準設定のままでインストールすることを推奨します。
- 他社製ウイルス対策ソフトまたは総合セキュリティソフトとの併用はトラブルの原因となるので、サポート対象外とさせていただきます。
- ESET セキュリティ製品は、完全にサポートを終了する OS でも利用できますが、できる限りセキュリティ対策が施された新しい OS へアップデートしていただくことを強く推奨します。
- 一部のメールサーバーおよびアプリケーションサーバーの環境によっては、除外設定が必要な場合があります。
- クライアント管理機能やミラーサーバー機能を利用するためには、クライアント PC がサーバーにアクセスできる必要があります。

最新の動作環境については、弊社ホームページにて必ずご確認ください。

弊社ホームページ
→ http://canon-its.jp/product/eset/license

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのクライアントPCへのインストールおよび各種設定方法は、34ページ以降を参照してください。

クライアント管理用ソフトウェアについて

対象ソフトウエア	概要
ESET Remote Administrator V4.0 Windows 用プログラム ERA	管理サーバーおよびウイルス定義データベースなどのアップデートに必要なミラーサーバーの構築に利用します。

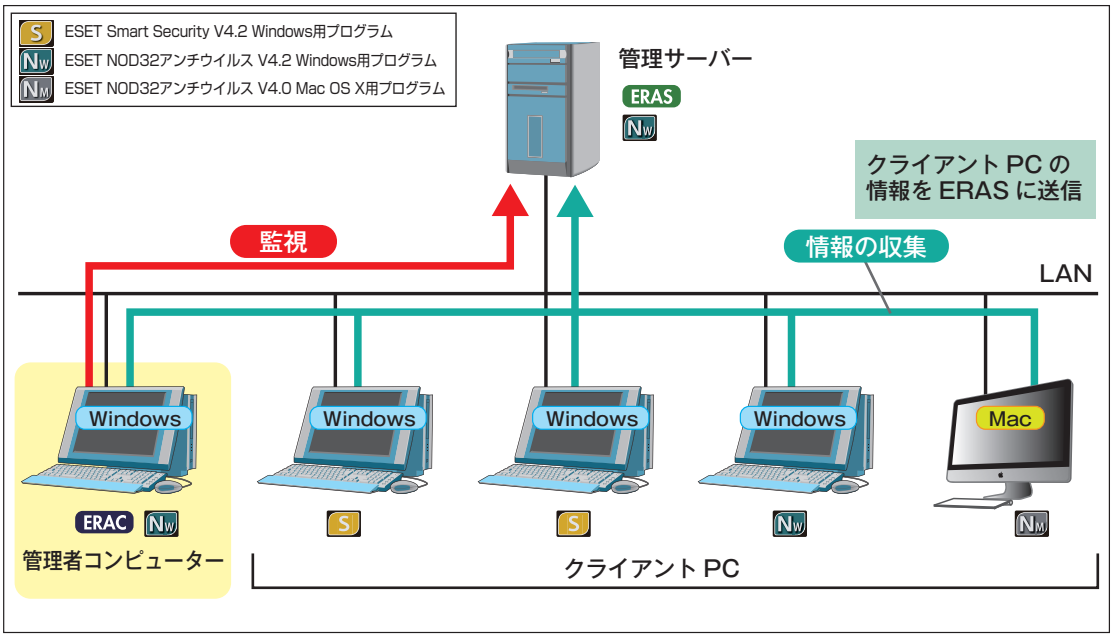
▼

ERA を構成するソフトウェア	
ESET Remote Administrator Server ERAS	クライアントPCとのデータのやり取りを行う管理サーバー用ソフトウェア。
ESET Remote Administrator Console ERAC	ERASで収集した各種情報の閲覧やクライアントPCなどに対する設定、操作を行う管理者PC用ソフトウェア。
ESET コンフィグレーションエディタ	ESETセキュリティソフトウェアの設定ファイルの作成・編集を行うためのソフトウェア。ERACと一緒にインストールされます。

ESETライセンス製品には、クライアント管理用ソフトウェアであるESET Remote Administrator V4.0 Windows用プログラムが付属しています。WindowsサーバーにERAを導入することで、クライアントPCの一元管理やウイルス定義データベース更新用のミラーサーバーの構築が行えます。

クライアント管理機能 ERA

ERAを利用して管理サーバーを構築することで、クライアントPCのセキュリティ情報の収集･閲覧や、設定変更などの一括管理が行えます。詳細はWindows用のユーザーズガイド 導入編をご参照ください。



ミラーサーバー機能

対象ソフトウェア	概要
ESET Remote Administrator V4.0 Windows 用プログラム ERA	ERA は管理サーバーの機能だけでなく、ミラーサーバー機能も有しています。
ESET NOD32アンチウイルス V4.2 Windows用プログラム NW	ESET NOD32アンチウイルス V4.2 Windows用プログラムはクライアントPC用ソフトウェアとしてセキュリティ対策機能を提供しますが、ミラーサーバー機能も有しています。管理サーバーを設置しないような環境では、ERAを導入しなくてもESET NOD32アンチウイルス V4.2 Windows用プログラムをインストールしたコンピューターをミラーサーバーとして利用できます。

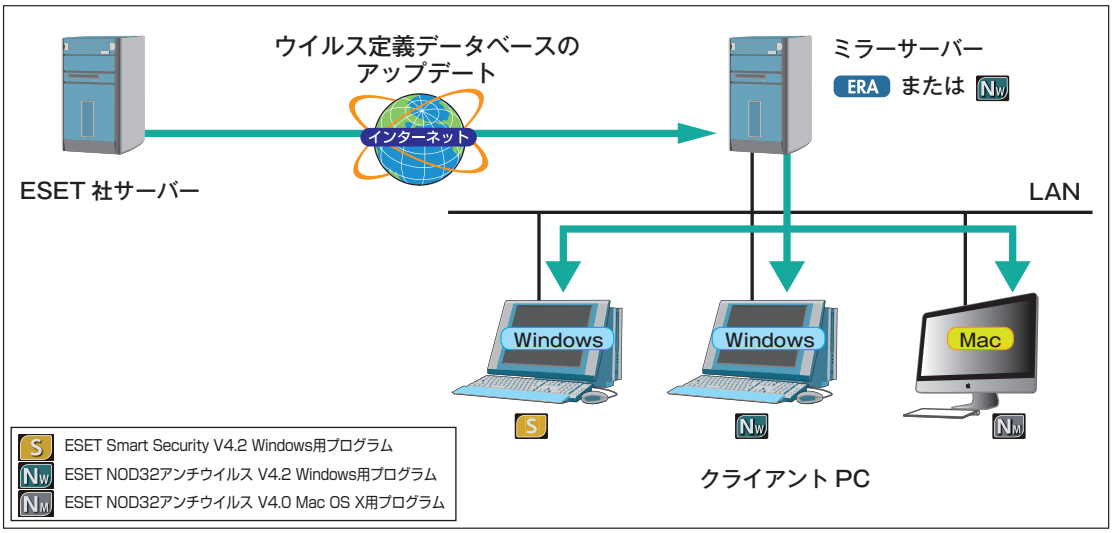
通常、ウイルス定義データベースを更新する際にクライアントPCはインターネットを通じてESET社からファイルをダウンロードします。LAN内にウイルス定義データベースのミラーサーバーを構築することによって、クライアントPCはインターネットへのアクセスを行わずにLAN内に設置されたミラーサーバーからウイルス定義データベースを取得できます。

ミラーサーバーを構築するには、ERAまたはESET NOD32アンチウイルス V4.2 Windows用プログラムを利用します。また、Microsoft Internet Information Services（IIS）と組み合わせることで、大規模構成のミラーサーバーとしても運用できます。詳細はWindows用のユーザーズガイドをご参照ください。

ミラーサーバーを構築することにより、以下のような利点があります。

●インターネット側のネットワーク負荷が軽減

●インターネットへ直接アクセスできないクライアントのアップデートが可能



CAUTION

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、ミラーサーバー機能を搭載していません。ミラーサーバーの構築には、ERAまたはESET NOD32アンチウイルス V4.2 Windows用プログラムが必要になります。

ESET NOD32アンチウイルス V4.2 Windows用プログラムとの違いについて

クライアントPC用ソフトウェアとして提供されているESET NOD32アンチウイルスは、Windows用プログラムとMac OS X用プログラムがあります。ここでは、両者の機能の違いについて説明します。

●保護機能

Windows用プログラムでは、複数の機能でクライアントPCを保護するのに対し、Mac OS X用プログラムでは基本的にリアルタイムファイルシステム保護のみでクライアントPCを保護します。Windows用プログラムにあってMac OS X用プログラムにない機能は、リアルタイムファイルシステム保護が補います。

●ERAからのリモートインストール

Windows用プログラムは、ERAを使用することでクライアントPC対してリモートインストールを行えますが、Mac OS X用プログラムでは、この機能に対応していません。Windows用プログラムにおける設定済みパッケージ（設定組み込み済みインストーラー）の作成はMac OS X用プログラムのインストーラーで行います。また、リモートインストールは、Apple社が販売する有償のリモート管理ソフト「Apple Remote Desktop」などを利用して行います。

●ミラーサーバー作成機能

Windows用プログラムでは、ミラーサーバー作成機能が搭載されていますが、Mac OS X用プログラムには、ライセンスキー登録機能がなく、ミラーサーバー作成機能は搭載されいません。

●ウイルス定義データベースのアップデート

Windows用プログラムでは、HTTP接続、共有フォルダー、USBメモリーなどに保存したローカルファイルからウイルス定義データベースのアップデートが行えますが、Mac OS X用プログラムでは、HTTP接続のみをサポートし、共有フォルダー/ローカルファイルからのアップデートには対応していません。

●主な機能の違い

	Windows 用	Mac OS X 用
オンデマンド検査	○	○
リアルタイムファイルシステム保護	○	○
Web アクセス保護	○	−
電子メール保護	○	−
ドキュメント保護	○	−
未感染ファイルのキャッシュ	−	○
メインウィンドウへのドラッグ＆ドロップによるフォルダー / ファイルの検査	−	○
ERA を使用したリモート管理	○	○
ERA を使用したリモートインストール	○	−
ERA を使用した設定組み込み済みインストーラー作成	○	−
付属のインストーラーを利用した設定済みパッケージの作成	−	○
ミラーサーバー作成機能	○	−
共有フォルダー / ローカルフォルダーからのアップデート機能	○	−
メールソフトウェアの統合	○	−
アップデートプロファイル	○	−
メール通知（警告と通知）	○	−
システムアップデートの通知	○	−
ESET SysInspector	○	−
ESET SysRescue	○	−

01-03 ライセンスについて

ライセンスの提供

ESETライセンス製品のライセンスは、「ライセンスキーファイル」により提供いたします。ライセンスの詳細やライセンスキーファイルの取得・登録方法などについては、Windows用のユーザーズガイド 導入編をご参照ください。
また、ESETライセンス製品のライセンス数は、以下のようにカウントされます。

ESET Smart Security V4.2 Windows用プログラム ESET NOD32アンチウイルス V4.2 Windows用プログラム ESET NOD32アンチウイルス V4.0 Mac OS X用プログラム	クライアントPC、サーバーに関わらず、導入したコンピューター 1台につき1ライセンスとしてカウントされます。
ESET Remote Administrator V4.0 Windows用プログラム	ERAS・ERAC共に、導入に際してライセンス数としてカウントされません。

なお、Mac用プログラムには、ライセンスキーファイルの登録機能はありません。

導入編

[Chapter 2]
ESET ライセンス製品の導入とその際の検討事項

02-01 ESETライセンス製品の運用と構成

ESETライセンス製品は、クライアントPC用ソフトウェアとクライアント管理ソフトウェアで構成されます。本節では、クライアントPC用ソフトウェアにESET NOD32アンチウイルス V4.0 Mac OS X用プログラムを利用する場合の運用方法について説明します。ESETライセンス製品の運用方法の詳細につきましては、Windows用のユーザーズガイド 導入編をご参照ください。

運用と構成方法の検討

ESETライセンス製品の運用方法には、クライアントPC用ソフトウェアのみの運用と、管理サーバーやミラーサーバーを設置した運用があります。本製品の導入にあたっては、最初にクライアント数を考慮し、管理サーバーやミラーサーバーの必要性などについて検討を行ってください。

クライアント管理機能導入の検討

クライアント管理用ソフトウェア「ESET Remote Administrator V4.0 Windows用プログラム」を利用することで、クライアントPCのウイルス警告やイベントログなどの情報の取得や各種設定の配布が行えます。ERAの導入は必須ではありませんが、WindowsおよびMac OS Xを搭載したクライアントPCのセキュリティ管理を一元化できるので、クライアント数が多い場合はERAを導入することをお勧めします。

また2台以上の管理サーバーがある場合は、「複製機能」により各種データを集約することもできます。

なお、ERAの対応OSは、Windowsのみです。Mac OS Xでは動作しません。ERAを使用する場合は、Windowsが必要になります。

ミラーサーバー機能導入の検討

ミラーサーバーを設置すると、クライアントPCはインターネットへのアクセスを行わずに、LAN内に設置されたミラーサーバーからウイルス定義データベースなどのアップデートファイルを取得できます。ミラーサーバーは、ESET Remote Administrator V4.0 Windows用プログラムやESET NOD32アンチウイルス V4.2 Windows用プログラムまたはIISで構築できます。

また、アップデートファイルの配布方法には、HTTP経由のアップデート、共有フォルダーを利用したアップデート、リムーバブルメディアを利用したアップデートがありますが、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、HTTP経由のアップデートのみに対応します。クライアントPCにMac OS XとWindowsが混在する環境でミラーサーバーを構築する場合は、この点に留意し、HTTP経由でアップデートが行えるミラーサーバーを必ず、1台以上設置してください。

サーバー動作環境／接続するクライアント数とネットワーク環境の検討

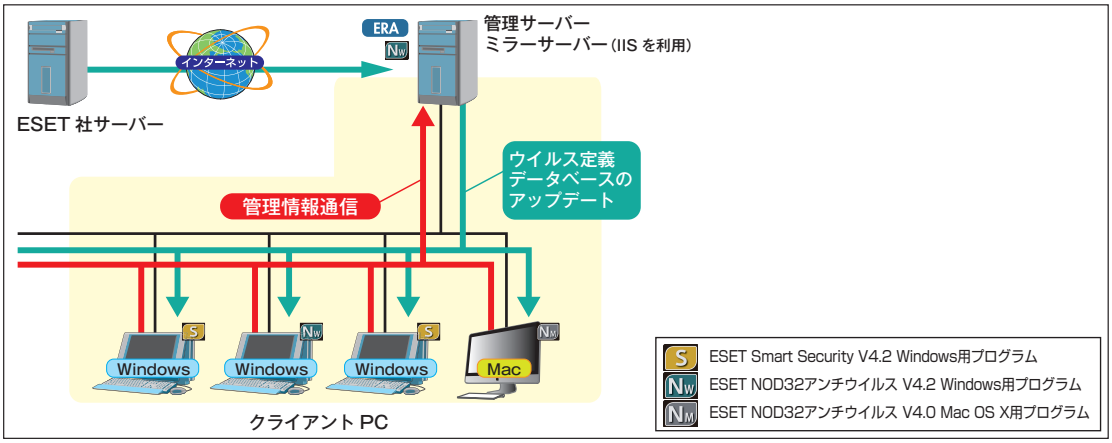
管理サーバーやミラーサーバーを設置して運用する場合、注意しなければならないのがサーバーやネットワークに対する負荷の集中です。管理サーバーは、各クライアントPCの情報を収集するため定期的にクライアントPCとの通信を行います。そのため、クライアントの情報取得頻度を上げたり、同じ情報取得頻度でもクライアント数が増加するとそれだけサーバーやネットワークへの負荷が高まります。また、ウイルス定義データベースは頻繁に更新されるため、ミラーサーバーと兼用している管理サーバーは、管理サーバー機能のみで運用している場合よりも負荷が高くなります。
サーバーのスペックが予想される負荷に耐え得るか、負荷を分散させるために2台以上のサーバーを導入するかなどの点を検討します。

POINT

ERAを導入したり、ミラーサーバーを設置する場合は、そのサーバーに接続するクライアント数を必ず確認してください。クライアント数が増加するとサーバー負荷が高くなります。運用の目安となるユーザー数と構成例はWindows用のユーザーズガイド導入編で詳細に紹介していますので、そちらを参考にサーバーのスペックをご検討ください。

サーバー構成のモデルケース
クライアントPCにMac OS Xがある場合

1台のサーバーで、管理サーバー兼ミラーサーバーとして運用します。
ミラーサーバーには、Microsoft Internet Information Services（IIS）を利用します。このモデルケースにおける接続クライアント数の上限は2,000台です。
このモデルケースでは管理機能をERAが、ミラー機能をESET NOD32アンチウイルス V4.2 Windows用プログラム（もしくはERA）が担います。



構成

- ●1台のサーバーで管理サーバーとミラーサーバーを運用
- ●ミラーサーバーは、Microsoft Internet Information Services（IIS）を利用してアップデートファイルを配布
- ●データベースは、Microsoft SQL Server 2005 Standard Editionを利用

クライアント数の目安

- ●～2,000台

サーバースペック

- ●インテル Core 2 Duo　2.4GHzと同等以上の性能を有したDual Core以上のCPU
- ●4GB以上のメモリー
- ●100Mbpsまたは1Gbpsのネットワークアダプター
- ●6GB以上のHDD空き容量

クライアントの接続間隔

- ●管理サーバーへの接続間隔：30分
- ●ミラーサーバーへの接続間隔：360分

CAUTION

上記は、参考値です。管理可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定により異なります。なおサーバーへの負荷が高い場合には、管理サーバーとミラーサーバーを 別々に設置することをお勧めします。

02-06 移行プランの検討

移行プランの検討では、既存ソフトウェアの削除方法や導入するクライアントPC用ソフトウェアの導入方法を検討し、具体的な移行プランを作成します。以下の点に着目して検討を行ってください。

チェックポイント

①他社製ソフトウェアのアンインストール方法の検討

現在利用している他社製セキュリティソフトウェアのアンインストール方法を確認します。一般的には、以下の方法でアンインストールできます。

●手動アンインストール
●他社製ソフトウェアの管理サーバーからリモートアンインストール
●開発元から提供されている削除ツールを利用してアンインストール

②クライアントPC用ソフトウェア導入方法の検討

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをクライアントPCにインストールする方法を、規模やネットワーク環境に合わせて検討します。

インストール方法には、手動インストールとApple社が販売する有償のリモート管理ソフト「Apple Remote Desktop」などを利用したリモートインストールがあります。また、付属のインストーラー(.dmg)は、管理サーバーへの接続設定やウイルス定義データベースのアップデート設定などの項目を事前に設定しておいた設定済みパッケージ(.pkg)を作成する機能を搭載しています。この機能を利用して作成した設定済みパッケージ(.pkg)を手動インストールやリモートインストールで利用すると、導入後の初期設定などの作業を軽減できます。

導入編

[Chapter 4]
ミラーサーバーの導入

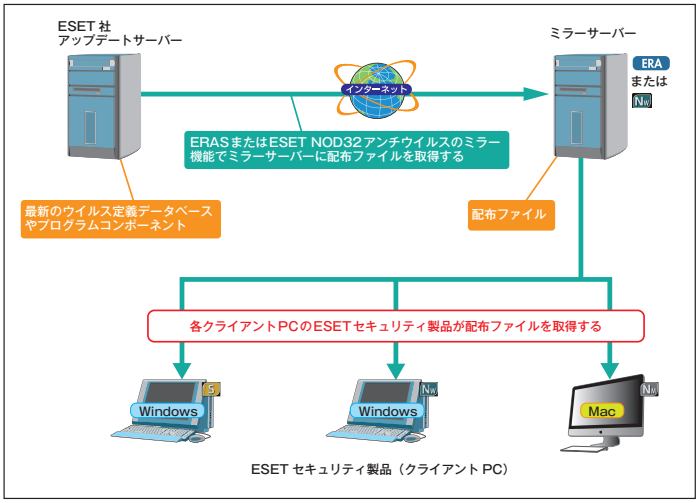
04-01 ミラー機能とは

ミラー機能とは、ESET社がインターネット上で提供するアップデートサーバーを複製したサーバーを社内に設置することで、各クライアントPCがインターネットに接続することなく、ウイルス定義データベースの更新を行える機能です。本節では、ミラーサーバー利用時のアップデート方法について説明します。

ミラーサーバー利用時のアップデート方法について

ミラーサーバーを設置した場合のアップデートファイルの配布方法には、HTTP経由、共有フォルダー、リムーバブルメディアの利用の3種類がありますが、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、HTTP経由のアップデートのみに対応します。また、HTTP経由でアップデートファイルを提供するミラーサーバーの構築方法には、ESET Remote Administrator Serverを利用する方法、ESET NOD32アンチウイルス V4.2 Windows用プログラムを利用する方法、Microsoft Internet Information Services（IIS）を利用する方法があります。ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、これらすべての方法に対応しています。ミラーサーバーの詳細については、Windows用のユーザーズガイド 導入編をご参照ください。

アップデート方法	Windows 用	Mac OS X 用
HTTP 経由	○	○
共有フォルダーを利用	○	−
リムーバブルメディアを利用	○	−



ESET Smart Security V4.2 Windows用プログラム

ESET NOD32アンチウイルス V4.2 Windows用プログラム

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラム

CAUTION

ミラーサーバーの構築には、ESET Remote Administrator V4.0 Windows用プログラムやESET NOD32アンチウイルス V4.2 Windows用プログラムが必要です。ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムでは、ミラーサーバーを構築できないのでご注意ください。

04-02 HTTP経由によるアップデート ～ Mac OS X編

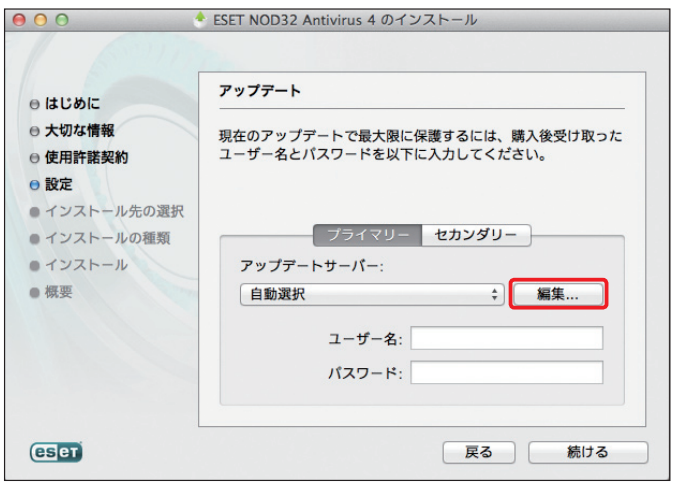
ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのアップデートファイル取得先の既定値は、「自動選択（ESET社のサーバー）」に設定されています。ミラーサーバーを利用する場合は、この設定を変更します。ここでは、ミラーサーバーを利用する場合のアップデートサーバーの設定について説明します。

アップデートサーバーの設定方法

アップデートサーバーの設定は、付属のインストーラー（.dmg）でインストールするとき（71ページの手順⑩参照）、または設定済みパッケージ（.pkg）作成時（58ページの手順⑩参照）に行えるほか、インストール後に設定できます。

インストール時または設定済みパッケージ（.pkg）作成時に変更する場合

1 設定を変更します



付属のインストーラー（.dmg）でインストールする、または設定済みパッケージ（.pkg）の作成を行うと、途中でアップデートサーバーの設定画面が表示されます。設定を変更する場合は、[編集] ボタンをクリックします。

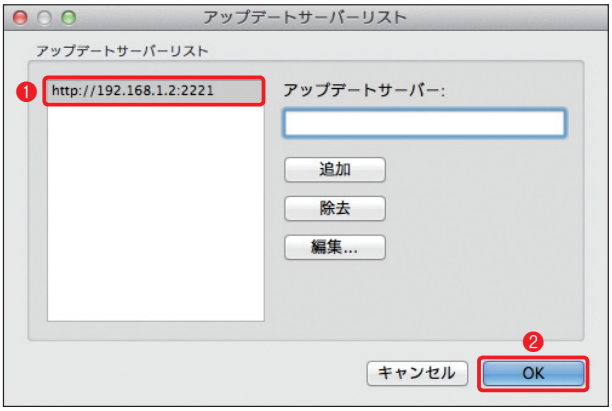
2 アップデートサーバーの情報を入力します

❶［アップデートサーバー］欄にIPアドレス（またはホスト名）とポート番号を「http://xxx.xxx.xxx.xxx:ポート番号」の形式で入力し、❷［追加］ボタンをクリックします。

POINT

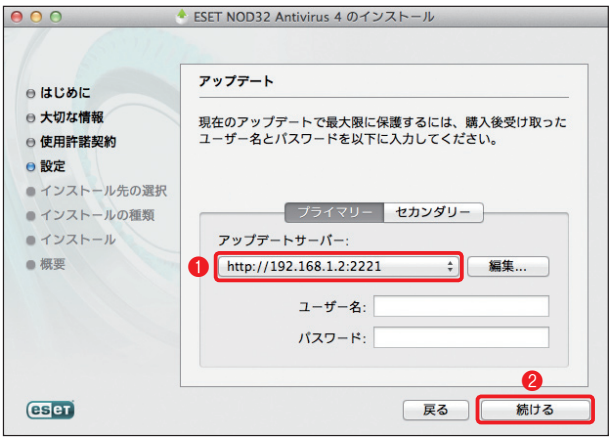
パス名まで指定されている場合は、「http://xxx.xxx.xxx.xxx:ポート番号/パス名/」の形式で入力します。「http://」を付け忘れたり、ポート番号の入力を間違えるとウイルス定義データベースのアップデートが行えないのでご注意ください。

3 アップデートサーバーの情報が登録されます



❶［アップデートサーバリスト］に登録されるので、❷［OK］ボタンをクリックします。

4 プルダウンメニューから選択します



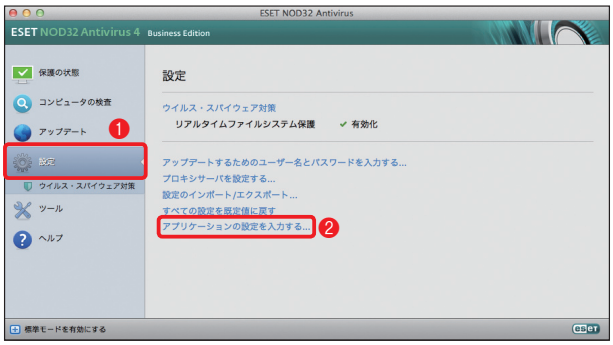
❶［アップデートサーバー］のプルダウンメニューから手順3で登録した情報を選択します。❷［続ける］ボタンをクリックします。

POINT

アップデートサーバーに接続認証が設定されているときは、「ユーザー名」「パスワード」の入力も行います。また、セカンダリーのアップデートサーバーを設定する場合は、［セカンダリー］をクリックし、同じ手順で設定を行います。

インストール後に設定を変更する場合

1 メインウィンドウを開きます

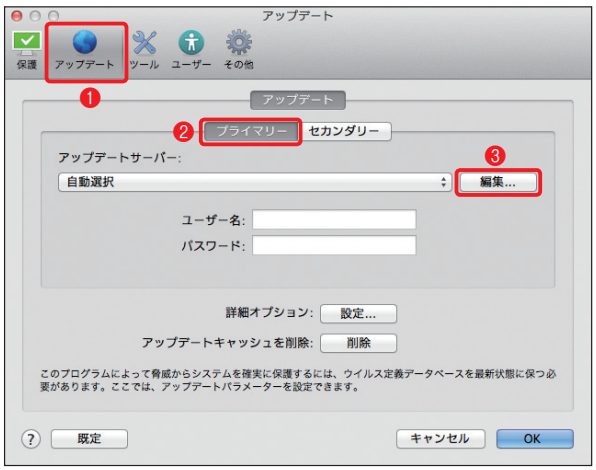


メインウィンドウを開いて、詳細モードに切り替えてから、❶[設定]ボタンをクリックし、❷[アプリケーションの設定を入力する]をクリックします。

POINT

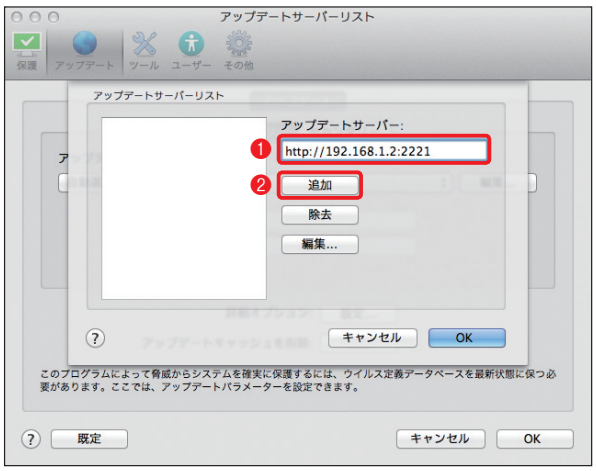
標準／詳細モードへの切り替えは、画面左下のボタンから行えます。

2 アップデートサーバーの登録します



❶[アップデート]ボタンをクリックし、❷[プライマリー]をクリックします。❸[編集]ボタンをクリックします。

3 アップデートサーバーの情報を入力します

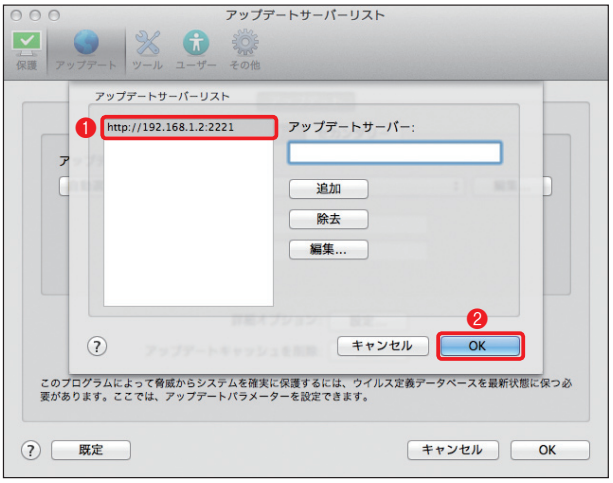


[アップデートサーバーリスト]が表示されたら、❶[アップデートサーバー]欄にIPアドレス（またはホスト名）とポート番号を「http://xxx.xxx.xxx.xxx:ポート番号」の形式で入力し、❷[追加]ボタンをクリックします。

POINT

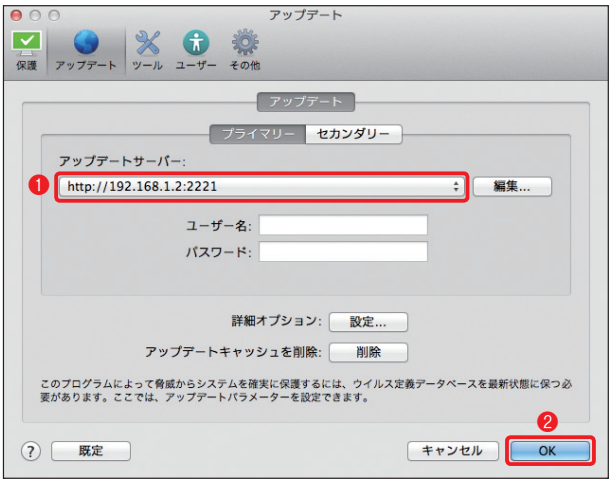
パス名まで指定されている場合は、「http://xxx.xxx.xxx.xxx:ポート番号/パス名/」の形式で入力します。「http://」を付け忘れたり、ポート番号の入力を間違えるとウイルス定義データベースのアップデートが行えないのでご注意ください。

4 アップデートサーバーの情報が登録されます



サーバー情報が❶[アップデートサーバリスト]に登録されるので、❷[OK]ボタンをクリックします。

5 プルダウンメニューから選択します



❶[アップデートサーバー]のプルダウンメニューから、手順4で設定したアップデートサーバーの設定を選択して、❷[OK]ボタンをクリックします。

POINT

アップデートサーバーに接続認証が設定されているときは、「ユーザー名」「パスワード」の入力も行います。また、セカンダリーのアップデートサーバーを設定する場合は、[セカンダリー]をクリックし、同じ手順で設定を行います。

導入編

[Chapter 5]
ESET ライセンス製品のインストールと初期設定 ～クライアント PC 用ソフトウェア編

05-01 クライアントPC用ソフトウェア導入の流れ

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、お客様の多様な環境に応じるように、いくつかのインストール方法を用意しています。本節では、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの各種インストール方法の概要および導入の流れを説明します。

インストール方法

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのインストール方法は、以下の通りです。インストールにあたっては、クライアントPCの設置環境や導入台数、運用方法などに応じて選択してください。

インストール方法	必要なファイル	特徴	参照ページ
手動インストール	付属のインストーラー（.dmg）	製品パッケージに付属するインストーラーをそのまま利用してインストールを行います。カスタムインストールを行うことで、管理サーバーやミラーサーバーへの接続設定などを行えます。	68 ページ
	設定済みパッケージ（.pkg）	アップデートサーバーへの接続設定や管理サーバーへの接続設定、権限ユーザーの設定などを行った設定済みパッケージ（.pkg）を利用してインストールを行います。設定済みパッケージ(.pkg)は、付属のインストーラー（.dmg）を利用して作成します。	63 ページ
リモートインストール	設定済みパッケージ（.pkg）	Apple 社のリモート管理ソフト「Apple Remote Desktop」などを利用して、リモートインストールを行います。インストールには、付属のインストーラー（.dmg）で作成した設定済みパッケージ（.pkg）が必要です。アップデートサーバーへの接続設定や管理サーバーへの接続設定、権限ユーザーの設定などを事前に行っておくことができます。	85 ページ

手動インストールする場合の導入の流れ

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムを手動でインストールする場合は、以下の流れで行います。他社製のセキュリティソフトウェアを利用している場合は、必ず、そのソフトウェアのアンインストールを行ってから、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのインストールを実施してください。

STEP1 他社製セキュリティソフトのアンインストール

他社製のセキュリティソフトウェアを利用している場合は、そのソフトウェアのアンインストールを行います。

↓

STEP2 設定済みパッケージの作成（必要に応じて） → 55 ページ参照

付属のインストーラー（.dmg）を利用して、アップデートサーバーへの接続設定や管理サーバーへの接続設定、権限ユーザーの設定などを行った設定済みパッケージ（.pkg）を作成します。

↓

STEP3 イントール作業の実施 → 63 ページまたは 68 ページ参照

STEP2 で作成した設定済みパッケージ（.pkg）や付属のインストーラー（.dmg）を利用して、各クライアントが手動でインストールします。

↓

STEP4 設定ファイルの配布 → 75 ページまたは 83 ページ参照

ERA を利用して各種設定をクライアント PC に配布するか、ESET NOD32アンチウイルス V4.0 Mac OS X 用プログラムからエクスポートした設定ファイルを利用して、クライアント PC の各種設定を変更します。

リモートインストールする場合の導入の流れ

Apple社が販売しているMac OS X用のリモート管理ソフト「Apple Remote Desktop」などを利用すると、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをリモートインストールできます。Apple Remote Desktopを利用する場合は、以下の流れで行います。

STEP1　他社製セキュリティソフトのアンインストール

他社製のセキュリティソフトウェアを利用している場合は、そのソフトウェアのアンインストールを行います。

↓

STEP2　クライアント PC の設定

クライアント PC を Apple Remote Desktop でリモート管理できるように設定を変更します。詳しい設定については、Apple Remote Desktop の取り扱い説明書をご参照ください。

↓

STEP3　設定済みパッケージの作成　→ 55 ページ参照

付属のインストーラー（.dmg）を利用して、アップデートサーバーへの接続設定や管理サーバーへの接続設定、権限ユーザーの設定などを行った設定済みパッケージ（.pkg）を作成します。

↓

STEP4　イントール作業の実施　→ 86 ページ参照

STEP3 で作成した設定済みパッケージ（.pkg）を Apple Remote Desktop を利用してクライアント PC にリモートインストールします。

↓

STEP5　設定ファイルの配布　→ 75 ページまたは 83 ページ参照

ERA を利用して、各種設定をクライアント PC に配布するか、ESET NOD32アンチウイルス V4.0 Mac OS X 用プログラムからエクスポートした設定ファイルを利用し、クライアント PC の各種設定を変更します。

05-02 クライアントPC用ソフトウェア設定のポイント

本節では、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムを利用する上で推奨される設定について説明します。

設定のポイントと注意点

クライアントPCでは、コンピューターの安全の維持を最優先に設定する必要があります。また、利用環境に応じた設定も重要なポイントになります。弊社では、以下のような点に着目して設定を行うことを推奨しています。

リモート管理／アップデート

管理サーバーや、ウイルス定義データベースのアップデートに利用されるミラーサーバーなどを設置する場合は、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの各サーバーへの接続に関する設定を既定値から変更する必要があります。

定期検査

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの既定値では、コンピューターの定期的な検査スケジュールは用意されていません。本製品は、定期検査のスケジュールを自由に設定できるだけでなく、検査対象とするデータなども設定できます。コンピューターの安全を維持するためにも、1週間に1回の頻度を目安に定期的な検査を実施するように設定することをお勧めします。

スケジュールされたアップデートの冗長化

コンピューターの安全を確保するには、ウイルス定義データベースの迅速なアップデートが欠かせません。ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムはスケジュールされたアップデートに対して、プライマリーとセカンダリーの2つのアップデートサーバーの設定を行えます。2つのアップデートサーバーを設定しておくことで、プライマリーのアップデートサーバーが利用できないときは、自動的にセカンダリーのアップデートサーバーに切り替えてアップデートを行います。たとえば、プライマリーに社内に設置されたミラーサーバーを、セカンダリーにESET社のアップデートサーバーを設定することで、社内で利用しているコンピューターを社外に持ち出して利用する場合でも常に最新のウイルス定義データベースが適用されます。

権限ユーザー

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、すべての設定を自由に変更できる権限ユーザーをアカウントごとに選択できます。この機能を使うと、管理者として登録された権限ユーザーのみがESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの詳細な設定を行えるようになります。

ウイルス検出時のアクション（リアルタイムファイルシステム保護）

ウイルスなどの脅威を検出した場合、既定値ではESET NOD32アンチウイルス V4.0 Mac OS X用プログラムが自動で駆除または削除を行うように設定されています。この処理は、ユーザーが毎回対処方法を選択できるように変更できます。ユーザーが処理方法を選択する場合は、ウイルスなどの脅威を検出した際に処理方法を選択する画面が表示されます。

検査対象からの除外

ユーザーが独自に開発したアプリケーションなどが、ウイルスや疑わしいファイルとして検出される場合があります。安全であると確信できるソフトウェアがウイルスとして検出された場合、該当ファイルをウイルス検査の対象から除外してください。また、該当ファイルを再び検出しないようにウイルス定義データベースを修正するためには、サポートセンターまでお問い合わせください。

ThreatSense.Net早期警告システム

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、疑わしいファイルを検出した場合に、ESET社へそのファイルの提出を求める場合があります。提出に同意すると、そのファイルをESET社に送信します。

プロキシサーバー

アップデートなどのHTTP通信がプロキシサーバーを経由する場合、この設定を行う必要があります。

05-03 設定ファイルの作成

本節では、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの設定ファイルについて説明します。

設定ファイルについて

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムに行ったサーバーへの接続設定やコンピューターの検査に関する設定などは、ファイルに保存（エクスポート）できます。また、設定を保存したファイルをESET NOD32アンチウイルス V4.0 Mac OS X用プログラムに読み込む（インポート）ことで、その設定を反映させることができます。複数のクライアントPCを運用するような場合、環境や管理・運用方法に合わせて設定ファイルをカスタマイズすることによって、より効果的な運用が可能になります。また、設定ファイルを用いることで、インストール後に行う各種設定を簡素化できます。設定ファイルは、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムを利用して作成できます。

CAUTION

設定ファイルを作成できるのは、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの権限ユーザーに登録されているユーザーのみです。権限ユーザーに登録されていないユーザーは、設定をファイルを作成できません。権限ユーザーの設定については、次ページ以降をご参照ください。

設定ファイルの制限事項

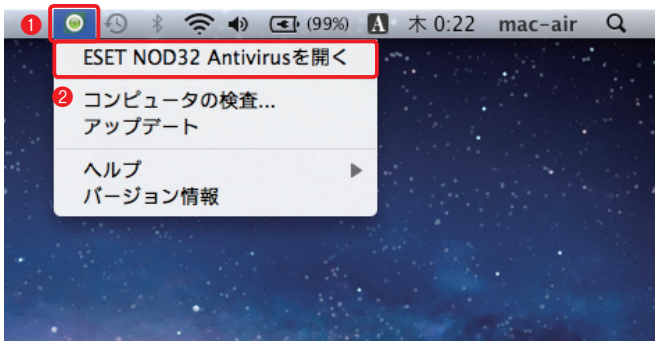
ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムで作成した設定ファイルは、ERAで利用される設定ファイル（.xml）との互換性がありません。ESET NOD32アンチウイルス V4.0 Mac OS X用プログラム同士で設定ファイルのインポート／エクスポートを行ってください。

設定ファイルの読み込みを行うと、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのすべての設定が上書きされます。権限ユーザーの設定も上書きされるのでご注意ください。

設定ファイルの作成手順

ここでは、すでに導入済みESET NOD32アンチウイルス V4.0 Mac OS X用プログラムを利用した設定ファイルの作成手順を説明します。なお、設定ファイルは権限ユーザーのみが作成できます。

1 メニューバーのアイコンをクリックします

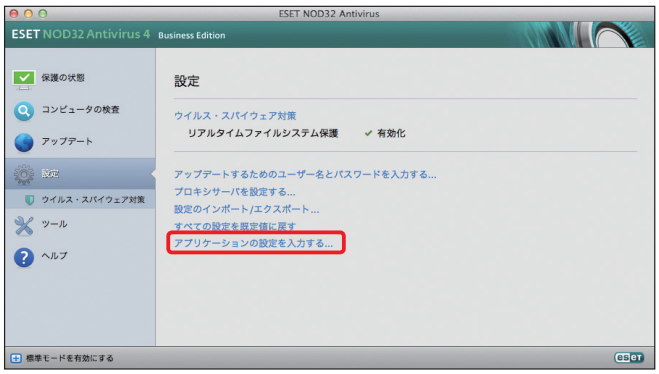


❶メニューバーにあるESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのアイコンをクリックし、❷[ESET NOD32 Antivirusを開く]をクリックします。

2 詳細モードに切り替えます

❶[設定]ボタンをクリックして、❷[詳細モードを有効にする]または[詳細モードへ切り替え]をクリックします。

3 設定を開始します



[アプリケーションの設定を入力する]をクリックします。

4 権限ユーザーの設定を行います

❶[ユーザー]ボタンをクリックし、❷[権限]をクリックします。❸権限ユーザーに登録されているユーザーをクリックして、❹[除去]をクリックします。

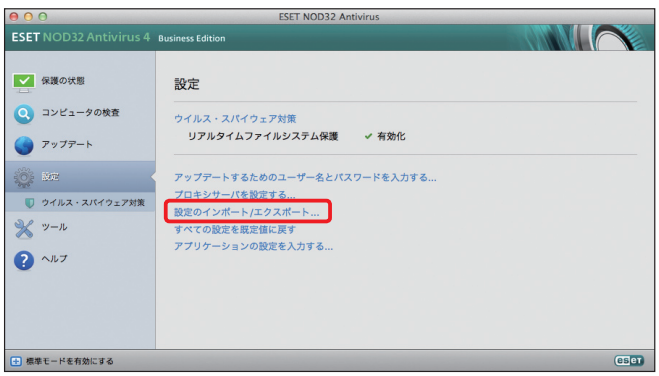
5 「全てのユーザー」を権限ユーザーにします

選択したユーザーが権限ユーザーから削除されます。手順4の作業を繰り返して、すべての権限ユーザーを削除し、❶権限ユーザーの欄に「全てのユーザー」と表示されたら、❷[OK]ボタンをクリックします。

POINT

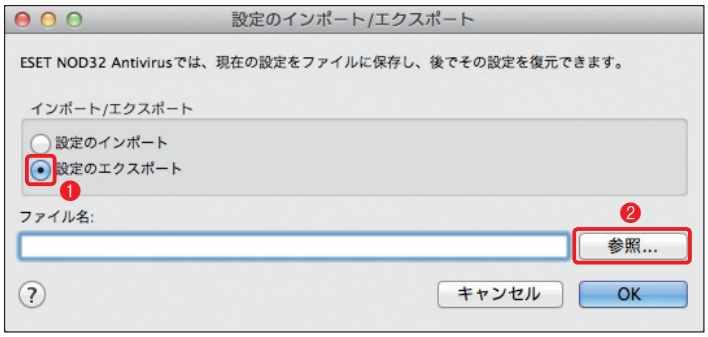
ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの他の設定例は、43ページ以降で紹介しています。実際の設定は、これを参考に行ってください。

6 設定のエクスポートを開始します



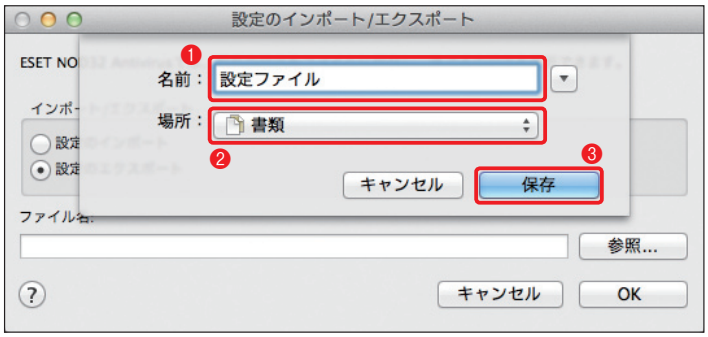
メインウィンドウに戻ります。[設定のインポート/エクスポート]をクリックします。

7 設定ファイルの保存先を設定します



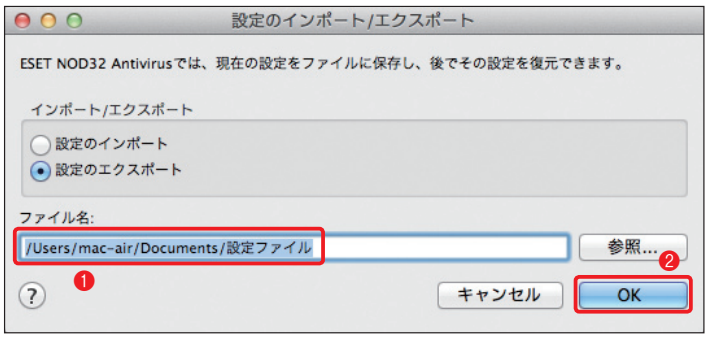
❶[設定のエクスポート]にチェックを入れ、❷[参照]ボタンをクリックします。

8 設定ファイルの保存先を選択します



❶ファイル名を入力し、❷保存先を場所のプルダウンメニューから選択します。❸[保存]ボタンをクリックします。

9 設定ファイルのエクスポートを行います



❶保存するファイルがフルパスで表示されます。❷[OK]ボタンをクリックすると、設定ファイルが保存されます。

クライアントソフトウェアの設定例

設定ファイルを作成するときは、クライアントPCにインストールされているESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの設定を直接編集します。ここでは、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをコンピューターにインストールしたときの設定例を説明します。実際の設定を行う際の参考にしてください。

●クライアント PC に必要な設定例

設定内容	概要	参照ページ
リモート管理	ERAS への接続設定です。この設定を行うことで、クライアント PC と管理サーバー間の情報の送受信ができます。	45 ページ
アップデート ～アップデート先 (ミラーサーバー) の設置	ウイルス定義データベースなどのアップデートを行うための設定です。ミラーサーバーを設置している場合、ミラーサーバーの IP アドレスなどを設定します。また、最新のウイルス定義データベースを適用するために、プライマリー、セカンダリーのアップデートサーバーを設定できます。プライマリー、セカンダリーの両方を設定しておくと、プライマリーのサーバーに接続できないときに、自動的にセカンダリーのサーバーに接続を試みます。これによって、社内 / 社外を気にすることなく、常に最新のウイルス定義データベースを使用できます。	45 ページ
定期検査	コンピューターの定期的な検査スケジュールや検査対象とするデータなどを設定します。	47 ページ
権限ユーザー	管理者などの特定のユーザーのみが詳細な設定を行えるようにします。	49 ページ
ウイルス検出時のアクション (リアルタイムファイルシステム保護)	ウイルスなどの脅威を検出した際の対処方法を設定します。	51 ページ
検査対象からの除外	一部のアプリケーションソフトウェアは、ウイルスや疑わしいファイルとして誤検出される場合があります。その際の対処方法を設定します。	51 ページ
ThreatSense.Net 早期警告システム	疑わしいファイルを検出した際に、ESET 社へそのファイルの提出が求められる場合があります。その際の対応を設定します。	53 ページ
プロキシサーバー	アップデートなどの HTTP 通信がプロキシサーバーを経由する場合、この設定を行う必要があります。	53 ページ

クライアントPCに必要な各設定の変更手順

ここでは、43ページで取り上げた設定項目を変更する手順を説明します。ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの詳細設定は、以下の手順で設定画面を開いて行います。また、定期検査の設定などの一部は、スケジューラで設定を行います。なお、これらの設定は権限ユーザーで行います。

設定画面の開き方

1 メニューバーのアイコンをクリックします

❶メニューバーにあるESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのアイコンをクリックし、❷[ESET NOD32 Antivirusを開く]をクリックします。

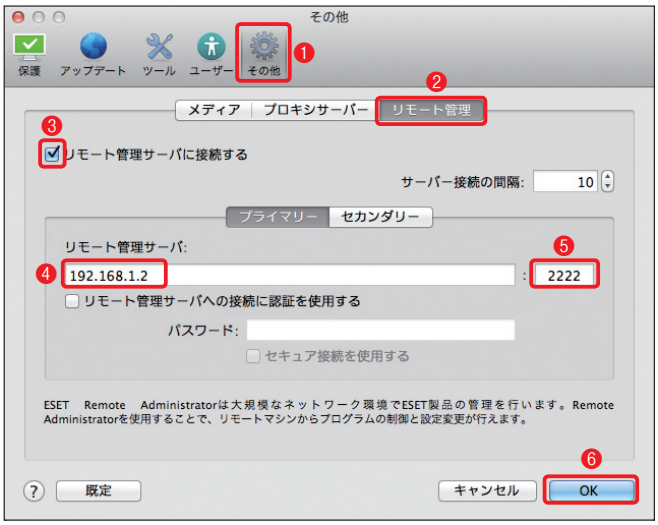
2 詳細モードに切り替えます

❶[設定]ボタンをクリックして、❷[詳細モードを有効にする]または[詳細モードへ切り替え]をクリックします。

3 設定を開始します

[アプリケーションの設定を入力する]をクリックします。

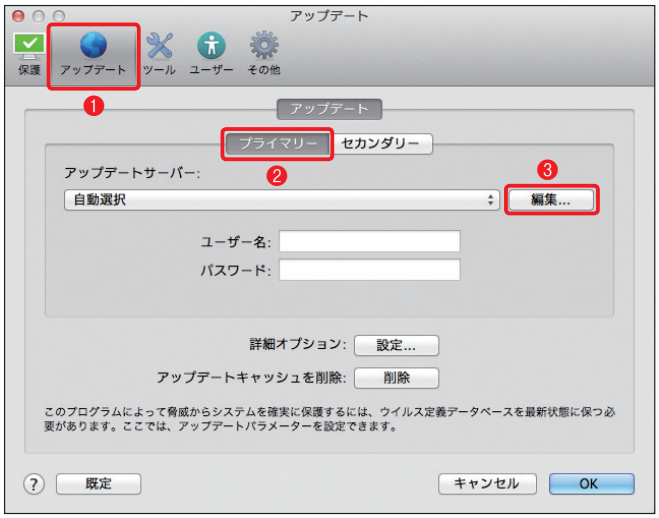
リモート管理～管理サーバーへの接続設定



管理サーバーへの接続設定は、❶[その他]ボタンをクリックし、❷[リモート管理]をクリックします。設定を行う場合は、❸[リモート管理サーバに接続する]にチェックを入れ、❹[リモート管理サーバ]に管理サーバーのIPアドレス(またはホスト名)、❺[ポート]にポート番号を入力し、❻[OK]ボタンをクリックします。

アップデート～アップデート先(ミラーサーバー)の設定

1 アップデート先を設定します

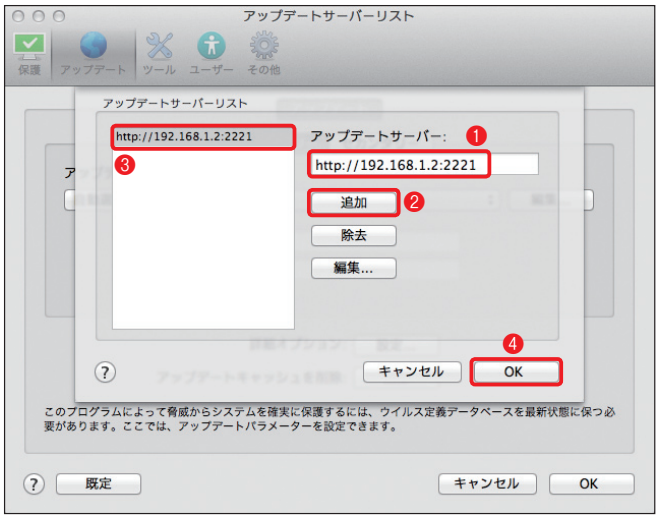


アップデート先(ミラーサーバー)の設定は、❶[アップデート]ボタンをクリックします。設定を行う場合は、❷[プライマリー]をクリックし、❸[編集]ボタンをクリックします。

POINT

プライマリーに社内に設置されたミラーサーバーを設定し、セカンダリーを[自動選択]に設定して、「ユーザー名」と「パスワード」を入力しておくと、PCを社外に持ちだしたときなどミラーサーバーにアクセスできない場合は、自動的にESET社のサーバーにアクセスします。

2 サーバー情報を設定します

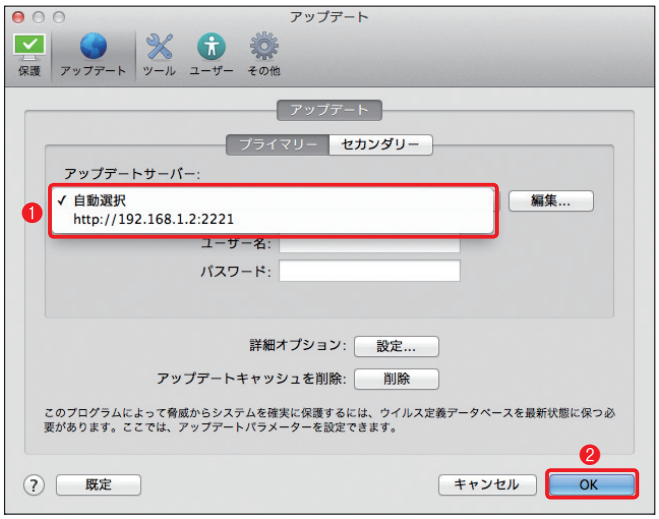


[アップデートサーバーリスト]が表示されたら、❶[アップデートサーバー]欄に接続先のサーバー情報を入力し、❷[追加]ボタンをクリックします。❸[アップデートサーバーリスト]に登録されるので、❹[OK]ボタンをクリックします。

POINT

社内に設置されたミラーサーバーを利用する場合は、IPアドレス(またはホスト名)とポート番号を「http://xxx.xxx.xxx.xxx:ポート番号」の形式で入力してください。

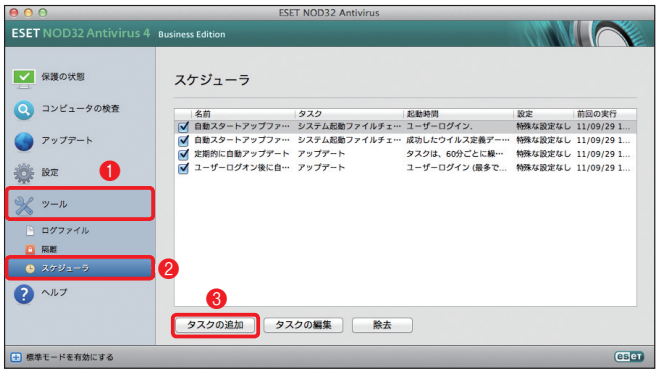
3 アップデート先を選択します



❶アップデートサーバーのプルダウンメニューから、先程設定したアップデートサーバーの設定を選択して、❷[OK]ボタンをクリックします。また、アップデートサーバーの冗長化を行うときは、[セカンダリー]をクリックして、手順1、2を参考にアップデートサーバーの設定を行います。

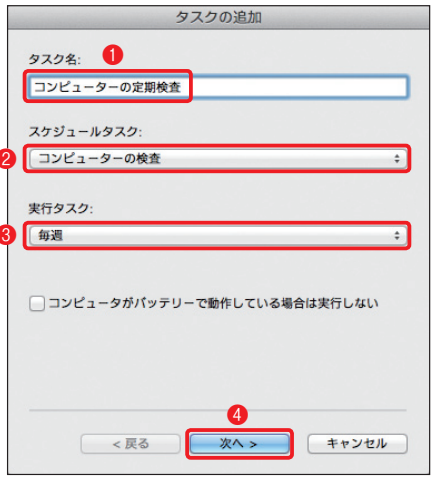
定期検査

1 定期検査の設定を行います



定期検査の設定は、❶メインウィンドウの[ツール]ボタンをクリックし、❷[スケジューラ]ボタンをクリックして[コンピュータの検査]タスクを追加することで行います。定期検査を追加するときは、❸[タスクの追加]ボタンをクリックします。

2 タスクを設定します



「タスクの追加」画面が表示されます。ここでは週に1回パソコンの検査を行うタスクを例に紹介します。❶タスク名を入力し、❷スケジュールタスクのプルダウンメニューから[コンピューターの検査]を選択して、❸[実行タスク]のプルダウンメニューから[毎週]を選択します。❹[次へ]ボタンをクリックします。

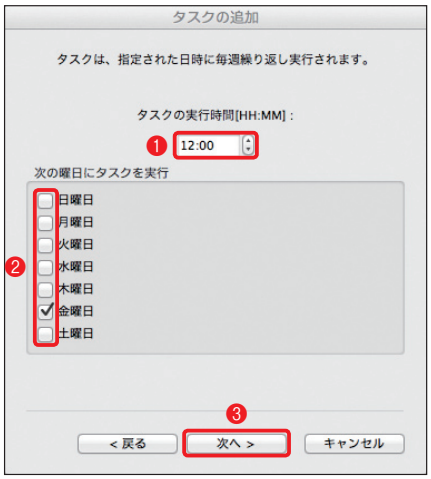
3 検査を行う場所を設定します

❶[プロファイルの選択]のプルダウンメニューから、[Smart検査]を選択し、❷起動ドライブ(ここでは、「Macintosh HD」)左のチェックボックスにチェックを入れ、❸[▶]をクリックします。

4 起動ドライブのみ検査するように設定します

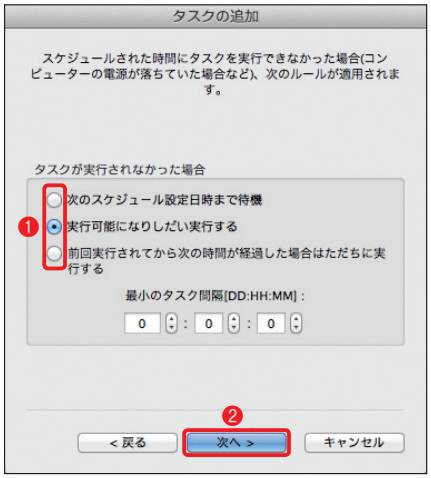
❶「検査の対象」を選択し、❷[次へ]ボタンをクリックします。

5 タスクの実行時刻と曜日を選択します



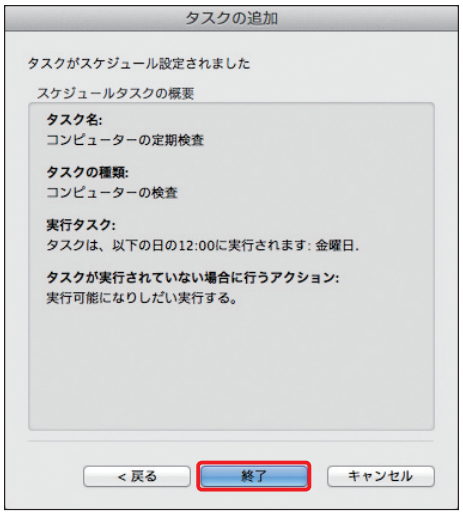
❶「タスクの実行時間」を設定し、❷実行する曜日(ここでは、「金曜日」)にチェックを入れ、❸[次へ]ボタンをクリックします。

6 タスクが実行されなかったときのアクションを選択します



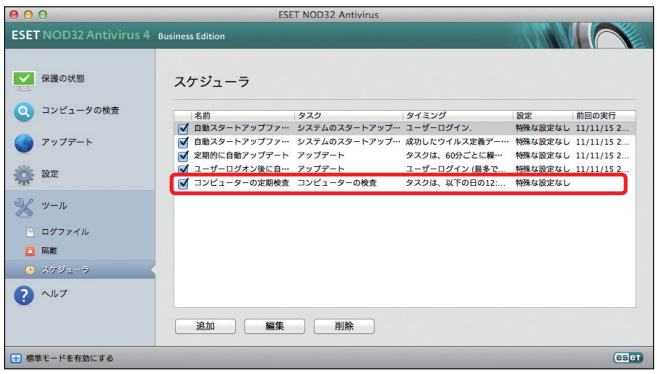
❶タスクが実行されなかったときのアクション(ここでは「実行可能になりしだい実行する」)を選択して、❷[次へ]ボタンをクリックします。

7 設定内容の確認を行います



設定に誤りがある場合は[戻る]ボタンをクリックして再設定してください。問題がなければ[終了]ボタンをクリックします。

8 スケジューラに登録されます



作成した設定(ここでは、「コンピューターの定期検査」)が、スケジューラに登録されます。

権限ユーザー

1 権限ユーザーを設定します

権限ユーザーを設定する場合は、❶[ユーザー]ボタンをクリックし、❷[権限]をクリックします。❸権限ユーザーに登録したいユーザーを「ユーザー」グループから選択し、❹[追加]ボタンをクリックします。

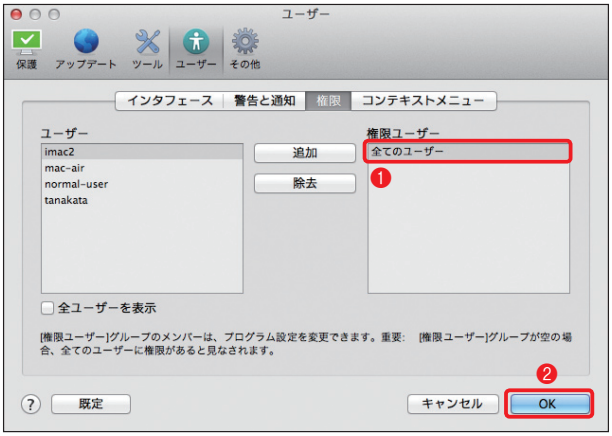
2 権限ユーザーが追加されます

❶選択したユーザーが権限ユーザーに追加されました。❷[OK]ボタンをクリックします。

3 全てのユーザーを権限ユーザーにします

全てのユーザーを権限ユーザーにする場合は、❶「権限ユーザー」グループからユーザーを選択し、❷「除去」ボタンをクリックして、全てのユーザーを除去します。

4 設定を終えます



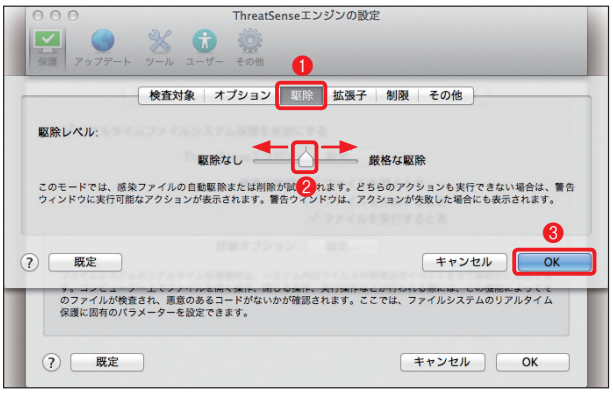
❶「権限ユーザー」グループのユーザーをすべて除去すると「全てのユーザー」に表示が変わります。❷[OK]ボタンをクリックします。

ウイルス検出時のアクション（リアルタイムファイルシステム保護）

1 ウイルス検出時のアクションを設定します

ウイルス検出時のアクションを設定する場合は、❶[保護]ボタンをクリックし、❷[リアルタイム保護]をクリックします。続いて❸[ThreatSenseエンジン]の[設定]ボタンをクリックします。

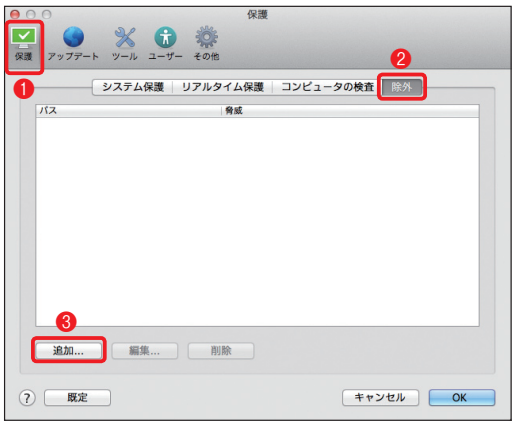
2 アクションの設定を行います



❶[駆除]をクリックし、❷スライドバーをドラッグして駆除の方法を設定します。❸[OK]ボタンをクリックします。

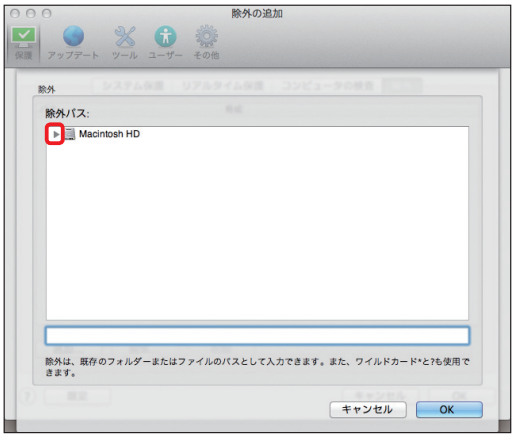
検査対象からの除外

1 除外設定を行います



検査対象からの除外の設定は、❶[保護]ボタンをクリックし、❷[除外]をクリックします。❸[追加]ボタンをクリックします。

2 フォルダー一覧を表示します

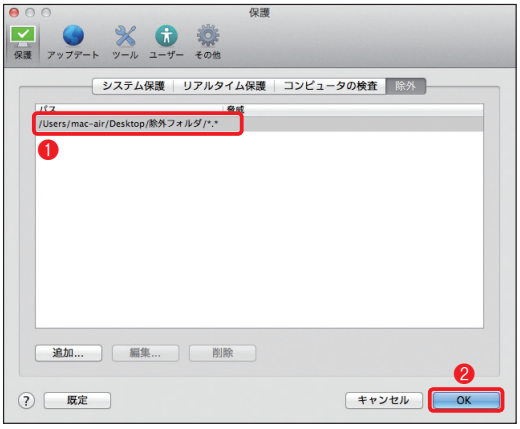


[▶]をクリックします。

3 除外したいファイル／フォルダーを選択します

❶除外したいファイル/フォルダーをクリックし、❷[OK]ボタンをクリックします。

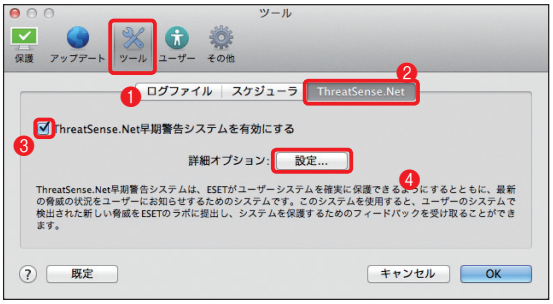
4 リストに登録されます



❶選択したファイル/フォルダーがリストに登録されます。❷[OK]ボタンをクリックします。

ThreatSense.Net早期警戒システム

1 設定を始めます

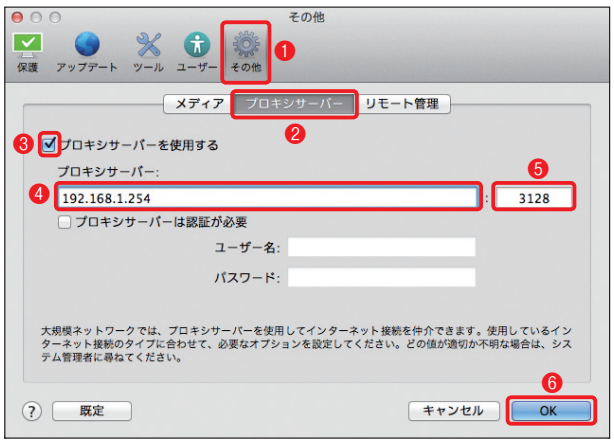


ThreatSense.Net早期警戒システムの設定は、❶[ツール]ボタンをクリックし、❷[ThreatSense.Net]をクリックします。❸この機能を利用しない場合は、[ThreatSense.Net]のチェックを外します。設定を行う場合は、❹[設定]ボタンをクリックします。

2 不審なファイルを検出したときの動作を設定します

❶[不審なファイルの提出]プルダウンメニューでは、不審なファイルの提出に関する設定が行えます。❷[匿名情報と統計情報の提出]プルダウンメニューでは、統計情報をESET社に送信するかどうかなどの設定が行えます。❸[提示配布]プルダウンメニューでは、提出先の設定が行えます。❹設定を行ったら、[OK]ボタンをクリックします。

プロキシサーバー



プロキシサーバーの設定は、❶[その他]ボタンをクリックし、❷[プロキシサーバー]をクリックします。❸[プロキシサーバーを使用する]にチェックを入れ、❹プロキシサーバーのIPアドレス(またはホスト名)を入力し、❺ポート番号を入力します。❻[OK]ボタンをクリックします。

POINT

認証が必要な場合は、[プロキシサーバーは認証が必要]にチェックを入れて、「ユーザー名」および「パスワード」も入力します。

CAUTION

外出先でアップデートを行う際など、プロキシサーバーの設定が不要になった場合は、手順❸のチェックを外してください。

05-05 手動インストール

本節では、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをクライアントPCに手動インストールする方法全般について説明します。

インストールに利用するファイルについて

手動インストールには、付属のインストーラー（.dmg）を利用する方法と設定済みパッケージ（.pkg）を利用する方法があります。両者は、それぞれ以下のような特徴があります。

インストーラーの種類	備考
設定済みパッケージ（.pkg）	付属のインストーラーを使ってユーザーが、作成するインストーラーです。手動インストールだけでなく、リモートインストールでも使用できます。以下の設定を事前に行えます。 [事前に設定可能な項目] ・アップデートサーバーへの接続設定 ・プロキシサーバーの設定 ・権限ユーザーの設定 ・リモート管理の設定
付属のインストーラー（.dmg）	本製品に付属する標準のインストーラーです。手動インストールに利用できるだけでなく、設定済みパッケージ（.pkg）作成機能も搭載します。

設定ファイルの配布

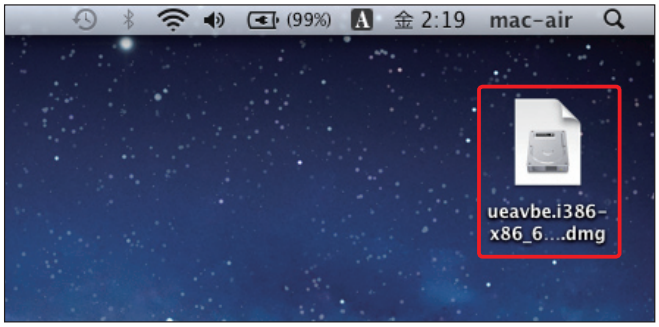
ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをインストールしたら、各種設定を行います。設定方法には、以下の方法があります。

設定方法	内容	参照ページ
ERA を利用	ERA からリモート操作で一括してクライアント PC の各種設定を変更する方法です。この方法を利用するには、ESET NOD32 アンチウイルス V4.0 Mac OS X 用プログラムをインストールした PC が管理サーバーへ接続するように設定されている必要があります。	75 ページ
設定ファイルを利用	設定ファイルを ESET NOD32 アンチウイルス V4.0 Mac OS X 用プログラムをインストールした PC で読み込むことで設定を行います。この方法を利用するには、ESET NOD32 アンチウイルス V4.0 Mac OS X 用プログラムをインストールした PC で事前に設定ファイルを作成しておく必要があります。	83 ページ

設定済みパッケージ(.pkg)の作成手順

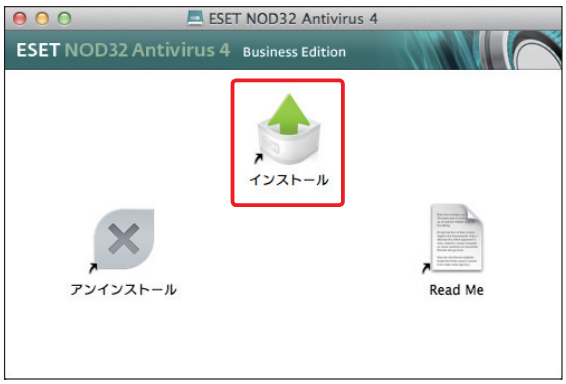
ここでは、付属のインストーラー(.dmg)を使って、アップデートサーバーや権限ユーザー、管理サーバーへの接続、などの設定を組み込んだ設定済みパッケージ(.pkg)を作成する手順を説明します。

1 インストーラーを開きます



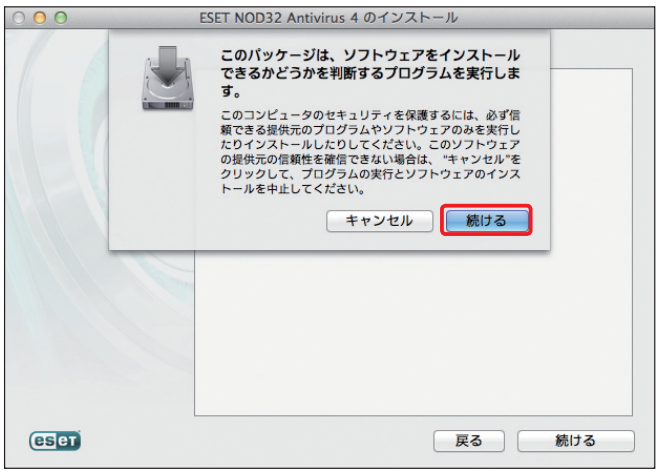
インストーラー(.dmg)をダブルクリックします。

2 インストールを開始します



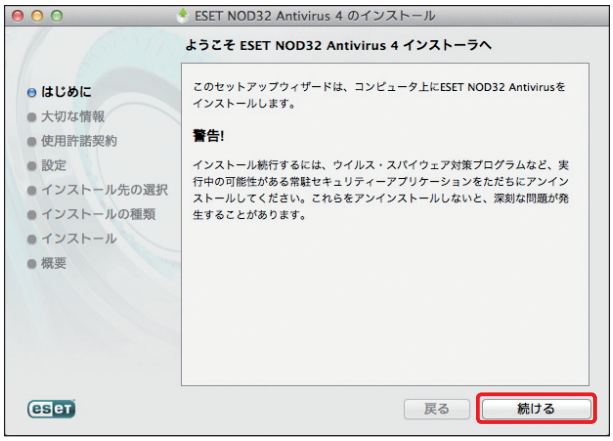
[インストール]をダブルクリックします。

3 ボタンをクリックします



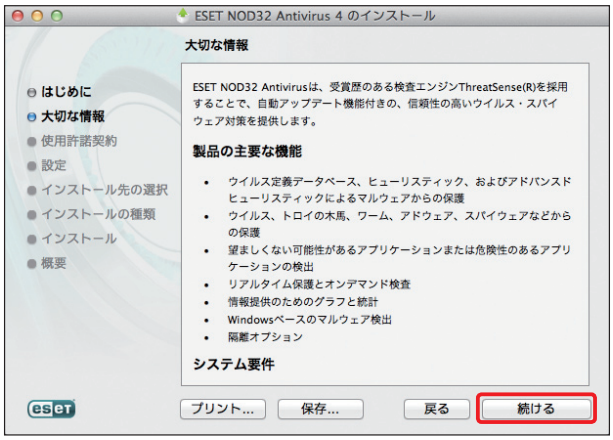
[続ける]ボタンをクリックします。

4 「はじめに」が表示されます



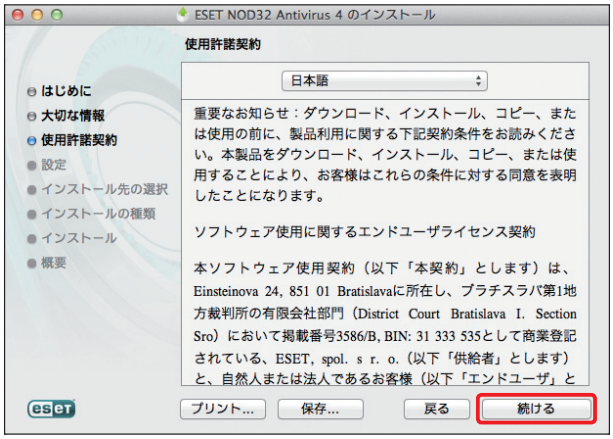
内容を確認し、[続ける]ボタンをクリックします。

5 「大切な情報」が表示されます



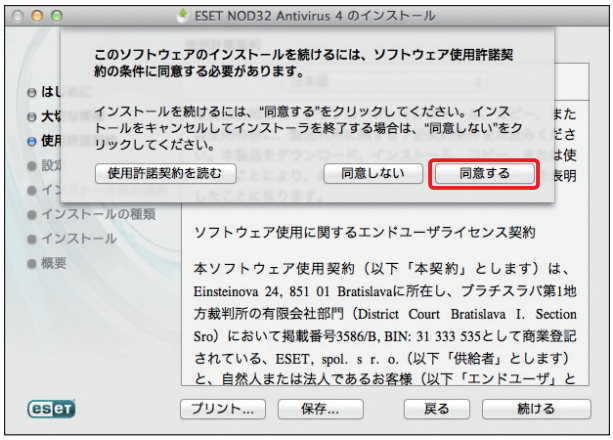
内容を確認し、[続ける]ボタンをクリックします。

6 「使用許諾契約」が表示されます



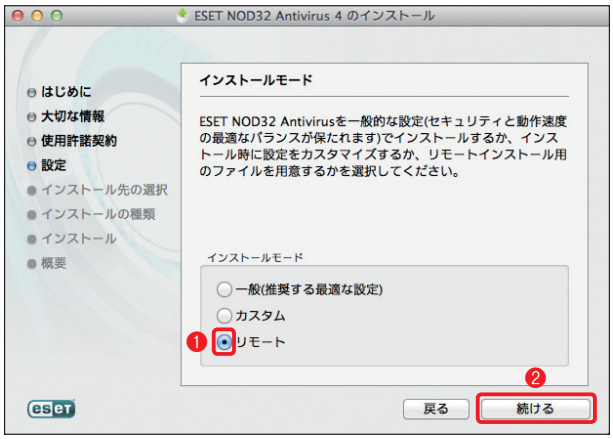
内容を確認し、[続ける]ボタンをクリックします。

7 「使用許諾契約」に同意します



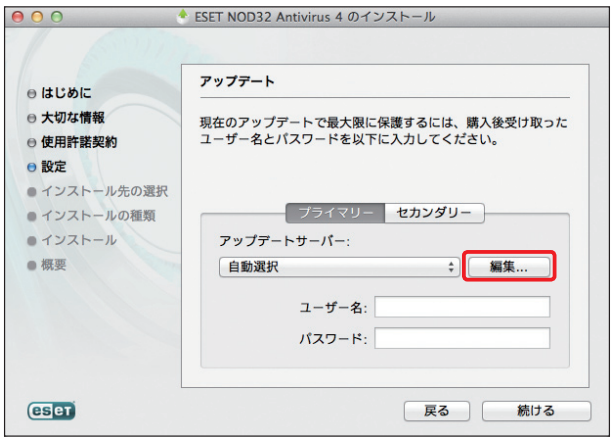
[同意する]ボタンをクリックします。

8 インストールモードを選択します



❶[リモート]にチェックを入れ、❷[続ける]ボタンをクリックします。

9 アップデートサーバーを設定をします



[編集]ボタンをクリックします。

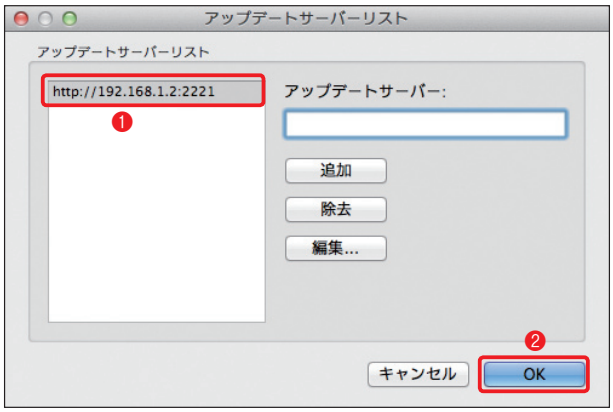
10 アップデートサーバーの情報を登録します

❶[アップデートサーバー]欄に接続先のサーバー情報を入力し、❷[追加]ボタンをクリックします。

POINT

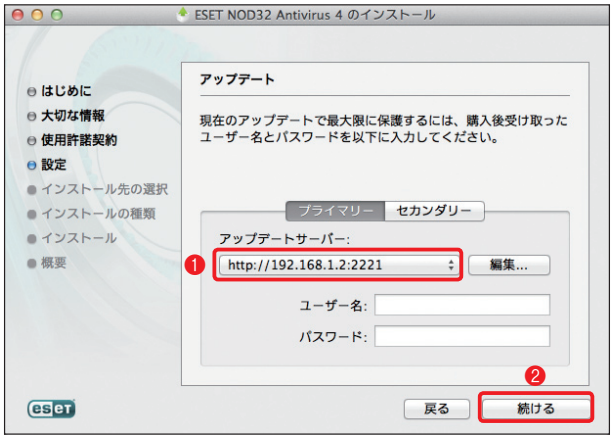
社内に設置されたミラーサーバーを利用する場合は、IPアドレス(またはホスト名)とポート番号を「http://xxx.xxx.xxx.xxx:ポート番号」の形式で入力してください。また、ミラーサーバーを使用する場合の詳細な設定については、29ページをご参照ください。

11 アップデートサーバーの登録を終了します



❶[アップデートサーバーリスト]に情報が登録されるので、❷[OK]ボタンをクリックします。

12 登録したアップデートサーバーを選択します

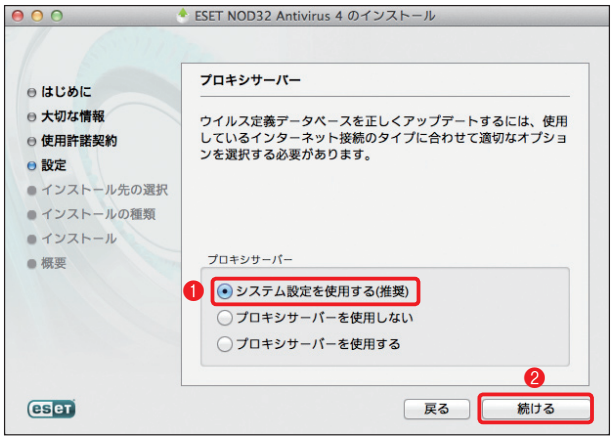


❶[アップデートサーバー]のプルダウンメニューから手順11で登録した情報を選択します。❷[続ける]ボタンをクリックします。

POINT

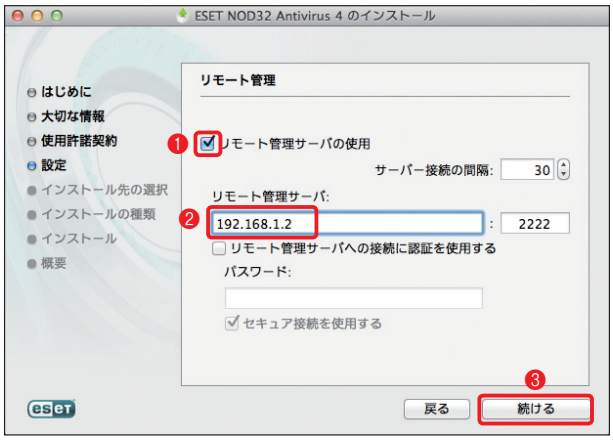
アップデートサーバーに接続認証が設定されているときは、「ユーザー名」「パスワード」の入力も行います。

13 プロキシサーバーを設定します



アップデートなどのHTTP通信がプロキシサーバーを経由する場合、この設定を行う必要があります。❶[システム設定を利用する(推奨)]にチェックが入っていることを確認し、❷[続ける]ボタンをクリックします。

14 管理サーバーの設定を行います

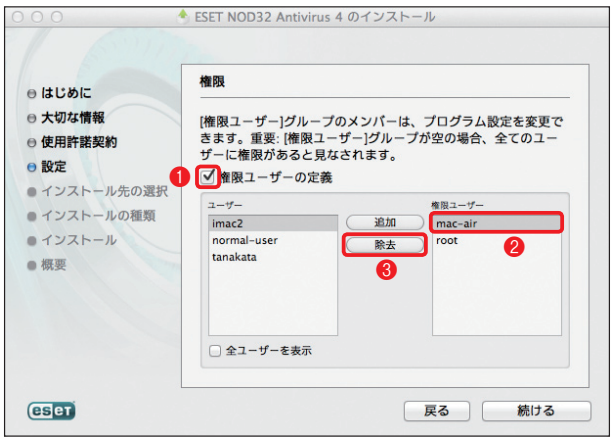


❶[リモート管理サーバの使用]にチェックを入れ、❷[リモート管理サーバ]欄にIPアドレス(またはホスト名)を入力します。❸[続ける]ボタンをクリックします。

POINT

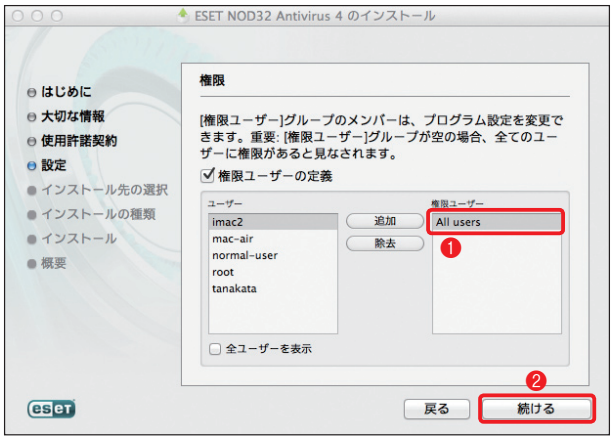
管理サーバーを利用しない場合は、この設定を行う必要はありません。

15 権限ユーザーの設定を行います



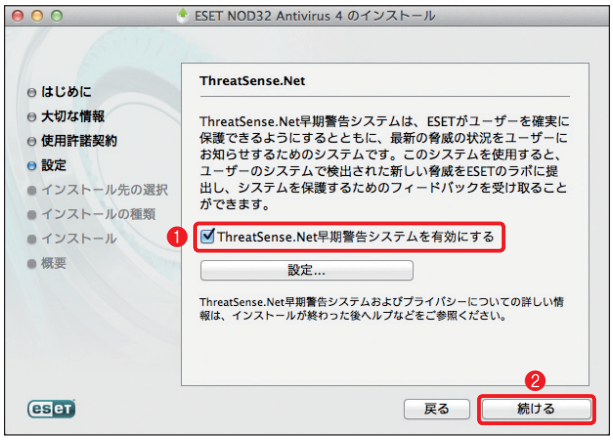
❶[権限ユーザーの定義]にチェックを入れます。❷「権限ユーザー」グループに登録されているユーザーをクリックし、❸[除去]をクリックします。手順❷❸の作業を繰り返し、すべてのユーザーを「権限ユーザー」グループから除去します。

16 すべてのユーザーを権限ユーザーに設定します



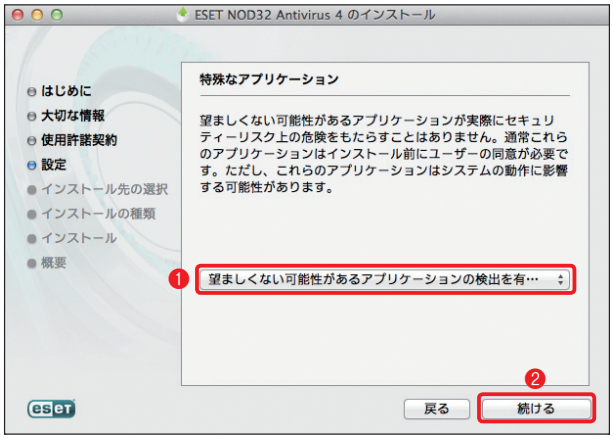
❶[権限ユーザー]グループのユーザーをすべて除去すると[All users]に表示が変わります。❷[続ける]ボタンをクリックします。

17 ThreatSense.Netの設定を行います



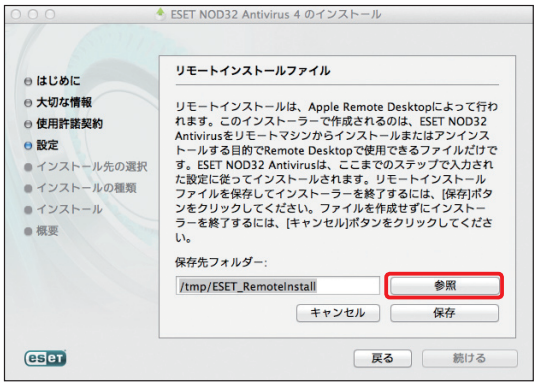
❶[ThreatSense.Net早期警告システムを有効にする]にチェックが入っていることを確認し、❷[続ける]ボタンをクリックします。

18 特殊なアプリケーションの設定を行います



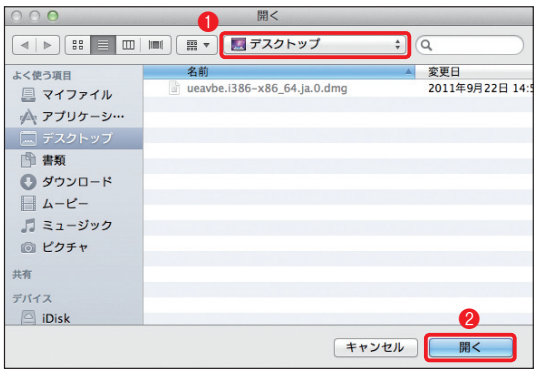
❶プルダウンメニューから[望ましくない可能性があるアプリケーションの検出を有効にする]を選択し、❷[続ける]ボタンをクリックします。

19 保存先を設定します



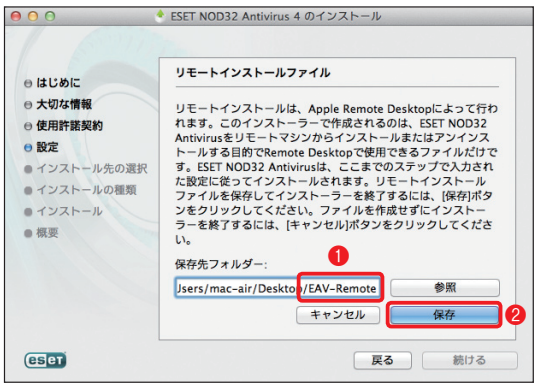
[参照]ボタンをクリックします。

20 保存先を選択します



❶保存先を選択し、❷[開く]ボタンをクリックします。

21 保存を開始します

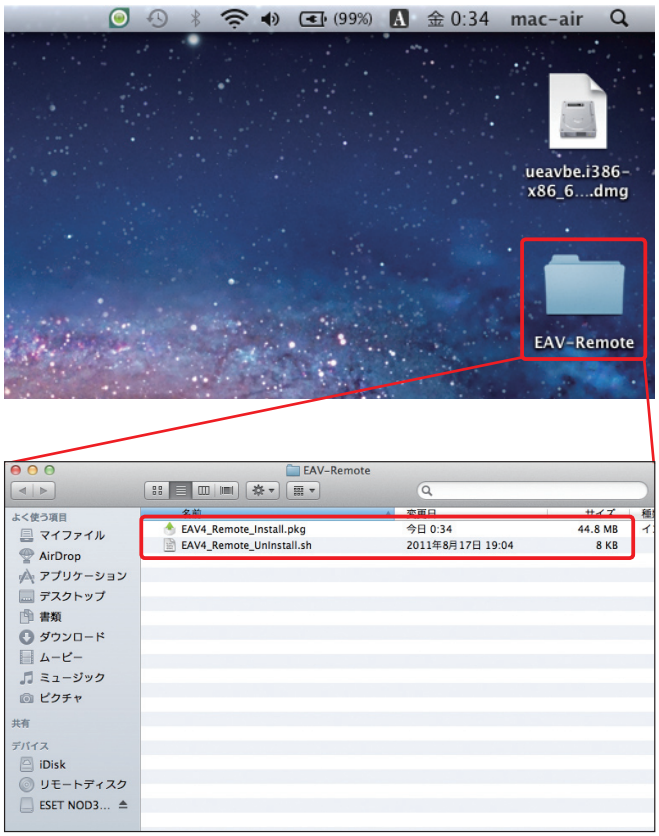


❶入力された保存先をクリックして保存するフォルダー名(ここでは、「/EAV-Remote」)を追加します。ここで入力した名称のフォルダーが保存先フォルダー内に新規作成されます。設定済みパッケージ(.pkg)は、このフォルダー内に保存されます。❷[保存]ボタンをクリックします。

POINT

手順19で[参照]ボタンをクリックして保存先を選択した場合は、保存先フォルダー名の追加入力を行わないと、設定済みパッケージ(.pkg)の作成ができません。また、既定値で設定されている「/tmp」フォルダーは、Finderの既定値では表示されないフォルダーです。「/tmp」フォルダーを表示するには、メニューバーの[移動]をクリックし、[フォルダーへ移動]を選択して[/tmp]と入力して、[移動]ボタンをクリックします。

22 設定済みパッケージ(.pkg)が作成されます

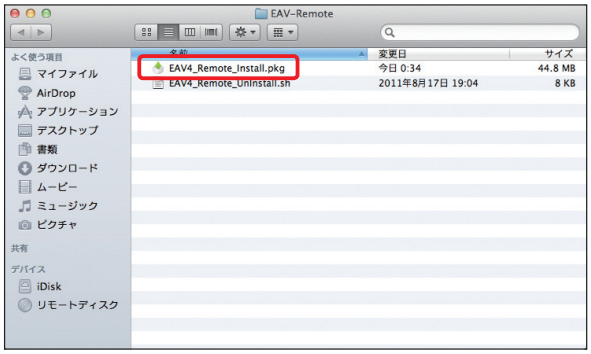


設定済みパッケージ(.pkg)が指定したフォルダー内に作成されます。「EAV4_Remote_Install.pkg」が、設定済みパッケージ(.pkg)です。「EAV4_Remote_Uninstall.sh」は、アンインストール用のシェルスクリプトです。

手動インストール手順～その1 設定済みパッケージ(.pkg)

ここでは、設定済みパッケージ(.pkg)を利用した手動インストールの手順を説明します。

1 設定済みパッケージ(.pkg)を開きます

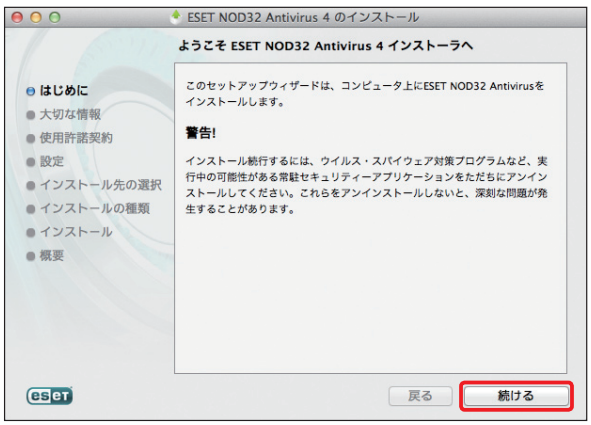


設定済みパッケージ(.pkg)をダブルクリックします。

2 インストールを開始します

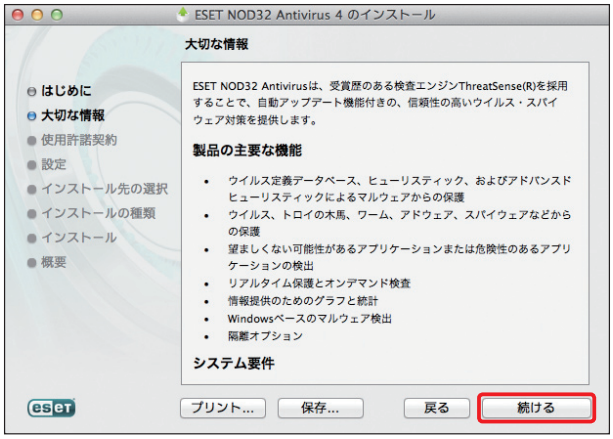
[続ける]ボタンをクリックします。

3 「はじめに」が表示されます



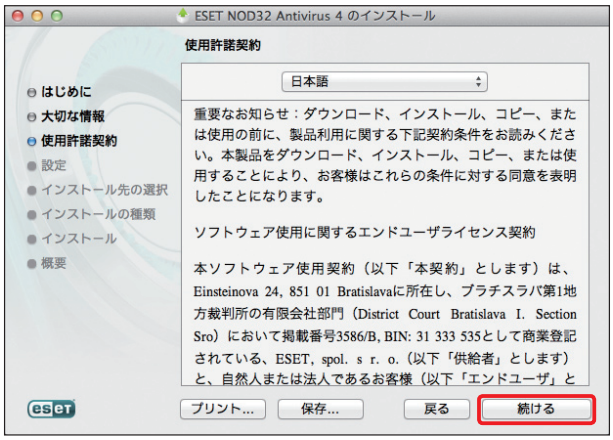
内容を確認し、[続ける]ボタンをクリックします。

4 「大切な情報」が表示されます



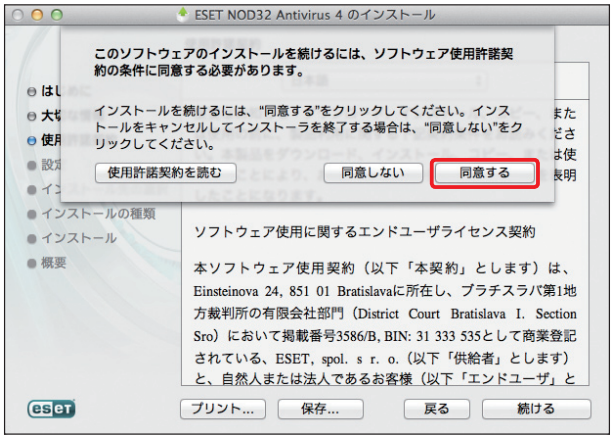
内容を確認し、[続ける]ボタンをクリックします。

5 「使用許諾契約」が表示されます



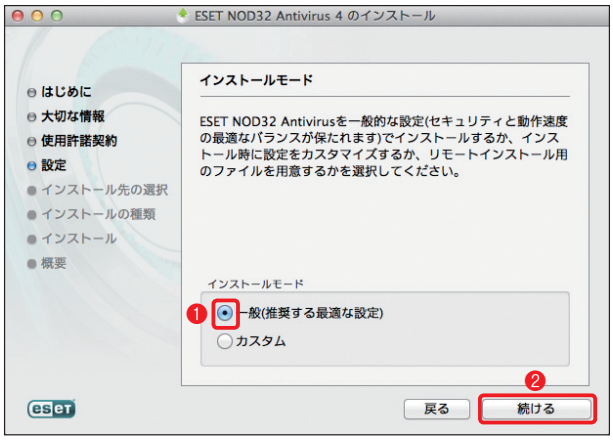
内容を確認し、[続ける]ボタンをクリックします。

6 「使用許諾契約」に同意します



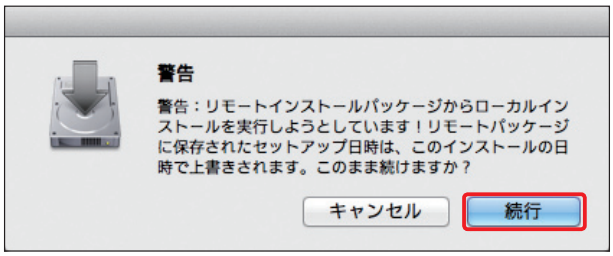
[同意する]ボタンをクリックします。

7 インストールモードを選択します



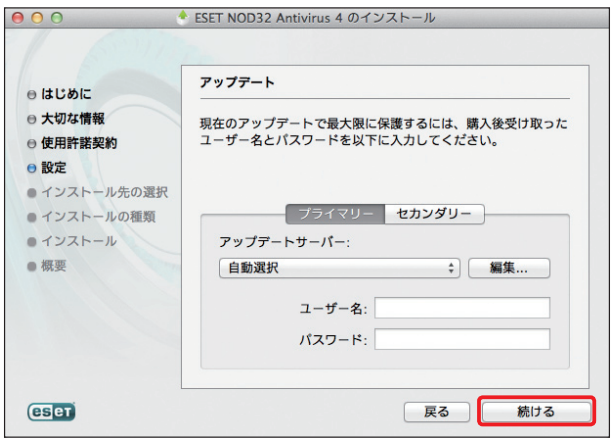
❶[一般(推奨する最適な設定)]にチェックを入れ、❷[続ける]ボタンをクリックします。

8 ダイアログが表示されます



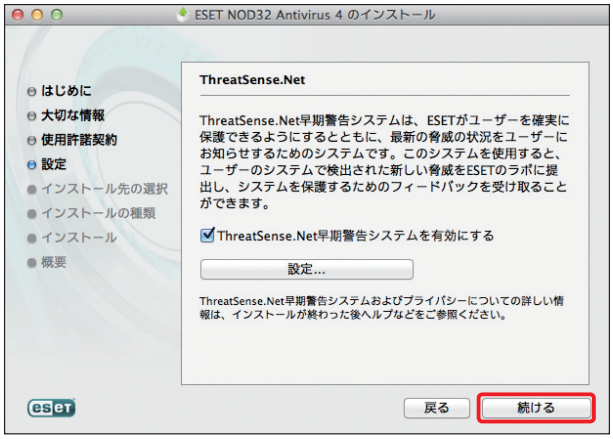
[続行]ボタンをクリックします。

9 次の設定に進みます



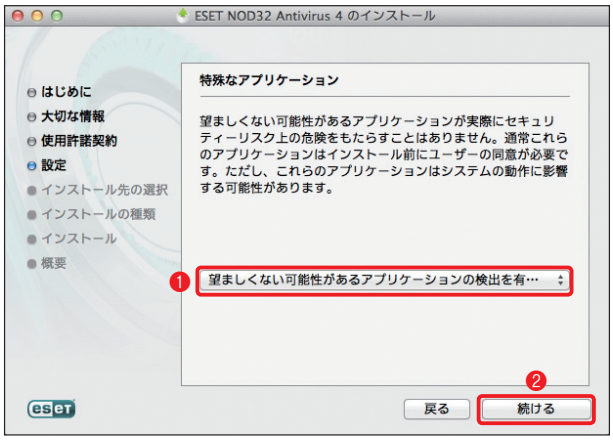
[続ける]ボタンをクリックします。設定済みパッケージ(.pkg)を利用しているときは、各種設定を行う必要はありません。設定値は表示されませんが、あらかじめ設定された内容が自動的に反映されます。

10 次の設定に進みます



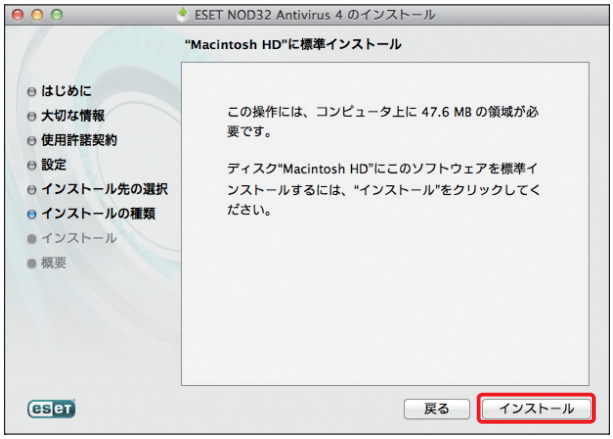
[続ける]ボタンをクリックします。

11 特殊なアプリケーションの設定を行います



❶プルダウンメニューから[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]を選択し、❷[続ける]ボタンをクリックします。

12 インストールを開始します

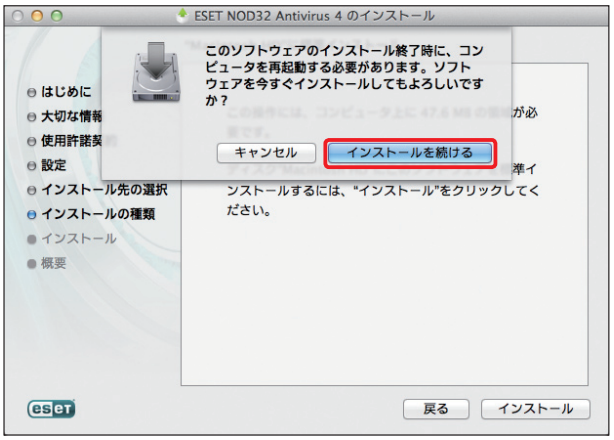


[インストール]ボタンをクリックします。

13 管理者アカウントを入力します

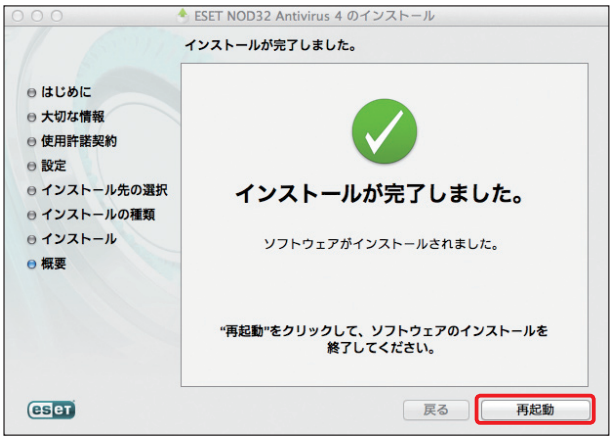
❶管理者アカウントの[名前]と[パスワード]を入力し、❷[ソフトウェアをインストール]ボタンをクリックします。

14 インストールを続行します



[インストールを続ける]ボタンをクリックします。

15 インストール作業が完了しました



インストールが始まり、進捗状況が表示されます。「インストールが完了しました。」と表示されたら、インストールは終了です。[再起動]ボタンをクリックして、PCを再起動します。

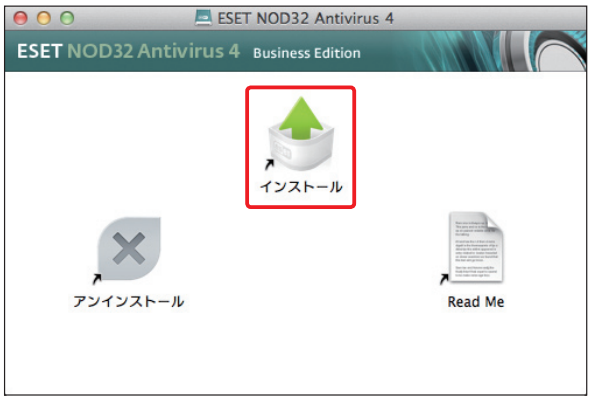
手動インストール手順～その２
付属のインストーラー（.dmg）

ここでは、管理サーバーを利用していることを前提に付属のインストーラー（.dmg）を利用した手動インストールの手順を説明します。

1 インストーラーを開きます

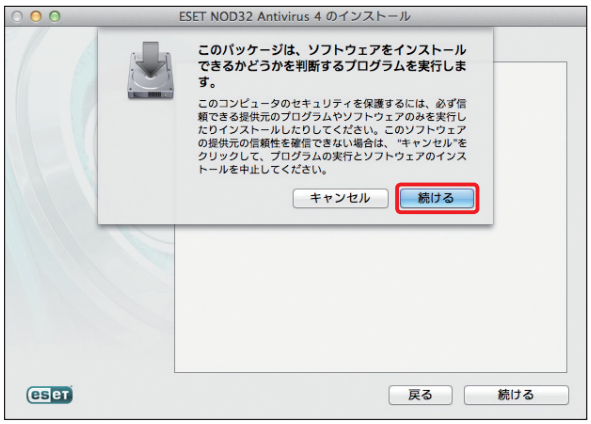
インストーラー(.dmg)をダブルクリックします。

2 インストール作業を始めます



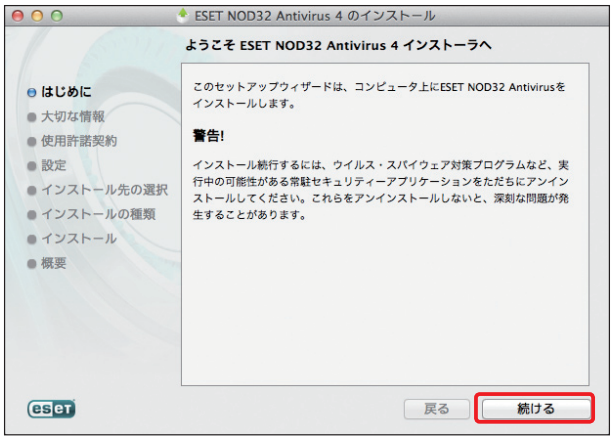
[インストール]をダブルクリックします。

3 インストーラーが起動します



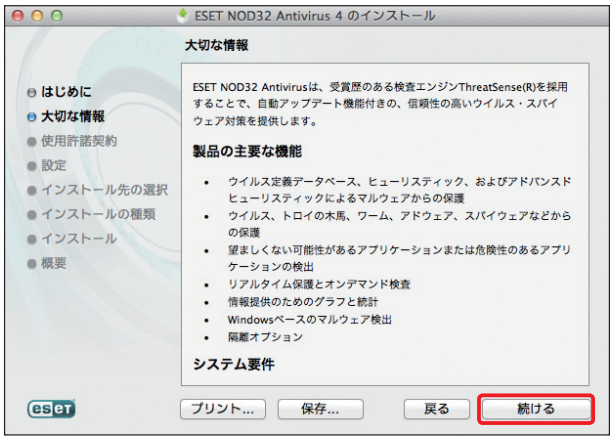
[続ける]ボタンをクリックします。

4 「はじめに」が表示されます



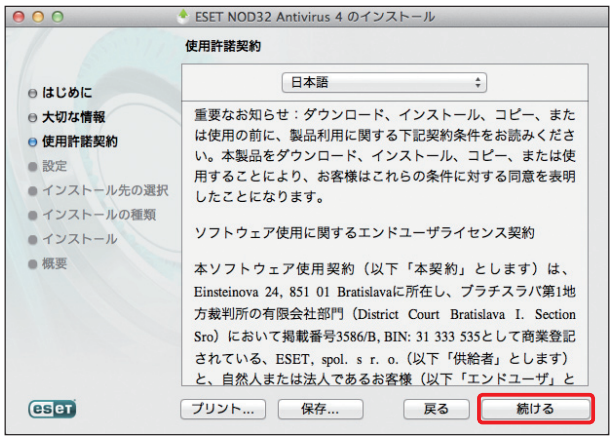
内容を確認し、[続ける]ボタンをクリックします。

5 「大切な情報」が表示されます



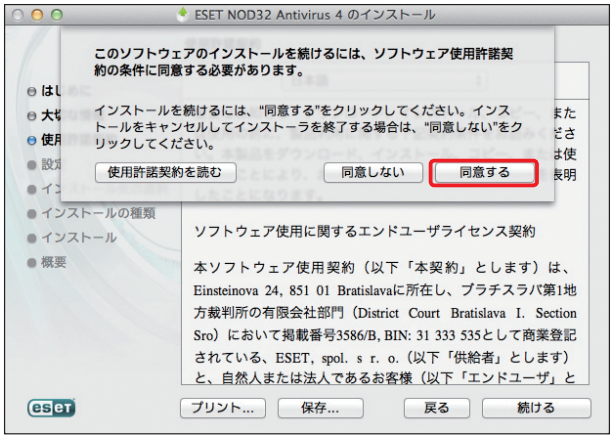
内容を確認し、[続ける]ボタンをクリックします。

6 「使用許諾契約」が表示されます



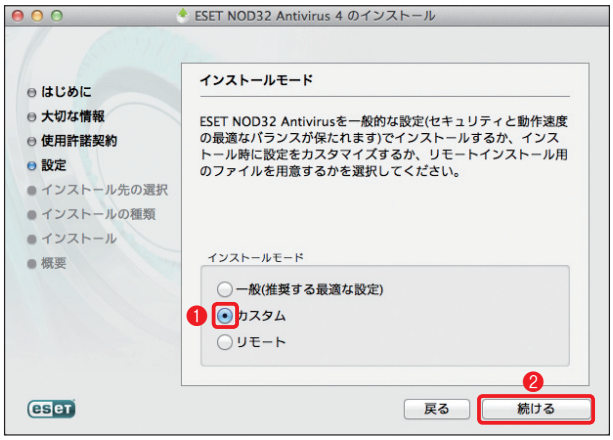
内容を確認し、[続ける]ボタンをクリックします。

7 「使用許諾契約」に同意します



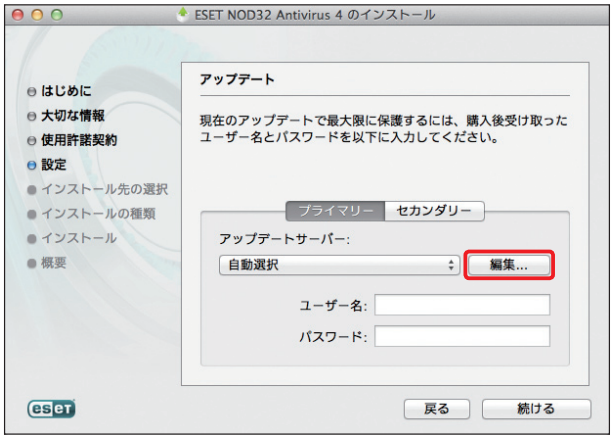
[同意する]ボタンをクリックします。

8 インストールモードを選択します



❶[カスタム]にチェックを入れ、❷[続ける]ボタンをクリックします。

9 アップデートサーバーの設定を行います



[編集]ボタンをクリックします。

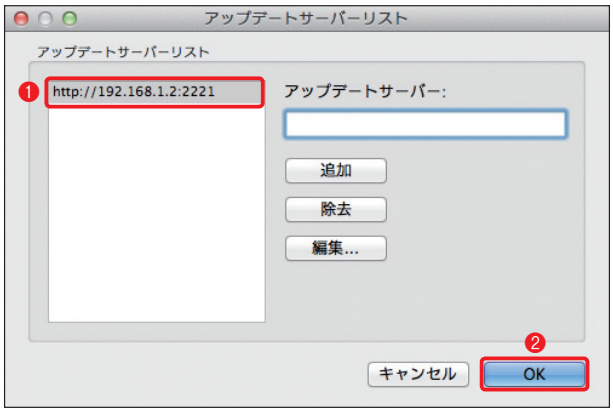
10 アップデートサーバーの接続情報を入力します

❶[アップデートサーバー]欄に接続先のサーバー情報を入力し、❷[追加]ボタンをクリックします。

POINT

社内に設置されたミラーサーバーを利用する場合は、IPアドレス(またはホスト名)とポート番号を「http://xxx.xxx.xxx.xxx:ポート番号」の形式で入力してください。また、ミラーサーバーを使用する場合の詳細な設定については、29ページをご参照ください。

11 アップデートサーバーの情報が登録されました



❶接続情報が[アップデートサーバーリスト]に登録されるので、❷[OK]ボタンをクリックします。

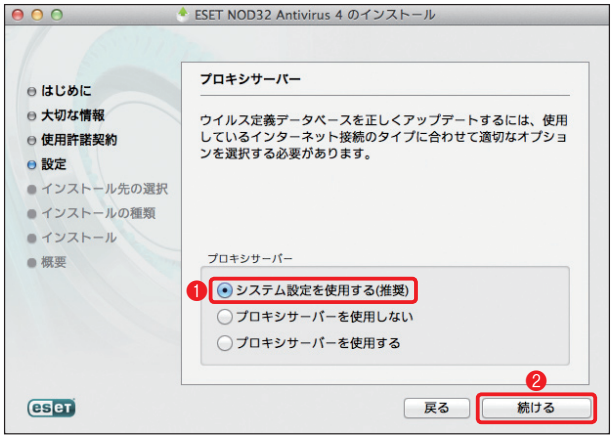
12 登録したアップデートサーバーを選択します

❶アップデートサーバーのプルダウンメニューから手順11で登録した情報を選択します。❷[続ける]ボタンをクリックします。

POINT

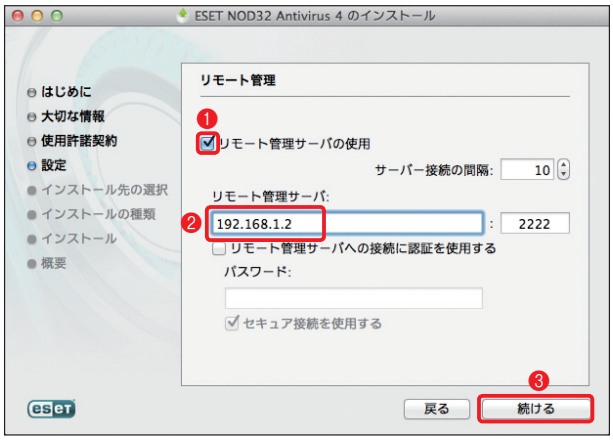
アップデートサーバーに接続認証が設定されているときは、「ユーザー名」「パスワード」の入力も行います。

13 プロキシサーバーの設定を行います



アップデートなどのHTTP通信がプロキシサーバーを経由する場合、この設定を行う必要があります。❶[システム設定を利用する(推奨)]にチェックが入っていることを確認し、❷[続ける]ボタンをクリックします。

14 管理サーバーの設定を行います

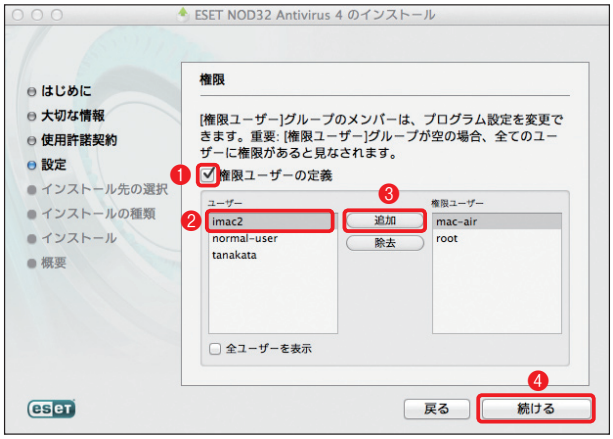


❶[リモート管理サーバの使用]にチェックを入れ、❷リモート管理サーバの欄にIPアドレス(またはホスト名)を入力します。❸[続ける]ボタンをクリックします。

POINT

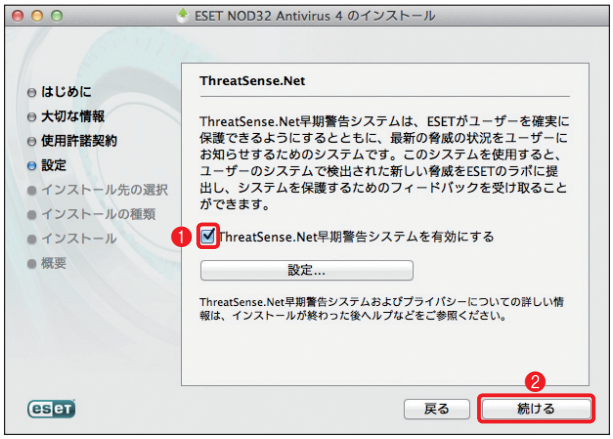
管理サーバーを利用していない場合は、この設定を行う必要はありません。

15 権限ユーザーの設定を行います



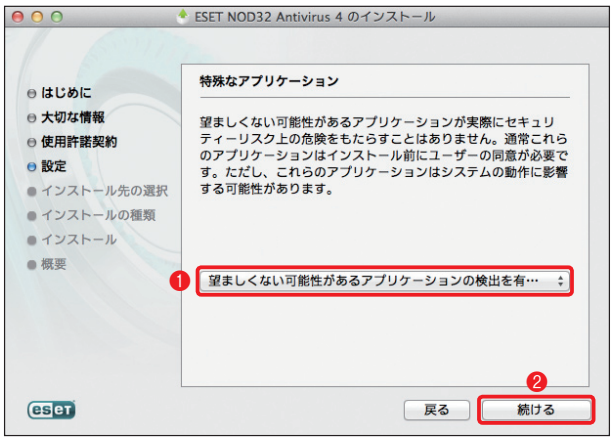
❶[権限ユーザーの定義]にチェックを入れます。❷権限ユーザーに登録したいユーザーを「ユーザー」グループから選択し、❸[追加]ボタンをクリックします。手順❷❸の作業を繰り返し、権限ユーザーに登録したいユーザーをすべて登録したら、❹[続ける]ボタンをクリックします。

16 ThreatSense.Netの設定を行います



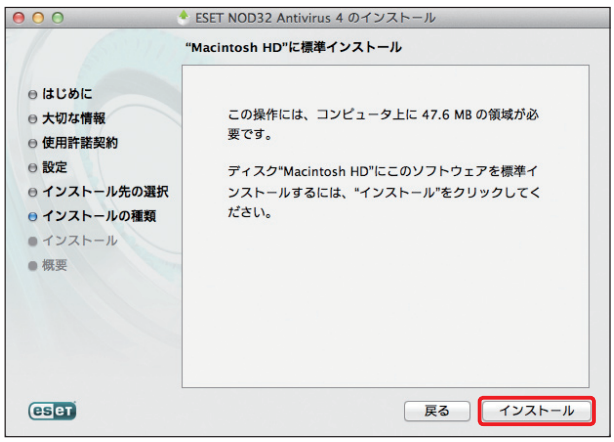
❶[ThreatSense.Net早期警告システムを有効にする]にチェックが入っていることを確認し、❷[続ける]ボタンをクリックします。

17 特殊なアプリケーションの設定を行います



❶プルダウンメニューから[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]を選択し、❷[続ける]ボタンをクリックします。

18 インストールの準備ができました

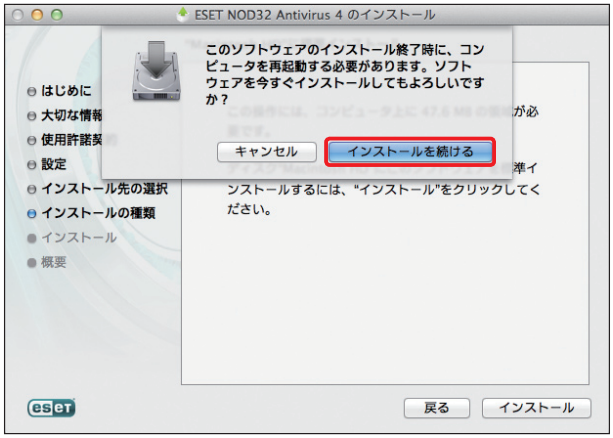


[インストール]ボタンをクリックします。

19 管理者アカウントを入力します

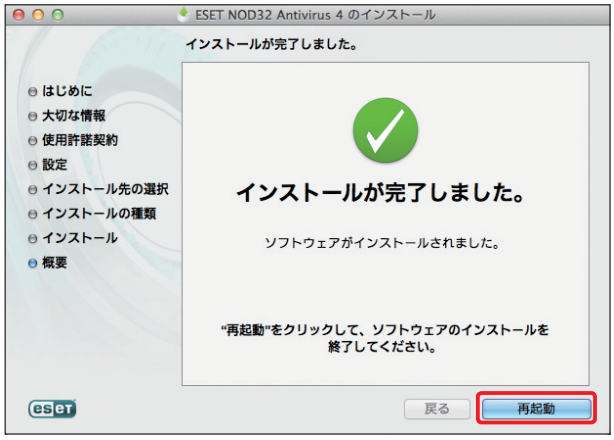
管理者アカウントの❶[名前]と[パスワード]を入力し、❷[ソフトウェアをインストール]ボタンをクリックします。

20 インストールを開始します



[インストールを続ける]ボタンをクリックします。

21 インストール作業が完了しました



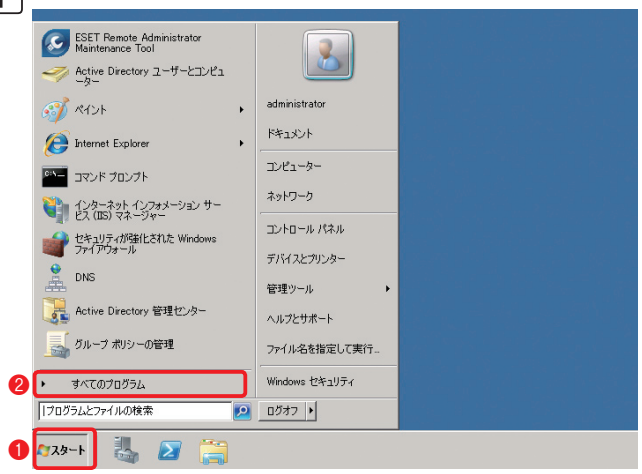
インストールが始まり、進捗状況が表示されます。「インストールが完了しました。」と表示されたら、インストールは、終了です。[再起動]ボタンをクリックして、パソコンを再起動します。

設定ファイルの配布～ ERA編

管理サーバー（ERA）への接続設定が行われている場合、ERAからリモート操作で一括してクライアントPCにインストールされたESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの設定を変更できます。インストーラー（.dmg）で手動インストールを行うときに管理サーバーへの接続設定を行うか、インストーラーパッケージ（.pkg）作成時に管理サーバーへの接続設定を行っておくと、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのインストール後、すぐにリモート操作機能を利用して各種設定を変更できます。ここでは、ERAからリモート操作で設定を変更する手順を説明します。

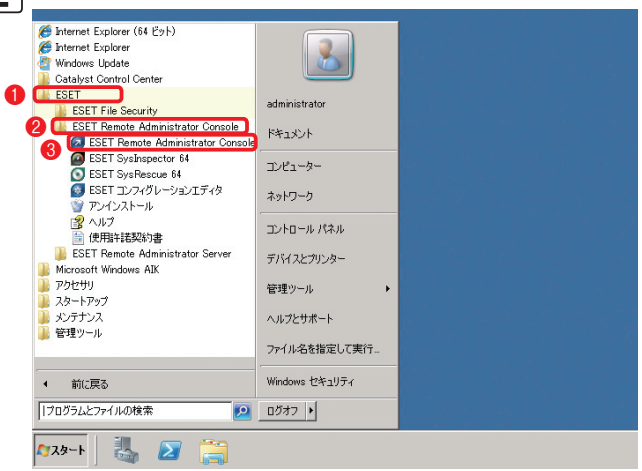
重要
この操作は、ERAS（ESET Remote Administrator Server）を操作するERAC（ESET Remote Administrator Console）が、インストールされたパソコンで行います。ERACの詳細な利用方法については、Windows用のユーザーズガイド 運用編 / 導入編をご参照ください。

1 すべてのプログラムを開きます



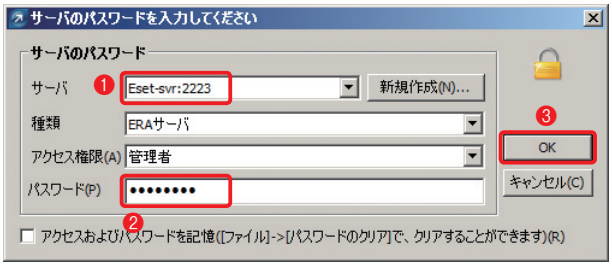
❶[スタート]ボタンをクリックし、❷[すべてのプログラム（プログラム）]をクリックします。

2 ERACを起動します



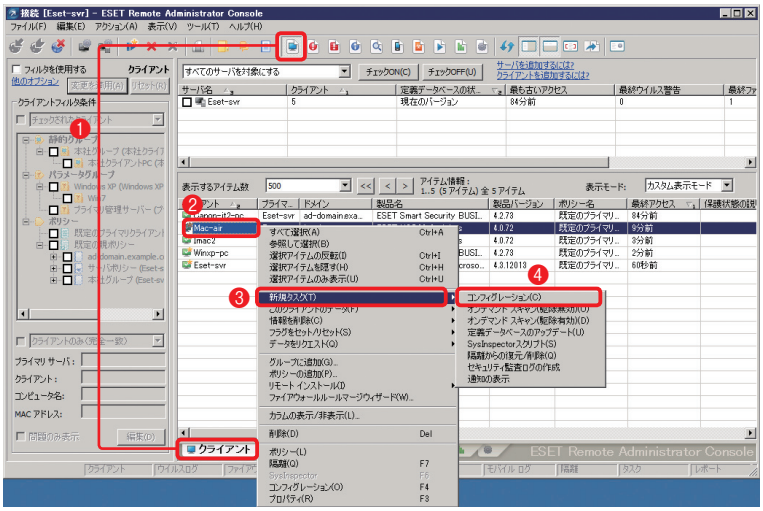
❶[ESET]をクリックし、❷[ESET Remote Administrator Console]をクリックして、❸[ESET Remote Administrator Console]をクリックします。

3 ERASへの接続設定を行います



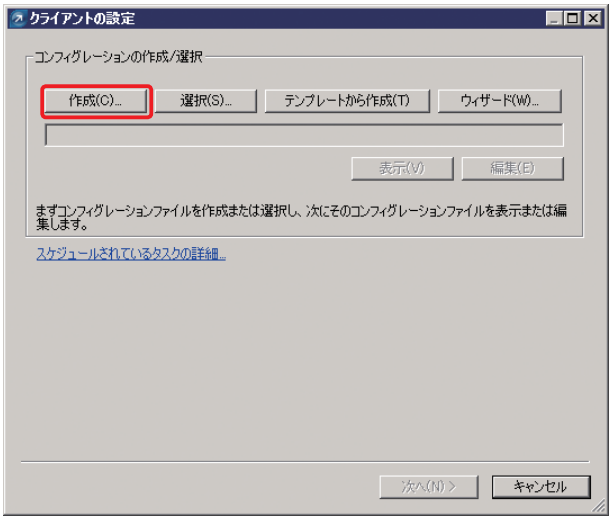
❶接続先サーバーを選択し、❷[パスワード]を入力します。❸[OK]ボタンをクリックします。

4 操作したいクライアントPCを選択します



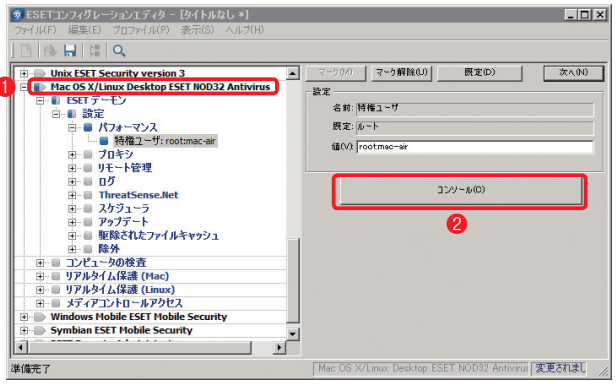
❶[クライアントペインを表示]ボタンまたは[クライアント]タブをクリックし、❷設定の変更を行いたいクライアントを右クリックします。❸[新規タスク]を選択し、❹[コンフィグレーション]をクリックします。

5 配布したい設定を作成します



[作成]ボタンをクリックします。

6 設定を入力します

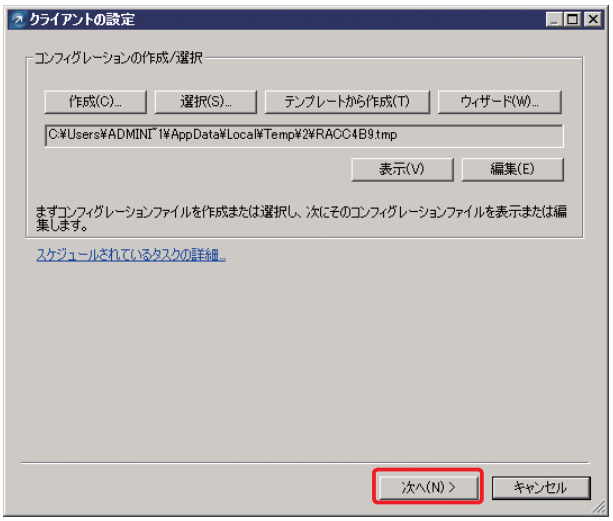


ESET コンフィグレーションエディタが起動します。❶[Mac OS X/Linux Desktop ESET NOD32 Antivirus]をクリックし、各種設定を行います。❷設定を終えたら、[コンソール]ボタンをクリックします。

POINT

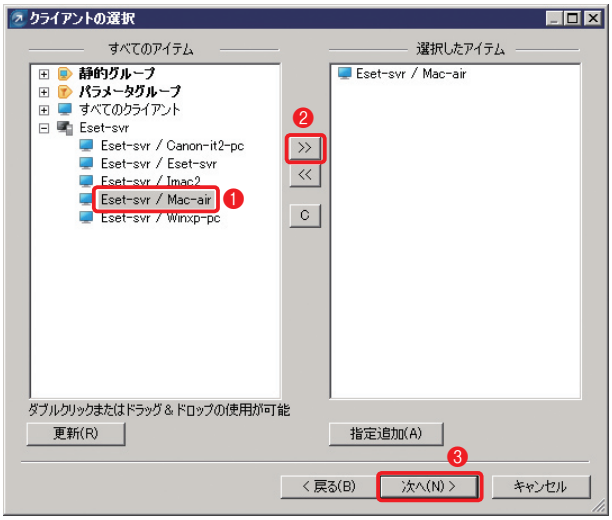
ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの他の設定例は、79ページ以降で紹介しています。実際の設定は、これを参考に行ってください。

7 次の作業に進みます



[次へ]ボタンをクリックします。

8 操作したいクライアントPCを選択します

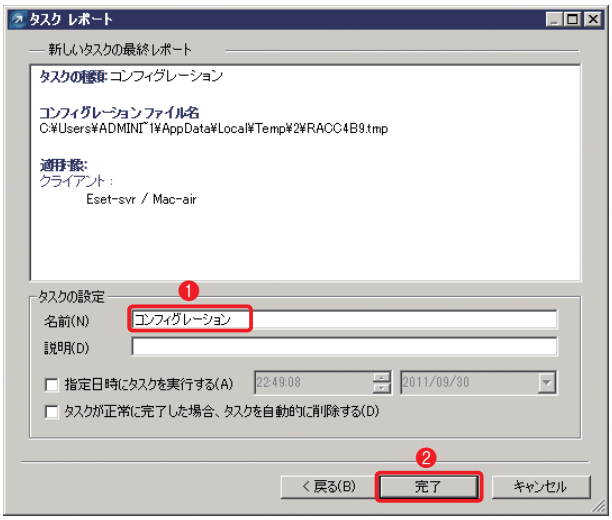


設定を変更したいクライアントPCを[選択したアイテム]リストに追加します。❶[すべてのアイテム]リストから追加したいグループまたはクライアントPCをクリックし、❷[クライアントの追加([>>])]ボタンをクリックします。追加し終えたら、❸[次へ]ボタンをクリックします。

POINT

グループを選択すると、そのグループ内すべてのクライアントPCを登録できます。また、[選択したアイテム]リスト内のグループおよびクライアントPCをクリックし、[クライアントの削除([<<])]ボタンをクリックすると、選択を解除できます。[クリア([C])]ボタンをクリックすると、すべての選択を解除できます。

9 配布タスクの名称を入力します

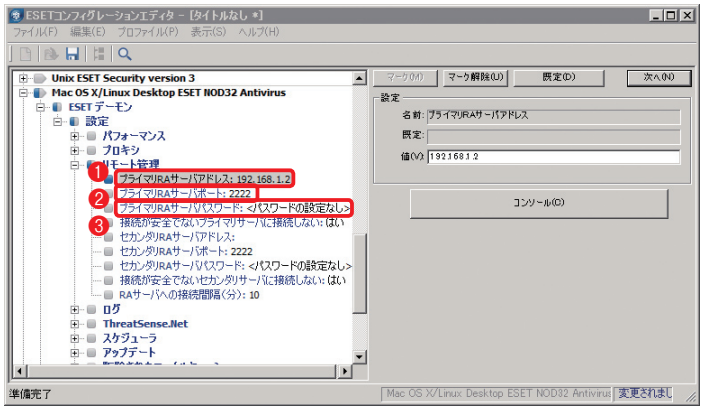


❶タスクの名前を入力し、❷[完了]ボタンをクリックします。

ERAから配布するタスクの設定例

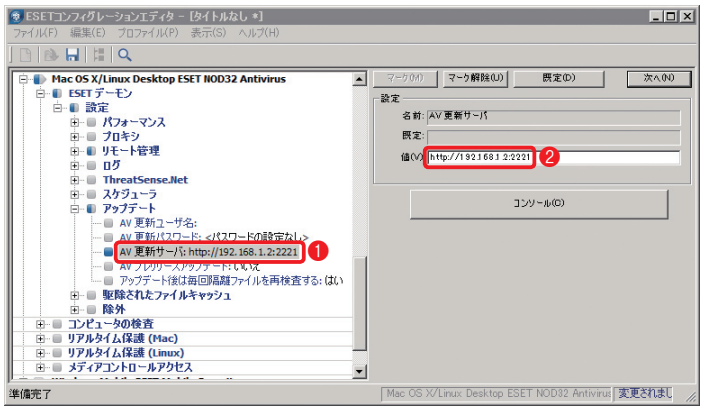
ここでは、43ページで取り上げた設定項目を例に、ERAから配布するタスクの設定方法（77ページの手順6で行う設定例）を説明します。

リモート管理～管理サーバーへの接続設定



管理サーバーへの接続設定は、[ESETデーモン]→[リモート管理]項目内の、❶[プライマリRAサーバアドレス]、❷[プライマリRAサーバポート]の各項目を編集することで行います。また、セカンダリーサーバーの接続設定は、[セカンダリRAサーバアドレス]と[セカンダリRAサーバポート]を編集することで行います。接続にパスワードが必要な場合は、❸[プライマリサーバパスワード]を編集します。

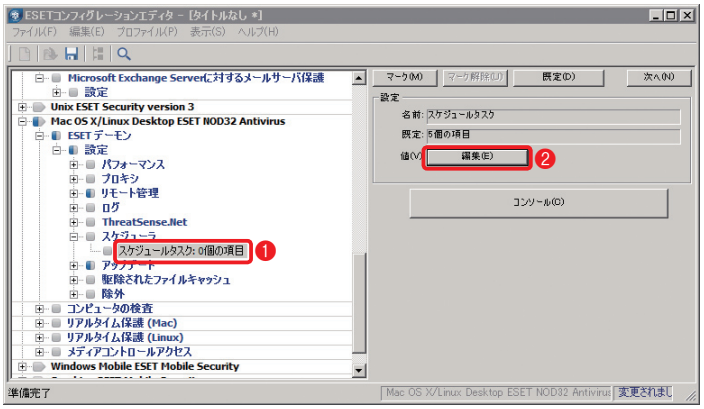
アップデート～アップデート先（ミラーサーバー）の設定



アップデート先（ミラーサーバ）の設定は、[ESETデーモン]→[アップデート]項目内の❶[AV更新サーバ]をクリックし、❷[値]にアップデートサーバー（ミラーサーバ）のIPアドレス（またはホスト名）とポート番号を「http://xxx.xxx.xxx.xxx:xxxx」の形式で入力します。

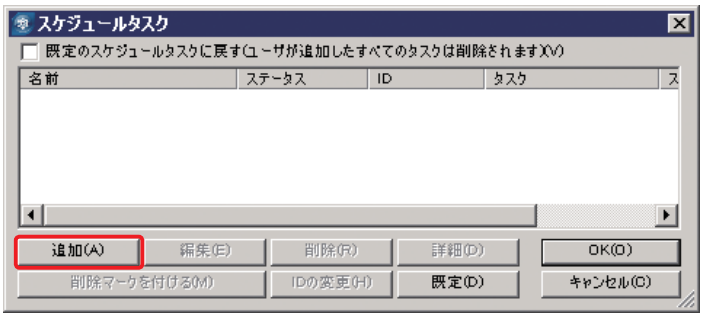
定期検査

1



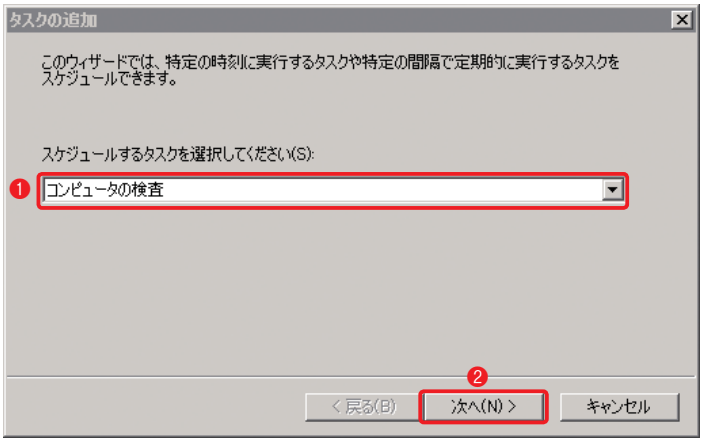
定期検査の設定は、[ESET デーモン] → [設定] → [スケジューラ] 項目内の❶ [スケジュールタスク] で行えます。設定を行う場合は、❷ [編集] ボタンをクリックして表示される [スケジュールタスク] ダイアログで、[コンピュータの検査] タスクを作成します。

2



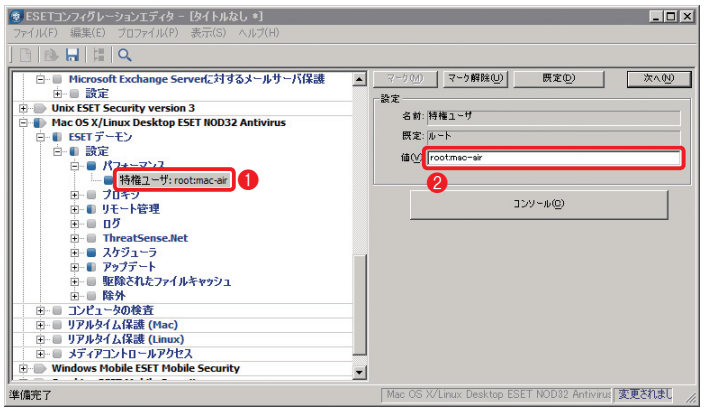
[スケジュールタスク] ダイアログが表示されます。[追加] ボタンをクリックします。

3



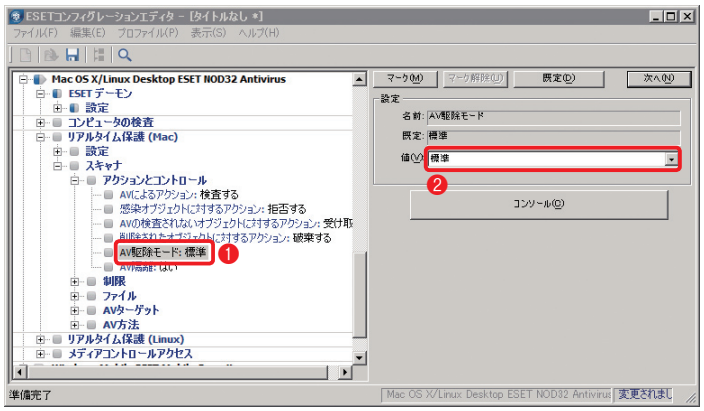
[タスクの追加] ダイアログが表示されます。❶ [コンピュータの検査] を選択して、❷ [次へ] ボタンをクリックします。続いて、ウィザードの指示に従って操作を行いタスクを作成します。

権限ユーザー



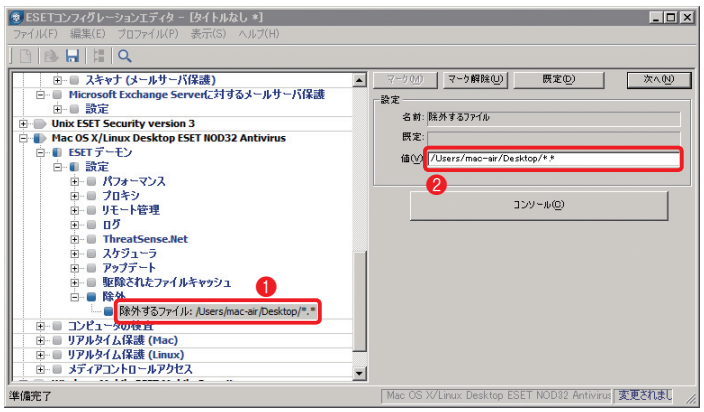
権限ユーザーの設定は、[ESETデーモン]→[設定]→[パフォーマンス]項目内の❶[特権ユーザ]で行えます。設定を行う場合は、❷[値]に権限ユーザーとして登録するユーザー名を入力します。複数名を設定する場合は、「:(コロン)」で区切ってユーザー名を入力します。

ウイルス検出時のアクション(リアルタイムファイルシステム保護の場合)



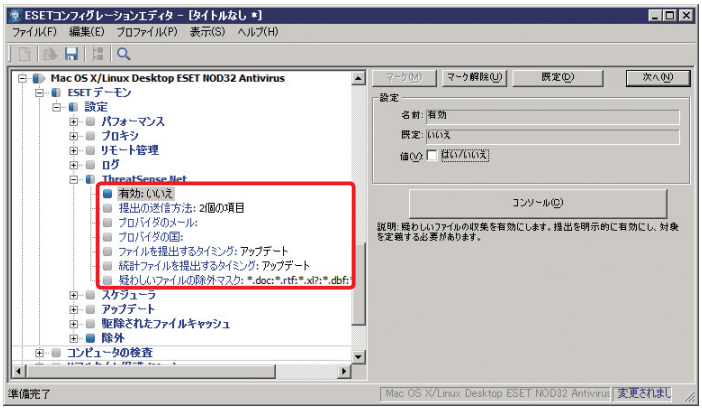
ウイルス検出時のアクションは、[リアルタイム保護(Mac)]→[スキャナ]→[アクションとコントロール]項目内の❶[AV駆除モード]の❷[値]で設定を変更できます。

検査対象からの除外



検査対象からの除外の設定は、[ESETデーモン]→[設定]→[除外]項目内の❶[除外するファイル]で行えます。設定を行う場合は、❷[値]に除外したいファイル名を絶対パスで入力します。また、フォルダーを除外したいときは、「フォルダー名/*.*」と入力します。

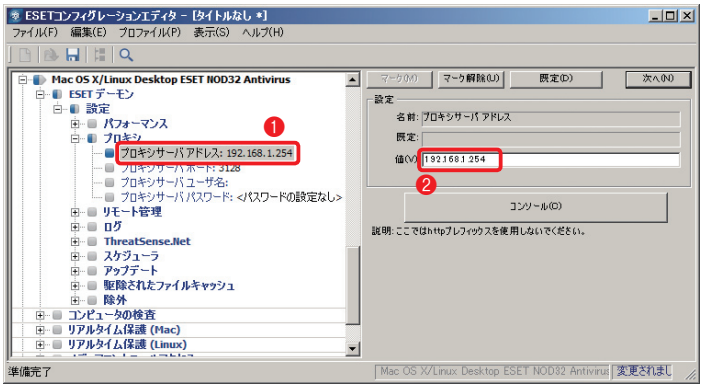
ThreatSense.Net早期警告システム



ThreatSense.Net早期警戒システムの設定は、[ESETデーモン]→[設定] →[ThreatSense.Net] 内 の各項目を編集することで行います。この機能を利用しない場合は、[有効] をクリックし、[値] のチェックを外します。

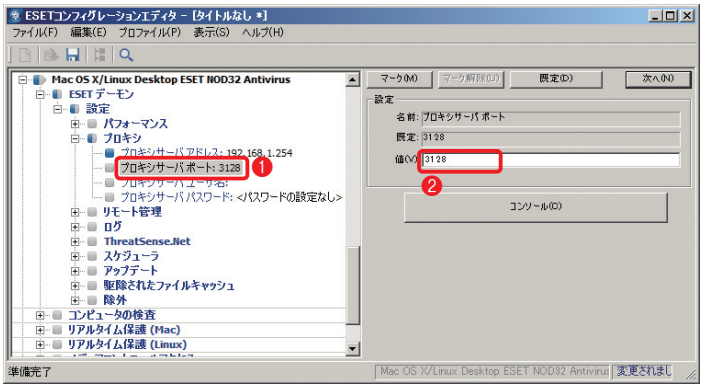
プロキシサーバー

1



プロキシサーバーの設定は、[ESET デーモン] →[設定] →[プロキシ] 内の各項目を編集することで行います。設定を行う場合は、❶[プロキシサーバアドレス] をクリックし、❷[値] にプロキシサーバーのIPアドレス（またはホスト名）を入力します。

2



❶[プロキシサーバポート] をクリックし、❷[値] にポート番号を入力します。

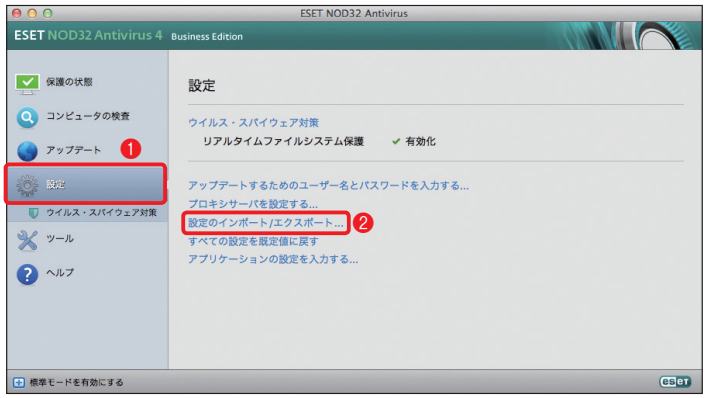
POINT

認証が必要な場合は、[プロキシサーバユーザ名] にユーザー名を入力し、[プロキシサーバパスワード] にパスワードを入力します。

設定ファイルの配布～ESET NOD32アンチウイルス V4.0 Mac OS X用プログラム編

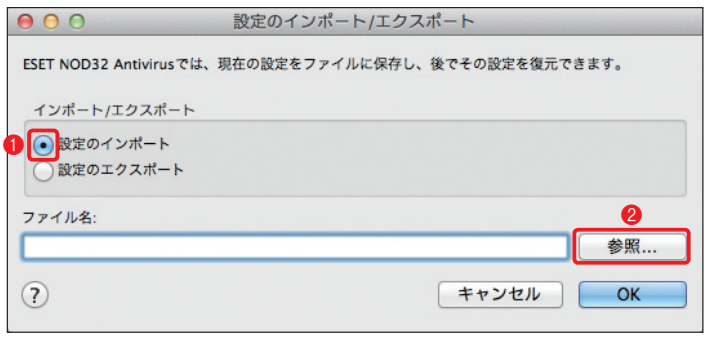
ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、あらかじめ準備しておいた設定ファイルを各クライアントPCで読み込むことで、各種設定を一括変更できます。ここでは、40ページの手順で設定ファイルが作成されているものとして、その読み込み手順を説明します。

1 メインウィンドウを開きます



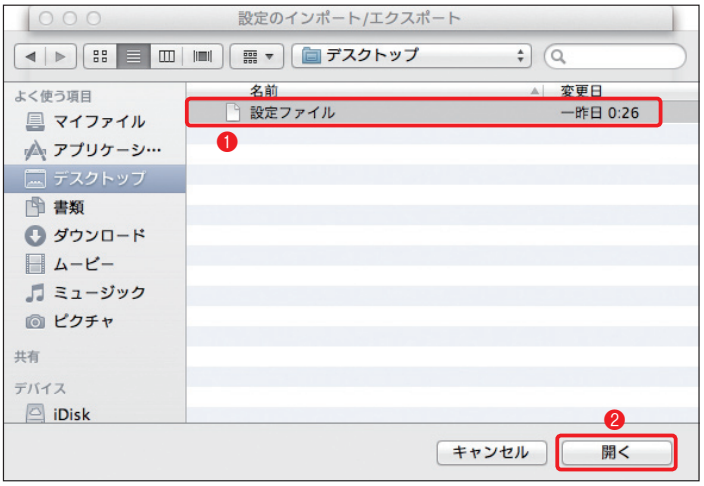
ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのメインウィンドウを開き、詳細モードに切り替えてから、❶[設定]ボタンをクリックし、❷[設定のインポート/エクスポート]をクリックします。

2 設定ファイルの読み込みを開始します



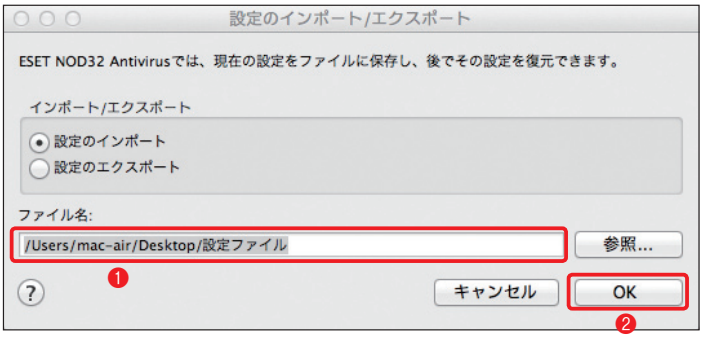
❶[設定のインポート]にチェックを入れ、❷[参照]ボタンをクリックします。

3 読み込みたいファイルを選択します



❶インポートしたい設定ファイルを選択し、❷[開く]ボタンをクリックします。

4 設定ファイルが読み込まれました



❶選択したファイルが登録されます。❷[OK]ボタンをクリックします。

05-06 Apple Remote Desktopを利用したリモートインストール

本節では、Apple Remote Desktopを利用したESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのインストールについて説明します。

リモートインストールに必要なもの

Apple社の販売する有償ソフトウェア「Apple Remote Desktop」は、Mac OS Xをインストールしたパソコンをネットワーク経由で管理/操作するリモート管理ソフトウェアです。このようなソフトウェアを利用することで、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをリモートでインストールできます。

この方法でインストールする場合は、インストール先のパソコンが、Apple Remote Desktopで操作できるように設定されている必要があります。また、事前に付属のインストーラー（.dmg）を使って設定済みパッケージ（.pkg）を作成しておく必要があります。

リモートインストールに利用するインストーラーについて

リモートインストールで利用する設定済みパッケージ（.pkg）は、付属のインストーラー（.dmg）を使って作成します。作成方法については、55ページをご参照ください。

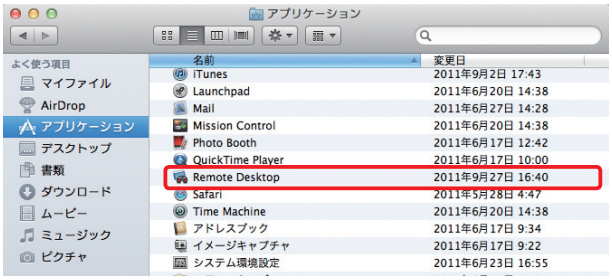
リモートインストールを実施する

ここでは、Apple Remote Desktopを利用して、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをインストールする手順を説明します。

1 クライアントPCを設定します

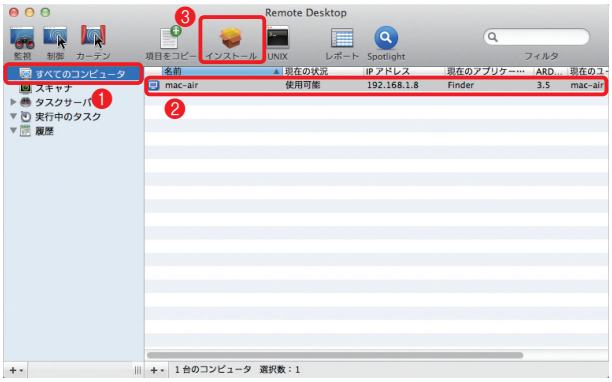
クライアントPC側で、リモート操作を可能とするための設定を行います。

2 管理者側でRemote Desktopを起動します



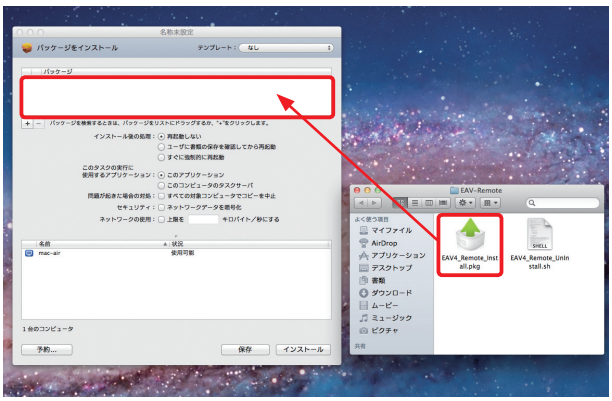
Finderで[アプリケーション]フォルダーを開き、[Remote Desktop]をダブルクリックします。

3 操作したいパソコンを選択します



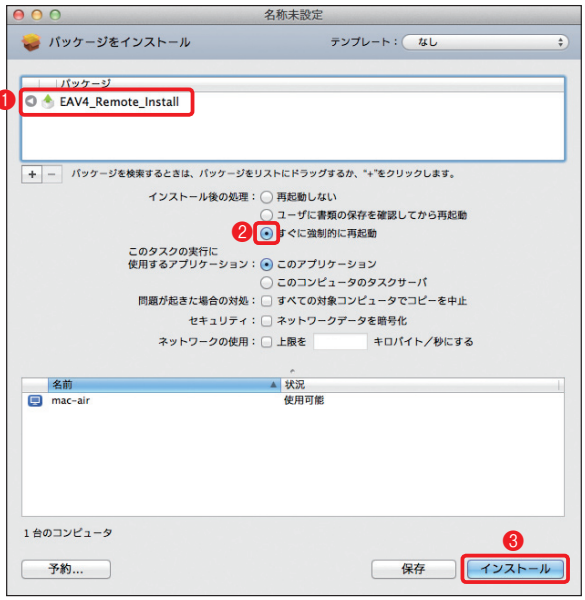
❶[すべてのコンピュータ]をクリックし、❷リモートインストールを行いたいPCをクリックします。❸[インストール]ボタンをクリックします。

4 設定済みパッケージを登録します



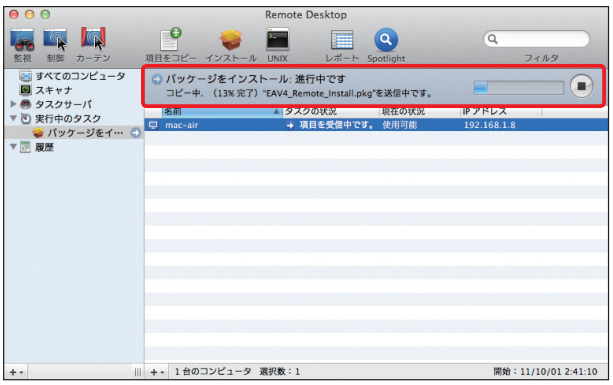
設定済みパッケージ(.pkg)を[パッケージ]欄にドラッグ&ドロップします。

5 インストール作業を開始します



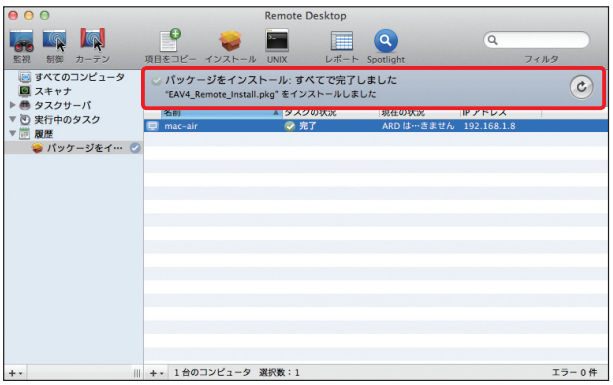
❶設定済みパッケージが登録されます。❷インストール後の処理（ここでは、［すぐに強制的に再起動］）にチェックを入れ、❸［インストール］ボタンをクリックします。

6 リモートインストールが始まります



リモートインストールが始まり、進捗状況が表示されます。

7 リモートインストールが完了しました



「パッケージをインストール：すべてで完了しました」と表示されたら、リモートインストールは完了です。

POINT

クライアントPCの再起動後に、アンチウイルス機能が有効になります。

設定ファイルの配布～ ERA 編

管理サーバーへの接続設定が行われている場合、リモート操作でクライアントPCにインストールされたESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの設定を変更できます。ERAからリモート操作で設定を変更する場合は、75ページの手順を参考に作業してください。

設定ファイルの配布～ ESET NOD32アンチウイルス V4.0 Mac OS X用プログラム編

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムは、あらかじめ準備しておいた設定ファイルを読み込むことで、各種設定を一括変更できます。設定ファイルを利用して各種設定を一括変更する場合は、83ページの手順を参考に作業を行います。

05-09 クライアントPC用ソフトウェアのアンインストール

本節では、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのアンインストール方法について説明します。

アンインストール方法について

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムのアンインストール方法には、手動でアンインストールを行う方法とApple Remote Desktopなどを利用してリモートアンインストールを行う方法があります。以下にそれぞれの方法で必要なファイルと特徴をまとめておきます。クライアントPCの設置環境や導入台数、運用方法などに応じて選択してください。

アンインストール方法	必要なファイル	特徴	参照ページ
手動アンインストール	標準付属のインストーラー（.dmg）	製品パッケージに付属するインストーラー（.dmg）を利用してアンインストールを行う方法です。	90 ページ
リモートアンインストール	シェルスクリプト（.sh）	Apple 社のリモート管理ソフト Apple Remote Desktop などを利用して、リモートアンインストールを行います。アンインストールには、標準付属のインストーラー（.dmg）で設定済みパッケージ（.pkg）を作成したときに一緒に作成されるアンインストール用のシェルスクリプト（.sh）を利用します。	92 ページ

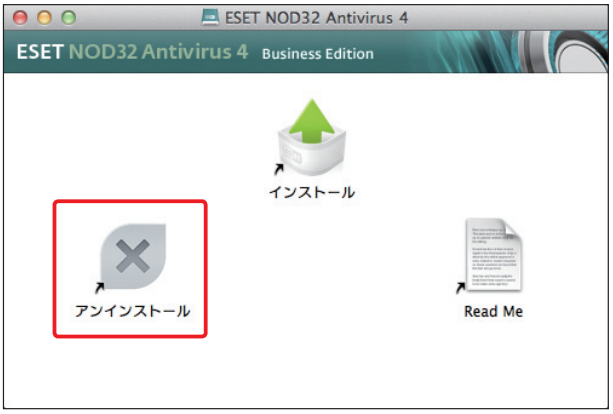
手動アンインストール手順

ここでは、付属のインストーラー(.dmg)を利用して、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムを手動でアンインストールする手順を紹介します。

1 インストーラー(.dmg)を起動します

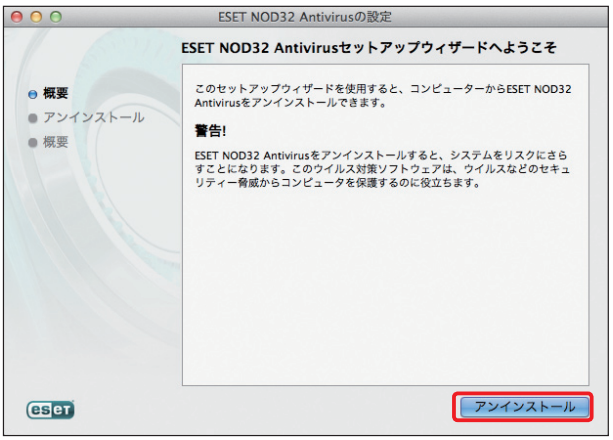
インストーラー(.dmg)をダブルクリックします。

2 アンインストールを開きます



[アンインストール]をダブルクリックします。

3 アンインストールを開始します



[アンインストール]ボタンをクリックします。

4 管理者アカウントを入力します

❶管理者アカウントの[名前]と[パスワード]を入力し、❷[OK]をクリックします。

5 アンインストール作業が終了しました

アンインストール作業が始まり、進捗状況が表示されます。「アンインストールが完了しました」と表示されたら、[閉じる]をクリックします。

6 再起動します

❶[アップルメニュー]をクリックし、❷[再起動]をクリックして、OSを再起動します。

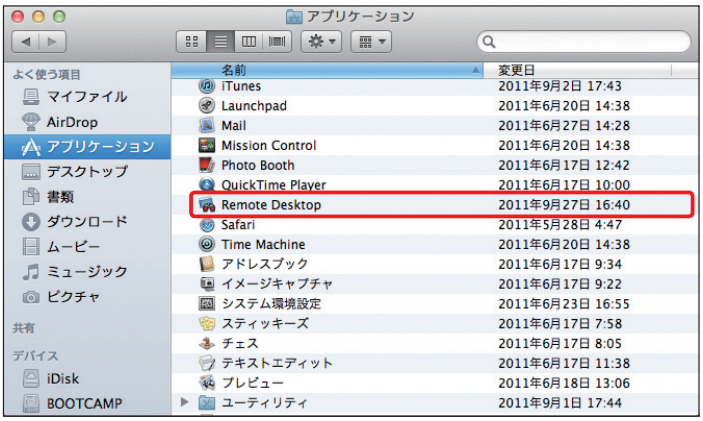
リモートアンインストールを実施する

ここでは、Apple Remote Desktopを利用して、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムをリモートアンインストールする手順を説明します。

1 クライアントPCを設定します

クライアントPC側で、リモート操作を受けつける設定を行います。

2 管理者側でRemote Desktopを起動します

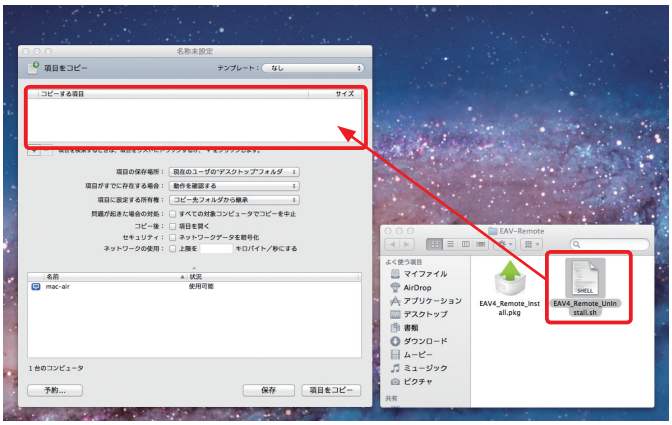


Finderで[アプリケーション]フォルダーを開き、[Remote Desktop]をダブルクリックします。

3 パソコンを選択します

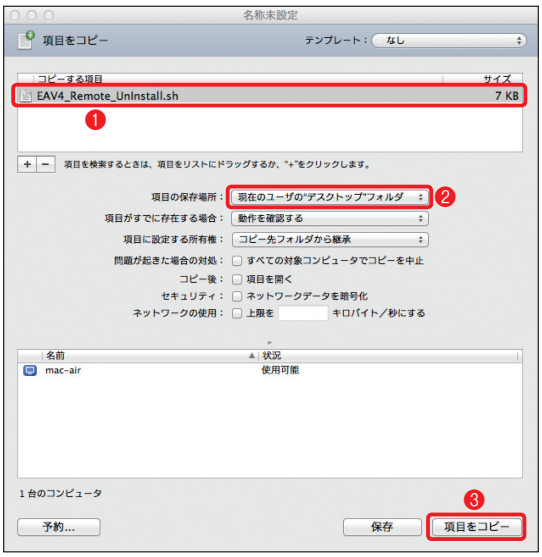
❶[すべてのコンピュータ]をクリックし、❷リモートアンインストールを行いたいPCをクリックします。❸[項目をコピー]ボタンをクリックします。

4 シェルスクリプト(.sh)を登録します



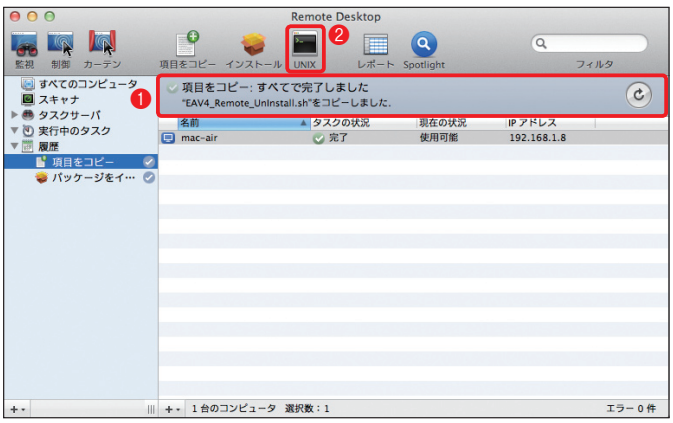
アンインストール用のシェルスクリプト(.sh)を[コピーする項目]欄にドラッグ&ドロップします。

5 シェルスクリプト(.sh)をコピーします



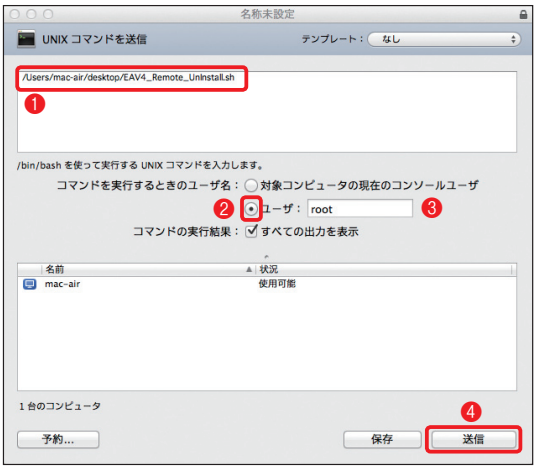
❶シェルスクリプト(.sh)が登録されます。❷[項目の保存場所]のプルダウンメニューから保存場所を選択し、❸[項目をコピー]ボタンをクリックします。

6 コピー作業が完了します



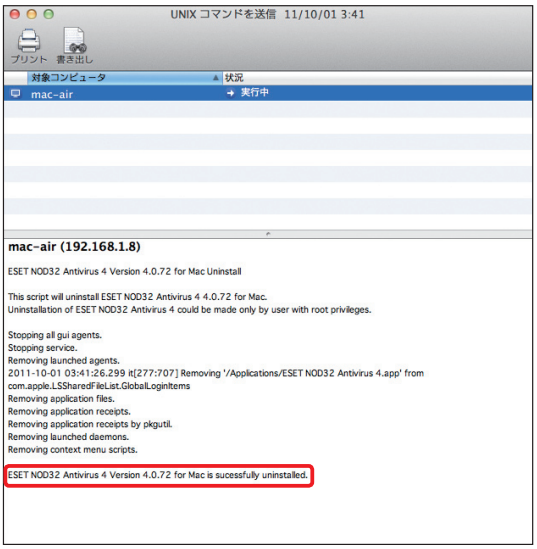
❶[項目をコピー：すべてで完了しました]と表示されたらシェルスクリプト(.sh)のコピーは完了です。❷[UNIX]ボタンをクリックします。

7 コマンドを送信します



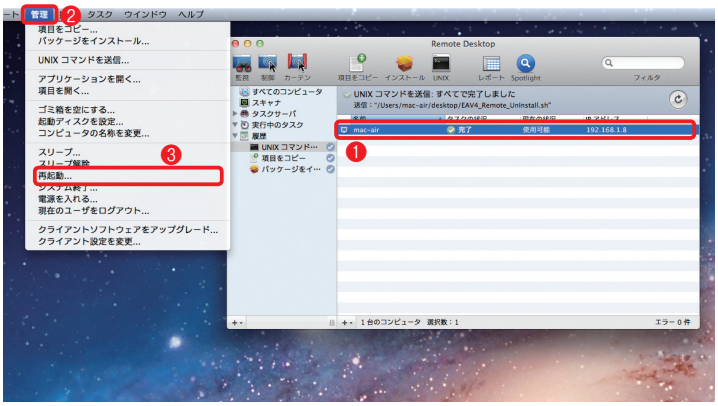
❶シェルスクリプト(.sh)のコピー場所のパスを入力し、❷ユーザにチェックを入れ、❸ユーザー名に「root」と入力し、❹[送信]ボタンをクリックします。

8 コマンドが送信されました



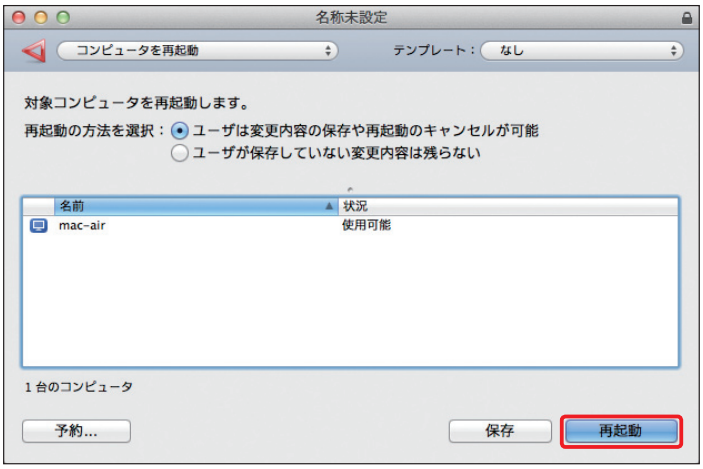
コマンドの送信ログが表示されます。履歴の最後に「sucessfully unsinstalled」と表示されていたらアンインストールは完了です。続いて、アンインストールを行ったPCを再起動します。

9 リモートでコンピュータを再起動します



❶アンインストールを行ったPCをクリックし、❷メニューバーの[管理]をクリックして、❸[再起動]をクリックします。

10 再起動を実行します

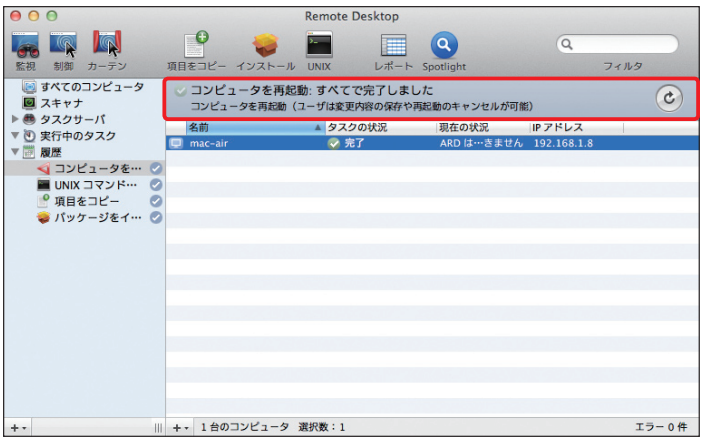


[再起動]ボタンをクリックします。

CAUTION

この手順を実行後、対象となるPCは強制的に再起動されます。

11 コンピュータが再起動されます



「コンピュータを再起動：すべてで完了しました」と表示されたら、コンピュータの再起動は完了です。

運用編

運用編

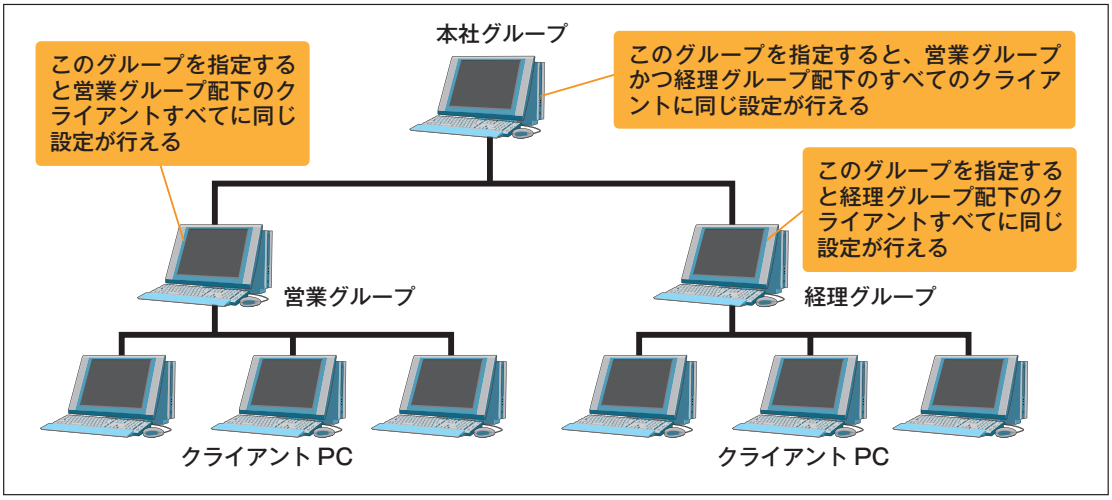
[Chapter 2]
クライアントPCの効率的な管理方法

02-02 グループ機能

グループ機能は、クライアントPC を特定のグループに分類して管理するための機能です。ここでは、グループ機能について説明します。

グループ機能とは

ESET Remote Administrator Server（ERAS）を利用したクライアントPCの操作は、クライアントPC単位だけでなく、グループ単位で一括して行うことも可能です。このグループを作成する機能を「グループマネージャ」といいます。グループマネージャによって作成したグループは、新規タスクの一括配布やポリシー（セキュリティの設定）の一括適用などに利用できます。また、グループは自由に作成できるほか、Active Directoryのグループ情報と同期して利用することもできます。グループ機能の詳細については、Windows用のユーザーズガイド 運用編をご参照ください。



グループの種類について

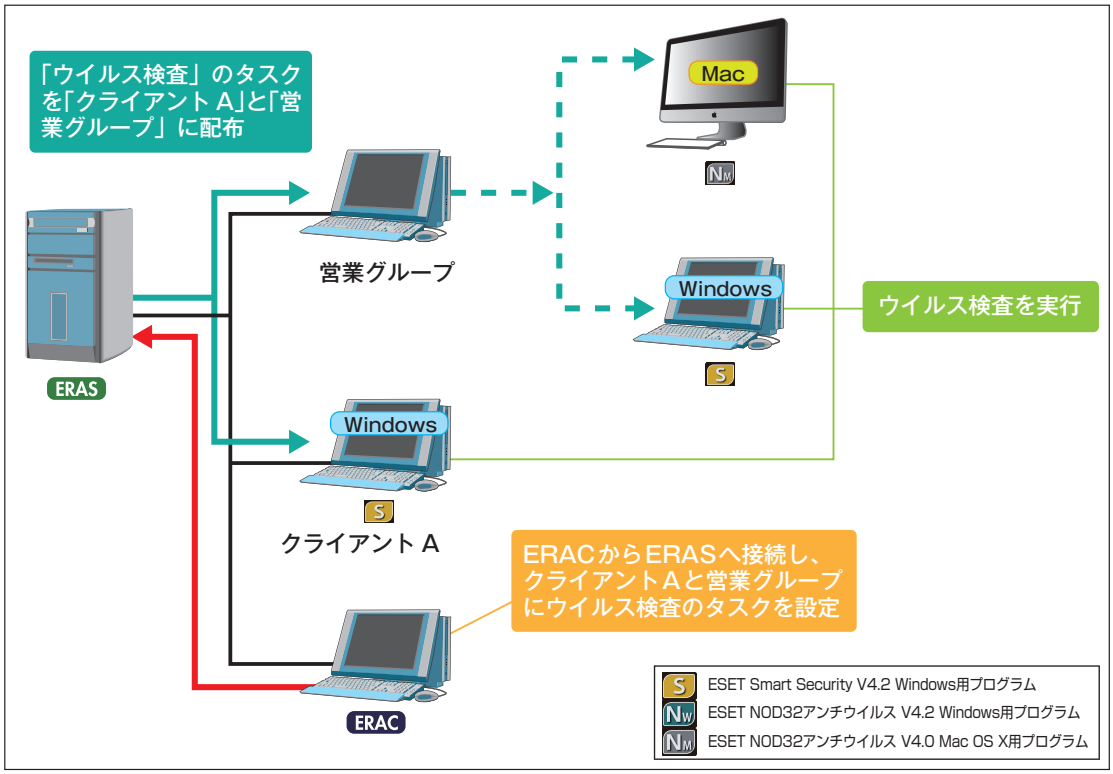
グループは、「静的グループ」と「パラメータグループ」に大別できます。静的グループは、クライアントPCを手動でグループ分けするときに利用します。Active Directoryを利用している場合は、Active Diectoryで利用しているグループとの同期機能も利用できます。パラメータグループは、グループに登録する条件を指定し、その条件を満たすクライアントPCを自動的にグループ登録します。

02-03 タスク機能

ESET Remote Administrator（ERA）には、クライアントPCを効率的に管理し、スムーズな運用を実現するために便利なタスク機能が備えられています。本節では、ERAに搭載されたタスク機能について説明します。

タスク機能とは

タスク機能とは、リモート操作でクライアントPCに様々な指示（タスク）を送り、実行させる機能です。クライアントPCは定期的にERASに接続して、自身の各種情報を送信します。その際にタスクがあると、クライアントPCはERASからタスクを受信し、それを実行します。タスク機能の詳細については、Windows用のユーザーズガイド 運用編をご参照ください。



タスクの種類について

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムで実行できるタスクには、以下の種類があります。タスクはクライアントPC単位だけでなく、グループ単位でも実行できます。

●タスクの種類

種類	概要
コンフィグレーション	クライアント PC の各種設定を変更するときに利用します。たとえば、定期的な検査スケジュールの登録や管理サーバー / アップデートサーバーへの接続設定、ウイルス検出時のアクションの設定など様々な設定が行えます。
オンデマンドスキャン（駆除無効）	ウイルス発見時の駆除を無効に設定したウイルス検査をクライアント PC に実行させたいときに利用します。このウイルス検査は検査によるログが作成されるだけで、感染ファイルに対するアクションは実行されません。
オンデマンドスキャン（駆除有効）	ウイルス発見時の駆除を有効に設定したウイルス検査をクライアント PC に実行させたいときに利用します。このウイルス検査は、ウイルスを発見すると駆除を実行します。
定義データベースのアップデート	ウイルス定義データベースのアップデートを強制的に実行したいときに利用します。このタスクを設定したクライアント PC は、強制的にウイルス定義データベースのアップデートが実行されます。

02-04 ポリシー機能

ポリシー機能とは、クライアントPCに対する特定の設定（コンフィグレーション）を継続的に保守し、強制的に適用させる機能です。本節では、ポリシーについて説明します。

ポリシー機能とは

ポリシーは、タスク機能に用意された［コンフィグレーション］タスクと同等の機能を提供しています。［コンフィグレーション］タスクが1度きりの設定であるのに対し、ポリシー機能では継続的に設定が適用されます。ポリシーの変更を行った場合、その変更点はクライアントPCが自身の各種情報を送信するためにERASへ接続した後、すぐに適用されます。ポリシー機能の詳細については、Windows用のユーザーズガイド 運用編をご参照ください。

02-05 通知機能

ERAには、ウイルスが検出された場合などセキュリティ上の問題が発生したとき、管理者などに異常を知らせるための通知機能が搭載されています。ここでは通知機能について説明します。

通知機能とは

通知機能は、セキュリティ上の問題が発生したときなどに、管理者に電子メールなどでメッセージを通知する機能です。さまざまな通知条件を設定でき、たとえば、一定数以上のPCがウイルスに感染した場合に通知するなど設定が行えます。通知機能は、［通知マネージャ］を利用することで通知内容の設定や通知の方法、各種警告などをカスタマイズできます。通知機能の詳細については、Windows用のユーザーズガイド 運用編をご参照ください。

コラム

Boot Campや仮想PCを利用しているクライアントの管理

ERAにおけるクライアントPCの識別について

ERAでは、以下のような識別子に基づいてクライアントPCを認識しています。

コンピューター名 + MACアドレス + プライマリサーバー

識別子が同一の場合、ERAは、クライアントPC1台と認識し、識別子が異なる場合は、別のクライアントPCと認識します。このため、Mac OS XとBoot Camp上のWindowsの両方を同じパソコンで利用している場合、Macアドレスが同一となるため、コンピューター名とプライマリサーバーが同一であれば、同じクライアントPC（クライアントPC1台）と認識します。また、Mac OS Xで動作する仮想PCソフトを利用し、Windowsを利用した場合、異なるMACアドレスの仮想NICが利用されるため、別のクライアントPCと認識されます。つまり、パソコン1台で2台のクライアントPCと認識されます。

ERAへのログ反映時の仕様について

Mac OS XとBoot Camp上のWindowsの両方を同じパソコンで使用している場合など、ERAで同じPCと認識された場合、MacとWindowsの切り替えによって上書きされるログ情報（行数が増えない）と追加されるログ情報（行数が増える）があるのでご注意ください。

上書きされるログ情報	クライアント／隔離
追加されるログ情報	ウイルスログ／イベントログ／スキャンログ

運用編

[Chapter 4]
ウイルス対策における運用

04-05 ウイルス誤検出時の対応

ウイルス対策の運用は、日常の運用フェーズと緊急時の運用フェーズに大別されますが、日常の運用において問題のないファイルを、アンチウイルスソフトがウイルスと判定してしまうことがあります。本節では、クライアントPC用ソフトウェアが問題のないファイルをウイルスとして検出してしまった場合の対処法を説明します。

ファイルがウイルスとして検出された場合の対応手順

誤検出の判定

●弊社 HP にて、該当ファイルの検出情報があるかを確認
（http://canon-its.jp/product/eset/）
●サポートセンターに誤検出判定問い合わせ、および対応方法を確認

↓

復元作業の実施

●誤検出であれば、隔離された該当ファイルを復元

↓

防止策の実施

●クライアント PC 用ソフトウェアでの対象ファイル／フォルダーの除外設定（推奨）
※フォルダー、拡張子、アプリケーション単位での除外設定
※ ERA を利用した、クライアント PC への一括設定
●最新のウイルス定義データベースへのアップデート（推奨）
● ESET セキュリティ製品における検査機能の設定変更（上記対応ができない場合）

POINT

ウイルス対策における運用や詳細については、Windows用のユーザーズガイド 運用編をご参照ください。

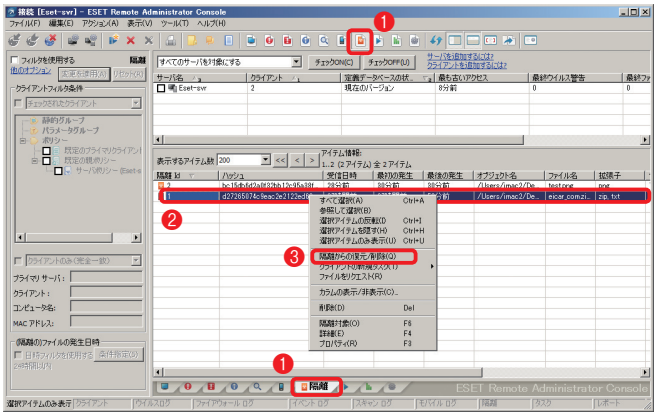
隔離されたファイルの復元手順～ ERA編

ここでは、隔離されたファイルの復元をERAを利用してリモート操作で行う手順を説明します。

1 ERACを起動します

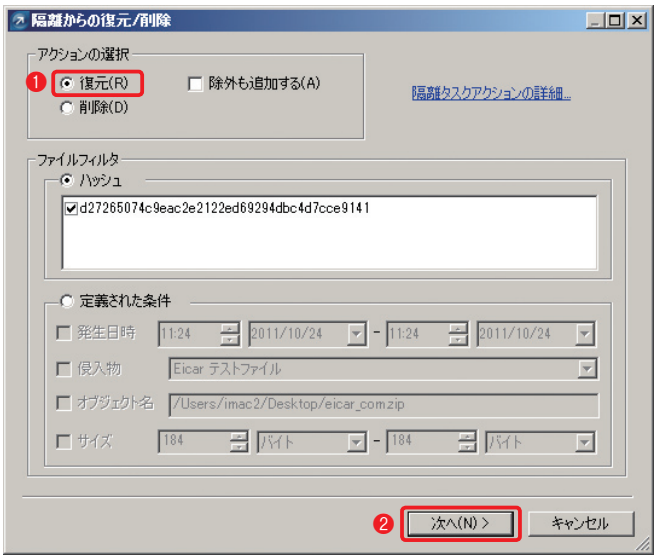
ERACを起動し、ERASにログオンします。

2 復元作業を始めます



❶[隔離] タブまたは [[隔離] ペインを表示] ボタンをクリックし、❷復元したいファイルを右クリックして❸[隔離からの復元/削除] をクリックします。

3 復元を実行します

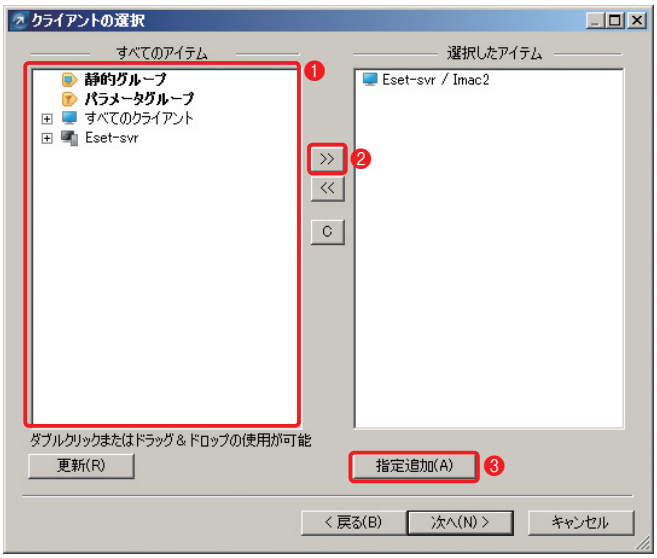


❶[復元] にチェックを入れ、❷[次へ] ボタンをクリックします。

POINT

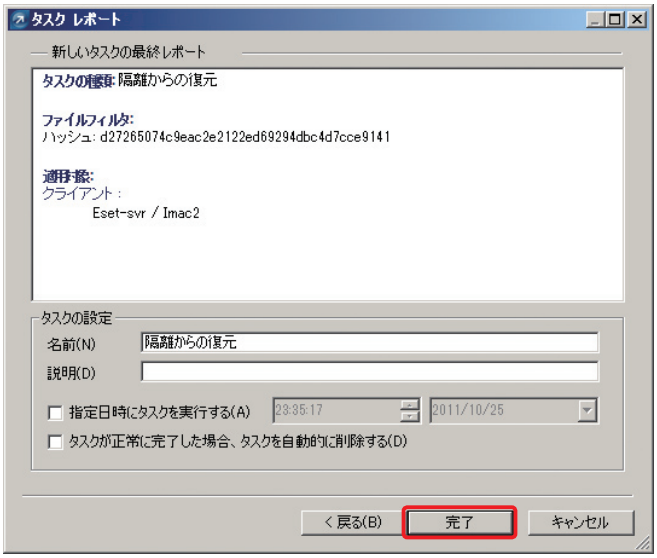
[除外を追加する] は、新種・未知のウイルスとして検出されたファイルのみ有効になります。

4 クライアントを選択します



❶［すべてのアイテム］リストから復元先のグループおよびクライアントPCをクリックし、❷［クライアントの追加（[>>]）］ボタンをクリックします。追加し終えたら、❸［次へ］ボタンをクリックします。

5 ファイルの復元を開始します



［完了］ボタンをクリックし、復元を開始します。

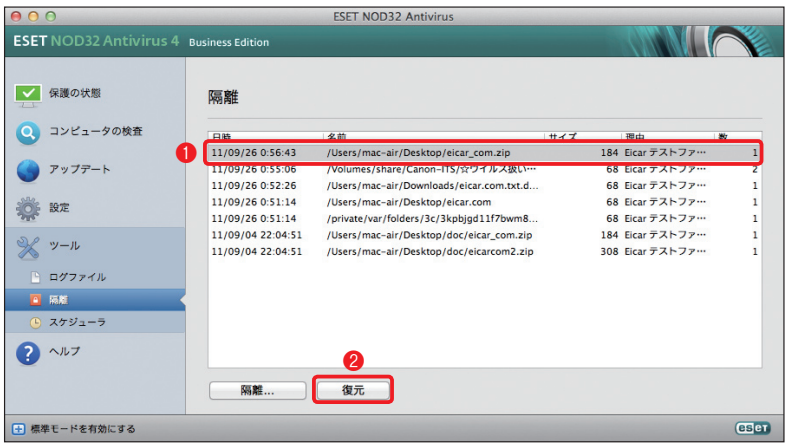
隔離されたファイルの復元手順～クライアントPC編

ここでは、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムでウイルスとして検出され、隔離されたファイルの復元手順を説明します。

1 メインウィンドウを開きます

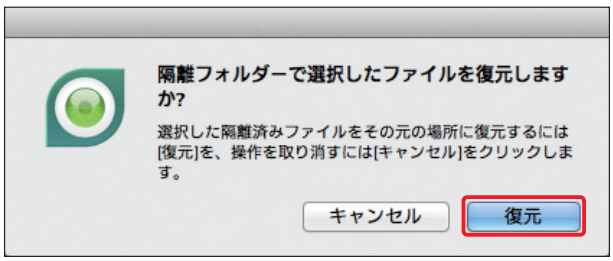
メインウィンドウを開き、詳細モードに切り替えて、❶[ツール]ボタンをクリックし、❷[隔離]ボタン、もしくは[隔離]をクリックします。

2 隔離されたファイルの一覧が表示されます



❶復元したい項目をクリックし、❷[復元]ボタンをクリックします。

3 復元を行います



[復元]ボタンをクリックします。隔離前にファイルが存在したフォルダーに、誤って検出されたファイルが復元されます。

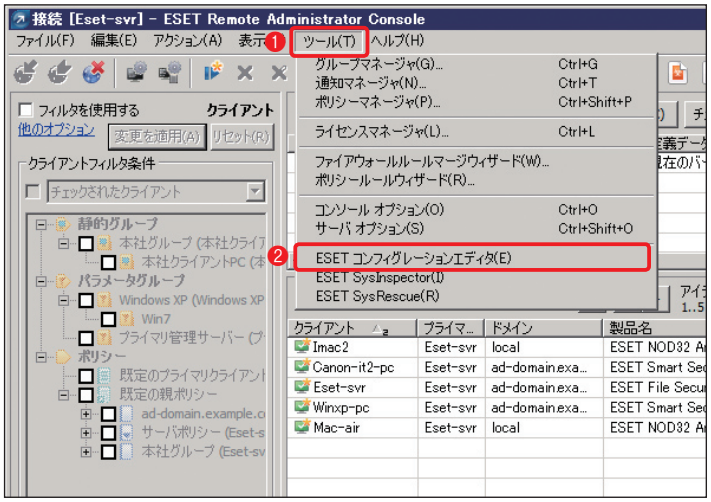
ウイルスとして検出されたファイルを検査対象から除外する～ ERA編

ウイルスとして検出されたファイルを、ウイルス検査の対象から除外します。除外設定を行ったファイルはウイルス検査の対象から外されるので、設定後は誤って削除や隔離などが行われることはありません。ここでは、ウイルスとして検出されたファイルの除外設定をERAを用いて行う方法を説明します。ERAを利用する場合はESET コンフィグレーションエディタでファイルの除外設定を作成し、[新規タスク] または [ポリシーマネージャ] から一括して配布します。

1 ERACを起動します

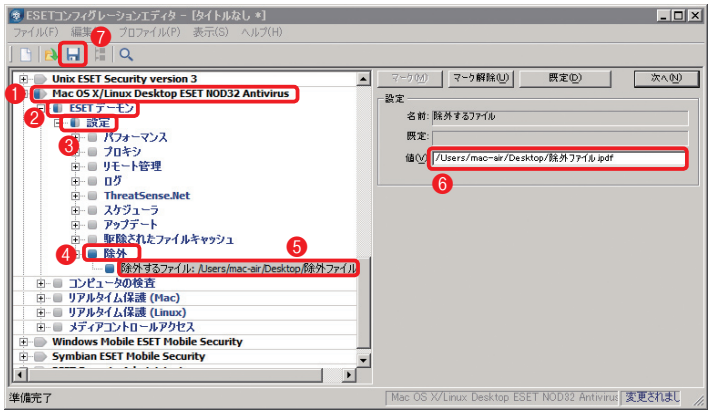
ERACを起動し、ERASにログオンします。

2 ESET コンフィグレーションエディタを開きます



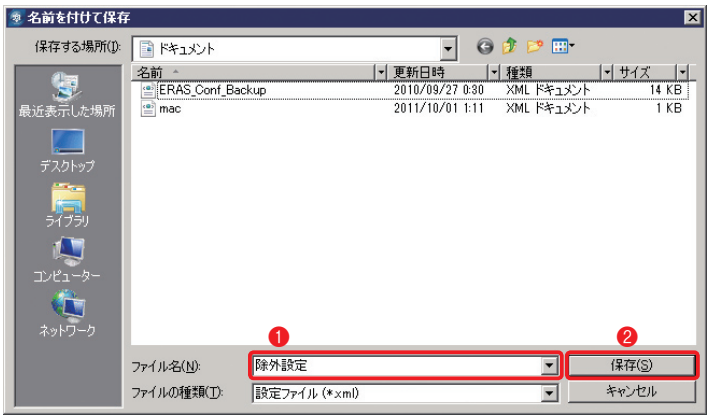
❶ [ツール] メニュー、❷ [ESET コンフィグレーションエディタ] をクリックします。

3 除外ファイルの登録を行います



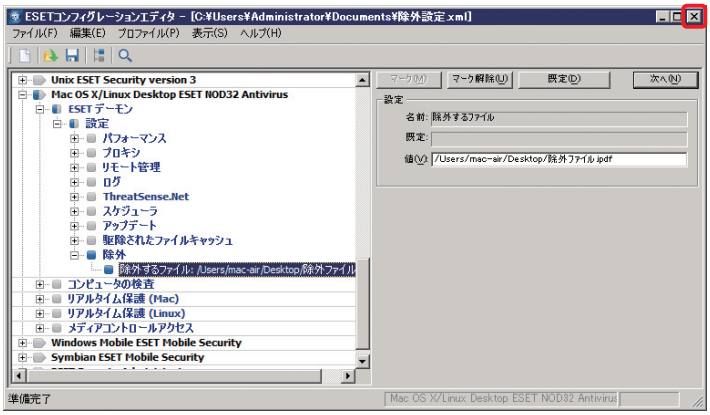
❶ [Mac OS X/Linux Desktop ESET NOD32 Antivirus] をクリックし、❷ [ESET デーモン]、❸ [設定]、❹ [除外] と順にクリックしていき、❺ [除外ファイル：] をクリックします。❻「値」の欄に除外したいファイルをフルパスで入力します。❼「保存」ボタンをクリックします。

4 設定ファイルを保存します



❶ファイル名を入力し、❷[保存] ボタンをクリックします。

5 ESET コンフィグレーションエディタを閉じます



[閉じる] ボタンをクリックし、ESET コンフィグレーションエディタを閉じます。

POINT

作成したファイルを新規タスクまたはポリシーマネージャーを利用して配布する方法については、Windows用のユーザーズガイド 運用編をご参照ください。

6 保存した設定ファイルを [新規タスク] または [ポリシーマネージャ] から一括して配布します。

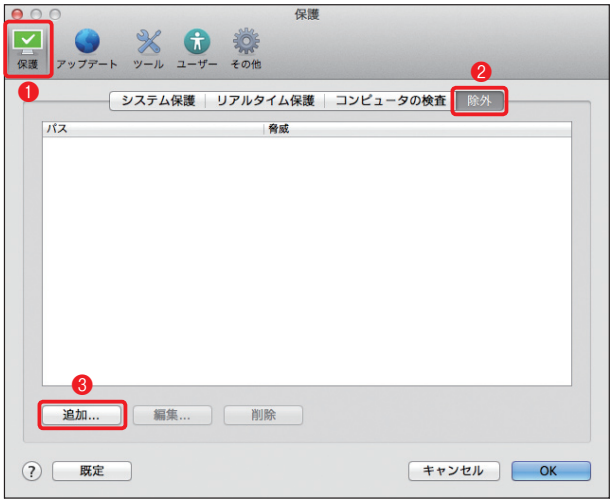
ウイルスとして検出されたファイルを検査対象から除外する～クライアントPC編

ここでは、クライアント側でファイルの除外設定を行う手順を説明します。

1 メインウィンドウを開きます

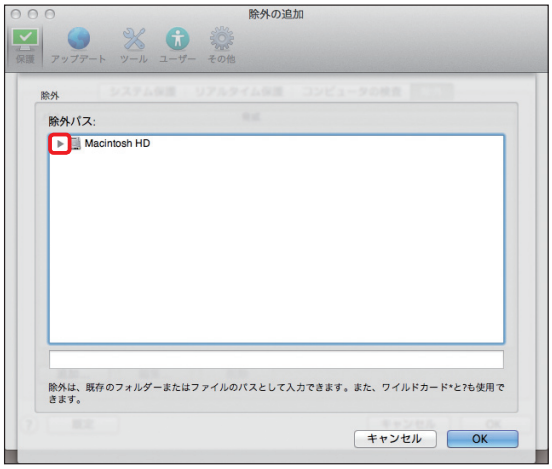
メインウィンドウを開き、詳細モードに切り替えて、❶[設定]ボタンをクリックし、❷[アプリケーションの設定を入力する]をクリックします。

2 除外したいファイルの登録作業を開始します



❶[保護]ボタンをクリックし、❷[除外]をクリックします。❸[追加]ボタンをクリックします。

3 フォルダー一覧を表示します

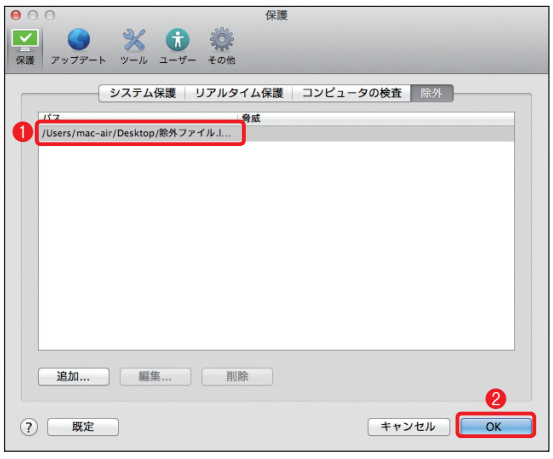


[▶] をクリックします。

4 除外したいファイルを選択します

❶除外したいファイルをクリックし、❷[OK] ボタンをクリックします。

5 ファイルが登録されます



❶選択したファイルが除外ファイルに登録されます。❷[OK] ボタンをクリックします。

POINT

除外リストには、フォルダーも登録できます。フォルダーを除外するときは、手順4で、フォルダーを選択し、[OK] ボタンをクリックするか[除外] 欄に除外したいフォルダーのフルパスを入力し、[OK] ボタンをクリックします。

運用編

[Chapter 5]
クライアントPC用ソフトウェアの利用方法

05-01 クライアントPC用ソフトウェアの使い方について

本節では、クライアントPC用ソフトウェアESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの「ヘルプ」の閲覧方法について説明します。

クライアントPC用ソフトウェアの操作を確認するには

クライアントPC用ソフトウェアには、各種操作方法や詳細な設定方法を記載した「ヘルプ」が準備されています。各クライアントが各種設定を行う場合や操作方法および設定方法の確認を行いたい場合は、ヘルプをご確認ください。

なお、ヘルプの閲覧方法には、すべてのヘルプを確認する方法と各種設定画面に準備された［ヘルプ］ボタンを利用する方法があります。前者のすべてのヘルプを確認する場合は、ヘルプ内の文字検索を利用することで必要な情報を検索できます。後者の［ヘルプ］ボタンを利用した場合は、その画面に応じたヘルプが表示されます。必要に応じて、ご活用ください。

すべてのヘルプを表示するには

すべてのヘルプを表示したいときは、以下の手順で行います。

1 メインウィンドウを開きます

本プログラムのメインウィンドウを開き、❶[ヘルプ]ボタンをクリックし、❷[ヘルプを開く]をクリックします。

2 ヘルプが表示されます

本プログラムのヘルプが表示されます。❶閲覧したい項目をクリックすると、それに対応したヘルプが表示されます。❷検索ボックスを利用するとキーワード検索が行えます。

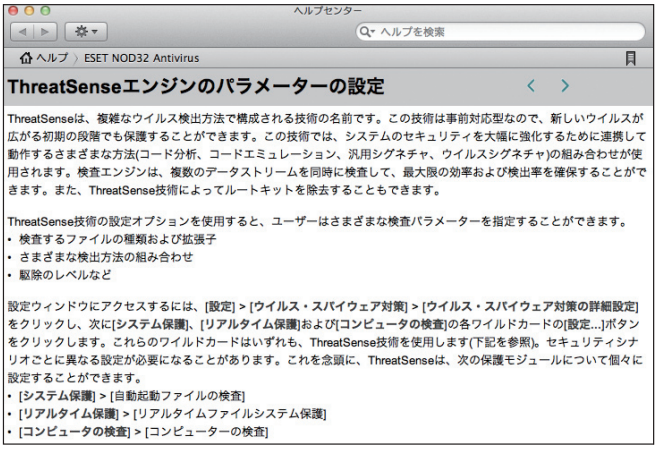
[ヘルプ] ボタンでヘルプを表示するには

各種設定画面に準備された [ヘルプ] ボタンでヘルプを表示したいときは、以下の手順で行います。

1 設定画面を開きます

詳細設定画面を開きます。[?] ボタンをクリックします。

2 ヘルプが表示されます



画面に対応したヘルプが表示されます。

[FAQ]
よくある質問

質問事項一覧

	質問事項	参照ページ
01	Mac OS Xでのコンピュータの検査に時間がかかる	123ページ
02	スプラッシュ画面を非表示にするには	124ページ

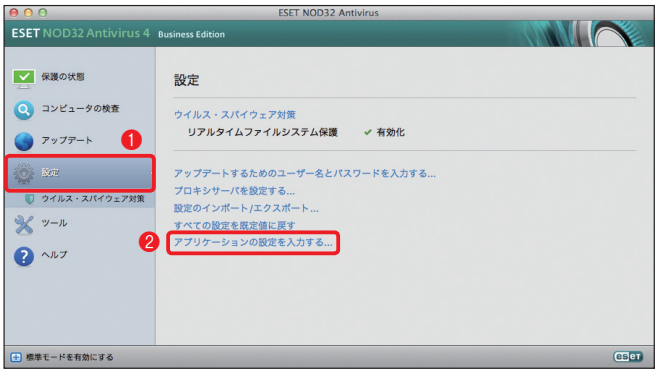
Mac OS Xでのコンピューターの検査に時間がかかる

起動ディスク以外にマウントされているディスクなどを併せて検査の対象とすると、検査の対象数が多くなり、検査に時間がかかります。検査時間を短縮したい場合は、「カスタム検査」の検査対象から「/Volumes」下のネットワークドライブ、Time Machineのバックアップ先などを外して検査を行ってください。

スプラッシュ画面を非表示にするには

ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの起動時に表示されるスプラッシュ画面を非表示にしたいときは、以下の手順で設定を行います。

1 メインウィンドウを開きます



メインウィンドウを開き、詳細モードへ切り替えてから、❶[設定]ボタンをクリックし、❷[アプリケーションの設定を入力する]をクリックします。

2 設定を行います

❶[ユーザー]ボタンをクリックし、❷[インタフェース]をクリックします。❸[起動時にスプラッシュウィンドウを表示する]のチェックを外し、❹[OK]ボタンをクリックします。

お問い合わせの際に

弊社では、お客様からのお問い合わせの際、サポート対応を迅速にするために以下のファイルなどの取得をお願いすることがあります。

●取得をお願いする情報の例

取得情報	含まれている情報	取得する目的	参照ページ
システム情報の取得	端末にインストールされているアプリケーションやハードウェア、ネットワーク環境などの情報が含まれています。	不具合が発生するアプリケーションの有無の確認や動作環境に問題がないかを確認するために取得します。	126 ページ
コンソールメッセージ	コンピューターで実行された各種タスクやアプリケーションの動作ログが含まれています。	アプリケーション実行時などに発生したエラー情報などを確認するために取得します。	128 ページ
プロセス情報の取得	コンピューター上で動作中のドライバやアプリケーションなどの情報が含まれています。	不具合が発生するアプリケーションの有無などを確認するために取得します。	130 ページ
ESET 製品の設定ファイル	端末にインストールされている、ESET 製品の設定内容が含まれています。	不具合の原因となる誤った設定の有無などを確認するために取得します。	132 ページ
スクリーンショット	ディスプレイ上に表示されている、画面のみの情報です。	実際に表示されたエラー画面などを確認するために取得します。	134 ページ

CAUTION

取得する情報には、ユーザー名／パスワードなどの個人情報が含まれている場合があります。お取り扱いには十分ご注意ください。

システム情報の取得方法

ご利用のパソコンのシステム情報の取得は、以下の手順で行います。ここでは、Mac OS X Lion v10.7のシステム情報の取得手順を説明します。

1 アップルメニューをクリックします

❶[アップルメニュー] をクリックし、❷[この Mac について] をクリックします。

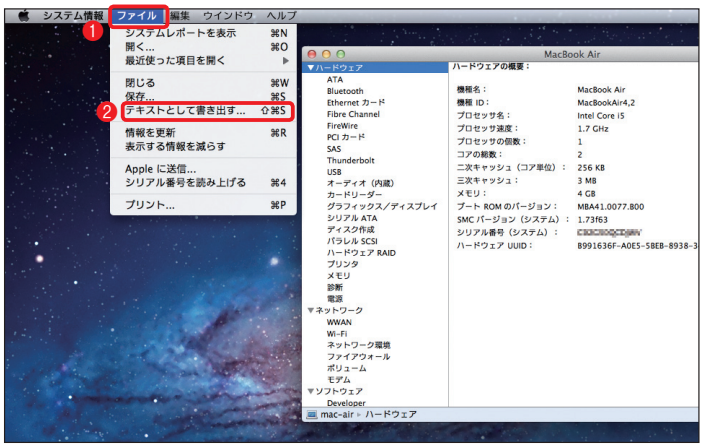
2 画面が表示されます

[詳しい情報] ボタンをクリックします。

3 画面が切り替わります

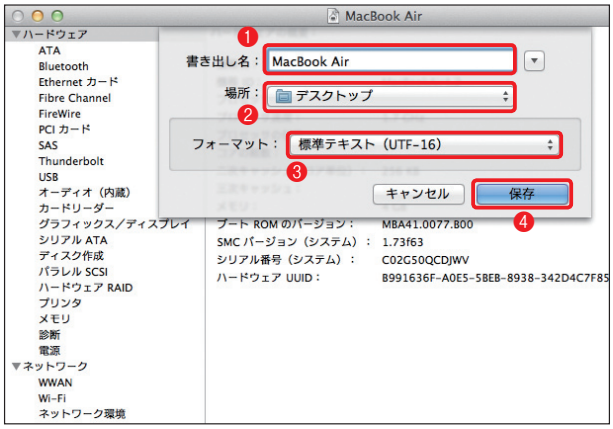
[システムレポート] ボタンをクリックします。

4 システムレポートが表示されます。



❶メニューバーの [ファイル] をクリックし、❷ [テキストとして書き出す] をクリックします。

5 ファイルを保存します



❶ファイル名を入力し、❷ [場所] のプルダウンメニューから保存場所を選択し、❸ [フォーマット] のプルダウンメニューから [標準テキスト (UTF-16) を選択し、❹ [保存] ボタンをクリックします。

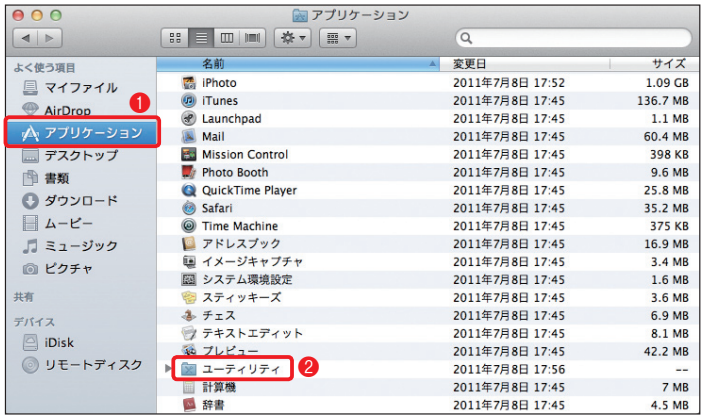
6 ファイルが保存されます

システムレポートが保存されます。

コンソールメッセージの取得方法

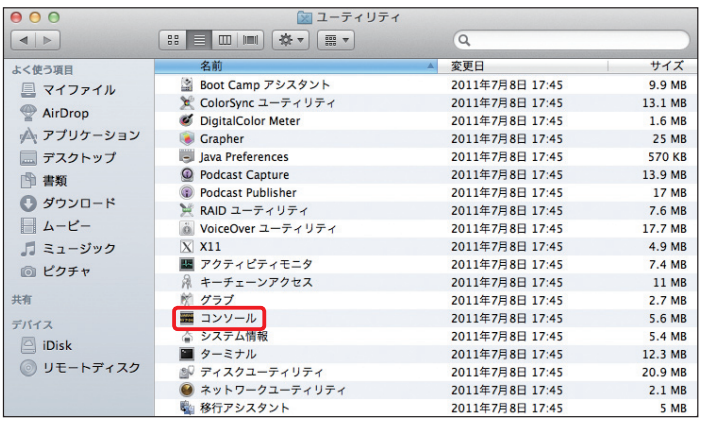
ご利用のパソコンのコンソールメッセージの取得は、以下の手順で行います。

1 Finderを起動します



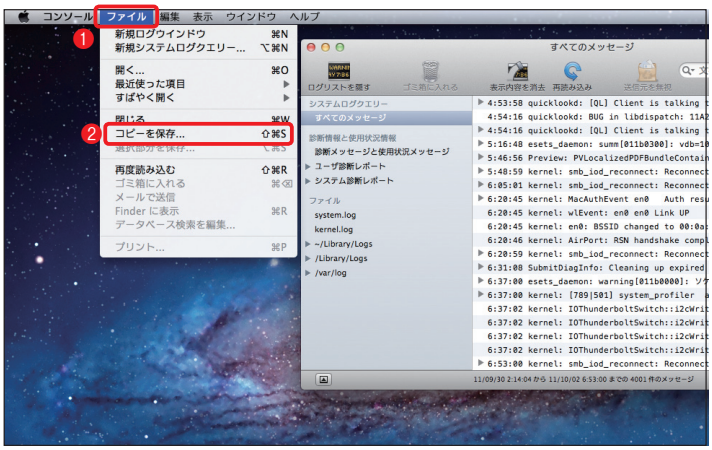
Finderを開き、❶[アプリケーション]をクリックして、❷[ユーティリティ]フォルダーをダブルクリックします。

2 コンソールを起動します



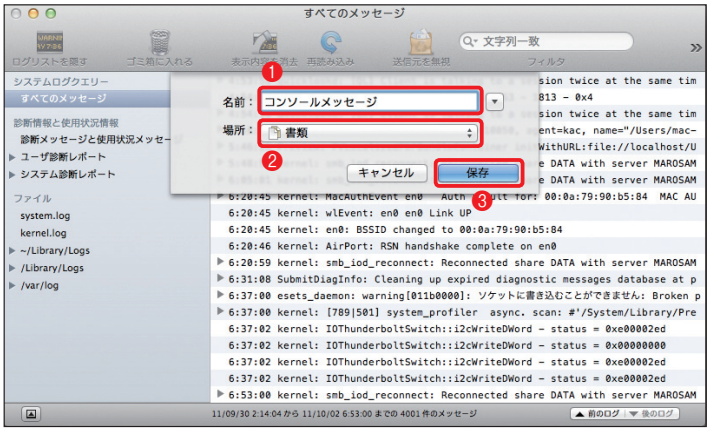
[コンソール]アイコンをダブルクリックします。

3 ファイルの保存を始めます



コンソールが起動します。❶メニューバーの［ファイル］をクリックし、❷［コピーを保存］をクリックします。

4 ファイルを保存します

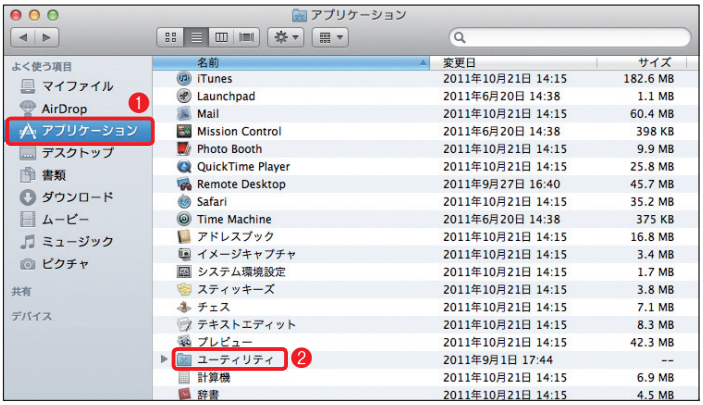


❶ファイル名を入力し、❷［場所］のプルダウンメニューから保存場所を選択します。❸［保存］ボタンをクリックします。

プロセス情報の取得方法

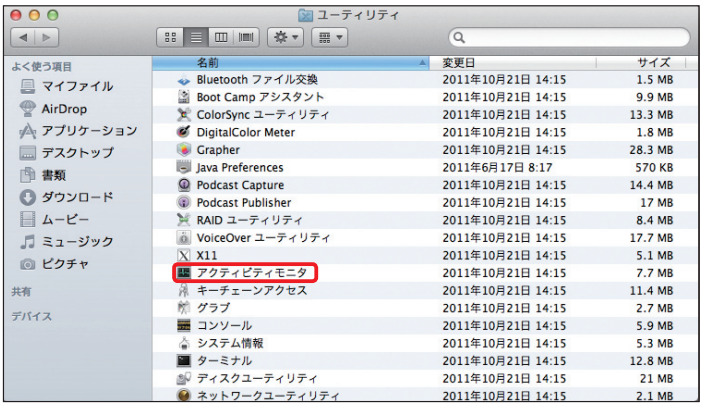
ご利用のパソコンのプロセス情報の取得は、以下の手順で行います。

1 Finderを起動します



Finderを開き、❶[アプリケーション]をクリックして、❷[ユーティリティ]フォルダーをダブルクリックします。

2 アクティビティモニタを起動します



[アクティビティモニタ]アイコンをダブルクリックします。

3 ファイルの保存を始めます

アクティビティモニタが起動します。❶メニューバーの［ファイル］をクリックし、❷［保存］をクリックします。

4 保存を実行します

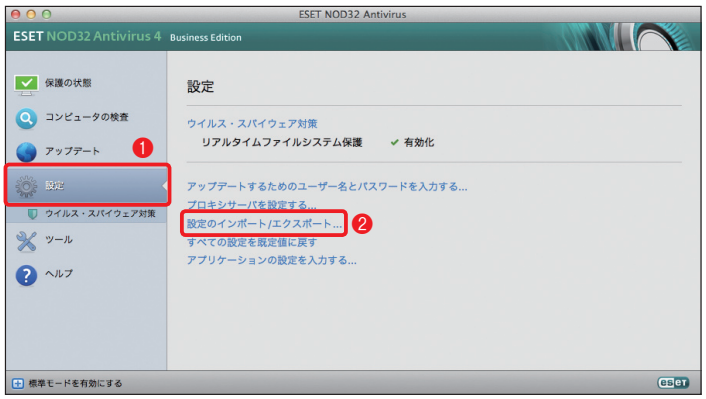
❶ファイル名を入力し、❷［場所］のプルダウンメニューから保存場所を選択します。❸［標準テキスト］にチェックを入れ、❹［保存］ボタンをクリックします。

ESET製品の設定ファイルの取得方法

ESET製品の設定ファイルには、クライアントPC用ソフトウェアの設定ファイルとESET Remote Administrator（ERA）の設定ファイルがあります。クライアントPC用ソフトウェアの設定ファイルは、クライアントPC用ソフトウェアを直接操作することで取得できます。ERAの設定ファイルは、ESET Remote Administrator Maintenance Tool（ERAメンテナンスツール）を利用して取得します。ここでは、ESET NOD32アンチウイルス V4.0 Mac OS X用プログラムの設定ファイルの取得方法を説明します。

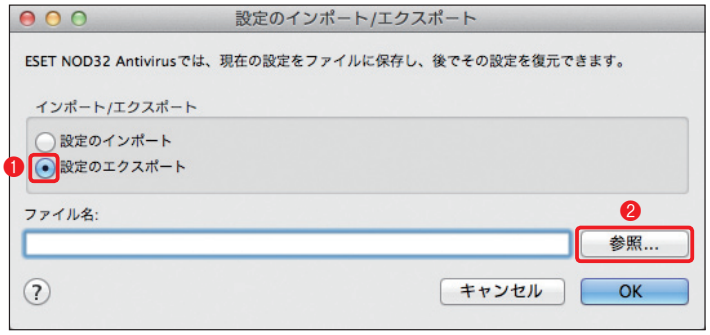
ERAの設定ファイルの取得方法については、Windows用のユーザーズガイド 運用編をご参照ください。

1 メインウィンドウを開きます



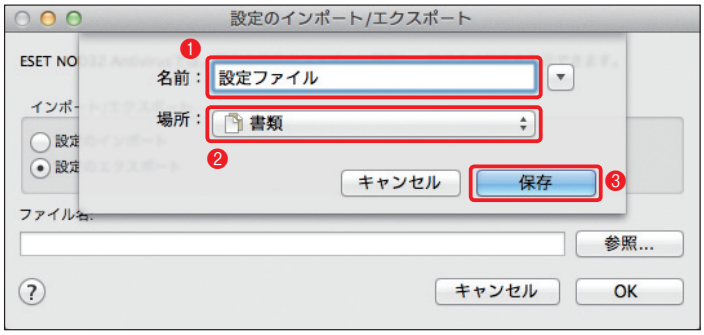
メインウィンドウを開き、詳細モードに切り替えてから、❶[設定]ボタンをクリックして、❷[設定のインポート/エクスポート]をクリックします。

2 設定ファイルの保存を開始します



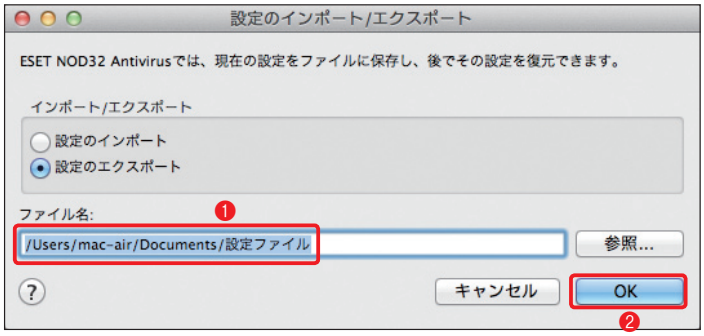
❶[設定のエクスポート]をクリックし、❷[参照]ボタンをクリックします。

3 保存先などを設定します



❶ファイル名を入力し、❷保存先を［場所］のプルダウンメニューから選択します。❸［保存］ボタンをクリックします。

4 設定ファイルを保存します



❶保存するファイルがフルパスで表示されます。❷［OK］ボタンをクリックすると、設定ファイルが保存されます。

スクリーンショットの作成方法

ご利用のパソコンのスクリーンショットの取得は、以下の手順で行います。

フルスクリーンでスクリーンショットを取得する場合

[shift] キーと [command] キーを押しながら、[3] キーを押します。デスクトップ上にファイルが作成されます。

選択したウィンドウのスクリーンショットを取得する場合

[shift] キーと [command] キーを押しながら、[4] キーを押し、続いて [スペース] キーを押します。マウスポインターがカメラアイコンに変わるので、スクリーンショットを取得したいウィンドウ上で、クリックします。デスクトップ上にファイルが作成されます。

POINT

ERAなどに関するFAQはWinows用のユーザーズガイド 運用編をご参照ください。