

目次

目次			
Chapter 1	1.1	ESET ライセンス製品の運用と構成	8
ESET ライヤンス製品の導入		1.1.1 運用と構成方法の検討	8
とその際の検討事項		1.1.1.1 クライアント管理機能導入の検討	8
		1.1.1.2 ミラーサーバー機能導入の検討	8
P.7		1.1.1.3 利用するクライアント用プログラムの選択	9
		1.1.1.4 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	… 10
	1.2	新規導入や他社製品からの乗り換えによる導入の流れ	· 11
		1.2.1 導入の流れ	… 11
	1.3	STEP1 クライアント用プログラムの検討	· 12
		1.3.1 チェックポイント	12
		1.3.1.1 クライアント用プログラムの選択	12
		1.3.1.2 動作環境の確認	… 12
		1.3.1.3 既存のセキュリティ製品との違いを確認	… 12
	1.4	STEP2 サーバー構成の検討	· 13
		1.4.1 チェックポイント	13
		1.4.1.1 管理サーバーの必要性	13
		1.4.1.2 ミラーサーバーの必要性	··· 15
		1.4.1.3 ミラーサーバーの種類の検討	··· 15
		1.4.1.4 データベースの種類の検討	··· 16
		1.4.1.5 動作環境の確認	··· 17
		1.4.2 サーバー構成のモデルケース	… 18
		1.4.2.1 診断フロー	18
		1.4.2.2 モデルケース1	
		クライアント用プログラムのみを利用する場合	19
		管理サーハーを利用する場合 (ミフーサーハーなし)	20
		1.4.2.4 モテルゲース3 100ユーサー以下・官埕機能なし	22
		1.4.2.5 モデルケース4 1,000 グライアント以下・官理機能なし	23
		1.4.2.7 モデルケース5 400ユーリー以下	24
		1.4.2.7 モブルケース7 1.000~ 5.000ユーザー程度(1)	26
		1.4.2.9 モデルケース8 1,000 ~ 5,000 ユーザー程度⑦	27
		14210 モデルケース9 5000~ 10000 フーザー程度	28
		1.4.2.11 モデルケース10 10.000ユーザー以上複数拠点がある場合	29
		1.4.3 Android 端末の管理構成	30
		1.4.3.1 Wi-Fiを利用してERAに接続	30
		1.4.3.2 VPNを利用して ERA に接続	30
	1.5	STEP3 ネットワーク環境の検討	· 31
		1.5.1 チェックポイント ······	31
		1.5.1.1 ネットワーク負荷の検討	31
		1.5.1.2 インターネットへの通信経路の確認	31
		1.5.1.3 サーバーとクライアントPC間の通信経路の確認	31
		1.5.2 トラフィックの制御	32
		1.5.2.1 ①クライアント管理に伴うトラフィック	32
		1.5.2.2 ウイルス定義データベースのアップデートに伴うトラフィック	33

1.6	STE	P4 移行	テプランの検討	34
	1.6.1	チェック	/ポイント	34
		1.6.1.1	他社製プログラムのアンインストール方法の検討	34
		1.6.1.2	クライアント用プログラム導入方法の検討	34
		1.6.1.3	移行プランの作成	35
	1.6.2	クライブ	?ント用プログラム導入方法~ Windows 編	36
		1.6.2.1	診断フロー	36
		1.6.2.2	導入の流れ	37
		1.6.2.3	リモートインストール利用時の条件	39
	1.6.3	クライブ	?ント用プログラム導入方法~ Mac OS X編 ⋯⋯⋯⋯⋯	41
		1.6.3.1	インストール方法	41
		1.6.3.2	手動インストールする場合の導入の流れ	42
		1.6.3.3	リモートインストールする場合の導入の流れ	43
	1.6.4	クライブ	′ント用プログラムの導入方法~ Linux 編 ───────────	44
		1.6.4.1	インストール方法	44
		1.6.4.2	手動インストールする場合の導入の流れ	44
	1.6.5	クライア	ント用プログラムの導入方法~ Android 編	• 45
		1.6.5.1	インストール方法	45
		1.6.5.2	設定読み込み型インストールする場合の導入の流れ	45
		1.6.5.3	Link Generatorを利用してインストールする場合の導入の流れ	47
	1.6.6	複数の扱	L点がある場合のインストール	53
		1.6.6.1	クライアント展開のポイント	53
		1.6.6.2	ポリシー機能とグループ機能を利用した展開の流れ	54
	1.6.7	クライブ	パント用プログラムと	
		サーバー	-用プログラムの設定のポイントと注意点	55
1.7	STE	P5 移行	行作業	58
1.8	バー	ジョンア	'ップによる導入	59
	1.8.1	バージョ	ンアップ時のポイント ・・・・・	59
	1.8.2	ESET 2	キュリティ ソフトウェア シリーズ ライセンス製品 V4.2	
		からのパ	バージョンアップ	60
		1.8.2.1	クライアントPCのみで運用している場合のバージョンアップ手順…	60
		1.8.2.2	管理サーバーとクライアントPCで運用している場合の	
			バージョンアップ手順	61
		1.8.2.3	ミラーサーバーとクライアントPCで運用している場合の	
			バージョンアップ手順	62
		1.8.2.4	管理サーバーとミラーサーバーによる運用をしている場合の	
			バージョンアップ手順1 ~管理サーバーとミラーサーバーが	
			同じコンピューターの場合	63
		1.8.2.5	管理サーバーとミラーサーバーによる運用をしている場合の	
			バージョンアップ手順2 ~管理サーバーとミラーサーバーが	
			異なるコンピューターの場合	64

Chapter 2	2.1
クライアント PC の	
効率的な管理方法	2.2
P.67	
	2.3

2.1	効率的な管理を行うための機能・・・・・	68
	2.1.1 主な管理機能	68
2.2	ダッシュボード機能・・・・・	69
	2.2.1 ダッシュボード機能とは	69
2.3	グループ機能・・・・・	70
	2.3.1 グループ機能とは	70
	2.3.2 静的グループとパラメータグループ	71
	2.3.2.1 静的グループ	71
	2.3.2.2 パラメータグループ	72
2.4	タスク機能・・・・・・	73
	2.4.1 タスクとは	73
	2.4.2 タスクの種類	74
	2.4.3 タスクの設定手順	75
	2.4.4 [コンフィグレーション]タスクの設定方法	76

目次

目次			
		2.4.4.1 新規作成	76
		2.4.4.2 作成済みの設定ファイル (.xml)を利用	76
		2.4.4.3 テンプレートから作成	76
	2.5	ポリシー機能・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	· 77
		2.5.1 ポリシー機能とは	77
		2.5.2 ポリシーの親子関係	77
		2.5.3 ポリシーを利用した設定適用の流れ	78
	2.6	通知機能	· 79
		2.6.1 通知ルール作成の流れ	79
	2.7	ロールバック機能・・・・・・	· 81
		271 ロールバック機能とは	81
	28	ミラー機能	· 82
	2.0		02
		2.0.1 アップブートファイルの配布とミノー機能 2.8.2 アップデートファイルの配布方法	83
		2.8.2 アラフラードアティルの記憶の法	84
		2831 ミラーサーバーの構成例1~ミラーサーバーが1台の場合	84
		2.8.3.2 ミラーサーバーの構成例2~ミラーサーバーが2台以上の場合	85
		2.8.4 ミラーサーバー構築時の注意点	86
		2.8.4.1 ライセンスキーファイル ·····	86
		2.8.4.2 プロキシサーバーが設置されている場合	86
		2.8.4.3 プログラムコンポーネントのダウンロード設定について	86
		2.8.4.4 共有フォルダーを利用する場合	86
		2.8.4.5 リムーバブルメディアを利用する場合	86
		2.8.5 オフライン環境での更新	··· 87
		2.8.6 ウイルス定義データベースの時差配信	88
		2.8.6.1 遅延アップデートを利用した時差配信	88
		2.8.6.2 ミラーサーバーの多段構成による時差配信	89
	2.9	Android 端末の管理	· 90
		2.9.1 Android端末の識別	90
Chapter 3	3.1	障害対策のポイント	· 94
ERA のログ管理		3.1.1 バックアップを利用したサーバーの復旧	94
P.93	3.2	バックアップの作成	· 95
		3.2.1 ERASの設定ファイルのバックアップ作成手順	95
		3.2.2 クライアント情報のデータベースのバックアップ作成手順	100
		3.2.3 データフォルダーのバックアップ方法	104
		3.2.4 データフォルダーのバックアップ方法の流れ	104
	3.3	バックアップファイルの復元	· 105
		3.3.1 バックアップした ERASの設定ファイルの復元手順	105
		3.3.2 バックアップしたクライアント情報のデータベースの復元手順	108
		3.3.3 データフォルダーのリストア(復元)	112
		3.3.4 データフォルダーのリストア (復元)の流れ	112
	3.4	ログ管理のポイント	· 113
		3.4.1 ERAサーバーログ	113
		3.4.2 クライアントPC情報ログ	113
		3.4.3 ERAサーバーログの設定変更手順	114
		3.4.4 クライアントPC情報ログの設定変更手順	115

Chapter 4	4.1	ウイルス対策のポイント・・・・・	· 118
ウイルス対策における運用		4.1.1 ウイルス対策における運用	118
D 117	4.2	日常の運用	· 119
		4.21 日堂の運用フェーズ	119
		422 クライアントPCの状態を確認するには	120
	43	ウイルス検出時(緊刍時)の対応	· 122
	4.0		100
	4.4		100
	4.4	リイルス検工時の対応例	• 123
		4.4.1 ウイルスが検出されたときの対処手順	123
		4.4.2 STEP1 管理者への通知	124
		4.4.3.1 ERAを利用したリモート検査の実施手順	125
		4.4.3 STEP2 ワイルスの隔離・駆除・削除	125
		4.4.4 STEP3 報告~レホートの作成 ····································	128
	4 5	4.4.5 STEP4 防止・抑止束の週用 ·······	130
	4.5	ワイルス誤検出時の対応	• 131
		4.5.1 ファイルがウイルスとして検出された場合の対応手順	131
		4.5.2 隔離されたファイルの復元手順~クライアントPC編(Windowsの場合)	132
		4.5.3 隔離されたファイルの復元手順~クライアントPC編(Mac OS Xの場合) …	133
		4.5.4 隔離されたファイルの復元手順~クライアントPC編 (Linuxの場合)	134
		4.5.5 隔離されたファイルの復元手順~クライアントPC編 (Androidの場合)	135
		4.5.6 隔離されたファイルの復元手順~ ERA編	137
		4.5.7 ウイルスとして検出されたファイルをウイルス検査対象から	
		除外する手順~クライアントPC編(Windowsの場合)	139
		4.5.8 ウイルスとして検出されたファイルを検査対象から	
		除外する手順~クライアントPC編(Mac OS Xの場合)	141
		4.5.9 ワイル人として検出されたノアイルを検査対象から	
		除外する手順 (Linuxの場合) ····································	143
		4.5.10 ウイルスとして検出されたファイルをウイルス検査対象から	
		מדער רו באוין עי לין לאין	140
Chapter 5		質問事項一覧	150
よくあろ質問		お問い合わせの際に	168
		環境設定ファイル (SysInspector)の情報 (*.zip)の取得方法	169
わ向い合わせの際に		Windowsのシステム情報 (*.txt) の取得方法	172
P.149		Mac OS Xのシステム情報の取得方法	173
		Mac OS Xのコンソールメッセージの取得方法	175
		Mac OS Xのプロセス情報の取得方法	177
		ESET製品の設定ファイル (.xml)の取得方法	179
		スクリーンショットの作成方法	190

■本書について

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

○文中に出てくるERAは「ESET Remote Administrator」、ERASは「ESET Remote Administrator Server」、ERACは「ESET Remote Administrator Console」のことです。

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

○文中に出てくるクライアントPCは、Windows端末、Mac端末およびAndroid端末を総称しています。

■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が異なっている場合があります。また本書の内容は、 改訂などにより予告なく変更することがあります。

○本製品の一部またはすべてを無断で複写、複製、改変することはその形態を問わず、禁じます。

- ○本書の著作権は、キヤノンITソリューションズ株式会社に帰属します。ESETセキュリティ ソフトウェア シリーズの各 プログラムの著作権は、ESET, spol. s r.o. に帰属します。
- ○ESET、NOD32、ThreatSense、ESET Endpoint Protection、ESET Endpoint Security、ESET Endpoint アンチウイ ルス、ESET File Security、ESET Remote Administrator、ESET Smart Security、ESET NOD32アンチウイルス、 ESET Mobile Securityは、ESET, spol. s r.o. の商標です。
- ○Microsoft、Windows、Windows Vista、Windows Server、Active Directory、Access、SQL Serverは、米国Microsoft
 Corporationの米国、日本およびその他の国における登録商標または商標です。
- Apple、Apple Remote Desktop、App Store、AirDrop、AirPort、Boot Camp、ColorSync、Finder、FireWire、 iDisk、iTunes、iPhoto、Launchpad、Macintosh、Mac、Mac OS、MacBook Air、Mission Control、Photo Booth、 QuickTime、Safari、Time Machineは、米国およびその他の国で登録されているApple Inc. の商標です。

[Chapter]] ESET ライセンス製品の 導入と その際の検討事項

1.1	ESET ラ	イセンス製品の運用と構成	8
1.2	新規導入	や他社製品からの乗り換えによる導入の流れ	11
1.3	STEP1	クライアント用プログラムの検討	12
1.4	STEP2	サーバー構成の検討	13
1.5	STEP3	ネットワーク環境の検討	31
1.6	STEP4	移行プランの検討	34
1.7	STEP5	移行作業	58
1.8	バージョン	ンアップによる導入	59

1.1 ESET ライセンス製品の 運用と構成

ESET ライセンス製品は、クライアント用プログラムとクライアント管理用プログラムで構成されます。本節では、規模に応じたESET ライセンス製品の運用方法について説明します。

1.1.1 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、クライアント用プログラムのみの運用と、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。

|1.1.1.1 クライアント管理機能導入の検討

クライアント管理用プログラム「ESET Remote Administrator (ERA)」を利用することで、クライアントPCのウイル ス警告、ファイアウォール警告、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、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。

管理するクライアント数が多い場合など2台以上の管理サーバーを設置する場合は、「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。ERAを使用する場合は、Windowsが必要になります。

POINT

クライアント管理用プログラムの主な機能については、「ESET ライセンス製品 ご利用の手引」をご参照ください。

|1.1.1.2 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。ミラーサーバーの構築は、ESET Remote AdministratorやESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、 ESET File Security for Linuxで構築できます。

また、ミラーサーバーからのアップデートファイルの配布方法には、以下の方法が準備されています。クライアント用 にインストールするセキュリティプログラムによって対応する配布方法が異なりますので、ミラーサーバーを構築する 場合は、この点に留意して、設置を行ってください。

Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ

●アップデートファイルの配布方法とセキュリティプログラムの対応一覧

		Windows用 セキュリティプログラム	Mac OS X用 セキュリティプログラム	Linux用 セキュリティプログラム
配布方法	プログラム	ESET Endpoint Security ESET Endpoint アンチウイルス ESET File Security for Microsoft Windows Server Windows用プログラムの旧バー ジョン	ESET NOD32アンチウイルス	ESET File Security for Linux
HTTP経由による	製品内蔵のHTTP サーバー機能を 利用	0	0	0
アップデート	Microsoft Internet Information Service(IIS)を利用	0	0	0
共有フォルダーを 利用したアップ	製品をインストール したコンピューター の共有フォルダーを 利用	0	×	×
デート	他のコンピューター の共有フォルダーを 利用	0	×	×
リムーバブルメ ディアを利用した アップデート	CD-RやDVD-R、 USBメモリー など	0	×	×

|1.1.1.3 利用するクライアント用プログラムの選択

ESET ライセンス製品は、ライセンス形態ごとに複数のクライアント用プログラムが提供されます。お客さまは、提供 されたクライアント用プログラムの中からOSや用途に応じて自由に利用するセキュリティプログラムを選択できます。

	プログラム	概要
Widnows クライアント用	ESET Endpoint セキュリティ 🔝	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プログラム。
	ESET Endpoint アンチウイルス EAw	
Windows サーバー用プロ グラム	ESET File Security for Microsoft Windows Server	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プログラ
Mac OS X用プログラム	ESET NOD32アンチウイルス 🔤	Δ_{\circ}
Linux サーバー用プログラ ム	ESET File Security for Linux 🚯	
Android用プログラム	ESET Endpoint セキュリティ for Android <u>ESA</u>	ウイルス・スパイウェア対策をはじめ、迷惑メール対策、盗難対策などの 機能を搭載した総合セキュリティプログラム。

>>> POINT

各プログラムの主な機能については、「ESET ライセンス製品 ご利用の手引」をご参照ください。

1.1

|1.1.1.4 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PC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アップデートされるため、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どうか、また、負荷を分散させるために2台以上のサーバーを導入 するかどうかなどを検討します。

>>> 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を13ページで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。



新規導入や他社製品からの 乗り換えによる導入の流れ

本節では、他社製のセキュリティプログラムからESET ライセンス製品に乗り換える場合の移行方法について説明します。新規導入の際も、導入の流れは同様です。

1.2.1 導入の流れ

他社製品からの移行を行う場合に重要なのが、移行期間においてセキュリティレベルを低下させることなくスムーズな 移行を行うことです。弊社では、スムーズな移行のために以下のステップで作業を行うことを推奨しています。



1.2

STEP1 クライアント用プログラムの 検討

クライアント用プログラムの検討では、クライアント用プログラムの動作環境や既存のセキュリティ製品との違いを確認し、変更を行った場合にどのような変化が発生するのかを検討します。以下のような点に着目して検討してください。

1.3.1 チェックポイント

1.3

1.3.1.1 クライアント用プログラムの選択

ESET ライセンス製品は、製品ごとに複数のクライアント用プログラムが提供されます。提供されるクライアント用プログラムの機能などを検討し、どのセキュリティプログラムを利用するのが適しているかを検討します。

プログラム	製品	ESET Endpoint Protection Advanced	ESET Endpoint Protection Standard
Windowett	総合セキュリティプログラム ESET Endpoint Security	0	_
WINDOWS用	ウイルス・スパイウェア対策プログラム ESET Endpoint アンチウイルス	0	0
Mac OS X用	ウイルス・スパイウェア対策プログラム ESET NOD32アンチウイルス	0	0
Windowsサーバー用	ウイルス・スパイウェア対策プログラム ESET File Security for Microsoft Windows Server	0	0
Linuxサーバー用	ウイルス・スパイウェア対策プログラム ESET File Security for Linux	0	0
Android用	総合セキュリティプログラム ESET Endpoint Security for Android	0	0

1.3.1.2 動作環境の確認

導入予定のクライアントPCが、各セキュリティプログラムの動作環境を満たしているかどうかを確認します。クライアント用プログラムの動作環境については、各セキュリティプログラムのユーザーズマニュアルをご参照ください。

1.3.1.3 既存のセキュリティ製品との違いを確認

現在利用しているセキュリティ製品との違いを把握して、ESET ライセンス製品を導入することによって発生する変化 を検討します。たとえば、ESET Endpoint Securityを導入すると、ファイアウォール機能が導入されるので、これま で行えていたアプリケーションとの通信が遮断される可能性があります。このため、ESET Endpoint Securityを導入 する場合は、ファイアウォールルールの変更などを検討する必要があります。

>>> POINT

各プログラムの主な機能については、「ESET ライセンス製品 ご利用の手引」をご参照ください。

1.4 STEP2 サーバー構成の検討

サーバー構成の検討では、クライアント管理機能やミラーサーバーの必要性を検討し、サーバーの動作環境などを確認 します。以下の点に着目して検討してください。

1.4.1 チェックポイント

1.4.1.1 管理サーバーの必要性

クライアント管理用のサーバーを導入すると、クライアントPCの状況を集中管理したり、クライアントPCに導入した ESET ライセンス製品の動作設定などを配布できます。

管理サーバーの導入

管理サーバーの導入にあたっては、管理サーバーとして運用するコンピューターにESET Remote Administrator Server (ERAS) を、ERASをリモート操作する管理用コンピューターにESET Remote Administrator Console (ERAC) をインストールします。それぞれのインストールは、弊社ユーザーズサイトからダウンロードしたインストー ラーを実行することで行います。

なお、ERASおよびERACはWindows用プログラムです。またERAのインストールには、「ライセンスキーファイル(.lic ファイル)」が必要です。ESET ライセンス製品ご利用の手引を参考に、弊社ユーザーズサイトからライセンスキーファ イル (.licファイル)をあらかじめダウンロードしてください。



POINT

ERASのリモート操作に利用するERACは、複数のコンピューターにインストールできます。また、ERASをインストールしたコンピューターにもインストー ルできます。 3

4

1.4

STEP2 サーバー構成の検討

ERA導入時の注意点

ここでは、ERAを導入するときの注意点について説明します。ERAは、ネットワークを利用してクライアントPCの情報 を取得したり、ウイルス定義データベースのアップデートを行います。適切な設定を行わないと、情報の取得や操作が 正常に行えないのでご注意ください。

■ プロキシサーバー

インターネット接続にプロキシサーバーの経由が必要な環境にミラーサーバーを設置する場合は、ミラーサーバーがプロキシサーバー経由でESET社の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するように設定する必要があります。設定手順については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

なお、ウイルス定義データベース (*.nup) は、プロキシサーバーでキャッシュを行わないように設定してください。プロキシサーバーのキャッシュ仕様によっては、ウイルス定義データベースがもつデジタル署名が不整合を起こし、クライアントPCでのアップデートができなくなります。

■ファイアウォールソフトの設定

ERASをインストールしたコンピューターやミラーサーバーに設定したコンピューターでファイアウォール機能を搭載 したプログラムが動作していると、クライアントPCがウイルス定義データベースのアップデートに失敗したり、ERAC をインストールした管理用コンピューターからリモート操作が行えない場合があります。

ERACからのリモート操作が行えない場合やクライントPCがウイルス定義データベースのアップデートに失敗する場合 は、ファイアウォール機能を搭載したプログラムが動作しているかどうかを確認してください。ファイアウォール機能 を搭載したプログラムが動作している場合は、その設定を確認し、ERASがERACとの通信に利用するポートおよびクラ イアントPCとの通信に利用するポートを開放します。ミラーサーバーの場合も同様に、クライアントPCがアップデー トに利用するポートを開放します。ERASやミラーサーバーでは、既定値として以下の通信ポートを利用します。

プロトコル	ポート番号	用途
TCP	2221	クライアントPCからミラーサーバーへの接続
	2222	クライアントPCからERASへの接続
	2223	ERACからERASへの接続
	2224	リモートインストール用エージェントからERASへの接続
	2225	ダッシュボードサーバーからERASへの接続
	2846	管理サーバー(ERAS)を複数設置した場合に、下位の管理サーバー(ERAS)から上位の管理サーバー(ERAS) への接続

■既存ネットワークに新たにERAを導入する場合の確認事項

ERAはWindows環境で動作するため、「Windows Server Client Access License (CAL)」の確認が必要です。新 規のコンピューターを導入するときなど、追加でCALを購入するケースが発生することがあるのでご注意ください。 Windows CALの詳細については、Microsoft社にご確認ください。

POINT

ミラーサーバーにおけるウイルス定義データベースの保存先をCALの概念のない、NASやストレージサーバー、Linuxで構築したサーバーに置くことで CALが必要ないケースもあります。 ミラーサーバーを設置すると、ウイルス定義データベースなどのアップデートをミラーサーバー経由で行えます。これ によりクライアントはウイルス定義データベースのアップデートの際にインターネット接続が不要になるので、インター ネット回線への負荷が軽減されます。

ミラーサーバーの構築は、ESET Remote AdministratorやESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxで構築できます。また、ESET Remote Administrator やESET Endpoint アンチウイルスでミラーサーバーを構築した場合は、差分アップデート(ナノアップデート)やSSL 接続などの機能も利用できます。

プログラム	ESET Remote Administrator	ESET Endpoint アンチウイルス	ESET File Security for Microsoft Windows Server	ESET File Security for Linux
差分アップデート機能	0	0 ×		×
ミラーサーバーのSSL対応	0	0	×	×
メリット	 IISと組み合わせて構築することで、大規模環境でのミラーサーバーとして利用するできる インターネット側のネットワーク負荷の軽減 インターネットへ直接アクセスできないクライアントPCのアップデートが可能 USBメモリーやCD-Rを経由した、オフラインによるアップデートが可能(Windows用プログラムのみ対応) 	 クライアントOSで利用 できるため、小規模環境 でミラーを構築できる インターネット側のネッ トワーク負荷の軽減 インターネットへ直接ア クセスできないクライア ントPCのアップデート が可能 USBメモリーやCD-Rを 経由した、オフラインに よるアップデートが可能 (Windows用プログラム のみ対応) 	 Windows Serverでミ ラーサーバーを構築する 場合に利用 インターネット側のネッ トワーク負荷の軽減 インターネットへ直接ア クセスできないクライア ントPCのアップデート が可能 USBメモリーやCD-Rを 経由した、オフラインに よるアップデートが可能 (Windows用プログラム のみ対応) 	 Linuxでミラーサーバー を構築する場合に利用 インターネット側のネッ トワーク負荷の軽減 インターネットへ直接ア クセスできないクライア ントPCのアップデート が可能
デメリット	 ウイルス検査機能が搭載 されていないため、ウイ ルス検査機能をもったプ ログラムと併用する必要 がある。 	●サーバー OSで利用でき ないため、大規模環境で は利用できない	●差分アップデートが利用できないため、ベースアップ デート時には約30MBの定義ファイル配信が発生する	

※ESET Endpoint SecurityおよびMac OS X用のESET NOD32アンチウイルスは、ミラーサーバー構築機能をサポートしていません。

1.4.1.3 ミラーサーバーの種類の検討

ミラーサーバーを設置してアップデートファイルを配布する方法には、HTTPサーバーを利用した配布や共有フォルダー を利用した配布があります。HTTPサーバーを利用する場合の配布方法およびクライアントPCの台数は以下を目安にご 検討ください。

HTTPサーバー	クライアント数
ESET Remote Administrator Server(ERAS)内蔵のHTTPサーバー	400台
ESET Endpoint アンチウイルス内蔵のHTTPサーバー	100台
ESET File Security for Microsoft Windows Server内蔵のHTTPサーバー	100台
ESET File Security for Linux内蔵のHTTPサーバー	1,000台
Microsoft Internet Information Services(IIS)	3,000台
Apache	3,000台

STEP2 サーバー構成の検討

2

3

1.4

|1.4.1.4 データベースの種類の検討

ERASをインストールした管理サーバーでは、クライアントPCで発生したログをデータベースに登録して管理します。 ここでは、ERASで利用するデータベースについて説明します。

利用できるデータベースの種類と最大容量

管理サーバーで利用されるデータベースは、登録できる保存容量の違いによって以下のデータベース形式をサポート しています。既定値では、1,000クライアントで3カ月間のログを保存することを目安とした最大保存容量「2GB」の Microsoft Access形式のデータベースが利用されます。1,000クライアント以上で利用する場合は、「クライアント数」 とログの「保存期間」を考慮してデータベースの形式を決定してください。

●利用できるデータベースの形式と最大保存容量

データベースの形式	登録可能な最大容量
Microsoft Access(既定のデータベース形式)	最大2GB
Microsoft SQL Server 2005 / 2008 Express Edition	最大4GB
Microsoft SQL Server 2008 R2 Express Edition	最大10GB
Microsoft SQL Server 2005 / 2008 Standard Edition	最大値なし

利用データベースの選定の目安

管理サーバーに保存されるクライアントログの容量は、管理するクライアント数とログの保存期間によって変動します。 必要なデータベースの容量は、以下の例を目安に計算します。

●データベース形式選定の目安

ログの容量	1回あたり約2.1KB
クライアント用に作成される1日あたりのログ	6件
 ログの保存期間	3カ月(90日)

POINT

ログの保存期間の既定値は、ウイルスログが6カ月間、その他のログが3カ月間です。

例

クライアント数1,000の環境で、3カ月間ログを保存した場合のデータベース容量

1,000台 (クライアント数)×6件 (件/日)×2.1KB (1回あたりのログ容量)×90日 (保存期間)

=1134MB

●クライアント数に応じた推奨データベース形式

クライアント数	3カ月間保存した場合の推定容量	利用できるデータベースの形式
1,000	1134MB	Microsoft Access, Microsoft SQL Server 2005/2008 Express Edition
2,000	2268MB	Microsoft SQL Server 2005/2008 Express Edition
3,000	3402MB	Microsoft SQL Server 2005/2008 Express Edition
4,000	4536MB	Microsoft SQL Server 2008 R2 Express Edition
5,000以上	5670MB	Microsoft SQL Server 2008 R2 Express Edition

CAUTION

ERAとMicrosoft SQL Serverとの接続は、SQL Server認証を推奨します。Windows認証を利用し、かつERASとデータベースサーバーが異なるコンピュー ターの場合は、ERASのサービスの動作アカウントには、データベースへのアクセス権限があるユーザー(ドメインアドミニストレーターなど)を設定してく ださい。アクセス権がない場合は、インストールに失敗します。

Chapter	

1.4.1.5 動作環境の確認

管理サーバーやミラーサーバーを設置する場合は、サーバーとして利用するコンピューターが推奨される動作環境を満たしているかどうかを確認します。クライアント管理用プログラムの動作環境については、弊社製品ホームページ上を ご参照ください。

1.4.2 サーバー構成のモデルケース

ここでは、サーバー構成のモデルケースと、各ケースのサーバースペック例を紹介します。サーバー構成を検討する際 の参考にしてください。

1.4.2.1 診断フロー

ネットワーク構成 ケース診断



1.4.2.2 モデルケース1 クライアント用プログラムのみを利用する場合

クライアント用プログラムのみを用いた運用では、サーバーの設置が不要です。

なお、この構成で利用する場合、各クライアントはインターネットに接続し、ESET社のサーバーから最新のウイルス定 義データベースなどのアップデートファイルを取得するように設定します。



構成

クライアントのみで構成します。サーバーは必要ありません。

FAQ

1.4

|1.4.2.3 モデルケース2 管理サーバーを利用する場合(ミラーサーバーなし)

管理サーバーのみを用いた運用の場合は、クライアント管理用プログラム(ERA)を導入し、ERAを利用して各クライア ントを管理します。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は、各クライアントPCが直接ESET社のサー バーから取得します。

このモデルケースでは、クライアント数が400台程度でサーバー要件が変わる点にご注意ください。



構成

■クライアント数400台未満

- ●1台のサーバーで管理サーバーを運用
- ●データベースは、既定のMicrosoft Access形式 (mdb) を利用

■ クライアント数400台以上

- ●1台のサーバーで管理サーバーを運用
- ●データベースは、Microsoft SQL Server 2005以降を利用 ※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

サーバースペック

■ クライアント数400台未満

- ●インテル Pentium4 2.4GHzと同等以上の性能を有したCPU
- ●2GB以上のメモリー
- ●1Gbpsのネットワークアダプター

■ クライアント数400台以上

- ●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
- ●1Gbpsのネットワークアダプター

クライアントの接続間隔

■クライアント数400台未満

●管理サーバーへの接続間隔:10分

■ クライアント数400台以上

●管理サーバーへの接続間隔:30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、サーバーの設定などにより異なります。

|1.4.2.4 モデルケース3 100ユーザー以下・管理機能なし

ミラーサーバーは、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社内LAN経由でクライアントPCに提供 するものです。ミラーサーバーを設置することで、各クライアントPCはアップデートのためのインターネット接続が不 要になります。これにより、インターネット接続にかかわるトラフィックが軽減されるほか、インターネット接続環境 にないクライアントPCにもアップデートファイルを容易に配布できます。

ミラーサーバー機能は、クライアント管理用プログラムであるERAと、Windows用のクライアント用プログラムであるESET Endpoint アンチウイルスおよびESET File Security for Microsoft Windows Server、Linuxサーバー用のESET File Security for Linuxに搭載されています。また、ESET Endpoint アンチウイルスは、サーバーOSをサポート対象外としていますので、Windowsサーバーでご利用の場合は、ESET File Security for Microsoft Windows Serverを使用してください。

ESET Endpoint アンチウイルスおよびESET File Security for Microsoft Windows Serverを利用してミラーサー バーを構築する際、クライアントPCの台数は100台以下を推奨しています。



構成

●1台のサーバーでミラーサーバーを運用

●ESET Endpoint アンチウイルスまたはESET File Security for Microsoft Windows Server、ESET File Security for Linux内蔵のHTTPサーバー機能を利用してアップデートファイルを配布

クライアント数の目安

●100台

サーバースペック

●インテル Pentium4 2.4GHzと同等以上の性能を有したCPU

●2GB以上のメモリー

●1Gbpsのネットワークアダプター

クライアントの接続間隔

●ミラーサーバーへの接続間隔:60分

CAUTION

上記は、参考値です。接続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、サーバーの設定などにより異なります。

1.4.2.5 モデルケース4 1,000クライアント以下・管理機能なし

ESET File Security for Linuxをミラーサーバーとして運用します。

アップデートファイルの配布にはESET File Security for Linuxの内部HTTPサーバーである[ESET Mirror http daemon]を利用します。

このモデルケースでは、ミラーサーバーにLinuxを利用しますのでCALが不要となり、コストを軽減することができますが、ESET File Security for Linuxでミラーサーバー機能を利用する場合、差分アップデート機能に対応していないため、ウイルス定義データベースのアップデート時にネットワーク負荷がかかる場合があります。



構成

●一台のサーバーでミラーサーバーを運用

●ESET File Security for Linuxの内部HTTPサーバー機能を利用してアップデートファイルを配布

クライアント数の目安

●~1,000台

サーバースペック

- ●インテルPentium 4 互換プロセッサ2.0GHzと同等以上の性能を有したCPU
- ●2GB以上のメモリー
- ●1Gbpsのネットワークアダプター

クライアントの接続間隔

●ミラーサーバーへの接続間隔:60分

>>> POINT

クライアント数が1,000台以上ならApacheを利用してアップデートファイルを配布してください。

CAUTION

上記は、参考値です。接続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って異なります。

4

FAQ

1.4

|1.4.2.6 モデルケース5 400ユーザー以下

ERAは、管理機能だけでなくミラー機能も搭載しています。そのため、ERAをインストールするだけでサーバーを管理 サーバー兼ミラーサーバーとして運用させることが可能です。

2つの機能を1台のサーバーで兼用させる場合、それぞれの機能による負荷が1台のサーバーにかかることになります。 サーバーに大きな負荷がかかる場合は、管理サーバーとミラーサーバーを別々に設置すること、さらには各サーバーを それぞれ2台以上設置することをご検討ください。



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
```

●ESET Remote Administrator Server (ERAS) 内蔵のHTTPサーバー機能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、既定のMicrosoft Access形式 (mdb) を利用

クライアント数の目安

●~400台

サーバースペック

●インテル Pentium4互換のプロセッサ 2.4GHzと同等以上の性能を有したCPU

●2GB以上のメモリー

●1Gbpsのネットワークアダプター

クライアントの接続間隔

●管理サーバーへの接続間隔:10分

●ミラーサーバーへの接続間隔:120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。
```

|1.4.2.7 モデルケース6 400~1,000ユーザー程度

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。

アップデートファイルの配布には、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1.000台です。

このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。



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
- ●Microsoft Internet Information Services (IIS) を利用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以降を利用
- ※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

●~1.000台

サーバースペック

- ●インテル Pentium4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- ●4GB以上のメモリー
- ●1Gbpsのネットワークアダプター

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。
```

1.4

1.4.2.8 モデルケース7 1,000~5,000ユーザー程度①

管理サーバーとミラーサーバーを別々のコンピューターで運用します。

アップデートファイルの配布には、Microsoft Internet Information Services (IIS) を利用します。このモデルケース における管理サーバーの接続クライアント数の上限は5,000台です。また、アップデートファイルの配布に利用するIIS のミラーサーバーの接続クライアント数は、3,000台です。そのため3,000台以上のクライアントが接続する場合は、 IISのミラーサーバーを複数台設置してください。

このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。 また、外部のデータベースを利用することで、管理サーバーとデータベースを分離します。



構成

- ●管理サーバーとミラーサーバーを別々のコンピューターで運用(管理サーバー1台/ミラーサーバー1台以上)
- Microsoft Internet Information Services (IIS) を利用してアップデートファイルを配布 (接続クライアント数が、3,000台を超える場合は、IISのミラーサーバーを複数台設置)
- ●データベースは、Microsoft SQL Server 2005以降を利用
 ※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

●~5,000台

サーバースペック

- ●インテル Pentium4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- ●4GB以上のメモリー
- ●1Gbpsのネットワークアダプター

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:60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。

1台のサーバーを管理サーバー兼ミラーサーバーとして運用しますが、ストレージにRAID 0構成のHDDまたはSSDを利用します。

アップデートファイルの配布には、Microsoft Internet Information Services (IIS) を利用します。このモデルケース における管理サーバーの接続クライアント数の上限は5,000台です。また、アップデートファイルの配布に利用するIIS のミラーサーバーの接続クライアント数は、3,000台です。そのため3,000台以上のクライアントが接続する場合は、 IISのミラーサーバーを複数台設置してください。

このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。



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

(クライアント数が3,000台以上の場合は別途ミラーサーバーを設置)

●Microsoft Internet Information Services (IIS) を利用してアップデートファイルを配布 (接続クライアント数が、3,000台を超える場合は、IISのミラーサーバーまたはApacheのミラーサーバーを複数台 設置)

●データベースは、Microsoft SQL Server 2005以降を利用 ※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

●~5,000台

サーバースペック

- ●インテル Pentium4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- ●4GB以上のメモリー
- ●1Gbpsのネットワークアダプター

●RAID O構成のHDDまたはSSD

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:60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。

1.4

|1.4.2.10 モデルケース9 5,000~10,000ユーザー程度

管理サーバーとミラーサーバーを別々のコンピューターで運用します。また、ミラーサーバーは、ストレージにRAID 0 構成のHDDまたはSSDを利用します。アップデートファイルの配布には、Microsoft Internet Information Services (IIS)を利用します。このモデルケースにおける管理サーバーの接続クライアント数の上限は10,000台です。また、アッ プデートファイルの配布に利用するIISのミラーサーバーの接続クライアント数は、3,000台です。そのため3,000台以 上のクライアントが接続する場合は、IISのミラーサーバーを複数台設置してください。

このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。 また、外部のデータベースを利用することで、管理サーバーとデータベースを分離します。



構成

- ●管理サーバーとミラーサーバーを別々のコンピューターで運用(管理サーバー1台/ミラーサーバー1台以上)
- ●Microsoft Internet Information Services (IIS) を利用してアップデートファイルを配布 (接続クライアント数が、3,000台を超える場合は、IISのミラーサーバーを複数台設置)
- ●データベースは、Microsoft SQL Server 2005以降を利用

※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

●~10,000台

管理サーバーのサーバースペック

●インテル Pentium 4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU ●2GB以上のメモリー

●1Gbpsのネットワークアダプター

ミラーサーバーのスペック

●インテル Pentium 4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU

●4GB以上のメモリー

●1Gbpsのネットワークアダプター

●RAID O構成のHDDまたはSSD

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:60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。

1.4.2.11 モデルケース10 10,000ユーザー以上複数拠点がある場合

複数の拠点がある場合は、前ページまでの構成例を目安に、各拠点または部署ごとに管理サーバーやミラーサーバーを 設置します。このモデルケースでは、下位管理サーバーのデータを複製する機能を利用して、VPNなどを介して本社な どに設置された上位管理サーバーへ集約します。



構成

●設置する拠点や部署の規模に応じて、小規模や中規模の構成例を目安にする

サーバースペック

●設置する拠点や部署の規模に応じて、小規模や中規模の構成例のスペックを目安にする

クライアントの接続間隔

●設置する拠点や部署の規模に応じて、小規模や中規模の構成例を目安にする

1.4

1.4.3 Android 端末の管理構成

ERAを利用してESET Endpoint Security for Androidを管理する場合、Wi-FiやVPNを利用してERAに接続する方法 があります。なおESET Endpoint Security for Androidの主な機能はERAで管理しなくても利用可能です。

1.4.3.1 Wi-Fiを利用してERAに接続

Wi-Fiを利用してESET Endpoint Security for AndroidをERAに接続します。この構成ではWi-Fiに対応した無線LAN アクセスポイント機器などを社内に設置し、Android端末のWi-Fi接続機能を利用し社内ネットワークに接続します。



1.4.3.2 VPNを利用してERAに接続

VPNを利用してESET Endpoint for AndroidをERAに接続します。この構成ではVPN装置を設置し、Android端末の VPN接続機能を利用してインターネット(社外)から社内に設置したERAへセキュアに接続できます。





ネットワーク環境の検討では、ESET ライセンス製品を導入することで発生する社内ネットワークの負荷の影響や、クライアントPCとサーバー間の通信経路を確認します。以下の点に着目して検討してください。

1.5.1 チェックポイント

1.5.1.1 ネットワーク負荷の検討

ESET ライセンス製品を導入することで発生する通信トラフィックが、他業務などのネットワーク環境に影響を与えないかを検討します。ESET ライセンス製品の導入によって発生する通信トラフィックについては、32ページをご参照ください。

1.5.1.2 インターネットへの通信経路の確認

ミラーサーバーは、インターネットを利用してESET社のアップデート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の入手を行います。インターネット接続の経路上にプロキシサーバーやファイアウォールが設置 されていないかを確認し、ミラーサーバーの通信に影響がないかを確認します。

|1.5.1.3 サーバーとクライアントPC間の通信経路の確認

管理サーバーとミラーサーバーは、定期的にクライアントPCとの通信を行います。管理サーバー/ミラーサーバーとク ライアントPC間の通信経路を確認し、ファイアウォールなどで通信が遮断される可能性がある場合は、設定の変更を検 討します。 1.5

STEP3

ネットワーク環境の検討

2

4

FAQ

1.5.2 トラフィックの制御

管理サーバーやミラーサーバーを導入すると、各種サーバーとクライアントPCとの間で定期的に通信が行われます。 ESET ライセンス製品を導入することで発生する通信トラフィックは、クライアント管理に伴うトラフィックとウイル ス定義データベースのアップデートに伴うミラーサーバー向けのトラフィックに大別されます。



|1.5.2.1 ①クライアント管理に伴うトラフィック

クライアントPCと管理サーバー間の通信です。定期的(既定値では10分間隔)にクライアントPCからログなどの情報 が送信されます。また、管理サーバーからは設定ポリシーの配布などが行われます。

クライアント管理に伴うトラフィックは、以下の項目の設定を変更することによって制御することができます。 ●ログレベル

管理サーバーがクライアントPCから取得するログの種類を減らすことによって、トラフィックを減少させます。 ●定期検査のタイミング

クライアントPCに定期検査を設定している場合、検査を行う日時をグループ分けすることによってスキャンログを分 散させます。

通信内容	サイズ	備考
ウイルスログ	数KB	クライアントが検出したウイルス情報です。
ファイアウォールログ (※ESET Endpoint Securityのみ)	数KB	ARP・DNSなどを利用した侵入検出の通信情報です。この情報は、環境によっては、 1台で1日に数十件発生することもあります。
イベントログ	数KB	ウイルス定義データベースアップデートの成功・失敗などのイベントです。 環境によっては、1台で1日に数十件発生することもあります。
スキャンログ	数KB~数100KB	スキャン対象の設定により、ログの容量が変動します。
隔離ログ	数KB	クライアントがウイルスを隔離したログです。ウイルスの蔓延状況によりログの容量 が変動します。
HIPSログ	数KB	マルウェアやコンピューターのセキュリティに悪影響を与えようとする望ましくない活動からシステムを保護するHIPSのログです。既定値では、このログは取得されません。
デバイスコントロールログ	数KB	USBストレージやCD / DVDなどのデバイスの制御動作のログです。既定値では、このログは取得されません。
Webコントロールログ	数KB	Webコントロール動作のログです。既定値では、このログは取得されません。
モバイルログ	数KB	セキュリティ監査やスパム対策の情報です。
ESET Live Grid	数KB ~	ヒューリスティック機能により検出したウイルス情報をESET社に送付します。データ 量は、検知したウイルスファイルと同等のサイズになります。
コンフィグレーション	数KB	ESET製品の設定情報になります。
保護機能・保護状態	数KB	ESET製品の保護状態の情報になります。
システム情報	数KB	HW、SW、ウイルス定義データベースのバージョンなどの情報です。

CAUTION

ウイルスログ、スキャンログ、ファイアウォールログ、イベントログが大量に発生した場合、サーバーやネットワークに大きな負荷がかかります。大規模な 環境では、ログの保存期間の設定などによるサーバー負荷の減少を検討する必要があります。

1.5.2.2 ウイルス定義データベースのアップデートに伴うトラフィック

クライアントPCとミラーサーバーなどのアップデートサーバー間の通信です。主にクライアントPCのウイルス定義デー タベースのアップデート時に発生します。

ウイルス定義データベースのアップデートに伴うトラフィックは、以下の項目の設定を変更することによって制御する ことができます。

●アップデートの間隔

クライアントPCをグループ分けし、グループごとにアップデートの時間を変えることで、アップデートサーバーへの トラフィックを分散します。ただし、アップデートの間隔を長く設定するほど、ウイルスに対するリスクが増える可 能性があります。

●差分アップデート機能

ESET ライセンス製品は、ウイルス定義データベースのコンパイルのためにパッキングされたファイル (パッキング ファイル)を配信する事があります。これをベースアップデートと呼び、通常、年に3、4回の頻度でベースアップデー トが実施されます。

差分アップデートは、ウイルス定義データベースのコンパイルに必要な情報のみを配信することで、ベースアップデー ト時でも通常のアップデートとほぼ同等サイズのアップデートファイルの配信を行う機能です。これによってベース アップデート時のネットワーク負荷を減らすことができます。

CAUTION

※ESET File Security for Microsoft Windows ServerまたはESET File Security for Linuxでミラーサーバーを構築した場合、差分アップデート機能は サポートされません。このため、ESET File Security for Microsoft Windows ServerまたはESET File Security for Linuxで構築したミラーサーバー からウイルス定義データベースのアップデートを実施した場合、ベースアップデート時には最大約40MBのファイルが配信されます。 ※1週間程度ウイルス定義データベースをアップデートしていない場合は、差分アップデート機能は適用されません。

通信内容		サイズ	備考	
定義データベース		数KB ~数百KB	ウイルス定義データベースになります。	
ベーフマップデート①	差分アップデート 未適用時	数MB ~約15MB	 年に3~4回程度配信されるウイルス定義データベース効率化のためのパッ キンパキャをファイルです	
	差分アップデート 適用時	約数KB~約数百KB	- キンクされにファイルとす。 ※2012年6月2日の実績は約2.2MBとなります。	
ベーフマップデートの	差分アップデート 未適用時	約40MB	年に1回程度配信されるウイルス定義データベース効率化のためのパッキン ダネカをファイルです	
	差分アップデート 適用時	約数KB~約数百KB	※2012年3月27日の実績は約40MBとなります。 	
新モジュール追加		約1MB~約3MB	不定期に新モジュールが追加される場合があります。 ※2012年3月14日の実績は約2MBとなります。	

●ミラーサーバー向けトラフィックの通信仕様

CAUTION

インストール後の初回アップデート時は、通常時と比較してネットワーク負荷が高くなることが予想されるので、ネットワーク障害が発生しないように考慮 する必要があります。

1.5

1.6 STEP4 移行プランの検討

移行プランの検討では、既存プログラムの削除方法や導入するクライアント用プログラム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。

1.6.1 チェックポイント

1.6.1.1 他社製プログラム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プログラム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

●他社製プログラム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

1.6.1.2 クライアント用プログラム導入方法の検討

クライアント用プログラムのインストール方法を、規模やネットワーク環境に合わせて検討してください。クライアント用プログラムのインストール方法には、大きく「手動インストール」と「リモートインストール」の2種類があります。 Windows用プログラムの場合は36ページ、Mac OS X用プログラムの場合は41ページ、Linux用プログラムの場合は45ページをご参照ください。



Chapter	1	

1.6.1.3 移行プランの作成

具体的な移行プランを作成します。移行期間にセキュリティレベルを低下させることを避け、スムーズに移行するため に、新規サーバーでESET製品環境を構築し、十分な検証を行った上で他社製品から順次移行することを推奨しています。 以下に弊社で作成したサンプルプランを掲載しておきますので参考にしてください。

●サンプルプラン

項目	1 カ月目	2カ月目	3 カ月目	4 カ月目
1.サーバー機器、ESET ライセンス製品の手配				
2. サーバーの構築				
3. サーバーの設置				
4. クライアントの展開 (既存プログラムの削除と ESET 製品のイン ストール)				
5. 既存プログラムのライセンス終了 (既存プログラム用サーバーの撤去)				
6.ESET 製品の本番運用				
※既存プログラムと ESET 製品の共存期間		-		

1.6.2 クライアント用プログラム導入方法 ~ Windows編

ESETセキュリティ製品では、クライアント用プログラムのインストールに際して、お客さまの多様な環境に応じるように、いくつかの方法を用意しています。本節では、クライアント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。

1.6.2.1 診断フロー

Windows用プログラムの導入方法は、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複数の方法が用 意されています。以下の診断フローを参考に環境に合わせた導入方法を検討してください。



●クライアント展開の診断フロー
FAQ

1.6.2.2 導入の流れ

設定組み込み済みインストーラーを利用したインストールまたは設定読み込み型インストールを実施する場合は、最初 に組み込む設定内容を検討します。次に、設定組み込み済みイントーラーまたは設定ファイルの作成を行い、利用環境 に応じたインストール方法でクライアント用プログラムをインストールします。





クライアント用プログラム設定のポイント

クライアント用プログラムは、コンピューターの使用環境に応じた設定を施すことによって、より安全かつ効率的な運用が行えます。

設定ファイルの作成

クライアント用プログラムには、サーバーへの接続設定やコンピューターの検査設定など、様々な設定が施されています。 そして、これらの設定はファイルとして保存されており、この設定ファイルをカスタマイズすることによって、多数の コンピューターがあるような環境において、効率的な管理・運用が可能なほか、クライアント用プログラムのインストー ルも容易に行えます。

設定ファイルは、ESET Remote Administrator (ERA) で作成できるほか、クライアント用プログラムでも作成できます。作成方法については、それぞれのユーザーズマニュアルをご参照ください。

1.6

インストール方法

クライアント用プログラムのインストールにあたっては、インストールの実施方法がいくつか用意されているので、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。以降に、インストーラーの違いによる インストール方法およびリモートによるインストールの方法を記載していますので、参考にしてください。

●手動インストール

インストール方法	必要なファイル	特徴
インストーラー (.msi)を利用	●インストーラー(.msi)	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。 サーバークライアント用プログラムの各種設定は、すべて既定値が利用されるので、管理 サーバーやミラーサーバーを設置する場合は、それらへの接続設定など最低限必要となる 設定を、各自プログラムインストール後に行う必要があります。
設定読み込み型 インストール	●インストーラー(.msi) ●設定ファイル ●バッチファイル	クライアント用プログラムの設定ファイルを事前に作成し、その設定ファイルとインストー ラー(.msi)を組み合わせてインストールを行います。設定ファイルの内容をインストール 時に適用できるので、インストール後の設定が不要または最小限にすることができます。 また、設定ファイルの作成に、クライアント用プログラムからのエクスポートを利用した 場合、ESET Remote Administrator(ERA)を利用しなくても、このインストール方法を 利用できます。実際のインストールには、インストーラー(.msi)と設定ファイルの他にイ ンストール用のバッチファイルが必要になります。なお、ESET Endpoint Securityをイ ンストールする場合は、インストールコマンドの引数に"REMOVE=機能名"を付けて実行 することでインストールするコンポーネントを選択できます。詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。
設定組み込み済み インストーラーを 利用	●設定組み込み済みインストー ラー ●バッチファイル(サイレント インストールを行う場合)	インストーラー(.msi)に独自の設定を施したインストーラー(設定組み込み済みインストー ラー)を作成し、それを利用してインストールを行います。設定ファイルの内容をインストー ル時に適用できるので、インストール後の設定が不要または最小限にすることができます。 設定組み込み済みインストーラーの作成には、ERAを利用する必要があります。なお、イ ンストールウィザードを表示しないサイレントインストールを行うには、インストール用 のバッチファイルが必要になります。なお、ESET Endpoint Securityをインストールす る場合は、バッチファイルに記載するインストールコマンドの引数に "REMOVE = (機能 名) "を付けて実行することで必要なコンポーネントのみをインストールすることができま す。詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

※各インストーラーなどは、リムーバブルメディアや共有フォルダーに保存し、各クライアントPC上にコピーして利用します。

●リモートインストール

インストール方法	必要なファイル	特徴
プッシュ インストール	●インストールパッケージ	ERAを利用し、リモートでクライアントPCにログオンしてインストールを行う方法です。 1度の操作で複数のクライアントPCに対して操作を実行できるので、インストール効率は 高くなります。ただし、この方法でインストールを実施するには、対象クライアントPCの 環境に関して各種条件があります。
ログオンスクリプト を利用	●インストールパッケージ	Active Directoryのドメインログオン時にログオンスクリプトを利用して自動インストールを行う方法です。インストールが自動実行されるので、インストール効率は高くなります。ただしこの方法は、Active Directory環境でネットワークを構築している場合にのみ利用できます。
電子メールを利用	●インストールパッケージ	インストールパッケージの一部を電子メールに添付してクライアントPCに送り、ユーザー がそれを実行し、インストールを開始する方法です。インストールパッケージ本体をERA から取得するため、クライアントPCとERAが通信できる必要があります。

※インストールパッケージはERAを利用して作成します。各クライアントPCに適用する内容およびインストール時のオプションを設定することが できます。また、ESET Endpoint Securityをインストールする場合は、必要なコンポーネントのみをインストールするインストールパッケージ を作成できます。詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

● Active Directory 環境とワークグループ環境のそれぞれで推奨されるインストール方法

	インストール方法	Active Directory環境	ワークグループ環境
	インストーラー (.msi)を利用	0	\bigcirc
手動インストール	設定読み込み型インストール	0	\bigcirc
	設定組み込み済みインストーラーを利用	0	0
	プッシュインストール	0	△※ 1
リモートインストール	ログオンスクリプトを利用	0	×
	電子メールを利用	0	∆%2

※1 インストール先のクライアントPCにログオンするためのユーザー名とパスワードが必要。クライアントPCごとにこれらが異なっている場合 は、各々に対して入力する必要があります。

※2 あらかじめ指定したユーザー名とパスワードを利用するため、クライアントPCごとの管理者権限をもつユーザー名とパスワードがすべて同一 でない限り、お勧めできません。

1.6

STEP4

移行プランの検討

3

4

FAQ

|1.6.2.3 リモートインストール利用時の条件

プッシュインストール、ログオンスクリプトを利用したインストール、電子メールを利用したインストールでは、次の 利用条件を満たしている必要があります。インストール作業を実施する前に環境が整っているか必ずご確認ください。 なお、リモートインストールの実施の具体的な手順については、「ESET Remote Administrator ユーザーズマニュア ル」をご参照ください。

①クライアントPCとERASがLAN経由で通信が可能なこと

②クライアントPCがActive Directory環境のメンバの場合、ドメインアドミニストレーター権限を持ったア カウントが利用可能であること

※Active Directory環境の場合、ドメインアドミニストレーター権限のパスワードが空白ではないこと ※プッシュインストール実行時にアカウント名とパスワードの指定が必要となります。

③クライアントPCがワークグループ環境のメンバの場合、各クライアントPCの管理者権限を持ったア カウントが利用可能であること

※管理者権限を持ったアカウントのパスワードが空白ではないこと

※プッシュインストール実行時にアカウント名とパスワードの指定が必要となります。

④クライアントPCのOSがWindows 2000/XP/Vista/7、Windows Server 2003/2008であること

⑤クライアントPC側の通信ポートが通信可能な状態になっていること

●リモートインストール時に利用されるクライアントPCの通信ポート

ポート番号/プロトコル	備考
137/TCP,UDP	NetBios 名前サービス
138/UDP	NetBios データグラムサービス
139/TCP	NetBios セッションサービス
445/TCP,UDP	SMB ダイレクトホスティングサービス

⑥クライアントPCで「Remote Registry」サービスが開始されていること

Remote Registryサービスが開始されているかどうかは、[スタート] メニュー→[コントロールパネル] → [システ ムとセキュリティ] → [管理ツール] → [サービス] で確認できます。Remote Registryサービスが開始されていな い場合は、[Remote Registry] をダブルクリックし、[全般] タブにある [開始] ボタンをクリックしてください。



⑦クライアントPCの共有フォルダーおよびプリンター共有が有効になっていること

⑧クライアントPCのフォルダーオプションで「簡易ファイルの共有を使用する(推奨)」が無効になっていること

※環境によって設定が異なりますので、必ずご確認ください。

- ⑨Windows Vista以降のOS (Windows Server 2008) にリモートインストールする場合、ERASは管理者権限を持つアカウントで動作させること
 - **Active Directory環境の場合は、ドメインアドミニストレーター権限を持ったアカウント、ワークグループ環境の場合は、コンピューターの管理者権限を持ったアカウントで動作させてください。

Chapter 1

Chapter 2

FAQ

1.6.3 クライアント用プログラム導入方法 ~ Mac OS X編

ESET NOD32アンチウイルス は、お客さま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。ここでは、ESET NOD32アンチウイルス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。

1.6.3.1 インストール方法

ESET NOD32アンチウイルス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。

●手動インストール

インストール方法	必要なファイル	特徴
付属のインストー ラー(.dmg)を利用	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。
設定組み込み済みイ ンストーラー(.pkg) を利用	設定組み込み済みインス トーラー(.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。設定組み込み済み インストーラー(.pkg)は、付属のインストーラー(.dmg)を利用して作成します。

●リモートインストール

インストール方法	必要なファイル	特徴
プッシュインストー ル	インストールパッケージ	ERAを利用し、リモートでクライアントPCにログオンしてインストールを行う方法です。1 度の操作で複数のクライアントPCに対して操作を実行できるので、インストール効率は高く なります。ただし、この方法でインストールを実施するには、対象クライアントPCの環境に 関して各種条件があります。
Apple Remote Desktopを利用	設定組み込み済みインス トーラー(.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)で作成した設定組み 込み済みインストーラー(.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。

|1.6.3.2 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プロ グラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET NOD32アンチウイルスのイ ンストールを実施してください。

STEP1 他社製セキュリティプログラムのアンインストール 他社製のセキュリティプログラムを利用している場合は、そのプログラムのアンインストールを行います。 STEP2 設定組み込み済みインストーラーの作成(必要に応じて) 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組み込み済みインストーラー(.pkg)を作成します。

STEP3 イントール作業の実施

STEP2で作成した設定組み込み済みインストーラー(.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

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。

C	ha	nt	er	1	

1.6.3.3 リモートインストールする場合の導入の流れ

ERAは、SSH経由でESET NOD32アンチウイルスをプッシュインストールできます。プッシュインストールを行う場合は、以下の流れで行います。



CAUTION

ERAからプッシュインストールを行うには、以下の条件を満たしている必要があります。

- ・クライアントPCは、SSHを経由したリモートログインが行えるように設定されている必要があります。
- ・ERAがリモートログインに利用するSSHアカウントは、管理者権限のアカウントである必要があります。

POINT

ESET NOD32アンチウイルスは、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」を利用したリモートインストー ルも行えます。詳細は、ESET NOD32アンチウイルス Mac OS Xのユーザーズマニュアルをご参照ください。 1.6

STEP4

移行プランの検討

1.6.4 クライアント用プログラムの導入方法~ Linux 編

ここでは、ESET File Security for Linuxの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。

1.6.4.1 インストール方法

ESET File Security for Linuxのインストール方法は、以下の通りです。

●手動インストール

インストール方法	必要なファイル	特徴
インストーラー (.bin)を利用	インストーラー(.bin)	弊社ユーザーズサイトからダウンロードしたインストーラー(.bin)を利用して、コマンドラ インで作業を行います。インストール作業は、root権限(スーパーユーザー)で行う必要があ ります。また、ソフトウェアの各種設定は、インストール作業完了後にすべて手動で行います。

1.6.4.2 手動インストールする場合の導入の流れ

ESET File Security for Linux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プロ グラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET File Security for Linuxのイ ンストールを実施してください。



1.6.5 クライアント用プログラムの導入方法~ Android 編

Chapter 2

ESET Endpoint Security for Androidは、お客さま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。ここでは、ESET Endpoint Security for Android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。

1.6.5.1 インストール方法

Chapter 1

ESET File Security for Androidのインストール方法は、以下の通りです。インストールの際は、端末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。

●手動インストール

インストール方法	必要なファイル	特徴			
インストーラー (.apk)を利用 インストーラー(.apk)		弊社ユーザーズサイトからダウンロードしたインストーラー(.apk)を利用して、インストー ルを行います。ソフトウェアの各種設定は、インストール作業完了後に手動で行います。			
設定読み込み型イン ストール	インストーラー(.apk) 設定ファイル(xml)	設定ファイルを事前にERA付属のESET コンフィグレーションエディターで作成し、その 設定ファイルとインストーラー(.apk)を組み合わせてインストールを行います。設定ファ イルの内容をインストール時に適用できるので、インストール後の設定を最小限にするこ とができます。設定ファイルは、「settings.xml」というファイル名で保存する必要があり ます。また、インストールを行うときは、設定ファイルをAndroid端末の「/mnt/sdcard」 フォルダーにコピーしてインストール作業を実施します。			
Link Generator を 利用	Generatorを インストーラー(.apk) お定ファイルをERAで事前に作成し、ESET社が提供するLink Generatorで作 ンクとインストーラー(.apk)を組み合わせてインストールを行います。インス (.apk)を利用してインストールした後、対象とするAndroid端末に配布したリン プすることで、Android端末が自動的にERAに接続し、設定が反映されるので、イ ル後の設定を最小限にすることができます。				

1.6.5.2 設定読み込み型インストールする場合の導入の流れ

ESET Endpoint Security for Androidを設定読み込み型インストールする場合を説明します。他社製のセキュリティ プログラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET Endpoint Security for Androidのインストールを実施してください。

設定ファイルの作成はERAで行います。ESET コンフィグレーションエディターを起動して、[製品フィルタ] で [ESET Endpoint Security for Android]を選択し、必要な設定を行ってください。設定後、ファイル名を「settings.xml」でセーブし、Android端末の「/mnt/sdcard」フォルダーにコピーしてインストール作業を実施します。

ここから、設定ファイルの作成手順を説明します。

] [スタート] ボタン>[すべてのプログラム] >[ESET] >[ESET Remote Administrator Console] >[ESET コンフィグレーションエディタ] をクリックしてESET コンフィグレーションエディターを起動します。

🕥 🖉 ESETコンフィグレーションエディター [タイ	(トルなし)
ファイル(E) 編集(E) プロファイル(E) 表示	F(S) ^J/7(B)
」 🛅 🔥 🖬 🖾 🔍 製品フィルタ:	
 Windows製品ラインv3およびv4 Windowsデスクトゥブv5 	ESET Endpoint Artisynus ESET Endpoint Security for Android ESET Endpoint Security for Android ESET Endpoint Security for Android
	EST File South y for Unau(SO)Solario EST File South y for Unau(SO)Solario EST File South y for Microsoft Windows Server EST File South y 4.5 for Microsoft Windows Server EST File South y 4.5 for Microsoft Windows Server Care EST Gateway South y 3 for Unau(SSO)Solario
Remote Administrator	Let valenting relative view transpoorpools is a second of the second of

[製品フィルタ]で[ESET Endpoint Security for Android]を選択します。

1.6



[モバイルログ] > [Endpoint Security for Android] で必要な設定を行います。

	🦉 名前を付けて保存	Ŧ					×
4	(保存する場所(1):	۱۲۶۲۲۶۶ 💽		•	G 🗊 🕩 📴		
	 最近表示した場所 デスクトップ デイフジ シイフジ コンピュージー 	<u>2</u>		 / 更新日時	- 1 ∰28	<u> • </u> サ イズ	
	ネットワーク		0			2	
		ファイル・名(N):	settinesxml			(条存(S)	
		ファイルの種類(T):	設定ファイル (*xml)			キャンセル	

[ファイル] > [名前を付けて保存] をク リックして①ファイル名に[settings. xml]と入力して②[保存]をクリックしま す。

この設定ファイルをAndroid端末の「/mnt/sdcard」フォルダーにコピーしてインストール作業を実施します。

設定読み込み型インストールをする場合は、以下の流れとなります。



設定読み込み型インストールで、ERA付属のESET コンフィグレーションエディターを利用して設定できない項目は、[信頼するSIMカードを定義]、[ESET をデバイス管理者として設定]、[管理者連絡先の定義]です。

1.6.5.3 Link Generatorを利用してインストールする場合の導入の流れ

Link Generatorとは、ESET社が提供しているコマンドラインプログラムです。Link Generatorを利用すると、ERAへ 接続するためのリンクが生成されます。ERAのポリシーマネージャと組み合わせて利用することで、ESET Endpoint Security for Androidをインストール後にリンクをクリックすると同時に設定を反映させることが可能です。 Link Generatorは弊社ユーザーズサイトからダウンロードしてください。

ここでは、Link Generatorを利用してESET Endpoint Security for Androidをインストールする場合を説明します。 他社製のセキュリティプログラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET Endpoint Security for Androidのインストールを実施してください。

ここからLink Generatorを利用したESET Endpoint Security for Androidのインストールから初期設定反映までの 設定例を説明します。お客さまのご利用の環境に合わせて設定を変更してください。

ここではポリシーを二つ作成して、ERAに初めて接続したときに割り当てるポリシーと二回目以降にERAに接続したと きに割り当てるポリシーの作成方法を説明します。



ERACを起動して「ツール」→「ポリシーマネージャ」をクリックします。

Server Poicy (Eset-test-30-pc)	ポリシーなり 既定の既初リー
	現ポリシー(j) N/A
	ポリシーの(見明())
	下位サーバが上位サーバの既定のボリシーを継承するために使用 される仮想ポリシーです。
	一根パンーのエンフィグレーション
	マージを表示(型)。 ・ (単単)(型)。 第121-1725(11)。
	25 (20) 49(0) (1)
	グローバルボリシー設定
	グローバルボリシー設定(0)。
ポリシーツリーの更新(R) ポリシーのインボート(D)	▼ グループからインボード(E)

●「既定の親ポリシー」を選択して2「新し い子ポリシーの追加」をクリックします。



「新しいポリシーを作成」画面で●任意のポリシー名を入力して ❷「OK |をクリックします。

3

1.6



●手順③で作成したポリシー名を選択して、
 で備集」をクリックします。



「ESETコンフィグレーションエディタ」の ●「モバイルログ」→「Endpoint Security for Android」の必要な部分の設定値を入 力し、設定が終了したら2コンソールを クリックし、「はい」をクリックします。

2	
	 シールールウィザード()). テ
現明知力 クライアントフ イルタバウメー	 <u>ے</u>

「ポリシーマネージャ」の**①**「ポリシールー ル」タグをクリックし、**②**「新規作成」をク リックします。 Chapter 2

FAQ

🔊 新しいポリシールールの作成 x 7 ポリシールールの設定 名前(N) 1 New Mobile Client 説明(D) 6 クライアントフィルタパラメータ(E) FROM プライマリサーバ 編集(E) ٠ Ψ. ポリシー(P) 2 New Mobile Client (Win2008r2dc) OK(O) キャンセル(()

Chapter 1

「新しいポリシールールの作成」画面で 「名前」に任意の名前を入力して ②「ポリ シー」で手順③で作成したポリシーを選択 して ③「編集」をクリックします。

4

Q	スルールエディタ		x	
0	ルールの条件			
	□ クライアンド名マスクIN(指定) □ HAS IPv4マスク(指定)	🔊 ルールの条件	A	×
	□HAS IPv4範囲(指定)	ルールの各件を入力(E)	2	3
	 HAS IPv6 ネットワーク識別(指定) 	ESET Endpoint Security for	Android	;宣加(A)
	□HAS 定義済みポリシー(指定)	ルールの条件のリスト(R)		
	▼製品名 IN (指定)			育切除(D)
	□ 家品バージョン 15 (指定) □ カライマット/0月7月/ 休録1 マフト			
	パラメータ			
	9へての東洋かー致した場合に、ル) *v/t//(C)
	以品名 IN 指定) 1			
	1		1 A. 1. A. 1	
			4770AC)	

「ルールエディタ」画面で「ルールの条件] で[IS 新規クライアント]、[製品名IN(指 定)]にチェックを入れ、①「指定」をクリッ クします。[ルールの条件] 画面が開きま すので?[ESET Endpoint Security for Android」と入力して?[追加]、?[OK]、 [OK]とクリックします。

※ [IS 新規クライアント] にチェックを入 れるとERAに初めて接続したクライアン トにのみポリシーが適用されます。

 ●「ポリシールールを今すぐ実行」をク リックし確認画面が出てくるので[はい]、
 [OK]をクリックして、2「適用」、3[OK]
 をクリックします。

R inken	1501	オパシー 歴史のプライマリクライアットオ
[MANTO I REPAIRS I ATOMINATION INTO A	カリシールールウィザード(田). (*)
PORTOX.52.	Merch: 694420 1200-140- 4	
オプション 12時(1) クライアントフ にはがらたー	(ESET Endpoint Security for Android)	
ボルロシンク ボリントフ ジライアントフ ジライアントフ ジライアントフ ジライアントフ ジライアントフ ジライアントフ	N (ESET Endpoint Security for Android)	

手順2から望を繰り返します。その際、手順3で別のポリシー名を入力し、手順5で二回目以降に割り当てるポリシーを作成します。二回目以降に割り当てるポリシーに対して、手順8で[製品名IN(指定)]にだけチェックを入れます。

次にLink Generatorの使用方法を説明します。

コマンドプロンプトを起動させ、Link Generatorの実行ファイル [linkGen.exe] のあるフォルダーに移動して以下のコマンドを実行させます。

linkGen.exe < ERA の IP アドレス> < ERA に接続するポート番号> < TRUE/FALSE > < ERA へ接 続するためのパスワード>

<TRUE/FALSE>:「TRUE」を入力すると自動的に挿入しているSIMカードが信頼するSIMカードとして登録されま す。「FALSE」を入力した場合、信頼するSIMカードに自動的に登録されませんので、手動で信頼するSIMカードを入力 してください。

<ERAへ接続するためのパスワード>:ERAへとの接続にパスワード認証を有効にしている場合のみ入力してください。

入力例

ERAのIPアドレスが192.168.xxx.xxx、ポート:2222、信頼するSIMカードを挿入してERAにクライアントが接続する時にパスワード認証が「password」の場合の以下のようになります。

linkGen.exe 192.168.xxx.xxx 2222 TRUE password

以下、Ling GeneratorをCドライブの「EESA_Link_Generator」フォルダー内に置いて、条件は上記の場合の使用方法 について説明します。

│ [スタート] ボタン→ [すべてのプログラム] → [アクセサリ] からコマンドプロンプトを起動します。



「cd C: ¥EESA_Link_Generator」と入 力してEnterキーを押下します。 「EESA_Link_Generator」フォルダー の中にLink Generatorのプログラム 「linkGen.exe」があります。

3

am コマンド プロンプト Wicrosoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:VUsersVeset-test-80>cd C:VEESA_Link_Generator C:VEESA_Link_Generator?[LinkGen.exe 192.168.xxxx.xxx 2222 TRUE password > Link.txt] 「linkGen.exe 192.168.xxx.xxx 2222 TRUE password > link.txt」と入力して Enterキーを二回押します。



「EESA_Link_Generator」フォルダーにlink.txtが作成されます。



link.txtを開いて内容を確認します。Link のhttp://からが今回作成したリンクとな ります。

メールでリンクを配布する場合は6へ、 Webでリンクを公開する場合は7に進ん でください。

作成したリンクの例

http://ems/E7enlenAy5NrVAWdjPkgR8IAHYRsgKF0ZaV/pbqrOHwheWpi5I2KcluDmXf79x2 DQGNrnnRmj5DwP7yjDDAd1IcAwsQGBjadivAwHZaJOfcRE1jen+Ffq5Su



メールでリンクを配布する場合は、http://からリンクをすべてコピーし、本 文に貼り付けてください。

ESET Endpoint Security for Androidをインストール後、メールで配布さ れたリンクをタップします。

リンクをタップした後、[アプリケーションを選択] 画面が表示されますので、 「ESET Endpoint Security」を選択するとAndroid端末が自動的にERAに接 続し、設定が反映されます。

※タップしてから設定の反映までしばらくかかる場合があります。

7 作成したリンクをWebで公開する場合、以下のHTMLタグを公開するHTMLファイルに挿入してください。

<a href="ems:< 作成したリンクの http://ems/ 以降の部分 >"> 任意の文字

記述例

 設定はこちら

上記の記述例の場合、ESET Endpoint Security for Androidをインストール後、Android端末のブラウザーで作成した Webページを開いて、[設定はこちら]をタップするとAndroid端末が自動的にERAへ接続し、設定が反映されます。 ※タップしてから設定の反映までしばらくかかる場合があります。 1.6

Link Generatorを利用してインストールする場合は、以下の流れとなります。



POINT

Link Generatorを利用して設定できない項目は、[ESETをデバイス管理者として設定]、[管理者連絡先の定義]です。

1.6.6 複数の拠点がある場合のインストール

本社と支社など複数の拠点がある場合は、それぞれの環境に応じたクライアント用プログラムのインストール方法を検討します。クライアント用プログラムを展開する際、Windows用の設定組み込み済みインストーラーやMac OS X用の設定組み込み済みインストーラーを利用するとともに、ESET Remote Administrator (ERA)のポリシー機能やグループ機能を利用するとインストーラーやコンフィグレーションの管理などが容易になります。

1.6.6.1 クライアント展開のポイント

ESET Remote Administrator (ERA) には、クライアントPCを効率的に管理し、スムーズな運用を行うために「グルー プ機能」や「ポリシー機能」が搭載されています。クライアント用プログラムをインストールしたコンピューターが、ERA (管理サーバー)の管理対象となっていれば、これらの機能を利用して設定の管理を容易に行えます。

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機能です。グループは、手動で作成する「静的 グループ」のほか、特定の条件を指定して自動的にグループ分けを行う「パラメータグループ」を作成できます。たとえば、 複数の拠点がある場合は、パラメータグループを利用することで、グループ分けを自動化できます。グループ機能の詳 細については70ページをご参照ください。

ポリシー機能

クライアントPCに特定の設定 (コンフィグレーション)を強制的に適用できる機能です。この機能を利用すると、グループ機能で作成した特定のグループに対して同じ設定を強制的に適用できます。たとえば、パラメータグループを利用するとグループ分けが自動化され、グループごとのポリシー適用を自動化できます。ポリシー機能の詳細については77ページをご参照ください。

1.6

FAQ

|1.6.6.2 ポリシー機能とグループ機能を利用した展開の流れ

ポリシー機能とグループ機能を利用して、本社と支社間などの複数の拠点にクライアント用プログラムを展開する場合は、以下の流れで行います。ここでは、各拠点ごとに準備されたミラーサーバーに接続する設定をグループ機能とポリシー 機能で一元管理する場合を例に流れを説明しています。





FAQ

※インストーラーを作成する際に、「リモート管理」の設定を間違えると、ポリシーの配布ができません。また、ERAに アクセスができませんので、タスクでの設定修正はできません。

※クライアントは複数のグループに所属できます。どのポリシーが適用されるかは、ポリシールールで設定された順番 により決定されます。

1.6.7 クライアント用プログラムと サーバー用プログラムの設定のポイントと注意点

クライアント用プログラムは、クライアントPCだけでなく管理サーバーにも導入できますが、両者ではポイントとなる 設定項目が異なります。ここでは、それぞれの利用環境に合わせた運用を行うための設定のポイントを説明します。ク ライアント用プログラムの設定を検討するときに重要なのが、導入するコンピューターの役割です。クライアントPCで はコンピューターの安全の維持が最優先ですが、サーバーに導入する場合は、安全性だけでなく、サーバー負荷をでき るだけ減らすような工夫も重要です。それぞれの場合で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。

クライアントPCの設定のポイントと注意点
 リモート管理 アップデート 定期検査 設定変更のパスワードロック(パラメータ設定の保護) **Windows用 プログラムのみ 権限ユーザー **Mac OS X用プログラムのみ アップデートの冗長化 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) 検査対象からの除外 ThreatSense.Net早期警告システム

サーバーの設定のポイントと注意点

●一部検査機能の無効化
 ●データベースなどのアプリケーションの検査除外
 ●コンポーネントアップデート時のOS再起動の無効化

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、クラ イアント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

クライアント用プログラムは、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。

設定変更のパスワードロック(パラメーター設定の保護)

Windows用プログラムの設定は、既定値ではユーザーの判断(操作)で変更が可能になっています。この設定は、ユーザー による自由な設定変更ができないようにパスワード保護をかけ、変更が必要な場合は管理者が行うようにするものです。 なお、パスワード保護をかけることにより、クライアント用プログラムのアンインストールにもパスワード入力が必要 となります。

権限ユーザー

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クライアント用プログラムの詳細な設定を行えるようになります。

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。クライアン ト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、プライマリとセカンダリの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、プライマリのアップデートサーバーが利用で きないときに自動的にセカンダリ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 マリにミラーサーバーを、セカンダリに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。 なおWindows用プログラムの場合、手動でのアップデート時は、現在設定されたサーバー(プロファイル)のみを利用 しますので、手動で切り替える必要があります。

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、既定値ではクライアント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

独自開発され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 と確信できるプログラムがウイルスとして検出された場合、まずは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。次に、隔離された該当ファイルを復元してください。

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。

ESET Live Grid (ThreatSense.Net早期警告システム)

本製品は、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。

1.6 STEP4 移行プランの検討 3

FAQ

4

コラム

「設定のポイントと注意点」

常に安定した動作を求められるサーバーにクライアント用プログラムを導入する場合は、サーバーの負荷が増加しない ようにするなどの工夫を行うことを推奨しています。サーバーに導入する場合は、以下のような点を参考にチューニン グを行ってください。

一部検査機能の無効化

サーバーでは不要な検査を行わないように設定することで、サーバーの負荷を軽減できます。たとえば、ドキュメントの閲覧や電子メールの閲覧、Webの閲覧などを行わないサーバーでは、これらの検査を行わないように設定することが 推奨されます。

■無効化する検査の例

- ●Microsoft Officeドキュメントの検査
- ●電子メールのウイルス検査
- ●Web閲覧時のウイルス検査

データベースなどのアプリケーションの検査除外

データベースのウイルス検査を行うと、コンピューターのCPU使用率が高くなる可能性があります。そのような場合は、 データベースなどをウイルス検査対象から除外してください。

コンポーネントアップデート時のOS再起動の無効化

本製品では、プログラムコンポーネントアップデートと呼ばれる、コンピューターの再起動をともなうバージョンアッ プが行われる場合があります。常時稼働が前提となっているサーバーでは、プログラムのバージョンアップなどによる 再起動ができない場合があります。このような環境では、プログラムコンポーネントアップデートが行われた際、OS を自動的に再起動しないよう設定してください。

STEP5 1.7 移行作業

作成した移行プランに沿って移行作業を行います。以下に、移行例をご紹介します。

クライアント用プログラム	ESET Endpoint Security
クライアント数	2,000
管理サーバー数	1
ミラーサーバー数	1
ミラーの種類	IIS
既存プログラムの削除方法	バッチファイルを利用
参照モデルケース	モデルケース 6



4

FAQ

本節では、ESET ライセンス製品の旧バージョンからバージョンアップを行う場合の方法や注意点について説明します。

バージョンアップによる 導入

1.8.1 バージョンアップ時のポイント

ESET ライセンス製品のバージョンアップは、基本的に上書きインストールが行えますが、旧バージョンのESET NOD32アンチウイルスからESET File Security for Microsoft Windows Serverへアップデートする場合に限って、ESET NOD32アンチウイルスのアンインストールが必要です。

	現行環境	 バージョンアップ環境	上書き インストール
	ESET Remote Administrator V4.0	ESET Remote Administrator V5.0	0
Windows用プログラム	ESET Smart Security V4.x	ESET Endpoint Security	0
	ESET NOD32アンチウイルス V4.x	ESET Endpoint アンチウイルス	0
		ESET File Security for Windows Server	×
Mac OS X用プログラム	ESET NOD32アンチウイルス V4.0	ESET NOD32アンチウイルス V4.1	0

●上書きインストールが可能な環境

現行環境

1.8

管理サーバー	ESET Remote Administrator V4.0
ミラーサーバー	ESET Remote Administrator V4.0
クライアント用プログラム	ESET Smart Security V4.2またはESET NOD32アンチウイルス V4.2
-	



管理サーバー	ESET Remote Administrator V5.0
ミラーサーバー	ESET Remote Administrator V5.0
クライアント用プログラム	ESET Endpoint SecurityまたはESET Endpoint アンチウイルス

1.8.2 ESETセキュリティ ソフトウェア シリーズ ライセン ス製品 V4.2からのバージョンアップ

ESETセキュリティ ソフトウェア シリーズ ライセンス製品 V4.2からV.5.0へのバージョンアップの際、既存のESET セキュリティ製品をアンインストールする必要はありません。上書きインストールでバージョンアップすることができ ます。

1.8.2.1 クライアントPCのみで運用している場合のバージョンアップ手順

クライアントPCのみで運用している場合は、最初に1台だけバージョアップを行い、そのコンピューターの動作確認と 設定を行います。次に、バージョンアップ済みのコンピューターの設定ファイルを保存し、それを適用して残りのクラ イアントPCのバージョアップを行います。



2

3

4

FAQ



1.8.2.3 ミラーサーバーとクライアントPCで運用している場合のバージョンアップ手順

ミラーサーバーとクライアントPCで運用している場合は、最初にミラーサーバーのバージョンアップを行い、接続確認 を行った後、クライアントPCのバージョンアップを行います。この場合のクライアントPCのバージョンアップは、「ク ライアントPCのみで運用している場合のバージョンアップ手順」と同じです。



1.8.2.4 管理サーバーとミラーサーバーによる運用をしている場合のバージョンアップ手順1 ~管理サーバーとミラーサーバーが同じコンピューターの場合

管理サーバーとミラーサーバーを同一のコンピューターで構築している場合も、最初に管理サーバーのデータベースの バックアップを行います。次に管理サーバー(ERA)の上書きインストールを行い、続いてERACを上書きインストール すれば、管理サーバー、ミラーサーバー共にバージョンアップ完了です。

クライアント用プログラムのバージョンアップは、インストール用の設定組み込み済みインストーラーを作成し、この インストーラーを利用して上書きインストールで行います。



1.8

バージョンアップによる導入

2

3

1.8.2.5 管理サーバーとミラーサーバーによる運用をしている場合のバージョンアップ手順2 ~管理サーバーとミラーサーバーが異なるコンピューターの場合

管理サーバーとミラーサーバーが異なるコンピューターで構築されている場合は、最初に59ページと同じ手順で管理 サーバー側のバージョンアップを行います。

次にミラーサーバーを上書きインストールでバージョンアップし、続いて設定組み込み済みインストーラーを作成して、 上書きインストールでクライアントPCのバージョンアップを行います。



2

3

4

FAQ

FAQ



[Chapter 2] クライアント PC の 効率的な管理方法

2.1	効率的な管理を行うための機能	68
2.2	ダッシュボード機能	69
2.3	グループ機能・・・・・	70
2.4	タスク機能・・・・・	73
2.5	ポリシー機能・・・・・	77
2.6	通知機能	79
2.7	ロールバック機能・・・・・	81
2.8	ミラー機能・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	82
2.9	Android 端末の管理	90



効率的な管理を行うための機能

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の機能が備えられています。

2.1.1 主な管理機能

ESET Remote Administrator (ERA) には、「ダッシュボード機能」「グループ機能」「タスク機能」「ポリシー機能」「通知機能」などのクライアントPC管理機能を搭載しています。また、ウイルス定義データベースを効率的に配布管理する「ロールバック機能」「ミラー機能」なども搭載しています。

●主な管理機能

機能	概要	参照ページ
ダッシュボード機能	各クライアントPCから収集した各種情報やESET Remote Administrator Server(ERAS)のCPU負 荷やデータベースの負荷などのパフォーマンス情報をWebブラウザー経由で閲覧できます。ダッシュ ボードに表示する情報は、ESET Remote Administrator Console(ERAC)からカスタマイズできま す。また、ダッシュボードは暗号化された接続(HTTPS)にも対応しています。	69ページ
グループ機能	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。グループは、「グループマネージャ」を使うことで作成できます。グループマネージャで作成したグループは、タスクの一括配布やポリシーの一括適用などに利用できます。	70ページ
タスク機能	ERASを利用したリモート操作でクライアントPCに指示(タスク)を出す機能です。クライアントPCの 各種設定を変更したり、ウイルス検査の実行指示など様々な指示を出すことができます。タスクは、グ ループ単位またはクライアントPC単位で実行できます。	73ページ
ポリシー機能	クライアントPCの特定の設定(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。タスク機能に用意されたクライアントPCの各種設定を行う[コンフィグレーション]タスクと同等の 機能も提供します。ポリシー機能は、グループ単位またはクライアントPC単位で実行できます。	77ページ
通知機能	セキュリティ上の問題が発生したときなどに、管理者にメッセージを通知する機能です。	79ページ

●ウイルス定義データベース関連機能

機能	概要	参照ページ
ロールバック機能	クライアントPCに適用したウイルス定義データベースやモジュールを適用前のバージョンに戻す機能で す。また、ウイルス定義データベースのアップデートを一定時間無効にすることもできます。	81ページ
ミラー機能	ESET社がインターネット上に設置しているウイルス定義データベースのアップデートサーバーを複製し、これと同等の機能を備えたサーバーを社内に設置できる機能です。この機能を利用すると、社内LANなどのローカルネットワーク内に、ウイルス定義データベースを配布するサーバーを設置できます。	82ページ



ダッシュボード機能

ESET Remote Administrator (ERA) には、Webブラウザー経由で各クライアントPCから収集した情報やESET Remote Administrator Server (ERAS) のパフォーマンス情報を閲覧する「ダッシュボード」機能が備わっています。 ここでは、ダッシュボード機能について説明します。

2.2.1 ダッシュボード機能とは

ダッシュボード機能を利用すると、各クライアントPCから収集したウイルスや迷惑メールに関する情報、ブロックさ れたWebサイトなどのさまざまな情報やESET Remote Administrator Server (ERAS)のパフォーマンス情報などを Webブラウザー経由で閲覧できます。この機能を利用することで、簡単に各クライアントの状況やERASをインストー ルしたコンピューターの負荷などを知ることができます。また、ダッシュボードに表示する情報は、ESET Remote Administrator Console (ERAC) から自由にカスタマイズできます。ダッシュボードは、暗号化された接続 (HTTPS) にも対応しています。ダッシュボード機能の詳細な使い方は、「ESET Remote Administrator ユーザーズマニュアル」 をご参照ください。



1

2.2

ダッシュボード機能

3

2.3

グループ機能

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。 ここでは、グループ機能について説明します。

2.3.1 グループ機能とは

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機能です。グループは、グループマネージャに よって作成でき、「静的グループ」と「パラメータグループ」に大別されます。また、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。静的グループは、手動でクライアントPCをグループ分けするときに利用する小規模 の管理に向いています。パラメータグループは、特定の条件を指定しその条件にあったクライアントPCのみでグループ を構成できます。パラメータグループは、条件を指定するだけでグループ分けを自動化できるので、大規模な管理に向 いています。

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。



2.3.2 静的グループとパラメータグループ

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、それぞれ以下のような特徴があります。

POINT

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。この機能の使い方については、 「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

2.3.2.1 静的グループ

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。静的グループの作成手順については、 「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



1

2.3.2.2 パラメータグループ

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。パラメータグループの作成手順については、「ESET Remote Administrator ユーザーズマニュアル」をご参 照ください。



条件の例

- ●グループ
- ●ドメイン
- ●コンピューター名
- ●IPアドレス
- ●クライアント用プログラムの製品名やバージョン
- ●ウイルス定義データベースのアップデート状況
- •0S
タスク機能 2.4

タスク機能は、ESET Remote Administrator Sever (ERAS) からクライアントPCの設定などをリモート操作で変更 する機能です。ここではタスクの配布について説明します。

2.4.1 タスクとは

タスクとは、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。



1

3

4

2.4

タスク機能

2.4.2 タスクの種類

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。また、 一部のタスク(オンデマンド検査タスクやウイルス定義データベースのアップデートタスク)は、各クライアントPCの タスク実行時間をランダムに遅らせることができます。

●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さまざ まな設定が行えます。
オンデマンドスキャン	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。また、このタスクは、各クライア ントPCのタスク実行時間をランダムに遅らせることができます。
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。また、このタスクは、各クライアントPCのタスク実行時間をランダムに遅らせることがで きます。
今すぐアップデート	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。また、こ のタスクは、各クライアントPCのタスク実行時間をランダムに遅らせることができます。これにより、 ウイルス定義データベースのアップデートを分散でき、ミラーサーバーやネットワークに負荷を軽減し ます。
SysInspectorスクリプト	このタスクでは、対象のクライアントPC上でSysInspectorスクリプトを実行します。このスクリプト は、望ましくない可能性があるオブジェクトをシステムから削除したい場合などに利用します。※1
保護機能	クライアントPCの各保護機能(ドキュメント保護、リアルタイム保護、Webアクセス保護など)の有効/ 無効を切り替えたいときに利用します。設定を無効にする場合は、一定時間経過すると設定値を元に戻 す(有効にする)期間が選択できます。※2
スケジュール済みタスクの実行	クライアントPCに登録されているスケジュールタスクを実行したいときに利用します。※2
隔離からの復元/削除	クライアントPCで発見され、隔離中のファイルを復元または削除するときに利用します。誤ってウイル スと判断され隔離されたファイルなどをリモート操作で復元するときなどに利用します。※1
ウイルス定義データベースの ロールバック	クライアントPCに適用したウイルス定義データベースやモジュールに不具合が見つかった場合、適用前のバージョンにロールバックしたいときに利用します。また、クライアントPCのウイルス定義データベースのアップデートを一定期間無効にすることもできます。※2
クライアントの アップデートキャッシュのクリア	クライアントPCのアップデートキャッシュを削除したいときに利用します。ウイルス定義データベース のアップデートが成功していない可能性がある場合、クライアントPCのアップデートキャッシュをクリ アし、最新のアップデートをダウンロードします。※2
セキュリティ監査ログの作成	Android端末のバッテリレベル、Bluetoothステータス、ディスクの空き領域、デバイスの可視性、ホームネットワーク、および実行中のプロセスなどをチェックしたログを作成したいときに利用します。※3
通知の表示	Android端末に通知(警告メッセージなど)を送信したいときに利用します。※3

※1 ESET Smart Security V4以降またはESET NOD32アンチウイルス V4以降でのみ利用できます。

※2 ESET Endpoint SecurityまたはESET Endpoint アンチウイルスでのみ利用できます。

※3 ESET Endpoint Security for Androidでのみ利用できます。

2.4.3 タスクの設定手順

クライアントPCに対して各種タスクを設定するときは、以下の手順に沿って作業します。選択したタスクの種類によっ てタスクの設定方法は異なりますが、基本的な手順は以下の通りです。

STEP1 タスクの選択

新規タスクの種類から[コンフィグレーション]を選択します。
●コンフィグレーション
●オンデマンドスキャン(駆除無効)
●オンデマンドスキャン(駆除有効)
●定義データベースのアップデート
●SysInspectorスクリプト
●隔離からの復元/削除

<u>STEP2</u>タスクの設定

ESET コンフィグレーションエディターを利用してタスクの詳細設定を行います。他のタスクは、画面内のオプションを設定することで詳細設定を行います。

STEP3 タスクを配布するクライアントPCの選択

タスクを配布するクライアントPCは、クライアントPC単位で指定できるだけでなく、グループ単位 でも指定可能です。クライアントPCのグループ分けは、グループマネージャを利用して行えます。

STEP4 タスクの配布(実行)

3

1

2.4

タスク機能

2.4.4 [コンフィグレーション]タスクの設定方法

[コンフィグレーション] タスクの設定は、基本的にESET コンフィグレーションエディターを利用して行いますが、その方法には大きく分けて以下の3種類の方法があります。

2.4.4.1 新規作成

新規設定を作成する方法です。①[作成]ボタンをクリックするとESET コンフィグレーションエディターが起動するので、これでクライアントPC用の設定を作成します。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

|2.4.4.2 作成済みの設定ファイル(.xml)を利用

事前にESET コンフィグレーションエディターなどを利用して作成しておいたクライアントPC用の設定ファイル (.xml)を利用する方法です。 2 [選択] ボタンをクリックすると、[ファイルを開く] ダイアログが開くので、事前に 準備しておいた設定ファイル(.xml)を読み込みます。ファイルを選択した後に、[表示] ボタンをクリックすると設 定を確認でき、[編集] ボタンをクリックするとその設定ファイル(.xml)を編集できます。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

2.4.4.3 テンプレートから作成

作成済み設定ファイル (.xml) を利用した方法によく似た方法で、事前に準備しておいたテンプレート用の設定ファイル (.xml) を利用して設定を行います。③[テンプレートから作成] ボタンをクリックすると[ファイルを開く] ダイアログ が開くので、事前に準備しておいたテンプレート設定ファイル (.xml) を読み込みます。ファイルを選択した後に、[表示] ボタンをクリックすると設定を確認でき、[編集] ボタンをクリックするとテンプレート設定ファイル (.xml) を編集できます。詳細は [ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

POINT

[ウィザード] ボタンをクリックすると、「パーソナルファイアウォールマージウィザード] 画面が起動します。この設定により、稼働中のクライアントPCで 利用されているファイアウォールルールを読み出して、それを利用して新しいファイアウォールルールを作成できます。

スクライアントの設定	_ 🗆 ×
- コンフィグレーションの作成/選択 1 2 3 作成(R) 選択(S) テンプレートから作成(T) ウィザー	<(W)
まずコンフィグレーションファイルを作成または選択し、次にそのコンフィグレーションファイルを表示(∀) 編	集(E) (示または編
集します。 スケジュールされているタスクの詳細	
沃へ(N)	キャンセル

2.5

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。ここでは、ポリシーについて説明します。

2.5.1 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。

2.5.2 ポリシーの親子関係

ポリシーでは、「継承」という概念が導入されています。子ポリシーは親ポリシーの設定を継承でき、設定をマージ(統合) できます。通常、親ポリシーと子ポリシーの設定が異なっている場合、子ポリシーの設定が優先されますが、逆に親ポ リシーが子ポリシーの設定を上書きし、強制的に親ポリシーの設定を子ポリシーに適用することもできます。

●通常の親子のポリシー



▲通常は、親ポリシーと子ポリシーの設定が異なっている場合、子ポリシーの設定が優先されます。

●親ポリシーを強制的に適用



▲親ポリシーと子ポリシーの設定が異なっている場合に、親ポリシーを強制的に適用することも可能です。

1

2.5

ポリシー機能

3

4

2.5.3 ポリシーを利用した設定適用の流れ

クライアントPCのポリシーを変更することで各種設定を行うときは、以下の流れで作業します。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



通知機能 2.6

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。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。

2.6.1 通知ルール作成の流れ

[通知マネージャ]を利用して電子メールで通知を行うには、あらかじめERASに電子メールの送信設定を行っておく必要があります。また[通知マネージャ]には、[事前定義のルール]が準備されていますが、既定ではすべてのルールが無効に設定されています。通知ルールは、事前定義のルールが利用できるほか、新規ルールの作成や事前定義のルールをカスタマイズして利用することもできます。通知ルールの作成は、以下の手順に沿って作業します。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



1

3

2.6

通知機能



作成したルール(条件)を満たしたときの動作の設定を行います。[電子メール][SNMPトラップ][実行(サーバ上)][ファイルにログを保存する(サーバ上)][Syslogにログを保存する][ログ]から選択できます。

STEP6 [メッセージ] を設定する

通知に利用するメッセージを設定します。メッセージには変数が利用できます。

ロールバック機能



クライアントPCに適用したウイルス定義データベースを適用前のバージョンに戻す機能を「ロールバック」機能と呼びます。ここでは、ロールバック機能について説明します。

2.7.1 ロールバック機能とは

ESET Endpoint SecurityおよびESET Endpoint アンチウイルスには、適用したウイルス定義データベースを適用前のバージョンに戻すロールバック機能が備わっています。この機能によって、ウイルス定義データベースの特定バージョンでウイルスに感染していないプログラムを誤検出した場合、適用前のバージョンに戻すことでその不具合を回避できます。

また、ERASからクライアントPCへのウイルス定義データベースのアップデートを一定期間(12時間、24時間、48時間) 無効にすることもできます。一部のWindows システムファイルやアプリケーションで利用されるファイルをウイルス の疑いがあるファイルとして判定したときなどに、ロールバックを行い、ウイルス定義データベースのアップデートを 一定期間無効とすることで暫定的な対応とするという運用も行えます。



※ロールバック機能は、ESET Endpoint SecurityおよびESET Endpoint アンチウイルス以降でのみ利用できます。 ESET File Security for Microsoft Windows ServerまたはESET NOD32アンチウイルス、ESET File Security for Linux、ESET Endpoint Security for Androidではこの機能をサポートしていません。 1

2.7

ロールバック機能

3

4

ミラー機能 2.8

ESET社はインターネット上でウイルス定義データベースのアップデートサーバーを提供しています。ミラー機能とは、 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アップデートを行える機能です。本節では、ミラー機能について説明します。

2.8.1 アップデートファイルの配布とミラー機能

ウイルスなど悪意のある不正なプログラムは、日々新種や亜種が登場しています。これらの脅威からコンピューターを 守るには、常に最新のウイルス定義データベースが必要です。アップデートサーバーはそのために設置されています。 また、アップデートサーバーは最新のウイルス定義データベースを配布するだけでなく、必要に応じてプログラムコン ポーネントのアップデートの配布も行っています。

ミラー機能は、社内LANなどのローカルネットワーク内に、ウイルス定義データベースを配布するサーバーを設置する ことで実現します。各クライアントPCがローカルネットワーク内のミラーサーバーからアップデートすることにより、 インターネット接続にかかわる回線の負荷が軽減されます。また、インターネットへの接続が制限されている環境や、ネッ トワークへの接続環境がないクライアントにも最新のウイルス定義データベースを提供しやすくなります(次ページ参 照)。

ミラーサーバーは、ESET Remote Administrator Server (ERAS) またはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linux のいずれかを利用して構築します。 ミラーサーバーは、規模に応じて複数台設置できます。たとえば、各拠点ごとに複数台のミラーサーバーを設置できます。 なお、ミラーサーバーの構築にはラインセンスキーファイルの登録が必要です。

CAUTION

ESET Endpoint SecurityおよびMac OS X用プログラムのESET NOD32アンチウイルスは、ミラーサーバーの構築をサポートしていません。

FAQ

1

3

4

FAQ

2.8

ミラー機能

2.8.2 アップデートファイルの配布方法

ミラーサーバーを構築してウイルス定義データベースやプログラムコンポーネントを配布する際には、以下の方法があ ります。利用環境に応じて、配布方法をご検討ください。なお、Mac OS X用プログラムのESET NOD32アンチウイ ルスは、HTTP経由によるアップデートのみをサポートします。他のアップデート方法はサポートしていないのでご注意 ください。

アップ	デート方法	概要	クライアントPC接続 台数の目安 [※]
	ERAS	ERASとESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linux	400台
	ESET Endpoint アンチウイルス ESET File Security for Microsoft Windows Server	にはミラーサーバー機能が搭載されており、内蔵のHTTPサーバー 機能を利用してウイルス定義データベースなどのアップデートファ イルを配布できます。この機能を利用すれば、別途Webサーバー を用意することなく、アップデートファイルを各クライアントPC に配布できます。アップデートファイルを提供する方法としては、 これが最も簡単です。なお、この方法でアップデートファイルを配	100台
HTTP経由による アップデート	ESET File Security for Linux	布する場合のクライアント数としては、ESET Endpoint アンチウ イルス、ESET File Security for Microsoft Windows Serverを 利用した場合は100台以下、ESET File Security for Linuxを利 用した場合は1,000台以下、ERASを利用した場合は400台以下 を推奨しています。	1,000台
	Microsoft Internet Information Services (IIS)	ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxがミラーサーバー用に取得した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、IISまたはApacheのWebサー バーで配布する方法です。この方法は、Webサーバーに搭載され	3.000 /1
	Apache	た帯域制御機能や同時接続制御機能などを利用することでネット ワーク負荷を制御できるというメリットがあります。大量のクライ アントPCが同時にアップデートを行う可能性がある場合に効果的 な方法です。なお、この方法でアップデートファイルを配布する場 合のクライアント数としては、3,000台以下を推奨しています。	
	ERAS	ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Serverがミラーサーバー用に	_
 共有フォルダーを 利用」たマップデート	ESET Endpoint アンチウイルス	取得した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 共有フォルダーに保存し、各クライアントPCがファイル共有機能	
	ESET File Security for Microsoft Windows Server	を利用してアップデートを行う方法です。	_
他のPCの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 アップデート	利用した	ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxがミラーサーバー用に取得した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USBメモリーやCD-Rなどに保存 し、各クライアントPCのアップデートを行う方法です。クライア ントPCが既存のネットワークと切り離されている場合や、スタン ドアロンで利用されている場合にこの方法を利用します。なお、 アップデートファイルは、ユーザーズサイトでも提供しています。	_

※ ミラーサーバー 1 台あたりのクライアント PC 接続台数です。

83

2.8.3 ミラーサーバーの構成例

ここではミラーサーバーの構成例として、ミラーサーバーを1台設置する場合と、2台以上設置する場合を紹介します。 実際には、ご利用の規模に応じて設置するミラーサーバーの台数をご検討ください。なお、ミラーサーバーの設置には インターネット接続環境が必要になります。

|2.8.3.1 ミラーサーバーの構成例1~ミラーサーバーが1台の場合

ミラーサーバーに設定したコンピューターがESET社のアップデート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します。各クライアントPCは、ミラーサーバー上の配布ファイルを取得します。



Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ

2.8.3.2 ミラーサーバーの構成例2~ミラーサーバーが2台以上の場合

ミラーサーバーに設定したコンピューターがESET社のアップデート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します。各クライアントPCは利用環境に応じて、アップデート先のミラーサーバーを設定 します。



1

3

4

2.8

ミラー機能

2.8.4 ミラーサーバー構築時の注意点

ミラーサーバーを構築する場合、ネットワーク構成によっては問題が発生する場合があります。ここでは、ミラーサーバー 構築時の注意点を説明します。

2.8.4.1 ライセンスキーファイル

ミラーサーバーの構築には、ラインセンスキーの登録が必要です。ライセンスキーファイルは弊社ユーザーズサイトからダウンロードできます。詳しくは、「ESET ライセンス製品 ご利用の手引」をご参照ください。

2.8.4.2 プロキシサーバーが設置されている場合

インターネット接続にプロキシサーバーを利用している場合、ミラーサーバーを構築するERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxにプロキ シ設定を行ってください。プロキシ設定の方法ついては、ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxのユーザーズマニュアルをご参照ください。 なお、ウイルス定義データベースのファイル (*.nup)は、プロキシサーバーなどで強制キャッシュを行わないように設定 してください。プロキシサーバーなどのキャッシュの仕様によっては、ウイルス定義データベースのデジタル署名に不 整合を起こす可能性があります。

2.8.4.3 プログラムコンポーネントのダウンロード設定について

ERASのミラーサーバーの既定値では、プログラムコンポーネント(ESET セキュリティ製品のバージョンアッププロ グラム)のアップデート用ファイルのダウンロードを行いません。ESET Endpoint アンチウイルスおよびESET File Security for Microsoft Windows Server、ESET File Security for Linuxのミラーサーバーは、ダウンロードする前 に確認ダイアログが表示されます。また、プログラムコンポーネントをダウンロードし、配布したい場合は、必要なコ ンポーネントを設定します。

ただし、製品の新しいバージョンが公開されても、必ずしもコンポーネントアップデートが行われるわけではありません。 その場合は、アップデート用のプログラムコンポーネントは表示されません。

|2.8.4.4 共有フォルダーを利用する場合

ファイル共有機能を利用してアップデートを行う場合は、共有フォルダーへのアクセス権限を適切に設定してください。 アクセス権限の設定が間違っていると、共有フォルダーにアクセスできずアップデートを行えないことがあります。なお、 Mac OS X用プログラムのESET NOD32アンチウイルスおよびESET File Security for Linuxは、共有フォルダーか らのアップデートをサポートしていません。

|2.8.4.5 リムーバブルメディアを利用する場合

Mac OS X用プログラムのESET NOD32アンチウイルスおよびESET File Security for Linuxは、リムーバブルメディ アからのアップデートをサポートしていません。

2.8.5 オフライン環境での更新

セキュリティ上の問題などでインターネットやミラーサーバに接続できないオフライン環境のコンピューターは、USB メモリーやCD-Rなどのリムーバブルメディアを利用してアップデートを行います。アップデート用のファイルは弊社 ユーザーズサイトから入手する方法と、ミラーサーバーに保存されたファイルを使用する方法があります。弊社ユーザー ズサイトから、アップデート用のファイルを取得しUSBメモリーやCD-Rなどのリムーバブルメディアを利用したアッ プデートは、以下のような流れで行います。



※詳細な手順については、弊社ユーザーズサイトに掲載されている「オフライン更新手順書(http://canon-its.jp/ product/eset/users)」を参照ください。また、ミラーサーバーに保存された配布用ファイルを使用する場合はこち らのURL (http://canon-its.jp/supp/eset/est00000031.html)を参照ください。 4

3

1

2.8

ミラー機能

2.8.6 ウイルス定義データベースの時差配信

ウイルス定義データベースの時差配信を行うことで、ウイルス定義データベースの障害や誤検知などのリスクを軽減で きます。ウイルス定義データベースの時差配信は、ESET Remote Administrator (ERA) およびESET Endpoint アン チウイルスに搭載された「遅延アップデート」を利用する方法と多段構成でミラーサーバーを構築する方法があります。

2.8.6.1 遅延アップデートを利用した時差配信

ERAおよびESET Endpoint アンチウイルスには、「遅延アップデート」機能が搭載されています。遅延アップデート機能とは、一般向けに公開されているウイルス定義データベースより一定時間(12時間)遅らせたウイルス定義データベースをESET社のアップデートサーバーから取得する機能です。この機能を利用してミラーサーバーを構築すると、常に一定時間(12時間)遅らせたウイルス定義ファイルを公開できます。この機能により、誤検知などのリスクを軽減できます。遅延アップデートの詳細については、ERAまたはESET Endpoint アンチウイルスのユーザーズマニュアルをご参照ください。



※遅延アップデート機能は、ESET Remote Administrator V5.0およびESET Endpoint アンチウイルスでのみサポートされます。ESET File Security for Microsoft Windows Server、ESET File Security for Linuxはこの機能を搭載していません。

※遅延アップデートを行うと、常に一定時間(12時間)前の古いウイルス定義データベースを利用するためウイルス感 染などのリスクが増加しますのでご注意ください。

Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ

2.8.6.2 ミラーサーバーの多段構成による時差配信

ミラーサーバーを多段構成で設置し、ウイルス定義データーベースの取得時間をずらすことで、ウイルス定義データー ベース配信を任意の時間ずらす構成を組むことができます。ミラーサーバーを多段構成で利用する場合は、以下のよう な構成でミラーサーバーを構築します。



※ウイルス定義データベースの時差配信を行うと、古いウイルス定義データベースを利用するためウイルス感染などの リスクが増加しますのでご注意ください。 1

2.8



ESET Endpoint Security for AndroidがインストールされたAndroid端末をESET Remote Administrator(ERA)で 識別し管理する方法を説明します。

2.9.1 Android 端末の識別

Android端末をERAに接続した場合に登録されるクライアント名(コンピュータ名)は、SIMカードを挿入できるAndroid端末の場合は、IMEI(International Mobile Equipment Identity)またはMEID(Mobile Equipment Identifier)となり、SIMカードを挿入できないAndroid端末の場合はWi-Fi MACアドレスとなります。

また、ERAに登録されるMACアドレスはAndroid端末のWi-Fi MACアドレスとなります。

これらはアルファベットと数字で構成されており、複数台のAndroid端末を管理する場合、クライアント名(コンピュー タ名)がどのAndroid端末に対応しているかを識別しにくいため、クライアント名を任意の識別しやすい名前に変更する ことをおすすめします。

] 事前にAndroid端末のIMEI、MEIDまたはWi-Fi MACアドレスを確認します。

SIMカードを挿入できるAndroid端末:IMEIまたはMEID (ご利用の携帯電話事業者によって変わります) SIMカードを挿入できないAndroid端末:Wi-Fi MACアドレス

POINT

1

IMEI、MEIDおよびWi-Fi MACアドレスは、Android端末で、[設定]>[端末情報]>[端末の状態]>[IMEI]、[MEID]または[Wi-Fi MACアドレス]で確認できます。端末によっては操作が異なる場合がございます。

サーバ名	Dみ対象にす。 ON(C) 」クライアント マ	0FF(U)	<u>クライアント</u> 2ライアント 言義データ	1019-00-007 を追加するには? ペースの状。 て』 最も	も古いアクセス、	4 最終ウイル	ス警告	最終ファイアウォール	レニー 🗤 最終イベント警
Win2008r2fix	8		後台が古い	パージョン 1か	月前	1		0	0
表示するアイテム s	00 • <<	5 2 7171	_情報:	007/217/21m	表示モード(M);	カスタム表示モード	•		
(1) (1) 小名 (1)	175/2014 5-1	KN() V.	刻品	主のアイナムアイナム中	「製品バージョン」	(リカエストされたポ	「赤いー名	最終77htr2	1 (\$10111102/01488
Win2008r2fix	Win2008r2fix	example.com	ESE	NOD32 Antivirus _	4.2.73	既定のプライマリ	既定のプライマリ.	. 48 秒前	1408000000-73
📑 au_iida	Win2008r2fix		ESE	Endpoint Security_	1.2.111	EESA (Win2008		2週間前	
🐷 Aquos	Win2008r2fix		ESE	F Endpoint Security_	1.2.111	EESA (Win2008	EESA (Win2008	. 46 分前	Antitheft module
# A00000305def0-	Win 2008/26iv		ESE.	Endpoint Security_	1.2.111	EESA (Win2008	EESA (Win2008	_ 26 分前	Antitheft module
990000591738	9へ()選択(A) 会部1 7384P(D)		Utri+A	Endpoint Security_	1.2.103	EESA (Win2008	既定のプライマリ	か月前	
V 742f681113d1	3月月日の日本(1)		Child	Endpoint Security_	1.2.111	EESA (Win2008		4日前	
S085a9303b28	選択アイテムを非表示(H)		Gtrl+H	Endpoint Security_	1.2.111	EESA (Win2008	EESA (Win2008	. 33 分前	
🗳 000000000000000	選択アイテムのみ表示(U)		Ctrl+U	Endpoint Security_	1.2.111	EESA (Win2008		1か月前	Antitheft module
	新規々3.2(T)								
	このクライアントのデータ(F)			•					
	(攝車服を再III余(C)		1	•					
	フラグをセット/リセット(S)		1	•					
	データのリクエスト(E)		1	•					
	グループ(ci倉加(G)								
	ポリシーの設定(P)_								
	リモートインストール(D			•					
	ファイアウォールルールマー	ジウィザード(W)							
	カラムの表示/非表示(N)								
	育/郎永(D)		Del						
	(1)								

ERACの [クライアント] タブで、事前に 確認したIMEIなどからAndroid端末を特 定し、該当のクライアントを選択して、右 クリックから [プロパティ] をクリックし ます。

Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ

-

● [一般] タブの [クライアント名] に任意の識別しやすいクライアント名を入力し
 ❷ [OK] をクリックします。

1

[Chapter 3] ERA のログ管理

3.1	障害対策のポイント・・・・・	94
3.2	バックアップの作成・・・・・	95
3.3	バックアップファイルの復元	05
3.4	ログ管理のポイント	13

3.1 障害対策のポイント

ESET Remote Administrator (ERA) のバックアップを取得しておくと、管理サーバーに障害が発生した場合の復旧 に利用できます。ここでは、サーバーの障害対策について説明します。

3.1.1 バックアップを利用したサーバーの復旧

ERAをインストールした管理サーバーに何らかの障害が発生したときに有効なのが、バックアップを用いたサーバーの 復旧です。バックアップがあれば、ERAをインストールした管理用サーバーコンピューターを、他のサーバーコンピュー ターに復元できます。ERA導入直後にバックアップを作成しておきます。設定変更を行ったときや日常運用でも定期的 にバックアップを作成しましょう。

ESET Remote Administrator Server (ERAS) の動作設定やクライアント情報のデータベースのバックアップは、 ERASと共にインストールされる「ESET Remote Administrator Maintenance Tool (ERAメンテナンスツール)」 を利用することでバックアップを作成できるほか、ERASがインストールされたフォルダーを手動でバックアップするこ とで行えます。また、ESET Remote Administrator Console (ERAC)の設定情報のバックアップは、ERACがインス トールされたフォルダーを手動でバックアップすることで行えます。



▲管理サーバーのバックアップと障害復旧作業の標準的なステップ

3.2 バックアップの作成

ここでは、ESET Remote Administrator Server (ERAS)の設定ファイルおよびクライアント情報のデータベースを バックアップする方法を説明します。

3.2.1 ERASの設定ファイルのバックアップ作成手順

ここでは、ERAメンテナンスツールを利用して、ERASの設定ファイルのバックアップを作成する手順を説明します。 ESET Remote Administrator Maintenance Tool(ERAメンテナンスツール)は、ERASをインストールした管理サー バーにインストールされているため、すべての作業を管理サーバーで行います。バックアップ作成の際は、同じコンピュー ターにESET Remote Administrator Console (ERAC) もインストールして、以下の手順を行ってください。

1	 ビス (IS) マネージャー ビス (IS) マネージャー ビネコリティが強化された Windows アノアウォール DNS アンインストール 	デバイスとプリンター 管理ツール ・ ヘルプとサポート ファイル名を指定して実行…
	 すべてのプログラム 	Windows セキュリティ
	プログラムとファイルの検索	<u>ログオフ</u> ・
	AZ&-H 🛛 🥾 😰 🚞	1

●管理サーバーの[スタート] ボタンをクリックし、
 ②[す
 べてのプログラム]をクリックします。



ERAメンテナンスツールを起動します。①[ESET]、② [ESET Remote Administrator Server]、 ③[ESET Remote Administrator Maintenance Tool] と順にク リックします。 1

2

3.2

バックアップの作成





アታ	/ョンの選択 保守9スクの種類選択
- (29	הראק
105	C EDA Comunication (C)
	C FRA Serverを記動(T)
	○ データベースの転送(種類の異なる同川バージョンのデータベースに転送)(A)
	○ データベーフのバッカマップ(外部の)パーションのジーダイ へにまたとへい
	 データベースの復元(外部以)/ブライルから)(R)
	 ○ テーブルを削除(データベースをリヤット)(E)
	○ ストレージのバックアップ(外部ダンプファイル)
	○ ストレージの復元(外部ダンプファイルに)
	○ 新しいライセンスキーをインストール(W)
	1 💿 サーバのコンフィグレーションを変更(ERA Consoleのインストールが必要)(M)
+-	
	「相手能をありたりもには、して決め、ロカバラフをシケケラしより

ERAメンテナンスツールが起動します。 [次へ] ボタ ンをクリックします。

[サーバ情報] ダイアログが表示されます。[次へ] ボタンをクリックします。

[アクションの選択] ダイアログが表示されます。1 [サーバのコンフィグレーションを変更] にチェック を入れ、2 [次へ] ボタンをクリックします。

		Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ	
6	参ERA Maintenance で 保守の準備が整いまし Maintenance Tool	「ool 」た ウィザードは、(保守タスクを開始する準備が	(壁(はした	■ [開始] ボタ] ©■	ンをクリックします。	,	
	現在選択されて(保守タスクを開始 戻るをクリックしま	いるタスか 「サーバのコンフィグレーションを するには、開始台をクリックします。(保守タス すす。ワイザードを続くするには、(キャンセル	変更 少の設定を確認または変更する場合は、 」をクリックします。	ε			
			すべての設定をファイルに保存	F(A)			3. バックアップの
		< 戻	る(B) 開始(S)> キャンセ	z)l(C)			作成



ESET コンフィグレーションエディターが起動しま す。[Remote Administrator]をクリックします。

1

2

4

FAQ

① [ファイル] メニュー、② [マークした項目をエク
 スポート] をクリックします。





設定ファイルを保存します。●保存先を選択して、 ②ファイル名を入力し、③[保存]ボタンをクリック します。



[×] ボタンをクリックして、ESET コンフィグレー ションエディターを終了します。



ダイアログが表示されます。①[OK] ボタンをクリックし、 [処理タスク] ダイアログの②[閉じる] ボタンをクリック します。

	Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ	
		·				
ESET ADMINISTRATO MAINTENANCE TOOL	^R 保守タスク: た	が正常に完了しまし	■ ERAメノナ ンをクリッ	クします。	しまり。[終]]小グ	1
	ESET Remote A を終了するには す。別の保守交 リックにます。	dministrator Maintenance To 、「終了」ボタンをクリックしま スクを実行するには、「戻る」を	ol ク			2
						3.2 バッ ク ア
(ESET)	<≅	る(B) 終了(F) キャンセ	лисо <u> </u>			ッ プ の 作 4 成
▶>> POINT EBASの設定は、	EBACを利用することです	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	利用してERASの設定を係	そ在する場合は、「ツール」メ	ニュー、「サーバオプショ	FAQ

ERASの設定は、ERACを利用することでも保存できます。ERACを利用してERASの設定を保存する場合は、[ツール] メニュー、[サーバオプション] をクリックし、[サーバオプション] ダイアログを開きます。[詳細] タブをクリックし、[詳細設定を編集] ボタンをクリックするとESET コンフィ グレーションエディターが開くので、97~98ページの手順⑦~⑨を参考に設定ファイルを保存してください。

3.2.2 クライアント情報のデータベースの バックアップ作成手順

ここでは、ERAメンテナンスツールを利用してクライアントPCのログのバックアップを作成する手順を説明します。 ERAメンテナンスツールはERASをインストールした管理サーバーにインストールされているため、すべての作業を管 理サーバーで行います。

CAUTION

クライアントPCのログのバックアップを作成しているときは、ERASの動作が停止します。



95~96ページの手順1~3を参考に、ERAメンテ ナンスツールを起動し、[アクションの選択] ダイア ログを開きます。①[データベースのバックアップ] にチェックを入れ、②[次へ] ボタンをクリックしま す。

デ	ータベースタイプ(T):		Access		
デ	ータベースの場所(D): 2 🖸 🖓	rogramData¥ESB	ET¥ESET Remote	e Administrator¥Server¥datat
接	聽文字列(S):				
ב	ーザ:名(U):	8		-	
19	スワード(P):	í Í		-	ファイルから設定をロード(0)
7	キーマ名(M):			-	設定をファイルに保存(S)
		4 接	総のテスト(E)	現在のサー	

バックアップするデーターベースを設定します。 [データベースタイプ] および? [データベースの場 所] を選択します。 ⑧[接続文字列][ユーザ名][パ スワード][スキーマ名]など接続に必要な情報を設 定します。すべての設定を行ったら、 ④[接続のテ スト]ボタンをクリックします。

POINT

ERASの既定値のデータベースである「Microsoft Access」を利用し、かつデータベースの保存場所を変更していない場合は、この設定を行う必要はありません。また、Microsoft Access以外のデータベースを利用している場合は、[接続文字列]や[ユーザ名][パスワード][スキーマ名]などを正確に入力しないとバックアップが行えません。

and the second sec
--



 「ダンプファイル]ダイアログが表示されます。[ファ イルを参照] ボタンをクリックします。
 「
 「
 「
 「
 「
 「
 「
 「
 「
 」
 「
 」
 「
 」
 」
 「
 」
 」
 「
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 』
 「
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 」
 』
 」
 」
 』
 」
 』
 、
 』
 、
 』
 、
 」
 、
 』
 、
 」
 、
 」
 、
 」
 、
 」
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、
 、





ファイルの保存先を設定します。①保存先を選択して、2ファイル名を入力し、3[開く]ボタンをクリックします。

1

2

3.2

バックアップの作成

4

FAQ





[開始] ボタンをクリックします。



バックアップが完了すると、ダイアログが表示されます。 [OK] ボタンをクリックし、[処理タスク] ダイアログの [閉 じる] ボタンをクリックします。

	Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ	
		I				1
9	ool R 保守タスク: た ESET Remote A を終了するには す。別の保守ジ リックします。	が 正 常に 完 了しまし dministrator Maintenance To [終了床女ノをクリックしま スクを実行するには、[戻る]を 3(B) 終7(F) キャンセ	■ ERAメンテ ンをクリック	ナンスツールを終了 クします。	します。[終了] ボタ	3.2 バックアップの作成

FAQ

3.2.3 データフォルダーのバックアップ方法

ERASおよびERACは、特定のデータフォルダーをバックアップすることで各種設定や情報などをバックアップできま す。ERASは、インストール時に既定の内蔵DB (Microsoft Access)をデータベースに選択した場合に限って、以下 のデータフォルダーをバックアップすることで、取得したクライアント情報、ログなどの全ての情報をバックアップで きます。データベースにMicrosoft SQL Server 2005 Express Edition / Standard Editionなどの既定の内蔵DB (Microsoft Access)以外を利用している場合は、以下のフォルダーをバックアップしても取得したクライアント情報、 ログなどを記録したデータベースはバックアップされません。既定の内蔵DB以外を利用している場合は、利用している データベースのマニュアルなどを参考にデータベースのバックアップを別途行なってください。なお、リストア(復元)は、 バックアップしたフォルダーをバックアップ時と同じフォルダーに上書きすることで行えます。

Windows Server 2003の場合

ERAS	C: ¥Documents and Settings¥All Users¥Application Data¥ESET¥ESET Remote Administrator¥Server
ERAC	$C: {\tt VDocuments} \ and \ {\tt Settings} {\tt VAII} \ {\tt Users} {\tt VApplication} \ {\tt Data} {\tt VESET} {\tt ESET} \ {\tt Remote} \ {\tt Administrator} {\tt VOnsole} \ {\tt VAII} $

Windows Server 2008 / 2008 R2の場合

ERAS	C:¥ProgramData¥ESET¥ESET Remote Administrator¥Server
ERAC	C: ¥ ProgramData ¥ ESET ¥ ESET Remote Administrator ¥ Console

Windows Server 2012 Standardの場合

ERAS	C: ¥ ProgramData ¥ ESET ¥ ESET Remote Administrator ¥ Server
ERAC	C:¥ProgramData¥ESET¥ESET Remote Administrator¥Console

CAUTION

バックアップするERAとリストアするERAのホスト名およびバージョンが同一でないとリストア後に正常に動作しません。サーバー環境を再構築する場合は、必ず同じホスト名とバージョンに設定してください。

3.2.4 データフォルダーのバックアップ方法の流れ

ERASおよびERACのデータフォルダーをバックアップするときは、以下の流れで作業します。ERASのバックアップ を行うときは、ERASのサービスを停止する必要がある点にご注意ください。





す。

Ø フ<u>ァイルを聞く</u>

१७२७-

ファイルの場所(I): 🚺 DBバックアップ

a

ファイル名(N):

ファイルの種類(T):

ERAS Conf Backup

設定ファイル (*xml)

名前 ^ ____ERAS_Conf_Backup

3

バックアップファイルの復元

バックアップファイルの復元 ここでは、バックアップしたERASの設定ファイルおよびクライアント情報のデータベースを復元する方法を説明しま

バックアップしたERASの設定ファイルの復元手順 3.3.1

ここでは、バックアップしたERASの設定ファイルを復元する手順を説明します。ERAメンテナンスツールはERASを インストールした管理サーバーにインストールされているため、バックアップの作成時と同様にすべての作業を管理サー バーで行います。

95~96ページの手順①~⑤を参考に、ERAメンテナンスツールを起動し、「サーバーのコンフィグレーションを 1 変更]を選択して手順を進め、ESET コンフィグレーションエディターを起動します。

×

21 KB

- サイズ

開((0)

キャンセル

• G 🜶 📂 📰•

•

•

更新日時 2012/07/22 20:00 XMLドキュメント



● [ファイル] メニュー、 2 [設定ファイルをインポー ト]をクリックします。

設定ファイルを選択します。
①バックアップしてお いた設定ファイルを選択し、2[開く]ボタンをク リックします。

FAQ

1

2



ダイアログが表示されます。① [既存とのマージ] にチェックが入っている ことを確認し、② [OK] ボタンをクリックします。



 ● [ESET Remote Administrator] をク リックし、
 ● [保存] ボタンをクリックし ます。続いて
 ● [×] ボタンをクリックし、
 ESET コンフィグレーションエディター を終了します。



ダイアログが表示されます。**①**[OK] ボタンをクリックし、**②**[処 理タスク] ダイアログの [閉じる] ボタンをクリックします。

	Chapter 1	Chapter 2	CI	hapter 3	Chapter 4	FAQ	
	R 保守タスク: た	が正常に完了しまし	X	ERAX クテランをクリック	テンスツールを終了 クします。	しまり。「終了」小グ	1
	ESET Remote A を終了するには、 す。別の保守タン	dministrator Maintenance To 〔終了ボダンをクリックしま スクを実行するには、[戻る]を	ol ク				2
	リックしまり。						3.3 バッ ク
eset							アップ
	〈戻	る(B) 終了(F) キャンセ	UN(C)				ファ 4 イル
▶▶▶ POINT	有一け FPAC からも行う	マレゼズキェオ EDACをす		RASの設定を復	ニオス提合け 「ツール」マ	「艹_バナプシュ	の 復 元 FAC

設定ファイルの復元は、ERACからも行うことができます。ERACを利用してERASの設定を復元する場合は、[ツール]メニュー、[サーバオプション]をクリックし、[サーバオプション]ダイアログを開きます。[詳細]タブをクリックし、[詳細設定を編集]ボタンをクリックするとESET コンフィ グレーションエディターが開くので、手順[2]~⑤を参考に設定ファイルをインポートします。次に、[コンソール]ボタンをクリックしてダイアログが 表示されたら、[はい]ボタンをクリックします。これで設定が復元されます。

3.3.2 バックアップしたクライアント情報のデータベースの 復元手順

ここでは、バックアップしたクライアント情報のデータベースをERASに復元する手順を説明します。復元には、ERA メンテナンスツールを利用します。ERAメンテナンスツールはERASをインストールした管理サーバーにインストール されているため、すべての作業を管理サーバーで行います。

CAUTION

クライアントPCのログを復元しているときは、ERASの動作が停止します。



95~96ページの手順①~③を参考に、ERAメンテ ナンスツールを起動し、[アクションの選択] ダイア ログを開きます。①[データベースの復元]にチェッ クを入れ、②[次へ] ボタンをクリックします。

2	Service Serv				
	データベース接続のプロパラ	řイ			
	データベースタイプ(T): 1	MS Access			
	データベースの場所(D): 2 接続文字列(S):	C:¥ProgramData¥ESET	F¥ESET Remot	e Administrator¥Server¥datat	
	ユーザ名(U): 3				
	パスワード(P):			ファイルから設定をロード(0)
	スキーマ名(M):		J	設定をファイルに保存(S).	<u> </u>
	4	接続のテスト(E)	現在のサ	ーバのコンフィグレーションをロード(.L)
		□ サーバの接続設定を	置き換える(R)		
			< 戻る(B)	次へ(N) > キャン	セル(C)

復元先のデーターベースを設定します。●[データ ベースタイプ]および②[データベースの場所]を選 択します。⑧[接続文字列][ユーザ名][パスワード] [スキーマ名]など接続に必要な情報を設定します。 すべての設定を行ったら、④[接続のテスト]ボタン をクリックします。

POINT

ERASの既定値のデータベースである「Microsoft Access」を利用し、かつデータベースの保存場所を変更していない場合は、この設定を行う必要はありません。また、Microsoft Access以外のデータベースを利用している場合は、[接続文字列]や[ユーザ名][パスワード][スキーマ名]などを正確に入力しないとデータベースの復元が行えません。
Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ



[ダンプファイル]ダイアログが表示されます。[ファ イルを参照] ボタンをクリックします。 1

2

3.3

バックアップファイルの復元

4

FAQ





- ①バックアップしたデータベースファイルを選択
 - し、2[開く]ボタンをクリックします。



- [処理タスク実行時にサーバを停止する] にチェッ
- クを入れ、2[次へ]ボタンをクリックします。



 8
 eratool
 区

 <td
 <td

ダイアログが表示されたときは、[はい] ボタンをクリック します。 9





ダイアログが表示されます。1 [OK] ボタンをクリックし、 [処理タスク] ダイアログの2 [閉じる] ボタンをクリックし ます。

1

2

ERAメンテナンスツールを終了します。[終了] ボタ ンをクリックします。

3.3.3 データフォルダーのリストア(復元)

ERASおよびERACのデータフォルダーをバックアップしたときは、バックアップしたフォルダーをバックアップ時と 同じフォルダーに上書きすることでリストア(復元)できます。また、ERASを既定の内蔵DB (Microsoft Access)を データベースに利用していた場合は、取得したクライアント情報、ログなどの全ての情報をリストアできます。デー タベースにMicrosoft SQL Server 2005 Express Edition / Standard Editionなどの既定の内蔵DB (Microsoft Access)以外を利用している場合は、ERASの設定情報など一部の情報のみがリストアされます。

Windows Server 2003 / 2003 R2の場合

ERAS	C: ¥Documents and Settings ¥AII Users ¥Application Data ¥ESET ¥ESET Remote Administrator ¥Server
ERAC	C:¥Documents and Settings¥AII Users¥Application Data¥ESET¥ESET Remote Administrator¥Console

Windows Server 2008 / 2008 R2の場合

ERAS	C:¥ProgramData¥ESET¥ESET Remote Administrator¥Server
ERAC	C:¥ProgramData¥ESET¥ESET Remote Administrator¥Console

Windows Server 2012 Standardの場合

ERAS	C: ¥ ProgramData ¥ ESET ¥ ESET Remote Administrator ¥ Server
ERAC	C: ¥ ProgramData ¥ ESET ¥ ESET Remote Administrator ¥ Console

CAUTION

バックアップするERAとリストアするERAのホスト名およびバージョンが同一でないとリストア後に正常に動作しません。サーバー環境を再構築する場合は、必ず同じホスト名とバージョンに設定してください。

3.3.4 データフォルダーのリストア(復元)の流れ

バックアップしておいたERASおよびERACのデータファルダーをリストア(復元)するときは、以下の流れで作業します。なお、ERASのリストアを行うときは、ERASのサービスを停止する必要がある点にご注意ください。



3.4 ログ管理のポイント

ここでは、ESET Remote Administrator Server (ERAS) で管理されるログについて説明します。ERASで管理しているログは、「ERAサーバーログ」と「クライアントPC情報ログ」に大別されます。

3.4.1 ERAサーバーログ

ERAサーバーログは、ERASの動作に関するログです。管理サーバーに障害が発生したときの原因究明に利用でき、管理者への通知内容をログとして保存することもできます。

3.4.2 クライアントPC情報ログ

クライアントPC情報ログは、クライアントPCから収集したログです。以下のような種類のログがあり、管理者は ERACを利用してその内容を確認できます。

クライアント	クライアントPCの最新情報を確認したいときに利用します。クライアントPCのウイルス定義データベースのバージョンや、警告の有無などを確認できます。
ウイルスログ	クライアントPCで検出されたウイルスを確認したいときに利用します。クライアントPCで検出されたウイルス名やウイルスの 検出日時などを確認できます。
ファイア ウォールログ	クライアントPCで検出されたファイアウォールの警告が確認できます。ESET Endpoint SecurityおよびESET Smart Securityを利用しているクライアントPCのみ、このログが報告されます。
イベントログ	クライアントPCで発生したシステムイベントを確認できます。
HIPSログ	マルウェアやコンピューターのセキュリティに悪影響を与えようとする望ましくない活動からシステムを保護するHIPSのログを 確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログを開き、[サーバの保守] タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。
デバイスコン トロールログ	USBストレージやCD / DVDなどのデバイスの制御動作のログを確認できます。既定値では、このログは取得されません。取得 するには、[サーバオプション]ダイアログを開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設 定を行う必要があります。
Webコント ロールログ	Web制御動作のログを確認できます。既定値では、このログは取得されません。取得するには、 [サーバオプション]ダイアログ を開き、 [サーバの保守]タブにある [ログ収集パラメータ] ボタンをクリックして、設定を行う必要があります。ESET Endpoint Securityを利用しているクライアントPCのみ、このログが報告されます。
迷惑メール対 策ログ	迷惑メール対策のログを確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログ を開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。ESET Endpoint SecurityおよびESET Smart Securityを利用しているクライアントPCのみ、このログが報告されます。
グレーリスト ログ	グレーリストのログを確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログ を開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。なお、このログは、 日本語版では確認できません。
検査ログ	クライアントPCで実行されたスキャン結果を確認できます。
モバイルログ	ERASで管理しているAndroid端末の詳細なログが表示されます。
隔離	隔離されたウイルスに関する情報を確認できます。
タスク	ESET Remote Administrator Console(ERAC)を利用してERAS から実行されたタスクの動作結果などの情報を確認できます。

3.4 ログ管理のポイント

1

3.4.3 ERAサーバーログの設定変更手順

ここでは、ERAサーバーログの設定を変更する方法を説明します。ERAサーバーログの設定は、ERACを利用してERAS にログオンすることで行います。



ERACを起動し、ERASにログオンします。[ツール] メニュー、[サーバオプション] をクリックして、[サーバオ プション] ダイアログを開きます。



 ● [ログ] タブをクリックします。ERAサーバーログに関する設定 を行い、
 ② [OK] ボタンをクリックします。設定内容については、 以下をご参照ください。

	監査ログ
データベースにログを 保存する	チェックを入れると、データベースに監査ログを記録します。監査ログは、すべてのERACユーザーによるコン フィグレーションの変更および実行されたアクションを監視して記録します。
	チェックを入れると、監査ログをテキストファイル形式で保存します。[ファイルの設定]ボタンをクリックすると、 作成するログファイルの名称やログをいつ削除するかなどの設定が行えます。このログは、既定値では以下のフォ ルダーに保存されます。
テキストファイルにログを 保存する	Windows Server 2003/2003 R2の場合 C: ¥Documents and Settings ¥AII Users ¥Application Data ¥ESET ¥ESET Remote Administrator ¥Server ¥logs
	Windows Server 2008/2008 R2の場合 C: ¥ProgramData ¥ESET ¥ESET Remote Administrator ¥Server ¥logs
OSのアプリケーションログ に記録する	チェックを入れると、OS のイベントビューアに監査ログの情報をコピーします。
Syslogにログを保存する	チェックを入れると、Syslogに監査ログ情報を保存し、保存するログレベルを設定できます。ログレベルは、既 定値の[レベル2]で利用することを推奨しています。
	サーバログ
テキストファイルにログを 保存する	チェックを入れると、ログをテキストファイル形式で保存します。ログレベルは、既定値の[レベル2]で利用す ることを推奨しています。また、[ファイルの設定]ボタンをクリックすると、作成するログファイルの名称やロ グをいつ削除するかなどの設定が行えます。このログは、既定値では監査ログと同じフォルダーに保存されます。
OSのアプリケーションログ に記録する	チェックを入れると、OS のイベントビューアにサーバーログの情報をコピーします。
Syslogにログを保存する	チェックを入れると、Syslogにサーバーログ情報を保存し、保存するログレベルを設定できます。ログレベルは、 既定値の[レベル2]で利用することを推奨しています。
	デバックログ
テキストファイルにログを 保存する	チェックを入れると、デバックログをテキストファイル形式で保存します。[ファイルの設定]ボタンをクリック すると、作成するログファイルの名称やログをいつ削除するかなどの設定が行えます。このログは、既定値では 監査ログと同じフォルダーに保存されます。また、デバックログの推奨設定はオフです。
Syslogにログを保存する	チェックを入れると、Syslogにデバックログ情報を保存します。また、デバックログの推奨設定はオフです。

3.4.4 クライアントPC情報ログの設定変更手順

ここでは、クライアントPC情報ログの設定を変更する方法を説明します。クライアントPC情報ログの設定は、ERACを利用してERASにログオンすることで行います。

BRACを起動し、ERASにログオンします。[ツール]メニュー、[サーバオプション]をクリックして、[サーバオ プション]ダイアログを開きます。

2	▼サーバオブション[Eset-svr]	×
	一般 セキュリティ サーバの保守 ログ 【複製 】アップデート】その他の設定 【詳細】	
	サーバメンテナンス中に実行できるクリーンアップの設定および複数のタスクがあり、一 部はここで構成することが可能です。	
	ログ収集パラメータ(L)	
	時間間隔でクリーンアップ	
	クリーンアップの設定(N)	
	— ログ記録の数による高度なクリーンアップ	
	クリーンアップの誕祥和醋設定(V)	
	クリーンアップ 毎1日開始時刻 03:00 (サーバのローカルタイム) 変更(A)	
	<u>フタソンサーフアサノ(0)</u> 正体と修復のフレジューラ	
	正1162183度のスケシューラ 圧縮 毎 15日開始時刻 23:00 (サーバのローカルタイム) 変更(H)…	
	54/ m/t #70	
	□	
	OK(O) キャンセル	

 ● [サーバの保守] タブをクリックします。クライ アントPC情報ログの保存に関する設定を行い、
 ● [OK] ボタンをクリックします。設定内容について は、以下をご参照ください。

4

1

2

3.4 ログ管理のポイント

ログ収集パラメータ	サーバーが受信するログのレベルを定義できます。HIPSログやデバイス制御ログ、Web制御ログ、迷惑メー ル対策ログ、グレーリストログは、既定値では取得されません。この設定を変更したいときは、ここで行います。
クリーンアップの設定	ログを削除するまでの期間を設定できます。設定は、各ログごとに行えます。
クリーンアップの詳細設定	常時保存しておくログの最大件数を設定できます。設定は各ログごとに行え、ここで指定した件数を超えると 古いログから順に削除されます。また、クリーンアップの設定も併用すると、先に設定した条件を満たしたほ うが優先されます。
圧縮と修復のスケジューラ	データベースの圧縮と修復を行う間隔を設定します。圧縮と修復を行うと、不整合や誤作動がなくなり、デー タベースとの通信速度が向上します。[変更]ボタンをクリックすると、データベースの圧縮と修復を行う間隔 を設定できます。また、[今すぐ圧縮]ボタンをクリックすると、直ちにデータベースの圧縮と修復を開始され ます。
クリーンアップスケジューラ	指定された間隔でデータベースのクリーンアップを実行します。[変更]ボタンをクリックすると、クリーンアッ プを実行する間隔を設定できます。また、[今すぐクリーンアップ]ボタンをクリックすると直ちにクリーンアッ プが開始されます。

※データベースのクリーンアップおよび圧縮と修復は、スケジューリングしてサーバの負荷が最少のときに実行することをお勧めします。既定では、3カ月または6カ月を経過したエントリとログは削除され、15日ごとにデータベースの圧縮と修復が実行されます。

[Chapter 4] ウイルス対策における運用

4.1	ウイルス対策のポイント
4.2	日常の運用119
4.3	ウイルス検出時(緊急時)の対応
4.4	ウイルス検出時の対応例
4.5	ウイルス誤検出時の対応



ここでは、ESET ライセンス製品を利用したウイルス対策の運用方法について説明します。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。

4.1.1 ウイルス対策における運用



運用フェーズ	概要	参照ページ
日常の運用	ESET ライセンス製品導入後、日頃からクライアント PC の各種ログやウイル ス定義データベースのバージョンなどを確認します。	119ページ
ウイルス検出時(緊急時) の対応	クライアントPCがウイルスに感染した場合、報告から初動対応、詳細調査、防止・ 抑止策の実施などを行います。	122 ページ
ウイルス誤検出時の対応	Windows や Mac OS X のシステムファイルやアプリケーションで利用される 問題のないファイルを誤ってウイルスと判定する場合があります。その際、隔 離ファイルの復元や除外設定などを行います。	131 ページ

4.2 日常の運用

ここでは、ESET ライセンス製品導入後の日常の運用について説明します。

4.2.1 日常の運用フェーズ

ESET ライセンス製品導入後の日常の運用は、「確認」「適用」「追加導入」の3つのフェーズがあります。それぞれのフェー

ズで実施すべき主な事柄は、以下のとおりです。

確認	 ・ウイルス定義データベースのバージョン確認 ・プログラムのバージョン確認 ・ライセンス期限/クライアント数の確認 ・各種ログの確認 ・ウイルス検出状況の確認 ・設定状況の確認
適用	 ・最新ウイルス定義データベースへのアップデート オフライン環境でのアップデート/時差配信 ・最新プログラムへのアップグレード ・ポリシーの適用・タスクの適用
導入	 ・新規のコンピューターにクライアント用プログラムをインストール ・ライセンスの更新

1

2

4.2.2 クライアントPCの状態を確認するには

「確認」フェーズでは、ESET Remote Administrator Console (ERAC) を利用してクライアントPCの状態を確認しま す。クライアントPCの状態は、[クライアント] [ウイルスログ] [ファイアウォールログ] [イベントログ] [HIPSログ] [デ バイスコントロールログ] [Webコントロールログ] [迷惑メール対策ログ] [グレーリストログ] [検査ログ] [モバイルロ グ] などのペインを利用して確認できます。また、各ペインに表示する項目は[ツール]、[コンソールオプション] をクリッ クして [コンソールオプション] ダイアログを開き、[カラム-表示/非表示] タブで変更できます。

■[クライアント]ペイン

[クライアント]ペインは、クライアントPCの様々な情報を総合的に確認するときに利用します。確認できる項目は、 利用しているESET ライセンス製品の製品名やバージョン、ポリシー名、最終アクセス日時、保護状態の説明、定義デー タベースのバージョン、最終ウイルス警告、最終ファイアウォール警告、最終イベント警告、最終感染ファイル、最終 駆除ファイル、最終検査日時、再起動要求、OS名などがあります。

■ [ウイルスログ] ペイン

[ウイルスログ]ペインでは、クライアント用プログラムによって検出されたウイルスに関する詳細なログを確認できます。

■ [ファイアウォールログ] ペイン

[ファイアウォールログ]ペインでは、ESET Endpoint SecurityおよびESET Smart Securityによって検出されたファ イアウォールに関する詳細なログを確認できます。

■ [イベントログ] ペイン

[イベントログ] ペインでは、クライアントPCで発生したイベント(アップデートの成功・失敗などに関する詳細なログ を確認できます。

■[HIPSログ]ペイン

[HIPSログ] ペインでは、マルウェアやコンピューターのセキュリティに悪影響を与えようとする望ましくない活動か らシステムを保護するHIPSのログを確認できます。既定値では、このログは取得されません。取得するには、「サーバ オプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリックして、設定を行う 必要があります。

■ [デバイスコントロールログ] ペイン

[デバイスコントロールログ]ペインでは、USBストレージやCD/DVDなどのデバイスの制御動作のログを確認できま す。既定値では、このログは取得されません。取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」 タブにある「ログ収集パラメータ」ボタンをクリックして、設定を行う必要があります。

■ [Webコントロールログ] ペイン

[Webコントロールログ] ペインでは、Web制御動作のログを確認できます。既定値では、このログは取得されません。 取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリッ クして、設定を行う必要があります。ESET Endpoint Securityを利用しているクライアントPCのみ、このログが報 告されます。

■[迷惑メール対策ログ]ペイン

[迷惑メール対策ログ]ペインでは、迷惑メール対策のログを確認できます。既定値では、このログは取得されません。 取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリッ クして、設定を行う必要があります。ESET Endpoint SecurityおよびESET Smart Securityを利用しているクライ アントPCのみ、このログが報告されます。

■ [グレーリストログ] ペイン

[グレーリストログ]ペインでは、グレーリストのログを確認できます。既定値では、このログは取得されません。取得 するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリック して、設定を行う必要があります。

■[検査ログ]ペイン

[検査ログ]ペインでは、クライアントPCで実行された[コンピュータの検査]に関するログを確認できます。

■ [モバイルログ] ペイン

[モバイルログ]ペインでは、ERASで管理しているAndroid端末の詳細なログが表示されます。

1

日常の運用



ウイルス検出時(緊急時)の対応

ウイルス感染などの緊急時には、運用フェーズにおける、すみやかな対応が必要になります。ここでは、ウイルスを検 出したクライアントPCが発見された場合の対応ステップの例を紹介しますので、運用の際の参考にしてください。

4.3.1 ウイルス検査時の対応の流れ

STEP1 ウイルスの発見および報告

- ・ウイルスの発見
- ・管理者への通知(通知マネージャを利用し電子メールで管理者へ通知)
- ・ウイルスが検出されたコンピューターの利用者、その他関係者への連絡

STEP2 初動対応の実施

・ウイルスが検出されたコンピューターの利用中止(ネットワークケーブルを外し、該当PCをネット ワークから切断する)

- ・ローカルドライブのウイルス検査の実施
- ・ウイルスの隔離・駆除・削除の実施
- ・ウイルスの駆除・削除ができない場合、サポートセンターへのお問い合わせ

STEP3 ウイルスの詳細調査・報告

- ・ウイルスの特定と感染範囲の把握
- ・システムへの影響範囲の特定と対応
- ・感染経路の特定(原因特定)
- ・感染状況の報告

STEP4 防止・抑制策の実施

- ·OSやアプリケーションのセキュリティパッチ適用/コンピューターの構成変更(設定変更)
- ・感染源へのアクセス制御



ウイルス検出時の対応例

ここでは、ウイルスが検出された場合の実際の対処例を元に具体的な運用例を紹介します。運用の際の参考にしてくだ さい。

4.4.1 ウイルスが検出されたときの対処手順

仮定する状況

- ・クライアントPC 複数台でウイルスを検出
- ・最新のウイルス定義データベースでウイルスの駆除が可能
- ・上層部ヘウイルスの発生状況の報告が必要
- ・感染経路は、ユーザー私物のUSBメモリー



ウイルス検出時の対応例 FAQ

4.4

1

2

4.4.2 STEP1 管理者への通知

ウイルスが発見された場合、まず管理者に通知します。管理者への通知は[通知マネージャ]を利用し、一定数以上のク ライアントPCでウイルスが検出された場合に、電子メールで管理者に通知することで実現します。この機能を利用する と、緊急性を即座に感知し迅速な対応が行えます。[通知マネージャ]は各種警告をカスタマイズでき、日常の運用事項 を登録することで安全な運用が行えます。

[通知マネージャ]を利用し管理者に様々な情報を電子メールで通知するには、[サーバオプション]の[その他の設定] タブ内の[SMTP設定]で、電子メール送信に利用するSMTPサーバーが設定されている必要があります。また、[通 知マネージャ]で[通知ルール]を事前に登録しておく必要があります。通知機能の詳細については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



1

2

3

4.4

ウイルス検出時の対応例

FAQ

4.4.3 STEP2 ウイルスの隔離・駆除・削除

ウイルス検出時は管理者への通知と共に、ウイルスの蔓延を防止することに注力します。ウイルスの蔓延を防ぐために 重要なポイントは、ウイルスの隔離・駆除・削除を行った後に再度ウイルス検査を実施し、二重、三重のチェックを行う ことです。再度のウイルス検査を実施することによって、別ウイルスによるさらなる蔓延を防止できます。該当ウイル スを検出していないクライアントPCでもウイルス検査を実施し、安全を確認します。

なおウイルス検査を実施する場合は、各クライアントPCのローカルディスク全体を検査対象とします。ウイルス検査の 実施は、管理者がERAを利用したリモート操作で一括して行うこともできます。

4.4.3.1 ERAを利用したリモート検査の実施手順

ERACを起動し、ERASにログオンします。

ここでは、ERAを利用してクライアントPCにリモート検査を実施する方法を説明します。

「 フィルタを使用する(U) クライアント	すべてのサーバを対象にする	 <i>¥195 ¥195</i>	サーバを追加す クライアントを追け	<u>るには?</u> 加する				
他のオブション 変更を運用(A) リセット(R)	サーバ名 ム	051721	定義データベース	の状態	最も古いアクセス	最終	フイルス警告	最終ファイアウ
クライアントフィルタ条件	Eset-svr	5	現在のバージョン		3 分前	0		0
5.1. MARIE - 7								
B ad-domain.example.com (
Computers (Active Dir	•							
	表示するアイテム	P4	テム情報:		W-T 1000	カフカノ あテエ	- 12	
□ ③ 本社((本社)//-/)	(0)		5 (5アイテム)全5ア	የイテムアイテ	4 SETTE-P(M):	DIVIDABOICU		(month but
	Firet-our		1901-0-22	Juity Micro	co 4512002	歴史のプライマ	サード 時常のせらくマリ	2 公前
	Eset-win7-pc	「小田田(A) 「田して湯田(D)	Ctrl+A	Antivirus	5.0.2122	大田(0)2515	し、 以近のフライマリ	4秒前
□···· ホリント □□□□ 既定のプライマリカライアント	🗳 Eset-winxp	監択アイテムの反転(D)	Ctrl+I	Security	5.0.2122	既定のプライマ	リ 既定のプライマリ.	12 秒前
白	Kitagawa-no-m j	置択アイテムを非表示(H)	CtrHH	ntivirus	4.1.86	既定のプライマ	リ 既定のプライマリ.	3分前
— 🗖 🔛 サーバがジシー (Eset-s	User-pc j	蟹択アイテムのみ表示(U)	CtrH+U	Security	5.0.2122	現定のフライマ	リ 以定のフライマリ.	. 54 秒前
	3	所規タスク(T)		מירעיד	()			
		ノリシフィアンドリアニシ(F) 素板を利用金(C)	-	オンデマン	ンドスキャン(D)	(0)		
		15グをセット/リセット(S)	- 4	今すぐア	ップデート(U)	107		
		データのリクエスト(E)		SysInsp	ectorスクリプト(S)			_
		バルーブ(こ)自加(G)…		保護機能	能(P) いないわてわの書に(P	A		
	,	約シーの設定(P)		「高部から	ール省のタベクの美口に「 の復元/削除(Q)	Ŷ		
■ /5/(ア)トのみ (フレーズ接受) ▼		モートインストール(D) 19イアウォールルールフージウィザッ	- K(W)	ウイルス	データベースのロールバッ	ታ(Z)		
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			1407	クライアン	/トのアップデートキャッシ	100/JP(X)		
754 YJJ =/1(P):]		37ム切象示/非象示(N)		 通知の満 	「1111日ロンの「FB3((G) 表示(N)			
クライアント名(C):	P P	川『余(D)	Del	1				
コンピュータ名(0):	2	約シー(L)						
MACアドレス(M):		高高新(Q)	F7	_				
		iysinspector(Y) N/T//TL/=S/s/(A))	FA	-				
□ 問題の3-表示(Y) 編集(0)				-				

 ● [クライアント] タブまたは [[ク ライアント] ペインを表示] ボタン
 をクリックし、 ② [クライアント]
 ペインに表示されているクライン
 トPCを右クリックします。 ③ [新
 規タスク] → ④ [オンデマンドス
 キャン]をクリックします。

POINT

[オンデマンドスキャン]ダイアログは、[アクション]メニューをクリックし、[新規タスク]、[オンデマンドスキャン]を選択することでも 開けます。



[オンデマンドスキャン] ダイアログが表示されま す。Windows端末のウイルス検査を行うときは、 設定セクションに①[Windows ESETセキュリ ティ製品のオンデマンドスキャンタスク]が選択さ れていることを確認します。②ローカルドライブに チェックが入っていることを確認し、③[次へ] ボタ ンをクリックします。

POINT





クライアントPCを選択します。①[すべてのアイテム]リストからオンデマンドスキャンを実施するグ ループまたはクライアントPCをクリックし、②[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、③[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。

1

2

3

4.4

ウイルス検出時の対応例

FAQ

●タスクの実行日時などの設定を行い、 2 [終了] ボ え タスク レポート 新しいタスクの最終レポート タンをクリックします。 タスクの種類オンデマンド スキャンと駆除 コンフィグレーション ファイル名 C:¥Users¥ADMINI Ĩ¥AppData¥Local¥Temp¥RAC5AA4.tmp **適時級** グループ WindowsOS/ タスクの設定・ オンデマンド スキャンと駆除 名前(N) 説明(D) Г □ 指定日時にタスクを実行する(A) 2012/08/04 -タスクが正常に完了した場合、タスクを自動的に削除する(E) ランダムに遅らせる開始時間の上限(R) 60 分間 ÷ 上のオプションはESET製品5以上のみに適応可能です。 0 終了(F) 戻る(B) キャンセル

>>> POINT

5

[指定日時にタスクを実行する] にチェックを入れ、日時を指定すると、指定した日時にオンデマンドスキャンのタスクが配布されます。また、 ESET Endpoint SecurityまたはESET Endpoint アンチウイルスに対してオンデマンドスキャンタスクを配布する場合は、[ランダムに遅らせる開 始時間の上限] にチェックを入れ、時間を設定すると、タスクの遅延実行を行えます。

CAUTION

オンデマンドスキャンタスクは、WindowsとMac OS X、Linux、Androidで別々にタスクを配布する必要があります。たとえば、Windowsがイン ストールされたクライアントPCにMac OS X用のオンデマンドスキャンタスクを配布すると、タスクが実行されずにエラーとなります。オンデマン ドスキャンタスクを配布するときは、各OSごとに行ってください。

4.4.4 STEP3 報告~レポートの作成

ウイルス検出時と終息時には、レポートを作成します。ERAは、管理しているクライアントPC情報ログをもとにレ ポートを作成する機能を搭載してます。この機能を利用すると、ウイルス検出状況の詳細を簡単にレポート化できます。 また終息時にも同一フォーマットでレポートを作成することで、ウイスル感染から事態の終息までを視覚化できます。 ERASを利用したレポートの作成は以下の手順で行います。

■ ERACを起動し、ERASにログオンします。

お気に入り	ダッシュボードテンプレー	レポートテンプレート	1005れたレポート 2005	
	デンブレート名 「「「クイルスが 」「「クイルスが 」「「クライアント 」「「問題の多	対ティブなクライアント な 躍サマリ な 模要 な りうライアント な	(成 最終刊ガー し 17週間前 し 12間前 し 12 し	120月 未販除ウイルスの検出されたウライアント すべてのウライアントのカスタム(1487-ハールドのサマ) すべてのウライアントの基本ステータスのサマリを表示 問題の後3時の多いウライアント
		パート ね フーの攻撃レポート ね パート ね ペールレポート ね	し 15年間前 し 15年間前 し 15年間前 し 15年間前	366820株果(近差107月) はないアーンは第400年の後にした107月) 19年10月20日 1月2
	(県作(6) オブション インター/	名前を付けて(保存(A)_ い スケジューラ		インボート(0. ・ 頭定のテンプレート
	会讨论者到的存住	nt at 5(G)		
	今マぐ書給りを当 レポート 種類(P) スタイル(S)	。成する(G) 「総合カスタムレポ 「ブルースキーム	~h	×
	 今マく鮮や92 レポート 種類(P) スタイル(S) フィルタ 対象のクライアント 骨廠(T) 	成する(Q) 総合カスタムレポ ブルースキーム C) すべて すべて		× × ×

 [レポート] タブをクリックし、②[レ ポートテンプレート] タブをクリックしま
 す。③レポートテンプレートから作成し
 たいレポートをクリックします。

POINT

[対象のクライアント]や[脅威]のドロップダウンボタンをクリックすると、選択したクライアントPCやウイルスに絞り込んでレポートを作 成できます。また、[追加設定]ボタンをクリックし[レポート詳細設定]ダイアログを開くと、CSV形式でレポートを保存するなどの設定が 行えます。

★ お気に入り	ダッシュボードテンプレート レポート テンプレー	-ト 作成されたレポート		
A DADO	レポートテンプレート		1 =	1 mars
	テンプレート名 /	頻度	最終刊ガー	1R ^B H
		r 440	13298091	**乾杯ワイルスの狭心されたジライアフト オイアのたちノアントのもうたい状態の シールドの分支の
	□ 1000000000000000000000000000000000000	20		マンプルクライアンドのガスタム酸剤リオールドのウマク
	口に開発の多いかっていた	ttl.		問題の種類のもいわらくアント
	□ IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	201 x1	1週間前	SMSの概要(過去1か月)
	□ 12総合ネットワーク攻撃レポート	なし	1週間前	ネットワーク攻撃の概要(過去1か月)
	□ 脱総合脅威レポート	なし	1週間前	ウイルス概要(過去1か月)
	□ 1120総合迷惑メールレポート	なし		速惑メールの概要(過去1か月)
	オブション インターバル スケジューラ	F(A)	新規	(ンポートロ
	1年1433 360210101年4 オブジュン (ンターバル) スケジューラ 特徴 現在(2) 1 日 で 現在(2) 1	(A) (FIDB(E)		(2オートロ・) 既定のデン2
		(A) (A)(A)(E) 	00 a	○オートロ. ▼ 其電の522

期間を設定します。①[インターバル]タ ブをクリックします。②[次の日時から] にチェックを入れ、③ドロップダウンボ タンをクリックして、ログの取得開始日 時を設定します。

1

2

3

4.4

ウイルス検出時の対応例

FAQ

ア接続 [Eset-svr] - Administrator - ESET Remo ファイル(F) 編集(E) アウション(A) 表示(V) ツール(T) びびびび (A) 単一 (A) マション(A) また(V) ツール(T) te Administrator C ヘルプ(H) 4) 👂 📋 49 🛄 📰 📧 😹 💷 🤐 • ダッシュボードテンプレート レポートテンプレート 作成されたレポート お気に入り 🚖 お気に入り 923素-ド5270-トレード本キト5270
 レート・
 レステート
 マンガレート

 マンガレート

 マンガレート

 マンガレート

 マンガレート

 マンガレート

 マンガレート

 マンガレール

 マンガレー

 マンガー

 アンガー

 アンガー

 アンガー

 アンガー

 アンガー

 アンガー

 アンガー

 アンガー

 ア 【2時間 未包括ウイルスの検出交れたウライアント すべてのウライアントの立な人は個子イッドのウマリ すべてのウライアントの基本ステージスのサマリを表示 問題の優美知らや、セライアント SMAの側層(電気)かり、 からの間の(電気)があり、 注意メールの側層(過去)か月) ■ 最終回方ー 1週間前 (保存(S) 名前を付けて保存(A).. 単版(E) 新規 インボート(D.. ・ 既定のテンプレート オブション インターバル スケジューラ | 時間 ・現在(X) 日 ○ 過去(M) 5(F) 1821:30 201 2012年8月 • 注意: 11-1-1-10-1 問機管によって使用されます。 : ± 3 **4** 2 3 9 10 16 17 23 24 30 31 81 7 14 21 28 1 8 15 22 29 6 18 20 27 18 25 今日: 2012/08/04 ■ ク... | 0 ウイ... | 1 ファ... | 0 イベ... | 0 | ⑧ グレ... | Q 検... | 圓 モバ... | 圓 隔離 | ▶ タスク | ┣ レポート | ◎ リモ... |

終了日時を設定します。[次の日時まで] のドロップダウンボタンをクリックし、終 了日時を設定します。

T BALAU	- LW-h => - Ch = 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	ブレート 作成されたレオ	*	
	Fridue ka	1 85107	暴怒知者。	1 IGAB
	IP IP ウイルスがアクティブなクライ	アントなし	1,5982,61	未駆除ウイルスの検出されたクライアント
	□ 12カスタム情報サマリ	なし	1742740707	すべてのクライアントのカスタム情報フィールドのサマリ
	口」「アクライアント概要	なし		すべてのクライアントの基本ステータスのサマリを表示
	□ 127問題の多いクライアント	なし		問題の種類の多いクライアント
	IP 総合SMSレポート	なし	1週間前	SMSの概要(過去1か月)
	□ 12部総合ネットワーク攻撃レポー	-ト なし	1週間前	ネットワーク攻撃の概要(過去1か月)
	□ 副総合會感レポート	なし	1週間前	ウイルス概要(過去1か月)
	□ 122総合迷惑メールレポート	なし		迷惑メールの概要(過去1か月)
	(保存(S) 名前を付けて) (保存(S) 名前を付けて) (フターバル スケジューラ のまく時かまた #まま(A)	(\$17(A) B(B)((E) 新規	インボードロ. マ 既定のデンプレー
	(森祥(5) 名前を付けて (森祥(5) 名前を付けて (1) (オブジョン) (シターバル スケジューラ (2) 今すぐ論りた生成する(0) レポート	(#1\$(A)	(E) <u>3ff38</u>	インボードロ. • 閲覧のデンフレー
	(保存(S)) 名前を付けてい 1 (子7525) (1)ター(74) スクジューラ 2 (今うく時約5を主成する(G) しボート 種類(P) 総会力	(梁存(A) 前頃() 7 りスタムレポート	(E) 3折规	インボードロ 取取のデンプレー 取取のデンプレー
	(译称(S) 金額を付けて 1 (学校(S) 2 (小みー(小) スカフューラ 9 (分前の完全近する(G) レポート 総数(P) 総合式 スカイル(S) 7 ルー	(保存(A) 前数) う りスタムレポート スキーム	(E) 新規	400m-H0
	(単常い) 名前射付けて 1 (オジシン・ハルーバ) スカジュース ・ パート ・ パート 一 (ポート 一 (ポート 一 (ポート) 一 (ポート) - スト(ル(5)) 7(ルー) - スト(ル)	(保存(A)) 前頃後(う) りスタムレポート スキーム	(E) 1 fr/tt,	12#-K0. *
		(梁存(A)」 削減(う) り入タムレポート スキーム	(E) <u>¥hija</u>	インボード0. v 「放金のテンプレー
		(留存(A)) 前頃の ラ) りスクムレポート スキーム	(E)	450年-K0

レポートを作成します。**①** [オプション] タブをクリックし、**②** [今すぐ作成] ボタ ンをクリックします。



レポートが作成されます。レポート作成 中は、進捗状況が表示されます。作成し 終わるとWebブラウザーが開き、レポー トが表示されます。

4.4.5 STEP4 防止・抑止策の適用

今回の例では、USBメモリー(外部デバイス)経由でウイルスに感染したことが前提となっているので、防止・抑止策として、クライアントPCに対して外部デバイス(USBメモリーやUSB HDD、CD-R、DVD-Rなど)の利用を禁止する設定を行うか利用できるデバイスを制限します。設定は[ポリシーマネージャ]を利用し、全クライアントPCに外部デバイスの使用禁止ルールまたは利用できる機器を制限するルールを一括配布するか、コンフィグレーションタスクで同様の設定を作成しそれを配布します。以下にデバイスを制御する場合の運用例を掲載しておきますので参考にしてください。

運用例1

許可されたデバイスのみ利用可能とする

デバイスコントロール機能を利用すると、各クライアントPCで利用できる外部デバイスを指定でき、特定のUSBデバイスのみ利用可能にしたり、利用不可にすることができます。たとえば、私物のUSBメモリーを利用不可にし、許可されたUSBメモリーのみを利用可能に設定できます。この機能は、ESET Endpoint Security、ESET Endpoint アンチウイルスおよびESET NOD32アンチウイルスで利用できます^{*}。

※ESET NOD32アンチウイルスでは一部機能制限があります。



運用例2

特定のパソコンのみ外部デバイスの利用を許可

外部デバイスの利用可/不可をパソコン単位で制御します。たとえば、特定のパソコンのみUSBデバイスの利用を許可し、その他のPCについてはUSBデバイスの利用を制限することができます。





ウイルス誤検出時の対応 4.5

誤検出とは、WindowsやMac OS Xのシステムファイルやアプリケーションで利用される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です。ここでは、クライアント用プログラム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。

4.5.1 ファイルがウイルスとして検出された場合の対応手順



4.5

1

2

4.5.2 隔離されたファイルの復元手順~クライアントPC編 (Windowsの場合)

ここでは、ESET Endpoint SecurityまたはESET Endpoint アンチウイルス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。







● [復元] したいファイルをクリックし、
 ❷ [復元] をクリックします。



確認ダイアログが表示されます。[はい] ボタンをク リックします。

隔離されたファイルの復元手順~クライアントPC編 (Mac OS Xの場合) 4.5.3

ここでは、ESET NOD32アンチウイルス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。



メインウィンドウを開き、詳細モード に切り替えて、 1 [ツール] ボタンをク リックし、2[隔離]ボタン、もしくは[隔 離] をクリックします。

	0 0		ESET NOD32 Antivirus			-
	SET NOD32 Antivirus 4	Business Edition				\frown
	保護の状態	隔離				
	コンピュータの検査	日時	名前	サイズ	理由	数
		11/09/26 0:56:43	/Users/mac-air/Desktop/eicar_com.zip	184	Eicar テストファ…	
	アップデート	11/09/26 0:55:06	/Volumes/share/Canon-ITS/☆ワイルス扱い…	68	Eicar テストファ…	
		11/09/26 0:52:26	/Users/mac-air/Downloads/eicar.com.txt.d	68	Eicar テストファ…	
3	2 設定	11/09/26 0:51:14	/Users/mac-air/Desktop/eicar.com	68	Eicar テストファ…	
3	1 ⁶	11/09/26 0:51:14	/private/var/folders/3c/3kpbjgd11f7bwm8	68	Eicar テストファ…	
S	W-11.	11/09/04 22:04:51	/Users/mac-air/Desktop/doc/eicar_com.zip	184	Eicar テストファ…	
3		11/09/04 22:04:51	/Users/mac-air/Desktop/doc/eicarcom2.zip	308	Eicar テストファ…	
	🕒 ログファイル					
	🖸 隔離					
	🕒 スケジューラ					
	? ヘルプ					
		隔離	復元 2			

3

か?

す。

●復元したい項目をクリックし、 2 [復 元] ボタンをクリックします。



ウイルス誤検出時の対応

FAQ

1

4.5.4 隔離されたファイルの復元手順~クライアントPC編 (Linuxの場合)

ここではESET File Security for Linuxでウイルスとして検出されたファイルの復元手順を説明します。

) コマンドラインで以下のように入力し、隔離されているファイルを一覧表示します。

/opt/eset/esets/sbin/esets_quar -I

隔離ファイルの一覧表示例

id="5834281359974756716", date="17.01.2013 14:11:12", name="./eicar.com", size="68", reason="Eicar test file", count="1" id="5834280538916396591", date="17.01.2013 14:07:41", name="/root/testfile.txt", size="61", reason="added by user", count="1"

ファイルを復元します。上記の隔離ファイルの一覧例から「testfile.txt」を「/tmp」ディレクトリに復元する場合 は以下のように入力します。

/opt/eset/esets/sbin/esets_quar -r /tmp -object-name=/root/testfile.txt

POINT

2

復元された後のファイル名は「5834280538916396591.testfile.txt」のように「ID.元のファイル名」になります。

	コラム	
豪離された	ファイルのダウンロード マイルをダウンロードしたいときは、以下の手順で作業します	。 Webブラウザーを開き、Webインタ-
ESET Server See Partimut/bd0/sdurie Home Licenses Configu Update On-Demand Scan Statistics Couramine 2	Curity 1 artice Control Help Logout Quarantine Search criteria Bearch criteri	フェースのページを開きます。 ①[Control]をクリックし、 ②[Quarantine]をクリックします。ダウンロードしたいファイルの ③[Download]ボタンをクリックし、ファイルを保存します。
	Import file into quarantine: Date File Size Reason Count D6 01 2013 05 30 59 test4 eve 903 added by user 1 Detelle Size Count 3 06 01 2013 06 30 59 test4 eve 903 added by user 1 Detelle Size Count 3 06 01 2013 06 40 54 Anome/share/test2 zip 114 Exar test file 1 Detelle Size Countoin 3 04 01 2013 06 43 44 Anome/share/test/leizar_com zip 104 Exar test file 1 Detelle Size	

4.5.5 隔離されたファイルの復元手順~クライアントPC編 (Androidの場合)

ここでは、ESET Endpoint Security for Android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。

■ ESET Endpoint Security for Androidのメイン画面を開きます。





[隔離] をタップします。

1



2	<u>↓</u> ⊚	6:37
U		
	/mnt/sdcard/Download/eicar_com.zip 2013/05/09 6:31:17	>
	▲ 実行しますか?	
	選択したファイルを復元しますか	?
	はい いいえ	
		י ק

復元したいファイルをタップします。

ダイアログが表示されます。[復元] をタップします。

確認画面が表示されます。[はい]をタップします。

4.5.6 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。

│ ERACを起動し、ERASにログオンします。



復元作業を始めます。①[隔離]タブをク リックし、2復元したいファイルを右ク リックして3[隔離からの復元/削除]をク リックします。

2	7 隔離からの復元/削除	×
U	アクションの違択	
	ファイルフィルタ ○ ハッシュ(H) ☑ bec 1b52d350d721c7e22a6d4bb0a92909893a3ae	
	 ○ 定義された条件(C) □ 発生日時(C) 20:33 ま 2012/07/23 ▼ - 20:33 ま 2012/07/23 ▼ □ 侵入(0) Eicer テストファイル 	
	Tプジェクト名 (B) C¥Users¥user¥Desktop¥eicarcom2zip	
	🗖 サイズ(S) 308 🚍 バイト 🔽 - 308 🚍 バイト 🔽	
	2 次へ(N) キャンセル	

復元を実行します。①[復元]にチェックを入れ、② [次へ] ボタンをクリックします。

POINT

[除外も追加する]は、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。

1

2

3

FAQ



クライアントを選択します。①[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、②[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、③[次へ] ボタンをクリックします。

5	🗾 タスク レポート	_ 🗆 ×
J		
	タスクの態度 隔離からの復元	
	ファイルフィルタ: ハッシュ: bec1b52d350d721c7e22a6d4bb0a92909893a3ae	
	通野旅: クライアント: Eset-svr / User-pc	
	- タスクの設定 - 名前(N) [隔離からの復元 	
		<u>.</u>
	□ タスクが正常に完了した場合、タスクを自動的に削除する(E)	
	戻る(B) 戻る(B) 終了(F) キャン	1211

ファイルの復元を開始します。[終了] ボタンをク リックし、復元を開始します。

※ESET Endpoint Security for AndroidおよびESET File Security for Linuxの隔離ファイルには対応しており ません。

1

2

3

4.5

ウイルス誤検出時の対応

FAQ

4.5.7 ウイルスとして検出されたファイルをウイルス検査対象から 除外する手順~クライアントPC編(Windowsの場合)

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、設定後は間違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、ESET Endpoint SecurityまたはESET Endpoint アンチウイルスでファイルの除外設定を行う手順を説明します。





[設定]、
 [詳細設定を表示する]をクリックします。

3	ESET Endpoint Security	? ×
	詳細設定	(CSCT)
	(編集在)	
	 (す) (t) (t)	既定(T)

 [コンピュータ] をダブルクリックし、
 [ウイルス・スパイウェア対策の設定] を ダブルクリックします。
 [パスによる除 外] をクリックし、
 [追加] ボタンをク リックします。



除外するファイルを選択します。●除外 するファイルを選択し、2[OK] ボタンを クリックします。



除外リストにファイルが登録されます。

>>> POINT

除外リストには、フォルダーやファイルの拡張子も登録できます。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。拡張子を登録するときは、[除外] 欄に [c:¥test¥*.doc]のような形式で入力します。

4.5.8 ウイルスとして検出されたファイルを検査対象から 除外する手順~クライアントPC編(Mac OS Xの場合)

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。

iness Edition 設定 ウイルス・スパイウェア対策 リアルタイムファイルシステム保護 ✓ 有効化
設定 ウイルス・スパイウェア対策 リアルタイムファイルシステム保護 ✓ 有効化
ウイルス・スパイウェア対策 リアルタイムファイルシステム保護 ✓ 有効化
リアルタイムファイルシステム保護 ✓ 有効化
アップデートするためのユーザー名とパスワードを入力する
プロキシサーバを設定する
すべての設定を既定値に戻す
アプリケーションの設定を入力する
(6

メインウィンドウを開き、詳細モードに 切り替えて、①[設定]ボタンをクリック し、②[アプリケーションの設定を入力す る]をクリックします。



【保護】ボタンをクリックし、2 [除外]
 をクリックします。3 [追加] ボタンをクリックします。

1





フォルダー一覧を表示します。[▶]をクリックします。

除外したいファイルを選択します。●除外したいファイル をクリックし、22[OK]ボタンをクリックします。



●選択したファイルが除外ファイルに登録されます。
 (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。 Chapter 1

Chapter 2

ウイルスとして検出されたファイルを検査対象から 除外する手順(Linuxの場合) 4.5.9

ここでは、ESET File Security for Linuxで指定したファイルを検査から除外する手順を説明します。



Webブラウザーを開き、Webインター フェースのページを開きます。

- [Configuration] をクリックし、
- ②[Scanner options]をクリックします。

Update options	Scanner options			
Scanner options	- Actions & Control		AV Targets	
Antispam options	Anti-Virus action	(scan)	Files	(yes)
Scheduler	On virus infected	(reject)	Archives	(yes)
Profiles	On virus not scanned	(accept)	E-mails	(yes)
DAC	On deleted	(discard)	Mailboxes	(no)
MIRD	Cleaning mode	(standard)	SFX archives	(yes)
PAC	Smart optimization	(yes)	Runtime packers	(yes)
wwwi	Querentine		AV Methods	
Apply shapped	Quarantine	(no)	Signatures	(yes)
Appry changes	Quarantine rescan	(yes)	Heuristics	(yes)
Porget changes			Advanced heuristics	(yes)
	Limits		Adware/Spyware/Riskware	(yes)
	Maximum object size	(0)	Potentially unsafe apps	(no)
	Maximum archive depth	(10)	Potentially unwanted apps	(no)
	Archive scanning fimeout			
	Active seaming amount	L (0)		
	Files	_		
	Extensions exclude	0		
	- Exclusions	0 2		
	Exclusions	/tmp/test.zip		

[Exclusions] にチェックを入れ、 外したいファイルをフルパスで入力しま す。③[Save Chages]をクリックします。

>>> POINT

/usr以下のすべてのファイルを除外したい場合は/ usr/*.*::、複数指定したい場合は/usr/*.*::/var/*.*:: と連続して入力してください。なお、オンデマンド スキャンで検査を除外したいファイルは、検査を 実行する時に[Control] →[On Demand Scan] の [Exclunde paths] で設定してください。

FAQ

1



[Apply changes] をクリックします。

Home Licenses C	onfiguration Control Help Logout	
Profiles DAC MIRD PAC WWWI Apply changes	Apply all changes?	
Forget changes	1	

[Yes]をクリックします。
FAQ

1

2

3

4.5

ウイルス誤検出時の対応

FAQ

4.5.10 ウイルスとして検出されたファイルを ウイルス検査対象から除外する手順~ ERA編

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ー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] を利用して一括配布します。

■ERACを起動し、ERASにログオンします。

2	🗾 接続 [Eset-svr] - Administrator - E	ESET Remote Ad	ministrator	Console		
	ファイル(F) 編集(E) アクション(A) 表示(V)	ツール(T) ヘルプ	?(H)			
	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	グループマネージ 通知マネージャ ポリシーマネージ	ジャ(G) (N) ジャ(P)	Ctrl+ Ctrl+ Ctrl+	·G ·T ·Shift+P] 💷 🔹 ナーバを追加する
	他のオブション 変更を適用(A) リセット(R)	ユーザマネージ+ ライセンスマネー	ァ(U) ジャ(L)	Ctrl+ Ctrl+	·M ·L	<u>クライアントを追け</u> : 議データベース(、 合が1つ前のバ
	□ チェックしたクライアントを表示 💌	ファイアウォールル ポリシールールウ	ルールマージウィ スィザード(C)…	ſザード(₩)		
	ロージ 静的グループ ローロ & ad-domain.example.com (ローロ & Computers (Active Dir	コンソールオプシ サーバオプション 監査ログビュー7	∃ン(O) (S) 7(A)	Ctrl+ Ctrl+	∙O Shift+O	
	Controllers (A Main Controllers (A Main Controllers (A Main Controllers (A	Web上のダッシュ	1ボード(こ移動)	D)	•	.情報: アイテム)全5ア
	WindowsOS (WindowsOS)	ESET <u>בעב</u>	レーションエディ	タ(E)		
	□ ○ ブライマリ管理サーバー	ESET SysInsp ESET SysRes	ector(I) cue(R)			Security Mi point Antivir
	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	📑 Eset-winxp	Eset-svr	ad-domain.e	ESET End	lpoint Securi
	□ □ □ 既定の親ポリシー	🕎 Kitagawa-no	Eset-svr	local	ESET NO	D32 Antivirus
	ー □ 💭 サーバポリシー (Eset-s	Ser-pc	Eset-svr	ad-domain.e	ESET End	lpoint Securi

ESET コンフィグレーションエディター を開きます。①[ツール]メニュー、② [ESET コンフィグレーションエディタ] をクリックします。

ון	※ ESETコンフィグレーションエディタ - 【タイトルなし】 ファイル(F) 編集(E) プロファイル(P) 表示(S) ヘルプ(H)	-	
וי	🗈 🏊 🔚 🔚 🔍 製品フィルタ: 📃		▼ Ut291
			マーク(M) マーク所研修(U) 既定(D) 法へ(N) 請定 名前: 除外 【規定: ○「師の可用目 (他(Y) 編集(E) 6)
	進備完了		Windowsデスクトップッ5

①設定を行いたいプログラムから②[カーネル (Mac OS X/Linuxの場合は [ESET デーモン])]、③[設定]、④[除外]と順に クリックしていき、最後に⑤[除外]をク リックし、⑥[編集]ボタンをクリックし ます。

>>> POINT

Windows用のESET Endpoint SecurityおよびESET Endpoint アンチウイルスの設定を行う場合は、[Windowsデスクトップv5] を選択してくだ さい。ESET File Security for Microsoft Windows Serverの設定を行う場合は、[Windows Server V4.5] を選択してください。Mac OS X用 のESET NOD32アンチウイルスの設定を行う場合は、[Unixデスクトップv4] を選択してください。ESET File Security for Linuxの設定を行う 場合は、[Unixサーバ V4]を選択してください。Windows用のESET Smart SecurityおよびESET NOD32アンチウイルスの設定を行う場合は、 [Windows製品ラインv3およびv4] を選択してください。



[除外] ダイアログが開きます。①[新規アイテム] 欄に除外したいファイルまたはフォルダーをフルパ スで直接入力し、②[追加] ボタンをクリックします。

POINT

除外リストへの登録は、フォルダーやファイルの拡張子も登録できます。フォルダーを除外するときは、「C:¥testdata¥*.*」のような形式で、 フルパスでフォルダー名を入力し、ファイル名を「*.*」とします。また、拡張子で指定する場合は、「c:¥testdata¥*.doc」のような形式で入力 します。



入力したファイルが登録されます。
 ②[OK]ボタンをクリックします。

CAUTION

[フォルダ]ボタンや[ファイル]ボタンをクリックすると、ダイアログを利用してファイルやフォルダーの指定が行えますが、このダイアログは、現 在操作しているコンピューター内のみを表示します。



Chapter 2

1

2

3

4.5

ウイルス 誤検 出時の 対応



7	🦧 名前を付けて保存	F. III					×
	保存する場所(1):	🌗 各種設定ファイノ	ŀ	•	🗿 🤌 📂 🖽 •		
		名前 -	 検索条件に-	▼ 更新日時 -致する項目はあ	▼ 種類 りません。	- サイズ	<u> • </u>
	取込まれのごあり デフカトップ						
	5-175U						
	גער בארביעב						
	マントワーク ネットワーク			0		2	
		ファイル名(N):	Endpoint用除外設定	-		保存(S)	
		ファイルの種類(T):	設定ファイル (*xml)		_	キャンセル	

設定ファイルを保存します。①ファイル 名を入力し、②[保存]ボタンをクリック します。

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

9 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]を利用して一括配布します。

[FAQ] よくある質問 お問い合わせの際に

質問事項一覧	150
お問い合わせの際に	168
環境設定ファイル(SysInspector)の情報(*.zip)の取得方法	169
Windows のシステム情報(*.txt)の取得方法	172
Mac OS X のシステム情報の取得方法	173
Mac OS X のコンソールメッセージの取得方法	175
Mac OS X のプロセス情報の取得方法	177
ESET 製品の設定ファイル(.xml)の取得方法	179
スクリーンショットの作成方法	190

質問事項一覧

番号	質問事項	参照ページ
01	ERAC上での時間の表示形式を変更するには?	152ページ
02	クライアントPCの設定をERASからリモートで変更するには?	152ページ
03	クライアントPCにアップデートを行わせるには?	153ページ
04	クライアントPCにコンピューターの検査を行わせるには?	153ページ
05	ERASのパスワードを変更するには?	153ページ
06	表示されるアイテムのフィルタリングを行うには?	154ページ
07	ERASで管理されていないコンピューターを検出するには?	155ページ
08	ウイルス定義データベースが最新でないクライアントのみを表示する には?	156ページ
09	画面表示の更新を停止するには?	158ページ
10	コマンドラインオプションについて	159ページ
11	複製が正常にできないのですが?	159ページ
12	[リモートイントール]ペインで検出されないコンピューターがあるの ですが?	159ページ
13	[最終ウイルス警告]に表示されている警告が消えないのですが?	160ページ
14	[最終イベント警告]に表示されている警告が消えないのですが?	160ページ
15	簡単にフィルタを利用する方法は?	161ページ
16	タスクがなかなか配布されないのですが?	161ページ
17	ERASとERACは同一のコンピューターにインストールする必要があ りますか?	161ページ
18	初めてERASへの接続時に入力するパスワードは何ですか?	162ページ
19	ERAS、ERACはインストール台数に制限がありますか?	162ページ
20	ERASを導入する際に利用するポート番号は?	162ページ
21	ウイルス定義データベースをUSBメモリーやCD-Rで配布するには?	163ページ

Chapter	1
---------	---

表示にするには?

22

23

24

Chapter 2

プログラムコンポーネントのミラーを作成するには?

Mac OS Xでのコンピューターの検査に時間がかかる

セキュリティ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

Chapter 4

FAG

165ページ

165ページ

167ページ

1
2
3

お問い合わせの際に	168ページ	
		1

Faq

4

151

01 ERAC上での時間の表示形式を変更するには?

時間の表示形式は、既定では [相対] であり、下図のように現在の時刻との差が表示されます。

<	アイテム情報: > 15 (5 アイテム)全5 7	? イテムアイテム中	」 表示モード(M):	カスタム表示モート	. .	
	製品名	製品バージ	リクエストされた	実際のポリシー名	最終接続	保護の状態
ie	ESET File Security Mi	4.5.12002	既定のプライマリ	既定のプライマリ	3分前	
e	ESET Endpoint Antivir	5.0.2122	既定のプライマリ	既定のプライマリ	1分前	
.e	ESET Endpoint Securi	5.0.2122	既定のプライマリ	既定のブライマリ	1分前	
	ESET NOD32 Antivirus	4.1.86	既定のプライマリ	既定のプライマリ	22秒前	
ie	ESET Endpoint Securi	5.0.2122	既定のプライマリ	既定のプライマリ	1分前	

ERAC上での時間の表示形式を変更するには、以下の操作を行います。

■ERACを起動し、ERASへログオンします。

2 [ツール] メニューから、[コンソールオプション] をクリックします。



[コンソールオプション] ダイアログが表示されますの で、[日付/時刻] タブをクリックします。 [絶対] [相対] [地域] から、表示形式を選択します。

02 クライアントPCの設定をERASからリモートで変更するには?

クライアントPCの設定をERASからリモートで変更するには、設定変更の対象となるクライアントPCに対して、[コン フィグレーション] タスクを割り当てます。

※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

03 クライアントPCにアップデートを行わせるには?

クライアントPCにアップデートを行わせるには、対象となるクライアントPCに対して、[今すぐアップデート]タスクを割り当てます。

※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

04 クライアントPCにコンピューターの検査を行わせるには?

クライアントPCにコンピューターの検査を行わせるには、対象となるクライアントに対して、[オンデマンドスキャン] または [オンデマンドスキャン (駆除無効)] タスクを割り当てます。

※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

05 ERASのパスワードを変更するには?

ERASのパスワードを変更するには、[サーバオプション]ダイアログの[セキュリティ]タブで設定を行います。 ※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

スサーバオプション[Eset-svr]	x
一般 セキュリティ サーバの保守 ログ 複製 アップデート その他の	の設定 詳細
パスワードの編集は、取り消すことはできません。パスワードはコンフ ルには保存されず、サーバに直接送信されます。	ィグレーションファイ
―― コンソールセキュリティ設定	
🥅 Windows/ドメイン認証を使用する(W)	
■ 他のドメインに所属しないWindows/ドメインユーザ(活売 み取りロールを使用する(U)	
ユーザマネージャー(M)	
サーバのセキュリティ設定	
クライアント(ESETセキュリティ製品)のパスワード	変更(A)
複製のパスワード	変更(H)
ESETJモートインストーラ(エージェント)のパスワード	変更(N)
✓ クライアントの非認証アクセスを有効にする(ESETセキュリティ製品)(L)	
 Face のチョン・ロークシェント・ラの非認証アクセスを有効にする (エージェント)() 	0
目前一日 「「「「「」」「「」」」「」」「」」「」」「」」「」」「」」」「」」」「」」	
注意:[既定値に戻す]ボタンは、パスワードには適用されません。	
OK(0)	キャンセル

2

FAQ

1

06 表示されるアイテムのフィルタリングを行うには?

[レポート] ペインと [リモートインストール] ペインを除く、各ペインに表示されるアイテムのフィルタリングを行うには、[フィルタ] 機能を有効にし、フィルタリング条件を指定します。フィルタリングの条件には、[共通フィルタ] と [ペイン固有フィルタ] が準備されています。共通フィルタでは、グループマネージャで作成したグループ単位でフィルタリングできるほか、[プライマリサーバ] や [クライアント] [コンピュータ名] [MACアドレス] などのクライアントの条件を指定したフィルタリングも行えます。

フィルタ機能を有効にする



フィルタ機能を有効にするには、[フィルタを使用する] にチェックを入れます。フィルタ機能を無効にする場合 は、チェックを外します。

グループを利用してフィルタリングする

x ah 🔉 💀 🐋 🗤 🗸						
e e e e e e e e e e e e e e e e e e e	·	• • • • •				
マフィルタを使用する(U) クライアント	すべてのサーバを対	縁にする	 チェック ON(C) 	チェック OFF(U) クライアントを追	<u>əl.l.a.</u>	
他のオプション 変更を適用(A) リセット(R)	サーバ名 🛆	25	ドアント	定義データベース	の状態	最も古いアクセス
クライアントフィルタ条件	🔲 🖷 Eset-svr	5		現在のバージョン		4分前
▼ チェックしたクライアントを表示 ▼						
- +24h W.s4						
日日 静的クルーフ						
Computers (Active Dir	•					
Domain Controllers (A				、マイテル特婦・		
	表示するアイテム	500	• << <	> 1.4 (4 7/7/.)247	レルタマイテム	アイ 表示モート
😑 😰 パラメータグループ	カライアント /	プライマリサー	1.158/12	製品名	製品バージー	/ 」 リクエストされた
WindowsOS (WindowsOS)	Eset-svr	Eset-svr	ad-domain.e	ESET File Security Mi	4.5.12002	既定のプライマ
·····································	📑 Eset-win 7-pc	Eset-svr	ad-domain.e	ESET Endpoint Antivir	5.0.2122	既定のプライマ
	😻 Eset-winxp	Eset-svr	ad-domain.e	ESET Endpoint Securi	5.0.2122	既定のプライマ
白 🗖 🔄 既定の親ポリシー	User-pc	Eset-svr	ad-domain.e	ESET Endpoint Securi	5.0.2122	既定のプライマ
■ りライアントのみ (フレーズ検索) 💌						
 クライアントのみ (フレーズ検索) プライマリサーバ(P): 						
□ クライアントのみ (フレーズ検索) ▼ プライマリサーバ(P): クライアント名(C):						
ううイアントのみ (フレーズ検索) ブライマリサーバ(P): クライアント名(C): アノドューダ系(Q):						
□ クライアントのみ (フレーズ検索) マ フライマリサーバ(P): クライアント名(C): コンピュータ名(O):						
□ 05イアントのみ・Cレーズ検索) マ ブライマリサーバ(P): クライアント名(C): コンピュータ名(O): MACPFトレス(M):						
□ からイアントのみ・クレーズ検索) ▼ カライマリサーバ(P): ケライアントを(C): ンピュータを(O): MACアドレス(M): 「問題のみます(M)」 (三年の)						
「 757(72)-K03k (72)ズ発生) ⊻ 757(72)+3√(9): 757(72)+54(0): コンピュータ43(0): ■ (問題のみ表示(Y) 座毛(C)) ■ (問題のみ表示(Y) 座毛(C))						

グループを利用してフィルタリングするには、以下の操 作を行います

● [フィルタを使用する] にチェックを入れ、フィルタ
 機能を有効にします。

②チェックボックスにチェックを入れます。

 ●表示したいグループにチェックを入れます。条件がす ぐに反映され、チェックを入れたグループのみが表示さ れます。

	Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ		
'トを 打	旨定した条件でフ	ィルタリングする)				

クライアン	トを指定した条件でフィルタリングする

クライアントPCを指定条件でフィルタリングするには、以下の操作を行います。

📝 接続 [Eset-svr] - Administrator - E	SET Remote Adm	ninistrat	or Console			
ファイル(F) 編集(E) アクション(A) 表示(V)	ツール(T) ヘルプ((H)				
🚺 🖑 🏈 📽 📽 🖡 🗙 🗙	- 🖾 🖪 👂		67 🗖 🗖 🗖	2	•	
アイルタを使用する(U) クライアント	すべてのサーバを対象	象にする	 チェック ON(C) 	チェック OFF(U) サーバを クライアン	<u>自加する(には?</u> <u>トを追加する</u>	
1回(0月7-2912) 変更を適用(A) リセット(R)	サーバ名 ム		クライアント	定義デー	タベースの状態	最も古いアクセス
クライアントフィルタ条件	🔲 🖣 Eset-svr		5	現在のバー	ージョン	4分前
▶ チェックしたクライアントを表示 ▼						
日上 静的グループ						
Computers (Active Dir	•					
	表示するアイテム (c)	500	• << <	> アイテム'情報: > 15 (5 アイテム	.)全5 フィルタア・	イテムアイ 表示モート
B-5 パラメータクループ	クライアント /	プライマリサ	L. 15342	製品名	製品バ	ージ リクエストされた
	📑 Eset-svr	Eset-svr	ad-domain.e	ESET File Securit	y Mi 4.5.120	.02 既定のプライマ
白ーシボリシー	📓 Eset-win7-pc	Eset-svr	ad-domain.e	ESET Endpoint Ar	itivir 5.0.212	.2 既定のプライ*
	Eset-winxp	Eset-svr	ad-domain.e	ESET Endpoint Se	curi 5.0.212	2 既定のプライマ
白-ロ標 既定の親ポリシー	Kitagawa-no	Eset-svr	local	ESET NOD32 Anti	virus 4.1.86	既定のフライマ
	Ser-pc	ESet-SVr	ad-domain.e	ESET Endpoint Se	curi 5.0.212	2 玩走のノフ1・
2						
▶ クライアントのみ (フレーズ検索)						
プライマリサーバ(P): eset-svr						
クライアント名(C):						
コンピュータ名(0):			-			
MACアドレス(M):						
□ 問題のみ表示(Y) / / / / / / / / / / / / / / / / / / /	_					
					1	
■ クライアント ● ウ ■ フ	<u> </u> € イ] © HI		デ [🍔 We]	◎迷 ◎グ] Q 検	. <u> </u> ∎ €]⊡ K
クライアン 客り	岐ログ ファイアウ イ・	ベント []	HIPSログ デバイス	Web制 J迷惑メー	·	検査ログ「モバイル…」

[フィルタを使用する] にチェックを入れ、フィルタ機 能有効にします。

1

2

3

FAQ

②チェックボックスにチェックを入れ、フィルタリング の方法を設定します。

⑧ [プライマリサーバ] [クライアント] [コンピュータ名] [MACアドレス] の各エディットボックスにフィルタリ ング条件を入力します。複数のエディットボックスに入 力した場合、すべての条件にあてはまるアイテムを表示 します。

④ [変更を適用] ボタンをクリックします。

07 ERASで管理されていないコンピューターを検出するには?

ERASに接続していないコンピューターや、ESET セキュリティ製品がインストールされていないコンピューターを検 出するには、以下の操作を行います。

ERACを起動し、ERASへログオンします。

7 接続 [Eset-svr] - Administrator - ファイル(F) 編集(E) アクション(A) 表示(ESET Remote Admi v) ツール(T) ヘルプ(ト	inistrator Console ()				💵 🌒 [リモートインストール] タブをクリック
🧉 👉 🥌 📽 📽 🖡 🔀 🗙	× 🖻 🖪 🖻	🛯 🕼 🗖 🚍		- 😃		
・検索タスク - 総索タスク - - - - - - - - - - - - -	コンピュータ インス	~-N920				
0	<u>コンピュータ名</u> ■ Mac-air	 コンピュータドメイン Ad=domain.exa 	IPv4 192.168.1.19	IPv6	コンピュータのOS	
#28-00028 + 15						2 [既定の検査タスク]をクリックします。
東行 新規検索 検索結果フィルター 4						
□ □ □ Active Directory検索 □ □ ◎ MNet検索						3 [未登録のコンピュータのみを表示] に
						チェックを入れます。
						● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
✓ 未登録のコンピュータのみを表示(U) 最終アクセス警告のあるクライアント	3					
(W) 展視されたコンピュータを非表					-	2

3 登録されていないコンピューターが [リモートインストール] ペインに表示されます。



[クライアント]ペインで、ウイルス定義データベースが最新でないクライアントのみを表示するには、以下の操作を行います。



] ERACを起動し、ERASへログオンします。

2 [クライアント] タブをクリックします。

→ →	🧉 👉 可 📽 📽 😰 🗙	× 🖾 🖪 🖗		47 🗖 🗖	🗆 💌	•	•					
Card 2010 (1995年) Card 2010 (1995 (1995) (1995) Card 2010 (1995 (1995) (1995) (1995) Card 2010 (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995 (1995) (1995) (1995 (1995) (1995 (1995) (1995) (1995 (1995) (1995 (1995) (1995 (1995) (1995) (1995 (1995) (1995 (1995) (1995 (1995) (1995) (1995 (1995) (1995 (1995) (1995 (1995) (1995 (1995) (1995) (1995 (1995) (1995 (1995) (1995 (1995) (1995) (1995 (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (1995) (1995) (1995 (□ フィルタを使用する(U) クライアン	すべてのサーバをす	なにする	• FI9	7 チェック OFF(U)	25172	自加するには トを追加する	<u>t2</u> 5				
	1000才752m2 安地を延用(A) リセット(R)	サーバ名 /		クライアント		定義デー	マベースの状	102	最も古いアクセス		最終會威警告	最終ファイン
■ ■	クライアントフィルタ条件	U W Eset-sw		5		数台かり	明のハージョ	32 3	20月18日16月		U	U
● ●	▶ チェックしたクライアントを表示 下											
	□-● 静的グループ											_
	ad-domain.example.com (ad-domain.example.com (•									1	
● # 355 (#1235-7) ● > 1.5 (#74/24)(#574/24)(#74/2	- 🗖 🛐 Domain Controllers (A	表示するアイテル			1 174	テム情報:				- Leen	_	
	□ □ ▶ 本社G (本社グループ)	(0)	500	<	< > 1	5 (5 アイテム)全5 アイテ.	ムアイテムロ	p 表示モード()	n: カスタム	表示モード 🔟	
	WindowsOS (WindowsOS)	クライアント /	7517	ドメイン	製品名	劉品/に	リクエス。	実際のポ	り最終措統	保. 白イ	117 完善デーカペー7	最終雪 感警告 :
Compared State S		Eset-win7-pc	Eset-s.	ad-domain	ESET End.	5.0.2122	既定の	現定のブ	フー 420 mg ラ. 55秒前	732	3 (C TAXT BEIRIA)	
	□	Eset-winxp	Eset-s.	ad-domain	ESET End	5.0.2122	既定の	既定のブ	う 2時間前	732	2(: 参照して選択(B)	47(D
Control (19) - Garder	□ □ □ 既定の親ポリシー	Kitagawanno	Eset-s.	local ad demain	ESET NO	4.1.86	既定の	既定のプ	58秒前	732	3(: 選択アイテムを非	表示(H) 🛃
	ーロ日 サーバボリシー (Eset-s	Ser-pc	E38(~8.	au-oomain	ESET ENU	0.0.2122	ADEU.	KAJE007	J. 175 NU	102	312 選択アイテムのみ	表示(U)
											新規タス5(T)	-
											このジライアントの 情報を削除(C)	τ−9(F)
											フラグをセット/リセ	5/F(S)
											データのリクエスト	(E)
	レクションシャンシャンション マレージを使う マ										グループに注意力の(の	0
	w- (milt 17m) and an										リモートインストー	7 16(D
2017-07-06-07-07-07-07-07-07-07-07-07-07-07-07-07-	794 899 W/WP: Jeserson										ファイアウォールル	ールマージウィザード
	054 PDF86(c):										カラムの表示/非	表示(N)_
MACFF23(9): 第100-100 (100-100) (10	1061-996(0):										南川島約(D)	
「 「 (2015)(次示(1) 「 (2015)(次示(1) 「 (2015)(次示(1) 「 (2015)(次示(1) 「 (2015)(次示(1) 「 (2015)(次示(1) 「 (2015)(次示(1) 」 (2015)(2015	MACPIFU2.(M):										おりっ(1)	
Systemeter(Y) Type: Systemeter(Y)	図 問題の決決示(Y) 原案(D)										5馬馬線(Q)	
		• [1						Sysinspector(Y)	(0)

●最新のウイルス定義データベースを利用しているクライアントの[ウイルス定義データベース]欄を右クリックして、
 2[参照して選択]をクリックします。

●再度右クリックして、 2 [選択アイテムを非表示]をクリックします。



Chapter 1 Chapter 2 Cha	pter 3 Chapter 4	FAQ

5 ダイアログが表示されます。[OK] ボタンをクリックします。

 ディルタを使用する(U) 	× 🖾 🔂 🖗 Þ 🛛 🕸	「象にする」	• 1 19: • 19:		EE 40 1 <u>サーバを</u> 25イアン	・ <u>創加する(2()</u> トを追加する	<u>12</u>				
他のオブション 変更を適用(A) リセット(R)	サーバ名 🔺		クライアント		定義デー	マースの状	態	最も古いアクセス		最終會威警告	最終77/
クライアントフィルタ条件	u a Eset-sw		5		報告から	間のハーン	עב	243181101		U	0
ナエシクしたクライアントを表示 /											
□-※ 静的グループ □-□ ※ ad-domain.example.com (
Computers (Active Dir	•				<u> </u>						
	表示するアイテム	500	• <<	< > 71	テム情報: 8アイテムの3	もまティーマ	(74)	表示モード(M): 力2	、タム表示モード <u>●</u>	I
ロージ パラメータグループ	クライアント △	17517-	FX12	製品名	製品バ	19512.	実际のオ	り_ 最終接続	保	ウイルス定義データペース	、 最終脅威警告
ジライマリ管理サーバー	Eset-winxp	Eset-s	ad-domain	ESET End	5.0.2122	既定の	既定のこ	75. 2時間前		7322 (20120723)	-
□・○ ポリシー し□□ 四字のプライフリカライアン											
□-□□ 既定の親ポリシー											
ーーロション サーバボリシー (Eset-s											
▶ りライアントのみ (フレーズ検索) ▶											
プライマリサーバ(P): eset-svr											
クライアント名(C):											
コンピュータ名(0):											
MACアドレス(M):											
■ 問題のみ表示(Y) 編集(D)	1										

ウイルス定義データベースが最新でない
クライアントのみが表示されます。

2 3 4

FAQ

1

POINT

表示をもとに戻すときは、[表示]メニューの「選択アイテムのみ表示]をクリックするか、[更新]ボタンをクリックします。キーボードの[F5] キーを押すことでも表示をもとに戻せます。

09 画面表示の更新を停止するには?

画面表示の更新を停止するには、以下の操作を行います。

ERACを起動し、ERASへログオンします。

7	🛛 接続 [Eset-svr] - Administrator - E	SET Remote Ad	ministrator	Console					
	フィイル(F) 編集(E) アクション(A) 表示1 ● ● ● ● ● ● ● ● ● ● ● × × ワンルなを使用する(U) クライアント ● クイアントフィルな条件 F 3120にたりライアントを表示	ツール(T) ヘルス クループマネージ 通知マネージャ ポリシーマネージ ユーザマネージ ライセンスマネー ファイアウォール ポリシールールが	(H) N) ヤ(P) ヤ(P) ジャ(L) ジャ(L) レールマージウ. レールマージウ.	Ctri Ctri Ctri Ctri イザード(W)	+G +T +Shift+P +M +L	〕 ・ ナーバを追加す フライアントを追 議データベース 見在のバージョン	<u>るには?</u> <u>加する</u> の状態	最も古いアクセス 85分前	
	 ● ● ●●●○ / ●○ / ●○ / ●○ / ●○ / ●○ / ●○	コンソールオプション サーバオプション 整査ログビュー7 Web上のダッシュ ESET コンフィグ ESET SysInsp ESET SysInsp	ョン(O) (S) ?ー(A) !ボードに移動 レーションエデ- ector(I) :ue(R)	Ctri Ctri (D) (ð(E)	+0 +Shift+0	,情報: アイテム)全57 Security Mi point Antivir	² イテムアイテム 製品バージ 4.5.12002 5.0.2122	ー中 表示モード(M) - 「リクエストされた 既定のプライマリ 既定のプライマリ	: 加 実際 () () () () () () () () () ()
	□ 日 既定のガライマリクライアン1 □ □ □ 既定の規ポリシー □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	😻 Eset-winxp 😻 Kitagawa-no 😴 User-pc	Eset-svr Eset-svr Eset-svr	ad-domaine local ad-domaine	ESET End ESET NO ESET End	lpoint Securi D32 Antivirus Ipoint Securi	5.0.2122 4.1.86 5.0.2122	既定のプライマリ 既定のプライマリ 既定のプライマリ	既定既定

● [ツール] メニューをクリックし、 ② [コ ンソールオプション]をクリックします。

2	スコンソールオプション	×
U	接続 カラム - 表示/非表示 配色 パス 日付/時刻 その他の設定	
	①	
	フィルク設定	
	✓ 変更を自動的に適用する(T) 有効にした場合、「フィルタ」ペインのサーバ / クライアント名を除くすべての設定が、変更され、次第、自動的に適用されます。	
	Remote Administratorのアップデート	
	アップデートの確認(F) 毎月 💌	
	前回の確認 4日前	
	次回の確認予定 2012/08/21 2:27:40	
	オブション情報メ	
	✓ クリットフインを表示する(G) 反 カライア・ホキ「サード/フ・ポュータ/MAC Iで(けか/ 「サード/名前」でまデオス(D)	
	▼ タスクトレイ アイコンを表示する(Y)	
	▼ 最小化時にタスクバーに表示する(W)	
	□ 問題のあるクライアントが存在する場合、ハイライトされたタスクトレイ アイ コンを使用する(B)	
	その他の設定 すべて表示(N) すべて非表示(S)	
	<u>3</u>	
	OK(O) キャンセル	

● [その他の設定] タブをクリックし、 2 [自動更新 を使用する(分)]のチェックを外します。 3 [OK] ボ タンをクリックします。

2

FAQ

1

10 コマンドラインオプションについて

Windows用プログラムのインストールパッケージは、作成の際にさまざまなコマンドラインオプションを指定できます。詳細については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

11 複製が正常にできないのですが?

複製がうまくいかない場合、以下の項目をご確認ください。

- ●下位サーバーは上位サーバーが指定したポート番号(既定値は「2846」)へ接続できる必要があります。
- ●上位サーバーが下位サーバーを指定する際は、「IPアドレス」ではなく「コンピューター名」によって指定する必要があります。
- ●管理情報の複製は、下位サーバーが上位サーバーへ接続した際に実行されます。複製が行われるまでに時間がかかる ことがあります。
- ●上位サーバーから下位サーバー配下のクライアントPCへタスクを発行した場合、下位サーバーが上位サーバーへ接続 した時点で実際のタスクが発行されます。このため、クライアントPCがタスクを受け取るまでに時間がかかることが あります。

12 [リモートイントール]ペインで検出されないコンピューターがあ るのですが?

検出には、NetBIOSを利用します。[リモートイントール] ペインで検出することができるコンピューターには、 Windowsがファイル共有時に利用する [Microsoftネットワーク用ファイルとプリンター共有] や [Microsoftネット ワーク用クライアント] などの機能がインストールされている必要があります。

13 [最終ウイルス警告]に表示されている警告が消えないのですが?

[最終ウイルス警告]には、クライアントPCが最後に検出したウイルスの名称が表示されますが、クライアントPC側で ウイルスの駆除、または削除を行っても[最終ウイルス警告]に表示されている警告は消えません。[最終ウイルス警告] に表示されている警告を消すには、以下の操作を行います。

[最終ウイルス警告]欄に表示されている文字を消したいクライアントPCを右クリックします。



表示されるコンテキストメニューから [情報を削除]をクリックし、2["最終脅 威警告"情報を削除]をクリックします。

14 [最終イベント警告]に表示されている警告が消えないのですが?

[最終イベント警告]に表示されている警告を消すには、以下の操作を行います。

[最終イベント警告]に表示されている文字を消したいクライアントPCを右クリックします。

□ フィルタを使用する(U) クライアント	すべてのサーバオ	注対象にする	▼ ³ / ₂	(ック) チェッ	ク サーバ	を追加する	12(22)					
他のオブション 使更を抽用(A) リセット(R) ゆライアントフィルタ条件	サーバ名 A	r	0		0) 定義デ 現在の	ータベースの バージョン)状態 :	最も古いアクセ 8時間前	2		最終脅威警告 1	
「 チェックしたクライアントを表示 ▼ 「 チェックしたクライアントを表示 ▼ 日・● 静的グループ 日・● 読 ad-domain.example.com (日・● 読 Computers (Active Dir 日 ● Dir Computers (Active Dir 日 ● Dir Dir Constraintse (A	•											
	表示するアイテム (O)	500	• <	< < >	アイテム情報 15 (5 アイ・	: テム)全5 アイ	(テムアイテムロ	p 表示モー	F(M):	カスタム	表示モード	•
□····································	051P △	プライマ		製品名	製品バ	U012.	実際のポリ	最終接続	保.	ウイルー	最終脅威警告	最終
	Eset-svr	Eset-s	ad-domain	ESET File	4.5.12002	既定の	既定のプラ.	3分前		7322	W. 00 /t	1123
白 ※ ポリシー	Eset-win7	Eset-s	ad-domain	ESET End.	5.0.2122	既定の	既定のプラ.	56分前		7322	winoz/install	4123
 一日 医 以定のフライマリクライアンド 自一日 医 研究の根 ボバッー 	😻 Kitagawa	Eset-s	local	ESET NO	4.1.86	既定の	既定のプラ.	2時間前		7322		
L 日見サーバポリシー (Eset-s	User-pc	Eset-s	ad-domain	すべて選択 参照して選 選択アイティ 選択アイティ 選択アイティ	(A) 択(B) ムの反転(D) ムを非表示(I) ムのみ表示(I	H) J)	C#+ C#+ C#+	A 980 L H U		7322		
				新規タスク(T)			•				
【 クライアントのみ (フレーズ検索) <u>・</u> ライマリサーバ(P): eset-svr ライアント名(C):			0	このクライア 情報を削除 フラクをセット データのリク	ントのデータ(X(C) トバリセット(S) エスト(E)	F)		1日 1日 1日 1日	8音成音 87ァイア 8イベン	8告"情報 2013年一日 ト警告"情	日を計(15余(17) 1925年 - (吉本日を計(15) 青華服を許(15余(15)	K(F)
コンピュータ名(0):	L			グループに逃	自力D(G)			2 tak	●検査」	情報的のの	リア(L) たお(Re(A)	_
MACPFL2(M):				ポリシーの影	健定(P)			- +7.5		* 50.77/1	0	
-				ファイアウォー	-ルルールマ・	ージウィザー	F(W)	1000	LAIRES	8997 M	,,	
[[]]題()が表示(Y)				カラムの表示	示/非表示(N	I)						
			1.	前順余(D)			Del		- PT 4	.	6 I.I.	1.0
	<u></u> 1 [6	mu. I	≥ ⊤ [8	ポリシー(L)							× [h V	
				a second s				10112 / 11			I DOMENTIAN	

表示されるコンテキストメニューから [情報を削除]をクリックし、2["最終イ ベント警告"情報を削除]を選択します。

¹

[クライアント]ペインに表示される [最終ウイルス警告] [最終ファイアウォール警告] [最終イベント警告] などのカラ ムは、フィルタに利用できます。この機能を利用すると、特定のクライアントPCの指定カラムに関連するログ情報のみ を表示することができます。たとえば、特定のクライアントPCの [最終ウイルス警告] に関するログ情報のみを表示し たいときは、そのクライアントPCの [最終ウイルス警告] カラムをダブルクリックします。

対を使用する(U) クライアント	すべてのサーバを対	像にする	 Ť1% ON(C) 	2 チェック OFF600	<u>サーバを注</u> クライアン	自動する(計) トを追加す	<u>12</u> 3							
(点) 表更を適用(A) リセット(R)	サーバ名 🔺		クライアント		定義デーク	ベースの状	38	最も古い:	アクセス		最終會	威警告		最終75
ットフィルタ条件	Eset-svr		5		現在のパー	・ジョン		2時間前			1			0
っちしたクライアントを表示														
お伯ヴルーフ	-													
- ad-domain.example.com (
- 🗖 🛐 Computers (Active Dir	•													
Domain Controllers (A 本社G (本社グループ)	表示するアイテム	500	• <<	< > 71	テム情報:		17/-1	由 表示	SE-KM	: <u>カスタ</u>	し表示モー	-K 💌		
パラメータグループ	(0) /	75/2	18840	915.4	81815	1±3717	1 3882/0	en lass	81925	12 104	山田和	-0.000C	1.00.00	1994.
WindowsOS (WindowsOS)	Eset-svr	Eset-s	ad-domain	ESET File.	4.5.12002	既定の	現定の	75. 25	Ħ	732	2 -	Hongo	1 400. 140	merce
■ 21 フラ1マツ管理サーバー 劇品に	😂 Eset-win7-pc	Eset-s	ad-domain	ESET End.	5.0.2122	既定の	現金の	75. 19	前	732	2 _ Wini	12/install_	45分前	
■ 既定のブライマリクライアント	Set-wirep	Eset-s	ad+domain	ESET End.	5.0.2122	既定の	既定の	75 1時	間約	732	2			
既定の現状パシー	Kitagamanno	Eset-s	local	ESET NO	4.1.86	既定の	既定の	75 284	間約	732	2 _			
サーバボリシー (Eset s	User-pc	Eset-s	ad+domain	ESET End.	5.0.2122	既定の…	既定の	75. 45	沙前	732	2			
100000000														
いんのみ パリー・ディー 水の水い														
/S/P): eset-svr														
:):														
	-													
(80):														
attens letters 1														
ATTROTICT) NEW (D)														

 $\mathbf{\nabla}$

フィルタリングして表示したいクライアントPCのカラム 欄(ここでは、[Eset-win7-pc]の[最終ウイルス警告]) をクリックすると、[ウイルスログ]ペインに、選択した クライアントPCのログ情報のみが表示されます。

FAQ

1

2

3

ファイル(F) 編集(E) アクション(A) 表示(V) ツール(T) ヘル	dministrator Co J(H)	nsole						
🥳 🖑 🏈 📽 📽 😰 🗙 🕽	(📾 🔂 (è 🔲 49 🖸		. 🛄 🗉					
マ フィルタを使用する(U) 脅破ログ	すべてのサーバを	対象にする 💽	チェック ON(C) 0FF(U)	サーバを追加 クライアントを注	<u>#300(\$2</u> 8)10(\$3				
他のオフション 王正を適用(A) リセット(R)	サーバ名 🛆	0541	P21	定義データベー	スの状態	最も古いアクセス	最終會威警告	1	最終ファイ、
クライアントフィルタ条件	Eset-svr	5		現在のバージョ	2	2時間前	1		0
■ 「チェックしたクライアントを表示 💌									
□-● 靜的ガループ ▲									
🖻 – 🛄 🤮 ad-domain.example.cc									
Computers (Active 💌	•								•
マ クライアントのみ (フレーズ株式) マ	表示するアイテム (0)	200 •	最近7日間 ▼	<< >	アイテム情報	: 」、 全3 フィルタアイテム中、1	数近7日間で		
	骨膜ID で	クライアント名	プライマリサーバ	受信日	第生日	1.000	スキャナー	オブジェクト	18
J54 VUT=/VP): Eset-sw		Eset-win7-pc	Eset-svr	44分前	46分前	重大な警告	リアルタイムファイー	7711	0.
クライアント名(C): Eset-win7-pc	④ 常板158	Eset-win7-pc	Esethsyr	44分前	46分前	重大な警告	リアルタイムファイニ	7711	C:
コンピュータ名(O): Eset-win7-pc	曾殿167	Eset-win7-pc	Eset-svr	44分前	47分前	重大な智告	リアルタイムファイー	7711	0.5
MACアドレス(M): 6cf04954fd59									
「食感ログのレベル	-								
レベル4・レベル3+診断									
IFM									
■ 骨板のみ (フレーズ検索) ■									
骨戚:									
□ オンデマンドスキャナログなし	-								
骨板ログの日付									
日時フィルタを使 条(生物定(の)									
一 用42(D)									
	•								
🖉 ク 😝 ウイルスログ 😫 フ	010	H ●デ	┃ # We ◎ 递	0 5	오検	◎モ □ 隔離 ▶	タ hレ	o y	
クライアンド 香	破ログ ファイアウ	KANNE HIPSE	17 デバス. Web本	御. 迷惑メー	グレーリス、 オ	11日の「もうり」、「開握」	タスク レポート リモート・	T	机械

16 タスクがなかなか配布されないのですが?

クライアントに対して発行したタスクは、クライアントがERASへ接続した際にクライアントへ配布されます。クライアントがERASへ接続するまで、タスクは配布されません。

17 ERASとERACは同一のコンピューターにインストールする必要 がありますか?

必要ありません。ERASとERACは、異なるコンピューターにインストールしても運用できます。ただし、ERASをイン ストールしたコンピューターでERAメンテナンスツールを利用する際には、ERASとERACは同一のコンピューターに インストール必要があります。

18 初めてERASへの接続時に入力するパスワードは何ですか?

既定の状態では、ERASにはパスワードが設定されていませんので、[パスワード]ダイアログには何も入力せずに[OK] ボタンをクリックしてください。

19 ERAS、ERACはインストール台数に制限がありますか?

ERAS、ERAC共に特に制限は設けておりませんので、必要な台数分インストールしてください。

20 ERASを導入する際に利用するポート番号は?

ERASを導入した環境で利用されるポートは、以下の通りです。

プロトコル	ポート番号	用途
	2221	クライアント PC がミラーサーバーへ接続するときに参照
	2222	クライアント PC が ERAS へ接続するときに参照
TCP	2223	ERAC が ERAS へ接続するときに参照
	2224	クライアント PC が ERAS へ接続するときに参照
	2225	ダッシュボートサーバー
2846 管理サーバー(ERAS)を複数設置した 位の管理サーバー(ERAS)へ接続する		管理サーバー(ERAS)を複数設置した場合に、下位の管理サーバー(ERAS)から上 位の管理サーバー(ERAS)へ接続するときに参照

また、プッシュインストール時には、ERASから、インストール対象となるクライアントPCの以下のポートに対して通 信できる必要があります。

プロトコル	ポート番号
TCP,UDP	137
UDP	138
TCP	139
TCP,UDP	445

21 ウイルス定義データベースをUSBメモリーやCD-Rで配布する には?

ウイルス定義データベースをUSBメモリーやCD-Rを利用して、クライアントPCに配布する方法は、以下の2通りが あります。それぞれ以下の手順で作業します。なお、この方法でウイルス定義データベースのアップデートが行えるの は、Windows用のセキュリティプログラムのみです。ESET NOD32アンチウイルス Mac OS X用およびESET File Security for Linux、ESET Endpoint Security for Androidは、この方法でのウイルス定義データベースのアップデー トに対応していません。

●ユーザーズサイトからダウンロードしたファイルを利用

●ミラーサーバーに保存されたファイルを利用

ユーザーズサイトからダウンロードしたファイルを利用

弊社ユーザーズサイトにて、ウイルス定義データベースをダウンロードし、ダウンロードしたファイルをUSBメモリーやCD-Rに書き込んで利用します。ダウンロード方法、およびファイルの利用手順については、ユーザーズサイトの「オフライン更新手順書」をご参照ください。

CAUTION

弊社ユーザーズサイトへログインするには、有効な「シリアル番号」および「ユーザー名」が必要です。

ミラーサーバーに保存されたファイルを利用

ミラーサーバーに保存されたファイルを利用する場合は、ミラーサーバーを構築し、最新のウイルス定義データベー スをダウンロードする必要があります。ミラーサーバーは、ESET Remote Administrator (ERA) またはESET File Security for Microsoft Windows ServerおよびESET Endpoint アンチウイルス、ESET File Security for Linuxで 構築できます。ミラーサーバーの構築手順については、各プログラムのユーザーズマニュアルをご参照ください。

- 1.ウイルス定義データベースのアップデートを行います。ウイルス定義データベースのアップデート方法については、 各プログラムのユーザーズマニュアルをご参照ください。
- 2.ウイルス定義データベースが保存されたフォルダーをUSBメモリーやCD-Rなどに書き込みます。既定値では、以下 フォルダーにウイルス定義データベースが保存されています。

●ERAの場合

Windows Server 2003/2003 R2の場合

C: ¥Documents and Settings ¥All Users ¥Application Data ¥ESET ¥ESET Remote Administrator ¥Server ¥ Mirror

Windows Server 2008/2008 R2の場合 C: ¥ProgramData ¥ESET ¥ESET Remote Administrator ¥Server ¥mirror

Windows Server 2012 Standardの場合 C: ¥ProgramData ¥ESET ¥ESET Remote Administrator ¥Server ¥mirror

●ESET File Security for Microsoft Windows ServerおよびESET Endpoint アンチウイルスの場合 ミラーサーバー構築時に指定した [配布用ファイルの保存先] フォルダーをUSBメモリーやCD-Rに書き込みます。

163

FAQ

1

2

3

●ESET File Security for Linuxの場合

/var/opt/eset/esets/lib/mirror

詳細設定	? ×
アップデートモード HTTPプロキシ LAN ミラー	
▼ 配布用アップデートを作成する(M)	
アップデートファイルへのアクセス	
■ 「小廠のFITPリーハよリアックテートファイルを提供する(F) 詳細調定しい… 配布用ファイルの保存先(F):	-
C#ProgramData¥ESET¥ESET File Security¥mirror フォルダ(L)	
ユーザー名(U): パスワード(P):	
77/14	
利用可能なハージョン(A):	-
OK(0) キャンセ	ι(C)

画面はESET File Security for Microsoft Windows Serverの場合。ESET Endpoint アンチウイルスも同じ画面で[配 布用ファイルの保存先] フォルダーを確認できます。

クライアントPCの設定

■ Windows用プログラムのユーザーズマニュアルを参考に基本画面を開き、詳細設定画面または設定画面を開きます。

2 [アップデートサーバ] の設定を行います。Windows用プログラムのユーザーズマニュアルを参考に設定画面を開き、「編集」ボタンをクリックします。

3 [アップデートサーバ] に、●USBメモリーやCD-Rの「mirror」フォルダのパス (例: D: ¥mirror)を入力し、❷「追加」 ボタンをクリックします。 ③「OK」ボタンをクリックします。

アップデートサーバリスト	? x
アップデートサーバ(U): 1	
d:¥mirror	
アップデートサーバリスト	
	追加(A) 2
	削除(R)
	編集(E)
<u> </u>	
ОК(О)	キャンセル(C)
OK(0)	キャンセル(C)

[**4**] [アップデートサーバ] ドロップダウンメニューより、手順3で設定したフォルダパスを選択し、「OK」ボタンをク リックします。

5 アップデートを実行します。

22 プログラムコンポーネントのミラーを作成するには?

ミラーサーバーにプログラムコンポーネントを保存する場合の設定は、ERASおよびESET Endpoint Securityまたは ESET Endpoint アンチウイルスのユーザーズマニュアルをご参照ください。ただし、製品の新しいバージョンが公開 されても、必ずしもコンポーネントアップデートが行われるわけではありません。その場合は、アップデート用のプロ グラムコンポーネントは表示されません。また、この機能はWindows用プログラムのみで利用できます。

23 セキュリティプログラムの起動時に表示されるスプラッシュ画面 を非表示にするには?

セキュリティ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。

Windows用プログラムの設定を直接変更する場合

] ESET Endpoint SecurityまたはESET Endpoint アンチウイルスのメイン画面を開きます。 [設定] をクリックし、[詳細設定を表示する] をクリックします。

2	SET Endpoint Security	(C)
	エンピュータ ネットワーク Webとメール アップテート マッン・ マッション・ マー・ マッション・ マー・ マッション・ マー・ マッション・ マー・ マッション・ マー・ マッション・ マー・ マッション・ マー・ マッション・ マー・ マッション・ マー・	ユーザーインタフェース ユーザーインタフェース要素 ■ グラフィカルユーザーインタフェース(G) ② 「P 基礎特に入了シウンコ画面を表示する(r)) ③ アクティフなコントロール要素を選択状態にする(k) 効果 ③ アクティフなコントロールを使用する(c) 速度(P)
•		 く

[ユーザーインタフェース]をダブルクリックし、
 [グラフィックス]をクリックします。③[起動時にスプラッシュ画面を表示する]のチェックを外します。④[OK]ボタンをクリックします。

1

2





ESET コンフィグレーションエディターを利 行いたいクライアント用プログラム(ここでは [Windowsデスクトップv5])をクリックし、 2 [カーネル] →3 [設定] →4 [ユーザインタ フェースの既定値] とクリックして開き、 6 [起 動時にスプラッシュ画面を表示する] で6 [値] のチェックを外し、7[ユーザーの設定を無視 する]も同様に「値]のチェックを外します。

POINT

Windows用のESET Endpoint SecurityおよびESET Endpoint アンチウイルスの設定を行う場合は、「Windowsデスクトップv5」を選択して上 記の手順で作業します。 ESET File Security for Microsoft Windows Serverの設定を行う場合は、「Windows Server V4.5」を選択し、 [File Security 4.5 for MS Windows Server] → [一般設定] → [ユーザインターフェース] → [ユーザインターフェースの既定値] とダブルクリックして設定 を行います。また、Windows用のESET Smart SecurityおよびESET NOD32アンチウイルスの設定を行う場合は、「Windows製品ラインv3お よびv4]を選択して設定を行います。なお、Mac OS X用プログラムは、ESET コンフィグレーションエディターで起動時に表示されるスプラッ シュ画面の非表示を設定することはできません。

Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ
1	•	1	1	

Mac OS X用プログラムの設定を直接変更する場合

000

 \checkmark

X

保護 アップデート ツール

? 既定

R

Ö

その他

ユーザーインタフェースを最適な状態に調整すると、これまで以上に簡単にかつ便利な方法でESET NOD32 Antivirusのアクセスと制御が行えるようになります。ユーザーインタフェース設定は、ユーザーごとに独自で…

2

✔ 保護の状態	設定	
● コンピュータの検査	ウイルス・スパイウェア対策	
マップデート (1)	リアルタイムファイルシステム保護 ✓ 有効化	
i de	アップデートするためのユーザー名とパスワードを入力する	
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	プロキシサーバを設定する	
200	設定のインポート/エクスポート	
× 9-1	すべての設定を既定値に戻す	
7 NUT	アプリケーションの設定を入力する	
•		

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、2[アプリケーションの設定を入力
する]をクリックします。

1

2

3

4

FAQ

ユーザー 2 インタフェース 警告と通知 権限 コンテキストメニュー グラフィカルインタフェース: 🗹 詳細モード クリックします。 3 起動時にスプラッシュウィンドウを表示する アプリケーションをドックに表示する 標準メニューを使用する: □ 標準モードで □ 詳細モードで ✓ ツールヒントを表示 □ 隠しファイルを表示する

4

OK

● [ユーザー] ボタンをクリックし、 ② [イ ンタフェース]をクリックします。3[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、4 [OK] ボタンを

Mac OS Xでのコンピューターの検査に時間がかかる 24

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。

キャンセル

お問い合わせの際に

弊社では、お客さま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(Windowsの場合)

取得情報	含まれている情報	取得する目的	参照ページ
環境設定ファイル (ESET SysInspector)	端末にインストールされているアプリケー ションや、読み込まれているドライバーの情 報、レジストリ情報などが含まれています。	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。また、レジ ストリ情報からウイルスの有無などを確認す るために取得します。	169ページ
Windowsのシステム情報	端末にインストールされているアプリケー ションやサービスの情報、PC 機器の情報な どが含まれています。	ネットワークドライバーの詳細なバージョン や、Windows のエラー報告などを確認する ために取得します。	172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。	179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。	190 ページ

●取得をお願いする情報の例 (Mac OS Xの場合)

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。	173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。	175 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。	177 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。	181 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。	191 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。

1

2

3

4

FAQ

環境設定ファイル (SysInspector)の情報 (*.zip)の取得方法

SysInspectorの情報は、情報を取得したいコンピューターを直接操作して取得する方法とESET Remote Administrator Console (ERAC)を利用してリモート操作で取得する方法があります。

コンピューターを直接操作して取得する



[スタート]ボタンから、[すべてのプログラム] (もしくは[プログラム])、[ESET]、[ESET Endpoint Security] (または [ESET Endpoint Antivirus]) とクリックし、最後に [ESET SysInspector] をクリックします。Windows Vista/7をご利用の場合は、[ユーザーアカウント制御] ダイアログが起動します。Windows Vistaをご利用の場合は [はい] ボタンをクリックします。

CAUTION

SysInspectorの起動には数分かかる場合があります。



 [ファイル]をクリックし、②[ログの保存]をク リックします。



保存先とファイル名を入力します。①保存先を選択 し、②[ファイルの種類]が[ESET SysInspector 圧縮ログ(*.zip)]であることを確認して、③[ファ イル名]を入力します。④[保存]ボタンをクリック します。



保存されたことを知らせるダイアログが表示される ので、[OK] ボタンをクリックします。

SysInspectorを終了します

5

[閉じる] ボタンをクリックして、ESET SysInspectorを終了します。

ERACのリモート操作で取得する

[スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[ESET]、[ESET Remote Administrator Console] とクリックし、最後に [ESET Remote Administrator Console] をクリックします。



Chapter 1	Chapter 2	Chapter 3	Chapter 4

隔離

0

更新(R)

リクエスト(Q)

キャンセル

「 グループのメンバ 」 タスク 「 コンフィグレーション | 保護状態 | 保護機能

ダウンロードしたSysInspector情報を指定ファイルに保存します。

▼ その後、ESET SysInspectorビューアーを実行してファイルを表示します(T)。

SysInspector



SysInspectorの情報は、対象コンピュー

ターがリクエスト処理実行後、管理サー

バー(ERAS)に接続したときにERASへ

送信されます。情報が送信されたら、①[更

新]ボタンをクリックしてください。

SysInspectorの情報がダウンロードされ

ます。2[名前をつけて保存]ボタンをク

リックします。

1
2
3

FAQ

4

POINT

オプロパティ

 \bigcirc

リクエストオプション

2012/07/24

ダウンロードしたSysInspectorログ

名前を付けて保存(S)...

0

一般

システム情報

SysInspector情報 日付:2012-07-24 03:35:18 (1秒未満前)

SysInspector情報を利用できます: (作成 2012-07-24 03:34:18 (47秒前))。Dクエスト】をク リックして、最新の情報を再度リクエストしてください。

SysInspector情報がダウンロードされました

表示(V) ダウンロードしたログをESET SysInspector Viewerで表示します。

🔲 スナップショットを作成する(結果のログをクライアントでも記録する)(E)

指定した時刻より前の最新のスナップショットとの比較を含める(1)

- 3:32:13

4

[ESET SysInspector ビューアーを起動し、ファイルを表示する] にチェックを入れて保存すると、保存終了後にESET SysInspector Viewer が起動し、取得した情報の閲覧が行えます。

OK(O)



 ●保存先を選択し、2 [ファイルの種類]
 が [ESET SysInspector圧 縮 ファイル (*.zip)] であることを確認して、3 [ファ イル名]を入力します。4 [保存] ボタンを クリックします。

Windowsのシステム情報(*.txt)の取得方法

Windowsのシステム情報は、Windowsに標準インストールされている[システム情報]を利用して取得します。 Windows XP以降のすべてのWindows OSで同じ手順で取得できます。



[スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[アクセサリ]、[システムツール] とクリッ クし、最後に[システム情報]をクリックします。



🦉 システム情報			
ファイル(F) 編集(E)	表示(V) へル	プ(H)	
❶ 開<(0)	Ctrl+0		値
閉じる(C)			Microsoft Wir
上書き保存(S)	Ctrl+S	ジョン	6.1.7601 Ser
2 エクスポート(E)		加情報	利用不可
EUBI(P)	Ctrl+P	造元	Microsoft Cor
Flauh3/L.)	Cultr	■山名	ESET-WIN7-
終了(X)		Fム製造元	Gigabyte Teo
	シス	テムモデル	X58A-UD7
	シス	、テムの種類	x64-ベース PI
		the set of	Convince Inte

1[ファイル]をクリックし、2[エクスポート]をクリックします。



3 保存先とファイル名を入力します

ファイルのエクスポート	ラリ → ドキュメント →	▼ 4 F≠1×>>	
整理 ▼ ●新しいフォノ	レダー		
☆ お気に入り ダウンロード	ドキュメント ライブラリ 対象フォルダー: 2か所	並べ替え:	フォルダー 🔹
■ デスクトップ 500 日本の目的 500 日本の目的 500 日本の目前 5	名前	更新日時	種類
🍃 ライブラリ		A 100 9 0 C 00	
 ■ トキュメント ■ ピクチャ ■ リーマオ 			
EFA シミュージック			
2	• • [
ファイル名(N): Win	dowsシステム情報		
ファイルの種類(T): テキ	ストファイル		

●保存先を選択し、2[ファイル名]を入力します。 8 [保存] ボタンをクリックします。システム情報の 保存が行われます。保存中は、進捗状況画面が表示 されます。

Chapter 2

Mac OS Xのシステム情報の取得方法

ご利用のMac端末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。



アップルメニューをクリックします



● [アップルメニュー] をクリックし、 ② [この Mac について] をク リックします。 1

2 画面が表示されます この Mac について ぼ しい情報] ボタンをクリックします。 ぼ しい情報] ボタンをクリックします。 ぼ しい情報] ボタンをクリックします。



[システムレポート] ボタンをクリックします。



システムレポートが表示されます



●メニューバーの[ファイル]をクリックし、2 [テキストとして書き出す]をクリックします。





●ファイル名を入力し、 2 [場所] のプルダウンメニュー から保存場所を選択し、③[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、4 [保存] ボタンをクリックします。

ファイルが保存されます 6

システムレポートが保存されます。

Mac OS Xのコンソールメッセージの取得方法

ご利用のMac端末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。

┃ Finderを起動します

00	🔤 アプリケーシ	ヨン	
		Q	
よく使う項目	名前	▲ 変更日	サイズ
□ マイファイル	🛃 iPhoto	2011年7月8日 17:52	1.09 GB
AlaDana 1	ITunes	2011年7月8日 17:45	136.7 MB
AirDrop	Launchpad	2011年7月8日 17:45	1.1 MB
🗚 アプリケーション	🖲 Mail	2011年7月8日 17:45	60.4 MB
デスクトップ	Mission Control	2011年7月8日 17:45	398 KB
四 書類	💭 Photo Booth	2011年7月8日 17:45	9.6 MB
	🔇 QuickTime Player	2011年7月8日 17:45	25.8 MB
09990-1	🍥 Safari	2011年7月8日 17:45	35.2 MB
ムービー	Time Machine	2011年7月8日 17:45	375 KB
ニ ミュージック	📔 アドレスブック	2011年7月8日 17:45	16.9 MB
のピカチャ	■ イメージキャプチャ	2011年7月8日 17:45	3.4 MB
	図 システム環境設定	2011年7月8日 17:45	1.6 MB
共有	竇 スティッキーズ	2011年7月8日 17:45	3.6 MB
デバイス	チェス	2011年7月8日 17:45	6.9 MB
	🎯 テキストエディット	2011年7月8日 17:45	8.1 MB
	福 プレビュー	2011年7月8日 17:45	42.2 MB
◎ リモートディスク	▶ 🔄 ユーティリティ 🛛 🙎	2011年7月8日 17:56	
	計算機	2011年7月8日 17:45	7 MB
	1 辞書	2011年7月8日 17:45	4.5 MB

Finderを開き、① [アプリケーション] をクリッ クして、② [ユーティリティ] フォルダーをダブ ルクリックします。 1

2 コンソールを起動します

00	🔯 ユーティリティ		
		Q	
よく使う項目	名前	▲ 変更日	サイズ
□ マイファイル	📓 Boot Camp アシスタント	2011年7月8日 17:45	9.9 MB
	🗶 ColorSync ユーティリティ	2011年7月8日 17:45	13.1 MB
AirDrop	Ø DigitalColor Meter	2011年7月8日 17:45	1.6 MB
🎤 アプリケーション	阑 Grapher	2011年7月8日 17:45	25 MB
🔜 デスクトップ	🗐 Java Preferences	2011年7月8日 17:45	570 KB
① 本和	Podcast Capture	2011年7月8日 17:45	13.9 MB
	Podcast Publisher	2011年7月8日 17:45	17 MB
0 9990-6	💥 RAID ユーティリティ	2011年7月8日 17:45	7.6 MB
ムービー	🗴 VoiceOver ユーティリティ	2011年7月8日 17:45	17.7 MB
ニ ミュージック	X X11	2011年7月8日 17:45	4.9 MB
レクチャ	1日 アクティビティモニタ	2011年7月8日 17:45	7.4 MB
101 ビジチャ	🕅 キーチェーンアクセス	2011年7月8日 17:45	11 MB
共有	然 グラブ	2011年7月8日 17:45	2.7 MB
デバイス	コンソール	2011年7月8日 17:45	5.6 MB
	🍙 システム情報	2011年7月8日 17:45	5.4 MB
	ターミナル	2011年7月8日 17:45	12.3 MB
◎ リモートディスク	■ ディスクユーティリティ	2011年7月8日 17:45	20.9 MB
	◉ ネットワークユーティリティ	2011年7月8日 17:45	2.1 MB
	🖏 移行アシスタント	2011年7月8日 17:45	5 MB

[コンソール] アイコンをダブルクリックしま

す。

コンソールが起動します。 ①メニューバーの [ファイル]をクリックし、 ②[コピーを保存] をクリックします。





FAQ



●ファイル名を入力し、
 ② [場所]のプルダウンメニューから保存場所を選択します。
 ③ [保存]ボタンをクリックします。

Chapter 2

1

2

3

FAQ

Mac OS Xのプロセス情報の取得方法

ご利用のMac端末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

,	00	🔤 アプリケーショ	ョン	
			Q	
	よく使う項目	名前	▲ 変更日	サイズ
	□ マイファイル	ITunes	2011年10月21日 14:15	182.6 MB
		Launchpad	2011年6月20日 14:38	1.1 MB
	AirDrop 🛡	😹 Mail	2011年10月21日 14:15	60.4 MB
	🗚 アプリケーション	Mission Control	2011年6月20日 14:38	398 KB
	デスクトップ	📕 Photo Booth	2011年10月21日 14:15	9.9 MB
	15	QuickTime Player	2011年10月21日 14:15	25.8 MB
	「」音規	🙀 Remote Desktop	2011年9月27日 16:40	45.7 MB
	🔮 ダウンロード	🍥 Safari	2011年10月21日 14:15	35.2 MB
	ムービー	Time Machine	2011年6月20日 14:38	375 KB
	1 ミュージック	📔 アドレスブック	2011年10月21日 14:15	16.8 MB
	OVATE	■ イメージキャプチャ	2011年10月21日 14:15	3.4 MB
		■ システム環境設定	2011年10月21日 14:15	1.7 MB
	共有	🧐 スティッキーズ	2011年10月21日 14:15	3.8 MB
		🚸 チェス	2011年10月21日 14:15	7.1 MB
	THIX	🜍 テキストエディット	2011年10月21日 14:15	8.3 MB
		194 プレビュー	2011年10月21日 14:15	42.3 MB
		▶ 🕅 ユーティリティ 🛛 🙎	2011年9月1日 17:44	
		計算機	2011年10月21日 14:15	6.9 MB
		◎ 辞書	2011年10月21日 14:15	4.5 MB

Finderを開き、① [アプリケーション] をクリッ クして、② [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		
		🔛 三 一 戸 一 回 📖 🔆 🔻 🗮 🔻	Q	
	よく使う項目	名前 4	変更日	サイズ
	マイファイル	 Bluetooth ファイル交換 Boot Camp アシスタント 	2011年10月21日 14:15 2011年10月21日 14:15	9.9 MB
	ATDrop A アプリケーション	💥 ColorSync ユーティリティ 🧭 DigitalColor Meter	2011年10月21日 14:15 2011年10月21日 14:15	13.3 MB 1.8 MB
	□ デスクトップ	Grapher Java Preferences	2011年10月21日 14:15 2011年6月17日 8:17	28.3 MB 570 KB
	 当 香規 ダウンロード 	Podcast Capture Podcast Publisher	2011年10月21日 14:15 2011年10月21日 14:15	14.4 MB 17 MB
	- L-L-	RAID ユーティリティ	2011年10月21日 14:15	8.4 MB
	□ ミューシック ◎ ピクチャ	X11	2011年10月21日 14:15	5.1 MB
	共有	アクティビティセータ 派 キーチェーンアクセス	2011年10月21日 14:15 2011年10月21日 14:15	11.4 MB
	デバイス	☆ グラブ ■ コンソール	2011年10月21日 14:15 2011年10月21日 14:15	2.7 MB 5.9 MB
		☆ システム情報 ■ ターミナル	2011年10月21日 14:15 2011年10月21日 14:15	5.3 MB
			2011年10月21日 14:15 2011年10月21日 14:15	21 MB 2.1 MB

[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

タファイル	表示	ウインドウ	ヘルプ		-	-			and the second se	- t.	
閉じる 保存 2	жw жs	000			アクティ	ピティモニ	9				
at a titlete	0.000		1	3		自分の	プロセス	:	Q- 711	9	
ページ設定 プリント	ਪ ਲ P ¥P	プロセスを料	と了 詳細を表示 プロ	ロセスのサンプルを	E取る		表示		7	ィルタ	Second Second
· · · · · ·	001	PID 7	ロセス名			ユーザ	% CPU	スレッド	実メモリ	種類	
		198	AirPort Base Sta	tion Agent		imac2	0.0	3	1.9 MB	Intel ((64 ピット)
		629	AppleSpell.serv	ice		imac2	0.0	2	10.8 MB	Intel (64 ピット)
		176	com.apple.doci	.extra		imac2	0.0	4	11.6 MB	Intel (64 ピット)
		926	com.apple.hise	vices-xpcservice	1	imac2	0.0	3	4.3 MB	Intel (64 ピット)
		821	CVMCompiler			imac2	0.0	1	18.2 MB	Intel (64 ピット)
		814	DashboardClier	it		imac2	0.1	8	28.1 MB	Intel (64ピット)
		148	distnoted			imac2	0.6	10	3.0 MB	Intel (64 ピット)
		152	Dock			imac2	1.0	5	60.9 MB	Intel (64ピット)
		202	esets_gui			imac2	1.4	6	32.9 MB	Intel	
		155	Finder			imac2	0.3	8	61.8 MB	Intel (64ピット)
		160	fontd			imac2	0.0	2	4.4 MB	Intel (64 ピット)
											area a
			CPU	システムメモ	リーディスクロ	の動作 ラ	ディスクの空き	ネットワ	-2		
							CPU 使用#				
		%	ユーザ: 3.00		スレッド: 376						
		8.2	374: 200		70+72: 78						
		26 10	SERVIE - 95.00	-							
											1.1
							C. C. C. C. C.				
							1 10				The Man

アクティビティモニタが起動します。 **①**メ ニューバーの[ファイル]をクリックし、 **②**[保 存]をクリックします。



●ファイル名を入力し、
 ② [場所]のプルダウンメニューから保存場所を選択します。
 ③ [標準テキスト]にチェックを入れ、
 ④ [保存] ボタンをクリックします。

1

2

3

4

FAQ

ESET製品の設定ファイル(.xml)の取得方法

ESET製品の設定ファイル (.xml) には、クライアント用プログラムの設定ファイルとESET Remote Administrator (ERA)の設定ファイルがあります。WindowsおよびMac OS Xのクライアント用プログラムの設定ファイルは、クラ イアント用プログラム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。また、ESET File Security for Linux および ESET Endpoint Security for AndroidはERAを利用して設定ファイルを取得します。

クライアント用プログラムの設定ファイル(.xml)の取得方法(Windowsの場合)

1 ESET Endpoint SecurityまたはESET Endpoint アンチウイルスのメイン画面を開きます。

 ESET Endpoint Security - 0 **X** 2 ESET ENDPOINT SECURITY ✔ 保護の状態 設定 Q コンピュータの検査 コンピュータ リアルタイムファイルシステム保護 デバイスコントロール 🔇 アップデート ✓ 有効
✓ 有効
✓ 有効 HIPS 🌞 設定 プレゼンテーションモード アンチステルス保護 無効 ✔ 有効 💥 ツール ネットワーク パーソナルファイアウォール ✔ 有効 ? ヘルプとサポート Webとメール Webアクセス保護 電子メールクライアント保護 迷惑メール対策機能 ✔ 有劲 ✓ 有効
✓ 有効 設定をインポート/エクスポートする... 詳細設定を表示する.. eser [設定]をクリックし、②[設定をイン ポートおよびエクスポートする]をクリッ クします。

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

3 設定のインポート/エクスポート
 ESET Endpoint Security の現在の設定をXMLファイルに保存し、必要に応じて復元できます。
 インポート/エクスポート
 ③ 設定のインポート(I)
 ④ 設定のエクスポート(E)
 ファイル名(F):
 OK(O)
 キャンセル(C)



 ●保存先を選択し、②[ファイル名]を入 力します。③[保存]ボタンをクリックし ます。

5	設定のインポート/エクスポート 2 ×
	ESET Endpoint Security の現在の設定をXMLファイルに保存し、必要に応じ て復元できます。
	インポート/エクスポート
	◎ 設定のインボート(I)
	 ・ ・ ・
	ファイル名(F):
	C:¥Users¥user¥Desktop¥EES設定ファイル.xml
	<u>ок(о)</u> キャンセル(с)

設定ファイルを保存します。[OK] ボタンをクリッ クします。
Chapter 1	Chapter 2	Chapter 3	Chapter 4	FAQ

クライアント用プログラムの設定ファイル (.xml)の取得方法 (Mac OS Xの場合)

メインウィンドウを開きます 1 ESET NOD32 Antivirus ✓ 保護の状態 設定 ○ コンピュータの検査 ウイルス・スパイウェア対策 リアルタイムファイルシステム保護 ✓ 有効化 **マップデート** 0 アップデートするためのユーザー名とパスワードを入力する... プロキシサーバを設定する... 設定のインポート/エクスポート... 2 🕕 ウイルス・スパイウェア対策 **≫** *ツ*−ル べての設定を既定値に戻す アプリケーションの設定を入力する... ? ヘルプ eser 標準モードを有効にする

メインウィンドウを開き、詳細モードに 切り替えてから、①[設定]ボタンをクリッ クして、②[設定のインポート/エクスポー ト]をクリックします。 1

2

3

4

FAQ

ESET NOD32 Antivirusでは、現在の設定をファイルに保存し、後でその設定を復元できます インポート/エクスポート 設定のインポート 〕 ② 設定のエクスポート	0	設定のインポート/エクス	ポート	
 ○ 設定のインポート ● ● 設定のエクスポート 	NOD32 Antivirusでは、3 ノポート/エクスポート	現在の設定をファイルに保存し、	後でその設定を復元でき	ます。
	設定のインポート 設定のエクスポート			
ファイル名:	イル名:			2 参照

● [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。



ESET NO	名前:	設定ファイル	,		•
インポー	場所:	1 書類		÷]	
 ● 設定 ● 設定 	255-5 2255-5	2	والم الم الم		
ファイル ね.	-		キャンセ		
					参照

●ファイル名を入力し、2保存先を[場所]のプ ルダウンメニューから選択します。3[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



①保存するファイルがフルパスで表示されま す。 ②[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。

クライアント用プログラムの設定ファイル(.xml)の取得方法(Linuxの場合)

] [スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[ESET]、[ESET Remote Administrator Console] とクリックし、最後に [ESET Remote Administrator Console] をクリックします。

フィルタを使用する(U) クライアント	すべてのサーバを対	象にする 🔻	チェック チェック	サーバを追加するには?				
(他のオプション) 変更を適用(A) リセット(R)	サーバ名 🗛	105172	DN(C) OFF(U) ト 스ュ	」 201727を20119のには? 定義データベースの状 ▽2	最も古いアクセス	最終ウイノ	レス警告	1.
クライアントフィルタ条件	Eset-svr	3		現在のバージョン	1時間前	0		0
								+
パラメータグループ								
	ホテオスアイテル ロ			テム情報:				
白- 日 日 日 日 日 日 日 日 日 日 日 日 日	(0)		<< < > 13	(3 アイテム)全3 アイテムアイティ	_{以中} 表示モード(M):	: カスタム表示モート		
Callers	クライアント名 /	プライマリサーバ	ドメイン	製品名 FSET Factorial Security (製品バージョン	リクエストされたポ	ポリシー名	
2	Eset-smb	Eset-syr	ad-domain.exa	ESET Security	408	既定のプライマリ	既定のプライマリ.	
	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	so 4.5.12002	既定のプライマリ	既定のプライマリ	
	Set-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	so 4.5.12002	既定のプライマリ	既定のブライマリ	
	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	so 4.5.12002	既定のプライマリ	既定のプライマリ.	
4 3	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	a. 45.12002	既定のプライマリ	既定のプライマリ.	
۲ <u>۲</u>	Eset-svr 🖉	Eset-svr	ad-domain.exa	ESET File Security Micros	45.12002	既定のプライマリ	既定のプライマリ.	
「 」 ううイアントのみ クレーズ検索) マ	Set-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	so 45.12002	既定のプライマリ	既定のブライマリ.	
 	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	4.5.12002	脱定のブライマリ	既定のブライマリ.	
 ・ ・	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	so 4.5.12002	脱定のブライマリ	既定のプライマリ.	
「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 」 「 「 」 「 「 」 「 「 」 「 「 」 「 「 」 「 「 「 」 「 「 」 「 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 」 「 」 」 「 」	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micros	so 4.5.12002	既定のブライマリ	既定のブライマリ.	
	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micro	4.5.12002	既定のプライマリ	既定のブライマリ	
	Eset-svr	Eset-svr	ad-domain.exa	ESET File Security Micro	so 4 .5.12002	規定のプライマリ	既定のブライマリ	

[クライント]ペインをクリック
 し、2設定ファイルを取得したい
 コンピューターをダブルクリック
 します。

1

2

3

4



 [コンフィグレーション]をク リックし、?[その後、ESETコン フィグレーションエディタを実行 してファイルを編集]のチェックを 外します。?[名前を付けて保存] をクリックします。



①保存先を選択し、2[ファイルの種類]が[ESET 設定ファイル(*.xml)]であることを確認して、
③[ファイル名]を入力します。
④[保存]をクリックします。

え プロパティ	
J 一般 グループのメンバ タスク コンフィグレーション 保護状態 保護機能 シス	テム情報 隔離
ゴンフィグレーション 日時:2013-05-09 17:07:15 (56 分前)	
コンフィグレーションを利用できます	
	更新(R)
ダウンロード済みのコンフィグレーション	キャンセル(C)
ダウンロードしたコンフィグレーション	
表示(V) ダウンロードしたコンフィグレーションを ESET コンフィグレーション	エディタで表示します。
名前を付けて保 存(S)… ダウンロードしたコンフィグレーションを指定ファイルに保存します。 下 その後、ESETコンフィグレーションエディタを実行してファイル	を編集
新規タスク(T) 🖂 ダウンロードしたコンフィグレーションを新しいコンフィグレーショ	ンタスクで使用します
	K(O) キャンセル

[OK] をクリックして、プロパティ 画面を閉じます。

クライアント用プログラムの設定ファイル(.xml)の取得方法(Androidの場合)

] [スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[ESET]、[ESET Remote Administrator Console] とクリックし、最後に [ESET Remote Administrator Console] をクリックします。



[クライント]ペインをクリック
 し、2設定ファイルを取得したい
 コンピューターをダブルクリック
 します。

1

2

3

4



 [コンフィグレーション]をク リックし、?[その後、ESETコン フィグレーションエディタを実行 してファイルを編集]のチェックを 外します。?[名前を付けて保存] をクリックします。



1保存先を選択し、2[ファイルの種類]が[ESET 設定ファイル(*.xml)]であることを確認して、
[ファイル名]を入力します。
(保存]をクリックします。

5	🔊 ว่ามหัวง
	一般 「グループのメンバ」タスク コンフィグレーション 【保護状態】保護機能 「システム情報」
	ロンフィグレーション 日時:2013-05-09 09:46:10 (8時間前)
	コンフィグレーションを利用できます
	更新(R)
	ダウンロード済みのコンフィグレーション キャンセル(C)
	「ダウンロードしたコンフィグレーション
	表示(V) ダウンロードしたコンフィグレーションを ESET コンフィグレーション エディタで表示します。
	名前を付けて保 存(S) ダウンロードしたコンフィグレーションを指定ファイルに保存します。 下 その後、ESETコンフィグレーションエディタを実行してファイルを編集
	新規タスク(T) ダウンロードしたコンフィグレーションを新しいコンフィグレーションタスクで使用しま?
	OK(O) キャンセル

[OK] をクリックして、プロパティ 画面を閉じます。

Chapter	1	

ERASの設定ファイルの取得方法

1

[スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[ESET]、[ESET Remote

Administrator Server]、[ESET Remote Administrator Maintenance Tool]とクリックします。

1
2
3
4

2 ERAメンテナンスツールが起動したら、[次へ] ボタンをクリックします。 [サーバ情報] が表示されます。[次へ] ボタンをクリックします。 3 Server Maintenance Tool × 4 アクションの選択 eset 保守タスクの種類選択... 保守タスク・ ○ ERA Serverを停止(S) OF ○ データベースの転送(種類の異なる同じバージョンのデータベースに転送)(A) データベースのバックアップ(外部ダンプファイルに)(U)
 データベースの復元(外部ダンプファイルから)(R) ○ テーブルを削除(データベースをリセット)(E) ○ ストレージのバックアッフィット ○ ストレージの復元(外部ダンプファイルに) ストレージのバックアップ(外部ダンプファイル) ○ 新しいライセンスキーをインストール(W) ● サーバのコンフィグレーションを変更(ERA Consoleのインストールが必要)(M) サーバ情報を表示する(こは、[く戻る(B)]ボタンをクリックします ファイルからすべての設定をロード(L) 0 < 戻る(B))次へ(N) > キャンセル(C)

[アクションの選択] ダイアログが表示されます。①[サーバのコンフィグレーションを変更]にチェックを入れ、②[次へ] ボタンをクリックします。

Faq

Maintenance Toolウィザードは、(保守タスクを開始する準備が整いました 現在選択されているタスク: サーバのコンフィグレーションを変更 (保守タスクを開始するには、開始にたりリックします。(保守タスクの)設定を確認または変更する場合は
現在選択されているタスク: サーバのコンフィグレーションを変更 保守タスクを開始さるには、開始したクリックします。(保守タスクの設定を確認または変更する場合は 見てたらいっか」ます、ウィザードを終っするです。(保守タスクの設定を確認または変更する場合は
(保守タスクを開始するには、開始)をクリックします。(保守タスクの設定を確認法たは変更する場合は 言うためしゅのします、ウムザードを終くするには、ほかいたいためしゅのします。
Marchandrase (A.) Lickel and reactive random and range
すべての設定をファイルには

[開始] ボタンをクリックします。



. 準備完了

ESET コンフィグレーションエディター が起動します。 [Remote Administrator] をクリックし ます。

- 🗆 🗙

次へ<mark>(ℕ</mark>)

既定(D)

	製品: Remote Administrator Server
Ctrl+W	
Gtrl+H Ctrl+J	
a8E08.tmp	
Alt+F4	
	CtrI+W OtrI+H CtrI+J a8E08tmp Ait+F4

▼ リセット

マーク(M) マーク解除(U)

製品: Remote Administrator Server

設定のエクスポートを行います。 1[ファ イル] メニューをクリックし、2[マーク した項目をエクスポート]をクリックしま す。



保存先とファイル名を入力します。①保 存先を選択し、2[ファイル名]を入力し ます。3[保存]ボタンをクリックします。

1

2

3

4



Chapter 2

FAQ



ダイアログが表示されます。①[OK]ボタンをクリッ クし、2[処理タスク]ダイアログの[閉じる]ボタ ンをクリックします。

> ERAメンテナンスツールを終了します。 [終了] ボタンをクリックします。

11	SERA Maintenance Tool	×
	ESET REMOTE ADMINISTRATOR MAINTENANCE TOOL	保守タスクが正常に完了しまし た
		ESET Remote Administrator Maintenance Tool を終了するには、「終了」ボタンをクリックしま す。別の保守タスクを実行するには、「戻る」をク リックします。
	eset	
		< 戻る(B) 終了(F) キャンセル(C)



Windowsの場合

弊社では、スクリーンショットの提出をお願いする場合があります。ここでは、Windows端末における一般的なスクリー ンショットの作成方法を紹介します。

│ スクリーンショットを取ります

スクリーンショットを作成したい画面を表示します。フルスクリーンでスクリーンショットを作成したいときは [PrintScreen] キーを押します。アクティブウィンドウ(作業対象のウィンドウ)のスクリーンショットを作成し たいときは、[Alt]キーを押しながら[PrintScreen] キーを押します。

2 [ペイント]を起動します

[スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[アクセサリ] とクリックし、最後に [ペイント] をクリックします。



[ペイント]に、[Ctrl]キーを押しながら[V] キーを押して、スクリーンショットをペー ストします。

スクリーンショットを保存します

[ファイル] メニュー、[名前を付けて保存] とクリックします。[名前を付けて保存] ダイアログが表示されたら、 保存先を選択し、ファイル名を入力してJPEG形式で[保存] ボタンをクリックします。

4

Chapter 1	Chapter 2	Chapter 3	Chapter 4	F٨

Mac OS Xの場合

ご利用のMac端末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。

FAQ

1

2

3

4

Q