

ESET[™] ENDPOINT PROTECTION
イーセツト エンドポイント プロテクション

ESET セキュリティ ソフトウェア シリーズ製品 運用ガイド

ベースアップデート編

第 13 版
最新アップデート日 2018/12/13

© Canon IT Solutions Inc. 2018

本資料の著作権は、キヤノン IT ソリューションズ株式会社へ帰属します。キヤノン IT ソリューションズ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本資料の作成にあたり、細心の注意を払っていますが、本書の記述内容に誤りや欠落があっても、キヤノン IT ソリューションズ株式会社はいかなる責任も負わないものとします。また、本資料の内容は、予告なしに変更される場合があります。

ESET、ESET Security Management Center、ESET Remote Administrator、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ThreatSense は、ESET, spol.s r.o.の商標です。

Microsoft、Windows、Windows Server、Active Directory 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。

目次

1	はじめに	4
2	本資料の構成	4
3	ベースアップデートについて	5
3.1	ベースアップデートとは	5
3.2	ベースアップデート時の検出エンジン（ウイルス定義データベース）容量	6
3.3	ベースアップデート時に発生しやすい障害	8
4	障害を発生させないために	11
4.1	障害を発生させないための設定	11
4.2	障害の回避方法	12
4.3	障害が発生した場合の対処方法	19
5	ケース別設定事例	25
5.1	同じ時間帯に検出エンジン（ウイルス定義データベース）をアップデートしている場合	25
5.2	1 台のミラーサーバーで多数のクライアントがアップデートする場合	37
5.3	拠点間のネットワーク帯域が細い場合	46
6	よくある質問とトラブルシューティング	56
7	製品サポート情報	58
7.1	ご意見、ご質問のお問い合わせ先	58
7.2	製品 Q&A について	58
8	補足資料	59
8.1	アップデートタスクの配布手順	59
8.2	検出エンジン（ウイルス定義データベース）のダウンロード方法	62
8.3	オフライン更新の手順	64
8.4	検出エンジン（ウイルス定義データベース）のアップデート手順	66
8.5	クライアントの設定画面からアップデートスケジュールを変更する手順	68
8.6	クライアントの設定画面からアップデートサーバーを変更する手順	71
8.7	ESET File Security for Microsoft Windows Server を利用したミラーサーバー構築手順	73

1 はじめに

本資料は、ESET セキュリティ ソフトウェア シリーズ製品 運用ガイド ベースアップデータ編です。ESET 製品の検出エンジン（ウイルス定義データベース）のアップデート時に発生するベースアップデータについて、説明した資料です。

なお、以下のプログラムで構築したミラーサーバー機能にはナノアップデート機能が搭載され、ベースアップデータ時の負荷が軽減されます。

- ・ ESET Remote Administrator V5.3
- ・ ESET File Security for Microsoft Windows Server V6.2 以降
- ・ ESET Endpoint Security V6.2 以降
- ・ ESET Endpoint アンチウイルス V5.0 以降

また、「ミラーツール」で取得した検出エンジン（ウイルス定義データベース）をミラーサーバーで公開する場合も、ナノアップデート機能が有効になり、ベースアップデータ時の負荷が軽減されます。

詳細は『3.2 ベースアップデータ時の検出エンジン（ウイルス定義データベース）容量』をご参照ください。

2 本資料の構成

本資料は、主に4つの構成に分かれています。

はじめに、『3 ベースアップデータについて』をお読みいただき、ベースアップデータについてご理解いただいた後、ご使用の環境に応じて『4 障害を発生させないために』、『5 ケース別設定事例』に記載されている設定を実施してください。また、弊社サポートセンターにお問い合わせが多い質問をまとめた『6 よくある質問とトラブルシューティング』についても、あわせてご参照ください。

本資料の構成

『3 ベースアップデータについて』

『ベースアップデータについて』では、ベースアップデータの仕組みやベースアップデータが実施された場合に発生しやすい障害について説明します。

『4 障害を発生させないために』

『障害を発生させないために』では、ベースアップデータ実施に障害が発生しないための設定や障害が発生した場合の対処方法について説明します。

『5 ケース別設定事例』

『ケース別設定事例』では、3つの構成を例に設定の変更例について説明します。

『6 よくある質問とトラブルシューティング』

『よくある質問とトラブルシューティング』では、弊社サポートセンターにお問い合わせが多い質問について説明します。

3 ベースアップデートについて

この章では、ベースアップデートの仕組みやベースアップデート実施時に発生しやすい障害について説明します。

3.1 ベースアップデートとは

はじめにベースアップデートについて説明します。

ESET 製品の検出エンジン（ウイルス定義データベース）のアップデートは、通常差分アップデートでおこなわれます。

差分アップデートでは、基準となる検出エンジン（ウイルス定義データベース）から、最新の検出エンジン（ウイルス定義データベース）との差分情報のみ配信します。これにより、アップデートサーバーからすべての検出エンジン（ウイルス定義データベース）を配信する必要がなく検出エンジン（ウイルス定義データベース）の容量を抑えることができます。

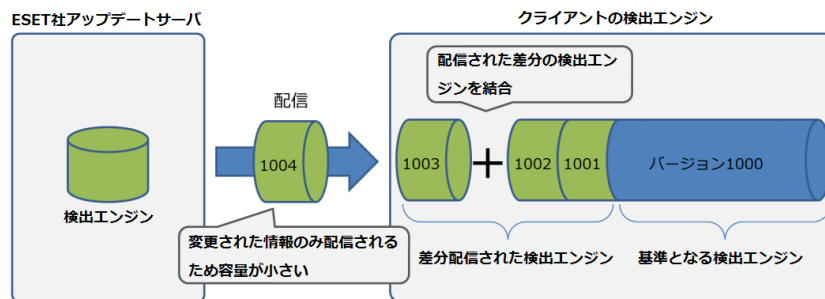


図 1 差分アップデートのイメージ

しかし、この差分アップデートは、検出エンジン（ウイルス定義データベース）のアップデート処理を繰り返すことにより、フラグメントが発生します。

そのため、検出エンジン（ウイルス定義データベース）の容量が肥大化し、効率的にウイルス検査がおこなえない欠点があります。

そこで、ESET 製品は、検出エンジン（ウイルス定義データベース）の容量が一定の容量を超えると、検出エンジン（ウイルス定義データベース）の再構築をおこない、再構築した検出エンジン（ウイルス定義データベース）を配信しています。弊社では、この再構築した検出エンジン（ウイルス定義データベース）の配信とアップデート処理のことを、『ベースアップデート』と呼んでいます。

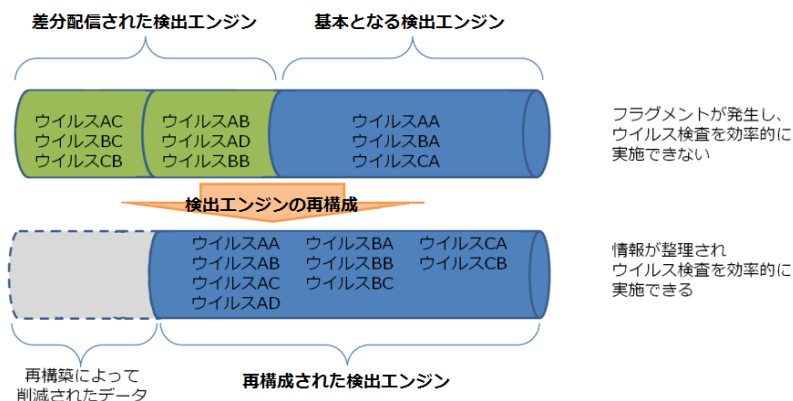


図 2 検出エンジン（ウイルス定義データベース）の再構成イメージ

3.2 ベースアップデート時の検出エンジン（ウイルス定義データベース）容量

ここでは、ベースアップデート時に配信される検出エンジン（ウイルス定義データベース）の容量について説明します。

ESET 製品では、通常 1 日に 4～5 回程度、数 KB から数百 KB 程度の検出エンジン（ウイルス定義データベース）が配信されます※1。

しかし、ベースアップデートが実施された場合、再構築された検出エンジン（ウイルス定義データベース）が配布されるため、容量の大きいデータ（最大約 40MB 前後※2）が配信されます。

実施日時（日本時間）	検出エンジン （ウイルス定義データベース）のサイズ
2016 年 07 月 19 日	最大約 46MB
2016 年 05 月 26 日	最大約 15MB
：	：
2010 年 04 月 19 日	約 25MB

表 1 過去に実施されたベースアップデート

※1 検出エンジン（ウイルス定義データベース）の間隔、容量は、ウイルスの発生状況などにより変動します。

※2 ベースアップデート時の検出エンジン（ウイルス定義データベース）容量は固定（約 40MB 前後）ではありません。

ウイルスの発生状況などにより容量が増加、減少する可能性があります。

※3 2010 年以降、ベースアップデート時に配信される検出エンジン（ウイルス定義データベース）のサイズは最大 40MB まで増加しています。また、数 MB～約 15MB のベースアップデートが月に 1 回程度配信されています。

なお、以下のプログラムのミラーサーバー機能にはナノアップデート機能が搭載されています。

- ESET Remote Administrator V5.3
- ESET File Security for Microsoft Windows Server V6.2 以降
- ESET Endpoint Security V6.2 以降
- ESET Endpoint アンチウイルス V5.0 以降

また、「ミラーツール」で取得した検出エンジン（ウイルス定義データベース）をミラーサーバーで公開する場合も、ナノアップデート機能が有効になります。

本機能によりクライアントがミラーサーバー経由でベースアップデートを実施する際に、クライアントが ESET 社のアップデートサーバーから直接検出エンジン（ウイルス定義データベース）をアップデートする場合と同様に、通常サイズ（数 KB～約 5MB）の少ない容量で検出エンジン（ウイルス定義データベース）をアップデートでき、ベースアップデート時の負荷が軽減されます。

(注意事項)

ナノアップデート機能を適用する場合は、前述のプログラムのミラーサーバー機能をご利用いただくか、直接インターネット上から検出エンジン（ウイルス定義データベース）を取得してください。ESET File Security for Microsoft Windows Server V4.5、ESET File Security for Linux V4.0 / V4.5 で構築したミラーサーバーから検出エンジン（ウイルス定義データベース）をアップデートする場合はナノアップデートの対象になりませんのでご注意ください。

ナノアップデートは差分アップデートです。差分が有効な期間の目安としては最終アップデートから約4日間ですので、こまめに検出エンジン（ウイルス定義データベース）をアップデートしてください。また、ミラーサーバー自身の検出エンジン（ウイルス定義データベース）のアップデートは、ナノアップデートの対象にはなりませんのでご注意ください。

なお、検出エンジン（ウイルス定義データベース）のアップデートがこまめにおこなえないなどナノアップデートが使用できない場合は、ベースアップデート対策が必要となる場合があります。引き続き本文書を参照いただき、環境にあった対策をご検討ください。

3.3 ベースアップデート時に発生しやすい障害

ここでは、ナノアップデートが適用されない環境でベースアップデートが実施された場合に発生しやすい障害について説明します。

前項目『3.2 ベースアップデート時の検出エンジン(ウイルス定義データベース)容量』でも説明したように、ベースアップデートが実施された場合、ナノアップデートが適用されない環境では、通常配信される検出エンジン(ウイルス定義データベース)より容量の大きな検出エンジン(ウイルス定義データベース)(最大約 40MB 前後)が配信されます。そのため、以下のような障害が発生する場合があります。

【 ベースアップデート時に発生しやすい障害 】

- 障害① ネットワークトラフィックが増加する
- 障害② ミラーサーバーに負荷がかかり、サーバーのレスポンスが低下する
- 障害③ 検出エンジン(ウイルス定義データベース)のアップデートに失敗する

以下に、ナノアップデートが適用されない環境でベースアップデートが実施された場合に発生しやすい障害について説明します。

障害① ネットワークトラフィックが増加する

ベースアップデートが実施された場合、通常のアップデートに比べ容量の大きな検出エンジン(ウイルス定義データベース)のダウンロードが必要になります。そのため、インターネット回線や社内ネットワーク回線の帯域が小さい場合、ネットワークトラフィックが増加する可能性があります。

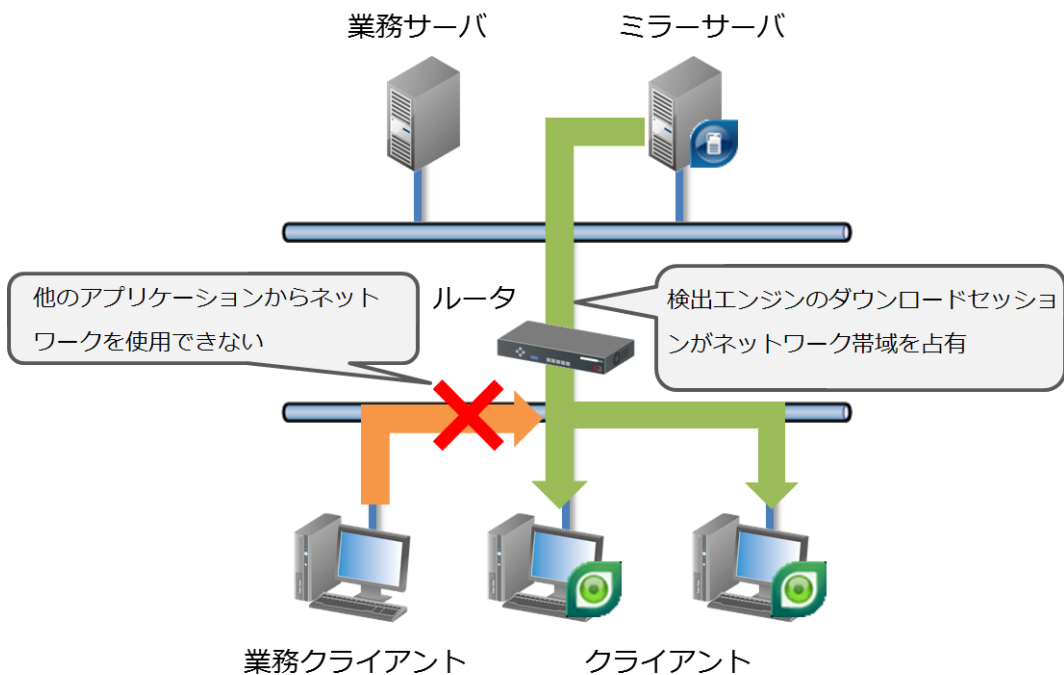


図 3 障害イメージ

障害② ミラーサーバーに負荷がかかり、サーバーのレスポンスが低下する

検出エンジン（ウイルス定義データベース）が実施された場合、通常のアップデートに比べ容量の大きな検出エンジン（ウイルス定義データベース）のダウンロードが必要になります。そのため、検出エンジン（ウイルス定義データベース）のダウンロードに時間がかかります。1 台のサーバーで多数のクライアントをアップデートしている場合、接続数が増加し、ミラーサーバーに負荷がかかる可能性があります。また、他のシステム（業務アプリケーションやデータベースサーバーなど）がインストールされているコンピューターにミラーサーバーを構築している場合、一時的にコンピューターのレスポンスが低下し、他のシステムの動作に影響を及ぼす場合があります。

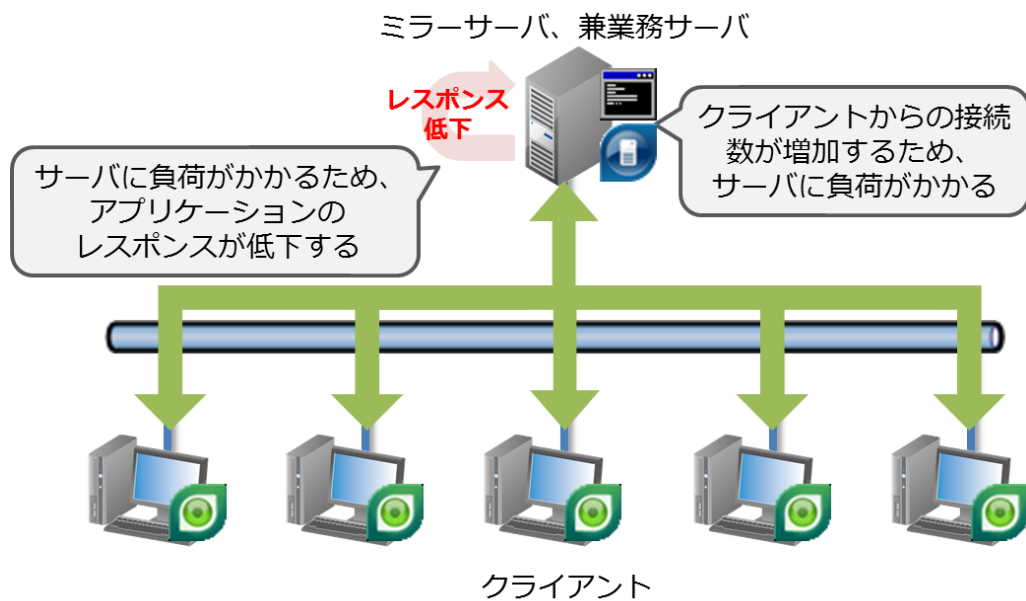


図 4 障害イメージ

障害③ 検出エンジン（ウイルス定義データベース）のアップデートに失敗する

ベースアップデートが実施された場合、通常の配信に比べ容量の大きい検出エンジン（ウイルス定義データベース）が配信されます。そのため、ESET 社のアップデートサーバーとミラーサーバーまたはクライアントの間に、プロキシサーバーやキャッシュ型のファイアウォールが存在する場合、ネットワーク機器に実装されているダウンロードサイズの制限機能などにより、検出エンジン（ウイルス定義データベース）のダウンロードが失敗する場合があります。

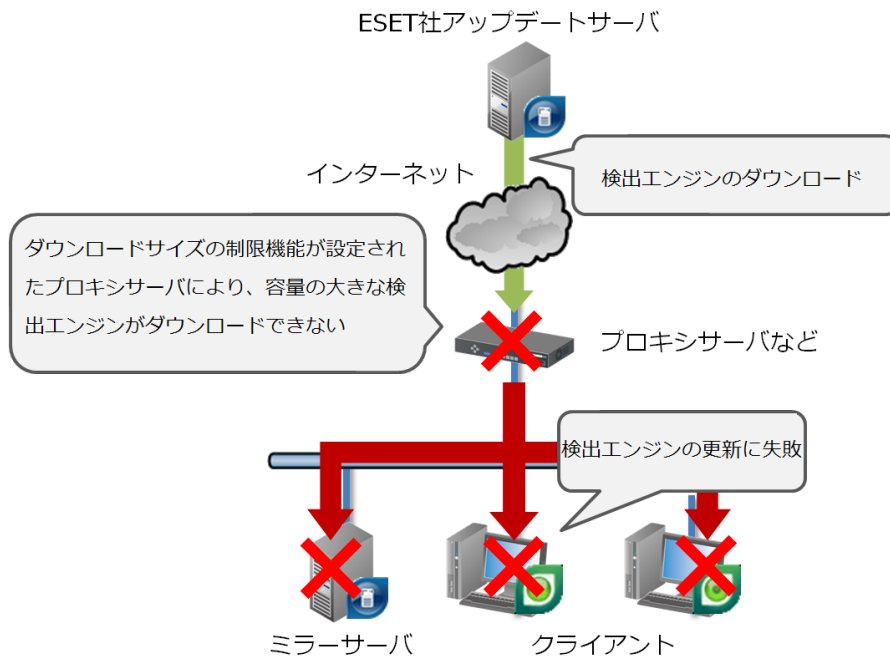


図 5 障害イメージ

以上のように、ナノアップデートが適用されない環境でベースアップデートが実施された場合、容量の大きなデータが配信されるため、通常の検出エンジン（ウイルス定義データベース）のアップデートに比べ、障害が発生する可能性が高くなります。

次の章では、これらの障害を未然に防ぐための設定について説明します。

4 障害を発生させないために

この章では、ナノアップデートが適用されない環境でベースアップデートが実施された場合に、発生しやすい障害を未然に防ぐための設定について説明します。

4.1 障害を発生させないための設定

ここでは、ナノアップデートが適用されない環境でベースアップデートが実施された場合に発生しやすい障害を未然に防ぐための設定について説明します。『3.1 ベースアップデートとは』でも説明しましたが、ナノアップデートが適用されない環境でベースアップデートが実施された場合、通常より大きな容量の検出エンジン（ウイルス定義データベース）が配信されます。そのため、ネットワークトラフィックの増加やミラーサーバーのレスポンス低下などの現象が発生することがあります。上記現象は、以下のような設定をおこなうことで回避することが可能です。

【現象を回避するための設定】

方法① クライアントのアップデート時間を分散する

方法② IISサーバーを構築し、検出エンジン（ウイルス定義データベース）を公開する

方法③ 拠点ごとにミラーサーバーを構築し、アップデートサーバーを分散する

方法④ 管理サーバーからアップデートタスクを配布する

方法⑤ ネットワーク機器を利用し帯域制御をおこなう

方法⑥ CD-ROM や USB メモリなどを利用したオフライン更新をおこなう

回避方法		更新の手間	設定変更の手間	サーバの構築	ネットワークへの負荷	規模	前提条件
方法① 更新時間を分ける	ESMC / ERA を使用してクライアントを管理していない場合	手間がかからない	手間がかからない	必要がない	軽減される	小～中規模	ESMC / ERA サーバーを使用してクライアントを管理している
	ESMC / ERA を使用してクライアントを管理していない場合	手間がかからない	手間がかかる	必要がない	軽減される	小規模	
方法② IISサーバを構築する		手間がかからない	少し手間がかかる	必要がある (IISサーバ)	軽減される	中～大規模	IISのインストール
方法③ ミラーサーバを構築する	ESMC / ERA を使用してクライアントを管理していない場合	手間がかからない	少し手間がかかる	必要がある (ミラーサーバ)	大幅に軽減される	中～大規模	ESMC / ERA サーバーを使用してクライアントを管理している
	ESMC / ERA を使用してクライアントを管理していない場合	手間がかからない	手間がかかる	必要がある (ミラーサーバ)	大幅に軽減される	小規模	
方法④ 更新タスクを配布する		手間がかかる	手間がかからない	必要がない	軽減される	小～中規模	ESMC / ERA サーバーを使用してクライアントを管理している
方法⑤ ネットワーク機器による制御		手間がかからない	手間がかかる	必要がない	軽減される	小～中規模	ネットワーク機器が必要
方法⑥ オフライン更新	ESMC / ERA を使用してクライアントを管理していない場合	手間がかかる	手間がかからない	必要がない	大幅に軽減される	小規模	ESMC / ERA サーバーを使用してクライアントを管理している
	ESMC / ERA を使用してクライアントを管理していない場合	手間がかかる	手間がかかる	必要がない	大幅に軽減される	小規模	

表 2 各回避方法の特徴

次の項では、ナノアップデートが適用されない環境でベースアップデートが実施された場合に発生しやすい障害を未然に防ぐための具体的な設定方法と各方法の特徴およびメリット・デメリットについて説明します。

4.2 障害の回避方法

ここでは、『3.3 ベースアップデート時に発生しやすい障害』で説明した、ナノアップデートが適用されない環境でベースアップデートが実施された場合に発生しやすい障害を回避するための具体的な設定について説明します。以下の各設定方法を参照いただき、ご使用の環境に合った設定変更や運用方法を実施してください。

方法① クライアントのアップデート時間を分散する

多数のクライアントから同時に検出エンジン（ウイルス定義データベース）のアップデートがおこなわれると、ネットワークトラフィックの増加やミラーサーバーに負荷がかかります。そのため、各クライアントのアップデートスケジュールをいくつかのグループに分け、同じ時間帯にアップデート処理をするクライアントを分散します。

この方法は、クライアントのアップデートスケジュールを変更することで、簡単に設定することができます。具体的な設定手順については、『5.1 同じ時間帯に検出エンジン（ウイルス定義データベース）をアップデートしている場合』をご参照ください。

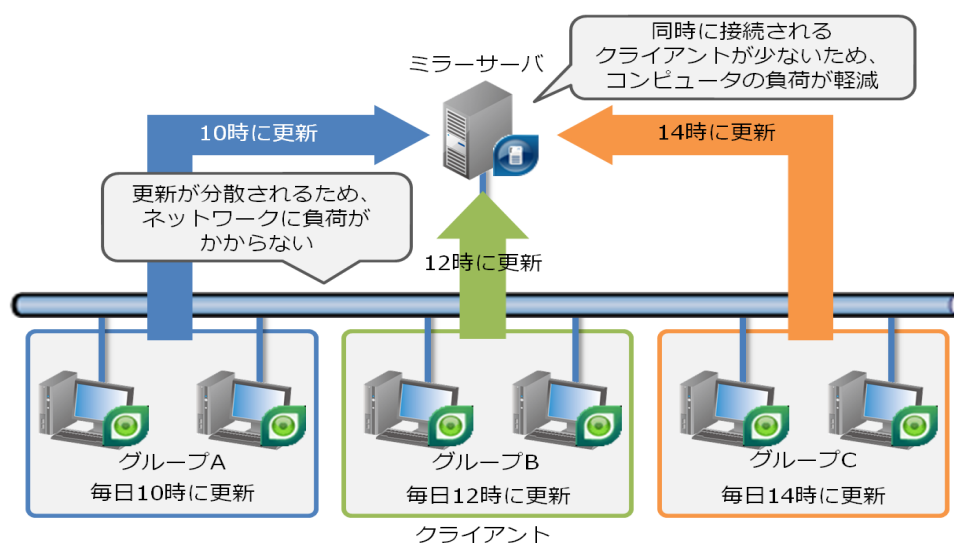


図6 各クライアントのアップデート時間を分散する場合

項目	説明
特徴	ミラーサーバーの追加やネットワーク構成を変更できない場合に最適な方法です。
設定・運用手順	① 各クライアントのグループ分けとアップデート時間の検討 ② アップデートスケジュールの変更 (ESMC/ERA からコンフィグレーションの配布など) ③ 検出エンジン (ウイルス定義データベース) の配布確認
メリット	検出エンジン (ウイルス定義データベース) のアップデートタイミングを変更するだけで簡単に変更することができる
デメリット	各グループのアップデート処理が重ならないように設定する必要がある

表 3 回避方法の特徴とメリット、デメリット

方法② IIS サーバーを構築し、検出エンジン（ウイルス定義データベース）を公開する

ESET 製品のミラーサーバーは、多数のクライアントから同時に検出エンジン（ウイルス定義データベース）をアップデートすることができません。また、帯域制御機能や接続数制限機能が実装されていません。そのため、Windows Server に標準で実装されている Internet Information Service (IIS) を利用して、検出エンジン（ウイルス定義データベース）を公開をします。大規模向けに設計されている IIS を利用することにより、多数のクライアントから同時に検出エンジン（ウイルス定義データベース）をアップデートすることができます。

また、IIS に実装されているネットワーク制御機能を使用し、帯域制御や接続数の制限をおこなうこともできます。具体的な設定手順については、補足資料『5.2 1 台のミラーサーバーで多数のクライアントがアップデートする場合』をご参照ください。

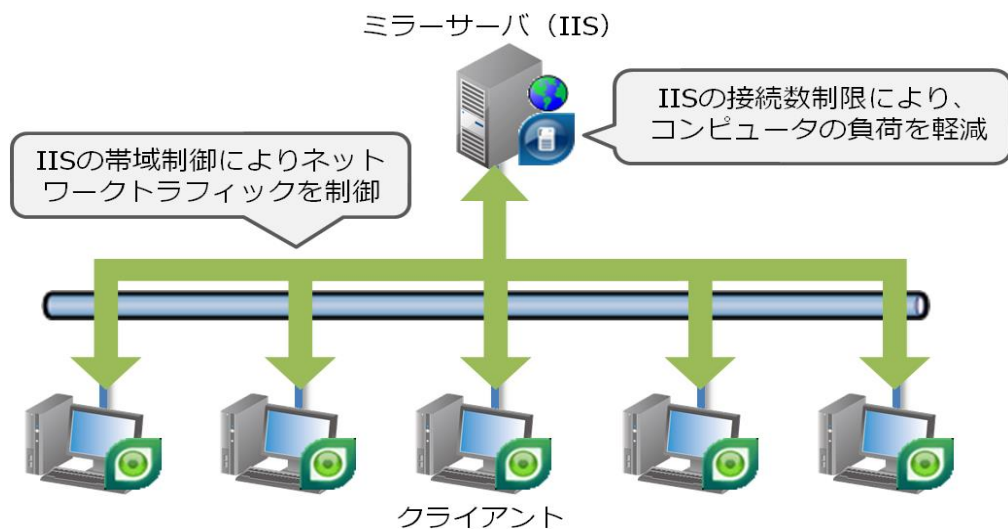


図 7 IIS サーバーを構築し、検出エンジン（ウイルス定義データベース）を公開する

項目	説明
特徴	1 台のミラーサーバーで多くのクライアントをアップデートしている場合やネットワークトラフィックの増加を一定量に押さえたい場合に最適な方法です。
設定・運用手順	① IIS を構築 ② 既存のミラーサーバーの停止 ③ ミラーサーバーの設定（仮想 WEB ページの設定） ④ 検出エンジン（ウイルス定義データベース）配布確認
メリット	1 台の IIS サーバーで、多くのクライアントの検出エンジン（ウイルス定義データベース）をアップデートすることが可能
デメリット	IIS の構築および管理が必要になる

表 4 回避方法の特徴とメリット、デメリット

方法③ 拠点ごとにミラーサーバーを構築し、アップデートサーバーを分散する

VPN や ISDN など帯域の狭いネットワークを経由して、検出エンジン（ウイルス定義データベース）のアップデートをおこなっている場合、ナノアップデートが適用されない環境でベースアップデートが実施されるとネットワークトラフィックが増加し、検出エンジン（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があります。そのため、拠点ごとにミラーサーバーを構築し、検出エンジン（ウイルス定義データベース）のアップデート先を分散します。検出エンジン（ウイルス定義データベース）のアップデート先が分散されるため、ネットワークトラフィックが軽減されます。具体的な設定手順については、『5.3 拠点間のネットワーク帯域が細い場合』をご参照ください。

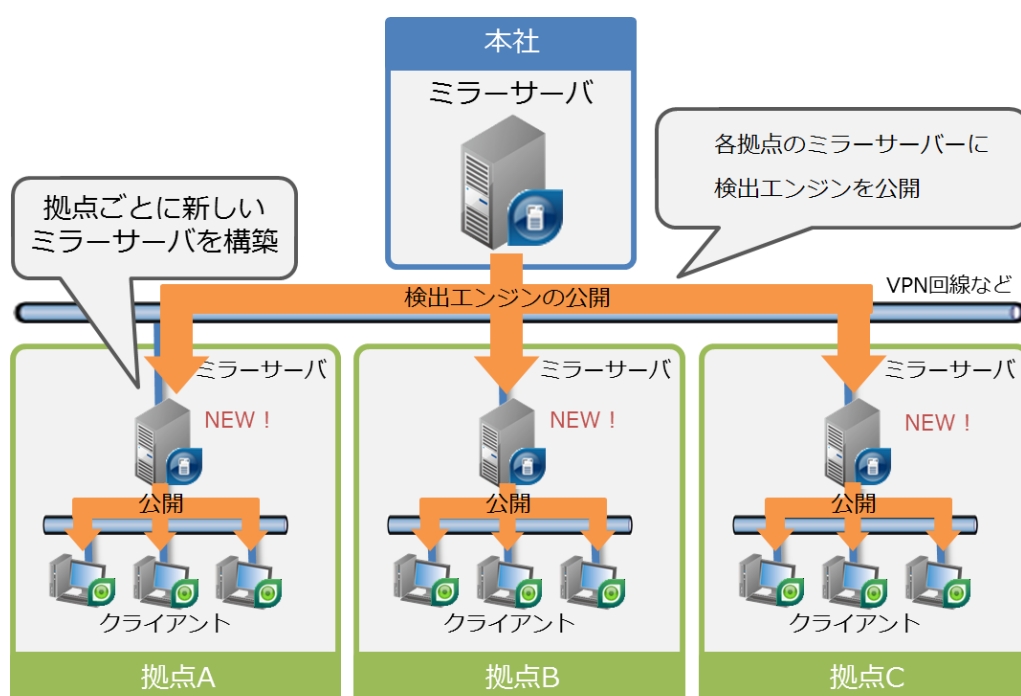


図 8 拠点ごとにミラーサーバーを構築する

項目	説明
特徴	複数の拠点がある場合や拠点間のネットワーク回線が細い場合に最適な方法です。
設定・運用手順	① ミラーサーバーにするコンピュータの検討 ② ミラーサーバーの設定 ③ クライアントのアップデートサーバーを変更 ④ 検出エンジン（ウイルス定義データベース）の配布確認
メリット	検出エンジン（ウイルス定義データベース）のアップデート先が分散されるため、ネットワーク負荷が軽減される
デメリット	拠点ごとに新しいミラーサーバーを構築、管理する必要がある

表 5 回避方法の特徴とメリット、デメリット

方法④ 管理サーバーからアップデートタスクを配布する

検出エンジン（ウイルス定義データベース）のアップデートを自動的におこなわず、ESET Security Management Center（ESET Remote Administrator）から検出エンジン（ウイルス定義データベース）のアップデートタスクを配布することにより、検出エンジン（ウイルス定義データベース）のアップデートをおこないます。

これにより、任意のタイミングで検出エンジン（ウイルス定義データベース）のアップデートをおこなうことが可能です。しかし、自動的にアップデートをおこなう場合に比べ、アップデートタスクの配布操作を手動でおこなう必要があるため管理工数が増加します。具体的な設定手順については、補足資料『8.1 アップデートタスクの配布手順』をご参照ください。

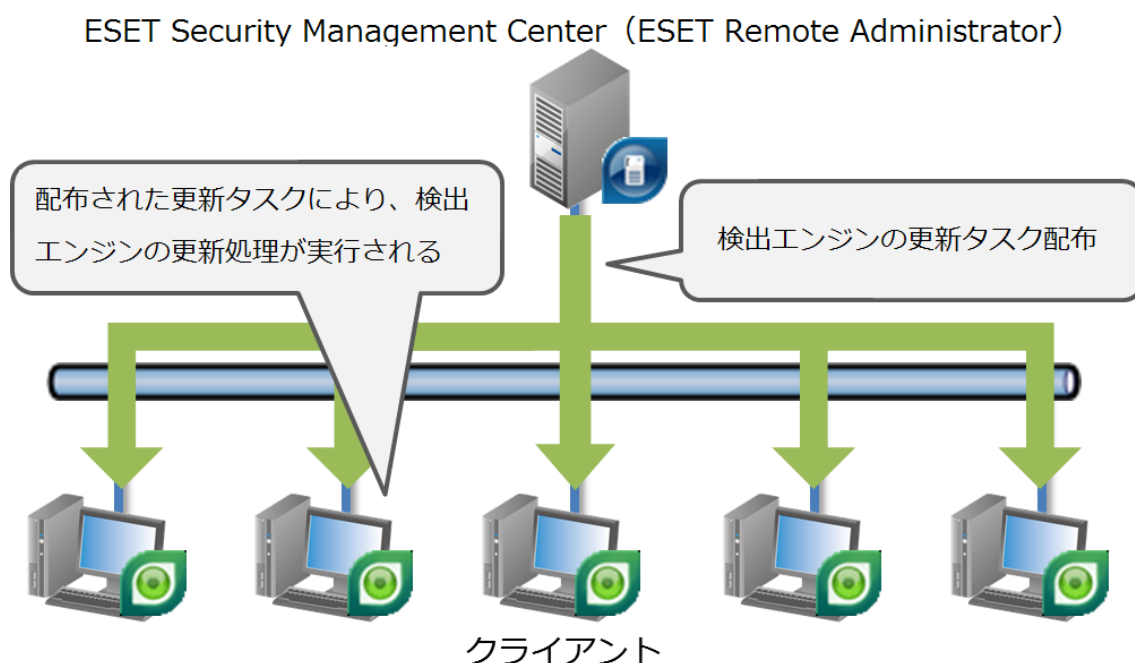


図9 管理サーバーからアップデートタスクを手動で配布する

項目	説明
特徴	一部のクライアントで検証をおこなった後、ベースアップデートをおこないたい場合に最適な方法です。
設定・運用手順	① クライアントのアップデートスケジュールを無効にする ② アップデートタスクの配布 ③ 検出エンジン（ウイルス定義データベース）の配布確認 ④ 定期的に手順②、③を繰り返す
メリット	管理者が任意のタイミングで検出エンジン（ウイルス定義データベース）のアップデートをおこなうことができる
デメリット	アップデートタスクの配布操作を手動で実行する必要があるため、管理工数が増加する

表6 回避方法の特徴とメリット、デメリット

方法⑤ ネットワーク機器を利用し帯域制御をおこなう

ナノアップデートが適用されない環境でベースアップデートが実施された場合、容量の大きな検出エンジン（ウイルス定義データベース）が配信されるため、ネットワークトラフィックが増加します。そのため、ネットワーク機器（帯域制御機能付きルーターやハブなど）を利用し、帯域を制御します。ESET 製品の設定変更をおこなう必要はありませんが、一方で帯域制御するためのハードウェアが必要になります。

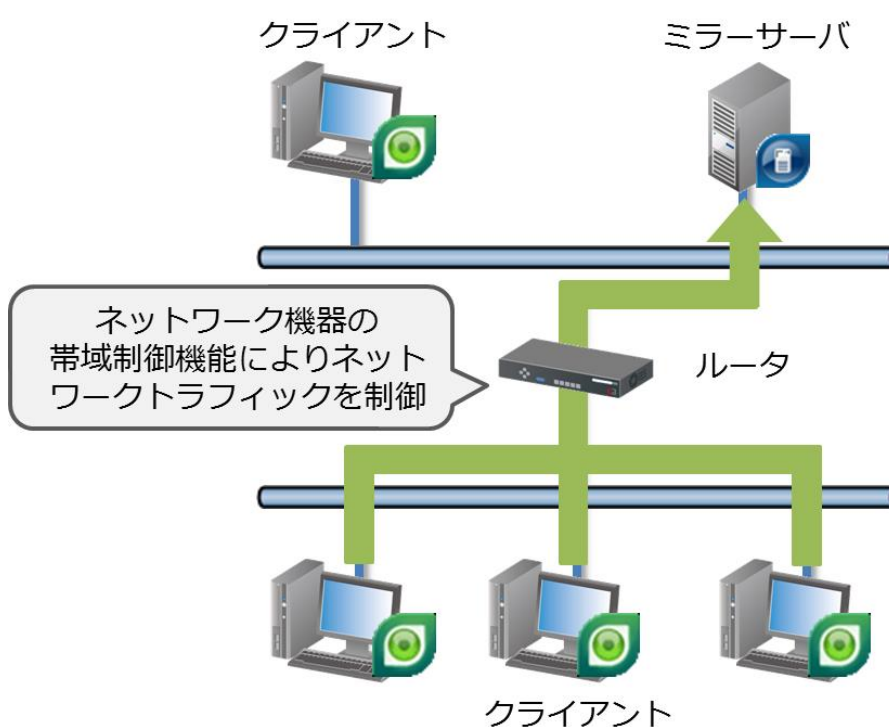


図 10 ネットワーク機器を利用し帯域制御をおこなう

項目	説明
特徴	帯域制限機能に対応したネットワーク機器を準備できる場合や ESET 製品の設定を変更できない場合に最適な方法です。
設定・運用手順	① ネットワーク機器の設置場所を検討 ② ネットワーク機器の設置 ③ 検出エンジン（ウイルス定義データベース）の配布確認
メリット	ESET 製品の設定変更が必要ない
デメリット	ネットワークトラフィックを制御するためのハードウェア（帯域制御機能付きルーターやハブなど）やネットワーク構成の変更が必要

表 7 回避方法の特徴とメリット、デメリット

方法⑥ CD-ROM や USB メモリなどを利用したオフライン更新をおこなう

ナノアップデートが適用されない環境でベースアップデートが実施された場合、通常のアップデートに比べ容量の大きな検出エンジン（ウイルス定義データベース）が配信されるため、ネットワークトラフィックが増加します。そのため、CD-ROM や USB メモリなどを利用し、各クライアントの検出エンジン（ウイルス定義データベース）をアップデートします。CD-ROM や USB メモリ経由で検出エンジン（ウイルス定義データベース）をアップデートするため、ネットワーク負荷がかかりません。具体的な設定手順は、補足資料『8.3 オフライン更新の手順』をご参照ください。

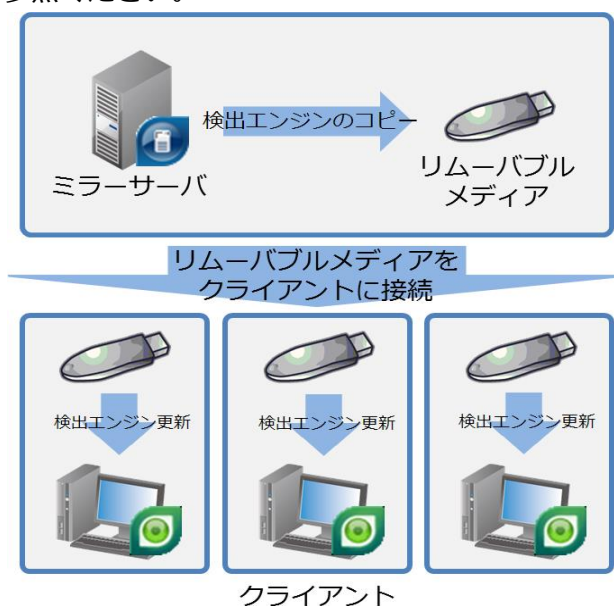


図 11 CD-ROM や USB メモリなどを利用したオフライン更新をおこなう

項目	説明
特徴	社内ネットワークやインターネット回線の帯域が細い場合やネットワークに負荷を与えないで検出エンジン（ウイルス定義データベース）のアップデートをおこなう場合に最適な方法です。
設定・運用手順	① クライアントのアップデートスケジュールを無効化 ② リムーバブルメディアに検出エンジン（ウイルス定義データベース）をコピー ③ クライアントごとに検出エンジン（ウイルス定義データベース）をアップデート
メリット	ネットワークトラフィックが増加しない
デメリット	クライアントごとに検出エンジン（ウイルス定義データベース）のアップデート操作をおこなう必要がある

表 6 回避方法の特徴とメリット、デメリット

以上のように、障害を回避するための方法は複数あります。そのため、各回避方法で説明した特徴およびメリット、デメリットを考慮し、ご使用の環境に最適な設定や運用方法を実施してください。

4.3 障害が発生した場合の対処方法

ここでは、『3.3 ベースアップデート時に発生しやすい障害』で説明したような障害が発生した場合の対処方法について説明します。

『3.3 ベースアップデート時に発生しやすい障害』で説明したような障害が発生した場合、以下のような現象が発生します。

【 発生する現象 】

現象① ミラーサーバーの検出エンジン（ウイルス定義データベース）のアップデートが失敗する

現象② クライアントの検出エンジン（ウイルス定義データベース）のアップデートが失敗する

上記のような現象が発生した場合、以下の項目を確認してください。

現象① ミラーサーバーの検出エンジン（ウイルス定義データベース）のアップデートが失敗する場合

ミラーサーバーの検出エンジン（ウイルス定義データベース）のアップデートが失敗している場合は、はじめにミラーフォルダー（検出エンジンが保存されているフォルダー）に、検出エンジン（ウイルス定義データベース）が正常に保存されているか確認します。

【 検出エンジン（ウイルス定義データベース）ファイルの確認手順 】

手順1 ミラーサーバーを構築しているコンピューターにログインします。

手順2 Explorer から「mirror」フォルダーを開きます。ミラーフォルダーの保存先については、以下の Web ページをご参照ください。

[Q&A] ミラーフォルダーが正しく作成されているか確認するには
https://eset-support.canon-its.jp/faq/show/113?site_domain=business

手順3 手順2 で開いたフォルダーに、数 MB から 40MB 前後（※）の検出エンジン（ウイルス定義データベース）ファイルが作成されていることを確認します。

ファイルが作成されている場合は、ミラーサーバー用の検出エンジン（ウイルス定義データベース）が正常にダウンロードされています。一方、ファイルが作成されていない場合は、ミラーサーバー用の検出エンジン（ウイルス定義データベース）のダウンロードに失敗している可能性があります。

※ サイズは、実施されたベースアップデートによって異なります。

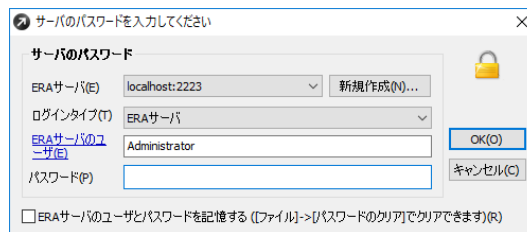
検出エンジン（ウイルス定義データベース）が正常に格納されていない場合は、検出エンジン（ウイルス定義データベース）を再度ダウンロードします。

以下に、ESET Remote Administrator V5.3 でミラーサーバーを構築している場合の手順を説明します。

なお、ESET File Security for Microsoft Windows Server を使用してミラーサーバーを構築している場合は、以下の手順 1～4 を実行した後、手動で検出エンジン（ウイルス定義データベース）のアップデートをおこなってください。

【 検出エンジン（ウイルス定義データベース）の再ダウンロード手順（ESET Remote Administrator V5.3 の場合） 】

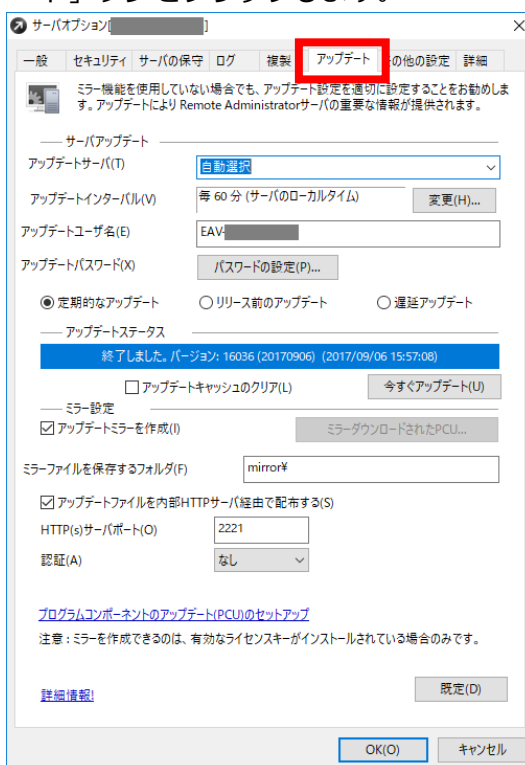
- 手順1 Explorer を起動し、検出エンジン（ウイルス定義データベース）が保存されるフォルダーを開きます。
- 手順2 手順 1 で開いたフォルダー内のファイルをすべて削除します。
- 手順3 手順 1 と同様に、Explorer を起動し、ミラーフォルダーを開きます。
- 手順4 手順 3 で開いたフォルダー内のファイルをすべて削除します。
- 手順5 ESET Remote Administrator Console を起動します。
- 手順6 ログイン画面で、ログインに必要な情報（パスワードなど）を設定し、ESET Remote Administrator Server にログインします。



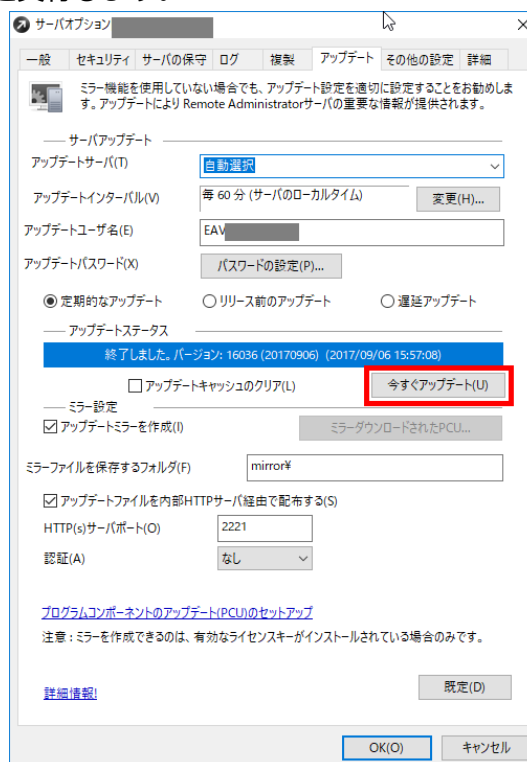
手順7 メニュー「ツール」 - 「サーバオプション」の順に選択し、「サーバオプション」ダイアログを表示します。



手順8 「アップデート」タブをクリックします。

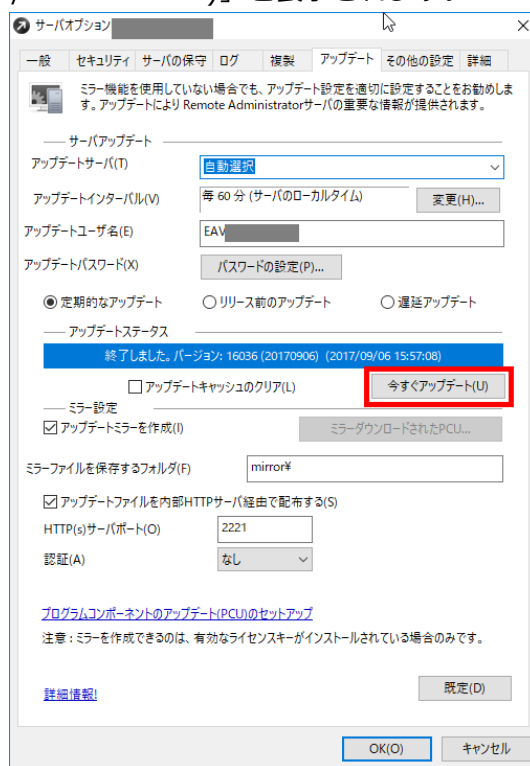


- 手順9 「アップデート用ユーザ名」および「アップデートパスワード」にユーザー名、パスワードが正しく入力されていることを確認します。
- 手順10 「アップデートミラーを作成」または「ミラーを作成する」チェックボックスが有効になっていることを確認します。
- 手順11 「今すぐアップデート」または「定義データベースのアップデート」ボタンをクリックし、検出エンジン（ウイルス定義データベース）のアップデートを実行します。



- 手順12 検出エンジン（ウイルス定義データベース）のダウンロードが開始されます。

- 手順13 検出エンジン（ウイルス定義データベース）が正常に完了した場合、「アップデートステータス」に「終了しました。バージョン：XXXX（20XX/XX/XX XX:XX:XX）」と表示されます。



- 手順14 [OK] ボタンをクリックし、ダイアログを閉じます。

以上で、検出エンジン（ウイルス定義データベース）の再ダウンロードが完了しました。

また、検出エンジン（ウイルス定義データベース）が正常に格納されている場合は、ネットワーク上の問題など複数の要因が考えられます。

そのため、製品 Q&A ページ (<https://eset-info.canon-its.jp/support/>) をご参照いただいたうえで、製品購入時にご案内させていただいた問い合わせ先にご連絡ください。

現象② クライアントの検出エンジン（ウイルス定義データベース）のアップデートが失敗する場合

クライアントの検出エンジン（ウイルス定義データベース）のアップデートが失敗する場合、ミラーサーバーに検出エンジン（ウイルス定義データベース）のアップデート接続が集中し、検出エンジン（ウイルス定義データベース）のアップデートに失敗している可能性があります。時間をおいて、再度検出エンジン（ウイルス定義データベース）のアップデートが成功するかご確認ください。

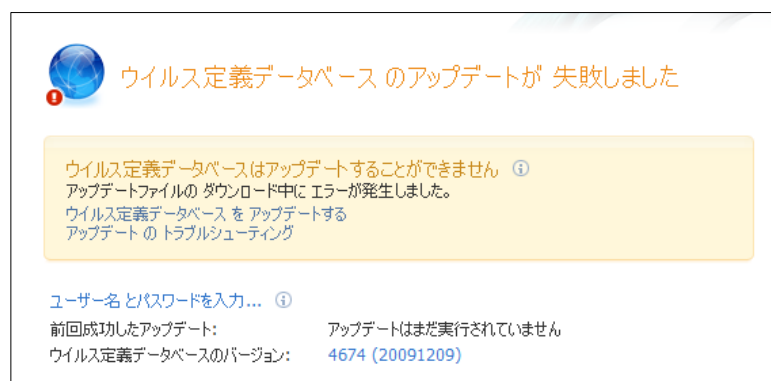


図 12 検出エンジン（ウイルス定義データベース）のアップデートが失敗した場合の画面

もし、上記対処方法を実行した後も現象が改善されない場合は、弊社製品 Web ページ (<https://eset-info.canon-its.jp/>) に記載されている重要なお知らせおよび、製品 Q&A ページ (<https://eset-info.canon-its.jp/support/>) をご参照いただいた上で、製品購入時にご案内させていただいたお問い合わせ先にご連絡ください。

5 ケース別設定事例

この章では、3つの環境を例にナノアップデートが適用されない環境でベースアップデートが実施された場合に発生しやすい障害の回避方法の設定例を説明します。

5.1 同じ時間帯に検出エンジン（ウイルス定義データベース）をアップデートしている場合

ここでは、同じ時間に各クライアントの検出エンジン（ウイルス定義データベース）をアップデートしている場合の設定例について説明します。

【 検出エンジン（ウイルス定義データベース）のアップデート方法 】

- 1台のミラーサーバーで検出エンジン（ウイルス定義データベース）のアップデートをおこなっている
- 各クライアントはミラーサーバーに接続し、検出エンジン（ウイルス定義データベース）をアップデートしている（ESET社のアップデートサーバーからアップデートをおこなっていない）
- 各クライアントのアップデート時間は、毎日12:00に実行している

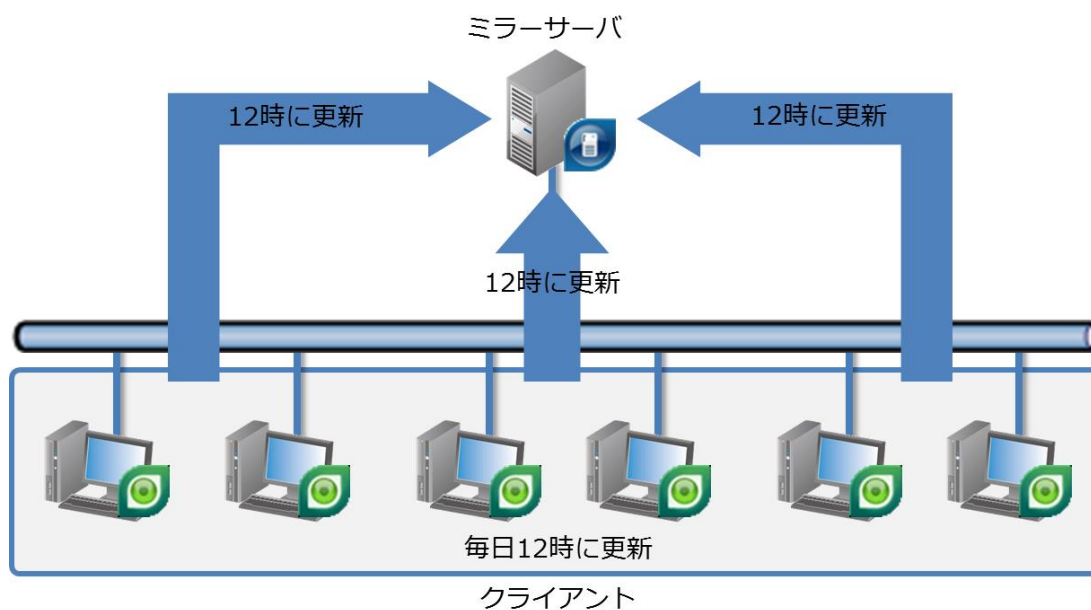


図 13 システム構成

各クライアントの検出エンジン（ウイルス定義データベース）のアップデートを、同じ時間帯に実行している場合、ベースアップデートが実行されると以下の障害が発生する可能性があります。

【 発生しやすい障害 】

- ネットワークトラフィックが増加し、ネットワーク速度が低下する
- ミラーサーバーに負荷がかかる
- 各クライアントの検出エンジン（ウイルス定義データベース）のアップデートに失敗する

以上のように、障害を発生させないためには、各クライアントの検出エンジン（ウイルス定義データベース）のアップデート時間を変更する方法や Internet Information Server（IIS）を利用する方法があります。

ここでは、各クライアントをいくつかのグループに分け、グループごとに異なる時間帯に検出エンジン（ウイルス定義データベース）のアップデートをおこなう設定手順（『4.2 障害の回避方法』 - 『方法①クライアントのアップデート時間を分散する』）について説明します。

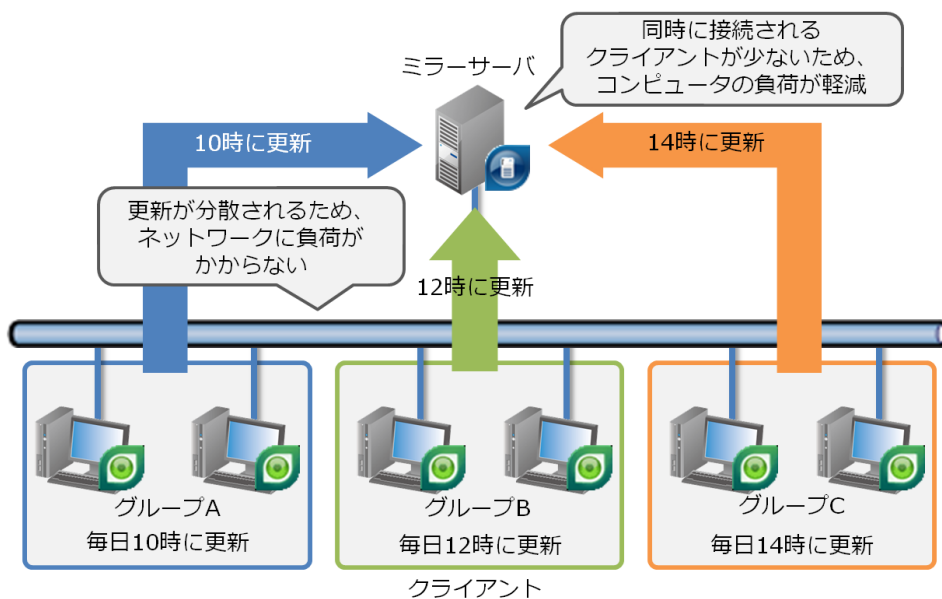


図 14 各クライアントのアップデート処理を分散する

各クライアントをいくつかのグループに分け、グループごとに異なる時間帯に検出エンジン（ウイルス定義データベース）のアップデートをおこなう場合、以下の手順でおこないます。

【 検出エンジン（ウイルス定義データベース）のアップデート方法 】

- ① 各クライアントのグループ分け
- ② 各グループのアップデート時間を決定
- ③ グループごとにアップデート時間を変更
- ④ 検出エンジン（ウイルス定義データベース）のアップデート確認

- ① 各クライアントのグループ分け
各クライアントをいくつかのグループに分けます。グループの分け方は、ご使用のクライアント数やご利用の環境（クライアントの場所や組織など）によって異なります。できるだけ管理しやすい単位でグループ分けをおこなってください。
- ② 各グループのアップデート時間を決定
次に、各グループのアップデート時間を決定します。アップデート時間は、できるだけグループごとのアップデート処理が重ならないように設定します。
- ③ グループごとにアップデート時間を変更
次に、クライアントの検出エンジン（ウイルス定義データベース）のアップデート時間を変更します。アップデート時間を変更するには、ESET Security Management Center（ESET Remote Administrator）から設定変更タスクを配布する方法と各クライアントの設定画面から直接アップデートスケジュールを変更する方法があります。
- ④ 検出エンジン（ウイルス定義データベース）のアップデート確認
最後に、設定した時間帯に各クライアントの検出エンジン（ウイルス定義データベース）が正常にアップデートされることを確認します。

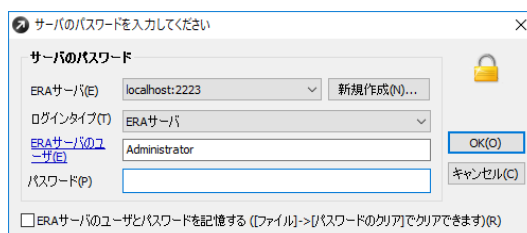
【 検出エンジン（ウイルス定義データベース）のアップデート方法 】

- ESET Security Management Center（ESET Remote Administrator）から設定変更タスクを配布する
- 各クライアントの設定画面から直接アップデートスケジュールを変更する

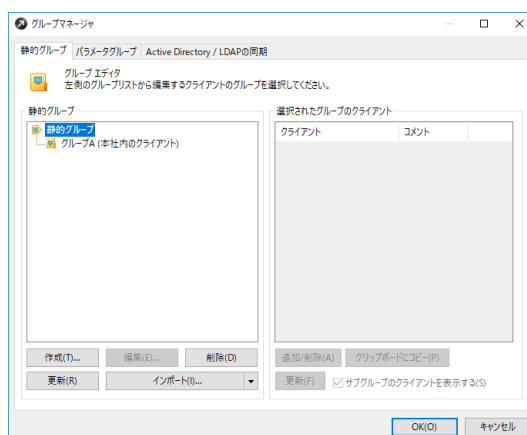
本資料では、ESET Remote Administrator V5.3 から設定変更のタスクを配布する方法について説明します。なお、各クライアントの設定画面からアップデートスケジュールを変更する場合は、補足資料『8.5 クライアントの設定画面からアップデートスケジュールを変更する手順』をご参照ください。

【 ESET Remote Administrator V5.3 から設定変更タスクを配布する手順 】

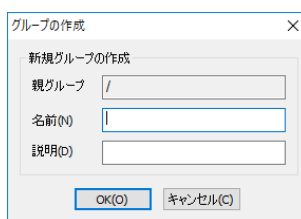
- 手順1 ESET Remote Administrator Console を起動します。
- 手順2 ログイン画面で、ログインに必要な情報（パスワードなど）を入力し、ESET Remote Administrator Server にログインします。



- 手順3 メニュー「ツール」 - 「グループマネージャ」をクリックし、「グループマネージャ」を起動します。

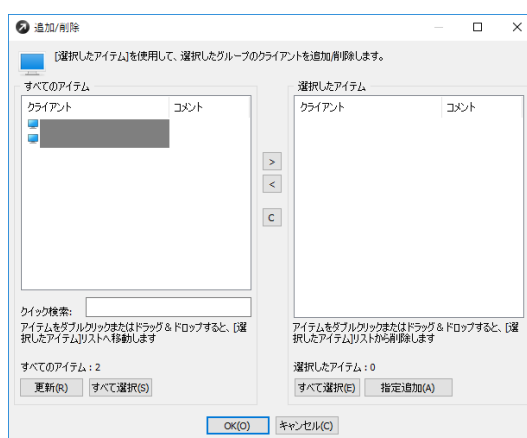


- 手順4 [作成] ボタンをクリックし、「グループの作成」ダイアログを開きます。

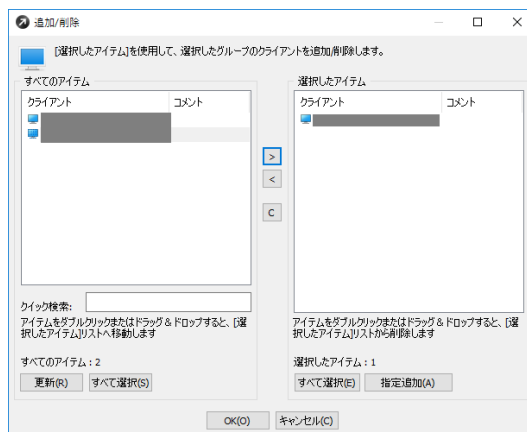


- 手順5 「名前」と「説明」に、グループ名とグループの説明を入力し、[OK] ボタンをクリックします。

- 手順6 手順 5 で作成したグループを選択し、[選択されたグループのクライアント] の [追加/削除] ボタンをクリックします。「追加/削除」ダイアログが表示されます。



- 手順7 「追加/削除」ダイアログの「すべてのアイテム」からグループに追加するクライアントを選択し、[>] または [>>] ボタンをクリックします。「選択したアイテム」に選択したクライアントが移動します。

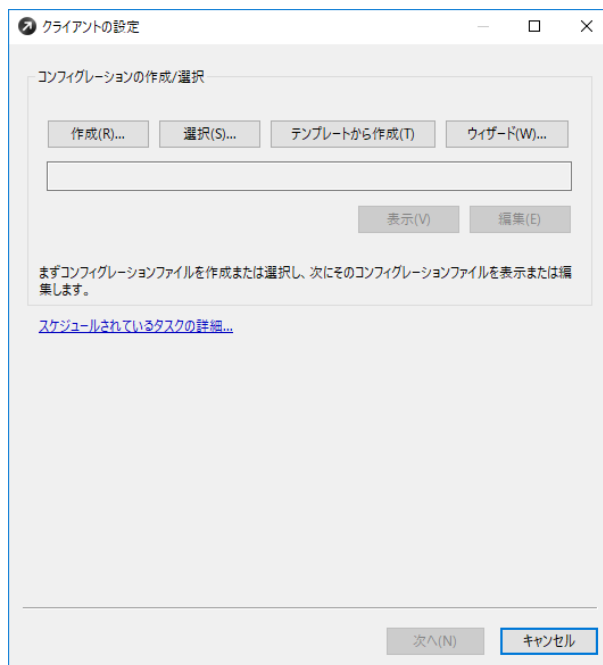


- 手順8 [OK] ボタンをクリックし、クライアントをグループに追加します。
- 手順9 作成するグループの数だけ、手順4～8までの操作を繰り返し、グループの作成とクライアントの追加をおこないます。最後に、[OK] ボタンをクリックし、ダイアログを閉じます。
以上で、グループの作成とクライアントの追加が完了しました。

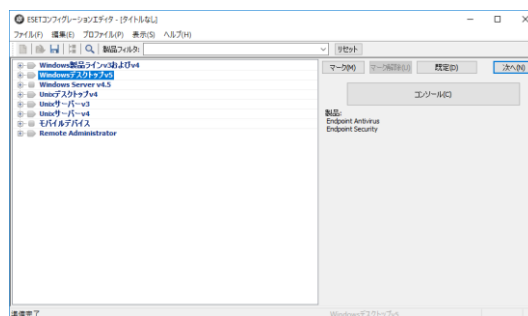
次に、各クライアントの検出エンジン（ウイルス定義データベース）のアップデート時間を変更します。なお、以下の手順では、既定の検出エンジン（ウイルス定義データベース）のアップデートスケジュールを毎日 12:00 におこなうように変更する場合の手順を説明します。

- 手順10 メニュー「表示」 - 「[クライアント] ペイン」の順にクリックし、クライアントペインを表示し、任意のクライアントを選択します。

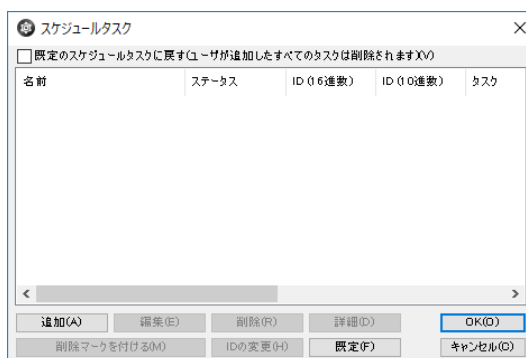
- 手順11 メニュー「アクション」-「新規タスク」-「コンフィグレーションタスク」または「コンフィグレーション」の順にクリックし、クライアントの設定ダイアログを表示します。



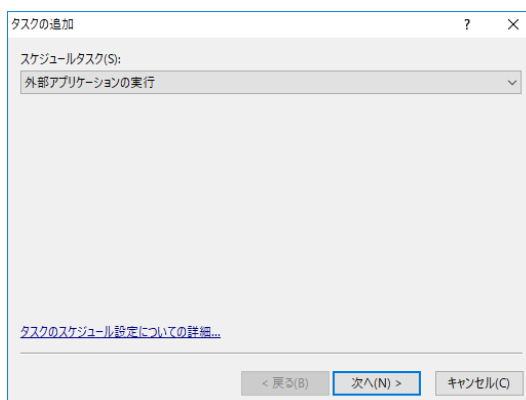
- 手順12 「コンフィグレーションの作成/選択」にある「作成」ボタンをクリックし、ESET コンフィグレーションエディタを起動します。



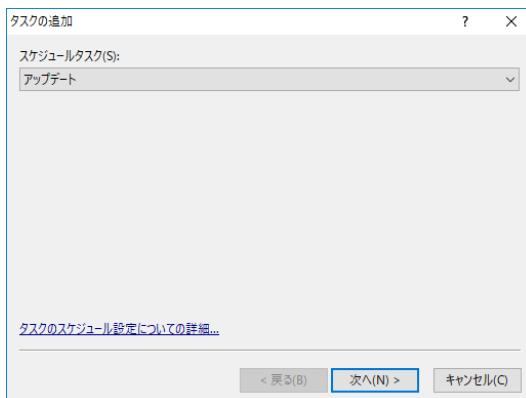
- 手順13 「Windows デスクトップ v5」 - 「カーネル」 - 「設定」 - 「スケジューラ/プランナー」 - 「スケジューラ/プランナー」の順にクリックし、画面左の [編集] ボタンをクリックします。「スケジュールタスク」ダイアログが表示されます。



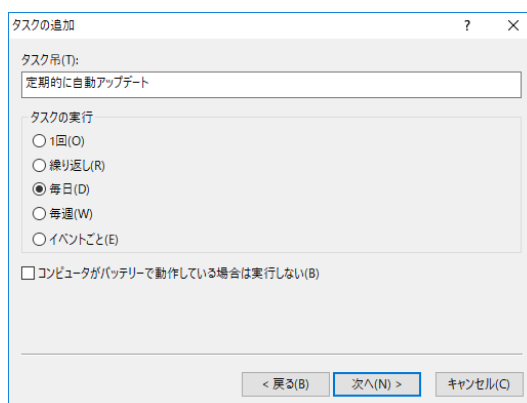
- 手順14 [追加] ボタンをクリックし、「タスクの追加」ウィザードを起動します。



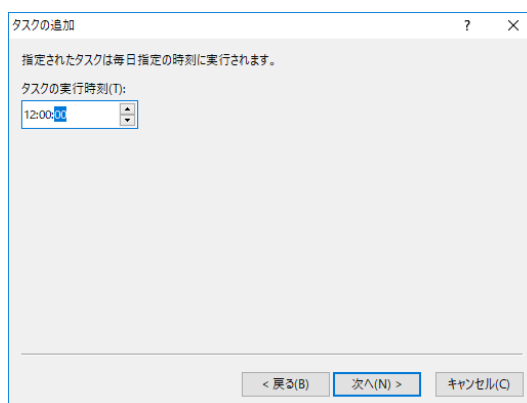
- 手順15 「スケジューラタスク」から「アップデート」を選択し、[次へ] ボタンをクリックします。



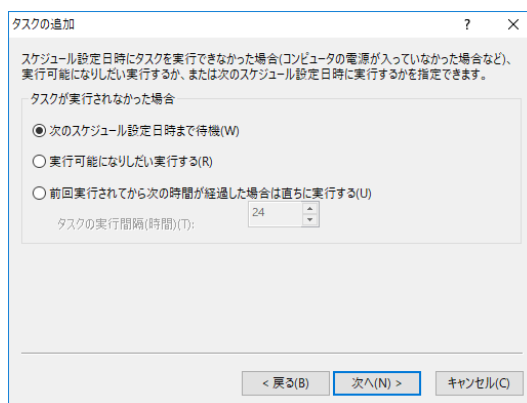
- 手順16 「タスク名」テキストボックスに、「定期的に自動アップデート」と入力し、「タスクの実行」から「毎日」を選択した後、[次へ] ボタンをクリックします。



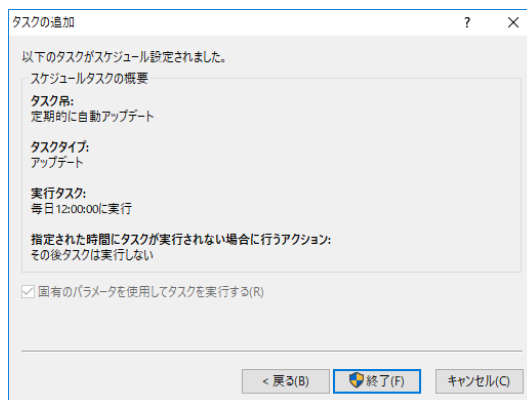
- 手順17 「タスクの実行時間」の値を「12:00」に変更し、[次へ] ボタンをクリックします。



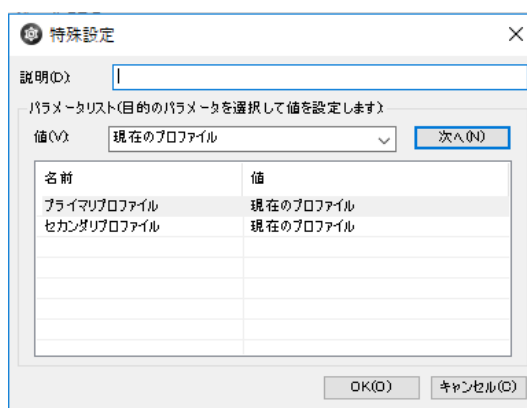
- 手順18 検出エンジン（ウイルス定義データベース）のアップデートが実行される時間に、コンピューターが起動していないなど、アップデート処理を実行できなかった場合の動作を選択し、[次へ] ボタンをクリックします。



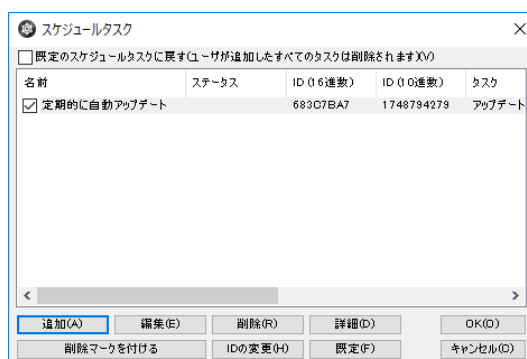
手順19 「スケジュールタスクの概要」に表示されている内容を確認し、[終了] ボタンをクリックします。



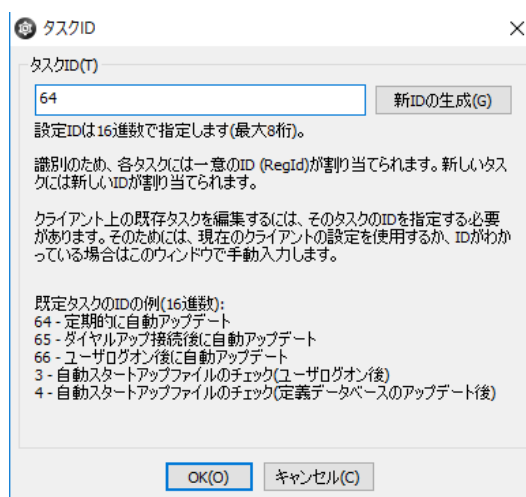
手順20 表示された「特殊設定」ダイアログが表示された場合は、[OK] ボタンをクリックします。



手順21 [IDの変更] ボタンをクリックします。

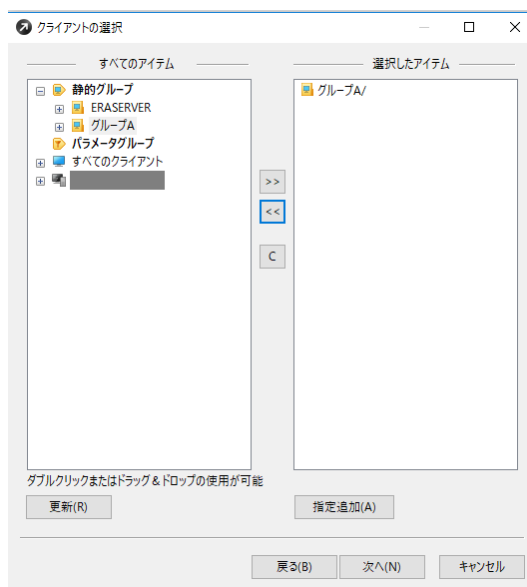


- 手順22 表示された「タスク ID」ダイアログのテキストボックスに“64”（既定で設定されているアップデートタスク“定期的に自動アップデート”の ID）を入力し、[OK] ボタンをクリックします。



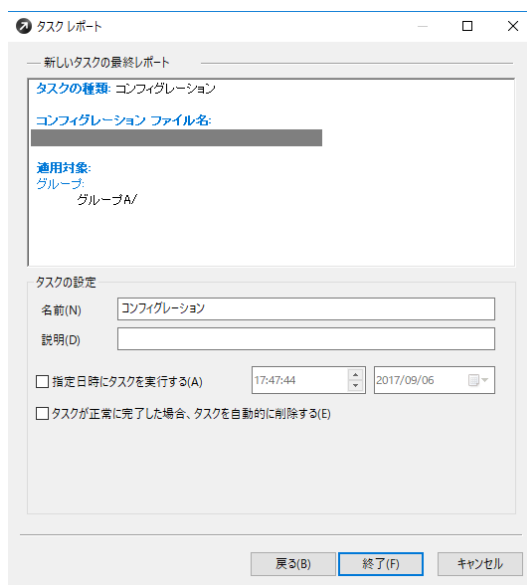
- 手順23 [OK] ボタンをクリックし、「スケジュールタスク」ダイアログを閉じます。
- 手順24 メニュー「ファイル」 - 「終了」の順に選択します。
- 手順25 保存の確認メッセージが表示された場合は、[はい] ボタンをクリックします。
- 手順26 「クライアントの設定」ダイアログの [次へ] ボタンをクリックします。

手順27 「クライアントの選択」ダイアログで、アップデート時間を変更するグループを選択し、[>>] ボタンをクリックします。右の「選択したグループ」に、グループ名が表示されます。



手順28 [次へ] ボタンをクリックします。

手順29 「新しいタスクの最終レポート」に表示されている値を確認し、[終了] または [完了] ボタンをクリックします。検出エンジン（ウイルス定義データベース）のアップデートタスクが配布されます。



手順30 メニュー「表示」 - 「[タスク] ペイン」の順にクリックします。

手順31 手順 29 で配布したタスクの状態を確認し、タスクの状態が“終了”になるまで待機します。
タスクの状態が“終了”と表示されると、クライアントの検出エンジン（ウイルス定義データベース）の設定変更が完了します。

以上で、ESET Remote Administrator V5.3 からの設定変更タスク配布が完了しました。

以上で、すべての設定が完了しました。

5.2 1 台のミラーサーバーで多数のクライアントがアップデートする場合

ここでは、1 台のミラーサーバーで多数のクライアントがアップデートする場合の設定変更例について説明します。

【システム構成例】

- ミラーサーバー1 台で、多くのクライアントの検出エンジン（ウイルス定義データベース）をアップデートしている

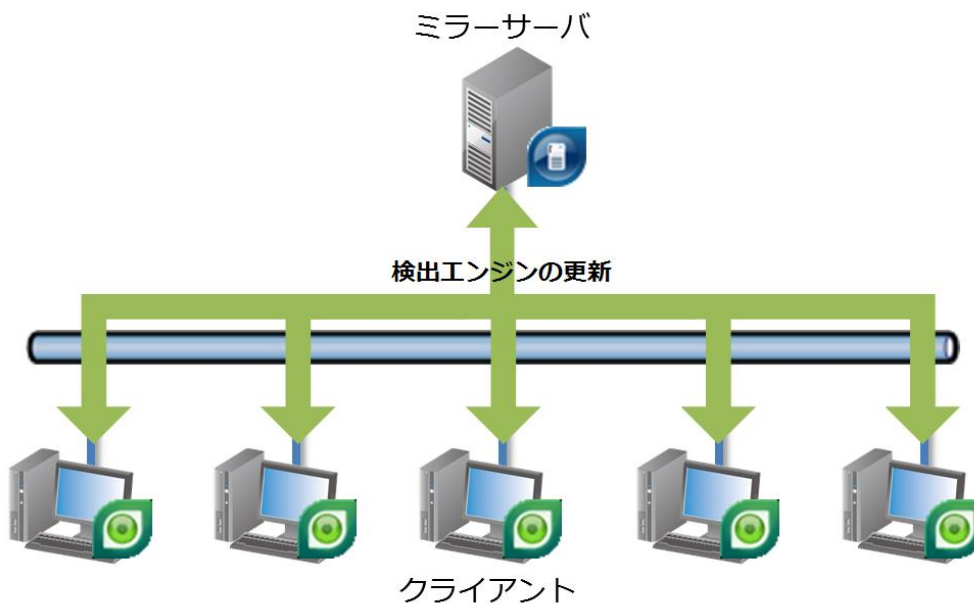


図 15 システム構成

1 台のミラーサーバーで、多数のクライアントが検出エンジン（ウイルス定義データベース）をアップデートしている場合、ベースアップデート時に以下の障害が発生する可能性があります。

【発生しやすい障害】

- ネットワークトラフィックが増加し、ネットワーク速度が遅くなる
- ミラーサーバーに負荷がかかる
- 各クライアントの検出エンジン（ウイルス定義データベース）のアップデートが失敗する

以上のような障害を発生させないためには、Internet Information Server (IIS) を利用して検出エンジン（ウイルス定義データベース）を配布する方法やクライアントをいくつかのグループに分け、検出エンジン（ウイルス定義データベース）のアップデート時間帯を分散させる方法必要があります。

ここでは、Windows Server に標準で実装されている Internet Information Service 7.0 (IIS) を使用して、検出エンジン (ウイルス定義データベース) を配布する方法 (『4.2 障害の回避方法』 - 『方法②IIS サーバーを構築し、検出エンジン (ウイルス定義データベース) を

公開する』) について説明します。

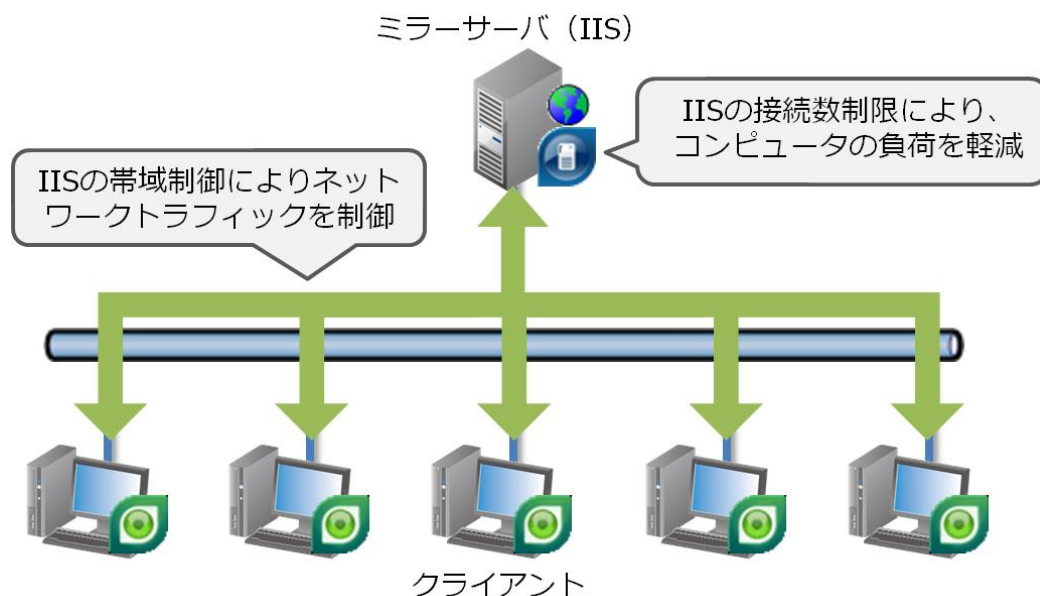


図 16 IIS サーバーを構築し、検出エンジン (ウイルス定義データベース) を配布する

IIS サーバーを使用して検出エンジン (ウイルス定義データベース) の配布をおこなう場合、以下の手順でおこないます。

【 設定変更手順 】

- ① IIS サーバーを構築
- ② 既定のミラーサーバーを停止
- ③ 仮想 WEB ページの設定
- ④ 検出エンジン (ウイルス定義データベース) のアップデート確認

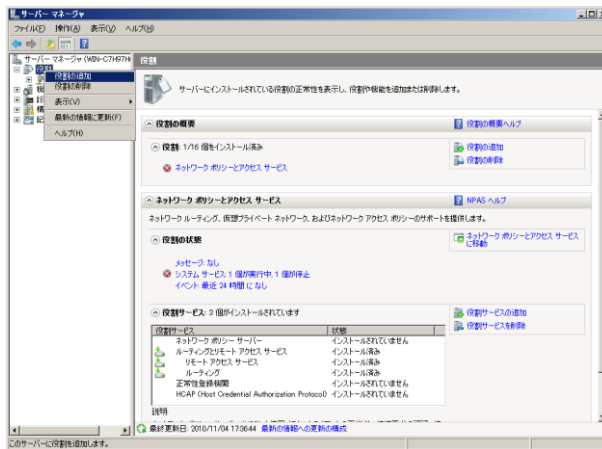
① IIS サーバーを構築

はじめに、Internet Information Service 7.0 (IIS) を構築します。IIS の構築をおこなうには、以下の手順に従って、構築をおこなってください。

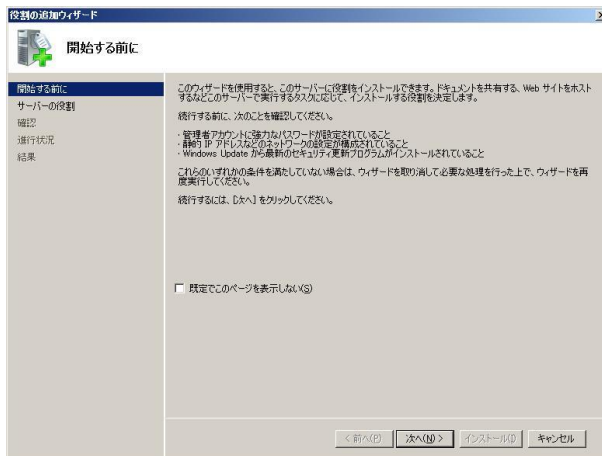
【 IIS サーバーの構築手順 】

手順1 「スタート」-「管理ツール」-「サーバマネージャ」の順に選択し、サーバマネージャを起動します。

手順2 サーバマネージャ左にあるツリーから、「役割」を右クリックし、表示されたメニューから「役割の追加」を選択します。



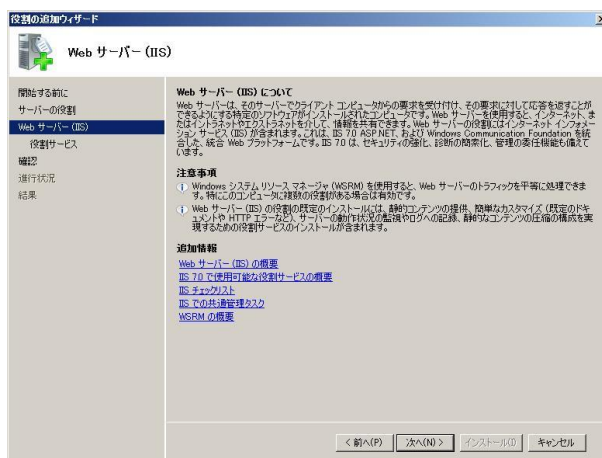
手順3 表示されたサーバマネージャ画面左の「役割」を右クリックし、メニューから「役割の追加」をクリックします。「役割の追加ウィザード」画面が起動します。



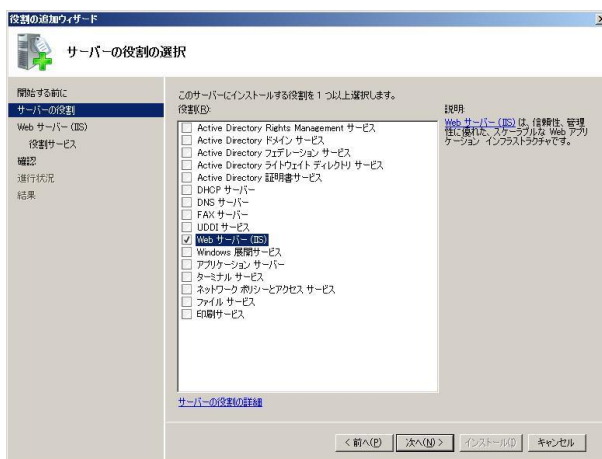
手順4 [次へ] ボタンをクリックします。

手順5 「サーバの役割の選択」画面から「Web サーバー (IIS) 」を選択し、[次へ] ボタンをクリックします。

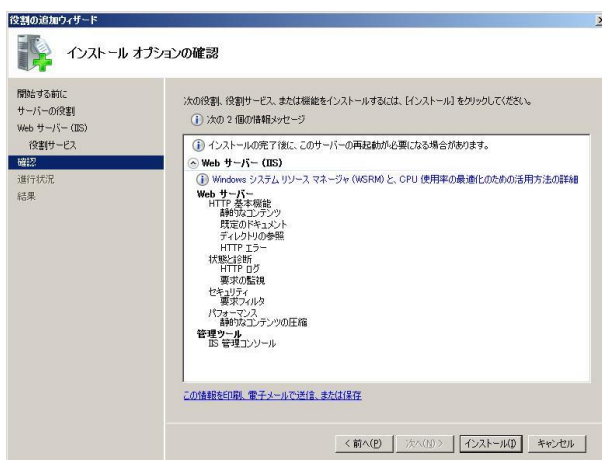
手順6 「Web サーバ (IIS)」画面で、[次へ] ボタンをクリックします。



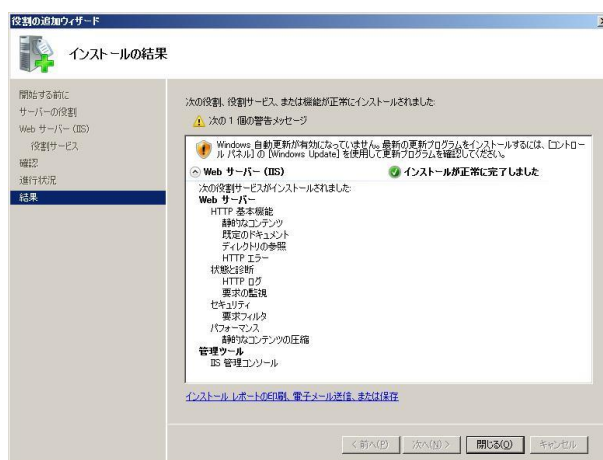
手順7 「役割サービスの選択」画面で、[次へ] ボタンをクリックします。



手順8 「インストールオプションの確認」画面で、内容を確認し、[インストール] ボタンをクリックし、IIS のインストールをおこないます。



- 手順9 以下の画面が表示されたら、IIS のインストールが完了します。[閉じる] ボタンをクリックし、ウィザードを閉じます。

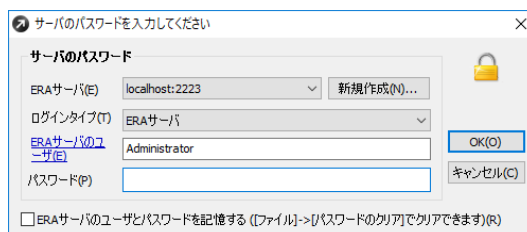


以上で、IIS サーバーの構築が完了しました。

- ② 既定のミラーサーバーを停止
次に、現在使用しているミラーサーバーを停止します。ここでは、ESET Remote Administrator Server V5.3 でミラーサーバーを構築している場合の手順を説明します。
ESET File Security for Microsoft Windows Server でミラーサーバーを構築している場合は、補足資料『8.7 ESET File Security for Microsoft Windows Server を利用したミラーサーバー構築手順』を参考にミラーサーバーを停止してください。

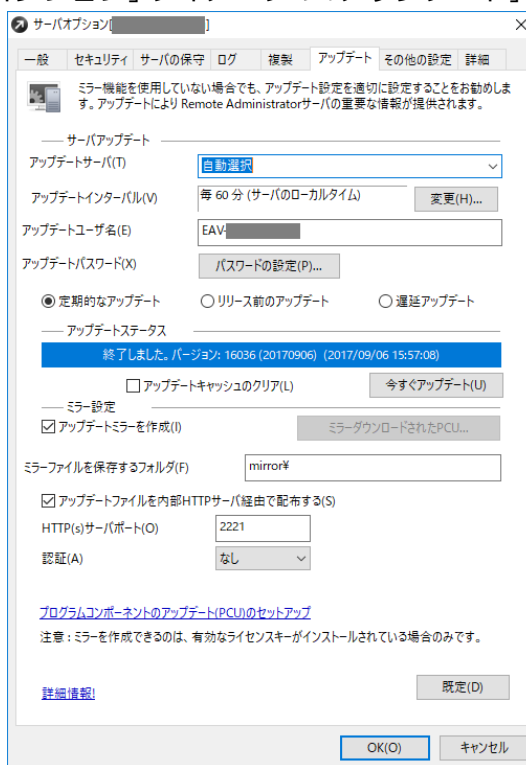
【ミラーサーバーの停止手順】

- 手順1 ESET Remote Administrator Console を起動します。
- 手順2 ログイン画面で、ログインに必要な情報（パスワードなど）を入力し、ESET Remote Administrator Server にログインします。

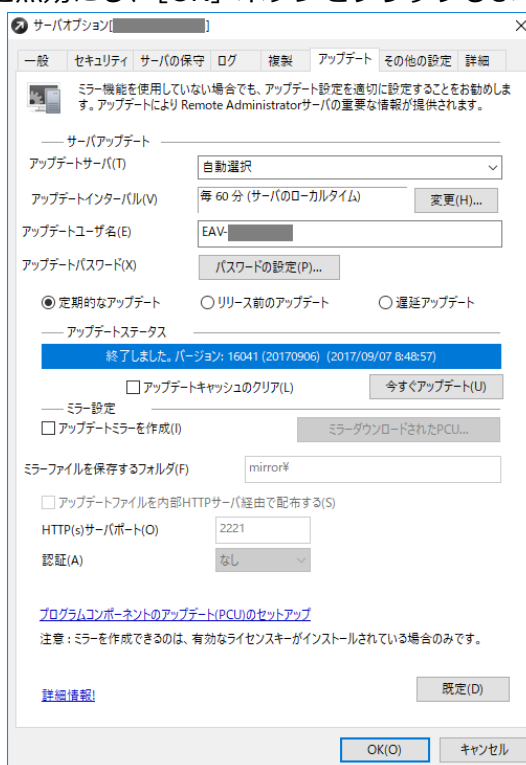


- 手順3 メニュー「ツール」 - 「サーバオプション」の順にクリックし、「サーバオプション」ダイアログを表示します。

手順4 「サーバオプション」ダイアログの「アップデート」タブを選択します。



手順5 「アップデートファイルを内部 HTTP サーバ経由で配布する」チェックボックスを無効にし、[OK] ボタンをクリックします。



手順6 ESET Remote Administrator Console を閉じます。

以上で、ミラーサーバーが停止しました。

③ 仮想 WEB ページの設定

次に、仮想 WEB ページの設定をおこないます。仮想 WEB ページを作成するには、以下の手順で操作をおこなってください。

【仮想 WEB ページの設定手順】

手順1 「スタート」-「管理ツール」-「インターネットインフォメーションサービス (IIS) マネージャ」の順に選択し、サーバマネージャを起動します。

手順2 インターネットインフォメーションサービス (IIS) マネージャのツリーから、「役割」-「Web サーバ」-「インターネットインフォメーションサービス (IIS) マネージャ」を選択します。

手順3 表示された画面左のツリーからご使用のサーバー名を選択し、「Web サイトの追加」を選択します。

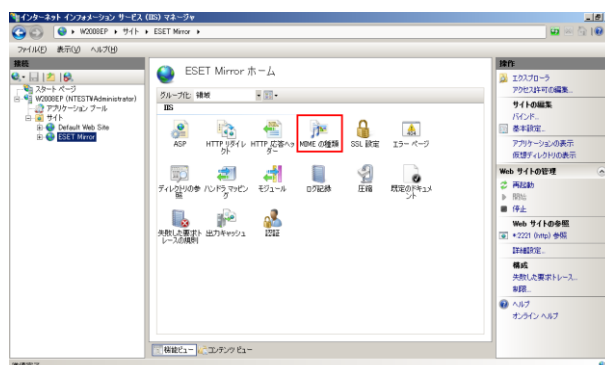
手順4 「Web サイトの追加」ダイアログが表示されたら、以下の値を入力します。



設定	値
サイト名	ESET Mirror
物理パス	Mirror フォルダ 既定では、“C:\ProgramData\ESET\ESET remote Administrator\Server\mirror”に作成されます。
種類	http
IP アドレス	未使用の IP アドレスすべて
ポート	2221
ホスト名	空白

表 7 「Web サイトの追加」ダイアログの設定

手順5 手順4で作成した Web サイト“ESET Mirror”を選択し、画面右に表示されている項目から「MIMEの種類」をダブルクリックします。



手順6 画面右の「追加」ボタンをクリックします。

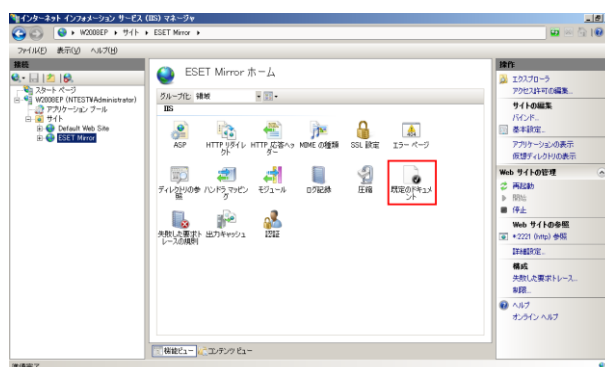
手順7 「MIMEの種類の追加」ダイアログが表示されたら、以下の設定をおこないます。



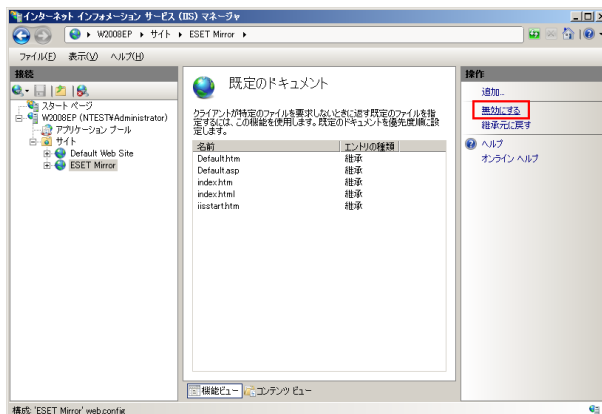
設定	値
ファイル名の拡張子	*
MIMEの種類	application/octet-stream

表 8 「MIMEの種類の追加」の設定

手順8 手順5と同様に、手順4で作成した Web サイト“ESET Mirror”を選択し、画面右に表示されている項目から「既定のドキュメント」をダブルクリックします。



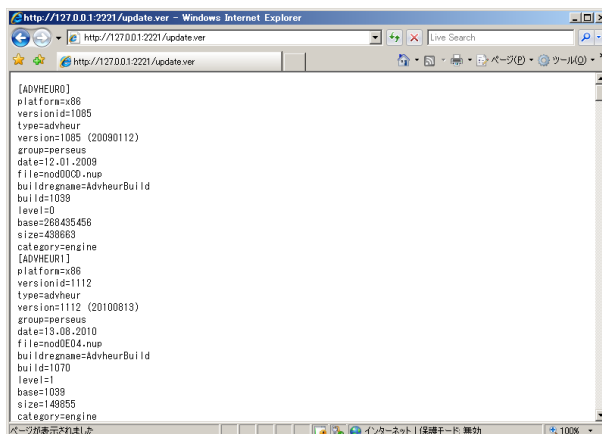
手順9 画面左の「操作」から「無効にする」をクリックします。



手順10 Internet Explorer を起動し、URL に以下のアドレスを入力します。

URL:http://アップデートサーバーの IP アドレス:2221/update.ver

手順11 Internet Explorer に以下のような画面が表示されることを確認します。



以上で、Web ページの設定が完了しました。

- ④ 検出エンジン（ウイルス定義データベース）のアップデート確認
最後に、クライアントから検出エンジン（ウイルス定義データベース）がアップデートできることを確認します。具体的な検出エンジン（ウイルス定義データベース）のアップデート手順は、補足資料『8.4 検出エンジン（ウイルス定義データベース）のアップデート手順』を参照してください。

5.3 拠点間のネットワーク帯域が細い場合

ここでは、拠点間のネットワーク帯域が細い環境で ESET 製品をご使用場合の設定変更例について説明します。

【システム構成例】

- 各拠点のクライアントは、本社のミラーサーバーに接続し、検出エンジン（ウイルス定義データベース）をアップデートしている
- 各拠点とミラーサーバー間のネットワークは帯域が細い（帯域の細いVPN回線やISDN回線を利用）

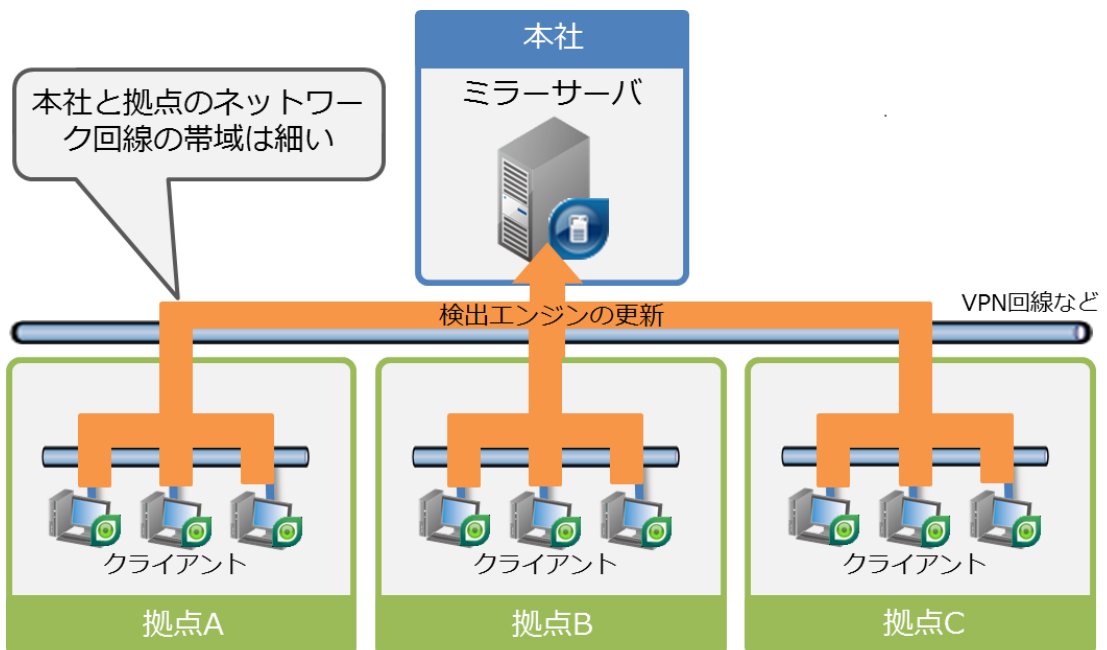


図 17 システム構成

ネットワーク帯域が細い回線を経由して検出エンジン（ウイルス定義データベース）のアップデートをおこなっている場合、ベースアップデート時に、以下のような障害が発生する可能性があります。

【発生しやすい障害】

- ネットワークトラフィックが増加し、クライアントのアップデートに失敗する
- 他のアプリケーションから、他拠点への通信ができなくなる

以上のような障害を発生させないためには、各クライアントでオフライン更新をおこなう方法や拠点ごとにミラーサーバーを構築し、拠点間のネットワークトラフィックを減らす必要があります。

ここでは、拠点ごとにミラーサーバーを構築する方法（『4.2 障害の回避方法』 - 『方法③拠点ごとにミラーサーバーを構築し、アップデートサーバーを分散する』）について説明します。

拠点ごとにミラーサーバーを構築するには、以下の手順でおこないます。

【 設定の変更手順 】

- ① ミラーサーバーを設置する場所の決定
 - ② ミラーサーバーの構築
 - ③ クライアントのアップデートサーバーを変更
 - ④ 検出エンジン（ウイルス定義データベース）のアップデート確認
-
- ① ミラーサーバーを設置する場所の決定
はじめに、ミラーサーバーを設置する場所を決定します。拠点ごとに設置するなど、なるべくネットワークに負荷がかからない場所にミラーサーバーを構築します。

 - ② ミラーサーバーの構築
次に、ミラーサーバーを構築します。ミラーサーバーは、以下のサーバー・クライアント用プログラムがインストールされているコンピューター、または、ツールがダウンロードされているコンピューターで構築することが可能です。

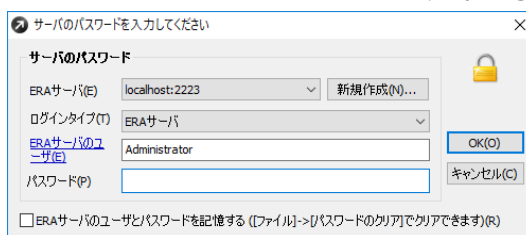
【 ミラーサーバーを構築できる製品 】

- ESET Remote Administrator Server V5.3
- ESET File Security for Microsoft Windows Server V4.5 以降
- ESET File Security for Linux V4.0 以降
- ESET Endpoint Security V6.2 以降
- ESET Endpoint アンチウイルス V5.0 以降
- ミラーツール

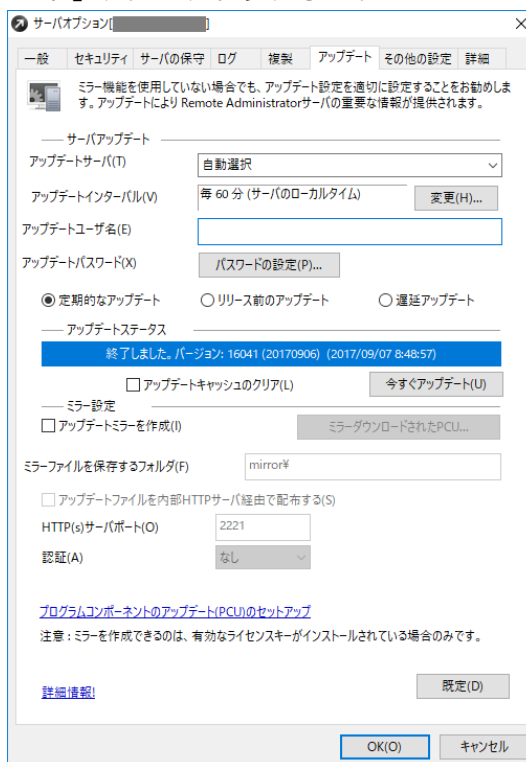
ここでは、ESET Remote Administrator Server V5.3 を利用してミラーサーバー（HTTP）を構築する手順を説明します。なお、ESET File Security for Microsoft Windows Server を利用して、ミラーサーバーを構築する場合は、補足資料『8.7 ESET File Security for Microsoft Windows Server を利用したミラーサーバー構築手順』を参照してください。

【 ESET Remote Administrator Server V5.3 を利用した構築手順 】

- 手順1 ESET Remote Administrator Console を起動します。
- 手順2 ログイン画面で、ログインに必要な情報（パスワードなど）を入力し、ESET Remote Administrator Server にログインします。

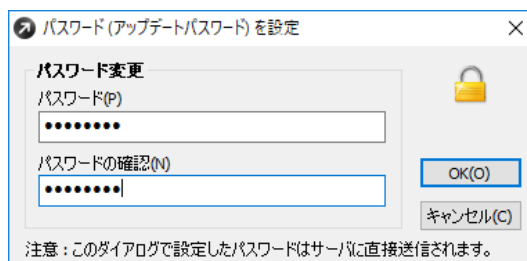


- 手順3 メニュー「ツール」 - 「サーバオプション」の順に選択し、「サーバオプション」ダイアログを表示します。
- 手順4 「アップデート」タブをクリックします。



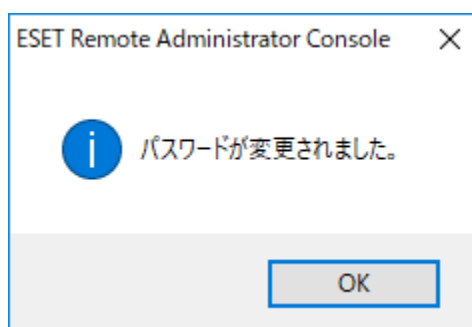
- 手順5 「アップデートユーザ名」または「アップデート用ユーザ名」テキストボックスに、ユーザー名を入力します。

- 手順6 「パスワードの設定」または「パスワードを設定」ボタンをクリックし、「パスワード（アップデートパスワード）を設定」ダイアログを表示します。



- 手順7 「パスワード」（または「新規パスワード」）および「パスワードの確認」（または「新規パスワードの再入力」）にパスワードを入力し、[OK] ボタンをクリックします。

- 手順8 表示された確認メッセージ「パスワードが変更されました」の [OK] ボタンをクリックします。

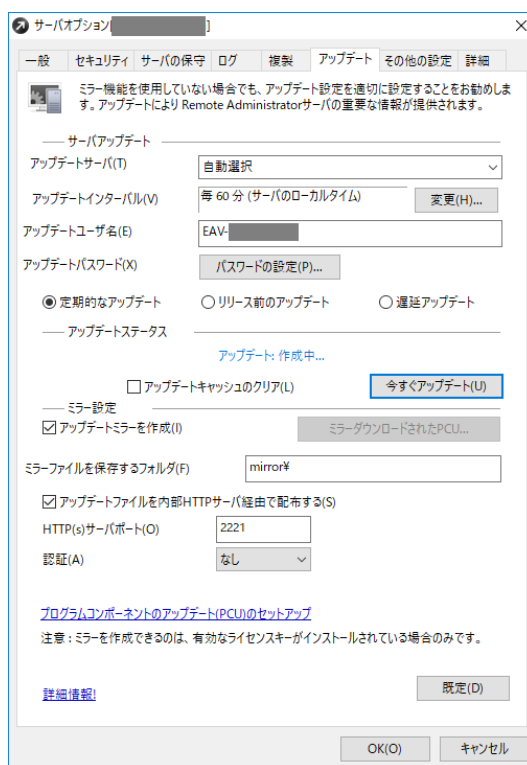


- 手順9 「アップデートミラーを作成」または「ミラーを作成する」チェックボックスを有効にします。

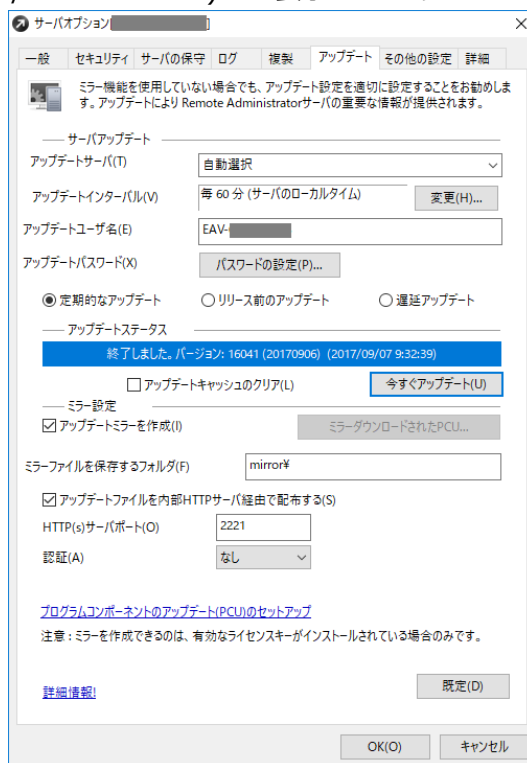
- 手順10 「アップデートファイルを内部 HTTP サーバ経由で配布する」または「内臓の HTTP サーバよりアップデートファイルを提供する」チェックボックスを有効にします。

手順11 「今すぐアップデート」または「定義データベースのアップデート」ボタンをクリックし、検出エンジン（ウイルス定義データベース）をダウンロードします。

手順12 検出エンジン（ウイルス定義データベース）のダウンロードが開始されます。



- 手順13 検出エンジン（ウイルス定義データベース）のダウンロードが完了すると、「アップデートの状況」に“終了しました。バージョン：XXXX（20XX/XX/XX XX:XX:XX）”と表示されます。



- 手順14 [OK] ボタンをクリックし、ダイアログを閉じます。

以上で、ミラーサーバーの設定が完了しました。

- ③ クライアントのアップデートサーバーを変更
次に、クライアントの検出エンジン（ウイルス定義データベース）のアップデート先（アップデートサーバー）を変更します。クライアントのアップデートサーバーを変更するには、以下の方法があります。

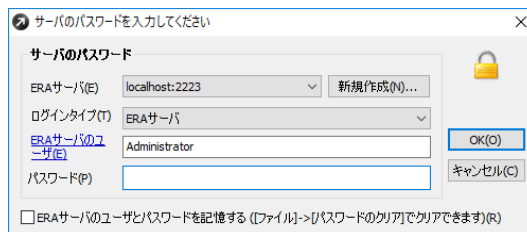
【 クライアントのアップデートサーバーの変更方法 】

- ESET Remote Administrator を使用して変更する
- クライアント画面から直接設定を変更する

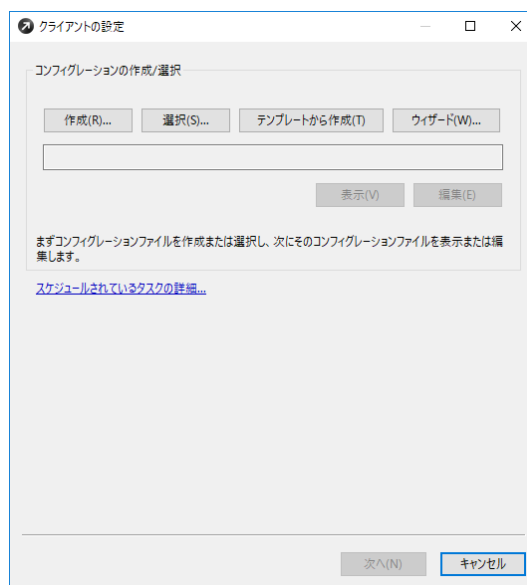
ここでは、ESET Remote Administrator V5.3 を使用して、アップデートサーバーを変更する手順を説明します。なお、クライアント画面から直接設定を変更する場合は、補足資料『8.6 クライアントの設定画面からアップデートサーバーを変更する手順』を参照してください。

【 ESET Remote Administrator V5.3 を使用してアップデートサーバーを変更する手順 】

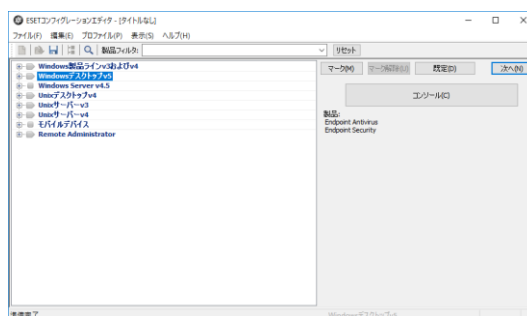
- 手順1 ESET Remote Administrator Console を起動します。
- 手順2 ログイン画面で、ログインに必要な情報（パスワードなど）を入力し、ESET Remote Administrator Server にログインします。



- 手順3 メニュー「アクション」-「新規タスク」-「コンフィグレーション」の順に選択し、「クライアントの設定」ダイアログを表示します。

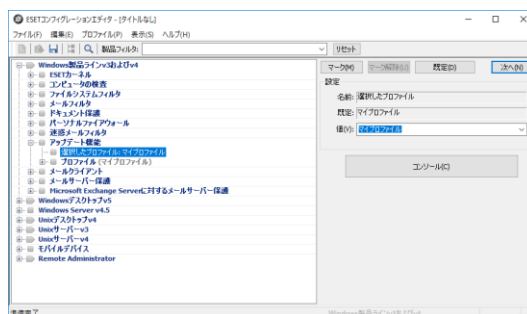


- 手順4 「コンフィグレーションの作成/選択」にある【作成】ボタンをクリックし、コンフィグレーションエディタを起動します。



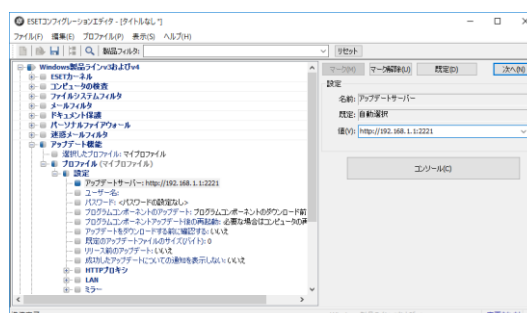
手順5 「Windows デスクトップ v5」-「アップデート」の順にクリックします。

手順6 「選択したプロファイル」をクリックし、右側に表示されたプロファイルの選択画面の「値」から使用するプロファイルを選択します。



手順7 「プロファイル (選択したプロファイル名)」 - 「設定」 - 「アップデートサーバー」をクリックします。

手順8 「アップデートサーバー」の「値」に、変更するアップデートサーバーを入力します。(例 : `http://192.168.1.1:2221` など)
また、認証などをおこなっている場合は、ユーザー名、パスワードなどの設定をおこないます。

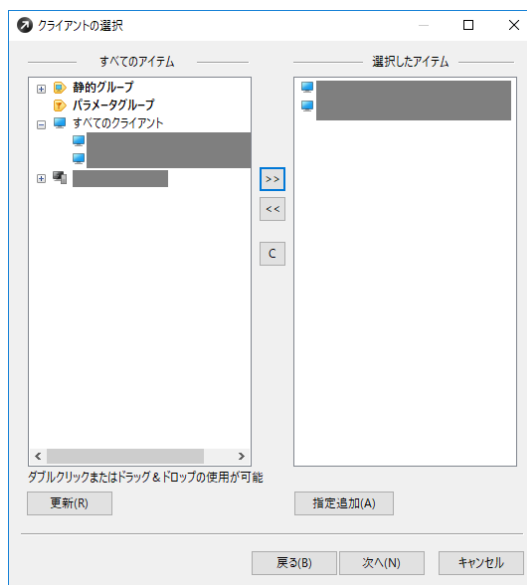


手順9 「ファイル」 - 「終了」の順に選択します。

手順10 確認メッセージが表示された場合は、[はい] ボタンをクリックします。

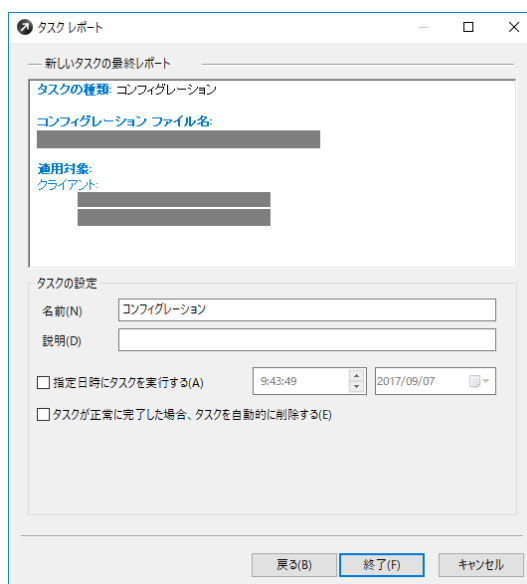
手順11 「クライアントの設定」ダイアログの [次へ] ボタンをクリックします。

- 手順12 「クライアントの選択」ダイアログで、アップデートサーバーを変更するクライアントやグループを選択し、[>>] ボタンをクリックします。右の「選択したグループ」に、選択したクライアント名が表示されます。



- 手順13 [次へ] ボタンをクリックします。

- 手順14 「新しいタスクの最終レポート」に表示されている値を確認し、[終了] または [完了] ボタンをクリックします。検出エンジン（ウイルス定義データベース）のアップデートタスクが配布されます。



- 手順15 メニュー「表示」 - 「[タスク] ペイン」の順にクリックします。

手順16 手順 14 で配布したタスクの状態を確認し、タスクの状態が“終了”になるまで待機します。タスクの状態が“終了”と表示されると、クライアントの検出エンジン（ウイルス定義データベース）の設定変更が完了します。

以上で、アップデートサーバーの変更が完了しました。

- ④ 検出エンジン（ウイルス定義データベース）のアップデート確認
最後に、クライアントから検出エンジン（ウイルス定義データベース）がアップデートできることを確認します。具体的な検出エンジン（ウイルス定義データベース）のアップデート手順は、補足資料『8.4 検出エンジン（ウイルス定義データベース）のアップデート手順』を参照してください。

6 よくある質問とトラブルシューティング

ここでは、お問い合わせの多いベースアップデートに関するご質問をまとめています。

質問①

ベースアップデートは、どのくらいの間隔で実施されますか？

回答

ベースアップデートの実施間隔は、マルウェアの発生状況により日々変化するため不定期に実施されます。ただ、過去に実施されたベースアップデートの例では、約 3～6 カ月ごとに実施されています。

質問②

ベースアップデートが実施される前に、連絡することは可能ですか？

回答

開発元の ESET 社では、ベースアップデートの実施時期を公開しておりません。そのため、現在のところベースアップデートが実施される前に、弊社より事前にご連絡することは難しい状況です。大変申し訳ありません。

質問③

ベースアップデートが実施された場合にダウンロードされる検出エンジン（ウイルス定義データベース）の容量はどのくらいですか？

回答

ベースアップデートが実施された場合、最大で約 40MB 前後の検出エンジン（ウイルス定義データベース）のダウンロードが必要となります。

実施日時（日本時間）	検出エンジン（ウイルス定義データベース）のサイズ
2016 年 07 月 19 日	最大約 46MB
2016 年 05 月 26 日	最大約 15MB
：	：
2010 年 07 月 23 日	約 24MB
2010 年 04 月 19 日	約 25MB

表 9 過去に実施されたベースアップデート

なお、毎日定期的に ESET 社のアップデートサーバーからアップデートしている場合（ミラーサーバーを利用してアップデートしていない場合）、ベースアップデートが実施されても、ナノアップデートが適用されて、ダウンロードする検出エンジン（ウイルス定義データベース）のサイズが小さい（数百 KB 程度）場合があります。

質問④

オフライン更新用の検出エンジン（ウイルス定義データベース）はどこからダウンロードできますか？

回答

オフライン更新用の検出エンジン（ウイルス定義データベース）は、弊社ユーザーズサイトからダウンロードすることが可能です。弊社ユーザーズサイトのログイン方法および検出エンジン（ウイルス定義データベース）のダウンロード方法については、補足資料『8.2 検出エンジン（ウイルス定義データベース）のダウンロード方法』を参照してください。

7 製品サポート情報

7.1 ご意見、ご質問のお問い合わせ先

ESET 製品に関するご意見、ご質問がございましたら、製品購入時にご案内させていただきましたお問い合わせ先までお問い合わせください。

7.2 製品 Q&A について

弊社では、お問い合わせの多いご質問をまとめた製品 Q&A ページをご用意しております。弊社サポートセンターにお問い合わせをおこなう前に、以下の Web ページより、お問い合わせの内容があるかご確認ください。

製品 Q&A ページ

<https://eset-info.canon-its.jp/support/>

また、法人向け製品をご使用のお客さま専用の Web ページ（ユーザースサイト）もご用意しております。ユーザースサイトでは、最新プログラムや製品マニュアル、オフライン用検出エンジン（ウイルス定義データベース）のダウンロードをおこなうことができます。上記製品 Q&A ページと合わせてご確認ください。

ユーザースサイト（法人向けサーバー・クライアント用製品）

<https://canon-its.jp/product/eset/users/index.html>

ユーザースサイト（法人向けサーバー専用製品）

https://canon-its.jp/product/eset/users/index_fs.html

なお、ユーザースサイトへログインするには、シリアル番号およびユーザー名が必要となります。シリアル番号およびユーザー名は、製品購入時にご案内させていただいたライセンス証書をご確認ください。

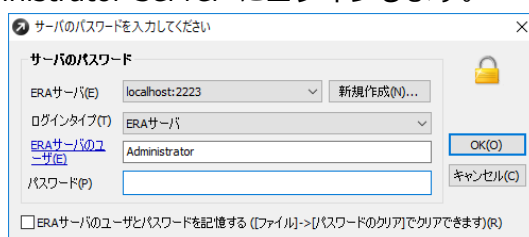
8 補足資料

8.1 アップデートタスクの配布手順

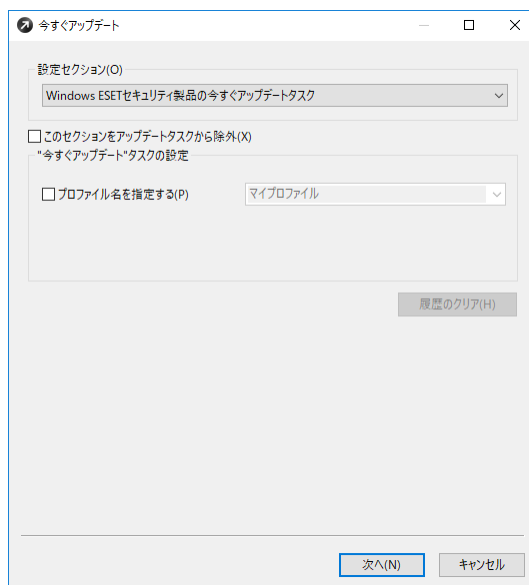
以下の手順は、ESET Remote Administrator V5.3 を例にご案内しています。

手順1 ESET Remote Administrator Console を起動します。

手順2 ログイン画面で、ログインに必要な情報（パスワードなど）を入力し、ESET Remote Administrator Server にログインします。

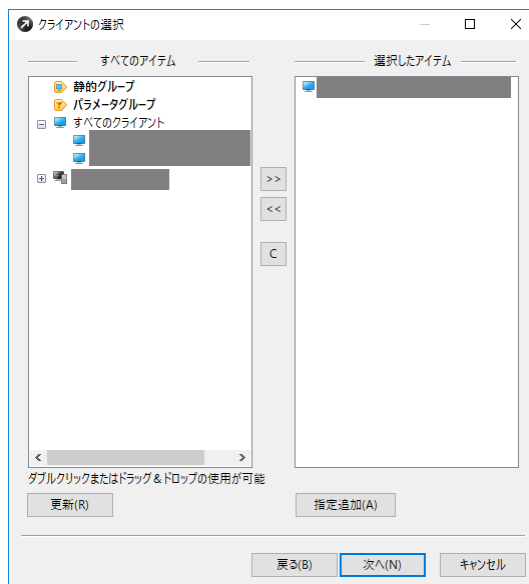


手順3 「アクション」 - 「新規タスク」 - 「今すぐアップデート」または「定義データベースのアップデート」の順に選択し、「今すぐアップデート」ダイアログを表示します。



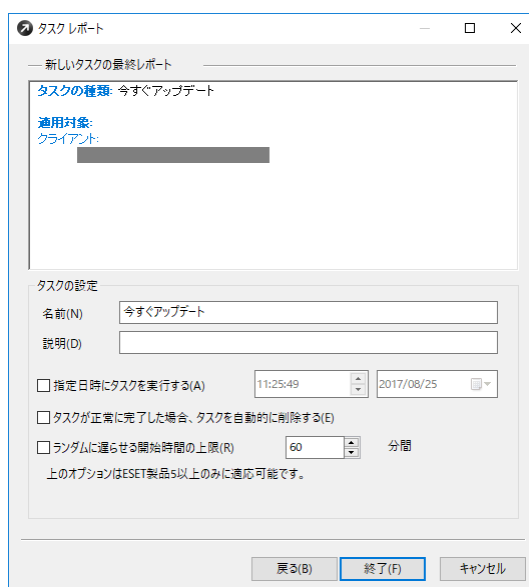
手順4 「設定セッション」の値を“Windows ESET セキュリティ製品の今すぐアップデートタスク”または“Windows 版 ESET セキュリティ製品の定義データベースのアップデートタスク”に変更し、[次へ] ボタンをクリックします。

手順5 左側の「すべてのアイテム」からアップデートタスクを配布するクライアントやグループを選択し、[>>] ボタンをクリックします。選択したクライアントが右側の「選択したアイテム」に移動します。



手順6 [次へ] ボタンをクリックします。

手順7 「新しいタスクの最終レポート」の値を確認し、[終了] または [完了] ボタンをクリックします。



手順8 「表示」 - 「[タスク] ペイン」の順にクリックします。

手順9 手順 7 で配布したタスクの状態を確認し、タスクの状態が“終了”になるまで待機します。タスクの状態が“終了”と表示されると、アップデートタスクの配布が完了します。

以上で、アップデートタスクの配布が完了しました。

8.2 検出エンジン（ウイルス定義データベース）のダウンロード方法

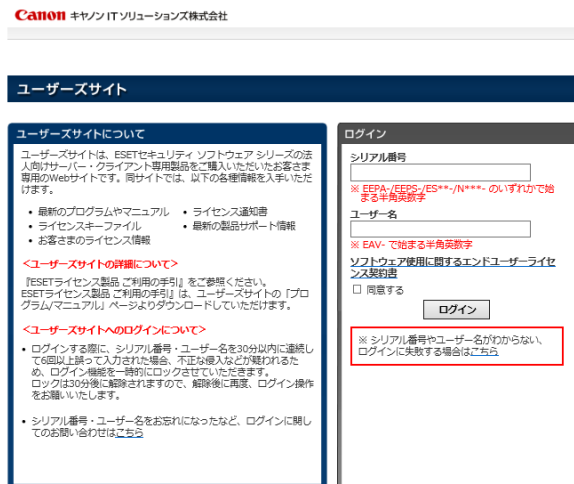
手順1 ご使用の Web ブラウザー（Internet Explorer）を起動し、以下の Web ページアクセスします。

【 ユーザーズサイト（法人向けサーバー・クライアント用製品） 】
<https://canon-its.jp/product/eset/users/index.html>

【 ユーザーズサイト（法人向けサーバー専用製品） 】
https://canon-its.jp/product/eset/users/index_fs.html



手順2 「ログインページに移動」ボタンをクリックし、ログインページに移動します。

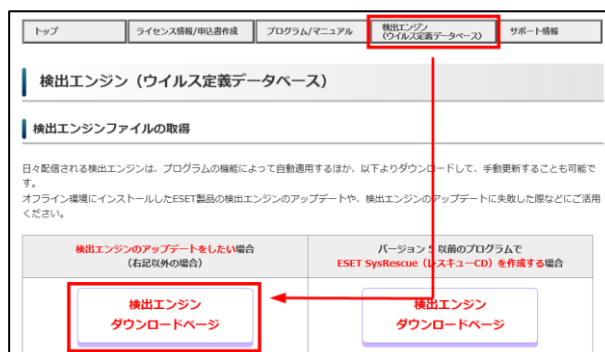


手順3 ログイン画面の「シリアル番号」、「ユーザー名」に、製品購入時にご案内したライセンス証書、または、メールに記載されたシリアル番号およびユーザー名を入力します。

手順4 「ソフトウェアライセンス使用許諾書」をクリックし、ソフトウェアライセンス使用許諾書をお読みいただいた後、同意される場合は、「同意する」チェックボックスを有効にします。

手順5 [ログイン] ボタンをクリックし、ユーザーズサイトへログインします。

手順6 ページ上部の「検出エンジン（ウイルス定義データベース）」をクリックし、画面左側の「検出エンジンのアップデートをしたい場合」の「検出エンジン ダウンロードページ」ボタンをクリックします。



手順7 「検出エンジン ダウンロード」から「最新 20XX 年 XX 月 XX 日 XX 時 XX 分 検出エンジンファイル」ボタンをクリックし、検出エンジン（ウイルス定義データベース）をダウンロードします。

以上で、検出エンジン（ウイルス定義データベース）のダウンロードが完了しました。

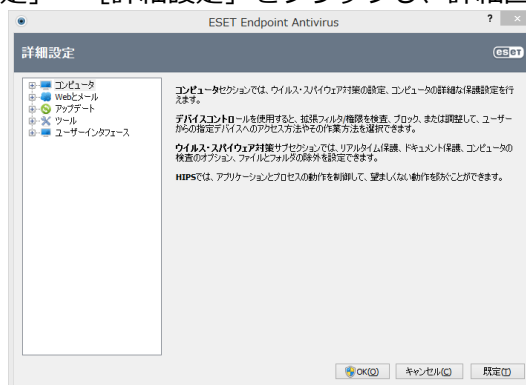
8.3 オフライン更新の手順

以下の手順は、ESET Endpoint アンチウイルス V5.0 を例にご案内しています。

手順1 『8.2 検出エンジン（ウイルス定義データベース）のダウンロード方法』の手順に従って、検出エンジン（ウイルス定義データベース）をダウンロードします。

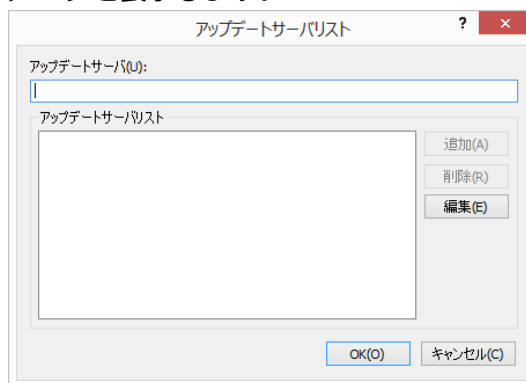
手順2 通知領域（タスクトレイ）の ESET 製品のアイコンをダブルクリックし、基本画面を表示します。

手順3 基本画面の [設定] → [詳細設定] をクリックし、詳細画面を開きます。



手順4 詳細画面左側のツリーから「アップデート」 - 「一般」をクリックします。

手順5 アップデート画面右側にある [編集] ボタンをクリックし、「アップデートサーバリスト」ダイアログを表示します。

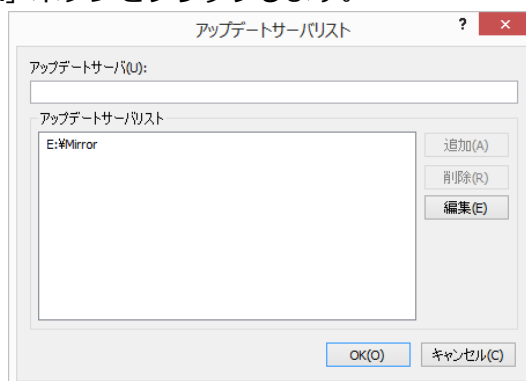


手順6 「アップデートサーバ」テキストボックスに、検出エンジン（ウイルス定義データベース）が格納された場所を入力し、[追加] ボタンをクリックします。

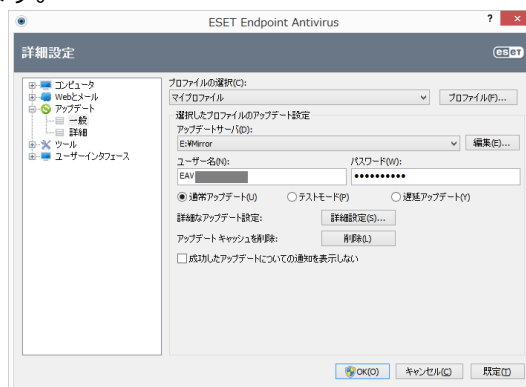
例：USB メモリ（E:ドライブ）内の“Mirror”フォルダーに検出エンジン（ウイルス定義データベース）が格納されている場合

入力する値：“E:¥Mirror”

手順7 「アップデートサーバリスト」に手順 6 で追加した場所が表示されていることを確認し、[OK] ボタンをクリックします。



手順8 「アップデートサーバ」の値を手順 6 で入力した場所に変更し、[OK] ボタンをクリックします。



手順9 『8.4 検出エンジン（ウイルス定義データベース）のアップデート手順』の手順に従って、検出エンジン（ウイルス定義データベース）のアップデートをおこないます。

以上で、オフライン更新が完了しました。

8.4 検出エンジン（ウイルス定義データベース）のアップデート手順

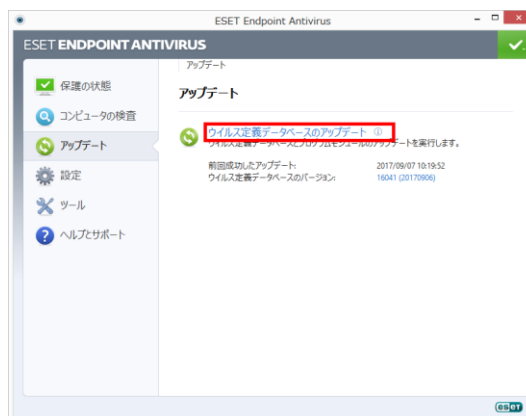
以下の手順は、ESET Endpoint アンチウイルス V5.0 を例にご案内しています。

手順1 通知領域（タスクトレイ）にある ESET 製品のアイコンをダブルクリックし、基本画面を表示します。

手順2 基本画面右側にある「アップデート」メニューをクリックします



手順3 アップデート画面にある「ウイルス定義データベースのアップデート」を選択し、検出エンジン（ウイルス定義データベース）のアップデートを実行します。



- 手順4 検出エンジン（ウイルス定義データベース）のアップデートが正常に完了すると、以下の画面が表示されます。



正常にアップデートできない場合は、以下の原因が考えられます。

【 主な原因 】

- Windows Server 標準のファイアウォールで接続が遮断されている
- クライアントのアップデートサーバー設定に誤りがある
- プロキシサーバーが正しく設定されていない

必要に応じて、上記設定の確認、変更をおこなってください。また、上記設定が正しい場合は、弊社サポートセンターまでお問い合わせください。

以上で、検出エンジン（ウイルス定義データベース）のアップデートが完了しました。

8.5 クライアントの設定画面からアップデートスケジュールを変更する手順

以下の手順は、ESET Endpoint アンチウイルス V5.0 を例にご案内しています。

手順1 通知領域（タスクトレイ）の ESET 製品のアイコンをダブルクリックし、基本画面を表示します。

手順2 基本画面左側のメニューから「ツール」-「スケジューラ」の順にクリックします。



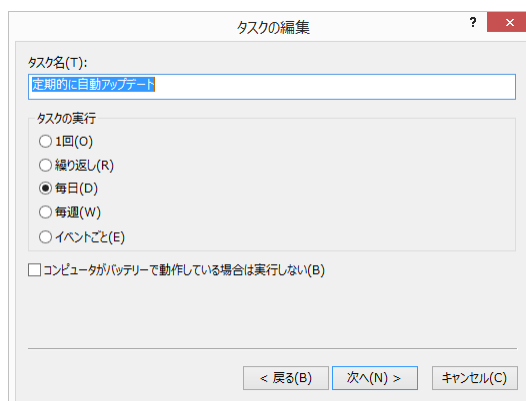
手順3 スケジューラ画面から検出エンジン（ウイルス定義データベース）のアップデートスケジュール（既定では、“定期的に自動アップデート”）を選択し、[編集] ボタンをクリックします。

手順4 表示された「タスクの編集」ダイアログ画面の「スケジュールタスク」が“アップデート”になっていることを確認し、[次へ] ボタンをクリックします。

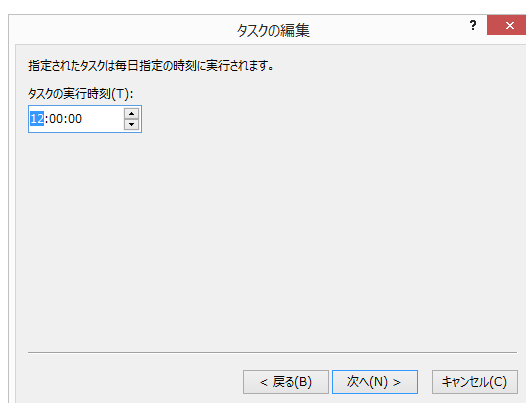


手順5 「タスクの実行」から検出エンジン（ウイルス定義データベース）をおこなう間隔を設定します。「毎日」チェックボックスを有効にし、[次へ] ボタンをクリックします。

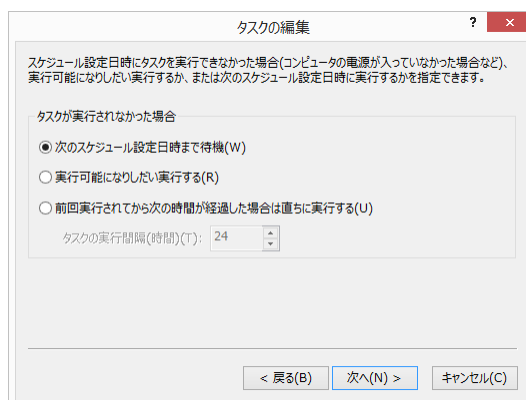
ここでは、毎日 12:00 に検出エンジン（ウイルス定義データベース）を実行する例を説明します。



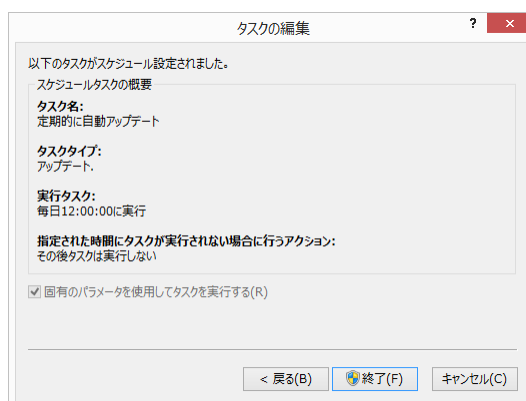
手順6 「タスクの実行時刻」に“12:00:00”と入力し、[次へ] ボタンをクリックします。



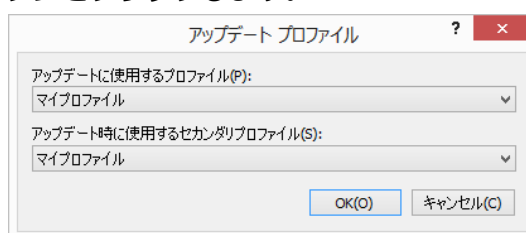
手順7 検出エンジン（ウイルス定義データベース）のアップデートが実行される時間に、コンピューターが起動していないなど、アップデート処理を実行できなかった場合の動作を選択し、[次へ] ボタンをクリックします。



手順8 「スケジュールタスクの概要」に表示された設定を確認し、[終了] ボタンをクリックします。



手順9 表示された「アップデートプロファイル」ダイアログの「アップデートに使用するプロファイル」および「アップデート時に使用するセカンダリプロファイル」から、アップデートプロファイル（既定では、「マイプロファイル」）を選択し、[OK] ボタンをクリックします。



手順10 手順 4 で選択したスケジューラの「タイミング」の値が、手順 6～7 で指定した値に変更されていることを確認します。



手順11 基本画面を閉じます。

以上で、アップデートスケジュールの変更が完了しました。

8.6 クライアントの設定画面からアップデートサーバーを変更する手順

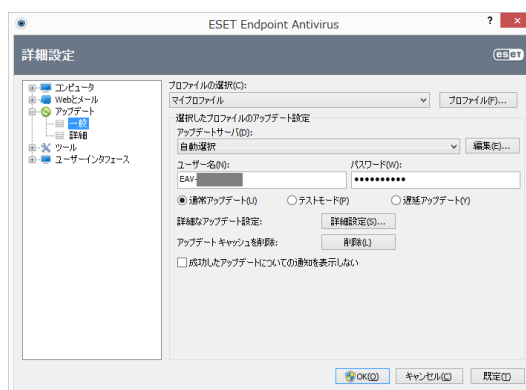
以下の手順は、ESET Endpoint アンチウイルス V5.0 を例にご案内しています。

手順1 通知領域（タスクトレイ）の ESET 製品のアイコンをダブルクリックし、基本画面を表示します。

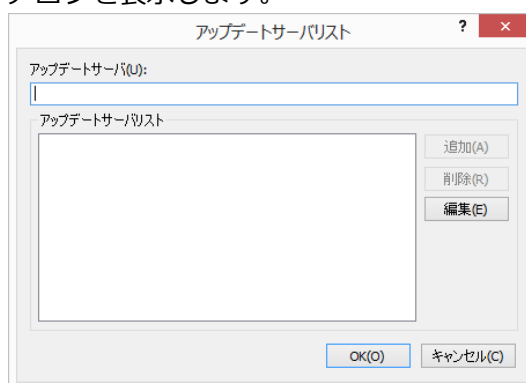
手順2 基本画面の [設定] → [詳細設定] をクリックし、詳細画面を開きます。



手順3 詳細画面左側のツリーから「アップデート」 - 「一般」をクリックします。

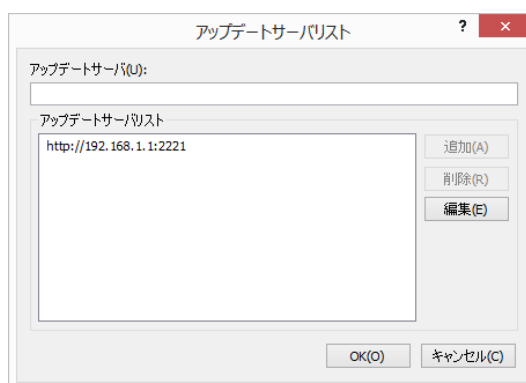


手順4 アップデート画面右側にある [編集] ボタンをクリックし、「アップデートサーバーリスト」ダイアログを表示します。



手順5 「アップデートサーバ」テキストボックスに、アップデートサーバのアドレス（例：http://192.168.1.1:2221 や“¥¥192.168.1.1¥mirror”など）を入力し、[追加] ボタンをクリックします。

手順6 「アップデートサーバリスト」に手順5 で追加した場所が表示されていることを確認し、[OK] ボタンをクリックします。



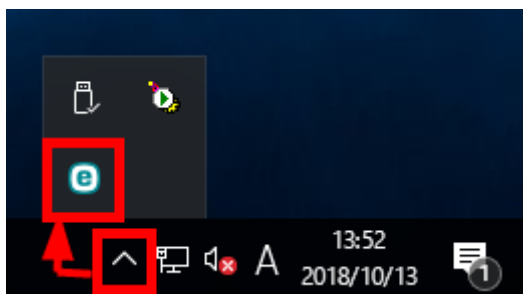
手順7 「アップデートサーバ」の値を手順5 で入力した場所に変更し、[OK] ボタンをクリックします。

以上で、アップデートサーバの変更が完了しました。

8.7 ESET File Security for Microsoft Windows Server を利用したミラーサーバー構築手順

以下の手順は、ESET File Security for Microsoft Windows Server V7.0 を例にご案内しています。

手順1 通知領域 (タスクトレイ) にある ESET 製品のアイコンをダブルクリックし、基本画面を表示します。



手順2 基本画面の [設定] → [詳細設定] をクリックして、設定画面を開きます。



手順3 [アップデート] → [プロファイル] → [アップデート] と展開します。[モジュールアップデート] の [自動選択] にチェックが入っていることを確認します。

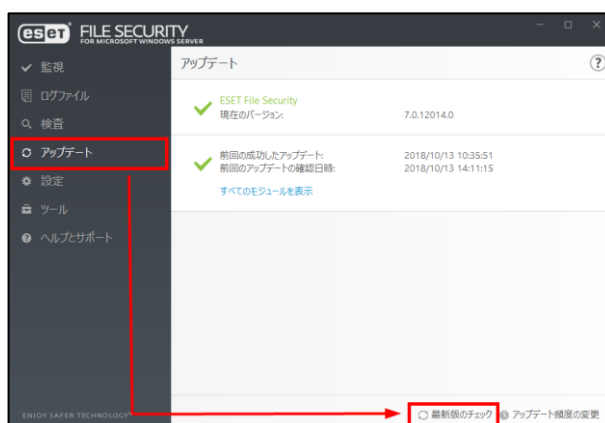


- 手順4 画面下の[アップデートミラー]を展開します。[アップデートミラーの作成]と [HTTP サーバーを有効にする] にチェックを入れます。



- 手順5 [OK] ボタンをクリックします。

- 手順6 基本画面の [アップデート] → [最新版のチェック] をクリックして、アップデートをおこないます。



- 手順7 アップデートが終了したら、[前回の成功したアップデート] にアップデートをおこなった日が、[すべてのモジュールを表示] より最新の検出エンジン (ウイルス定義データベース) のバージョンが確認できます。

以上で、ミラーサーバーの設定が完了しました。