

Kaspersky Security Center 14 Kaspersky Endpoint Security 12 ポリシー・タスク設定 実践編

2023/09/20 株式会社カスペルスキー セールスエンジニアリング本部 Ver 2.0

1.	はじめに	3
1	1. 本資料の目的	3
2.	デバイスのパフォーマンス改善	4
2	1. スキャン対象形式を調整する	4
2	.2. 新規作成または更新されたファイルのみをスキャン対象にする	6
2	.3. クライアントと管理サーバーの同期間隔を変更	8
2	.4. デバイスへの定義データベース配信に伴う管理サーバー負荷を軽減	9
3.	ネットワーク設定	11
3	.1. ファイアウォール設定	11
3	.2. 管理サーバーのプロキシサーバー設定1	14
3	.3. クライアントデバイスのプロキシサーバー設定	15
4.	タスクのスケジュール設定	17
4	.1. 定義データベースの更新スケジュールを設定する	17
4	.2. 各デバイスのスキャン実施完了日時を確認	19
4	.3. スキャンタスクの作成	21
5.	その他	27
5	.1. デバイス情報の削除方法(ライセンスの解放)	27
5	.2. グループタスク開始・停止をユーザーに許可する	32
5	.3. ローカルタスクの開始・停止をユーザーに許可する	34
5	.4. グレーウェアを検知対象に含める	36
5	.5. Windows 共有フォルダーへのアクセスを許可する	38

1. はじめに

1.1. 本資料の目的

本資料では、Kaspersky Endpoint Security for Business におけるポリシー、およびタスクの目的別の設定 についてご説明します。

ポリシー、タスク設定の考え方については、別資料「ポリシー・タスクの考え方 KSC/KES 対応版」をご参照ください。

各種資料は以下サイトから閲覧、ダウンロードすることができます。 法人のお客様向けダウンロード資料 (https://kasperskylabs.jp/biz/) **kaspersky** 2. デバイスのパフォーマンス改善

2.1. スキャン対象形式を調整する

スキャンの対象を減らすことでパフォーマンスが改善されることがあります。

また、実行スケジュールでスキャンの間隔や時間帯を調整する方法(「4.タスクのスケジュール設定」参照)もご 検討ください。

ここでは、スキャンの対象をファイル形式によって調整する方法についてご説明します。

「Kaspersky Endpoint Security(KES)」ではスキャンの対象を以下の3種類から選択できます。

・すべてのファイルをスキャン - スキャン対象がもっとも多く完了まで時間がかかる可能性がありますが、高いセキュリティを保つことができます。

- •ファイル形式でファイルをスキャン ファイルヘッダを精査し感染の可能性のあるファイル形式のみスキャンします。 既定ではこの設定が選択されており、セキュリティとパフォーマンスのバランス が取られています。
- ・拡張子でファイルをスキャン ファイルヘッダは確認せずファイル名の拡張子のみで感染の可能性のあるファイ ル形式かを判断し、スキャンします。ファイル名の拡張子が変更されていると、感 染の可能性があるファイル形式であってもスキャンがスキップされる可能性があり ます。
- (1) 管理コンソールにて「管理対象デバイス」を 開きます。
 右画面にて「ポリシー」タブを開き、「KES」
 のポリシーを右クリックして「プロパティ」を選 択します。

Kaspersky Security Center 7r(ル(F) 操作(A) 表示(V) ヘルブ(H) ◆ ⇒ 2 〒 □ □ □ 0 □ 0 □ □ □ □ 0 □ □ □ □ □ 0 □			- B X
K Kapperlay Security Center General Security Center General Security Center General Security Center General Security Control General Security Control General Security Control General Security Center General Security	<u> 生理サーバー KSC</u> > 管理対象デバイス (*) ポリシー デバイス ポリシー ダスク 新潟パリンー オリシーをファイルからインオ	4-> Busing-alle	20-2020/94
 ■ #4	名目 ■ Karpersky Troppint Security for Windows (12.20) Karpersky Court (2017 - 2017 - 21)	ステータス アプリケーション アウキィブ Kaseensky Factoriant Security for Windows (アウチィブがジッー	リロマー Kaspersky Endpoint Security for メイ Windows (12.2.0) アプリケーションス Kaspersky Endpoint
	Cauparday Sociality Canter 79(19-92-92)	#U)-を始めがり-ととおいく 17.70ポードは3 アイズをラスプロし ン アイズをラスプロし ン アイズをラスプロし ン アイズをラスプロし ン アイズをラスプロし ン アイズをラスプロし ン アイズをフィーン フレイトロン ス フレイトロン ス フレイトロン ス アイン アイン アイン アイン アイン アイン アイン アイン	Scienty for Window 104: 2020 (96) 1233-90 2020 (96) 1233-90 2020 (96) 1233-93 High, 25(9) (97) - 2220 (96) 1233-93 High, 25(9) (97) - 2220 (96) 123-93 High, 25(9) (97) - 2220 (96) 123-93 High, 25(9) (97) (97) (97) (97) (97) (97) (97) (
	¢	,	■ #UU-ØBE ■ #mothe <u>∧UZ</u> • kaspersky

(2)「脅威対策」-「ファイル脅威対策」セクションを開きます。 方面面にて「セキュリティレベル」欄内の「設定」をクリックします。



(3)「全般」タブの「ファイル種別」欄で対象を 選択します。

> 設定後、「OK」をクリックして設定を反映さ せます。

2.2. 新規作成または更新されたファイルのみをスキャン対象にする

スキャンの対象を新規作成または更新されたファイルに限定することで、スキャン対象を減らすことができます。この 機能によりスキャンのパフォーマンスを向上させることができます。

既定では有効になっています。

(本機能が有効な場合、iSwift/iChecker 方式でのスキャンは行われません)

 (1) 管理コンソールにて「管理対象デバイス」を 開きます。
 右画面にて「ポリシー」タブを開き、「KES」
 のポリシーを右クリックして「プロパティ」を選 択します。

(2)「脅威対策」-「ファイル脅威対策」セクションを開きます。 右画面にて「セキュリティレベル」欄内の「設定」をクリックします。



(3)「パフォーマンス」タブを開き、「新規作成ま たは更新されたファイルのみスキャン」にチェ ックを入れます。



(4)「詳細」タブを開き、「スキャン技術」欄でそれぞれの有効/無効を設定します。

設定後、「OK」をクリックして設定を反映さ せます。

2.3. クライアントと管理サーバーの同期間隔を変更

ネットワークエージェントは、定期的に管理サーバーに接続してデバイスの情報やステータスの送信、ポリシーなど 設定に更新があるか確認しています。管理下のクライアント台数などにより、この同期が管理サーバーのパフォーマン スやネットワークトラフィックに影響を及ぼす可能性があります。

この確認の間隔を延ばすことで、ネットワークと管理サーバーにかかる負荷を抑えることができます。初期設定では 15分間隔となっています。



2.4. デバイスへの定義データベース配信に伴う管理サーバー負荷を軽減

デバイスへの定義データベースの配信は、既定で管理サーバーから行われます。 同時に実行する台数が多い場合、パフォーマンスに影響を及ぼす可能性があります。 タスクの実行を分散化することで管理サーバーやネットワークの負荷を軽減できる可能性があります。



- ランダム実行時間、クライアント台数とアップデートのタイミングについて
 - ◆ ランダム実行時間:L 分
 - ◇ クライアントの台数:N 台
 - ◆ アップデートのタイミング: [L/N]分間隔
 - 例 : ランダム実行時間 : 100 分 クライアントの台数 : 50 台
 - 開始時刻:09:00:00





3.1. ファイアウォール設定

使用可能なネットワークを設定するネットワークの動作をファイアウォールで監視するネットワークの設定を行いま す。



(3)「ファイアウォール」画面が表示されます。 「ネットワーク」タブを開き、「追加」をクリック します。



(4) 「ネットワーク接続」画面が表示されます。 ネットワークの「名前」、「状態」、「IP アドレ スの編集」を設定します。

「状態」は、「パブリックネットワーク」、「プラ イベートネットワーク」、「許可するネットワー ク」より選択します。 設定後、「OK」をクリックして設定を反映さ せます。

ネットワーグ	接続	0	×
名前:			
状態:	パブリックネットワーク		\sim
IP アドレス:			
何]:	1.2.3.4/24、1234::cdef/	96	
	ОК	キャン	セル

パブリックネットワーク、プライベートネットワーク、許可するネットワークについての説明は以下の通りです。

パブリックネットワーク: アンチウイルス製品、ファイアウォール、またはフィルターによって保護されないネットワークのステータス(インタ ーネットカフェのネットワークなど)です。このようなネットワークに接続されているコンピューターのユーザーに対 して、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザー は、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモ ートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケー ションに設定されたネットワークルールに従ってフィルタリングします。

● **プライベートネットワーク**:

そのネットワークからユーザーがこのコンピューターのファイルやプリンターにアクセスすることを信頼するネットワーク (LAN またはホームネットワークなど) に割り当てます。

● 許可するネットワーク:

コンピューターが攻撃されない、または不正にアクセスされない安全なネットワークに割り当てます。このステー タスのネットワークの場合、ファイアウォールは指定されたネットワーク内のすべてのネットワークの動作を許可し ます。

kaspersky 3.2. 管理サーバーのプロキシサーバー設定

インターネットへの接続がプロキシサーバーを経由する環境である場合、管理サーバーは定義データベース情報を ダウンロードするためにプロキシサーバーの設定が必要となります。

管理サーバーのプロキシサーバー設定は以下のように行います。



3.3. クライアントデバイスのプロキシサーバー設定

クライアントデバイスのプロキシサーバーの設定は以下のように行います。



(3)「プロキシサーバー設定」画面が表示され ます。 「プロキシサーバーを使用する」を有効にし

て、必要な項目を設定します。

※「プロキシサーバーを自動的に検出する」に設定した場合はOSの設定に従い動作します。

設定後、「OK」をクリックして設定を反映さ せます。

✔ ブロキシサーバー設定		0	×
☑ フロキシサーバーを使用する			
● プロキシサーバー設定を自動的に検出	けする		
○ プロキシサーバー設定を使用する			
アドレス:	ポート:		
	: 80 🔺		
🗌 プロキシサーバー認証を使用する			
ユーザー名:	パスワード:		
	•••••		
🗹 ローカルアドレスにはプロキシサーバーを	使用しない		
	ОК	閉じる	



4.1. 定義データベースの更新スケジュールを設定する

定義データベースの更新タスクの実行スケジュールを設定します。



- 「未実行のタスクを実行する」にチェックを入れておくと、設定したスケジュールの時刻に電源が OFF になっていた端末は、次回起動後にタスクが実行されます。
- 「タスクを実行するまでの時間を自動的に設定する」にチェックを入れておくと、設定スケジュール以降でクライアントがランダムな時間を設定しタスクを開始します。この設定によって管理サーバーの負荷が分散されます。(「2.4.デバイスへの定義データベース配信に伴う管理サーバー負荷を軽減」を参照してください。)

●スケジュール設定例

スケジュール設定	概要	設定例
N 時間ごと	設定した開始日時から「N 時 間」間隔でタスクが実行される。	間隔:1時間ごと 開始時間: 2016年1月1日 09:00:00
N 日ごと	設定した開始日時から「N 日」 間隔でタスクが実行される。	間隔 : 1 日ごと 開始時間 : 09:00:00
N 分ごと	設定した開始日時から「N 分」 間隔でタスクが実行される。	間隔 : 30 分ごと 開始時間 : 09:00:00
每週	毎週指定した曜日、時間で 1 回実行される。	毎週:月曜日 開始時間:09:00:00
毎月	毎月指定した日、時間で一回 実行される。	毎月:1日 開始時間:09:00:00
1 🖸	指定した日時で一回実行され る。	実行日:2014/01/01 開始時間:09:00:00
手動	管理コンソールでタスクの「開 始」をクリックした際に実行され る。	「開始」クリック時
アプリケーション開始時	OS が起動して、KESのサービス が開始されてから 1 回実行され ます。	アプリケーション開始時 タスクを実行するまでの時間: 15 分
新しいアップデートがリポジト リにダウンロードされ次第	管理サーバーに新しい定義 DB がダウンロードされ次第、1 回実 行される。 (管理サーバーは 1 時間毎に定 義 DB をチェックしている。)	新しいアップデートがリポジトリ にダウンロードされ次第
ウイルスアウトブレイク検知 次第	ウイルスのアウトブレイクが発生し たイベントをトリガーに 1 回実施 される。	「ウイルスアウトブレイク」ステー タスは別途定義される。
他のタスクが完了次第	他のタスクが完了したことをトリガ ーにして 1 回実施される。	「他のタスク」を指定する。

4.2. 各デバイスのスキャン実施完了日時を確認

ウイルススキャンの最終実施時間はグループの「デバイス」タブの列情報にて確認することができますが、既定では 表示されません。

この列の項目を設定することで、スキャン実施日時などの情報を表示することができます。



(3) 列の項目に、ウイルススキャンの最終実施 時間が追加され、実行時間を確認するこ とができます。

Kaspersky Security Center							- 0	×
ファイル(F) 操作(A) 表示(V) ヘルブ(H)								
《 Kaspersky Security Center 》 目 管理サーバー×SC □ 管理サーバー×SC □ 管理サーバー×SC □ デバイスを理 □ デバイスを理 □ デバイスを理 □ デバイス ジ ポリシー □ デスク	 管理サーバー KSC >> 管理対象デバ デバイス ポリシー 	管理対象デバイ イス 932	7				ジルーゴのゴロ	<u>1974</u>
G) カスペルスキーのライセンス With ### ま ユーザーアカウント ン ロ アプリケーションの管理 、 豆 リモードインストール ビリモードインストール	デバイスをグループに	移動 新規グ	ループ 処理	を実行・ 列の適加と利	1			<u>88</u>
	▶ フィルターが指定	されていません	·。 レコードのき	計:3 列をデキストで	検索			Q
 インストールパッケージ ・ インストールパッケージ ・ 自 データ増与化と保護機能 ・ Q、デパイスの検索 	ステータスを選択: 💋 覧 連択したグループおよびそのサ	(為:1 22 音告) (フクルーフ内にある)	0 🔽 OK: 2 版注したステータスの	テバイス教が上昇に表示されます	. €0709201228	したクループ内のテバイスのみが高	manz <i>s</i> .	
□ 削除されたオブジェクト	名前	前回の管理サー	キットワークエージ	リアルタイム保護のステータス	作成日	グループの完全名	前回の完全スキャ	ツ援制
U4030U 🖬 c	DESTOR-SEQUED DESTOR-SEGEN KSC	3 没有 2 分前 1 分前	√ (3) √ (3) √ (3)	0 2/7+	.36分积 10分积 13强励的	署理は表示化ス 管理は急手がイス 管理は急手がイス	321	
	<							

「前回の完全スキャン」列には完全スキャンタスクが最後に完了した時間が記録されます。 記録される条件として、タスク設定のスキャン対象範囲に最低限、次の内容が含まれている必要があります。

【スキャン対象領域】

・カーネルメモリ

- ・実行中のプロセスおよびスタートアップオブジェクト
- ・ディスクブートセクター
- ・すべてのハードディスク

「前回の完全スキャン」が空白の場合、上記フォルダーを含むウイルススキャンが完了していない状態です。 初期設定ではこの状態が14日以上続いた場合、もしくは上記フォルダーを範囲に含むウイルススキャン実施から 14日以上経過した場合、各クライアントは「**緊急**」ステータスに移行します。



スキャンタスクは既定で作成されません。以下の手順で、完全スキャンや範囲を指定したスキャンタスクを作成す ることができます。

- - <u>管理サーバー KSC</u> > 管理対象デバイス ロージパイスの抽出 ローデバイスの抽出 ローネ制り当てデバイス デバイス ポリシー タスク ホリシー タスク カスペルスキーのライセンス タスクをファイルからインボート 利の油加と制作 -ロ ユーザーアカウント アプリケーションの管理 リモートインストール ・ デバイスイメージの ・ インストールパッケ データ増号化と保護科 デバイスの快幸 2 H 111 v 68 アプリケーション タスク種別 ステータス 実行中 正常... 头致 充了... アップデート [1] アンデートログロタール Kengeraky Endpoint Security for Windows (1220) アンデデート 正美林? 0 1 0 0 BHはとアプリー・シンロカープチー・白味草 日朝日をとアプリー・フェンロカープー、 Kengeraky Security Center ネットリー・フェーント 教育性とアプリー・フェンロル 0 1 0 0 <u>∧u</u>, kaspersky \times _ 新規タスクウィザード タスク種別の選択 Kaspersky Endpoint Security for Windows (12.2.0) 📋 BitLocker 保護の管理 📋 IOC スキャン 📋 アップデート アップデートのロールバック 1ンベントリ _____ 回 コンポーネントの変更 □ データの消去 || ファイルの隔離 📋 ファイルの削除 📋 ファイルの取得 📋 プロセスの終了 プロヤスを開始 📋 マルウェアのスキャン 📋 ライセンスの追加 _____ 整合性チェック _____ 認証エージェントアカウントの管理 E Taspersky Security Center 管理サーバー □ アップデートのインストールと脆弱性の修正 📋 アプリケーションのリモートインストール 🗉 🌄 詳細 次へ(N) キャンセル
- (2)「タスク種別の選択」画面が表示されます。
 「KES」配下にある「マルウェアのスキャン」を 選択し、「次へ」をクリックします。

(3)「スキャン範囲」画面が表示されます。

ここでスキャンする範囲を設定します。 既定では、完全スキャンに該当するメモリ ーや全てのハードディスクなどが範囲として 含まれています。

スキャンタスクの完了時間を「前回の完全 スキャン」列に表示させる場合、最低限以 下の項目のチェックが必要です。

「カーネルメモリ」 「実行中のプロセスおよびスタートアップオブ ジェクト」 「ディスクブートセクター」 「すべてのハードディスク」

(4)「KES の処理」画面が表示されます。 脅威を検出したときの処理を選択し、「次 へ」をクリックします。



		×
←	新規タスクウィザード	
	Kaspersky Endpoint Security for Windows の処理	
	- 脅威の検知時の処理	_
	 ・ ・ ・	
		_
	✓コンピューターを使用していないときにのみ実行する	
	次へ(N) キャンセル	

(5)「タスクを実行するアカウントの選択」画面 が表示されます。 ここでは既定値のまま、「次へ」をクリックし ます。	 ★ 新規タスクウィザード タスクを実行するアカウントの選択 ② タスクの実行に使用するユーザーアカウントを指定します。 ③ 既定のアカウント(0) ○ アカウントの指定(5) 組織レベルの爆密データ(ドメインまたはグルーフ管理者の資格情報など)は、保存しないことを推奨します。 アカウント: パスワード:
(6) 「タスクスケジュールの設定」画面が表示さ れます。 任意の実行スケジュールを設定します。 ここでは「手動」と設定し、「次へ」をクリック します。	次へ(N) キャンセル × ← 新規932094ザード タスクスケジュールの設定 実行予定: 手動

(7)「タスク名の定義」画面が表示されます。 任意のタスクの名前を入力し、「次へ」をク リックします。	 新規9スクウィザード タスク名の定義 		×
(8) 正常に作成されたことを確認し、「完了」を クリックします。	 新規9スクワイザード ダスク作成の終了 「兜了]をクリックし、「兜全スキャン」の作成処理を兜了し、ウイザードを閉じます。	(次へ(N))	キャンセル ×
			キャンセル

- (9) 一覧に作成したタスクが表示されていることを確認します。
 開始する場合、作成したスキャンタスクを 選択し、「開始」ボタンをクリックします。
 (もしくはタスクを右クリックし「開始」を選 択します)
- (10) タスクの実行状況は詳細画面にて確 認することができます。

(11) タスクが完了すると、詳細画面にて
 「完了したデバイス数」に加算されます。
 「履歴の表示」をクリックすると、各デバイス
 毎のステータスを確認することができます。



(12) 管理コンソールにて「管理対象デバイス」を開きます。
 「デバイス」タブを開きます。
 「前回の完全スキャン」列に完全スキャンタスクが最後に完了した時間が記録されています。

Kaspersky Security Center							- 🗆	×
ファイル(F) 操作(A) 表示(V) ヘルブ(H)								
【 Kappendy Security Conter ● 目 管理サーバーKSC ■ 管理対象デバイス > □ モジイルデバイス管理 ● デバイスの抽出 □ ポリンコー	 管理サーバー KSC > き 管理対象デバー デバイス ポリシー 	部理対象デバイ。 イス 927	z				21	\$ 7 4
目 ジスグ 日 カスペルスキーのライセンス 学 課題 詳細 単 コーザーアカウント	デバイスをグループにす	新規グ	ループ 処理	を実行* 列の通知と来る	ž			# #
 ・ ・ ・	▶ フィルターが指定。	されていません	レコードの含	計:3 列をデキストで	検索			Q,
> Q、デバイスの快速 可能除されたオブジェクト 日、1時された	60 ^	前回の管理サー	ネットワークエージ	リアルタイム保護のステータス	作成日	グループの完全名 単常分会デバイフ	前回の完全スキャ) 1 分前	ì
> 🗄 9#959	CESKTOP-SGUKKD	32/17 2分前 1分前	く m く m 人 助	N 377	38.分积 10分的 1 通營約	법로건축가(12) 문행대축予パイス 管理되습주パイス	3 22 R]

本章は以上です。

kaspersky その他

5.

デバイス情報の削除方法(ライセンスの解放) 5.1.

契約期間中にデバイスの故障や交換など、入れ替えなどが発生した場合の設定をします。

KSCの管理下にあるデバイスが破損した、または買い換えの為に利用しなくなったデバイスがある場合、KSCはし ばらくの間※1そのデバイスがまだライセンスを利用しているものとしてカウントします。

そのため、不要なデバイスが発生した場合は、KSC 上からデバイスを削除してライセンスを開放してから新しく追 加するデバイスに KES と NA をインストールします。

[※1]既定では、デバイスから管理サーバーへの接続がない状態で 60 日経過すると管理サーバーの管理下から外れ、 ライセンスを開放します。設定箇所は後述します。

現在のライセンスの状態は、左側のコンソールツリーにて「カスペルスキーのライセンス」で確認できます。

(1) 管理コンソールにて「カスペルスキーのライセ ンス」を開きます。 右画面にて確認したいライセンスを右クリッ クし、「プロパティ」を選択します。



■ プロパティ: 349E259A5869438E8563A4C43D8B3CC2 × (2) ライセンスのプロパティ画面が表示されま デバイス す。 全般 デバイス アクティベ グループ ステ... 有効期限 制服 管理対象デバイス 現在... 2024/01/12 管理対象デバイス 現在... 2024/01/12 DESKTOP-E5SB613 1970/01 「デバイス」セクションを開くと、このライセン 顧客情報 2023/01 テクニカルサオ スが割り当てられているデバイス情報を確 デバイス 認することができます。 ファイルへのエクスポート(E)... ヘルプ OK キャンセル 適用(A)

続いて、デバイスを KSC の管理から外し、ライセンスを解放するには以下の手順を実施します。

Kaspersky Security Center (儿(F) 操作(A) 表示(V) ヘルプ(H) 中 20 11 日 日 0 日 11 11 (1) 管理コンソールにてライセンスを解放したい デバイスのグループ(ここでは「管理対象デ 管理サーバー KSC > 管理対象デバイス 日 管理対象デバイス ○ 管理対象デバイス 日 デバイスの抽出 日 未割り当てデバイス バイス」)を開きます。 デバイス ボリシー タスク カスペルスキーのライセンス 詳細 新焼グループ 処理を実行▼ 列の追加と無味 更新 「デバイス」タブを開き、該当のデバイスを右 ・ザーアカウント ガリケーションの管理 ▶ フィルターが指定されていません。レコードの合計:3 列をテキストで使用 クリックして「削除」を選択します。 ステータスを歴況: 💟 緊急:1 💟 警告:0 💟 OK:2 確認したクルーフおよびそのサフクルーフ内にある。指定したステータ: インストールハッ・ デーク増号化と保護制 ニーマの検索 前田の管理サー... ネットワークエーシ リアルタイム保護のステータス
ま行中 (res DESKTOP-E5SB61 デバイスのステータス:08 プロパティ DNSドメイン名: アプリケーションのインストールル デバイスに撮続 カスタムツールIMO オフラインモードでのアクセスを許可する IP アドレス: スパムからの保護ス テータス: 192.168.100.147 デバイスからのデーダ。 データ濃度対策のス テータス: ********* Endpoint Sensor のス テータス: イスからのデータは いえからのデータロ AIR いったものデータな (n) のエクフォート/S kaspersky プロバティ(P) グループ:0.デパイス:3 (2) 削除を確認するメッセージが表示されるの Kaspersky Security Center で、「はい」をクリックします。 デバイス「DESKTOP-E5SB613」をグループから削除しますか? /Τ はい(Y) いいえ(N)

(3) グループから削除するとデバイスは「未割り 当てデバイス」に移動します。

> ※端末の自動振り分け(資料「ポリシータ スクの考え方」の「2.3 デバイスの自動振 り分け」)を使用している場合、再度グル ープへ自動的に移動することがあります。 この場合は管理コンソールにて「未割り当 てデバイス」の「プロパティ」を開き、該当す る割り当てルールのチェックマークを"オフ"に して一時的に振り分けを無効にしてくださ い。



 (4) 管理コンソールにて「未割り当てデバイス」
 を開きます。
 該当のデバイスを右クリックして「削除」を 選択します。

(5) 削除を確認するメッセージが表示されるの で、「はい」をクリックします。 これでこのデバイス情報は KSC 上から完 全に削除されます。



(6) 削除するとライセンスが解放されます。
 ライセンスのプロパティの「デバイス」セクションにも対象のデバイスが表示されなくなります。

■ プロパティ: 349E259A5869438E8563A4C4	43D8B3CC2				- 1	D X
セクション	デバイス					
全般 制限 顧客情報 テンフカルサポート	デバイス 見DESKTOP-9G5UK8D	グループ 管理対象デバイス	_{ステ} 現在	有効期限 2024/01/12		アクティベ 2023/01
デバイス						
	<					>
				771/1/10	Dエクスポート	(E)
<u>^#</u> 2			ОК	キャンセノ	þ j	適用(A)

ライセンスが解放されたことを確認し、新しく追加するデバイスに KESと NA をインストールします。

既定では、デバイスから管理サーバーへの接続がない状態で60日経過すると、管理サーバーからデバイス情報が自動的 に削除され、ライセンスも開放されます。これは管理グループに設定されています。





(2) グループのプロパティ画面が表示されます。 🔳 プロパティ:管理対象デバイス デバイス 「デバイス」セクションを開きます。 全般 ネットワーク上のデバイスのアクティビティ デバイス ☑次の期間デバイスが不可視の場合管理者に通知(日): 既定では以下のように設定されています。 自動インストール ☑ 次の期間デバイスが不可視の場合グループから削除(日): デバイスのステータス 変更履歴 ブから維承する □子グループへ強制的に継承する ・次の期間デバイスが不可視の場合管理 者に通知:7日間 通信がない状態で7日間経過すると管 理サーバーにイベントが記録されます。 ・次の期間デバイスが不可視の場合グルー プから削除:60日間 通信がない状態で 69 日間経過する と、自動的にグループからデバイスが削 除されます。 ヘルプ ОК

デバイスを自動で削除されないようにする 場合は、「次の期間デバイスが不可視の 場合グループから削除」のチェックを外し無 効化します。

本節は以上です。

7 🔺

60

キャンセル 適用(A)

5.2. グループタスク開始・停止をユーザーに許可する

管理サーバー上で作成されたグループタスクは、既定では管理下のデバイスを使用するユーザーが開始・停止す ることはできません。ユーザーに操作権限を付与するには以下の設定を行います。



(3)「グループタスクの管理を許可する」が無効 <ユーザーに操作権限がない場合>

の場合、ユーザーが KES のコンソールを開 いた際に操作するボタンは表示されず、ユ ーザーはタスクに対し何もすることができま せん。

設定が有効の場合、タスクに「実行」ボタン が追加され、ユーザーは手動でタスクを開 始することができます。 また開始中のタスクを「停止」ボタンにて留 めることもできます。



<ユーザーに操作権限がある場合>





5.3. ローカルタスクの開始・停止をユーザーに許可する

ローカルタスクとは、通常 KES をスタンドアロンで使用する場合に使用するタスクです。

このタスクは管理サーバーの管理下であっても有効化することができ、ユーザーは KES 上で設定や操作することができます。

既定ではタスクは表示されておらず、ユーザーが設定・開始・停止することはできません。タスクを表示させ、ユーザ ーに操作権限を付与するには以下の設定を行います。



(2)「ローカルタスクの使用を許可する」が無効 <ユーザーにローカルタスクの操作権限がない場合>



オプジェクトスキャン スキャンするオブジェクトを選択してください。

リムーバブルドライブのスキャン リレーパブル SS メモリなど、コンピューターに接続された外付けデバイスをスキャンします。

選択

本節は以上です。

0

•



リモート接続アプリケーションなどは、それを操作する利用者によって正規なツールにも不正なツールにもなりえます。 既定ではこのようなグレーウェアのファイルを検知しません。検知するように設定するには以下のように設定します。

 (1) 管理コンソールにて「管理対象デバイス」を 開きます。
 右画面にて「ポリシー」タブを開き、「KES」
 のポリシーを右クリックして「プロパティ」を選 択します。



(2)「全般設定」→「除外リストとオブジェクトの 種別」を開きます。 「検知するオブジェクトの種別」の「設定」を クリックします。



(3) ア	ドウェア、オートタイヤラーなど」欄の コン	🚶 検知するオブジェクトの種別		0 ×	
ピュ	ーターや個人データに損害を与える目	マルウェア			1
的て	れ罪者によって悪用される可能性の	☑ ウイルス、ワーム			
ある	ソフトウェアを検出する」にチェックを入	☑ 下□101本馬 ☑ 悪意のあるツール			
nŧ	す 。	 アドウェア、オートダイヤラーなど アドウェア アドウェア オートダイヤラー ユーザーに損害を与える目的で悪用される。 を検出する パッカー 一 悪意のあるコードを保護するために圧縮され ダ重圧縮オブジェクト 	可能性があるその している可能性が	/他のソフトウェア あるオブジェクト	
			OK	キャンセル	
(4) チェ	yクを入れると確認のメッセージが表示	🚶 検知するオブジェクトの種別			×
され	されますので、「OK」をクリックします。	このチェックボックスをオンにすると、悪意を持って使用される可能性がある特定の種別のアプリケーションが、指定されたプロテクション設定とスキャン設定に従って処理されます。 す。削除されたファイルはバックアップに移動されます。			
					ОК
(5) [Oł	く」をクリックして設定を反映させます。	🚶 検知するオブジェクトの種別		0 ×	
		 マルウェア ウイルス、ワーム トロイの木馬 悪意のあるツール アドウェア、オートダイヤラーなど アドウェア オートダイヤラー ユーザー(ご慣菁を与える目的で悪用されること検出する) パッカー 感意のあるコードを保護するために圧縮され、 タ重圧縮オブジェクト 	可能性があるその ている可能性が	/他のソフトウェア あるオブジェクト	
		ſ	ОК	キャンセル	
					1

5.5. Windows 共有フォルダーへのアクセスを許可する

KES をインストールしたデバイスは、既定で OS のファイアウォールが無効となり、KES のファイアウォールコンポーネントが有効となります。

KES のファイアウォールでは、以下の条件を満たすデバイス上にある Windows 共有フォルダーへのアクセスは可能です。

- (1) プライベートネットワークに所属しているデバイス。(以下の IP アドレスが設定されているデバイス)
 - · 172.16.0.0/12
 - · 192.168.0.0/16
 - · 10.0.0/8

(2) KES のファイアウォールで設定した「許可するネットワーク」に所属している。

社内で使用しているクライアント PC は、(1)に該当することが多いと考えられます。

上記以外に該当するクライアント PC に対して、共有フォルダーへのアクセスを許可する場合、「3.1 ファイアウォー ル設定」を参照してネットワーク範囲を「許可するネットワーク(またはプライベートネットワーク)」に追加するか、以下 の様にファイアウォールを設定します。

(1) 管理コンソールにて「管理対象デバイス」を

開きます。

右画面にて「ポリシー」タブを開き、「KES」 のポリシーを右クリックして「プロパティ」を選 択します。



III プロパティ:Kaspersky Endpoint Security for Windows (12.2.0) × (2)「脅威対策」-「ファイアウォール」を開きま 保護レベル:高 すべての推奨される保護機能が有効です。 す。 ファイアウォール 全般 ☑ ファイアウォール 🔎 「ファイアウォールルール」内の「ネットワーク イベントの設定 指定したルールに従ってネットワークパケットをフィルタリングします。 先進の脅威対策 ファイアウォールの設定 パケットとデータストリームのルールを設定し 脅威対策 設定 オペレーティングシステム内のアプリケーションネットワークルールを設定します。 ファイル脅威対策 ます。」欄の「設定」をクリックします。 ウェブ脅威対策 ネットワークパケットとデータストリームのルールを設定します。 設定 メール登蔵対策 ファイアウォール 使用可能なネットワーク ネットワーク脅威対策 設定 ネットワーク接続を設定します。 有害 USB 攻撃ブロック AMSI 保護 Detection and Response セキュリティコントロール データ暗号化 ローカルタスク 全般設定 ポリシーのプロファイル 変更履歴 ヘルプ OK キャンセル 適用(A) (3) 「ネットワークパケットルール」タブで以下の k ファイアウォール アプリケーションネットワークルール ネットワークパケットルール ネットワーク 項目を右クリックして「許可」に設定しま ネットワークパケットのルールの設定 Kaspersky Endpoint Security for Windows は既定で作成されるネットワークパケットルールを使用して、送信および受信のネットワーク動作を監視します。ネットワークパケットルールを追加または編集することで、ネットワークパケットおよびデータストリームに対する新し い条件や処理を作成できます。 す。 🕂 追加 🖉 編集 🗙 削除 💡 上へ 👃 下へ 🚞 ネットワークサービス 権限 ^ ・ローカルポート経由の TCP 接続 ✓ TCP 経由の DNS サーバーへの要求 ¥ ☑ UDP 経由の DNS サーバーへの要求 Ŧ ・ローカルポート経由の UDP 接続 ✓ メールの送信
 ✓ 任意のネットワーク動作 **₽** 許可するネットワーク □ 日意のネットワーク動作
 □ リモートデスクトップのネットワーク動作 プライベートネットワーク パブリックネットワーク • 0 ✓ # ✓ □ - カルボート経由の UDP 接続
 ✓ TCP ストリームの受信 設定後、「OK」をクリックして設定を反映さ 0 ⊘ ブロック ☑ UDP ストリームの受信 4 🗊 アプリケーションルールに準拠 せます。 ☑ ICMP「宛先到達不可能」応答の受信 ~ ☐ ICMP IIー応答の受信パケット ✓ ICMP「時間切れ通知」応答の受信 ■ イベントを記録 ~ ☑ ICMP ストリームの受信 ☑ ICMP v6 Tコー東求の受信パケット 000 🗸 - 許可 🖉 - ブロック 🖾 - アプリケーションルールによる処理 ОК 閉じる

本章は以上です。

株式会社カスペルスキー

〒101-0021 東京都千代田区外神田 3-12-8 住友不動産秋葉原ビル 7F

https://www.kaspersky.co.jp/ | https://kasperskylabs.jp/biz/

©2023 Kaspersky Labs Japan. Kaspersky Anti-Virus および Kaspersky Security は、AO Kaspersky Lab の登録商標です。 その他記載された会社名または製品名などは、各社の登録商標または商標です。なお、本文中では、TM、®マークは明記していません。 記載内容は 2023 年 9 月現在のものです。記載された内容は、改良の為に予告なく変更されることがあります。