

Kaspersky Security Center 14 Kaspersky Endpoint Security for Windows 初期設定ガイド

2023/1/27 株式会社カスペルスキー セールスエンジニアリング部 Ver. 1.0

目次

1.	はじめに	3
1	1. 本資料の目的	3
1	2. 導入から運用開始までの流れ	4
2.	前提	5
3.	事前準備(KES のポリシー、タスク作成)	6
3	8.1. ポリシーの作成	7
3	8.2. アップデートタスクの作成	11
3	3.3. スキャンタスクの作成	15
4.	必要な設定項目	20
4	1.1. パスワードによるアプリケーションの保護	20
	4.1.1.KES ポリシーの設定	20
	4.1.2.NA ポリシー設定	27
4	h.2.「ディストリビューションポイント」の自動割り当て解除	30
4	1.3. イベント通知設定	32
4	Ⅰ.4. ウイルスアウトブレイク通知設定	38
4	.5. 除外設定	42
4	↓.6. ウェブコントロール設定(バナー広告ブロック)	43
4	1.7. ログオンの監査の有効化	50
A	nondiv	F1

Ap	pendix	51
1.	「管理サーバークイックスタートウィザード」をキャンセルした場合	51
2.	インターフェイスの設定	52

1. はじめに

1.1. 本資料の目的

本資料では、法人向け製品を使用した環境を構築後、運用を開始する前に、Kaspersky Security Center や Kaspersky Endpoint Security for Windows において、必ず設定していただきたい項目 についてご説明します。

カスペルスキー製品の導入から運用開始までの流れ、および本資料の位置づけについてご説明します。



STEP 2.	管理サーバー機能のインストール、及びアンチウイルス製品のインストール → 「KSC14 簡単インストールガイド」
	「KES14 簡単リモートインストールガイド」をご参照ください。

STEP 3.	ポリシー・タスクの設定 → 「ポリシータスクの考え方」「ポリシータスク設定 実践編」をご参照ください。



	· · · · · · · · · · · · · · · · · · ·
STEP 5.	運用開始 → 「Kaspersky 運用ガイド」を参照し、各手順に従い運用してください。

上述の各資料は、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 (<u>https://kasperskylabs.jp/biz/</u>)

本資料は、以下の環境構成を前提としております。

- ✓ 管理サーバーとして Kaspersky Security Center が導入されている。
- ✓ 管理下の Windows に Kaspersky Endpoint Security for Windows が導入されている。
- ✓ 管理サーバーにてデバイスが管理されている。



■ 用語説明

① 管理サーバー:

Kaspersky Security Center がインストールされた Windows サーバーです。

- ② Kaspersky Security Center (以降 KSC):
 管理サーバーにインストールされた Kaspersky 製品を管理するアプリケーションです。
 Kaspersky Security Center ネットワークエージェントがインストールされたデバイスの管理と、定義データベースの配信を行います。
- ③ Kaspersky Endpoint Security for Windows (以降 KES):
 デバイスを保護するアンチウイルスアプリケーションです。
 管理サーバー及び管理下のコンピューターにインストールされます。
- ④ Kaspersky Security Center ネットワークエージェント(以降 NA):
 KSC とデバイスが通信をするために必要となるアプリケーションです。
 管理下のデバイスにインストールされます。(管理サーバーは KSC に含まれています)

3. 事前準備(KES のポリシー、タスク作成)

KSC14 では KES のインストールパッケージは同梱されておらず、使用する場合は以下のうちいずれかの方法でインストールパッケージ(アプリケーション管理プラグインも同様)を登録する必要があります。

● 「管理サーバークイックスタートウィザード」内で登録

手順は「KSC14 簡単インストールガイド」の「3.2 KSC の初期設定」をご参照ください。 この手順を実施した場合、KES のポリシー、および定義データベース更新タスクは自動で作成されます ので、「3.1 ポリシーの作成」および「3.2 アップデートタスクの作成」は実施不要です。 「3.3 スキャンタスクの作成」を参考に、スケジュールを設定したスキャンタスクを作成してください。

手順は「KSC14簡単インストールガイド」の「Appendix 1. KSCに対しインストールパッケージの登録」 をご参照ください。 この手順を実施した場合、ポリシー、タスクは自動的に作成されません。 本章の手順<u>「3.1 ポリシーの作成」</u>、「<u>3.2 アップデートタスクの作成」</u>、「<u>3.3 スキャンタスクの作成」</u>を 実施してポリシー、各タスクを作成してください。

参考:「Kaspersky Security Center 14 簡単インストールガイド」 https://kasperskylabs.jp/biz/



ここでは、KES のポリシーを作成する手順をご説明します。

(1)管理コンソールにて「管理対象デバイス」を Kaspersky Security Center 14 ファイル(F) 操作(A) 表示(V) ヘルプ(H) 開き、右画面にて「ポリシー」タブを開きま 🗢 🏟 🖄 📷 🛍 🛯 🖼 🧟 🛛 🖬 Kaspersky Security Center 14 ジ 目 管理サーバーKSC す。 管理サーバー KSC > 管理対象デバイス 🖵 管理対象デバイス ポリシー 「新規ポリシー」ボタンをクリックします。 デバイス ポリシー タスク デ パッシー
 菌 タスク
 ⑤ カスペルスキーのライセンス
 > ■ 詳細 ポリシーをファイルからインポート 列の追加 ステータス アプリケーション 名前 Kaspersky Security Center ネットワークエージェント ▲ Kaspersky Security Center ネットワークエージェント アクティブ Kaspersky Sec (2)新規ポリシーウィザードが起動します。 х 新規ポリシーウィザード [Kaspersky Endpoint Security for グループポリシー作成対象のアプリケーションを選択 Windows(xx.xx.xx)」を選択し、「次へ」 をクリックします。 ポリシーを作成するアプリケーションを選択します: k Kaspersky Security Center 管理サーバー Kaspersky Security Center ネットワークエージェント Kaspersky Endpoint Security for Windows (11.11.0) 次へ(N) キャンセル

(4)既定値のまま「次へ」をクリックします。

(3)任意のポリシー名を入力し、「次へ」をクリッ

クします。

× 4 新規ポリシーウィザード グループポリシーの名前を入力 名前: Kas □ 旧バージョンのアプリケーションのポリシー設定を使用する(U) 次へ(N) キャンセル × 4 新規ポリシーウィザード ポリシー作成モード ポリシー作成モードを選択すると、新しいポリシーを容易に作成できます。 既定の設定を選択した場合、必要な設定は、信頼するアプリケーションのリストとKSN への参加のみです。 ● 既定の設定でポリシーを作成 ○ ポリシーをウィザードで設定: ハッジーをパリートであた: ・ 設定のインボート ・ Kaspersky Security Network (2関する声明 ・ プロテカションの設定 ・ コントロールの設定 ・ 皆号代の設定 ・ 全般語定 ・ そ級語定 ・ パスワードによる(保護 次へ(N) キャンセル

- (5)「Kaspersky Security Network の使 用に同意する」にチェックを入れ、「次へ」を クリックします。
 - ※ インターネット接続のないクローズド環 境の場合は「・・・同意しない」にチェッ クを入れてください。

- (6)ポリシーのステータスにて「アクティブポリシー」 にチェックがあることを確認し、「完了」をクリ ックします。
 - ※ 作成だけ行い、デバイスに適用させたく ない場合は「非アクティブポリシー」を選 択して作成してください。 設定後、ポリシーのプロパティにて「アク ティブ」に変更するとデバイスへ適用さ れます。

		×
4	新規ポリシーウィザード	
к	aspersky Security Network への参加	
***	・新しい脅威にすばやく対応 ・保護機能のパフォーマンスを向上 ・誤検知率を低減	KSN
	5hm	\sim
50	Kaspersky Security Network(KSN)に関する声明 - Kaspersky Endpoint Security 11 for Windows	^
	Kaspersky Security Network に関する声明化に下FICSN 声明したい、オオンズ コンピューターソフトウェア Kasper Security 11をWindows(ビードホンフトウェルといいます)に適用れれます。 「データ処理に関する条件・10項をはじめに本ンフトウェアの使用料括契約および KSN 声明では、KSN 声明で 転送および逸望に関する条件。費用なもよび手続き(こついて説明します。同意する前に、KSN 声明の条項およ 参照される文書を注意深ん誘惑べださい。	sky Endpoint 示されるデータの J KSN 声明内で
	お客様が KSN の使用を有効にする際は、データ主体の個人データの処理が、とくに、一般データ保護規則(EL Protection Regulation、GDPR)(規則 2016/679)の第 6 条の 1 の (a) から (f) の規定(データ主体が取り付達 場合)、または、機密情報、個人情報およびデータ保護に関する法律を含む、適用される法律に定っているこ のとします。	J) (General Data 合内に存在する こに義務を負うも
	データの保護わよび処理 KSN の使用中に権利者がお客様から受け取るデーダは、権利者のブライバシーポリシー (https://www.kaspersky.co.jp/products-and-services-privacy-policy)に従って扱われます。	
	データ処理の目的 信頼税ネトリワーク上のセキュリティの脅威に対して本ソフトウェアの対応を早めることに役立てることを目的にして 目的は次の項目により実現します: - スキャンされるオブジェクトの評価の決定 - ネルやのに適切な手段を誘いることでの、お客様の端末上で保存および処理するデータの保護レベルの向上 - 読ん教の可能性の減少 - 読ん教の可能性の減少 - ふいとわっての機能の対率の向ト	こいます。前述の : : ・
() Kaspersky Security Network の使用に同意する	新規ウィンドウで開く
	次へ(N)	キャンセル
÷	新規ポリシーウィザード	×
ד	プリケーションのグループポリシーを作成	
	[完了]をクリックし、「Kaspersky Endpoint Security for Windows (11.11.0)」の作成処理を完了し、ウ じます。	ィザードを閉
	「ポリシーのステータス:	
	 アクティブポリシー 	
	○モバイルユーザーボリシー	
	□ ポリシーの作成後すぐにプロパティを開く	

(7)一覧に KES のポリシーが作成されているこ とを確認します。 ステータスが「アクティブ」となっているポリシー がクライアントに適用されます。

2 51				
	<u>管理サーバー KS</u> ● ポリシー	C > 管理対象デバイス		
	デバイス ポリシ	929		
	新規ポリシー	ポリシーをファイルからイン	オート	列の遺加と削除
	名前 	A	ステータス	アプリケーション
	Caspersky Endpo	oint Security for Windows (11.11.0)	アクティブ	Kaspersky Endpoint Security for Windows (11.11.0)
	Kaspersky Security	Center ネットワークエージェント ty Center ネットワークエージェント	アクティブ	Kaspersky Security Center ネットワークエージェント

本節は以上です。



ここでは、KES に対し、KSC から定義データベースを更新するためのタスクを作成する手順をご説明します。

Kaspersky Security Center 14 (1)「管理対象デバイス」を開き、右画面にて ファイル(F) 操作(A) 表示(V) ヘルプ(H) 「タスク」タブを開きます。 🗢 🔿 🙍 📅 📋 📾 🐼 🖬 Kaspersky Security Center 14 「新規タスク」ボタンをクリックします。 <u>管理サーバー KSC</u> > 管理対象デバイス □ 管理サーバーKSC 🖵 管理対象デバイス □ モハイルテハイス管理 □ デバイスの抽出 ⊙ グループタスク ■ 未割り当てデバイス デ ポリシー デバイス ポリシー タスク 新規夕フ タスクをファイルからインポート 列の追加 アプリケーション タスクを 名前 脆弱性とアプリケーションのアップデートの検索ー □ 脆弱性とアプリケーションのアップデートの検索 Kaspersky Sec... 脆弱性 Х (2)新規タスクウィザードにて「Kaspersky 新規タスクウィザード Endpoint Security for Windows」配 タスク種別の選択 下の「アップデート」を選択し、「次へ」をクリ 🖃 👿 Kaspersky Endpoint Security for Windows (11.11.0) ックします。 📋 BitLocker 保護の管理 IOC スキャン
 アップデート 📃 アップテートのロールバック インベントリ 📋 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 💼 プロセスを開始 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 ■ 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

 (3) アップデート元として「Kaspersky Security Center」が選択されていることを確認 し、「次へ」をクリックします。



(4)タスクを実行するアカウントの選択では、既 定値のまま「次へ」をクリックします。

(5)タスクスケジュールの設定にて任意のスケジ ュールを設定し、「次へ」をクリックします。 ここでは、KSC が新しい定義データベースを ダウンロードした場合に随時更新されるよう 「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」と設定しています。	← 新規9スクウィザード タスクスケジュールの設定 実行予定: 新しいアップデートがリボジトリにダウンロードされ次第	×
	 □ 未実行のタスクを実行する(R) □ タスクの開始を自動的かつランダム(ご遅延させる(A) □ タスクの開始を決か時間範囲内でランダム(ご遅延させる(分)(D): 1 	
(6)任意のタスク名を入力し、「次へ」をクリック します。 ここでは、「アップデートのインストール」という 名前を設定しています。	← 新規9スクウィザード タスク名の定義	×
	名前: アップデートのインストール	
	次へ(N) キャンセル	

(7)正常に作成されたことを確認し、「完了」を クリックします。	← 新規タスクウイザード タスク作成の終了 [完了] をクリックし、「アップデートのインス	トール」の作成処理を完了し、ウイザードを閉じます。	×
	□ ウィザードの終了後にクスクを実行(R)		
		完了(F)	キャンセル
(8)タスクの一覧に作成したタスクが表示されて	Kaspersky Security Center 14		
	ファイル(F) 操作(A) 表示(V) ヘルプ(H)		
ς ιδςς σμεπιά Ο α 9 °	 	 管理サーバー KSC > 管理対象デバイス ⑦ グループタスク デバイス ポリシー タスク 新規タスク タスクをファイルからイン 名前 アップデート アップデート アップデートの1ンストール Ka 院弱性とアプリケーションのアップデートの検索 福朝性とアプリケーションのアップデートの検索 	ポート <u>列の追</u> ガリケーション spersky Endpoint Se spersky Security Cer

本節は以上です。



ここでは、KES に対し、KSC から定義データベースを更新するためのタスクを作成する手順をご説明します。 スキャンを定期的に実行することで、セキュリティレベルの設定が低いなどの理由により、保護コンポーネントで検知 されない悪意のあるソフトウェアが拡散する可能性を排除できます。

KSC インストール後にクイックスタートウィザードを実行すると、KES のポリシーやタスクが自動的に作成され ますが、KES のスキャンタスクは作成されないため、本手順を参照しスキャンタスクを作成してください。

(1)「管理対象デバイス」を開き、右画面にて 「タスク」タブを開きます。 「新規タスク」ボタンをクリックします。



 (2)新規タスクウィザードにて「Kaspersky Endpoint Security for Windows」配 下の「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) 任意のスキャン範囲を選択し、「次へ」をクリ ックします。

ここでは既定値を設定しています。

(4)処理の設定では、既定値のまま「次へ」をク

リックします。



(5)タスクを実行するアカウントの選択では、既 定値のまま「次へ」をクリックします。

(6)タスクスケジュールの設定にて任意のスケジ ュールを設定し、「次へ」をクリックします。 ここでは、毎週水曜日 12:00 から開始さ れるよう設定しています。	÷	新規タスクウィザード タスクスケジュールの設定 実行予定: 毎週 曜日: 開始時刻:	水昭晋日 12:00:00 🔹	~	×
		□ 未実行のタスクを実行する(R) ☑ タスクの開始を自動的かつランダムに近延され □ タスクの開始を次の時間範囲内でランダムに	さ(A) 遅延させる(分)(D):		¢
				次八(N) キャ	ッセル
(7)任意のタスク名を入力し、「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			×
ここでは、「定時スキャン(毎週水曜 12 時)」という名前を設定しています。					
		名前: スキャン(毎週水曜12時)			

次へ(N) キャンセル

(8)正常に作成されたことを確認し、「完了」を X 4 新規タスクウィザード クリックします。 タスク作成の終了 [完了]をクリックし、「スキャン(毎週水曜12時)」の作成処理を完了し、ウイザードを閉じます。 □ ウィザードの終了後にタスクを実行(R) 完了(F) キャンセル Kaspersky Security Center 14 (9)タスクの一覧に作成したタスクが表示されて ファイル(F) 操作(A) 表示(V) ヘルプ(H) いることを確認します。 💠 🏟 🙍 📷 📋 🗂 🕿 Kaspersky Security Center 14 【 Kaspersky Security Center 1 ● 目 管理サーバー KSC ● 日 管理サネデバイス ● 日 新規グループ ● 日 ボイルデバイス管理 日 デバイスの抽出 ■ 計 未割り当てデバイス デア ポリシー ● ロ マローク 管理サーバー KSC > 管理対象デバイス ☞ グループタスク デバイス ポリシー タスク タスクをファイルからインポート 列 名前 アプリケーション アップデート・ 📋 アップデートのインストール Kaspersky Endpoi 🗍 スキャン (毎週水曜12時) Kaspersky Endpoi 脆弱性とアプリケーションのアップデートの検索 ■ 脆弱性とアプリケーションのアップデートの検索 Kaspersky Security

本章は以上です。

KSC にて KES を管理している環境下において、必要な設定項目についてご説明します。 セキュリティの保護、また不要なトラブルを避けるために、以下にご案内いたします設定を必ず実施してください。

4.1. パスワードによるアプリケーションの保護

KES、及び NA に対し、パスワードによる保護を設定することができます。(既定では無効) パスワードによる保護を設定することで、デバイスの利用者がKESプロセスを終了しようとした場合や、アンインスト ールしようとした場合に、パスワード入力を求める画面が表示されます。

意図的な KES プロセスの停止やアンインストールを制限することでデバイスの保護を強固にします。

【注意】

KSC から KES のアップグレードやアンインストールを行う場合は、「パスワードによる保護」を一時的に 無効化する必要があります。

以下に KES、NA に対し、「パスワードによる保護」を有効化する手順をご説明します。

4.1.1. KES ポリシーの設定

Kaspersky Security Center 14 (1)「管理対象デバイス」を開き、右画面にて ファイル(F) 操作(A) 表示(V) ヘルプ(H) 🔶 🧼 🙇 💼 🗈 🛯 🖬 🙆 🖬 「ポリシー」タブを開きます。 Kaspersky Security Center 14 > 目 管理サーバーKSC 管理サーバー KSC > 管理対象デバイス KES のポリシーを右クリックし、「プロパティ」 ⊚ ポリシー を開きます。 デバイス ポリシー タスク マボリシー 自 タスク 引 カスペルスキーのライセンス > ### ポリシーをファイルからインポート 列の追加と削除 名前 ステータス アプリケーション v Endpoint Security for Windows (11.11.0 Kaspersky Endpoint Security for Windows (11.11.0)
 アクティブポリシー Vind ポリシーを他のポリシーと比較(C) 📓 Kaspersky Security Center ネットワークエージェント -7I エクスポート(E) すべてのタスク(1) 列でグループ分けする 初り取りにつ ∃ピ-(C) 削除(D) リストのエクスポート(E) プロパティ(P)

(2)ポリシーのプロパティ画面にて、「全般設定」 III プロパティ: Kaspersky Endpoint Security for Windows (11.11.0) 保護レベル:高 すべての推奨される保護機能が有効です。 -「インターフェイス」セクションを開きます。 セクション インターフェイス 全般 イベントの設定 先進の脅威対策 □ アプリケーション動作モニターセクションを非表示
 ○ 簡略化したインターフェイスを表示する 右画面にて「パスワードによる保護」の「設 脅威対策 〇 表示しない Detection and Response 定」ボタンをクリックします。 🗑 - ið m -セキュリティコントロール Kaspersky Endpoint Security for Windows の操作中に発生したイベントの通知の設定 設定 データ暗号化 ローカルタスク ■ - 状態・ 全般設定 設定 通知領域の Kaspersky Endpoint Security for Windows アイコンの警告 アプリケーション設定 「ローカル定義データベースのステータスに関する通知 ―― 定義データベースの未アップデートを通知する未アップデート期間 ネットワークの設定 除外リスト 定義データベースの長期間未アップデートを通知する未アップデート期間 レポートと保管領域 - パスワードによる保護 インターフェイス パスワードによる保護が無効 ポリシーのプロファイル 設定 変更履歴 ゴーユーザーサポート・ 設定 サポート情報 AH7 Γ ОК (3)「パスワードによる保護を有効にする」にチェ ໄ パスワードによる保護 ックを入れます。 パスワードによる保護を使用すると、Kaspersky Endpoint Security for Windows の機能や設定の 一部またはすべての管理に制限を設定できます。制限を設定することで、本製品の機能が不正に 変更されたり、意図せずに変更してしまったりする危険性を低減できます。ユーザー名の推奨既定 値は KLAdmin です。 「KLAdmin lを選択し、「編集 lをクリックし ます。 ☑ パスワードによる保護を有効にする 権限 ※「KLAdmin」は、既定で設定されてい + 追加 🖉 編集 × 削除 ユーザーまたはグループ Δ 権限 るパスワード保護のアカウント名です。 Everyone レポートの表示; 太製品の設定。 (4)で変更することも可能です。 木製品の

×

3 🗘 日

7 🖨 🗄

キャンセル 適用(A)

0

×

9

キャンセル

OK



NLAUMIN		バスワード
権限		
 本製品の終了 保護機能の停止 管理コンボーネントの停止 管理コンボーネントの停止 Kaspersky Security Center ライセンスの削除 ライセンスの削除 本製品の削除 / 変更 / 修 暗号化されたドライブ上の: レボートの表示 バックアップから復元 すべて選択 すべて選択解除 	r ポリシーの無効化 約 データへのアクセスの	/復元
		101
	ОК	キャンセノ
	ОК	キャンセル

(5)「パスワード」と「新しいパスワードの確認」を 入力し、「OK」をクリックします。

```
以下のパスワード要件を満たさない場合、
警告が表示されます。(設定は可能)
・8 文字以上
・次の各文字種別から1文字以上使用:
```

```
-大文字アルファベット
-小文字アルファベット
```

```
-数字
```

```
-特殊文字(~!@#%^{}[]<>?;':,/¥-_=+)
```

170-k.		
•••••	0 🗸	
所しいパスワードの確認:		
•••••	~	

(6)「OK」をクリックし、設定を保存します。 既定では、すべての操作がパスワード保護 の対象になっています。

 \odot × 【 ユーザーまたはグループの権限 ユーザーまたはグループ パスワード... KLAdmin 権限 ☑ 本製品の設定 ☑ 本製品の終了 ☑ 保護機能の停止 ☑ 管理コンボーネントの停止 ✓ Kaspersky Security Center ポリシーの無効化 ☑ ライセンスの削除 ☑本製品の削除/変更/修復 ☑ 暗号化されたドライブ上のデータへのアクセスの復元 ☑ レポートの表示 ☑ バックアップから復元 すべて選択 すべて選択解除 キャンセル OK 🚶 パスワードによる保護 × パスワードによる保護を使用すると、Kaspersky Endpoint Security for Windows の機能や設定の 一部またはすべての管理に制限を設定できます。制限を設定することで、本製品の機能が不正に 変更されたり、意図せずに変更してしまったりする危険性を低減できます。ユーザー名の推奨既定 値は KLAdmin です。 ☑ パスワードによる保護を有効にする 権限 + 追加 Ø 編集 × 削除 9 ユーザーまたはグループ 権限 Δ レポートの表示; Everyone KLAdmin OK キャンセル

(7)「OK」をクリックし、設定を保存します。

(8)「OK」をクリックしてポリシーのプロパティ画面 を閉じます。



設定は以上になります。

デバイスに KES ポリシーが適用されると、パスワード保護機能が有効となります。

デバイス側で KES を終了しようとした場合、以下のようにダイアログが表示されます。

(1) デバイスにて、タスクバーの KES アイコンを 右クリックし、「終了」を選択します。	
	Kaspersky Endpoint Security for Windows
	保護機能の一時停止
	ポリシーを無効にする
	設定
	サポート
	製品情報
	释了
	🔌 💿 k
(2) ユーザー名とパスワードの入力を求めるダイ アログが表示されます。	kaspersky X
正しいユーザー名、パスワードを入力しな	Kaspersky Endpoint Security for Windows を 終了しますか?
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。 認証方法 :
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。 認証方法: ユーザー名とパスワード ~
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。 認証方法: ユーザー名とパスワード 〜 ユーザー名:
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。 認証方法: ユーザー名とパスワード ~ ユーザー名: KLAdmin
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。 認証方法: ユーザー名とパスワード ~ ユーザー名とパスワード ~
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。 認証方法: ユーザー名とパスワード ~ ユーザー名とパスワード ~ ユーザー名とパスワード ~ ユーザー名とパスワード ~ コーザー名とパスワード ~ コーザー名とパスワード ~ パスワード:
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終了しますか? コンピューターの安全性が低下します。 認証方法: ユーザー名とパスワード ~ ユーザー名とパスワード ~ ユーザー名・ ドLAdmin ノスワード: 「 「
正しいユーザー名、パスワードを入力しな いと、KES を終了させることはできません。	Kaspersky Endpoint Security for Windows を 終 了しますか? コービューターの安全性が低下します。 認証方法: ユーザー名とパスワード ~ ユーザー名とパスワード ~ ユーザー名: ドLAdmin ユーザー名の既定値:KLAdmin パスワード:

また、デバイスにて KES をアンインストールしようとした際にも、以下のようにアカウントの入力を求められます。

 デバイスにて「コントロールパネル」-「プログ ラムと機能」から KES をアンインストールし ようとすると、ウィザード内で右のようにアカ ウントの入力を求められます。

> 正しいユーザー名、パスワードを入力しな いと、KES をアンインストールすることはでき ません。

🖟 Kaspersky Endpoint Security for Windows		
本製品の変更、修復、アンインストール用パスワード Kaspersky Endpoint Security for Windows のパスワードを入う	りしてください。	
Kaspersky Endpoint Security for Windows を変更、修復、ま ーアカウント名とパスワードを入力してください。	たはアンインストールで	するには、ユーザ
ዎታታን/ትዳ:		
, パスワード:		
-(c) 2022 AO Kaspersky Lab	次^ >	キャンセル

本項は以上です。



(1)「管理対象デバイス」を開き、右画面にて
 「ポリシー」タブを開きます。
 NAのポリシーを右クリックし、「プロパティ」を
 開きます。



「アンインストール用パスワードを使用する」 にチェックを入れ、「変更」ボタンをクリックし ます。





(3) ダイアログに新しいパスワードを入力し、 「OK」をクリックします。



(4) ステータスに「パスワードが設定されていま す」と表示されていることを確認後、「OK」 をクリックし、プロパティ画面を閉じます。

設定は以上になります。

デバイスにNAポリシーが適用されると、パスワード保護機能が有効となります。

クライアント側で NA をアンインストールしようとした場合、以下のようにダイアログが表示されます。

 デバイスにて「コントロールパネル」-「プログ ラムと機能」から NA をアンインストールしよ うとすると、ウィザード内で右のようにアカウ ントの入力を求められます。

> 正しいパスワードを入力しないと、NA をア ンインストールすることはできません。

17	-		×
アンインストール用パスワード アプリケーションのアンインストール用パスワードを入力します。			
Kaspersky Security Center ネットワークエージェント は、許可な〈アン1	シストールされ	1ないよう(こパス
ワードで保護されています。アンインストールを続行するには、アンインス てください。	ヘトール用パス	ワードを打	皆定し
< 戻る(8) 次	^(N) >	キャン	セル

本節は以上です。

4.2. 「ディストリビューションポイント」の自動割り当て解除

「ディストリビューションポイント」とは、定義データベースやインストールパッケージの配信元となる機能です。 ディストリビューションポイントを設定することで、管理下のデバイスは定義データベースをディストリビューションポイン トから取得するようになるため、ネットワークトラフィックや KSC の負荷を軽減することができます。

このディストリビューションポイントは、既定で自動的に端末に対して割り当てられる設定となっております。 そのため、業務系アプリケーションサーバーや、普段使用しているデバイスが指定される可能性があり、ディスク使 用量の増加やリソースの消費、意図しない通信の発生など、予期せぬ問題が発生する可能があります。

アップデートエージェントの詳細や、手動による割り当て手順は以下サイトにある「ディストリビューションポイント設 定ガイド」をご参照ください。

法人のお客様向けダウンロード資料 (https://kasperskylabs.jp/biz/)

以下に、ディストリビューションポイントが割り当てられる設定を「自動」から「手動」へ変更する方法についてご説 明します。

ディストリビューションポイントの自動割り当てを解除した場合、KSC 管理サーバーの管理下にある全デバイ スは、直接 KSC 管理サーバーへ接続し定義データベースのダウンロードを行います。

(1)「管理サーバー」を右クリックし、「プロパテ ィ」を開きます。



(2)「ディストリビューションポイント」セクションを 開きます。



当て」にチェックを入れます。

す。

「OK」をクリックしプロパティ画面を閉じま

本節は以上です。



ウイルス検知など、管理下のデバイスにて重要なイベントが発生した場合、管理サーバーから管理者へメールを送 信することができます。

以下に、KSC にて管理者のメールアドレスを設定し、特定のイベント発生時にメール通知を行う設定についてご 説明します。

(1)「管理サーバー」を右クリックし、「プロパテ ィ」を開きます。

(2)「通知」セクションを開きます。 宛先に送信先となるメールアドレス、 SMTP サーバーアドレス、ポートを入力しま す。

認証など、詳細な設定を行う場合は「設定」をクリックします。



(3)「件名」には、メール通知時の件名を設定 することができます。

送信者のメールアドレスを指定したい場合 は「送信者のメールアドレス」のフィールドに 入力します。指定しない場合は、宛先に 指定したアドレスが送信者として表示され ます。

ESMTP 認証を使用する場合は、 「ESMTP 認証を使用する」にチェックを入 れ、「ユーザー名」「パスワード」を入力しま す。

SMTP サーバーの TLS 設定を指定する場合は、「SMTP サーバーの TLS 設定を指定」をクリックします。

(4) SMTP サーバーの TLS 設定をします。

「TLS を使用する(SMTP サーバーがサ ポートする場合)」を選択した場合、管理 サーバーは TLS をサポートしていない SMTP サーバーとは TLS を使用せずに接 続します。

「TLS を常に使用し、サーバー証明書の 有効性をチェックする」を選択した場合、管 理サーバーは TLS をサポートしていない SMTP サーバーへ接続できません。

クライアント証明書を指定する場合は、 「TLS を常に使用し、サーバー証明書の 有効性をチェックする」を選択し、「クライア ント証明書の設定」をクリックします。

牛名:	
き信者のメールアドレス:指定され 主意:実在しないアドレスは使用し	, Cいない場合は、受信者のアドレスを使用します。 しないでください。
✓ ESMTP 認証を使用する(E)
組織しベルの機密データ(ドまイ	
ADDREED STOLEN	
フーザータ・	XXXXX
ユーザー名: パスワード:	xxxxxx
ユーザー名: パスワード:	xxxxx
ユーザー名: パスワード:	xxxxx
ユーザー名: パスワード: MTP サーバーの TLS 設定を指定	xxxxx
ユーザー名: パスワード: MTP サーバーの TLS 設定を指定	xxxxx
ユーザー名: パスワード: MTP サーバーの TLS 設定を指定	xxxxx
ューザー名: パスワード: <u>MTP サーバーの n.s 設定を指定</u>	xxxxx

SMTP TLS 設定	
○TLS を使用しない(N)	
◯ TLS を使用する(SMTP サーバーがサポートする場合)(U)	
● TLS を常に使用し、サーバー証明書の有効性をチェックする(T):	
SMTP サーバーで使用する TLS バージョン:	
TLS 1.2 以降のバージョンのみ使用する	· · · · · · · · · · · · · · · · · · ·
サポートされる任意のバージョン	
TLS 1.2 以降のハーションのみ使用する	
	^
<	>
	参照
クライアント証明書の設定	
	OK キャンセル

(5) 証明書を指定するため「参照」をクリックし ます。

(6) 「証明書の種別」にて「x.509 証明書」か 「PKCS#12 コンテナー」を選択します。

> 「参照」をクリックし、秘密鍵や証明書ファイ ルを選択します。

> 設定後、「OK」をクリックして設定を保存します。

(7)「OK」をクリックし、設定を保存します。

署名用の証明書			×
 証明書ファイルの選択:			
	לם גליד גע ו	81	R全(わ)
-30-98(D)	/U/\/1(P)	E'.	pr(D)
		OK	キャンセル
			X
			^
■ 証明書の種別:	X.509 証明書		~
9年-21日22月至22.3。	PKCS #12 コンラ	֠	
秘密鍵 (*.prk, *.pem):	X.509 証明書	_	
		参照	l
パスワード:			
証明書 (*.cer):		¬	
		参照	l
		OK	キャンパフル
設定			? ×
件名:			
送信者のメールアドレス:指定されていない場合は 注意:実在しないアドレスは使用しないでください。	t、受信者のアドレス	を使用します。	
「CENTD 羽耳た使用オス/E)			
● こうていて 正正をに入り 多し()	******	湯かど)け (見方しかい)	ことた雄将します
	/ 6 × 1 1 (V) (U) (1 1 (1 4	18/8とハ&、1本1子()/86 い	CC21E X UA90
	XXXXXX		
パスワード:	•••••		
<u>SMIPリーハーのILS iR定位指定</u>			
		OK	キャンセル

(8)「OK」をクリックし、通知の設定を保存しま

す。

- 💽 プロパティ:管理サーバー KSC Х 通知 全般 🐱 メール 🔛 SMS 🗔 実行ファイル イベントの設定 ライセンス 受信者(メールアドレス): KSN プロキシ admin@kaspersky.com 管理サーバー接続設定 XXX.XXX.XXX.XXX SMTPサーバー: ウイルスアウトブレイク 25 SMTP サーバーのポート: トラフィック イベンドリポジトリ DNS MX ルックアップを使用(M) Web サーバー 設定(S) 変更履歴リポジトリ 通知メッセージ: イベント「NEVENTK」が Windows ドメイン「NDOMAINK」のデパイス「NCOMPUTERK」で NRISE_TIMEK に発生しましたNDESORN アプリケーションカテゴリ • 暗号化アルゴリズム カスペルスキーからの通知 ディストリビューションポイント タグルール グローバルサブネットのリスト 通知 変更履歴 頻出イベントのブロック 副羊糸田 通知数の上限を設定する テストメッセージの送信(S) <u>^1+7</u> ОК キャンセル 適用(A) Kaspersky Security Center 14 ファイル(F) 操作(A) 表示(V) ヘルブ(H)
 マーマン
 < 管理サーバー KSC > 管理対象デバイス ⊙ ポリシー デバイス ポリシー タスク ポリシーをファイルからインポート 列の追加と削除 名前 ステータス アプリケーション v Endpoint Security for Windows (11.11. Kaspersky Endpoint Security for Windows (11.11.0) Vind アクティブポリシー Kaspersky Security Center ネットワークエージェント Kaspersky Security Center ネットワークエージェント ポリシーを他のポリシーと比較(C) -71 エクスポート(E) すべてのタスク(L) 列でグループ分けする 切り取り(C) JK-(C) 削除(D) リストのエクスポート(E) プロパティ(P)
- (9)「管理対象デバイス」を開き、右画面にて
 「ポリシー」タブを開きます。
 KES のポリシーを右クリックし、「プロパティ」
 を開きます。

(10) 「イベントの設定」セクションを開きます。

管理者へ通知したいイベントを選択し、 「プロパティ」をクリックします。 (ここでは「悪意のあるオブジェクトが検知 されました」を指定しています)

- III プロパティ:Kaspersky Endpoint Security for Windows (11.11.0) X 保護レベル:高 すべての推奨される保護機能が有効です。 セクション イベントの設定 全般 🕕 緊急 🕕 機能エラー 🔺 警告 🕕 情報 イベントの設定 ● 編集をロック ~ ①-先進の脅威対策 脅威対策 保管期間 イベント種別 Detection and Response ライセンス違反です 30 日 ライセンスの有効期間が終了します
 ライセンスの有効期間が終了します
 定義データベースが存在しないか、破損しています
 定義データベースが長期間アップデートされていません
 コンピューター起動時の自動起動が無効です <保存しな(い> セキュリティコントロール <保存しない> <保存しない> データ暗号化 ローカルタスク 30日 アクティベーションエラー 30 H 全般設定 アクティイトーションコン アクティブな者感が検知されました。特別広駆除を開始する必要があ... KSNサーバーが使用できません 隔離の保管領域に十分な空き容量がありません 30日 30日 ポリシーのプロファイル 30日 変更履歴 時続のJRを管理版にてかな空客音量がありません。 オブジェクトは掲載的や音呼添されませんでした。
 オブジェクトは掲載から音呼添されませんでした。
 アブリケーションが信頼をれない証明書を持つ Web サイトとの接続を、
 時春化をおわたは感を検醒でなせんでした。ドメイ・友陸分川フトに定 意意のあるオブジェクトが検知されました。(ローカル定義データベース) 30日 30日 30日 30 E 思想のあるオフン 駆除できません 削除できません 悪気のあるブンゴントル使知。
 駆除できません。
 削除できません。
 削除できません。
 処理エラー
 プロセスが終了しました。
 プロセスな終了できません。
 危険なリンクを打っかしました。
 危険なリンクを打きました。
 しば割買いたのためた。 30 ⊟ 30 ⊟ 30 ⊟ <保存しない> 30日
 <(保存しない> 0 0 0 30日 30日 に以前開いた危険なリンクを検知しました プロセスの処理がブロックを検知しました キーボードが認証されませんでした 30 ⊟ 30 ⊟ 30 ⊟ < プロパティ(P) すべて選択(S) 1117 ОК キャンセル 適用(A)
- (11) プロパティ画面にて、「メールで通知」 にチェックを入れ、「OK」をクリックします。

管理サーバーで設定した宛先とは別の宛 先を設定する場合、「設定」をクリックする ことでカスタマイズが可能です。

プロパティ:悪意のあるオブジェクトが検知されました(ローカル定義データベース)		×
イベント登録		
図管理サーバーのデータベースに保存(日)(S):	30	
□ Syslog 経由で SIEM システム(ニエクスポートする(Y)		
□デバイスの OS イベントログに保存(D)		
□管理サーバーの os イベントログに(保存(A)		
イベント通知		
☑ メールで通知(E)		
SMS で達美知(S)		
□実行ファイルまたはスクリプトの実行で通知(R)		
□ SNMP 経由で通知(M)		
既定では、管理サーバーの設定タブで設定された)触知設定が使用されます(たとえ スなど)。各設定を変更するには、[設定]をクリックします。	は、受信者のアドレ	
	設定	
Of	く キャンセル	

(12) 通知設定されたイベントには、メール のアイコンが表示されます。

「OK」をクリックし設定を保存します。



本節は以上です。

管理下のデバイスにて大量のウイルス検知が発生した場合、「ウイルスアウトブレイク」の通知を発信することができます。管理者は通知を受け取ることで、マルウェアの脅威に対して迅速に対応することができます。

以下に、アウトブレイクの通知を有効化する設定についてご説明します。

(1)「管理サーバー」を右クリックし、「プロパテ ィ」を開きます。

(2)「通知」セクションを開きます。
 宛先に送信先となるメールアドレス、
 SMTP サーバーアドレスを入力します。

※設定済みの場合、本手順は不要で す。



(3)「ウイルスアウトブレイク」セクションを開きま す。

> 「ワークステーションとファイルサーバー向けア ンチウイルス」にチェックを入れます。

既定では管理下のデバイスにて「10分 間」に「10個」のマルウェアが検知した場 合、アウトブレイクを通知する設定となって おります。

運用に合わせ設定を変更してください。



(4)「イベントの設定」セクションを開きます。

「緊急イベント」タブ内にある、「ウイルスアウ トブレイク」を選択し、プロパティをクリックし ます。

キャンセル 適用(A)

ОК

(5)「メールで通知」にチェックを入れ、「OK」を クリックします。



(6)「ウイルスアウトブレイク」にメールアイコンが 設定されていることを確認し、「OK」をクリッ クします。

管理下のデバイスからのウイルス検知イベント受 信数がしきい値を超えた場合、右記の「ウイル スアウトブレイク」イベントが記録されます。

同時に設定したメールアドレスへメール通知が 行われます。

	A 101.		
	主版		
全般	ילאגדילי !	10	
	深刻度:	緊急	
	アプリケーション:	Kaspersky Security Center 管理サーバー	
	パージョン:	14.0.0.10902	
	タスク名:		
	デバイス:	管理サーバー <ksc></ksc>	
	グループ:	管理対象デバイス	
	日時:	2023年1月18日 17:21:02	
	仮想管理サーバー名:		
	 党 月:		
∧⊮ Ź		< 戻る(8) 次へ(14) > グリップボード(こ	」ピー(C) 問いる

本節は以上です。

資産管理、バックアップなどのアプリケーションは、その動作の性質上、KES に検知される可能性があります。

業務上必要となるアプリケーションで、検知など KES による影響を受けたくないものがある場合、KES の監視対象から除外設定を実施することで対応が可能です。

また、イントラネットサイトや、業務上閲覧する必要があるサイトがある場合、URL を KES の検知から除外することもできます。

KES の検知対象から除外が必要なアプリケーション、ファイル、URL の確認を行い、運用開始前に設定を実施 してください。

手順は以下サイトにある「除外設定ガイド」をご参照ください。 法人のお客様向けダウンロード資料 (https://kasperskylabs.jp/biz/)

本節は以上です。

4.6. ウェブコントロール設定 (バナー広告ブロック)

本章では、「ウェブコントロール」機能にて、バナー広告をブロックする設定についてご説明します。

「ウェブコントロール」とは、Webリソースへのアクセスを制限、またはブロックする機能です。ギャンブルサイトや SNS など、コンテンツを指定して制御することができます。

コンテンツの一つとして「バナー」を制御することができます。

不正なバナー広告にアクセスした場合、悪意のあるWebサイトへの転送や、フィッシングの被害にあう可能性もありますが、本設定を実施することで不正なバナー広告自体を非表示とすることができます。

以下に、「ウェブコントロール」を使用して、バナーの表示をブロックする設定をご説明します。

(1)「管理対象デバイス」を開き、右画面にて
 「ポリシー」タブを開きます。
 KES のポリシーを右クリックし、「プロパティ」
 を開きます。



(2)「セキュリティコントロール -「ウェブコントロー	🔳 プロパティ:Kaspersky Endpoint Secu	rity for Windows (11.11.0) - 🗆 🗙
	保護レベル:高	すべての推奨される保護機能が有効です。
ル」ビクションを用きます。	セクション 金融	
	イベントの設定	ビリエノコントロール ■ ユーザーの Web リソースへのアクセスをコントロールします。
ウェブコントロール設定面面にて「追加」をク	先進の脅威対策	
	肖敬州東 Detection and Response	+ 追加
リックします。	セキュリティコントロール	1/14 レジュ ル ルーム アイス アン パン
	Windows イベントロク監視 アプリケーションコントロール	
	รี/หี/גבントロール	
	ウェブコントロール	
	アダプティブアノマリーコントロール ファイル変更監視	
	データ暗号化	油田オスコーザー,
	ローカルタスク 全般語定	データ種別で約り込み:
	ポリシーのプロファイル	コンテンツの力テゴリで絞り込み:
	変更履歴	適用するアドレス:
		リレールの処理:
		メッセージのテンプレートの設定
		テンプレート 推奨されない Web ページまたは Web サイトが閲覧されたときに表示されるメッセージのテンプレートを設定します。
		詳細設定
		詳細設定
	<u>^#7</u>	OK キャンセル 適用(A)
(3)「名前」に仕意の名前を人力します。(ここ	🚶 Web リソースへのアクセ	27.11-11 🛈 X
では「バナーブロック」としています)		
	名前: バナーブロック	
	コンテンツのフィルタリング:	すべてのコンテンツ ~
	適用するアドレス:	すべてのアドレス ~
	適用するユーザー:	すべてのユーザー ~
	処理:	許可 🗸
	ルールのスケジュール:	常時 ~ 設定
		OK キャンセル
(4)「コンテンツのフィルタリング」のリストボックス	🚶 Web リソースへのアクセ	2711-11 🗿 🗙
から「コンテンツカテゴリ」を選択します。		
	名前: バナーブロック	
	コンテンツのフィルタリング:	すべてのコンテンツ ~
	適用するアドレス:	すべてのコンテンツ
	適用するユーザー:	テータ種方り コンテンツカテゴリとデータ種別
	処理:	ブロック マ
	ルールのスケジュール:	常時 > 設定
		and the state of
		いん イヤノセル

(5)カテゴリを選択する画面が表示されるので、 「バナー広告」にチェックを入れます。

「処理」の項目を「ブロック」と設定します。

設定後、「OK」をクリックして画面を閉じま す。



ルールの処理:

メッセージのテンプレートの設定

テンプレート

詳細設定

(6)追加した「バナーブロック」が一番上にあるこ とを確認します。 「OK」をクリックし設定を保存します。

ポリシーが適用されたデバイスは、不正なバ ナー広告の表示がブロックされます。

キャンセル 適用(A)

推奨されない Web ページまたは Web サイトが閲覧されたときに表示されるメッセー ジのテンプレートを設定します。

OK

カテゴリの一つに、「日本の警察庁主導の取組 みによる禁止対象」があります。

日本の警察庁が危険と設定したサイトの閲覧 をブロックできます。

ブロックするカテゴリの一つとしてご検討ください。

名前: バナーブロック			
コンテンツのフィルタリング:	コンテンツカテゴリ		~
 ビデオゲーム アダルト アルコール、タバコ、ドラッ・ ギャンブル、宝くじ、懸賞 国・地域の法律による禁 ロシア連邦の法律による ベルギーの法律による マ日本の警察庁主導の 	コンテンツカテゴリ び 止対象 なる禁止対象 禁止対象 D取組みによる禁止対象		~
適用するアドレス:	すべてのアドレス		~
適用するユーザー:	すべてのユーザー		~
処理:	ブロック		Ý
ルールのスケジュール:	常時	~	設定

【補足】ウェブコントロールによるブロック設定後のイベント抑止

ウェブコントロールによるブロックを設定後、管理下のデバイスでブロック対象のサイトを閲覧した場合や、バナーが ブロックされた場合、KSC にもブロックされた情報が通知されます。

ユーザーの利用状況により、このイベントが大量に記録され、他のイベントが埋もれてしまう可能性があります。

・イベント画面(例)
----------	----

Kaspersky Security Center 14						- 🗆 X
ファイル(F) 操作(A) 表示(V) ヘルプ(H)						
 Kaspersky Security Center 14 ・ ・ ・	管理サーバー KSC	(KSC\kaspersky)				
 □ モバイルチバイス管理 □ デバイスの抽出 □ 未割り当てデバイス 	監視 統計	レポート イベント			1	ナーバーのプロパティ
デブポリシー 直 タスク 国 カスベルスキーのライセンス	イベントの抽出 最	<u>近のイベント</u> ▼ ★		<u>ii</u>	主とイベントのエク	スポートの設定 🔻
> ■■ 詳細	抽出を実行 抽	出のプロパティ	抽出の作成 インポート/コ	エクスポート ▼		更新
	列の追加と削除			列を:	テキストで検索	Q
	日時	デバイス	イベント	1.128月	グループ	アプリケーシ ^
	0 2023年1月19日 16:1	11 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16:1	11 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
r	4 2023年1月19日 16:1	10 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	 管理対象デバイス 	Kaspersky
	16:1	10 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	4 2023年1月19日 16:1	10 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16::	10 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16:0	9 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	 管理対象デバイス 	Kaspersky
	0 2023年1月19日 16:0	5 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16:0	5 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	 管理対象デバイス 	Kaspersky
	0 2023年1月19日 16:0	4 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16:0	04 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16:0	04 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	 管理対象デバイス 	Kaspersky
	0 2023年1月19日 16:0	04 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	 管理対象デバイス 	Kaspersky
	0 2023年1月19日 16:0	04 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	4 2023年1月19日 16:0	04 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16:0	3 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	16:0	3 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	0 2023年1月19日 16:0	3 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky
	4 2023年1月19日 16:0	3 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	 管理対象デバイス 	Kaspersky
	16:0	3 DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別:アクセスが拒否されました アプリケー	管理対象デバイス	Kaspersky 🖌
					~ルプ ▼	kaspersky
Const March						
1/1/1:636						

以下に、「ウェブコントロール」によるブロックイベントを KSC へ通知しない設定についてご説明します。

 (1)「管理対象デバイス」を開き、右画面にて 「ポリシー」タブを開きます。
 KES のポリシーを右クリックし、「プロパティ」 を開きます。



(2)「イベントの設定」セクションを開きます。

「緊急タブ」にて以下のイベントをそれぞれ 選択し、「プロパティ」をクリックします。

<設定対象イベント>

 「アクセスが拒否されました(ローカル定 義データベース)」

・「アクセスが拒否されました(KSN)」



- (3)「管理サーバーのデータベースに保存」のチ ェックを外し、「OK」をクリックします。
- プロパティ:アクセスが拒否されました(ローカル定義データベース) X イベント登録 * 30 □管理サーバーのデータベースに保存(日)(s): Syslog 経由で SIEM システムにエクスポートする(Y) □ デバイスの OS イベントログに保存(D) □管理サーバーの OS イベントログに保存(A) イベント通知 - メールで通知(E) SMS で通知(S) □実行ファイルまたはスクリプトの実行で通知(R) SNMP 経由で通知(M) 既定では、管理サーバーの設定タブで設定された通知設定が使用されます(たとえば、受信者のアドレ スなど)。各設定を変更するには、「設定」をクリックします。 設定 OK キャンセル III プロパティ: Kaspersky Endpoint Security for Windows (11.11.0) × 保護レベル:高 すべての推奨される保護機能が有効です。 イベントの設定 全般 🕕 緊急 🕕 機能エラー 🔺 警告 🕕 情報 イベントの設定 ● 編集をロック ~ **(**)-先進の脅威対策 脅威対策 イベント種別 保管期間 危険なリンクを開きました 以前開いた危険なリンクを検知しました プロセスの処理がブロックされました 30 ⊟ 30 ⊟ 30 ⊟ Detection and Response セキュリティコントロール データ暗号化 キーボードが認証されませんでした 30 H イムボーバルを通じていたくいたい。 AMSIリクエストはブロックされました ネットワーク動作がプロックされました ネットワーク攻撃が検知されました アプリケーションの起動が禁止されました ローカルタスク 30日 30日 30日 全般設定 ポリシーのプロファイル 30日 記動前 変更履歴 アクセスが拒否されました (ローカル定義データベース)
 アクセスが拒否されました (KSN) <保存しない> <保存しない> テハイスを使用した採作がフロッ ネットワーク接続がブロックされました 30 H ネッドノーク/お店の/しつジーにはないこ
 コンボーネントのアップデートエラー
 コンボーネントのアップデートの配信エラー
 ローカルのアップデートエラー
 ネットワークアップデートエラー <保存しない> <保存しない> <保存しない> <保存しない> インドラークテクフ 2 つの久久を同時に開始できません アプリケーションの定義データベースおよびモジュールの検証中にエラ・ Kaspersky Security Center との対話中にエラーが発生しました 30 目 30 目 30日 アップデートされていないコンポーネントがあります 30日 アップテートされていないコンボーネントがあります アップデートは正常に完了しましたが、アップデートの配信に失敗しました 内部ウスセラー パッチをインストールできませんでした パッチをロールパックできませんでした <保存しない>
 <保存しない> 30日 30 H < > すべて選択**(**S) プロパティ(P) 112 ОК キャンセル 適用(A)
- (4) 設定したイベントの「保管期間」が「<保存 しない>」変更されたことを確認し、「OK」 をクリックしてポリシーを閉じます。

ポリシー適用後は管理サーバー上にイベン トが記録されないようになります。

本節は以上です。

ここでは、Windows において「ログオンイベントの監査」の有効化についてご説明します。

KES の保護コンポーネントの一つである「ふるまい検知」の機能として、「外部からの暗号化に対する共有フォルダーの保護」という機能があります。

この機能において、特定デバイスからの暗号化通信は除外する設定(除外リスト)がありますが、この機能を有効にするためには、Windows において「ログオンイベントの監査」を有効化する必要があります。

参考として、Active Directory グループポリシー、ローカルセキュリティポリシーそれぞれの設定箇所をご案内します。

• Active Directory グループポリシー

 「リレーブボリシー管理エディター ファイル(F) 操作(A) 表示(V) ヘルブ(H) ◆ ・ ・ ▲ ・		-
 □ Default Domain Policy [WIN-1MURPDVIDGN.SETEST.C × ▼ (● コンピューターの構成 ▼ (● コンピューターの構成 ▼ (● コンピューターの構成 ▼ (● マンパントログ > ● マンパント(スタートアップ/シャットダウン) > ● 名前解決ボリシー ※ スクリプト(スタートアップ/シャットダウン) > ● 使われたプリンター ▼ (● コンディングントボリシー ▼ (● コンディングントボリシー > ● コークル・ボリシー > ● ユーブー権利の割り当て > ● イントログ 	 ポリシー ^ ボウントログオンイベントの監査 アカウント管理の監査 オブジェクトアクセスの監査 ジススムイベントの監査 ディレクトリサービスのアクセスの監査 ディレクトリサービスのアクセスの監査 ボリシーの変更の監査 ログアクレイントの監査 ログアクレイントの監査 特権使用の監査 	ポリシー設定 未定定義 未定定義 未定定義 未定定義 未定定義 未定定義 未定定義 未定

ローカルセキュリティポリシー

 □ーカル セキュリティボリシー ファイル(F) 操作(A) 表示(V) ヘルブ(H) ◆ ◆ 2 前 ※ ◎ ▶ 2 前 		– 🗆 X
 ■ セキュリティの設定 ■ アカウントポリシー ■ ユーザー権利の割り当て > ■ ユーザー権利の割り当て > ■ ユーザー権利の割り当て > ■ セキュリティオブション ■ セキュリティオブション ■ セキュリティオブション ■ セキュリティオブション ● セキュリティオブション ● セキュリティの制限のポリシー ○ ソフトウェアの制限のポリシー ○ アブリケーション制御ポリシー > ● レキュリティポリシー(ローカルコンピュータ > ● 監査ポリシーの詳細な構成 	 ポリシー アカウントログオンイベントの監査 アカウント管理の監査 アカウント管理の監査 システムイベントの監査 ディレクトリサービスのアクセスの監査 プロセス追跡の監査 ポリシーの変更の監査 ログオンイベントの監査 ログオンイベントの監査 特権使用の監査 	セキュリティの設定 監査しない 監査しない

「ログオンイベントの監査」の詳細につきましては、以下マイクロソフト社のサイトをご参照ください。

https://learn.microsoft.com/ja-jp/windows/security/threat-protection/auditing/basic-au dit-logon-events

kaspersky **Appendix**

本章では、初期設定における補足事項についてご説明します。

1.「管理サーバークイックスタートウィザード」をキャンセルした場合

KSC のインストール完了後、自動的に「管理サーバークイックスタートウィザード」が起動し、KSC における初期設 定や必要なタスクの作成を行うことができます。

このウィザードをキャンセルした場合でも、再度ウィザードを起動することができます。



本節は以上です。



KSC の初期状態では、すべてのインターフェイスを表示する設定になっておりません。

アクセス権の設定を行う「セキュリティ」設定や、KSC をプライマリ・セカンダリと階層管理するための設定は初期状態で表示されておりません。

インターフェイスの設定を変更するためには以下の手順を実施します。

(1)「管理サーバー」を右クリックし、「表示」-「イ Kaspersky Security Center 14 ファイル(F) 操作(A) 表示(V) ヘルプ(H) ンターフェイスの設定」をクリックします。 🗢 🔿 🙍 📷 🗙 🛅 🛛 🖬 Kaspersky Security Center 14 答理++-パー KSC (KSC\kaspersky) □ 管理サーバー KSC 管理サーバーから切断(O) 管理対象
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 //
 ///
 //
 //
 //
 //
 //

 ・ 日 モバイルデバー
 ・

 ・ デバイスの抽
 アプリケーションのインストール(I) 1+ レポート イベント 检索(A) 東 未割り当てデ すべてのタスク(K) シ ポリシー 直 タスク (1) カスペルスキ) 11 詳細 表示(V) インターフェイスの設定(C) 削除(D) カスタマイズ(U)... の作成 プロパティ(R) ヘルプ(H) (2)「インターフェイスの設定」画面が表示されま ? × インターフェイスの設定 す。 表示する機能 ☑ 脆弱性とパッチ管理の表示(A) 必要な項目にチェックを入れ、「OK」をクリッ ☑データ暗号化と保護機能の表示(D) クします。 □エンドポイントコントロール設定の表示(D) マモバイルデバイス管理の表示(M) □ セカンダリ管理サーバーの表示(A) ✓セキュリティ設定タブの表示(S) キャンセル OK (3) 右記のダイアログが表示されるので、「OK」 Kaspersky Security Center 13.2 \times をクリックし、KSC管理コンソールを閉じ、再 変更を反映するには、管理コンソールを再起動してください。 度管理コンソールを開きます。 機能の表示を有効または無効にできます。専用のライセンスが必要な機能 ※OS やサービスの再起動は不要です。 の表示を有効にしたがライセンスがない場合、その機能に関連するインターフ エイス要素が管理コンソールに表示されますが、機能自体は使用できませ ho OK

(4)管理コンソール起動後、設定したインターフェイスが表示されていることを確認します。

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

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

©2023 Kaspersky Labs Japan. Kaspersky Anti-Virus および Kaspersky Security は、Kaspersky Lab ZAO 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 1 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。