クラウドサービス for サーバーセキュリティ

初期設定パラメータ

Ver 1.1

リコージャパン株式会社

はじめにお読みください

本資料は、Windows Server 2008 R2 (64 bit) のサーバに対して
Deep Security as a Service を新規インストールした状態での初期設定値を記載しています。

侵入防御ルール、変更監視ルール、ログ監視ルールの情報は2015年2月17日時点の情報となります。

また、本資料は、サービスご利用開始時に本商品にて初期設定を行う項目のみ記載しています。

コンポーネントのインストール状況や、ライセンス有無、インストール時の設定内容、
旧バージョンからのバージョンアップ、インストール先のプラットフォームにより、
設定に表示されない項目や初期設定値が異なる場合があります。

＜本資料のご利用方法 ＞

・ ご利用開始時に設定されている項目には、網掛けされています。

記載例：

◉ すべてのファイル
○ トレンドマイクロの推奨設定 -実際のファイルタイプで判断する

☑ IntelliTrapを有効にする
☐ トレンドラボにIntelliTrapサンプルを送信する

・ プルダウンリストから設定が選択できる場合は、下記のように表記されています。

アプリケーションログの詳細レベル:

標準 ▼
標準
詳細
診断
デバッグ

プルダウンリスト内で、黄色い網掛けが設定されている項目が初期設定です。
また、選択肢が多数存在する場合は、注釈にて選択可能な内容をご案内しています。

データベースのアップデート間隔: 01 ▼ 分 *1　　*1 … 01 から 60 まで設定可能です。

・ 設定項目が存在しない箇所は記載を割愛しています。
あらかじめご了承ください。

例：[ログ] - [クエリ] メニューなど

更新履歴

Ver	公開日	更新内容
1.0	2015/8/26	初版
1.1	2016/1/28	「RJ Policy(2K3_32bit)」、「管理(システム設定）」を追加

目次

・アラート …… 5
・ポリシー(RJ Policy) …… 37
・ポリシー (RJ Policy(2K3_32bit)) …… 70
・管理(システム設定) …… 103
・管理(予約タスク) …… 106

アラート

[アラート]

[アラート設定]

アラート	重要度	オン
Agent/Applianceのアップグレードが必要	警告	✓
Agent/Applianceのアップグレード推奨	警告	✓
Agent/Applianceのアップグレード推奨 (新しいバージョンが使用可能)	警告	✓
Agent/Applianceのアップグレード推奨 (非互換のセキュリティアップデート)	警告	✓
Agent/Applianceのディスク容量の不足	警告	✓
Agentのアップグレード推奨 (Applianceと非互換)	警告	✓
Agentの設定パッケージが大きすぎる	警告	✓
Agentインストールの失敗	重大	✓
Agentソフトウェアのアップグレード失敗	警告	✓
Deep Security Managerソフトウェアのアップグレード推奨 (非互換のセキュリティアップデート)	警告	✓
Filter Driverとの接続失敗	重大	✓
Filter Driverのアップグレード推奨 (新しいバージョンが使用可能)	警告	✓
Relayアップデートサービスを利用不可	重大	✓
Smart Protection Serverとの接続失敗	警告	✓
Virtual ApplianceとFilter Driverの互換性なし	警告	✓
VMware Toolsがインストールされていない	重大	✓
Webレピュテーションイベントアラート	警告	✓
まもなくライセンシーとの数の上限に達します	警告	✓
アカウントの残高がありません	重大	✓
アカウントの残高が少なくなっています	警告	✓
アプリケーションの種類の推奨設定	警告	
アプリケーションの種類の誤った設定	警告	✓
イベントの切り捨て	警告	✓
イベントの抑制	警告	
コンピュータがアップデートを受信していない	警告	✓
コンピュータの再起動が必要	警告	✓
セキュリティログ監視エンジンがオフライン	重大	✓
セキュリティログ監視ルールに設定が必要	警告	✓
セキュリティログ監視ルールの推奨	警告	
セキュリティログ監視ルールアラート	警告	✓
ソフトウェアパッケージが見つからない	重大	✓
ネットワークエンジンモードの非互換性	警告	✓
ファイアウォールエンジンがオフライン	重大	✓
ファイアウォールルールの推奨	警告	✓
ファイアウォールルールアラート	警告	✓
ファイルで不正プログラムを検索できませんでした	警告	✓
ポリシー送信の失敗	重大	✓

[アラート] (つづき)

アラート	重要度	オン
ユーザのロックアウト	警告	✓
ユーザパスワードがまもなく有効期限切れ	警告	✓
ライセンスの有効期限が間もなく終了します	警告	
ライセンス期限切れ	重大	✓
ライセンスシート数の上限に達しました	重大	✓
ルールのアップデートが利用可能	警告	✓
不正プログラムの予約検索がスキップされました	警告	✓
不正プログラムの遠隔ファイルがストレージ制限を超過	警告	✓
不正プログラム対策アラート	警告	✓
不正プログラム対策エンジンがオフライン	重大	✓
不正プログラム対策コンポーネントのアップデートの失敗	警告	✓
不正プログラム対策コンポーネントの障害	重大	✓
不正プログラム対策保護がないか、期限切れ	警告	✓
不正プログラム対策保護でコンピュータの再起動が必要	警告	✓
仮想マシンインタフェースの非同期	警告	✓
侵入防御エンジンがオフライン	重大	✓
侵入防御ルールの削除の推奨	警告	
侵入防御ルールの推奨	警告	
侵入防御ルールの設定が必要	警告	✓
侵入防御ルールアラート	警告	✓
保護されていないESXiサーバへの仮想マシンの移動	警告	✓
別のESXiへの移動後に仮想マシンが保護されていない	警告	✓
変更監視のTPMが無効	警告	
変更監視のTPMのレジスタ値の変更	警告	✓
変更監視エンジンがオフライン	重大	✓
変更監視ルールのコンパイルエラー	重大	✓
変更監視ルールの推奨	警告	
変更監視ルールの設定が必要	警告	✓
変更監視ルールアラート	警告	✓
推奨設定	警告	✓
攻撃の予兆の検出: OSのフィンガープリント調査	警告	✓
攻撃の予兆の検出: TCP Null検索	警告	✓
攻撃の予兆の検出: TCP SYNFIN検索	警告	✓
攻撃の予兆の検出: TCP Xmas検索	警告	✓
攻撃の予兆の検出: ネットワークまたはポートの検索	警告	✓
新しいバージョンのソフトウェアが利用可能	警告	✓
新しいパターンファイルアップデートがダウンロード済みで利用可能	警告	✓
新しいルールアップデートがダウンロード済みで利用可能	警告	✓
時計の変更の検出	警告	✓
有効化に失敗	重大	✓
異常な再起動の検出	警告	✓
空のRelayグループの割り当て	重大	✓
複数の有効化されたApplianceの検出	警告	✓
設定が必要	警告	✓
通信の問題の検出	警告	✓
通信不能	重大	✓
重複するコンピュータの検出	警告	✓

[アラート] (つづき)

アラート	重要度	オン
重複する一意のIDの検出	警告	✓
非互換のAgent/Applianceバージョン	警告	✓

[各アラートのプロパティ]

Agent/Applianceのアップグレードが必要

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Agent/Applianceのアップグレード推奨

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Agent/Applianceのアップグレード推奨 (新しいバージョンが使用可能)

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート] (つづき)

Agent/Applianceのアップグレード推奨 (非互換のセキュリティアップデート)

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Agent/Applianceのディスク容量の不足

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Agentのアップグレード推奨 (Applianceと非互換)

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

Agentの設定パッケージが大きすぎる

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Agentインストールの失敗

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Agentソフトウェアのアップグレード失敗

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

Deep Security Managerソフトウェアのアップグレード推奨 (非互換のセキュリティアップデート)

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Filter Driverとの接続失敗

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Filter Driverのアップグレード推奨 (新しいバージョンが使用可能)

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

Relayアップデートサービスを利用不可

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

まもなくライセンシーとの数の上限に達します

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

アカウントの残高がありません

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

アカウントの残高が少なくなっています

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Smart Protection Serverとの接続失敗

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Virtual ApplianceとFilter Driverの互換性なし

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

VMware Toolsがインストールされていない

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

Webレピュテーションイベントアラート

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

アプリケーションの種類の推奨設定

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

アプリケーションの種類の誤った設定

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

イベントの切り捨て

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

イベントの抑制

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

コンピュータがアップデートを受信していない

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

コンピュータの再起動が必要

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

セキュリティログ監視エンジンがオフライン

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

セキュリティログ監視ルールに設定が必要

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

セキュリティログ監視ルールの推奨

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

セキュリティログ監視ルールアラート

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☐ (ルール設定に関係なく) すべてのルールでアラート

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

ソフトウェアパッケージが見つからない

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

ネットワークエンジンモードの非互換性

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ファイアウォールエンジンがオフライン

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

ファイアウォールルールの推奨

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ファイアウォールルールアラート

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☐ (ルール設定に関係なく) すべてのルールでアラート

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ファイルで不正プログラムを検索できませんでした

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ポリシー送信の失敗

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ユーザのロックアウト

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

ユーザパスワードがまもなく有効期限切れ

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ライセンスの有効期限が間もなく終了します

◯ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ライセンスの期限切れ

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

- 重大
- 警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ライセンスシート数の上限に達しました

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ルールのアップデートが利用可能

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

不正プログラムの予約検索がスキップされました

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

不正プログラム対策の隔離ファイルがストレージ制限を超過

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

不正プログラム対策アラート

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☐ (ルール設定に関係なく) すべてのルールでアラート

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

不正プログラム対策エンジンがオフライン

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

不正プログラム対策コンポーネントのアップデートの失敗

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

不正プログラム対策コンポーネントの障害

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

不正プログラム対策保護がないか、期限切れ

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

不正プログラム対策保護でコンピュータの再起動が必要

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

仮想マシンインタフェースの非同期

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

侵入防御エンジンがオフライン

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

侵入防御ルールの削除の推奨

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

侵入防御ルールの推奨

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

侵入防御ルールの設定が必要

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

侵入防御ルールアラート

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☐ (ルール設定に関係なく) すべてのルールでアラート

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

保護されていないESXiサーバへの仮想マシンの移動

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

保護モジュールライセンスがまもなく期限切れ

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

保護モジュールライセンスが期限切れ

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

別のESXiへの移動後に仮想マシンが保護されていない

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

変更監視のTPMが無効

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

変更監視のTPMのレジスタ値の変更

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

変更監視エンジンがオフライン

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

変更監視ルールのコンパイルエラー

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

変更監視ルールの推奨

○ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◉ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

変更監視ルールの設定が必要

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

変更監視ルールアラート

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☐ (ルール設定に関係なく) すべてのルールでアラート

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

変更監視情報の収集の遅延

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

推奨設定

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

攻撃の予兆の検出: OSのフィンガープリント調査

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

攻撃の予兆の検出: TCP Null検索

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

攻撃の予兆の検出: TCP SYNFIN検索

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

攻撃の予兆の検出: TCP Xmas検索

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

攻撃の予兆の検出: ネットワークまたはポートの検索

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

新しいバージョンのDeep Security Managerが利用可能

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

新しいパターンファイルアップデートがダウンロード済みで利用可能

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

新しいルールアップデートがダウンロード済みで利用可能

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

時計の変更の検出

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

有効化に失敗

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

異常な再起動の検出

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

空のRelayグループの割り当て

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

複数の有効化されたApplianceの検出

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

設定が必要

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

通信の問題の検出

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

通信不能

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 重大 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

○ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

[アラート]つづき

重複するコンピュータの検出

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

重複する一意のIDの検出

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

非互換のAgent/Applianceバージョン

◉ オン

オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度： 警告 ▼

重大

警告

☑ このアラートの発令時、通知のメールを送信する

☑ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☑ このアラートが存在しなくなったとき、通知のメールを送信する

◯ オフ

オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

ポリシー (RJ Policy)

[ポリシー]

[ポリシー] > [RJ Policy:詳細] > [概要] > [一般]タブ

一般 | このポリシーを使用しているコンピュー | イベント

一般

名前 : RJ Policy

説明:

継承

親ポリシー: なし

モジュール

不正プログラム対策:	オン	リアル: *1
Webレピュテーション:	オン	オン
ファイアウォール:	初期設定 (オフ)	オフ, ルールなし
侵入防御:	オン	防御or検出,ルールなし
変更監視:	初期設定 (オフ)	オフ, ルールなし
セキュリティログ監視:	オン	オン,2ルール

*1 ... モジュールの選択肢は下記4項とも共通です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [一般]タブ

一般 | Smart Protection | 詳細 | 隔離ファイル | イベント

不正プログラム対策

不正プログラム対策のステータス: オン ▼ オフ

リアルタイム検索

☐ 初期設定

不正プログラム検索設定: Default Real-Time Scan Configuration ▼ 編集

スケジュール: Every Day All Day ▼ 編集

手動検索

☐ 初期設定

不正プログラム検索設定: Default Manual Scan Configuration ▼ 編集

予約検索

☐ 初期設定

不正プログラム検索設定: Default Scheduled Scan Configuration ▼ 編集

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [Smart Protection]タブ

一般 | **Smart Protection** | 詳細 | 隔離ファイル | イベント

スマートスキャン

- [x] 初期設定
- (●) Deep Security Agentはオン、Virtual Applianceはオフ
- ( ) オン
- ( ) オフ

ファイルレピュテーションサービス用のSmart Protection Server

- [x] 初期設定
- (●) Global Smart Protectionサービスへの直接接続
  - [ ] Global Smart Protectionサービスへのアクセス時にプロキシを使用 なし ▼ 編集
    - なし
    - 新規...

※プロキシサーバ有りの場合、プロキシサーバの設定が入ります。

- ( ) ローカルにインストールされたSmart Protection Serverの使用

追加
削除

- [ ] ドメインに参加していない場合はGlobal Smart Protectionサービスに接続 (Windowsのみ)

Smart Protection Serverへの接続の警告

Smart Protection Serverへの接続が切断された場合に警告: 初期設定 (はい) ▼

- 初期設定 (はい)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [詳細]タブ

一般 | Smart Protection | **詳細** | 隔離ファイル | イベント

隔離ファイル

- [x] 初期設定

隔離ファイルの保存に使用される最大ディスク容量: 1024 MB

検索の制限

- [x] 初期設定

検索するファイルの最大サイズ: 0 MB

不正プログラム検索用のリソース割り当て

不正プログラム検索でマルチスレッド処理を使用 (利用可能な場合): 初期設定 (いいえ) ▼

- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [詳細]タブ(つづき)

許可するスパイウェア/グレーウェア

追加
削除

ローカルイベント通知

不正プログラムの検出時にローカル通知を表示: 初期設定 (はい)

- 初期設定 (はい)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [一般]タブ

一般 | 除外 | SmartProtection | 詳細 | イベント

Webレピュテーション

Webレピュテーションのステータス: オン

セキュリティレベル

☑ 初期設定

○ 高　ブロック対象のページ:
危険: 不正、または脅威の既知の発信源であると確認されたページ
非常に不審: 不正または脅威の発信源である可能性が疑われたページ
不審: スパムメールに関連付けられている、または感染している可能性のあるページ

◉ 中　ブロック対象のページ:
危険: 不正、または脅威の既知の発信源であると確認されたページ
非常に不審: 不正または脅威の発信源である可能性が疑われたページ

○ 低　ブロック対象のページ:
危険: 不正、または脅威の既知の発信源であると確認されたページ

☐ トレンドマイクロでテストしていないページをブロック

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [除外]タブ

一般 | 除外 | SmartProtection | 詳細 | イベント

許可

許可リストに追加するURL (1行に1つずつ):

追加»

削除… | エクスポート…

許可するURL	範囲

◉ ドメイン内すべてのURLを許可する
○ URLを許可する

ブロック

ブロックリストに追加するURL (1行に1つずつ):

追加»

削除… | エクスポート…

ブロックするURL	範囲

◉ ドメイン内すべてのURLをブロックする
○ URLをブロックする
○ このキーワードを含むURLをブロックする

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [Smart Protection]タブ

一般 | 除外 | Smart Protection | 詳細 | イベント

Webレピュテーションサービス用のSmart Protection Server

☑ 初期設定
◉ Global Smart Protectionサービスへの直接接続
☐ Global Smart Protectionサービスへのアクセス時にプロキシを使用 なし ▼ 編集
なし
新規…
○ ローカルにインストールされたSmart Protection Serverの使用
追加
削除
☐ ドメインに参加していない場合はGlobal Smart Protectionサービスに接続 (Windowsのみ)

Smart Protection Serverへの接続の警告

Smart Protection Serverへの接続が切断された場合に警告: 初期設定 (はい) ▼
初期設定 (はい)
はい
いいえ

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [詳細]タブ

一般 | 除外 | Smart Protection | **詳細** | イベント

ブロックページ

☑ 初期設定

ブロックされているページの再評価をユーザが依頼できるようにするため、
ブロックページに表示するリンクを指定します。

リンク: http://sitesafety.trendmicro.com

例: http://intranet.supportdesk.example.com/またはmailto:administrator@example.com

アラート

アラート: 初期設定 (いいえ) ▼

- 初期設定 (いいえ)
- はい
- いいえ

ポート

有害な可能性のあるWebページを監視するポート: 初期設定 (80,8080) ▼

- 初期設定 (80,8080)
- (ポートリスト一覧) *1

*1 ...[ポートリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーションテーション] > [詳細]タブ（つづき）

ローカルイベント通知

不正なWebサイトへのアクセスのブロック時にローカル通知を表示: 初期設定 (はい)

- 初期設定 (はい)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [一般]タブ

一般 | インターフェイス制限 | 攻撃の予兆 | 詳細 | イベント

ファイアウォール

ファイアウォールステータス: 初期設定(オフ)

- 初期設定(オフ)
- オン
- オフ

ファイアウォールステートフル設定

グローバル (すべてのインタフェース) Enable Stateful Inspection 編集

- 継承 (なし)
- 新規...
- Enable Stateful Inspection
- Deep Security Manager Stateful
- Web Server Stateful
- FTP Server Stateful
- No Stateful Inspection

割り当てられたファイアウォールルール

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [インタフェース制限]タブ

一般 | **インターフェイス制限** | 攻撃の予兆 | 詳細 | イベント

インタフェース制限

◉ 初期設定を使用:
インタフェース制限の有効化: いいえ

○ インタフェース制限の有効化

○ インタフェース制限の無効化

インタフェースパターン備考 *1

優先度	
高 ↑	^ローカル エリア接続.*
	^ワイヤレス ネットワーク接続.*
優先度 低	

追加
削除
アップ
ダウン

☐ 1つのアクティブインタフェースに制限

*1 …「インタフェース制限」で、「インタフェース制限の有効化」を選択の場合に変更可能です。

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [攻撃の予兆]タブ

一般 | インターフェイス制限 | **攻撃の予兆** | 詳細 | イベント

攻撃の予兆検索

攻撃の予兆の検出の有効化: 初期設定(はい) ▼
- 初期設定(はい)
- はい
- いいえ

☑ OSのフィンガープリント調査 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼ *1
- いいえ
- 1 分
- 2 分
- 5 分
- 10 分
- 15 分
- 30 分

☑ ネットワークまたはポートの検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼

☑ TCP Null検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼

☑ TCP SYNFIN検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼

☑ TCP Xmas検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼

検出を実行するコンピュータ/ネットワーク: 初期設定 (すべて) ▼
- 初期設定 (すべて)
- すべて
- (IPリスト一覧) *2

検出を実行しないIPリスト: IPリスト: Ignore Reconnaissance ▼
- 初期設定 (なし)
- なし
- IPリスト: Ignore Reconnaissance *2
- (IPリスト一覧)

*1 … [トラフィックのブロック:]は、[攻撃の予兆の検出の有効化]で「はい」を選択すると変更できます。選択肢は下記4項とも共通です。

*2 …[IPリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [詳細]タブ

一般 | インターフェイス制限 | 攻撃の予兆 | **詳細** | イベント

イベント

「ポリシーの許可外」のパケットのファイアウォールイベントを生成: 初期設定 (はい) ▼

- 初期設定 (はい)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [侵入防御] > [一般]タブ

一般 | 詳細 | イベント

侵入防御

侵入防御のステータス: オン ▼

- 初期設定 (オフ)
- オン
- オフ

侵入防御の動作 *1

◉ 防御　※申込み詳細シートに従い「防御」「検出」のどちらか選択されます

◯ 検出

現在割り当てられている侵入防御ルール

推奨設定

現在のステータス: 0個の侵入防御ルールが割り当てられています

侵入防御の推奨設定を自動的に適用 (可能な場合): はい ▼

- 初期設定 (いいえ)
- はい
- いいえ

*1 …「設定」で、「オン」を選択の場合に変更可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [侵入防御] > [詳細]タブ

一般 | **詳細** | イベント

イベントデータ

各ルールの最初の検出に関するデータの取り込みを侵入防御ルールに許可する (期間内): 初期設定 (はい) ▼
- 初期設定 (はい)
- はい
- いいえ

ルールアップデート

アップデートされたアプリケーションの種類および侵入防御ルールの依存関係に応じて、新しい侵入防御ルールを自動的に割り当て: 初期設定 (はい) ▼
- 初期設定 (はい)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [変更監視] > [一般]タブ

一般 | 詳細 | イベント

変更監視

変更監視のステータス: 初期設定 (オフ) ▼
- 初期設定 (オフ)
- オン
- オフ

リアルタイム検索の有効化

☐ リアルタイム

現在割り当てられている変更監視ルール

推奨設定

現在のステータス: 0個の変更監視ルールが割り当てられています

変更監視ルールの推奨設定を自動的に適用 (可能な場合): 初期設定(いいえ) ▼
- 初期設定(いいえ)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [変更監視] > [詳細]タブ

一般 | **詳細** | イベント

コンテンツハッシュアルゴリズム

- [x] 初期設定
  - [x] SHA-1
  - [ ] SHA-256

仮想マシンの検索キャッシュ

変更の検索キャッシュの設定: Default Integrity Monitoring Scan Cache Configuration

- 初期設定 (なし)
- 新規...
- なし
- Default Integrity Monitoring Scan Cache Configuration
- (不正プログラム検索設定一覧) *1

CPU使用率

変更監視のCPU使用率レベル: 初期設定(高)

- 初期設定(高)
- 高
- 中
- 低

*1 ...[不正プログラム検索設定]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [セキュリティログ監視] > [一般]タブ

一般 | 詳細 | イベント

セキュリティログ監視

セキュリティログ監視のステータス: オン

- 初期設定 (オフ)
- オン
- オフ

現在割り当てられているセキュリティログ監視ルール

1002792-Default Rules Configuration
1002795-Microsoft Windows Events

推奨設定

現在のステータス: 0個のセキュリティログ監視ルールが割り当てられています

セキュリティログ監視ルールの推奨設定を自動的に適用 (可能な場合): 初期設定 (いいえ)

- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [セキュリティログ監視] > [詳細]タブ

一般 | **詳細** | イベント

重要度のクリッピング

Agent/Applianceイベントが次の重要度以上の場合に、イベントをSyslogに送信:	初期設定 (中 (6)) ▼	*1
Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDSMに送信	初期設定 (中 (6)) ▼	*1

*1 ...初期設定 (中 (6)) ,低 (0) ,低 (1) ,低 (2) ,低 (3) ,中 (4) ,中 (5) ,中 (6) ,中 (7) ,
高 (8) ,高 (9) ,高 (10) ,高 (11) ,重大 (12) ,重大 (13) ,重大 (14) ,重大 (15)より設定可能です。

[ポリシー] > [RJ Policy:詳細] > [インタフェースの種類]

ネットワークインタフェースの種類

◉ ルールをすべてのネットワークインタフェースに適用

○ ルールを特定のインタフェースに適用

[ポリシー] > [RJ Policy:詳細] > [設定] > [コンピュータ]タブ

コンピュータ | ネットワークエンジン | 検索 | SIEM

通信方向

Deep Security ManagerとAgent/Applianceの通信方向: 初期設定 (双方向) ▼

- 初期設定 (双方向)
- Agent/Applianceから開始
- Managerから開始
- 双方向

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [コンピュータ]タブ（つづき）

ハートビート

ハートビート間隔 (分):

初期設定 (10 分) ▼
- 初期設定 (10 分)
- 1 分
- 2 分
- 5 分
- 10 分
- 20 分
- 30 分
- 60 分
- 2 時間
- 4 時間
- 8 時間
- 12 時間
- 24 時間

次の数を超えるハートビートが失われた場合にアラートを発令:

初期設定 (2) ▼
- 初期設定 (2)
- 無制限
- 1
- 2
- 5
- 10
- 20
- 30
- 60

ハートビート間でコンピュータのローカルシステム時間が次の時間を超えて変更された場合にアラートを発令:

初期設定 (無制限) ▼
- 初期設定 (無制限)
- 無制限
- 5 分
- 10 分
- 20 分
- 30 分
- 60 分

非アクティブな仮想マシンに対してオフラインエラーを発令:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [コンピュータ]タブ（つづき）

ポリシーの変更をすぐに送信

ポリシーの変更をコンピュータに自動的に送信:

初期設定 (はい) ▼
- 初期設定 (はい)
- はい
- いいえ

トラブルシューティング

ログレベル:

初期設定 (オーバーライドしない) ▼
- 初期設定 (オーバーライドしない)
- オーバーライドしない
- 完全なファイアウォールイベントのログ記録
- 完全な侵入防御イベントのログ記録
- 完全なログ記録

Agentセルフプロテクション

ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否:

はい ▼
- 初期設定 (いいえ)
- はい
- いいえ

ローカルでの変更許可にパスワードを要求:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

パスワード:

パスワードの確認入力:

環境変数のオーバーライド:

環境変数の表示

※ 上記[環境変数の表示]クリックすると、[環境変数のオーバーライド]が表示されます。
[新規]

環境変数のプロパティ

名前:

値 :

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ

コンピュータ | **ネットワークエンジン** | 検索 | SIEM

ネットワークエンジンモード

ネットワークエンジンモード: 初期設定 (インライン) ▼
- 初期設定 (インライン)
- インライン
- タップ

イベント

イベントログファイルの最大サイズ (Agent/Appliance): 初期設定 (4 MB) ▼
- 初期設定 (4 MB)
- 512 KB
- 1 MB
- 2 MB
- 3 MB
- 4 MB
- 5 MB
- 10 MB

保管するイベントログファイル数 (Agent/Appliance): 初期設定 (3) ▼
- 初期設定 (3)
- 1
- 2
- 3
- 5
- 10
- 15
- 20
- 25

次の送信元IPのイベントは記録しない: 初期設定 (なし) ▼
- 初期設定 (なし)
- (IPリスト一覧) *1

*1 ...[IPリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

イベント

キャッシュサイズ:

初期設定 (128)
- 初期設定 (128)
- 0
- 1
- 2
- 4
- 8
- 16
- 32
- 64
- 128
- 256
- 512
- 1024

キャッシュの寿命:

初期設定 (30 分)
- 初期設定 (30 分)
- 1 分
- 15 分
- 30 分
- 45 分
- 60 分

キャッシュの有効期間:

初期設定 (15 分)
- 初期設定 (15 分)
- 1 分
- 15 分
- 30 分
- 45 分
- 60 分

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

コンピュータ | **ネットワークエンジン** | 検索 | SIEM

ネットワークエンジンの詳細設定

Agentの設定パッケージが最大サイズを超えた場合にアラートを生成する: 初期設定 (はい)
- 初期設定 (はい)
- はい
- いいえ

☑ 初期設定

CLOSEDタイムアウト: 初期設定 (0 秒) *1
- 初期設定 (0 秒)

SYN_SENTタイムアウト: 初期設定 (20 秒) *1
- 初期設定 (20 秒)

SYN_RCVDタイムアウト: 初期設定 (60 秒) *1
- 初期設定 (60 秒)

FIN_WAIT1タイムアウト: 初期設定(2 分) *1
- 初期設定 (2 分)

ESTABLISHEDタイムアウト: 初期設定 (3 時間)
- 初期設定 (3 時間)
- 1 時間
- 2 時間
- 3 時間
- 4 時間
- 12 時間
- 24 時間
- 2 日

ERRORタイムアウト: 初期設定 (10 秒) *1
- 初期設定 (10 秒)

DISCONNECTタイムアウト: 初期設定 (60 秒) *1
- 初期設定 (60 秒)

CLOSE_WAITタイムアウト: 初期設定 (2 分) *1
- 初期設定 (2 分)

*1 … 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

CLOSINGタイムアウト:	初期設定(1 秒) 初期設定 (1 秒) *1
LAST_ACKタイムアウト:	初期設定 (30 秒) 初期設定 (30 秒) *1
ACKストームタイムアウト:	初期設定 (1 秒) 継承 (1 秒) *1
ブートスタートタイムアウト:	初期設定 (20 秒) 初期設定 (20 秒) *1
コールドスタートタイムアウト:	初期設定 (5 分) 初期設定 (5 分) *1
UDPタイムアウト:	初期設定 (10 秒) 初期設定 (10 秒) *1
ICMPタイムアウト:	初期設定 (60 秒) 初期設定 (60 秒) *1
Null IPを許可:	初期設定 (はい) 初期設定 (はい) はい いいえ
バージョン8以前のAgentとApplianceでIPv6をブロック:	初期設定 (はい) 初期設定 (はい) はい いいえ
バージョン9以降のAgentとApplianceでIPv6をブロック:	初期設定 (いいえ) 初期設定 (いいえ) はい いいえ

*1 ... 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

接続クリーンナップタイムアウト:	初期設定 (10 秒) 初期設定 (10 秒) *1
最大接続数 (クリーンナップ単位):	初期設定 (1000) 初期設定 (1000) *2
送信元と送信先が同じIPアドレスをブロック:	初期設定 (はい) 初期設定 (はい) はい いいえ
最大TCP接続数:	初期設定 (1000) 初期設定 (1000) *2
最大UDP接続数:	初期設定 (1000) 初期設定 (1000) *2
最大ICMP接続数:	初期設定 (10000) 初期設定 (10000) *2
最大イベント数 (秒単位):	初期設定 (100) 初期設定 (100) 100 200 300 400 500

*1 ... 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

*2 ... 100, 500, 1000, 2000, 3000, 4000, 5000, 6000, 7000, , 8000, 9000, 10000, 20000, 30000, 40000, 50000, 60000, 70000, 80000, 90000, 100000, 200000, 300000, 400000, 500000, 600000, 700000, 800000, 900000, 1000000 ,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

TCP MSSの制限:

初期設定 (無制限) ▼

- 初期設定 (無制限)
- 536 バイト
- 600 バイト
- 700 バイト
- 800 バイト
- 900 バイト
- 1000 バイト
- 1100 バイト
- 1200 バイト
- 1276 バイト
- 1300 バイト
- 1360 バイト
- 1400 バイト
- 1440 バイト
- 1452 バイト
- 1460 バイト
- 無制限

イベントノードの数:

初期設定 (20000) ▼

- 初期設定 (20000)
- 1000
- 5000
- 10000
- 15000
- 20000
- 25000
- 30000
- 40000
- 50000
- 75000
- 100000
- 150000
- 200000
- 250000

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

ステータスコードの無視: 初期設定 (なし) ▼ 初期設定 (なし) *1

ステータスコードの無視: 初期設定 (なし) ▼ 初期設定 (なし) *1

ステータスコードの無視: 初期設定 (なし) ▼ 初期設定 (なし) *1

*1 ... 下記イベントステータスの選択肢より設定可能です。

継承 (なし)	不正なデータオフセット
なし	IPヘッダなし
セッション情報なし	読み取り不能なイーサネットヘッダ
不正なフラグ	未定義
不正なシーケンス	送信元および送信先IPが同一
不正なACK	不正なTCPヘッダ長
内部エラー	読み取り不能なプロトコルヘッダ
CEフラグ	読み取り不能なIPv4ヘッダ
不正なIP	不明なIPバージョン
不正なIPデータグラム長	不正なアダプタ設定
フラグメント化	重複しているフラグメント
不正なフラグメントオフセット	ACK再送の上限
最初のフラグメントが最小サイズ未満	切断された接続上のパケット
範囲外のフラグメント	再送の破棄
最小オフセット値以下のフラグメント	未定義
IPv6パケット	ポリシーで未許可 (オープンポート)
受信接続の上限	新しい接続の開始
送信接続の上限	無効なチェックサム
SYN送信の上限	無効なフック
ライセンスの期限切れ	IPペイロードがゼロ
不明なIPバージョン	IPv6ソースがマルチキャスト
不正なパケット情報	無効なIPv6アドレス
内部エンジンエラー	最小サイズ以下のIPv6のフラグメント
許可されていないUDP応答	無効なトランスポートヘッダ長
許可されていないICMP応答	メモリ不足
ポリシーで未許可	最大TCP接続数
不正なポートコマンド	最大UDP接続数
SYN Cookieエラー	

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

詳細なログ記録ポリシー:

初期設定 (初期設定)
- 初期設定 (初期設定)
- バイパス
- 初期設定
- 標準
- 下位互換性モード
- 詳細モード
- ステートフルおよび正規化の抑制
- ステートフル、正規化、およびフラグメントの抑制
- ステートフル、フラグメント、および検証機能の抑制
- タップモード

サイレントTCP接続拒否:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

デバッグモードを有効にする:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

デバッグモードで保持するパケットの数:

初期設定 (8)
- 初期設定 (8)
- 8
- 16
- 24
- 32
- 40
- 48
- 56
- 64

すべてのパケットデータをログに記録する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

期間内で1つのパケットデータのみをログに記録する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

1つのパケットデータのみをログに記録する期間:

初期設定 (5 分)
- 初期設定 (5 分)
- 0 秒
- 10 秒
- 30 秒
- 60 秒
- 2 分
- 3 分
- 4 分
- 5 分
- 10 分
- 20 分
- 40 分
- 50 分
- 100 分

パケットデータがキャプチャされたときに格納する最大データサイズ:

初期設定 (1500 バイト)
- 初期設定 (1500 バイト)
- 0 バイト
- 16 バイト
- 32 バイト
- 64 バイト
- 68 バイト
- 128 バイト
- 512 バイト
- 1024 バイト
- 1500 バイト
- 2048 バイト
- 4096 バイト

TCPの接続イベントを生成する:

初期設定 (いいえ)
- 初期設定(いいえ)
- はい
- いいえ

ICMPの接続イベントを生成する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

UDPの接続イベントを生成する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

Cisco WAAS接続のバイパス:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

回避再送の破棄:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

TCPチェックサムの確認:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

最小フラグメントオフセット:

初期設定 (60) ▼
- 初期設定 (60)
- 0
- 30
- 60
- 90
- 120

最小フラグメントサイズ:

初期設定 (120) ▼
- 初期設定 (120)
- 0
- 60
- 120
- 180
- 240

SSLセッションのサイズ:

初期設定 (低 - 2500) ▼
- 初期設定 (低 - 2500)
- 低 - 2500
- 中 - 5000
- 高 - 10000

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

SSLセッションの時間:

初期設定 (24 時間)
- 初期設定 (24 時間)
- 60 分
- 2 時間
- 4 時間
- 8 時間
- 12 時間
- 16 時間
- 20 時間
- 24 時間

IPv4トンネルのフィルタ:

初期設定 (IPv4トンネルの検出の無効化)
- 初期設定 (IPv4トンネルの検出の無効化)
- IPv4トンネルの検出の無効化
- トンネルパケットの解読
- トンネルパケットのドロップ (イベントによる)

IPv6トンネルのフィルタ:

初期設定 (IPv6トンネルの検出の無効化)
- 初期設定 (IPv6トンネルの検出の無効化)
- IPv6トンネルの検出の無効化
- トンネルパケットの解読
- トンネルパケットのドロップ (イベントによる)

厳密なTeredoのポート確認:

初期設定 (はい)
- 初期設定 (はい)
- はい
- いいえ

Teredoの異常のドロップ:

初期設定 (はい)
- 初期設定 (はい)
- はい
- いいえ

最大トンネル深度:

初期設定 (1)
- 初期設定 (1)
- 1
- 2
- 3
- 4

最大トンネル深度超過時の処理:

初期設定 (ドロップ)
- 初期設定 (ドロップ)
- ドロップ
- バイパス

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

IPv6拡張タイプ0のドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
最小MTU未満のIPv6フラグメントのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
IPv6予約済みアドレスのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
IPv6サイトローカルアドレスのドロップ:	初期設定 (いいえ) 初期設定 (いいえ) はい いいえ
IPv6 Bogonアドレスのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
6to4 Bogonアドレスのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
ゼロペイロードのIPパケットのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
不明なSSLプロトコルを破棄:	初期設定 (はい) 初期設定 (はい) はい いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

フラグメントタイムアウト:

初期設定 (60 秒) ▼

初期設定 (60 秒)

*1

保持するフラグメント化されたIPパケットの最大数:

初期設定 (1000) ▼

初期設定 (1000)
10
50
100
200
500
1000
5000
10000

フラグメント化されたパケットのタイムアウトを超過したことを示すためにICMPを送信する:

初期設定 (はい) ▼

初期設定 (はい)
はい
いいえ

*1 ... 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [検索]タブ

コンピュータ | ネットワークエンジン | **検索** | SIEM

開いているポート

検索するポート: 初期設定 (1-1024) ▼ 編集

- 初期設定 (1-1024)
- 1-1024
- (ポートリスト一覧) *1

推奨設定

推奨設定の継続的な検索を実行: 初期設定 (いいえ) ▼

- 初期設定 (いいえ)
- はい
- いいえ

継続検索の間隔: 初期設定 (7 日) ▼

- 初期設定 (7 日)
- 5 分
- 10 分
- 20 分
- 30 分
- 60 分
- 2 時間
- 3 時間
- 6 時間
- 12 時間
- 24 時間
- 2 日
- 3 日
- 7 日
- 2 週
- 3 週
- 4 週

*1 ...[ポートリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [検索]タブ(つづき)

Virtual Appliance

Virtual Appliance同時検索の最大数:

初期設定 (1) ▼
- 初期設定 (1)
- 1
- 5
- 10
- 15

不正プログラムの手動検索キャッシュの最大エントリ数:

初期設定 (500000) ▼
- 初期設定 (500000)
- 100000
- 250000
- 500000
- 750000
- 1000000
- 2500000
- 5000000
- 7500000
- 10000000

不正プログラムのリアルタイム検索キャッシュの最大エントリ数:

初期設定 (500000) ▼
- 初期設定 (500000)
- 100000
- 250000
- 500000
- 750000
- 1000000
- 2500000
- 5000000
- 7500000
- 10000000

変更監視の検索キャッシュの最大エントリ数:

初期設定 (500000) ▼
- 初期設定 (500000)
- 100000
- 250000
- 500000
- 750000
- 1000000
- 2500000
- 5000000
- 7500000
- 10000000

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [SIEM]タブ

コンピュータ | ネットワークエンジン | 検索 | **SIEM**

イベント転送の頻度 (Agent/Applianceから)

イベントの送信間隔: 初期設定 (60 秒) ▼
初期設定 (60 秒)
*1

不正プログラム対策イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:
リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼
ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼
Common Event Format

◯ イベントを転送しない

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [SIEM]タブ（つづき）

Webレピュテーションイベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

○ イベントの転送先:

○ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

○ イベントを転送しない

ファイアウォールと侵入防御イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

○ イベントの転送先:

○ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

○ イベントを転送しない

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [SIEM]タブ（つづき）

変更監視イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

◯ イベントを転送しない

セキュリティログ監視イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

◯ イベントを転送しない

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [オーバーライド]

オーバーライド		
不正プログラム対策		
不正プログラム対策設定	2個のオーバーライド	削除
割り当てられた不正プログラム検索設定	3個のオーバーライド	削除
Webレピュテーション		
Webレピュテーションの設定	継承	削除
ファイアウォール		
ファイアウォールの設定	1個のオーバーライド	削除
オーバーライドされたファイアウォールルール	継承	削除
割り当てられたファイアウォールステートフル設定	1個のオーバーライド	削除
侵入防御		
侵入防御の設定	継承	削除
オーバーライドされた侵入防御ルール	継承	削除
オーバーライドされたアプリケーションの種類	継承	削除
変更監視		
変更監視の設定	1個のオーバーライド	削除
オーバーライドされた変更監視ルール	継承	削除
セキュリティログ監視		
セキュリティログ監視の設定	継承	削除
オーバーライドされたセキュリティログ監視ルール	継承	削除
システム		
オーバーライドされたコンピュータ設定	1個のオーバーライド	削除

ポリシー (RJ Policy(2K3_32bit))

[ポリシー]

[ポリシー] > [RJ Policy:詳細] > [概要] > [一般]タブ

一般 | このポリシーを使用しているコンピュー | イベント

一般

名前 : RJ Policy(2K3_32bit)

説明:

継承

親ポリシー: なし

モジュール

不正プログラム対策:	オン	リアル *1
Webレピュテーション:	オン	オン
ファイアウォール:	初期設定 (オフ)	オフ, ルールなし
侵入防御:	オン	防御or検出,1つのルール
変更監視:	初期設定 (オフ)	オフ, ルールなし
セキュリティログ監視:	オン	オン,2ルール

*1 ... モジュールの選択肢は下記4項とも共通です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [一般]タブ

一般 | Smart Protection | 詳細 | 隔離ファイル | イベント

不正プログラム対策

不正プログラム対策のステータス: オン ▼ オフ

リアルタイム検索

☐ 初期設定

不正プログラム検索設定: Default Real-Time Scan Configuration ▼ 編集

スケジュール: Every Day All Day ▼ 編集

手動検索

☐ 初期設定

不正プログラム検索設定: Default Manual Scan Configuration ▼ 編集

予約検索

☐ 初期設定

不正プログラム検索設定: Default Scheduled Scan Configuration ▼ 編集

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [Smart Protection]タブ

一般 | **Smart Protection** | 詳細 | 隔離ファイル | イベント

スマートスキャン

- [x] 初期設定
- (●) Deep Security Agentはオン、Virtual Applianceはオフ
- ( ) オン
- ( ) オフ

ファイルレピュテーションサービス用のSmart Protection Server

- [x] 初期設定
- (●) Global Smart Protectionサービスへの直接接続
  - [ ] Global Smart Protectionサービスへのアクセス時にプロキシを使用 なし ▼ 編集
    - なし
    - 新規...
- ( ) ローカルにインストールされたSmart Protection Serverの使用
  - 追加
  - 削除
  - [ ] ドメインに参加していない場合はGlobal Smart Protectionサービスに接続 (Windowsのみ)

Smart Protection Serverへの接続の警告

Smart Protection Serverへの接続が切断された場合に警告: 初期設定 (はい) ▼

- 初期設定 (はい)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [詳細]タブ

一般 | Smart Protection | **詳細** | 隔離ファイル | イベント

隔離ファイル

- [x] 初期設定

隔離ファイルの保存に使用される最大ディスク容量: 1024 MB

検索の制限

- [x] 初期設定

検索するファイルの最大サイズ: 0 MB

不正プログラム検索用のリソース割り当て

不正プログラム検索でマルチスレッド処理を使用 (利用可能な場合): 初期設定 (いいえ) ▼

- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [不正プログラム対策] > [詳細]タブ(つづき)

許可するスパイウェア/グレーウェア

追加
削除

ローカルイベント通知

不正プログラムの検出時にローカル通知を表示: 初期設定 (はい)

- 初期設定 (はい)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [一般]タブ

一般 | 除外 | SmartProtection | 詳細 | イベント

Webレピュテーション

Webレピュテーションのステータス: オン

セキュリティレベル

☑ 初期設定

○ 高　ブロック対象のページ:
危険: 不正、または脅威の既知の発信源であると確認されたページ
非常に不審: 不正または脅威の発信源である可能性が疑われたページ
不審: スパムメールに関連付けられている、または感染している可能性のあるページ

◉ 中　ブロック対象のページ:
危険: 不正、または脅威の既知の発信源であると確認されたページ
非常に不審: 不正または脅威の発信源である可能性が疑われたページ

○ 低　ブロック対象のページ:
危険: 不正、または脅威の既知の発信源であると確認されたページ

☐ トレンドマイクロでテストしていないページをブロック

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [除外]タブ

一般 | 除外 | SmartProtection | 詳細 | イベント

許可

許可リストに追加するURL (1行に1つずつ):

追加»

削除… エクスポート…

許可するURL	範囲

◉ ドメイン内すべてのURLを許可する
○ URLを許可する

ブロック

ブロックリストに追加するURL (1行に1つずつ):

追加»

削除… エクスポート…

ブロックするURL	範囲

◉ ドメイン内すべてのURLをブロックする
○ URLをブロックする
○ このキーワードを含むURLをブロックする

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [Smart Protection]タブ

一般 | 除外 | Smart Protection | 詳細 | イベント

Webレピュテーションサービス用のSmart Protection Server

☑ 初期設定
◉ Global Smart Protectionサービスへの直接接続
☐ Global Smart Protectionサービスへのアクセス時にプロキシを使用 なし ▼ 編集
※プロキシサーバ有りの場合、プロキシサーバの設定が入ります。
なし
新規…
○ ローカルにインストールされたSmart Protection Serverの使用
追加
削除
☐ ドメインに参加していない場合はGlobal Smart Protectionサービスに接続 (Windowsのみ)

Smart Protection Serverへの接続の警告

Smart Protection Serverへの接続が切断された場合に警告: 初期設定 (はい) ▼
初期設定 (はい)
はい
いいえ

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーション] > [詳細]タブ

一般 | 除外 | Smart Protection | **詳細** | イベント

ブロックページ

☑ 初期設定

ブロックされているページの再評価をユーザが依頼できるようにするため、
ブロックページに表示するリンクを指定します。

リンク: http://sitesafety.trendmicro.com

例: http://intranet.supportdesk.example.com/またはmailto:administrator@example.com

アラート

アラート: 初期設定 (いいえ) ▼

- 初期設定 (いいえ)
- はい
- いいえ

ポート

有害な可能性のあるWebページを監視するポート: 初期設定 (80,8080) ▼

- 初期設定 (80,8080)
- (ポートリスト一覧) *1

*1 ...[ポートリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [Webレピュテーションテーション] > [詳細]タブ（つづき）

ローカルイベント通知

不正なWebサイトへのアクセスのブロック時にローカル通知を表示: 初期設定 (はい)

- 初期設定 (はい)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [一般]タブ

一般 | インターフェイス制限 | 攻撃の予兆 | 詳細 | イベント

ファイアウォール

ファイアウォールステータス: 初期設定(オフ)

- 初期設定(オフ)
- オン
- オフ

ファイアウォールステートフル設定

グローバル (すべてのインタフェース) Enable Stateful Inspection 編集

- 継承 (なし)
- 新規...
- Enable Stateful Inspection
- Deep Security Manager Stateful
- Web Server Stateful
- FTP Server Stateful
- No Stateful Inspection

割り当てられたファイアウォールルール

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [インタフェース制限]タブ

一般 | **インターフェイス制限** | 攻撃の予兆 | 詳細 | イベント

インタフェース制限

◉ 初期設定を使用:
インタフェース制限の有効化: いいえ
○ インタフェース制限の有効化
○ インタフェース制限の無効化

インタフェースパターン備考 *1

優先度 高 ↑ 優先度 低

^ローカル エリア接続.*
^ワイヤレス ネットワーク接続.*

追加
削除
アップ
ダウン

☐ 1つのアクティブインタフェースに制限

*1 …「インタフェース制限」で、「インタフェース制限の有効化」を選択の場合に変更可能です。

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [攻撃の予兆]タブ

一般 | インターフェイス制限 | **攻撃の予兆** | 詳細 | イベント

攻撃の予兆検索

攻撃の予兆の検出の有効化: 初期設定(はい) ▼
- 初期設定(はい)
- はい
- いいえ

☑ OSのフィンガープリント調査 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼ *1
- いいえ
- 1 分
- 2 分
- 5 分
- 10 分
- 15 分
- 30 分

☑ ネットワークまたはポートの検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼
☑ TCP Null検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼
☑ TCP SYNFIN検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼
☑ TCP Xmas検索 ☑ DSMにただちに通知 トラフィックのブロック: いいえ ▼

検出を実行するコンピュータ/ネットワーク: 初期設定 (すべて) ▼
- 初期設定 (すべて)
- すべて
- (IPリスト一覧) *2

検出を実行しないIPリスト: IPリスト: Ignore Reconnaissance ▼
- 初期設定 (なし)
- なし
- IPリスト: Ignore Reconnaissance *2
- (IPリスト一覧)

*1 … [トラフィックのブロック:]は、[攻撃の予兆の検出の有効化]で「はい」を選択すると変更できます。選択肢は下記4項とも共通です。

*2 …[IPリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [ファイアウォール] > [詳細]タブ

一般 | インターフェイス制限 | 攻撃の予兆 | **詳細** | イベント

イベント

「ポリシーの許可外」のパケットのファイアウォールイベントを生成: 初期設定 (はい) ▼

- 初期設定 (はい)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [侵入防御] > [一般]タブ

一般 | 詳細 | イベント

侵入防御

侵入防御のステータス: オン ▼

- 初期設定 (オフ)
- オン
- オフ

侵入防御の動作 *1

◉ 防御　※申込み詳細シートに従い「防御」「検出」のどちらか選択されます

◯ 検出

現在割り当てられている侵入防御ルール

	名前	アプリケーションの種類	優先度	重要度	モード	・・・	・・・	・・・
	動作確認用-テストルール	動作確認用-テストルール	2-標準	中	防御	・・・	・・・	・・・

推奨設定

現在のステータス: 0個の侵入防御ルールが割り当てられています

侵入防御の推奨設定を自動的に適用 (可能な場合): はい ▼

- 初期設定 (いいえ)
- はい
- いいえ

*1 …「設定」で、「オン」を選択の場合に変更可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [侵入防御] > [詳細]タブ

一般 | **詳細** | イベント

イベントデータ

各ルールの最初の検出に関するデータの取り込みを侵入防御ルールに許可する (期間内): 初期設定 (はい) ▼
- 初期設定 (はい)
- はい
- いいえ

ルールアップデート

アップデートされたアプリケーションの種類および侵入防御ルールの依存関係に応じて、新しい侵入防御ルールを自動的に割り当て: 初期設定 (はい) ▼
- 初期設定 (はい)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [変更監視] > [一般]タブ

一般 | 詳細 | イベント

変更監視

変更監視のステータス: 初期設定 (オフ) ▼
- 初期設定 (オフ)
- オン
- オフ

リアルタイム検索の有効化

☐ リアルタイム

現在割り当てられている変更監視ルール

推奨設定

現在のステータス: 0個の変更監視ルールが割り当てられています

変更監視ルールの推奨設定を自動的に適用 (可能な場合): 初期設定(いいえ) ▼
- 初期設定(いいえ)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [変更監視] > [詳細]タブ

一般 | **詳細** | イベント

コンテンツハッシュアルゴリズム

- [x] 初期設定
  - [x] SHA-1
  - [ ] SHA-256

仮想マシンの検索キャッシュ

変更の検索キャッシュの設定: Default Integrity Monitoring Scan Cache Configuration

- 初期設定 (なし)
- 新規...
- なし
- Default Integrity Monitoring Scan Cache Configuration
- (不正プログラム検索設定一覧) *1

CPU使用率

変更監視のCPU使用率レベル: 初期設定(高)

- 初期設定(高)
- 高
- 中
- 低

*1 ...[不正プログラム検索設定]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [セキュリティログ監視] > [一般]タブ

一般 | 詳細 | イベント

セキュリティログ監視

セキュリティログ監視のステータス: オン

- 初期設定 (オフ)
- オン
- オフ

現在割り当てられているセキュリティログ監視ルール

1002792-Default Rules Configuration
1002795-Microsoft Windows Events

推奨設定

現在のステータス: 0個のセキュリティログ監視ルールが割り当てられています

セキュリティログ監視ルールの推奨設定を自動的に適用 (可能な場合): 初期設定 (いいえ)

- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー] > [RJ Policy:詳細] > [セキュリティログ監視] > [詳細]タブ

一般 | **詳細** | イベント

重要度のクリッピング

Agent/Applianceイベントが次の重要度以上の場合に、イベントをSyslogに送信:	初期設定 (中 (6)) ▼	*1
Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDSMに送信	初期設定 (中 (6)) ▼	*1

*1 ...初期設定 (中 (6)) ,低 (0) ,低 (1) ,低 (2) ,低 (3) ,中 (4) ,中 (5) ,中 (6) ,中 (7) ,
高 (8) ,高 (9) ,高 (10) ,高 (11) ,重大 (12) ,重大 (13) ,重大 (14) ,重大 (15)より設定可能です。

[ポリシー] > [RJ Policy:詳細] > [インタフェースの種類]

ネットワークインタフェースの種類

◉ ルールをすべてのネットワークインタフェースに適用

○ ルールを特定のインタフェースに適用

[ポリシー] > [RJ Policy:詳細] > [設定] > [コンピュータ]タブ

コンピュータ | ネットワークエンジン | 検索 | SIEM

通信方向

Deep Security ManagerとAgent/Applianceの通信方向: 初期設定 (双方向) ▼

- 初期設定 (双方向)
- Agent/Applianceから開始
- Managerから開始
- 双方向

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [コンピュータ]タブ（つづき）

ハートビート

ハートビート間隔 (分):

初期設定 (10 分) ▼
- 初期設定 (10 分)
- 1 分
- 2 分
- 5 分
- 10 分
- 20 分
- 30 分
- 60 分
- 2 時間
- 4 時間
- 8 時間
- 12 時間
- 24 時間

次の数を超えるハートビートが失われた場合にアラートを発令:

初期設定 (2) ▼
- 初期設定 (2)
- 無制限
- 1
- 2
- 5
- 10
- 20
- 30
- 60

ハートビート間でコンピュータのローカルシステム時間が次の時間を超えて変更された場合にアラートを発令:

初期設定 (無制限) ▼
- 初期設定 (無制限)
- 無制限
- 5 分
- 10 分
- 20 分
- 30 分
- 60 分

非アクティブな仮想マシンに対してオフラインエラーを発令:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [コンピュータ]タブ（つづき）

ポリシーの変更をすぐに送信

ポリシーの変更をコンピュータに自動的に送信:

初期設定 (はい) ▼
- 初期設定 (はい)
- はい
- いいえ

トラブルシューティング

ログレベル:

初期設定 (オーバーライドしない) ▼
- 初期設定 (オーバーライドしない)
- オーバーライドしない
- 完全なファイアウォールイベントのログ記録
- 完全な侵入防御イベントのログ記録
- 完全なログ記録

Agentセルフプロテクション

ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否:

はい ▼
- 初期設定 (いいえ)
- はい
- いいえ

ローカルでの変更許可にパスワードを要求:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

パスワード:

パスワードの確認入力:

環境変数のオーバーライド:

環境変数の表示

※ 上記[環境変数の表示]クリックすると、[環境変数のオーバーライド]が表示されます。
[新規]

環境変数のプロパティ

名前:

値 :

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ

コンピュータ | **ネットワークエンジン** | 検索 | SIEM

ネットワークエンジンモード

ネットワークエンジンモード: 初期設定 (インライン) ▼

- 初期設定 (インライン)
- インライン
- タップ

イベント

イベントログファイルの最大サイズ (Agent/Appliance): 初期設定 (4 MB) ▼

- 初期設定 (4 MB)
- 512 KB
- 1 MB
- 2 MB
- 3 MB
- 4 MB
- 5 MB
- 10 MB

保管するイベントログファイル数 (Agent/Appliance): 初期設定 (3) ▼

- 初期設定 (3)
- 1
- 2
- 3
- 5
- 10
- 15
- 20
- 25

次の送信元IPのイベントは記録しない: 初期設定 (なし) ▼

- 初期設定 (なし)
- (IPリスト一覧) *1

*1 ...[IPリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

イベント

キャッシュサイズ:

初期設定 (128)
- 初期設定 (128)
- 0
- 1
- 2
- 4
- 8
- 16
- 32
- 64
- 128
- 256
- 512
- 1024

キャッシュの寿命:

初期設定 (30 分)
- 初期設定 (30 分)
- 1 分
- 15 分
- 30 分
- 45 分
- 60 分

キャッシュの有効期間:

初期設定 (15 分)
- 初期設定 (15 分)
- 1 分
- 15 分
- 30 分
- 45 分
- 60 分

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

コンピュータ | **ネットワークエンジン** | 検索 | SIEM

ネットワークエンジンの詳細設定

Agentの設定パッケージが最大サイズを超えた場合にアラートを生成する: 初期設定 (はい)
- 初期設定 (はい)
- はい
- いいえ

☑ 初期設定

CLOSEDタイムアウト: 初期設定 (0 秒) *1
- 初期設定 (0 秒)

SYN_SENTタイムアウト: 初期設定 (20 秒) *1
- 初期設定 (20 秒)

SYN_RCVDタイムアウト: 初期設定 (60 秒) *1
- 初期設定 (60 秒)

FIN_WAIT1タイムアウト: 初期設定(2 分) *1
- 初期設定 (2 分)

ESTABLISHEDタイムアウト: 初期設定 (3 時間)
- 初期設定 (3 時間)
- 1 時間
- 2 時間
- 3 時間
- 4 時間
- 12 時間
- 24 時間
- 2 日

ERRORタイムアウト: 初期設定 (10 秒) *1
- 初期設定 (10 秒)

DISCONNECTタイムアウト: 初期設定 (60 秒) *1
- 初期設定 (60 秒)

CLOSE_WAITタイムアウト: 初期設定 (2 分) *1
- 初期設定 (2 分)

*1 … 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

CLOSINGタイムアウト:	初期設定(1 秒) 初期設定 (1 秒) *1
LAST_ACKタイムアウト:	初期設定 (30 秒) 初期設定 (30 秒) *1
ACKストームタイムアウト:	初期設定 (1 秒) 継承 (1 秒) *1
ブートスタートタイムアウト:	初期設定 (20 秒) 初期設定 (20 秒) *1
コールドスタートタイムアウト:	初期設定 (5 分) 初期設定 (5 分) *1
UDPタイムアウト:	初期設定 (10 秒) 初期設定 (10 秒) *1
ICMPタイムアウト:	初期設定 (60 秒) 初期設定 (60 秒) *1
Null IPを許可:	初期設定 (はい) 初期設定 (はい) はい いいえ
バージョン8以前のAgentとApplianceでIPv6をブロック:	初期設定 (はい) 初期設定 (はい) はい いいえ
バージョン9以降のAgentとApplianceでIPv6をブロック:	初期設定 (いいえ) 初期設定 (いいえ) はい いいえ

*1 ... 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

接続クリーンナップタイムアウト:	初期設定 (10 秒) 初期設定 (10 秒) *1
最大接続数 (クリーンナップ単位):	初期設定 (1000) 初期設定 (1000) *2
送信元と送信先が同じIPアドレスをブロック:	初期設定 (はい) 初期設定 (はい) はい いいえ
最大TCP接続数:	初期設定 (1000) 初期設定 (1000) *2
最大UDP接続数:	初期設定 (1000) 初期設定 (1000) *2
最大ICMP接続数:	初期設定 (10000) 初期設定 (10000) *2
最大イベント数 (秒単位):	初期設定 (100) 初期設定 (100) 100 200 300 400 500

*1 ... 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

*2 ... 100, 500, 1000, 2000, 3000, 4000, 5000, 6000, 7000, , 8000, 9000, 10000, 20000, 30000, 40000, 50000, 60000, 70000, 80000, 90000, 100000, 200000, 300000, 400000, 500000, 600000, 700000, 800000, 900000, 1000000 ,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

TCP MSSの制限:

初期設定 (無制限) ▼

- 初期設定 (無制限)
- 536 バイト
- 600 バイト
- 700 バイト
- 800 バイト
- 900 バイト
- 1000 バイト
- 1100 バイト
- 1200 バイト
- 1276 バイト
- 1300 バイト
- 1360 バイト
- 1400 バイト
- 1440 バイト
- 1452 バイト
- 1460 バイト
- 無制限

イベントノードの数:

初期設定 (20000) ▼

- 初期設定 (20000)
- 1000
- 5000
- 10000
- 15000
- 20000
- 25000
- 30000
- 40000
- 50000
- 75000
- 100000
- 150000
- 200000
- 250000

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

ステータスコードの無視: 初期設定 (なし) ▼ 初期設定 (なし) *1

ステータスコードの無視: 初期設定 (なし) ▼ 初期設定 (なし) *1

ステータスコードの無視: 初期設定 (なし) ▼ 初期設定 (なし) *1

*1 ... 下記イベントステータスの選択肢より設定可能です。

継承 (なし)	不正なデータオフセット
なし	IPヘッダなし
セッション情報なし	読み取り不能なイーサネットヘッダ
不正なフラグ	未定義
不正なシーケンス	送信元および送信先IPが同一
不正なACK	不正なTCPヘッダ長
内部エラー	読み取り不能なプロトコルヘッダ
CEフラグ	読み取り不能なIPv4ヘッダ
不正なIP	不明なIPバージョン
不正なIPデータグラム長	不正なアダプタ設定
フラグメント化	重複しているフラグメント
不正なフラグメントオフセット	ACK再送の上限
最初のフラグメントが最小サイズ未満	切断された接続上のパケット
範囲外のフラグメント	再送の破棄
最小オフセット値以下のフラグメント	未定義
IPv6パケット	ポリシーで未許可 (オープンポート)
受信接続の上限	新しい接続の開始
送信接続の上限	無効なチェックサム
SYN送信の上限	無効なフック
ライセンスの期限切れ	IPペイロードがゼロ
不明なIPバージョン	IPv6ソースがマルチキャスト
不正なパケット情報	無効なIPv6アドレス
内部エンジンエラー	最小サイズ以下のIPv6のフラグメント
許可されていないUDP応答	無効なトランスポートヘッダ長
許可されていないICMP応答	メモリ不足
ポリシーで未許可	最大TCP接続数
不正なポートコマンド	最大UDP接続数
SYN Cookieエラー	

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

詳細なログ記録ポリシー:

初期設定 (初期設定)
- 初期設定 (初期設定)
- バイパス
- 初期設定
- 標準
- 下位互換性モード
- 詳細モード
- ステートフルおよび正規化の抑制
- ステートフル、正規化、およびフラグメントの抑制
- ステートフル、フラグメント、および検証機能の抑制
- タップモード

サイレントTCP接続拒否:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

デバッグモードを有効にする:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

デバッグモードで保持するパケットの数:

初期設定 (8)
- 初期設定 (8)
- 8
- 16
- 24
- 32
- 40
- 48
- 56
- 64

すべてのパケットデータをログに記録する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

期間内で1つのパケットデータのみをログに記録する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

1つのパケットデータのみをログに記録する期間:

初期設定 (5 分)
- 初期設定 (5 分)
- 0 秒
- 10 秒
- 30 秒
- 60 秒
- 2 分
- 3 分
- 4 分
- 5 分
- 10 分
- 20 分
- 40 分
- 50 分
- 100 分

パケットデータがキャプチャされたときに格納する最大データサイズ:

初期設定 (1500 バイト)
- 初期設定 (1500 バイト)
- 0 バイト
- 16 バイト
- 32 バイト
- 64 バイト
- 68 バイト
- 128 バイト
- 512 バイト
- 1024 バイト
- 1500 バイト
- 2048 バイト
- 4096 バイト

TCPの接続イベントを生成する:

初期設定 (いいえ)
- 初期設定(いいえ)
- はい
- いいえ

ICMPの接続イベントを生成する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

UDPの接続イベントを生成する:

初期設定 (いいえ)
- 初期設定 (いいえ)
- はい
- いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

Cisco WAAS接続のバイパス:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

回避再送の破棄:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

TCPチェックサムの確認:

初期設定 (いいえ) ▼
- 初期設定 (いいえ)
- はい
- いいえ

最小フラグメントオフセット:

初期設定 (60) ▼
- 初期設定 (60)
- 0
- 30
- 60
- 90
- 120

最小フラグメントサイズ:

初期設定 (120) ▼
- 初期設定 (120)
- 0
- 60
- 120
- 180
- 240

SSLセッションのサイズ:

初期設定 (低 - 2500) ▼
- 初期設定 (低 - 2500)
- 低 - 2500
- 中 - 5000
- 高 - 10000

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

SSLセッションの時間:

初期設定 (24 時間)
- 初期設定 (24 時間)
- 60 分
- 2 時間
- 4 時間
- 8 時間
- 12 時間
- 16 時間
- 20 時間
- 24 時間

IPv4トンネルのフィルタ:

初期設定 (IPv4トンネルの検出の無効化)
- 初期設定 (IPv4トンネルの検出の無効化)
- IPv4トンネルの検出の無効化
- トンネルパケットの解読
- トンネルパケットのドロップ (イベントによる)

IPv6トンネルのフィルタ:

初期設定 (IPv6トンネルの検出の無効化)
- 初期設定 (IPv6トンネルの検出の無効化)
- IPv6トンネルの検出の無効化
- トンネルパケットの解読
- トンネルパケットのドロップ (イベントによる)

厳密なTeredoのポート確認:

初期設定 (はい)
- 初期設定 (はい)
- はい
- いいえ

Teredoの異常のドロップ:

初期設定 (はい)
- 初期設定 (はい)
- はい
- いいえ

最大トンネル深度:

初期設定 (1)
- 初期設定 (1)
- 1
- 2
- 3
- 4

最大トンネル深度超過時の処理:

初期設定 (ドロップ)
- 初期設定 (ドロップ)
- ドロップ
- バイパス

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

IPv6拡張タイプ0のドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
最小MTU未満のIPv6フラグメントのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
IPv6予約済みアドレスのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
IPv6サイトローカルアドレスのドロップ:	初期設定 (いいえ) 初期設定 (いいえ) はい いいえ
IPv6 Bogonアドレスのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
6to4 Bogonアドレスのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
ゼロペイロードのIPパケットのドロップ:	初期設定 (はい) 初期設定 (はい) はい いいえ
不明なSSLプロトコルを破棄:	初期設定 (はい) 初期設定 (はい) はい いいえ

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [ネットワークエンジン]タブ（つづき）

ネットワークエンジンの詳細設定

フラグメントタイムアウト:

初期設定 (60 秒) ▼

初期設定 (60 秒)

*1

保持するフラグメント化されたIPパケットの最大数:

初期設定 (1000) ▼

初期設定 (1000)
10
50
100
200
500
1000
5000
10000

フラグメント化されたパケットのタイムアウトを超過したことを示すためにICMPを送信する:

初期設定 (はい) ▼

初期設定 (はい)
はい
いいえ

*1 ... 0 秒, 1 秒, 2 秒, 3 秒, 4 秒, 5 秒, 6 秒, 7 秒, 8 秒, 9 秒, 10 秒, 15 秒, 20 秒, 25 秒, 30 秒, 45 秒, 60 秒, 90 秒, 2 分, 3 分, 4 分, 5 分, 10 分,より設定可能です。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [検索]タブ

コンピュータ | ネットワークエンジン | **検索** | SIEM

開いているポート

検索するポート: 初期設定 (1-1024) ▼ 編集

- 初期設定 (1-1024)
- 1-1024
- (ポートリスト一覧) *1

推奨設定

推奨設定の継続的な検索を実行: 初期設定 (いいえ) ▼

- 初期設定 (いいえ)
- はい
- いいえ

継続検索の間隔: 初期設定 (7 日) ▼

- 初期設定 (7 日)
- 5 分
- 10 分
- 20 分
- 30 分
- 60 分
- 2 時間
- 3 時間
- 6 時間
- 12 時間
- 24 時間
- 2 日
- 3 日
- 7 日
- 2 週
- 3 週
- 4 週

*1 ...[ポートリスト]シートの選択肢が表示されます。

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [検索]タブ(つづき)

Virtual Appliance

Virtual Appliance同時検索の最大数:

初期設定 (1) ▼
- 初期設定 (1)
- 1
- 5
- 10
- 15

不正プログラムの手動検索キャッシュの最大エントリ数:

初期設定 (500000) ▼
- 初期設定 (500000)
- 100000
- 250000
- 500000
- 750000
- 1000000
- 2500000
- 5000000
- 7500000
- 10000000

不正プログラムのリアルタイム検索キャッシュの最大エントリ数:

初期設定 (500000) ▼
- 初期設定 (500000)
- 100000
- 250000
- 500000
- 750000
- 1000000
- 2500000
- 5000000
- 7500000
- 10000000

変更監視の検索キャッシュの最大エントリ数:

初期設定 (500000) ▼
- 初期設定 (500000)
- 100000
- 250000
- 500000
- 750000
- 1000000
- 2500000
- 5000000
- 7500000
- 10000000

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [SIEM]タブ

コンピュータ | ネットワークエンジン | 検索 | **SIEM**

イベント転送の頻度 (Agent/Applianceから)

イベントの送信間隔: 初期設定 (60 秒) ▼
初期設定 (60 秒)
*1

不正プログラム対策イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:
リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼
ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼
Common Event Format

◯ イベントを転送しない

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [SIEM]タブ（つづき）

Webレピュテーションイベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

◯ イベントを転送しない

ファイアウォールと侵入防御イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

◯ イベントを転送しない

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [設定] > [SIEM]タブ（つづき）

変更監視イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

◯ イベントを転送しない

セキュリティログ監視イベントの転送 (Agent/Applianceから)

◉ 初期設定を使用:

リモートコンピュータにイベントを転送する (Syslog経由): いいえ

◯ イベントの転送先:

◯ 直接転送する

◉ Manager経由でリレーする

イベントの送信先のホスト名またはIPアドレス:

イベントの送信先UDPポート:

Syslogファシリティ: ローカル0 ▼

ローカル0
ローカル1
ローカル2
ローカル3
ローカル4
ローカル5
ローカル6
ローカル7

Syslog形式: Common Event Format ▼

Common Event Format

◯ イベントを転送しない

[ポリシー]メニュー(つづき)

[ポリシー] > [RJ Policy:詳細] > [オーバーライド]

オーバーライド		
不正プログラム対策		
不正プログラム対策設定	2個のオーバーライド	削除
割り当てられた不正プログラム検索設定	3個のオーバーライド	削除
Webレピュテーション		
Webレピュテーションの設定	継承	削除
ファイアウォール		
ファイアウォールの設定	1個のオーバーライド	削除
オーバーライドされたファイアウォールルール	継承	削除
割り当てられたファイアウォールステートフル設定	1個のオーバーライド	削除
侵入防御		
侵入防御の設定	継承	削除
オーバーライドされた侵入防御ルール	継承	削除
オーバーライドされたアプリケーションの種類	継承	削除
変更監視		
変更監視の設定	1個のオーバーライド	削除
オーバーライドされた変更監視ルール	継承	削除
セキュリティログ監視		
セキュリティログ監視の設定	継承	削除
オーバーライドされたセキュリティログ監視ルール	継承	削除
システム		
オーバーライドされたコンピュータ設定	1個のオーバーライド	削除

管理（システム設定）

[管理]メニュー

[管理メニュー]

システム設定	システム設定 *1
予約タスク	
イベントベースタスク	
Managerノード	
ライセンス	
ユーザ管理	
ユーザ	
役割	
連絡先	
システム情報	*2
アップデート	
セキュリティ	
ルール	
パターンファイル	
ソフトウェア	
ダウンロードセンター	
ローカル	
Relayグループ	

*1 ... 左側の選択したメニュー名が表示されます。

*2 ... 各メニューの設定内容は下記より記載します。

[システム設定]

システム設定タブ一覧

- Agent
- アラート
- コンテキスト
- SIEM
- SNMP
- ランク付け
- システムイベント
- セキュリティ
- アップデート
- スマートフィードバック
- SMTP
- ストレージ
- プロキシ
- 詳細

Copyright © 2015 Trend Micro Incorporated. All rights Reserved.

[管理]メニュー（つづき）

[システム設定] > [Agent]タブ

ホスト名

- ☐ IPがホスト名として使用されており、Agent/Applianceからの通信または検出時にIPの変更が検出された場合は、[ホスト名] エントリをアップデート
- ☐ IPがホスト名として使用されておらず、Agentからの通信または検出後にIPの変更が検出された場合は、[ホスト名] エントリをアップデート

Agentからのリモート有効化

- ☐ Agentからのリモート有効化を許可
  - ◉ 任意のコンピュータ
  - ○ 既存のコンピュータ
  - ○ 次のIPリストにあるコンピュータ: なし ▼
    - なし
    - Corporate Network IPs
    - Domain Controller(s)
    - Ignore Reconnaissance
    - Network Broadcast
    - Off Domain
    - IPs VPN Tunnel IPs

割り当てるポリシー (有効化スクリプトによってポリシーが割り当てられていない場合): なし ▼
- なし
- (登録ポリシー名)

- ☑ Agentによるホスト名指定を許可

同じ名前のコンピュータがすでに存在する場合: 有効化を許可しない ▼
- 有効化を許可しない
- 同じ名前で新規コンピュータを有効化
- 既存のコンピュータの再有効化

※プロキシサーバ利用時は、
「同じ名前で新規コンピュータを有効化」
が選択されます。

- ☐ クローン仮想マシンの再有効化を許可
- ☐ 不明な仮想マシンの再有効化を許可

データプライバシー

- ☐ 暗号化されたトラフィック (SSL) のパケットデータの取り込みを許可

AgentなしのvCloud保護

- ☐ ApplianceによるvCloud仮想マシンの保護を許可

Copyright © 2015 Trend Micro Incorporated. All rights Reserved.

[管理]メニュー（つづき）

[システム設定] > [プロキシ]タブ

プロキシサーバの使用

Agent、Appliance、およびRelayで使用するセキュリティアップデート用プロキシサーバ:

※プロキシサーバ有りの場合、後述の「プロキシサーバ」で設定されたプロキシサーバが入ります。

なし

なし

プロキシサーバ ※プロキシサーバ有りの場合、申込み詳細シートに従い、プロキシサーバの設定が入ります。

[新規] > [新しいプロキシサーバ] > [一般]タブ

一般情報

名前: 新しいプロキシ

説明:

プロキシ設定

プロキシプロトコル ◉ HTTP ○ SOCKS4 ○ SOCKS5

アドレス:

ポート:

☐ プロキシサーバへの接続に認証を使用

ユーザ名:

パスワード:

[新規] > [新しいプロキシサーバ] > [割り当て対象]タブ

割り当て対象

プロキシは使用されていません。

Copyright © 2015 Trend Micro Incorporated. All rights Reserved.

管理 (予約タスク)

[管理]メニュー

[管理メニュー]

システム設定 予約タスク イベントベースタスク Managerノード ライセンス ユーザ管理 ユーザ 役割 連絡先 システム情報 アップデート セキュリティ ルール パターンファイル ソフトウェア ダウンロードセンター ローカル Relayグループ	予約タスク *1 *2

*1 ... 左側の選択したメニュー名が表示されます。

*2 ... 各メニューの設定内容は下記より記載します。

[管理]メニュー（つづき）

[予約タスク]

[セキュリティアップデートを週単位確認] > [一般]タブ

一般　タスク詳細

一般情報

名前: コンポーネントアップデートタスク

種類: セキュリティアップデートの確認

タスクの有効化: ☑

スケジュール情報

- ○ 時間単位
- ○ 日単位
- ◉ 週単位
- ○ 月単位
- ○ 1回のみ

スケジュール詳細 (週次)

開始時刻: 01:00

1 週ごと

- ☐ 日曜
- ☐ 月曜
- ☐ 火曜
- ☐ 水曜
- ☑ 木曜
- ☐ 金曜
- ☐ 土曜

[セキュリティアップデートを週単位確認] > [タスク詳細]タブ

一般　タスク詳細

対象ホストの詳細

- ◉ すべてのコンピュータ
- ○ グループ: コンピュータ
  - ☐ サブグループも含める
- ○ 使用ポリシー: なし
  - ☐ サブポリシーも含める
- ○ コンピュータ: （ホスト名）

[管理]メニュー（つづき）

[予約タスク]

[レポートの生成および送信を月単位確認] > [一般]タブ

一般 | タスク詳細

一般情報

名前: 月単位概要レポート

種類: レポートの生成および送信

タスクの有効化: ☑

スケジュール情報

- ○ 時間単位
- ○ 日単位
- ○ 週単位
- ◉ 月単位
- ○ 1回のみ

スケジュール詳細 (月次)

開始時刻: 00:00 *1

◉ 日 1 *3

○ *4

○ 月の最終日

月を指定: ☑ 1月 ☑ 2月 ☑ 3月 ☑ 4月 ☑ 5月 ☑ 6月 ☑ 7月 ☑ 8月 ☑ 9月 ☑ 10月 ☑ 11月 ☑ 12月

一般 | タスク詳細

レポート: 概要レポート

形式: ポータブルドキュメントフォーマット (PDF)

タグ

- ◉ すべて
- ○ タグなし
- ○ タグ

期間

過去 1 か月間

コンピュータ

- ◉ すべてのコンピュータ
- ○ グループ: コンピュータ
  - ☐ サブグループも含める
- ○ 使用ポリシー: なし
  - ☐ サブポリシーも含める
- ○ コンピュータ: （ホスト名）

[管理]メニュー（つづき）

[予約タスク]

[レポートの生成および送信を月単位確認] > [タスク詳細]タブ（つづき）

レポート受信者

- (●) すべてのユーザおよび連絡先
- ( ) ユーザ:
  - [ ] (ユーザ名)
  - 連絡先:
    - (連絡先はありません)

[予約タスク]

[コンピュータの推奨設定検索を週単位確認] > [一般]タブ

一般 | タスク詳細

一般情報

名前: 週単位コンピュータの推奨設定を検索

種類: コンピュータの推奨設定検索

タスクの有効化: [✓]

スケジュール情報

- ( ) 時間単位
- ( ) 日単位
- (●) 週単位
- ( ) 月単位
- ( ) 1回のみ

スケジュール詳細 (週次)

開始時刻: 02:00

1 週ごと

- [ ] 日曜
- [ ] 月曜
- [ ] 火曜
- [ ] 水曜
- [✓] 木曜
- [ ] 金曜
- [ ] 土曜

[コンピュータの推奨設定検索を週単位確認] > [タスク詳細]タブ

一般 | タスク詳細

対象ホストの詳細

- (●) すべてのコンピュータ
- ( ) グループ: コンピュータ
  - [ ] サブグループも含める
- ( ) 使用ポリシー: なし
  - [ ] サブポリシーも含める
- ( ) コンピュータ: (ホスト名)