

- 下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒WebレピュテーションとURLフィルタリングのHTTPS通信検知ログを元とした注意が必要なイベントが発生しなくなります。

- ①管理コンソールへログイン後、
「ポリシー」-「グローバルセキュリティエージェント設定」-「セキュリティ設定」タブにて下記を設定

「HTTPS Web評価」の項目から

[Chrome、FirefoxおよびMicrosoft EdgeでWebレピュテーションとURLフィルタリングのHTTPS確認を有効にする] をオン
(チェックを入れた状態)

- ②保存をクリック

The screenshot displays the 'Global Security Agent Settings' page in the Microsoft Intune management console. The left-hand navigation pane shows the 'Global Security Agent Settings' option selected. The main content area is divided into several sections:

- Compression File Search Limit:** Includes checkboxes for 'Enable compression file search limit' (checked), 'Enable compression file virus removal' (checked), and 'Enable OLE objects search' (checked). It also features input fields for file size (2 MB) and search depth (100 files).
- Endpoint Protection:** Includes a checkbox for 'Enable endpoint Windows shortcut menu search' (unchecked).
- HTTPS Web evaluation:** This section is highlighted with a red box. It contains a checked checkbox for 'Enable Chrome, Firefox and Microsoft Edge with Web Reputation and URL Filtering HTTPS Confirmation' and a note: 'Note: To use this feature, the administrator must enable the anti-malware service in policy management.' Below it is another checked checkbox for 'Display notification when Chrome or Firefox requires an update'.

The 'Save' button at the bottom of the page is also highlighted with a red box.

対象者：② [WebレピュテーションおよびURLフィルタのログをサーバに送信する] がオフのユーザ

- 下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒ VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールへログイン後、
「ポリシー」-「グローバルセキュリティエージェント設定」-「エージェントコントロール」タブにて下記を設定
[WebレピュテーションおよびURLフィルタのログをサーバに送信する]：オン（チェックを入れた状態）

②保存をクリック

ダッシュボード
セキュリティエ...
ユーザ
ポリシー
レポート
ログ
管理

ポリシー設定

追加の設定

グローバルセキュリティエージェント設定

グローバル除外リスト

ポリシーリソース

アプリケーションコントロールルール

グローバルセキュリティエージェント設定

グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール

警告

7 日経過してもウイルスパターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

セキュリティエージェントのログ

WebレピュテーションおよびURLフィルタのログをサーバに送信する

脅威イベントの詳細を強化型脅威分析のためにサーバに送信する

監視サービス

セキュリティエージェントの監視サービスを有効にする:

セキュリティエージェントのステータスを 1 分間隔で確認

セキュリティエージェントを再起動できない場合、 5 回まで再試行

管理者への問い合わせの通知

セキュリティエージェントに管理者への問い合わせ情報を表示する

アンインストール

保存

対象者：③ [脅威イベントの詳細を強化型脅威分析のためにサーバに送信する] がオフのユーザ

- 下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒ VBBSS検知ログを元とした注意が必要なイベントが発生しなくなります。

①管理コンソールへログイン後、
「ポリシー」-「グローバルセキュリティエージェント設定」-「エージェントコントロール」タブにて下記を設定
[脅威イベントの詳細を強化型脅威分析のためにサーバに送信する]：オン（チェックを入れた状態）

②保存をクリック

ダッシュボード
セキュリティエー...
ユーザ
ポリシー
レポート
ログ
管理

ポリシー設定

追加の設定

グローバルセキュリティエージェント設定

グローバル除外リスト

ポリシーリソース

アプリケーションコントロールルール

グローバルセキュリティエージェント設定

グローバル設定はサポートされるすべてのセキュリティエージェントに適用されます。

セキュリティ設定 エージェントコントロール

警告

7 日経過してもウイルスパターンファイルがアップデートされていない場合、Windowsタスクバーに警告アイコンを表示する

セキュリティエージェントのログ

WebレピュテーションおよびURLフィルタのログをサーバに送信する

脅威イベントの詳細を強化型脅威分析のためにサーバに送信する

監視サービス

セキュリティエージェントの監視サービスを有効にする:

セキュリティエージェントのステータスを 1 分間隔で確認

セキュリティエージェントを再起動できない場合、 5 回まで再試行

管理者への問い合わせの通知

セキュリティエージェントに管理者への問い合わせ情報を表示する

アンインストール

保存

対象者：④[webレピュテーション] がオフのユーザ

- 下記の設定を有効にしない場合、下記設定に関連するEDRの機能がご利用できません。
⇒Webレピュテーション検知を元とした、注意が必要なイベントが発生しなくなります。

①管理コンソールへログイン後、
「セキュリティエージェント」-「開通時初期設定」※-「ポリシーの設定」-対象のOSを選択し、
「webレピュテーション」タブにて下記を設定
[webレピュテーション] をオン

②保存をクリック

使用しているOSを
ご指定ください



ポリシーの設定: 開通時初期設定

対象とサービスの設定

Webレピュテーション

Webレピュテーションは不正Webサイトの脅威からの保護を強化します。

オン

セキュリティレベル

	危険	極めて不審	不審
<input type="radio"/> 高	⊗	⊗	⊗
<input checked="" type="radio"/> 中 (初期設定)	⊗	⊗	
<input type="radio"/> 低	⊗		

Webサイトのアクセスをブロックします ①

未評価のURL

トレンドマイクロによる評価が完了していないWebサイトをブロックする ①

ブラウザ脆弱性対策

不正なスクリプトを含むWebサイトをブロックする

保存 キャンセル

※「開通時初期設定」とは、お申込み時に申請いただいた内容の設定情報を反映させたポリシーグループになります。新たなポリシーを作成している際は、作成したポリシーグループをご指定ください。