

MR-EP 誤検知で隔離されたファイルのオーバーライドと復元

MR-EP によって正当なソフトウェアが不正判定されてしまうことがあります。

オーバーライドの作成とファイルの復元を行うことで Webroot のクラウド判定にかかわらず、ファイルの実行を許可します。

〈事業体からの手順〉

- ① Web コンソールにログインします。
- ② [事業体]タブ > [すべての事業体] をクリックします。
- ③ 対象のデバイス名をクリックします。

opentext Management Console CE 24.4

事業体

グループ	名前	③	状態	ポリシー	最終確認日時	最近の感染
+			保護されています	2 ポリシー	12月 09, 2024 (18:21)	10月 10, 2024 (16:31)
すべての事業体			保護されています	MR-EP推奨設定	12月 06, 2024 (09:20)	8月 30, 2024 (10:17)
デフォルトのグループ	5		要対応	MR-EP推奨設定	12月 12, 2024 (14:54)	12月 12, 2024 (14:54)
営業部	0		保護されています	IS部検証用		
総務部	2		保護されています	MR-EP推奨設定	12月 05, 2024 (16:03)	
開発部	0		保護されています	MR-EP推奨設定	本日 (15:16)	2月 07, 2024 (16:14)
非アクティブ化済みデバイス	6		保護されています	2 ポリシー	本日 (14:30)	11月 27, 2023 (16:44)

- ④ [検出された脅威]の数字をクリックします。

概要 検出された脅威 Web Threat Shield のブロック スキャン履歴 プロセスログ

デバイス情報

一般

状態: 保護されています

最終確認日時: 12月 09, 2024 (18:21)

現在のユーザー: 0000

ホスト名: [Redacted]

グループ: デフォルトのグループ

キーコード: [Redacted]

ポリシー

エンドポイント ポリシー: 変更ポリシー

ENDPOINT PROTECTION

アクティビティ

検出された脅威: ④ 1

ブロックした URL (過去 90 日間): 0

プロパティ

有効期限: 5月 01, 2025

エージェントのバージョン: 9.0.36.40

修復: 有効

スキャンのスケジュール: 有効

スキャン頻度: 毎日

シールドの状態

リアルタイム シールド: 有効

ルートキット シールド: 有効

Web Threat Shield: 有効

USB シールド: 有効

オフライン シールド: 有効

ID シールド: 有効

フィッシング シールド: 有効

スクリプトシールド: 無効にされています。

ファイアウォール: 有効

Webroot Infrared: 有効

⑤ [操作] > [許可リストにファイルを追加]をクリックします。

The screenshot shows the '検出された脅威' (Detected Threats) section of the Web Threat Shield interface. It features a table for 'ファイル脅威の検出' (File Threat Detection) with columns for 'ファイル名' (File Name), 'パス名' (Path Name), and 'マルウェアグループ' (Malware Group). The first row contains 'WEBROOTTESTFILE.EXE', '%temp%\c095e620-ed36-4151-899d-8378...', and 'W32.Webroottestfile'. A red box highlights the '許可リストにファイルを追加' (Add file to allow list) button in the '操作' (Action) column. Another red box highlights the information icon in the same column, with a circled '5' next to it. Below the table, there is a section for 'EVASION SHIELD スクリプト検出' (Evasion Shield Script Detection) with a message: '一致する結果は見つかりませんでした' (No matching results were found).

⑥ 許可オーバーライドの作成の種類で[MD5]を選択します。

ここでは MD5 は指定されている為、入力不要です。

(1) オーバーライド名を付けます。

(2) [ポリシーに関連付ける]…グローバルポリシーを含む特定のポリシーにオーバーライドを適用する場合はチェックを入れ、適用したいポリシーを選択します。

(3) [保存]をクリックします。

The screenshot shows the '許可オーバーライドの作成' (Create Allow Override) dialog box. It has sections for '許可/ブロック' (Allow/Block) with '許可' (Allow) selected, '種類' (Type) with 'MD5' selected, and 'Webrootクラウド判定' (Webroot Cloud Judgment) with 'MD5' entered. There is a 'クラウド判定' (Cloud Judgment) section with a red error icon and the text '不正' (Invalid). The '名前 * (1)' (Name) field contains '支援システム'. There is a 'ポリシーに関連付け (2)' (Associate with Policy) checkbox which is unchecked. At the bottom, there are '閉じる' (Close) and '保存 (3)' (Save) buttons.

⑦ [操作] > [隔離先から復元]をクリックします。

The screenshot shows the Microsoft Defender console interface. At the top, there are navigation tabs: 概要 (Overview), 検出された脅威 (Detected threats), Web Threat Shield のブロック (Web Threat Shield blocks), スキャン履歴 (Scan history), and プロセスログ (Process log). The '検出された脅威' tab is selected. Below this, there are two sections: 'ファイル脅威の検出' (File threat detection) and 'EVASION SHIELD スクリプト検出' (Evasion Shield script detection). The 'ファイル脅威の検出' section contains a table with columns: ファイル名 (File name), バス名 (Path), マルウェアグループ (Malware group), and 操作 (Action). The first row shows the file 'WEBROOTTESTFILE.EXE' at the path '%temp%\c095e620-ed36-4151-899d-8378...' with the malware group 'W32.Webroottestfile'. A context menu is open over the '操作' column, showing options: '許可リストにファイルを追加' (Add file to allow list) and '隔離先から復元' (Restore from quarantine). A red circle with the number 7 is next to the '操作' column header, and a red box highlights the '隔離先から復元' button. A red arrow points from the box to the button. Below the 'EVASION SHIELD スクリプト検出' section, there is a message: '一致する結果は見つかりませんでした' (No matching results were found).

⑧ [コマンドの送信]をクリックします。

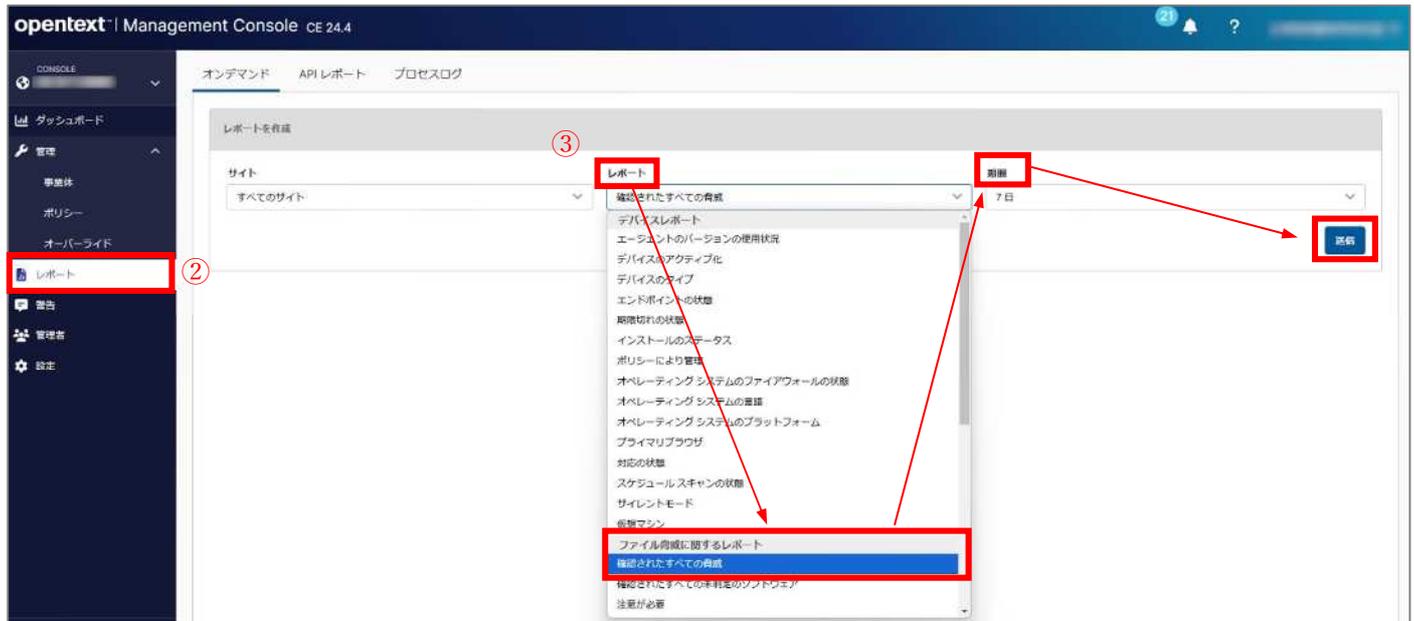
The screenshot shows the 'ファイルを復元' (Restore file) dialog box. At the top, it says 'ファイルを復元' (Restore file) and 'コマンドはデバイスに対してのみ実行できます。' (Commands can only be executed against the device). Below this, there are two input fields: 'ファイル名' (File name) and 'ファイルハッシュ' (File hash). The 'ファイル名' field contains the text 'WEBROOTTESTFILE.EXE'. At the bottom of the dialog, there are two buttons: 'キャンセル' (Cancel) and 'コマンドの送信' (Send command). A red circle with the number 8 is next to the 'コマンドの送信' button.

〈レポートからの手順〉

[レポート] では特定のレポートで脅威が検出されたエンドポイントの検索が可能です。この時ファイルの MD5 値はすでに特定されているため、オーバーライドをすばやく適用することができます。

- ① Web コンソールにログインします。
- ② [レポート]タブをクリックします。
- ③ レポートを作成 > レポート > [ファイル脅威に関するレポート]の中から[確認されたすべての脅威]を選択 > [期間]を指定 > [送信]をクリック > 画面の下半分にレポートが表示されます。

※脅威検知の数が多いとレポートが完成するまでに時間がかかる場合があります。



- ④ 許可したいファイル名の[このファイルをホワイトリストに記録する]をクリックします。



⑤ 許可オーバーライドの作成の種類で[MD5]を選択します。

ここでは MD5 は指定されている為、入力不要です。

(4) オーバーライド名を付けます。

(5) [ポリシーに関連付ける]…グローバルポリシーを含む特定のポリシーにオーバーライドを適用する場合はチェックを入れ、適用したいポリシーを選択します。

(6) [保存]をクリックします。

許可オーバーライドの作成

許可/ブロック

許可

ブロック

種類

フォルダ/ファイル

MD5

Webrootクラウド判定

MD5

クラウド判定

不正

名前 *

支援システム

ポリシーの関連付け

閉じる

保存

オーバーライド作成後、ファイルを元のフォルダ場所に戻します。

⑥ [このファイルを隔離先から復元する]をクリックします。

オンデマンド API レポート プロセスログ

レポートを作成

サイト: すべてのサイト

レポート: 確認されたすべての脅威

期間: 90日

送信

確認されたすべての脅威

CSV にエクスポート

ファイル名	パス名	マルウェアグループ	最終確認日時	デバイス名	サイト	アクション
WebrootTestFile.exe	\\Users\istechno\Downlo...	W32.Webroottestfile	12月 12 2024, 14:...	🗑️
WEBROOTTESTFILE.EXE	%temp%\c095e620-ed3...	W32.Webroottestfile	10月 10 2024, 16:...	🗑️ ↩️

⑦ [ファイルを復元]をクリックします。

ファイルを復元

i コマンドはデバイスに対してのみ実行できます。IPアドレスには使用できません。

ファイル名
WEBROOTTESTFILE.EXE

ファイルハッシュ
[ハッシュ値]

キャンセル ⑦ ファイルを復元

オーバーライドの作成と復元のコマンドを送信が完了したら下記の2つのコマンドも同時に送信します。

- ① [事業体] > [すべての事業体]をクリックします。
- ② 対象の端末をチェックします。
- ③ [エージェントコマンド] > [すべてのファイルとプロセスを再検証する]をクリックします。

The screenshot shows the 'opentext Management Console CE 24.4' interface. On the left sidebar, the '事業体' (Business Entity) menu item is highlighted with a red box and a circled '1'. In the main area, the '事業体' table has 'すべての事業体' (All Business Entities) selected with a red box and a circled '2'. Below this, the 'USER01' device is checked with a red box and a circled '2'. On the right, the 'エージェントコマンド' (Agent Command) dropdown menu is open, with 'すべてのファイルとプロセスを再...' (Verify all files and processes...) selected, highlighted with a red box and a circled '3'. Other commands like 'スキャン', 'クリーンアップ', and 'アンインストール' are also visible in the dropdown.

④ [コマンドの送信]をクリックします。

すべてのファイルとプロセスを再検証する
コマンドはデバイスに対してのみ実行できます。

次回のスキャン時に、選択したデバイスのローカルデータベースにあるコンテンツを再検証します。

キャンセル ④ コマンドの送信

⑤ 再び[エージェントコマンド] > [スキャン]をクリックします。



⑥ [コマンドの送信]をクリックします。



※管理コンソールから送られたコマンドをエンドポイントに反映するためには、ポリシーにて設定されてあるポーリング間隔をお待ちいただくか、エンドポイント上にてタスクトレイにあるウェブルートのアイコンを右クリックし、[設定のリフレッシュ]を選択すると、コンソールから送られたコマンドや変更が即座に反映されます。

以上で作業は完了です。