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。

④ [検出された脅威]の数字をクリックします。

⑤ [操作] ＞ [許可リストにファイルを追加]をクリックします。

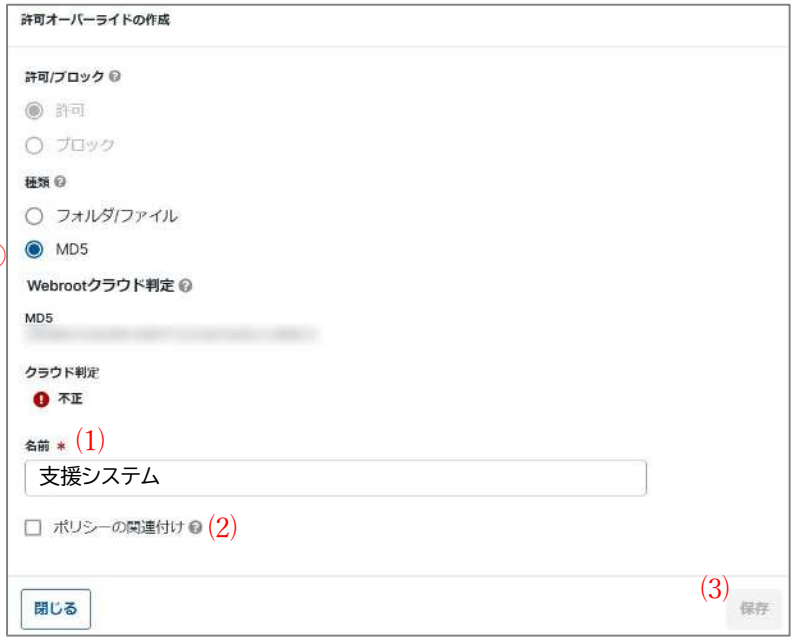
⑥ 許可オーバーライドの作成の種類で[MD5]を選択します。

ここでは MD5 は指定されている為、入力不要です。

⑴ オーバーライド名を付けます。

⑵ [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。

⑶ [保存]をクリックします。



⑦ [操作] ＞ [隔離先から復元]をクリックします。

⑧ [コマンドの送信]をクリックします。

〈レポートからの手順〉

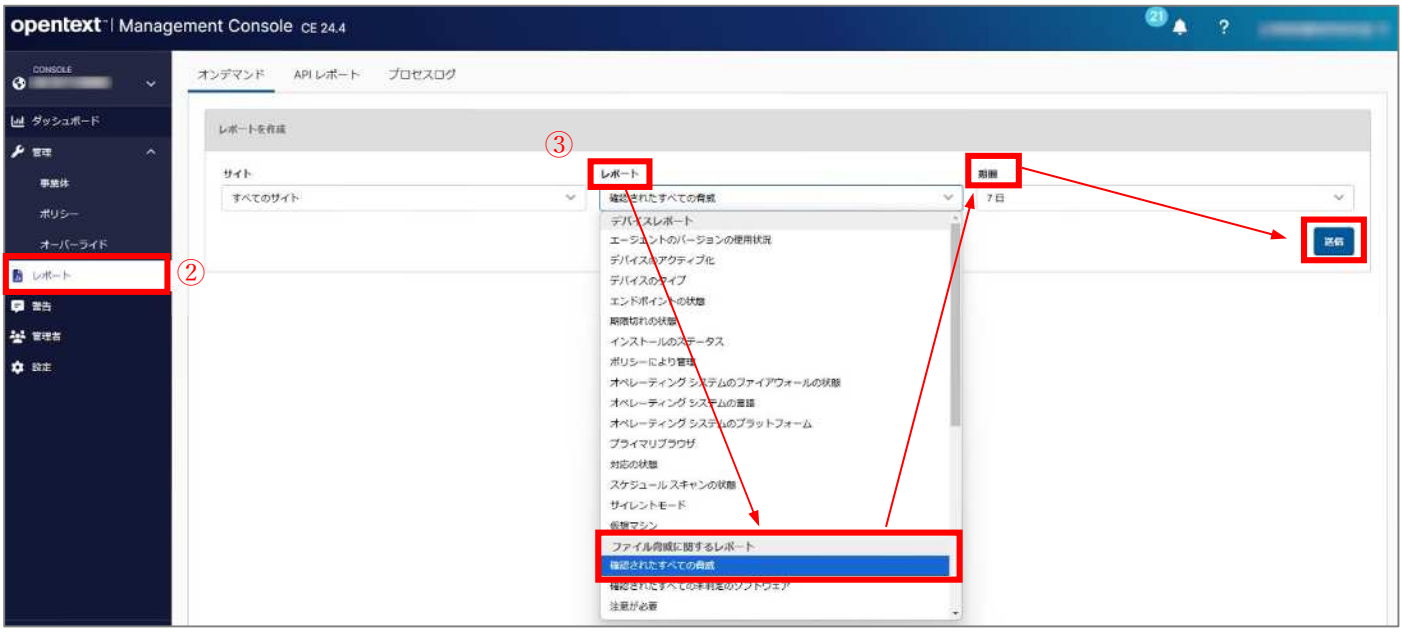
[レポート] では特定のレポートで脅威が検出されたエンドポイントの検索が可能です。この時ファイルの MD5 値はすでに特定されているため、オーバーライドをすばやく適用することができます。

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。

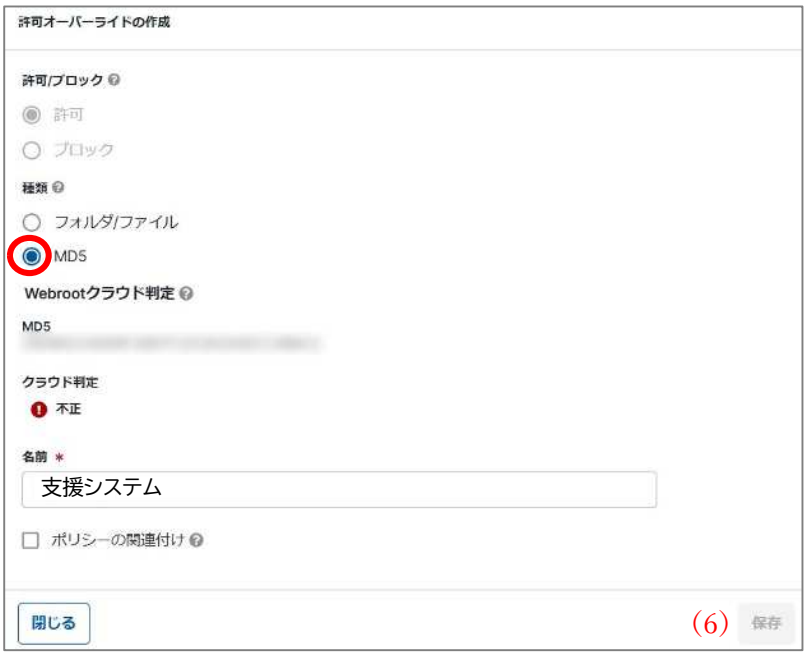
⑤　許可オーバーライドの作成の種類で[MD5]を選択します。

ここでは MD5 は指定されている為、入力不要です。

⑷　オーバーライド名を付けます。

⑸　[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。

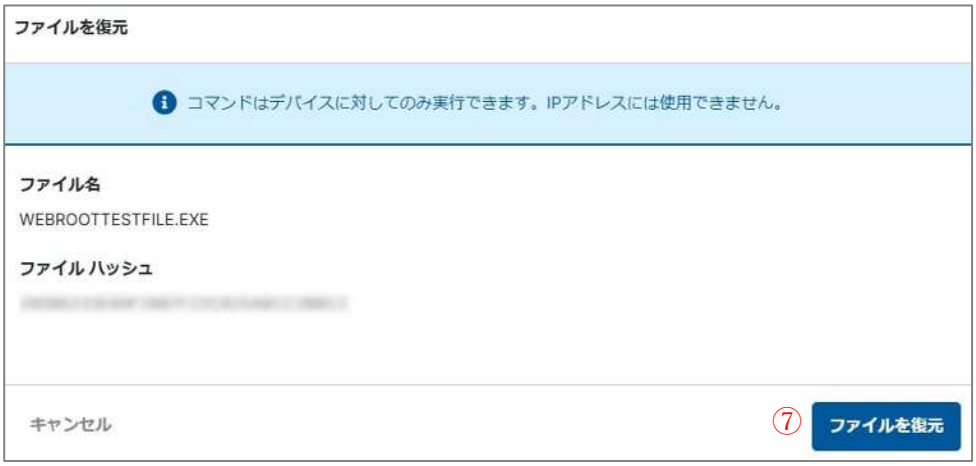
⑹　[保存]をクリックします。



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。

⑦ [ファイルを復元]をクリックします。



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。

④ [コマンドの送信]をクリックします。

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。