MR-EP　グレー判定のファイル/フォルダのオーバーライド手順

MR-EP は安全であるかマルウェアであるかを判定できないファイルを未判定（グレー判定）に分類します。グレー判定されたファイルはジャーナリング機能により常に監視・ログ記録される状態となりますが、ソフトウェアはそのまま使用できます。しかし稀にパフォーマンスに影響が出るケースがあります。その場合、「オーバーライド」を行いホワイトリストに登録します。
ファイル単位の他、関連フォルダ全体を一括でオーバーライドすることも可能です。
オーバーライドの方法はいくつかありますが、代表的な操作手順を説明します。

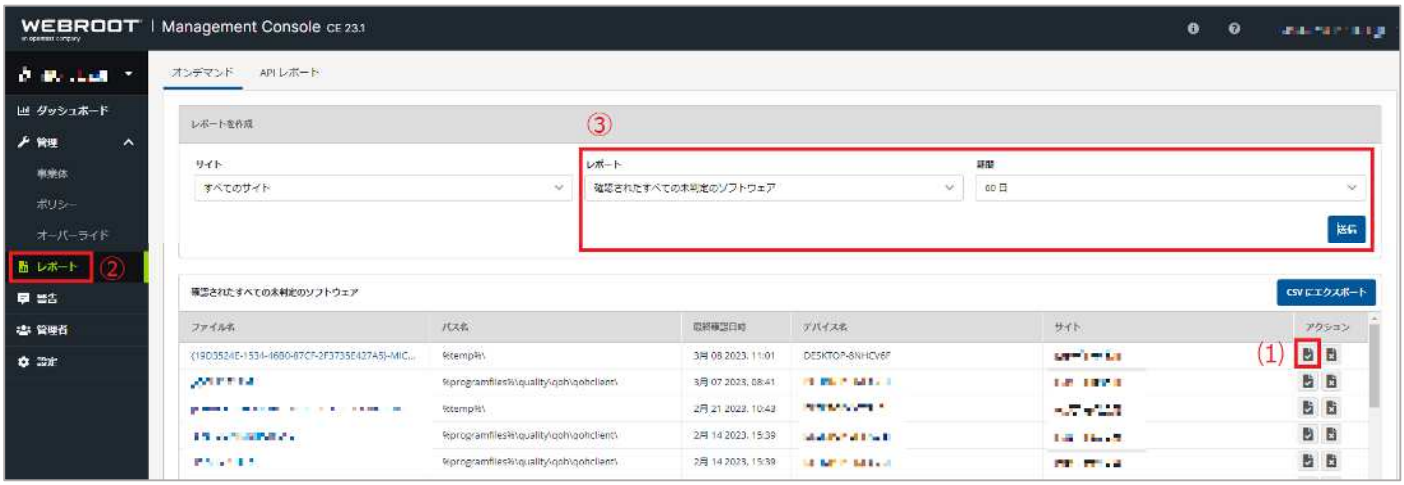
ファイル単位のオーバーライド手順

① 管理コンソールにログインします。
② [レポート]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未判定のソフトウェア]または[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント]を選択 ＞ [期間]を指定 ＞ [送信]をクリックします。

※未判定として検知された数が多いと、レポートの完成までに少し時間がかかる場合があります。

[確認されたすべての未判定のソフトウェア] の場合

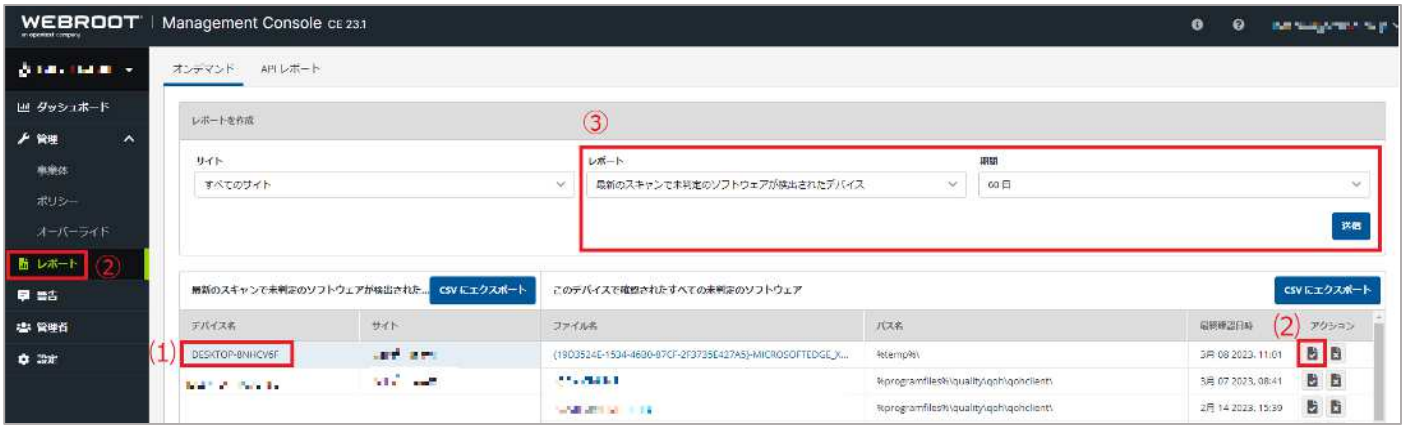
⑴　許可したいファイル名の[このファイルをホワイトリストに記録する]をクリックします。



[最新のスキャンで未判定のソフトウェアが検出されたデバイス]の場合

⑴　対象のデバイス名をクリックします。

⑵　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。



④　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。

⑤　[名前]…入力必須です。オーバーライド名を入力します。任意で分かりやすいものを設定しておきます。

※…[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ここでチェックを入れ、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。

以上でファイル単位のオーバーライドの作成は完了です。

フォルダ単位のオーバーライド手順

① 管理コンソールにログインします。

② [オーバーライド]をクリック ＞ [ファイルのオーバーライド]に変移します。

③ [オーバーライドを追加]をクリックします。

④ [許可/ブロック]で[許可]を選択します。

⑤ [種類]で[フォルダ/ファイル]を選択します。

⑥ [フォルダ]…フォルダパスを入力します。パス設定には環境変数が利用できます。

下記の例では c:¥Program Files にある基幹システムフォルダを指定しています。

⑦ [サブフォルダを含める]…対象フォルダ内のすべてのサブフォルダにオーバーライドを適用する場合に、このチェックボックスを選択します。

⑧ [悪意のある場合は検出]…選択または選択を解除します。

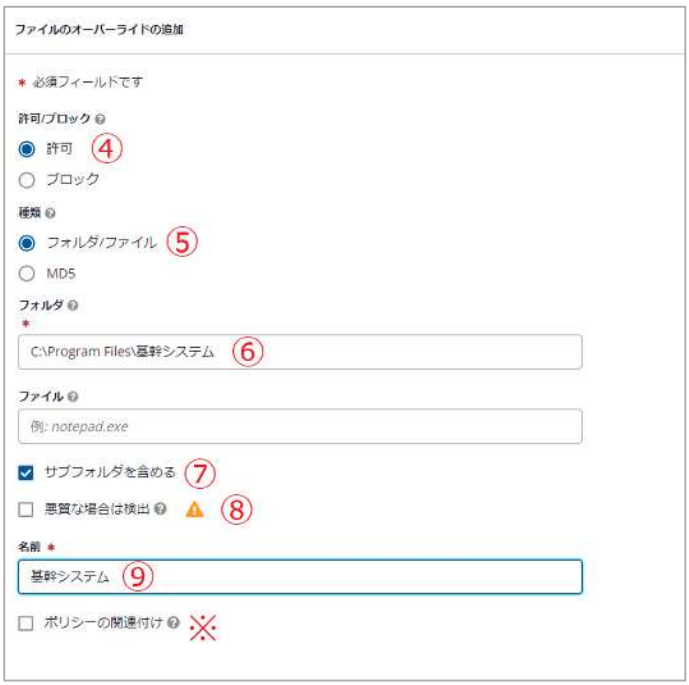
・選択する…監視とジャーナルは無効になりますが、エージェントはその場所で悪質なファイルの動作の確認を続けます。悪質なファイルが検出された場合は、ポリシーの設定に従って修正されます。

・選択を解除する…この場所のファイルは Webroot の保護なしで実行できるようになります。

⑨ [名前]…入力必須です。オーバーライド名を入力します。任意で分かりやすいものを設定しておきます。

※…[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ここでチェックを入れ、適用したいポリシーを選択します。

⑩ [保存]をクリックします。



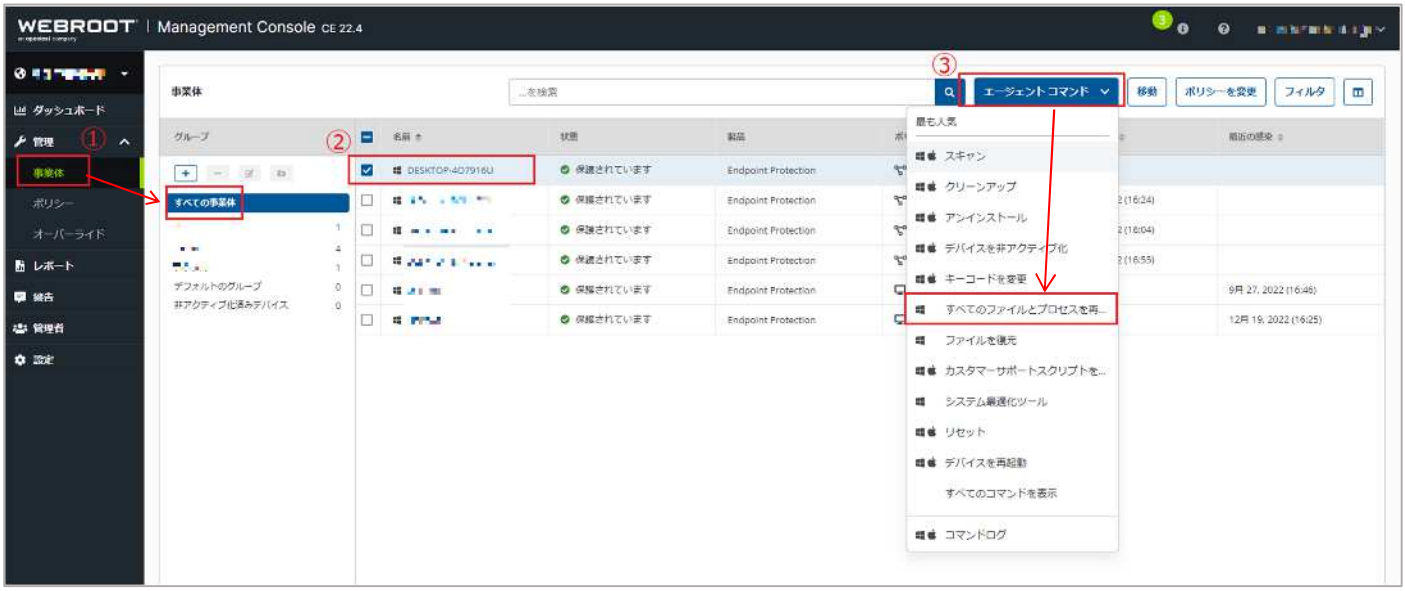
以上でフォルダ単位のオーバーライドの作成は完了です。

オーバーライドの作成後に下記の２つのコマンドを送信します。

① [事業体] ＞ [すべての事業体]をクリックします。

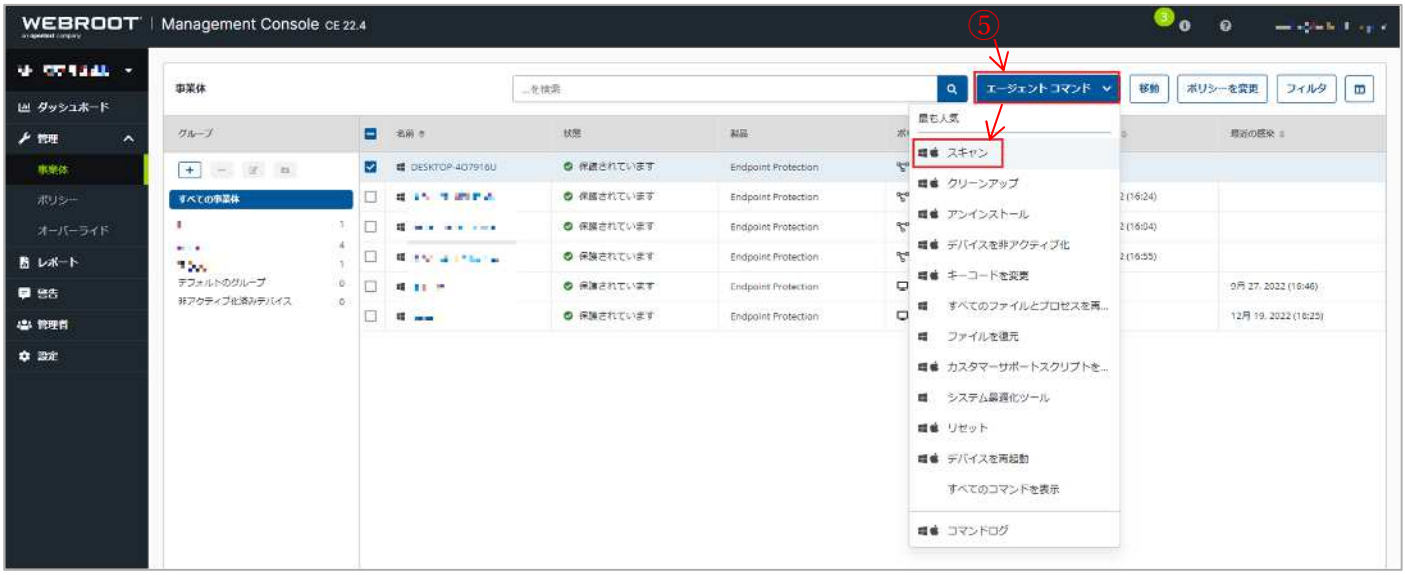
② 対象の端末をチェックします。

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。

※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。