

MR-EP ID シールドで特定のアプリケーションを許可する方法

ID シールドはキーロガーやスクリーングラバーなどの情報盗用技術から個人情報等のデータを保護する機能ですが、オンラインバンキングなど一部サービスで影響が出る場合があります。

その際は、ID シールドで保護されているアプリケーションを[許可]に変更します。

【エージェントコマンドでの許可】、【デバイス側での許可】の 2 つの方法があります。

【エージェントコマンドでの許可手順】

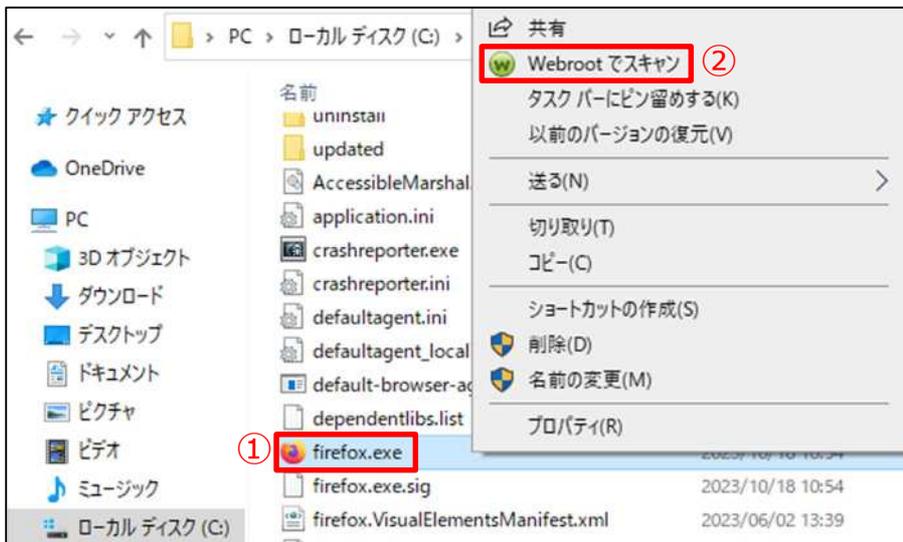
(1) MD5 の確認

許可したいアプリケーションの MD5 値を確認します。

① 許可したいアプリケーションの実行ファイルを右クリックします。

② [Webroot でスキャン]をクリックします。

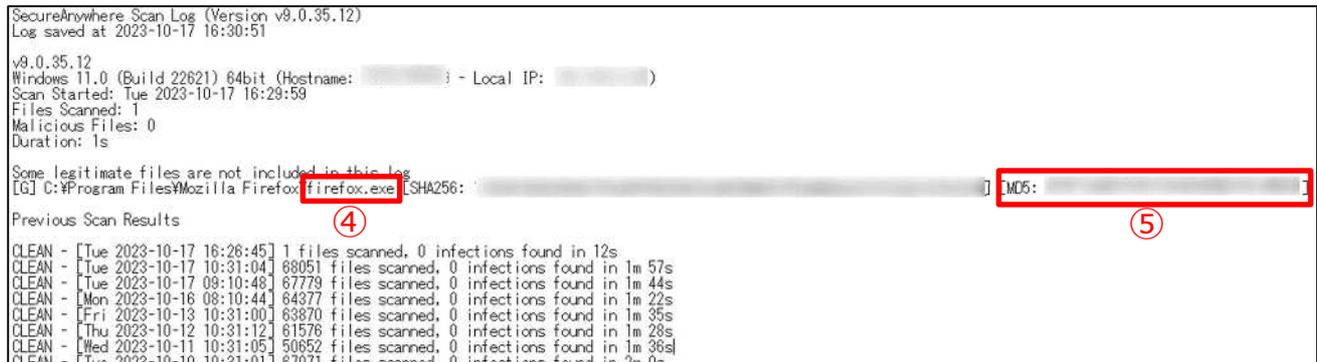
※Windows11 の場合は、右クリック後に[その他のオプションを確認]をクリックしてから、[Webroot でスキャン]をクリックします。



③ スキャンが終わったら[スキャンログの保存]をクリックして、任意の場所に保存します。

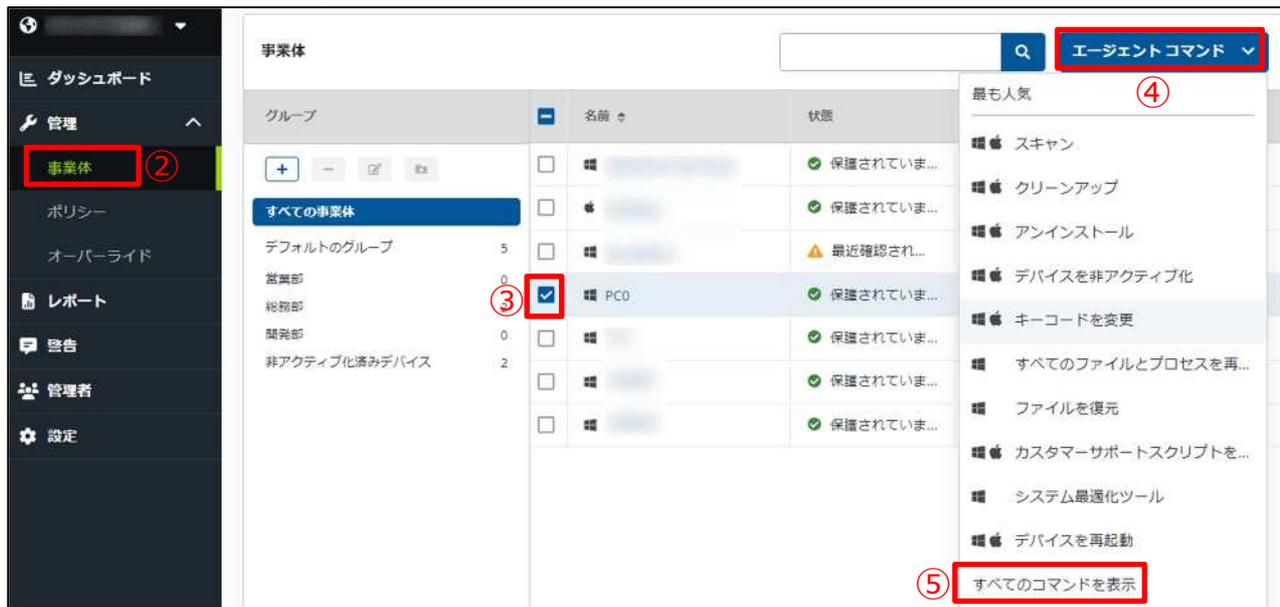


- ④ ログを開いて実行ファイルを検索します。
- ⑤ ファイル名の後に[MD5:xx]と表記があり、
こちらの 32 文字が MD5 となります。



(2) エージェントコマンドの送信

- ① Web コンソールにログインします。
- ② [事業体]をクリックします。
- ③ 許可するデバイスの[名前]の左側にチェックを入れます。
- ④ [エージェントコマンド]をクリックします。
- ⑤ [すべてのコマンドを表示]をクリックします。



⑥ [アプリケーションを許可]をクリックします。



⑦ 許可するアプリケーションの MD5 を入力します。

⑧ [コマンドの送信]をクリックします。

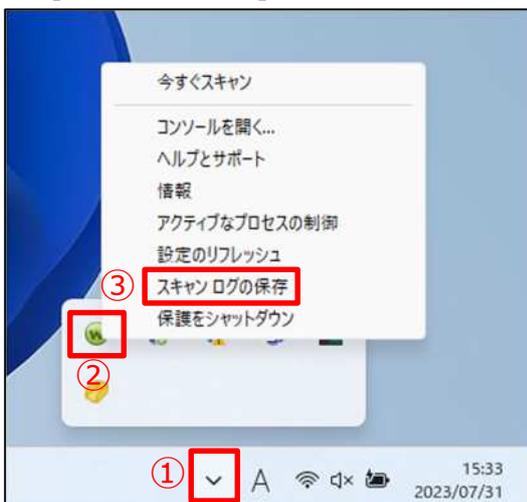


(3) 設定のリフレッシュ

デバイス側では定期ポーリングや再起動のタイミングで信号を受信します。

即時受信したい場合は以下の方法で信号を受信します。

- ① デスクトップ画面右下のタスクトレイをクリックします。
- ② Webroot アイコンを右クリックします。
- ③ [設定のリフレッシュ]をクリックします。

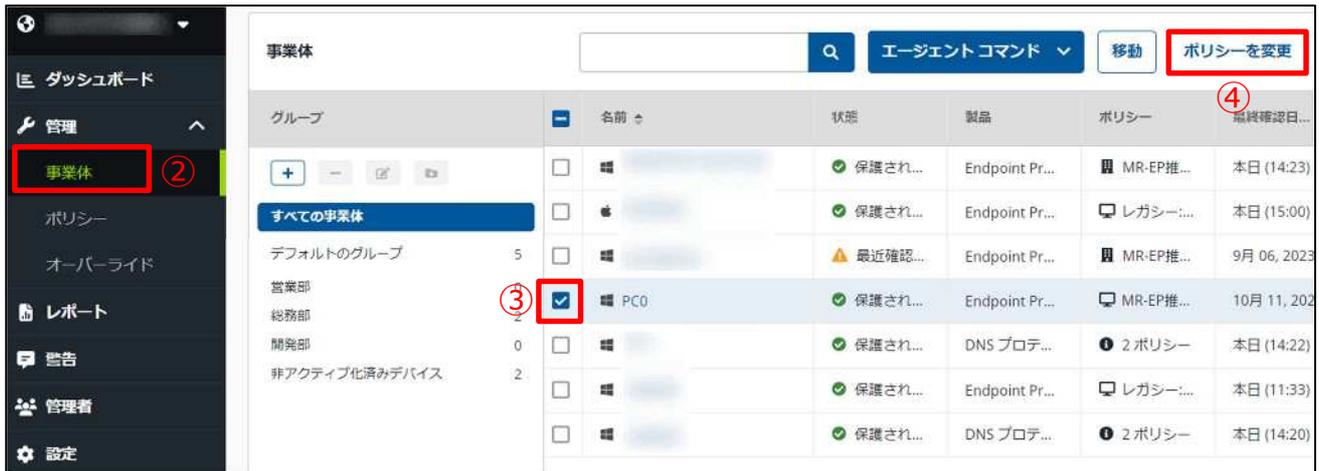


【デバイス側での許可手順】

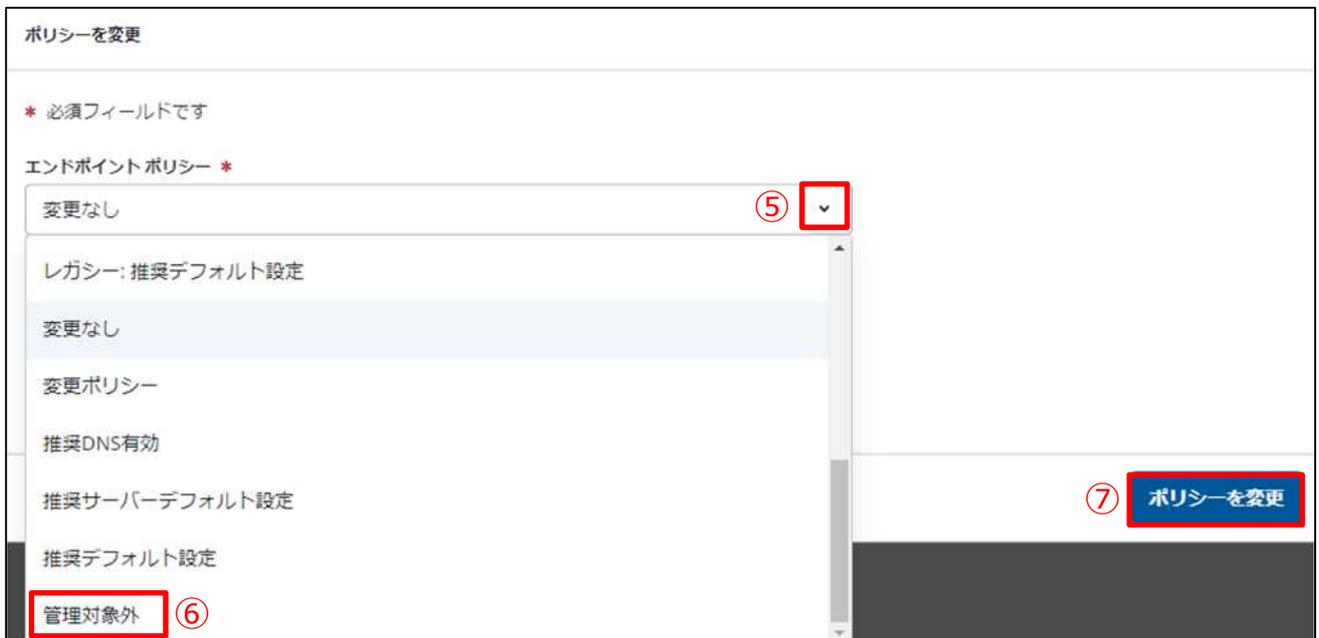
(1) ポリシーの変更

デバイス側で許可するには、ポリシーを[管理対象外]に変更します。

- ① Web コンソールにログインします。
- ② [事業体]をクリックします。
- ③ 許可するデバイスの[名前]の左側にチェックを入れます。
- ④ [ポリシーを変更]をクリックします。



- ⑤ プルダウンをクリックします。
- ⑥ [管理対象外]をクリックします。
- ⑦ [ポリシーを変更]をクリックします。



以上で[管理対象外]への変更は完了です。

※ポリシーをデバイスに即時適用するには設定のリフレッシュを行います。

手順については 3 ページの(3)設定のリフレッシュをご参照ください。

(2) アプリケーションの許可

- ① デスクトップ画面右下のタスクトレイをクリックします。
- ② Webroot アイコンをダブルクリックします。



- ③ [ID の保護]の横の歯車をクリックします。



- ④ [アプリケーション保護]をクリックします。
- ⑤ 許可するアプリケーションの[許可ボタン]をクリックします。



- ⑥ 表示されている文字を入力します。
- ⑦ [続行]をクリックします。



- ⑧ アプリケーションが許可された状態になります。

