



インストールマニュアル

第 1.3 版



S O M P O リスクマネジメント株式会社

目次

1.	はじめに	2
2.	動作環境	3
3.	SOMPO SHERIFF エージェントのインストール	4
4.	SOMPO SHERIFF エージェント ログ送信画面の表示.....	11
5.	FAQ.....	14

1. はじめに

この度は SOMPO SHERIFF をダウンロードしていただき誠にありがとうございます。SOMPO SHERIFF エージェントは、エンドポイントのフォレンジックデータ（揮発性データ）及び、ログデータを定期的に取り得し分析サーバに送信します。マルウェアや機密情報の漏えいといった不正な挙動を検知し、クライアント企業の管理者へ分析結果をレポートとして送信します。

2. 動作環境

本章では、SOMPO SHERIFF エージェントが動作する環境について以下に示します。

動作対象 OS

- Windows 10
- Windows 11

推奨動作環境

- ハードディスク：500M 以上の空き容量を推奨

その他ソフトウェア

- .NET Framework 4.x 系が導入済みであること

注意事項

- SOMPO SHERIFF エージェントを動作させる端末では、UAC（User Access Control）機能を無効にしないでください。

3. SOMPO SHERIFF エージェントのインストール

本章では、SOMPO SHERIFF エージェントのインストール手順を以下に示します。

- ◆ SOMPO SHERIFF エージェントは、Windows のシステム情報を取得するため、アンチウイルス製品で誤検出される可能性があります。インストールする前に、アンチウイルス製品の例外リストへ登録を実施してください。
 - ✓ アンチウイルス製品の例外リストに「C:\¥eiss」フォルダを追加してください。
例外リストの設定方法は、各種アンチウイルス製品のホームページを参照してください。

- ① SOMPO SHERIFF のお申込み後に、SOMPO SHERIFF ダウンロードサイト
[<https://site.somposheriff.com/login>]にログインするためのアカウント情報をご案内します。

その情報をもとに SOMPO SHERIFF ダウンロードサイトにログインしてください。

- ✓ アカウント情報：
サイト ID … CIXXXXXXXXX
パスワード … 8 文字の半角英数記号文字列



図 1 ダウンロードサイトログインページ

② 図 2 に示す赤枠で囲った「ダウンロード」ボタンをクリックし、インストーラをダウンロードしてください。



図 2 インストーラのダウンロード

※PC やブラウザによっては、下記の警告が表示されますが、問題ございませんので、そのままダウンロードください。

以下、Google Chrome の場合

(1) 「^」をクリックします。



(2) 「継続」をクリックします。



以下、Microsoft Edge の場合

(1) 三点リーダー「…」をクリックします。



(2) 再び三点リーダーが表示されるので「…」をクリックします。



(3) 「保存」をクリックします。



(4) 「詳細表示」をクリックします。



(5) 「保存する」をクリックします。



- ③ SOMPO SHERIFF ダウンロードサイトからダウンロードした「CIXXXXXX_eiss_install.zip」を Zip 解凍ツール等で解凍してください。

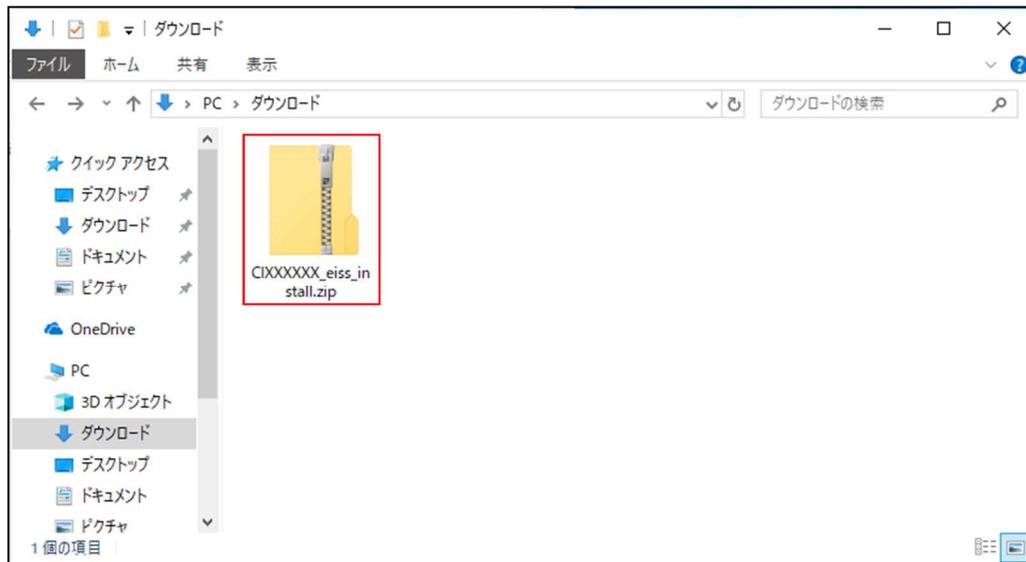


図 3 CIXXXXXX_eiss_install.zip

- ④ Zip ファイルの解凍後、解凍したフォルダ内の「EissAgentInstall.exe」を実行してください。
- ✓ インストールを行う際は、必ずインターネットに接続していることを確認してください。

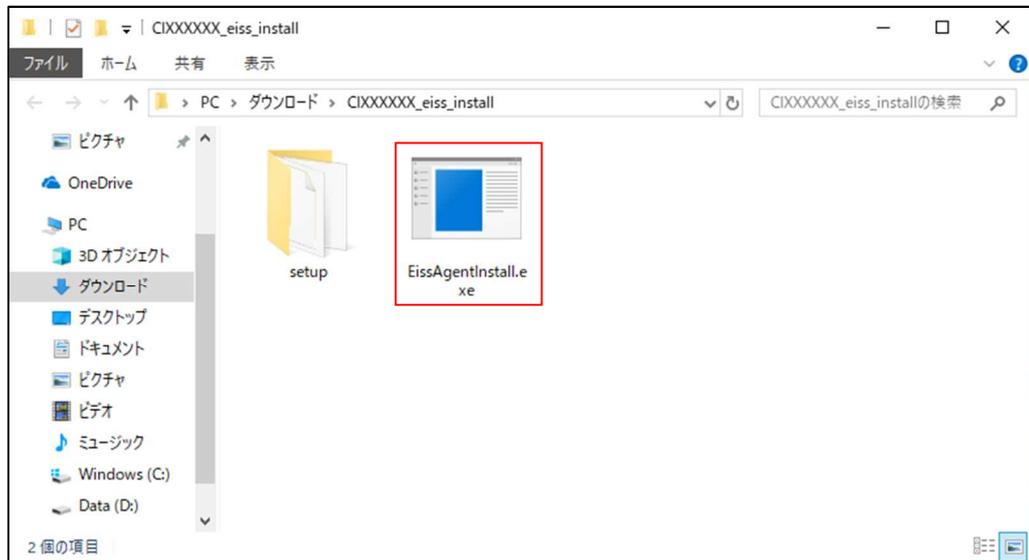
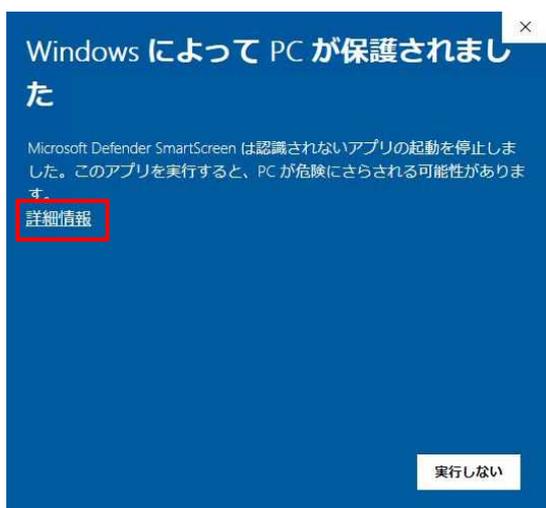


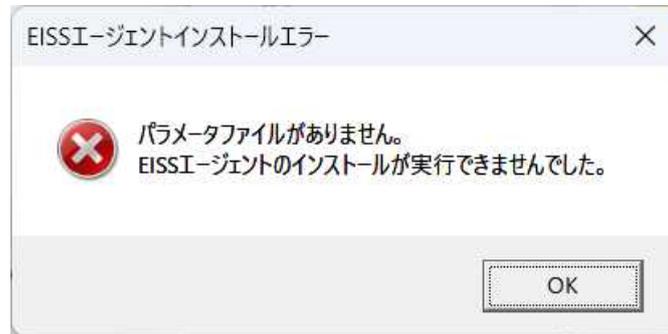
図 4 インストーラの実行

※「setup」フォルダ内のファイルは実行しないでください。

※端末によりインストーラを実行した際に、Microsoft Defender SmartScreen の確認画面が表示されることがあります。確認画面が表示された場合、「詳細情報」を選択した後、「実行」をクリックしてください。



※ダウンロードした Zip ファイルを解凍しないでインストーラを実行した場合、下記のエラーメッセージが表示される場合があります。



エラーメッセージが表示された場合、手順③で Zip ファイルの解凍後、解凍したフォルダ内の「EissAgentInstall.exe」を実行してください。

- ⑤ インストーラの実行後、図 5 に示すセットアップ完了ウィンドウが表示されます。「Close」ボタンをクリックし、ウィンドウを閉じてください。

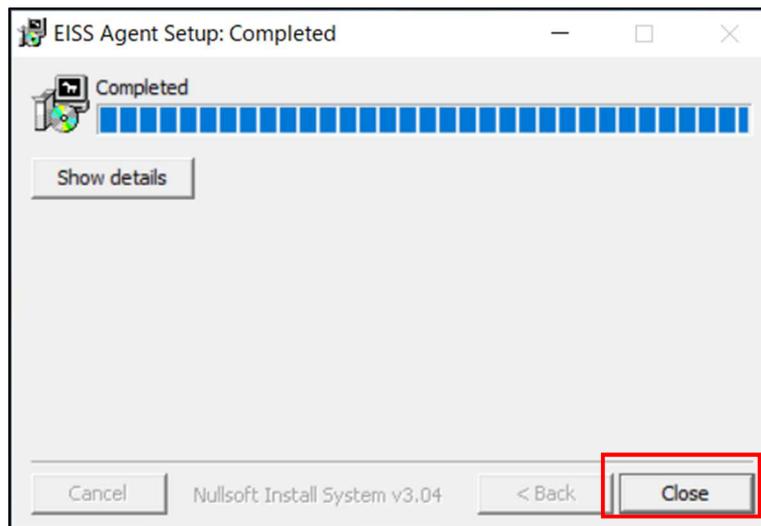


図 5 セットアップ完了ウィンドウ

- ⑥ セットアップ完了ウィンドウを閉じた後、ユーザーアカウント制御（UAC）のダイアログボックス画面が表示されますので、「はい」を選択してください。

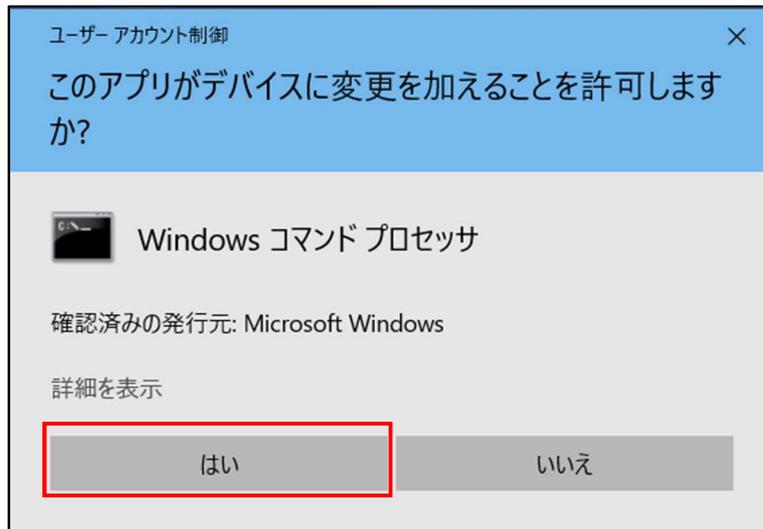


図 6 UAC ダイアログボックス

- ⑦ SOMPO SHERIFF エージェントのインストールが正常に終了した場合、図 7 に示すようなウィンドウが表示されます。「OK」ボタンをクリックしウィンドウを閉じてください。

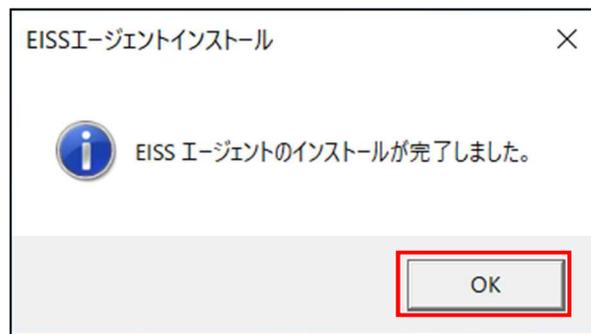


図 7 インストール完了ウィンドウ

4. SOMPO SHERIFF エージェント ログ送信画面の表示

本章では、SOMPO SHERIFF エージェントのログ送信画面の内容を以下に示します。

◆ 初回のログ送信について

SOMPO SHERIFF エージェントのインストールが正常に完了すると、ログ送信が行われますが、端末によってログ送信の間隔が異なり、反映に時間を要します。

インストール直後は 1 時間程 PC 端末を起動したままとして、時間を置いてご確認ください。

- ① デスクトップ右下のタスクバーから下図のアイコンをダブルクリックしてください。

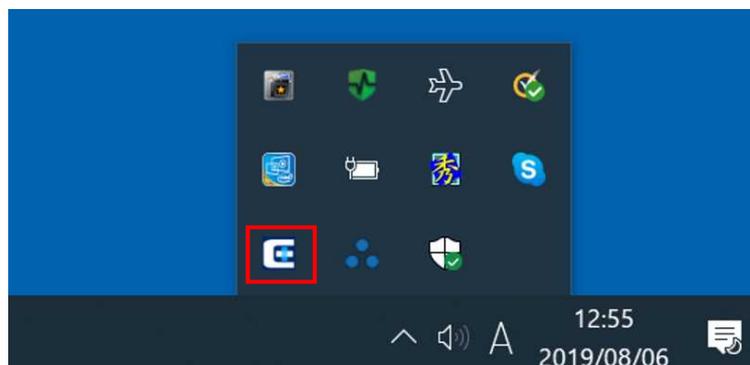


図 8 デスクトップのアイコン

※タスクバーにアイコンが表示されない場合、エクスプローラーを開き、「C:\%eiss%agent%app%bin」フォルダに遷移し、「LogTransmissionStatus.exe」をダブルクリックして実行してください。

- ② ダブルクリック後、SOMPO SHERIFF エージェントのログ送信画面が表示されます。
下図赤枠内のメッセージ欄でログが正常に送信されたか確認できます。

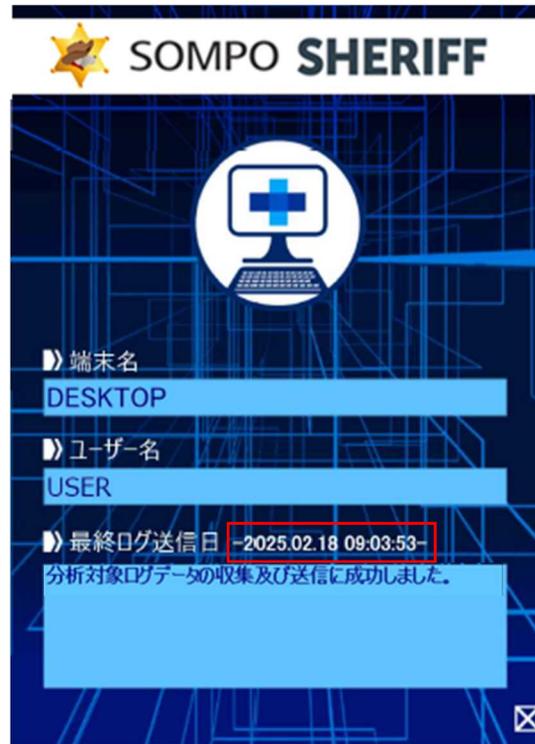


図 9 ログ送信画面

エラーが発生した場合、下図赤枠内のメッセージ欄で詳細が確認できます。



「最終ログ送信日」右の赤枠内で最終ログ送信日が確認できます。



◆ ログ分析結果の確認について

SOMPO SHERIFF は、1 週間に一回ログ分析結果をレポートで送付いたします（管理者メールアドレス宛）

分析レポートにて、確認が必要なアラートを検知した場合は、アラート詳細を管理画面よりご確認ください。

なお、管理画面の確認方法は「管理画面マニュアル」をご参照ください。

■ 管理画面マニュアル

https://www.sompocybersecurity.com/dcms_media/other/somposheriffadmin_manual_02.pdf

5. FAQ

本章では、SOMPO SHERIFF エージェントに関するよくある質問について以下に示します。

SOMPO SHERIFF に関するよくある質問は下記に集約しましたので下記 URL よりご確認ください。

- SOMPO SHERIFF インストール QA
https://www.sompocybersecurity.com/dcms_media/other/sheriffInstall_QA.pdf
- SOMPO SHERIFF QA（運用全般含む）
https://www.sompocybersecurity.com/service/smb/sheriff/sheriff_qa.html

SOMPO SHERIFF お問い合わせフォーム：

ご不明点・ご質問は、下記お問い合わせフォームよりお問い合わせください。

対応時間：9:00～17:00(土日祝を除く)

<https://srm.sompocybersecurity.com/lp/sheriff/contact/index.php>

SOMPOリスクマネジメント株式会社