

# インストールマニュアル

第1.3版



Copyright © 2022, Sompo Risk Management Inc. All Rights Reserved.



# 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。
- 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 ・・・ CIXXXXXXXX

パスワード・・・8 文字の半角英数記号文字列

SOMPO SHERIFF ダウンロード Sompo Risk Management Inc.

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。

サンプル様	3
SOMPO SHERIFF Agent SOMPO SHERIFF エージェントダウン	/ロード
対応パージョン	Windows 10 Windows 11
ダウンロード	9050-F 🛓
器定方法	SOMPO SHERIFFインストールマニュアル 🖸 SOMPO SHERIFFアンインストールマニュアル 🖸
22.83.9448	SOMPO SHERIFFエージェント動作条件 ・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。 ・Windows 64bit数が対象です。Windows 32bit数は対象外となります。

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。

SOMPO SHERIFF Agent		
OMPO SHERIFF エージュ	ントダウンロード	
州応バージョン	Windows 10 Windows 11	
ダウンロード	9000-K 🛎	
设定方法	SOMPO SHERIFFインストールマニュアル 「D SOMPO SHERIFFアンインストールマニュアル 「D	

(2)「継続」をクリックします。

ナンブル 様		Ξ
SOMPO SHERIFF Agent		
SOMPO SHERIFF エージェントダウン	-D-K	
見聞バージョン	Windows 10 Windows 11	
90>0-K	905a - P ±	
設定が法	50MP0 5HERFFインストールマニュアル 10 50MP0 5HERFFプンインストールマニュアル 10	
2070	5 他式 トージェント総合条件 デエージェントや設合させる国家では、UAC(User Access Control 相談や激気にしないてください。 がお用いたのかっ22ml気は分野からなり3.4、	
C11900 _eiss_inst	v l C1190083, wiss, jnstzip	-



### 以下、Microsoft Edge の場合

(1) 三点リーダー「…」をクリックします。

サンプル様			
SOMPO SHERIFF Agent SOMPO SHERIFF エージェントダウン	/□- K		
対応バージョン	Vindows 10 Vindows 11		
ダウンロード	9930-F 🛓		
設定方法	SOMPO SHERFFインストールマニュアル D SOMPO SHERFFアンインストールマニュアル D		
注意事项	SOMPO SHERFエージェント動作事件 - SOMPO SHERFエージェント動作者性を出る地帯では、UAC(User Access Control)相応を開設にしないでください。 - Windows Gabully計画です。Windows SZbMEA1開始となります。		

### (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。

サンプル様	ダウンロード C Q … 公 (122ess_matal.pgl==級的にダウン 由 …		
	CO2exis_initial.zipEBV(R)CL_BF	Ξ	
SOMPO SHERIFF Agent			
SOMPO SHERIFF エージェン	トダウンロード		
対応バージョン	Windows 10 Windows 11		
ダウンロード	90xa-F 🛓		
設定方法	SOMPO SHERIFFインストールマニュアル		
注意事項 2004の9480時でエジェント執行者です。UKD (New Access Control) 機能を無効にしないでください、 ・90400964057エジェントを動作させる施までは、UKD (New Access Control) 機能を無効にしないでください、 ・Windows 6430回が対象です。Windows 32040回は30条かとなります。			

### (3)「保存」をクリックします。

		ダウンロード	Ľ Q … ♪	
サンプル様		CI22 .eiss_inst CI22 eiss inst	all.zipは一般的にダウン ① … all.zipを聞く的に、信用	Ð
SOMPO SHERIFF Agent		(保有 (20)	*	
SOMPO SHERIFF エージェン	ットダウンロード 	17.6	情報	
対応パージョン	Windows 10 Windows 11	G 17	>ロードリンクのコピー	
	99>0-F 🛎			
即走方法	SOMPO SHERIFFインストールマニュアル ロ SOMPO SHERIFFアンインストールマニュアル	SOMPO SHERFFインストールマニュアル <sup>1</sup> SOMPO SHERFFアンインストールマニュアル <sup>1</sup>		
注意車項	SOMPO SHERIFFエージェント動作条件 - SOMPO SHERIFFエージェントを動作させる端末では、UAC(User Access Control)機能 - Windows 64bit版が対象です、Windows 32bit版は対象外とよります。	SOMPO SHERFFエージェント動作条件 ・SOMPO SHERFFエージェントを動作させる場米では、UAC(User Access Control)機能を開始にしないでください。 ・Windows defability制度です。Manoos Szbatkist制作かとなります。		

### (4)「詳細表示」をクリックします。

サンプル様		▲ CI22 _eiss_install.zipを開 く前に、信頼できることを確認し てください
SOMPO SHERIFF Agent		このファイルは一般的にダウンロードされていない ため、Microsoft Defender SmartScreen はこ のフォイル・ポッチャンドから第日アスキャル 2月
SOMPO SHERIFF エージ	ェントダウンロード	しのアールの支払のこのを通知としている た。がウンゴードしているファイルまたはそのソースが 信頼できることを確認してから、ファイルを開いて くだねい。
対応バージョン	Windows 10 Windows 11	名前: Cl22eiss_install.zip 発行元:不明
ダウンロード	<i>ダ</i> ウンロード 👤	詳細表示 🗸
認定方法	SOMPO SHERIFFインストールマニュアル 「 SOMPO SHERIFFアンインストールマニュアル 「	前はキャンセル
注意事项	SOMPO SHERIFFエージェント動作条件 ・ SOMPO SHERIFFエージェント動作条件 ・ SOMPO SHERIFFエージェントを動作させる端末では、UAC(User Acc ・ Windows 64bit版が対象です。Windows 32bit版は対象外となります。	cess Control)機能を無効にしないでください。



(5)「保存する」をクリックします。

サンプル様	1	▲ Cl22eiss_install.zipを開 く前に、信頼できることを確認し てください	Ξ
SOMPO SHERIFF Agent		このファイルは一般的にダウンロードされていない ため、Microsoft Defender SmartScreen はこ のファイルがGene Vうかた地球型のませょう	
SOMPO SHERIFF エージェ	ントダウンロード	た。ダウンロードしているファイルまたはそのソースが 信頼できることを確認してから、ファイルを開いて ください。	
対応パージョン	Windows 10 Windows 11	名前: Cl22eiss_install.zip 発行完 不明	
ダウンロード	<u>ダウンロ</u> −ド 🛓	表示数を減らす へ	
設定方法	SOMPO SHERIFFインストールマニュアル	保持する このアプリは安全であることを報告する	
注意事项	SOMPO SHERIFエージェント動作条件 - SOMPO SHERIFエージェントを動作させる確実では、UAC (User Access Control) 機能 - Windows 64b能防分像です。Windows 32b批版は対象外となります。	詳細情報 削除 キャンセル	

 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 CIXXXXX\_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。

I I I I I I I I I I I I I I I I I I I						
ファイル ホーム 共有	有 表示					~ 🕜
	PC » ダウンロード » CIXXX	XXX_eiss_install	√ Č	CIXXXXXX_eiss_ins	tallの検索	Q
📰 ピクチャ 🛛 🖈	^					
la OneDrive						
S PC						
🧊 3D オブジェクト		<b>F A B B</b>				
🖊 ダウンロード	setup	EissAgentinstall.e xe				
📃 デスクトップ		49.62				
ドキュメント						
📰 ピクチャ						
📕 ビデオ						
♪ ミュージック						
Windows (C:)						
Data (D:)	~					
2 個の項目						

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。

Windows によって PC が保護されまし	Windows によって PC が保護されまし
た	た
Microsoft Defender SmartScreen は認識されないアプリの起動を停止しま した。このアプリを実行すると、PC が危険にさらされる可能性がありま す。 詳細情報	Microsoft Defender SmartScreen は認識されないアプリの起動を停止しま した。このアプリを実行すると、PC が危険にさらされる可能性がありま す。 アプリ: EissAgentInstall.exe 発行元: SECURE INNOVATION, K.K. 実行 実行しない



※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。

LIDDT		i.
8	パラメータファイルがありません。	
	EISSエージェントのインストールが実行で	きませんでした。
		1
		ОК

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。

🛃 EISS Agent Setup: Completed	-		$\times$
Completed			
Show details			
Cancel Nullsoft Install System v3.04	< Back	Clo	se

### 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)のダイヤ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。

ューザー アカウント制御 このアプリがデバイスに変更 か?	× を加えることを許可します
<b>Windows</b> コマンドプロ 確認済みの発行元: Microsoft Wind	コセッサ dows
詳細を表示	
はい	いいえ

図 6 UAC ダイヤログボックス

 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、時間をお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。



Sompo <b>Sheriff</b>
》端末名 DESKTOP
<ul> <li>&gt;&gt; ユーザー名</li> <li>USER</li> <li>&gt;</li></ul>
7 時代は、ログラム16111-2020/02-18-05/05/33 分析対象ログデータの収集及び送信に成功しました。

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いただけます。

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)
   <a href="https://www.sompocybersecurity.com/service/smb/sheriff/sheriff\_qa.html">https://www.sompocybersecurity.com/service/smb/sheriff/sheriff\_qa.html</a>

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

CS2400006