



管理画面マニュアル (企業管理者向け)

第 1.5 版



SOMPOリスクマネジメント株式会社

目次

1.	はじめに	2
2.	ログイン	3
3.	管理画面の説明	4
①	ダッシュボード トップページとなる画面です。最新の分析状況が表示されます。	4
②	設定情報	4
③	端末情報	5
④	分析レポート管理	7
⑤	セキュリティ対策状況	12
4.	分析レポートの見方	16
5.	機能設定	18
①	MAC アドレスのホワイト登録	18
②	USB 利用制限およびネットワーク接続先制限の設定	20
③	IP アドレス制限の設定	23

1. はじめに

この度は SOMPO SHERIFF をダウンロードいただき誠にありがとうございます。本マニュアルでは、SOMPO SHERIFF の管理画面について説明いたします。

✓管理画面を閲覧する際は、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。

2. ログイン

SOMPO SHERIFF 管理画面情報を基に SOMPO SHERIFF 管理画面にアクセスしてください。

SOMPO SHERIFF 管理画面 URL	https://www.somposheriff.com/login
企業 ID	CIXXXXXXXX
メールアドレス	管理者メールアドレス
パスワード	12 文字の半角英数記号文字列



図 1 SOMPO SHERIFF 管理画面

トップページとなる画面です。最新の分析状況が表示されます。



ご契約時に頂いた情報が表示されます。



②-2 登録ユーザー

SOMPO SHERIFF 管理画面を閲覧できるユーザー(管理者)が登録されています。

管理画面を閲覧できるユーザー(管理者)は各企業 1 名です。



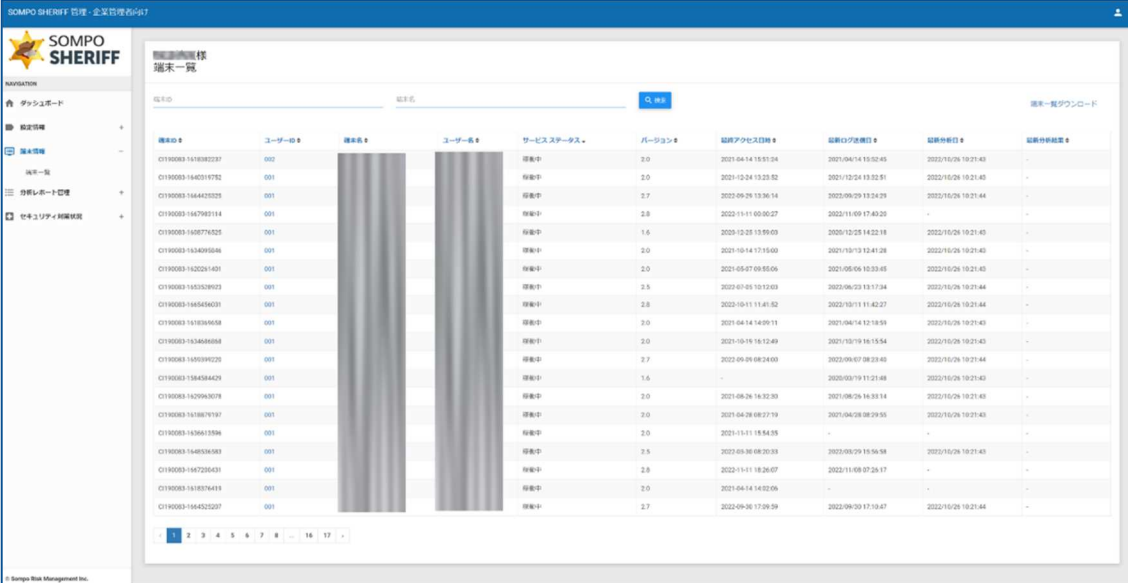
No	姓	名	メールアドレス	編集
1				
2				
3				

図 4 ユーザー一覧画面

③ 端末情報

③-1 端末一覧

SOMPO SHERIFF エージェントをインストールした端末の情報が確認できます。



端末ID	ユーザーID	端末名	ユーザー名	サービスステータス	バージョン	最終アクセス日時	最終ログ送信日時	最終検出日時	最終検出結果
C11R003-1318182237	002			稼働中	2.0	2021-04-14 15:51:24	2021-04-14 15:52:45	2022-10-26 19:21:43	-
C11R003-1340314782	001			稼働中	2.0	2021-12-24 13:25:52	2021-12-24 13:25:51	2022-10-26 19:21:43	-
C11R003-1344272325	001			稼働中	2.7	2022-09-29 13:36:14	2022-09-29 13:34:29	2022-10-26 19:21:44	-
C11R003-134792114	001			稼働中	2.8	2022-11-11 00:00:27	2022-11-09 17:42:29	-	-
C11R003-1328774225	001			稼働中	1.6	2023-12-25 13:59:03	2023-12-25 14:22:18	2022-10-26 19:21:43	-
C11R003-1324091046	001			稼働中	2.0	2021-10-14 17:19:00	2021-10-13 12:41:28	2022-10-26 19:21:43	-
C11R003-1322261401	001			稼働中	2.0	2021-05-07 09:55:06	2021-05-06 10:33:45	2022-10-26 19:21:43	-
C11R003-1323291023	001			稼働中	2.5	2021-07-05 10:12:03	2022-06-23 13:17:34	2022-10-26 19:21:44	-
C11R003-1345454031	001			稼働中	2.8	2022-10-11 11:41:52	2022-10-11 11:42:27	2022-10-26 19:21:43	-
C11R003-1313034058	001			稼働中	2.0	2021-04-14 14:00:11	2021-04-14 12:19:59	2022-10-26 19:21:43	-
C11R003-1314040058	001			稼働中	2.0	2021-10-16 19:12:49	2021-10-16 16:15:54	2022-10-26 19:21:43	-
C11R003-1303191220	001			稼働中	2.7	2022-09-05 08:24:00	2022-09-07 08:29:40	2022-10-26 19:21:44	-
C11R003-1334454429	001			稼働中	1.6	-	2020-03-19 11:21:49	2022-10-26 19:21:43	-
C11R003-1322993079	001			稼働中	2.0	2021-08-26 16:32:30	2021-08-26 16:33:14	2022-10-26 19:21:43	-
C11R003-1313879197	001			稼働中	2.0	2021-04-28 08:27:19	2021-04-28 08:29:55	2022-10-26 19:21:43	-
C11R003-1336613394	001			稼働中	2.0	2021-11-11 15:54:35	-	-	-
C11R003-1345353083	001			稼働中	2.5	2022-05-30 08:20:33	2022-05-29 15:56:58	2022-10-26 19:21:43	-
C11R003-1367220431	001			稼働中	2.8	2022-11-11 18:26:07	2022-11-09 07:26:17	-	-
C11R003-1318274419	001			稼働中	2.0	2021-04-14 14:02:06	-	-	-
C11R003-1344222237	001			稼働中	2.7	2022-09-30 17:29:39	2022-09-30 17:10:47	2022-10-26 19:21:44	-

図 5 端末一覧画面

EISS 端末 ID	端末と紐づく SOMPO SHERIFF エージェントの ID が表示されます。
ユーザーID	端末のユーザー毎に採番される ID が表示されます。 端末に複数ユーザーがいる場合は「002」「003」と追加されます。 クリックでき、端末の情報が確認できます。 ※【③-1-1 端末情報】画面へ遷移
端末名	SOMPO SHERIFF エージェントをインストールした端末名が表示されます。 ※端末名は PC のデバイス名となります。

	<p>※端末名が変更された場合、管理画面では自動で更新されません。</p> <p>端末名を変更した場合は、下部に記載の問い合わせフォームよりご連絡をお願いします。</p> <p>※画面右上の「端末一覧ダウンロード」から端末の一覧がダウンロードできます。</p>
ユーザー名	端末のユーザーアカウント名が表示されます。
サービスステータス	<p>端末のステータスが確認できます。</p> <p>※アンインストールを行った端末は「アンインストール」と表示されます。</p>
バージョン	SOMPO SHERIFF エージェントのバージョン番号が表示されます。
最終アクセス日時	端末が直近で起動した日時（SOMPO SHERIFF エージェントが直近で起動された日時）
最新ログ送信日	端末がログを送信した日時
最新分析日	<p>端末がログを分析した日時</p> <p>※通常であれば翌日が分析日となります。</p>
最新分析結果	<p>端末の最新分析結果が表示されます。</p> <p>「-」で表示される場合は、セキュリティリスクはみられません。</p>

③-1-1 端末一覧（詳細情報）

「ユーザーID」を押下すると端末の詳細情報が表示されます。MAC アドレス、OS 名、ユーザー権限、ログ受信時間などもこちらで確認できます。

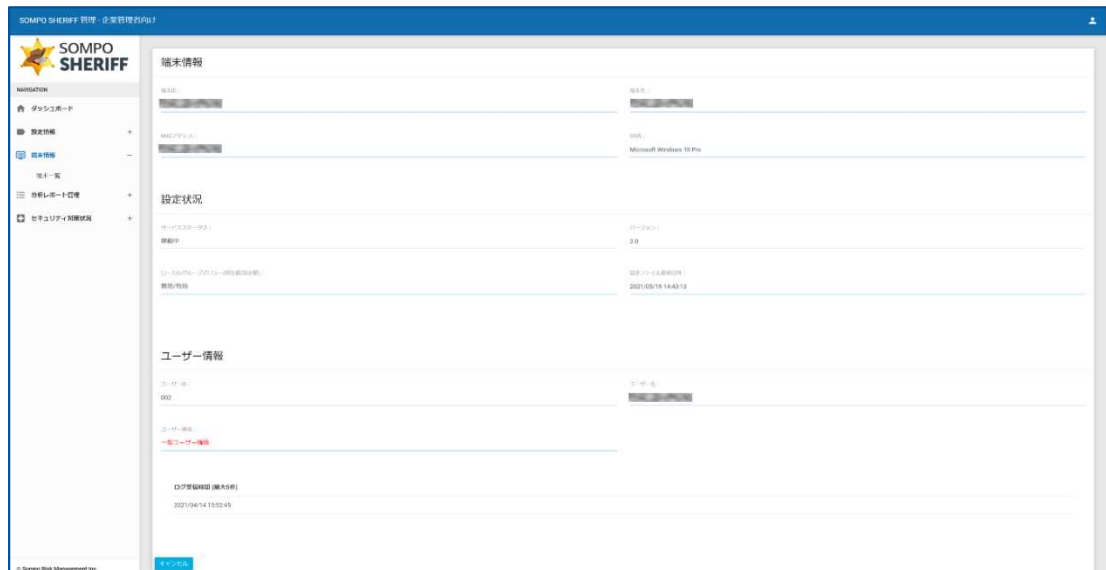


図 6 端末情報画面

④ 分析レポート管理

④-1 レポート一覧

週次でお送りしている分析レポートの内容が確認できます。

SOMPO SHERIFF 管理 - 企業管理画面

SOMPO SHERIFF

NAVIGATION

ダッシュボード

設定情報

基本情報

分析レポート一覧

レポート一覧

通知設定

セキュリティ対策状況

分析レポート一覧

分析レポート一覧

レポートID

報告日

分析対象期間

ログ送信期間

警告利用端末数

ログ送信ユーザー数

分析結果

分析レポート

C1160003-000001

2022/05/05 10:21

過去

2022/05/01 - 2022/05/04

30 台

64

セキュリティリスクは発生していません。

☐

C1160003-000002

2022/05/05 17:15

過去

2022/05/01 - 2022/05/04

30 台

63

セキュリティリスクは発生していません。

☐

C1160003-000003

2022/05/05 13:02

過去

2022/05/01 - 2022/05/04

30 台

63

セキュリティリスクは発生していません。

☐

C1160003-000004

2022/05/05 10:16

過去

2022/05/01 - 2022/05/04

30 台

63

セキュリティリスクの発生があります。

☐

C1160003-000007

2022/05/06 23:11

過去

2022/05/05 - 2022/05/04

30 台

35

セキュリティリスクの発生があります。

☐

C1160003-000005

2022/05/13 18:51

過去

2022/05/08 - 2022/05/11

30 台

21

セキュリティリスクの発生があります。

☐

C1160003-000006

2022/05/13 17:49

過去

2022/05/08 - 2022/05/11

30 台

21

セキュリティリスクの発生があります。

☐

C1160003-000008

2022/05/13 16:19

過去

2022/05/08 - 2022/05/11

30 台

21

セキュリティリスクの発生があります。

☐

C1160003-000003

2022/05/13 15:02

過去

2022/05/08 - 2022/05/11

30 台

21

セキュリティリスクは発生していません。

☐

C1160003-000002

2022/05/07 18:01

過去

2022/05/01 - 2022/05/05

30 台

30

セキュリティリスクの発生があります。

☐

C1160003-000001

2022/05/06 15:59

過去

2022/05/01 - 2022/05/05

30 台

30

セキュリティリスクは発生していません。

☐

C1160003-000003

2022/05/03 18:17

過去

2022/05/01 - 2022/05/02

30 台

21

セキュリティリスクは発生していません。

☐

C1160003-000009

2022/05/02 16:18

過去

2022/05/01 - 2022/05/01

30 台

30

セキュリティリスクの発生があります。

☐

C1160003-000008

2022/05/02 18:32

過去

2022/05/01 - 2022/05/01

30 台

28

セキュリティリスクは発生していません。

☐

C1160003-000005

2022/05/03 17:46

過去

2022/05/01 - 2022/05/01

30 台

28

セキュリティリスクは発生していません。

☐

C1160003-000006

2022/05/03 15:30

過去

2022/05/01 - 2022/05/01

30 台

28

セキュリティリスクは発生していません。

☐

C1160003-000003

2022/05/03 14:19

過去

2022/05/01 - 2022/05/01

30 台

28

セキュリティリスクは発生していません。

☐

C1160003-000004

2022/05/03 13:33

過去

2022/05/01 - 2022/05/01

30 台

28

セキュリティリスクの発生があります。

☐

C1160003-000003

2022/05/01 17:33

過去

2022/05/01 - 2022/05/01

30 台

28

セキュリティリスクの発生があります。

☐

C1160003-000002

2022/05/01 09:57

過去

2022/05/01 - 2022/05/01

30 台

28

セキュリティリスクの発生があります。

☐

図 7 レポート一覧画面

レポート NO	分析レポートを一意に識別する番号です。 クリックでき、分析期間中のログ送信が行われたユーザーの詳細が表示されます。 ※【④-1-1 分析結果レポート 詳細】画面へ遷移
報告日	ご契約時に決めたレポート送信日（曜日）が報告日となります。
分析対象間隔	週次のみ
ログ送信期間	ログ送信を受け付けている期間です。この期間に受け付けたログを分析しています。
契約利用端末数	ご契約時に決めた契約台数です。
ログ送信ユーザー数	ログ送信期間内にログを送信したユーザー数です。
分析ユーザー数	ログ送信期間内に分析されたユーザー数です。
分析結果	以下のコメントが記載されます。 セキュリティリスクの恐れがあります。 セキュリティリスクの疑いがあります。 セキュリティリスクはみられません。
分析レポート	分析レポートメールで添付された PDF ファイルが表示されます。

④-1-1 分析結果レポート 詳細

レポート一覧画面の「レポート NO」をクリックすると、「分析結果レポート 詳細」が表示されます。

アラート検知した端末は「対処方法」が記載されます。

様 分析結果レポート 詳細						
端末分析NO			Q 検索			
端末分析NO	EISS端末ID	ユーザーID	端末名	ユーザー名	検知内容	対処方法
CI210162-000009-000001	CI210162-1624491809	001			セキュリティリスクはみられません。	
CI210162-000009-000002	CI210162-1625189055	001			セキュリティリスクはみられません。	
CI210162-000009-000003	CI210162-1625204566	001			セキュリティリスクはみられません。	

図 8 分析結果レポート 詳細画面

端末分析結果

端末分析NO : CI200040-000009-000001					
<p>対処方法</p> <p>セキュリティリスクの恐れがあります。</p> <p>継続的にアラートが表示される場合は、メールで宛先：eiss-support@secure-iv.comまで、お問合せください。</p> <p> 端末分析結果 MITRE検知結果 </p>					
<p>分析結果</p> <p> アラートタイプ ▼ 検知内容 ▼ ログ収集日 ▼ 検索 </p>					
No	検知内容	検知詳細	アラートタイプ	ログ収集日時	対応内容
2872088	不正と思われるレジストリ情報を検知しました。 【T1546.008 : アクセス補助機能の悪用】	レジストリ情報が更新されました。 レジストリキー : SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	注意	2020/12/15 12:22	
2872089	不正と思われるレジストリ情報を検知	レジストリ情報が更新されました。	注意	2020/12/15	

MITRE 検知結果

端末分析NO : CI200040-000009-000001	
<p>対処方法</p> <p>セキュリティリスクの恐れがあります。</p> <p>継続的にアラートが表示される場合は、メールで宛先：eiss-support@secure-iv.comまで、お問合せください。</p> <p> 端末分析結果 MITRE検知結果 </p>	
初期アクセス 実行 永続化 ▲ 権限昇格 ▲ 防衛回避 認証情報アクセス 探索 横断関 収集 C&C(Command and Control)	
持ち出し 影響	
ブートまたはログオン時の初期化スクリプト タスク/ジョブスケジューリング プロセスインジェクション 特権昇格のための悪用 正当なアカウントの悪用 アクセストークンの操作 グループポリシーの変更 不正なWindowsサービスの追加 イベントトリガー実行 ▼ 36 ブートまたはログオン時の自動開始実行 ▼ 不正使用の昇格制御メカニズム ▼ 実行フローハイジャック	

④-2 速報通知検索

危険度がとても高いと判断されるアラートを確認出来ます。

対象アラートを検知した場合、以下の件名でサポート窓口から速報通知メールが届きます。

件名：[EISS：■■■■]【重要】セキュリティリスクの確認お願いします | ■■■■様 (SOMPO SHERIFF)

管理画面の「分析レポート管理」→「速報通知検索」から対処方法をご確認ください。

検知内容のコメントを押下すると、「速報検知内容」へ画面が遷移します。

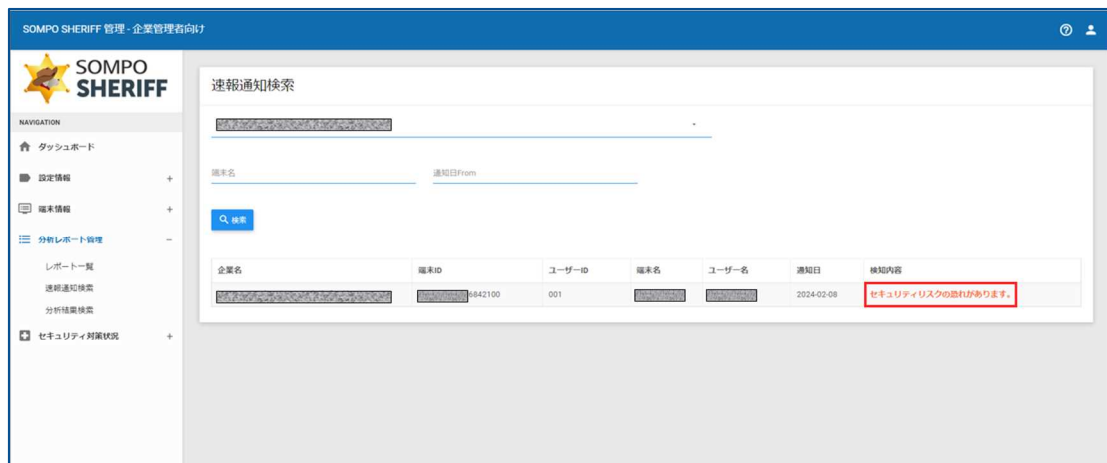


図 9 速報通知検索画面

企業名	企業名が表示されます。
端末 ID	端末と紐づくエージェントの ID が表示されます。
ユーザーID	端末のユーザー毎に採番される ID が表示されます。 端末に複数ユーザーがいる場合は「002」「003」と追加されます。
端末名	エージェントをインストールした端末名が表示されます。 ※端末名は PC のデバイス名となります
ユーザー名	端末のユーザーアカウント名が表示されます。
通知日	端末のアラートを通知した日時です。
検知内容	以下のコメントが記載されます。 ※コメントは「速報検知内容」へのリンクとなっています セキュリティリスクの恐れがあります。

④-2-1 検知内容と対応方法の確認「速報検知内容」画面では、検知内容、検知詳細、アラートタイプ、ログ収集日時、対応内容へのリンクが確認できます。



図 10 速報通知内容画面

対応内容を押下すると検知内容の詳細や対処方法が確認できます。

イベントログの削除 検知

アラートタイプ

警告

検知内容

攻撃者が悪用する可能性があるツールの動作を検知しました。

本アラート（イベントID：104、イベントID：1102）は、イベントログ削除の検知になります。
ログの削除は、不正攻撃を隠蔽するため、実施される可能性もございます。
そのため、サイバー攻撃も疑われるため、アラートとして検知しております。
検知詳細には、対象のイベントログを表示しています。

検知詳細の見方	
例）表示値	補足内容
不正なツールが検知されました。	-
イベントタイプ：system	イベントログ種類
プロバイダ名：Microsoft-Windows-Eventlog	イベントログのプロバイダ名
イベントID：104	検知対象のイベントID
イベントログ作成時間：2022-02-28 23:43:28	イベント実行されログが作成された時間

対処方法

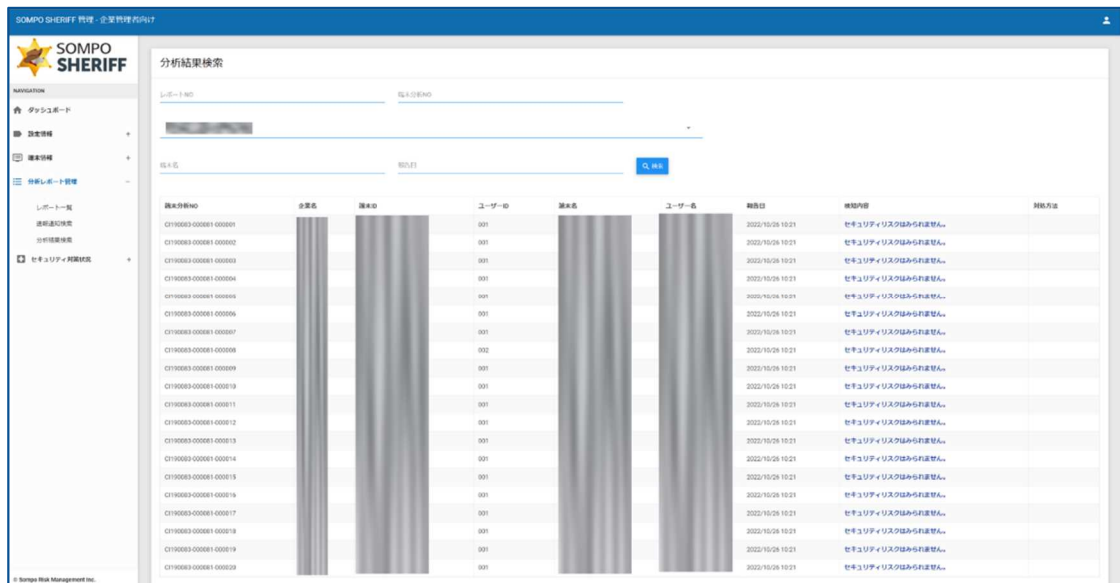
イベントログの削除に心当たりがございましたら、問題ございません。
対象の端末に対してクリーンアップツール等の利用でもイベントログが削除される可能性があります。

もし、何も心当たりのない場合は、最新状態にしたウイルス対策ソフトでのスキャンをお薦めします。
何も心当たりがなく、継続してアラートが出る場合はヘルプデスクまでご連絡ください。

④-3 分析結果検索

端末名や分析レポート報告日などで絞り込みしたい場合に利用できます。以下の項目で検索が可能です。

- ・ レポート NO
- ・ 端末分析 NO
- ・ 端末名
- ・ 報告日



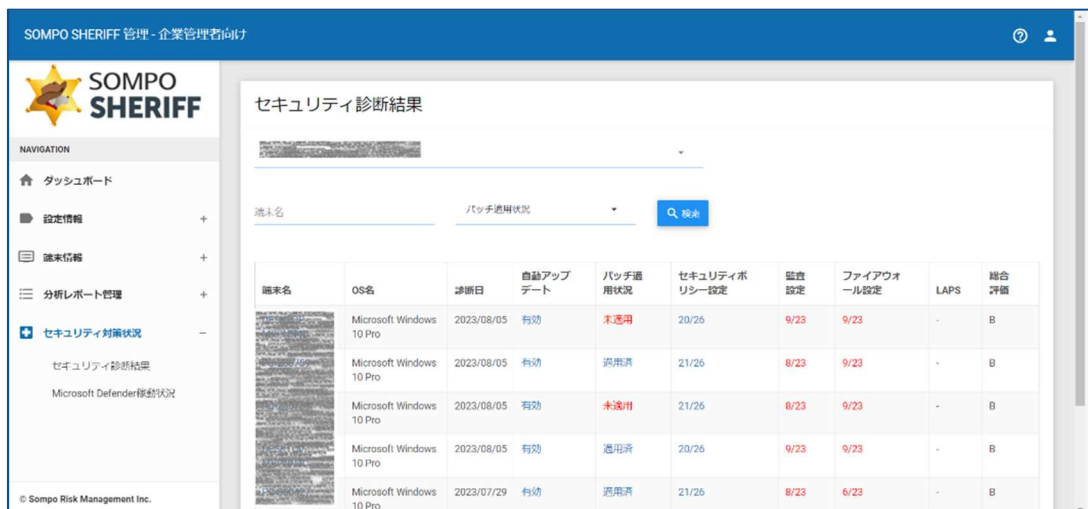
端末分析NO	企業名	端末ID	ユーザーID	端末名	ユーザー名	報告日	検出内容	対策方法
C1100003-000001-000001			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000002			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000003			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000004			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000005			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000006			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000007			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000008			002			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000009			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000010			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000011			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000012			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000013			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000014			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000015			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000016			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000017			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000018			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000019			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	
C1100003-000001-000020			001			2023/10/26 10:21	セキュリティリスクはみられませんでした。	

図 11 分析結果検索画面

⑤ セキュリティ対策状況

⑤-1 セキュリティ診断結果

端末ごとのセキュリティ診断結果の一覧が表示されます。



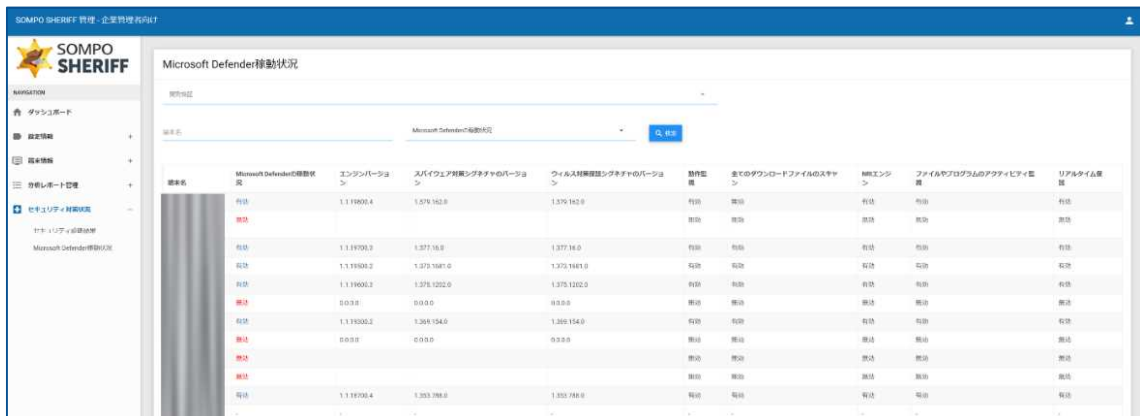
端末名	OS名	診断日	自動アップデート	パッチ適用状況	セキュリティポリシー設定	監査設定	ファイアウォール設定	LAPS	総合評価
	Microsoft Windows 10 Pro	2023/08/05	有効	未適用	20/26	9/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/08/05	有効	適用済	21/26	8/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/08/05	有効	未適用	21/26	8/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/08/05	有効	適用済	20/26	9/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/07/29	有効	適用済	21/26	8/23	6/23	-	B

図 12 セキュリティ診断結果画面

端末名	端末名（PC のデバイス名）が表示されます。 端末名をクリックすると【③-1-1 端末情報】へ遷移します。
OS 名	OS 名が表示されます。
診断日	該当端末からセキュリティ診断情報を取得した日です。
自動アップデート	該当端末の自動アップデートの「有効」「無効」が表示されます。
パッチ適用状況	パッチ適用状況について「パッチ適用済」「パッチ未適用」「ログ未送信」が表示されます。 パッチ未適用の場合、クリックすると未適用パッチの KB 番号を確認できます。 ※表示が「-」の場合はログ未送信端末のため適用状況が確認できていません。
セキュリティポリシー設定	セキュリティ構成フレームワーク レベル 1 の「セキュリティテンプレートポリシー」について推奨値との比較を表示しています。
監査設定	セキュリティ構成フレームワーク レベル 1 の「監査ポリシー」について推奨値との比較を表示しています。
ファイアウォール設定	セキュリティ構成フレームワーク レベル 1 の「Windows Defender ファイアウォールポリシー」について推奨値との比較を表示しています。
LAPS	ローカル管理者アカウントのパスワードを管理する LAPS の有効化状態を表示します。
総合評価	「パッチ適用状況」「セキュリティポリシー設定」「監査設定」「ファイアウォール設定」の 4 項目がセキュリティ構成フレームワークの推奨値に則しているかを A, B, C 評価で表示します。

⑤-2 Microsoft Defender 稼働状況

Microsoft Defender をご利用になられているお客様のみ、Microsoft Defender の稼働状況が確認できます。



端末名	Microsoft Defenderの稼働状況	エンジンバージョン	スバイウェア更新シグナチャのバージョン	ウイルス定義更新シグナチャのバージョン	動作状態	全てのダウンロードファイルのスキャン	検索エンジン	ファイルやプログラムのアクティビティ監視	リアルタイム保護
端末名	有効	1.1.1900.4	1.379.162.0	1.379.162.0	有効	有効	有効	有効	有効
	有効	1.1.1900.3	1.377.16.0	1.377.16.0	有効	有効	有効	有効	有効
	有効	1.1.1900.2	1.379.160.0	1.379.160.0	有効	有効	有効	有効	有効
	有効	1.1.1900.2	1.379.162.0	1.379.162.0	有効	有効	有効	有効	有効
	無効	0.0.0.0	0.0.0.0	0.0.0.0	無効	無効	無効	無効	無効
	有効	1.1.1900.2	1.380.154.0	1.380.154.0	有効	有効	有効	有効	有効
	無効	0.0.0.0	0.0.0.0	0.0.0.0	無効	無効	無効	無効	無効
	無効				無効	無効	無効	無効	無効
	有効	1.1.1900.4	1.383.160.0	1.383.160.0	有効	有効	有効	有効	有効

図 13 Microsoft Defender 稼働状況画面

端末名	端末名（PC のデバイス名）が表示されます。 端末名をクリックすると【③-1-1 端末情報】へ遷移します。
Microsoft Defender の稼働状況	Microsoft Defender の稼働状況について「有効」「無効」が表示されます。 有効の場合、クリックすると【⑤-2-1 Microsoft Defender 詳細画面】へ遷移します。 ※表示が「-」の場合はログ未送信端末のため稼働状況が確認できていません。
エンジンバージョン	AM（Anti Malware）エンジンのバージョンが表示されます。
スパイウェア対策 シグネチャのバージョン	スパイウェア対策シグネチャバージョンが表示されます。
ウィルス対策保護 シグネチャのバージョン	ウィルス対策保護シグネチャバージョンが表示されます。
動作監視	動作監視の状況について「有効」「無効」が表示されます。
全てのダウンロード ファイルのスキャン	全てのダウンロードファイルのスキャン状況について「有効」「無効」が表示されます。
NRI エンジン	NRI（Network Inspection System）エンジンの状況について「有効」「無効」が表示されます。
ファイルやプログラムの アクティビティ監視	ファイルやプログラムのアクティビティを監視の状況について「有効」「無効」が表示されます。
リアルタイム保護	リアルタイム保護の状況について「有効」「無効」が表示されます。

⑤-2-1 Microsoft Defender 稼働状況詳細

「Microsoft Defender の稼働状況」を押下すると、端末ごとの、Microsoft Defender のより詳細な稼働状況が確認できます。

SOMPO SHERIFF

NAVIGATION

ダッシュボード

設定情報

調査依頼

分析レポート管理

セキュリティ対策状況

セキュリティ診断結果

Microsoft Defender稼働状況

© Sompo Risk Management Inc.

端末情報 - PC-280759

OS

Microsoft Windows 10 Pro

Microsoft Defender稼働状況

有効

Microsoft Defender設定情報

分類	項目名	設定値
マルウェア対策	エンジンバージョン	1.1.23060.1005
	製品バージョン	4.18.23050.9
	エンジン	有効
	サービスバージョン	4.18.23050.9
スバイウェア対策	スバイウェア対策保護	有効
	スバイウェア対策シグネチャの更新経過日数	0
	スバイウェア対策シグネチャの最終更新日時	2023/08/06 15:12

図 14 Microsoft Defender 稼働状況詳細画面

4. 分析レポートの見方

分析レポート（PDF ファイル）に記載されている項目の説明です。

ログ送信期間	ログ送信の受付期間です。	
契約内容	利用端末数	ご契約いただいた端末数です。
	インストール端末数	インストール済みの端末数です。
	インストールユーザー数	インストール済みのユーザー数です。
	サービス開始終了期間	ご契約いただいたサービス利用期間です。
分析ユーザー情報	送信ユーザー数	今回の「ログ送信期間」にログ送信されたユーザー数です。
	分析ユーザー数	「送信ユーザー数」のうち、分析実施したユーザー数です。
分析結果概要	リスクのレベル毎の件数と、その構成比率を円グラフで表示しています。 セキュリティリスクはみられません。 : 分析ユーザー数 セキュリティリスクの疑いがあります。 : 分析ユーザー数 セキュリティリスクの恐れがあります。 : 分析ユーザー数	
分析結果詳細	分析ユーザー毎の検知内容です。	



分析結果詳細

端末名	ユーザー名	端末分析NO	検知内容
Windows10-base	siv-user1	CI190000-000001-000001	セキュリティリスクの恐れがあります。
Windows10-base	siv-user2	CI190000-000001-000002	セキュリティリスクはみられません。
Windows11-base	siv-user3	CI190000-000001-000003	セキュリティリスクはみられません。
Windows10-base	eiss-user1	CI190000-000001-000004	セキュリティリスクはみられません。
Windows11-base	eiss-user2	CI190000-000001-000005	セキュリティリスクはみられません。
Windows10-base	eiss-user3	CI190000-000001-000006	セキュリティリスクの恐れがあります。
Windows10-base	eiss-user4	CI190000-000001-000007	セキュリティリスクはみられません。
Windows11-base	Okinawa	CI190000-000001-000008	セキュリティリスクはみられません。
Windows10-base	Nahako	CI190000-000001-000009	セキュリティリスクはみられません。

5. 機能設定

① MAC アドレスのホワイト登録

業務上利用しているネットワーク接続につきましては、SOMPO SHERIFF にて検知されないように管理画面より検知除外設定をすることが可能です。

①-1 サイドバーにある「企業管理」を選択し、「企業情報」に遷移します。

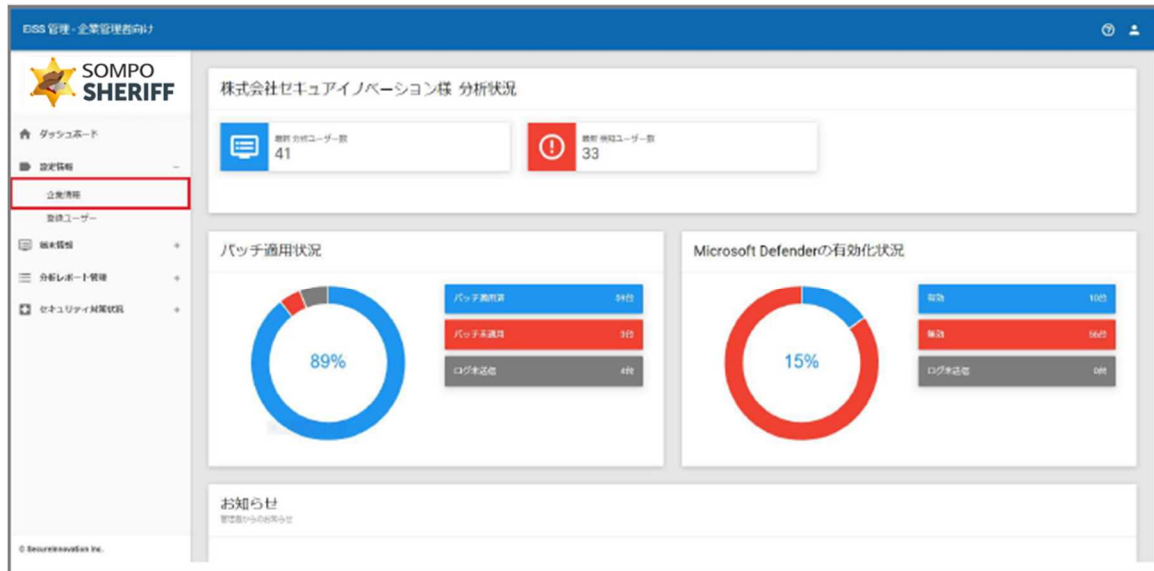


図 15 企業情報選択画面

①-2 画面下にスクロールし、「編集」ボタンを選択します。

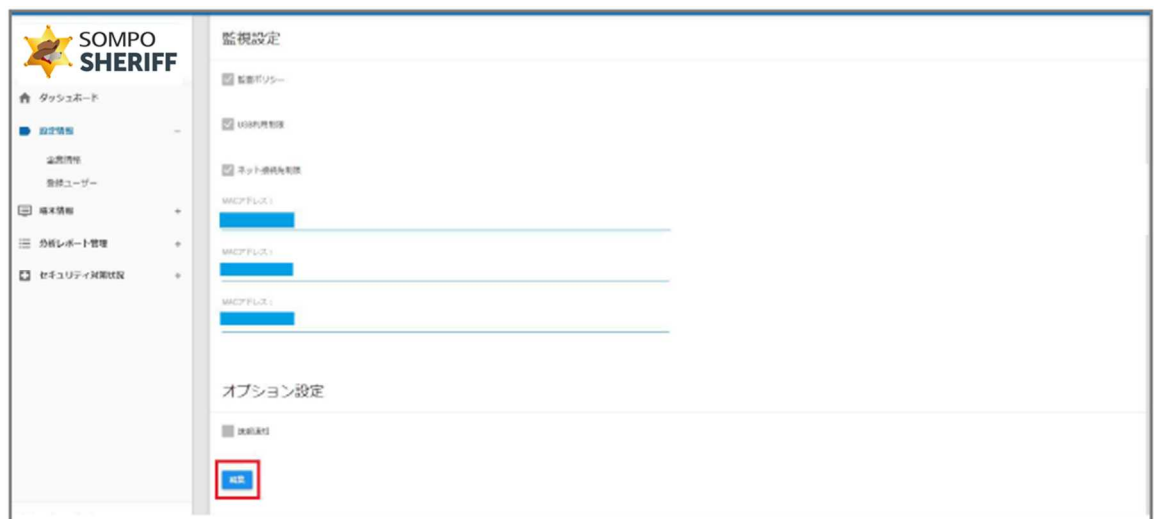


図 16 編集詳細画面-1

- ①-3 再度下までスクロールし、「MAC アドレスを追加で設定する」を選択します。
※この時、「ネット接続先制限」にチェックが無い場合は、チェックをつけます。

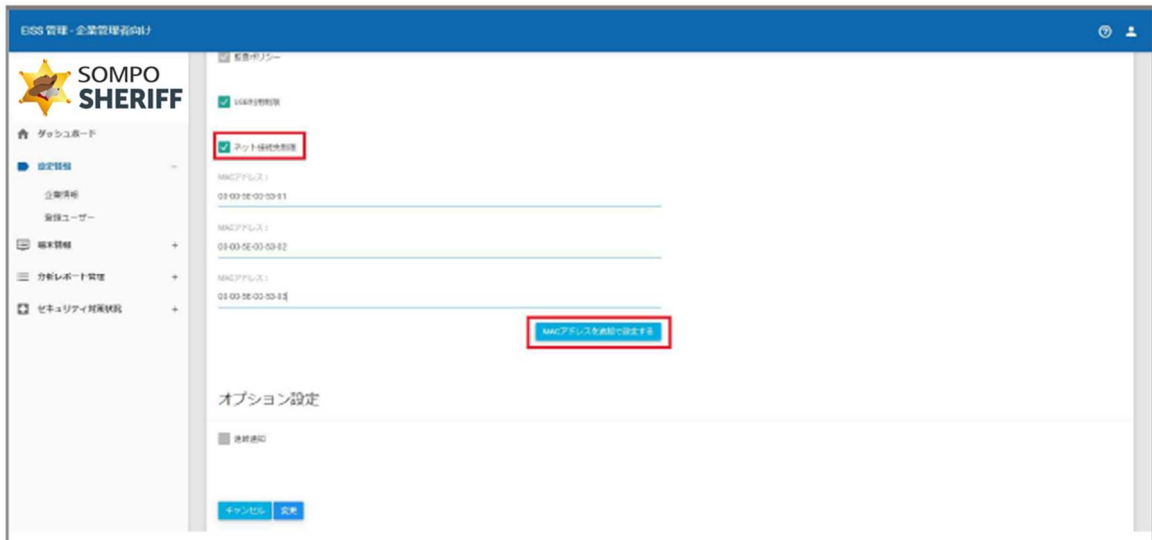


図 17 編集詳細画面-2

- ①-4 展開された入力欄に対象の MAC アドレスを追加します。追加する MAC アドレスが複数ある場合は都度「MAC アドレスを追加で設定する」を選択し、下記の様に追加してください。

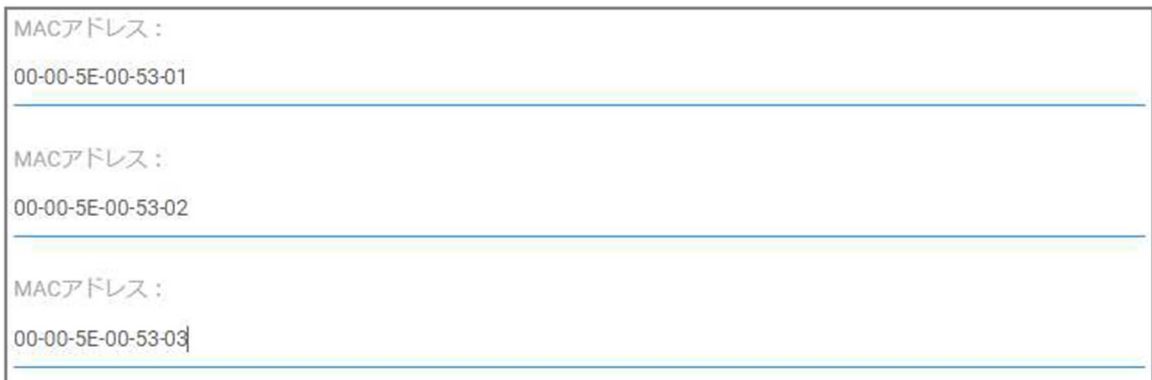


図 18 MAC アドレス追加画面

※注意点※

MAC アドレスを入力する記号は必ず「-」（ハイフン）をご使用ください。
別の区切り記号（カンマやスラッシュ）を入力した場合、正常に登録できず、
下記エラーメッセージが表示されます。



図 19 MAC アドレス追加時のエラーメッセージ画面

①-5 確認後、一番下の「変更」を選択します。



図 20 設定情報変更画面

「更新が完了しました。企業情報一覧からご確認ください」とメッセージが出ましたら、無事に登録完了です。

② USB 利用制限およびネットワーク接続先制限の設定

業務上利用している USB につきましては、SOMPO SHERIFF にて検知されないように管理画面より検知除外設定をすることが可能です。

②-1 サイドバーにある「企業管理」を選択し、「企業情報」に偏移します。

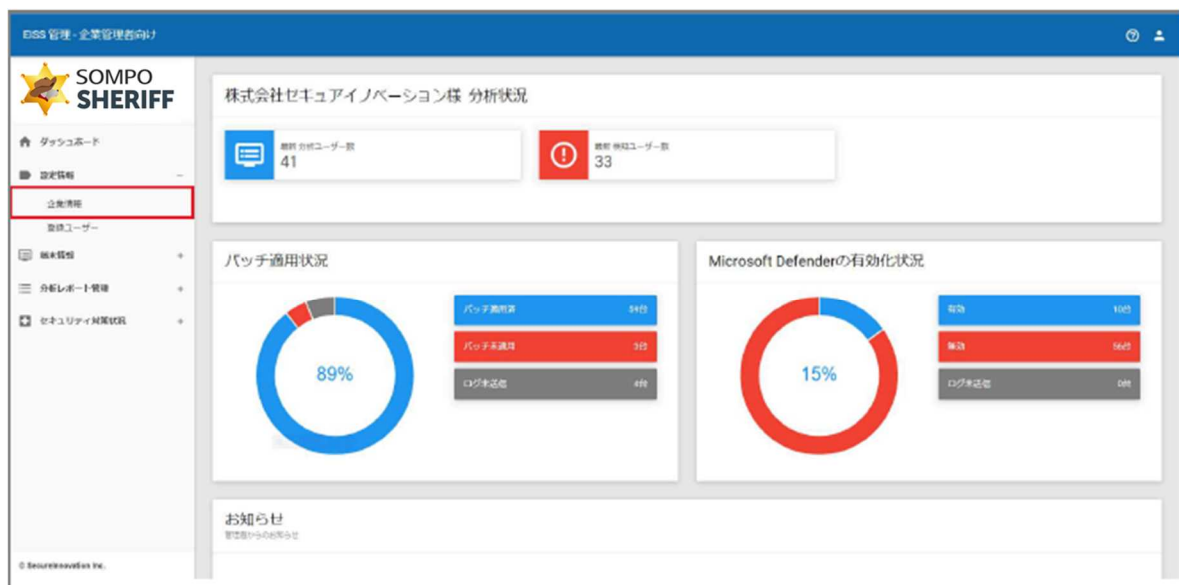


図 21 設定情報選択画面

②-2 画面下にスクロールし、「編集」ボタンを選択します。



図 22 編集詳細画面-1

②-3 再度下までスクロールし、USB 利用制限 / ネット接続先制限のチェックボックスをオン（またはオフ）にします。各機能については下記をご参照ください。

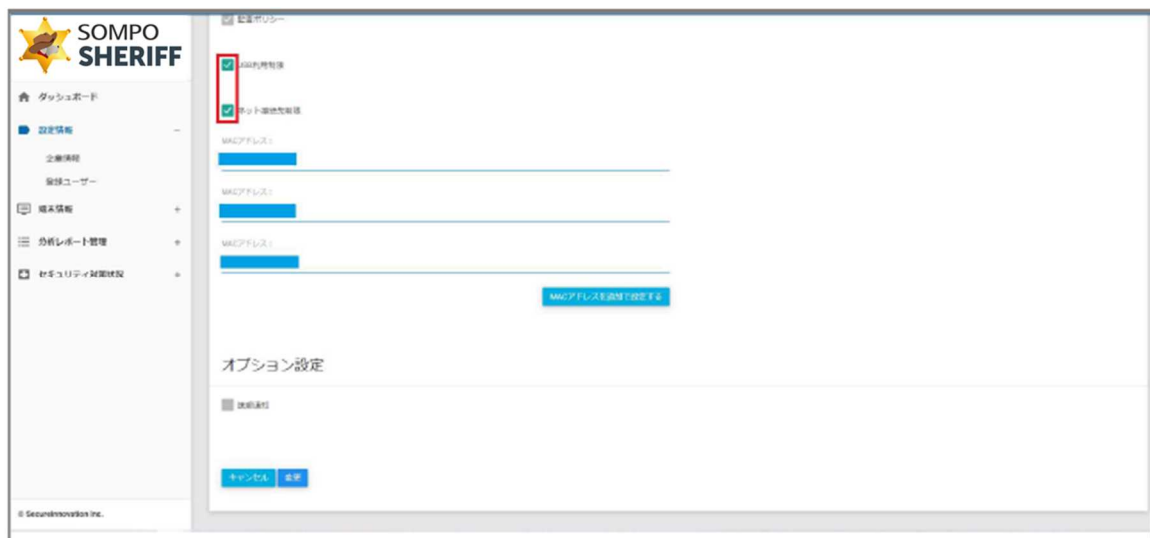


図 23 編集詳細画面-2

USB 利用制限

チェックボックスが「オン」の場合、対象のログ修習期間内に USB の接続の痕跡がある場合、検知します。
検知詳細には、USB の情報が表示されます。

検知内容	検知詳細	アラート タイプ
USBの利用が検知されました。	マウントされたデバイスが確認されました。 \\?\Volume{4eff93c0-8664-11ee-9dc0-f01db ca59bbf} USB_DISK_2.0 PMAP	警告

図 24 USB 検知画面

ネット接続先制限

チェックボックスが「オン」の場合、登録されているネットワーク以外への接続が確認された場合、検知します。
検知詳細には、ネットワーク接続の情報が表示されます。

検知内容	検知詳細	アラート タイプ
登録されていないネットワークへの 接続が検知されました。	2023/07/05 10:09:20.811に、 登録されていないMACアドレスの接続 を確認しました。	警告

図 25 ネットワーク検知画面

②-4 確認後、一番下の「変更」を選択します。

オプション設定

☐ 遠隔通知

キャンセル

変更

図 26 設定情報変更画面

「更新が完了しました。企業情報一覧からご確認ください」とメッセージが出ましたら、無事に登録完了です。

③ IP アドレス制限の設定

IP アドレス制限は、指定の IP アドレスからのみ管理画面にアクセスできるようにするセキュリティ機能です。
自社オフィスの IP アドレスだけを許可することで、第三者による不正アクセスを防げます。

③-1 サイドバーにある「アクセス制限」を選択し、「IP アドレス接続制限」に偏移します。

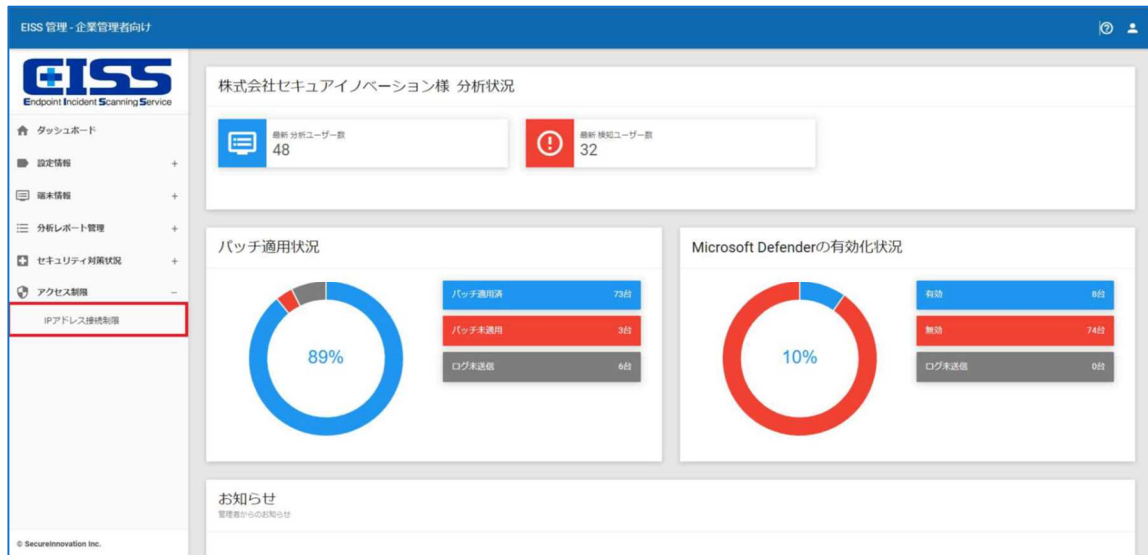


図 27 設定情報選択画面

③-2 画面右端の「IP アドレス接続制限追加」を選択します。



図 28 編集詳細画面

③-3 登録する IP アドレス（自社オフィスの IP アドレス等）を入力し、追加ボタンを選択します。

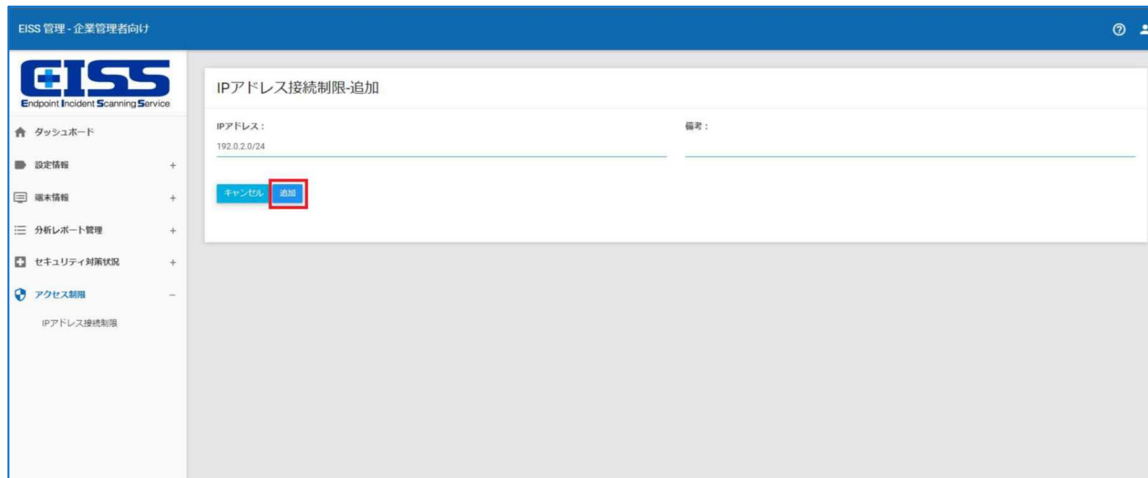


図 29 設定情報追加画面

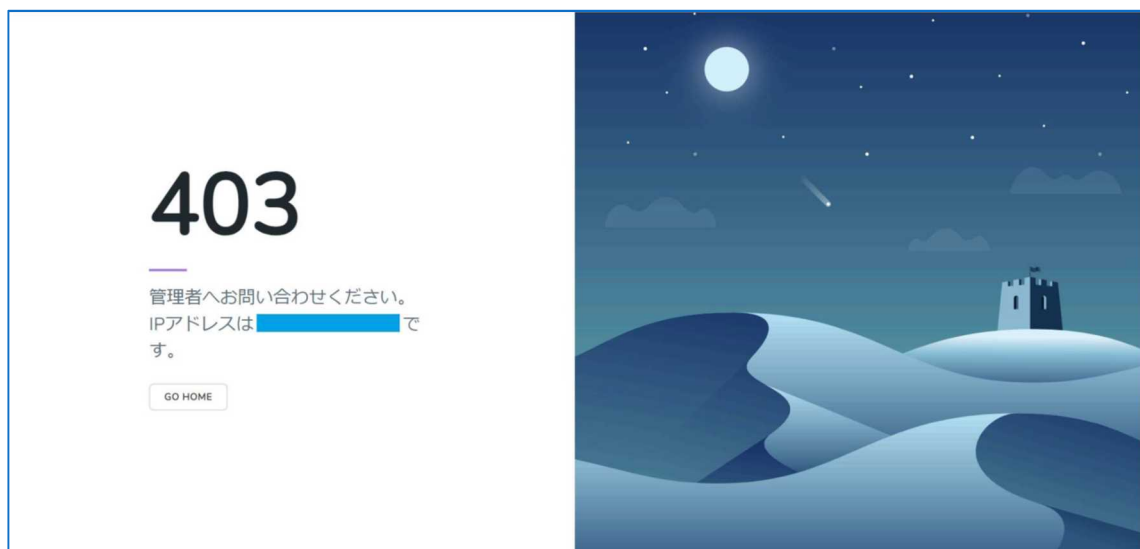
③-4 下記完了画面が表示されると、無事登録完了となります。



図 30 登録完了画面

※ご注意※

誤った IP アドレスを登録すると、制限機能により管理画面へのアクセスがブロックされお客様ご自身での操作が出来なくなります。





お手数をおかけいたしますが、IP アドレスの修正は弊社お問い合わせ窓口へご連絡ください。
その際、ブロックされたページに記載されている正しい IP アドレスをお問い合わせの際にご記載ください。

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。

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

対応時間: 9:00~17:00(土日祝を除く)
SOMPOリスクマネジメント株式会社