



管理画面マニュアル (企業管理者向け)

第 1.4 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
4.	分析レポートの見方.....	16

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	CIXXXXXXXXX
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

3. 管理画面の説明

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。

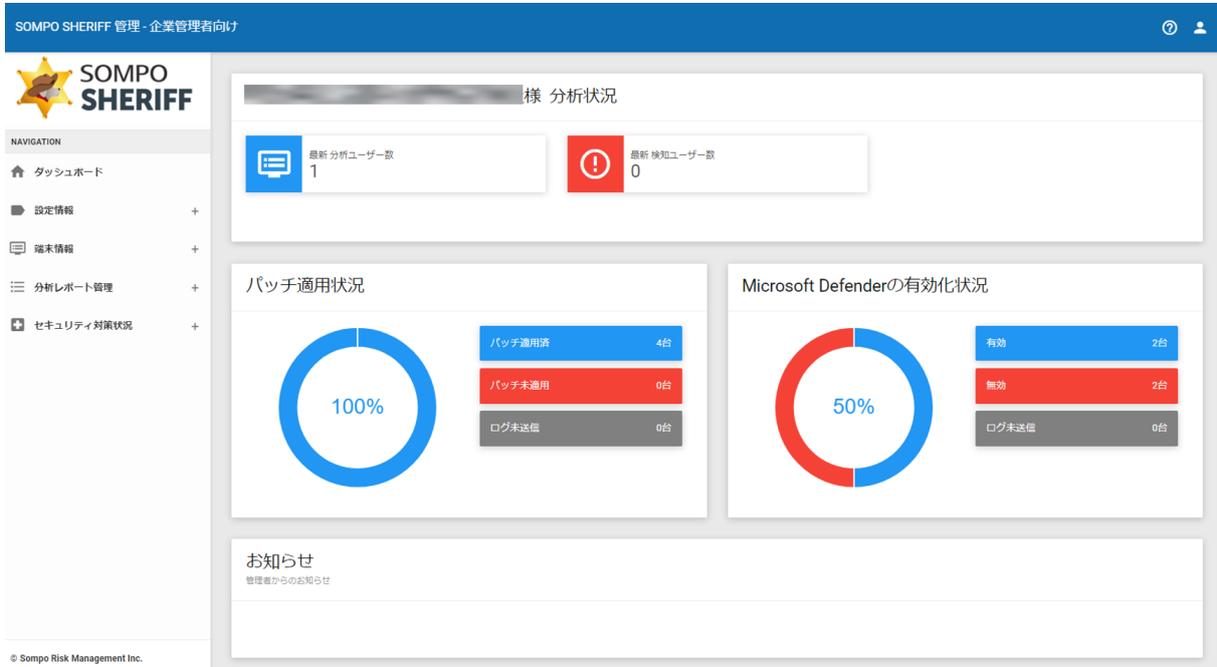


図 2 ダッシュボード画面

② 設定情報

②-1 企業情報

ご契約時に頂いた情報が表示されます。

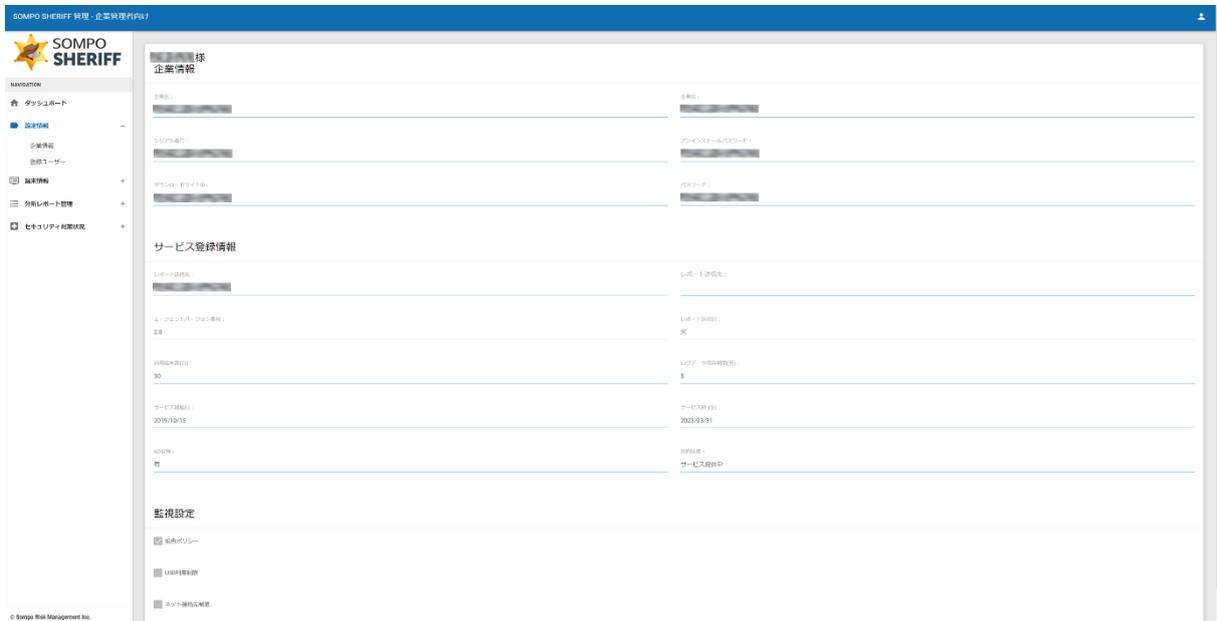


図 3 企業情報画面

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。

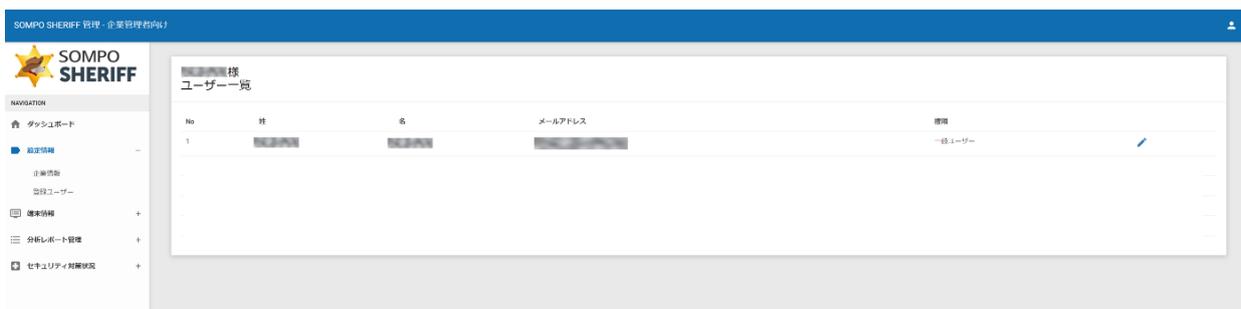
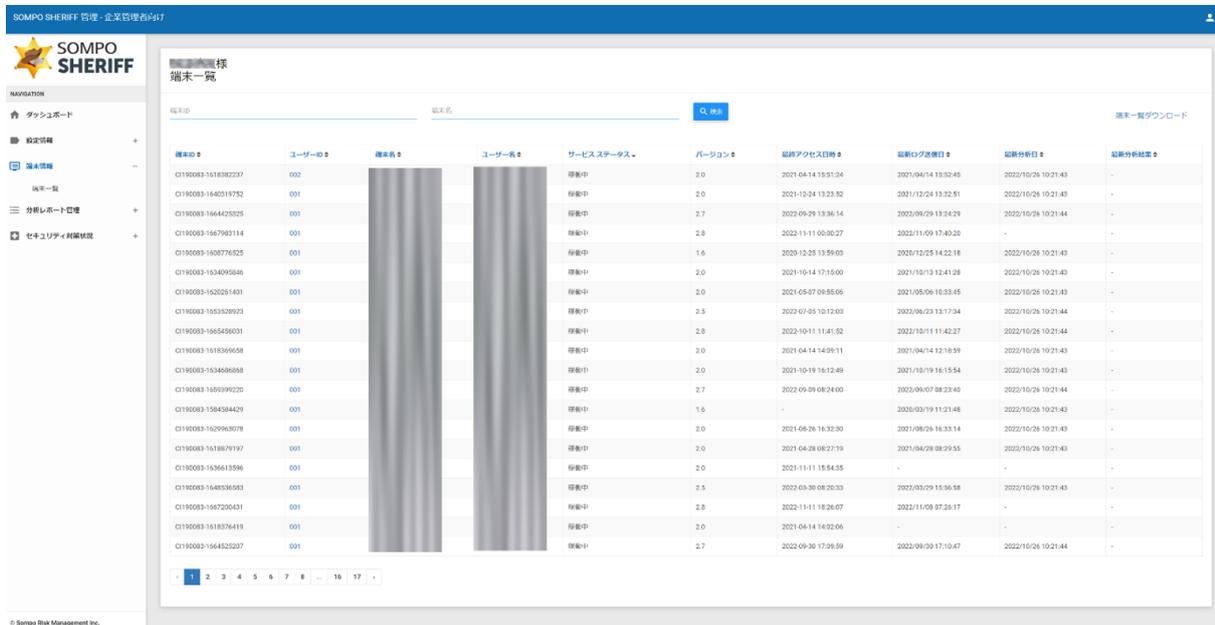


図 4 ユーザー一覧画面

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	最終ログイン日時	最終更新日時	最終分析日時
C190003-1618382237	002			稼働中	2.0	2021-04-14 13:51:24	2021/04/14 13:52:45	2022/10/26 10:21:43	-
C190003-1640319752	001			稼働中	2.0	2021-12-24 13:23:52	2021/12/24 13:22:51	2022/10/26 10:21:43	-
C190003-1664425225	001			稼働中	2.7	2022-09-29 13:36:14	2022/09/29 13:24:29	2022/10/26 10:21:44	-
C190003-1667982114	001			稼働中	2.8	2022-11-11 00:50:27	2022/11/09 17:40:20	-	-
C190003-1608776025	001			稼働中	1.6	2020-12-25 13:59:00	2020/12/25 14:22:18	2022/10/26 10:21:43	-
C190003-1634093846	001			稼働中	2.0	2021-10-14 17:15:00	2021/10/13 12:41:28	2022/10/26 10:21:43	-
C190003-1620261401	001			稼働中	2.0	2021-05-07 09:55:06	2021/05/06 16:33:45	2022/10/26 10:21:43	-
C190003-1653282923	001			稼働中	2.5	2022-07-05 10:12:03	2022/06/23 13:17:34	2022/10/26 10:21:44	-
C190003-1656456031	001			稼働中	2.8	2022-10-11 11:41:52	2022/10/11 11:42:27	2022/10/26 10:21:44	-
C190003-1618389658	001			稼働中	2.0	2021-04-14 14:09:11	2021/04/14 12:18:59	2022/10/26 10:21:43	-
C190003-1634698866	001			稼働中	2.0	2021-10-19 16:12:49	2021/10/19 16:15:54	2022/10/26 10:21:43	-
C190003-1659399220	001			稼働中	2.7	2022-09-09 08:24:00	2022/09/07 08:23:40	2022/10/26 10:21:44	-
C190003-1584584429	001			稼働中	1.6	-	2020/03/19 11:21:48	2022/10/26 10:21:43	-
C190003-1629963078	001			稼働中	2.0	2021-08-26 16:32:30	2021/08/26 16:33:14	2022/10/26 10:21:43	-
C190003-1618879197	001			稼働中	2.0	2021-04-28 08:27:19	2021/04/28 08:29:55	2022/10/26 10:21:43	-
C190003-1636613396	001			稼働中	2.0	2021-11-11 18:54:35	-	-	-
C190003-1648536083	001			稼働中	2.5	2022-03-30 08:20:33	2022/03/29 15:36:58	2022/10/26 10:21:43	-
C190003-1667202431	001			稼働中	2.8	2022-11-11 18:26:07	2022/11/09 07:26:17	-	-
C190003-1618376419	001			稼働中	2.0	2021-04-14 14:02:06	-	-	-
C190003-1664522027	001			稼働中	2.7	2022-09-30 17:39:59	2022/09/30 17:10:47	2022/10/26 10:21:44	-

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	<p>端末のユーザー毎に採番される ID が表示されます。</p> <p>端末に複数ユーザーがいる場合は「002」「003」と追加されます。</p> <p>クリックでき、端末の情報が確認できます。</p> <p>※【③-1-1 端末情報】画面へ遷移</p>
端末名	<p>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。</p> <p>※端末名は PC のデバイス名となります。</p> <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	端末がログを分析した日時 ※通常であれば翌日が分析日となります。
最新分析結果	端末の最新分析結果が表示されます。 「-」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。

③ 端末情報

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。

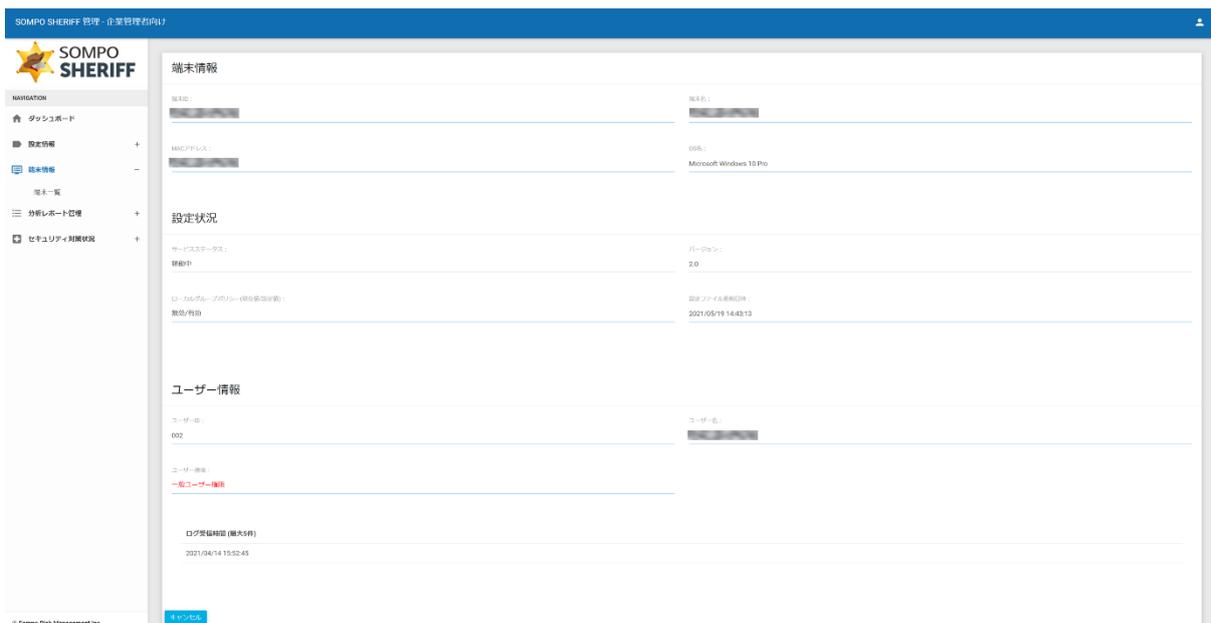
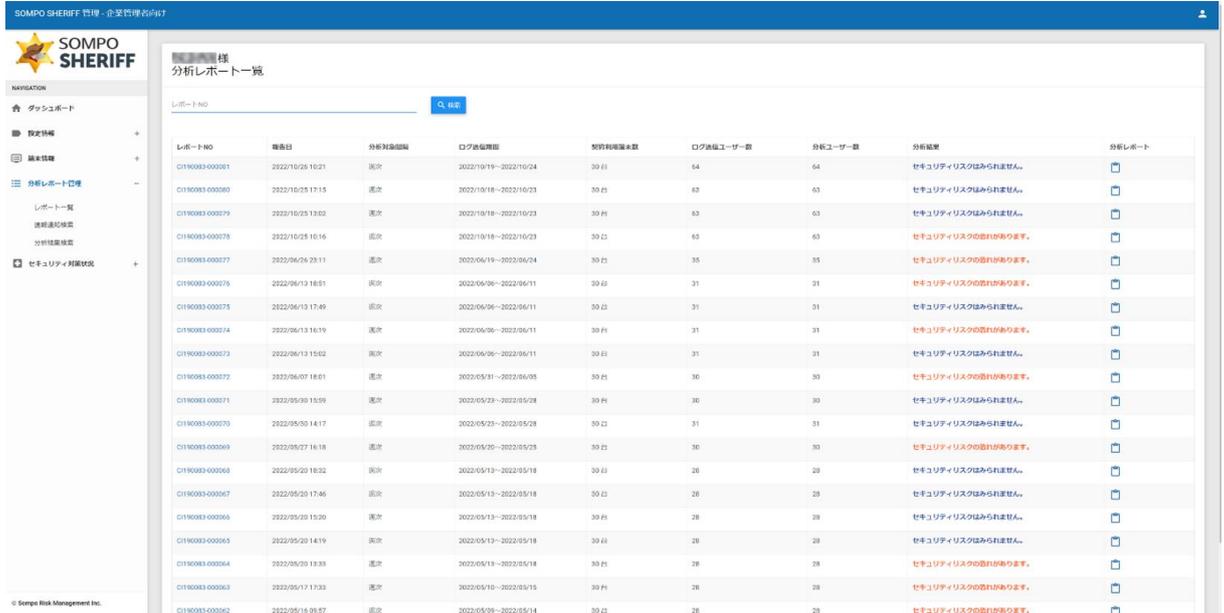


図 6 端末情報画面

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。



レポートNO	報告日	分析対象期間	ログ送信期間	契約利用端末数	ログ送信ユーザー数	分析ユーザー数	分析結果	分析レポート
C190083-000081	2022/10/25 10:21	週次	2022/10/19 - 2022/10/24	30台	64	64	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000080	2022/10/25 17:15	週次	2022/10/18 - 2022/10/23	30台	63	63	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000079	2022/10/25 13:02	週次	2022/10/18 - 2022/10/23	30台	63	63	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000078	2022/10/25 10:16	週次	2022/10/18 - 2022/10/23	30台	63	63	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000077	2022/06/26 23:11	週次	2022/06/19 - 2022/06/24	30台	35	35	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000076	2022/06/13 18:51	週次	2022/06/06 - 2022/06/11	30台	31	31	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000075	2022/06/13 17:49	週次	2022/06/06 - 2022/06/11	30台	31	31	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000074	2022/06/13 16:19	週次	2022/06/06 - 2022/06/11	30台	31	31	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000073	2022/06/13 15:52	週次	2022/06/06 - 2022/06/11	30台	31	31	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000072	2022/06/07 18:01	週次	2022/05/31 - 2022/06/05	30台	30	30	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000071	2022/05/30 15:59	週次	2022/05/23 - 2022/05/28	30台	30	30	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000070	2022/05/30 14:17	週次	2022/05/23 - 2022/05/28	30台	31	31	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000069	2022/05/27 16:18	週次	2022/05/20 - 2022/05/25	30台	30	30	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000068	2022/05/20 18:22	週次	2022/05/13 - 2022/05/18	30台	28	28	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000067	2022/05/20 17:46	週次	2022/05/13 - 2022/05/18	30台	28	28	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000066	2022/05/20 15:20	週次	2022/05/13 - 2022/05/18	30台	28	28	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000065	2022/05/20 14:19	週次	2022/05/13 - 2022/05/18	30台	28	28	セキュリティリスクはみられません。	<input type="checkbox"/>
C190083-000064	2022/05/20 13:33	週次	2022/05/13 - 2022/05/18	30台	28	28	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000063	2022/05/17 17:33	週次	2022/05/10 - 2022/05/15	30台	28	28	セキュリティリスクの恐れがあります。	<input type="checkbox"/>
C190083-000062	2022/05/16 09:57	週次	2022/05/09 - 2022/05/14	30台	28	28	セキュリティリスクの恐れがあります。	<input type="checkbox"/>

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。

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

対処方法
セキュリティリスクの恐れがあります。
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。

端末分析結果 MITRE検知結果

分析結果

アラートタイプ 検知内容 ログ収集日

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

対処方法
セキュリティリスクの恐れがあります。
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。

端末分析結果 MITRE検知結果

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 構築間 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 ▼
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。

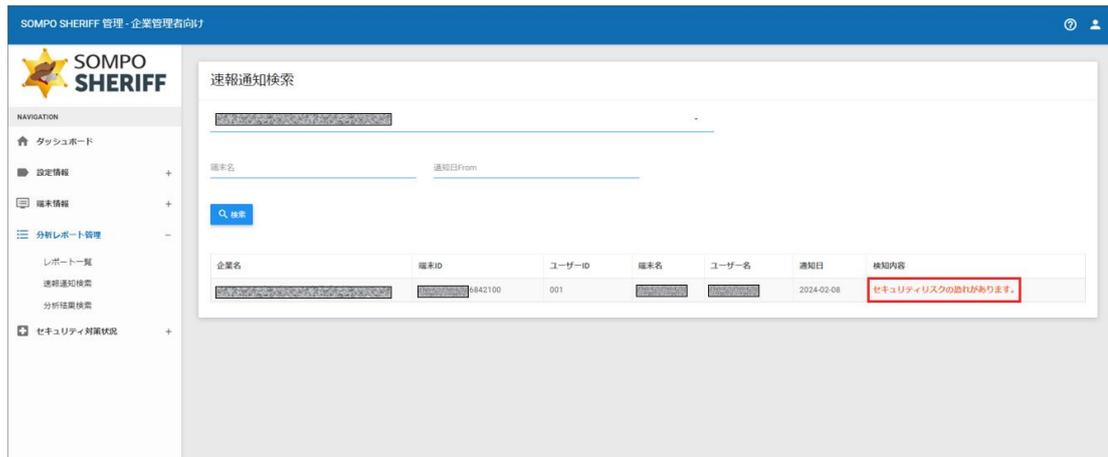


図 9 速報通知検索画面

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

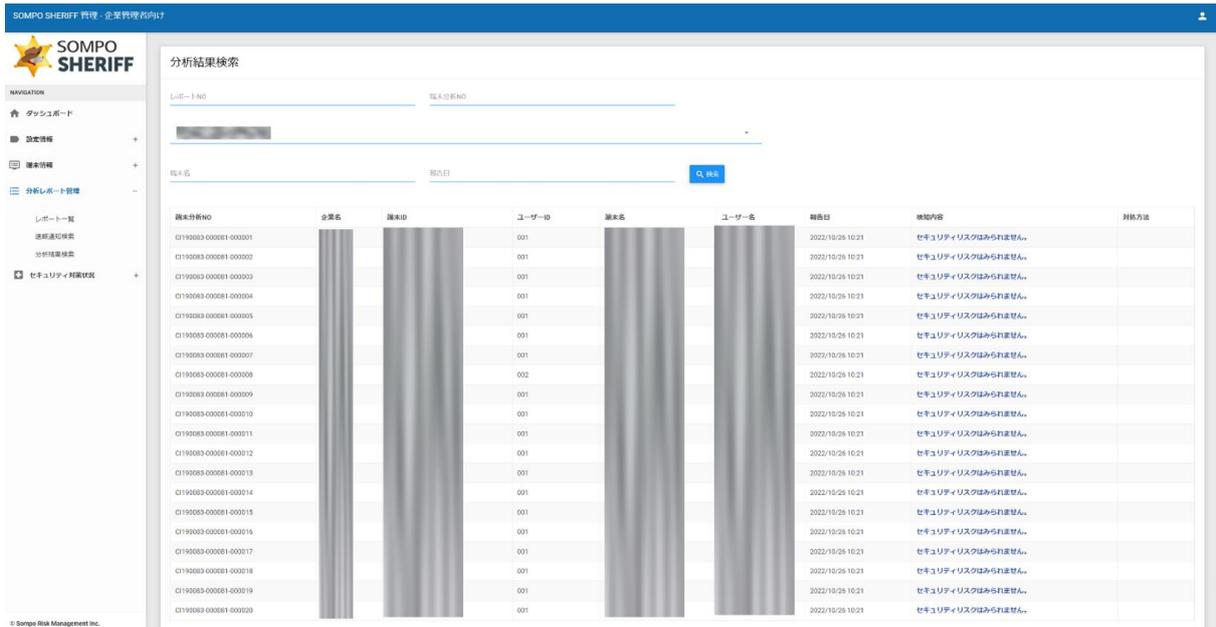
イベントログの削除に心当たりがございましたら、問題ございません。対象の端末に対してクリーンアップツール等の利用でもイベントログが削除される可能性があります。

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勧めします。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



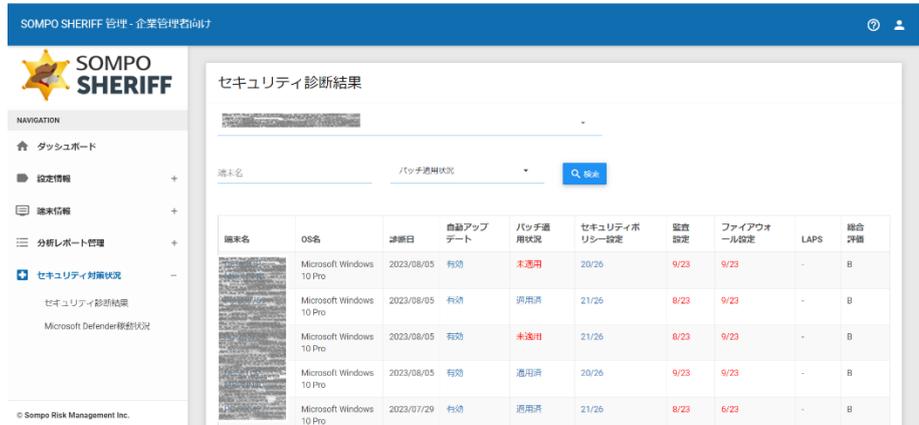
端末分析NO	企業名	端末ID	ユーザーID	端末名	ユーザー名	報告日	検知内容	判別方法
CI190083-000081-000001			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000002			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000003			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000004			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000005			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000006			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000007			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000008			002			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000009			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000010			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000011			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000012			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000013			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000014			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000015			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000016			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000017			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000018			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000019			001			2022/10/26 10:21	セキュリティリスクはみられませんでした。	
CI190083-000081-000020			001			2022/10/26 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	20/25	9/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/08/05	有効	適用済	21/25	8/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/08/05	有効	未適用	21/25	8/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/08/05	有効	適用済	20/25	9/23	9/23	-	B
	Microsoft Windows 10 Pro	2023/07/29	有効	適用済	21/25	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。

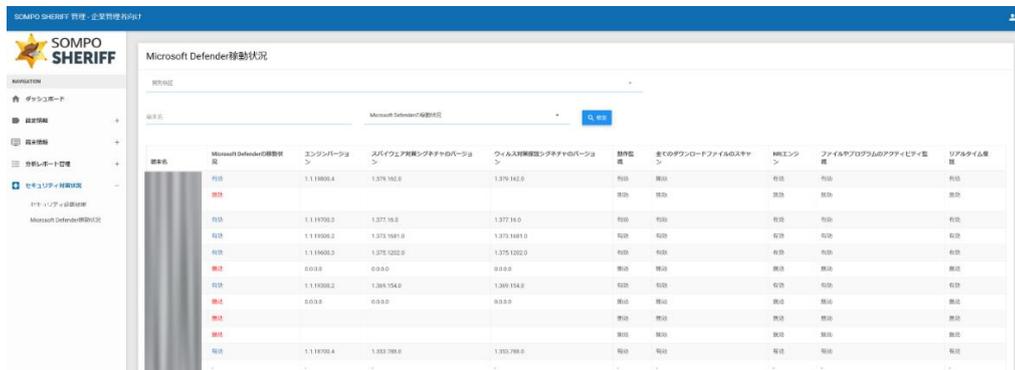


図 13 Microsoft Defender 稼働状況画面

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 管理 - 企業管理者向け

端末情報 - PC-280759

OS名
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
	追加バージョン	4.18.23050.9
	エンジン	有効
	サブエンジン	4.18.23050.9
スバイウェア対策	スバイウェア対策有効	有効
	スバイウェア対策シグネチャの更新回数	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

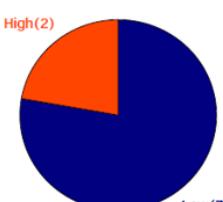
© Sompo Risk Management Inc.

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。	

レポートNO: CI190000-000001	
ログ送信期間	
2022/05/01 ~ 2022/05/06	
契約内容	
利用端末数	: 10台
インストール端末数	: 8台
インストールユーザー数	: 15ユーザー
サービス開始終了期間	: 2022/04/01 ~ 2023/03/31
分析ユーザー情報	
送信ユーザー数	: 9ユーザー
分析ユーザー数	: 9ユーザー
分析結果概要	
セキュリティリスクはみられません。	: 7
セキュリティリスクの疑いがあります。	: 0
セキュリティリスクの恐れがあります。	: 2
	

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。

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

CS2400007