

管理画面マニュアル (企業管理者向け)

第1.5版



SOM P Oリスクマネジメント株式会社

Copyright©2024 Sompo Risk Management Inc. All Rights Reserved.



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	
1	MAC アドレスのホワイト登録	
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	CIXXXXXXX
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

SOMPO SHERIFF 管理面面 Sompo Risk Management Inc.
■ 企業ID
⊻ メールアドレス

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。

SOMPO SHERIFF 管理 - 企業管	理者向(kt	0 🛓
	:	様 分析状況	
NAVIGATION			
合 ダッシュホード			
▶ 設定情報	+		
🗐 端末情報	+		
三 分析レポート管理	+	パッチ適用状況 Microsoft Defenderの有効化状況	2
セキュリティ対応状況	+	(パッチ通用が 化式 パッチ通用が 化式 パッチ規制 の行 ログ非逆信 の任	約約 2台 総約 7台 ログ末送信 0台
© Sompo Risk Management Inc.			

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。

50Mr0.0(63FFH#263H#260)							
Harcanon 🛉	141.	240					
会議部編 (1983) - ザー	50(545)	2040-6400-FL					
() axon •	97101-97110	40) fr					
± 880-8-188	bearsa	DED MA					
□ E410948888 +							
	サービス登録情報						
	Life-Pare 1	(Set (Sente)					
	2-02378-022484	x (50) x					
	annadara. 30	1					
	2019/52/15	2-001/0					
		7-1380年					
	監視設定						
	E satur-						
	- unitar						
C Songe Risk Management Inc.	III in y SHELOHE						

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。

SOMPO SHERIFF 管理	SOMPO SHERIFF 管理 - 企業管理者向け ⑦									
	PO RIFF	SOMF	POリスクマネジメン ゲー一覧	卜株式会社様						
∮ ダッシュホード		No	姓	a.	メールアドレス	海集				
設定情報	-	1				1				
企業情報 登録ユーザー		2				1				
第末情報	+	3				1				
			1.00	10	Dis Land American and In					

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。

SHERIFI	F II	NUDIMEN									
		端末一覧									
104		64.0			16		0.000				
51 7 -F											徳末一覧タウンロー
活相	•	-							and the second second		
1.48		Sec. 1	7-9-08	den f	1-9-61	9-EXXF-9X.	V-2328	BULL DEVENUE	100000000	AG40274913 #	ALM:779170.80 0
-12		C1190083-1618382237	002			080	2.0	2021-04-14 15:51:24	2021/04/14 15:52:45	2022/10/26 10:21:43	
		01190003-1640319752	001			12401	2.0	2021-12-24 13:23:82	2021/12/24 13:32:51	2022/16/26 10:21:45	
		C1190083-1464425325	001			598/P	2.7	2022-09-29 13:36:14	2022/09/29 13:24:29	2022/16/26 10.21.44	
リティ対策状況	•	C1192083-1667983114	001	- 11 1 1 1		1240-P	2.0	2022-11-11 00:00:27	2022/11/09 17:40:20		
		C1190083-1608776525	001			6480-P	1.6	2029-12-25 13:59:03	2020/12/25 14:22:18	2022/10/26 10:21:40	
		C1195063-1634095646	001	- 10 1 10 1		10140-1-	20	2021-10-14 17:15:00	2021/10/13 12:41:28	2222/10/26 10:21:40	
		C1190083-1620251401	001			0160-0	2.0	2021-05-07 09:55:06	2021/05/06 10:33:45	2022/10/26 10:21:45	
		CI190083-1653528923	001			超級中	2.5	2022-07-05 10:12:03	2022/06/23 13:17:34	2022/10/26 10:21:44	
		CI190083-1665456031	601			10140-01	2.8	2022-10-11 11:41:52	2022/10/11 11:42:27	2022/16/26 10:21:44	
		CI190083-1618365658	001			総動中	2.0	2021-04-14 14:09:11	2021/04/14 12:18:59	2022/10/26 10:21:43	
		CI190083-15346868688	001	10.000		10640-11	2.0	2021-10-19 16:12:49	2021/10/19 16:15:54	2022/10/26 10:21:45	
		C1190063-1659394220	001	10.0100		得象中	2.7	2022-09-09-08:24:00	2022/09/07 08:23:45	2022/10/26 10:21:44	
		CI190003-1584584429	001			1040-0	1.6		2020/00/79 11:21:48	2022/16/26 10:21:43	
		C1190083-1629963078	001			经最中	2.0	2021-08-26 16:32:30	2021/08/26 16:33:14	2022/10/26 10:21:48	
		C1190083-1618879197	001	100100		2010年	2.0	2021-04-28 08:27:19	2021/04/28 08:29:55	2022/10/26 10:21:43	
		CI190083-1636613596	001	100100		和他中	2.0	2021-11-11 15:54:35			
		C/190083-1648536583	001	100101	100100	印象中	2.5	2022-05-36 08:20:33	2022/03/29 15 56 58	2022/10/26 10:21:43	
		CI190083-1667230431	001	100101	100101	108-1	2.8	2022-11-11 18:26:07	2022/11/08 07:25:17		
		CI190083-1518376419	001			标版中	2.0	2021-04-14 14:02:05			
		CI190083-1664525207	001			8580-P	2.7	2022-09-30 17:09:59	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	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。



	 ※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。 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。 ※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。
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	端末のステータスが確認できます。 ※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。
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。



③-1-1 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。

SOMPO SHEREF RUT OF SHEREF	art	<u>+</u>
	織未傳報	
NAMESTER	818.	auto:
育 ダッシュホード	D. J. T.	
ID 921546 +	MC2PDOX.	008.
🗊 жанна —	INCOME.	Memori Wednes 10 Pm
%र्म- छ		
□ 9€レポート目电 +	設定状況	
E#107-18808 +	19-1/2020-2231 19-1/2020-2231	(H=2m): (20
	- 	282-71-624903 282-96445 19445 19
	ユーザー傍報	
	3-4-6	2-9-8
	002	bearsa
	2-0-80 -82-0-80	
	ログ常経時間(第六5日)	
	2021/04/14 1E52 45	
© Serryo Bisk Management Ins.	(1)258	

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。

O SHERIFF 管理 - 企業管理									
SOMPO	様 分析レポート-	-覧							
ON				· · · · · · · · · · · · · · · · · · ·					
シュボード	Litt-I-NO			Q, 60.00					
1546 +									
a +	L-IK-I-NO	联告日	分析对象图响	ログ送信期間	经给利用漏水数	ログ活催ユーザー数	分析ユーザー数	分析結果	分析レポート
- 100	C1110083-003081	2822/10/26 10:21	362r	2022/10/19-2022/10/24	30 #1	54	64	セキュリティリスクはみられません。	
«-rba -	C(190083-002080	2022/10/25 17:15	愿次	2022/10/18~2022/10/23	30 fs	63	63	セキュリティリスクはみられません。	
	Ci140083 003079	2022/10/25 13:02	速次	2022/10/18~-2022/10/23	30 <u>fr</u>	63	63	セキュリティリスクはみられません。	0
信葉検索	C1190083-003078	2922/10/25 10:16	重次	2022/10/18~2022/10/23	30 £1	65	63	セキュリティリスクの恐れがあります。	۵
リティ対策状況 +	CI140083-003077	2022/06/26 23:11	透次	2022/06/19~2022/06/24	30 23	35	35	セキュリティリスクの恐れがあります。	۵
	C1190083-000076	2022/06/13 18:51	#22	2022/06/06~2022/06/11	30 83	31	31	セキュリティリスクの恐れがあります。	۵
	C1190093-003075	2222/06/13 17.49	<i>B</i> R	2022/06/062022/06/11	90.43	91	21	セキュリティリスクセルられません。	۵
	C/1100003-003074	2222/36/13 16:19	82	2022/06/06~-2022/06/11	30 H	33	31	セキュリティリスクの訪れがあります。	۵
	C1140083-000073	2022/06/13 15/02	302	2022/06/06~-2022/06/11	30 81	31	31	セキュリティリスクはみられません。	۵
	CI190083-003072	2022/06/07 18:01	速次	2022/05/31~2022/06/05	30.B	30	30	セキュリティリスクの恐れがあります。	0
	CI1100083-003071	2022/05/30 15:59	進次	2022/05/23~2022/05/28	30 M	30	30	セキュリティリスクはみられません。	٥
	CI190083-000070	2022/05/30 14:17	道次	2022/05/23~2022/05/28	30 22	31	31	セキュリティリスクはみられません。	۵
	C1140083-000069	2022/05/27 16:18	進次	2022/05/202022/45/28	30.03	30	30	セキュリティリスクの恐れがあります。	0
	CI190083-003068	2022/05/20 18:32	18.0e	2022/05/132022/05/18	30.61	28	28	セキュリティリスクはみられません。	۵
	CI190083-003067	2022/05/20 17:46	御 注	2022/05/13~-2022/05/18	30.03	28	28	セキュリティリスクはみられません。	٥
	CI140083-003066	2222/05/20 15:20	速次	2022/05/13~-2022/05/18	30 ft	28	28	セキュリティリスクはみられません。	0
	C1190003-003065	2022/05/20 14:19	演次	2022/05/13~-2022/05/18	30.61	26	28	セキュリティリスクはみられません。	۵
	C1150083-000064	2022/05/20 13:33	退 次	2022/05/13~2022/05/18	30 21	28	28	セキュリティリスクの恐れがあります。	0
	C1100003 003063	2022/05/17 17:33	週次	2022/05/10~-2022/05/15	30 Fi	28	28	セキュリティリスクの恐れがあります。	٥
Management Inc.	CI190083-003062	2922/05/16 09:57	15.2	2022/05/09~2022/05/14	39.23	28	28	セキュリティリスクの恐れがあります。	m

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。



図 8 分析結果レポート 詳細画面



端末分析結果

端末分析	端末分析NO:Cl200040-000009-000001										
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:eis	s-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 	イブ • 検知内容	 ログ収集日 	Q	検索							
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清報を検知 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\C urrentVersion\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 横展開 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									
タスクバ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。

SOMPO SHERIFF 管理 - 企業	管理者向	tt							0 🛓
	F	速報通知検索							
NAVIGATION 合 タッシュホード									
▶ 設定情報	+	施未名	通知日From		_				
🗐 端末情報	+	Q. 施东							
 ジャレポート発理 レポート一覧 送税通知検索 分析結果検索 	-	228	建来iD Internetingenetinge 6842100	ユーザーID 001	端未名 「No.4311004600	ユーザー名	通知日 2024-02-08	秋辺内容 セキュリティリスクの恐れがあります。	
 セキュリティ対策状況 	+								

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。

SOMPO SHERIFF 管理 - 企業	管理者向	1(†							⊘ ≗
	F	速報検知内容	P H						
NAVIGATION		総統的にアラートがあ	秋示される場合は、ヘルプデスクまで、お問合せください。						
合 ダッシュホード									
13/21846	+	分析結果							
三 端末情報	+								
※ 分析レポート管理 レポート一覧	-	アラートタイプ	- 930内容		- ログ収集日	Q 8	я		
违報通知検索 分析结果検索		No	被如内容	称初批		アラートタイプ	ログ 収集日時	対応内容	
セキュリティ対策状況	*	53009571	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。	不正なツールが検知されました。 イベントタイプ:security プロパイグ名:Microsoft-Windows-Eventlog イベントロ:1102 イベントログ作成時間:2024-02-06 09:40:53		製作	2024/02/07 09:11	Ü	
									_

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	ロしました。							
本アラート (イベントID:104、イベントID:110 ログの削除は、不正攻撃を隠蔽するため、実施され そのため、サイバー攻撃も疑われるため、アラー 検知詳細には、対象のイベントログを表示していま	2)は、イベントログ削除の検知になります。 1る可能性もございます。 ~として検知しております。 ます。							
検知詳細の見方								
例)表示値	補足內容							
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、 対象の端末に対してクリーンアップツール等の利用	問題ございません。 目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 何も心当たりがなく、継続してアラートが出る場合	とウイルス対策ソフトでのスキャンをお薦めします。 含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

SOMPO SHERIFF 代理 - 企業代理者向								
	分析結果検索							
AVIGATION	L-IK1-NO		IG-1-2/ENO					
9752#-F								
· 32.06	DK D PARK							
B 1884546 +					-			
0.00 x 1.000	64.6		621		Q. HE			
- HELA-LEA	(a. 12)	1.000		1211				
レポート一覧	湖东分析NO	226 220	2-9-10	3×8	2-9-8	100	63548	网络方法
进标进和快会	C1190063-000061-000001		001			2022/10/26 10:21	セキュリティリスクはみられません。	
201116-808-8	C1190083-000081-000002		001			2022/10/26 10:21	セキュリティリスクはみられません。	
3 セキュリティ対義状化 +	C1190083-00081-000803		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000004		001			2022/10/26 10 21	セキュリティリスクはみられません。	
	CITODER3 CODERT CODERS		100			2022/10/26 10:21	0+107-02043-5hatta.	
	C1190083-C00081-C00006		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	CI190083 000081 000067		001			2022/10/26 10:21	ゼキュリティリスクはみられません。	
	C1190083-000081-000008		002			2022/10/26 10:21	セキュリティリスクはかられません。	
	CI190063-000061-000009		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000010		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000011		001	10.000		2022/10/26 10:21	セキュリティリスクはみられません。	
	CI190083-000081-000012		901	10.010		2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000013		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000814		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000015		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190003-000001-000016	10.0	001.			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000017	100 100	001	10000		2022/10/26 10:21	セキュリティリスクはみられません。	
	CI190083-00081-000818	1011 1030	001			2022/10/26 10:21	セキュリティリスクはみられません。	
	C1190083-000081-000019		001			2022/10/26 10:21	セキュリティリスクはみられません。	
	(1192083-200283-000829		927	_		2022/10/26 10:21	##311#x112/08%655##4	

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。

SOMPO SHERIFF 管理 - 企業管理者向け											+
NAVIGATION						*					
合 ダッシュボード											
設定情報 +	+ 端末名		パッチ適用	状况	<u> </u>	Q. 68.4					
□ 建末情報 +											
注 分析レポート管理 +	端末名	05名	診断日	自動アップ デート	パッチ適 用状況	セキュリティボ リシー設定	監査 設定	ファイアウォ ール設定	LAPS	総合評価	
セキュリティ対策状況 -		Microsoft Windows 10 Pro	2023/08/05	有効	未選用	20/26	9/23	9/23		В	
セキュリティ診断結果	Real Providence	Microsoft Windows 10 Pro	2023/08/05	有効	適用清	21/26	8/23	9/23	•	В	
Microsoft Defender稼働状況	- 105 and	Microsoft Windows 10 Pro	2023/08/05	有効	未適用	21/26	8/23	9/23		В	
		Microsoft Windows 10 Pro	2023/08/05	有効	適用済	20/26	9/23	9/23	*	в	
© Sompo Risk Management Inc.	PGreek	Microsoft Windows 10 Pro	2023/07/29	有効	通用清	21/26	8/23	6/23	•	в	

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 稼動状況

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。											
SOMPO SHERIFF 管理 - 企業門	里和向的	t)≑									
		Microsoft I	Defender稼動状況								
NUMBETICN		NUT-IN AL									
# 9953#-F											
● 起之情報	e:	846			Manuarit Schenders 7680552	· 9.45					
□ 前未請請 □ 方前レポート管理	•	###5	Microsoft DefenderD碰数仪 兄	1>9>//-93	スパイウェア対策シグネチャのバーショ ン	ウィルス対策提盟ングネチャのバーショ ン	10件里 現	全てのダウンロードファイルのスキャ ン	MRX>S	ファイルやプログラムのアウティビティ目 調	リアルタイム症
C. and a lot of the second		1000	may .	1.1.19802.4	1.579.162.0	1.579 182.0	4120	R (1)	4603	1938 -	112
L CTIOTENMON			10.10 M				11120	8.9	10.75	III.D)	20
Marsson Defender#800008		1111	610	1.1.19703.2	1.377.16.0	1.377.16.0	1120	616s	math	610	112
		1111	neth	1.1.19501.2	1.073 THAT G	1.373.1681.0	98	68	有助	40h	432
			- MAR	1.1.19602.2	1.078.1202.0	1.375.1202.0	9120	102	418	0(0)	62
				1038	0000	82.5.5	#68	#i0	10.5	新幼	保治
			40	1.1.19300.2	1.358.154.0	1,369,154,0	998	50P	410	45.01	63.
			#41	0030	coap	0328	mia	9Eig	.00,10	無心	推动
		10.00	M 24				mito.	mai .	mit	無助	80
			BKA.				18150	WE23	3655	30.30	80
			40	1.1.18202.4	1.353.788.0	1.355.748.9	99.00	44	有战	4 /0	40
			2	D2	- 31 	15 C	12	2	15	*	24

図 13 Microsoft Defender 稼動状況画面



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 の稼動状況	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 稼動状況詳細

「Microsoft Defender の稼動状況」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 ⑦										
	端末情報 - PC-280759									
NAVIGATION	Microsoft Wi	indows 10 Pro								
- 決定情報 +	Microsoft Defender泰助 右动	UR.								
(1) 減末信報 +	19.00									
注 分析レホート管理 +	Microsoft Defender設定情	与報								
セキュリティ対策状況 -	分類	项目名	設定領							
セキュリティ診断結果	マルウェア対策	エンジンパージョン	1.1.23060.1005							
Microsoft Defender根始状况		製品パージョン	4.18.23050.9							
		エンジン	有効							
		サービスバージョン	4.18.23050.9							
	スパイウェア対策	スパイウェア対策保護	有効							
		スパイウェア対策シジネチャの実新経過日数	0							
© Sompo Risk Management Inc.		スパイウェア対策シジネチャの最終要新日時	2023/08/06 15:12							

図 14 Microsoft Defender 稼動状況詳細画面



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。

ESS 管理 - 企業管理者向け	Ø	•
	株式会社セキュアイノベーション様 分析状況	
 ▲ ダッシュホード ■ 設定協範 - 立実満用 	E ал 2012-У-В 41	
202-7- ■ 86483 • = 966-8-1480 • 2 07-148008 •	バッチ適用状況 バッチ適用状況 バッチ適用 ポ況 パッチ適用 ポ況	
	09% 0%26 (f) 0%26 (f) 53950 0%26 (f) 0%26 (f) 53950 0%26 (f) (f) (f) (f) 53950 0%26 (f) (f) (f) (f) (f) 53950 0%26 (f) (f) (f) (f) (f) (f)	
0 Secureirovation Inc.	54/94/95	-

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。

SOMPO	監視設定
	副 新新市(55
D235 -	
2.売請味 登録ユーゼー	
■ ##### +	MCPFLX)
Ⅲ 恐折レポート管理 +	WETFLAS
セキュリティ対策状況 ※	
	WCPFUX (
	オプション設定
	matiket

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。

EISS 管理 · 企業管理者向け		⊚ ≛
SOMPO	[2] K前中(15-]] [2]	
SHERIFF	I constanting	
A 40528-F	マント会社会部部	
- 121111	MMC2FEL21	
企業得受	01 90 20 02 00 11	
8181-5-	MMEPPL/3 1	
🖂 exttel +	01-00-36-01-50-45	
三 分析レポート常理 +	NBCPTUX:	
	02 00 55 03 55 43	
	オプション設定	
	RMRU RMRU	
	49,705 22	

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。

00-00-5E-00-53-01	
MACアドレス:	
00-00-5E-00-53-02	
MACアドレス:	
00-00-5E-00-53-03	

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。

有効なMACアドレスを設定してください(例 00-00-5E-00-53-FF)

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。

オプション設定	
速報通知	
キャンセル 変更	

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。

DSS 管理 - 企業管理者向け		÷
	株式会社セキュアイノベーション様 分析状況	
 А Уураж-К В 22550 - К 		
立た清苑		
- HAUSE +	パッチ適用状況 Microsoft Defenderの有効化状況	
Ξ 966-к-1-88 +	No.7 28/104 No.7 28/103 SHO SHO <th></th>	
C laurebauglin IV.	お知らせ ^{WEERPORESE}	
C DEGLEGROWTER DE.		

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。

監視設定
図 転車ボリシー
C UDAUTER
12 ネット曲線を取
99(27 %-X)
WK77FL-2,1
MACTY LOC.
オプション設定
Weilard

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。

SOMPO	22 11月10日
SHERIFF	
合 ダッシュボード	🔽 Poj-Fanekon II.
22254# -	M577623
之意消除	
発酵ユーザー	WKC7FL-Z:
(2) 現本情報 +	
Ⅲ 分析レポート管理 +	WKZ?FLZ1
☐ #\$±07+MEMR +	
	940.7 F (2.2 K det 1922 F 4
	オプション設定
	aniasi
	4e>ds 28
@ SecureInnovation Inc.	

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。 \??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	
速報通知	
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。

EISS 管理 - 企業管理者向け		0 🛓
CEISSS Endpoint Incident Scanning Service ↑ ダッシュホード ・ 記述技術 +	株式会社セキュアイノベーション様 分析状況	
⇒ 分析レポート管理 + ご セキュリティ対所状況 + ② アクセス制限 - IPアドレス掛洗制限	バッチ適用状況 バッチ適用状況 バッチ適用状況 バッチ適用状況 バッチ適用 785 バッチ適用 785 バッチ適用 785 「パッチ適用 785 パッチ適用 785 「パッチ適用 785 「パッチ」の 「パッチ」の 「パッチ」の 「パッチ」の 「パッチ」の 「パッチ」の 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パッチョーの 「パーの 「 「パーの 「 「 「パーの 「 「 「 「 「 「 「 「 「 「 「 「 「	4 1 84
© SecureInnovation Inc.	お知らせ WRan-oosNot	-

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。

EISS 管理 - 企業管理者向け							0 =
Endpoint Incident Scanning Serv		IPアドレス接	統制限				
脅 ダッシュホード							● IPアドレス接続時間通知
▶ 設定情報	+	(Pアドレスを入力)	してください	● 備考を入力してください		Q. (8):8	
🗐 端末情報	+						
注 分析レポート管理	+		IPPFDX		66.7	163	
セキュリティ対策状況	+	成当9 67 9 2 使来	1. K. C.				
アクセス制限	-						
IPアドレス接続制限							

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。

EISS 管理 - 企業管理者向け		0	
Endpoint Incident Scanning Se	D rvice	IPアドレス接続制限-追加	
骨 ダッシュホード		IPアドレス: 192.02.0/4	
● 設定情報	+		
📃 端末情報	+	++>ts	
三 分析レポート管理	+		
🚦 セキュリティ対策状況	+		
● アクセス制限	-		
IP アドレス 接続 制限			

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。

	設定情報	+	
۲	端末情報	+	4920/ 201
=	分析レポート管理	+	
	セキュリティ対策状況	+	
0	アクセス制限		遠加しました!
	IPアドレス接続制限		-18A83 807188173

図 30 登録完了画面

※ご注意※

403 <sup>
</sup> 管理者へお問い合わせください。 IPアドレスは で す。 Cutode

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

CS2400007