SOMPO SHERIFF

セキュリティレポートマニュアル

SOMPOリスクマネジメント株式会社

作 成 日	2020年5月7日
最 終 更 新 日	2022年1月20日

第1.2版

目次

■ 目次 .1
■ セキュリティレポートマニュアルについて .2
■ SOMPO SHERIFF 有料サービスのご案内 .2
■ 表紙 .2
■ 1.総合評価 .3
■ 2.診断結果
□ 2.診断結果 - 診断項目別判定 .4
□ 2.診断結果 - 診断項目別詳細 .5
□ 2.診断結果 - パソコン別 .6
■ 3.項目別検出一覧
□ 3.項目別検出一覧 - 危険度の高い不正プログラム .6
□ 3.項目別検出一覧 - 不正プログラム .7
□ 3.項目別検出一覧 - 不正プログラム配布サイト .7
□ 3.項目別検出一覧 - フィッシングサイト .8
□ 3.項目別検出一覧 - 悪意のあるサイト .8
□ 3.項目別検出一覧 - 安全とは言えないサイト .9
□ 3.項目別検出一覧 - Wi-Fi 接続(SSID 別) .9
□ 3.項目別検出一覧 - Wi-Fi 接続(パソコン別) .10
□ 3.項目別検出一覧 - USB 接続 .10
□ 3.項目別検出一覧 -インストールされたプログラム .11
□ 3.項目別検出一覧 - Disk 故障予兆 .11
■ パソコン動作記録(ログ)の収集状況一覧について .12
■ 今後の対応策 .14
■ よくあるご質問 .14
■ さいごに .15
■ サポート情報 .15

セキュリティレポートマニュアルについて

セキュリティレポートマニュアルは、『セキュリティレポート』の各項目について説明しています。

※セキュリティレポートは、SOMPO SHERIFF を導入したパソコンからログを収集し、収集したログを元に分析を行い、
脅威関連情報及び端末関連情報並びにこれに係る評価等を記載したレポートです。

SOMPO SHERIFF 有料サービスのご案内

有料サービスには Light プラン 及び 標準プラン の 2 つのプランがございます。
サービス内容およびレポート内容は下記のとおりとなります。

【サービス内容】

	Lightプラン	標準プラン
初期費用	1社 0円	1社 38,500円(税込み)(初年度のみ)
サービス利用料(月額)	パソコン1台 550円(税込み)	パソコン1台 1,650円(税込み)
検知・緊急アラート	○	○
セキュリティレポート	○	◎ ※エンジニアによる詳細調査別評価
脅威ハンティング	駆除業者紹介	○
ハンティング費用	自己負担	保険補償

※SOMPO SHERIFF 有料サービスにつきましては、
セキュリティレポートと併せて CSV ファイルをご提供します。

※○→過検知が含まれます。
※◎→過検知精査をします。

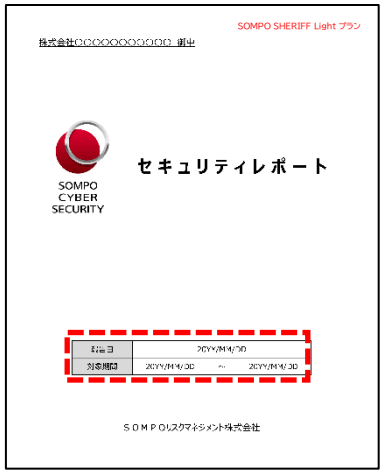
【レポート内容】

項目	パソコン無料セキュリティ診断	Lightプラン	標準プラン
総合評価	○	○	◎
診断結果-診断項目別判定	○	○	◎
診断結果-診断項目別詳細	ー	ー	◎
診断結果-パソコン別	ー	○	◎
危険度項の不正プログラム	○	◎	◎
不正プログラム	○	○	◎
不正プログラム配布サイト	○	○	◎
フィッシングサイト	○	○	◎
悪意のあるサイト	○	○	◎
安全とは言えないサイト	○	○	◎
Wi-Fi接続(SSID別)	◎	◎	◎
Wi-Fi接続(パソコン別)	◎	◎	◎
USB接続	◎	◎	◎
インストールされたプログラム	◎	◎	◎
Disk故障予兆	◎	◎	◎
CSV	ー	○	◎

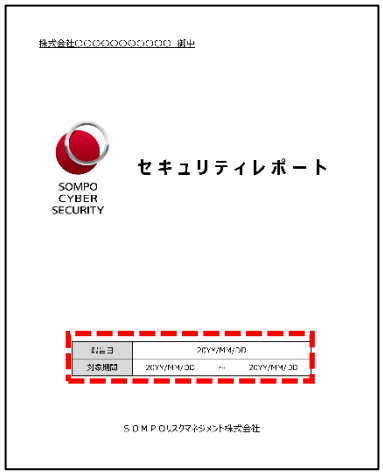
表紙

【パソコン無料セキュリティ診断】

【SOMPO SHERIFF Light プラン】



【SOMPO SHERIFF 標準プラン】



①対象期間

レポート作成の対象としたログの収集期間を指しています。
・パソコン無料セキュリティ診断:導入日～1ヵ月後
・有料サービス:ご契約日～3ヵ月毎(3 ヶ月間)

1.総合評価

【パソコン無料セキュリティ診断】○ 【Light プラン】○ 【標準プラン】○

②総合評価・評価基準

『不正プログラムの有無』と『感染ルートの状況』の2つの面から評価をしています。

総合評価	評価内容
A	不正プログラム・感染ルートともに問題なし。継続して現在の状態を維持する
B	不正プログラムは検知されなかったが、感染ルートの問題が検出されている
C	危険度が低いと考えられる不正プログラムを検知。緊急性は低いが、対策を講じることが必要
D	「危険度高」の不正プログラムを 1 台のパソコンで検知。速やかな対策・予防策が必要
E	「危険度高」の不正プログラムを複数台のパソコンで検知。速やかな対策・予防策が必要

③総合評価に関するご説明

各々の総合評価に関する説明を表示しています。

また、総合評価に対して弊社が推奨する予防策として、システム面での予防策」と「②人的側面での予防策」の2つの面における策を記載しています。

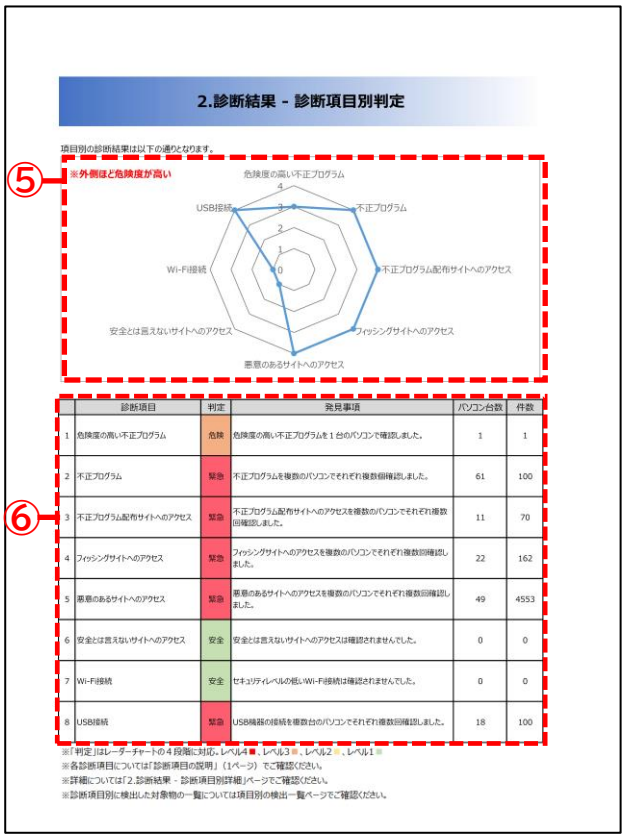
④「危険度の高い不正プログラム」の検知数

総合評価が **D・E** の場合、「危険度高の不正プログラム」の検知数を表示いたします。

2.診断結果

2.診断結果 - 診断項目別判定

【パソコン無料セキュリティ診断】○ 【Light プラン】○ 【標準プラン】○



⑤レベル

レーダーチャートは下記判定基準に基づいた
各診断結果の判定レベルを示しています。

診断項目	危険度高の不正プログラム	その他
レベル1	安全	安全
レベル2	-	経過観察
レベル3	危険	要注意
レベル4	緊急	危険

※パソコン無料セキュリティ診断および
SOMPO SHERIFF Light プランでは、
以下の項目に過検知が含まれます。

項目	
・危険度高の不正プログラム （パソコン無料セキュリティ診断のみ） ・診断結果 – パソコン別 ・不正プログラム	・不正プログラム配布サイトへのアクセス ・フィッシングサイトへのアクセス ・悪意のあるサイトへのアクセス ・安全とは言えないサイトへのアクセス

⑥診断項目別判定

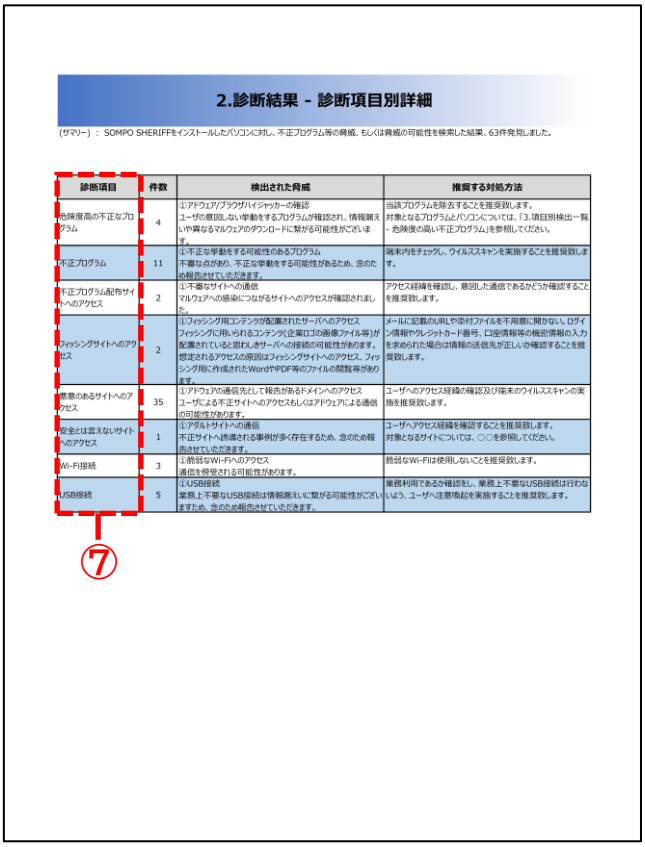
診断項目とそれに対する各々の判定基準は、下記のとおりです。

	診断項目	レベル1（安全）	レベル2	レベル3（危険）	レベル4（緊急）
1	危険度の高い不正プログラム	検知されない	-	1台の PC で検知	複数台の PC で検知

	診断項目	レベル1（安全）	レベル2（経過観察）	レベル3（要注意）	レベル4（危険）
2	不正プログラム	検知されない	1台の PC で検知	複数の PC で検知	複数の PC で それぞれ複数個検知
3	不正プログラム配布サイトへのアクセス	検知されない	1台以上の PC で それぞれ1回検知	1台の PC で 複数回検知	複数の PC で 複数回検知
4	フィッシングサイトへのアクセス	検知されない	1台以上の PC で それぞれ1回検知	1台の PC で 複数回検知	複数の PC で 複数回検知
5	悪意のあるサイトへのアクセス	検知されない	1台以上の PC で それぞれ1回検知	1台の PC で 複数回検知	複数の PC で 複数回検知
6	安全とは言えないサイトへのアクセス	検知されない	1台以上の PC で それぞれ1回検知	1台の PC で 複数回検知	複数の PC で 複数回検知
7	Wi-Fi 接続	検知されない	1台以上の PC で それぞれ1回検知	1台の PC で 複数回検知	複数の PC で 複数回検知
8	USB 接続	検知されない	1台以上の PC で それぞれ1回検知	1台の PC で 複数回検知	複数の PC で 複数回検知

2.診断結果 - 診断項目別詳細

【パソコン無料セキュリティ診断】×【Light プラン】×【標準プラン】○



2.診断結果 - 診断項目別詳細

(サマリー) : SOMPO SHERIFFをインストールしたパソコンに対し、不正プログラム等の脅威、もしくは脅威の可能性を検索した結果、63件発見しました。

診断項目	件数	検出された脅威	推奨する対処方法
危険度高の不正なプログラム	4	①アドウェア/ブラウザハイジャッカーの確認 ユーザの意図しない挙動をするプログラムが確認され、情報漏えいや異なるマルウェアのダウンロードに繋がる可能性がございます。	当該プログラムを除去することを推奨致します。 対象となるプログラムとパソコンについては、「3.項目別検出一覧 - 危険度の高い不正プログラム」を参照してください。
不正プログラム	11	①不正な挙動をする可能性のあるプログラム 不審な点があり、不正な挙動をする可能性があるため、念のため報告させていただきます。	端末内をチェック、ウイルススキャンを実施することを推奨致します。
不正プログラム配布サイトへのアクセス	2	①不審なサイトへの通信 マルウェアへの感染につながるサイトへのアクセスが確認されました。	アクセス経緯を確認し、意図した通信であるかどうか確認することを推奨致します。
フィッシングサイトへのアクセス	2	①フィッシング用コンテンツが配置されたサーバへのアクセス フィッシングに用いられるコンテンツ(企業ロゴの画像ファイル等)が配置されていると思われるサーバへの接続の可能性があります。 想定されるアクセスの原因はフィッシングサイトへのアクセス、フィッシング用に作成されたWordやPDF等のファイルの閲覧等があります。	メールに記載のURLや添付ファイルを不用意に開かない、ログイン情報やクレジットカード番号、口座情報等の機密情報の入力を求められた場合は情報の送信先が正しいか確認することを推奨致します。
悪意のあるサイトへのアクセス	35	①アドウェアの通信先として報告があるドメインへのアクセス ユーザによる不正サイトへのアクセスもしくはアドウェアによる通信の可能性があります。	ユーザへのアクセス経緯の確認及び端末のウイルススキャンの実施を推奨致します。
安全とは言えないサイトへのアクセス	1	①アダルトサイトへの通信 不正サイトへ誘導される事例が多く存在するため、念のため報告させていただきます。	ユーザへアクセス経緯を確認することを推奨致します。 対象となるサイトについては、○○を参照してください。
Wi-Fi接続	3	①脆弱なWi-Fiへのアクセス 通信を傍受される可能性があります。	脆弱なWi-Fiは使用しないことを推奨致します。
USB接続	5	①USB接続 業務上不要なUSB接続は情報漏えいに繋がる可能性がございますため、念のため報告させていただきます。	業務利用であるか確認をし、業務上不要なUSB接続は行わないよう、ユーザへ注意喚起を実施することを推奨致します。

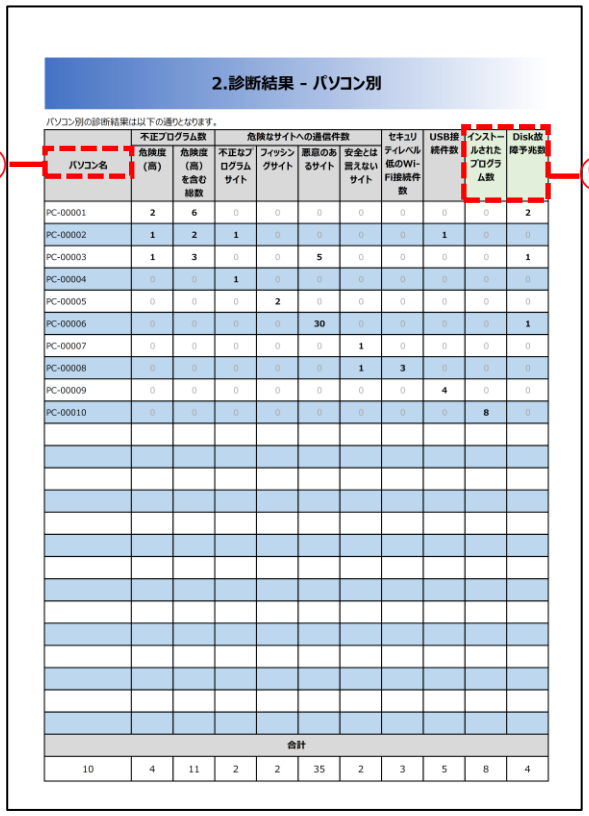
⑦

⑦診断項目

診断項目	内容
危険度高の不正プログラム	不正プログラムの中でも遠隔操作型ウイルス、情報漏えい型ウイルス、不正送金型ウイルス、ファイル改ざんの機能を有すると考えられる不正プログラム。 その他、事業継続上重大なリスクをもたらすと考えられる、危険度の高いウイルスの可能性があるプログラム。
不正プログラム	不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称。
不正プログラム配布サイトへのアクセス	アクセスすることで不正プログラムがダウンロードされるサイト、または不正プログラムがダウンロードされる可能性があるサイト。
フィッシングサイトへのアクセス	フィッシングサイト(正規のサイトに似せて作った偽の Web サイト)と思われる Web サイト。アクセスすると正規の Web サイトになりすましたサイトが表示され、アカウント情報やクレジットカード情報を入力してしまうと、それらを悪用される恐れがあります。
悪意のあるサイトへのアクセス	Web を閲覧した際に、不正広告が表示されたり PC が乗っ取られてしまうなど、ユーザに悪影響を及ぼす危険性のあるサイト。また、過去にマルウェアが配布されていた可能性のあるもの。
安全とは言えないサイトへのアクセス	「悪意のあるサイト」より、ウイルスを引き起こす可能性は低いが、ハッキングされている可能性があり、アクセスには十分注意が必要であるサイト。
Wi-Fi 接続	安全性の低い Wi-Fi への接続や、暗号化されていない Wi-Fi の接続は通信の内容が盗み見され、情報漏えいの恐れが高いため注意が必要です。
USB 接続	USB 機器が接続された回数。マルウェアの感染経路として USB メモリが多く発見されています。どのパソコンにどんな USB 機器が接続されたかを確認することができるため、USB の使用の管理としてお使いいただけます。

2.診断結果 - パソコン別

【パソコン無料セキュリティ診断】× 【Light プラン】○ 【標準プラン】○



2.診断結果 - パソコン別

パソコン別の診断結果は以下の通りとなります。

パソコン名	不正プログラム数 危険度（高）	不正プログラム数 危険度（高）を含む総数	危険なサイトへの通信件数 不正なプログラムサイト	危険なサイトへの通信件数 フィッシングサイト	危険なサイトへの通信件数 悪意のあるサイト	危険なサイトへの通信件数 安全とは言えないサイト	セキュリティレベル低のWi-Fi接続件数	USB接続件数	インストールされたプログラム数	Disk故障予兆数
PC-00001	2	6	0	0	0	0	0	0	0	2
PC-00002	1	2	1	0	0	0	0	1	0	0
PC-00003	1	3	0	0	5	0	0	0	0	1
PC-00004	0	0	1	0	0	0	0	0	0	0
PC-00005	0	0	0	2	0	0	0	0	0	0
PC-00006	0	0	0	0	30	0	0	0	0	1
PC-00007	0	0	0	0	0	1	0	0	0	0
PC-00008	0	0	0	0	0	1	3	0	0	0
PC-00009	0	0	0	0	0	0	0	4	0	0
PC-00010	0	0	0	0	0	0	0	0	8	0
合計										
10	4	11	2	2	35	2	3	5	8	4

⑧パソコン名

パソコン名（ホスト名）は、各々のパソコンの設定画面からご確認頂けます。

・[スタート] – [設定] – [システム] – [バージョン情報]

・[バージョン情報]にある「デバイス仕様」の

『**デバイス名**』がパソコン名となっております。

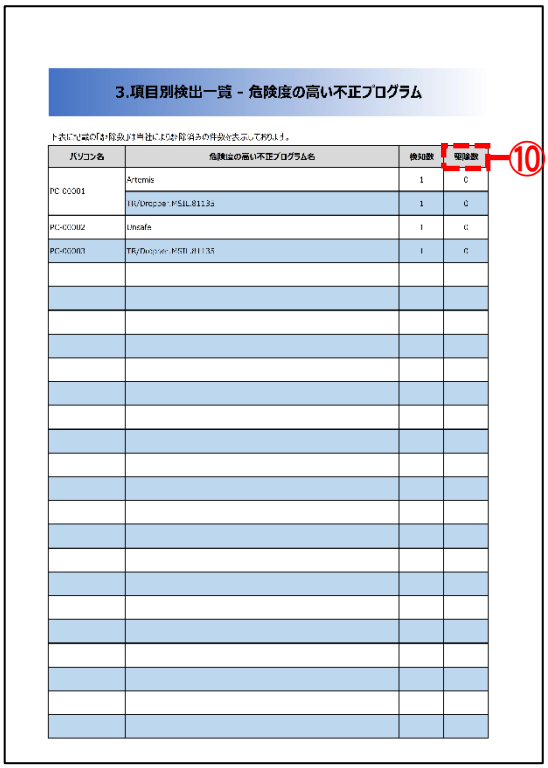
⑨インストールされたプログラム数・Disk 故障予兆

許可されていないプログラムやアプリケーションの管理等にお使い頂けます。

3.項目別検出一覧

3.項目別検出一覧 - 危険度の高い不正プログラム

【パソコン無料セキュリティ診断】○ 【Light プラン】○ 【標準プラン】○



3.項目別検出一覧 - 危険度の高い不正プログラム

下表にて端末の駆除が当社により駆除済の件数を表示しております。

パソコン名	危険度の高い不正プログラム名	検知数	駆除数
PC-00001	Artemis	1	0
	TR/Dropper.MSIL.81138	1	0
PC-00002	Uneafe	1	0
PC-00003	TR/Dropper.MSIL.81135	1	0

■ウイルス等不正なプログラムのうち、危険度が高いと考えられるプログラム、検出したパソコン名検知数、駆除数等に関する情報をご提供します。

■危険度が高い不正プログラムの早期駆除に向けた作業管理等にご活用いただけます。

⑩駆除数

緊急アラートにより通知され、当社提携会社にて駆除対応済の件数を表示します。

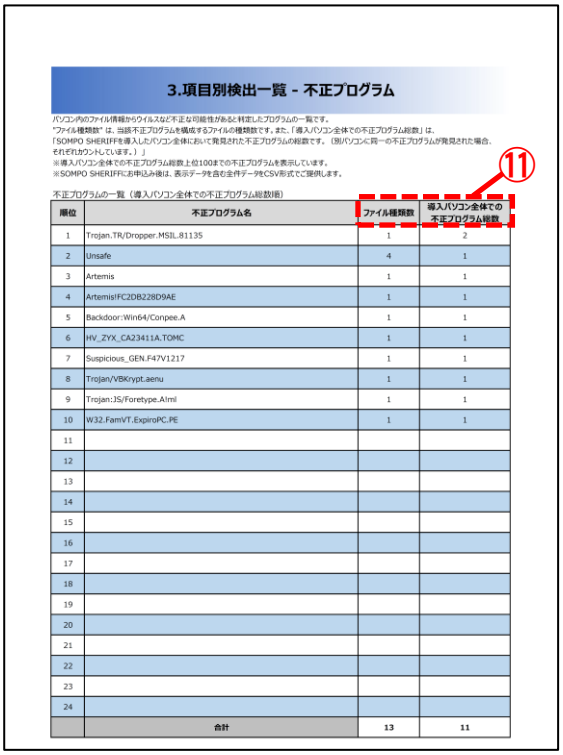
---＜パソコン無料セキュリティ診断をご利用のお客さま＞---

SOMPO SHERIFF 標準プランにお申込みいただきますと、弊社にて対象プログラムを無料で調査・駆除いたします。

なお、SOMPO SHERIFF Light プランにお申込みいただきますと、弊社から駆除業者を紹介いたします。

3.項目別検出一覧 - 不正プログラム

【パソコン無料セキュリティ診断】○【Light プラン】○【標準プラン】○



3.項目別検出一覧 - 不正プログラム

パソコン内のファイル情報からウイルスなど不正な可能性があると判定したプログラムの一覧です。
"ファイル種類数"は、当該不正プログラムを構成するファイルの種類数です。また、「導入パソコン全体での不正プログラム総数」は、「SOMPO SHERIFFを導入したパソコン全体において発見された不正プログラムの総数です。（当パソコンに同一の不正プログラムが発見された場合、それぞれカウントしています。）」
※導入パソコン全体での不正プログラム総数上位100までの不正プログラムを表示しています。
※SOMPO SHERIFFにお申込み後は、表示データを含む全件データをCSV形式でご提供します。

⑪

不正プログラムの一覧（導入パソコン全体での不正プログラム総数順）

順位	不正プログラム名	ファイル種類数	導入パソコン全体での不正プログラム総数
1	Trojan.TR/Dropper.MSIL.81135	1	2
2	Unsafe	4	1
3	Artemis	1	1
4	Artemis!FC2DB228D9AE	1	1
5	Backdoor:Win64/Conpee.A	1	1
6	HV_ZYX_CA23411A.TOMC	1	1
7	Suspicious_GEN.F47V1217	1	1
8	Trojan/VBKrypt.aenu	1	1
9	Trojan:JS/Foretype.AIml	1	1
10	W32.FamVT.ExpiroPC.PE	1	1
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
	合計	13	11

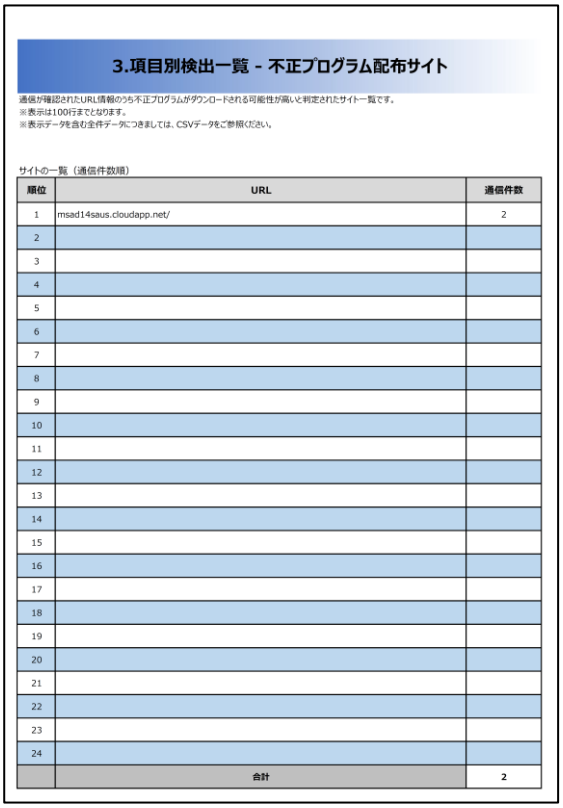
■危険度の高低問わず、不正プログラムの全量に関する情報をご提供します。
■不正プログラムを量的な側面で捉え、パソコン別等、様々な角度から分析することにより、感染の未然防止等に活用いただけます。

⑪ファイル種類数・導入パソコン全体での不正プログラム数

1つの不正プログラムが複数のファイルで形成されているケースもあります。

3.項目別検出一覧 - 不正プログラム配布サイト

【パソコン無料セキュリティ診断】○【Light プラン】○【標準プラン】○



3.項目別検出一覧 - 不正プログラム配布サイト

通信が確認されたURL情報のうち不正プログラムがダウンロードされる可能性が高いと判定されたサイト一覧です。
※表示は100行までとなります。
※表示データを含む全件データにつきましては、CSVデータをご参照ください。

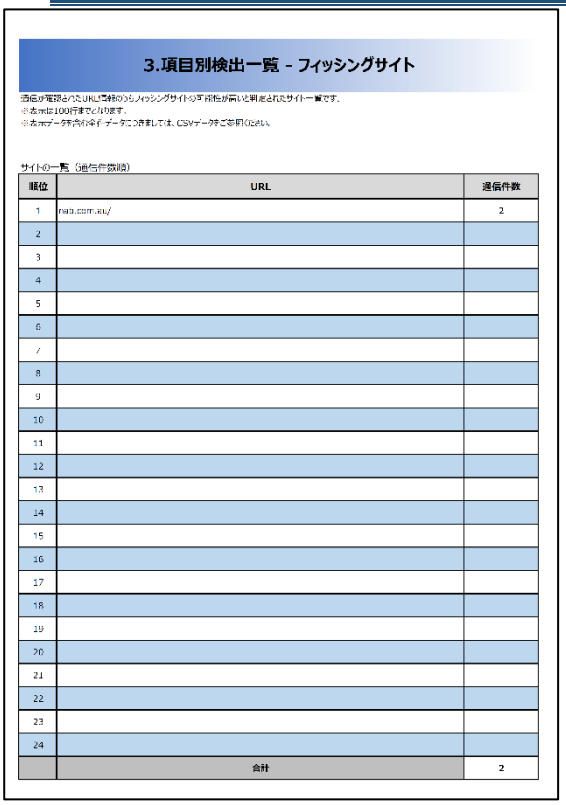
サイトの一覧（通信件数順）

順位	URL	通信件数
1	msad14saus.cloudapp.net/	2
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
	合計	2

■不正プログラムがダウンロードされるサイトへのアクセス状況をご提供します。
■アクセスすると、ウイルスやスパイウェアなど不正プログラムがダウンロードされ、パソコンが感染してしまう可能性があります。
■こうした状況をパソコン別等、様々な角度から分析することにより、感染の未然防止等に活用いただけます。

3.項目別検出一覧 － フィッシングサイト

【パソコン無料セキュリティ診断】○【Light プラン】○【標準プラン】○



3.項目別検出一覧 - フィッシングサイト

通信が確認されたURL情報のうちフィッシングサイトの可能性が高いと判定されたサイト一覧です。
※表示は100行までとなります。
※表示データを含む全件データにつきましては、CSVデータをご参照ください。

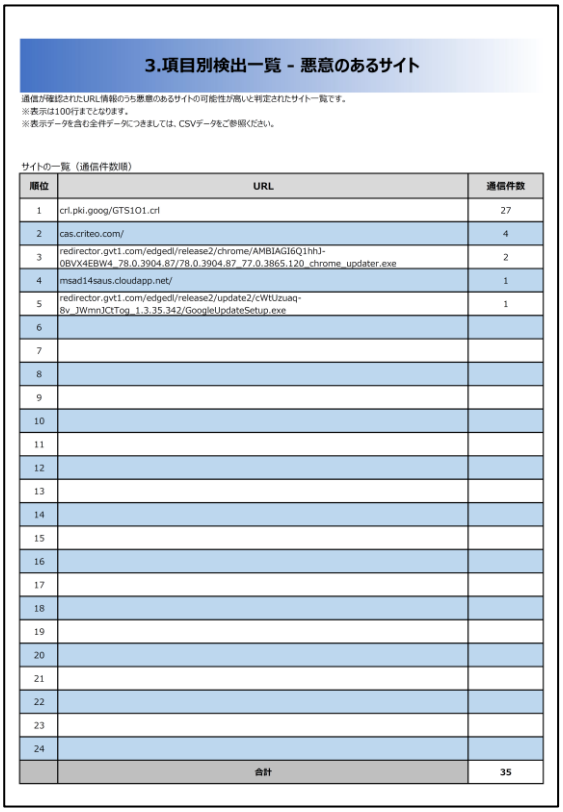
サイトの一覧（通信件数順）

順位	URL	通信件数
1	rsib.com.au/	2
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
	合計	2

■正規のサービスになりすました Web 上の詐欺サイトへのアクセス状況をご提供します。
■アクセスすると、正規の Web サイトになりすましたサイトが表示され、アカウント情報やクレジットカード情報を入力してしまうと、これらの情報を窃取され悪用される恐れがあります。
■こうした状況をパソコン別等、様々な角度から分析することにより、情報窃取の未然防止等に活用いただけます。

3.項目別検出一覧 － 悪意のあるサイト

【パソコン無料セキュリティ診断】○【Light プラン】○【標準プラン】○



3.項目別検出一覧 - 悪意のあるサイト

通信が確認されたURL情報のうち悪意のあるサイトの可能性が高いと判定されたサイト一覧です。
※表示は100行までとなります。
※表示データを含む全件データにつきましては、CSVデータをご参照ください。

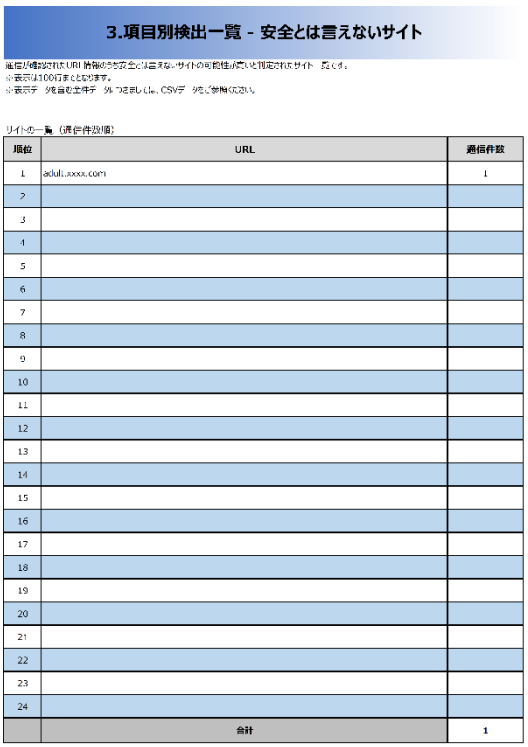
サイトの一覧（通信件数順）

順位	URL	通信件数
1	crl.pki.goog/GTS1O1.crl	27
2	cas.criteo.com/	4
3	redirector.gvt1.com/edgedl/release2/chrome/AMBIAGI6Q1hhJ-0BVX4EBW4_78.0.3904.87/78.0.3904.87_77.0.3865.120_chrome_updater.exe	2
4	msad14saus.cloudapp.net/	1
5	redirector.gvt1.com/edgedl/release2/update2/cWtUzuaq-8v_JWmnJCtTog_1.3.35.342/GoogleUpdateSetup.exe	1
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
	合計	35

■様々な悪意を持ったサイトへのアクセス状況をご提供します。
■アクセスすると、不正なスクリプトや脆弱性を利用した攻撃により、パソコンに様々な被害が及ぶ可能性があります。
■こうした状況をパソコン別等、様々な角度から分析することにより、被害の未然防止等に活用いただけます。

3.項目別検出一覧 － 安全とは言えないサイト

【パソコン無料セキュリティ診断】○ 【Light プラン】○ 【標準プラン】○



3.項目別検出一覧 - 安全とは言えないサイト

通信が確認されたURL情報のうち安全とは言えないサイトの可能性が高いと判定されたサイトを表示します。
☆表示は100行までとなります。
☆表示データを含む全件データはCSVデータをご参照ください。

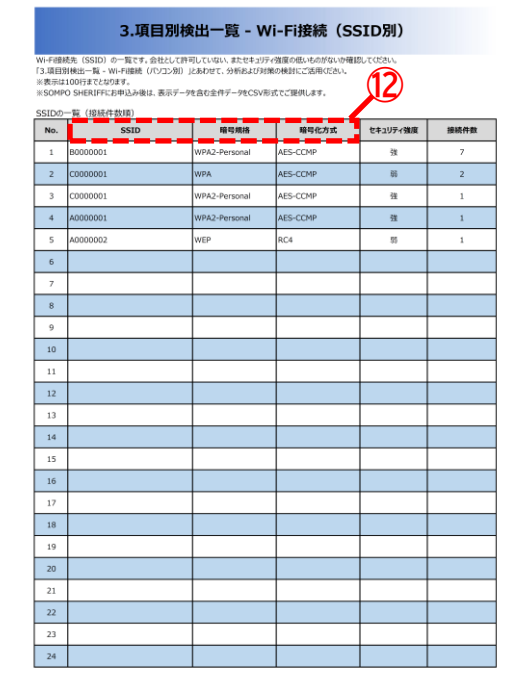
リストの一覧（通信件数順）

順位	URL	通信件数
1	adult.xxxx.com	1
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
	合計	1

■ハッキングされている可能性のある Web サイトへの
アクセス状況をご提供します。
■これらのサイトは、ハッキングにより
不正プログラム配布サイト、フィッシングサイト、
悪意のあるサイトに改ざんされている可能性があります。
■こうした状況をパソコン別等、様々な角度から分析する
ことにより、被害の未然防止等に活用いただけます。

3.項目別検出一覧 - Wi-Fi 接続（SSID 別）

【パソコン無料セキュリティ診断】○ 【Light プラン】○ 【標準プラン】○



3.項目別検出一覧 - Wi-Fi接続（SSID別）

Wi-Fi接続先（SSID）の一覧です。会社として許可していない、またセキュリティ強度の低いものがないか確認してください。
「3.項目別検出一覧 - Wi-Fi接続（パソコン別）」とあわせて、分析および対策の検討にご活用ください。
※表示は100行までとなります。
※SOMPO SHERIFFにお申込み後は、表示データを含む全件データをCSV形式でご提供します。

⑫

SSIDの一覧（接続件数順）

No.	SSID	暗号規格	暗号化方式	セキュリティ強度	接続件数
1	B0000001	WPA2-Personal	AES-CCMP	強	7
2	C0000001	WPA	AES-CCMP	弱	2
3	C0000001	WPA2-Personal	AES-CCMP	強	1
4	A0000001	WPA2-Personal	AES-CCMP	強	1
5	A0000002	WEP	RC4	弱	1
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					

■Wi-Fi 接続の全量および、このうちセキュリティレベルの
低い接続に関する情報をご提供します。
■セキュリティレベルの低い接続は、通信傍受や不正侵入の
ターゲットにされる可能性があります。
■こうした状況を接続先（SSID）別/パソコン別等、
様々な角度から分析することにより、被害の未然防止等に
活用いただけます。

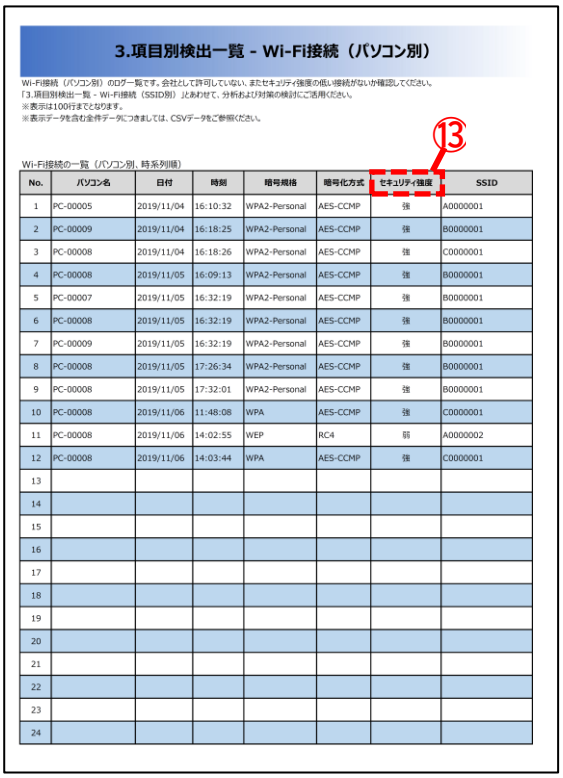
※p.10 のパソコン別と併せてご覧ください。

⑫SSID・暗号規格・暗号方式

SSID	Wi-Fi に接続するときの、接続先となる ルーター等の基地局名
暗号規格	無線 LAN の暗号化の際の規格である セキュリティ方式
暗号化方式	通信の暗号化の方法

3.項目別検出一覧 – Wi-Fi 接続(パソコン別)

パソコン無料セキュリティ診断】○ 【Light プラン】○ 【標準プラン】○



3.項目別検出一覧 - Wi-Fi接続（パソコン別）

Wi-Fi接続（パソコン別）のログ一覧です。会社として許可していない、またセキュリティ強度の低い接続がないか確認してください。
「3.項目別検出一覧 - Wi-Fi接続（SSID別）」とあわせて、分析および対策の検討にご活用ください。
※表示は100行までとなります。
※表示データを含む全件データにつきましては、CSVデータをご参照ください。

⑬

Wi-Fi接続の一覧（パソコン別、時系列順）

No.	パソコン名	日付	時刻	暗号規格	暗号化方式	セキュリティ強度	SSID
1	PC-00005	2019/11/04	16:10:32	WPA2-Personal	AES-CCMP	強	A0000001
2	PC-00009	2019/11/04	16:18:25	WPA2-Personal	AES-CCMP	強	B0000001
3	PC-00008	2019/11/04	16:18:26	WPA2-Personal	AES-CCMP	強	C0000001
4	PC-00008	2019/11/05	16:09:13	WPA2-Personal	AES-CCMP	強	B0000001
5	PC-00007	2019/11/05	16:32:19	WPA2-Personal	AES-CCMP	強	B0000001
6	PC-00008	2019/11/05	16:32:19	WPA2-Personal	AES-CCMP	強	B0000001
7	PC-00009	2019/11/05	16:32:19	WPA2-Personal	AES-CCMP	強	B0000001
8	PC-00008	2019/11/05	17:26:34	WPA2-Personal	AES-CCMP	強	B0000001
9	PC-00008	2019/11/05	17:32:01	WPA2-Personal	AES-CCMP	強	B0000001
10	PC-00008	2019/11/06	11:48:08	WPA	AES-CCMP	強	C0000001
11	PC-00008	2019/11/06	14:02:55	WEP	RC4	弱	A0000002
12	PC-00008	2019/11/06	14:03:44	WPA	AES-CCMP	強	C0000001
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							

⑬セキュリティ強度

セキュリティ強度は、暗号規格と暗号化方式の組み合わせによって決まります。

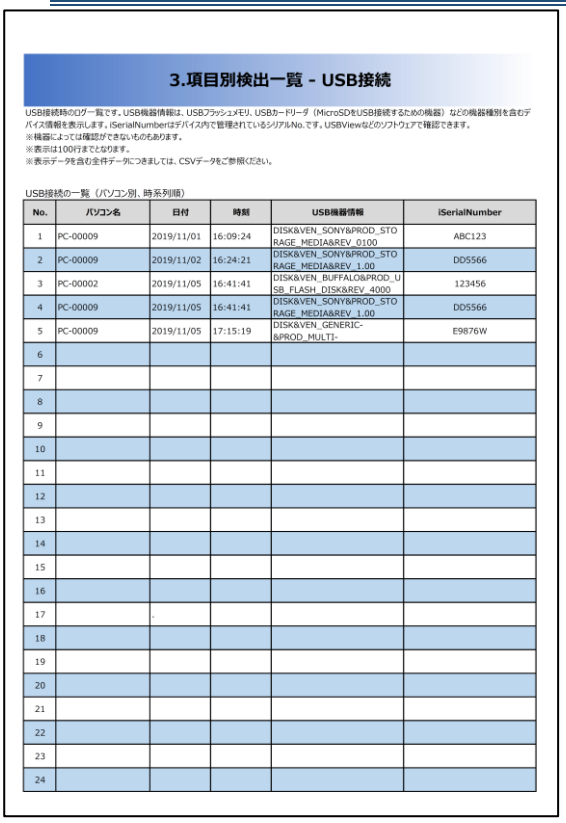
【セキュリティ強度の判定基準】

暗号規格	WPA2、WPA2-Personal
暗号化方式	AES、AES-CCMP

・暗号規格と暗号化方式の組み合わせの要素がそれぞれ上記のものである　→**「強」**
・その他の組み合わせ　→**「弱」**

3.項目別検出一覧 – USB 接続

【パソコン無料セキュリティ診断】○ 【Light プラン】○ 【標準プラン】○



3.項目別検出一覧 - USB接続

USB接続時のログ一覧です。USB機器情報は、USBフラッシュメモリ、USBカードリーダ（MicroSDをUSB接続するための機器）などの機器種別を含むデバイス情報を表示します。iSerialNumberはデバイス内で管理されているシリアルNo.です。USBViewなどのソフトウェアで確認できます。
※機器によっては確認ができないものもあります。
※表示は100行までとなります。
※表示データを含む全件データにつきましては、CSVデータをご参照ください。

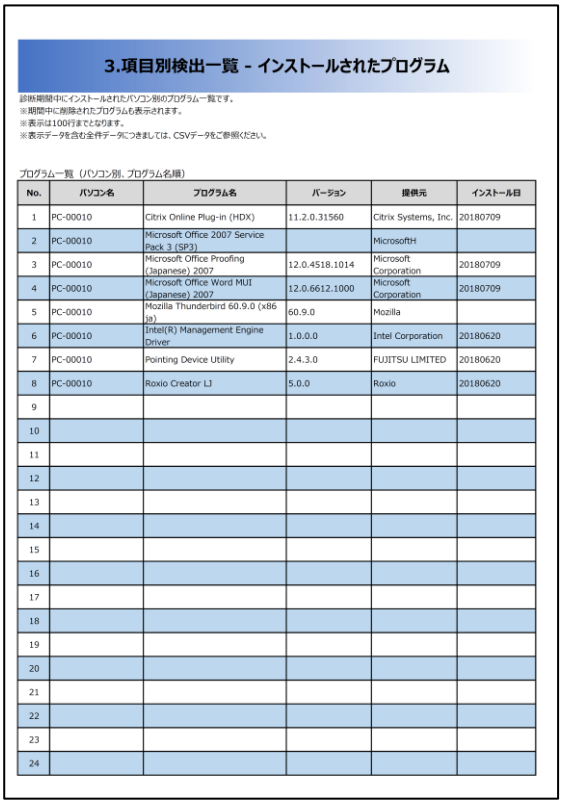
USB接続の一覧（パソコン別、時系列順）

No.	パソコン名	日付	時刻	USB機器情報	iSerialNumber
1	PC-00009	2019/11/01	16:09:24	DISK&VEN_SONY&PROD_STORAGE_MEDIA&REV_0100	ABC123
2	PC-00009	2019/11/02	16:24:21	DISK&VEN_SONY&PROD_STORAGE_MEDIA&REV_1.00	DD5566
3	PC-00002	2019/11/05	16:41:41	DISK&VEN_BUFFALO&PROD_USB_FLASH_DISK&REV_4000	123456
4	PC-00009	2019/11/05	16:41:41	DISK&VEN_SONY&PROD_STORAGE_MEDIA&REV_1.00	DD5566
5	PC-00009	2019/11/05	17:15:19	DISK&VEN_GENERIC-&PROD_MULTI-	E9876W
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					

■USB 接続に関して件数や接続日時等に関する情報をご提供します。
■無許可の USB 機器の使用によるウイルス持ち込みや、社外への個人情報の大量持ち出し等の可能性があります。
■こうした状況をパソコン別等、様々な角度から分析することにより、感染や情報漏えいの未然防止等に活用いただけます。

3.項目別検出一覧 – インストールされたプログラム

【パソコン無料セキュリティ診断】○【Light プラン】○【標準プラン】○



3.項目別検出一覧 - インストールされたプログラム

診断期間中にインストールされたパソコン別のプログラム一覧です。
※期間中に削除されたプログラムも表示されます。
※表示は100行までとなります。
※表示データを含む全件データにつきましては、CSVデータをご参照ください。

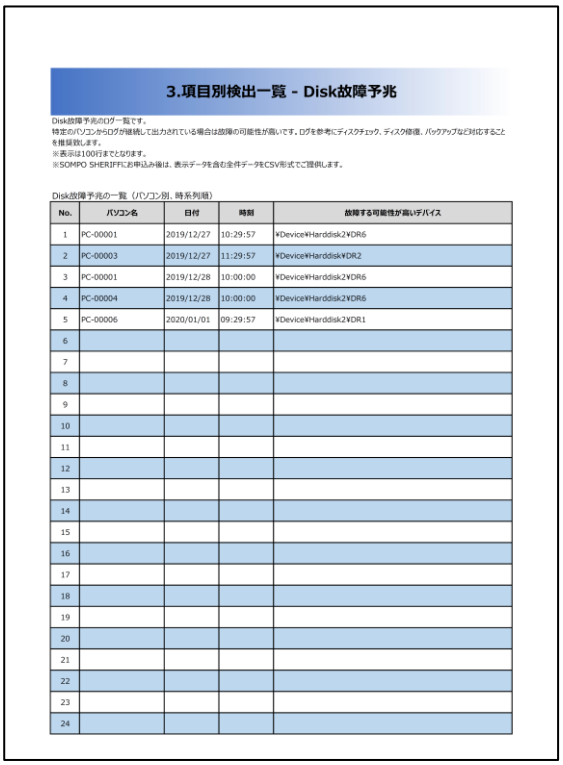
プログラム一覧（パソコン別、プログラム名順）

No.	パソコン名	プログラム名	バージョン	提供元	インストール日
1	PC-00010	Citrix Online Plug-in (HDX)	11.2.0.31560	Citrix Systems, Inc.	20180709
2	PC-00010	Microsoft Office 2007 Service Pack 3 (SP3)		MicrosoftH	
3	PC-00010	Microsoft Office Proofing (Japanese) 2007	12.0.4518.1014	Microsoft Corporation	20180709
4	PC-00010	Microsoft Office Word MUI (Japanese) 2007	12.0.6612.1000	Microsoft Corporation	20180709
5	PC-00010	Mozilla Thunderbird 60.9.0 (x86 ja)	60.9.0	Mozilla	
6	PC-00010	Intel(R) Management Engine Driver	1.0.0.0	Intel Corporation	20180620
7	PC-00010	Pointing Device Utility	2.4.3.0	FUJITSU LIMITED	20180620
8	PC-00010	Roxio Creator LJ	5.0.0	Roxio	20180620
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					

■パソコン上のプログラム名、バージョンアップや導入日時等に関する情報をご提供します。
■脆弱なバージョンのプログラムや会社未承認の通信プログラム等により、不正なサイトへのアクセス、ウイルス感染、情報漏えい、ライセンス違反等の可能性があります。
■こうした状況をパソコン別等、様々な角度から分析することにより、会社未承認のプログラムの除去や不正導入の牽制等に活用いただけます。

3.項目別検出一覧 - Disk 故障予兆

【パソコン無料セキュリティ診断】○【Light プラン】○【標準プラン】○



3.項目別検出一覧 - Disk故障予兆

Disk故障予兆のログ一覧です。
特定のパソコンからログが継続して出力されている場合は故障の可能性が高いです。ログを参考にディスクチェック、ディスク修復、バックアップなど対応することを推奨致します。
※表示は100行までとなります。
※SOMPO SHERIFFにお申込み後は、表示データを含む全件データをCSV形式でご提供します。

Disk故障予兆の一覧（パソコン別、時系列順）

No.	パソコン名	日付	時刻	故障する可能性が高いデバイス
1	PC-00001	2019/12/27	10:29:57	¥Device¥Harddisk2¥DR6
2	PC-00003	2019/12/27	11:29:57	¥Device¥Harddisk¥DR2
3	PC-00001	2019/12/28	10:00:00	¥Device¥Harddisk2¥DR6
4	PC-00004	2019/12/28	10:00:00	¥Device¥Harddisk2¥DR6
5	PC-00006	2020/01/01	09:29:57	¥Device¥Harddisk2¥DR1
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				

■Windows のイベントログから Disk 故障予兆のログが検知されたホストの一覧です。
■どのパソコンが故障の危険性があるのかを確認できます。
■予兆が発生したパソコンは早急に修理やデータのバックアップを行って頂くことをご検討ください。

パソコン動作記録(ログ)の収集状況一覧について （2022 年 1 月から提供開始）

直近 1 か月間のパソコン動作記録(ログ)の収集状況が確認できる『パソコン動作記録(ログ)の収集状況一覧』について説明します。

パソコン動作記録(ログ)の収集状況一覧(202XXX16-202XXX15)

				木	水	火	月	日	土	金	⑤
①	②	③	④	12							
ホスト名	会社名	契約種別	ログ種別	9	8	7	6	5	4	3	
PC-001	○○○○株式会社	標準	通信								
PC-001	○○○○株式会社	標準	ファイル								
TARO-PC	○○○○株式会社	標準	通信								⑥
TARO-PC	○○○○株式会社	標準	ファイル								
Hanako-PC	○○○○株式会社	標準	通信								
Hanako-PC	○○○○株式会社	標準	ファイル								⑦
Keiri-PC	○○○○株式会社	ライト	通信								
Keiri-PC	○○○○株式会社	ライト	ファイル								
eigyo	○○○○株式会社	ライト	通信								⑧
eigyo	○○○○株式会社	ライト	ファイル								
soumu	○○○○株式会社	ライト	通信								
soumu	○○○○株式会社	ライト	ファイル								⑨

① ホスト名

SOMPO SHERIFF をインストールされているパソコン名です。

【ホスト名確認手順】

1.「Windows キー」を押してください

2.「cmd」と入力してエンターボタンを押してください

3. 更に「hostname」と入力してください

4. ホスト名が表示されます

② 会社名

貴社名が記載されております。

③ 契約種別

SOMPO SHERIFF の契約プランが記載されております。

標準プランの場合‥「標準」

Light プランの場合‥「ライト」

④ ログ種別

SOMPO SHERIFF をインストールした端末から取得しているログ(パソコンの動作記録)の種別を記載しております。

通信　　:パソコンがブラウザなどでアクセス(通信)をする場合のログです
ファイル :パソコン内のファイルに書き込み処理などが行われた場合に出るログです

⑤ 日付

ログ取得期間における日付を表示しています。

＜ ⑥ ～ ⑨ ＞

ログが到着している場合はセルに色がついております。
以下、ログの取得状況の確認方法について、例示します。

⑥【正常に動作しています】

通信のログとファイルのログが到着している状態です。SOMPO SHERIFF は正常に動作しております。(一部、ログが到着していない日につきましては、休日等でパソコンの利用をしていない状態と考えられます。)

⑦【ご利用環境要確認】

全てのログが届いていない状況です。
既に対象のパソコンをご利用されていない、パソコンを入れ替えている、または SOMPO SHERIFF をアンインストールしたパソコンの可能性が考えられます。
また対象のパソコンを業務でご利用、かつインターネットに接続している状態で、この状態が発生している場合は、パソコンの環境を確認させて頂くことがございます。

(注)
VPN をご利用になられている場合、製品の仕様上、「通信ログ」は届きません。

⑧【正常に動作しております】

過去にログが到着していない状態が見受けられますが、一時的なもので、最新時点ではログが到着しているため正常に動作しております。

⑨【ご利用環境要確認】

ログが到着していない状態が継続しています。
この状態が発生している場合は、パソコンの環境を確認させて頂くことがございます。

(注)
VPN をご利用になられている場合、製品の仕様上、「通信ログ」は届きません。

今後の対応策

＜「危険度の高い不正プログラム」が検知されたお客さま＞

【パソコン無料セキュリティ診断のお客さま】

ウイルスに感染しているパソコンから情報漏えいや、ファイル改ざんなどにより業務に支障をきたす恐れがありますので、早急に駆除が必要です。

SOMPO SHERIFF 標準プランにお申込みいただきますと、弊社にて対象プログラムを無料で調査・駆除いたします。

なお、SOMPO SHERIFF Light プランにお申込みいただきますと、弊社から駆除業者を紹介いたします。

＜「危険度の高い不正プログラム」以外の項目で件数が表示されているお客さま＞

【パソコン無料セキュリティ診断のお客さま】

SOMPO SHERIFF にてパソコンを引き続き監視することにより、リスクを可視化して万が一に備えておくことをお勧めします。

よくあるご質問

Q.	A.
部署単位でレポートを発行してもらえないか？	いたしかねます。部署単位でご契約いただく必要がございます。
個人名を特定できるか？	ホスト名での特定は可能ですが、 個人名とホスト名を紐づけられません。
インストールされているプログラムについて、 ソフトウェアバージョンを確認できるか？	バージョンまでの確認は可能ですが、 それが最新かどうかの判定はできません。
フィッシングサイトへの接続があったようだが、 どのような情報が搾取されたかを特定できるか？	特定することはできません。 別途フォレンジック等で詳細な調査を行う必要があります。
不正なプログラムサイトと悪意あるサイトとの違いは？	不正なプログラムサイトはウイルスをダウンロードしてしまうようなサイトです。 悪意あるサイトは PC の脆弱性を利用して攻撃してきてしまうようなサイトです。
USB メモリ上のファイル情報を取得することは可能か？	できません。あくまでも接続の状態を確認しているのみとなります。
端末を入れ替えたがレポート監視対象に入っているか？	SOMPO SHERIFF をインストールしていただければ 監視/レポート対象に入ります。
台数の増減はどうなるのか。 増加した場合でもレポートには情報が出るのか。	更新時に台数の増減を確認します。 また同一のインストーラを使って台数が増加した場合であれば、 レポートには反映されます。
危険度の高いプログラムが発見されたけど 教えていただいたファイルパスに見当たらない。	既に入っているウイルス対策製品により隔離済の可能性が ございます。
不正なプログラムサイトや悪意のサイト項目も注意すべきか？	サイトの項目も注意していただく必要がございます。 サイトをきっかけにウイルスが入ってくるケースもございます。

さいごに

セキュリティ対策は、継続して状況を把握しリスクを早期発見、早期対応することが重要です。
パソコンのセキュリティ対策はウイルス対策ソフトだけでは、防げない時代になってきています。
ウイルス対策ソフトでは、新種のウイルスなどの場合、パターンファイルに反映されるまでに時間を要する場合があります。
SOMPO SHERIFF では、新種のウイルスも、日々の監視により早期発見が可能です。

ウイルスは常に進化しています。
御社のセキュリティ対策に、進化した次世代型セキュリティ対策「SOMPO SHERIFF」をぜひお役立てください。

サポート情報

SOMPO SHERIFF に関するお問い合わせは、下記連絡先までご連絡ください。

SOMPO リスクマネジメント株式会社
サイバーセキュリティ事業本部

Mail：somposheriff@sompo-rc.co.jp