SOMPO CYBER SECURITY

サイバー攻撃の実態と対策に関するサービス例のご紹介（ お助け隊事業の事例から）

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

本日の目次

１．サイバー攻撃の実態
千葉県　サイバーセキュリティお助け隊での観測結果のご紹介

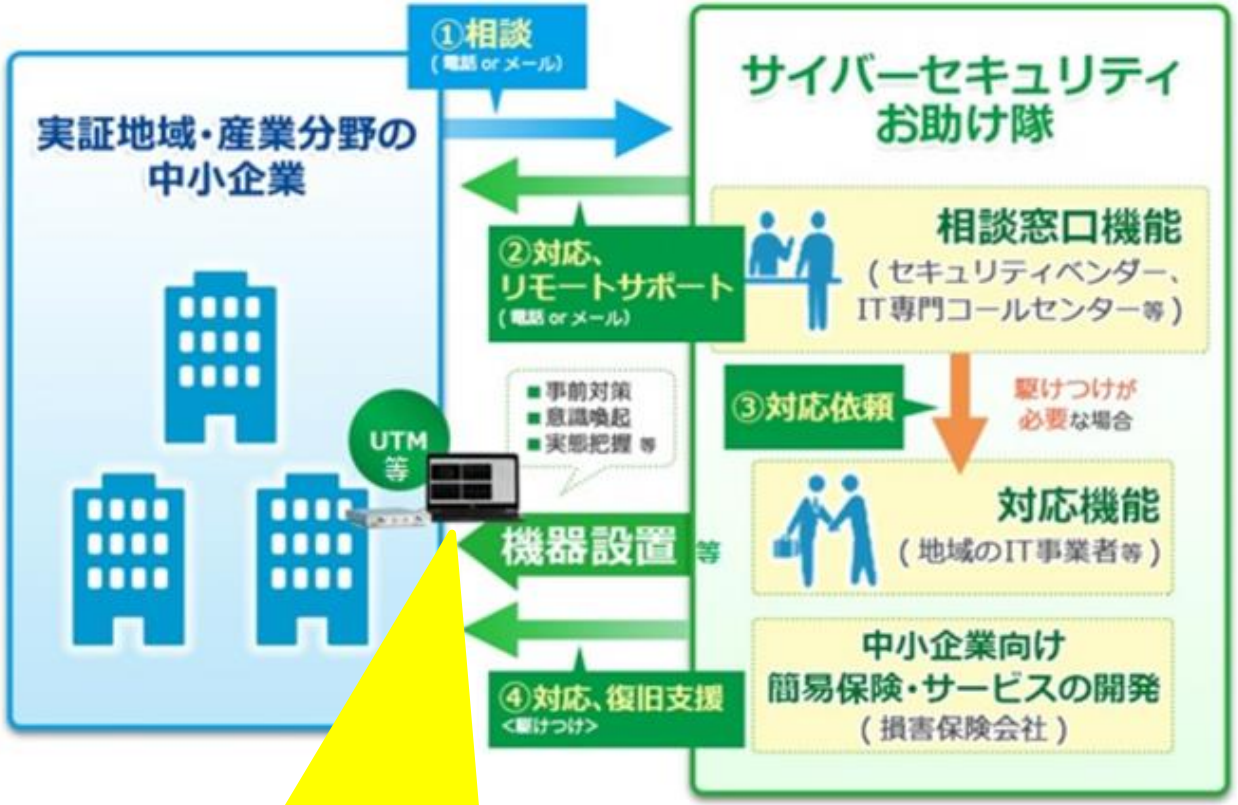
２．すぐにはじめられる対策のご紹介
サイバーセキュリティお助け隊サービス『SOMPO SHERIFF』

１.サイバー攻撃の実態

千葉県　サイバーセキュリティお助け隊での観測結果のご紹介

千葉県　サイバーセキュリティお助け隊について

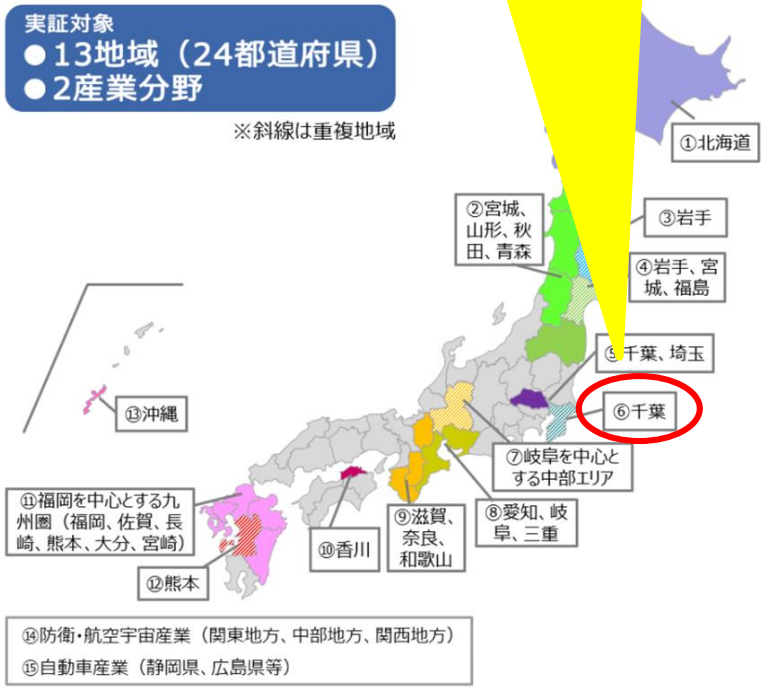
サイバーセキュリティお助け隊事業のイメージ



実際にサイバー攻撃を観測

SOMPOは千葉県で実施

令和2年度の実施地域



出典：独立行政法人情報処理推進機構

© 2020 Sompo Risk Management Inc. All rights reserved.

千葉県での実証参加事業者

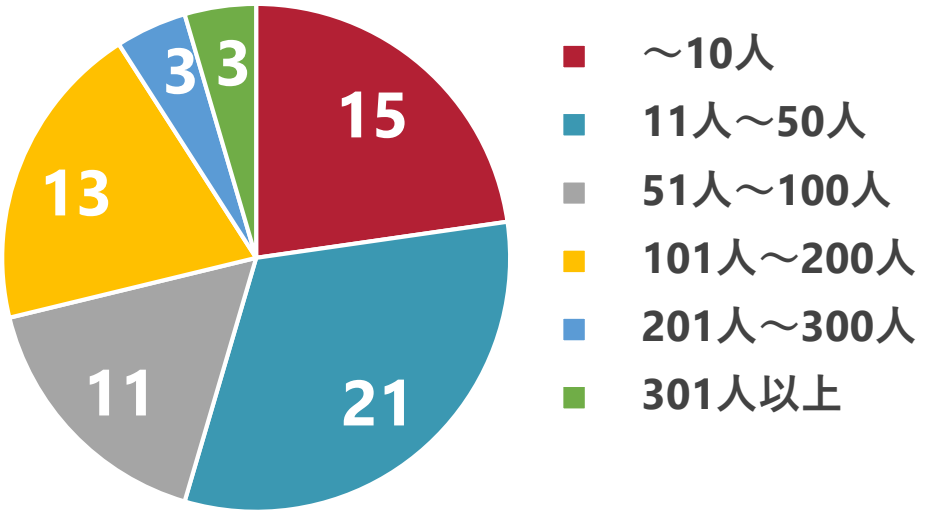
千葉県内に事業所を構える66社が参加

業種別

	業種分類	社数
D	建設業	11
E	製造業	11
R	サービス業（他に分類されないもの）	11
H	運輸業、郵便業	8
P	医療、福祉	6
J	金融業、保険業	5
I	卸売業、小売業	4
K	不動産業、物品賃貸業	4
L	学術研究、専門・技術サービス業	2
G	情報通信業	1
N	生活関連サービス業、娯楽業	1
Q	複合サービス事業	1
T	分類不能の産業	1
総計		66

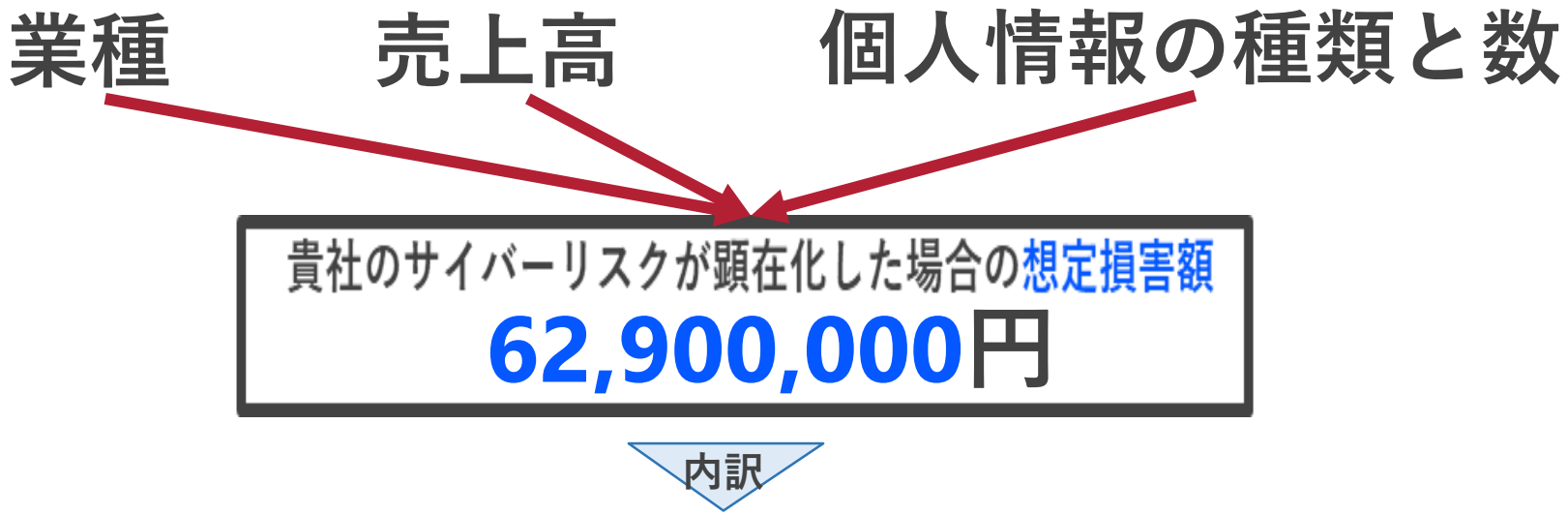
※「日本標準産業分類」の大分類による分類

従業員人数別



© 2020 Sompo Risk Management Inc. All rights reserved.

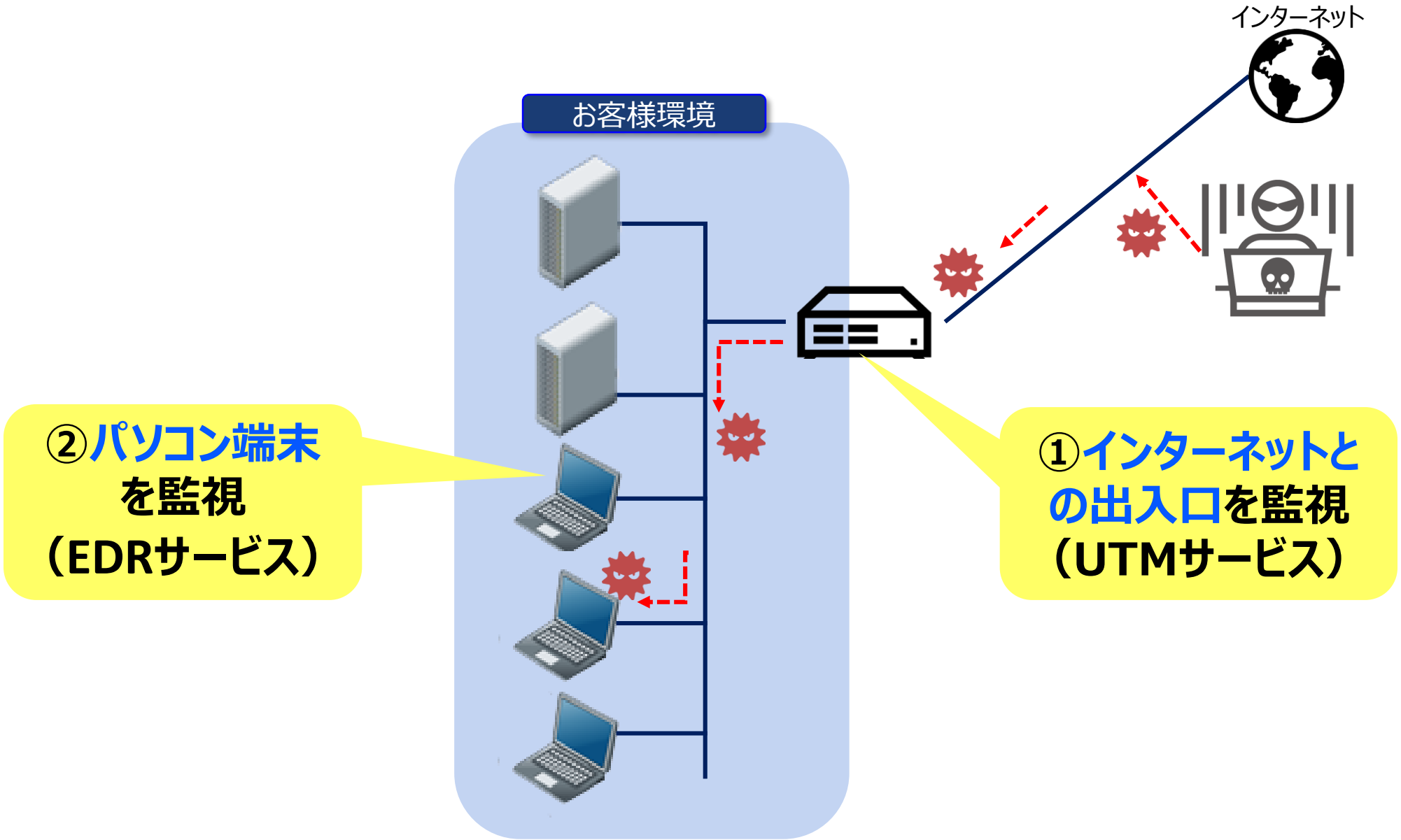
サイバー事故発生時の想定損害額（セキュリティに関するアンケートより）



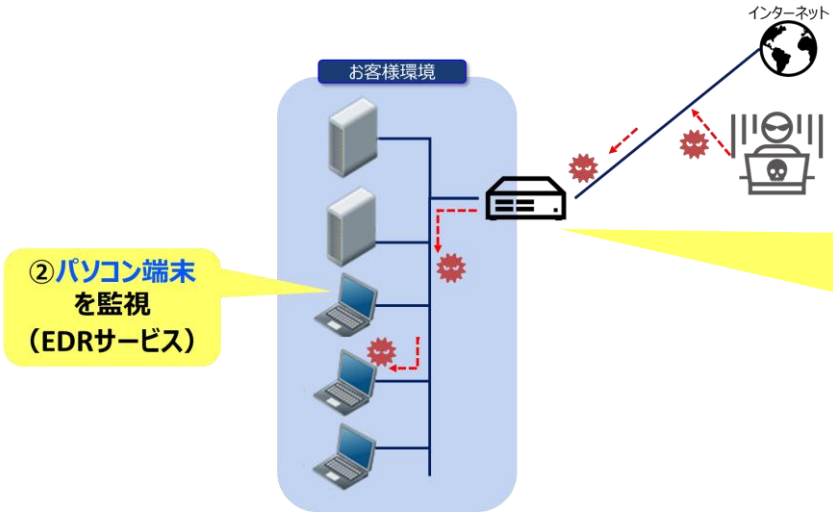
損害賠償費用	6,130,000円	情報漏えいやシステム障害・停止に起因して損害賠償を請求された場合の損害賠償金および賠償請求に関する訴訟対応費用
事故対応費用	9,320,000円	サイバー攻撃を受けたかどうかや攻撃を受けた場合の影響範囲や原因を調査するための費用（フォレンジック費用）やデータ・ソフトウェアの復旧費用、応急処置や再発防止のためのセキュリティ強化費用
お詫び対応費用	10,060,000円	個人情報が漏えいしたお客さまに対するお詫び文章やお詫びのしるし（お見舞金・金券）の送付とその諸経費
売上機会損失額	37,390,000円	サイバー攻撃に起因してECサイトや社内システムの停止によって、業務が停止し、本来得られるはずだった売り上げ機会の損失額

© 2021 Sompo Risk Management Inc. All rights reserved.

サイバー攻撃の観測方法



①インターネットとの出入口での観測結果（UTMサービス）



①インターネットとの出入口を監視

使用したUTM
WatchGuard社 FireBox

観測した主な攻撃	観測した件数
スパムメール（迷惑メール）	**67,080件**
外部からの攻撃など不正な通信	**490件**
ウイルス感染等の可能性がある不正なサイトへのアクセス	**118,141件**

© 2021 Sompo Risk Management Inc. All rights reserved.

【参考】UTMサービス　監視結果　　スパムメールとは

スパムメール・迷惑メールの種類

種類		特徴等
広告宣伝メール		出会い系・アダルト系サイト、サービスや商品販売などに関する広告する内容のメール。 予測されやすいメールアドレスである場合や、他の迷惑メールに記載されたURLへのアクセス等をきっかけになり送られてくる。
架空請求メール		知らないサイトから突然「情報料の請求」や「自宅まで回収しに行く」といった内容のメールが送られてくるケース 業者は適当なメールアドレスにランダムに送っているにすぎないので、無視をして問題ないのがほとんど。
詐欺・なりすましメール		
	フィッシング詐欺	ネットバンキングやクレジットカード会社、有名企業になりすまして個人情報等をだましとる 企業からのメールを装って本物そっくりに偽装したホームページへ誘導し、ログインID、パスワード、クレジットカード番号などの個人情報を入力させ窃取する。
	なりすましメール	パソコンメールは、メールソフトで送信者アドレスを自由に設定できることを利用して、知り合いや有名企業などを装った「なりすましメール」を送信する手法。
	ウイルスメール	メールを開いたときに気づかれないようパソコンに侵入し乗っ取ってしまうボットウイルスを仕込んだメール。 乗っ取られてしまったパソコンは、ボットウイルスに感染した他のパソコンと共にボットネット（パソコン群）の一部となり、外部の司令塔から遠隔操作を受けて大量の迷惑メールを世界中に送信してしまうようになる。

© 2021 Sompo Risk Management Inc. All rights reserved.

【参考】外部からの不正な通信の内容

UTMが検知した外部から内部に向けられた不正な通信の主な内容

WEBクロスサイトスクリプティングの通信 ・この攻撃は、標的サイト（例:SNSや掲示板など）では無く、**そのサイトを利用したエンドユーザに、なりすましやID/パスワード盗用などの被害を与える可能性がある。**	64件
WEBクロスサイトスクリプティング(cookieの盗難)の試みの通信 ・この攻撃は、標的サイト（例:SNSや掲示板など）では無く、**そのサイトを利用したエンドユーザに、cookieに保存された情報の盗用などの被害を与える可能性がある。**	33件
Photodex ProShow Producer 5.0.3256 バッファオーバーフローの脆弱性を狙った通信 ・この脆弱性を利用されると、**パソコンの乗っ取り、誤作動、他のパソコンを攻撃するなどの被害が発生する可能性がある。**	21件
WEBディレクトリトラバーサルの脆弱性を狙った通信 ・この脆弱性を利用されると、**本来アクセスできないファイルを閲覧・ダウンロードされる等により、情報漏洩が発生する可能性がある。**	16件

© 2021 Sompo Risk Management Inc. All rights reserved.

【参考】アクセスが確認されたウイルス感染等の可能性がある不正なサイト

検知数トップ５の内容

	カテゴリー	件数	
1	Games	42,723	■ゲームサイトへのアクセス ・ユーザーがゲームをプレイまたはダウンロードできるようにするサイトへのアクセス。 ・セキュリティ上、望ましくない可能性のあるソフトウェアをインストールされる可能性がある。
2	Social Web - Facebook	16,068	■Facebookへのアクセス ・Facebookへのアクセス。 ・業務上必要性が低いサイトへのアクセスをブロックした。 ・マルウェアに感染する恐れがある。
3	Sex	13,603	■成人/アダルトコンテンツサイトへのアクセス ・アダルトコンテンツを含むサイトへのアクセス ・マルウェアに感染したり、詐欺サイトや脅迫サイトに誘導される恐れがある。
4	Elevated Exposure	7,699	■不正の可能性の高いサイトへのアクセス ・本来の性質を偽造している、または潜在的な悪意を示唆する要素を含むサイトへのアクセス。 ・マルウェア感染、情報窃取などの恐れがある。
5	Potentially Unwanted Software	6,129	■望ましくない可能性のあるソフトウェアをインストールされるサイトへのアクセス ・予期しない影響を及ぼす可能性のあるアプリケーションをインストールできるサイトへのアクセス。 ・自端末へのパフォーマンス負荷の増加や、マルウェア感染、情報窃取などの恐れがある。

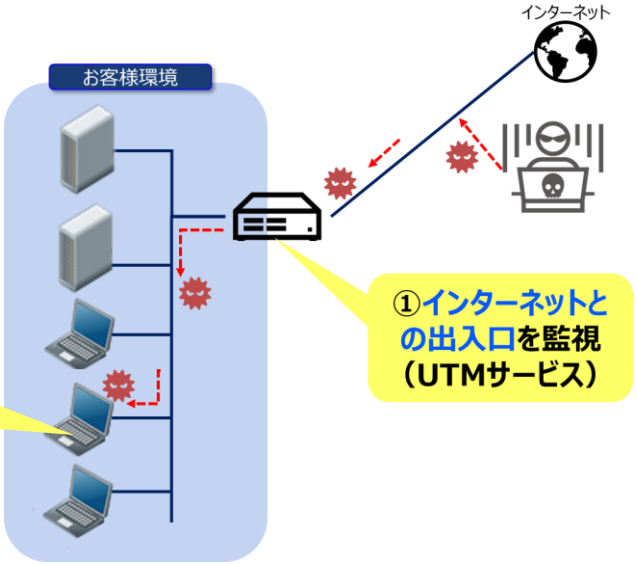
© 2021 Sompo Risk Management Inc. All rights reserved.

②パソコン端末での観測内容（EDRサービス）

②パソコン端末を監視
※一部のパソコンが対象

使用したEDR

SOMPO SHERIFF

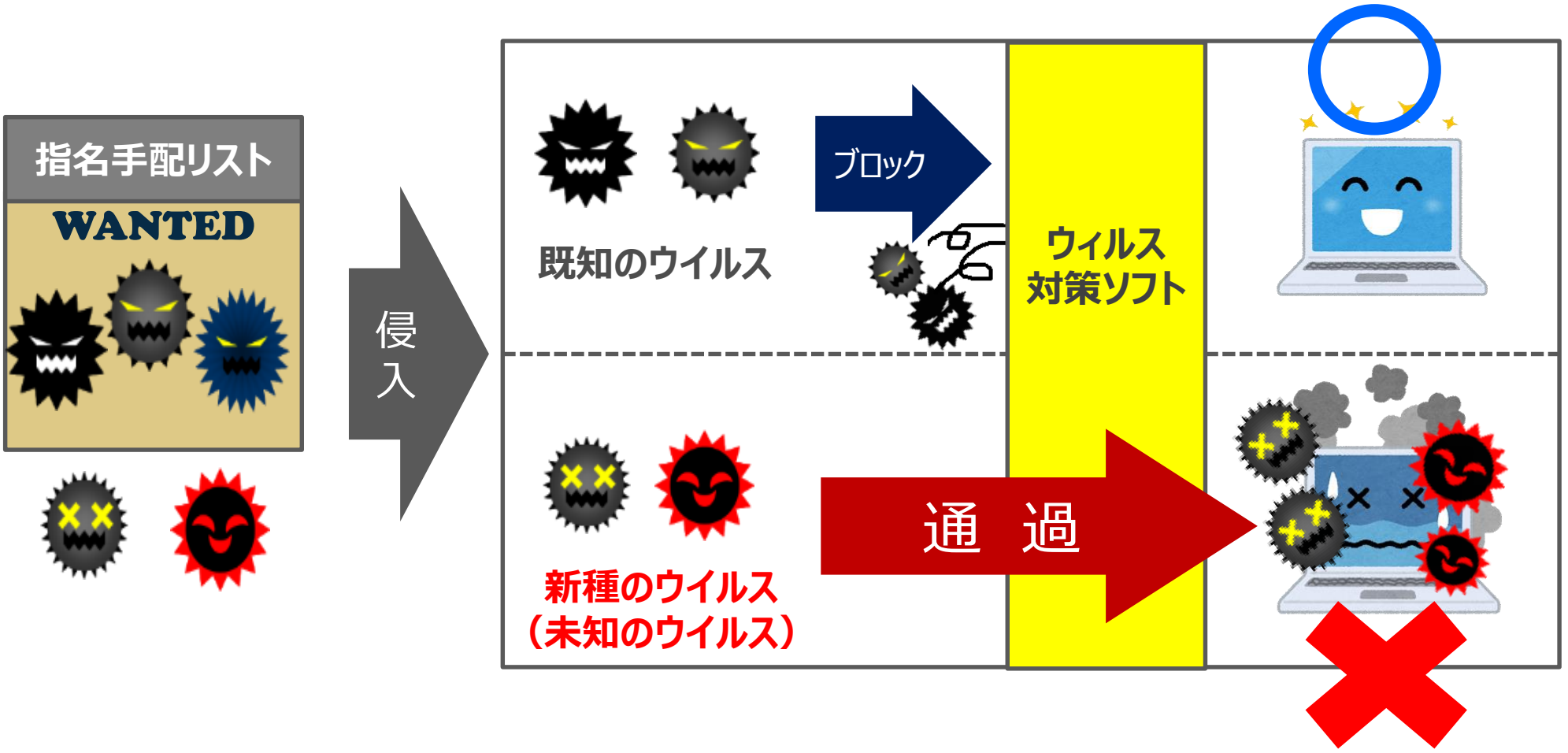


観測した主な攻撃	観測した件数
ウイルスなどの不正なプログラム	**4,122件**
ウイルス感染等の可能性がある不正なサイトへのアクセス	**891件**
パスワードの掛かっていない安全性の低いWi-Fi接続	**46件**

© 2020 Sompo Risk Management Inc. All rights reserved.

２.すぐにはじめられる対策のご紹介
サイバーセキュリティお助け隊サービス『SOMPO SHERIFF』

ウイルス対策ソフトを通過してしまうウイルスがある



『 新種のウイルス 』はウイルス対策ソフトをすり抜けてしまう

© 2021 Sompo Risk Management Inc. All rights reserved.

SOMPO SHERIFF のご紹介

© 2021 Sompo Risk Management Inc. All rights reserved.

特徴１ 『安心』

すり抜けてくるウイルスを解析検知・復旧支援

SOMPO SHERIFFは、送信ログ、ディレクトリ作成履歴などを監視し、不審な挙動をチェックします。
ウイルス対策ソフトをすり抜け潜伏した**新種のウイルスも挙動を監視し検知**します。
加えて、標準プランでは、検知したウイルスをハンティング（駆除）！
この際の駆除費用は保険で補償されるため、更に安心！（Lightプランには保険による補償は付帯しません。）

駆け付け駆除 技術的な知識を有しないお客さまを対象とすることを前提としていますので、「遠隔対応の可否」と「駆け付けの有効性」を踏まえた上でお客さまと協議し、駆け付け支援を行うかどうかを決定します。(交通費は別途必要になります。)

※Lightプランの脅威ハンティングは当社からの駆除業者紹介となります。

© 2021 Sompo Risk Management Inc. All rights reserved.

【ご参考】サイバー攻撃による被害イメージ

侵入後、ウイルス対策ソフトの監視をすり抜けて攻撃が始まった場合…

自社のみならず、
顧客や取引先にも広がる損害

ID・パスワードが盗まれ、
個人情報や取引先の機密情報が外部に流出！

オンライン・バンキングの乗っ取りによる不正送金で、取引先への支払が不能に！

大切なファイルが強制的に暗号化されて、業務が停止！

乗っ取られたパソコンが取引先のシステムへの攻撃に悪用され、取引停止に！

© 2021 Sompo Risk Management Inc. All rights reserved.

特徴２　簡単

パソコンに
ソフトウェアをインストールするだけ！

解析検知・復旧支援を実現するSOMPO SHERIFFの導入はソフトウェアをインストールするだけ。
インストール後は自動的に監視をスタートし
パソコンに侵入した「危険そうなプログラムやソフトウェア」をセキュリティレポートで報告します。

※ レポートの内容は、後述の『パソコン無料セキュリティ診断』で提供するものと同じです。

© 2021 Sompo Risk Management Inc. All rights reserved.

特徴３　低価格

	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	○	◎ ※エンジニアによる診断項目別詳細
脅威ハンティング	× Lightプランの脅威ハンティングは 当社からの駆除要否紹介となります。	○
ハンティング費用	自己負担	保険補償 ※1

© 2021 Sompo Risk Management Inc. All rights reserved.

その他の特徴

３ヶ月ごとに作成されるセキュリティレポートで
パソコンのリスクを『 見える化 』できます！

1ヶ月の体験版でパソコン無料セキュリティ診断が
できます！

© 2021 Sompo Risk Management Inc. All rights reserved.

サービス紹介サイト

ウイルス感染を取り締まる パソコン監視・分析サービス

SOMPO CYBER SECURITY
powered by SOMPO RISK MANAGEMENT

SOMPO SHERIFF （標準プラン）

サイバーセキュリティ CSお助け隊

簡単に導入でき、すり抜けてくるウイルスを解析・検知

《 未知のウイルスを挙動で検知 》

- ✓ ソフトウェアをインストールするだけで簡単に導入でき、面倒な設定や調整は不要
- ✓ パソコンの送信ログやディレクトリ作成履歴などを常時監視し、ウイルス対策ソフトをすり抜けてくる新種のウイルスも解析・検知

検知したウイルスを早期分析・駆除（ 駆除費用はサイバー保険で補償 ）

《 セキュリティエンジニアによる人的精査 》

- ✓ 緊急アラートでお知らせしたウイルスは、専門のセキュリティエンジニアが早期に分析し、リモートアクセスや駆付けにより駆除
  （対応方法は、お客さまと協議して決定）
- ✓ 専用のサイバー保険(*)が付帯されており、駆除費用は保険金が充当

（*）引受保険会社：損害保険ジャパン株式会社

セキュリティレポートでパソコンのリスクを「見える化」

《 Wi-Fi や USB などの接続履歴も定期チェック 》

- ✓ 導入前に「パソコン無料セキュリティ診断」で一部機能を体験可能
- ✓ 導入後は、３か月毎にセキュリティレポートを提供
- ✓ 侵入した不正なプログラムや、パソコンの利用状況を見える化し、ウイルス対策ソフトだけでは分らなかった「従業員のパソコンがどれだけ危険な環境にあるのか」を把握可能

サービス内容の詳細や、『 パソコン無料セキュリティ診断 』のお申込みは、専用Webサイトをご覧ください。

https://www.sompocybersecurity.com/lp/sheriff/index.php

© 2020 Sompo Risk Management Inc. All rights reserved.

お問合せ先

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　　担当：千葉
E-mail: hchiba82@sompo-rc.co.jp

© 2020 Sompo Risk Management Inc. All rights reserved.