

経済産業省／独立行政法人情報処理推進機構(IPA)

令和2年度

サイバーセキュリティお助け隊 実証事業（千葉県・埼玉県）

事業説明会資料

2020年9月24日：千葉県

2020年9月25日：埼玉県

富士ゼロックス株式会社

サイバー攻撃

供給網の穴

「次は取引停止」迫る大手

下請けを含めたセキュリティ対策が求められている



防衛

- ・米国防総省は2018年以降、セキュリティ対策のできていない企業を納入不可に
- ・取引先からの情報漏洩も自社の経営責任に
- ・日本の防衛省も21年にも同等の調達基準を実施



自動車

- ・欧州連合(EU)は22年7月以降の新車販売で、下請けも含めたサイバー攻撃対策を自動車メーカーに義務づける
- ・日本や韓国、ロシアなど50以上の国と地域でも同様の規制が適用される見込み



通信

- ・米国が19年8月、ファーウェイなど5社の製品の政府調達を禁止
- ・20年8月以降は機器を利用している企業との取引も禁止に
- ・下請け企業での利用も取引停止につながる可能性がある

車・防衛…各国で規制強化

中小、人・カネ乏しく苦慮



米国防総省はセキュリティ対策に不備がある企業からの調達を止めている—ロイター

「注意で済ますのは今年が最後ですよ」
関東の部品メーカー社長は7月、重電大手の担当からこの告げられた。サイバー攻撃からの復旧支援を依頼したところ、複数の不備が判明した。セキュリティ対策が甘いままなら、取引停止もあり得るという。人お金もないなかで、どう対応すればいいのか。社長は頭を抱える。

大阪商工会議所が2019年に実施した調査では、取引先がサイバー攻撃を受けて自社に被害が及んだ場合、29%の企業が「取引停止」を検討すると回答した。

中小企業のサイバー対策支援を手掛けるキヤノンマーケティングジャパンの小野寺徹氏は、昨年から自動車や建設業界で取引停止に追い込まれる企業が増えていると話す。特に事故後の調査・対応の不備が問題視されるケースが多いという。大手が取引先のサイバー対策に神経を遣う理由は2つある。

まずはサプライチェーン(供給網)を標的にしたサイバー攻撃の急増だ。自動車や航空機の製造には何万もの企業に関わり、設計書など様々な情報がやり取りされる。防衛が手薄な中小の取引

先や業務委託先が攻撃にサイトも晒し制限されさらされると、そこから「打たれ回す」ことになる。トヨタ自動車や三菱重工業などの取引先が相

22年から義務化防衛産業だけではなく

「注意で済ますのは今年が最後ですよ」

関東の部品メーカー社長は7月、重電大手の担当からこの告げられた。サイバー攻撃からの復旧支援を依頼したところ、複数の不備が判明した。セキュリティ対策が甘いままなら、取引停止もあり得るという。人お金もないなかで、どう対応すればいいのか。社長は頭を抱える。

大阪商工会議所が2019年に実施した調査では、取引先がサイバー攻撃を受けて自社に被害が及んだ場合、29%の企業が「取引停止」を検討すると回答した。

「注意で済ますのは今年が最後ですよ」

すでに中小企業にもサイバーセキュリティ対策が求められています！

まずはサプライチェーン(供給網)を標的にしたサイバー攻撃の急増だ。自動車や航空機の製造には何万もの企業に関わり、設計書など様々な情報がやり取りされる。

もう一つは規制の強化だ。米国防総省は18年以降、取引企業に対してサイバー防衛ガイドライン「NIST SP800-171」の準拠を義務付けた。情報の暗号化や事故対応など約100の要件を満たせない企業は、調達先から締め出される。日本の防衛省も21年にも、同様の要件を調達基準に盛り込む。

サイバーセキュリティお助け隊 実証事業（千葉県・埼玉県）

経済産業省の令和2年度補正予算「中小企業サイバーセキュリティ対策促進事業」により補助を受けた独立行政法人情報処理推進機構（IPA）が実施する「令和2年度中小企業サイバーセキュリティ対策支援体制構築事業」のうち、富士ゼロックス株式会社が千葉県・埼玉県で実施する実証事業

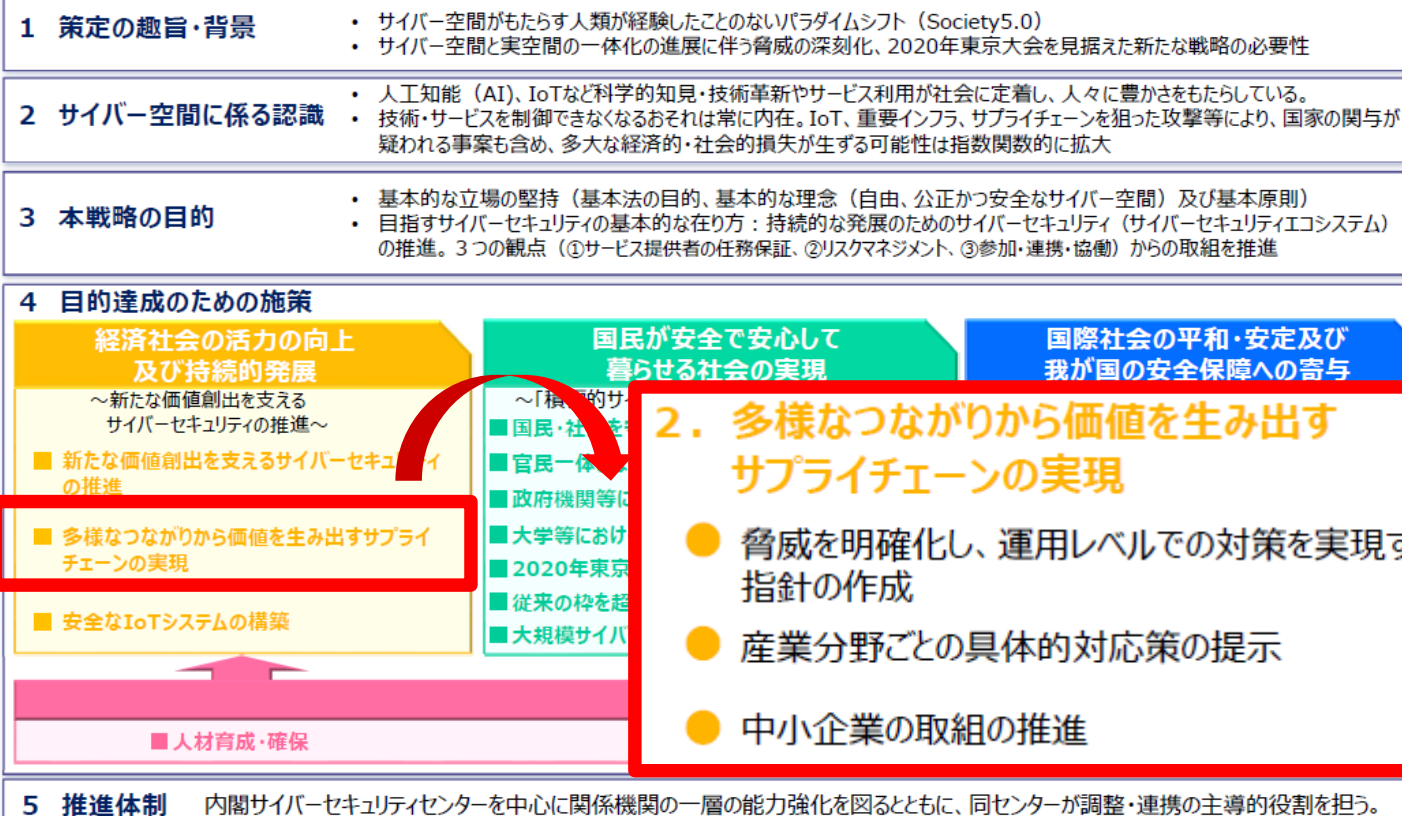
サイバーセキュリティに関する政策

昨今のサイバーセキュリティの重要性を受け、内閣サイバーセキュリティセンター（NISC）を中心にサイバーセキュリティ政策を展開しています。近年は、サプライチェーン全体の中で、セキュリティ対策の弱い中小企業を対象とするサイバー攻撃やそれに伴う大企業等への被害が顕在化しているといわれています。

サイバーセキュリティ戦略（2018年）・サイバーセキュリティ2020（2020年7月21日サイバーセキュリティ戦略本部決定）の概要

- ◆ サイバーセキュリティ戦略(2018年7月)は、サイバーセキュリティ基本法に基づく2回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後3年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの
- ◆ サイバーセキュリティ2020は、同戦略に基づく2019年度年次報告・2020年度年次計画として策定されたもの。各府省庁はこれに基づき、施策を着実に実施

＜新戦略（2018年戦略）（平成30年7月27日閣議決定）の全体構成＞



【出典】内閣サイバーセキュリティセンター サイバーセキュリティ戦略・サイバーセキュリティ2020の概要
サイバーセキュリティ戦略（閣議決定）の詳細概要

サイバーセキュリティお助け隊事業の概要

サイバーセキュリティお助け隊事業は、経済産業省の令和2年度補正予算「中小企業サイバーセキュリティ対策促進事業」により補助を受けた独立行政法人情報処理推進機構（IPA）が実施する「令和2年度中小企業サイバーセキュリティ対策支援体制構築事業」として、昨年度に引き続き実施される実証事業です。

中小企業サイバーセキュリティ対策促進事業

令和2年度補正予算額 **7.7億円**

商務情報政策局 サイバーセキュリティ課
03-3501-1253
中小企業庁 技術・経営革新課
03-3501-1816

事業の内容

事業目的・概要

- 新型コロナウイルス対応の一環で、中小企業がテレワーク等の業務のデジタル化を急速に進める中で、中小企業にとってサイバー攻撃の脅威は増大しています。中小企業が、サイバー攻撃の脅威から身を守りつつ、デジタル化による恩恵を享受するためには、サイバーセキュリティ対策の強化が急務です。
- 本事業では、①専門家派遣による事前支援の体制構築、②インシデント発生時の駆け付け支援や簡易保険による事後支援の体制構築に向けた地域実証を実施します。【補助】
- また、中小企業へのセキュリティの普及啓発や情報共有を行うため、全国各地でセキュリティコミュニティの形成や取組の拡大に向けた支援を実施します。【委託】

成果目標

- 本事業を通じ、テレワーク等の業務のデジタル化を進める中小企業において、基本的なセキュリティ対策の実施を促すとともに、セキュリティ運用・事後支援の全国での体制構築を目指します。

条件（対象者、対象行為、補助率等）

(1)、(2)



(3)



事業イメージ

(1) 登録セキスベ派遣事業（事前支援）

- 平成30年度第2次補正予算「中小企業等強靱化対策事業」にて、情報処理安全確保支援士（登録セキスベ：全国に約20,000人）を中小企業に派遣し、セキュリティ基本方針や関連規定の策定支援を行う事業を実施。96.4%の企業で「成果を得ることが出来た」との結果。
- こうした実績を踏まえ、全国で中小企業に登録セキスベを派遣し、テレワーク等のITシステムの基本的なセキュリティ対策を確認する取組を地元の団体等とも連携して実施。

(2) サイバーセキュリティお助け隊事業（事後支援）

- 平成30年度第2次補正予算「中小企業等強靱化対策事業」にて、損害保険会社、ITベンダー、地元の団体等が連携し、中小企業にセキュリティ監視機器等を設置。インシデントの発生時に駆け付け支援や簡易保険での対応を行う体制構築のための実証事業を実施したところ、実証地域のほぼ全てでサイバー事案が発生。
- 中小企業のデジタル化が全国で加速することも踏まえ、全国でセキュリティ運用・事後支援体制を確立するとともに重要分野のサプライチェーンを対象とする実証も実施。

(3) 各地域での施策の普及・セキュリティ情報の共有

- 現在、関西地域等では、経済産業局・総合通信局や民間団体を中心となったセキュリティコミュニティによる情報共有が進展。
- こうした取組を全国各地に広げ、中小企業向けのセキュリティ対策の施策の普及やセキュリティ情報の共有のためのコミュニティ形成を促進。

42

【出典】経済産業省 令和2年度補正予算の事業概要（PR資料）

サイバーセキュリティお助け隊事業（昨年度）

昨年度の事業では、全国8地域、1,064社の中小企業にUTM等のセキュリティ機器を設置し、実証期間中のインシデント対応は合計128件（12%の中小企業）発生しており、中小企業でも例外なくサイバー攻撃の脅威にさらされている実情が明らかになりました。当社は長野県、群馬県、栃木県、茨城県、埼玉県にて実証事業を行いました。

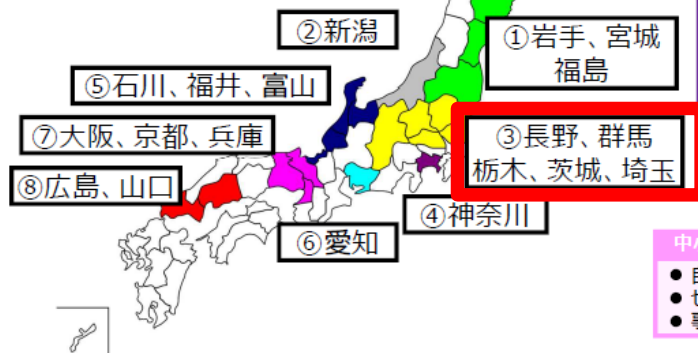
多様なつながりから価値を生み出す
サプライチェーンの実現

中小企業における現場対応の徹底支援（経済産業省資料）

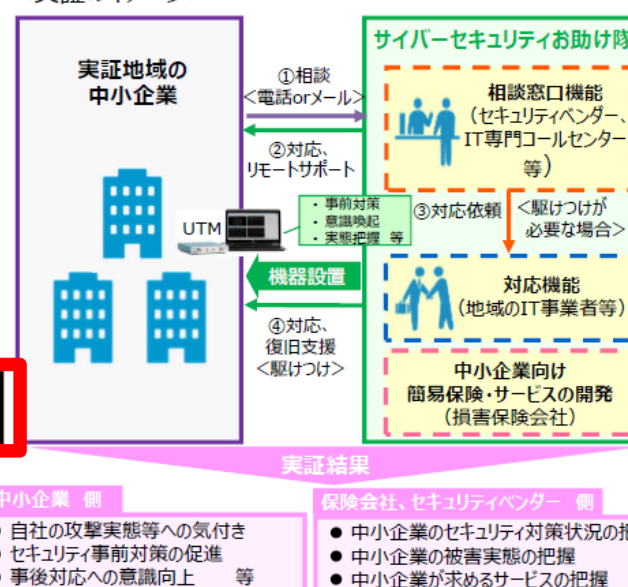
- 全国**8地域**において、地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした**実証事業**を実施。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指す。**

<実証地域>

計1,064社の中小企業が参加



<実証のイメージ>

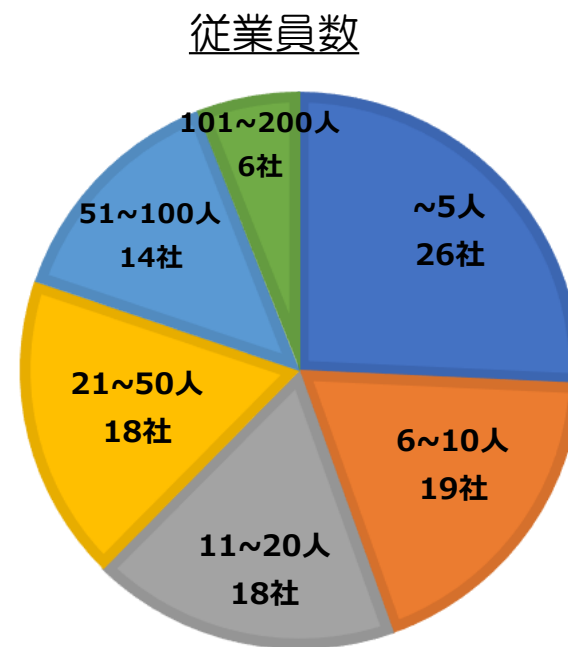
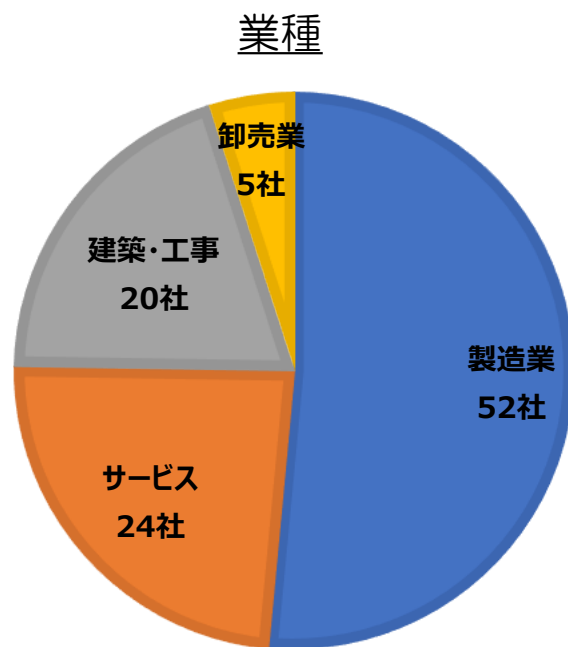
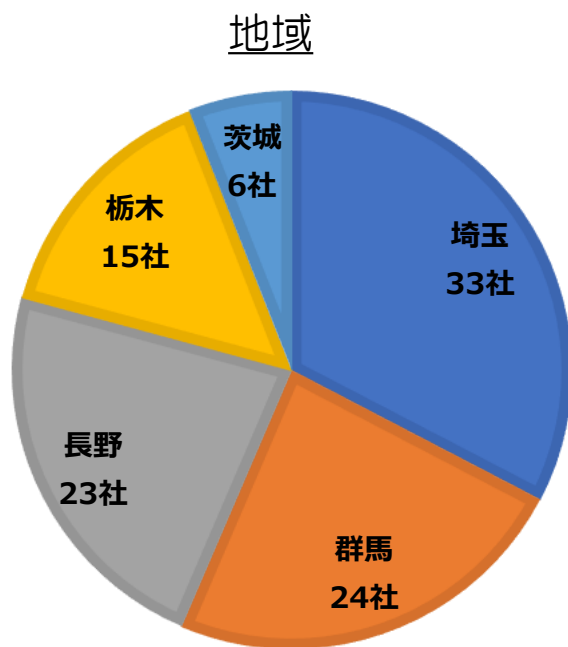


25

【出典】内閣サイバーセキュリティセンター サイバーセキュリティ戦略・サイバーセキュリティ2020の概要

昨年度のサイバーセキュリティお助け隊事業の結果（弊社） 長野県、群馬県、栃木県、茨城県、埼玉県

- 昨年度は長野、群馬、栃木、茨城、埼玉の合計 112 社の中小企業様にご参加
※UTM設置企業は 101 社
- 製造業が全体の半数以上
- 約半数の 45 社が従業員数 10 名以下の事業者
- セキュリティ機器であるUTMを設置し、調査期間中（2019年9月5日 ～ 2020年1月末）のログ情報を収集、分析することにより、サイバー攻撃被害等の実態について調査を実施



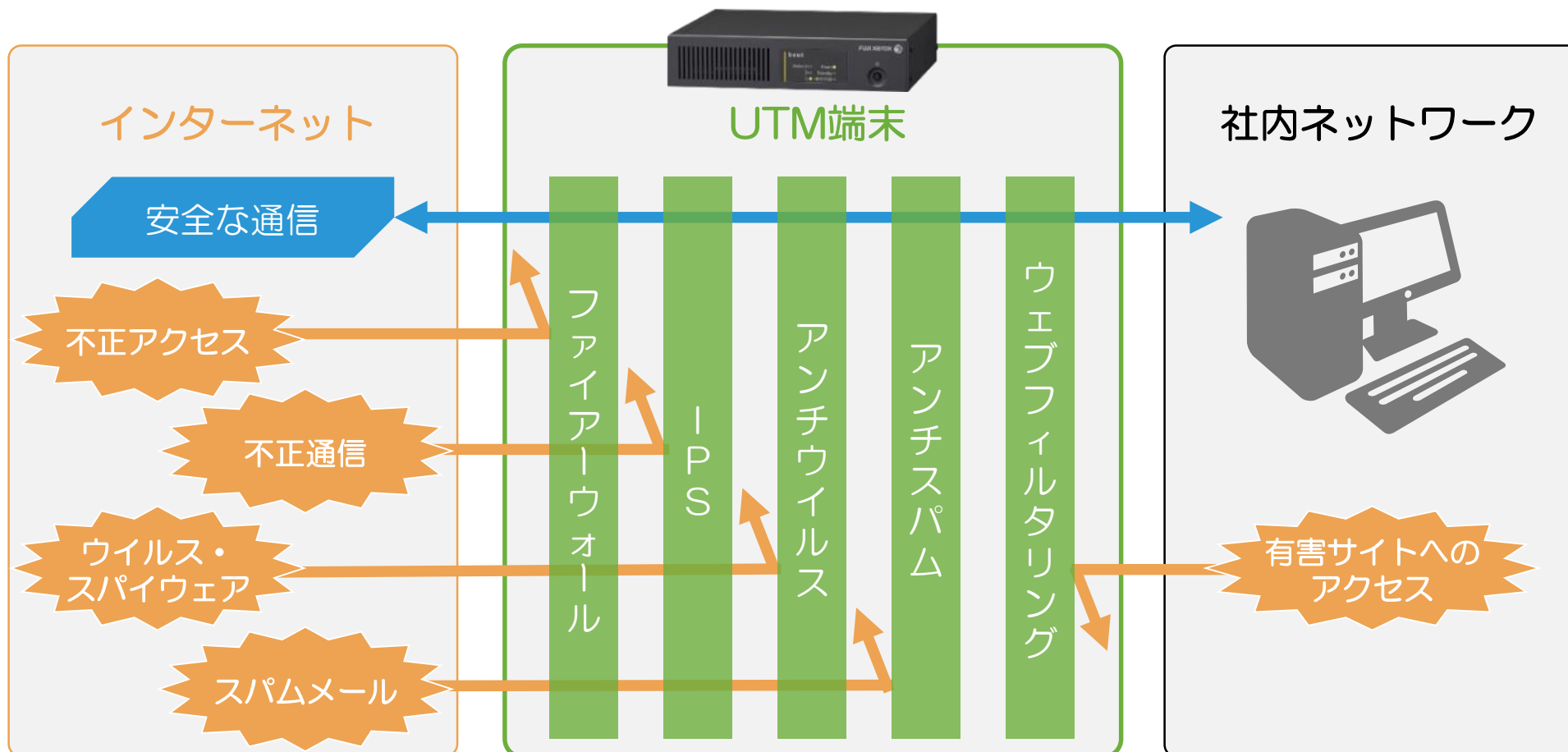
調査手法：

UTM端末のログ分析とは

UTM (Unified Threat Management)

インターネット上のあらゆる脅威への対策に必要なシステムが1つに集約され、ウイルスなどの脅威を含まない安全な通信のみを通すことができます

→ ログを分析することで、どのようなセキュリティリスクが発生しているかがわかります



IPSは「Intrusion Prevention System」の略で、日本語では「不正侵入防止システム」と呼ばれます

昨年度の実証事業の結果 全セキュリティアラートの結果

当社が昨年度実施した実証事業においても、中小企業でも例外なくサイバー攻撃の脅威にさらされている実情が明らかになりました

モニタリング項目	発生件数 (合計)	対策
ping/port-scanの検知数 (外部からの偵察行為)	64,444件	ファイアウォール機能 等
不正通信の検知数 (内部から外部)	4,892,530件	IPS (Intrusion Prevention System) 等
HTTP・FTPウイルスの検知数 (Web経由でダウンロードされたウイルス)	29件	アンチウイルス、社員教育 等
受診メールに含まれる ウイルスの検知数	195件	アンチウイルス、社員教育 等
受診メールに含まれる スパムメールの検知数	75,992件	アンチスパム、社員教員 等
有害なWebサイトへのアクセス数 (社内から)	2,541,796件	Webフィルタリング機能、社員教育 等

調査対象：UTM 100台、調査期間：2019/9/5～2019/12/31

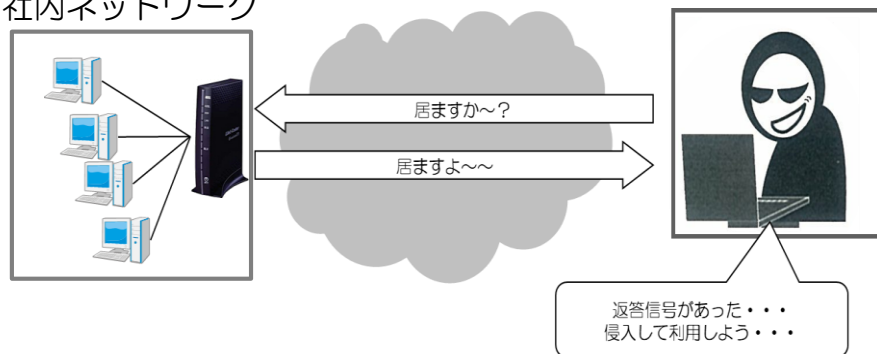
外部からの「偵察」行為

ping/port-scan

インターネットの世界では、特別な通信を使って、会社や家庭のネットワークの中に侵入しようとする試みが行われています。

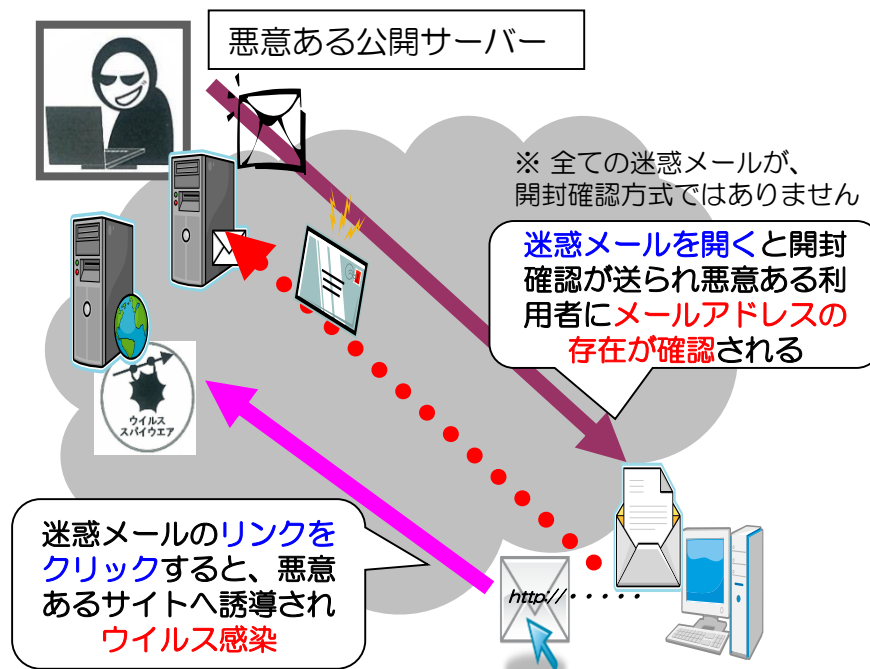
現実の世界に例えると、住宅街を不審者が四六時中徘徊し、玄関や窓の施錠確認をしています。施錠されてなければ、空き巣に入られることになります。

社内ネットワーク



スパムメール

スパム（迷惑）メールの中には、自分自身や知人・政府機関などのメールアドレスを詐称している物があり、十分な注意が必要です



昨年度の実証事業の結果

中小企業におけるサイバー攻撃被害等の実態

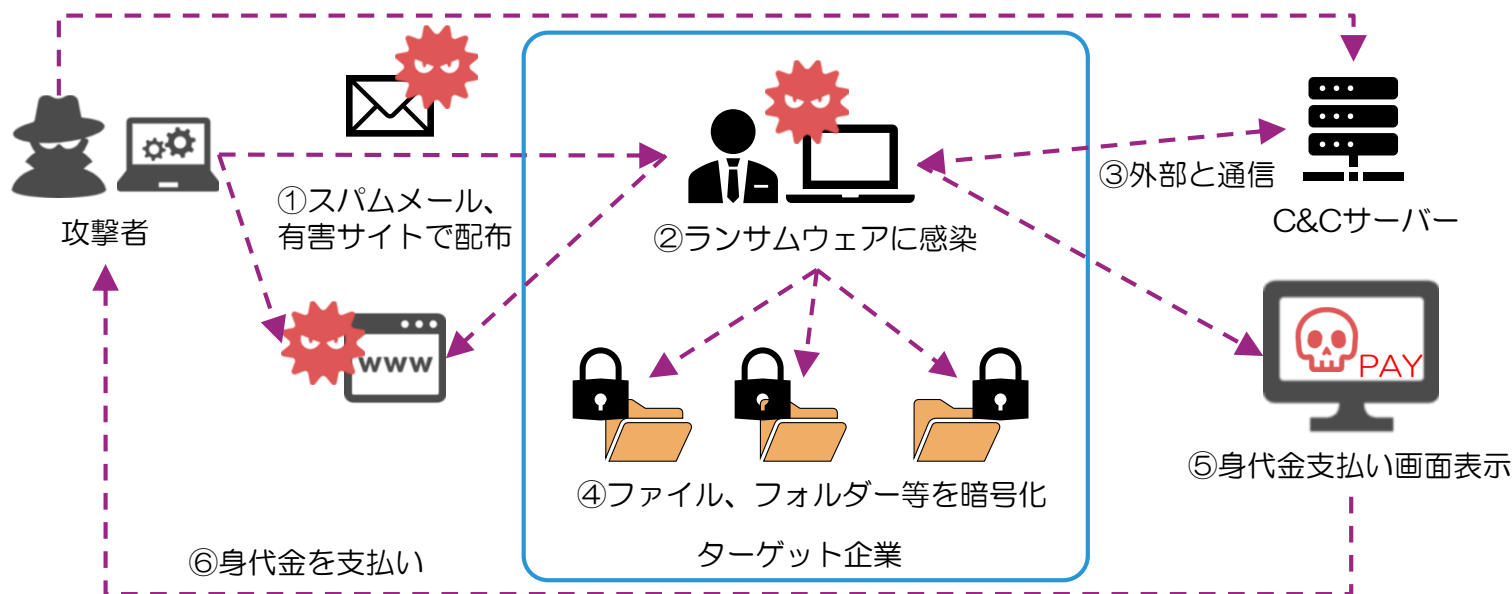
調査結果から、対象地域の中小企業において、以下の4種類のサイバー攻撃に関する脅威シナリオが確認されました

脅威シナリオ	内容	頻度	影響度
ランサムウェアによる被害	PC（サーバー含む）やスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、復旧に金銭を支払うよう脅迫するランサムウェアと呼ばれるウイルスへの感染が確認されている。組織においては、業務を遂行する上で必要な情報を暗号化された場合、事業継続にも支障がでるおそれがある。また、脅迫に従った場合、金銭的な被害も発生する。	低	データをロックされてしまう等、業務停止に追い込まれることが多く、関連会社への納品ができなくなるなど、影響度は高い
標的型攻撃による被害	企業や民間団体そして官公庁等、特定の組織から重要情報を窃取することを目的とした標的型攻撃が発生している。 攻撃者はメールの添付ファイルや悪意のあるウェブサイトを利用し、組織のPCをウイルスに感染させる。その後、組織内部へ潜入し、組織内部の侵害範囲を拡大しながら重要情報や個人情報を窃取する。	低	関係する会社から情報が盗み取られた場合など、継続的に標的にされる可能性が高く、被害が大きく拡大する可能性が高い
内部不正による情報漏えい	組織の従業員や元従業員等、組織関係者による機密情報の漏えい、悪用等の不正行為が発生している。組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失等により、組織に多大な損害を与える。	高	クラウド等の利用により、外部に大量データを保持することがあり、そのデータ流出によっては、被害が大きくなる可能性が高い
不注意による情報漏えい	組織や企業では、情報管理に対する意識の低さや確認漏れ等により、従業員による個人情報や機密情報の漏えいが後を絶たない。漏えいした情報が悪用される等の二次被害も懸念される。	高	WEBサービスに組み込まれているAPIから、情報が盗み取られる可能性があり、信頼できるサービスか否かの判断が随時必要である

脅威シナリオ① ランサムウェアによる被害

【攻撃手順】

- ①スパムメール、または有害サイトを利用してランサムウェアを配布する
- ②PCがランサムウェアに感染
- ③外部（C&Cサーバー）と通信して不正ファイルを実行する
- ④⑤⑥ファイル、フォルダー等を暗号化し、身代金支払い画面が表示され、被害者による身代金の支払いが行われる



【今回の実証結果】

- ・①スパムメール：約14件/日・台
- ・①有害サイト：約8割の企業で何らかの有害サイトにアクセスし、期間中29件のマルウェアをダウンロード（ブロック）
- ・③不正通信：WannaCryのC&Cサーバーとの通信を検出・ブロック(1社PC1台)

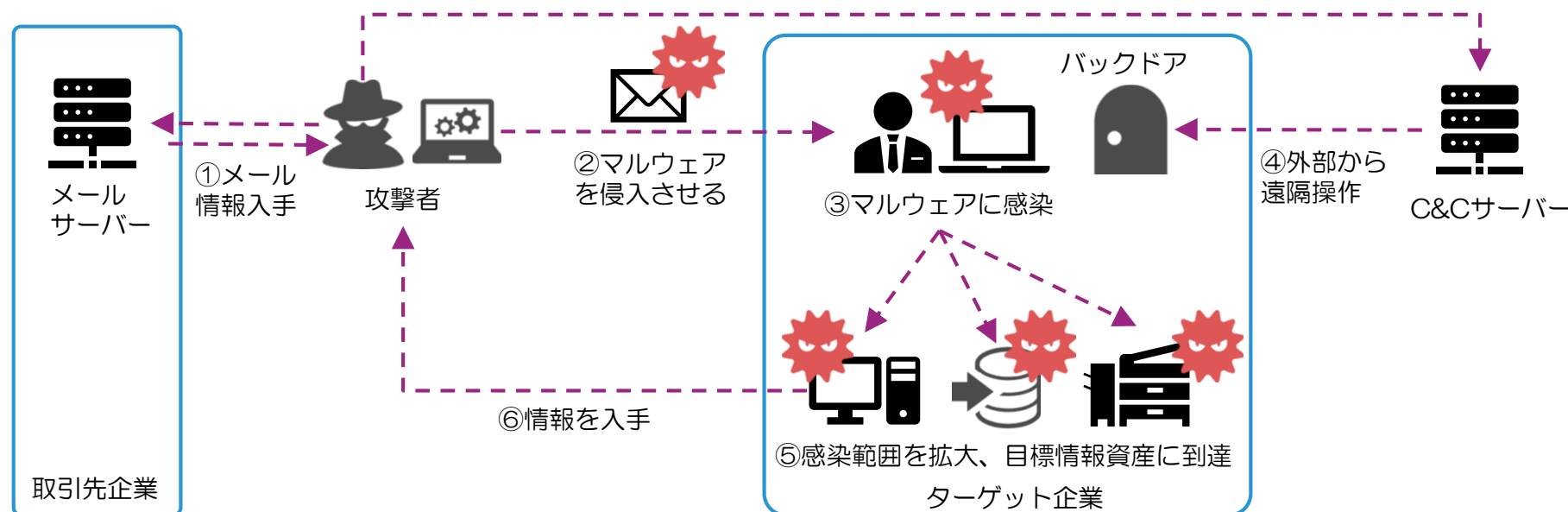
【考えられる対策案】

- ・アンチウイルス、アンチスパム機能によりマルウェアを検知、駆除する
- ・IPS/IDS機能により不審な通信を検知、ブロックする
- ・マルウェアを端末側で検知し、端末を隔離する
- ・スパムメール訓練等による社員教育を実施する
- ・バックアップを取得しておく

脅威シナリオ② 標的型攻撃による被害

【攻撃手順】

- ①ターゲット企業への攻撃の成功率を上げるため、取引先企業等のメールサーバーを攻撃し、メール情報を入手
- ②取引先企業になりすまし、メールへの返信を装う形でマルウェア付き、もしくはURL付きのメールを送りマルウェアを侵入させる
- ③～⑥外部からの遠隔操作から更なる感染拡大による情報漏えい、またはランサムウェアによる身代金攻撃等の被害が発生する



【今回の実証結果】

- ・①メール情報入手：取引先企業からメール情報を入手
- ・②マルウェア付きメール：期間中に195件
- ・⑤不正通信：外部のWebサーバ・FTPサーバを攻撃する通信を検出・ブロック(1社PC3台)

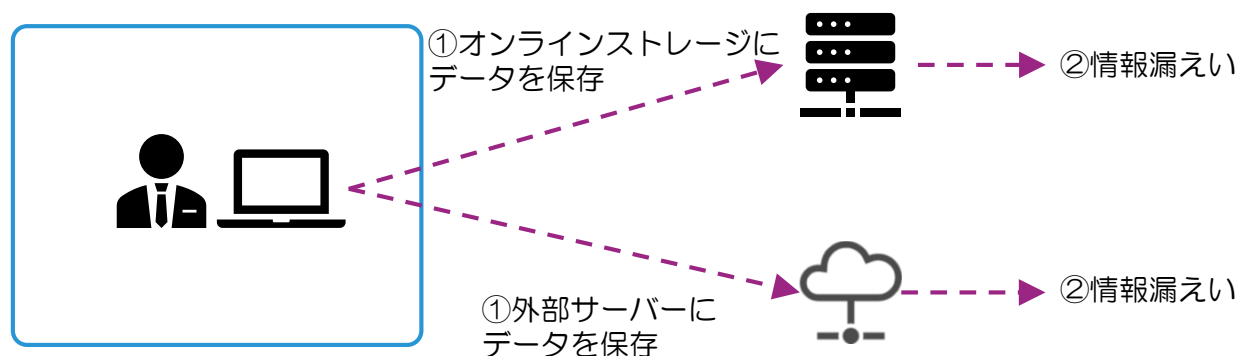
【考えられる対策案】

- ・アンチウイルス、アンチスパム機能によりマルウェアを検知、駆除する
- ・IPS/IDS機能により不審な通信を検知、ブロックする
- ・マルウェアを端末側で検知し、端末を隔離する
- ・標的型メール訓練等による社員教育を実施する

脅威シナリオ③ 内部不正による情報漏えい

【発生順】

- ①従業員が（業務上許可されていない）オンラインストレージや外部サーバーに機密情報を保存
- ②外部に機密情報を持ち出し、または機密情報が漏えい



【今回の実証結果】

- ・①オンラインストレージ：全100台のUTMの1/5にあたる20台でアクセスを検知
- ・①外部サーバー：全100台のUTMの約1/5にあたる22台で遠隔地のPCへ接続する通信を検知

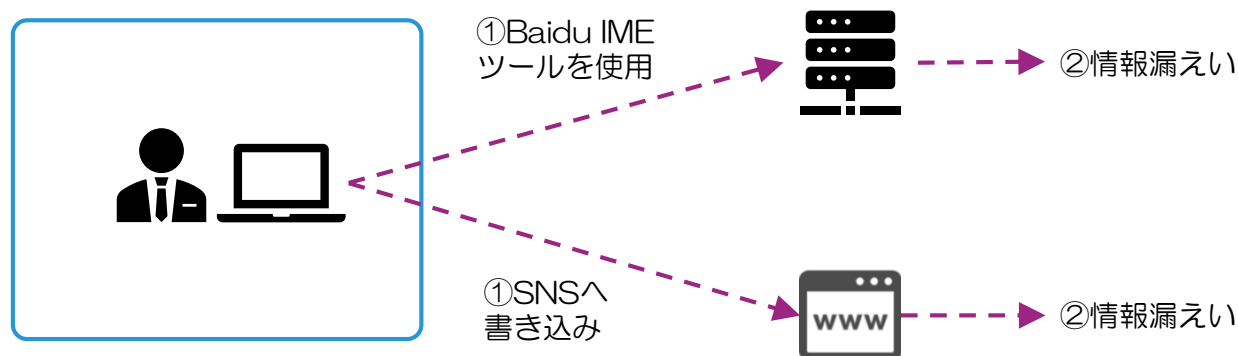
【考えられる対策案】

- ・セキュリティポリシーを策定する
- ・システムの操作履歴を監視する
- ・コンプライアンスに関する社員教育を実施する

脅威シナリオ④ 不注意による情報漏えい

【発生順】

- ①従業員がBaidu IMEツールを使用
- ①従業員がSNSに機密情報を書き込み
- ②外部に機密情報が漏えい



【今回の実証結果】

- ・①全100台のUTMの約1/3にあたる34台でBaidu社のサーバとの通信を検出・ブロック
- ・①SNS：全100台のUTMの約1/4にあたる27台でSNSやWebメールへのアクセスを検知

【考えられる対策案】

- ・セキュリティポリシーを策定する
- ・利用しているシステムの情報を監視する
- ・サイバーセキュリティに対する意識啓発の教育を実施する

中小企業が取り組むべきサイバーセキュリティ対策について

昨年度の実証事業からみえてきた中小企業が取り組むべきサイバーセキュリティ対策を示します

まずはここから！

サイバー攻撃の実態把握、セキュリティ対策の重要性を認識すること

本日はここ！

- ・ 自社が保有する情報資産を管理できているか？
 - ・ もしもの場合の被害について検討できているか？
 - ・ セキュリティポリシーは策定できているか？
- 情報セキュリティ対策ガイドラインに沿ってできるところから始めることが重要です

サイバー利用のルール作りと運用、社員へのセキュリティ教育の徹底

実証事業で！

- ・ オンラインストレージ、外部サーバー等の利用ルールを決めているか？その通り運用できているか？
 - ・ SNSの個人アカウントで機密情報を扱ったりしていないか？
 - ・ リスクのある無料ソフトや入力ツール等を気付かぬまま使用していないか？
- 社員のPC利用状況等について、把握しておくことが重要です

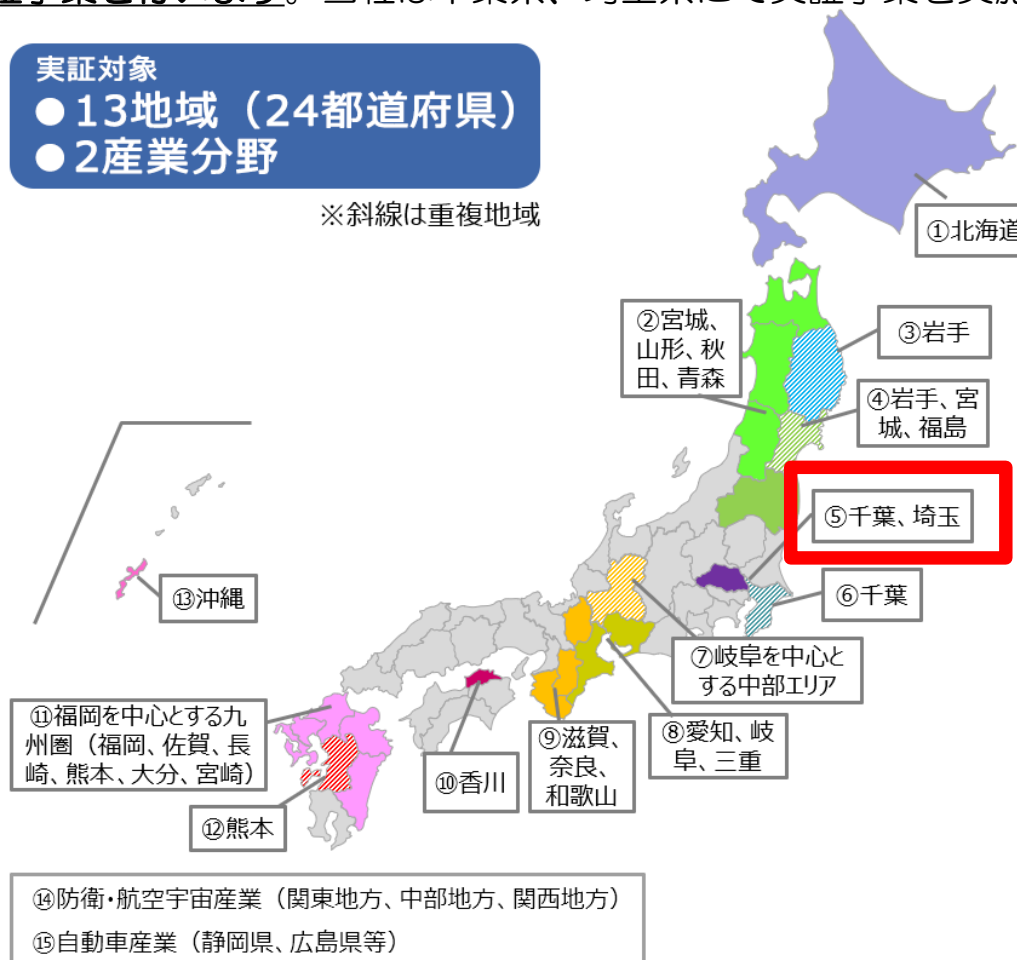
高度化するサイバー攻撃への対策、監視ツールや専門家による定期診断の必要性

実証事業で！

- ・ ランサムウェアや標的型攻撃への対策ができているか？
 - ・ サイバーセキュリティに関する最新情報を把握できているか？
- 関連セミナーや専門家への相談から、自社に必要なセキュリティ対策を定期的に検討することが重要です

本年度のサイバーセキュリティお助け隊事業

本年度は昨年度の結果も踏まえて、地域特性・産業特性等を考慮したマーケティング、機器・ソフトウェア・サービスの導入負荷の低減、説明会等を通じた普及啓発、支援内容のスリム化によるコスト低減等を目指し、24道府県13地域と2産業分野の中小企業を対象として、中小企業の実態に即したサイバーセキュリティ対策支援体制の構築に向けた実証事業を行います。当社は千葉県、埼玉県にて実証事業を実施します。



【出典】IPA サイバーセキュリティお助け隊（令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業）
<https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html>

本年度の実証事業の概要

- 概要
- スケジュール
- 参加のメリット

実証事業の概要

地域：千葉県、埼玉県

期間：2020年9月～2021年1月

参加企業数：2県で50社程度

実施内容：ご提供する実証内容は、参加事業者様に応じて、異なる場合がございます。

UTM設置数は2県で30社程度を見込んでおります。

実施項目		概要
UTMモニタリングによるサイバー攻撃の実態把握	・ UTMを設置してサイバー攻撃の実態把握	UTMを設置し、企業様へのサイバー攻撃の検知、ログの取得、不正アクセスの検知等のセキュリティサービスを提供します
	・ コンタクトセンターによる相談受付 ・ 駆け付け隊によるサポート	サイバーセキュリティに関する相談受付、初期対応を行うコンタクトセンター、セキュリティインシデント発生時のサポートを行う駆け付け隊を設置します
専門家のヒアリングによるセキュリティのリスク診断、アドバイス等	・ IT専門家のヒアリングによるセキュリティリスク診断、アドバイス	ヒアリングにより企業様のセキュリティ対策レベルを確認し、企業様ごとに適切なセキュリティ対策支援についてアドバイスいたします。
	・ 自己診断Webツールによるリスク診断	サイバーセキュリティに関する最新情報の提供、企業様ごとのセキュリティリスクに関する評価を体験いただき、意識を高めていただきます。

- ・ UTMから取得されるログデータは、今後のセキュリティ対策支援体制の検討のため、IPAへ提供することを予めご了承下さい。ログデータはサイバー攻撃の実態分析を行うための一般的な内容で、参加企業様が特定できる情報や企業秘密情報等は含まれません。
- ・ 個人情報に関する取扱いについて：ご提供頂いた情報は、IPA、経済産業省、事業実施者である富士ゼロックス 株式会社、本事業に関する説明会の運営および本事業を実施する為に利用する他、IPA、富士ゼロックス株式会社からの中小企業向け他事業に関するご案内(電話/メール/郵送等)をする為に利用します。

実証事業のスケジュール

※スケジュールについては変更となる可能性があります

2020年9月24日：千葉県 事業説明会開催（オンライン）

2020年9月25日：埼玉県 事業説明会開催（オンライン）

～予定数に達するまで：参加申込

→UTM設置に関する現地調査等

→企業様ごとに参加決定の通知

参加決定後～2020年12月：UTM設置

→UTMモニタリング、駆け付け支援等

専門家によるヒアリング

2020年12月～2021年1月：事後アンケート回答（ヒアリング）

2021年1月：成果報告会開催

実証事業参加のメリット

1. 実証期間中は無償でUTMを設置し、自社に対するサイバー攻撃の実態を可視化した診断レポート等が受けられます。
2. 自社のサイバーセキュリティ対策の現状とリスクの把握、追加対策等の必要性について専門家からアドバイスを受けられます。
3. 自社でサイバーインシデントが発生した場合の想定被害の算出(範囲、金額)等、もしもの場合を想定したシミュレーションツールが受けられます。
4. ウィルス感染などのサイバーセキュリティで困ったときの相談、駆けつけ支援等を受けられます。

UTMによるサイバー攻撃の実態の可視化

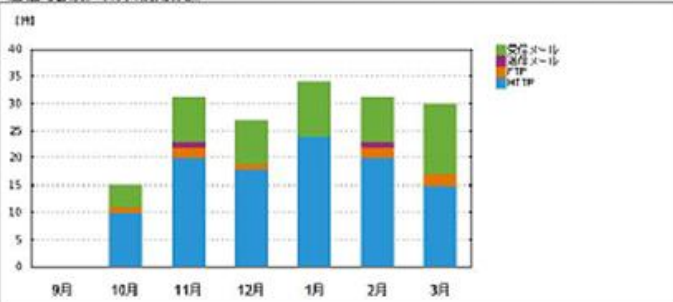
UTMのログから、自社に対するサイバー攻撃の実態を可視化

ウイルス検知状況

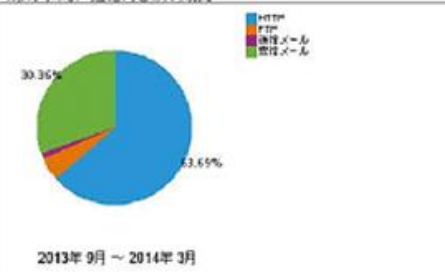
→ヘルプ: ウィルス検知状況

通信内容（メール送信・メール受信・ウェブアクセス・FTPアクセス）ごとに、検知したウィルスの件数を表示しています。
ウィルスが検出されたデータはbeatが自動的にブロックし、削除または無効化されています。

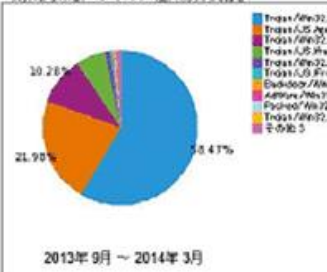
通信内容別ウィルス検知件数



期間内累計 通信内容別構成比



期間内累計 ウィルス種類別構成比



インシデントを想定したシミュレーションツール

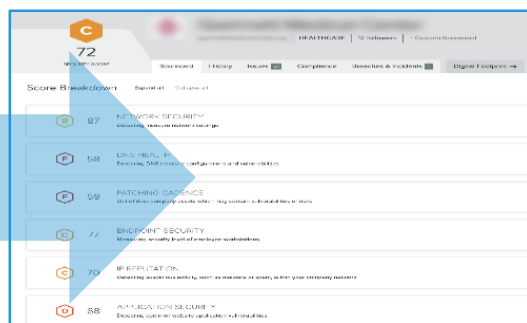
東京海上日動火災保険様が無償提供している「サイバーセキュリティ・外部診断」「予想損失額シミュレーション」「標的型攻撃メール訓練」を利用して、自社のリスクを評価できます。



powered by SecurityScorecard

サイバーセキュリティ・外部診断

外部視点で企業・組織のセキュリティリスクを10のファクターごとに5段階で分析・評価します。



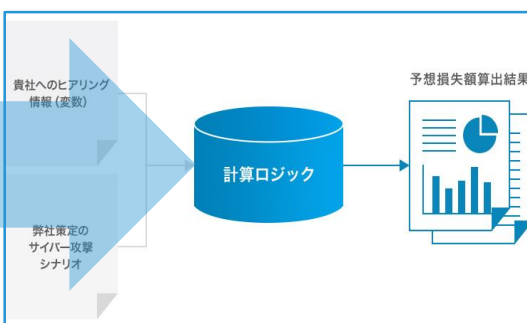
米国SecurityScorecard社が常時収集している膨大なデータを解析し、システムの運用に影響を与えることなく、外部視点から企業・組織のサイバーセキュリティリスクを10のリスクファクターごとに5段階で評価・スコアリングします。




Breach Cost Calculator

予想損失額シミュレーション

各設問に回答を入力すると、サイバー攻撃による被害が生じた場合の「予想損失額」を算出します。

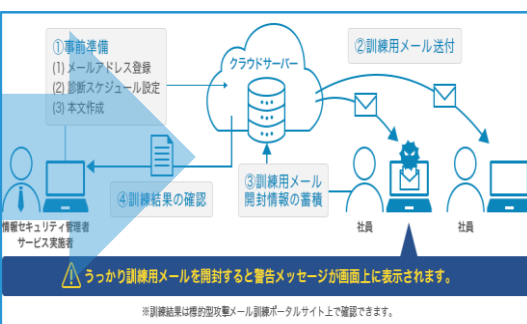


サイバー攻撃による被害について、シナリオごとの「影響度」（縦軸）、特に経済的損失を定量的に評価します。本シミュレーションで取り扱うシナリオは、「サイバー攻撃のおそれ」「個人情報の漏えい」「Web改ざん」「DoS攻撃」の4つです。



標的型攻撃メール訓練

ウイルス対策だけでは完全に防ぐ事が難しい「標的型攻撃メール」の対策を訓練を通して意識づける事ができます。



インターネット接続環境で「標的型攻撃メール」を疑似体験する訓練サービスです。ウイルス対策だけでは完全に防ぐことは難しいと言われている「標的型攻撃メール」への対策として、社員の訓練を通じて、“不審なメールを開かない”ように意識づけれます。



<https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s>

実証事業への申込について

- 申込方法
- 参加対象企業
- 問い合わせ先

実証事業への申込方法

1. 本日の説明会終了後にメールで送付する参加意向確認書（兼アンケート用紙）にご回答いただき、スキャンして電子メールにてご送付をお願いいたします。

【送付先】 fx-Ipa-2020otasuke@fujixerox.co.jp

2. 参加希望いただいた企業様に、弊社から参加決定通知をメールにてご連絡いたします。

※残念ながらご参加いただけない場合も、その旨メールにてご連絡いたします。

3. 参加企業様には、その後のスケジュール等について、別途ご連絡いたします。

実証事業参加対象企業

1. 千葉・埼玉の2県に事業所を置いていること
2. 中小企業基本法に基づく中小企業および法人格を有する団体等であること（下表）
3. 反社会的勢力の関与がないこと
4. 本実証事業の目的を理解し、実証機器類設置(UTM)、ヒアリング、アンケート等へのご協力に対応いただけること

業種分類	定義
①製造業、建設業、運輸業	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
②卸売業	資本金の額又は出資の総額が1億円以下の会社又は常時使用する従業員の数が100人以下の会社及び個人事業主
③サービス業（ソフトウェア業又は情報処理サービス業、旅館業を除く）	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が100人以下の会社及び個人事業主
④小売業	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が50人以下の会社及び個人事業主
⑤ゴム製品製造業（自動車又は航空機用タイヤ及びチューブ製造業並びに工場用ベルト製造業を除く）	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が900人以下の会社及び個人事業主
⑥ソフトウェア業又は情報処理サービス業	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
⑦旅館業	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が200人以下の会社及び個人事業主
⑧その他の業種（上記以外）	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
⑨医療法人、社会福祉法人	常時使用する従業員の数が300人以下の者
⑩学校法人	常時使用する従業員の数が300人以下の者
⑪商工会・都道府県商工会連合会及び商工会議所	常時使用する従業員の数が100人以下の者
⑫中小企業支援法第2条第1項第4号に規定される中小企業団体	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑬特別の法律によって設立された組合又はその連合会	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑭財団法人（一般・公益）、社団法人（一般・公益）	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑮特定非営利活動法人	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者

問い合わせ先

サイバーセキュリティお助け隊事務局（千葉県、埼玉県）

富士ゼロックス株式会社

柴田／池

TEL：080-1104-0427

メール：fx-Ipa-2020otasuke@fujixerox.co.jp

