独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

サイバーセキュリティお助け隊事業
（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）
全体報告書（概要版）

2021年5月

独立行政法人情報処理推進機構
セキュリティセンター 中小企業支援グループ

目次

報告書サマリー

2020年度実証事業で明らかになった実態

【中小企業の被害実態の把握】

- 実証参加中小企業において、サイバー攻撃そのものでなくとも**業種や規模を問わず不審な通信等の脅威にさらされており、**ウィルス対策ソフト等の既存の対策では防ぎきれていない実態が明らかとなった。
- ある特定の1社で、11月～12月に「C&Cコールバック」と見られる攻撃を4,126件受けている事例や、「トロイの木馬」と想定されるものが多く検知されるなど**特定の企業が集中的に攻撃を受けている事例**も明らかとなった。

【中小企業が求めるサービスの把握】

- 今後希望するサービスとして**「相談窓口」**を希望される企業が多かった。
- セキュリティ対策に支払可能な金額は、**月額1万円程度**の回答が多かった。

【中小企業におけるセキュリティ対策にかかる課題】

- セキュリティ対策の課題は、**専門人材の不足**、社員や専門人材に対する**教育**がなされていない、**費用**を捻出することが困難といった点が挙げられた。
- 実証参加中小企業における**テレワークの実施率**はそれほど**高くなかった**が、テレワークに取り組む企業におけるセキュリティ上の課題としては、リモートツールやネットワーク環境の未整備等の**技術的な対策**が挙げられた。

今後の課題

【サイバー攻撃への対策不足】

- 中小企業に望まれる、**導入負荷がかからず**、**低価格**で提供可能なセキュリティ機器・サービスの開発と普及促進が必要。

【セキュリティ対策における人的リソース不足】

- 中小企業は、セキュリティに詳しい人材がいないことが多く、セキュリティ全般について相談可能な「**相談窓口**」の設置が肝要。
- 特定の企業が集中的に攻撃を受けるケースもあり、中小企業自らが対応することは難しく、外部の専門家からのサポートや業界団体や地域団体等の支援など**専門家の活用**が必要。

【セキュリティ対策への予算割当てが困難】

- 中小企業がセキュリティ対策費用としてかけられるのは、月額１万円程度であり、**セキュリティ対策費用でカバーできないインシデント発生時の対応支援までカバーしたサービス**が必要。

【セキュリティに対する情報不足】

- セキュリティに関する**普及啓発活動**の実施。
- 今後、中小企業においてもテレワーク・DX推進が進むと、**技術的な対策についての情報提供**や**セキュリティ製品・導入支援**が必要になる。

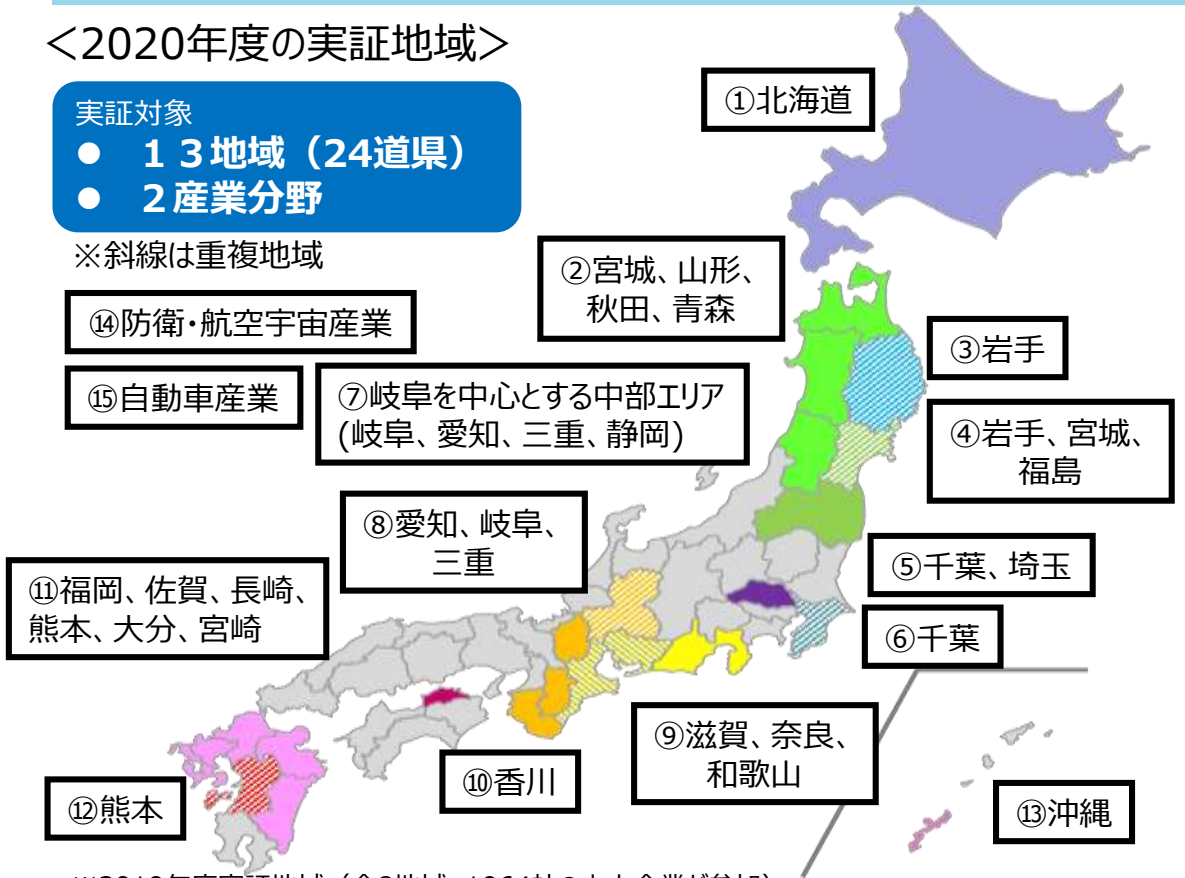
事業概要

- 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**を実施した（全国で**15件**実施）。
- 本事業により、**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**を目指し、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った。

＜2020年度の実証地域＞

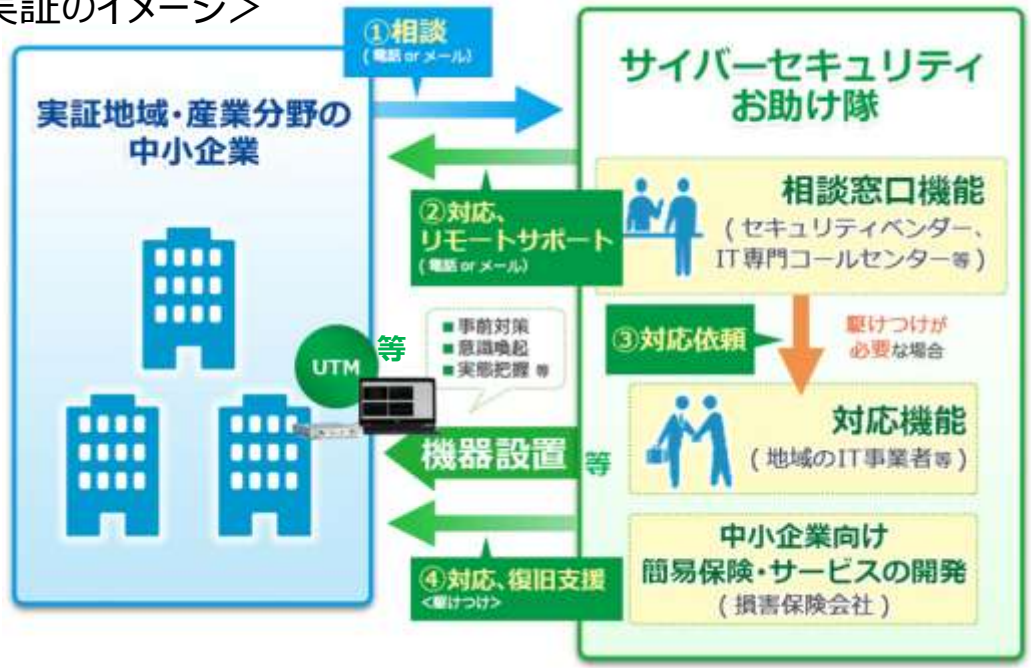
実証対象
- **１３地域（24道県）**
- **２産業分野**

※斜線は重複地域



※2019年度実証地域（全8地域、1064社の中小企業が参加）：
①宮城、岩手、福島②新潟③長野、群馬、栃木、茨城、埼玉④神奈川⑤石川、富山、福井⑥愛知⑦大阪、京都、兵庫⑧広島、山口

＜実証のイメージ＞



実 証 結 果

中小企業　側
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

2020年度実証事業のポイント

- 2019年度事業の結果を踏まえ、地域特性・産業特性を考慮したマーケティングを行うため、**13地域（24道県）**と**2産業分野**の中小企業等を対象に実施
- **2021年度以降の民間でのサービス展開に繋げる**べく、サービス内容のスリム化や導入・運用負荷を下げる検討を推進

2019年度実証事業で明らかになった実態・課題等

- **業種や規模を問わず**内外に向けた不正通信等を数多く検知
- **地域特性、産業特性**等の考慮が必要
- 無償の実証事業でも参加の**必要性を感じない**中小企業が多い
- 中小企業が自社のNW構成図を把握していなかったり人手不足により、**機器設置に対応できないケースが多い**
- 中小企業の多くはセキュリティ対策に**コストを割けない**

2020年度実証事業のポイント

- 全国で**15件**実施（2019年度の8地域より拡大）
- **地域特性や産業特性等を考慮**して進める
- セキュリティ対策への理解を促す**意識啓発（継続）**
- セキュリティサービスの**導入・運用負荷を下げる**方法の検討
- サービス内容のスリム化、事前対策等とのセットによる**リスク低減方法の検討**
- **テレワークに留意した実証**も実施（例 テレワーク環境での実態調査、テレワークにも対応した機器 等）

2021年度以降
民間でのサービス展開

実証参加状況

● 全国**13地域(24道県)／2産業分野**で請負事業者が事業主体となって実施体制を組織し、実証対象の中小企業に実証事業を周知し、参加を呼びかけることで、**計1,117社**の中小企業が本事業に参加した。

	地域／産業分野	実施主体	実施体制	実証参加企業数	
				計画	実績
①	北海道	東日本電信電話株式会社	東京海上日動火災保険株式会社	100社	143社
②	宮城、山形、秋田、青森	東北インフォメーション・システムズ株式会社	株式会社ハイテックシステム、株式会社アキタシステムマネジメント、あいおいニッセイ同和損害保険株式会社	40社	40社
③	岩手	富士ソフト株式会社	東京海上日動火災保険株式会社	70社	71社
④	岩手、宮城、福島	株式会社デジタルハーツ	損害保険ジャパン株式会社、東日本電信電話株式会社	50社	56社
⑤	千葉、埼玉	富士ゼロックス株式会社	東京海上日動火災保険株式会社	50社	60社
⑥	千葉	ＳＯＭＰＯリスクマネジメント株式会社	ちばぎんコンピューターサービス株式会社、株式会社千葉銀行、株式会社ラック、損害保険ジャパン株式会社	50社	66社
⑦	岐阜を中心とする中部エリア	MS&ADインターリスク総研株式会社	中部電力株式会社、株式会社中電シーティーアイ、中部電力ミライズ株式会社、三井住友海上火災保険株式会社、あいおいニッセイ同和損害保険株式会社	50社	76社
⑧	愛知、岐阜、三重	名古屋商工会議所	株式会社日立システムズ、西日本電信電話株式会社、東京海上日動火災保険株式会社、損害保険ジャパン株式会社	100社	140社
⑨	滋賀、奈良、和歌山	大阪商工会議所	日本電気株式会社、東京海上日動火災保険株式会社、キューアンドエー株式会社	50社	53社
⑩	香川	高松商工会議所	株式会社STNet、キヤノンマーケティングジャパン株式会社、株式会社青柳、四国オフィスオートメーションシステム株式会社、四国特機株式会社、西日本電信電話株式会社、損害保険ジャパン株式会社、東京海上日動火災保険株式会社	70社	70社
⑪	福岡を中心とする九州圏（福岡、佐賀、長崎、熊本、大分、宮崎）	株式会社BCC	日本電気株式会社、東京海上日動火災保険株式会社、ＮＥＣフィールディング株式会社	50社	54社
⑫	熊本	西日本電信電話株式会社熊本支店	株式会社くまなんピーシーネット、東京海上日動火災保険株式会社、一般社団法人熊本県サイバーセキュリティ推進協議会	100社	105社
⑬	沖縄	沖電グローバルシステムズ株式会社	株式会社セキュアイノベーション、ファーストライディングテクノロジー株式会社、損害保険ジャパン株式会社、那覇商工会議所、沖縄電力株式会社	100社	102社
⑭	防衛・航空宇宙産業（関東地方、中部地方、関西地方）	株式会社PFU	株式会社エヴァアビエーション、損害保険ジャパン株式会社、富士通株式会社	50社	50社
⑮	自動車産業（静岡、広島等）	東京海上日動リスクコンサルティング株式会社	東京海上日動火災保険株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社、NTTセキュリティ・ジャパン株式会社、NTTコムソリューションズ株式会社、ジェイズ・コミュニケーション株式会社	30社	31社

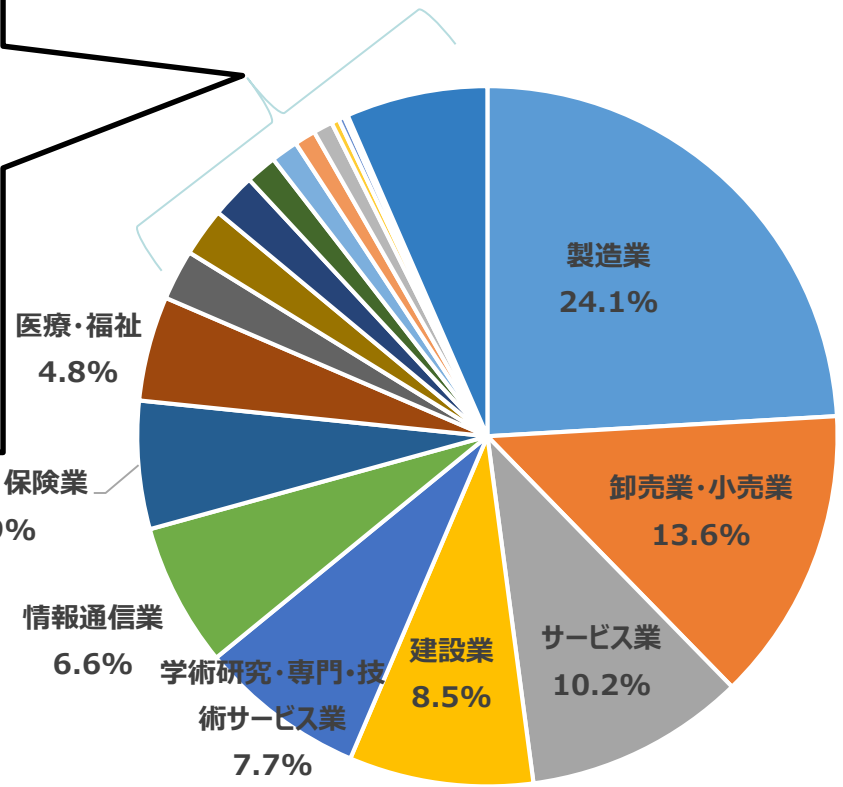
計 1,117社

実証参加企業の属性

- **計 1,117社実証参加企業の業種別内訳**は、「製造業」が24.1%で最も多かったものの、「卸売業・小売業（13.6%）」や「サービス業（10.2%）」など、**様々な業種より参加。**
- **実証参加企業の従業員数別内訳**としても、「1～5人」が24.3%、次いで「21～50人」が20.2%であったものの、「201人～300人」も3.1%含まれるなど、**多様性があった。**

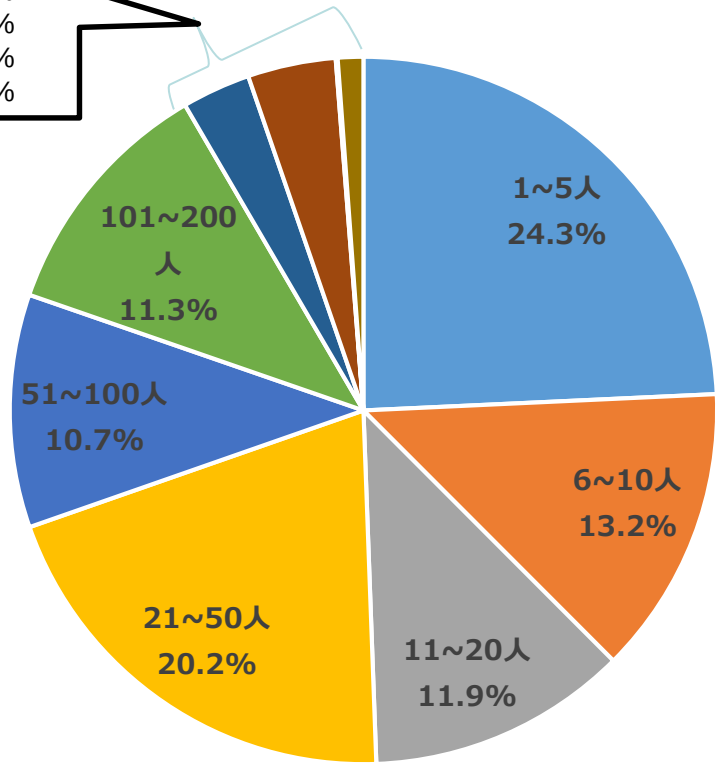
＜業種別一覧＞

不動産業・物品賃貸業　2.3%
宿泊業・飲食店　2.2%
運輸業・郵便業　2.1%
教育学習支援業　1.4%
複合サービス事業　1.3%
生活関連サービス業・娯楽業　1.0%、
農業・林業　0.9%
電気・ガス・熱供給・水道業　0.4%、
鉱業・採石業・砂利採取業　0.3%
公務　0.2%
分類不能の産業　6.5%



＜従業員数別一覧＞

201~300人　3.1%
301人以上　4.0%
1001人以上　0.1%
不明　1.2%



セキュリティ機器等によるサイバー攻撃の実態把握

- 各事業主体が選定したセキュリティ機器（UTM 機器、EDR ソフト等）を実証参加企業に設置（延べ1,190社）することで中小企業へのサイバー攻撃の実態を把握した。

＜セキュリティ機器等によるサイバー攻撃の実態把握＞

事業主体	実証参加企業数（社）	セキュリティ機器等によるサイバー攻撃の実態把握	
		内訳	設置社数（延べ数）
東日本電信電話	143	UTM機器	134
東北インフォメーション・システムズ	40	UTM機器	40
富士ソフト	71	ネットワークセンサー	71
デジタルハーツ	56	UTM機器	22
		MDR付きEDRソフト	24
富士ゼロックス	60	UTM機器	36
ＳＯＭＰＯリスクマネジメント	66	UTM機器	59
		EDRソフト	51
MS&ADインターリスク総研	76	UTM機器	50
		EDRソフト	50
名古屋商工会議所	140	UTM機器	29
		Defender監視ツール	6
		Web対策ツール	41
		メール対策ツール	7
大阪商工会議所	53	UTM機器	53
高松商工会議所	70	UTM機器(キヤノン)	16
		UTM機器(NTT西日本)	24
BCC	54	UTM機器	54
		EDRソフト	42
西日本電信電話	105	UTM機器	105
		EDRソフト	105
沖電グローバルシステムズ	102	UTM機器	15
		クラウドWAF	8
		簡易EDR	68
PFU	50	PCの脅威検知	50
東京海上日動リスクコンサルティング	31	UTM機器	30
合計	**1,117**		**1,190**

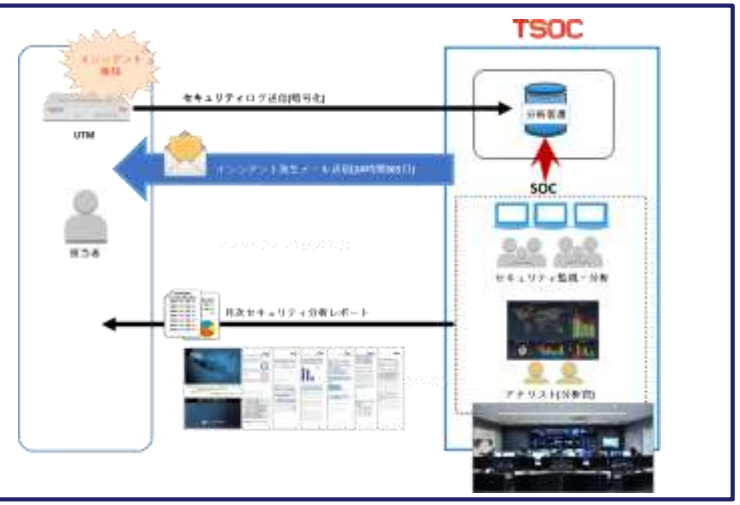
検知および監視の仕組みと実証結果

東日本電信電話株式会社（実証対象：北海道）

セキュリティ機器	＜UTM＞ 「おまかせサイバーみまもり」サービス	**設置社数（延べ数）**	**134**社
提供内容	UTM機器を設置し、通信監視・ログ把握による不正アクセス等の状況を把握する。 各企業のセキュリティ対策状況に応じた、更に必要となる対策を個別にレコメンド提供する。 一元窓口（サポートデスク）による各種困りごと受付、インシデント判断、遠隔・訪問サポートを行う。		
実証結果	**不正侵入(IPS)**は実証参加企業の**約80%**で検知し、**スパムメール**は実証参加企業の**約69%**で検知した。 **ランサムウェア**を実証期間内で**129件**検知した参加企業もあり、集中的にサイバー攻撃を受けている企業も存在していることが確認された。		

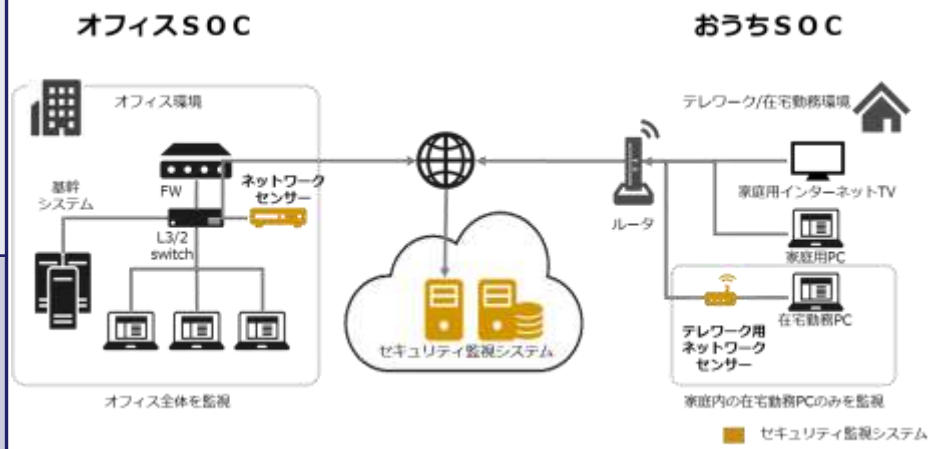
東北インフォメーション・システムズ株式会社（実証対象：青森県、秋田県、宮城県、山形県）

セキュリティ機器	＜UTM＞ FortiGate(Fortinet社製) WatchManBox MR(株式会社ハイテックシステム社製)	**設置社数（延べ数）**	**40**社
提供内容	UTMを設置し、ログを監視・分析を行う。 インシデントを検知した場合は、電子メールにて実証企業へ通知し、インシデント対応支援を行う。 セキュリティログを分析した結果をレポートに取りまとめ、月に一回レポートを提供する。		
実証結果	**外部からの不審なアクセス**は、**110件**検知・防御した。 **マルウェア**を**115件**検出・駆除した。 ・Webサイト経由で送られたマルウェア:**48件** ・電子メール経由で送られたマルウェア:**67件**		



富士ソフト株式会社（実証対象：岩手県）

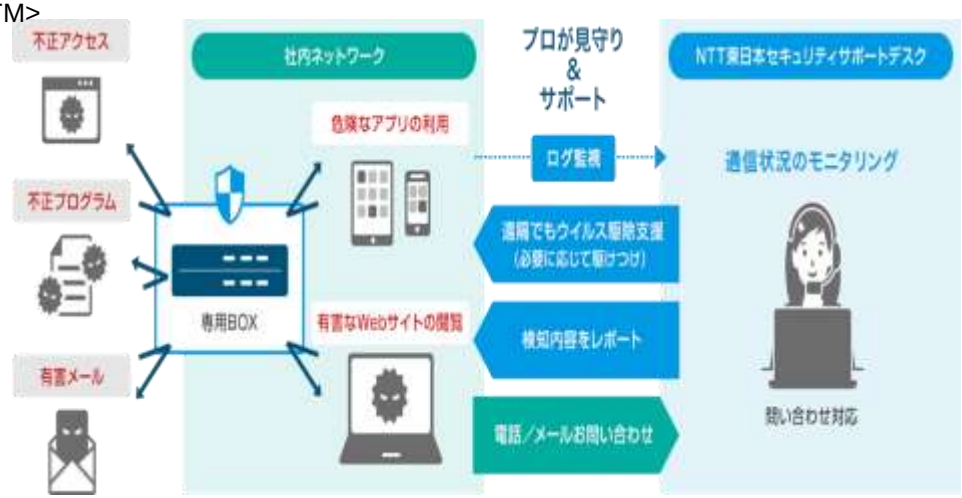
セキュリティ機器	＜ネットワークセンサ＞ オフィスSOC および おうちSOC	**設置社数（延べ数）**	**71**社
提供内容	対象企業のIT環境内に、ネットワークセンサーを設置し、対象企業のオフィス環境およびテレワーク環境におけるネットワーク挙動をセキュリティ監視システムとアナリストにて、監視、分析する。セキュリティ監視システムにて検出したアラートをアナリストが分析した結果、通報が必要と判断したものをインシデントとして対象企業に通知し、インシデント対応支援を行う。		
実証結果	水面下で侵攻するサイバー攻撃の状況をセキュリティ監視システムにて観測・収集し、AI基準で洗い出した結果、合計**3,539件**のアラートを検出した。 この結果を基に専門家による分析を行い、**7件**通報が必要と判断し、インシデントとして対象企業に通報し、リモートでの対処を実施した。 ・迷惑メールに分類されるソフトウェアの利用痕跡を検出(**アドウェア感染**）。通報し削除等の対応を実施した。 ・**フィッシングサイトへアクセス**した痕跡を検出。通報し、利用者の特定と情報入力していないかの確認と対策を実施した。 ・不審なIPアドレスからインターネット上の公開端末にURLスキャンが実施され、レスポンスを返していたことを検出(**不正なURLスキャンへの応答**）。通報し、公開している端末のログイン履歴確認と脆弱性対策を実施した。		



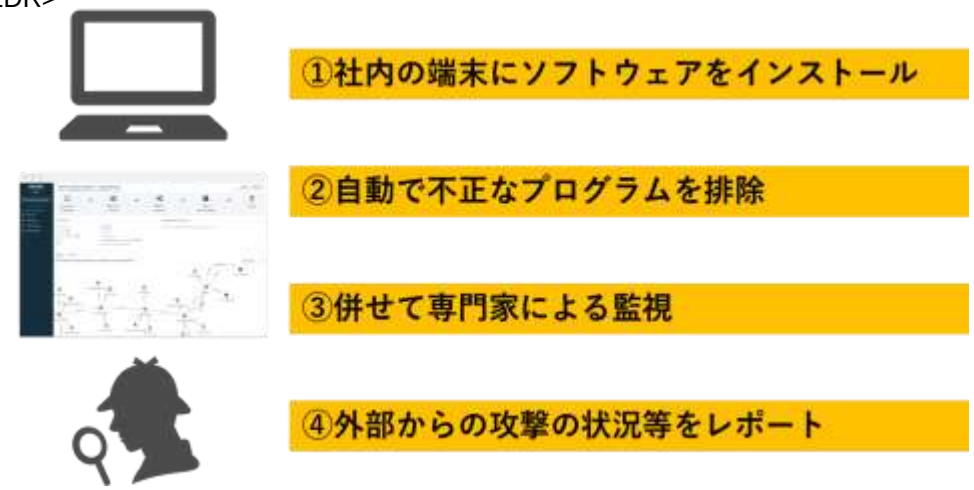
株式会社デジタルハーツ (実証対象：岩手県、宮城県、福島県)

セキュリティ機器	＜UTM＞ Cloud Edge(トレンドマイクロ社) +「おまかせサイバーみまもり」サービス(NTT東日本)	**設置社数(延べ数)**	＜UTM＞ **22**社
	＜EDR＞ Intercept X Advanced with EDR(Sophos社)		＜EDR＞ **24**社
提供内容	＜UTM＞ 対象企業のネットワークにUTMを設置し、セキュリティ対策を強化するとともに、通信状況をモニタリングする。 不正通信を行った場合などのインシデント発生の際には原因究明・環境復旧のサポートを行う。		
	＜EDR＞ 対象企業の各クライアント端末にEDRクライアントをインストールし、常時監視により適切な対応(専門家の解析、脅威除去支援、再発防止施策支援）を行う。		
実証結果	・UTM、EDRともに岩手県での検知が多く、福島県での検知が少ない結果となった。 ・UTM、EDRともに資本金5000万円～1億円未満の企業群での検知が多い結果となった。 ・UTMについて従業員21-50人の企業群、EDRについて従業員21人以上の企業群での検知が多い結果となった。 実証期間が短く、かつ、サンプル数も少ないため一概には判断できないが、地域や企業規模により変動が見られ、**一定以上の規模の企業において**相対的に**アラート件数が多く検出される**結果となった。		

<UTM>



<EDR>

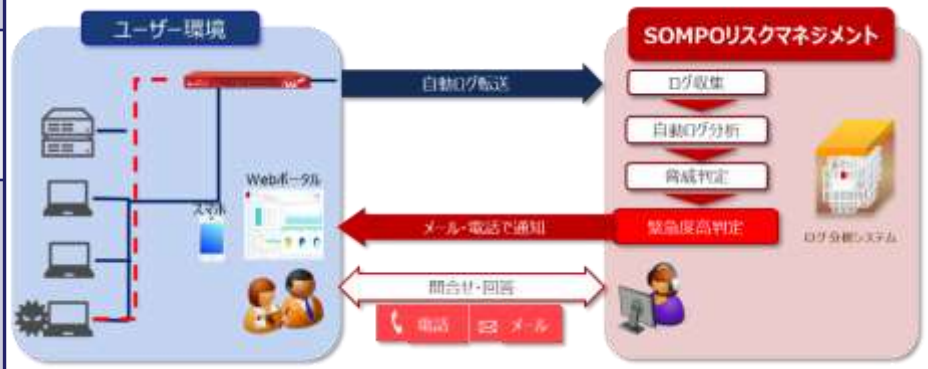


富士ゼロックス株式会社（実証対象：千葉県、埼玉県）

セキュリティ機器	＜UTM＞ beat-box(富士ゼロックス社)	**設置社数（延べ数）**	**36**社
提供内容	実証参加企業にUTM端末を設置し、調査期間中に収集したログ情報を分析し、グラフ等で可視化したレポートを実証参加企業に提供する。 異常を検知した場合は、ポート完全遮蔽により不正通信をブロックし、コンタクトセンターにて情報把握と対応を行う。		
実証結果	・検知したping/port-scanは、78ヵ国から合計17,958件、**1日あたり約17件/台**の**偵察行為**を受けていた。 ・不正と考えられる内部から外部への通信検知数は139,109件、1日あたり約86件/台に上った。 ・ブロックしたWebサイト数は364,413件、1日あたり約191件/台、外部へのアクセスをブロックした。 ・10月に埼玉県で請求書を装う**なりすましメール**を1件、 12月には千葉県で**ウイルス感染している可能性のある報告書が添付されたメール**が3日間に渡って**同じ企業に送付される事象**が確認された。(いずれもUTMで防御) ・全受信メール中、約11%でスパムメールを検知、1日あたり約8件/台のスパムメールを受信していた。		

ＳＯＭＰＯリスクマネジメント株式会社 (実証対象：千葉県)

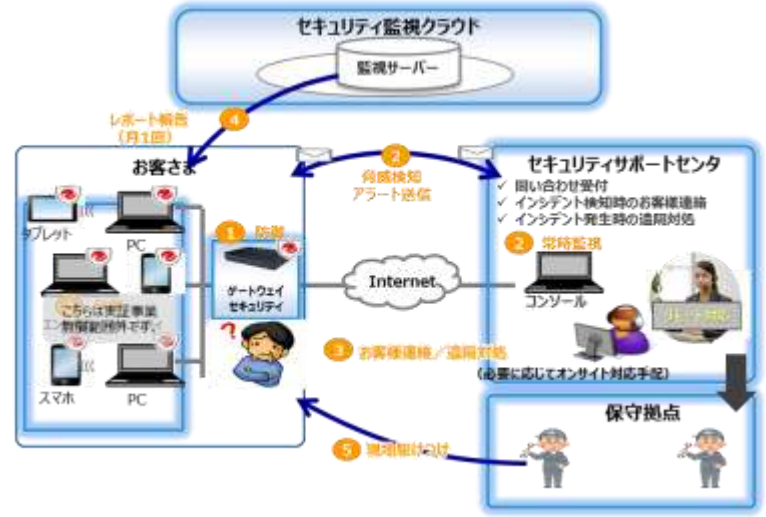
セキュリティ機器	＜UTM＞ Fireboxシリーズ(Watchguard社)	**設置社数(延べ数)**	**59**社
提供内容	UTMのセンサー（ファイアウォール機能、IPS機能、ウェブフィルタリング機能、スパムフィルタ機能およびアンチウイルス機能）によりセキュリティインシデントを検出する。また、ログを「セキュリティログ自動分析システム」に送信し分析し、3段階のランク付けを行い可視化する。		
実証結果	トロイの木馬、アドウェアといったウイルス侵入を、**約14%**の企業で検出され、駆除した。 スパムメールの侵入を、**約73%**の企業で検知され、防御した。 不正侵入(IPS)は**約32%**の企業で検知され、防御した。 悪意のあるWebサイトへの接続を、**約88%**の企業で検知され、防御した。 UTMの不正侵入(IPS)では検出できなかった**「不正なIPアドレスへの通信」**が成立していることをSOC機能にて検知し、緊急度「高」のアラートを発信し、リモートによる支援を実施した。		



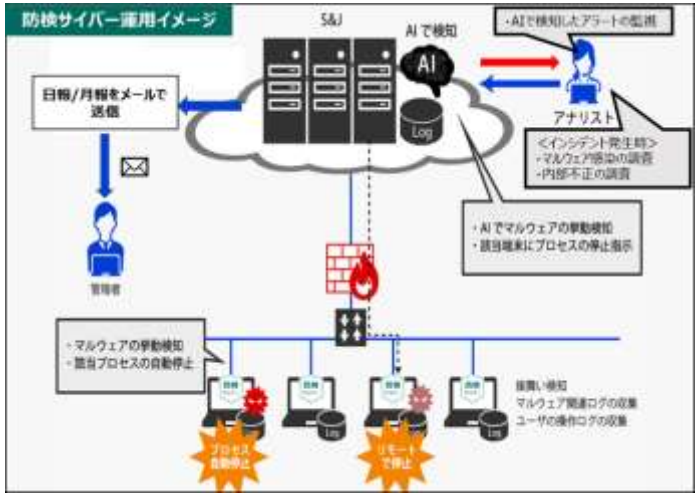
セキュリティ機器	＜EDR＞ エンドポイントセキュリティ対策ソフトウェア(SOMPOリスクマネジメント社)	**設置社数(延べ数)**	**51**社
提供内容	エンドポイントセキュリティ対策ソフトウェアを用いて、パソコンの挙動ログを収集し、セキュリティエンジニアが分析することで、不正プログラムの感染などのセキュリティインシデントを検出する		
実証結果	**不正プログラム**が**75%**の企業で検出され、駆除した。 不正なプログラムを配布しているサイトといった**不正なサイトへのアクセス**についても**47%**の企業で検出され、防御した。 **ブラウザ・ハイジャッカー**を検知し、駆除方法を案内したが自力で対応出来なかったため、**リモートで駆除**を実施した。		

MS&ADインターリスク総研株式会社 (実証対象：岐阜県を中心とする中部エリア)

セキュリティ機器	＜UTM＞ CloudEdge(トレンドマイクロ社)	**設置社数(延べ数)**	**50社**
提供内容	UTMの提供、監視サービス、各種照会が可能なコールセンター、有事の駆けつけをワンストップで提供する。 ・異常通信や振る舞いを検知・駆除する。 ・脅威検知内容をレポート化して参加企業に報告する。(月１回)		
実証結果	・UTM設置してすぐに**「C&Cコールバック」と見られる通知**を検知、防御し、リモートによるインシデント対応を実施した。 ・IPS（侵入防御システム）にて検知、防御が必要な通信を多数検知(約8万件）し、中小企業においてもサイバー攻撃の標的とされていることが確認された。 ・スパムメール対策機能による検知・駆除は、計23万件にものぼった。 ・ランサムウェアを１社で検知したものの、UTMで防御しており、感染被害はなかった。		



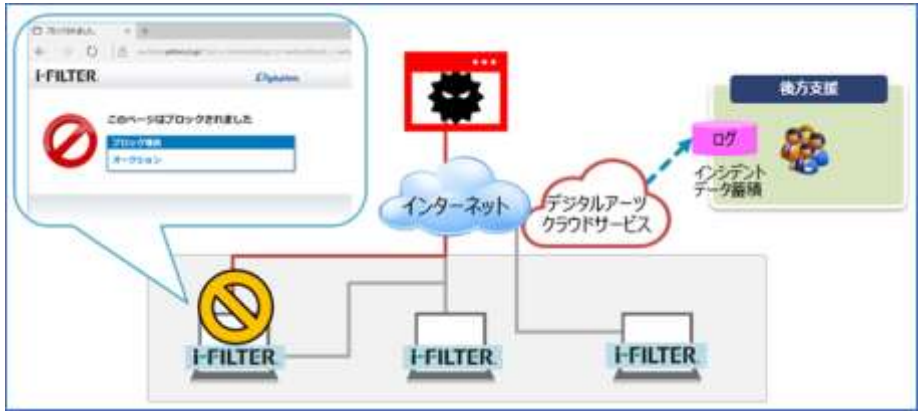
セキュリティ機器	＜EDR＞ 防検サイバー(MS&ADインターリスク総研)	**設置社数(延べ数)**	**50社**
提供内容	EDR導入による端末の遠隔監視、ログ保存、AIとアナリストによる防御・検知機能を提供し、コールセンターによる問い合わせ窓口の設置および異常と判断した場合の駆けつけ支援を行う。		
実証結果	「不審なコマンド実行」や「不審なプロセス起動」を合計1万件検知したが、アナリストによる調査の結果、大半が過検知によるものであった。 **サポートが終了した**メンテナンスされない**ソフトウェア（プラグイン）の振る舞いを検知**したため、注意喚起を行った。		



名古屋商工会議所 (実証対象：愛知県、岐阜県、三重県)

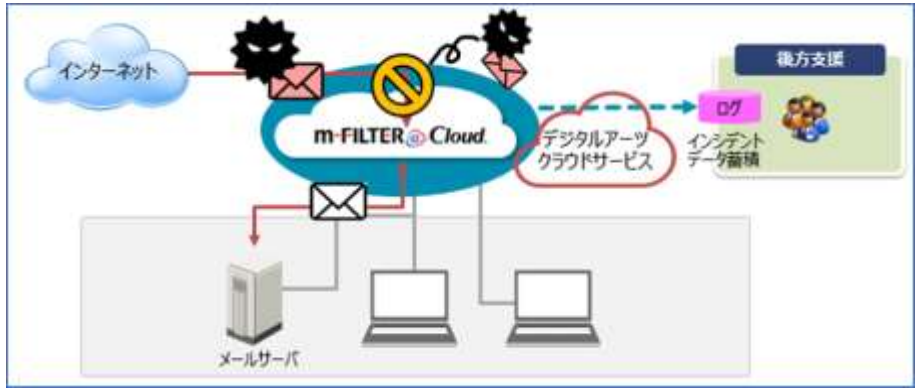
セキュリティ機器	＜UTM＞ CloudEdge(トレンドマイクロ社)	**設置社数(延べ数)**	**29**社
提供内容	導入企業のネットワーク上に統合脅威管理装置(UTM)を設置し、不正通信を抑止、インシデントのリモート監視を行う。インシデント発生時にはコールセンターからの遠隔サポートを行う。 また、UTMによる防御状態について毎月レポートを送付する。		
実証結果	**不正サイトへのアクセス**を合計で**400万件超**、検知・防御した。 これは導入企業1社1日平均で500件超の検知数であり、中小企業においても日々サイバー攻撃の脅威にさらされている実態を確認した。 **マルウェア**の検知・駆除で**19件**、**不正アクセス検知・防御**で**576件**の防御実績があった。		

セキュリティ機器	＜Web対策ツール＞ i-FILTER(デジタルアーツ社)	**設置社数(延べ数)**	**41**社
提供内容	導入企業の監視対象PCへi-FILTER（Agent）をインストールし、危険サイト閲覧を防止する。i-FILTERは、Webフィルタリングソフトに当たるが、マルウェア等の通信先である不正サイトへの通信において、ブラウザーを使用しない場合でも遮断することが可能である。		
実証結果	**不正サイトへのアクセス**を合計**624件**、検知・防御した。 そのほとんどが、「違法ソフト・反社会的サイト」であった。 導入企業の75%の企業は、ブロック数は10回以下であったが、１部の企業ではブロック数が200回近くに上る企業もあった。		



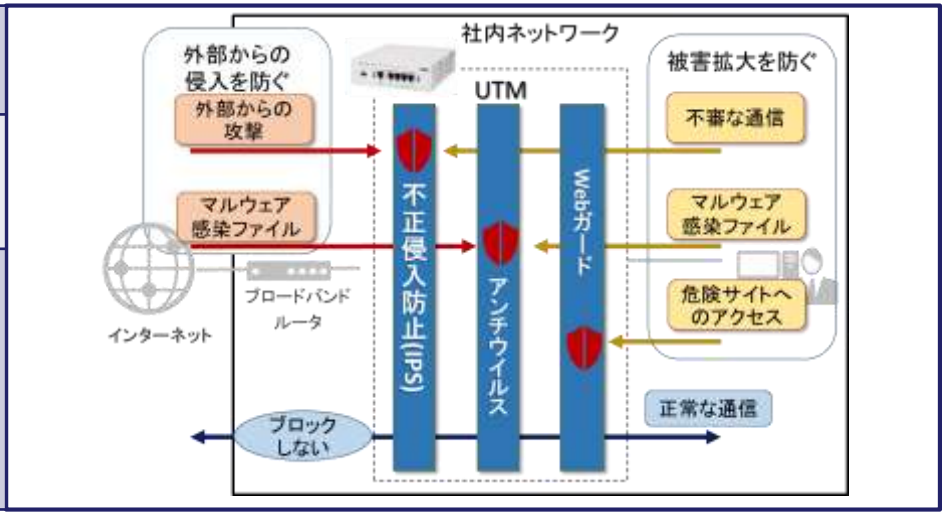
名古屋商工会議所 (実証対象：愛知県、岐阜県、三重県)

セキュリティ機器	<メール対策ツール> m-FILTER@Cloud（デジタルアーツ社）	**設置社数(延べ数)**	**7**社
提供内容	メール受信時に「送信元」「添付ファイル」「本文・URL」の偽装判定を行い、安全なメールだけを受信する。 危険なメールは隔離およびメール無害化を実施する。		
実証結果	セキュリティインシデントとして、標的型攻撃メール（疑い）の検知はなかったが、**スパムメール受信**を**60件**検知し、防御した。		



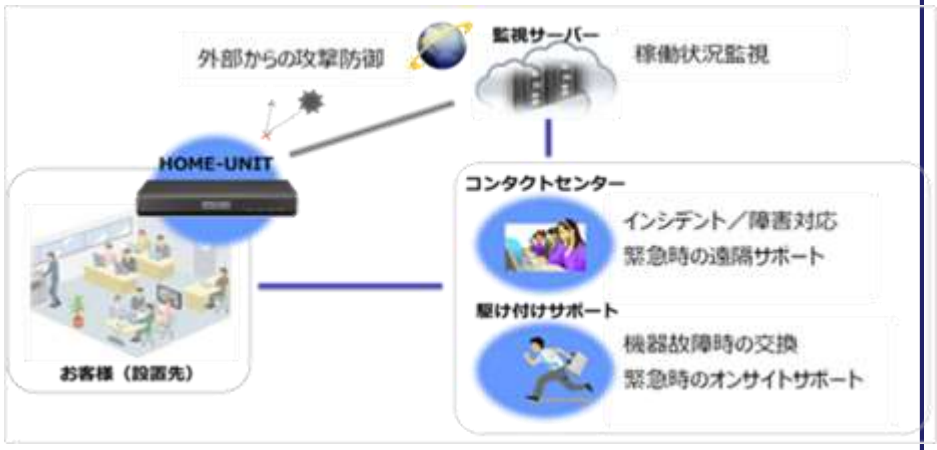
大阪商工会議所 (実証対象：滋賀県、奈良県、和歌山県)

セキュリティ機器	<UTM> 簡易UTM機器(NEC社)	**設置社数(延べ数)**	**53**社
提供内容	UTMをインターネット接続機器と監視対象端末(PC,モバイル機器など）の間に設置し、企業LANとインターネットの通信を監視。感染が疑われる場合、「重要アラート」として参加企業へメール通知し、駆けつけ支援又はリモート支援を実施する。		
実証結果	「外部からの攻撃」を約56%(30社)の企業において検知・防御した。 「外部への不正通信」「内部の脆弱性」を43%(23社)の企業において検知・防御した。 UTMがトロイの木馬を検知し、アラート通知。アラート通知をきっかけに、当該企業から相談を受け、リモート支援を実施し、**フルスキャンを実施した結果、内在していた別の脅威**を検出し、合わせて**駆除**した。		

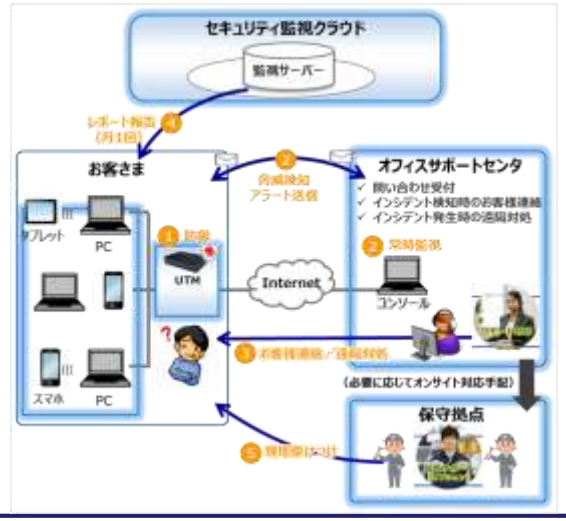


高松商工会議所 (実証対象：香川県)

セキュリティ機器	＜UTM①＞ HOMEネットワークセキュリティサービス(キヤノンマーケティングジャパン社)	**設置社数(延べ数)**	**16**社
提供内容	実証参加企業にUTMを設置し、通信ログを収集、レポート配信する。 正常稼働を監視し、障害発生時にはコンタクトセンターから遠隔サポートおよび保守委託拠点から駆け付けサポートを行う。		
実証結果	DoS/DDoS攻撃が70%の企業で検知され、防御した。 スパムメールが18%の企業で検知された。その多くはショッピングサイト、インターネット通販事業者からのメールがスパムメールと判定されていたが、一部不審なドメインも散見され、**フィッシングサイトへ誘導するようなメール**の可能性もあった。 URLフィルタリング検知は、全ての参加企業において検知された。その多くは、アダルト／兵器・武器／ショッピングなどのサイトへのアクセスであったが、**マルウェア／フィッシングサイト／違法ソフトへのアクセス**が約1割見られた。		



セキュリティ機器	＜UTM②＞ セキュリティおまかせプラン(NTT西日本社)	**設置社数(延べ数)**	**24**社
提供内容	実証参加企業にUTMを設置し、通信ログを収集する。 セキュリティ脅威の検知状況をまとめたレポートを送付する。(月１回) インシデント検知時はサポートセンタから連絡し、必要に応じて現地駆けつけ対応を行う。		
実証結果	**ランサムウェアが27件検知**され、防御したが、1社のみ特定の日に１つのWebサイトにて検知されていた。 スパムメールが計43,887件検知されたが、11月に検知数が大幅に増えており※1、 JPCERT/CC 等から注意喚起されている、「Emotet」および「IcedID」等の攻撃があったと推測される。		



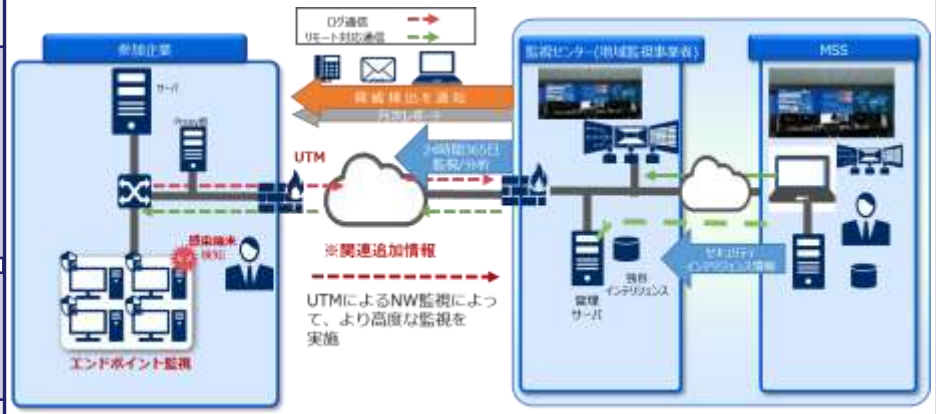
※1 スパムメール検知数は、9月:16件、10月:3,827件、11月:29,966件、12月:10,078件であった。

株式会社BCC

(実証対象：福岡県、佐賀県、長崎県、熊本県、大分県、宮崎県)

セキュリティ機器	＜UTM＞ サイバーセキュリティ見守りサービス(NEC社)	**設置社数(延べ数)**	**54社**
提供内容	中小企業が容易に設置および運用できるよう設計したUTMで通信を監視し、不正な通信の遮断やウイルスの無害化、有害Webサイトへのアクセス遮断を行う。 サイバーインシデントと判断された場合、相談窓口がリモートサポートによる対応もしくは駆け付け対応を行う。		
実証結果	UTMにより外部からの攻撃や外部への不正通信を検知および遮断した社数は、24社 特定の１社にて、UTM設置後、毎日10件程度検知された。(※1) 検収件数が突出している2社は、「情報通信業」であった。 **「アドウェア」に分類されるマルウェア**を1件検知し、駆けつけ対応により駆除を行った。ヒアリングした結果、不正プログラムはインターネットからダウンロードしたフリーソフトであったことが判明した。		

セキュリティ機器	＜EDR＞ エンドポイント監視サービス Type-Y(NEC社)	**設置社数(延べ数)**	**42社**
提供内容	実証への参加企業のエンドポイント端末にエージェントソフトを導入し、常時エージェントを監視する。異常を検知した際に通知を行い、対処を行う。パターンファイルに依存しない振る舞い検知型のマルウェア対策エンジンにより、未知のマルウェアを防御することが可能。		
実証結果	・検知総数は229件あり、そのうち**対応が必要な要注意検知(マルウェアの疑いがある検知）**があった社数は**20社**であり48%を占めた。 ・要注意検知数が最も多かった業種は「教育学習支援業」であり、62%を占めた。組織に属さない利用者に端末を貸し出して利用する機会もあり、組織のポリシーに則った利用がされない可能性が高いためと思われる。		

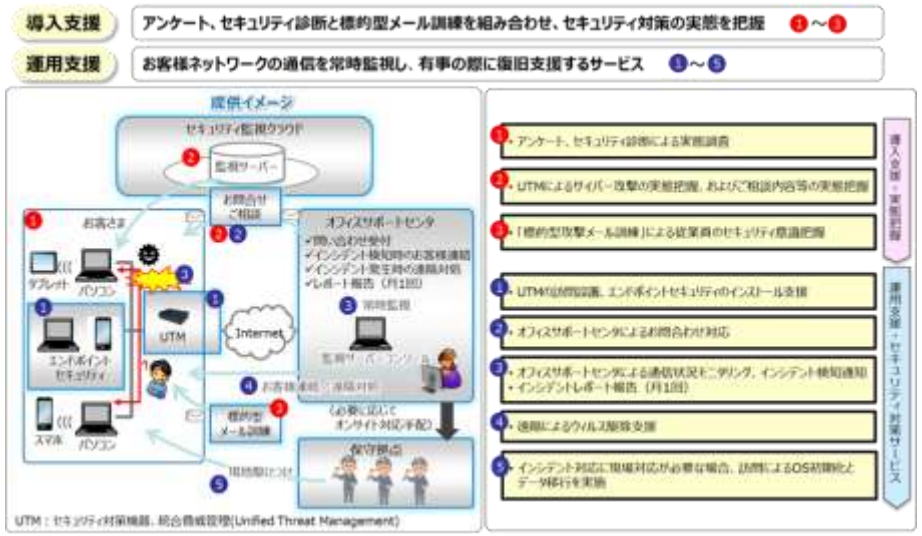


※1 WindowsNTからプリンタへの通信であり、問題ないものと確認後、検知対象から除外した。

西日本電信電話株式会社　熊本支店　(実証対象：熊本県)

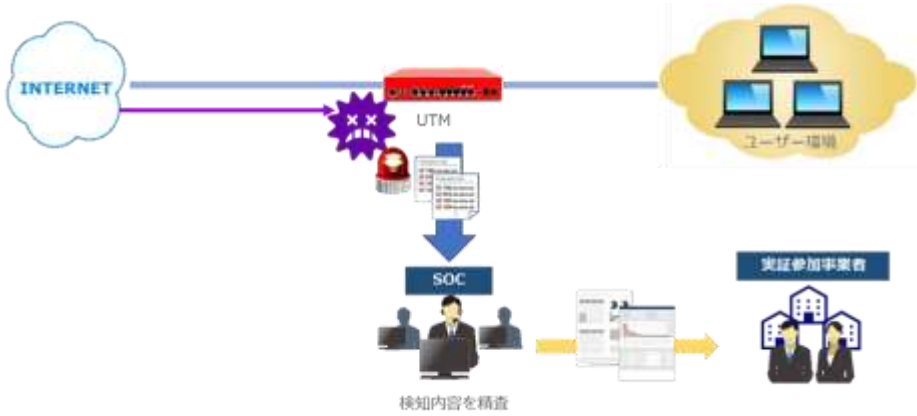
セキュリティ機器	＜UTM＞ CloudEdge(トレンドマイクロ社)	**設置社数(延べ数)**	**105社**
提供内容	導入したUTMのアラート状況を常時監視し、有事の際に必要な支援（遠隔支援、駆付け支援、データ復旧支援）を行う。未知の脅威に対しても対応が可能であり、ウイルスなのか判別できない場合、必要に応じてクラウド上に隔離された「サンドボックス」で試し実行し、ふるまいを解析し、危険なものはUTMで防御する。		
実証結果	スパイウェアの駆除/無効化およびWebフィルタリングは、参加企業数が増えた10月からは毎月発生した。 Webフィルタリングでは、**偽の通販サイト、詐欺サイト、フィッシングサイトなどへのアクセス**を防御しており、参加企業の社員教育が必要と考えられる。		

セキュリティ機器	＜EDR＞ セキュリティおまかせプラン　プライム(NTT西日本)	**設置社数(延べ数)**	**105社**
提供内容	エンドポイントセキュリティツールを導入した端末のアラート状況を常時監視し、有事の際に必要な支援（遠隔支援、駆付け支援、データ復旧支援）を行う。 エンドポイントセキュリティでは、ウィルス検知・駆除等を実施する。		
実証結果	代表的なウイルスとしては、EMOTEDと考えられる**トロイの木馬**が検出された。 ADW/PUAといった、フリーソフトウェアなどにバンドルされ、同時にダウンロード/インストールされている可能性が高い**グレイウェア**も検出された。		

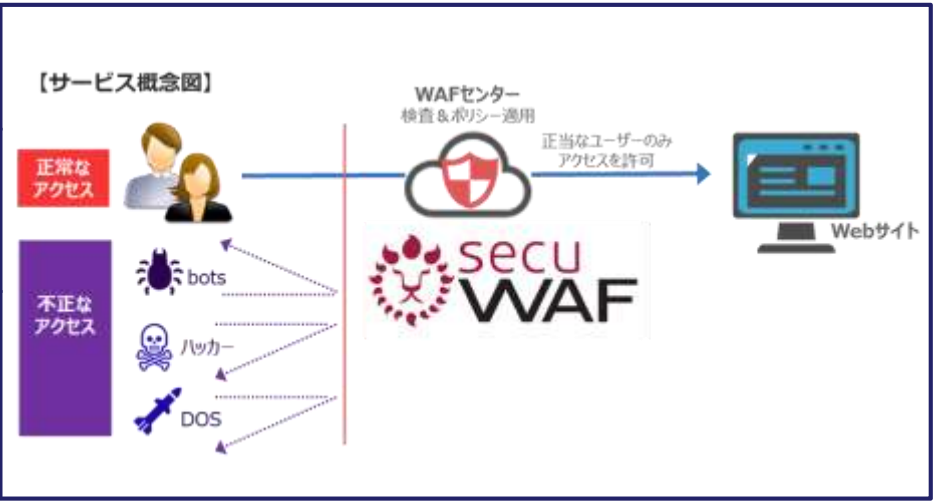


沖電グローバルシステムズ株式会社 (実証対象：沖縄県)

セキュリティ機器	＜UTM＞ Fireboxシリーズ(Watchguard社)	**設置社数(延べ数)**	**15社**
提供内容	UTM機器を設置し、不正な通信や不正アクセスやスパムメール、危険なWebサイトへの誘導等のサイバー攻撃を検知・防御する。UTMで攻撃を検知した際は参加企業へ直接アラートを通知するのではなく、一度SOC側にてアラートを受けて検知内容を精査し、対応が必要な場合にのみ通知する。		
実証結果	フィッシングサイトのような不正なWebサイトや評価の低い（危険度が高い） Webサイトへのアクセスを検知・防御した。 無意識に不正サイトへアクセスしている様子もあり、UTMの有効性が確認された。		

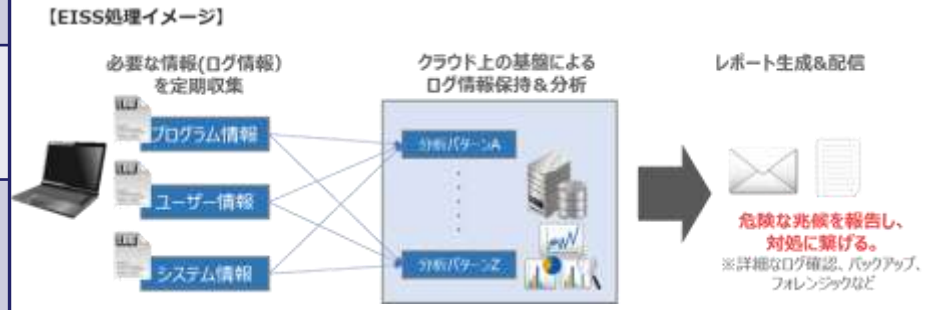


セキュリティ機器	＜クラウド型WAF＞ secuWAF(セキュアイノベーション社)	**設置社数(延べ数)**	**8社**
提供内容	Webサイトの改ざんやクレジットカード情報の搾取等のサイバー攻撃をWAFセンターで検査し、正当なユーザのみWebサイトのアクセスを許可する。		
実証結果	クラウドWAF側で有している検出ポリシーに基づき、**Webサイトへの攻撃を合計27,099件検知してブロック**をした。 導入した全てのWebサイトにおいて少なからず攻撃があることが判明した。 攻撃の種類を大別すると、**偵察行為にあたる攻撃が大半を占める**結果であった。		



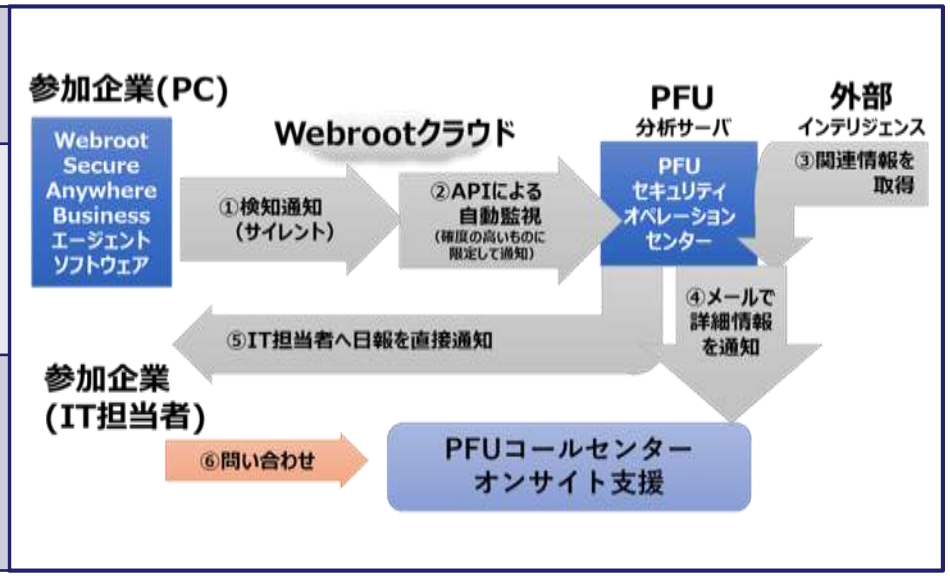
沖電グローバルシステムズ株式会社 (実証対象：沖縄県)

セキュリティ機器	＜簡易EDR＞ EISS(セキュアイノベーション社)	**設置社数(延べ数)**	**68社**
提供内容	エンドポイント（Windowsパソコン）における操作や生成ファイルなどのログ情報を記録・保持し、マルウェア感染後に発生する活動かどうかを定期的に分析し、情報漏洩などの被害に繋がる可能性に気付かせ、即時対応を行う。		
実証結果	「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の恐れがあります」というアラートが出た端末数は113端末であった。 詳細確認をした結果、過剰検知と判定しマルウェア感染をした端末の検出には至らなかった。		



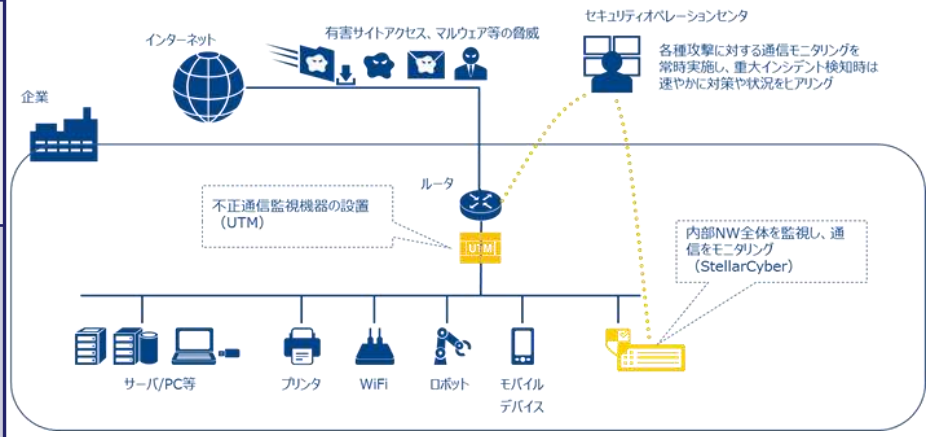
株式会社PFU (実証対象：防衛・航空宇宙産業（関東地方、中部地方、関西地方））

セキュリティ機器	＜PCの脅威検知ツール＞ 「SecureAnywhere Business」（WEBROOT社）	**設置社数(延べ数)**	**50社**
提供内容	参加企業のPCにWEBROOT社 SecureAnywhere Businessを導入し、クラウド上で管理する方式でサービスを提供する。ソフトウェアは、通常のアンチウイルスソフトの機能に加えて、未知の脅威を識別でき、クラウド上から隔離操作（処置）ができる機能を有している。 参加企業のPCがマルウェア等に感染し、参加企業自身で対処できないと判断した場合、駆け付けて状況調査やマルウェア駆除支援などの初動対応支援を行う。		
実証結果	アンチウィルスなどの既存対策をすり抜けた脅威として、業務上好ましくないアドウェア、ダウンローダーと呼ばれるものが、**1,766件検出**された（緊急に対処は必要でなかったものの、その後、脅威に繋がる可能性はあるもの）。		



東京海上日動リスクコンサルティング株式会社 （実証対象：自動車産業（静岡県、広島県等））

セキュリティ機器	以下の２パターンの監視機器を設置 <UTM>　Cloud Edge(トレンドマイクロ社) <ネットワークセンサー>　StellarCyber (StellarCyber社)	**設置社数（延べ数）**	**30**社　※1
提供内容	UTM機器を設置し、企業内の通信状態をモニタリングし、有害サイトへのアクセス等の不正な通信や不正アクセスを検知、必要に応じて自動で遮断を行う。 セキュリティインシデント発生時は、トラブル相談窓口を通じて状況を確認し、リモートサポートにて事象の解決を行う。また、リモートサポートによる解決が困難と判断した場合は、現地への駆け付け対応を行う。		
実証結果	検知された不正プログラム、ランサムウエアの数は、合計32件であり、特定企業において検知が多かった。 URLフィルタリング機能にて、有害または業務に無関係の通信として、約1900万件のアクセスを防御した。そのうち、99%はWeb広告で、Web広告以外でのアクセスブロック数は、1,612件であった。1,612件うち、詐欺サイトへ誘導されるケースが75%と大半であった。 インシデントと判断し、リモート支援を２件行った。 うち、１件はStellarCyberによる通信の監視にて**C&C通信と思われる不正アクセス**を検知し、当該端末をネットワークから切り離し、ウイルススキャンの実施を行った。 実際に通信を行っている端末の特定、疑わしい通信の特定については、当該企業の業務都合等の理由により、詳細調査を行えず、特定に至っていない。		



※1 StellarCyber　3社、CloudEdge27社

セキュリティ機器等による検知結果

- セキュリティ機器等により、サイバー攻撃に関する様々なアラート等を検知および防御した。
  アラート種別ごとの検知状況の取りまとめは以下のとおり。

アラート種別	アラート種別の説明	主なアラート検知状況
①外部からの不審なアクセス検知および防御（外→内）	外部からの不審なアクセス通信を検知・遮断し、バッファオーバーフローやWebクロスサイトスクリプティング等のソフトウェアやネットワークの脆弱性をついた攻撃を防御	外部からの**サイバー攻撃の探索活動である「ポートスキャン」が数多く行われている**ことを確認した。また、**直接的な攻撃**である「バッファオーバフロー」「クロスサイトスクリプティング」「Dos攻撃」等の攻撃も**数多く検知および遮断**した。また、PCをリモートで制御するためのツールをインストールするためのバックドアを検知、ブロックする事例もあり、新たな脅威も確認された。
②内部からの不正通信や不正プログラム検知および防御（内⇔外）	マルウェアの侵入が疑われる内部から外部への不正通信や不正プログラムの存在が疑われる通信を検知、感染を防御	不正プログラムの存在が疑われる通信を数多く検知し、防御した。特に**C&Cサーバへの通信**と考えられる不審な通信先へのアクセスを**検知および防御**した。同一企業で約4,000件発生した事例については、リモートによるインシデント対応を実施し、処置した。
③不正および不許可サイトへのアクセスブロック（内→外）	予め登録したセキュリティ上のリスクがある不正サイトや業務上許可されていないWebサイトへの接続をブロック（URLフィルタリング）	ほぼ全ての企業において、不正サイトへのアクセスを検知し、ブロックした。**特定企業に突出して発生する**傾向も見られた。また、業務上許可されていないWebサイトだけでなく、**偽の通販サイト**、**詐欺サイト**、**フィッシングサイト**などへのアクセスもブロックしており、**社員教育が必要**と考えられる。
④マルウェアの検知および無害化	メール添付ファイルやWebからのダウンロードファイルに含まれるウイルス、ランサムウェア、アドウェア等の検知と無害化	身代金要求型のマルウェアである**「ランサムウェア」を多く検知および無害化**した事例が数多く見られた。また、ウィルスが仕組まれていると思われる報告書を添付した、なりすましメールが３日間にわたって同じ企業に送付される事例も発生した。
⑤エンドポイントでのアラート検知および処置	パソコン端末にインストールしたEDRソフト等で不正プログラムの検知および防御や不正サイトおよび不許可サイトへのアクセスブロック	EDRソフト等により、相当数の**ランサムウェア**や**トロイの木馬**などの不正プログラムや不正サイトおよび不許可サイトへのアクセス痕跡等を検知し、ウィルスの駆除やブロック等の処置を行った。
⑥その他のアラート検知	スパムメールの検知や内部の脆弱性を検知	スパムメール検知では、導入した企業の7割超の企業で何らかの迷惑メールを受信していた。多くは広告メールであったが、フィッシングサイトへ誘導するような**悪意のあるメール**もあり、注意が必要である。内部の脆弱性では、バージョンの古いソフトウェアの使用や、不正アクセスを試みようとする疑いのあるコードが見つかるなど**Webサイトの脆弱性**が複数確認された。

- 事業主体によりセキュリティ機器や環境設定が異なるため、検知件数にバラツキはあるものの、導入したほとんどの中小企業で何らかのアラートが検知されており、**その業種や規模を問わずサイバー攻撃の脅威にさらされている実態が明らかに。**
- アラート種別やアラート内容も多岐に渡ることもあり中小企業自らこれを管理することは困難であるといえ、**セキュリティの専門家の活用が求められるところ。**

＜ネットワーク一括監視型(UTM機器等)による検知結果①＞

事業主体	設置社数	①外部からの不審なアクセス検知および防御（外→内）	②内部からの不正通信や不正プログラム検知および防御（内⇔外）	③不正および不許可サイトへのアクセスブロック（内→外）	④マルウェアの検知および無害化	⑥その他のアラート検知
東日本電信電話(UTM)	134	19,650	18,993	710	299	59,182
東北インフォメーション・システムズ(UTM)	40	110	0	–	115	–
富士ソフト(ネットワークセンサー)	71	2,121	1,348	70	–	–
デジタルハーツ(UTM)	22	430	219	52	7	2,385
富士ゼロックス(UTM)	36	17,958	139,109	364,413	6	8,566
ＳＯＭＰＯリスクマネジメント(UTM)	59	490	–	118,141	52	67,080
MS&ADインターリスク総研(UTM)	50	78,659	4,168	361	97	236,842

＜ネットワーク一括監視型(UTM機器等)による検知結果②＞

事業主体	設置社数	①外部からの不審なアクセス検知および防御（外→内）	②内部からの不正通信や不正プログラム検知および防御（内⇔外）	③不正および不許可サイトへのアクセスブロック（内→外）	④マルウェアの検知および無害化	⑥その他のアラート検知
名古屋商工会議所(UTM)	29	576	26	4,286,363	19	60(※1)
大阪商工会議所(UTM)	53	7,906	2,091	76	524	199
高松商工会議所(UTM①)	16	134	33,151	5,401	8	8,465
高松商工会議所(UTM②)	24	705	18	140	27	43,887
BCC(UTM)	54	25,698	118	66	90	25
西日本電信電話(UTM)	105	–	–	298	61	–
沖電グローバルシステムズ(UTM)	15	–	49	207	8	–
沖電グローバルシステムズ(クラウド型WAF)	8	27,099	–	–	–	–
東京海上日動リスクコンサルティング(UTM)	30	–	3,587	19,301,698	32	–

※1 メール対策ツールにて、スパムメールを60件検知した。

＜端末監視型(EDRソフト等)によるアラート等検知結果＞

事業主体	設置社数	⑤エンドポイントでのアラート検知および処置
デジタルハーツ (EDRソフト)	24	392
SOMPOリスクマネジメント (EDRソフト)	51	4,122
MS&ADインターリスク総研 (EDRソフト)	50	10,723
名古屋商工会議所 (Defender監視ツール/Web対策ツール)	47	624
BCC (EDRソフト)	42	229
西日本電信電話 (EDRソフト)	105	93
沖電グローバルシステムズ (EDRソフト)	68	0
PFU (PCの脅威検知ツール)	50	1,766

脆弱性診断等によるセキュリティ対策状況等の把握

● 事業主体ごとに、希望する中小企業に対して、①インターネット上に公開している自社のホームページやサービスサイト等に情報漏えいやページの改ざんに繋がる脆弱性（弱点）がないかを診断する**「外部診断（Webアプリケーション診断）」**、②社内PC上に脆弱性がないかを診断する**「社内PC脆弱性診断」**、又は③参加企業に対してヒヤリング等を行い、その結果を分析しセキュリティ対策レベルを診断する**「簡易セキュリティ診断」**等の診断サービスを実施した。

＜脆弱性診断等の実施状況＞

事業主体	脆弱性診断等によるセキュリティ対策状況等の把握	
	診断方法	実施社数
東日本電信電話	Webセキュリティ診断	108
東北インフォメーション・システムズ	脆弱性診断	3
	制御システム簡易リスクアセスメント	2
富士ソフト	簡易セキュリティ診断	71
デジタルハーツ	脆弱性診断（簡易）	43
	脆弱性診断（詳細）	5
富士ゼロックス	専門家によるヒアリング	53
ＳＯＭＰＯリスクマネジメント	公開情報の外部評価	57
MS&ADインターリスク総研	簡易セキュリティ診断	53
名古屋商工会議所	簡易セキュリティアセスメント	140

事業主体	脆弱性診断等によるセキュリティ対策状況等の把握	
	診断方法	実施社数
大阪商工会議所	簡易セキュリティ診断	57
高松商工会議所	簡易セキュリティ診断	72
BCC	セキュリティ簡易診断アセスメント	48
沖電グローバルシステムズ	Webアプリケーション診断	33
	プラットフォーム診断	23
PFU	情報セキュリティ整備状況診断	50
	社内PCの脆弱性診断	50
東京海上日動リスクコンサルティング	外部診断	30
	内部診断(社内PCの脆弱性診断)	31
	マルウェア対策診断	30
合計		**959**

脆弱性診断等によるセキュリティ対策状況等の把握実施結果

- **外部診断(Webアプリケーション診断）**を計278社に実施した結果、クロスサイトスクリプティング(※1)、ディレクトリインデックス(※2)、OSコマンドインジェクション(※3)といった危険度の高い脆弱性が合計**116件**確認され、**技術的支援**を実施した。

- **社内PCの脆弱性診断**は、計81社に実施した結果、セキュリティリスクが高い脆弱性が合計**15件**確認され、**技術的支援**を実施した。

- **簡易セキュリティ診断**においても、多くの事業主体において参加企業の**約7割**の企業で**セキュリティリスクが高い状況にある**と確認された。

※1「クロスサイトスクリプティング」とは、Webサイト利用者のブラウザに悪意のあるスクリプト(簡易プログラム）を送り込み、実行させることを許してしまう脆弱性
※2「ディレクトリインデックス」とは、Webコンテンツを格納するディレクトリ(フォルダ）配下のファイルが一覧表示されてしまう脆弱性
※3「OSコマンドインジェクション」とは、悪意のあるリクエスト(OSへの命令）により、不正に操作されてしまう脆弱性

相談・インシデント対応ほか技術的支援の状況

- 事業主体ごとに実証に関する相談受付および対応等の実施体制（コールセンター）を構築し対応した。
- セキュリティ機器による検知、および脆弱性診断等の結果に基づき、**合計293件のインシデント対応ほか技術的支援を行った。**
- セキュリティ機器の導入・設置支援等のための訪問対応が257件と多く、2019年度事業と同様に、中小企業において**セキュリティ監視機器の自力での設置が困難**な状況が確認された。

＜相談・インシデント対応ほか技術的支援の状況＞

対応種別	総数	相談・インシデント対応ほか技術的支援の状況	発生件数
コールセンター対応	**616件**	実証参加に関する問合せ	**78件**
		セキュリティ機器設置等の問合せ	**285件**
		セキュリティ対応の相談(各サービスの製品情報・必要性の相談、表示内容の見方、操作・設定方法等の運用に関する問合せ)	**56件**
		その他	**197件**
インシデント対応ほか技術的支援	**293件**	**電話およびリモート等によるインシデント対応ほか技術的支援(※)**	**291件**
		訪問によるインシデント対応（駆け付け対応）	**2件**
その他訪問対応	**283件**	機器設置等のトラブル対応	**26件**
		その他（セキュリティ機器の導入・設置支援等）	**257件**

※「電話およびリモート等によるインシデント対応ほか技術的支援」には、訪問によるインシデント対応の一次対応を含む

インシデント対応事例

- 新型コロナウイルス感染症拡大の影響もあり、**リモートにより管理可能なサービスの提供**が多く行われ、インシデント発生に際しても**概ねリモートによる支援対応**を実施した。

＜2020年度実証事業における具体的な対応事例＞

事例１	UTMサービスを導入した企業において、同一ホストにて断続的に**要注意検知が発生していることが確認**されたため、お助け隊事業者が駆けつけ支援を実施。 対象の**マルウェアと判定されたプログラム**は、インターネットからダウンロードしたフリーソフトであったことが判明、**駆除を実施**した。
事例２	UTMサービスを導入した企業において、PCの「ウィルス対策ソフト」を導入済みであったものの、**「不正なIPアドレスへの通信(※)」が成立していることが確認**されたため、緊急度「高」のアラートを発報、支援を実施した。 本件では、被害は確認されていないが、仮に情報漏えい等の被害に至っていた場合の被害試算額は、54,760,000円であった。 (※)直近1カ月の間にマルウェアの通信先になっていたことが確認されているIPアドレスへの通信
事例３	UTMサービスを導入した企業において、**マルウェアへの感染の疑いがある通信をUTMで検知**、リモート支援により駆除を実施。該当端末(PC)をLANから分離した上でフルスキャンを実施した結果、**Hacktoolおよびトロイの木馬、計6件のマルウェアを発見したため駆除を実施**した。
事例４	EDRサービスを導入した企業において、**不正プログラム「ブラウザハイジャッカー」**をEDRで検知、駆除方法を案内したが自力で対応出来なかったため、お助け隊が**リモート支援により駆除を実施**した。

アンケート、標的型メール訓練によるセキュリティ対策状況等の把握

- 事業主体ごとに参加企業等に対しアンケートによる調査を行い、セキュリティ対策状況等を把握した。併せて、実証参加企業のセキュリティに関する意識の向上を図る目的で、希望する企業に対して標的型メール訓練を実施した。
- 状況調査の結果、**ウィルス対策ソフト**は**9割程度**の中小企業で導入されているものの**UTM**の導入は**2割程度**しか導入が進んでいない実態が明らかとなった。**標的型メール訓練**では、開封率にバラつきがあったものの**開封率0の企業はなく、この点でのセキュリティリスクは残ると言わざるを得ない。**

＜アンケート調査の実施状況＞

事業主体	アンケートの回答社数	
	実証開始時 (事業説明会開催時も含む)	実証終了時 (成果報告会開催時も含む)
東日本電信電話	73	50
東北インフォメーション・システムズ	62	18
富士ソフト	90	
デジタルハーツ	59	22
富士ゼロックス	8	18
ＳＯＭＰＯリスクマネジメント	65	12
MS&ADインターリスク総研	51	42
名古屋商工会議所	136	29
大阪商工会議所	50	
高松商工会議所	72	45
BCC	43	39
西日本電信電話	104	82
沖電グローバルシステムズ	85	25
PFU	9	13
東京海上日動リスクコンサルティング	64	69

＜標的型メール訓練の実施状況＞

事業主体	実施社数
東日本電信電話	140
東北インフォメーション・システムズ	18
デジタルハーツ	56
富士ゼロックス	15
MS&ADインターリスク総研	51
高松商工会議所	30
西日本電信電話	60
計	**370**

実証参加企業から寄せられた声

- 2020年度実証参加企業のアンケート結果より、多くの声が寄せられた。

＜2020年度実証参加企業から寄せられた声＞

自社へのサイバー攻撃動向が把握できた

- 傾向の把握、他社比較が参考になった。
- サイバー攻撃の数値化ができた
- 要注意のメールやサイトの傾向や情報が得られた。
- 取引先のサイトが危険な状態であったことが理解できた。
- 自社の現時点での弱点が分かった。その対応策についてのアドバイスが得られた。

社員のサイバーセキュリティ意識・知識が向上した

- サイバーセキュリティの知識が身に付いた。
- 説明会で最新の知識を得ることができた。
- 実際に異常が感知されたため安全意識が高まった。
- セキュリティ対策を社内で検討した。
- 自社のセキュリティ面での改善に向けて、およそ何をすれば良いかを明確にすることができた。

自社へのサイバー攻撃・情報流出等が防げた

- 攻撃内容が見える化され回避・遮断によって安心できた。
- PC、NASからの不審なアクセスが確認できた。
- セキュリティ対策を行っていることで自社の社会的信用が向上した。
- 何かあった時に駆け付け支援してもらえるので安心できる。

経営層に今後のセキュリティ対策提案がしやすくなった

- セキュリティレベルが客観的に審査されることにより、経営層に今後のセキュリティ対策提案がしやすくなった。
- 情報セキュリティ計画を策定することになった。
- サイバーセキュリティ対策について自社のやり方が正しいか、全体を俯瞰してコンサルティングするサービスをしてほしい。

本実証事業のまとめ①　中小企業のセイバーセキュリティ対策の実態

セキュリティ機器等によるサイバー攻撃の実態把握

●サイバー攻撃そのものでなくとも**業種や規模を問わず不審な通信等の脅威にさらされており、**ウィルス対策ソフト等の既存の対策では防ぎきれていない実態が明らかとなった。

●インシデント対応ほか技術的支援は、2020年度は新型コロナウィルス感染症拡大の影響もあり、当初からリモートによる管理可能なサービス提供が多く行われたこともあり、**概ねリモートによる支援対応**となった。

●ある特定の1社で、11月～12月に「C&Cコールバック」と見られる攻撃を4,126件受けている事例や、「トロイの木馬」と想定されるものが多く検知されるなど**特定の企業が集中的に攻撃を受けている事例**が明らかとなった。

脆弱性診断等によるセキュリティ対策状況等の把握

●インターネット上に公開している自社のホームページやサービスサイト等に脆弱性診断において、実施した企業のほとんどで何らかの脆弱性が発見された。加えて、そのうち概ね**２割の企業**においては**重大なインシデントに繋がる可能性があると診断**された。

●脆弱性が指摘されている**古いバージョンのまま運営している事例**や暗号化等の**セキュリティ対策の設定がされていない**などの事例が報告された。

●工場ネットワークに繋がれたIT機器の調査を実施したところ、**サポートが切れているOSを使用している端末**が**14%**も見つかった。また、工場を保有している企業の88%は工場とオフィスのネットワークがつながれており、オフィスだけでなく工場のIT機器においてもセキュリティリスクが高い実態が明らかとなった。

アンケート、標的型メール訓練によるセキュリティ対策状況等の把握

- **ウィルス対策ソフト**は**9割程度**の中小企業で導入されているものの、**UTM**の導入は**2割程度**しか導入が進んでいないことが明らかとなった。
- サイバーセキュリティ対策に対しての課題は顕在化しているが、「具体的に何を対策すればよいのか」「どこまで対策すればよいのか」といった意見が多数寄せられた。
- セキュリティポリシーやルールの策定、インシデント対応体制の構築等の組織的な対応は遅れていることが分かった。また、IT資産に関する情報については半数以上が管理されていないとの報告もあった。
- 工場の端末においては、古いOSの残存やセキュリティパッチ適用が進んでいない状況が見られた。
- セキュリティ対策について予算は全くかけていない、あるいは最低限のみ対策費用をかけているという企業が多かった。セキュリティ対策に支払可能な金額は、**月額1万円程度**の回答が多かった。
- セキュリティ対策の課題は、**専門人材の不足**、社員や専門人材に対する**教育**がなされていない、**費用**を捻出することが困難といった点が挙げられた。

- 取引先からのセキュリティ要求については、30%～50%弱の企業で何らかのセキュリティ対策の要求があるという状況であった。**自動車産業**においては、**8割近くの企業がセキュリティ対策に関する要求を受けていた**。
- 中小企業における**テレワークの実施率**は**2割弱**であり、それほど高くない結果であった。
- テレワークを実施している企業におけるセキュリティ上の課題としては、リモートツールの未整備、私物端末の利用、ネットワーク環境の未整備等の**技術的な対策**が挙げられた。

- **標的型メール訓練**においては、開封率は1割～3割程度と実施内容によりバラバラであったが、**開封率0の企業はなかった**ことを踏まえれば、この点でのセキュリティリスクは残ると言わざるを得ない。
- 標的型メール訓練により、社員のセキュリティ対策意識が向上したと感じている企業が6割以上と一定の効果は得られたものの、それでも「一度で良い」と考えている企業も多く、**繰り返し実施することの必要性を伝えることが課題**。

本実証事業のまとめ②　セキュリティ簡易保険サービスのあり方

●実証結果で得られた結果を元に、各事業主体において、中小企業が利用しやすいセキュリティ簡易保険サービス（サイバー保険）のあり方について検討を行った。

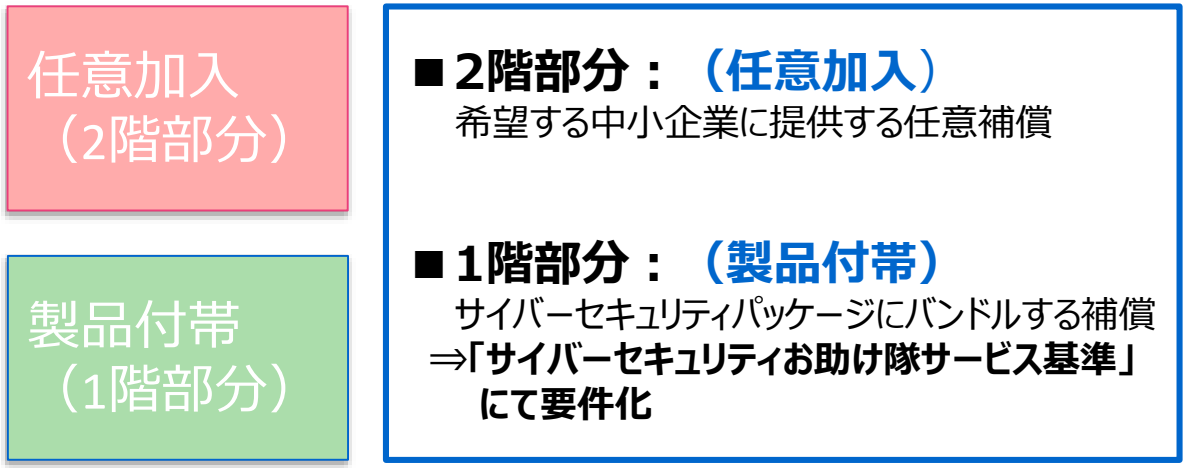
●サイバー保険に対する認知度は50%程度のところもあるなど、認知度が上がっていることが確認できたが、**サイバー保険に加入している企業は、10%未満と極めて低い水準**であった。

●その理由としては、サイバーリスクは目に見えないため、**必要性を感じていない**という声が多かった。一方で、必要性は認識しているものの加入しない理由としては「**予算がない**」という意見が多かった。

●上記を踏まえ各事業主体で検討した結果、①**サイバー保険は製品やサービスの付帯保険として提供され**、中小企業にとって加入しやすい価格帯とする、そして②インシデントが発生した場合の賠償費用やフォレンジック等の本格的な調査・対処費用については、**任意保険として提供する**という考え方が多数であった。

●他方で、中小企業によって**必要な補償範囲は異なる**ため、企業の規模やニーズに合わせて保険内容を変更することが出来る個別契約のサイバー保険の提供が望ましいという意見もあった。

セキュリティ簡易保険のイメージ図



本実証事業のまとめ③　実証終了後のサービス提供の可能性

実証終了後の民間サービスへの移行状況

- 中小企業が導入しやすいように必要なツールや支援サービスを全てパッケージ化した**エンドポイント型のサービスを提供予定。**（PFU）
- 2020年実証参加中小企業**105社のうち、約5割の53社が有償サービスを継続利用予定。**（NTT西日本）
- 実証終了後も本実証で提供したUTM**「SOMPO SOC」**とEDR**「SOMPO SHERIFF」**サービスを提供予定。（ＳＯＭＰＯリスクマネジメント）

2021年度以降の取組みイメージ（参考）

2019年度
（実証１年目）

2020年度
（実証２年目）

2021年度以降（民間で自走）

攻撃実態の把握

ニーズを踏まえたサービスのスリム化

地域特性・産業特性の考慮

実証事業：
中小企業が利用しやすい安価なセキュリティサービスの開発

意識啓発

事前対策とのセットによるリスク低減

導入・運用負荷を下げる方法の検討

お助け隊サービス審査登録制度：
一定の基準を満たすサービスに「お助け隊マーク」の利用を許諾。

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供

中小企業

自社の信頼性をアピール

取引先（大企業等）

サイバーセキュリティ お助け隊

お助け隊サービス利用の推奨等の中小企業の取組支援