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

（サイバーセキュリティお助け隊事業）

（実証対象：福岡県、佐賀県、長崎県、熊本県、大分県、宮崎県）

成果報告書

請負事業者：株式会社 BCC

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

目次

1. サマリー

本報告書は、株式会社 BCC（以下「BCC」という。）が「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」において実施した実証内容を報告するとともに、結果に基づき中小企業のサイバーセキュリティ対策について提言するものである。

福岡県、佐賀県、長崎県、熊本県、大分県、宮崎県内の中小企業 54 社を対象に、以下のサイバーセキュリティ対策サービスを提供し、それぞれの結果から、中小企業のサイバーセキュリティ対策の実態を把握し、今後中小企業が継続的に利用可能なサービスおよび保険について検討を実施した。

- セキュリティ診断
- エンドポイント監視サービス Type-Y
- セキュリティ対策機器（UTM）

2. 実証事業の全体像

2.1. 背景と目的

近年、対策が弱いとされる中小企業を対象とするサイバー攻撃やサプライチェーン全体の中で中小企業を踏み台とした大企業などへの被害が顕在化してきている。多くの中小企業はサイバーセキュリティ攻撃に対する意識が低く、自社がサイバー攻撃に遭うと思っていないため、サイバー攻撃に遭っていることに気付かず、その結果、サイバー攻撃の被害が拡大するケースも発生している。また、IT やサイバーセキュリティに関する知識が乏しく、トラブルが発生した場合に何が原因であるかを判断することが困難な状況にある。

サイバーセキュリティ対策を定着させていくことを目的に、持続可能な中小企業サイバーセキュリティ対策支援体制を構築するうえでは、中小企業のサイバーセキュリティの意識向上や実態・ニーズの把握や必要である。今回、中小企業のセキュリティ対策強化を図るうえで、IT ベンダー、損害保険会社、地元の団体などが連携し、実証事業を通じて実態に即した中小企業向けのサイバーセキュリティ対策支援サービスの検討を行う。

2.2. 実証事業の要旨と事業スキーム概要

2.2.1. 実証事業の要旨

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　サイバーセキュリティお助け隊事業（実証対象：福岡県、佐賀県、長崎県、熊本県、大分県、宮崎県）（以下、本実証事業）は、下記 3 項目を事業目的とした。

- 中小企業に対して、「エンドポイントセキュリティ監視サービス」「UTM 監視サービス」を提供（設置支援も対応）し、サイバーセキュリティの予防とサイバーインシデント発生状況の把握
- 「相談窓口（TEL、メールを含む）」「リモートサポート」などを提供し、中小企業のサイバーセキュリティに関する悩みの調査やインシデント発生時に必要となるリモート支援内容の検証
- 「インシデント判断支援」および必要に応じ「詳細なセキュリティ診断サービス」などを提供し、インシデントの深刻度の確認や緊急処置などインシデント時の総合的な対処、支援内容の検証（オプションサービスの追加の必要性を検証）

上記サービスをパッケージとして実証事業スキームを構築し、対象地域の中小企業に普及・浸透させるべく「地域コミュニティを起点とした事業説明会や地域実証」を実施する。また、実証事業を通じて、当該事業スキームをベースに中小企業が加入し易いサイバー保険の仕組みを検討する。

2.2.2. 事業スキーム概要

事業目的を実現するため、BCC を主体に業務ごとに役割を設け各専門分野について、それぞれ有力事業者へ再請負して対応した。

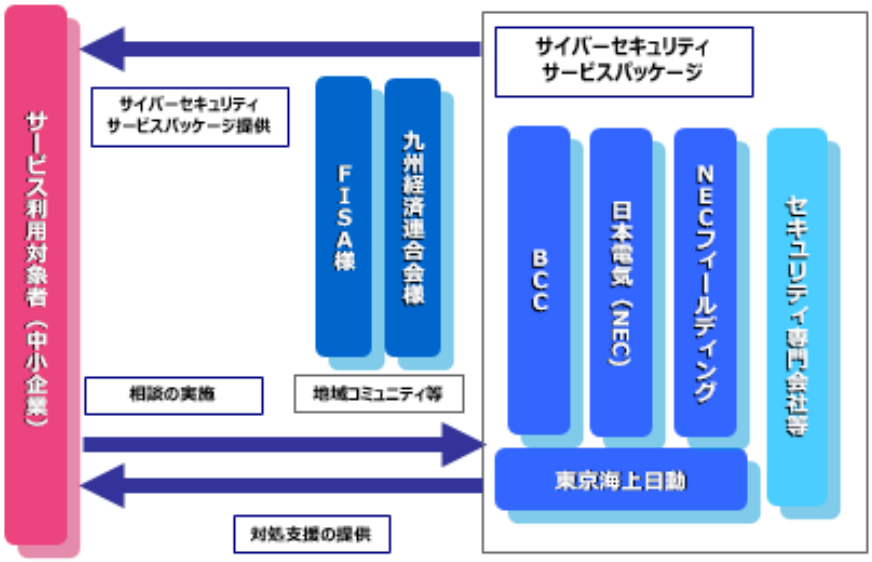


図 2.2.2-1 事業体制

企業名	業務ごとの役割
株式会社 BCC	実証事業の実施主体であり、全体の統括、運営を管理。 また、サービスパッケージを構築し、中小企業へ提供。その有効性を確認するとともに、普及活動を実施。
日本電気株式会社	既存セキュリティサービス、UTM などを提供、各種データ収集および検討を支援
NEC フィールディング株式会社	相談窓口、リモートサポート、駆け付けサービスなどを提供、各種データ収集および検討を支援
東京海上日動火災保険株式会社	本サービスパッケージに対応する保険の検討
セキュリティ専門会社など	中小企業の「セキュリティ実現」にかかわる対応などに関する評価、検討の支援、インシデント対応などの支援
地域コミュニティなど	中小企業への上記パッケージの普及支援

表 2.2.2-1 事業スキーム概要

2.3. サイバーセキュリティ対策の現状と課題の整理

- **想定される中小企業の現状**

現状としての課題と対応を仮定し、本実証事業での取り組み内容と整合させた。

- **課題と対応①**

課題	中小企業の多くは、セキュリティ対策実施の必要性や、自身のセキュリティ状態（インシデント発生）に気付けていない
対応	サイバー攻撃の予防対策とサイバー攻撃の認識ができる仕組みが必要
取組	既存サービスの活用により、エンドポイントでのマルウェアの挙動検知や不正アクセスの予防、インシデント発生の有無を判定する

表 2.3-1 課題と対応①

- **課題と対応②**

課題	中小企業の多くは、インシデント発生に気付いたとしても、対処方法もわからず、コストをかけての対処もできていない（大きな問題がなければ放置されている）
対応	気軽に相談できる窓口や、簡易処置を提供できる体制が必要
	何かあった時に的確に判断し対処ができる仕組みが必要
取組	相談窓口やリモートサポートの提供とインシデント発生時には、適切な助言を実施し、専門サービスの提供もしくは提案が可能
	初期対策および簡易対策費用の負担などによる行動変容により、任意加入保険の普及促進（＝サイバー対策の普及）も検討

表 2.3-2 課題と対応②

- **課題と対応③**

課題	仕組みを構築しても、中小企業への普及が不十分
対応	中小企業へのアクセスの充実した団体などを通じて、中小企業に適した仕組みを提供できる体制が必要
取組	中小企業がアクセスし易い地域コミュニティなどと連携することで、持続的で広範囲にわたる普及および促進を図る

表 2.3-3 課題と対応③

2.4. 現状の課題を踏まえた支援モデル

中小企業のサイバーセキュリティ対策の課題を「人間の健康状態」に置き換えると次の事項が課題であり、中小企業におけるサイバーセキュリティ分野では、いつでも誰でも気軽に受診できる仕組みの担い手がいないことが最大の課題（安定、継続性）である。

- 病気の予防をしていない、症状に気付いていない。（セキュリティ対策をしていない。サイバー攻撃に遭ったかどうかわからない。）
- 医師の診断（原因の特定）、治療（事後対応）を受けていない。
- 3 割負担の概念がない。（リスクの特定とコスト負担）

今回、支援モデルの検討に際し、中小企業向けに安定、継続的なサービスとして、遍く社内に普及、展開させるうえで、下記の仕組みを地域コミュニティなどの協力を得て運営することが必須であると判断して支援モデルの全体像を構築した。

- 病気の予防をしていない、症状に気付いていない。
  → 予防対策の復旧とサイバー攻撃の認識のため、既存サービスを有効活用する
- 医師の診断（原因の特定）、治療（事後対応）を受けていない。
  → 相談窓口の設置、リモートサポートの実施
- 3 割負担の概念が無い。（リスクの特定とコスト負担）
  → 初期対策・簡易対策費用の負担などを実施（任意保障にも繋がり易い仕組み作り）

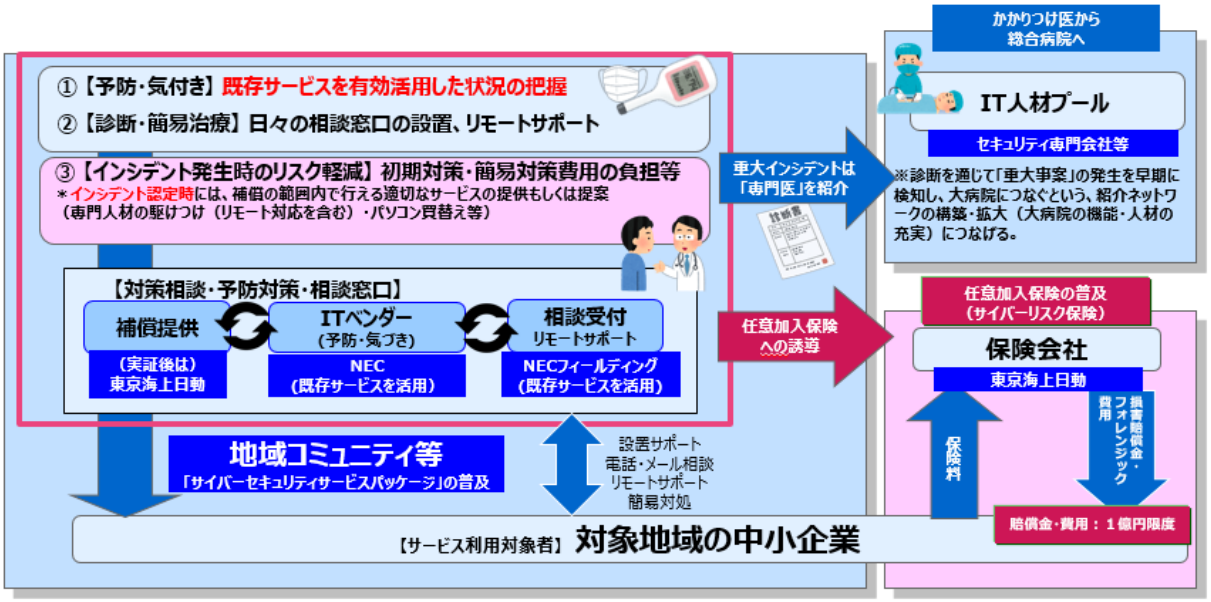


図 1.4-1 本実証事業の支援モデル

3. 実証参加企業の募集

3.1. 実証地域の選定

3.1.1. 九州地域の概況

IoT の普及やクラウド化が進み、外部攻撃も多様化し、従来のネットワークやサーバーの監視だけではマルウェアなどの外部からの侵入に対して十分にセキュリティを担保できない状況である。

近年のサイバー攻撃は、数や変化のスピードが速く、かつ巧妙化しているため、従来のゲートウェイ対策だけでは防御することが困難であり、中小企業におけるセキュリティ対策は、十分に行われていない。高度なセキュリティ対策を行ううえで、「エンドポイント保護の強化」が最も効果的な解決策と考える。しかし、一般的に高額となり中小企業がセキュリティ対策にかけられるコスト面から、かなり無理があること、更に大手企業が提供するサービスを使った場合、発見後の対処はエンドユーザーに委ねられ、その機能を十分に活用しきれないなどの課題が存在する。福岡県ならびに九州の他県も残念ながら、その類に漏れず、サプライチェーンを構成する中小企業各社は十分なセキュリティ対策が行われていない状況である。

3.1.2. 福岡県を中心とした九州圏の選定理由

九州エリアは国内でも高い生産年齢人口を占める政令指定都市福岡市を中心に、政府や行政機関、金融、空港、鉄道、電力、ガス、医療、物流、 化学などの重要社会インフラが密に集結しており、これらの下請けや孫請けを担う中小企業は福岡県を超えて、全九州エリアに広がっている。

福岡県の事業者数は、事業所数 13.5 万社であり、うち 99%を中小企業が占め、他県も福岡県以上の比率である。また、九州 7 県全体の従業者では、従業者総数 299 万人のうち 84%を中小企業が占めている。[i]

また、インバウンドの急増が顕著になると想定され、サービス業を中心に、外国の企業や個人と直接メールでやり取りするケースなども増加すると思われる。

以上のような九州地域のセキュリティ状況、理由から、九州圏で求められるサイバーセキュリティ対策サービスは、エンドポイントとネットワーク（社内ネットワークとインターネットの境界部分）の両面をカバーした安価かつ簡便なサイバーセキュリティ対策サービスであり、以下の内容を満たすパッケージサービスと考える。

- 簡易、安価なエンドポイント端末の「お守り（安全）」
- 簡易、安価なネットワークの 「お守り（安全）」
- 簡易、安価な SOC による「見守り」

[i] 中小企業庁 都道府県・大都市別企業数、常用雇用者数、従業者数 PDF（平成 30 年 12 月 14 日更新）
https://www.chusho.meti.go.jp/koukai/chousa/chu_kigyocnt/181130kigyou2.pdf（2021/1/22 参照）

- 簡易、平明なアラート通知による「気付き」
- いつでも電話相談できる窓口による「安心」
- 万が一の場合の現地への「駆け付け」
- 簡易、安価な保険による「補償」

そこで、本実証事業では、福岡県を中心とする九州 6 県（福岡、佐賀、長崎、熊本、大分、宮崎）の中小企業に対して上記を満たすパッケージサービスを提供し実施した。

なお、本実証事業では、低コストでの管理を考え、現時点で駆け付けの実行体制整備が難しい離島など含め一部の地域を除いている。

3.2. 参加募集の概要

3.2.1. 説明会による参加募集

以下の概要で本実証事業の説明会を実施し、実証参加企業を募集した。

(1) 説明会概要 （約 40 分）

- 本実証事業について
  → IPA お助け隊事業の説明
- 本実証事業に対する BCC の取り組みについて
  → 本実証事業および本実証事業のベースとなる BCC の取組みについての説明
- 提供する内容について
  → 今回の実証事業で提供するサービスについての説明
- 参加する企業様へ
  → 本実証事業へ参加するメリットや注意事項の説明
- 質疑応答およびアンケート記入
  → 質疑応答および中小企業のセキュリティ実態把握のためのアンケート実施

(2) 募集方法

説明会への主な参加募集方法は以下のとおりである。

- 九州経済連合会の会員（約 900 社）に対する FAX 配信での案内（2 回配信）
- 福岡県情報サービス産業協会の会員（178 社）に対する DM 配信（2 回配信）
- 福岡商工会議所のメルマガ会員（約 6,000 社）への DM 配信
- 九州経済産業局主催コミュニティなどの参加企業（約 4,000 社）への DM 配信

(3) ウェビナー開催

以下の日程でウェビナーでの説明会を実施した。

日程	説明会参加企業数	実証参加企業数
2020/09/07	0	0
2020/09/08	17	1
2020/09/14	4	0
2020/09/15	7	0
2020/09/16	2	2
2020/09/17	4	3
2020/09/23	1	0
2020/09/24	3	2
2020/09/28	0	0
2020/09/29	0	0
2020/09/30	3	2
2020/10/05	0	0
2020/10/07	0	0
2020/10/09	1	0
2020/10/12	0	0
2020/10/14	3	2
2020/10/19	2	0
2020/10/23	1	0
計	**48**	**12**

表 3.2.1-1 ウェビナーの日程

(4) 実地での説明会開催

以下の日程で実地での説明会を実施した。

日程	場所	説明会参加企業数	実証参加企業数
2020/09/10 09:30	九州経済連合会 会議室	0	0
2020/09/10 11:00	九州経済連合会 会議室	2	0

表 3.2.1-2 実地での説明会日程

3.2.2. 直接訪問による参加募集

以下の概要で直接訪問により、参加を募集した。

時期	参加要請数	参加企業数
2020/09	10	8
2020/10	47	34
2020/11	0	0
計	**57**	**42**

表 3.2.2-1 直接訪問による参加募集

3.3. 参加募集の結果

3.3.1. 実証参加企業数の推移

本実証事業における参加募集のイベントと申込数の推移は以下のとおりである。

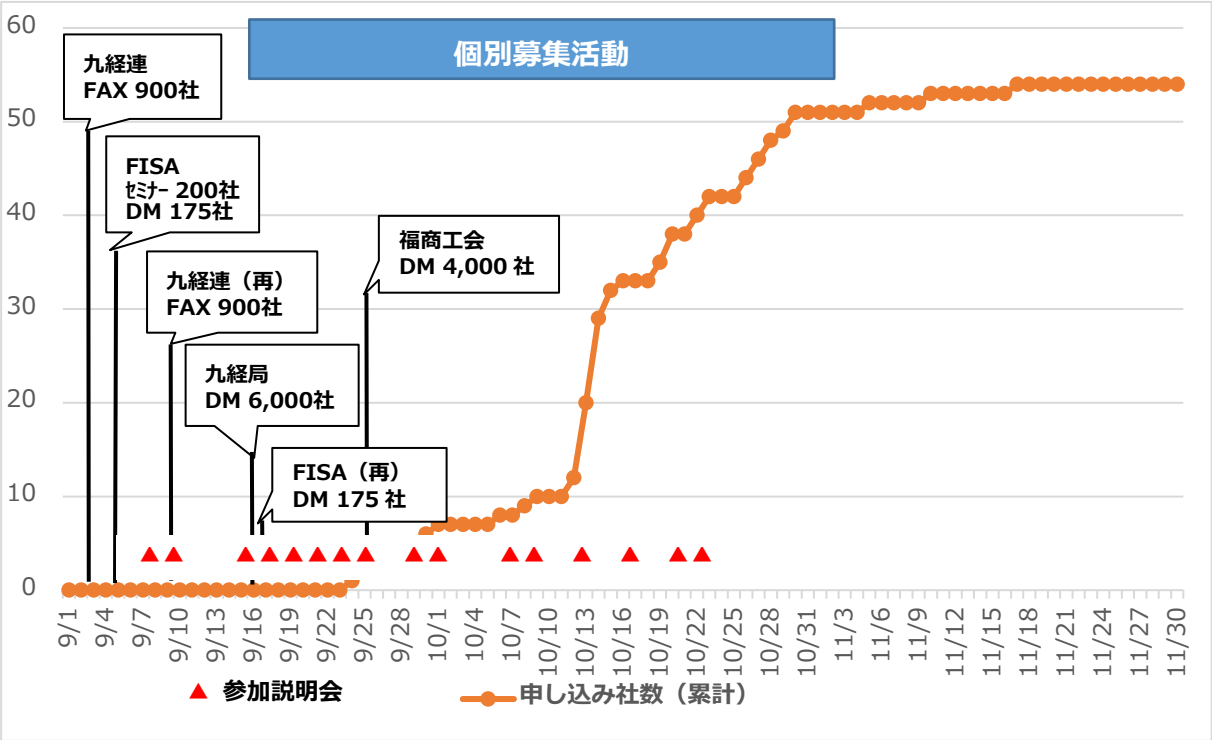


図 3.3.1-1 参加申込推移

3.3.2. 実証参加企業数

(1) 実証参加企業数（規模（従業員）別）

規模（従業員）別での実証参加企業数は以下のとおりである。

実証参加企業の規模（従業員）	実証参加企業社数（割合）
10 人未満	10（18.5%）
10 人以上 50 人未満	19（35.2%）
50 人以上 100 人未満	10（18.5%）
100 人以上 200 人未満	6（11.1%）
200 人以上 300 人未満	7（13.0%）
300 人以上 500 人未満	0（0%）
500 人以上	2（3.7%）

表 3.3.2-1 実証への参加企業数（規模（従業員）別）

実証参加企業は 10 人以上 50 人未満の規模（従業員）が最も多かった（19 社（35.2%））。本実証事業で使用した UTM の監視規模台数が 100 台までであったため、規模（従業員）も 100 人未満が 70%以上になったと推測する。

(2) 実証参加企業数（県別）

県別での実証参加企業数は以下のとおりである。

	福岡	佐賀	長崎	熊本	大分	宮崎
実績数 （割合）	29（54%）	7（13%）	6（11%）	3（5%）	2（4%）	7（13%）
会員数比	35（70%）	3（6%）	3（6%）	4（8%）	3（6%）	2（4%）
中小企業数比	21（42%）	4（8%）	7（14%）	8（16%）	5（10%）	5（10%）

表 3.3.2-2 実証参加企業数（県別）

目標値としていた経済団体の会員割合と比べ福岡県の割合が低かったが、参加実績は、九州における中小企業数の実際の割合に近づき、より現実に沿った実証に繋がった。

(3) 実証参加企業数（業種別）

業種別での実証参加企業数は以下のとおりである。

実証参加企業の業種	実証参加企業社数（割合）
A 農業・林業	-
B 漁業	-
C 鉱業・採石業・砂利採取業	-
D 建設業	2（3.7%）
E 製造業	9（16.7%）
F 電気・ガス・熱供給・水道業	2（3.7%）
G 情報通信業	13（24.0%）
H 運輸業・郵便業	6（11.1%）
I 卸売業・小売業	4（7.4%）
J 金融業・保険業	-
K 不動産業・物品賃貸業	2（3.7%）
L 学術研究・専門技術サービス業	-
M 宿泊業・飲食店	1（ 1.9%）
N 生活関連サービス業・娯楽業	-
O 教育学習支援業	2（3.7%）

実証参加企業の業種	実証参加企業社数（割合）
P 医療・福祉	3（5.5%）
Q 複合サービス事業	-
R サービス業（他に分類されないもの）	10（18.5%）
S 公務（他に分類されるものを除く）	-
T 分類不能の産業	-

表 3.3.2-3 実証参加企業数（業種別）

全業種の企業からの参加には至らなかったが、業務で IT 環境を利用しにくい第一次産業を除いた数多くの業種からの参加を得られた。本実証事業で提供するサービスへの賛同企業の参加が一定数あった。

(4) 実証参加企業募集に対する課題と考察

九州経済連合会、福岡県情報サービス産業協会、福岡商工会議所、九州経済産業局など多くの地域団体の協力で約 900 社への FAX、延べ 12,000 社以上のメルマガ配信など福岡を中心にした九州 6 県の多く中小企業への説明会案内の周知を行ったが、48 社の説明会参加に留まった（実証事業への参加 12 社）。このことから九州地域の中小企業のセキュリティに関する意識は未だ低いと考える。説明会参加から実証事業へ参加した企業は、全体の 25%程度であった。実証参加企業の業界や業種、県別における特徴的な偏りはほとんど見あたらなかった。

コロナ禍により、説明会はオンラインでの開催（動画のウェビナー配信）が主となった。オンラインでは、複数回の開催が容易に実現でき、開催日時の選択の幅が広がったことで、参加し易かったという意見が多く、主催者側の開催負担も少なかった。一方で、現地開催に比べてコミュニケーションが取りづらく、主催者側の想いや参加のメリットなどが伝わりにくい点が、説明会参加からの実証事業への参加が少なかった要因の一つであったと感じた。

4. 中小企業のセキュリティ実態把握

4.1. 実態把握の方法

4.1.1. サイバーセキュリティに関するアンケート調査

(1) 目的

九州圏の地域性や業種、企業規模などの違いによる中小企業のサイバーセキュリティの実態を見える化する。

(2) サイバーセキュリティに関するアンケート

サイバーセキュリティの実態の測定にあたり、事業参加説明会に参加した企業に対し、アンケート形式で収集した。

現地説明会への参加企業に対しては紙でのアンケート、オンラインでの参加企業に対してはオンライン説明会参加時にアンケート回答ツールにて収集を実施した。

アンケートは、地域、業種、企業規模などの基準に、企業内のセキュリティ対策の実情やセキュリティインシデント発生の実態を偏りなく確認することを目的としている。

(3) アンケート概要

アンケートは、10 項目の質問から構成（表 4.1.1-1）され、それぞれの質問について択一形式、複数選択形式で参加企業に回答してもらい、その結果からサイバーセキュリティの実態を見える化した。

質問	選択
保有されている端末／サーバーの台数は、おおよそ何台くらいでしょうか？	1～5 台
	6～10 台
	11～20 台
	21～30 台
	31～50 台
	51～70 台
	71～100 台
	101 台～
セキュリティ対策への取り組みは十分でしょうか？	十分できている
	最低限は実施している
	不十分
	わからない
サイバー攻撃の被害を受けたことがありますか？（受けたことがある被害をすべてお答えください）	メール経由でのウイルス感染
	Web 経由でのウイルス感染
	USB などによるウイルス感染

質問	選択
	DoS 攻撃
	HP 改ざん
	情報漏えい被害
	システムダウン被害
	データ損壊、暗号化被害
	金銭流出
	わからない
サイバー攻撃を受けたときはどうされていますか？	クリアインストール
	専門業者依頼
	未対処
	その他
セキュリティ対策の状況を教えてください。 （対処されているものをすべてお答えください）	アンチウイルスソフト
	ファイアウォール
	UTM
	メールセキュリティ対策
	データの暗号化・パスワード設定
	情報セキュリティ基本方針の作成＆社内周知
	社員教育
	サイバー保険
システム担当者は専任ですか？	専任者あり
	専任者なく IT 業者に外注
	専任者なく、兼任者のみ
	担当者はいない
サイバー対策に年間どのくらいの費用をかけていますか？	5 万円以下
	5～10 万
	11～20 万
	21～30 万
	31～40 万
	51～100 万
	101 万～
	わからない
取引先からのサイバー攻撃対策の指示はありますか？	取引要件となっている
	依頼されている
	何も言われていない
	わからない
SECURITY ACTION の登録状況を教えてください。	一つ星

質問	選択
	二つ星
	検討中
	登録する予定なし
	知らなかった
本実証事業への参加意思のご確認	ぜひ参加したい
	参加方向で社内検討
	より詳細な説明を聞きたい
	参加予定なし
	わからない

表 4.1.1-1 サイバーセキュリティに関するアンケート

● アンケート収集期間および収集件数

- アンケート収集期間

アンケートは、以下の期間の現地説明会 2 回とオンライン説明会 13 回で収集した。

2020 年 9 月 8 日（火） ～ 2020 年 10 月 14 日（水）

- アンケートの収集件数

説明会の参加企業からのアンケート回答状況は以下（「表 4.1.1-2」）のとおりである。

説明会の参加企業数	48
有効回答数	43

表 4.1.1-2 アンケート回答状況

4.1.2. 5 分でできる！情報セキュリティ自社診断

(1) 目的

IPA の「5 分でできる！情報セキュリティ自社診断」を実証参加企業各社に実施してもらい、中小企業のセキュリティの弱点を認識し、SECURITY ACTION ★2 レベルに到達するのに必要な課題を整理する。また、「5 分でできる！情報セキュリティ自社診断」は、実証前と実証後の 2 回実施し、実証参加により、セキュリティ意識の変化があったかを検証する。

(2) アセスメント概要

「5 分でできる！情報セキュリティ自社診断 」の 25 項目の各社の平均値を算出する。算出した平均値から、九州地区の中小企業を業種、地区などで分析し、弱点とするセキュリティ対策と今後の必要な課題を明確にする。

4.1.3. セキュリティ簡易診断アセスメント

(1)　目的

実証参加企業のセキュリティレベルを測定し、九州都市部、郡部の地域性の違いによるセキュリティ到達度を見える化する。

(2)　セキュリティ簡易診断アセスメントシート

セキュリティレベルの測定にあたり、セキュリティ簡易診断アセスメントシートを用いた。

セキュリティ簡易診断アセスメントシートは、お客様のセキュリティ対策状況を技術面・運用面・物理面から広い視点で確認し、課題を絞り込むためのリスクアセスメント支援ツールであり、製品やサービスの導入有無だけでなく、技術面・運用面・物理面から広い視点で確認することを目的とした。

(3)　アセスメント概要

アセスメントシートは、5 つの分類と 20 項目の質問から構成（4.1.3-1）され、それぞれの質問について 5 段階（表 4.1.3-2）で実証参加企業から回答を得た。

分類	No.	項目名
組織的・人的 セキュリティ対策	1	情報資産の分類・管理
	2	要情報の持ち出し制限
	3	外部委託管理
	4	セキュリティ教育の実施
物理的 セキュリティ対策	5	外部からの物理的侵入対策
	6	端末の物理的対策
	7	外部媒体管理
	8	記録媒体の処分
技術的 セキュリティ対策	9	ネットワークのアクセス制御
	10	ログ管理・分析
	11	バックアップ実施
	12	ネットワークの二重化・暗号化
	13	ウイルス対策
	14	データやシステムのアクセス制御
開発・運用時の セキュリティ対策	15	システム開発時の事故・不正行為対策
	16	データの完全性確保
	17	修正プログラムの適用
インシデントの 予防、発生時の対応	18	インシデント対応体制の構築・模擬訓練
	19	定期的な脆弱性調査
	20	定期的な監査・是正処置

4.1.3-1 アセスメント概要

評価	評価内容
5	事業環境の変化に合わせて常に改善しており、他社の模範となるレベル
4	全社的に方針やルールを定め周知・実施し、責任者により定期的に確認
3	全社的に周知・実施しているが、状況の確認ができていない
2	方針やルールを整備・周知しつつあるが、一部しか実現できていない
1	実施できていない、ルールがない

表 4.1.3-2 評価内容

実証参加企業各社の回答から分類ごとに平均値を算出し、実証参加企業ごとに実証参加企業平均に対してどの位置にいるのかをレーダーチャート化することで見える化を行った。また今後どのような対策が必要かを診断結果とし記載したものを各社へ返送した。

以下、各社へ返送したセキュリティ簡易診断アセスメントのサンプルを示す。

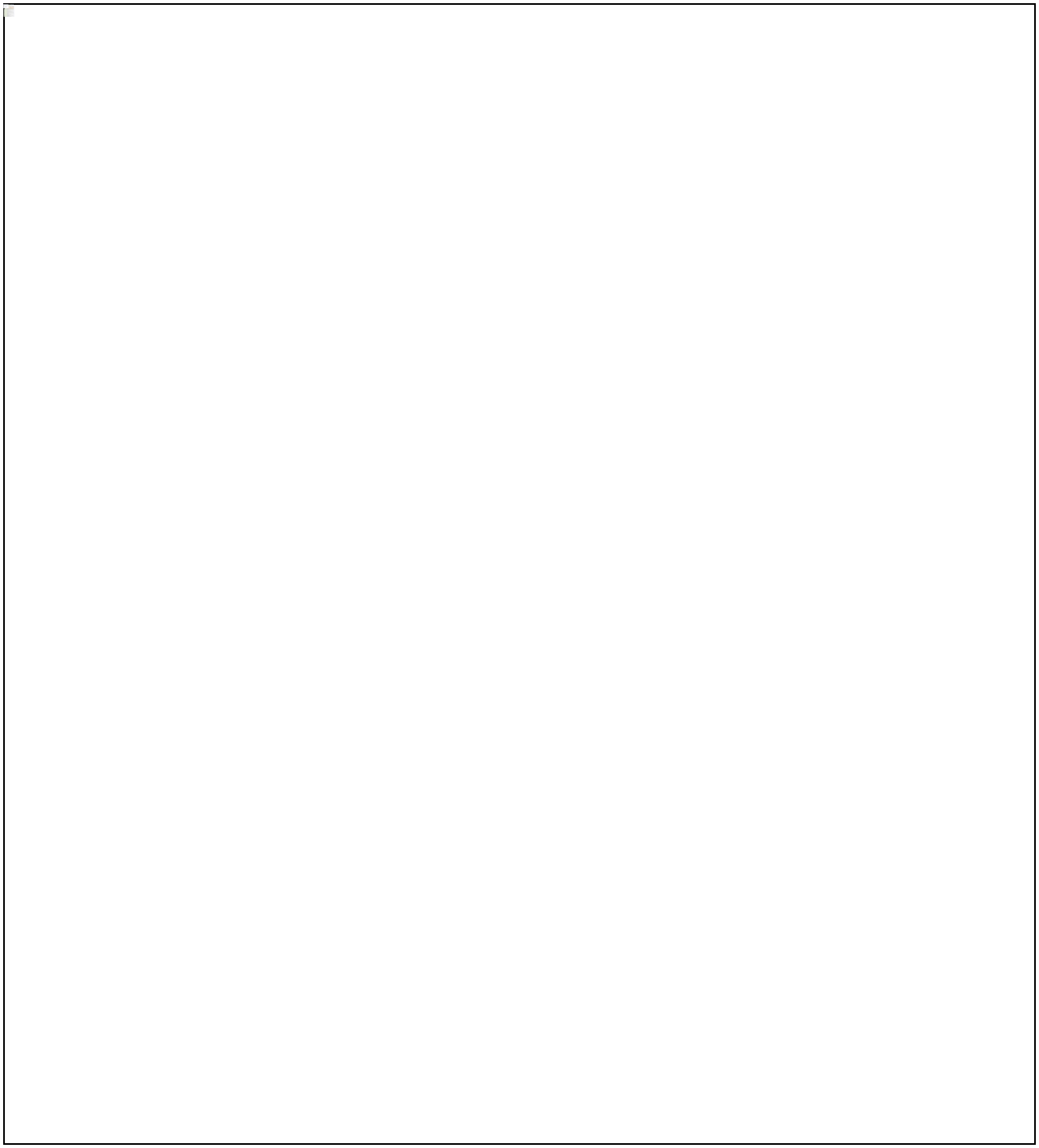


図 4.1.3-1 セキュリティ簡易診断アセスメントシートのサンプル

4.2.　実態把握結果

4.2.1. サイバーセキュリティに関するアンケート調査の結果

● セキュリティ対策への取り組み　（有効回答数：43 件）

セキュリティ対策への取り組みは以下のとおりである。
80%以上の企業が最低限のセキュリティ対策を行っていることがわかった。

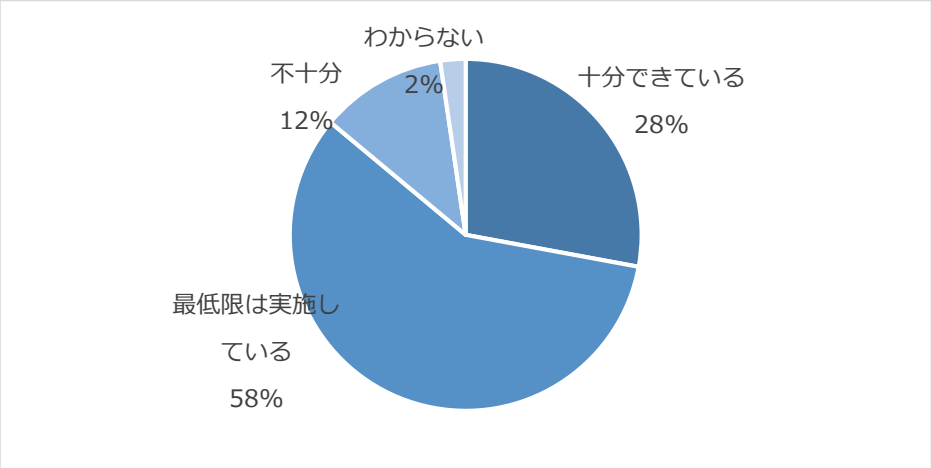


図 4.2.1-1 セキュリティ対策への取り組み

内容	回答数（割合）
十分できている	12（2%）
最低限は実施している	25（5%）
不十分である	5（12%）
わからない	1（2%）

表 4.2.1-1 セキュリティ対策への取り組みの詳細

(1)　セキュリティ対策の現状　（有効回答数：43 件　※複数回答可）

セキュリティ対策の現状は以下のとおりである。ウイルス対策ソフトの導入が 100%に満たない状況が判明したが、ファイアウォールの導入などによる IT システムでの対策を取り組んでいる企業の割合は多かった。一方で、「方針作成＆社内周知」や「社内教育」の非 IT 面での対策を取り組んでいる企業の割合は半数程度に留まった。

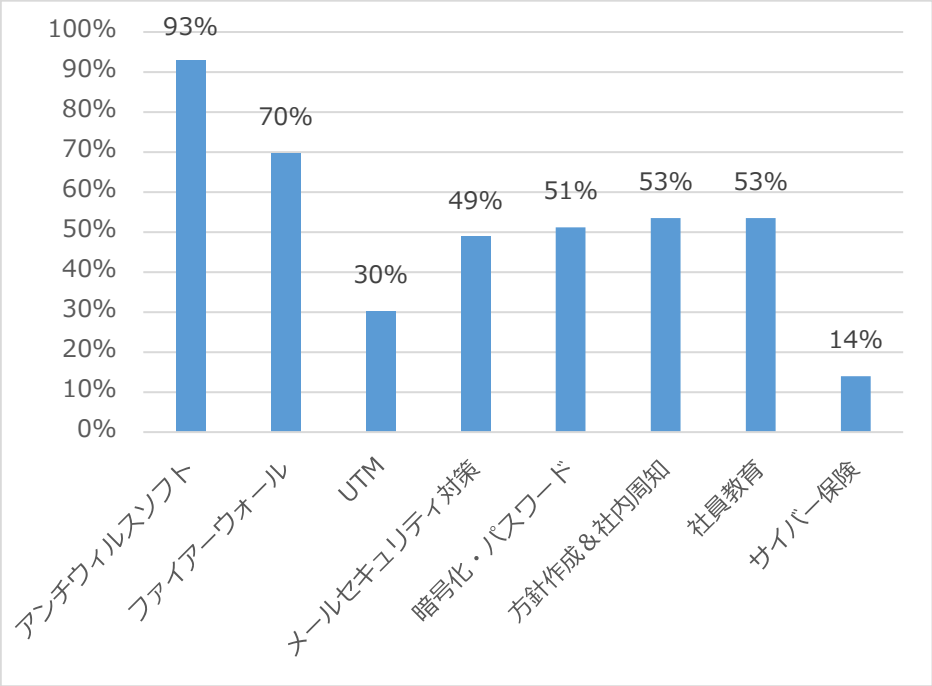


図 4.2.1-2 セキュリティ対策の現状

内容	回答数（割合）
アンチウイルスソフト	40（93%）
ファイアウォール	30（70%）
UTM	13（30%）
メールセキュリティ対策	21（49%）
暗号化・パスワード	22（51%）
方針作成＆社内周知	23（53%）
社員教育	23（53%）
サイバー保険	6（14%）

表 4.2.1-2 セキュリティ対策の現状

(2)　サイバー攻撃、被害の経験有無（有効回答数：43 件　※複数回答可）

サイバー攻撃や被害の状況は以下のとおりである。90%以上の企業がウイルス対策ソフトを導入しているが、ウイルス感染被害が発生していることが判明した。

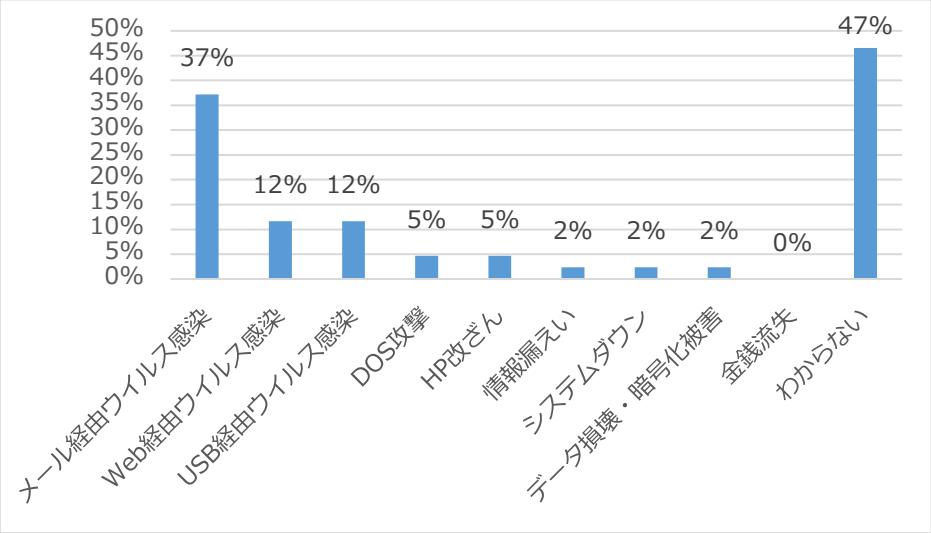


図 4.2.1-3 サイバー攻撃、被害の経験有無

内容	回答数（割合）
メール経由ウイルス感染	16（37%）
Web 経由ウイルス感染	5（12%）
USB 経由ウイルス感染	5（12%）
DoS 攻撃	2（5%）
HP 改ざん	2（5%）
情報漏えい	1（2%）
システムダウン	1（2%）
データ損壊・暗号化被害	1（2%）
金銭流失	0（0%）
わからない	20（47%）

表 4.2.1-3 サイバー攻撃、被害の経験有無

(3)　サイバー攻撃を受けた際の対処（有効回答数：43 件）

サイバー攻撃を受けた際の対処状況は以下のとおりである。「クリアインストール」や「専門業者に依頼」で半数以上であり、業務や費用への影響が大きい対処が必要となっている状況が判明した。

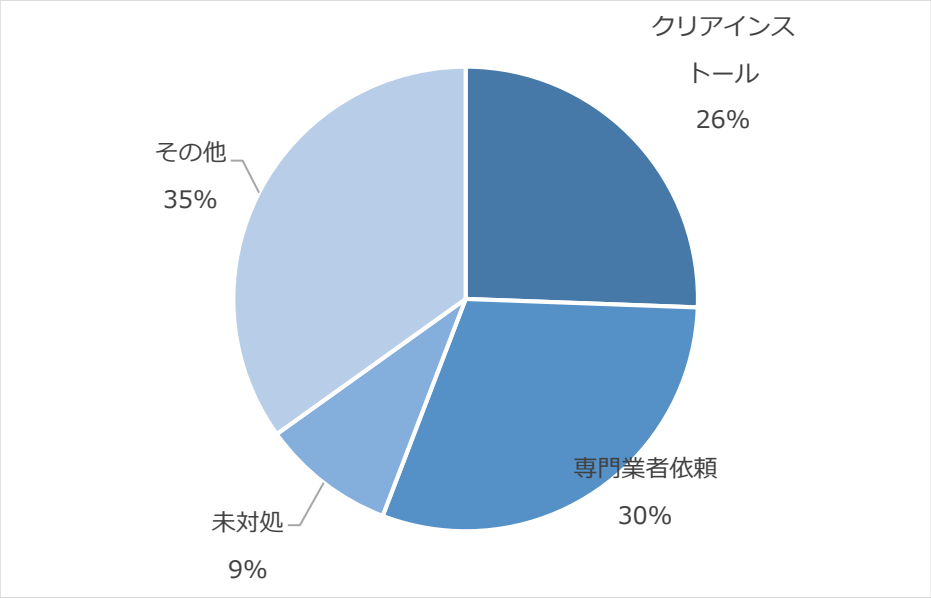


図 4.2.1-4 サイバー攻撃を受けた際の対処

内容	回答数（割合）
クリアインストール	11（26%）
専門業者依頼	13（30%）
未対処	4（9%）
その他	15（35%）

表 4.2.1-4 サイバー攻撃を受けた際の対処

(4)　サイバー対策年間経費（有効回答数：43 件）

サイバー対策の年間経費の状況は以下のとおりである。半数近くの企業が 1 年間あたり 50 万円以下であり、総務省が発表している 2013 年の一社平均の情報セキュリティ対策費用とほぼ変わらない。[i]

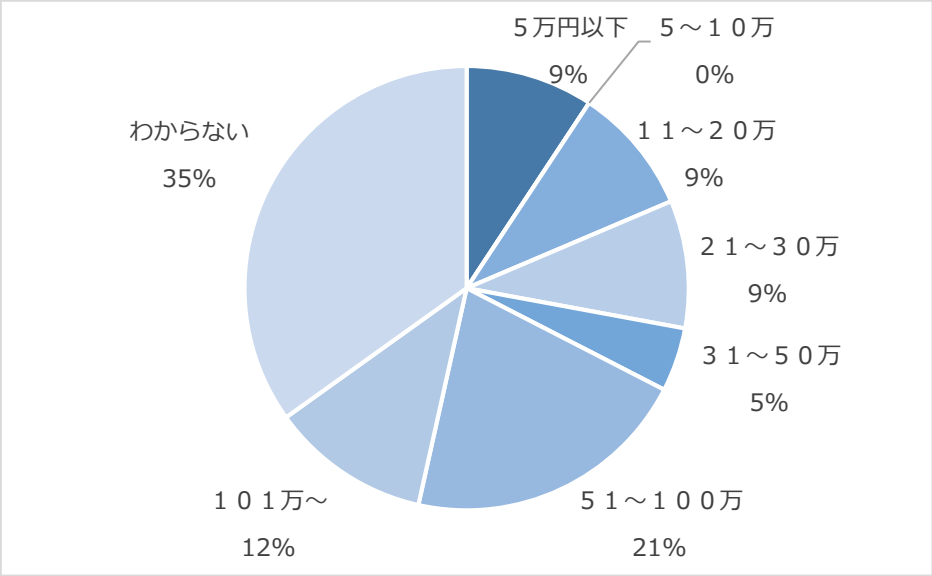


図 4.2.1-5 サイバー対策年間経費

内容	回答数（割合）
5 万円以下	4（9%）
5～10 万円	0（0%）
11～20 万円	4（9%）
21～30 万円	4（9%）
31～50 万円	2（5%）
51～100 万円	9（21%）
101 万円～	5（12%）
わからない	15（35%）

表 4.2.1-5 サイバー対策年間経費

[i]経済産業省：中小企業白書 2016 年版
https://www.chusho.meti.go.jp/pamflet/hakusyo/H28/h28/html/b2_4_3_1.html（2021/1/22 参照）

(5)　取引先からのサイバー攻撃対策指示（有効回答数：43 件）

取引先からのサイバー攻撃に対する対策指示を受けている企業の状況は以下のとおりである。半数近くの企業が取引先から対策を求められており、今後も更に増える可能性が高い。

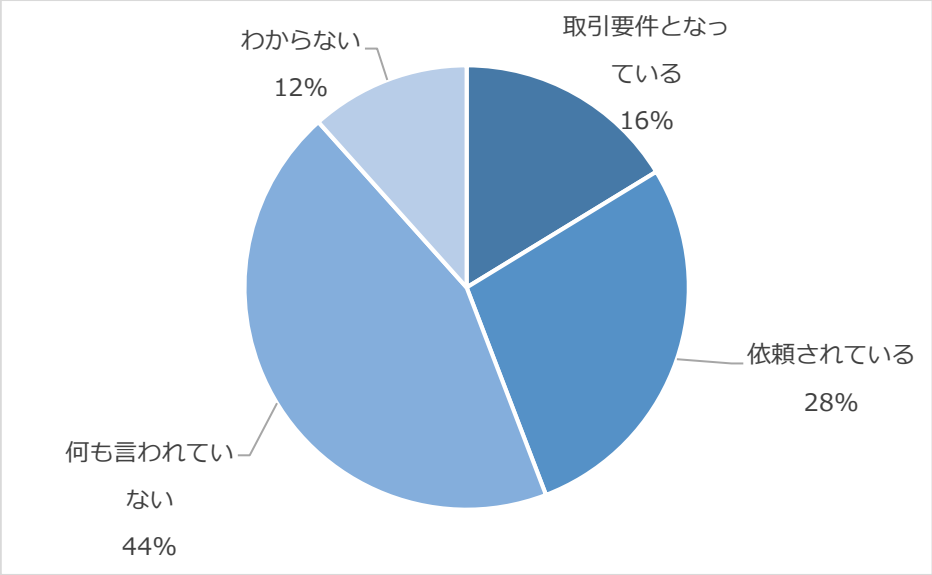


図 4.2.1-6 取引先からのサイバー攻撃対策指示

内容	回答数（割合）
取引要件となっている	7（16%）
依頼されている	12（28%）
何も言われていない	19（44%）
わからない	5（12%）

表 4.2.1-6 取引先からのサイバー攻撃対策指示

(6)　サイバーセキュリティ対策の実態（全体考察）

九州圏の多くの中小企業は、ウイルス対策ソフトの導入など最低限の対策を行っているにも関わらず、メールや Web、USB 経由でのウイルス感染に遭い、業務や経費へのインパクトが大きい対処を行っていることがわかった。また、取引先からのセキュリティ対策が増えているにも関わらず、社内周知や教育などマネージメント、スキル面の強化も不足しており、セキュリティに費やす経費も少ないという実態もわかった。

これらのことから、ウイルス感染の疑いが発生した時点で検知できることや感染してもリスクが拡大する前に最小限の被害に押さえることが最も有効な対策であると考える。また、セキュリティ対策のマネージメントを含んだエンドポイントとネットワークの監視サービスが安価に提供することができれば中小企業にとって大きなメリットであると考える。

4.2.2. セキュリティ診断の結果

「4.1.2 5 分でできる！情報セキュリティ自社診断」に基づき、実証参加企業から回収したセキュリティ診断シート回答を集計し分析を行った。

●セキュリティ診断回収期間および回答件数

- アセスメント回収期間

  アセスメント配布から回収までの期間は、以下のとおりである。

  2020 年 10 月 1 日（木） ～ 2020 年 12 月 18 日（金）

  アセスメントシートの回収は、10 月 1 日（木）の実証実験開始より当初 10 月末までとしていたが、回収の状況が悪かったため、最終的には、12 月 18 日（金）で回答を締め切り、集計を行った。

- アセスメント簡易診断シートの回答件数

  アセスメント簡易診断シートの実証参加企業からの回答状況は以下（「表 4.2.2-1」）のとおりである。

参加企業数	54
回答企業数	49
未回答	5

表 4.2.2-1 アセスメント簡易診断シートの回答数

その他の未回答の実証参加企業についても、定期的な回答促進を実施したが最終的に回答が得られなかった。

- 検証後の回答件数

  検証終了後のセキュリティ診断の回答件数は、38 社であった。

(1) 診断結果による検証前のセキュリティ状況

実証参加企業のカテゴリー平均、各診断内容の点数は以下のとおりである。

診断項目	No.	診断内容	カテゴリー平均	参加企業平均
				60.18
Part1	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	2.60	3.41

基本的対策	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？		3.45
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？		1.96
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？		2.63
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？		1.57
Part2	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	2.41	3.14
従業員としての対策	7	電子メールや FAX の宛先の送信ミスを防ぐ取組みを実施していますか？		1.73
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？		2.29
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？		2.59
	10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？		2.27
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？		2.94
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？		2.47
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？		1.78
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？		2.08
	15	関係者以外の事務所への立ち入りを制限していますか？		2.69
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？		1.55
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？		2.78

	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？		2.98
Part3 **組織としての対策**	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	2.27	3.27
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？		2.41
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？		2.10
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？		2.69
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？		2.29
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？		1.51
	25	情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？		1.61

表 4.2.2-2 セキュリティ診断シート診断結果

- 実証参加企業全体での平均点は 60.18 点であり、診断結果としては「対策が行き届いてないところが目立ちます。」であった。
- 1 点台が 6 項目あり、No.5 の脅威に対する社内共有の仕組み作りや、No.24 のセキュリティ事故発生時の体制整備や対策手順のルール作り、その他の項目についてもセキュリティに対する教育やルールの制定ができていないために低い点数となっていることが判明した。
- 3 点台は 4 項目あり、OS の最新化、ウイルス対策ソフトの導入とウイルス定義ファイルの最新化、メール添付ファイルや URL に気をつけている、守秘義務の徹底が高い状況であった。最新化については、自動的に最新化になり人が気にしなくてよいことで点数が高いと思われる。メール添付のファイルや URL については一般メディアでのセキュリティ事故報道もありその認識が高いと思われる。
- 3 つの Part の平均では、大きく点数は変わらないが、いずれも 2 点台であり総じてセキュリティ診断としては低い点数となった。

IPA の定義する点数分布で社数を示すと以下のとおりである。

点数	採点結果	社数（割合）
100	入門レベルのセキュリティ対策は達成です、ステップアップを検討しましょう	3（ 6%）
70~99	ほぼ、できていますが、部分的に対策が不十分な点があるようです	18（37%）
50~69	対策が行き届いていないところが目立ちます	8（16%）
49 以下	いつ情報流出などの事故が起きても不思議ではありません	20（41%）

表 4.2.2-3 社数別の点数分布

- 100 点満点が 3 社であった。
- 49 点以下が一番多く 40%強を占めるが、70~99 点も 37%であり、セキュリティ対策がほぼできている企業とセキュリティ対策が不十分でセキュリティ事故が起きやすい企業で 2 極化している。

(2) 実証前と実証後の意識変化

実証前と実証後のセキュリティ診断を比較し、実証参加によるセキュリティ意識の変化を検証した。

実証前	実証後	差
60.18	64.03	+3.84

表 4.2.2-4 実証前と実証後の参加企業の平均値

- 実証前と実証後での、実証参加企業の平均点は、以下のとおり 3.84 点向上している。
- 実証参加企業により再度内容を精査され、項目的に点数が上がったもの、下がったものがあるが、平均点からすると本検証によりセキュリティの状況としては上がっている。

(3) 診断内容による意識変化

実証参加企業において現在できていない対策について、今後対策を行いたい項目を追加で回答してもらい、対策を行いたい項目の中で社数の多い上位 5 つは以下のとおりである。

診断項目	No.	診断内容	社数
Part3	25	情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？	8

Part1	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	6
Part2	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	6
Part2	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	5
Part3	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	5

表 4.2.2-5 対策を行いたい項目（上位 5 位）

- 最も多い対策が「ルール化した内容を従業員へ明示する」で 8 社であった。各セキュリティ対策をルール化し、従業員へ明示することでセキュリティ意識を植え付けることを優先したい企業が多いことが判明した。
- 次に多い対策は、「セキュリティ脅威やその手口を共有する」、「メール誤送信対策」であった。最新のセキュリティトレンドや最新情報を入手したいと思っており、サービス提供側からの情報の発信が重要であり、企業側はその情報を従業員へ展開する仕組みが必要であることがわかった。

(4) 診断項目による意識変化

診断項目の 3 つのパート単位で平均値がどのように変化したかを示す。

診断項目	実証前	実証後	差
Part1 基本的対策	2.60	2.72	+0.12
Part2 従業員としての対策	2.41	2.53	+0.12
Part3 組織としての対策	2.27	2.51	+0.24

表 4.2.2-6 診断項目別の実証前と実証後の平均値

- 「Part3 組織としての対策」が +0.24 であり、本検証を通じて意識が変わっていることがわかった。できていない企業も今後実施する項目として、Part3 の「ルール化した内容を従業員へ明示する」を選択している企業が 8 社で最も多く、この検証を通じて実証参加企業が変化した項目も「Part3 組織としての対策」であり、まずは組織として対応、ルール化、従業員への明示を重要視していることが判明した

(5) SECURITY ACTION ★2 レベルに到達に向けての課題

今回の実証参加企業へは、「5 分でできる！情報セキュリティ自社診断」を実施してもらい、49 社からの回答を得た。回答した実証参加企業に対しては、2021 年 1 月 14 日（木）、15 日（金）に開催した報告会において、情報セキュリティ基本方針を定め方、外部への公開方法を展開した。

検証後のアンケートでは、「SECURITY ACTION」を認知されていない実証参加企業や、今回未回答の実証参加企業もおられ、九州地区の中小企業に対しては、継続的な「「SECURITY ACTION」

認知のための啓発活動が必要であり、またその啓発活動を通じてセキュリティ対策の重要性、必要性を知ってもらう活動が必要である。

セキュリティ診断の回答の中には、「取組みにあたってどのような方法があるのか情報提供をいただけると助かる」とのコメントをもらった実証参加企業もあり、「SECURITY ACTION ★2」の取得に合わせて、具体的な取り組み方法の提示も重要であり、セキュリティ意識の向上と実際のセキュリティ対策方法の情報発信も必要である。

4.2.3. セキュリティ簡易診断アセスメントの結果

「4.1.2 5 分でできる！情報セキュリティ自社診断」に基づき、実証参加企業から回収したセキュリティ簡易診断アセスメントの回答を集計し分析を行った。

● アセスメント回収期間および回答件数

- アセスメント回収期間

アセスメント配布から回収までの期間は、以下のとおりである。

2020 年 10 月 1 日 （木）～ 2020 年 12 月 18 日（金）

アセスメントシートの回収は、10 月 1 日の実証実験開始より当初 10 月末までとしていたが、回収の状況が悪かったため、最終的には、12 月 18 日（金）で回答を締め切り、集計を行った。

- アセスメント簡易診断シートの回答件数

アセスメント簡易診断シートの実証参加企業からの回答状況は以下のとおりである。

参加企業数	54 社
回答企業数	48 社
未回答	6 社

表 4.2.3-1 アセスメント回収状況

- 未回答のうち、1 社はセキュリティ上の制約のため回答が得られなかった。
- その他の未回答の実証参加企業についても、定期的な回答促進を実施したが最終的に回答が得られなかった。
- 回答があっても質問に回答されていない項目があり、未回答項目においてコメント欄に記載があるものは、適切な 5 段階評価をレベル判定し、コメントがないものについては、「1：実施できていない、ルールがない」レベルと判定して集計を行った。
- 「管理を親会社が実施している」とのコメント付きで一部未回答となっていた実証参加企業においては、該当箇所を親会社のものと同じ評価とした。

(1)　全体の平均による考察

20 項目の質問および 5 つの分類での実証参加企業平均値を以下のとおり算出した。

分類	No.	項目名	参加企業平均	参加企業分類平均	NEC 調査全業種平均	望まれる水準
組織的・人的セキュリティ対策	1	情報資産の分類・管理	2.34	2.63	3.27	4.18
	2	要情報の持ち出し制限	2.68			
	3	外部委託管理	2.96			
	4	セキュリティ教育の実施	2.57			
物理的セキュリティ対策	5	外部からの物理的侵入対策	2.79	2.63	3.34	4.19
	6	端末の物理的対策	2.38			
	7	外部媒体管理	2.47			
	8	記録媒体の処分	2.91			
技術的セキュリティ対策	9	ネットワークのアクセス制御	3.00	2.90	3.43	4.22
	10	ログ管理・分析	2.28			
	11	バックアップ実施	3.26			
	12	ネットワークの二重化・暗号化	2.26			
	13	ウイルス対策	3.47			
	14	データやシステムのアクセス制御	3.19			
開発・運用時のセキュリティ対策	15	システム開発時の事故・不正行為対策	2.49	2.42	3.38	4.17
	16	データの完全性確保	2.19			
	17	修正プログラムの適用	2.60			
インシデントの予防、発生時の対応	18	インシデント対応体制の構築・模擬訓練	2.19	2.14	3.12	4.06
	19	定期的な脆弱性調査	1.83			
	20	定期的な監査・是正処置	2.43			

表 4.2.3-2 セキュリティ簡易診断アセスメント項目

- 全分類において平均値が「2」となっており、全体的にセキュリティに関する方針やルールを整備中、またはそのルールの周知を行っている最中であるが、一部しか実施、実現できていない状態であることがわかった。
- 5 つの分類の中で平均値が最も高い点数は、「2.90」の「技術的セキュリティ対策」についてであり、ほぼ「3」で実証参加企業の中では他の分類と比較し高い点数となった。アクセス権の制御、ウイルス対策、データバックアップなどの各項目も数値が高いことから、比較的セキュリティ対策としてはわかり易く取り組みやすいことが高い点数の要因と考えられる。

- 5 つの分類の中で平均値が最も低い点数は、「2.14」の「インシデントの予防、発生時の対応」についてであった。インシデント発生を想定した取組みができておらず、実際にインシデントが発生していない、もしくは発生していてもそのインシデントに気付いておらず、その必要性を感じていないために低い点数となっている可能性がある。
- 今回の実証参加企業における全体的な平均は「2」であったが、NEC が実施している今回のセキュリティ簡易診断アセスメントを使用した大企業、中小企業を含めた全業種での平均は「3」であり、また NEC が定義している望まれる水準としては「4」であることから、九州地域としての中小企業のセキュリティ対策状況としては、総じて低い状況であると判断する。

(2) 業種別による考察

実証参加企業業種別のレベル判定の件数と、業種ごとのレベル判定件数割合は以下のとおりである。

業種	企業数（割合）	A	B	C	D	未回答
建設業	3（5.6%）	2（67%）	0	0	1（33%）	0
製造業	8（14.8%）	1（13%）	0	1（13%）	3（38%）	3（38%）
電気・ガス・熱供給・水道業	2（3.7%）	0	0	2（100%）	0	0
情報通信業	12（22.2%）	8（67%）	0	3（25%）	1（8%）	0
運輸業・郵便業	6（11.1%）	1（17%）	0	0	5（83%）	0
卸売業・小売業	5（9.3%）	2（40%）	0	0	2（40%）	1（20%）
不動産業・物品賃貸業	2（3.7%）	0	0	1（50%）	1（50%）	0
学術研究・専門技術サービス業	1（1.9%）	0	0	1（100%）	0	0
宿泊業・飲食店	1（1.9%）	0	0	0	1（100%）	0
教育学習支援業	2（3.7%）	0	0	0	1（50%）	1（50%）
医療・福祉	2（3.7%）	0	0	1（50%）	1（50%）	0
サービス業（他に分類されないもの）	10（18.5%）	1（10%）	0	6（60%）	2（20%）	1（10%）

表 4.2.3-3 業種別によるレベル判定

- 業種別の件数で見ると、「情報通信業」の「A」ランク 8 件が突出しており、「情報通信業」の業種であるためにセキュリティ意識が高いことは必然的であると考えられる。しかし、実証参加企業全体からすると「C」、「D」ランクも「情報通信業」中で 3 割以上であるため、他業種同様にセキュリティ意識の向上と対策は必要である。

- 「運輸業・郵便業」が「C」ランク 5 件である、業種別の件数としては最も低い結果となっている。
- 業種ごとのランク割合を見ると、やはり「情報通信業」が「A」ランクの割合が高いが、「建設業」も「A」ランクの割合 50%以上となっており高い結果となっている。
- その他の業種については、ほぼ「C」、「D」ランクとなっており、セキュリティに対する対策が必要な状況である。

(3) 地域別による考察

実証参加企業における地域別でのレベル件数と、業種ごとのレベル判定件数割合は以下のとおりである。

地域	企業数（割合）	A	B	C	D	未回答
福岡	29（53.7%）	8（28%）	0	9（31%）	9（31%）	3（10%）
佐賀	7（13.0%）	1（14%）	0	1（14%）	3（43%）	2（29%）
長崎	6（11.1%）	2（33%）	0	2（33%）	2（33%）	0
熊本	3（5.6%）	3（100%）	0	0	0	0
大分	2（3.7%）	0	0	1（50%）	1（50%）	0
宮崎	7（13.0%）	1（14%）	0	2（29%）	3（43%）	1（14%）

表 4.2.3-4 地域別によるレベル判定

- 地域別の件数で見ると、「福岡」の「A」ランク 8 件と多いが、「福岡」の実証参加企業数が他地域と比較しても多いため、「A」ランクも多くなったと考えられる。
- 地域ごとの割合で見ると、「熊本」が「A」ランクが 100%と最も高い数値となっている。しかし件数が 3 件であり、またその業種が 3 件とも「情報通信業」であるため地域性というより、参加した「熊本」の業種により高くなったと考える。

(4) 全体考察

今回のセキュリティ簡易診断アセスメントで、実証参加企業の平均から業種別、地域での考察を行ったが、一概にどの地域のセキュリティレベルが高いのか、低いのかの判断はつかない結果であったが、「②全体平均による考察」にも記載したとおり、NEC が実施しているセキュリティ簡易診断アセスメントを使用した大企業、中小企業を含めた全業種の平均と比較すると、九州地域としての中小企業のセキュリティ対策状況としては、総じて低い状況であることが判明した。

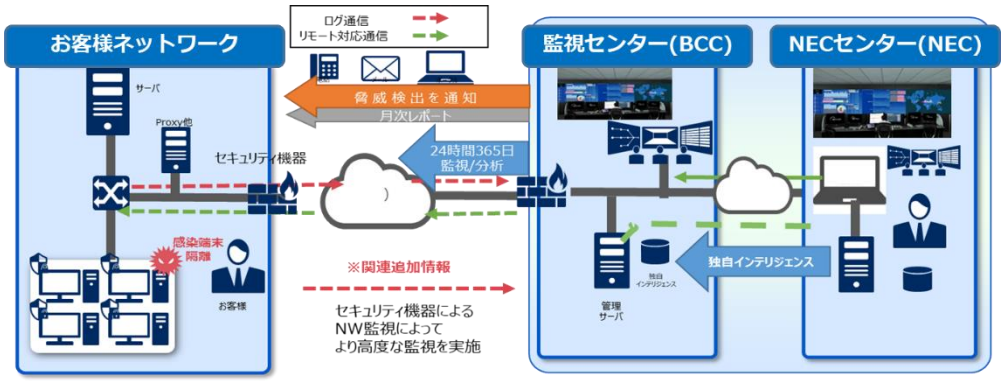
業種別では、「情報通信業」が他業種に比較してセキュリティレベルが高い傾向にあることがわかり、「情報通信業」のとある実証参加企業では、ISMS 認証、PMS 認証による定期的な監査の実施や、従業員への理解度テストの実施、情報セキュリティ自己診断チェック実施などを行うなどセキュリティ意識を高い状態で保つ施策を行っており、このようなセキュリティ意識向上を他業種、各地域へ啓発し、大企業だけでなく中小企業においてもセキュリティ対策を安価でかつ簡易に実施できるサービス、製品が必要であると考える。

5. 地域実証の事業内容

5.1. サービス概要

エンドポイント端末に対するマルウェアなどの標的型攻撃状況を「エンドポイント監視サービス Type-Y」にて監視し、ネットワークセキュリティ状況を UTM による「サイバーセキュリティ見守りサービス」にて監視する。エンドポイント監視サービス Type-Y が異常を検知した端末をサイバーセキュリティ見守りサービスにて監視することで、実証参加企業内部から外部へのデータ流出を検知できる。エンドポイント監視サービス Type-Y をエンドポイントに組み込み、インターネットとの境界にサイバーセキュリティ見守りサービスを導入することで、エンドポイントとネットワークの両面から実証参加企業の実態を多角的に把握し、セキュリティ専門知識を持った人材によりエンドポイントのマルウェア感染状況や外部からのサイバー攻撃状況、データ流出状況を監視する。

図 4.1-1 サービス概要



5.1.1. エンドポイント監視サービス Type-Y

エンドポイント監視サービス Type-Y は、実証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する。常時エージェントを監視し、異常を検知した際に通知を行うサービスである。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を可能とし、中央省庁や金融サービスを中心に約 74 万クライアントへの導入実績がある。

(1) 使用したソフトウェアについて

5 つの保護エンジンで多層的な防御を実現する NEC の Act Securexを利用した。検知項目は以下のとおりである。

項目	仕様
脆弱性を狙った攻撃の検知	メールや Web ページ閲覧時の攻撃など、既知および未知の脆弱性を狙ったウイルス攻撃を防御。任意コード実行型脆弱性の攻撃を防御。
静的解析による検知	プログラムを動作させることなく分析。「PE 構造分析」「リンカー分析」「パッカー分析」「想定オペレーション分析」など多数の分析手法で検知。

項目	仕様
サンドボックスによる検知	仮想 CPU や仮想メモリ、仮想 Windows サブシステムなどで構成される仮想環境上でプログラムを実行し検知
動的解析による検知	実行中プログラムの動作を監視。他プログラムへの侵入や異常なネットワークアクセス、キーロガー、バックドア的な動作などの挙動を検知。
機械学習による検知	マルウェアに関するビッグデータをもとに実行中のプログラムを監視。ビッグデータ上の振る舞い特性を抽出し、機械学習で分析した特徴により端末上の悪意ある挙動を検知。

表 5.1.1-1 5 つの検知項目

(2) 主な検知実績について

今回の実証における検知実績は以下のとおりである。

発生・報道時期	防御エンジンリリース時期	当時の未知脅威および標的型攻撃
2018/07	2018/03	マルウェア「Emotet」
2018/07	2017/12	マルウェア「Clipboard Hijacker」
2018/04	2017/06	ランサムウェア「Satan」
2018/04	2017/06	ランサムウェア「GandCrab」
2017/12	2017/05	仮想通貨採掘マルウェア「CoinMiner」
2017/10	2017/01	ランサムウェア「Bad Rabbit」
2017/08	2016/10	国内防衛産業を標的としたマルウェア
2017/05	2016/10	ランサムウェア「WannaCry/WannaCrypt」

表 5.1.1-2 主な検知実績

(3) ソフトウェアの動作要件について

ソフトウェアの動作要件は以下のとおりである。

- H/W 環境
  - CPU：1GHz 以上 （デュアルコア必須）
  - メモリ：2GB 以上
  - ハードディスク：1GB 以上の空き容量
  - ファイルシステム：システムドライブ、インストールドライブは NTFS 必須
  - 仮想化環境：動作可能
- OS 環境
  - Windows 7 （32/64 ビット）
  - Windows 8.1 （32/64 ビット）

- Windows 10 （32/64 ビット）
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019

- 同居可能なウイルス対策ソフトの主なベンダー
  - Microsoft、 TrendMicro、 Symantec、 McAfee、 ESET、 F-Secure、 Sophos

(4) 導入について

- エンドポイント監視サービス Type-Y エージェントソフトのインストーラーとインストール手順書を実証参加企業に送付し、担当者自身でインストールするよう依頼した。その際、当該ソフトの動作環境を明記した資料を提示し、システム要件に基づいたインストールを判断してもらった。
- 当該ソフトは、既存のウイルス対策ソフトと同居した構成での運用を推奨した。同居可能なウイルス対策ソフトの主なベンダーを明記した資料を送付し、同居非推奨なウイルス対策ソフトを利用している場合は、相談窓口へ問合せするよう依頼した。
- 脅威通知サービスの準備として、担当者に通知先メールアドレスを選定および提供を依頼した。その後、サービス提供者が通知の設定作業を行った。
- 当該ソフトは、インストール後に自動でフルスキャン処理が実行されるため、フルスキャン後に実証に協力してもらった。

(5) 運用について

- 脅威を検知した場合、通知先メールアドレス宛に以下の内容が記載されたアラートメールが送信される。アラートメールには以下の内容が記載されており、自身で初動対応を実施してもらうよう依頼した。
  - 検知日時
  - 検知端末
  - 検知したプロセス
  - 解析結果
  - 対応手順
- 月初めには、前月分の検知結果レポートを送付した。

5.1.2. サイバーセキュリティ見守りサービス

「サイバーセキュリティ見守りサービス」は、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、表 5.1.2-1 に示すセキュリティ機能により、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い、安全なセキュリティを提供するサービスである。

(1) 使用した UTM について

サービスで使用した UTM の仕様とセキュリティ機能は以下のとおりである。

項目		仕様
WAN インタフェース	ポート数	1 ポート
LAN インタフェース	ポート数	4 ポート
無線 LAN インタフェース	アンテナ	内蔵アンテナ
	規格	IEEE802.11n
		IEEE802.11g
		IEEE802.11b
電源（AC アダプタ）		AC100V～240V 50/60Hz
動作保障環境		温度：0～40℃　湿度：10～90%
消費電力		35VA（21W）以下
外形寸法（WHD）		約 174×195×40 mm
本体質量		0.9 kg以下
設置方法		横置き、縦置き
セキュリティ機能	不正侵入防止検出/防止（IDS/IPS）	ネットワークに対する攻撃を認識／防止
	アンチウイルス	ホームページ閲覧時やメール受信、その他のアプリケーションの通信を監視し、ダウンロードするファイルにウイルスが混入していないかをチェックし、発見時には無害化
	Web ガード	フィッシングサイトなどの詐欺サイトや、閲覧によりマルウェア感染の可能性がある危険なサイトへのアクセスをガードする
	URL フィルタリング	サイトの URL をカテゴリーごとに登録し、登録済みカテゴリーに対してアクセス禁止などの制御
	URL キーワードフィルタリング ※本機能は実証では使用せず	Web 閲覧において、あらかじめユーザーが設定した特定の文字列を URL に含むページのアクセスをブロック
	アプリケーションガード	チャット、ファイル交換ソフト、SNS サイト、動画サイトなど、アプリケーションの通信を検出し、制御
	ファイアウォール ※本機能は実証では使用せず	お客様のネットワーク環境（イントラネット）とインターネットの境目（エッジ）に設置し、その間の通信をポート制御することで、イントラネットからインターネット接続を損なわず、インターネットからお客様のネットワーク環境のアクセスを制限

表 5.1.2-1 UTM の仕様とセキュリティ機能

- 本実証事業では、UTM をインターネット接続機器（ONU やブロードバンドルーターなど、PPPoE を終端している機器。以下、ブロードバンドルーター）と監視対象端末（パソコンやモバイル機器など）の間に設置する想定である。
- 既存の UTM は、約 100 台の端末を監視でき、中小企業にとって十分であると考え選定した。また、100 台を超過した場合、通信速度低下の可能性があるため、募集の際に条件として考慮した。
- WAN インタフェースに関して、中小企業では、ブロードバンドルーターやキャリアとの回線は単一であると想定し、1 ポートの既存 UTM をベースとした。仮に複数のブロードバンドルーターが存在する場合は、業務で使用頻度の高い回線を対象とする前提である。
- LAN インタフェースに関して、仮にブロードバンドルーターが 4 ポート以上ある場合は、別途 HUB を用意する前提である。
- ブロードバンドルーターの無線機能を使用している場合、端末からの通信はブロードバンドルーター配下に設置した UTM を経由しないため、UTM による監視は不可能である。上記環境下で UTM による監視を行うためには、ブロードバンドルーターの無線機能は無効にし、UTM の無線機能を使用する必要がある。
- ブロードバンドルーター以外の無線 LAN アクセスポイントを使用している場合は、無線 LAN アクセスポイントとブロードバンドルーターの間に UTM を設置することで、無線 LAN アクセスポイントおよび配下端末の設定変更なしで監視可能である。

(2) UTM の設置について

- 中小企業の実態を把握するため、ブロードバンドルーターと監視対象端末の間に UTM を設置し、企業 LAN とインターネットの通信を監視した。
- 以下の理由より、UTM の動作は「ブリッジモード」を採用した。
  - ネットワーク構成の変更を最小限に抑制
  - 万一、UTM で問題が発生した場合、業務停止を最小限に抑制

UTM の設置例を以下に示す。

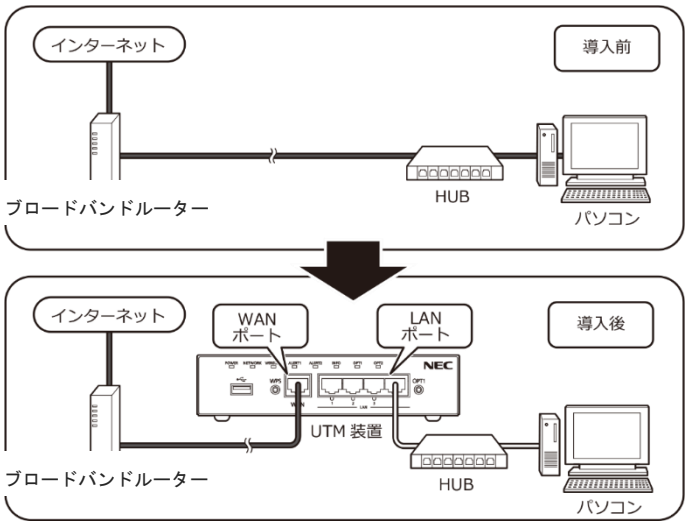


図 5.1.2-1 設置例①：ルーターなどの配下に HUB を使用している場合

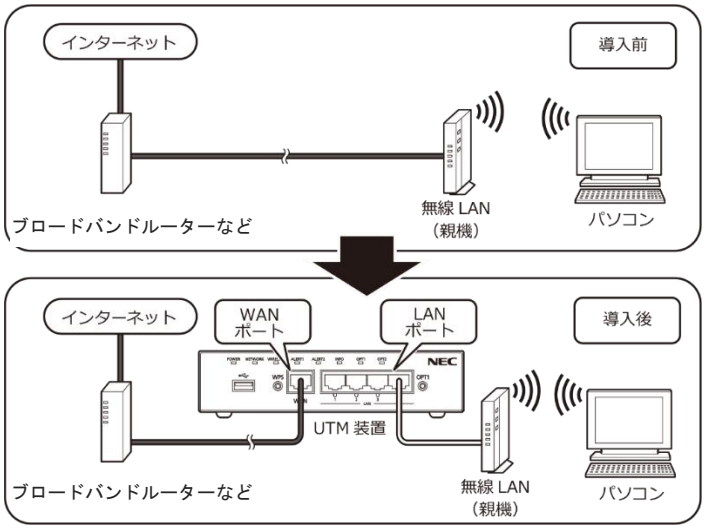


図 5.1.2-2 設置例②：ルーターなどの配下に無線 LAN（親機）を使用している場合

(3) 使用した UTM のセキュリティ機能、運用手法

UTM では、以下のセキュリティ機能を使用した。以降、各セキュリティ機能は表 5.1.2-2 中の略称にて記載する。

セキュリティ機能	略称	説明
不正侵入防止	IPS	通信データ内の攻撃コードなどの異常なデータが含まれていることを検知し防御する機能。 あらかじめ登録された侵入手口のパターンとマッチングさせることにより検知し、通信を遮断することで、ネットワークに対する攻撃に対して防御する。
アンチウイルス	AV	マルウェアや危険なコードが含まれるファイルを検知した場合に内容を書き換え無害化する機能。 ホームページの閲覧やメール受信、その他のアプリケーションの通信を監視し、ダウンロードまたはアップロードするファイルにマルウェアが混入していないかをチェックする。ダウンロードまたはアップロードするファイルにマルウェアが混入している場合、ファイルの内容を書き換えてファイルを無害化する。
Webガード	WG	フィッシングサイトや閲覧によってマルウェア感染を起こすなどの有害なWebサイトへのアクセスを遮断する機能。あらかじめ定義されている有害なWebサイトに対するアクセスを検知し通信を遮断する。
URLフィルタ	UF	あらかじめ用意されているWebサイトのカテゴリーに該当するWebサイトへのアクセスを検知する。
アプリケーションガード	APG	ファイル交換ソフトや動画共有、メッセンジャーなど、不特定多数の個人が情報交換可能なアプリケーションを利用した際の通信を検知する。

表 5.1.2-2 UTM のセキュリティ概要

- UTM のセキュリティ機能のうち、IPS、AV、WG で検知した通信を遮断することにより、外部からの攻撃（不正アクセスやマルウェアの侵入）や、外部への不正通信（マルウェア感染などによる企業内部から外部への被害拡大）を防ぐ。
- UTM が攻撃通信を検知および遮断したアラート情報をクラウドで収集した。
- 通常の運用では、IPS や AV、WG で検知および遮断した際に管理者へ通知メールを送信し注意を促す。しかし、本実証事業では、実証参加企業の負担軽減を目的とし、サービス事業者にて当該検知内容を確認のうえ、対応が必要であるもののみ連絡する運用とした。実証参加企業の管理者負担を軽減することを目的としている。

- UTM での IPS、AV、WG で検知、遮断した際の通知方法は、通信の性質によって異なる。
  - 内部から外部（インターネット）への不正通信（以下、外部への不正通信）の場合、すでに端末がマルウェアに感染しているなど被害が発生している可能性があり、ログの記録に加え、重要アラート（「★★★」または「★★」）としてサービス事業者へメール通知を行い、「エンドポイント監視サービス Type-Y」での検知状況をもとに対処の要否を判定する。要対処の場合、実証参加企業の担当者へ連絡および対処依頼を行う。
  - 外部（インターネット）から内部への攻撃（以下、外部からの攻撃）の場合、UTM で通信を遮断していることから対処は不要であり、ログの記録のみとして、メール通知および担当者への連絡は行わない。
  - 脆弱なパスワードなどの「内部の脆弱性」として検知および遮断した場合、ログの記録に加え、重要アラートとしてサービス事業者へメール通知を行う。
- マルウェアへの感染が疑われるアラートをクラウドで自動判定し、検知したアラートの内容および対処内容を記載し、「重要アラート」としてサービス事業者宛にメール通知を行った。通知は 1 時間に 1 回、検知したアラートをまとめて通知を行った。同種のアラートが繰り返し発生し、大量の通知メールによって重要なメールが埋もれてしまい対処されない可能性を考慮したためである。
- UTM のセキュリティ機能のうち、UF と APG を使用し、Web アクセスやアプリケーションの使用状況を確認できるが、本実証事業では利用しなかった。なお、本機能はログの記録のみで、遮断は行わない。

5.1.3. リモートサポート対応

実証参加企業からのサイバーセキュリティに関する相談窓口を開設する。

コールセンターを設置し、メールおよび電話での受付を行い、相談内容に応じて駆け付け対応の要否を判断する。リモートで対応が可能なものについては、電話およびメールにて営業時間内に回答を行う。駆け付け対応が必要な内容については駆け付け隊と連携し、駆け付け対応を実施する。本実証事業終了後、低コストで実運用へスムーズに移行するため、コールセンターは問合せ内容をナレッジとして蓄積する。

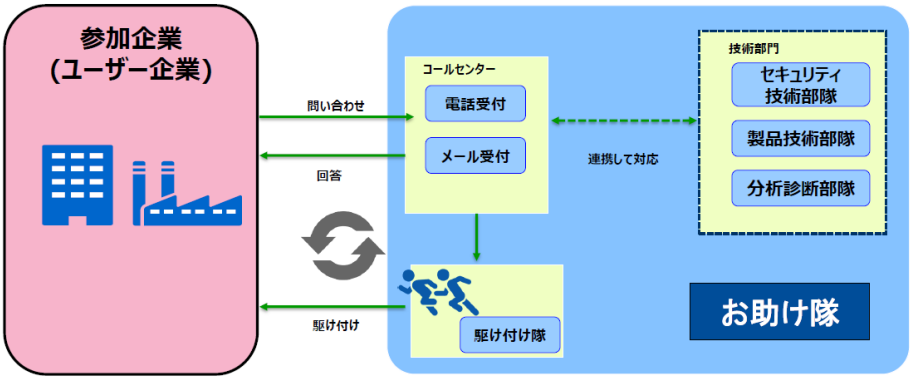


図 5.1.3-1 リモートサポート対応イメージ

5.1.4. 駆け付け対応

駆け付け対応では、スピードとコストの観点から以下の内容で対処方法を検討および選択する。

① 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解決を試みる
② NEC フィールディングの既設の駆け付けサービス（オンサイト保守サービス）を活用する
③ 上記①、②組み合わせて対応する

上記①～③の運用プロセスが、本実証事業終了後にスムーズに商用展開できることを確認する。インシデント時には、インシデントの兆候を検知してから保全ツールによりデータの解析を行い、フォレンジクス調査を行う。

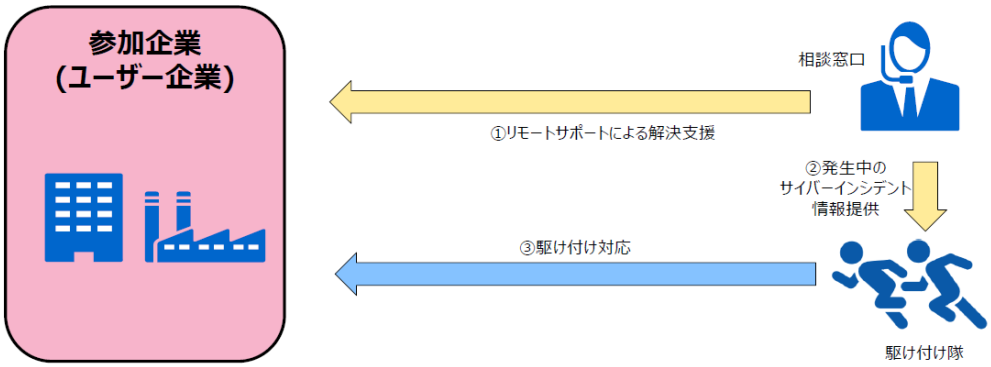


図 5.1.4-1 駆け付け対応イメージ

5.2. スケジュール

実証参加企業に対し、2020 年 9 月に実証サービス準備および導入を依頼し、10 月 1 日（木）～12 月 31 日（木）の期間で監視を行った。

	2020年9月	10月	11月	12月	2021年1月
参加募集	9/7～10/23 18回ウェビナー開催 ▼ 9/10 実地での説明会開催 直接訪問による参加募集				
実証サービス導入/準備		9/29 ～ UTM設置/Type-Yインストール 9/29 ～ セキュリティ診断シート/ アセスメントチェックシート記入			
実証期間		10/1 ～ 12/31 実証監視期間・相談窓口設置			
撤去/実証後アンケート記入				12/25 ～ セキュリティ診断シート 実証後アンケート記入 撤去	

図 4.2-1 スケジュール

6. 地域事業の実証結果

6.1. 実証導入における結果と考察

6.1.1. エンドポイント監視サービス Type-Y における導入

Type-Y エージェントの配布 ID 数と導入 ID 数の推移は以下のとおりである。

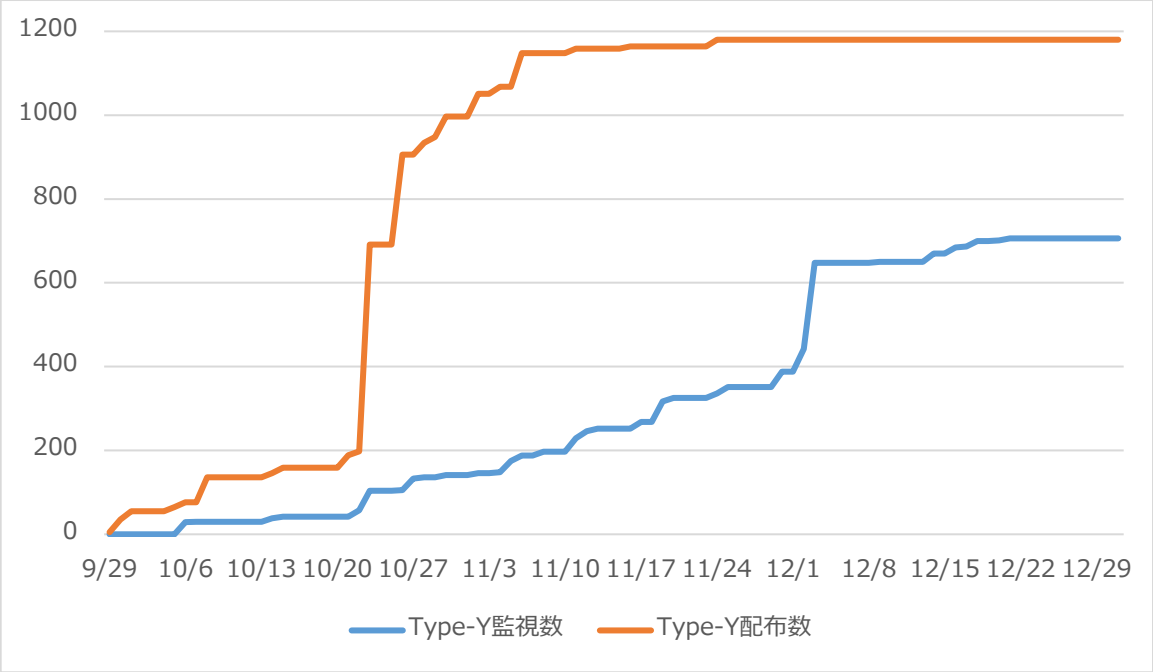


図 6.1.1-1 Type-Y エージェントの配布 ID 数と導入 ID 数の推移

	イベント
2020/09/29	Type-Y エージェントを配布開始
2020/11/19	導入 ID 数が 300ID に到達
2020/11/24	導入予定の Type-Y エージェント 1,180ID を配布完了
2020/12/03	導入 ID 数が 600ID に到達 （1 社にて 178ID が導入され、導入 ID 数が急増）

表 6.1.1-1 実証期間における Type-Y のイベント

図 6.1.1-1 を見ると、Type-Y エージェントの配布 ID 数に対して導入が進まず、最終的に導入 ID 数との間に大きく乖離が生じている。これは、何らかの要因で導入が不可能であるか、導入が停滞したためと考える。乖離の要因を以下の観点から分析、考察する。

(1)　導入に伴う既存環境への変更有無

Type-Y の導入にあたり、既存環境に対して設定変更が必要な事例が見られた。導入に付帯する作業量や難易度によって導入の障壁となった可能性を考える。

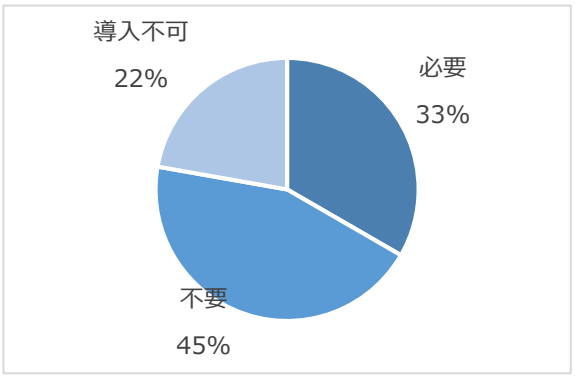


図 6.1.1-2 導入に伴う既存環境への変更要否

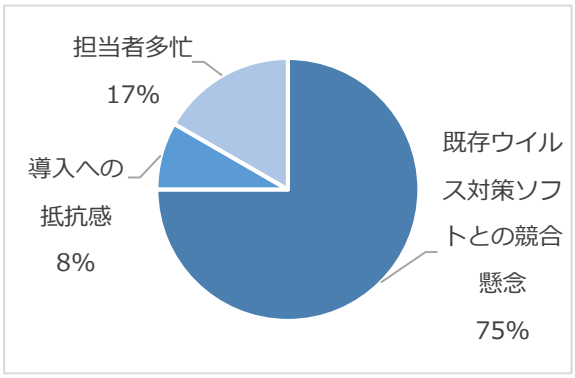


図 6.1.1-3 導入不可の理由

- 約 3 割の企業が、Type-Y の導入のために既存環境への変更が必要であった。主な変更は、既存ウイルス対策ソフトの設定変更であり、導入作業に影響を与えていた。
- 既存ウイルス対策ソフトとの競合の懸念により Type-Y を導入できず、配布 ID 数と導入 ID 数に大きな乖離が生じたことがわかった。

(2)　導入の難易度

実証参加企業にとって Type-Y の導入難易度が、導入の障壁となった可能性を考える。実証参加企業に対するアンケート結果から、Type-Y 導入の難易度を分析する。

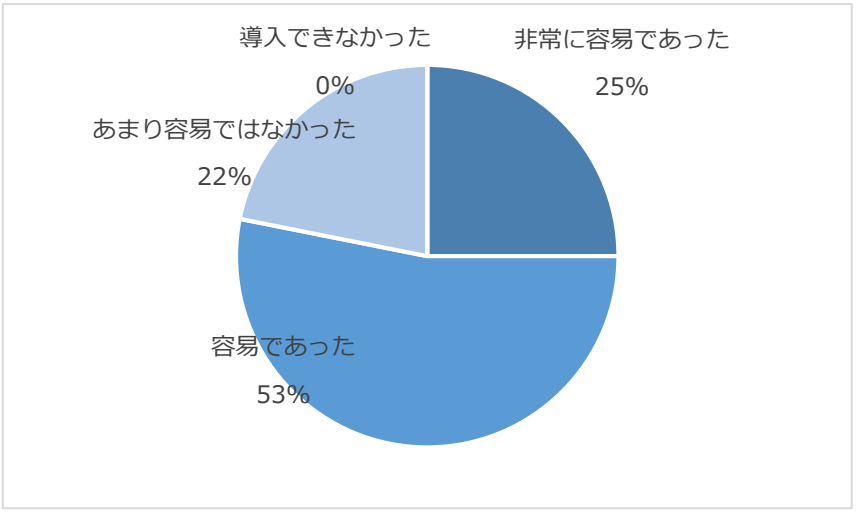


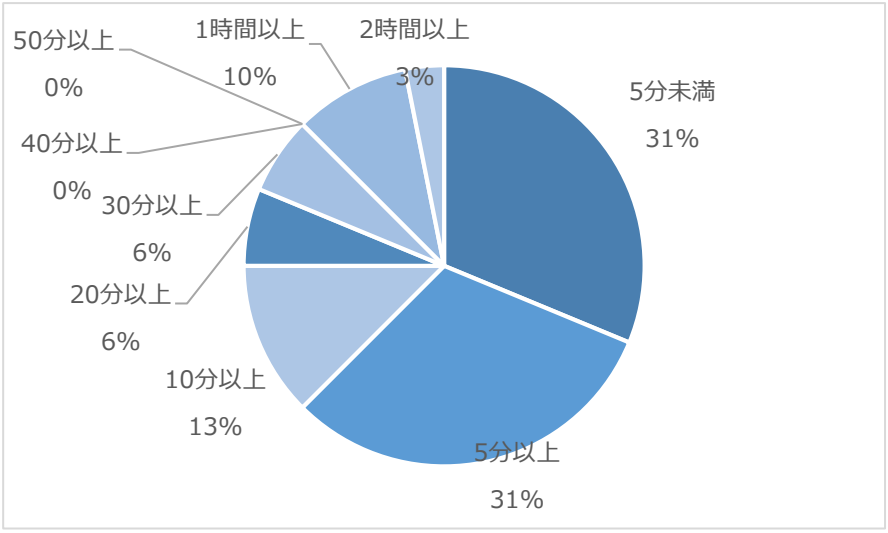
図 6.1.1-4 Type-Y 導入の難易度（有効回答数：32）

- 約 8 割の企業が、Type-Y 導入を容易であると感じたことがわかった。Type-Y をスムーズに導入できたと考えられるため、導入 ID 数への影響は小さい。

(3)　導入の所要時間

Type-Y 導入の所要時間が長く、導入への抵抗感から導入の障壁となった可能性を考える。実証参加企業に対するアンケート結果から、端末 1 台あたりの Type-Y 導入の所要時間を分析する。

図 6.1.1-5 端末 1 台あたりの Type-Y のインストール所要時間（有効回答数：32）



- 6 割の企業が、10 分未満で Type-Y を導入できたことがわかる。Type-Y をスムーズに導入できたと考えられるため、導入 ID 数への影響は小さい。

(4)　マニュアルのわかり易さ

手順書などのマニュアルがわかりにくく、導入の障壁となった可能性を考える。実証参加企業に対するアンケート結果から、マニュアルのわかり易さを分析する。

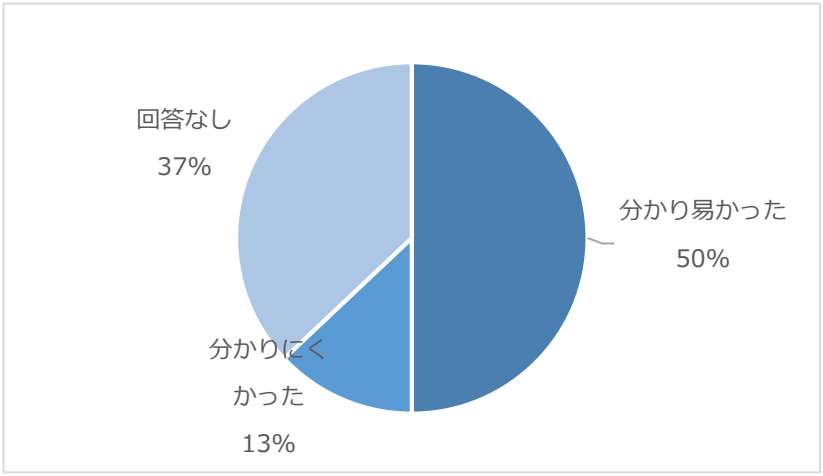


図 6.1.1-6 マニュアルのわかり易さ

- 5 割の企業が、マニュアルがわかり易かったと感じたことがわかった。スムーズな導入を支援できたと考えられるため、導入 ID 数への影響は小さい。

上記の 4 つの観点から、Type-Y エージェントの配布 ID 数と導入 ID 数の乖離は、導入に伴う既存環境への変更が必要であることが原因と考えられる。特に、既存ウイルス対策ソフトとの競

合の懸念については、前述のように事前提供資料にてフォローしていたが回避できなかった。サービス利用申込段階でのヒアリング実施や事前提供資料のブラッシュアップなどが必要である。

次に、図 6.1.1-7 に示す推移の変動が大きい点に着目する。

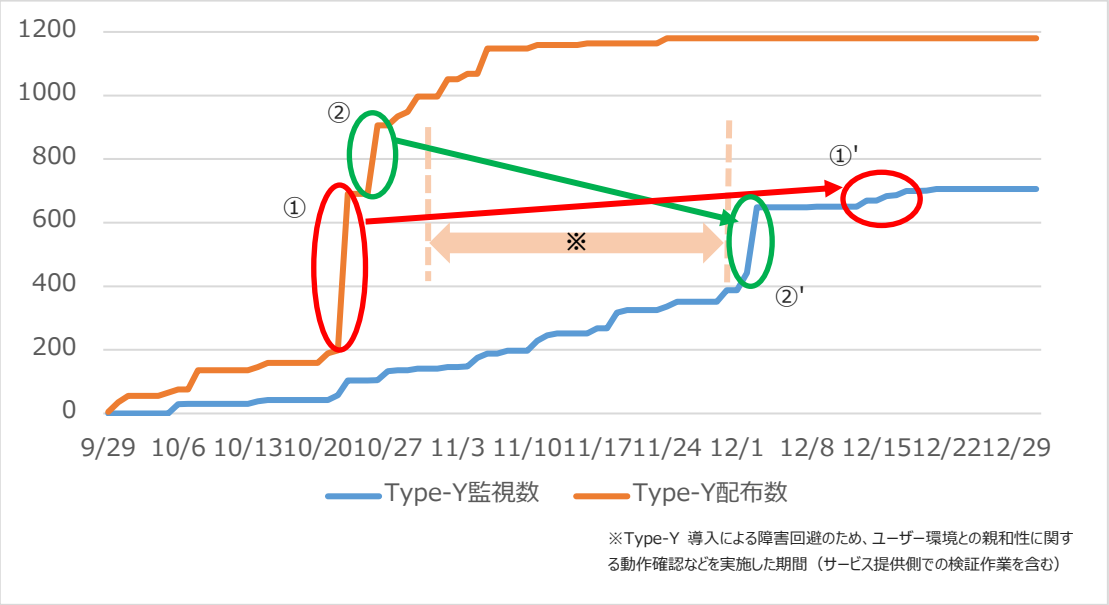


図 6.1.1-7 Type-Y エージェントの配布 ID 数と導入 ID 数の推移（特異点分析）

①、②：特定の 1 社に対する配布 ID 数

①’：実証参加企業が相談窓口を利用せず、単独で導入作業を行った場合の導入 ID 数

②’：相談窓口の支援による効率的な導入作業を行った場合の導入 ID 数

①と①’、②と②’はそれぞれ対応する配布 ID 数・導入 ID 数である。①と①’では大きな乖離が生じているが、②と②’では乖離が小さいことがわかる。導入先の環境確認を含めたサービス提供元の導入支援がエンドユーザーの作業負荷を軽減させ、導入の促進に繋がったと考えられる。なお、図 6.1.1-7 中の※印の期間については Type-Y 導入による障害回避のため、既存環境との親和性に関する動作確認を実施した期間であり、導入までに時間を要した。

6.1.2. サイバーセキュリティ見守りサービスの導入

(1) UTM 到着から導入までのリードタイム

実証参加企業へのUTM到着から設置後、オンラインを確認するまでの期間は以下のとおりである。

リードタイム	社数（割合）
1 週間以内	23 （43%）
2 週間以内	11 （20%）
3 週間以内	6 （11%）
4 週間以内	9 （17%）
5 週間以内	1 （2%）
6 週間以内	3 （6%）
7 週間以内	0 （0%）
8 週間以内	1 （2%）
合計	**54**

表 6.1.2-1 UTM 到着からオンライン確認までのリードタイム

- 全体の約 60%が、UTM 到着後 2 週間以内に設置を完了し監視を開始できている。
- 平均 14 日（2 週間以内）で設置を完了したことがわかった。
  →商用に向け、設置から監視開始までのリードタイムを短縮するサポートが必要である。
- 8 週間以内となった 1 社については、55 日後の設置となっている。
  →設置作業を担当するネットワーク業者との調整に時間を要した。

(2) UTM の自力設置

UTM を実証参加企業自身でどの程度設置できたかを調査した。なお、設置作業において、サービス事業者が個別対応を行ったケースがあるため、以下の項目で社数を調査した。

設置方法	社数（割合）
実証参加企業で自力設置	23（43%）
問合せを実施後自力で設置	16（30%）
駆け付け対応	2 （4%）
サービス事業者で設置	13（24%）
合計	**54**

表 6.1.2-2 UTM の自力設置

- 全体の約 70%が自身で設置できたことがわかった。「サービス事業者で設置」の 13 件についても、自力設置できた可能性はあり、90%程度は自力設置可能であったと推測する。

- 既設のネットワーク機器が存在するケースでは、当該機器の設定変更が必要であった。

(3) UTM 設置の所要時間

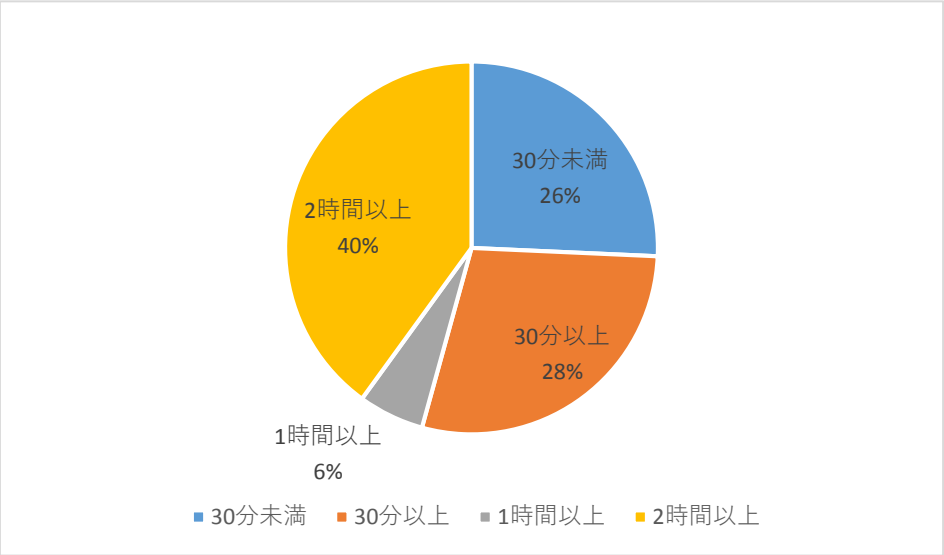


図 6.1.2-1 UTM 設置の所要時間（有効回答数：35）

実証後アンケートにて、UTM 設置の所要時間を調査した。

- 「2 時間以上」が最も多かった。
- 短時間で設置を完了している実証参加企業が一定数いるため、自社のネットワーク環境を把握度合いにより差が生じていると推測する。

(4) UTM 設置の難易度

実証後アンケートにて、UTM 設置の容易性について調査した。

回答	社数（割合）
非常に容易であった	4（10%）
容易であった	14（36%）
あまり容易ではなかった	17（44%）
設置できなかった（駆け付けサービスを利用した）	4（10%）

表 6.1.2-3 UTM 設置の容易性

- 「あまり容易でなかった」が 4 割以上となった。

  →前述のように、UTM は容易に設置できるよう設計しているが、エンドユーザーとの感覚にギャップがあることがわかった。
- エンドユーザーが容易でないと感じた理由を以下に示す。
  - 専門知識を持つ人材がいなかった
  - アクティベーションできなかった
  - 既存システムに影響が出た
  - NW を切断するので容易ではない

・ ネットワーク業者へ依頼する必要があり調整の時間がかかった

(5) 手順書やマニュアルの内容のわかり易さ

実証後アンケートにて、手順書およびマニュアルのわかり易さについて調査した。

回答	社数
わかり易かった	26（68%）
わかりにくかった	12（32%）

表 6.1.2-4 手順書やマニュアルのわかり易さ

- 全体の約 7 割が「わかり易かった」と回答した。理由を以下に示す。（重複回答あり）
  - ・ 内容が簡潔にまとまっていた。（13 社）
  - ・ 専門的な知識がなくても理解できる内容になっていた。（15 社）
- 「わかりにくかった」と回答した理由を以下に示す。
  - ・ 専門的な言葉が多く、理解に時間がかかった。（5 社）
  - ・ 説明が不十分な箇所があった。（4 社）

上記調査の結果、設置を簡素化する施策の検討が必要であることがわかった。また、手順書やマニュアルに記載する用語や表現に改善の余地があることがわかった。

6.2. 実証結果の詳細

6.2.1. エンドポイント監視サービス Type-Y での検知結果

(1) 監視期間

監視期間は以下のとおりである。

監視期間	ID 数（割合）
60 日以上	141（20%）
45 日以上 60 日未満	245（35%）
30 日以上 45 日未満	174（24%）
15 日以上 30 日未満	127（18%）
15 日未満	19（2%）
計	**706**

表 6.2.1-1 Type-Y 監視期間

- 平均監視期間は 1ID あたり 43 日であり、最長の監視期間は 87 日間である。
- 当初、90 日間を監視期間として計画していたが、実証参加企業募集およびサービス導入が遅れたことで、監視期間の平均は期待値の半分程度に留まった。
- サービスの特性上、アラート検知数の推移は、監視期間の長短に依存しないと（サービス導入したタイミングから 1 週間程度での端末内チェックに対するアラートが大半と推測）見込んでおり、最短の監視期間でも想定範囲は十分にクリアできていることから、計画より監視期間が短かったことに対する影響はないと判断した。

(2) 検知状況

実証期間中の検知状況は以下のとおりである。

検知詳細	検知数	検知台数（割合） （検知率 n=706）	検知社数（割合） （検知率 n=42）
要注意検知 ※1	90	35（5%）	20（48%）
過検知 ※2	139	36（5%）	22（52%）
合計（重複を除く）	**229**	**60（8%）**	**26（62%）**

※1 要注意検知：マルウェアの疑いがある検知、※2 過検知：解析の結果、無害なファイルと判定した検知

表 6.2.1-2 Type-Y 検知状況

- 検知総数は 229 件であり、そのうち対応が必要な要注意検知は 77 件あり、検知全体の 39%を占めた。

- Type-Y がインストールされた 706 台のうち、検知があった台数は 60 台であり 8%を占めた。
- Type-Y がインストールされた 42 社のうち、検知があった社数は 26 社であり 62%を占めた。

日別の検知数は以下のとおりである。

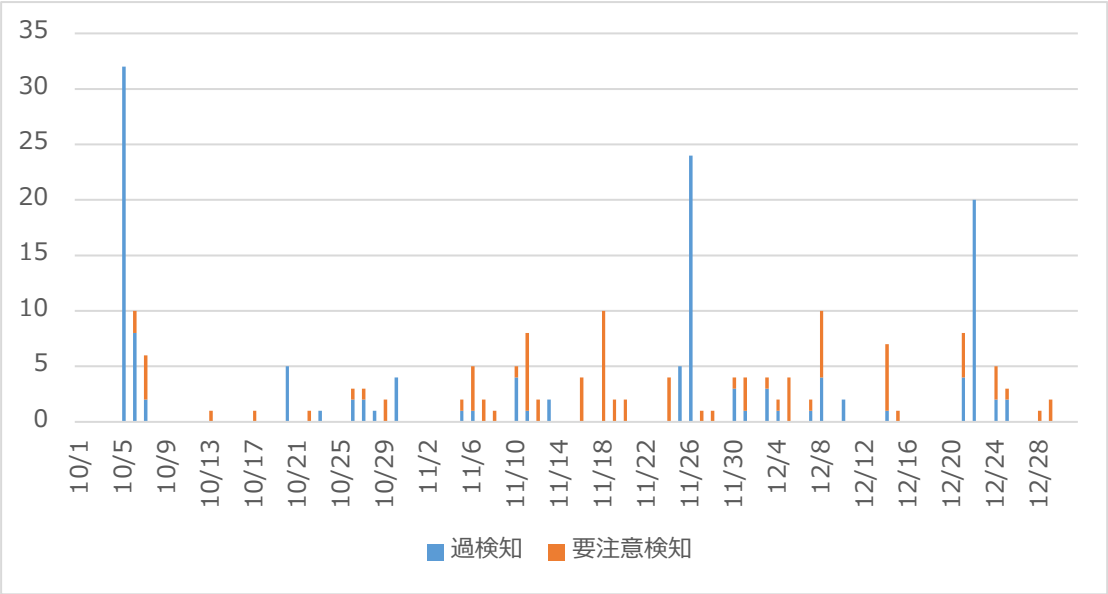


図 6.2.1-1 検知数の日次推移

- 監視 ID 数が増えることで、検知数も増加することを想定していたが、監視 ID 数との直接的な関連性は見られなかった。

検知エンジン別による検知詳細は以下のとおりである。

検知エンジン	要注意検知		過検知	
	検知数	検知ファイル数	検知数	検知ファイル数
静的解析による検知	72	26	123	38
脆弱性を狙った攻撃の検知	13	5	7	4
動的解析による検知	4	1	6	6
サンドボックスによる検知	1	1	2	2
機械学習による検知	0	0	1	1
計	**90**	**33**	**139**	**51**

表 6.2.1-3 エンジン別検知数結果

- 静的解析エンジンでは、マルウェアや、悪意あるコードが隠ぺいされている可能性を含むパッカーを検知した。
- 脆弱性を狙った攻撃では、不審なファイルの生成や危険な動作を検知した。
- 動的解析エンジンでは、不審なファイル検索を検知した。
- サンドボックスエンジンでは、不審な命令の実行を検知した。
- 機械学習エンジンでは、要注意検知はなかった。

静的解析による要注意検知の詳細は以下のとおりである。

検知詳細	検知数
マルウェアとして定義されています。	46
パッカーを検出しました。悪意あるコードが隠ぺいされている可能性があります。	15
セキュリティソフトウェアに対して攻撃を行う可能性があります。	4
マルウェア特有の行動を取る可能性があります。	3
不審なファイルです。	2
コードセクションの構造に異常を検出しました。悪意あるコードが隠ぺいされている可能性があります。マルウェア特有の行動を取る可能性があります。	1
コードセクションの構造に異常を検出しました。悪意あるコードが隠ぺいされている可能性があります。不審なセクション構造を検出しました。マルウェア特有の行動を取る可能性があります。	1

脆弱性を狙った攻撃の要注意検知の詳細は以下のとおりである。

検知詳細	検知数
危険な動作を検出しました。	10
不審なファイルが生成されました。マルウェアである可能性があります。	3

動的解析による要注意検知の詳細は以下のとおりである。

検知詳細	検知数
隠しプロセスが自身で生成したバッチファイルを実行しようとしました。	4

サンドボックス解析による要注意検知の詳細は以下のとおりである。

検知詳細	検知数
不審な命令を実行しようとしています。	1

実証参加企業別の 1ID あたりの要注意検知数は以下のとおりである。

企業	1ID あたりの要注意検知数	総要注意検知数	実証 ID 数	業種
企業 001	6.00	6	1	O 教育学習支援業
企業 002	2.67	16	6	O 教育学習支援業
企業 003	1.33	4	3	R サービス業（他に分類されないもの）
企業 004	1.00	1	1	G 情報通信業
企業 005	0.62	8	13	D 建設業
企業 006	0.48	10	21	E 製造業
企業 007	0.40	12	30	E 製造業
企業 008	0.36	4	11	G 情報通信業
企業 009	0.30	7	23	G 情報通信業
企業 010	0.20	1	5	R サービス業（他に分類されないもの）
企業 011	0.18	4	22	E 製造業
企業 012	0.13	2	16	I 卸売業・小売業
企業 013	0.09	3	35	M 宿泊業・飲食店
企業 014	0.08	2	25	E 製造業
企業 015	0.08	1	13	H 運輸業・郵便業
企業 016	0.06	3	49	R サービス業（他に分類されないもの）
企業 017	0.04	1	23	G 情報通信業
企業 018	0.03	2	73	G 情報通信業
企業 019	0.02	3	174	F 電気・ガス・熱供給・水道業

表 6.2.1-4 実証参加企業別 1ID あたりの要注意検知数

- 1ID あたりの要注意検知数が最も多かった企業は 6.00 件であった。
- 1ID あたりの要注意検知数が最も多かった業種は「O 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く、検知数も増加傾向にあったと推測する。
- 2 番目以降の 1ID あたりの要注意検知数多かった業種は順に「G 情報通信業（12%）」、「R サービス業（他に分類されないもの）（11%）」、「E 製造業（8%）」であり、「F 電気・ガス・熱供給・水道業」を除いて、業種別の割合の順番と同じ結果となった。

(3) 検知後の対応状況

対応が必要な要注意検知の対応状況は以下のとおりである。

対応結果	対応内容	件数
対応実施	実証参加企業のみで駆除作業を実施	24
	相談窓口問合せ後、実証参加企業のみで駆除作業を実施	1
	サポートからの連絡後、実証参加企業のみで駆除	10
	サポートからの連絡後、相談窓口の支援を受けて駆除	2
未対応	サポートからの連絡後、実証参加企業での駆除作業待ち	53

表 6.2.1-5 要注意検知後の対応状況

- 要注意検知に対して、対応を実施した割合は 41%であった。
- 対応を実施した 37 件に対して、「実証参加企業のみで駆除作業を実施」や「相談窓口問合せ後、実証参加企業のみで駆除作業を実施」の、自発的に駆除作業を実施した割合は、68%であった。アラートに気付き、対応まで実施可能な割合が結果として得られた。
- 対応を実施した 37 件に対して、サポートからの連絡後に対応を実施した割合は 32%であった。およそ 3 件のうち 1 件は実証参加企業のみで自発的に対応されないことが判明した。

対応を実施した要注意検知後の対応状況は以下のとおりである。

	検知から駆除までの平均日数	サポート連絡から駆除までの平均日数
実証参加企業のみで駆除作業を実施	2.31	-
相談窓口問合せ後、実証参加企業のみで駆除作業を実施	2.05	-
サポートからの連絡後、実証参加企業のみで駆除作業を実施	11.63	5.69
サポートからの連絡後、相談窓口の支援を受けて駆除作業を実施	0.11	0.04

表 6.2.1-6 対応にかかる日数

- 検知から駆除までの平均日数は 4.03 日であった。
- 自発的に駆除作業を実施した「実証参加企業のみで駆除作業を実施」や「相談窓口問合せ後、実証参加企業のみで駆除作業を実施」は 3 日以内に対応できることが判明した。
- サポート連絡から駆除までの平均日数は 4.34 日であった。システムの自動通知のみでは、約 3 割が対応できないことが判明した。

6.2.2. サイバーセキュリティ見守りサービスでの検知結果

(1) 監視台数と監視期間

UTM による監視は、10 月 1 日から順次開始。監視台数の推移は以下のとおりである。

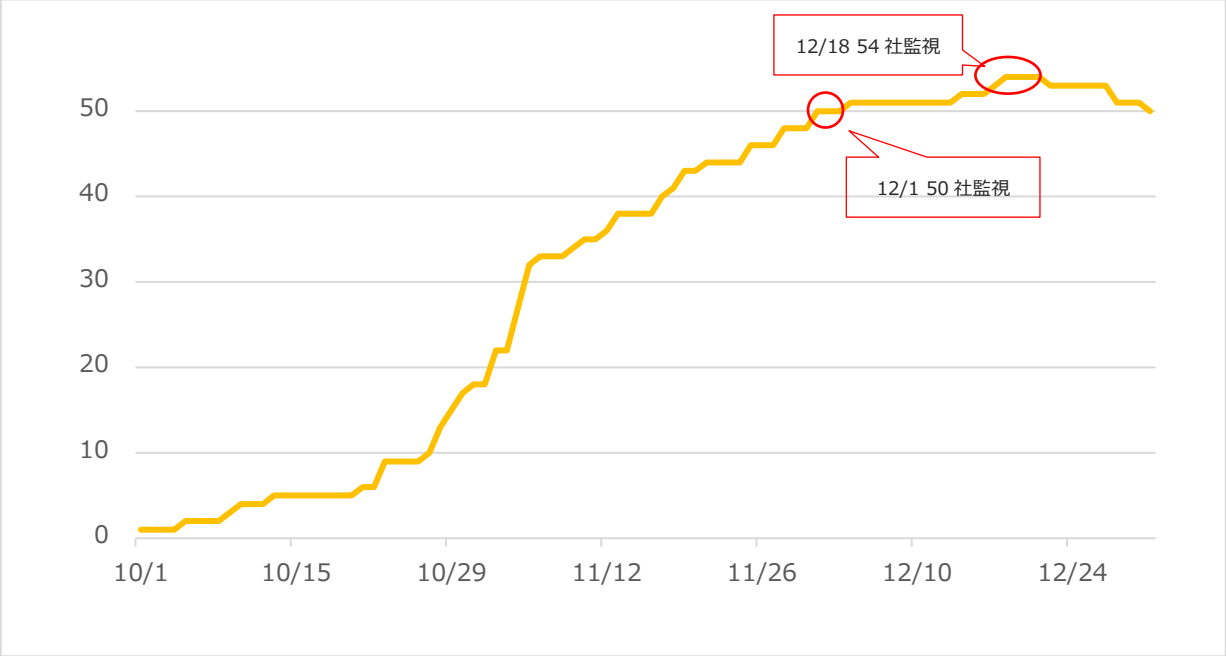


図 6.2.2-1 UTM 監視台数の推移

- 12 月 1 日に監視対象企業数が目標の 50 社に達した。
- 実証参加企業のうち 2 社が、同一 LAN でのフロア共有を行っており、2 社を UTM1 台で共有し監視しているため、UTM 機器の設置数は 53 台であった。
- 監視台数のピークは、12 月 18 日から 12 月 21 日の 54 社であった。
- 監視最終日の設置企業数は、50 社であった。
- 平均監視期間は 54 日であった。
- 12 月 22 日以降、監視対象企業の都合（年末に際し電源を切るなど）により、UTM の監視台数が減少した。

UTM 監視期間	社数（割合）
30 日以下	4（7%）
31 日以上 45 日以下	13（24%）
46 日以上 60 日以下	20（37%）
61 日以上	17（31%）
計	**54**

表 6.2.2-1 UTM 監視期間

(2) 実証参加企業におけるサイバー攻撃の検知状況

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以下のとおりである。

検知状況	検知した通信	社数
あり	外部からの攻撃	23
	外部への不正通信	13
	（外部からの攻撃と外部への不正通信の両方を検知した社数）	12
	合計	36
	合計（重複を除く）	24
	内部の脆弱性（「外部からの攻撃」と重複）	1
	検知あり合計（重複を除く）	24
なし		30
合計（重複を除く）		54

表 6.2.2-2 検知および遮断が発生した社数

- 特定の 1 社にて UTM 設置後、以下検知名の通信が毎日 10 件程度検知された。
  - WINDOWS Microsoft Windows SMB anonymous user request detected tcp 139
    →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
- 外部への不正通信を検知した 13 社のうち、マルウェアに感染していると思われるアラート（重要度「★★★」）は無かった。
- 外部からの攻撃を検知している実証参加企業のうち、1 日あたりの検知および遮断件数上位 10 社を以下に示す。
  - 1 日あたりの平均検知および遮断件数は、9.42 件（突出している 2 社を除いた場合、0.26 件）であった。

企業	1 日あたりの件数	UTM 設置日数	業種	従業員数
企業 201	634.71	28	情報通信業	201~300
企業 202	87.63	83	情報通信業	21~50
企業 203	2.74	65	サービス業（他に分類されないもの）	101~200

企業 204	2.05	80	建設業	201~300
企業 205	1.08	53	製造業	301~
企業 206	0.86	57	情報通信業	6~10
企業 207	0.94	49	サービス業（他に分類されないもの）	6~10
企業 208	2.14	14	情報通信業	21~50
企業 209	0.45	58	電気・ガス・熱供給・水道業	101~200
企業 210	0.76	34	医療・福祉	101~200

表 6.2.2-3 1 日あたりの検知および遮断件数上位 10 社

- 件数が突出している 2 社は、「情報通信業」であった。（上位 10 社のうち約 40%）
- 検証期間中の外部からの攻撃（日別）を以下に示す。
- 大きく 2 つの山があり、①の山については、実証参加企業（企業 202）の設置後、「WINDOWS Microsoft Windows SMB remote code execution attempt（EternalBlue）tcp 445」の大量検知が続き、10/21 以降急激に検知が減少し、10/29、30 で再度検知が増えるが 11 月以降検知されなくなっている。②の山は、実証参加企業（企業 1）の設置後、「CAN SIPVicious User-Agent Detected」が検知されており、検証終了したが現在も攻撃は続いていると思われる。いずれも攻撃原因は不明であるが、グローバル IP の使用により、外部からアクセス可能な機器があると攻撃は多くなっている可能性があるが、今回の検証においては、攻撃を検知し通信を遮断しているため詳細調査は行っていない。

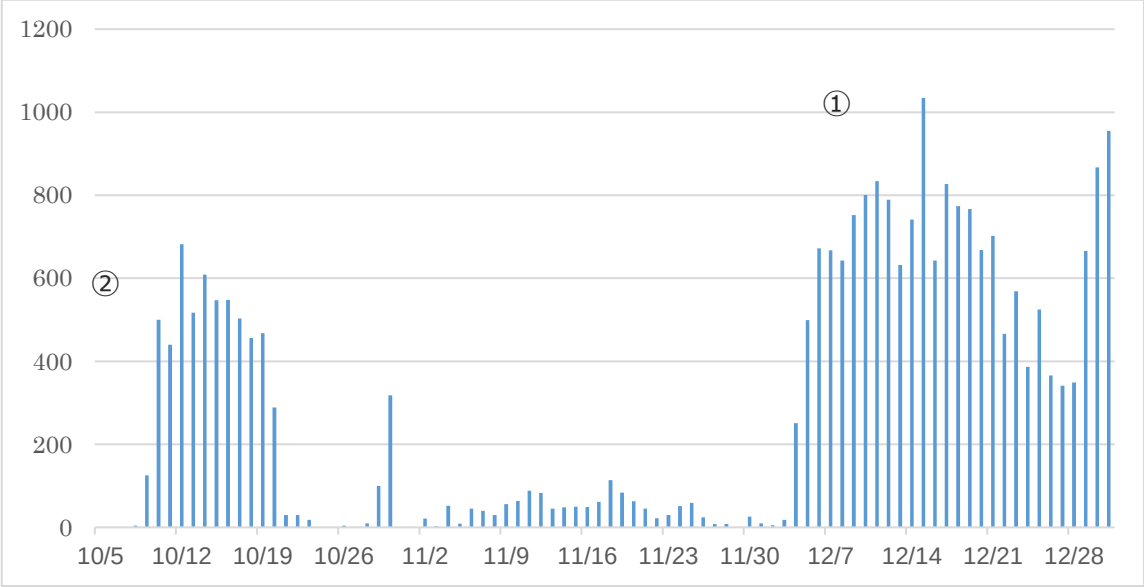


図 6.2.2-2 IPS 検知数（外部からの攻撃）

● 簡易 UTM でのサイバー攻撃の検知および遮断件数

本実証における UTM の検知および遮断件数、社数は以下のとおりである。1 回のインシデントで複数回の検知および遮断を行うこともあり、その場合も、検知・遮断した件数をカウントしている。

検知した通信	機能	件数	社数
外部からの攻撃	IPS	25,698	21
	AV	90	8
外部への不正通信	IPS	118	11
	AV	0	0
	WG	66	6
内部の脆弱性	IPS	25	1
合計		**25,997**	-
外部からの攻撃（IPS）を除く		**299**	

表 6.2.2-4 UTM の検知および遮断件数、社数

外部からの攻撃を除いた月別での検知・遮断件数は以下となる

検知月	AV	IPS （外部への不正通信）	WG	内部の 脆弱性
10 月	13	8	0	0
11 月	44	45	42	25
12 月	33	65	24	0
合計	**90**	**118**	**66**	**25**

表 6.2.2-5 検知、遮断件数（月別）

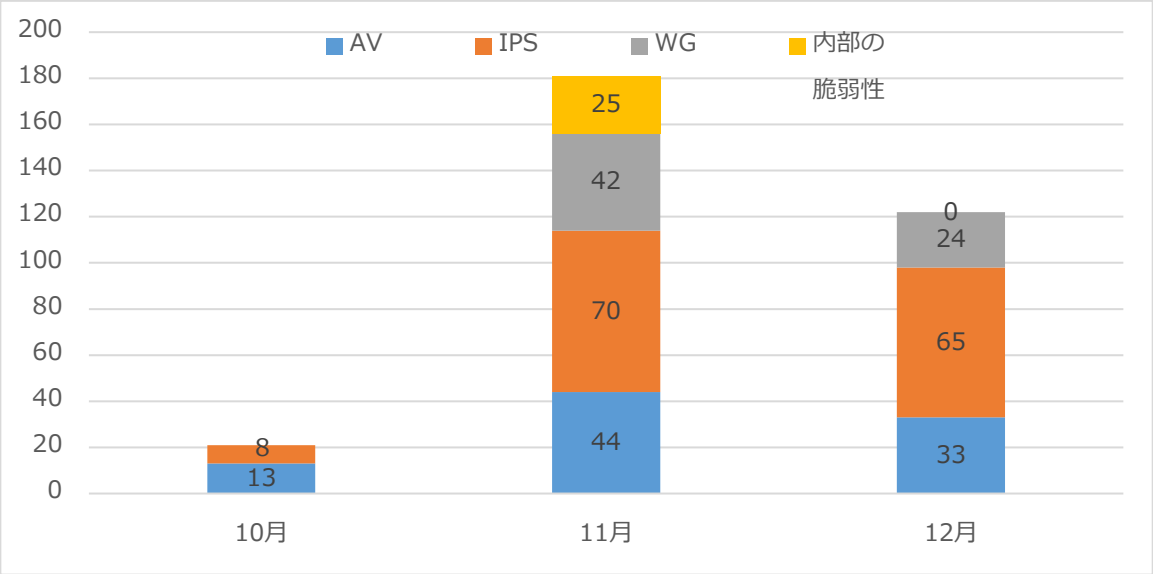


図 6.2.2-3 月別検知数（外部からの攻撃（IPS）を除く）

- 上記検知数では、前述の「WINDOWS Microsoft Windows SMB anonymous user request detected tcp 139」の検知分と誤検知分は除いている。
- 10 月の検知が少ないのは、設置台数が少ないためであるが、設置台数が最も多かった 12 月と比較し 11 月の方が検知・遮断件数が多い結果となっている。内部の脆弱性を除くと 11 月、12 月でほぼ横ばいではある。

  →設置台数増加とともに件数も増加するが、月別で見ると件数は増減しており、検知傾向や特異点などは見られなかった。

検知件数の多い順で検知機能別にまとめると以下となる。

企業	AV	IPS（外部への不正通信）	WG	内部の脆弱性	検知件数合計	設置日数	1 日あたりの件数
企業 301	55	0	0	0	55	92	0.60
企業 302	9	21	17	0	47	28	1.68
企業 303	0	0	38	0	38	43	0.88
企業 304	0	35	3	0	38	65	0.58
企業 305	0	0	0	25	25	57	0.44
企業 306	0	25	0	0	25	75	0.33
企業 307	0	13	0	0	13	34	0.38
企業 308	0	9	3	0	12	57	0.21

企業 309	8	0	0	0	8	83	0.10
企業 310	8	0	0	0	8	60	0.13
企業 311	1	5	0	0	6	52	0.12
企業 312	0	5	0	0	5	80	0.06
企業 313	5	0	0	0	5	58	0.09
企業 314	2	2	0	0	4	34	0.12
企業 315	0	2	2	0	4	72	0.06
企業 316	0	0	3	0	3	56	0.05
企業 317	2	0	0	0	2	45	0.04
企業 318	0	1	0	0	1	64	0.02
合計	**90**	**118**	**66**	**25**	**299**	**1,055**	**0.28**

表 6.2.2-6 検知機能別件数

- 外部からの攻撃（IPS）を除き、検知および遮断が確認された企業は、54 社中 18 社であった。
- 1 日あたりの件数の 0.28 件は、実証企業全体ではなく、検知・遮断された企業に対しての件数である。

(3) 簡易 UTM でのサイバー攻撃の検知状況（業種別）

実証参加企業の業種により、外部からの攻撃や外部への不正通信の検知状況に傾向があるか確認した。業種別の検知社数の状況は以下のとおりである。

検知状況	検知した通信	建設業	製造業	電気・ガス・熱供給・水道業	情報通信業	運輸業・郵便業	卸売業・小売業	不動産業・物品賃貸業	学術研究・専門・技術サービス業	宿泊業・飲食店	教育学習支援業	医療・福祉	サービス業（他に分類されないもの）
	（事業構成比）	**6%**	**15%**	**4%**	**22%**	**11%**	**9%**	**4%**	**2%**	**2%**	**4%**	**4%**	**19%**
あり	外部からの攻撃	1	3	1	6	2	1	1	0	1	1	1	5
	外部への不正通信	1	0	0	2	2	2	1	0	0	1	1	2
	内部の脆弱性	0	1	0	0	0	0	0	0	0	0	0	0

	（外部からの攻撃と外部への不正通信の両方を検知した社数）	1	1	0	2	2	1	1	0	0	1	1	2
	合計	**2**	**4**	**1**	**8**	**4**	**3**	**2**	**0**	**1**	**2**	**2**	**7**
	検知あり合計（重複を除く）	**1**	**3**	**1**	**6**	**2**	**2**	**1**	**0**	**1**	**1**	**1**	**5**
	検知率	4%	13%	4%	25%	8%	8%	4%	0%	4%	4%	4%	21%
なし		2	5	1	6	4	3	1	1	0	1	1	5
合計（重複を除く）		**3**	**8**	**2**	**12**	**6**	**5**	**2**	**1**	**1**	**2**	**2**	**10**

表 6.2.2-7 検知社数（業種別）

- 今回の実証では、「情報通信業」や「サービス業（他に分類されないもの）」での実証参加企業数が多いため、それに応じて検知社数も多くなっている。
- 「学術研究・専門・技術サービス業」のみ検知がなかったが、同業種の実証参加企業が 1 社であったため、母数が増えれば検知された可能性はあり、それを踏まえると、どの業種でも一定の割合で外部からの攻撃や外部への不正通信を検知している。
- 業種による偏りは見受けられず、業種ごとの参画構成比率と検知率は大きく変わらずほぼ同じである。

(4) 簡易 UTM でのサイバー攻撃の検知・遮断件数（業種別）

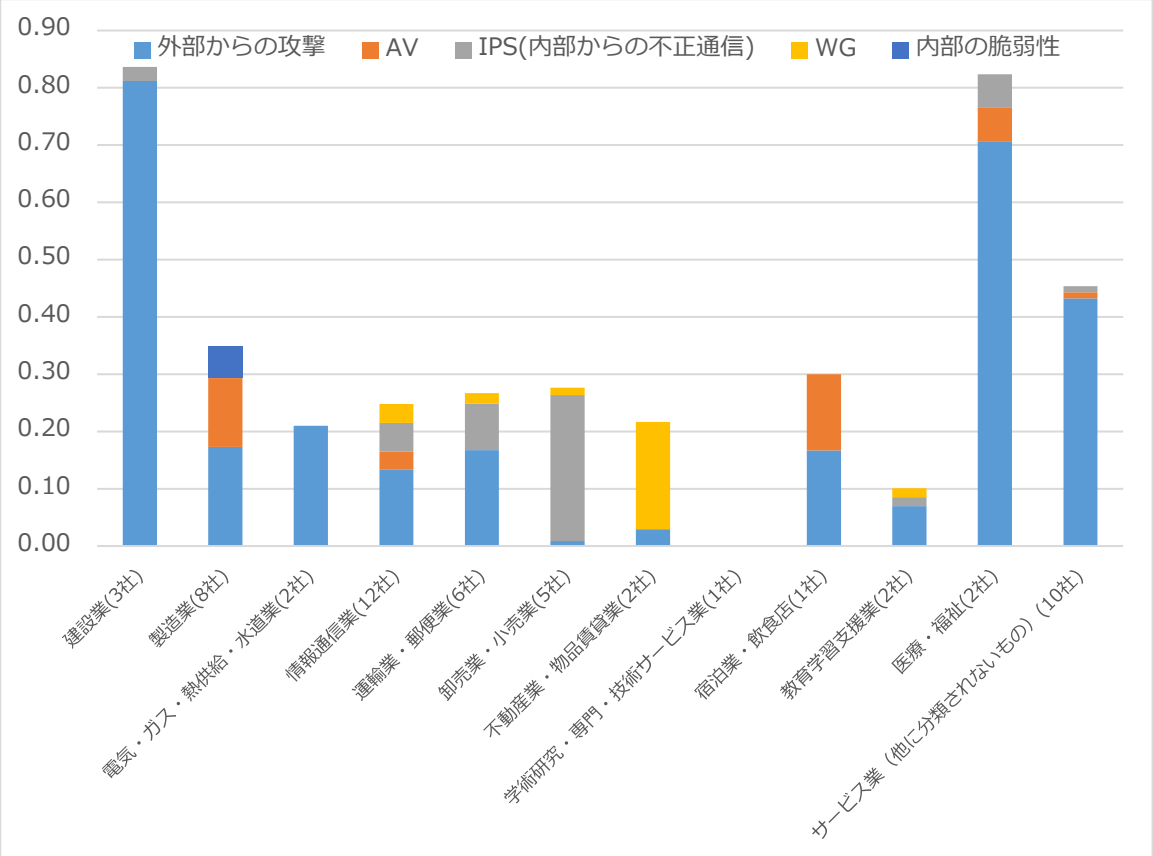
業種別の検知・遮断件数の状況は以下のとおり。

検知した通信	建設業	製造業	電気・ガス・熱供給・水道業	情報通信業	運輸業・郵便業	卸売業・小売業	不動産業・物品賃貸業	学術研究・専門・技術サービス業	宿泊業・飲食店	教育学習支援業	医療・福祉	サービス業（他に分類されないもの）
（事業別社数）	3	8	2	12	6	5	2	1	1	2	2	10
外部からの攻撃	164	79	26	81	27	2	6	0	10	9	24	242
AV	0	55	0	19	0	0	0	0	8	0	2	6
IPS（内部からの不正通信）	5	0	0	30	13	60	0	0	0	2	2	6
WG	0	0	0	20	3	3	38	0	0	2	0	0

内部の脆弱性	0	25	0	0	0	0	0	0	0	0	0	0
合計	**169**	**159**	**26**	**150**	**43**	**65**	**44**	**0**	**18**	**13**	**28**	**254**

表 6.2.2-8 検知・遮断数（業種別）

- 外部から攻撃が多い 2 社の「外部からの攻撃」件数は、集中的に攻撃されていることは判明しており他の数値を大幅に凌駕する件数のため除いている。
- 業種ごとの実証参加企業数や設置日数が異なるため、監視総日数から 1 社 1 日あたりの検知・遮断件数については以下のとおりとなる。



- **図 6.2.2-4 1 社 1 日あたりの検知および遮断件数（業種別）**

- 外部からの攻撃多い「情報通信業」の 2 社の件数を除いているため、「建設業」と「医療・福祉」が共に 1 日 0.8 件を超えており、攻撃が多い傾向が出ている。
- 「学術研究・専門・技術サービス業」が 0 件ではあるが、実証参加企業数が 1 社のため、他業種同様に母数が増えると攻撃される企業があると推測する。
- それ以外の業種では、多少の差はあるものの概ね 1 日 0.5 件を下回っている件数であるが、外部からの攻撃、外部への不正通信が確認されている。
- 参考として「情報通信業」の外部からの攻撃を除かない場合の情報通信業の 1 日あたりの件数は、41.6 件であった。

(5)　重要度別検知数

UTM の検知では、下記のとおり検知内容に重要度を定義し、その重要度により実証参加企業への対応を決定している。

重要度	定義	お客様の対応
★★★	・内部（お客様環境）からの通信で、マルウェアの振る舞いとして検知したもの（特定のマルウェア通信と一致 または 酷似したもの）	お客様は至急マルウェアへの対処が必要
★★☆	・内部からの通信で、マルウェアの振る舞いであることの特定にまで至らないが攻撃の振る舞いとして検知したもの ・特定のソフトウェアや機器の脆弱性に対しての振る舞いとして検知したもの	マルウェアによる攻撃の可能性があるため、通信元や通信先に対しのマルウェア感染の確認や使用ソフトウェアや機器の利用状況確認などが必要
★☆☆	・通常の通信かマルウェア感染による通信かの判断が初見では難しいが、セキュリティ上リスクがある通信であるため UTM で遮断するもの 例）アクセス解析ツールの通信、 単純なパスワードによる認証通信 など	UTM が遮断していることもあり、お客様はセキュリティ的には至急の対処は不要

表 6.2.2-9 重要度の定義

- 本実証では、Type-Y がエンドポイントとしてインストールされているため、重要度が「★★★」の検知アラートメールが発報された場合、実証参加企業への連絡と対処方法の提示と対処の実施依頼を行うこととした。
- 重要度別の検知数は以下のとおり。

重要度	AV	IPS	WG
★★★	0	0	0
★★	0	74	66
★	90	69	0
合計	**90**	**143**	**66**

表 6.2.2-10 検知、遮断数（重要度別）

- 本実証では、最重要アラートとなる「★★★」は検出しておらず、特に実証参加企業へ対応を依頼するインシデントは発生しなかった。

(6)　検知詳細

本実証で検知した、AV、IPS の詳細と WG で通信を止めたアクセス先は、以下のとおりである。

No.	検知内容	説明	件数
1	Trojan.MSWord.Agent.a	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	26
2	Hacktool.MSOffice.Generic.3	ウイルス、ワーム、トロイの木馬などを生成し、他の端末をハッキングする疑いのあるファイルの送受信を検知	14
3	Trojan.Multi.Generic.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	12
4	Trojan.MSOffice.SAgent.4	トロイの木馬の疑いのあるファイルの通信を検知	8
5	Trojan.Win32.Razy.tr7J	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	8
6	Trojan.MSExcel.Logan.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	3
7	Trojan.MSWord.Macro.4	利用者の口座番号などの個人情報や秘匿情報を盗み出したり、攻撃者により端末がコントロールされたりする可能性があるトロイの木馬の疑いのあるファイルの送受信を検知	2
8	Trojan.Script.Generic.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	2
9	Trojan.MSOffice.Agent.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	2
10	Trojan.JS.Redirector.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	2
11	Trojan.MSWord.Generic.4	利用者の口座番号などの個人情報や秘匿情報を盗み出したり、攻撃者により端末がコントロールされたりする可能性があるトロイの木馬の疑いのあるファイルの送受信を検知	1

12	Trojan.MSIL.Taskun.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	1
13	Trojan.PDF.Fraud.4	銀行口座番号などの個人情報や秘匿情報を窃取する Windows のトロイの木馬の疑いのあるファイルの送受信を検知	1
14	Trojan.PDF.Generic.O	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	1
15	Trojan.MSOffice.Alien.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	1
16	Trojan.MSOffice.SLoad.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	1
17	Trojan.MSExcel.Agent.a	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	1
18	Trojan.MSExcel.Agent.4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	1
19	Trojan.MSIL.NanoBot.m	Windows 端末をリモートからハッキングする疑いのあるファイルの送受信を検知	1
20	Trojan.BAT.Crypter.tqa8	Windows 端末のファイルを暗号化し、身代金を要求する疑いのあるファイルの送受信を検知	1
21	Trojan.MSIL.Noon.l	キーストロークやマウスの操作内容を搾取するトロイの木馬の疑いのあるファイルの送受信を検知	1
合計			**90**

表 6.2.2-11 検知一覧（アンチウイルス）

- 検知のほとんどがトロイの木馬の疑いのあるファイルの送受信である。
- メール添付ファイルでの検知がほとんどであり、検知したファイルはすべて無害化されている。
- 実証期間終盤の 12 月中旬以降にファイル転送での検知も 11 件確認された。

No.	検知内容	説明	件数
1	SCAN SIPVicious User-Agent Detected	検証ツール SIPVicious のスキャンを検出	16,733

2	WINDOWS Microsoft Windows SMB remote code execution attempt（EternalBlue） tcp 445	Windows のファイル共有サービス（SMB）の脆弱性（CVE-2017-144、-146）を狙った攻撃の疑いのある通信を検知	4,782
3	EXPLOIT Netcore Router Udp 53413 Backdoor	Netcore 社製ルーターの UDP ポート 53413 が WAN 側から接続できる不具合を狙った疑いのある通信を検出	1,011
4	JSIG-UDP : Netcore-Cmd-Exec	Netcore 社製ルーターに存在するコマンド実行の脆弱性を悪用した疑いのある通信を検知	723
5	WINDOWS Microsoft Windows SMB anonymous user request detected tcp 445	Windows のファイル共有サービス（SMB）の脆弱性を狙った攻撃の疑いのある通信を検知	365
6	SQL xp_reg* - registry access	プロテクトされたネットワークに外部から直接 SQL サーバーにアクセスする通信を検知	262
7	Brute Force Attack	同じ IP アドレスから短期間に複数の不正ログイン試行を検出	253
8	Cross Site Script attack	利用者が入力時に不正なスクリプトを挿入できる脆弱性をついて行われる攻撃を検知	246
9	HTTP Basic Auth Null Password Login attempt	Null パスワードによるログインができる脆弱性をついた攻撃を検知（バッファオーバーフロー/無認証ログイン）	220
10	JSIG-WEB phpMyAdmin-Code-Injection-1	Web アプリケーション phpMyAdmin に存在する脆弱性をつき、リモートから任意の PHP コードを注入したとみられる試みを検知	210
11	JSIG-WEB : Netgear-Setup-CGI-Cmd-Exec	Netgear 社製ルーターに存在するコマンド実行の脆弱性を狙った疑いのある通信を検知	167
12	WINDOWS Microsoft Windows SMB anonymous user request detected tcp 139	Windows ネットワークのファイル共有サービス（SMB）の脆弱性を狙った攻撃の疑いのある通信を検知	133
13	JSIG-SNMP : Systeminfo-Probe-Request	Cisco ASA の脆弱性に対する攻撃の疑いがある通信を検出	92
14	PHP-CGI Remote File Include Attempt	プログラミング言語 PHP を使用したプログラムに対する攻撃の疑いがある通信を検知	86
15	JSIG-WEB : GPON-Access	光通信規格のルーターの脆弱性を狙った攻撃の疑いのある通信を検知	76
16	dark nexus Netgear DGN1000 series routers arbitrary command execution attempt	Netgear 製ルーターDGN1000 シリーズの任意のコードを実行される脆弱性を狙った攻撃の疑いのある通信を検知	52

17	dark nexus Netgear DGN1000 series routers authentication bypass attempt	Netgear 製ルーターDGN1000 シリーズの任意のコードを実行される脆弱性を狙った攻撃の疑いのある通信を検知	50
18	JSIG-WEB : IIS-HTTP-Sys-Dos-4	Internet Information Services（IIS）においてHTTP プロトコルスタック（HTTP.sys）に存在する脆弱性（CVE-2015-1635、MS15-034）をついたリモートからの不正操作を検知	44
19	JSIG-WEB : MVPower-Shell-Access	MVPower DVR デバイスに存在するコマンド実行の脆弱性を狙った疑いのある通信を検出	38
20	TROJAN ZeroAccess Outbound UDP Traffic Detected	トロイの木馬による通信を検知	35
21	TROJAN Infostealer.Banprox	特定の Web サイト （通常は銀行） からネットワークトラフィックを悪質なプロキシにリダイレクトし、侵入先のコンピューターから機密情報を盗み取るトロイの木馬による通信を検知	30
22	Windows DNSAPI Remote code execution	Windows DNSAPI のリモートでコードが実行される脆弱性（CVE-2018-8225）を狙った攻撃の疑いのある通信を検知	23
23	JSIG-RAT GH0ST-Activity-1	マルウェア（Ghost rat）と疑わしい通信を検知	18
24	JSIG-RAT GH0ST-Activity-10	マルウェア（Ghost rat）と疑わしい通信を検知	18
25	HTTP Basic Auth Default Password Login attempt （admin） -2	サイトのベーシック認証においてログイン試行（総当たり攻撃）の対象にされている通信を検知	8
26	JSIG-WEB : Tomcat-PUT-JspFile-2	Apache Tomcat の脆弱性に対する攻撃の疑いがある通信を検知	7
27	JSIG-WEB MS-SQL-cmdshell-2	SQL Injection 攻撃を検知	6
28	HTTP Basic Auth Default Password Login attempt （root） -5	Web トラフィックの中に、Basic 認証（基本認証）を使い、不正アクセスを試みようとする疑いのあるコードを検知	4
29	JSIG-WEB Sql-Substr-Password-2	Webアプリケーションの脆弱性を悪用したSQLインジェクション攻撃を検出	2
30	WEB-CGI WhatsUpGold configuration access	Ipswitch の WhatsUp Gold の 8.03Hotfix 以前のバージョンで the_maincfgret.cgi スクリプトの中のオーバーフローを引き起こす攻撃を検知	2
31	TROJAN Netwire RAT Check-in	マルウェア Netwire に感染した疑いのある通信を検知	1

32	Adobe PDF With Embedded U3D Detected	Adobe Reader/Acrobat の U3D 処理の脆弱性（CVE-2011-2462）を狙った攻撃の疑いのある通信を検知	1
合計			**25,698**

表 6.2.2-12 検知一覧（IPS「外部からの攻撃」）

- No.1 と No.2 が「実証参加企業におけるサイバー攻撃の検知状況」で記載した外部からの攻撃で大きな山 2 つとなった攻撃である。
- No.1 の攻撃は、検証としては終了したが現在も攻撃されている可能性が高いと思われる。

No.	検知内容	説明	件数
1	Angler Exploit Kit CVE-2015-0311	脆弱性（CVE-2015-0311）がある Adobe Flash Player のバージョンの通信を検知	44
2	JSIG-SNMP : Systeminfo-Probe-Request	Cisco ASA の脆弱性に対する攻撃の疑いがある通信を検出	29
3	JSIG-WEB : Htaccess-File-Access	Web サーバーなどの htaccess ファイルの不正なアップロードや不正な書き換えを狙った疑いのある通信を検知	25
4	JSIG-WEB : IIS-HTTP-Sys-Dos-4	Internet Information Services（IIS）において HTTP プロトコルスタック（HTTP.sys）に存在する脆弱性（CVE-2015-1635、MS15-034）をついたリモートからの不正操作を検知	6
5	Windows NTP server DoS attempt	Windows サーバーにおいて NTP の 4.2.8p9 までの Ntpd を使用している場合に、サービス停止を狙った攻撃の疑いのある通信を検知	5
6	JSIG-WEB MWI-Activity-1	Microsoft Officeの脆弱性に対する攻撃の疑いがある通信を検知	3
7	TROJAN Netwire RAT Check-in	マルウェア Netwire に感染した疑いのある通信を検知	2
8	JSIG-RAT GH0ST-Activity-6	マルウェア（Ghost rat）と疑わしい通信を検知	2
9	JSIG-RAT GH0ST-Activity-9	マルウェア（Ghost rat）と疑わしい通信を検知	2
合計			**118**

表 6.2.2-13 検知一覧（IPS「内部からの不正通信」）

- 本実証では、エンドポイントに Type-Y を導入しており、Type-Y での検知が無かったため、特に実証参加企業への対応依頼はしていないが、ウイルス対策ソフト未導入の PC、またはサーバーからの通信の可能性もあり、ウイルス対策ソフトの全台導入と、導入済みのウイル

ス対策ソフトの定義（パターン）ファイルが最新であるか確認し、また従業員への最新定義ファイルへの更新意識を高める必要がある。

No.	検知内容	説明	件数
1	HTTP Basic Auth Null Password Login attempt	Null パスワードによるログインができる脆弱性をついた攻撃を検知（バッファオーバーフロー/無認証ログイン）	21
2	HTTP Basic Auth Default Password Login attempt（admin） -2	Web トラフィックの中に、Basic 認証（基本認証）を使い、不正アクセスを試みようとする疑いのあるコードを検知	3
3	HTTP Basic Auth Default Password Login attempt（admin） -3	Web トラフィックの中に、Basic 認証（基本認証）を使い、不正アクセスを試みようとする疑いのあるコードを検知	1
合計			**25**

表 6.2.2-14 検知一覧（内部の脆弱性）

- 脆弱なパスワードを使用した（デフォルトのパスワードを使用、短いパスワードを使用など）HTTP Basic 認証の通信を検知しており、「デフォルトのパスワードのまま使用しない」、「短い文字数や単純なパスワードは使用しない」など、従業員のセキュリティ意識を向上させる必要がある。

No.	検知内容	件数
1	eu.dspultra.com/api/submit_form_request	36
2	bbuseruploads.s3.amazonaws.com	17
3	images2.imgbox.com	8
4	p238000.infopicked.com/adServe/domainClick	3
5	apps.identrust.com/roots/dstrootcax3.p7c	2
合計		**66**

表 6.2.2-15 検知一覧（Web ガード）

- 検知の最も多かった企業へ確認したところ、動画サイトを見ていたとの報告があり、それが原因の可能性が高いが、業務に影響はなかったとのことであった。

6.2.3. リモートサポート対応結果

(1)　リモートサポート対応数

問合せ内容や傾向（メール・電話）は以下のとおりである。

項目	2020/09	2020/10	2020/11	2020/12	累計
メール	2	16	9	2	29
電話	1	23	19	11	54
計	**3**	**39**	**28**	**13**	**83**

表 6.2.3-1 メール、電話の問合せ件数（月別）

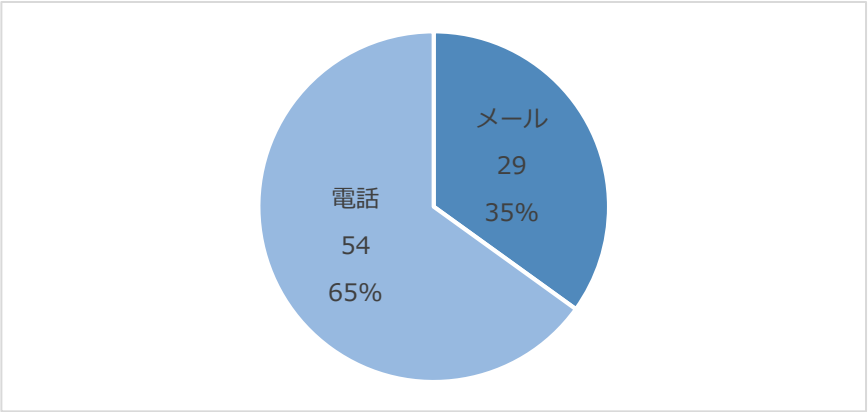


図 6.2.3-1 メール、電話の問合せ傾向（割合）

- 問合せに関しては 9 月 28 日（月）から 12 月 28 日（月）の平日 9 時から 17 時までという時間帯において、電話およびメールにて対応した結果としている。メールなどで時間帯外に連絡を受けた場合は、翌営業日受付を行った。
- 電話とメールとの割合は 6 割以上が電話での相談で、残り 3 割強がメールによる相談となった。電話による相談が多いものの営業時間内に問合せることが難しい企業や、NW 環境や OS インストールのバージョン確認など、口頭でのやり取りが難しいケースもあり、結果としてメールでの問合せも一定の割合を占めた。

サービス別に関する問合せは以下のとおりである。

項目	2020/09	2020/10	2020/11	2020/12	累計
Type-Y に関して	0	8	6	5	19
UTM に関して	3	31	22	8	64
計	**3**	**39**	**28**	**13**	**83**

表 6.2.3-2 Type-Y、UTM に関する月別問合せ件数

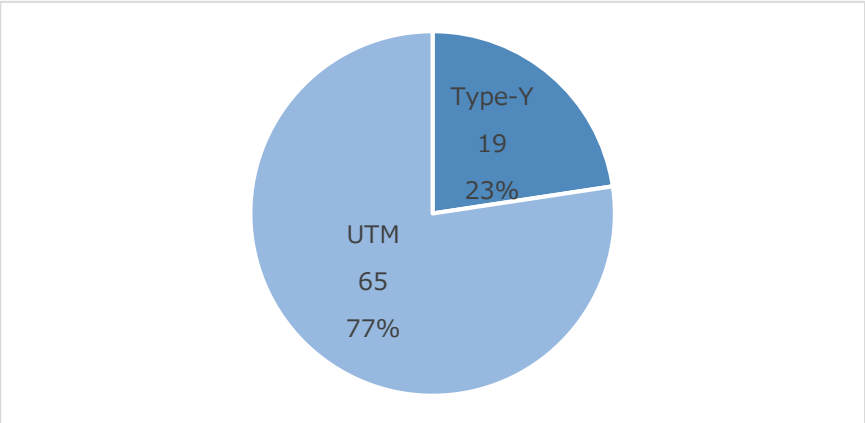


図 6.2.3-2 Type-Y、UTM に関する問い合わせ割合

今回、83 件受付のうち、UTM の問合せが全体の 8 割近い問合せがあった。また、問合せが多かったのが 10 月（39 件：47%）に集中した。

(2) リモートサポート対応数の内訳

Type-Y の月別の問合せは以下のとおりである。

	2020/09	2020/10	2020/11	2020/12	累計
製品関連	0	6	1	2	9
インストール関連	0	0	3	2	5
運用関連	0	2	1	1	4
撤去関連	0	0	0	0	0
その他	0	0	1	0	1
計	**0**	**8**	**6**	**5**	**19**

表 6.2.3-3 Type-Y に関する月別の問合せ内容

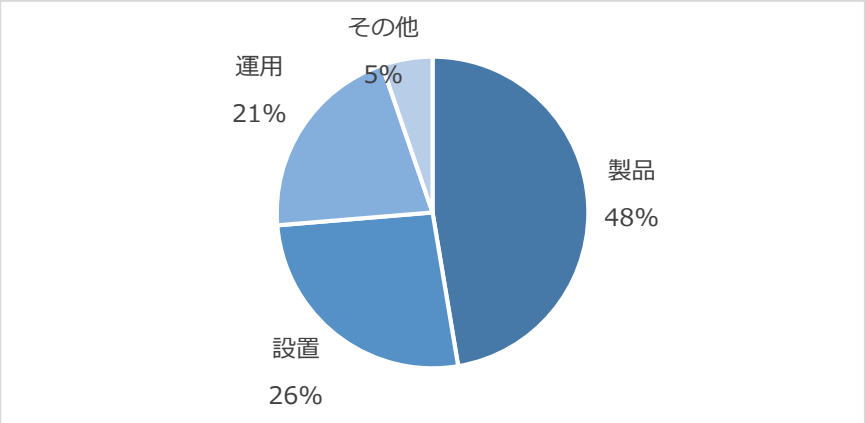


図 6.2.3-3 Type-Y に関する問合せ内容（割合）

カテゴリーとしては製品関連の問合せが半数近く、次にインストール関連、運用関連という順となっている。実証参加企業のうち 12.9%（7 社/54 社中）の問合せを受けた。主な問合せとしては、本製品インストール時にすでに実証参加企業にて導入しているウイルス対策ソフトの同居可能なのかなどの問合せが多かった。また、インストール関連の問合せに関しては、インストールマニュアルにない画面（ポップアップ）の問合せやインストール後にサービス停止中という問合せを受けるという内容であった。

UTM の月別の問合せは以下のとおりである。

	2020/09	2020/10	2020/11	2020/12	累計
製品関連	1	5	2	3	11
設置関連	1	17	15	3	36
運用関連	0	8	3	1	12
撤去関連	0	0	0	1	1
その他	1	1	2	0	4
計	**3**	**31**	**22**	**8**	**64**

表 6.2.3-4 UTM に関する月別の問合せ内容

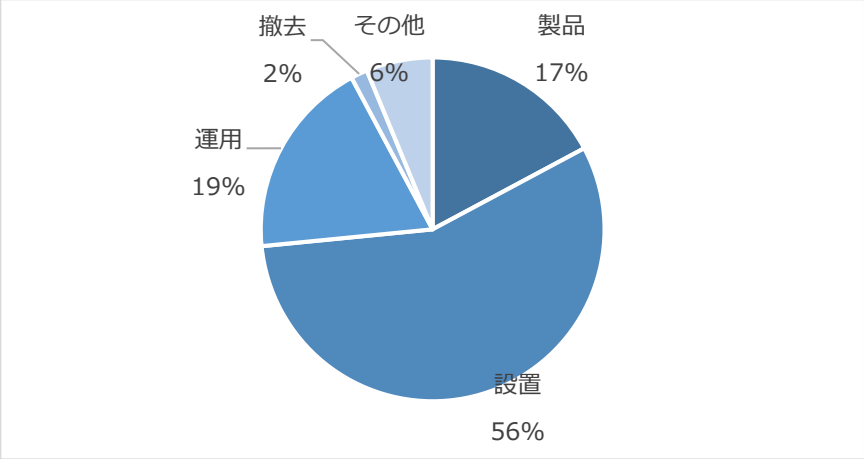


図 6.2.3-4 UTM に関しての問合せ（割合）

問合せ内容は設置関連の問合せが最も多く、全体の半分以上を占めている。また、実証参加企業のうち 24.5%（13 社/53 社中）から問合せを受けている。内容としては「アクティベーションができない」や「UTM の設置位置がよくわからない」などの相談を受けた。また「固定 IP の設定の仕方」や「すでに FW 製品があるがその際の設定方法」など、高度な質問を受けるケースもあった。運用後は「検知レポート」や「ランプに関して」などの質問があった。

その他の問合せとしては UTM 到着日時に関しての問合せが最も多かったが、問合せの中で、「インシデントが発生した際の対処方法」や「迷惑メール対策は本サービスで対処できるか」など一部の実証参加企業ではあるが、サイバー攻撃に対して実証参加企業が困っている内容に関しての質問も受けた。

(3) ケース 1 Type-Y インストール後にサービスが停止

Typy-Y インストール後において「サービスが停止中」という連絡を受けた。実証参加企業ヒアリングを行ったところ、実証参加企業側にプロキシサーバーが設置しておりそれが原因だと判明した。今回の実証の際に Type-Y のインストールプログラム配布時において、プロキシサーバーが実証参加企業環境にないという想定でソフトウェア配布を行ったため、今回の問合せがあったものと推察する。

(4) ケース 2 UTM 設置におけるアクティベーション

UTM 設置に関して、アクティベーションができないという問合せを受けた。センター側の環境も「オフライン」状態ということもあり、ヒアリングを継続したところ、実証参加企業環境下において、DHCP ではなく「固定 IP」での設定が必要ということが判明した。固定 IP アドレスの設定はマニュアルを送付していることもあり、その後実証参加企業にてマニュアルを見ながら作業を行うことで設置が無事に完了した。

(5)　ケース３　UTM 設置における既設ネットワーク機器との関係性

UTM 設置に関して、実証参加企業環境下にすでに FW を設置している実証参加企業から問合せを受けた。ヒアリングを行ったところ、FW の配下に今回 UTM を設置して運用したいという実証参加企業だったため、FW にホワイトリストの設定に必要な情報を提示し、実証参加企業にて設定を依頼して完了した。

6.2.4. 駆け付け対応結果

実証期間中、駆け付け対応は 1 件であった。

業務上必要なファイルが、同一ホストにて断続的に要注意検知が発生しており、正常性に問題がないか、ログの保全と調査を行った。検知内容は以下のとおりである。

検知日時	検知端末	検知企業	検知詳細
2020/11/24 09:53:00	検知端末 H	企業 401	静的解析による検知
2020/11/24 17:25:47	検知端末 H	企業 401	静的解析による検知
2020/12/07 18:22:03	検知端末 H	企業 401	静的解析による検知
2020/12/25 11:25:01	検知端末 H	企業 401	静的解析による検知

表 6.2.4-1 駆け付け対応を行った検知内容

現地にて取得した資料から、検知日時の前後で不審な動作がないか、レジストリやイベントログを確認した。また、ハッシュ値から本検知名のマルウェアは「アドウェア」に分類することが判明し、ユーザーが意図しない広告をポップアップなどで表示させる機能を有する可能性が高かった。しかし、広告表示以外の機能を有していないとの情報もあり、外部へのデータ送信やシステム破壊などの動作を行わない可能性が高い解析結果となった。

ユーザーにヒアリングした結果、今回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した。ダウンロード元サイトがどこであったかは記憶に残っておらず、正規の配布元以外から、アドウェアが同梱されたものをダウンロードしてしまった可能性も考えられる。

駆け付け対応についての概要は以下のとおりである。

駆け付け対応日	出動日時	作業開始日時	作業終了日時	退去日時	作業対応時間
2021/01/04	15:35	16:00	16:34	16:40	1.05H

表 6.2.4-2 駆け付け対応の概要

保全ツールを利用した現地での情報収集は 30 分程度であり、加入必須の簡易保険メニューに収まるコスト間で対応できた。

7. 報告会などによる事業成果の周知

7.1. 報告会開催概要

7.1.1. 報告会の内容

以下の概要で本実証事業の成果報告会を実施した。

開催方法は、現地開催 1 回（同時オンライン開催）とウェビナー形式のオンライン開催 1 回の計 2 回実施した。

なお、報告会では IPA 主催の「中小企業のための情報セキュリティセミナー」も合わせて実施した。

【報告会概要（約 90 分）】

- 地域実証事業の状況報告（40 分）
  - 本実証事業の実施内容の説明と実証成果の報告（質疑応答あり）
- 中小企業のための情報セキュリティセミナー（40 分）
  - 中小企業向け情報セキュリティ対策支援事業についての説明（IPA 主催）
  - 中小企業のための情報セキュリティセミナー（IPA 主催）
- アンケート回答および全体質疑応答（10 分）
  - 参加者への成果報告およびセキュリティセミナー開催後のアンケート実施

7.1.2. 参加募集方法

報告会への主な参加募集方法は以下のとおりである。

- 実証参加企業 54 社への個別募集活動（DM2 回配信＋個別連絡）
- 九州経済連合会の会員（約 900 社）に対する FAX 配信での案内
- 福岡県情報サービス産業協会の会員（178 社）に対する DM 配信
- 九州経済産業局主催コミュニティの参加企業など（約 4,000 社）への DM 配信

7.1.3. 報告会参加

報告会への参加企業数、参加者数は以下のとおりである。

開催日	参加企業数	（実証参加企業数）	参加者数	アンケート回答
2021/01/14　15:30~17:00 現地開催	1	1	1	1
2021/01/14　15:30~17:00 オンライン開催	28	12	35	27
2021/01/15　10:30~12:00 オンライン開催	12	5	20	11
合計	**41**	**18**	**56**	**39**

表 7.1.3-1 報告会の実績

なお、実証参加企業で報告会に参加できなかった企業に対しては、別途報告会資料を送付した。

7.1.4. アンケート概要

アンケートは、10 項目の質問から構成（表 7.1.4-1）され、それぞれの質問について択一形式で実証参加企業から回答を得た。その結果を今後のサービス商用化への取組みに活用することを目的とした。

質問	選択
貴社の所在地をお答えください	福岡県
	佐賀県
	熊本県
	長崎県
	大分県
	宮崎県
	鹿児島県
	九州以外
貴社の業種をお答えください	製造業、建設業、運輸業
	卸売業
	サービス業（ソフトウェア業または情報処理サービス業、旅館業を除く）
	小売業
	ゴム製品製造業（自動車または航空機用タイヤおよびチューブ製造業並びに工場用ベルト製造業を除く）
	ソフトウェア業または情報処理サービス業
	旅館業
	医療法人、社会福祉法人
	学校法人
	その他の業種（上記以外 財団法人、組合または連合会など）
貴社の社員数をお答えください	1～5 名
	6～10 名
	11～20 名
	21～30 名
	31～50 名
	51～70 名
	71～100 名
	101 名～
報告会に参加いただいたご自身のお立場をお答えください	経営層
	管理職

	一般従業員
	パート、アルバイト
	IT、セキュリティ担当
	その他
報告会の内容は今後サイバーセキュリティ対策を検討する上で有用でしたか	はい
	いいえ
	どちらともいえない
本サービスが商用化されたら利用を検討しますか	はい
	いいえ
	どちらともいえない
SECURITY ACTION に興味はありますか	興味がある
	興味はない
	今回、初めて知った
SECURITY ACTION を申し込む予定はありますか	すでに申し込み済み
	申し込みを今後検討する
	今後申し込む予定はない
「中小企業のための情報セキュリティセミナー」の理解度をお答えください	理解できた
	ほぼ理解できた
	理解できなかった
「中小企業のための情報セキュリティセミナー」の満足度をお答えください	有意義であった
	まあまあ有意義であった
	有意義ではなかった

表 7.1.4-1 アンケート項目

7.2. アンケート結果と今後のマーケティング活用法

7.2.1. アンケート結果

アンケート回答企業数 39 社のアンケート結果は以下のとおりである。

(1) 県別の参加企業数

県別の参加企業数は以下のとおりである。熊本（別事業者のお助け隊実証事業対象地域）と鹿児島（実証対象地域外）を除き県別中小企業数比に近い参加企業数で県別による特徴はなかったが、実証事業対象地域ではない九州以外からの参加が 3 社あった。

	福岡	佐賀	長崎	熊本	大分	宮崎	鹿児島	九州以外
参加企業数（割合）	21（54%）	2（5%）	7（18%）	1（2%）	2（5%）	3（8%）	-	3（8%）

表 7.2.1-1 県別の参加企業数

(2) 業種別参加企業数

業種別での参加企業数は以下のとおりである。参加活動を行っていない学校、医療法人を除いて多くの業種からの参加があった。その中でもセキュリティサービスを業務として取り扱うソフトウェア業・情報処理サービス業の参加企業が多く、九州以外の参加 3 社のうち 2 社はソフトウェア業であった。

内容	企業数		
	実証参加	不参加	計（割合）
製造業、建設業、運輸業	4	4	8（20.5%）
卸売業	1	0	1（2.6%）
サービス業（ソフトウェア業または情報処理サービス業、旅館業を除く）	2	4	6（15.4%）
小売業	4	0	4（10.3%）
ゴム製品製造業（自動車または航空機用タイヤおよびチューブ製造業並びに工場用ベルト製造業を除く）	-	-	-
ソフトウェア業または情報処理サービス業	5	6	11（28.2%）
旅館業	1	0	1（2.6%）
医療法人、社会福祉法人	-	-	-
学校法人	-	-	-
その他の業種（上記以外 財団法人、組合または連合会など）	1	7	8（20.5%）

表 7.2.1-2 業種別の参加企業数

(3) 規模別参加企業数

企業規模別での参加企業数は以下のとおりである。社員数 100 名以上の企業が半数以上あった。

	社員数							
	1~	6~	11~	21~	31~	51~	71~	101~
参加企業数（割合）	2（5%）	0	4（10%）	1（3%）	3（8%）	6（15%）	1（3%）	22（56%）

表 7.2.1-3 社員規模別参加企業数

(4) 参加者の役職

参加者の役職は以下のとおりである。参加者の 2/3 が企業のセキュリティを推進する立場の参加者であり、40%以上が経営者や管理職であった。

	経営者	管理職	一般従業員	パート、アルバイト	IT、セキュリティ担当	その他
参加企業数（割合）	4（10%）	13（33%）	12（31%）	0	9（23%）	1（3%）

表 7.2.1-4 県別参加企業数

(5) 実証事業の成果とサービス利用

成果報告会の有効性と商用のサービス利用については以下のとおりである。ほとんどの企業が報告会の内容は有用であると回答したが、この時点で商用化の利用の検討を行うと回答した企業は30%に留まり、60%以上の企業がどうするか決めかねている状況である。

なお、商用化利用の検討を行うと回答した 12 社のうち、IT、セキュリティ担当者が回答したのは 1 社だけであった。

質問	回答	企業数	
		実証参加	不参加
報告会の内容は今後サイバーセキュリティ対策を検討する上で有用でしたか	はい	17	18
	いいえ	0	0
	どちらともいえない	1	3
本サービスが商用化されたら利用を検討しますか	はい	7	5
	いいえ	1	1
	どちらともいえない	10	15

表 7.2.1-5 成果報告会と商用サービス利用について

(6) SECURITY ACTION

SECURITY ACTION に関する回答は以下のとおりである。ほとんどの企業が興味を持っており、すでに申し込んでいるおよび今後申込みを検討する企業が 70%以上であった。

質問	回答	企業数	
		実証参加	不参加
SECURITY ACTION に興味はありますか	興味がある	15	14
	興味はない	0	0
	今回、初めて知った	3	7
SECURITY ACTION を申込む予定はありますか	すでに申込み済み	3	1
	申込みを今後検討する	13	12
	今後申込む予定はない	2	8

表 7.2.1-6 SECURITY ACTION について

(7) 「中小企業のための情報セキュリティセミナー」

中小企業のための情報セキュリティセミナーに関する回答は以下のとおりである。セミナーの内容を理解できなかった企業はおらず、1 社を除いて満足度も高かった。

質問	回答	企業数	
		実証参加	不参加
「中小企業のための情報セキュリティセミナー」の理解度をお答えください	理解できた	8	12
	ほぼ理解できた	10	9
	理解できなかった	0	0
「中小企業のための情報セキュリティセミナー」の満足度をお答えください	有意義であった	10	13
	まあまあ有意義であった	8	7
	有意義ではなかった	0	1

表 7.2.1-7 情報セキュリティセミナーについて

7.2.2. 今後のマーケティング活用法

報告会アンケートの結果をもとに、今後のマーケティングに以下のように活用する。

(1)　パートナーとのアライアンス展開

実証参加企業にソフトウェア業、情報処理サービス業の企業が多く、九州以外からの参加もあったことから、今回の実証事業は利用する立場だけでなくセキュリティサービス提供を業務として取り扱う立場の企業にも関心が高いと考える。そこで、地域を限定せず全国のパートナー企業とアライアンスを組んで容易に提供できるサービス化を推進する。

(2)　経営、上位層へのアプローチ

企業の IT、セキュリティの担当者だけではサービス利用検討の可否を決めるのが難しい可能性も高いと考察されることから、できるかぎり経営者や上位層への直接のアプローチを行う。

(3)　個別アプローチの充実

ほとんどの実証参加企業が「報告会の有用性」「SECURTY ACTION の必要性」「中小企業のための情報セキュリティセミナーの満足感」を高く回答されていることから、セキュリティ対策の必要性も十分に感じていると考える。しかしながら、60%以上の企業が商用利用を迷っていることから、個別アプローチを充実させ、迷いの要因を解決し商用利用に繋げていく。

8. 地域向け支援体制構築を踏まえた考察

令和元年度に全国 8 地域で実施された「中小企業向けサイバーセキュリティ事後対応支援実証事業」から中小企業においても業種や規模を問わず例外なくサイバー攻撃を受けている状況が確認されるとともに、検知および防御のための対策や社内体制の構築ができていない企業が多いことが確認された。今後対策普及に向けた取り組みを推進させるポイントは以下 2 点である。[i]

- 地域特性や産業特性などを十分に考慮し、セキュリティ関連のみならず地域コミュニティを形成する様々な企業、機関、団体等との連携が有効。
- 実証サービスのビジネス化を促すため、事業主体などがコンソーシアムを形成するなど、今後のビジネス化に向けた必要な情報共有や検討を実施することができる仕組みの構築が有効。

8.1. 支援体制構築の留意点

- **支援サービスが、実証参加企業の発注元企業などにとって必要性が高いこと**

  本実証事業で対象とした九州地区でも中小企業マーケットでは、USB メモリの持ち込みや、端末機器の持ち込みなど、外部からの侵入がネットワークのみに依存しないことが多くみられることから、企業ネットワークの中に接続されるエンドポイント端末そのもののセキュリティ監視を行ったうえで、外部ネットワークとの接続の有無をネットワークセキュリティ監視と組み合わせて監視することが重要である。また、当事者となる地域中小企業各社もさることながら、サプライチェーンの上位に位置する大手企業は、末端の関連企業のセキュリティ運用管理を行いきれないことがわかっている。本実証事業では、発注元企業が管理できていないエンドポイントセキュリティを起点に、UTM（ネットワークセキュリティ）を組み合わせることで、サプライチェーンを構成する中小企業としてあるべきセキュリティの点から更に改善するための最善な手法を検証した。

- **自立的サービス展開を実現するうえでの、発注元企業・地域コミュニティとの連携**

  福岡県と、サプライチェーンを構成する関連九州エリア（福岡以外）で必要とされる中小企業向けエンドポイントセキュリティの展開の在り方についてエンドポイント端末を起点として検証した。各地域の経済団体（九州経済連合会）、業界団体（福岡情報サービス産業協会）、地域の発注元企業の地域コミュニティなどに協力を求め、説明会を共催するなどして募集・事業運営を行った。

[i] IPA：中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）の報告書について、https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html（2021/1/22　参照）

- **商用サービスが、内容・費用面で中小企業などの利用し易いものとなるような工夫**

  既存のエンドポイントセキュリティサービスとネットワークセキュリティサービスを組み合わせ、地域 SOC と、MSS（Managed Security Service）を組み合わせた効率的な運用プロセスを構築することで、利用する中小企業の運用負荷を低減するとともに利用価格低減を目指した。また、インシデント支援対応をリモートサポートと駆け付け作業に仕分けすることで、提供価格の更なる削減を図りつつ、駆け付け隊は、固定費でなく変動費で対応するスキームを検討することで売価転嫁を最小限にするなどの手段を模索した。

- **商用移行を踏まえ、実証参加企業に対し、契約などを行うことを想定した実証事業の推進**

  実証事業終了後は商用化にスムーズに移行できるようセキュリティサービスについては、実証と商用を同一のものとすることで、付け替えにかかる手間、コスト、セキュリティ対策の空白期間の発生に伴うリスク低減を図った。

- **取引先視点での優先順位や対策レベルを踏まえたサービス内容精査と導入負荷低減**

  地域ごと、業種ごとに実証参加企業のうち数社から取引先の紹介を受け、当該取引先企業に対してヒアリングを行い、中小企業などに求めるサイバーセキュリティ対策の優先順位や実施レベルなどの情報収集を行い、サービス内容の精査や機器・ソフトウェア・サービスの導入負荷の更なる低減の検討を行った。

8.2. 地域向け支援体制構築を踏まえたセキュリティ対策の検討

8.2.1. 中小企業向けのセキュリティ保険サービスの在り方、マーケティング方法

- **グローバルベースでのサイバーリスクについて**

  サイバーリスクは年々高まっており、世界経済フォーラムのレポート[i]では、「発生頻度」と「発生した場合の影響度」の 2 つの観点でサイバー攻撃にかかわるリスクが高いことが示されている。米国のサイバーセキュリティ企業サイバーセキュリティベンチャーズ社は、グローバルベースのサイバー犯罪被害額が 2021 年には 660 兆円（2015 年当時は約 330 兆円）に達する見込みであると発表した。[ii]

  上記より、グローバルベースでサイバーリスクに関する注目度が高まっており、サイバーリスクに備える動きが活発化していると考えられる。また、2020 年 6 月 24 日の国連の自動車基準調和フォーラム「WP29」でサイバーセキュリティとソフトウェアアップデートの国際基準が決定しており、自動車メーカーにサプライチェーン全体の管理が義務付けられるとともに、部品サプライ

[i] [The Global Risks Report 2020」
https://jp.weforum.org/reports/the-global-risks-report-2020（2021/1/22 参照）

[ii] サイバーセキュリティベンチャーズ：[Cybercrime To Cost The World $10.5 Trillion Annually By 2025」
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021（2021/1/22 参照）

ヤーにも連携が求められるようになっているなど、業界全体でサイバーリスク対策を強化する動きが見受けられる。

- **日本国内（特に九州エリア）におけるサイバーリスクについて**

  サイバーリスクの発生頻度や発生した場合の影響度が高まっており、強固な対策が求められるのは日本国内も同様である。世界的ビッグイベントである東京オリンピック、パラリンピックの開催に伴い、日本および海外所在の日系企業が、有数のハッカー集団からサイバー攻撃の標的とされる危険性が高まっていると考えられる。また、IoT 機器の急速な普及に伴いあらゆるモノがネットワークに繋がっていることから、サイバー攻撃が多様化、複雑化している実態が確認できる。日本国内のサイバーリスクを正確に認知し、適切な備えが重要である。3.1.2 にも記載のとおり、九州エリアは政令指定都市福岡市を中心に、政府や行政機関、金融、空港、鉄道、電力、ガス、電力、医療、物流、化学などの重要社会インフラが密に集結しており、これらの下請けや孫請けを担う中小企業は全九州エリアに広がっている。このことからも、同エリアでサイバー被害が増加すると考えられるため、サイバーセキュリティ保険を付保するなどの対策が必要である。

8.2.2. 中小企業向けセキュリティ対策サービスの内容、マーケティング手法、支援体制、提供の可能性

本実証事業の参加募集説明会にて実施したサイバーセキュリティに関するアンケート結果から、最低限のセキュリティ対策を実施していると回答した企業は 8 割以上で、ウイルス対策ソフトの導入が 9 割、ファイアウォールの導入が 7 割という結果であった。

一方で、セキュリティ簡易診断アセスメントの結果から、実証参加企業のセキュリティレベルは、全業種での平均値（表 4.2.3-2 セキュリティ簡易診断アセスメント項目）よりも低く、期待する水準に達していなかった。このことからセキュリティ対策のレベルに対する実証参加企業の認識に課題があることがわかった。

更に、アンケートの結果から、最低限のセキュリティ対策を実施しているにも関わらずサイバー攻撃の被害に遭った企業は 5 割以上あり、クリアインストールなどの対応を行ったことが判明した。実証結果からもインシデントが発生した社数はエンドポイント監視にて 26 社、ネットワーク監視にて 24 社であり、約 5 割の参加企業にてインシデントが発生した。

なお、インシデント発生時の対応を実証参加企業だけで実施できないケースが 4 割あり、実証参加企業でインシデント発生時の対応を実施できたケースにおいても、解決までに 2～3 日という長い期間を要した。

今回、エンドポイント監視にて 68 件、ネットワーク監視で 133 件のインシデントが発生したが、双方の関連性はなかった。

マルウェアの代表的な挙動として、エンドポイントでの不審な活動とともに C&C サーバーなどへの不正通信を発するものが多くあり、このケースはネットワーク監視のみで被害を食い止めることもできるが、エンドポイント側で何が起こっているのか把握できない。その結果、他の端末への感染拡大リスクが残る。本実証事業では、エンドポイント監視とネットワーク監視相互に関連が見られるようなインシデントの発生はなく、被害拡大を抑止する意味での効果は確認できなかった。しかし、被

害を最小限に留める意味で、速やかにインシデント発生を検知し、そのインシデントの状況をいち早く把握するための手段としては、本実証事業のような複合サービスが有効であると考える。

大半の中小企業で専任のシステム担当者がおらず、インシデント発生時の対応に時間を要している。本実証事業では、窓口への問合せ 83 件に対し、運用に関する問合せは 16 件と 2 割程度に留まり、駆け付け対応も 1 件であった。これは実証期間が短かったことが要因であると捉え、サービスの本質、継続利用モデルでのサービス形態から、運用（特にインシデント対応）に関する問合せや駆け付け対応への柔軟な支援体制の構築がサービスのコアであるという方針に変更を及ぼす結果ではないと判断した。商用化を検討するうえで、地域に依存しない相談窓口や駆け付け体制支援の枠組みが必要であると考える。

また、地域コミュニティからの募集により、成果報告会には本実証事業に参加していない企業からも多数参加があった。サービスの普及と中小企業のセキュリティ意識向上のため、今後もこの支援体制や SECURITY ACTION 制度を活用しつつ、啓発活動を継続していく。

9. 実証結果を踏まえた商用サービスの検討

9.1. セキュリティ簡易保険サービスの検討

サイバーリスクの危険性が高まる一方、本リスクへの対策優先度は高まっていない事実がある。つまりサイバーリスク保険付保に対して積極的な姿勢は一部に限定されており、その傾向は特に中小企業に強く見られる。そこでサイバーセキュリティお助け隊事業という枠組みを最大限に有効活用することで、中小企業が必要とする補償を遍く提供することを実現していきたい。補償内容はあくまでも中小企業にとって必要最低限の内容とし、万が一の際に必要不可欠な補償を提供する保険とする予定である。中小企業向けに簡易保険を提供することは STEP1 であり、段階的に保険の必要性を訴求していく過程で、STEP2 として簡易保険では対応できない本格的な対処（フォレンジックなど）や賠償責任リスクへの備えとして簡易保険の上乗せ・任意保険の導入を促すサイクルを実現したい。

今回の実証事業を通して、アラート検知時にシステムの自動通知および別途、サポートから連絡後に速やかに駆除が行われなかったケースがあった。これは実証参加企業に対して「緊急対応が必要」だと認識してもらうため、通知側の伝え方にも更なる改善が必要だと考える。また、速やかに駆除が行われない場合、時間の経過とともにインシデントが深刻化し、同時に事後調査（フォレンジック調査を含む）において原因究明に時間と費用を要してしまう可能性がある。本実証事業で実施した現地での保全作業では、事後調査に必要なログファイルの一部がすでに更新されていたことが判明した。インシデント通知後の事後調査に関しては、どのような対処が必要か判断するために事後調査に必要なログの保全が必要不可欠であると考える。そのため、自力で保全ができない中小企業に対して、駆け付けを行い保全する部分までを標準サービスに組み込む必要があり、駆け付けを行う部分については STEP1 のサービスに付保する簡易保険で提供し、必要となる本格的な対処については、STEP2 の任意保険での対応が考えられる。

9.2. セキュリティ対策サービスの検討

上述のとおり、本実証事業から九州圏における中小企業のセキュリティ対策レベルや、サイバー攻撃状況、インシデント発生状況、セキュリティニーズなどの実態把握を行うことができた。

エンドポイント監視サービス Type-Y やサイバーセキュリティ見守りサービスは、新規開発のサービスではなく、既設サービスであるが、これら既設サービスの組み合わせかつ、運用負荷や運用コスト低減のため、機能のスリム化により中小企業にとっての最適なセキュリティサービスを目指した。

これまで個々のサービスは、利用する際に利用者自身がログ検知後のインシデント判断などの専門知識が必要であったり、高額になったりするものが多く、中小企業で導入することが難しかった。しかし、本実証事業では実証参加企業が容易に利用できる新たな運用プロセスを追加することで、実証参加企業が SECURITY ACTION に準じたセキュリティ対策が実現可能であることを検証した。

また、今後のセキュリティ対策サービス設計のための基礎情報収集として、アンケートや簡易セキュリティ診断によるセキュリティレベル把握も行った。

更に、セキュリティインシデント発生時の対応方法の工夫と監視センター業務の役割見直し（地域監視事業者と MSS の分割）を行うことで検証後商用展開時にコスト低減が見込めることを実証した。

これらの観点で実証を行った結果、以下の課題が明らかとなり、今後商用サービス提供にあたって対策検討を継続することとした。

- 実証で明らかになった課題
  - 九州地域のセキュリティ意識や対策レベルが全国と比較して低い
    技術面、運用面、物理面の各カテゴリーにおいて求められるレベルに達しておらず、全業種平均と比較しても、すべてのカテゴリーにおいて劣る結果であった。

  - セキュリティサービス導入に手間取った
    エンドポイント監視サービス Type-Y については配布ライセンス総数（1,180 ID）に対し、実インストール数は 60%に留まった。
    UTM については配布数に対する導入比率は高いものの、UTM 到着から導入完了までの日数が長くかかっており、自力での導入ができなかった企業も多くあった。

  - より安価で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
    想定するサービス費用と実証参加企業が考える費用感との格差が明らかになっており、サービス商用化においては更なる価格低減を行う必要がある。
    なお、アンケートではエンドポイント監視サービス Type-Y は月額 440 円以下（回答 27 社平均）、サイバーセキュリティ見守りサービス（UTM）は月額 5,330 円以下（回答 18 社平均）との回答を得た。

9.3. 実証終了後の商用サービス提供の可能性

本実証事業の結果から、今回提供したセキュリティサービスにより多くのマルウェア検知や不正通信遮断を確認でき、サービス導入による一定の効果が認められた。しかしながら、前節で述べたように、複数の課題が残っている。特にサービス導入時の容易性については、改善の必要性が高い。

サービス導入時に自力で導入設置を行えない場合、技術者によるオンサイト導入支援作業が発生し、結果的にサービスコスト増加に繋がる。このため、マニュアルの改善や導入プロセス（機能）面の改善に加え、コールセンターによるリモート対応方法改善を継続検討する。

これらの課題を除けば商用サービス提供の可能性は十分にあり、エンドポイントとネットワークの両面をカバーした安価かつ簡便な中小企業向けサイバーセキュリティ対策サービスを提供できると考える。

本実証事業のアンケート結果から、自社での保有端末・サーバー台数が 10 台以下の企業が全体の 23%、年間のサイバー対策経費が 20 万以下の企業が全体の 18%存在する結果が得られており、サービスを広く普及させるうえで、これらの指標は商用化に向けたメニュー作りの題材として重要であると考える。

2021 年 4 月からの商用サービスは、下記メニュー構成を想定し、将来的に地域を限定せず全国のパートナー企業とアライアンスを組んで提供できるサービス化を目指す。

メニュー内容（案）

- エンドポイント監視サービス Type-Y 5ID
- サイバーセキュリティ見守りサービス UTM 1 台
- 運用監視、相談窓口
- 駆け付け対応（保険との組み合わせを検討）

提供価格（案）

- 月額 1 万円程度　（初期費用は別途）

以上