|  |
| --- |
| 東京都　産業労働局 御中 |

東京都中小企業サイバーセキュリティ  
向上支援事業運営業務委託

実施報告書

2021年3月31日

東日本電信電話株式会社

目次

[1. サイバーセキュリティ対策の現状について 1](#_Toc67933469)

[1.1 **サイバー攻撃の現状、サイバーセキュリティ脅威のトレンド・動向** 1](#_Toc67933470)

[1.2 **企業におけるサイバーセキュリティ対策状況** 5](#_Toc67933471)

[2. 本事業の支援内容と支援対象企業 7](#_Toc67933472)

[2.1 **本事業のスケジュール** 7](#_Toc67933473)

[2.2 **本事業の支援業務概要** 7](#_Toc67933474)

[2.3 **支援対象企業の募集（セミナーによる普及啓発活動）** 10](#_Toc67933475)

[2.4 **支援対象企業の属性** 12](#_Toc67933476)

[3. 支援開始時の東京都内における中小企業のセキュリティ対策の現状 14](#_Toc67933477)

[3.1 **中小企業の実態（人的対策と技術的対策）** 14](#_Toc67933478)

[3.2 **サイバーセキュリティ対策の障壁把握** 42](#_Toc67933479)

[4. 支援期間中のサイバーセキュリティ脅威の状況と対策支援状況 43](#_Toc67933480)

[4.1 **UTMのログから見える脅威のアタックとブロック状況** 43](#_Toc67933481)

[4.2 **標的型攻撃メール訓練開封率（支援期間中2回の比較）** 50](#_Toc67933482)

[4.3 **テレワーク実施企業のクラウドアプリセキュリティ診断** 53](#_Toc67933483)

[4.4 **セキュリティサポートデスクへの問い合わせ内容** 55](#_Toc67933484)

[4.5 **全体的なサイバーセキュリティ上のトピックス** 56](#_Toc67933485)

[5. 支援後の中小企業の意識の変化と実態把握 57](#_Toc67933486)

[5.1 **支援終了時のアンケート結果** 57](#_Toc67933487)

[5.2 **支援終了時の個社ヒアリングの結果** 72](#_Toc67933488)

[6. まとめ・提言 83](#_Toc67933489)

[6.1 **企業におけるサイバーセキュリティ対策のあるべき姿** 83](#_Toc67933490)

[6.2 **新たなサービス・支援事業等に関する提言** 83](#_Toc67933491)

# **サイバーセキュリティ対策の現状について**

## **サイバー攻撃の現状、サイバーセキュリティ脅威のトレンド・動向**

昨今、中小企業を含む取引先や海外展開を進める企業の海外拠点、更には新型コロナウイルスの感染拡大に伴うテレワークの増加に起因する隙など、攻撃者が利用するサプライチェーン上の「攻撃起点」が拡大している。この状況を踏まえ、経済産業省は、2020年12月18日にサイバーセキュリティの取組の強化に関してウェブサイトで注意喚起[[1]](#footnote-1)を行った。その中で経済産業省は、「最近の攻撃の特徴と目的を明らかにし、企業やその関係機関等が対応する際に注意すべき点を整理することで、企業の経営者の方々に対し、サイバーセキュリティの取組について一層の強化を促す」としている。通達の中で経済産業省は、以下の3点をサイバー攻撃の現状として注意喚起している。

（１）中小企業を巻き込んだサプライチェーン上での攻撃パターンの急激な拡がり

昨今、中小企業を含む取引先や海外展開を進める企業の海外拠点、更には新型コロナウイルスの感染拡大に伴うテレワークの増加に起因する隙など、攻撃者が利用するサプライチェーン上の「攻撃起点」がますます拡大している。

（２）大企業・中小企業等を問わないランサムウェアによる被害の急増

暗号化したデータを復旧するための身代金の要求に加えて、暗号化する前にあらかじめデータを窃取しておき、身代金を支払わなければデータを公開するなどと脅迫する、いわゆる「二重の脅迫」を行うランサムウェアの被害が国内でも急増しつつある。背景には、攻撃者の側でランサムウェアの提供や身代金の回収を組織的に行うエコシステムが成立し、高度な技術を持たなくても簡単に攻撃を行えるようになっていることがある。

（３）機微性の高い情報の窃取等を目的としたと考えられる海外拠点を経由した攻撃

ビジネスのグローバル化に伴い海外拠点と密に連携したシステム構築が進む一方で、十分な対策を採らないまま海外と日本国内のシステムをつなげてしまった結果、セキュリティ対策が不十分な海外拠点で侵入経路を構築され、国内に侵入されるリスクが増大している。

　経済産業省からの注意喚起は、中小企業に対するサイバーセキュリティ対策を強く促すものとなっている。このことから、サイバーセキュリティの脅威は社会インフラや大企業だけではなく、中小企業にも影響を及ぼし始めていることがうかがえる。

　また、経済産業省が現在の被害状況から注意喚起している主なサイバー攻撃もあわせて紹介[[2]](#footnote-2)する。

（１）Emotet（エモテット）

＜Emotetとは＞

Emotetと呼ばれるウイルスへの感染を誘導する高度化した攻撃メールが国内外の組織へ広く着信。

実在の相手の氏名、メールアドレス、メールの内容等の一部を流用して正規のメールへの返信を装っていたり、業務上開封してしまいそうな巧妙な文面となっている場合があり、注意が必要。

＜最近の傾向＞

2020年7月末から国内外に向けてEmotetに感染させるメールの配信活動が再び活発化。過去に感染した被害組織から窃取された情報を使ってなりすまされたメールが配信されている状況。

Emotetは、情報の窃取等の直接攻撃に悪用されることに加え、他のウイルス等による攻撃の侵入口として悪用されるウイルスでもあり、一度感染すると拡散していく傾向。

（２）ネットワーク貫通型：VPN機器の脆弱性を悪用したネットワークへの侵入

VPN機器の脆弱性が相次いで報告され、そうした脆弱性を悪用するコードが公開されるなど深刻な状況が発生。

攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入し、攻撃を展開。2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、国内外900以上の事業者からVPNの認証情報が流出。2020年11月、Fortinet製品のVPN機能の脆弱性の影響を受ける約5万台の機器に関する情報が公開。認証情報等が悪用されることで容易に侵入されるおそれ。

どちらのケースも既に悪用されている可能性があるため、機器のアップデートや多要素認証の導入といった事前対策に加え、事後的措置として侵害有無の確認や、パスワード変更等の対応が必要。

（３）ランサムウェア（Ransomware）とその手口の変化（二重の脅迫）

＜ランサムウェアとは＞

「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。

感染したパソコンのデータを暗号化するなど使用不可能にし、その解除と引き換えに金銭を要求する。

＜新たな（標的型）ランサムウェア攻撃（二重の脅迫）とは＞

ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫をするサイバー攻撃。

システムの復旧に対する金銭要求に加えて、窃取したデータを公開しない見返りの金銭要求も行うので、二重の脅迫と恐れられる。窃取された情報に顧客の情報や機微情報を含む可能性がある場合には、被害組織はより困難な判断を迫られることになる。

（４）海外拠点経由の攻撃

ビジネスのグローバル化に伴って、海外拠点とのネットワークを国際VPN等によりWAN（広域社内ネットワーク）に取り込んで構築しているケースが増加。海外とのビジネス効率化に寄与する一方で、海外拠点への不正侵入によって、即国内ネットワークまで侵入される危険も伴っている。

海外拠点（海外支社の他、関連会社、提携先、取引先等を含む）においては様々な原因により、日本国内と同等なレベルのセキュリティ対策が十分に取れないケースが多い。

* 安価だが品質管理が不十分なソフトウェアが利用されている（コピー版等の利用により最新の脆弱性管理が適用されない）
* 本社のガバナンスが行き届かず、システムの脆弱性が放置され、インシデントの監視・対応体制も十分に確保できていない
* 従業員教育が十分でなく、私用機器やソフトウェアなどが許可なくシステムに接続されている
* 信頼性の低いプロバイダを利用せざるを得ない　等

このような国内環境よりも脆弱な海外拠点において不正侵入を許してしまい、そこを足掛かりに、国内システムの奥深くまで到達されるケースが増加。

一般企業をとりまくサイバー攻撃の脅威について、より具体的に見ていく。独立行政法人情報処理推進機構（以下、IPA）では、「情報セキュリティ10大脅威2021」を公表[[3]](#footnote-3)している。

表 1‑1　情報セキュリティ10大脅威　2021　（組織）

|  |  |
| --- | --- |
| 順位 | 組織向け脅威 |
| 1位 | ランサムウェアによる被害 |
| 2位 | 標的型攻撃による機密情報の窃取 |
| 3位 | テレワーク等のニューノーマルな働き方を狙った攻撃 |
| 4位 | サプライチェーンの弱点を悪用した攻撃 |
| 5位 | ビジネスメール詐欺による金銭被害 |
| 6位 | 内部不正による情報漏えい |
| 7位 | 予期せぬIT基盤の障害に伴う業務停止 |
| 8位 | インターネット上のサービスへの不正ログイン |
| 9位 | 不注意による情報漏えい等の被害 |
| 10位 | 脆弱性対策情報の公開に伴う悪用増加 |

IPAは、あわせて以下のように提唱している。[[4]](#footnote-4)

* 「10大脅威」の順位は毎回変動するが、基本的な対策の重要性は長年変わらない。（表1-2）

表 1‑2　情報セキュリティ対策の基本

|  |  |  |
| --- | --- | --- |
| 攻撃の糸口 | 情報セキュリティ対策の基本 | 目的 |
| ソフトウェアの脆弱性 | ソフトウェアの更新 | 脆弱性を解消し攻撃によるリスクを低減する |
| ウイルス感染 | セキュリティソフトの利用 | 攻撃をブロックする |
| パスワード窃取 | パスワード管理・認証の強化 | パスワード窃取によるリスクを低減する |
| 設定不備 | 設定の見直し | 誤った設定を攻撃に利用されないようにする |
| 誘導（罠にはめる） | 脅威・手口を知る | 手口から重要視するべき対策を理解する |

* 脅威に備えるためには攻撃手口や動向、及び自組織が抱える要因等を把握することが重要。
* 「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしない。組織ごとの状況を考慮して対策の優先度を決定する。

中小企業は、このような脅威・手口について理解し、自社に必要な対策とは何かを理解し、サイバーセキュリティ対策の予防的措置として、徹底した対策を採ることが重要である。サイバー攻撃の対象は、脆弱性が比較的高くなるリモートワーク、海外に触手を伸ばしており、日本の中小企業も標的となる可能性が十分にある。事業規模にかかわらず、十分な対策をしておかなければ、大きな損失を被りかねない状況であることを認識し、対策に努めなければならない。

## **企業におけるサイバーセキュリティ対策状況**

経済産業省は、「1.1　サイバー攻撃の現状、サイバーセキュリティ脅威のトレンド・動向」で紹介した注意喚起の中で、経営者に対して以下を提言[[5]](#footnote-5)している。

1. サイバー攻撃による被害が深刻化し、被害内容も複雑になっており、経営者の一層の関与が必要となる。
2. ランサムウェア攻撃によって発生した被害への対応は企業の信頼に直接かかわる重要な問題であり、その事前対策から事後対応まで、経営者のリーダーシップが求められる。
3. サイバーセキュリティを踏まえた事業のグローバル・ガバナンス構築の必要がある。
4. 改めて「基本行動指針（共有・報告・公表）」に基づいた活動を徹底して欲しい。

つまり、経営者が危機意識を持ち、率先して社内だけでなく、事業領域全体におけるサイバーセキュリティ対策への取組が必要ということである。

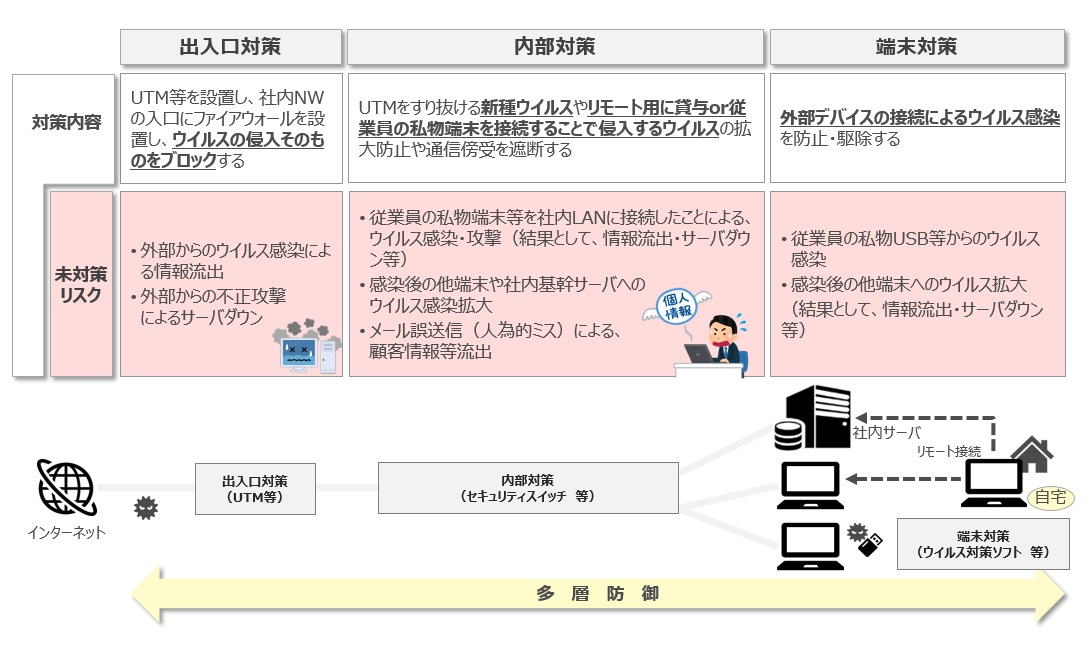
それでは、中小企業の経営者はどのような対応を取るべきか、サイバー攻撃の特性から考える必要がある。サイバー攻撃は、その種類によりセキュリティ対策の方法が異なる。単一の攻撃を防ぐだけでは情報セキュリティを担保することはできない。様々な攻撃から防御するためには、多層防御を前提に複合的に行う必要がある。

企業の働き方が変わり、リモートワークが定着すると、利用する端末や外部デバイス等の管理が困難になる。接続端末の登録や外部への情報流出防止等、既知のウイルスだけでなく未知のウイルスにも攻撃されることを前提とした出入口対策・内部対策・端末対策が重要である。

また、そのような予防措置、事後措置だけでは不十分であり、従業員の不注意を利用した攻撃から企業を守るためにも従業員のセキュリティ意識向上も重要な対策となる。

従業員のセキュリティ意識向上にあたっては、セキュリティ対策を怠った場合の経営リスクまで踏み込んで、サイバーセキュリティ対策の重要性を認識させることが効果的であると考えられる。

図 1‑1　（参考）多層防御イメージ図



以上のように、中小企業がサイバー攻撃の脅威から身を守りつつ、デジタル化による恩恵を享受するためには、中小企業が自社のセキュリティの実態に目を向け、必要な対策を講じることが重要である。しかしながら、多くの中小企業は、その知識や経営資源を有していない状況にある。

中小企業サイバーセキュリティ向上支援事業（以下、本事業）は、こうした中小企業のサイバー攻撃の実態把握やインシデントへの対応支援を行い、自立的なサイバーセキュリティ対策の後押しをすると共に、これらの取組を広く紹介することで、中小企業のサイバーセキュリティ対策に対する意識の向上を図っていくものである。

# **本事業の支援内容と支援対象企業**

## **本事業のスケジュール**

本事業に係る全体スケジュールは表2-1のとおり。2021年11月以降、支援対象企業の募集やサイバーセキュリティ対策に関する普及啓発・実態把握を行った。

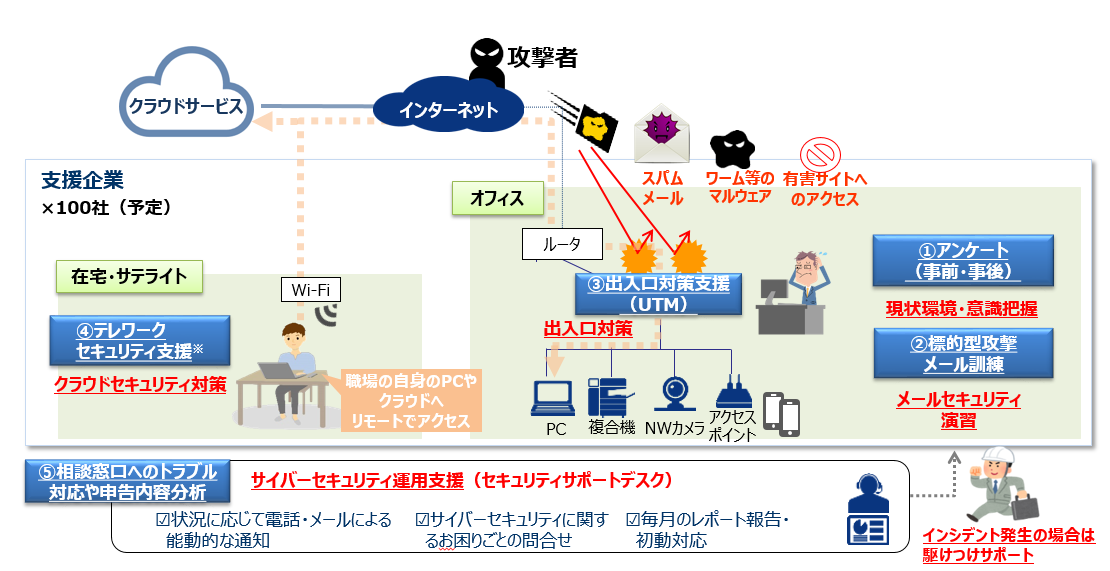
表 2‑1　本事業の全体スケジュール

|  |  |
| --- | --- |
| 時期 | 主な業務内容 |
| 契約確定の日の翌日～令和２年11月30日 | 事業の企画等業務 |
| 令和２年11月～12月 | 支援対象企業募集、決定 |
| 令和２年11月～令和３年２月 | サイバーセキュリティ対策支援業務 |
| 令和３年２月～令和３年３月 | 実施結果のとりまとめ及び分析  事後対応業務 |

## **本事業の支援業務概要**

本事業において、実施した支援業務の概要を以下に記載する。

図 2‑1　支援業務全体像



1. セキュリティ実態把握

中小企業へのサイバー攻撃の実態把握に向けて、NTT東日本として提供実績のあるサイバーセキュリティ対策サービスを主要ツールとして、「出入口対策」「標的型攻撃メール訓練演習」「一元受付サポートデスク」「現地駆けつけ」を円滑に実現し、サイバー攻撃や企業のセキュリティ意識の実態を把握。

また、アンケートについては、中小企業の実態把握だけでなく、今後の事業構築・改善に向けた観点で集客時（事前）と、事業終了時（事後）の2回実施することで、中小企業の現状の対策状況に加え、意識の変化など実態把握に活用する。

セキュリティ実態把握の具体的な手段は表2-2のとおり。

表 2‑2　セキュリティ実態把握の具体的な手段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 実態把握の手段 | 狙い・目的 | 対象 | 得られる情報 |
| 1 | アンケートの実施（事前・事後の2回） | * 事業開始前・開始後に2回のアンケートを実施することで本事業による意識の変化や効果を把握する | 全社 | 事業を通した意識の変化・環境の実態 |
| 2 | 標的型攻撃メール訓練 | * 疑似メールを企業の代表社員に送信し、開封状況や開封した人の傾向の実態を把握する * 支援期間中に2回実施することで、演習によるセキュリティ意識の醸成を図り開封要因などの実態を把握する | 全社 | 疑似メール開封結果と開封者の傾向等（定量・定性） |
| 3 | UTM設置による出入口対策支援 | * 支援企業にUTMを設置し、不正アクセス等通信監視・ログ取得により実際のアタック状況を把握する * サイバーセキュリティ対策運用について中小企業が実施せずに対策をおまかせできる環境を提供する | 全社 | 支援企業全体・個社毎のUTMアタックログ（攻撃状況） |
| 4 | テレワーク実施者向けセキュリティ対策 | * テレワーク実施時のクラウドサービス・領域に対する状況を把握する * テレワーク接続環境におけるセキュリティ対策支援を実施する | 該当企業選定 | クラウドサービス（条件有）に対する攻撃ログ |
| 5 | 相談窓口への 問合せ内容分析 | * 支援企業からどのような問合せや相談が来ること多いのかニーズやお困りごとについて把握する | 全社 | 問合せや申告に関する件数・内容・頻度等 |

1. インシデント対応

支援企業からの相談･問い合わせに対しては、一元窓口（セキュリティサポートデスク）を設け、各種お困りごとやインシデント判断・遠隔駆除を実施。（受付時間：24時間365日）また、現地駆けつけが必要な場合には都内の各拠点から対応。（駆けつけ対応時間：9:00～17:00）

なお、本事業における支援期間において、支援対象企業にインシデントは発生していないため、現地駆け付けの実績はない。詳細は、4.4に記す。

1. 相談等の受付及び対応業務

インシデント発生時以外にも「セキュリティサポートデスク」にてセキュリティに関する相談・問合せを一元的に受け付け、対応を実施。（受付時間：24時間365日）相談内容の詳細は表2-3のとおり。

表 2‑3　セキュリティサポートデスクでの問い合わせ内容

|  |  |
| --- | --- |
| 問い合わせ項目 | 具体的な問い合わせ内容 |
| サイバーセキュリティ全般に関する問合せ | ・セキュリティトレンド情報や用語・必要な対策方法等の相談  例：Emotetとは何か、どんなリスクがあるのか  ・USBなど利用における注意事項などの相談対応  例：USBを社内で使う際にサイバーセキュリティの観点で気を付けるべきことは何か |
| UTMログレポートに関する問合せ | ・アタック状況やUTMの通信ログに関するフィードバック・相談  例：アタック状況や不正通信の状況など検知した攻撃の解説をしてほしい、UTMログレポートの見方を知りたい |
| UTMの設置・設定に関する問合せ | UTMの設置・設定に関する相談  例：社内で特定ジャンルのWebサイトの閲覧を制限したい（フィルタリング）  例：UTM導入後、インターネットがつながらないことがある（ネットワーク接続確認）  例：特定メールアドレス以外を完全に受信しないようにしたい（ホワイトリスト） |
| 脅威に関する問合せ | ・ウイルス感染の疑いに関する相談  例：ウイルスに感染したかもしれないので状況を確認してほしい |

1. ヒアリングの実施

ヒアリングについてはアンケート結果を踏まえたサイバーセキュリティ意識の高低や支援事業から得た情報、企業属性を鑑み、5社選定し実施。ヒアリング内容についてはアンケート調査をベースに深堀を行った。

1. 支援終了後の継続支援

事業終了後においては、地域主体・各団体と引き続き連携し、中小企業のサイバーセキュリティ対策の意識啓発を実施。

支援終了後、支援対象企業が支援内容の継続希望される場合には事前対策支援をはじめ、個社ごとに必要なサイバーセキュリティ対策全般の支援をコンサルティングから構築・運用支援まで継続的な取組を行う。

## **支援対象企業の募集（セミナーによる普及啓発活動）**

以下の方法により参加企業を募った。最終的に101社の中小企業に本事業に参加いただいた。内、実態把握に加えて「出入口対策」等の支援を実施したのは99社。

募集方法に関する詳細内容は以下のとおり。

1. 説明会（セキュリティセミナー）による案内

本事業の支援対象企業募集に関する周知だけでなく、参加企業のサイバーセキュリティ対策に関する意識向上を目的に、有識者による講演やサイバーセキュリティ関連事業の紹介などを行う「サイバーセキュリティセミナー」を開催した。

＜開催日＞　令和2年12月8日（火）15：00-16：30

＜開催形式＞　オンライン形式

＜セミナー参加企業数＞　15社

＜説明会コンテンツ＞

|  |  |  |  |
| --- | --- | --- | --- |
|  | **所用時間** | **プログラム** | **講話者** |
| **第一部** | 50分 | 広がるテレワーク環境と セキュリティ対策のポイント | トレンドマイクロ株式会社 |
| **第二部** | 20分 | サイバーセキュリティ対策関連施策紹介 | 独立行政法人情報処理 推進機構 |
| **第三部** | 10分 | 事業概要説明（セキュリティ対策事業） | 東日本電信電話株式会社 |
| **質疑応答** | 5分 | Q&Aタイム | － |

＜説明会への集客方法＞

* 東京都HPへの掲載・周知
* NTT東日本の営業担当者からの周知

＜セミナー参加企業アンケート結果＞

セミナー参加企業には、セミナーコンテンツや本事業、企業のセキュリティに係る現状に関してアンケート調査を行った。

（１）アンケート回答企業数

セミナー参加企業15社のうち、7社から回答があった。

（２）個別回答結果

個別回答結果の内容は以下の通り。

* 本セミナーを知ったきっかけは、「東京都のホームページから」が一番多い。
* 本セミナーについて「大変良かった」「良かった」と回答した企業が5社、良くも悪くもないと回答した企業が2社。
* プログラムで最も印象に残った内容は、トレンドマイクロ株式会社が講演をした『広がるテレワーク環境とセキュリティ対策の強化』だった。また、その理由として「知らず知らずのうちにメールを開封したり、ダウンロードしてしまう危険が常にあり、心配になった。」等、中小企業への意識啓発につながったと思われる。
* 本セミナーを受けて、セキュリティ対策の意識に変化があったと回答した企業が5社、「特に意識の変化はなかった」と回答した企業が2社。
* 本セミナー参加者は、5社がテレワーク導入済み、2社が導入を検討している。
* セキュリティ対策に関して、相談したいことは、各社傾向にばらつきがある。
* アンケート回答者全員が東京都中小企業サイバーセキュリティ向上支援事業に興味があると回答。

1. NTT東日本の営業担当者による案内

東京都内の日頃からリレーションのある中小企業のお客様に対して、NTT東日本の営業担当社員が直接コンサルティング等を実施しながら本事業の周知を行った。

## **支援対象企業の属性**

アンケートに回答していただいた企業101社の業種や従業員数別の分布は以下の通り。

表 2‑4　業種別にみた企業数

|  |  |
| --- | --- |
| 業種 | 回答企業数（社） |
| 卸売業、小売業 | 30 |
| 製造業 | 13 |
| サービス業 | 13 |
| 情報通信業 | 7 |
| 不動産業、物品賃貸業 | 7 |
| 医療、福祉 | 7 |
| 建設業 | 6 |
| 宿泊業、飲食店 | 5 |
| その他 | 5 |
| 運輸業、郵便業 | 4 |
| 生活関連サービス業、娯楽業 | 3 |
| 金融業、保険業 | 1 |
| 学術研究、専門・技術サービス業 | 1 |
| 計 | 103[[6]](#footnote-6) |

表 2‑5　従業員数別にみた企業数

|  |  |
| --- | --- |
| 従業員数 | 回答企業数（社） |
| ～20名 | 57 |
| 21名～100名 | 24 |
| 101名～ | 20 |
| 計 | 101 |

表 2‑6 従業員数別、業種数

|  |  |  |  |
| --- | --- | --- | --- |
| 業種 | 企業規模 | | |
| ～20名 | 21～100名 | 101名～ |
| 卸売業、小売業 | 15 | 8 | 7 |
| 製造業 | 6 | 4 | 3 |
| サービス業 | 10 | 1 | 2 |
| 情報通信業 | 7 | 0 | 0 |
| 不動産業、物品賃貸業 | 6 | 0 | 1 |
| 医療、福祉 | 3 | 4 | 0 |
| 建設業 | 3 | 1 | 2 |
| 宿泊業、飲食店 | 1 | 0 | 4 |
| その他 | 0 | 3 | 2 |
| 運輸業、郵便業 | 2 | 1 | 1 |
| 生活関連サービス業、娯楽業 | 1 | 1 | 1 |
| 金融業、保険業 | 0 | 1 | 0 |
| 学術研究、専門・技術サービス業 | 1 | 0 | 0 |
| 教育学習信楽 | 1 | 0 | 0 |
| 計 | 56 | 24 | 23 |

# **支援開始時の東京都内における中小企業のセキュリティ対策の現状**

## **中小企業の実態（人的対策と技術的対策）**

2020年12月から、東京都における中小企業のセキュリティ対策の調査を行うにあたり、各企業のセキュリティの現状を把握すべく、アンケート調査を行った。

（１）アンケート内容

＜対象者＞　説明会参加企業・本事業参加企業

＜回答数＞　101社

＜支援開始時アンケート内容＞

|  |  |
| --- | --- |
| Q1. サイバーセキュリティ対策に関心をお持ちですか | |
| 1. | すぐにでも、検討しようと思った |
| 2. | とても関心があり、いずれ検討しようと思った |
| 3. | 関心はあるが、検討するかは分からない |
| 4. | 関心はない |

|  |  |
| --- | --- |
| Q２. ご存知のセキュリティ脅威がございましたらお答え願います。（いくつでも） | |
| 1. | 標的型攻撃による機密情報の窃取 |
| 2. | 内部不正による情報漏えい |
| 3. | ビジネスメール詐欺による金銭被害 |
| 4. | サプライチェーンの弱点を悪用した攻撃 |
| 5. | ランサムウェアによる被害 |
| 6. | 予期せぬIT基盤の障害に伴う業務停止 |
| 7. | 不注意による情報漏えい |
| 8. | IoT機器の不正利用 |
| 9. | 妨害攻撃によるサービスの停止 |
| 10. | インターネット上のサービスからの個人情報の窃取 |

|  |  |
| --- | --- |
| Q3. 貴社で脅威と感じている、対策が必要だと思うセキュリティ脅威がございましたらお答え願います。（いくつでも） | |
| 1. | 標的型攻撃による機密情報の窃取 |
| 2. | 内部不正による情報漏えい |
| 3. | ビジネスメール詐欺による金銭被害 |
| 4. | サプライチェーンの弱点を悪用した攻撃 |
| 5. | ランサムウェアによる被害 |
| 6. | 予期せぬIT基盤の障害に伴う業務停止 |
| 7. | 不注意による情報漏えい |
| 8. | IoT機器の不正利用 |
| 9. | 妨害攻撃によるサービスの停止 |
| 10. | インターネット上のサービスからの個人情報の窃取 |

|  |  |
| --- | --- |
| Q4. 貴社で過去に被害のあったセキュリティ脅威がありましたらお答え願います。（いくつでも） | |
| 1. | 標的型攻撃による機密情報の窃取 |
| 2. | 内部不正による情報漏えい |
| 3. | ビジネスメール詐欺による金銭被害 |
| 4. | サプライチェーンの弱点を悪用した攻撃 |
| 5. | ランサムウェアによる被害 |
| 6. | 予期せぬIT基盤の障害に伴う業務停止 |
| 7. | 不注意による情報漏えい |
| 8. | IoT機器の不正利用 |
| 9. | 妨害攻撃によるサービスの停止 |
| 10. | インターネット上のサービスからの個人情報の窃取 |

|  |  |
| --- | --- |
| Q5. 貴社で導入しているサイバーセキュリティ対策をお教えください。(いくつでも) | |
| 1. | ウイルス対策ソフト |
| 2. | 出入口対策（UTM等の設置） |
| 3. | 社員教育 |
| 4. | セキュリティ管理者の設置 |
| 5. | セキュアな無線環境 |
| 6. | セキュアな拠点間通信 |
| 7. | 重要なファイルのバックアップ |
| 8. | サイバーリスク保険加入 |
| 9. | セキュリティポリシーの策定 |

|  |  |
| --- | --- |
| Q6. 貴社で今後導入を検討しているサイバーセキュリティ対策をお教えください。（いくつでも） | |
| 1. | ウイルス対策ソフト |
| 2. | 出入口対策（UTM等の設置） |
| 3. | 社員教育 |
| 4. | セキュリティ管理者の設置 |
| 5. | セキュアな無線環境 |
| 6. | セキュアな拠点間通信 |
| 7. | 重要なファイルのバックアップ |
| 8. | サイバーリスク保険加入 |
| 9. | セキュリティポリシーの策定 |

|  |  |
| --- | --- |
| Q7. 現在セキュリティ対策にかけている月額費用はいくらぐらいですか。 | |
| 1. | 3,000円以下 |
| 2. | 3,000円～5,000円 |
| 3. | 5,000円～10,000円 |
| 4. | 10,000円～20,000円 |
| 5. | 20,000円～ |
| 6. | 費用はかけていない |

|  |  |
| --- | --- |
| Q8. 今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。 | |
| 1. | 3,000円以下 |
| 2. | 3,000円～5,000円 |
| 3. | 5,000円～10,000円 |
| 4. | 10,000円～20,000円 |
| 5. | 20,000円～ |
| 6. | 費用はかけていない |

|  |  |
| --- | --- |
| Q9. サイバーセキュリティ対策に関して、貴社の課題を教えてください | |
| 1. | セキュリティポリシーの策定 |
| 2. | 管理体制の構築 |
| 3. | リスクの洗い出し、評価 |
| 4. | グループ会社、取引先も含めた対策の実施 |
| 5. | セキュリティ対策費予算の確保 |
| 6. | セキュリティ対策専門人材の確保 |
| 7. | インシデント発生時の体制の構築 |
| 8. | 情報収集（最新技術動向や事故事例） |
| 9. | なし |

|  |  |
| --- | --- |
| Q10. 以下の項目の中で、過去に貴社の取引先企業から実施を義務付けられたものがあれば教えてください（いくつでも） | |
| 1. | ウイルス対策ソフト |
| 2. | 出入口対策（UTM等の設置） |
| 3. | 社員教育 |
| 4. | セキュリティ管理者の設置 |
| 5. | セキュアな無線環境 |
| 6. | セキュアな拠点間通信 |
| 7. | 重要なファイルのバックアップ |
| 8. | サイバーリスク保険加入 |
| 9. | セキュリティポリシーの策定 |
| 10. | SECURITY ACTIONの自己宣言 |

|  |  |
| --- | --- |
| Q11. 現在、セキュリティ対策について相談できる相手はいますか | |
| 1. | いる |
| 2. | いない |

|  |  |
| --- | --- |
| Q12. 上記（Q11）で（1）いると答えた方にお聞きします。相談相手はどのような方ですか。 | |
| 1. | システムベンダ |
| 2. | 社外の有識者（税理士や電話業者、詳しい知人） |
| 3. | その他 |
|  | （その他フリーアンサー） |

|  |  |
| --- | --- |
| Q13. インシデント発生した際に、ご相談できる相手はいますか | |
| 1. | いる |
| 2. | いない |

|  |  |
| --- | --- |
| Q14. 上記（Q13）で（1）いると答えた方にお聞きします。相談相手はどのような方ですか | |
| 1. | システムベンダ |
| 2. | 社外の有識者（税理士や電話業者、詳しい知人） |
| 3. | その他 |
|  | （その他フリーアンサー） |

|  |  |
| --- | --- |
| Q15. 貴社は現在テレワークを導入していますか | |
| 1. | 導入している（週3日以上） |
| 2. | 導入している（週1～2日程度） |
| 3. | 導入していない |

|  |
| --- |
| Q16. （Q15で「導入している」と回答された方に伺います）実施しているセキュリティ対策や運用ルールがあれば教えてください（自由回答） |

|  |
| --- |
| Q17. （Q15で「導入していない」と回答された方にお伺いします）テレワーク導入に関する懸念事項があれば教えてください（自由回答） |

|  |  |
| --- | --- |
| Q18. 業務で利用されているサービスについて教えてください  <1.メールサービス＞ | |
| 1. | Microsoft365（Exchange Online） |
| 2. | Google Workspace※（Gmail） |
| 3. | サイボウズ Office |
| 4. | その他 |
|  | （その他フリーアンサー） |
| 5. | 利用なし |
| 6. | わからない |

|  |  |
| --- | --- |
| Q18.業務で利用されているサービスについて教えてください  <2.ストレージサービス＞ | |
| 1. | Microsoft365（OneDrive） |
| 2. | Google Workspace※（Google ドライブ） |
| 3. | Dropbox |
| 4. | Box |
| 5. | その他 |
|  | （その他フリーアンサー） |
| 6. | 利用なし |
| 7. | わからない |

|  |  |
| --- | --- |
| Q18.業務で利用されているサービスについて教えてください  <3.WEB会議＞ | |
| 1. | Microsoft365（Microsoft Teams） |
| 2. | Google Workspace※（Google Meet） |
| 3. | Zoom |
| 4. | Cisco Webex |
| 5. | その他 |
|  | （その他フリーアンサー） |
| 6. | 利用なし |
| 7. | わからない |

|  |  |
| --- | --- |
| Q19.本支援事業に参加したきっかけについて教えてください | |
| 1. | 新型コロナウイルス感染拡大（テレワーク導入） |
| 2. | 新型コロナウイルス感染拡大（テレワーク導入以外） |
| 3. | オリンピック・パラリンピック開催（テレワーク導入） |
| 4. | オリンピック・パラリンピック開催（テレワーク導入以外） |
| 5. | 取引先からの要望 |
| 6. | 社内からの要望 |
| 7. | 実際にサイバー攻撃を受けた |
| 8. | その他 |
|  | （その他フリーアンサー） |
| 9. | 未設定 |

|  |
| --- |
| Q20.サイバーセキュリティに関するご意見・ご要望を自由にご記入ください。（自由回答・任意） |

（２）個別回答結果

① Q1：サイバーセキュリティ対策に関心をお持ちですか

サイバーセキュリティに関しては、回答企業の70%が関心を持ち、対応を検討している。いずれの企業規模においても「いずれ検討」（オレンジ）が、「すぐにでも検討」（ブルー）を上回っており、サイバーセキュリティ対策の必要性を感じつつも、自社に直面する課題として認知されていないと考えられる。

|  |
| --- |
| ＜図の数字＞  社数、割合（％）  ＜凡例＞ |
| 図 3‑1 Q1への回答（全体） |

|  |  |
| --- | --- |
| 図 3‑2 Q1への回答（～20名） | 図 3‑3 Q1への回答（21名～100名） |
| 図 3‑4 Q1への回答（101名～） | ＜凡例＞ |

② Q2：ご存知のセキュリティ脅威がございましたらお答え願います。（いくつでも）

主要なセキュリティ脅威について、企業の認知度を確認した。メールも含む、ネットワーク環境を利用したセキュリティ脅威の認知度が高いという結果となった。IoT機器の不正利用や、サブライチェーンの弱点を悪用した攻撃に対する認知度は低い。これは、各企業がネットワーク環境を利用して業務を遂行しているものの、IoT機器等のデジタル技術を活用して業務プロセスやビジネスモデルの変革を行うデジタルトランスフォーメーションの途上段階であるため、業務ツールや業務プロセスに関する脅威については脅威と捉えていない可能性がある。

図 3‑5 Q2への回答

③ Q3：貴社で脅威と感じている、対策が必要だと思うセキュリティ脅威がございましたらお答え願います。（いくつでも）

　企業規模にかかわらず、セキュリティ脅威への対策への関心は高い。その多くは情報漏洩につながる脅威である。サプライチェーンの弱点を悪用した攻撃や、サービス妨害攻撃によるサービスの停止への関心は相対的に低く、情報漏洩対策を先行対応する傾向となった。

図 3‑6 Q3への回答

④ Q4：貴社で過去に被害のあったセキュリティ脅威がありましたらお答え願います。（いくつでも）

企業が被害にあったセキュリティ脅威は、いずれも10%未満であり、実害は少ない。あるいは、実害があっても、企業としてそれを認知していない可能性も考えられる。認知されている被害では、標的型攻撃による機密情報の搾取、ビジネスメール詐欺による金銭被害、ランサムウェアによる被害が多い。メールを起点としたセキュリティ脅威は中小企業に拡大しつつあると考えられる。

図 3‑7 Q4への回答

⑤ Q5：貴社で導入しているサイバーセキュリティ対策をお教えください。(いくつでも)

サイバーセキュリティ対策は、ウイルス対策ソフトの導入が突出して高く、ほとんどの企業が導入済である。次いで、重要なファイルのバックアップとなる。それ以外の対策は、企業規模にかかわらず、実装がまだ進んでいない。メールを起点とした情報搾取に対するシステム対応に注力している段階と考えられる。

図 3‑8 Q5への回答

⑥ Q6：貴社で今後導入を検討しているサイバーセキュリティ対策をお教えください。（いくつでも）

　Q5ですでに導入しているサイバーセキュリティ対策に加え、どのような対策で事業を防御しようと考えているのか、企業規模別に確認した。

　ウイルス対策ソフトは全社対策済または検討中となった。検討中の対策では、出入口対策（UTM等の設置）が突出している。ウイルス対策ソフト、出入口対策（UTM等の設置）、重要なファイルのバックアップのようなシステム整備を先行する企業が多い。

　その反面、セキュリティ管理者の設置やサイバーリスク保険加入への関心は低く、未知のウイルスへの対応や、感染後の事後対応まで検討するゆとりがないと考えられる。

図 3‑9 Q6への回答（全体）

20名以下の企業は、対応済の対策が少ない。さらに検討している対応も少ない。セキュリティ脅威への対策を直面する課題とはとらえられていない可能性がある。

図 3‑10 Q6への回答（～20名）

21名～100名以下の企業は、会社規模別で最もセキュリティ脅威への対策意識が高い。出入口対策（UTM等の設置）は80%の企業が検討（導入済含む）している。また、半数以上の企業が社員教育を導入済または、検討しており、システム整備に加えて、運用対策にも注目している。

図 3‑11 Q6への回答（21～100名）

101名以上の企業も、出入口対策（UTM等の設置）への関心が最も高い。サイバーリスク保険加入に関心を示す企業はなく、セキュリティ脅威による損失補填という観点には及んでいないと考えられる。

図 3‑12 Q6への回答（101名～）

⑦ Q7： 現在セキュリティ対策にかけている月額費用はいくらぐらいですか。

セキュリティ対策コストは、企業規模に比例すると考えられるため、全体統計は割愛し、企業規模ごとにその傾向を確認する。

|  |  |
| --- | --- |
| 20名以下の企業の投資額は、費用をかけない企業も含め5000円未満が76％を占める。  セキュリティ対策に取り組む資金のゆとりがないこと、セキュリティ対策の即時性が期待できない（狙われる対象ではないとの思い込み）があり、投資に対して消極的になっている可能性がある。 | 図 3‑13 Q7への回答（～20名） |
| 21名以上100名以下の企業では5,000円以上の費用をかける企業が72%と大半を占めた。多くの企業がセキュリティ脅威への対策に関心を持ち、投資しているという結果となった。 | 図 3‑14 Q7への回答（21～100名） |
| 101名以上の会社は、50%の会社が月額3,000円以下で、セキュリティ脅威への対策が遅れている。言い換えれば、それ以外の会社は5,000円以上の投資をしており、会社によるセキュリティ脅威への意識の格差が大きいとの結果が出た。 | 図 3‑15 Q7への回答（101名～） |
| ＜凡例＞ | |

⑧ Q8：今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

会社規模によって投資規模が異なる。20名以下の会社は5,000円から20,000円程度の月額費用を見込む会社が55%と最も多く、それ以上の規模の会社は、10,000円以上の投資を見込む会社が多く、その半数は20,000円以上の投資を見込んでいる。

半面、投資に積極的でない企業も会社規模に依らず一定数あり、企業のセキュリティ対策意識の差が表れた。

|  |  |
| --- | --- |
| 図 3‑16 Q8への回答（全体） | 図 3‑17 Q8への回答（～20名） |
| 図 3‑18 Q8への回答（21～100名） | 図 3‑19 Q8への回答（101名～） |
| ＜凡例＞ | |

⑨ Q9：サイバーセキュリティ対策に関して、貴社の課題を教えてください

サイバーセキュリティ対策に関する課題認識も、企業規模が大きいほうが課題意識を持っているという結果となった。特に100名以上の企業では、8つの選択肢のうち7つの課題に対して30%以上の企業が課題認識を持っている。7つの課題はいずれも自社対応に関する課題であった。残りの1課題はグループ会社や取引先企業も含めた対策を行うもので、まずは自社で実施できる課題への対応が優先と考えている。

図 3‑20 Q9への回答

⑩ Q10：以下の項目の中で、過去に貴社の取引先企業から実施を義務付けられたものがあれば教えてください（いくつでも）

アンケートの回答を見る限り、取引先からセキュリティ対策を詳細に指示されている企業は少ない。ウイルス対策ソフトに関しても、義務付けられている企業は少なく、多くの企業が自主的にセキュリティ対策を行っている模様。

図 3‑21 Q10への回答

⑪ Q11：現在、セキュリティ対策について相談できる相手はいますか。

⑫ Q12：上記（Q11）で（1）いると答えた方にお聞きします。相談相手はどのような方ですか。

企業規模が20名以下の会社は、セキュリティ対策を相談できる専門家がいない場合が多い。社内システムが未整備で、システムを相談するきっかけがないことも要因の一つと考えられる。

|  |  |
| --- | --- |
| 図 3‑22 Q11への回答（～20名） | 図 3‑23 Q12への回答（～20名） |

企業規模が21名～100名の会社では、システムベンダや専門家による支援を受けている企業が多い。社内システムを保守するシステムベンダに確認する傾向が強い。

|  |  |
| --- | --- |
| 図 3‑24 Q11への回答（21～100名） | 図 3‑25 Q12への回答（21～100名） |

企業規模が101名以上の会社は、100名以下の会社よりも相談者がいる割合が低い。相談者がいる場合、対象はシステムベンダが多い。システムベンダに頼れない場合、社外有識者が単独で支援するにはシステム規模が大きいことから、システムベンダに相談するものと想定される。

|  |  |
| --- | --- |
| 図 3‑26 Q11への回答（101名～） | 図 3‑27 Q12への回答（101名～） |

その他のフリーコメントは以下（そのまま記載）。

* NTT（2社）
* 親会社
* 社内のセキュリティ管理者

⑬ Q13：インシデント発生した際に、ご相談できる相手はいますか。

⑭ Q14：上記（Q13）で（1）いると答えた方にお聞きします。相談相手はどのような方ですか。

20名以下の企業の場合、相談先として社外の有識者を指定することが特色である。システムベンダを利用していない、あるいは保守契約を結んでいない企業が多いと考えられる。

|  |  |
| --- | --- |
| 図 3‑28 Q13への回答（～20名） | 図 3‑29 Q14への回答（～20名） |

企業規模が21名～100名の会社では、セキュリティ対策の相談先とインシデント発生時の相談先は同一の傾向となった。

|  |  |
| --- | --- |
| 図 3‑30 Q13への回答（21～100名） | 図 3‑31 Q14への回答（21～100名） |

企業規模が101名以上の会社でも、セキュリティ対策の相談先とインシデント発生時の相談先は同一の傾向となった。

|  |  |
| --- | --- |
| 図 3‑32 Q13への回答（101名～） | 図 3‑33 Q13への回答（101名～） |

その他のフリーコメントは以下（そのまま記載）。

* NTT（2社）
* 社内のセキュリティ管理者
* 上司
* 親会社

⑮ Q15：貴社は現在テレワークを導入していますか

テレワークを導入している、あるいは、導入を検討している企業は、21～100名規模が最も多い。しかし、テレワークの導入を検討していない企業が半数以上を占める。業種的にテレワーク化できないこと、テレワークに対する投資余力がないこと、勤務形態を変えることが困難であることが要因と考えられる。

|  |  |
| --- | --- |
| 図 3‑34 Q15への回答（～20名） | 図 3‑35 Q15への回答（21～100名） |
| 図 3‑36 Q15への回答（101名～） | ＜凡例＞ |

⑯ Q16：（Q15で「導入している」と回答された方に伺います）実施しているセキュリティ対策や運用ルールがあれば教えてください（自由回答）

以下、コメントをそのまま記載する。

* セキュリティ対策
* NTT東日本-IPA「シン・テレワークシステム」の活用（2社）
* 覗き見防止フィルター、ハードディスク暗号化（PINによる暗号化解除）
* 社内NAS接続にはメーカー提供の専用ソフトからのアクセスのみとしている
* IPアドレス制御、リモートツールの活用、ログインIDとパスワード
* 社内LANにVPN接続し、リモートデスクトップ接続による社内PCへの接続によって、社外へのファイル等の流出を防止している。
* 社内端末、在宅用貸与端末へのセキュリティソフトの導入と管理。在宅用端末とのVPN接続等。
* Microsoft365 を利用し　TEAMSでグループ内で情報共有している。
* 会社支給のセキュリティソフト導入ノートPC、HDDにて作業
* 会社専用PCを利用
* ウイルス対策ソフトの導入、バックアップ
* 運用ルール
* IT資産持出に関する誓約書の提出
* セキュリティに対する社員教育
* お客様情報を私用のPCに保存しない。
* リモートデスクトップによる操作。ノートPCにデータを保存しない。
* 社内ネットワークに社外から入らないようにしている。
* 基本的に自宅のみでの接続とし、家族等の同居人に画面等が見られないようにルール化した。
* 個人PCでの作業禁止。VPN通信による社内ネットワーク接続。
* 会社貸与以外へのデータ出力禁止
* USBでのやりとり禁止
* その他
* スマートフォンのテザリングでインターネット接続
* 一部仮導入のため、ルール等は今後策定予定
* 導入しているが建設業なので実施していません

⑰ Q17：（Q15で「導入していない」と回答された方にお伺いします）テレワーク導入に関する懸念事項があれば教えてください（自由回答）

テレワーク導入への懸念は、業務特性により、対応が困難との意見が大多数を占める。以下コメントをそのまま記載する。

* 業務特性
* 業務内容的に出来ない（5社）
* テレワークできる環境は整っていますが、実務的にテレワークが困難な側面はあります。また、現状コロナ禍の中、仕事量の減少もあり、テレワークするほどの業務量がないことも挙げられます。
* 個人情報の閲覧等を含む証券営業端末を利用しており、セキュリティの面から、営業所等の指定された場所に置かれたＰＣからのアクセスに限定されており、現時点ではテレワークに馴染まない業務形態である。当該営業端末の利用条件等が今以上に緩和されない限り、テレワークは難しい。
* 業務内容的に、得意先への訪問を省くことが出来ない。
* 小規模で駅前というロケーションで対面営業中心のため
* 人材派遣業のためクライアントによる作業を伴う業務がある
* 第三波での自粛要請の対象外のため
* インフラ、セキュリティ
  + 情報漏洩（2社）
  + コールセンター業務による受電番号と送信番号表示についてとセキュリティ保持の観点について懸念しています。
* その他
  + 従業員が高齢のため心配だが、どうすればよいか分からない。（2社）
  + 業務効率、担当業務の違いによる公平性
  + 導⼊・運⽤費⽤
  + セキュリティ面、コスト面、運用期間の見定めが難しい。勤怠管理がし辛い。
  + ３月から新事務所を立ち上げる予定だが、その際導入検討中。
  + 現在、導入に向けてテレワーク業務の可否の洗い出しを行っている最中。

⑱ Q18：業務で利用されているサービスについて教えてください

<1.メールサービス＞

メールサービスは、企業規模が大きいほどMSツールを利用する傾向が高い。これは従業員のパソコン利用率が高く、標準ソフト利用が規定されているためと予想される。

20名以下の企業では、メールサービスを利用していない企業が25%（わからないも含めると４７％）となっており、企業としてのツールの統一利用が図られていない可能性がある。21名～100名の会社ではメールサービスを利用していない企業は減少（12%）するが、101名以上の企業では増加（19%、わからないも含めると24%）している。

企業規模の大小にかかわらず、メールのようなコミュニケーションツールは利用されていると考えられる。利用無し、わからないと回答した企業は、システム使用規定や運用ルールが確立されていないのではないかと想定できる。

|  |  |
| --- | --- |
| 図 3‑37 Q18\_1への回答（全体） | 図 3‑38 Q18\_1への回答（～20名） |
| 図 3‑39 Q18\_1への回答（21～100名） | 図 3‑40 Q18\_1への回答（100名～） |
| ＜凡例＞ |  |

凡例以外のメールサービス利用については以下（そのまま記載）。

* Outlook（4社）
* 基本インストールソフト
* MozillaThanderbird
* gmail
* Active! mail
* Knowredge suite
* リコーセンターサービス
* 大塚商会 アルファプレミア
* MFクラウド、楽楽販売
* メール＆ビジネススウェブ
* KDDI
* Nifty
* lolipop
* プロバイダメール

<2.ストレージサービス＞

　ストレージサービスもメールサービス同様、企業規模が大きくなるほどMSツールの頻度が高い。ストレージサービスを利用していない企業は、自社サーバによってファイル共有しているものと推察される。ストレージサービスを利用していない比率は21名～100名規模の企業が最も多く46%となっている。他の質問への回答状況から今回の参加企業の中でこの規模の企業が最もセキュリティ意識が高かったことも起因していると想定される。

|  |  |
| --- | --- |
| 図 3‑41 Q18\_2への回答（全体） | 図 3‑42 Q18\_2への回答（～21名） |
| 図 3‑43 Q18\_2への回答（21～100名） | 図 3‑44 Q18\_2への回答（101名～） |
| ＜凡例＞ |  |

凡例以外のストレージサービス利用については以下（そのまま記載）。

* あずけーるPRO（2社）
* OneDrive　及び　AOSBOX
* NAS
* fileforce
* Direct Cloud
* Apple iCloud
* 社内ファイルサーバ
* 詳細は申し上げられない

<3. WEB会議＞

WEB会議は、全体では60%の企業が利用しているという結果となった。しかし、20名以下の企業では利用している企業は43%に留まる。これは、テレワークの普及率も低く、会社全体のコミュニケーションも通常の会議で賄えるためと考えられる。21名以上の企業では80%程度がweb会議をコミュニケーションツールとして利用している。利用するツールは企業規模にかかわらずZOOMが最も多く、選定条件として、知名度、操作性、利便性が重視されていると考えられる。

|  |  |
| --- | --- |
| 図 3‑45 Q18\_3への回答（全体） | 図 3‑46 Q18\_3への回答（～21名） |
| 図 3‑47 Q18\_3への回答（21～100名） | 図 3‑48 Q18\_3への回答（100名～） |
| ＜凡例＞ |  |

凡例以外のストレージサービス利用については以下（そのまま記載）。

* Skype（3社）
* ライン
* Loop Gate
* Calling
* Slack
* 注：zoomは、検証してテスト使用実績はありますが、zoomを常時使用しての会議は実施していません。

⑲ Q19：本支援事業に参加したきっかけについて教えてください

20名以下の企業では、その他項目が最も多かった。多くの企業は勧められたことを契機に事業に参加している。20名以下の企業に対しては、情報発信だけでなく、情報の伝え方を工夫する必要がある。

図 3‑49 Q19への回答（～20名）

　その他の内訳

* NTT東日本からの紹介（7社）
* 東京都労働局の事業（2社）
* オリンピックに関わる仕事をするため
* ニュース等で怖さを聞いているので
* UTMの効果を実感してみたかったため
* セキュリティ評価を見たいから
* 試してみたかった
* 対策の必要性は感じていたが検討のきっかけがなかった

21名～100名規模の会社では、未設定、次いで社内からの要望が多く、個別事象を解決するための参加ではなく、今後の事業展開を見据えて参加している傾向が強い。

図 3‑50 Q19への回答（21～101名）

その他の内訳

* ＮＴＴ東日本からの紹介（3社）
* 今後の備えとして

　101名以上の企業は、未設定が多く、次いでその他となる。こちらも事業規模に応じたリスク管理の一環としての参加が多いと考えられる。

図 3‑51 Q19への回答（101名～）

　その他の内訳

* NTTからの紹介（2社）
* 会社規模拡大における情報セキュリティ強化
* 危機感が高まってきたため
* セキュリティ評価を見たいから
* 勉強のため

⑳ Q20：サイバーセキュリティに関するご意見・ご要望を自由にご記入ください。（自由回答・任意）

* 色々相談できる窓口があればいいと思っている。
* ポイントごとではなく、組織全体のサイバーセキュリティ対策を設計から選定・導入まで一括して提供いただけるサービスがあると、業務負担が軽減します。
* 先日取引先がEmotetに感染し、自社にもメールが届いている。何か有効な対策があれば教えてほしい。
* 現在、全国に事業所があり出入口対策を検討している状況。今回は東京都にあるその一つの事業で参加予定。
* アナログな上を今後説得する材料の一つにでもなれば・・・
* ウイルス対策
* 相談できる窓口があればいいと思っている。
* 対策をしても100%、攻撃を防げるもので無いこと、また、サイバーセキュリティ対策費用負担が増えていることに不安を感じる。
* 現在も大塚商会のUTMを利用しているが、以前よりＮＴＴ営業担当からセキュリティ対策強化の提案を受けていて今回お願いすることにした。機器を取り付けるだけではなく監視サポートがしっかりしている点、これまでのサイバーセキュリティに関する安心感が増すと思う。
* UTMを設置したいと考えていた。
* どこにどういうリスクがあるかわかりにくい。
* 教育もやりたい

## **サイバーセキュリティ対策の障壁把握**

今回のアンケートにより、中小企業のサイバーセキュリティ対策の状況は概ね以下のとおりであることを確認した。

* 主要なサイバーセキュリティ脅威は認識している。
* サイバーセキュリティ対策の必要性を感じている。
* セキュリティ脅威に直面した企業は少なく、直面する課題との認識は低い。
* 検討するセキュリティ対策はシステム整備（セキュリティソフト、バックアップ等）に特化している。
* 人材育成やサイバーリスク保険への投資は進んでいない。
* 中規模（21～100名規模）の企業のセキュリティ対策意識が高い。

中小企業は、サイバーセキュリティに対する知識はあるものの、直面する課題意識は低い。そのため、管理体制は未整備である場合が多く、セキュリティシステムへの投資以上に積極的に教育や運用管理に計画的に投資する企業はまだ少ない。

取引先企業からの外圧によりサイバーセキュリティ対策を求められる機会も少ないため、自助努力での整備に留まっている。限られた予算、要員で対応できるところからはじめている、というのが実情と考えられる。従業員教育の必要性は認識しているものの、重要視されておらず、サイバーセキュリティ対策の定着化の障壁となっているものと考えられる。

この状況を打開するためには、企業自身によるサイバーセキュリティ対策への意識改革が求められると同時に、国や自治体からの更なるサポート（業種別、規模別ガイドラインの策定や、IT専門家による助言、対応費用の助成等）により、企業の改革を支援することも検討の余地があると考えられる。

# **支援期間中のサイバーセキュリティ脅威の状況と対策支援状況**

## **UTMのログから見える脅威のアタックとブロック状況**

UTMで検知した事象は、以下表4-1の種別の通りログとして把握できる。

表 4‑1 UTMで検知する事象の種別及びその内容

|  |  |
| --- | --- |
| 種別 | 内容 |
| ①不正プログラム／スパイウェア | 不正プログラム検索機能により、不正プログラム(マルウェア)、スパイウェアであることを検知 |
| ②不正侵入防止（IPS[[7]](#footnote-7)） | 通信がIPS機能で定義されたルールにマッチしたかを検知 |
| ③不正サイト | Webレピュテーション機能により、危険とされるURL[[8]](#footnote-8)へのHTTPリクエストまたはTLSネゴシエーション[[9]](#footnote-9)等を検知 |
| ④スパムメール | メールセキュリティ機能により、スパムメールを検知 |
| ⑤ランサムウェア | 不正プログラム検索機能により、ランサムウェアであることを検知 |
| ⑥C＆Cコールバック | C&Cコールバック[[10]](#footnote-10)とされるURLへのHTTPリクエストを検知 |
| 【参考1】禁止アプリケーション | ポリシー設定で禁止したアプリケーションからの通信要求を検知 |
| 【参考2】URLカテゴリフィルタ | トレンドマイクロがカテゴライズしたURLカテゴリに該当したHTTPリクエストまたはTLSネゴシエーションを検知 |

以下では事象の種別ごとにその検知数や特徴を見ていく。

①不正プログラム／スパイウェア

「不正プログラム／スパイウェア」は、コンピュータに害悪を及ぼすプログラムであり、コンピュータが不正に操作され、社内の情報をインターネットに対して送り出してしまう脅威がある。UTMにより、不正な通信、プログラムによる攻撃を検知し、どのような通信が行われているかを判別し、内部感染を早期に発見できる。

2020年12月から2021年3月の間に「不正プログラム／スパイウェア」を検知した件数は、表4-2の通り、2020年12月は0件、2021年1月は22件、2月は8件、3月は5件であった。期間中の検知件数が最も多かった2021年1月で1社あたり0.4件であり、期間全体を通して不正プログラム／スパイウェアはそれほど目立たなかったと言えよう。

表 4‑2 不正プログラム／スパイウェアの検知件数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月[[11]](#footnote-11) |
| 社数[[12]](#footnote-12) | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| 検知件数 | 0 | 22 | 8 | 5 |
| 1社あたり検知件数 | 0 | 0.4 | 0.1 | 0.1 |

「不正プログラム／スパイウェア」について、プログラム名称別の件数内訳でみると、表4-3の通り、様々なプログラムが存在しており、中でも表計算関連ファイル（拡張子が.xlsm）が複数検知された。表計算関連ファイルのように業務上利用頻度が高いと思われるファイルに不正プログラムが含まれるのは特徴の一つといえる。

表 4‑3 不正プログラム／スパイウェアの名称別累計検知件数及び該当社数

（2020年12月）

| 不正プログラム名 | 累計件数 | 該当社数 |
| --- | --- | --- |
| なし | 0件 | 0社 |
| 合計 | 0件 | - |

（2021年1月）

| 不正プログラム名 | 累計件数 | 該当社数 |
| --- | --- | --- |
| xl/vbaProject.bin | 5件 | 1社 |
| RFQ# Tengco\_270121.doc | 3件 | 1社 |
| 004023520760\_1.xlsm | 1件 | 1社 |
| 004046763587\_1.xlsm | 1件 | 1社 |
| 004069384229\_1.xlsm | 1件 | 1社 |
| 004096707116\_2.xlsm | 1件 | 1社 |
| 004097721212\_1.xlsm | 1件 | 1社 |
| 1 Total New Invoices-Thursday January 21 2021.xlsm | 1件 | 1社 |
| 1-Total New Invoices Monday Dec 14 2020.xlsm | 1件 | 1社 |
| 1\_Total New Invoices-Thursday January 21\_2021.xlsm | 1件 | 1社 |
| Statement of Account as of 01\_20\_2021.xlsm | 1件 | 1社 |
| 3131\_50SG0BK00T1,pdf.iso | 1件 | 1社 |
| PO\_PO21\_00126\_20210120\_114626,pdf.iso | 1件 | 1社 |
| W21\_0191,pdf.iso | 1件 | 1社 |
| 不明 | 2件 | - |
| 合計 | 22件 | - |

（2021年2月）

| 不正プログラム名 | 累計件数 | 該当社数 |
| --- | --- | --- |
| Statement\_as\_of FEB\_01\_2021.xlsm | 1件 | 1社 |
| Statement\_of\_Account\_as\_of FEB\_01\_2021.xlsm | 1件 | 1社 |
| Lowes\_Quotation\_PN#16392021.xlsx | 1件 | 1社 |
| 30-080 719\_pdf.gz | 1件 | 1社 |
| S-Bulkers.rar | 1件 | 1社 |
| noon emirates.gz,1783423\_PDF.r00 | 1件 | 1社 |
| Statement of Account as of Monday 01\_25\_2021.xlsm | 1件 | 1社 |
| install.bat,RDPCheck.exe,RDPConf.exe,RDPWInst.exe,update.bat | 1件 | 1社 |
| 合計 | 8件 | -- |

（2021年3月）

| 不正プログラム名 | 累計件数 | 該当社数 |
| --- | --- | --- |
| printouts of outstanding\_as\_of\_03\_01\_2021.xlsm | 1件 | 1社 |
| printouts\_of\_outstanding\_as\_of\_03\_01\_2021.xlsm | 1件 | 1社 |
| Image001.gz | 1件 | 1社 |
| TT COPY\_PDF.gz | 1件 | 1社 |
| 640588958937.xlsm | 1件 | 1社 |
| 合計 | 5件 | -- |

1. 不正侵入

「不正侵入」は、ソフトウェアやネットワークの脆弱性を利用してシステムが乗っとられたり、その結果機密情報が漏えいしてしまったりする脅威がある。UTMにより、ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信を検知しブロックできる。

2020年12月から2021年3月の間に「不正侵入防止（IPS）」を検知したマッチ回数は、表4-4の通りであった、月別の変化を1社あたりマッチ件数でみても、2021年2月の多さが際立っている。

表 4‑4 不正侵入防止（IPS）のマッチ回数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月 |
| 社数[[13]](#footnote-13) | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| マッチ件数 | 71 | 10,290 | 111,106 | 35,821 |
| 1社あたりマッチ件数 | 35.5 | 177.4 | 1,194.7 | 393.6 |

「不正侵入防止（IPS）」について、ルール名称別の件数内訳を表4-5に示した。2020年12月の「1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 (CVE-2017-3731):CVE-2017-3731」のように複数社で検知されたり、月を跨いで検知されたりするルールがあり、特にこのルールに関していえば1月に36社、2月に22社、3月に3社が該当していることがわかる。

また、2021年1月の第1位になったルール「4043309077:ICMP Error Message:MISC:RFC 792」は、該当社数は1社ではあるが、2月、3月でも第1位になっており、この期間の特徴となっている。

表 4‑5不正侵入防止（IPS）のルール名別累計マッチ回数及び該当社数（累計マッチ回数上位10ルールまで）

（2020年12月）

|  | IPSルール名 | 累計  マッチ回数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | 1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 (CVE-2017-3731):CVE-2017-3731 | 65回 | 2社 |
| 2 | 1130226 | 5回 | 1社 |
| 3 | 4043309087:Bad TCP Flag:MISC:RFC 791 | 1回 | 1社 |

（2021年1月）

|  | IPSルール名 | 累計  マッチ回数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | 4043309077:ICMP Error Message:MISC:RFC 792 | 4,031回 | 1社 |
| 2 | 1049193:SHELLCODE x86 NOOP – 1 | 2,181回 | 1社 |
| 3 | 4043309087:Bad TCP Flag:MISC:RFC 791 | 1,861回 | 7社 |
| 4 | 1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 (CVE-2017-3731):CVE-2017-3731 | 653回 | 36社 |
| 5 | 1056952:TCP Paws Elimination:MISC:RFC 1323 | 602回 | 1社 |
| 6 | 1133480:EXPLOIT Remote Command Execution via Shell Script -2:CVE-2017-unknown | 196回 | 3社 |
| 7 | 1132982 | 175回 | 4社 |
| 8 | 1055299 | 121回 | 5社 |
| 9 | 1130226 | 83回 | 13社 |
| 10 | 1133253:WEB Remote Command Execution via Shell Script -1.h:msf; CVE-2016-unknown | 75回 | 3社 |

（2021年2月）

|  | IPSルール名 | 累計  マッチ回数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | 4043309077:ICMP Error Message:MISC:RFC 792 | 90,972回 | 1社 |
| 2 | 4043309087:Bad TCP Flag:MISC:RFC 791 | 16,086回 | 8社 |
| 3 | 1049193:SHELLCODE x86 NOOP – 1 | 2,568回 | 2社 |
| 4 | 1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 (CVE-2017-3731):CVE-2017-3731 | 335回 | 22社 |
| 5 | 1054742:EXPLOIT Microsoft Client Service for NetWare Memory Corruption (CVE-2006-4688):CVE-2006-4688 | 296回 | 2社 |
| 6 | 1058626:WEB Generic XXE Information Disclosure -1:CVE-2018-10613; CVE-2018-3600; EDB-32623; CVE-2013-5014; CVE-2013-6447; CVE-2013-6429; CVE-2014-0002 | 145回 | 3社 |
| 7 | 1058077:WEB SQL injection attempt -1.b:CVE-2018-8734; CVE-2018-7501; CVE-2014-0763; CVE-2007-1729; BID-23161; OSVDB-94448; CVE-2017-7973; ZDI-18-485; | 141回 | 1社 |
| 8 | 1133253:WEB Remote Command Execution via Shell Script -1.h:msf; CVE-2016-unknown | 137回 | 3社 |
| 9 | 1133480:EXPLOIT Remote Command Execution via Shell Script -2:CVE-2017-unknown | 69回 | 2社 |
| 10 | 1134610:WEB Dasan GPON Routers Command Injection -1.1 (CVE-2018-10561):CVE-2018-10561; CVE-2018-10562 | 60回 | 3社 |

（2021年3月）

|  | IPSルール名 | 累計  マッチ回数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | 4043309077:ICMP Error Message:MISC:RFC 792 | 33,653回 | 1社 |
| 2 | 1049193:SHELLCODE x86 NOOP – 1 | 1,492回 | 2社 |
| 3 | 4043309087:Bad TCP Flag:MISC:RFC 791 | 253回 | 7社 |
| 4 | 1133253:WEB Remote Command Execution via Shell Script -1.h:msf; CVE-2016-unknown | 99回 | 3社 |
| 5 | 1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 (CVE-2017-3731):CVE-2017-3731 | 88回 | 3社 |
| 6 | 1058626:WEB Generic XXE Information Disclosure -1:CVE-2018-10613; CVE-2018-3600; EDB-32623; CVE-2013-5014; CVE-2013-6447; CVE-2013-6429; CVE-2014-0002 | 66回 | 3社 |
| 7 | 1134610:WEB Dasan GPON Routers Command Injection -1.1 (CVE-2018-10561):CVE-2018-10561; CVE-2018-10562 | 38回 | 3社 |
| 8 | 1136426:WEB Remote Command Execution via Shell Script -3:msf; CVE-2016-unknown | 28回 | 3社 |
| 9 | 1056055:WEB PHP CGI Argument Injection:CVE-2012-1823; msf | 20回 | 3社 |
| 10 | 1054873:EXPLOIT Microsoft Windows OLE Automation Remote Code Execution (CVE-2011-0658):CVE-2011-0658; MS11-038 | 15回 | 3社 |

③不正サイト

「不正サイト」は、不正なWebサイトへのアクセスによる不正プログラムへの感染や実行、フィッシング詐欺被害等の発生につながる脅威がある。UTMにより、IPアドレスの情報から、どのユーザが不正サイトへのアクセスを試みているかを把握することが可能で、不正サイトへの接続を検知しブロックできる。

2020年10月から12月の間の「不正サイト」を検知した件数は、表4-6の通り、2020年12月は1件、2021年1月は35件、2月は311件、3月は333件であった。3月分のデータが12日までであることを鑑みると、増加傾向が見てとれる。

表 4‑6 不正サイトの検知件数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月 |
| 社数 | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| 検知件数 | 1 | 35 | 311 | 333 |
| 1社あたり検知件数 | 0.5 | 0.6 | 3.3 | 3.7 |

「不正サイト」について、不正サイト名称別の件数内訳を表4-7に示した。期間を通じ、複数社が該当した不正サイトはいくつかあるものの、全体としては不正サイト自体が多様に存在しており、そこへのアクセスが個別化している状況が見てとれる。不正サイトが身近に存在していることを示唆していると言えよう。

表 4‑7 不正サイトのサイト名称別累計検知件数及び該当社数（累計件数上位10サイト）

（2020年12月）

|  | 不正サイト名称 | 累計件数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | koreateen.top | 1件 | 1社 |
| 小計（上位10サイト） | | 1件 | - |
| 合計 | | 1件 | - |

（2021年1月）上位10サイトが累計件数全体に占める割合：82.8%

|  | 不正サイト名称 | 累計件数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | rare-jav.club | 12件 | 1社 |
| 2 | colorful-yourlife.com | 4件 | 1社 |
| 3 | t.aeoyhl.com | 2件 | 1社 |
| 4 | not-used.com | 2件 | 1社 |
| 5 | dividedscientific.com | 2件 | 1社 |
| 6 | [www.trisquel.shop](http://www.trisquel.shop) | 2件 | 1社 |
| 7 | ctuk-8.settlement-fancy.co | 2件 | 1社 |
| 8 | image.colorful-yourlife.com | 1件 | 1社 |
| 9 | rookmemorizevoluntary.com | 1件 | 1社 |
| 10 | tilltucked.com | 1件 | 1社 |
| 小計（上位10サイト） | | 29件 | - |
| 合計 | | 35件 | - |

（2021年2月）上位10サイトが累計件数全体に占める割合：89.7%

|  | 不正サイト名称 | 累計件数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | [www.aww799.com](http://www.aww799.com) | 226件 | 1社 |
| 2 | yabi.qdprz.xyz | 18件 | 1社 |
| 3 | d24ak3f2b.top | 9件 | 2社 |
| 4 | fwma-umbrella.bid | 8件 | 1社 |
| 5 | [www.masksjp.xyz](http://www.masksjp.xyz) | 4件 | 1社 |
| 6 | wilfulpessimistic.com | 3件 | 2社 |
| 7 | allaboutnice.shop | 3件 | 2社 |
| 8 | dividedscientific.com | 3件 | 1社 |
| 9 | website.drupalthemes.website | 3件 | 1社 |
| 10 | topownsale.shop | 2件 | 1社 |
| 小計（上位10サイト） | | 279件 | - |
| 合計 | | 311件 | - |

（2021年3月）上位10サイトが累計件数全体に占める割合：95.8%

|  | 不正サイト名称 | 累計件数 | 該当社数 |
| --- | --- | --- | --- |
| 1 | leverselll.com | 202件 | 1社 |
| 2 | [www.aww799.com](http://www.aww799.com) | 95件 | 1社 |
| 3 | lilacdefencelessroyal.com | 9件 | 1社 |
| 4 | [www.vldnb.xyz](http://www.vldnb.xyz) | 3件 | 1社 |
| 5 | topinhere.top | 2件 | 1社 |
| 6 | glandtest.com | 2件 | 1社 |
| 7 | hollywoodprofessional.top | 2件 | 1社 |
| 8 | salesfire.top | 2件 | 1社 |
| 9 | everforgoods.shop | 1件 | 1社 |
| 10 | sdfhht.airdate.info | 1件 | 1社 |
| 小計（上位10サイト） | | 319件 | - |
| 合計 | | 333件 | - |

④スパムメール

「スパムメール」は、宣伝広告目的で、ユーザの同意なしに勝手に送られてくる迷惑メールで、アクセスのみで感染にいたるURLが記されている場合は誤ってアクセスすることで情報漏えい等につながる脅威がある。UTMにより、スパムメールを判定して、件名に「スパムメール」と付与する処理を行いユーザが誤ってURLにアクセスしないよう注意を喚起できる。

2020年10月から12月の間の「スパムメール」を検知した件数は、表4-8の通り、2020年12月は53件、2021年1月は3,154件、2月は14,475件、3月は13,360件であった。3月が月途中までの件数であることを勘案すると、1社あたり検知件数でみても増加傾向となっている可能性がある。

表 4‑8 スパムメールの検知件数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月 |
| 社数 | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| 検知件数 | 53 | 3,154 | 14,475 | 13,360 |
| 1社あたり検知件数 | 26.5 | 54.4 | 155.6 | 146.8 |

⑤ランサムウェア

「ラムサムウェア」は、PC内のファイルの暗号化やロックにより、それを元に戻すことと引き換えに「身代金」（Ransom）を要求する不正プログラムで、業務で使っているPC等が使用できない状況に追いこまれる脅威がある。UTMにより、ランサムウェアの侵入を検出しブロックした件数と、宛て先となっていたユーザを把握できる。

2020年12月から2021年3月の間で「ランサムウェア」を検知した件数は、表4-9の通り0件であった。

表 4‑9 ランサムウェアの検知件数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月 |
| 社数 | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| 検知件数 | 0 | 0 | 0 | 0 |
| 1社あたり検知件数 | 0 | 0 | 0 | 0 |

⑥C＆Cコールバック

「C＆Cコールバック」は、ボットネットや感染コンピュータのネットワークに対し、不正なコマンドを遠隔で頻繁に送信するために利用されるC&Cサーバに通信が発生した場合、特定のWebサイトへ負荷を与えるDDoS攻撃や、サーバから重要な機密情報を抜き取りなどの被害が発生する脅威がある。UTMにより、C&Cサーバ接続を検知・ブロックし、IPアドレスにより、どのユーザがC&Cサーバへの通信を実施しているか把握できる。

2020年12月から2021年3月の間の「C＆Cコールバック」を検知した件数は、表4-10の通り、2021年1月に検知された26件が目立つ結果となった。

表 4‑10 C＆Cコールバックの検知件数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月 |
| 社数 | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| 検知件数 | 0 | 26 | 0 | 0 |
| 1社あたり検知件数 | 0 | 0.4 | 0 | 0 |

以降では、参考情報としてUTMで検知した「禁止アプリケーション」の検知件数と「URLカテゴリフィルタ」の検知件数を示す。

【参考1】禁止アプリケーション

「禁止アプリケーション」の検知件数は、ポリシー設定で禁止したアプリケーションからの通信要求が検知された件数を示す（以下表4-11）。

表 4‑11 禁止アプリケーションの検知件数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月 |
| 社数 | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| 検知件数 | 2 | 261,126 | 367,747 | 62,684 |
| 1社あたり検知件数 | 1 | 4,502.2 | 3,954.3 | 688.8 |

【参考2】URLカテゴリフィルタ

「URLカテゴリフィルタ」の検知件数は、HTTPリクエストまたはTLSネゴシエーションをもとにトレンドマイクロがカテゴライズしたURLカテゴリに該当した場合、そのアクセス件数（HTTPリクエストまたはTLSネゴシエーション試行単位）を示す（以下表4-12）。

表 4‑12 URLカテゴリフィルタの検知件数（月別）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2020年12月 | 2021年1月 | 2021年2月 | 2021年3月 |
| 社数 | 2 (2) | 60 (58) | 98 (93) | 99 (91) |
| 検知件数 | 222,750 | 4,133,816 | 13,206,790 | 9,162,745 |
| 1社あたり検知件数 | 111,375 | 71,272.7 | 142,008.5 | 100,689.5 |

## **標的型攻撃メール訓練開封率（支援期間中2回の比較）**

標的型攻撃メール訓練は期間中、異なる内容の訓練を2回実施した。第1回目訓練は添付ファイルのあるメールを、第2回目訓練では添付ファイルはなくURLが含まれるメールをそれぞれ送信した。訓練対象は第1回目が91社の128ユーザ、第2回目が99社の141ユーザである。

訓練メールの具体的な内容は表4-13に示す。なお訓練期間中、訓練についての事前の通知は行っておらず、事後に訓練完了通知を行った。

表 4‑13 訓練メールの内容

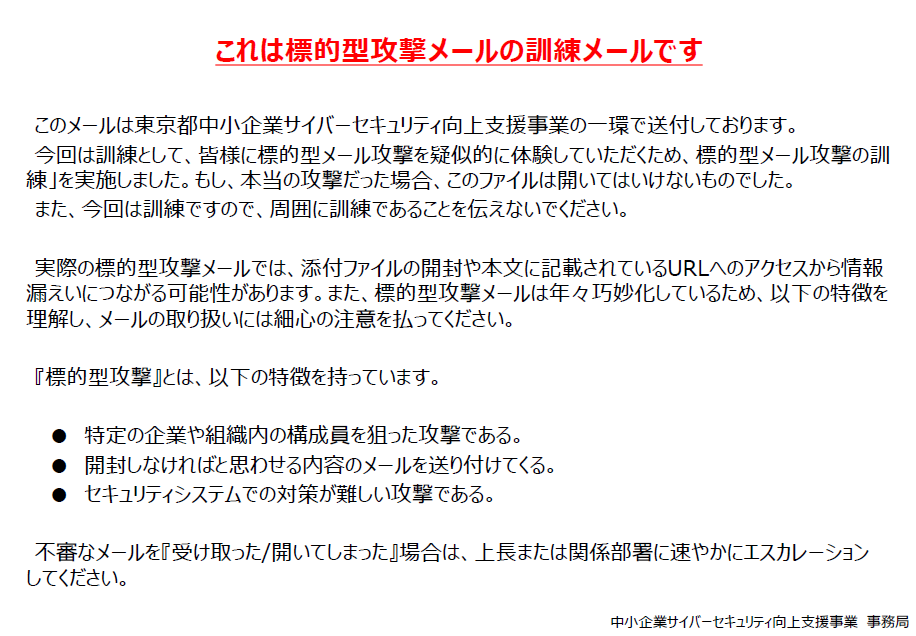
（第1回目）2021年2月8日（月）10時～2月13日（土）10時の間

|  |  |
| --- | --- |
| 送信元 | 総務<soumu.kyoyu@infomaton.com> |
| 送信日時 | 2021年2月8日（月）10:00 |
| メール件名 | 落とし物の確認 |
| 本文 | 各位  お疲れ様です。  総務より連絡です。  スマートフォンの落し物（添付ファイル参照）を預かって  おりますので、持ち主の方は総務までお越しください。  何卒、宜しくお願い致します。 |
| 添付ファイル | 落とし物.pdf（圧縮無し、パスワード無し、42KB） |
| ポイント | * 送付元アドレス（送付元「総務」やアドレスの綴り） * 送信先アドレス表示がご自身や普段やり取りしている関係者が設定している署名と異なる（訓練では申込書のご担当者名をそのまま活用） |

（第2回目）2021年2月22日（月）14時～2月27日（土）14時の間

|  |  |
| --- | --- |
| 送信元 | 健康管理センター<tokyo\_healthmanagement@a7nx3dmh.com> |
| 送信日時 | 2021年2月22日（月）14:00 |
| メール件名 | 【ご案内】新型コロナウイルス健康管理調査について |
| 本文 | 東京都内の事業者様へ  健康管理センターです。  いつもお世話になっております。  このたび、新型コロナウイルス感染拡大防止対策の一環で  東京都内の企業様における従業員の健康管理状況を把握するために、  アンケートを実施させていただきます。  お忙しいところ大変申し訳ございませんが、  以下のURLにアクセスいただき、ご報告をお願いいたします。  http://www.\*\*\*\*略\*\*\*\*.com/\*\*\*\*略\*\*\*\*  以上、よろしくお願いいたします。 |
| 添付ファイル | 無し |
| ポイント | * 怪しい送信元メールアドレス * 本文内容とURL |

図 4‑1 （参考）添付ファイル開封またはURLクリックした場合の検知画面



まず、ユーザ単位でその結果を見ると、第1回目は検知率（開封率）3.9%（対象者数は128、検知数（開封数）は5件）、第2回目は検知率3.5%（対象者数は141、検知数は5件）と、第2回目の検知率が約0.4ポイント低いもののほとんど差がない結果となった（以下表4-14）。

表 4‑14 標的型攻撃メール訓練の実施概要及び結果概要（ユーザ単位）

|  | 訓練期間 | 対象数 | 検知数 | 検知率 |
| --- | --- | --- | --- | --- |
| 第1回目 | 2021年2月8日（月）10時～2月13日（土）10時 | 128 | 5 | 3.9% |
| 第2回目 | 2021年2月22日（月）14時～2月27日（土）14時 | 141 | 5 | 3.5% |

次に、企業単位の結果として、その企業に所属するユーザの少なくとも1人が検知された企業の割合は、第1回目が5.5%、第2回目が5.1%であった。ユーザ単位での結果と同様に第2回目の割合が約0.4ポイント低い結果となっている（以下表4-15）。

標的型攻撃メールを開いてしまった場合、その被害を受けるのはメールを開いてしまった本人に留まらず、社内のネットワークを通じる等で会社全体に被害が広がる可能性がある。標的型攻撃メールの受信及び開封に伴いその被害を受ける可能性のある企業は潜在的には約1割弱存在することを示しており、メールの利用においては一人ひとりが安易に添付ファイルを開いたり、リンクをクリックしたりしないよう留意しておくことが強く求められることを示した結果と考える。

表 4‑15 標的型攻撃メール訓練の実施概要及び結果概要（企業単位）

|  | 訓練期間 | 対象数  （社数） | 検知数  （社数） | 検知率 |
| --- | --- | --- | --- | --- |
| 第1回目 | 2021年2月8日（月）10時～2月13日（土）10時 | 91 | 5 | 5.5% |
| 第2回目 | 2021年2月22日（月）14時～2月27日（土）14時 | 99 | 5 | 5.1% |

## **テレワーク実施企業のクラウドアプリセキュリティ診断**

テレワーク先で業務を遂行するためのツールとして手軽に導入・運用できるMicrosoft 365やGoogle Workspaceに代表されるSaaSサービスを利用している企業に対し、不正プログラムや不正メール等、クラウドサービスへの攻撃状況を診断した。

＜対象者＞　Ａ社

＜診断期間＞　3週間

＜診断結果＞

1. 診断結果概要

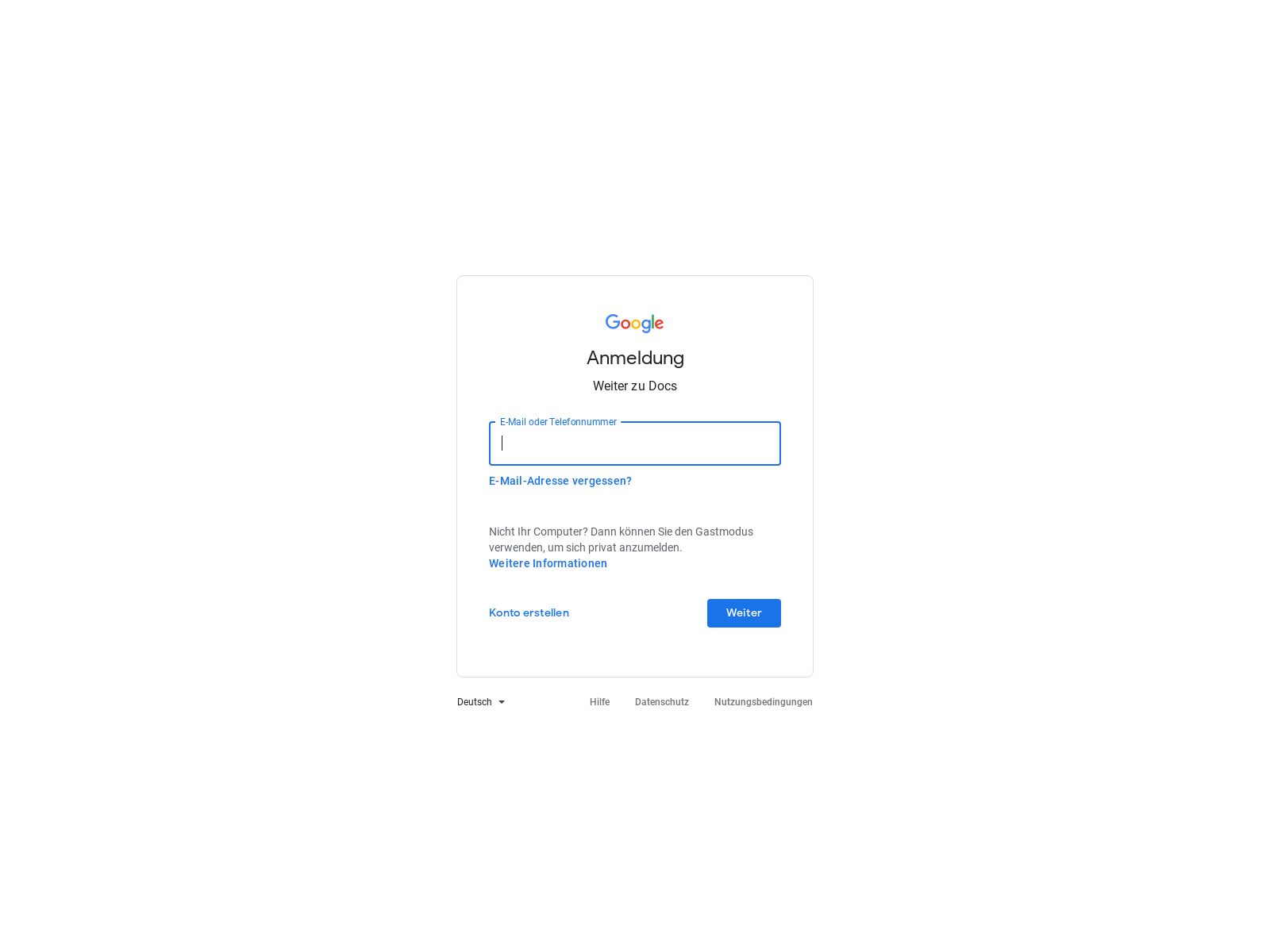
Ａ社が業務にて利用する複数のクラウドアプリケーションについて診断を実施し、400件以上の「脅威の可能性があるプログラム」が検知された。

1. 脅威検知状況の詳細

「脅威の可能性があるプログラム」の検知の中には不正プログラムの配信サイト・フィッシングサイトがあることが判明。[[14]](#footnote-14)

確認の結果、対象のウェブサイトは偽のログインサイトが表示されていたため、Ａ社にはこのような身に覚えのないメールは開かないように社内の注意喚起をすることを推奨した。

（参考）偽のログインサイト画面



## **セキュリティサポートデスクへの問い合わせ内容**

本事業の支援期間中において、21社から計29件のセキュリティサポートデスクへの問い合わせがあった。大部分は、UTM機器の設定確認・変更依頼であるが、支援対象企業自身が自社へのアタック状況を確認したいという意識も見てとれた。

なお、本支援期間中において、支援対象企業にてセキュリティインシデントは発生しておらず、技術者による駆け付けサポート等は実施していない。

問い合わせ内容と件数は表4-16の通り。

表 4‑16 サポートデスクへの問い合わせ内容

|  |  |  |
| --- | --- | --- |
| 内容 | | 件数 |
| UTMの設定確認・変更依頼 | | 18件 |
|  | （再掲）特定URLブロック設定・解除 | 9件 |
| （再掲）支援対象企業からの機器ステータス確認 | 4件 |
| （再掲）サポートデスクからの機器状況確認 | 3件 |
| （再掲）業務時の不具合対応 | 2件 |
| UTMのアタック状況等内容確認 | | 6件 |
|  | （再掲）レポート内容の確認 | 4件 |
| （再掲）管理コンソール画面の確認 | 2件 |
| ウイルス感染疑い対応…詳細① | | 2件 |
| レポートに関する対応相談…詳細② | | 1件 |
| その他 | | 2件 |

中でも、特徴的であった問い合わせに関して、詳細を紹介する。

1. 「ウイルス感染疑い対応」の詳細

＜申告内容＞

「送った覚えのないメールが送信されており、受信先でウイルス検知されたようだ。UTMのログを確認してほしい。」

＜対応内容＞

* 以下の三つの可能性及び対策をご説明。

1. PCがマルウェアに感染している（対策はPCフルスキャン）
2. 情報が抜き取られ、アドレスを偽装されている（対策はPW変更などのセキュリティ強化）
3. サーバが不正に操作されている（対策はメールサーバへの問い合わせ）

* フルスキャン実施のためのウイルス対策ソフトの確認等を遠隔で実施し、フルスキャンの対応を行った。

1. 「レポートに関する対応相談」の詳細

＜申告内容＞

「レポートを見ると危ない通信をたくさんブロックした形跡があるがどうしたらよいか。」

＜対応内容＞

* IPアドレス等の申告内容詳細を確認し、UTMのログ等を確認。支援対象企業が申告したIPアドレスだけでなくそれ以外のIPアドレスも検知されており、発生源の特定不可。
* 根本的な原因がローカルPCにある場合が想定されるため、PC側のフルスキャンをご案内。

## **全体的なサイバーセキュリティ上のトピックス**

期間中、駆け付け対応等が必要な重大インシデントの発生には至らなかったものの、UTMのログで検知した事象や標的型攻撃メール訓練等の結果から、知らず知らずのうちに不正サイトにアクセスしてしまう可能性、通常のメールを装い不正なファイルが添付されて送られてくる等、日常的に様々なサイバーセキュリティ上の脅威が身近に存在することを改めて確認した。

業務で利用する情報システムにおける脆弱性の存在は攻撃者に攻撃機会を与え、企業自体やその顧客は予期せぬ被害を受けてしまう契機となるため、継続的なログの確認及びセキュリティ診断、その結果をふまえた脆弱性の除去等、速やかな対応が必要といえる。

# **支援後の中小企業の意識の変化と実態把握**

## **支援終了時のアンケート結果**

＜対象者＞　説明会参加企業・本事業参加企業

＜回答数＞　99社

＜回答企業属性＞

表 5‑1　業種別にみた企業数

|  |  |
| --- | --- |
| 業種 | 回答企業数（社） |
| 卸売業、小売業 | 30 |
| 製造業 | 13 |
| サービス業 | 13 |
| 情報通信業 | 7 |
| 不動産業、物品賃貸業 | 7 |
| 医療、福祉 | 7 |
| 建設業 | 5 |
| 宿泊業、飲食店 | 5 |
| その他 | 4 |
| 運輸業、郵便業 | 4 |
| 生活関連サービス業、娯楽業 | 3 |
| 金融業、保険業 | 1 |
| 学術研究、専門・技術サービス業 | 1 |
| 教育学習信楽 | 1 |
| 計 | 101[[15]](#footnote-15) |

表 5‑2　従業員数別にみた企業数

|  |  |
| --- | --- |
| 従業員数 | 回答企業数（社） |
| ～20名 | 57 |
| 21名～100名 | 22 |
| 101名～ | 20 |
| 計 | 99 |

表 5‑3 従業員数別、業種数

|  |  |  |  |
| --- | --- | --- | --- |
| 業種 | 企業規模 | | |
| ～20名 | 21～100名 | 101名～ |
| 卸売業、小売業 | 15 | 8 | 7 |
| 製造業 | 6 | 4 | 3 |
| サービス業 | 10 | 1 | 2 |
| 情報通信業 | 7 | 0 | 0 |
| 不動産業、物品賃貸業 | 6 | 0 | 1 |
| 医療、福祉 | 3 | 4 | 0 |
| 建設業 | 3 | 0 | 2 |
| 宿泊業、飲食店 | 1 | 0 | 4 |
| その他 | 0 | 2 | 2 |
| 運輸業、郵便業 | 2 | 1 | 1 |
| 生活関連サービス業、娯楽業 | 1 | 1 | 1 |
| 金融業、保険業 | 0 | 1 | 0 |
| 学術研究、専門・技術サービス業 | 1 | 0 | 0 |
| 教育学習信楽 | 1 | 0 | 0 |
| 計 | 56 | 22 | 23 |

＜支援実施後アンケート内容＞

|  |  |
| --- | --- |
| Q1.本事業参加前と参加後で、サイバーセキュリティ対策に関する意識に変化があれば教えてください。 | |
| 1. | セキュリティ対策意識が高まった |
| 2. | セキュリティ対策意識に変化はなかった |
| 3. | セキュリティ対策意識は低くなった |

|  |  |
| --- | --- |
| Q2.本事業に参加して、感じたことがあれば教えてください。（いくつでも） | |
| 1. | UTM機器を設置し、出入口対策の必要性を感じた |
| 2. | 標的型攻撃メール訓練を受けて、攻撃メール対策の必要性を感じた |
| 3. | インシデント発生時の体制構築の必要性を感じた |
| 4. | セキュリティ対策の相談窓口（社内人材or外部有識者等）の必要性を感じた |
| 5. | セキュリティに関する社員教育の必要性を感じた |
| 6. | その他 |
|  | （その他フリーアンサー） |

|  |  |
| --- | --- |
| Q3.サイバーセキュリティ対策に関して、現在の貴社の課題を教えてください。 | |
| 1. | セキュリティポリシーの策定 |
| 2. | 管理体制の構築 |
| 3. | リスクの洗い出し、評価 グループ会社、取引先も含めた対策の実施 |
| 4. | セキュリティ対策費予算の確保 |
| 5. | セキュリティ対策専門人材の確保 |
| 6. | インシデント発生時の体制の構築 |
| 7. | 情報収集（最新技術動向や事故事例） |
| 8. | なし |

|  |  |
| --- | --- |
| Q4.現在、貴社で導入しているサイバーセキュリティ対策をお教えください。(いくつでも) | |
| 1. | ウイルス対策ソフト |
| 2. | 出入口対策（UTM等の設置） |
| 3. | 社員教育 |
| 4. | セキュリティ管理者の設置 |
| 5. | セキュアな無線環境 |
| 6. | セキュアな拠点間通信 重要なファイルのバックアップ |
| 7. | サイバーリスク保険加入 セキュリティポリシーの策定 |

|  |  |
| --- | --- |
| Q5.現在、セキュリティ対策にかけている月額費用はいくらぐらいですか。 | |
| 1. | 3,000円以下 |
| 2. | 3,000円～5,000円 |
| 3. | 5,000円～10,000円 |
| 4. | 10,000円～20,000円 |
| 5. | 20,000円～ |
| 6. | 費用はかけていない |

|  |  |
| --- | --- |
| Q6.今後、導入を検討したいサイバーセキュリティ対策をお教えください。（いくつでも） | |
| 1. | ウイルス対策ソフト |
| 2. | 出入口対策（UTM等の設置） |
| 3. | 社員教育 |
| 4. | セキュリティ管理者の設置 |
| 5. | セキュアな無線環境 |
| 6. | セキュアな拠点間通信 |
| 7. | 重要なファイルのバックアップ |
| 8. | サイバーリスク保険加入 |
| 9. | セキュリティポリシーの策定 |
| 10. | その他 |
|  | （その他フリーアンサー） |

|  |  |
| --- | --- |
| Q7.今後、セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。 | |
| 1. | 3,000円以下 |
| 2. | 3,000円～5,000円 |
| 3. | 5,000円～10,000円 |
| 4. | 10,000円～20,000円 |
| 5. | 20,000円～ |
| 6. | 費用をかけるつもりはない |

|  |  |
| --- | --- |
| Q8.情報漏えいやシステム停止などのインシデントが発生した場合の対応（役割・手順・連携先等）を決めていますか。 | |
| 1. | 決めている |
| 2. | 決めていない |
| 3. | 検討中 |

|  |  |
| --- | --- |
| Q9.情報漏えいやシステム停止などのインシデント発生した場合の業務への影響として想定しているものを教えてください。 | |
| 1. | 影響の範囲（親会社・サプライチェーンなどへの影響） |
| 2. | 対応にかかる費用(システム復旧、損害賠償等) |
| 3. | 対応にかかる労力（人件費） |
| 4. | 売上・事業への影響 |
| 5. | その他 |
|  | （その他フリーアンサー） |

|  |  |
| --- | --- |
| Q10.本事業で実施した標的型攻撃メール訓練についてお聞きします。送付された訓練メールについて、不審に感じた点はどこですか。（いくつでも） | |
| 1. | メールの件名、本文 |
| 2. | 差出人の名前や送信元のメールアドレス |
| 3. | 添付ファイルのファイル名 |
| 4. | 特に不審な点はなかった |
| 5. | その他 |
|  | （その他フリーアンサー） |

|  |  |
| --- | --- |
| Q11.取引先から貴社のサイバーセキュリティ対策について尋ねられたことはありますか。 | |
| 1. | ある |
| 2. | ない |

|  |  |
| --- | --- |
| Q12.今後、セキュリティ対策支援事業において実施してほしい内容がありましたらお教えください。（３つまで） | |
| 1. | セキュリティ対策に役立つ情報の提供 |
| 2. | 出入口対策（UTM等の設置） |
| 3. | セキュリティ管理者の育成 |
| 4. | 自社システム・NWのセキュリティ診断 |
| 5. | セキュリティインシデントの対応実習 |
| 6. | セキュリティに関する社内規定等の作成支援 |
| 7. | 社員に対するセキュリティセミナー |

|  |
| --- |
| Q13.サイバーセキュリティに関するご意見・ご要望を自由にご記入ください。（自由回答・任意） |

① Q1.本事業参加前と参加後で、サイバーセキュリティ対策に関する意識に変化があれば教えてください。

　69%の企業が、セキュリティ意識が高まったと回答しており、中小企業のサイバーセキュリティ対策意識の向上に役立った。セキュリティ意識に変化はなかったと回答した企業31%の多くは、もともとセキュリティ対策意識を持っており、セキュリティ対策の重要性を再認識したと解釈できる。

|  |  |
| --- | --- |
| 図 5‑1 Q1への回答（全体） | ＜図の数字＞  社数、割合（％）  ＜凡例＞ |

② Q2.本事業に参加して、感じたことがあれば教えてください。（いくつでも）

　企業規模の大小にかかわらず、本事業でサイバーセキュリティ対策の重要性を感じている。UTM機器の設置は、いずれの企業規模においても50%以上の企業が必要性を感じており、意識改革のきっかけとなった。人材育成や体制構築については、企業規模が大きいほど、意識が高まった傾向であるが、いずれも50%未満にとどまり、インフラ整備に意識が偏重していることがうかがえる。

図 5‑2 Q2への回答（全体）

その他の回答

* 設置したばかりなのでまだ分かりません

③ Q3.サイバーセキュリティ対策に関して、現在の貴社の課題を教えてください。

　課題認識については、企業規模にかかわらずばらつきが出た。総じて企業規模が大きいほど、課題認識も強い傾向となった。その中でも、21～100名規模の会社の管理体制の構築、インシデント発生時の体制の構築に対する課題意識は、他の企業規模の会社の課題意識に比べて高く、事業拡大に伴い、組織管理の在り方を見直すきっかけとなったと考えられる。

図 5‑3 Q3への回答（全体）

④ Q4.現在、貴社で導入しているサイバーセキュリティ対策をお教えください。(いくつでも)

　ウイルス対策ソフトはほとんどの企業で導入している。それ以外は今後導入が期待される。UTMの設置やファイルのバックアップ、セキュアな拠点間通信といった、システム整備については比較的導入が進みつつあるが、社員教育やセキュリティポリシー策定、サイバーリスク保険加入といった、運用については導入が進んでいないという結果となった。

図 5‑4 Q4への回答（全体）

⑤ Q5.現在、セキュリティ対策にかけている月額費用はいくらぐらいですか。

　企業規模が大きいほど、セキュリティ対策にかけている月額費用は高いという結果となった。人数が多い分、パソコン導入台数も多いため、ウイルス対策ソフトのライセンス数が多いためと考えられる。費用はかけていないと回答した企業は、ライセンス費用は年払いであり、月額費用ではないと解釈したものと想定される。

|  |  |
| --- | --- |
| 図 5‑5 Q5への回答（全体） | 図 5‑6 Q5への回答（～20名） |
| 図 5‑7 Q5への回答（21～100名） | 図 5‑8 Q5への回答（101名～） |
| ＜凡例＞ | |

⑥ Q6.今後、導入を検討したいサイバーセキュリティ対策をお教えください。（いくつでも）

　企業規模にかかわらず、UTM等の設置の割合が高い、という結果となった。ウイルス対策ソフトの導入については、パターンファイルの最新化を想定して回答した企業が一定数存在するものと考えられる。20名以下の企業は、重要なファイルのバックアップの比率も高く、システム面での整備を検討するきっかけとなった。21～100名の企業は社員教育の意識が高まった。101名以上の企業は、セキュリティポリシーの策定の意識が高まった。しかし、いずれも参加企業の半数には到達せず、運用面に対する意識はシステム面に比べて相対的に低い。

図 5‑9 Q6への回答（全体）

⑦ Q7.今後、セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

　本質問については、今後の月額費用と解釈した企業と、現在の月額費用に加える必要のある費用と解釈した企業が混在したと考えられる。他の回答内容から、今後セキュリティ対策にかける月額費用を減額する企業はないものと推察される。

|  |  |
| --- | --- |
| 図 5‑10 Q7への回答（～20名） | 図 5‑11 Q7への回答（21～100名） |
| 図 5‑12 Q7への回答（101名～） | ＜凡例＞ |

⑧ Q8.情報漏えいやシステム停止などのインシデントが発生した場合の対応（役割・手順・連携先等）を決めていますか。

　検討中も含め、2名～100名規模の企業が、インシデントが発生した場合への備えの意識が高いという結果となった。これは、管理体制構築（Q3）を課題と考える企業が多かったことに連動しているものと予想される。

|  |  |
| --- | --- |
| 図 5‑13 Q8への回答（～20名） | 図 5‑14 Q8への回答（21～100名） |
| 図 5‑15 Q8への回答（101名～） | ＜凡例＞ |

⑨ Q9.情報漏えいやシステム停止などのインシデント発生した場合の業務への影響として想定しているものを教えてください。

　企業規模にかかわらず、半数近くの企業がインシデント発生時の影響を懸念している。影響は想定しつつも、回答の傾向からは、システムの整備（既知のウイルスの予防）段階であり、運用（未知のウイルスの予防としての社員教育、事後対策としての社員教育や保険加入）への対応まで至らない企業が多いと考えられる。

図 5‑16 Q9への回答（全体）

その他の回答

* あまり想定していません
* 具体的には想定していない

⑩ Q10.本事業で実施した標的型攻撃メール訓練についてお聞きします。送付された訓練メールについて、不審に感じた点はどこですか。（いくつでも）

　訓練メールに気付いたのは、メール件名、本文、アドレスといった、こちらの意図した内容に対する気づきが多かった。一方、添付ファイルのファイル名に不審を感じた企業や、特に不審な点はなかったと回答した企業もあり、社員教育によるセキュリティ意識のレベルアップの必要性が顕在化したと考えられる。

図 5‑17 Q10への回答（全体）

その他の回答

* 訓練メールに気づかなかった（2社）
* テストメール内容を把握していない為、回答できませんでした。
* 未実施（2社）
* 『標的型攻撃メール訓練』は行なっていません。
* まだ来ていないのではないかと思われます。（2社）

⑪ Q11.取引先から貴社のサイバーセキュリティ対策について尋ねられたことはありますか。

　100名以下の企業では、40%程度がサイバーセキュリティ対策について取引先から確認されている。一方、101名以上の企業は25%程度となっている。101名規模の会社であれば、サイバーセキュリティ対策は当然実施しているものと取引先自体が判断しているのではないかと考えられる。

|  |  |
| --- | --- |
| 図 5‑18 Q11への回答（～20名） | 図 5‑19 Q11への回答（21～100名） |
| 図 5‑20 Q11への回答（101名～） | ＜凡例＞ |

⑫ Q12.今後、セキュリティ対策支援事業において実施してほしい内容がありましたらお教えください。（３つまで）

　どの企業規模においても、具体的な取組よりも、セキュリティ対策に役立つ情報の提供を期待している傾向となった。具体的な施策への落とし込みというよりは、自社の状況を見極め、優先順位を決めて対策するための検討への支援を期待されていると想定される。

図 5‑21 Q12への回答（全体）

⑬ Q13.サイバーセキュリティに関するご意見・ご要望を自由にご記入ください。（自由回答・任意）

会社規模（～20名）

* サイバー攻撃、ウイルス感染した場合にNTTで対応してくれる窓口を用意してもらいたい。
* UTMに関しては、必要性をあまり感じていません。
* 月次リポートをお送りいただいておりますが、専任の人員がいないため内容が理解できない部分が多いです。

会社規模（21～100名）

* 当社ではセキュリティ管理者を選任で儲けることが難しい。そのため、包括的にセキュリティ関連のサービスをお任せできると助かります。
* 今回無償でUTMを試せるのは有難いと思ったので参加したが、試す期間が短く、今後の検討をするにも時間が足りなかった。もう少し余裕を持って検討できれば良かった。ただ、中々費用を掛ける項目に上がりづらい内容（保険のようなもの）なので、社内で議題に上げられただけでも良かったと思う。

会社規模（101名～）

* これまでは機器が設置されていただけで機能しているのか不確かだったので、今後利用を開始するNTTのUTMとサポートサービスには期待している。
* 今回のUTM導入にあたり、サイバーセキュリティの足掛かりとなり、セキュリティ意識が高まったものの、依然としてサイバーセキュリティ対策に後れを取っている感がある為、引き続きサイバーセキュリティに関する情報、サービス提案を希望。
* 具体的なリスク事例情報を知りたいです。
* 今後も引き続き定期的な情報提供してください

今回非常に効果的なご提案頂きお礼申し上げます。今後ともご指導・ご鞭撻賜りますようお願い申し上げます。

## **支援終了時の個社ヒアリングの結果**

本事業の支援対象企業のうち、サイバーセキュリティ意識の高低や支援事業から得た情報、企業属性を鑑み、5社を選定し、ヒアリングを実施。ヒアリング内容は、アンケート調査をベースに深堀を行った。

詳細のヒアリング内容は以下の通り。

1. ヒアリング内容

|  |  |
| --- | --- |
| Q1 | 毎日働く中で、情報セキュリティ的観点で気になっていることはありますか |
| Q2 | 会社として何か取り組んでいることはありますか |
| Q3 | 脅威と感じていて、対策が必要だと思うセキュリティ脅威について、どうしてそう考えるのですか |
| Q4 | セキュリティ対策を導入するうえでの相談できる方（社内外問わず）はいらっしゃいますか |
| Q5 | 情報セキュリティ対策を行いたくても行なえない領域・事情・環境等ありますか |
| Q6 | 取引先とのやりとりで気を付けていることはありますか |
| Q7 | 社内のやりとりで気を付けていることはありますか |
| Q8 | （テレワークを実施している企業への質問） 社内のやりとりで気を付けていることはありますか |
| Q9 | （テレワークを実施している企業への質問） 新型コロナウイルス感染拡大前からテレワークを実施していますか。コロナウイルス感染拡大に伴い導入したのですか |
| Q10 | （テレワークを実施している企業への質問）セキュリティ対策ルールはありますか |
| Q11 | （テレワークを実施していない企業への質問）テレワーク導入に関する懸念事項はありますか |
| Q12 | 具体的なセキュリティサービスの導入状況について教えてください |
| Q13 | セキュリティサービスを導入する場合、誰が、どのような検討を行い、導入に至りますか |
| Q14 | 本支援事業をきっかけにセキュリティ意識に変化はありましたか。また、具体的な対策は講じましたか |

（２）個別ヒアリング内容

1. Ａ社

＜ヒアリング日＞　令和3年2月25日（木）

＜ヒアリング対象企業基本情報＞

|  |  |
| --- | --- |
| 業種 | 不動産業、物品賃貸業 |
| 従業員規模 | 130人 |
| テレワーク実施有無 | 週3日以上実施 |
| ヒアリング回答者 | 施設管理部　副部長 |

＜ヒアリング内容＞

Q1. 毎日働く中で、情報セキュリティ的観点で気になっていることはありますか

|  |
| --- |
| 社員一人一人のセキュリティ意識に差がある。 |

Q2. 会社として何か取り組んでいることはありますか

|  |
| --- |
| 課題意識は持っているが、特段セキュリティ教育等は行っていない。担当している部署はなく、コンピュータに詳しい人もいない。 |

Q3. 脅威と感じていて、対策が必要だと思うセキュリティ脅威について、どうしてそう考えるのですか

|  |
| --- |
| 社員のセキュリティ意識の差があり、迷惑メールを開いてしまう等（ランサムウェア等にかかった経験はない） |

Q4. セキュリティ対策を導入するうえでの相談できる方（社内外問わず）はいらっしゃいますか

|  |
| --- |
| ・親会社。  NWは親会社のものを利用しており、大もとのセキュリティ対策は実施しているので安心している（出口のファイアウォールは親会社のものを利用）  ・ベンダー（親会社とは別会社） |

Q5. 情報セキュリティ対策を行いたくても行なえない領域・事情・環境等ありますか

|  |
| --- |
| 現在は親会社が大規模に行っておりカバーできているから良いが、自社だけでは難しい（親会社に準拠している限りは基本的には安心できる部分が多い） |

Q6. 取引先とのやりとりで気を付けていることはありますか

|  |
| --- |
| メール送付時に添付ファイルにパスワード（zip化）を付ける。メール以外は特になし。 |

Q7. 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| 特にない。良くないと思いつつも、メールでのファイルのやりとりが主。最近はメール添付ではなく、OneDrive等に切り替えていかなければいけないと考えている |

Q8.（テレワークを実施している企業への質問） 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| 私物端末を利用（会社が補助金を出して購入してもらっている）。  私物パソコンからメールの送受信を行っており、会社でしか出来ない業務についてはリモート接続し、利用している（ポイントポイントでリモート接続している）。 |

Q9.（テレワークを実施している企業への質問） 新型コロナウイルス感染拡大前からテレワークを実施していますか。コロナウイルス感染拡大に伴い導入したのですか

|  |
| --- |
| コロナ前はテレワークの利用はなし。ここ半年くらいで環境を整えて実施。 |

Q10.（テレワークを実施している企業への質問） セキュリティ対策ルールはありますか

|  |
| --- |
| 明確化していない。コロナ禍で走りながら行っているのであいまいな状況。 |

Q11.テレワーク実施済み企業のため質問割愛

Q12. 具体的なセキュリティサービスの導入状況について教えてください

|  |
| --- |
| ウイルス対策ソフトを利用。  今までは親会社から指定のものを導入していたが、今後は自社で独自に対応しなければならなくなり、セキュリティ対策が急務。 |

Q13. セキュリティサービスを導入する場合、誰が、どのような検討を行い、導入に至りますか

|  |
| --- |
| 回答者がサービス等を見つけて提案し、総務担当にて決裁し導入。社内に詳しい人がいないので、一人で情報収集（ベンダー等を通じて）行っている。 |

Q14. 本支援事業をきっかけにセキュリティ意識に変化はありましたか。また、具体的な対策は講じましたか

|  |
| --- |
| 特別なことは行っていないが、どのようなセキュリティ対策ができるか、どのようなリスクがあるか考えるようになった。 |

1. Ｂ社

＜ヒアリング日＞　令和3年3月1日（月）

＜ヒアリング対象企業基本情報＞

|  |  |
| --- | --- |
| 業種 | 情報通信業 |
| 従業員規模 | 3人 |
| テレワーク実施有無 | 週3日以上実施 |
| ヒアリング回答者 | 代表取締役 |

＜ヒアリング内容＞

Q1. 毎日働く中で、情報セキュリティ的観点で気になっていることはありますか

|  |
| --- |
| 業務上、情報収集や担当する業務について、ネットで検索することが多い。そのため意図せず危険なサイトにアクセスしてしまわないか常に心配している。セキュリティソフトは常時必要と感じ、導入している。ウイルス対策ソフトは各PCに入っている。ウイルス対策ソフトに付随して、簡易的なものではあるがファイアウォール機能やメールのチェック機能がついている法人向けセキュリティソフトを利用している。 |

Q2. 会社として何か取り組んでいることはありますか

|  |
| --- |
| 会社としてはセキュリティソフトを導入している。（業務を行っていてPCがおかしい等）何かあった際は早めの報告をもらっている。今のところ被害等の報告事例はない。 |

Q3. 脅威と感じていて、対策が必要だと思うセキュリティ脅威について、どうしてそう考えるのですか

|  |
| --- |
| 業務上、いわゆる18禁と呼ばれている業務も入っており、そういう会社は広告等ポップアップで対応されていることが多く、気を付けないといけないと考えている。特に被害にあった訳ではないがヒヤリとする事があり、数年前から基本的に法人向けセキュリティソフトに切り替えている。 |

Q4. セキュリティ対策を導入するうえでの相談できる方（社内外問わず）はいらっしゃいますか

|  |
| --- |
| 知り合いのシステムエンジニアがセキュリティも含めてかなり詳しいので、最近の機器やセキュリティソフトの動向等の情報収集を行っている（ベンダー等ではない）。 |

Q5. 情報セキュリティ対策を行いたくても行なえない領域・事情・環境等ありますか

|  |
| --- |
| 今は特に感じていない。行おうと思えば網羅的にセキュリティ対策を行えており、現状問題はない。 |

Q6. 取引先とのやりとりで気を付けていることはありますか

|  |
| --- |
| 日々のファイルはメール添付でやり取りしているが、納品物や初期の相手先からの重要資料等は、メール添付や外部のストレージ、無料ファイル転送サービス等は極力利用せず、自社で法人契約しているOffice365の領域内にあるOneDriveでやり取りするよう心掛けている。名目上、セキュリティ担保されているものを利用している。 |

Q7. 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| 簡単なものはメール添付やWeb会議上で画面共有を行っている。納品物や気を付けるべき資料についてはOneDriveの領域に格納してやり取りしている。 |

Q8.（テレワークを実施している企業への質問） 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| ノートPCを会社から支給。移動中は私物のスマホを利用する場合もあるが、緊急時以外はノートPCを利用するよう指示している。  シンクライアントシステムやクラウドではなく、スタンドアローンのPCを利用。 |

Q9.（テレワークを実施している企業への質問） 新型コロナウイルス感染拡大前からテレワークを実施していますか。コロナウイルス感染拡大に伴い導入したのですか

|  |
| --- |
| 昨年3月の緊急事態宣言時から開始。 |

Q10.（テレワークを実施している企業への質問） セキュリティ対策ルールはありますか

|  |
| --- |
| 簡素な物だが気を付ける点を記載したものを頒布した。気を付けるポイント等は社員に共有しているが、それがきちんとしたルールかと言われると何とも言えない。そういった点をサポートしていただける「最低限抑えてほしいポイント」のような雛形があるとよい。弊社も含めて小さい会社でセキュリティやPCが得意ではない会社になればなるほど、何を抑えるべきかわからないので、ルールの雛形（ポイント集）があるといいと感じている。 |

Q11.テレワーク実施済み企業のため質問割愛

Q12. 具体的なセキュリティサービスの導入状況について教えてください

|  |
| --- |
| 各PCについてはセキュリティソフト（法人サービス）を利用。NASを利用しているのでNAS専用のセキュリティ対策ソフトを利用している。 |

Q13. セキュリティサービスを導入する場合、誰が、どのような検討を行い、導入に至りますか

|  |
| --- |
| 回答者が選定し（今は無料期間があるのものが中心）、管理領域が使いやすいかを検証。実際に使用して、PCが遅くならないか、業務上支障が出ていないか等、現場にもテスト導入して様子見し、問題がなければ導入。改善が必要であれば別のものを検討している。最終的には現場の意見をふまえて決めている。 |

Q14. 本支援事業をきっかけにセキュリティ意識に変化はありましたか。また、具体的な対策は講じましたか

|  |
| --- |
| 改めて本事業に参加・導入することを社員に伝えたので、社員へ意識づけできたかと思う。管理領域に入って、確認頻度を上げている。 |

1. Ｃ社

＜ヒアリング日＞　令和3年3月2日（火）

＜ヒアリング対象企業基本情報＞

|  |  |
| --- | --- |
| 業種 | 建設業 |
| 従業員規模 | 107人 |
| テレワーク実施有無 | 導入していない |
| ヒアリング回答者 | 担当者 |

＜ヒアリング内容＞

Q1. 毎日働く中で、情報セキュリティ的観点で気になっていることはありますか

|  |
| --- |
| メールでの添付ファイル送付が気掛かり。添付ファイルをクリックしたことにより、使用しているクライアントコンピュータへのリスク、情報流出やデータ消出、マルウェア等の心配事がある。 |

Q2. 会社として何か取り組んでいることはありますか

|  |
| --- |
| ユーザへの注意喚起。効果は定かではないが、各クライアントにセキュリティソフトを導入している。 |

Q3. 脅威と感じていて、対策が必要だと思うセキュリティ脅威について、どうしてそう考えるのですか

|  |
| --- |
| ニュースも含めてだが、実際に不審なメールが送られてきて、ユーザから問い合わせがあったり、社内から不審メールのエスカレーションがあったり等、ウイルスには感染しなかったがヒヤリハットすることがあった。元請先（ゼネコン）や取引先の名前を名乗って送られてくる。メールの中身を確認すると辻褄が合っていないのでわかるが、アドレスだけで判断するのは難しい。 |

Q4. セキュリティ対策を導入するうえでの相談できる方（社内外問わず）はいらっしゃいますか

|  |
| --- |
| システムベンダ―。クライアントに導入しているセキュリティソフト以外で、UTM等の複合的なセキュリティ対策の提案をいただいている。 |

Q5. 情報セキュリティ対策を行いたくても行なえない領域・事情・環境等ありますか

|  |
| --- |
| BtoB（一対一のつながり）がメインで、いわゆるコンシューマーとのやり取りはないため、特に気にしていない（元請先とのやりとりのみ） |

Q6. 取引先とのやりとりで気を付けていることはありますか

|  |
| --- |
| メール送付は気に掛けている。それ以外で特に思いつくことはない。 |

Q7. 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| 基本的に拠点間はメールがメイン。同じようにメール送付は気に掛けている |

Q8.テレワーク未導入企業のため質問割愛

Q9.テレワーク未導入企業のため質問割愛

Q10.テレワーク未導入企業のため質問割愛

Q11. テレワーク導入に関する懸念事項はありますか

|  |
| --- |
| テレワークではなく、時間をズラしても出勤や三密回避を実施している。  書類を扱う（紙が必要）仕事が多く、個人が持っていると不都合なためどうしても社内に置いている。そのため、なかなかテレワークが出来ない。 |

Q12. 具体的なセキュリティサービスの導入状況について教えてください

|  |
| --- |
| ウイルス対策ソフトを利用（個人向け）と今回、本支援事業で導入したUTM。 |

Q13. セキュリティサービスを導入する場合、誰が、どのような検討を行い、導入に至りますか

|  |
| --- |
| 回答者が検討して導入。 |

Q14. 本支援事業をきっかけにセキュリティ意識に変化はありましたか。また、具体的な対策は講じましたか

|  |
| --- |
| 本支援事業でUTMを設置してまだ短期間なので、レポートを見て精査したい。攻撃型メール訓練1回目で開封してしまったが、セキュリティ意識醸成に役立った。 |

1. Ｄ社

＜ヒアリング日＞　令和3年3月2日（火）

＜ヒアリング対象企業基本情報＞

|  |  |
| --- | --- |
| 業種 | 金融業、保険業 |
| 従業員規模 | 49人 |
| テレワーク実施有無 | 導入していない |
| ヒアリング回答者 | 管理部　管理本部長 |

＜ヒアリング内容＞

Q1. 毎日働く中で、情報セキュリティ的観点で気になっていることはありますか

|  |
| --- |
| 漠然と情報セキュリティ全般に不安を感じている。 |

Q2. 会社として何か取り組んでいることはありますか

|  |
| --- |
| 本日、NTT担当者より本支援事業のレポート説明をいただいたので今後、具体的に取り組んでいきたい。細かいところでは、OSのアップデートから1つ1つ進めていこうと考えている。また、ウイルスソフトを導入している。 |

Q3. 脅威と感じていて、対策が必要だと思うセキュリティ脅威について、どうしてそう考えるのですか

|  |
| --- |
| スパムメールが多いことや、フィッシングが話題になっており、ニュースを見て対策が必要だと感じている。直接不審なメールが届いたことはない。ウイルス対策ソフトを利用しているが全てが防げるものでもない（すり抜けてくることもある）と感じている。 |

Q4. セキュリティ対策を導入するうえでの相談できる方（社内外問わず）はいらっしゃいますか

|  |
| --- |
| 今後はNTT担当者が第一の窓口になると思っている。 |

Q5. 情報セキュリティ対策を行いたくても行なえない領域・事情・環境等ありますか

|  |
| --- |
| 特にないと思う。金融商品仲介業なので、親会社のサーバを経由して業務を行っている。顧客情報は親会社が管理しており、端末で情報を確認した後のセキュリティ管理は弊社となるが、特にない認識。直接顧客情報の管理は行っていない。 |

Q6. 取引先とのやりとりで気を付けていることはありますか

|  |
| --- |
| 専用ポータルを通じて実施している。  個人情報が入ったメールのやりとりは行わない。メール送付が必要な時は必ず暗号化している。 |

Q7. 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| 特にない。個人情報はパスワードでガードして送付している。 |

Q8.テレワーク未導入企業のため質問割愛

Q9.テレワーク未導入企業のため質問割愛

Q10.テレワーク未導入企業のため質問割愛

Q11. テレワーク導入に関する懸念事項はありますか

|  |
| --- |
| 個人情報を扱っており、セキュリティの観点から会社の端末から確認することになっている。  セキュリティ端末は最低2名以上でないとアクセスできない等の制約があり、取引先からの条件を加味するとテレワークは難しい。 |

Q12. 具体的なセキュリティサービスの導入状況について教えてください

|  |
| --- |
| ウイルス対策ソフト（トレンドマイクロ：ウイルスバスター個人向け）  他に、本支援施策で導入したUTM。 |

Q13. セキュリティサービスを導入する場合、誰が、どのような検討を行い、導入に至りますか

|  |
| --- |
| 回答者で検討の上、役員等に相談し、話し合いで決定。 |

Q14. 本支援事業をきっかけにセキュリティ意識に変化はありましたか。また、具体的な対策は講じましたか

|  |
| --- |
| 本日、説明を受けたこともあるが、OSのアップデートを行うよう、社員教育が必要と感じた。 |

1. Ｅ社

＜ヒアリング日＞　令和3年3月4日（木）

＜ヒアリング対象企業基本情報＞

|  |  |
| --- | --- |
| 業種 | 宿泊業、飲食店 |
| 従業員規模 | 200人 |
| テレワーク実施有無 | 週3日以上実施 |
| ヒアリング回答者 | 管理部取締役 |

＜ヒアリング内容＞

Q1. 毎日働く中で、情報セキュリティ的観点で気になっていることはありますか

|  |
| --- |
| 特にない。何もしていないことが気になっている。 |

Q2. 会社として何か取り組んでいることはありますか

|  |
| --- |
| 特にない。ウイルス対策ソフトの導入なし。 |

Q3. 脅威と感じていて、対策が必要だと思うセキュリティ脅威について、どうしてそう考えるのですか

|  |
| --- |
| 特にない |

Q4. セキュリティ対策を導入するうえでの相談できる方（社内外問わず）はいらっしゃいますか

|  |
| --- |
| いない |

Q5. 情報セキュリティ対策を行いたくても行なえない領域・事情・環境等ありますか

|  |
| --- |
| ない |

Q6. 取引先とのやりとりで気を付けていることはありますか

|  |
| --- |
| 個人情報はメールに掲載しない・ファイル添付しない（担当によっては他のツールを利用しているかもしれないが、状況は把握していない）。 |

Q7. 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| 特にない。セキュリティポリシー的なものも作成していない。 |

Q8.（テレワークを実施している企業への質問） 社内のやりとりで気を付けていることはありますか

|  |
| --- |
| 端末は会社貸与。クラウド上で作業している。 |

Q9.（テレワークを実施している企業への質問） 新型コロナウイルス感染拡大前からテレワークを実施していますか。コロナウイルス感染拡大に伴い導入したのですか

|  |
| --- |
| 回答なし |

Q10.（テレワークを実施している企業への質問） セキュリティ対策ルールはありますか

|  |
| --- |
| 特になし。 |

Q11.テレワーク実施済み企業のため質問割愛

Q12. 具体的なセキュリティサービスの導入状況について教えてください

|  |
| --- |
| 何もなし。ウイルス対策ソフトもなし。 |

Q13. セキュリティサービスを導入する場合、誰が、どのような検討を行い、導入に至りますか

|  |
| --- |
| 回答者にて検討し決定。 |

Q14. 本支援事業をきっかけにセキュリティ意識に変化はありましたか。また、具体的な対策は講じましたか

|  |
| --- |
| 何かセキュリティ対策をしないといけないと考えている。具体的な対策はNTTと検討を始めた。 |

今回個別にヒアリングをした企業は、サイバーセキュリティ対策導入状況や業務上の対応等については、各社の業務内容や環境、考え方によって様々であることが分かった。企業によりITの利用範囲や業務内容が異なるため、一様に推奨されるサイバーセキュリティ対策は存在せず、自社の業務内容に適したサイバーセキュリティ対策を講じることが求められる。

対象企業においては、本事業をきっかけにして、セキュリティ意識が向上したといえる。

# **まとめ・提言**

## **企業におけるサイバーセキュリティ対策のあるべき姿**

業務効率化や生産性向上のため既に多くの企業がITを活用している。その際、サイバーセキュリティの必要性や重要性を強く意識し、対策を講じたうえでITを活用することが求められる。サイバーセキュリティ対策が不十分なまま万一サイバー攻撃を受けてしまった場合、その企業は様々な不利益を被る可能性や、法的責任が問われる可能性があるためだ。

サイバー攻撃に対するセキュリティ対策には物理的対策や技術的対策に加え、組織的対策、人的対策が含まれる。これらの対策には費用を要するため、サイバーセキュリティ対策の費用対効果をふまえて必要な投資を行うことが企業のあるべき姿といえる。

サイバー攻撃による影響範囲や想定被害額を考慮し、自社にとって適切なセキュリティ対策投資を行う必要がある。加えて、様々なセキュリティ対策を講じてもリスクは残るため、この残留リスクをどこまで許容するかには経営判断が求められる。UTM等のセキュリティ機器の有効性は本事業の支援によって中小企業も知るところとなったが、そのような物理的対策はどれだけ投資してもその残留リスクは残ることから、従業員の教育等の人的対策や組織的対策も行うことが重要であると考えられる。

また、本事業における2度のアンケートの結果や、5.2に記したヒアリングの結果からもうかがえるとおり、企業によりITの利用範囲や内容が異なるため、一様に推奨されるサイバーセキュリティ対策は存在しない。企業には、自社の業務内容に適したサイバーセキュリティ対策を講じることが求められる。

その際、情報セキュリティ対策診断（例：IPAがウェブサイトにて公開している「情報セキュリティ対策ベンチマーク」[[16]](#footnote-16)等）を行うことが有益となる。その結果を参考に、取り組むべきセキュリティ対策や強化すべき対策を把握し、費用対効果を見極めながら対策を講じていくことが推奨される。

## **新たなサービス・支援事業等に関する提言**

＜新たなサービスに関する提言＞

企業の働き方はますます多様化が進み、様々な場所から様々なNWやデバイスを利用し企業の機密情報にアクセスしているのが現状。

本事業参加企業のセキュリティ対策の実態や課題を踏まえ、企業のサイバーセキュリティ対策として導入を推奨するサービスについて以下の通り考察する。

1. クラウドアプリケーション向けのセキュリティ対策

社内やテレワーク先で利用するためのツールとして手軽に導入・運用できるMicrosoft 365やGoogle Workspaceに代表されるSaaSサービスを活用し、メール、ストレージ、コミュニケーションツールを利用する企業が増加している。3.1に記載したアンケート結果でも示す通り本事業参加中小企業においても41％はテレワークを導入済みであり、今後クラウドアプリケーションの利用はますます高まると想定される。

4.3で記載した通り、クラウドアプリケーションにおいてもサイバー攻撃を受ける可能性は大きい。このようなSaaS型サービスはその構成上、元々企業が用意している社内防御機能（UTM、FW等）が働かないケースが増えるため、SaaS型サービスに特化したセキュリティ対策が必要である。

1. エンドポイントセキュリティ対策の強化（EDR[[17]](#footnote-17)）

EmotetやIcedID[[18]](#footnote-18)等に代表される新種、亜種マルウェアを活用した未知脅威の攻撃が拡大し、サイバーセキュリティ脅威の悪質化・巧妙化は日に日に進化している。セキュリティ対策のベースとなるGW型セキュリティ、エンドポイント型セキュリティ対策といった基本となる多層防御だけでは防ぎきれず、実際に取引先がマルウェア感染したという事例も散見される。

高度化を続ける脅威の侵入を完全に予防することは困難であるため、予防的対策だけに頼らず、脅威の侵入を前提として被害拡大を回避するための対策が必要である。EDRで、ホスト上のプロセスを監視し、組織内に侵入した未知の脅威を素早く検知し、影響範囲の特定と隔離等の対処を実現するセキュリティ対策が必要である。

＜中小企業向けの支援事業に関する提言＞

本事業において把握した実態の示す通り、中小企業はサイバーセキュリティ対策について関心はあるものの自社の直面する課題として認知できていない傾向があるが、我が事として捉えられる意識啓発をしたり対策導入や運用サポート等の支援を実施したりすることでセキュリティ対策向上は実現できる。本事業に参加した中小企業は、本事業を通じてサイバーセキュリティ対策が大企業だけでなく、自社も直面する問題であることを実感し、対策の必要性を認識したことは非常に有意義であった。多くの参加企業が現状ではセキュリティ対策は不十分であり、追加の対策が必要と認識し、常に進化するサイバー攻撃に対応するという心構えを持った。

今回参加された企業は、サイバーセキュリティ対策として、システム整備を検討しており、自己防衛の意識を強めている。しかし、世の中の働き方の多様化、デジタル化も進み、その時流に乗ってサイバー攻撃は常に進化する。そういったITの利用機会がますます広がることを見据え、企業が自社の業務内容に適したサイバーセキュリティ対策を講じることが実現できるように、各社のIT業務ツールの利用形態に即して、様々なNW・デバイスから機密情報にアクセスすることを前提とした意識啓発・サービス導入支援が必要求められる。

また、システム整備だけでは既知の攻撃への対処とだけではすべての攻撃を防ぎきれない可能性があることを考慮する必要がある。

そのためには、社員教育による判断力の向上や、セキュリティに関する体制の整備（セキュリティポリシー策定含む）及び、事後対応としてのセキュリティ保険への加入も選択肢として考える必要がある。企業単独では様々な制約により、多面的な視点での評価、対策が取れないこともある。企業の自助努力に加え、専門家を活用し、精緻な分析、多面的な評価による支援が必要と考えられる。専門家の客観的な視点により、自社の状況や今後の対応を冷静に判断し、適切な対応を行うことが、サイバーセキュリティから自社を守るうえで重要と考える。

1. 出典：経済産業省ウェブサイト（<https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html>） [↑](#footnote-ref-1)
2. 出典：経済産業省ウェブサイト「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」（<https://www.meti.go.jp/press/2020/12/20201218008/20201218008-1.pdf>）p6-p9 [↑](#footnote-ref-2)
3. 出典：独立行政法人情報処理推進機構ウェブサイト「情報セキュリティ10大脅威2021」（https://www.ipa.go.jp/security/vuln/10threats2021.html） [↑](#footnote-ref-3)
4. 独立行政法人情報処理機構ホームページ「情報セキュリティ10大脅威　2021～よもや自組織が被害に！呼吸をあわせて全力防御！～［組織編］」（<https://www.ipa.go.jp/files/000089239.pdf）p5、p75>を基に記載 [↑](#footnote-ref-4)
5. 出典：経済産業省ウェブサイト（<https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html>） [↑](#footnote-ref-5)
6. 回答企業数は101社であるが、業種未回答企業が1社、複数の業種に該当する企業が2社あるため、一致しない。 [↑](#footnote-ref-6)
7. IPSとは、Intrusion Prevention Systemの略で、不正侵入防止システムを指す。 [↑](#footnote-ref-7)
8. URLとは、Uniform Resource Locatorの略で、インターネット上のホームページ等の所在地を特定するための書式を指す。アドレスとも呼ばれる。 [↑](#footnote-ref-8)
9. TLSとは、Transport Layer Securityの略で、Webページにセキュリティ機能を追加する技術の一つ。TLSネゴシエーションでは、通信の相手側に適切にセキュリティ機能が具備されているかのやり取りを行う。 [↑](#footnote-ref-9)
10. C&Cとは、Command and Controlの略。ネットワーク内部から外部の攻撃者側のC&Cサーバに接続するとC&Cコールバックとなり、攻撃者に次なる攻撃の機会を与えてしまう。 [↑](#footnote-ref-10)
11. 「2021年3月」は、2021年3月12日までが対象。以降の表でも同じ。 [↑](#footnote-ref-11)
12. 括弧内はUTM設置企業のうちデータ送受信のあった企業数を示す。以降の表でも同じ。 [↑](#footnote-ref-12)
13. 括弧内はUTM設置企業のうちデータ送受信のあった企業数を示す。以降の検知件数を示す表においても同じ。 [↑](#footnote-ref-13)
14. 「脅威の可能性があるプログラム」として検知されたものの大多数は、パスワード付圧縮ファイル及びドキュメントであり、メール件名から「入館データ」や「店舗一覧」など顧客情報と推測できるため、パスワード保護は適切な処置であり脅威ではないと判断。 [↑](#footnote-ref-14)
15. 回答企業数は99社であるが、業種未回答企業が1社、複数の業種に該当する企業が2社あるため、一致しない。 [↑](#footnote-ref-15)
16. 参考：「情報セキュリティ対策ベンチマーク」独立行政法人情報処理機構ウェブサイト（https://www.ipa.go.jp/security/benchmark/） [↑](#footnote-ref-16)
17. Endpoint Detection and Responseの略語であり、出入口対策等で防御出来ずに侵入してきたウイルスや不正プログラムを検知し隔離等の対応をするサービス。 [↑](#footnote-ref-17)
18. メールやブラウザなどの情報を窃取するトロイの木馬型の不正プログラム。 [↑](#footnote-ref-18)