IPA Better Life with IT

令和4年度中小企業等に対するサイバー攻撃の実態調査

調査実施報告書

2023年4月

独立行政法人情報処理推進機構

セキュリティセンター

目次

1．報告書サマリー

- 取引先企業への攻撃の足掛かりとして、サイバー攻撃を受ける恐れが大きいと考えられる中小企業等を対象に、ネットワーク環境・セキュリティ対策の状況把握とネットワーク及び端末における異常を監視する等により、攻撃の実態について調査・分析した。

※調査にご協力いただいた企業の6割は、従業員数が100名超、あるいは売上高10億円超である。

ネットワーク環境・セキュリティ対策の状況把握

- ルール・ポリシーの有無、ネットワークのセキュリティ対策状況、セキュリティ製品の運用状況をヒアリングで確認。
- UTMを既に設置している企業が多かったものの、アラートの確認はベンダ任せになっている。
- ヒアリングで「できていない」と認識している事項として、ポリシー策定、USB対策、工場LAN対策が挙げられた。

産業分野	対象者数	UTM既設	アラート確認		
			自社	ベンダ	無し
半導体	5	3	0	2	1
自動車部品	24	17	1	16	0
航空部品	11	4	1	2	1
防衛装備	3	2	1	1	0

ネットワーク及び端末における異常監視

- 既設UTMレポートの活用と、新規にUTMを17者、EDRを30者に導入いただき、インターネット側から社内ネットワークへ届く攻撃や社内ネットワーク内で発生する不正な通信を監視した。
- ランサムウェアやC&Cサーバとの通信といったセキュリティ侵害に当たる攻撃は検知されなかった。
- 民間のUTM監視サービスや、過去のサイバーセキュリティお助け隊サービスの実証事業結果と比較しても、特定産業分野のサプライチェーンに属する企業ではインターネット側から攻撃が多く、内部侵入のきっかけになるような動作も多いことから、リスクがより高いと考えられる。

- ✓ **メールやWebを契機としたウイルス感染に対しては、UTMとEDRの双方で防ぎ、被害拡大を防止する事が有効。**
- ✓ **定期的に検知レポートを確認し、不審なアプリケーションやサイバー攻撃の兆候を把握し、対策を継続的に行うことが有効。**
- ✓ **セキュリティの有識者等適切な知識経験を有した人員によるネットワーク構成の確認や検証が有効。**

2．事業の目的および概要

事業の目的

本事業は、サプライチェーン全体のサイバーセキュリティ対策強化のために必要な対策や、その実装に向けて有効な業界全体としての取組みの検討に供する目的のもと、外部からの情報窃取や取引先企業への攻撃の足掛かりとしてのサイバー攻撃を受けるおそれが大きいと考えられる経済安全保障上重要となるサプライチェーン上の中小企業を対象に、ネットワーク環境・セキュリティ対策の状況について把握した上で、ネットワーク及び端末における異常を監視する等により攻撃の実態（数・手法・被害に遭った場合の影響など）について調査・分析を行った。

事業の概要

2.1 対象中小企業の選定

経済安全保障上重要かつ重要産業である「半導体」、「自動車部品」、「航空部品」の3分野の中小企業、及び防衛装備庁よりの紹介企業3者（以下、「防衛装備」と記す。）を加えた43者を選定した。

2.2 事前準備等の実施

調査の実施に先立って、対象中小企業等に対してセキュリティ専門家を派遣してヒアリングを実施し、対象中小企業等におけるネットワーク環境、及びセキュリティ対策状況について現況調査を実施した。

2.3 調査・分析の実施

本事業では、対象中小企業等において、UTM（Unified Threat Management）等のネットワークセキュリティ監視装置を用いて企業内外のネットワーク通信を監視するとともに、EDR（Endpoint Detection and Response）等のエンドポイントセキュリティソフトウェアを用いて企業内ネットワークに接続された端末における挙動を監視する等の方法により、対象中小企業のネットワーク及び端末の双方について一定期間監視し、ログを収集、統合的に分析した。分析にあたっては、インターネットからのサイバー攻撃、ネットワーク内部におけるマルウェアの感染拡大状況、及び不審な挙動、そしてその相関関係を明らかにすることにより、どれだけの数、どのような手法によりサイバー攻撃が行われているか、また、その侵入深度や経緯分析、仮に対処しなかった場合の被害想定額（理論値）についても分析を行った。

2.4 収集情報のフィードバック

本事業に参加する中小企業等に対して、調査により収集・分析した情報について、レポートの発行等を通じてフィードバックを実施した。対処が必要なサイバー攻撃等を検知した場合においてはその旨の通報・レポートの発行と合わせて推奨される対処方法を具体的に提示する等により、インシデント対応が必要である旨を対象中小企業等に覚知させた。

3．産業分野別の業界状況

- 本事業の前提として対象分野の状況を理解するため、各分野のサプライチェーン構造やセキュリティ対策の状況をデスクトップ調査により確認した。各分野のサイバーセキュリティリスクと業界としての取り組み状況は以下のとおり。

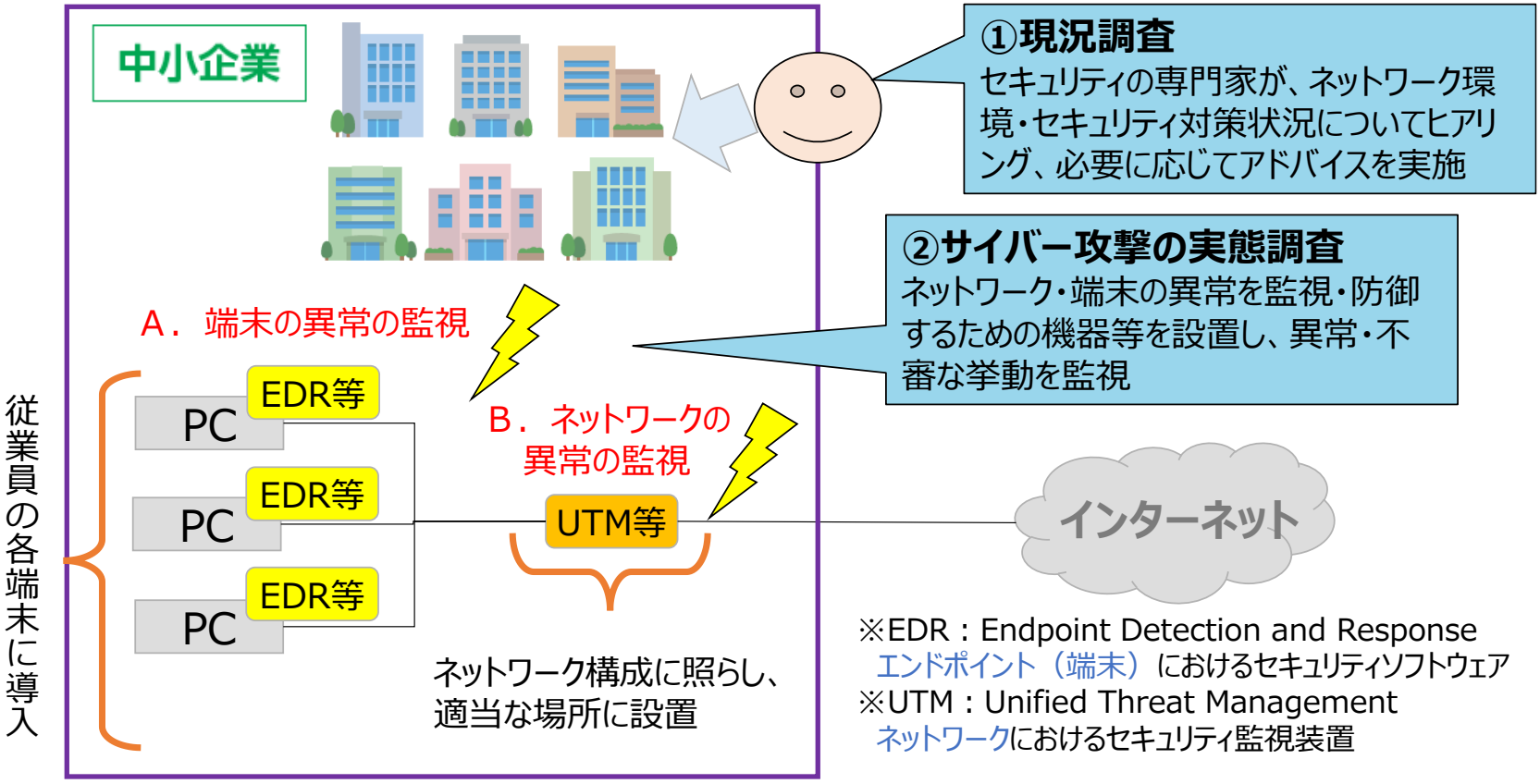
	半導体分野	自動車部品分野	航空部品分野
①サプライチェーン全体のリスク	複数の企業による複雑な生産工程のリレーを経て製造された半導体が、様々な電子機器に組み込まれた形で世の中に行き渡っている。半導体の製造に当たっては、サプライチェーンを構成する部素材等が必要であるが、一つでも構成要素が欠ければ半導体は製造できず、供給途絶のリスクが増加。	ピラミッド構造で多くの企業が製造工程に関与している一方、ジャストインタイム制で完成車メーカーが部品在庫を極小化している。即ち、極めて効率化されている一方、冗長性に乏しい状況であり、ピラミッドのどこかで遅延が生じると全体に波及するリスクが存在している。	航空部品は少量生産であるほか、極めて厳格な工程管理や検査が求められることから、取引先も固定され、取引先情報や受発注情報などの情報流通量が少なく、情報セキュリティ対策はあまり進んでいないと推察される。
②工場システムへの侵害	半導体製造装置は導入時のシステムのまま使われることが多く、バージョンアップなどセキュリティ対策が実施できないことがある。また、これら製造装置の保守メンテナンスが、ウイルス感染の契機になり得る。	完成車メーカーの工場は国内に複数拠点存在するほか、グローバルに展開している。その中の相対的にセキュリティの弱い部分が狙われる事態が発生した。	航空機メーカーは欧米企業が多いことから、グローバルな生産体制となっている。実際にはベルギーに拠点を置く航空機部品メーカーのサーバがランサムウェアの被害を受け、システムが停止したことにより、製造ラインが停止し、グローバルに影響を及ぼした。
③組み込みソフトウェアへの侵害	－	実被害は報告されていないが、デモンストレーションでは危険性が証明された事例がある。	装備品に搭載されているソフトウェアが、機体上の制御系と干渉して攻撃の影響を受けるリスクがある。
④機密情報等の重要情報の漏洩	安全保障に直結する重要な戦略技術であり、設計や製造に関するノウハウや情報の漏えいが重大リスクとなり得る。半導体産業の知財に狙いを定める脅威グループも存在。	個人情報等の情報漏洩が生じた事例がある。電動化の研究開発等のデータは情報の価値が高いと推察され、漏洩のリスクは存在する。	航空機部品製造には高い技術力や認証が必要なこともあり、機密情報の入手を企図したサイバー攻撃が散見される。
⑤業界としての取り組み	業界団体によるサイバーセキュリティ規格の策定・公表や、会員企業への普及啓発等が実施されている。	業界団体により、セキュリティガイドラインの作成、また、完成車メーカーが下請け企業まで含めた対策を講じるなどしている。	業界団体によるサイバーセキュリティ規格の策定や公表は見受けられなかった。

4．実施内容

- 本調査で実施した内容について具体的に示す。

4.1 実施内容の全体像

本事業の実施にあたっては、対象となる中小企業等を選定の上、セキュリティ専門家による「①現況調査」を行った上で、ネットワーク・端末の異常を監視・防御するための機器などを設置した「②サイバー攻撃の実態調査」を行った。なお、本調査の結果については、調査対象先へフィードバックを行い、必要に応じて推奨される対処方法を案内した。



※サイバー攻撃の実態調査は、UTM、EDRの他、クラウドメールセキュリティ、WAF（Web Application Firewall）により情報収集を行った。

4．実施内容

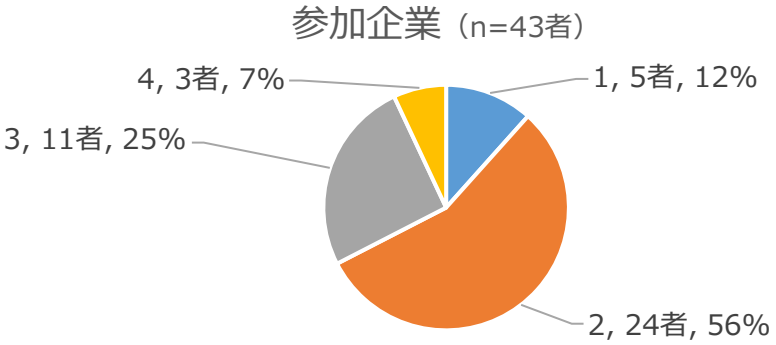
4.2 対象分野･参加企業

本事業における調査対象は、選定した対象分野（半導体、自動車部品、航空部品）の中から公募により参加企業を選定した。

■ 参加企業の対象分野別の割合

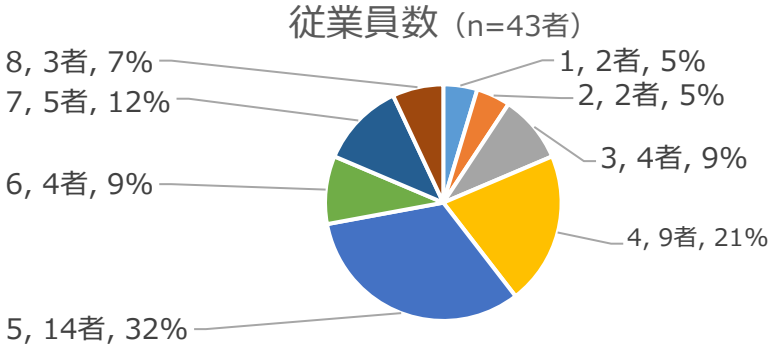
参加企業の産業分野別内訳は、「自動車部品」が24者（56%）で最も多く、「航空部品」11者（25%）、「半導体」5者（12%）である。

また、選定した対象分野に加え、防衛装備庁よりの紹介企業が3者（7%）が本調査に協力いただいた（以下、「防衛装備」として記す）。



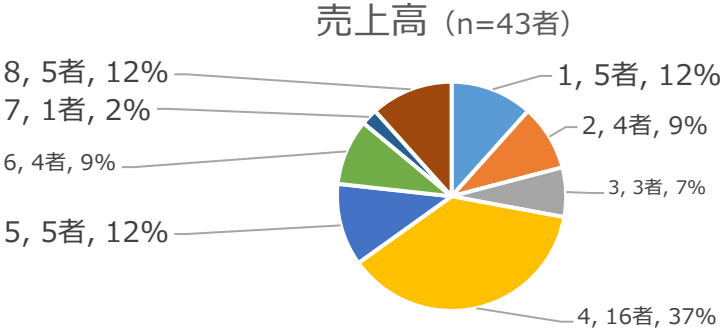
■ 参加企業の従業員数別の割合

参加企業の従業員数別内訳としては「101人～200人」が14者（32%）で最も多く、次いで「51人～100人」が9者（21%）、「301人以上～1,000人」が5者（12%）となっている。



■ 参加企業の売上高別の割合

参加企業の売上高としては「1,000～5,000百万円」が16者（37%）で最も多く、次いで「0～100百万円」及び「5,000～10,000百万円」がそれぞれ5者（12%）となっている。



4．実施内容

4.3 事前準備の実施

本事業の参加企業の公募、事前説明会および個別説明会を実施した。

(1) 参加企業の公募

本事業では、半導体分野と航空部品分野においては地域の業界クラスター関連団体の協力を得て、また、自動車部品分野においては一般社団法人日本自動車工業会（JAMA/自工会）ならびに一般社団法人日本自動車部品工業会（JAPIA/部工会）の協力を得て、調査への参加企業を公募した。

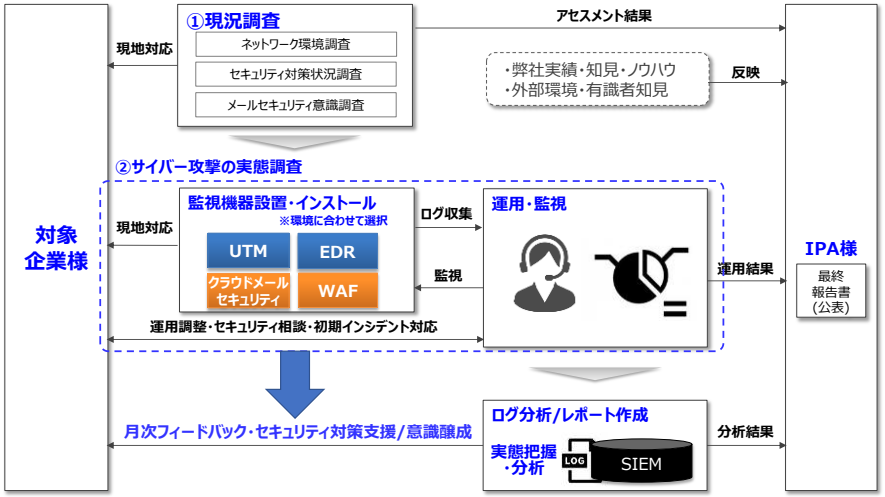
(2) 事前説明会の実施

事前説明会では本事業の概要や調査方法、今後のスケジュールについて参加企業へ説明した。事前説明会は2022年8月25日、8月26日、8月29日の計3日間ウェビナー形式で実施した。

■説明会の概要

開催日時	2022年8月25日、8月26日、8月29日
開催方法	Microsoft社のTeamsを使用して、ウェビナー形式で開催
参加企業数	43者中26者参加（25日10者、26日8者、29日8者）
アジェンダ	1．事業の目的・調査の概要 2．調査の詳細 ①現況調査 ②サイバー攻撃の実態調査 ③その他 3．スケジュール 4．ご依頼事項

■調査のフロー



(3) 個別説明会の実施

事前説明会と並行して参加企業の募集を実施していたため、本事業への参加前もしくは業務都合等で事前説明会へ参加できない企業に対しては、事前説明会の内容について個別説明を実施した。

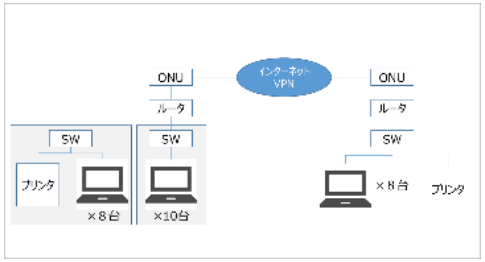
4．実施内容

4.4 現況調査の実施

現況調査ではネットワーク環境、セキュリティ対策状況、及びメールセキュリティ意識調査の3つの調査を実施した。現況調査実施後は、参加企業へ結果のフィードバックを行い、セキュリティに対するリスクや啓発を行った。（例.USBが利用可能な状況であり、ウイルスの持ち込みや、情報を不正持ち出しされるリスクがある）

ネットワーク環境調査
（訪問確認）

システムエンジニアが現地に訪問し、ヒアリングや環境確認を行い、ネットワーク調査と構成図等を作成した。



セキュリティ対策状況調査
（事前アンケート+訪問確認）

セキュリティ専門家が現地に訪問。事前に回答いただくアンケート結果をもとにセキュリティ対策状況をヒアリングした。

「中小企業の情報セキュリティ対策ガイドライン」、「5分でできる！情報セキュリティ自社診断」等の情報を活用し調査を実施

メールセキュリティ意識調査
（疑似攻撃メール送信）

一部の従業員の方に**疑似攻撃メール**を送信し、開封状況を確認。従業員の方のメールに関するセキュリティ意識を調査した。

4．実施内容

4.5 サイバー攻撃の実態調査の実施

参加企業のネットワーク・端末の異常を監視・防御するための機器等を設置し、検知レポートの収集および分析を行った。実施内容を以下に示す。

	実施内容	狙い・目的	得られる情報・実施対象	有効性
1	社内ネットワークに対する攻撃の実態調査・分析 (ネットワーク出入口対策)	【UTM】 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 (導入済みの場合は既設レポートを活用)	ネットワークへの攻撃状況	対象企業に対する攻撃実態やリスクを把握
2	社内ネットワーク接続された端末に対する攻撃の実態調査・分析 (エンドポイント対策)	【EDR】 クライアントPCにEDRエージェントを導入し、各PCのプロセス監視、ログ収集・解析を行い不正な挙動の有無や検知実態を把握	端末の不正挙動 (不審なファイル削除、ネットワーク通信、プロセス起動、レジストリの変更等)	クライアントPC毎に対する攻撃実態やリスクを把握
3	不正メールによる攻撃の実態調査・分析 (メールセキュリティ対策)	【クラウドメールセキュリティ】 対象企業が利用しているクラウドメールサーバー（Microsoft 365、Google Workspace）に対する不正メール攻撃と受信実態・傾向を把握	不正メールの情報 ・受信実態	UTMやEDRで検知しきれない不正メールの攻撃実態を把握
4	Webサイトにおける攻撃の実態調査・分析 (Webセキュリティ対策)	【WAF】 Webサイトに対する不正攻撃の実態・傾向を把握	Webサーバに対する ・不正攻撃	Webサイトへの攻撃実態を把握

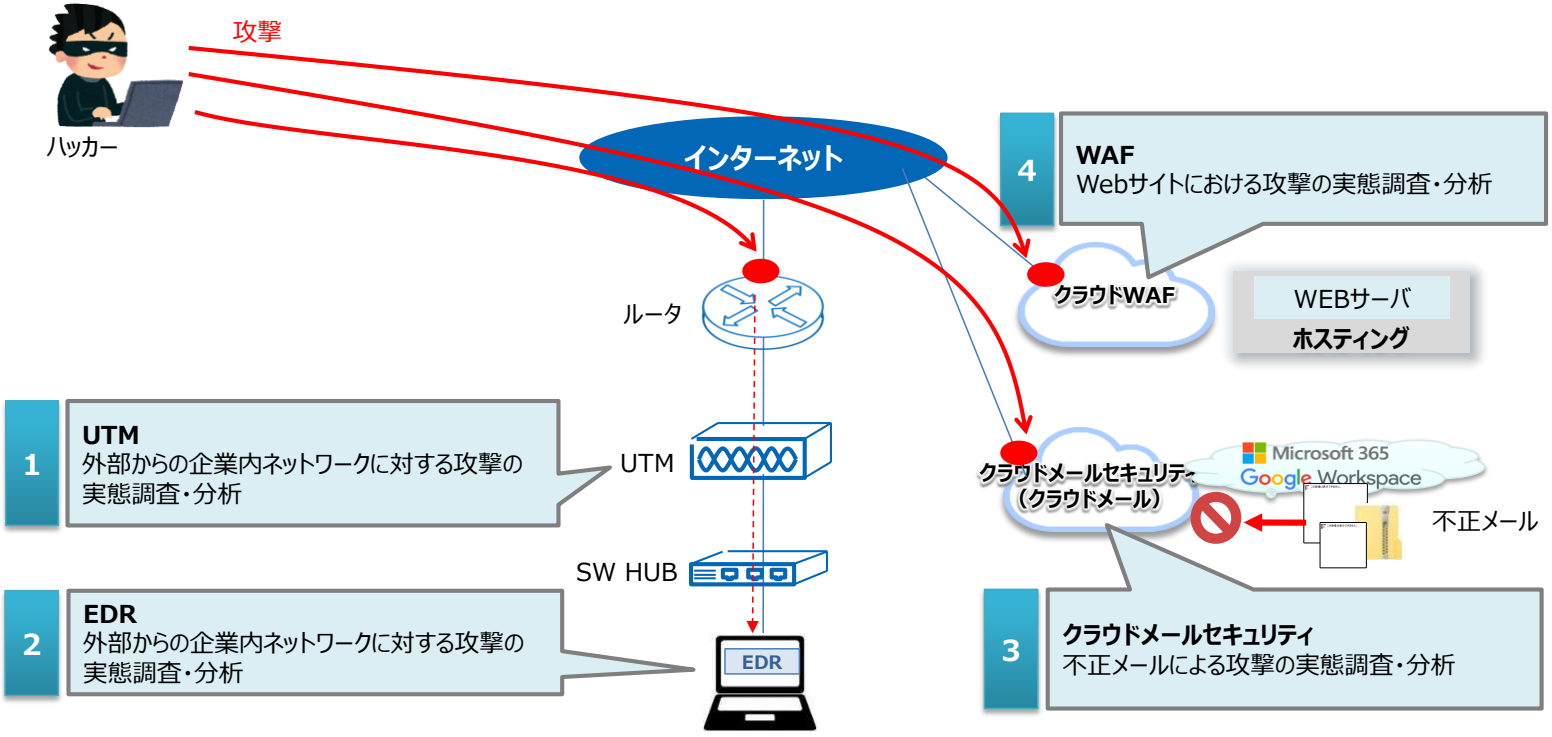
4．実施内容

4.5 サイバー攻撃の実態調査の実施（つづき）

(1) セキュリティ機器の設置構成

本事業では、UTMは参加企業の負担軽減のため、既設ルータの移設等のネットワーク構成変更を伴わないルータ下部に設置することとした。UTMにはIPアドレスのルーティングや変換等を行わず通信を中継するだけの透過型設定を行うことで、参加企業側にはネットワーク構成変更が不要となる。

EDRは参加企業の有する全端末、クラウドメールセキュリティはMicrosoft365もしくはGoogleWordspaceを利用する企業の全ユーザー、WAFはWebサーバを対象とする。



補足：赤色の丸はGlobalIPが設定される箇所であり、インターネット経由でハッカー等の不特定多数が接続できる箇所である。ルータには社内端末がリクエストした社外サーバとの通信しか許可しない設定を行うことが一般的であり、ハッカーがポートスキャン等を試みてもルータから先の社内端末には到達できない。

4．実施内容

4.5 サイバー攻撃の実態調査の実施（つづき）

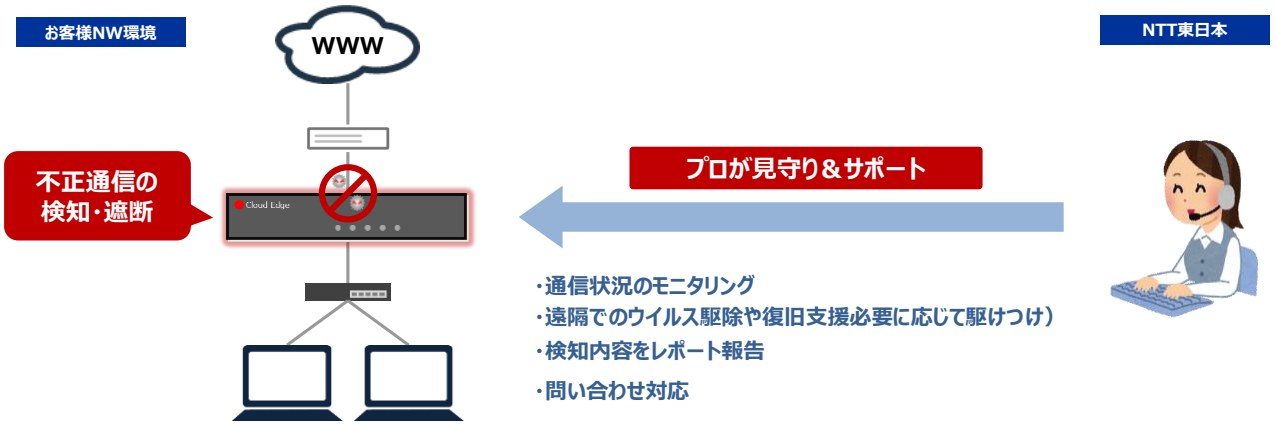
(2) セキュリティ機器の概要

①UTM（Unified Threat Management）の概要

UTMは様々なセキュリティ脅威対策をひとまとめにした統合脅威管理のセキュリティ機器である。ルータ配下に専用機器を設置することでネットワークの出入り口を監視し、不正通信を検知・遮断する。本事業で用いたUTMは東日本電信電話株式会社が提供する「おまかせサイバーみまもり」であり、UTM機能に加え、情報セキュリティのプロが通信状況をモニタリングし、有事の際は遠隔でのウイルス除去や検知内容のレポート報告、問合せ対応を行えるサポートが一体となったサービスを導入した。

セキュリティインシデント 監視・復旧支援サービス
おまかせサイバーみまもり ＝「UTM」と「サポート」が一緒になったサービス

UTM＝「統合脅威管理」
様々なセキュリティ脅威対策をひとまとめにしたセキュリティ機器。ルータ配下に専用BOXを設置することで**ネットワークの出入口を監視**し、**不正通信を検知・遮断**します！



▶ **社内ネットワーク全体の見守りが可能**

4．実施内容

4.5 サイバー攻撃の実態調査の実施（つづき）

■UTMの検知項目

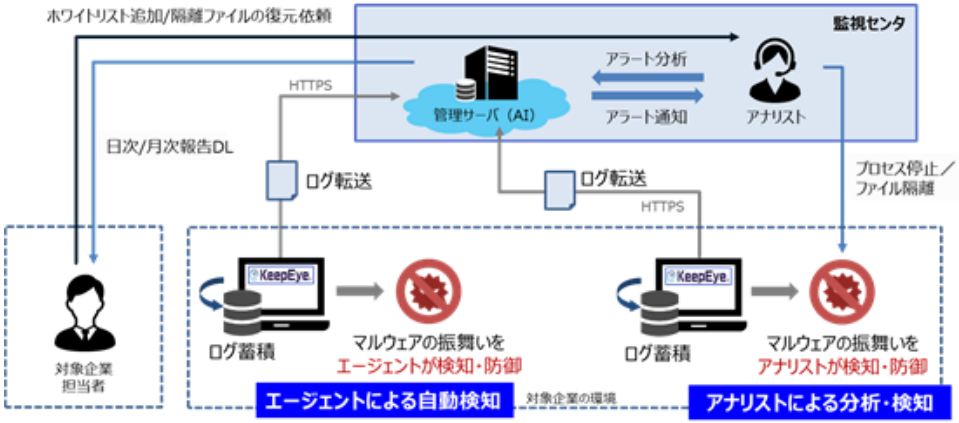
No	検知項目	検知項目の内容及びUTMの機能
1	不正プログラム	コンピュータに害悪を及ぼすプログラムであり、コンピュータが不正に操作され、社内の情報をインターネットに対して送り出してしまう脅威がある。UTMにより、不正な通信、プログラムによる攻撃を検知し、どのような通信が行われているかを判別し、内部感染を早期に発見できる。
2	不正侵入防止（IPS）	ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信を検知しブロックする。ソフトウェアやネットワークの脆弱性を利用してシステムが不正侵入され、その結果、機密情報が漏えいする脅威がある。UTMにより、それらの通信を検知・ブロックし、通信が合致した脆弱性に関するルール毎の件数を把握できる。
3	不正サイト	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、URLやIPアドレスの情報から、どのユーザー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。
4	スパムメール	宣伝広告目的で、ユーザー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、ユーザーが誤ってURLにアクセスしないよう注意を喚起できる。
5	ランサムウェア	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、宛先となっていたユーザーを把握できる。
6	C&Cコールバック	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サーバへの通信である。C&Cコールバックが発生した場合、特定のWebサイトへ負荷を与えるDDoS攻撃に利用され、サーバから重要な機密情報を抜き取られる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、どのユーザーがC&Cサーバへの通信を実施しているか把握できる。
7	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が検知された件数を示す。
8	URLカテゴリフィルタ	HTTPリクエスト、又はTLSネゴシエーションをもとにカテゴライズした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、又はTLSネゴシエーション試行単位）を示す。

4．実施内容

4.5 サイバー攻撃の実態調査の実施（つづき）

②EDR（Endpoint Detection and Response）の概要

本事業にて提供するEDRサービスは、エージェントによる自動検知とアナリストによる分析・検知により、マルウェアの振舞いやPC端末の不正な挙動を検知・解析することでプロセス停止やファイル隔離を行う機器を導入した。製品は300名以下の企業で国内シェアNo.1※のEDR「KeepEye（S&J株式会社）」を導入した。KeepEyeはS&J株式会社のSOC運営事業で培われたノウハウを基にした国産のEDR製品である。



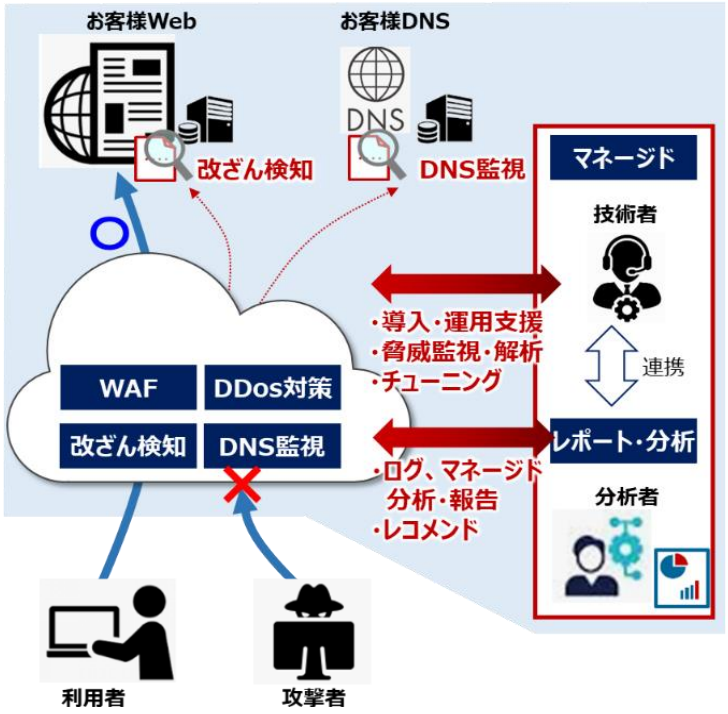
4．実施内容

4.5 サイバー攻撃の実態調査の実施（つづき）

③WAF（Web Application Firewall）の概要

WAFとはWebアプリケーションの脆弱性をついた攻撃から守るためのセキュリティサービスである。本事業ではクラウド型のWAFサービスを活用し、Webサーバに対するDDoS対策・改ざん検知・DNS監視を行った。

サービスイメージ



サービスメニュー

WAF

- クラウド型の提供形態のため**対象企業NWの変更不要**
- シグニチャーに加え、振る舞い検知・AIエンジンの解析による**高い検知精度**

マネージド

- 導入～運用まですべて**プロの技術者におまかせ**
- 過検知・誤検知・ホワイトリストの設定等も**すべて代行**

レポート・分析

- 検知・攻撃状況を**ダッシュボードで提供**
- ログ・マネージド内容の分析に基づく**レコメンド等きめ細かいサポート**

DDos対策

- 対象企業Webサーバと異なるNWでDDoS対策を実施するため、**大量の攻撃でも対象企業Webサーバへ影響なし**

改ざん検知・DNS監視

- WAF・DDoS対策以外にWebサイトの改ざん検知・DNSのハッキング監視も**基本サービス内で対応**

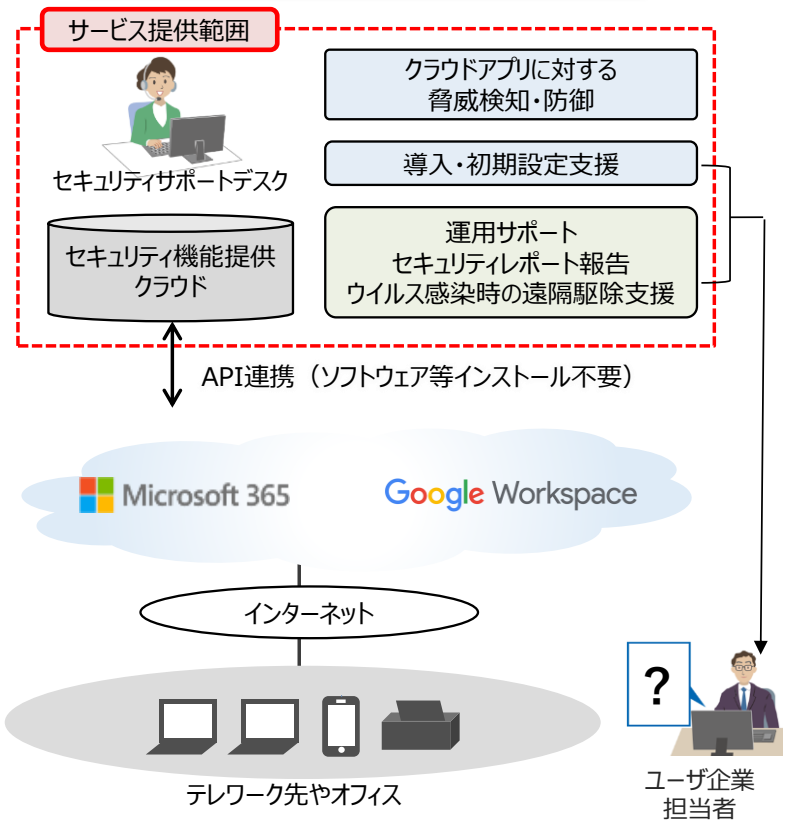
4．実施内容

4.5 サイバー攻撃の実態調査の実施（つづき）

④クラウドメールセキュリティの概要

クラウドメールセキュリティは巧妙化するメール攻撃から、クラウドアプリケーションのメールなどを保護するセキュリティサービスである。新種／亜種等のマルウェアやフィッシング攻撃から情報資産を守る機能が備わっている。Microsoft365またはGoogle Workspaceをご利用の参加企業を対象として導入した。

サービスイメージ



サービスメニュー

不正メール対策	• メールの本文や件名、ドメインや送信アドレスの手動書き換えのメールを検知
不正プログラム対策	• パターンマッチングやAI技術を活用して不正プログラムを検知し、防御
不正URLアクセスブロック	• 不正プログラムへの感染、フィッシング詐欺被害をもたらすサイトへの接続を未然に防止
クラウドサンドボックス	• 不正プログラム対策や不正URLアクセスブロック機能で発見できなかった未知の脅威の可能性のあるファイルやURLを仮想OS上で動的に解析し、検知・防御
情報漏えい対策	• メールやファイル内の情報を検索し、個人情報の利用状況を可視化
ライティングスタイル分析	• メールヘッダーや本文からビジネスメール詐欺と断定できない場合、なりすまされたものであるかを判別 • ユーザの書き方をAIが学習し、受信時に本文の特徴を比較することでなりすましメールを検知
アクティベーション※	• ご利用中のクラウドアプリへの連携作業
レポーティング	• 脅威検知状況の簡易レポーティング
ウイルス感染時の駆除支援※	• ウイルス感染時の遠隔駆除支援 （ウイルスの感染または感染疑い発生時、遠隔から感染疑いのあるPC端末のウイルス駆除を支援）

※お問い合わせ・運用サポートの受付時間は9:00～21:00（年中無休）

4.5 サイバー攻撃の実態調査の実施（つづき）

(3) UTMとEDRを双方設置することで確認できる事項

本事業はインターネットの出入り口にUTM、エンドポイントにEDRを導入することから、これらを双方用いてサイバー攻撃の経路を確認することが期待できる。どのように確認ができるか例により示した。例としてメールによりウイルスが侵入し、外部へ通信した場合を想定し、記載した。

ウイルス感染後の動作パターンを以下３つ想定する。

想定動作①基本

：端末内のファイルが暗号化され、端末に脅迫メッセージが表示される。

想定動作②感染を通知

：上記①に加え、端末がC&Cサーバへ通信を行いハッカーに対して感染を通知。その通知をハッカーが受け取り感染を認知。

想定動作③ハッキングツールをインストール

：上記①②に加え、端末がC&Cサーバからハッカーの不正なツール（ハッキングツール）をダウンロードしてインストールする。

動作パターンにおいて、UTM及びEDRが検知できるポイントを時系列順並べると以下のとおりである。

検知機器	検知対象
EDR	端末内のファイル暗号化や脅迫メッセージ表示等動作
EDR	C&Cサーバへのリクエスト（リクエストしたURLの検査）
UTM	C&Cサーバへのリクエスト（リクエストしたURLの検査）
UTM	ハッキングツールダウンロード時（http通信の場合のみ検査可）
EDR	ハッキングツールインストール後の動作

検知ポイントを追跡すると、ウイルス感染後の動作パターンが想定できる。

例）全てのポイントを検知していた場合は、想定動作③であったと考えられる。

4．実施内容

4.5 サイバー攻撃の実態調査の実施（つづき）

以上の内容をまとめ、図表に示す。

NO	場所	機器	ウイルス（ランサムウェア）の動作		
			想定動作① 基本	想定動作② 感染を通知	想定動作③ ハッキングツールをインストール
1	社内	端末/アプリ領域	ファイル暗号化処理	ファイル暗号化処理	ファイル暗号化処理
2		端末/アプリ領域	脅迫メッセージ表示	脅迫メッセージ表示	脅迫メッセージ表示
3		端末/EDR	動作検知	動作検知	動作検知
4		端末/ブラウザ	—	C＆Cサーバへリクエスト	C＆Cサーバへリクエスト
5		端末/EDR	—	リクエストしたURL検査	リクエストしたURL検査
6		UTM	—	リクエストしたURL検査	リクエストしたURL検査
7		ルータ	—	URLリクエスト	URLリクエスト
8	社外	C&Cサーバ	—	ハッカーが感染を認知	ファイル送信
9	社内	ルータ	—		ファイル送信
10		UTM	—		通信検査 (httpの場合のみ)
11		端末/ブラウザ	—		ファイル受信・開封
12		端末/アプリ領域	—		ウイルス感染
13		端末EDR	—		ファイル検査

UTMとEDRの双方を確認して期待できる事項（⇒ 感染後の詳しい動作を把握）

(4) UTMおよびEDRに加え、WAFおよびクラウドメールセキュリティを設置することで確認できる事項

UTMおよびEDRの属する参加企業のネットワークに関わらない外部に独立して設置され、相関が想定されないことから、WAFおよびクラウドメールセキュリティについては個々の検知結果を確認することとする。

5．現況調査の結果と分析

- 本事業で実施した、ネットワーク環境調査、セキュリティ対策状況調査、メールセキュリティ意識調査の結果を以下に記載する。

5.1 ネットワーク環境調査の結果と分析

本事業の参加企業（43者）のネットワーク環境について、参加企業へ訪問（2者については企業側の要望によりリモート会議）により、インターネット接続点の構成、及びセキュリティ機器構成とその運用に関する事項について確認した。

インターネット接続点の構成の調査により、ルータがUTM機能を有しており、ルータとUTMを同一機器としている企業が13者、DMZを構成している企業は無いことがわかった。

セキュリティ機器の構成とその運用の調査により、既にUTMを設置していた企業が26者あり、そのうちUTMのログを集計した検知レポートを作成している企業は12者であった。また、既設UTMの企業26者のうち、アラート情報の確認者がUTMの導入ベンダーである企業は21者、ユーザー自身が3者、確認していないが2者であった。

ID	分野	端末台数	ルータ機種名	ルータのUTM機能有無	DMZ有無	既設UTM有無	既設UTM機種名	検知レポート作成有無	アラート情報確認者
101	半導体	1,000	Fortigate	有	-	有	Fortigate	-	ベンダー
102	半導体	160	Fortigate60F	有	-	有	Fortigate60F	-	確認していない
103	半導体	150	RTX1210	-	-	-	-	-	-
104	半導体	50	OG810Xa	-	-	有	Fortigate	-	ベンダー
105	半導体	150	FWX120	-	-	-	-	-	-
201	自動車部品	60	BizBoxN500	-	-	有	CloudEdge50	有	ユーザー
202	自動車部品	20	VSR602j	有	-	有	VSR602j	-	ベンダー
203	自動車部品	62	CatoSocket	-	-	-	-	-	-
204	自動車部品	300	Cisco4300	-	-	有	Fortigate	-	ベンダー
205	自動車部品	50	IX2105	-	-	-	-	-	-
206	自動車部品	40	RTX830	-	-	有	CloudEdge50	-	ベンダー
207	自動車部品	31	WSR-2533DHPL-C	-	-	有	EasySOC	有	ベンダー
208	自動車部品	100	WatchGuard	有	-	有	WatchGuard	-	ベンダー
209	自動車部品	150	AR450S	-	-	-	-	-	-
210	自動車部品	30	RTX1210	-	-	有	CloudEdge100	有	ベンダー

5．現況調査の結果と分析

5.1 ネットワーク環境調査の結果と分析（つづき）

ID	分野	端末台数	ルータ機種名	ルータのUTM機能有無	DMZ有無	既設UTM有無	既設UTM機種名	検知レポート作成有無	アラート情報確認者
211	自動車部品	120	IX2215	-	-	-	-	-	-
212	自動車部品	120	NVR510	-	-	有	CloudEdgeSB	有	ベンダー
213	自動車部品	250	Fortigate100E	有	-	有	Fortigate100E	有	ベンダー
214	自動車部品	250	Fortigate	有	-	有	Fortigate	有	ベンダー
215	自動車部品	1,000	SEIL/X1	-	-	有	SRX340	-	ベンダー
216	自動車部品	60	Fortigate100D	有	-	有	Fortigate100D	-	ベンダー
217	自動車部品	800	Fortigate	有	-	有	Fortigate	-	ベンダー
218	自動車部品	1,500	C1111-8P	-	-	有	PaloAlto	有	ベンダー
219	自動車部品	40	RTX1210	-	-	有	CloudEdge50	有	ベンダー
220	自動車部品	120	RTX830	-	-	-	-	-	-
221	自動車部品	75	RTX1210	-	-	有	CloudEdgeCE110	有	ベンダー
222	自動車部品	80	RT58i	-	-	-	-	-	-
223	自動車部品	80	RTX1210	-	-	-	-	-	-
224	自動車部品	24	Fortinet/YT-FG400E	有	-	有	Fortinet/YT-FG400E	有	ベンダー
301	航空部品	15	ZC1000	-	-	有	SS5000Ⅱ	-	確認していない
302	航空部品	50	Fortigate100E	有	-	有	Fortigate100E	-	ベンダー
303	航空部品	20	RT107e	-	-	-	-	-	-
304	航空部品	14	AtermWG1200HS	-	-	-	-	-	-
305	航空部品	30	RTX1210	-	-	-	-	-	-
306	航空部品	70	UTX100	有	-	有	UTX100	有	ユーザー
307	航空部品	20	RTX830	-	-	有	CloudEdge	有	ベンダー
308	航空部品	100	Vario/VSR602j	-	-	-	-	-	
309	航空部品	20	TP-link-AC2600-mimo	-	-	-	-	-	
310	航空部品	16	E-WMTA2.2	-	-	-	-	-	
311	航空部品	155	RTX1210	-	-	-	-	-	
401	防衛装備	90	Fortigaete80F	有	-	有	Fortigate80F	-	ユーザー
402	防衛装備	50	RTX810	-	-	-	-	-	
403	防衛装備	40	Fortigate100E	有	-	有	Fortigate100F	-	ベンダー

5．現況調査の結果と分析

5.2 セキュリティ対策状況調査の結果と分析

本事業の参加企業（43者）のセキュリティ対策状況を確認するため、IPA「中小企業の情報セキュリティ対策ガイドライン 」及びIPA「情報セキュリティ10大脅威 2022 」を参照し、調査項目を作成した。

調査項目は参加企業に対しWeb形式のアンケートにより取得した。アンケート結果の取得後、参加企業へ現地訪問、またはリモート会議にて、セキュリティ専門家がヒアリングによりアンケート回答内容を確認し、必要に応じて回答の修正を実施した。

ヒアリング項目は下記5分類ごとの項目と、その他取引先の対策要請や被害経験の項目、合計49問を用意した。
各設問の回答はその他の項目を除き、「できている」、「一部できている」、「できていない」、「わからない」の4つとした。

分類	① 経営層の リスク認識や 関与の度合い	② 情報 セキュリティ 運用・管理	③ 情報 セキュリティ 技術的対策	④ 情報 セキュリティ 物理的対策	⑤ リモート アクセスの 活用状況	その他 対策要請有無 被害経験有無
設問数	5	16	12	7	7	2

5．現況調査の結果と分析

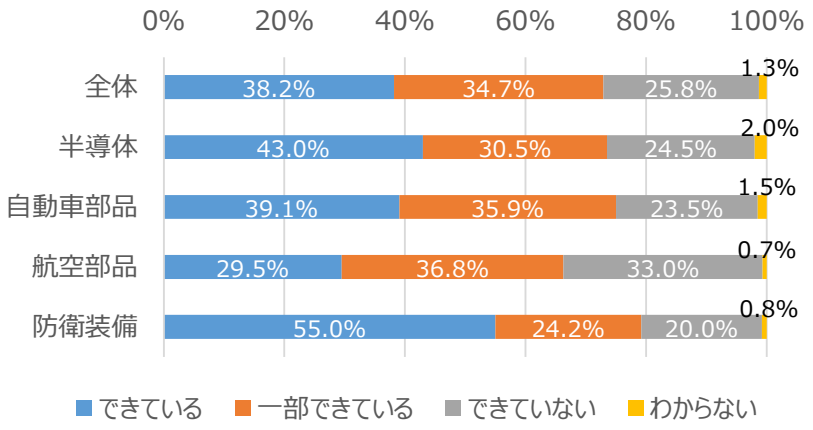
5.2 セキュリティ対策状況調査の結果と分析（つづき）

＜アンケート集計結果及びヒアリング状況＞

全アンケート項目（「リモートアクセスの活用状況」を除く）に対する回答結果は右の図表のとおり。※「リモートアクセスの活用状況」はリモートワークをしている場合の限定質問のため除外。

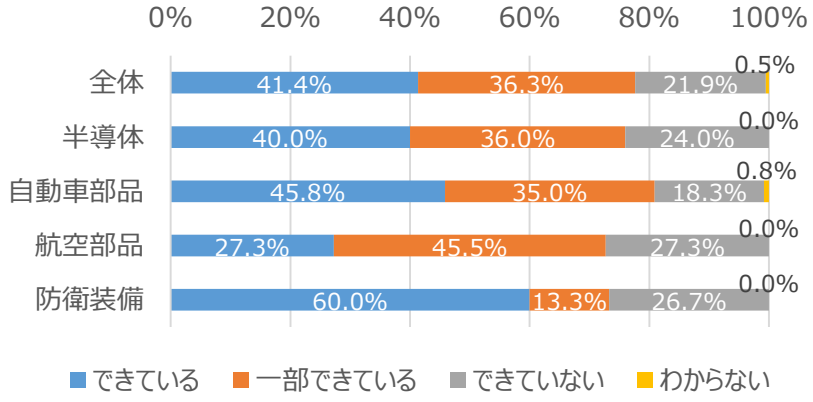
3分野（半導体、自動車部品、航空部品）の差異を見ると、僅かな差であるが、「できている」の割合は半導体分野が多く、「できている」「一部できている」を合わせた割合は自動車部品分野が多い。

「すべての項目」に対する回答結果



「経営層のリスク認識や関与の度合い」カテゴリについては、3分野では自動車部品分野が最も高かった。自動車部品分野においては、2022年3月の大手自動車メーカーの全工場の稼働停止事案を契機に、メーカーからセキュリティ対策を要請されているという状況を訪問ヒアリングで確認しており、その影響があるものと思われる。

「経営層のリスク認識や関与の度合い」に対する回答結果



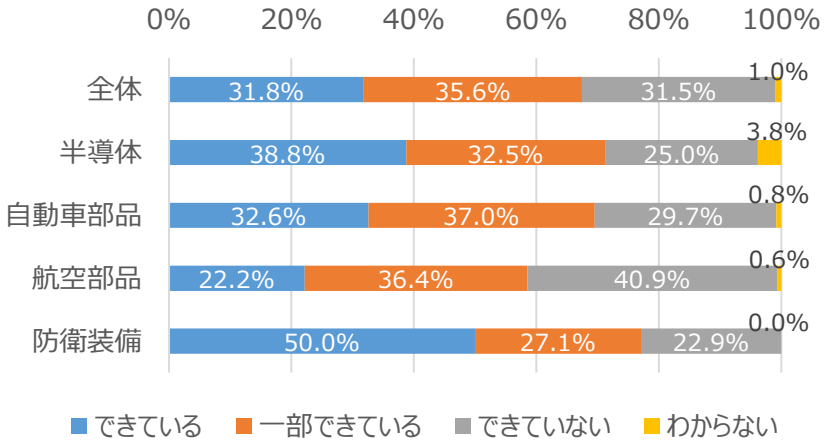
5．現況調査の結果と分析

5.2 セキュリティ対策状況調査の結果と分析（つづき）

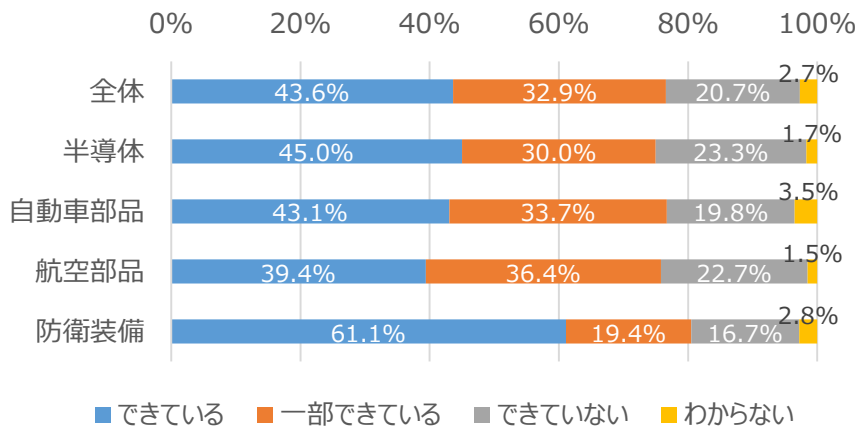
「情報セキュリティ対策状況」の「運用・管理」カテゴリ、「技術的対策・取組」カテゴリ、「物理的対策・取組」カテゴリの3つの結果においては、半導体分野がそれぞれにおいて「できている」の割合が最も多かった。半導体分野では、数年前から大手半導体商社が取引先のセキュリティ指導を行っていることを訪問ヒアリングで確認しており、その影響があるものと思われる。

また、訪問ヒアリングにて、「技術部門のCADパソコンが社内LANに接続されているが管理できていない」、「工場のFA端末は社内LANとは別のLANを利用し管理できていない」等、工場系LAN等の管理が情報システム部門の管理外である実態が確認できた。一方、「工場のFA端末等一部端末はウイルス対策ソフトが未導入」、「USBメモリは製造部門で自由に使っている可能性がある」等、情報システム部門の管理外でのウイルス感染の可能性があることが確認された。

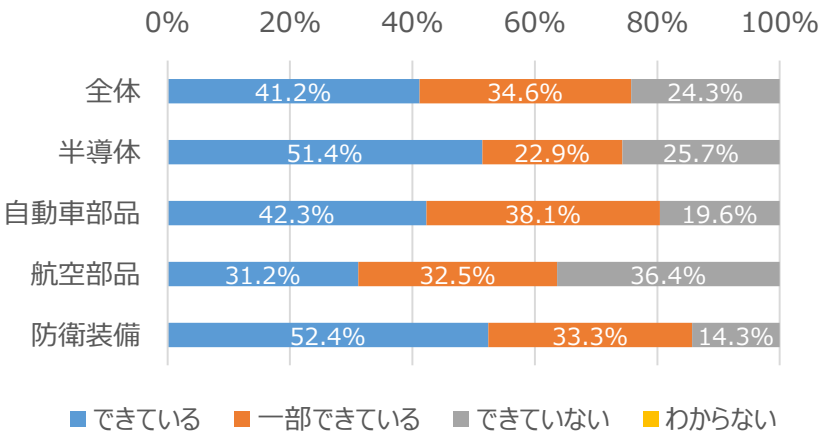
「情報セキュリティ対策状況　運用・管理」に対する回答結果



「情報セキュリティ対策状況　技術的対策・取組」に対する回答結果



「情報セキュリティ対策状況　物理的対策・取組」に対する回答結果



5．現況調査の結果と分析

5.2 セキュリティ対策状況調査の結果と分析（つづき）

「リモートアクセスの活用状況」カテゴリの結果を示す。このカテゴリは、リモートワークを実施している場合にのみ、運用ルールの有無やシステム状況などを質問した。

リモートワークの実施有無については、半導体分野が最も実施している企業が多かった。全体としては、外部から社内に接続することへのリスクを感じる企業が多く、約2割しか策定していなかった情報セキュリティポリシーと比して、対策がされている状況であった。

※主な対策（できている、一部できていると答えた企業）

-リモートアクセスのルール策定：約7割

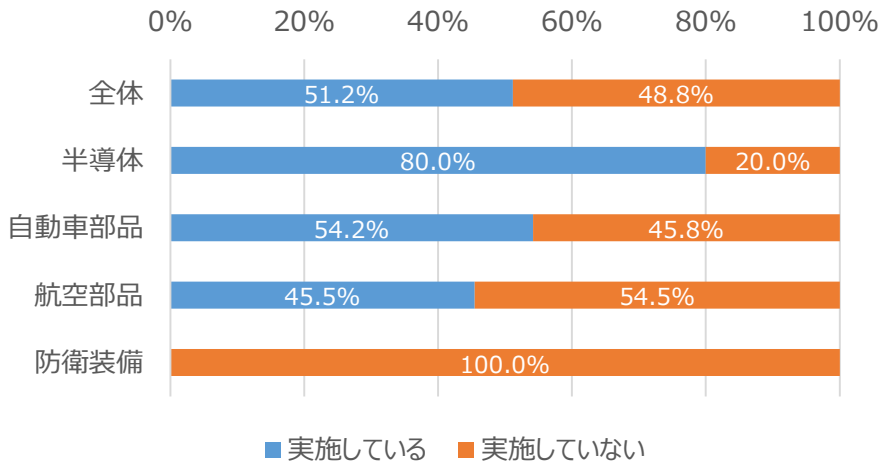
-OSやソフトウェアの最新化：約9割

-不正アクセス対策：約8割

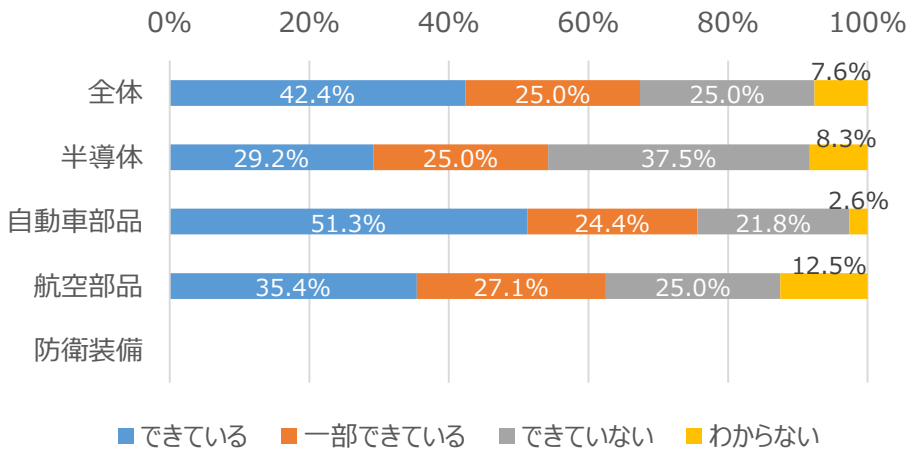
-ログの確認：約6割

なお、防衛装備分野については、参加企業3者のいずれもリモートワークを許可しておらず、セキュリティ対策に万全を期すため許可していないとのことであった。

「リモートワークの実施有無」に対する回答結果



「リモートアクセスの活用状況」に対する回答結果

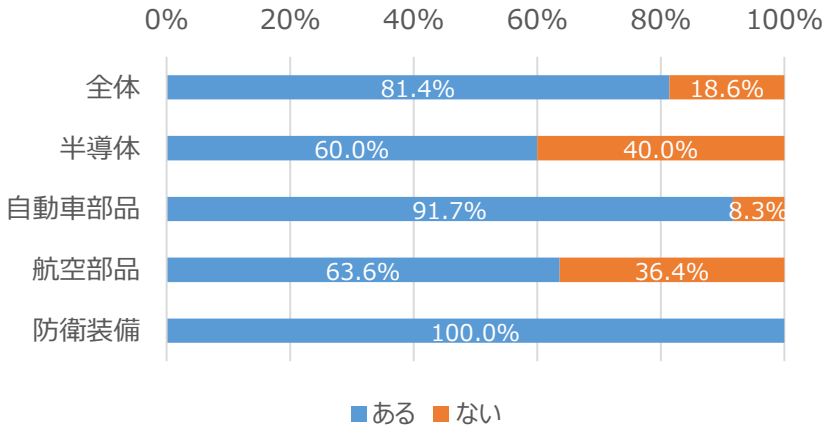


5．現況調査の結果と分析

5.2 セキュリティ対策状況調査の結果と分析（つづき）

「取引先等からの情報セキュリティ対策要請の有無」に対する回答では、「3.産業分野別の業界状況」では航空部品分野は業界として取り組みがないと想定していたが、アンケートでは「ある」という回答が63.6%だった。これを訪問ヒアリングで確認したところ、欧米の航空機メーカーから品質管理の監査項目の一部に設計情報等の保護に関する項目があったためである。しかし、この項目は自動車部品分野の業界団体ガイドラインや、本調査のアンケート項目のように、情報セキュリティ対策として体系だてたものではないとのことであった。

「取引先等からの情報セキュリティ対策要請の有無」に対する回答結果

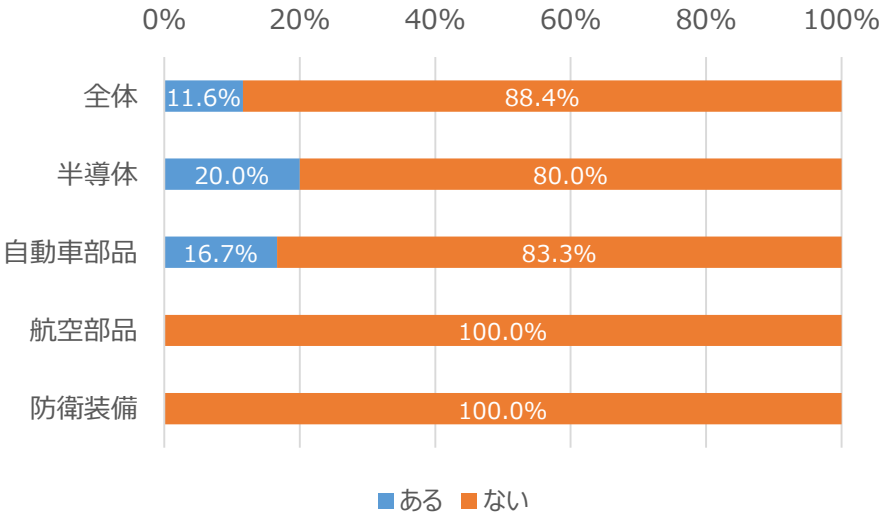


「過去3年間の情報セキュリティ被害経験の有無」に対する回答では、半導体分野と自動車部品分野で被害経験のある企業が5者あり、航空部品分野と防衛装備分野にはなかった。「3.産業分野別の業界状況」では、「航空部品は少量生産であるほか、極めて厳格な工程管理や検査が求められることから、取引先も固定され、取引先情報や受発注情報などの情報流通量が少ない」との調査結果があり、情報の流通量がインシデントの発生確率に影響を与えていることが想定される。

【情報セキュリティ被害経験】

- メールによりランサムウェア及びエモテットに感染、いずれも社内で数日以内に解決。
- メールによりウイルス感染、すぐに端末のLANケーブルを抜いたため影響は端末1台にとどまった。
- ウイルスにより外部にメールが送信された。フォレンジック調査を行い数日以内に解決したが、この事件を契機にEDRを導入。
- 別拠点の工場の端末がワームに感染し、本社との通信ができなくなった。復旧に数日を要し、その間は生産管理システムの投入ができなかった。
- メールが不特定多数に送られるエモテットと疑われる挙動を確認したが、確認後速やかにウイルスチェック等を行い復旧した。

「過去3年間の情報セキュリティ被害経験の有無」に対する回答結果



5．現況調査の結果と分析

5.3 メールセキュリティ意識調査の結果と分析

メールセキュリティ意識調査は、標的型攻撃メールを模したメールを従業員等へ送り、メール本文のURL押下や添付ファイル開封をサーバ側で検知し結果を伝えることで、従業員へのセキュリティ対策意識を醸成し、本物の標的型攻撃が来た際の影響度合いをはかることができる。今回の調査では、攻撃者がメール受信者に対しフィッシングやウイルス感染を行うための不正サイトへ接続させる状況を想定し、URLが含まれるメールを送信した。1者あたり最大20アドレス迄として訓練対象を募集し、39者610アドレスを対象に調査を行った。

■送信したメールの内容

送信日時	2022/10/6 13:00頃
検知期間	2022/10/6～2022/10/15
件名	セキュリティパッチの更新
本文	部署名　役職名　●● 様 お疲れ様です。 総務より連絡です。 ニュースでも報道されておりますが、弊社も利用しているメーカーのPCに脆弱性が発見されております。 以下のURLから手順書とセキュリティパッチをダウンロードし、各自対応願います。 ※本メールは対象者のみに送付しております。 https://toresavi.com/beacon?token=XXX宛先ごとに異なるURLXXX 本件は国内でもセキュリティ事故の発生が報告されているため、早急な対応をお願いします。 何卒、宜しくお願い致します。
URLクリック時のイメージ	

■結果

ユーザー単位（メールアドレス単位）で結果を見ると、URLクリック率（参加アドレス数に対するメール本文のURLをクリックしたアドレス数）は全体で16.7%だった。分野別にみると、自動車部品、航空部品、半導体、防衛装備の順にURLクリック率が多かった。

企業単位で結果を見ると、URLクリックした企業数（1件でもURLをクリックしたユーザーがいた企業）から算出したURLクリック率は、全体で66.7%だった。分野別にみると、半導体と防衛装備が100%であり、次いで自動車部品、航空部品の順にURLクリック率が多かった。

ユーザー単位の集計結果

分野	参加アドレス数 [件]	URLクリックしたアドレス数 [件]	URLクリック率 [%]
半導体	100	12	12.0
自動車部品	352	70	19.9
航空部品	122	17	13.9
防衛装備	36	3	8.3
全体	610	102	16.7

企業単位の集計結果

分野	企業数 [者]	URLクリックした企業数 [者]	URLクリック率 [%]
半導体	5	5	100.0
自動車部品	21	15	71.4
航空部品	10	3	30.0
防衛装備	3	3	100.0
全体	39	26	66.7

6．サイバー攻撃の実態調査の結果と分析

- 本事業で実施した、サイバー攻撃の実態調査の結果を以下に記載する。

6.1 セキュリティ機器の導入結果

本事業にて新規UTM、EDR、WAF、クラウドメールセキュリティを導入した者数を一覧に記載する。

	導入者数		
	11月	12月	1月
UTM	11者	12者	13者
EDR	30者	30者	30者
WAF	4者	8者	8者
クラウドメールセキュリティ	1者	2者	2者
（既設UTM検知レポート活用）	3者	3者	3者

既設UTMの検知レポートは検知レポートを作成しかつ同意が得られた企業から収集した。条件（本事業で導入したUTMと同機種かつ同検知レポート形式）を満たした3者分の検知レポートを本事業のUTM検知レポート項目の集計件数に加算した。

なお、本事業にて新規に導入したUTM、EDR、WAF、クラウドメールセキュリティの組み合わせ別及び分野別の導入状況は以下である。

	合計者数	分野別者数			
		半導体	航空部品	自動車	防衛装備
UTM導入、EDR導入	12者	2者	6者	3者	1者
UTM未導入、EDR導入	18者	2者	3者	11者	2者
UTM導入、EDR未導入	1者	0者	0者	1者	0者
UTM未導入、EDR未導入、WAFかクラウドメールセキュリティ導入	4者	1者	0者	3者	0者
全て未導入	8者	0者	2者	6者	0者
合計	43者	5者	11者	24者	3者

6．サイバー攻撃の実態調査の結果と分析

6.2 セキュリティ機器の検知結果

セキュリティ機器の検知件数は以下のとおり。なお、UTMの検知項目には探索活動検知（ping/ポートスキャン等）は含まれていない。

機器名	検知項目	検知結果 [件] ()内は1者1か月あたりの件数			
		11月	12月	1月	合計※1
UTM	不正プログラム	101 (7.2)	74 (4.9)	101 (6.3)	276 (6.2)
	不正侵入防止（IPS）※2	152 (10.9)	412 (27.5)	160 (10.0)	724 (16.1)
	不正サイト	0 (0.0)	308 (20.5)	273 (17.1)	581 (12.5)
	スパムメール	6,672 (476.6)	12,843 (856.2)	11,753 (734.6)	31,268 (689.1)
	ランサムウェア	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
	C&Cコールバック	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
	禁止アプリケーション	2,970 (212.1)	3,502 (233.5)	4,107 (256.7)	10,579 (234.1)
EDR		206 (6.9)	149 (5.0)	72 (2.4)	427 (4.7)
WAF		15,296 (3,824.0)	13,177 (1,647.1)	7,953 (994.1)	36,426 (2,155.1)
クラウドメールセキュリティ		633 (633.0)	2,953 (1,476.5)	3,535 (1,767.5)	7,121 (1,292.3)

※1：合計の()内件数は11月から1月の1者1か月あたりの件数合計を3で割り算出。
※2：お客様機器の不具合と想定される検知結果40,726件を除き算出。

6．サイバー攻撃の実態調査の結果と分析

6.2 セキュリティ機器の検知結果（つづき）

(1) UTMのログから見える脅威のアタックとブロック状況

■ 不正プログラム

- 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
- 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

- 対象期間中に「不正プログラム」を検知した１者1か月あたりの検知件数は、最も多い11月で7.2件、最も少ない12月で4.9件であった。

	11月	12月	1月	合計
検知件数 [件]	101	74	101	276
１者1か月あたり [件]	7.2	4.9	6.3	6.2

- 商品や注文情報に誤認するプログラムが多かった。

（検知された不正プログラムの名称の例）

- NLT90470 ORDER 8793 2023.cab
- PAYMENT SLIP.zip
- Purchase order.zip

■ 不正侵入防止(IPS)

- 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不正侵入され、その結果、機密情報が漏えいする脅威
- 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

- 対象期間中に「不正侵入検知（IPS）」の**1**者1か月あたりの検知件数は最も多い12月で27.5回、最も少ない1月で10.0回と月による変動が認められた。

	11月	12月	1月	合計
検知件数 [件]	152	412	160	724
１者1か月あたり [件]	10.9	27.5	10.0	16.1

- 1者でLand攻撃（送信元IPアドレスと送信先IPアドレスが同一のパケットを攻撃対象コンピュータに送ることで成立する、DoS攻撃の一種）が40,726件検知していた。調査の結果、参加企業側設備の不具合の可能性があるため、上記集計からは除外した。

6．サイバー攻撃の実態調査の結果と分析

6.2 セキュリティ機器の検知結果（つづき）

(1) UTMのログから見える脅威のアタックとブロック状況

■ 不正サイト

- 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
- UTMにより、URLやIPアドレスの情報から、どのユーザー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

- 対象期間中に「不正サイト」を検知した件数は、最も多い12月で308件、最も少ない11月で0件と推移した。

	11月	12月	1月	合計
検知件数 [件]	0	308	273	581
1者1か月あたり [件]	0.0	20.5	17.1	12.5

- 違法に漫画を配信するサイトの検知が最も多かった。

（検知された不正サイトの例）

- 13dl[.]net

■ スパムメール

- 宣伝広告目的で、ユーザー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
- 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ーが誤ってURLにアクセスしないよう注意を喚起

- 対象期間中に「スパムメール」を検知した件数は、1社あたり検知件数は476.6件～856.2件で推移した。

	11月	12月	1月	合計
検知件数 [件]	6,672	12,843	11,753	31,268
1者1か月あたり [件]	476.6	856.2	734.6	689.1

■ ランサムウェア

- 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
- 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ーを把握

- 対象期間中に「ランサムウェア」を検知した件数は0件だった。

■ C&Cコールバック

- 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が抜き取られるなどの被害が発生する脅威
- 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、どのユーザーがC&Cサーバへの通信を実施しているか把握

- 対象期間中に「C&Cコールバック」を検知した件数は0件だった。

6．サイバー攻撃の実態調査の結果と分析

6.2 セキュリティ機器の検知結果（つづき）

(2) EDRによる不審な挙動の検知状況

- EDRによりエンドポイントの操作や動作を監視することで、異常や不審な挙動を検知および対処し、インシデント発生時の初動対応が実施できる。
- 3か月合計した1者あたりの検知件数は4.7件であった。

検知結果：EDRの検知件数（月別）

	11月	12月	1月	合計
検知件数 [件]	206	149	72	427
1者1か月あたり [件]	6.9	5.0	2.4	4.7

検知結果：検知分類別の累計検知件数及び該当企業数
（累計検知件数上位5位までの検知分類）

検知分類名	検知件数 [件]
アプリがOSコマンド実行	190
アプリから別アプリを起動	164
Microsoft Defenderによる検知	38
アプリがファイル生成	19
不審なOSコマンド実行	10
総計	421

(3) WAFによる不審な挙動の検知状況

- WAFによりWebアプリケーションの通信を監視することで、不正なアクセスを検知およびブロックし、脅威となる様々な脆弱性や危険からWebサイトを保護することができる。
- 3か月合計した1者あたりの検知件数は2,155.1件であった。

検知結果：WAFの検知件数（月別）

	11月	12月	1月	合計
検知件数 [件]	15,296	13,177	7,953	36,426
1者1か月あたり [件]	3,824.0	1,647.1	994.1	2,155.1

【WAF】攻撃目的別の累計検知件数
(累計検知件数上位5位までの攻撃目的)

攻撃目的名	検知件数 [件]
Webサイトの変造/偽造	17,027
個人情報の漏えい	14,526
新たな脆弱性	2,951
悪意あるコード挿入	1,066
脆弱性スキャン	615
総計	36,185

(4) クラウドメールセキュリティによる不審な挙動の検知状況

- クラウドメールセキュリティによりクラウドメールの通信を監視することで、ランサムウェや標的型メールの侵入や情報漏えいを防止することができる。
- 3か月合計した1者あたりの検知件数は1,292.3件であった。検知内容はスパムメールが最も多い。

検知結果：クラウドメールセキュリティの検知件数（月別）

	11月	12月	1月	合計
検知対象の受信メール [件]	3,000	16,749	19,459	39,208
受信メールのうち検知した件数[件]	633	2,953	3,535	7,121
1者1か月あたり [件]	633.0	1,476.5	1,767.5	1,292.3

【クラウドメールセキュリティ】受信メールのうち検知した項目別の検知件数

項目名	検知件数 [件]
スパムメール対策	5,762
不正プログラム検索	1,287
Webレピュテーション	72
総計	7,121

6．サイバー攻撃の実態調査の結果と分析

6.2 セキュリティ機器の検知結果（つづき）

(参考) 民間のUTM監視サービス及び過去のサイバーセキュリティお助け隊実証事業結果との比較

本事業の対象分野における検知件数が、一般市場における検知件数や、過去に実施したお助け隊実証における検知件数とどの程度乖離しているか比較を行った。比較においては条件を揃える必要があるため、本事業と同一機種のUTM（Cloud Edge）使用した、①NTT東日本のUTMサービスの全契約者のUTM検知件数（一般市場における検知件数のデータ）、②サイバーセキュリティお助け隊実証事業における検知件数のデータ（令和2年度NTT東日本の北海道エリア調査）のデータを用いて比較することとした。

①NTT東日本のUTMサービスの全契約者のUTM検知件数との比較

NTT東日本のUTMサービスの全契約者のUTM検知件数と本事業のUTM検知件数を、検知項目6項目に対して比較した結果、本事業のUTM検知件数は、不正プログラムとスパムメールの2項目が多かった。

1者1か月あたり [件]	不正プログラム	不正侵入防止(IPS)	不正サイト	スパムメール	ランサムウェア	C&Cコールバック
NTT東日本のUTMサービスの全契約者のUTM検知件数	0.6	560.0	25.3	195.0	0.1	0.0
本事業のUTM検知件数	6.2	16.1	12.5	689.1	0.0	0.0

＜算出条件＞
UTMサービス（おまかせサイバーみまもり）の20221年12月～2022年11月の全社検知実績を契約者数で割り算出。なお、NTT東日本のおまかせサイバーみまもり契約者は2022年11月末時点で276,468者。

②お助け隊実証事業（NTT東日本）調査結果との比較

令和2年度NTT東日本の北海道エリア調査のUTM検知件数と本事業のUTM検知件数を、検知項目6項目に対して比較した結果、本事業のUTM検知件数は、不正プログラムと不正サイト、スパムメールの3項目が多かった。

1者1か月あたり [件]	不正プログラム	不正侵入防止(IPS)	不正サイト	スパムメール	ランサムウェア	C&Cコールバック
令和元年度お助け隊実証事業新潟エリアのUTM検知件数	6.8	6,522.0	28.4	2,187.0	0.0	0.0
令和2年度お助け隊実証事業北海道エリアのUTM検知件数	0.2	57.8	2.4	185.1	0.8	1.5
本事業のUTM検知件数	6.2	16.1	12.5	689.1	0.0	0.0

＜算出条件＞
お助け隊実証事業のNTT東日本の調査では、本事業と同一機種であり、また、様々な業種の企業が含まれている。ただし、北海道エリアという地域と、集計期間が異なる。

6．サイバー攻撃の実態調査の結果と分析

6.3 UTM及びEDRの検知内容から想定されるリスク

2022年11月～2023年1月の3か月間のUTM及びEDR検知レポートの内容をセキュリティ専門家が確認し、リスクが想定される事項を確認し、各企業へ指摘した。その結果を以下に示す。

■UTM及びEDRの検知内容から想定されるリスク

No	機器	検知内容	確認したのべ者数	想定されるリスク
1	UTM	スパムメールを配信するようなサイト、ファイル転送サービス、漫画を違法にダウンロードできるサイトにアクセス	9者 <内訳> 11月3者 12月4者 1月2者	違法サイトへのアクセスによりウイルス感染
2	UTM	社内LANに公開Webサーバがあり、ロシア、中国、アメリカ等のIPアドレスからの攻撃を検知	3者 <内訳> 11月1者 12月1者 1月1者	Webサーバがウイルスに感染した際、同一ネットワーク内の端末へ拡散
3	EDR	Windows Defenderがウイルス検知した情報（イベントログ）をEDRで検知	5者 <内訳> 11月1者 12月3者 1月1者	ウイルス感染
4	EDR	アドウェアの利用を確認	4者 <内訳> 11月2者 12月1者 1月1者	不要ソフトを気が付かず導入しウイルス感染 ※企業側に確認したところ、アドウェアを意図せず導入していたとのこと。
5	EDR	アプリケーションが想定外の挙動をしているためEDRが検知（アプリが別アプリ起動、OSコマンド実行等）	24者 <内訳> 11月7者 12月8者 1月9者	Emotet等、正規ソフトに隠れたプログラムによるウイルス感染
6	EDR	OSコマンドの利用をEDRが検知	3者 <内訳> 11月2者 12月1者 1月0者	従業員によるハッキング
7	EDR	OSに登録のないアプリケーションの利用をEDRが検知	10者 <内訳> 11月2者 12月4者 1月4者	不審なアプリケーションのインストールによるウイルス感染

7．本調査の分析結果の考察

- 本事業で実施した、現況調査の分析結果およびサイバー攻撃の実態調査の分析結果を用い、経済安全保障上重要となるサプライチェーン上の中小企業に対するリスクと有効な対策を以下のとおり考察した。

7.1 検知したサイバー攻撃のリスク

本事業の調査結果から、以下３点のサイバー攻撃リスクがあると考えられる。

①メールやWebを契機としたウイルス感染リスク

標的型攻撃メールは多くの事案が報告されているところ、「メールセキュリティ意識調査」においては、ユーザー単位（メールアドレス単位）では約2割、**企業単位で約7割が標的型攻撃メールを模したメール開封**しており、中小企業側の意識が依然として高くない状況が伺える。また、「サイバー攻撃の実態調査」においては、**不正プログラムの検知件数が1者1か月あたり平均6.2件、スパムメールの検知件数が1者1か月あたり平均689.1件検知**されており、**外部からの攻撃にさらされている状況**が確認できた。Webの利用に関しても、**不正サイトへのアクセス検知件数が1者1か月あたり12.5件検知**されており、Webの利用において**利用者が意図せずに不正サイトにアクセスしている事象が発生している可能性**があると考えられる。

②不審なアプリケーションを気づかず導入し、ウイルス感染するリスク

「サイバー攻撃の実態調査」において、「**アプリケーションが想定外の挙動をしている事象**（アプリが別アプリ起動、OSコマンド実行等）」を**のべ24者（11月-1月） EDRが検知**した。確認したところ、危険を伴う挙動とは認識していなかったケースもあった。また、**アドウェアの利用をのべ4者（11月-1月） EDRが検知**したが、確認したところ、情報システム担当では導入を把握しておらず、利用者も導入した記憶がなく、不要なアドウェアが意図せず導入されていた。これらのことから、**Emotet等、正規のアプリケーションに隠れて不正なプログラムが動作されることに気が付かないリスク**がある。

③工場系LAN等の情報システム部門管理外設備でのウイルス感染リスク

「セキュリティ対策状況調査」において、「技術部門のCADパソコンが社内LANに接続されているが管理できていない」、「工場のFA端末は社内LANとは別のLANを利用し管理できていない」等、**工場系LAN等の管理が情報システム部門の管理外である実態**が確認できた。一方、「工場のFA端末等一部端末はウイルス対策ソフトが未導入」、「USBメモリは製造部門で自由に使っている可能性がある」等、**情報システム部門の管理外でのウイルス感染の可能性**があると考えられる。

7．本調査の分析結果の考察

7.2 サイバー攻撃のリスクへの対策

本事業の調査結果から考えられる３つのサイバー攻撃リスクに対し、有効な対策について考察を行った。サイバー攻撃に有効な対策を要約すると、「①サイバー攻撃をUTMとEDRの双方で防御」し、「②検知レポートを定期的に確認してリスクを把握」し、「③セキュリティ有識者等の目線で工場系ネットワーク設計を適正化」することである。

リスク１

想定されるサイバー攻撃	有効な対策
メール・Web契機としたウイルス感染	UTMとEDRの双方で防ぎ、被害拡大を防止 • UTMでスパムメールやウイルス添付メールをブロック • EDRでメール開封時のウイルス感染を検知 • UTMとEDRでC＆Cサーバへの通信をブロック

リスク２

想定されるサイバー攻撃	有効な対策
不審なアプリを気づかず導入し、ウイルス感染	UTMとEDRの双方で端末の挙動を定期的に確認 • UTMで異常な通信（ある端末だけトラフィックが多い等）を検知 • EDRでアプリケーションの異常な挙動（ファイル生成、他アプリ起動、OSコマンド実行等）を検知

リスク３

想定されるサイバー攻撃	有効な対策
工場系LAN等の情報システム部門管理外設備でウイルス感染	セキュリティの有識者等によるネットワーク構成の確認 • OSのバージョンが古くウイルス対策などが行われていない工場系LAN内の端末がウイルス感染しても、社内LAN経由で感染拡大しないようUTMとEDRで検知・ブロックする等、セキュリティ有識者の目線で確認を行い、ネットワーク設計の適正化を行う

7．本調査の分析結果の考察

7.3 対策実施のために必要な要件

サイバー攻撃に有効な対策である、「①サイバー攻撃をUTMとEDRの双方で防御」、「②検知レポートを定期的に確認してリスクを把握」、「③セキュリティ有識者等の目線で工場系ネットワーク設計を適正化」の実施に向けての必要な要件について以下に記載する。

①サイバー攻撃をUTMとEDRの双方で防御

効果：多層防御、およびUTMとEDRの双方を調べることでサイバー攻撃の挙動を把握
要件：UTMとEDRの双方の検知レポートを確認して被害箇所を特定できる体制

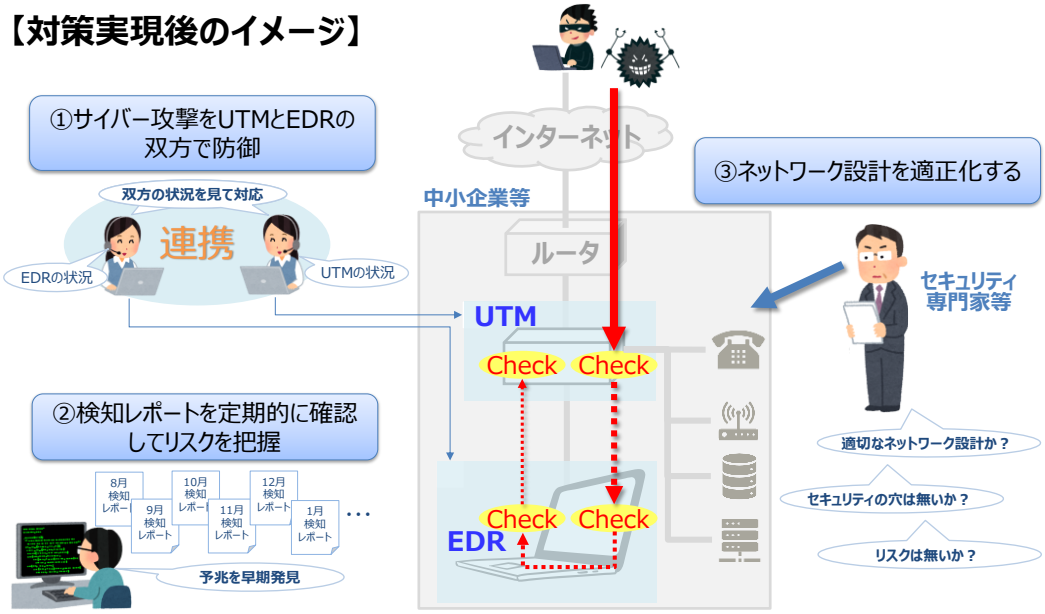
②検知レポートを定期的に確認してリスクを把握

効果：人手では気付けないリスクに対処できる
要件：セキュリティ専門家等による検知レポートの定期的な確認

③セキュリティ有識者等の目線でネットワーク設計を適正化

効果：企業が抱えるセキュリティホールを無くす
要件：セキュリティ専門家等によるネットワーク全体の見直しとリスクの把握・備え。

【対策実現後のイメージ】



【検討課題】

- サービス価格が中小企業が導入し易い価格帯にできるか。特に人手に関わる費用対策
- セキュリティ有識者等の専門家の効率的なリソース確保