令和２年度中小企業サイバーセキュリティ対策支援体制構築事業

（サイバーセキュリティお助け隊事業）

（実証対象：自動車産業（静岡県、広島県等））

成果報告書

請負事業者：東京海上日動リスクコンサルティング株式会社

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

目 次

1. サマリー

本報告書は、東京海上日動リスクコンサルティング株式会社（以下「東京海上日動リスクコンサルティング」という。）が「令和２年度中小企業サイバーセキュリティ対策支援体制構築事業」において実施した実証内容を報告するとともに、結果に基づき中小企業のサイバーセキュリティ対策について提言するものである。

自動車産業に関わる中小企業 31 社を対象に、以下のサイバーセキュリティ対策サービスを提供し、それぞれの結果から、中小企業のサイバーセキュリティ対策の実態を把握し、今後中小企業が継続的に利用可能なサービスおよび保険について検討を実施した。

- 問診
- 外部診断（インターネット公開情報に対する診断）
- 内部診断（社内ネットワーク PC 等に対する脆弱性診断）
- マルウェア対策診断
- 不正通信監視（監視機器（UTM 等）の設置）

2. 背景・目的

2.1 背景

近年、IoT 等の技術革新やテレワークの普及に伴うオンライン業務の増加等により、企業を標的とするサイバー攻撃は増加の一途を辿っている。サイバー攻撃の手法も高度化・巧妙化するなど、企業はセキュリティ対策などのリスク軽減策だけではサイバー攻撃の被害から完全に逃れることは難しくなってきている。また、「サプライチェーン攻撃」と呼ばれる中小企業サプライヤーを踏み台として大企業を狙う新たな攻撃に焦点があたっており、経済産業省「サイバーセキュリティ経営ガイドライン」においても、サプライチェーンマネジメントの重要性が掲げられている。

とりわけ、日本の基幹産業である自動車産業においても、コネクテッドカーや自動運転等の技術革新が進む中、WP29[1] において自動車サイバーセキュリティに関する国際基準がグローバルベースで整備されようとしている。日本においても OEM[2]メーカーをはじめとしたサプライチェーン全体のセキュリティ対策が急ピッチで進められている。通常、OEM メーカーは多くの部品をサプライヤーから調達しており、一次サプライヤーを Tier1、一次サプライヤーに納入するサプライヤーを Tier2 と呼ぶなど、自動車産業はこれらが多層化された産業構造になっている。これら多層にわたる中小企業サプライヤーを含めたサプライチェーン全体のリスクマネジメントは極めて重要であり、喫緊の課題である。

2.2 目的

本実証事業の目的は、自動車産業における中小企業サプライヤーに焦点をあて、そのセキュリティ状況の実態を把握し、セキュリティ意識向上を図りながら、セキュリティ対策の定着を図ることにある。

上記のとおり、自動車産業では、OEM メーカーを中心としたセキュリティガバナンス態勢強化が本格的に進められようとしているが、実際には多層にわたる中小企業サプライヤーのセキュリティ対策の普及には多くの課題が散在している。本実証事業では、有事の際の事後対応の支援にとどまらず、平時のセキュリティ対策状況の実態把握や今後の支援をスコープに入れ、自動車産業に属する中小企業サプライヤーの課題やニーズを調査し、多層にまたがるサプライチェーンのセキュリティ強化を目的とした今後のビジネス化に向けた考察を実施することも視野に入れる。

---

[1] 自動車基準調和世界フォーラム（World Forum for Harmonization of Vehicle Regulations）の略称。

[2] 一般的には他社ブランドの製品を製造することを指すが、自動車産業では完成車メーカーを指す。

3. 実証事業の概要

3.1 実証対象（地域／産業分野）の選定

実証対象の選定にあたっては、日本の基幹産業であり多くの中小企業を傘下に抱えるサプライチェーン産業である自動車産業に焦点をあてた。自動車産業においては、既に多くのサイバー攻撃に晒されるなど、中小企業サプライヤーに対するサイバーセキュリティ対策の底上げが急務であり、その実態に迫ることは大きな意義があると考え、本実証事業では当該産業を実証対象として選定した。

また、実証事業終了後も全国のサプライチェーンで広く活用できるモデルの構築を実現するため、サイバーセキュリティ支援企業が比較的少ないと想定される地域（首都圏、中京圏、近畿圏でないこと）での実態が把握できることも加味した上で、実証対象地域として静岡エリアおよび広島エリアを選定した。

3.2 スケジュール

本実証事業のスケジュールは、以下のとおりである。

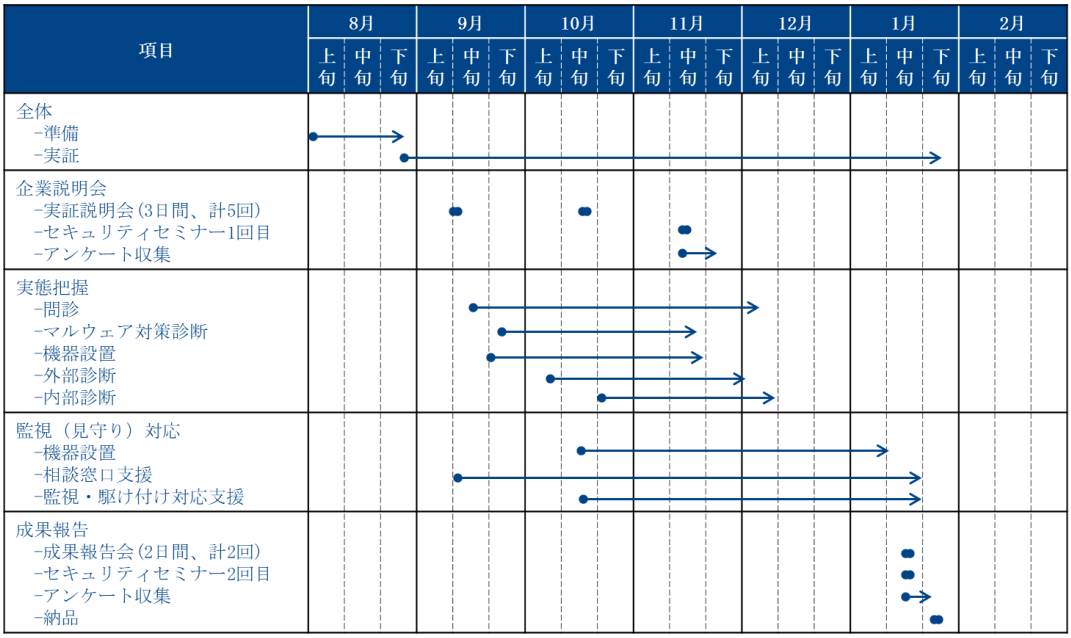


図 1 実証事業スケジュール

3.3 実証参加企業

（1） 実証参加企業数

本実証事業には、静岡エリアおよび広島エリアから中小企業サプライヤー31 社（静岡エリア：23 社、広島エリア：8 社）が参加した。実証参加企業の内訳は以下のとおり。

（2） 実証参加企業属性内訳

① 業種別

実証参加企業 31 社の業種は、全て「E. 製造業」である。

② 資本金別

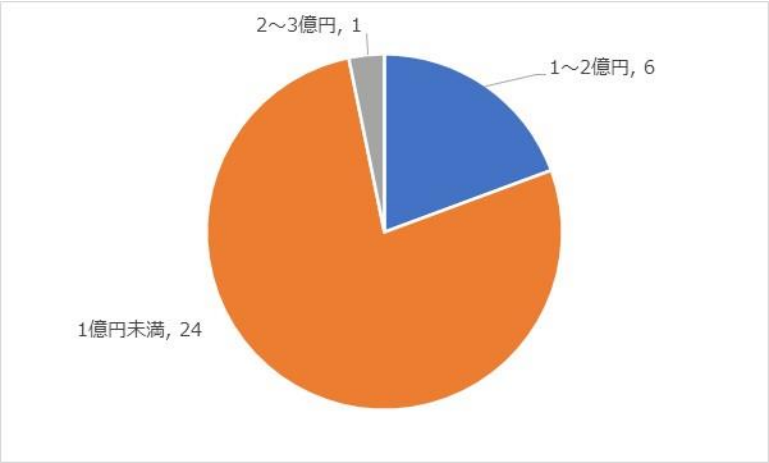


図 2 実証参加企業資本金内訳

③ 従業員数別

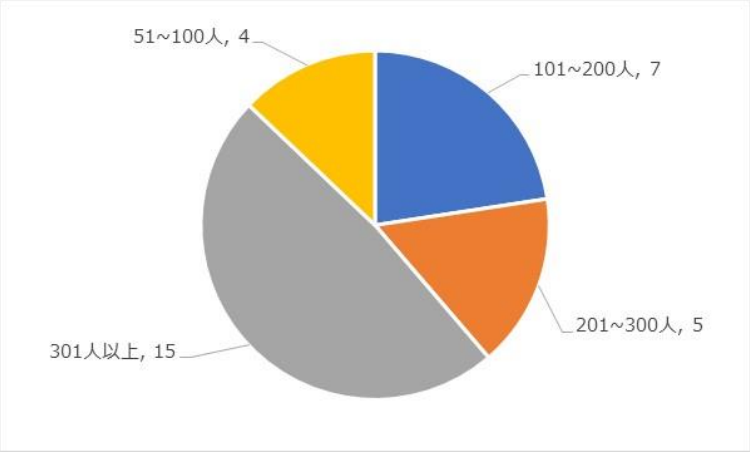


図 3 実証参加企業従業員数内訳

3.4 実施内容

3.4.1 実施内容の全体像

本実証事業では、以下のセキュリティ対策実行サイクルを構成する 6 つの要素から 4 つを実施した。

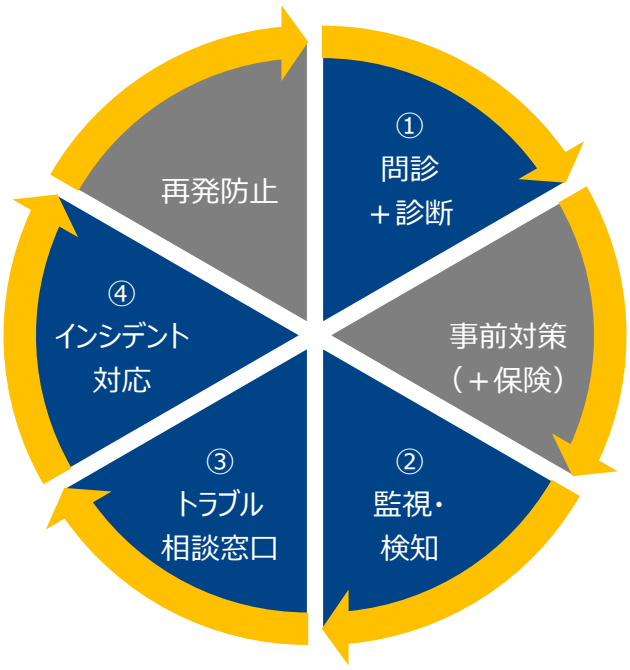


図 4 セキュリティ対策実行サイクル

上記サイクルにおける各要素の説明は以下のとおりである。

（1） 問診＋診断：

問診（セキュリティアセスメント）は、IT 担当者におけるセキュリティ意識に関する事態把握を行う目的で、また診断は、企業のシステム環境におけるセキュリティ管理レベルや脆弱性等の実態把握を行う目的で実施した。本実証事業では双方を実施することで企業環境のセキュリティ対策状況を「セキュリティマネジメントの観点」と「技術的対策の観点」において、実態把握を行った。

また、自動車産業の中小企業サプライヤー複数社を調査対象とすることで、企業単体では見えない傾向を把握し、業界全体の底上げに必要な支援策の検討に活用する。

（2） 監視・検知：

実証参加企業にセキュリティ監視機器を設置し、不正な通信の発生等を定常的にモニタリング（見守り）することで、中小企業サプライヤーに対するサイバー攻撃の実態を把握するために実施した。

（3） **トラブル相談窓口**：

実証参加企業が電話もしくはメールにて気軽に相談できる窓口を用意し、本実証事業ならびに情報セキュリティ等に関わる全ての相談を受け付けた。

（4） **インシデント対応**：

実証参加企業に設置したセキュリティ監視機器によるモニタリング（見守り）において、インシデント（重篤な問題）を検出した場合は、トラブル相談窓口を通じて速やかに企業の担当者と連携し、リモートサポートで解決を試み、リモートサポートによる解決が困難と判断した場合には、現地へ駆け付け対応を実施した。

＜補足＞

実証後に、中小企業が費用面でも導入しやすいサービスを検討するため、本実証事業ではリモートサポートでの解決を優先的に実施した。

【参考】

本実証事業では実施しなかった以下の 2 つについても実証後のサービス検討時には検討を行う想定である。

・事前対策（＋保険）：

問診＋診断で収集した情報から到達すべき最低限のセキュリティ対策レベルを満たしていない場合にモデル化された事前対策の実施およびリスク移転としてのサイバー保険加入を含めた事前対策サービスの検討を行う予定である。

・再発防止：

本実証事業で得た実態をもとに、インシデント発生後の対策相談や専門家派遣等を含めた再発防止に必要な要素についても保険サービスとして実現可能性の検討を行う予定である。

3.4.2 実施内容の詳細

(1) 問診

① 目的

問診は実証参加企業の IT 担当者におけるセキュリティ意識に関する実態把握を目的に実施した。

② 実施内容／実施方法

本問診の実施においては、自動車産業の特性に応じた問診を実施することが望ましいため、東京海上日動リスクコンサルティングや NTT グループで保有する知見を用いて、OEM メーカーのセキュリティガイドラインも加味した上で、サプライヤーの実態把握に即した問診を実施した。

また、実施方法についても Web 画面を用いたオンラインでの問診に回答してもらうだけでなく、回答してもらった内容をもとに、約 3 時間各実証参加企業担当者とリモート会議による回答内容をベースとしたヒアリングを行い、回答内容の深堀りや項目の解釈誤り、回答漏れの追加確認等を行うことで、企業ごとの回答レベルの偏りをなるべく排除し、正しい傾向が取得できるよう実施した。

以下が実際の実施フローである。

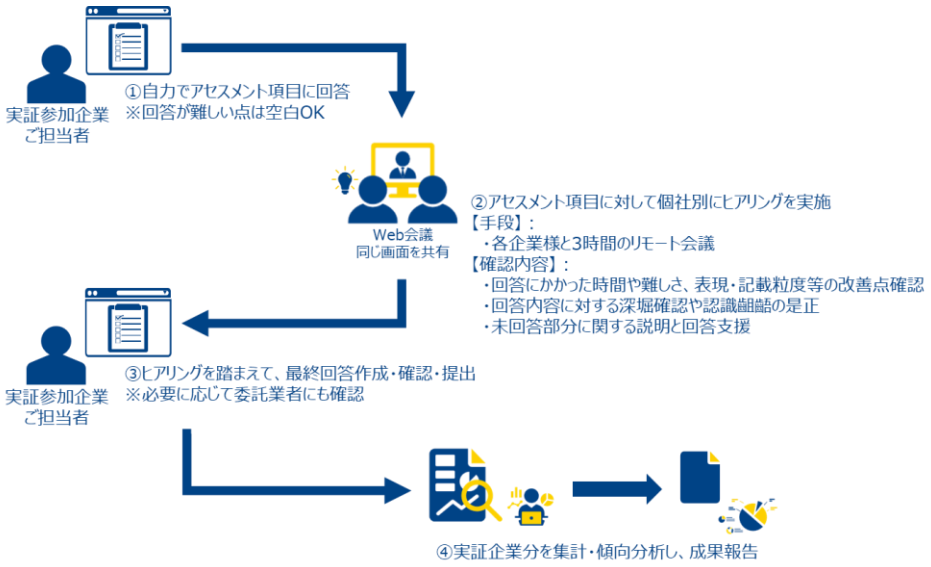


図 5 問診実施フロー

【参考】

Web 画面を用いたオンライン問診ツール（Atlas）についての特徴・機能および画面イメージは下記のとおりである。

表 1 Atlas の特徴および機能

特徴	機能
・サプライチェーン向けサイバーリスク管理にフォーカスしたアンケートシステム ・オンラインでのアンケート配布・回答システムであり、周期的に実施される問診・アセスメントに関し、AI 処理により回答者の負担を軽減	・オンラインでのアンケートの配布・回答、進捗管理 ・外部診断で評価可能な設問について、回答結果と診断結果を相関させた客観的判断が可能 ・アンケート回答に対する問題点や具体的な指示・改善事項に関するレポートをオンラインで提示

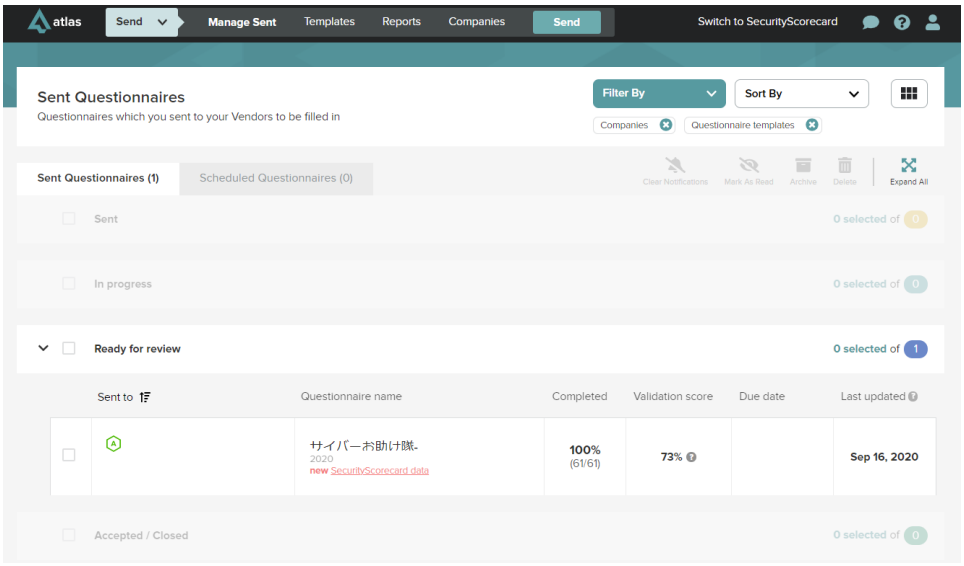


図 6 Atlas の画面イメージ 1（サンプル）

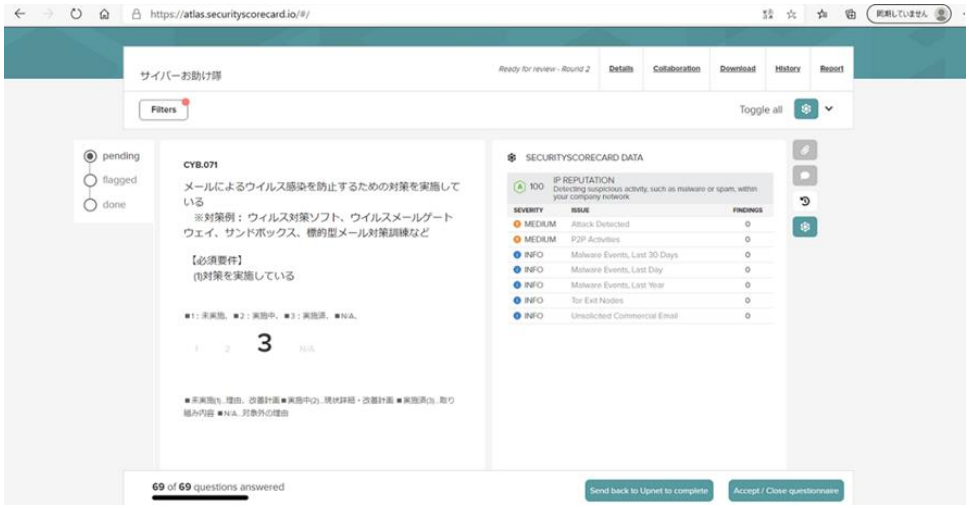


図 7 Atlas の画面イメージ 2（サンプル）

③ 確認／検証ポイント

ア　アセスメント実施全般に関する実態

①アセスメント全体の回答にかかった時間
②アセスメントの難易度
③セルフチェックとその後の回答支援に関する効果
④アセスメントツールの使いやすさ

イ　実証参加企業の IT 担当者におけるセキュリティ意識に関する実態

(2) 外部診断

① 目的

外部診断は実証参加企業が利用している企業ホームページ等のインターネットに公開されている情報に対する診断を行うことで、セキュリティ管理レベルの実態把握を目的に実施した。

＜補足＞
セキュリティ管理レベルとは、診断対象企業のセキュリティリスク対策状況を他企業の対策状況と比較し、相対的に評価したスコアおよびレーティングされたランクを指す。

② 実施内容／実施方法

本診断については、SecurityScorecard という外部診断用ツールを用いて、実証参加企業のインターネットに公開している企業ホームページ等に関するサイトのドメインを対象に非攻撃的診断によるセキュリティ管理レベルを評価することで実態把握を行った。

以下が実施イメージである。

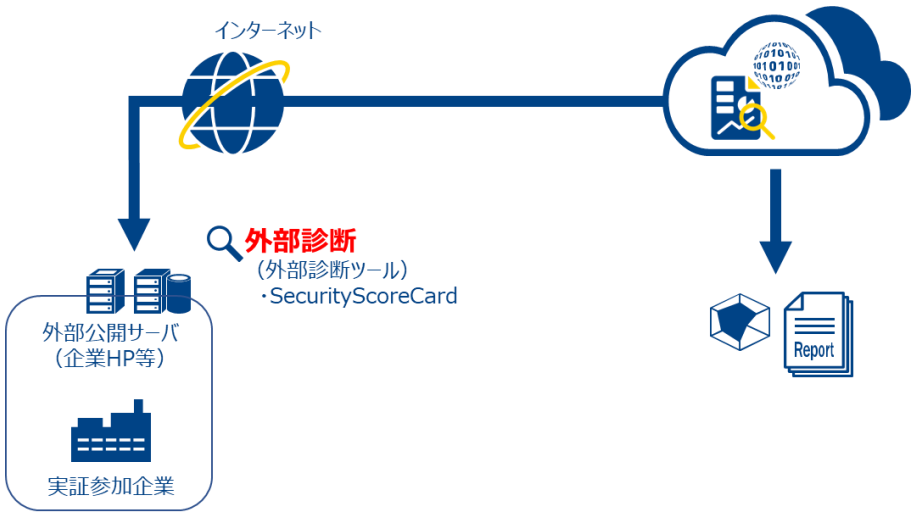


図 8 外部診断実施イメージ

③ 確認／検証ポイント

実証参加企業を自動車産業サプライチェーンの標準的な集団として、以下の 5 点を評価軸に実態把握を実施した。

- 自動車産業サプライチェーンと製造業全体のセキュリティ管理レベルの比較
- 自動車産業サプライチェーンのリスク傾向
- インターネット上で悪用される可能性の高いアプリケーションポート（データベース、Windows ファイル共有、リモートデスクトップ）の利用状況
- シャドーIT の可能性がある SSL 証明書期限切れサーバーのチェック

・マルウェアの影響と見られる通信状況のチェック

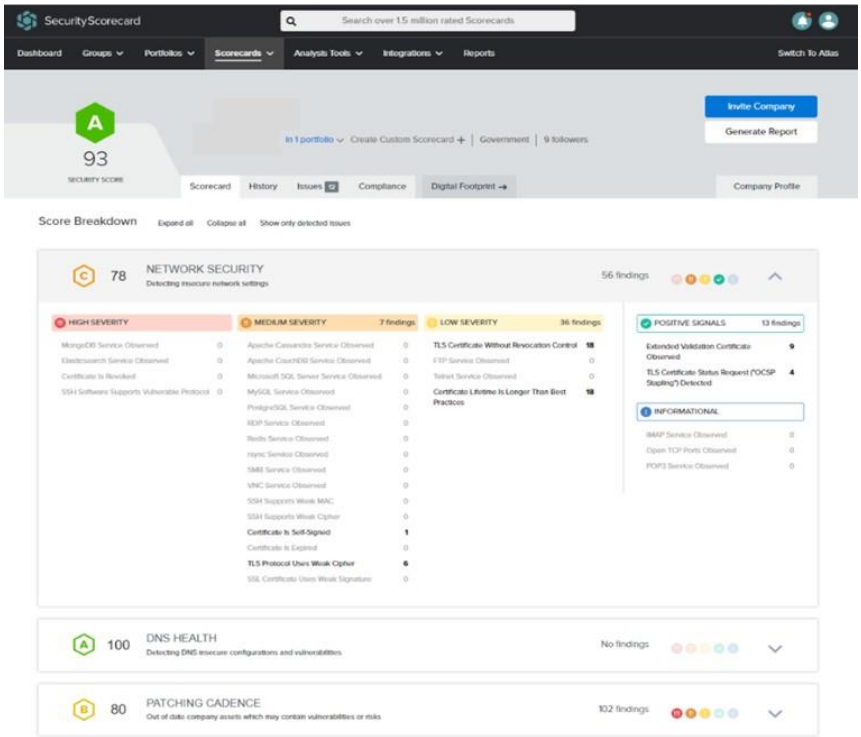
【参考】

外部診断で用いた診断ツール（SecurityScorecard）についての特徴・機能および画面イメージは下記のとおりである。

表 2　SecurityScorecard の特徴および機能

特徴	機能
・インターネットに公開されている企業ドメインに紐付いたシステムの「サイバーリスク管理レベル」を判定 ・自社保有ドメイン以外に、他社システムも公開情報をベースに客観評価が可能	・企業のドメイン名に関連したインターネット上のデジタル資産を見える化 ・10 分類、87 項目のセキュリティチェック ・検出した課題の詳細レポート ・100 万社のチェック結果の統計分析による客観的なリスクマネジメントレベルのレーティング

図 9　SecurityScorecard の画面イメージ（サンプル）



(3) 内部診断

① 目的

内部診断は実証参加企業の社内ネットワークに接続されたパソコン等に対する脆弱性診断を行うことで、企業内部に潜む脆弱性等の実態把握を目的に実施した。

② 実施内容／実施方法

実証参加企業における社内ネットワークの一部セグメントに対して、Linux BOX を設置し、脆弱性診断を実施。あるいは、普段利用しているクライアント端末（パソコン）に Tenable の Nessus Agent をインストールし、端末の脆弱性診断を実施した。

以下が実施イメージである。

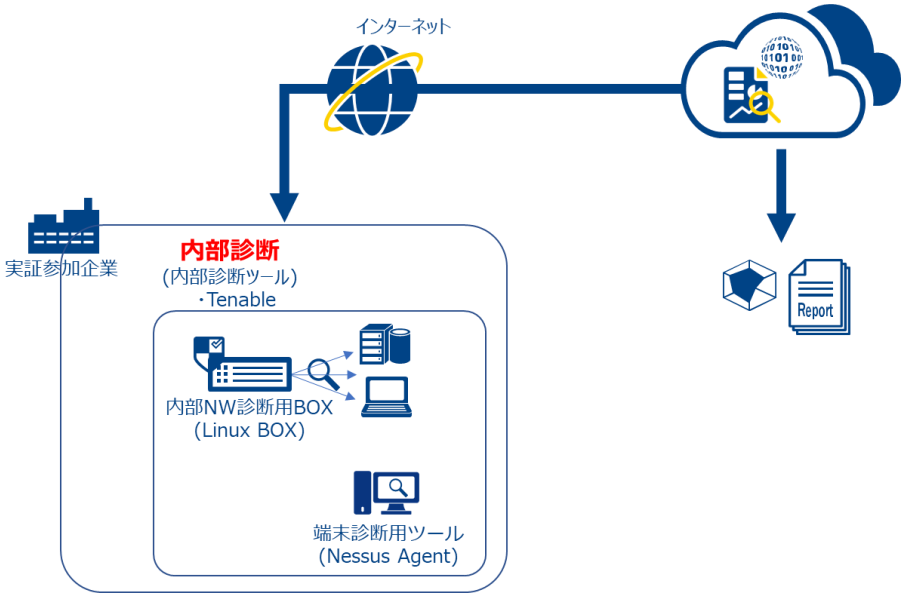


図 10 内部診断実施イメージ

③ 確認／検証ポイント

・診断ネットワーク上の端末のパッチマネジメント（CVSS[3]スコア 7.0 以上の脆弱性がどの程度存在しているか。）は適切に実施できているか。
・サポート切れ OS が利用されていないか。

[3] 共通脆弱性評価システム（Common Vulnerability Scoring System）の略称。 IT 機器の脆弱性（攻撃されやすさ）を示す指標で、脆弱性の危険度をスコア（0.0～10.0）で表す。10.0 は最も危険度が高い脆弱性を示し、一般にスコア 7.0 以上の危険度を持つ脆弱性は優先度を高く、対応することが推奨されている。

【参考】

内部診断で用いた診断ツール（Tenable）についての特徴・機能および画面イメージは下記のとおりである。

表 3　Tenable の特徴および機能

特徴	機能
・ネットワーク内外からサーバーやアプリケーションの脆弱性を詳細に検出することが可能 ・SaaS 型の脆弱性診断、実装やスキャン開始のリードタイムが少ない ・今回の施策では事前に設定済のため、専用の Linux BOX を社内ネットワークに繋ぐだけで簡単導入 ・端末にソフトウェアを入れることで詳細の診断が可能	・IT 資産に対する脆弱性診断の実施 ・複数の脆弱性検査手法を有しており、同時にパソコンやネットワーク機器など複数の対象についての脆弱性検査を実施 ・脆弱性の管理や対応を効果的に行う支援ツール ・検出した診断情報をもとに様々な角度から脅威を可視化、サイバーリスクの常時スコアリング実施、リスク対策の運用を支援するツール ・脆弱性/資産価値に基づいたリスクレーティング機能 ・診断結果や診断実施を外部のシステムと連携する API 機能

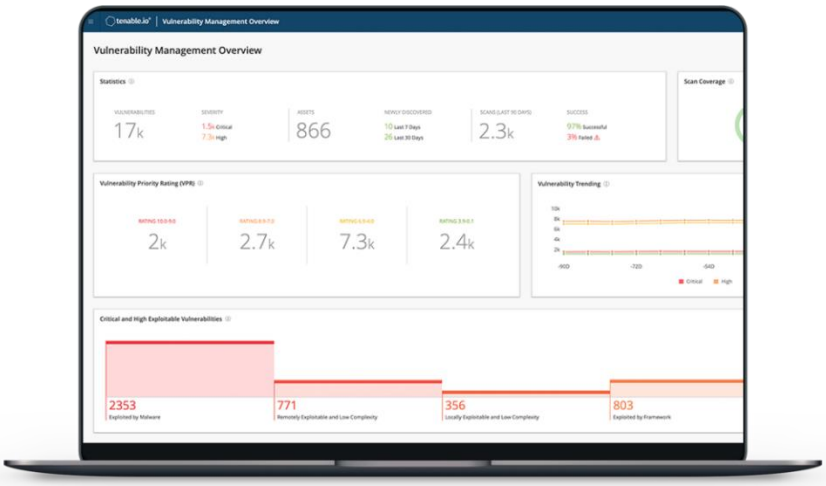


図 11　Tenable の画面イメージ

Tenable：https://jp.tenable.com/products/tenable-io?tns_redirect=true（2020/1/15 参照）

(4) マルウェア対策診断

① 目的

実証参加企業のクライアント端末におけるマルウェア対策の状況や傾向に関する実態把握を目的に実施した。

② 実施内容／実施方法

本診断においては、無害の「疑似マルウェア（zip 形式）」および「実行形式ファイル（exe 形式）」をそれぞれ準備し、診断対象者へ以下 2 パターンの実証を実施した。

・メール添付ファイルとして受信
・試験用サイトからのファイルダウンロード

なお、診断結果については、診断対象者に結果票を記載して返送する形式で実施した。

以下が実施イメージおよび結果票のサンプルである。

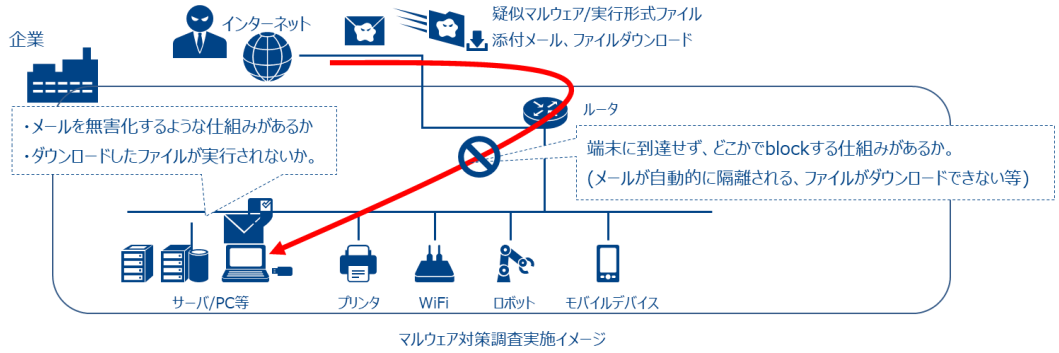


図 12 マルウェア対策調査実施イメージ

メール診断結果

	確認事項	回答欄
診断メール① （疑似マルウェア添付）	・添付は、無害な疑似マルウェアファイルです。 ・メールを受信したか、添付ファイルの実行ができたか、確認致します。	
1-1.メール受信確認	**＞件名：【お助け隊事務局】【メール診断：２通目】診断メール①（疑似マルウェア添付のメールを受信しましたか？** 回答欄の **a.受信した** または **b.受信しなかった** を選択してください。	
1-2.診断作業 （添付ファイルの実行）	**＞メールを受信した場合、添付ファイルを解凍し、解凍後のファイルの実行(開くこと)はできましたか？** 回答欄の **a.実行できた**、**b.実行できなかった**、**c.ファイルが添付されていなかった** の中から１つを選択してください。	
診断メール② （実行形式ファイル添付）	・添付は、診断用に作成された無害のファイルです。 ・受信したか、ファイルを実行できたか、確認致します。	-
2-1.メール受信確認	**＞件名：【お助け隊事務局】【メール診断：３通目】診断メール②（実行形式ファイル添付）のメールを受信しましたか？** 回答欄の **a.受信した** または **b.受信しなかった** を選択してください。	
2-2.診断作業 （添付ファイルの実行）	**＞メールを受信した場合、添付ファイルの実行(開くこと)はできましたか？** 回答欄の **a.実行できた**、**b.実行できなかった**、**c.ファイルが添付されていなかった** の中から１つを選択してください。	
診断メール③ （URLからダウンロード）	・メール本文に記載されているURLは、診断メール用に作成されたサイトです。 ・URLリンクをクリックすると、無害な疑似マルウェアファイル（hogehoge.zip）と無害な実行形式ファイル(hogehoge.exe）のダウンロードされるか、ブラウザが起動して文字列が表示されます。 ・ファイルがダウンロードできた場合は、ファイルをダブルクリックして実行してください。	-
3-1.診断作業 （疑似マルウェアファイルのダウンロード）	**＞URL先（右記）よりhogehoge.zipをダウンロードできましたか？** 回答欄の **a.ダウンロードできた** または **b.ダウンロードできなかった** を選択してください。	URLリンク
3-3.診断作業 （疑似マルウェアファイルの実行）	**＞ダウンロードしたhogehoge.zipを解凍し、解凍後のファイルの実行(開くこと)はできましたか？** 回答欄の **a.実行できた**、または **b.実行できなかった** を選択してください。	
3-6.診断作業 （実行形式ファイルのダウンロード）	**＞URL先（右記）のhogehoge.exeをダウンロードできましたか？** 回答欄の **a.ダウンロードできた** または **b.ダウンロードできなかった** を選択してください。	URLリンク
3-8.診断作業 （実行形式ファイルの実行）	**＞ダウンロードしたhogehoge.exeの実行(開くこと)はできましたか？** 回答欄の **a.実行できた**、または **b.実行できなかった** を選択してください。	

図 13 試験結果記入票（サンプル）

③ 確認／検証ポイント

・添付メール経由および Web サイトからのファイルダウンロード経由による「疑似マルウェア」が端末まで到達することなく、防御できているか。また、到達した場合でも端末側でファイル実行が抑止できているか。

「到達して実行ができる＝診断端末で実マルウェアに感染するリスクが極めて高い」

・添付メール経由および Web サイトからのファイルダウンロード経由による「実行形式ファイル」が端末まで到達することなく、防御できているか。また、到達した場合でも端末側でファイル実行が抑止できているか。

「到達して実行ができる＝悪意あるファイルが実行され、感染に繋がる」

(5) 不正通信監視

① 目的

実証参加企業のインターネット通信における不正通信の状況や傾向に関する実態把握、および対象企業におけるセキュリティインシデントの防止を目的に実施した。

② 実施内容／実施方法

以下 2 パターンの監視機器を設置し、企業内の通信状態をモニタリングした。

ア　パターン 1：UTM（Cloudedge）の設置

企業内の通信状態をモニタリングし、有害サイトへのアクセス等を検知、必要に応じて自動で遮断を行った。

イ　パターン 2：StellarCyber の設置

企業内部ネットワークの通信状況をモニタリングし、外部からの攻撃だけでなく、内部ネットワークの振る舞いなどを、マシンラーニング／AI 技術を活用することで、SOC（セキュリティオペレーションセンター）業務における過検知負担や効率性、検知精度向上を図る。

また、パケットレベルでの監視により詳細な実態把握が可能となる。

以下が実施イメージである。

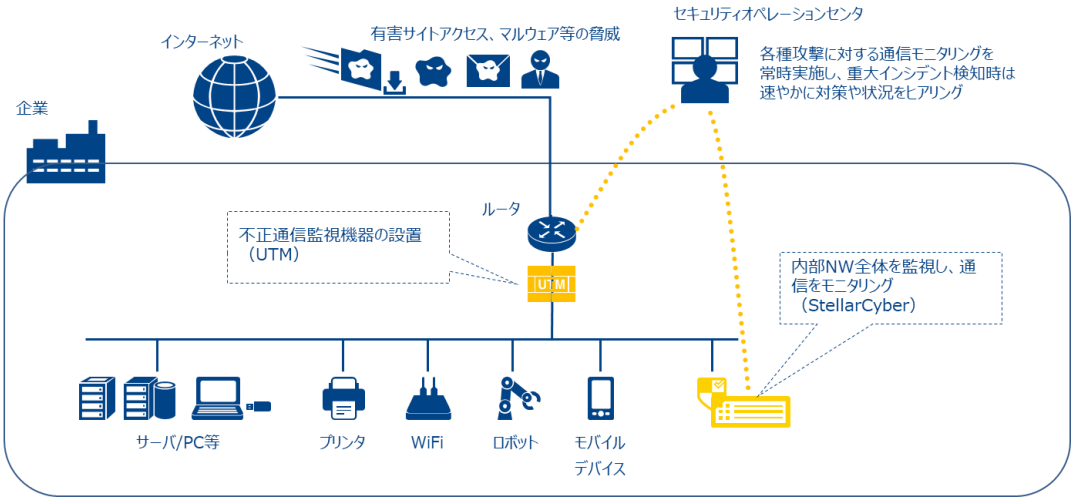


図 14 通信モニタリング実施イメージ

【参考】

不正通信の監視で用いた機器（Cloudedge および StellarCyber）についての特徴・機能は下記のとおりである。

表 4 不正通信監視機器（Cloudedge）の特徴および機能

特徴	機能
・事前に設定済のため、専用機を社内ネットワークに繋ぐだけで簡単導入 ・既存ネットワークの通信経路上への設置となるため、検知だけでなく遮断を実施することも可能 ・重大アラートのみを通知することで、参画企業の見落とし防止 ・一元窓口による相談受付	・アプリケーション利用制限 ・Web サイトアクセスブロック ・URL 指定によるアクセス制御 ・不正プログラム侵入対策 ・メールセキュリティ対策 ・ファイアウォール機能等のセキュリティ機能 ・状態通知機能（メール）

表 5 不正通信監視機器（StellarCyber）の特徴および機能

特徴	機能
・事前に設定済のため、専用機を社内ネットワークに繋ぐだけで簡単導入 ・ミラーポートへ設置となるため、既存ネットワークへの影響はなし。 ・トラフィック（パケットレベル）をマシンラーニング/AI 技術を利用して分析を行うため、怪しい通信を振る舞い挙動ベースで検知することが可能 ※シグネチャベースでは検知できない未知の攻撃をより精度高く検出することができる。 ・重大アラートのみを通知することで、参画企業の見落とし防止 ・一元窓口による相談受付	・マシンラーニング/AI を利用したトラフィック（フルパケット）ベースの振る舞い検知、分析 ・侵入検知システム、ファイルベース検知システムを利用した高度な検知、分析 ・マシンラーニング/AI を利用したログベースでの分析 ・複数のサードパーティ製品のログ取り込み、分析 ・オンプレ、仮想、クラウドなど様々な環境への対応、検知、分析

③ 確認／検証ポイント

自動車産業における中小企業サプライヤーについて、日常業務（定常時）のモニタリングを行うことで、どういった脅威が検出されるか等の実態を把握する。

(6) トラブル相談（一元窓口）

① 目的

本実証事業を進めるにあたり、実証参加企業が問合せ先に迷うことがないよう、本実証事業に関する全ての問合せおよび一次対応を行う窓口を設置し、サポートを実施した。

② 実施内容

メールと電話（フリーダイヤル）による一元窓口を設置し、インシデント発生時以外においても各種の困り事に関する受付を実施した。また、機器の監視から発生するアラートについても能動的にインシデントを判断し、状況に応じて、速やかにインシデント対応支援を行う体制を準備した。

以下が実施イメージである。

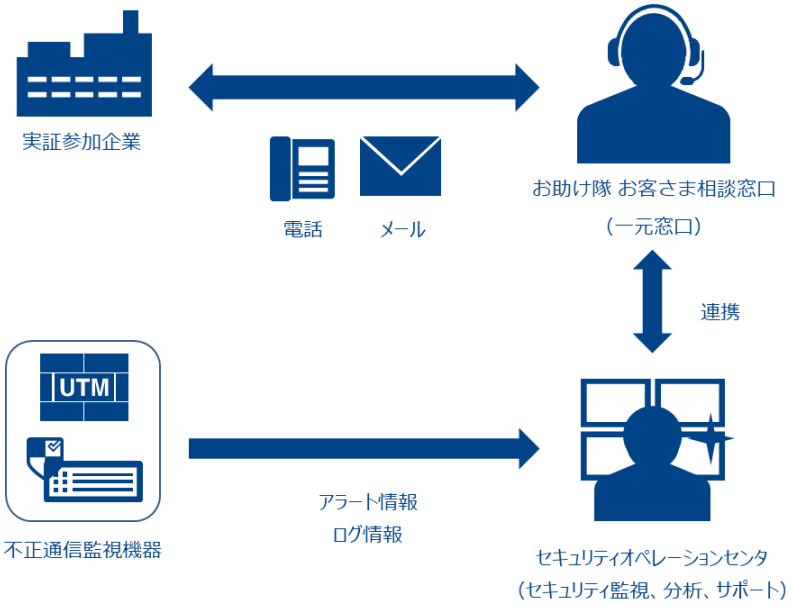


図 15 一元窓口サポートイメージ

(7) インシデント対応

① 目的

実証期間中に発生する様々なセキュリティインシデントに対して、事象の解決に向けたサポートを行うとともに、将来のサービス化に向けた詳細ヒアリング等を通じて実態把握を目的に実施した。

＜補足＞セキュリティインシデントとは、JPCERT/CC の定義によれば、情報および制御システムの運用におけるセキュリティ上の問題として捉えられる事象のこと。本実証事業では特に重篤な問題が発生し、サポートが必要な事象を指すものである。

② 実施内容

セキュリティインシデント発生時（モニタリングアラートだけでなく、実証参加企業の担当者からの申告も含む）は、トラブル相談窓口を通じて状況を確認し、リモートサポートにて事象の解決を優先的に実施した。

また、リモートサポートによる解決が困難と判断した場合には、現地への駆け付け対応を実施した。

以下が実施イメージである。

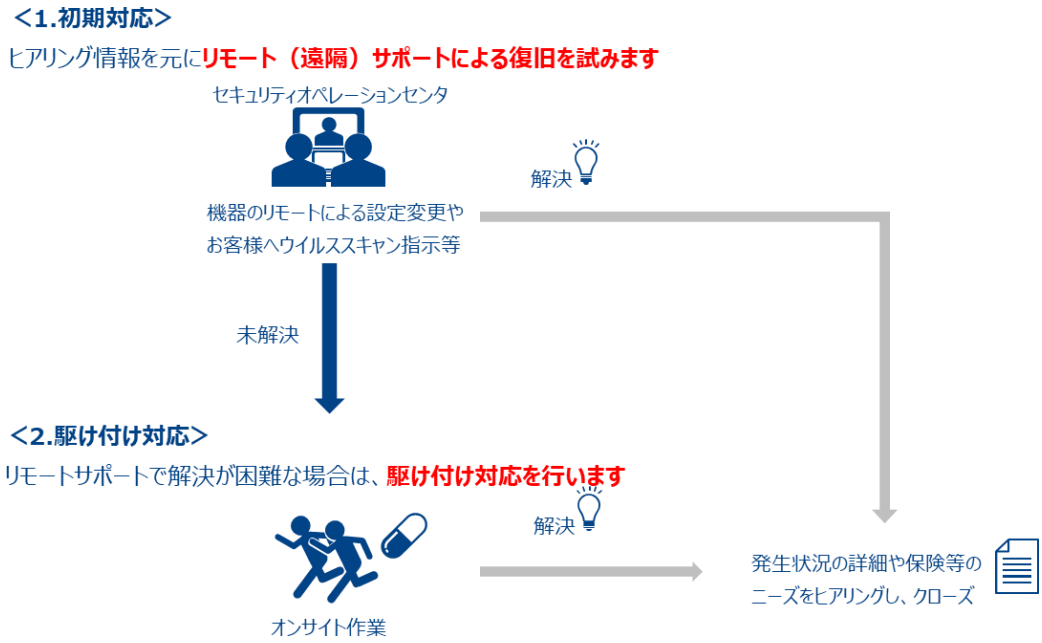


図 16 インシデント対応実施イメージ

4. 地域実証の結果

4.1 事業説明会の開催

本実証事業に参加する中小企業サプライヤーの募集を目的として、事業説明会を開催した。事業説明会の開催にあたり、静岡エリアおよび広島エリアを基盤とする各 OEM メーカーや OEM メーカーの取引先サプライヤーが複数加盟する各協同組合より、チラシ配布やメール配信による参加募集、サプライヤー経営者への電話による参加勧奨等の活動実施などの協力を得られ、本事業説明会へのスムーズな参加募集が実現し、早期に必要参加企業数を確保することができた。具体的な実施内容は以下のとおり。

4.1.1 開催日時・場所・実証参加企業

静岡エリアおよび広島エリアにおいて、事業説明会を以下のとおり合計 5 回開催した。開催については、新型コロナウィルスの影響もあり現地開催は断念し、全てオンライン形式での開催となった。

表 6 静岡エリア　事業説明会

名称	第 1 回「サイバーセキュリティお助け隊」事業説明会
開催日時	2020 年 9 月 9 日（水）13:00～15:00
形態	オンライン形式（Zoom 開催）
参加者数	13 名（8 社）

名称	第 2 回「サイバーセキュリティお助け隊」事業説明会
開催日時	2020 年 9 月 10 日（木）13:00～15:00
形態	オンライン形式（Zoom 開催）
参加者数	19 名（11 社）

名称	第 3 回「サイバーセキュリティお助け隊」事業説明会
開催日時	2020 年 10 月 10 日（木）15:00～17:00
形態	オンライン形式（Zoom 開催）
参加者数	23 名（10 社）

表 7 広島エリア　実証事業説明会

名称	第 1 回「サイバーセキュリティお助け隊」事業説明会
開催日時	2020 年 9 月 9 日（水）15:30～17:30
形態	オンライン形式（Zoom 開催）
参加者数	20 名（6 社）

名称	第 2 回「サイバーセキュリティお助け隊」事業説明会
開催日時	2020 年 9 月 10 日（木）15:30～17:30
形態	オンライン形式（Zoom 開催）
参加者数	23 名（11 社）

4.1.2 実施内容

事業説明会の実施内容は以下のとおり。静岡エリアおよび広島エリアにおける開催内容は全て以下同様の内容で実施した。

表 8 事業説明会の実施内容

第 1 章	本実証事業について
第 2 章	実施概要 ✓ セキュリティ対策実行サイクルの全体像と本実証事業の範囲 ✓ 対策支援サービス概要 ✓ システム構成
第 3 章	スケジュールについて
第 4 章	実施内容 ✓ 現状調査について ✓ セキュリティ対策における実態把握（問診および内部診断・外部診断）について ✓ マルウェアに対する実態把握について ✓ サイバー攻撃等の脅威に対する実態把握（設置機器について） ✓ 実証期間における相談・インシデントサポート対応について ✓ 相談受付について ✓ セキュリティインシデント対応について ✓ その他ご依頼事項について
第 5 章	実施体制について
第 6 章	参加規約について

4.2 セキュリティセミナーの開催

本実証事業に参加する中小企業サプライヤーの実態に関する情報収集、セキュリティ意識向上、サイバーセキュリティ対策普及に向けた国等の支援事業の周知等を目的として、セキュリティセミナーを以下のとおり開催した。業界の有識者等、外部講師を 3 名招聘し、最後にセキュリティ事態把握アンケートを実施した。

4.2.1 開催日時・場所・実証参加企業

表 9 セキュリティセミナー概要

開催日時	2020 年 11 月 12 日（木）15:00～16:50
形態	オンライン形式（Zoom 開催）
参加対象企業	静岡エリア・広島エリアの自動車産業に属する中小企業サプライヤー（本実証事業参加企業を含む）
参加者数	138 名（80 社）

表 10 セキュリティセミナー詳細

題目	自動車産業に属するサプライヤー企業が取るべきセキュリティ対策
セミナー内容	【Session 1】15:00-15:30 題目：サイバー脅威の現状と対応（一般財団法人日本サイバー犯罪対策センター（JC3）） 内容：ニューノーマルの中で DX が進み、情報システムの活用とそのセキュリティが一体となっている現在において、サイバー脅威の現状の解説とその対応の在り方を解説。 【Session 2】15:30-16:00 題目：自動車産業の大変革と新たなサプライチェーンマネジメント（J-Auto-ISAC） 内容：自動車製造・販売からモビリティビジネスに変わりつつある自動車産業の現状と、車両のコネクテッド化に伴って求められる新たなサプライチェーンマネジメントについて解説。 【Session 3】　16:00-16:20 題目：中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について（IPA） 内容：経済産業省および IPA の中小企業にサイバーセキュリティ対策普及に向けた支援事業について説明。 【Session 4】16:20-16:40 題目：サプライヤー企業が取るべきセキュリティマネジメントとサイバー保険（東京海上日動火災保険） 内容：サイバー保険の開発者としてこの保険の最も有効で効果的な活用ポイントや中小企業に有益な Web サイト（Tokio Cyber Port）を説明。
アンケート	セキュリティ実態把握アンケートの実施

4.2.2　セキュリティ実態把握アンケート結果

中小企業サプライヤーのセキュリティ実態把握を目的として、実証参加企業のほか、静岡エリアおよび広島エリアにおける他の中小企業サプライヤーも対象としたアンケートを実施した。主な集計結果を以下のとおり。（有効回答：n=64）

＜アンケート集計結果＞

Q1：業種を教えてください。　（ n=64 ）

実証参加企業の大半は「E. 製造業」であったが、一部製造業以外の業種からも 4 名回答を得た。

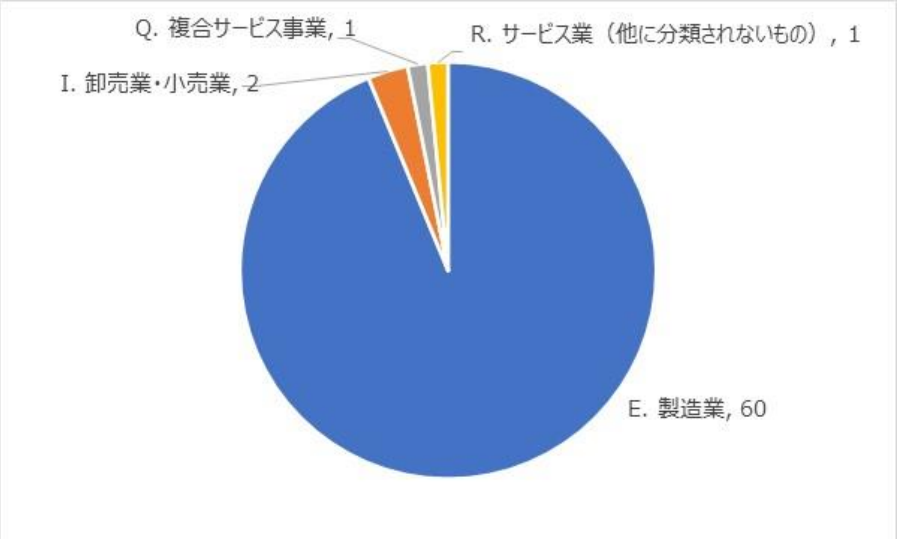


図 17 アンケート参加企業業種

Q2：Q1 で、「E. 製造業」を選択された場合、どのような製品を製造されているか教えてください。（ n=57 ）

「E. 製造業」の業種内訳として、約 80%と大半の企業がパワートレイン・シャシー等のエレキを含まない装置製造で、約 20%が制御系システム製造となった。

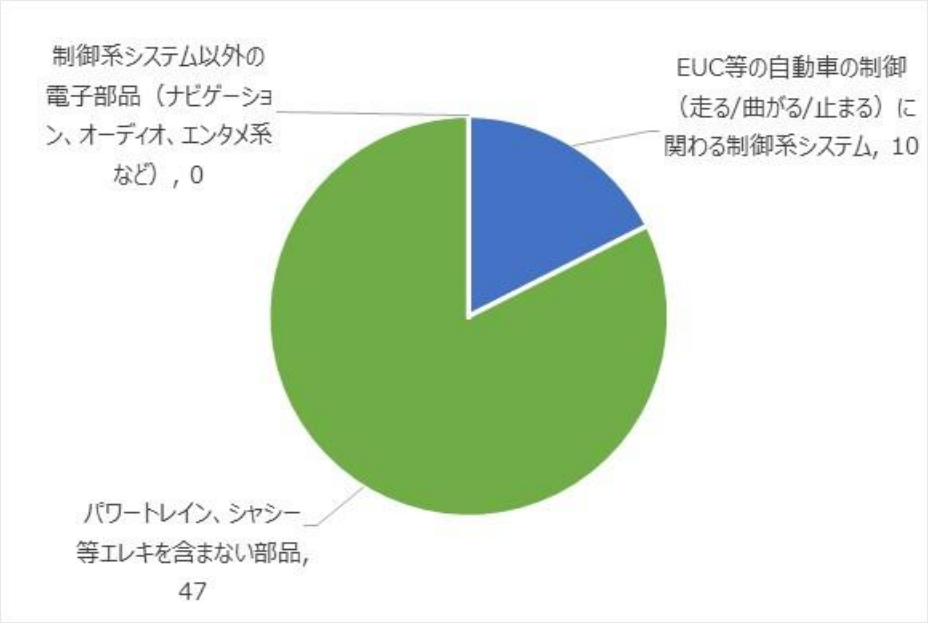


図 18 製造業者業種内訳

Q3：貴社に情報システムの専任担当者はいますか？ （ n=64 ）

情報システムの専任担当者が「いる」と回答したのは 36 名（56%）であった。そのうち 24 名については「1～4 名」と回答。「11 名以上」という回答も 4 名いた。

一方、「いない」と回答した 28 名のうち、情報システム管理をどの部門が担当しているかという追加質問について、「総務部門」が最も多く 12 名、次いで「営業部門」4 名、「生産管理部門」3 名と続いた。

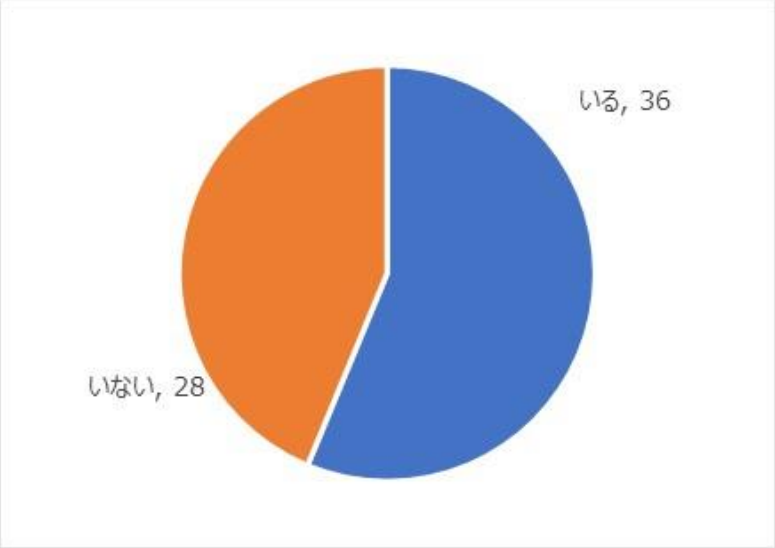


図 19 情報システム専任担当者有無

Q4：貴社のセキュリティ対策として不十分だと思う対策はどのようなことですか？
（ n=64 ）

回答のうち約 63%の回答者が「ガバナンス：ポリシー（基本方針）、スタンダード（対策基準）、プロシージャー（実施手順）の整備」と回答している。平時・有事のルール作りを含めたセキュリティマネジメントに関わる取組みが遅れている実態が明らかになった。

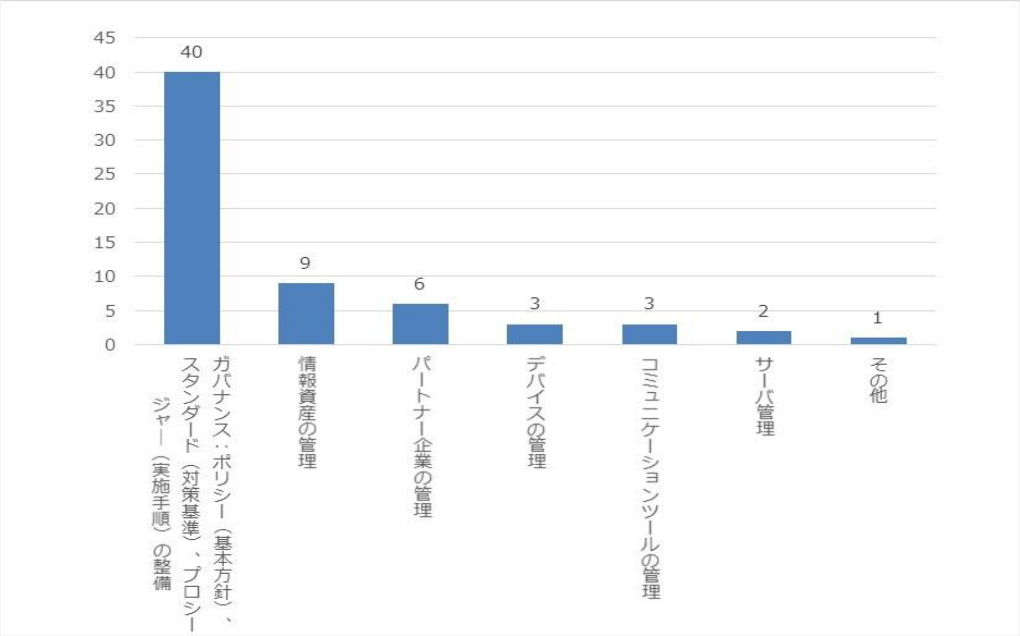


図 20 セキュリティ対策の課題について

Q5：貴社では情報セキュリティ対策にどの程度の外注費用をかけていますか？

（ n=63 ）

43 名（約 68%）の回答者が「年間 100 万円未満」と回答した。自動車産業といえどもセキュリティ対策資金に経費を捻出できない実態が明らかになる一方、100 万円以上 1,000 万円未満の外注コストをかけている回答も 20 名あった。

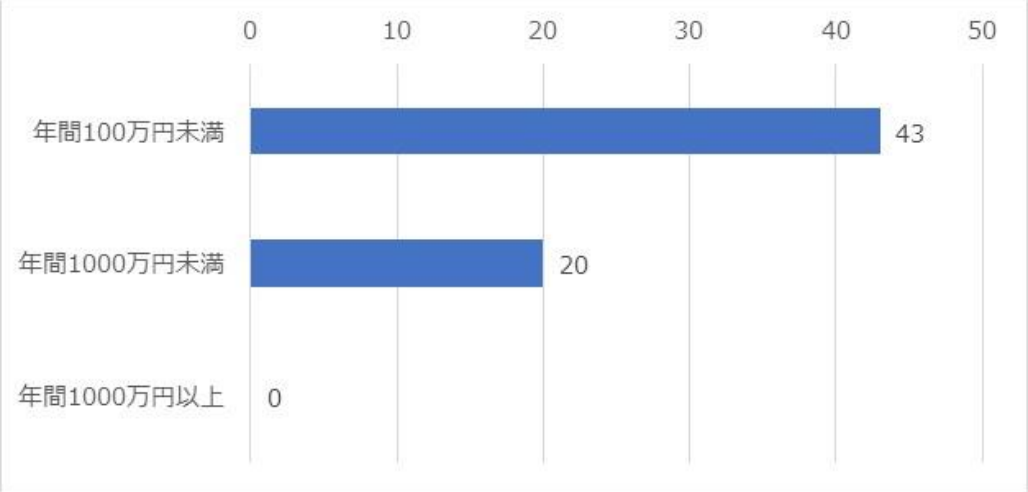


図 21　セキュリティ対策費用水準について

Q6：貴社のセキュリティ対策の状況について教えてください。 （ n=64 ）

セキュリティ対策に関する自己認識に関する質問について、30 名が「十分な対策がなされている」または「社内は十分な対策がなされている」と回答したのに対して、28 名は「不十分である」と回答するなど、回答が分かれる結果となった。実態はともかくとして、自己評価が高い回答割合が過半数を占めるという興味深いデータが取得できた。

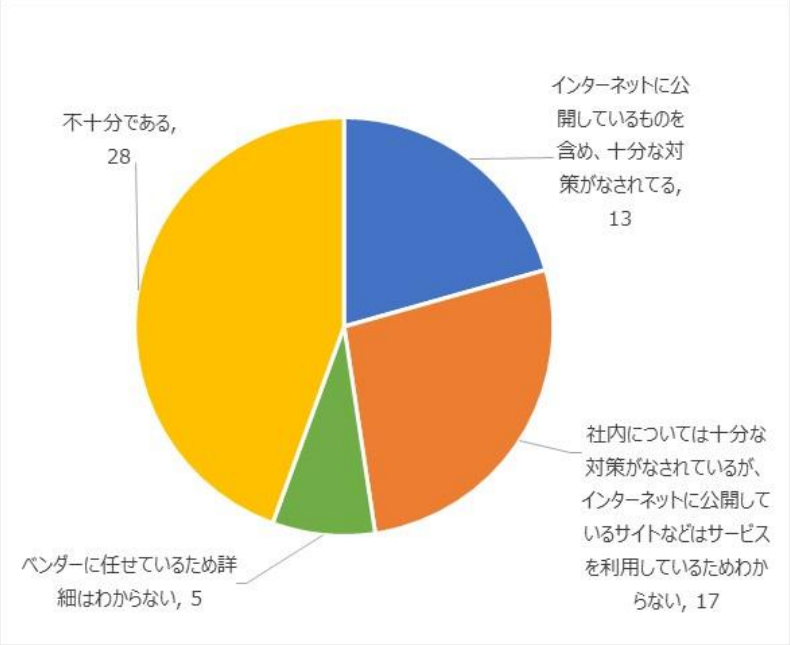


図 22　セキュリティ対策状況について

Q7：貴社で情報セキュリティ対策を進める上での課題を教えてください。（複数回答可）（ n=64 ）

多くの中小企業が、技術面、人材面で課題を抱えている結果が明らかになった。また、対策の進め方が分からないという専門性の欠如に関する課題に関する回答も目立った。

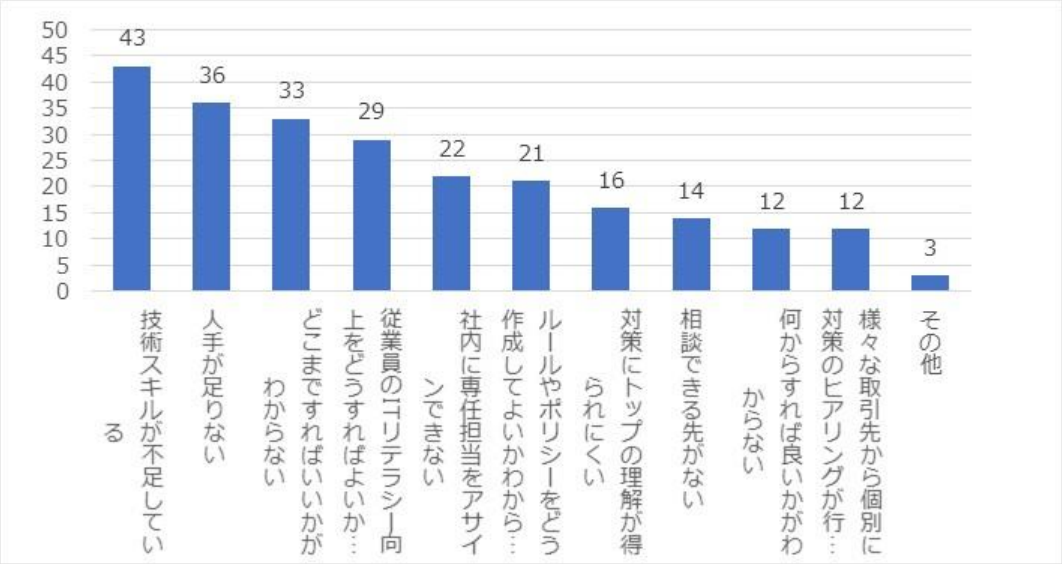


図 23　セキュリティ対策状況について

Q8：セキュリティ診断についてどのようにお考えですか？ （ n=63 ）

今後も診断を受けたくない企業と、何らかの診断を受けたいとする企業が二分する結果となった。

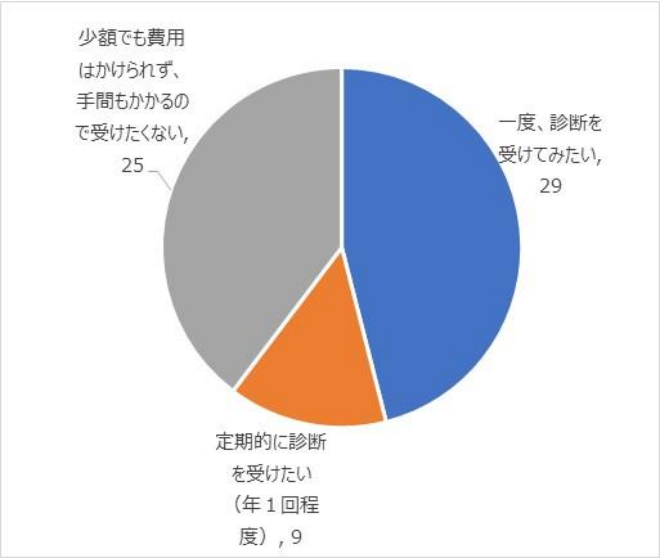


図 24　セキュリティ診断について

Q9：取引先からサイバーセキュリティ対策について何らかの要求はありますか？
（ n=63 ）

8 割以上の回答者が、OEM メーカーを含めた取引先企業から「具体的な要求がある」または「要求が始まりつつある」と回答しており、自動車産業特有の実態が明らかになった。

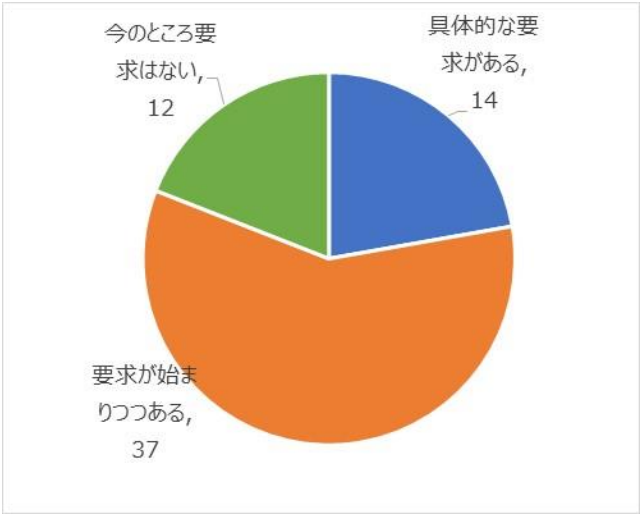


図 25　取引先からの要求事項の有無について

Q10：**テレワークの導入状況を教えてください。**　（ n=63 ）

テレワークについては、34 名（約 54%）が「導入していない」と回答している。この要因としては、「環境・インフラ、社内規定が未整備である」、「テレワークでできる業務がない」、「セキュリティが不安」が主な回答であった。

一方、部分的も含めて 29 名（約 46%）が「導入済み」と回答しているが、「営業・事務関連業務など実施可能な業務に制限して実施」という回答が大半であった。

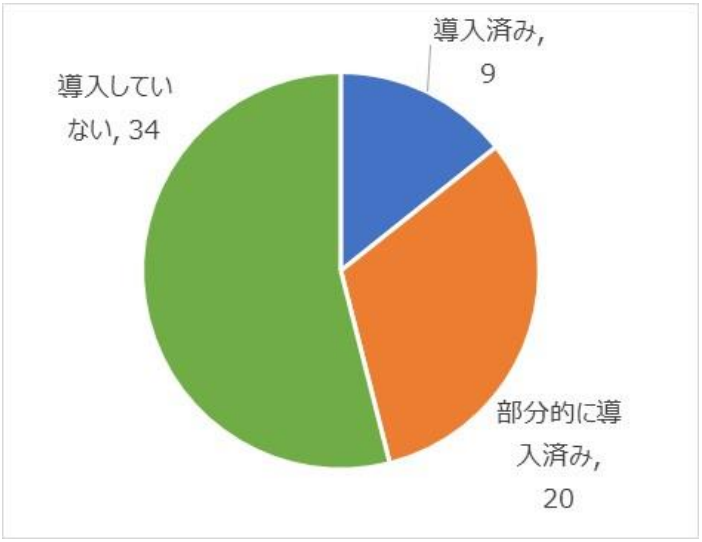


図 26　テレワーク導入状況について

Q11：**貴社は、過去サイバー攻撃の被害に遭ったことがありますか？（複数選択可）**
（ n=64 ）

約 60%の回答者が過去何らかのサイバー攻撃による被害に遭ったと回答している。「ウィルス感染」が最も多く、次いで「ランサムウェア」被害の実態も確認できた。「上記以外」として、「サーバーが踏み台」、「生産設備に付帯する PC のウィルス感染による操業の部分停止」という事象も確認できた。一方、25 名（約 40%）については「これまで被害はない」と回答した。被害について検知できていない可能性もある。

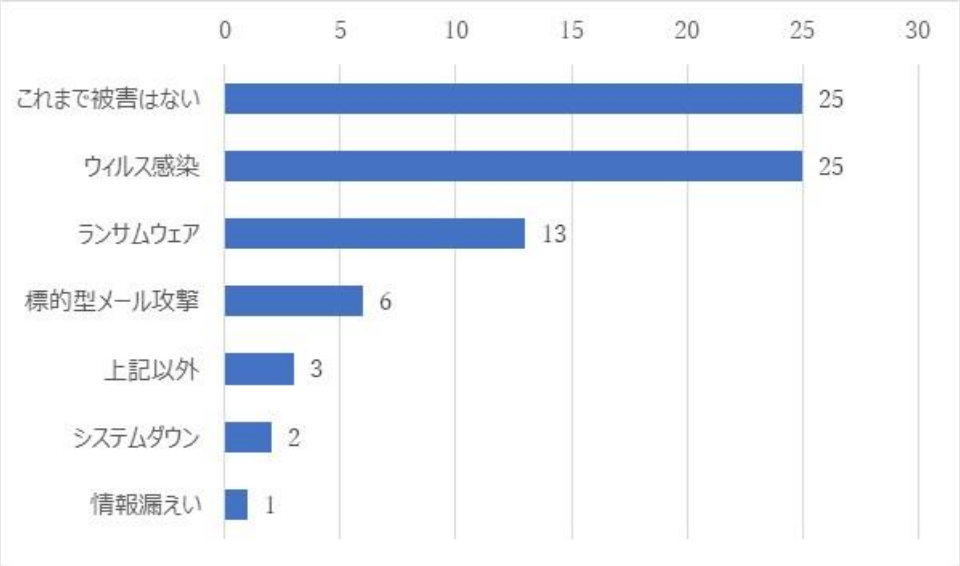


図 27　サイバー攻撃の被害有無について

Q12：今後どのようなサービスがあれば利用しますか？（複数選択可）　（ n=64 ）

「自社のセキュリティ対策状況を可視化できるサービス」が最も多く、次いで「困った時の相談サービス」となった。

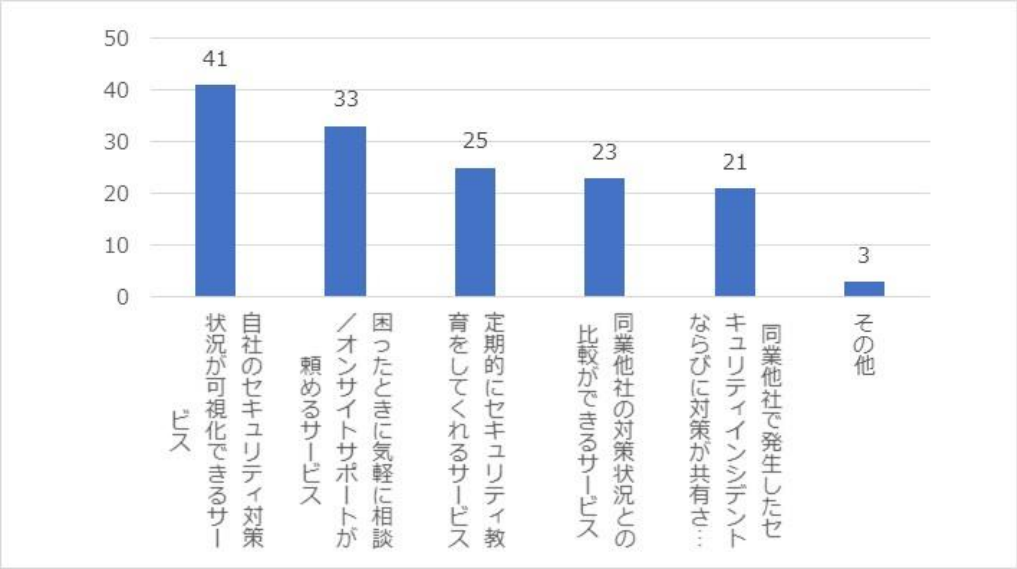


図 28　今後求めるサービス内容について

Q13：貴社がサイバー攻撃を受けた時に最も必要となるサポートを教えてください。（複数回答可）　（ n=64 ）

大半の企業が「原因調査・影響範囲把握」に関するサポートが必要と回答。次いで、「駆け付けによる初動対応」、「復旧にかかる費用の補償」と続く。

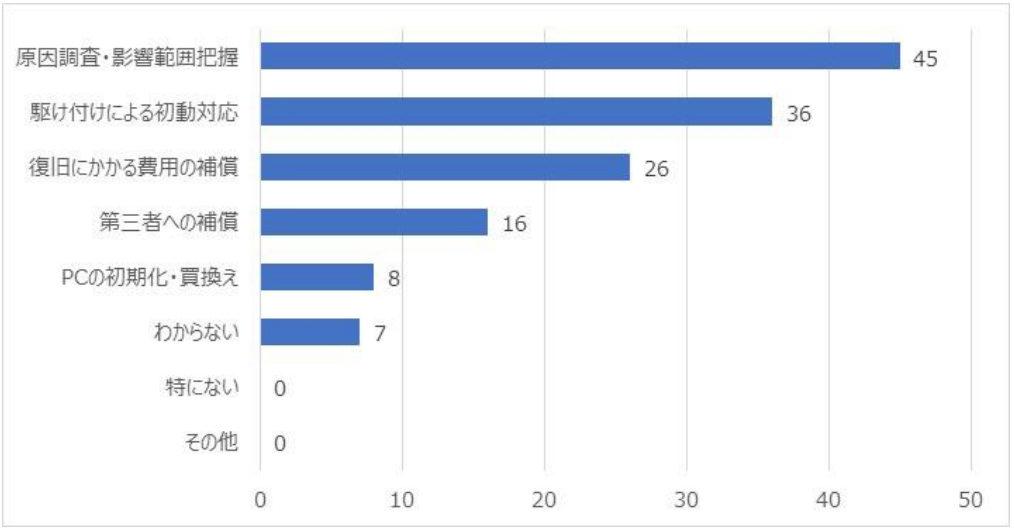


図 29　サイバー攻撃の際に必要な補償について

4.3 実証の実施結果

4.3.1 問診・診断

(1) 問診結果（実施企業数：30 社）

① アセスメント実施全般に関する実態

ア　アセスメント全体の回答にかかった時間

静岡エリアでのアセスメント項目（質問：約 50 問、実施状況を 3 段階のレベルで回答）については、約半数の企業が 1～2 時間以内での回答であり、比較的短時間での回答であった。一方で回答に半日以上、もしくは数日を要したケースもあった。

なお、時間がかかった要因としては、主に以下の 2 点であった。

・担当者自身にとって、アセスメント内容が難しかった。

・問診項目が、具体的に社内のどこに該当するかを把握することや、複数の社内担当者へ確認を行いながら回答を進める必要があった。

広島エリアでのアセスメント項目（質問：約 70 問、実施状況を 5 段階のレベルで回答）については、分量は多かったものの、後述の「表 3-6 各エリアにおけるアセスメント項目の特徴」でも述べるとおり、既に実施したことのあるアセスメント項目をベースにしたため、一部実証参加企業からは比較的スムーズに回答できたとの声が聞かれた。

イ　アセスメントの難易度

セルフチェックの段階で、実証参加企業の回答担当者より、概ね全ての質問に事前回答を得られた。難易度については「適切」との声があった一方で、質問の内容が難しい、専門用語が分からない場合がある等、回答に戸惑うこともあったとの意見も受けた。

ウ　セルフチェックとその後の回答支援に関する効果

セキュリティマネジメントに関するポイントを網羅的に確認することにより、実証参加企業におけるセキュリティ上の問題点を明確にするとともに、自社のセキュリティ面での改善に向けて、およそ何をすれば良いかを明確にすることができたとの声があった。

また、実証参加企業の担当者に回答をもらった後、本実証事業のアセスメントメンバーが Web 会議形式で個社別に約 3 時間の面談を行い、質問内容についての補足説明と回答内容のチェックを行った。その結果、担当者のセルフチェックだけでは不明な質問内容について、確認をしてもらうことができた。

なお、セルフチェックの内容をアセスメントメンバーが確認したところ、回答内容の認識相違により、面談後に評価レベルを変更するケースがあったため、評価結果の客観性を保つためには今回実施したような面談を行うことが望ましいことも明らかになった。

結果としてアセスメント項目の回答、およびその後の面談を通じて、実証参加企業の実態を把握するとともにセキュリティ担当者におけるセキュリティスキルの向上にも役立つことができた。

エ　アセスメントツールの使いやすさ

オンラインの Web 問診ツールについては、多くの企業が特に支障なくスムーズに進めることができた。ただし、質問内容や回答の記述量が多い場合には、表計算ソフト等を利用した回答のほうが 取組みやすいとの声が一部あった。

また、オンライン問診ツールに回答するための ID 発行等の手続きは、問診ツールから自動発信されるメールを利用したが、実証参加企業の受信メールフィルタリングシステムによりメールがブロックされ、オンライン問診の開始に手間取るケースがあった。加えて、Web ブラウザの種類、バージョンが問診ツールに対応していないため、同様に実証参加企業において問診ツールの回答に手間取るケースがあった。

② 実証参加企業の IT 担当者におけるセキュリティ意識に関する実態

問診については、静岡エリアおよび広島エリアで異なるアセスメント項目を用いている。各エリアでのアセスメント項目の内容は次のとおりである。

表 11 各エリアにおけるアセスメント項目の特徴

	静岡エリア	広島エリア
項目の内容	自動車産業向けに作成済のアセスメント項目をベースに実施した。	OEM メーカーのアセスメント項目に左記項目を追加して実施した。
評価方法	各項目について 1～3 までの 3 段階評価とした。	各項目について 1～5 までの 5 段階評価とした。
評価レベルの定義	1：未実施 2：実施中 3：実施済	1：未実施＆未検討 2：未実施だが検討中 3：実施に向けて着手した 4：一部実施中 5：全て実施

問診による集計結果は以下のとおりである。

ア　企業別の傾向（全項目平均）

① 全問診項目での現状レベルの平均は、静岡エリアで 1.85（3 点満点）、広島エリアで 3.35（5 点満点）となる。総じてセキュリティ対策に取り組み始めているが、完全に実施できておらず、対策の内容によっては未着手な点がある（対策の抜け漏れ）状態である。

② 全問診項目の現状レベルが「一部実施」のレベル（静岡エリア：レベル 2 以上、広島エリア：レベル 4 以上）に達している企業の割合は少数に過ぎず（静岡レベルで 18%、広島エリアで 25%）、中小企業全体でのセキュリティ対策水準の底上げが必要である。

③ 対策の取組みが遅れている企業（平均レベルが、静岡エリアで 1.5 以下（実施中までは至っていないが、着手中として判断できる値）が 4 社、広島エリアで 3.0 以下が 2 社）も一定数が含まれており、こうした企業に対して短期間で一定レベルに引き上げるための施策が必要である。

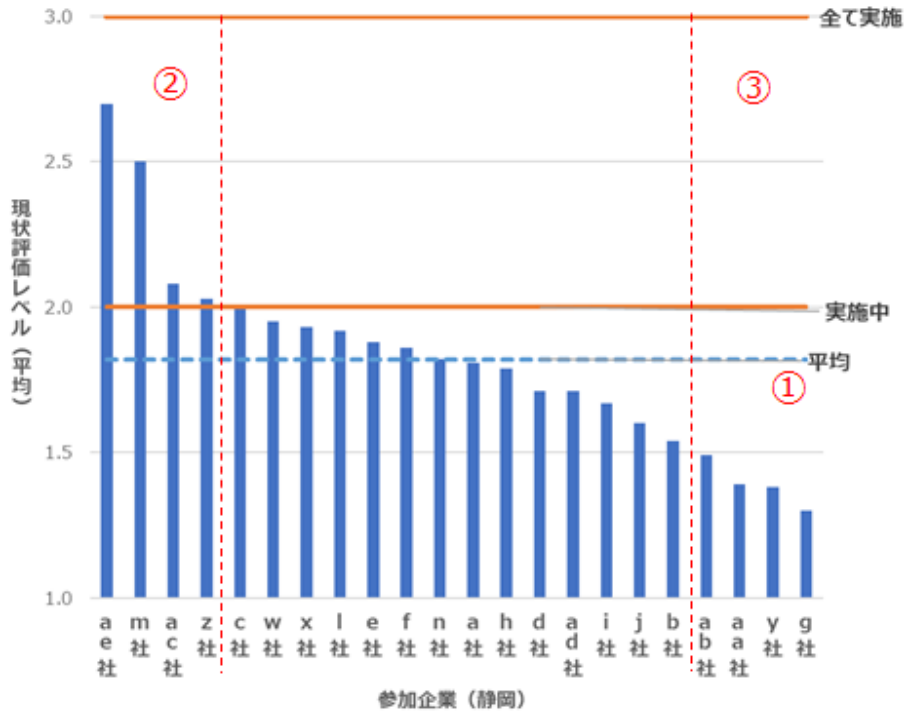


図 30 静岡エリアにおける企業別の現状レベル（全項目平均）

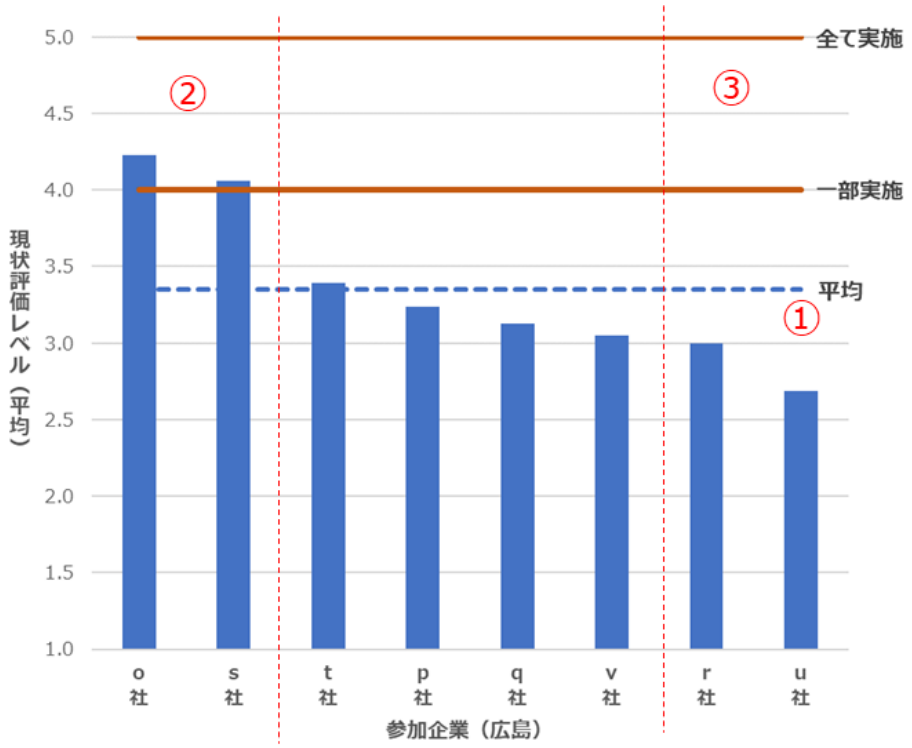


図 31 広島エリアにおける企業別の現状レベル（全項目平均）

イ　カテゴリ別の傾向

静岡エリアにおいて評価レベルの平均が 2（実施中）以上に達しているのは、「デバイス管理」、「社内ネットワーク」、「外部との通信ルールとファイアウォール」の 3 カテゴリである。一方、広島エリアにおいて評価レベルの平均が 4（一部実施中）以上に達しているのは、「ポリシーと組織」、「オフィスツール」の 2 カテゴリである。

また、両エリアにおいてセキュリティ・マネジメントに関するカテゴリについては、技術対策に関するカテゴリと比較して全体的に評価レベルが低い傾向が見られる。

なお、両エリア・カテゴリで確認すると以下のカテゴリで評価レベルが低い傾向が見受けられる。

【静岡エリア・広島エリア共通】
- ①「セキュリティ水準の維持・改善プロセスの構築」
- ②「セキュリティインシデント発生時の対応」
- ③「取引先のセキュリティ状況の把握/指導」
- ④「サーバーの管理」

【静岡エリアのみ】
- ⑤「個人認証の実装」
- ⑥「オフィスツール」

【広島エリアのみ】
- ⑦「工場領域の情報セキュリティ」
- ⑧「工場内の PC/PLC のセキュリティ対策」

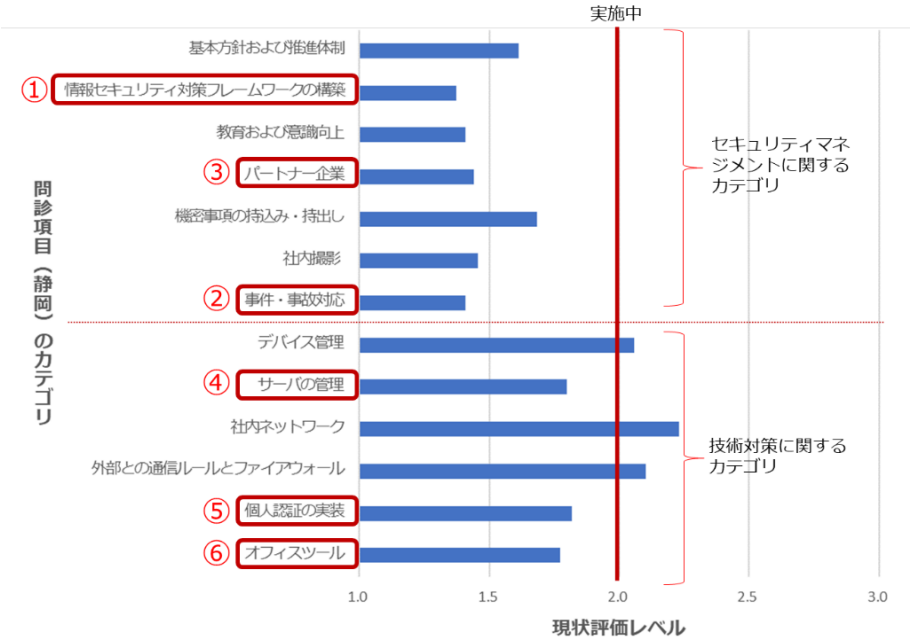


図 32 静岡エリアにおけるカテゴリ別の現状レベル（全項目平均）

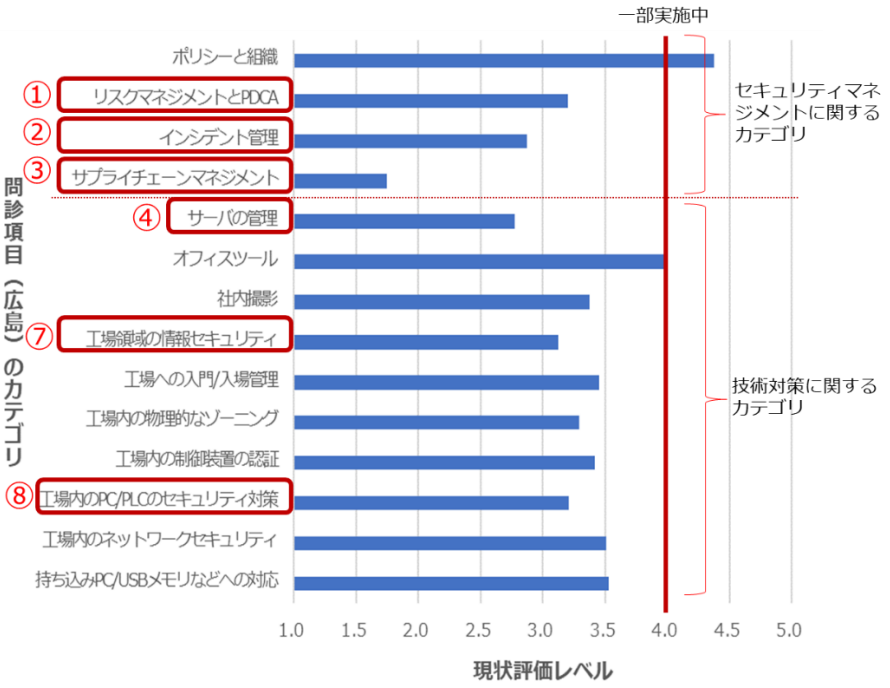


図 33 広島エリアにおけるカテゴリ別の現状レベル（全項目平均）

ウ　項目別の傾向

前項に記載した評価レベル平均が低い①～⑧カテゴリにおいて、特徴のある診断項目の回答数分布を記す。

① セキュリティ水準の維持・改善プロセスの構築（両エリア）

※各エリア、以下のカテゴリが該当

静岡エリア：「情報セキュリティ対策フレームワークの構築」

広島エリア：「リスクマネジメントと PDCA」

・守るべき重要な情報資産を定義し、セキュリティチェックや内部監査を実施する等、セキュリティ水準を維持するための個々の施策は一定程度進んでいるが、継続的な改善を進めるところまで取組みが進んでいない。

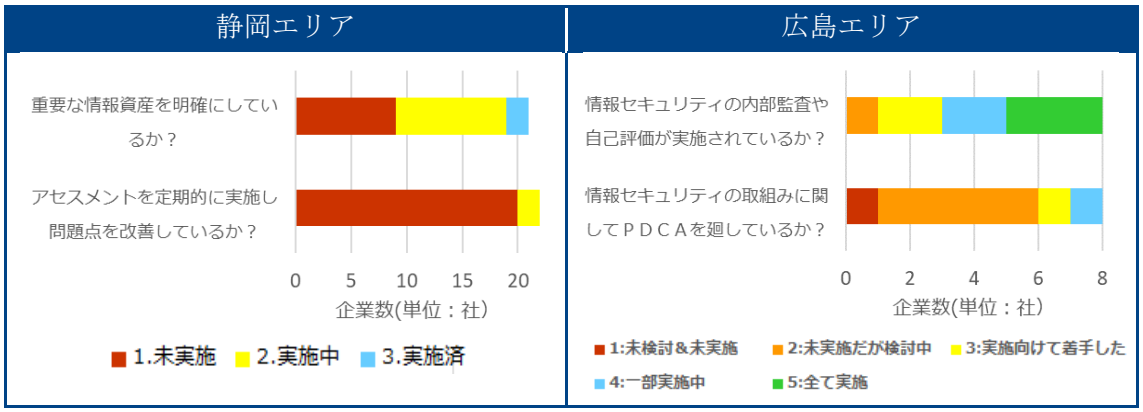


図 34「セキュリティ水準の維持・改善プロセスの構築」の項目別回答数分布

② セキュリティインシデント発生時の対応（両エリア）

※各エリア、以下のカテゴリが該当

静岡エリア：「事件・事故対応」

広島エリア：「インシデント管理」

・セキュリティインシデント発生時に IT 担当に連絡する等、最初の連絡先は決まっている企業が多いが、それ以降の組織的な対応方法が決まっていない企業が多い。

・セキュリティインシデント発生時に、サプライチェーン全体のリスクを軽減させるための体制・プロセスが十分に整備されていない。

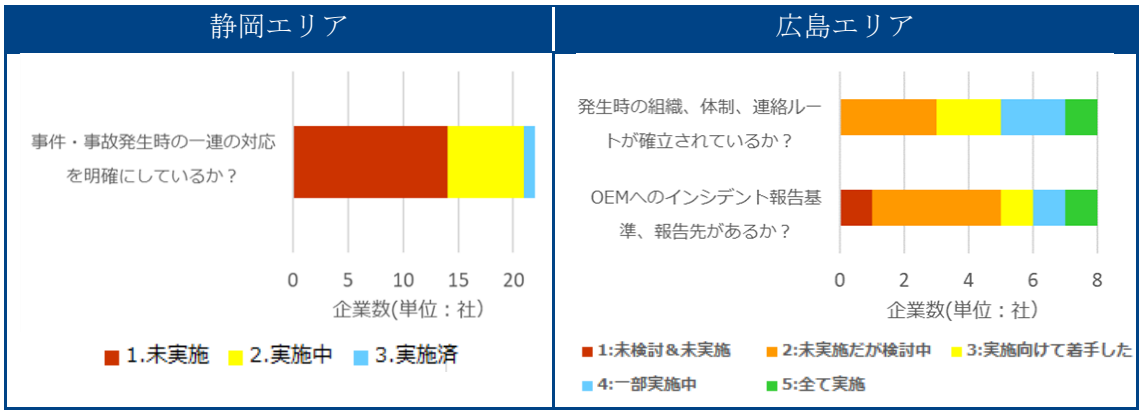


図 35「セキュリティインシデント発生時の対応」の項目別回答数分布

③ 取引先のセキュリティ状況の把握/指導（両エリア）

※各エリア、以下のカテゴリが該当

静岡エリア：「パートナー企業」

広島エリア：「サプライチェーンマネジメント」

・取引先のセキュリティ状況の把握や指導といった自社製品のサプライチェーンセキュリティの取組みはほとんど行われていない。現時点では自社のセキュリティ対策の整備に手一杯で、取引先のセキュリティ対応まで手が回っていない状況である。

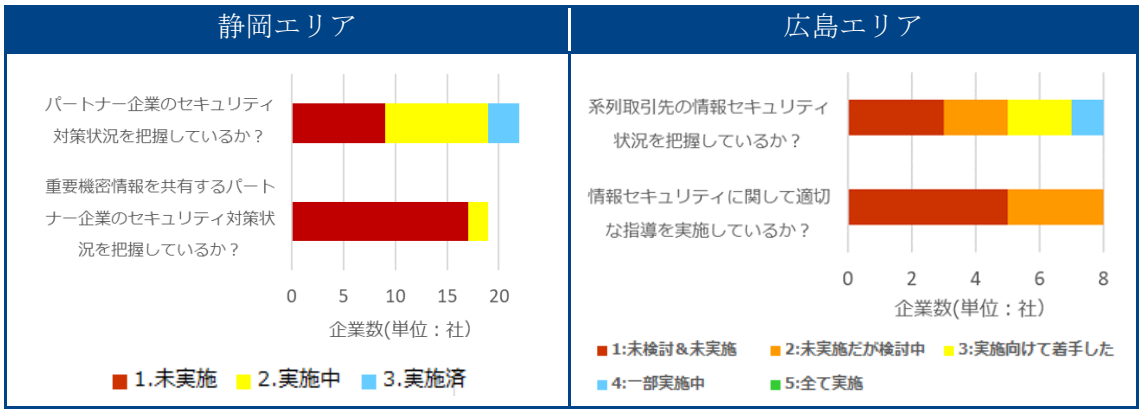


図 36「取引先のセキュリティ状況の把握/指導」の項目別回答数分布

④ サーバーの管理（両エリア）

・セキュリティパッチ適用については、社内基準をもとに実施している場合もあるが、取組みが遅れている企業や、パッチ適用時の動作保証ができない等の理由で適用していない場合がある。

・ファイルサーバー等の社内システムはクラウドではなく、オンプレで保有しているケースが多いが、ファイルサーバー等でクラウドサービスを利用した場合のセキュリティ対策（要件や利用ルール）が決まっていない企業が多い。

・ホームページの安全点検等、公開サーバーに関するセキュリティチェックが不十分。

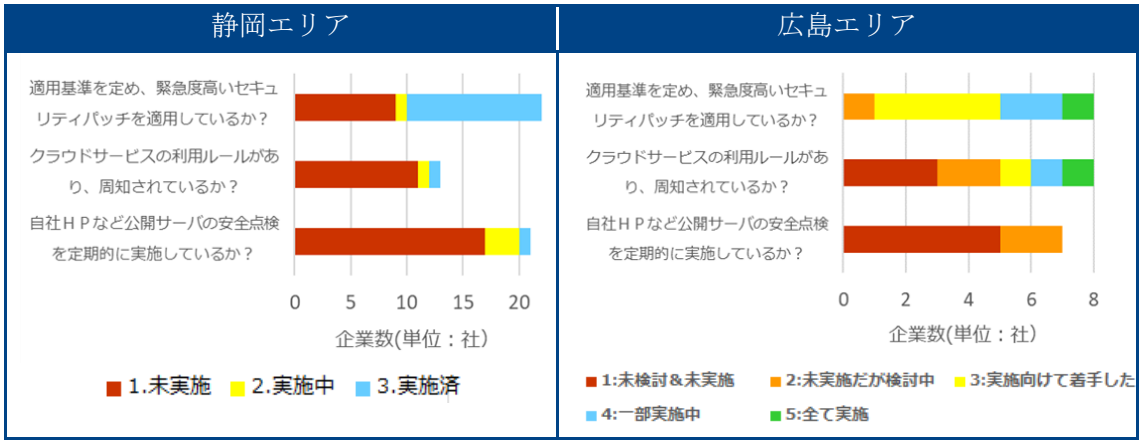


図 37「サーバーの管理」の項目別回答数分布

⑤ 個人認証の実装（静岡エリアのみ）

・ユーザーID に関する何らかの管理作業は行っているものの、「登録→アクセス権変更→削除」の一連の手続きや「定期的なアカウントの棚卸し」といった作業が整備（ルール化）されている企業はない。

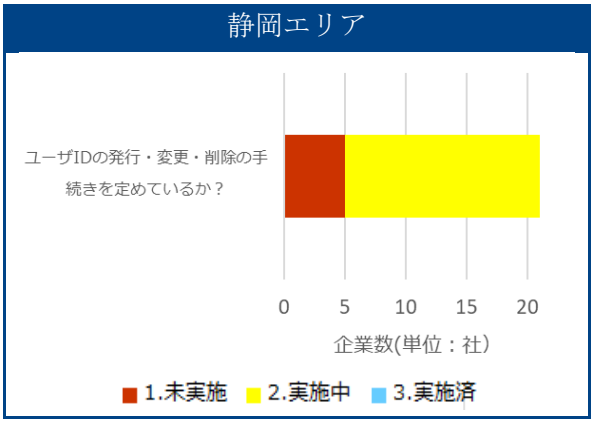


図 38「個人認証の実装」の項目別回答数分布

⑥ オフィスツール（静岡エリアのみ）

・メールによるウイルス感染対策は実施されているが、その他の対策については、未実施もしくは実施中の段階にある実証参加企業が多い。標的型攻撃やビジネスメール詐欺等、メールを通じた高度な攻撃への対応のためには、メールゲートウェイ等の導入によりメールを通じた侵入対策を検討する必要がある。

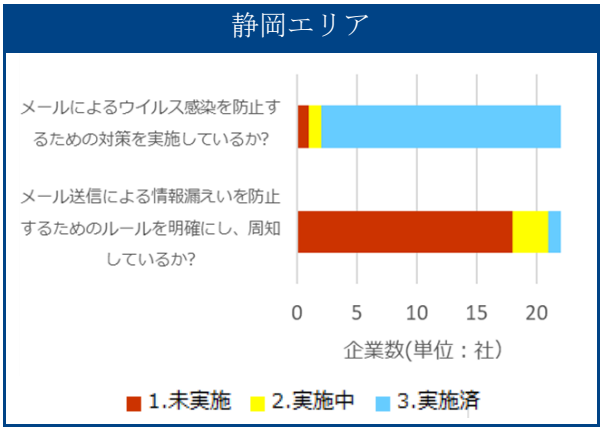


図 39「オフィスツール」の項目別回答数分布

⑦ 工場領域の情報セキュリティ（広島エリアのみ）

・機密事項の多い工場領域の情報資産について、何らかの形式で重要度の定義を行っている企業が多い。

・しかしながら、情報資産の管轄を製造部門が行っている、取扱製品が多く管理が難しい等の工場特有の理由により、台帳の整備等、十分な情報資産管理が行われていない。

・情報資産の定義は、リスク分析等の客観的なものではなく、サプライチェーンの要件としてセキュリティ対策が充足されていないおそれがある。

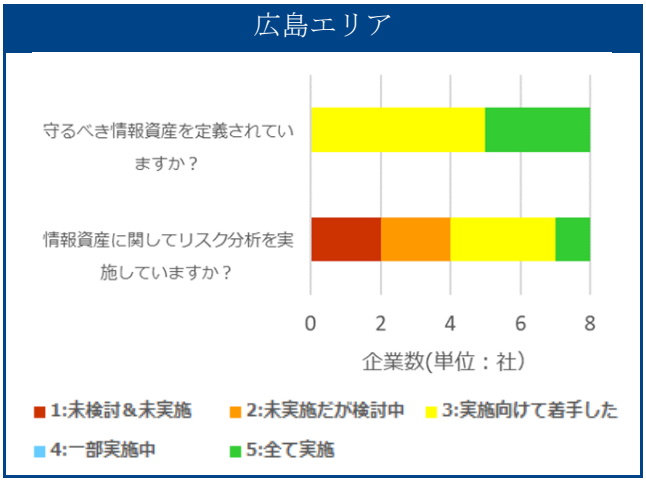


図 40「工場領域の情報セキュリティ」の項目別回答数分布

⑧ 工場内の PC/PLC のセキュリティ対策（広島エリアのみ）

・設備制御用の PC/PLC について、Windows 等のセキュリティ対策が適用可能なものについては、ウイルス対策ソフトウェアやセキュリティパッチを適用している企業もある。

・ただし、パッチ適用時に設備が動作しなくなる等の懸念や、ネットワークに接続していない等の理由で、ウイルス対策ソフトやセキュリティパッチ適用ができていない企業も多い。制御用 PC や PLC は古い OS を利用しているケースもあり、セキュリティ上のリスクが残る。

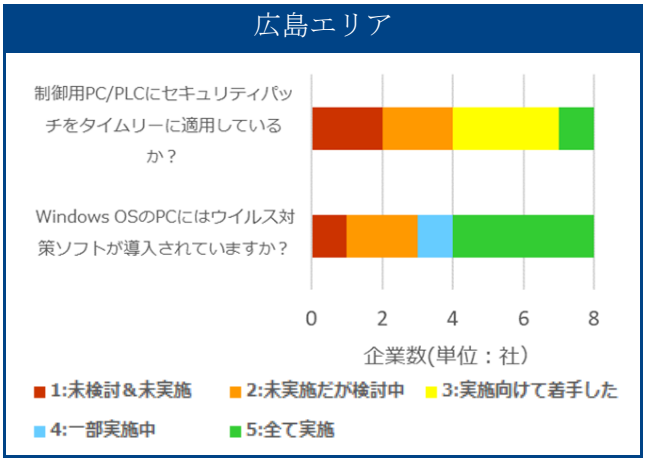


図 41「工場内の PC/PLC のセキュリティ対策」の項目別回答数分布

＜補足＞

その他、注意すべき項目として、以下があげられる。（両エリア）

※各エリア、以下のカテゴリの一部項目が該当

静岡エリア：「社内ネットワーク」

広島エリア：「工場内のネットワークセキュリティ」

・外部との通信を制御するためのファイアウォールの設置等、基本的なネットワークセキュリティについては既に対策済の企業は多かったが、IDS/IPS のように不正通信を監視、遮断するシステムの導入については十分に進んでいるとはいえない。特に制御用 PC/PLC や生産管理システム等、セキュリティ対策が十分ではない端末が接続する FA ネットワークについては、異常通信の監視システムがまだ導入されていない企業が多い。

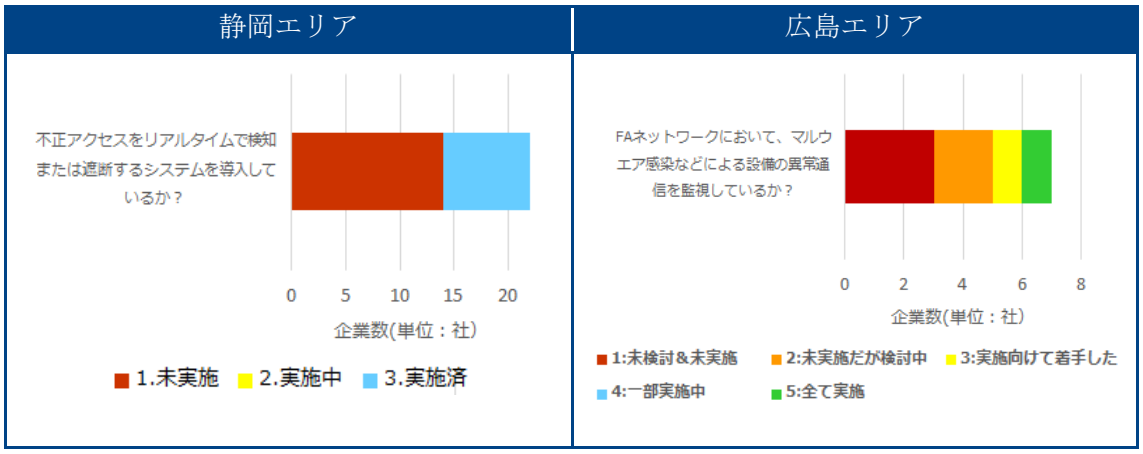


図 42「ネットワーク監視」の項目別回答数分布

(2) 外部診断結果（実施企業数：30 社、32 サイト/ライセンス）

実施内容で記載した確認／検証ポイントに関して実態を把握したものである。
結果は以下のとおり。

① 自動車産業サプライチェーンと製造業全体のセキュリティ管理レベルの比較

実証参加企業全体のセキュリティ管理レベルの平均は、製造業の平均と比べ比較的高い水準にあり、主要な検証カテゴリの全てにおいて実証参加企業の平均スコアが製造業の平均より高い水準にあることが確認された。

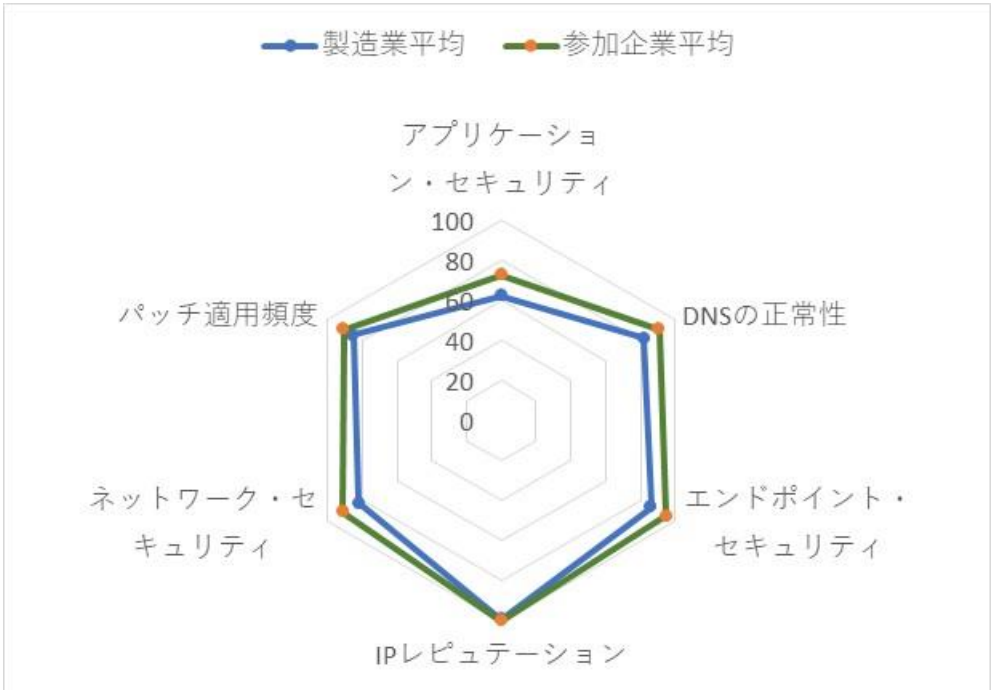


図 43 実証参加企業および製造業のセキュリティ管理レベル比較

② 自動車産業サプライチェーンのリスク傾向

実証参加企業のインターネットに公開しているサイトのセキュリティ管理レベルについて、SecurityScorecard のトータルランク分布で安全性が懸念される C ランク以下の企業が確認された。

具体的には、実証参加企業の多くは安全性の高い A ランク（44%）および B ランク（44%）であったが、インシデント発生リスクが高くなる C ランク以下の企業が 12%（4 社）存在した。

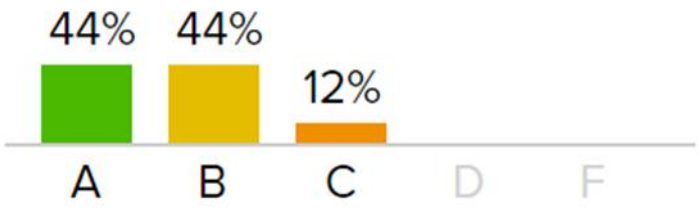


図 44 自動車産業サプライチェーンのリスク傾向

実証参加企業のセキュリティ管理レベルを分類ごとに掘り下げると、どの企業も総じて Web サーバーのセキュリティ実装を検査する「アプリケーション・セキュリティ」が低い傾向にあり、75%以上の企業が C ランク以下のスコア（うち F ランク 8 社）であった。また、サーバーの脆弱性パッチ適用状況を評価する「パッチ適用頻度」で 3 社、企業ネットワーク内で使用されている OS やブラウザのバージョンを評価する「エンドポイント・セキュリティ」で 1 社が、最もセキュリティ管理レベルの低い F ランクの指摘があった。

参加企業	a社	b社	c社	d社	e社	f社	g社	h社	i社	j社	k社	l社	m社	o社	p社	q社
トータルランク	A	C	A	B	B	B	B	C	B	B	B	B	A	B	B	A
セキュリティスコア	95	75	93	85	82	87	84	74	89	89	82	89	96	89	89	92
アプリケーション・セキュリティ	B	F	A	D	F	D	F	F	D	D	B	D	B	C	C	A
キュービット・スコア	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
DNSの正常性	A	A	A	A	A	A	A	A	A	A	B	A	A	A	A	A
エンドポイント・セキュリティ	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
ハッカーチャッター	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
IPレピュテーション	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
ネットワーク・セキュリティ	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
漏洩された情報	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
パッチ適用頻度	A	A	A	B	A	A	A	A	A	A	F	B	A	F	A	A
ソーシャル・エンジニアリング	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A

参加企業	r社	s社	t社	u社	u社	u社	v社	w社	x社	y社	z社	aa社	ab社	ac社	ad社	ae社
トータルランク	A	B	A	A	B	B	C	A	A	B	A	A	A	B	C	B
セキュリティスコア	94	80	91	97	88	89	70	91	94	85	92	93	92	89	72	86
アプリケーション・セキュリティ	B	F	A	A	D	A	B	C	C	F	C	C	C	C	F	F
キュービット・スコア	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
DNSの正常性	A	B	A	A	A	A	A	A	A	A	A	A	A	A	A	A
エンドポイント・セキュリティ	A	B	A	A	A	B	F	A	A	A	A	A	A	A	A	A
ハッカーチャッター	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
IPレピュテーション	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
ネットワーク・セキュリティ	A	A	A	A	A	A	C	A	A	A	A	A	A	A	A	A
漏洩された情報	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
パッチ適用頻度	A	A	C	A	A	C	A	A	A	A	A	A	A	A	F	A
ソーシャル・エンジニアリング	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A

図 45 実証参加企業インターネットサーバーのリスク評価

③ インターネット上で悪用される可能性の高いアプリケーションポート（データベース、Windows ファイル共有、リモートデスクトップ）の利用状況

アクセス可能な状態になっていると悪用される可能性が高いアプリケーションポートの確認を実施したところ、実証参加企業内の 3 社で不特定多数の接続元から接続可能な状態にあることが確認された。

3 社で接続可能な状態が確認されたのはデータベース系サービスで、デフォルトポートがそのまま利用され、インターネット上からアクセス可能な状態となっていた。

④ シャドーIT の可能性がある SSL 証明書期限切れサーバーのチェック

SSL 証明書の期限切れサーバーの確認を実施し、実証参加企業内の 1 社で SSL 証明書の期限切れが確認された。当該サーバーの SSL 証明書期限は約 1 年前で切れていた。

このように管理対象から外れ、適切なセキュリティ運用（廃止忘れやパッチ適用漏れ等）が実施されていない可能性のあるサーバーが脆弱なシャドーIT として残存することで、企業のセキュリティリスク高める可能性がある。

⑤ マルウェアの影響と見られる通信状況のチェック

SecurityScorecard 社のマルウェア通信検出システムによるマルウェア通信の有無を確認したが、実証参加企業のドメイン名に紐付いた IP アドレスからマルウェア通信の可能性があるトラフィックは確認されず、診断時点でウイルス感染によるマルウェア通信は見られなかった。

(3) 内部診断結果（実施企業数：31 社）

内部診断では、診断対象の端末数に対して、CVSS スコア 7.0 以上の脆弱性を保有する端末がどの程度の割合で存在するか、サポート切れ OS を利用している端末がどの程度存在するか、についての傾向を調査したものである。

なお、本実証事業では、特定のネットワークセグメントの診断を実施しており、本結果が企業全体の状況を示しているわけではない。

結果は以下のとおりである。

① 診断端末全体数に占める CVSS スコア 7.0 以上の脆弱性を保有している端末の割合

・診断端末 50 台以上については、端末数に関わらず、全社が脆弱性のある端末を保有していた。なお、傾向としては、保有率が 1 割以下で、ある程度の対応を実施できている企業と、4 割を超える企業に 2 極化している状況である。
・診断端末 50 台未満については、100%となっている企業が多数あり、これは端末台数が 10 台未満で発生している傾向がある。このことから全ての端末で同じ脆弱性を抱えている可能性があり、全体で脆弱性を保有していることが推測できる。

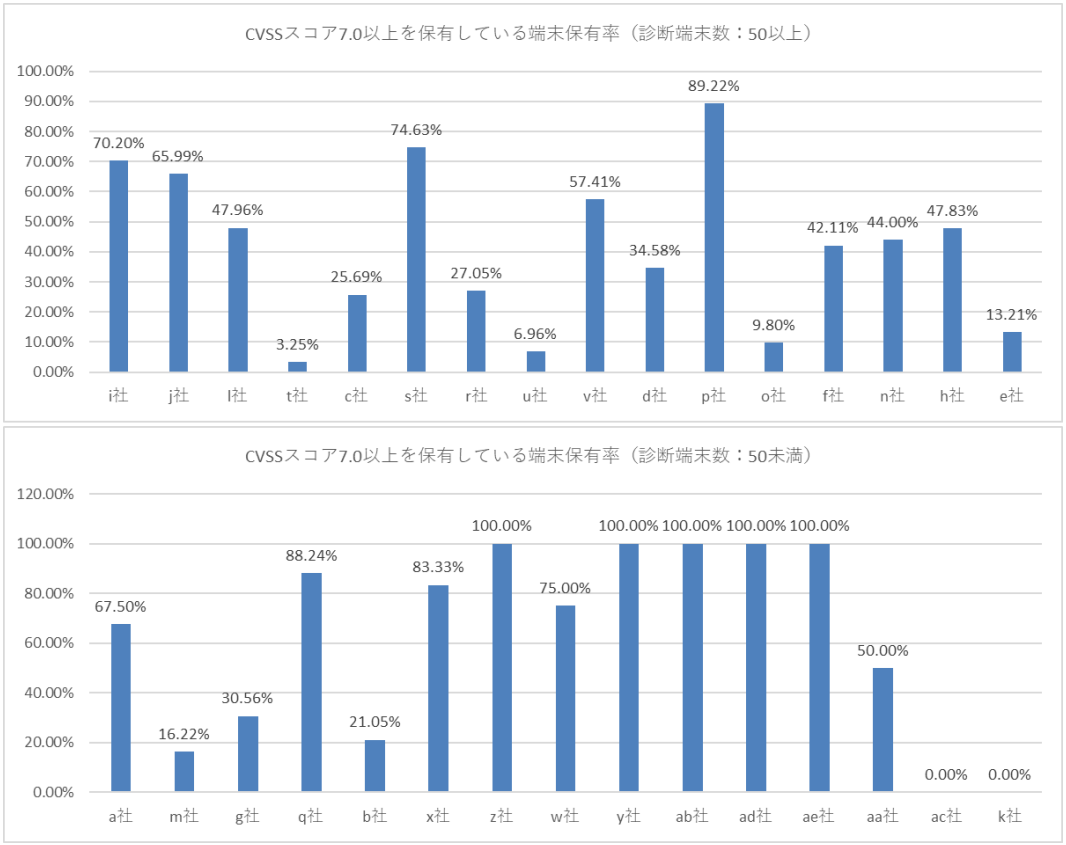


図 46 CVSS スコア 7.0 以上の端末保有率（端末数≧50 台、端末数＜50 台）

＜補足＞

・同じ脆弱性が複数の端末で検出されている場合があり、その脆弱性を解消することで、保有率の割合が低くなる可能性はある。

② 診断端末全体数に占めるサポート切れ OS の端末数およびその割合

・診断を実施した企業に対して、明確にサポート期限が切れている OS を利用している端末が存在した企業は全体の約半数の 15 社となっている。
・サポート切れ OS を利用している端末の数は、診断端末台数に比例はせず、各企業により特性（「できている企業」と「できていない企業」に二極化）が見受けられる傾向である。
・サポート切れ OS を利用している端末の数が少ない企業と多い企業の傾向として、少ない企業は 1 割以下、多い企業は 3 割～4 割となっている。
・端末台数が少ない企業ほどサポート切れ OS は少なくなっている傾向であった。

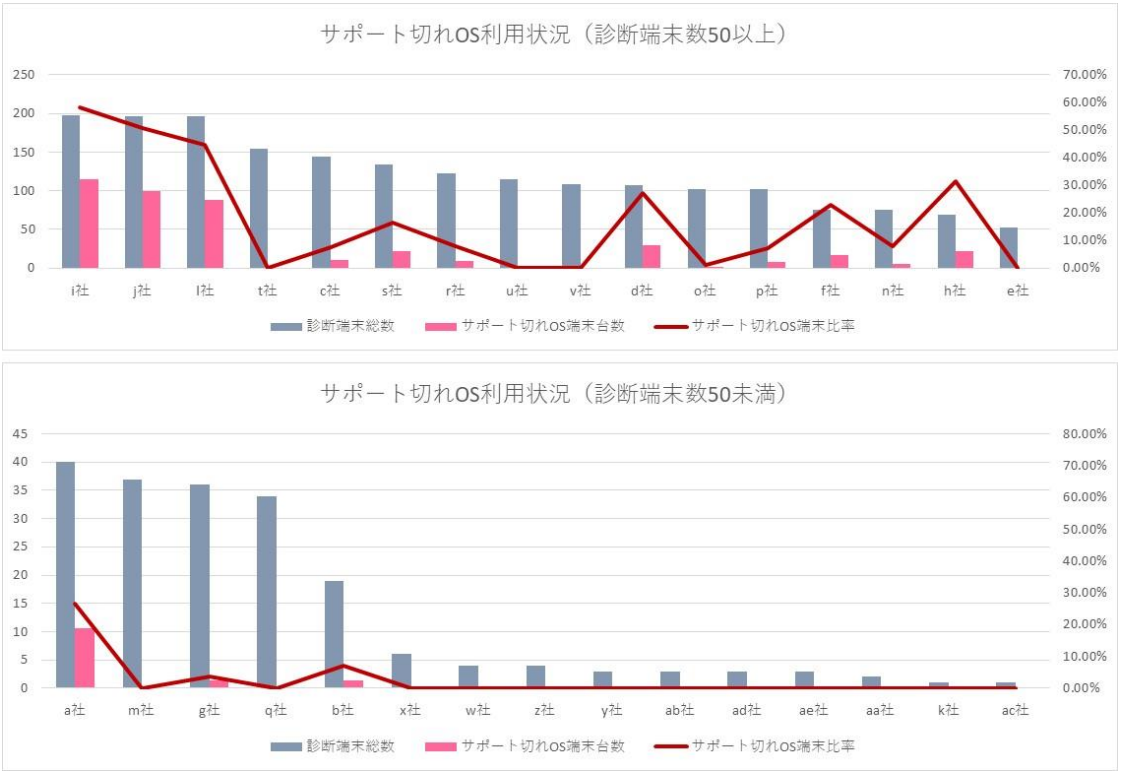


図 47 サポート切れ OS 利用状況（診断端末数≧50 台、診断端末数＜50 台）

(4) マルウェア対策診断結果（実施企業数：30 社）

マルウェア対策の診断では、診断対象者より得られた有効回答を企業ごとに集計した。なお集計に際しては、同一企業においても回答内容に差異が見られたが、企業ごとの合否判定は、不良回答を優先して判定に採用している。また、診断対象者による誤記や特定項目が空白の状態での回答等も見受けられたが、可能な限り診断結果に組み入れて集計を実施している。

結果は以下のとおりである。

① 企業ごとの合否結果

「メール添付ファイル」および「Web サイトからのファイルダウンロード」において、何れかの経路で疑似マルウェアまたは実行形式ファイルを実行できた企業を不合格と判定している。

結果として全体の「60%」の企業が不合格の判定となった。

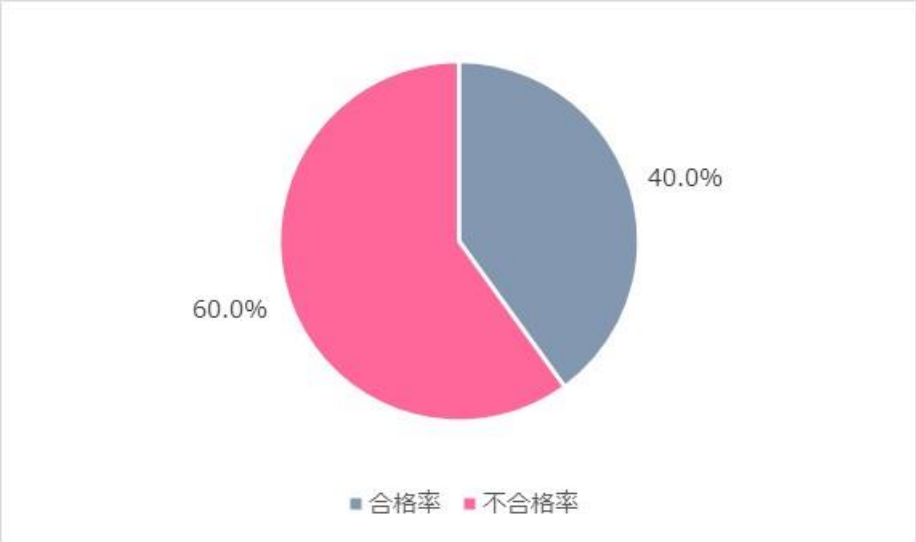


図 48 企業ごとの合否結果

② 疑似マルウェア添付（zip）

メール添付において疑似マルウェアを実行できた企業は全体の 3.3%であった。

図 49 疑似マルウェア添付（zip）

③ 実行形式ファイル（exe）

メール添付において実行形式ファイルを実行できた企業は全体の 26.7%であった。

図 50 実行形式ファイル（exe）

④ 疑似マルウェア（zip）DL

Web ダウンロードおいて疑似マルウェアを実行できた企業は全体の 3.3%であった。

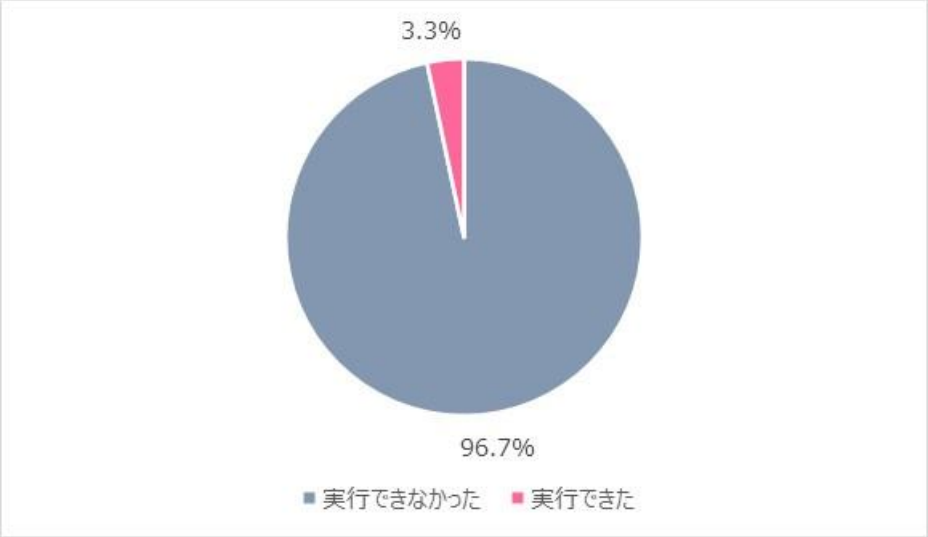


図 51 疑似マルウェア（zip）DL

⑤ 実行形式ファイル（exe）DL

Web ダウンロードおいて実行形式ファイルを実行できた企業は全体の 46.7%であった。

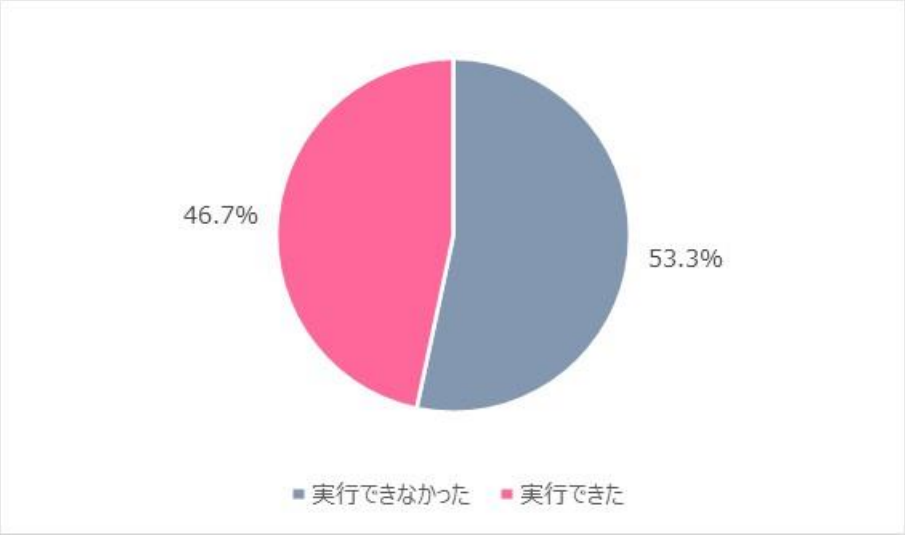


図 52 実行形式ファイル（exe）DL

4.3.2 監視・検知

(1) 不正通信監視結果（実施企業数：30 社）　※StellarCyber3 社、Cloudedge27 社

不正通信監視では、対象企業より得られたアラート情報等を集計した。
結果は以下のとおりである。

① 結果サマリ

表 12 サイバー攻撃に関するアラート種別と検知状況

アラート種別	件数	説明	検知状況とそこから読み取れるサイバー攻撃の動向
外部からの不正アクセス検知および防御（外→内）	―	外部からの不正アクセス通信を検知・遮断し、バッファーオーバーフローや SQL インジェクション等のソフトウェアやネットワークの脆弱性をついた攻撃を防御	本実証事業では各企業の拠点側に機器を設置しており、直接外部からの攻撃であるかの判別できないためカウント不可。
内部不正プログラム検知および防御（内⇔外）	0 件	ボットネットとの通信など、マルウェア感染等による内部から外部への不正通信や不正プログラムが含まれる通信を検知、感染を早期発見し防御	C&C コールバック等の検知はなく緊急性の高いインシデントは発生していない。
不正サイトへのアクセスブロック（内→外）	19,301,698 件	内部端末から、予め登録したセキュリティ上のリスクがある不正サイトへの接続をブロック（URL フィルタリング）	Web 広告、詐欺サイト、不正プログラムによる外部アクセス等を検知したが UTM にてブロックしておりインシデントには発展してない。なお、ブロックしたカテゴリは Web 広告が多く全体の 99.9%を占める。
マルウェアの検知および無害化	32 件	メール添付ファイルや Web からのダウンロードファイルに含まれるウイルス、ランサムウェア、ア	不正プログラム検知したが UTM にてブロックしておりインシデントには発展してない。

		ドウェア等の検知と無害化	
その他	3,587 件	マルウェアの混入が疑われる P2P アプリケーションの通信を検知・遮断し、不正通信やウイルス感染の発端となる通信をブロック	特定の P2P アプリケーションによる通信が多く検知されている。

② 不正プログラム、ランサムウェアの検知数

検知された不正プログラム等の数は合計 32 件であった。

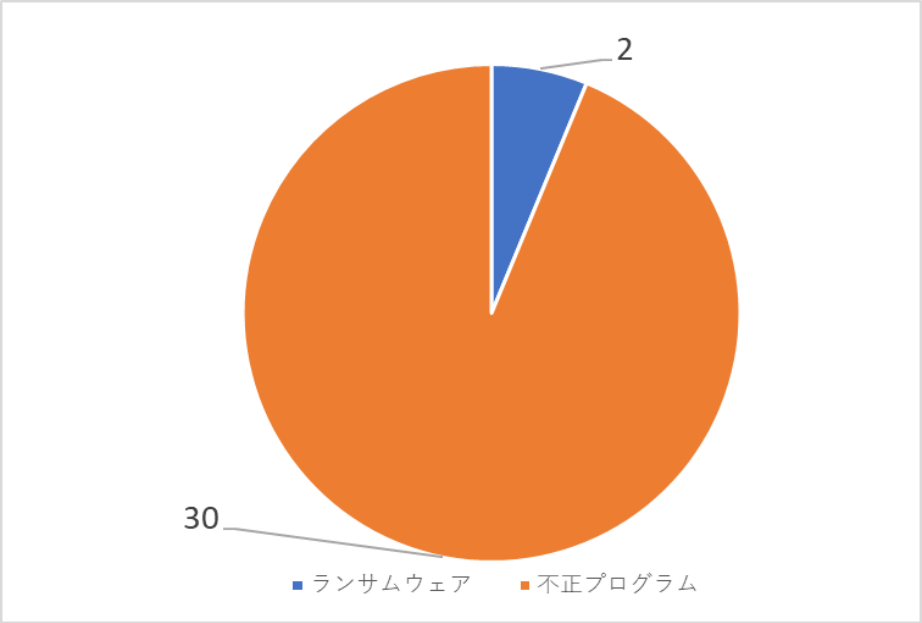


図 53 不正プログラム、ランサムウェアの検知

③ ブロックした URL カテゴリ

有害または業務に無関係の通信として、約 1900 万件のアクセスをブロックした。そのうちの 99%以上は Web 広告が占めている。そのため集計から除外し、Web 広告以外で、ブロックした URL カテゴリ比率を集計した。（n=1612）

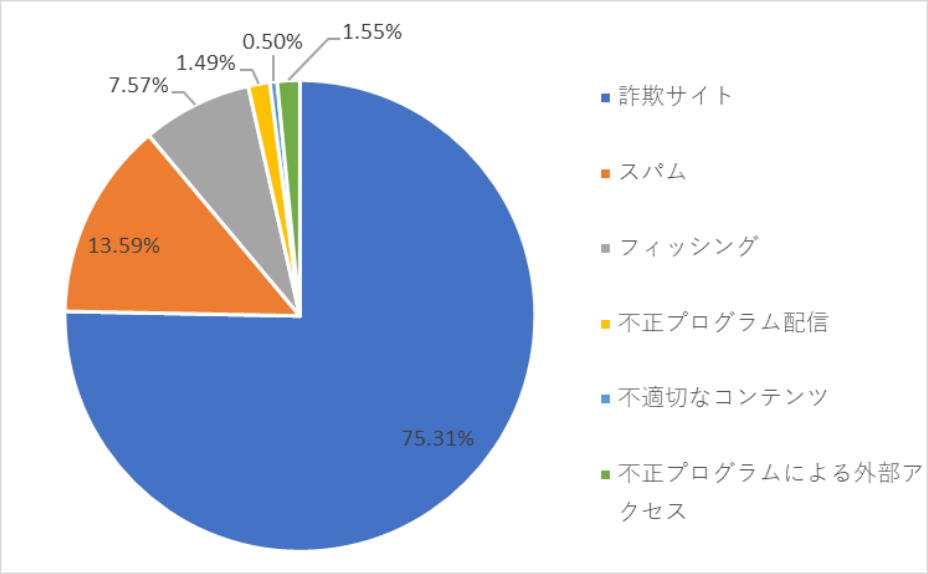


図 54 ブロックした URL カテゴリ比率

4.3.3 トラブル相談（一元窓口）

(1) 窓口受付の結果（～1 月 15 日（金））

トラブル相談（一元窓口）では、実証参加企業からの問合せについて、その対象と内容を分類して集計した。対応総件数は 75 件。1 件の問合せに複数の内容が含まれる場合は重複してカウントし集計している。

結果は以下のとおりである。

① 対象カテゴリ

実証期間中に問合せ等の対応が発生した対象は以下のとおり。診断に関する問合せが多くなっている。

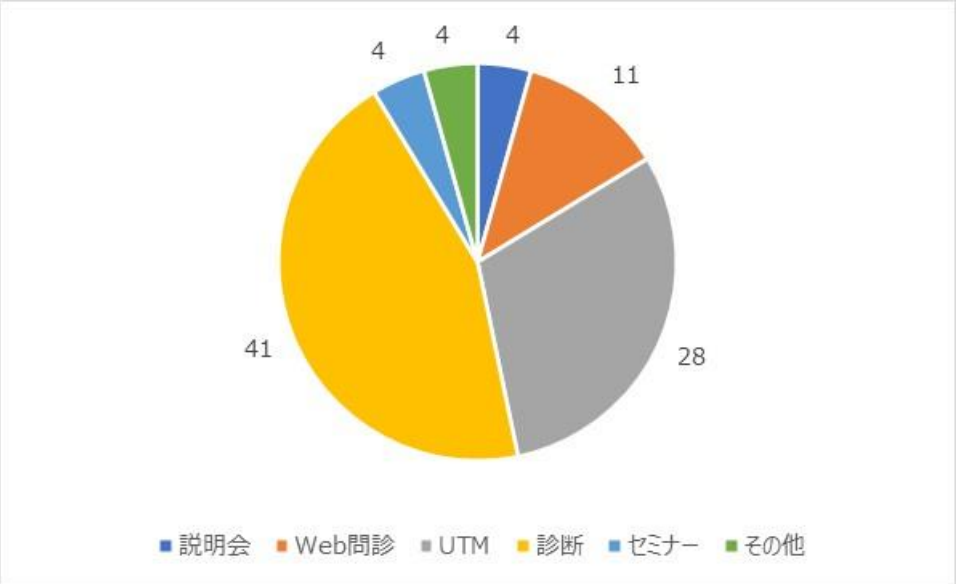


図 55 対象カテゴリ

② 内容分類

実証期間中に問合せ等の対応が発生した内容の分類は以下のとおり。申込書の書き方や実証に用いたツールのインストール方法などの手順に関する問合せが多くなっている。

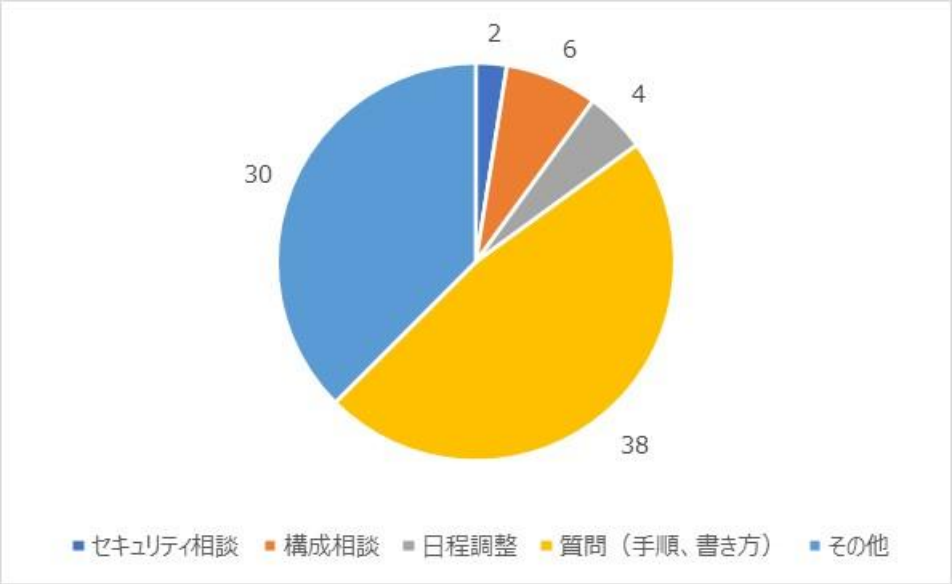


図 56 内容分類

4.3.4 インシデント対応

実証期間中のインシデント対応は 2 件だった。また、インシデントについては、内容や結果と考察を本節にて合わせて記載している。

(1) インシデント対応結果

表 13 インシデント対応一覧

対応 No	事象・被害（おそれ）	受診方法	対処結果
1	端末への不正侵入の可能性	申告	勘違い（被害なし）
2	C&C 通信の検知	検知	調査中（被害不明）

① インシデント対応 No.1

ア　インシデントの内容

・発生日時：2020/12/14　19 時頃
・事象および被害状況：2020/12/15　9:15　実証参加企業より下記申告メールを受信
【症状】2020/12/14　19 時頃ネットワーク接続状態で端末の操作を開始しようとしたところ
・デスクトップ上の「Outlook2019」アイコンが勝手に移動した。
・デスクトップ上のフォルダ（PDF ファイル格納）が消えた。
・デスクトップ上のフォルダが勝手に開いた。
【緊急対応】
・LAN ケーブルを抜いて、即時パソコンシャットダウン

イ　対処内容

・端末のウイルス対策ツールによるフルスキャン実施
・設置している UTM のログ調査
・関連事象の調査
・端末復旧方法の調査（当該パソコンが業務に必須であるため）

ウ　結果について

・被疑端末利用者の IT リテラシーが低いため勘違いがあったとの連絡あり対応完了。
（実証参加企業より、お助け隊に「インシデントの対応方法が正しいか確認の意味で相談した」と後日連絡を受領。）

② インシデント対応 No.2

ア　インシデントの内容

実証参加企業の UTM（パターン 2：StellarCyber による通信のトラフィック監視・IDS シグネチャ検知・振る舞い異常検知）の監視において C&C 通信と思われる不正アクセスを検知（2020 年 12 月 23 日（水）　10:34　アラート発生）

イ　対処内容

実証参加企業への指示および依頼事項
① SOC レポートの通知、該当端末のネットワークからの切り離しとウィルススキャンの実施をアドバイス
② 検知の通信は何れも内部のプロキシ通信と思われ、SOC 監視で得られている情報からは実際に通信している端末の特定はできなかった。そのため、不正アクセス検知の

情報以外にプロキシの通信をトラフィックログから調査して実証参加企業に報告し、実証参加企業側にて実際の通信を行っている端末の特定および端末の状況確認を依頼した。

③ プロキシ通信を行っている端末を特定し、その端末の確認、隔離、スキャン実施を指示したが、実証参加企業が実際に通信を行った端末調査に苦労している様子であったため、トラフィックログと該当検知を相関分析し、プロキシ通信のログを調査した内容を連絡した。

ウ　結果および対策実施状況について

実証参加企業には端末の特定および端末の状況確認を依頼したものの、下記理由により具体的な対処ができていない状況となった。

・今回の不正アクセス検知の対象ホストがプロキシであるため、~~お~~客先のネットワーク構成や端末情報についての内部調査把握が必要となる。
・分析すべきログの情報が限られているため、明らかにインシデントかどうかの判断に至っていない。
・疑わしい状況なので本来は調査（フォレンジック）をするのが望ましいが、実証参加企業において調査コストもかかるため詳細調査ができない状況で、被疑端末の限定および疑わしい通信の遮断には至っていない。

⑵ インシデント対応に関する問題点

実証参加企業への十分なサポートができなかった（限界があった）点として、以下の問題点があったと考える。

① アラートの信憑性

今回のアラートの信憑性を判断するためには取得するログが十分ではなかった。そのため、明らかに重大なインシデントであるとは明言できなかった。

② 実証参加企業への調査依頼の限界

ある程度の具体的な調査内容を依頼したが、実証参加企業の事情（調査コストがかかる）もあり、十分な回答を得られない状況となった。

③ 本実証事業の対応範囲

本実証事業として、駆け付けまでは想定していたものの、現地調査（フォレンジック）を実施するまでの対応は考えていなかった。コロナで現地対応はできなかったこともあり、ログ分析をできる限り実施し実証参加企業の支援に留めざるを得なかった。

(3) インシデント対応に関する考察

本実証事業で使用した UTM は下記の 2 パターンである。インシデント対応 No.2 はパターン 2 にて検知された。

・パターン 1：UTM（Cloudedge）　：
　不正通信の遮断タイプ
・パターン 2：StellarCyber　　：
　シグネチャのみならず、振る舞い検知による不正通信の検知通知タイプ

振る舞い検知ができるような UTM（サイバーキルチェーンを監視検知）を設置する場合は、不確かなアラートを闇雲に通知することは極力避けるためにも、対象企業の構成情報、通信状況（トラフィックログ）、Web アクセスログ、その他サーバーや端末のログを十分に取得・把握した上で設置する必要がある。アラートの正確性と合わせて、どのタイミングでアラートを通知するかについても難しいテーマである。情報収集段階で通知するのか、稼働確認段階で通知するのか等を予め定めておく必要がある。

また、アラートを通知した場合は、対象企業との連携を密にして、インシデントの詳細について、事象の把握、端末の特定、対処策の選定等を共有して対処していく必要がある。ただし、一般的に中小企業の場合は専門的な内容についての判断ができないので、専門家が主導的に通信断等の対処をすることが望ましいと考える。

UTM の導入においては、業務影響も考慮した上でパターン 1：UTM のように、不正通信と思われるものはできる限り遮断し、その後必要な通信をオープンにする方法が有効と思われる。標的型メール攻撃等の高度な攻撃への対応が必要な場合は、パターン 2 のようにプロキシや AD、通信パケット等のできるだけ多くのログを総合的に分析できるタイプの UTM を導入し、サイバーキルチェーンの状況を把握する必要がある。

今後は、中小企業が導入しやすい価格であることおよび構成情報等を調査する必要が無いことを前提に、AI やマシンラーニングを利用した SIEM エンジンによる自動化ツールにより、正確なアラート情報および遮断等の対処ができるサービスを開発し提供する必要がある。

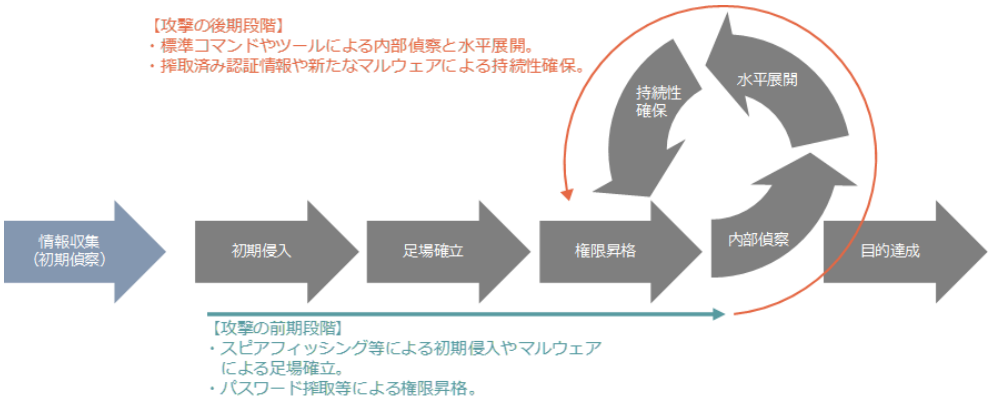


図 57 サイバーキルチェーン

4.4 成果報告会の開催

本実証事業に関する成果の報告および今後のビジネス拡大に向けたサービス周知を目的として、以下のとおり成果報告会を開催した。本成果報告会の開催にあたっては、今後のお助け隊ビジネスの展開対象となりうる自動車産業の中小企業サプライヤーにも幅広く参加募集を実施した。具体的な実施内容は以下のとおり。

4.4.1 開催日時・場所・実証参加企業

静岡エリアおよび広島エリアにおいて、それぞれ 1 回開催した。開催については、新型コロナウィルスの影響も勘案し、現地開催は断念し全てオンライン形式での開催となった。

表 14 静岡エリア　成果報告会

名称	「サイバーセキュリティお助け隊」成果報告会
開催日時	2021 年 1 月 14 日（木）13:00～14:50
形態	オンライン形式（Zoom 開催）
参加者数	66 名（54 社、うち実証参加企業 16 社）

表 15 広島エリア　成果報告会

名称	「サイバーセキュリティお助け隊」成果報告会
開催日時	2021 年 1 月 19 日（火）13:00～14:50
形態	オンライン形式（Zoom 開催）
参加者数	35 名（20 社、うち実証参加企業 8 社）

4.4.2 実施内容

成果報告会の実施内容は以下のとおり。静岡エリアおよび広島エリアについて全て同様の内容で実施した。

表 16 成果報告会の実施内容

第 1 部	はじめに
第 2 部	実証結果報告会　13:05-14:00 （1）成果報告 ・Web 問診（アセスメント）結果について ・メールおよびファイル DL 診断結果について ・外部診断結果について ・内部診断／端末診断結果について ・不正通信モニタリング結果について ・総評 （2）　今後に向けた取組みについて ・総評から見た今後必要なサービス検討について（案） （3）　実証終了後のお願い事項について
第 3 部	セキュリティセミナーの開催 【Session 1】14:00-14:30 題目：中小企業経営者が考えるべき with コロナ時代のサイバーセキュリティ「新常識」（株式会社 CISO） 【Session 1】14:30-14:45 題目：できるところからはじめよう！コストをかけず SECURITY ACTION！（IPA）
第 4 部	セキュリティ実態把握アンケート（実証終了時アンケート）の実施

4.4.3　セキュリティ実態把握アンケート結果

自動車産業に属する中小企業サプライヤーのセキュリティ実態把握を目的として、本実証参加企業のほか、静岡エリアおよび広島エリアのその他中小企業サプライヤーも対象としてアンケートを実施した。成果報告会へ参加しなかった実証参加企業からは、別途回答の取り付けを行った。集計結果は以下のとおり。（有効回答 n=69）

＜アンケート集計結果＞

Q1：今回の「サイバーセキュリティお助け隊事業」は御社にとって有益でしたか？
（実証参加企業のみ n=31）

全実証参加企業のうち、28 社（約 90%）が「はい」と回答した。「いいえ」と回答したのは 3 社のみであった。実証参加企業の主な声は以下のとおり。

＜有益であった＞

・問題点を具体的に指摘して頂けたことは今までにない評価がされて刺激になり有益だった。
・サイバーセキュリティの実態が把握でき、意識レベルがあがった。無料でこのようなことができたのは大変有益。
・弊社のセキュリティの状態を把握することができた。
・経営側の認識が高まった。
・攻撃型メール訓練等具体的な活動に繋げることができた。
・現状の理解に繋がり、今後の対策に生かせるものでした。
・弊社のセキュリティレベルが客観的に審査されることにより、経営層に今後のセキュリティ対策提案がしやすくなった。
・自社の現時点での弱点が分かった。その対応策についてのアドバイスが得られた。

＜有益でなかった＞

・有益な事項がはっきりしなかった。
・当社独自に先行して情報セキュリティの強化を行っていた最中だったため、ご提案して頂く内容がなかった。

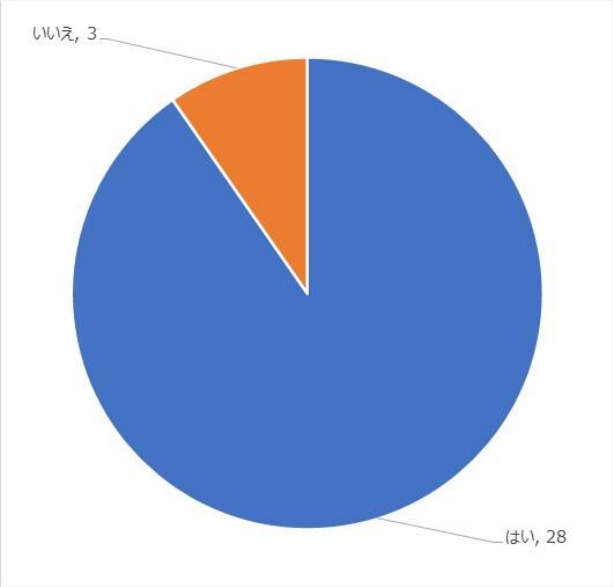


図 58 本実証事業の満足度について

Q2：今回のお助け隊事業で実施したサービスのうち、平時、有事のどちらが優先度が高いとお考えでしょうか？ （ n=69 ）

「平時・有事ともに重要」と回答した企業が圧倒的に多かった。主な意見として、「平時の時に対策していないと大きな事故にも繋がる」、「被害のリスクを考慮した場合、平時のセキュリティ対策が重要」など平時対策を重視する声が比較的多い一方で、「事故は毎日発生するわけではないが、発生した時は迅速かつ適切な対応を求められる」、「有事は専門性や緊急度が高く、外部の支援が必要」といった有事を重視する意見もあった。

自動車産業のサプライヤーとして、自社のセキュリティ対策の必要性を強く自覚している企業が多い印象であった。

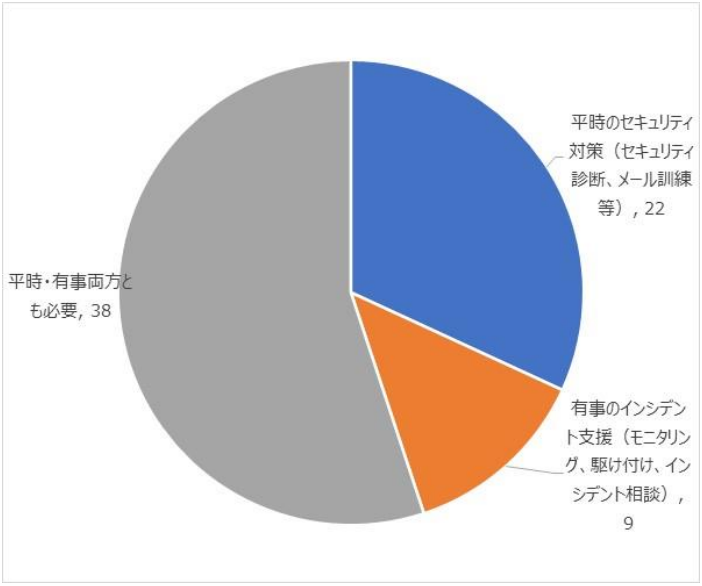


図 59 平時・有事対策の優先度について

Q3：今後「サイバーセキュリティお助け隊事業」がサービス化すれば、利用したいと思いますか？ （ n=69 ）

「費用対効果を考えながら検討したい」が圧倒的に多数を占めるなど、コスト面の課題を意識した回答が多数であった。セキュリティ意識が高い企業が多く、「必要性を感じないので利用しない」という回答者は少なかったが、一方で「すぐに利用したい」という回答はなかった。取引先からの要請など、何らかのきっかけがなければセキュリティ対策に重い腰があがらないという実態も垣間見えた。

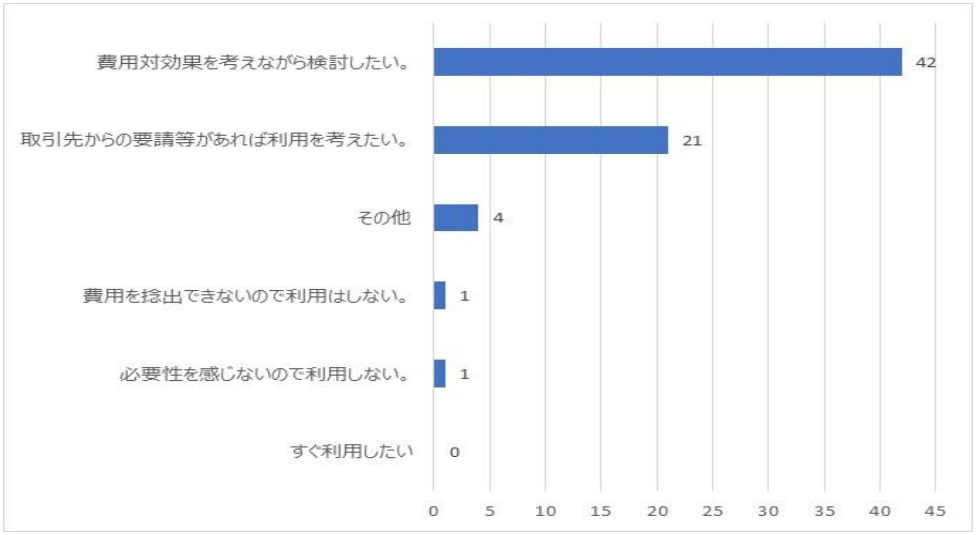


図 60 お助け隊サービスの今後の利用意向について

Q4：**サイバー保険について、貴社の加入状況を教えてください。　（ n=65 ）**

「既に加入している」という回答は 4 名（約 6.1%）と少なく、「加入していない」という回答が 61 名（約 93.9%）と圧倒的に多い結果となった。加入していない理由としては、「これまで提案を受けたことがなかったから」、「保険の存在を知らなかったから」というように、サイバー保険の認知度の低さが顕在化する結果となった。また、「今のところサイバー保険の必要性を感じていないから」という回答も多く、そもそもニーズがまだ顕在化していない実態が明らかになった。

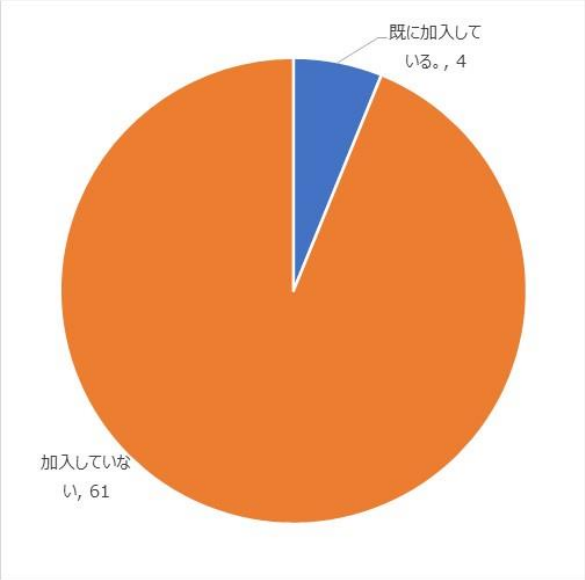


図 61 サイバー保険の加入状況について

Q5：貴社がサイバー保険の保険料として支出できる（支出している）保険料水準はどの程度でしょうか。 （ n=69 ）

サイバー保険の保険料として支出できる水準としては「分からない」が 38 名（約 55%）と圧倒的に多かった。保険の認知度が低く、妥当な保険料水準に見当がついていない実態が確認できた。年間 10 万円以上かけられるのは 5 名のみとなるなど、保険として支出できる水準は極めて低いという実態が分かった。

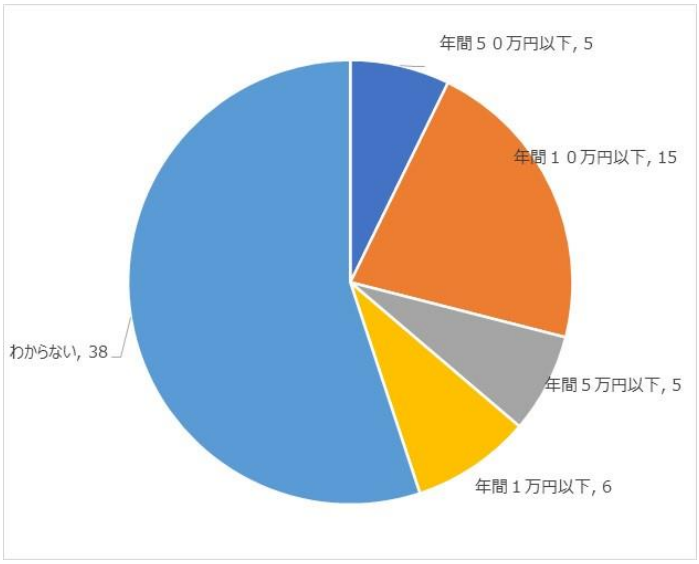


図 62 サイバー保険の許容保険料水準について

Q6：仮に今後サイバー保険加入を検討する場合、どのような手段で保険加入したいですか。 （ n=69 ）

サイバー保険に関する認識が低いことから「わからない」という回答が最も多く、次に「自動車業界の団体・組織等の割安な保険制度を利用したい」という回答が多かった。業界の特徴として、OEM メーカーやサプライヤー団体組織など、業界の繋がりを利用することを好む傾向があることが分かった。

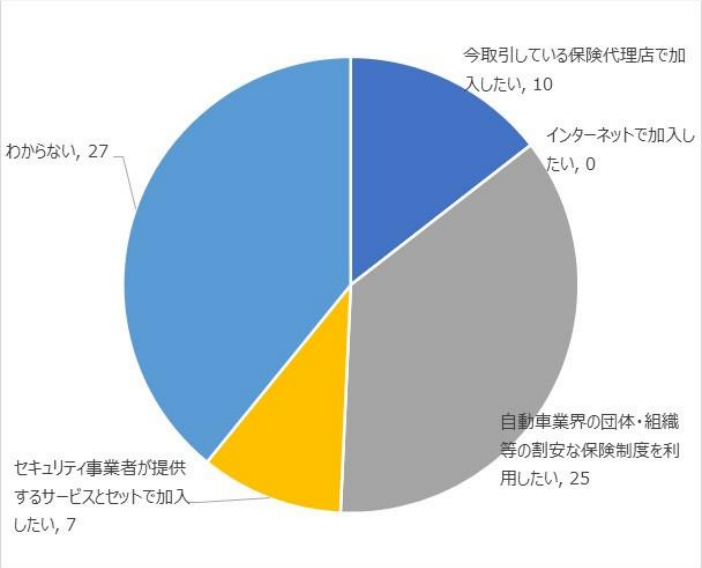


図 63 サイバー保険の加入手段について

Q7：貴サイバー保険では補償対象とならない以下のリスクについて、今後貴社においてリスク対策を検討されているまたは経営上のリスクとして認識しているものがあれば選択してください。なければ選択不要です。　（ n=69 ）

本設問は、中小企業サプライヤーが自社ネットワークが狙われる IT リスク以外の製品開発リスクとして、「①自社製品の欠陥が原因で完成車がサイバー攻撃に遭い、死傷者が出た場合の PL リスク」、「②自社製品の欠陥が原因で完成車がサイバー攻撃を受ける可能性があり、リコールとなるリスク」をどの程度懸念しているかを把握する目的で実施した。結果、75%の企業が当該リスクを今のところ感じていないという事実が分かった。一方、両方のリスクを感じている回答者も 25%存在し、これらは制御系システムや、電子部品など、外部からの攻撃を受ける可能性がある製品を取り扱う企業であった。

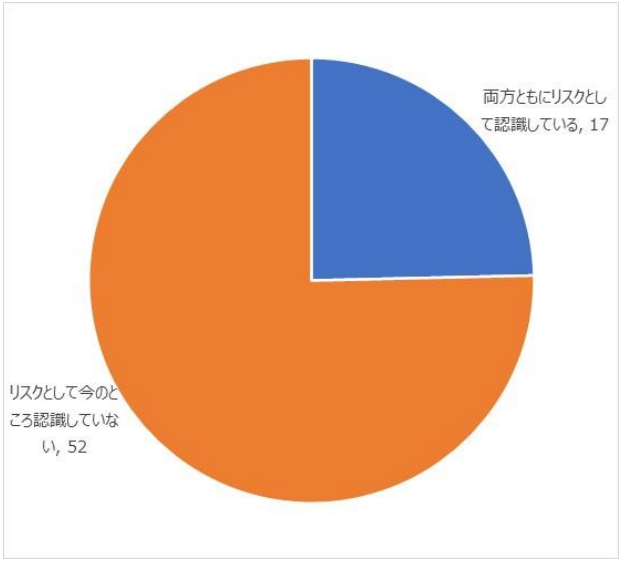


図 64 サイバー関連その他の経営リスク認知度について

Q8：IPA が推進している「SECURITY ACTION」の存在を知っていましたか
（ n=69 ）

「SECURITY ACTION」を認識している回答者は、25 名（約 36%）であった。

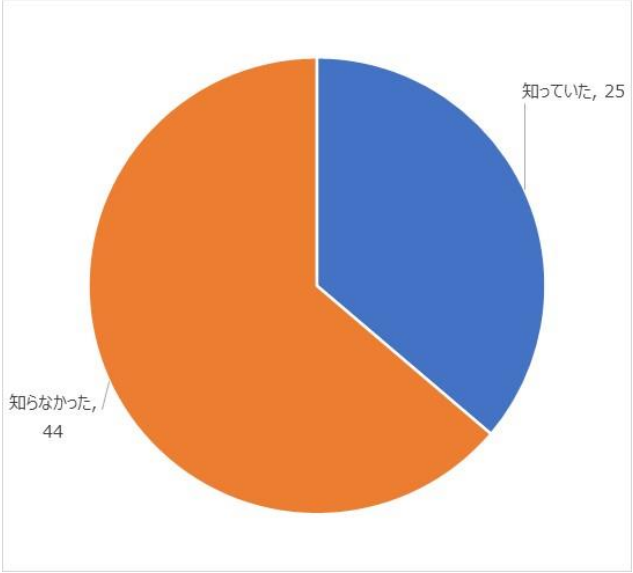


図 65 「SECURITY ACTION」の認知度について

Q9：上記で「①知っていた」を選択した場合、「SECURITY ACTION」自己宣言を実施していますか？ （ n=25 ）

「SECURITY ACTION」を認知している回答のうち、自己宣言を実施していると回答したのは４名であった。大半の企業はまだ実施されていない実態が判明した。

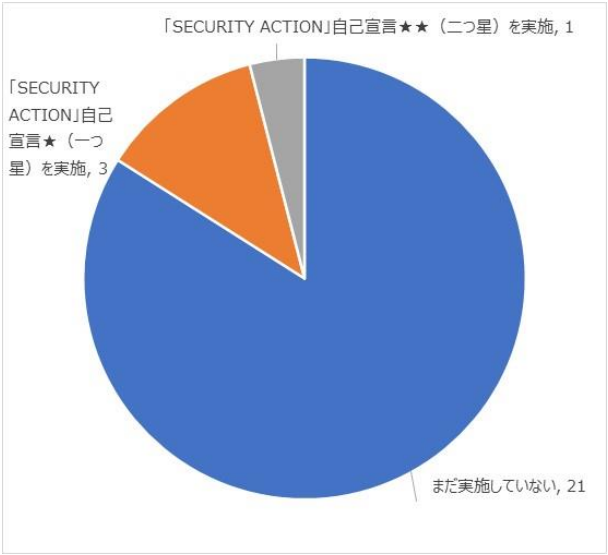


図 66 「SECURITY ACTION」の取組状況について

5. 考察

5.1 実証参加企業におけるサイバー攻撃に対する取組みの実態

自動車産業においては、サイバーセキュリティへの取組みに対する取引先からの要求が始まりつつあるものの、全体としては十分な対策ができていない傾向が見受けられる。

対策が進まない背景として、金銭的および人的なリソース不足等により、以下のようなセキュリティマネジメントに関わる取組みが遅れている実態が明らかとなった。

・ガバナンスの整備
※ポリシー（基本方針）、スタンダード（対策基準）、プロシージャー（実施手順）の策定等を示す。
・資産の記録や管理等の IT 運用
・セキュリティに関する社員教育

また、一部の企業では取組みは進んでいるが、そこでも継続的な改善を進めるところまでは、至っていないという状況であった。

そのため、運用に必要なドキュメントの標準化やセキュリティ専門家派遣や相談窓口の設置に関する支援を期待する声が多く聞かれた。また、システム導入等の技術的なセキュリティ対策を低コストかつ簡易導入で実現することもさることながら、企業経営に関わるセキュリティマネジメントについても支援する仕組みが求められている。

更に、実証参加企業担当者への問診では一定の対策を実施済であると回答している一方で、その後に実施したセキュリティ診断からは十分に対策がなされてない、あるいは対策が十分に機能していないと見受けられるケースが散見された。これは日々、脆弱性に関する情報が配信され、サイバー攻撃の脅威が多様化し、またエンドユーザーによるシャドーIT 利用が進む等、常に IT 環境が変化するため、IT 担当者がその健全性を網羅的に把握できていないことを示してるものと推察される。

このようなセキュリティへの取組み状況において、日本の基幹産業である自動車産業の中小企業サプライヤーがどの程度サイバー攻撃の脅威に晒されているかについて、UTM を実証参加企業に設置し、攻撃の実態を把握した。

結果として、「表 3-7 サイバー攻撃に関するアラート種別と検知状況（P51）」に記載のとおり、不正プログラムやランサムウェアが検出され UTM が遮断したケースや、詐欺サイトやスパムサイトへの誘導を UTM が遮断したケースが多数検出され、仮に UTM がなければ、マルウェア感染等の重大なセキュリティインシデントに繋がる可能性のあるサイバー攻撃が実際に発生している実態が見受けられた。

これは、中小企業を踏み台として大企業を狙うサプライチェーン攻撃が日常的に発生していることを示しており、サプライチェーン全体が常態的にサイバー攻撃の危険に晒されていることを裏付ける結果となった。

加えて、UTM を既に導入している企業においても、UTM のパターンファイルのアップデートや定期的なルール見直し等を含めたセキュリティ運用がおざなりにされるなど、十分なセキュリティ対策に繋がっていないという実態がヒアリングから浮き彫りとなっている。

こうしたセキュリティ対策の隙をつくようにサイバー攻撃の初期段階である、危険な Web サイトへの誘導やそれに類する不要なアクセス、標的型メールの受信は日常的に発生しており、致命的なセキュリティインシデントに発展するリスクは中小企業サプライヤーにおいても常に潜在している。UTM の未導入企業においても、その導入によって、一定のサイバーセキュリティ対策へ寄与はするが、導入後の運用も含めた支援が必要である。

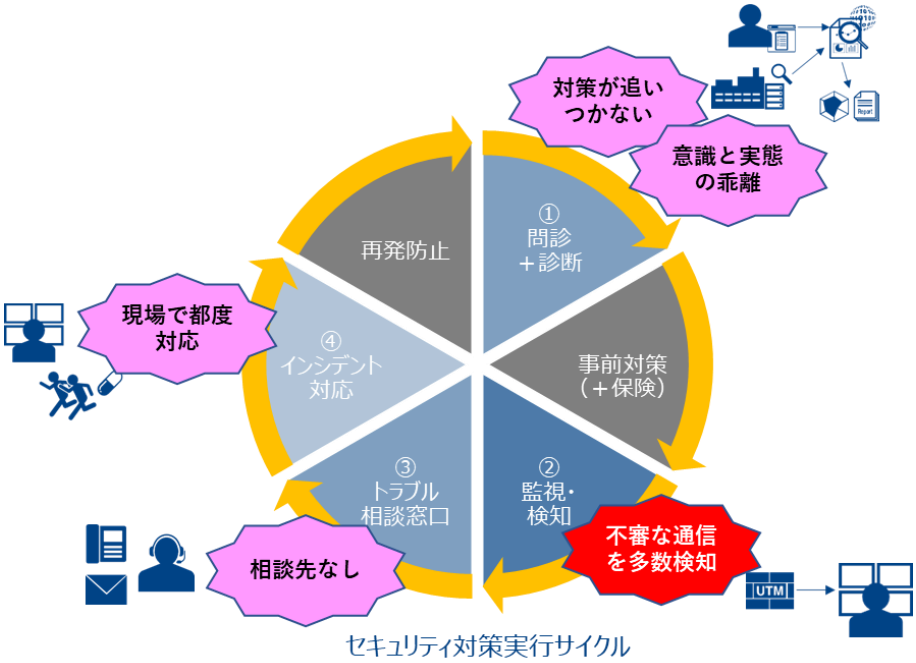


図 67　中小企業におけるセキュリティ対策の実態

5.2 中小企業におけるセキュリティ対策を進める上での課題

中小企業においてセキュリティ対策を進めるにあたっては、大企業と同様の考え方に基づき、検討を進められることが望ましい。しかし、中小企業においては、その規模や組織、人員等の特色を考慮した施策の立案および優先度付けと実行が必要である。そのため、既に実施済の対策状況の把握も含め、**「技術的な側面でのセキュリティ対策（システム導入等）」**と**「マネジメント的な側面でのセキュリティ対策（ポリシー策定や社員教育等）」**のそれぞれの観点において現状を把握し対策を行っていくことが不可欠である。

そこで、本実証事業においては、セキュリティ対策実行サイクルを鑑み、以下の観点で課題を抽出した。

（1） 問診

① セキュリティに対する全社的な課題認識の不足

自動車産業では、「セキュリティインシデント発生時の組織的な対応方法が決まっていない」という傾向にも見られたとおり、セキュリティへの対応が全社的な課題として認識されていない企業も見受けられる。

一方で、生産を行う工場領域に対するセキュリティを強化する上で、IT 部門が FA 系の IT を所管していないことも多く、生産部門を含め関係部門との連携の必要性を認識しているケースもあった。

また、セキュリティ対策に取り組むための投資の必要性が高まっている一方、自動車産業のおかれる事業環境は厳しい状況にあり、セキュリティ対策に対する積極的な予算確保が難しい状況であるが、経営者に対して、セキュリティインシデントが発生した場合の被害の大きさを認識してもらい、リスク対応を経営課題として捉えるとともに、セキュリティ投資を促すための啓発活動が課題となる。

② セキュリティ対策における人的リソースの不足

「セキュリティ対策について継続的な改善を進めるところまで取組みが進んでいない」、「取引先のセキュリティ対応まで、セキュリティ担当者の手が回っていない」といったように、対策を強化したいとの意欲を持っていても要員の不足により体制が整っておらず、十分な取組みが行えていない企業が多かった。

実際に、セキュリティ担当者がいても、CISO 等のセキュリティ責任者までは任命されておらず、経営層と連携してセキュリティ対応を実施する体制となっていないケースも多かった。また、専任の IT 部署を持つ企業は少なく、総務部等の共通部署内に担当者を就ける（兼任を含む）ケースや、IT 部署がある場合でも少ない担当者でセキュリティ対応を行っているケースがあり、セキュリティ体制が十分整備されておらず、結果として、担当者のスキル向上にも結び付かない状況といえる。

一方で、自動車産業においては専任のセキュリティ担当の配置要請が高まりつつあるが、中小企業においては、セキュリティ専任の部署を設置するなどの大規模な体制を構築することは難しい。したがって、CISO の任命等の「継続的な改善を含めたセキュリティ運用を実施していくために必要な最低限のセキュリティ管理体制」を明確にするとともに、少ない社内要員でも必要十分なセキュリティ管理を行えるよう、中小企業のセキュリティ担当者が気軽に利用できる相談窓口の整備や外部セキュリティ人材の活用を行える環境の整備が課題となる。

③ セキュリティ標準として何をどこまで規定すべきか不明確

問診結果において「セキュリティ水準の維持・改善プロセスの構築」、「セキュリティインシデント発生時の対応」といったセキュリティマネジメントに関連するカテゴリの多くで評価レベルが低い傾向が見受けられ、セキュリティポリシーや対応ルール、罰則規定等の文書化が遅れている。

原因として人手が足りていないこともあげられるが、それ以外にも「どのようなものが必要か。どこから始めれば良いか。どのレベルで作ったら良いのかが分からない」といった取組み方法に関する悩みも多く聞かれた。

このような声に対して、セキュリティマネジメントに関する底上げを遂行するには、OEM

メーカーがサプライヤーに求めるセキュリティマネジメントの要件を踏まえた上で、各サプライヤーが活用可能なひな形を業界や団体とともに、取扱製品種別なども加味した上で、整備・公開することが望ましい。

加えて、ひな形を具体的に自社へ適用するために、外部の専門家による教育、アドバイス、コンサルティングといったサービスをサプライヤーが利用できる環境整備も課題となる。

④ 不正アクセスの検知など、サイバー攻撃への一歩踏み込んだ対策が不十分

端末へのウイルス対策ソフトウェアの導入等、基本的な対策は進んでいるが、サイバー攻撃が高度化している現在において、従来のウイルス等のリスクを社内に持ち込まない対策だけでは不十分であり、万一侵入された場合も、その兆候をいち早く検知し、情報漏洩等の被害を発生させない対策を合わせて取ることが望ましい。

また特に FA ネットワークについては、生産制御用のパソコンや生産管理サーバー等、ソフトウェアの最新化やウイルス対策が取れない端末が存在するため、不正アクセスをリアルタイムで検知や遮断をするシステムの導入が望ましいが、取組みが進んでいない企業も多い。

以上より、ネットワークでの防御対策として、中小企業でも導入しやすい、経済的な不正通信の監視サービスの開発が課題となる。

⑤ 自社の取引先に対するセキュリティ状況の把握

2021 年の CS/SU 法の施行に備え、最終的には全階層のサプライヤーに対し、セキュリティ上の要件を満たすことが求められるが、現時点では自社（および自社のグループ会社）におけるセキュリティ対策が手一杯で、自社のサプライヤーに対するセキュリティ状況の把握や指導にまでは手が及んでいない企業がほとんどである。

また、サプライヤーの取り扱い製品の特性によりセキュリティ要件のレベルが異なるとともに、企業規模により対策に投資可能な予算規模には制約があるため、どこまでの水準を求めれば良いか分からないと困惑している企業が多かった。

こうした背景から、企業の状況や取扱製品に応じて、何パターンかのセキュリティ基準を設けるとともに、セキュリティチェックシート等を通じてサプライヤー自身で定期的な改善に取り組める仕組み作りが課題となる。

（2） 外部診断

実証参加企業の 75%以上の企業で Web サーバーのセキュリティ設定にリスクがあることが分かった。これらは Firewall や UTM の設置でリスク低減可能なネットワーク関連の対応と異なり、サーバープログラムの動きや仕様の理解が必要になるため、非専任の IT 担当者の多い中小企業ではセキュリティ対応の敷居が高いことが窺える。自社設計または外注時の委託仕様として手軽に利用できるガイドラインや、ガイドラインの遵守レベルを確認できる簡便なチェック手法など、IT 担当者の負荷を増やさずにセキュリティ対策が実施できる支援体制の拡充が必要である。

なお、外部診断の対象となる公開サイトはクラウドサービスやホスティングサービスを利用している中小企業が多く、サーバーへの脆弱性パッチ適用など一定の対策がなされていた。しかしながら、より詳細な診断（セキュリティリスクをあぶり出すペネトレーションテスト等）を実施するにあたっては、利用サービスの提供元へ個別に実施可否を確認する等が必要であり、IT 担当者に調整等の負担が発生するケースがあるため、クラウドサービス

やホスティングサービスを利用している場合に、どのようにサイトの健全性を確認するかといった今後の課題も明らかとなった。

外部診断においては、IT 担当者の負担なく安価で簡易に実施できる診断をベースとし、簡易診断結果から必要に応じて的を絞って詳細診断が限定的に実施できる多段階の診断手法の整備が望まれる。

（3） 内部診断

実証参加企業の大半において、社内ネットワークに接続している端末に対するパッチマネジメントが適切に行われておらず、サポート切れ OS を利用しているケースも多数あり、企業内部に侵入されると即座に被害が拡散するリスクがある状況であった。

このことから、今後も診断を通じて、企業内部の脆弱性を可視化し効果的な対策の検討に繋げられる点においては、診断サービスメニューの一部として提供していくことは効果があると考える。

一方で、問診（アセスメント）からも実態が明らかになっているように、重要資産の定義や、資産の定期的な棚卸し等の運用・管理が継続的に実施できていないこともあり、セキュリティマネジメント観点での対策（IT 資産管理やセキュリティ運用に関するルールの策定）を先行して実施することで、パッチの適用漏れやシャドーIT 資産の廃止等、脆弱な端末を一定数削減できるとも考えられる。

したがって、セキュリティマネジメント観点での対策と内部診断による資産の可視化をセットで実施することで、恒常的に企業内部のセキュリティリスクを最小化することが望ましいと考える。また、企業によっては、利用しているシステムの都合でパッチ適用や端末の入れ替えが難しいケースも一定数は残存すると考えられるため、そうした資産を明確にした上で、それらを対象とした防御対策（FW による通信先相手のフィルタリングやネットワークセグメントの分離等）を講じ、防御対象に適したリスク軽減策を実施することで、効果的なセキュリティ投資に繋げることが重要であり、ケースに応じて取るべき対策を問診や診断結果からより分かりやすく提示できるかが課題である。

また、診断についても実証を通じた実態を把握する中で課題が見つかっており、自動車産業の中小企業サプライヤーは大企業同様に、複数拠点や多数の端末を抱えている企業が多いため、全体を診断対象とした網羅的な診断は実施事業者（診断サービス提供者）側の提供コストに影響するだけでなく、診断を受ける企業側の IT 担当者の負担も大きい。内部診断においては、対象企業の健全性を計るにあたり、対策実施の指標となる妥当な診断対象数および診断対象の選定方法の確立が必要である。

（4） マルウェア対策

マルウェア混入に対する対策状況を診断するためには、標的型訓練メールのような開封チェックを行うだけではなく、無害の疑似マルウェアや不正プログラム等の実行可否を確認する必要がある。今回の実証では、一歩踏み込んだ診断（疑似マルウェアの実行確認等）を行うことで、より詳細な実態把握を実施したが、以下の課題が表面化した。

- メールの送達や URL のクリック等の仕組みでは、端末まで到達しなかった場合に多層防御の一端を確認できるに過ぎず（「どこかで防御された。」は証明できるが、「どこでどうやって防御された」のかが証明できない。）、実際のマルウェア感染リスクが 0 であることが断言できない。

・対象者の回答による診断では、誤記や認識齟齬もあり診断精度に限界があるとともに、回答矛盾に対する個別ヒアリング等を踏まえると、低コスト化が難しい。

上記より、効果的かつ踏み込んだマルウェア対策診断を実現するためは、診断対象者に依存せず、低コストでエンドツーエンドのセキュリティ対策状況を診断できる手法の確立が必要である。

一方でマルウェア混入を防ぐ仕組みも様々なセキュリティ製品に組み込まれており、システム的にどこで遮断されたかの証跡を示し中小企業が自身で証明することが難しい実態にあるため、様々な種類のマルウェアや実行ファイルの検体を準備するなど診断側の仕組みを高度化することが課題である。

（5） 検知・監視

UTM の設置により、外部から攻撃や不正なサイトへのアクセスを検知し、不正通信をブロックしたアラートを検出することはできるため、セキュリティ攻撃への対策に対して導入効果は見受けられるが､それらの全ての原因を調査･追及していては時間や費用がかかり、低コスト化を図ることができない。したがって、重篤なインシデントに発展する予兆を効率よく検出し、水際で防ぐ監視・運用方法の確立が必要である。加えて必要最低限の分かりやすいレポートをユーザー通知するだけの仕組みもあわせて提供することが必要となる。

また、UTM の導入・設置においても、今回は企業内に機器を設置する形式で実証を行ったが、機器設置においても、自社のネットワークを担当者が十分に把握できていないことが一部で浮き彫りとなり、設置までに非常に多くの時間を要したケースもあった。

加えて、自動車産業のサプライヤーでは地理的に離れた複数の工場を保有しているケースも多くあり、機器設置型の UTM を各拠点で導入することは、IT リソースが不足しているサプライヤーには保守・運用の観点で、今後大きな負担になる可能性も想定される。したがって、クラウド型の UTM メニュー等、企業特性に応じた導入プランを設けることも普及・促進には重要である。

今後、自動車産業においては、UTM による脅威検知・防御だけでなく、UTM で防御できていない攻撃に対しても不審な「振る舞い」を監視し、サイバー攻撃による情報漏洩等に対して未然に防止する対応が、制御部品等のソフトウェア開発を行うサプライヤーを皮切りに求められる状況になってくるため、SIEM（Security Information and Event Management）と連携した UTM サービス等の検討も重要となる。

（6） トラブル相談

自社のセキュリティに関して中小企業が相談したい内容は多岐にわたり、内容の難易度も異なるため､その対応に求められるスキルセットも様々である｡利用する企業側にとって、相談したい時にすぐ相談でき、問合せるための手間も少ない窓口を設置するとともに、簡単な質疑については自動応答で返答するなどの効率化により、応対の低コスト化が必要である。また、問合せ件数の削減に繋がる IT 担当者のスキル向上の助けとなる育成プログラム等の仕組みもあわせて提供することが必要である。

（7） インシデント対応

インシデント対応においては被害の拡大を抑えるため初動が重要であるが、その課題と

して以下の２つがあると考える。

①インシデントであるかの判断が難しい

インシデント対応結果でも記載したとおり、高度な攻撃に対する振る舞い検知が可能なUTM を一部の実証参加企業に設置したが、UTM のアラートの信憑性を判断するためにはプロキシ等のログとの相関分析が必要となり、具体的な調査内容を伝えても、実証参加企業の事情（調査コストがかかる）もあり、十分な回答を得られないといった課題も明らかとなった。

そのため、高度な攻撃に対応が求められる場合には、アラートを適切に判断する仕組みの検討が必要であり、内部の通信ログ等も収集可能なセンサー等を組み合わせた提供方法を検討することが重要である。

②インシデント対応ルールが不明確。

CSIRT のような仕組みがないと、インシデントと判明しても誰がどのように何を調べて、どう対応して良いかが判らない状況に陥ってしまう。効率的にインシデント判断ができる仕組みと、インシデント発生時の初動対応のルール化が必要である。

5.3 中小企業において必要なセキュリティ対策

サイバー攻撃からサプライヤーの生産活動を守り、サプライチェーンを継続させるためには、前項の課題を踏まえると以下のような解決の方向性を提供していくことが重要であると想定される。

また、提供にあたっては、1 社 1 社個別に提供するのではなく、業界団体や組合、OEM メーカー等と連携して普及・促進をすることで、経済的で簡易に提供できる仕組みを構築することが重要である。

（1）中小企業の経営者向け啓発活動

経営者向けセミナーの開催等により、セキュリティが経営活動上の大きなリスクとなることを訴求し、経営層の理解を深める活動が不可欠である。

（2）サプライチェーンの業界団体や組合、OEM メーカー主導によるセキュリティ標準の策定

サプライヤーである中小企業が求めているのは、一般的なガイドラインではなく、サプライチェーンの業種業態、取り扱い製品等に応じた活用しやすいガイドラインや各種ドキュメント標準のひな形の公開であり、これらにサプライヤーに必要な最低限のセキュリティ管理・運用に関するスキルの取得支援や標的型訓練等の社員教育に関わるコンテンツ提供を行うことで、マネジメントレベルのセキュリティ意識の底上げを実現することである。（業界と連携して支援を行っていくことが重要）

課題と解決の方向性のイメージは以下となる。

図 68 企業が抱えている悩み

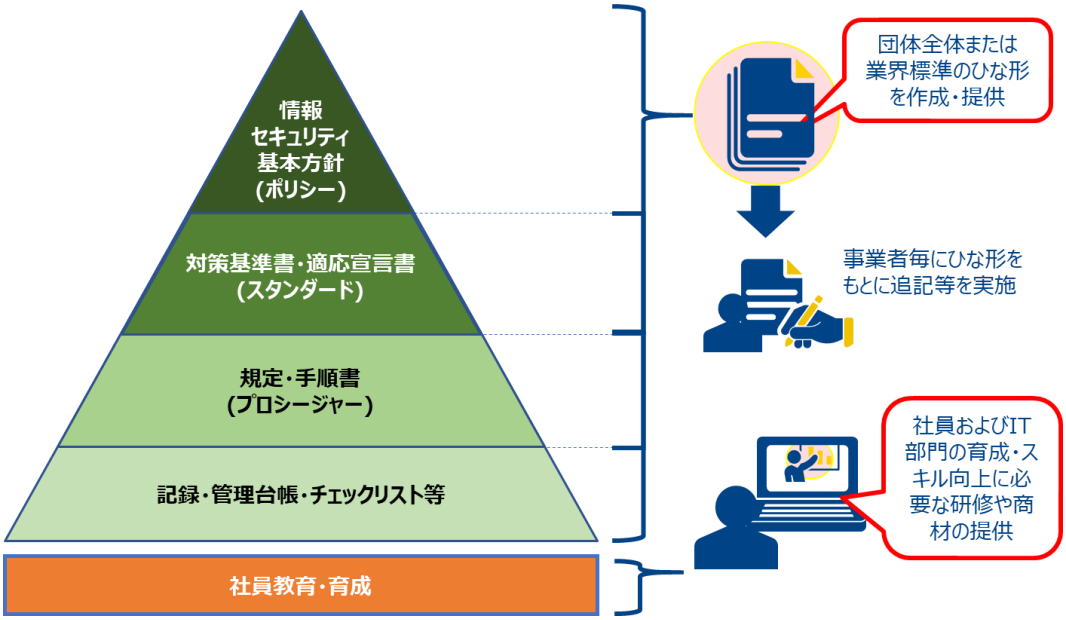


図 69 解決の方向性

（3）セキュリティ対策レベルの把握および対策に向けたセキュリティ診断の定期的な実施

自動車産業においては、一般的な診断項目だけではなく、業種業態や取扱製品等も踏まえた IT リスク診断が求められており、業界団体や組合、OEM メーカー等の求める要件を満たした統一されたアセスメント項目かつ具体的に何を実施することで必須要件を満たすのかが示されていることが必要である。また、比較的自社と関係性の近い同業他社との対策状況が比較できることも重要である。

課題と解決の方向性のイメージは以下となる。

図 70 企業が抱えている悩み

	①簡易診断	②アセスメント	③診断結果評価
概要	サイバーリスク対応評価	Web問診	①と②の結果を踏まえたトータル評価
特徴	・インターネットに公開されている企業ドメインのシステム運用状況をチェックしレーティング結果(スコア)を評価、技術的施策の課題や問題点を把握 ・同業他社とのスコア比較が可能	・問診票のカスタマイズが可能 業界で統一されたアセスメント項目であり、何をやる事で要件が満たせるのかが具体的にわかることが重要 ・サイバーセキュリティリスクへの技術的な対応状況が問診対象の会社やグループの水準と比してどの程度のレベルにあるのか可視化し、問診結果から課題を把握	・①と②での診断結果に加えてトータル評価およびアクションプランなどのアドバイスを実施

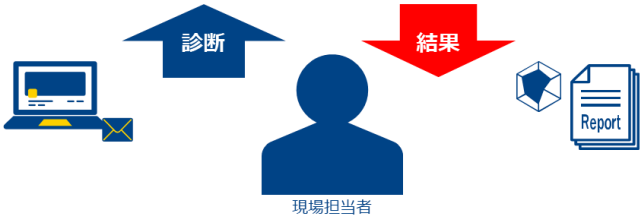


図 71 解決の方向性

（4）中小企業が経済的に利用できるセキュリティ監視・侵入防御サービスの提供（UTM+SOC サービス）

重要なのは、（3） の診断と紐付いたソリューションメニューと、診断結果をベースとした優先度の高い対策を選択して導入できることである。

課題と解決の方向性のイメージは以下となる。

図 72 企業が抱えている悩み

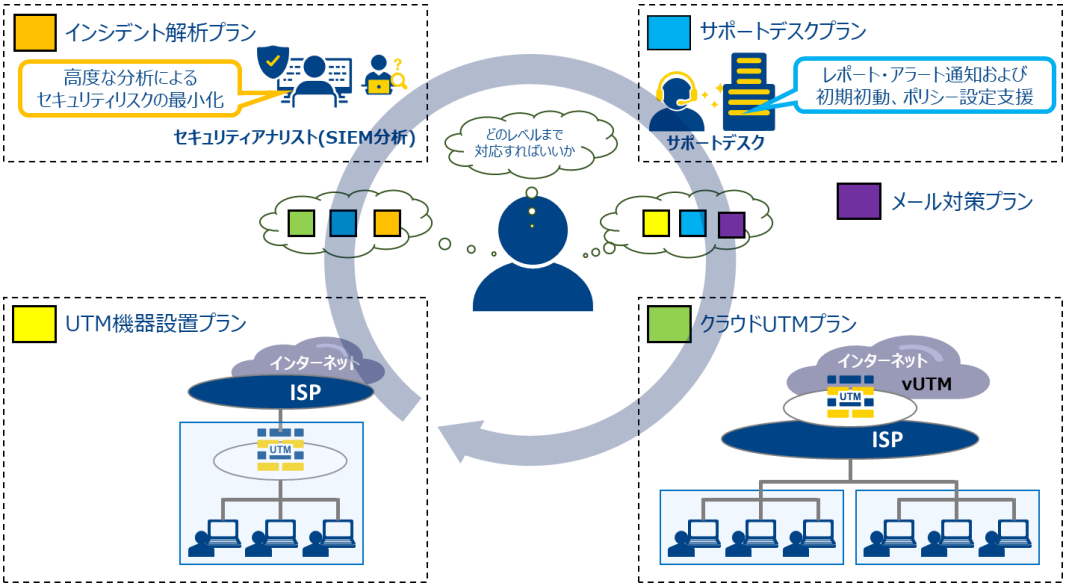


図 73 解決の方向性

（5） 中小企業のセキュリティ担当者が気軽に相談できる窓口の整備

自動車産業においては、セキュリティ専門家としてのアドバイスと業界事情に精通した判断が必要となるケースがあるため、課題の解決にはこの 2 つの視点で支援できる体制構築をどのように実現するかといったことがポイントである。

5.4 中小企業におけるセキュリティ対策の効果

自動車産業の中小企業サプライヤーでは、取引先からのサイバーセキュリティ対策に関する要求が始まりつつある状況であるが、限られた予算、IT 担当者のリソースに対して、自社の企業活動（利益拡大）に直結しないセキュリティ対策は導入効果の測定が難しく、取組みに優先順位が付けらないため、対策を進められていない現状であった。

また、同業他社の取組み状況についても横の繋がりによる断片的な情報収集にとどまり、自社のおかれたセキュリティ対策状況を客観的に分析して経営層へ報告し、予算化に結び付けることが難しく、その結果として、セキュリティインシデントが発生してから対策を実行する等、後手に回るリスクが IT 担当者の悩みでもあった。

そうした背景もあり、本実証事業で実施した内容は、客観的かつ同業者と比較して自社のおかれた状況を「セキュリティマネジメントの観点」と「技術的対策の観点」から把握することができ、今後の対策実行に向け経営層を説得していく上でも有用なものであったとの声が実証参加企業より挙がった。また自社の認識と実際の対策状況の乖離も発見することができ、問診を通じたアセスメントメンバーとのやり取りの中で、すぐにセキュリティポリシーを見直すなど、セキュリティ強化のきっかけとなる気づきを得ることができたとの反応も受けている。

こうしたことから、セキュリティ意識の向上やセキュリティ対策の進展に関しては、同業他社における対策状況も踏まえ、自社にとって適正なセキュリティ対策の計画を立案し、セキュリティ対策投資に関する経営層の理解を得るための材料（内容が分かりやすく、自動車産業の取扱製品に応じた「問診」や「技術的診断」の結果）を提供する取組みが有効であったと考えられる。

これらを 1 社 1 社個別に対応するのではなく、業界や団体を通じた枠組みの中で実現することで、相互扶助を醸成し、経済的な支援サービス・体制を構築することにより、自動車産業のサプライチェーンが計画的かつ継続的にサイバーセキュリティ対策に取り組むことで、日本の基幹産業である自動車産業全体の底上げに効果が見込まれる。

6. 実証を踏まえたビジネス化に向けた検討

6.1 中小企業に最適なサイバー保険の活用

（1）中小企業サプライヤーの保険認識実態について

日本市場においてサイバー保険の展開が本格的に始まった 2015 年以降、本保険の活用を含めたセキュリティ対策が注目されている。2018 年に損害保険協会が実施した「サイバー保険に関する調査 2018」[4]によると、企業全体のサイバー保険の加入率は 12%、製造業では 8.5%という調査結果になっており、国内における本保険の普及状況はまだまだ十分ではない。本実証事業で実施したセキュリティ実態調査アンケート結果（P64）においても、中小企業サプライヤーの加入率は約 6.1%と低水準の結果となった。中小企業サプライヤーが回答した本保険への未加入の理由（上位 3 位）は以下のとおり。

＜未加入の理由（上位 3 位）＞
・これまで提案を受けたことがなかったから
・今のところサイバー保険の必要性を感じていないから
・保険の存在を知らなかったから

上記理由から考察すると、まず保険加入以前に、中小企業にサイバー保険の存在や補償・サービス内容が行き届いていないということが推測できる。多くの中小企業は、その存在や内容を認識しておらず、その効果や必要性について検討したことがないというのが中小企業サプライヤーの現時点の実態である。

また、サイバー保険に支出できる保険料水準に関するアンケート（P64-65）においても、半数が「分からない」と回答している。ここからも本保険の情報が中小企業サプライヤーに行き届いていないため、どの程度の保険料が妥当かという判断ができなかったことが分かる。

（2）中小企業サプライヤーにとってのサイバー保険の活用意義と活用方式の考察

① サイバー保険の活用意義について

自動車産業では OEM メーカーからの要請が始まりつつあるなど、今後サプライチェーン全体でサイバーセキュリティに関する体制構築が急務であり、本実証実験においても中小企業サプライヤーの意識が徐々に高まっていることが分かった。一方、中小企業サプライヤーにはセキュリティに投資できる経済的な余裕がなく、一から体制構築するには相当な時間と資金、人材が必要となるなど、現実的ではない。このような厳しい状況下におかれた中小企業サプライヤーが、迅速で効率的にセキュリティ体制を強化する手段として、サイバー保険や損害保険会社が提供する各種サービスを活用するという選択肢を考えたい。サイバー保険には、本来の機能であるファイナンス機能のほか、以下のとおり損害保険会社が有するノウハウやサービスを活用することにより、中小企業サプライヤーが平時・有事に必要とする情報や機能を効率的に活用できる可能性がある。

---

[4] 損害保険協会：サイバー保険に関する調査 2018
https://www.sonpo.or.jp/news/release/2018/1903_02.html （2021/1/17 参照）

＜サイバー保険等 損害保険会社が有する主なサービス＞
・サイバーセキュリティに関する最新情報・基礎知識の提供収集機能（平時）
・サイバートラブル発生時のアドバイス機能（平時・有事）
・インシデント発生時の初動対応に関する専門的なアドバイス機能（有事）
・損害保険会社が有するセキュリティ専門事業者とのネットワークの活用（平時・有事）

② サイバー保険の活用方式について

中小企業サプライヤーがサイバー保険を活用する場合の方式について考察する。本保険の活用にあたっては、主に以下の方式が想定される。それぞれの方式にはメリット、デメリットがあるため、下表に整理する。

ア　簡易保険（サービス付帯方式）

セキュリティ事業者等が提供するセキュリティ製品やサービスに一律で付帯されている保険を活用する方式。セキュリティ事業者等が補償等を決定し、サービス購入者全員に一律で提供することが一般的である。

イ　本格保険（任意加入方式）

加入企業が自らの意思に基づいて任意で保険に加入する方式。加入企業が補償等を自ら決定し、保険契約を締結して加入するもの。

表 17 サイバー保険活用方式別のメリット・デメリットについて

	メリット	デメリット
簡易保険（サービス付帯方式）	・サービス料に保険料が含まれており負担感がない。 ・保険加入手続きが不要で、個別に判断する必要性がない。	・自社が必要な補償を自ら確保することができない。 ・比較的小さな補償しか確保できない場合が多い。
本格保険（任意加入方式）	・自社が必要な補償を自ら決定することが可能。 ・比較的大きな補償を確保することができる。	・保険料が高額になる場合が多く、負担感が高い。 ・保険加入手続きが発生し、加入の意思決定が必要。

加入する企業のニーズや保険活用目的に応じて、上記活用方式を組み合わせることで、中小企業にとってコスト面においても無駄がなく、バランスの良い最適な保険活用が実現できる。

6.1.1 中小企業に必要な補償内容の考察

中小企業サプライヤーがおかれた自動車産業特有の動向やアンケート結果や個社企業からのヒアリング結果等から洗い出された企業ニーズ等を踏まえて、中小企業サプライヤーが必要とする補償内容を考察した。

（1）企業 IT リスクに関連する補償ニーズ

中小企業サプライヤーがサイバー攻撃を受けた際に最も必要とするサポートに関するアンケート結果（P30）によると、中小企業サプライヤーは主に以下の補償に対して高い関心を示していることが分かる。それぞれの補償について以下考察する。

① 原因・影響範囲調査ニーズ

一般的に、インシデント発生時の初期の段階で発生する代表的な費用として、フォレンジックと呼ばれる原因調査に要する費用があげられる。この調査を実施する企業の目的は、自社の被害の原因や被害範囲を特定し、早期に再発防止を図ることにある。あわせて、取引先やその他のステークホルダーへの説明責任という観点がある。第三者による客観的な調査を入れ、合理的な企業判断をしたという事実を関係者と共有し、自社のレピュテーション下落リスクを極小化するという目的である。これらは通常大企業のニーズであり、一般的な中小企業が、このような原因調査に高額の費用を費消するケースは比較的少ない。

一方、自動車産業においてはサプライチェーンを構成する中小企業が狙われる「サプライチェーン攻撃」が多発しており、これらの事象が発生した場合には、OEM メーカーや上位のサプライヤーが関与することになり、中小企業サプライヤーは精緻な原因究明と再発防止策の提示を求められる可能性がある。このような場合は、自社が好むと好まざるとに関わらず、フォレンジック調査が必須となり、パソコン 1 台あたり約 100 万円～150 万円が相場といわれる費用を必然的に負担することになる。したがって、自動車産業における中小企業サプライヤーは、一般的な中小企業と比較して、一定規模の原因調査費用を補償する保険を手配しておく必要性が高いといえる。

② 駆け付け・初動対応費用ニーズ

次にニーズとして高いのが、駆け付けや初動対応に関する費用ニーズである。これは、インシデント対応に不慣れな中小企業共通のニーズであり、中小企業サプライヤーも例外ではない。インシデント発生時には迅速で適切な対応を産業として求められることから、必要な補償と考える。このニーズには、金銭的な費用補償ニーズに加えて、外部機関の駆け付けや専門的アドバイス等を求めるサービスニーズも含まれており、本実証事業で提供したトラブル相談窓口をサイバー保険とセットで提供できることが望ましい。

③ 復旧にかかる費用補償ニーズ

復旧に関する補償ニーズが高いのも中小企業サプライヤーの特徴である。自動車産業では、サプライチェーン攻撃による事業停止リスクが大きなリスクのうちの一つであり、OEM メーカーへの供給が停止してしまうことはサプライヤー企業にとって死活問題である。これら事業停止リスクを極小化するために、ウイルス駆除などの迅速な復帰対応や再発防止に要する費用、事業を継続するための各種費用に関するニーズが想定される。また、製造業では、IT ネットワークのほかに、工場の制御システム等の OT（Operational Technology）システムが攻撃の対象となるリスクも想定に入れる必要がある。本実証事業は主に IT セキュリティを対象としたものであったが、自動車産業では今後 OT セキュリティに関するニーズの高まりにも焦点をあてる必要がある。

④ 第三者への補償（賠償）

中小企業サプライヤーには第三者への補償、つまり OEM メーカー等の取引先への損害

賠償責任に関する補償ニーズがあることも確認できた。これは、自社が「踏み台」となり、取引先が不正アクセスを受けた場合や、図面等の製品製造に関する知的財産が社外に流出する場合の損害賠償責任など、取引先へ負の影響を及ぼした場合の補償についても懸念している実態が窺えた。

（2） 企業の製品開発リスクに関連する補償ニーズ

自動車産業においては、コネクテッドカーや自動運転技術の進展に伴って、自動車自体のサイバーセキュリティ対策が喫緊の課題になりつつあるが、これらの対策は自動車を構成する各部品のセキュリティに依存する要素が大きく、OEM メーカーをはじめとしたサプライチェーン全体でセキュアな自動車開発に取り組むことが前提となる。

中小企業サプライヤーにとって、前述のとおり自社がサイバー攻撃を受けるリスクのほか、自社製品がサイバー攻撃を受けるリスクについても想定しておく必要があると考えた。例えば、自社製品が外部からのサイバー攻撃を受ける可能性がある場合、当該製品の欠陥に起因してインシデントが発生し死傷者が出るケースや、その欠陥に起因したリコールが行われるケース等を想定した。この観点で、中小企業サプライヤーには自社製品の欠陥が顕在化した場合のリスク対策として、PL 保険やリコール保険等の補償ニーズがあるという仮説を立てた。

上記に関してアンケートによる意識調査（P66）を実施したところ、大半の企業がこのようなリスクを現時点では認識していないという結果となった。ただし、電子部品等を製造する一部のサプライヤーは、上記リスクを経営リスクとして認識しているという回答が得られた。

今回実証事業に参加した中小企業サプライヤーには、自動車のサイバーセキュリティに直接的に影響を与える電子部品や制御システム等を製造する企業が比較的少なく、上記のような PL・リコールリスクのニーズは小さく表れたが、サプライヤーの中でも、電子部品等を製造する企業層には、当該リスクに対する補償ニーズは存在することから、今後は製造する製品サプライヤーによって補償内容をアレンジしていくことが望ましい。

6.1.2 中小企業が加入しやすい保険制度

（1）中小企業サプライヤーに望ましい保険内容

5.1.1 で考察したとおり、自動車産業に属する中小企業サプライヤーのサイバー保険に関するニーズは、一般的な中小企業ニーズと比較して異なるニーズが存在すると考えた。サプライチェーンとして取引先企業とより密接な関係を保持してきた自動車産業の特性から、インシデント発生時などの有事の際には、OEM メーカーやその他の取引先への影響を考慮しながら連携した対応を実施する傾向があり、原因究明や早期の復旧をより重視する傾向があることが分かった。中小企業サプライヤーの主要ニーズである原因・影響範囲調査費用や復旧に関する費用については、大きな補償額を必要とし、個社ごとにその補償ニーズが異なることから、これらの補償を確保するために、前述の簡易保険を活用することは適切ではない。個社ごとに必要補償額を個別に設定できる本格保険を活用することが望ましい保険手当ての方法である。

一方、中小企業サプライヤーでは、サイバーに関する専門的な人材が不足しており、インシデント発生時の駆け付けや初動対応に関する支援については全社共通のニーズである。

これらの駆け付け等に関する費用は比較的軽微であり、中小企業サプライヤー個社ごとのニーズ差が出にくい補償であることから、簡易保険を活用することが最適である。これらは日常の監視・検知のサービスに付随して補償を提供することが望ましい。

（2） 自動車産業の業界団体における各種保険制度の発足

中小企業サプライヤーはどのような手段で保険に加入することが最適なのかについても考察する。本実証事業で実施したアンケート（P65）で、「今後サイバー保険加入を検討する場合どのような手段で保険加入したいですか」という調査を実施した。「わからない」という回答に次いで、多数を占めた回答は「自動車業界の団体・組織等の割安な保険制度を利用したい」という回答であった。自動車産業は、OEM メーカーやサプライヤー企業間の結束が強く、既にこれらの団体・組織が有効に機能していることから、保険についてもこれらの組織を通じて加入したいという意向が明らかになった。

中小企業サプライヤーは、通常特定の各 OEM メーカーのサプライチェーン傘下で事業を行っていることから、当初は保険制度についても各 OME メーカー単位での制度化を実現することが有効と考えていたが、今回の実証事業で複数の OEM メーカーとの取引がある中小企業サプライヤーが存在することが分かった。このようなケースでは、OEM メーカーごとに保険制度を設立することは、中小企業サプライヤーにとって分かりにくく、無駄が多い保険制度となってしまうおそれがある。

これらの状況を踏まえると、自動車産業では保険加入においても、中小企業サプライヤーが個社ごとに検討をするのではなく、また OEM メーカーごとに保険制度を検討するのでもなく、自動車産業共通で一貫した保険制度の組成・運営が望ましい。例えば、J-Auto-ISAC[5]のような業界横串組織で保険制度を発足し、制度の中で各種サービスと同時に展開していくことが非常に有効と考える。このような会員向けのセキュリティサービスと保険制度が、中小企業サプライヤーに広く普及することで、自動車産業全体のセキュリティのレベルアップを図ると同時に、インシデント対応時のノウハウや最新のサイバー脅威の情報共有にも繋がるものと考える。

6.2 中小企業向けセキュリティビジネス化に向けた課題・検討

6.2.1 ビジネス化に向けたサービスイメージ

(1) セキュリティ投資に関する基本的な考え方

「セキュリティ対策＝コスト」という考え方からの脱却は難しいテーマとなっている。「投資効果が見えにくい」、「どんな対策からすれば効果的かが分かりにくい」等の課題が解決されない限り経営者の理解が得られにくい状況にある。

[5] 一般社団法人日本自動車工業会内のサイバーセキュリティに関するインシデント情報等を共有する組織。2021 年 4 月に一般社団法人化が予定されている。

自社のセキュリティ対策レベルを客観的に知ることで効果の可視化が可能となり、対策の優先順位も分かるため、結果的にセキュリティ対策の ROI（投下資本利益率）が向上すると考える。以下の図は、平時からの適切なセキュリティ投資と企業価値の増減に関する相関を考察したものである。

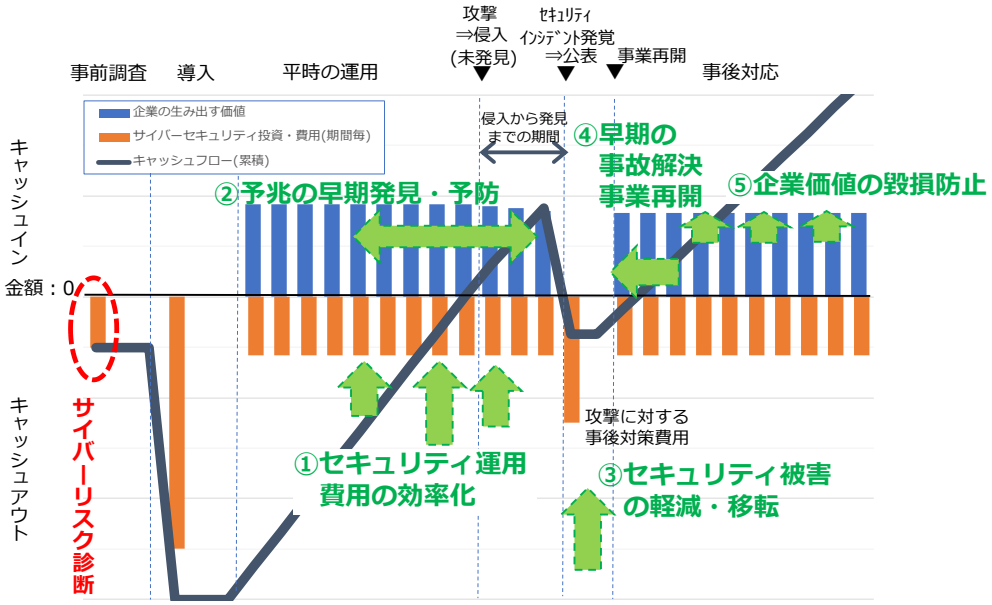


図 74 セキュリティ投資と企業価値について

① セキュリティ運用費用の効率化

適切な診断によるリスク管理を行うことで、平時のセキュリティ運用を効率的、安定的に実施することにより、セキュリティ対策費用を必要最低限に抑えることができる。

② 予兆の早期発見・予防

リスクの変化や攻撃の予兆を早期に発見することで重大インシデントの発生を予防できる。

③ セキュリティ被害の軽減・移転

重大なセキュリティインシデントが発生した場合にも、被害を最低限に抑え、短期間での事業回復を実現し、企業価値の低下を抑止する。

④ 早期の事故解決・事業再開

万一のセキュリティインシデントに対し、早期の事故解決を行うことで事業停止期間を最短化し逸失利益を最小化する。

⑤ 企業価値の毀損防止

企業のレピュテーションリスクを最小化することで、毀損を防止することが可能となる。

(2) サイバーエコシステムについて

人間の健康診断のように、自社のサイバーリスクについて定期的に診断する仕組みと、医療制度のように、万一のインシデント対応を補償するサイバー保険の活用を前提とし、体系的にサービス提供を実現することを検討する。

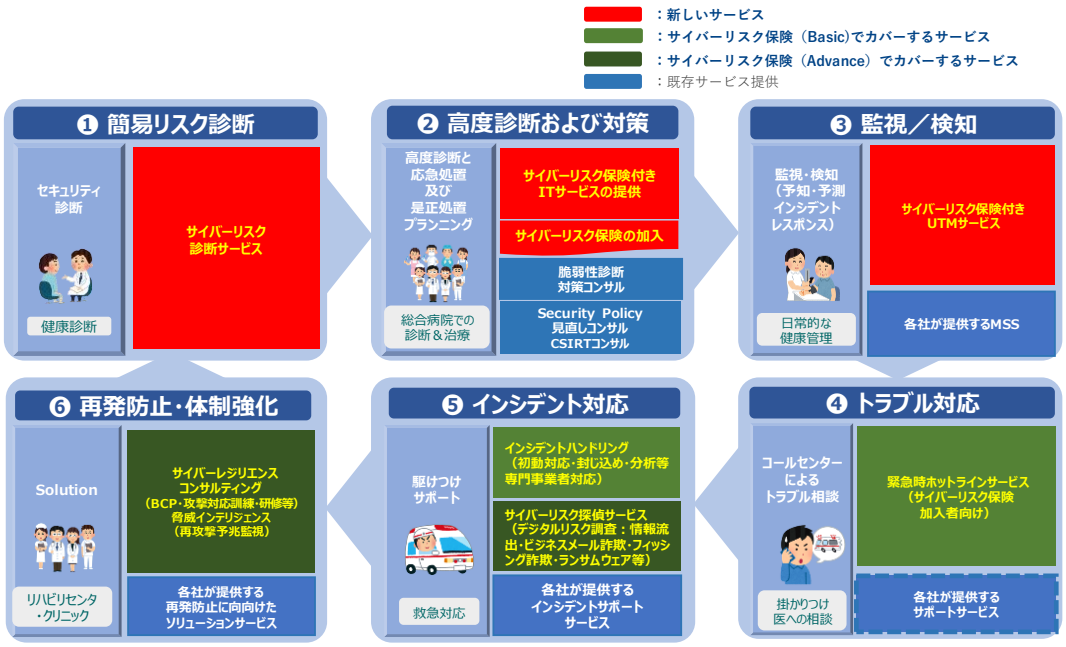


図 75 サイバーエコシステムについて

① 簡易リスク診断（サイバーリスク診断）サービスについて

診断は、企業のセキュリティに関する「組織的施策」、「人的施策」、「物理的施策」、「技術的施策」の実施状況について、体系的に評価できる内容とする。また、外部診断、内部診断といった技術的な診断を加えることでより正確でかつ客観的なリスク診断を行えるようにする。技術診断は最低限実施すべき対策の可否を判断できる内容に絞ったチェックを行うことで、診断コストを低減する。

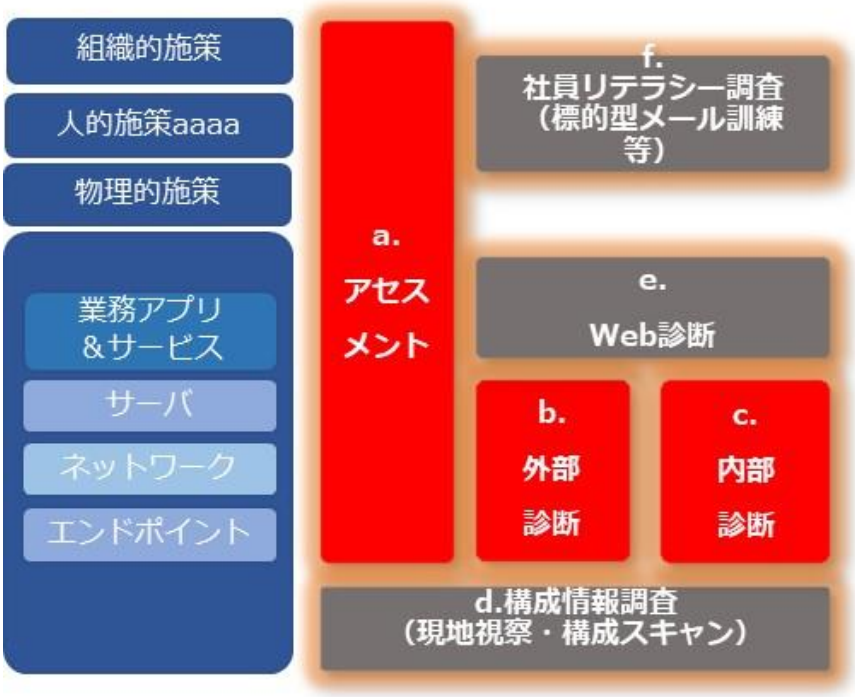


図 76 サイバーリスク診断サービス概要

a. アセスメント

問診内容は「セキュリティマネジメント」および「技術対策」に分けて構成する。特徴として、「Minimum：最低限実施すべき事項」、「Basic: 業界としてここまでは実施しておいてほしい事項」、「Advance：実施が望ましい事項」と 3 段階で準備し、対象企業の成熟度に合わせた設問とする。また、設問には「必須要件」として具体的に実施すべき内容を明確化することで、回答者のスキルによって回答のブレができるだけ少なくなるように考慮する。

b. 外部診断

SecurityScorecard 等の診断ツールを活用することで、技術的な観点での客観的な評価を診断項目に追加する。

c. 内部診断

外部診断で確認できない、サーバー、端末、ネットワーク機器等の社内機器について、脆弱性診断ツールを用いて診断する。また、疑似マルウェアの受信テストを行うことで、マルウェア感染対策の有無についての事実を確認する。

d. 構成情報調査

必要に応じて、企業の IT 環境の構成情報に関して現地調査や診断ツールを用いて調査することで、未管理端末等のシャドーIT の発見や管理体制の不備について実態を把握する。

e. Web 診断

外部診断で分からない、ホームページや業務システムのアプリケーションの脆弱性について診断する。

f. 社員リテラシー調査

企業に所属する社員やパートナー社員の IT リテラシーに関する調査をリテラシーテストや標的型メール訓練等にて把握し、社員のレベルアップに活用する。

ビジネス化に向けて、「a.+b.」を基本サービス、c. d. e. f.をオプションとしたメニューを整理し、自動車産業向けのサービスとして展開を検討する。

また、簡易リスク診断サービスに関する提供価格について検討を実施した。上記基本サービスについて、約 10 万円（年額）程度とする見込みである。なお、本価格はあくまでサービス化に向けた現時点での目安となる。オプションについては、今後サービス要件を含め検討を予定している。

② 高度診断および対策

ア　技術対策について

アセスメント結果から何らかの技術対策が必要とされる場合は、NTT コミュニケーションズまたは NTT グループが提供するセキュリティ関連サービスの提供を行う。今後 NTT コミュニケーションズの提供するサービスは、東京海上日動火災保険のサイバー保険を全件付帯し簡易保険として中小企業サプライヤーが利用しやすいサービスとする。更に大きな補償を要する場合には、本格的リスクの移転としてのサイバー保険の加入の促進を図る。

イ　マネジメント対策について

アセスメント結果からセキュリティマネジメントに関する対策が必要となった場合は、情報セキュリティ基本方針（ポリシー）の見直しや各種規定類の作成、見直しに関する支援サービスを検討する。

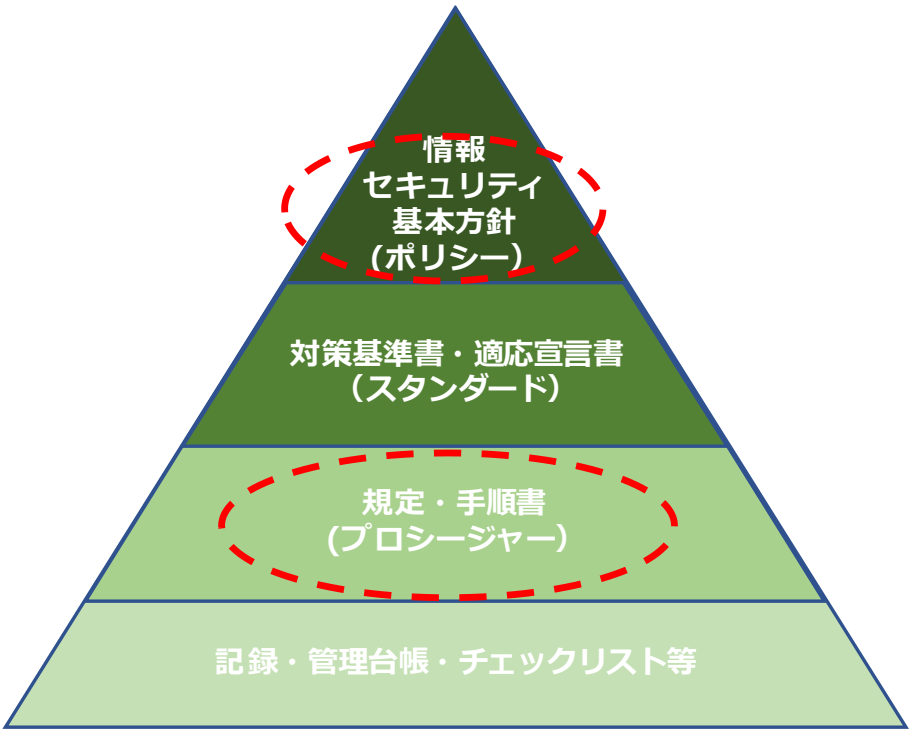


図 77 マネジメント対策支援

＜提供サービス例＞

・情報セキュリティ基本方針（ポリシー）見直し：
罰則規定の見直し CSIRT 規定整理等

・手順書に関する部分的支援（IT 担当教育を含む）：
インシデントフローおよび定義の整理、クラウドサービス利用規定、テレワークに関する規定等

マネジメント対策に関する提供価格について検討を実施した。現時点における提供価格案は以下のとおり。なお、本サービスは個社ごとにサービスレベルが異なると想定されることから価格は目安となる。

Basic：自動車業界向けひな形の提供　数万円～数十万円
または導入コンサルティング　数十万円～
例：インシデントフローおよび定義の整理、クラウドサービス利用規定、テレワーク規定等々の手順書に関する部分的支援

Standard：コンサルティング　数百万円
例：罰則規定の見直し、CSIRT 規定整理等、IT 担当者教育を含む

③ 監視・検知

自動車産業のサプライヤーは企業規模が小さくても ECU 等の重要部品の提供をしている企業もあり、監視・検知において高度なログ分析が必要となる場合もある。よって、UTM のサービスは安価な見守りサービスから高度なログ分析が可能なサービス等、複数のラインナップを検討する。

本分野に関する提供価格について検討を実施した。現時点における提供価格案は、以下のとおり。なお、本価格はあくまでサービス化に向けた現時点での目安となる。

UTM ソリューション

Basic：月額 1~2 万円 （簡易保険を含む）

Standard：月額 5~10 万円 （セキュリティ簡易分析＋簡易保険を含む）

Advanced：月額 10 万円~ （セキュリティ高度分析＋簡易保険を含む）

④ トラブル相談

東京海上日動火災保険のサイバーリスク保険に付帯される「緊急時ホットラインサービス」を有効活用し、中小企業サプライヤーの有事の際の相談ニーズに対応する。

本サービスは、任意加入方式のサイバーリスク保険 （Basic）の加入者に提供することを想定しており、提供保険料水準は、約 5 万円 （年額）を想定している。

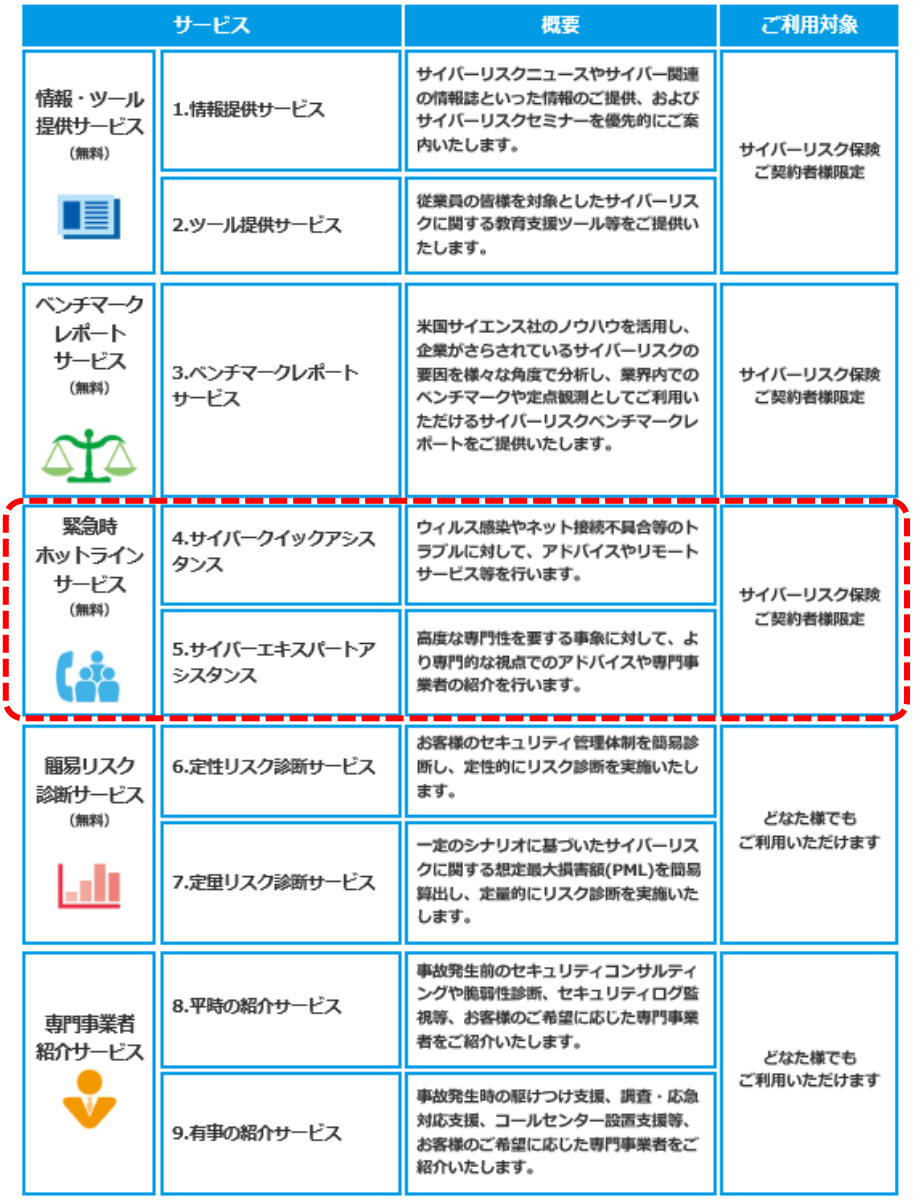


図 78 「緊急時ホットラインサービス」の概要

⑤ インシデント対応

ア　インシデントハンドリング

有事の初動対応やフォレンジック調査等の専門事業者の手配を含めたインシデントハンドリングサービスを検討する。本サービスは、任意加入方式のサイバーリスク保険（Basic）の加入者に提供することを想定しており、提供保険料水準は、約 5 万円（年額）程度を想定している。

イ　サイバーリスク探偵サービス

インシデント発生時の被害調査（情報流出の規模、損害の範囲等）および攻撃者（ビジネスメール詐欺・フィッシング詐欺・ランサムウェア等）の目的や狙いについて調査することで、被害の全貌、再発防止に活用できるサービスを検討する。本サービスは、任意加入方式のサイバーリスク保険（Advance）の加入者に提供することを想定しており、提供保険料水準は、約 15 万円（年額）程度を想定している。

⑥ 再発防止・体制強化

サイバーレジリエンスコンサルティングとして、再発防止に向けた様々な対策（BCP・攻撃対応訓練・研修等）についてアドバイスをするとともに、脅威インテリジェンス（再攻撃予兆監視等）の情報提供を行うサービスを検討する。本サービスは、任意加入方式のサイバーリスク保険（Advance）の加入者に提供することを想定しており、提供保険料水準は、約 15 万円（年額）程度を想定している。

6.2.2 サービスの普及に向けて

(1) 自動車産業における今後の動向

2022 年 7 月に全ての新型車に WP29 の下記要件が適応されるため、OEM メーカー等の自動車産業関係者にとって「サイバーセキュリティ基盤構築」が急務とされている。

① WP29 国際基準概要

自動運転に関する国際基準において、主に「サイバーセキュリティ」と「ソフトウェアアップデート」の法的要件が整備されている。そのことにより、認証当局による OEM メーカーのプロセス認可（体制や仕組みの認可と監査）が初期・3 年ごとに行われることになるため、サプライヤーも含めた全体でのプロセス構築運用が必要となる。

②「サイバーセキュリティ」に求められる要件

ア　CSMS[6]の存在

車両の開発・生産・生産後フェーズ（廃車まで）を含めたライフサイクル全般にわたってセキュリティマネジメント（PDCA）が実施されていること

イ　型式証明への対応

車両に対する型式要件の審査への対応として、予備審査で取得したプロセスにしたがって車両のセキュリティ設計と評価結果を審査する。3 年ごとに外部審査による OEM メーカーの CSMS を認定し、認証を受けたプロセスを適用して開発されたことを詳細技術ファイルにより説明する。

---

[6] Cybersecurity Management System の略称。産業用オートメーションおよび制御システムに対するセキュリティマネジメントに関する国際標準。

⑵ サービス普及に繋がる環境変化

① 部品調達仕様書の条件

今後、OEM メーカーは WP29 への対応のため、各サプライヤーに対し調達仕様にサイバーセキュリティ対策に関する要件を追加することが想定される。サプライヤーは OEM メーカーとの取引を継続するためにはサイバーセキュリティ対策要件を満たすことが必須となる。また OEM メーカーの CSMS 要件は、Tier1 から Tier2 へ、Tier2 から Tier3 へと要求され、最終的には中小企業のサプライヤーも含めて多くのサプライヤーが CSMS 要件を満たす必要がある。

② OEM メーカー各社の状況

現在、OEM メーカーの調達仕様における CSMS 要件は OEM メーカー個別に検討している状況となっている。

③ 業界標準化に向けて

CSMS 要件は基本的な部分では同様であるため、自動車産業全体でサプライヤー認定に関する規定を整備していくことが求められている。

OEM メーカーの求めるサイバーセキュリティ対策の具体的な要件を満足できるレベルにあるかどうかについては、サイバーリスク診断の内容を自動車産業における CSMS への対応要件に適応していくことで標準化を図り、自動車産業へ広く普及させることを検討中である。結果として中小企業のセキュリティ対策レベルの向上を図る。

⑶ サービス普及に向けた取組み

① OEM メーカー各社のサプライヤーマネジメントへの活用

ア　実証参加企業が所属する団体・組合等への展開

今回の実証事業を通じて、静岡エリア・広島エリアの OEM メーカーにおける課題とニーズを把握することができたので、具体的なサービスの提供を開始できるよう継続的に提案活動を行う。

イ　OEM メーカー各社への展開

OEM メーカー各社の WP29 への対応およびサプライヤーマネジメントの実状を把握した上で、同様のサービスの展開が可能かを引き続き検討する。

② 自動車産業への展開

2021 年 4 月に J-Auto-ISAC が一般社団法人化され、自動車産業のサプライヤーの会員としての参加が可能となる。会員サービスの一つとして、自社のサイバーリスク診断サービスの提供を検討する。

⑷ ビジネス化に向けた課題について

中小企業サプライヤーへ本サービスを普及拡大させるための今後の課題について整理する。

① サービスメニューの整備

自動車産業のサプライチェーンマネジメントのニーズを継続的に把握するとともに、提供サービスメニューについてサイバー保険のセットを前提に整備する。

② デリバリー体制の構築

日本全国の中小企業へ展開できるデリバリー体制として、地域の SI 企業や NTT グループ全体での体制を整備する。

③ 導入事例の拡大

実証事業の継続としての導入事例を増やすとともに、実用性の高い事例をできるだけ多く作る。

④ 新たな市場拡大

自動車産業以外のマーケットにも横展開することで、新た市場の開拓余地の可能性を模索する。

⑤ 提供サービスおよびデリバリー体制の見直し

業界の動向やニーズにしっかり適合をするために、サービスの見直し、適正価格に向けたデリバリー体制見直しを継続的に実施する。

以 上