2025 年 4 月 7 日

レポート

中堅・中小企業のセキュリティ対策の進め方

～セキュリティ診断のススメ～

コンサルティング事業本部
デジタルイノベーションビジネスユニット 業務 IT コンサルティング部
コンサルタント　庄田　智祐

1. はじめに

国立研究開発法人情報通信研究機構の「NICTER 観測レポート 2024[1]」によると、2015 年から 2024 年の 10 年間において、年間総観測パケット数は増加傾向にあると報告されている（【図表 1】）。年間総観測パケット数とは、インターネット上のスキャン活動（ネットワークデバイスの脆弱性などを検知する行為）の活発さを計測する指標であり、年間総観測パケット数の増加は、サイバー攻撃などのセキュリティリスクの増加とも推測できる。

このように、セキュリティリスクが年々増加している状況下では、企業は自社の情報資産を守るために、効果的なセキュリティ対策を講じる必要がある。

【図表 1】年間総観測パケット数の統計（2015 年～2024 年）

年	年間総観測パケット数	観測 IP アドレス数	1 IP アドレスあたりの年間総観測パケット数
2015	約 631.6 億	270,973	245,540
2016	約 1,440 億	274,872	527,888
2017	約 1,559 億	253,086	578,750
2018	約 2,169 億	273,292	806,877
2019	約 3,756 億	309,769	1,231,331
2020	約 5,705 億	307,985	1,849,817
2021	約 5,180 億	289,946	1,747,685
2022	約 5,226 億	288,042	1,833,012
2023	約 6,197 億	289,686	2,260,132
2024	約 6,862 億	284,445	2,427,977

（出所）国立研究開発法人　情報通信研究機構「NICTER 観測レポート 2024」

[1]国立研究開発法人 情報通信研究機構「NITCTER 観測レポート 2024」（2025 年 2 月 13 日）
https://www.nict.go.jp/press/2025/02/13-1.html（最終確認日：2025/03/14）

セキュリティ対策は、まず自社に求められるセキュリティレベルと、現状のセキュリティ対策のギャップを分析するところから始まる。これがいわゆる、セキュリティ診断である。セキュリティ診断により、企業は自社の情報システムやネットワークなどに存在する、セキュリティ上の脆弱性を明らかにし、それらが引き起こす潜在的なリスクを適切に評価できる。

しかし、セキュリティ診断の手法はまだ一般的に浸透しておらず、全ての企業が独力で実施できるわけではない。特に、セキュリティに知見のある社員が不足しがちな中堅・中小企業では、独力でのセキュリティ診断が困難である。そのため、本レポートでは、セキュリティ対策の第一歩となるセキュリティ診断の流れについて紹介し、中堅・中小企業のセキュリティレベルの向上に寄与したい。

2. セキュリティ診断の概要

セキュリティ診断では、「物理的脆弱性の診断」、「技術的脆弱性の診断」、「人的脆弱性の診断」の 3 種類の診断を行う。1 つでも脆弱性が存在すると、それをきっかけにセキュリティリスクが顕在化する恐れがあるため、全てのセキュリティ診断を漏れなく行う必要がある。以下(【図表 2】)に、各診断の概要を示す。

【図表 2】セキュリティ診断の種別と概要

#	診断種別	診断の概要
1	物理的脆弱性	企業の物理的施設や設備のセキュリティ対策状況を評価する。例えば、監視カメラの設置状況や、機密エリア(サーバールームや役員室など)の施錠管理状況などを評価する。
2	技術的脆弱性	企業のシステムやアプリケーション、ネットワークなどのセキュリティ対策状況を評価する。例えば、ファイアウォールの設定や、アプリケーションへのセキュリティ対策パッチの適用状況などを評価する。
3	人的脆弱性	企業のセキュリティ関連規定の整備状況や、セキュリティ対策に関わる手順の適切性を評価する。例えば、セキュリティポリシーやインシデント対応フローの整備状況などを評価する。

(出所) 当社作成

3. セキュリティ診断の流れ

セキュリティ診断は、「事前準備」、「リスク評価」、「課題設定と対策検討」、「実行計画の策定」の 4 つのステップから構成される。以下(【図表 3】)に、各ステップの概要を示す。

【図表 3】セキュリティ診断の 4 つのステップ

(出所) 当社作成

(1) 事前準備

セキュリティ診断の最初のステップでは、セキュリティ診断の目的と対象範囲を明確にする。目的や対象範囲が不明確なまま進行すると、場当たり的な評価となり、組織全体の網羅的なセキュリティ診断ができない可能性がある。そのため、始めに目的と対象範囲を明確にすることが肝要である。

次に、セキュリティ診断のプロジェクトチームを立ち上げる。プロジェクトチームは情報システム部門のみならず、現場部門の社員も組み入れることを推奨する。現場部門の社員を含めることで、実務に即したセキュリティ診断へとつながる。さらに、経営層がプロジェクトチームに参画することも重要である。経営層がリーダーシップを発揮することで、セキュリティ対策が組織全体の取り組みとして認識され、全社員一丸となってセキュリティ対策に臨める。

続いて、セキュリティ診断を効率的かつ一貫性をもって行うために、ガイドラインとチェックシートを準備する。ガイドラインはさまざまなものがあるが、ここでは「自動車産業サイバーセキュリティガイドライン[2]」の利用を推奨する。当ガイドラインは自動車メーカー向けとして作成されているが、複数のセキュリティ対策フレームワークを基に作成されており、バランスの取れた診断内容となっている。チェックシートについても、ガイドラインに付属の「自動車産業セキュリティチェックシート(【図表 4】)[3]」の利用を推奨する。なお、ガイドラインやチェックシートは不定期に更新されるため、利用前に最新版であるか確認が必要となる。

【図表 4】自動車産業セキュリティチェックシートの一部抜粋

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
1方針	会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる	自社の情報セキュリティ対応方針を策定し自組織内に周知していること	1	Lv1	自社の情報セキュリティ対応方針(ポリシー)を策定している	・自社の情報セキュリティ対応方針を策定し、文書化すること
			2	Lv2	自社の情報セキュリティ対応方針(ポリシー)の内容を確認し、必要に応じて見直ししている	【規則】 ・社内外の環境変化を踏まえて、内容を確認し、適宜見直ししていること 【頻度】 ・情報セキュリティ対応方針(ポリシー)の内容を確認、改善 -1回以上/年 ※別途、重大な変化が発生した場合には迅速に対応すること
			3	Lv1	情報セキュリティ対応方針(ポリシー)を社内に周知している	【規則】 ・情報セキュリティ対応方針(ポリシー)を容易に確認できる状態にすること 【対象】 ・役員、従業員、社外要員(派遣社員等) 【頻度】 ・定常的に、かつ、情報セキュリティ対応方針の改正時に周知すること

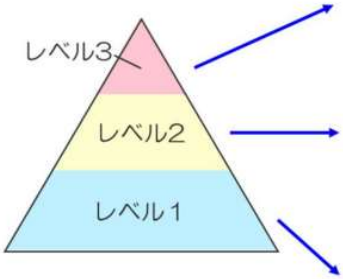
(出所)一般社団法人 日本自動車工業会「自工会/部工会・サイバーセキュリティガイドライン V2.2」

[2]一般社団法人 日本自動車工業会「自工会/部工会・サイバーセキュリティガイドライン 自動車産業におけるサイバーセキュリティ対策の一層の進展のために V2.2」(2024年8月1日)
https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_02.pdf(最終確認日:2025/03/14)
[3]一般社団法人 日本自動車工業会「自動車産業セキュリティチェックシート V2.2」
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html(最終確認日:2025/03/14)

(2) リスク評価

2 つ目のステップでは、ガイドラインに基づき目標とするセキュリティレベルを定める。ガイドラインは自動車業界を基準に定義されているため、自社が所属する業界に読み替えてセキュリティレベルを定義する(【図表 5】)。

【図表 5】自動車産業サイバーセキュリティガイドラインのセキュリティレベル定義



レベル	定義	各レベルの達成を目指すべき会社
Lv3	現時点*で自動車業界が到達点として目指すべき項目 *2022年4月	・会社規模・技術レベルの観点で自動車業界を代表し牽引すべき立場の会社またはそれを目指す会社 ◆Lv1～3の全項目を達成
Lv2	自動車業界として標準的に目指すべき項目	以下のいづれかに該当する会社 ・サプライチェーンにおいて社外の機密情報（技術・顧客情報等）を取り扱う会社 ・自動車業界として重要な自社技術／情報を有する会社 ・相応の規模／シェアを有し、不慮の供給停止等により業界のサプライチェーンに多大な影響を及ぼし得る会社 ◆Lv1,2の全項目を達成
Lv1	自動車業界として最低限、実装すべき項目	・自動車業界に関係する全ての会社 ◆Lv1の全項目を達成

(出所)一般社団法人　日本自動車工業会「自工会/部工会・サイバーセキュリティガイドライン V2.2」

「自動車産業セキュリティチェックシート」では、セキュリティレベルを選択すると自動的に診断項目が設定されるため、診断項目ごとに担当者を割り当てる。その後、各診断項目の目的、要求事項、達成条件、達成基準を担当者が理解し、それらを基に、自社のセキュリティ対策が適切かどうかを「該当なし」、「未実施」、「対応中」、「対応完了」の 4 段階で評価する。書類を基に評価可能なものは机上で評価し、必要に応じて現場部門にヒアリングを行う。

その後、担当者が評価した結果を基に議論を行い、プロジェクトチームとしての評価を行う。この際に大事なことは、単に評価結果を確認することではなく、評価根拠を確認することである。診断項目ごとに適切な評価が行われているのか、プロジェクトチームメンバーとのディスカッションを通じて、全て確認する。また、拠点やシステムを複数保有する企業は、全ての拠点やシステムで達成条件を満たしているかを確認する必要がある。

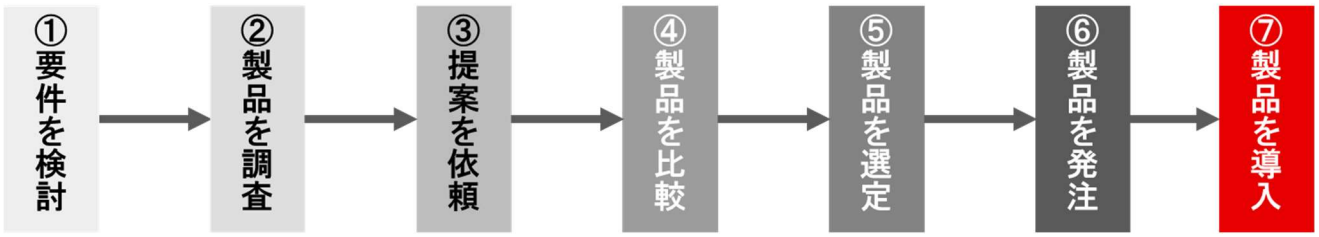
例えば、“インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限している”という達成条件の場合、1 つでもファイアウォールが設置されていない拠点があると、対策不十分と判断され、「対策完了」とはならない。なお、「物理的脆弱性」と「人的脆弱性」は、自社の担当者だけで判断可能な内容も多く含まれているが、「技術的脆弱性」は自社の担当者だけでは判断できない場合がある。そのような場合は、システムの保守を担当しているベンダーへ問い合わせることを推奨する。

(3) 課題設定と対策検討

3 つ目のステップでは、評価結果が「未実施」または「対応中」の診断項目について、課題と対応策を検討する。課題は、原則的に達成条件または達成基準の裏返しになる。例えば、「インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限している」という達成基準であれば、課題は「インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限する」となる。あるいは、「自社のセキュリティ対応方針(ポリシー)を策定している」という達成基準であれば、課題は「自社のセキュリティ対応方針(ポリシー)を策定する」となる。

しかし、課題設定しただけでは、どのようなプロセスを経て課題を達成するのか分からないため、設定した課題を基に、具体的な対応プロセスを検討する。以下(【図表 6】)は、「インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限する」という課題の対策プロセスの例である。

【図表 6】課題の対策プロセス例



(出所) 当社作成

上記の課題の対策プロセスは、以下(【図表 7】)の 5 つのステップで検討する。

【図表 7】課題の対策プロセス検討に関わる 5 つのステップ

(出所) 当社作成

上図の通り、最初に達成基準を満たしていない事項を抽出し、リスト化する。次に、リスト化した未達事項を細かく分解し、具体的なタスクに落とし込む。例えば、「ファイアウォールの設置」を、「製品を調査」、「製品を発注」、「製品を導入」などのタスクに分解する。これにより、具体的な作業が明確になり、実行可能な単位に分けることができる。

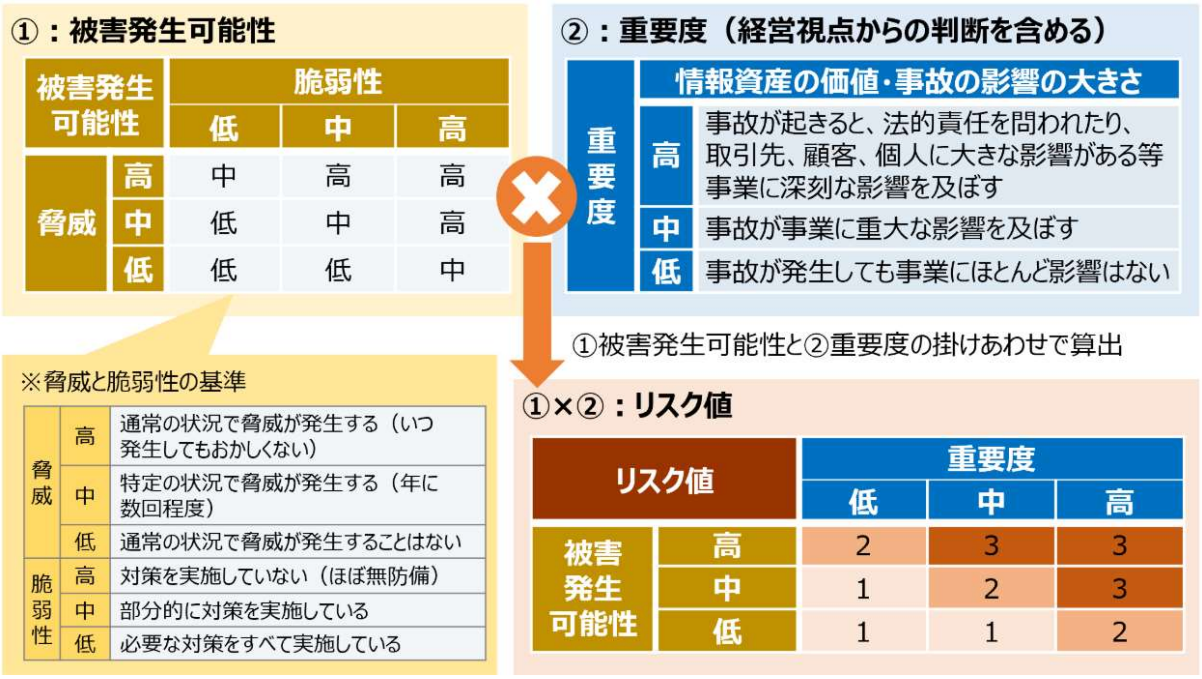
続いて、各タスクの前後関係を検討し、どのタスクが他のタスクに依存しているかを明確にする。これにより、タスクの実行順序が決定する。その後、前後関係を考慮して、タスクを時系列に並べる。これにより、一連のプロセスを把握することができる。

最後に、プロセスの所要期間を見積もる。もしプロセスの所要期間がうまく見積もりできない場合は、タスクの粒度が粗過ぎる可能性がある。そのため、タスクをより細かく分解してから再度見積もりを行うことを推奨する。

(4) 実行計画の策定

最後のステップでは、課題ごとの優先度を「高」、「中」、「低」の 3 段階で設定し、優先度に応じた実行計画を策定する。優先度は、「被害発生可能性」と「重要度」を掛け合わせて算出したリスク値を基に設定する。課題ごとの優先度を決めずに実行計画を策定すると、優先度の考慮がなされていない計画が出来上がるため、必ず実行計画の策定前に、リスク値を基に優先度を決める必要がある。リスク値の算出方法は、情報処理推進機構（以下、IPA）のプラクティス・ナビで紹介されている、被害発生可能性と重要度からリスク値を判定する方法の例（【図表 8】）[4] が参考となる。

【図表 8】被害発生可能性と重要度からリスク値を判定する方法の例



（出所） 独立行政法人 情報処理推進機構「プラクティス 4-1 経営への重要度や脅威の可能性を踏まえたサイバーセキュリティリスクの把握と対応」

セキュリティ対策は数年がかりになることもあるため、実行計画は全体の概略スケジュールを立てた上で、年単位にスケジュールを落とし込む。そして、年単位のスケジュールをさらに四半期単位、あるいは月次単位で具体化することにより、進捗が管理しやすくなる（【図表 9】）。

[4] 独立行政法人 情報処理推進機構「プラクティス 4-1 経営への重要度や脅威の可能性を踏まえたサイバーセキュリティリスクの把握と対応」https://www.ipa.go.jp/security/economics/practice/practices/Practice211/（最終確認日：2025/03/14）

【図表 9】実行計画のスケジュールの粒度

（出所） 当社作成

また、スケジュールだけではなく、セキュリティ製品の導入費用についても検討する必要がある。ベンダーの公式ホームページに、セキュリティ製品の費用が掲載されている場合もあるが、導入の前提条件により費用が異なるため、導入製品ごとにベンダーへ見積もり依頼すべきである。さらに、ベンダーごとに対応範囲や費用が異なるため、できるだけ複数のベンダーへ見積もり依頼をし、各ベンダーのメリットとデメリットを比較することを推奨する。

スケジュールと費用の検討完了後は、検討内容を実行計画へ反映し、実行計画について経営層の承認を得る。その後は、実行計画通りにサイバーセキュリティ対策を推進する。以上が、セキュリティ診断の一連の流れである。

4. おわりに

サイバー攻撃などのセキュリティリスクが年々増加する一方で、多くの中小企業では、十分なセキュリティ対策ができていないのが現状である。そのことは、IPA のセキュリティ対策状況の調査結果[5]にも表れている。IPA は、令和 4 年度に企業のセキュリティ対策状況を確認するため、43 社に合計 49 問のアンケートを実施した（【図表 10】）。

【図表 10】セキュリティ対策状況確認用のアンケート分類と設問数

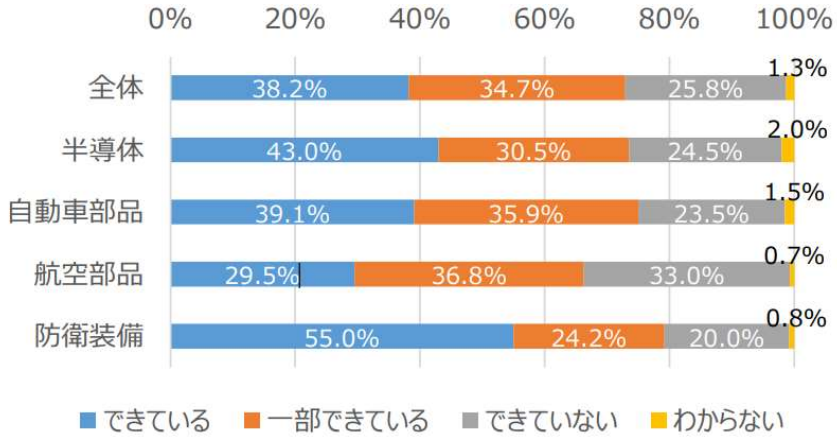
分類	① 経営層の リスク認識や 関与の度合い	② 情報 セキュリティ 運用・管理	③ 情報 セキュリティ 技術的対策	④ 情報 セキュリティ 物理的対策	⑤ リモート アクセスの 活用状況	その他 対策要請有無 被害経験有無
設問数	5	16	12	7	7	2

（出所） 独立行政法人 情報処理推進機構
「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」

全アンケート項目（⑤リモートアクセスの活用状況を除く）の回答結果は下図（【図表 11】）の通りであるが、セキュリティ対策が「できている」と回答した企業は、全体の 38.2%にとどまる。

[5] 独立行政法人 情報処理推進機構「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）
https://www.ipa.go.jp/security/reports/sme/ps6vr7000001b5t7-att/Kougeki-jittai-houkoku2023.pdf（最終確認日：2025/03/14）

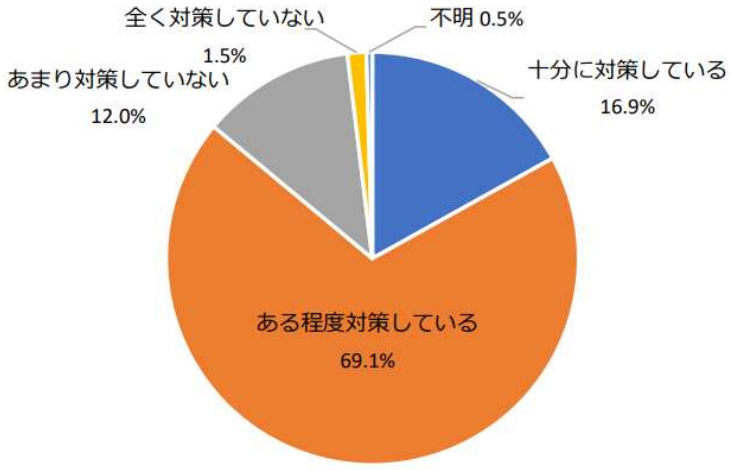
【図表 11】セキュリティ対策状況確認のアンケート結果(「全ての項目」に対する回答結果)[6]



(出所) 独立行政法人 情報処理推進機構「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」

また、東京商工会議所が実施した調査結果[7]にも、多くの中小企業でセキュリティ対策が不十分であることが表れている。サイバーセキュリティ対策の状況(【図表 12】)は、「ある程度対策している」と回答した企業が最も多いが、「ウイルス対策ソフトのインストール」や、「OS/ソフトウェアの定期的なアップデート」などの初歩的な対策にとどまる企業が多数を占め、「社内教育、研修の実施」や「セキュリティ診断の実施」など、人材育成や専門的な対策を実施している企業は 3 割未満にとどまる(【図表 13】)。

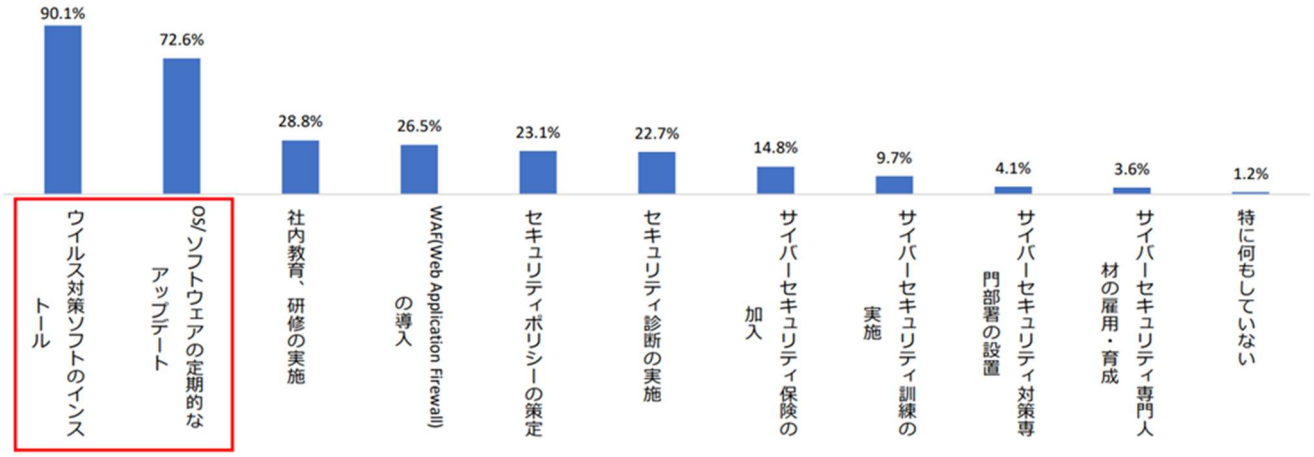
【図表 12】サイバーセキュリティ対策の状況



(出所) 東京商工会議所 中小企業のデジタルシフト・DX 推進委員会
「中小企業のデジタルシフト・DX 実態調査集計結果」

[6]【図表 11】の"全体"は「半導体」、「自動車部品」、「航空部品」の 3 分野の中小企業、および防衛装備庁の紹介企業(「防衛装備」と記す)を加えた 43 社を指す。
[7] 東京商工会議所 中小企業のデジタルシフト・DX 推進委員会「中小企業のデジタルシフト・DX 実態調査集計結果」(2023 年 7 月 12 日)https://www.tokyo-cci.or.jp/file.jsp?id=1200374(最終確認日:2025/03/14)

【図表 13】サイバーセキュリティ対策の内容



（出所） 東京商工会議所 中小企業のデジタルシフト・DX 推進委員会
「中小企業のデジタルシフト・DX 実態調査集計結果」

上記 2 つの調査結果から、多くの中小企業では、十分なセキュリティ対策が実施できていないことがうかがえる。中には、何から手を付けてよいのか全く分からないという企業も少なくない。そのような企業にこそ、自社に求められるセキュリティレベルと、現状のセキュリティ対策のギャップについて、セキュリティ診断を通じて分析を行い、セキュリティ対策の第一歩を踏み出すことを推奨する。

【関連サービス】

サイバーセキュリティ

【関連レポート・コラム】

中堅・中小企業の情報セキュリティマネジメントの現状と今後の展望