企業規模・業種別に見るセキュリティ投資・人員数の目安値
～DX with Security を実現するために必要なリソース水準とは～

【要旨】

(1) DX の進展、脅威の深刻化・複雑化により、サイバーセキュリティの必要性は明らかに高まっているにもかかわらず、多くの企業でセキュリティ投資や人員といったセキュリティリソースの確保が進んでいない。その原因の 1 つは、投資や人員数の妥当性を測る指標が存在しないことではないか。

(2) 本レポートでは、この課題を解決するため、日本で初めて企業規模・業種別の「セキュリティ投資額および人員数の目安値」を提示する。さらに、その目安値を用いて、セキュリティ責任者と経営層が対話し、適切な投資判断と中長期的なセキュリティリソースを確保するための提言を取りまとめた。なお、本レポートで用いる「目安値」とは、法令や関連ガイドラインへの準拠、現行リスクへの対応が実施されていることを前提としつつ、DX を推進する企業が今後直面する可能性のある新たなリスクも見据えて設定する、実行可能で現実的な水準を指す。

#	企業の類型		セキュリティ投資額/売上高の目安値	セキュリティ人員数/全従業員数の目安値
	企業規模	業種		
1	大企業（売上高1000億円~）	金融	売上高の 0.6%	全従業員の 0.8%
2		IT・情報通信	0.5%	0.6%
3		社会インフラ	0.3%	0.3%
4		製造	0.2%	0.2%
5		小売・サービス・その他	0.1%	0.2%
6	中堅企業（売上高100億円~1000億円）		0.3%	0.2%

図 1 セキュリティリソースの目安値概要

【セキュリティ責任者向け提言】

- **提言 1 ：目安値を使って、現在地を経営層に示せ**
- **提言 2 ：目安値を使って、目的地を経営層に示し必要なセキュリティリソースを確保せよ**

【経営層向け提言】

- **提言 1 ：目安値を使って、現在地を把握せよ**
- **提言 2 ：目安値を使って、目的地達成のためのセキュリティリソース確保にコミットせよ**

(3) 重要なのは、目安値を単なる参考値として軽視する、逆に絶対値として神聖視することではなく、自社の現在地と将来必要な水準を客観的に示すための経営層との「共通言語」として徹底的に活用することである。目安値を使うことで、これまで説明困難だったセキュリティリソースの妥当性を明確にし、中長期的なリソース確保と計画的なセキュリティ強化に向けた意思決定を強力に後押しできる。企業には、目安値を積極的に活用し、自社のセキュリティ成熟度を着実に引き上げていくことを強く期待したい。

目次

本レポート刊行にあたって

JCIC では、2022 年 3 月に「社内のセキュリティリソースは『0.5%以上』を確保せよ」（以下、前回レポート）を発刊し、企業が「DX with Security 戦略」を策定するうえで必要となるアプローチとして、以下 3 点を提言しました[1]。

① サイバーリスク数値化モデルによるリスクの可視化
② DX with Security 戦略の策定
③ セキュリティ KPI の設定と定期的なモニタリング

特に②の提言では、DX の実現に向けて解決すべきセキュリティ課題とその対策が生み出す効果を「ストーリー」として説明する重要性を示すとともに、中長期的なリソース計画の必要性を指摘しました。そのリソースの目安値として、

- セキュリティ投資額は、連結売上高の 0.5%以上を投資すべきである
- セキュリティ人材は、全従業員数の 0.5%以上を確保すべきである

を提示したところ、多くの企業で経営層への説明に活用されたほか、日本経済新聞や日経クロステックなど多数の媒体で取り上げられ、大きな反響をいただきました[2]。一方で、前回は金融機関のデータを中心に算出した一律の値であったことから、「企業規模・業種別でより実態に即した指標を示して欲しい」というご意見も多く寄せられました。

さらに前回発刊以降、企業を取り巻く環境は劇的に変化しています。DX の進展とともに企業が守るべき範囲が従来の境界を超えて大きく広がったことで、大規模な情報漏えいや、サプライチェーンを起因とした攻撃などセキュリティリスクも高まっています。また、地政学リスクの高まりにより、国家レベルのサイバー攻撃も活発化し、企業が直面するリスクの深刻化も進んでいます。

本レポートでは、前回レポートの反響と、こうした環境変化を踏まえ、企業規模・業種別の観点から、より実態に沿ったセキュリティ投資額および人員数の指標を示すことを目指しました。加えて、CISO やセキュリティ部門長へのインタビューを通じて、投資確保の工夫、経営層への説明方法、人材不足への対応といった現場の実情をヒアリングしました。これらのリアルな声は、企業の皆様がセキュリティに取り組むにあたり、示唆に富んだ内容となっており、ぜひ参考にしていただきたいと考えています。

---

[1] JCIC「社内のセキュリティリソースは『0.5%以上』を確保せよ」（2022 年 3 月），
https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf

[2] 日本経済新聞朝刊「転ばぬ先の『サイバー査定』 情報漏洩のリスク軽減」（2023 年 4 月），
https://www.nikkei.com/article/DGXZQOUC287ZB0Y3A220C2000000/;
日経クロステック「サイバー攻撃による『損失額』を見積もる、セキュリティー投資を引き出す材料に」（2024 年 11 月），
https://xtech.nikkei.com/atcl/nxt/column/18/03009/111900001/

本レポートを執筆している最中にも、日本国内で国民生活に影響を及ぼす大規模なセキュリティインシデントが発生しました。セキュリティは、もはや特定の企業や業種に限られたテーマではなく、産業界全体、さらには社会全体で取り組むべき課題へと発展しています。本レポートが、企業が自社の状況を客観的に捉え、セキュリティ責任者と経営層の双方にとって対話を深める契機となり、DX with Security 実現の一助となれば幸いです。

最後に、本レポートの執筆にあたり、貴重なお時間を割き、現場の実情や率直なご意見をお寄せくださった企業の皆さまに、心より御礼申し上げます（企業名・個人名はご意向により割愛しております）。セキュリティは性質上外部に共有しづらいにもかかわらず、快くご協力いただいたことで、皆さまから伺った生の声が本レポートを形づくる大きな力となりました。重ねて感謝申し上げます。

2026 年 2 月

一般社団法人 日本サイバーセキュリティ・イノベーション委員会（JCIC）

執筆者 一同

1. 本レポート執筆の背景と本レポートの目的

本章では、DX の進展や脅威の深刻化・複雑化といった、企業を取り巻く環境の変化を整理する。その上で、セキュリティの必要性が高まる中でセキュリティ投資や人員の確保が進まない要因を分析し、本レポートで提示するセキュリティリソースの目安値がなぜ必要なのかを示す。

1.1 環境の変化①：DX の進展とセキュリティリスクの高まり

前回レポートを発表した 2022 年以降、企業の DX は着実に進展している[3]。クラウドシフトの加速や IT/OT 融合の進展に加え、近年は生成 AI の活用も多様な業務領域で拡大しており、DX の強力な推進力となっている。

また、その変化は生活者の行動様式にも波及している。セルフレジでの QR コード決済、スマートフォンによるタクシー配車、飲食店でのモバイルオーダー、行政手続きのオンライン化など、日常生活のあらゆる場面でデジタルサービスがなくてはならない基盤となりつつある。

経済産業省が「2025 年の崖」として警鐘を鳴らしたように、このような状況下で DX に取り組まないことは、競争力や市場機会の喪失に直結する[4]。DX はもはや「取り組むかどうか」を判断する局面ではなく、企業にとって不可避であり、必須の取り組みとなっている。

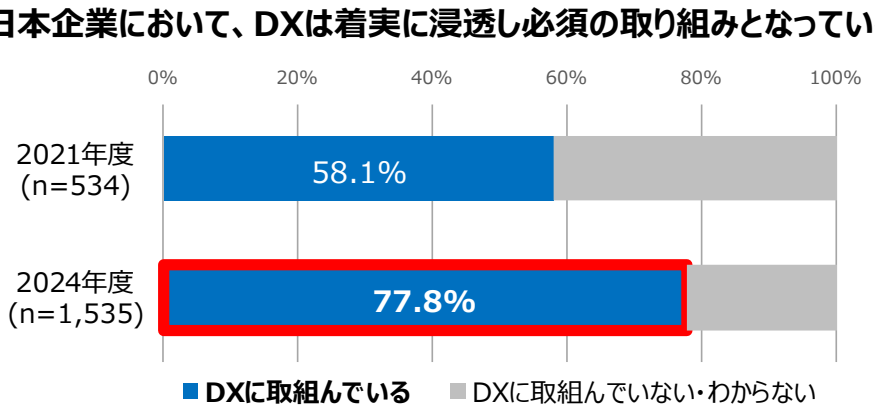


図 2 日本企業における DX 取り組み状況の変化
（IPA「DX 動向 2024/2025」をもとに作成）

一方で、DX の進展に伴い、サイバー空間におけるリスクも増大している。あらゆる機器がネットワークを介して繋がったことで、アタックサーフェスが増加し、従来の境界型防御では十分に対応できない状況となった。さらに企業のデータはクラウドや外部サービスなどに分散して管理されるようになり、情報漏えいや不正アクセスのリスクが高まっている。加えて、取引先や業務委託先などとのシステム連携・データ連携が急速に拡大したことで、それらを経由して自社システムが侵害され被害が連鎖的に拡大する、サプライチェーンを起因としたサイバー攻撃事例が多発している。

---

[3] IPA「DX 動向 2024」（2024 年 6 月）, https://www.ipa.go.jp/digital/chousa/dx-trend/eid2eo0000002cs5-att/dx-trend-2024.pdf; IPA「DX 動向 2025」（2025 年 7 月）, https://www.ipa.go.jp/digital/chousa/dx-trend/tbl5kb0000001mn2-att/dx-trend-2025.pdf

[4] 経済産業省「DX レポート ～IT システム「2025 年の崖」の克服と DX の本格的な展開～」において、DX のために必要な、既存システムのブラックボックス状態の解消や、全社横断的なデータ活用ができない場合、「2025 年以降、最大 12 兆円/年の経済損失が生じる可能性がある」と述べられている。https://www.meti.go.jp/policy/it_policy/dx/20180907_01.pdf

1.2　環境の変化②：地政学リスクと AI の関わりによる脅威の深刻化・複雑化

企業を取り巻く脅威環境も、ここ数年でかつてない速度で深刻化・複雑化している。特に近年顕著なのは、国家支援型の高度標的型攻撃（APT）が質的に次元の異なるレベルへ進化している点である。地政学的緊張の高まりを背景に、国家が支援する犯罪グループは資金力・技術力・持久力を活かしたサイバー作戦を強化しており、日本においても幅広い企業が標的となっている[5]。

さらに、生成 AI の進展も攻撃の巧妙化と高速化を著しく押し上げている。生成 AI は前述のとおり DX の強力な促進力になっている一方で、攻撃者側の能力を向上させるという負の側面もある。具体的には生成 AI は、攻撃者に以下の能力を与えている：

- 脆弱性情報をもとに攻撃コードを即時生成し、悪用までのリードタイムを劇的に短縮
- サイバー攻撃の自動化により、短時間で多数の標的へ同時侵入を試みることが可能に
- 自然で高度な日本語の文面を短時間で生成し、標的の役職・業務文脈に合わせて精密にパーソナライズしたフィッシングメールを作成

スピード・量・質が飛躍的に高まった攻撃を前に、もはや場当たり的なセキュリティ対策では太刀打ちできないと言わざるを得ない。

さらに、こうした脅威の増大を受け、経済安全保障・国家安全保障や企業保護の観点から、各国ではセキュリティ関連の法規制が急速に強化されている。企業は、規制に迅速に対応しなければならないだけではなく、対応を怠れば、巨額の制裁金、行政処分、事業停止、さらには信用の失墜といった事態に陥ることになる。

[5] 2024 年度には、国家が関与するとみられる重大インシデントが日本国内で相次ぎ、NISC（現 NCO：国家サイバー統括室）および警察庁が MirrorFace（中国関連）、TraderTraitor（北朝鮮）、APT40（中国）など、国家支援型攻撃グループによる活動への注意喚起を発出している。また、IPA「情報セキュリティ 10 大脅威 2025」（2025 年 1 月 30 日公表）において、「地政学的リスクに起因するサイバー攻撃」が初めて選出（7 位）されたことからも、国家レベルの脅威が一般企業にも直接影響する段階に入ったことが伺える。
https://www.ipa.go.jp/security/10threats/10threats2025.html

1.3　セキュリティの必要性の高まりと実行のギャップ：何が障壁となっているのか

前述したように、DX の進展、脅威の深刻化・複雑化により、セキュリティの必要性は明らかに高まっており、セキュリティはもはや「やるべきことの一つ」ではなく、「事業継続の前提条件」へと位置づけが変わった。しかしその一方で、多くの企業では必要なセキュリティ投資・人員の確保が依然として進んでいないという実態がある[6]。

多くの日本企業では、セキュリティ投資やセキュリティ人材が不足している

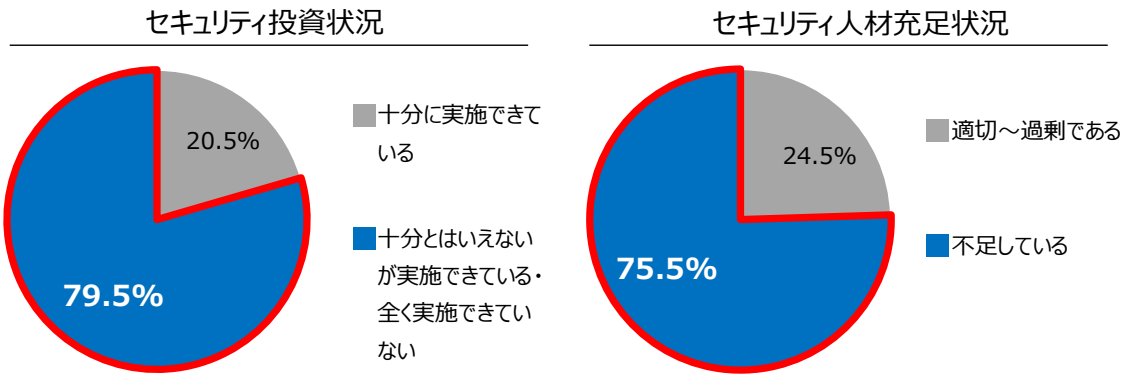


図 3 日本企業におけるセキュリティ投資・人材充足状況
（レバテック株式会社「企業におけるセキュリティ対策の実態調査」，
KPMG「サイバーセキュリティサーベイ 2025」をもとに作成）

なぜ必須であるにもかかわらず進まないのか。その原因の 1 つは、セキュリティ投資や人員数の妥当性を測る指標が存在しないことではないか。これにより、次の 2 つの妥当性を説明・判断できない状態が生じている。

①　現状の妥当性を説明・判断できない

多くの企業では、投資額や人員数が部門ごとに管理され、全社としてセキュリティにどれだけリソースを投じているのかを正確に把握できていない。さらに可視化できていたとしても、指標がないために、必要な対策の積み上げで経営層に必要性を訴える「積み上げ型」の説明にとどまっている。しかしこの方法では、施策単位での必要性は説明できても、経営層が必ず質問する次の問いに対して客観的に説明することができない。

- 今の水準は適切なのか。
- 同業他社と比べて高いのか、低いのか。

経営層が重視するのは個別施策の詳細ではなく「全体としてみた時に、この投資は妥当かどうか」という全体感であり、これがわからなければ投資判断ができない。こうして経営判断は滞り、投資は進まなくなる。

②　将来の妥当性を説明・判断できない

経営層が次に求めるのは、

- 今後、どの水準を目指すべきなのか。
- そのために、どれほどのリソースが必要なのか。

という問いへの説明である。しかし、現状の妥当性と同様、指標がない状態では、中長期計画の妥当性を説明・判断できない。

---

[6] レバテック株式会社「企業におけるセキュリティ対策の実態調査」（2025 年 7 月），
https://levtech.co.jp/research/3733975/; KPMG「サイバーセキュリティサーベイ 2025」（2025 年 4 月），
https://kpmg.com/jp/ja/home/media/press-releases/2025/04/kc-cybersecurity-survey.html

以上のように、指標がないために、現状および将来の妥当性の説明・判断ができない。その結果、経営判断が遅れ、予算は都度承認になり、必要なセキュリティ投資・人員の確保が進まない状況に陥っているのである。

1.4　本レポートの目的

前節で述べたように、JCIC は必要なセキュリティ投資や人員といったセキュリティリソースの確保が進まない原因は、指標が欠けていることにあると考えた。本レポートは、この課題を解消するため、企業が経営判断に活用できる実務的な指標（以下、目安値）を提示することを目的に作成した。

必要なセキュリティリソースは、企業規模によって大きく異なる。また、業種ごとの事業構造、リスク特性やセキュリティ成熟度がもたらす影響も極めて大きい。そこで本レポートでは、「企業規模×業種」別の目安値を定義した。加えて、CISO・部門長クラスへのインタビューを通じて、数値の裏付けとなる実態、経営層への説明の工夫、人材・組織の課題など、定量データだけでは捉えきれない現場の知見も示している。

1.5　本レポートの対象読者

本レポートの対象読者は、前回レポートと同様に、企業におけるセキュリティ責任者（CISO、セキュリティ部門長など）を主な対象とする。あわせて、取締役・監査役・経営層をはじめ、経営企画、総務、リスク管理、人事、財務、情報システム・DX 推進、広報・IR・サステナビリティ、購買・調達など、組織横断的にマネジメントを担う幅広い層にも読んでいただきたい。

なお、前回レポートでは、「DX with Security 先進企業」を主な対象企業としたが、本レポートは、特定のセキュリティ成熟度の企業に限定したものではなく、またあらゆる企業規模や業種を対象としている。

2. 本レポートの前提

本章では、次章以降で提示する目安値を適切に活用するために、前提となる主要用語の定義、類型の考え方、そして目安値の算出アプローチを示す。

2.1 主要用語の定義

(1) セキュリティ投資

まず、本レポートで用いる「投資」という用語は、会計上の資本的支出（CapEx）に限定されるものではなく、経費（OpEx）を含む広義の概念として用いている。すなわち、セキュリティ対策のために発生する全ての支出を対象とし、それらを将来のリスク低減や事業継続力向上のための「投資」として捉えている。これは、セキュリティを単なるコストではなく、経営資源として位置づけるために意図的にこの表現を用いている。

本レポートでの「セキュリティ投資」は、情報セキュリティおよびサイバーセキュリティ領域における、技術的および組織・人的対策に関する投資全般を対象とする。具体的には以下を含む。

- セキュリティ製品/サービスの導入・運用費
- 人件費（定義は次項を参照）
- 外部委託費
- 教育・訓練費
- リスク管理・ガバナンス活動に関する費用

なお、クラウドサービス・ネットワーク・複合的な機能を持つ機器の利用、ガバナンス活動など、セキュリティ投資を他の投資と明確に切り分けることが難しい場合もある。その場合は、Gartner の分類や NIST CSF などのフレームワークを参照しつつ、自社の実態に合わせた定義を作り、整理するのが望ましい[7]。

また、目安値は売上高比率で示している[8]。これは、既存データの多くが同指標を採用しており、かつ経営層と共通の尺度で議論しやすいという実務上の利点があるためである。一方で、企業によっては IT 投資額を基準とした指標の方が実態に即しているケースもある。実際、インタビューでは「IT 投資額に対するセキュリティ投資比率も参考にしたい」との声が複数寄せられた。そのため、本レポートでは売上高比率に加え、IT 投資額比率も併記している[9]。

(2) セキュリティ人員数

本レポートでの「セキュリティ人員数」は、セキュリティ部門内外を含め、セキュリティ機能を担う社員と外部リソースを合わせた、FTE（Full-Time Equivalent）ベースの実質的なリソース量と定義する。具体的には以下を含む。

- セキュリティの専任担当者
- セキュリティを兼務している担当者
- 外部委託先から割り当てられている人員

---

[7] Gartner「IT Key Metrics Data 2025: IT Security Measures — Framework Definitions」, https://www.gartner.com/en/documents/5966439; NIST Cybersecurity Framework (CSF), https://www.nist.gov/cyberframework

[8] 業種によっては売上高ではなく、経常収益や営業収益など異なる指標が用いられる場合がある。本レポートにおける売上高比率は、各業種において一般的に用いられる代表的な収益指標に読み替えて解釈されたい。

[9] 本レポートでは、実務上の観点から IT 投資額に対するセキュリティ投資比率を記載しているが、セキュリティ投資は必ずしも IT 投資の一部と位置付けられるものではない。インタビューでも、セキュリティ投資は事業リスク対応の一環として捉えるべきという意見があった。経営層は、IT 投資の一部として制限せず、必要なセキュリティ投資を確保することが望ましいと言えよう。

主たる職務や役割としてはセキュリティ機能を担っておらず、本業に加えてセキュリティ知識を活用して業務を遂行する人材（プラス・セキュリティ人材）は対象外とする。

(3) 補足事項

本レポートの目安値は以下の前提を置いている。活用する場合は、以下の 3 点に留意されたい。

① セキュリティ投資には人件費を含む

セキュリティ対策の実行においては、人材の確保・育成が最も重要な要素であり、その費用を除外すると実態を過小評価してしまう。そのため、本レポートにおけるセキュリティ投資は、セキュリティに関する人件費を含む値としている。日本企業では人件費は IT 部門やセキュリティ部門が直接把握できないことが多く、人件費を投資額に含めていないケースも見られる。しかし、人件費を含めて投資額を算出することで、より現実的かつ国際的な水準との比較が可能になる[10]。

② 対象は自社セキュリティに限定し、顧客向け・製品セキュリティに関する投資は含まない

本レポートの対象は自社の事業運営および情報資産の保護を目的としたセキュリティ投資である。顧客向けに提供するセキュリティ機能や、自社製品・サービスに組み込まれる製品セキュリティに関する投資は含めていない。

③ IT・セキュリティ部門が把握し得る範囲を対象とする

本レポートで参照したデータは、主に本社の IT・セキュリティ部門による回答および公開情報をもとに集計している。多くの企業ではセキュリティ投資・人員数の方針策定・決定が本社主導で行われていることから、本レポートの数値は全社的な傾向を一定程度反映する参考値として位置づけられるが、部門・拠点・海外現地法人における投資・人員数は、厳密には反映されていない。

2.2 類型の考え方

本レポートでは、企業を「企業規模」と「業種」の 2 軸で、以下 6 つの類型に分類した。

#	企業の類型	
	企業規模	業種
1	**大企業** (売上高1000億円~)	**金融**
2		**IT・情報通信**
3		**社会インフラ**
4		**製造**
5		**小売・サービス・その他**
6	**中堅企業** (売上高100億円~1000億円)	

図 4 本レポートにおける企業類型

[10] セキュリティ関連人材の人件費を試算する際の参考情報として、厚生労働省「職業情報提供サイト（job tag）」がある。同サイトでは、職種ごとの平均年収などを確認できるため、自社における人件費試算の際、必要に応じて参照されたい。なお、掲載のリンクは、厚生労働省「職業情報提供サイト（job tag）」で「セキュリティ」というキーワードとして入力した結果表示される職種ページである。
（職業情報提供サイト：https://shigoto.mhlw.go.jp/User/Search/Result?keyword=セキュリティ）

(1) 企業規模の定義

企業規模については、売上高ベースで以下の 2 区分を設定した。

① 大企業：年間売上高 1,000 億円以上

国内の統計や産業分類においても、1,000 億円という値は投資規模・体制整備の分岐点として実務的な閾値とされているため、1,000 億円以上を大企業として分類した。セキュリティに関する投資計画や意思決定プロセスが明確に確立しており、セキュリティ単独の予算枠を設けるケースが多い。また、セキュリティ専門組織や専任者を配置し、セキュリティガバナンスを整備している点が特徴である。さらに、本レポートでは、次節に示すように、業種の特徴を踏まえて 5 つに分類している。

② 中堅企業：年間売上高 100 億円～1,000 億円

セキュリティ対策への取り組みを拡大している一方で、対策実装度合いや体制の確保状況にばらつきが見られる層である。このため、セキュリティ対策においては、業種による特徴よりも、経営資源の制約といった共通課題の方が影響を与えると考え、本レポートでは中堅企業は業種横断的な類型として整理した。

なお、売上高 100 億円未満の企業については、セキュリティ投資および人員数のデータが限定的であり、また継続的な投資体制の構築が難しいと考えられることから、本レポートでは対象外とした[11]。

(2) 業種の定義

大企業は、ビジネス観点の特徴、リスク特性、セキュリティ成熟度を踏まえ、以下の 5 業種に分類した。

業種	主なセクター	ビジネス観点の特徴	リスク特性	セキュリティ成熟度
金融	銀行、証券、保険、投資銀行、クレジットカード	機微性の高い顧客情報を保有するため、法規制に基づく厳格な対策が求められる。近年はデジタル化・API連携による新サービス展開が進展	情報漏洩やシステム停止が顧客の信頼や事業継続に影響を及ぼし、社会的・法的影響が大きい	法規制対応を背景に先進的な体制整備が進んでおり、全体的に成熟度は高い
IT・情報通信	ソフトウェア開発、通信、クラウドサービス、SIサービス、インターネットサービス事業	デジタルサービスやクラウド・通信インフラ等の情報基盤を通じて顧客の業務を支える。技術革新や新サービス展開が活発	サービス停止や脆弱性の悪用が多くの顧客に重大な影響を与えるリスクがある	企業によっては自社サービスも活用して対策を実施しており、成熟度は高い傾向にある
社会インフラ	電力、ガス、水道、石油、鉄道、空港、運輸	社会活動全般を支える業種であり安定運用と安全確保が最優先。OT/ICSシステムなど制御系システムを中心に構成される	国家レベルの攻撃対象となる可能性がありシステム停止の影響が社会全体に波及する可能性がある	法規制に準拠した対策を推進中だが、現状はレガシーシステムやOT領域を中心に対策が遅れている企業が多く、今後の強化が急務
製造	重工業、輸送機器、産業用機器、化学、製薬、消費財、素材	工場・生産ラインを中心にOTとITが融合。原材料・部品・設備・物流など多様な関係者との連携が不可欠で、サプライチェーン全体での品質・安定供給が重視される	OTを含め攻撃対象が拡大しておりシステム停止によりサプライチェーン全体に影響が及ぶ可能性がある	人命・安全性など他のリスク対応の優先度が高くセキュリティは劣後している場合もあり。OT領域のセキュリティ対策は特に遅れが目立つ
小売・サービス・その他	小売・卸売、メディア・娯楽、その他サービス	顧客と直接接点を持つ事業が多く、店舗・オンライン・アプリ・プラットフォームなど多様なチャネルを通じて商品やサービスを提供する。DXの進展に伴いデジタル依存度が高まっている	情報漏洩やサービス停止による顧客離反やブランド毀損のリスクが顕在化している	業界に依存するが、概して対策はあまり進んでいない。デジタル依存の高まりに比して、セキュリティ投資が追いついていない傾向

図 5 本レポートにおける業種の定義

[11] 中小企業のセキュリティ投資に関する調査については、以下に示す資料も参考となる。
IPA「2024 年度中小企業における情報セキュリティ対策に関する実態調査 －報告書－」（2025 年 5 月），
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf; 株式会社 MCA「18 業界別中堅企業（300～999 人）の IT（セキュリティ）投資予算とゼロトラスト導入実態」（2025 年 7 月），
https://www.mca.co.jp/ifr/NewsRelease/202507security%20report%20NR.pdf

2.3　目安値の算出アプローチ

目安値の算出にあたっては、既存データ分析と企業インタビューの 2 つのアプローチを採用した。定量と定性の両面から分析を行うことで、日本企業の実態を踏まえた現実的な目安値を算出した。

(1) 既存データ分析

Gartner、ENISA、JUAS、Deloitte、Cybersecurity Advisors Network などの国際・国内調査機関による業界別セキュリティ投資・人員数データ（過去 3 年分）をもとに分析を行った（詳細は「付録 1. 参考資料」参照）。これらのデータを、本レポートで設定した分類の枠組みに合わせて再整理、各調査の定義差（例：人件費の扱い、対象範囲など）を補正し、類型ごとの目安値を算出した。

(2) 企業インタビュー調査

既存データ分析の結果を実態面から検証するため、国内企業の CISO やセキュリティ部門長へのインタビュー調査を実施し、得られた知見を目安値に反映した。

- 協力企業数：22 社
- 実施期間：2025 年 7 月～12 月
- インタビュー形式：1 時間程度の半構造化インタビュー
- 主な質問項目:
  ・セキュリティ関連投資の規模および動向
  ・セキュリティ人員の規模および動向
  ・セキュリティに関する課題認識や将来展望　など

3. 目安値と考察

上記の手法で導出した類型別のセキュリティ投資額および人員数の目安値を以下に示す。例えば、年間売上高 500 億円、従業員数 1,000 人の企業の場合、下記の中堅企業に該当するため、セキュリティ投資額は、500 億円×0.3%=1.5 億円、セキュリティ人員数は、1,000 人×0.2%=2 FTE が目安となる。本章では、この目安値を起点に、各類型の特性や課題、インタビューを踏まえた考察を示す。

#	企業の類型		セキュリティ投資額/売上高の目安値		IT投資額/売上高の前提		セキュリティ投資額/IT投資額の割合	セキュリティ人員数/全従業員数の目安値
	企業規模	業種						
1	大企業(売上高1000億円~)	金融	**0.6%**	=	**5%**	×	**12%**	**0.8%**
2		IT・情報通信	**0.5%**	=	**5%**	×	**10%**	**0.6%**
3		社会インフラ	**0.3%**	=	**2%**	×	**15%**	**0.3%**
4		製造	**0.2%**	=	**2%**	×	**10%**	**0.2%**
5		小売・サービス・その他	**0.1%**	=	**1%**	×	**10%**	**0.2%**
6	中堅企業(売上高100億円~1000億円)		**0.3%**	=	**2%**	×	**15%**	**0.2%**

図 6 セキュリティリソースの目安値

3.1 金融

主なセクター：銀行、証券、保険、投資銀行、クレジットカード

本業種は、顧客の個人情報や決済・取引情報を大量に保有していることから、サイバー攻撃の主要標的となっている。加えて、監督省庁による厳格な規制対応が求められることから、投資額・人員比率ともに全業種の中で最も高水準となっている。同業種の中でも、銀行業では本レポートの目安値を上回る企業もある一方で、他の業態では、当該水準を高めと感じるケースも想定される。しかし、近年これらの業態を狙うサイバー攻撃が激化していることから、本レポートでは金融業全体として一体的に捉え、リスク認識と対策意識を高める観点から同一の分類に含めた。

本業種では、2024 年 10 月に策定された金融庁の「サイバーセキュリティガイドライン」への対応が喫緊の課題となっており、インタビュー企業でも、サプライチェーン管理や検知・対応体制強化といった要件への対応で追加投資や業務負荷の増加が見られた。一方で、「策定を追い風と捉え、経営層への説明材料として積極的に活用している」との前向きな声も聞かれた。対策が遅れている企業にとっては、この機を捉えて自社の現状を見直し、戦略的に取り組みを加速させることが自社のセキュリティ成熟度を高める一つの有効な手立てとなるだろう。

【今後考慮すべき事項】

今後は、非対面チャネルの拡大に伴う eKYC、Web ポータル、AI ヘルプデスクのセキュリティ対策、およびデジタル通貨・暗号資産（デジタル円、ステーブルコイン、トークン化証券）、デジタル技術を悪用したマネーロンダリングへの対策など、新領域への対応も重要になる。また、耐量子コンピューター暗号（PQC）の導入においては、影響範囲が広く、移行計画が複雑化することが想定されるため、莫大なリソースが必要となる。これらの新技術領域では、従来の内部統制やガイドラインを超えた、新しい枠組みでのリスク評価・監視体制が求められるだろう。

3.2　IT・情報通信

主なセクター：ソフトウェア開発、通信、クラウドサービス、SI サービス、インターネットサービス事業

本業種は、クラウドサービス、通信基盤、ソフトウェア開発など、社会全体の DX を支える基盤を提供しており、事業そのものがセキュリティと密接に結びつくものも多い。そのため、セキュリティ投資は単なるコストではなく、自社の信頼性確保や競争優位の源泉と位置づけられやすいため、金融業に続く高い目安値となっている。

AI や自動化ツールの積極的活用により、セキュリティ関連業務の効率化が進められている一方で、高度なリスクに対応する専門性の高い人材の確保が依然として課題となっている。インタビューでは、「CISSP 保持者を売上 100 億円あたり 1 名配置することを目標にしている」「事業部門においてもセキュリティ人材を育成している」といった声があり、中央のセキュリティ部門単独では対策が行き届かないとの認識のもと、各事業部門や現場でのセキュリティ対応力の強化を図る動きが見られた。

【今後考慮すべき事項】

生成 AI の普及により、自動コード生成や CI/CD パイプラインの高度な自動化、DevSecOps の更なる浸透が進むため、新たなリスクへの対応が求められる。さらに、衛星通信や SDN、Open RAN など通信基盤の仮想化、IOWN・6G・エッジコンピューティングといった新たなアーキテクチャが拡大することで、ネットワーク構造の複雑化と攻撃面の増大が避けられず、次世代インフラ特有のリスク評価枠組みを整備する必要性が高まるだろう。

3.3　社会インフラ

主なセクター：電力、ガス、水道、石油、鉄道、空港、運輸

設備投資比率が高い産業構造のため、セキュリティ投資額は売上比で見ると相対的に低く見える傾向がある。しかし、本業種は、国民生活や経済活動の基盤を担うことから、サイバー攻撃が社会的影響を及ぼすリスクが極めて高く、対策が急務となっている。

政府も重要インフラ防御や経済安全保障の観点から関与を強めており、経済安全保障推進法に基づく基幹インフラ設備の事前審査制度や、能動的サイバー防御の導入といった施策を通じて、事業者に対しセキュリティ強化と報告体制の構築を求めている。このように社会インフラを担う企業は、セキュリティをコストではなく公共的責任と位置づけた対応が求められている。

もっとも、一口に社会インフラといっても、業態や組織のデジタル化の度合いにより成熟度には大きな差がある。レガシー設備が多く、デジタル化や DX の取り組みが限定的にとどまっている企業もあれば、デジタル技術を活用して運用高度化や事業変革を進めるなど、DX を積極的に推進している企業も存在する。今回インタビューした企業の中には、「データドリブン経営」を掲げ、経営層自らが「セキュリティなくして DX は成り立たない」との強い認識を示し、積極的にセキュリティの取り組みを進めている企業もあった。こうした先進企業では、セキュリティが DX 推進の前提条件として位置づけられていた。本業種全体としても、規制対応にとどまらず、DX と一体でセキュリティを進化させ、全社的なセキュリティ成熟度を引き上げていく姿勢が今後一層求められるだろう。

【今後考慮すべき事項】

社会インフラでは、IT/OT のさらなる一体化や人口減少を背景としたリモートメンテナンスの拡大、AI ロボットによるオートメーション化などにより、従来の OT 設備には存在しなかった新たなデジタル接点が増加し、攻撃対象領域の広がりが不可避となる。また、スマートシティの拡大により、都市全体のデータが相互接続される環境が進むと見込まれる。こうした複数インフラの相互依存化が進む中では、「全体連携を前提としたセキュリティアーキテクチャ」の確立が今後の重要な検討領域となる。

3.4　製造

主なセクター：重工業、輸送機器、産業用機器、化学、製薬、消費財、素材

製造業では、設備停止が事業に与える影響が極めて大きいため、工場の生産設備や制御系システムは長期間にわたり継続利用されることが一般的である。また、専用 OS やベンダー固有の仕様に基づいて構築されている場合も多く、システム更新や統一が進みにくい。その結果、脆弱性対応やパッチ適用といった基本的なセキュリティ対策も十分に講じられないケースが多い。一方で、工場や OT 環境を標的としたサイバーリスクが急速に高まっており、セキュリティ投資は喫緊の課題となっている。

他方で、「費用対効果」を重視する経営文化が根強く、セキュリティ投資の成果は定量化しにくいために、経営層の理解・判断を得る上での障壁となっている。インタビューでも「経営層も頭ではセキュリティの重要性は理解しているが、投資の必要性を数値で説明してほしいと言われるので、納得させるのが難しい」との声が複数聞かれた。

こうした中、近年ではサプライチェーン全体のセキュリティリスクが注目されており、BtoB 取引においては、取引先のセキュリティ水準が選定判断の要素として重視されるようになってきている。セキュリティ対策に主体的に取り組むこと自体が、企業としての信頼性を示す指標となり、顧客からの評価や競合との差別化にもつながり得る。インタビューでは「経済安全保障推進法や JC-STAR などの制度整備により、十分な対策を講じていない企業はサプライチェーンから外されるケースが出てきており、製造業にとってはセキュリティ強化の追い風になるのではないか」とのコメントもあった。今後は、セキュリティを単なる防御手段として捉えるのではなく、事業競争力の一部として積極的に取り組む姿勢が求められる。

【今後考慮すべき事項】

AI ロボットや自律搬送、デジタルツインによるスマートファクトリー化が進むにつれ、製造現場にはこれまで以上に多様なデジタル機器が入り込み、攻撃対象領域が拡大する。また、グローバルサプライチェーンの複雑化により、海外部材・海外工場を含む広域でのセキュリティ保証が必須となりつつある。加えて、IT/OT 一体化が加速する中では、単に工場の防御を強化するだけでなく、製品ライフサイクル全体を通じたリスク評価と連動した体制構築が求められるだろう。

3.5　小売・サービス・その他

主なセクター：小売・卸売、メディア・娯楽、その他サービス

本業種は、他業種と比べてセキュリティ投資が低く位置づけられる傾向がある。これは、保有する個人情報の価値や漏えいリスクが過小評価され、対策コストが低く見積もられてきたことが背景にあると考えられる。一方で、全国に店舗や拠点が分散していることが多いため、投資額に比べてセキュリティ人員比率は高い傾向がみられる。

近年、オンラインサービスの普及に伴い、多くの企業が Web サイトやスマートフォンアプリを通じて顧客接点を持つようになった。これにより、企業が扱う顧客情報の量・種類は大きく拡大し、同時にアタックサーフェスも広がっている。その結果、決済情報や行動データなど、価値の高い個人情報を狙った攻撃も顕在化し、情報漏えいのリスクは確実に高まっている。こうした状況を踏まえると、これまで相対的に対策が後手に回っていた本業種においても、セキュリティを経営課題として捉え直すことが求められている。

特に小売業では、現場の IT リテラシーのばらつきや、属人的な運用に起因するセキュリティリスクも無視できない。拠点数の多さに反してセキュリティ専門人材の配置は難しく、「人は増やせない」という前提の中で限られたリソースをどう活かすかが重要な課題となっている。インタビューでも、「人海戦術を前提とせず、外部ベンダーやツールを活用して少人数で回せる仕組みに切り替えてきた」「少ないリソースでも、Security by Design の考え方で設計段階から対策を組み込んでいる」といった声が聞かれた。

【今後考慮すべき事項】

小売・サービス領域では、セルフレジや無人店舗、遠隔監視といった非対面化の加速に伴い、デバイス・ネットワーク・認証の三層で新たな管理ポイントが発生する。さらに、QR 決済・デジタルクーポンなど多様化する決済手段の採用は利便性を高める一方、決済プロバイダや外部サービスとの複雑な連携に起因するリスクを増大させる。また、需要予測や接客への AI 活用が拡大するにつれ、AI モデルの不正利用やサプライチェーンのブラックボックス化への対応も新たな論点となる。

3.6 中堅企業

売上規模に対して固定費の比率が高くなりやすいため、売上高を分母とした場合、投資比率が相対的に高く見える傾向があるが、実態はセキュリティ対策の必要性を認識しながらも、予算や専任人材の制約により体制整備が進んでいない。また、中堅企業では「自分たちは大企業ではないので狙われないだろう」という誤った安心感が依然として見られる。しかし実際には、セキュリティ体制が整っていないために攻撃者にとって格好のターゲットになっている[12]。

今回のインタビュー企業にはセキュリティ専任者が配置されていたが、そもそもセキュリティ以前に IT 専任者も不在で、IT を兼任で担っているケースも少なくない。そのため、最低でも IT 専任 1 名、できれば、IT 専任 1 名＋セキュリティ担当 1 名を確保することが出発点となる。セキュリティを理解する人材を社内に置くことで「どのように外部ベンダーを活用するか」「どのような人材を追加で採用すべきか」といった判断が可能になる。その意味で、最初の 1 人を社内に置くこと自体が、セキュリティ投資の第一歩といえる。

【今後考慮すべき事項】

中堅企業では、人件費の高騰と少子高齢化に伴う慢性的な人材不足が今後さらに深刻化する可能性が高い。こうした中では、限られた人員で事業を継続させるための自動化・外部サービスの活用・クラウド移行が一段と重要になる。加えて、採用競争力の低下が予想されるため、社内での人材育成と外部リソースの併用を前提とした「ハイブリッド体制」を早期に構築し、持続的にセキュリティレベルを維持できる仕組みを整えていく必要がある。これらのセキュリティ投資や人件費は、価格転嫁すべきであり、取引先との値上げ交渉の材料にすることが望ましい。

4. セキュリティリソースの確保に向けた提言【セキュリティ責任者向け】

本章では、セキュリティ責任者向け（CISO、セキュリティ部門長など）に向け、目安値を使ってどのようにリソースを確保していくべきかについて JCIC としての提言をまとめる。重要なのは、目安値そのものの達成ではなく、目安値を使い、現状（現在地）と将来（目的地）を客観的に説明し、経営層と中長期のセキュリティリソース計画を合意することである。

提言 1 ：目安値を使って、現在地を経営層に示せ

まずは、現状を把握し、目安値と照らして自社の現在地を客観的に説明できるようにすることが、必要なリソースを確保するために大切である。

---

[12] 警視庁によると、ランサムウェア被害の企業・団体等の規模別報告件数において、大企業よりも中小企業の被害が多い状況が数年継続しており、令和 7 年上半期の統計データでは、中小企業が件数・割合ともに過去最多で、全体の約 3 分の 2 を占めた。
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

そのためには、可視化によって自社のリソース状況を把握することが重要である。多くの企業では、セキュリティ関連投資が IT 投資や人件費の中に埋もれ、全体像が十分に把握できていない。人員に関しても同様である。しかし、可視化なくして妥当性は示せない。まずは、自社のリソースを整理・集計し、「見える化」することが出発点である。ここで重要なのは 1 円単位、1 人単位まで精緻に把握することではなく、「どの程度の投資・人員を投じているか」という全体感をつかむことである。インタビューでも、「複合的な機能を持っている製品の費用をどこに計上すべきか悩んでいる」「IT 部門とセキュリティ部門の費用分担が定まらず、数値の整理が進まない」「兼任者をどこまでカウントすべきかわからない」といった声が聞かれ、まずどう集計するかの段階で立ち止まる企業が多かった。一方、現状を可視化できている企業は過度に精緻化を求めず、一定の整理軸を設けて全体感を把握していた。Gartner の分類や NIST CSF などのフレームワークを参照しつつ、この機に自社の実態に合わせた定義を作り、整理してみてほしい。

可視化によって現状のリソースが整理できたら、次に行うべきは目安値との比較である。ここで重要なのは、「目安値より高い/低い」こと自体ではなく、自社の事業構造・DX 戦略・リスク特性を踏まえ、「なぜその水準なのか」を説明できる状態にすることである。例えば、本レポートの目安値より高い/低い場合でも、以下のような理由があれば、それは妥当となるケースもある。このように、まずは現状を可視化し、目安値と照らして自社の水準がなぜそうなのか、を客観的に説明することが、経営層が判断可能な状態をつくり、必要なリソースを確保するための基盤となる。

状況	目安値より高い場合	目安値より低い場合
理由例	• Web公開システムやクラウドサービス利用、外部連携が多く、攻撃対象となる範囲が広い • 高度な機密情報、重要な個人情報、事業・国家安全保障に関わる情報を扱っている • 拠点・事業所が多い • セキュリティ基盤の刷新・強化を進めており、一時的に投資が集中している	• Web公開システムや外部接続が限定的でインターネット経由の攻撃を受ける可能性が小さい • 機密性の高い情報や大規模な個人情報を扱っていない • 拠点・事業所が少ない • 過去にセキュリティ対策に関する大規模投資を実施済みであり、直近では運用が中心となっている

図 7 目安値との差分が生じる理由例

提言 2：目安値を使って、目的地を経営層に示し、必要なセキュリティリソースを確保せよ

提言 1 により自社の現在地が客観的に説明できたら、次に必要なのは、目的地、すなわち将来どの水準を目指すかを経営層と合意することである。セキュリティ対策は単年度で完結するものではなく、継続的な体制強化と能力強化が前提となる活動である。単年度のプロジェクト対応に終始すると、担当者依存や場当たり的な投資となり、計画的に成熟度を上げるのが難しい。そのため、3～5 年を目安とした中長期的なリソース計画を策定し、経営層と合意することが不可欠である。

具体的には、可視化した結果を整理し、

- 足元のギャップ（どれだけ不足/過剰なのか）
- 将来どの水準を目指すのか（目的地）
- その水準が目安値と整合しているか（妥当な目標か）

を経営層に説明する。これにより、施策の積み上げだけではなく、全体感を示し、経営層が判断しやすい状態を作ることができる。

提言の考え方を具体的に示すため、参考としてモデルケースを 2 つ例示する。

モデルケース１：製造業のＸ社

【ビジネス概要】電子部品を主力とするメーカー。同社の製品は、顧客の最終製品やシステムに組み込まれる形で使用されており、BtoB ビジネスを中核としている。生産・販売拠点を国内外に展開しており、海外売上高比率は高い水準にある。近年は、従来の部品提供に加え、製品のデジタル化を通じて得られる稼働データを活用した予兆保全や遠隔保守などの運用支援を目的とした IT サービスの提供にも取り組み始めている。

項目	例	
企業情報	年間売上高：8,000億円	従業員数：20,000人
現在のセキュリティリソース状況（現在地）	投資額：0.4%（32億円）	人員数：0.3%（60 FTE）
＜製造＞の目安値	投資額：0.2%	人員数：0.2%
目安値とのギャップ	＋0.2ポイント	＋0.1ポイント
理由	• 数年前に同業界で発生したランサムウェア被害を契機として、EDRの刷新、工場へのIDS導入、インシデント発生時を想定した訓練の定常化などの対応に取り組み、セキュリティ対策を強化している。 • 設計データや製造プロセスに関するノウハウなど、競争力の源泉となる知的財産を保護するため、情報管理およびアクセス統制を強化している。 • 国内外に点在する生産・販売拠点に対し、拠点単位での責任体制を構築し、グローバルで統一的なガバナンスを維持しているため、人員数が相対的に多い。	
中長期計画（現在地→目的地）	投資額：0.4%→**0.5%**	人員数：0.3%→**0.5%**
理由	• 同業界で発生したインシデントを契機としたセキュリティ対策強化については、本年度をもって主要な対応は完了する見込みであり、一時的な費用は今後落ち着く見込み。一方で、製品提供に加え、予兆保全や遠隔保守といったITサービスにも取り組んでいることから、こうした事業構造の変化に伴うセキュリティリスクへの対応を見据え、3年後までにセキュリティ投資は＜IT・情報通信＞の目安値である売上高比0.5%水準まで段階的に引き上げる方針とする。 • クラウド、データ活用、グローバルSOC運用などを支える体制強化のため、人員数については3年後までに全従業員比0.5%水準を目指す。	

図 8 モデルケース 1 製造業の X 社

モデルケース２：金融業のＹ社

【ビジネス概要】個人および法人向けに金融サービスを提供する事業会社。主な提供形態は、社外の販売・業務パートナーを通じた間接型のビジネスモデルであり、全国に広がるパートナーネットワークを通じて事業を展開している。近年は、業務プロセスのデジタル化やデータ活用を通じた業務効率化、顧客対応の高度化に取り組み始めており、IT 活用領域および外部接点が拡大している。

項目	例	
企業情報	年間売上高：10,000億円	従業員数：10,000人
現在のセキュリティリソース状況（現在地）	投資額：0.3%（30億円）	人員数：0.3%（30 FTE）
＜金融＞の目安値	投資額：0.6%	人員数：0.8%
目安値とのギャップ	▲0.3ポイント	▲0.5ポイント
理由	• 本社主導で一定のセキュリティ施策は進めてきたものの、パートナーとの連携システムに対する統制整備が後手となっており、投資が限定的であった。 • セキュリティの重要性は認識しているものの、現状はIT部門が運用・開発と兼務して対応しており、専任しての推進体制が十分に整っていない。結果として投資・人員数ともに金融業の目安値を下回る水準にとどまっている。	
中長期計画（現在地→目的地）	投資額：0.3%→**0.6%**	人員数：0.3%→**0.4%**
理由	• 監督省庁の各種ガイドラインへの対応に加え、業務プロセスのデジタル化やデータ活用を通じた業務効率化、顧客対応の高度化に取り組み始めており、IT活用領域および外部接点が拡大している。このため、セキュリティ専任部署を新設し、ガバナンスから実運用までを一体で推進する体制を構築し、各種対策を推進することから、セキュリティ投資を3年後までに＜金融＞の目安値である売上高比0.6%水準まで段階的に引き上げる方針とする。 • 人員数については、監視・インシデント対応について外部サービスを活用することで、効率的な体制強化を図り、3年後までに全従業員比0.4%を目指す。	

図 9 モデルケース 2 金融業のＹ社

5. セキュリティリソースの確保に向けた提言【経営層向け】

本章では経営層向けに、目安値を使ってどのようにリソースの妥当性を評価し、投資判断をしていくべきかについてJCICとしての提言をまとめる。重要なのは、目安値そのものの達成ではなく、目安値を使って、現状（現在地）と将来（目的地）の妥当性を判断し、中長期的な投資判断を行うことである。

提言１：目安値を使って、現在地を把握せよ

経営層がまず行うべきは、目安値を用いて自社の現在地を客観的に把握することである。目安値は、以下の問いに答えるための経営判断の物差しとなる。

- 今の水準は適切なのか。
- 同業他社と比べて高いのか・低いのか。

重要なのは、目安値より高い/低いという数字そのものではない。自社の事業構造・DX 戦略・リスク特性を踏まえ、現状のリソース水準がどの位置にあるのかを俯瞰的に捉えることが肝要である。

提言２：目安値を使って目的地達成のためのセキュリティリソース確保にコミットせよ

現在地が把握できたら、次に経営層がすべきは目安値を参考に、中長期で目指すべきリソース水準を見定め、計画的な投資判断を行うことである。セキュリティは単年度では完結しない。セキュリティ対策の導入、運用体制の確立、人材の確保・育成など、主要な取り組みは複数年で積み上げる活動であり、単年度の都度承認では対策が完了せず、体制も整わないまま、結果として対策が後手に回る状況から抜け出せない。中長期的な投資こそが、セキュリティ成熟度を段階的・計画的に高める唯一の方法である。だからこそ経営層は、中長期計画に基づくセキュリティリソースの確保を明確にコミットすべきである。

6. まとめ

本レポートでは、DX の進展、脅威の深刻化・複雑化により、企業におけるセキュリティの重要度がかつてないほど高まっている一方で、適切なセキュリティリソースの確保が進まず、対策が後手に回っている原因を、経営判断に必要な妥当性を判断するための指標が存在しないことである、と整理した。

これを踏まえ、本レポートは、日本で初めて、企業規模・業種別の「セキュリティ投資額および人員数の目安値」を提示した。ただ重要なのは、この目安値を絶対視するのではなく、自社の現在地を客観的に可視化し、将来に向けて必要なリソース水準を経営層と共有するための「共通言語」として活用することである。目安値を活用することで、従来多くの企業が抱えていた現在地や目的地を説明できないという構造的な課題を解消できる。結果として、経営層との合意形成が進み、中長期的なセキュリティリソース確保と計画的なセキュリティ強化を実現することができる。目安値は、企業が中長期的にセキュリティ成熟度を高めていくための意思決定を支える確かな拠り所となるだろう。

最後に、今回の企業インタビューでは、目安値に対する以下のような追加ニーズも寄せられた。

- 重要データの有無・レベルに応じた目安値
- グローバル拠点の割合を考慮した目安値
- 拠点数の多さを反映した目安値
- 目安値の中での固定費・変動費の割合の提示
- 定期的な目安値の更新

こうした意見を踏まえ、JCIC では、企業の実態に即した指標や知見の充実を図りながら、日本全体のセキュリティレベル向上に向け、今後も研究・執筆を続けていく所存である。

7. コラム～インタビューから見えてきた現場のリアル

7.1 ROI だけでは測れない――経営層に「実感」を与える説明とは

前回の JCIC レポートでは、経営層の共通言語である「お金」でリスクを議論するために、サイバーリスクを定量化して議論することの重要性も提言のひとつとして掲げた[13]。実際、リスクベースで想定損失額を試算することは、経営層にサイバーリスクを自分ごととして捉えてもらうことの契機になる。

しかし、この試算をもとに、セキュリティを他のビジネス領域と同じように ROI（投資対効果）のみで説明し、経営層から投資判断を得ようとすることには限界がある。セキュリティ投資のリターンは通常、想定損失額で表現されるが、近年はその算定自体がますます困難になっている。サプライチェーンや外部連携を通じて被害が連鎖的に拡大するケースが増え、波及部分の影響を織り込むことが難しい。また、生成 AI などの新しい攻撃手法の影響は予測が難しく、既存のリスクモデルでは捉えきれない領域が広がっている。加えて、セキュリティインシデントはブランド毀損・風評被害・顧客離脱による機会損失といった無形の間接被害を引き起こすが、企業に最も深刻な影響を与えるこうした要素は数値化が困難であり、定量的に扱うには限界がある。

インタビューでは、多くのセキュリティ責任者が、「想定損失額を用いて ROI を説明することもあるが、それよりも『実際にインシデントが発生した時に何が起きるか』を示した方が経営層に伝わる」と語った。他社のインシデントを自社に置き換えて「もし同じことが自社で起きたら」という具体的なストーリーの方が経営層の意思決定を促す力を持つのである。

実際に、ある企業では「同業界の企業が重大なセキュリティインシデントにより数か月間にわたり業務停止を余儀なくされた事例が大きな転換点となった」と語った。被害を受けた企業が「何が原因だったのか」「事業にどのような影響が及んだのか」「本来どのような対策を講じておくべきだったのか」というリアルな声を業界内に共有したことで、経営層の危機意識が一気に高まり、結果として業界全体のセキュリティが底上げされた、という。

想定損失額の試算は、経営層の自分ごと化に非常に有効である。まだ実施していない企業には、まず試算してみることを推奨したい。そのうえで、経営層の危機意識を継続させセキュリティ投資への理解を得るために、他社のインシデント事例を踏まえた「自社換算シナリオ」を定期的に作成し、経営層に説明するという手法も積極的に取り入れてみてほしい。

7.2 「選択と集中」こそが、戦略的投資のカギ

今回のインタビューでは複数の企業から、「自社に限らず、他社や業界全体を見渡しても、リスクアセスメントが十分に行われておらず、守るべき資産の優先順位を付けられていない企業が意外と多い」という声が聞かれた。多くの企業では、プロジェクト単位・事業部門単位で対策を判断しており、「どの資産を最優先で守るべきか」という共通認識が欠けがちである。DX の進展により、クラウドや AI の活用、外部連携の拡大などによって新たな守るべき領域が増えた結果、

[13] サイバーリスクの簡易的な定量のために、JCIC では Excel ツール「サイバーリスク指標モデル『想定損失額の目安』簡易シミュレーション」を公開している。https://www.j-cic.com/pdf/report/CyberRiskEstimationModel-2022-03.xls; また、IPA も「情報セキュリティ 10 大脅威 2022」に基づくサイバー攻撃シナリオ毎の損害額を試算する Excel ツール「NANBOK」を開発している。https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/visualization-costs.html

対策範囲が際限なく広がり、「あれもこれも」とパッチワーク的な対策に追われているケースが少なくない。その結果、対応の重複や抜け漏れ、リソースの分散といった無秩序な投資が発生している。

一方で、限られたリソースの中でセキュリティ対策を推進している企業では、「選択と集中」という言葉が挙げられた。ある企業では、各事業部門へのヒアリングを通じて重要資産を洗い出し、事業部門自身に重要度を三段階で評価してもらう仕組みを導入していた。その後、IT・セキュリティ部門が全社横断で評価を統合し、重複や抜け漏れがないように最終優先順位を調整するプロセスを構築していた。特筆すべきは、この評価をグローバル共通の基準で運用していた点である。地域や事業ごとに判断基準が異なれば、どこかに防御の穴が生まれかねないが、基準を統一することでそのリスクを最小化していた。

多くの企業がリスクアセスメント自体は実施しているものの、その結果が「全社として何を最優先で守るのか」という合意や、「限られたリソースをどこに集中させるのか」という意思決定にまで十分に結び付いていないケースが少なくないのではないか。脅威が複雑化する一方で、守るべき領域も広がる今、全てを同じ強度で守るという発想はもはや現実的ではない。自社にとって本当に守るべきものは何か、「選択と集中」の観点から改めて考えてみる必要がある[14]。

7.3 人材不足時代のセキュリティ体制――インタビューから見えた現実的アプローチ

今回のインタビューでは、複数の企業が共通して「人材不足が最大の課題である」と回答した。この傾向は日本だけでなく世界共通であり、採用市場の逼迫や育成に要する時間を踏まえると、採用だけで解決するアプローチはすでに限界を迎えているといえる。多くの企業では、新卒や中途人材の採用を進めているものの、採用市場の逼迫、即戦力人材の確保の難しさなどの制約から、短期間で十分な体制を整えることが困難である。このような中で有効なのが、「外部活用」と「現場へのシフト」のアプローチだ。

外部に委ねられていた領域としては、主に以下の 2 つが挙げられた。

- 標準化・パターン化された領域（例：ログ監視、脆弱性スキャン、端末管理、運用保守）
- 高度専門性が必要なため、内製が非効率な領域（例：ペネトレーションテスト、フォレンジック、アドバンスド SOC）

ただし、インタビューで印象的だったのは、「何でも外に出すのが正解ではない」という点である。実際、「自社で理解できないものを外に出すのは危険」「外部任せにしすぎると内部の判断力が育たない」といった声が複数聞かれた。人材不足時代に外部活用は欠かせないが、重要なのは、内外で担うべき領域を定義し、限られた自社のリソースを、戦略立案・意思決定・全体統制といったコア業務に集中させることである。

もう一つ多くの企業で見られたのが、中央集権的にセキュリティを担う組織を配置するだけではなく事業部門・拠点に分散してセキュリティ管理者を配置するという「現場へのシフト」の取り組みである。事業側にセキュリティの知識をつけることで、人材不足を補う効果もあるが、これにより DX や外部連携が急速に進む現場のスピードに対応するという効果にもつながっている。「あえて中央の組織は有事の際の CSIRT や相談役としての小さな政府とすることで、各々がセキュリティの考えを持つようにしている」とまで語った CIO もいた。

人材不足が深刻化する中で、こうしたアプローチは万能ではないものの、限られた人員で実効性の高いセキュリティ体制を構築するためのヒントとして参考になるだろう。

---

[14] 個社ごとに事業構造やリスク特性が異なる以上、セキュリティリソースをどこに配分するかは、最終的には経営判断に委ねられるべきものである。ただ、インタビューでは「限られた予算の中で、どの領域に重点的に配分すべきか判断が難しい」といった声も一定数聞かれた。参考情報として、調査機関によるセキュリティ投資の配分傾向の情報を掲載する。自社の投資配分を検討する際に、必要に応じて参照されたい。
Gartner「IT Key Metrics Data 2025: IT Security Measures – Analysis」（Figure 9、Figure 10）；
IANS, Artico Search「2025 Security Budget Summary Report」（Figure 6）

付録 1. 参考資料

目安値の策定にあたり、以下を参考にした。

- Gartner「IT Key Metrics Data 2023: IT Security Measures – Analysis」, https://www.gartner.com/en/documents/4021813
- Gartner「IT Key Metrics Data 2024: IT Security Measures – Analysis」, https://www.gartner.com/en/documents/5004731
- Gartner「IT Key Metrics Data 2025: IT Security Measures – Analysis」, https://www.gartner.com/en/documents/5938807
- Gartner「IT Key Metrics Data 2023: Industry Measures - Executive Summary」, https://www.gartner.com/en/documents/4021658
- Gartner「IT Key Metrics Data 2024: Industry Measures - Executive Summary」, https://www.gartner.com/en/documents/5014331
- Gartner「IT Key Metrics Data 2025: Industry Measures - Executive Summary」, https://www.gartner.com/en/documents/5971171
- JUAS「企業 IT 動向調査報告書 2023」, https://juas.or.jp/cms/media/2023/07/JUAS_IT2023.pdf
- JUAS「企業 IT 動向調査報告書 2024」, https://juas.or.jp/cms/media/2025/01/JUAS_IT2024.pdf
- JUAS「企業 IT 動向調査報告書 2025」, https://juas.or.jp/cms/media/2025/04/JUAS_IT2025.pdf
- Deloitte「Cybersecurity insights 2023: Budgets and benchmarks for financial services institutions」, https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2024/cybersecurity-insights-2023-budgets-benchmarks-financial-services-institutions.pdf
- Cybersecurity Advisors Network「Cybersecurity Investments in Global Banking: Comparative Analysis and Case Studies」, https://cybersecurityadvisors.network/2025/03/04/cybersecurity-investments-in-global-banking-comparative-analysis-and-case-studies/
- ENISA「NIS Investments 2023」, https://www.enisa.europa.eu/publications/nis-investments-2023
- ENISA「NIS Investments 2024」, https://www.enisa.europa.eu/publications/nis-investments-2024

付録 2. インタビュー結果

インタビュー内容について、各社より掲載の承諾を得た内容を掲載する。

類型	金融		
企業	A 社	B 社	C 社
役職	情報セキュリティ統括	リスク管理責任者	サイバーセキュリティ統括
セキュリティ関連投資額の算出方法、経営層への説明方法に関するコメント	・投資額は、投資対効果やベンチマークによって決めるのではなく、リスクに応じて決めている。新たなリスクやアタックサーフェスの広がりを考慮して追加投資を判断する。	・投資額は、同業他社の水準やベンチマークを参照しつつ、同業他者の中で先進的な水準を目指し、中期計画を策定している。	・金融庁のガイドラインをベースに、自社のリスクを踏まえた対策の積み上げで、投資額は決めている。 ・「IT 投資に対するセキュリティ投資比率」は、経営会議でも値を示すことがある。 ・経営層はもともとセキュリティに対して前向きである。特に昨年度からは、金融庁のガイドライン対応が求められているため、投資がしやすい環境になっている。経営層からは、金額よりも内容として何が不足しているのかを聞かれることが多い。
セキュリティ関連投資の動向に関するコメント	・今後は AI に関する投資や、脆弱性管理強化に関する投資が増える見込み。	・中期経営計画に基づきセキュリティを強化させており、投資額は増額を見込む。 ・追加投資の目的は、主に金融庁のガイドラインを踏まえたセキュリティのレベルアップと、ゼロトラストの導入である。	・経営層はサイバーセキュリティの重要性を理解しているものの、長年、コスト抑制してきた文化が強く、加えて、現場では「外部ネットワークに接続していない」「これまでインシデントが発生していない」といった理由から、サポート切れを受容しようとするケースも見られる。 ・こうした状況に対しては、ガイドラインに対応しないことは、法令違反につながる可能性があることを示すなど、説明の仕方を工夫しながら理解を得つつ、リスクを踏まえた対策を段階的に進めている。
セキュリティ人員の規模および動向に関するコメント	・現時点での主な課題は、予算面ではなく、必要な施策を推進できるスキルセットを保有する人材の不足である。 ・基本的なセキュリティ対策を担うエントリーレベルの人材ではなく、戦略を担う人材が必要である。エントリーレベル業務については、AI 活用やアウトソーシングを通じた効率化を進めることも必要となっていると感じる。一方で、従来、セキュリティとは切り離されていた地政学リスクや内部不正リスクに対応できる人材や、技術的知見を戦略的にアクションに繋げられる人材の需要も高まっている。	・人材採用では、数年前から理系の新卒人材を直接 IT 部門に採用するほか、システム開発経験者などのキャリア採用を継続的に実施している。 ・キャリアパスの提示や資格取得支援を通じて、中長期的な人材育成を図っているが、即戦力が必要な領域は外部リソースも活用しながら補完している。	・実態としては、外部リソースを活用することも多い。例えばフォレンジックは専門人材を社内に雇うほど頻繁にインシデントは起きない。24 時間 SOC も内製化は難しい。 ・IT 子会社では IT 専門人材の経験者採用も積極的に行っている。また、育成枠の若手を採用し、社内のサイバーセキュリティ認定制度を用いて育成している。持ち株会社では、CISSP の取得推進、更新費用の補助などにより、自己研鑽を支援している。 ・金融業の中でも、ビジネス特性の違いにより必要とされる体制には差が生じる。金融取引がリアルタイムで発生する業態、もしくは 24 時間金融取引を提供する業態では、サイバー攻撃を受ける機会が多くなり、体制も多く必要になると考えられる。一方、金融取引頻度が比較的低い、もしくは限定的な業態では、その取引を狙ったサイバー攻撃を受ける機会も限定的であり、一般的な企業の体制と同様でも良いように思う。

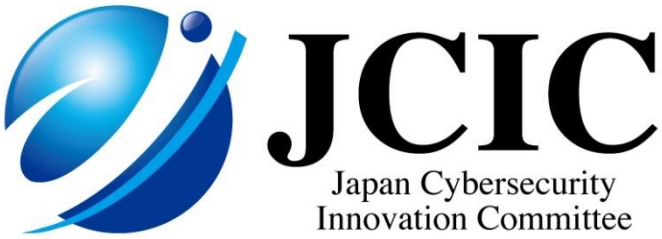
類型	金融		IT・情報通信	
企業	D 社	E 社	F 社	G 社
役職	情報システム部　マネージャ	CISO	CISO	CISO
セキュリティ関連投資額の算出方法、経営層への説明方法に関するコメント	・投資額は、事業費の内訳として含まれており、個別にセキュリティ投資は確保していない。対策内容は、金融庁のガイドラインをベースとして自社に必要な部分を見極めて判断している。 ・経営層は、顧客情報などの保護に必要な費用は投資せよという考えであり、予算確保には苦労していない。IT 投資の中で必要投資として組み込んでおり、その中からセキュリティを削ることはない。	・投資額は、グローバル企業と日本企業で算出方法が異なる可能性がある。グローバル企業では CISO 予算として明確に確保している場合もあるが、多くの日本企業は SIer 主導の慣行により、システム構築費とセキュリティ費用を分けることが難しい。そのため、数値が小さく出る傾向があるのではないか。	・投資額は、基本的に必要な施策ごとに積み上げ方式で決めているが、追加投資に関して取締役会に説明する際には、Gartner などの外部ベンチマークや JCIC の前回レポートなども活用し、必要性と妥当性の理解を得ている。 ・役員は、投資を増やすことよりも脅威に対して適切な対策が取れているかを重視しているため、防御率や施策のデータを可視化し、理解を促す工夫も行っている。	・自社でセキュリティ事業を展開していることから、投資判断においては金額や ROI といった数値指標よりも、「どのようなリスクが存在し、セキュリティ製品の導入によりどれだけリスクを低減できるか」という実効性を重視している。 ・自社内で得られたセキュリティ対策の知見を顧客向けサービスに転換できる点が、追加投資の正当化要因となっている。
セキュリティ関連投資の動向に関するコメント	・グループ内の業態ごとに監督省庁・ガイドラインは異なるため高い基準に合わせる、という方針にしている。 ・金融庁のガイドラインに対応する中で、必然的にフィッシング対策や AI を用いる攻撃の対策にも取り組んでいる。	・近年の脅威動向を踏まえると、現状のリソースで十分だとは考えていない。ただし、予算は必要に応じて増額できても人員の確保は困難であるため、課題は予算よりも人材にあると考えている。	・AI を活用したオペレーション自動化を進めているが、同時に新たなセキュリティリスクも生じているため、「AI 導入＝コスト削減」と単純には捉えられないと感じている。	・顧客企業の傾向として、アタックサーフェスが広く、リスクの高い資産を保有している企業ほど、セキュリティ投資に積極的であると感じている。特に、EC サイトを運営している企業では、システム停止がそのまま業務停止につながるため、投資意欲が高い傾向にある。
セキュリティ人員の規模および動向に関するコメント	・セキュリティ人材は、経営管理側のガバナンス担当と、IT 側の技術担当の 2 つに大きく分かれる。総務も社員の PC 管理、物理的な入退室管理などのセキュリティ業務を兼務で担っている。 ・人材不足が一番の課題である。脅威の高まりに応じて、増員とスキルセット底上げの両軸で考えていく。専門性を高めたい分野には、専門部署の設置や、専門人材を配置しつつ、事業部を含む全員がセキュリティの知識を身に付けることが重要だと考えている。 ・既にグローバルチームでの情報共有は行っておりガバナンスを効かせやすくなっている。今後は技術面で協力していくために、グローバル人材の取り込みにも取り組みたい。	・現状の人員数は圧倒的に足りていないと感じる。社員を増やすのは難しいため、外部人材も活用している。海外採用の拡大や、専門人材の給与体系の作成にも着手している。 ・ペネトレーションテストや脅威インテリジェンス分析など、高度なスキルを持つ人材は一定数必要。一方で、現実的には各種施策を推進できる人材も不足しているため、採用のバランスが重要。 ・各事業部にセキュリティ専門人材を置くことはできていないが、システム構築においてセキュリティレビューを必須化しており、セキュリティ要件を満たしていないものは承認されず、是正を求める運用によってガバナンスを効かせている。	・セキュリティ管理者は、部門・事業単位で必要だと考え、配置している。 ・CISSP 保有者については「売上 100 億円あたり 1 名」という社内目標を設定し、事業部側でセキュリティの知見を有する人材を増加させた。 ・地政学リスクや AI 関連リスクなど、IT 部門だけでは対応できない局面が増加しており、他部門との連携スキルの必要性が増している。	・数年前からは、プロジェクトの規模やリスクレベルに応じて、セキュリティ教育を受けた人材を必ず配置するようにしている。これにより、現場レベルでのセキュリティ意識向上が進んでいる。 ・専門人材の確保については、短期的にエキスパートを増やすことは難しいとの認識のもと、脆弱性対応や監視といったルーチン業務は協力会社に委託することで、限られたリソースを戦略的業務に集中させている。

類型	社会インフラ		
企業	H 社	I 社	J 社
役職	CISO	情報セキュリティ部門長	コーポレート管理部門長
セキュリティ関連投資額の算出方法、経営層への説明方法に関するコメント	・セキュリティ投資は、IT 投資の中でセキュリティ関連投資として申請・確保している。インフラなど他部門と重複する部分は、セキュリティ部門ではなく、セキュリティ強化の目的であることを示したうえで、他部門で予算を確保している。 ・経営層はセキュリティの投資に積極的である。「データドリブン経営」を掲げているため、セキュリティは手を抜けないと感じていると思う。他方で、安定的なサービスの提供、人命と比べて投資対効果が妥当なのか、という議論が起きることもある。 ・セキュリティの投資効果は見せづらいため、経営層への説明においては他社のインシデント事例が最も効果がある。	・経営層はセキュリティ投資へ理解があり、インフラに関わる事業のため、サイバー攻撃により事業停止すると社会への影響が非常に大きいことを定性的に説明すると、投資の必要性は理解してもらえる。 ・経営層に定期的な報告をするために、セキュリティ投資額は日頃から可視化している。	・過去のインシデントの経験を踏まえ、経営層はセキュリティ対策に対して積極的で理解があり、予算獲得には苦労していない。
セキュリティ関連投資の動向に関するコメント	・すでにシステム障害でシステム停止した際には省庁に報告しているので、能動的サイバー防御法によって対策コストが跳ね上がることは現状ない見込みである。他方で、個人情報については、GDPR や個人情報保護法の改正により、ガイドラインに照らして報告する作業に負荷がかかっている。	・投資は増やしていきたいと感じている。投資を増やすうえでの課題はコスト面よりも人材不足である。 ・今後、自社で AI エージェントを開発することも目指し、DX 領域に関わるセキュリティ投資を強化している。AI を活用するためのセキュリティに関しては、経営層からも多くの課題が指摘されており、AI ガバナンスは今後、投資の重点分野になると思う。 ・経済安全保障法や能動的サイバー防御法など、インフラ事業者は新しいルールや規制を受けると感じている。特に、能動的サイバー防御法は、官民連携の強化で得られるメリットも期待できる一方、これまでになかった仕組みや対応が求められると考えている。	・グループ全体で共有しているシステムのセキュリティは、ホールディングス側で管理しており、自社では主に当該システムで管理しないデータに関するセキュリティを担当している。 ・デジタル化は積極的に進めようとしている。例えば AI、OCR を用いて顧客情報の突合を自動化できないか検討している。
セキュリティ人員の規模および動向に関するコメント	・全体として専任は少ない。セキュリティ専門人材は IT 業界を選んでしまうため、採用には苦労している。 ・人材不足への対応として、業務側の人材にセキュリティ知識をつけてもらうことが重要だと考えている。30-40 名程度のグループ単位で、数か月間の育成カリキュラムを継続的に実施している。 ・今後はデータガバナンスができる人材が必要である。具体的には、AI が生成したデータの中から異常値の検証ができる人や、AI のチューニングに必要なデータの加工・選別ができる人であり、業務知識を持つ人が必要だと感じている。また、野良クラウドや野良 AI が増えている中で、基本的なセキュリティを徹底する意味でも、業務・セキュリティ両面の知識を持った人が必要と感じる。 ・ログ分析などの定型業務はアウトソースで対応可能だが、どの領域に優先的に投資するかといった戦略判断は自社が主体的に定めるべきである。「何を任せ、何を自社で担うか」という目利きをすることも本社のセキュリティ人材の重要な役割であると認識している。	・人材確保には苦労している。キャリア採用を強化しているが、昨今はそれも厳しいため、若手から育てることも視野に入れて対応している。 ・今後は、法律対応も含めガバナンス対応のできる人材や、セキュリティ専門性の高い人材がバランスよく必要だと思う。セキュリティ専門性については社内教育だけでは難しいため、外部のプログラムなども活用している。 ・ルール整備、アセスメント、資産管理、共通基盤の運用は、本社が主体となってガバナンスを効かせていることで効率化できている面もあると感じる。	・セキュリティを専門とする人員はほぼいない。各拠点ごとに、ネットワークの責任者や、個人情報保護の責任者を任命しており、通常業務に加えて兼任でセキュリティを担っている。 ・理想をいえば IT 人材を増やしたいが、グループのシステムを利用しているため、個社でのセキュリティ含む IT 人材採用の優先度は高くない。また、採用数自体が限られているため、IT だけに人員を割くことは難しい。 ・DX を推進する部署がホールディングス側に設立され、グループ全体で人材育成に取り組んでいる。年に一度報告会があり、各社が取り組む DX の成果報告や評価を行っている。

類型	製造			
企業	K 社	L 社	M 社	N 社
役職	情報セキュリティ部門長	情報セキュリティ部門長	情報システム部門長 （情報セキュリティ機能の責任も持つ）	IT・DX 統括
セキュリティ関連投資額の算出方法、経営層への説明方法に関するコメント	・投資を確保しやすくするため、ネットワーク・インフラ・クラウド含め、セキュリティに関する予算は全てセキュリティ部門で管理している。 ・CIO と CISO が兼任の場合、DX や AI、SAP などの攻めの投資に偏りがちになるため、CISO は独立させた方が機能すると考えている。 ・社長が、サイバーセキュリティにおいて業界をリードする立場を目指すべきだという考えを持っているため、予算獲得には苦労していない。社外取締役からのセキュリティ強化に関する要望があることも、セキュリティ投資の確保に前向きに作用している。	・投資の確保において、経営層の説得に苦労することがある。 ・日本の社外取締役は、海外と比較してセキュリティへの関心が薄い傾向があるため、海外の社外取締役がいるかどうかも、セキュリティ予算の確保しやすさに影響すると感じている。 ・基本的にセキュリティ投資は全社で一括管理しているが、 工場セキュリティは一律の管理は現状難しく、情報セキュリティとは分けて投資を確保している。	・投資額は、必要対策を積み上げた金額をできるだけ確保していた。必要なセキュリティレベルと現状とのギャップが大きいと感じていたため、IT 予算の中でもセキュリティ関連費用は削減対象とせず、優先的に確保していた。セキュリティ投資額を IT 予算比で固定する考えはなく、リスクと必要性を基準に判断していた。	・投資額は、必要対策の積み上げに加え、同業他社のベンチマークおよび費用対効果の観点を組み合わせて決めている。 ・過去にインシデントが発生した領域については、再発防止の観点から対策の必要性を示すことで、経営層の理解が得られやすい。一方で、リスクがまだ顕在化していない領域については必要性を理解してもらうのが難しい場合もあり、そのような場合は他社の被害事例を引用しながら対策の必要性を説明している。
セキュリティ関連投資の動向に関するコメント	・製造業では、セキュリティレベルの高さが製品の信頼性を高め、競争力を高める差別化要因にもなると考えている。 ・業界全体として、グローバルと比較して日本のセキュリティ意識が低いと感じる。危機感を持ってグローバルの議論に参加することが必要。	・メーカーでは納期・品質が優先される傾向があり、セキュリティは専門組織がやるものという意識が根強い。セキュリティの民主化（従業員一人一人がセキュリティを自分事として捉えるカルチャーを作ること）が重要だと考え、グループのセキュリティ責任者に最新の脅威情報を共有したり、一般社員向けにホラーストーリーを紹介したりしている。 ・サプライチェーンリスクが高まっている。そのため、取引先も含め同じ目線でセキュリティに取り組むという意識、意見交換が重要である。 ・経済安保法、JC-STAR、サイバーレジリエンス法（CRA）などの制定により、With Security でない製品はサプライチェーンから外されるようになってきている。製造業にとってはセキュリティ強化の追い風となっていると感じる。	・数年前、海外の某大手製造業が大規模なランサムウェア被害により数か月操業停止に追い込まれた事例が、業界全体に大きな影響を与えた。同社が被害内容と対応策を同業他社に詳細に共有したことで、業界内の経営層の危機意識が一気に高まった。 ・セキュリティは建物の屋根のようなもの。屋根をつけることは当然で、重要なのは機能である。つまり、セキュリティとは「やる・やらない」や「いくらかけるか」の議論ではなく、事業継続性を確保するために必要な機能をどのように実装するかの議論であるべきだと感じている。	・DX 推進部が所管する IT 予算の中でセキュリティ関連費用を確保しているため、社内では「IT 投資に対するセキュリティ投資比率」も管理指標の一つとして活用している。 ・数年前のインシデントを契機に対策を進めており、対策完了まで継続的な投資を実施する計画である。 ・AI 技術の進展により攻撃手法が多様化し、セキュリティリスクは右肩上がりに上昇している。投資拡大の必要性を認識しつつも、最新脅威に伴う潜在的損失や対策効果は定量化することが難しいため、投資額を増やすことに難しさを感じている。
セキュリティ人員の規模および動向に関するコメント	・SOC の一部、脅威インテリジェンス、フォレンジック、問い合わせ窓口はアウトソースしているが、それ以外は基本的に内製化している。 ・各国の拠点で、事業部側にもセキュリティ専任をそれぞれ数人ずつ配置し、報告は本社の情報セキュリティ部に集約している。 ・東京以外でセキュリティ人材を確保するのは非常に難しい。地方工場には出向という形で配置したり、現地で業務委託したりして対応している。 ・人材のローテーションが前提となっている業界では、サイバーセキュリティの専門人材が育ちにくい、という課題がある。また、専門性を高めようとしても異動によってキャリアが分断されやすく、その結果、専門性を重視する人材ほど転職を選択してしまう傾向がある。セキュリティは継続的な経験と知見の蓄積が不可欠である、という意識を組織として明確にすることが重要である。	・現状、セキュリティ専任は少数であり、各部門で数名が兼任でセキュリティも担っている形である。理想的には、指示された対策に留まらず何が必要かを選択できる人材＝セキュリティ専門人材の強化が必要だと考えている。また社内セキュリティと事業セキュリティの両者を考えられる、セキュリティの責任者を設置することが望ましい。 ・AI の広まりにより、コンプライアンスやセキュリティのリスクを併せて考える必要性が高まっており、あらゆるリスクを統括するリスク管理体制を作りたいと考えている。 ・一方で、現在の日本において、外部から人材を確保することは難しい状況である。日本企業と外資企業の給与水準の違いはその一因である。そのため、社内育成が重要であり、開発・生産の人員の中で、プラス・セキュリティ人材を育成するべく、資格・認定制度を整備し運用している。 ・プロアクティブな防御などは事業会社で行うのは困難であり、業務内容によってはアウトソースの活用も必要である。	・アウトソースを積極的に活用することで、限られた社員で対応していた。24 時間継続性・反復性の高い領域や専門性の高い領域を事業会社の社員で実施する必要はないと考え、社員は意思決定や連携、およびアウトソース先への事業の意識づけ（ただシステムセキュリティを見ているわけではない）に注力していた。	・昨年、本社にセキュリティ専任チームを立ち上げ、既存の人員を再配置するとともに専門性を持つ人材を集約したことは、一つの工夫といえる。一方で、セキュリティに特化した人材の新規採用には苦労している。 ・本部レベルでは体制は一定の水準に達していると感じているため、今後は各拠点のセキュリティ担当者の配置を強化したい。

類型	製造			
企業	O 社	P 社	Q 社	R 社
役職	情報セキュリティ部門長	情報セキュリティ部門長	CIO	CISO
セキュリティ関連投資額の算出方法、経営層への説明方法に関するコメント	・経営層の説得に苦労する場面もある。製造業では費用対効果という考え方が浸透しているため、損害額に対する投資として妥当なのかわからない、というコメントを受けることがある。数値だけでは経営層は妥当性を判断できないため、社外の脅威に対してどれくらい対策が打てているかを見せるように対応していく。 ・以前、経営者から「セキュリティはいつまでに何をやればいいかわからない」という指摘があった。そこで、サイバー経営ガイドライン（経済産業省）を参考に現状のレベルを数値化し、目標水準との差分を経営課題として抽出して経営層に提示し、アクションを取っている。	・インシデントが起きた直後は、セキュリティに対する経営層の意識が非常に高まるが、時間が経つと意識が薄れがちであり、風化させない取り組みが重要である。	・投資額は、リスクベースでの必要施策の積み上げや、他社のベンチマークを組み合わせて複合的に決めている。 ・インシデント発生以来、セキュリティ予算は確保しやすい状況になっている。今後はインシデント対策だけでなく、外部アセスメントを入れながら対策を検討していくフェーズだと認識している。 ・経営層はセキュリティに肯定的だが、コスト面の制約はあるため、セキュリティ以外の IT 予算を効率化、圧縮してセキュリティにお金をかけていきたいと考えている。	・経営層はセキュリティ投資への理解はある。事業特性から、供給が止まると社会への影響が大きいため説得しやすい。また、ERM（エンタープライズリスクマネジメント）の手法が導入されており、「事象が発生した場合の影響」、「発生確率」、「影響を及ぼすまでのスピード」などの要素で自社に関係するリスクの大きさを比較しているため、リスクの大きいセキュリティが優先的に対応すべき対象であることは説明しやすい。 ・とはいえ、投資額が高すぎるのではないかという議論は生じるため、目指すレベルを成熟度で表し、極端に高い水準を目指しているわけではなく、現状から目標水準に引き上げるための必要額であることを示して説明している。ベンチマークとして、外部の調査データや、他企業との情報交換も参考にしている。 ・経営層からは中長期的なリソースの全体像を求められるが、現実的には資産管理を終える前に順次対策を始める必要があるため、把握が進むにつれ追加費用を申請せざるを得ないことが、説明の難しさにつながっている。
セキュリティ関連投資の動向に関するコメント	・投資の変化として、セキュリティ脅威への対策に対する理解と受容が進んできたと感じている。例えば、メール訓練の外部ツールを使うことについても経営層の理解が得られるようになった。ネットワーク監視でも AI を活用したシステムを導入することの承認が得られ、不要なアラートの削減と、それに伴う担当者の負担軽減が実現しつつある。 ・最近の新たな課題としては、社員による AI 利用に伴う情報流出やシャドーAI といったセキュリティリスクが挙げられる。これに対応するため、社内での利用ガイドラインの整備や、ガードレールとなる仕組みの導入について検討を進めている。	・国家的な背景から、経済の混乱に直結する電力会社や工場が狙われやすくなっている。また、OT デバイスをネットワークに繋げるようになりアタックサーフェスが増えているため、OT セキュリティは世の中のベースインフラになると感じている。 ・今後は、サプライチェーンセキュリティがより重要になっていくと感じているため、経産省の評価制度を活用し強化していきたい。	・事業部門ごとに何を最も守りたいのかを明確にし、優先度をつけて守ることが重要である。各部門の資産の重要性をグローバルで横串で比較することで、ガバナンスを効かせながら効果的な対策を実施できる。 ・誰でも簡単に攻撃できるようになり、全ての攻撃を防ぎきることは難しいため、自社の特に守る必要がある部分を決め、そこにフォーカスして攻撃を確実に検知することに重きを置いている。 ・アナログの方が低コストで保護できる場合もある。GenAI の広まりによりセキュリティにおいても人間の役割は変化しており、人間が介在する意味を考えてデジタルとアナログを混ぜて対策をすることが重要である。	・IT ソリューションやアウトソースの費用はセキュリティとその他の費用を明確に切り分けられないため、従来はセキュリティ関連投資を把握するのに苦労していた。完全に正確である必要はないと考え、FW はセキュリティ投資、Office ソフトウェアは一定の割合をセキュリティ投資とする、などと暫定的な定義を決めることで、この 1 年ほどで大枠を把握できるようになった。 ・従来はサイバー攻撃対策としてシステム防御にコストをかけてきたが、今後、情報管理やデータガバナンスにも注力する必要がある。データの所在と信頼性を明確にすることは、インシデント発生時に情報単位で被害評価をする、および AI に自社のデータを学習させていくためにも重要になる。
セキュリティ人員の規模および動向に関するコメント	・人材不足については、採用と教育の両面で対応している。 ・事業部側のセキュリティ人材育成については、事業部にもトップダウンでセキュリティ担当者を配置し、教育を実施している。具体的には、社内セキュリティ部門が独自の資格制度を設け、知識の底上げを行っている。 ・本社のセキュリティ部門は特に、多部門との連携が必要であるため、プロジェクトマネジメント（PM）ができる人材が必要である。セキュリティと PM の両知識を持つ人材は少ないため、PM スキルを持つ又は、素養の有る人材にセキュリティ教育をすることを優先している。	・企画戦略を担ったり責任を取ったりする中央組織の専任人材はもちろん増強したい。加えて、現場の担当者も、中央組織と連携しながらセキュリティを実装していくことが必要であるため、知識の底上げをしたい。 ・人材不足に対しては、スキルを持つ人材の獲得と社内での育成の両面から対応している。社内育成としては、内部の人材育成プログラムを立ち上げているほか、IPA 中核人材育成プログラムを活用している。人材のローテーションを行い、各組織にデジタル人材を置くようにしている。 ・各国の規制強化によりセキュリティを個社の責任にはできなくなっているため、将来的には情報セキュリティ部門がグループ全体にガバナンスを効かせる体制を目指している。	・人数自体は理想値と近く、大きく増やす予定はないが、高い専門性を持つ人材の確保が課題である。事業会社にはエンジニアリングなどの技術力を持つセキュリティ人材が集まりにくいため、採用・育成ともに苦労している。 ・パートナー企業に任せきりにならないよう、コントロールできる人材が社内に必要。SOC の運用などはアウトソースしているが、社員が内容を把握していることが重要である。 ・少ない人数で必要なセキュリティを実施するため、グローバルでの IT 部門の統合などにより、効率化とセキュリティ強化の両立を目指している。	・データガバナンスのスキルを持つ人員が足りていない。製造から IT サービスに事業を広げていく、今後 AI を活用していく中で、データガバナンスのスキルが必要である。 ・外部活用はバランスが重要である。労働力としては外部活用も必要だが、外部に任せすぎると品質を担保できないため、品質管理は社内で責任を持たなければならないと思っている。 ・社員に求められるスキルセットとアウトソースに求められるスキルセットは全く異なるため、その違いを考慮した教育・育成が重要である。 ・グローバル観点では、拠点ごとの CISO はコミュニケーション能力が高い人を選定し、その下に配置する人員はあえて少なくしている。責任範囲を明確化し、密なコミュニケーションを前提とした運営を行い、ガバナンスを効かせている。

類型	小売・サービス・その他		中堅	
企業	S 社	T 社	U 社	V 社
役職	CIO	IT・DX 統括	情報システム部門長	IT・DX 統括
セキュリティ関連投資額の算出方法、経営層への説明方法に関するコメント	・投資方針を決めるうえでは、まずリスクアセスメントを実施し、自社のどの部分が攻撃を受けやすいかを可視化したうえで、リスクの内容に応じて優先順位をつけて対策を講じるのが重要である。 ・経営層がセキュリティ投資のみならず、IT 全体の投資に関する理解をすることが重要であると感じている。	・セキュリティ投資は、費用対効果を定量的に説明することは難しいため、常に世の中の最新情報を把握し、対策を取るべき部分とリスクを許容する部分を都度判断している。	・投資額は必要な対策の積み上げ方式で決めている。 ・経営層への説明の際には「投資を行わなかった場合にどのような影響が生じるか」を定性的に示すことで理解を得ている。	・投資額はリスクベースで決めている。セキュリティリスクが増しているため、実態として年々金額は増加している。 ・IT 全体の投資額については経営層と議論するが、セキュリティの投資額に関しては担当理事に一任されている。 ・事業特性から、経営層からの IT、セキュリティに対する要求レベルは高い。ただし、「ビジネスのためのセキュリティ」であることを忘れず、セキュリティが足かせとなることのないよう、ビジネスに必要なセキュリティ対策を取る方針としており、DX とセキュリティのバランスを重視している。
セキュリティ関連投資の動向に関するコメント	・取引先が多岐にわたる業態では、サプライチェーン全体のセキュリティ対策が重要な課題である。システムを共有していなくても、サプライヤ側のサイバー攻撃が自社の生産や供給に影響を及ぼすリスクもある。取引先に任せず、本社が責任をもってセキュリティ対策を進められれば良いが、現実的には取引先任せの企業も多いのが実態であると感じる。	・今後もリスクは高まると考えているが、セキュリティ対策は上限がないため、投資額は闇雲に増やさずに自社のリスクに見合ったセキュリティ対策を取る予定である。 ・昨今の脅威は一般企業が自社だけで守れるものではないため、ほぼ 100%外部サービスを活用している。日々変化するセキュリティリスクに対し、随時機能追加してくれるようなモデルでないと対応しきれない。 ・近年はリスクの高まりだけでなく、円高の影響を受けて投資額が高くなっている。	・製造業ではまず「人の命を守る安全対策」が最優先であり、セキュリティ対策はその次の優先度とされている。安全対策には惜しみなく投資する一方、セキュリティは限られた予算の中で取捨選択を迫られているのが実情である。	・システム規模やグローバル展開の状況を踏まえたうえで、どの領域に、どの程度のセキュリティ対策を講じるかを見極めることが重要である。
セキュリティ人員の規模および動向に関するコメント	・小売業や製造業では、規模によってセキュリティ専任の人材が置かれていない企業も存在する。そうすると、管理・統制する人員も限られるため、アウトソースを含めても総量が少なくなる。 ・特に、海外グループ企業では、人員が非常に限られており、ごく少人数で全分野を担っていることも多い。セキュリティ担当者がいない拠点もあり、不安で、人数を増やしたいが、現地法人の管理下のため口出しできないのが現状である。 ・セキュリティ部門に任せきりになることを防ぐために、意図的に中央集権的に人を置くことを避けている。相談役や CSIRT としては機能するが、各々がセキュリティの考えを持って進めるようにしている。	・セキュリティの専門会社ではないため、人材を急激に増やすことは考えていない。人海戦術の方が脆弱だと考えており、外部活用、ツールによる自動化などにより、少ない人数で対応できるように工夫してきた。 ・海外子会社では日本以上にセキュリティ人材の採用が難しく、専任はほぼいない。 ・対策の不十分なところがリスクとならないよう、グローバル全体の底上げを意識している。具体的には、ツールをグローバルで統合し、日本の SOC で集中監視しているほか、本社から定期的に教育や脆弱性検知を行っている。	・中堅規模の企業では、売上比率や社員数比でリソースを設定するのは難しく、段階ごとの目安を置くのがよいと感じている。まずは総務・経理部門が存在する規模の企業であれば、少なくとも IT 専任者を 1 名配置すべきだと考えている。IT・セキュリティを理解して戦略を立てられる人が不在のままツールのみを導入しても効果は期待できない。専任者を配置することの意義を、経営層に理解してもらうことが何より重要である。	・当社の方針として、各部門少数精鋭で構成する方針の下、特に共通部門はスリム化が前提となっており、今後も人を大きく増やす予定はない。 ・通常時は数名がセキュリティを兼任、インシデントが起きた際には現場のメンバーも動く体制となっている。 ・セキュリティに関してどのような人材が必要かを判断できる人が 1 人でもいることが重要である。採用をエージェントに任せきりにすると期待に合わないこともある。



[本調査に関する照会先]

プロジェクト主任研究員　山田沙也佳 yamada@j-cic.com

プロジェクト研究員　西井菜緒 nishii@j-cic.com

主任研究員　上杉謙二 uesugi@j-cic.com

JCIC 事務局　info@j-cic.com