Google

日本社会における
サイバーセキュリティの課題と方策

by Google サイバーセキュリティ研究拠点

「日本社会におけるサイバーセキュリティの課題と方策」発行に寄せて

「デジタルの世界を安全で、自由で、公正な場所にするために」

Google 日本法人 代表
奥山 真司

Google は創業以来、「世界中の情報を整理し、世界中の人がアクセスして使えるようにすること」というミッションのもと、テクノロジーによる社会課題の解決に向けて歩んできました。日本においても「AI の力で解き放とう、日本の可能性」というビジョンを掲げ、個人の可能性の開花、持続可能な経済成長、そして複雑な社会課題の解決に貢献するべく取り組んでいます。

しかし今、私たちは技術と社会の大きな転換点に立っています。AI がかつてない速度で進化し、私たちの生活に多大な恩恵をもたらすと共に、社会の在り方を根本から変えようとしています。テクノロジーの進化に伴い社会・経済活動の基盤がデジタルへ移行している今日、サイバー空間の脅威もまた複雑化・多様化の一途を辿っています。

このような状況下において、断片的な対策のみで複雑な脅威に対抗することはもはや困難です。だからこそ Google は、包括的な防御を可能にする「フルスタック・アプローチ」によるレジリエンスの構築に取り組んでいます。海底ケーブルなどの物理インフラから、クラウド、AI モデル、そしてアプリケーションに至るすべての階層にセキュリティを組み込み、デジタル世界を統合的に保護するアプローチです。誰もが安心してテクノロジーの恩恵を享受できるデジタル社会の基盤を守り抜くことに、Google は重い責任があると考えています。

この思いのもと、Google は 2024 年 3 月、東京に「サイバーセキュリティ研究拠点」を設立し、日本およびアジア太平洋地域におけるレジリエンス向上を目指し「政策対話」「人材育成」「研究支援」の 3 本柱を軸に活動を展開してきました。さらに 2025 年 3 月には、より体系的で包括的なセキュリティ強化を推進すべく、本拠点が発起人となり「Japan Cybersecurity Initiative (JCI)」を発足しました。

このイニシアティブの柱として、JCI ではサイバーセキュリティの最新動向や政策課題を深く議論し、実効性のある対応策を検討する産学官の有識者会議を定期開催しています。本レポートは、一連の議論やインサイトを基軸に独自調査を交え、日本社会の強靭化に向けた産学官連携の在り方と今後の課題を取りまとめました。サイバーセキュリティの課題は技術的な対策に限定されず、社会全体の意識変革、組織体制、人材育成など全方位的なアプローチが不可欠です。業界の垣根を越え、産学官がより一層一体となってエコシステム全体の安全性を高める努力が今まさに求められています。

本レポートが、日本のサイバーセキュリティの底上げに向けた実効性のある議論を加速させ、安全で自由かつ公正なデジタル社会を共創していくための一助となれば幸いです。

「AI 前提時代」を支える サイバーセキュリティと 日本の責任

Japan Cybersecurity Initiative (JCI) 有識者会議 座長
慶應義塾大学 特別特区特任教授
村井 純氏

日本のサイバーセキュリティを取り巻く環境が大きく変化するなか、2025 年度に有識者による議論の場として開催された有識者会議は、極めて象徴的なタイミングで実施された取り組みでした。5 年前、COVID-19 を契機に DX が社会全体で急速に進展し、デジタル技術は一部の専門領域ではなく、国民一人ひとりの生活や経済活動の基盤となりました。同時に、サプライチェーンの複雑化や重要インフラを含むオペレーション領域への攻撃など、サイバーセキュリティの影響範囲は大きく広がっています。あれから 5 年、もはや、「自分は関係ない」と言える領域が無くなり、社会のあらゆる主体が向き合うべき課題となりました。こうした転換点において本会議が開催されたこと自体が、非常にタイムリーで意義深いものでした。

さらに現在は、AI が社会の前提となる段階に入りつつあります。私はこれを「AI 時代」ではなく「AI 前提時代」と称しています。特別な存在として時代を主導するのではなく、インターネットがあらゆる生活やサービスの前提となった状況と同様に、AI が社会の基盤として存在する環境が形成されていくためです。この社会では、安心して安全にデータを共有し活用できるデジタル環境が不可欠となります。その意味でサイバーセキュリティは、単なる防御技術ではなく、デジタル社会の信頼を支える基盤そのものです。技術の進化と共に悪用・濫用も生まれる以上、技術的対策と社会制度の双方から、持続的に対応していく必要があります。

本会議の大きな特徴は、こうした課題を人間の視点から議論したことにあります。サイバーセキュリティに関する会議は通常、国家戦略や制度設計、あるいは専門家コミュニティの、いわゆるサプライサイドに議論の焦点が当たりがちです。しかし本会議では、「国民意識」「経営」「人材のすそ野拡大」というテーマのもと、ユーザーやビジネス現場の視点から議論が展開されました。すなわち、一人ひとりの立場からサイバーセキュリティを考えるというアプローチです。これは、これまでのセキュリティ関連の会議体ではあまり見られないユニークで意義ある試みであり、かつ Google らしい取り組みであると感じています。また、グローバル企業である Google が日本のサイバーセキュリティという課題に向き合い、議論の場を設けたことも印象的でした。国際的な視点と日本社会の課題を接続して議論を進めることで、新しい視点が生まれたことを実感しました。

そして今後、日本のデジタル社会を支えていく若い世代に伝えたいメッセージがあります。それは特別に難しいものではなく、「好きなことを徹底的にやってほしい」ということです。AI 前提の社会では、知識を一方的に伝達する教育だけでなく、個々の関心や強みを持ち寄り、新しい課題に挑戦していく創造的な連携が重要になります。個人が本当に夢中になることに挑戦し、その取り組みが組み合わさることで新しい価値が生まれる。そうした環境こそが、これからの AI 前提時代を支える力になるのです。

安心して安全にデータを活用できる環境を整えることは、テクノロジーの精度や品質を誇る日本社会にとって重要な責任です。本会議での議論が、その実現に向けた一歩となることを期待しています。

INDEX

JCI

「Japan Cybersecurity Initiative」について

社会全体のサイバーセキュリティ底上げに向けた、3 つの重点領域

国内で大手企業や重要インフラを標的としたサイバー攻撃が増加するなか、社会全体で実効性のある対策を講じることは喫緊の課題です。特に、エネルギー、通信、金融といった基幹インフラへの攻撃は、社会機能の麻痺や経済活動の停滞を招き、国民生活の根幹を揺るがしかねません。この脅威に対処するためには、国民一人ひとりがサイバーセキュリティを「自分ごと」として捉え、産学官が密に連携し、強靭な体制を構築していくことが不可欠です。

このような課題を背景に、2025 年 3 月、Google サイバーセキュリティ研究拠点を主幹として発足した「Japan Cybersecurity Initiative（JCI）」では、主に以下 3 つの柱を軸に活動を展開しています。

1 産学官の有識者会議の開催

多様な専門家による産学官の有識者会議では、産学官の枠組みを超えて知見や最新事例を共有し、課題抽出から解決策の検討までを進めています。「国民の意識向上」「経営者が取り組むべきサイバーセキュリティ」「サイバーセキュリティ人材のすそ野拡大」を重点テーマに据えた議論の詳細および関連調査の結果については、本レポートの 7〜41 ページに掲載しています。

2 経済産業省と連携した全国の中小企業向けの普及活動の実施

日本企業の 99.7%を占め、サプライチェーン全体の安全確保に不可欠な中小企業に対し、経済産業省との連携のもと、普及活動を展開しています。経済産業省の「実践的方策ガイド β 版」に準拠した無料オンライントレーニングプログラムを開発し、全国の中小企業へ対面での無償トレーニング提供も行っています。

3 最新のサイバーセキュリティに関する情報共有・専門人材育成支援

高度化・巧妙化する脅威に対処するため、パートナー企業・団体への支援を展開しています。Google Threat Intelligence や Mandiant による最新の脅威インテリジェンスの提供、サイバーセキュリティ分野で即戦力として活躍するためのスキルを習得できる「Google サイバーセキュリティプロフェッショナル認定証」講座の無償提供（5,000 枠限定）に加え、国内外の最新動向を解析し、実効性のある戦略策定を支援するセミナーやワークショップを開催しています。

産学官で安心・安全なデジタル社会の構築を目指す

社会全体のサイバーセキュリティの底上げは、日本経済の持続的発展に不可欠な礎です。JCI は、産学官の協働により、安心・安全な日本のデジタル社会の構築に貢献することを目指し、取り組みを推進していきます。

第１回

会議テーマ

国民の意識向上

第１回

サイバーセキュリティの「自分ごと化」へ

定着に向けた３つのアプローチ

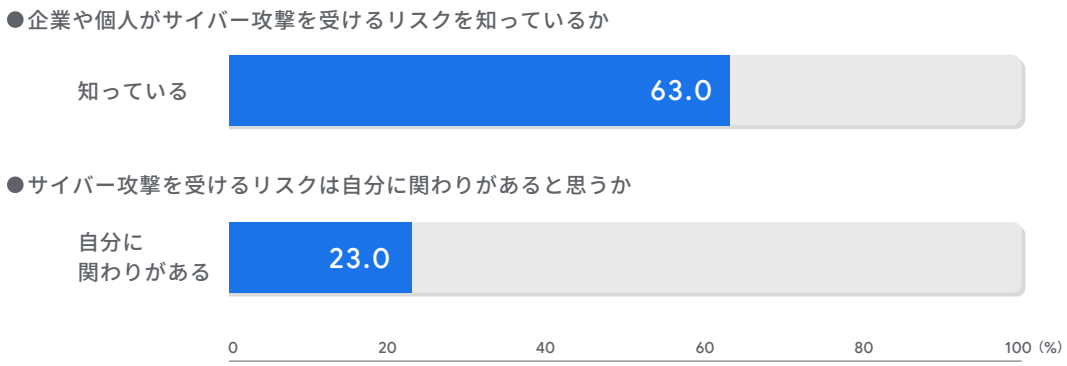
近年、システム障害による業務停止や物流遅延などの事案が相次ぎ、サイバーセキュリティへの関心は着実に高まっています。「企業や個人がサイバー攻撃を受けるリスクを知っているか」という設問（図１）で「知っている」と回答した人は 63.0%でした。一方で、上記のリスクについて「自分に関わりがある」と回答したのは認知者中の 36.4%（調査対象者全体の 23.0%）に留まっていることから、**リスクの認知は一定程度進んでいるものの、日常生活や業務との具体的な接点として十分に認識・対応されている状況ではない**といえます。加えて、サイバー空間は国境を越えて広がるグローバルな領域であり、国内の出来事も海外の動向と密接に結びついています。こうした特性を踏まえ、サイバーセキュリティの「自分ごと化」には、地球規模での視野から日本の状況を捉える意識も重要となります。

有識者会議では、**国民の認知と行動のギャップをどう埋めるか**が主要な論点となり、一人ひとりがサイバーセキュリティを身近な課題として理解することが、社会全体の安全性向上に寄与するとの見解が多く示されました。

そこでサイバーセキュリティ研究拠点では、国民のサイバーセキュリティの「自分ごと化」に向けて「周知」「浸透」「制度化」の 3 つの観点を軸に、今後検討が期待される具体的な方向性を提起します。

図１　リスクを「自分ごと化」できていない

「企業や個人がサイバー攻撃を受けるリスクを知っているか」との質問に対し、63.0%がリスクを「知っている」と回答。一方で、「自分に関わりがある」との認識は 認知者中の 36.4%（調査対象者全体の 23.0%）に留まった。リスクの存在は理解されているものの、当事者意識の形成には課題がある。



JCI「サイバーセキュリティ調査（第 1 回）」より。日本国内在住の 12 歳～60 歳、計 2,000 人を対象にオンラインで 2025 年 11 月実施

❶「周知」一人ひとりへ認知を広げる

有識者会議での議論では、サイバーセキュリティに対する関心が高くない層にどう情報を届けるかが大きな論点となりました。
その第一段階として、「サイバーセキュリティ対策を怠ると、自分にどのような被害が及ぶのか」という基本情報を、分かりやすく伝える取り組みの必要性が指摘されています。

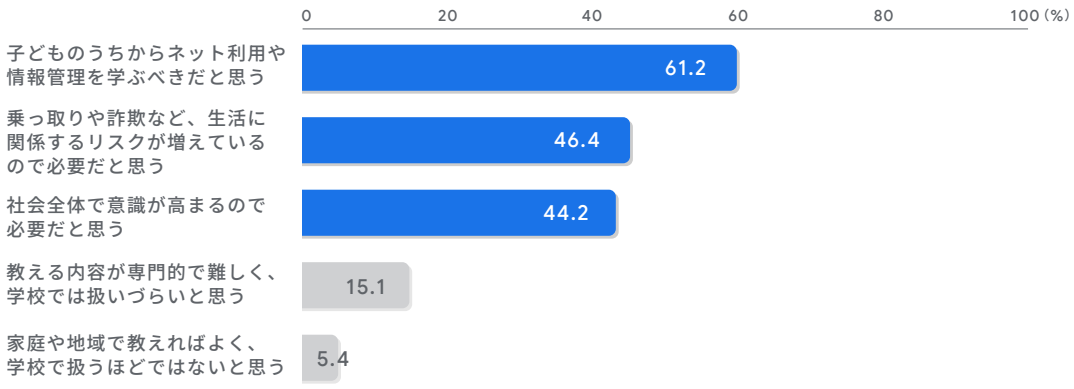
交通安全教育が示すロールモデル

有識者会議では、IT 分野に限らず、幅広い層が日常的にサイバーセキュリティ関連情報に接する環境づくりの重要性が強調されました。**専門知識としてではなく、生活に根ざした基礎的リテラシーとして位置づける視点**です。

参考事例として挙げられるのが、日本における交通安全教育の取り組みです。1970 年代には年間 1 万 6,000 人を超える交通事故死者が発生していましたが、国を挙げた事故防止施策や啓発活動が進められ、犠牲者の数は大幅に減少しました。そのなかで、警察と学校が連携して実施した交通安全教室は重要な役割を果たしたとされています。

現在、交通安全は幼稚園教育要領から高等学校の学習指導要領まで段階的に組み込まれ、反復的に学ぶ機会が設けられています。JCI の調査において、サイバーセキュリティを義務教育のカリキュラムに組み込むことへの見解を問うたところ、「子どものうちからネット利用や情報管理を学ぶべき（61.2%）」「乗っ取りや詐欺など生活に関係するリスクが増えているので必要（46.4%）」といった意見が多く聞かれました。この回答結果から、交通安全と同様に、**学校教育においてサイバーセキュリティ教育をより充実させていくことへの期待**が見て取れます。一方で、「内容が専門的で難しく、学校では扱いづらいと思う（15.1%）」という懸念も散見されており、テーマ選定や難易度の設定には十分な検討が必要といえます（図 2）。

図 2　サイバーセキュリティを学校教育に組み込むことに対する認識（複数回答）



JCI「サイバーセキュリティ調査（第 1 回）」より。日本国内在住の 12 歳～60 歳、計 2,000 人を対象にオンラインで 2025 年 11 月実施

また、特定の IT 関連科目に限定せず、あらゆる進路を選択する児童・生徒が触れられる設計とすることが重要といえます。その点においても、交通安全教育の取り組みがロールモデルになるとの見解が示され、併せて教員の負担を考慮し、外部機関との連携を図ることも方策として挙げられました。

近年、警察組織ではサイバー犯罪対策に関する専門教育が強化されています。こうした専門人材が学校や地域に出向き、自治体と連携した啓発活動を行うことで、サイバーセキュリティに関する情報との接触機会の拡充が期待されます。

デジタルサイネージなどの活用で不特定多数に伝える

学校教育以外にも、市民が日常的に利用する公共施設や生活拠点における情報提供の可能性が議論されました。

一例として、郵便局や医療機関の待合スペースなどに設置されているデジタルサイネージの活用が挙げられます。**不特定多数が接触する媒体を通じて基本的な注意喚起や対策情報を発信する**ことは、サイバーセキュリティを日常生活の文脈に位置付ける有効な手段となります。

❷「浸透」響く言葉で認識を深める

会議では、情報を届けるだけでなく、受け手にとって理解しやすく、行動に結びつきやすい表現を工夫する必要性も議論されました。用語の選択やメッセージの設計は、「自分ごと化」を促進する上で重要な視点となります。

「オタク」→「推し活」でポジティブに、「電話での詐欺」→「オレオレ詐欺」で伝わりやすく。「サイバーセキュリティ」→ どう伝えるか

JCI の調査では、「サイバーセキュリティ」という言葉に「印象がない」と回答した人、つまり具体的な印象を持たない層の存在が明らかになっています。

この点について、有識者会議では、**専門的に聞こえる用語をより直感的な言葉へ置き換える、あるいは補助的な呼称を併用するアプローチ**が提案されています。

言葉の転換によって社会的受容が変化した例として、「推し活」という表現が挙げられます。従来は「オタク」という語が持っていたニュアンスが、新しい呼称の浸透によってポジティブに再解釈された側面があります。また、犯罪手口を端的に表現した「オレオレ詐欺」という呼称は、直感的な理解を促し、社会的な警戒心を高める一因となりました。

これらを踏まえ、「サイバーセキュリティ」という言葉に対し、例えば「ネット安全」といった補助的で分かりやすい呼称を併用することも、「自分ごと化」を促す有効な手法と考えられます。

総務省や情報通信研究機構によるプロジェクト「NOTICE」では、「さあ！ネットにも戸締まりを。」という表現を用いて日常行為に例えることで理解促進を図っており、このような比喩的表現の活用も参考事例として共有されました。

言葉のインパクトと伝えるタイミングが重要

有識者会議では、メッセージの内容だけでなく、その表現方法や提示の仕方も、行動変容に影響を与える要素として議論されました。状況によっては、あえて印象に残る強い言い回しを用いることが有効に機能する場合もあると考えられます。

例えば、金融機関を装って偽サイトへ誘導するフィッシング詐欺が広がるなか、「メール内容を確認しましょう」「詐欺に注意しましょう」といった一般的な呼びかけだけでは、注意喚起として十分に機能しない可能性があります。

JCI の調査で、11 種の異なる表現を用いた注意喚起を例示し「とるべき行動をよりイメージしやすいのは、どのような表現の注意喚起か」を質問したところ、推奨される行動の記載や、避けるべき行動の警告など**「受け手の解釈に左右されないほど具体的に示したメッセージが分かりやすい」**と評価される傾向が確認されました。一方で、とるべき行動が曖昧でイメージしづらい表現は下位となる傾向がありました（図 3）。

さらに、メッセージを伝える手段やタイミングについても検討の余地があります。例えば、日本郵便が提供するレターパックでは、品名欄に「『レターパックで現金送れ』はすべて詐欺です※1」と赤字で注意書きが記載されていることで、利用者が実際に発送作業を行う直前に目に入る設計となっており、行動とメッセージが接続されているといえます。

このように、言葉の選び方だけでなく、「どの場面で」「どの媒体を通じて」届けるかを含めて設計することが、施策の浸透度に影響を及ぼす要素となります。

図 3　伝わりやすいリスク喚起メッセージの方向性

「怪しいなと思ったら、開かない」－それが一番のセキュリティ対策です	46.0%
不審なリンクは絶対に開かないでください	38.6%
99%の詐欺メールが「本物そっくり」に作られています	36.9%
「本当にそのメール、信じられますか？」クリックする前に、3 秒だけ疑う習慣を	31.2%
怪しいメールは即削除！開けば終わり	30.8%
あなたの 1 クリックが、家族や会社全体を危険にさらすかもしれません	20.6%
クリック詐欺で全財産が溶ける！一瞬の判断が命取り	19.6%
「うっかりクリック」は誰にでも起こる。だからこそクリックしないルールを自分に	19.6%
添付ファイルは送信元を確認してから開いた方が安全です	18.6%
「開いてみたらウイルスだった」－後悔する前に止まる勇気を	18.6%
“社長からの依頼メール”でも添付を開く前に確認を	13.4%

JCI「サイバーセキュリティ調査（第 1 回）」より。日本国内在住の 12 歳～60 歳、計 2,000 人を対象にオンラインで 2025 年 11 月実施

※1 2026 年 2 月現在

❸「制度化」ルール整備で行動を促す

会議では、**意識向上や自主的取り組みに加え、法律を含めた制度やルールの整備を通じて行動変容を後押しする視点**についても議論が行われました。制度設計の在り方については、社会的受容や実効性を踏まえた慎重な検討が前提となります。

「安全運転管理者制度」を参考にルールづくりへ

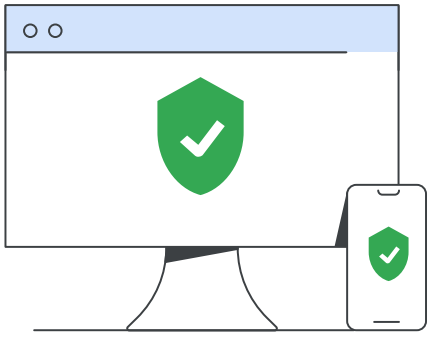
参考事例として挙げられるのが、道路交通法に基づく「安全運転管理者制度」です。これは、一定台数以上の自動車を保有する事業者に対し、安全運転管理者の選任や教育実施を義務付ける仕組みです。

こうした制度設計を応用し、**一定規模以上の IT 機器を保有する事業者に対し、サイバーセキュリティ管理責任者の設置や定期的な教育実施を求める枠組み**の検討も期待されます。

ライセンス制度も有効に機能する

また、パソコンやスマートフォンの購入時、あるいはインターネット契約時に、基本的なセキュリティ知識を学ぶ機会を設ける「ライセンス型」の仕組みも一案と考えられます。運用主体や厳格性など検討事項は多いものの、日常の接点に学習機会を組み込む発想は実効性を有します。

こうした仕組みを通じて、利用者である消費者一人ひとりがセキュリティ対策や製品・サービスの安全性に関心を持ち、そのセキュリティ性能を選択の一つの基準として捉える意識が求められます。**消費者の意識が変化していくことで、企業に対してもセキュリティ品質の向上を促す動きに繋がり、市場全体の安全性を高めていく循環を生み出します。**制度を起点に、学び・意識・選択が繋がっていくことで、サイバーセキュリティを社会全体で支える基盤が築かれていくことが見込まれます。

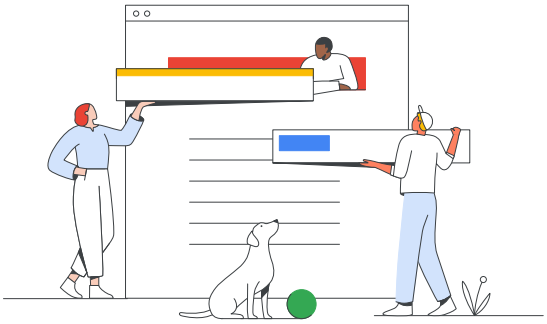


社会全体で取り組む「自分ごと化」

サイバーセキュリティ研究拠点では、これまでの有識者会議および調査結果を踏まえ、「周知」「浸透」「制度化」の 3 つの観点から今後の方向性を提起しました。

会議では、近年のサイバー空間をめぐる脅威が高度化する一方で、個人レベルでの対策は不十分というギャップを埋める鍵として、国民一人ひとりの「自分ごと化」が重要であるとの認識で一致しました。インターネットが社会生活の基盤となった現在、その安全性は個人の生活のみならず、家族や所属組織、ひいては社会全体の安定とも密接に関連しています。

本レポートで整理した 3 つの観点は、こうした状況を踏まえ、サイバーセキュリティをより身近なものとして捉える環境をどのように整えていくかという問いに対する一つの方向性を提示するものです。今後も、社会全体での対話と検討を重ねながら、持続的な取り組みを推進してまいります。



Column

セキュリティ性能を可視化する「適合評価制度」にも着目

経済産業省と独立行政法人 情報処理推進機構（IPA）が創設した「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」は、制度化の一例として挙げられます。

同制度では、IoT 関連製品のセキュリティ性能を独自基準に基づき 4 段階で評価し、ラベル表示を行います。これにより、製品の購入を検討する消費者や企業が、その安全性を明確に判別できる仕組みとなっています。

現時点では対象製品が限定的ですが、客観的で分かりやすい評価軸が整備されることにより、消費者が製品の購入を検討する際、セキュリティについて考える機会が生じます。このことがセキュリティの「自分ごと化」、およびセキュリティ水準底上げの契機となります。

第 1 回会議テーマ

「国民の意識向上」まとめ

サイバーセキュリティ研究拠点は、国民一人ひとりがサイバーセキュリティを「自分ごと」として捉える環境をいかに整備するかという観点から、以下 3 つの方向性を提起します。

❶ 周知　一人ひとりへ認知を広げる

IT 分野に従事する人に限らず、幅広い層がサイバーセキュリティに関する情報へ日常的に接する機会を確保できる仕組みづくりが重要な論点となりました。
専門的知識としてではなく、学校での教育やデジタルサイネージを活用した注意喚起や情報発信など、生活に根ざした基礎的リテラシーとして位置付けていく視点が求められます。

❷ 浸透　響く言葉で認識を深める

意識向上を図る上では、用語の選択やメッセージ設計の在り方が重要であるとして議論されました。
「サイバーセキュリティ」という専門的な表現と「ネット安全」のような直感的に理解しやすい呼称との併用や、受け手の解釈に左右されないほど具体的に示すメッセージの設計が、「自分ごと化」を促進する要素となります。

❸ 制度化　ルール整備で行動を促す

個人の自発的な取り組みと共に、法律を含めた制度やルールの整備を通じて行動変容を促す視点も提示されました。
サイバーセキュリティ管理責任者の設置や、消費者に向けたライセンス制度の設計といった、法律やガイドライン、評価制度などの仕組みを通じた環境整備が、意識と行動の双方に働きかけるための基盤となります。

第２回

会議テーマ

経営者が取り組むべき
サイバーセキュリティ

第 2 回

拡大するサプライチェーンリスク

企業経営に求められるサイバーセキュリティ戦略

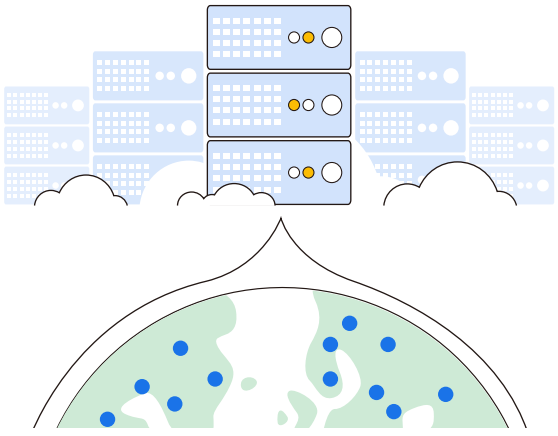
2025 年 10 月に発足した高市内閣は、日本成長戦略本部を立ち上げ、「AI・半導体」「情報通信」「量子」「コンテンツ」など、全 17 の戦略分野で投資を強化することを表明しています。分野ごとに担当閣僚を配備し、戦略的に財政出動を行うことで国内産業の抜本的な体質改善・強化を図る狙いです。

この戦略分野の一つであり、かつ、国内産業の競争力の根幹を支える基盤として、サイバーセキュリティの重要性は一段と高まっています。

現在、企業活動を支える IT システムは、多様な外部企業やネットワークと接続されています。その結果、攻撃対象となる領域は企業単体に留まらず、サプライチェーン全体へと拡張しています。システム停止や機密情報漏えいの防止策をはじめ、セキュリティ対策の強化は企業価値や信用に直結する経営課題となっています。

しかしながら、経営層によるサイバーセキュリティ対策への関与の度合いには、企業間で格差が見られます。高度な対策を経営主導で進める企業が増加する一方、依然として「情報システム部門の課題」として扱う企業も一定数存在します。認識格差の背景には、サイバー脅威の実態や自社への影響に対する把握の度合い、すなわち危機意識の差があると考えられます。こうした状況を踏まえ、経営層が主体的に関与し「強い経済」の基盤となるサイバーセキュリティ体制を構築することが求められています。

サイバーセキュリティ研究拠点では、あらゆる企業の経営者に対してサイバーセキュリティ対策の重要性を周知すると共に、経営層の視点に立った有効な対策の在り方について、多角的な議論を行っています。



第 2 回

❶ 経営層にとっての「リスク対策の障壁」

経営層のサイバーセキュリティへの関与が限定的になる背景として、経営層と IT 専門職社員との間に、「リスク」に対する認識のギャップがあると考えられています。また、サイバーセキュリティが既存の経営プロセスや意思決定の枠組みと十分に結びついていないことも要因と考えられます。

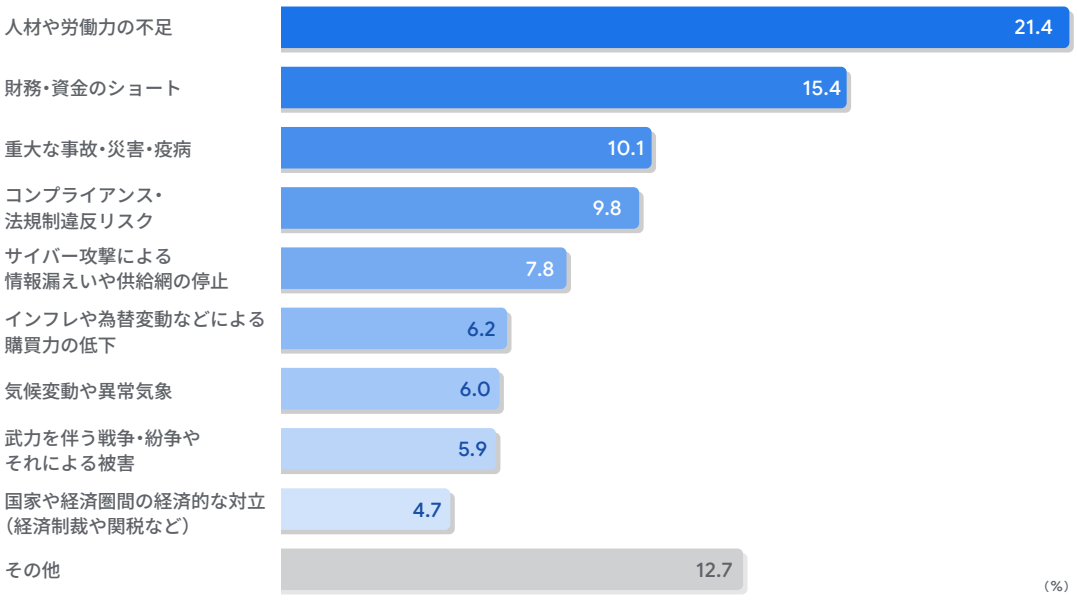
経営層と IT 部門のリスク認識におけるギャップ

一般的に、経営層が「リスク」として重視するのは、財務・市場・人材などを含む広義の「経営リスク」です。一方、情報セキュリティを担当している社員がリスクという言葉から第一に想起するのは、一般的にシステム停止や情報漏えいといった「サイバーリスク」です（図 1）。

サイバーリスクは基本的に「回避・除去すべきもの」であるのに対し、経営リスクは戦略上あえて「取る」こともあります。こうしたビジネス上の視座・判断基準の違いに加え、デジタル領域を専門外と捉える心理的境界が、IT 専門職と経営者との間でのサイバーセキュリティ対策議論の障壁となっています。

図 1　最も重要視している経営リスク

「最も重要視している経営リスク」の設問に対し、サイバーセキュリティを挙げた経営者は 7.8%に留まった。人材不足や資金繰りなどと比較して、後回しにされがちな面が見て取れる。



JCI「サイバーセキュリティ調査（第 2 回）」より。日本国内在住の経営者・役員クラス、計 1,000 人を対象にオンラインで 2025 年 12 月実施

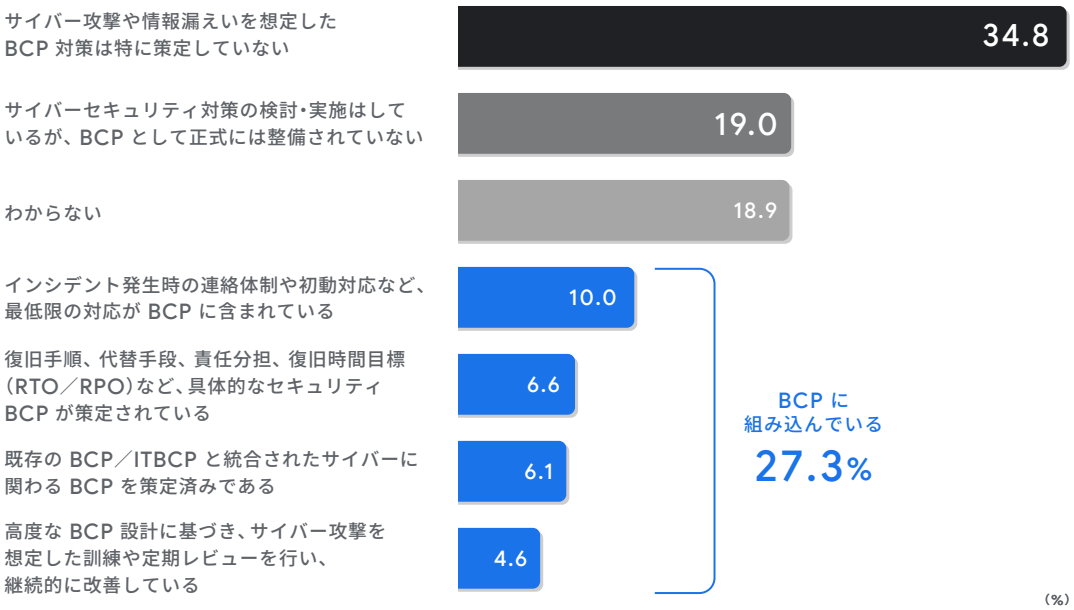
第 2 回

BCP との接続や金融機関との対話で意識変容へ

経営層がサイバーセキュリティを「自分ごと化」するためには、既存の経営プロセスとの接続が有効とされています。その一例が BCP（事業継続計画）です。サイバーリスク対策を「事業継続のための手段」と位置付け、BCP の枠組みにセキュリティ対策の検討・実施を組み込みます。調査対象者の経営者のうち 3 割弱が「既に BCP にサイバーセキュリティを組み込んでいる」と回答しており、徐々にこうした取り組みが広まりつつある一方で、全体としては BCP への組み込みまで至らない／把握していないケースの方が多いのが現状で、サイバーセキュリティ対策の進捗には格差が見られ始めています（図 2）。

図 2　所属する組織がサイバーセキュリティ対策を BCP に組み込んでいるか

「組み込んでいる」と回答した経営者の割合は全体の約 27%。BCP未策定が多数派の現状。

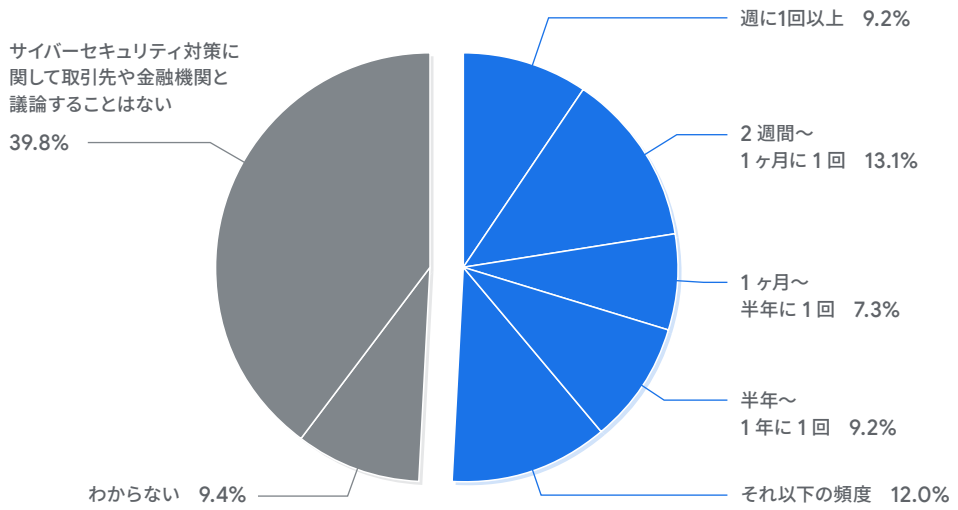


JCI「サイバーセキュリティ調査（第 2 回）」より。日本国内在住の経営者・役員クラス、計 1,000 人を対象にオンラインで 2025 年 12 月実施

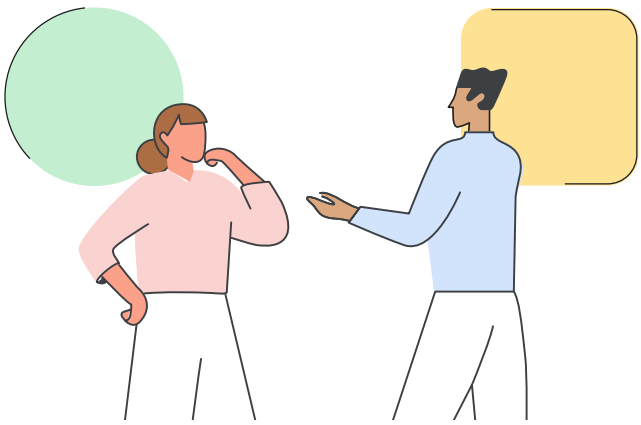
また近年、金融機関や取引先とのコミュニケーションにサイバーセキュリティに関するトピックを織り込む動きが出てきており、金融機関が経営層向けにデジタルアドバイザリサービスを提供する事例も見られます。調査においては約半数が「サイバーセキュリティに関して外部機関と議論することがある」と回答しました（図 3）。融資リスク管理の観点から、企業のデジタル成熟度やセキュリティ体制を重視する動きが広がりを見せており、こうした**外部との対話を通じて自社のセキュリティ水準を客観視することは、経営層が意識変容を進める契機となります。**

図 3　取引先などの外部機関とサイバーセキュリティの議論を行うことがあるか

議論を行っていた経営者は約半数。月 1 回以上など定期的に／頻度高く議論を行っている層は全体の 22%ほどだが外部機関とのコミュニケーションのテーマにおいてサイバーセキュリティが挙がるケースが増えてきている。



JCI「サイバーセキュリティ調査（第 2 回）」より。日本国内在住の経営者・役員クラス、計 1,000 人を対象にオンラインで 2025 年 12 月実施



❷ 中小企業の制約を踏まえたセキュリティ強化

経営者が自社のサイバーセキュリティ対策を推進し、一区切りを迎えた際にあらためて直面するのは「自社だけ守ればよいわけではない」という現実です。
日本には数百万社にのぼる中小企業があり、それらが自社の事業活動を支えている場合もあります。しかし、中小企業の多くは情報・資金・人材のいずれも不足しがちで、IT 担当者が専任でいない場合も少なくありません。
こうした個々の企業の限界を放置したままでは、真の意味で安全な事業環境は手に入りません。サイバーセキュリティ能力を企業単位の課題に留めず、事業を支えるサプライチェーン、ひいては社会全体でその能力を底上げしていく必要があります。

「垂直」「水平」「ピンポイント」のアプローチ

数百万社にのぼる中小企業すべてに対して、一様に対策を進めることは現実的ではありません。会議では、以下 3 方向からのアプローチが提起されました。

●垂直方向のアプローチ

自動車産業や建設業のように、発注者から一次・二次請け企業へと、工程や責任範囲が明確に連なるサプライチェーン構造に沿って対策を展開する手法です。一例として、完成車メーカーが Tier 1（一次サプライヤー）、Tier 2（二次サプライヤー）企業に対してセキュリティ基準の遵守を求めるガイドラインを提示する方法が挙げられます。また、一般社団法人 日本自動車工業会や一般社団法人 全国建設業協会などの業界団体が主導して、体系的にセキュリティ水準を引き上げる取り組みも含まれます。

●水平方向のアプローチ

地域という単位に着目し、企業規模や業種を横断してセキュリティ対策の浸透を図る手法です。地方自治体、警察、商工会議所、業界団体などが連携して地域全体の対策水準を引き上げます。また、地域内で影響力を持つ経営者が中心となり、経営者同士の勉強会などを通じて啓発を行うケースもあり、ロータリークラブやライオンズクラブが主体的に取り組みを進める地域も見られます。デジタル分野に精通していなくとも地域社会において影響力を持つキーパーソンの理解と協力を得ることが、浸透を加速させる要素となります。

●ピンポイントのアプローチ

特定企業を重点対象として、集中的にセキュリティ強化を図る手法です。とりわけ重要部品や基幹技術を担い、複数のサプライチェーンにおいて代替が困難な企業を「バイタルパート（重要防御区画）」と位置付け、優先的に対策の導入を進めます。これらの企業は、産業基盤や経済安全保障の観点からも重要な役割を担っているとの認識に基づき、対策や管理体制

の高度化など、より踏み込んだ措置が求められます。サプライチェーン全体への波及リスクを抑制する観点から、戦略的に重点化を行う点が特徴です。

外部サービスの活用も選択肢に

中小企業の経営者にとって、自社のみによる専門人材の確保や、高度なセキュリティシステムの構築は容易ではありません。こうした課題に対し、外部サービスの活用は一つの現実的な選択肢となり得ますが、JCI の調査では、既に利用しているとの回答は 1 割に満たないことが明らかになりました（図 4）。

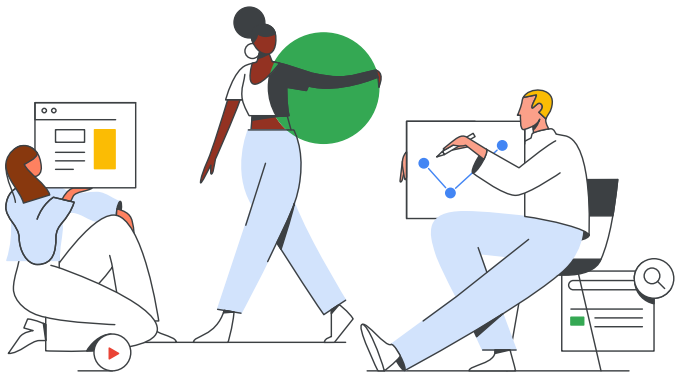
図 4　サイバーセキュリティ対策支援サービスの受容について

「利用しているサイバーセキュリティ対策支援サービス」の設問に対し、従業員のリテラシー向上、脆弱性診断、セキュリティ監視などのサービスとの回答が上位となった。こういったサービス利用の検討は、自組織のセキュリティレベル向上の契機となる。

	利用していると回答した人の割合
従業員向けセキュリティ教育・訓練：標的型メール訓練などで従業員のセキュリティ意識を高める支援	8.9%
脆弱性診断（Web／ネットワーク）：攻撃に悪用される弱点がないか専門家が調査する診断	7.2%
クラウドセキュリティ設定管理支援：AWS などのクラウド設定ミスやリスクをチェックし改善する支援	6.7%
セキュリティ監視（SOC）サービス：不審なアクセスや異常通信を 24 時間体制で監視するサービス	6.5%
EDR／XDR の導入・運用支援：端末の不審挙動を検知し、感染を早期に食い止める仕組みの導入支援	5.3%
セキュリティコンサルティング（ガバナンス・リスク）：リスク評価やポリシー整備など全体的なセキュリティ基盤の強化支援	5.0%
侵入テスト（ペネトレーションテスト）：攻撃者の手口を模して侵入可能性を検証するテスト	4.9%
24 時間 365 日体制の異常監視や緊急時の駆け付け、簡易サイバー保険などをワンパッケージで提供するサービス	4.5%
CSIRT 構築・インシデント対応支援：サイバー事故に備えた組織的な対応体制を整える支援	4.3%
インシデントレスポンス／フォレンジック：攻撃発生後に原因調査・被害特定・復旧方針を行う専門対応	3.4%
ゼロトラスト導入支援：アクセスを“常に検証”する仕組みを導入するための支援	3.1%

JCI「サイバーセキュリティ調査（第 2 回）」より。日本国内在住の経営者・役員クラス、計 1,000 人を対象にオンラインで 2025 年 12 月実施

外部サービスの代表例が、経済産業省と独立行政法人 情報処理推進機構（IPA）の認定を受けた民間事業者が提供する「サイバーセキュリティお助け隊サービス」です。同サービスでは、24 時間 365 日体制の異常監視、緊急時の駆け付け対応、簡易サイバー保険などをワンパッケージで提供しています。月額 1 万円前後から利用できるコストパフォーマンスの高さも大きな特長であり、2021 年の提供開始以降、既に 1 万社以上が導入しています。



Column

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

従来のサイバーセキュリティ関連ガイドラインは、個々の企業の取り組みを対象とするものが主流でした。例えば、米国立標準技術研究所（NIST）が策定したサイバーセキュリティフレームワーク（CSF）は、組織単位でのリスク管理を体系化した代表的な枠組みとして広く参照されています。これに対し、経済産業省が 2019 年に公表したサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）は、視点をサプライチェーン全体へと拡張した点に特徴があり、「全体を護る」という発想のもと、企業間の連関を前提としたリスクマネジメントを提示しています。

CPSF では、経営層向けの指針に加え、ビル、自動車、電力、製造業など産業分野別のガイドライン、実務層向けのガイダンスやツール、サービスの整備も進められています。企業にとっては、自社の対策水準を点検し、サプライチェーン全体との整合性を図るための実践的な足掛かりとなる枠組みといえます。

❸ サプライチェーン全体を護る

社会全体の底上げに加え、経営層がより強い関心を寄せるのは、自社のサプライチェーン、とりわけ**重要事業を支える部品・サービス提供企業を含めたセキュリティ対策の実効性**です。これは前述の垂直方向のアプローチに近接しますが、より自社の事業継続に直結する領域へ焦点を絞った取り組みといえます。

セキュリティ要件の明確化が鍵

中核企業の経営者には、まずサプライチェーン全体の構造を「見える化」する視点が求められます。特定企業の供給停止が前後工程にどのような影響を及ぼすのか、代替可能性はあるのか、さらに各社のセキュリティ対策水準がどの程度確保されているのかを把握することが出発点となります。各社の取り組みを後押しして徹底する、あるいは高いセキュリティレベルを継続的に維持するために、満たすべきセキュリティ要件やルールを定めることも重要です。

実務的な参考となるのが、クラウドサービス分野で一般化している SLA（サービス品質保証）の概念です。SLA はサービス品質を客観的に示したもので、要件未達時の補償内容や免責事項などを明示し、ユーザーとクラウドサービスプロバイダの間の信頼関係を制度的に担保しています。

サプライチェーンにおいても、発注者と受注者（サプライヤー）間で同様の枠組みを設けることで、責任範囲の明確化が図られます。**契約書にセキュリティ要件や遵守事項を組み込み、その達成度を評価する仕組みを導入することで、各主体が自律的に対策を講じる契機となります。**米国では、発注者の要求事項を契約条件に組み込み、その遵守状況を踏まえて契約継続を判断する仕組みが有効だとされています。受注者にとっては、対策の未実施が取引停止につながり得るため、強い動機付けとなります。日本においては、法制度が異なるためそのまま導入することは現実的ではありませんが、参考となるアプローチの一つといえます。

さらに国内でも、企業間の合意形成を下支えする制度整備が進められています。経済産業省が 2026 年度の開始を目指す「サプライチェーン強化に向けたセキュリティ対策評価制度」は、企業・組織のセキュリティレベルを 5 段階で格付け・公開する構想です。発注企業が契約審査の基準として活用するほか、対策実施を促す根拠としての活用が想定されています。

例えば「レベル 4 以上を必要水準とする」とあらかじめ取り決めておくことで、インシデント発生時の責任分担の整理や係争期間の短縮といった効果が期待されます。さらに、評価結果を金融機関が融資判断に活用するなど、ポジティブなインセンティブ設計も考えられます。こうした**評価制度の戦略的活用は、セキュリティを「コスト」から、企業価値や取引信頼性に直結する「信用資本」へと転換させるための重要な経営判断となります。**

第 2 回

❹ セキュリティ投資と経営判断

セキュリティ対策の高度化には、人的体制の整備やシステム投資など一定のコストを伴います。**取引先や社会から求められる水準に応えるための費用を製品・サービス価格へ反映することは、合理的な経営判断の一環と位置づけられます。**
今後、価格転嫁の議論が一層重要性を増すことが想定されるなか、市場全体でセキュリティに関わる費用を「共通のコスト」として認識し、受容する姿勢が求められます。

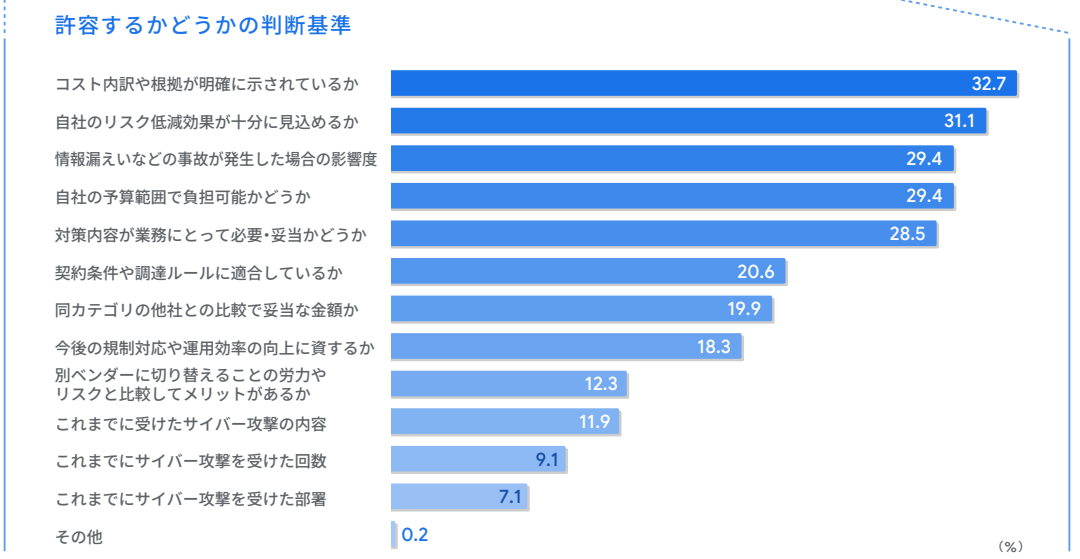
セキュリティを戦略投資として捉える

価格転嫁を円滑に進めるためには、**対策の効果を定量的に示すことが不可欠です。**インシデント件数のみならず、「攻撃を受けた回数」「防御・遮断した回数」「攻撃手法の傾向」などのデータを提示することで、投資対効果の客観的な説明が可能となります（図 5）。

図 5　サプライヤーの価格転嫁を許容できるか／許容するかどうかの判断基準

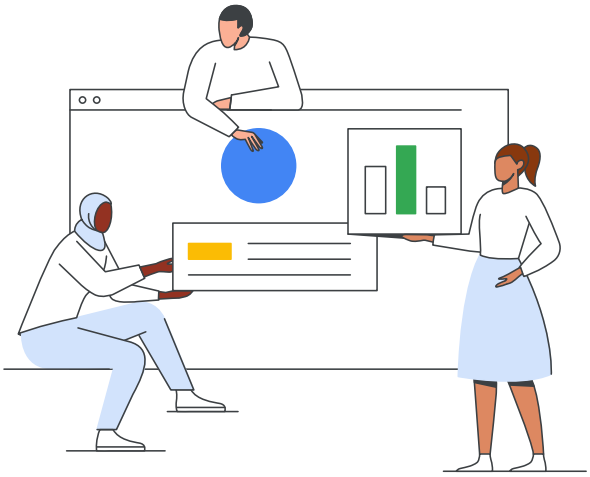
セキュリティ対策に必要なコストを、サプライヤーが価格に転嫁することを許容できると回答したのは約 56%。許容するかどうかの判断基準は、費用面のほか、自社のリスク低減に対する期待値やインシデント発生時の影響などの明示が上位となった。価格転嫁を検討する企業は、相手のメリットを分かりやすく提示することが有効性を持つ。

●サプライヤーや委託先がセキュリティ向上のためのコストを価格転嫁することを容認できる



JCI「サイバーセキュリティ調査（第 2 回）」より。日本国内在住の経営者・役員クラス、計 1,000 人を対象にオンラインで 2025 年 12 月実施

一方、発注側や顧客側においても、状況に応じて価格転嫁を許容することや、どのコストを誰が負担するのかを事前に整理しておくことが、将来的な齟齬の回避に繋がります。もっとも、すべてのリスクをゼロにすることは現実的ではなく、**リスク発生の可能性と影響度を踏まえ、優先順位を明確化した上で戦略的な投資判断を行うことが重要です。**そのために、経営層にはサプライチェーンリスクの理解、ビジネスプロセスの把握、そして最新のサイバー脅威動向に関する知見を統合し、多面的に意思決定を行うことが求められます。



Column

セキュリティ対策の実施は「経営者」の責任か

米国では、サイバー攻撃を受けた企業に対し株主代表訴訟が提起される事例が見られ、「セキュリティ対策の実施は経営者の責任か否か」が争点の一つとなっています。2025 年 9 月時点で、経営者個人の責任を直接認定した確定的判例は確認されていません。しかしながら、リスク管理を適切に実施しないことが「経営判断として合理性を欠く」あるいは「社会的相当性を逸脱する」と評価され得る潮流が強まりつつあります。

この動向は日本にも波及する可能性があります。今後、関連ガイドラインや業界ルールの改訂が段階的に進むことも想定されます。また近年、日本においても大手企業によるランサムウェア被害が相次いで報道されており、サイバー攻撃が企業経営に重大な影響を及ぼし得るリスクであることは広く認識されつつあります。こうした状況を踏まえると、経営者にとってサイバーリスクの「予見可能性」は従来と比べて高まっているといえます。こうした際に問われるのは、インシデント発生後の対応のみならず、平時からどのような体制整備や意思決定プロセスを構築していたかという点です。

セキュリティを IT 部門の課題に留めず、経営課題として位置づけているかどうかが、今後の重要な判断軸となります。

第 2 回

⑤ サプライチェーンを超えた連携へ

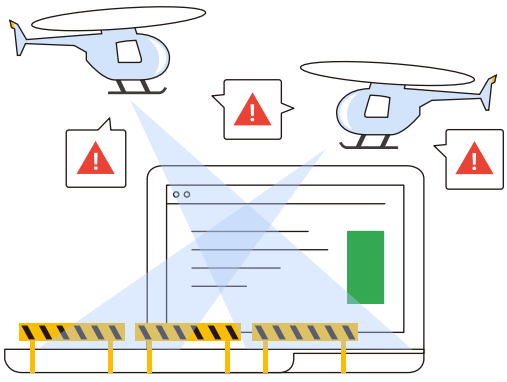
近年、個別企業や特定業界に留まらず、エネルギー、通信、物流など社会インフラ全体がサイバー脅威の対象となっています。**攻撃の影響は単一のサプライチェーンに収まらず、国家レベルの安全保障にも波及し得る**ものです。
こうした状況を踏まえ、受動的な事後対応型対策から、未然に防止する「能動的サイバー防御」への転換が重要性を増しています。

社会全体で支えるセキュリティ基盤

日本政府は、2022 年に閣議決定した国家安全保障戦略に基づき、2025 年 5 月に「サイバー対処能力強化法及び同整備法」を公布しました。ここで掲げられた中核概念が「能動的サイバー防御」です。従来は被害者に焦点を当てた取り組みや攻撃発生後の対応が中心でしたが、今後はこれに加え、攻撃者側に対抗する脅威の兆候把握や未然の防御・抑止を重視する枠組みへと移行します。警察や自衛隊による攻撃元サーバーの無害化措置は、その具体例の一つです。

「能動的サイバー防御」の実現には、リスクの予兆や対処知見を共有するための、組織間連携のエコシステムの構築が前提となります。企業においても、外部との情報共有を従来以上に積極性を持って進める姿勢が求められます。

セキュリティ対策のステークホルダーは自社のサプライチェーンに限られるものではありません。サイバー攻撃が単一の企業やサプライチェーンの枠を超えた国家の安全保障を脅かすリスクになっている現在、**自社のサプライチェーンとは一見すると無関係な企業・組織、官公庁（行政機関、警察、自衛隊）なども重要なステークホルダーとして位置付けられます。**
そのため、企業経営者にはより広い視野からセキュリティの在り方を再考することが期待されています。



第 2 回

第 2 回会議テーマ

「経営者が取り組むべきサイバーセキュリティ」まとめ

サイバーセキュリティ研究拠点は、企業経営においてサイバーセキュリティをいかに「経営課題」として位置づけ、サプライチェーンや社会との連携を視野に入れながら実効性のある対策を推進していくかという観点から、以下 5 つの方向性を提起します。

① 経営関与 サイバーリスクを経営課題として捉える

企業のサイバーセキュリティ対策をより有効にするためには、経営層自身がサイバーリスクを経営判断の一部として捉える視点が不可欠です。財務・市場などの「経営リスク」と IT 部門が認識する「サイバーリスク」とのギャップを踏まえ、BCP（事業継続計画）との接続や取引先などとの対話を通じて、経営層の主体的関与を促すことが重要です。

② 底上げ 中小企業の制約を含めた対策強化

企業活動を支えるサプライチェーンの多くは中小企業によって構成されていますが、人材・資金・情報の制約から十分な対策を講じることが難しい場合も見られます。そのため、サイバーセキュリティを個別企業の課題に留めず、外部支援サービスの活用も含めながら、産業全体・地域社会全体で対策水準の底上げを図る取り組みが求められます。

③ 見える化 サプライチェーン全体を護る

経営者には、自社のサプライチェーン構造を把握し、重要部品やサービスを担う企業を含めたセキュリティ対策の状況を「見える化」する視点が求められます。契約や評価制度を通じて満たすべきセキュリティ要件を明確化し、保護することがサプライチェーン全体のレジリエンス向上に寄与します。

④ 戦略投資 セキュリティ投資と経営判断

セキュリティ対策の高度化には、人材確保やシステム整備など一定のコストを伴います。こうした費用を単なる負担ではなく事業継続や企業価値に関わる戦略投資として位置づけ、対策の効果を示すデータなどを基に取引先や顧客との理解を形成しながら、適切な費用分担を図っていくことが求められます。

⑤ 社会連携 企業の枠を超えたセキュリティ体制へ

サイバー攻撃は個別企業の枠を超え、社会インフラや国家安全保障にも影響を及ぼす規模へと拡大しています。企業間の連携に加え、行政機関や治安機関などとの情報共有を含む広範な協力体制を構築し、社会全体でセキュリティ基盤を支えていくことが期待されます。

第３回

会議テーマ

サイバーセキュリティ人材のすそ野拡大

第 3 回

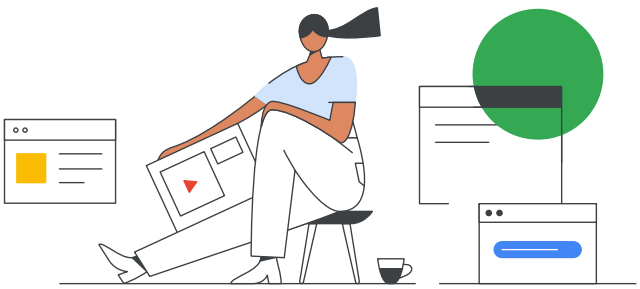
不足する 17 万人をどう確保するか

国を挙げた セキュリティ人材育成の 方法論と実践のアプローチ

サイバー攻撃の高度化やデジタル化の進展に伴い、サイバーセキュリティ人材の確保は、国内外で重要な課題となっています。日本においても人材不足が指摘されており、持続的なセキュリティ体制を構築していく上で、その確保と育成が重要な論点となっています。

こうした状況のもと、セキュリティ体制を強化していくためには、専門人材の確保・育成に取り組むと同時に、組織内外でセキュリティに関わる人材のすそ野を拡大していく視点も重要となります。

International Information System Security Certification Consortium（ISC2）が2024 年に公表した「ISC2 Cybersecurity Workforce Study」によれば、世界のセキュリティ人材は約 545 万人である一方、必要数に対して約 470 万人が不足しているとされています。同様に、日本国内におけるセキュリティ人材は約 50 万人であり、必要数とされる約 67 万人に対して、およそ 17 万人が不足している状況が報告されています。さらに、同調査の 2025 年版では、新たに「スキル不足と人材需給のミスマッチ」という課題も指摘されています。全体としてスキルの不足傾向が見られると共に、採用側と求職側の認識の差も明らかになりました。サイバーセキュリティ分野において、採用担当者が問題解決能力やコミュニケーション能力などの非技術的スキルを最優先して求めている一方で、現場の専門家（実務者）は非技術的スキルの重要性を認めつつも、AI やクラウドといった実践的な技術スキルも同等に需要が高いと認識しており、両者の優先順位にズレが生じています※1。



※1　ISC2「ISC2 Cybersecurity Workforce Study」（2024 年版および 2025 年版）より引用・作成。

第 3 回

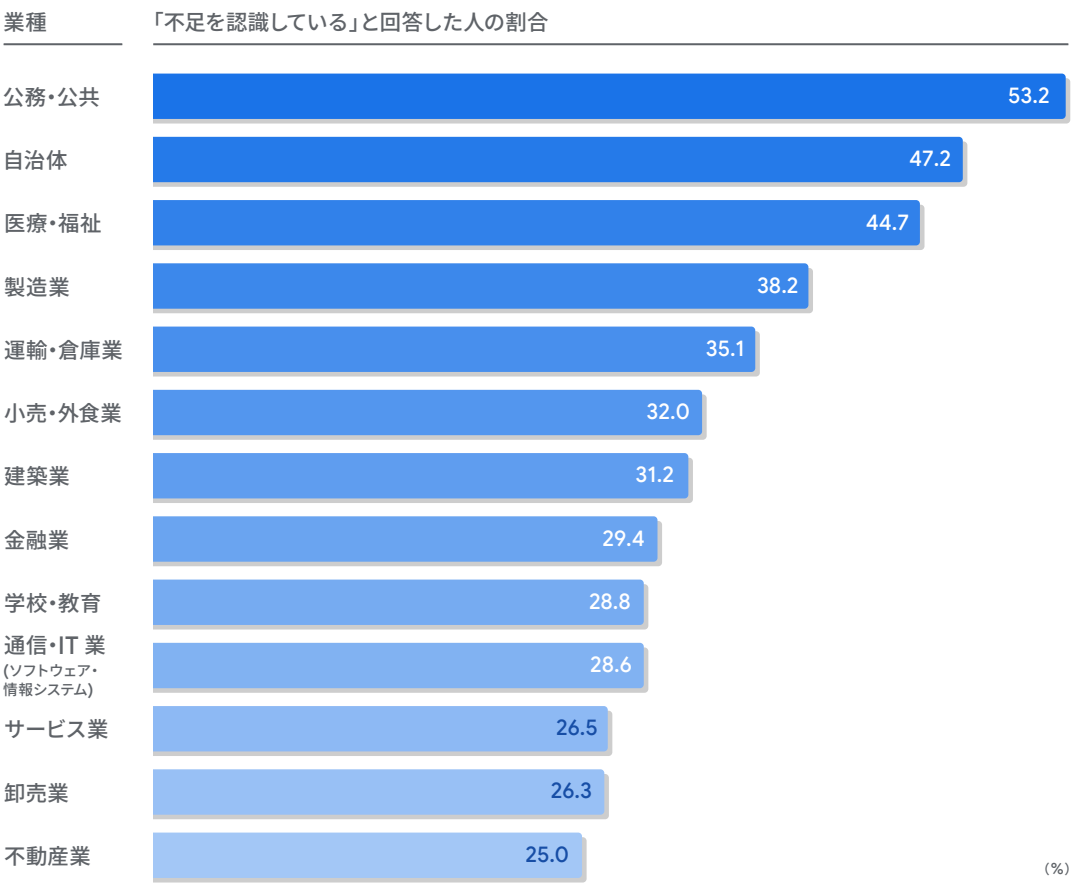
JCI の調査においても、セキュリティ人材の不足を実感している企業・組織が多いことが示されています。いずれの役職・業種においても「セキュリティ領域に十分な人材が配置されている」と回答した割合は 2 割未満に留まり、特に公務・公共、自治体、医療・福祉などの分野では、回答者の約半数がセキュリティ人材の不足を認識していると回答しています（図 1）。

こうした状況を踏まえると、**抜け漏れのないセキュリティ対策を実施し、安心・安全なデジタル環境を維持していくためには、サイバーセキュリティ人材のすそ野を拡大する取り組みが不可欠であるといえます。**

そこでサイバーセキュリティ研究拠点では、まず現在どのようなセキュリティ人材が不足しているのかを可視化し、その上で適切な人材育成の方法を検討します。さらに、評価制度やキャリアパスの設計までを視野に入れながら、セキュリティ人材のすそ野を広げるための実効的なアプローチを提起します。

図 1　多くの業種で不足するセキュリティ人材

「勤務先でサイバーセキュリティに関する領域に従事する人員は十分に配置されているか」との設問に対し、公務・公共、自治体、医療・福祉などの分野では、回答者の 4〜5 割がセキュリティ人材の不足を認識していると回答した。さらに、日常的にセキュリティ業務に関わる職種ほど、不足感を抱く割合が高い傾向も示されている。



JCI「サイバーセキュリティ調査（第 3 回）」より。日本国内在住の経営者・役員クラス、人事担当者、サイバーセキュリティ関与者 各 500 人：計 1,500 人を対象にオンラインで 2026 年 2 月実施

第 3 回

❶ 不足するセキュリティ人材の「本質」

「サイバーセキュリティ」といっても、その対象領域は広範です。「どの領域で」「どのレベルの人材が」「どの程度不足しているのか」を十分な解像度で構造的に把握しなければ、実効性のある取り組みを進めることは困難です。

不足しているのは、セキュリティ「も」担える人材

人材のすそ野拡大を図るにあたっては、まず求める人材像を明確にする必要があります。参考となるのが、日本と同様にセキュリティ人材の不足に直面している米国の取り組みです。米国立標準技術研究所（NIST）は、サイバーセキュリティに関わる職種・職域ごとの能力評価の指標として「NICE（National Initiative for Cybersecurity Education）フレームワーク」を策定しています。

このフレームワークでは、セキュリティ人材を「監督・統治」「設計・開発」「導入・運用」「保護・防衛」「捜査」の 5 カテゴリ、計 41 の人材像に分類し、それぞれに求められる 942 のタスク、631 の知識、538 のスキルを整理しています※2。

特徴的なのは、41 の人材像の中に、従来はセキュリティ人材とみなされてこなかった職種が含まれている点です。これは、製品・サービスの設計やデザイン、あるいは販売・提供などに関わる人材も、セキュリティ人材であると定義され始めたことを意味します。

米国の人材関連調査プロジェクトである CyberSeek も、同様の考え方を提示しています。同プロジェクトでは、米国におけるセキュリティ人材の不足数を約 50 万人と試算していますが、そのうち、セキュリティ業務に専門的に従事する従来型の「セキュリティ専門人材」の割合は約 6 分の 1 に留まるとされています。

この比率を日本に当てはめると、不足している約 17 万人のうち、セキュリティ専門人材は約 3 万人程度となり、残る約 14 万人は多様な職種・職域に従事する「非セキュリティ専門人材」であると考えられます。すなわち、**本質的に不足しているのは、セキュリティ業務を専門とする人材だけではなく、本来の業務を担いながらセキュリティにも関与できる人材であるといえます。**

こうした人材を育成し、セキュリティ人材のすそ野を広げると共に組織全体のレジリエンスを向上するためには、以下 2 つの視点が重要となります。

- 「IT 事業者や IT 部門に所属する非セキュリティ専門人材」ならびに「ビジネス部門の人材」に、いかにセキュリティの知見を習得させるか
- セキュリティ専門人材に、いかにビジネス実務への理解を促しスキルを習得させるか

※2　NICE フレームワーク コンポーネント v 2.1.0（2025 年 12 月）

第 3 回

不足人材を可視化する日本独自のフレームワーク

人材像の可視化に関する国内の取り組みとしては、内閣官房 国家サイバー統括室（NCO）が策定を進めている「サイバーセキュリティ人材フレームワーク」があります。これは、日本が今後確保・育成すべきセキュリティ人材の役割を整理すると共に、各職種・職域で求められる能力を体系的に示すものです。

米国の NICE フレームワークを参考に、人材カテゴリを「意思決定・戦略策定」「情報収集・分析・共有」「法務」「プロジェクト管理」など約 13 のカテゴリに分類し、カテゴリごとに必要となるタスク・知識・スキルを整理した上で、4 段階のレベル区分を設けることが検討されています。

人材像が明確になれば、自社組織に不足している人材の可視化や、採用後のミスマッチの防止に繋がります。さらに、働き手にとっても、求められるスキルがカテゴリごとに整理されることで、将来のキャリアパスを描きやすくなる効果が期待されます。

Column

未来を担う若年層のためのサイバーセキュリティ教育

2025 年 11 月、内閣官房 国家サイバー統括室（NCO）主催による「International Cybersecurity Challenge TOKYO 2025」が千葉県で開催されました。本大会は、26 歳以下の若手人材が地域別に競い合うサイバー競技（CTF※3）の国際大会であり、アジアでの開催は初めてです。

特筆すべきは、競技の実施に留まらず、小中高生を対象とした見学機会の提供や、セキュリティ関連のカンファレンス・展示会が併催された点です。こうした取り組みは、若年層が早期に高度なサイバー技術に触れ、将来的なキャリアパスを具体的に描く機会を提供するものといえます。

サイバーセキュリティ人材のすそ野を拡大するためには、単発のイベント開催に留まらず、教育課程における学習環境の整備や、産学官が連携した持続的なエコシステムの創成が不可欠です。国際大会を契機とした若年層の関心向上と、それを専門的な教育へと繋げる環境整備の加速が、日本のデジタル競争力を支える人材基盤の強化に寄与することが期待されます。

※3　Capture The Flag の略。ネットワーク解析やプログラミング、脆弱性解析技術など、幅広いサイバーセキュリティスキルを駆使して問題を攻略する技術競技。参加者が実践的なセキュリティスキルを身に付け、創造性と論理的思考力を鍛えることも目的とする。

第 3 回

② 人材育成の方法を考える

次に、セキュリティ人材のすそ野拡大に向けた具体策を整理します。鍵となるのは二つのアプローチです。一方は、非セキュリティ専門人材にセキュリティの知見を身に付けてもらうこと。他方は、セキュリティ専門人材にビジネスの実務への理解を深めてもらうことです。それぞれの実践策を確認していきます。

非セキュリティ専門人材にセキュリティの知見を「プラス」

サイバー攻撃の巧妙化に伴い、もはやセキュリティ専門人材だけで企業・組織や社会を守ることは困難になっています。実効性のあるセキュリティ対策を講じるためには、各職能にセキュリティの視点を加え、組織全体で守るという視点が重要です。

ここで鍵となるのが、**「プラス・セキュリティ人材※4」の育成**です。現在は非専門職にある人材であっても、セキュリティに関する知見を体系的に習得することで、こうした人材へと転換することは十分に可能です。このような人材が増えることで、日常業務やビジネス上の意思決定の場面に、セキュリティの視点を織り込むことができるようになります。

育成の手法としては、まず業務プロセスの中で小規模に取り組みを開始し、少数の社員を先行的に育成する方法が考えられます。**育成された社員が中心となって社内研修を展開**していくことで、組織全体への知識の浸透を図ることが可能になります。加えて、**外部の専門スタッフを常駐させたり、経験豊富なシニア人材を活用**したりすることで、疑問や課題を随時相談できる環境を整えることも効果的です。さらに、**ジョブローテーションや兼務を通じた現場での OJT（On-the-Job Training）は、実践的な経験を積みながら実務に即した知見を獲得するための手段として有効**と考えられます。

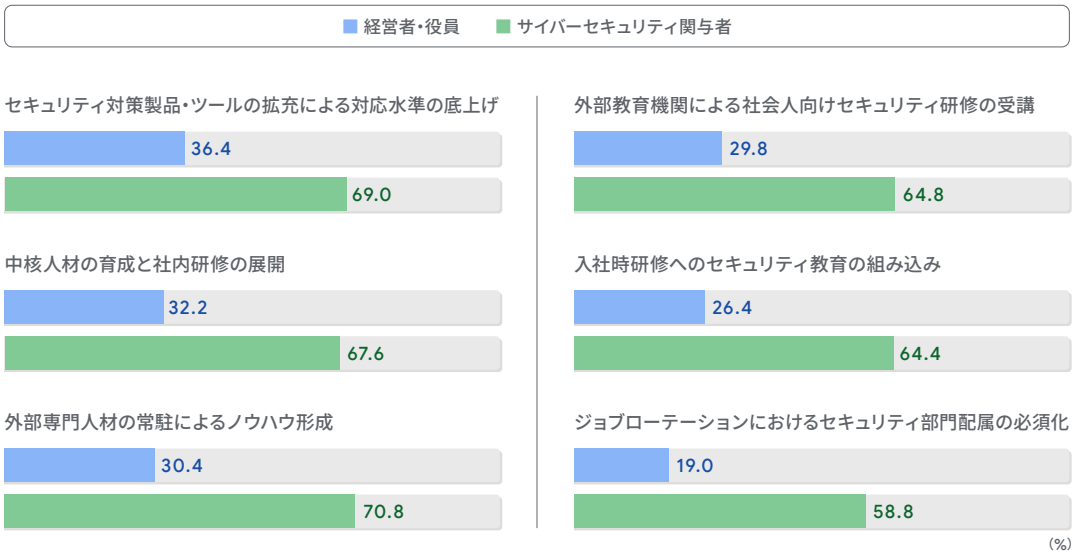
上記に挙げた育成方法に対する評価を JCI 調査にて聴取したところ、経営層では外部ツール・外部スタッフの活用や必要最低限の人員への知見集約を主に志向しており、労力や難度が高いと考えられるためかジョブローテーションや全社員を対象とした課題・研修の導入には、あまり前向きでない印象です。

※4　経営層や DX を推進するマネジメント人材層など、IT やセキュリティに関する専門知識や業務経験を必ずしも有していない場合にも、社内外のセキュリティ専門家と協働するに当たって必要な知識として、時宜に応じてプラスして習得すべき知識（「プラス・セキュリティ知識」）を補充している人材を指す。

一方で、サイバーセキュリティ関与者（日常的あるいは一時的にサイバーセキュリティ対策に関わる人）においては外部研修の受講や入社時の研修実施に対してある程度積極的な姿勢が見受けられており、従業員教育の取り組みにおいて一定の協力を得られる可能性が高いとも考えられます（図 2）。

図 2　有効だと思う人材育成の方法

「勤務先でサイバーセキュリティ対策を担当する人材を育成するとした場合、これらの育成方法は有効であるか」との設問に対して「そう思う」と回答した人の割合。経営者層とサイバーセキュリティ関与者との間に意識のギャップが見て取れる。



JCI「サイバーセキュリティ調査（第 3 回）」より。日本国内在住の経営者・役員クラス、サイバーセキュリティ関与者 各 500 人：計 1,000 人を対象にオンラインで 2026 年 2 月実施

セキュリティ専門人材のビジネスプロセスへの関与を進める

一方で、既存のセキュリティ専門人材がビジネスや実務に関する理解を深めることも重要です。専門人材を各部門に適切に配置し、ビジネスプロセスに即した形でセキュリティ対策を組み込むことで、組織全体のレジリエンスは大きく向上します。

専門人材がビジネスプロセスで真に力を発揮するためには、**技術的な知識やノウハウだけでなく、業務プロセスへの深い理解や、経営層・現場双方と円滑に対話できるコミュニケーション能力が不可欠です。**こうしたスキルの習得においても、プラス・セキュリティ人材の育成と同様に、現場への参画を通じた OJT が有効な手段となります。

市場ニーズと連動した人材育成を図る

多くの企業・組織が人材不足に直面するなか、人材育成にかかる教育コストの負担は決して小さくありません。そのため、育成を進める際には、現場経験を積むことが本人のキャリア形成にどのように寄与するのかを具体的に示し、主体的な参画を促すことが重要です。

現在、セキュリティ分野の専門性を持つ人材の市場価値は依然として高い水準にありますが、求められるスキルの傾向には変化の兆しが見られます。これまではポータビリティの高い汎用的なセキュリティ技術に注目が集まっていましたが、近年では、特定の業界や企業の業務に精通したドメイン知識を併せ持つ人材への需要が一段と高まっています。こうした動向を踏まえると、セキュリティの専門性に加えて、業務プロセスへの理解や組織内外の関係者と円滑に連携するコミュニケーション能力も、専門人材の価値をさらに高める要素として位置付けられる傾向にあります。組織としても、これらのスキルが単に社内業務への適応に留まらず、個人のキャリア形成においても評価される重要なスキルであることを、周知していくことが求められます。

個人にとっての市場価値向上と、組織のセキュリティ強化という目的をすり合わせながら、共にキャリアを形成していく姿勢こそが、実効性のある人材育成の動機付けに繋がるといえるでしょう。

人材育成を円滑にするためには環境整備も

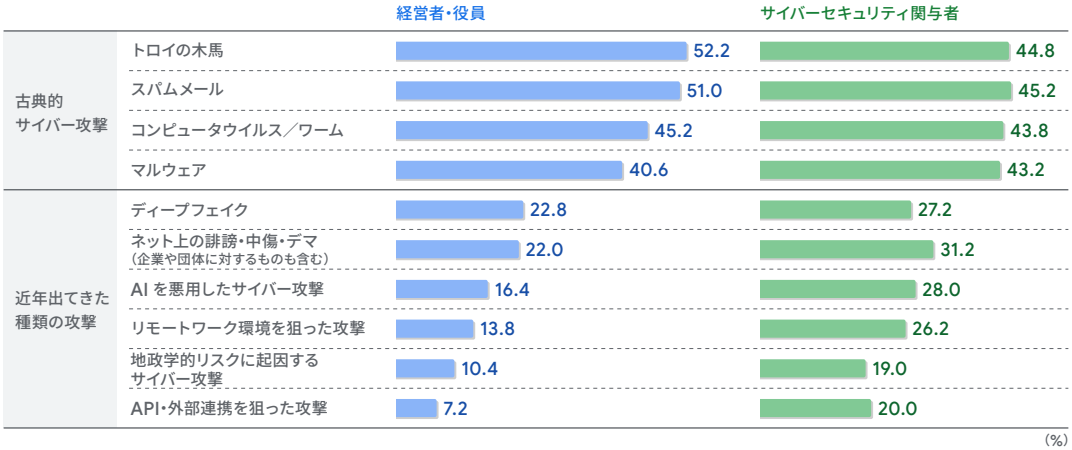
サイバーセキュリティ人材の育成を加速する上で、企業・組織に求められる視点と具体的なアプローチについて整理します。

[1] 過去事例やグローバル動向から学ぶ

日常的にセキュリティ業務に携わっているかどうかにかかわらず、新たに出現する攻撃手法への認知は古典的な手法に比べて大きく下回っています（図 3）。通常業務の範囲内で触れる情報からだけでは、次々に生まれるサイバー攻撃や脅威のトレンドを把握しきれていないことが見て取れます。

図 3　知っているサイバー攻撃の種類

「サイバーセキュリティに関する内容についてご自身が知っている・見聞きしたことがあるもの」を尋ねたところ、古典的サイバー攻撃、ならびに近年出てきた種類の攻撃に対し、経営者・役員層とサイバーセキュリティ関与者との間に意識のギャップが存在することが確認された。



JCI「サイバーセキュリティ調査（第 3 回）」より。日本国内在住の経営者・役員クラス、サイバーセキュリティ関与者 各 500 人：計 1,000 人を対象にオンラインで 2026 年 2 月実施

こうした状況を踏まえると、有識者による専門的な研修や体系的な教育プログラムを策定・実施することは、経営者および従業員のセキュリティリテラシー向上に向けた有効な施策といえます。これらの取り組みは、具体的な対策を講じる際の動機付けとしても機能し、不測の事態に備えた組織のレジリエンス強化にも寄与します。

また、諸外国の先行事例は、国内における将来的な環境変化を見通す上で重要な指標となります。例えば、フィジカル AI※5 や AI エージェントの高度化、米国における耐量子計算機暗号（PQC：Post-Quantum Cryptography）※6 の社会実装に向けた動向など、グローバルな技術潮流を早期に共有することは、国内での先導的な対応の必要性を認識する上で重要です。

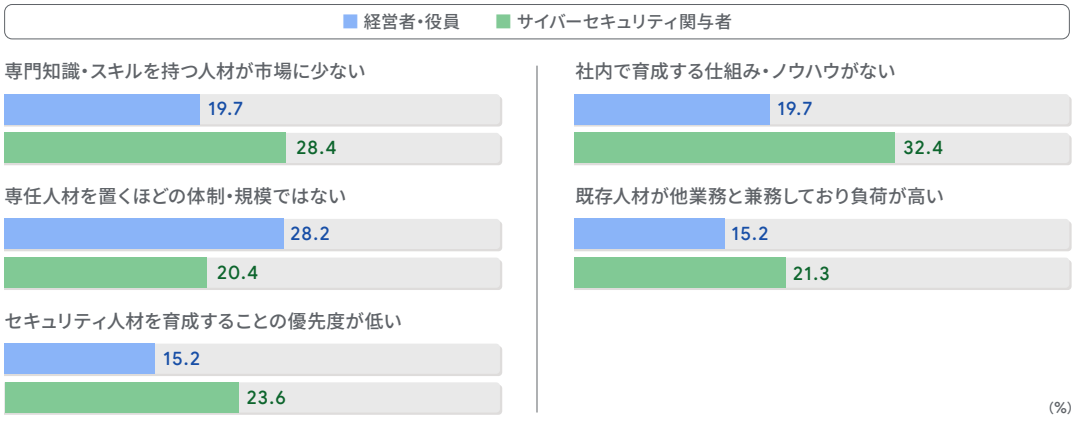
こうした情報を併せて周知することで、組織全体のセキュリティリテラシーを一層高めることが期待されます。

[2] セキュリティ人材育成への投資を促進する

サイバーセキュリティ人材の重要性が指摘される一方で、冒頭に述べた JCI 調査の回答からもセキュリティ人材の不足に悩む企業・団体は多いと推測されます。同調査で「セキュリティ人材が確保できている」と回答しなかった人に対して十分な配置ができていない理由について質問したところ、必要な知見・スキルを持つ人材を採用・育成することの難しさを感じていることや小規模企業を中心にセキュリティ対策専任者を配置する人的余裕がなく、人材配置の優先度を高められないという事情が浮き彫りになりました（図 4）。経営戦略においてこの優先順位をいかに高めるかは、一企業の課題に留まらず、官民が連携して取り組むべき重要なテーマです。

図 4　セキュリティ人材を十分に配置できていない理由

「サイバーセキュリティを担う人材を十分に配置できていない要因は何か」との設問に対し、注目すべきは、経営者・役員において「専門人材を置くほどの体制・規模ではない」という回答が最も多かった点。サイバーリスクが高まり続けるなか、この認識の妥当性については改めて検討する必要がある。



JCI「サイバーセキュリティ調査（第 3 回）」より。日本国内在住の経営者・役員クラス、サイバーセキュリティ関与者 各 500 人：計 1,000 人を対象にオンラインで 2026 年 2 月実施

※5　カメラやセンサーを通じて物理空間を認識・理解し、自律的に行動する、身体を持った AI のこと。
※6　次世代技術である量子コンピュータが普及すると、現行の暗号化技術は容易に解読されてしまうため、セキュリティ上のリスクが指摘されている。そのため米国を中心に、量子コンピュータの解読に耐える暗号化技術を模索・検討する動きが始まっている。

また、日本においてセキュリティ意識を持つ人材が増えていかない背景の一つとして、セキュリティ部門以外の人材の貢献が適切に評価されにくい点が挙げられます。仮にセキュリティに関する知識を持ち、周囲の社員に対して助言や支援を行っていたとしても、それが正式な評価に繋がらず、結果として「セキュリティに詳しい便利な人」に留まってしまうケースが少なくありません。こうした人材を適切に評価するためには、セキュリティを経営課題の一つとして位置付け、人事評価制度などと連動させる仕組みが重要となりますが、そういった企業は、現状では極めて少数です。

現在、多くの企業で浸透しつつある「人的資本経営」の観点から見ても、**セキュリティ分野の人材を単なる「コスト」ではなく、価値を生み出す「資本」と捉え、その価値を最大化する取り組みを進めていくことが求められます。**もっとも、多くの企業にとって人的投資の拡大は容易ではありません。そのため、国による支援も重要となります。助成金制度のさらなる拡充などを通じて、人材育成を後押しする環境整備が期待されます。

企業が個別の「点」として人材育成に取り組むだけでなく、産学官が連携し、「線」や「面」として次世代人材を育むエコシステムを構築していくことが重要です。こうした取り組みこそが、中長期的に日本のサイバー防御力を支える盤石な礎となります。

Column

未来の経営層に求められる IT リテラシー

2021 年 6 月に改訂されたコーポレートガバナンス・コード（上場企業に求められる企業統治の指針）では、上場企業の取締役会におけるスキル・マトリックスの開示が強く推奨されています。多くの企業が取締役会メンバーのスキルの可視化を進めるなかで、浮き彫りになったのが「スキルの偏り」という課題です。

「営業」「総務」といったビジネス系スキルを持つメンバーは多数存在する一方で、「システム開発」や「セキュリティ」といった IT 系スキルを有するメンバーは限られています。このアンバランスを是正するため、IT 系スキルを持つ社外取締役を迎えたいと考える企業は増えていますが、人材の絶対数が少ないため容易ではありません。

こうした課題の解決には時間がかかりますが、本レポートで論じてきたセキュリティ人材のすそ野拡大は、将来のマネジメント層を育てる取り組みでもあります。IT／セキュリティリテラシーの高い人材の絶対数を増やすことが、取締役会のスキル・マトリックスのバランス化、ひいては企業経営の適正化にも寄与します。人材のすそ野拡大に取り組む上では、こうした視点を持つことも重要です。

第 3 回

❸ 評価制度とキャリアパスを設計する

セキュリティ人材に求められる役割が拡大するにつれ、その活動実績や事業への貢献度を適切に評価する仕組みの整備が急務となっています。実効性のある評価制度を構築するためには、単なるスキルの測定に留まらず、自社の事業におけるサイバー人材の位置づけの明確化、採用・育成計画と連動させた制度設計が求められます。

階層ごとの評価指標を明確に示す

セキュリティ人材に求められる能力は、職位や役割によって大きく異なります。そのため、各階層に応じた評価指標を多面的に設計し、明確に提示する必要があります。

● 若手・初級クラス

スキル習得や資格取得、担当業務を着実に遂行する能力を中心に評価します。この段階では、専門性の基盤を築くための自己研鑽を正当に評価することが、成長を促す要素となります。

● 中堅・マネジャークラス

業務プロセスへの深い理解を踏まえた対策の企画立案や、チームの育成、体制整備、組織設計など、組織へのコミットメントが主な評価軸となります。

● 幹部・シニアクラス

組織全体を俯瞰したビジョンの提示に加え、業界団体への参画や情報発信などを通じた「ソートリーダーシップ（業界への影響力）」も重要な評価対象となります。

専門性を尊重し、自律的成長を支える

こうした階層ごとの人材像を具現化するためには、経験豊富な専門人材によるメンター制度などの導入も有効です。特に高度な専門人材については、研究者育成に近い形で自己研鑽を重視した育成・評価プログラムを導入し、業界での活動を積極的に評価に組み込むことが望まれます。

また、組織のメンバーが「このセキュリティ対策によって、自社の収益や信頼がどれほど守られたのか」を金額換算で考える視点を持つことも重要です。こうした視点は、セキュリティ人材の貢献度を可視化する一助となります。

「目指したくなるキャリア」を提示する

評価制度の設計において重要なのは、**働き手自身がその組織でサイバー人材として歩むことに、キャリアとしての魅力を見いだせるかどうかです。**技術を極めるスペシャリストの道もあれば、経営に近い立場で組織全体のセキュリティ戦略を担う道もあります。さらに、社内に留まらず社会的なプレゼンスを高めるキャリアを築くことも可能です。

このように、**社内外の双方で評価されるキャリアの姿を明確に示し、それを支える育成環境や評価制度を整備して初めて、人材の定着と活躍が実現します。**

経営層も自ら「プラス・セキュリティ人材」に

加えて、**管理職や経営層が自ら IT リテラシーを高め、セキュリティ人材の価値を正しく理解することも欠かせません。**その上で、**専門性に見合った適切な処遇や評価を明確に示すことが求められます。**

こうした経営層の姿勢は、人材育成を推し進めるだけでなく、組織全体にセキュリティの視点を根付かせる基盤となり、持続的なセキュリティ文化の醸成を促します。

セキュリティ人材育成の障壁

サイバーセキュリティ人材不足の背景には、日米の IT 人材の偏在という構造的課題が深く関わっています。米国では IT 人材の約 7 割がユーザー企業、つまり情報システムやソフトウェアを自社業務のために開発・導入し、実際に利用する発注側の企業に所属しているのに対し、日本ではその割合が約 3 割に留まり、IT 人材の多くが IT ベンダー企業に集中しています。

この構造は、ユーザー企業側において、外部に委託する際の「適切な要件定義」や「リスク判断」を担う人材が不足しやすい状況を生んでいます。特に、企業数の 9 割以上を占める中小企業において、IT 専門人材を自社で抱えることは現実的に容易ではありません。

しかし、DX の本質が、自社の業務を深く理解した上で IT を利活用し、価値を創出することにある以上、すべての業務を外部任せにすることはできません。セキュリティにおいても同様であり、専門家を自社で雇用することだけが解ではなく、既存の業務に精通した社員がセキュリティの視点を持つ「プラス・セキュリティ人材」として、ベンダー企業と対等に意思疎通を図り、自社の守りを主導できる体制を整えることが、日本型の現実的かつ不可欠なアプローチといえます。

第 3 回

第 3 回会議テーマ
「サイバーセキュリティ人材のすそ野拡大」まとめ

サイバーセキュリティ研究拠点は、不足する 17 万人の人材をいかに確保し、育成していくかという観点から、専門家のみに頼らないすそ野の広い人材基盤を構築するため、以下 3 つの方向性を提起します。

❶ 再定義 「セキュリティ人材」を可視化する

不足している人材の多くは、必ずしも高度な専門家ではなく、本来の業務を担いながらセキュリティの視点を持てる「セキュリティ人材」であるという認識の転換が必要です。国内外のフレームワークを活用し、組織内で「どのレベルの・どのような役割」が不足しているのかを解像度高く定義することが、育成の出発点となります。

❷ 実践的育成 OJT と相互理解でスキルを補完する

非セキュリティ専門人材にセキュリティの知見を習得させると同時に、セキュリティ専門人材にはビジネスプロセスへの理解を促すという双方向のアプローチが求められます。社内外の専門人材による育成に加え、業務に即したジョブローテーションや現場での OJT を通じて、技術と実務が分断されない生きたスキルを習得できる環境を整えることが、人材の活躍を促進します。併せて、セキュリティ分野の人材を「コスト」ではなく「資本」と捉え、その価値を最大化する取り組みが期待されます。

❸ キャリアデザイン 目指したくなる評価制度を整える

セキュリティ人材がその組織で働き続け、自身の市場価値を高められるよう、技術を極める道や経営に関わる道など、多様なキャリアパスを明示する必要があります。個人の専門性や社会的な貢献度を正しく評価し、処遇に反映させる制度を構築することで、人材の定着と自律的な成長を支えるエコシステムを実現します。

特別対談

Google 日本法人 代表
奥山 真司

慶應義塾大学 名誉教授
竹中 平蔵氏

サイバーの脅威が経営リスクに

奥山 Google は、デジタル社会を安全で自由、そして公正な場所にする責任を負っています。中でも、企業と生活者を守るためにサイバーセキュリティに取り組むことは、最先端のテクノロジーハブとしての日本の地位の確立と持続可能な成長のために不可欠なものです。JCI は、まさにそうした責任感から始まった活動です。

竹中 インターネットが社会の基盤になった一方で、最近では規模を問わず様々な企業がサイバー攻撃を受けるニュースを頻繁に目にするようになりました。そうした状況のなかで、Google が主導的に取り組む意義は大きいと感じます。

奥山 竹中先生は、世の中でサイバーセキュリティの重要性が注目されるよりも随分前から、その必要性を訴えてこられました。そもそも、先生がこの分野に関心を持たれたきっかけは何だったのでしょうか。

竹中 社会インフラや経済の仕組みがデジタル化によって大きく変化していくなかで、「これは単なる技術課題では終わらない」と感じたのが発端です。サイバー攻撃は社会の土台に影響を与える。早い段階で、そうした構造的なリスクに着目していました。

奥山 今や、その懸念が現実になりつつありますね。実際に社会インフラが止まるようなインシデントも発生しています。

竹中 だからこそ、サイバーセキュリティのリスクを経営リスクとして捉えることが不可欠であるという認識が浸透しつつあります。経営者にとって、これは「守りの話」に留まりません。正しく取り組めば、企業価値を高め、競争力の源泉にもなり得ます。サイバー対策が整っている企業ほど事業のレジリエンスが高く、投資家からの信頼が得やすくなるでしょう。セキュリティは「コスト」ではなく「価値創造」の一部として捉えるべきと考えます。

経営層の「自分ごと化」が組織を変える

奥山 JCI で先日行われた会議では「経営層が取り組むべきサイバーセキュリティ」を議題に掲げました。竹中先生は、議論をどのようにご覧になりましたか？

竹中 行政や学術機関だけでなく、弁護士や企業経営層の方も参加されていて、多面的な議論をできた点が非常に有意義でした。サイバーセキュリティは技術の面に留まらず、経営、法務、政策などの複合的な視点が不可欠です。

奥山 特に印象的だったのは、サプライチェーンに関する議論でしょうか。大企業は一定の対策が進んでいますが、関連する中小企業は対策に十分なリソースを割きづらい側面もあり、その隙を突かれるリスクもあります。

竹中 そうですね。大企業の経営層が見るべき範囲は自社だけでは不十分で、サプライチェーン全体に広げる必要があります。どこにリスクが潜んでいるのかを把握し、その上で対策を講じること。中小企業には、IPA（独立行政法人 情報処理推進機構）が実施している「サイバーセキュリティお助け隊サービス」といった廉価な支援策の活用も有効だという意見も出ましたね。

奥山 Google でも、無償での人材育成支援を拡充しています。これまで 1,000 万人以上の方々に受講いただいているデジタルスキルトレーニング Grow with Google の中でも、現在、最も急速に受講者が増えているのが、サイバーセキュリティのプログラムです。しかし、現場の努力だけでは限界があります。だからこそ、経営層が「自分ごと」として捉えることが何よりも大切だと考えます。実際、経済産業省と IPA がまとめた「サイバーセキュリティ経営ガイドライン」においても、経営者が自らのリーダーシップのもとで対策を進めることが重要であるとしています。

竹中 まさに自分ごと化が肝心ですね。経営者に法的責任の自覚を促すことも有効です。例えばアメリカでは、インシデント後に株主代表訴訟が起きることもあります。社会全体として「対策は経営者の責務」という理解が進むことが、意識改革の第一歩だと思います。

経済安全保障の時代に求められる企業戦略

奥山 高市政権が掲げる 17 の戦略分野の一つにもサイバーセキュリティが入りました。竹中先生は 2024 年、当時経済安全保障担当大臣でいらした高市総理と対談をされていましたね。

竹中 はい。2025 年 5 月に施行されたセキュリティ・クリアランス法について対談をさせていただきました。こちらは国家における情報安全措置の一環としての制度ですが、対象に民間企業の従業員も含まれるというところで、今この記事を読んでくださっている皆さまにも決して遠い話ではないと思います。

奥山 こういったセキュリティ対策の新たな潮流が、サイバーセキュリティと向き合う企業の経営層や従業員にも変化をもたらしていくのではないでしょうか。

竹中 そうですね。日本が情報安全制度を強化することによって諸外国からの信頼性が高まり、企業のビジネス機会が拡大していくことも期待されます。そういった意味でも、サイバーセキュリティの重要性が今後ますます高まっていくことになりそうです。

社会インフラを守る Google の最先端技術

奥山 今後ますますサイバーセキュリティの重要性が高まっていくなか、Google にはどのような役割を期待されますか。

竹中 サイバー攻撃は、もはや一企業の損失に留まりません。銀行や行政、交通などが止まれば、社会全体が麻痺します。つまり、企業がサイバーセキュリティに取り組むことは、社会インフラを守ることに繋がります。だからこそ、グローバルな知見を持つ Google が日本の産学官と連携して人材育成や情報提供に取り組むと同時に、最先端の技術を開発・提供していることには意義があります。

奥山 はい。近年、攻撃側が AI を悪用するなど脅威は高度化していますが、Google は圧倒的な規模のデータと精度で AIを「防御」に活用しています。私たちは世界中で膨大な脅威データを収集し、AI が常に学習し続けることで、人間では検出不可能なパターンや異常を見つけ出します。例えば Google Cloud のインフラは毎日発生する DDoS 攻撃や不正アクセスに対し、AI による自律的な防御を休むことなく実行しています。インフラレベルのセキュリティが最初から組み込まれている（セキュア・バイ・デザイン）ことで、リソースの限られる中小企業や自治体でも、安心して事業を推進いただけます。「防御側をより有利にする」ことこそが、技術を持つ私たちの使命だと考えています。

竹中 頼もしいですね。社会全体を見据えた取り組みを今後も期待しています。

株式会社 ＤＴＳ 執行役員 業務＆ソリューションセグメント 副セグメント長

阿部 展久 氏

地政学リスクの高まりや生成 AI などの飛躍的な技術進化を背景に、サイバー攻撃の脅威は一層深刻化しています。近年、国内でもサプライチェーン全体に影響が及ぶインシデントが相次いでおり、サイバーリスクが企業経営に直結する重要課題であるとの認識は、大企業のみならず中堅・中小企業にも広がりつつあります。
一方で、サプライチェーンの重要な一翼を担う中堅・中小企業では、セキュリティ対策に充てられる予算や人員などのリソースに限界があるのも現実です。
こうした状況を踏まえると、企業経営者が自社のビジネスモデルに応じた対策を講じることはもちろん、業界横断での連携やサプライチェーン全体で支え合う「共助」、さらには政府などによる「公助」を組み合わせた取り組みが不可欠です。社会全体で取り組むべき経営課題として、Japan Cybersecurity Initiative の場も活用し、より実効性を高めていければと考えます。

デロイト トーマツ サイバー合同会社 執行役員

伊藤 益光 氏

サプライチェーン攻撃は事業継続を脅かす常在戦のリスクとなり、経営層には全体を俯瞰したレジリエンス向上の視座が不可欠です。
特にリソースに制約のある地方・中小企業では、対策が「コスト」と見なされがちですが、「事業を止めない」という BCP 意識の高さこそが強みです。この意識を起点に、対策を「事業継続投資」へと転換することが実効性を高める第一歩となります。
しかし、個社努力には限界があります。そこで提言したいのが、英国のモデルを参考に、地域単位で産学官が連携する「サイバークラスター」の形成です。人材育成や脅威情報の共有、相互支援体制を地域エコシステムとして構築するのです。このような地域主導のボトムアップ・アプローチこそが、個社の壁を越え、日本全体のサプライチェーン・レジリエンスを真に高める礎となると確信しています。

公益財団法人 中曽根康弘世界平和研究所 主任研究員

大澤 淳 氏

国民生活に影響が出るサイバー攻撃が顕在化しており、普通の人がサイバー攻撃の被害者となる一方で、普通の人が使う Wi-Fi ルータや IT 機器などが乗っ取られてサイバー攻撃に使われる事例も増えている。意図せずに攻撃の加害者にもなり得る時代が来ているといえよう。そのようななか、誰もが利用する IT 企業の Google が、「国民意識の向上」をテーマに発信することは、日本のサイバー安全を確保する上で大変意義がある。
議論のなかでも、一般の人にどうセキュリティ意識を持ってもらうか、また、地方の中小企業にセキュリティ意識をどう浸透させるかについて有識者会議で検討できたことは、サイバーセキュリティの政策実務面でも、大変有意義であった。今後とも、日本社会のセキュリティ意識の向上のために、Google 社には力を尽くしていただきたい。

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 代表理事

梶浦 敏範 氏

かつては「サイバーセキュリティは技術課題」という誤解が、企業経営者にはありました。しかし近年ランサムウェアなどで事業停止に追い込まれる大企業の姿を見れば、それが誤りだったことは明らかです。したがって今回取り上げられた「経営のためのサイバーセキュリティ」というテーマは、まさに時宜を得たものです。しかし「サイバーセキュリティは経営課題」であることに気づいた経営者は、その後いくつもの課題に直面します。社内体制の整備、IT ガバナンスの確立、従業員への徹底、予算の確保、専門家の採用や育成とサプライチェーンの安全確保。さらには事案が起きた時誰に力を借りるか、その連絡網はどう確保するか等々、対応に対する訓練も欠かせません。経営者にとっては難題ではありますが、今回この場で議論されたようなことを一つ一つ、着実に学んで対処する姿勢があれば、事態は改善してゆくと考えます。

順天堂大学 教授

加藤 雅彦 氏

大学でサイバーセキュリティの教育を行っていると「すそ野を拡大する」ことの困難さを実感する。世間の人々はセキュリティそのものにそれほどの関心は無いばかりか、面倒くさい、難しい、コストがかかるなど、マイナスイメージも多いのではないだろうか。「すそ野を拡大」するためには、マイナスイメージを払しょくすること、加えてプラスイメージを持ってもらうこと、両面からのアプローチが重要と思われる。マイナスイメージに対しては、低コストで簡単にセキュリティ対策が実現できることなどが必要であり、研究者や事業者が努力すべき領域である。また、セキュリティへの理解が自分のメリットにつながるとなれば、人々も興味を持ち、能動的に動くことができるだろう。それには処遇改善など、社会的なバックアップも必要である。「すそ野の拡大」といった人材育成には銀の弾丸は無い。全方位の対策無くして、「すそ野の拡大」は無いのではないだろうか。

一般財団法人 日本サイバー犯罪対策センター 業務執行理事

櫻澤 健一 氏

サイバー犯罪・攻撃は、私たちが使っている様々な IT 機器の技術的な脆弱性を狙っているだけでなく、被害者側の心理、環境、業務フローなどに潜む弱さを確実に狙って行われています。したがって、攻撃の回避や被害の軽減には、「技術・人・環境・仕組み」への対策が必要不可欠です。「気を付けよう」と注意喚起しても、何が狙われているのか、何に注意を払うべきか、どのような対策が有効かなどの情報が確実に発信されなければ、意味がありません。企業であれば、システム担当者が担うべき責任もありますが、それ以上に企業の全体像を把握している経営者が行動するような注意喚起が求められます。

頼ることも重要です。警察（交番）、地方自治体、通信事業者、システム・セキュリティ事業者、金融機関、商工会議所などが、支援できる能力を備え、積極的に行動することが必要なのです。官民連携で、市民・企業の「ネット安全」を守りましょう。

株式会社 BLUE 代表取締役
千葉工業大学変革センター 研究員

篠田 佳奈 氏

日本社会には、公衆衛生や災害対応に見られるように「守る行動」を社会全体で共有する文化が根付いている。サイバーセキュリティも同様に、専門家だけの課題ではなく、社会全体で守る文化として定着させていくことが望ましい。サイバーセキュリティが「デジタル時代の公衆衛生」として、また社会全体で共有されるべき文化として醸成できればと、議論を通じてあらためて感じた。

一方で、技術者に限らず、専門人材の育成においては、教育機関だけでなくコミュニティが大きな役割を担ってきた。コミュニティは学習や実践の機会を提供し、人材を発掘・育成し、人的ネットワークを通じて社会へと接続する場となっている。しかし、教育・コミュニティ・企業を結ぶキャリアパスや企業側の投資、社会における認知は、まだ十分とはいえない状況にある。人材パイプラインを社会の戦略として設計し、社会における文化としての意識醸成と、専門人材育成を並行して進めることが、日本社会におけるサイバーセキュリティの持続的な基盤形成に繋がると考えている。

株式会社セブン＆アイ・ホールディングス 常務執行役員 兼 グループ DX 本部長
株式会社セブン-イレブン・ジャパン 執行役員 システム本部長
SpireX 株式会社 代表取締役社長

西村 出 氏

今回の有識者会議を通じてあらためて痛感したのは、サイバーセキュリティはもはや「IT 部門の課題」ではなく、経営の根幹に関わるリスク管理の問題であるという点です。

小売・流通業においては、サプライチェーンの複雑さと、膨大な顧客データを扱う責任の重さが、他業種以上にセキュリティリスクを高めています。しかし現実には、経営層がサイバーリスクを財務・人材リスクと同列に捉えられているかというと、まだ十分とはいえません。会議での議論でも、経営層と IT 部門の間にある「リスク認識のギャップ」が鋭く指摘されており、深く共感しました。

重要なのは、セキュリティ投資を「コスト」ではなく「信用資本」として位置付ける経営判断です。インシデントが発生してから対応するのではなく、平時から体制を整え、サプライチェーン全体を「見える化」することが、企業価値の維持・向上に直結します。

私自身も経営の一端を担う者として、セキュリティを経営課題に位置付け、主体的に関与する文化を根付かせることが、日本全体のサイバーレジリエンス強化への第一歩だと確信し、まい進していく所存です。

株式会社ラック シニアコンサルタント

持田 啓司 氏

サイバー攻撃の洗練化・巧妙化が進展し、新たなリスクも増大している状況のなかで、組織運営に関わる多様な人材がサイバーセキュリティインシデントの未然防止・被害抑制のために活躍することが必要となっています。

セキュリティ対策を進めるためには、サイバーセキュリティの専門知識を持った人材の育成・確保が必要です。

しかし、昨今のサイバーセキュリティリスクに対抗するには、実際に事業推進を行う事業部門の従業員も、セキュリティ専門部署・人材を支援し、自ら行動するフォロワーシップが求められますし、それぞれの業務に関係するサイバーリスクを知り、有事の際には早期復旧を支える必要があるのです。

このように、サイバーセキュリティに関わる人材のすそ野拡大を進めることが、組織を強くし、ひいては日本全体のサイバーセキュリティ強化に繋がっていくものと考えています。

国際大学グローバル・コミュニケーション・センター（GLOCOM）　教授 博士（経済学）

山口 真一 氏

サイバーセキュリティの問題は、技術的な対策だけで解決できるものではなく、人々の意識や行動が大きく影響する社会的課題です。デジタル化が進む現在、一人ひとりの行動は個人の被害に留まらず、社会全体の安全や信頼にも関わります。その意味で、「国民意識の向上」は極めて重要なテーマです。

とりわけ大切なのは、一度きりの啓発ではなく、行動変容に繋がる取り組みを継続していくことです。人は知識を得ただけでは必ずしも行動を変えるとは限りません。リスクを自分ごととして理解し、日常の行動のなかで自然に安全な選択ができる環境を整えることが重要です。

政府、企業、教育機関などのステークホルダーが連携し、分かりやすく実践的な情報発信や教育啓発を積み重ねていくことが、日本社会全体のサイバーセキュリティ水準の向上に繋がると考えています。

免責事項

本レポートは、Google 日本法人（以下「当社」）が主催する Japan Cybersecurity Initiative における議論および調査結果を取りまとめたものです。

本レポートに記載された情報・見解・分析は、執筆時点における有識者の知見および調査データに基づくものであり、当社の公式見解を代表するものではありません。また、情報セキュリティの脅威・技術・規制環境は急速に変化するため、本レポートの内容が常に最新の状況を反映しているとは限りません。

本レポートは情報提供および参考資料の提供を目的としており、特定のセキュリティ対策・製品・サービスの導入を推奨・保証するものではありません。本レポートの内容に基づいて行われた判断・対応・意思決定により生じたいかなる損害・損失についても、当社およびレポート執筆に関わった有識者は責任を負いかねます。

本レポートに含まれる第三者のデータ・引用・統計については、各出典元の情報に基づくものであり、当社はその正確性・完全性を保証しません。

独自調査データ 本レポートを構成するにあたり、以下の JCI 独自調査が実施・引用されています。

- JCI「サイバーセキュリティ調査（第 1 回）」
  対象: 日本国内在住の 12 歳〜60 歳、計 2,000 人　実施時期・方法: 2025 年 11 月実施（オンライン）
- JCI「サイバーセキュリティ調査（第 2 回）」
  対象: 日本国内在住の経営者・役員クラス、計 1,000 人　実施時期・方法: 2025 年 12 月実施（オンライン）
- JCI「サイバーセキュリティ調査（第 3 回）」
  対象: 日本国内在住の経営者・役員クラス、人事担当者、サイバーセキュリティ関与者 各 500 人（計 1,500 人）
  実施時期・方法: 2026 年 2 月実施（オンライン）

※本文およびグラフ内のデータ構成比の算出にあたっては、小数点第 2 位以下を四捨五入しているため、内訳の合計が 100%と一致しない場合があります。

引用・参照されている主な外部資料・フレームワーク

- ISC2（Cybersecurity Certifications and Continuing Education）:「ISC2 Cybersecurity Workforce Study」（2024 年公表版、2025 年版）
- 米国立標準技術研究所（NIST）:「NICE フレームワーク コンポーネント v2.1.0」（2025 年 12 月）、「サイバーセキュリティフレームワーク（CSF）」
- CyberSeek：米国におけるセキュリティ人材に関する調査プロジェクト
- 経済産業省/独立行政法人情報処理推進機構（IPA）:
  「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」（2019 年公表）　「サイバーセキュリティ経営ガイドライン」
- 内閣官房 国家サイバー統括室（NCO）:「サイバーセキュリティ人材フレームワーク」（策定中）


Google