日本のデジタル安全保障を支えるサイバーセキュリティ

～安全保障を契機とした官民サイバーセキュリティ思想の転回を～

本財団の 2022 年度事業の一つとしてデジタル経済に関して有識者を集め、調査を通じて、セキュリティに関する新たな提言をまとめた。13 ヵ国調査の概要と、議論・インタビューを通じて改めて浮き彫りにした日本のサイバーセキュリティの現状と対応策について、特に最近の方針転換が著しい「サイバー安全保障」と「サイバーセキュリティ」の間の双方向の関係が深まりつつあることを述べる。従来の日本のサイバーセキュリティの課題を、「安全保障」議論の中で捉えることにより、より明確な位置付けと方向性、動機づけが図れる。

1. セキュリティ、その守るべき対象が「個」から「全体」へ

本財団では、2022 年度に「データの利活用とセキュリティに関する意識調査」（資料編参照）と、「デジタルニューノーマルへの環境整備に関するタスクフォース」を運営し、日本におけるセキュリティ議論についての課題の明確化と対応策の提言を目指して活動してきた。

議論において、特に共通の関心対象となったのが、①脅威の多様化、②多様な対抗手段の可能性、③顕著になる安全保障要素、の 3 点であった。最初の 2 点（①と②）により、これまでの「専門分野」として独立性高く捉えられていたセキュリティ議論の対象が格段に多様化し、社会的課題（ランサムウェア等）化したことで、無数の「守るべきもの」（無線通信機器、IoT、データ、風評、人権等）が新たに生じてきたことが懸念された。

こうした変化に対応するためには、官民はじめ、全てのステークホルダーが協力し、議論に参加する必要がある。一個人、一企業だけを考えるのではなく、少なくとも日本全体規模での「デジタル安全保障」確保のためのサイバーセキュリティを意識しなくてはならない。

政府における政策議論もこの方向にあることは歓迎できる。2022 年 12 月に閣議決定された「国家安全保障戦略」の中での「能動的サイバー防御」の記述は、これまでの「防御」一辺倒であったセキュリティ思想を前進させることに役立つだろう。タスクフォースでも議論された国家を背景に持つサイバー攻撃に対抗するためには、これまでの常識からくる日本特有のセキュリティ文化の一部をあらためて行く必要もあるだろう。

この提言書においては、新たな時代に向けて、日本を主語としたサイバーセキュリティ思想の転回についての考えをまとめる。現在の変化はまだ「兆し」かもしれないが、近い将来ここで述べられたことの一端でも大きく進展し、激動する世界情勢の中で日本のデジタル安全保障が安定して確立する一助になることを願う。

2. サイバーセキュリティにおける日本の課題

2.1. 2022 年 13 ヵ国調査の概要（詳細報告は付録を参照）

調査は、日本（JP)、アメリカ（US)、シンガポール（SG)、フィリピン（PH)、インド（IN)、オーストラリア（AU)、中国（CN)、タイ（TH)、インドネシア（ID)、台湾（TW)、マレーシア（MY)、ベトナム（VN)、ベルギー（BE） の合計 13 か国を対象に、2022 年 4 月に行った。回答者数は各国で各属性それぞれ 100 名、合わせて 400 名に達するまで募集して、総合計 5,200 名である。それぞれ、主観的なセキュリティに関する意識と、実際に日常生活、勤務を通じて行っている行動を質問し、その中から共通した特徴、各国の特徴と中でも日本の特異性を見出そうとしたものである。以下、この調査の一部ではあるが、本提言の結論に結びつく部分のみを抜粋して紹介する。

[対策の遅れ]（企業・消費者ともに日本のセキュリティ対策が遅れている）

勤労者の勤務先が導入しているセキュリティ管理策の数について、日本は 13 か国中 12 位であり、米国やアジア諸国に比べて遅れている。特に、「対策なし」の回答は目立って多かった（図表 1)。また、消費者が実施しているセキュリティ管理策に至っては 13 か国中最も少なく、対策なしの回答が最も多かった（図表 2)。言語の壁に守られるなど、サイバーセキュリティを脅威として感じる機会が少なかった理由もあるのかもしれないが、攻撃者の目からするとこうした日本の現状は格好の標的となりうる。

[他者への無関心]（日本では取引の際、他社・他者のセキュリティ対策は無関心）

取引先（サプライチェーン）からセキュリティを理由として排除された経験は他国に比べて少なく（図表 3)、セキュリティに関する規制によりビジネスモデルの変換を迫られた比率も日本が極端に低い（図表 4)。事象の表面化の頻度自体が少ないこともあるだろうが、個々の企業の中での対策に専念し、取引先企業・関連企業のセキュリティの管理については関心が少ないことの結果と見られる。産業分野全体、社会全体としてのセキュリティを共同で向上させる経験がないことが他国との比較で推測される。

[希薄な経営者意識]（経営課題としてのセキュリティ意識は日本が最も低い）

セキュリティ対策のきっかけはトップダウンであることは他国と大差はないが（図表 5)、セキュリティ対策への CEO の関与は他国に比べ少なく、特に「経営者は対策の重要性を理解していない」との回答は目立って多かった（図表 6)。情報システムは、依然として道具にすぎず、経営の関心事項の中核にはなっていない現状から、「何事もなく安全に運用されていて当たり前」という意識から、なかなか離れられていない。

[ユーザーの無関心]（消費者も勤労者もユーザーとしてのセキュリティに対する関心が低い）

セキュリティやネット上のリスクに関する用語のうち、聞いたこともない気にかけたこともない言葉をすべて選択する問について、消費者も勤労者も日本の選択数が最も多く、関心のある項目を選択する問についても、消費者も勤労者も、日本が最も少なかった（図表 7、図表 8)。地政学上の

著しい環境変化により、天然の水際対策に守られていた日本の環境が一気に悪化する恐れがあるだろう。サービスの提供者側だけに努力を求めるだけでは限界が近い。

2.2. 課題をめぐる顕著な論点と新たな視点（議論と対話と通じて）

有識者によるタスクフォースやインタビューを通じて、統計的な分析を補足した。2022 年度の議論と会話の中から、特に重要とされた項目を紹介する。

[形式主義からの脱却]（日本のセキュリティは形式的で、役割を演じるだけの「セキュリティシアター」）

PPAP（日本に特有の暗号化付き圧縮ファイルをメールで送り、直後にその解除パスワードを別メールだが同じ経路で送る習慣）に代表されるように、セキュリティ事象の本質を捉えきれず、一度習慣として定着した形式的な対策を維持し続けるのが責任と考えてしまう傾向がある。結果、暗号化されていることにより、サーバー側で添付ファイルに潜む脅威のチェックができないなど、かえってリスクを増大させているなどの批判があるが、一度根付いた習慣をなかなか変えようとする機運が高まらない。

「セキュリティシアター」も同様の概念であり、作られた「型」を遵守してそこから逸脱せず、役割を演じることが最重要とみなされ、環境の変化や本質的な脅威に対応できない。また、事前対策としては有効であるが、脅威が現実化したあとのレジリアンス対応においては、お手本とすべき「型」やマニュアルが存在しない場合、対応策を見失い混乱が広がる傾向にある。

[人材・教育]（人材開発、セキュリティ教育の貧弱さが課題）

セキュリティ対策は企業経営上、最低限に抑えるべき「コスト」であるという考え方から抜け出せず、「何事もなく安全に稼働している状態が当たり前」という経営側の意識もあり、人材に投資をして対策を充実させようとする意識を持ちにくいことも事実である。そうしたセキュリティ管理部門に専任の人材を充当できる企業は、ある程度の規模以上のものに限られる。また、一般にセキュリティ関連の技能・知識・経験を持つ人材は希少であると同時に彼らのキャリアパスも十分整備されていないので、その役割の重要性に見合う報酬も提供できていない。さらに、従業員に対し、日常業務の中で時間を捻出してセキュリティ関係の知識を習得させるような余裕がある企業は限られる。

[新たな手法へ展開]（サイバー保険など、新たな手法によるリスクに対応の活用と留意点）

OECD のサイバーセキュリティに関する報告書が議論の中で紹介されたが、その中で新しいタイプの対策実効化の動きとして、「サイバー保険」が話題となった。日本でもすでに保険商品に取り組んでいる企業もある。過度の安心感により本来の対策が疎かにならないよう配慮も必要との意見があったが、一方で単に「セキュリティは重要」と唱え続けることから一歩踏み出すこともできる。保険加入に伴う各企業の実態の診断を経て、予防措置や対策を高度なものにするモティベーションを与える（保険契約条件を優遇）など、意識を高めるきっかけづくりになる可能性がある。

[設計思想]（デジタル変革と表裏一体としてのセキュリティ・バイ・デザイン）

セキュリティ対策は長い間、本来のシステム機能に後から必要に応じて追加される付属品として捉えられていた。コロナ禍の社会状況変化も後押しして、利益を生み出し新たな事業を展開し収益に結びつける「デジタル変革」は、濃淡あるものの成果を挙げつつある。一方で、付随機能としてのセキュリティ対策については、受動的発想でシステムの動作を監視、制限する付け足し機能の範囲からなかなか進展していない。

システム設計の最初の段階からリスクを排除・低減する思想を持ち、新たなコストや付加機能に頼らない、「バイ・デザイン」思想が提唱され続けているが、特に日本においてはより「能動的」な対応に転化させるため、もう一段の意識改革が必要である。

[協力・参加意識]（社会全体、サプライチェーンを通じた協力・参加意識）

米国はじめ海外においては、民間事業者への攻撃情報が官民・民民で共有され、攻撃方法の分析と対処、予防につなげる機能がある程度役割を果たしているところも多い。日本においては個別企業や産業分野などで CERT や CSIRT（対応チーム）の設置を広げる活動が進んでいるが、さらに大きな情報共有、対応協力の仕組みが求められる。また、議論や活動を通じて、参加意識を高めていくことにもつながる。

[教訓を生かす]（大規模なインシデントを教訓として危機意識を高めていった米国）

「なぜ日本において危機意識が低いままなのか」をめぐる議論では、日本における大規模インシデント（事件）が狭い範囲の一過性の事件として集結してしまい、その後の分析、再対策の努力が個別に消極的に行われるだけで終わってしまう傾向にあることが指摘された。米国では大規模なインシデント等が大々的に報道され、継続して議論を重ね、対策の評価にも専門家が参加する。このため企業や政府機関のセキュリティに対する危機感が高くなったといえる。

[競争力に結びつける]（実効性のあるセキュリティ対策を競争力として、グローバル市場を目指すアジア企業）

アンケート調査結果に関する議論において、日本を除く各国の勤労者が、いずれもセキュリティ対策をより積極的な競争力要素として捉え、リスク評価に従い包括的なガバナンス対策を行う意識が高いことが語られた。アジア諸国においてもセキュリティ上の信頼を競争力と捉え、グローバル市場へ参入するための条件として能動的に捉えている。

2.3. 内部改革、外部連携、長期視点による日本のサイバーセキュリティ改革

前節までで、①13 カ国アンケート調査、②タスクフォースにおける議論、③国内外有識者へのインタビュー結果を通じて、課題と改善の方向性について述べた。これらを改めて俯瞰してみると、「内部改革」、「外部連携」、「長期視点」の 3 つの共通した行動の要点が浮かび上がる。これらは現状をめぐる調査と議論において、共通して語れる横串となり、また実効性のある行動計画を考える際の基礎となる。

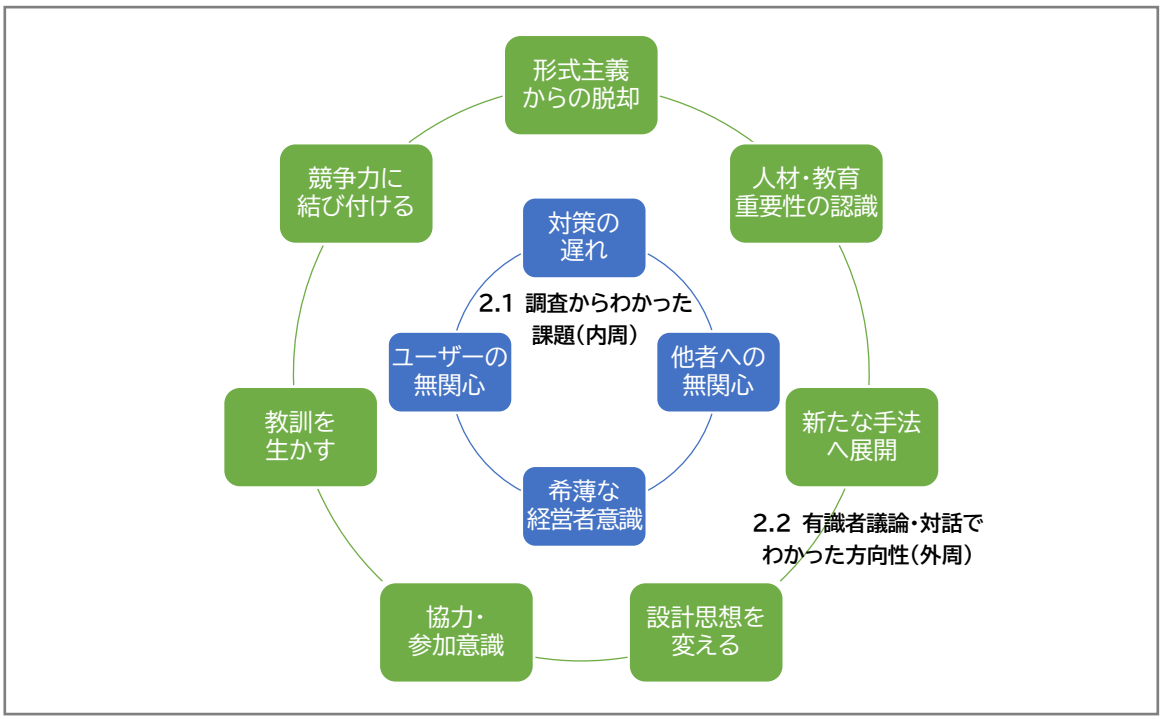


図 1　日本のサイバーセキュリティ課題と改善の方向性

（内部改革）まずは企業内部の改革を

図 1 に示された課題各項目のうち、『対策の遅れ』、『経営者意識』、『ユーザーの無関心』については、企業内部の問題として真剣に取り組むことが急務である。その結果、『形式主義からの脱却』、サイバー保険を適切に活用し、『参加意識を高める』など解決方向性の各項目については、まず企業内部の改革に取り組むことが必要である。

そうした日本に特徴的な悪習慣は、セキュリティに限らないが、たとえば、PPAP からなかなか抜け出せないでいる理由として、「新たな仕組みへ移行する際の責任をとりたくない」という意識が強い可能性がある。これまでは変化が少なくセキュリティ脅威を身近に感じることがなかった日本において、「環境変化に対応する必要性」を実感して行動に起こせる経営者は一握りに限られるであろう。

経営的側面においては、サイバー保険などの新たな仕組みに懐疑的であることや、リスク対策を競争力と捉えて積極的に取り組みを進める意識の低さが目立つ。これらは日本に特徴的な責任回避型マネジメントと考えられ、抜本的な企業内部改革を経ないと改善は実現できないであろう。

「新たな発想」を採用することに消極的なのは消費者ユーザーも同じではないかと考えられる。自己の評価基準よりはインフルエンサーなどの影響力に身を委ね、そうしたきっかけがない限り、合理的であっても新しいものに鈍感な層は一定数存在するようである。そうでないグループの存在を否定するものではないが、総じてかなり大きなインパクトがない限り、新たなリスクは「回避姿勢」が基本となる。

（外部連携）他社・他者、異業種との連携

図 1 に示した項目の中には、個社の内部の改革と同様に、外部との連携が必要な項目が多い。

「形式主義」、「新たな手法」への取り組みは、直接利益やコスト削減には結びつかないだろう。事業に直接関連する企業間連携について、日本は比較的意識が強いが、サイバーセキュリティについては、「本業の付け足し」としての認識が強く「他社との連携」に積極的になれない。さらに協力・連携にまで至らず、サイバー攻撃を受けた場合にも情報を抱え込んでしまい、広く警戒感を共有する前に、自社の名誉を重んじるような傾向も懸念される。

「協力・参加意識」を意図的に醸成する必要があり、このためには産業団体、経済団体の役割が大きいだろう。また、その中には図 1 において、「教訓を活かす」を重点的に考えるべきである。教訓を個社だけでなく社会全体に共有し、全体最適を図ることでリスクを低下させることが必要であり、そのために「他社」のみならずあらゆる連携先を含めた「他者」を意識する必要がある。つまり、「新たな手法の展開」においても、その適用の対象を個社のみならず業界全体、社会全体にまで広げて考える発想が求められる。

「協力によるセキュリティ確保」、つまり「コラボラティブ・セキュリティ（collaborative security）」という言葉についても今回議論されたが、攻撃があった際の情報連携、レスポンスにおける連携、消費者も含むユーザーとの連携が今後必要とされるだろう。

（長期的視点）長期的視点に立つ息の長い対策が必要

ここまでの論点は全て、長期的視点の必要性にも繋がっている。人材・教育の点で、サイバーセキュリティの確保に必要な技術では、ネットワークに関する知識が基礎となる。しかしながら、情報技術者処理試験の応募、合格状況を見ると、必ずしもネットワーク技術者の分野は人気が高くないようである。直接収益に結びつくというよりは、コストカットの対象とすべき部分として捉えられているためかもしれない。

長期的な視点は、「設計思想を変える」ためにも必要である。セキュリティ・バイ・デザイン、つまり設計時にセキュリティ対策を内包した思想が重要なことを掛け声のみで終わらせてはならない。この視点が欠けると、セキュリティ維持をコストとしか捉えられず、その場しのぎのセキュリティ維持体制や欠員補充、安定した運用、日々の組織としてのスキルアップなどについて配慮が疎かにもなり、形式主義的なセキュリティ対策からも抜け出せない。

3. 「サイバー安全保障」への転換（安全保障文書改訂を契機として）

（2022 年 12 月「防衛 3 文書改訂」）

2022 年末、政府は安全保障政策に関する 3 文書（国家安全保障戦略、国家防衛戦略、防衛力整備計画）の改定を閣議決定した。中でも内閣官房の NISC（内閣サイバーセキュリティセンター）の中に「サイバー安全保障体制整備準備室」が設置され、サイバー安全保障分野の政策を一元的に総合調整することが予定されていることは、前章までに述べた日本の多くの課題に立ち向かうために、大きな契機となることが期待される。

サイバー安全保障分野における対応能力の向上を図り、主要国並みとすることを目的としており、（1）能動的サイバー防御の導入（2）民間部門のサイバーセキュリティ強化（3）政府機関のサイバーセキュリティ強化（4）サイバー安全保障に関する政府内の体制・法制度・国際連携――などに取り組むとされる。

中でも「能動的サイバー防御」は、これまで実質「攻撃や被害を受けてから」始まっていた、政府や民間の対応を一歩進めて、「可能な限り未然に攻撃者のサーバー等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする」[1]と明記され、これまでの概念を大きく転換する。サイバーセキュリティをより大きな国家戦略として「安全保障」に結びつけたことで、軍事的な国家防衛、経済安全保障、技術安全保障、データの安全保障、ネットワークの安全保障と言ったより広く「守るべき対象」と必要な連携体制が示された。

まず、サイバー犯罪に対する刑事法の整備が重要である。サイバー攻撃やデータ侵害、不正アクセスなどの行為に対して、明確な罰則を規定する法律が必要である。これにより、犯罪者への抑止力を高めることができる。

また、個人情報や機密情報の保護に関する法的枠組みも重要である。個人情報保護法との整合性や、企業が適切なセキュリティ対策を講じることを促す法律の整備が必要である。個人や組織のデータを適切に保護するためには、情報漏洩や不正利用への罰則が明確に定められた法律が必要である。特に改正電気通信事業法（2023 年 6 月 16 日施行）や不正アクセス禁止法を念頭に、どのような状況下で攻撃側の通信情報を取得できるか条件を詰める必要がある。

（2023 年 7 月「サイバーセキュリティ 2023」）

さらに、国家レベルのサイバーセキュリティに関する法的枠組みも整備されるべきである。内閣官房より「サイバーセキュリティ 2023」が 2023 年 7 月 4 日に発表され、国家の重要インフラや政府機関へのサイバー攻撃に対する防御策や対応策を規定したが、上記の改正電気通信事業法のように、今後は各事業分野における既存法制度が実効的に機能できるよう、関連法制度や規則、省令、ガイドライン等との整合性を図ることが必要である。これにより、国家の安全保障を確保し、サイバー攻撃に対して迅速かつ効果的な対策を講じることができる。

サイバー安全保障における法制度整備は、社会全体のセキュリティを確保するために不可欠である。法的枠組みの整備により、サイバー犯罪の摘発や防止、個人や組織のデータ保護、国家の安全保障を強化することができる。

---

[1] 内閣官房「国家安全保障戦略 2022」30 頁

（方向性を明示しつつあるサイバー安全保障戦略）

従来はバランスよく多様な対応策や選択を、多方向に向けて対応してきた感がある。これに対して、地政学的な緊張やサイバーセキュリティの脅威の変化を踏まえて、最近のサイバーセキュリティ議論においては、より方向性を明確にした方針が示されるようになったことは歓迎すべきである。

例えば、「友好国」とする民主主義と法の支配の尊重を共有する各国との連携を優先することで、国際間の協力を迅速に進めることができる。また上記「サイバーセキュリティ 2023」計画においても、特に ASEAN 諸国を含むインド太平洋および島嶼国支援、日米豪印（いわゆる QUAD）のランサムウェア対策連携が特に国際連携の計画として記されている。

急速に変化しつつある環境の中で、より能動的、機動的にサイバーセキュリティ対策を捉える機運が熟しつつある今、安全保障意識の高まりを契機として、社会全体における変革の必要性を捉えるべきである。サイバーセキュリティを真に動かすために、この機会に社会全体での取り組みを進めるべきであろう。

4. 2023 年「サイバー安全保障」議論を契機とした５提言

これまで日本のサイバーセキュリティについての課題認識(2.1 節)、変革の方向性（2.2 節）を整理し、内部改革、外部連携、長期的視点という 3 つの要素(2.3 節）の重要性を述べた。また、昨年末頃からの「安全保障」意識の高まりが、サイバーセキュリティのこれまでの課題を大きく変革させる契機となりうることを述べた(3 章)。

こうした変化を捉えて、本財団のみならず政府・学術界・民間それぞれ多くの主体が新たなサイバーセキュリティに関する提言を発信している状況の中で、重複を恐れず本財団においても重要な項目について３年間にわたる事業の成果として提起しておきたい。提言を構成するのは次の５項目である。それぞれ 2.3 節の分類である内部改革、外部連携、長期視点のそれぞれからまとめている。

（提言１）サイバー安全保障に合わせた企業の組織改革（内部改革）
（提言２）教育・資格・人材制度の戦略的改革（内部改革）
（提言３）サプライチェーン連携の強化（外部連携）
（提言４）省庁間連携と官民連携の強化（外部連携）
（提言５）国際視点を持ったサイバーセキュリティへ（長期視点）

4.1. （提言 1）サイバー安全保障に合わせた企業の組織改革（内部改革）

サイバー安全保障に合わせた企業の組織改革は、2.3 節に挙げた内部改革の一つである。調査においても日本が遅れている点の一つであり、また有識者議論との対話においても重要事項として必ず挙げられた項目である。企業がサイバーセキュリティを重視し、組織全体でのセキュリティ意識と対策レベルを高めるため、事業環境における「安全保障」の確保と能動的サイバー防御の考え方を通じて、後向きではなく競争力の源泉としてセキュリティに取り組むことが必要である。以下に、その一例をいくつか示す。

- 経営層の意識改革を促す: まず、企業トップの技術的な知識、経営課題としての認識を醸成する必要がある。ランサムウェアやサイバー攻撃による実害が蓄積されている中で徐々に改善されているが、中小企業を含めより加速した意識改革が必要である。
- サイバーセキュリティ専門チームの設置: サイバーセキュリティを専門に担当するチームや部署を設置することで、組織内でのセキュリティ対策を一元的に統括し、専門知識を活用してセキュリティの強化を図ることができる。
- セキュリティポリシーの策定によるガバナンスの強化: 組織全体でのセキュリティ方針やガイドラインを策定し、従業員に周知徹底することが重要である。組織としてのセキュリティポリシーを明確にすることで、セキュリティ対策を組織全体で一貫して実施することができ、ガバナンスが強化される。
- セキュリティ教育・トレーニングの実施: 提言２で詳細を触れるが、経営課題としても重要な項目である。全従業員に対して定期的なセキュリティ教育やトレーニングを実施することで、サイバーセキュリティの重要性や最新の脅威についての情報を共有し、従業員の

セキュリティ意識を向上させることができる。

- インシデント対応体制の整備: セキュリティインシデントが発生した場合、迅速かつ適切に対応するために、対応プロセスやチームを整備することが重要である。インシデントの検知、分析、対応のための手順や責任を明確にし、組織内での迅速な対応を実現する。
- サプライチェーンのセキュリティリスク管理: 提言 3 と関連するが、サプライチェーンを構成するパートナーやサプライヤーのセキュリティ対策を管理することも重要である。セキュリティ要件を含んだ契約や取引条件を設定し、必要な点検・評価・監査を行うことで、サプライチェーン全体のセキュリティを確保する。

これらの取り組みにより、企業は組織全体でのサイバーセキュリティの重要性を認識し、適切な対策を講じることができる。また、外部のセキュリティ専門家やコンサルタントとの協力や、業界団体との情報共有も重要な要素となる。

4.2. （提言２）教育・資格・人材制度の戦略的改革（内部改革）

教育、資格、人材制度の戦略的改革は、サイバーセキュリティの専門知識とスキルを持つ人材の育成と確保を促進するための重要な取り組みであり、2.2 節において議論の一端を説明している。

- 教育プログラムの充実: サイバーセキュリティに関連する教育プログラムを充実させることが重要である。大学や専門学校におけるサイバーセキュリティのカリキュラムを強化し、専門の研修やトレーニングプログラムを提供することが求められる。
- 資格制度の整備: サイバーセキュリティに関連する資格制度の整備も重要である。これにより、専門知識とスキルを持つ人材を認定することができる。具体的な資格としては、情報セキュリティ管理者（CISM）、情報システム監査人（CISA）、情報セキュリティ専門家（CISSP）などがある。
- 人材育成の支援: サイバーセキュリティの人材育成を支援するためのプログラムや取り組みを展開することも重要である。企業や業界団体が研修や継続教育プログラムを提供し、留学制度を導入し、若手人材の採用や育成に力を入れることが必要である。
- セキュリティ意識の向上: サイバーセキュリティに関連する教育とトレーニングにより、従業員や一般の人々のセキュリティ意識を向上させることも重要である。定期的な教育プログラムや啓発キャンペーンを通じて、サイバーセキュリティの重要性やベストプラクティスについての情報を提供し、セキュリティ意識を高めることが求められる。
- 産学連携の強化: 産業界と学術界の連携を促進することで、実践的なサイバーセキュリティのスキルや知識を育成することができる。企業とのパートナーシップや産学共同研究、インターンシッププログラムなどを通じて、実務経験を積みながら専門知識を身につける機会を提供することが重要である。

これらの戦略的な改革により、サイバーセキュリティの教育や人材育成の環境が整い、適切な人材が企業や組織においてサイバーセキュリティに取り組むことができる。

4.3. （提言３）サプライチェーン連携の強化（外部連携）

サイバーセキュリティにおけるサプライチェーン連携の強化は、重要な取り組みである。現代の

ビジネス環境では、サプライチェーン上の一つの脆弱なポイントでも攻撃が成功すれば、全体のセキュリティが脅かされる可能性があるからである。

- コミュニケーションと情報共有の強化：パートナーとのコミュニケーションと情報共有の強化が重要である。セキュリティに関するベストプラクティスや脅威情報を定期的に共有し、相互に学び合うことで、サプライチェーン全体のセキュリティレベルを向上させることができる。
- セキュリティ要件の策定と遵守：セキュリティに関する契約や取引条件を明確にし、パートナーとの合意を形成することで、セキュリティ対策の一貫性と信頼性を確保することができる。
- 定期的なリスク評価と監査：パートナーのセキュリティ対策やリスク管理体制を定期的に評価し、必要に応じて改善を促すことで、全体のセキュリティを向上させることができる。
- 認証制度の活用：組織として、セキュリティ対策の成熟度を客観的に評価し、その結果得た認証をサプライチェーン上の連携において採用することで、局所的な脆弱性から全体にリスクが広がることをある程度防止することができる。
- 新たなテクノロジーやツールの活用：人工知能（AI）やマシンラーニング、ブロックチェーンなどの技術を活用し、サプライチェーン上の異常な活動や攻撃を監視・検知し、迅速な対応を可能にすることができる。

以上の取り組みにより、サイバーセキュリティにおけるサプライチェーン連携の強化が実現される。サプライチェーン内の全てのパートナーが協力し、セキュリティに対する共通の目標を持ち、持続的なセキュリティの向上を追求することが重要である。

4.4. （提言４）省庁間連携と官民連携の強化（外部連携）

省庁間連携と官民連携の強化は、サイバーセキュリティの重要な要素である。以下に、それぞれの連携の強化における重要性と具体的な取り組みを示す。

- 省庁間連携の強化: 省庁間連携は、政府機関が協力してサイバーセキュリティに対処するために重要である。異なる省庁がそれぞれの専門知識とリソースを共有し、統合的な政策策定を行うことが重要である。

  具体的な取り組みとしては、サイバーセキュリティに関連する省庁や組織の間での定期的な会議や協議の開催、情報共有のプラットフォームの構築、共通のガイドラインや基準の策定などが挙げられる。また、異なる省庁間での人材交流や研修プログラムの実施も重要であり、政府全体でのサイバーセキュリティの一体感と連携を促進する。
- 官民連携の強化: 官民連携は、政府と民間企業が協力してサイバーセキュリティに取り組むために重要である。民間企業はサイバーセキュリティにおいて広範な経験と専門知識を持っており、政府は法的権限と規制の制定において重要な役割を果たしている。

  具体的な取り組みとしては、政府と民間企業の間での定期的な対話や協議の場の提供、セキュリティ情報の共有、脅威情報の交換などが挙げられる。また、民間企業の協力による研究開発プロジェクトや技術移転、セキュリティ対策に関する情報セミナーやワークショップの実施なども重要である。

官民連携の強化により、政府と民間企業は相互に補完し合いながら、より効果的なサイバーセキュリティ対策を実施することができる。情報共有や協力の促進により、早期の脅威の検知や迅速な対応が可能となり、より強固なサイバーセキュリティ体制の構築が期待できる。

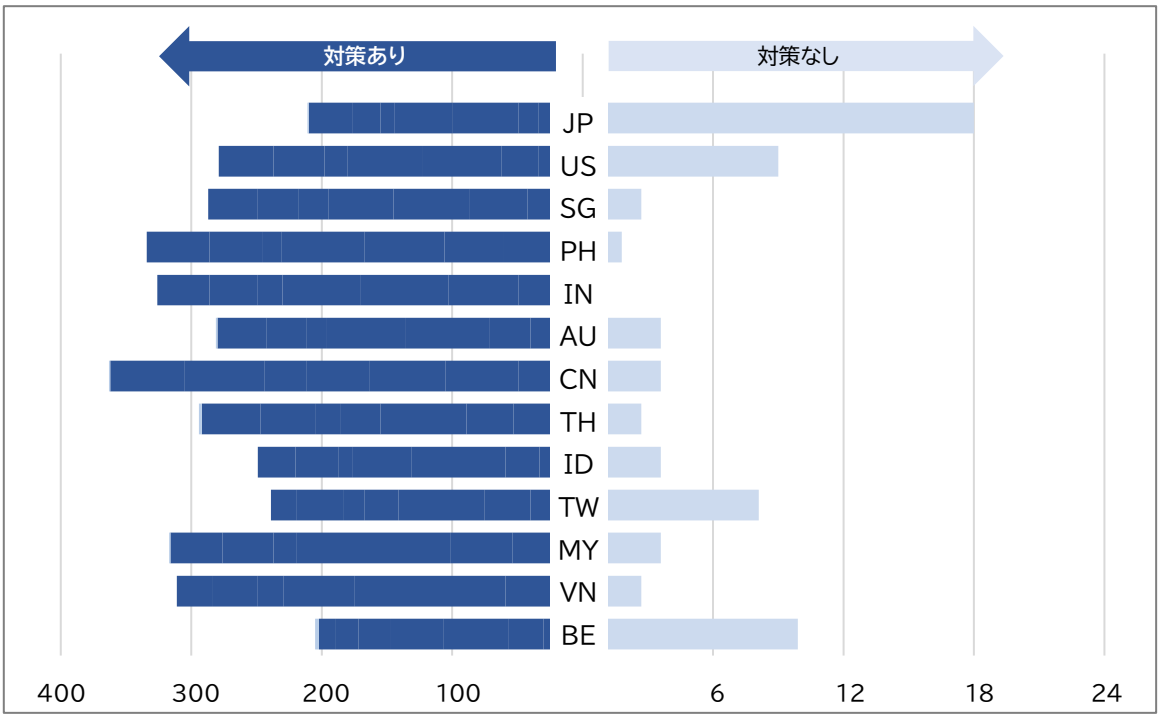
4.5. （提言５）国際視点を持ったサイバーセキュリティへ（長期視点）

国際視点を持ったサイバーセキュリティへの進化は、グローバルなサイバーセキュリティ脅威に対処するために不可欠である。異なる国や組織が連携し、情報共有や協力を通じて、より強固なサイバーセキュリティの実現を目指す必要がある。

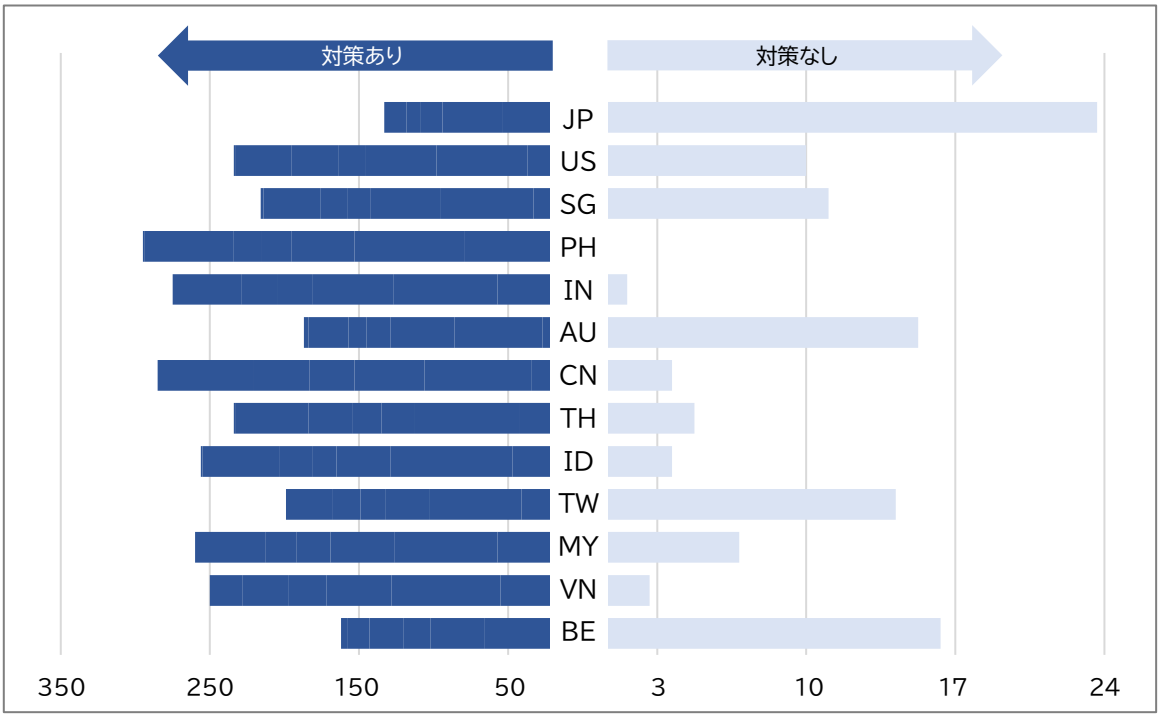
- 国際協力の強化：異なる国や組織間での情報共有や脅威情報の共有、ベストプラクティスの共有を行うことで、グローバルなサイバーセキュリティ対策を推進することができる。国際組織や協定に参加し、共通の目標に向けて連携を深めることも重要である。
- 標準化と規制の促進：国際的なサイバーセキュリティ標準や規制の枠組みの確立を進めることで、異なる国や組織間でのセキュリティのレベルや要件を統一し、一貫性のあるサイバーセキュリティ対策を実現することができるのである。
- サイバーセキュリティ人材の育成：国際的な資格制度や認定プログラムの導入、異文化や異なる法制度に対応できるグローバルな教育プログラムの提供などにより、国際的な視点を持つ人材の育成を促進する必要がある。
- グローバルな情報共有プラットフォームの構築：国際的なサイバーセキュリティ情報の共有は、迅速な脅威の検知や対応において重要である。国際的な情報共有プラットフォームやインシデントレスポンスネットワークの整備により、異なる国や組織がリアルタイムで情報を共有できる仕組みを構築することが必要である。

これらの取り組みにより、国際視点を持ったサイバーセキュリティが実現され、国境を越えた脅威に対処する能力が向上する。グローバルな協力と連携により、より強固なサイバーセキュリティの枠組みが構築され、サイバースペースの安全と信頼性が確保される。

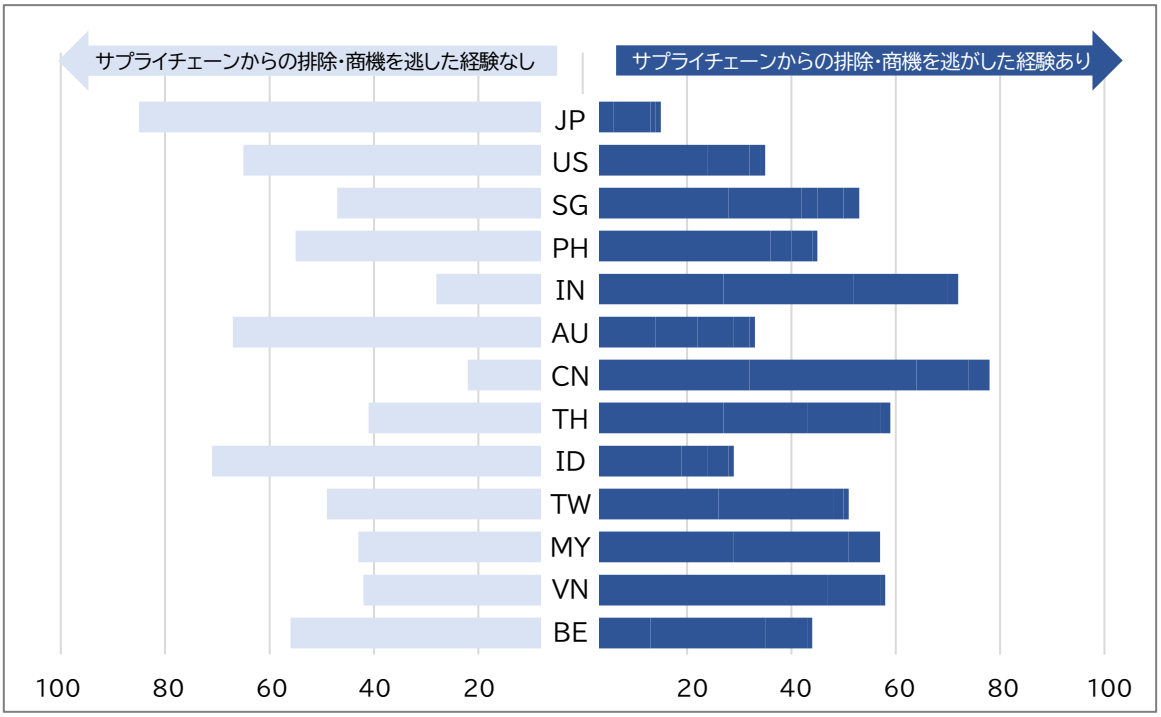
5. 添付　アンケート結果（抜粋）



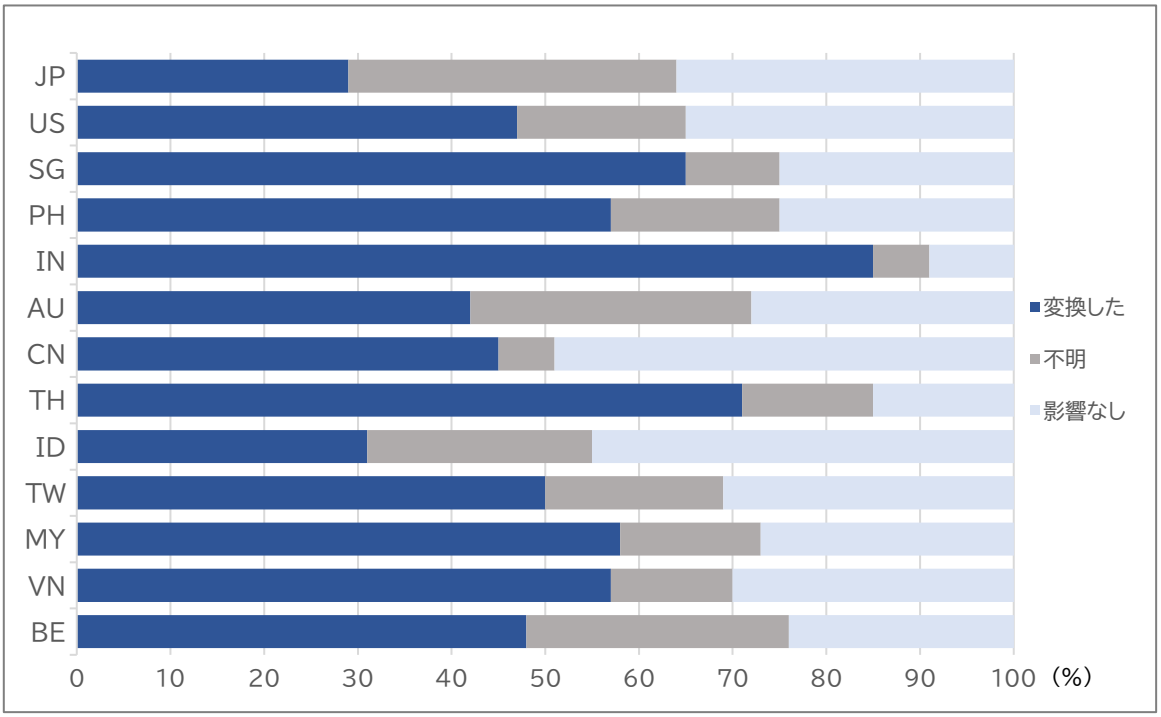
図表 1　勤労者対象・セキュリティ編　実施しているセキュリティ対策



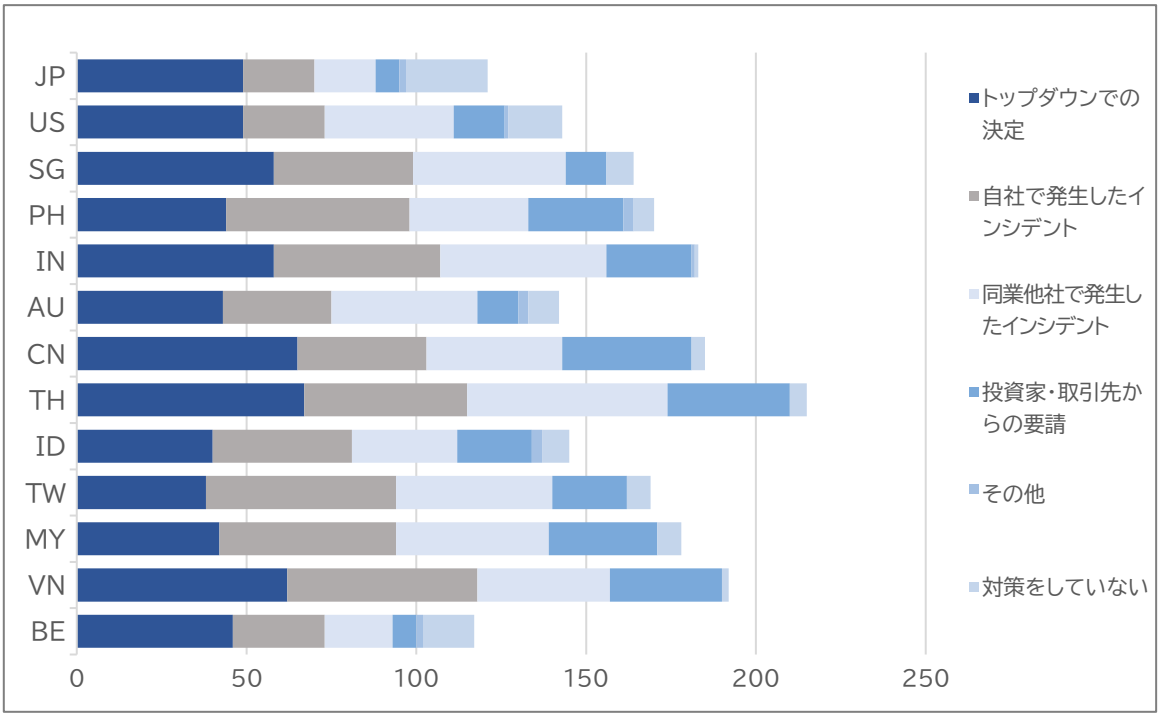
図表 2　消費者対象・セキュリティ編　実施しているセキュリティ対策



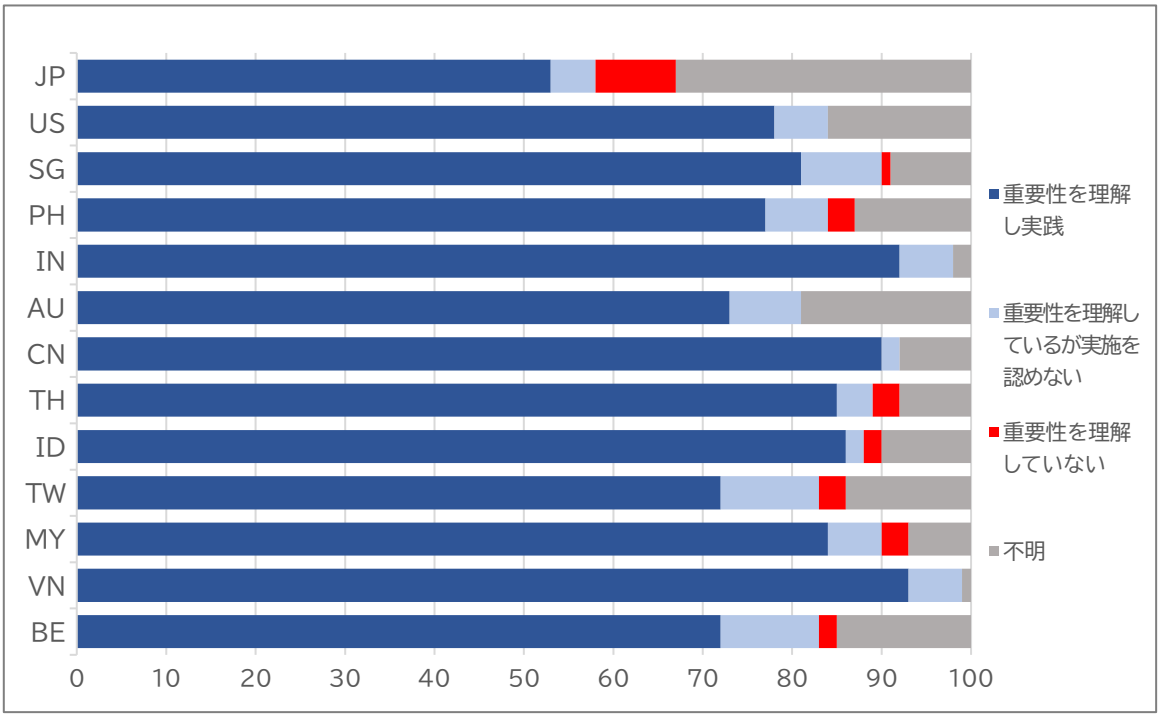
図表 3　勤労者対象・セキュリティ編　サプライチェーンからの排除経験



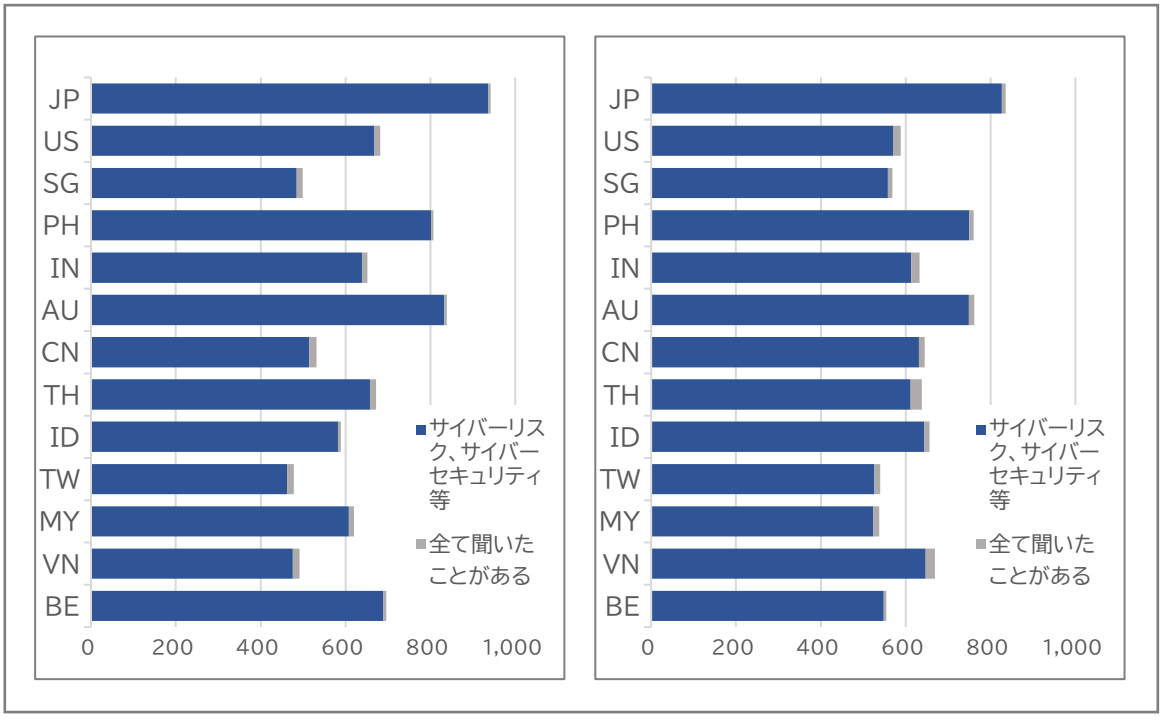
図表 4　勤労者対象・セキュリティ編　セキュリティ規制でビジネスモデル変換を要した経験



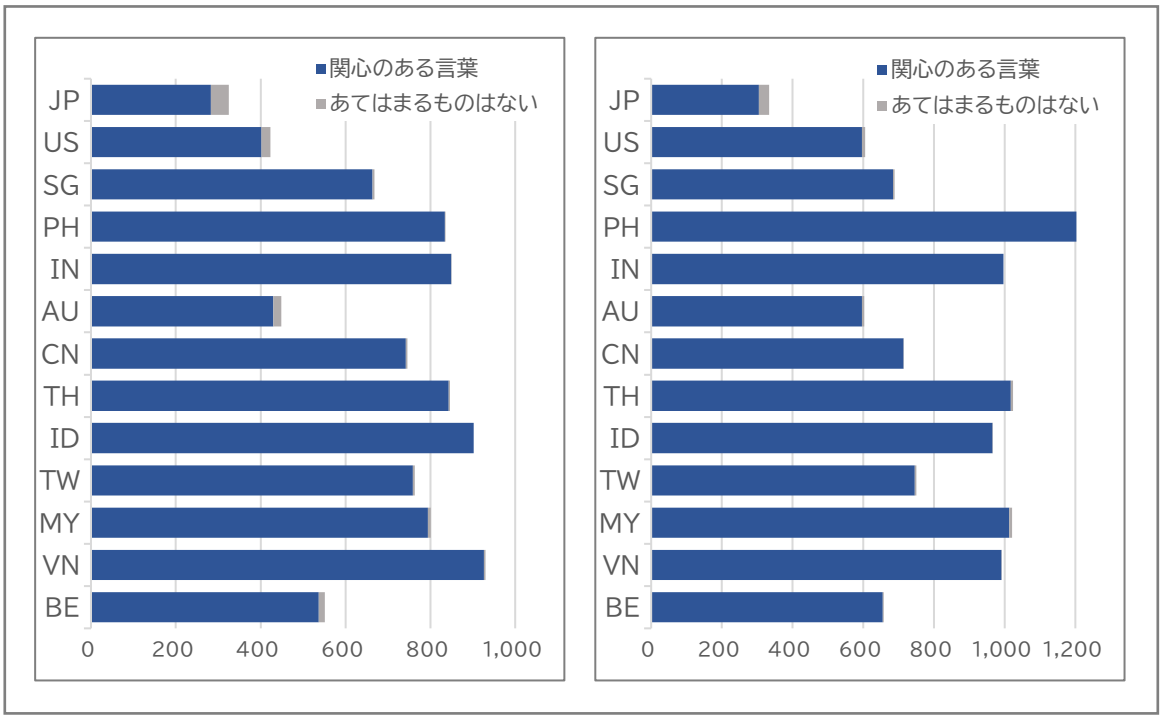
図表 5　勤労者対象・セキュリティ編　セキュリティ対策を取ることになったきっかけ



図表 6　勤労者対象・セキュリティ編　経営者のセキュリティ対策への関与度



図表 7　消費者対象・セキュリティ編　聞いたことも気にかけたこともない言葉



図表 8　勤労者対象・セキュリティ編　聞いたことも気にかけたこともない言葉