KnowBe4
Human error. Conquered.

日本初のセキュリティトレーニングの視点からのサイバーセキュリティ実態調査

はじめに

日本企業を標的とするサイバー攻撃が急増していることは、共通理解となってきています。では、なぜサイバー攻撃が減らないのでしょうか。皆さんの会社や組織は、巨額な資金をサイバーセキュリティ対策に投じているのではないでしょうか。その結果、莫大の数のサイバー攻撃は遮断されています。しかしながら、無視できない数のサイバー攻撃がこのセキュリティ対策の防御網をすり抜けています。

日本企業・団体は、サイバーセキュリティの人的防御対策において立ち遅れているのか？ この実態を知り、今後のサイバーセキュリティの人的防御を考える。

ここには、サイバー攻撃がテクノロジー（IT 部門）の問題と捉えられているという根本的な原因があるとKnowBe4 は考えています。2010 年 8 月の創立以来13 年にわたり、ヒューマンエラーという「人」が抱える生来の問題にフォーカスして、サイバーセキュリティの人的防御対策に取り組んできていますが、全世界でテクノロジー主導のサイバーセキュリティ対策は主流です。これまで、KnowBe4 では、サイバーセキュリティの人的防御対策において日本が立ち遅れていることを指摘してきました。

KnowBe4 は、日本市場におけるセキュリティ教育（セキュリティ意識向上トレーニング）の現状について調査するために、日本企業・団体のオフィスワーカーと IT 意思決定者を対象に実態調査を 2022 年 12 月に実施しました。本稿は、この調査結果を解析して、セキュリティ意識向上トレーニングプログラムにいかに取り組み、サイバーセキュリティの人的防御対策をいかに展開していくべきかを提案するために作成しました。これまで、日本では、独立行政法人情報処理推進機構（IPA）が情報セキュリティに対する意識調査や実態調査を実施していますが、セキュリティトレーニングの視点からのサイバーセキュリティ実態調査*は日本では行われていません。

KnowBe4 が実施したサイバーセキュリティ実態調査について

本実態調査は、日本のほか、オーストラリアおよびシンガポールにおいても同一設問で実施されました。不特定多数を対象にした、開かれた実態調査とするために、KnowBe4 の社名は一切公開せずに行われました。日本においては、2022 年 12 月 9 日～14 日の間に日本企業および団体を対象に無作為抽出でオンラインにて実施されました。本調査アンケートは、日本においては株式会社日本リサーチセンター（NRC）と共同で、英国市場調査会社 YouGov 社によって日本語によって収集され、YouGov 社によって統計集計され、その後、KnowBe4 Japan が分析しました。

- **調査対象者およびサンプル数**:
  - **日本企業・団体のオフィスワーカー 1,038 名（業種不問）**
    （IT およびサイバーセキュリティに関する意思決定権を持たないオフィス勤務者、在宅勤務者を含む）
  - **日本企業・団体の IT 意思決定者　225 名（業種不問）**
    （IT およびサイバーセキュリティに関する意思決定権を持つ上級管理職、IT 担当マネージャーおよびセキュリティ担当者を含む）
- **アンケート調査票は YouGov が英文で作成し、NRC が日本語に翻訳しています。**
- **インタビュー終了後、オフィスワーカーのデータは、日本の最新の人口推計を反映し、年齢、性別、地域による重み付けが行われました。**
- **本稿では、日本企業および団体のオフィスワーカー（IT およびサイバーセキュリティに関する意思決定権を持たないオフィス勤務者）の方と IT 意思決定者（IT およびサイバーセキュリティに関する意思決定権を持つ上級管理職）の両方の調査結果を対比して統計分析しています。**

*独立行政法人情報処理推進機構（IPA）が情報セキュリティに対する意識調査や実態調査については、https://www.ipa.go.jp/security/products/products.html を参照してください。

本サイバーセキュリティ実態調査の注目ポイント

KnowBe4 では、次の 9 つの注目ポイントとしてまとめています。

- **業務環境でのメール/SMS の利用について**
- **フィッシングと BEC（ビジネスメール詐欺）のリスクについて**
- **職場でサイバーセキュリティのトレーニングについて**
- **ITチームの支援について**
- **2023 年に投資／支出を計画しているサイバーセキュリティ対策について**
- **セキュリティカルチャーについて**
- **フィッシングメールの見極めについて**
- **サイバーセキュリティ攻撃から組織を守る責任の所在について**
- **サイバーセキュリティ対策における政府の責任について**

この詳細については、本稿の添付資料をご参照ください。

本稿では、日本、オーストラリア、シンガポールの 3 地域の調査結果を比較することで、日本におけるサイバーセキュリティ対策の現状を次の 7 つから KnowBe4 Japan が考察しています。

- **サイバーセキュリティトレーニングの受講状況と受講者の評価**
- **フィッシングへの対応・報告とフィッシングを見抜く自信**
- **サイバーセキュリティリスクの現状**
- **サイバーセキュリティ攻撃から組織を守る責任の所在**
- **フィッシングと BEC（ビジネスメール詐欺）のリスク**
- **IT チームの支援について**
- **セキュリティカルチャーについて**

考察ポイント1：
サイバーセキュリティトレーニングの受講状況と受講者の評価

最初の考察ポイントとして、本実態調査結果から、日本でのサイバーセキュリティ教育がどれだけ普及しているかを見てみた。サイバーセキュリティ教育を受講したことがない日本のオフィスワーカーは、半数以上の 51%となっている。他の 2 地域と比較してみると、オーストラリアとシンガポールと比べて、日本の受講率は低い。しかしながら、受講者の頻度やトレーニングの形式を見てみる、ほぼ内容的に変わりない。受講トレーニングの評価については、3 地域ともポジティブな評価がネガティブな評価を大幅に上回っている。KnowBe4 が「New School」呼ぶような新しい形態のセキュリティトレーニングがどれだけ受講されているかは、評価のデータ「集合トレーニング」「インタラクティブ」を見る限りでは、日本は他の 2 地域より遅れを取っていると思われる。この調査の結果と日本市場での KnowBe4 の引き合い状況から見ると、日本市場では集合型のセキュリティ教育が主流で、セキュリティ意識向上トレーニングは大手企業では浸透し始めたものの、まだ中堅・中小企業でのセキュリティ意識向上トレーニングは緒についたばかりと KnowBe4 Japan は分析している。

日本のオフィスワーカーの半数以上（51％）がサイバーセキュリティトレーニングを受講していない。これに対して、オーストラリアでは 23%、シンガポールでは 34%が受講していない。

		日本	オーストラリア	シンガポール
サイバーセキュリティに関するトレーニングを受講しているか？				
受講していない		51%	23%	34%
受講している		48%	60%	53%
	フィッシングメールの模擬演習を含むトレーニングを受けている	32%	35%	41%
	年に 2 回受講している	13%	13%	12%
	年に 1 回受講している	26%	13%	21%
どのようなサイバーセキュリティ教育を受けているか？				
対面でのトレーニングを受けている		26%	52%	37%
	講義やプレゼンテーション形式のグループ形式の集合トレーニングを受けている	85%	66%	73%
オンラインでのトレーニングを受けている		75%	63%	72%
	30 分未満の e ラーニングのショートセッションを受けている	78%	65%	73%
受講セキュリティトレーニングの評価				
	「役に立った」	36%	43%	49%
	「自分の職務と関係があった」	24%	40%	38%
	「退屈」	8%	12%	7%
	「無関係」	3%	7%	5%
	「興味深い」	17%	29%	22%
	「最新で現状を反映している」	10%	27%	32%
	「インタラクティブ」	2%	29%	18%

考察ポイント 2:
フィッシングへの対応・報告とフィッシングを見抜く自信

2 つ目の考察ポイントとして、フィッシングを受けた場合にどのような対応を取っているかを見てみた。日本のオフィスワーカーの 5 人に 3 人（57%）が疑わしいメールには関与しない（リンクを開ける、返信するなど）、また約半数（47%）が疑わしい SMS（ショートメッセージ）に関与しない（リンクを開ける、返信するなど）と回答している。疑わしいメールや SMS メッセージをセキュリティ担当の IT チームに報告していかについては、5 人に 1 人（18%）しか報告していないん。ほとんどが疑わしいメールや SMS メッセージと判断しても、受信ボックスから削除するだけで、報告していないと考えられる。リンクを開けたり、返信するなどの結果は、3 地域ともほぼ同様となっているが、報告については日本は他の 2 地域に比べるとかなり劣っている。これは、多くの日本の中小企業や営業所・支社などの組織において、セキュリティ担当者が不在など、連絡先が明確になっていないためと考えられる。また、この結果はセキュリティ人材の不足に悩む日本の IT 部門の実態を反映していると思われる。また、フィッシングメール／SMS の判断については、自信がないと回答する日本のオフィスワーカーの割合はメールに関しては 84%、SMS に関しては 85%と他の 2 地域と比べると極めて高い結果となっている。これは、日本のオフィスワーカーのセキュリティトレーニング（フィッシングメールの模擬演習を含む）の受講率が他の 2 地域に比べて低いことに起因していると思われる。

日本のオフィスワーカーの 5 人に 3 人（57%）が疑わしいメールに的確に対応していると思っているが、セキュリティ担当の IT チームに報告していると答えた人は 5 人に 1 人（18%）に過ぎない。

	日本	オーストラリア	シンガポール
疑わしいメールには関与しない（リンクを開ける、返信するなど）	57%	56%	61%
疑わしい SMS（ショートメッセージ）に関与しない（リンクを開ける、返信するなど）	47%	54%	57%
疑わしいメールや SMS メッセージをセキュリティ担当の IT チームに報告している	18%	40%	35%
メールが本物で、どれが偽物か、詐欺なのかを完全に見分ける自信がない	84%	45%	54%
SMS メッセージが本物で、どれが偽物か、詐欺なのかを完全に見分ける自信がない	85%	48%	52%

考察ポイント 3:
サイバーセキュリティリスクの現状

3 つ目のポイントでは、従業員一人ひとりのサイバーセキュリティリスクを考察している。具体的には、BYOD（個人所有）デバイスと業務用のメールアドレスについて調査している。BYOD（個人所有）デバイスについては、日本企業の多くは、セキュリティポリシー（業務規程）で、BYOD（個人所有）デバイスの業務システムへの接続を厳しく制限していることがこの結果に反映していると思われる。しかし、セキュリティリスクへの危機感は欠如していることは明白です。リモートワークの常態化に伴うセキュリティポリシーの見直しは、すべての日本企業において喫緊の課題と考える。その一方で、オーストラリアおよびシンガポールの調査結果は、BYOD（個人所有）デバイスでの業務メール閲覧の許可が一般化しているものかと推測する。また、業務以外の個人用途に業務用のメールアドレスを使用することを許可している割合が日本の 3%に比べて、極めて高い（オーストラリア 13% シンガポール 6%）。従業員一人ひとりのレベルでのセキュリティリスクへの危機感については、3 地域とも欠如していると言わざるを得ない。これは、セキュリティ教育が単なる知識教育になっていて、セキュリティ意識（アウェアネス）トレーニングがまだ十分に浸透していないのではないかと推測する。KnowBe4 の 3 地域でのオフィス開設時期を見ると、オーストラリアが 2019 年 4 月、シンガポールが 2018 年 5 月、日本が 2019 年 11 月であることから、セキュリティ意識向上トレーニング市場の成長は米国と比べると、これからであると思われます。特に、日本においては、セキュリティ意識向上トレーニングは大手企業では浸透し始めたものの、まだ中堅・中小企業では緒についたばかりとKnowBe4 Japan は分析している。

従業員一人ひとりのレベルでのセキュリティリスクへの危機感については、3 地域とも欠如していると言わざるを得ない。セキュリティ意識トレーニングがまだ十分に浸透していないのではないかと推測する。

	日本	オーストラリア	シンガポール
業務以外の個人用途に業務用のメールアドレスを使用している	3%	13%	6%
業務以外の個人用途に業務用の電話（スマートフォン）を使用している	2%	16%	13%
個人的な用途に業務用のメールアドレスを使用することが自分自身のセキュリティリスクを発生させるとは考えていない	70%	67%	57%
個人的な用途に業務用のメールアドレスを使用することが会社または雇用主のセキュリティリスクを発生させるとは考えていない	66%	60%	57%

考察ポイント 4:
サイバーセキュリティ攻撃から組織を守る責任の所在

サイバー攻撃から組織を守るのは全員の責任であると考えている傾向は 2 地域とも強い。その一方で、従業員の責任であると考える割合は、日本は他の 2 地域に比べて低い。

4 つ目のポイントしては、サイバー攻撃から組織を守る責任はどこにあるのかというの認識を調査してみた。日本の IT 意思決定者の約半数（54%）は、サイバー攻撃から組織を守るのは全員の責任であると考えている（オフィスワーカーより 12%高い）。また、日本においては、サイバーセキュリティに関するトレーニングを受けている回答者は、受けていない回答者に比べて、サイバー攻撃から組織を守ることは全員の 責任であると考える傾向が強い（57% vs 28%）。この傾向は他の 2 地域でも同様である。その一方で、従業員の責任であると答える割合は、日本は他の 2 地域に比べて低い。個人のミスが会社のサイバー攻撃被害を引き起こすことを考えれば、この結果は問題視する必要がある。

	日本	オーストラリア	シンガポール
サイバーセキュリティ攻撃から組織を守る責任の所在 オフィスワーカーの調査結果			
全員の責任	42%	47%	63%
IT 部門の責任	14%	25%	17%
従業員の責任	9%	16%	12%
政府の責任	9%	14%	8%
サイバーセキュリティ攻撃から組織を守る責任の所在 IT 意思決定者の調査結果			
全員の責任	54%	49%	60%
IT 部門の責任	19%	25%	25%
従業員の責任	9%	15%	23%
政府の責任	9%	21%	14%

考察ポイント 5:
フィッシングと BEC（ビジネスメール詐欺）のリスク

5 つ目のポイントとしては、4 つ目のポイントを深堀りして、サイバーインシデントやデータ侵害が発生した場合に取るべき措置が認識されているかを調査してみた。日本の IT 意思決定者の 5 人に 1 人（19%）しか、自社でサイバーインシデントやデータ侵害が発生した場合に取るべき措置を理解している自信があると回答していない。これに対して、オーストラリアおよびシンガポールの IT 意思決定者の 37%が自信があると回答している。同様に、日本の IT 意思決定者は、他の 2 地域と比べて、従業員のフィッシング/BEC（ビジネスメール詐欺）リスクへの認識・理解度を低く見ている。また、報告についても、同様に、他の 2 地域と比べて、低い。これは、考察ポイント 5 の調査結果の「サイバーセキュリティ攻撃から組織を守る責任が IT 部門にある」と回答した IT 意思決定者の割合を見れば、明確にサイバーセキュリティ対策に責任を持つセキュリティ担当者が日本の IT 部門では不足していると思われる。

日本の IT 意思決定者の 5 人に 1 人（19%）しか、自社でサイバーインシデントやデータ侵害が発生した場合に取るべき措置を理解している自信があると回答していない。これは、他の 2 地域に比べて明らかに低い。

	日本	オーストラリア	シンガポール
IT 意思決定者のうちで、フィッシングを組織にとってのリスクと考え、懸念している割合	25%	37%	45%
IT 意思決定者のうちで、自社でサイバーインシデントやデータ侵害が発生した場合に取るべき措置を理解している自信があると回答した割合	19%	37%	37%
IT 意思決定者のうちで、組織の従業員がサイバー攻撃の被害を受けた場合のビジネスへの影響を理解していると考えていると回答した割合	28%	42%	47%
IT 意思決定者のうちで、従業員がフィッシングや BEC メールを識別できると確信していると回答した割合	20%	38%	47%
IT 意思決定者のうちで、従業員が疑わしいと思うメールを報告すると考えていると回答した割合	23%	38%	41%

考察ポイント 6:
IT チームの支援について

6 つ目のポイントとして、オフィスワーカー見て、サイバーセキュリティに対する支援をどう考えているかを考察してみた。37%の日本のオフィスワーカーが、支援を依頼する IT チームがいないと回答していることは大きな問題である。他の 2 地域と比べて、日本の結果は極めて劣っている。これは、日本における IT 人材の不足にその要因があると考えられる。また、IT 担当者がいても、極めて多忙なため、依頼しにくい状況あると思われる。特に、中小規模の組織においては、専任の IT 担当者を配置していないことも多い。また、サイバーセキュリティ対策の予算化については、日本の IT 意思決定者の 5 人に 2 人（40%）が投資/支出を計画していると回答しているが、他の 2 地域と比べると、この数値も極めて低い。IT 人材の不足に悩む日本の IT 部門は、DX（デジタルトランスフォーメーション）といった攻めの投資に手一杯で、セキュリティ対策などの守りの投資への注力への余裕がない。このことが、この調査結果に表れていると思われる。

サイバーセキュリティリスクに対する意識は低い。これは他の 2 地域でも同様である。この背景には、セキュリティ意識向上トレーニングが全社レベルで実施されたいないことに起因していると思われる。

	日本	オーストラリア	シンガポール
支援を依頼する IT チームがない	37%	9%	15%
2023 年にサイバーセキュリティ対策への投資/支出を計画している	40%	68%	72%

考察ポイント 7:
セキュリティカルチャーについて

セキュリティカルチャーについては、日本では、基本的な認知と理解から始める必要がある。

最後に、セキュリティカルチャーについて考察してみる。まず、セキュリティカルチャーの基本的な認知と理解は、日本と他の 2 地域とは大きな差がある。セキュリティカルチャーについては、KnowBe4 Japan が昨年の当初より訴求を始めているが、他社はこのテーマはほどんど触れていない。また、このテーマについては、日本のメディアはこれまで取り上げていない。今回の調査結果は、この現状を反映している。日本においては、セキュリティカルチャーの基本的な認知と理解を促進する必要がある。セキュリティという文化を組織全体に根付かせて、巧妙化するサイバー攻撃に立ち向かうことを訴求していかなければならない。

	日本	オーストラリア	シンガポール
セキュリティカルチャー　オフィスワーカーの調査結果			
「セキュリティカルチャー」という言葉を聞いたことがない	73%	43%	53%
「セキュリティカルチャー」という言葉を雇用主から聞いたことがある	14%	34%	30%
「セキュリティカルチャー」の意味と自分の役割を明確に理解している	8%	25%	23%

サイバーセキュリティの人的防御対策をいかに展開していくべきか

進化し続けるサイバー攻撃に立ち向かうためのサイバーセキュリティトレーニングは、「1 回セットしたら終わり」というプロジェクトではありません。サイバーセキュリティトレーニング（セキュリティ意識向上トレーニング）を実施するにあたって理解すべきことは、セキュリティ意識向上トレーニングが「人」を狙う進化し続けるセキュリティ攻撃に対して継続的に対応することが求められるという終わりのない取り組みであることです。定期的に注意を喚起しなければ、いったん実現した行動の変化も、元の状態に戻ってしまいます。行動変化を常態化して、行動変容につなげる必要があります。これこそが、KnowBe4 が提案するサイバーセキュリティの人的防御対策（ヒューマンファイアウォール）の根幹です。

セキュリティ意識向上トレーニングを通して、セキュリティ意識向上から行動変容、そしてセキュリティカルチャーの醸成を達成しなければ、一過性の成果に終わってしまいます。サイバー攻撃の大半は、「人」の心理的な隙や、「人」が生み出す人的なミス（従業員の行動）から始まっています。サイバー攻撃者が狙っているのは、1 回のヒューマンエラーです。1 回の従業員のミスが自社の経営に影響するような惨事を引き起こします。進化し続けるサイバー攻撃に立ち向かうためには、全社一丸となって、継続的なセキュリティ意識向上トレーニングを実施することで、人的防御層（ヒューマンデフェンス・レイヤー）を構築することです。

セキュリティ意識向上は、サイバー攻撃から組織を守り、より安全な組織を築くと同時に、セキュリティカルチャーの醸成へつなげることでもあります。

サイバーセキュリティの人的防御対策を展開するにあたって、まず考えていただきたい。

1. サイバー攻撃対策をテクノロジーの問題と考えていませんか
2. サイバー攻撃者は最も脆弱なリンクから侵入してきているが、この根源はたった 1 回の「人」によるミスであることが十分に認識していますか
3. サイバーセキュリティは、従業員一人ひとりのコンプライアンスとして、取締役会で監査されるべき問題として捉えるべきことあることを理解していますか

この実態調査のデータをご覧いただき、上記 3 点を自問自答していただきたい。

まとめ

これまで、KnowBe4 では、サイバーセキュリティの人的防御対策において日本が立ち遅れていることを指摘してきました。KnowBe4 は、その現状を調査するために、日本企業・団体のオフィスワーカーと IT 意思決定者を対象に日本初の実態調査を実施しました。本稿は、この調査結果を解析して、セキュリティ意識向上トレーニングプログラムにいかに取り組み、サイバーセキュリティの人的防御対策をいかに展開していくべきかを提案するためのものです。この調査結果と自社の状況と対比して、まずは自社の現状を把握していただきたい。サイバーセキュリティの人的防御対策をいかに展開していくべきかをご検討いただけますと幸いです。

その他の関連情報

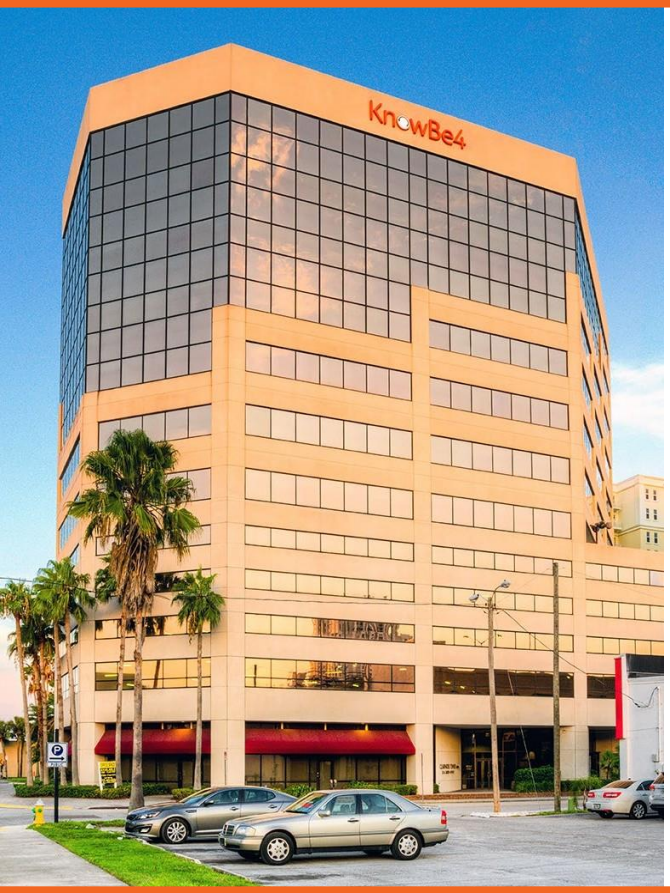
フィッシングセキュリティテスト
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。

セキュリティプログラムビルダー
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

Phish Alert ボタン
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

無償 Email Exposure Check ツール
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

無償なりすましドメインテスト
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。



＜KnowBe4 について＞

KnowBe4 は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4 は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4 プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

2022 年 12 月現在、5 万 6 千社を超える企業や団体が KnowBe4 を採用して、防御の最終ラインとして「人」による防御壁を構築しています。

詳しくは、www.KnowBe4.jp をアクセスしてください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社　〒100-6510 東京都千代田区丸の内 1－5－1
新丸の内ビルディング 10F　EGG 内
Tel: 03-4586-4540| www.KnowBe4.jp | Email: Info@knowbe4.jp

22/12/2022

サイバーセキュリティ実態調査 (日本)

YouGov®

調査企画担当:

B.
BENCH PR

Living Consumer Intelligence | business.yougov.com

方法論について

- 本調査は、2022年12月9日～14日の間に日本企業および団体を対象に無作為抽出でオンラインにて実施されました。本調査アンケートは、日本においては株式会社日本リサーチセンター（NRC）と共同で、英国市場調査会社YouGov社によって日本語によって収集され、YouGov社によって統計分析されました。また、同様な調査が、オーストラリア/ニュージーランドとシンガポールで同時に実施されました。
- 調査対象者およびサンプル数：
  - 日本企業・団体のオフィスワーカー（ITおよびサイバーセキュリティに関する意思決定権を持たないオフィス勤務者＊ 1,038名（業種不問） ＊在宅勤務者を含む
  - 日本企業・団体のIT意思決定者（ITおよびサイバーセキュリティに関する意思決定権を持つ上級管理職＊） 225名（業種不問） ＊IT担当マネージャーおよびセキュリティ担当者を含む
- アンケート調査票はYouGovが英文で作成し、NRCが日本語に翻訳しています。
- インタビュー終了後、オフィスワーカーのデータは、日本の最新の人口推計を反映し、年齢、性別、地域による重み付けが行われました。
- 本レポートでは、日本企業および団体のオフィスワーカー（ITおよびサイバーセキュリティに関する意思決定権を持たないオフィス勤務者）の方とIT意思決定者（ITおよびサイバーセキュリティに関する意思決定権を持つ上級管理職）の両方の調査結果を対比して統計分析しています。本調査結果は、YouGovが英文でまとめ、KnowBe4 Japanが日本語に翻訳して、訳注を付加しています。

YouGov®

調査結果の注目ポイント

YouGov®

調査結果の注目

業務環境でのメール/SMSの利用について(OWQ1)

- 日本のオフィスワーカーの10人に1人（9%）が、複数のアカウントに同じパスワードを使用していることを認めている。また、業務以外の個人用途に業務用のメールアドレスを使用することを認めるのは3%、業務用の電話（スマートフォン）を使用することを認めるのは2%にとどまっている。この反面、10人に7人（70%）の日本のオフィスワーカーは、個人的な用途に業務用のメールアドレスを使用することが自分自身のセキュリティリスクを発生させるとは考えていない。また、3分の2（66%）は個人的な用途に業務用のメールアドレスを使用することが会社または雇用主のセキュリティリスクを発生させるとは考えていない。日本企業の多くは、セキュリティポリシー（業務規程）で、BYOD（個人所有）デバイスの業務システムへの接続を厳しく制限していることがこの結果に反映していると思われる。しかし、セキュリティリスクへの危機感は欠如していることは明白である。リモートワークの常態化に伴うセキュリティポリシーの見直しは、すべての日本企業において喫緊の課題と考える。
- さらに、5人に3人（57%）が疑わしいメールには関与しない（リンクを開ける、返信するなど）、また約半数（47%）が疑わしいSMS（ショートメッセージ）に関与しない（リンクを開ける、返信するなど）と回答しているが、疑わしいメールやSMSメッセージをセキュリティ担当のITチームに報告していると答えた人は5人に1人（18%）に過ぎません。ほとんどが疑わしいメールやSMSメッセージを特定しても、受信ボックスから削除するだけで、報告していないと考えられる。
- 10人に8人以上が、どのメールが本物で、どれが偽物か、詐欺なのかを完全に見分ける自信がない（84%）、どのSMSメッセージが本物で、どれが偽物か、詐欺なのかを完全に見分ける自信がない（85%）、と答えている。
- また、リモートワークに伴い、不審なメールやSMSを見分ける自信が改善されたと答えた人はわずか5%にしか達していない。これは、リモートワーク環境はサイバー攻撃のリスクが大きく増幅させることを考えると、極めて危険な実態である。
- 疑わしいメールやSMSメッセージの報告については、セキュリティ担当のITチームに報告していると回答する傾向は、50-65歳（25%）は、35-49歳（16%）および65歳以上（13%）となっている。50-65歳代が高い。従業員一人に一台のPCや携帯電話（スマートフォン）が会社支給される前の時代を経験している非デジタルネイティブ世代とスマートフォンや個人PCが当たり前のデジタルネイティブ世代との差が表れている。

調査結果の注目ポイント (*続き...*)

フィッシングとBEC（ビジネスメール詐欺）のリスクについて (ITQ2)

- 日本のIT意思決定者の6人に1人(17%)は、従業員が個人所有の電話（スマートフォン）を業務用に使っていると考えており、10人に1人(8%)は会社支給の電話（スマートフォン）を個人的な用途に使っている(オフィスワーカーの調査結果より6%高い)と考えている。また、9%の従業員が業務用のメールアドレスを個人的用途に使っている（オフィスワーカーの調査結果より6%高い）と考えている。
- 驚いたことに、日本のIT意思決定者のうち、フィッシングを組織にとってのリスクと考え、懸念していると答えたのは4分の1（25%）に過ぎない。また、BECについては、リスクと考え、懸念していると答えたのはさらに少ない（20%）。これは、驚くべき結果です。
- 次に、懸念すべき調査結果としては、IT意思決定者の5人に1人（19%）しか自社でサイバーインシデントやデータ侵害が発生した場合に取るべき措置を理解している自信があると回答していないことである。
- さらに懸念すべきこととして、日本のIT意思決定者のうちで、組織の従業員がサイバー攻撃の被害を受けた場合のビジネスへの影響を理解していると考えていると回答した割合は平均で10人に3人（28%）、従業員がフィッシングやBECメールを識別できると確信していると回答した割合は平均で5人に1人（20%）、従業員が疑わしいと思うメールを報告すると考えていると回答した割合は平均で4分の1（23%）にしか達していない。
- この数値をさらに分析して、2023年のサイバーセキュリティへの投資/支出計画の担当者とそれ以外のIT意思決定者に比較してみると、フィッシングについては14%に対して36%、BECについては6%に対して36%、また、自組織でサイバーインシデントやデータ侵害が起こった場合に取るべき措置を理解している自信があるかについて11%に対して34%と、数値は大幅に改善されているが、依然として3分の1には達していない。これは、多くの日本企業はサイバー攻撃をテクノロジーの問題と捉えていて、サイバーセキュリティ対策を外部のシステムインテグレーターやIT子会社へ丸投げしている結果ではないかと考えられる。サイバー攻撃が引き起こす被害額や企業の信頼損失を考えれば、サイバーセキュリティは単なるテクノロジーの問題を超えて、企業の経営陣のすべてが監査すべき問題となっているのではないだろうか。

調査結果の注目ポイント (*続き...*)

職場でサイバーセキュリティのトレーニングについて (OWQ4、OWQ8、OWQ9)

- 日本のオフィスワーカーの半数（51%）が、サイバーセキュリティに関するトレーニングを職場で受けたことがないと回答している。

サイバーセキュリティトレーニングをこれまで受けたことがある回答者 (n=517)の回答内容をさらに分析してみると

- 半数（48%）は、会社で頻繁に的確なトレーニングを受けていると回答している。また、3分の1（32%）は、フィッシングメールの模擬演習を含むトレーニングを受けていると回答している。
- 受講頻度に関して、詳しく見てみると、13%は年に2回、26%は年に1回受講しているが、なんと6%は一度だけトレーニングを受けたが、それっきりだと回答している。
- 興味深いことに、年齢の高い従業員は、年齢の若い従業員よりも、サイバーセキュリティに関するトレーニングを職場で受けたことがあると答える傾向が強い（50～64歳が52%であるのに対して、35～49歳は44%）。

- 日本におけるセキュリティトレーニングの実態を見てみると、驚くことに、半数以上がセキュリティトレーニングを受けていない。日本企業を標的とするサイバー攻撃が急増していることを考えれば、これは憂うべき事態である。

調査結果の注目ポイント (*続き…*)

サイバーセキュリティに関するトレーニングを現在の会社または組織で受けたことがある回答者 (n=483) からトレーニングの内容を聞いてみると

- 4分の1(26%)は対面でのトレーニングを受けたことがあり、4分の3(75%)はオンラインでeラーニングトレーニングを受けたことがある。
- 興味深いことに、年齢の高い従業員は、年齢の若い従業員よりも、サイバーセキュリティに関するトレーニングをオンラインで受けたことがあると答える割合が多い（50～55歳が85%であるのに対して、35～49歳は74%）。これは、年齢の若い従業員は入社時の集合トレーニングの一環でセキュリティ教育を受けていることが多いためであると考える。

対面でのトレーニング (n=101) の詳細

- 大多数（85%）が講義やプレゼンテーション形式のグループ形式の集合トレーニングを受け、57%が短時間のセッション（2時間以内）、3人に1人（33%）が1日または半日のセッションだったと答えている。
- 一方、4分の1（24%）が対面での個別トレーニングで、10%が1日または半日のセッション、14%が短いセッション（2時間以下）と回答している。

オンラインでのトレーニング (n=387) の詳細

- 5人に4人（78%）が30分未満のeラーニングのショートセッションを受講している。また、4分の1（25%）が30分以上のeラーニングセッションも受講している。

- 今回の調査結果を分析してみると、eラーニングによるセキュリティ教育が増加している。また、30分未満のショートセッションが増えている。これは、入社時の集合トレーニングに加えて、リモートワークの増加に伴い、eラーニングによるセキュリティ教育が根付き始めていることの表れと思われる。

調査結果の注目ポイント (*続き…*)

サイバーセキュリティに関するトレーニングを現在の会社または組織で受けたことがある回答者 (n=483)に対してその効果を聞いてみると、

- セキュリティトレーニングについての評価は、「役に立った」（36%）、「自分の職務と関係があった」（24%）、「価値があった」（21%）と回答した回答者が一般的に多かった。
- 次いで、興味深い（17%）、最新で現状を反映している（10%）と回答している。
- しかし、8%が「退屈」、6%が「時間の無駄」、4%が「複雑すぎる」、3%が「時代遅れ」、3%が「無関係」と回答している。
- さらに、2%が受講したトレーニングを「インタラクティブ」であったと回答している。

- また、対面でのトレーニングを受けた回答者は、オンラインでeラーニングを受けた回答者よりも、トレーニングが自分の役割に関連していると考える傾向が高い（38% vs 20%）。
- さらに、55歳以上の回答者は、35～49歳の回答者よりも、受講したトレーニングが役に立った（51% vs 28%）、面白かった（25% vs 13%）と評価する傾向が高い。

- 総合的に見ると、セキュリティトレーニングの効果はそれなりに評価されているが、潜在的なトレーニングコンテンツへの不満があるように推測される。これは、インタラクティブなトレーニングはわずか2%しか提供されていないという数値にも表れている。

調査結果の注目ポイント (*続き...*)

ITチームの支援について (OWQ7)

- 5人に2人（37%）のオフィスワーカーが、支援を依頼するITチームがいないと回答している。

相談できるIT部門がある回答者 (n=654) の回答内容をさらに分析してみると

技術関連の質問について

- 5人に2人(41%)が、IT部門に技術的な質問をするのは問題ない、IT部門はいつでも喜んで助けてくれると答えている。
- しかし、6人に1人(17%)は、IT部門に支援を求めることに抵抗があると答えている。10人に1人(12%)は、面倒なので、技術的な質問があってもITチームにほとんど頼まない、3%はその後どうなるかが恐いためITチームには質問しない、3%はITチームに質問するのは恥ずかしい、または自分が無能に感じられるので質問しないと回答している。

セキュリティ関連の質問について

- セキュリティ関連の質問に関しては、技術関連の質問とほぼ同様の割合（39%）が「IT部門はいつでも喜んで助けてくれるから、セキュリティ関連の質問をするのは問題ないと回答している。
- しかし、ほぼ5人に1人(18%)は、IT部門に支援を求めることに抵抗があると答えている。14%は、面倒なので、技術的な質問があってもITチームにほとんど頼まない、2%はその後どうなるかが恐いためITチームには質問しない、4%はITチームに質問するのは恥ずかしい、または自分が無能に感じられるので質問しないと回答している。

- 総論として、37%の日本のオフィスワーカーが、支援を依頼するITチームがいないと回答していることは大きな問題である。これは、日本におけるIT人材の不足にその要因があると考えられる。また、IT担当者がいても、極めて多忙なため、依頼しにくい状況あると思われる。特に、中小規模の組織においては、専任のIT担当者を配置していないことも多い。

調査結果の注目ポイント (*続き...*)

2023年に投資／支出を計画しているサイバーセキュリティ対策について (ITQ1)

- 日本のIT意思決定者の5人に2人（40%）が、2023年にサイバーセキュリティ対策への投資/支出を計画していると回答している。

2023年にサイバーセキュリティへの投資・支出を予定している回答者 (n=91) から何に投資するかを尋ねてみると

- 新しいサイバーセキュリティソフトウェアソリューションへの投資/支出が最も多く（58%）、次いでインフラへのさらなる投資（41%）、サイバーセキュリティ保険（34%）となった。
- その他の投資分野としては、継続的かつ適切なサイバーセキュリティ意識向上トレーニングプログラム（32%）、サイバーセキュリティに関する従業員のポリシー変更（30%）、エンドユーザー向けのフィッシングやソーシャルエンジニアリングのシミュレーション・模擬演習（23%）などが挙げられている。

- 日本のIT意思決定者の5人に2人（40%）が、2023年にサイバーセキュリティ対策への投資/支出を計画していることは、まだ半数に満たないが、極めて明るい実態である。また、セキュリティ意識向上トレーニングプログラムやフィッシング/ソーシャルエンジニアリングのシミュレーション・模擬演習が予算化されていることは、日本においてセキュリティ意識の必要性が認知されてきていることを示している。

調査結果の注目ポイント (*続き...*)

セキュリティカルチャーについて (OWQ6、ITQ6、ITQ7)

セキュリティカルチャーについてオフィスワーカーの調査結果

- 約4分の3（73%）のオフィスワーカーが「セキュリティカルチャー」という言葉を聞いたことがない（IT意思決定者の46%も同様に回答している）。
- 雇用主から「セキュリティカルチャー」について聞いたことがあると答えたオフィスワーカーはわずか14%で、10人に1人（8%）しか「その意味と自分の役割を明確に理解している」と回答していない。また、6%のオフィスワーカーはその意味を全く理解していない。
- 一方で、オフィスワーカーの13%は、雇用主から「セキュリティカルチャー」について聞いたことがないと答え、6%はこの言葉を会社以外から聞いて、その意味を理解していると答え、7%はこの言葉を他で聞いたことがあるがその意味は分からないと答えている。
- 18～34歳では、4分の1（24%）が「この言葉は聞いたことがあるが、意味はわからない」と回答しており、18～34歳以上の年長者よりも高い割合となっている。
- さらに、サイバーセキュリティのトレーニングを受けたことがある回答者は、そうでない回答者に比べて、「セキュリティカルチャー」という言葉を聞いたことがあり、その意味も知っている割合が高い（19% vs 9%）。

セキュリティカルチャーについてIT意思決定者の調査結果

- IT意思決定者についての調査結果を見ると、IT意思決定者の半数以上（54%）が「セキュリティカルチャー」という言葉を聞いたことがあると答えているが、その意味を知っている割合は5人に2人以下（36%）にとどまった。
- 3%は、「セキュリティカルチャー」が何であるかは知っているが、自分の組織にそれが必要だとは思わないと回答している。
- 10人に1人（7%）が、「セキュリティカルチャー」が何であるか知っており、自分の組織にはそのような場所が必要だと考えているが、それをどのように達成すればよいかは分からないと回答している。一方、7%は「自社にはセキュリティカルチャーはない」と回答している。
- 6人に1人（17%）が「セキュリティカルチャー」とは何かを知っており、自分の組織には優れたセキュリティカルチャーがあると考え、3%が「セキュリティカルチャー」とは何かを知っているが、それは他の人の責任だと考えていると回答している。
- また、2023年サイバーセキュリティへの投資計画の担当者は、それ以外のIT意思決定者に比べて「セキュリティカルチャー」の意味を知っている割合が高い（56% vs 20%）。

調査結果の注目ポイント (*続き…*)

セキュリティカルチャーの意味を知っている回答者 (n=81) の回答内容をさらに分析してみると

- 「セキュリティカルチャー」とは、セキュリティ問題に対する認識と理解を持つこと（69%）、セキュリティは組織全体で共有する責任であるという認識（62%）、セキュリティが組織文化に組み込まれていること（58%）を意味すると最もよく回答している。
- 2人に1人（52%）は、セキュリティポリシーの遵守を意味すると考えている。
- さらに、10人に3人（31%）は、セキュリティカルチャーをセキュリティに関する決定に影響力を持つ回答者の正式なグループの設立に関することと考えている。

- セキュリティカルチャーについての調査結果を考察してみると、日本の多くの企業・組織はセキュリティ意識の必要性についての認知はかなり進んだものの、セキュリティカルチャーの認識はまだ始まったばかりと考えられる。人的防御対策の進化の道筋として、セキュリティ意識（アウェアネス）は出発点であるが、日本はこの初期フェーズが始まった段階と考えられる。セキュリティ意識から行動変容へと進化させ、セキュリティカルチャーとして組織全体に根付かせていくことが必要になっていくことの理解が必要である。

調査結果の注目ポイント (*続き...*)

フィッシングメールの見極めについて (OWQ2、OWQ3、ITQ5)

オフィスワーカーの調査結果

KnowBe4のフィッシングテンプレート1

PayPay

admin@kb4-demo.com

お客様のPayPayアカウントは異なる端末からのアクセスを確認しました。
アカウントは、一時利用停止されました。
PayPayアカウントの資金安全を確保するためにご本人でセキュリテイ強化、再開手続きの設定を行ってください。

■下記のURLをクリックしてログインを設定してください。
（設定してからPayPayアカウントの制限を解除します）
https://paypay.net.jp

■本メールは、PayPayアカウントにEメールアドレスをご登録いただいているお客様にご案内しております。
（December 09, 2022現在）
■本メールは、セキュリティ強化のため、電子署名を付けて送信しています。（PCメールのみ）
電子署名について詳しくはこちらから。↓
https://paypay.net.jp/e-sign

■本メールの送信アドレスは送信専用となっております。
返信メールでのお問い合わせはお受け出来かねますので予めご了承お願い申し上げます。

PayPayお問い合わせ窓口（ユーザ窓口）
PayPay携帯電話紛失盗難専用窓口
電話番号：0120-354-4567
営業時間：24時間受付/土日祝祭日を含む365日

PayPay株式会社
https://paypay.net.jp

KnowBe4のフィッシングテンプレート2

三井住友銀行

カード会員の皆様へ、

マネーロンダリングやテロ資金調達を防止する政府のガイドラインを遵守するために、金融機関には顧客の最新の情報を維持することが求められています。そのため、お客様の皆様にはプロファイル情報の更新をお願い申し上げます。

更新いただかない場合には、お客様のアカウントに関する新たなお取引をお断りする場合があります。速やかに更新いただくようにお願いします。

この操作は1回だけで完了します

最初に、このメッセージに添付された**記入用のHTML Webフォーム**が送信されます。添付のフォームを確認して、ダウンロードして開いて操作を続行します。

- このフォームはお客様の情報があらかじめ***記入されています。***
- アカウントのセキュリティを確保するために、いくつかのステップを完了する必要があります。
- 最後にフォームに必要事項を入力し、確認を終了します。

迅速な対応をお願いします。

敬具
三井住友銀行カスタマーサービス

実際のフィッシングメール

Amazon株式会社から緊急のご連絡メール番号:03716128

amazon

co.jp

以前に3通のメールを送信しましたが、確認情報を取得できませんでした。残念ながら、あなたのアカウントは24時間後に自動的に削除されます。Amazonアカウントを引き続き使用する必要がある場合は、24時間以内に個人情報を確認してください。Amazonへのサポートに感謝します。

確認するアカウント

※24時間以内にこのメッセージに応答しない場合、アカウントのステータスは1週間後に対象となり、完全に削除されるようにスケジュールされます。

Amazon.co.jpカスタマーサービス

- 日本のオフィスワーカーの10人に7人（69%）がKnowBe4のフィッシングテンプレート1を詐欺メールと正しく認識したが、約13%が正規のメールと誤認識し、19%が分からないと回答している。
- また、10人に7人（80%）がKnowBe4のフィッシングテンプレート2を詐欺メールと正しく認識したが、6%が正規のメールと誤認識し、16%が分からないと回答している。
- 実際のフィッシングメールを正規のものと誤認識したのは3%で、5人に4人（81%）が詐欺メールと正しく認識し、15%が分からないと回答した。

調査結果の注目ポイント (*続き...*)

フィッシングメールの見極めについて (OWQ2、OWQ3、ITQ5)

IT意思決定者の調査結果

KnowBe4のフィッシングテンプレート1


PayPay

admin@kb4-demo.com

お客様のPayPayアカウントは異なる端末からのアクセスを確認しました。
アカウントは、一時利用停止されました。
PayPayアカウントの資金安全を確保するためにご本人でセキュリテイ強化、再開手続きの設定を行ってください。

■下記のURLをクリックしてログインを設定してください。
（設定してからPayPayアカウントの制限を解除します）
https://paypay.net.jp

■本メールは、PayPayアカウントにEメールアドレスをご登録いただいているお客様にご案内しております。
（December 09, 2022現在）
■本メールは、セキュリティ強化のため、電子署名を付けて送信しています。（PCメールのみ）
電子署名について詳しくはこちらから。↓
https://paypay.net.jp/e-sign

■本メールの送信アドレスは送信専用となっております。
返信メールでのお問い合わせはお受け出来かねますので予めご了承お願い申し上げます。

PayPayお問い合わせ窓口（ユーザ窓口）
PayPay携帯電話紛失盗難専用窓口
電話番号：0120-354-4567
営業時間：24時間受付/土日祝祭日を含む365日

PayPay株式会社
https://paypay.net.jp

KnowBe4のフィッシングテンプレート2


三井住友銀行

カード会員の皆様へ、

マネーロンダリングやテロ資金調達を防止する政府のガイドラインを遵守するために、金融機関には顧客の最新の情報を維持することが求められています。そのため、お客様の皆様にはプロファイル情報の更新をお願い申し上げます。

更新いただかない場合には、お客様のアカウントに関する新たなお取引をお断りする場合があります。速やかに更新いただくようにお願いします。

この操作は1回だけで完了します

最初に、このメッセージに添付された**記入用のHTML Webフォーム**が送信されます。添付のフォームを確認して、ダウンロードして開いて操作を続行します。

- このフォームはお客様の情報があらかじめ***記入されています***。
- アカウントのセキュリティを確保するために、いくつかのステップを完了する必要があります。
- 最後にフォームに必要事項を入力し、確認を終了します。

迅速な対応をお願いします。

敬具
三井住友銀行カスタマーサービス

- 日本のIT意思決定者の10人に8人（80%）がKnowBe4のフィッシングテンプレート1を詐欺メールと正しく認識したが、約8%が正規のメールと誤認識し、11%が分からないと回答している。
- また、84%がKnowBe4のフィッシングテンプレート2を詐欺メールと正しく認識したが、6%が正規のメールと誤認識し、11%が分からないと回答している。

調査結果の注目ポイント (*続き...*)

サイバーセキュリティ攻撃から組織を守る責任の所在について (OWQ5、ITQ3)

オフィスワーカーの調査結果

- 日本のオフィスワーカーの5人に2人（42%）は、サイバー攻撃から組織を守るのは全員の責任であると考えている。その一方で、
- 14%はIT部門の責任だと考えている。
- 9%は従業員の責任だと考えている。
- 9%は政府の責任だと考えている。
- 10人に1人（10%）は、サイバー攻撃から組織を守るべきテクノロジーが提供されていると回答している。
- 年齢の高いオフィスワーカーは、若いオフィスワーカーよりも、サイバー攻撃から組織を守るのは全員の責任であると考える傾向がある（55歳以上51%、18～34歳35%、35～49歳39%）。
- サイバーセキュリティに関するトレーニングを受けている回答者は、受けていない回答者に比べて、サイバー攻撃から組織を守ることは全員の責任であると考える傾向が強い（57% vs 28%）。

IT意思決定者の調査結果

- 日本のIT意思決定者の約半数（54%）は、サイバー攻撃から組織を守るのは全員の責任であると考えている（オフィスワーカーより12%高い）。
- その一方で、19%はIT部門の責任だと考えている（オフィスワーカーより5%高い）。
- 9%は政府の責任だと考えている（オフィスワーカーと同程度）。
- 9%は従業員の責任だと考えている（オフィスワーカーと同程度）。
- そして、13%がサイバー攻撃から組織を守るべきテクノロジーを提供していると回答している（オフィスワーカーより3%高い）。
- また、2023年のサイバーセキュリティへの投資/支出計画の担当者とそれ以外のIT意思決定者に比較してみると、IT部門の責任（27% vs 13%）、従業員の責任（16% vs 4%）であると考えている。
- 一方、2023年にサイバーセキュリティへの投資を予定していない回答者は、予定している回答者よりも、サイバー攻撃から組織を守る責任は誰にもないと考えている回答者が多い（20% vs 3%）

調査結果の注目ポイント (*続き...*)

サイバーセキュリティ対策における政府の責任について (ITQ4)

- 日本のIT意思決定者の6人に1人（16%）が、サイバーインシデントやデータ侵害の政府報告に関する自分の組織の責任を理解していると確信していると答え、10人に7人（71%）が、日本企業をサイバー攻撃から守るために政府は以下のようなことをもっと行うべきだと考えている。
  - サイバーリスクとオンラインでの安全な生活の仕方について、すべての国民にもっと教育と認識を与えること (43%)
  - 日本企業へのサイバーリスクに関するトレーニングをもっと提供すること (40%)
  - 日本企業へのサイバー防御のための資金提供を強化すること (37%)
- さらに、2023年にサイバーセキュリティへの投資/支出を予定している担当者の87%が、日本企業をサイバー攻撃から守るために政府がもっと努力するべきだと感じており、その中には、日本企業に対するサイバーリスクに関するトレーニングをもっと提供すること(56%)、すべての国民に対してサイバーリスクおよびネット上での安全についてもっと教育と意識を与えること(52%)、日本企業に対するサイバー防御のための資金提供を強化すること (51%)が含まれている。