Advancing with you
MS&AD
INSURANCE GROUP

個人向けIoT機器に関するサイバーセキュリティ対策の意識調査報告書

MS&AD MS&ADインターリスク総研株式会社

近年、IoT機器を狙ったサイバー攻撃が増加傾向にあり、MS&ADインターリスク総研では、消費者1,000名を対象として「個人用IoT機器に関するサイバーセキュリティ対策に関する意識調査」を実施した。

調査の結果、IoT機器に関するサイバーリスクを具体的にイメージできる消費者は少ないものの、消費者は、IoT機器や関連サービスを提供する企業（以下、IoT機器関連企業という）が主体となったサイバーリスク対策の実施を求めていることが明らかになった。

また、一定数の消費者からは、サイバーセキュリティ対策にかかる費用に対して「自身で負担してもいい」との回答が得られたが、そのうちの大多数が許容できる負担額は少額にとどまった。

企業は、自らが提供するIoT機器や関連サービスの特性やリスクを見極め、限られた費用の中でもサイバーリスク対策を講じることが求められる。

今回の意識調査結果に基づき、３つの提言を行った。IoT機器関連企業にとって、本調査がサイバーリスク対策取り組みの一助となれば幸いである。

今回の意識調査で明らかとなった実態と、それに基づくIoT機器関連企業への提言は以下のとおり。

① 消費者に身近な存在となったIoT機器の正確なリスク把握と対策の実施

今回の意識調査では、「家庭用ルーター」、「テレビ・録画機」を使用したことがあるとの回答が特に多かった。消費者にとってIoT機器が必要不可欠な製品になってきている一方で、機器に対するサイバーセキュリティ対策が不十分な可能性があり、IoT機器関連企業は、自社が提供するIoT機器のリスクを正確に把握し、早期に対策を講じることが必要である。

② IoT機器を提供する企業こそが、サイバーセキュリティ対策の実施主体

今回の意識調査では、サイバーセキュリティ対策は「企業が診断を行うべき」、「企業が対応方法を提供すべき」との回答が多く、消費者が「自らの責任で機器を選定する」の回答はわずかにとどまっている。各IoT機器製品の仕組みを十分に把握しているわけではない消費者がセキュリティ対策を講じるのは困難であり、IoT機器関連企業や業界が対策を講じることや、対策オプションを消費者に提示することが求められる。

③ 重要なことは「費用と効果のバランスがとれた対策」

今回の意識調査では、IoT機器やサービスの販売価格とは別に、サイバーセキュリティにかかる対策費用を負担してもよいと回答した消費者が一定数存在した。

ただしその許容できる負担割合は“サービス金額の３％程度“と少ない。
IoT機器関連企業は自らが提供するIoT機器の特性やリスクを見極めつつ、費用と効果のバランスを考慮した対策を講じることが求められる。

効果的な対策を講じるためには、IoT機器に内在するリスクを正しく把握することが肝要であり、その方法のひとつとして外部のIoT機器セキュリティ診断サービスを活用することが挙げられる。IoT機器のリスク評価を行い、優先度の高い課題を特定し、開発にフィードバックして早期に対策することにより、より豊かで快適な生活を消費者に提供することができる。

１．調査概要

Advancing with you
MS&AD
INSURANCE GROUP

調査方法概要

調査方法	インターネットによる調査
対象者	①年代別：20代から10歳刻みで60代まで ②性　別　：男女比50%ずつ ③地域別：大都市圏とそれ以外 ※年代別・性別は均等割となるように設定
有効回答	1,000名（目標回答数に到達するまで調査を実施）
調査期間	2021年5月28日～2021年6月1日

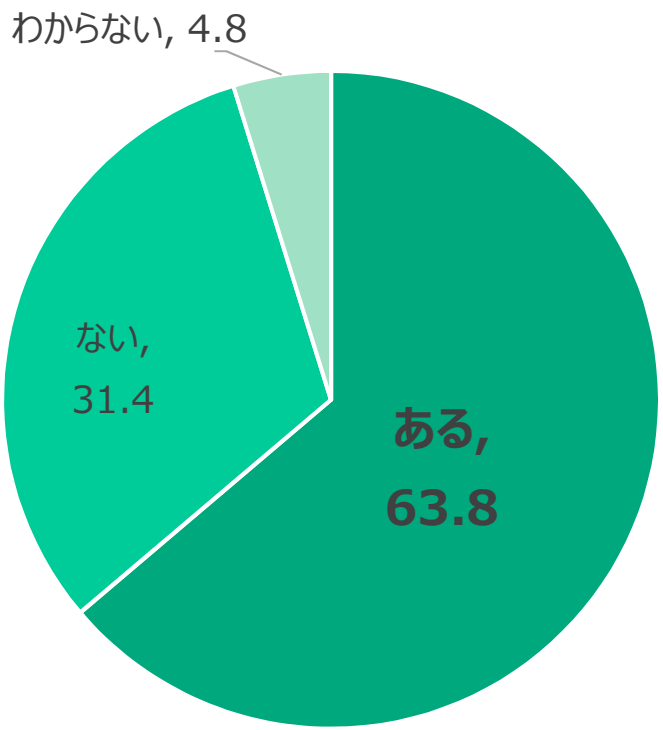
２．IoT機器の利用状況、リスクの認知度

（１）IoT機器の利用状況

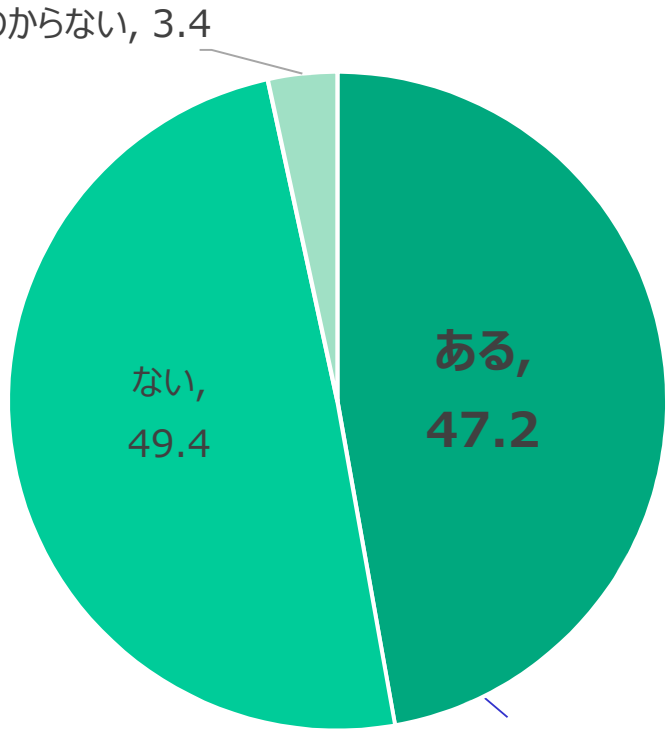
質問

「普段の生活又は職場環境において、IoT 機器を利用したことはありますか」

「家庭用ルーター」と**「テレビ・録画機」**は、実際に使ったことがあるとの回答が特に多かった。あらゆるものが無線インターネットでつながるIoT機器が日常生活に浸透しており、消費者にとって身近な存在となっていることがうかがえる。

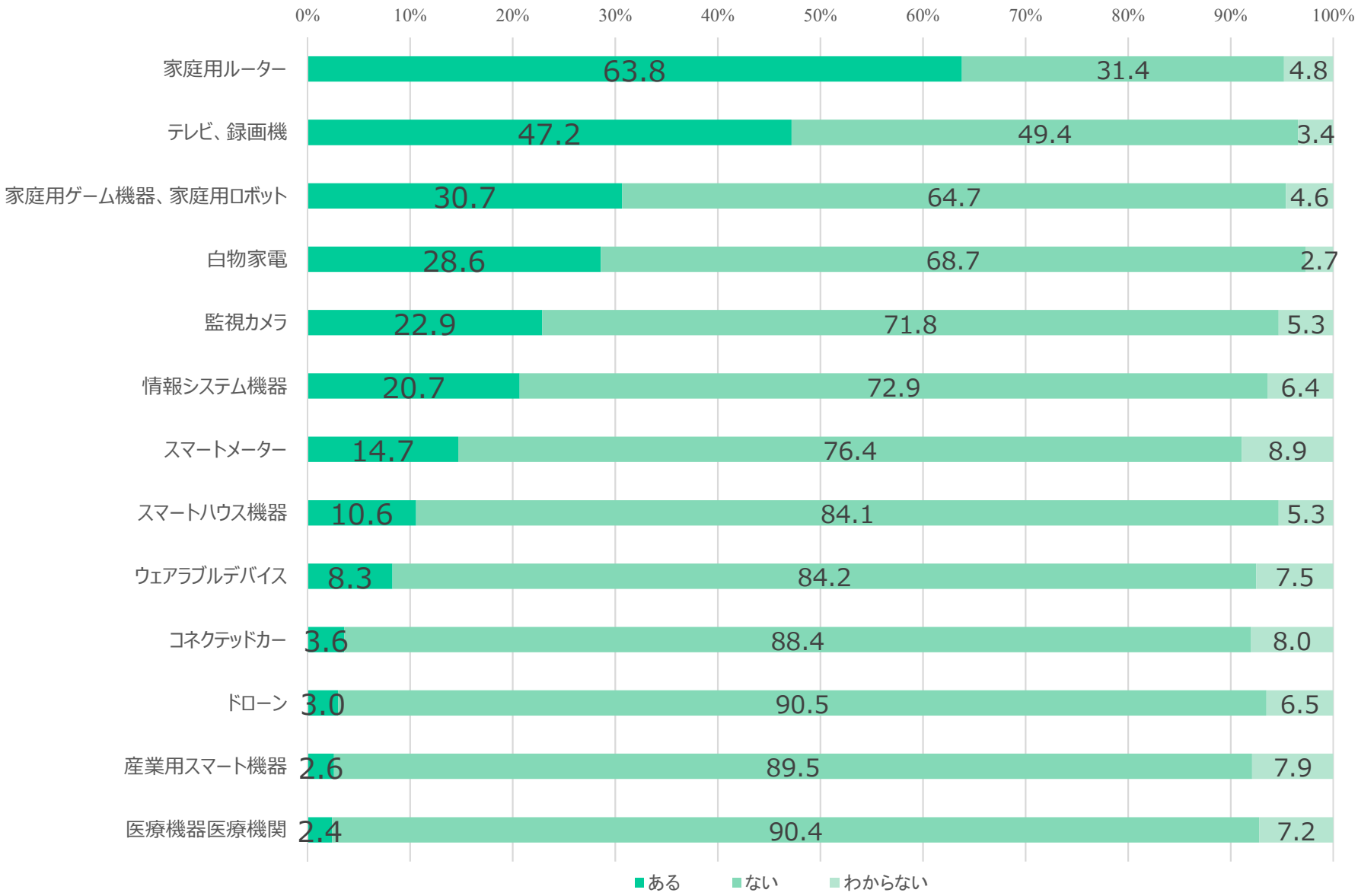


家庭用ルーター



テレビ・録画機

参考（IoT機器別の使用割合）

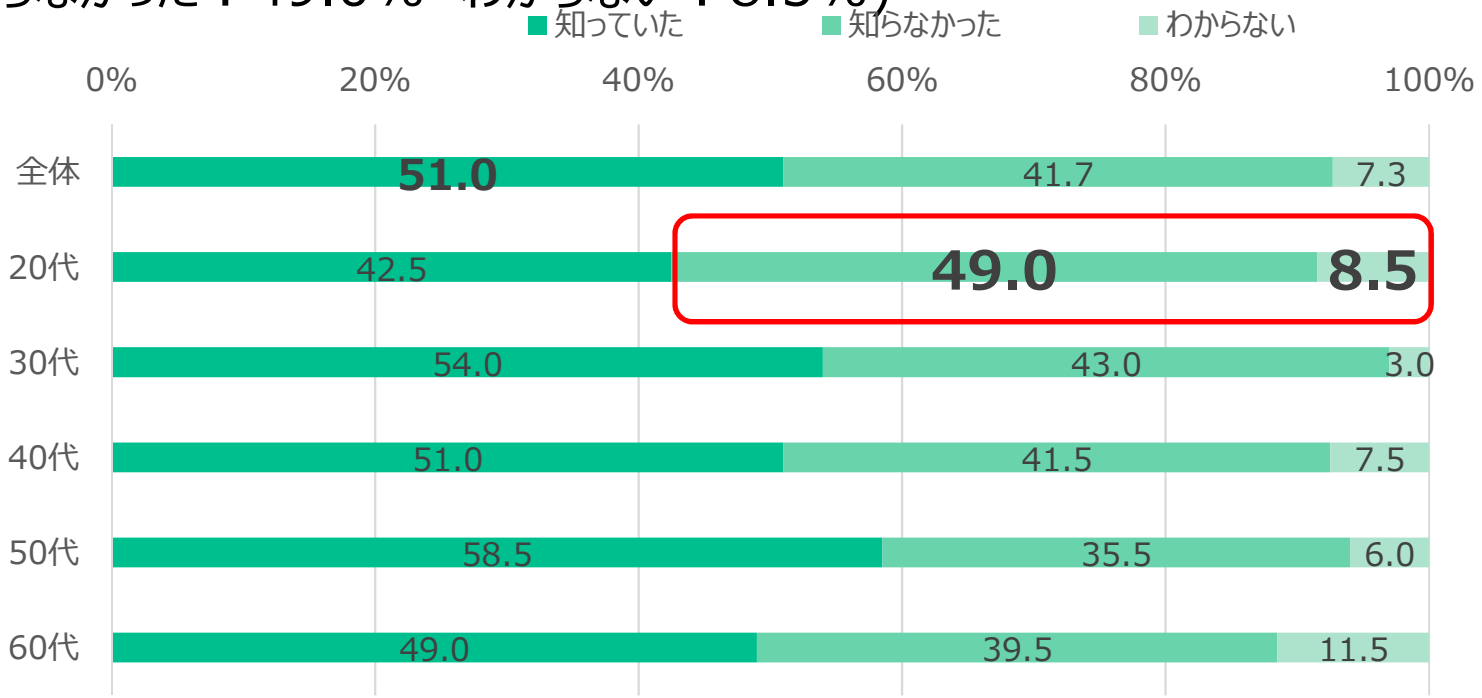


（２）IoT機器に関わるリスクの認知度

質問

「IoT 機器がデータを収集してクラウドにデータを送信することがあることをご存知ですか」

「知っていた」は51.0%、「知らなかった」は41.7%、「わからない」は7.3%であった。
IoT機器に関する潜在的なセキュリティリスクをイメージできている人は全体で半数以上存在するものの、年代別にみると**20代が最も認知度が低かった。**
（知らなかった：49.0%　わからない：8.5%）

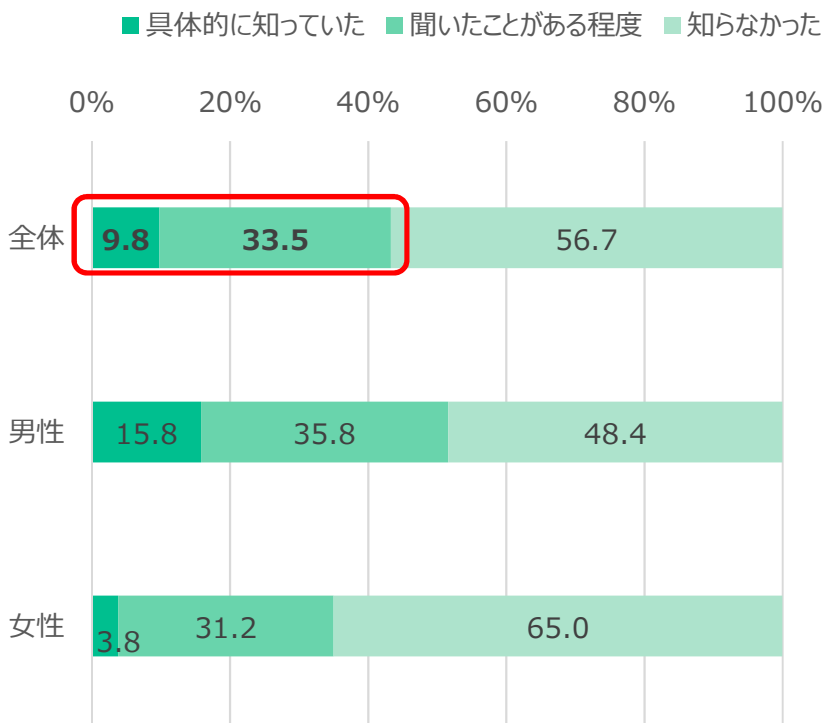


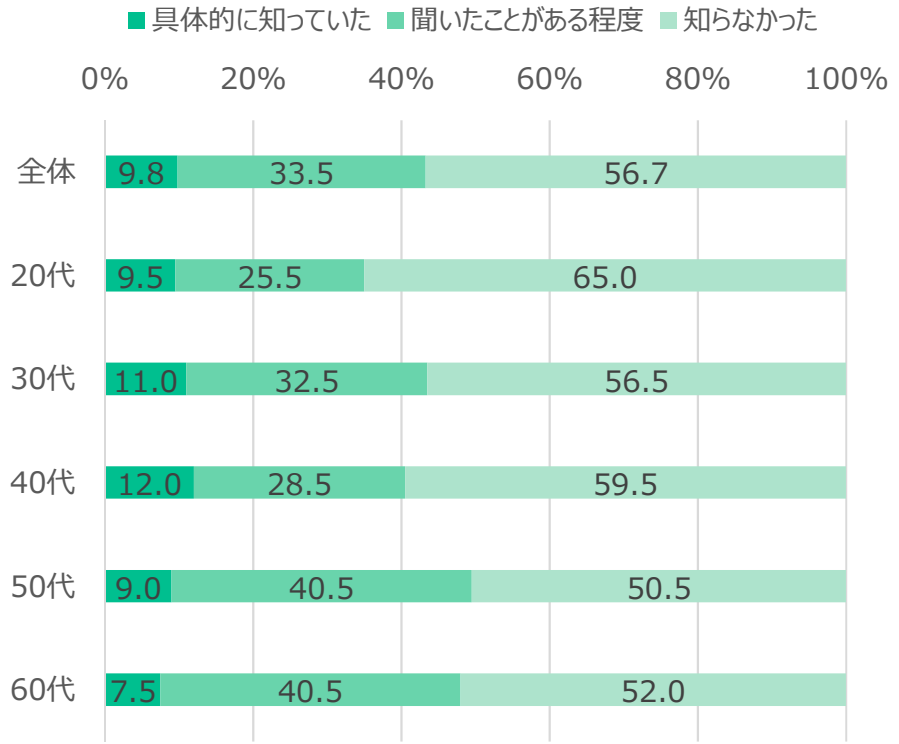
参考（IoT機器に関わるトラブルの認知度①）

事例①

「家庭内で使用していたネットワークカメラがリモートで不正に制御され、画像データがインターネット上に公開された」

監視カメラに関するトラブル事例は報道等で目にすることが多いためか、
「聞いたことがある程度」も含めた**全体の認知度は43.3%と高かった。**



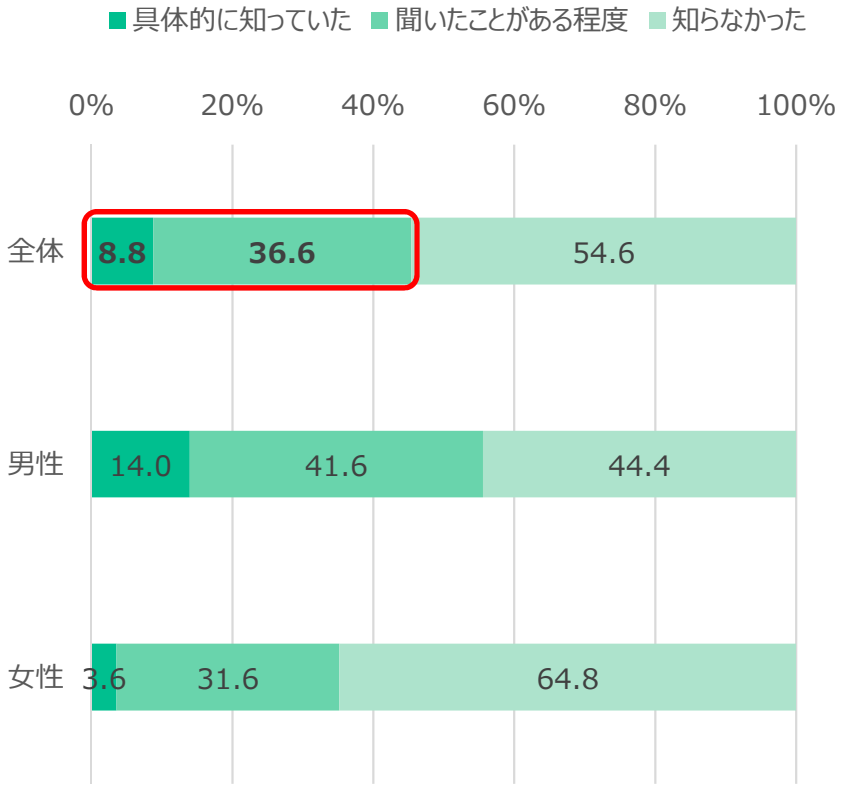


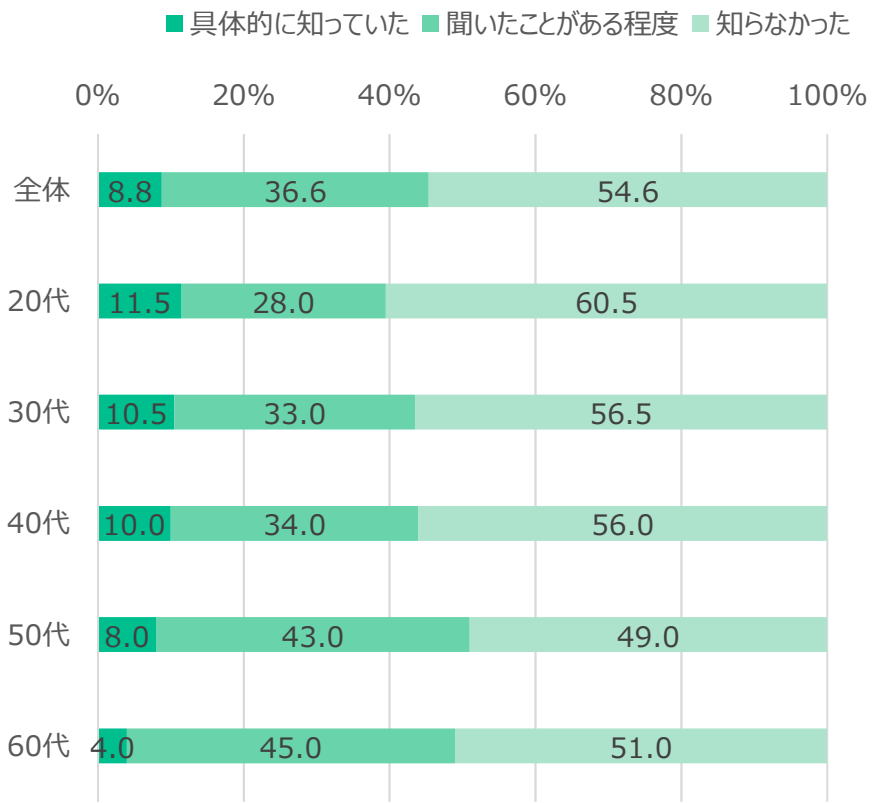
参考（IoT機器に関わるトラブルの認知度②）

事例②

「家庭内で使用しているルーターが不正に乗っ取られ、ルーターと接続しているＰＣ、スマホの通信が盗聴された」

実際に使ったことがある割合が高い家庭用ルーターに関するトラブル事例は、
「聞いたことがある程度」も含めた**全体の認知度が45.4%と高かった。**



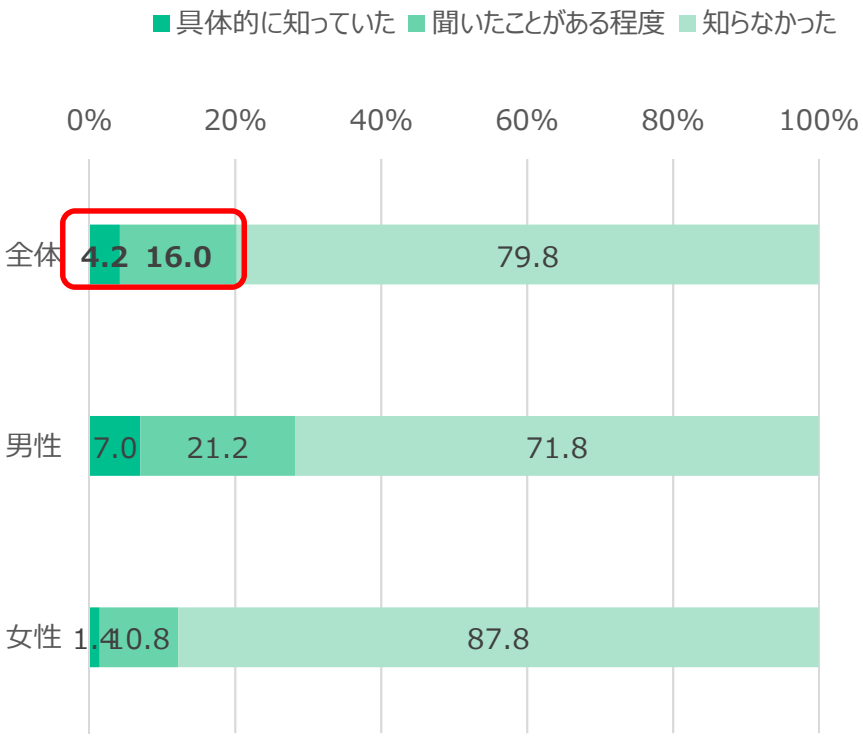


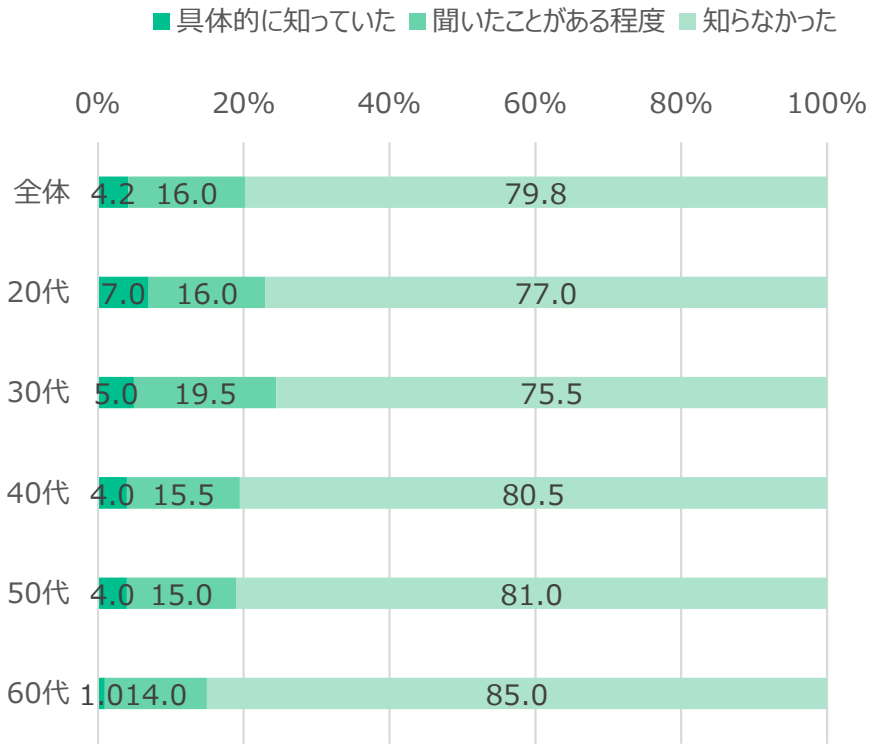
参考（IoT機器に関わるトラブルの認知度③）

事例③

「目の前にいない第三者によって、インスリンポンプとその制御装置(コントローラー)間の通信に含まれる患者の治療情報などが取得されたり、ポンプに対する操作が行われたりするなどの可能性があった」

医療現場におけるIoT機器のトラブル事例は、「聞いたことがある程度」も含めた
全体の認知度が20.2%と低かった。



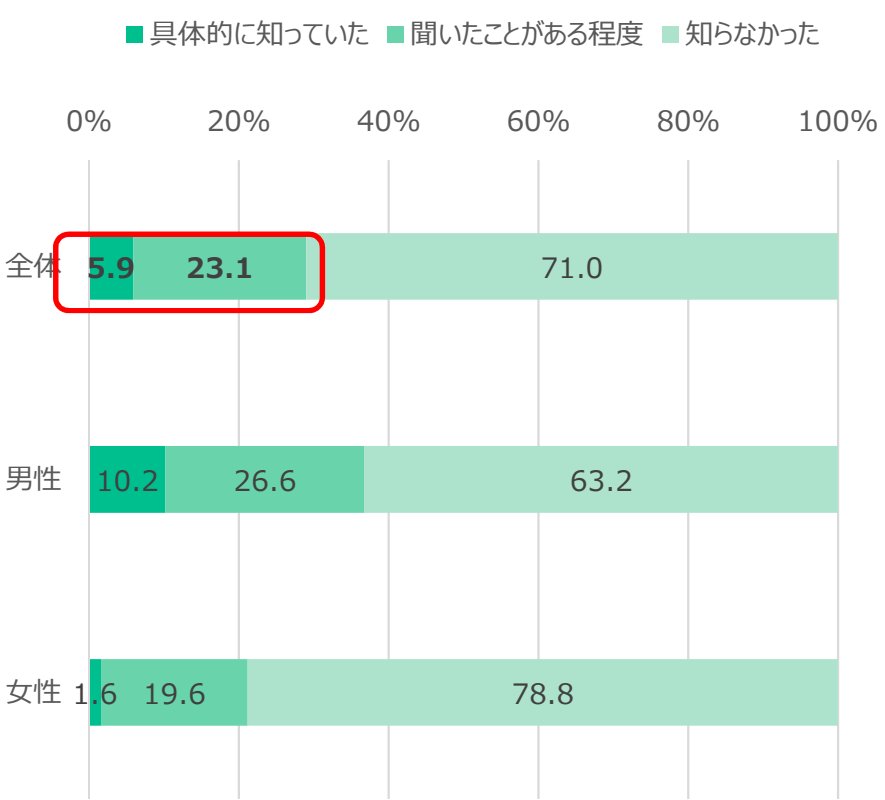


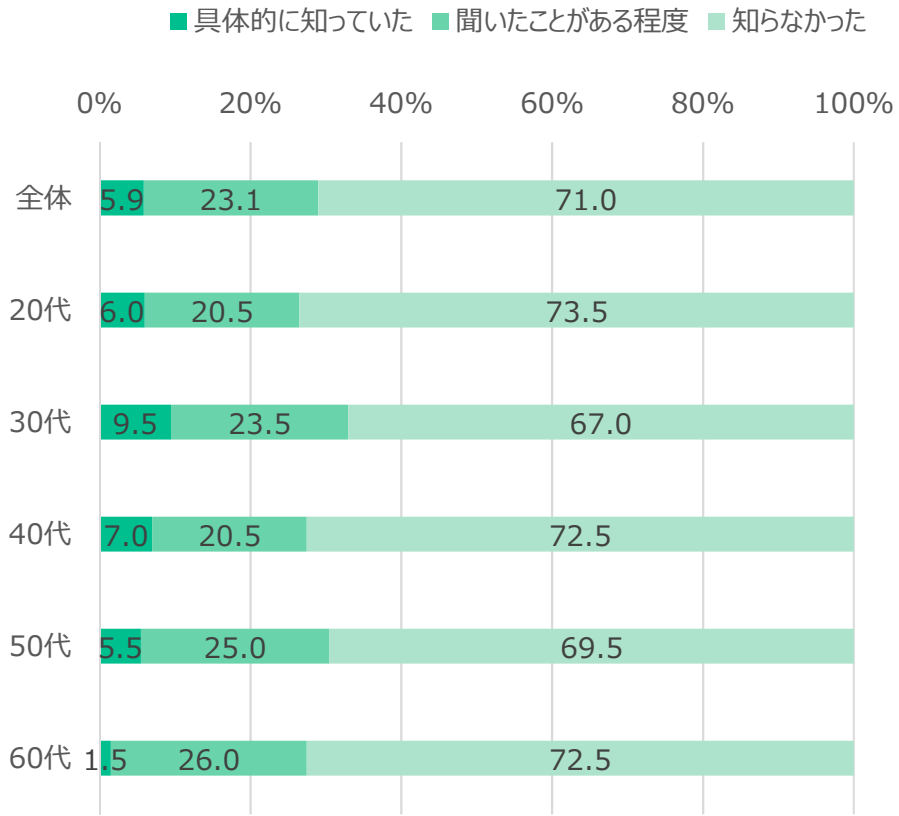
参考（IoT機器に関わるトラブルの認知度④）

事例④

「ネットワーク接続しているビデオレコーダーが不正に乗っ取られ、不正にアクセスされた」

ビデオレコーダーは身近にある機器ではあるものの、トラブル事例の認知度は低く、
「聞いたことがある程度」も含めた**全体の認知度は29.0%だった。**



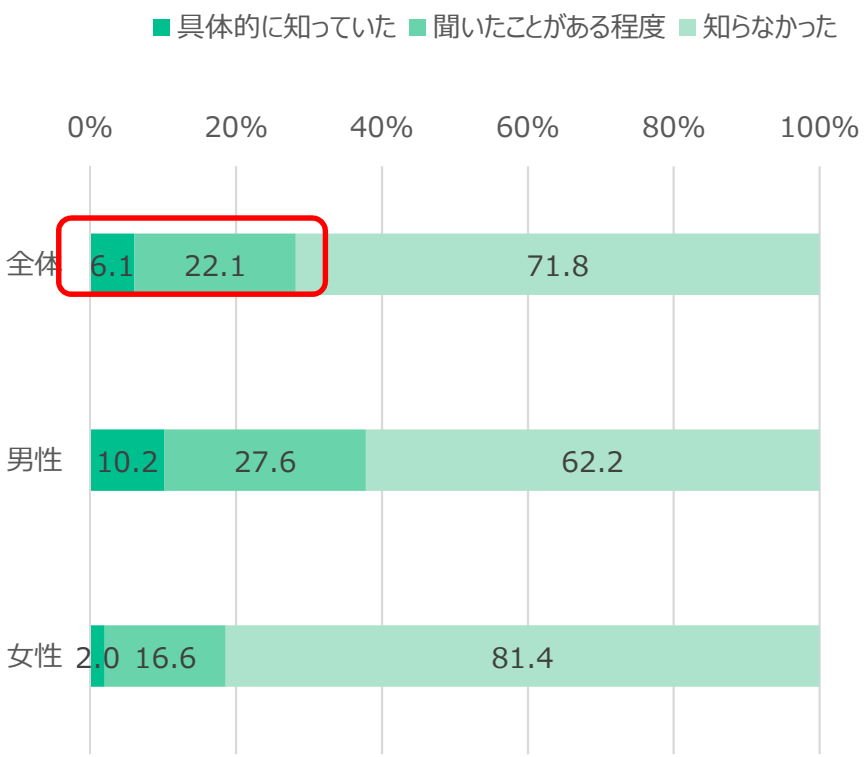


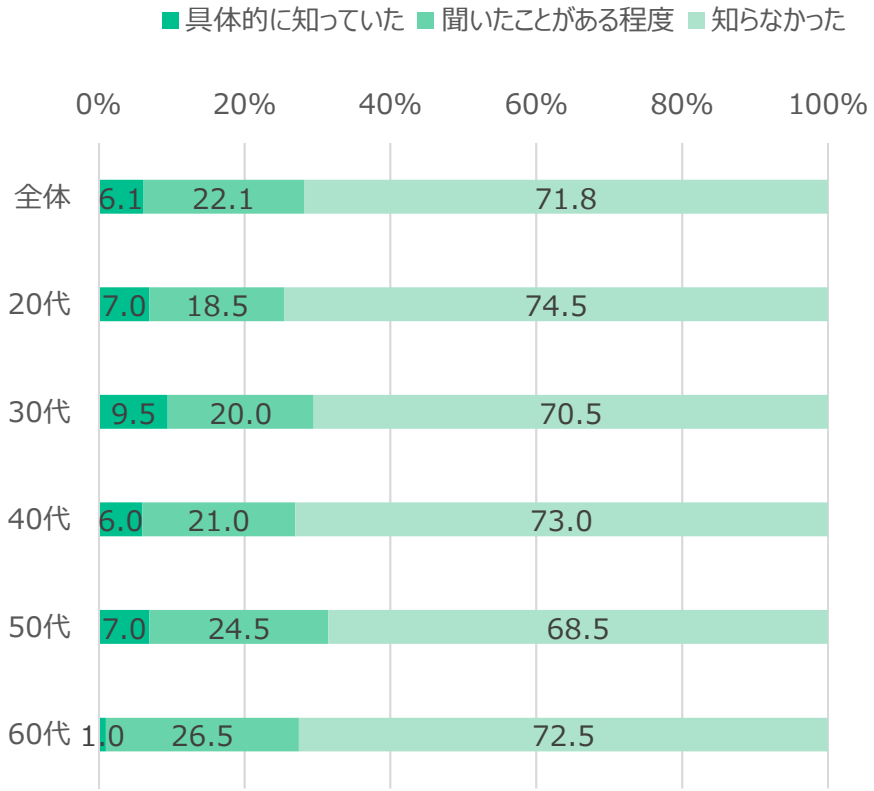
参考（IoT機器に関わるトラブルの認知度⑤）

事例⑤

「自動車の情報システム機器を外部の通信ネットワークからハッキングし、車両のプログラムを不正に改ざんできることが判明した。さらに改ざんによって、第三者がその場にいない状態で自動車の走行を操作できてしまう可能性があった 」

コネクテッドカーに関するトラブル事例の認知度は低く、「聞いたことがある程度」も含めた**全体の認知度は28.2%だった。**



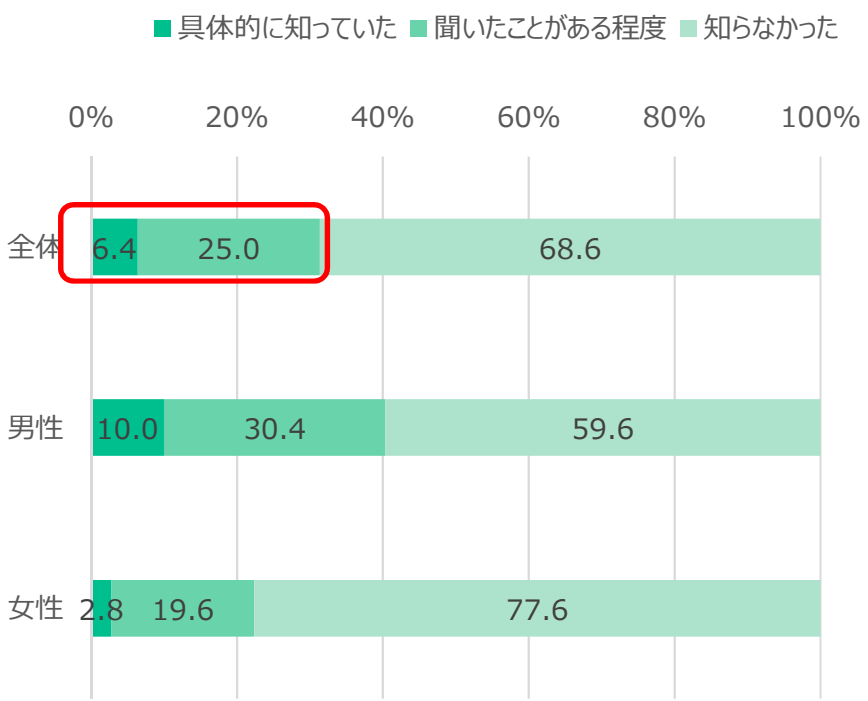


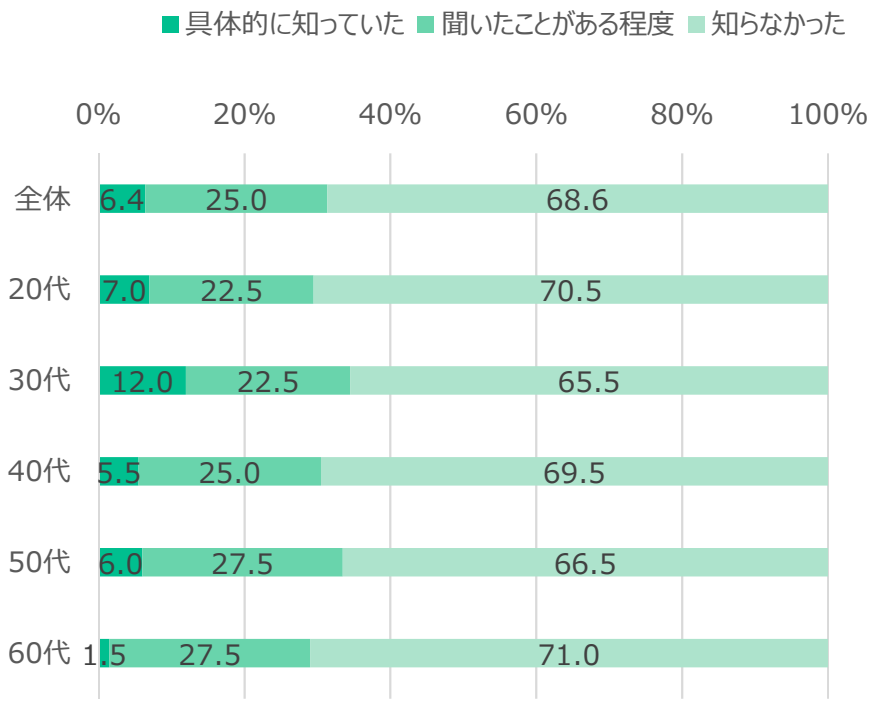
参考（IoT機器に関わるトラブルの認知度⑥）

事例⑥

「日本国内の大規模製造業の半数超において、サイバー攻撃によりスマート工場が生産を停止した」

各メディアで国内製造業がサイバー攻撃による被害を受けた報道がされており、このトラブル事例の「聞いたことがある程度」も含めた**全体の認知度は31.4%だった。**





3. サイバーセキュリティ対策

（１）サイバーセキュリティ対策の提供主体

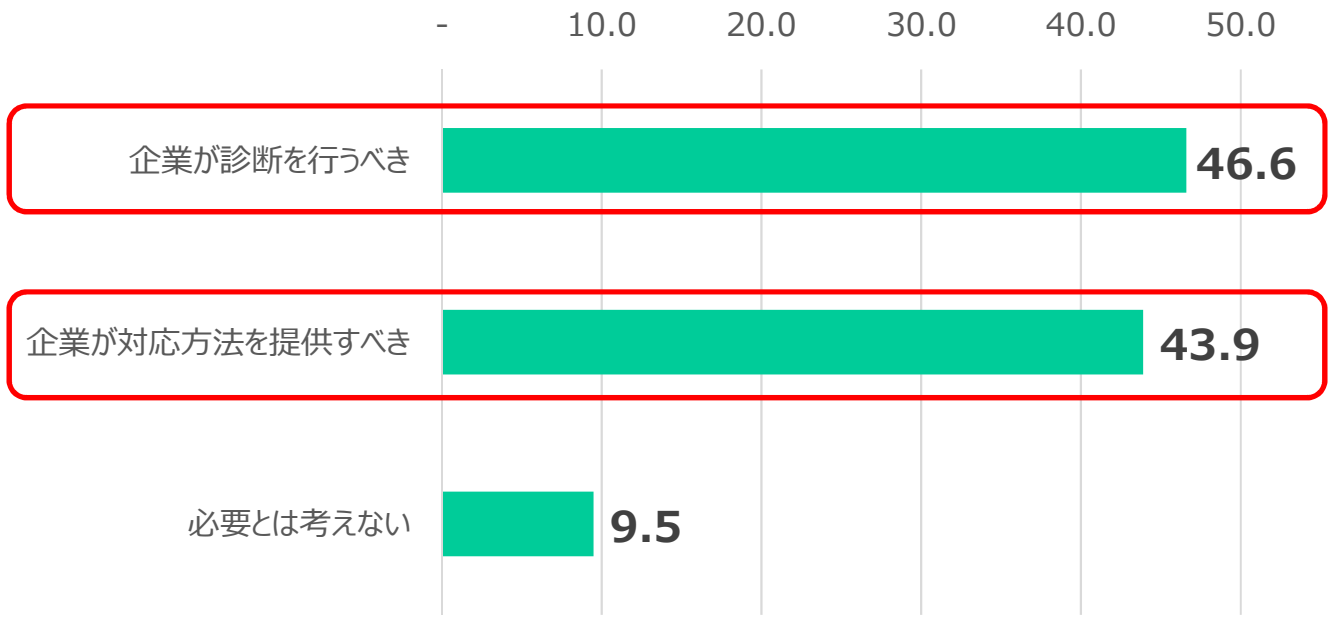
質問

「IoT 関連企業が、IoT 機器を提供するにあたり、どの程度サイバーセキュリティの対策をすべきと思いますか」

※IoT関連企業・・・「IoT機器を製造する企業やIoT機器を使ったサービスを提供する企業」を指す

「企業が診断を行うべき」46.6%、「企業が対応方法を提供すべき」43.9%、と両者の回答を合わせると90%を超えた。

消費者は、サイバーキュリティ対策をIoT機器やサービスを提供する企業（業界）に求める傾向が強いことがうかがえる。

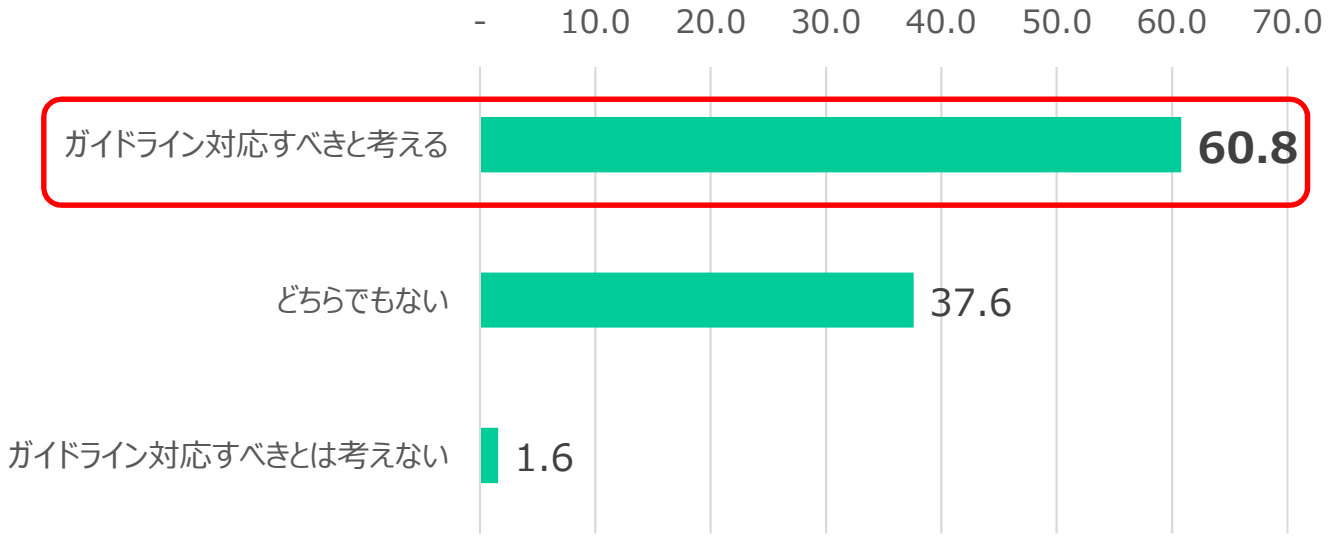


（１）サイバーセキュリティ対策の提供主体

質問

「『IoT 機器やIoT 機器を使ったサービスは、政府や業界団体が推奨、要求するサイバーセキュリティガイドラインなどの規格や標準を満たしているべきである』という考え方をどう思いますか」

「ガイドライン対応すべきと考える」との回答の割合が全体の６割を超えた。
消費者は、対策を講じるにあたって、ガイドライン等の指針に基づくべきと考えている傾向がうかがえる。
IoT機器を提供する企業（業界）にとって対策を講じることは不可欠であり、企業（業界）は、主体的に対策を講じるべきである。



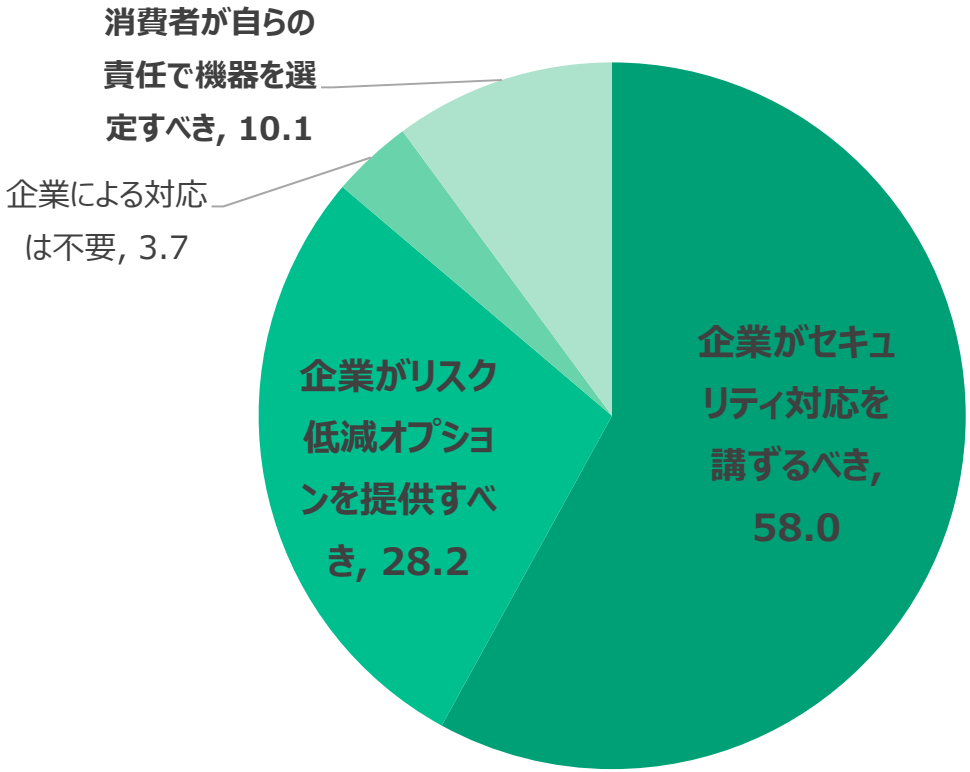
（２）企業に求めるサイバーセキュリティ対策

Advancing with you
MS&AD
INSURANCE GROUP

質問

「IoT関連企業が、IoT 機器を提供するにあたり、どの程度責任や対策を負うべきと思いますか」

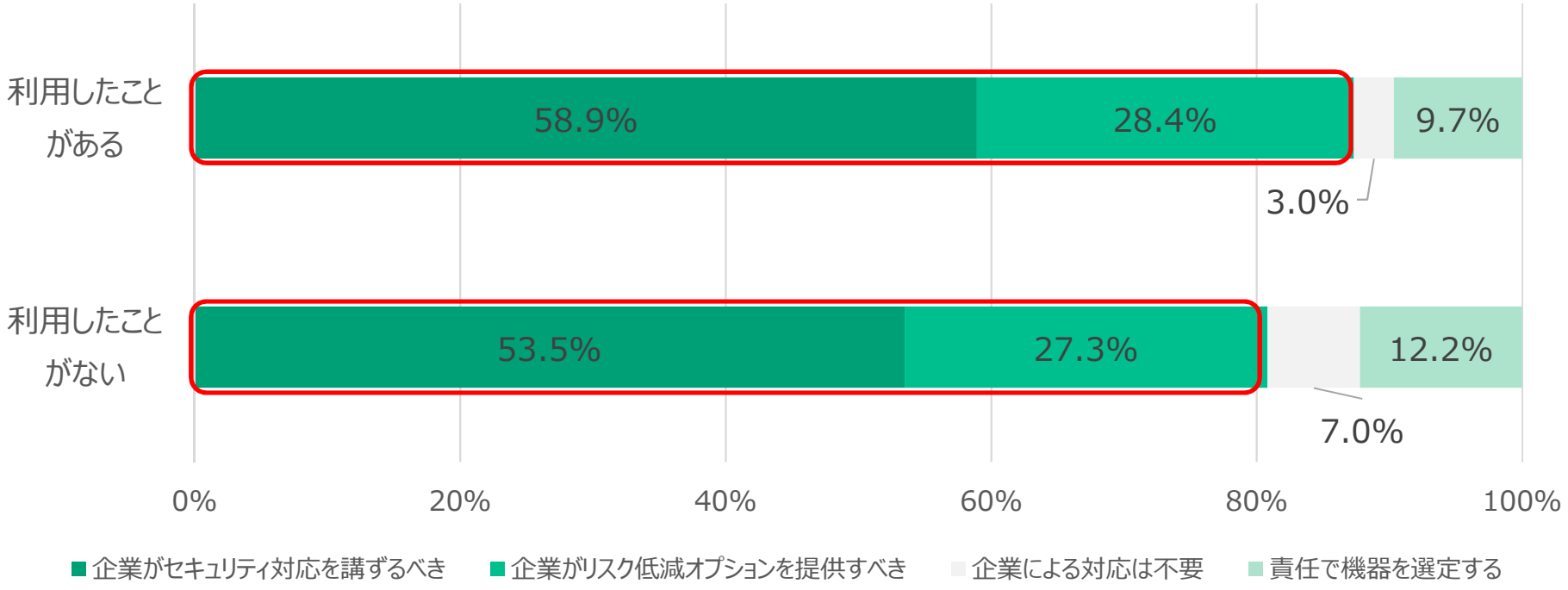
「企業がセキュリティ対応を講ずるべき」は58.0%、「企業がリスク低減オプション（※）を提供すべき」は28.2%の回答があり、**企業に主体的な対策を求める割合が高かった。**一方、消費者が自らの「責任で機器を選定する」の回答は10.1%にとどまった。



（※）リスク低減オプションの例：
IoT機器にサイバー攻撃を受ける可能性が発見されると、その対策を施した修正プログラムが提供される。

（２）企業に求めるサイバーセキュリティ対策

また、IoT 機器を「利用したことがある人」と「利用したことがない人」の間において、企業に対する要求に顕著な違いは見られず、いずれの立場の人も**「企業がセキュリティ対応を講ずるべき」**と**「企業がリスク低減オプションを提供すべき」**の回答の割合が多かった。

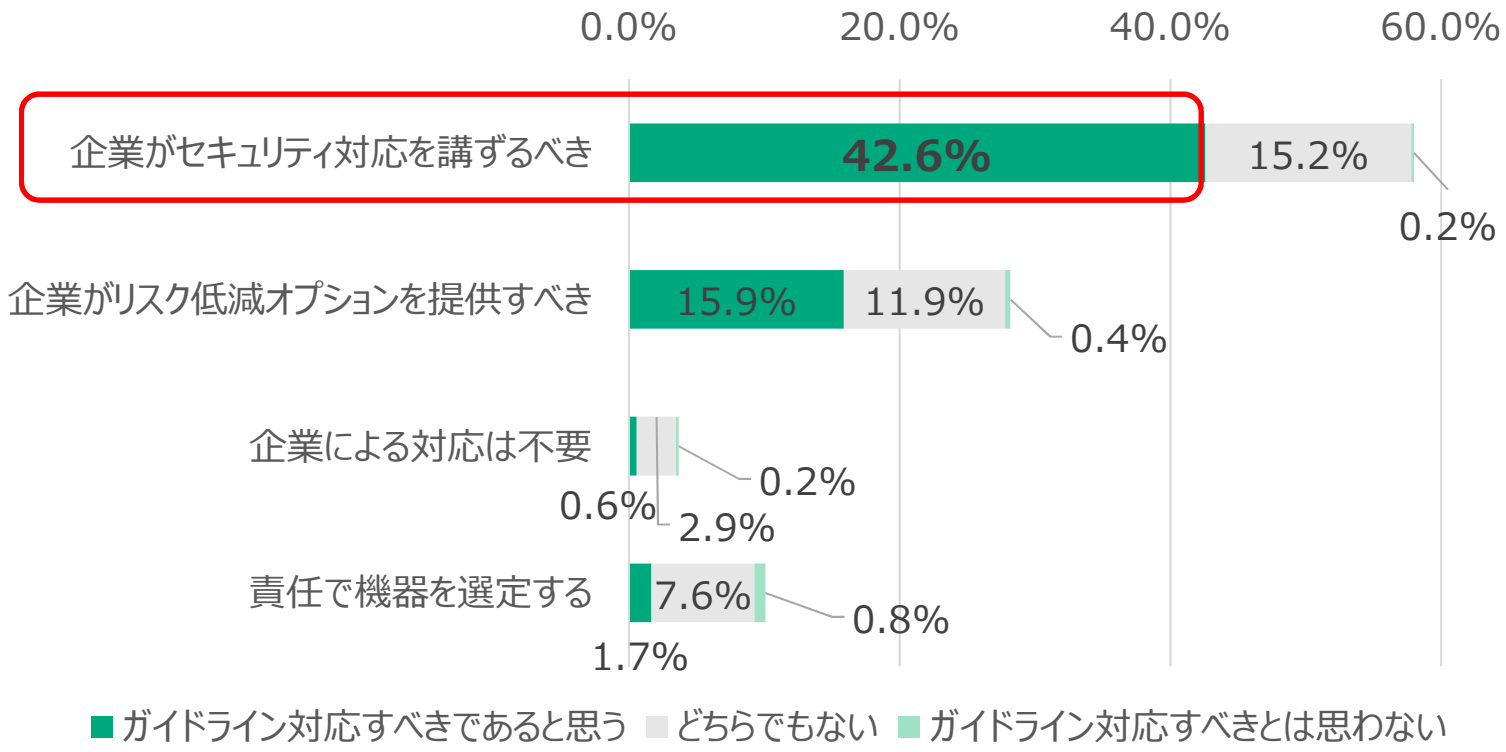


（２）企業に求めるサイバーセキュリティ対策

さらに、前ページの設問と下記の設問をクロス集計したところ、企業に対してガイドライン対応などの確かな対応・責任を求めている人の割合が**全体の４割を超えている**ことがわかった。

質問

「『IoT 機器やIoT 機器を使ったサービスは、政府や業界団体が推奨、要求するサイバーセキュリティガイドラインなどの規格や標準を満たしているべきである』という考え方をどう思いますか」

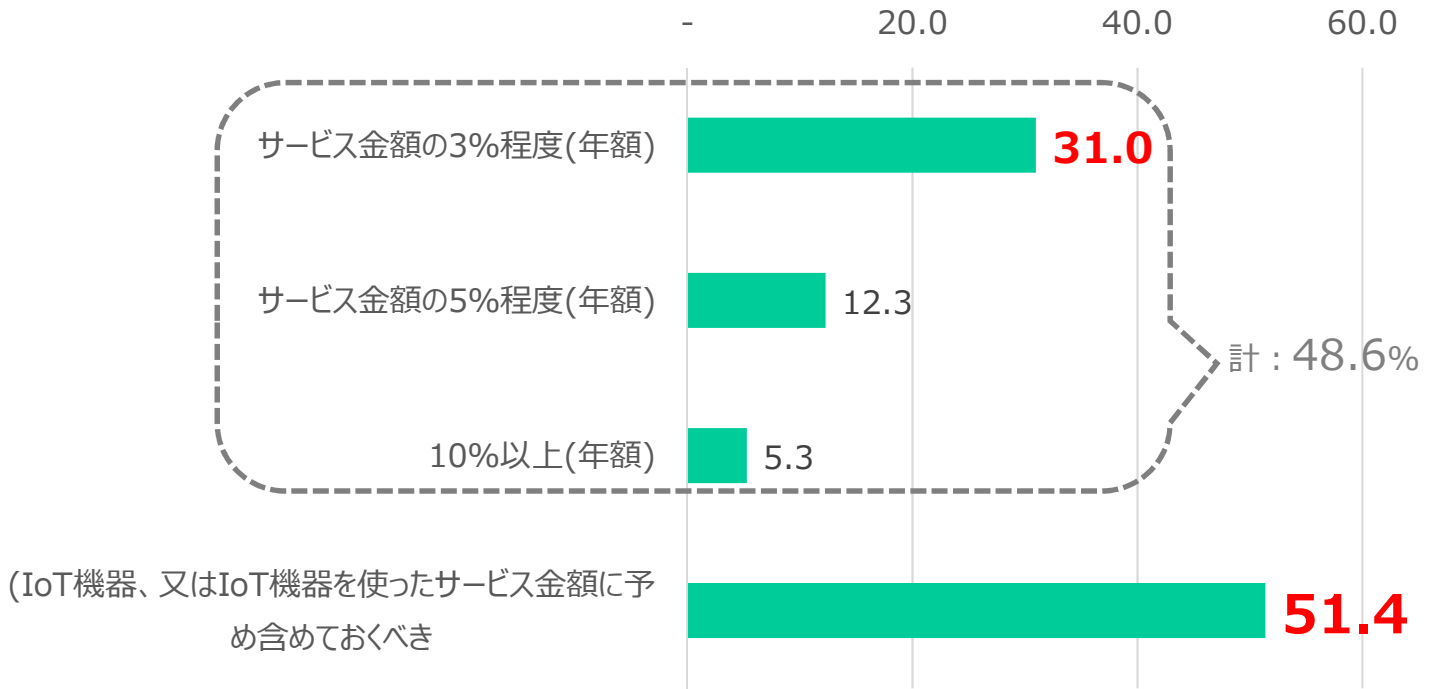


（３）セキュリティ対策費用の負担

質問

「IoT 機器の利用者として、あなたが負担してもよいと思うサイバーセキュリティ対策費用はいくらですか」

「サービス金額に予め含めておくべき」との回答が最も多かった（51.4%）。
全体の48.6%が、IoT機器やサービスの販売価格とは別に負担してもよいと回答したが、その負担割合は**「3%程度」と考える消費者の割合が30%**を超えていた。



MS&AD

MS&AD Insurance Group

MS&ADインターリスク総研株式会社
新領域開発部 サイバーリスク室

〒101-0063東京都千代田区神田淡路町２－１０５ワテラスアネックス
Tel：03-5296-8961／Fax：03-5296-8940
https://www.irric.co.jp/