2021.7.20

サイバーセキュリティニュース ＜2021 No.001＞

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
～IoT 機器を提供する事業者への提言～

【要旨】
■ 弊社では、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、IoT 機器や関連サービスを提供する企業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。
■ 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。

１．意識調査の背景

IoT（Internet of Things）とは、モノや機器がインターネットで結ばれる技術革新を指す。IoT が搭載された機器の具体例としては、スマート家電、家庭用ゲーム機、監視カメラ、自動運転車、ドローン、産業用ロボット、医療機器などが挙げられる。

これまでのインターネットは主にコンピュータ同士の通信に使われていたが、IoT 機器では、モノの状態や動き、自然現象、生物の動きなどをセンサーなどでデータ化して通信し、ネットワーク上でさまざまなデータの受け渡しや、離れた場所（サイバー空間）からモノの状態を把握したり、動きを制御することができる。例えば、スマートフォンのアプリなどを使い、外出先からインターネットを介して風呂を沸かしたり、テレビ番組の録画をしたりするなどが挙げられる。

個人用の IoT 機器・サービスが普及し、身近な暮らしがより便利になる一方で、IoT 機器に対するサイバー攻撃は年々増加傾向にある。例えば、マルウェアに感染した IoT 機器が大規模なサイバー攻撃を引き起こすための道具として悪用されてしまう事例が観測されている。

（詳細は、本レポートの【参考１】IoT 機器を標的としたサイバー攻撃の観測　を参照されたい）

IoT 機器に対するサイバー攻撃が年々増加する原因として､IoT 機器について管理が行き届きにくい、セキュリティ対策ソフト導入が困難、利用者の意識の低さなどが挙げられる。

弊社では、IoT 機器の利用実態や認知度、および 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（以下、IoT 関連企業）への要望を把握するために「個人用 IoT 機器に関するサイバーセキュリティ対策についての意識調査」を行った。

２．調査の概要

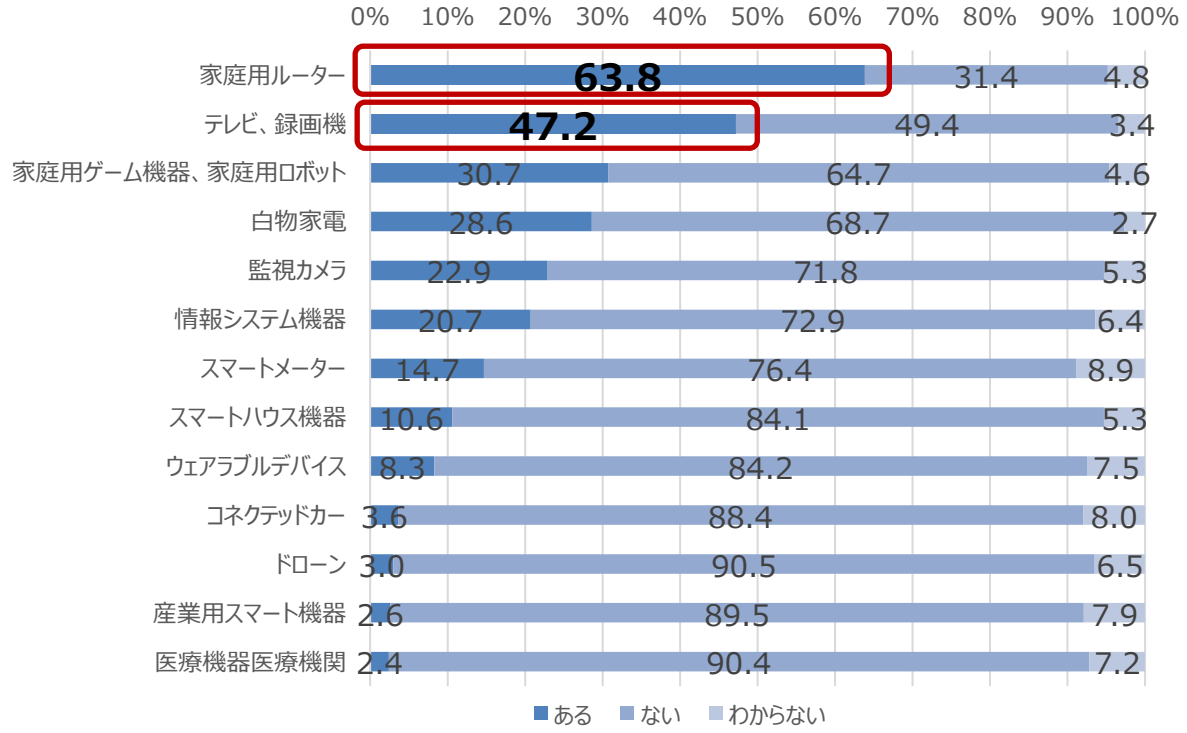
調査方法、対象者、有効回答者数は、以下のとおり。

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）

3. 調査の結果

（1） IoT 機器の利用状況

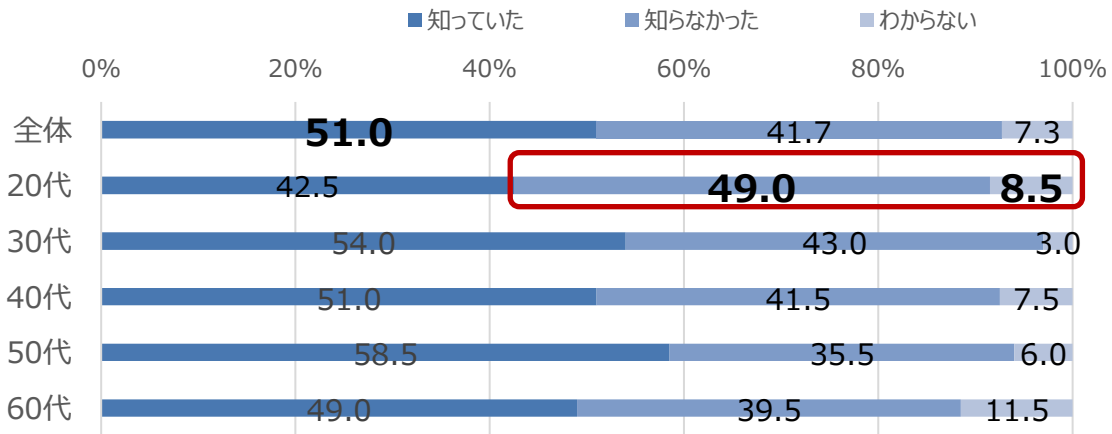
「普段の生活又は職場環境において、IoT 機器を利用したことはありますか」の問いに対し、特に「家庭用ルーター」と「テレビ・録画機」を実際に使ったことがあるとの回答が多かった。あらゆるものが無線インターネットでつながる IoT 機器が日常生活に浸透しており、消費者にとって身近な存在となっていることがうかがえる。



【図 1】IoT 機器別の使用割合

（2） IoT 機器に関わる潜在的リスクの認知度

「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」の問いに対し、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%）。

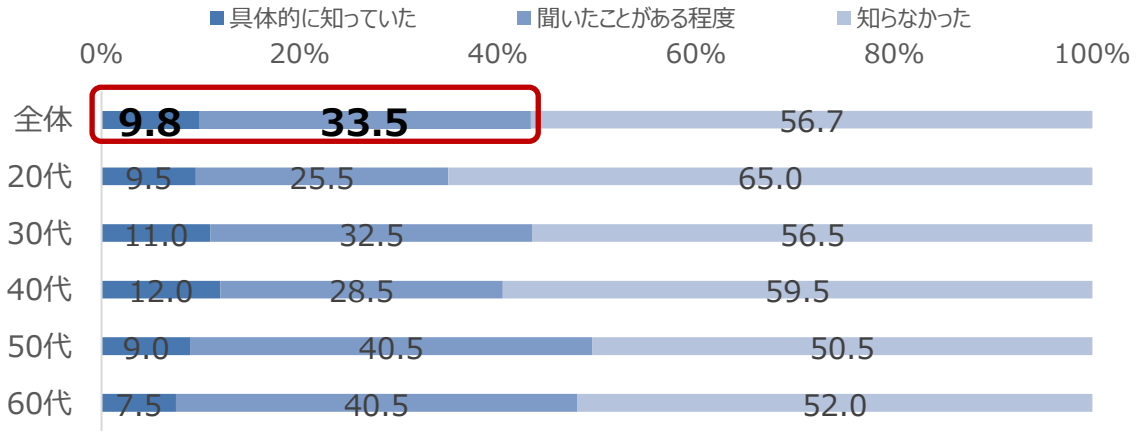


【図 2】IoT 機器に関わる潜在的リスクの認知度

（３）IoT 機器に関わる具体的リスクの認知度

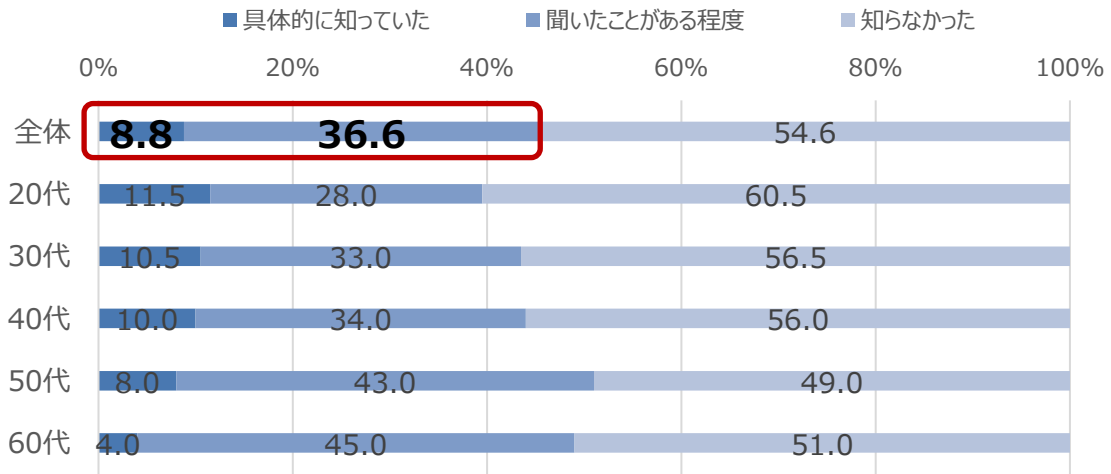
IoT 機器に関わるトラブル事例を複数挙げて、消費者の認知度を確認した。調査の結果、普段から利用されている機器に関わるトラブル事例の認知度が総じて高いわけではないことがわかった。

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』事象について知っているか」の問いに対し、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。



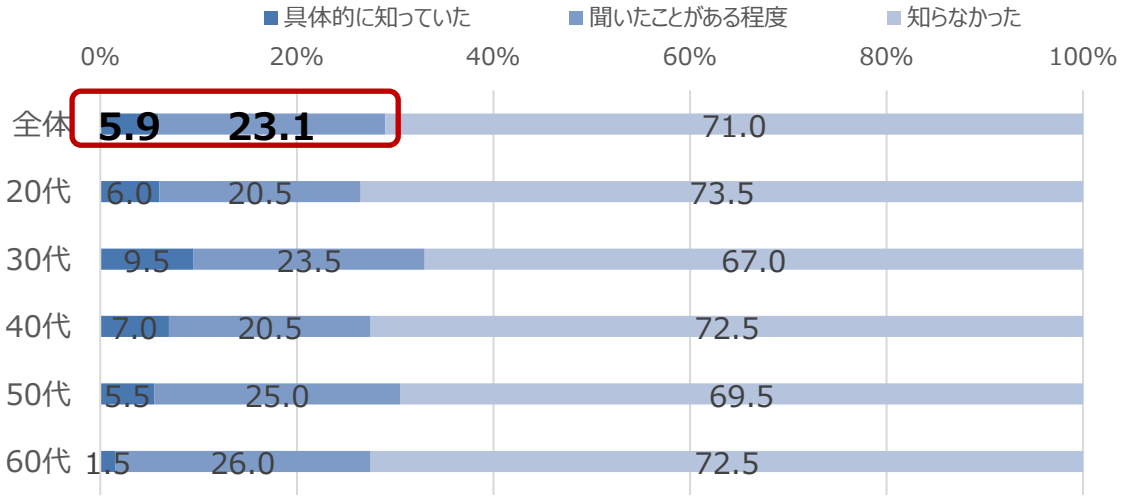
【図３】「ネットワークカメラのリモートによる不正制御」の認知度

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」事象を知っているか」の問いに対し、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。



【図４】「ルーター乗っ取りによる PC、スマホ通信の盗聴」の認知度

③ 「『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』事象を知っているか」の問いに対し、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。



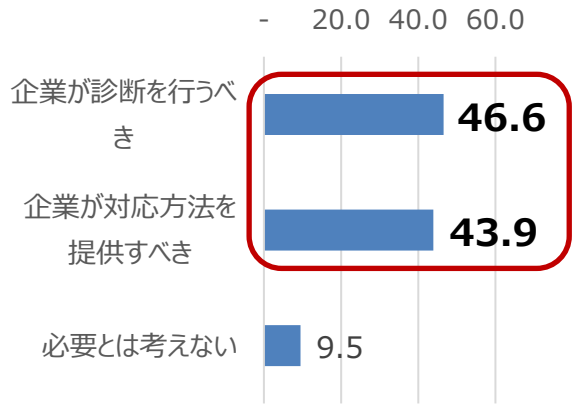
【図５】「ネットワーク接続されているビデオレコーダーの不正使用」の認知度

（４） 企業はどの程度サイバーセキュリティの対策をすべきか

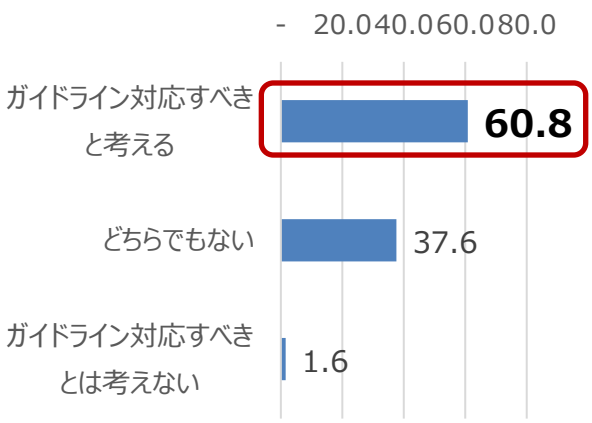
「IoT 関連企業が、IoT 機器を提供するにあたり、どの程度サイバーセキュリティの対策をすべきと思いますか」との問いに対し、「企業が診断を行うべき」46.6%、「企業が対応方法を提供すべき」43.9%、と両者の回答を合わせると 90%を超えた。消費者は、サイバーキュリティ対策を IoT 機器やサービスを提供する企業（業界）に求める傾向が強いことがうかがえる。

さらに「『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」との問いに対しては、「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。

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。



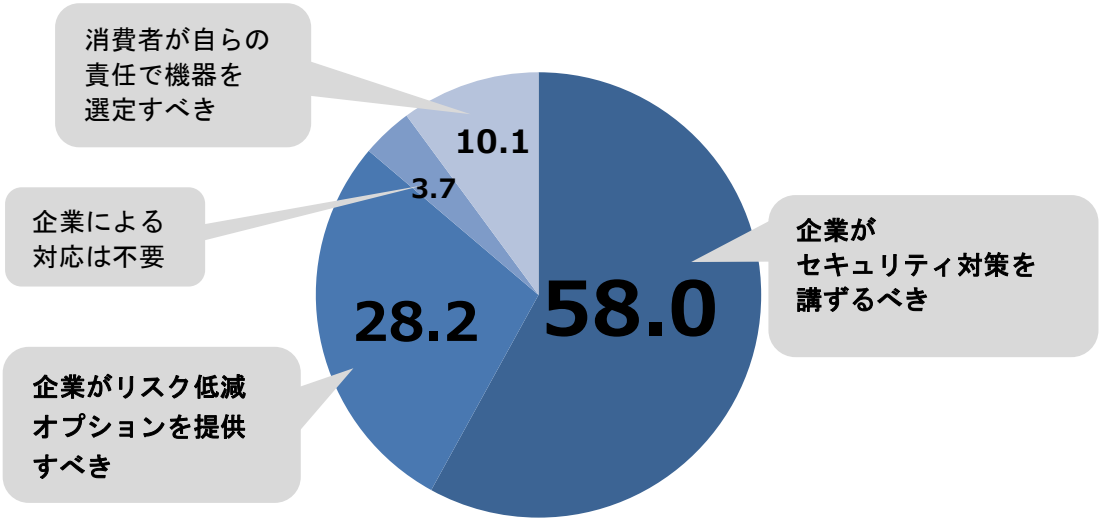
【図６】サイバーセキュリティ対策の提供主体



【図７】「ガイドライン対応」への考え

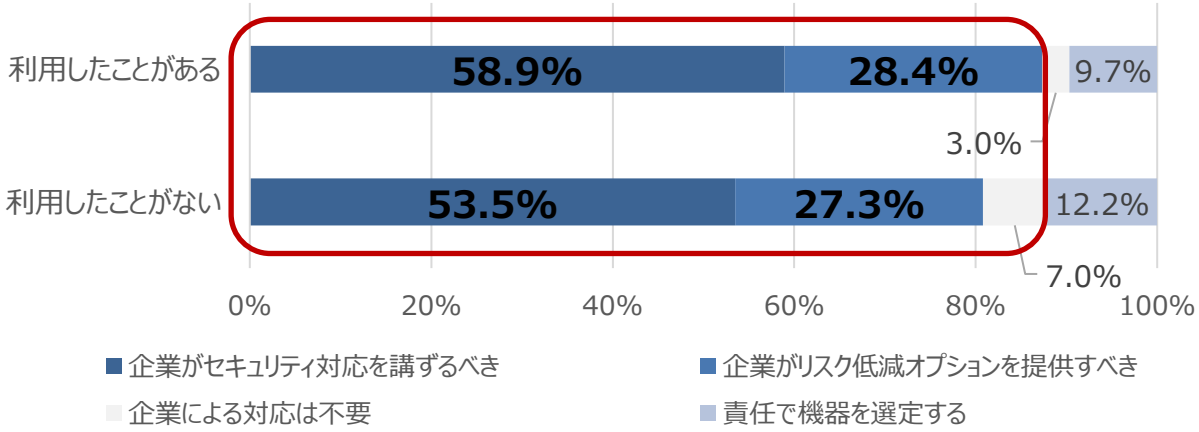
（５）　消費者は企業にどの程度のサイバーセキュリティ対策を求めているか

「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」との問いに対し、「企業がセキュリティ対策講ずるべき」と回答した消費者は58.0%、「企業がリスク低減オプション[1]を提供すべき」と回答した消費者は 28.2%にのぼり、企業に主体的な対策を求める割合が高いことがわかった。一方、消費者が自らの「責任でサイバーセキュリティ対策を行っている機器を選定する」という選択肢を選んだ消費者は 10.1%にとどまった。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事業者に求める傾向が強いことがうかがえる。



【図８】消費者が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」あるいは「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。



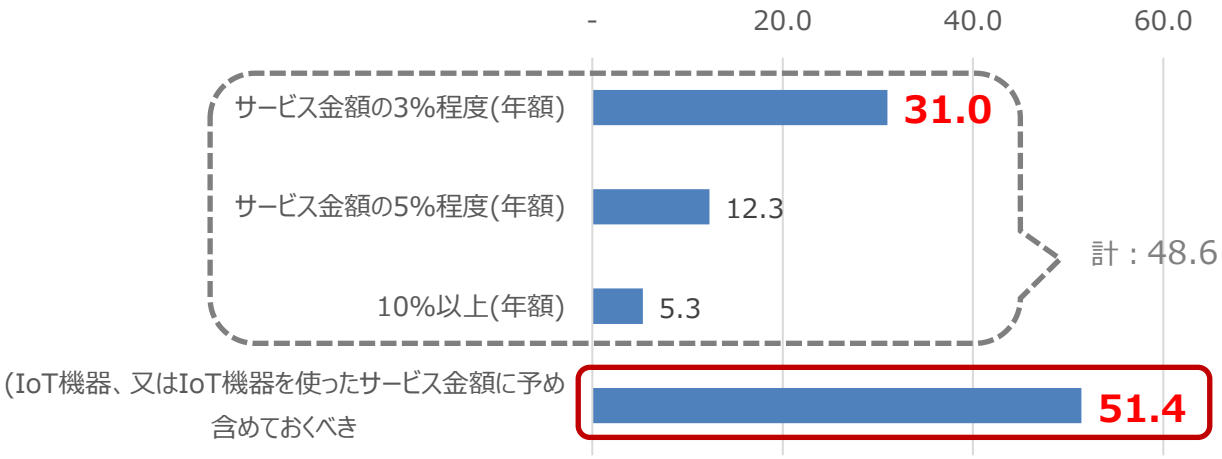
【図９】IoT 機器利用の有無による企業に求めるサイバーセキュリティ対策の違い

[1] 例として、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ことなどがある。

（６）消費者が負担してもよいと考えるセキュリティ対策費用とは

「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」という問いに対し、「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、サービス金額の 3%程度と考える消費者が最も多く、全体の 31%であった。



【図１０】消費者が負担してもよいと考えるセキュリティ対策費用

４． IoT 機器を提供する事業者への３つの提言

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、IoT 関連企業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。

今回の調査結果を踏まえた以下の３つの提言が IoT 機器関連企業における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。

（１）リスクを正確に把握し早期の対策が必要

消費者にとって IoT 機器は身近で必要不可欠な製品になってきており、IoT 機器に対する十分なサイバーセキュリティ対策が必要と考える。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）セキュリティ対策の主体は IoT 機器関連企業

消費者は 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。そのため、消費者がセキュリティ対策を講じるのは困難であるといえる。IoT 機器関連企業や業界が、セキュリティ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）セキュリティ対策は費用と効果のバランスが重要

消費者の半数は、対策費用を IoT 機器やサービスの販売価格とは別に負担してもいいと考えているが、許容する負担割合は少ない。

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。

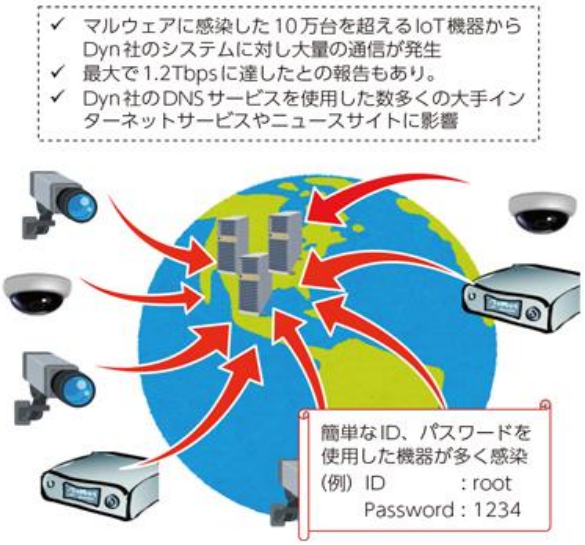
効果的な対策を講じるためには、IoT 機器に内在するリスクを正しく把握することが肝要であり、その方法のひとつとして外部の IoT 機器セキュリティ診断サービスを活用することが挙げら

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。

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
マネジャー・上席コンサルタント　岡田　道雄

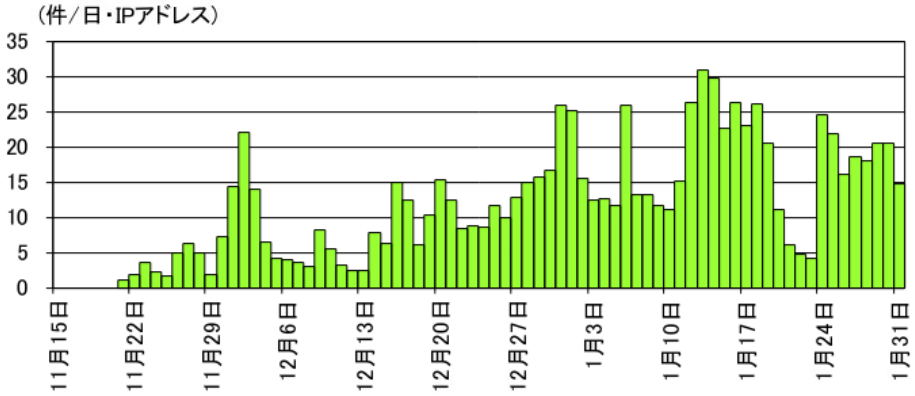
【参考１】IoT 機器を標的としたサイバー攻撃の観測

2016 年 10 月、米国では、「Mirai」と呼ばれるマルウェアに感染した IoT 機器が踏み台となり、大規模な DDoS 攻撃が発生、大手のインターネットサイトサービスやニュースサイトにアクセスできなくなるなど障害が発生した。



【図１１】マルウェア Mirai に感染した IoT 機器が悪用されたサイバー被害イメージ
総務省「平成 30 年版 情報通信白書－IoT 等に関する取組」より引用[2]

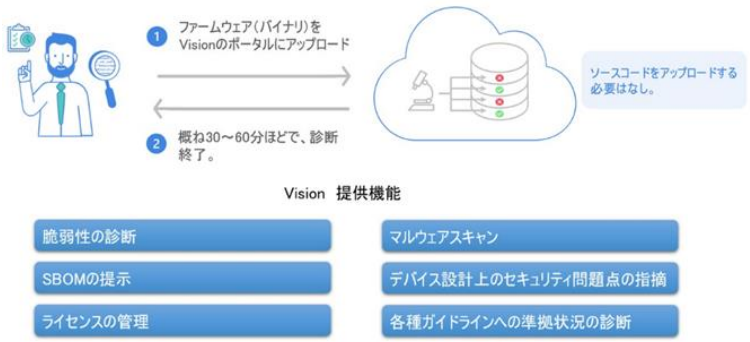
「Mirai」による大規模サイバー事故から５年が経過しているが、「Mirai」を一部改変して作られた亜種と思われるマルウェアが生み出され、依然としてインターネット上にばらまかれていることが観測されている。警察庁は、「脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等についてインターネット定点観測において」[3]と題するレポートを公表、警察庁が所有するインターネット定点観測点において、複数の IoT 機器を標的としたアクセスの増加を観測、アクセスの挙動を確認したところ、「Mirai」の特徴を有していたと報告している。



【図１２】Mirai の特徴を有するアクセス件数の推移
警察庁「脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等について」より引用

[2] 総務省「平成 30 年版　情報通信白書」2018 年 7 月 3 日:
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd245210.html (2020 年 7 月 14 日閲覧)
[3] 警察庁「脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等について」2021 年 3 月 5 日:
https://www.npa.go.jp/cyberpolice/detect/pdf/20210305.pdf (2020 年 7 月 14 日閲覧)

ＭＳ＆ＡＤインターリスク総研株式会社では、IoT 機器を対象としたサイバーセキュリティ診断サービスを提供しています。設計書やソースコード等を必要とせずに、IoT 機器に搭載されているソフトウェアそのままの形で数分から数十分程度で診断することが可能となります。



【診断例】

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
サイバーリスク・情報セキュリティに関するコンサルティング・セミナー等を実施しております。コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
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
千代田区神田淡路町2-105 TEL:03-5296-8961／FAX:03-5296-8941
https://www.irric.co.jp/