2024年10月16日
Capterra（キャプテラ）プレスリリース

【経営層のサイバーセキュリティに関する調査】
日本のIT担当者の75%が「一般社員よりも経営層がサイバー攻撃に遭いやすい」と指摘

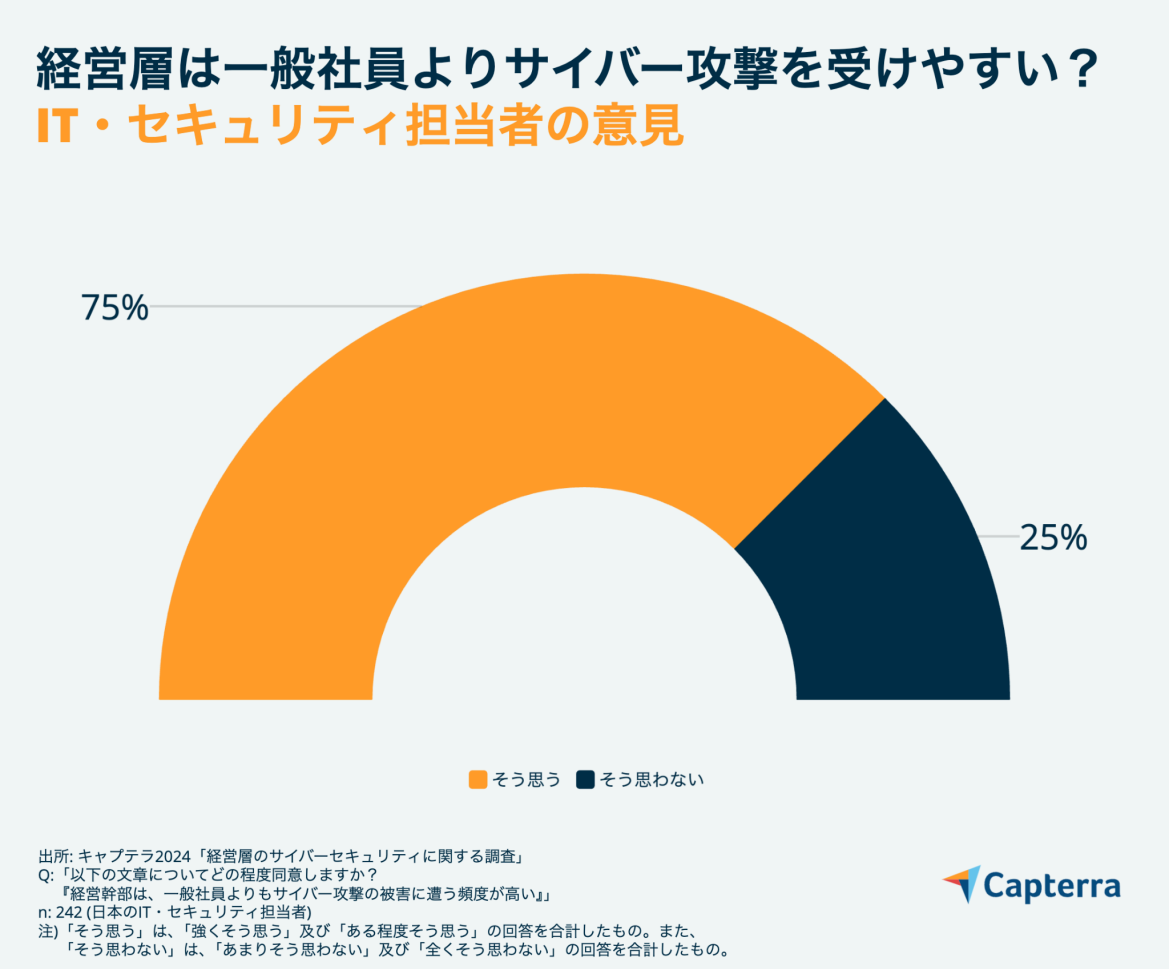
SaaSレビュープラットフォームのキャプテラはこの度、世界11カ国の2,648名（日本からは242名）の、IT・セキュリティ担当者に調査を行い、経営層が直面するサイバー攻撃の現状とその対策をまとめました。

本記事は、キャプテラ(Capterra)のWebサイトに掲載されている「経営層はサイバー攻撃に遭いやすい？IT担当者75%が指摘」の一部を抜粋したものです。調査内容の詳細は本記事文末でご覧いただけます。

本記事のポイント：

1. 日本のIT担当者の75%が、「一般社員よりも経営層がサイバー攻撃に遭いやすい」と指摘
2. 半数以上が「過去18ヶ月に経営幹部がサイバー攻撃の標的となった」
3. 日本の経営幹部が狙われるサイバー攻撃、最も多いのは「マルウェア攻撃」
4. 経営幹部に特別なセキュリティ研修を実施する企業の割合、日本は26%で最下位

1、日本のIT担当者の75%が、「一般社員よりも経営層がサイバー攻撃に遭いやすい」と指摘



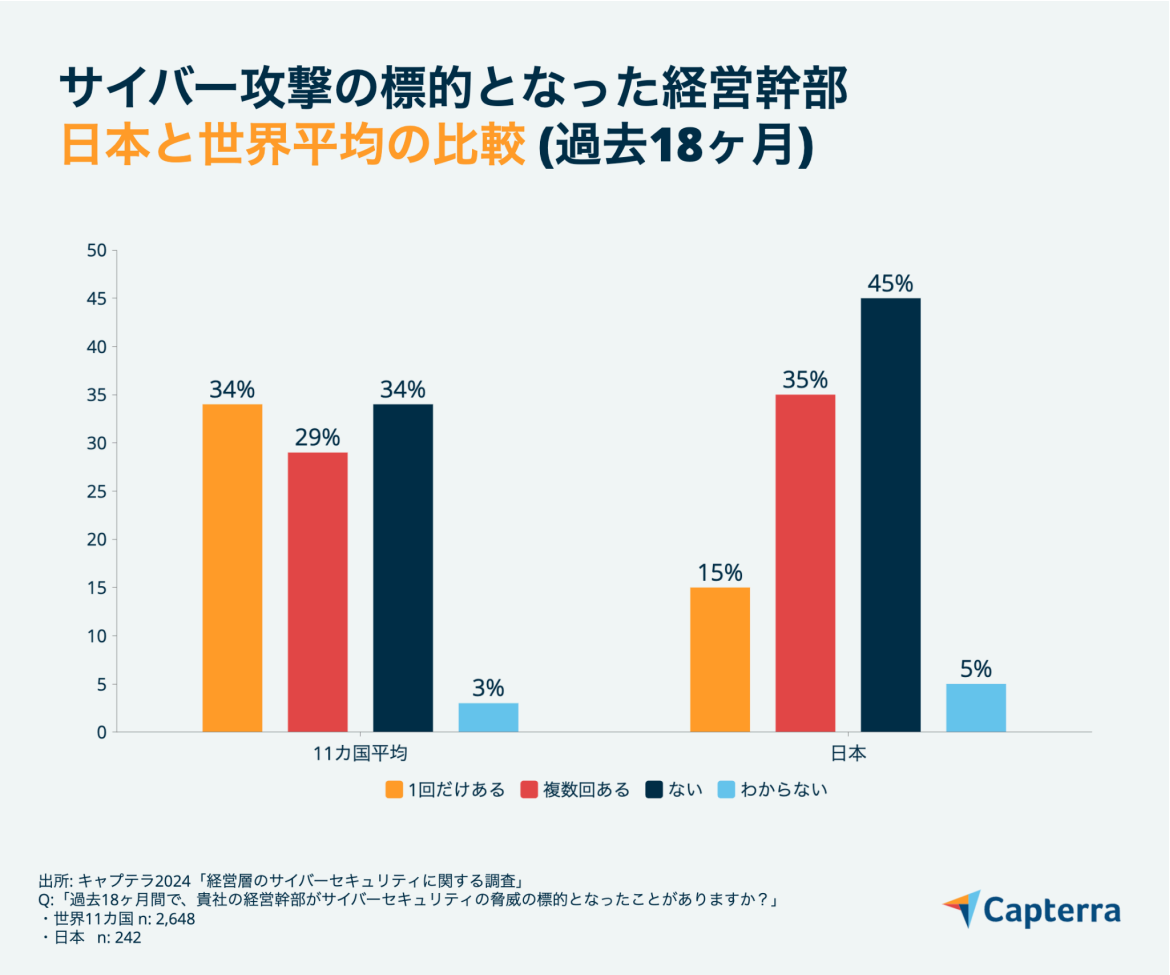
Q.「以下の文章についてどの程度同意しますか？」
経営幹部は、一般社員よりもサイバー攻撃の被害に遭う頻度が高い
注)「そう思う」は、「強くそう思う」及び「ある程度そう思う」の回答を合計したもの。また、「そう思わない」は、「あまりそう思わない」及び「全くそう思わない」の回答を合計したもの。

「そう思う」(75%)
「そう思わない」(25%)

日本のIT・セキュリティ担当者の大多数が、経営層は一般社員よりもサイバー攻撃に遭いやすいと指摘しています。一般社員だけではなく、企業経営陣に対しても適切なサイバーセキュリティトレーニングや効果的な対策が講じる必要性が見えました。

2、半数以上が「過去18ヶ月に経営幹部がサイバー攻撃の標的となった」

続いて、過去18ヶ月間に経営幹部がサイバー攻撃の標的になったかどうかを尋ねました。



Q.「過去18ヶ月間で、貴社の経営幹部がサイバーセキュリティの脅威の標的となったことがありますか？」

11カ国平均

- 一回だけある（34%）
- 複数回ある（29%）
- ない（34%）
- わからない（3%）

日本

- 一回だけある（15%）
- 複数回ある（35%）
- ない（45%）

- わからない（5%）

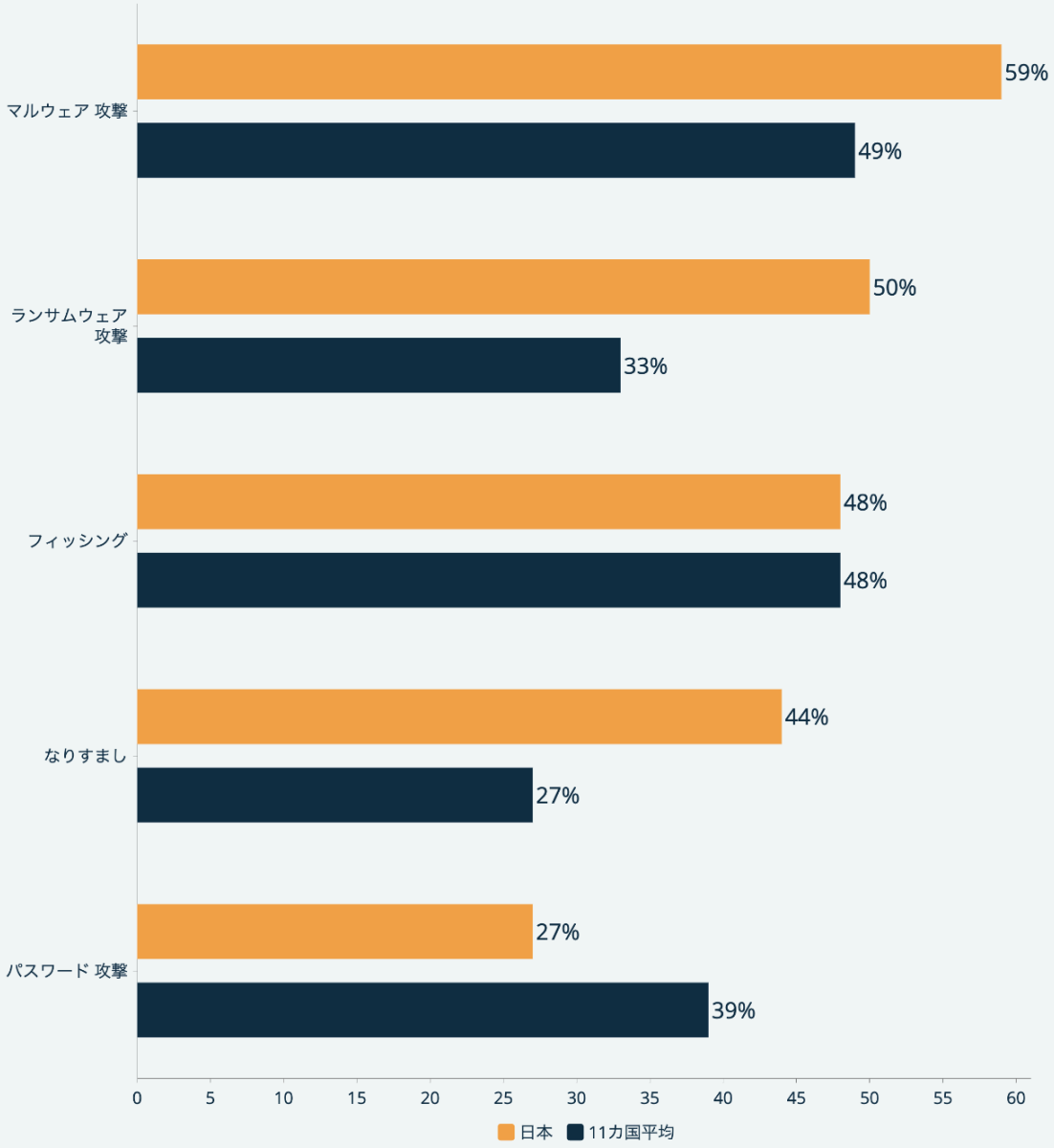
世界平均では、経営層がサイバー攻撃の対象に「一度だけ」または「複数回」なった回答を合わせると63%と半数を大きく超え、日本では50%となりました。

世界平均と比較して数字が低いとはいえ、過去18ヶ月の間に半数の経営層がサイバー攻撃の標的となった事実は決して安心できません。また、一度被害に遭うとサイバー犯罪者間で攻撃の詳細が共有され、同じ脆弱性を狙われるリスクが高まることも念頭に置いておく必要があります。

3、日本の経営幹部が狙われるサイバー攻撃、最も多いのは「マルウェア攻撃」

続いて、自社の経営幹部がサイバー攻撃を受けたことがあると答えた人に対して、具体的なサイバー攻撃の内容を質問しました。

経営幹部が標的となったサイバー攻撃の種類



出所: キャプテラ2024「経営層のサイバーセキュリティに関する調査」
Q:「過去18ヶ月間に、経営幹部はどのようなサイバー攻撃の標的になりましたか？」
・世界11カ国 n: 1,667
・日本　n:120
注) アンケート対象者のうち、自社の経営幹部がサイバーセキュリティの脅威の標的となったことがある、と回答したIT・セキュリティ担当者を対象に質問。複数回答のため、合計は100%にならない。回答数の多かった上位5項目のみを抜粋して掲載。

Q.「過去**18**ヶ月間に、経営幹部はどのようなサイバー攻撃の標的になりましたか？」
注）アンケート対象者のうち、自社の経営幹部がサイバーセキュリティの脅威の標的になった

ことがある、と回答したIT・セキュリティ担当者を対象に質問。複数回答のため、合計は100%
にならない。回答数の多かった上位5項目のみを抜粋して掲載。

マルウェア攻撃
日本（59%）、11カ国平均（49%）

ランサムウェア攻撃
日本（59%）、11カ国平均（49%）

フィッシング
日本（59%）、11カ国平均（49%）

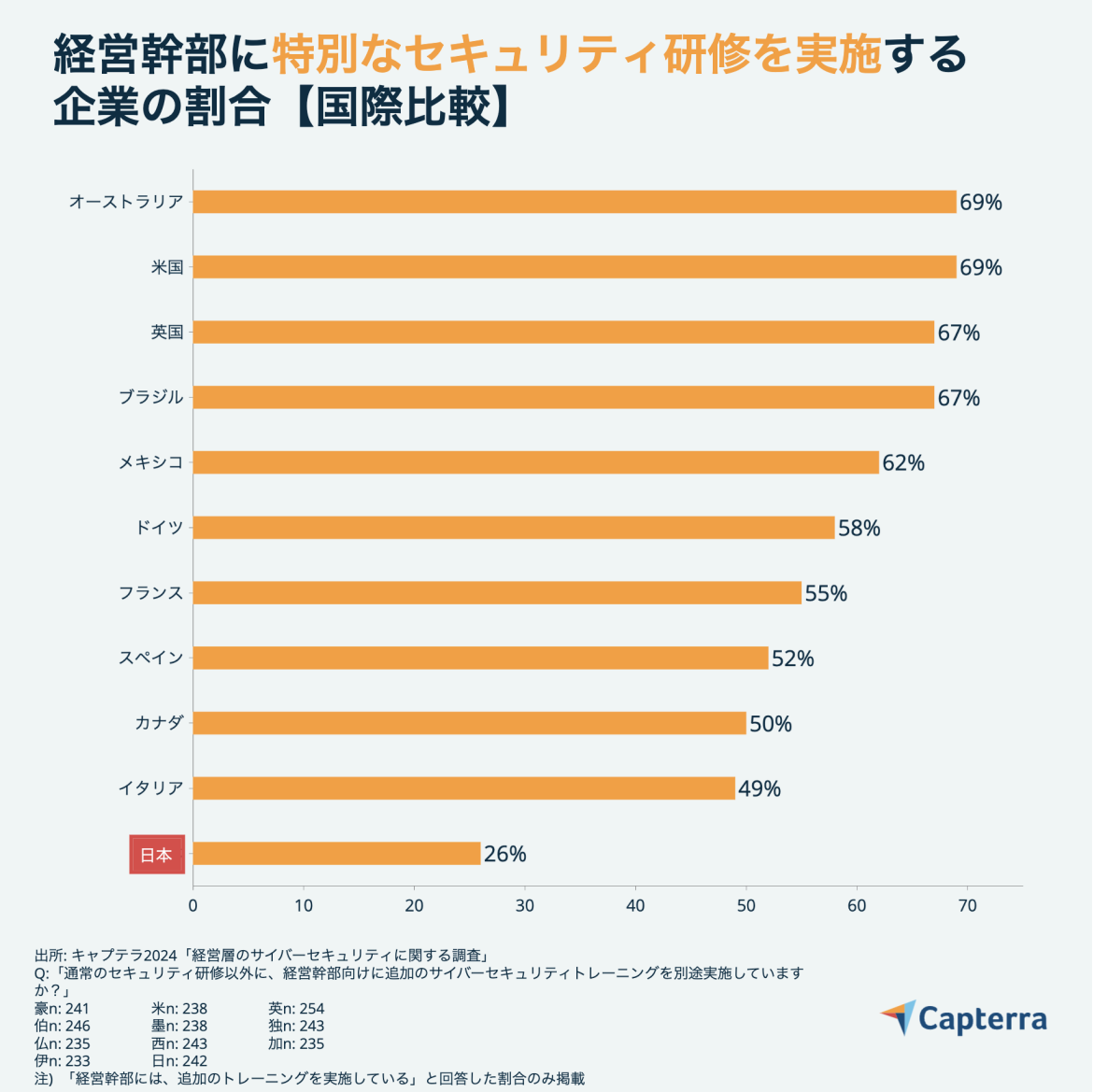
なりすまし
日本（59%）、11カ国平均（49%）

パスワード攻撃
日本（59%）、11カ国平均（49%）

日本の場合、最も多かった回答は「マルウェア攻撃」(59%) でした。次に多かったのが、企業の重要なデータやシステムを人質に取り、身代金を要求する「ランサムウェア攻撃」(50%)、そして詐欺メールや偽サイトを使って情報を盗む「フィッシング」(48%) の順となりました。このように、経営層を狙った攻撃は、企業の中枢機能や意思決定プロセスに対して深刻なリスクをもたらすことがわかります。

4、経営幹部に特別なセキュリティ研修を実施する企業の割合、日本は**26%**で最下位

一般社員よりも経営幹部の方がサイバー攻撃にあいやすいことが明らかになりましたが、日本を含む世界ではどのような対策を講じているのでしょうか。
経営幹部に対して、特別なセキュリティ研修を実施しているか質問しました。



Q.「通常のセキュリティ研修以外に、経営幹部向けに追加のサイバーセキュリティトレーニングを別途実施していますか？」
注)「経営幹部には、追加のトレーニングを実施している」と回答した割合のみ掲載

- オーストラリア（69%）
- 米国（69%）
- 英国（67%）
- ブラジル（67%）
- メキシコ（62%）
- ドイツ（58%）
- フランス（55%）
- スペイン（52%）

- カナダ（50%）
- イタリア（49%）
- 日本（26%）

日本の回答者で、経営陣に対して追加トレーニングが提供されていると答えたのは26%にとどまりました。これは今回同じ調査を行った11カ国の中で最下位であり、他国と比べて大きく遅れをとっていると言えます。

【まとめ】
今回の記事では、世界11カ国のIT・セキュリティ担当者に調査を行い、経営層が直面するサイバー攻撃の現状についてまとめました。

経営層がサイバー攻撃の標的となりやすいことが明らかになり、特に日本企業では経営層が複数回攻撃を受ける割合が多く、サイバーセキュリティ上の課題が浮き彫りになりました。さらに、経営層がサイバー攻撃の標的となりやすいことがわかっていながらも、日本では特別な経営層向けのサイバーセキュリティトレーニングが十分に行われていないことも明らかになりました。

経営層自身がまずそのセキュリティ意識を高めて、サイバー対策を講じる取り組みが求められると言えます。

♦キャプテラ「経営層のサイバーセキュリティに関する調査」:
経営層はサイバー攻撃に遭いやすい？IT担当者75%が指摘
https://www.capterra.jp/blog/6913/ai-in-project-management-efficiency
【最新IT市場の動向やマーケティングリサーチ調査一覧はこちら】

キャプテラの「経営層のサイバーセキュリティに関する調査」は2024年5月に回答者2,648名 (米国 (n=238), カナダ (n=235), ブラジル (n=246), メキシコ (n=238), 英国. (n=254), フランス (n=235), イタリア (n=233), ドイツ (n=243), スペイン (n=243), オーストラリア (n=241), 日本 (n=242)) に対してオンラインで実施されました。以下の条件に合致する方を対象としました。

- 組織の規模を問わず、自社のIT業務またはセキュリティ業務に携わっている
- 現在、会社でセキュリティソフトウェアを使用している
- 自社のサイバーセキュリティ対策に関わっている、または把握している

Capterra（キャプテラ）について

SaaS / ソフトウェア製品の無料比較プラットフォームのCapterra（キャプテラ）は、1999年の創業以来、多くの企業をサポートしてきました。900以上のカテゴリー、95,000以上のIT選択肢、95万件以上の検証済みレビューを元に、最適なSaaSを見つけて生産性を高め、更なるビジネスの成長にお役立てください。
詳しくは、当社ウェブサイト、またはX、YouTubeをご覧ください。

【本プレスリリースに関するお問い合わせ先】
キャプテラマーケティング・広報担当 塩入
kotoe.shioiri@gartner.com