KPMG

Cyber Security Survey 2026

KPMGジャパン

KPMG. Make the Difference.

2026年5月

Contents

はじめに

近年、デジタル技術の高度化やビジネス環境の変化に伴い、企業を取り巻くサイバーセキュリティリスクは、量・質ともに大きく変化しています。サイバー攻撃の巧妙化により、ひとたびインシデントが発生すると、長期間にわたる業務停止や甚大な経済的損失を引き起こすケースも増加しています。加えて、生成AIやAIエージェントといったAI技術の普及は、業務効率化や競争力強化といった大きな機会を生む一方で、新たなセキュリティリスクやガバナンス上の課題も顕在化させています。サイバーセキュリティはもはやIT部門だけの課題ではなく、AI活用を含めた企業活動全体を支える、重要な経営課題として認識されるようになっています。

このような状況を踏まえ、KPMGジャパンでは、日本企業におけるサイバーセキュリティの実態や課題を明らかにすることを目的として、「サイバーセキュリティサーベイ」を継続的に実施してまいりました。8回目となる本調査では、日本経済新聞社と共同で、サイバー攻撃の実態やセキュリティ管理態勢、具体的な対策状況に加え、子会社・委託先管理といった従来からの重要テーマ、AIの業務利用に伴うセキュリティ上の懸念や、適切な管理・活用に向けた取組み状況についても調査・分析を行いました。

本調査によって、過去1年間に発生したサイバーインシデントの年間合計被害額が10億円以上となったとの回答が今回初めて確認されるとともに、1億円以上の被害が発生したとの回答の割合も初めて1割を超えました。また、技術の進展スピードに対して、ルール整備やリスク管理が追いついていない実態も見受けられ、AI活用とセキュリティをどのように両立させていくかは、多くの企業に共通する課題であることが明らかになりました。

サイバーセキュリティに係る他社の取組み状況や課題認識を知ることは、自社の立ち位置を客観的に把握し、今後の方針を検討するうえで有益な示唆を与えてくれます。本調査結果が、サイバーセキュリティ対策の高度化や、AIを含むデジタル活用を安全に進めるための一助となることを願っております。

最後になりましたが、調査の実施にあたり、回答にご協力いただいた皆様に心から御礼申し上げます。

2026年5月

KPMGジャパン
サイバーセキュリティサーベイリーダー

KPMGコンサルティング株式会社
執行役員　パートナー

澤田 智輝

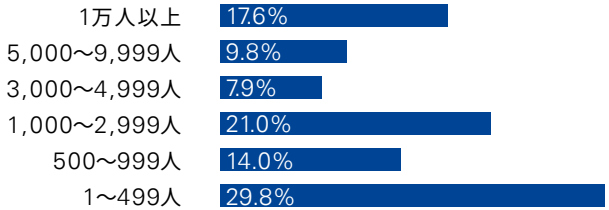
調査概要

サーベイの概要

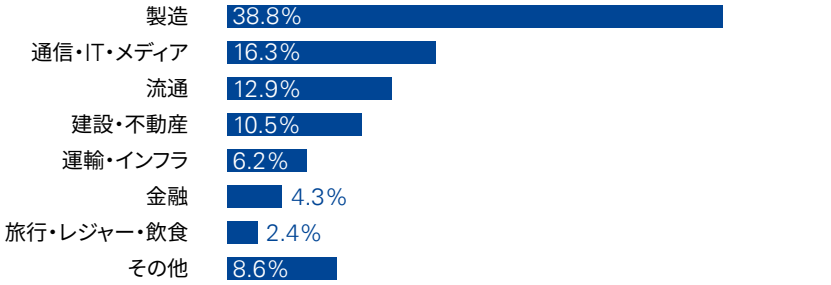
名称	サイバーセキュリティサーベイ2026
対象	国内上場企業の サイバーセキュリティ責任者・担当者
調査期間	2025年10月2日～11月28日
調査方法	メール／郵送によるアンケートの送付、 ウェブ／郵送によるアンケートの回収
発送数	4,035社
有効回答数	424社（回収率10.5%）

回答企業の属性

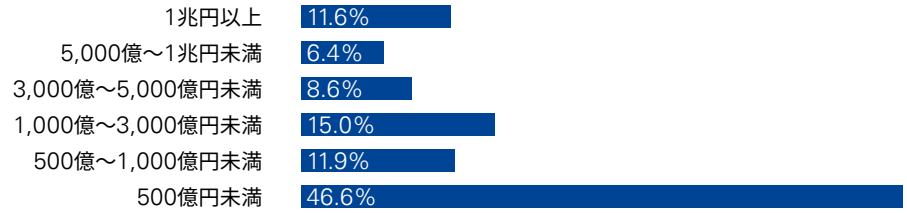
従業員数（連結）



業種



売上高（2024年度連結）



表記数値は小数点以下第2位を四捨五入しているため、パーセンテージ合計は100%とならない場合があります。

エグゼクティブサマリー

AIをはじめとした技術発展に伴いサイバーセキュリティリスクは一段と拡大し、
被害額の高額化が進むなど企業に与える影響は深刻さを増しています。
企業に対するリスクは新たな段階へ移行しており、
国内外子会社を含むサプライチェーン全体でセキュリティレベルを引き上げるためには、
予算の最適化や投資計画策定などの基本施策を改めて見直すことが重要なポイントとなります。

サイバー攻撃の巧妙化により、企業が被る被害は高額化・深刻化しており、今回の年次調査では初めて年間合計被害額が10億円以上となった企業が確認されました。被害は情報漏えいにとどまらず、システム停止による業務の遅延・中断など、事業継続に直接影響する事象へと広がっています。特に生成AIの普及を背景に、自然な日本語を用いたフィッシングやビジネスメール詐欺、ディープフェイクを用いた不正な送金指示といった新たな攻撃手法も確認されており、企業の事業継続リスクは一段と高まっています。

一方で、多くの企業ではサイバーセキュリティ予算や人材が十分に確保できておらず、中期的なセキュリティ計画や推進体制の整備も遅れがみられます。投資判断はインシデント発生後の事後対応型に偏りがちで、計画・予算・人材を一体として整備できていない企業も少なくありません。高度化する脅威に対応するためには、短期的な対応にとどまらない、持続的な管理態勢の構築が求められています。

また、子会社や委託先・取引先を含むサプライチェーン全体でのセキュリティ管理は不十分であり、特に海外子会社や国内の委託先を起点としたサイバーインシデントが多く確認されています。管理基準やセキュリティレベルのばらつき、監査やモニタリングの不十分さがリスクを高めており、グループ全体・サプライチェーン全体を見据えた統合的なリスク管理の必要性が高まっています。

さらに、AIは業務効率化を中心に急速に導入が進む一方で、セキュリティ目的での活用やガバナンス整備は後追いとなっています。評価・監査・レビューの仕組みやシャドーAI対策も十分とは言えず、AI活用の拡大が新たなリスクを生む可能性もあります。今後は、AI活用を含め、技術対策・運用・人材・統制を統合的に捉え、全社・グループ横断でサイバーリスクに対応していくことが重要な経営課題となっています。

各章のサマリー

01 サイバー攻撃の実態

8回目となる年次調査で初めて、サイバーインシデントによる年間合計被害額が10億円以上となった企業が確認され、被害の高額化が進んでいることが明らかになりました。サイバー攻撃の巧妙化に伴い、被害は情報漏えいにとどまらず、システム停止による業務の遅延・中断といった事業影響にも広がっています。特に、生成AIを悪用したフィッシングやビジネスメール詐欺など、自然な日本語を用いた攻撃が増加しており、ディープフェイクを用いた不正な送金指示といった新たな攻撃手法も確認されました。こうした状況を踏まえ、技術的対策に加え、社員教育を含む対策の徹底と実効性の向上が引き続き求められます。

02 サイバーセキュリティ管理態勢

サイバーセキュリティ予算は依然として不足感が強いものの、IT予算に占める投資比率は上昇しており、重要性の認識は高まりつつあります。一方で、投資判断はインシデント発生後の事後対応型に偏りがちで、中期的なセキュリティ計画が未整備な企業も多くみられます。また、サイバーセキュリティ推進組織については人材不足が深刻化しており、組織自体を設置していない企業も約4割にのぼっています。高度化するサイバー攻撃に対応するためには、計画・予算・人材を一体として整備していくことが引き続き重要な課題となっています。

03 子会社管理

国内子会社については約4割の企業で本社主導のサイバーセキュリティ管理が行われているものの、企業規模が小さくなるほど子会社任せとなる傾向がみられます。海外子会社では管理の分散・委任がさらに進んでおり、評価・教育・訓練といった対応の遅れが顕著です。加えて、グローバルでの人材不足を背景に、海外子会社に対策を一任することはリスクを高めており、実際に海外拠点を起点とした被害も多く確認されています。海外拠点リスクが高まるなか、国内外の子会社を含めたグループ横断でのセキュリティ対策の企画・推進が重要な課題となっています。

04 委託先・取引先管理

委託先・取引先に対するサイバーセキュリティ管理は全体的に遅れており、基本となるセキュリティ指針の整備や選定時の対策確認でさえ十分に実施されていない企業が多くみられます。特に製造業をはじめとする非金融業では、多層的なサプライチェーンのなかで委託先管理が行き届かず、情報漏えいや業務停止リスクが高まりやすい状況にあります。また、委託先の対策状況を継続的にモニタリングする仕組みも十分に整備されていません。今後は、委託先のリスクに応じたセキュリティ管理とモニタリング体制の強化が重要な課題となっています。

05 サイバーセキュリティ対策

多くの企業でサイバーセキュリティ対策ツールは不足しており、その背景には予算不足があることが明らかになりました。また、資産管理やID／アクセス管理、脆弱性管理などの対策は導入が進む一方で、運用定着に課題を抱える企業が多く、十分な効果を発揮できていない状況がみられます。さらに、インターネットに公開されているシステムであっても緊急度の高いパッチが迅速に適用されていないケースが多く、日常的な運用プロセスや管理体制の不十分さがセキュリティリスクを高める要因となっています。

06 AIセキュリティ

AIは業務効率化・自動化を中心に導入が進み、さまざまな活用が企業活動のなかに広く浸透してきています。一方で、セキュリティ目的でのAI活用は限定的にとどまっており、リスク検知や防御強化といった分野はこれからの導入が見込まれます。また、AI利用に対する評価・監査・レビューといったガバナンスが十分に整備されておらず、全社的な統制が追いついていないケースが少なくありません。さらに、シャドーAI対策についてもポリシー整備にとどまる企業が多く、教育や技術的制御を含めた実効性の確保が課題となっています。

01 サイバー攻撃の実態

01

本章の概要

サイバーインシデントによる被害金額は年々増加するとともに、生成AI・ディープフェイクを用いた新たな攻撃による被害も発生している。また、DXの進展により、サプライチェーン経由での業務停止リスクも拡大している

サイバーインシデントによる被害金額は増加。情報の漏えいだけでなく、業務の遅延・中断による被害も発生している

8回目となる今回の調査で初めて、年間の合計被害額が10億円以上となった企業が確認されるとともに、1億円以上の合計被害額となった割合は毎年増加しており、今回の調査では1割を超えました。
また、被害総額は売上規模が大きい企業ほど増加する傾向がみられました。加えて、サイバーセキュリティ推進組織の人員過不足状況別に分析すると、人員不足が深刻になるほど被害額が大きくなる相関が確認されました。
発生したサイバーインシデントで被った被害については、個人情報や機密情報の漏えいだけでなく、システム停止による業務中断を経験した企業が2割を超えました。

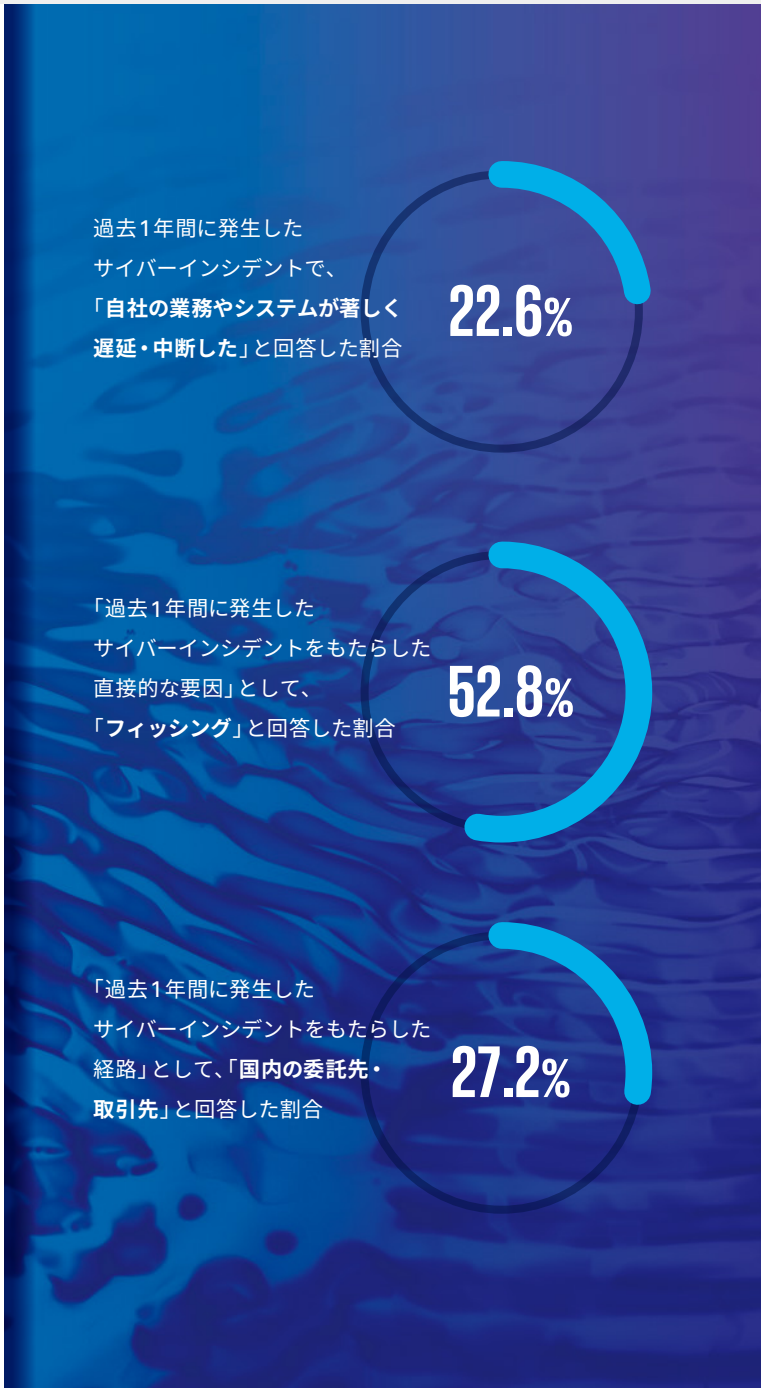
業務上の被害をもたらした攻撃はランサムウェアが最多。AIを用いたサイバー攻撃の高度化もみられる

前回調査に引き続き、業務上の被害があった攻撃手法としては、「ランサムウェア」が最多となりました。また、今回の調査で初めて設問に加えた「ディープフェイクを用いた不正な送金指示」も被害が発生していることが確認されました。

検知した攻撃としては「フィッシング」「メールを用いた不正な送金指示」が抜きんでており、およそ半数の企業が経験しています。生成AIの進展により、日本語としてきわめて自然な文章を用いたフィッシングやビジネスメール詐欺が増加しており、従来の「不自然な日本語」による見分けが困難になってきています。これにより、技術的対策だけでなく、社員教育の重要性が一層高まっています。

サイバーインシデントの発生経路は、国内の委託先・取引先が最も多い。「攻撃があったかわからない」との回答も多い

過去1年間に発生したサイバーインシデントについて、「攻撃があり業務上の被害があった」経路としては、最も回答が多かったのは、「国内の委託先・取引先」でした。
また、「攻撃があったかわからない」との回答は、「海外の委託先・取引先」が最も高く、「国内の委託先・取引先」が続いています。
DXの進展により、委託先・取引先とネットワークを接続するケースが増加している一方で、自社から見えにくい領域のリスク管理が十分でない可能性があります。
自社の情報や業務継続を保護するために、契約時にサイバーインシデントの報告を義務付けたり、委託する業務などに応じてアセスメントや監査を行うなど、委託先・取引先でのサイバーセキュリティの取組みをモニタリングする仕組みを導入することも重要となっています。



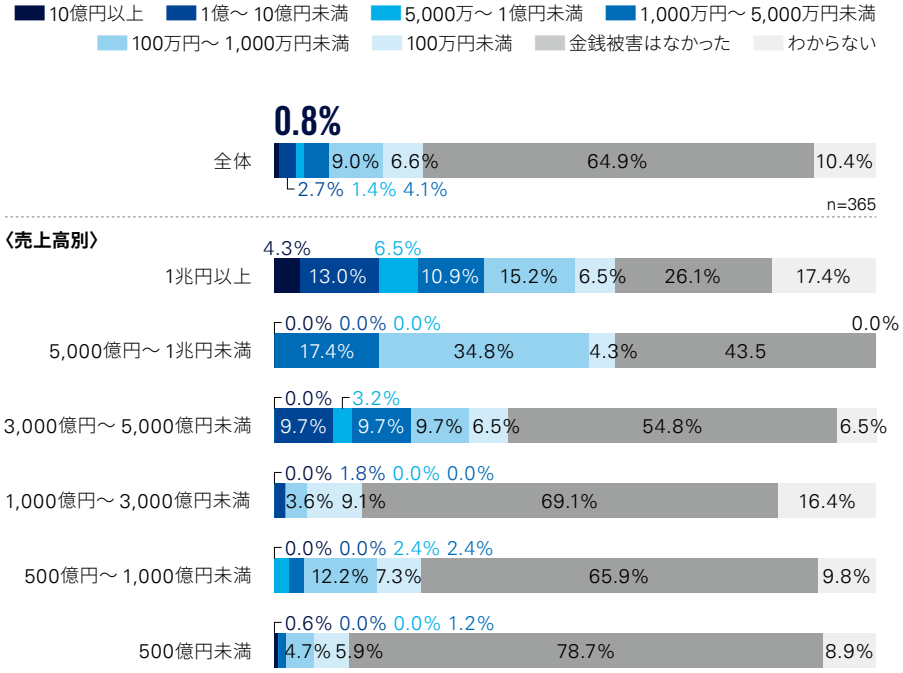
サイバーインシデントによる被害金額

回答企業の2割強において、過去1年間に金銭的被害を被るサイバーインシデントが発生していたことがわかりました。また、8回目となる今回の調査で初めて、過去1年間に発生したサイバーインシデントの合計被害額が10億円以上となったとの回答を得ました。ランサムウェアを代表とする金銭目的のサイバー攻撃では、身代金の金額を上げるため、企業ネットワークの隅々まで侵入し、事業運営に不可欠な情報やシステムを暗号化することを狙っています。

こういった攻撃にあうと、機密情報の漏えいだけでなく、事業活動の停止を招き、被害金額も高額になってしまうおそれがあります。また、売上高別にみると、合計被害額は売上規模に比例して大きくなっている傾向がみられました。
過去の調査結果と比較すると、年間被害金額が1億円以上を超えたとの回答割合が毎回増えており、今回の調査では1割を超えました。

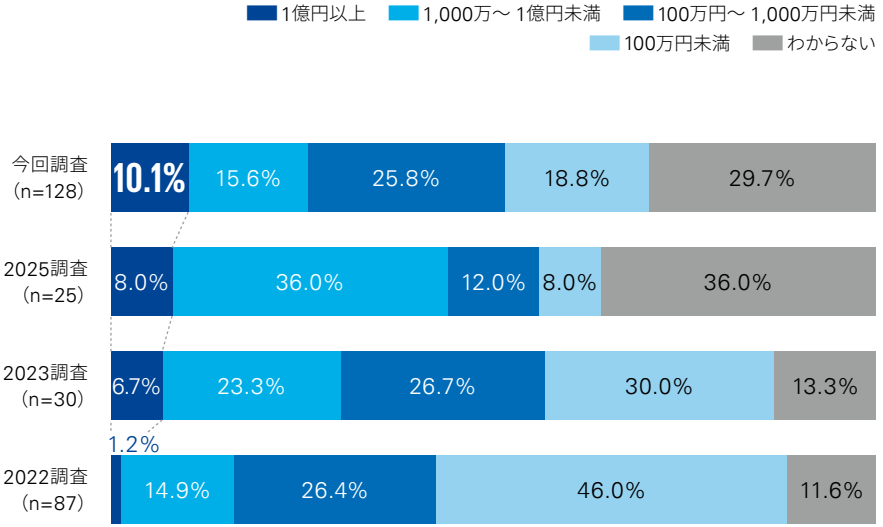
年間10億円以上の被害が発生

過去1年間に発生したサイバーインシデントで、どのくらいの合計損失がありましたか。



1億円以上の合計被害額となった割合は毎年増加し、1割を超えた

左記より「金銭的被害はなかった」を除き、発生した被害金額を過去の調査結果と比較



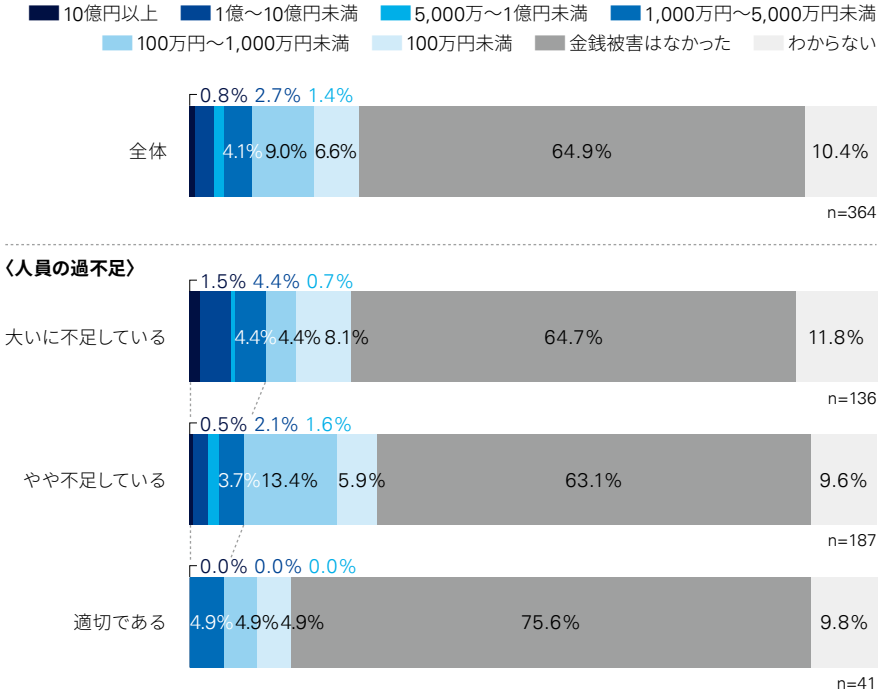
サイバーインシデントによって発生した被害

サイバーセキュリティ推進組織における人員の過不足に係る質問（P.20）との相関をみると、人員規模が「適切である」→「やや不足している」→「大いに不足している」と不足状況が厳しくなるにしたがって、被害金額が高くなっている傾向がみられました。セキュリティ推進組織の人員が不足することで検討・推進力が不足し、対策が十分に実装されておらず、被害が拡大しているおそれがあります。

サイバーインシデントによって業務やシステムが遅延・中断し、ひいては顧客や取引先に経済的な損失を発生させるサプライチェーンリスクが問題となっています。今回の調査においても、サイバーインシデントによって、個人情報漏えいだけでなく、サプライチェーンへの被害が発生している様子がみられました。

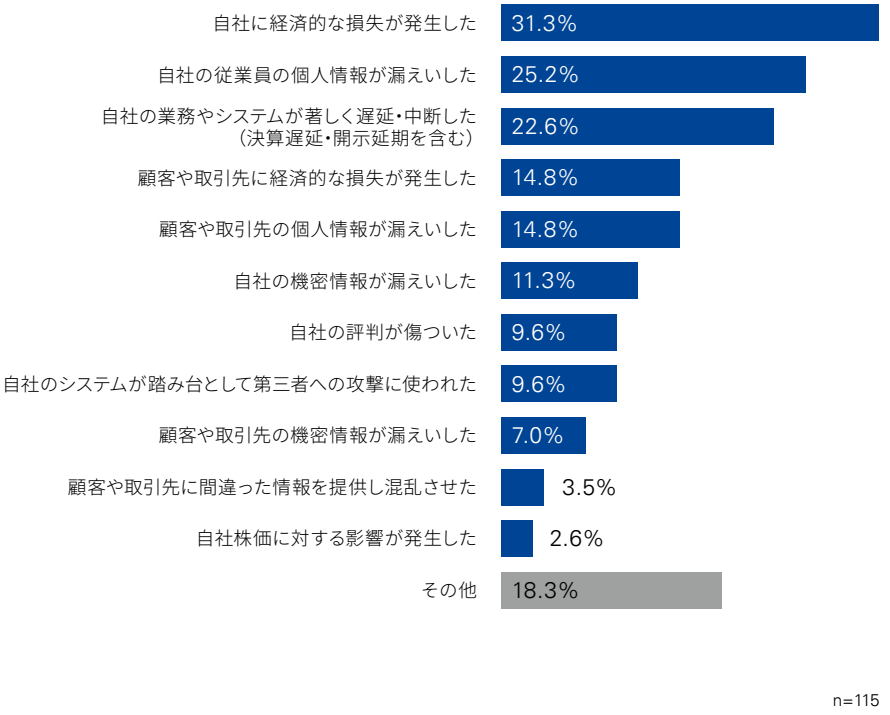
人員の過不足と被害額の相関

前項の合計被害額と、人員の過不足状況の質問（P.20）とのクロス分析（「金銭的被害はなかった」、人員が「やや過剰である」との回答を除く）



自社の業務遅延・中断や取引先への経済的な損失が発生

過去1年間に発生したサイバーインシデントで、どのような被害が発生しましたか。



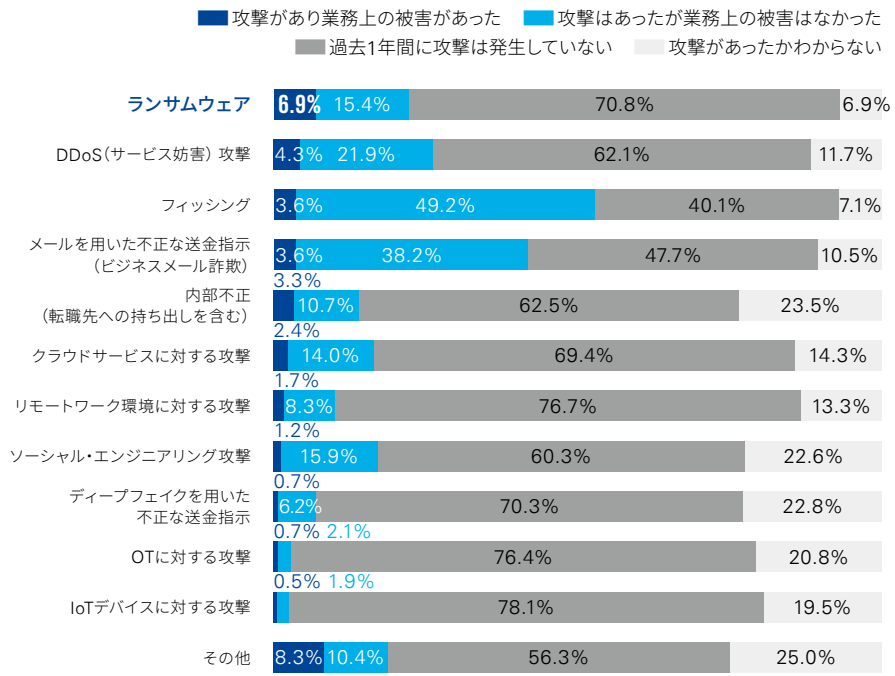
サイバーインシデントの発生要因（攻撃手法／攻撃対象）

業務上の被害があったサイバー攻撃は、前回調査と同様に「ランサムウェア」が6.9%と最も多くなりました。また、今回の調査では、「ディープフェイクを用いた不正な送金指示」に係る攻撃の有無を確認したところ、「攻撃があり業務上の被害があった」との回答が0.7%、「攻撃があったが業務上の被害はなかった」との回答が6.2%となりました。 AIの活用による攻撃の巧妙化が進んでいる様子がうかがえます。

生成AIを用いてより自然な日本語による攻撃が行われるようになってきています。「フィッシング」など生成AIを用いる可能性の高い攻撃について前回調査と比較したところ、いずれも前回よりも攻撃が増えている傾向がみられました。日本語の不自然さだけでは攻撃を見分けることが難しくなってきており、従業員等に対して、より一層の教育や注意喚起が必要となっています。

昨年に引き続き、ランサムウェアによる被害が最も多い

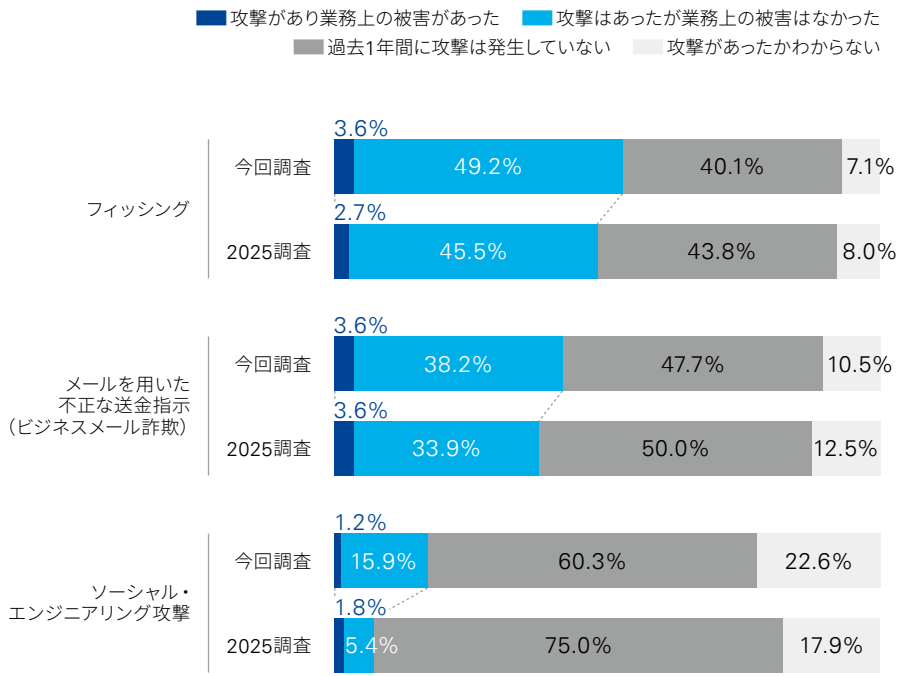
過去1年間に発生したサイバーインシデントをもたらした直接的な要因（攻撃手法および攻撃対象）と事業上の被害の有無についてご回答ください。



n=421

生成AIを用いた攻撃の巧妙化

生成AIによる日本語力向上に関連する攻撃の被害有無について、前回調査と比較



2025年 n=112、2026年 n=421

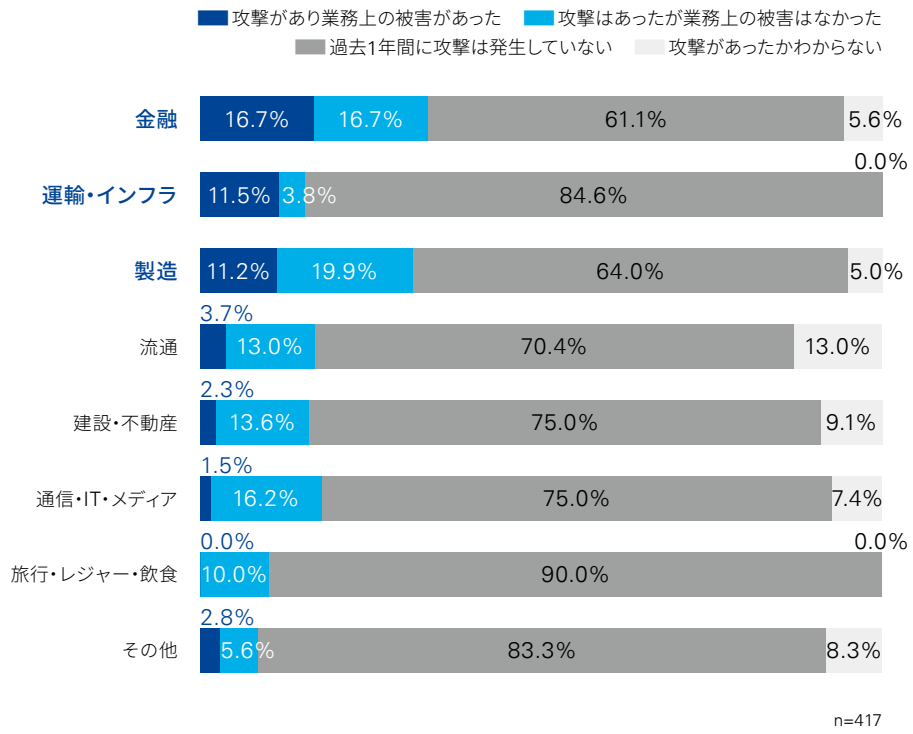
サイバーインシデントの発生要因（業界別分析）

過去1年間に発生したランサムウェア攻撃による事業上の被害の有無について、業界別に分析すると、「金融」「運輸・インフラ」「製造」で被害が多くなりました。ランサムウェアによってデータが暗号化されてしまうと、システムが使用不可となり長期の業務停止を招くおそれがあります。適切なデータバックアップに加え、セキュリティパッチ、アクセス権限の強化などの事前対策、発生時の対応計画（BCP）の整備を行う必要があります。

また、転職先へのデータ持ち出しなど内部不正について確認したところ、「運輸・インフラ」での被害発生率が高いことがわかりました。加えて、全業界を通して「攻撃があったかわからない」との回答が多くみられ、内部からの情報持ち出しにかかる制限や監視について対策が十分に施されていない可能性があります。

ランサムウェアは「金融」「運輸・インフラ」「製造」での被害が多い

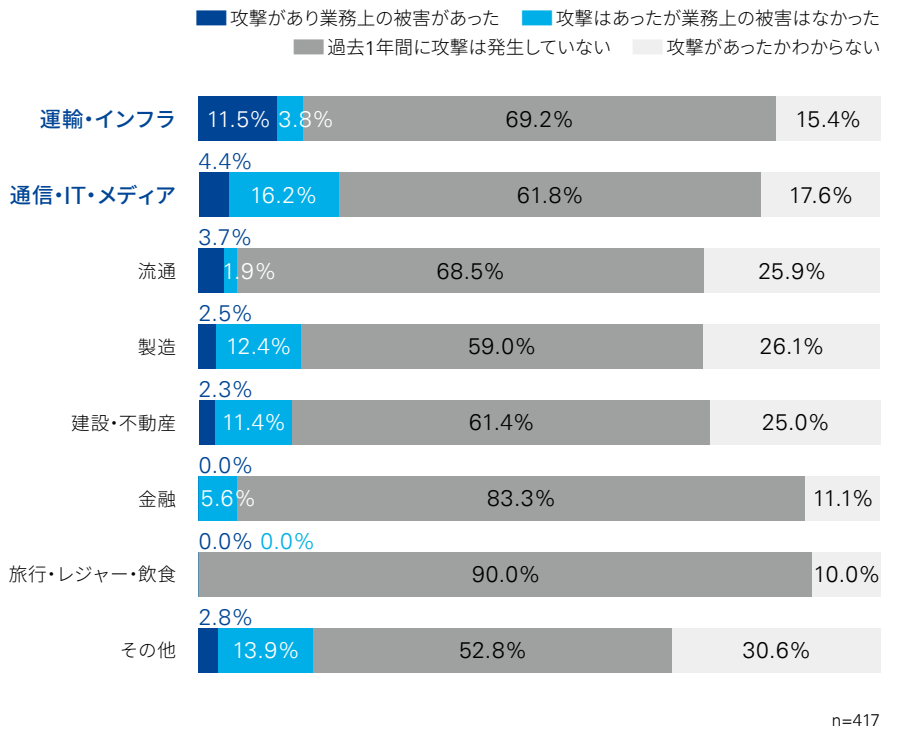
過去1年間に発生したランサムウェア攻撃による事業上の被害の有無について、業界別に分析



n=417

内部不正は、「運輸・インフラ」「通信・IT・メディア」での被害が多い

過去1年間に発生した内部不正（転職先への持ち出しを含む）による事業上の被害の有無について、業界別に分析



n=417

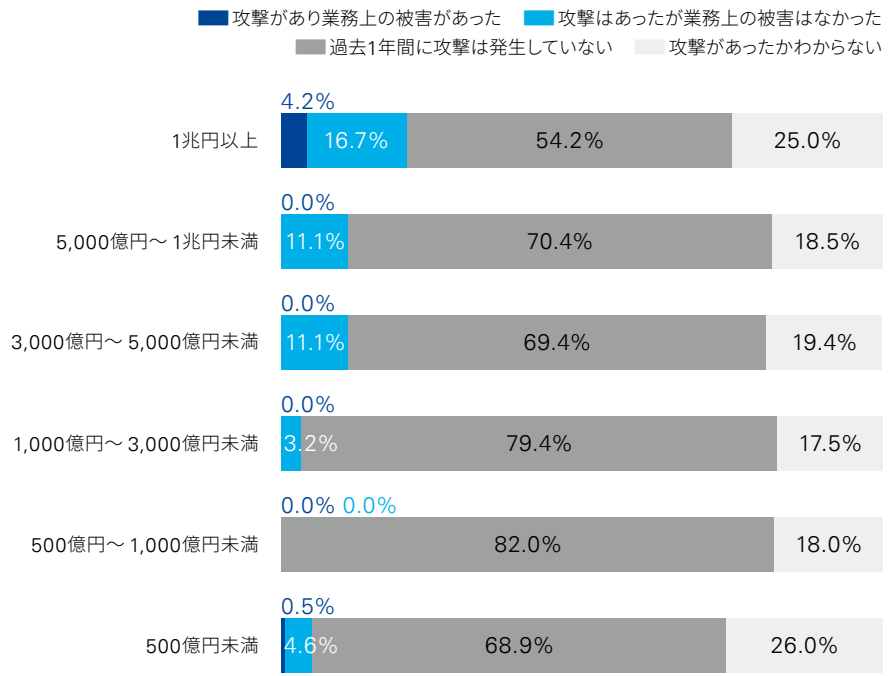
ディープフェイクによる被害とサイバーインシデントの発生経路

今回の調査で初めて、「ディープフェイクを用いた不正な送金指示」に係る攻撃の有無を確認しました。回答結果を売上規模とのクロス集計を行ったところ、売上規模が大きくなるほど攻撃が多くなる傾向がみられました。その他の攻撃と比較しディープフェイクによる攻撃は、標的組織の分析や動画の準備など手間のかかる攻撃となっており、売上規模の大きい組織が狙われやすい傾向がみられました。

サイバーインシデントをもたらした経路別にみると、「攻撃があり業務上の被害があった」が最も高くなったのは、「国内の委託先・取引先」経由の攻撃でした。DXの進展に伴い、サプライチェーンや委託先とネットワークをつなぐケースが増えていますが、さらなる対策が不可欠となっています。特に、委託先・取引先に対しての攻撃については、「わからない」が国内で3割弱、海外で4割弱程度となっており、契約に報告義務を盛り込むことも検討すべきです。

ディープフェイクによる攻撃が広がりつつあり、日本企業でも被害が発生

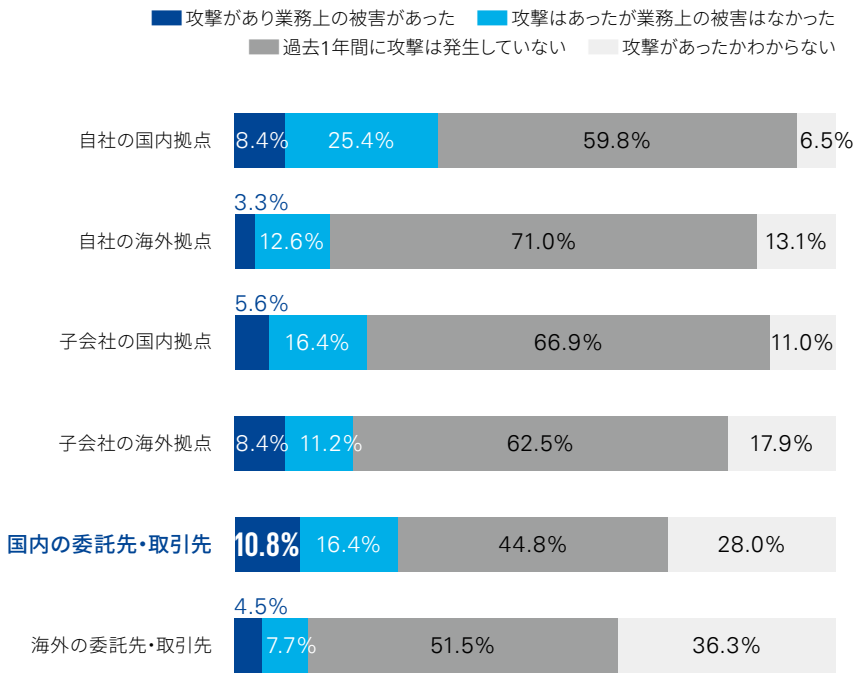
過去1年間に発生した「ディープフェイクを用いた不正な送金指示」による事業上の被害の有無について、売上規模別に分析



n=420

国内の委託先・取引先からのサイバーインシデント被害が多い

過去1年間に発生したサイバーインシデントをもたらした経路と事業上の被害の有無についてご回答ください。



n=418

攻撃者のAI活用により、「言語の壁」は崩れ去ってしまいました。

AI活用によりさらに巧妙化したサイバー攻撃という脅威に対し、私たちはすべてのセキュリティドメインにおいて最善を尽くし、組織全体の対応能力を向上させることが急務となっています。

楽天グループ株式会社
上級執行役員　**福本 佳成**

効果的といわれている技術的対策を講じたつもりでいても、その導入の範囲、各種設定、他製品との組合せ等の考慮漏れで、有効に機能していない事象が散見されます。

ソリューションは導入して終わりではなく、定期的な評価・見直しをする運用設計にすることが肝要です。

株式会社KPMG Forensic & Risk Advisory
執行役員　パートナー　**上原 豊史**

コラム｜ますます巧妙化するサイバー攻撃

技術的な対策だけでは不十分。運用面の強化も合わせた対策が不可欠

多要素認証（MFA）導入企業で発生した事例

ある企業において、取引先から「担当者を装った不審なメールが届いた」との連絡がありました。電子メールの件名や本文を確認したところ、実際の本人のやり取りと酷似しており、一見すると違和感の少ない内容でした。当該企業では、クラウド型メール環境においてMFA（IDとパスワードに加え、登録した端末を認証に利用する方式）を導入していましたが、調査の結果、攻撃者がフィッシングメールや偽装サイトを通じてID・パスワードに加え、認証後のセッション情報（セッションクッキー）を窃取し、不正アクセスが行われた可能性が高いことが示されました。その後、攻撃者は自身の端末をMFA用端末として登録する設定変更を行い、不正アクセスが継続可能な状態となったことが確認されました。さらに、メールボックス内の情報が継続的に閲覧され、それを基に偽装メールが作成されていたとみられる形跡が確認されました。本事例は、認証対策が導入されている環境であっても、認証後のセッションや設定変更が適切に統制されていない場合、不正利用が発生し得ることを示唆しています。

技術的対策の導入は十分条件ではない

MFAは、IDとパスワードのみの認証方式と比較して、安全性を高める重要なセキュリティ対策です。しかし本事例が示唆するのは、このような技術的対策の導入のみでは、攻撃リスクを完全に排除することは難しいという点です。

不正アクセスが発生する可能性を前提に、日頃からアクセス状況や設定変更などを継続的にモニタリングしていれば、本事案のような異常な挙動をより早期に検知し、その後の偽装メール送信といった被害拡大を抑止できた可能性も考えられます。

また、不正アクセスの端緒となったフィッシングメールへの対応についても、個人の注意力に依存するのではなく、組織として継続的な教育・訓練や注意喚起を実施し、リスク感度を高めていくことが重要です。

技術的対策の導入のみでは、経営リスクを十分に抑制できるとは限りません。導入後の運用、監視、教育といった統制活動とあわせて初めて、その効果が発揮されるものと言えます。

求められる対応とは？

結論として、技術的強化は重要であるものの、それだけで十分とは言い切れない状況にあると言えます。本調査でも、委託先・取引先経由でのインシデント発生や、「攻撃があったかわからない」との回答が一定程度存在していることが示されています。こうした状況を踏まえると、監視態勢の強化はリスク軽減に重要な役割を担うと考えられます。具体的には、以下のような取組みが考えられます。

- 技術的な認証対策の継続的な見直し
- 利用状況やアクセス状況のモニタリング強化
- 従業員への継続的な注意喚起・教育の徹底
- 委託先・取引先を含めた管理レベル向上

これらを継続的かつ計画的に進めていくことが求められます。

サイバー攻撃の巧妙化が進むなか、技術的対策と運用面の強化を両立させることが、被害の抑止および最小化につながると考えられます。認証対策の「導入済み」という状態にとどまらず、認証後の統制と運用成熟度を継続的に点検していくことが、企業価値の保全において重要な課題となっています。

02 サイバーセキュリティ管理態勢

02

本章の概要

サイバーセキュリティ予算、サイバーセキュリティ人材は引き続き不足している。特に、予算が不足している企業ほど中期的な計画が策定されていない。また、約4割の企業ではサイバーセキュリティ推進組織が設置されていない

サイバーセキュリティ予算は引き続き不足しているが、IT予算に占める比率は上昇している

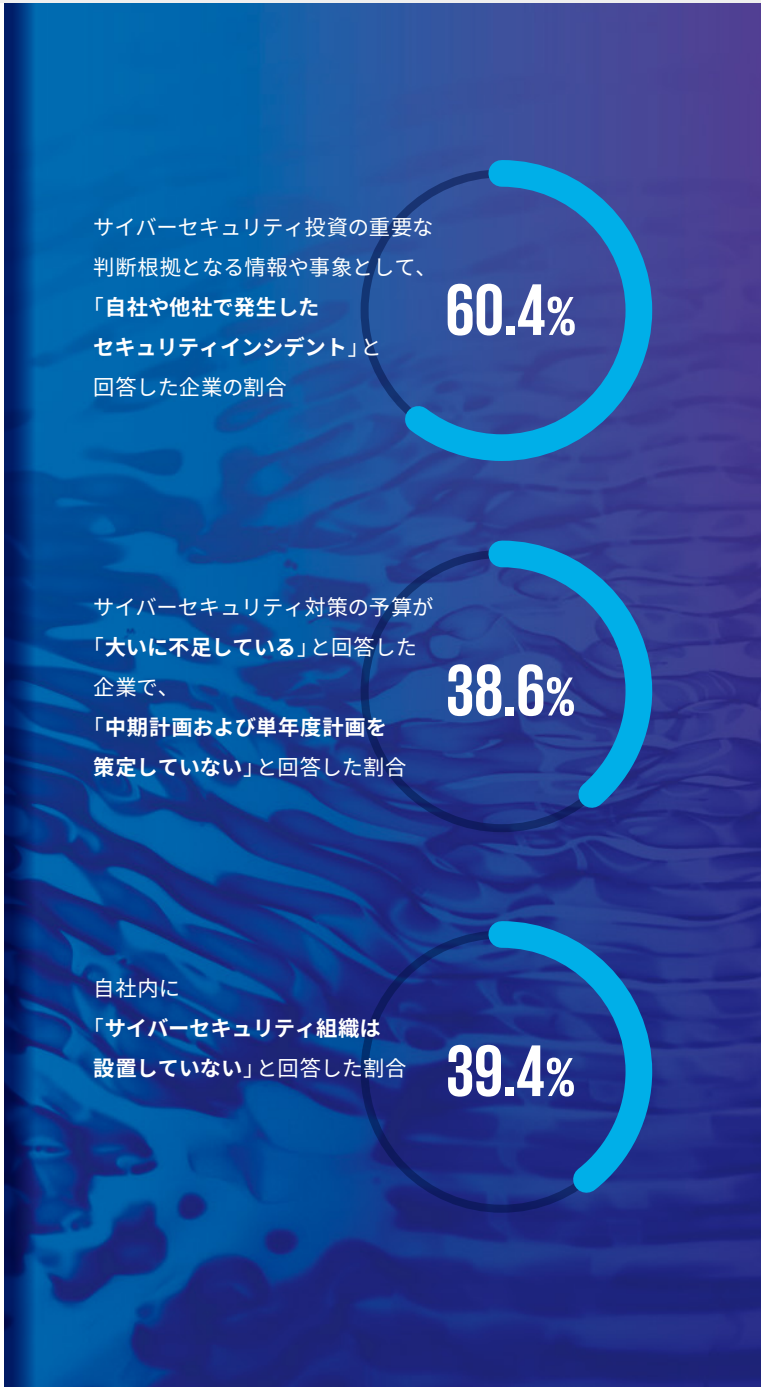
サイバーセキュリティ予算について、「大いに不足している」「やや不足している」と回答した企業は63.2%に達し、前回調査と同程度の水準で推移しており、多くの企業が十分な予算を確保できていない状況がみられました。
予算判断の主な根拠は、自社・他社で発生したセキュリティインシデントや監査・アセスメントでの指摘事項であり、インシデント発生後に投資判断を行う「事後対応型」の傾向が強くみられ、AIや量子暗号などの新技術への対応は後追いになりがちな傾向がみられました。
IT予算に占めるサイバーセキュリティ投資の割合は増加傾向にあり、約4割の企業がIT予算の5%以上をセキュリティに投資しています。これは前回調査から大きく伸長している傾向がみられました。

中期的なサイバーセキュリティ計画は依然として未整備。予算が不足している企業ほど計画が策定されていない

サイバーセキュリティの中期計画を策定していない企業は44.4%にのぼり、前回調査からは減少したものの、依然として高い水準にとどまっています。特に従業員規模が小さい企業ほど、中期・単年度計画を定期的に策定できていない傾向が顕著となっています。
また、予算が不足している企業ほど計画策定が不十分となっており、「計画がないために予算を確保できない」「予算がないために計画を立てられない」という悪循環となっている可能性があります。

サイバーセキュリティ推進組織は、9割弱の企業で人員不足。約4割の企業では組織自体が設置されていない

サイバーセキュリティ推進組織の人員について、「大いに不足している」「やや不足している」との回答は89.1%に達し、前回調査（75.5%）から不足感がさらに高まっていることがわかりました。特に「大いに不足している」との回答割合も増加しており、人材不足は一層深刻化している傾向がみられます。
また、サイバーセキュリティ推進組織の人員数は、組織規模に応じて増加する傾向がみられるものの、「組織を設置していない」との回答が最も多く、約4割の企業では推進組織が設置されていないことが明らかになりました。特に、従業員数3,000人未満の企業では約半数が未設置という結果となっています。
高度化・巧妙化するサイバー攻撃に適切に対応していくためには、専門的な知識・経験を有する人材によるセキュリティの企画・推進が不可欠であり、サイバーセキュリティ推進組織の重要性は今後さらに高まると考えられます。



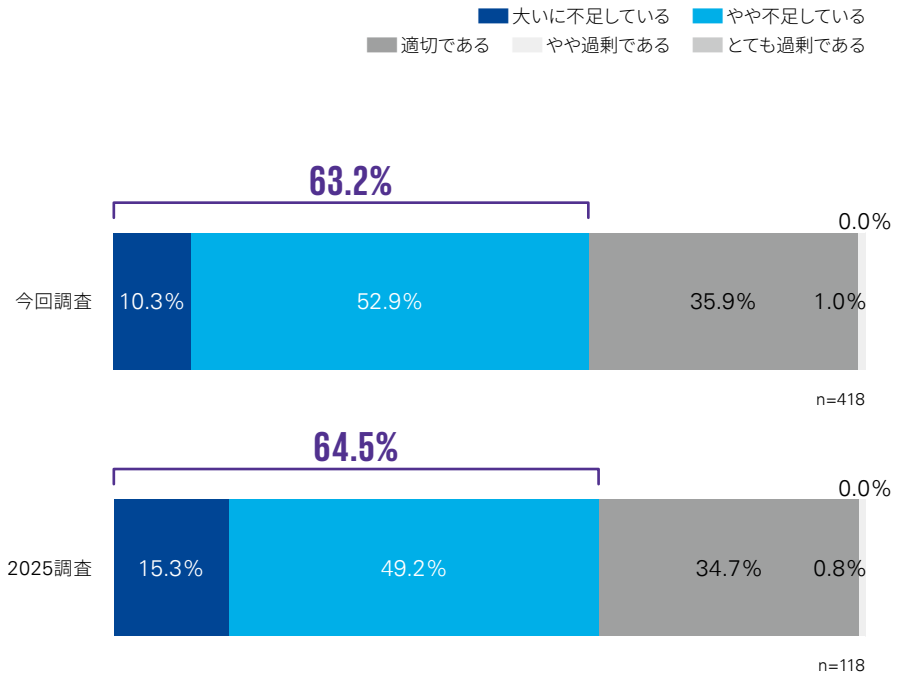
サイバーセキュリティ予算の状況

サイバーセキュリティ予算が「大いに不足している」「やや不足している」との回答の合計は63.2%となり、前回調査と同程度となりました。「大いに不足している」との回答割合は前回と比較し、若干改善がみられますが、大きな進展はなく、多くの企業が引き続きサイバーセキュリティの予算が十分ではないと認識しています。

サイバーセキュリティ予算に影響を与える事象としては「自社や他社で発生したセキュリティインシデント」が「重要な判断根拠となる」との回答が60.4%と最も多く、インシデントを起点とした対策立案が行われている様子がうかがえます。一方で、「AIや量子暗号等、新たな技術の動向」は「情報として留意する」との回答が最も多く、新技術への対応は後追いになりがちな傾向がみられます。

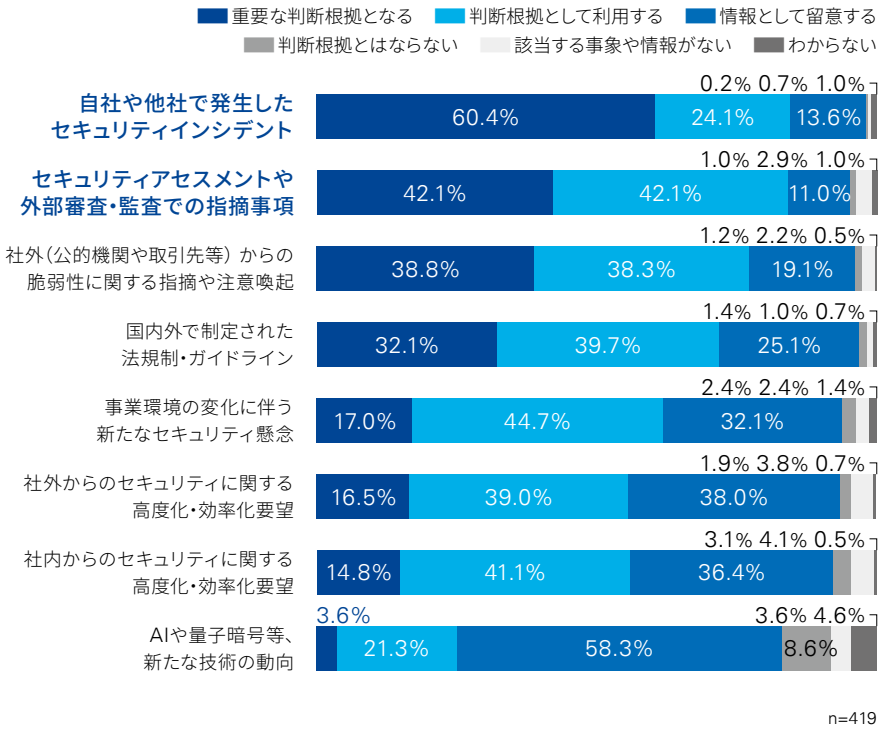
6割強の企業でサイバーセキュリティ予算が不足

貴社のサイバーセキュリティ対策への予算額は、適切だと思いますか。



サイバーセキュリティ予算の判断根拠は、セキュリティインシデントや監査指摘事項

サイバーセキュリティ投資に影響を与える事象や情報として、以下はどの程度重視しますか。



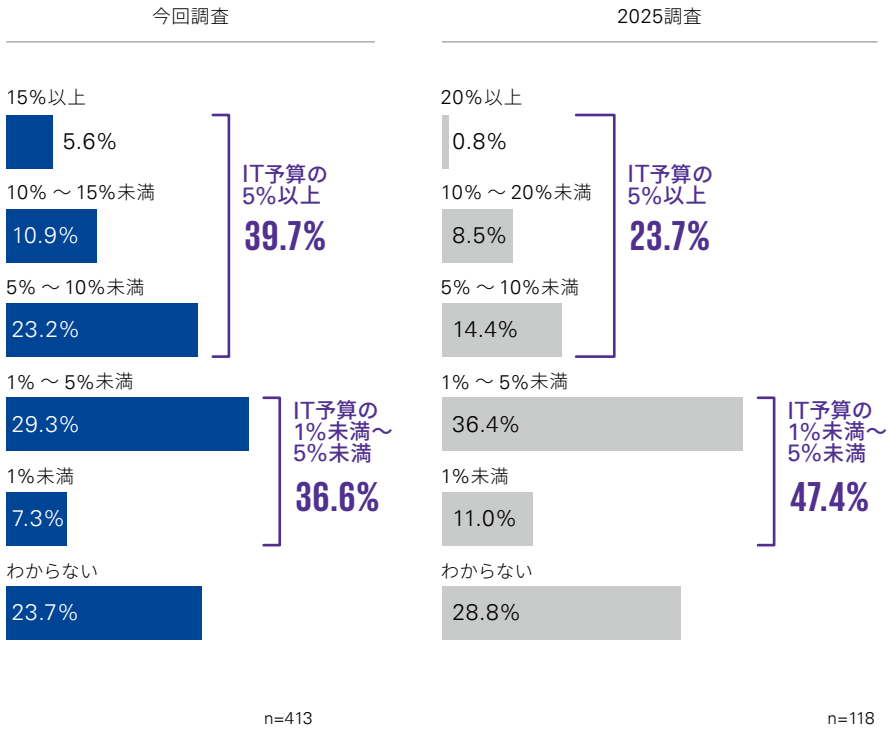
IT投資に対するサイバーセキュリティ投資の比率

IT予算に占めるサイバーセキュリティ予算の割合について前回調査とは若干選択肢を変更しました。1%未満～5%未満の回答割合は、前回調査の47.4%から36.6%と減少した一方、5%以上の回答割合は、前回調査の23.7%から39.7%と増加しており、回答企業の約4割はIT予算の5%以上をサイバーセキュリティ予算としていることがわかりました。

特に、IT予算の5%以上をサイバーセキュリティ予算としている回答の割合が高いのは、「製造」「流通」「金融」となりました。一方で、「旅行・レジャー・飲食」では「1%未満」の割合が他の業種に比べ最も高くなっています。

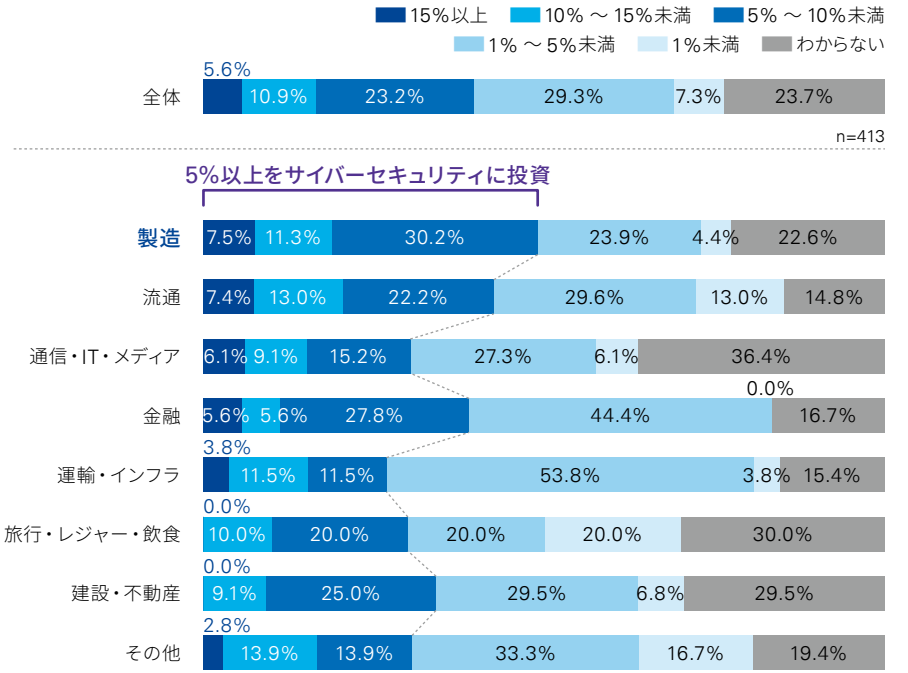
IT予算に占めるサイバーセキュリティ予算は増額傾向

貴社におけるサイバーセキュリティ投資（予算額）はIT投資に対し何%ですか。



IT投資に対してサイバーセキュリティ投資が高いのは「製造」

左記のサイバーセキュリティ投資のIT投資比率を業種別に分析



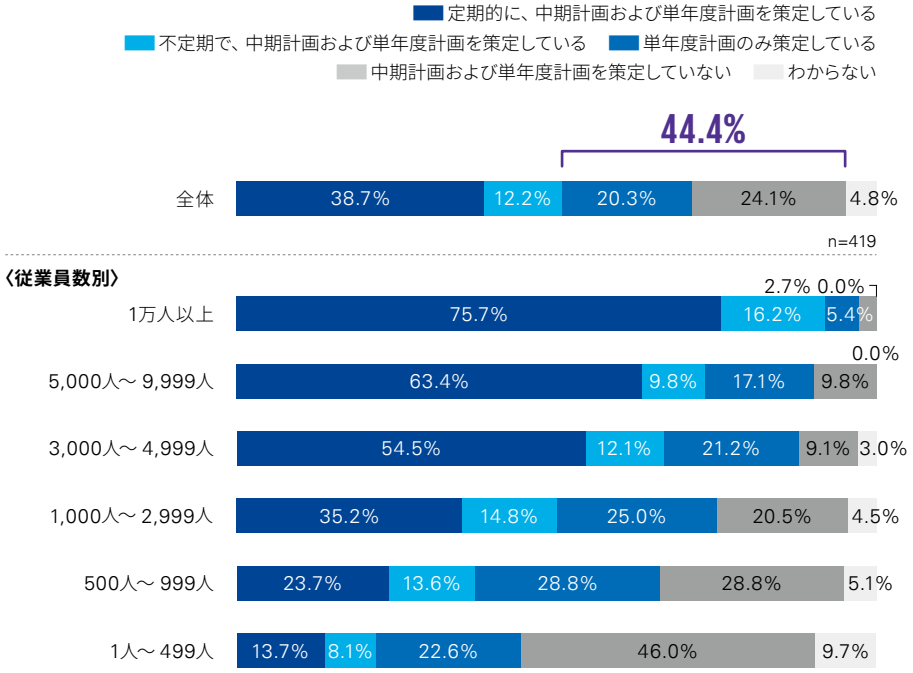
サイバーセキュリティの中期計画、単年度計画

従業員規模が大きくなるほど「定期的に、中期計画および単年度計画を策定している」と回答した企業の割合が増える傾向がみられました。サイバーセキュリティの中期計画を策定していない割合は前回調査（49.2%）より若干減りましたが、引き続き44.4%と高い水準にとどまっています。

予算が不足している企業では「定期的に、中期計画および単年度計画を策定している」と回答する割合が減っていることから、中期計画や単年度計画を定期的に策定していないために、セキュリティ予算が不足しているおそれがあります。

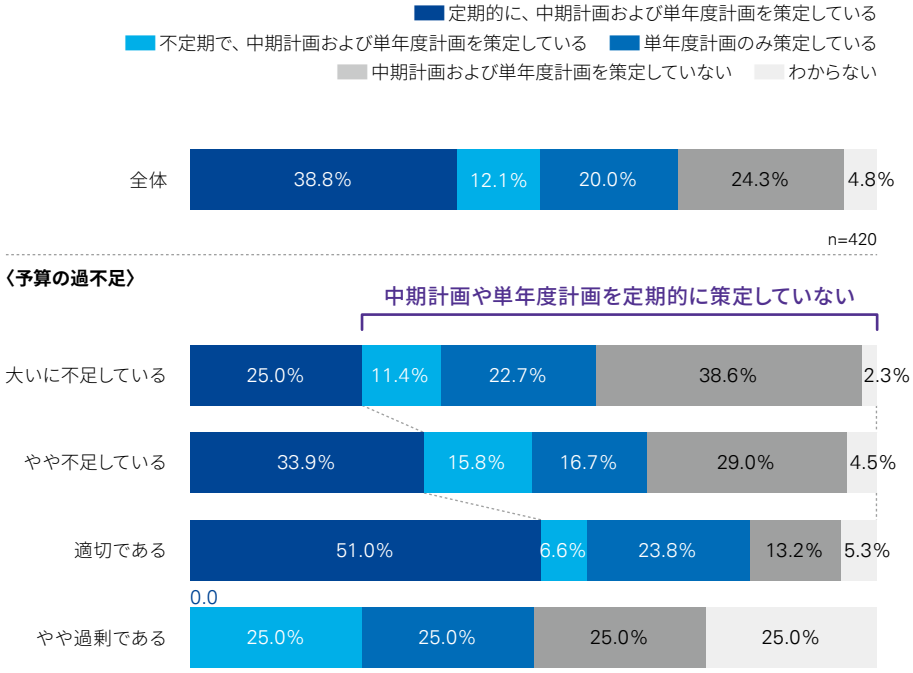
4割強の企業ではサイバーセキュリティの中期計画を策定していない

貴社では、サイバーセキュリティの中期計画、単年度計画を策定していますか。



予算が不足している企業では定期的な計画策定ができていない

左記と、予算過不足状況（P.17）をクロスで分析



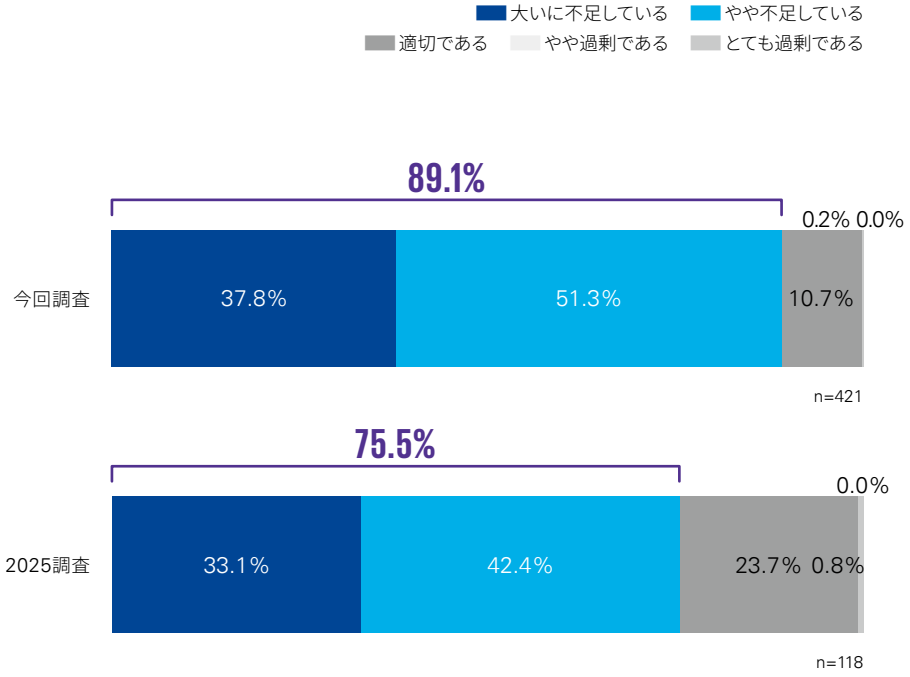
サイバーセキュリティ推進組織の人員

サイバーセキュリティ推進組織の人員が「大いに不足している」「やや不足している」との回答は89.1%となり昨年の調査（75.5%）よりも不足感が増していることがわかりました。特に、「大いに不足している」との回答割合も上がっており、サイバーセキュリティ組織の要員の不足感がさらに強まっている傾向がみられます。

また、約4割の企業が「サイバーセキュリティ推進組織は設置していない」と回答しており、特に、従業員数が3,000人未満の企業ではおよそ半数の企業でサイバーセキュリティ推進組織が設置されていないことがわかりました。

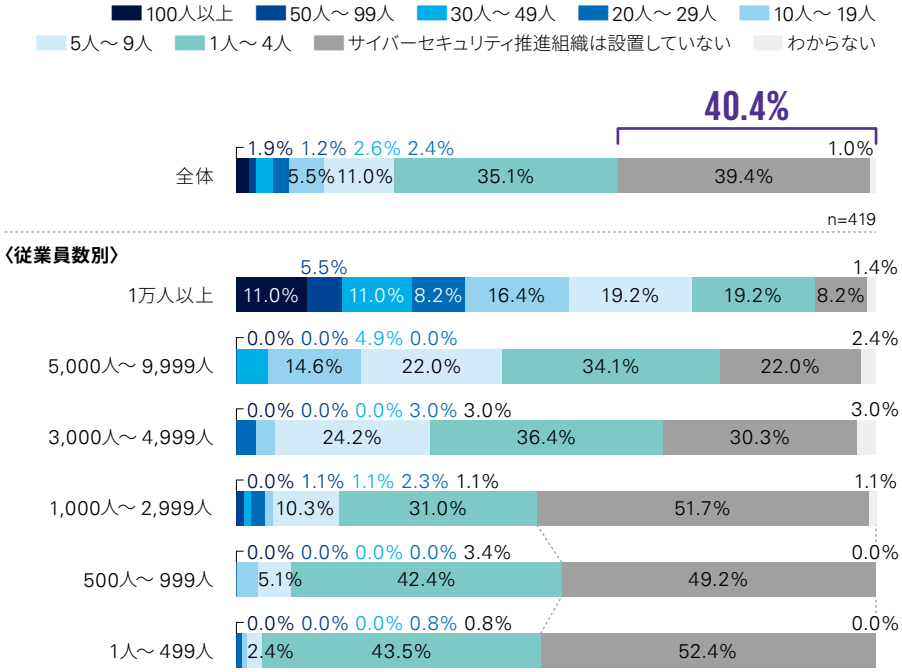
9割弱の企業でサイバーセキュリティ推進組織の人員は不足

貴社におけるサイバーセキュリティ組織の人員規模は、適切だと思いますか。



サイバーセキュリティ推進組織は設置していないが最多

貴社のサイバーセキュリティ組織における専任人数（従業員および委託常駐者を含め、兼務者を除く）は何人ですか。



コラム｜計画的なセキュリティ予算の獲得

必要なセキュリティ対策を単年度ですべて導入することは難しい。中期的な視野に立ち、計画を立て、予算を確保していく必要がある

サイバーインシデントは予測できません。だからこそ、事後対応ではなく、中長期的な計画に基づく投資と体制整備が不可欠です。

CISOは、経営と危機感を共有し、サイバーセキュリティを経営課題として議論・判断していく役割を担っています。

株式会社三菱UFJフィナンシャルグループ
常務執行役員グループCISO　松下 忍

企業が盤石な経営基盤を維持するには、巧妙化・高度化の一途を辿るサイバー攻撃の脅威や関連法規制の変化に継続的に対応することが不可欠です。

経営層のリーダーシップのもと、組織全体でPDCAサイクルを実効的に回す管理態勢の確立が求められています。

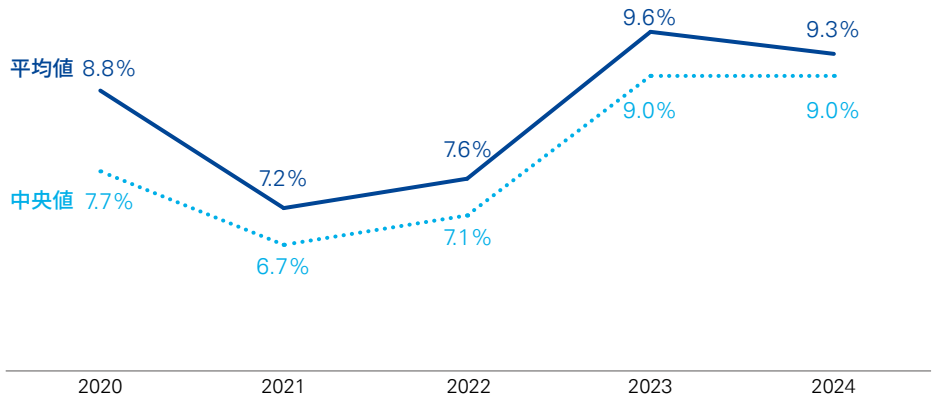
KPMGコンサルティング株式会社
執行役員 パートナー　関 憲太

セキュリティ攻撃の高度化により、保護対象も増え、導入すべきセキュリティ対策も増えている

企業により甚大な被害を発生させるため、攻撃者はセキュリティの脆弱性をより効率的に突破できるよう、サイバー攻撃を日々進化させています。

さらに、売上拡大やサービス品質向上を目的とした、ウェブサイトの拡充や他サイトとの連携、アプリ公開、そしてコロナ禍を契機に普及したリモートワークへの対応などによって、企業が保護しなければならない対象が大幅に広がりました。
こうした攻撃手法の高度化と保護対象の拡大が同時に進むなか、サイバー攻撃からの防衛は格段に複雑になっており、クラウド、ネットワーク、サーバ、エンドポイント、アプリを網羅的に保護することが必要となっています。
このようなニーズを背景にセキュリティソリューションも増えており、CNAPP、次世代SIEM、ASM、SASE、EDR、SBOM管理など、多様な製品・サービスが登場しており、企業は自社・自グループの業務や情報資産に合わせて、製品やサービスを適切に組み合せてセキュリティを強化していくことが求められています。

IT予算に占めるセキュリティ予算の割合（海外調査）



出典：NIS Investment 2025

必要なセキュリティ対策をしっかりと導入していくには、中期的な計画が必要となる

IT予算に占めるセキュリティ予算の割合は、本調査では「1～5%未満」との回答が最も多くなりましたが、グローバルの調査では、「9%」程度となっており、海外企業は日本企業の倍近い投資を行っている可能性があります。
4割強の企業ではサイバーセキュリティの中期計画が策定されていないとの結果でしたが、単年度の予算が限定されるなかでは、必要なセキュリティ対策を各年度にどの順番で導入していくのか、運用体制・プロセスと合わせて、中期的な計画を策定する必要があります。
また、策定した中期計画を経営層にわかりやすく説明し、合意のもとで予算を確保するプロセスが非常に重要となります。

コラム｜セキュリティ推進組織の立ち上げと拡大

やらなければならないセキュリティ業務は増える一方。
セキュリティ推進組織を立ち上げるとともに、中期的に拡大していく必要がある

セキュリティ対策は、検知策がより重要となっており、定常的に監視を行う常設の部署が必要となる

ファイアウォールでサイバー攻撃を防ぐことは今や不可能となり、現在は、PCの挙動などを基に、サイバー攻撃の疑いを早期に検知し、それが実際の攻撃であるか否かを的確に判断して対処することが求められています。セキュリティ対策の重要性が、防衛策から検知策へと移っており、定常的なセキュリティ監視を行い、不正プログラムの侵入を即座に検知する体制の整備が不可欠となっています。

本調査では、従業員数が3,000人未満の企業において、およそ半数の企業でサイバーセキュリティ推進組織が設置されていないことが明らかになりました。これらの企業では、発生したセキュリティインシデントへの対応といった、アドホックな対応にとどまっている可能性があります。

また、各国のセキュリティ規制に合わせた対策の検討、顧客向けアプリのセキュリティ対策の確認、預ける情報に応じた委託先チェックへの助言など、セキュリティにかかわる業務は、年々増加しています。

このような状況を踏まえ、既存組織との役割分担を整理して、担うべき業務を明確にしたうえで、常設のセキュリティ推進組織を立ち上げることが重要です。

セキュリティ推進組織の役割を定義し、中期的な計画に合わせてチーム組成、人材育成を行う

セキュリティ推進組織は立ち上げてから日が浅い企業も多く、総務や人事といったコーポレート組織と比較すると、組織内のチーム構成や役割分担が明確に整理されていないケースが少なくありません。

たとえば、人事部においては、採用チームと労務管理チームでは業務内容が異なり、それぞれにスキルや経験が異なります。同様に、セキュリティ推進組織においても、担当する業務に応じて必要となるスキルや経験が異なるため、役割を明確にしたうえで適切にチームを分けていくことが重要です。
セキュリティ推進組織の立ち上げ当初は、想定するチーム構成に対して十分な人数が揃っていないことが一般的ですが、将来的に目指すチームの姿を見据え、中期計画に従ってメンバーの採用や育成を進めていく必要があります。

特にセキュリティ人材の採用においては、入社後にどのような業務に携わり、どのような経験を積めるのか、またどのようなスキルを伸ばせるのかを重視する候補者が多くみられます。将来のチーム構成や役割を明確にし、候補者に期待する役割を具体的に伝えることで、入社後のイメージをもってもらいやすくなり、結果として優秀な人材の獲得につながります。

セキュリティ推進組織のチーム割の事例（OT/IoTセキュリティを除く）

戦略・企画	SOC・CSIRT※	セキュアシステム開発	セキュリティ監査
中期計画・単年度計画の策定	セキュリティ監視	システム・アプリ開発の規程整備・改訂	本体へのセキュリティ／プライバシー監査
規程整備・改訂・教育	脆弱性管理	システム・アプリ開発のセキュリティ仕様確認	グループ会社へのセキュリティ／プライバシー監査
個人情報保護	インシデント対応	システム・アプリ開発のセキュリティ実装確認	委託先へのセキュリティ／プライバシー監査
グループ会社／委託先管理	スレットハンティング	脆弱性診断／クラウドセキュリティ設定確認	
規制等の調査・把握	スレットインテリジェンス	クラウドサービスの利用許可	

※SOC: Security Operation Center　CSIRT: Computer Security Incident Response Team

03 子会社管理

03

本章の概要

国内子会社と比較して、海外子会社のサイバーセキュリティ対策は各社任せの傾向が強い。国内外子会社を含めたグループ横断でのセキュリティ対策推進が十分に行われていない

国内子会社管理は「本社主導型」が約4割。
会社規模が小さくなると、子会社任せとなる傾向がみられる

国内子会社に対するサイバーセキュリティ管理については、「本社によってルールの規定と実装方法の確認を行っている」と回答した企業が約4割と最も多く、一定程度の本社関与が進んでいることがわかりました。一方で、「必須となる対策のみ本社でセキュリティポリシー（方針）を規定し、実装方法は各社に任せている」や「基本的には各社に委ねており必要に応じて報告・相談を受けている」といった回答も少なくなく、グループ内での管理水準にはばらつきが存在しています。

特に、企業規模が小さくなるにつれて、子会社管理を各社任せとする傾向や、子会社の情報セキュリティ状況を十分に把握できていない企業が増加しており、本社の関与が限定的となっている可能性があります。

海外子会社のサイバーセキュリティ管理は国内と大きく異なり、対応が大幅に遅れている

海外子会社においては、「必須となる対策のみ本社でセキュリティポリシー（方針）を規定し、実装方法は各社に任せている」との回答が最も多く、管理の考え方が国内子会社以上に分散・委任型となっていることが明らかになりました。また、「基本的には各社に委ねており必要に応じて報告・相談を受けている」との回答も3割を超えており、本社による直接的な統制は限定的となっています。

セキュリティポリシーの整備は一定程度進んでいるものの、セキュリティ評価・アセスメントや教育・訓練については半数以上の企業で未実施となっており、国内子会社と比較して対応の遅れが顕著となっています。地域・拠点ごとの事情により対応が後回しになっている可能性がある一方で、グローバル全体としてのセキュリティ管理が進んでいない現状がうかがえます。

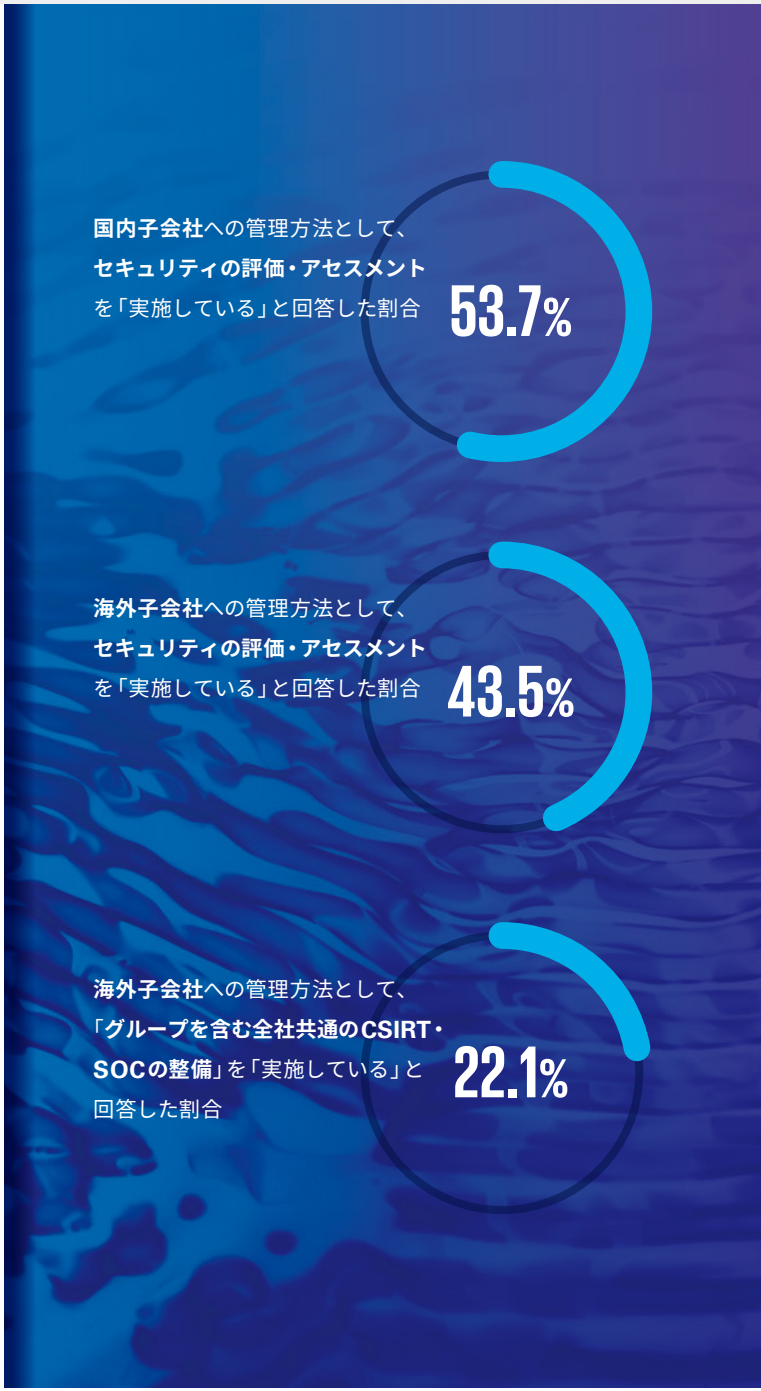
国内外子会社を含めたグループ横断でのセキュリティ対策推進が不十分となっている

国内子会社と海外子会社を比較すると、海外子会社では「基本的には各社に委ねており必要に応じて報告・相談を受けている」「子会社の情報セキュリティ状況を把握していない」とする割合が国内を大きく上回っており、セキュリティ対策を各社に一任している傾向がみられます。

一方で、サイバーセキュリティ人材はグローバルで不足しており、親会社と比べて規模の小さい海外子会社において、専門人材の採用・育成を単独で行うことは一層困難になっており、海外子会社にセキュリティ対策を委ねることは、グループ全体としてのリスクを高める要因となります。

本調査結果においても、サイバーインシデントの侵入経路として、「攻撃があり業務上の被害があった」との回答は、子会社の国内拠点よりも海外拠点の方が多い結果となりました。

海外拠点を起点としたサイバーインシデントのリスクが高まるなか、国内外の子会社を含めたグループ横断でのセキュリティ対策の企画・推進が強く求められています。



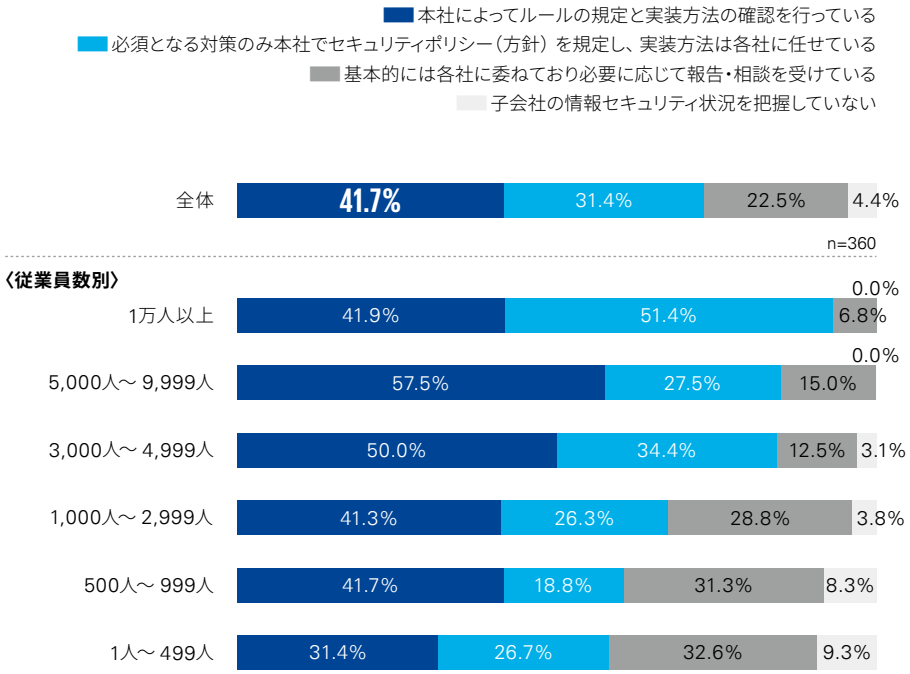
国内子会社に対するサイバーセキュリティ管理

国内子会社の情報セキュリティ管理は、「本社によってルールの規定と実装方法の確認を行っている」が最も多く、回答企業の41.7%となりました。従業員数が少なくなると「基本的には各社に委ねており必要に応じて報告・相談を受けている」「子会社の情報セキュリティ状況を把握していない」という回答割合が増え、小規模の会社においてグループ会社の管理が行き届いていない様子がうかがえます。

国内子会社の管理について、半数以上の企業において「セキュリティポリシー（方針）の整備」「セキュリティの評価・アセスメント」「セキュリティの教育・訓練」が行われていました。また、約1/3の企業において「グループを含む全社共通CSIRT・SOCの整備」「グループを含む全社共通の情報システム資産管理」が行われていました。

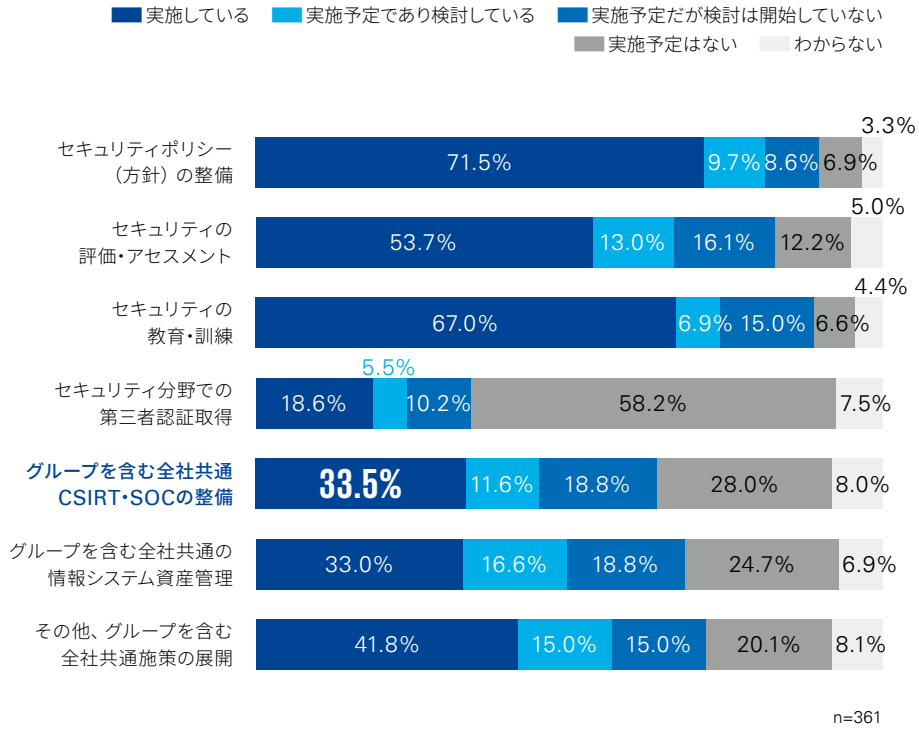
国内子会社は本社にてルール規定、実装方法の確認を行っているが約4割

貴社の国内子会社における情報セキュリティをどのように管理されていますか。



グループ共通CSIRT・SOCの整備は約3割

貴社の国内子会社管理について、実施・検討している対策を次のなかから選択してください。



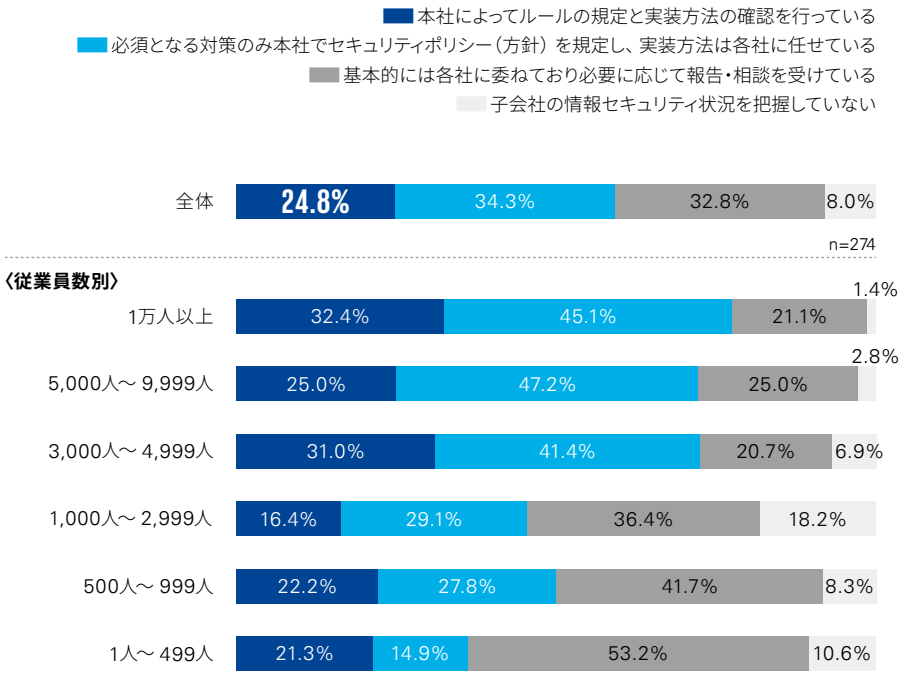
海外子会社に対するサイバーセキュリティ管理

海外子会社の情報セキュリティ管理は、「必須となる対策のみ本社でセキュリティポリシー（方針）を規定し、実装方法は各社に任せている」が最も多く、回答企業の34.3%となりました。一方、「基本的には各社に委ねており必要に応じて報告・相談を受けている」との回答割合も高い傾向（32.8%）がみられました。特に、小規模の会社においてグループ会社の管理が行き届いていない様子がうかがえます。

海外子会社の「セキュリティポリシー（方針）の整備」は6割以上の企業が「実施している」と回答しているものの、「セキュリティ分野での第三者認証取得」について、半数以上の企業が実施できていないと回答しています。国内子会社の管理と比較し、大幅に対応が遅れている様子がうかがえます。

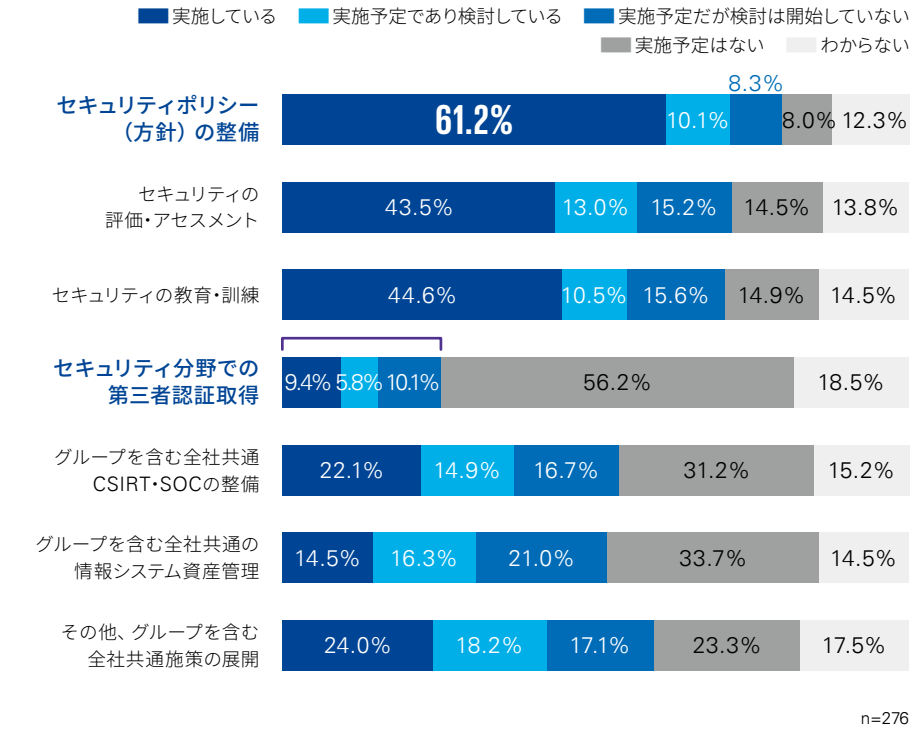
海外子会社は本社にてルール規定、実装方法の確認を行っているが約2割

貴社の海外子会社における情報セキュリティをどのように管理されていますか。



海外子会社の半数はアセスメントや教育が実施できていない

貴社の海外子会社管理について、実施・検討している対策を次のなかから選択してください。



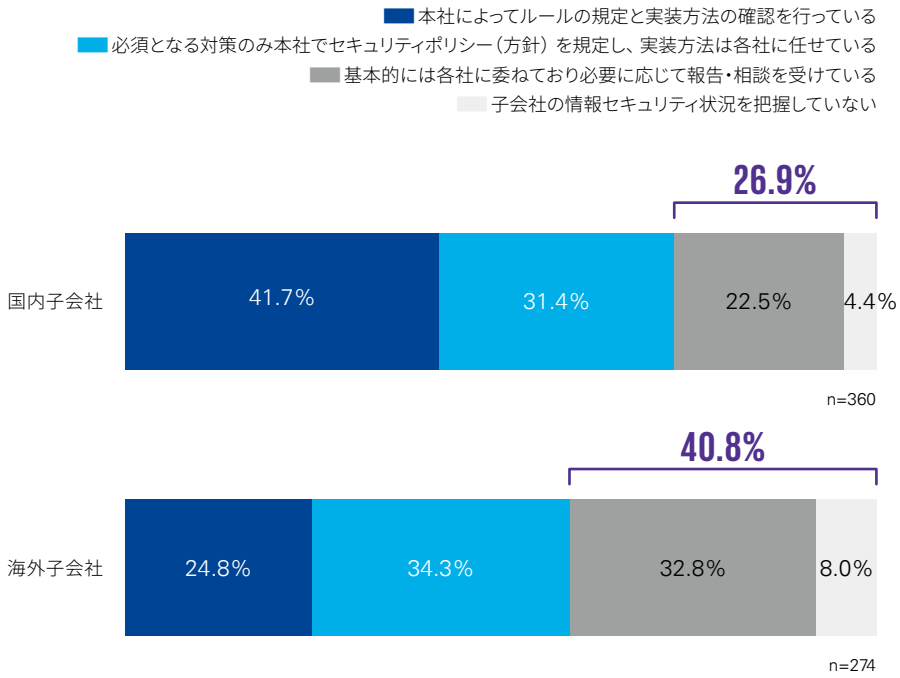
国内子会社と海外子会社への管理の比較

「基本的には各社に委ねており必要に応じて報告・相談を受けている」「子会社の情報セキュリティ状況を把握していない」との回答割合が、国内子会社では26.9%にとどまりましたが、海外子会社では40.8%にのぼり、国内子会社と比較して海外子会社の管理は各社に委ねている状況がみられました。

また、「グループを含む全社共通管理の情報システム資産管理」を「実施している」との回答は、国内子会社の33.0%に対し、海外子会社では14.5%にとどまりました。また、「実施予定はない」や「わからない」との回答も国内企業の31.6%に対し、海外企業では48.2%にのぼりました。

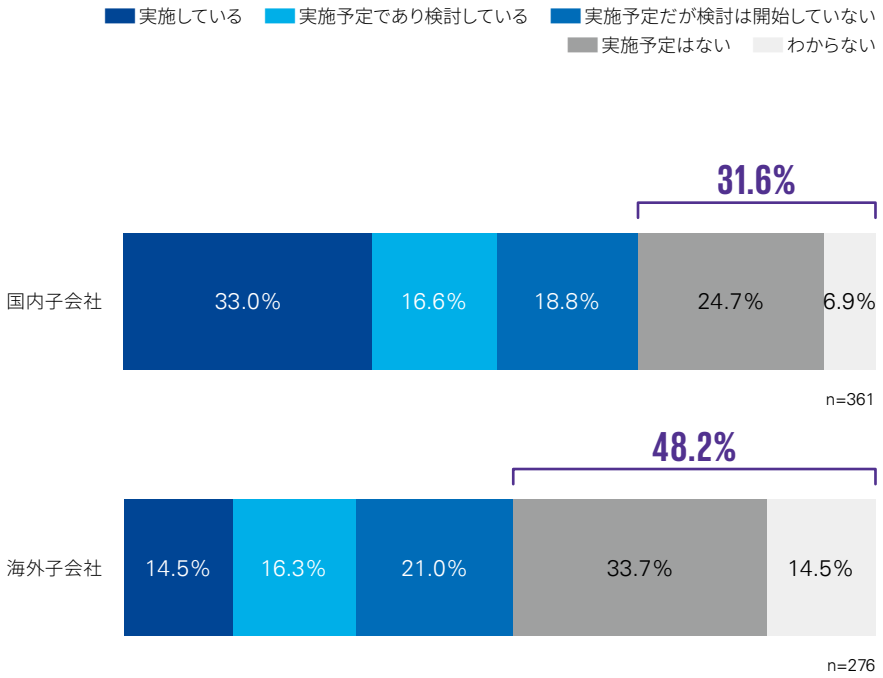
海外子会社の管理は国内子会社よりも各社に委ねている／把握していない割合が高い

貴社の子会社における情報セキュリティをどのように管理されていますか。



海外子会社ではグループを含む全社共通の情報システム資産管理ができていない

「グループを含む全社共通の情報システム資産管理」について、国内子会社と海外子会社を比較



コラム｜本社主導で進めるグループセキュリティ

本社と子会社のセキュリティ対策のギャップは、グループ全体のリスクとなる。人材不足を前提に、本社主導でツールと運用を標準化・可視化することが重要となる

本社と子会社のギャップがリスクになる

多くの企業で本社のセキュリティ対策は高度化していますが、国内外の子会社を含めたグループ全体でみると、対策水準にばらつきが残っているのが実情です。
サイバー攻撃は拠点や組織を区別せず、最も対策が弱いポイントを狙います。仮に、子会社で管理されている業務サーバーが侵入口となった場合、その影響は本社や他拠点へ波及しかねません。
子会社のセキュリティを現場任せにすること自体が、グループ全体のリスクとなっていると言えます。

セキュリティ対策は子会社任せでは進まない

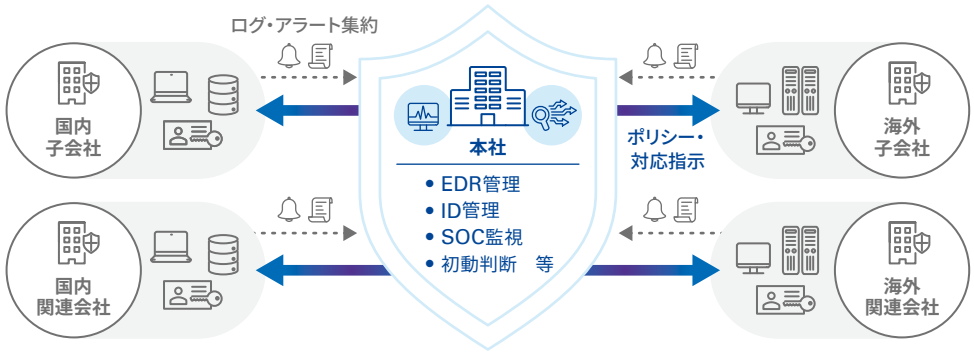
子会社ではIT人材や予算が限られ、端末管理やアカウントの棚卸し、ログ管理といった基本的な対策が後回しになりがちです。その結果、管理状況は属人化し、本社から実態が見えなくなります。
セキュリティは個別拠点の努力に委ねるものではなく、経営リスクとして本社が主導で管理すべき領域です。
本社がグループとして「最低限守るべき水準」を定め、対策状況を把握できる状態をつくることが重要です。

グローバル施策は「人が足りない」前提で考える

特に海外子会社では、ルールやポリシー自体は定められているものの、実装や運用が十分に行われていないケースが多くみられます。
実際にサーバーの棚卸しや資産調査を行うと、本社が把握していなかった運用や、管理対象から漏れていたサーバーが見つかることも少なくありません。
多くの場合、海外子会社に悪意があるわけではなく、「何を、どこまで対応すればよいのかわからない」という状態に置かれているのが実態です。

こうした課題に対して有効なのが、本社主導による仕組み化です。
たとえば、EDRなどのセキュリティ製品を本社で選定・統一し、子会社のサーバーにも共通導入することで、現地の運用負荷を抑えつつ、対策状況を可視化できます。
さらに、ログ監視やアラート対応をグローバルで集約すれば、各拠点に専門人材を配置せずとも、インシデントの早期検知や判断が可能になります。
子会社に対応を委ねるのではなく、本社がツール・運用・判断を担い、人材不足を前提とした体制を構築することが、実効性のあるグループセキュリティにつながります。

本社主導のグループセキュリティ



グループ全体の信頼性とブランドを守る観点から、海外子会社を含むセキュリティ水準の底上げは重要な経営課題です。対策を各社任せにせず、本社が基準を定め可視化し、集約的に統括することで、実効性あるガバナンスを確立し、サプライチェーン全体のレジリエンス強化を図ることが不可欠です。

株式会社ニコン
常務執行役員　CRO、CISO
葛西 洋一

子会社管理が重要であるとの認識は浸透してきていますが、実効性のある管理の実現には、まだ課題があるのが現状と思われます。形式を整えることではなく、実際にできる範囲、できない範囲を冷静に識別し、レジリエンス対応等の次善策を組み合せた、個社ごとに実現可能な対策を講じていくことが最終的な解決策だと考えます。

有限責任 あずさ監査法人
Digital Advisory事業部／パートナー
山口 達也

04 委託先・取引先管理

04

本章の概要

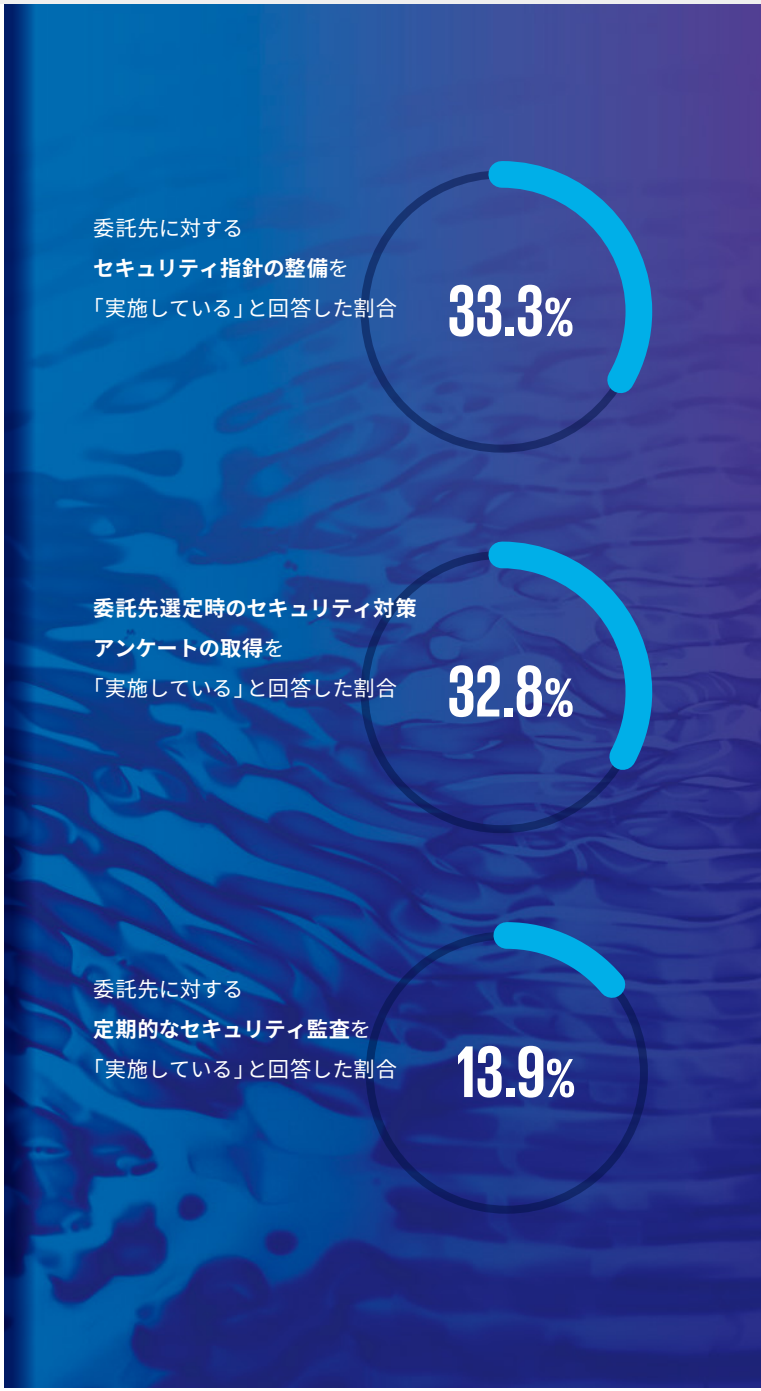
委託先・取引先に対するサイバーセキュリティ管理は全体的に遅れており、基本的な施策でも実施率は低い。特に非金融業では対応の遅れが目立ち、業種を問わずサプライチェーン全体を見据えた強化が求められる

委託先・取引先に対するセキュリティ管理の基本となる指針の整備すら対応が遅れている

委託先・取引先に対するサイバーセキュリティ管理については、いずれの施策においても実施率が4割を超えるものはなく、基本的な対応である「委託先に対するセキュリティ指針の整備」や「委託先選定時のセキュリティ対策アンケート取得」でも実施率は約3割にとどまっています。
特に、委託先に対するセキュリティ指針の整備については、「実施予定はない」が3割を超えていますが、サプライチェーン経由のセキュリティリスクが拡大するなか、委託する情報の機密度や、委託した業務が停止することで自社の業務が遅延・中断するリスクなどに応じて、委託先・取引先を選定する指針そのものが整備されていないのは大きな課題と言えます。
特に、多層構造で生産する製造業においては、自社はしっかりとした指針で委託先を選定しても、その下の委託先の選定がしっかりとされていない場合、情報の漏えいや業務が遅延・中断するリスクは高くなります。
製造業での「委託先に対するセキュリティ指針の整備」が行われている企業は2割にとどまっていましたが、リスクの大きさに鑑み、もう一段の取組みが望まれます。
さらに、委託先の対策状況をシステムやサービスを用いて一元管理している企業は1割未満との回答でしたが、自社の業務に照らして、委託先のセキュリティリスクを継続的にモニタリングするシステム・仕組みを構築していくことが求められます。

委託先管理の成熟度は業種によって大きな差があり、特に非金融業では対応の遅れが顕著となっている

委託先・取引先に対するサイバーセキュリティ管理の取組み状況には、業種間で大きな差がみられました。
特に、「委託先に対するセキュリティ指針の整備」や「委託先選定時のセキュリティ対策アンケート取得」といった基本的な施策については、金融業では高い実施率が確認される一方、「製造」「流通」「旅行・レジャー・飲食」などの業種では実施率が著しく低い結果となっています。
また、委託先に対する定期的なセキュリティ監査については、金融を除く多くの業種で、「実施予定はない」との回答が過半数を占めており、委託開始後の継続的なモニタリングが十分に行われていない実態が明らかになりました。
本調査においても、サイバーインシデントの侵入経路として、「攻撃があり業務上の被害があった」との回答は、「国内の委託先・取引先」が最多となりました。金融以外の業種においても、委託先・取引先のリスクに合わせたセキュリティ管理を行っていくことが求められます。



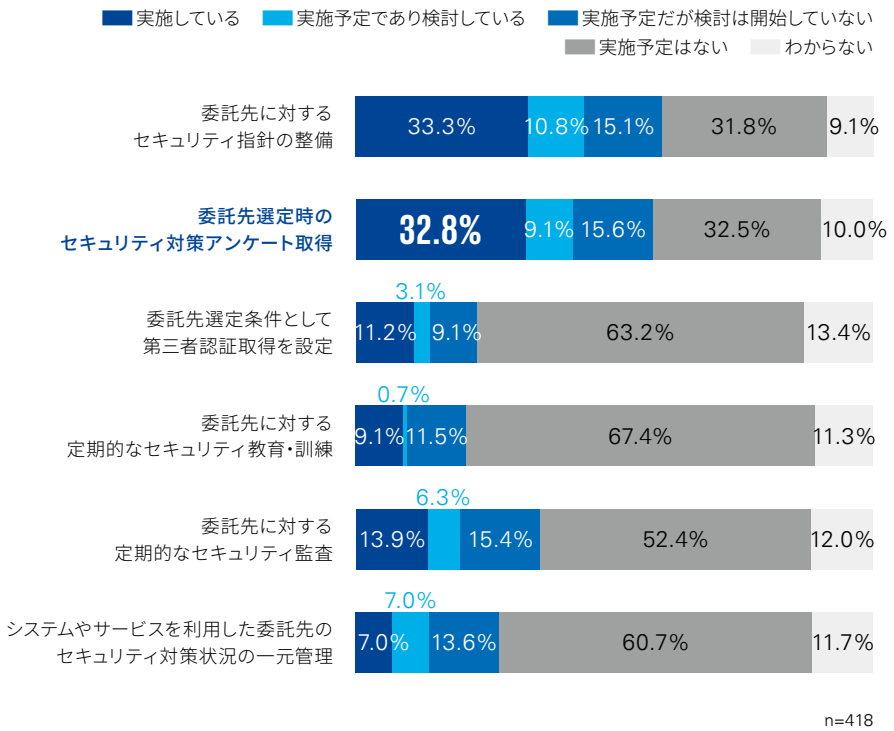
委託先・取引先に対するサイバーセキュリティ管理

委託先・取引先管理において、いずれの施策も実施率が4割を超える回答はなく、「委託先に対するセキュリティ指針の整備」「委託先選定時のセキュリティ対策アンケート取得」ですら、実施率は約3割にとどまりました。また、「システムやサービスを利用した委託先のセキュリティ対策状況の一元管理」については、7.0%にとどまりました。

委託する業務・サービスや預ける情報に応じて委託先の管理方法を定める「委託先に対するセキュリティ指針の整備」について、「金融」では7割近くの企業が実施しているのに対し、「旅行・レジャー・飲食」では10.0%の実施にとどまり、業種によって大きな差があることがわかりました。

委託先選定時のアンケート取得の実施は3割にとどまる

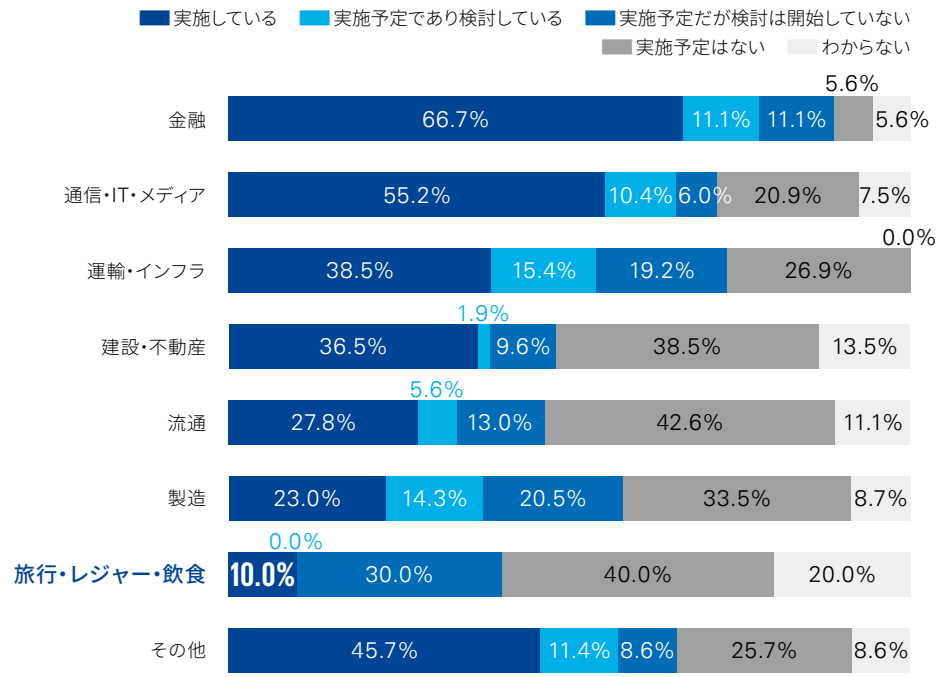
貴社の委託先・取引先の管理について、実施している対策を次のなかから選択してください。



n=418

セキュリティ指針の整備について、「旅行・レジャー・飲食」では1割の実施にとどまる

「委託先に対するセキュリティ指針の整備」について、業種別に分析



n=423

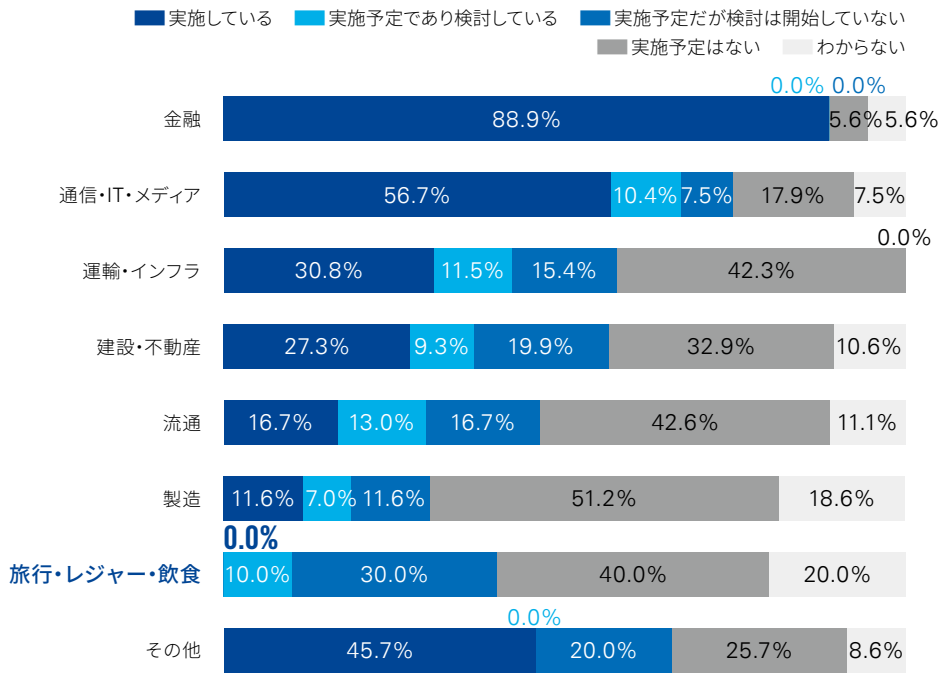
委託先・取引先に対するサイバーセキュリティ管理（つづき）

委託する業務・サービスや預ける情報に応じて委託先が十分なセキュリティ対策を講じているかを委託先選定時に確認するアンケート取得について、「金融」では約9割の企業が実施しているのに対し、「流通」では16.7%、「製造」では11.6%にとどまり、「旅行・レジャー・飲食」では０%となりました。

委託する業務・サービスが安全に継続できるか、預けた情報がしっかりと保護されているかを定期的に確認するセキュリティ監査の実施についても業種によって大きな差があることがわかりました。また、「流通」「運輸・インフラ」「製造」「建設・不動産」では、半数以上の企業が定期的なセキュリティ監査について、「実施予定はない」と回答しています。

セキュリティ対策アンケート取得について、「旅行・レジャー・飲食」では実施していない

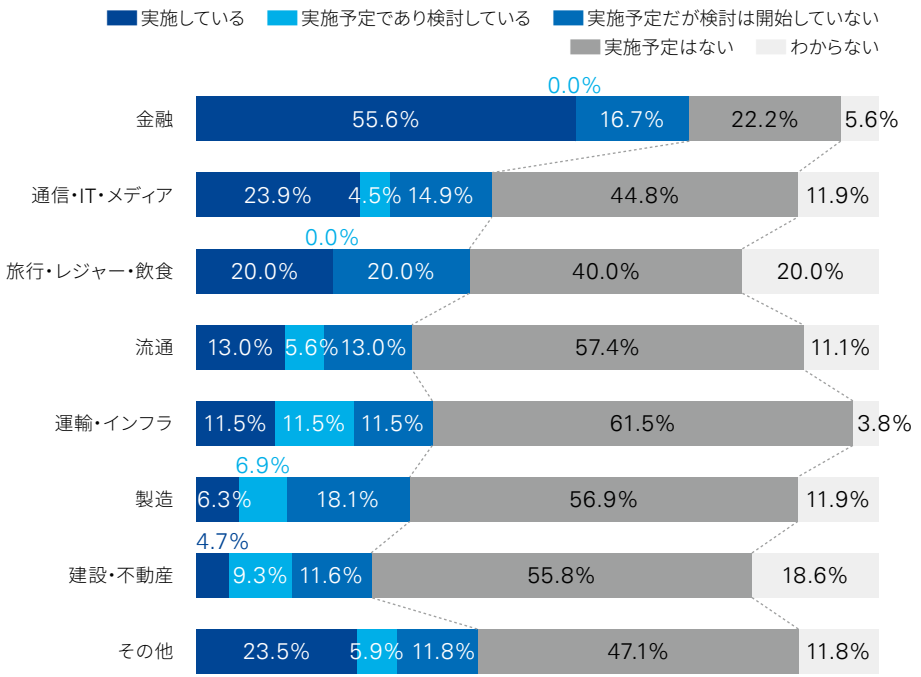
「委託先選定時のセキュリティ対策アンケート取得」について、業種別に分析



n=414

「金融」以外では多くの企業において、定期的なセキュリティ監査の実施予定がないと回答

「委託先に対する定期的なセキュリティ監査」について、業種別に分析



n=412

委託元の情報セキュリティに関する期待と、委託先が担うべき責任の目線を合わせることは非常に重要です。

その意味で、業務委託先に対するリスク評価と妥当性確認を適時で行うことに加え、委託先が実施するべき管理策を契約に盛り込むことは実効的な第三者管理策です。

ソニー株式会社
Executive Information Security Officer
EISO Office室長情報セキュリティ部 統括部長
谷澤 憲治

これまで他社には秘密にしていた「サイバーリスク」について、そのリスクが発動したらサプライチェーンはどういう事態になるか取引先と共通認識を持つことをスタートポイントとし、積極的に議論することで、今まで以上に信頼できるビジネスパートナーシップが醸成できると考えています。

株式会社KPMG Forensic & Risk Advisory
執行役員　パートナー　遠藤 正樹

コラム｜重要度に合わせた委託先・取引先管理

重要度に応じた委託先管理が不可欠であり、特に重要な委託先への監査や契約見直しを行う必要がある

すべての委託先に対して一律に同じ確認を行うのではなく、関係性や重要度に応じた確認が必要

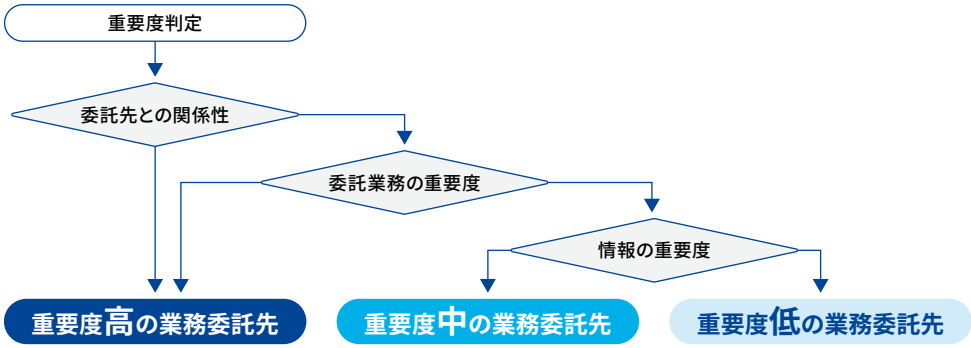
今回の調査結果から、金融以外の業種においては、委託先に対するサイバーセキュリティの確認が十分に行われていない実態が明らかになりました。
また、インシデントの発生経路に着目すると、国内の委託先・取引先において、過去1年間にサイバーインシデントが発生した割合は27.2％と高い水準に達しており、委託先を起点としたリスクが顕在化していることが分かります。
企業は、多様な委託先と連携しながら事業運営やビジネス推進を行っています。一口に委託先といっても、その重要度はさまざまであり、基幹業務を担う委託企業から、委託業務が一時的に停滞しても事業全体への影響が限定的な委託企業まで、幅広く分類することができます。
特に重要な業務を担う委託企業とは、業務やシステムが複雑に結びつき、切り離しが困難な関係となっているケースが少なくありません。そのような委託先でセキュリティインシデントが発生した場合、自社のビジネスに与える影響は避けられず、短期間で代替策を講じることが難しい構造となっていることが多いのが実情です。

一方で、委託先のサイバーセキュリティ対策の状況を確認することは、委託元・委託先の双方にとって、一定の労力やコストを伴います。そのため、すべての委託先に対して一律に同じレベルの確認を行うのではなく、委託先との関係性や重要度に応じていくつかの分類に分け、それぞれに適した方法でサイバーセキュリティの取組み状況を確認していくことが求められます。

重要な委託先にはチェックリスト形式ではなく、業務内容に合わせた監査を実施することが重要

特に重要な委託先に対しては、チェックリスト形式での確認にとどまらず、真にビジネスパートナーとして適切なサイバーセキュリティ対策が実践されているかを見極めるための監査が必要となります。監査を進める過程では、契約内容に立ち返る場面も少なくありません。日本の商慣習においては契約が自動更新され、結果として古い契約内容のままとなっているケースも散見されます。既存契約に対して、セキュリティ条項の追加や更新を変更契約として盛り込もうとすると、価格交渉につながる可能性があることから、現場レベルで反発が生じる場合もあります。しかしながら、こうした課題を理由に対応を先送りすることは、企業全体のリスクを高める結果になりかねません。
企業には、自社のビジネスや社会に与える影響を正しく認識したうえで、委託先との関係性を改めて見直し、説明責任を果たせる体制を整えることがこれまで以上に求められています。

重要度付けのイメージ



コラム｜外部サービス管理において企業が取るべき実践的対応

実効性を確保した外部サービスを活用しつつ、最終的には事業のレジリエンスを高める対応を含めた管理が必要

外部サービス利用に適応した概念

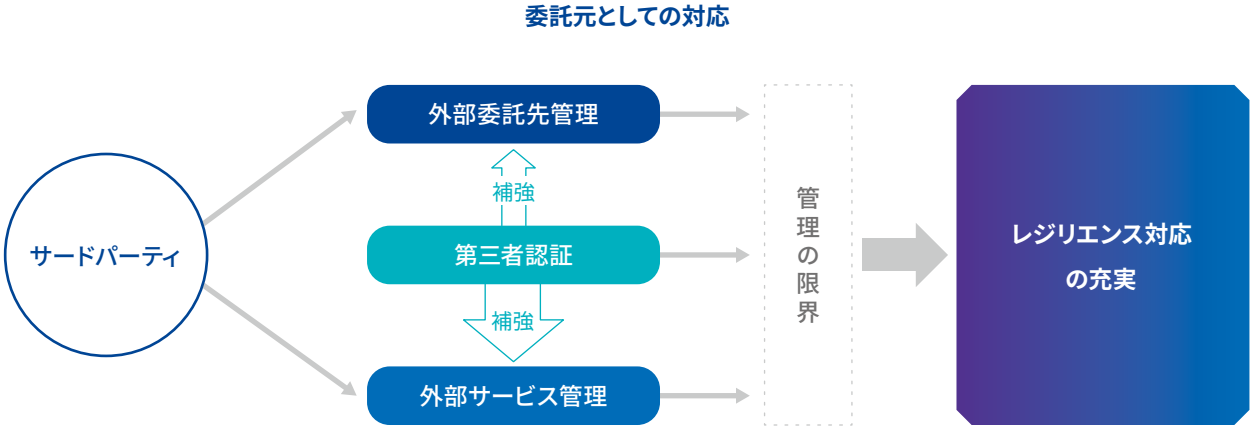
経済産業省・NCO（国家サイバー統括室）が現在検討中である「サプライチェーンリスク適合評価制度」において、発注企業、委託先企業それぞれに対し、

発注企業：
取引先におけるセキュリティ対策が可視化しづらく、要求事項（チェックリスト等）の適正性の担保も難しい

委託先企業：
複雑なサプライチェーン下でさまざまな取引先から要求事項を求められ、過度な負担につながっている（特に中小企業を中心に）

といった課題が提示されています。

これまでは、「外部委託先管理」というマネジメントフレームワークをベースに、いかに、より実効的・詳細に管理を実施していくかということが求められてきました。
しかしながらクラウドサービス等、外部委託先管理の枠組みでは管理しきれない形態＝外部サービス利用という関係が台頭してきたことを受けて、2019年には経済産業省のシステム管理基準において「外部サービス管理」という概念が提唱されることとなりました。



外部サービス管理＋第三者認証

外部サービス管理は、外部リソース活用において、それをどう管理していくのかという点で、外部委託先管理と非常に近い概念ですが、業務プロセスを詳細に管理できない、外部サービス提供企業の言うことが正しいという前提を置かざるを得ない等、管理レベル（信頼度）が限定的になる等の課題もあり、従来の外部委託先管理を置き換えるものとして活用するには限界があるともいわれています。

外部サービス管理という新しい概念が持つ課題を補完するため、セキュリティに関する評価・認証制度（ISMS、ISMAP等）や、保証報告書（SOC2保証報告書）等、委託先企業が発信している情報（言明書、経営者確認書等）の正確性を、独立した立場にある第三者が確認するという仕組みを併用することが現時点における現実的な解決法となっています。

今後は外部委託先管理だけでなく、外部サービス管理＋第三者認証の併用という形態の活用も、委託先管理において重要なポイントになってきます。

また、実際には最終的に委託先を完全に管理・コントロールすることは不可能である点も踏まえ、委託先で何らかの問題が発生しても、自社のビジネスへの影響を最小化するための「レジリエンス対応」の充実も重要性が増していくと考えます。

05 サイバーセキュリティ対策

05

本章の概要

多くの企業において、予算不足によりサイバーセキュリティ対策ツールは不足。技術的対策だけでなく、導入後の運用定着や迅速なパッチ適用といった運用プロセス、管理体制への対応も十分に行われていない

サイバーセキュリティ対策ツールは8割弱の企業で不足しており、予算不足が背景にある

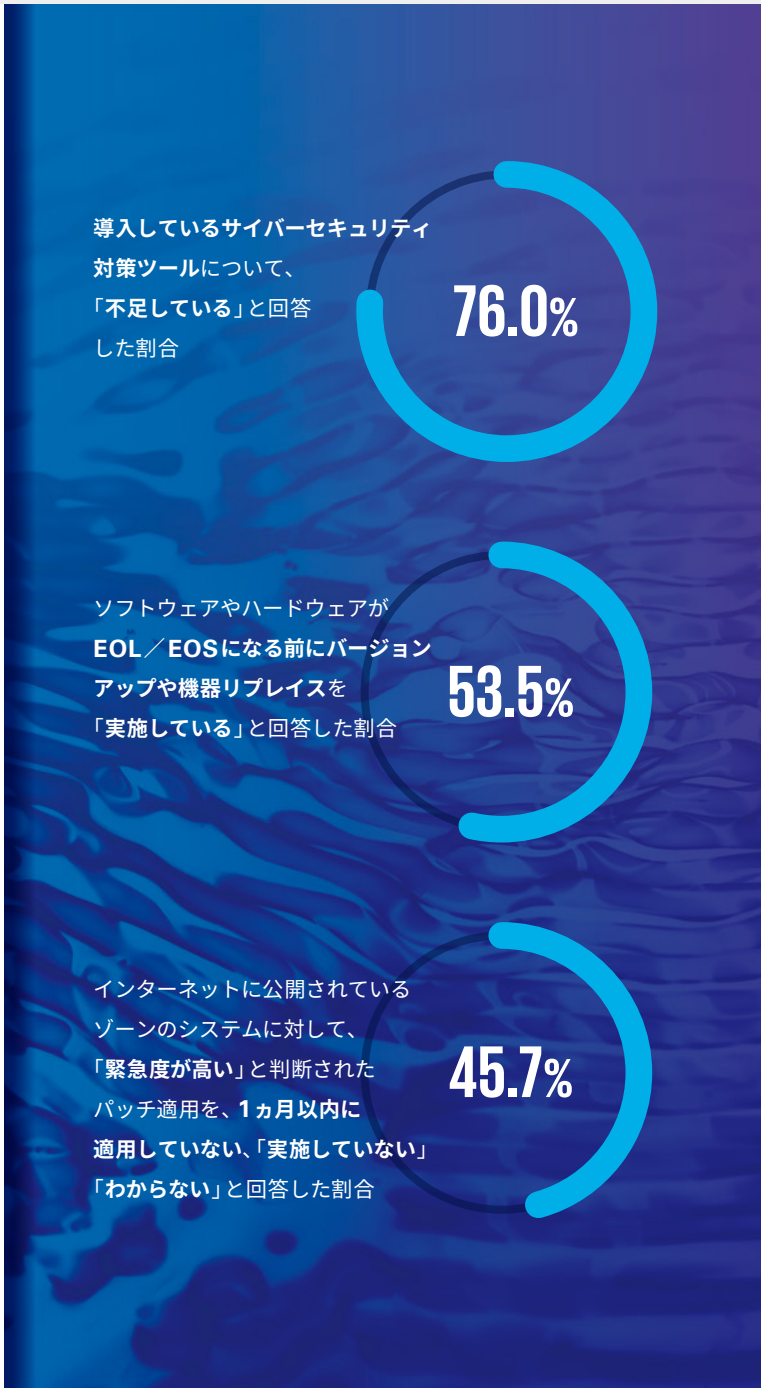
導入済みのサイバーセキュリティ対策ツールについて、「不足しているため、追加を検討する」「やや不足しているため、追加を検討する」と回答した企業は8割弱に達し、「適切である」と回答した企業を大きく上回っています。
特に、予算が不足している企業ほどセキュリティ対策ツールも不足している傾向が明確であり、対策ツール不足の主要因が予算不足にあることがうかがえます。結果として、必要性を認識しながらも十分な対策を講じられていない企業が多いと言えます。

サイバーセキュリティ対策の導入が進む一方、運用定着に課題を抱える企業は多い

アイデンティティ／アクセス管理、資産・脆弱性管理といったサイバーセキュリティ対策については、多くの企業で導入は進んでいる一方で、「導入し、十分に運用できている」と回答した企業は限定的であり、「導入したが、運用の一部に課題がある」「導入したが、想定通りに運用が機能していない」とする回答が一定割合を占めています。特に資産管理においては、導入後の運用に課題を感じている企業が多く、IT資産の把握や可視化が十分に行えていない状況がうかがえます。資産管理が不十分なままでは、脆弱性管理やパッチ適用の進捗管理が難しくなり、結果として他のセキュリティ対策の実効性にも影響を及ぼすおそれがあります。

インターネットに公開されているシステムでも、半数弱は緊急度の高いパッチが1ヵ月以内に適用されていない

公開された脆弱性のうち緊急度が高いものに対しても、速やかに（公開から1週間以内に）パッチを適用できている企業は限定的でした。特に、インターネットに公開されているシステムであっても、「公開から3ヵ月以内に適用」「期限を定めず検証完了後に適用」「実施していない」「わからない」と回答した割合の合計が半数弱となり、対応の遅れや未対応が一定数存在していることが明らかになりました。
本来、外部からの攻撃リスクが高い領域ほど迅速な対応が求められるにもかかわらず、検証や調整に時間を要し、結果として適用が後ろ倒しになっている実態がうかがえます。
パッチの未適用による侵入が多く報道されるなかで、この結果は、セキュリティ対策ツールの導入以前に、日常的な運用プロセスや管理体制が十分に整備されていないことを示唆しています。



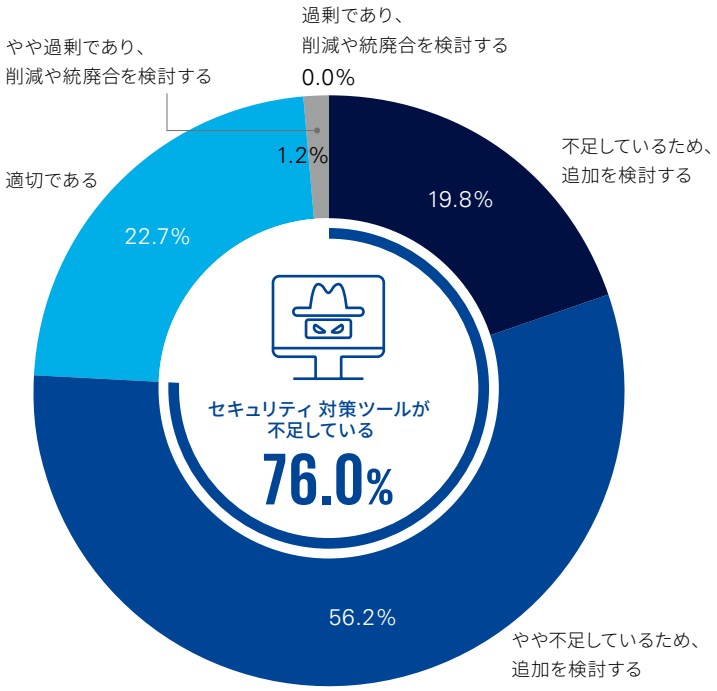
サイバーセキュリティ対策ツールの充足度合い

導入済みのサイバーセキュリティ対策ツール数について、「不足しているため、追加を検討する」「やや不足しているため、追加を検討する」と回答した企業は76.0%にのぼり、「適切である」（22.7%）を大幅に上回っていることがわかりました。一方、「やや過剰であり、削減や統廃合を検討する」と回答した企業は1.2%にとどまりました。

サイバーセキュリティ対策ツールの充足度と予算の過不足状況（P.17）をクロスで分析したところ、予算が「大いに不足している」と回答した企業の66.7%が対策ツールが「不足しているため、追加を検討する」と回答しています。また、予算が「やや不足している」と回答した企業の67.9%が対策ツールが「やや不足しているため、追加を検討する」と回答しており、対策ツールの不足は予算の不足が主な原因と読み取れます。

8割弱でサイバーセキュリティ対策ツールの導入が不足

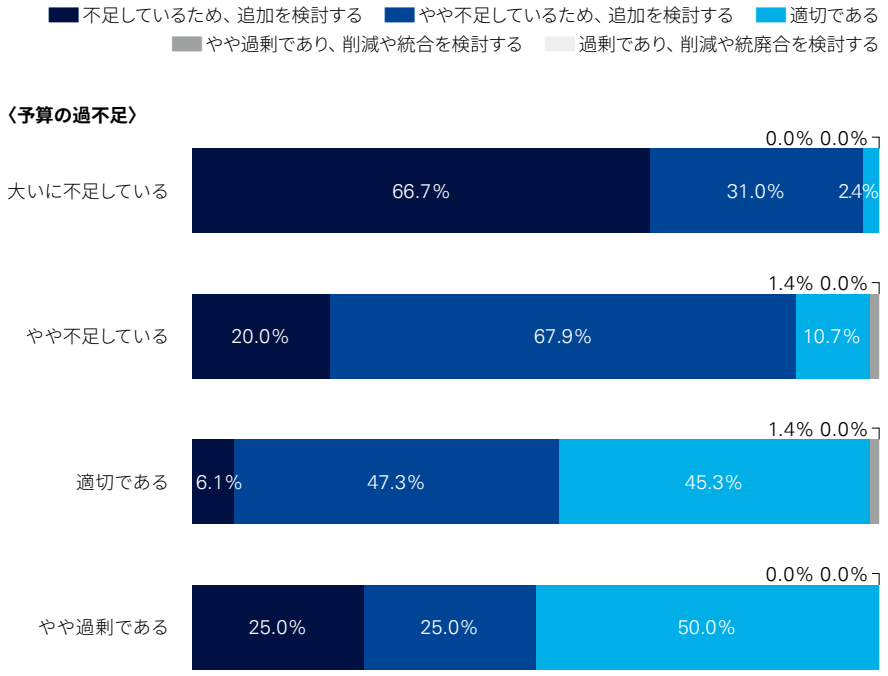
貴社が導入済みのサイバーセキュリティ対策ツール数について、該当するものを選択してください。



n=409

予算不足によるサイバーセキュリティ対策ツールの不足

左記と、予算過不足状況（P.17）をクロスで分析



n=409

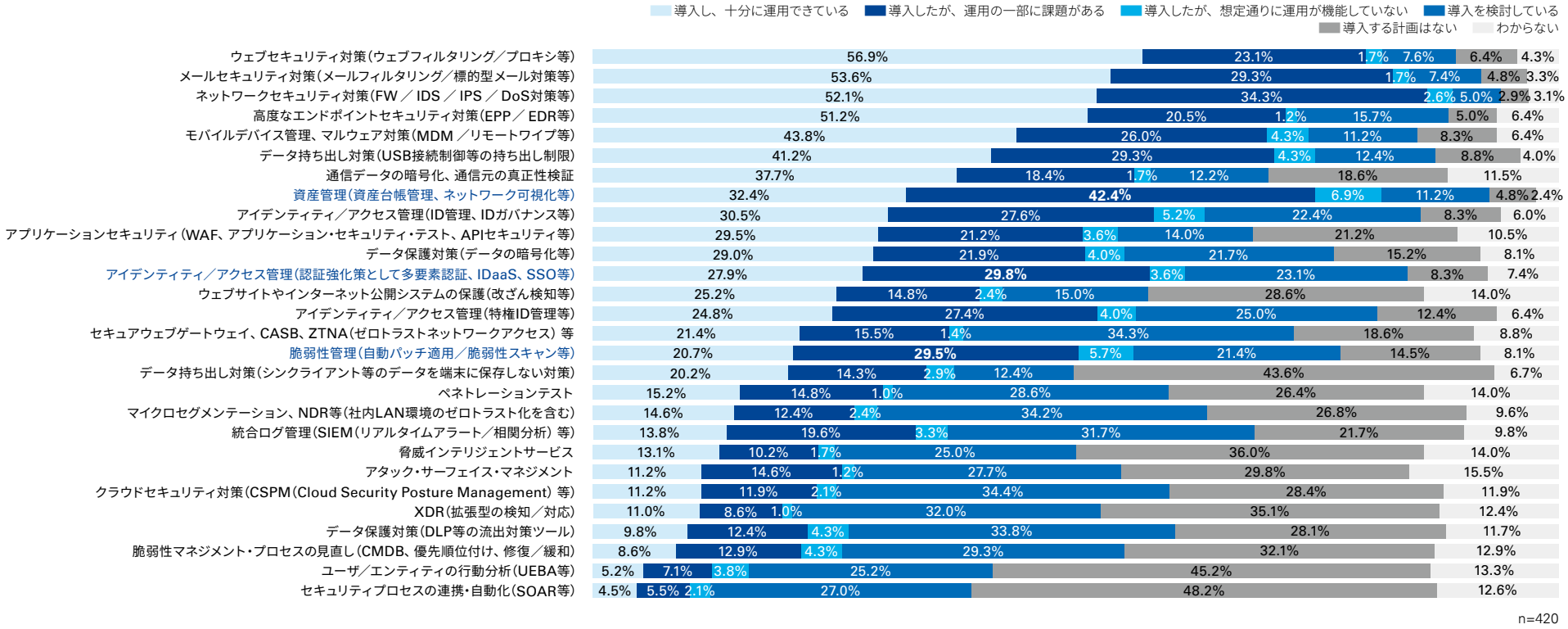
サイバーセキュリティ対策の導入状況

「導入し、十分に運用できている」よりも「導入したが、運用の一部に課題がある」との回答割合が高い対策は、「資産管理（資産台帳管理、ネットワーク可視化等）」（42.4%）「アイデンティティ／アクセス管理（認証強化策として多要素認証、IDaaS、SSO等）」（29.8%）「脆弱性管理（自動パッチ適用／脆弱性スキャン等）」（29.5%）などがありました。

また、「導入を検討している」の回答割合が多かった対策は、「クラウドセキュリティ対策（CSPM（Cloud Security Posture Management）等）」（34.4%）、「セキュアウェブゲートウェイ、CASB、ZTNA（ゼロトラストネットワークアクセス）等（インターネット境界の社外ネットワークアクセスゼロトラスト化を含む）」（34.3%）、「マイクロセグメンテーション、NDR等（社内LAN環境のゼロトラスト化を含む）」（34.2%）となりました。

資産管理、アイデンティティ／アクセス管理、脆弱性管理の導入が進みつつある

貴社のサイバーセキュリティ対策について、以下の対策を導入していますか。



n=420

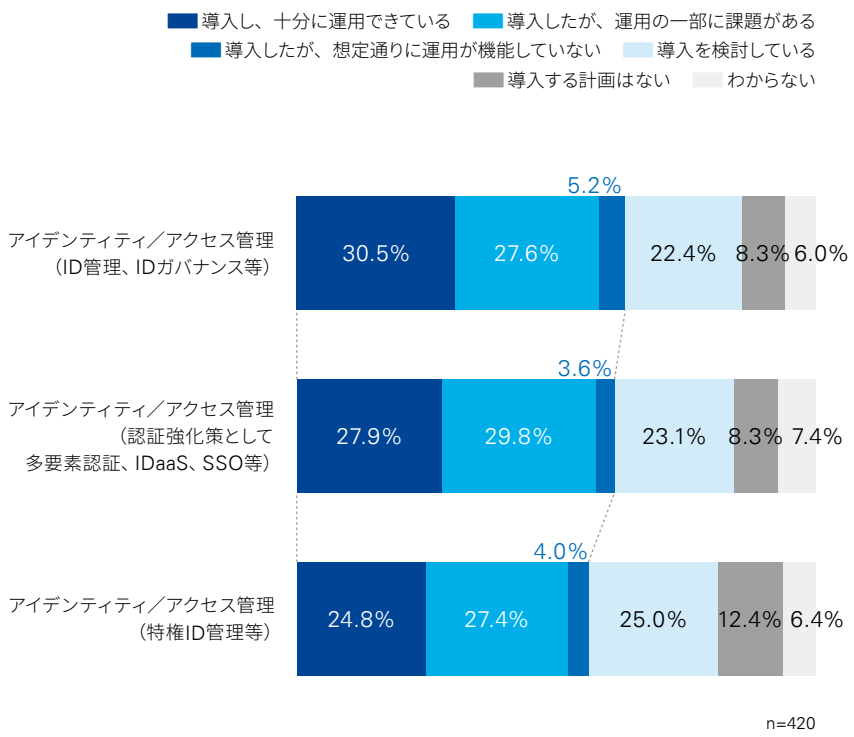
アイデンティティ／アクセス管理、資産・脆弱性管理の導入状況

アイデンティティ／アクセス管理については、ID管理／IDガバナンス、認証強化策（多要素認証、IDaaS、SSO等）、特権ID管理のいずれも導入済みが6割程度との回答を得ました。ただし、「十分に運用できている」と「運用の一部に課題がある」は半々となっており、導入後の運用定着に苦労している企業が多くみられました。

一般的に資産管理、脆弱性管理、脆弱性マネジメント・プロセスの見直しと導入を進める企業が多いですが、資産管理は他の対策と比較して、「導入したが、運用の一部に課題がある」の回答割合が最も高く、資産管理でつまずいている企業が多いと考えられます。

アイデンティティ／アクセス管理はいずれも6割程度導入済み

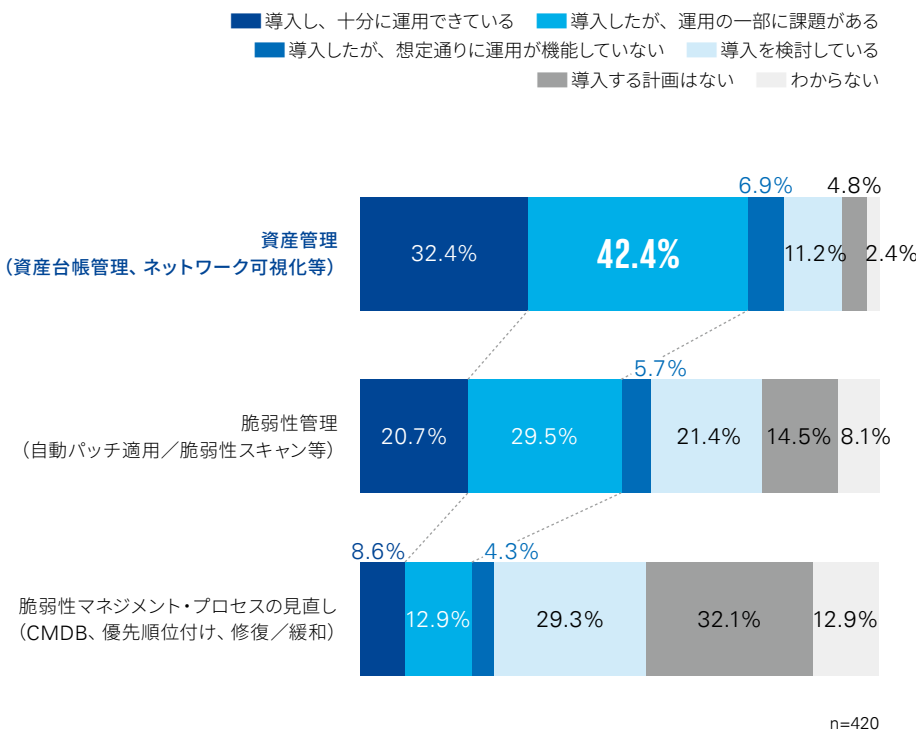
アイデンティティ／アクセス管理に係る対策の導入状況を選択してください。



n=420

資産管理の導入は進んでいるが、運用でつまずく企業が多い

資産管理、脆弱性管理に係る対策の導入状況を選択してください。



n=420

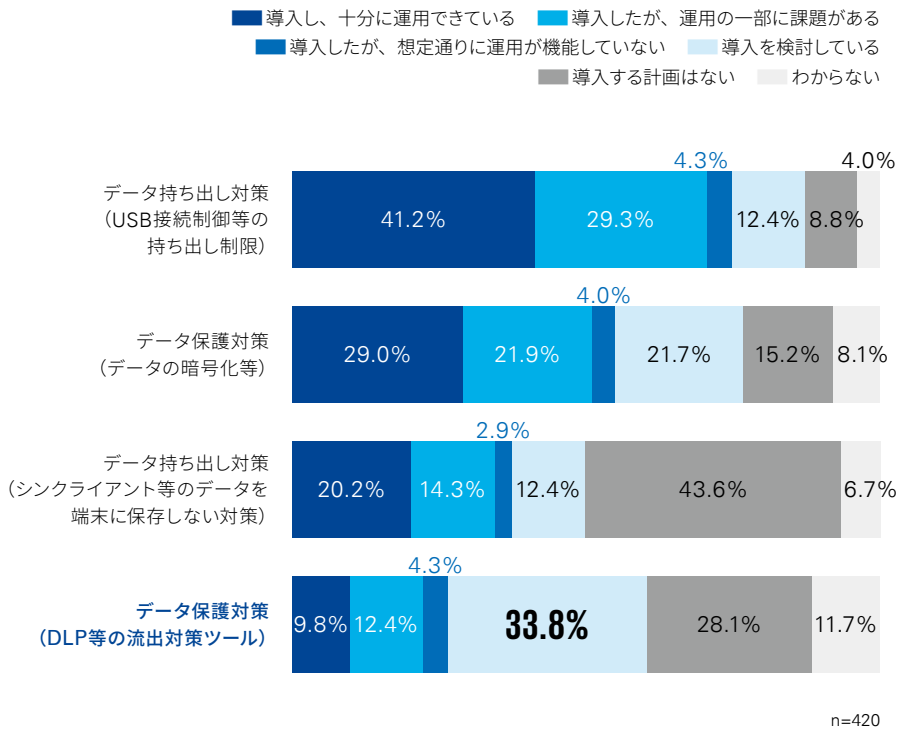
データ持ち出しの導入状況、EOL／EOS対応

データの持ち出し、保護に係る対策では、USB接続制御等の持ち出し制限は導入率が高く、7割以上で導入されていることがわかりました。ただし、「運用の一部に課題がある」「想定通りに運用が機能していない」との回答が3割以上にのぼり、運用方法に苦労している企業が多くみられました。DLP等の流出対策ツールの導入率は3割弱にとどまっていますが、「導入を検討している」と33.8%の企業が回答しており、今後導入が進むことが想定されます。

ソフトウェアやハードウェアのEOL／EOSに合わせた対応については、業種により大きな差があることがわかりました。「運輸・インフラ」「通信・IT・メディア」では「EOL／EOSになる前にバージョンアップや機器リプレイスを実施している」と回答した企業が約7割にのぼる一方、「建設・不動産」「旅行・レジャー・飲食」では「特に何も対応していない」と回答した企業が約2割となりました。

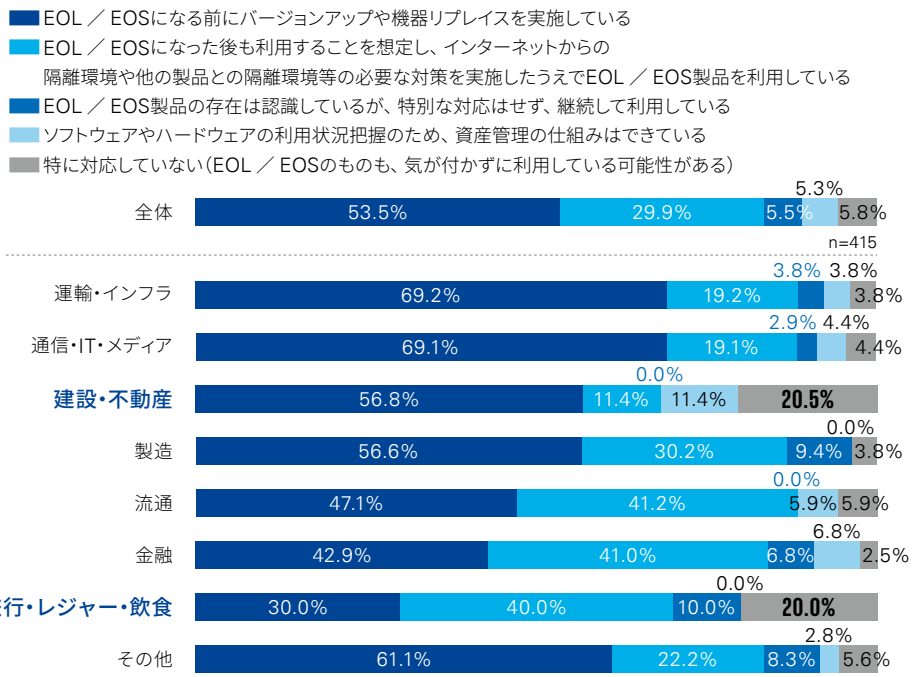
DLP等の流出対策ツールは、3割以上の企業が導入を検討している

データの持ち出し制限に係る対策の導入状況を選択してください。



「建設・不動産」「旅行・レジャー・飲食」では、特に対応していないが約2割

貴社のソフトウェアやハードウェアのEOL／EOS（EOL：販売終了、EOS：技術サポート終了を指し、ベンダー等によるバグ修正やセキュリティアップデートのサポートを受けられなくなること）への対応について、該当するものを次のなかから選択してください。



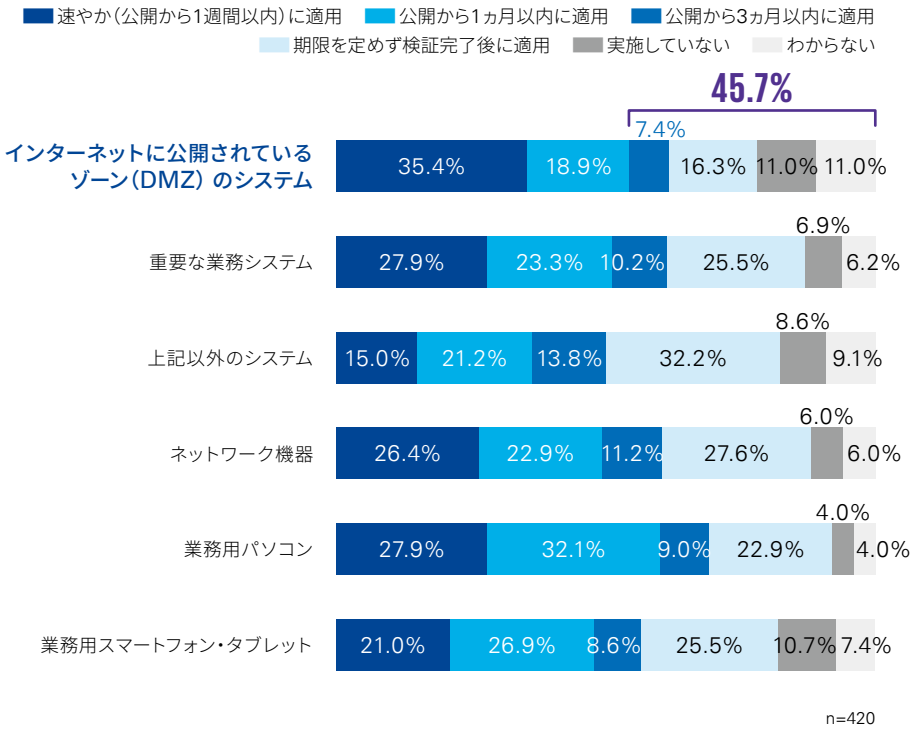
パッチ適用のタイミング

公開された脆弱性のうち「緊急度が高い」と判断されたものへのパッチ適用について、「速やか（公開から1週間以内）に適用」と回答した企業の割合は、インターネットに公開されているゾーンのシステムで35.4%となりました。「公開から3ヵ月以内に適用」「期限を定めず検証完了後に適用」「実施していない」「わからない」と回答した割合の合計が45.7%となり、半数近くが対応が遅れるか未対応であることがわかりました。

業種別にみると、「金融」「通信・ITメディア」では50%以上が「速やか（公開から1週間以内）に適用」と回答している一方、「建設・不動産」ではインターネットに公開されているゾーンのシステムでも29.5%がパッチ適用を「実施していない」と回答しています。

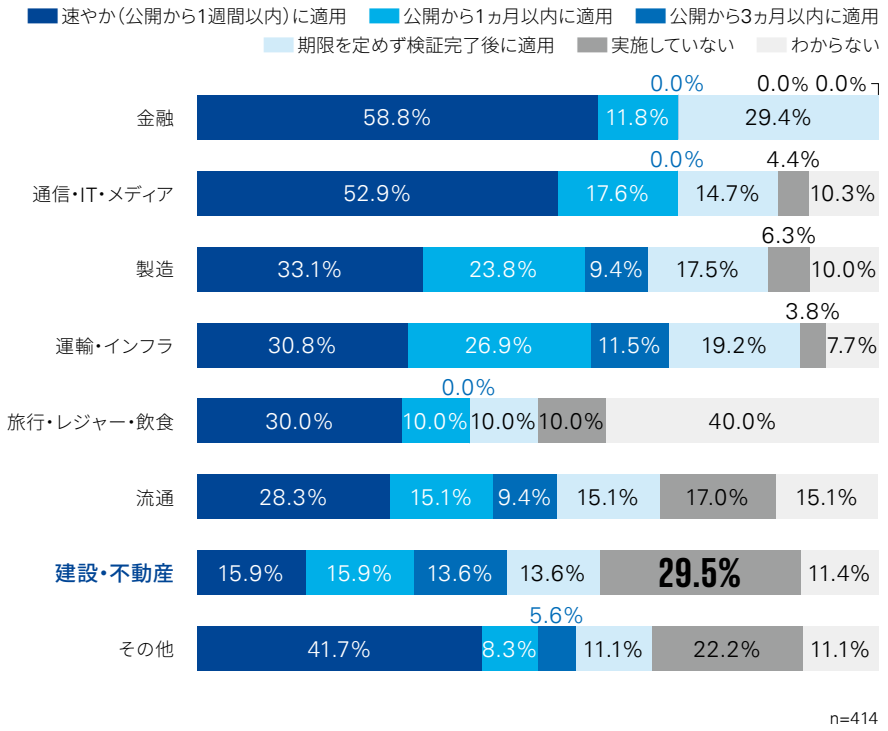
5割弱がインターネットに公開されているシステムでも1ヵ月以内にパッチ適用していない

貴社において、公開された脆弱性のうち、「緊急度が高い」と判断された脆弱性に対するパッチ適用の対応タイミングについて、該当するものを選択してください。



「建設・不動産」では約3割が、インターネット公開されているシステムでもパッチ適用していない

左記について、「インターネットに公開されているゾーン（DMZ）のシステム」のみを、業種別に分析



近年急激に拡大しているアタックサーフェスや、生成AIを活用したサイバー攻撃の高度化を踏まえると、従来型のツールだけではもはや十分に対抗できない状況にあります。

こうした環境のなかで、CISOは常に新しい製品やテクノロジーを探求し続けるプレッシャーにさらされています。

ソフトバンク株式会社
常務執行役員 兼CISO 兼CRO
リスクマネジメント室長
飯田 唯史

サイバー攻撃の高度化に伴って、導入しただけでは不十分で、定常の運用を確実に行う必要があるセキュリティソリューションが増えてきています。

こうした運用を着実に定着させるためには、導入時にしっかりと運用の体制や役割責任、プロセスを整備しておくことが重要となります。

KPMGコンサルティング株式会社
執行役員 パートナー　澤田 智輝

コラム｜セキュリティ対策の考え方

必要な対策を見極め、それを機能させる仕組みを整えてこそ、真のセキュリティ強化となる

その対策は、本当に自社に必要か

多様なセキュリティツールが次々と登場するなかで、導入そのものが目的化していないでしょうか。高度な検知技術や自動化機能は確かに魅力的に見えますが、それらが常に最優先の対策とは限りません。

実際、昨今発生しているセキュリティインシデントをみると、その原因は必ずしも高度な攻撃技術にあるとは言えず、「パッチ未適用」「設定不備」「不要アカウントの放置」「管理外IT資産の存在」など、基本的な管理の不徹底が原因となっている事例が少なくありません。こうした「セキュリティ衛生管理」の重要性は、ここ数年になって急に語られはじめたものではなく、何十年も前から、セキュリティ対策の基本中の基本として繰返し指摘されてきたものです。

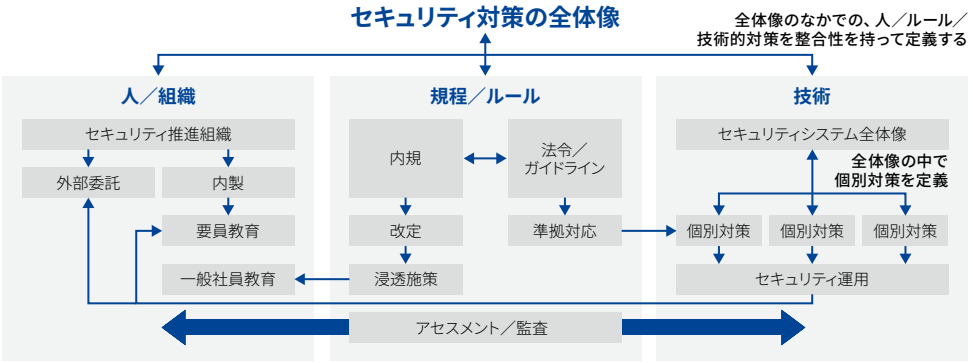
人間の衛生管理に例えるなら、手洗いやうがいに相当するものであり、医療技術がどれほど進歩しても、日常的な衛生習慣が疎かになれば感染リスクが高くなるのと同様、セキュリティ衛生管理が整っていない環境では、どれほど先進的なツールを導入しても、その効果は限定的にならざるを得ません。
新しい対策を検討する前に自社の衛生管理が機能しているか、確認することが重要です。

対策は、人・組織・ルールを含めて成立する

セキュリティ対策はツールの導入に焦点が当てられがちですが、実効性を確保するためには、ツールを運用する「人／組織」の体制をどう整えるか、また、その運用を継続的かつ適切に回すための「規程／ルール」をどう定めるかを併せて検討する必要があります。

これらが十分に整わないままツールだけを導入すると、運用はやがて形骸化し、本来の効果は発揮できなくなります。アラートが確認されない、設定や運用手順が更新されない、環境の変化に応じた見直しが行われない、そのような状態では、対策は実質的に機能しているとは言えません。

たとえば、SIEM（Security Information & Event Management）などはその代表例でしょう。高度な分析機能を備えていても、適切な監視体制や継続的なチューニングが伴わなければ、単なるログ保管基盤にとどまってしまいます。先進的なツールを次々と検討する前に、それを機能させ続ける体制が整っているかを問い直すことが重要です。対策の成否を分けるのは、製品の性能ではなく、運用の質です。
セキュリティ対策をさらに広く捉えると、対策の全体像を描き、「人／組織」「規程／ルール」「技術」の相互の関連性を踏まえて配置することが求められます。いずれかに偏らず、全体として整合した設計が不可欠です。
セキュリティ対策とは、製品を積み上げることではありません。組織として機能し続ける仕組みを構築し、見直しと改善を重ねていく活動です。人・組織・ルール・技術が一体となって初めて、実効性のあるセキュリティ対策が成立します。



06 AIセキュリティ

06

本章の概要

業務効率化を中心にAIの導入が進む一方、AI利用に対する評価・監査・レビューは十分に整備されていない。シャドーAI対策についてもポリシー整備にとどまる企業が多く、社員教育などの対策は今後の課題

AIは業務効率化を中心に導入が進む一方、セキュリティ目的での活用は限定的

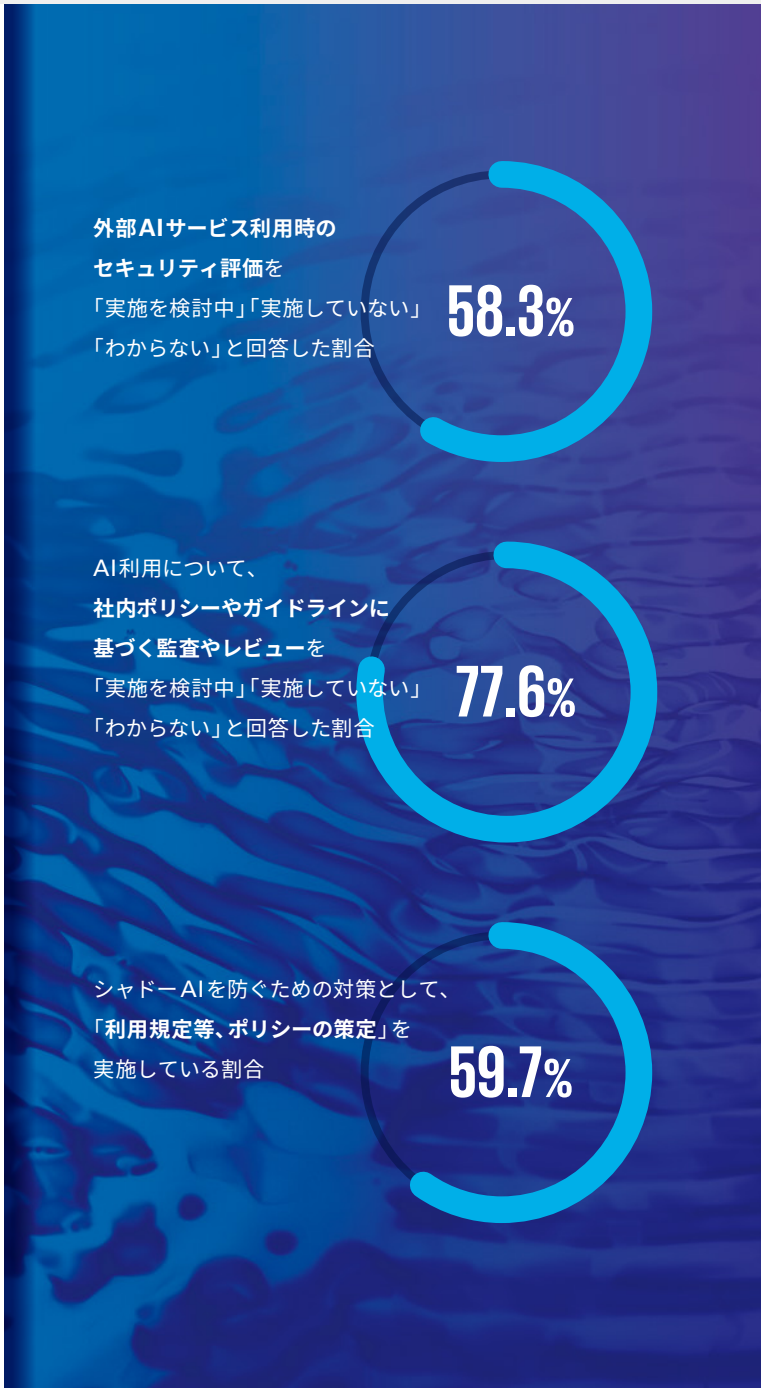
「業務効率化・自動化」を目的としたAIは導入済みが約6割と最も高く、生成AIを中心に幅広い業務領域へと急速に浸透しています。「データ分析・予測」「営業・顧客対応」といった用途でも導入が進んでおり、AIはすでに企業活動の一部として組み込まれつつあります。
一方で、「セキュリティ対策」を目的としたAI活用は導入済みが2割弱にとどまり、「導入を検討中」が3割強と最も高い結果となりました。 AI活用が業務側から先行するなかで、リスク検知や防御強化といったセキュリティ分野での活用は後追いとなっており、AI利活用の進展とリスク対応の間にギャップが生じていることが示唆されます。

AI利用に対する評価・監査・レビューは十分に整備されておらず、ガバナンスが追いついていない

外部のAIサービスを利用する際のセキュリティ評価について、「定期的に実施している」と回答した企業は2割弱にとどまり、「実施していない」は4割弱と、定期的に実施している企業を上回る結果となりました。 業種別にみると、金融では「定期的に実施している」との回答が相対的に高い一方、製造では「実施していない」が高いなど、取組み水準に差がみられます。また、AI利用に関する監査・レビューについても、実施している企業は2割強にとどまり、「実施していない」は約半数に達しています。
特に、企業規模が小さいほど、監査・レビューの実施率は低く、現場主導でAI利用が進む一方で、全社的なガバナンスが及んでいないケースが多くみられます。AIに係る規制が強化されていくなか、評価・監査・レビューを通じた継続的なリスク把握と統制の仕組み構築が、今後の重要な課題となります。

シャドーAI対策はポリシー整備にとどまり、実効性確保には課題が残る

正規に許可されていないAIツールの業務利用、いわゆるシャドーAIへの対策としては、「利用規定等、ポリシーの策定」を実施している企業が約6割と最も多く、一定の対応は進んでいます。一方で、「アクセス制御による利用防止」など、実効性を担保するための対策は3割以下にとどまっています。
この結果から、ルールは定めているものの、現場への浸透や遵守を担保する仕組みが十分でないケースが多いことがうかがえます。AIツールが容易に利用できる環境が広がるなかで、ポリシー策定に加え、教育・技術的制御・モニタリングを組み合せた多層的なシャドーAI対策が求められています。



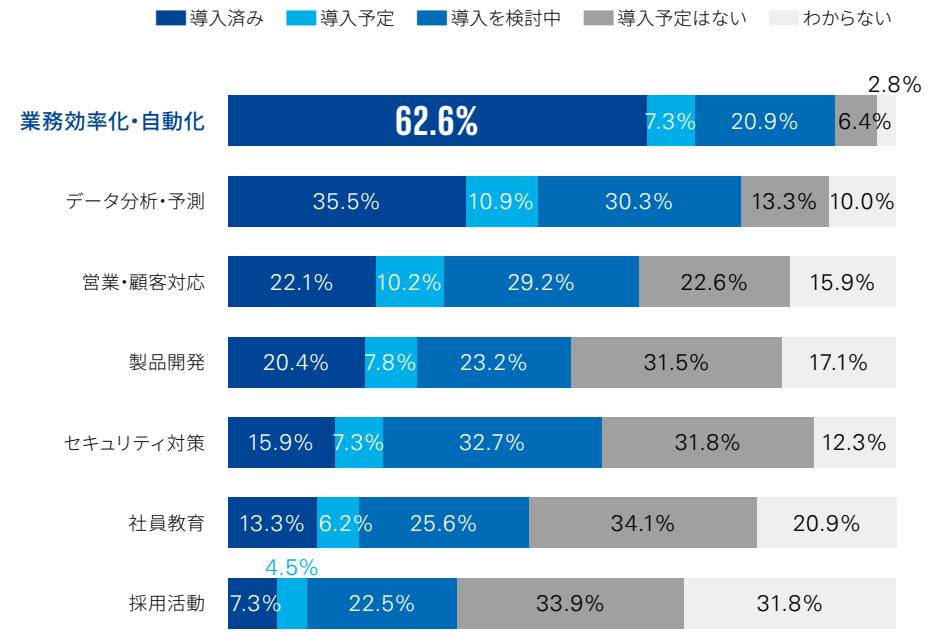
AIの導入状況

企業における目的別のAI導入状況を確認すると、「導入済み」との回答は、「業務効率化・自動化」（62.6％）が最も高く、次いで、「データ分析・予測」（35.5％）、「営業・顧客対応」（22.1％）となりました。「導入を検討中」との回答は、「セキュリティ対策」が最も高く、32.7%となりました。

利用しているAIを確認したところ、「生成AI（シングルモーダル）」が最も多く、半数以上の企業で利用されていました。続いて、「生成AI（マルチモーダル）」が47.9%、「LLM」が38.0％、「RAG」が37.0％、「AIエージェント」が21.0%となりました。

業務効率化・自動化のためにAIを導入している企業は6割超え

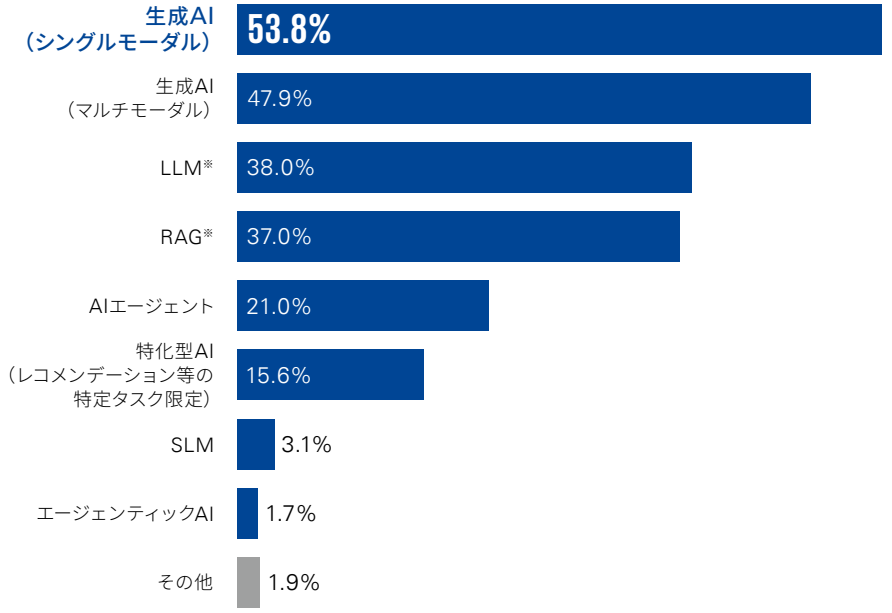
貴社は以下の目的に対しAIを導入しているか、該当するものを選択してください。



n=422

利用しているAIで最も多いのは生成AI

利用しているAIについて、該当するものを次のなかから選択してください。



※LLM:Large Language Models 大規模言語モデル
※RAG:Retrieval-Augmented Generation 検索拡張生成

n=424

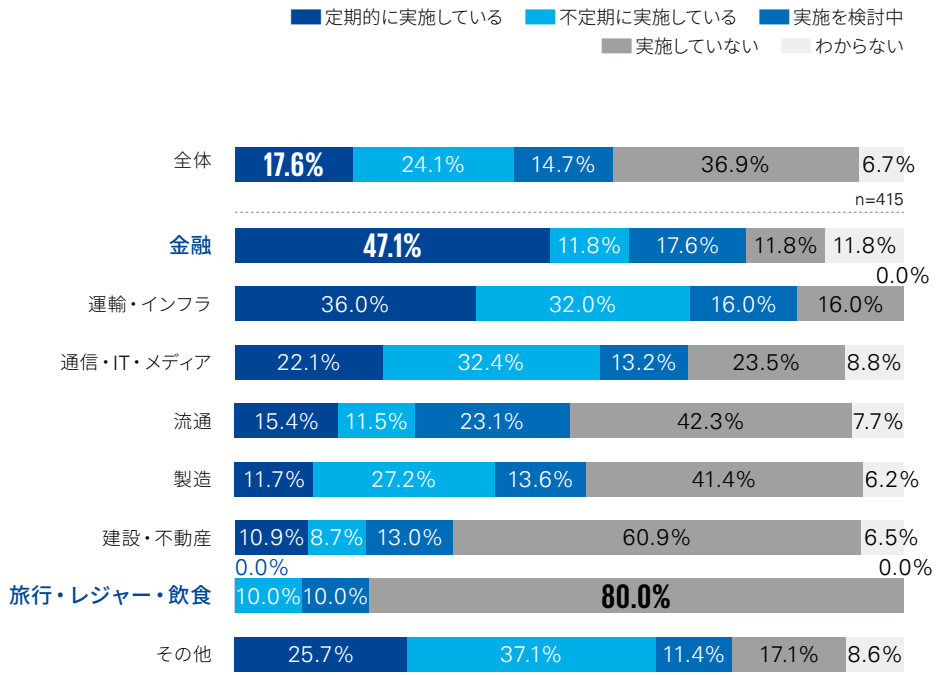
AI利用に係る評価、監査／レビュー

外部AIサービス利用時のセキュリティ評価を「定期的に実施している」と回答した企業は17.6%にとどまり、「実施していない」と回答した企業は約2倍の36.9%となりました。「金融」では「定期的に実施している」との回答割合が最も高く（47.1%）、「旅行・レジャー・飲食」では「実施していない」との回答割合が最も高く（80.0%）なりました。

AI利用について、社内ポリシーやガイドラインに基づく監査やレビューを実施している企業は22.4%にとどまり、「実施していない」と回答した企業は約2倍の48.0%となりました。企業規模別で監査やレビューの実施率は大きく異なり、従業員が1万人以上の企業では実施率が43.3%でしたが、1万人未満の企業ではその半分以下の実施率にとどまりました。

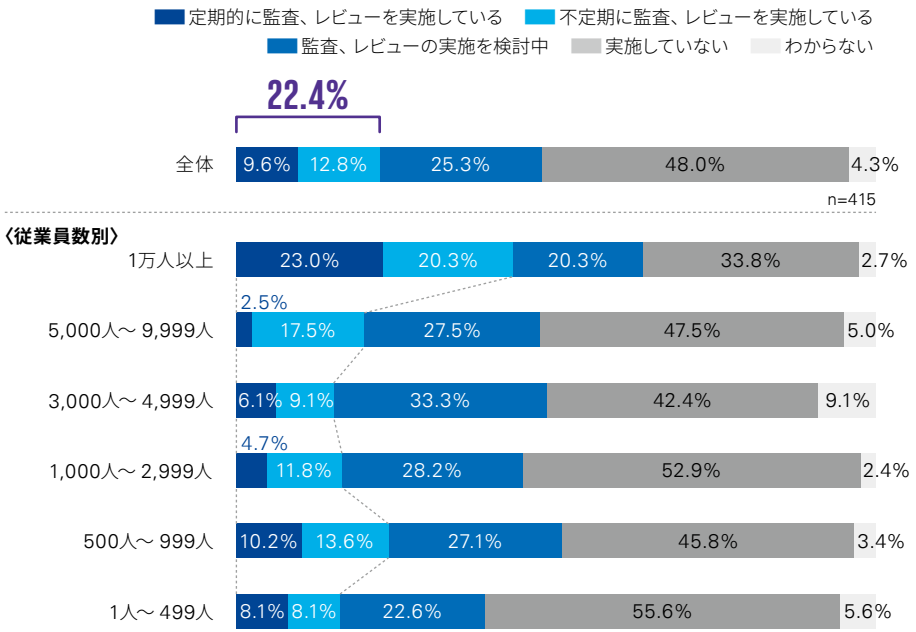
AIサービス利用時のセキュリティ評価の実施は業界により大きな差がある

貴社では、外部のAIサービスを利用する際にセキュリティ評価を実施していますか。



AI利用の監査、レビューを実施している企業は2割程度

貴社ではAI利用について、社内ポリシーやガイドラインに基づく監査やレビューを実施していますか。



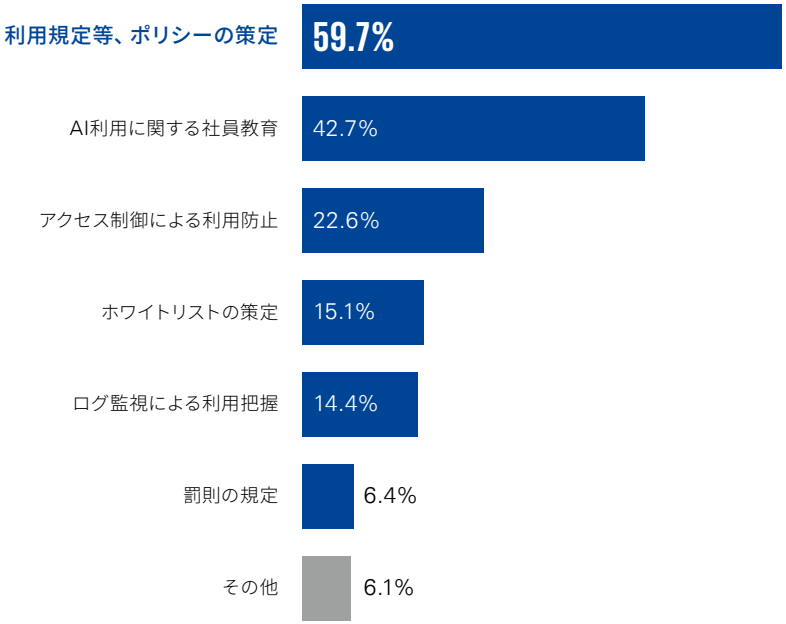
シャドーAIを防ぐための対策

正規に許可されていないAIツールの業務利用を防ぐための対策として、実施率が最も高かったのは「利用規程等、ポリシーの策定」（59.7%）でした。しかし、「AI利用に関する社員教育」は42.7%にとどまり、規定したポリシーが十分に徹底されていないおそれがあります。また、「アクセス制御による利用防止」も約2割にとどまりました。

「利用規定等、ポリシーの策定」の実施状況を業種別にみると、「運輸・インフラ」では84.6%が実施しており、「通信・IT・メディア」「製造」も比較的高い水準となりました。「流通」「旅行・レジャー・飲食」では40%台にとどまり、業種間で対応の差が顕著となりました。

シャドーAIの防止策として利用規定等、ポリシーを策定した企業が約6割

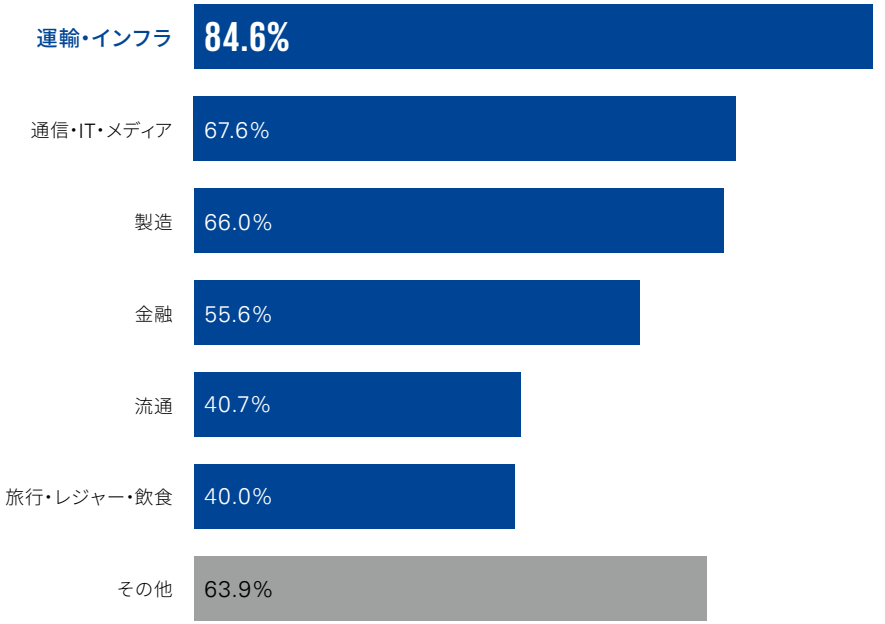
貴社では、シャドーAI（正規に許可されていないAIツールの業務利用）を防ぐための対策を実施していますか。



n=424

「運輸・インフラ」は9割近くが利用規定等、ポリシーの策定を行っている

左記の「利用規定等、ポリシーの策定」の実施状況を、業種別に分析



n=418

コラム｜AI活用の進展とAIセキュリティの現在地

AI導入の価値を高めるAIセキュリティ体制の構築が重要。AI活用の拡大と合わせて、AIの管理・監督にも注目すべき

AIの急激な進化・浸透とともに、AIセキュリティが最重要課題となっています。

これに対し、AI倫理をはじめとして、テクノロジーのうえにAIガバナンスを整備、「AIが間違っても社会と事業を守る」を理念として、加速して対策を進めています。

富士通株式会社
執行役員常務　CISO　太田 雅浩

AI活用が広がるなかで、仕事の在り方は大きく変わりつつあります。日常的なサービスにもAIが組み込まれるため、利便性の享受と同時に、見えにくいリスクへの備えが不可欠となります。個人のリテラシー向上と、組織としての統制基盤の整備を両輪で進めることが求められます。

KPMGコンサルティング株式会社
執行役員　パートナー　一原 盛悟

AI活用の拡大と遅れるセキュリティ対策

業務効率化やデータ分析・予測といった分野を中心に、企業におけるAI活用は着実に進展しています。

一方、セキュリティ対策領域でのAI導入は「導入を検討中」が最多となっており、AI活用の広がりに対してセキュリティ面の対応が後追いとなっている実態がうかがえます。特に外部AIサービス利用においても、業種によってセキュリティ評価の実施頻度が大きく異なり、必ずしも十分にセキュリティ評価が実施されていない業界も存在することが明らかになりました。これは各業界における規制環境の影響のほか、実際に導入されているAIの用途が限定的である等の理由が考えられます。
また、組織内でのAI利用に際し、社内ポリシーの策定や社員教育といった施策は実施されつつあるものの、ホワイトリスト作成やログ監視といった技術的な対応や監査等について未実施とする企業の割合が多く、セキュリティ対策の実効性の確保が依然として大きな課題であるとみられます。

今後は、AI導入そのものだけでなく、「どのように管理・監督するか」まで含めたAIセキュリティ体制の構築が、AI導入の投資効果の最大化、ひいては企業価値の向上を左右する大きな要素となると考えられます。

コメント・コラム執筆者 順不同・敬称略

コメント執筆者

福本 佳成
楽天グループ株式会社
上級執行役員

松下 忍
株式会社三菱UFJフィナンシャルグループ
常務執行役員グループCISO

葛西 洋一
株式会社ニコン
常務執行役員　CRO、CISO

谷澤 憲治
ソニー株式会社
Executive Information Security Officer
EISO Office室長情報セキュリティ部 統括部長

飯田 唯史
ソフトバンク株式会社
常務執行役員 兼CISO 兼CRO
リスクマネジメント室長

太田 雅浩
富士通株式会社
執行役員常務　CISO

コラム執筆者

KPMGコンサルティング株式会社

澤田 智輝
執行役員　パートナー

関 憲太
執行役員　パートナー

一原 盛悟
執行役員　パートナー

稲村 大介
執行役員　パートナー

川合 恵巳
アソシエイトパートナー

有限責任 あずさ監査法人

山口 達也
パートナー

近藤 純也
ディレクター

株式会社KPMG Forensic＆Risk Advisory

上原 豊史
執行役員　パートナー

遠藤 正樹
執行役員　パートナー

KPMGジャパンのサイバーセキュリティサービス

KPMGジャパンでは、以下のサービスを中心にサイバーセキュリティに関連する
さまざまな支援を実施しています。支援内容はホームページからもご確認いただけます。

kpmg.com/jp/cyber-security

サイバーストラテジー＆ガバナンス

新たなセキュリティリスクに対応するための管理態勢の構築・強化、戦略・方針策定、各種公的認証基準への準拠・維持・審査を支援します。

制御システム／IoTセキュリティ

スマート化する産業用制御システム、IoTサービスのシステムに求められるサイバーセキュリティ対策を支援します。

サイバーインシデントレスポンス

サイバーインシデントの発生時に、初動対応のサポート、侵入経路や原因・被害範囲の特定を目的としたフォレンジック調査、広報支援などのサービスを提供します。

サイバーディフェンス

サイバーセキュリティリスクに対し、テクノロジーの導入やアセスメント、アーキテクチャデザインなど技術的な視点から包括的に支援します。

オートモーティブサイバーセキュリティ

IT／OA、車両／製品、工場／FAの3領域にわたり、オートモーティブに関するサイバーセキュリティ全般を支援します。

サイバーフォレンジック

サイバーインシデントが発生した際の重要なプロセスである証拠保全、および被害内容の特定などの詳細分析について支援します。

プライバシー＆データ規制

グローバル企業における世界各国のデータ保護規制対応に関するサービスをはじめ、プライバシーに関するさまざまなサービスを提供します。

防衛・宇宙

防衛・宇宙に精通したプロフェッショナルが、KPMGの海外組織とも連携し、経営課題の解決を支援し、産業の成長に貢献します。

サイバーデューデリジェンス

ITデューデリジェンスのみならず、サイバーセキュリティやプライバシーリスクも交えた支援を行います。

ISMAP監査支援

ISMAPクラウドサービスリストへ登録された、もしくはこれから登録を目指す企業に、ISMAP監査基準に基づく監査を提供し、ガバナンス・マネジメント・セキュリティ対策状況を確認します。

Powered Enterprise Cyber

KPMGのソリューションである「Powered Enterprise Cyber」を活用し、デジタル時代のサイバーセキュリティ対策を支援します。

AIセキュリティ

AI活用時のセキュリティの強化におけるリスク評価や対策検討および組織のセキュリティ対策におけるAI活用の計画策定や導入を支援します。

お問合せ先

KPMGジャパン

有限責任 あずさ監査法人　KPMGコンサルティング株式会社　株式会社KPMG Forensic & Risk Advisory

kc@jp.kpmg.com
kpmg.com/jp/cyber-security

本レポートで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはKPMGコンサルティング株式会社までお問い合わせください。