



Cyber Security Survey

2026/27 速報版

2026年10月

KPMGジャパン

Contents

エグゼクティブサマリー	P.04
-------------	------

01	サイバー攻撃の実態	P.07
----	-----------	------

02	サイバーセキュリティ管理態勢	P.13
----	----------------	------

03	子会社管理	P.17
----	-------	------

04	委託先・取引先管理	P.23
----	-----------	------

05	サイバーセキュリティ対策	P.27
----	--------------	------

06	AIセキュリティ	P.34
----	----------	------

KPMGジャパンの サイバーセキュリティサービス	P.42
-----------------------------	------

調査概要

名称 企業のサイバーセキュリティへの取組みに関する調査

対象 国内上場企業および売上高1,000億円以上の
未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 2026年6月29日～8月12日

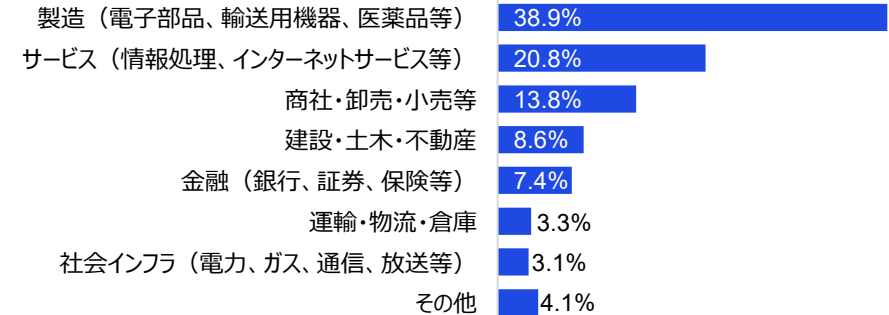
調査方法 郵送およびウェブによるアンケートの回収

調査依頼数 4,402社

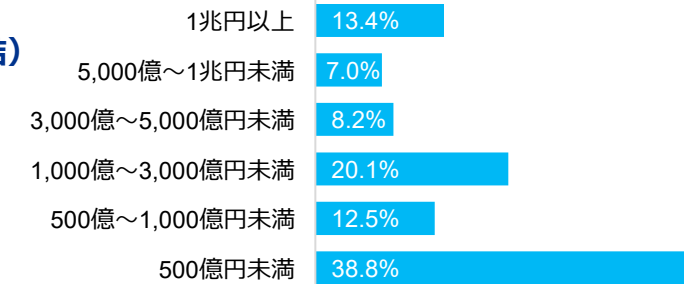
有効回答数 420社（回収率9.5%）

回答企業の属性

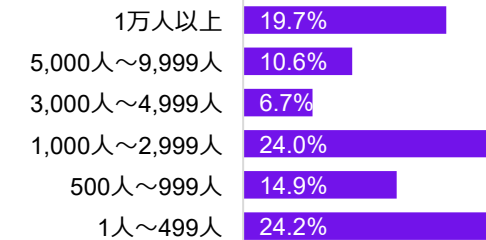
■ 業種



■ 売上高 （2025年度連結）



■ 従業員数 （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

各章のサマリー (1/2)

1

サイバー攻撃の実態

- サイバーインシデントの被害が高額化し、年間10億円以上の損失も発生
- インシデントにより経済的な損失と情報漏えいの被害が増加
- 生成AIの悪用が想定されるフィッシング等の攻撃が増加
- 委託先・取引先経由の被害が多く、管理強化が課題

2

サイバーセキュリティ 管理態勢

- 過半数の企業がセキュリティ予算を増加させているが、4割超はセキュリティの中期計画を未策定
- 売上高に対するサイバーセキュリティ投資比率は、0.1%未満が最多
- 9割弱の企業でサイバーセキュリティ推進組織の人員が不足
- サイバーセキュリティ推進組織の専任人数は約半数の企業で「0人」

3

子会社管理

- 国内子会社では本社主導の管理が進む一方、小規模企業ではグループ会社の管理が不十分
- 国内子会社ではグループ共通のCSIRT・SOCや情報システム資産管理が進展
- 海外子会社では対策や運用を各社に委ねる傾向が強い
- 海外子会社ではセキュリティの評価や教育・訓練が遅れている

各章のサマリー (2/2)

4

委託先・取引先 管理

- 委託する業務・サービスや預ける情報に応じた管理指針の整備は約3割にとどまる
- 委託先選定時のセキュリティ対策アンケート取得は4割弱にとどまる
- システム等を利用した委託先の対策状況の一元管理は1割未満
- SCS評価制度への関心は高く、5割超の企業が参照している

5

サイバーセキュリティ 対策

- バックアップ対策、資産管理、脆弱性管理、アイデンティティ／アクセス管理の導入が進みつつあるが、運用面で課題を抱える企業が多い
- インターネット公開システムでも約5割が緊急度が高いパッチを1か月以内に適用できていない
- ゼロトラスト導入は8割超で進む一方、サイバーBCP策定は約3割にとどまる

6

AIセキュリティ

- 生成AIはほぼ全ての企業で活用され、AIエージェントの導入も進展
- AIセキュリティの責任者や推進体制が未整備な企業が依然として多い
- AIエージェントに対しては、ガバナンスの整備や全社的な可視化が課題
- セキュリティ運用でのAI活用は、インシデント対応や脆弱性診断に高い期待が集まる

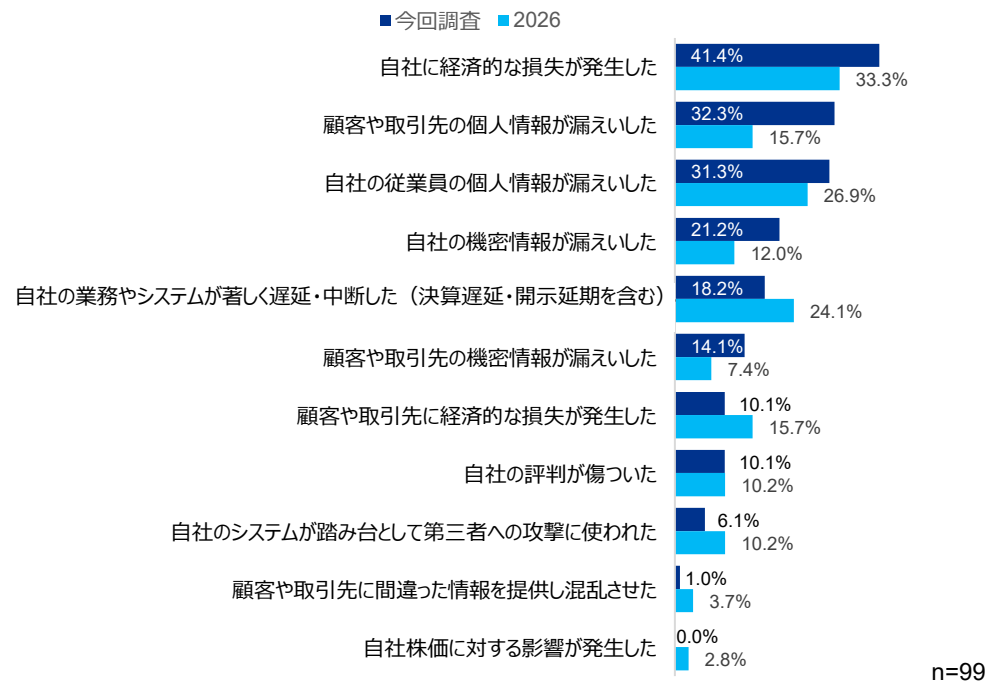


サイバー攻撃の実態

サイバーインシデントによって発生した被害

サイバーインシデントによって業務上の影響のあった企業の約4割で「自社に経済的な損失が発生」していたことがわかりました。また、約3割の企業で顧客・取引先または自社の従業員の個人情報が漏えいしていることがわかりました。前回調査と比較すると、自社への経済的な損失の発生や、個人情報や機密情報の漏えいといった被害が増えていました。「自社の業務やシステムが著しく遅延・中断した」との回答率は前回調査よりも低くなっていますが、

サイバーインシデントによる業務上の影響があった企業の約4割で、経済的損失が発生
過去1年間に発生したサイバーインシデントで、どのような被害がありましたか。（複数回答可）

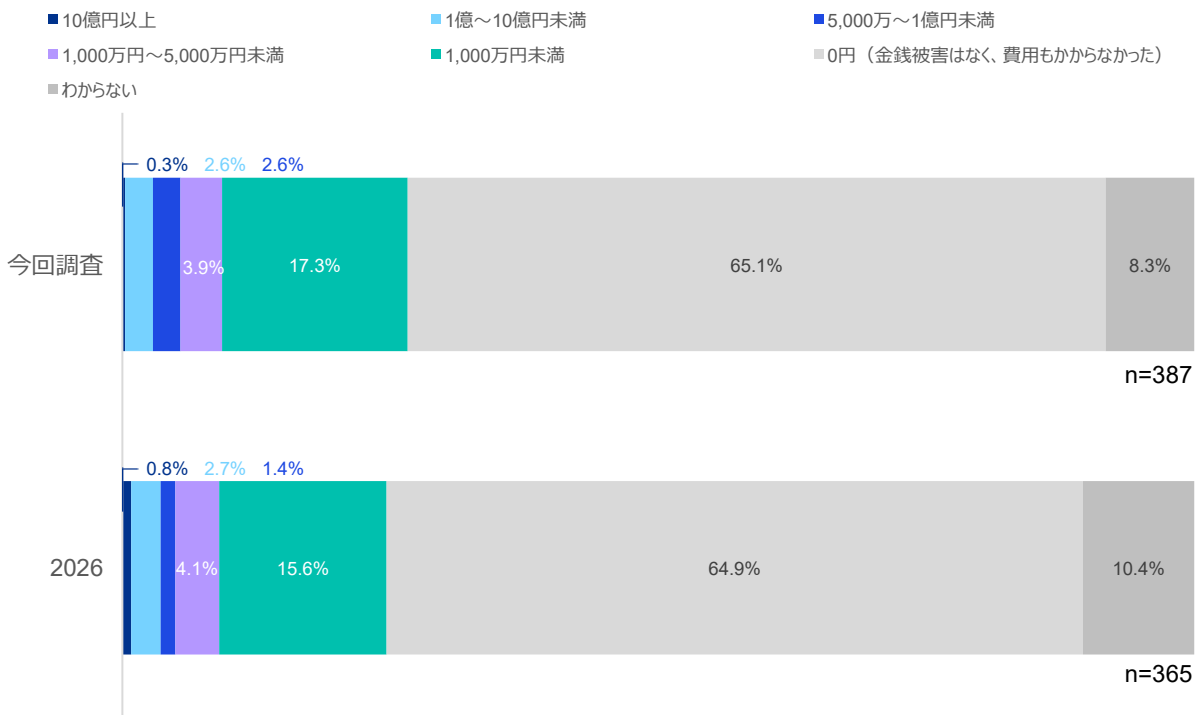


近年、業務のシステム依存度が高まっていることから、被害が発生した場合には、多大な影響が生じることが想定されます。

過去1年間に発生したサイバーインシデントの合計損失額の割合は前回調査と同様となりました。また、前回調査と同様に今回も合計損失が「10億円以上」となったとの回答を得ました。

前回調査と同様に、年間10億円以上の損失が発生

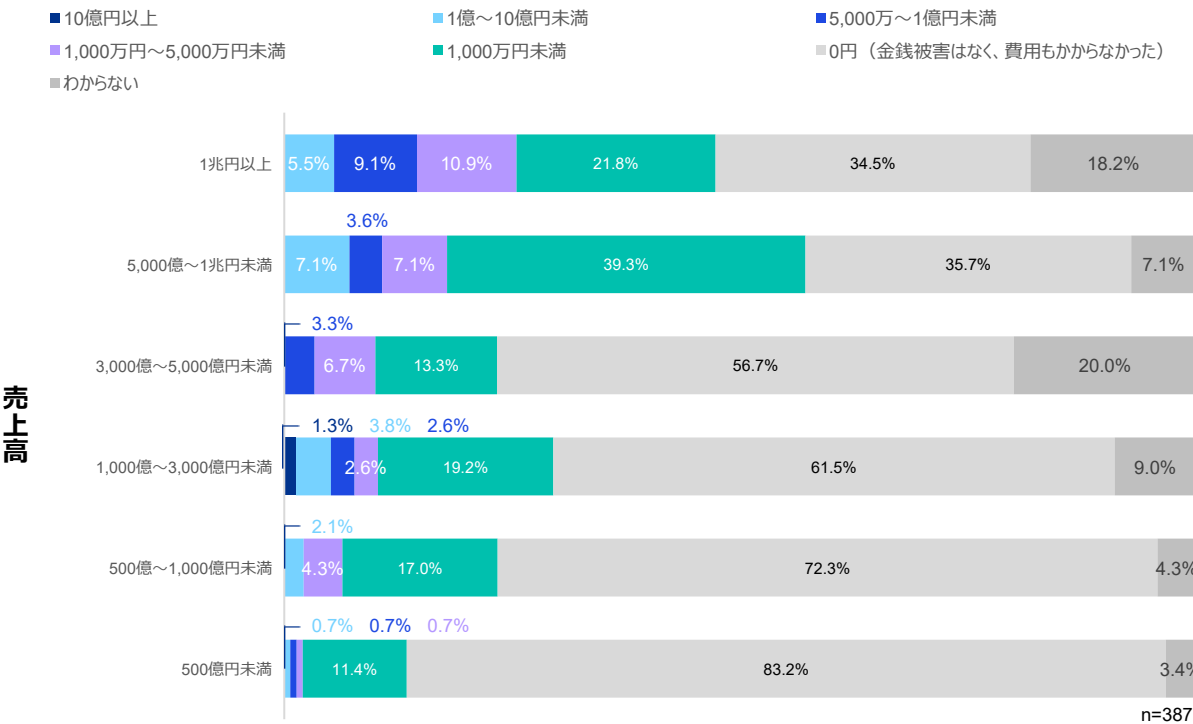
過去1年間に発生したサイバーインシデントで、どのくらいの合計損失がありましたか。



インシデントによって発生した被害（売上高別／業種別）

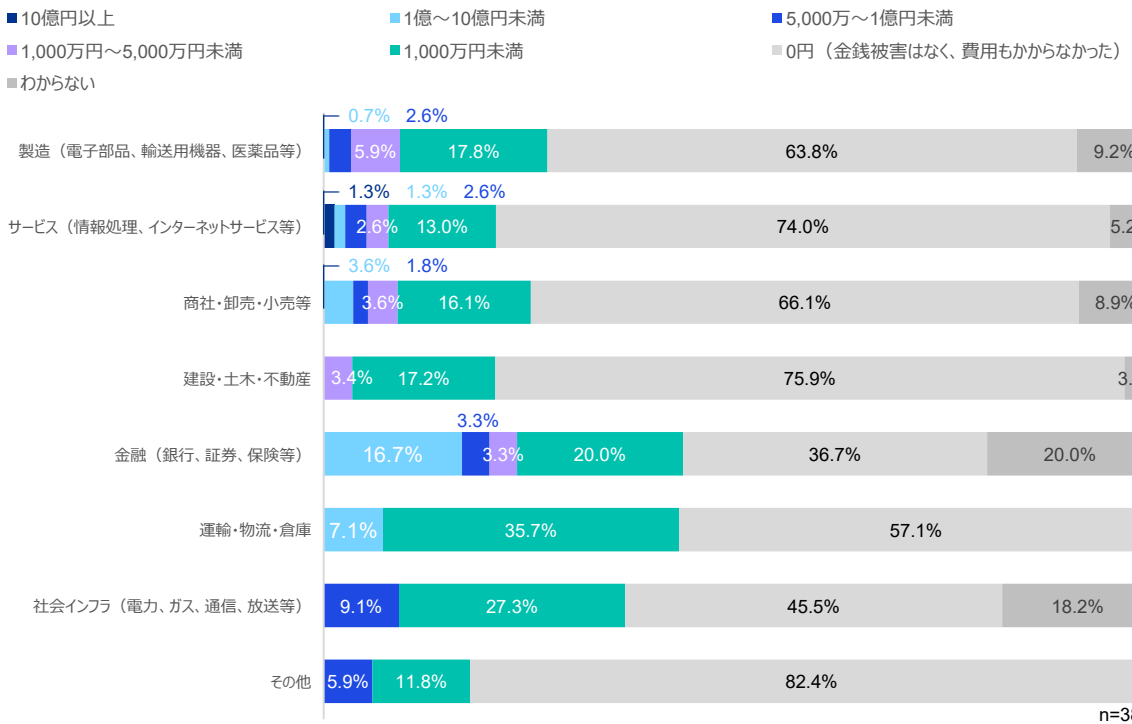
過去1年間に発生したサイバーインシデントの合計損失が1,000万円以上となった割合は、おおむね売上高が高いほど割合が上昇する傾向がみられました。また、「10億円以上」の合計損失は、売上高1,000億～3,000億円未満の企業で発生しており、売上規模にかかわらず発生し得ることが確認されました。

年間合計が1,000万円以上の損失はおおむね売上高が高いほど割合が上昇する傾向
過去1年間に発生した合計損失額を売上高別に分析



過去1年間の合計損失額を業種別に分析すると、「1億円以上」の損失額となった比率が高い順に、金融、運輸・物流・倉庫、商社・卸売・小売等となりました。特に、金融においては、16.7%に上ったことがわかりました。

年間の合計損失が1億円以上となった比率は金融、運輸・物流・倉庫で高い
過去1年間に発生した合計損失額を業種別に分析

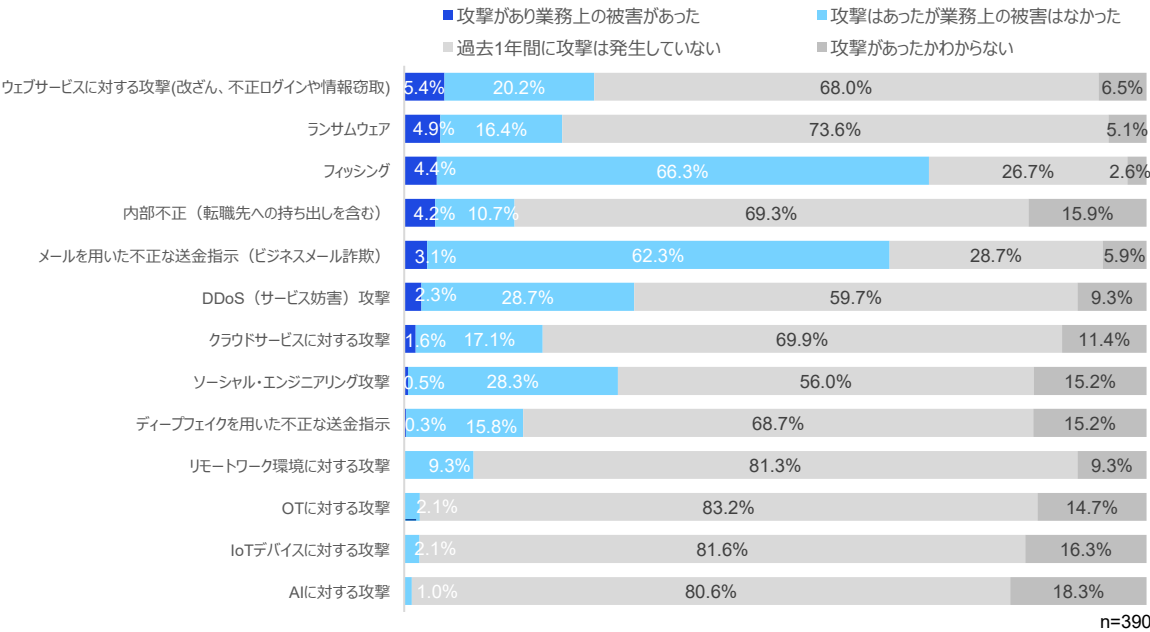


インシデントの発生要因（攻撃手法および攻撃対象）

業務上の被害があったサイバー攻撃はウェブサービスに対する攻撃と回答した企業が5.4%となり最も高くなりました。ランサムウェアは、「攻撃があり業務上の被害があった」との回答は4.9%となり、前回調査の6.9%より低くなりましたが、「攻撃はあったが業務上の被害はなかった」は、前回調査の15.4%から16.4%へ上昇したことが確認されました。

ウェブサービスに対する攻撃による被害が最も多い

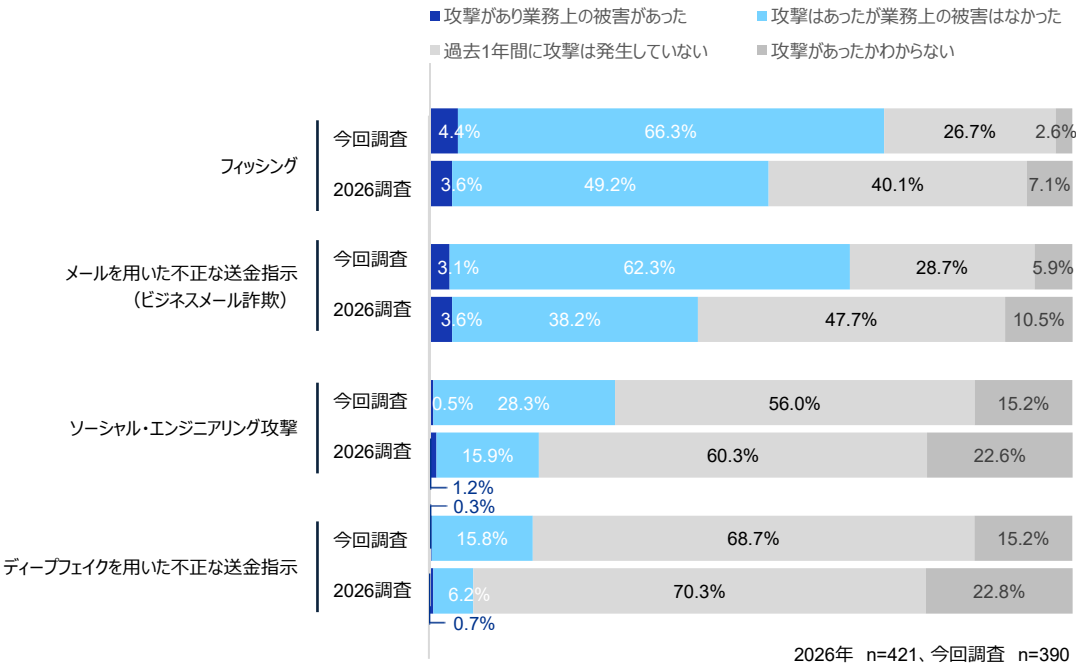
過去1年間に発生したサイバーインシデントをもたらした直接的な要因（攻撃手法および攻撃対象）と事業上の被害の有無についてご回答ください。



生成AIを用い、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。

生成AIを用いた攻撃の巧妙化

生成AIの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

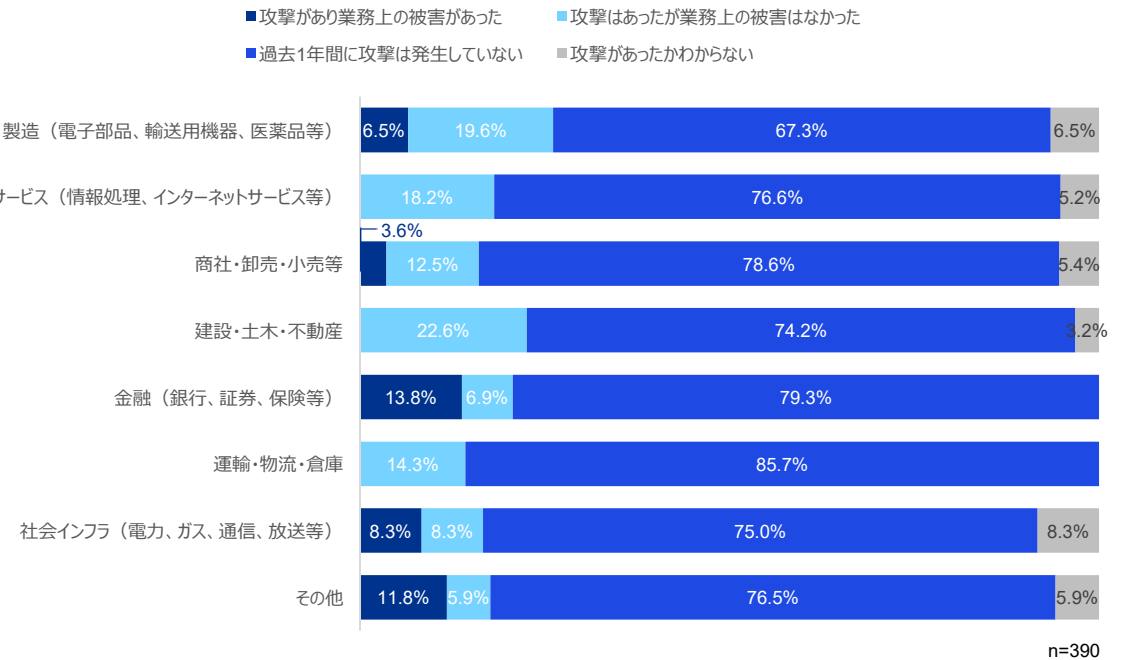


インシデントの発生要因（業種別分析）

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、業種別に分析すると、金融、社会インフラ、製造で被害が多くなりました。ただし、前回調査と比較すると金融での「攻撃があり業務上の被害があった」は、16.7%から13.8%に減少しているなど、改善がみられました。

ランサムウェアは金融、社会インフラ、製造での被害が多い

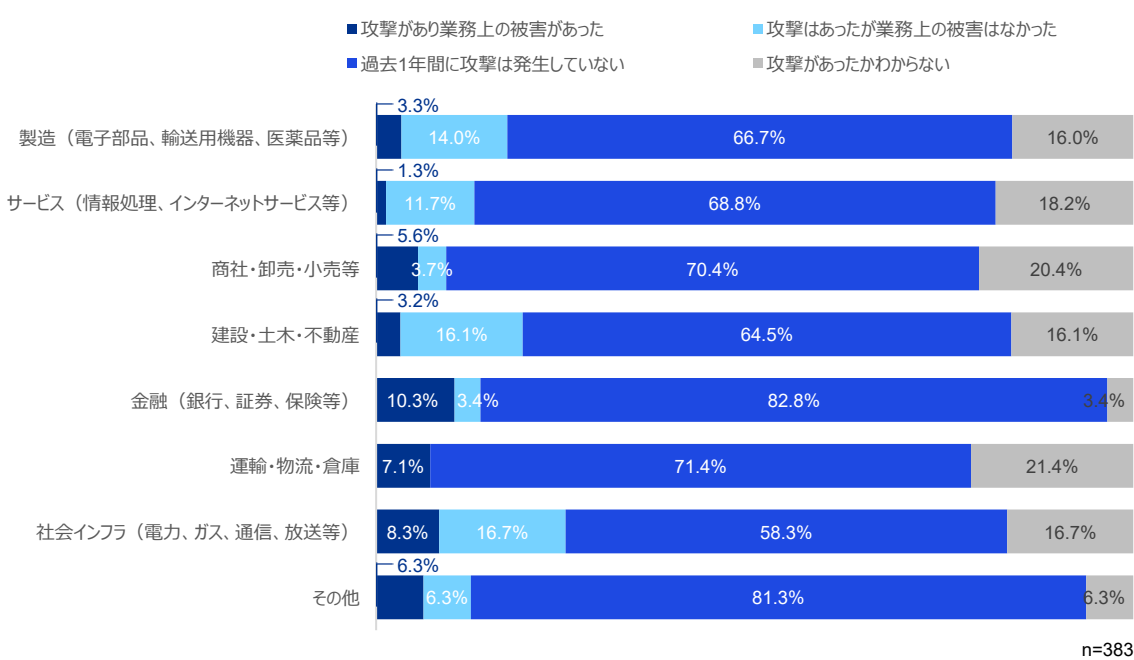
過去1年間に発生したランサムウェア攻撃による事業上の被害の有無について、業種別に分析



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、金融、社会インフラ、運輸・物流・倉庫において「攻撃があり業務上の被害があった」の比率が高いことがわかりました。特に、金融においては、前回調査の0.0%から10.3%と大幅に伸びていることが確認されました。

内部不正は、金融、社会インフラ、運輸・物流・倉庫での被害が多い

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、業種別に分析

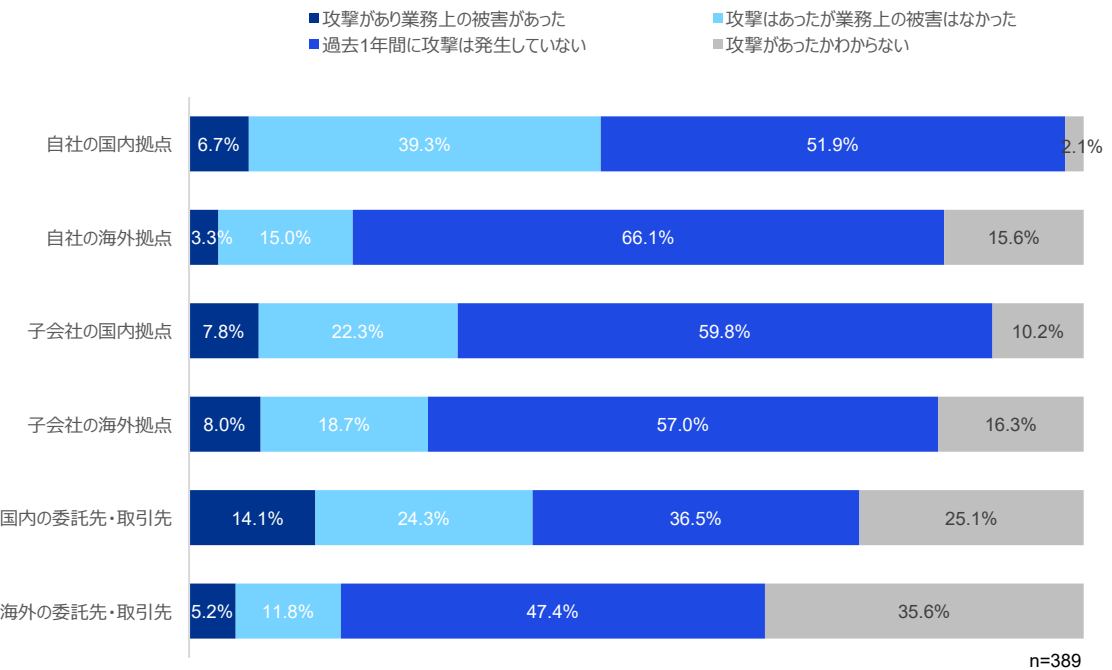


インシデントの発生経路

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して、国内の委託先・取引先との回答が最も多く、14.1%となりました。前回調査と比較すると国内の委託先・取引先経由での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」が10.8%から上昇しているとともに、「攻撃はあったが業務上の被害はなかった」も16.4%から24.3%と伸びていることが確認されました。

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

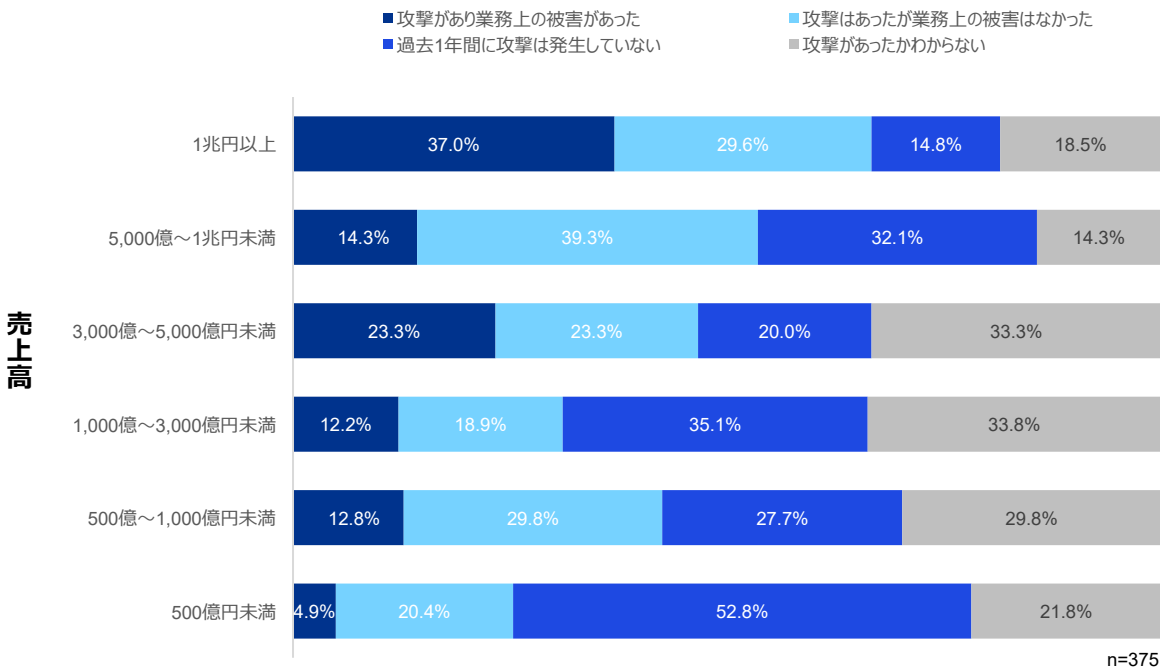
過去1年間に発生したサイバーインシデントをもたらした経路と事業上の被害の有無についてご回答ください。



国内の委託先・取引先経由でのサイバーインシデントについて、売上高別に比較したところ、売上1兆円以上の企業の4割弱において、「攻撃があり業務上の被害があった」と回答していることがわかりました。また、売上500億円～5,000億円未満の企業では約3割が「攻撃があったかわからない」と回答しており、契約に報告義務を盛り込むことも検討すべきです。

売上1兆円以上の企業では、約4割で国内の委託先・取引先でのインシデントが発生

過去1年間に発生した国内の委託先・取引先を経路としたサイバーインシデントの業務上の被害について、売上高別に分析





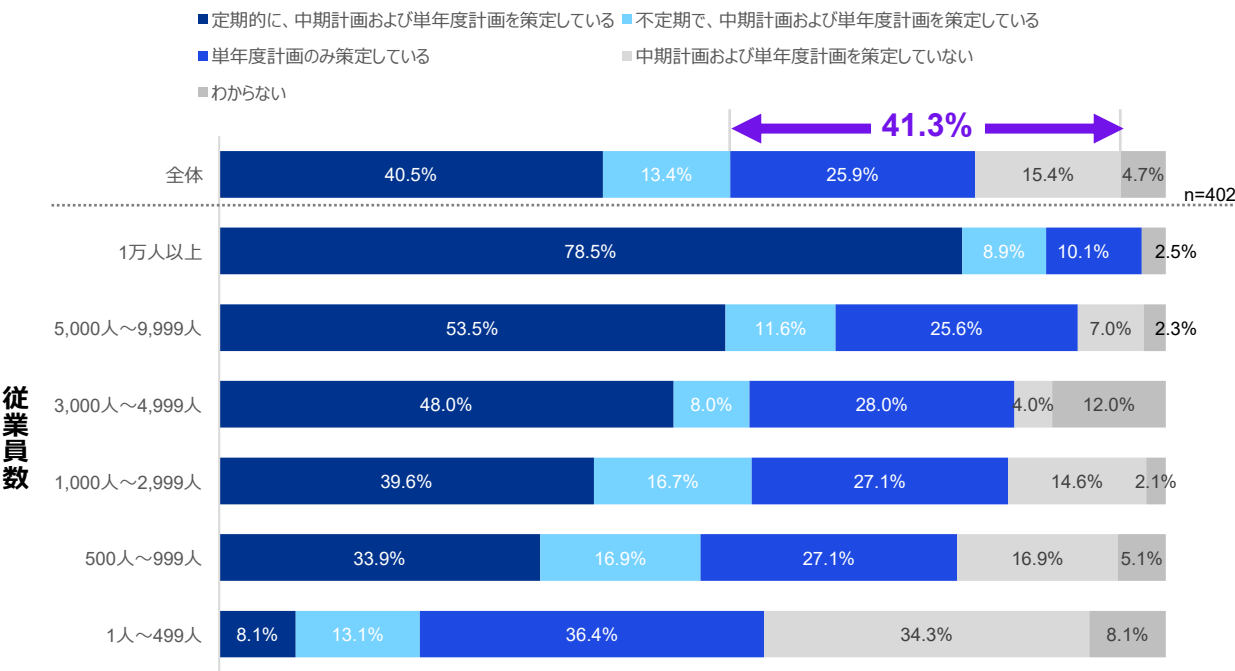
サイバーセキュリティ管理態勢

サイバーセキュリティ計画、予算の状況

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（44.4%）より若干減りましたが、引き続き41.3%と高い水準にとどまっています。

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

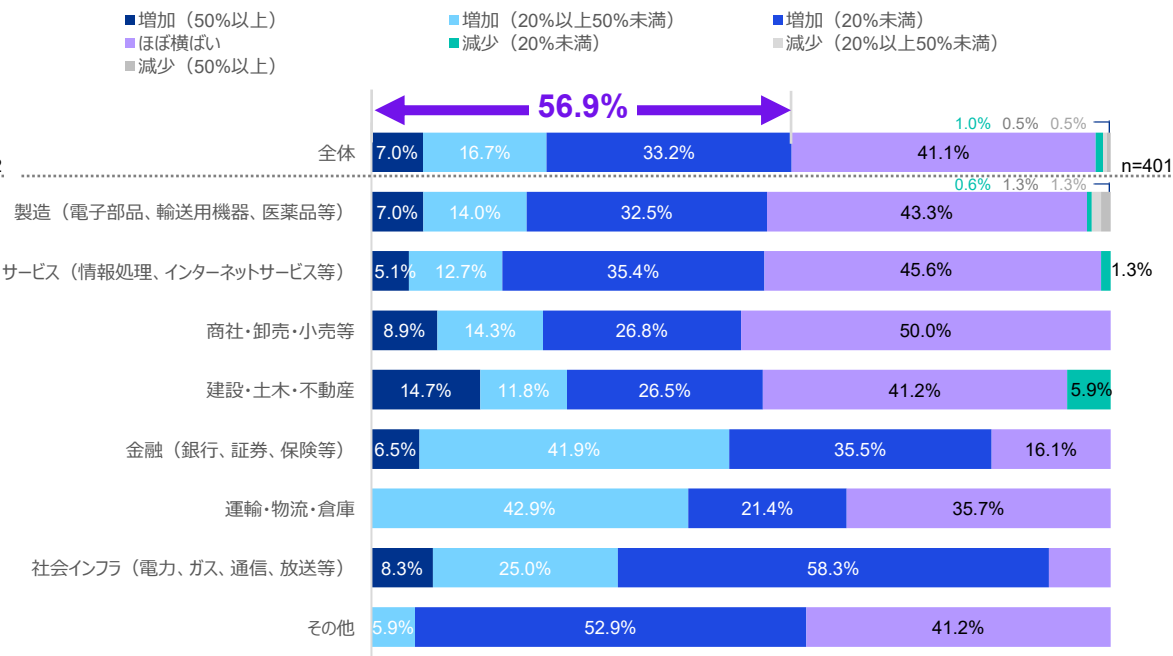
サイバーセキュリティの中期計画、単年度計画を策定していますか。



サイバーセキュリティ投資（予算額）を昨年比で増加させているとの回答は、56.9%となりました。業種別にみると、20%以上増加したとの回答比率は、金融（48.4%）、運輸・物流・倉庫（42.9%）、社会インフラ（33.3%）の順で高くなりました。

5割以上の企業でサイバーセキュリティ予算を増加させている

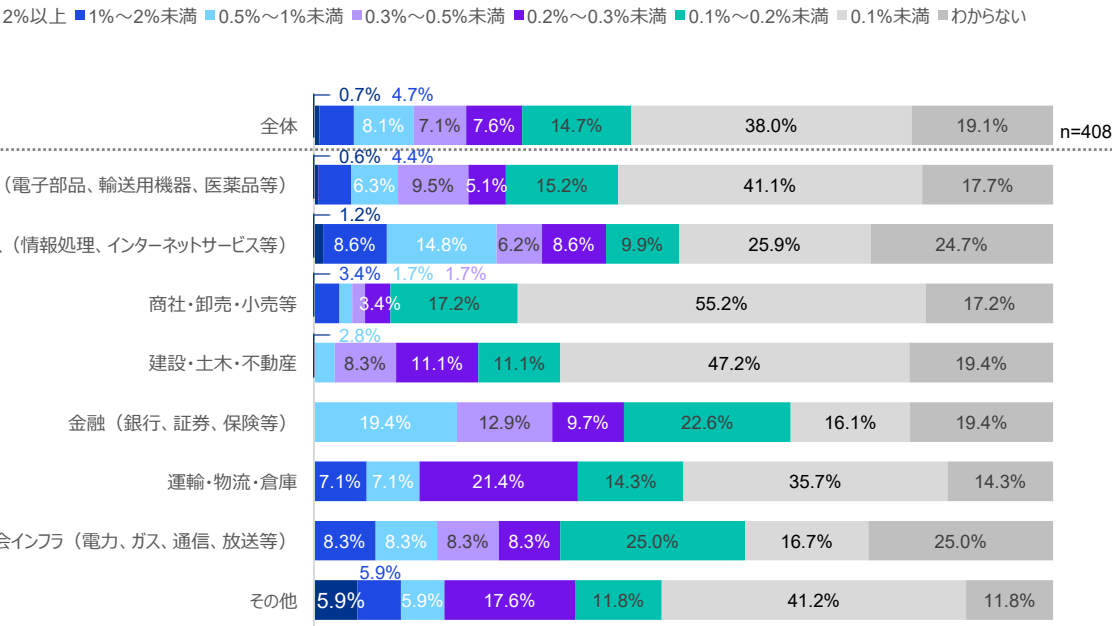
サイバーセキュリティ投資（予算額）は昨年比どの程度増加／減少していますか。



サイバーセキュリティ予算の比率

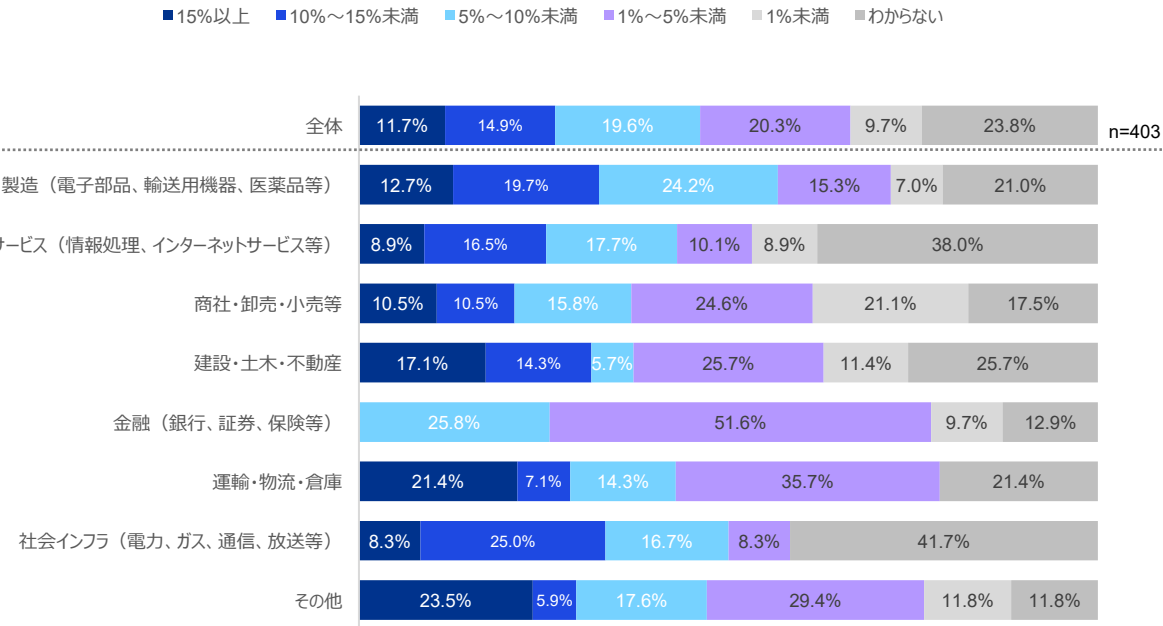
全体では、サイバーセキュリティ投資（予算額）は売上高の「0.1%未満」との回答が最も多く、38.0%となりました。また、業種別にみると、「売上の1%以上」をサイバーセキュリティに投資しているとの回答は、サービス（9.9%）、社会インフラ（8.3%）、運輸・物流・倉庫（7.1%）の順で高くなりました（その他を除く）。

サービスでは約1割が売上高の1%以上をサイバーセキュリティに投資している
サイバーセキュリティ投資（予算額）は売上高に対し何%ですか。



IT投資比では「わからない」を除くと、「1%～5%未満」との回答（20.3%）が最も高くなりました。IT投資の15%以上をサイバーセキュリティに投資しているとの回答は、運輸・物流・倉庫（21.4%）、建設・土木・不動産（17.1%）、製造（12.7%）の順で高くなりました（その他を除く）。

運輸・物流・倉庫では2割超がIT投資の15%以上をサイバーセキュリティに投資している
サイバーセキュリティ投資（予算額）はIT予算に対し何%ですか。

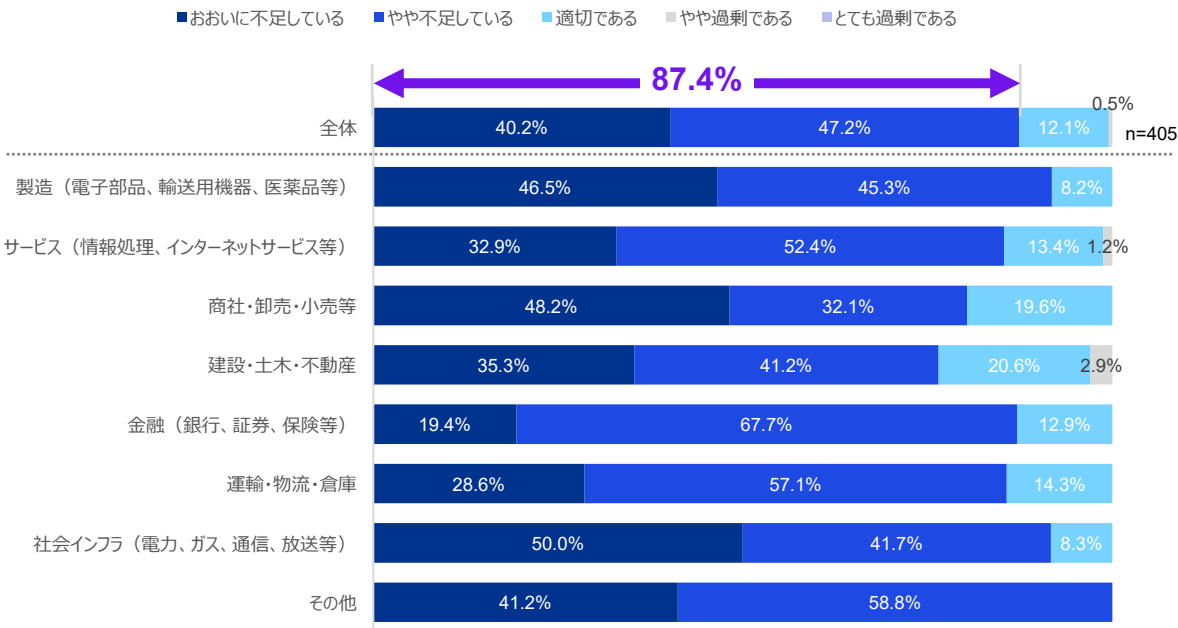


サイバーセキュリティ推進組織の人員

サイバーセキュリティ推進組織の人員が「おおいに不足している」「やや不足している」との回答は87.4%となり、前回調査（89.1%）に続き、要員不足が高い水準にあることがわかりました。特に、製造（91.8%）、社会インフラ（91.7%）、金融（87.1%）にて要員の不足感が強い傾向がみられます。

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

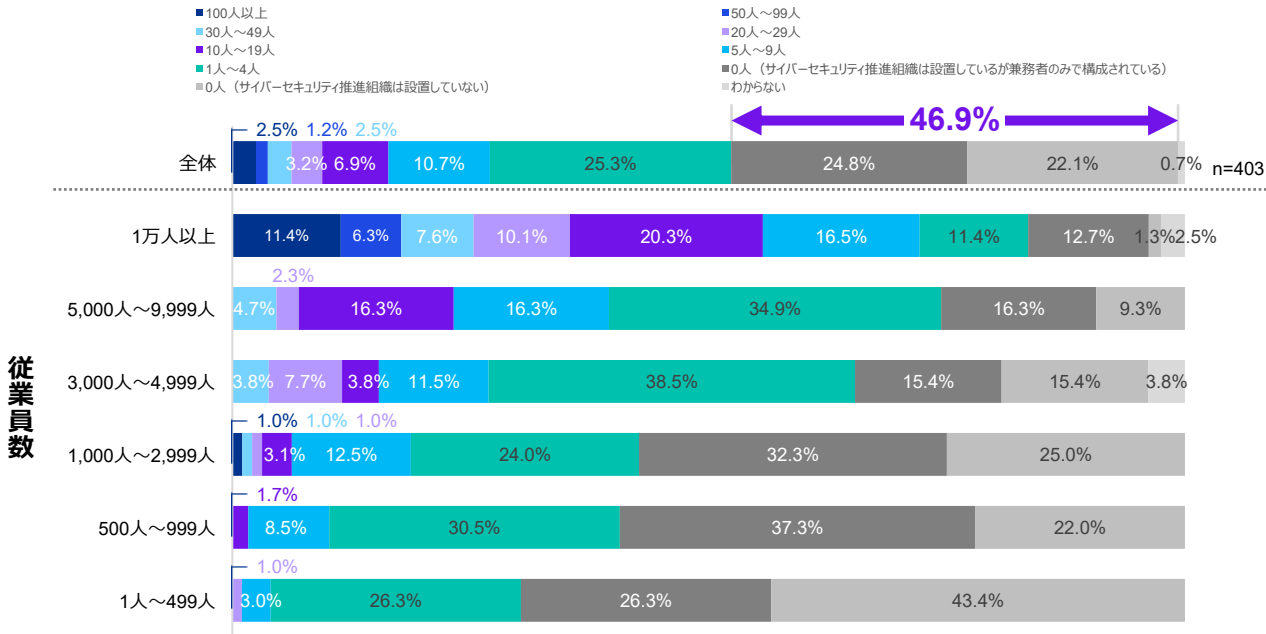
サイバーセキュリティ組織の人員規模は、適切だと思いますか。



サイバーセキュリティ推進組織の専任人数としては、「0人」との回答が46.9%を占めており、特に、従業員数が3,000人未満の企業では専任の要員の配置が難しく、半数以上の企業で「0人」となっていることがわかりました。

約半数の企業で専任者が0人

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。



03

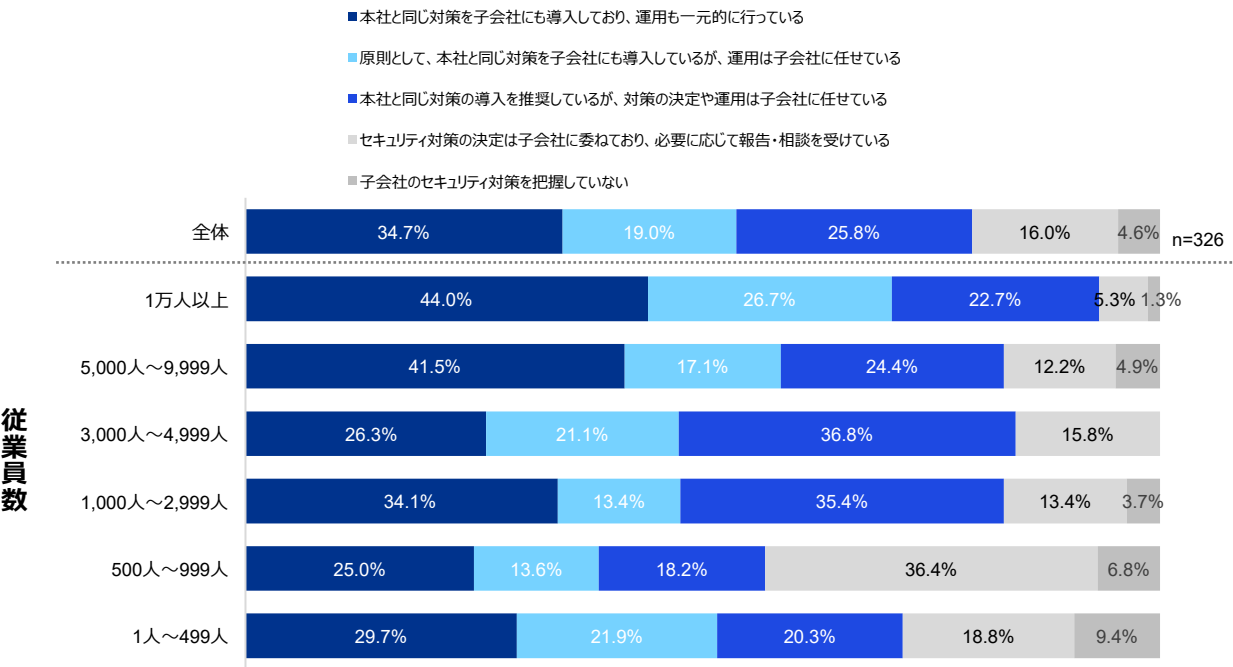
子会社管理

国内子会社に対するサイバーセキュリティ管理 1/2

国内子会社に対するセキュリティ対策の方針は、「本社と同じ対策を子会社にも導入しており、運用も一元的に行っている」が最も多く、回答企業の34.7%となりました。従業員数が少ない企業ほど「セキュリティ対策の決定は子会社に委ねており、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対策を把握していない」という回答割合が増え、小規模の企業において子会社の管理が行き届いていない傾向がみられました。

国内子会社に本社と同じ対策を導入している企業は5割強

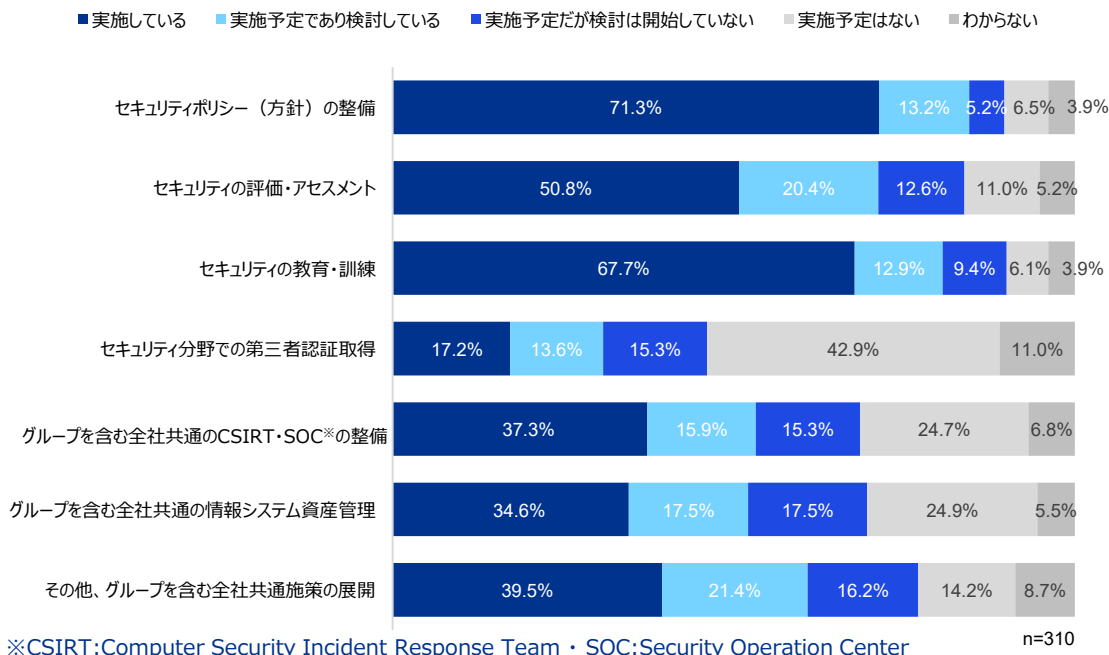
国内子会社におけるセキュリティ対策の方針について、最も近いものを選択してください。



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・訓練が実施されています。また、3分の1強の企業においてグループを含む全社共通の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す。

グループを含む全社共通のCSIRT・SOCの整備を実施している企業は約4割

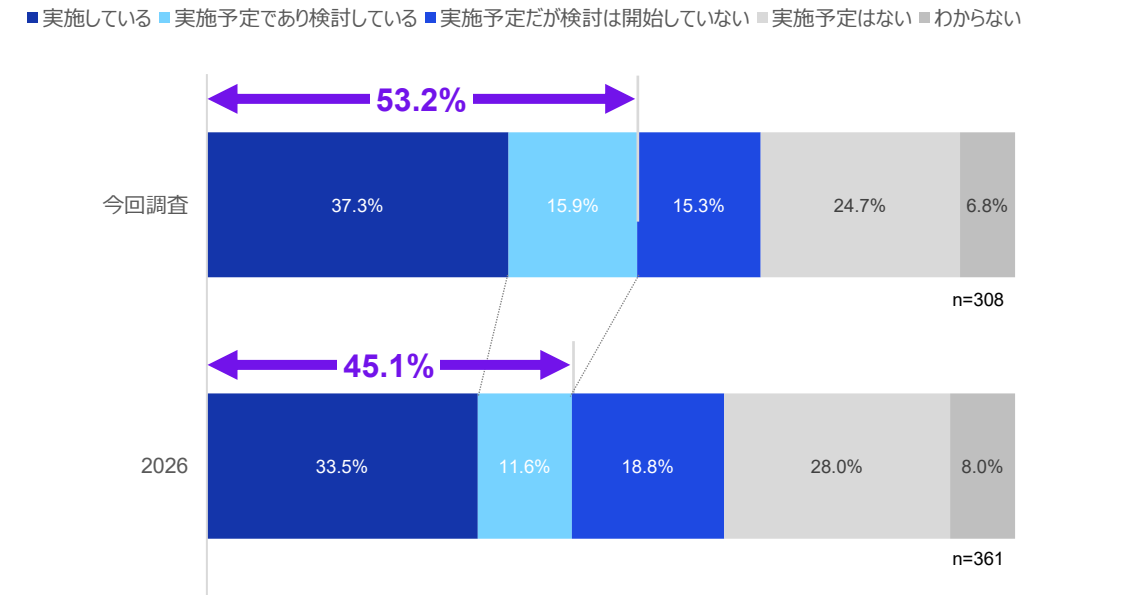
国内子会社管理について、実施・検討している対策を選択してください。



国内子会社に対するサイバーセキュリティ管理 2/2

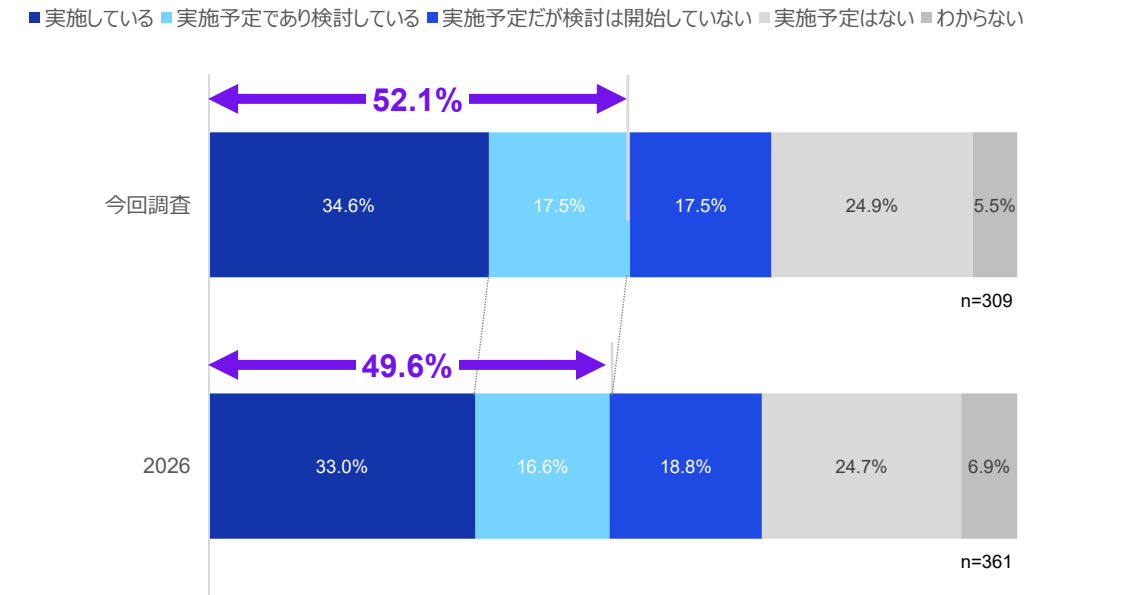
国内子会社に対するグループを含む全社共通のCSIRT・SOCの整備について、「実施している」「実施予定であり検討している」のいずれも前回調査より回答比率が高くなっていることがわかりました。また、「実施予定はない」「わからない」の比率も前回調査と比較して低くなっています。

国内子会社ではグループを含む全社共通のCSIRT・SOCの整備が進んでいる
「グループを含む全社共通のCSIRT・SOCの整備」の実施・検討状況の変化



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も同様に、「実施している」「実施予定であり検討している」のいずれも前回調査より回答比率が高くなっていることがわかりました。また、CSIRT・SOCの整備状況と同様に、「実施予定はない」「わからない」の合計比率も前回調査と比較して低くなっています。

国内子会社はグループを含む全社共通の情報システム資産管理を進めている
「グループを含む全社共通の情報システム資産管理」の実施・検討状況の変化

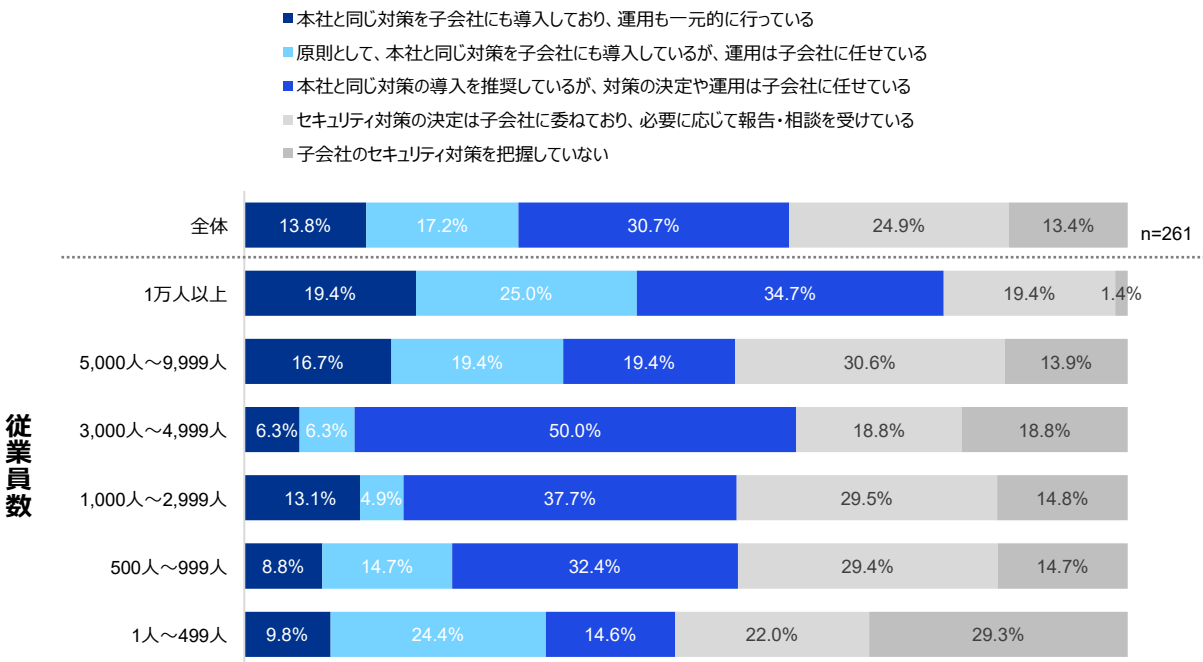


海外子会社に対するサイバーセキュリティ管理 1/2

海外子会社に対するセキュリティ対策の方針は、「本社と同じ対策の導入を推奨しているが、対策の決定や運用は子会社に任せている」が最も多く、回答企業の30.7%となりました。また、「セキュリティ対策の決定は子会社に委ねており、必要に応じて報告・相談を受けている」（24.9%）、「子会社のセキュリティ対策を把握していない」（13.4%）の回答割合も高い傾向がみられました。

海外子会社に本社と同じ対策を導入している企業は3割強

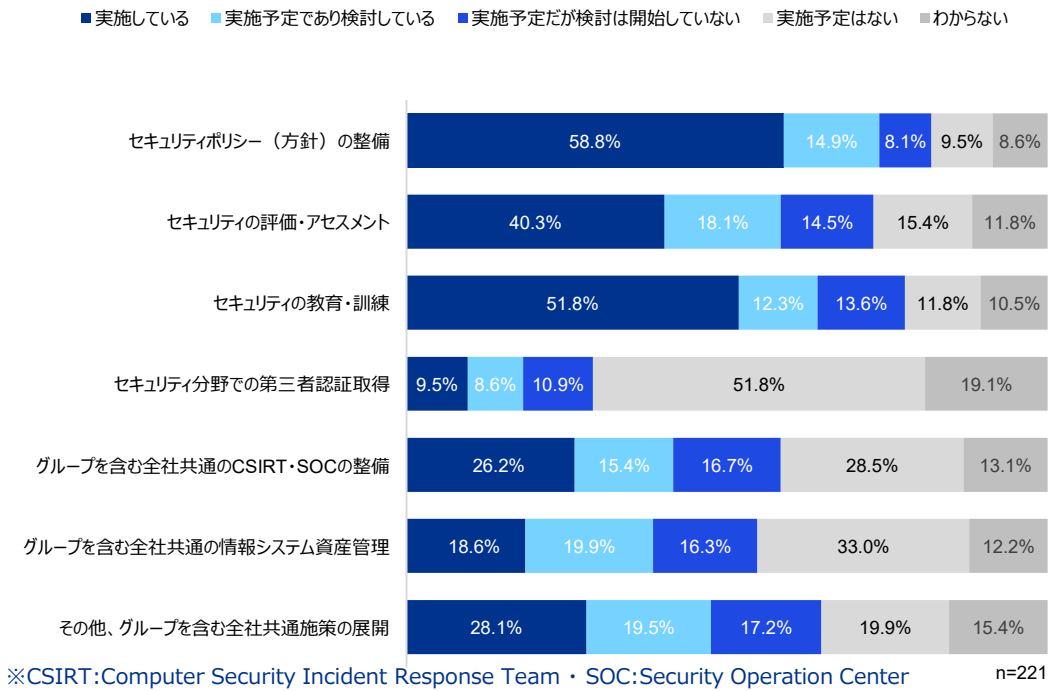
海外子会社におけるセキュリティ対策の方針について、最も近いものを選択してください。



海外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の整備、セキュリティの教育・訓練が実施されていました。セキュリティの評価・アセスメントを「実施している」との回答は、国内子会社では50.8%（P.18）の回答となったのに対し、海外子会社では40.3%にとどまり、国内子会社の管理と比較し対応が遅れている様子がうかがえます。

海外子会社のセキュリティ評価・アセスメントの実施は約4割

海外子会社管理について、実施・検討している対策を選択してください。



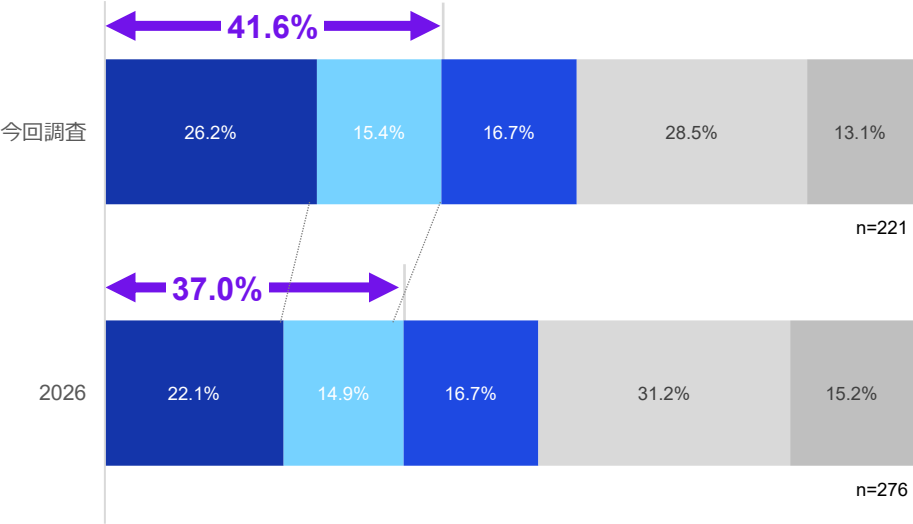
海外子会社に対するサイバーセキュリティ管理 2/2

海外子会社に対するグループを含む全社共通のCSIRT・SOCの整備について、「実施している」「実施予定であり検討している」のいずれも前回調査より回答比率が高くなっていることがわかりました。また、「実施予定はない」「わからない」の比率も前回調査と比較して、低くなっていることがわかりました。

海外子会社の共通CSIRT・SOC整備は前回調査から進展

「グループを含む全社共通のCSIRT・SOCの整備」について、実施・検討状況の変化

■実施している ■実施予定であり検討している ■実施予定だが検討は開始していない ■実施予定はない ■わからない

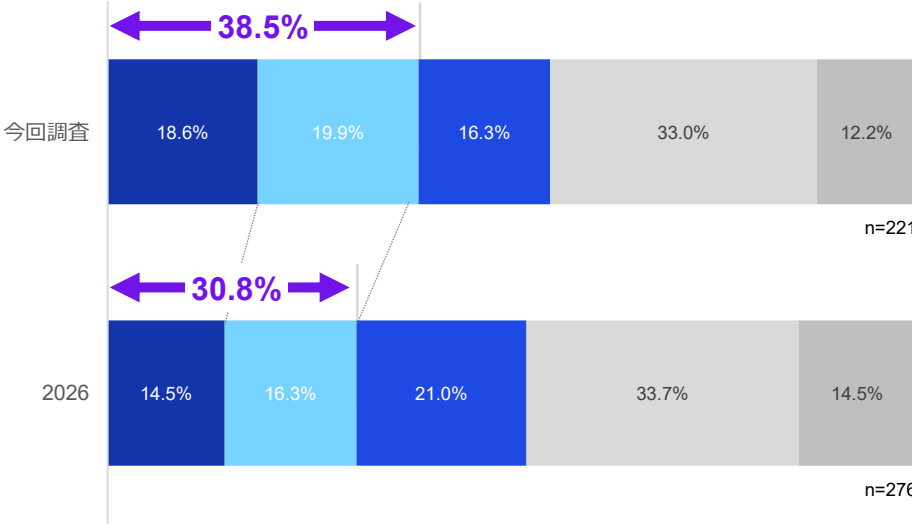


グループを含む全社共通の情報システム資産管理についても同様に、「実施している」「実施予定であり検討している」のいずれも前回調査より回答比率が高くなっていることがわかりました。また、CSIRT・SOCの整備状況と同様に、「実施予定はない」「わからない」の比率も前回調査と比較して、低くなっていることがわかりました。

海外子会社の共通情報システム資産管理、実施・検討が前回調査から進展

「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、実施・検討状況の変化

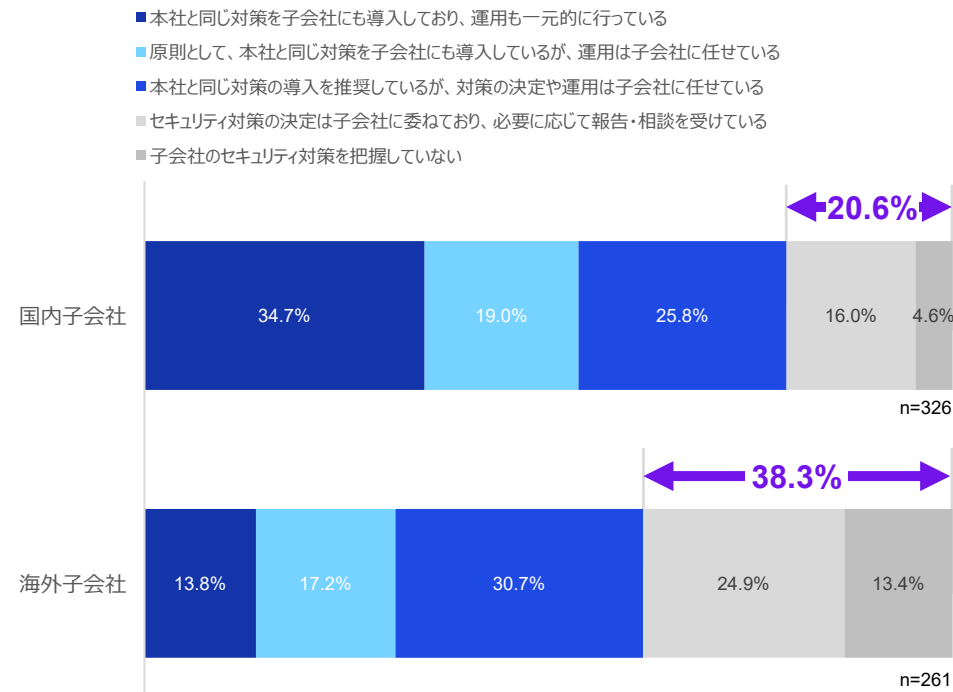
■実施している ■実施予定であり検討している ■実施予定だが検討は開始していない ■実施予定はない ■わからない



国内子会社と海外子会社に対する管理の比較

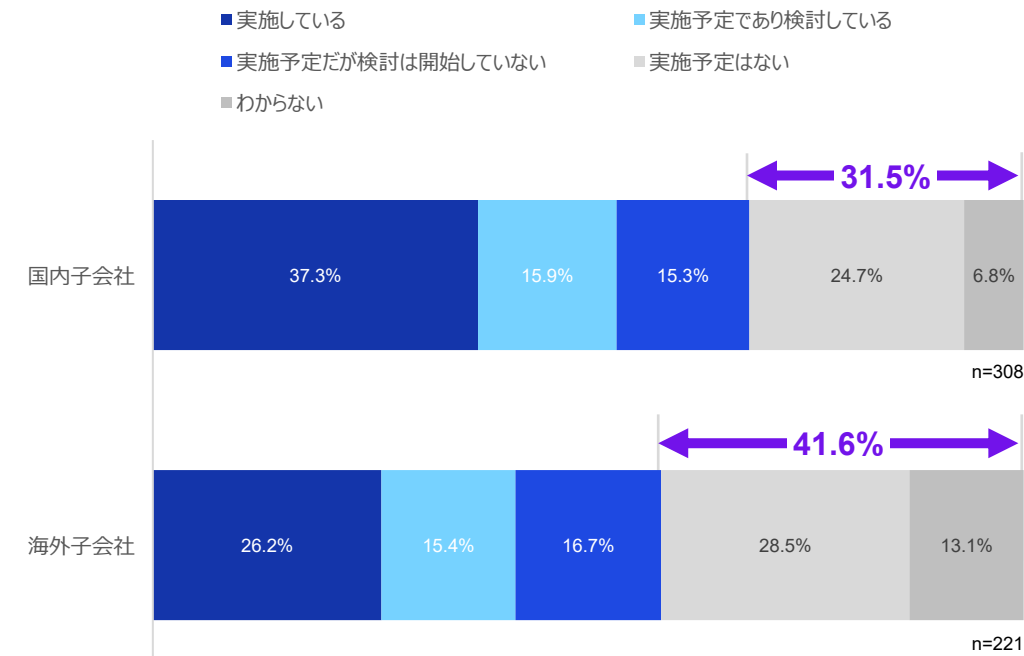
「セキュリティ対策の決定は子会社に委ねており、必要に応じて報告・相談を受けている」と「子会社のセキュリティ対策を把握していない」の回答割合の合計は、国内子会社では20.6%にとどまりましたが、海外子会社では38.3%にのぼり、国内子会社と比較して海外子会社の管理は各社に委ねている状況が確認されました。

海外子会社の管理は、各社に委ねている／把握していない割合が高い
子会社におけるセキュリティ対策の方針について、最も近いものを選択してください。



グループを含む全社共通のCSIRT・SOCの整備を「実施している」との回答は、国内子会社の37.3%に対し、海外子会社では26.2%にとどまりました。また、「実施予定はない」と「わからない」の回答割合の合計も国内子会社の31.5%に対し、海外子会社では41.6%にのぼりました。

海外子会社の約4割は、グループを含む全社共通のCSIRT・SOCの整備ができていない
「グループを含む全社共通のCSIRT・SOCの整備」について、国内子会社と海外子会社を比較



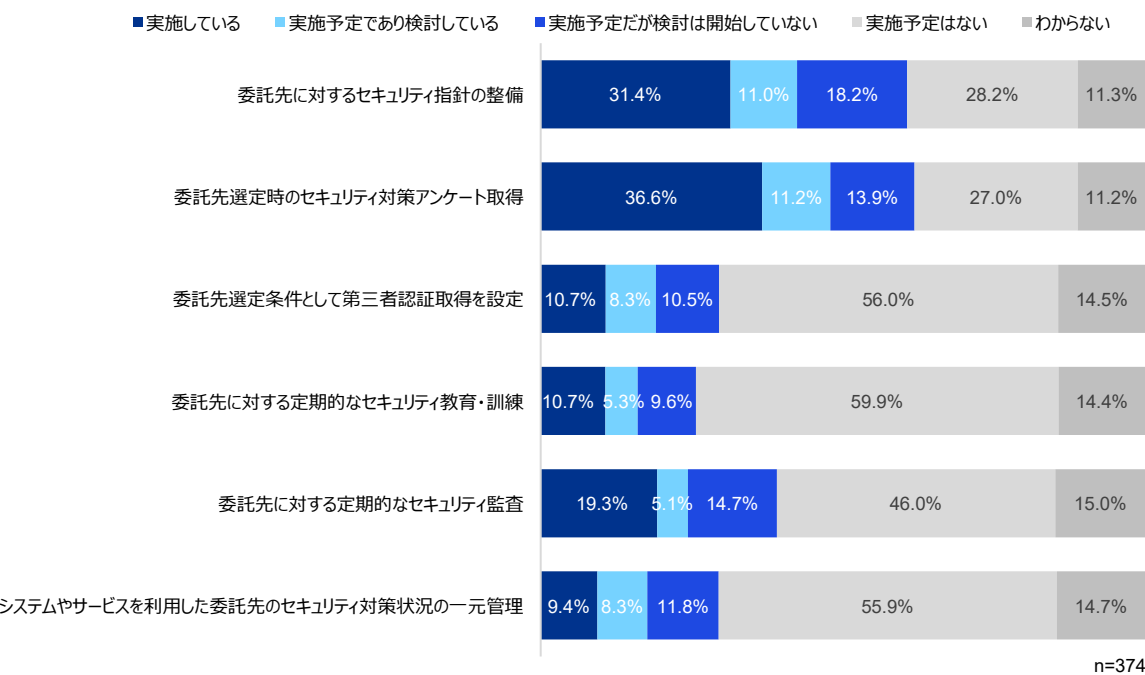
04

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 1/3

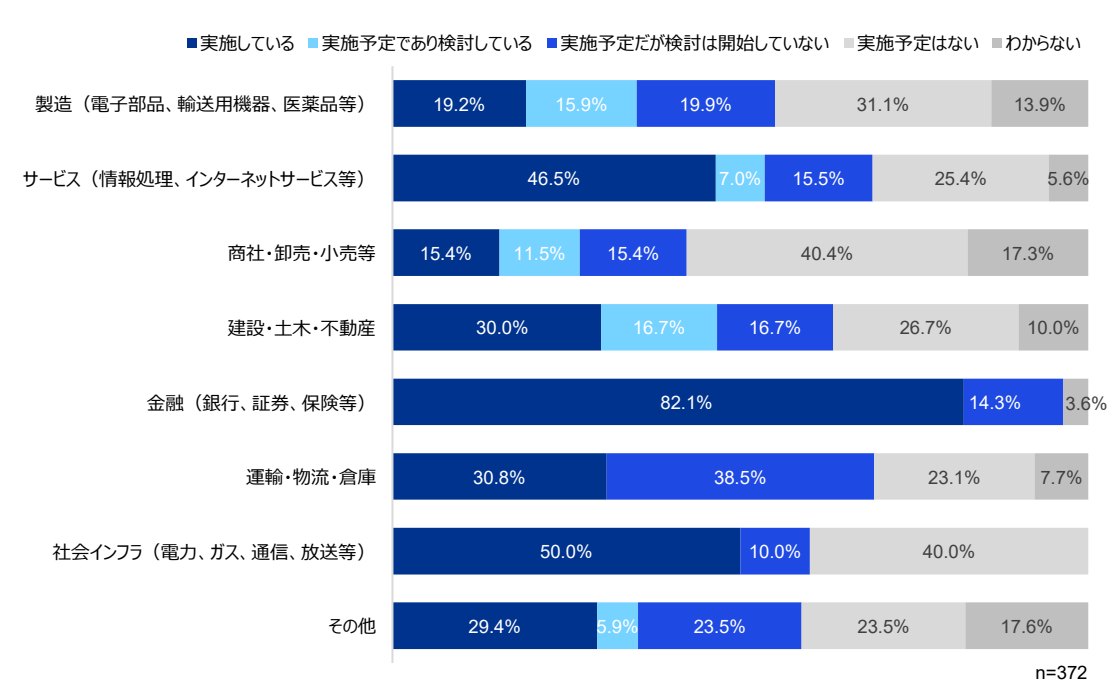
委託先・取引先管理において、いずれの対策も実施率は4割未満であり、委託先に対するセキュリティ指針の整備、委託先選定時のセキュリティ対策アンケート取得についても、実施率は3割強にとどまりました。また、システムやサービスを利用した委託先・取引先のセキュリティ対策状況の一元管理については、9.4%にとどまりました。

委託先選定時のセキュリティ対策アンケート取得の実施は4割弱にとどまる
委託先・取引先の管理について、実施している対策を選択してください。



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8割を超える企業が実施しているのに対し、商社・卸売・小売等では15.4%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。

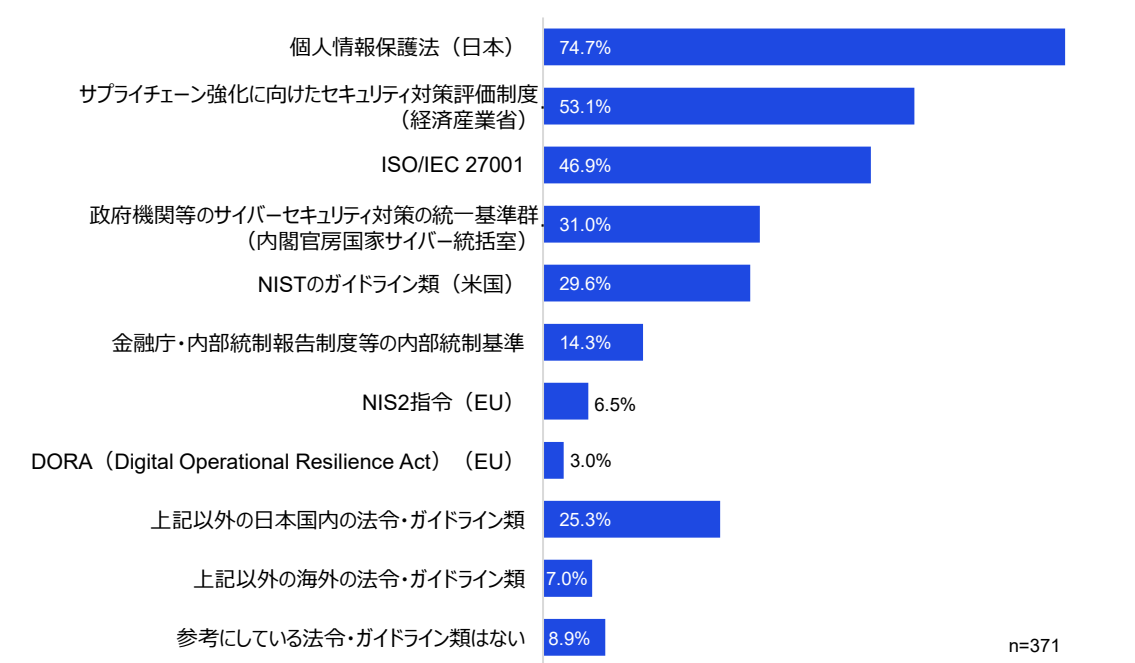
セキュリティ指針の整備について、製造、商社・卸売・小売では2割弱の実施にとどまる
「委託先に対するセキュリティ指針の整備」について、業種別に分析



委託先・取引先に対するサイバーセキュリティ管理 2/3

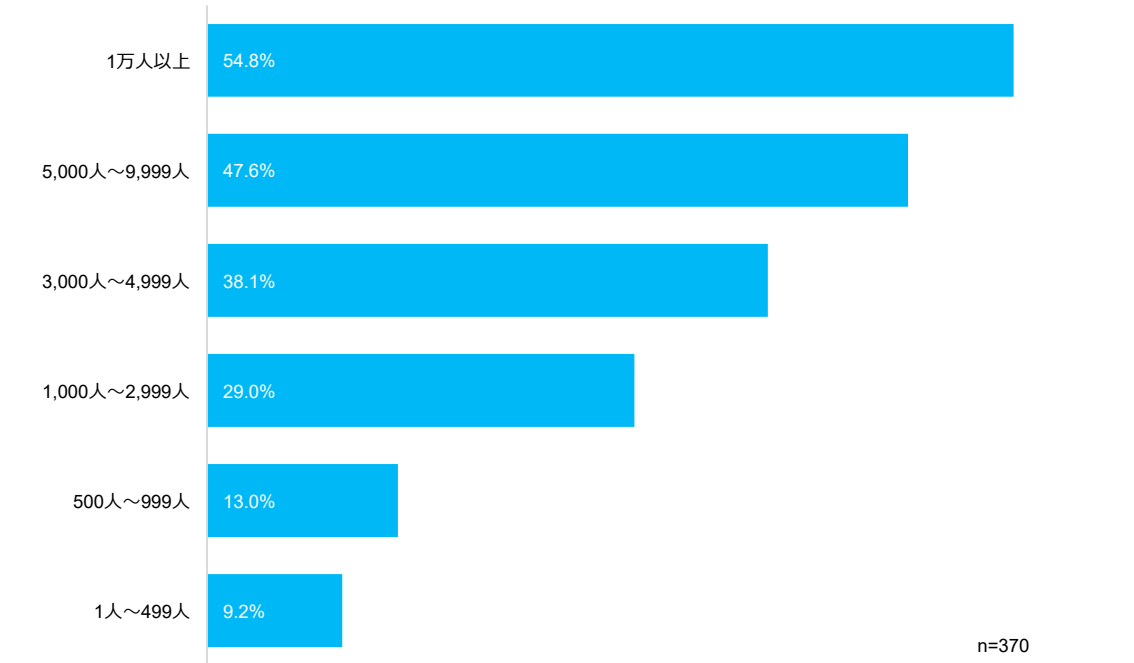
委託先・取引先に関するサイバーセキュリティの取組みにおいて参照している法令・ガイドライン類として、経済産業省および内閣官房国家サイバー統括室が主導している「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」を挙げた企業が5割を超えました。2026年度下期（1～3月）の運用開始が想定されていますが、すでに高い注目を集めています。

サプライチェーン強化に向けたセキュリティ対策評価制度を参照している企業は5割超
委託先・取引先に関するサイバーセキュリティの取組みにおいて参照している法令・ガイドライン類を選択してください。（複数回答可）



また、「NIST（米国）」が発行しているガイドラインやフレームワーク（サイバーセキュリティフレームワークやSP800シリーズ）については、組織規模の大きな企業で参照されており、従業員数が1万人を超える企業では、参照しているとの回答は5割を超えました。

組織規模が大きいほど、NIST（米国）のガイドライン類を参照する企業の割合が高い
NIST（米国）のガイドライン類を委託先・取引先に関するサイバーセキュリティの取組みにおいて参照している企業を組織規模別に分析



委託先・取引先に対するサイバーセキュリティ管理 3/3

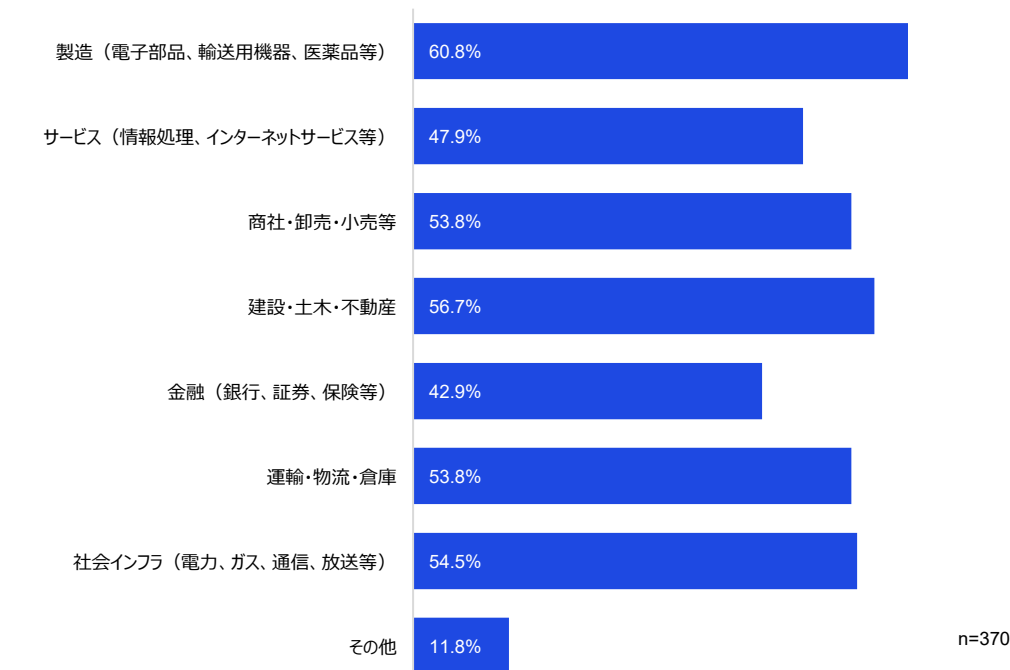
委託先・取引先管理について、経済産業省および内閣官房国家サイバー統括室が主導している「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）を参照している」との回答は、多くの業種で高い傾向となりました。特に、委託先・取引先の多い製

造業においては、6割を超える企業が「参照している」と回答しています。

また、従業員数別にSCS評価制度を参照している企業の割合を分析すると、組織規模にかかわらず、幅広い企業で参照していることが確認されました。

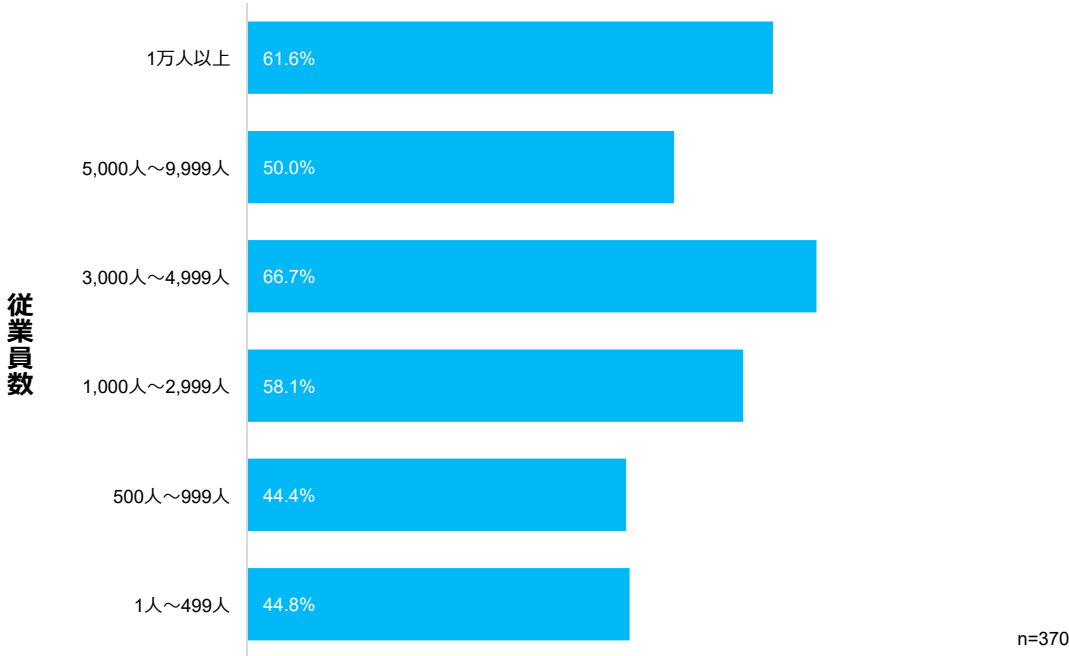
製造では、SCS評価制度を参照しているとの回答が6割を超える

「SCS評価制度」を委託先・取引先に関するサイバーセキュリティの取組みにおいて参照している企業を業種別に分析



組織規模にかかわらず、SCS評価制度を参照している企業は半数近くある

「SCS評価制度」を委託先・取引先に関するサイバーセキュリティの取組みにおいて参照している企業を組織規模別に分析



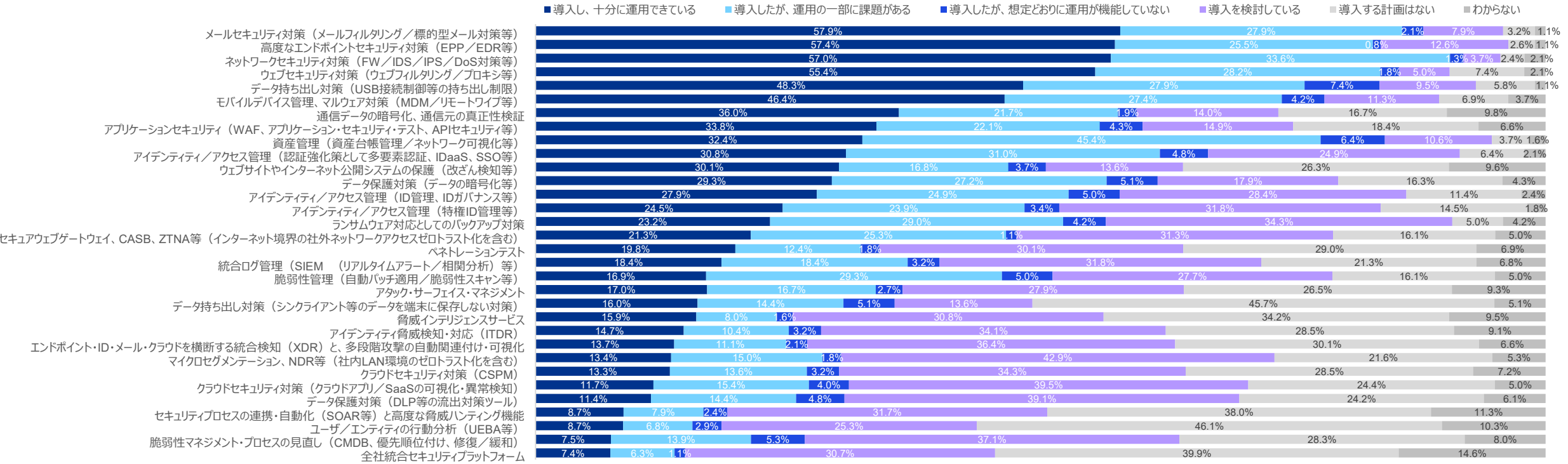
05

サイバーセキュリティ対策

サイバーセキュリティ対策の導入状況

「導入したが、運用の一部に課題がある」「導入したが、想定どおりに運用が機能していない」「導入を検討している」の回答率の高い順で、ランサムウェア対応としてのバックアップ対策（67.5%）、資産管理（62.4%）、脆弱性管理（62.0%）、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）（60.7%）、マイクロセグメンテーション、NDR等（59.7%）、アイデンティティ／アクセス管理（特権ID管理等）（59.2%）となり、導入が検討・進みつつあることが確認されました。

ランサムウェア対応としてのバックアップ対策、資産管理、脆弱性管理、アイデンティティ／アクセス管理、マイクロセグメンテーションの導入が進みつつある
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=381



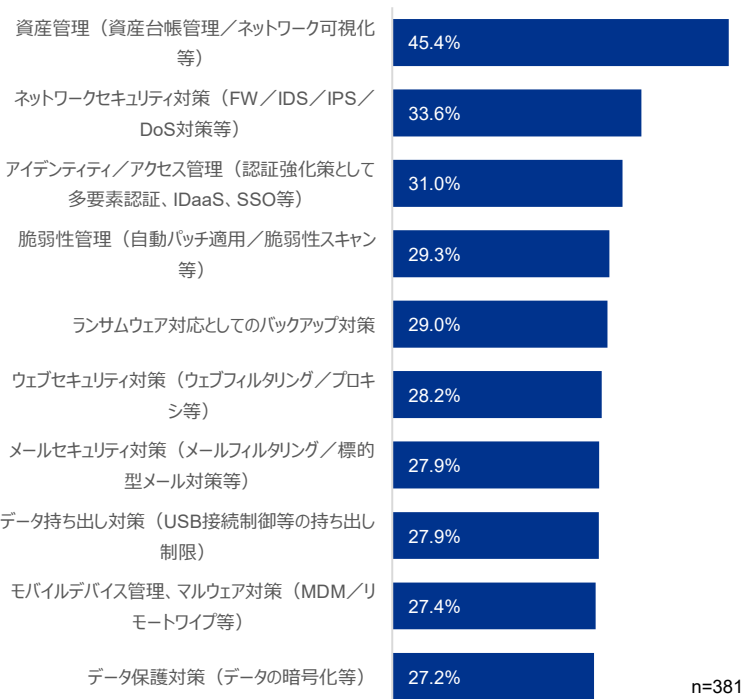
サイバーセキュリティ対策の導入状況の比較

「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（45.4%）、ネットワークセキュリティ対策（33.6%）などがありました。

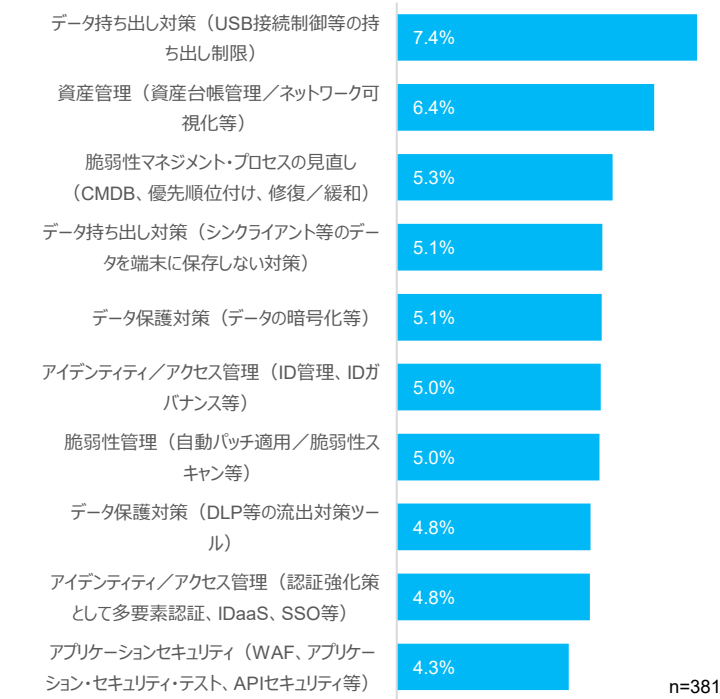
また、「導入したが、想定どおりに運用が機能していない」との回答割合が高い対策は、データ持ち出し対策（7.4%）、資産管理（6.4%）などがありました。

さらに、「導入を検討している」との回答割合が高い対策は、マイクロセグメンテーション、NDR等（42.9%）、クラウドセキュリティ対策（39.5%）などがありました。

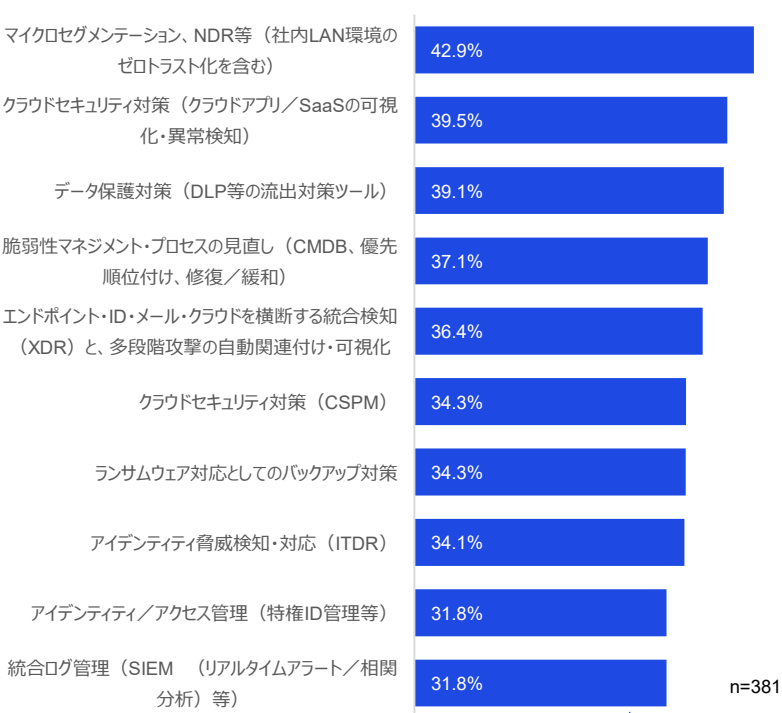
「導入したが、運用の一部に課題がある」 上位10の対策



「導入したが、想定どおりに運用が機能していない」 上位10の対策



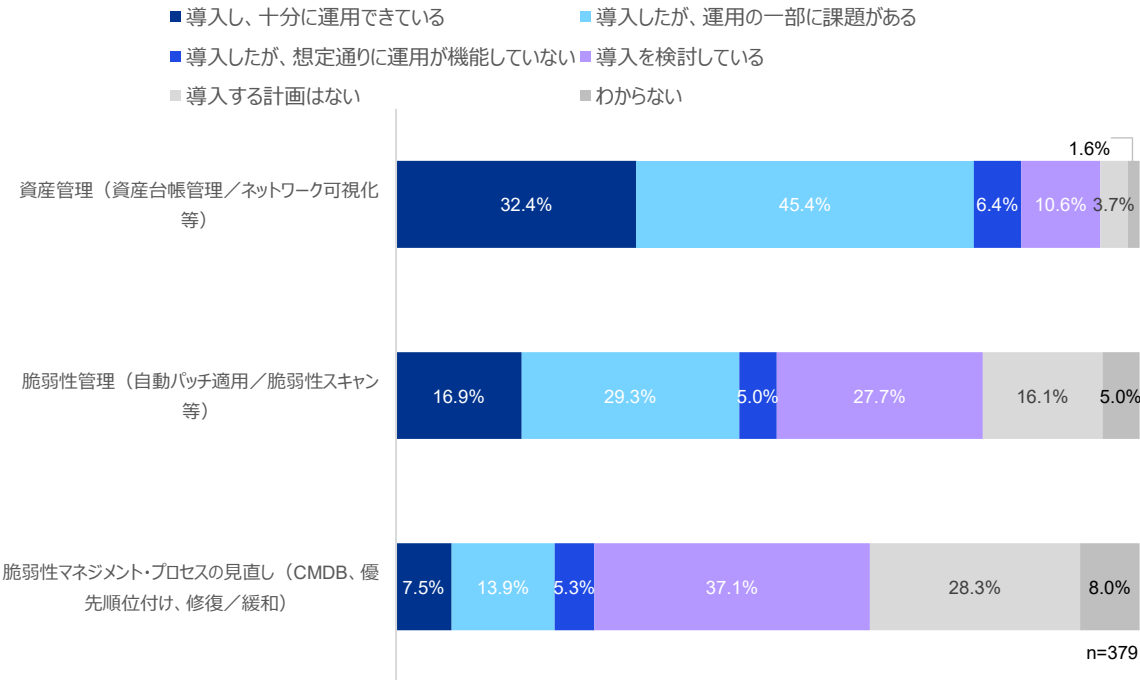
「導入を検討している」 上位10の対策



資産・脆弱性管理の導入状況とパッチ適用のタイミング

フロンティアAIによる脆弱性の高速・大量発見などのサイバー脅威への対策として、資産管理および脆弱性管理、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くなっています。調査においても、同様の傾向がみられました。しかし、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（45.4%）、資産管理でつまづいている企業が多いと考えられます。

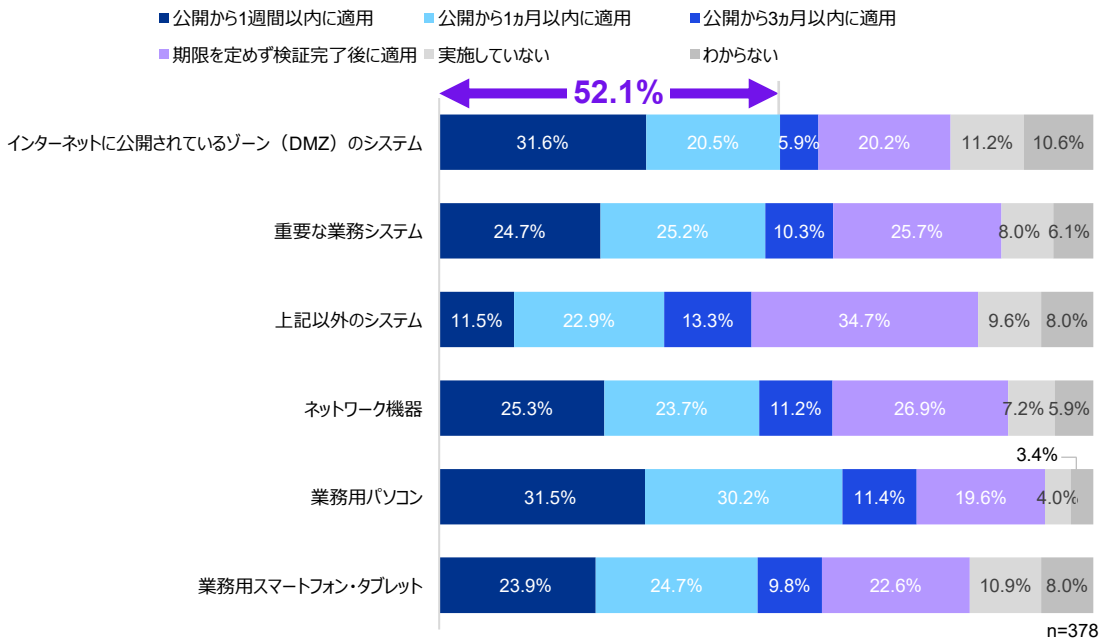
資産管理、脆弱性管理の導入は進んでいるが、運用でつまづく企業が多い
資産管理、脆弱性管理に係る対策の導入状況を選択してください。



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31.6%にとどまりました。また、「公開から1週間以内に適用」「公開から1ヵ月以内に適用」と回答した割合の合計が52.1%にとどまり、対応が遅れるか未対応である企業が多いことがわかりました。

インターネットに公開されているシステムでも1ヵ月以内にパッチを適用するのは約5割

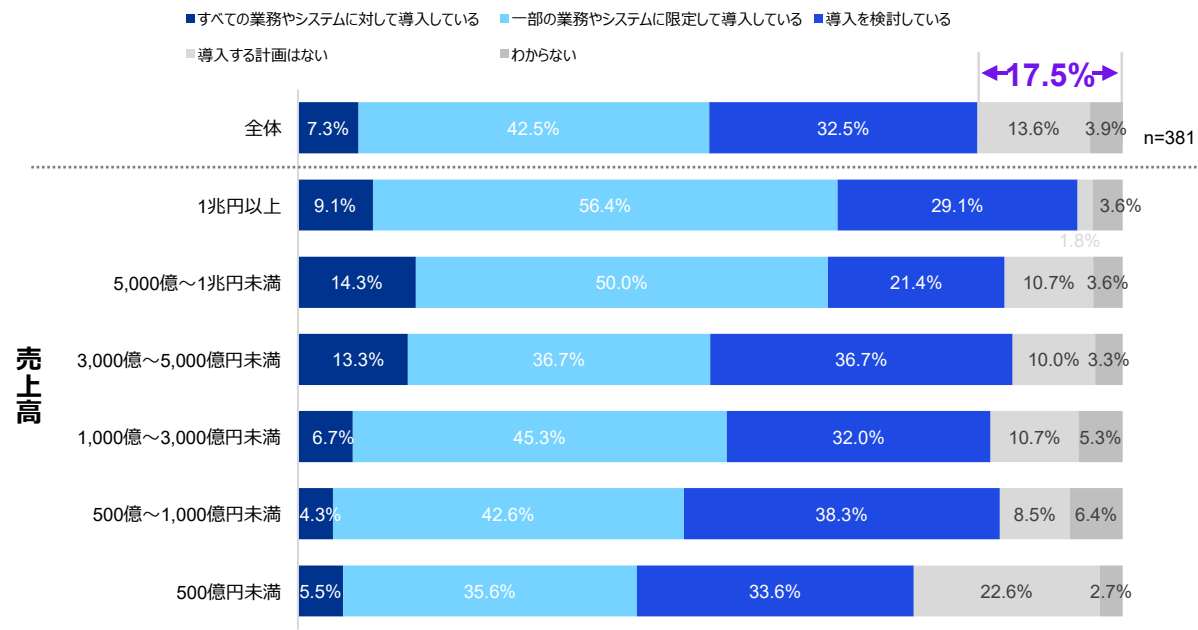
公開された脆弱性のうち、「緊急度が高い」と判断された脆弱性に対するパッチ適用の対応タイミングについて選択してください。



ゼロトラスト原則に基づくアクセス制御の導入状況

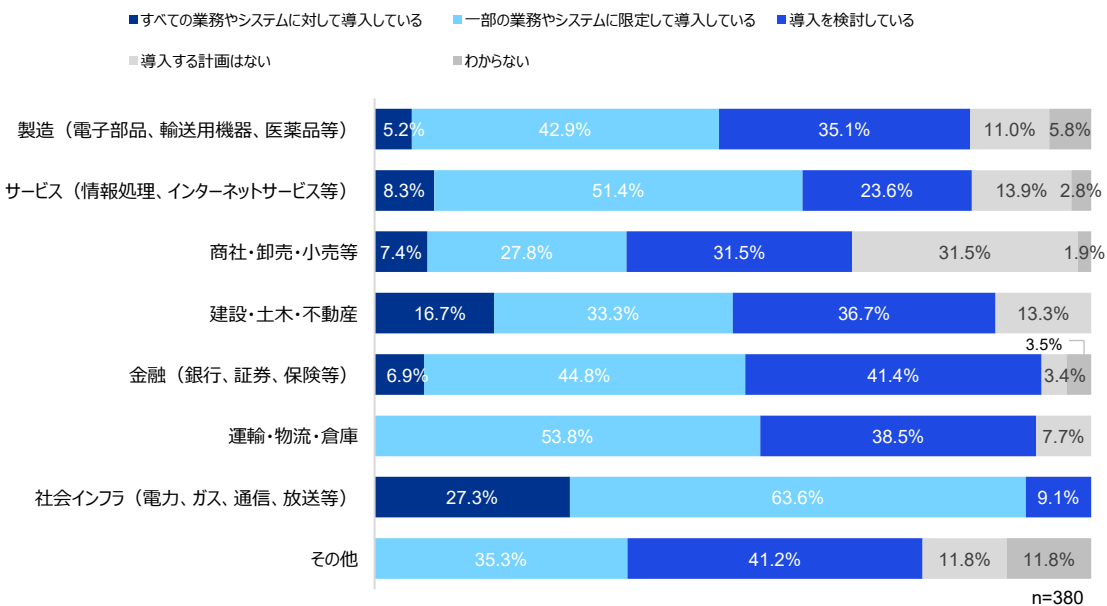
ゼロトラスト原則（社内・社外の境界によらず、アクセスのたびに認証・認可を実施する考え方）に基づくアクセス制御の導入については、「導入する計画はない」「わからない」との回答が17.5%にとどまり、8割以上の企業で導入が検討・進みつつあることが確認されました。売上高別に分析すると、「すべての業務やシステムに対して導入している」「一部の業務やシステムに限定して導入している」との回答は、おおむね売上高が高い企業ほど多い傾向にあることがわかりました。

ゼロトラスト原則に基づくアクセス制御は8割以上の企業で導入が進みつつある
ゼロトラスト原則に基づくアクセス制御の導入状況を選択してください。



業種別に分析すると、社会インフラでの導入が進んでおり、「すべての業務やシステムに対して導入している」「一部の業務やシステムに限定して導入している」を合計すると、9割以上の回答企業で導入されていることが確認されました。

社会インフラではすでに約3割の企業ですべての業務やシステムに対して導入している
ゼロトラスト原則に基づくアクセス制御の導入状況について、業種別に分析

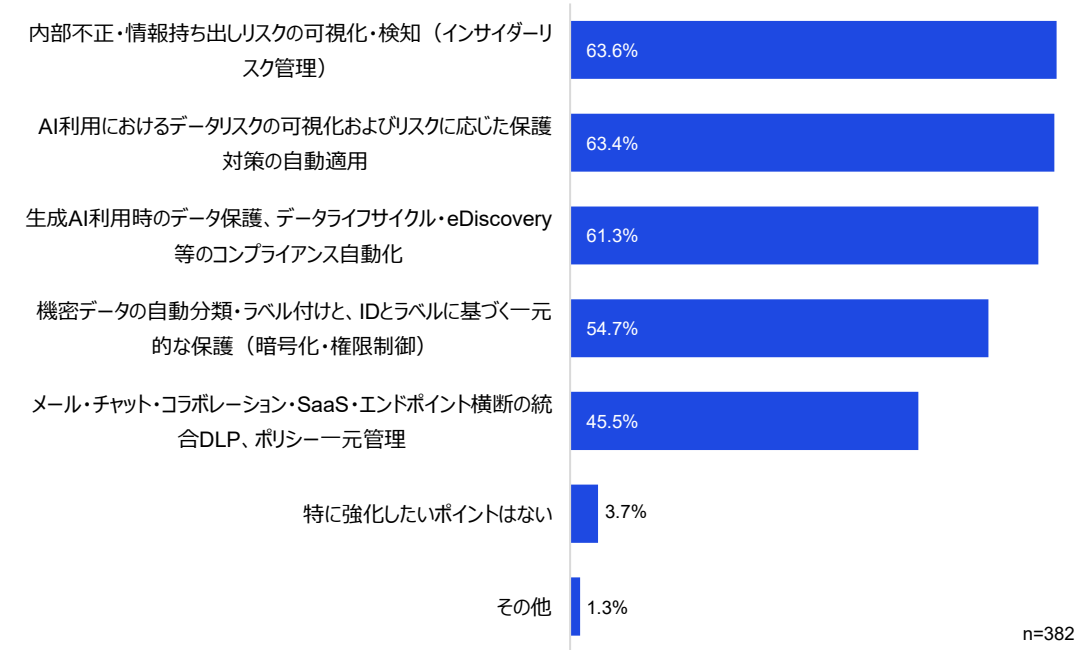


データ保護・情報ガバナンス領域での強化ポイント

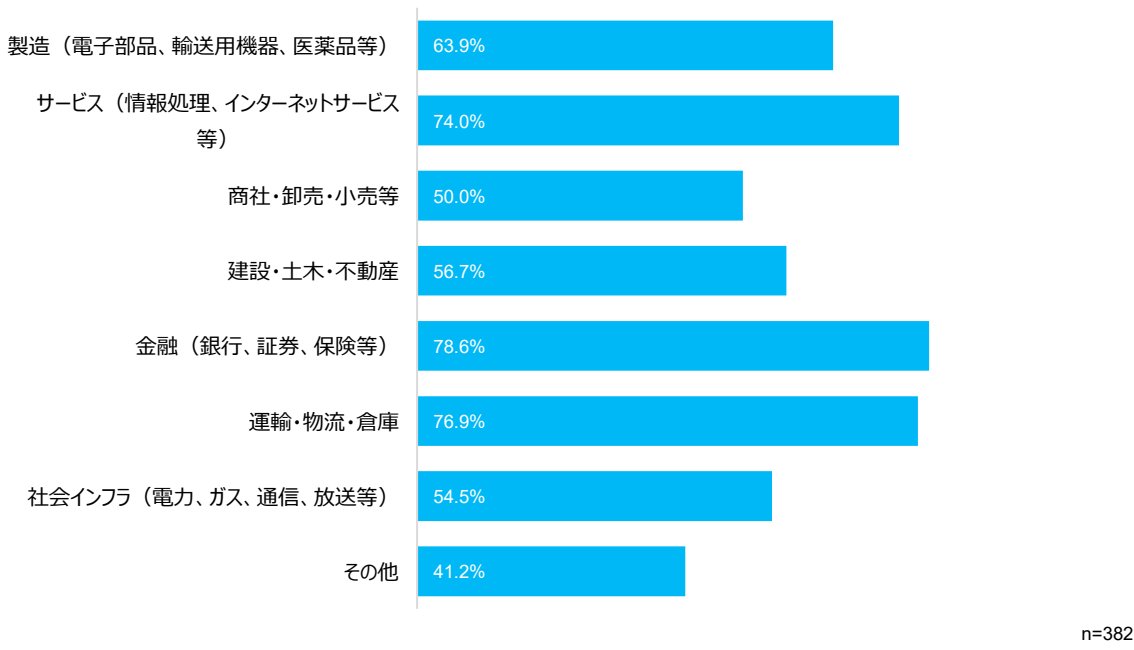
データ保護・情報ガバナンスの取組みについて、「内部不正・情報持ち出しリスクの可視化・検知」「AI利用におけるデータリスクの可視化およびリスクに応じた保護対策の自動適用」「生成AI利用時のデータ保護、データライフサイクル・eDiscovery等のコンプライアンス自動化」の観点で強化したいと回答した企業が6割を超えました。

特に、「AI利用におけるデータリスクの可視化およびリスクに応じた保護対策の自動適用」について、業種別に分析すると、金融、運輸・物流・倉庫、サービスにおいて強化したいとの回答が7割を超えました。

約6割の企業で内部不正、AI利用、コンプライアンス等の観点から強化意向あり
データ保護・情報ガバナンス領域で強化したいポイントを選択してください。（複数回答可）



金融、運輸・物流・倉庫、サービスでは7割超において、AI利用の観点から強化意向あり
「AI利用におけるデータリスクの可視化およびリスクに応じた保護対策の自動適用」との回答を業種別に分析

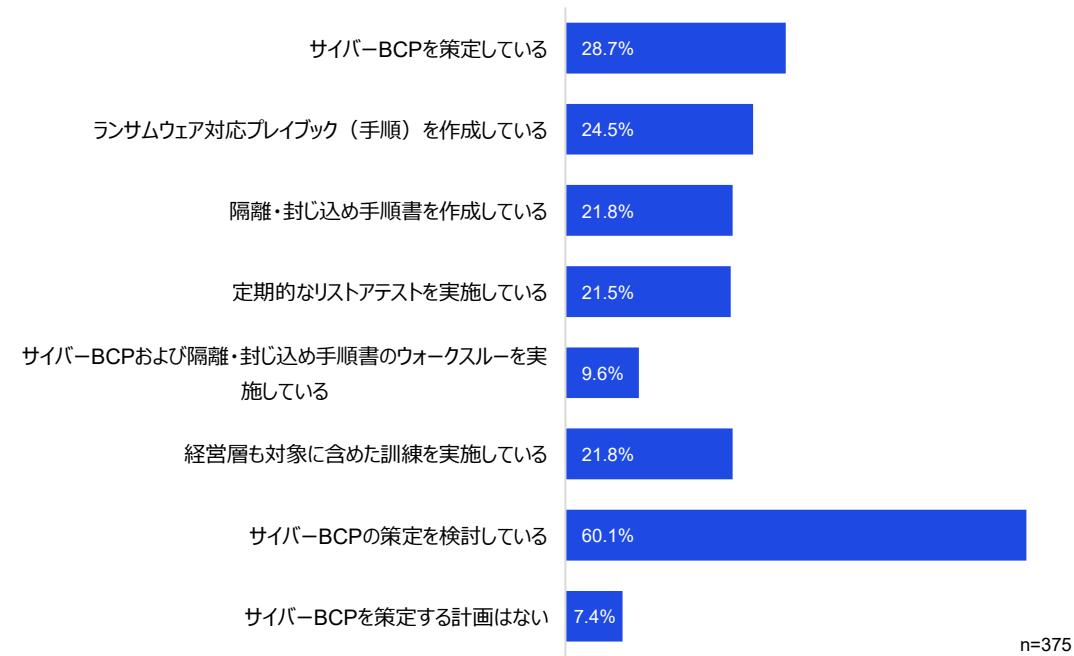


サイバーBCPの策定・訓練状況

近年、サイバー攻撃によって長期間の業務停止を余儀なくされる事例が相次いでいることから、サイバーBCPが注目されています。「サイバーBCPを策定している」と回答した企業は約3割、「サイバーBCPの策定を検討している」と回答した企業は約6割となりました。また、サイバーBCP・手順書に基づく、経営層も対象に含めた訓練、隔離・封じ込め手順書の作成、リストアテストなどを実施しているとの回答は約2割にとどまりました。

サイバーBCPの策定は約3割にとどまっている

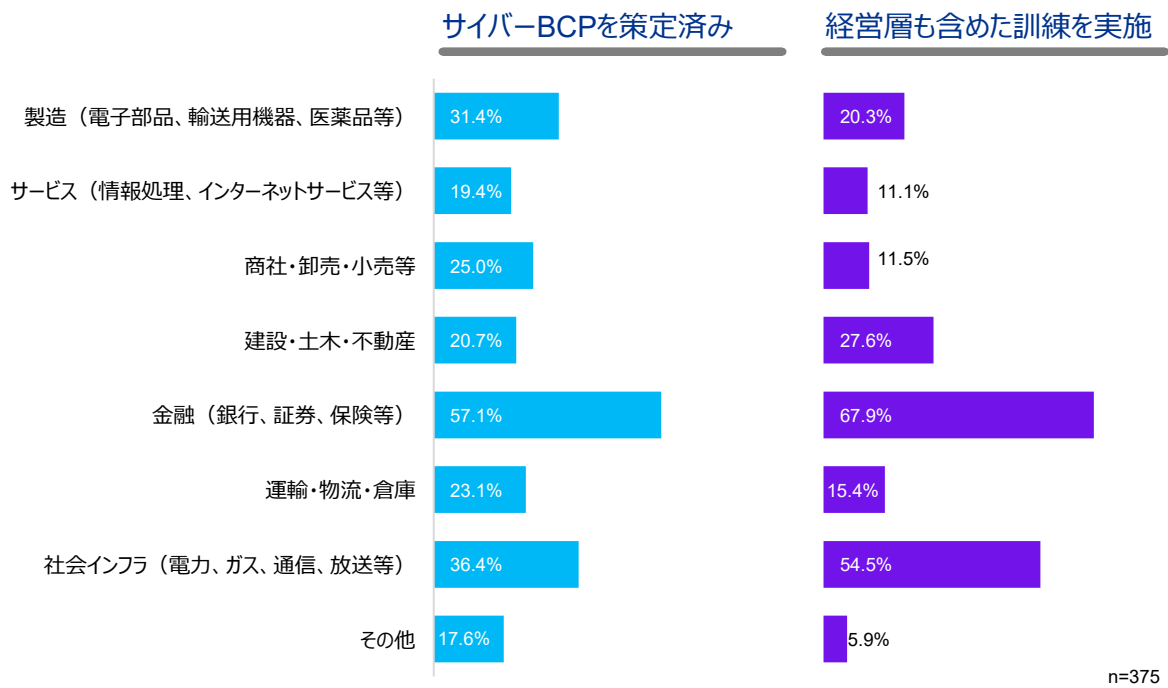
サイバーBCP（システム復旧観点のみではなく、サイバー被害を受けている期間中の業務継続も含む）の対応状況について選択してください。（複数回答可）



サイバーBCPの策定状況、経営層も含めた訓練の状況を確認すると、金融が最も高く、それぞれ57.1%、67.9%との回答を得ました。また、社会インフラが続ぎ、それぞれ36.4%、54.5%との回答となりました。

サイバーBCPの策定、経営層を含めた訓練は、金融が先行

「サイバーBCPの策定」「経営層も含めた訓練の実施」との回答を業種別に分析



016

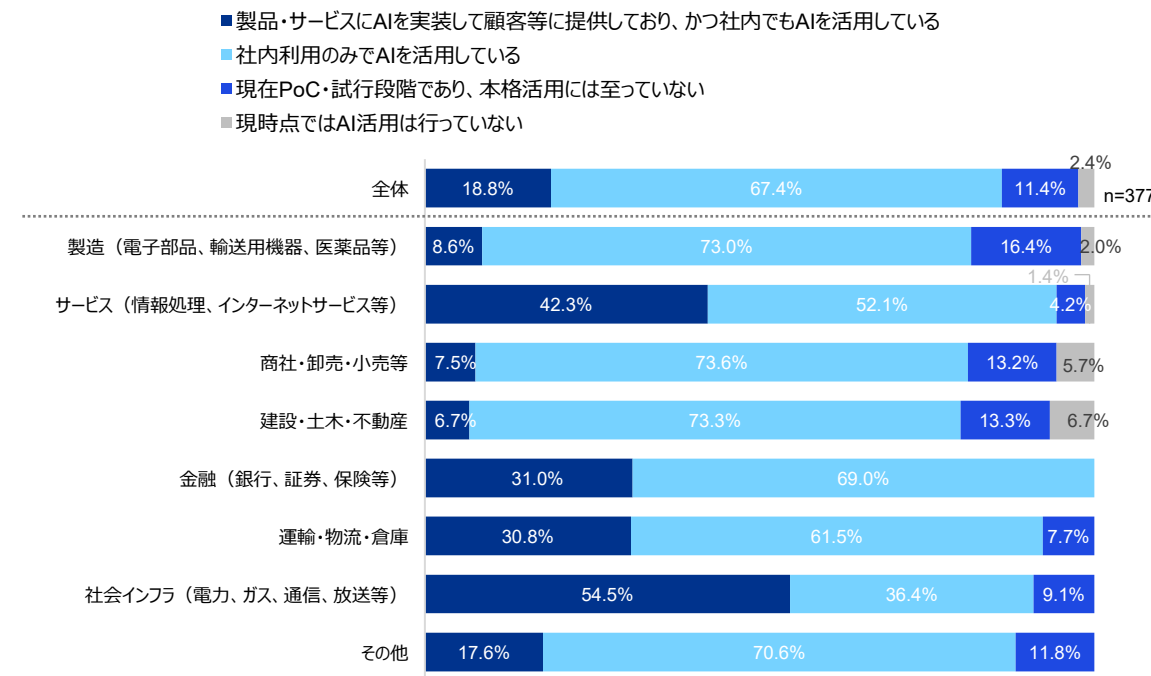
AIセキュリティ

AIの導入状況

AIの主な活用方法としては、「社内利用のみでAIを活用している」が最も多く、67.4%となりました。業種別に分析すると、社会インフラでは54.5%の企業が、サービスでは42.3%の企業が「製品・サービスにAIを実装して顧客等に提供しており、かつ社内でもAIを活用している」と回答しています。逆に、建設・土木・不動産、商社・卸売・小売等、製造の2割程度は、「現在PoC・試行段階であり、本格活用には至っていない」「現時点ではAI活用は行っていない」と回答しています。

社会インフラ、サービスでは、社内だけでなく顧客向けのAI活用も進んでいる

AIの主な活用方法として、最も近いものを次のなかから選択してください。

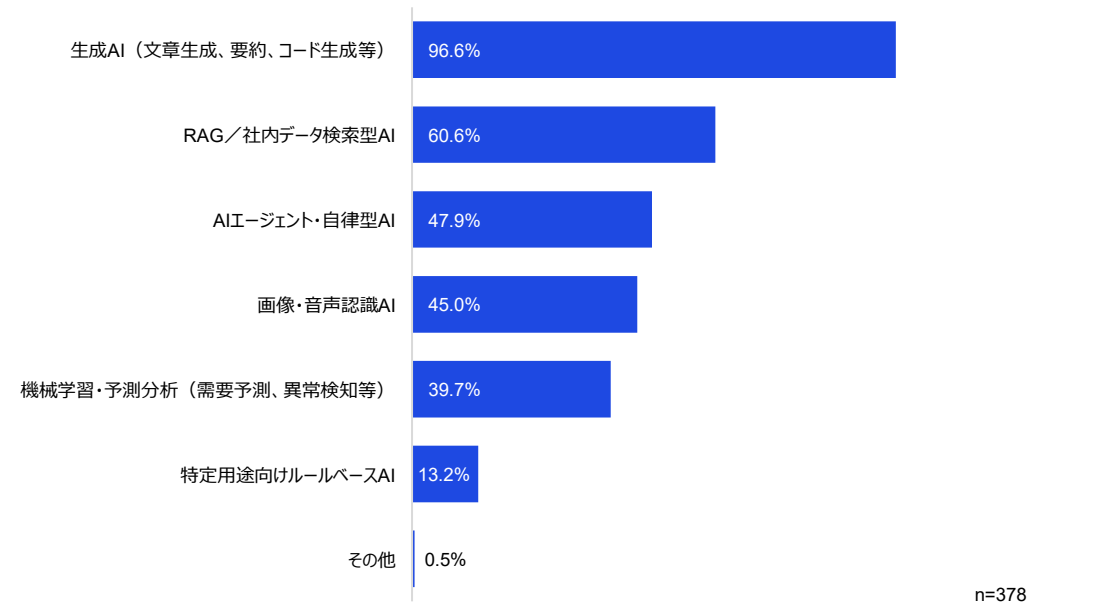


ない」と回答しています。

主に利用している（または検討している）AI技術・手法は、「生成AI（文章生成、要約、コード生成等）」が最も高く、「AIEージェント・自律型AI」についても、約5割の企業で導入・検討していることがわかりました。

約5割の企業でAIEージェント・自律型AIを導入・検討している

主に利用している（または検討している）AI技術・手法を選択してください。（複数回答可）



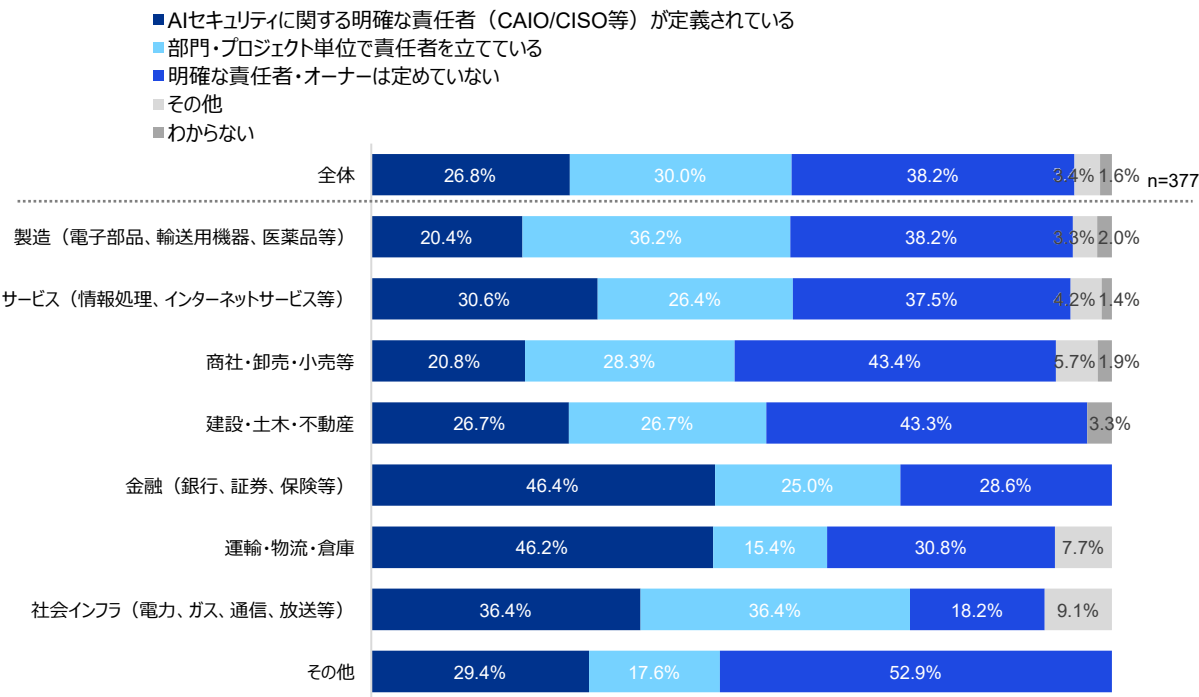
※RAG: Retrieval-Augmented Generation : 検索拡張生成

AIセキュリティの責任者、推進体制の整備

「AIセキュリティに関する明確な責任者（CAIO/CISO等）が定義されている」との回答は26.8%にとどまりました。ただし、金融、運輸・物流・倉庫では、4割を超える企業が、定義済みであると回答しています。一方で「明確な責任者・オーナーは定めていない」との回答が最も多く、38.2%となりました。特に、商社・卸売・小売等、建設・土木・不動産では、4割を超える企業が「定めていない」と回答しています。

4割弱の企業では、AIセキュリティについて明確な責任者・オーナーは定めていない

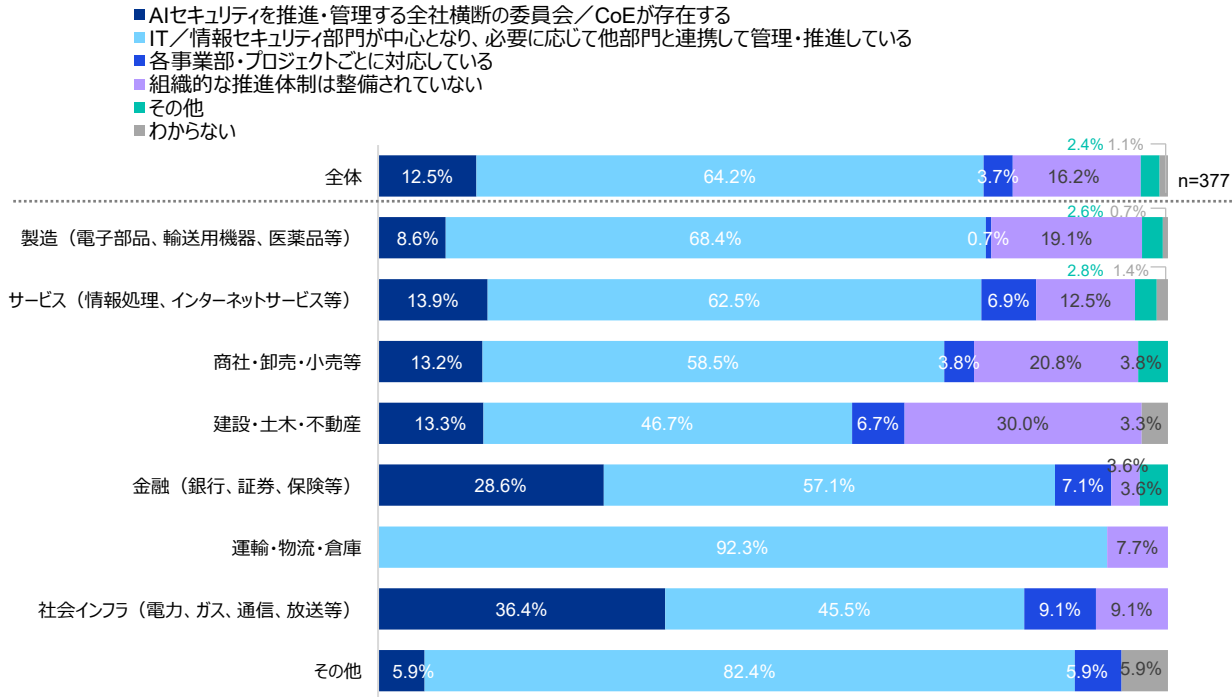
AIセキュリティに関する責任体制として、最も近いものを選択してください。



AIセキュリティの推進体制としては、IT／情報セキュリティ部門が中心となっているとの回答が6割を超え、「AIセキュリティを推進・管理する全社横断の委員会／CoEが存在する」との回答は約1割にとどまりました。ただし、社会インフラ、金融では、「AIセキュリティを推進・管理する全社横断の委員会／CoEが存在する」との回答割合が他業種より高くなりました。

6割強の企業では、IT／情報セキュリティ部門が中心となってAIセキュリティを推進

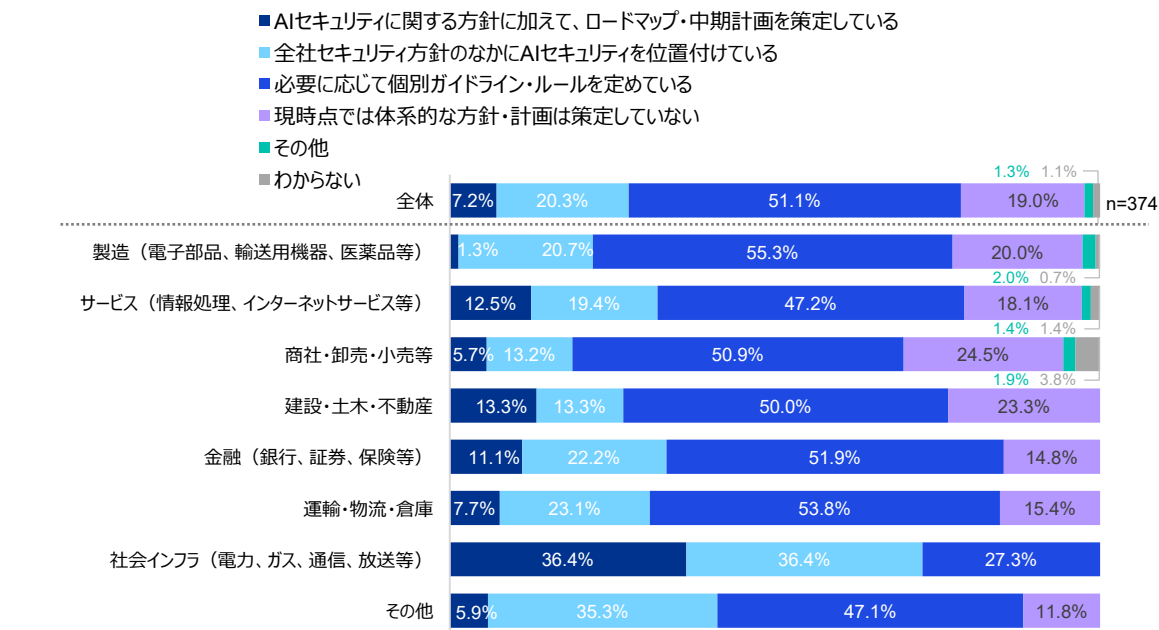
AIセキュリティを推進・管理する組織体制として、最も近いものを選択してください。



AIセキュリティ、生成AIに関する方針・ガバナンス

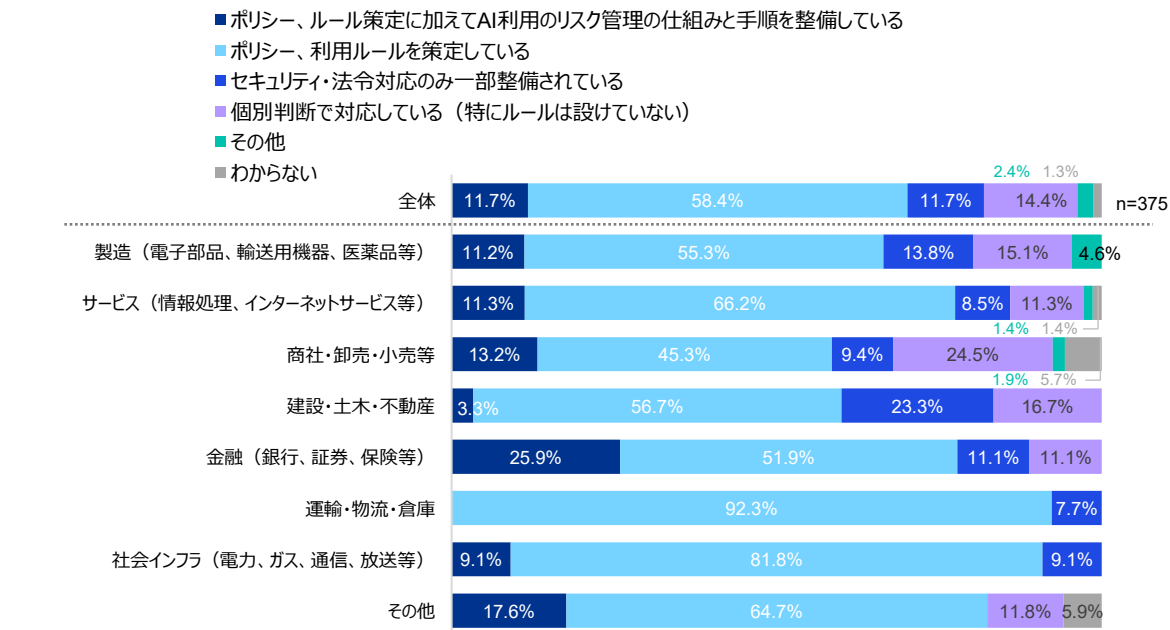
AIセキュリティに関する方針・計画については、約半数の企業が「必要に応じて個別ガイドライン・ルールを定めている」と回答しており、「現時点では体系的な方針・計画は策定していない」との回答は約2割にとどまりました。一方で社会インフラでは整備が進んでおり、36.4%の企業が、「AIセキュリティに関する方針に加えて、ロードマップ・中期計画を策定している」と回答しています。

約半数の企業は、必要に応じて個別にAIセキュリティに関する方針・計画を定めている
AIセキュリティに関する方針・計画の策定状況として、最も近いものを選択してください。



生成AI利用に関するルール・ガバナンスの整備については、「ポリシー、利用ルールを策定している」との回答が最も多く、約6割の企業が該当しました。「ポリシー、ルール策定に加えてAI利用のリスク管理の仕組みと手順を整備している」との回答は金融が最も高く、25.9%の企業が該当しています。

約6割の企業が、生成AIのポリシーや利用ルールを策定している
生成AI利用に関するルール・ガバナンスの整備状況として、最も近いものを次のなかから選択してください。

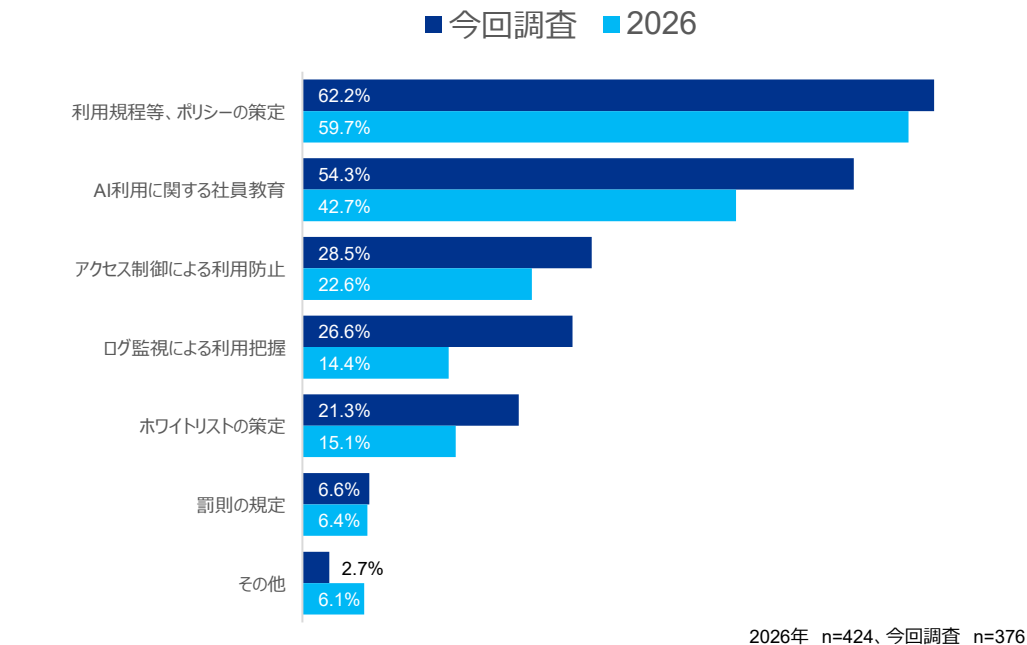


シャドーAIへの対策、外部AIサービスの評価

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は、いずれの対策も前回調査よりも導入が進んでいることがわかりました。「利用規程等、ポリシーの策定」「AI利用に関する社員教育」だけでなく、「アクセス制御による利用防止」「ログ監視による利用把握」「ホワイトリストの策定」といった技術的対策の導入も進みました。

前回調査と比較して、規程整備、教育だけでなく、技術的な対策も導入が進んだ

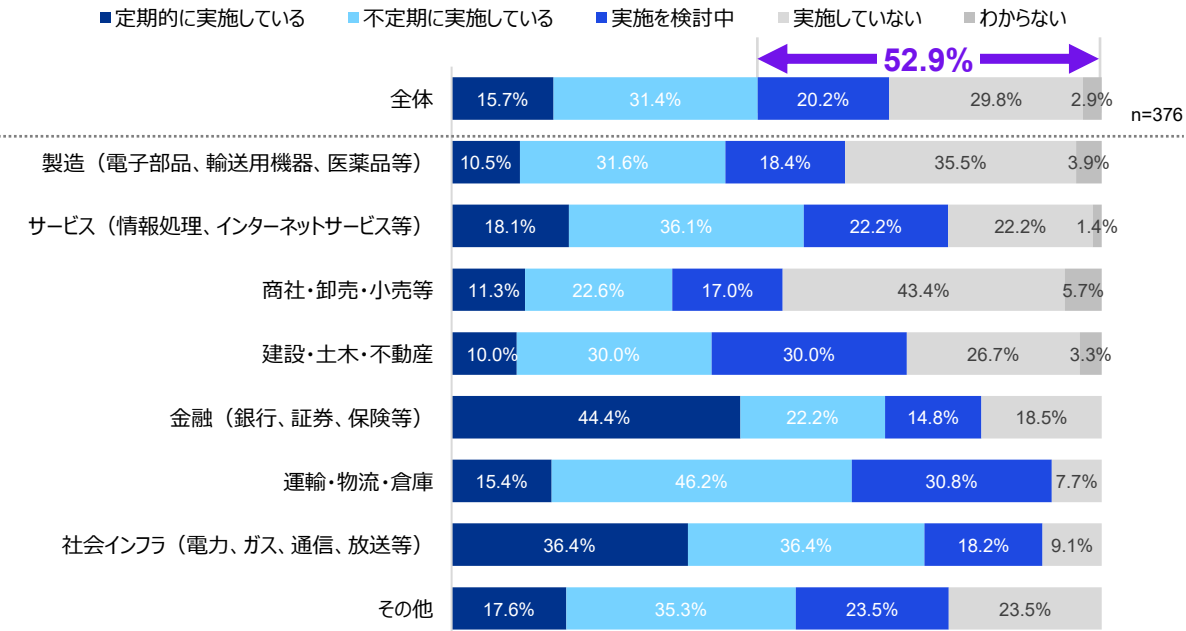
シャドーAI（正規に許可されていないAIツールの業務利用）を防ぐための対策を実施していますか。（複数回答可）



外部のAIサービス利用時のセキュリティ評価を「定期的実施している」と回答した企業は、金融は44.4%、社会インフラでは36.4%と3割を超えていますが、全体では15.7%にとどまりました。52.9%の企業では「実施を検討中」「実施していない」「わからない」と回答しています。

半数の企業では、外部のAIサービス利用時のセキュリティ評価が実施できていない

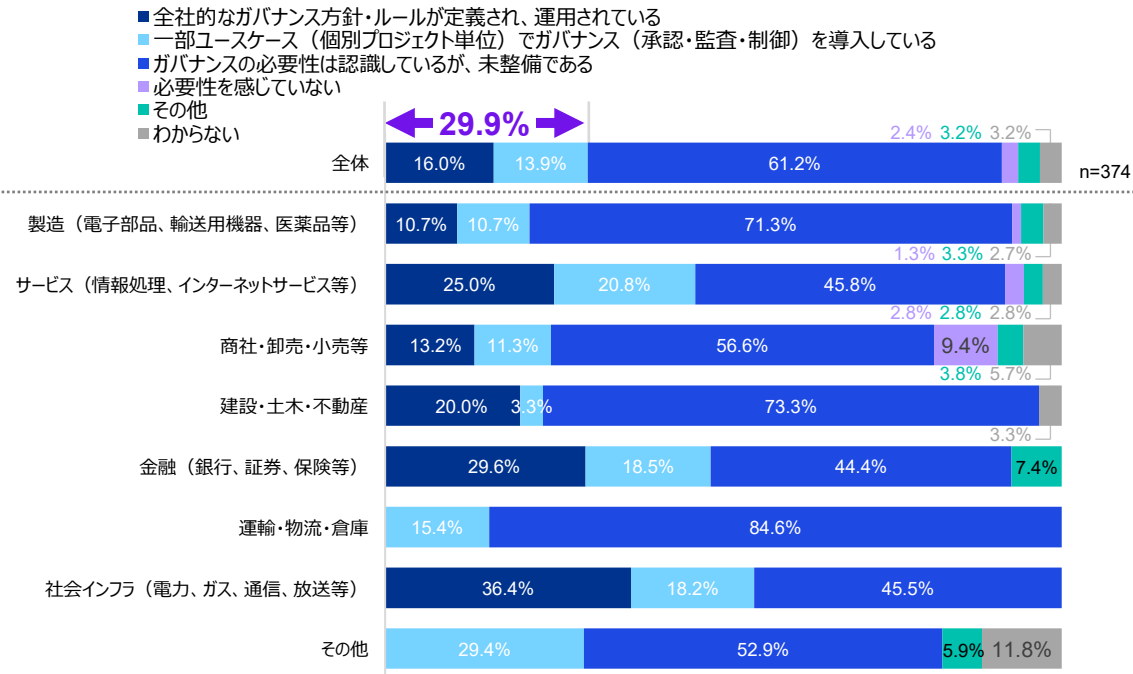
外部のAIサービスを利用する際に、そのAIに対するセキュリティ評価を実施していますか。



AIエージェント・自律型AIに関するガバナンス、台帳管理

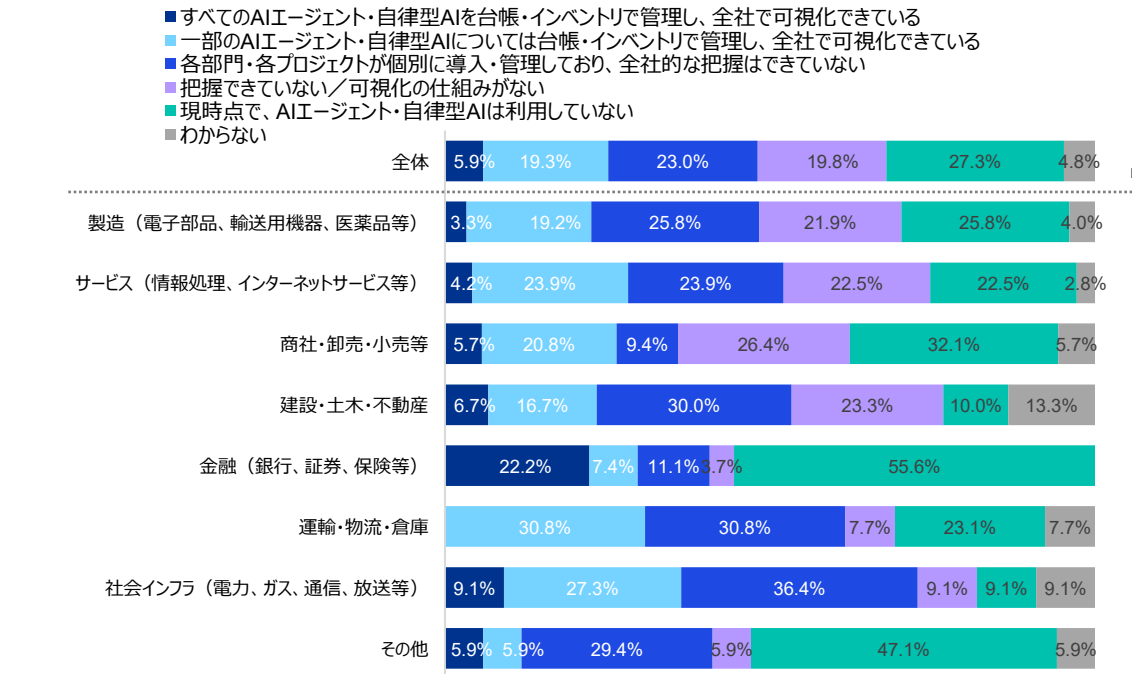
AIエージェント・自律型AIに対して、「ガバナンスの必要性は認識しているが、未整備である」（61.2%）との回答が最も多く、「全社的なガバナンス方針・ルールが定義され、運用されている」「一部ユースケースでガバナンスを導入している」と回答した企業は29.9%にとどまりました。

「ガバナンスの必要性は認識しているが、未整備」との回答が最も多く、6割を超える
AIエージェント・自律型AIのルール・ガバナンスの整備状況として、最も近いものを選択してください。



AIエージェント・自律型AIを利用している企業のうち、「各部門・各プロジェクトが個別に導入・管理しており、全社的な把握はできていない」との回答が23.0%で最も多く、次に多かった回答は、「把握できていない／可視化の仕組みがない」（19.8%）となりました。

AIエージェント・自律型AIを利用している企業のうち、「各部門・各プロジェクトが個別に導入・管理しており、全社的な把握はできていない」との回答が最も多い
業務に利用されているAIエージェント・自律型AIの数や所在を、どの程度把握できていますか。

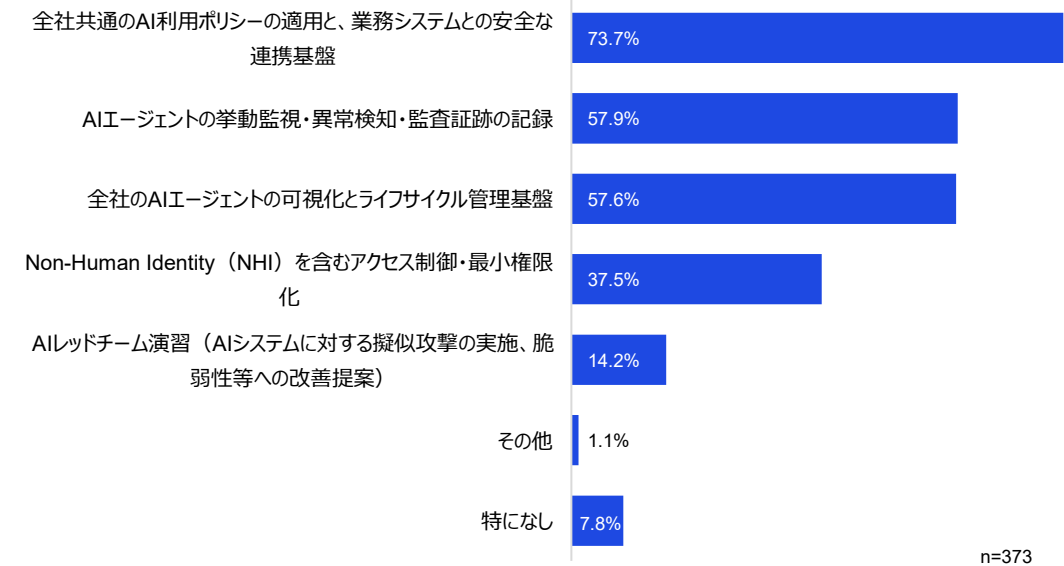


AIエージェントのセキュリティ・ガバナンス強化のポイント

AIエージェントのセキュリティ・ガバナンスを強化するうえで重視するポイントとして、「全社共通のAI利用ポリシーの適用と、業務システムとの安全な連携基盤」との回答が最も多く、7割超の企業が選択しました。すべてのAIエージェントを全社で可視化できている企業は、前項のとおり5.9%にとどまりましたが、57.6%の企業が「全社のAIエージェントの可視化とライフサイクル管理基盤」を重視するポイントとして選択しています。

7割超の企業が、「全社共通のAI利用ポリシーの適用と、業務システムとの安全な連携基盤」を選択

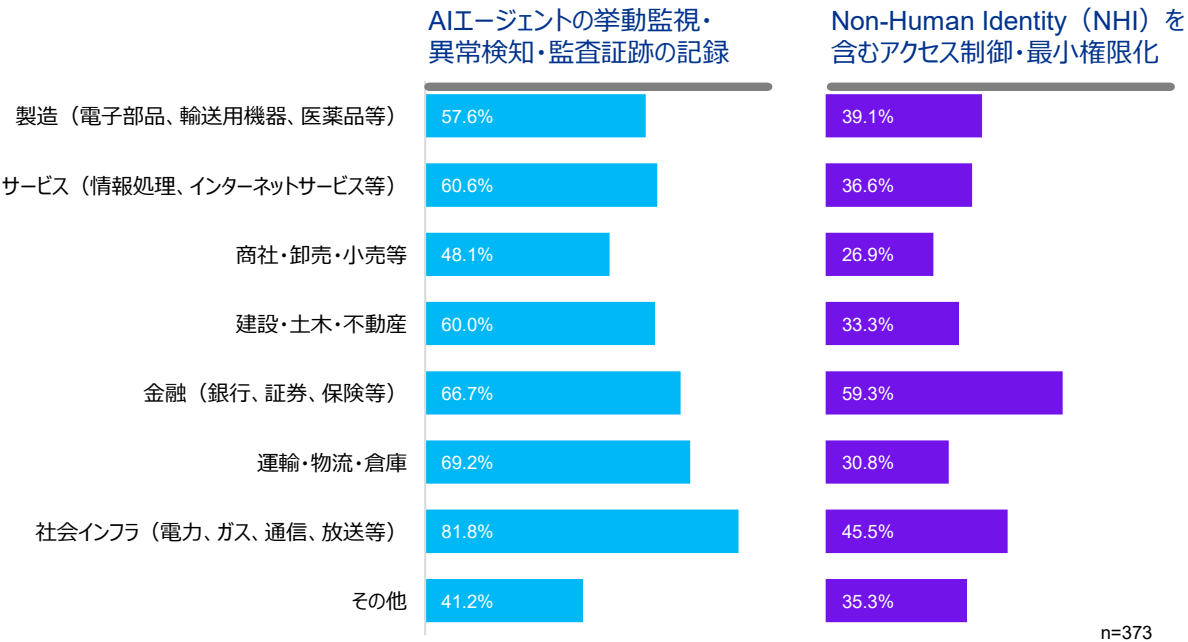
今後、AIエージェントのセキュリティ・ガバナンスを強化するうえで重視するポイントを選択してください。（複数回答可）



業種別にみると、「AIエージェントの挙動監視・異常検知・監査証跡の記録」は社会インフラで81.8%、「Non-Human Identity (NHI) を含むアクセス制御・最小権限化」は金融で59.3%と、それぞれ最も高くなりました。

AIエージェントへの対応では、挙動監視は社会インフラで、NHIを含むアクセス制御・最小権限化は金融にて最も重視されている

「AIエージェントの挙動監視・異常検知・監査証跡の記録」「Non-Human Identity (NHI) を含むアクセス制御・最小権限化」との回答を業種別に分析

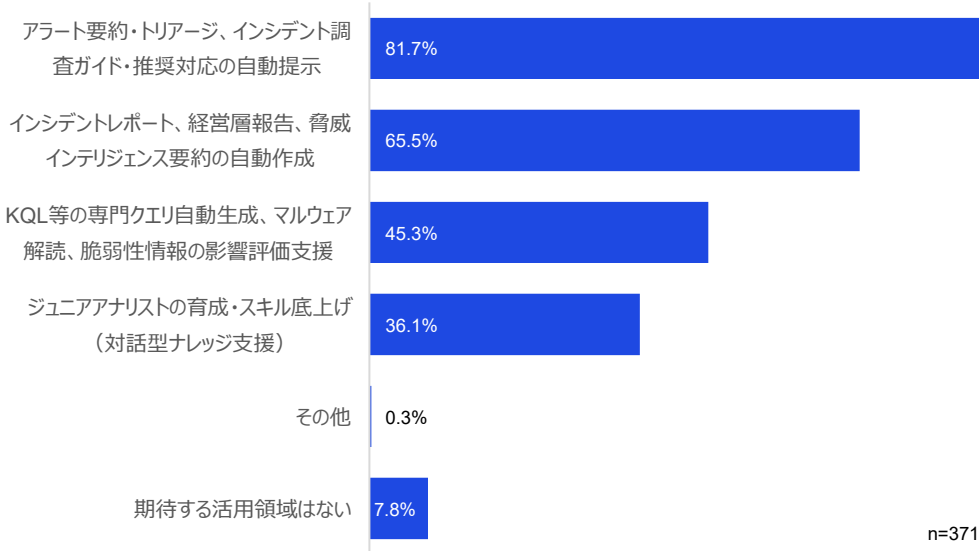


セキュリティ運用でのAI活用

セキュリティ運用におけるAIの活用領域への期待としては、「アラート要約・トリアージ、インシデント調査ガイド・推奨対応の自動提示」が最も高く、8割を超える企業が期待しています。また、「KQL等の専門クエリ自動生成、マルウェア解読、脆弱性情報の影響評価支援」は45.3%、「ジュニアアナリストの育成・スキル底上げ」は36.1%となっており、運用業務の効率化に加え、専門的な分析や人材育成へのAI活用も期待されていることがわかりました。

セキュリティ運用でのAI活用は、約8割の企業でアラート要約・トリアージに期待

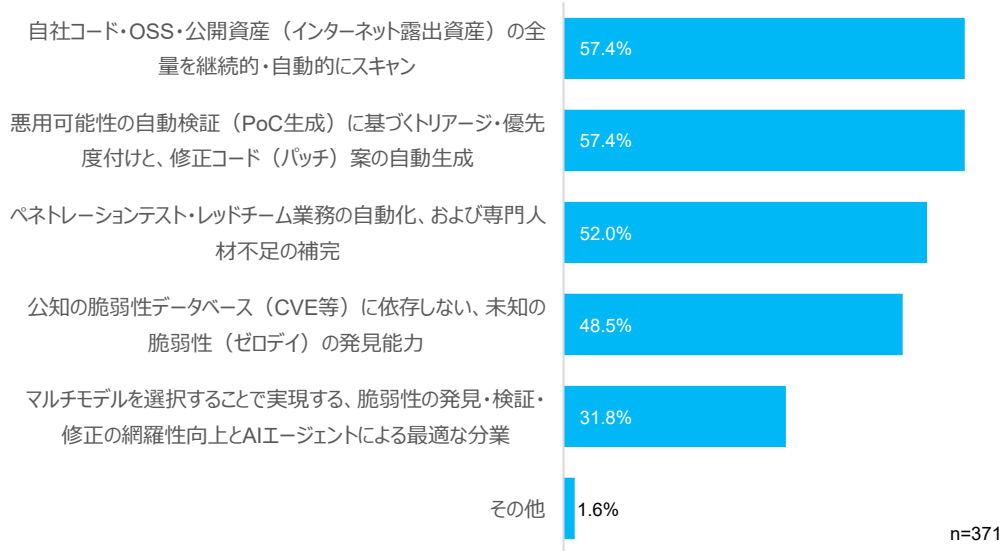
AIをセキュリティ運用に適用する場合、貴社で期待する活用領域を選択してください。（複数回答可）



AIが脆弱性の発見から悪用可能性の検証、修正コード提案までを自律的に実行するスキャン基盤に対しては、「自社コード・OSS・公開資産（インターネット露出資産）の全量を継続的・自動的にスキャン」と「悪用可能性の自動検証に基づくトリアージ・優先度付けと、修正コード（パッチ）案の自動生成」がともに57.4%と最も高く、半数を超える企業が期待を寄せています。

脆弱性のスキャン基盤については、自社コード・OSS・公開資産の全量スキャンに期待

「AIが脆弱性の発見から悪用可能性の検証、修正コード提案までを自律的に実行する基盤（複数のAIエージェントを連携させたスキャン基盤）」に対して、貴社が期待する機能・効果として該当するものを選択してください。（複数回答可）



KPMG日本のサイバーセキュリティサービス

KPMG日本のサイバーセキュリティサービス

KPMG日本では、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ご確認ください。



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。



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。



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。



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。



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。



オートモ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BCP

サイバー攻撃によるシステム停止を想定し、重要な業務やシステムの特定、代替運用・復旧手順の整備、経営層を含む訓練・演習による実効性の検証までを一貫して支援します。



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。



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。



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て支援します。



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。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供できるよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

文中の社名、商品名等は各社の商標または登録商標である場合があります。本文中では、Copyright、TM、Rマーク等は省略しています。

© 2026 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. C26-1053

© 2026 KPMG Forensic & Risk Advisory Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.