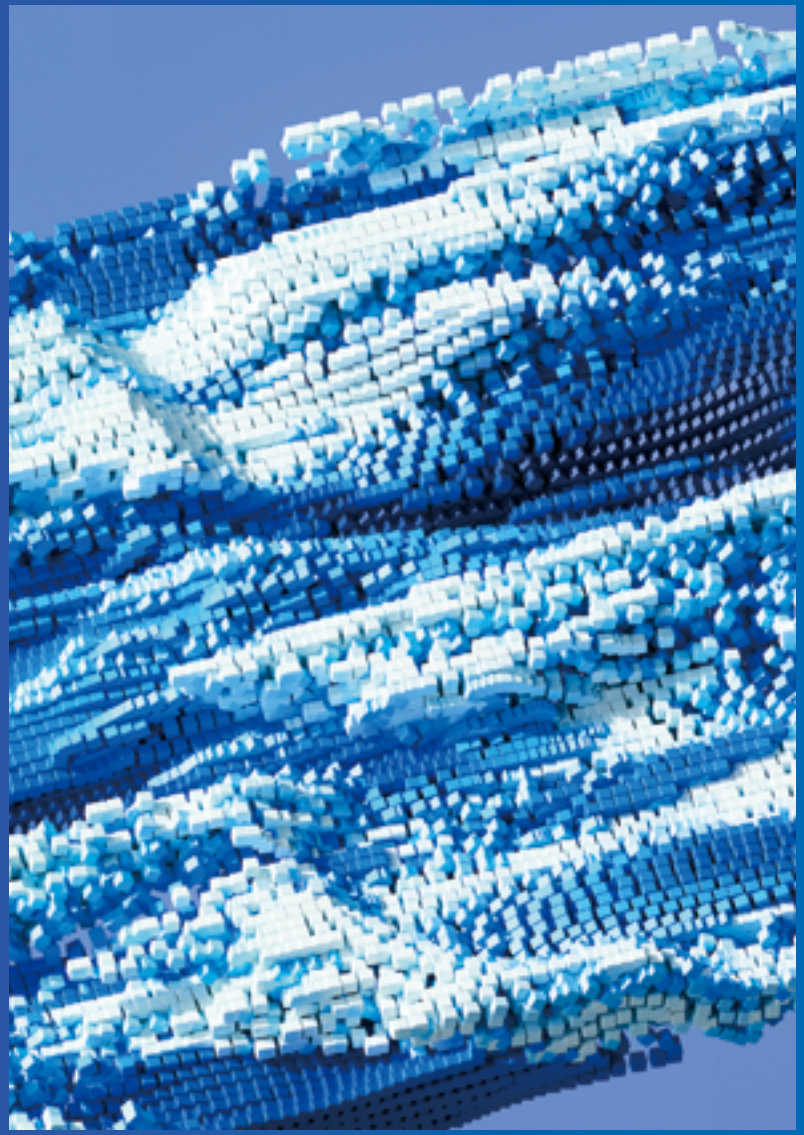
サイバーセキュリティサーベイ2025

KPMGジャパン



2025年4月

ご挨拶

生成AIの登場で、サイバー攻撃は一段と巧妙化しています。

特に、生成AIを使ったランサムウェア攻撃やAIが翻訳した自然な日本語が悪用される「ビジネスメール詐欺」の被害が増えています。ランサムウェアの身代金やサイバー攻撃の被害にあった企業の経済的な損失も深刻な問題になっており、サイバーセキュリティへの取組みは企業にとって重要な経営課題となっています。

OTセキュリティ、製品セキュリティ、AIセキュリティに関しては、海外での法整備が進み、日本企業においても海外の規制を考慮した対応が必須となりつつあります。

本レポートでは、2024年に実施したサイバーセキュリティに関する調査結果を基に、8つの重要テーマについてトレンドと必要となる取組みをまとめています。

皆様の今後のサイバーセキュリティ対策の高度化にお役立ていただけますと幸いです。

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。

2025年4月

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

© 2025 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.

Contents

ご挨拶 2

エグゼクティブサマリー 4

調査概要 49

KPMGジャパンの
サイバーセキュリティ
サービス 50

01 サイバー攻撃の実態 5

ランサムウェアによる企業への被害拡大
サイバーインシデントによる被害
サイバー攻撃の発生状況と攻撃手法
コラム｜サイバーインテリジェンスの活用

02 サイバーセキュリティ管理態勢 10

サイバーセキュリティに必要なリソースの明確化
サイバーセキュリティ人材
サイバーセキュリティ予算

03 サイバーセキュリティ対策 14

サイバーセキュリティ対策は最適な運用方法が重要
サイバーセキュリティ対策の実施状況
重要な情報の管理実態
コラム｜有事に備えたログ保管の重要性
脆弱性対応の実態
コラム｜ゼロデイ攻撃とNデイ攻撃
ハードウェア製品およびソフトウェア製品の
EOL/EOSへの意識
コラム｜経済安全保障推進法への対応
有事への備え
コラム｜サイバー保険とは

04 子会社管理 24

子会社ごとの取組みからグループ全体への取組みへ
子会社管理の実態
コラム｜サイバーセキュリティ業務の拡大に伴う
グローバル／グループでの取組み

05 委託先管理 28

サプライチェーンサイバーセキュリティ管理の厳格化
委託先管理の実態
コラム｜最新テクノロジーを用いた委託先管理の効率化

06 OTセキュリティ 32

海外企業に遅れるOTセキュリティ
制御システムサイバーセキュリティの成熟度
制御システムサイバーセキュリティアセスメント
コラム｜NIS2で求められるOTセキュリティ要件

07 製品セキュリティ 37

市場から求められる製品セキュリティ対応組織
製品セキュリティの成熟度
製品セキュリティ対策の実態
コラム｜CRAで求められるPSIRT/PSOC強化

08 AIセキュリティ 42

AI導入の拡大とリスク意識の高まり
AIの導入状況
AI導入のリスク
AIリスクを管理する組織、ルール、プロセスの整備状況
コラム｜AIリスクモニタリングの高度化

© 2025 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.

エグゼクティブサマリー

01 サイバー攻撃の実態

サイバー攻撃の巧妙化に伴い、被害金額が高額化しています。データを暗号化するだけでなく、内部システムに深く入り込み、高値で取引できそうな企業情報を抜き取り、それらを公表しないことと引き換えに高額な金銭を要求するケースが増えています。新たな攻撃手法に対する自社の取組みが十分か、定期的に確認し、継続的に改善することが求められます。

02 サイバーセキュリティ管理態勢

多くの企業で、サイバーセキュリティのリソース（人材・予算）不足が大きな課題となっています。サイバーセキュリティリスクへの対応は、社内のさまざまな部門にかかわるため、専任の担当部門を立ち上げ、サイバーセキュリティリスクに特化した責任範囲や指揮命令系統を整備することで、人材・予算を継続的に獲得する必要があります。

03 サイバーセキュリティ対策

サイバー攻撃の高度化に伴い、必要となる対策の種類・範囲が広がり、サイバーセキュリティ運用業務の負担が重くなっています。確保・育成した人材がサイバーセキュリティの企画業務にしっかりと携われるようにするために、運用業務の最適化が不可欠です。さらなる効率化を目指し業務でのAI活用が進みつつあり、サイバーセキュリティの運用においても、AIの有効活用を検討することが望まれます。

04 子会社管理

サイバーセキュリティ人材は、日本のみならず世界中で不足しており、（各国の）子会社ごとにサイバーセキュリティ対策を検討・導入・運用することが難しくなっています。子会社ごとに別々にサイバー攻撃に立ち向かうのではなく、限られた人材を有効に活用できるよう、世界中に分散するグループ企業全体で役割を分担し、最適なサイバーセキュリティ態勢を構築する必要があります。

05 委託先管理

他社と差別化された製品の生産にあたっては、サプライヤーに知的財産や機密情報を共有する必要がありますが、サプライヤーがサイバーセキュリティ対策を行っていない場合、これらの情報が悪意のある攻撃にさらされる可能性があります。サプライチェーンが攻撃を受け、部品やコンポーネントの生産が停止すると、製品の生産が停止するリスクがあります。

06 OTセキュリティ

欧州を中心に、サイバーセキュリティ法の整備が進んでおり、OT（Operational Technology）の領域も例外ではありません。日本企業では、海外企業と比較すると成熟度がまだ低く、改善の余地が大きい状況です。海外のサイバーセキュリティ法規制および海外企業の先進的な取組みを分析し、自社の取組みを継続的に改善することが望まれます。

07 製品セキュリティ

欧州サイバーレジリエンス法は、EU域内のデジタル製品に対するサイバーセキュリティ要件の厳格化を規定しており、同様の規制は英国や米国でも整備が進んでいます。製品セキュリティの対応については、対応する組織を設置していない企業も多く、グローバルで規制強化が進むなか、日本企業ではPSIRT/PSOC（Product Security Incident Response Team / Product Security Operation Center）の態勢整備が進んでいません。

08 AIセキュリティ

AIリスクを管理する組織、ルール、プロセスが「整備済みである」と回答した企業の割合は増加傾向にあるものの、全体の20%弱にとどまっています。AIを適切に活用しつつ競争力を高めるため、AIに関するガバナンス・態勢整備を進める必要があります。

© 2025 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.

サイバー攻撃の実態

01

ランサムウェアによる企業への被害拡大 6

サイバーインシデントによる被害 7

サイバー攻撃の発生状況と攻撃手法 8

コラム｜サイバーインテリジェンスの活用 9

© 2025 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.

ランサムウェアによる企業への被害拡大

新型コロナウイルス感染症の感染拡大を契機にテレワーク化が進み、各社のメール・インターネット等のOA環境がクラウドに移行したことで、ファイアウォールの内側で守る境界セキュリティから、ゼロトラスト環境へと移行しています。こうした変化に合わせて攻撃者も攻撃シナリオを変化させています。また、誰もがアクセスできるクラウド上に情報を保管することから、不注意による設定ミスをついた攻撃等も増加しています。

独立行政法人 情報処理推進機構（IPA）が公表する「情報セキュリティ10大脅威 2024（組織）」では、2024年に引き続き、2025年も「ランサム攻撃による被害」が1位となりました。ランサムウェアは、インターネット経由で不正に企業内に侵入し、データを暗号化して利用不可能にすることで身代金を要求するものです。国内でも被害が続出しており、数十万人規模の個人情報流出につながった事例もあります。

2016年から2022年頃まではEMOTET（エモテット）に代表される、メールシステムに感染して取引先など他社に拡散させられる“ばらまきメール”パターンが目立ち、不特定多数を対象としたものが多くありました。しかし近年は、ランサムウェアでデータを暗号化するだけでなく、内部システムに深く入り込み、ある程度の高値で取引できそうな企業情報（機密情報・個人情報等）を抜き取り、それらを公表しないことと引き換えに高額な金銭を要求するケースも増えてきています。

今回調査では、1,000万円以上の被害を受けた企業が前回調査の30.0%から44.0%に増加しています。また、1億円以上の被害を受けた企業も8.0%と前回調査の6.7%よりも増加しました。前述のとおり、最も高額で取引できる情報を抜き取るため企業ネットワーク内を探索する攻撃が増え、被害金額も高額化していると考えられます。また、今回の調査結果では、顧客や取引先への被害よりも自社への被害が発生した割合が大きく増加傾向となりました。

ランサムウェアによる攻撃で被害が発生した企業は10.7%となり、10社に1社はランサムウェアの被害があったことがわかりました。

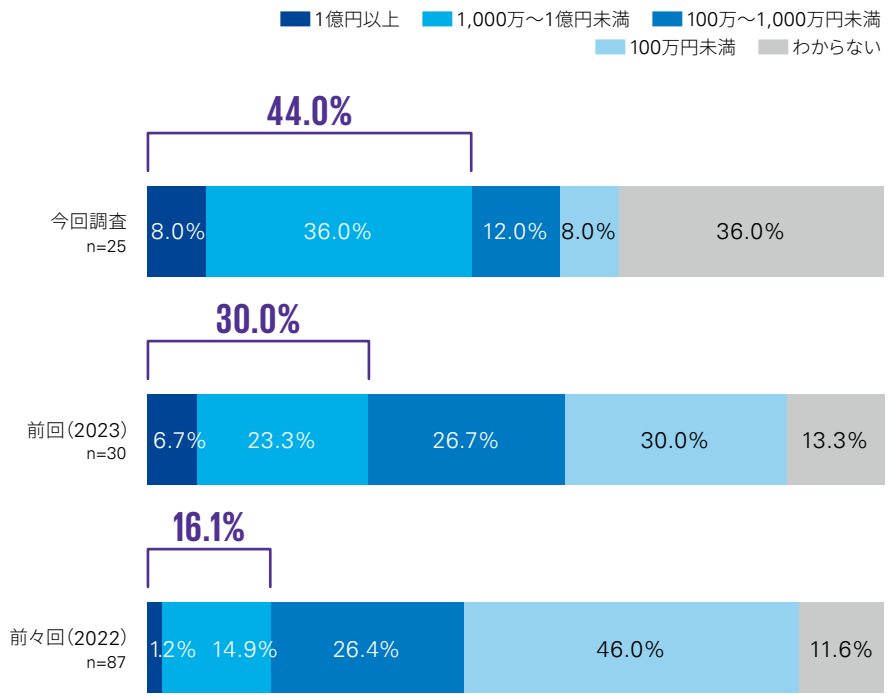
より高額な身代金を要求するため、サイバー攻撃はさらに巧妙化しています。セキュリティ対策は一度行えばよいというものではなく、攻撃手法の変化をしっかりと捉え、新たな攻撃手法に対して自社の取組みが十分かを定期的に確認し、継続的に改善していくことが求められます。

© 2025 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.

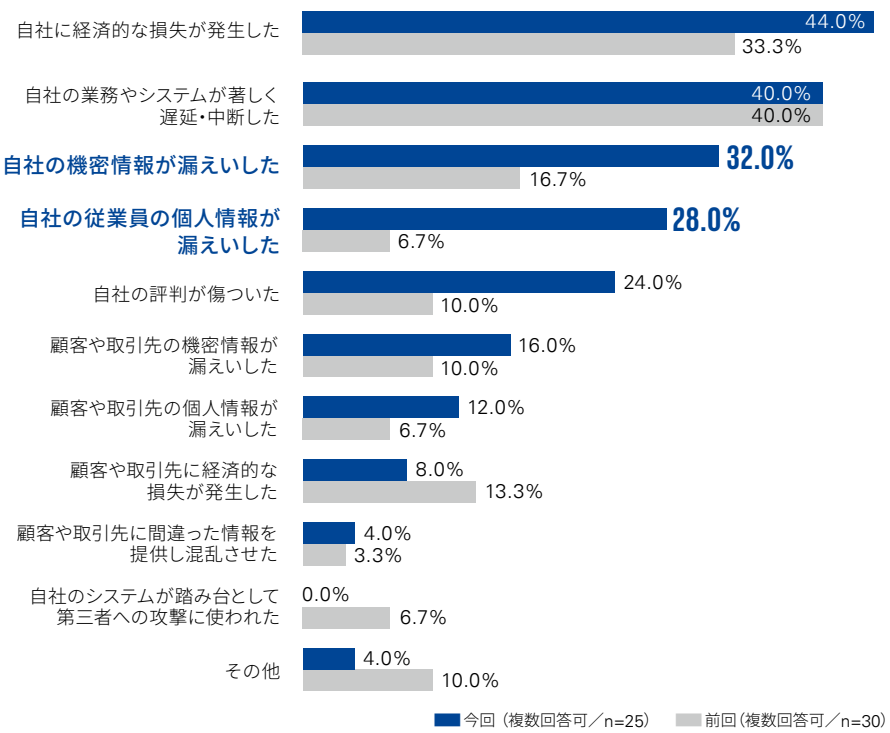
サイバーインシデントによる被害

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1,000万円以上となったとの回答は、前々回（2022年）調査が16.1%、前回（2023年）調査が30.0%、今回調査が44.0%と、年々高額化しています。また、1億円を超える被害があった企業も年々増加しています。
過去1年間に発生したサイバーインシデントによる被害内容についても、前回調査と比較し、ほとんどの項目で増加がみられます。特に、「自社の機密情報が漏えいした」「自社の従業員の個人情報が漏えいした」が大きく増加しています。

過去1年間に発生したサイバーインシデントの合計被害額



過去1年間に発生したサイバーインシデントによる被害内容

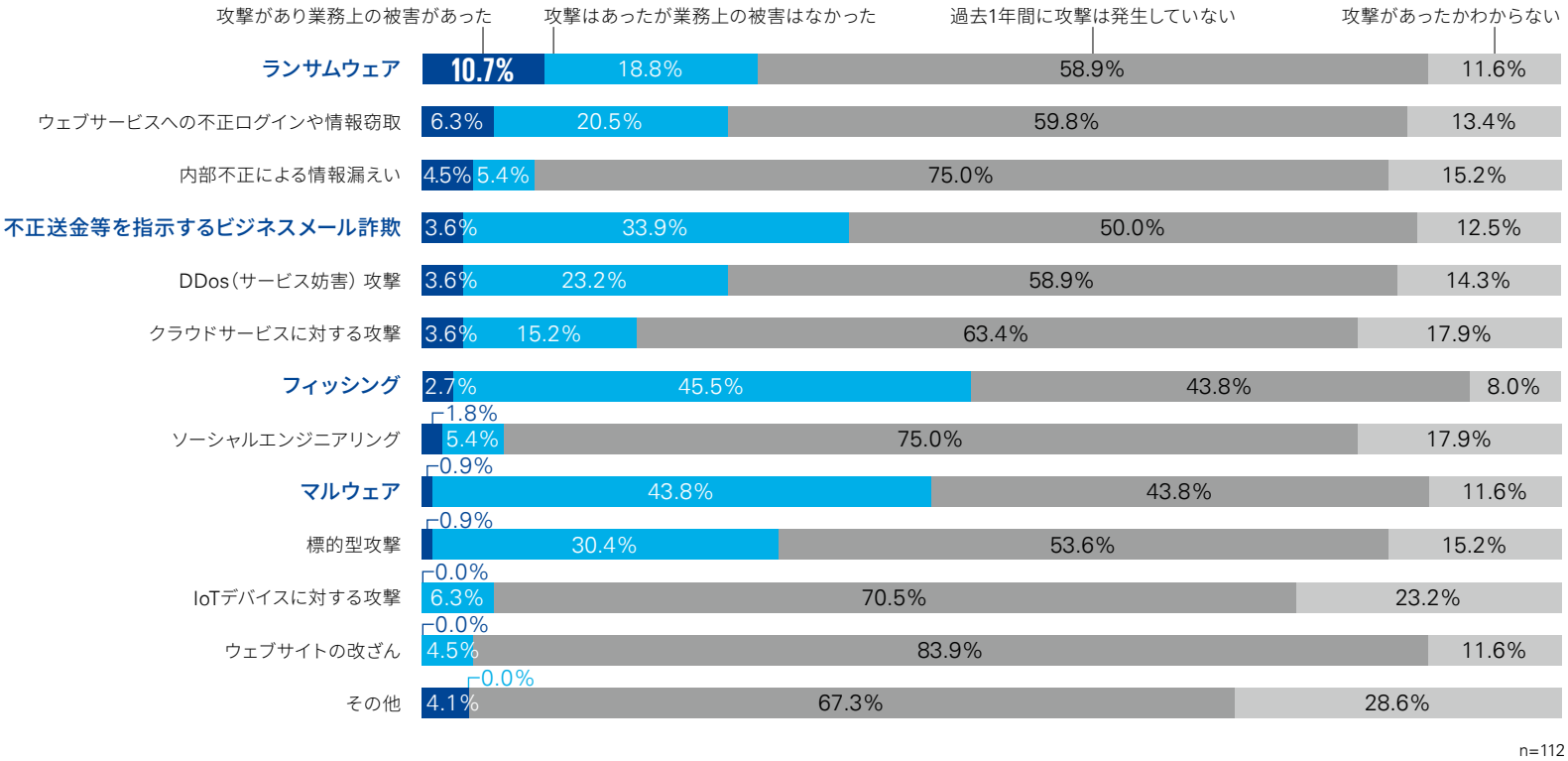


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

サイバー攻撃の発生状況と攻撃手法

業務上の被害があったサイバー攻撃は「ランサムウェア」という回答が10.7％と最も多くなりました。また、業務上の被害はなかった攻撃と合わせると「フィッシング」「マルウェア」に続いて、「不正送金等を指示するビジネスメール詐欺」の攻撃が多くみられました。生成AIの発達により、自然な日本語でのビジネスメール攻撃が増えており、企業はさらなる注意が必要です。

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）

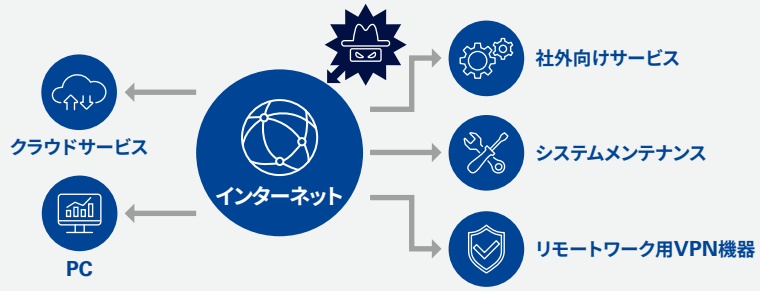


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

コラム サイバーインテリジェンスの活用

日々巧妙化するサイバー攻撃に対して、多くの企業でさまざまな取組みが行われていますが、自社のサイバーセキュリティリスク（攻撃に利用される可能性のあるセキュリティホールや機密情報の漏えい等）を発見することに着目した、サイバーインテリジェンスの活用が注目されています。
サイバーインテリジェンス調査では、攻撃者の目線でインターネットを介して侵入の入口となり得る“アタックサーフェス”の調査および、攻撃につながる可能性のある情報（侵入するためのキーとなるクレデンシャル情報、漏えいした機密情報、攻撃の兆候に関する情報等）のダークウェブ等での流通についての調査を実施します。
システム担当者やセキュリティ担当者が認識していないシステムの脆弱性や漏えいしたクレデンシャル情報が検出されるケースも多いため、定期的なチェックを実施することが望まれます。

アタックサーフェスの調査対象



- 多くのランサムウェア攻撃は、VPN機器の脆弱性や設定の不備を突かれて侵入されています。
- システム担当者が認識していない、シャドウIT（いわゆる野良サーバ等）が検出されるケースもあります。
- 攻撃者による侵入の入口となり得るインターネットとの接点における脆弱性（古いOSの利用、セキュリティパッチの未適用、ネットワーク設定の不備等）を探索します。

クレデンシャル情報等の調査対象

サーフェスウェブ	一般に公開されたウェブサイト 一般的な検索エンジンで検索できる
ディープウェブ	ログインを必要とする会員制サイト等 一般的な検索エンジンでは検索できない
ダークウェブ	匿名性が確保された特殊なネットワーク上のウェブサイト 通常のウェブブラウザでアクセスできず、特殊なソフトウェアを通じたアクセスが必要

- 社内ネットワークにアクセスするためのIDとパスワードが流通している場合、攻撃者が従業員に成りすまして侵入してくる可能性があります。
- 社内の決裁権限者のプロファイル情報が流通している場合、ビジネスメール詐欺等に利用されるケースがあります。
- ダークウェブへのアクセスはリスクが伴うため、調査は専門業者に依頼することを推奨します。

© 2025 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.

サイバーセキュリティ管理態勢

02

サイバーセキュリティに必要なリソースの明確化 11

サイバーセキュリティ人材 12

サイバーセキュリティ予算 13

© 2025 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.

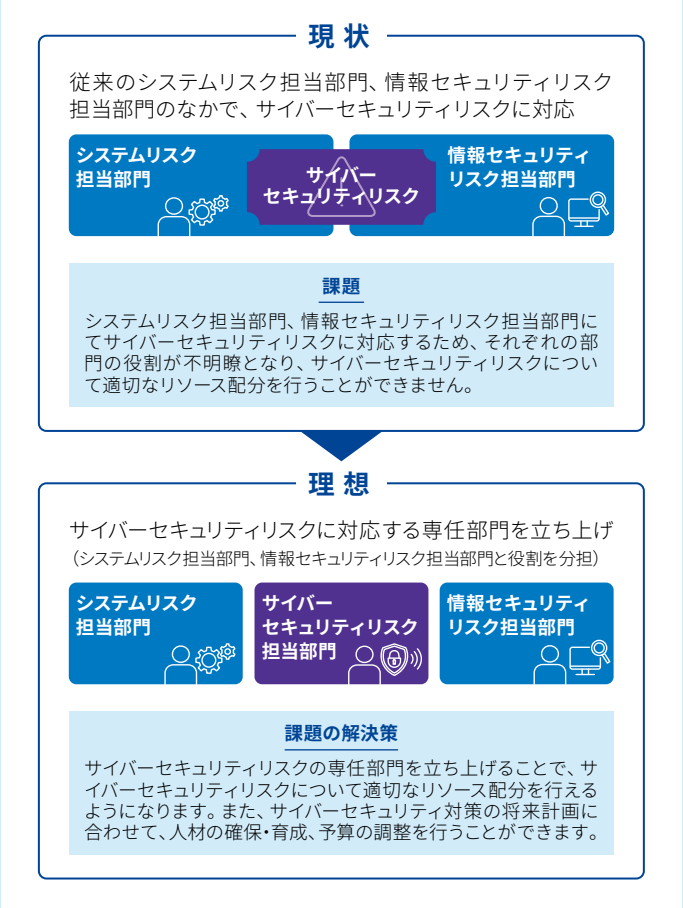
サイバーセキュリティに必要なリソースの明確化

サイバーセキュリティ人材の質的・量的不足は、総務省の情報通信白書にて毎年警鐘が鳴らされています。

今回調査においても、サイバーセキュリティ組織の規模（人数）は適切かという問いに対して70%以上の企業が不足していると回答しています。また、サイバーセキュリティ予算に関しても、不足していると感じている企業が約65%を占めています。

サイバーセキュリティ人材・予算のリソース不足を感じている背景としては、サイバーセキュリティリスクへの対応について役割分担が明確になっていないことが要因として考えられます。サイバーセキュリティは新しいリスクであり、従来のシステムリスクと情報セキュリティリスクにまたがるため、システムリスク担当部門、情報セキュリティリスク担当部門のみを置いている組織では、それぞれの部門の管掌のなかでサイバーセキュリティリスクに対応しなくてはなりません。このような環境では、それぞれの部門においてどこまでが管掌範囲となるのかが不明瞭で、人材・予算が不明確になりがちです。サイバーセキュリティリスクの高まりに合わせて、サイバーセキュリティリスク担当部門を独立させ、システムリスク担当部門、情報セキュリティリスク担当部門との関係を整理したうえで、サイバーセキュリティリスクに特化した責任範囲や指揮命令系統を整備することが重要です。

サイバーセキュリティリスクを経営上の重要課題としてしっかりと捉え、サイバーセキュリティリスクに関する基本方針および対応計画を定めることを推奨します。

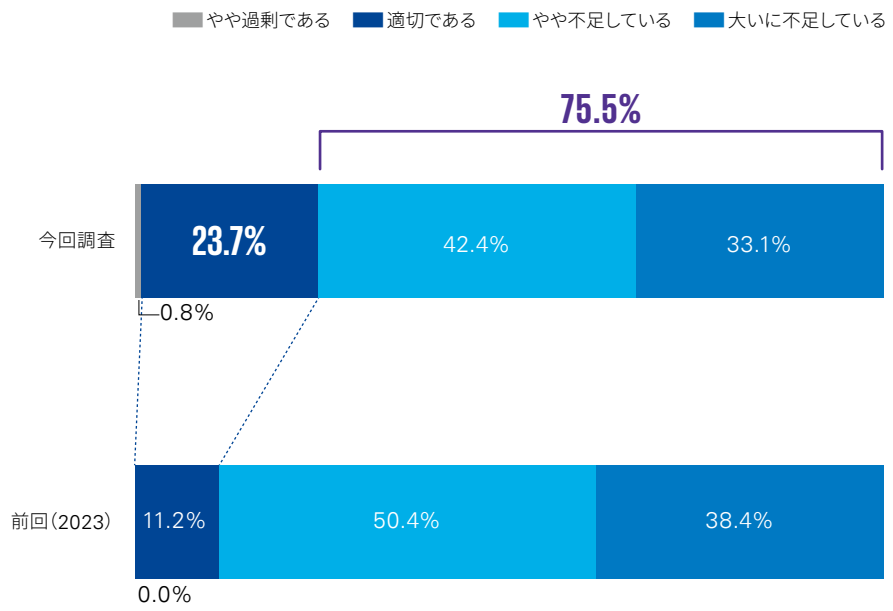


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

サイバーセキュリティ人材

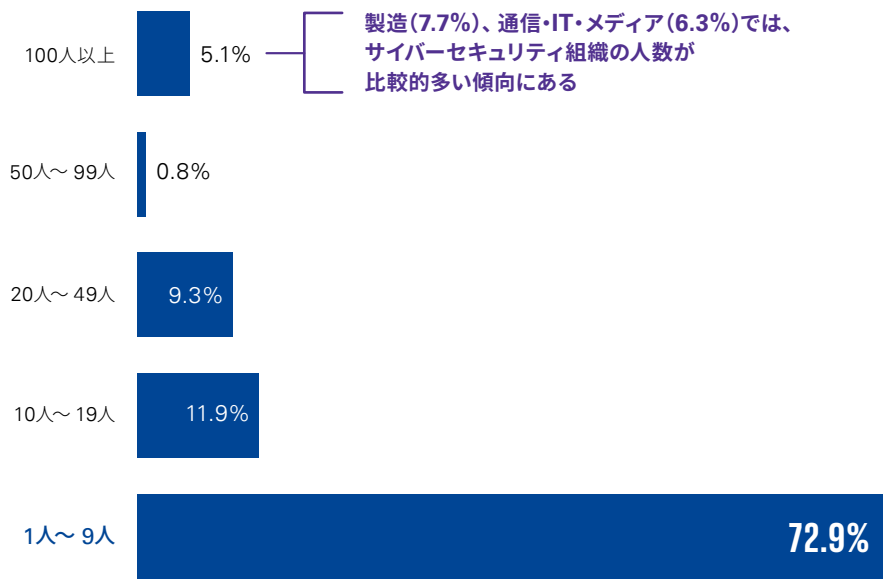
サイバーセキュリティ人材が「やや不足している」「大いに不足している」との回答は75.5%となり引き続き高い水準となっています。ただし前回調査と比較すると「適切である」との回答が11.2%から23.7%へと増加しています。
サイバーセキュリティ組織の人数は10人未満という回答が72.9%を占め、「やや不足している」「大いに不足している」との回答割合と重なります。サイバー攻撃の高度化に合わせて幅広い対策が必要となるなか、組織内の役割分担を明確にし、人材の専門性を高めていくことが求められています。

サイバーセキュリティ人材の充足・不足感



今回（n=118）／前回(n=258)

サイバーセキュリティ組織の人数



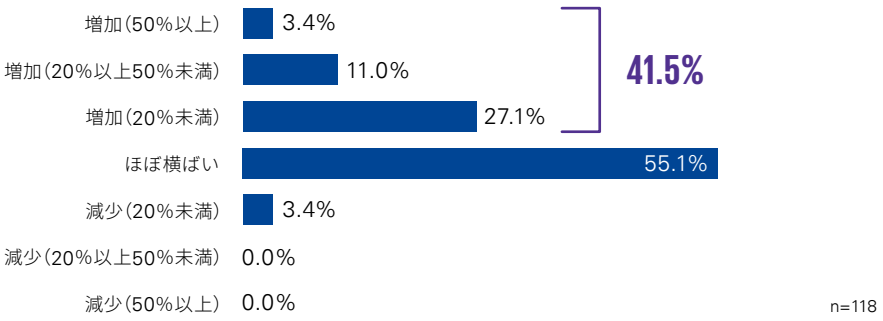
n=118

© 2025 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.

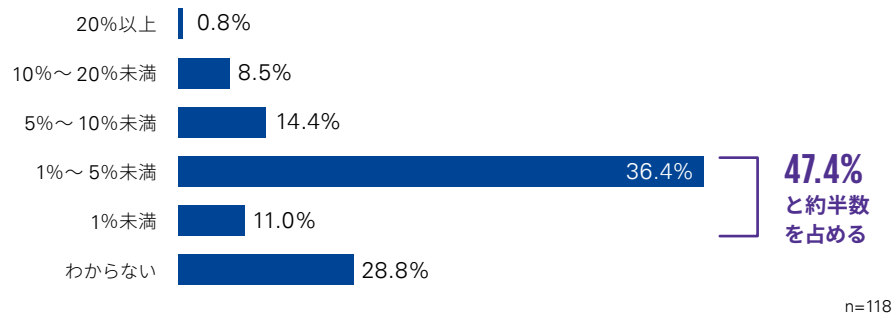
サイバーセキュリティ予算

2023年度から2024年度へのサイバーセキュリティ予算を増額したとの回答が41.5%となりました。しかし、サイバーセキュリティ予算が「やや不足している」「大いに不足している」との回答は64.5%と高い水準にとどまっています。また、IT予算全体に対するサイバーセキュリティ対策予算の比率が5%未満との回答は約半数となっています。
サイバーセキュリティの中期計画は49.2%の企業にて策定されていない結果となりました。

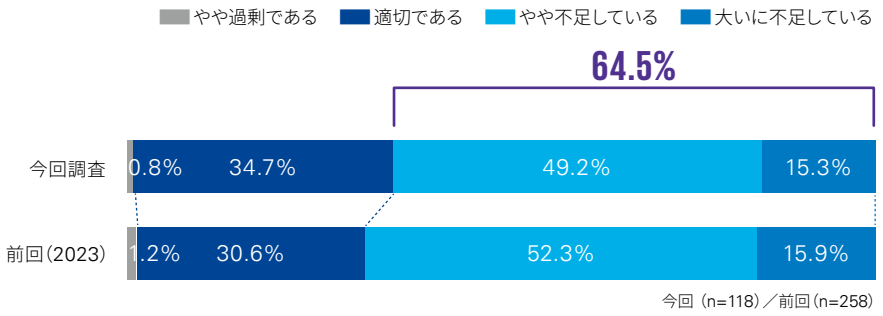
2023年度から2024年度へのサイバーセキュリティ予算額の推移



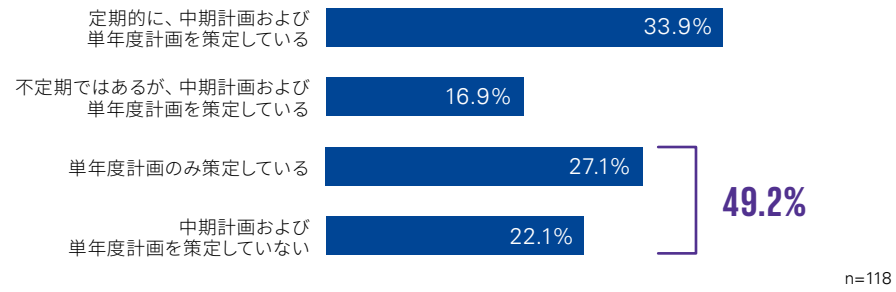
IT予算全体に対するサイバーセキュリティ対策予算の比率



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の中期計画、単年度計画の策定状況



© 2025 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.

サイバーセキュリティ対策

03

サイバーセキュリティ対策は最適な運用方法が重要 15

サイバーセキュリティ対策の実施状況 16

重要な情報の管理実態 17

コラム｜有事に備えたログ保管の重要性 18

脆弱性対応の実態 19

コラム｜ゼロデイ攻撃とNデイ攻撃 20

ハードウェア製品およびソフトウェア製品のEOL/EOSへの意識 21

コラム｜経済安全保障推進法への対応 22

有事への備え 23

コラム｜サイバー保険とは 23

© 2025 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.

サイバーセキュリティ対策は最適な運用方法が重要

今回調査では、一定のセキュリティソリューションを導入している状況が読み取れるものの、「導入したが、運用に一部課題がある」、「導入したが、うまく運用できていない」のように、不安視する声が多くありました。またサイバーセキュリティ対策について、右記の傾向がわかりました。

これらより、セキュリティソリューションごとの運用だけでなく、そもそもセキュリティの運用（1. 重要な情報の定義、2. 脆弱性対応の基準、3. IT資産管理）にも課題があることが読み取れます。

サイバー攻撃の高度化に伴い、セキュリティ対策とセキュリティ運用業務が増えています。セキュリティ人材が不足するなか、確保・育成した人材がセキュリティの企画業務にしっかりと携われるようにするために、運用業務の最適化を急ぐ必要があります。業務効率化の手助けとして、業務でのAI活用が進みつつあります。サイバーセキュリティ運用においても、AIの有効活用を検討することが望まれます。

1 重要な情報がどれなのかを明確に定義できていない

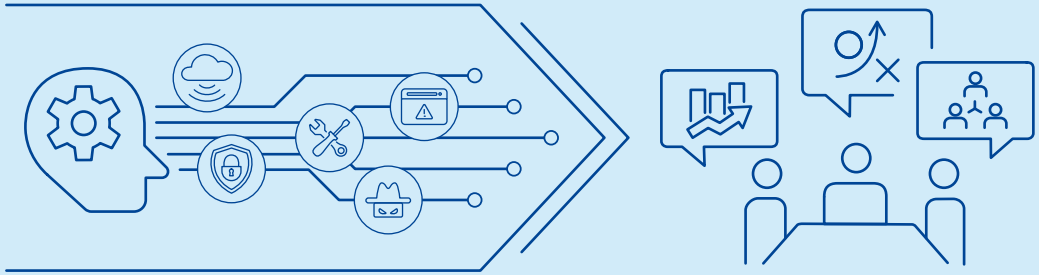
重要な情報を適切に管理できている企業は30.2%にとどまっています。
そもそも重要な情報の特定ができていない企業は30.6%となっています。

2 脆弱性対応の基準が定められていない

パッチ適用は高い割合で実施されていますが、
パッチ公開から適用までの期間を決めていない企業が39.2%を占めています。

3 IT資産管理ができていない

脆弱性管理の前提となるハードウェア製品やソフトウェア製品の
資産管理の仕組みができている企業は5.9%にとどまっています。

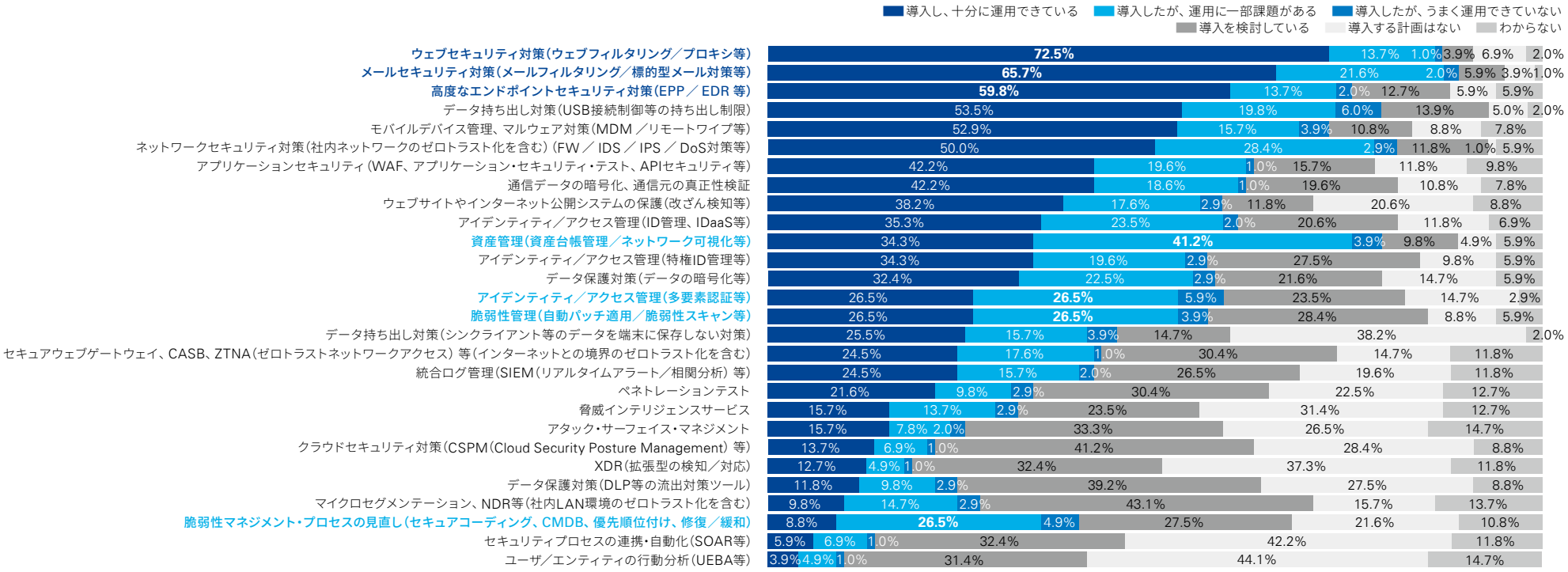


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

サイバーセキュリティ対策の実施状況

ウェブセキュリティ、メールセキュリティ、エンドポイントセキュリティ等の従前からある対策については、「導入し、十分に運用できている」との回答が約60%を超え、十分に運用できている様子がうかがえます。
一方、資産管理では41.2%、アイデンティティ／アクセス管理（多要素認証等）、脆弱性管理および脆弱性マネジメント・プロセスの見直しでは26.5%が「導入したが、運用に一部課題がある」と回答しています。

サイバーセキュリティ対策の導入状況

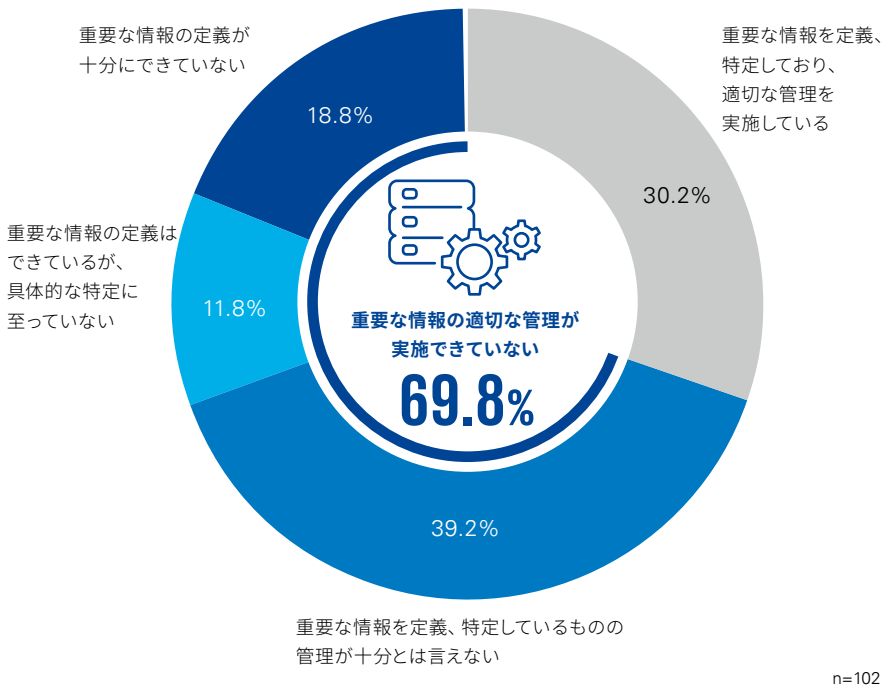


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

重要な情報の管理実態

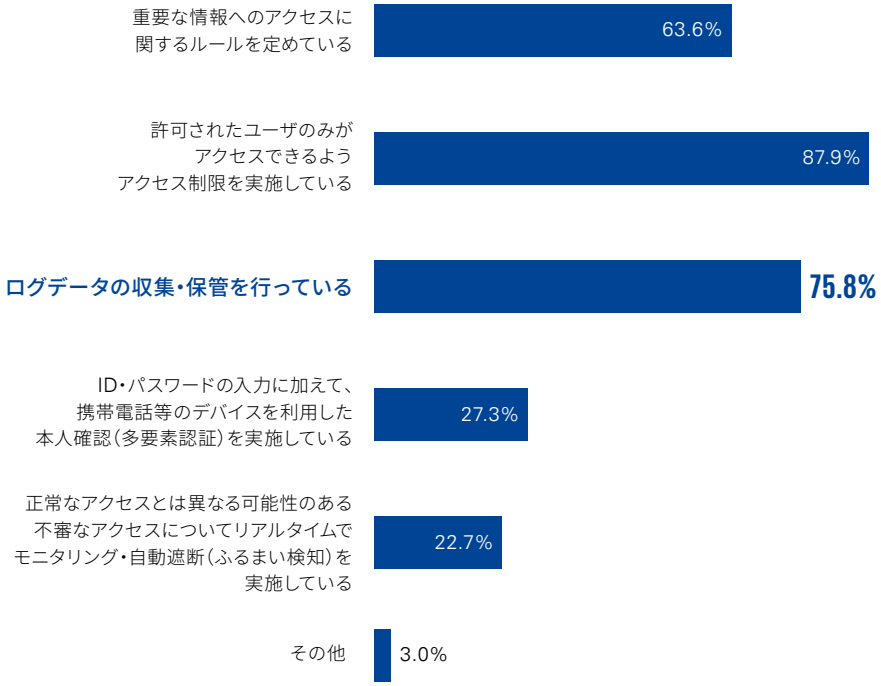
企業で扱うデータは多岐にわたり、クラウド環境・オンプレミス環境の共存やITインフラ環境の複雑化により、情報の管理は困難さを増しています。そのような状況のなか、重要な情報を定義、特定し、適切な管理を実施することは難しく、69.8%の企業が適切な管理が実施できていないと回答しています。
また、重要な情報に対する技術的措置について、ログデータの収集・保管を行っている企業は75.8%にとどまっています。リモートワークの浸透に伴い、内部不正による情報漏えい事案が増えており、いつ誰がアクセスしたのかをしっかりと記録することが求められます。

重要な情報の管理状況



n=102

重要な情報に対する技術的措置



複数回答可／n=102

© 2025 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.

コラム 有事に備えたログ保管の重要性

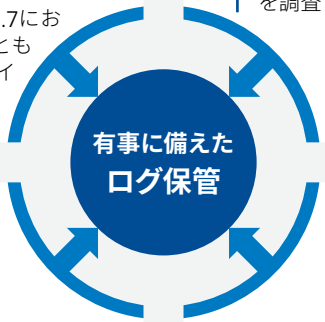
サイバーインシデント発生時には、ログを分析し、攻撃者の活動を解析することが重要となります。ログを分析することで、侵入経路や抜き取ったデータを特定することができるため、アクセスログ・監査ログの確保はきわめて重要です。しかし実際の調査の現場では、一部のログしか保管されていなかったり、保管期間が短く消えてしまったりして、十分な調査ができない状況が多くあります。またログは取得されていても、共通IDの使用等により個人が特定できないケースもみられます。
有事の際にサイバー攻撃の状況を正確に把握するためにも、不正アクセス等の異常をいち早く検知するためにも、統合的なログ管理を行うことが重要です。

1 ポリシー・ガイドラインの整備

- ログ保管に関するポリシーに、何のログをどの期間取得するのか具体的に明記されていない例が多くみられます。また、システムのデフォルト値のまま運用されている例も多数みられます。
- クレジットカードのセキュリティ基準であるPCIDSSの要件10.7において、「監査証跡の履歴を少なくとも1年間保持する。少なくとも3ヵ月はすぐに分析できる状態にしておく（オンライン、アーカイブ、バックアップから復元可能など）」と記載されています。

2 ログ収集対象の選定

- 認証システムやネットワークログ等、一部のシステム・機器のみをログ収集対象としている例がみられます。サイバー攻撃では、侵入後にネットワーク内を水平展開して偵察活動や権限昇格を行っていくため、攻撃の全容を調査するには、抜け漏れなくログが収集されていることが重要です。



3 ログ保管期間の最適化

- ログの種類（アクセスログ、認証ログ、イベントログ、アプリケーションログ、操作ログなど）ごとに保管期間を定めます。
- 定めた期間に確実に保管されているか、すべての取得対象のログについて確認を行い、抜け漏れを防止します。

4 保管方法・モニタリング

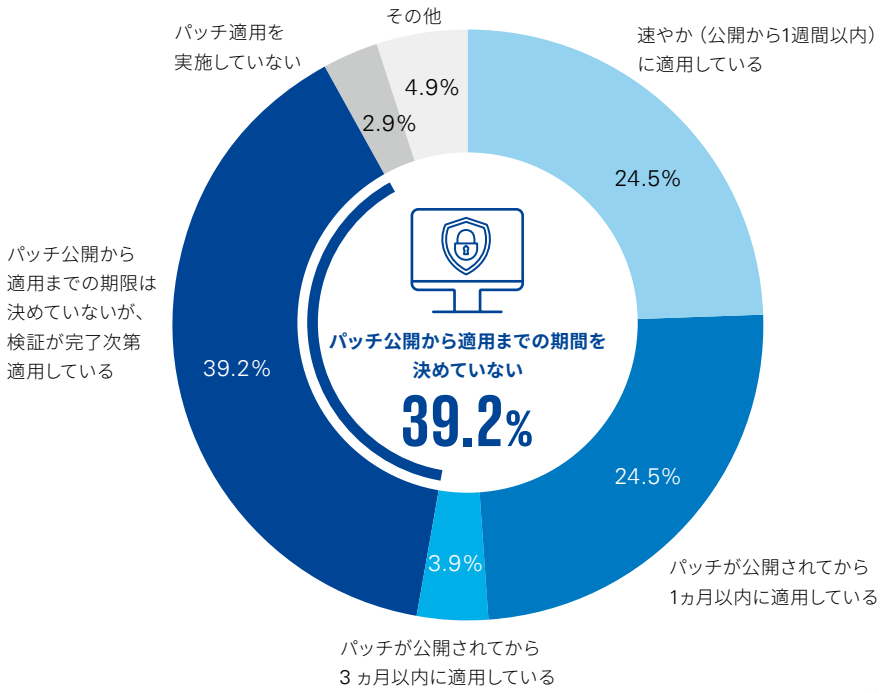
- 一定期間経過したログについてもオフラインで保管し、その後廃棄する運用サイクルを整備します。
- ログはシステム・機器ごとに保管するのではなく、統合ログ管理システムで一括管理を行うことが望まれます。
- 異常なふるまいの自動検知結果の確認頻度等、モニタリング方法を定期的に見直し、改善します。

© 2025 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.

脆弱性対応の実態

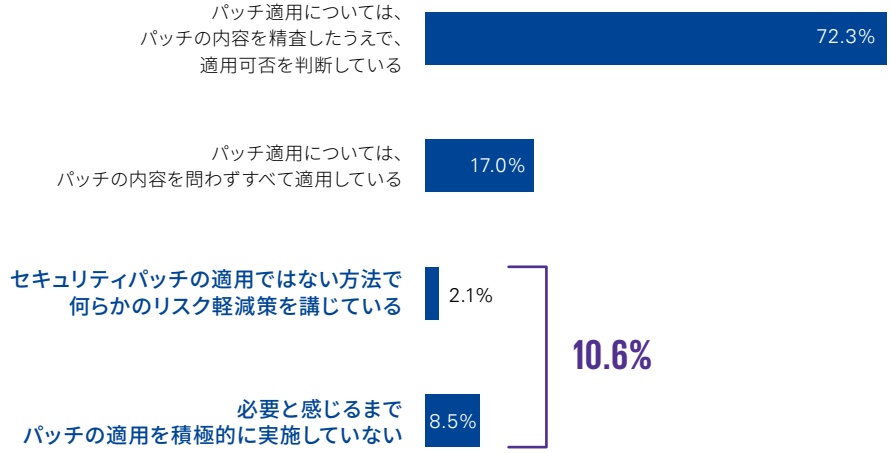
パッチ（修正プログラム）の適用は高い割合で実施されていますが、パッチ公開から適用までの期間を決めていない企業が39.2%を占めています。都度判断としている企業では緊急対応を要するパッチについて調整に時間がかかる例も見受けられるため、一定の基準を設けることが求められます。
また、パッチ適用によるシステムの不具合発生を想定し、10.6%の企業が「セキュリティパッチの適用ではない方法で何らかのリスク軽減策を講じている」「必要と感じるまでパッチの適用を積極的に実施していない」と回答しています。

脆弱性対応の実態



n=102

パッチの適用方針



n=102

© 2025 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.

コラム ゼロデイ攻撃とNデイ攻撃

すでに公開されている脆弱性を利用するNデイ攻撃については、リリースされているパッチを適用することで攻撃を防ぐことが可能です。
パッチがリリースされる前の脆弱性をつくゼロデイ攻撃については、万が一攻撃されたとしてもいち早く検知・対処できるように
ネットワークやエンドポイント等のセキュリティを強化し、「入口対策」だけでなく、「内部対策」・「出口対策」を行います。

	ゼロデイ攻撃	Nデイ攻撃
❶ 攻撃手法	• 未知の脆弱性（未公開あるいはベンダー・開発者自身もまだ知り得ない脆弱性で、パッチの対処方法が確立されていない状態）を利用し攻撃を行う	• すでに公開されている脆弱性を利用し、パッチの対処を行っていない企業を標的にして攻撃を行う
❷パッチ	• 未リリース	• リリース済み
❸攻撃者の技術ハードル	• 高い （未知の脆弱性を発見し、さらに修正プログラムのリリースまでのわずかな期間で攻撃を行う）	• 低い （悪用できる脆弱性の特定がリリース情報等により容易に可能、攻撃用のツールがダークウェブ等で入手可能）
❹ 攻撃者のタイプ	• 自身の技術力を誇示したい	• 効率的に攻撃したい （身代金の要求等、金銭が目的）
❺対策	• 未知の脆弱性に対する攻撃への予測・検知は困難なため、多層防御により攻撃を防ぐ ・OS／アプリケーションを最新版にアップデート ・アンチウイルスソフトの定義ファイルを常に最新化 ・ネットワークセキュリティの強化 ・EDR（不審なふるまいの検知）の強化	• 公開された脆弱性に対して迅速に対応を行う • パッチがリリースされない古いバージョンのハードウェア製品、ソフトウェア製品は利用しない

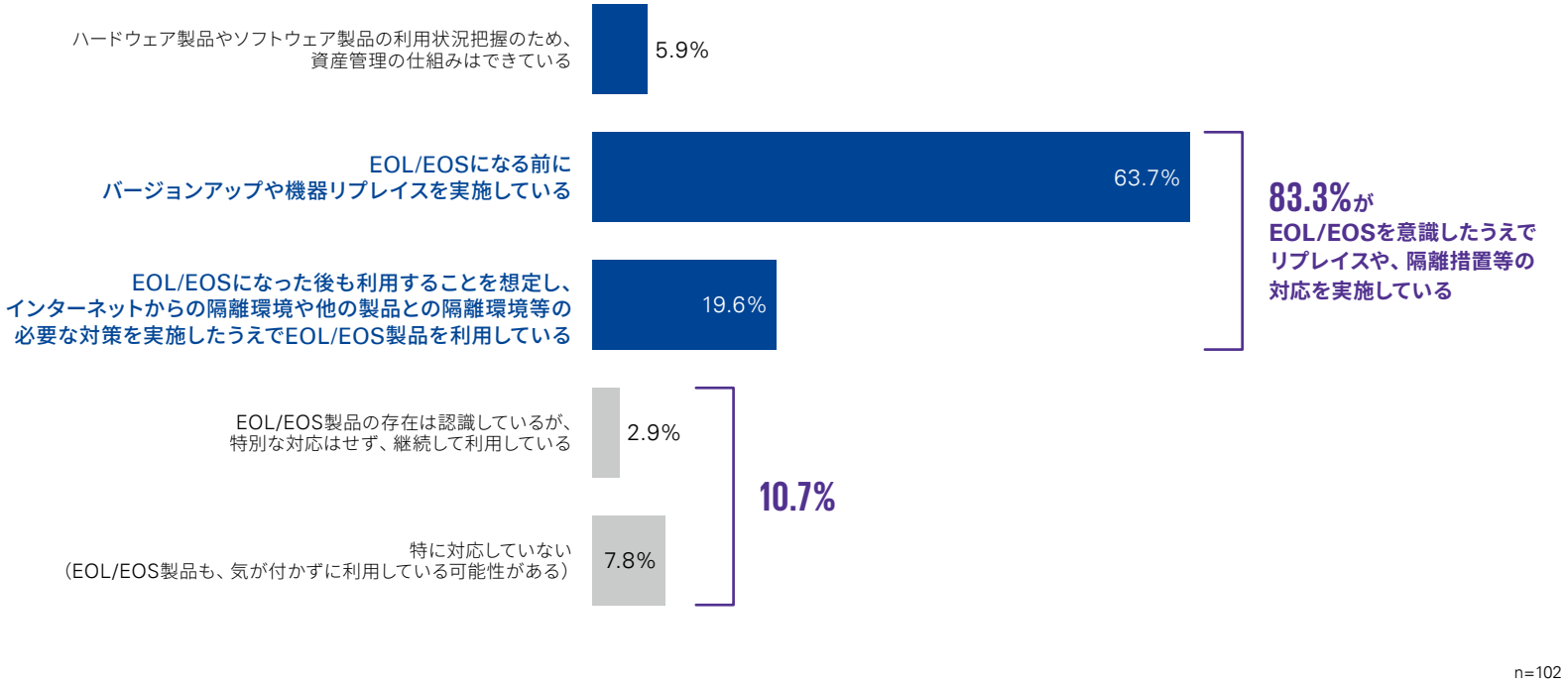
© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ハードウェア製品およびソフトウェア製品のEOL/EOSへの意識

サーバやネットワーク機器、クライアントPC等のハードウェア製品やセキュリティソフト含む各種ソフトウェア製品にはライフサイクルが存在し、いずれの製品も一定期間で販売・サポートが終了します。これらのライフサイクルを意識したうえで、回答者の83.3%がEOL※1/EOS※2を見越して計画的にバージョンアップや機器リプレイスを実施したり、継続利用する場合も必要な対策措置を実施したりしています。
一方で、10.7%の企業が「EOL/EOS製品の存在は認識しているが、特別な対応はせず、継続して利用している」「特に対応していない」と回答しています。

※1EOL：End of Life　※2EOS：End of Sales、もしくは、End of Support

EOL/EOSへの対応状況



© 2025 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.

コラム 経済安全保障推進法への対応

2024年5月より「基幹インフラ役務の安定的な提供の確保に関する制度」についての運用が開始され、電気、ガス、水道、鉄道、航空、放送、金融等の重要インフラを支える企業に適用されています。
また、独立行政法人 情報処理推進機構（IPA）より「重要情報を扱うシステムの要求策定ガイド」が公開されており、そのなかで「自律性確保のための要求事項（ソフトウェア）」として、脆弱性やEOL※1/EOS※2への対応についてのガイドラインが示されています。
以下の表では、ソフトウェアの完全性・可用性確保のための対策のうち、脆弱性対応やEOL/EOS対応に関する項目を抜粋し、一部加工しています。

※1EOL：End of Life　※2EOS：End of Sales、もしくは、End of Support

ソフトウェアの完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
C-5 ソフトウェアのメンテナンスポリシーの確立（バージョン管理含む）	• ソフトウェアに関する脆弱性などの問題が発生した際に適時解決が図れないことがないようにする	• ソフトウェア部品表に掲載された全ての要素について、脆弱性などの問題が発生した際のメンテナンスポリシーを事前に整理すること
C-6 ソフトウェアの継続的リスク評価	• ソフトウェアのメンテナンス終息や利用停止などが突然判明することがないようにする	• ソフトウェア部品表に掲載された要素の全てについて、定常運用に必要なバージョンアップの頻度や、バージョンアップの提供が断絶するリスクを継続的に評価すること
C-10 脆弱性などへの対応	• ソフトウェアの脆弱性などによって、システムが不適時に停止することを防止する。また、重要情報を扱うシステムの管理者が脆弱性などの情報を適時かつ十分に取得できないことで適切な対応が遅れる事態を防止する	• ソフトウェア部品表に掲載された要素に発見された脆弱性に対して速やかに適切な対応をするとともに、その対応状況を逐次共有すること • ソフトウェア部品表に掲載された要素について、公知のセキュリティ脆弱性情報などへの対応状況をリアルタイムに取得できるAPIまたは一覧できるダッシュボードなどを提供すること • 公知のセキュリティ脆弱性情報に対応するだけではなく、新たな脅威や脆弱性を発見して予防的対応を行える体制を保持していること

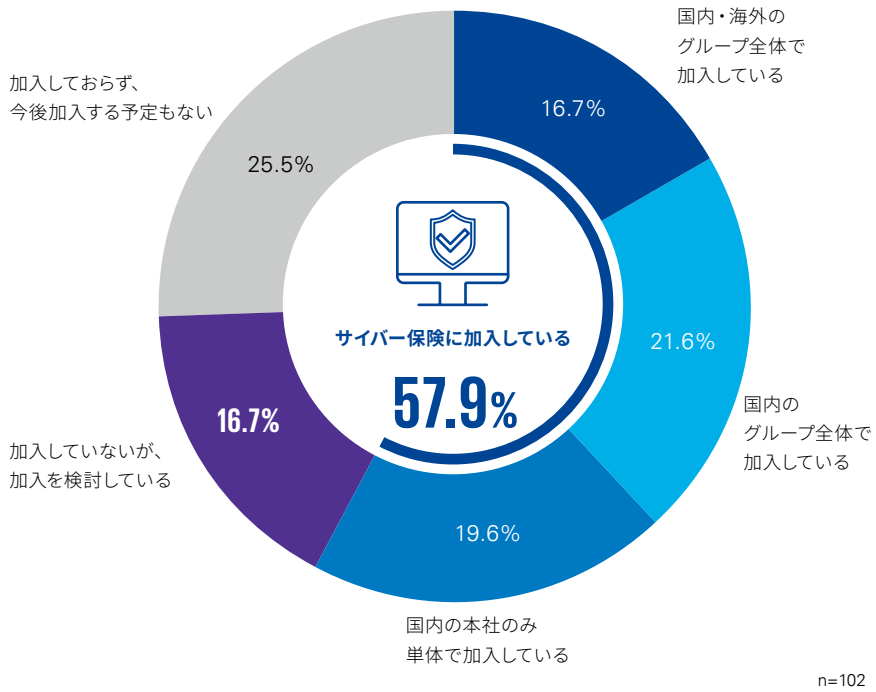
出所：独立行政法人 情報処理推進機構（IPA）「重要情報を扱うシステムの要求策定ガイド　Ver.1.0　2023年7月」版よりKPMG作成

© 2025 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.

有事への備え

さまざまなセキュリティ対策を講じていたとしても、サイバー攻撃により、システムの停止や情報漏えい等の被害が発生する可能性はあります。
サイバー攻撃の被害にあった際に損害賠償や調査等の費用を補償するサイバー保険について、57.9%が加入しており、16.7%が加入を検討していると回答しています。

サイバー保険の加入状況



n=102

コラム　サイバー保険とは

本調査においては、サイバー保険に加入しているとの回答が半数を超えましたが、中小企業においては加入しているケースは少ないのが現実です。

サイバー攻撃に対する危機意識が高まっているにもかかわらず、サイバー保険への加入が進まない背景には、保険の補償内容や保険料についての情報がわかりにくいことが根底にあると想定されます。

サイバー保険の主な補償内容を以下に整理しました。サイバー攻撃による被害は、情報流出による損害賠償金、調査費用、争訟費用、営業停止による利益損害、自社株価の下落等、多岐にわたり、それらの一部を補償してくれるのがサイバー保険です。

サイバーインシデントが発生して、サイバー保険に未加入の企業の場合、どうしても調査にかかるコストを意識しすぎて、スコープを小さくしようとする（場合によっては、復旧だけ実施して詳細な調査をしないといった）インセンティブが働いてしまう傾向があります。十分な調査や対策を実施することなく復旧を急いだことで、2次・3次攻撃を受けてしまった事例もあります。調査にかかるコストを意識しなくてよいのは、サイバー保険に加入するメリットの1つです。

サイバー攻撃手法の高度化により、すべての攻撃を完全に防ぐことは難しいため、万が一を想定し備えることが重要であると言えます。

損害賠償責任	被保険者が法律上負担する損害賠償金、争訟費用の補償
事故対応費用	サイバー事故に起因して発生した事故原因調査費用や、再発防止策の策定、法律相談等の各種費用の補償
利益損害・営業継続費用	IT機器等の機能停止によって生じた利益損害、営業継続費用の補償
（例外）補償対象外	ビジネスメール詐欺における口座入金、ランサムウェアの身代金

© 2025 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.

子会社管理

04

子会社ごとの取組みから
グループ全体への取組みへ 25

子会社管理の実態 26

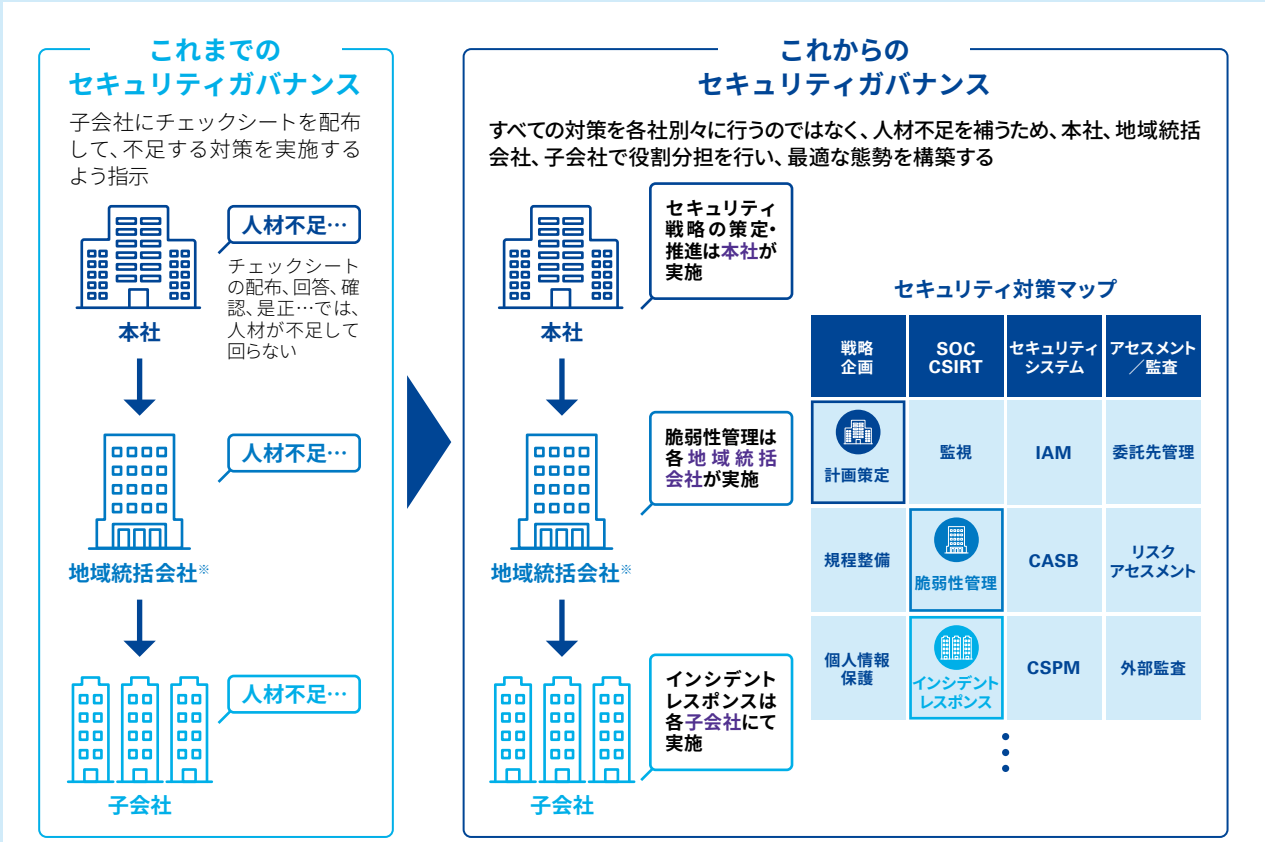
コラム｜サイバーセキュリティ業務の拡大に
伴うグローバル／グループでの取組み 27

© 2025 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.

子会社ごとの取組みからグループ全体への取組みへ

サイバーセキュリティ人材は、日本だけでなく世界的にも不足しています。

サイバー攻撃に子会社ごとに別々に立ち向かうのではなく、限られたセキュリティ人材を有効に活用できるよう、グループ企業全体で役割を分担し、グループ全体で立ち向かうサイバーセキュリティ態勢を構築する必要があります。



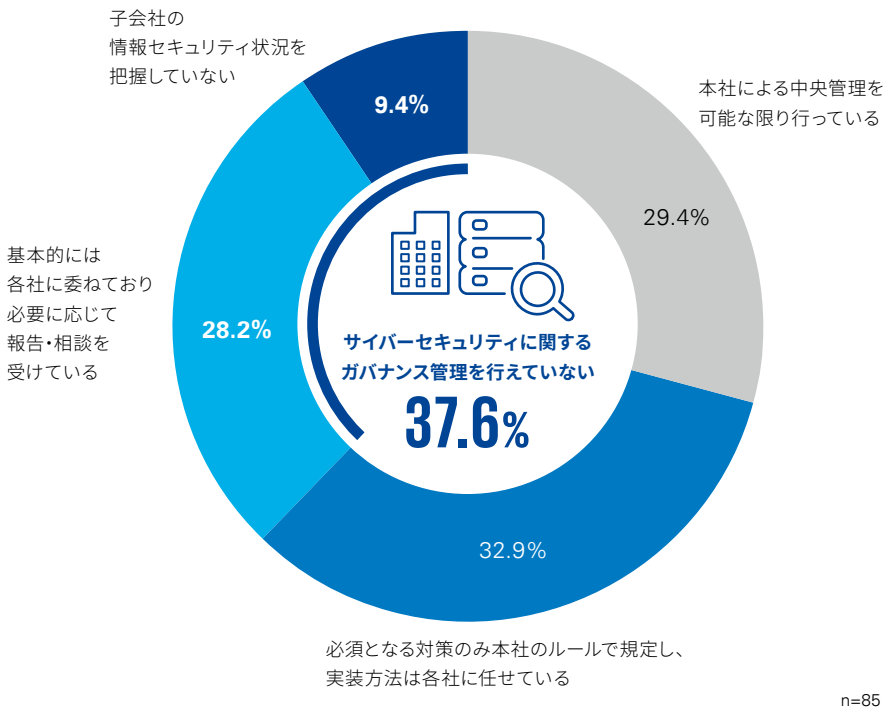
※海外子会社については、地域統括会社との役割分担を検討する。

© 2025 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.

子会社管理の実態

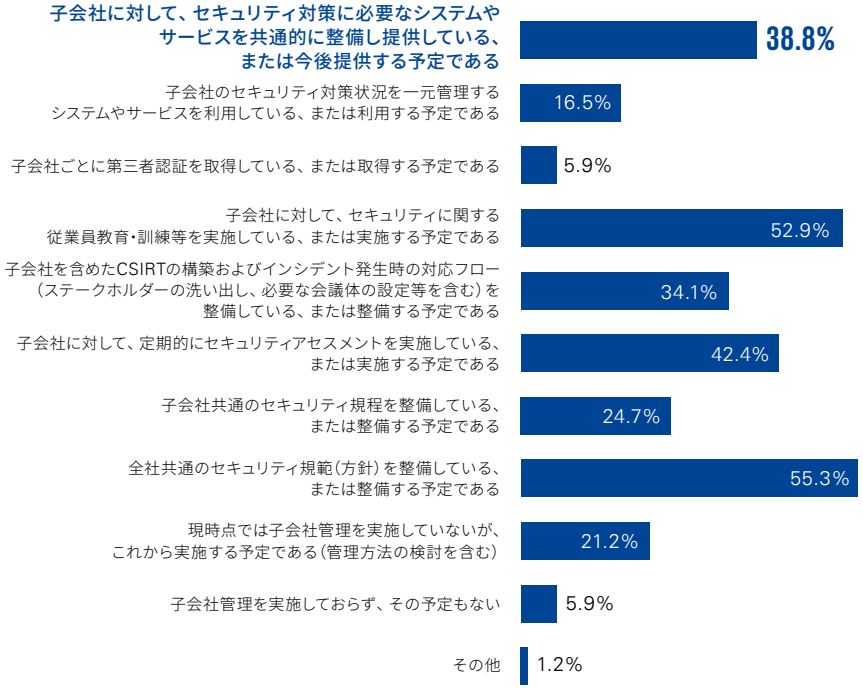
「基本的には各社に委ねており必要に応じて報告・相談を受けている」という回答が28.2%、「子会社の情報セキュリティ状況を把握していない」という回答が9.4%にのぼり、3分の1強の企業において、本社が子会社のサイバーセキュリティに関するガバナンス管理を行えていない状況がうかがえます。
一方、約40%の企業が「子会社に対して、セキュリティ対策に必要なシステムやサービスを共通的に整備し提供している、または今後提供する予定である」と回答しており、企業によって、子会社のサイバーセキュリティ対策高度化の方針がまったく異なる様子がうかがえます。

サイバーセキュリティにかかる子会社管理の状況



n=85

子会社管理で実施している対策



複数回答可／n=85

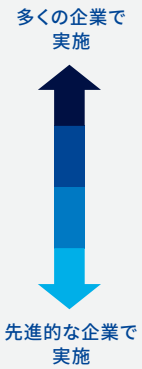
© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

コラム サイバーセキュリティ業務の拡大に伴うグローバル／グループでの取組み

サイバー攻撃の高度化に伴い、セキュリティ組織で実施すべき対策や業務が増加しています。
事業内容や事業規模、組織の成熟度合い、現在のセキュリティ人材の数やスキル等を踏まえ、グローバル／グループでのセキュリティ組織の在り方や、セキュリティ人材の育成について検討する必要があります。

セキュリティ組織で担当する役割（例）（OTセキュリティ／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	



© 2025 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.

委託先管理

05

サプライチェーンサイバーセキュリティ管理の厳格化 29

委託先管理の実態 30

コラム | 最新テクノロジーを用いた委託先管理の効率化 31

© 2025 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.

サプライチェーンサイバーセキュリティ管理の厳格化

製造業においてサプライチェーンサイバーセキュリティの重要性が増しています。他社と差別化された製品の生産にあたっては、協働するサプライヤーに知的財産や機密情報を共有する必要がありますが、サプライヤーがセキュリティ対策を行っていないと、これらの情報が悪意のある攻撃にさらされる可能性があります。またサプライチェーンが攻撃を受け、部品やコンポーネントの生産が停止すると、製品の生産も停止するリスクがあります。そのため、サプライヤーにセキュリティ対策を要求し、サプライチェーン全体でのセキュリティ管理を厳格化する動きが加速しています。

自動車、半導体、製薬などの知的財産保護が重要な業種や、医療機器、エネルギー、石油等の安全が重要視される業種において、認証取得が必要になるケースが多くみられます。サプライチェーンサイバーセキュリティに取り組むには、右記のような3段階でのアプローチが有効です。

		監査実施者	目的
第一者監査	内部監査	• 自社の内部監査員 • 自社の指定する専門家	自社のサイバーセキュリティ対策の現状を洗い出すとともに今後の対策を立てるための指針とする
第二者監査	利害関係者による外部監査	• 取引先の監査員 • 取引先が指定する専門家	取引先のサイバーセキュリティ基準を満たしていることを確認するとともに、不十分な内容がある場合は改善を促す
第三者監査	独立した組織による外部監査	• 独立した第三者機関（認証機関）の監査人	特定の基準（ISO規格等）に準拠していることを確認するとともに、規格への適合を認証する

より厳格

取引先の台帳化と重要度確認

- 取引先を台帳化するとともに、納入部品の詳細、代替品入手の可否、共有している情報の種類などを台帳化する
- 共有している情報が流出したときのリスク、生産が停止したときのリスクを基に重要度を付与し、より重要な取引先から優先的に対策を実施する

ギャップアセスメントの実施と対策

- 要求するサイバーセキュリティの基準を定義するとともに、取引先に対して自社監査を要求する
- 自社監査の結果提出を求めるとともに、重要な取引先に対しては第二者監査を実施する
- 発見されたギャップの改善計画提出を要求するとともに、改善されたことを確認する

契約への反映とモニタリング

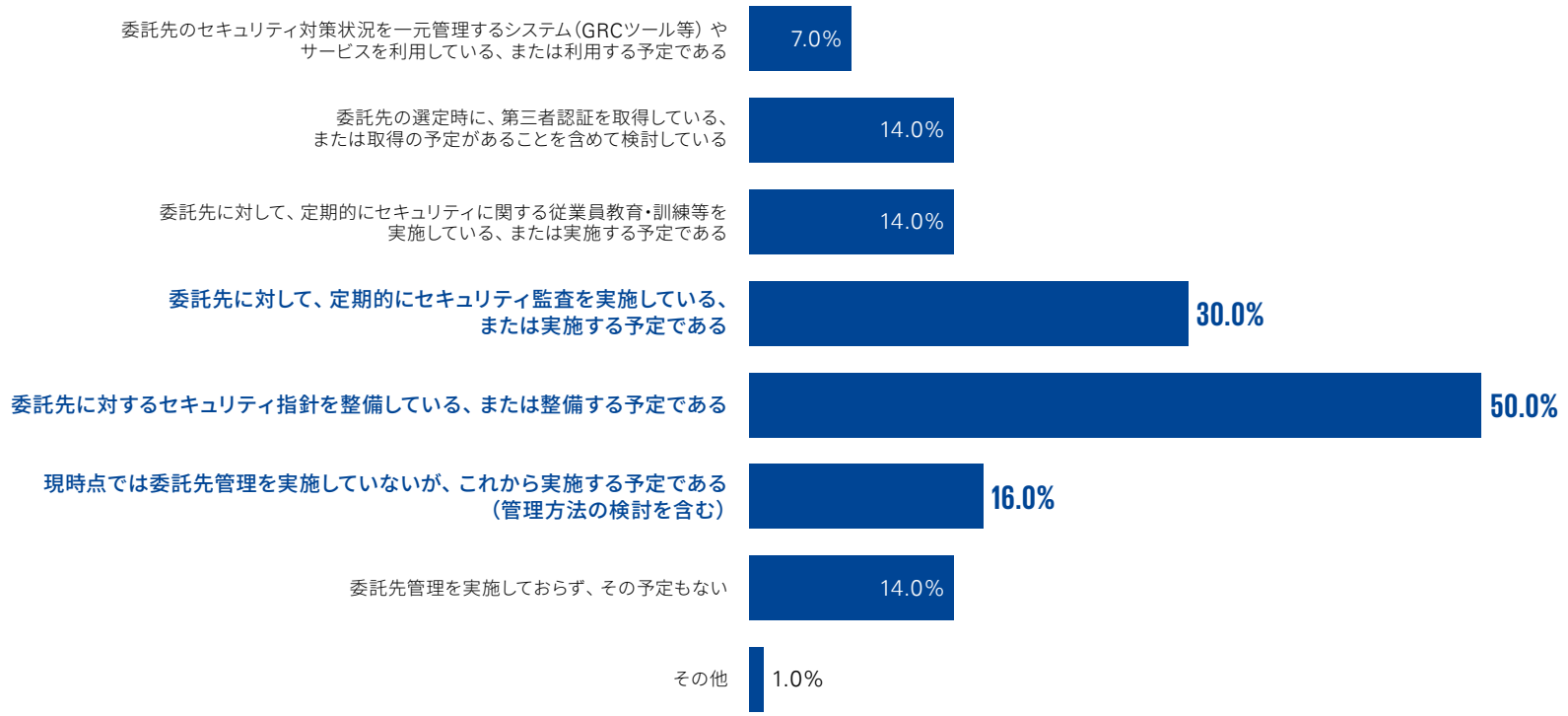
- 基本取引契約に、サイバーセキュリティ対策の履行を包含するとともに、違反時の責任について明確にする
- 取引先のセキュリティ対策が十分か、内部監査状況を定期的にモニタリングする
- 要求するセキュリティ水準が十分か定期的に検討を行い、必要に応じて要求事項を強化する

© 2025 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.

委託先管理の実態

委託先管理においては、「委託先に対するセキュリティ指針を整備している、または整備する予定である」との回答が50.0%、「委託先に対して、定期的にセキュリティ監査を実施している、または実施する予定である」という回答が30.0%、「現時点では委託先管理を実施していないが、これから実施する予定である」という回答が16.0%となっています。
外部委託先管理の不備が原因のセキュリティインシデントが後を絶たない昨今において、委託先におけるセキュリティの担保のために何らかの対策を実施する企業が増えていることがうかがえます。

委託先管理で実施している対策



複数回答可／n=100

© 2025 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.

コラム 最新テクノロジーを用いた委託先管理の効率化

サイバーセキュリティにおいて委託先管理の重要性が増すなかで、米国など海外企業の一部では、GRCプラットフォームを用いることで評価を自動化したり、AIや機械学習を活用することで単純作業を減らして効率化を図ったりしている事例があります。
一方、多くの日本企業では、表計算ソフトを用いた非効率な情報収集、改善指示結果等の手動での進捗確認など、従来型の委託先管理から進化しておらず、最新テクノロジーを用いた効率化への取組みが十分にできていません。

最新テクノロジーを用いた委託先管理の効率化コンセプト（例）

- 委託先管理のアセスメント手順を自動化し、委託先評価を効率的に実施
- 人工知能（AI）や、機械学習（ML）チャットボット等を活用し、委託先リスク管理をシステム化

1	2	3	4	5
評価の自動化（GRCプラットフォーム）	インテリジェンスモニタリング（外部視点）	共通アセスメント項目	AIフレームワーク	継続的評価＆モニタリング

© 2025 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.

OTセキュリティ

06

海外企業に遅れるOTセキュリティ 33

制御システムサイバーセキュリティの成熟度 34

制御システムサイバーセキュリティアセスメント 35

コラム｜NIS2で求められるOTセキュリティ要件 36

© 2025 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.

海外企業に遅れるOTセキュリティ

欧州を中心にグローバルではサイバーセキュリティ法規制の整備が進んでおり、OTセキュリティも例外ではありません。海外では高成熟度組織※が23.0%を占めるのに対して、日本は8.7%にとどまっています。また、成熟度がレベル1の企業は、海外では16.0%にとどまりますが、日本では36.8%と最も比率が高くなっています。

海外のサイバーセキュリティ法規制および海外の先進企業の取組みをしっかりと分析し、自社の取組みを継続的に改善していくことが望まれます。

※ 高成熟度組織：成熟度がレベル4、レベル5の組織
低成熟度組織：成熟度がレベル1、レベル2の組織

制御システムセキュリティの成熟度の海外・日本の比較

定義

★★★★★ レベル5
サイバーセキュリティプロセスは、既存のプロセスからのフィードバックにより継続的に改善され、組織のニーズにより適切に対応しています。

★★★★ レベル4
組織のサイバーセキュリティプログラムは、成果を向上させるためにデータの収集と分析を実施しています。

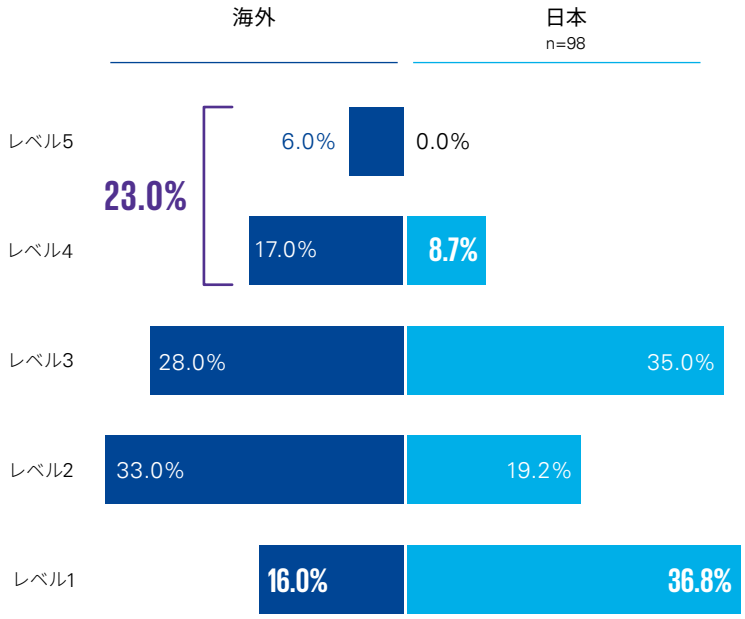
高成熟度組織

★★★ レベル3
サイバーセキュリティは、文書化されたプロセスや手順に基づき実施されています。

★★ レベル2
サイバーセキュリティの実装において、基本的なプロジェクトマネジメントが実施されています。

★ レベル1
サイバーセキュリティのプロセスは未整理で文書化されておらず、プログラムで整理されてもいません。

低成熟度組織



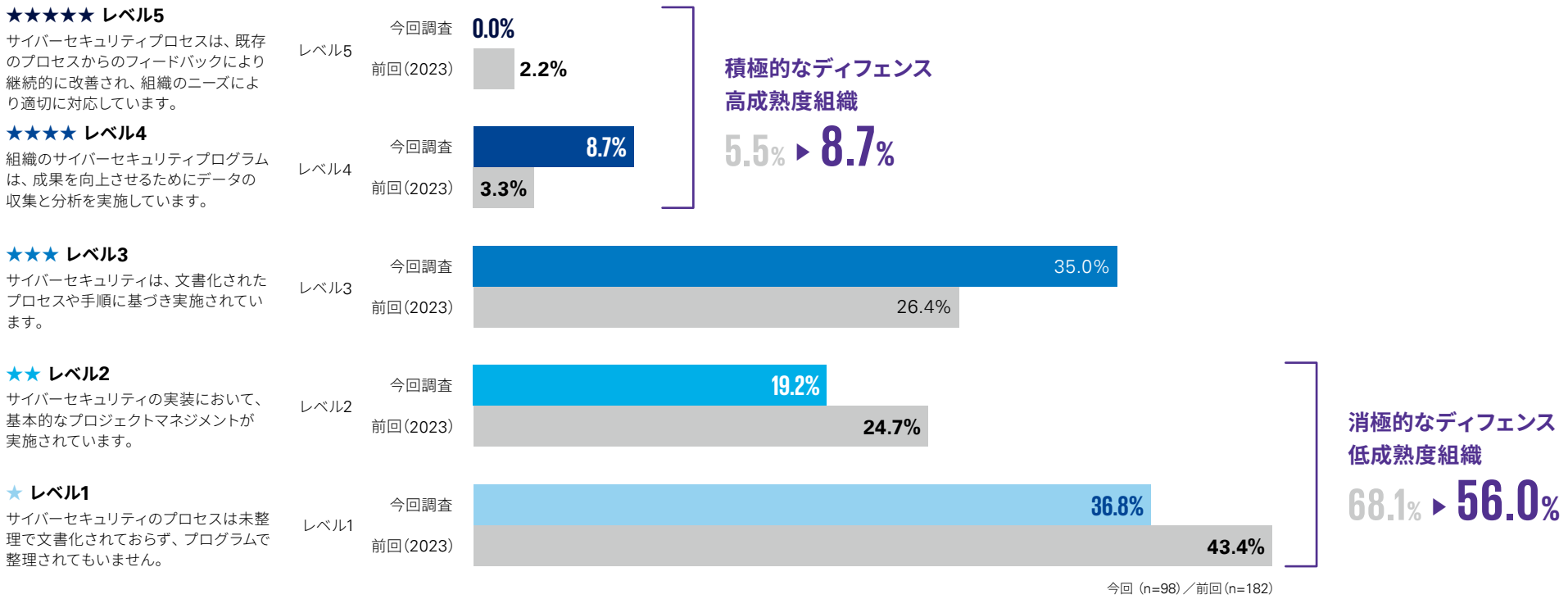
左表（海外） 出所:「(CS)2AI-KPMG制御システムサイバーセキュリティ年次報告書2024」
https://kpmg.com/jp/ja/home/insights/2024/10/cyber-controlsystem-report.html

© 2025 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.

制御システムサイバーセキュリティの成熟度

OTセキュリティの成熟度について「成熟度レベル1」という回答が最も多く、全体の36.8%にのぼることから、サイバーセキュリティのプロセスは未整備で文書化されておらず、プログラムでも整理されていないという企業が多数を占めていることがわかります。対して、高成熟度組織といわれる「成熟度レベル4」という回答は8.7%となっており、組織としてサイバーセキュリティを向上させるためにデータの収集と分析を実施している企業もあります。

制御システムセキュリティの成熟度の前回調査との比較



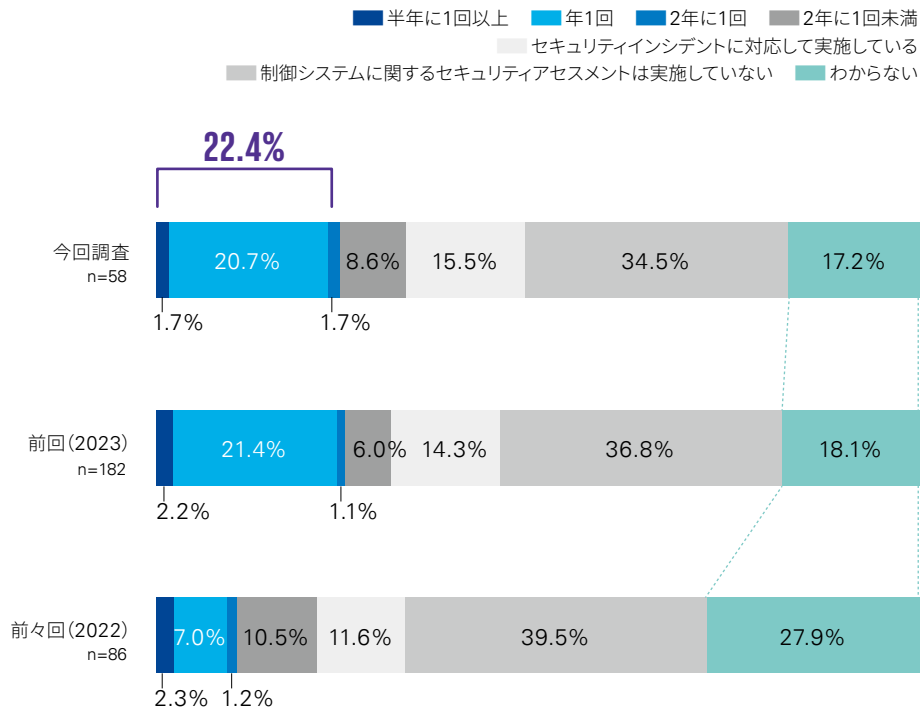
© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

制御システムサイバーセキュリティアセスメント

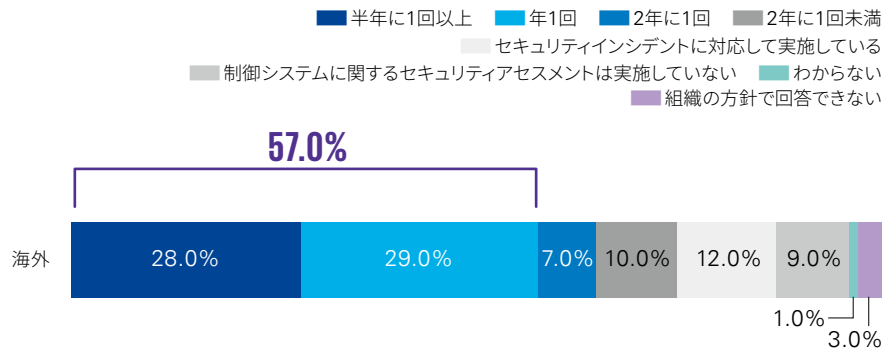
制御システムに関するセキュリティアセスメントを年に1回以上実施している日本企業は22.4%となっていますが、海外では低成熟度組織※でも57.0%の企業が年に1回以上実施しており、海外に大きく遅れを取っています。
一方で、前回調査に引き続き「わからない」という回答が減少しており、セキュリティアセスメントに対する認識が醸成されていることを示しています。

※低成熟度組織：成熟度がレベル1、レベル2の組織

制御システムに関するセキュリティアセスメントの実施頻度



海外における低成熟度組織の制御システムに関するセキュリティアセスメントの実施頻度



出所：「(CS) 2AI-KPMG制御システムサイバーセキュリティ年次報告書2024」
https://kpmg.com/jp/ja/home/insights/2024/10/cyber-controlsystem-report.html

© 2025 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.

コラム NIS2で求められるOTセキュリティ要件

NIS2指令（Network & Information Security Directive）は重要なインフラのサプライチェーンに不可欠な組織に焦点を当てています。欧州連合（EU）は、GDPR（EU一般データ保護規則：General Data Protection Regulation）と同様に、遵守できていない組織に対して罰金を科します。必要なコンプライアンス要件を備えるために、国際的に認められた枠組みを利用する必要があります。
NIS2指令では、OTシステムのセキュリティを確保することの重要性を強調しており、これを実現するためには、OT環境にかかわるIEC 62443シリーズ等の業界標準を利用すべきです。IEC 62443を採用することで、組織は従業員が安全な環境を維持するための訓練を受け、能力を養っていることを保証するだけでなく、OTシステムの脆弱性を特定して対処するなど、サイバーセキュリティ態勢を向上させることができます。

OTセキュリティ要件 NIS2・IEC 62443の比較

	NIS2	IEC 62443
ガバナンス＆プロセス	• リスク分析・情報システムセキュリティ方針 • サイバーリスク経営の有効性評価 • ビジネス継続性	• ポリシーと手順 • リスク管理 • 災害復旧とビジネス継続性 • セキュリティ要件 • 参照ネットワークアーキテクチャ
組織＆人	• 管理委員会によるサイバーリスク管理アプローチの承認・監督 • コンピュータの衛生習慣とサイバーセキュリティの訓練 • サプライチェーンのセキュリティ	• 役割と責任 • セキュリティトレーニング • サードパーティ
テクノロジー＆セキュリティケイパビリティ	• インシデント処理 • 暗号化とポリシー・手順 • 脆弱性の取扱いと開示 • 人材セキュリティ、アクセス制御ポリシー、資産管理 • 多要素認証と安全な通信システムの利用	• 棚卸資産 • ネットワークセグメンテーション • パッチおよび脆弱性の管理 • リモートアクセスセキュリティ

© 2025 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.

製品セキュリティ

07

市場から求められる
製品セキュリティ対応組織 38

製品セキュリティの成熟度 39

製品セキュリティ対策の実態 40

コラム｜CRAで求められるPSIRT/PSOC強化 41

© 2025 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.

市場から求められる製品セキュリティ対応組織

欧州委員会では、サイバー攻撃の3分の2は製品の脆弱性に起因しており、市場に出回っている製品の約60％[※1]にはサイバー攻撃に対する既知の脆弱性が含まれていると推計しています。EU（欧州）サイバーレジリエンス法（CRA）は、EU域内のデジタル製品に対するサイバーセキュリティ要件の厳格化を規定しており、同様の規制は、英国、米国でも整備が進んでいます。

規制強化による影響のためか、成熟度でみると、OTセキュリティよりも成熟度レベル5の比率が5.6%と比較的多くなっています。一方、製品セキュリティに対応する組織を設置していないと回答した企業の比率が42.6%と高く、対応が求められている組織とそうでない組織とで対応の差が生じていることが読み取れます。

グローバルでの規制が強化されていくなか、日本企業ではPSIRT/PSOC[※2]の態勢整備が進んでいません。法規制や国際標準・ガイドラインに基づいて、PSIRT/PSOCの構築・強化が求められます。

※1 出所：
引用元
Neue Verordnung über Cyberresilienz - Aktuelles von KPMG Law（https://www.kpmg-law.at/neue-verordnung-ueber-cyberresilienz/）

日本語訳
EUサイバーレジリエンス法がもたらす日本企業への影響とは - KPMGジャパン（https://kpmg.com/jp/ja/home/insights/2023/07/cyber-resilience-act.html）

※2
PSIRT：Product Security Incident Response Team
企業の製品やサービスに特化したセキュリティインシデントに対応する専門的なチーム

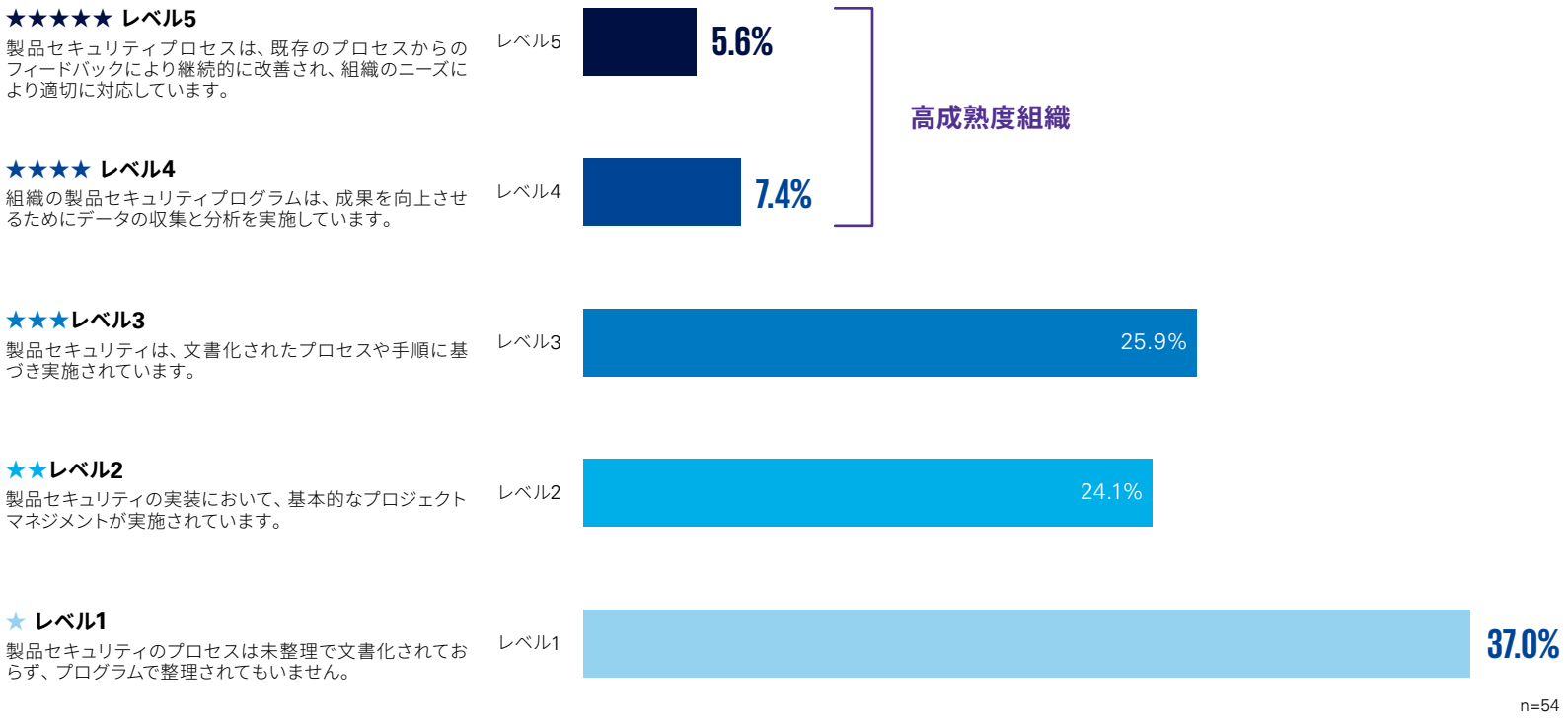
PSOC：Product Security Operation Center
企業の製品やサービスに特化したセキュリティ監視を行うチーム

© 2025 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.

製品セキュリティの成熟度

製品セキュリティの成熟度について「成熟度レベル1」という回答が最も多く、37.0%にのぼることから、製品セキュリティのプロセスは未整理で文書化されておらず、プログラムでも整理されていないという企業が多数を占めていることがわかります。対して、高成熟度組織といわれる「成熟度レベル4」という回答は7.4%、「成熟度レベル5」という回答は5.6%となっています。

製品セキュリティの成熟度

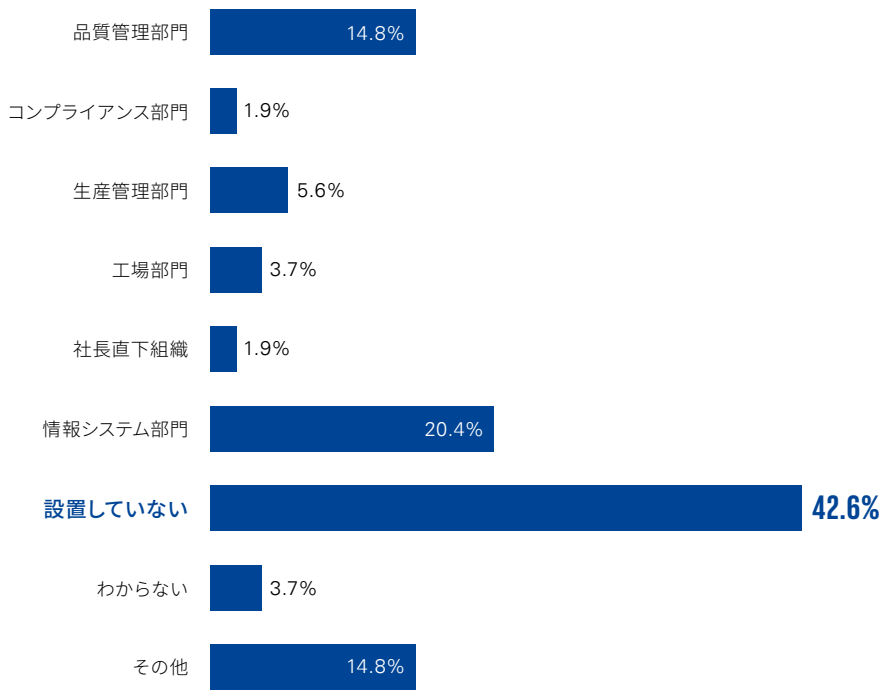


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

製品セキュリティ対策の実態

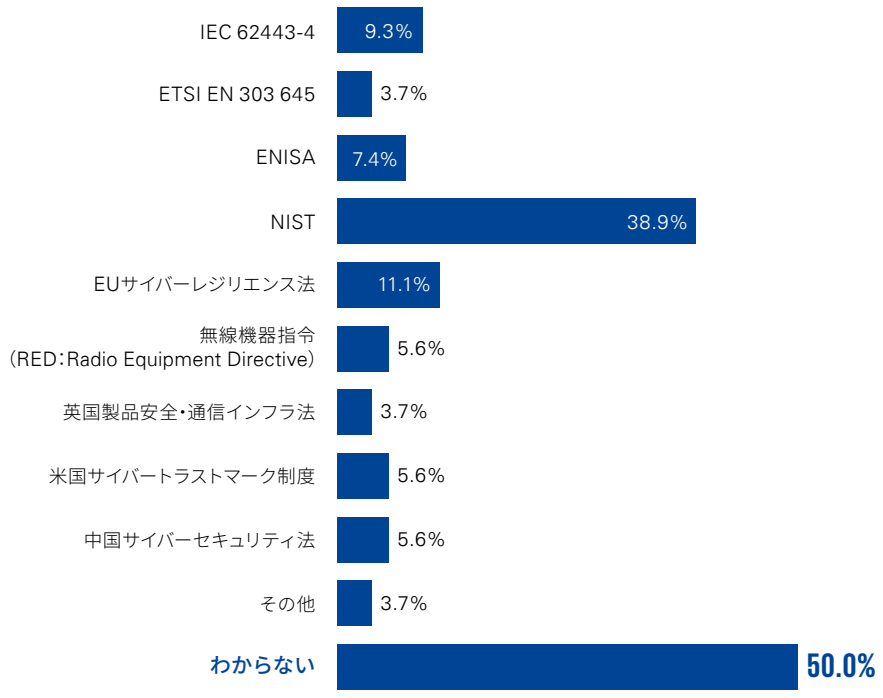
社内に製品セキュリティ組織を設置していないという回答が最も多く42.6%となりました。
また、製品セキュリティ活動で参照している法規・ガイドラインについては「わからない」という回答が50.0%と最も多く、
日本企業における製品セキュリティ対策の整備が進んでいない状況が浮き彫りになりました。

製品セキュリティ組織（PSIRT等）の設置部門



複数回答可／n=54

製品セキュリティ活動で参照している法規・ガイドライン



複数回答可／n=54

© 2025 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.

コラム CRAで求められるPSIRT/PSOC強化

EU（欧州）サイバーレジリエンス法（CRA）は、EU域内のデジタル製品に対するサイバーセキュリティ要件の厳格化を規定し、日本にもサプライチェーンのサイバーセキュリティを通じて製造業を中心に幅広い影響が見込まれており、日本企業もPSIRT/PSOCの構築・強化が求められます。
2024年11月20日付で、EU（欧州）サイバーレジリエンス法 2024/2847が欧州連合官報（OJ）に掲載され、その翌日から20日後に発効されました。
また本規則は、2027年12月11日より全面施行となりますが、Article 14（製造事業者の報告義務）については2026年9月11日より、Chapter IV（Article35～51、適合性評価機関の通知）については2026年6月11日より先行して施行されます。

1. 安全な製品と安全な使用

目的	製品のライフサイクルを通じて遵守すべき、デジタル要素を持つ製品に対する強制的なサイバーセキュリティ要件を導入すること
対象製品	デジタル要素を持つ製品（個別に市場に投入されることを意図したハードウェアまたはソフトウェア製品およびそのリモートコンピューティングソリューション）
対象者	一般的に経済事業者、すなわちデジタル要素を持つ製品の製造業者、製造業者の公認代理人、輸入業者、流通業者
目標	脆弱性の少ない安全な製品の開発と、それに伴う製品のライフサイクル全体に対する製造者の責任、消費者による製品の安全な選択と使用を確保すること

2. 製造者の義務

セキュリティ保証	製造業者は、製品を市場に出してから少なくとも5年間はセキュリティの脆弱性に責任を持ち、セキュリティアップデートを提供しなければならない
報告義務	積極的に悪用された脆弱性は、24時間以内に欧州連合サイバーセキュリティ機関（ENISA）に報告する必要がある
罰則	最高1,500万ユーロまたは全世界の年間売上高の2.5%（いずれか高い方）の制裁金を規定しており、加盟国は具体的な制裁規定を決定することが求められている
開発ライフサイクル	サイバーセキュリティは、製品のライフサイクルのすべての段階、すなわち開発段階だけでなく、計画、納品、保守の段階でも考慮されなければならない。DevOps（Development and Operations）のような概念はDev-SecOps（Development and Security Operations）に変更する必要がある
文書化	サイバーセキュリティのリスクは文書化する必要がある 脅威モデルの作成が有効となる
ユーザーマニュアル	明確で理解しやすい使用説明書がユーザーに提供されなければならない

© 2025 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.

AIセキュリティ

08

AI導入の拡大とリスク意識の高まり 43

AIの導入状況 44

AI導入のリスク 45

AIリスクを管理する組織、ルール、プロセスの整備状況 46

コラム｜AIリスクモニタリングの高度化 47

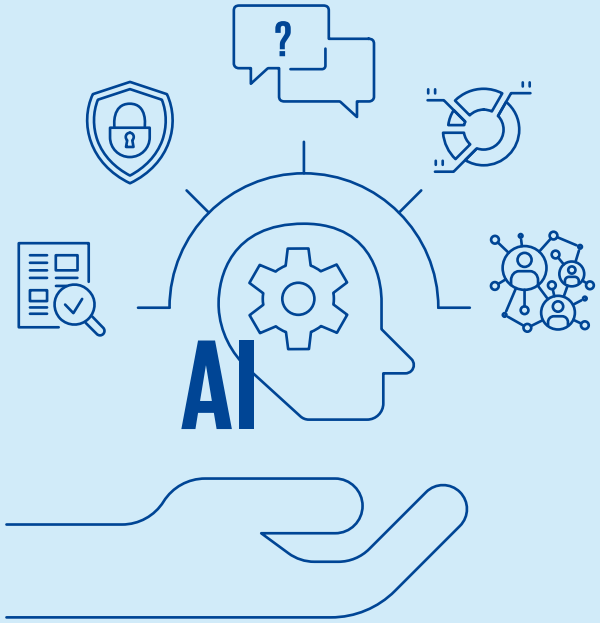
© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AI導入の拡大とリスク意識の高まり

生成AIの登場により、AIを用いた業務のさらなる効率化・高度化に大きな期待が高まっています。一方で、AIを用いることによるリスクについても着目されており、その一部は現実のものとなっています。AIを適切に活用しつつ競争力を高めるため、AIのガバナンスに注目が集まっています。

前回調査と比較し、幅広い分野でAIの導入が進んでいる様子がうかがえます。特に、「質問・問い合わせへのアシスト」については、およそ半数の企業が「導入済み」「導入予定」と回答しました。また、AIの導入が進むにつれてリスクへの認識も高まっており、前回調査と比較して、「アウトプットの正確性」や「アウトプットへの偏見」について「非常に懸念している」との回答が増加しました。このような背景から、AIリスクを管理する組織、ルール、プロセスの整備についても、「整備済みである」との回答が前回調査の4.3%から今回調査の18.4%へと大幅に増加しましたが、約80%の企業においては、整備はこれからの状況と言えます。

AIのリスクを過度におそれすぎず、しっかりとした成果へとつなげていくために、AIリスクを管理する組織、ルール、プロセスの整備を進めていく必要があります。

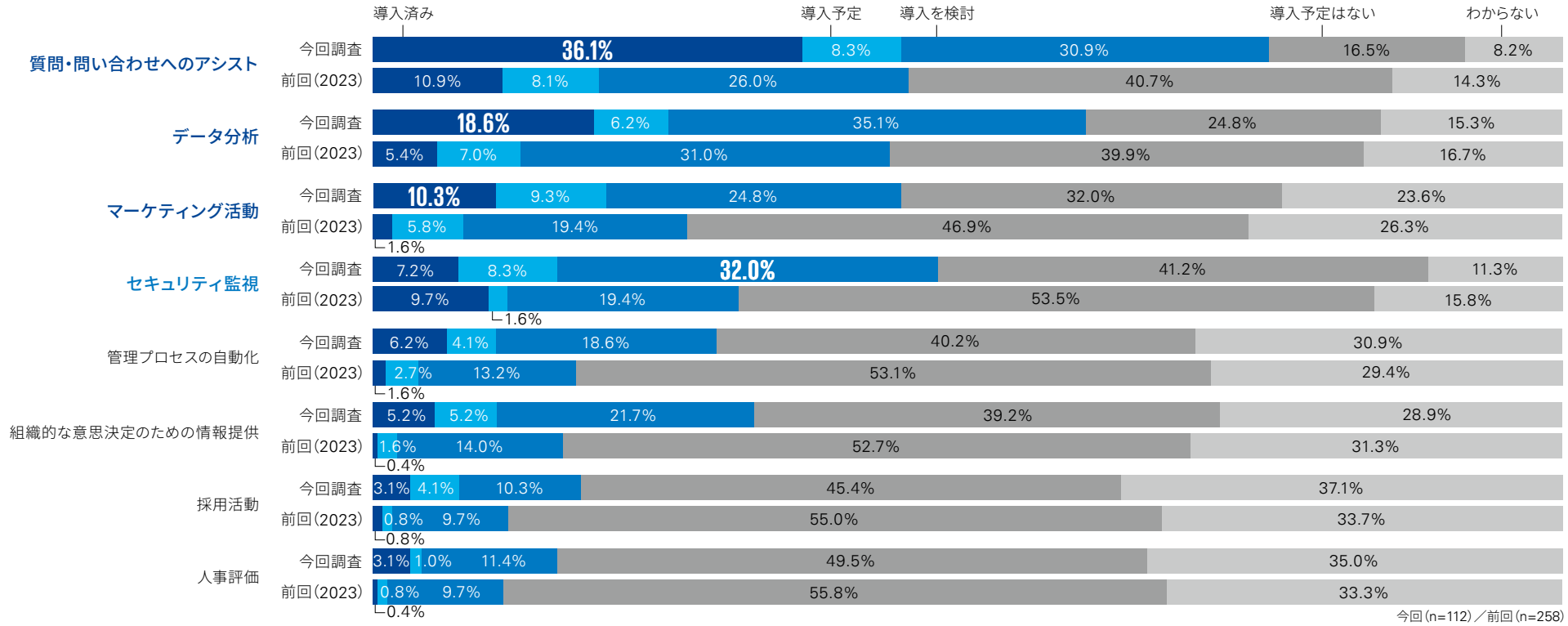


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AIの導入状況

前回調査と比較し、「質問・問い合わせへのアシスト」にAIを導入している企業が大幅に増えています。また、「データ分析」「マーケティング活動」等についても前回調査より導入済みの企業が増えています。
「セキュリティ監視」についても、導入を検討する企業が前回調査の19.4%から今回調査の32.0%と大幅に増えています。

AIの導入分野

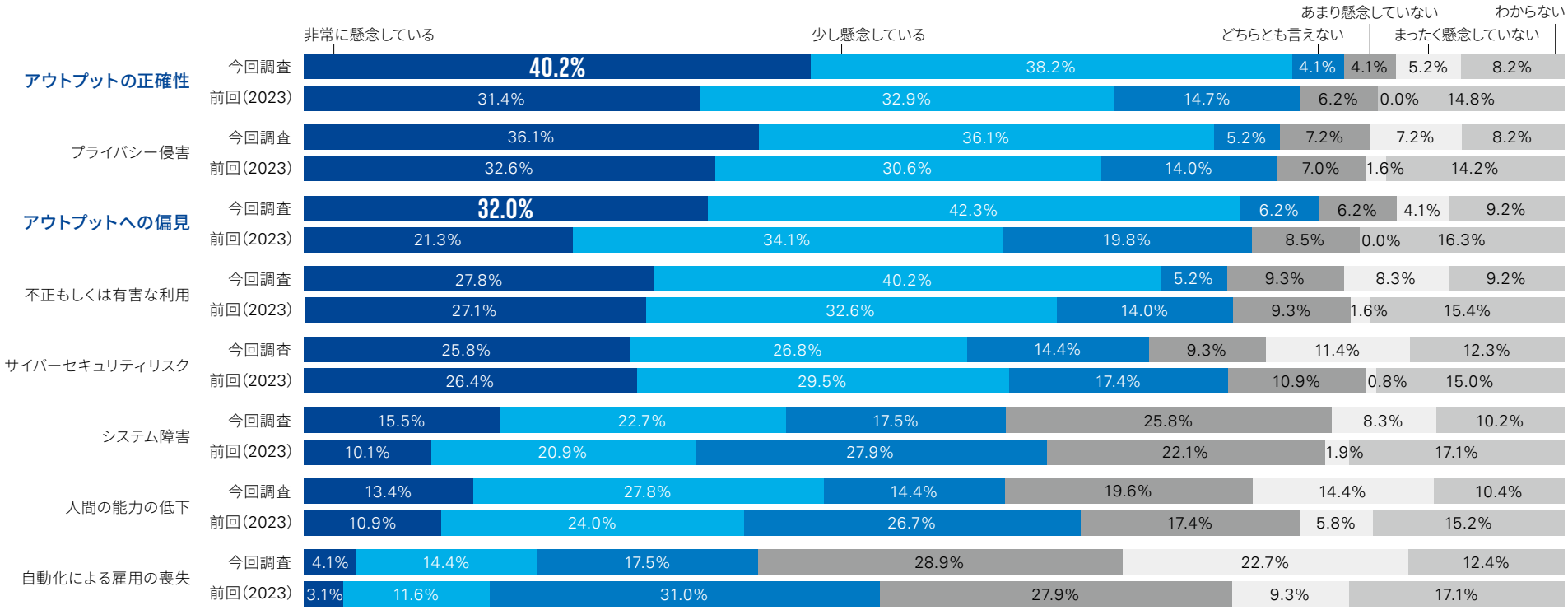


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AI導入のリスク

AIの本格利用の拡大が進むにつれて、リスクへの認識も高まっています。前回調査と比較して、「アウトプットの正確性」を「非常に懸念している」との回答は31.4%から40.2%に、「アウトプットへの偏見」を「非常に懸念している」との回答は21.3%から32.0%と大幅に増えています。これは、前回調査時点と比較してAIの導入が進み、AIへの幻想が薄れていることの表れだと考えられます。
AIを過度に信頼するのではなく、AIの得意分野・不得意分野に合わせて、業務に組み込んでいくことが求められます。

AI導入のリスク

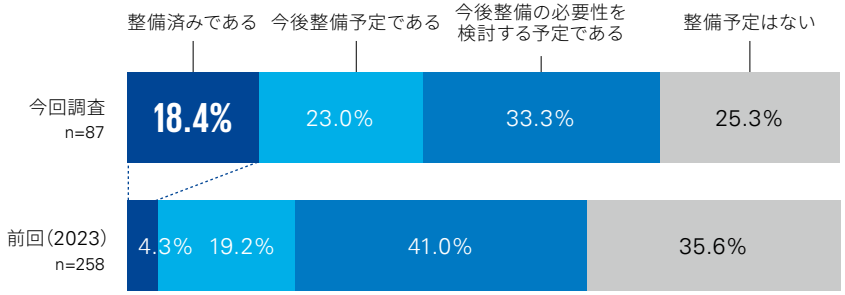


© 2025 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

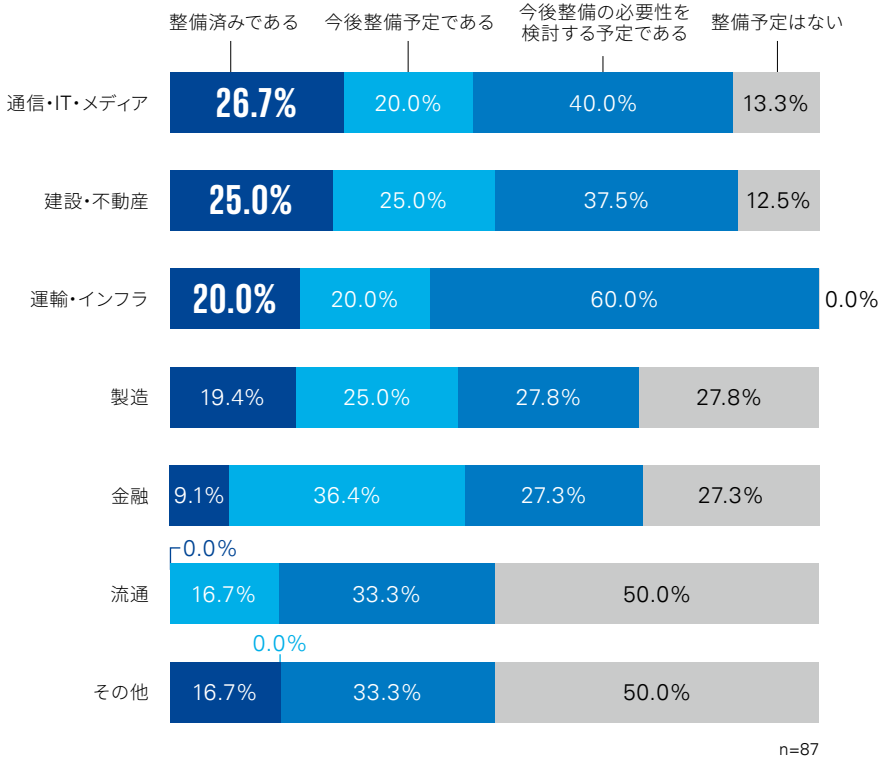
AIリスクを管理する組織、ルール、プロセスの整備状況

AIリスクに関する認識の高まりに合わせ、AIリスクを管理する組織、ルール、プロセスを整備済みの企業は、前回調査の4.3%から今回調査の18.4%と大幅に増加しました。「今後整備予定である」「今後整備の必要性を検討する予定である」との回答も多く、今後の整備が進むことが予想されます。
業種別では、「通信・IT・メディア」「建設・不動産」「運輸・インフラ」で整備済みとの回答が多くみられました。

AIリスクを管理する組織、ルール、プロセスの整備状況（全体）



AIリスクを管理する組織、ルール、プロセスの整備状況（業種別）



© 2025 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.

コラム AIリスクモニタリングの高度化

伝統的なシステムがあらかじめ定められたアルゴリズム・ロジックに従い安定的な処理を行うのに対し、現行のAIシステムは本質的にデータドリブンで、処理結果が統計的・確率的に得られるものであることを鑑みると、AIシステムの運用には、継続的なモニタリングと、適切な回答が得られることを確認する態勢の整備・維持が必要です。
AIリスクのモニタリングにあたっては、「ガバナンス＆プロセス」「組織＆人」「テクノロジー＆セキュリティケイパビリティ」の3つの軸でモニタリング指標を設定するとともに、関連部門で役割分担を行ったうえで自動モニタリングツール等の利用も検討することが重要と考えられます。

AIリスクモニタリングの整備ポイント

	モニタリングのための整備事項	整備上のポイント
ガバナンス＆プロセス	• モニタリング対象AIシステムの識別・洗い出し • ユースケースの固有リスクや規制要件に基づく重要リスク指標／重要業績評価指標（KPI）の設定 • リスク管理方針・手順書の策定	• 国内外の規制やガイドラインを参考に検討 ・AI事業者ガイドライン ・EU AI規制 ・NIST AI Risk Management Framework ・ISO/IEC 42001
組織＆人	• AIシステム所管部門、リスク管理部門、システム部門、内部監査部門等で職務分掌と相互牽制 • 人材教育と訓練 • 社内外のレポーティングラインの整備	• AIシステム導入段階はAIシステム所管部門が主となりリスク管理を実施 • 中長期的な本番運用を行うにあたり、十分な知見を有する複数の部門が関与した相互牽制の仕組みを整備
テクノロジー＆セキュリティケイパビリティ	• AIシステムの運用に合わせた継続的な重要リスク指標／重要業績評価指標（KPI）の測定 • AIモデルの変更やインフラ基盤の変更に合わせた指標の見直し	• 自動モニタリングツールの採用検討 • モニタリング結果をダッシュボード化し関連部門に適時連携

© 2025 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.

付録1:

調査概要

付録2：

KPMGジャパンの
サイバーセキュリティサービス

Appendix

© 2025 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.

調査概要

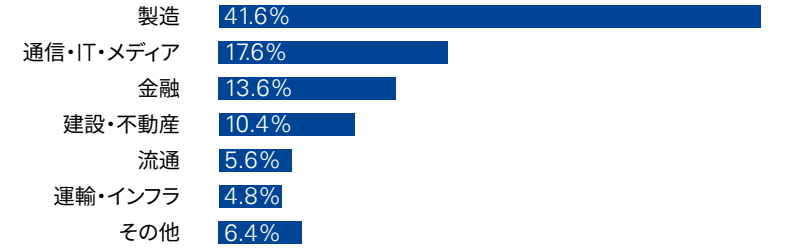
サーベイの概要

名称	サイバーセキュリティサーベイ2025
対象	国内上場企業、および売上高400億円以上の 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	2024年8月9日～10月25日
調査方法	メールによるアンケートの送付、 ウェブによるアンケートの回収
発送数	3,791社
有効回答数	125社（回収率3.3%）

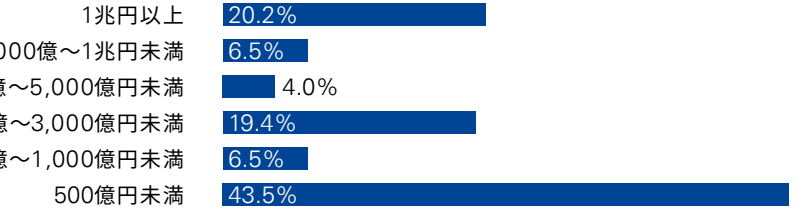
回答企業の属性

従業員数（連結）

業種



売上高（2023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。

© 2025 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.

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。

© 2025 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.

お問合せ先

KPMGジャパン

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するよう努めておりますが、情報を受け取られた時点及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。

© 2025 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. C25-1005

© 2025 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.

© 2025 KPMG FAS 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.