KPMG

Cyber Newsletter

April 2024

KPMG Japan、「サイバーセキュリティサーベイ2023」を発表

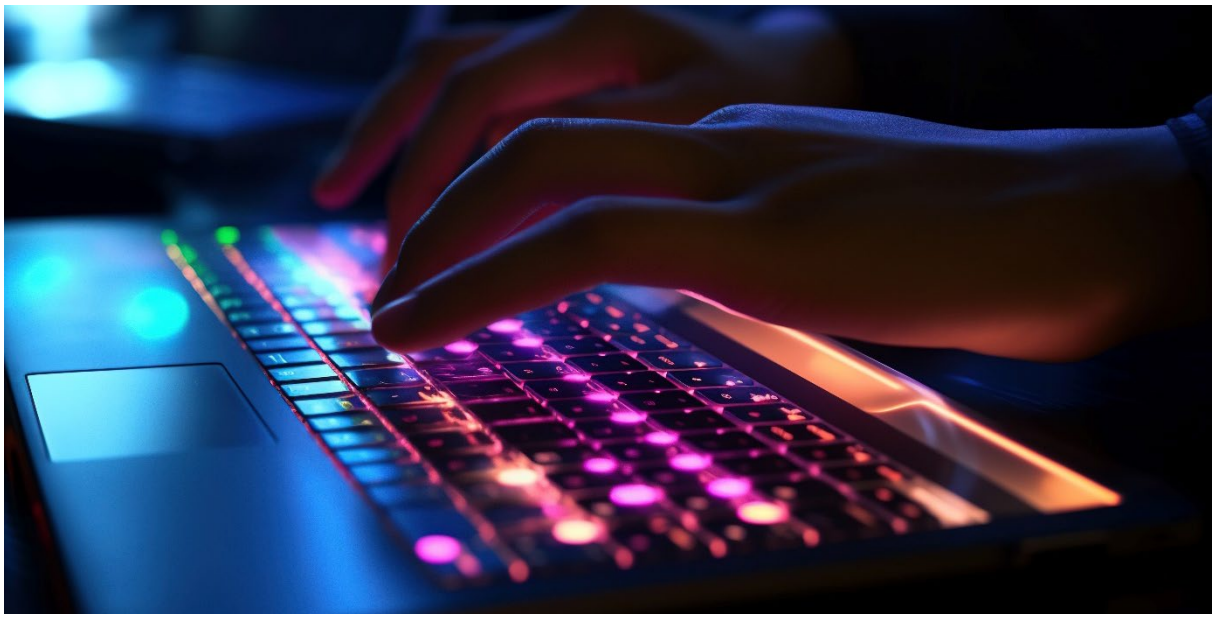
KPMGコンサルティング株式会社（本社：東京都千代田区、代表取締役社長 兼 CEO：宮原 正弘、以下、KPMGコンサルティング）は、国内の上場企業および売上高400億円以上の未上場企業を対象に実施した、企業のサイバーセキュリティに関する実態調査の結果をまとめたレポート「サイバーセキュリティサーベイ2023」を２月末に発表しました。

コロナ禍を経て社会のデジタル化が一段と進んだ結果、サイバー攻撃もより高度に、かつ巧妙になっています。最近では、脆弱性への対策が不十分な企業や組織への攻撃が増加傾向にあり、データの暗号化や機密データの窃取、さらに、重要データの暗号化に加え、持ち出した機密データで脅迫する二重脅迫型ランサムウェアなどにより、サイバーインシデントによる被害が深刻化しています。

6回目となる今回の調査では、回答企業の10社に1社が過去1年間にサイバー攻撃による被害を受けたと回答しています。このような状況において、サイバーセキュリティに関するリスクについて理解を深めるとともに、適時適切に対策を講じるために自社の現状を把握し、どこにリスクが潜んでいるかを理解することが企業を「守る」うえで重要となります。

調査結果まとめ

本レポートは、さまざまな業種や規模の企業から得られた回答をもとに、「サイバー攻撃の実態」「セキュリティ管理態勢と対策」「海外子会社管理」「制御システムセキュリティ」「AI導入およびAI導入に係るリスク管理」の5つのテーマごとにまとめています。



テーマ	サマリー
【テーマ01】 サイバー攻撃の実態	• 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は前回（2022年）の調査よりも高額化の傾向にある。 • 子会社や委託先を経由したサイバー攻撃が直接的な攻撃の2倍となっており、サプライチェーンでのセキュリティ強化に目を向ける必要がある。
【テーマ02】 セキュリティ管理 態勢と対策	• サイバーセキュリティ予算は68.2%の企業で、サイバーセキュリティ人材は88.8%の企業で不足している。 • リモートワークが浸透するなか、UEBAやSOARなど新しい領域の対策は進んでいない。
【テーマ03】 海外子会社管理	• 39.1%の企業において、海外子会社のセキュリティ対策状況を確認していない。 • 45.4%の企業において、発生したサイバーインシデントの再発防止策が国内外の子会社に展開されていない。
【テーマ04】 制御システム セキュリティ	• 「成熟度レベル1：プロセスが未整理で文書化されておらず、活動も整理されていない」にとどまる企業が43.4%を占めており、グローバルの16.0%と比較して日本企業の対応が大幅に遅れている。 • 制御システムセキュリティ対策が進んでいない課題として、約半数の企業が「知見のある実務担当が足りていない」「人的リソースが不足している」と回答している。
【テーマ05】 AI導入および AI導入に係る リスク管理	• AIの導入は71.4%の企業が計画しているが、AIリスク管理について整備済みの企業は4.3%にとどまり、AIリスク管理の整備が遅れている状況がうかがえる。 • 「採用活動」や「人事評価」といったプライバシーデータを扱う業務へのAI導入は消極的な傾向がみられる。

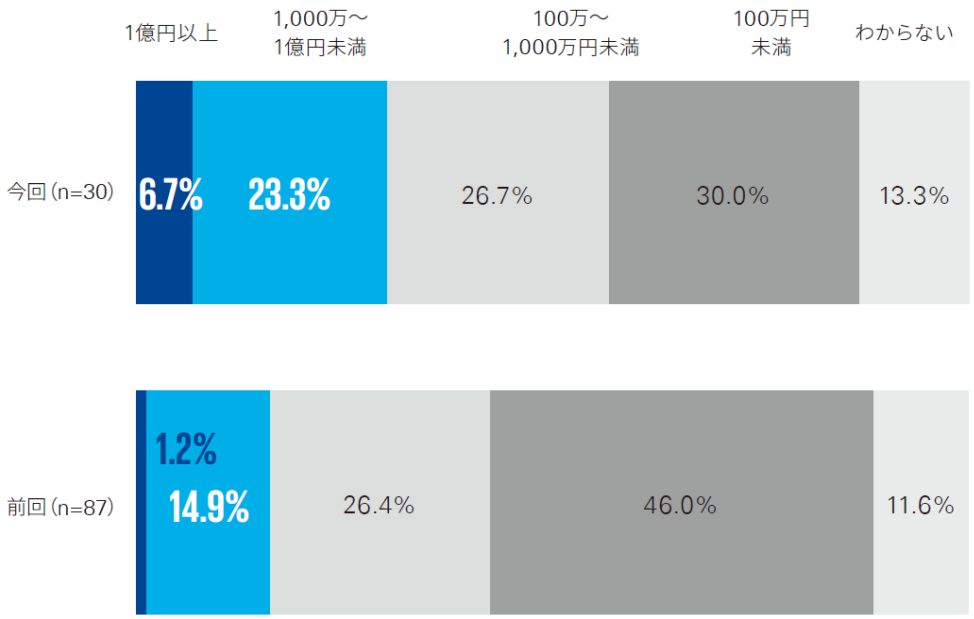
インドネシア拠点において特に注目すべきポイント

今回のNewsletterでは、インドネシア拠点において特に関連のある「テーマ01：サイバー攻撃の実態」、「テーマ02：セキュリティ管理態勢と対策」、「テーマ03：海外子会社管理」に関する調査結果をいくつか取り上げます。

テーマ01：サイバー攻撃の実態

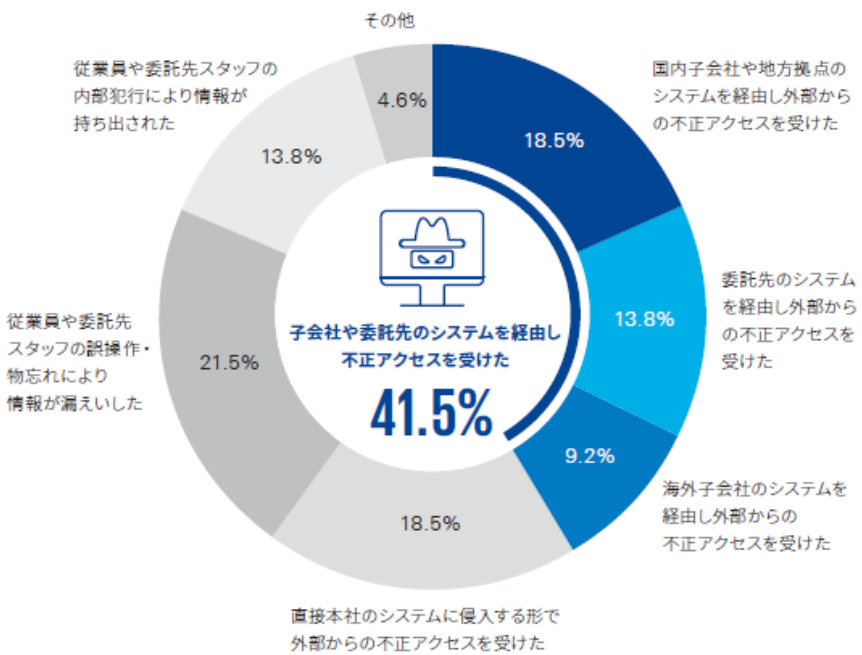
本調査では、回答企業の11.6%が、「過去1年間にサイバー攻撃で何らかの業務上の被害があった」と回答しています。また、サイバーインシデントによる被害額が「1億円以上」と回答した企業が、2022年に行った前回の調査の1.2%から6.7%に増加し、「1,000万円～1億円未満」でも14.9%から23.3%に大幅に増加しており、被害額が高額化の傾向にあることがうかがえます。攻撃手法としては「ランサムウェア」が最も多く、今後も継続して攻撃に備えておく必要があります。

【図1】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攻撃の侵入経路については、子会社や委託先のシステムを経由した攻撃が41.5%を占め、本社のシステムへの直接的な攻撃の約2倍となっており、サプライチェーン全体でのセキュリティの強化が不可欠であることが明らかになりました。

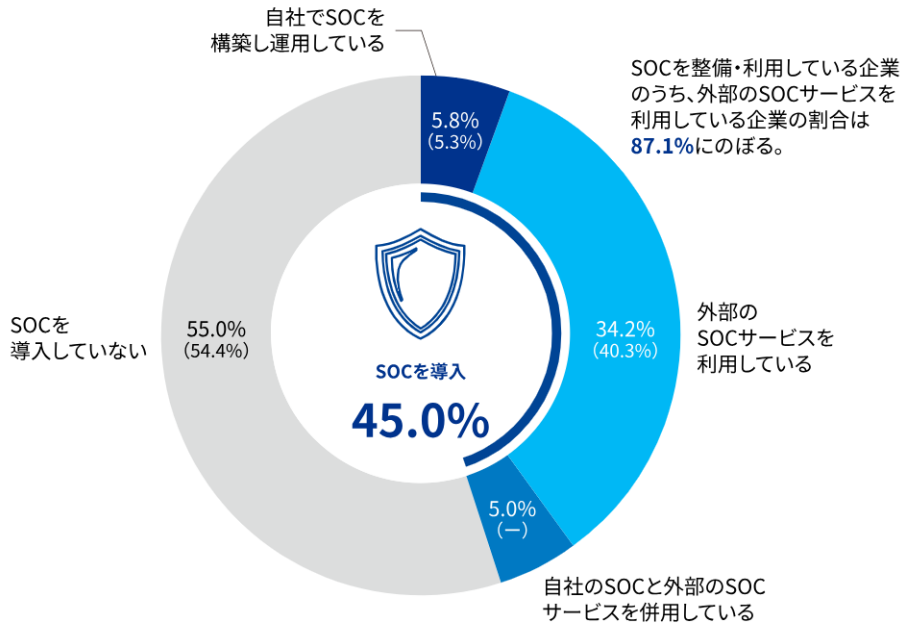
【図2】過去1年間に発生したサイバー攻撃の侵入経路



テーマ02：セキュリティ管理態勢と対策

今回の調査では、最高情報セキュリティ責任者（CISO）やサイバーセキュリティ責任者を設置していると回答した企業は60.9%にとどまりました。また、セキュリティオペレーションセンター（SOC）を導入していない企業は回答企業の半数以上の55.0%にのぼり、CSIRT（Computer Security Incident Response Team：セキュリティ事故対応チーム）を設置していない企業は72.7%にのぼるなど、セキュリティインシデントの発生に備えた体制の整備については改善の余地が残っていることがうかがえます。

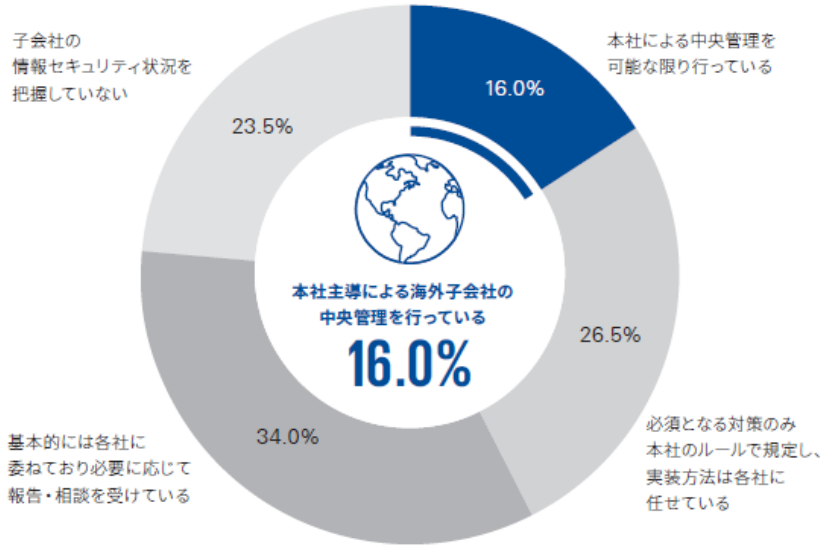
【図3】SOCの整備状況



テーマ03：海外子会社管理

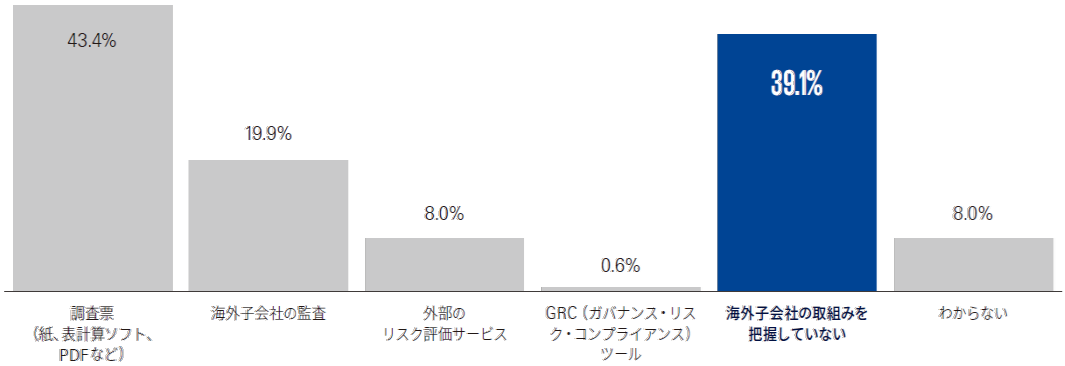
海外子会社のセキュリティ対策については、「基本的には各社に委ねており必要に応じて報告・相談を受けている」という回答が34.0%、「子会社の情報セキュリティ状況を把握していない」という回答が23.5%にのぼります。しかし、海外子会社がそれぞれ場当たり的に対策を講じるのではなく、本社主導で海外子会社（拠点）のセキュリティリスクを正確に把握し、グループ全体で整合性の取れたセキュリティ施策を計画し、導入することが望まれます。

【図4】海外子会社における情報セキュリティレベルの管理状況



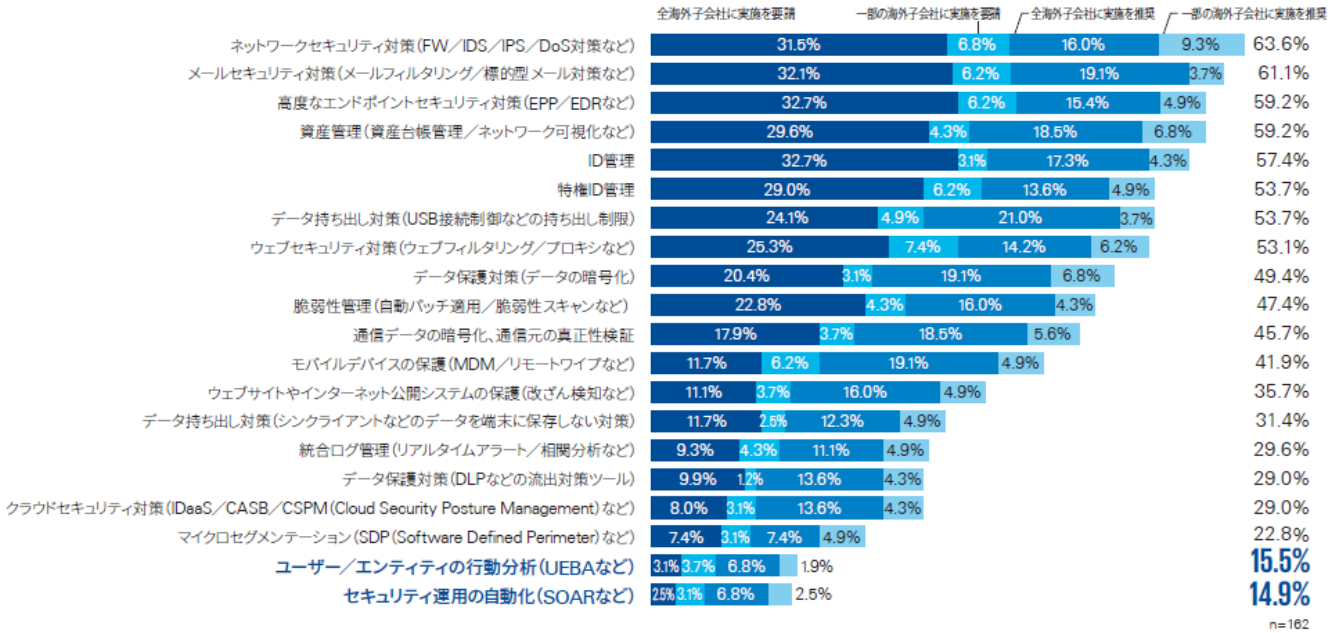
近年、海外を含めた子会社を経由したサイバー攻撃が増えるなか、今回の調査では、39.1%の企業が「海外子会社のセキュリティ対策の取組みを把握していない」と回答しており、子会社における取組みの実態の把握が求められます。また、海外子会社のセキュリティ対策状況の把握方法については、43.4%が「調査票」と回答し、「監査」と「外部のリスク評価サービス」は19.9%と8.0%にとどまり、今後外部サービスの活用やGRC（ガバナンス・リスク・コンプライアンス）ツールの活用が望まれます。

【図4】サイバーセキュリティ対策状況の把握方法



海外子会社へのサイバーセキュリティ対策の要請状況は、国内におけるサイバーセキュリティ対策実施状況と同様の傾向にあります。しかし、ネットワークセキュリティ、メールセキュリティ、エンドポイントセキュリティなどの従来からある対策に比べて、「ユーザー/エンティティの行動分析」、「セキュリティ運用の自動化」などの新しい領域の対策を要請・推奨する企業は15%にとどまります。高度化・巧妙化するサイバー攻撃へ対応するため、UEBAやSOARの導入によるセキュリティ監視・運用OODA（Observe・Orient・Decide・Act）ループを実現し、運用負荷の軽減や品質向上などを図ることが求められています。

【図5】海外子会社に要請・推奨しているセキュリティ対策



「サイバーセキュリティサーベイ2023」調査概要
名称：企業のサイバーセキュリティに関する調査
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
調査期間：2023年6月9日～7月3日
調査方法：郵送によるアンケート票の送付・回収、ウェブによるアンケートの回収
有効回答数：258社
本レポートの全文はこちらからダウンロードできます：「サイバーセキュリティサーベイ2023」

KPMGコメント

- 近年、サイバー攻撃は高度化・巧妙化しています。身代金を要求するランサムウェア攻撃が依然として猛威を振るっており、情報漏洩や操業停止などの経済的な実被害が発生しています。またセキュリティ対策が十分でない海外子会社や委託先を足がかりとした不正Z侵入が増加しており、特に東南アジアでは、各社の規模、法規制、リソース等の問題で海外グループ会社のセキュリティレベルが本社を下回っているケースが多く見られます。
- 海外グループ会社のセキュリティレベルを向上するには、本社と海外子会社それぞれの課題、役割を整理した上で、本社から海外グループ会社を管理するプロセスを明確にし、各子会社の状況を把握できるような仕組みを構築することが大切です。
- 海外子会社においては、サイバーセキュリティ監査や脆弱性診断、ペネトレーションテスト等を実施し、現在のセキュリティレベルを認識した上で、目指すべきセキュリティ体制・プロセス・対策を明確にすることが重要です。また、実際のサイバーインシデントに備えた対応手順の整備、定期的な見直しを実施する必要があります。

Contact us

KPMG SiddhartaAdvisory
21st Floor, Menara Astra
5-6, Jl. Jend. Sudirman
Jakarta 10220,
Indonesia
T: +62 21 8060 2828
F: +62 21 8060 2830

Irwan Djaja
Head of Advisory
Irwan.Djaja@kpmg.co.id

藤山 俊宏
Advisory Japan Desk Leader
Toshihiro.Fujiyama@kpmg.co.id

須藤 菊花
Advisory Japan Desk
Kikka.Sudo@kpmg.co.id

kpmg.com/id