KPMG

KPMG Newsletter

KPMG Insight

Vol.
54
May
2022

Topic ②

サイバーセキュリティ最新動向 2022
～ サーベイ結果を読み解く～

サイバーセキュリティ最新動向2022
～サーベイ結果を読み解く～

KPMGコンサルティング
テクノロジーリスクサービス
薩摩 貴人／パートナー

薩摩 貴人
Takato Satsuma

5回目を迎える「サイバーセキュリティサーベイ2022」では、KPMGコンサルティングとKPMG FASが共同で、国内の上場企業および売上高400億円以上の未上場企業のセキュリティ責任者を対象に調査を実施しました。2020年に新型コロナウイルス感染症（以下、「COVID-19」という）のパンデミックが起きたことにより、我々の働き方は一変しました。リモートワークやコミュニケーションツールの利用が浸透するなか、サイバー攻撃は新たな局面を迎えており、二重脅迫型ランサムウェアなどによる被害がさらなる拡がりを見せています。働き方の変化がサイバー攻撃をより複雑化させ、新たなリスクが生み出されている。それが現在のサイバーセキュリティの現状です。この状況が企業や組織の施策・計画に対してどのように影響したのかを知るために、本調査では「サイバーセキュリティ」「リモートワークセキュリティ」「制御システムセキュリティ」をテーマに調査を実施しました。
本稿では、サーベイ結果からうかがえる国内企業のサイバーセキュリティ動向とそこから読み取れるメッセージについて解説します。
なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りいたします。

POINT 1
セキュリティ被害の実態として回答企業の30.5%が不正侵入の痕跡を発見しており、前回（2019年）調査に比べて10ポイント近く上昇。その一方で、予算不足（65.6%）や情報セキュリティ人材不足（79.0%）により高度化・複雑化し続けるサイバー攻撃への対応に苦慮している様子がうかがえる。

POINT 2
COVID-19によるリモートワークを中心とした働き方の変化によって、回答企業の75.1%が在宅勤務を導入しているなか、回答企業の50.5%が従業員による内部不正を懸念と感じており、在宅勤務率が高いほど内部不正を懸念する企業が多い傾向が見られる。

POINT 3
わが国の屋台骨を支える製造業が抱える制御システムセキュリティの課題は根深く、対策の導入は海外に比べて大きく遅れている。

Ⅰ サイバーセキュリティの実態

1. 凶悪化するサイバー攻撃と被害の実態

近年、「二重脅迫型ランサムウェア」と呼ばれるサイバー攻撃の被害が後を絶ちません。従前のランサムウェアは暗号化したデータを元に戻すことを条件に金銭を要求してきましたが、二重脅迫型ランサムウェアはこれに加えて、窃取したデータを公開すると恐喝して身代金を要求するという合わせ技によって、より高額な金銭を要求してきます。

また、コロナ禍によるリモートワークの普及により、VPNと呼ばれる仮想ネットワークの利用が急増しましたが、自宅と会社をつなぐ接点となるVPNゲートウェイと呼ばれる装置の脆弱性を突いた不正アクセスが相次いで発生し、国内の企業や組織に大きな被害をもたらしています。さらに、ウクライナ情勢の悪化に伴い、サイバー攻撃件数が激増していることも報告されています。このように、サイバー攻撃は組織における脅威として無視できないものとなっています。

我々がセキュリティ被害の実態を調査したところ、サーベイ回答企業の30.5%が、過去1年以内に不正侵入の痕跡を発見したと回答しています。前回（2019年）調査に比べて10ポイント近く上昇していることからも、サイバー攻撃の対象が拡大していることは間違いありません。

サイバー攻撃による被害としては、「自社に経済的な損失が発生した」（28.7%）、「自社の業務やシステムが著しく遅延・中断した」（28.7%）という回答が多く、企業のビジネスに実害を及ぼしている様子がうかがえます。また、経済的な損失が発生した企業における損失合計額は「100万～1,000万円未満」（26.4%）が最も多いものの、1億円以上の損失も発生しています（図表1参照）。

2. リソース不足にあえぐ国内企業の姿

このような状況において、国内企業のセキュリティ対策は投資金額も人材も不足していることがサーベイの結果から明らかになりました。

セキュリティ投資額は全体として増加傾向にあるものの、高度化するサイバー攻撃への対策やコロナ禍によるリモートワーク化のための設備投資などが重なったことが影響したのか、65.6%の回答企業が「不足」と回答しています。一方、セキュリティ人材のほうも、79.0%の回答企業が「不足」と回答しています。前回（2019年）調査と比較して6.6%の改善が見られるものの、依然として深刻な情報セキュリティ人材不足の状況が続いています（図表2参照）。

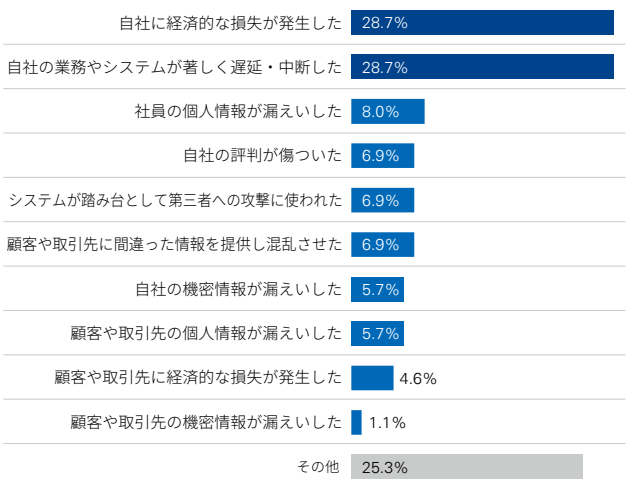
3. サプライチェーンを守れ

国内の製造業をはじめとした多くの企業がサプライチェーンを構成しており、サプライヤーの供給断による事業停止は大きな問題となっています。これは、サプライヤーが安定的に稼働し続けるための要点としてセキュリティが無視できなくなっているということです。また、近年ではサプライヤーから供給される物品やデータにマルウェアが混入し、感染被害を受け

図表1　サイバーインシデントの被害状況

サイバーインシデントの被害状況

約3割で経済的な損失やシステム遅延・中断が発生している

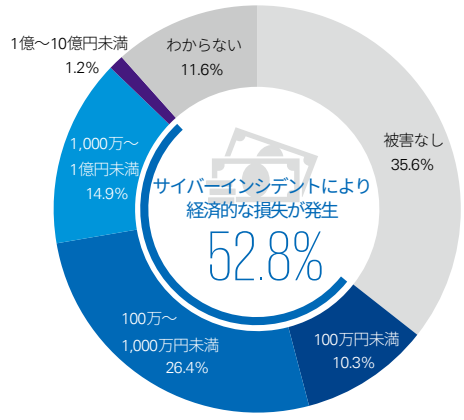


出典：KPMG作成

（複数選択可／n=87）

合計損失額

サイバーインシデントにより経済的な損失が発生している



（n=87）

るケースも珍しくなく、サプライチェーンリスクとして認識されるようになってきました。

このような状況下において、52.7%（未把握の7.8%を含む）の企業が業務委託先に対してセキュリティ対策を要請できていないという結果が明らかとなりました（図表3参照）。この結果からは、自社の事業を継続させるためにサプライチェーンを堅牢にする対応が不十分であることがわかります。なお、対策が不十分な理由には、先に述べたリソース不足も関連していると思われます。

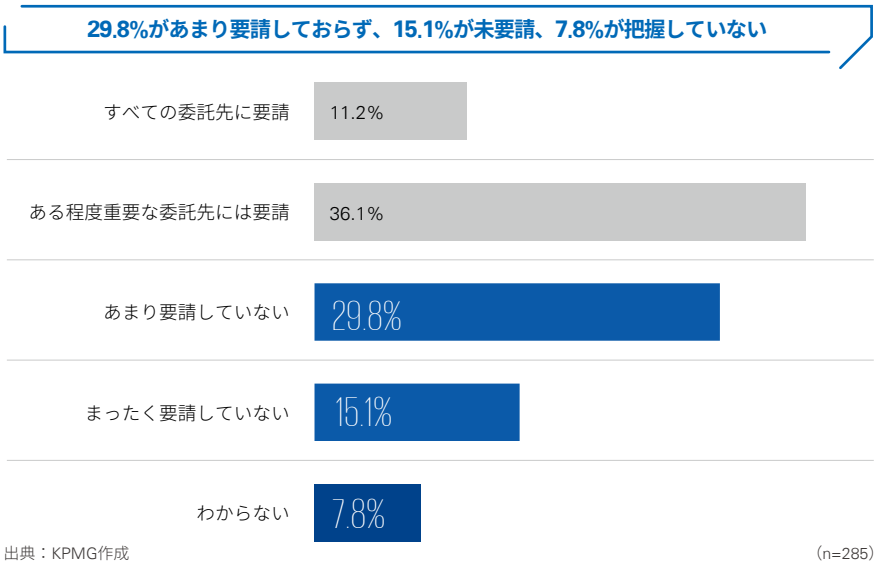
4. 事故前提でのインシデント対応能力を強化

リソース不足により十分な対策を講じることが困難な状況下においては、サイバー攻撃に遭うことを前提とし、いかに被害を最小限に食い止めるかということが、選択肢の1つになりえます。

それを裏付けるように、前回（2019年）調査よりも9.2%多い34.4%の回答企業がCSIRT（サイバー攻撃による情報漏えいや障害などに対処するための組織やチーム）を設置しています。また、回答企業の47.4%が初動対応手順を、42.5%が復旧手順を準備しているほか、32.6%がメディアへの連絡や広報の手順を準備しています。復旧対応については、51.7%が約1週間程度で対応完了するなど、インシデント対応能力の強化も目立ちます。

ただ依然として、SOARなどのインシデント対応をはじめとするセキュリティ運用

図表3　業務委託先に対するセキュリティ対策の取組みの要請状況

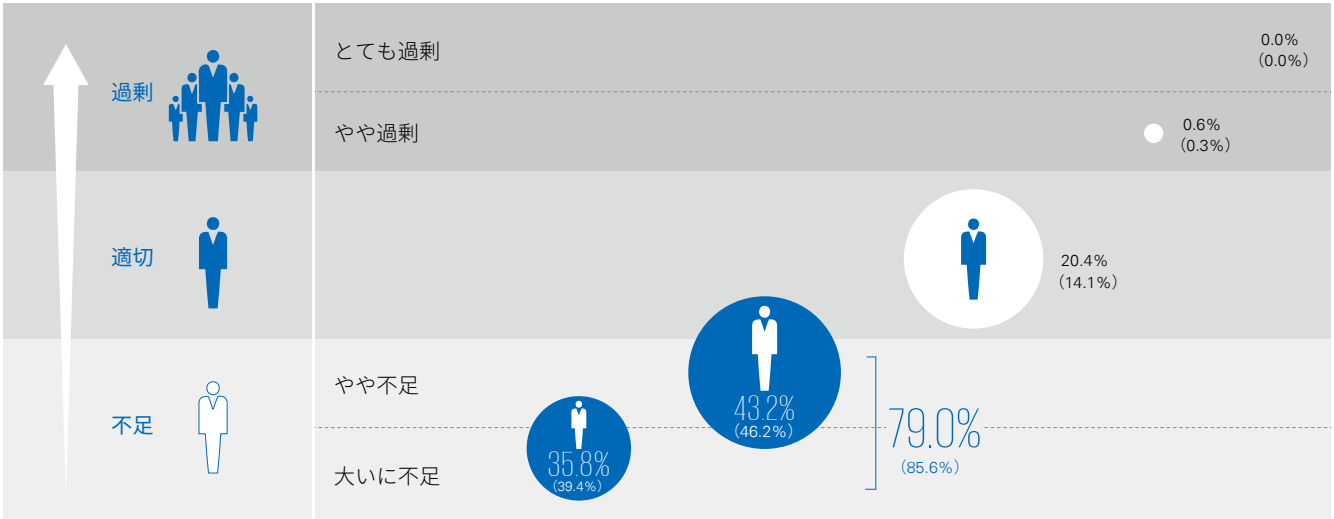


出典：KPMG作成　（n=285）

図表2　セキュリティ投資・セキュリティ人材の不足

サイバーセキュリティ対策組織の陣容（人数）規模

79.0%が人材不足を感じている



出典：KPMG作成

※（）内%は2019年度数値。2019年は0.4%が無回答（n=285）

を自動化するソリューションの導入率はまだ低い状況にあります（8.1%）。セキュリティ運用の自動化は、情報セキュリティ人材不足への対策として、今後の浸透が期待される領域です。

II リモートワークセキュリティ

1. リモートワークの実態

COVID-19によるリモートワークを中心とした働き方の変化によって、75.1%の回答企業が在宅勤務を少なからず導入しています。このような劇的な環境変化が生じているにもかかわらず、リモートワークにおけるサイバーセキュリティの対策方針を策定している企業は47.7%にとどまりました。

これもリソース不足が影響している可能性を否定できませんが、リモートワークの場合、従前のようにオフィスで勤務する場合とは異なるオペレーションが求められます。そのため、常時自宅で作業する環境下においてセキュリティ方針が明確に打ち立てられていない状況は、まさにリスクと隣り合わせであるといえます。

2. 従業員等による内部不正を懸念

このような状況において、回答企業の50.5%が従業員による内部不正を懸念しています。また、在宅勤務率が高いほど、内部不正を懸念する企業が多い傾向が見られます。一方、マルウェア感染やフィッシング詐欺、端末のセキュリティパッチ適用や紛失・盗難といった問題点については、在宅勤務率が低い企業ほど多くなる傾向にあります（図表4参照）。

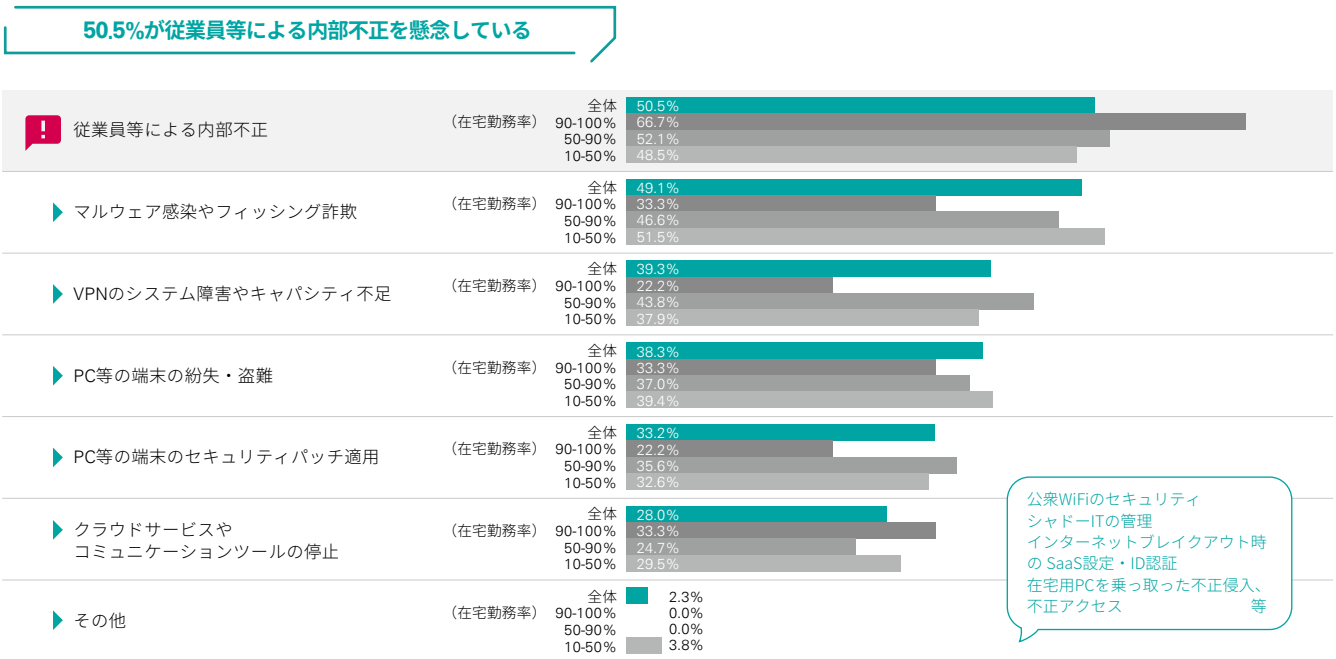
リモートワークセキュリティの対策としては、過半数の企業でハードディスクの暗号化やUSB接続の制限・禁止、モバイルデバイス管理（MDM）によるスマートフォン等のリモート消去など物理的な情報漏えい対策が講じられています。その一方で、eメール・ウェブ・クラウドといったネットワーク経由の情報漏えい対策（DLP）は17.3%にとどまっており、あまり普及していない状況が見受けられます。

本調査からは、リモートワークに変わったことにより、オフィスの入退室管理や周りの目などによる牽制といった物理的な対策が効いていた部分が無効化されたことで、全体のセキュリティレベルが低下していることが読み取れます。したがって、これを補完するための対策を講じることが急務といえます。

3. リモートワーク環境のセキュリティ対策

リモートワーク環境では、社内環境だけでなく、クラウドなどの社外環境、PCやスマートフォンなどのエンドポイントへの攻撃も想定されます。そのため、全体のセキュリティレベルを上げるには、社内環境、社外環境、エンドポイントそれぞれで次のような対策を講じることが求められます。

図表4　在宅勤務におけるセキュリティ面での問題



出典：KPMG作成

（複数選択3つまで可／n=214）

社内環境の脅威への対策:

不正侵入対策、社外からのアクセス制御、ネットワークの増強、セキュリティ監視・運用の強化など

社外環境の脅威への対策:

許可されていないクラウドの利用制限、利用しているクラウドのセキュリティ強化、本人認証の厳密化など

エンドポイントの脅威への対策:

BYODの許可判断、プライベート利用の制限、持出しPCのセキュリティ対策、端末からの情報漏えい対策など

Ⅲ 制御システムセキュリティ

1. サイバー攻撃の標的になりやすいスマートファクトリー

日本の製造業が抱える課題の解決策として、スマートファクトリーへの取組みはますます加速しています。スマートファクトリー化が進んだ工場では、さまざまなデバイスをネットワークに接続し、蓄積したデータを分析することでクラウド、人工知能（AI）、ロボットなどの最新テクノロジーを活用しています。従来の工場と比較して、スマートファクトリーはERPやSCMなど情報系との通信、クラウドやリモートなど外部との通信など、ネットワークの接続が多岐にわたります。

これは、スマートファクトリーがサイバー攻撃の標的になりやすいということでもあります。しかも、さまざまなデバイスがネットワークに接続するために、被害を受けた場合、操業に直接的なインパクトを与えることにもなります。

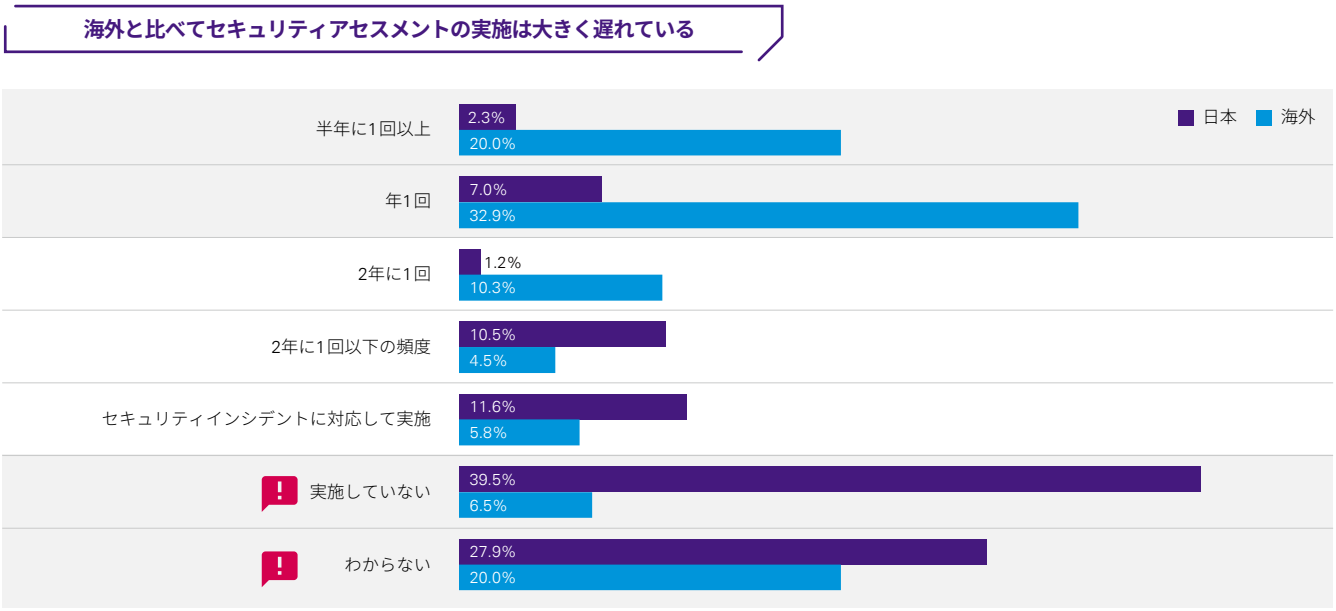
なお、制御システムへのサイバー攻撃は、日本でも海外でも、従来からのマルウェア感染したリムーバブルメディアや、悪意のある第三者からのeメール（フィッシング）を経路とすることが多いようです。ただ、日本の場合、42.7%の企業が攻撃経路がわからないと回答しており、これも大きな課題といえるでしょう。

2. 経営リスクとなっている制御システムのセキュリティ対策

回答企業の約3割は、工場やプラントにおける制御システムに関する事業に取り組んでいますが、そのうち海外工場が存在する企業において統制管理ができていると回答した企業はわずか13.4%でした。そして、68.7%の企業が「海外の工場は統制管理していない」と回答しています。この数字は、前回（2019年）調査とほぼ同じであることから、海外工場の統制管理はほとんど進んでいないと思われます。

前述したように、制御システムに対するセキュリティリスクが高くなっているにもかかわらず、日本では制御システムに対するセキュリティアセスメントは浸透しておらず、39.5%が「実施していない」、27.9%が「わからない」と回答しています。一方、海外では52.9%の企業が少なくとも年に1回以上実施しているという調査結果[1]があります。海外と比べると、日本はセキュリティアセスメントの実施において大きく

図表5 制御システムに対するセキュリティアセスメントの実施状況



出典：KPMG作成
出所：海外は「(CS)² AI-KPMG Control System Cyber Security Annual Report 2020」をもとに集計
https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/kpmg-control-system-cyber-security-annual-report.pdf

（日本：複数選択可／n=86）

遅れているといえます（図表5参照）。

また、日本は制御システムのセキュリティ監視を実施している企業はわずか9.3%である一方で、監視の計画がない企業が47.7%にのぼります。それに対して、海外では監視を実施している企業は30.3%、パイロットや実施予定を含めると9割近くとなっており、海外と日本とでは大きな開きがあります。

こうした状況を解決するための第一歩は、IT部門とOT（Operational Technology）部門が連携し、工場が抱えているサイバーセキュリティリスクを可視化、把握することです。

多くの企業にとって、制御システムに対するサイバー攻撃は経営リスクとなっています。今後は、スマート化された工場におけるリスクをどのように評価し、どのようなセキュリティ対策を導入するかが課題といえるでしょう。

Ⅳ 社内外すべてを「信用できない領域」としてセキュリティ対策を行う「ゼロトラスト」

リモートワークによって働く場所（ワークプレイス）がオフィスのみにとどまらず、社内と社外の区別が曖昧になっていることから、従前のセキュリティ対策で見られた、いわゆる「境界」で防御するという考え方が破綻しようとしています。そこで、新たなセキュリティの考え方として「ゼロトラスト」が提唱されています。ゼロトラストとは、社内外すべてを「信用できない領域」としてセキュリティ対策を行うことです。

ゼロトラストセキュリティの原則は多層防御です。ネットワークだけでなく、認証・認可の仕組み、データ保護、監視などの対策を多層に取り込むことで、防御・検知のポイントを増やします。

ただ、制御システムは情報システムのようにゼロトラストセキュリティを導入することは難しい状況にあります。工場ネットワーク内部の設備機器は古いものが多く、エンドポイントのセキュリティ対策も困難であることから、物理的な保護に頼らざるをえません。そのため、工場におけるセキュリティ対策は、ゼロトラストと他の境界型セキュリティとを組み合わせることで強化を図ります。

Ⅴ さいごに

国際的なスポーツイベントの開催、COVID-19によるリモートワークの進展など、大きな環境変化が起こったことが後押しとなり、デジタル・トランスフォーメーション（DX）が一気に加速しています。世の中の仕組みがインターネットに依存する割合が今後さらに高まるなか、サイバー攻撃が激化、凶悪化することは不可避でしょう。

COVID-19によるパンデミックは物理的空間での接触を困難なものにしましたが、翻ってサイバー空間におけるパンデミックの発生もまったく否定することはできません。社会的な営みを継続するためには、物理的空間、サイバー空間の両方が健全であることが望まれます。

KPMGは、サイバー空間の健全化を維持するために、サイバーセキュリティに対する支援を通じて社会に貢献してまいります。

1 「(CS)² AI-KPMG Control System Cyber Security Annual Report 2020」

Appendix：「サイバーセキュリティサーベイ2022」について

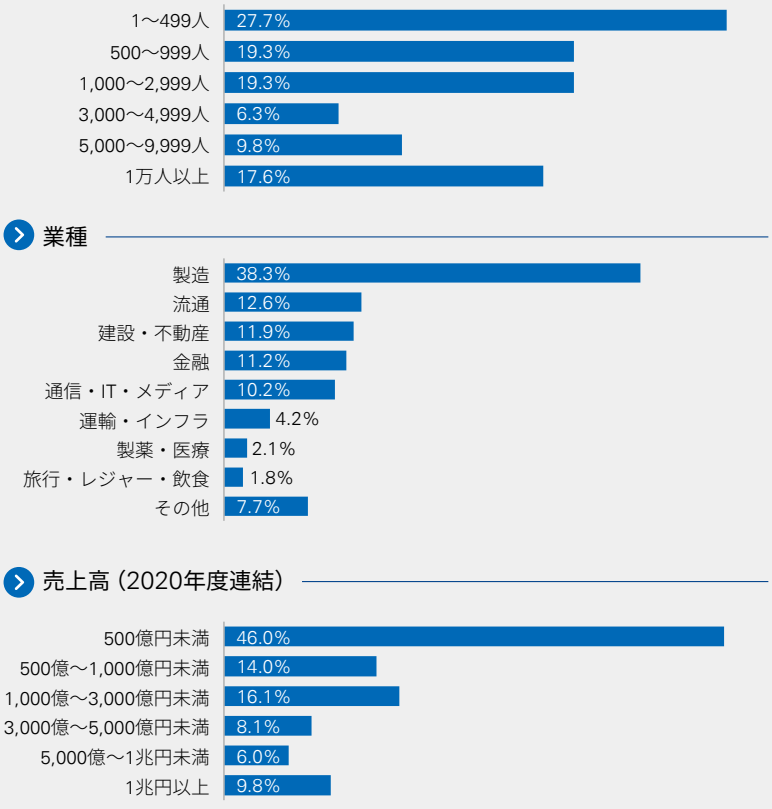
「サイバーセキュリティサーベイ2022」は、国内の上場企業および売上高400億円以上の未上場企業を対象に実施した、企業のサイバーセキュリティに関する実態調査の結果をまとめたレポートです。

本年で第5回目となる本調査は、KPMGコンサルティングとKPMG FASが共同で「サイバーセキュリティ」「リモートワークセキュリティ」「制御システムセキュリティ」をテーマに実施しました。新たな取組みとして、リモートワークセキュリティに関する設問を新設するとともに、サイバーセキュリティの評価フレームワークとして広く活用されている「米国国立標準技術研究所（NIST）サイバーセキュリティフレームワーク」を意識した構成としていることが特徴となっています。

調査概要は次のとおりです。

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　：2021年6月1日～7月31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：285件

回答企業の属性



出典：KPMG作成

関連情報

サイバーセキュリティサーベイ2022

2022年1月発行

本調査レポートは、ウェブリンクより閲覧、ダウンロードが可能 です。

home.kpmg/jp/cs-survey2022

本稿に関するご質問等は、
以下の担当者までお願いいたします。

KPMGコンサルティング株式会社
薩摩 貴人／パートナー

☎ 03-3548-5111（代表電話）
✉ takato.satsuma@jp.kpmg.com

KPMGジャパン
home.kpmg/jp

home.kpmg/jp/socialmedia