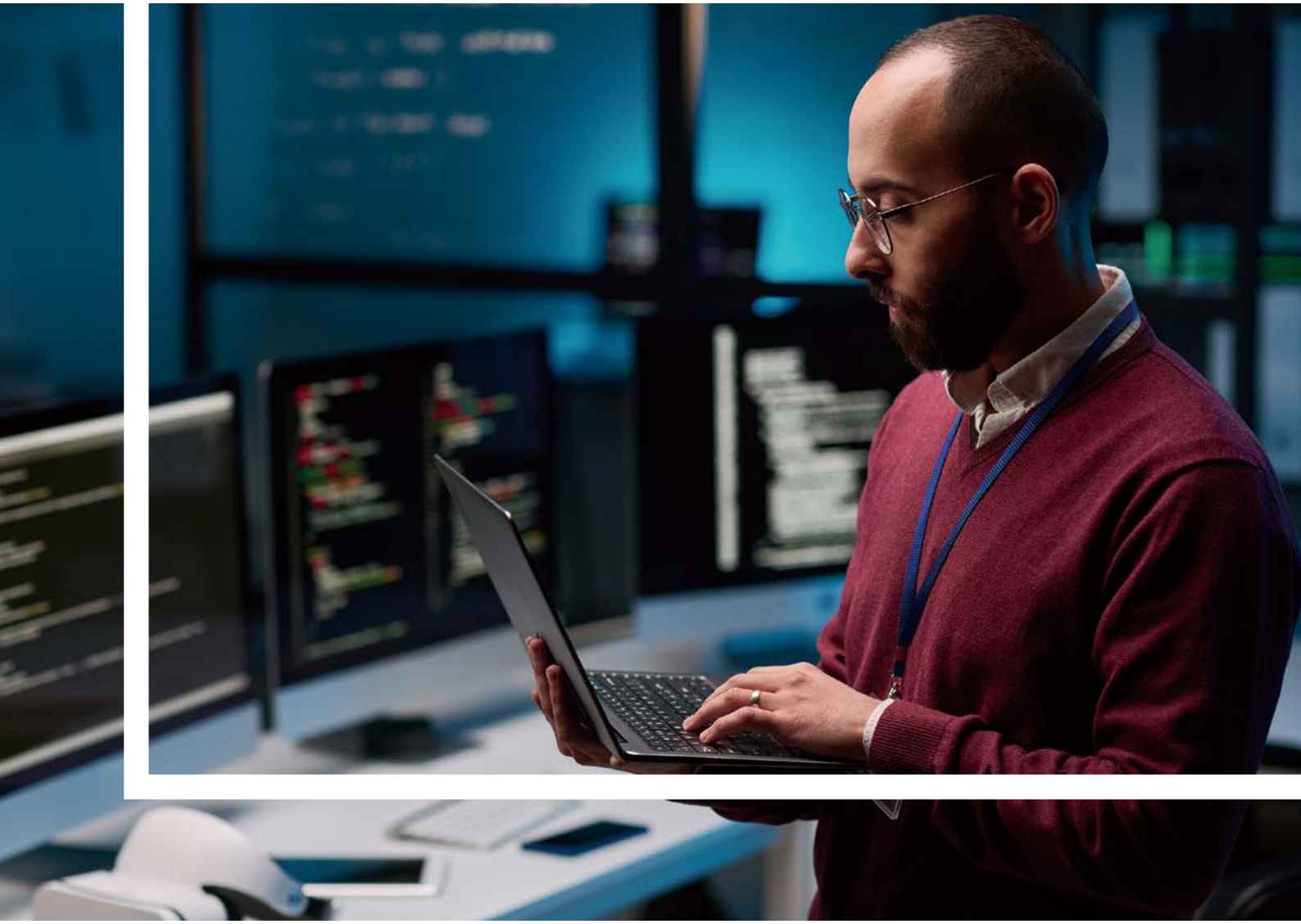
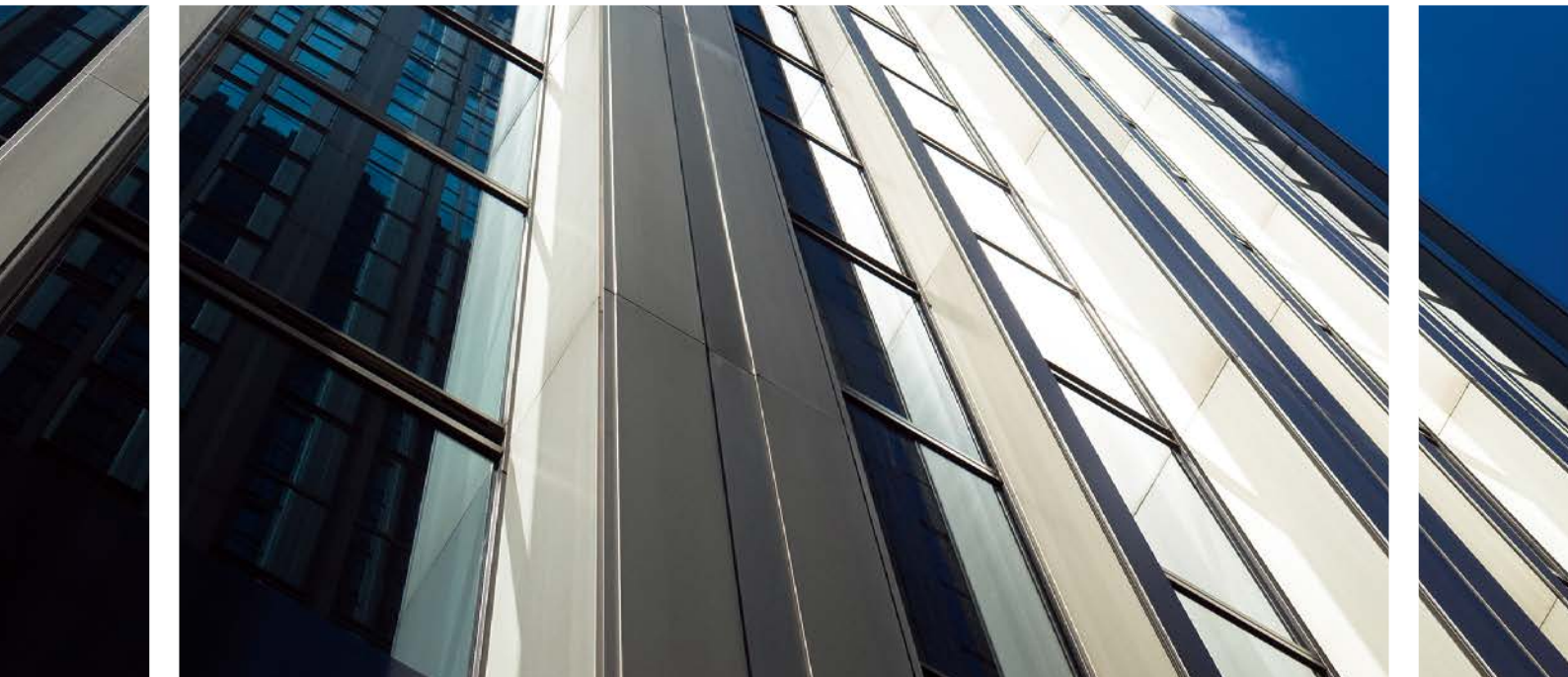
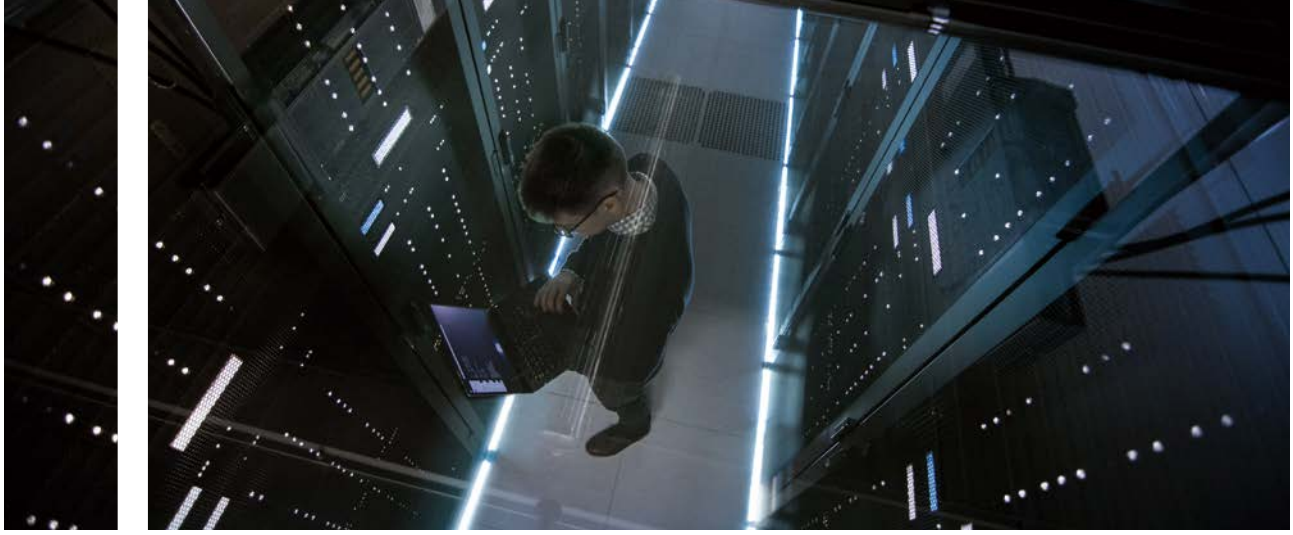
サイバーセキュリティに関する
財務報告リスクの高まりとその対策



pwc

www.pwc.com/jp





1 はじめに

サイバー攻撃は企業の業種、規模、所在地を問わず行われるものであり、一般的にどの企業においてもサイバーセキュリティリスクは存在します。昨今、Webサイトや新聞などで企業に対するサイバー攻撃のニュースを目にする機会は増加しており、中には、企業の経済活動が大きな損害を被るケースもあります。またサイバー攻撃により、財務報告に関連するシステムやデータが利用できず、本来の提出期限までに有価証券報告書を提出できなかったり、開示すべき重要な不備となったりした他、有価証券報告書にサイバー攻撃を原因とする特別損失を計上した事例もあります。

図表1は直近5年間のサイバー攻撃／不正アクセスに関連した適時開示の状況、有価証券報告書における損失計上の状況、監査上の主要な検討事項の状況の推移を集計したものです。各項目に該当する企業数は増加の傾向にあり、サイバーセキュリティに関する財務報告リスクの高まりが見てとれます。

内閣サイバーセキュリティセンターと経済産業省は、サイバーセキュリティに関する注意喚起を発令しています。経産省の「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティリスクをビジネス上のリスクとして識別するだけでなく、サイバーセキュリティ対策を実施すべきと記載されています。こうした動きからも分かるように、国もサイバーセキュリティ対策を講じることは重要だと呼びかけています。加えて、サイバーセキュリティに関する財務報告リスクが高まっている状況を受けて、金融庁は財務報告に係る内部統制の評価と監査の基準を、日本公認会計士協会は監査基準報告書と研究文書を公表。財務報告に関するサイバーセキュリティリスクの識別と評価の検討について触れています。

こうした状況を踏まえ、PwC Japan有限責任監査法人は、実際に企業が財務報告リスクを識別しているのか、また識別したリスクに対してどのように取り組んでいるのかを把握するために調査を実施しました。

図表1：サイバー攻撃／不正アクセス関連の適時開示および有価証券報告書の件数推移

サイバー攻撃／不正アクセス関連	2020年	2021年	2022年	2023年	2024年
適時開示の状況	5社	22社	16社	15社	25社
有価証券報告書における損失計上の状況	1社	6社	8社	10社	13社
監査上の主要な検討事項の状況	0社	2社	4社	3社	2社

出所：PwC作成

調査の概要

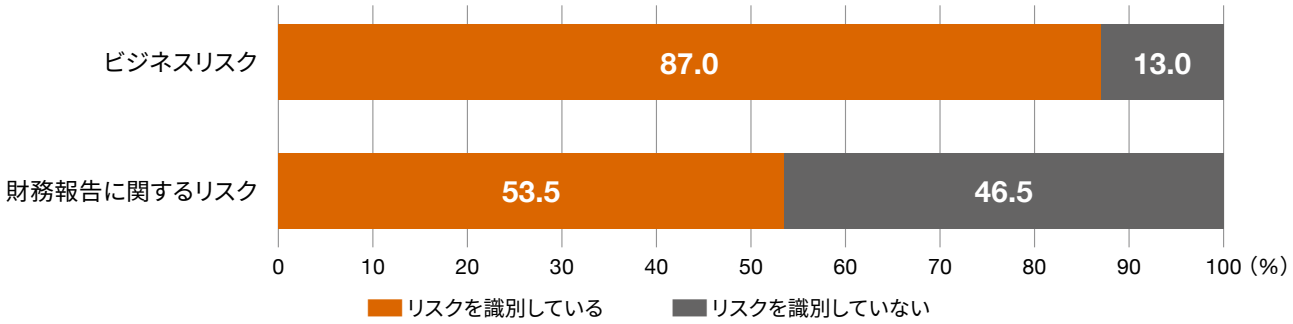
調査方法：財務報告に関するサイバーセキュリティリスクの識別状況についてアンケートを実施
時　　期：2025年2月
対　　象：上場・非上場会社の部長級以上
有効回答：200人（複数回答可の設問あり）
留意事項：複数回答可の設問があるため必ずしも合計が100%にはならない

2 財務報告の観点からの、サイバーセキュリティリスクの識別・評価

サイバーセキュリティに関する財務報告リスクの高まりを受けて、本調査では、企業における識別・評価の現状を財務報告の観点から分析しました。

図表2：サイバーセキュリティリスクの識別状況の比較（ビジネスリスク／財務報告に関するリスク）

設問：ビジネスリスク／財務報告の観点からサイバーセキュリティリスクを識別していますか



出所：PwC作成

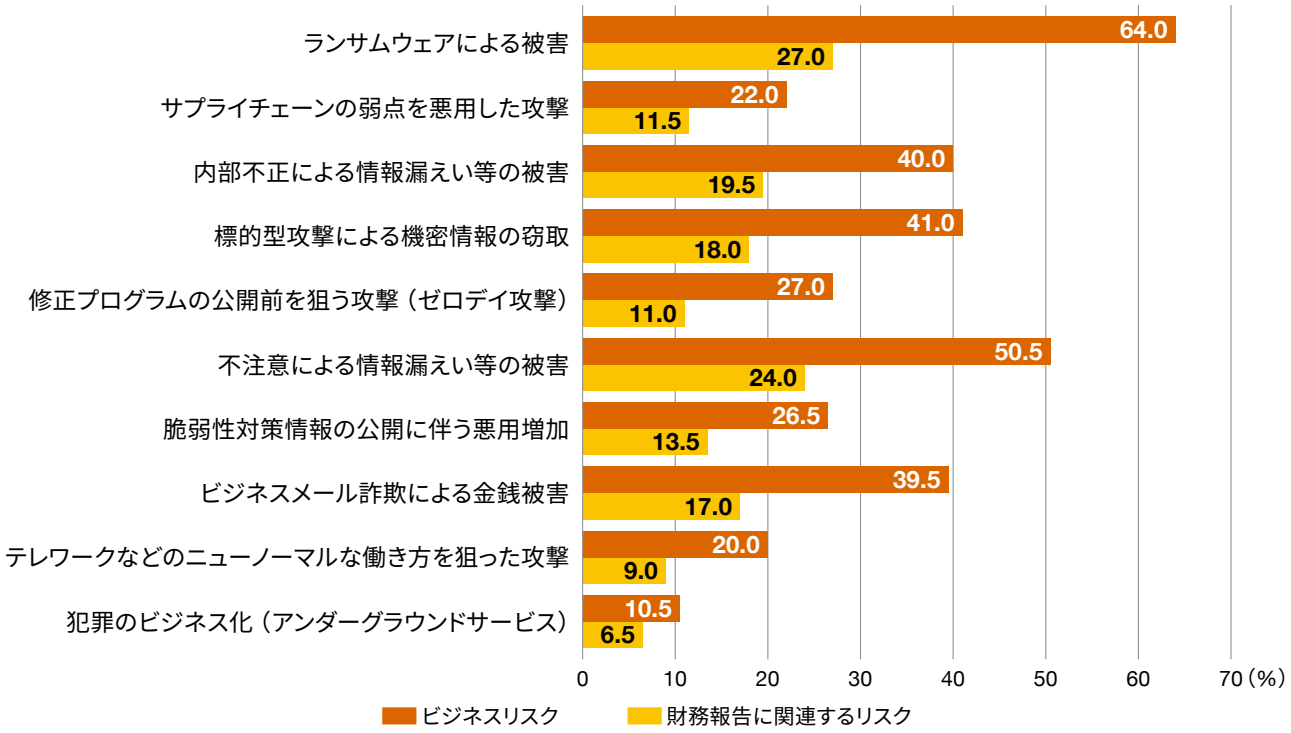
図表2、図表3から分かるとおり、多くの企業が規模や業種などを問わず、ビジネスリスクとしてサイバーセキュリティリスクを識別しています。「サイバーセキュリティリスクを識別していない」と回答した企業は全体の13.0%にとどまり、ほぼ全ての企業がサイバーセキュリティをビジネス上のリスクとして認識していることがうかがえます（図表2）。これは、昨今ランサムウェアやビジネスメール詐欺など、ビジネス上多大な影響を及ぼすセキュリティインシデントの発生を受け、サイバーセキュリティに対する各企業のリスク認識がアップデートされていることの表れであると考えられます。

一方、財務報告リスクとしてサイバーセキュリティリスクを識別している企業は、ビジネスリスクとしてサイバーセキュリティリスクを識別している企業に比べると、その割合が低いことが分かります。アンケート結果においても、全体の約半数の企業が、財務報告に関連するリスクとしてはサイバーセキュリティリスクを識別していないと回答しています（図表2。前段の質問でビジネスリスクとしてもサイバーセキュリティリスクを識別していない企業を含む）。

特に、「ランサムウェアによる被害」については、自社の財務報告に関連するリスクであると捉えている企業は全体の27.0%にとどまりますが（図表3）、サイバーセキュリティに関連して生じた開示すべき重要な不備のほとんどがランサムウェア攻撃に端を発しています。実際にランサムウェアに伴う開示すべき重要な不備の識別を余儀なくされた企業の事例を見ると、ランサムウェアの感染により四半期報告書や有価証券報告書などの開示が遅延し、その影響の大きさを鑑みて開示すべき重要な不備を識別している、といった事例が一定数見受けられます。

図表3：ビジネスリスクとして識別しているサイバーセキュリティリスクと、財務報告リスクとして識別しているサイバーセキュリティリスクの比較

設問：識別しているサイバーセキュリティリスクについて、あてはまるものを選択してください（いくつでも）



出所：PwC作成

多くの企業において、セキュリティインシデントが自社の情報資産や業務継続に影響を及ぼすリスクだと識別はできていても、それが財務報告プロセスにまで影響を及ぼしうる、という点についてはまだまだ認知が進んでいないと思われます。

しかしながら、読者の中には「たとえ財務報告という観点でサイバーセキュリティリスクを識別しなくとも、結果として取る対策が同じであれば、問題はないのではないか」と考える方もいらっしゃるかもしれません。果たして本当にそうでしょうか。

ビジネスリスクとしてサイバーセキュリティリスクを識別する場合、そのリスクへの対応策は、自社の保有する情報資産や、それに関連する脅威・ぜい弱性といったものをベースに決定することが一般的であると思われます。一方、財務報告としてのサイバーセキュリティリスクへの対応に際しては、情報資産としての純粋な価値のみならず、財務報告の継続性や保持する情報資産の財務諸表上の資産価値といった財務報告特有の観点も加味した上でリスク対応方針を決定する必要があります。実際に、上述したような、ランサムウェア攻撃によって開示すべき重要な不備を識別した企業においても、その不備の対象を特定のセキュリティ対策の不足ではなく、サイバーセキュリティのリスク評価や対応に着目する事例があり、不十分なリスク評価が財務報告リスクとして顕在化しうることを示しています。

企業が保有するデータに関連してサイバーセキュリティリスクを検討する際、自社の保有する個人情報の機密性をリスクとして認識している企業は多いようです。では、財務報告の継続性という観点から、財務データの可用性に関するリスクまで認識できているでしょうか。前者への対応方針として自社のネットワークの境界に侵入検知に関連するツールなどを導入することができていたとしても、財務報告に活用されるデータの可用性に関するリスクへの対応策としては、会計システムなどの財務報告において重要な影響を与えるアプリケーションについて、イミュータブルバックアップやテープバックアップなど、データの可用性に資する追加の対策を導入する必要があるかもしれません。

工場の操業継続など、コア業務に関してはBCP訓練を通じて対応力を高めている企業が多く見られます。こうした取り組みに対して、財務報告プロセスの業務継続の可否を含めて、BCPの計画内で検討や訓練が行われているでしょうか。セキュリティインシデントにより財務報告プロセスの継続性が損なわれるケースとしては、例えば自社の会計システムがバックアップデータを含めてランサムウェアに感染し、システムの再構築が必要となったために、従来の会計システムを利用せずに財務報告プロセスを実施する必要が生じるような場合が考えられます。このような場合には、手動で経理業務を継続する場合や別の会計システムを急遽導入し、経理業務を継続することを余儀なくされる可能性があります。

いずれの場合においても事前に対応方針を決定していない場合は相当な現場の混乱が生じる可能性があり、財務報告の継続性を保持するためには、セキュリティインシデントにより既存のシステムの可用性が損なわれた場合を想定したシナリオプランニングと訓練が必要かもしれません。以上の点を踏まえると、ビジネスリスクとしてのサイバーセキュリティリスクへの対応のみでは、財務報告の観点では不十分な対策となることがお分かりいただけたと思います。

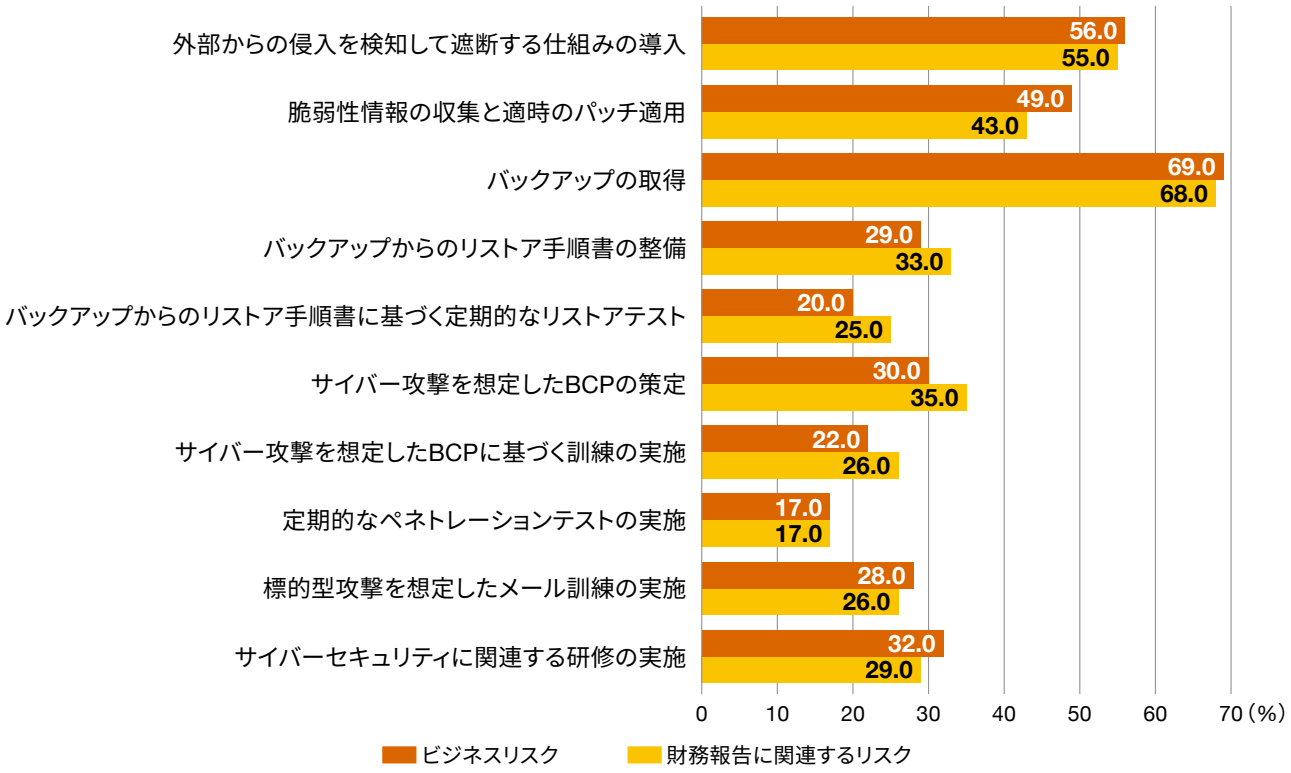
しかしながら、図表4の調査結果において示されているとおり、サイバーセキュリティリスクをビジネスリスクとして捉えるか財務報告リスクとして捉えるかの違いは、企業が実際に適用する対策の種別にはほとんど影響を及ぼしていないことがうかがえます。これはすなわち、上述したような財務報告特有のサイバーセキュリティリスクに対する対策が不十分である可能性を示唆しています。通常のビジネスリスクに対する備えだけでは、財務報告に関連するリスクへの対策としては不十分となる可能性があるということです。

さらに、2024年4月1日以降改訂された内部統制報告制度（J-SOX）においては、内部統制の基本的要素となる「ITへの対応」に関連して、サイバーリスクの高まりなどを踏まえた情報システムに係るセキュリティの確保が重要であることが明文化されました。これに伴い、企業は従来J-SOXにおいては特段考慮されていなかったセキュリティに関するリスクも考慮した上で内部統制を構築することが要求されているものといえるでしょう。

本対応に際しては、ビジネスリスクとしての全般的なサイバーセキュリティリスクではなく、適切に自社の財務報告に関連するサイバーセキュリティリスクを捉えることが肝要であると考えられます。自社の財務報告プロセスに影響を及ぼしうるサイバーセキュリティリスクをリスクベース・アプローチで検討し、そのリスクの低減に本質的に資するコントロールをマッピングする必要があります。自社ですでに実施しているサイバーセキュリティ対策をリストアップして、後付けでリスクをひもづけるといったやり方では、本来的に自社で担保すべき財務報告に関連するサイバーセキュリティリスクを見落としてしまう可能性があります。

図表4：ビジネスリスクとして識別しているサイバーセキュリティリスクと、財務報告リスクとして識別しているサイバーセキュリティリスクのそれぞれに対する対策の適用状況

設問：サイバーセキュリティリスクへの対策として、適用しているものを選択してください（いくつでも）



出所：PwC作成

3 財務報告観点からの識別・評価を推進するために

前項の調査では、サイバーセキュリティリスクをビジネスリスクとして識別・対策している企業は多数あるものの、財務報告リスクとして識別・評価している企業はそれほど多くない傾向が見られました。またJ-SOXにおいてサイバーセキュリティリスクに対応する統制を整備・運用している企業は、より少ない傾向にあります。

財務報告の観点からサイバーセキュリティリスクの識別・評価を推進するためには、次の事項を財務報告の関係者間で確認しておく必要があると私たちは考えます。

- サイバーセキュリティ対策の必要な財務報告に関連するシステムまたはデータは何か
- 仮にサイバー攻撃によって関連するシステムまたはデータが利用できなくなった場合、いつまでに復旧が必要か、いつ時点のデータをバックアップしておく必要があるか
- サイバー攻撃を受けた場合に、どのような損害が想定されるか
- 有事の連絡体制は明確になっているか　など

連結財務諸表の観点から、子会社・関連会社でも同様の確認が必要となります。特に海外の子会社・関連会社はサイバー攻撃が報告されるまでに時間を要する可能性が高いため、日頃からコミュニケーションを図ることが重要です。また財務報告に影響を及ぼすサイバー攻撃が発生した場合には、外部監査人である監査法人にも適時に情報を共有し、財務報告への影響を説明する必要があるため、平時からサイバーセキュリティリスクへの対応についてコミュニケーションをとり、有事の際は迅速に情報を共有できる体制を整えておくことが肝要です。

次に、財務報告に関するサイバーセキュリティリスクへの対策として、不正侵入検知、パッチ管理、バックアップ、リカバリーの観点から対策を検討することが有用です。外部からの不正アクセスを検知してネットワークを遮断する仕組みの導入や、既知の脆弱性に対応するためのパッチ適用といった施策は、事前の備えとして有効です。ただし、こうした対策を講じても、サイバー攻撃を完全に防ぐことはできない可能性があります。そのため、万が一に備えて、復旧手順の整備やバックアップの確保もおこなうことが重要です。上記以外に、財務報告リスクを題材として研修やサイバー攻撃を想定したBCP訓練を定期的に実施することなども有効な対策と言えます。

最後に、サイバー攻撃もしくは不正アクセスにより外部へのデータ流失が発生した場合、攻撃を受けた企業は被害を受けた側ですが、一方で、個人情報が流失した場合には情報を漏えいした側にもなることに留意が必要です。欧州の一般データ保護規則（GDPR）に違反した場合には高額な制裁金の対象となる可能性もあるため、改めて自社のサイバーセキュリティリスクの識別と十分な対策が実施できているかをご確認いただきたいと思います。

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約12,700人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界149カ国に及ぶグローバルネットワークに370,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

発刊年月：2025年5月　　管理番号：I202504-01