2025.7.9

ESG/統合報告トピック調査
サイバーセキュリティ対応

顧問　公認会計士 篠木 良枝

当調査では、日経225銘柄中、2024年1月から12月末の期間で発行が確認できた210社の狭義の統合報告書（※）を対象に、サイバーセキュリティへの対応についての調査を実施した。サイバーセキュリティ対応は、データやネットワーク・コンピュータなどをサイバー攻撃や過失、内部不正から守るための対策を指す。

(※)「狭義の統合報告書」とは、統合報告フレームワークなどの統合報告ガイダンスを参考にして制作されている報告書、または冊子やWEBサイトでレポート名を統合報告書・統合レポート等と題されている報告書を指す。

調査サマリー

■直近5年間で情報漏洩があった、あるいは可能性があった企業は52%

■サイバーセキュリティリスク管理体制を構築していることを記載しているのは96%

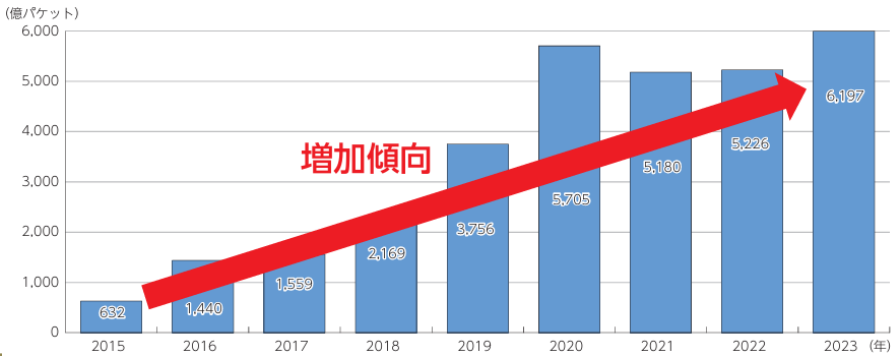
■サイバーセキュリティ対応のための資源を確保していることを記載しているのは87%

はじめに

総務省の令和6年版情報通信白書（注1）によると、サイバー攻撃は増加しており、サイバーセキュリティ上の脅威は増大している（図表１）。ビジネス活動においてIT活用の促進、デジタル・トランスフォーメーション（DX）は重要である反面、サイバー攻撃、不正アクセスによる情報漏洩の可能性のニュースが連日のように報道されている。そこで、サイバーセキュリティに関してどのような対応・開示が進んでいるか明らかにすることを目的として、調査を実施した。今回の調査対象210社※については、狭義の統合報告書、ウェブサイト、サイバーセキュリティレポート等を確認している。情報漏洩の事例については、企業名と「情報漏洩」というキーワードで検索し、企業のウェブサイト以外も参照したところ、直近５年間で情報漏洩があった、あるいはサイバー攻撃を受けて情報漏洩の可能性を否定できない企業が110社（52%）あった。当該110社の中には、情報を共有している先が情報を漏洩した場合を含めているが、サイバー攻撃を受けたものの情報漏洩がなかったことを明言している場合は含めていない。

※日経225対象企業のうち、2024年1月から12月末の期間で狭義の統合報告書の発行が確認できた210社

図表１：大規模サイバー攻撃観測網（NICTER）におけるサイバー攻撃関連の通信数の推移



（出典）総務省　令和6年版情報通信白書（国立研究開発法人情報通信研究機構「NICTER観測レポート2023」を基に作成）

調査結果　サイバーセキュリティ対応の開示状況

経済産業省、独立行政法人情報処理推進機構（IPA）が2023年3月に公表した、「サイバーセキュリティ経営ガイドラインVer.3.0」（注2）のサイバーセキュリティ経営の重要10項目を参考に調査項目を設定している。サイバーセキュリティ経営の重要10項目の指示４「サイバーセキュリティリスクの把握とリスク対応に関する計画の策定」は非常に重要であり、総花的な記載として有価証券報告書の「事業等のリスク」に記載されている可能性はあるが、秘密保持の観点から自社の特に重要と考えるリスクを開示している企業は少ないのではと思料されるため、調査項目から除外している。また、指示10「サイバーセキュリティに関する情報の収集、共有及び開示の促進」は、今回の調査全体で把握できると考え、調査項目から除外している。調査項目として、図表2の各事項について開示状況を調査したところ、以下の通りであった。

図表2：サイバーセキュリティ対応の開示状況（n=210社）

番号	開示することが考えられる事項	開示社数	開示割合
(a)	サイバーセキュリティへの対応方針、セキュリティポリシーの策定※	174 (116)	83% (55%)
(b)	サイバーセキュリティリスク管理体制の構築	201	96%
(c)	サイバーセキュリティ対応のための資源の確保	182	87%
(d)	サイバーセキュリティ専門人材の人材育成目標、育成方針、先端セキュリティ技術等への取り組み	115	55%
(e)	サイバーセキュリティリスクに効果的に対応する仕組み	132	63%
(f)	PDCAサイクルによるサイバーセキュリティ対応の継続的改善	117	56%
(g)	インシデント発生時の緊急対応体制の整備（CSIRT等）	148	70%
(h)	インシデントによる被害に備えた演習	144	69%
(i)	ビジネスパートナーや委託先等を含めたサプライチェーン全体のサイバーセキュリティの状況把握及び対応	99	47%

※（）内は、セキュリティポリシーを開示している社数で内数

（a）組織全体としてのサイバーセキュリティへの対応方針、セキュリティポリシーを策定している企業は174社（83%）であり、うちセキュリティポリシーを公表している企業は116社（55%）であった。当該116社の中には、サイバーセキュリティ経営宣言として、経営主導によるサイバーセキュリティ対応強化をうたう企業もあった。一方で、組織全体としてのサイバーセキュリティへの対応方針はあるものの内容を公表していない企業は58社（28%）あった。当該58社には、ポリシーよりも詳細について定めるセキュリティ規程を作成し、公表はせずに継続的に見直しを行っている旨を開示している企業なども含まれる。

（b）サイバーセキュリティリスク管理体制を構築し、開示している企業は201社（96%）であった。サイバーセキュリティ対応について開示している企業については、ほぼ全ての企業で管理体制についても開示が行われていた。情報セキュリティ委員会を設置している企業や、リスク管理委員会やサステナビリティ委員会の中で、他の対応すべき課題とともに情報セキュリティを扱っている企業があった。

（c）サイバーセキュリティ対応のための資源（予算、人材等）を確保しており、信頼できるベンダーへの委託や、セキュリティ担当者育成のための研修・トレーニングを行っていることが記載されている企業は182社（87%）であった。サイバーセキュリティリスク管理体制がある企業では、全役職員を対象としたセキュリティ研修をeラーニングで行っている旨を開示している企業が多く見られた。

（d）サイバーセキュリティ人材の育成目標人数などの人材育成目標、育成方針、先端セキュリティ技術への取り組みの記載がある企業は115社（55%）であった。DXに注力する企業において、人材育成目標を開示するだけでなく、情報セキュリティ人材として選ばれた高い専門知識を持った人材を、情報処理推進機構（IPA）や外部のセキュリティ専門企業に派遣し、業界の最前線で経験を積ませている例を開示している企業があった。

（e）サイバーセキュリティリスクに効果的に対応する仕組みについて記載がある企業は132社（63%）あった。サイバーセキュリティリスクに効果的に対応する仕組みは、例えば*多層防御、*脆弱性診断、*暗号化や電子署名、*ゼロトラストモデルに基づく対策、クラウドサービスのアクセス制限やアカウントの管理などを指す。好事例としては、図表３の2社が提示できる。

図表３：サイバーセキュリティリスクに効果的に対応する仕組みの好事例

好事例	業種
サイバー攻撃が高度化、巧妙化する中で、インテリジェンス（サイバー攻撃の早期警戒情報）を活用し、*ISAC（Information Sharing and Analysis Center）や*ダークウェブの調査などを含めて予防対策に活用。防御においてもゼロトラストの考え方を導入し、「操作する人・通信を発生させる機器・システム処理のプロセス」の3点をチェックし、信頼性を確保。	空運業
PC内での不審な挙動を検知するためのツール（EDR：Endpoint Detection and Response）を各自のPCや製造現場の端末、サーバに導入。パブリッククラウド特有の不適切な公開権限の設定などによるセキュリティリスクを可視化し、問題のある設定の早期検出・是正のため、セキュリティ設定ミスを検出するサービスCSPM（Cloud Security Posture Management）を活用し、クラウド利用時のリスクを低減。	その他製品

*各用語の内容は下記の通り。

多層防御：物理層、ネットワーク層からデータ層までの多層防御を導入することで、１つの機器やソフトウェアに依存する拠点防御対策や、単一の境界防御層（主としてネットワーク境界）に依存する対策の場合より、未知のマルウェアや新たな攻撃手法の登場により容易に突破されるリスクの軽減が期待される防御。

脆弱性診断：システム全体に対し、悪用できる脆弱性がないか確認する診断。

暗号化や電子署名：営業秘密や機微性の高い技術情報、個人情報などの重要な情報についての暗号化や電子署名など、情報を保護する仕組み。

ゼロトラスト：社内外すべてを信用できない領域として、全ての通信を検知し認証を行うという考え方。

ISAC：特定の業界に特化した情報共有と分析を行う組織。

ダークウェブ：一般的な検索エンジンからはアクセスできない領域で、匿名性保持や追跡回避の技術が使用されており、専用のソフトを使用しなければアクセスできないウェブサイト。

（f）PDCAサイクルによるサイバーセキュリティ対応の継続的改善について記載がある企業は117社（56%）であった。サイバー攻撃は変化が早く、現時点の対策としては十分だとしてもすぐに陳腐化する、攻撃者との終わりのない戦いを続けなければならない面があるので、継続的改善が求められている。

（g）インシデント発生時の緊急対応体制の整備（CSIRT等）について記載がある企業は148社（70%）であった。CSIRT（Computer Security Incident Response Team）は、コンピュータセキュリティにかかるインシデントに対応するための体制であるが、インシデント対応だけでなく、平常時においてもインシデントは起こりうるとの前提のもと演習を行い、社内理解を深めるための中心的な役割を担っている旨を記載しているケースが見られた。また、CSIRTを置くだけでなく、サイバーセキュリティ専門の子会社を設立しているケースも見られた。

（h）インシデントによる被害に備えた演習を行っていることを記載している企業は144社（69%）であった。当該記載の中には、全社員を対象とした標的型攻撃メールによる訓練演習を行っている例や、定期的なインシデント訓練を行っている例が見られた。緊急時の対応体制を整備し、演習を行わないと、実際にインシデントが発生した際に即時に適切な対応が取れないため、サイバー攻撃訓練を行っている企業が多く見られた。

（i）ビジネスパートナーや委託先等を含めたサプライチェーン全体のサイバーセキュリティの状況把握及び対応を記載している企業は99社（47%）であった。当該99社では、サプライヤー行動基準や選定基準として、情報セキュリティ対応を求めている企業が多い。サイバー攻撃は、簡単に攻略できるセキュリティが弱い組織が狙われやすいため、持続可能なサプライチェーンを維持するために取引先や業務委託先も目配りする必要がある。好事例としては、図表4の2社が提示できる。

図表4：サプライチェーン全体のサイバーセキュリティ対応の好事例

好事例	業種
サプライチェーンリスクアセスメントの項目に情報セキュリティがあり、デューデリジェンスのプロセスを構築し、リスクアセスメントを実施している。	小売業
サプライヤー向けサイバーセキュリティ対策活動として調査を実施し、結果のフィードバックを実施。サプライヤーのインターネット公開環境のツール診断と社内インフラの簡易調査を行い、リモート会議で各社へ、システムの脆弱性の診断結果とともにフィードバックを行っている。	電気機器

おわりに

当調査では、統合報告書等におけるサイバーセキュリティへの対応についての開示状況を明らかにした。結果、（a）～（i）の項目いずれもおおよそ半数以上で記載が見られた。したがって、ある程度のサイバーセキュリティ対応、開示が進んでいる傾向にあることが確認できた。ただ、直近5年間で情報漏洩があった、あるいは可能性があった企業は52%もあり、件数も深刻さも増大している印象が強い。サイバー攻撃が増えているので、情報漏洩リスクも増えているが、といってITに依存しないビジネスに戻ることは不可能であり、むしろ効率化・生産性向上のためにますますビジネス活動のデジタル化が求められる時代である。DX推進とサイバーセキュリティへの理解、投資は不可分の関係であり、経営課題として取り組む必要があると思われる。ただ、全てのサイバーセキュリティ対策を自前で対応することは難しいし、サイバー攻撃を100%防御することも難しい。外部の情報セキュリティ企業に依頼する範囲を明確にし、サイバー攻撃を受けることを前提として、攻撃を受けた場合に早期発見・早期対応する仕組みを構築し、継続的な改善活動を行うことが重要であると考えられる。そして、こうした「攻撃を前提とした早期発見・早期対応の仕組み」と「継続的な改善活動」が、実効的に機能していることを統合報告書等で積極的に開示することは、不測の事態への企業の対応力の高さを示すことになる。当該開示を通じて、事業継続性に対する投資家等の信頼を高め、安心感を与えることは、持続的な企業価値の維持・向上に繋がることになると考えられる。

注記

1. 総務省（令和6年7月）「令和6年版情報通信白書」 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/index.html （最終閲覧日2025年6月17日）

2. 経済産業省（2023年3月）「サイバーセキュリティ経営ガイドラインVer.3.0」 https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf （最終閲覧日2025年6月17日）

（出所）株式会社宝印刷D&IR研究所 IR/サステナビリティ研究室の調査による