# 経営リスクとしてのサイバーセキュリティ

## ―アンケート調査から読み解く企業の現状と監査役等の着眼点―

2026 年 10 月 29 日

公益社団法人日本監査役協会

ケース・スタディ委員会

（目次）

概要…… i

1．はじめに……1

2．サイバーセキュリティをめぐる環境の変化と取締役・監査役等の役割……2
(1) サイバーセキュリティをめぐる環境の変化……2
① サイバーセキュリティとは……2
② サイバーセキュリティをめぐる近年の動向……2
(2) 取締役・経営者に求められる役割……3
① サイバーセキュリティ経営ガイドライン……3
② サイバーセキュリティ経営の重要 10 項目……4
③ コーポレートガバナンス・コードと内部統制システム……5
④ サプライチェーンのリスクと対策……6
(3) 監査役等に求められる役割……7
① サイバーセキュリティに対する取締役・監査役等の法的責任……7
② 監査役等の監査の視点……7
③ 高まる有事対応の重要性……8

3．アンケート結果からみえるサイバーセキュリティ対策の現状……9
(1) アンケート調査の質問構成の趣旨と実施概要……9
(2) サイバーセキュリティをめぐる経営陣や取締役会等の現状……11
① 直近 1 年間における経営陣の意識の変化……11
② 取締役会等における報告や議論の状況……11
③ 直近 1 年間における議論の進展と実行された施策……13
④ 監査役等がサイバーセキュリティについて述べた意見の内容……16
(3) サイバーセキュリティリスク管理体制……18
① サイバーセキュリティ対策の最終責任者……18
② サイバーセキュリティリスクを管理・統括している組織の設置状況……19
③ サイバーセキュリティ対応方針の社内への周知状況……21
④ サイバーセキュリティリスク管理体制の構築・運用状況……22
⑤ サイバーセキュリティリスク評価の実施状況……23
⑥ 監査役等からみたサイバーセキュリティ対策の全体像……25
⑦ グループ会社におけるサイバーセキュリティの管理・統制状況……27

（4） サイバーインシデント発生時の緊急対応体制……29
① サイバーインシデントを想定したBCPの策定……29
② サイバーインシデントのBCPの運用状況……30
③ サイバーインシデントの訓練の実施状況……32
④ サイバーインシデントの報告・公表ルート……34
（5） サプライチェーン全体でのセキュリティ対策……35
① サプライチェーンのサイバーセキュリティ体制・対策へのアプローチ……35
② サプライチェーンのサイバーセキュリティ体制・対策に関する課題、工夫……36
（6） サイバーセキュリティをめぐる社内の課題……39
（7） 監査役等のサイバーセキュリティへの監査活動……40
① サイバーセキュリティと監査計画、重点監査項目……40
② サイバーセキュリティに対する監査役等のアプローチ方法……42
③ 監査役会等での議論……43
④ 内部監査部門との連携……44
⑤ 監査役等が参考にしているガイドライン……46
（8） サイバーインシデント発生後の対応……47
① サイバーインシデント発生の有無……47
② 監査役等のサイバーインシデントの把握……48

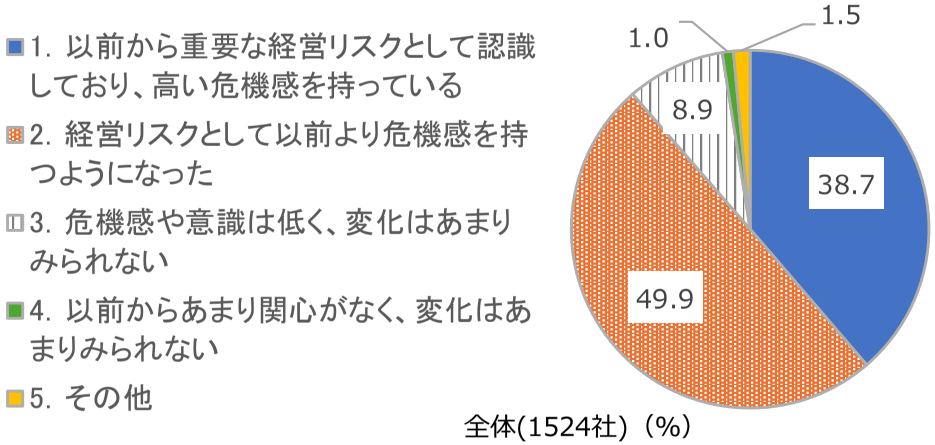
4．サイバーセキュリティに対する監査役等の着眼点と対応……51
（1） サイバーセキュリティが経営課題となっているか……51
（2） サイバーセキュリティリスク管理体制の整備・運用状況の確認……52
（3）「侵入後」を想定した有事対応体制が整備されているか……53
（4） グループ会社・海外拠点、取引先（委託先等）を含むサプライチェーン全体での対策がなされているか……53
（5） 監査計画・重点監査項目へのサイバーセキュリティの反映……54
（6） 有事での対応体制の監査、有事における監査役等自身の対応……55

5．おわりに……57

お問い合わせ・ご意見提出先
(公社)日本監査役協会
企画部企画課
section2@kansa.or.jp

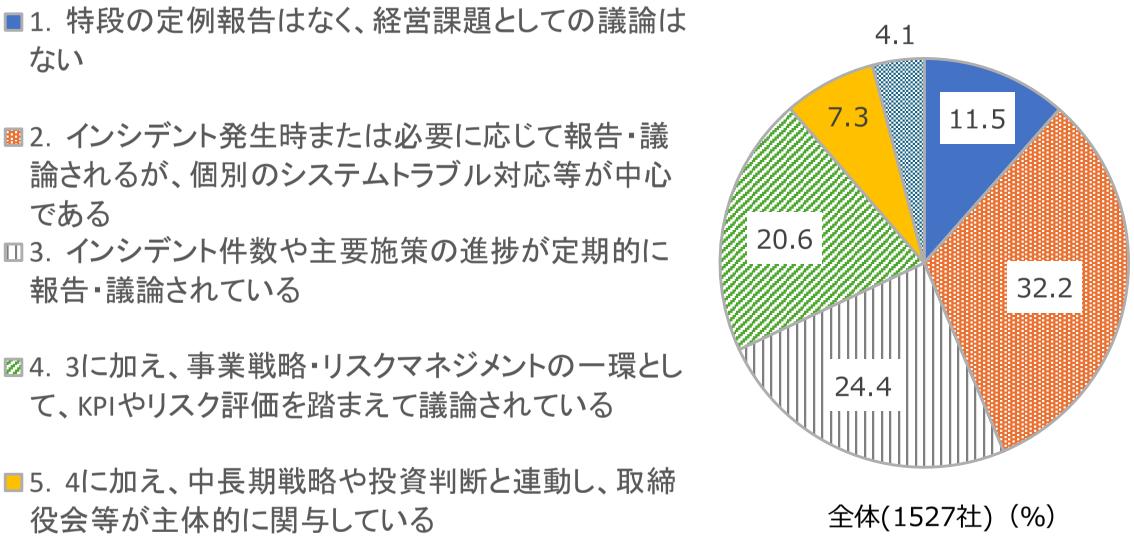
# 1. アンケート結果からみえる特色：サイバーセキュリティに対する経営陣の意識と取締役会の状況

## 経営陣のサイバーセキュリティに対する意識の変化




- 監査役等の認識によれば、「2．経営リスクとして以前より危機感を持つようになった」会社が約半数を占めており、「1．以前から高い危機感を持っている」と合計すると**88.6%**に達する。
- 選択肢3および4の経営陣の意識に「変化はあまりみられない」会社は全体で合計9.9%にとどまる。あらゆる会社において、サイバー攻撃に対しては明日は我が身という危機感が浸透してきていることがうかがえる。

## 取締役会等におけるサイバーセキュリティの報告や議論の状況




- 全体で最も多い「2．インシデント発生時または必要に応じて報告・議論されるが、個別のシステムトラブル対応等が中心である」会社32.2%と、「1．特段の報告や議論がない」11.5%を合計すると**43.7%**を占める。
- 上述の「経営リスクとして危機感を持つ」会社が88.6%を占めているにもかかわらず、<u>取締役会等での定例報告や経営課題としての議論には必ずしも結びついていないことが表れている。</u>

©公益社団法人日本監査役協会

# 2. サイバーセキュリティに対する監査役等の着眼点の例（抜粋）

監査役等には以下の事項を重点的に確認し、必要に応じて取締役会、経営陣、関係部門に対して改善を促していくことが期待される。
ただし、監査役等がすべてを直接確認することが求められるのではなく、社内の関係部門等への確認などを通して状況を把握することが考えられる。

## (1) サイバーセキュリティが経営課題となっているか

- サイバーセキュリティを重要な経営リスクとして認識
- 取締役会等での定期的な報告・議論
- CISOやリスク管理委員会などからの報告
- 経営トップからの対策の主導・関与

## (2) サイバーセキュリティリスク管理体制の整備・運用状況

- 担当組織や責任者の設置、役割と責任の明確化
- 事業への影響を踏まえたリスク評価
- 重要リスクの経営層への報告、対策計画への反映
- 内部監査、第三者評価、脆弱性診断結果の反映
- 役職員への教育・研修の実施

## (3) 「侵入後」を想定した緊急対応体制の整備

- サイバーインシデントのBCP策定
- 侵入後を想定したインシデント対応訓練の実施
- 訓練結果を踏まえたBCPの見直し
- バックアップ体制や復旧手順の策定
- 社内や監査役等への報告経路の明確化

## (4) グループ会社・サプライチェーンでの対策

- グループ共通のセキュリティ方針・対策の整備
- 重要な子会社、海外拠点のセキュリティ状況の把握
- 取引先・委託先等の範囲、重要性、優先順位の整理
- 取引先・委託先等との契約内容（セキュリティ対策、報告義務、監査権限など）と実態の確認

## (5) 監査計画へのサイバーセキュリティの反映と監査活動

- 執行側のリスク評価は適切か
- 当年度の監査計画への組み込み
- 監査結果の次年度の監査計画への反映
- 内部監査部門との連携、社内の部署との連携
- 社内外の専門家の評価・知見の活用

## (6) インシデント発生時の監査役等の対応

- 重大インシデントの報告基準・経路の運用の確認
- 初動対応体制の確認
- 監査役等への報告は適切か
- 監査役等の初動対応
- 社内外への報告・公表で監査役等が確認すべき事項


©公益社団法人日本監査役協会

# 3. サイバーセキュリティに対するガバナンスと監査役等の着眼点

監査役等は、サイバーセキュリティの経営課題化・リスク管理・緊急対応が機能しているかを確認する

平時

侵入の予防に加え、侵入後への備えが重要に

侵入後

平時における備え
・リスク管理体制構築
・緊急対応体制整備
・サプライチェーンを含めた対策

**サイバーセキュリティ＝経営リスク**

サイバーインシデント発生後の対応

(2) サイバーセキュリティリスク管理体制の構築
・担当組織や責任者の明確化
・リスク評価、対応計画への反映
・脆弱性診断や対策水準の検証
・役職員への教育・研修

(3) BCP策定、訓練・演習、見直しと改善

統制
報告
確認

(1) 取締役会での経営リスクとしての議論

確認

(5) 監査役(会)*の監査
・監査計画への反映
・内部監査部門の監査の報告、連携
・他部署へのアプローチ
・執行側への問題提起、対策等の監督

確認

*監査等委員会、監査委員会も同様

外部専門家

社内での対応
対策本部の設置、調査、分析、復旧、報告、再発防止策など

確認

(6) 監査役等の対応
・遅滞なく報告受領
・会議への出席、監督
・外部機関への対応や公表内容などの確認
・他部署との連携

確認

社外への対応
・警察への通報
・監督官庁・当局対応
・個人情報保護委員会への報告
・個人情報が漏えいした本人への通知　など

構築
統制

(4)-1 グループ会社の管理（国内・海外）
・グループ共通のセキュリティ方針・対策の整備
・セキュリティ状況の把握、報告体制など

(4)-2 サプライチェーンを含めた状況把握と対策
・取引先・委託先等の範囲、重要性などの整理
・契約内容、実態の確認など



©公益社団法人日本監査役協会

## 1. はじめに

近年、国内外でサイバー攻撃が多発しており、大企業だけでなく中小企業、医療機関や教育機関など、様々な規模・業種の企業や組織が標的となっている。特にランサムウェア攻撃により、機密情報や個人情報の窃取にとどまらず、製造ラインの停止、物流やサービスの停止、医療機関の診療停止など、社会やインフラに深刻な影響を及ぼしている。サイバーセキュリティ対策強化に乗り出していた大企業であっても、甚大な被害が発生し復旧に長期を要する事案が発生している。また、外部委託先への依存度が高まる中、サプライチェーンを狙った攻撃も増加している。自社の対策だけではセキュリティの確保は不十分であり、広範なリスク管理が求められている。さらに、近年急速に進化した生成 AI（文章、画像、音声、動画等を生成する人工知能）の利用により、サイバー攻撃が高度化しており、想定を超える巧妙さでセキュリティを突破される事案も発生している。

このように、あらゆる企業・組織においてサイバーセキュリティが重要な経営リスクの一つとなっている中、経営陣だけでなく監査役等（監査役、監査等委員、監査委員および監事をいう。以下同様）にもサイバーセキュリティリスクに対する役割が求められている。サイバーセキュリティは技術的な専門性が高い分野であり、多くの経営陣も監査役等もその専門家ではないであろう。しかし、サイバーセキュリティは企業経営に重大な影響を与えるリスクであるため、経営陣は危機意識を持ってリスクを管理し、対策を主導していく必要があり、監査役等はそれを適切に監視していく必要がある。

そこで、日本監査役協会ケース・スタディ委員会は、監査役等がサイバーセキュリティにどのように向き合い監査しているのか実態を調査し、その状況や事例を広く共有することを目的として、会員企業・組織を対象にアンケート調査を実施した。それをもとに、サイバーセキュリティに対する監査役等の着眼点を取りまとめることとした。

## 2. サイバーセキュリティをめぐる環境の変化と取締役・監査役等の役割

### (1) サイバーセキュリティをめぐる環境の変化

#### ① サイバーセキュリティとは

「サイバーセキュリティ」とは[1]、一般的には、デジタルデータやPC、サーバー、ネットワーク機器などのデジタル情報、情報システムおよび情報通信ネットワークを、不正アクセスやマルウェア、内部不正・過失、不備その他の要因による漏えい、滅失、毀損又は機能停止などから保護する技術的、人的および組織的な取組みを指す。また、「情報セキュリティ」とは、デジタルデータだけでなく紙や口頭の情報も対象とした情報資産全体を守る広い概念であり、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の3要素（CIA）を維持することが求められる[2]。情報セキュリティにはサイバーセキュリティが含まれるが、サイバーセキュリティの重要性は近年ますます増加している。

独立行政法人情報処理推進機構（IPA）が毎年公表している「情報セキュリティ 10 大脅威［組織］」[3]によると、2026年の第1位は「ランサム攻撃による被害」であり、2021年から連続で第1位となっている。第2位は「サプライチェーンや委託先を狙った攻撃」であり、サプライチェーンについては2023年から連続して第2位となっている。また、第3位は「AIの利用をめぐるサイバーリスク」であり、これは2026年に初選出された脅威である。

なお、本報告書では、近年頻発するサイバー攻撃への対応を重視し、「サイバーセキュリティ」を外部からの悪意ある攻撃（特にランサムウェア攻撃）に焦点を絞って検討している。

#### ② サイバーセキュリティをめぐる近年の動向

警察庁によれば、令和8年（2026年）上半期におけるランサムウェアの被害件数は123件であり、統計を取り始めた令和2年下半期以降、半期の件数としては最多となっている[4]。また、令和7年（2025年）の1年間におけるランサムウェアの被害報告件数は226件であ

---

[1] サイバーセキュリティ基本法第2条では、電磁的方式により記録・発信・伝送・受信される情報の漏えい、滅失又は毀損の防止など、情報の安全管理のために必要な措置が講じられること、また情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられること、並びにそれらの状態が適切に維持管理されていることをいう。

[2] 情報マネジメントシステム認定センター「ISMS（情報セキュリティマネジメントシステム）とは」。https://isms.jp/isms/

[3] https://www.ipa.go.jp/security/10threats/10threats2026.html

[4] 警察庁サイバー警察局『令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について』令和8年9月、9頁。なお、サイバー攻撃の準備として、攻撃者は攻撃対象を事前に探索する場合がある。警察庁が設置したセンサーにおいて令和8年上半期に検知した、脆弱性探索行為等の不審なアクセス件数は、1日・1IPアドレス当たり13,687件（前年比50.7%増）と急増しており、その大部分が海外を送信元とするアクセスで占められている（同5頁）。
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

り、高い水準で推移している[5]。被害企業を規模別でみると、前年と同様に中小企業が約6割を占めている（143件）。業種別では、製造業が約4割を占め（91件）、続いて卸売・小売業、サービス業、情報通信業が上位となっているが、様々な業種で被害が確認されている[6]。企業規模を問わず被害が発生しているものの、特に人的・資金的資源が限られる中小企業が被害を受けていることがうかがえる。また、近年はサプライチェーンへのサイバー攻撃の増加も大きな特徴である。取引先（委託先等）を経由して侵入する手法が増加しており、自社自身が被害を受けるだけでなく、取引先（委託先等）が攻撃の足掛かりとして利用されるリスクも高まっている。

さらに、サイバー攻撃による影響は、システム障害や事業停止にとどまらず、情報漏えいによる損害賠償、事業停止による収益機会の喪失、信用失墜や企業価値の低下など、経営に与える影響は極めて大きい。実際に、ランサムウェア被害を受けた企業・組織への調査では、調査・復旧に1か月以上を要した組織が約半数にのぼり、1,000万円以上の費用を要した組織も半数に達しているとの報告がある[7]。

このような状況を踏まえると、サイバーセキュリティはもはや情報システム部門のみの課題ではなく、企業の事業継続と持続的成長を支えるための重要な経営課題として取り組む必要がある。

### (2) 取締役・経営者に求められる役割

#### ① サイバーセキュリティ経営ガイドライン

サイバーセキュリティリスクを経営リスクとして認識して対策していないと、サイバーインシデントが発生した際、事業の中断や情報漏えいへの対応など全社的な経営判断が求められる場合に必要な意思決定が迅速になされず、結果的に被害の拡大を招くおそれが生じる。そのため、取締役はサイバーセキュリティを重要な経営リスクと認識し、サイバーセキュリティリスク管理体制を整備する必要があり、監査役等はそれが適切に構築・運用されているかについて監査していくことになる。

経営者を対象としたサイバーセキュリティ対策のガイドラインである「サイバーセキュリティ経営ガイドライン Ver 3.0」では[8]、「経営者が認識すべき3原則」が示されており、これらを認識して対策を進めることが重要であるとされている。

---

[5] 警察庁サイバー警察局『令和7年におけるサイバー空間をめぐる脅威の情勢等について』令和8年3月、13頁。https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

[6] 脚注5、14頁。

[7] 脚注5、14頁。

[8] 経済産業省および独立行政法人情報処理推進機構（IPA）が策定。2023年3月24日公表。
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

**経営者が認識すべき３原則**

| |
|---|
| (1) 経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要<br>(2) サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要<br>(3) 平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要 |

② サイバーセキュリティ経営の重要 10 項目

前述の「サイバーセキュリティ経営ガイドライン Ver 3.0」では、「サイバーセキュリティ経営の重要 10 項目」も示されている。

**経営者が CISO[9]等に指示すべき 10 の重要事項**（抜粋[10]）

| |
|---|
| **（指示 1）サイバーセキュリティリスクの認識、組織全体での対応方針の策定**<br>・サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針(セキュリティポリシー)を策定させる。これを対外的な宣言として公表させる。 |
| **（指示 2）サイバーセキュリティリスク管理体制の構築**<br>・サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構築させる。その構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。<br>⇒取締役・監査役は、サイバーセキュリティリスク管理体制が適切に構築・運用されているかを監査する。 |
| **（指示 3）サイバーセキュリティ対策のための資源（予算、人材等）確保**<br>・サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討させ、その実施に必要となる資源（予算・人材等）を確保した上で、具体的な対策に取り組ませる。 |
| **（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**<br>・事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。<br>・サイバー保険の活用のほか、リスク対応計画を策定させ、対応後の残留リスクを識別させる。 |
| **（指示 5）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構築**<br>・防御・検知・分析の各機能を実現する仕組みを構築させる。 |

[9] Chief Information Security Officer：最高情報セキュリティ責任者。

[10] 脚注 8『サイバーセキュリティ経営ガイドライン Ver 3.0』参照。抜粋は同ガイドラインをもとに(公社)日本監査役協会ケース・スタディ委員会が作成。

| |
|---|
| **（指示 6）PDCA サイクルによるサイバーセキュリティ対策の継続的改善**<br>・株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。 |
| **（指示 7）インシデント発生時の緊急対応体制の整備**<br>・サプライチェーン全体のインシデントに対応可能な体制（CSIRT 等）を整備させる。 |
| **（指示 8）インシデントによる被害に備えた事業継続・復旧体制の整備**<br>・復旧に向けた手順書策定や、復旧対応体制の整備をさせる。<br>・復旧対応についてサプライチェーンも含めた実践的な演習を実施させる。 |
| **（指示 9）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状況把握及び対策**<br>・国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況の把握を行わせる。<br>・サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。 |
| **（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**<br>・サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。 |

図表の重要 10 項目（指示）は、経営者から CISO 等へ単に指示すればよいのではなく、組織のリスクマネジメントの責任を負う経営者が自らの役割として実施方針の検討、予算や人材の割当て、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが求められる[11]。

③ コーポレートガバナンス・コードと内部統制システム

2026 年改訂コーポレートガバナンス・コード（以下「CGC」という）では、原則４－４の解釈指針において、サイバーセキュリティリスクについて言及されている[12]。

**【原則４－４．取締役会の役割・責務Ⅲ：経営陣・取締役に対する実効的な監督②】**

取締役会は、内部統制や全社的リスク管理体制を適切に整備すべきである。

**解釈指針**

内部統制や先を見越した全社的リスク管理は、適切なコンプライアンスの確保により持続的に信頼を維持し、リスクを最小化するために重要であるのみならず、経営陣が果断にリスクテイクを行うための裏付けとなり得るものであるから、取締役会は、グループ全体を含めたこれらの体制を適切に構築するとともに、内部監査部門を活用しつつ、その運用状況を監督すべきである。サイバーセキュリティリスク、国際的な経済安全保障を巡る環境変化等の地政学的要因によるサプライチェーン途絶リスク及び技術等の情報流出リスクへの対応等も、収益機会にもつながり得るものとして、リスク管理体制を整備する際の考慮事項に含まれ得るとともに、そうしたリスクへの対応等が適切に行われるべきである。

[11] 脚注 8『サイバーセキュリティ経営ガイドライン Ver 3.0』14 頁。

[12] 2026 年 7 月 21 日公表。https://www.jpx.co.jp/corporate/news/news-releases/1020/t13vrt000001jhgb-att/t13vrt000001jhlc.pdf

この解釈指針では、内部統制や全社的リスク管理体制を構築する際には、サイバーセキュリティに関するリスクも考慮する必要があるという考え方が示されている。

会社法上の内部統制システムにおいて[13]、サイバーセキュリティリスクは法令遵守体制、損失危険管理体制、情報保存管理体制等でのテーマとなる。

特に損失危険（リスク）管理体制については、リスク管理体制の大綱を定めさせる趣旨と考えられており、取締役はサイバーセキュリティリスク管理体制を整備する必要がある。また、その一内容としてサイバーセキュリティについての BCP 策定が求められていると考えられる[14]。当協会の「内部統制システムに係る監査の実施基準」においても、損失危険管理体制の監査の着眼点として、「会社に著しい損害を及ぼすおそれのある事故その他の事象が現に発生した場合に、適切な対応体制が構築・運用されていない結果、損害が拡大しあるいは事業が継続できなくなるリスク」を列挙している（第 10 条 1 項 3 号）。したがって、BCP やその他の対応計画が未整備であり、かつ、重大なインシデント発生時に重要事業を継続できない状態になった場合には、内部統制システムの不備と評価される可能性がある。

#### ④ サプライチェーンのリスクと対策

サプライチェーンを狙ったサイバー攻撃が増加している中、取引先（委託先等）にサイバーセキュリティ対策が講じられていないと、これらの企業が被害を受けた場合、自社にも事業停止などの被害が発生したり、個人情報の流出などの責任を問われる。そのため、サプライチェーン全体でサイバーセキュリティの実効性を向上する必要があるが、複数の会社が関係する上、外部からは状況が見えないため、対策は難しくなる。具体的な対策として、例えば契約書においてサイバーセキュリティ対策の責任主体を明確化する、サプライチェーン内で扱う情報の機密性や重要性のランク別に実施すべき対策を定め、過剰な対策や対策の形骸化が生じないようにする、サプライチェーン内でのサイバーセキュリティリスクに関する情報共有等を行う、などが考えられる[15]。

また、経済産業省および内閣官房国家サイバー統括室では、2026 年 3 月に「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）」の制度構築方針を公表した[16]。この制度は、サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、その状況を可視化する仕組みである。具体的には、2 社間の取引契約等において、発注企業が、受注側にセキュリティ対策の適切な段階を“★”印をつけたレベルで提示し、示された対策を促すとともに実施状況を確認することを想定している。

---

[13] 会社法第 348 条 3 項 4 号、同第 362 条 4 項 6 号、会社法施行規則第 100 条。

[14] 蔦大輔 編著・森・濱田松本法律事務所外国法共同事業サイバーセキュリティ法研究チーム著『クロスセクター・サイバーセキュリティ法』2025 年、339 頁。

[15] 脚注 8『サイバーセキュリティ経営ガイドライン Ver 3.0』29-30 頁。

[16] 2026 年 3 月 27 日に制度構築方針を公表。2026 年度末頃に制度開始予定。
https://www.meti.go.jp/policy/netsecurity/scs.html

### (3) 監査役等に求められる役割

#### ① サイバーセキュリティに対する取締役・監査役等の法的責任

会社法上、取締役は善良な管理者としての注意義務（善管注意義務）および忠実義務を負っている[17]。また、大会社等においては、業務の適正を確保するための体制（いわゆる内部統制システム）の整備に関する責務も負っている。このため、サイバーセキュリティリスクが企業活動に重大な影響を及ぼし得る状況においては、そのリスクを適切に把握し、必要な管理体制や対応方針を整備・運用することも、取締役の責務の一環として位置付けられると考えられる。

もっとも、サイバー攻撃は日々高度化・巧妙化しており、必要な対策を講じていた企業であっても被害を受ける事例は既に発生している。したがって、サイバーインシデントが発生したという結果のみをもって直ちに取締役の責任が問われるものではなく、当該企業の事業内容やリスクの特性に応じて、合理的な体制整備や監督を行っていたかが重要である。

一方、監査役等は、取締役の職務執行を監査する立場であるから、サイバーセキュリティ対策そのものを実施する責任を負うものではない。しかしながら、サイバーセキュリティが重要な経営リスクであることを踏まえ、取締役会等において適切な議論が行われているか、必要な体制整備が進められているかを監視し、必要に応じて意見を述べることが期待される。サイバーセキュリティに関する法的責任は、個々のサイバー攻撃の発生そのものではなく、平時からのリスク認識、体制整備および監督の適切性が問われる点に特徴がある。したがって、取締役および監査役等においては、サイバーセキュリティを企業価値の維持に関わる経営課題として捉えることが重要である。

#### ② 監査役等の監査の視点

サイバーセキュリティについて監査役等に求められる役割は、セキュリティ対策に関する個別技術の妥当性を判断することではなく、サイバーセキュリティが経営上の重要リスクとして認識され、適切に対応されているかという、ガバナンス、リスク管理および内部統制の観点からの監査である。前述の「内部統制システムに係る監査の実施基準」第 10 条 1 項 3 号から、監査役等は、サイバーセキュリティリスクが経営リスクであることを取締役が十分に認識しているか、取締役会等においてリスク分析を踏まえた慎重な議論を行い、リスク対応計画とその定期的なレビューが行われているかどうかを監視し検証していく必要がある[18]。具体的には、取締役会等においてサイバーセキュリティが経営課題として十分に議論されているか、当該リスクに対する体制・方針・資源配分が中長期戦略との関係で合理的に決定されているか、またサイバーセキュリティリスク管理体制が適切に構築・運用されているか、インシデント発生時を含め意思決定と情報連携が有効に機能する体制になってい

---

[17] 会社法第 330 条、同第 355 条、民法第 644 条、会社法第 423 条。

[18] 社団法人日本監査役協会『監査役に期待される IT ガバナンスの実践』2011 年 8 月 25 日、32 頁。

るかなどが重要な視点として挙げられる。

監査役等が個々の対策の技術的側面について判断するものではないが、報告等の形式的な確認にとどまらない実質的な問いかけをしていくことが求められる。

なお、監査役等が全ての着眼点について直接確認することが求められるのではない。CISOなどの責任者や、情報セキュリティ部門、サイバーセキュリティの専門組織への確認、内部監査部門等との連携などを通して、適切に状況を把握していくことが有効である。

### ③ 高まる有事対応の重要性

従来、企業のサイバーセキュリティ対策は、ファイアウォールの設置、ウイルス対策ソフトの導入、アクセス権限管理など、サイバー攻撃の侵入を防ぐための「予防的対策」に重点が置かれていた。もちろん、こうした取組みは現在でも重要であり、その継続的な強化が求められる。しかしながら、近年のサイバー攻撃は急速に高度化・巧妙化しており、必要な対策を講じていたとしても、攻撃を完全に防ぐことは困難になりつつある。このため、近年は「侵入させないこと」だけではなく、「侵入される可能性を前提とし、被害を最小化すること」に重点を置く考え方が主流となっている。すなわち、平時における予防的対策とともに、インシデント発生時の対応体制や事業継続体制を整備し、迅速な意思決定と早期の復旧を可能とすることが重要になっている。

有事対応においては、初動対応の成否が被害の規模や企業価値への影響を大きく左右する。インシデントを速やかに検知し、経営陣への報告、被害範囲の特定、関係当局や取引先（委託先等）への連絡、外部専門家との連携、広報対応などを迅速に実施できる体制が求められる。また、システム停止や情報漏えいが発生した場合にも、重要業務を継続または早期に復旧できるよう、BCP の整備やバックアップの確保、定期的な訓練の実施も重要となる。

監査役等においても、「有事を想定した準備がどこまで整備されているか」という視点がますます重要になっている。特に、インシデント発生時の報告ルートは明確か、そのルートに監査役等も含まれているか、経営陣は迅速な意思決定を行えるか、外部専門家との連携体制は確保されているか、適切な訓練が実施されているか、そこで発見された課題は改善されているかといった点は、監査上の重要な視点になると考えられる。

## 3. アンケート調査結果からみえるサイバーセキュリティ対策の現状

### (1) アンケート調査の質問構成の趣旨と実施概要

本アンケートは、サイバーセキュリティ経営ガイドラインを参考に、経営者が対応すべき事項、監査役等が監視・関与する局面を抽出して質問を構成した。サイバーセキュリティが経営上の重要リスクであることの認識が出発点となるため、以下の順で質問した。

(1) 取締役会等での報告・議論の状況（Q1、Q3)、経営陣の意識の変化（Q2)、監査役等の意見陳述（Q4）
(2) サイバーセキュリティリスク管理体制の構築状況
　責任者（Q5)、専門組織（Q6)、リスク評価（Q9-1)、セキュリティ対策の全体像（Q10-1)、グループ会社における管理（Q11）など
(3) サイバーインシデント発生時の緊急対応体制、BCP 策定・運用状況等（Q12～Q15）
(4) サプライチェーン全体でのセキュリティ対策（Q16）
(5) 監査役等の監査活動（Q17～Q21）
(6) 実際にサイバー攻撃を受けたことがある会社の有事対応（Q22～Q30）

また、監査役等が現在の自社の状況をどのように評価しているか、そして自社の水準が他社と比較してどのような状況にあるかを可視化するため、原則として各質問の選択肢を段階別（レベル別）に設計した。選択肢 1 を基礎的な段階・最低限の対策のレベルとし、選択肢 5 に向かって段階的に高度化・ハイレベルな段階となるように内容を設計している[19]。あわせて、監査役がどのような手段で自社の状況を確認しているか（確認の方法・内容）についても、段階別の選択肢を設計した。

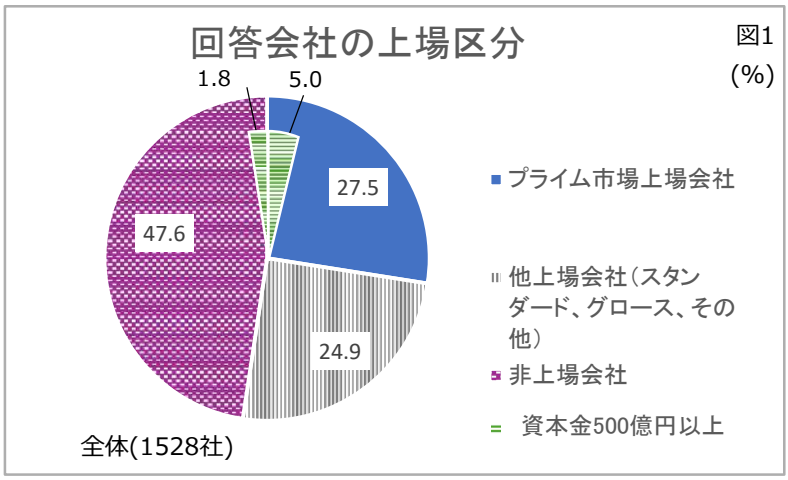
さらに、監査役等の活動状況として、サイバーセキュリティを監査計画に取り入れているか、サイバーセキュリティへのアプローチの方法、監査役会等（監査役会、監査等委員会、監査委員会をいう。以下同様）での議論、参考にしているガイドラインなどについても質問した。

このような構成をもとに、以下のとおりアンケート調査を実施した。

・調査名「サイバーセキュリティと監査役等の対応についてのアンケート調査」
・調査期間　2026 年 5 月下旬から 6 月上旬
・調査対象　当協会の法人会員 7,775 社
・総回答社数　1,528 社（回答率 19.7%）

[19] 本アンケートの段階別選択肢は、回答会社の状況を比較・整理するためにケース・スタディ委員会が独自に設計したものであり、第三者機関による認証などに基づくものではない。また、本アンケートの結果は、回答者である監査役等の認識に基づくため、実際の回答会社の整備・運用状況とは異なる可能性がある。

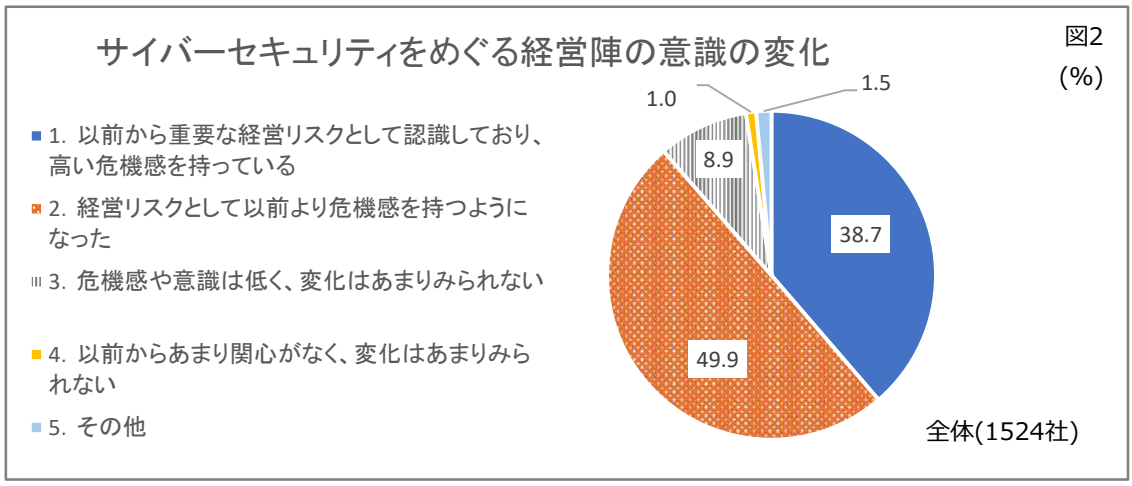
回答会社の上場区分は、上場会社 52.4%、非上場会社 47.6%であり、上場会社の内訳は図 1 のとおりである。また、回答会社を資本金区分でみると、最も多い層は 1 億円以上 5 億円未満の会社で 21.0%、 1 億円未満の会社は 14.3%である。非上場会社では 55.8%が資本金 5 億円未満の会社である。なお、資本金 500 億円以上の会社（104 社）のうち、プライム市場上場会社は 76 社（73.1%・全体では 5.0%）、非上場会社は 28 社（26.9%・全体では 1.8%）である。




アンケート結果の数値表では、回答会社全体の結果を「全体」と表示し、プライム市場上場会社の回答を「プライム市場」、プライム市場上場会社を除いた上場会社の回答を「他上場」、非上場会社の回答を「非上場」と表示している。また、資本金 500 億円以上の会社の回答は先進的な取組みがみられるため、「資本金 500 億～」と表示して紹介している。

### (2) サイバーセキュリティをめぐる経営陣や取締役会等の現状

#### ① 直近 1 年間における経営陣の意識の変化（Q2、図 2）

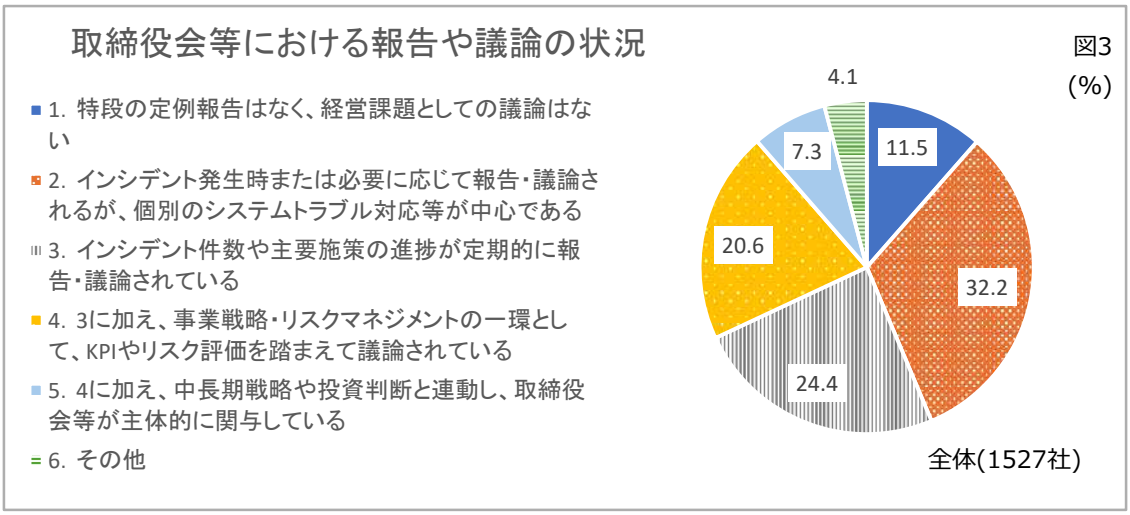



全体では「2. 経営リスクとして以前より危機感を持つようになった」が約半数を占めており、また選択肢 1 の「以前から高い危機感を持っている」と合計すると 88.6%に達する。監査役等の認識によれば、サイバーセキュリティに対して経営陣が高い危機感を持っている会社が大多数といえよう。また、資本金区分が大きくなるほど選択肢 1 の割合が増加する傾向にあり、資本金 500 億円以上の会社では選択肢 1 が 63.1%にのぼっている。

他方、選択肢 3 および 4 の経営陣の意識に「変化はあまりみられない」は全体で合計 9.9%にとどまっており、どの会社区分でも割合は低くなっている。あらゆる会社において、サイバー攻撃に対しては明日は我が身という危機感が浸透してきていることがうかがえる。

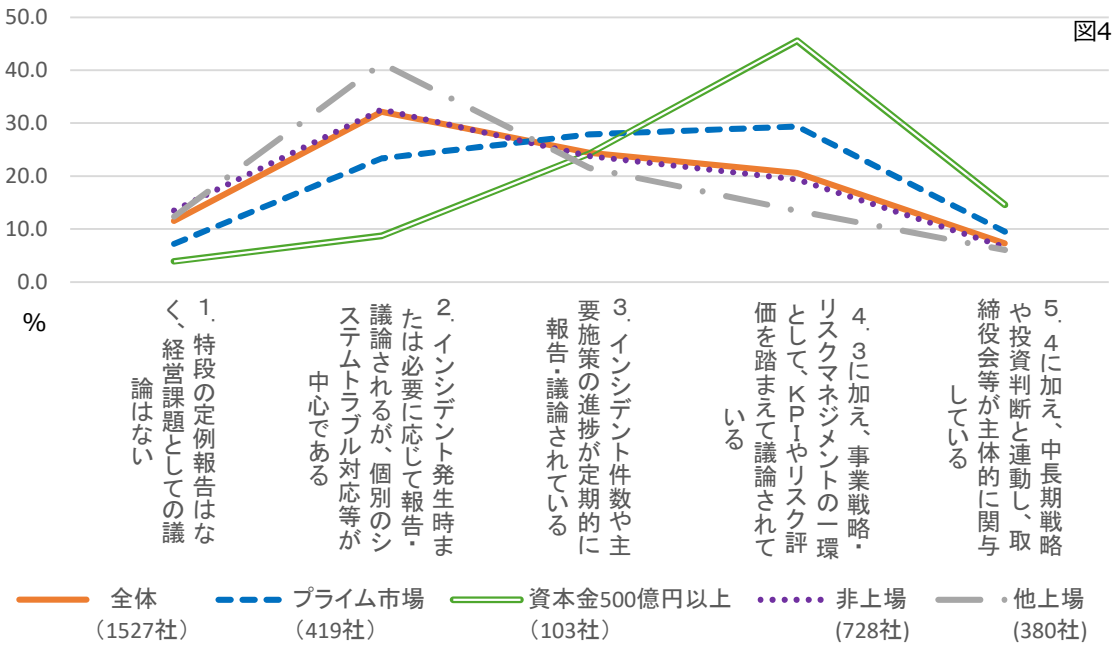
#### ② 取締役会等における報告や議論の状況（Q1、図 3・4）

取締役会等（経営会議等も含む。以下同様）におけるサイバーセキュリティに関する報告や議論の状況について質問した。



| Q1. 取締役会でのサイバーセキュリティの報告・議論の状況 （%、1 つ選択） | 全体 | プライム市場 | 資本金500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 特段の定例報告はなく、経営課題としての議論はない | 11.5 | 7.2 | 3.9 | 13.5 | 12.4 |
| 2. インシデント発生時または必要に応じて報告・議論されるが、個別のシステムトラブル対応等が中心である | 32.2 | 23.4 | 8.7 | 32.6 | 41.3 |
| 3. インシデント件数や主要施策の進捗が定期的に報告・議論されている | 24.4 | 27.9 | 24.3 | 23.8 | 21.6 |
| 4. 3 に加え、事業戦略・リスクマネジメントの一環として、KPI やリスク評価を踏まえて議論されている | 20.6 | 29.4 | 45.6 | 19.4 | 13.4 |
| 5. 4 に加え、中長期戦略や投資判断と連動し、取締役会等が主体的に関与している | 7.3 | 9.5 | 14.6 | 6.6 | 6.1 |
| 6. その他 | 4.1 | 2.6 | 2.9 | 4.3 | 5.3 |
| （回答社数） | 1,527 | 419 | 103 | 728 | 380 |

図4




全体で最も多いのは「2. インシデント発生時または必要に応じて報告・議論されるが、個別のシステムトラブル対応等が中心である」32.2%であり、これは「他上場」会社で 41.3%を占めていることが影響している。また、選択肢 1 の「特段の報告や議論がない」会社と合計すると、全体で 43.7%、他上場会社では 53.7%を占めている。前述 Q2 で経営リスクとして危機感を持つ会社が全体で 88.6%を占めているにもかかわらず、取締役会等での定例報告や経営課題としての議論には必ずしも結びついていないことが表れている。

他方、プライム市場上場会社では、「3. インシデント件数や主要施策の進捗が定期的に報告・議論されている」が 27.9%であり、さらに「4.3 に加え、事業戦略・リスクマネジメントの一環として、KPI やリスク評価を踏まえて議論されている」が最も多く 29.4%となった。特に資本金 500 億円以上の会社では、選択肢 4 が 45.6%にのぼり、選択肢 5 と合わせると 60.2%の会社で経営課題として定着していることがうかがえる。

**③ 直近 1 年間における議論の進展と実行された施策**（Q3、記述回答）

**ガバナンス面**では、情報セキュリティ委員会等の設置のほか、取締役会や経営会議、各種委員会でのセキュリティに関する報告・議論、CISO 等が取締役会で直接報告するなどの回答が比較的多くみられた。また**内部統制システム面**では、情報セキュリティ管理規程などの整備・改訂が挙がった。

**技術的対策**としては、VPN の脆弱性への対応、EDR/SOC 導入、CSIRT の設置、ゼロトラストへの移行、ペネトレーションテスト、脆弱性診断などが挙げられた。

**訓練・教育面**では、経営幹部向けの教育、全従業員向けの教育・研修、標的型メール訓練が多数あったほか、実際に侵入を許したケースを想定したインシデント対応訓練の実施などもみられた。

**BCP・復旧面**では、バックアップシステム強化、BCP へのサイバー攻撃項目追加、システム停止時の復旧手順確認が挙げられた。攻撃への備えから、攻撃発生後の被害最小化・早期復旧に重点を移しているという意見も多かった。また保険[20]への加入・増額も見られた。

さらに、**大規模な会社**や**親会社**では、グローバル・グループ横断的な管理、サプライチェーンを含む外部リスク管理への対応も検討されていた。他方、**子会社**では、「サイバーセキュリティに関しては親会社が統一的な施策を行っており、子会社独自の動きはない。」という傾向であった。「親子一体での対策訓練の実施、子会社役職員向けのサイバーセキュリティ研修会が実施されている。」という会社もある一方、親会社のセキュリティ対策が不十分と思われる場合には、「子会社の立場では親会社に注意を喚起するところまでが精一杯である。」という意見もあった。

なお、取締役会ではサイバーセキュリティについて議論はしていないという回答も一定数存在した。具体的には、「取締役会での議論ではなく、担当部署の施策として対策が進んでいる。」「取締役会には具体的に付議されていないが、他社事案により危機感は強く持つよう

---

[20] サイバー保険は一般的に、インシデント発生時の事故対応費用、第三者に対する損害賠償費用、事業停止に伴う利益損害や営業継続費用等を補償対象としている。サイバー保険の加入率は近年上昇傾向にあるものの、日本損害保険協会の調査によれば、中小企業における加入率は 8.8%にとどまっている（一般社団法人日本損害保険協会『中小企業におけるリスク意識・対策実態調査 2025 調査結果報告書』2025 年 12 月、36 頁）。https://www.sonpo.or.jp/sme_insurance/assets/pdf/survey/sme_report2025.pdf
他方、上場会社や大企業の方が加入率は比較的高く、サイバーセキュリティを経営リスクとして認識した上で、リスク移転の手段として活用する動きもみられる。

になった。」「他社のサイバー攻撃事例を受け、一時的にサイバー攻撃に対する対策等を議論するかに思えたが、その後議論が進んでいない。サイバーセキュリティ対策を重要課題として認識し、早急に全社的な議論が必要と考えている。」といった回答があった。

以下では、テーマのカテゴリー別に記述回答の抜粋を紹介する。回答例にあるように、CISO が取締役会へ直接報告する体制や、重大インシデントを契機に取締役会が主体的に監督を行った例は、サイバーセキュリティが経営課題として扱われているかを見極める手がかりとなるだろう。また、監査役・監査等委員の問題提起がリスク評価やペネトレーションテストの実施につながった例、報告・意思決定ルートの不備を教訓として体制整備を進めた例などは、監査役等の能動的な関与が対策を前進させ得ることを示している。

**ガバナンスの回答例（Q3）**

○サイバーセキュリティ対策を主眼においた全社の情報セキュリティ強化を目的に、経営戦略と連動した情報セキュリティ委員会を新設することを決定し運用を開始した。

○SOC・CSIRT を含むトータルセキュリティ体制の構築について、これまで情報システム部門を中心に準備を進めてきたが、本年にサイバーセキュリティ委員会を設置し、全社レベルでの取組みとした。

○リスク管理部門からの定期報告に加えて、常務執行役員である CISO が社内の具体的なサイバーセキュリティ対策等について、直接取締役会に報告し、議論を行うようになった。

○ISMS の認証を 1 年半前から議論し始め、半年前に取得した。経営管理部内に IT 専門部署を立ち上げ、人員の充実を図っている。

○グループ横断的なサイバーセキュリティ対策部署を設置。海外は更に対策チームを強化して対応。

○昨年サイバーセキュリティ上の重大インシデントが発生し、初動から原因究明、再発防止策、フォローアップに渡り、取締役会が主体的に監督を行った結果、セキュリティレベルは大幅に改善された。

○子会社がサイバー攻撃を受けて以来、執行側の温度感はかなり上がり、具体的な対策を講じるようになっている。取締役会でリスクマネジメント管掌役員、テクノロジー管掌役員より現状のリスク認識と対策の方向性について報告しており、取締役会としての認識は上がっている。

○子会社のため、親会社の設定したシステムを使う限りは親会社責任でサイバーセキュリティを担保してもらっているが、独自システムを使っている自らの子会社については、あらためてリスク評価を行うことを監査役から問題提起し、取締役会でその方向が提案された。

**内部統制システムの回答例（Q3）**

○IT セキュリティに関するガバナンスの強化のため、グローバル情報セキュリティポリシーの改定を決議。世界各拠点の子会社の責任者の責任と親会社の権限を明確にした。

○「金融分野におけるサイバーセキュリティに関するガイドライン」への取組みを議論し、セキュリティポリシーとセキュリティスタンダードの改正、情報セキュリティ管理規程、サイバーセキュリティ管理規程、AI 管理規程の制定が実行された。

○グループ会社に対する内部統制プロセスの追加・変更の検討。サイバーセキュリティ管理を主要統制の柱に加える内部統制基本方針の改定。

○昨年度、統合的リスク管理部署とシステム部門にて、金融庁のサイバーセキュリティガイドラインに基づきフィット＆ギャップを実施、課題整理を行い中期的なロードマップを策定。その進捗状況はリスク管理委員会で管理していく。またグループ全体としてのサイバーセキュリティリスク管理体制構築に向け、規定体系の再整備と人材育成、リテラシー向上に係る施策をスタート。技術的な施策を含め、各施策の進捗、実施状況を内部監査部門がモニタリングする。

**技術的対策、訓練の回答例（Q3）**

○情報セキュリティに関する脆弱性診断を実施。

○VPN の脆弱性をクリアするためにゼロトラストに移行する。

○監査等委員が問題提起したことを契機に、遅まきながらペネトレーションテストを実施することが取締役会で決まり、その結果も取締役会で報告された。

○自社のクリティカル・ビジネスを特定し、同ビジネスの依存度・インパクト評価・脆弱性シナリオ分析に基づくレジリエンステストを実施した。

○今年度新たに外部コンサルティング会社と契約を結び、現下におけるサイバーセキュリティ対策のブラッシュアップのために、諸施策のアドバイスを受けることを開始した。

○攻撃メール訓練で昨年度より開封者が増加したため、対応について意見交換した。

○部長以上の経営幹部を対象としたセキュリティ教育を実施したほか、インシデント対応訓練を予定。

○従業員全員を対象に、社内イントラを用いた情報セキュリティ教育を定期的に実施。

○社内システムをゼロトラストネットワークに変更する際、新たなセキュリティ対策について CISO および主管部を中心に対策の立案から実効性の評価、移行方法についても議論し、十分な移行期間を設けつつ完遂してきた。今後はそのセキュリティ対策の有効性を評価していく予定であり、注視していきたい。

○ミュトス対応について、短期的対応（脆弱性、バックアップ管理等）に関しては、「基本の徹底＋スピード」を周知徹底すること、中期的対応に関しては、「攻撃を受けることを前提」として、システム防御策を構築することを対応方針とした。

**BCP・復旧の回答例（Q3）**

○昨年度に攻撃を受けた際、攻撃の事実、攻撃範囲、被害の程度などを速やかに把握し、エスカレーションするまでの手続きに不備があることが判明したため、報告・意思決定ルートの整備と、実際にシステムがダウンした場合の BCP の検討を開始した。

○インシデントを完璧に防ぐという考えから、起きてしまった際の被害を極小化するという思考に変化しており、この考えに基づく手順書整備に取り組み始めている。

○従来は、インシデント発生時のシステムの復旧計画に注力していたが、システムが復旧するまでに手作業での業務対応が必要なことが分かり、手作業での業務手順等の整備と訓練を行うようになった。

○IT 賠償保険の保険内容を見直し、調査や復旧にかかる事故対応費用の賠償金額を増額した。

**サプライチェーンの回答例（Q3）**

○「サプライチェーン強化に向けたセキュリティ対策評価制度」に照らして自社のポジションを確認し、不足項目を確認し、順次対策を実施する計画を立て、26 年 4 月から対応している。

○3 年ほど前に取引先より情報セキュリティシステムの評価を受けたところ、非常に低い評価であり改善を促された。まずは取引先からの評価を改善することを目指し、改善が図れたあとは、積極的にサイバーセキュリティへの投資を行っている。具体的には、中期計画に織り込み、機器の管理、ネットワークの改修、教育・研修の回数の見直し、CSIRT 組成のための社内ルール整備などを進めている。

**④ 監査役等がサイバーセキュリティについて述べた意見の内容**（Q4）

全体として監査役等が「意見を述べたことはない」割合は 21.6%にとどまり、約 8 割の監査役等は、取締役会や経営会議等において、あるいは直接経営陣に対して、サイバーセキュリティについて意見を述べ、既に一定の関与を始めている。以下ではその意見の内容や、それに関連する監査役等の対応について、記述回答から抜粋して紹介する。

回答例にあるように、セキュリティ投資を収益状況にかかわらず先送りしないよう求めた例、サイバーセキュリティをリスクマップの重要項目に位置付けるよう提言した例、CSIRT[21]の組織化や BCP 策定、侵入後の初動対応の必要性を提起した例[22]などは、いずれも

[21] シーサート（CSIRT：Computer Security Incident Response Team）とは、コンピュータセキュリティにかかるインシデントに対処するための組織の総称である。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う。（一般社団法人日本シーサート協議会 HP より。https://www.nca.gr.jp/outline/about.html）

なお、xSIRT とは、CSIRT と同様の組織であるが対象がより広範となる。例えば PSIRT（Product Security Incident Response Team）であれば、自社製品の安全性を確保するため、製品の脆弱性管理やインシデント対応を専門に行う組織をいう。

[22] ランサムウェア攻撃によって暗号化されたデータを復号するための対価と称して、ランサムウェア攻撃グループから要求される金銭等（身代金）の支払いについては、経済産業省は「金銭の支払いは厳に慎むべきものである。」「金銭の支払いに対する対応は、複数の視点から自社への信頼をどのように維持するか、また、犯罪助長行為として支払い行為に対する制裁を用意する国もある中でコンプライアンス上の問題に

報告を受けるにとどまらない能動的な関与といえ、監査役等が意見を述べる際の切り口として参考になる。

**サイバーセキュリティリスク管理体制、セキュリティ対策の回答例（Q4）**

○セキュリティ高度化ロードマップの作成について提言。

○CSIRT の組織化の必要性について意見を述べた。

○外部コンサルタントによるリスク評価の実施を勧奨。

○模擬フィッシングメール等による従業員訓練の実施を勧奨。

○各種規程類（管理規程、管理要領）についての役員間事前協議の席で、規程文言、規程相互間の整合性、関連規程全体の構成上の不備などについて意見を述べた。

○取締役会の下部組織であるリスク管理委員会でサイバーセキュリティの脅威、対策の重要性を訴えた。リスク管理委員会での定例報告、特にランサムウェア対策の予算化において進捗が見られた。

**経営問題、ガバナンスの回答例（Q4）**

○他社事案を踏まえ、現状の当社のサイバーセキュリティの状況を取締役会で報告いただきたい旨を担当役員にリクエストした。

○コストカットによるリスク向上、犠牲を強いるのではなく一定の予算を確保する必要性を説いている。

○セキュリティ確保のための投資は、償却費負担増により営業利益が確保できない状況であっても先送りすべきでない。投資計画に加え、リテラシー教育を並行して実施すべきである。進捗状況を監査部にてモニタリングして取締役会に報告すべきである。

○監査等委員としても問題意識を持ち、執行側の担当部局とともに状況把握のアンケートを実施したので、その結果について、執行役員会で整備を急ぐべきだという意見を述べた。

○監査役の業務監査からサイバーセキュリティ対策のギャップ分析が必要と考え、親会社と連携した内部監査部門の監査により課題出しと対策について提言を出して前進することになった。

○監査役会ならびにグループ監査役連絡会において、情報セキュリティに関する監査役監査を実施する前提として、グループ全体の情報セキュリティポリシーに基づく運用の定着が図れ次第実施できるように、現時点で準備ならびに協議している。

○全社でセキュリティ対策評価制度の対応をすべきことのほか、システムの安定稼働、適切な障害対応、情報セキュリティの確保、将来課題に対応するため、IT 戦略の企画推進ができる人材の育成、確保が必要である旨、社長に報告している。

---

どう対応するか、ということであり、経営者が判断すべき経営問題そのものであるということを強く認識する必要がある。」と説明している。（経済産業省『最近のサイバー攻撃の状況を踏まえた経営者への注意喚起』2020 年 12 月 18 日、7 頁）。
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/001_07_00.pdf

**サイバーインシデントへの備えと発生後の対応の回答例（Q４）**

○サイバーインシデント発生によりすべてのシステムがダウンした場合のための BCP 策定の必要性について意見した。

○インシデント発生時は初動の迅速性と説明の透明性が、企業への信頼を左右する重要な要素であるとコメントした。

○いわゆる身代金の請求があった場合など、セキュリティを突破された場合の初動対応は訓練すべきとの提言を行った。

○インシデント発生直後から担当役員を呼んで状況を確認の上意見交換を行っている。初動から原因究明、再発防止策、フォローアップに至るまで、経営陣並びに取締役に対して意見を述べ、適切性・妥当性を監視した。

○経営陣を含む主要メンバーが参加してのセキュリティインシデント発生を想定した訓練を実施。従来、インシデント発生寸前で止まる想定にしていたが、今回は実際に侵入を許したケースを想定した。経営陣以下で実際に起こっていたことを考えると、さらに事前に検討しておくべき事項が多数あるという貴重な気付きが得られ、次の訓練の計画がシステムリスク部門で進められるに至っている。上記の訓練実施後に、検討課題と思われた事項を参加メンバーが回答するアンケートが実施され、そこにおいて監査役も意見や要望を述べている。

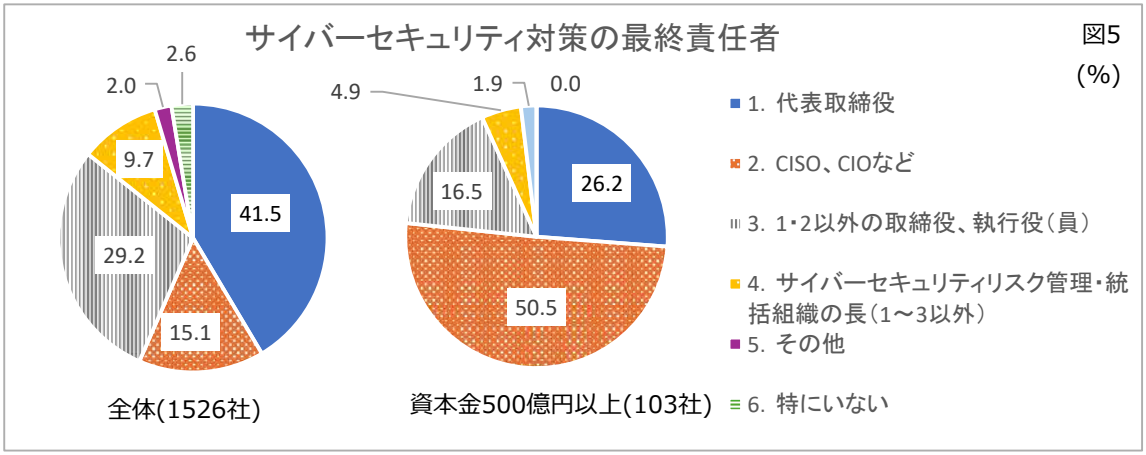
なお、サイバーインシデントの BCP の策定や訓練の実施については、「(4) サイバーインシデント発生時の緊急対応体制」（29 頁以降）において、また実際のサイバーインシデント発生後の対応については、「(8) サイバーインシデント発生後の対応」（47 頁以降）において詳述している。

### (3) サイバーセキュリティリスク管理体制

#### ① サイバーセキュリティ対策の最終責任者（Q5、図 5）

| Q5. サイバーセキュリティ対策の最終責任者（%、1 つ選択） | 全体 | プライム市場 | 資本金 500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 代表取締役 | 41.5 | 34.9 | 26.2 | 43.5 | 45.0 |
| 2. CISO、CIO[23]など | 15.1 | 22.2 | 50.5 | 14.8 | 7.6 |
| 3. 1・2 以外の取締役、執行役（員） | 29.2 | 32.1 | 16.5 | 26.4 | 31.3 |
| 4. サイバーセキュリティリスク管理・統括組織の長（1～3 以外） | 9.7 | 7.7 | 4.9 | 9.9 | 11.6 |
| 5. その他 | 2.0 | 1.9 | 1.9 | 2.5 | 1.1 |
| 6. 特にいない | 2.6 | 1.2 | 0.0 | 2.9 | 3.4 |
| （回答社数） | 1,526 | 418 | 103 | 728 | 380 |

[23] Chief Information Officer：最高情報責任者。CISO は脚注 9 参照。




全体では、「1. 代表取締役」41.5%と「3. 代表取締役・CISO 等以外の取締役・執行役(員)」29.2%が多く、どの会社区分でも同様の傾向である。ただし、資本金 500 億円以上の会社では「2. CISO、CIO など」が 50.5%を占めている。大規模な会社では CISO、CIO への特化が進む一方、中堅・中小規模会社では代表取締役や他の取締役等が兼務している構図が中心となっている。しかし、専任の体制がないことが直ちに問題となるわけではなく、重要なことは、最終的な責任者が明確に定められ、その責任者に必要な情報と権限が集約されているかである。特に中小規模会社においては、まずこの責任の所在と報告経路を明確にすることが、実効的な第一歩となると考えられる。

② サイバーセキュリティリスクを管理・統括している組織の設置状況（Q6）

| Q6. サイバーセキュリティリスク管理組織の設置状況 （%、複数選択可） | 全体 | プライム市場 | 資本金500億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. サイバーセキュリティリスク管理の専門組織はない | 9.6 | 3.8 | 0.0 | 12.3 | 11.1 |
| 2. 専門組織はないが部分的にある、または他の部門が兼務している | 44.1 | 37.0 | 19.2 | 43.1 | 53.9 |
| 3. サイバーセキュリティリスク管理の専門組織を設けている | 20.1 | 28.2 | 44.2 | 19.0 | 13.2 |
| 4. 全社的リスク管理組織の中にサイバーセキュリティも組み込まれている | 29.5 | 36.5 | 47.1 | 26.2 | 28.2 |
| 5. サイバーセキュリティリスク管理の専門組織がグループ全体(および委託先も含めた広範囲)のリスク管理・統括を行っている | 13.3 | 20.0 | 37.5 | 12.4 | 7.6 |
| 6. サイバーインシデントに対応可能な専門チーム(CSIRT など)を設けている | 14.2 | 26.0 | 51.9 | 11.8 | 5.5 |
| 7. その他 | 5.4 | 4.1 | 3.8 | 5.9 | 5.8 |
| （回答社数） | 1,525 | 419 | 104 | 726 | 380 |

全体では「2. 専門組織はないが部分的にある、または他の部門が兼務している」が最も多いが、これは特に「他上場」の会社で高い割合を占めていることが影響している。

選択肢 1 は全て単独回答であり、他の選択肢と組み合わせた回答はなかった。

プライム市場上場会社では、「4. 全社的リスク管理組織の中にサイバーセキュリティも組み込まれている」36.5%が選択肢 2（37.0%）と拮抗している。

また、「6. サイバーインシデントに対応可能な専門チーム（CSIRT など）を設けている」会社は、プライム市場上場会社では 26.0%と全体（14.2%）より高く、資本金額が大きいほど設置率は高い。特に資本金 500 億円以上の会社では 51.9%にのぼっている。この資本金 500 億円以上の会社では、選択肢 3 から 6 までをすべて選択した回答者が最も多い。CSIRT 等の専門チーム保有は単独の施策ではなく、「3. 専門組織」、「4. 全社的リスク管理体制」、「5. グループ統括機能」とセットで導入されている傾向が強い。

なお、「7. その他」の記述回答としては、親会社が管理しているケース、情報システム部門等が管理しているケースが多く見られた。また少数ながら外部委託のケースもあった。

サイバーセキュリティ管理組織への監査役等の確認事項の例を以下に紹介する。回答例にあるように、情報システム部門等へのヒアリング、資料の閲覧を通じたモニタリング、リスク管理委員会等への常勤監査役等の陪席など、報告を受け取るだけでなく会議体や現場を通じて実態を把握する工夫がみられる。

**サイバーセキュリティ管理組織への確認事項の回答例（Q6）**

○情報システム管理部門が広くセキュリティリスクへの対応も行っており、監査役はリスク管理の状況について情報システム管理部門にヒアリングを行っている。

○情報セキュリティの実務と統制は IT マネジメント委員会が主導しており、監査等委員は提出資料の閲覧等を通じてその運用状況をモニタリングしている。また、インシデント発生時はリスク対応する委員会へ情報が一元化される体制となっており、常勤監査等委員も同委員会のメンバーとして対応方針の確認等に関与している。

○IT 部門内にサイバーセキュリティリスク管理部署があり、また全社リスク管理部門が、サイバーセキュリティについてもモニタリングする体制になっている。インタビューなどを通じて個別に状況を確認できる機会があり、常勤監査等委員が陪席するリスク管理委員会を通じた状況把握も行っている。

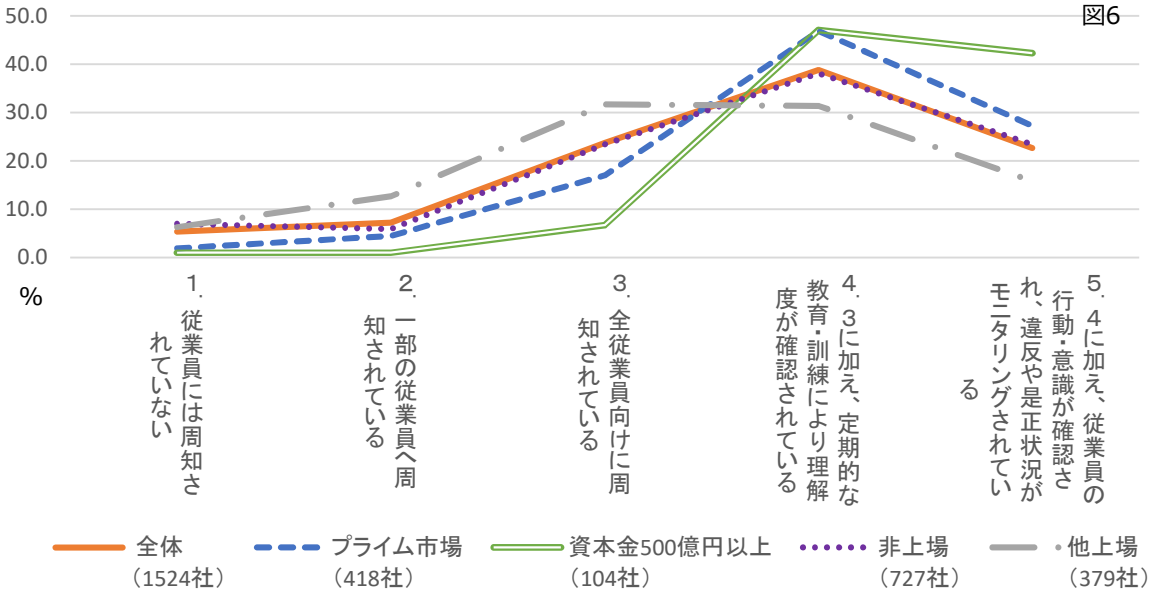
○グループ本社に行った際には、セキュリティ統括部と必ず情報交換を行っている。

○システム系はグループ運用のため、あまり情報は入らない。むしろ専門性が高いことから、サイバーリスクを含めて任せざるを得ない状況にある。

③ サイバーセキュリティ対応方針の社内への周知状況（Q7、図 6）

| Q7. サイバーセキュリティ対応方針の社内への周知状況 （%、1 つ選択） | 全体 | プライム市場 | 資本金500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 従業員には周知されていない | 5.4 | 1.9 | 1.0 | 7.0 | 6.3 |
| 2. 一部の従業員へ周知されている | 7.2 | 4.5 | 1.0 | 5.9 | 12.7 |
| 3. 全従業員向けに周知されている | 23.7 | 17.0 | 6.7 | 23.4 | 31.7 |
| 4. 3 に加え、定期的な教育・訓練により理解度が確認されている | 38.8 | 46.9 | 47.1 | 38.1 | 31.4 |
| 5. 4 に加え、従業員の行動・意識が確認され、違反や是正状況がモニタリングされている | 22.6 | 27.3 | 42.3 | 23.4 | 15.8 |
| 6. その他 | 2.2 | 2.4 | 1.9 | 2.2 | 2.1 |
| （回答社数） | 1,524 | 418 | 104 | 727 | 379 |

図6

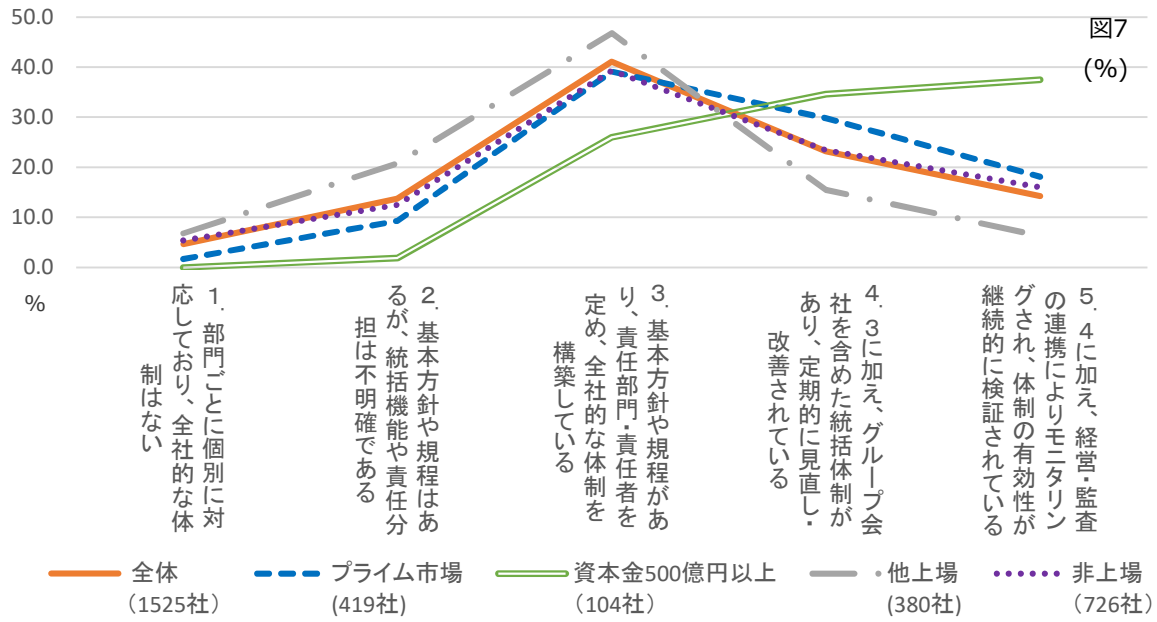



全体的な傾向として社内への周知・浸透は比較的進んでおり、監査役等からみて選択肢 4「3 の従業員向けの周知に加え、定期的な教育・訓練により理解度が確認されている」が最も多く全体で 38.8%、選択肢 5「4 の定期的な教育・訓練による理解度の確認に加え、従業員の行動・意識が確認され、違反や是正状況がモニタリングされている」と合計すると 61.4%に達する。選択肢 4 は、プライム市場上場会社では 46.9%を占め、それ以外の他上場会社も 31.4%に達している。

また、資本金 500 億円以上の会社では、選択肢 5 が 42.3%に達しており、従業員へのサイバーセキュリティ対応方針の周知・浸透がモニタリングも含めた高いレベルで実施されていることがうかがえる。

④ サイバーセキュリティリスク管理体制の構築・運用状況（Q8、図 7）

| Q8. サイバーセキュリティリスク管理体制の構築・運用状況 （%、1 つ選択） | 全体 | プライム市場 | 資本金500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 部門ごとに個別に対応しており、全社的な体制はない | 4.7 | 1.7 | 0.0 | 5.4 | 6.8 |
| 2. 基本方針や規程はあるが、統括機能や責任分担は不明確である | 13.7 | 9.3 | 1.9 | 12.5 | 20.8 |
| 3. 基本方針や規程があり、責任部門・責任者を定め、全社的な体制を構築している | 41.1 | 39.1 | 26.0 | 39.3 | 46.8 |
| 4. 3 に加え、グループ会社を含めた統括体制があり、定期的に見直し・改善されている | 23.2 | 29.8 | 34.6 | 23.4 | 15.5 |
| 5. 4 に加え、経営・監査の連携によりモニタリングされ、体制の有効性が継続的に検証されている | 14.2 | 18.1 | 37.5 | 16.0 | 6.3 |
| 6. その他 | 3.1 | 1.9 | 0.0 | 3.4 | 3.7 |
| （回答社数） | 1525 | 419 | 104 | 726 | 380 |

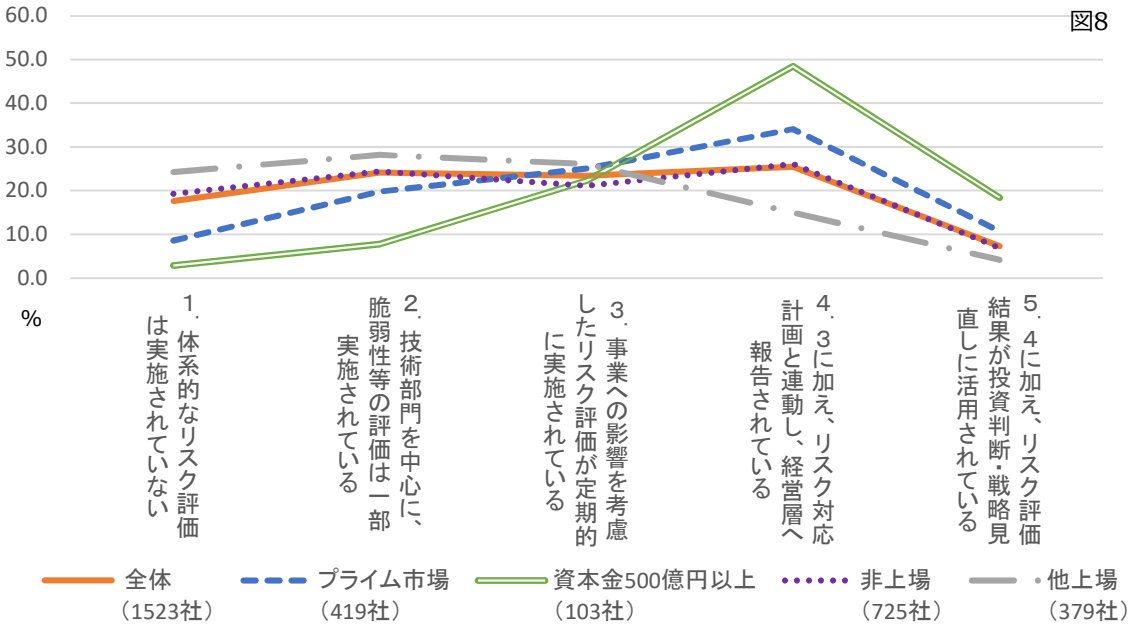



監査役等の視点によると、全体的に「3. 基本方針や規程があり、責任部門・責任者を定め、全社的な体制を構築している」会社が最も多く、全体では 41.1%である。特に他上場会社では 46.8%に達しており、中堅・中小規模の会社でも基本的な体制の構築に取り組んでいることがうかがえる。

また、資本金 500 億円以上の会社では、グループ全体でサイバーセキュリティリスク管理体制が構築・運用されている会社（選択肢 4 と 5）が合計 72.1%であり、その中でもモニタリングを含めて高度に運用されている会社（選択肢 5）が 37.5%存在している。

⑤ サイバーセキュリティリスク評価の実施状況（Q9-1、図 8）

| Q9-1.サイバーセキュリティリスク評価の実施状況（%、1 つ選択） | 全体 | プライム市場 | 資本金500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 体系的なリスク評価は実施されていない | 17.6 | 8.6 | 2.9 | 19.3 | 24.3 |
| 2. 技術部門を中心に、脆弱性等の評価は一部実施されている | 24.1 | 19.8 | 7.8 | 24.4 | 28.2 |
| 3. 事業への影響を考慮したリスク評価が定期的に実施されている | 23.4 | 25.1 | 22.3 | 21.1 | 26.1 |
| 4. 3 に加え、リスク対応計画と連動し、経営層へ報告されている | 25.5 | 34.1 | 48.5 | 26.1 | 15.0 |
| 5. 4 に加え、リスク評価結果が投資判断・戦略見直しに活用されている | 7.3 | 10.7 | 18.4 | 6.9 | 4.2 |
| 6. その他 | 2.0 | 1.7 | 0.0 | 2.2 | 2.1 |
| （回答社数） | 1,523 | 419 | 103 | 725 | 379 |




サイバーセキュリティのリスク評価（リスクアセスメント）とは、一般的には、重要資産を特定した上で、これらに対する脅威および脆弱性を識別し、その発生可能性および事業への影響を評価してリスクの優先順位を定め、リスク対応（回避・軽減・移転・受容）を計画するプロセスである。NIST サイバーセキュリティフレームワーク（CSF2.0）においても、脆弱性、脅威、発生可能性および影響度を用いてリスクを理解し、リスク対応の優先順位付けを行うことが求められている[24]。

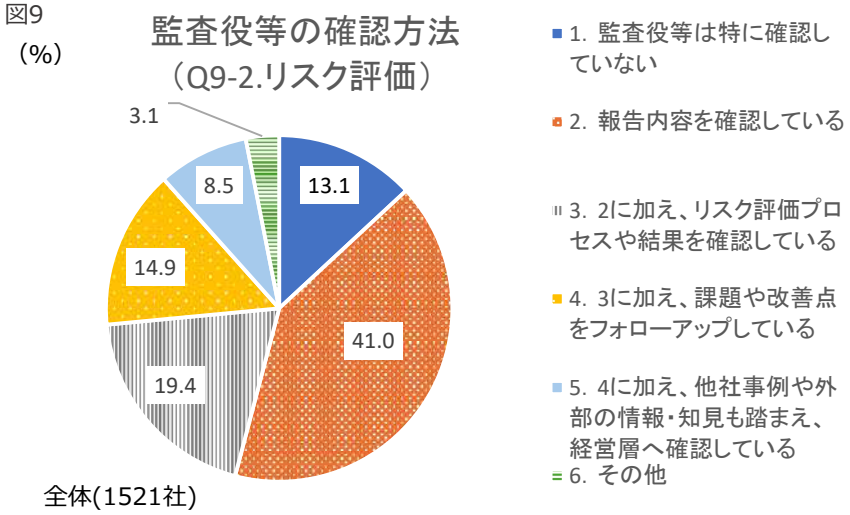
[24] NIST Cybersecurity Framework (CSF) 2.0, Appendix A, Risk Assessment (ID.RA-01～06)

アンケート結果では、全体では選択肢 2、3 および 4 がそれぞれ 20%台であり、全体的に実施状況に幅がみられる。また、「1. 体系的なリスク評価は実施されていない」会社が全体で 17.6%、他上場会社では 24.3%に達しており、やや懸念される。

プライム市場上場会社では「4. 3(事業への影響を考慮したリスク評価を定期的に実施)に加え、リスク対応計画と連動し、経営層へ報告されている」が最も多く 34.1%となっている。特に資本金 500 億円以上の会社では、選択肢 4 が最も多く 48.5%に達している。

また、**監査役等がサイバーセキュリティリスク評価の結果をどのように確認しているか**を質問した（Q9-2、図 9)。

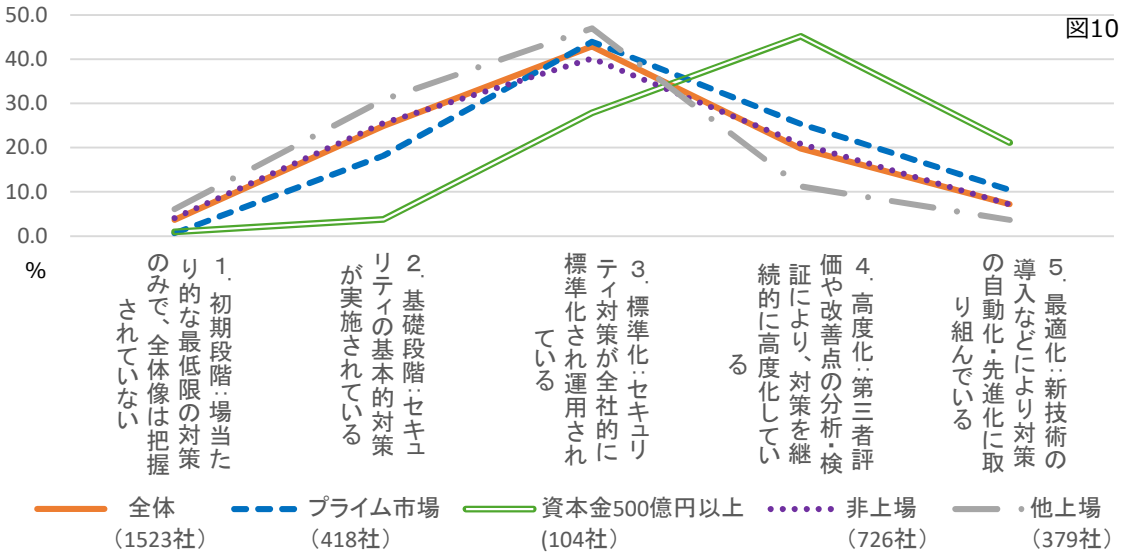
図9
(%)




全体では「2. 報告内容を確認している」が最も多く 41.0%、次に「3. 2(報告内容)に加え、リスク評価プロセスや結果を確認している」が 19.4%であり、どの会社区分でも同様の傾向であった。ただし、資本金 500 億円以上の会社では選択肢 3 が 32.7%であるほか、「4. 3 に加え、課題や改善点をフォローアップしている」も 27.9%と比較的高い割合になっている。

⑥ 監査役等からみたサイバーセキュリティ対策の全体像（Q10-1、図 10）

| Q10-1. サイバーセキュリティ対策の全体像※（%、1 つ選択） | 全体 | プライム市場 | 資本金500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 初期段階：場当たり的な最低限の対策のみで、全体像は把握されていない | 3.7 | 0.7 | 1.0 | 4.1 | 6.1 |
| 2. 基礎段階：セキュリティの基本的対策が実施されている | 24.9 | 18.2 | 3.8 | 25.6 | 30.9 |
| 3. 標準化：セキュリティ対策が全社的に標準化され運用されている | 42.9 | 44.0 | 27.9 | 40.2 | 47.0 |
| 4. 高度化：第三者評価や改善点の分析・検証により、対策を継続的に高度化している | 19.8 | 25.4 | 45.2 | 20.9 | 11.3 |
| 5. 最適化：新技術の導入などにより対策の自動化・先進化に取り組んでいる | 7.2 | 10.5 | 21.2 | 7.2 | 3.7 |
| 6. その他 | 1.5 | 1.2 | 1.0 | 1.9 | 1.1 |
| （回答社数） | 1,523 | 418 | 104 | 726 | 379 |




※アンケート実施時に各段階のイメージとして提示した具体例

1. 初期段階（例）ウイルス対策ソフトは導入されているが、その更新や管理、パスワードの管理は各自に任されている。
2. 基礎段階（例）セキュリティ製品・サービスの更新、セキュリティの基本方針や各種規程の策定、アクセス管理、情報資産の特定などが実施されている。
3. 標準化（例）サイバー攻撃の防御・検知・分析を実現する仕組み、データのバックアップの仕組みなどが整備され、定期的に更新されている。SOC（セキュリティ監視）や EDR（エンドポイント・セキュリティ）の導入、従業員への継続的な教育、リスクアセスメントの実施など。
4. 高度化（例）脆弱性診断やログ分析等を通じ、仕組みの有効性を確認している。
5. 最適化（例）攻撃者視点での組織的演習、ゼロトラストセキュリティの実装、EDR の高度化、AI による異常検知など。

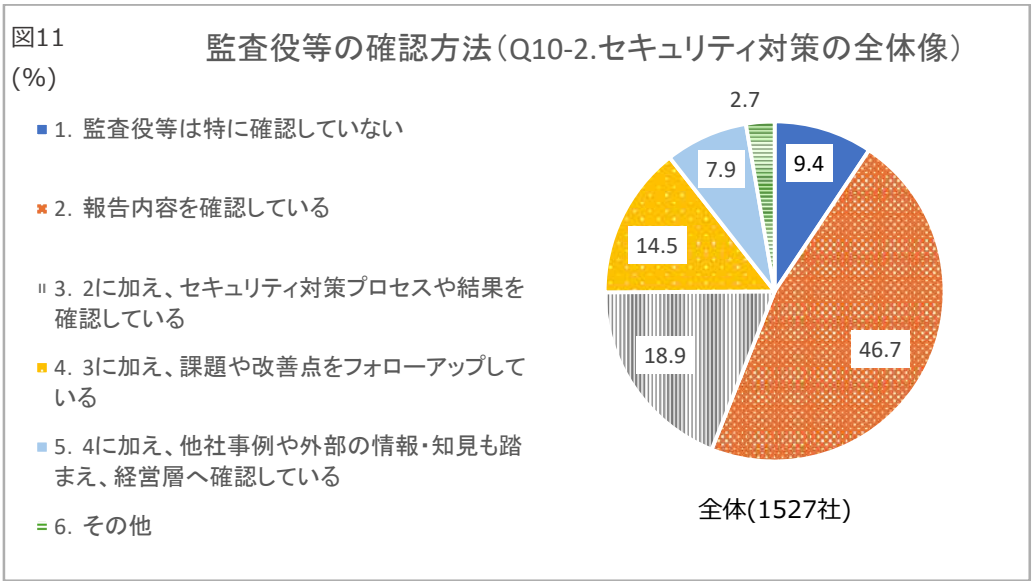
全体では「3. 標準化：セキュリティ対策が全社的に標準化され運用されている」が最も多く 42.9%である。プライム市場を除いた他上場会社では、この選択肢 3 が 47.0%、次に「2. 基礎段階：セキュリティの基本的対策が実施されている」が 30.9%となっており、基礎段階から標準化段階にある会社が合計 77.9%を占めている。

他方、プライム市場上場会社では、標準化やそれ以上（選択肢 3～5）の会社が合計で 79.9%を占めている。特に資本金 500 億円以上の会社では、「4. 高度化：第三者評価や改善点の分析・検証により、対策を継続的に高度化している」が 45.2%で最も多く、さらに「5.最適化：新技術の導入などにより対策の自動化・先進化に取り組んでいる」も 21.2%（22 社）存在している。

これらの結果は、自社のサイバーセキュリティ対策の成熟度が自社の脅威・リスクや業界の水準に照らして妥当かを評価するうえで一つの参考となるであろう。

また、**監査役等がサイバーセキュリティ対策の全体像をどのように確認しているか**を質問した（Q10-2、図 11）。

図11
(%)



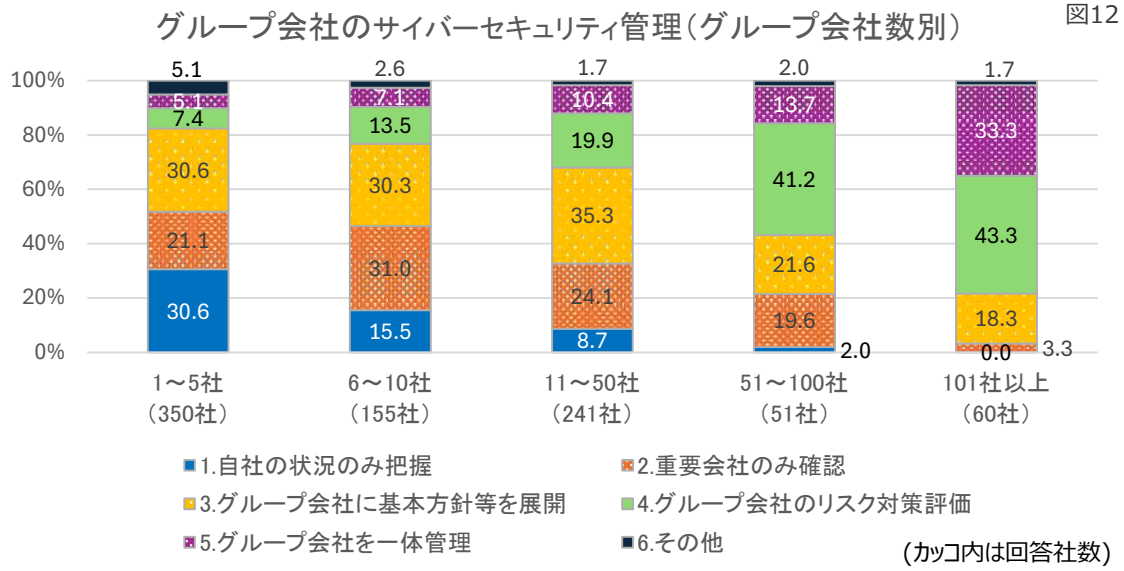

全体では「2. 報告内容を確認している」が最も多く 46.7%、次に「3. 2(報告内容)に加え、セキュリティ対策プロセスや結果を確認している」が 18.9%であり、どの会社区分でも概ね同様の傾向であった。ただし、資本金 500 億円以上の会社では、選択肢 2 は 26.9%にとどまり、「4. 3 に加え、課題や改善点をフォローアップしている」が最も多く 30.8%になっている。

### ⑦ グループ会社におけるサイバーセキュリティの管理・統制状況（Q11、図 12）

最終親会社全体で最も多いのは「3. グループ会社全体にセキュリティの基本方針や報告ルールなどを展開している」30.5%であるが、選択肢 1、2 および 4 もそれぞれ 1 割後半から 2 割超となっており、グループ会社の管理状況は様々である。「1. 自社以外の状況は把握されていない」会社が最終親会社全体で 17.9%、他上場会社では 22.2%存在している。実際のインシデントは海外グループ会社で発生する例が多いため（Q24 参照）、グループ会社の管理は重要である。他方、資本金 500 億円以上の会社では、「4. 3 に加え、グループ会社のセキュリティリスクやその対策状況を評価している」が最も多く 41.2%を占め、また「5. 4 に加え、インシデント対応・演習を含め、グループ会社を一体的に管理している」も 30.6%に達している。

| Q11. グループ会社におけるサイバーセキュリティの管理・統制状況（%、1 つ選択） | 全体 | プライム市場 | 資本金 500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 自社以外の状況は把握されていない | 17.9 | 10.1 | 2.4 | 28.6 | 22.2 |
| 2. 重要なグループ会社に限り、状況確認が行われている | 22.4 | 19.3 | 7.1 | 27.4 | 23.6 |
| 3. グループ会社全体にセキュリティの基本方針や報告ルールなどを展開している | 30.5 | 30.4 | 17.6 | 25.1 | 33.8 |
| 4. 3 に加え、グループ会社のセキュリティリスクやその対策状況を評価している | 16.6 | 23.9 | 41.2 | 8.6 | 11.3 |
| 5. 4 に加え、インシデント対応・演習を含め、グループ会社を一体的に管理している | 9.5 | 14.1 | 30.6 | 6.3 | 4.9 |
| 6. その他 | 3.3 | 2.3 | 1.2 | 4.0 | 4.2 |
| （回答社数） | 857 | 398 | 85 | 175 | 284 |

図12




グループ会社数別でみると、グループ会社数が増えるにつれ、「1. 自社の状況のみ把握」の割合は減少し、「4. リスク対策評価」や「5. 一体管理」の割合が高まっている。グループ

会社数が少ない「1～5 社」では、「1. 自社の状況のみ把握」と「3. 基本方針展開」がともに 30.6%で最多である。他方、グループ会社数 51 社以上の会社では、「4. グループ会社のセキュリティリスクやその対策状況を評価している」が最も多く 4 割以上を占めている。とくに「101 社以上」では、「5. グループ会社を一体管理」が 3 割以上を占め、大規模グループほど統合的な管理体制が進んでいる。

**グループ会社におけるサイバーセキュリティ体制の回答例（Q11）**

○親会社にセキュリティ統括部があり、グループ全社を統括しようとしている段階。その内容は自分から経営陣にも報告しているが、大きな考え方としては親会社のその統括部署と連動し、自社のシステム担当が自社内の対応を行うという方針であり、実際に連携して動いている。

○グループ会社が多く、親会社が求めるレベルのセキュリティー対策が出来るかなどはグループ会社ごとに事情が異なる。連結ベースで万全な対策が出来ているかどうかは常に検証が必要。

○グループ会社向けのサイバー保険に加入しており、サイバーインシデントについての報告や窓口が設けられていることから、気軽に連絡が取れる体制になっている。

○親会社にグループ会社全体の CSIRT が設置されており、個々の会社はチェックリストに基づき、評価とステップアップの計画を策定。個社の経営会議等で議論されている。

○過去に専門的な実戦演習をグループ会社や外部業者との連携で行ったことがある。

**グループ会社の監査役等としての対応の回答例（Q11）**

○グループ内のサイバーセキュリティ業務を支援していることから、グループ監査役連絡会にてよく議論している。

○親会社が推進しており、自社としての監査はしていない。ただし訓練状況やグループ会社での事例等は社内会議体で報告される内容を確認している。

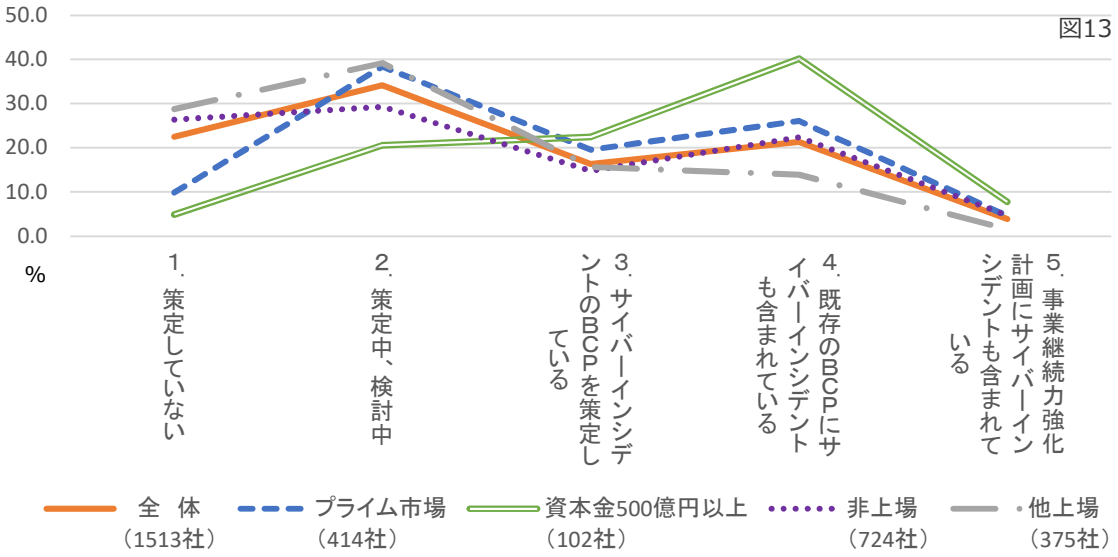
○特に海外グループ会社への監査インタビュー時にはサイバーセキュリティをヒアリング項目に追加し、対応状況を把握するようにしている。

### （4）サイバーインシデント発生時の緊急対応体制

サイバーインシデント発生時の緊急対応体制の整備については、特にランサムウェア攻撃を想定した BCP（Business Continuity Plan：事業継続計画）が策定されているかに着目して調査した。

#### ① サイバーインシデントを想定した BCP の策定（Q12、図 13）

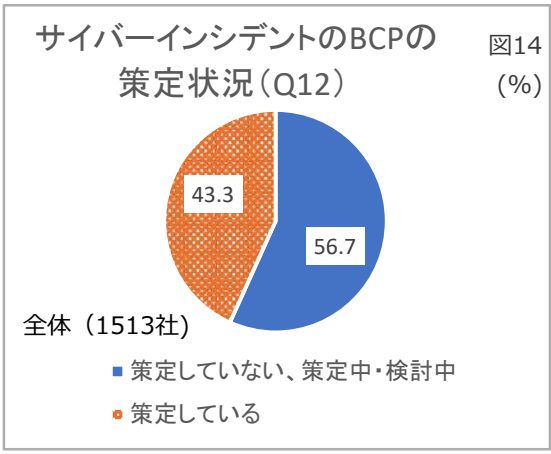
| Q12. サイバーインシデントを想定した BCP の策定状況（%、1 つ選択） | 全体 | プライム市場 | 資本金 500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 策定していない | 22.5 | 9.9 | 4.9 | 26.4 | 28.8 |
| 2. 策定中、検討中 | 34.2 | 38.4 | 20.6 | 29.3 | 39.2 |
| 3. サイバーインシデントの BCP を策定している | 16.3 | 19.6 | 22.5 | 14.8 | 15.7 |
| 4. 既存の BCP にサイバーインシデントも含まれている | 21.3 | 26.1 | 40.2 | 22.4 | 13.9 |
| 5. 事業継続力強化計画[25]にサイバーインシデントも含まれている | 3.9 | 4.6 | 7.8 | 4.7 | 1.6 |
| 6. その他 | 1.8 | 1.4 | 3.9 | 2.5 | 0.8 |
| （回答社数） | 1,513 | 414 | 102 | 724 | 375 |

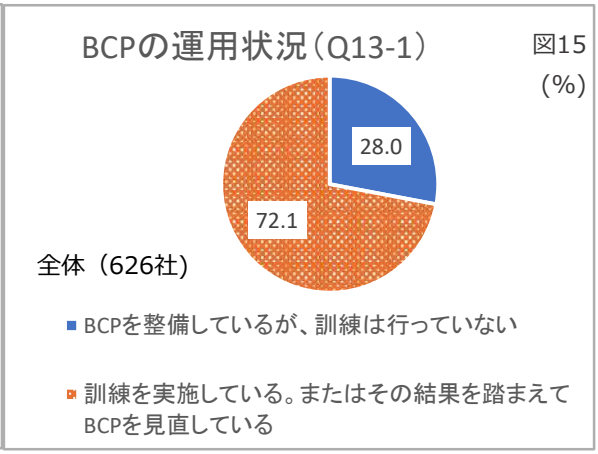



サイバー攻撃を想定した BCP を策定していない会社（選択肢 1 および 2）は全体で合計 56.7%（図 14）、他上場会社では 68.0%を占めている。当協会が実施した過去の調査では、災害等を想定した BCP を策定している会社は 54%であり、BCP の策定自体が必ずし

[25] 経済産業大臣が認定する中小事業者向けの BCP。なお、アンケート結果ではプライム市場上場会社や資本金額 500 億円以上の会社でもこの選択肢 5 への回答がみられるが、各社の中期経営計画などと混同された可能性がある。
https://www.chusho.meti.go.jp/keiei/antei/bousai/keizokuryoku.html#tebiki

も進んでいないという結果が出ていた[26]。サイバー攻撃による業務やシステムの停止はどの会社でも起こり得る事象であり、サイバーインシデントは BCP の重要なリスクである。そのため、サイバーインシデントの BCP の策定は、どの会社にも必要であろう。



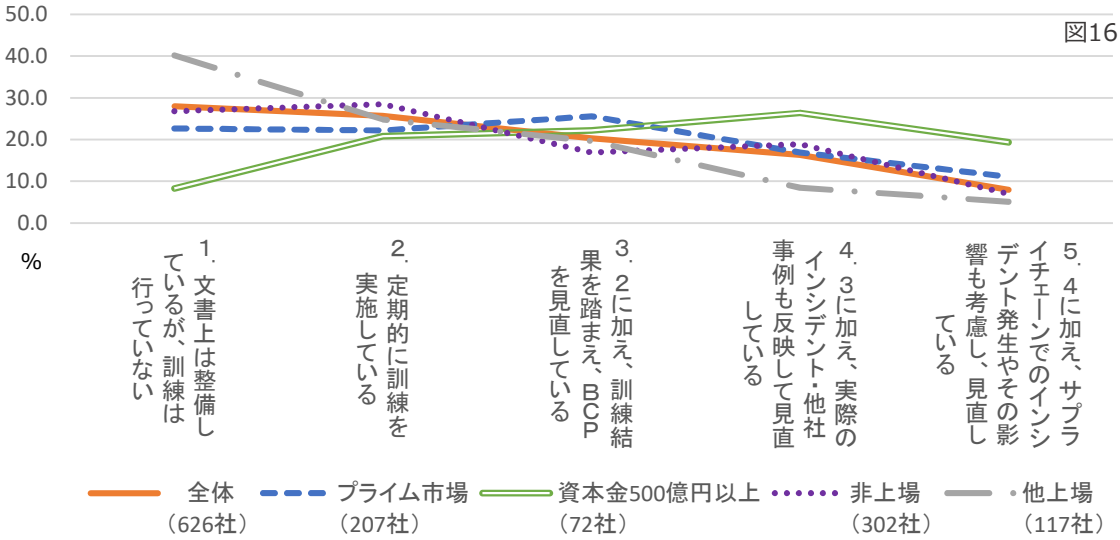




② サイバーインシデントの BCP の運用状況（Q13-1、図 16）

| Q13-1. サイバーインシデントの BCP の運用状況（%、1 つ選択） | 全体 | プライム市場 | 資本金500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 文書上は整備しているが、訓練は行っていない | 28.0 | 22.7 | 8.3 | 26.8 | 40.2 |
| 2. 定期的に訓練を実施している | 25.7 | 22.2 | 20.8 | 28.5 | 24.8 |
| 3. 2 に加え、訓練結果を踏まえ、BCP を見直している | 20.3 | 25.6 | 22.2 | 16.9 | 19.7 |
| 4. 3 に加え、実際のインシデント・他社事例も反映して見直している | 16.3 | 16.9 | 26.4 | 18.9 | 8.5 |
| 5. 4 に加え、サプライチェーンでのインシデント発生やその影響も考慮し、見直している | 8.0 | 11.1 | 19.4 | 7.0 | 5.1 |
| 6. その他 | 1.8 | 1.4 | 2.8 | 2.0 | 1.7 |
| （回答社数） | 626 | 207 | 72 | 302 | 117 |

[26] (公社)日本監査役協会『第 2 回適時調査 事業リスクと BCP の策定状況』2023 年 3 月 20 日、5 頁。

図16




サイバーインシデントの BCP を持つ会社においても、その 28.0%（他上場では 40.2%）が「1. 文書上は整備しているが、訓練は行っていない」と回答している。訓練を踏まえて見直しまで行う会社（選択肢 3 から 5）は全体で 44.6%である。BCP の実効性をもたせるためには、訓練の実施とその結果に基づいた適切な見直しが必要と考えられる。

なお、**BCP の見直しの頻度**については、「年に 1 回程度」が全体で 58.1%であり、次に「数年に 1 回程度」が 18.2%で続いている（Q13-2）。

また、サイバーインシデントを想定した BCP の策定や運用状況について、監査役等が関与していることがあるか質問した（Q13-3、記述回答）。取締役会において BCP の見直しや訓練の実施について助言したり、監査役等も訓練に参加するなどの参考例が寄せられた。

**サイバーインシデントの BCP への関与・確認の回答例（Q13-3）**

○BCP の見直しを取締役会等で進言している。

○BCP の文書化が完了した事は評価しつつ、訓練の実施が今期の課題であると取締役会で意見を表明した。

○訓練には監事も参加し、気づいたことや参加者からの意見等が計画に反映されているか確認している。

○昨年から BCP の訓練が始まったが監査役は呼ばれなかったので、今年の訓練には必ず監査役にも声をかけるよう依頼した。

○BCP の見直しやサイバーセキュリティに対応した IT-BCP の高度化について、定期的な面談を通じて確認を行っている。

○監査等委員は、全社的な内部統制システムおよび BCP に包含されたサイバーセキュリティのリスク管理の運用状況やインシデント発生時の集約情報を定期的にモニタリングするかたちで関与している。

③ サイバーインシデントの訓練の実施状況（Q14）

| Q14. サイバーインシデント訓練の実施状況（%、複数選択可） | 全体 | プライム市場 | 資本金500億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 役職員向けの標的型攻撃メール訓練、フィッシング訓練 | 68.3 | 80.0 | 90.3 | 69.8 | 52.4 |
| 2. サイバーセキュリティについての研修、e ラーニングなど | 75.0 | 81.4 | 95.1 | 76.9 | 64.4 |
| 3. 技術演習（ログ分析、マルウェア解析、フォレンジック演習など） | 11.3 | 19.6 | 35.0 | 9.4 | 5.9 |
| 4. 組織横断型演習（経営層・広報・法務なども参加） | 14.4 | 20.8 | 32.0 | 15.4 | 5.3 |
| 5. 復旧演習、バックアップデータの復元訓練 | 12.1 | 15.9 | 27.2 | 11.6 | 8.6 |
| 6. ペネトレーションテスト（第三者による侵入テスト） | 13.9 | 22.2 | 40.8 | 13.2 | 6.1 |
| 7. レッドチーム演習（攻撃者視点による組織全体での実践演習） | 2.6 | 4.1 | 13.6 | 3.0 | 0.3 |
| 8. その他 | 2.3 | 2.7 | 2.9 | 2.5 | 1.3 |
| 9. 特に実施していない | 10.4 | 5.3 | 1.0 | 9.0 | 18.7 |
| （回答社数） | 1,510 | 414 | 103 | 722 | 374 |

全体的に訓練内容は「研修・e ラーニング」75.0%と「標的型メール訓練」68.3%という「入口」に集中しており、どの会社区分でも概ね同様の傾向であった。

一方、インシデント発生を想定した実践型の演習である「組織横断型演習」は 14.4%、「ペネトレーションテスト」は 13.9%、「復旧演習」は 12.1%にとどまり、上位２つと比べると極めて実施割合が低い。その要因として、記述回答では専門組織や担当者の不在という人材不足が指摘されている。また、経営陣や社員の認識も課題として挙げられており、経営層が参加する実践的演習の実施が望まれる。

**サイバーインシデント訓練の課題と対応の回答例（Q14）**

**課題**

○会社として高度な IT 専門家がいないことから、技術演習、復旧演習までは行えていない。

○社員個々人がその影響度をしっかりと理解する必要があり、まだ周知が不足していると危惧される。

○実際にサイバー攻撃を受けたことがないこともあり、事業への影響について経営層は深刻に考えていない印象である。今後は、重大な影響があることを認識したうえで、実践演習・復旧演習などが必要となる。

○事故発生や環境の変化がなく施策の見直し頻度が少なくなると、形骸化するおそれがある。

**対応**

○システムは徐々に整備されてきているが、社員の意識向上のため、啓もう活動や訓練の頻度は高めた方がよいと考えている。

○施策を施すだけでなく、その運用面がしっかりしていないと施策の効果が発揮されないため、グループ社員の隅々まで役割に応じたレベルの認識を持つ必要がある。

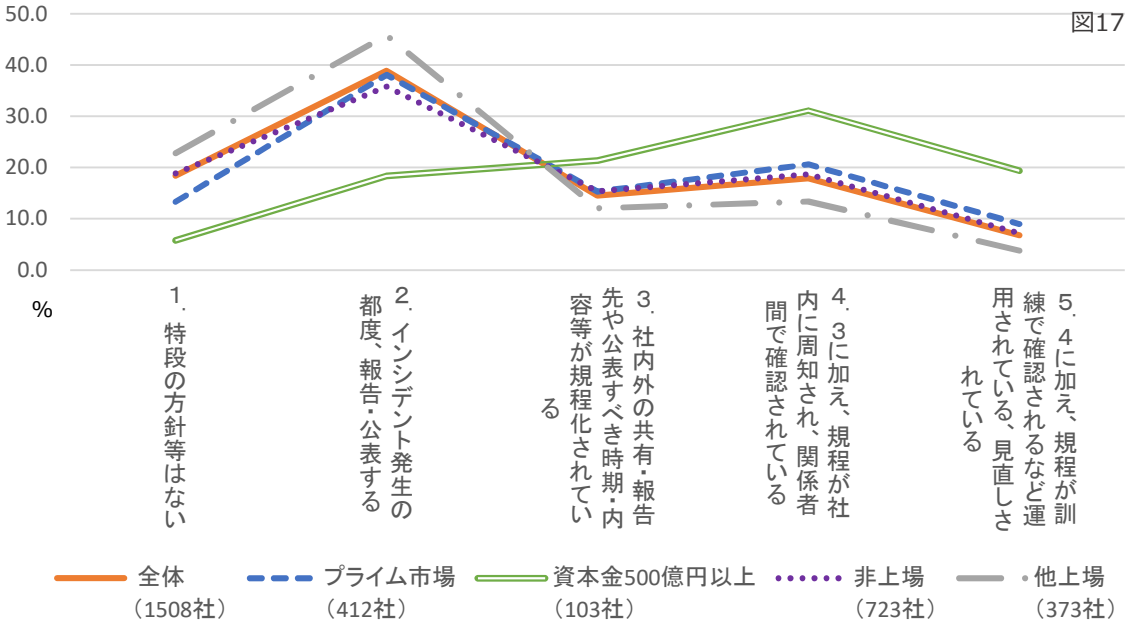
○訓練や研修を数回実施しただけでは効果は薄れていくことから、年間を通して複数回実施していくことに加えて、社長や組織長から社員向けにサイバーセキュリティに対してしっかり意識するようメッセージを発信していくことが重要と考える。

### ④ サイバーインシデントの報告・公表ルート（Q15、図 17）

社内外にサイバーインシデントを報告・公表するルートやタイミングなどが定められているかについて質問した。

| Q15. サイバーインシデントの報告・公表ルート（%、1 つ選択） | 全体 | プライム市場 | 資本金 500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 特段の方針等はない | 18.4 | 13.3 | 5.8 | 18.9 | 22.8 |
| 2. インシデント発生の都度、報告・公表する | 38.9 | 38.1 | 18.4 | 35.8 | 45.8 |
| 3. 社内外の共有・報告先や公表すべき時期・内容等が規程化されている | 14.5 | 15.3 | 21.4 | 15.4 | 12.1 |
| 4. 3 に加え、規程が社内に周知され、関係者間で確認されている | 17.9 | 20.6 | 31.1 | 18.7 | 13.4 |
| 5. 4 に加え、規程が訓練で確認されるなど運用されている、見直しされている | 6.8 | 9.0 | 19.4 | 7.2 | 3.8 |
| 6. その他 | 3.4 | 3.6 | 3.9 | 4.0 | 2.1 |
| （回答社数） | 1,508 | 412 | 103 | 723 | 373 |

図17




インシデントの報告・公表の手順が規程化されていない会社（選択肢 1 および 2）は全体で 57.3%、他上場会社では 68.6%にのぼる。有事に「誰に・いつ・何を報告するか」が定まっていなければ、初動は遅れ、社外への説明責任も果たせないおそれがある。

**サイバーインシデント発生時の報告体制の回答例（Q15）**

○社内での迅速な報告は定められているが、社外への連絡・公表は代表取締役をはじめ社内の関連部署で検討する。

○親会社への報告ルート・タイミングは定められている。

○インシデントが発生した際の専門家の要請先の確認、保険契約の確認、情報流出の際の対応策が整っていないように思えるため、状況の確認を行った。

○インシデント発生時における社内の体制図があり、実際に発生したことを想定した社内訓練も実施されている。また、その報告先として取締役会（監査等委員会設置会社）にて全役員が確認し報告を受ける仕組みである。

○当社では、情報セキュリティインシデント発生時の報告および公表に関するルートや手順を規程として整備しており、社内外への報告先、報告内容および公表の判断プロセスが明確化されている。外部機関への報告や社外公表については、CISO の承認および関係部門との協議を踏まえて実施する仕組みとなっている。また、当該規程は社内で周知されるとともに、インシデント対応体制（XSIRT 等）に基づく運用および訓練を通じて実効性の確保が図られている。

### （4） サプライチェーン全体でのセキュリティ対策

#### ① サプライチェーンのサイバーセキュリティ体制・対策へのアプローチ（Q16-1）

監査役等として、取引先（委託先等）のサプライチェーンのサイバーセキュリティ体制や対策などについて、どのようにアプローチしているか質問した。

| Q16-1. 監査役等のサプライチェーンのサイバーセキュリティ体制・対策へのアプローチ方法（%、複数選択可） | 全体 | プライム市場 | 資本金500億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 監査役等は確認していない、報告を受けていない | 38.4 | 33.2 | 16.3 | 40.3 | 40.6 |
| 2. 委託先の管理・統括部門に確認する | 13.8 | 12.7 | 15.4 | 15.3 | 12.3 |
| 3. サイバーセキュリティを管理・統括している部門、責任者に確認する | 41.0 | 44.9 | 63.5 | 40.3 | 38.2 |
| 4. 内部監査部門に確認する | 22.4 | 27.6 | 32.7 | 20.5 | 20.6 |
| 5. 取締役会等（経営会議等も含む）におけるサイバーセキュリティをめぐる報告や議論で確認する | 23.0 | 29.8 | 50.0 | 21.9 | 17.6 |
| 6. サイバーセキュリティの外部専門家に確認する | 1.0 | 1.0 | 1.0 | 1.0 | 1.1 |
| 7. 監査役等が直接現場部門に確認する、契約内容を確認する | 2.5 | 2.0 | 1.9 | 2.8 | 2.7 |
| 8. その他 | 1.8 | 1.5 | 1.0 | 2.2 | 1.3 |
| （回答社数） | 1,497 | 410 | 104 | 713 | 374 |

監査役等がサプライチェーンについて「1. 確認していない・報告を受けていない」割合が全体で 38.4%、他上場会社では 40.6%に達した。選択肢 1 は全て単独回答であり、他の選択肢と組み合わせた回答はなかったため、サプライチェーンについて確認しているか否かが明確に分かれている。「サプライチェーンや委託先を狙った攻撃」は IPA の「情報セキュリティ 10 大脅威」の第 2 位でありながら（2 頁参照）、監査役等が取引先（委託先等）の状況を確認することの難しさが表れている。まずはサイバーセキュリティの管理・統括部門や内部監査部門などから状況の報告を受ける仕組みを作ることが第一歩であろう。

確認をしている層で最も多いのは「3. サイバーセキュリティを管理・統括している部門、責任者に確認する」41.0%であり、この選択肢 3 を中心とした組み合わせがみられる。特に資本金 500 億円以上の会社では、選択肢 3 から 5 までを組み合わせた回答が一定数存在しており、様々なルートで取引先（委託先等）にアプローチしていることがうかがえる。

**② サプライチェーンのサイバーセキュリティ体制・対策に関する課題、工夫**（Q16-2）

取引先(委託先等)のサプライチェーンのサイバーセキュリティ体制や対策などについて、監査役等が気掛かりな点、課題または工夫している事項などを記述形式で質問した。

記述回答では、取引先（委託先等）の範囲・重要性の定義が不透明、取引先（委託先等）に中小・零細事業者が多く対策費用の負担が課題、再委託先等を含めた可視化が困難、といった課題が多く挙がった。他方で、実効性を高めるための好事例も見られた。以下では、テーマのカテゴリー別に記述回答の抜粋を紹介する。

**アンケート、チェックリストの使用についての回答例（Q16-2）**

○委託先等には、質問書形式でサイバーセキュリティ体制の自己評価を回答していただき、内容を評価しているが、本当にその通りか実態の確認までは行っていない。

○今まではチェック項目を設けてそのチェックシートを報告してもらうことに留まっていたが、報告に加えてパートナー各社を訪問し、実地に確認をするようにしている。

○委託先の状況に関するアンケートと改善要請程度は行っているが、明確な強制力はなく、また網羅的な確認に至っていない。契約書でもサイバーセキュリティに特化した条項はない。全役員出席のリスク管理委員会にて、主管部から委託先へのアンケート結果や改善要請状況などが報告され、必要に応じて質問や助言をしている。

**取引先（委託先等）の範囲、重要性、優先度の回答例（Q16-2）**

○サイバーセキュリティ体制を求めるサプライチェーンの範囲や定義付けがやや不透明。

○委託先には中小企業が多く、どこまで組織的な対策がなされているか、心配なところが多い。そもそも、サイバーセキュリティについて、委託先とは深い意見交換を行なっていないことが課題。

○委託先や取引先のサイバーセキュリティ対策を包括的に調査しデータ化していない。すべての取引先を調査する必要はないが、重要なパートナー企業を選定して、それらの企業からサイバーセキュリティ対策の整備状況を把握する必要がある。

○当社からの委託先には零細事業者等も多く、サイバーセキュリティ対策費用に関して発注者側に負担を求められることも懸念される。そのため委託内容や事業者規模等を踏まえ、優先度の高い委託先から実施する方針である。

**評価・監査関係の回答例（Q16-2）**

○委託先に関しては、第三者アセスメントを実施し、委託先のセキュリティ体制や対策について確認しており、要件を満たせない場合は取引を行わないか満たせない分を運用や契約で補完している。

○委託先の体制や対策を確認するには、社員にとってもある程度の知見が必要であり、それが可能な人材の確保は簡単ではない。

○往査先の事業所において委託先のサイバーセキュリティ体制の確認、指導の状況を聞き取り、必要に応じて改善等に関する意見を述べている。

○外部委託先管理の一環としてリスク管理されており、リスク管理統括部門長との面談を通じて確認を行っている。

○契約条項にセキュリティー体制や対策等の追加記載をするよう、契約の主管部門へ推奨している。

○調達部門等の委託先管理・統括部門を通じて状況を把握するとともに、当該内容は取締役会および全社リスク管理会議における報告・議論の中で確認されている。監査等委員は、これらの報告および議論を通じて、委託先を含めたサイバーセキュリティリスクの状況を把握している。

**その他サプライチェーンのサイバーセキュリティについての回答例（Q16-2）**

○委託先のサイバーセキュリティ体制が相当であるかを判断する知見が不足しており、統括部門や委託先の意見に頼らざるを得ないのが実態である。

○委託先が機能不全に陥った場合の代替案の検討が不足している。一方、当社の顧客から、セキュリティ対策の不足を要因として取引を停止される恐れもある。

○委託先におけるセキュリティ対策の水準や運用実効性のばらつき、並びにインシデント発生時の報告・連携体制の透明性は課題。特に再委託先を含めた管理範囲の不明確さや、定期的な評価・監査の実効性確保が重要な課題である。

○全ての外注先に対し、経産省 SCS 評価制度の★２以上をお願いしている。今期からは★３以上を依頼する予定だが、個人事業主には負担が大きく、効果的な体制構築は困難と考えられる。

○弊社では、委託先に対しても社内と同等のセキュリティ水準を求め、契約書の条文にもインシデント報告義務や再委託管理等を規定した上で、選定時評価や定期的な状況確認を実施している。一方で、再委託先を含めたサプライチェーン全体の可視化や、現場レベルでのセキュリティ意識・運用のばらつきには一定の課題がある。特に、１人親方の様な委託先や小規模な会社など、組織としての認識や教育制度が整っていない会社の社員一人一人への教育状況の把握は十分とは言えない。このため、今後も内部監査や関係部署を通じて、リスク評価、委託先を含めた教育・訓練の継続実施、インシデント対応訓練の強化等により、サプライチェーン全体のセキュリティ向上に取り組んでいく。

回答例には、外部からは見えにくい取引先（委託先等）を会社があるいは監査役等が確認する際に参考になる方法がいくつもみられる。チェックシートの報告にとどめず訪問・実地確認へ踏み込んだ例、第三者アセスメントを実施し要件を満たせない場合は取引しない例、取引先（委託先等）の重要度に応じて優先順位を付けて対応する例、契約条項にセキュリティ要件・報告義務・再委託管理を盛り込む例などは、実効性を高める具体的な工夫である。

### （6）サイバーセキュリティをめぐる社内の課題

監査役等からみたサイバーセキュリティをめぐる社内の課題について質問した（Q21）。

| Q21. サイバーセキュリティをめぐる社内の課題（多い順・複数選択可・%） | 全体 | プライム市場 | 資本金500億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 6. サイバーセキュリティを担当する人材の育成、人材獲得 | 50.5 | 56.0 | 70.6 | 49.6 | 46.0 |
| 4. 現場部門、従業員の教育、研修 | 42.5 | 37.5 | 36.3 | 44.6 | 44.1 |
| 9. サイバーインシデントを想定した緊急対応計画、体制、訓練 | 42.3 | 46.4 | 45.1 | 39.8 | 42.7 |
| 11. 委託先等のサプライチェーンのリスク評価、セキュリティ対策等 | 38.2 | 47.9 | 61.8 | 35.7 | 32.5 |
| 1. 経営陣の意識、経営リスクとしての認識 | 37.4 | 34.6 | 20.6 | 37.4 | 40.6 |
| 10. グループ会社のリスク評価、セキュリティ対策等 | 36.5 | 58.8 | 64.7 | 26.0 | 32.5 |
| 5. サイバーセキュリティ監査（内部監査部門の監査、IT 部門等の監査、外部専門組織の監査） | 34.5 | 37.3 | 26.5 | 33.4 | 33.3 |
| 2. 取締役会等（経営会議等も含む）におけるサイバーセキュリティの報告や議論の状況 | 29.9 | 31.6 | 16.7 | 27.6 | 32.3 |
| 3. サイバーセキュリティの管理・統括部門、責任者 | 28.4 | 24.9 | 16.7 | 28.8 | 31.5 |
| 8. サイバーセキュリティの対策の予算・費用、保険 | 23.8 | 24.7 | 25.5 | 23.0 | 24.2 |
| 7. サイバーセキュリティの外部専門組織との提携 | 16.7 | 17.3 | 16.7 | 16.6 | 16.1 |
| 12. その他 | 1.5 | 2.0 | 2.0 | 1.6 | 1.1 |
| 13. 特にない | 1.6 | 1.0 | 1.0 | 2.3 | 1.1 |
| （回答社数） | 1,486 | 405 | 102 | 709 | 372 |

全体として課題認識の第 1 位は「人材の育成・獲得」（50.5%）であり、特に資本金 500 億円以上の会社では 70.6%に達している。次いで従業員教育（42.5%）、緊急対応計画・体制・訓練（42.3%）、サプライチェーンのリスク評価・セキュリティ対策（38.2%）が続いている。これらの監査役等自身が課題と感じている領域は、本アンケートで対策が遅れている領域と概ね一致すると考えられる。例えば、サイバーセキュリティリスク管理の専門組織は部分的または兼務である会社が比較的多いこと（Q6）、サイバーインシデントを想定した BCP が策定されていない会社が多いこと（Q12）、サイバーインシデント発生を想定した実践型の演習は実施率が低いこと（Q14）、そしてサプライチェーンのサイバーセキュリティ体制・対策等の確認がなされていないこと（Q16-1）という結果との整合性がみられる。

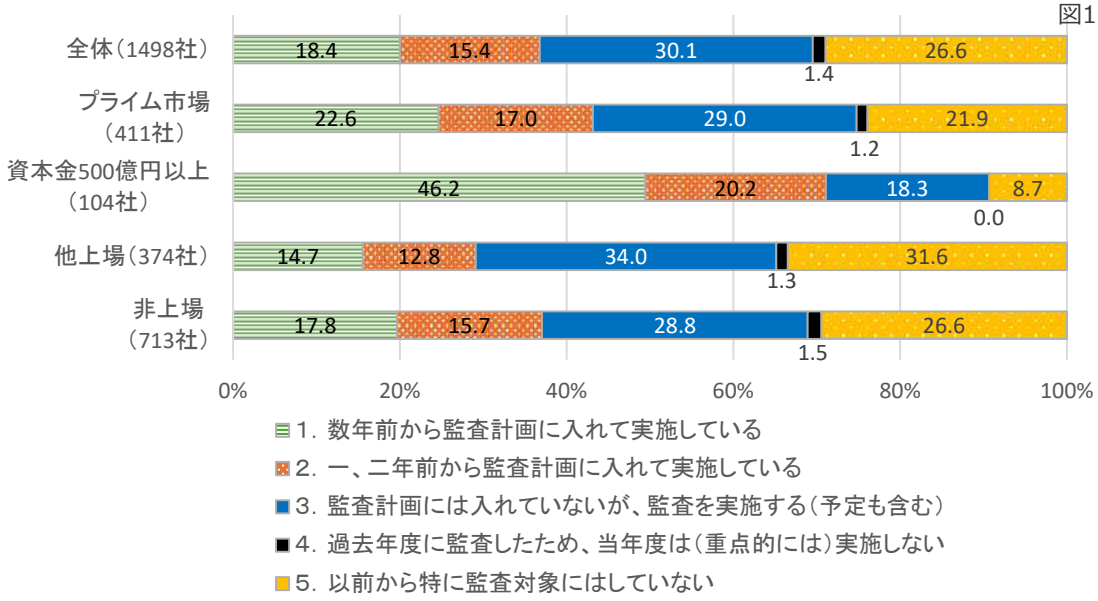
### （7）監査役等のサイバーセキュリティへの監査活動

#### ① サイバーセキュリティと監査計画、重点監査項目（Q17、図 18）

監査役等の監査計画の中に、サイバーセキュリティを入れているか質問した（Q17-1）。

| Q17. サイバーセキュリティを監査計画にいれているか （%、1 つ選択） | 全体 | プライム市場 | 資本金500 億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 数年前から監査計画に入れて実施している | 18.4 | 22.6 | 46.2 | 17.8 | 14.7 |
| 2. 1,2 年前から監査計画に入れて実施している | 15.4 | 17.0 | 20.2 | 15.7 | 12.8 |
| 3. 監査計画には入れていないが、監査を実施する（予定も含む） | 30.1 | 29.0 | 18.3 | 28.8 | 34.0 |
| 4. 過去年度に監査したため、当年度は（重点的には）実施しない | 1.4 | 1.2 | 0.0 | 1.5 | 1.3 |
| 5. 以前から特に監査対象にはしていない | 26.6 | 21.9 | 8.7 | 26.6 | 31.6 |
| 6. その他 | 8.2 | 8.3 | 6.7 | 9.5 | 5.6 |
| （回答社数） | 1,498 | 411 | 104 | 713 | 374 |

図18




全体で最も多いのは、「3. 監査計画には入れていないが、監査を実施する（予定も含む）」30.1%である。次に多いのは「5. 以前から特に監査対象にはしていない」26.6%であり、特に他上場会社では 31.6%に達し、選択肢 3 と同程度の割合となっている。

経営リスクの上位に位置するテーマが監査計画に十分反映されていない要因の 1 つとして、「監査対象となる執行側の体制等ができていない」ことが考えられる（Q19-2 記述回答より[27]）。確かに、アンケート結果では「サイバーセキュリティリスク管理の専門組織はない

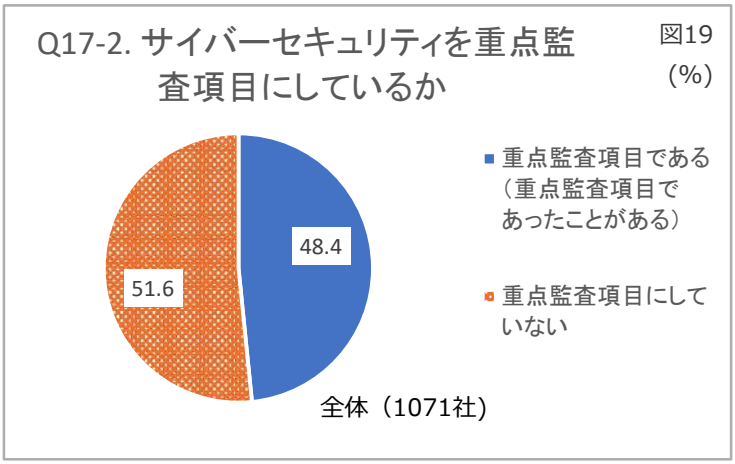
[27] Q19-2 では、Q19-1 で「2. サイバーセキュリティを監査計画に入れる予定はない」43.1%（170 社）にその理由を質問した。体制の不備の他、「（親会社の）内部監査部門や情報セキュリティ部門などが監査をしているため」、「監査役等が自らが監査するには技術的知見などに欠けるため」などの回答があった。

が部分的にある・他の部門が兼務している」会社が 44.1%であり（Q6）、サイバーセキュリティリスク管理の全社的な体制はない会社が 18.4%である（Q8 の選択肢 1 と 2 の合計）。記述回答でも、社内の体制が不十分な会社において「監査役だけで動いても意味がないので、まず執行側への働きかけを実施したいと思う。」という意見があったが、まずは執行側に体制の整備を促していく必要があるであろう。

また、他の要因としては、サイバーセキュリティのリスク評価が実施されていない会社が一定数存在する（全体で 17.6%、一部実施は 24.1%）ことも考えられる（Q9-1）。監査役会等は執行側のリスク評価をそのまま受け入れるのではなく、監査役会等自身もリスクを理解し、執行側のリスク認識の妥当性やリスクの評価プロセスの適切性などを改めて確認する必要があるだろう[28]。

なお、選択肢 5「監査対象にはしていない」会社の 56.9%が「今後監査計画に入れる予定がある」と回答しており（Q19-1 選択肢 1）、サイバーセキュリティの監査に前向きな姿勢がうかがえる[29]。

さらに、**サイバーセキュリティを重点監査項目にしているか**については、「重点監査項目である（重点監査項目であったことがある）」会社が約半数であった（Q17-2、図 19）。




会社規模が大きいほど、サイバーセキュリティを重点監査項目にしている会社が多く、プライム市場上場会社では 59.7%、資本金 500 億円以上の会社では 74.7%となっている。

[28] (公社)日本監査役協会ケース・スタディ委員会『多様化するリスクの把握と監査活動への反映及びその開示』2023 年 11 月 30 日、27 頁。

[29] なお、監査計画や重点監査項目の見直しの頻度は、過去の調査によると「毎年（年に 1 度）」と「原則毎年（必要なら期中でも見直し）」がそれぞれ 48%～49%であった。合計すると年に 1 度は見直すという会社がほとんどであるが、必要なら期中でも見直すかについては半々に分かれた（脚注 28、2 頁）。

② サイバーセキュリティに対する監査役等のアプローチ方法（Q18-1）

| Q18-1. サイバーセキュリティに対する監査役等のアプローチ方法 （%、複数選択可） | 全体 | プライム市場 | 資本金500億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. 経営陣への確認、対話 | 45.5 | 40.3 | 55.8 | 51.3 | 39.9 |
| 2. 取締役会等（経営会議等も含む）の報告や議論 | 49.6 | 59.1 | 69.5 | 44.6 | 47.8 |
| 3. サイバーセキュリティ対策の責任者への確認 | 62.7 | 69.1 | 73.7 | 61.1 | 58.1 |
| 4. サイバーセキュリティリスク管理・統括組織への確認、報告の受領、会議への参加など | 57.3 | 67.8 | 87.4 | 59.4 | 39.5 |
| 5. 内部監査部門からの報告、確認、監査の指示や依頼 | 48.7 | 57.8 | 68.4 | 44.3 | 46.2 |
| 6. サイバーセキュリティの外部専門組織への確認 | 2.8 | 4.1 | 3.2 | 2.5 | 2.0 |
| 7. 監査役等自身が直接確認する | 7.9 | 9.4 | 7.4 | 7.5 | 7.1 |
| 8. その他 | 1.5 | 0.9 | 1.1 | 2.3 | 0.4 |
| （回答社数） | 1,095 | 320 | 95 | 522 | 253 |

全体では「3. サイバーセキュリティ対策の責任者」62.7%、「4. サイバーセキュリティリスク管理・統括組織」への確認が 57.3%である。責任者は代表取締役や他の取締役である場合が多いが（Q5）、独立した専門組織が設置されていない会社は全体で 53.7%である（Q6）ことから、専門組織の設置状況が監査役等の確認経路に一定の影響を与えている可能性がある。また、「2. 取締役会等」での確認も 49.6%にとどまっているが、取締役会等でサイバーセキュリティの定期報告がされていない会社は全体で 43.7%存在している（Q1）ことが影響していると考えられる。

また、「7. 監査役等自身が直接確認する」は全体で 7.9%と少数である。監査役等の多くはサイバーセキュリティの専門家ではないため、他の選択肢の回答のとおり、統括組織や責任者、役員等を通じた確認が行われている。なお、「6. サイバーセキュリティの外部専門組織への確認」はどの会社区分でもごくわずかであり、ほとんど実施されていない。

**③ 監査役会等での議論**（Q18-2）

監査役会（監査等委員会、監査委員会または監事会等）において、サイバーセキュリティについて議論しているか、記述形式で質問した。監査役会等を単なる報告の場ではなく、議論と提言の場として活用していくことが期待される。

**監査役会等でのサイバーセキュリティの議論の回答例（Q18-2）**

○重点監査項目に入れており、サイバーセキュリティに関する体制整備状況やインシデント発生時における対応状況等について、議長（常勤監査役）より報告し、議論等を実施している。

○CIO を監査等委員会に招聘し、対策等の検討状況を定期的に確認し、進捗や対応方針・結果の相当性を確認している。

○サーバーの移行、情報セキュリティ基本規程の制定、情報セキュリティ委員会の発足などイベントごとに、監査役会への活動報告で、現状認識やあるべき体制について意見交換し認識の共有を行ってきた。

○監査役会にて社外監査役から常勤監査役へ、平時対応と有事対応の進捗具合に関する質問があり、常に状況が共有されている。

○非常勤の社外取締役（監査等委員）が他社の元 CIO でサイバーセキュリティの知見を有しており、適宜助言を受けている。

○監査役会において、自社のサイバーセキュリティリスクの現状や、内部監査部門が実施した IT 監査の結果、および指摘事項に対する改善状況について共有を受け、監査意見の形成や経営陣への提言に向けた議論を行っている。

○グループガイドラインへの対応状況の報告、リスクアセスメント結果などの情報を共有し、対応計画等について意見を表明している。

○サイバーインシデント対応の必要性についての認識向上を目的とした資料を常勤監査役が策定し、経営者会議において説明を行った。それらの内容について監査役会において報告を実施した。

○当社のような規模の会社で、どこまで投資をしてサイバーセキュリティを実施するのかを念頭に置いて、関係部署も含め議論している。

○当社はサイバーセキュリティサービス提供会社であるため、執行側が専門家であり、アドバイスを行う部署も存在している。監査役の知識ノウハウ等は執行側よりも低いので、全体を俯瞰して漏れが起きないかを確認する観点で議論を行っている。

○監査役会の実効性評価の中でサイバーセキュリティについても議論している。

回答例にある監査役会等の実効性評価は、年間の監査活動の PDCA をより効果的なものとし、監査役会等の継続的な改善を図るという監査役会等の組織のパフォーマンスの向上が 1 つの狙いである[30]。監査役等も自社を取り巻くサイバーセキュリティリスクやその統制状況を適切に把握し、監査計画等に織り込み、監査の方法や監査体制についても見直しをして

[30] (公社)日本監査役協会ケース・スタディ委員会『「監査役会等の実効性評価」の実施と開示の状況』2024 年 11 月 12 日、29 頁。

いくこと、また監査役会等でサイバーセキュリティを議論する際にも、これを実効性評価・監査活動の振り返りの枠組みの中に位置付けることで、サイバーセキュリティに対する監査の実効性の継続的な向上につなげることができるであろう。

**④ 内部監査部門との連携**（Q18-3）

監査役等が内部監査部門からサイバーセキュリティについて報告を受けたり監査の指示をするなどの連携をしている会社は、全体で 48.7%であった（Q18-1）。連携の内容としては、内部監査部門の監査結果の報告を受けているケースが多いが、監査役等と内部監査部門で合同監査を実施している例、また内部監査部門以外の他の部門が監査している例などもあった（Q18-3）。内部監査部門でもサイバーセキュリティのガバナンスやリスク管理などについて評価対象としている場合があり[31]、連携することでより効率的・実効的な監査となる。以下に回答例を抜粋して紹介する。

なお、記述回答では、内部監査部門にもサイバーセキュリティの専門性のある人材は乏しいため、「形式的な監査に留まっており詳細な監査はできていない。」、「内部者による監査の限界と対応策について随時意見交換している。」といった意見も一定数みられた。社内での監査の限界を認識し、外部の専門家の知見を活用することも検討の余地があろう[32]。社内外の知見を組み合わせてサイバーセキュリティの監査の実効性を高めることが望まれる。

---

[31] 内部監査人協会（IIA）2025 年 2 月 5 日「サイバーセキュリティ　トピック別要求事項」とその「ユーザーガイド」では、サイバーセキュリティは一般的にビジネス・プロセスの一部であるため、内部監査人は、個々のアシュアランス業務を計画し、対象範囲を決定し、個々の内部監査業務を実施する際には、サイバー関連のリスクを評価する必要があるとしている。
https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement_japanese.pdf
https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_tr_user_guide_japanese.pdf

[32] 脚注 31「サイバーセキュリティ　トピック別要求事項　ユーザーガイド」2 頁では、「内部監査部門長は、内部監査部門がトピック別要求事項に関する個々の内部監査業務を実施するために必要な知識を有していないと判断した場合には、当該業務をアウトソーシングする場合もある。」としている。

**内部監査部門からの結果報告、意見交換の回答例（Q18-3）**

○内部監査項目にセキュリティ診断、脆弱性診断に関する実施、評価、対策に関する事項を設定しており、定期的に内部監査部門と意見交換を行っている。

○定期的な三様監査（監査役・内部監査・会計監査）連絡会などの場において、内部監査計画におけるサイバーセキュリティ関連の監査項目の確認や、実際の監査結果・改善勧告の進捗状況について報告を受け、連携を図っている。

○個人情報の取扱い・データ管理、セキュリティ対策の実効性等を内部監査の項目とし、その結果について報告を受けている。そのうえで担当部署等に確認を行っている。

○今後、内部監査の際にサイバーセキュリティのチェックシートの作成や方法についても連携して進めることを話し合っている。

**内部監査部門との合同監査の回答例（Q18-3）**

○インシデント対応の規程の周知と一般的なセキュリティ対応の監査を、内部監査と監査役監査で行っている。

○委託先往査を内部監査部門と合同で実施している。

○親会社からのチェックリストにもとづき内部監査がおこなわれており、これに立ち会っている。

**他の部門（IT 部門等または外部者）による監査の回答例（Q18-3）**

○IT 部門内にセキュリティ管轄チームが設置され、同チームが毎年当社グループ会社のサイバーセキュリティ監査を実施。同チームから監査役に監査の進捗、結果について月次報告が行われている。

○グループのシステム会社に依頼してセキュリティについての評価を実施。その報告を受けている。

○監査部が外部専門家を起用してセキュリティの脆弱性を点検しており、毎年、その結果を共有してもらっている。

○情報システム部門が ISMS 認証更新審査のために行う内部監査結果の報告を受ける。

○監査法人の IT 統制の監査状況を報告してもらっている。

○内部監査部門が情報セキュリティ監査を情報システム部門と連携して行っており、その報告が監査等委員会に対して行われている。

○総務・法務スタッフが ISMS 認証維持の一環として、サイバーセキュリティの内部監査を実施している。実施前に常勤監査役が十分内容の吟味を行い、必要に応じて監査担当者とディスカッションをしている。また内部監査の現場に同席し、後日課題を監査担当者に渡し、内部監査改善の後押しをしている。

### ⑤ 監査役等が参考にしているガイドライン（Q20）

経済産業省の「サイバーセキュリティ経営ガイドライン」が全体で 57.3%、プライム市場上場会社では 71.1%にのぼった。IPA の「中小企業の情報セキュリティ対策ガイドライン」は全体で 20.0%、プライム市場を除く他上場会社では 24.2%、特にグロース市場上場会社では 30.3%であった。

| Q20. 監査役等が参考にしているガイドライン等（%、複数選択可） | 全体 | プライム市場 | 資本金500億～ | 非上場 | 他上場 |
|---|---|---|---|---|---|
| 1. サイバーセキュリティ経営ガイドライン（経済産業省） | 57.3 | 71.1 | 67.9 | 48.6 | 59.2 |
| 2. NIST サイバーセキュリティフレームワーク（NIST） | 10.2 | 16.5 | 27.4 | 10.1 | 3.9 |
| 3. 中小企業の情報セキュリティ対策ガイドライン（IPA） | 20.0 | 12.1 | 6.0 | 22.2 | 24.2 |
| 4. ISO／IEC27000 シリーズ | 12.0 | 9.8 | 6.0 | 11.7 | 14.7 |
| 5. サプライチェーン強化に向けたセキュリティ対策評価制度（案）[33]（SCS 評価制度） | 5.3 | 6.7 | 6.0 | 4.0 | 6.2 |
| 6. その他 | 26.6 | 20.0 | 25.0 | 32.2 | 22.9 |
| （回答社数） | 1,193 | 315 | 84 | 572 | 306 |

中小規模会社の監査役等にとっては、IPA（独立行政法人情報処理推進機構）の「中小企業の情報セキュリティ対策ガイドライン」（第 4.0 版）[34]が実務上の出発点として特に有用であろう。同ガイドラインは経営者編と実践編から構成され、個人事業主や小規模事業者も含めて「できるところから始める」ことを想定している。具体的には、まず取り組むべき基本対策をまとめた「情報セキュリティ 6 か条」（OS やソフトの更新、ウイルス対策、パスワード管理、共有設定の見直し、バックアップの取得、脅威・手口を知ること）や、付録の「5 分でできる！情報セキュリティ自社診断」「情報セキュリティ基本方針（サンプル）」「中小企業のためのセキュリティインシデント対応の手引き」など、中小規模会社ですぐに活用できるツールが提供されている。また、これらの基本対策に取り組むことを企業自らが宣言する「SECURITY ACTION」制度（★一つ星・★★二つ星）は、補助金の申請要件となる場合もある。中堅・中小企業の監査役等は、自社がこうした実務的なガイドラインやツールを活用しているかを確認し、活用されていない場合には、その活用を促していくことが考えられる。

[33] SCS 評価制度（案）はアンケート実施当時のものである。現在は脚注 16 参照。

[34] https://www.ipa.go.jp/security/guide/sme/about.html

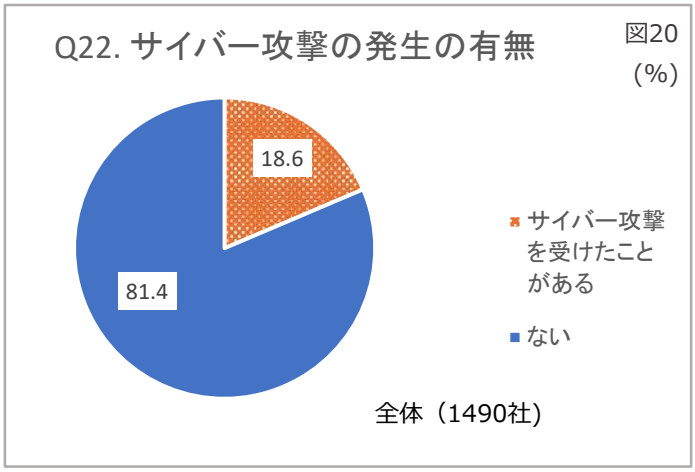
さらに、IPA からは「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」も公表されている[35]。この事例集は、126 社の中小企業を対象にした調査をもとに、脆弱性事例、被害事例、取組事例に分類した計 30 の事例が紹介されている。

このほか、記述回答で記載されたガイドラインとして、月刊監査役の連載「監査役等のためのサイバーセキュリティ入門」[36]、金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」[37]、経済産業省の「デジタルガバナンスコード 3.0」[38]、「システム管理基準」[39]「情報セキュリティ管理基準」[40]などが挙げられた。

### (8) サイバーインシデント発生後の対応

#### ① サイバーインシデント発生の有無（Q22、図 20）

サイバー攻撃により、重要業務の停止や大幅遅延、個人情報等の漏えいの懸念、外部通報・公表・当局への報告の検討、多額の損失や復旧費用が生じた場合など、事業に一定程度の影響を与えたサイバー攻撃を実際に受けたことがある会社は、全体で 18.6 %であった。




会社の規模が大きいほどその割合は増える傾向にあり、プライム市場上場会社では 31.5%、資本金 500 億円以上の会社では 36.5%が攻撃を受けていた。

当該サイバー攻撃の原因として（Q23）、75.2%が「マルウェア攻撃（ランサムウェア、ウイルス、ワーム、トロイの木馬等）」であり、次に「フィッシング」が 11.5%であった。

---

[35] https://www.ipa.go.jp/security/reports/sme/rcu1hd0000009k82-att/sme-jirei.pdf
また、月刊監査役 2026 年 10 月号（No.793）10-15 頁参照。

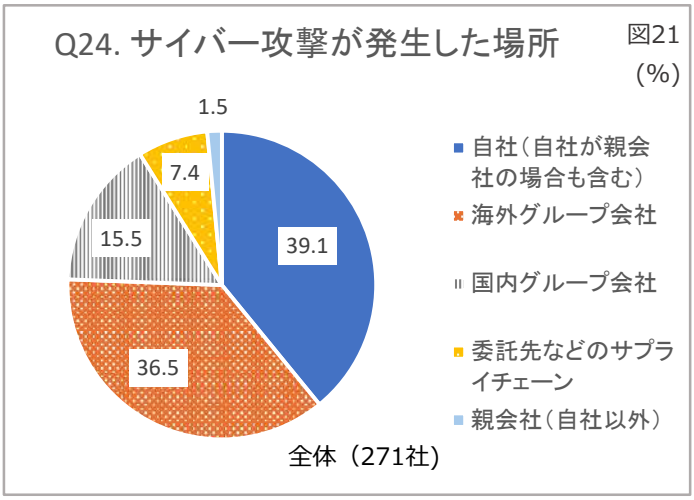
[36] 月刊監査役 2025 年 7 月号（No.777）～同年 12 月号(No.782)全 6 回。

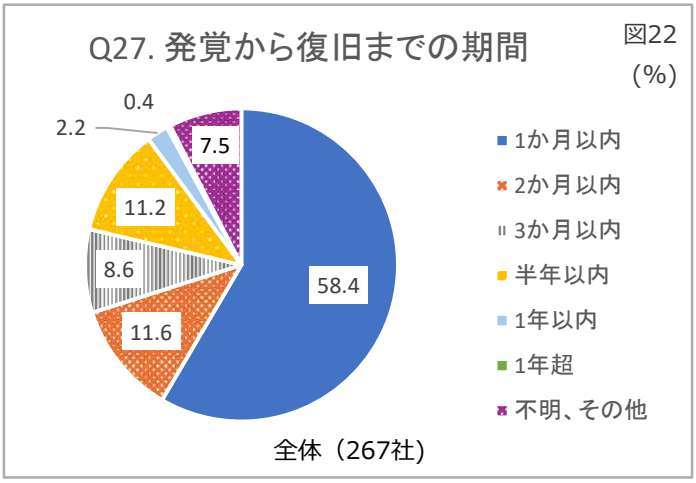
[37] https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf

[38] https://www.meti.go.jp/files/900016316.pdf

[39] https://www.meti.go.jp/policy/netsecurity/docs/secgov/2024_ZaimuHoukokuNiKakaruITTouseiGuidance.pdf

[40] https://www.meti.go.jp/policy/netsecurity/is-kansa/IS_Management_Standard_R7.pdf

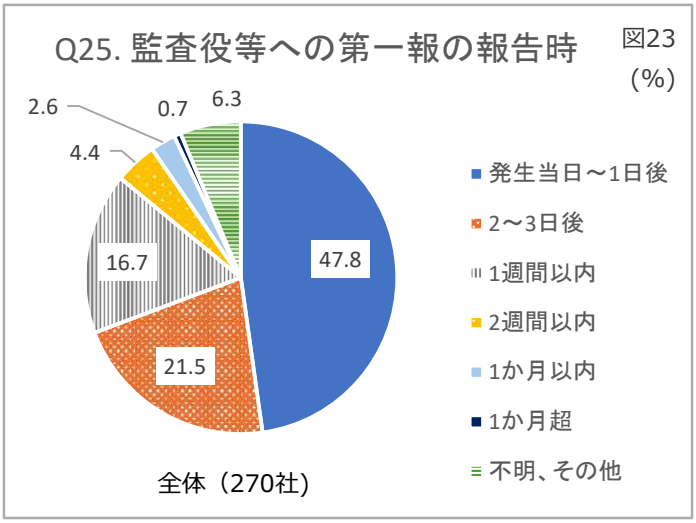


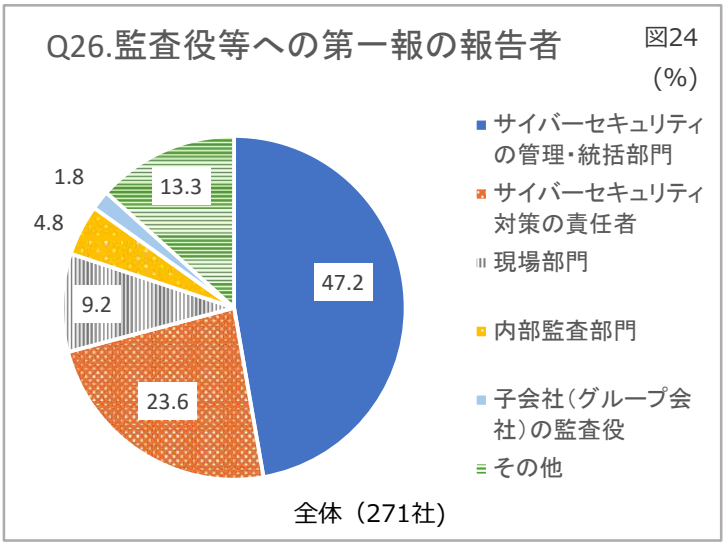

また、当該サイバー攻撃が発生した場所について（Q24、図 21）、「自社（自社が親会社の場合も含む）」が最多で 39.1%、次に「海外グループ会社」が 36.5%となった。会社の規模が大きいほど「海外グループ会社」の割合が増える傾向にあり、プライム市場上場会社では 55.6%になっている。

さらに、当該サイバー攻撃の発覚から復旧までにどの程度の期間がかかったか、製造やサービスなどが再開され、通常の業務運営にほぼ戻った状態までの期間について質問した（Q27、図 22）。 58.4%の会社が「1 か月以内」に復旧している。ただし、会社の規模が大きいほど 1 か月以上の割合が少し増加し、復旧までの期間が長くなりやすい傾向にある。

② 監査役等のサイバーインシデントの把握




監査役等が当該サイバー攻撃の第一報をどのタイミングで把握したかについては（Q25、図 23）、「発生当日～1 日後」までが 47.8%を占めており、会社がサイバー攻撃の発生を把握してからほぼ同じタイミングで監査役等にも第一報がある会社が半数近くに及んでいる。裏を返せば、半数近くの会社では監査役等への第一報が 2 日後以降にずれ込んでいる。なお、プライム市場上場会社では「発生当日～1 日後」が 40.8%とやや少なくなっている。




また、監査役等に対してサイバー攻撃の第一報を報告した者については（Q26、図 24）、「サイバーセキュリティの管理・統括部門」が 47.2%、「サイバーセキュリティ対策の責任者」が 23.6%であり、合計で 70.8%を占めている。

なお、実際にサイバー攻撃を受けた会社からは、有事における監査役等の関わり方（Q30）についても回答が寄せられた。有事対応を監視する監査役等の具体的な行動例（対策本部への出席・確認、モニタリング、個人情報保護委員会への報告[41]など）として参考になる。

**サイバーインシデント発生から復旧までの、執行側の課題の回答例（Q28）**

○インシデント発生時の対応手順が整備されていなかったため、復旧に想定以上の時間を要した。

○想定外の事象もあり、事前準備が難しい事象に対し混乱なく的確に対処する施策・対応力が課題。

○被害の全体を把握し理解できる人間がおらず、対応がその場しのぎになり、復旧や事業再開の優先順位が、声の大きい取締役の意見で進められていた。

○CSIRT での議論が浅く、安易に業務を再開してしまった。実被害がなかったため、検証よりも再開の要請が強かった。また、システム再開までの意思決定方法が曖昧で、役員への報告も遅れてしまった。

○非常災害の BCP はあったが、サイバーアタックを想定したものはなく、非常本部体制への移行、情報管理等ができず、情報が錯綜し、事実と推測の分離もできない混乱状況が半日ほど継続した。

○特に海外で発生した場合は初期対応を含め現地部門の対応・報告に委ねる部分が多く、全体像の把握までに時間を要してしまう。

○報告、対応状況、業務継続状況について現地からの報告が遅く、事実確認と影響度の把握に手間取った。海外現地での対応が主体になり、HD 情報システム部による統括もうまく機能しなかった。

[41] 個人情報取扱事業者は、取り扱う個人データの漏えい、滅失、毀損などの事態であって個人の権利利益を害するおそれが大きいものが発生したときには、個人情報保護委員会への報告義務がある。「速報」は事態を知った後速やかに行う報告（概ね 3～5 日以内）、「確報」は事態を知った日から 30 日以内に行う。これらの報告義務に加え、本人への通知義務もある。（個人情報保護法第 26 条 1 項・2 項、個人情報保護法施行規則第 7 条～10 条参照）

**復旧後、サイバーセキュリティリスク管理体制について見直された事項の回答例（Q29）**

○情報共有(エスカレーション)のスピードアップ。

○意思決定プロセスと責任の明確化。初期対応を厳密に規程。システム部門の権限の強化を検討。

○IT 部門の人員増加およびセキュリティリスクを管理する担当者を配置。

○委託先におけるサイバーセキュリティ管理体制を発注前に具体的に確認する手続きを追加した。

○海外グループ会社も含めたサイバー保険への加入、フォレンジック調査会社の事前選定、海外子会社への定期訪問・サイバーセキュリティ管理体制の確認。

**インシデント対策本部等と監査役等の関わり、監査活動の変化の回答例（Q30）**

○常勤監査役が対策本部の会議に出席し、社内外の被害状況を把握するとともに、復旧に向けた対策の有効性や進捗状況の確認を行い、毎月の監査役会にて社外監査役に情報共有を行った。

○取引先のインシデントだったため当社に対策本部は設置されなかったが、親会社の CSIRT が策定したチェックリストの運用状況を担当部署および内部監査部門と再確認した。

○対策本部は設置されなかったことから、常勤監査役は、ステークホルダーへの対応や担当部署のリカバリーのための出退勤状況、業務完遂状況などについて、直接各部署に確認した。

○監査役がインシデント発生時より対策本部に伴走し、対応マニュアルに従って適切に処理されているかを初動からしっかりとモニターし、担当役員に適宜助言を行ったことが、執行側の迅速で適切な対応に繋がったと評価している。サイバーセキュリティの重要度を再認識すると共に、今後リスク管理の整備・運用状況をどのように監査すべきかを検討課題としている。

○予め設定されていた対応プロセスに則っているかの監視と、インシデントを通して顕在化した対応プロセスの課題への対処について、後日監査で確認した。また、インシデントが発生した海外関係会社の往査時に改めて説明を受け、日本本社側のサポートの課題の有無について確認した。

○個人情報漏えいの懸念がある場合は、個人情報保護委員会への報告、HP での公表や個別メールでの顧客告知の実施などについて、適宜執行側にアドバイスをしている。

## 4. サイバーセキュリティに対する監査役等の着眼点と対応

本アンケート結果からは、多くの会社においてサイバーセキュリティに対する経営陣の危機意識が高まり、従業員への周知や教育に取り組んでいることがうかがえる（Q2、Q7、Q14）。しかしその一方で、取締役会等における経営課題としての議論、リスク評価、BCPの策定・運用、グループ会社・取引先（委託先等）を含むサプライチェーン管理、監査役等によるフォローアップには、会社規模により実施の有無や成熟度に差がみられる（Q1、Q9、Q11～Q13、Q16など）。

サイバーセキュリティは、もはや情報システム部門のみの課題ではなく、事業継続、企業価値、ステークホルダーからの信頼に直結する経営上の重要リスクである。このような状況を踏まえ、監査役等には以下の事項を重点的に確認し、必要に応じて取締役会、経営陣、関係部門に対して改善を促していくことが期待される。ただし、監査役等が全ての着眼点について直接確認することが求められるのではなく、内部監査部門等による監査結果の確認、サイバーセキュリティの専門組織や情報セキュリティ部門等への確認などを通して、状況を把握していくことが考えられる。

なお、以下の事項は大企業から中小規模会社まであらゆる企業・組織を念頭に置いたものであるが、中小規模会社や株式会社以外の組織においては、限られた人材・予算の中で、全てを一度に実施することは現実的ではないであろう。まずは、「責任者の明確化」、「基本方針の策定・周知」、「従業員教育」、「データのバックアップ」、「最低限のインシデント対応手順の整備」、といった基本的なことから着実に取り組み、自社のリスクと規模に応じて段階的に高度化していくことが現実的である。本アンケートでは各設問の選択肢を段階別（レベル別）に設計しているため、監査役等は、自社が現在どの段階にあり、次に何に取り組むべきかを把握した上で、自社の状況に合った着実な前進を促していくことが期待される。

### (1) サイバーセキュリティが経営課題となっているか

サイバーセキュリティを経営課題として取り扱うことが出発点となるため、監査役等は、取締役会においてサイバーセキュリティが重要な経営リスクとして認識され、継続的に議論・監督されているかを確認することが求められる。具体的には、インシデント件数や主要施策の進捗といった定例報告に加え、事業戦略、リスク評価、投資判断、人的資源配分、グループ管理との関係で議論されているかを確認することが望まれる。社外取締役からの多角的な視点や他社比較に基づく意見の共有も有効であろう。

また、サイバーセキュリティの施策について、CISOなどの責任者、サイバーセキュリティの専門組織あるいはリスク管理委員会等から取締役会に適切に報告されているかなど、取締役会にサイバーセキュリティリスクが上程されるプロセスについても、改めて確認する

ことが望まれる[42]。

もし取締役会等で十分な議論が行われていない場合には、監査役等から、定期的な報告機会の設定や、CISO・CIO・リスク管理部門等による説明の実施を促すことが考えられる。

**着眼点の例**

- サイバーセキュリティリスクが全社的に重要な経営リスクとして位置付けられているか
- 取締役会で定期的に報告・議論されているか
- 経営戦略や事業継続、企業価値の観点から議論されているか
- 経営トップが必要な指示・関与を行っているか
- サイバーセキュリティ投資はリスク評価や中長期戦略との関係で検討されているか

など

### (2) サイバーセキュリティリスク管理体制の整備・運用状況の確認

アンケート結果では、サイバーセキュリティの責任者を定め、社内にセキュリティ対応方針を周知している会社が多くみられる一方（Q5、Q7）、責任組織の設置、体系的なリスク評価やセキュリティ対策の実施には差がみられる（Q6、Q8～Q10）。サイバーセキュリティへの監査役等の対応においては、個別の技術対策よりも、リスク管理体制が適切に構築され、実際に機能しているかの確認が重要である。監査役等は、サイバーセキュリティのガバナンス体制やリスク管理体制が構築・運用されているかをモニタリングし、不十分な場合は執行側に働きかけていくことが求められる。

**着眼点の例**

- サイバーセキュリティ担当組織や最終責任者とその役割が明確か。権限と情報が責任者に集約されているか
- サイバーセキュリティのリスク評価が（定期的に）行われているか。事業への影響を踏まえて適切に行われているか
- 内部監査部門等によるモニタリング、検証が行われているか
- 内部監査、第三者評価、脆弱性診断等の結果が改善につながっているか
- 重要リスクが経営層へ報告されているか、投資判断や対策計画に反映されているか
- 役職員への教育・研修は実施されているか

など

[42] 脚注 28 参照。

### ⑶「侵入後」を想定した有事対応体制が整備されているか

アンケート結果では、サイバーインシデントに関する BCP を策定済みの会社がある一方、未策定または策定中・検討中の会社も相当数存在した（Q12）。また、研修や標的型攻撃メール訓練は比較的実施されているが、復旧演習、バックアップデータの復元訓練、組織横断型演習、侵入テストなど、実践的な訓練は限定的である（Q14）。サイバー攻撃を完全に防ぐことは困難であり、多くの企業は侵入後の対策を重視し始めている。監査役等は、侵入後の初動対応、報告、意思決定、復旧、対外公表、再発防止までを含めた計画が構築されているか、構築する目途がたっているかを確認することが考えられる。また、整備状況の確認にとどまらず、訓練や検証結果等を通じて実効性が検証されているかまで確認することが望ましい。

**着眼点の例**

- ランサムウェア等を想定したサイバーインシデントの BCP が策定されているか
- BCP は文書化にとどまらず、訓練結果や他社事例を踏まえて見直されているか
- 侵入後を想定したインシデント対応訓練が実施されているか
- バックアップ体制や復旧手順の有効性が検証されているか
- インシデント発生時に社内や監査役等へ速やかに報告されるルートが明確か
- 訓練結果が BCP や復旧手順の改善につながっているか

など

### ⑷ グループ会社・海外拠点、取引先（委託先等）を含むサプライチェーン全体での対策がなされているか

アンケート結果では、サイバー攻撃が発生した場所として、自社のほか海外グループ会社が多く挙げられていた（Q24）。他方、グループ会社のサイバーセキュリティ対策状況等は把握されていない会社が一定数存在している（Q11）。

特に最近のサイバー攻撃は、企業本体よりもセキュリティの弱い海外子会社や取引先（委託先等）を攻撃対象にするケースが多くみられる。監査役等は、自社（親会社）の対策が十分かだけではなく、グループ全体として管理されているかを確認することが求められる。子会社は人材やリソースが限られている場合があるため、親会社が主導して、グループ会社にサイバーセキュリティの支援をしていくことが必要である[43]。グループ会社、海外拠点、重要な取引先（委託先等）を含めたサプライチェーン全体のリスク管理状況を確認することが望まれる。

また、取引先（委託先等）のサイバーセキュリティ体制・対策について、監査役等が確認

[43]（公社)日本監査役協会ケース・スタディ委員会『グループ・ガバナンスと監査役等の監査について』2025 年 11 月 11 日、34 頁。

していない、または報告を受けていない会社も多く、サプライチェーンでの対策の難しさが表れている（Q16-1）。監査役等としては、まずは取引先（委託先等）の管理や契約などについて、サイバーセキュリティの管理・統括部門や内部監査部門などから報告を受ける仕組みを作ることが考えられる。

**着眼点の例**

- グループ共通のセキュリティ方針・対策が整備されているか
- 重要なグループ会社や海外拠点のセキュリティ状況が把握されているか
- 子会社・グループ会社からのインシデント報告体制が構築されているか。監査役等への報告も明確にされているか
- 取引先（委託先等）の管理の仕組みがあるか。取引先（委託先等）の範囲、重要性、優先順位が整理されているか
- 取引先（委託先等）との契約に、セキュリティ対策、報告義務、再委託管理、監査権限等が定められているか
- 取引先（委託先等）へのアンケート等による確認が形式的な自己申告にとどまっていないか
- 取引先（委託先等）でインシデントが発生した場合の連絡・復旧・代替手段が検討されているか

など

### (5) 監査計画・重点監査項目へのサイバーセキュリティの反映

アンケート結果では、サイバーセキュリティを監査計画に組み込んでいる会社がある一方、監査計画には入れていない会社（監査は実施する予定）や、監査対象にはしていない会社も多数みられる（Q17-1）。その要因として、監査対象となるサイバーセキュリティリスク管理の体制が不十分であることや（Q6、Q8）、会社としてサイバーセキュリティのリスク評価が十分に実施されていないことが考えられる（Q9-1）。監査役会等は執行側のリスク評価をそのまま受け入れるのではなく、監査役会等からもサイバーセキュリティが経営上の重要なリスクであることを助言し、経営陣・執行側のリスク認識の妥当性やリスクの評価プロセスの適切性などを改めて確認し、リスク評価を促していくことが重要である[44]。その上で、自社のリスク状況に応じて監査計画または重点監査項目に位置付けていくことが求められる。

[44] 脚注 28 参照。

また、グループ会社でサイバーセキュリティのリスク認識を含めた統一的な監査の視点を形成するために、グループ監査役連絡会などでサイバーセキュリティの体制や対策状況、監査計画についても対話していくことが求められる[45]。

さらに、単発的な確認ではなく、リスク状況の変化に応じて継続的に監査を実施していくことが考えられる。監査役会等は、実効性評価や監査活動の振り返り（PDCA）の機会において、サイバーセキュリティのような新たな経営リスクが監査計画・重点監査項目に適切に反映されているか、また経営環境の変化に応じて見直されているかを、継続的に点検していくことが望まれる[46]。

**着眼点の例**

- 執行側のサイバーセキュリティのリスク評価は適切か
- 当年度の監査計画にサイバーセキュリティを含める必要があるか
- 内部監査部門の監査計画にサイバーセキュリティ関連項目が含まれているか
- 監査役等は内部監査部門、IT 部門、リスク管理部門、外部専門家と適切に連携しているか
- 専門的事項について、適切な専門家の評価・知見を活用できているか
- 監査結果が次年度の監査計画へ反映されているか

など

### (6) 有事での対応体制の監査、有事における監査役等自身の対応

近年のサイバー攻撃の高度化・巧妙化により侵入を完全に防ぐことはますます難しくなり、侵入後の対応を重視する対策が主流となっている。監査役等は、インシデント発生後の初動対応、報告体制、意思決定体制および外部公表等について、執行側の対応を確認することが望ましい。

また、アンケート結果では、サイバー攻撃発生時に監査役等への第一報が発生当日から 2 日目以降となった会社が半数超であった（Q25）。有事において監査役等は、執行側の初動対応や様々な意思決定の相当性を監視する立場にある。そのため、平時から、有事における監査役等への報告ルート、監査役会等での情報共有、社外監査役等への連絡方法、取締役会・経営会議への関与方法を確認しておくことが考えられる。

---

[45] 脚注 44、36 頁。

[46] 脚注 28 参照。

**着眼点の例**

- 重大インシデントの報告基準、社内での報告ルートが明確か
- 初動対応体制が整備されているか
- インシデント発生時に監査役等へ誰が、いつ、何を報告するかが明確か
- 監査役等は初動対応において何を確認するかを整理しているか
- 対外公表、顧客対応、当局対応、原因究明、再発防止策について、監査役等が確認すべき事項を想定しているか

など

## 5. おわりに

本報告書では、監査役等からみたサイバーセキュリティに対する企業の取組み状況と、監査役等の対応の状況、課題と工夫について、アンケート調査結果をもとに考察し監査上の着眼点を取りまとめた。

調査結果からは、サイバーセキュリティが企業経営における重要リスクとして広く認識されるようになってきたことがうかがえた。経営陣の危機感は十分に高まっており、監査役等も取締役会や経営陣に対して意見を述べるなど、一定の関与をしている姿勢がみられた。一方で、その危機意識の高まりが、経営課題としての議論や実効性あるリスク管理体制の構築・運用にまで必ずしも十分に結びついてはいない状況も明らかになった。特に、グループ会社を含めた管理体制、有事を想定した訓練や BCP の運用、取引先（委託先等）のサプライチェーンの管理には、なお改善の余地がみられる。

サイバーセキュリティは技術的専門性の高い分野であり、「専門家ではない自分に何ができるのか」と感じる監査役等も少なくないであろう。しかし、監査役等に求められているのは、個々の技術対策の良し悪しを自ら判断することではない。サイバーセキュリティが一部門に委ねられた技術的課題ではなく、取締役会等において継続的に議論・監督されるべき経営課題として位置付けられているか、これに対応するガバナンスおよびリスク管理体制が適切に整備・運用され、実際に機能しているかを監査することが重要である。

そのため、監査役等には、「サイバーセキュリティが経営課題として十分に議論されているか」「リスク評価が体制整備、資源配分および経営判断に生かされているか」「侵入後を想定した BCP・訓練・有事対応は実効的なものとなっているか」「グループ会社や取引先（委託先等）まで視野に入っているか」といった問いかけを、執行側に継続的に投げかけることが求められる。そして、これらの視点が監査計画や重点監査項目に適切に反映されているかを確認し、監査役会等の実効性評価や監査活動の振り返りも活用しながら、サイバーセキュリティに対する監査の実効性を継続的に高めていくことが望まれる。アンケートの自由記述においても、監査役等の問題提起を契機として体制整備や訓練の充実、リスク評価の見直しなどが進んだ事例がいくつもみられたことは大きな示唆を与えている。

また、本アンケートでは、多くの設問において、スタンダード市場・グロース市場を中心とする上場会社（本報告書における「他上場会社」）では、プライム市場上場会社や資本金 500 億円以上の会社と比較し、取組みの成熟度が相対的に低い項目がみられた。経営課題としての議論、専門組織の整備、リスク評価、侵入後を想定した実効的対応、グループ会社・取引先（委託先等）の管理など、多くの項目で差が生じている。もっとも、必要な対策の内容や水準は、企業規模や上場区分だけでなく、業種、事業内容、保有する情報資産および想定されるリスク等に応じて異なる。各社の監査役等には、本アンケート結果を他社との比較だけではなく、自社の現状を見つめ直し、優先的に着手すべき課題を検討するために活用し

ていただきたい。サイバーセキュリティ対策は、必ずしも大規模な投資から始まるものではない。取締役会で経営課題として継続的に議論されているか、責任者や報告ルートが明確か、有事訓練が実施されているかといったガバナンスの基本を確認することから始めることができる。

さらに、今後は AI（人工知能）の発展がサイバーセキュリティをめぐる環境を大きく変えていく。生成 AI の利用により、サイバー攻撃の高度化・巧妙化をもたらす一方、ログ分析、異常検知、脆弱性管理、インシデント対応支援など、防御の高度化にも活用され得る。その上、フロンティア AI と呼ばれる最先端で高性能な汎用 AI モデルの発展により、攻撃と防御の双方が進化する時代になるといわれている。本アンケートでは AI 利用に関する十分な調査を行っていないため、具体的な対応は今後の検討課題となるが、監査役等も、AI に伴う新たなリスクと機会について経営陣がどのように認識し、管理しているかという観点から注視していくことが求められるであろう。

サイバーセキュリティに終わりはない。新たな技術が生まれれば新たな脅威も生まれ、対策を講じれば攻撃手法もまた変化する。本報告書の取りまとめ時期である 2026 年秋においても、国内では、企業や団体の Web サービス、業務システム、取引先（委託先等）への不正アクセスにより、個人情報の漏えいや業務への影響が公表される事案が相次いでいる。とりわけ、取引先（委託先等）への攻撃が複数の企業・組織へ波及する事案もみられ、サイバーセキュリティが自社のみの問題にとどまらないことを改めて示している。だからこそ、一度体制を整備しただけで十分とするのではなく、リスクの変化を把握し、対策の実効性を継続的に検証・改善することが求められる。監査役等には、自社を取り巻く環境変化に関心を持ち続け、経営陣との対話を通じて、サイバーセキュリティが真に経営課題として扱われているかを問い続けていただきたい。本報告書が、各企業・組織におけるサイバーセキュリティガバナンスの向上と、監査役等による実効性ある監査活動の一助となれば幸いである。

以上

## 第 53 期　ケース・スタディ委員会　委員

| | | | |
|---|---|---|---|
| 委 員 長 | 花岡　幸子 | 株式会社大和証券グループ本社 | 取締役監査委員 |
| 専門委員 | 渡辺　邦広 | 森・濱田松本法律事務所 外国法共同事業 | 弁護士 |
| 委　　員 | 永井　健藏 | LE.O.VE 株式会社 | 常勤監査役 |
| 委　　員 | 石原　基康 | プレミアアンチエイジング株式会社 | 常勤監査役 |
| | | 一般社団法人日本内部監査協会 | 監事 |
| 委　　員 | 竹川　浩史 | 京王電鉄株式会社 | 取締役監査等委員 |
| 委　　員 | 松崎　裕之 | 株式会社東京証券取引所 | 常勤監査役 |
| 委　　員 | 新熊　　聡 | 株式会社いつも | 取締役常勤監査等委員 |
| 委　　員 | 堤　あづさ | DOWA ホールディングス株式会社 | 常勤監査役 |
| 委　　員 | 後藤　敏文 | 公益社団法人日本監査役協会 | 専務理事 |
| 事 務 局 | 公益社団法人日本監査役協会企画部企画課 | | |
| | 横野 能将　佐藤 秀和　渡邉 彩子　新井 義洋　小西 真理 | | |
| | 岡田 倫太郎　山岡 翔輝 | | |