サイバーリスクに関する取締役会ガバナンスの原則

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー　**綾部 泰二**

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー　**川本 大亮**

はじめに

本稿では、2021年3月に世界経済フォーラムにて公開されたサイバーセキュリティのための取締役会ガバナンス原則を解説していきます。まずは、前提となるコーポレートガバナンス・コードとは何か、サイバーセキュリティ対策とどのような関係があるのかを簡単に触れた上で、サイバーセキュリティのための6つの取締役会ガバナンス原則について解説します。

1 コーポレートガバナンス・コードとは何か

2014年6月、日本政府が発表した成長戦略「『日本再興戦略』改訂2014年」※1では、日本企業の「稼ぐ力」をより高めていくために「コーポレートガバナンス（企業統治）」を強化する重要性が明示されました。そして、コーポレートガバナンスを実践するための原則・指針として、金融庁と東京証券取引所を事務局として原案を作成し、2015年3月に公表したものが「コーポレートガバナンス・コード原案」※2（以下、「本コード」と言う）です。

本コードにおけるコーポレートガバナンスは「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組み」を意味しており、コーポレートガバナンスに資する原則が提示されています。

本コードには、次の2つの特徴が存在します。

1. **プリンシプルベース・アプローチ**
   本コードにおいて示されている規範は、基本原則、原則、補充原則から構成されていますが、会社の規模や業種等さまざまであるため、会社が取るべき行動を詳細に規定する「ルールベース・アプローチ」（細則主義）ではなく、会社の置かれた状況に合わせて実効的なコーポレートガバナンスを実現するという観点から、「プリンシプルベース・アプローチ」（原則主義）が採用されています。
2. **コンプライ・オア・エクスプレイン**
   本コードは、法令と異なり法的拘束力を有する規範ではなく、その実施にあたっては「コンプライ・オア・エクスプ

※1　日本経済再生本部「『日本再興戦略』改訂2014 ―未来への挑戦―」（2014年6月24日）
https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/honbun2JP.pdf
※2　金融庁「コーポレートガバナンス・コード原案 ～会社の持続的な成長と中長期的な企業価値の向上のために～」（2015年3月5日）
https://www.fsa.go.jp/news/26/sonota/20150305-1/04.pdf

レイン」（原則を実施するか、実施しない場合には、その説明をするか）の手法が採用されています。本コードの各原則（基本原則・原則・補充原則）の中に、自らの個別事情に照らして実施することが適切でないと考える原則があれば、それを「実施しない理由」を十分に説明することにより、一部の原則を実施しないことも想定しているものとなっています。

また、本コードは、以下の5点を基本原則[※3]として、その目的にしています。

- **基本原則1**：株主の権利・平等性の確保
  - ・株主の実質的な平等の確保を実施する。
- **基本原則2**：株主以外のステークホルダーとの適切な協働
  - ・株主以外の従業員、顧客、取引先、債権者、地域社会といったさまざまなステークホルダーとの適切な共同を実施する。
- **基本原則3**：適切な情報開示と透明性の確保
  - ・会社の財務情報だけではなく、非財務情報についても主体的に開示を実施する。
- **基本原則4**：取締役会等の責務

  取締役会の責務として下記を実施する。
  - ・企業戦略等の大きな方向性を示すこと
  - ・経営陣幹部による適切なリスクテイクを支える環境整備を行うこと
  - ・独立した客観的な立場から、経営陣（執行役およびいわゆる執行役員を含む）・取締役に対する実効性の高い監督を行うこと
- **基本原則5**：株主との対話
  - ・株主総会以外の場でも、株主と対話を実施する。

2 コーポレートガバナンス・コードとサイバーセキュリティ対策の関係

近年サイバーセキュリティインシデントが多くの企業で発生し、会計監査の世界でも監査上重要な検討事項となってきています。また、後述する世界経済フォーラムのレポートでも、サイバーセキュリティへの対応が重要な経営課題として挙げられています。前述した「コーポレートガバナンス・コード」の観点からサイバーセキュリティ対策を考えた場合、次の3つの原則について検討事項が存在します。

基本原則2［株主以外のステークホルダーとの適切な協働］

上場会社は、会社の持続的な成長と中長期的な企業価値の創出は、従業員、顧客、取引先、債権者、地域社会をはじめとするさまざまなステークホルダーによるリソースの提供や貢献の結果であることを十分に認識し、これらのステークホルダーとの適切な協働に努めるべきである。

取締役会・経営陣は、これらのステークホルダーの権利・立場や健全な事業活動倫理を尊重する企業文化・風土の醸成に向けてリーダーシップを発揮すべきである。

基本原則2の「考え方」には、次のように記されています。

「持続可能な開発目標」（SDGs）が国連サミットで採択され、気候関連財務情報開示タスクフォース（TCFD）への賛同機関数が増加するなど、中長期的な企業価値の向上に向け、サステナビリティ（ESG要素を含む中長期的な持続可能性）が重要な経営課題であるとの意識が高まっている。こうした中、わが国企業においては、サステナビリティ課題への積極的・能動的な対応を一層進めていくことが重要である。

多くのステークホルダーへ影響を及ぼしかねないサイバー攻撃に備えることはサステナビリティ課題・経営課題の1つであると考えられるため、基本原則2のステークホルダーとの適切な協働の観点からも、サイバーセキュリティへの対応は必要だと想定されます。

基本原則3［適切な情報開示と透明性の確保］

上場会社は、会社の財政状態・経営成績等の財務情報や、経営戦略・経営課題、リスクやガバナンスに係る情報等の非財務情報について、法令に基づく開示を適切に行うとともに、法令に基づく開示以外の情報提供にも主体的に取り組むべきである。

その際、取締役会は、開示・提供される情報が株主との間で建設的な対話を行う上での基盤となることも踏まえ、そうした情報（とりわけ非財務情報）が、正確で利用者にとって分かりやすく、情報として有用性の高いものとなるようにすべきである。

※3 東京証券取引所「コーポレートガバナンス・コード ～会社の持続的な成長と中長期的な企業価値の向上のために～」（2021年6月11日）
https://www.jpx.co.jp/news/1020/nlsgeu000005ln9r-att/nlsgeu000005lne9.pdf

基本原則3は、財務情報だけではなく、会社の財政状態、経営戦略、リスク、ガバナンスや社会・環境問題に関する事項（いわゆるESG要素）などの非財務情報の開示も求められています。2021年6月の改正においては、補充原則3-1③が追加され、「上場会社は、経営戦略の開示に当たって、自社のサステナビリティについての取組みを適切に開示すべきである。また、人的資本や知的財産への投資等についても、自社の経営戦略・経営課題との整合性を意識しつつ分かりやすく具体的に情報を開示・提供すべきである」としています。

近年の「コーポレートガバナンス・コード」の改訂や、その背景にある考え方を踏まえると、企業の非財務的な情報開示が重要視される傾向にあることがわかります。さらに、サイバーセキュリティ対策についても、経営戦略・経営計画の一環として「コーポレートガバナンス・コード」の付属文書である「投資家と企業の対話ガイドライン」で機関投資家と企業の対話において重点的に議論することが期待される事項として挙げられています。このような状況から、企業が開示する非財務的な情報にはサイバーセキュリティ対策を含めることが望ましいと考えられます。

基本原則4［取締役会等の責務］

上場会社の取締役会は、株主に対する受託者責任・説明責任を踏まえ、会社の持続的成長と中長期的な企業価値の向上を促し、収益力・資本効率等の改善を図るべく、

(1) 企業戦略等の大きな方向性を示すこと

(2) 経営陣幹部による適切なリスクテイクを支える環境整備を行うこと

(3) 独立した客観的な立場から、経営陣（執行役及びいわゆる執行役員を含む）・取締役に対する実効性の高い監督を行うこと

をはじめとする役割・責務を適切に果たすべきである。

こうした役割・責務は、監査役会設置会社（その役割・責務の一部は監査役及び監査役会が担うこととなる）、指名委員会等設置会社、監査等委員会設置会社など、いずれの機関設計を採用する場合にも、等しく適切に果たされるべきである。

また、補充原則4-2②では、取締役会の責務として「取締役会は、中長期的な企業価値の向上の観点から、自社のサステナビリティを巡る取組みについて基本的な方針を策定すべきである。また、人的資本・知的財産への投資等の重要性に鑑み、これらをはじめとする経営資源の配分や、事業ポートフォリオに関する戦略の実行が、企業の持続的な成長に資するよう、実効的に監督を行うべきである」としています。前述のとおり、サイバーセキュリティ対策は、サステナビリティや経営戦略の一環で情報開示が求められていることから、同様に取締役には実際にサイバーセキュリティ対策に取り組む責務があると考えられます。

さらに、補充原則4-3④では、「内部統制や先を見越した全社的リスク管理体制の整備は、適切なコンプライアンスの確保とリスクテイクの裏付けとなり得るものであり、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し、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」としています。内部統制やリスク管理体制の構築を通じて、サイバーセキュリティ対策を実施することが、取締役の責務であると考えられます。

これまで見てきたとおり、株主以外のステークホルダーとの適切な協働、情報開示および取締役会等の責務といった観点からも取締役はサイバーセキュリティ対策に取り組む必要があります。一方で、「コーポレートガバナンス・コード」では具体的な取り組み方法が厳格に決められているわけではないため、当該内容は有効に機能していないという意見も存在します。それでは、取締役は具体的にどのようなことを念頭にサイバーセキュリティ対策に取り組むべきでしょうか。世界経済フォーラムで発表された6つの原則が指針になると考えられます。

3 世界経済フォーラムにて公開された6つの原則

2020年3月、世界経済フォーラム（WEF）は、PwCや全米企業取締役協会、インターネット・セキュリティ・アライアンスと協力し、「サイバーリスクに関する取締役会ガバナンスの原則」※4を発表しました。このレポートでは、ガバナンスの原則だけではなく、今後12か月で会社に最大の影響を与えると予想される5つのトレンドの1つとして、「サイバーセキュリティ脅威の変化」が示されており、取締役が取り組むべき重要な課題として示されています。さらに、レポートではサイバーリスクに関する取締役会ガバナンスの原則として、以下の6つの原則が提唱されており、組織が戦略的目標の推進とサイバーレジリエンスの確立を共に達成するにあたり、取

※4 World Economic Forum, Principles for Board Governance of Cyber Risk, 2021 https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk

締役会が効果的なガバナンスを発揮することを支援するように設計されています。

原則1：サイバーセキュリティは戦略的なビジネスイネーブラーである

サイバーセキュリティへの対応は、今や業界を問わずすべての組織にとって重要な経営リスクとなっています。組織の効果的なサイバーセキュリティ対応を実現すべく、取締役会は、サイバーセキュリティの意思決定に関するリーダーシップの発揮、およびサイバーセキュリティへの対応を積極的に推し進める企業文化の醸成に貢献することが求められます。そのため取締役会は、主要な業務上および戦略上の意思決定時、さらにはデジタルトランスフォーメーション等の新たな企業の取り組みの意思決定時に、サイバーセキュリティの問題を重要な経営リスクの一部として分析および検討を行うだけでなく、サイバーセキュリティへの対応を市場における差別化要因として利用するよう積極的に経営陣に働きかけていくことが望まれます。

取締役会での主な検討事項

- 取締役会の議題としてサイバーリスクを定期的に取り上げるなど、主要な業務上および戦略上の意思決定プロセスでサイバーリスクを考慮するようにする
- 新しいデジタルトランスフォーメーションの主要な取り組みをサイバーリスクの観点から検討する
- どの取締役会委員会がサイバーリスクの問題を主に監督すべきかを決定する
- サイバーセキュリティの問題を、企業リスクの一部として分析する。さらに、サイバーセキュリティの問題に関する事業戦略やビジネスモデルの考慮事項を分析する
- サイバーセキュリティを市場の差別化要因やビジネスドライバーとして利用する機会を特定するよう経営陣に求める

原則2：サイバーリスクの経済的要因と影響を理解する

組織はビジネス上の意思決定においてサイバーリスクを考慮する際に、組織の財務上の影響に焦点を当てる必要があります。取締役会は、意思決定に必要なサイバーリスク許容度を財務的に定義し、組織がサイバーリスク許容度を確立することが望まれます。また、リスクシナリオの影響と発生可能性を見積もるためのフレームワークの確立や、サイバーリスクの業界標準の比較測定基準の調査等を経営陣に要求することで、組織のサイバーリスク管理の意思決定を支援することの必要性についても述べています。

取締役会での主な検討事項

- 経営陣が以下の検討事項を確認することにより、組織のサイバーリスク許容度を見直し、承認する
  - 定期的なリスク管理の枠組みの一環として、特定したサイバーリスクの根拠（顧客、財務、レピュテーション、その他の関連する影響等）を確認する
  - 意思決定に必要なサイバーリスク許容度を財務的に定義し、サイバーリスク管理のパフォーマンスを測定するための主要な指標を開発する
  - 組織のリスクプロファイルに合致するサイバーリスクシナリオを特定し、リスク許容度を確立することを目的としたプログラムを導入する
- サイバーセキュリティシナリオの潜在的な経済的影響と可能性を計算するために、業界で認められているリスク定量化モデルを使用して、一貫したフレームワークを確立するよう経営陣に指示する
- サイバーリスクの業界標準の比較測定基準の継続的な調査を要求する
- リスク事象の潜在的な影響と可能性、および機能的な損失やエクスポージャーに基づいて、サイバーリスク管理の意思決定を行う

原則3：サイバーリスクマネジメントをビジネスニーズに合わせる

サイバーリスクへの対応時には、組織はビジネスニーズと定義されたリスク許容度との整合性を明確にすることが求められます。取締役会は、組織の事業戦略と推進要因（デジタル成長など）を、サイバーリスクへの影響を考慮して批判的に検討する必要があります。また、経営陣に対して、自身のサイバーセキュリティへのコミットメントやサイバーリスク管理の計画、サイバーリスクの重要性の判断基準といった事項について取締役会に報告するよう要求することで、組織のサイバーセキュリティ活動に対して効果的なガバナンスを発揮することが求められます。

取締役会での主な検討事項

- 組織の事業戦略と推進要因（デジタル成長など）を、サイバーリスクへの影響を考慮して批判的に検討する
- 経営陣に対し、関連するサイバーリスク、リスクオーナーシップ、企業リスク管理プログラムとの整合性、サイバーリスクに関する意思決定の追跡方法など、自らの活動のサイバーセキュリティへの影響について取締役会に報告するよう求める

- 経営陣に対して、十分に開発され、文書化され、テストされた計画を取締役会に報告するよう求める
- 経営陣に対し、重要なビジネス上の意思決定にサイバーリスク分析を統合し、情報の質と包括性を効果的に保証することを求める
- 経営陣に対し、規制上の義務を果たすために会社がリスクの重要性をどのように判断するかについてのロードマップを取締役会に提供するよう求める

原則4：組織設計がサイバーセキュリティをサポートするようにする

組織は、明確なオーナーシップ、権限、重要業績評価指標（KPI）を定義することで、企業全体でサイバーセキュリティに対処する内部ガバナンス構造を設計する必要があります。ガバナンスの設計にあたって、取締役会は、サイバーセキュリティに関する組織構造、役割およびリソースの配分といった事項について、積極的に監視および提言を行うことで、効果的なガバナンスを発揮することが求められます。加えて、取締役会は、サイバーセキュリティに関する利害関係者間のコラボレーションを促進し、組織のサイバーセキュリティ文化の醸成に貢献することも求められます。

取締役会での主な検討事項

- 組織構造を見直し、サイバーセキュリティ機能が事業、社内グループ、リーダーシップ全体で適切に表現されていることを確認する
- サイバーセキュリティ戦略、ポリシー、および実行に関する重要な役割と説明責任の根拠を理解し、その割り当てに異議を唱える
- サイバーセキュリティとサイバーリスク機能が適切な人員と資金を受け取ることへの期待を設定し、これらの決定の有効性を監視する
- サイバーセキュリティ文化を鼓舞し、サイバーセキュリティ機能と、さまざまなレベルのサイバーリスクに関連し、説明責任を負うすべての利害関係者との間のコラボレーションを促進する
- 説明責任者が、組織全体のサイバーリスク戦略を調整する権限と責任を持ち、組織がデータガバナンスのための包括的な計画を持っていることを確認する

原則5：取締役会のガバナンスにサイバーセキュリティの専門知識を組み込む

取締役会がサイバーセキュリティに関する効果的なガバナンスを発揮するには、内外の専門知識を活用しつつ、取締役自身がサイバーセキュリティに関する知識を継続的に拡大するように努める必要があります。加えて、サイバーに関する専門家の取締役会への参加促進や、第三者のアドバイザーによる取締役会への定期的な報告、独立した第三者機関による組織のサイバーセキュリティ強度の定期的な監査を検討することで、取締役会のガバナンスにサイバーセキュリティの専門知識を組み込むことが求められます。

取締役会での主な検討事項

- サイバーセキュリティに関する戦略的意思決定に必要な専門知識を提供できる社内のステークホルダーとの関係を構築し、サイバーに関する専門家を取締役会に参加させる
- サイバーリスクに関する取締役の基本的な知識レベルを向上させる機会に参加する
- 経営陣を効果的に監督するために、定期的に取締役会に報告する第三者のアドバイザーや評価者を求める
- 独立した第三者機関による定期的な監査、サイバーセキュリティ強度のレビュー、ベンチマークを検討する
- 取締役会との定期的な会議を実施し、最近のサイバーインシデント、トレンド、脆弱性、リスク予測についてグループに最新情報を提供する。必要に応じて外部の第三者機関を利用し、正確性と能力を確保する

原則6：システムの回復力とコラボレーションを促進する

高度に組織間が接続された現代では、自社のサイバーセキュリティの確保のみならず、組織を超えたサイバーレジリエンスに向けた協働が求められます。経営陣は、組織間全体のサイバーレジリエンスを向上させるために、業界全体および公的および民間の利害関係者とのコラボレーションを奨励するとともに、取締役自身も他の取締役を含むピアネットワークの構築に尽力必要があります。

取締役会での主な検討事項

- 事業を取り巻く広範な環境において、社会的責任を果たす当事者として活動するために、組織のリスクとレジリエンスの態勢を360度の視点で把握する
- 組織の境界を越えて最良のガバナンス手法を共有するために、他の取締役を含むピアネットワーク（1対1の関係）を構築する
- 経営陣が、サイバーレジリエンスの向上に関して、特に公共部門との効果的な連携のための計画を持っていることを確認する

- 経営陣が、より広範な業界のつながり（第三者、ベンダー、パートナーなど）に起因するリスクを考慮していることを確認する
- 業界団体や知識・情報共有プラットフォームへの経営陣の参加を奨励する

4 取締役が取り組むべきこと

「コーポレートガバナンス・コード」の「考え方」にも記載されているとおり、取締役の責務の発揮や非財務情報の開示等には具体的なルールが存在しないため、現在の企業から開示された情報だけでは、付加価値に乏しい場合も少なくないという意見が多々存在します。今回解説した世界経済フォーラムの6つの原則は、サイバーセキュリティという観点ではありますが、取締役会で検討すべき事項が明示されています。したがって、サイバーセキュリティ対策状況についてどのように取り組んでいくべきか、開示すべきかを悩んでいる企業においては、まずこの6つの原則をベースに現在の会社のサイバーセキュリティ対策状況をとりまとめることにより、多くのステークホルダーにとって付加価値のある情報提供ができるようになります。本稿をそのための第一歩として頂ければ幸いに存じます。

【執筆協力】
PwCあらた有限責任監査法人　シニアマネージャー　佐々木 章
PwCあらた有限責任監査法人　アソシエイト　川井 歩夢
PwCあらた有限責任監査法人　アソシエイト　美原 きらら

綾部 泰二（あやべ たいじ）
PwCあらた有限責任監査法人　システム・プロセス・アシュアランス部
パートナー
大手監査法人に入所後、システム子会社へ出向し、主にビジネスプロセスの変革などを実施。また、銀行、保険、証券会社、大手メーカー、大手通信、大手自動車など、業種を問わずサービスを提供している。現在はサイバーセキュリティ、プロジェクト監査、ITガバナンス、システムリスク管理関連業務の責任者として多数のクライアントにサービスを提供している。特にITガバナンスの知見を生かしたサイバーセキュリティにおけるガバナンスを検討することを得意としている。またインシデントが発生した場合の再発防止策検討や有効性評価の実績を多数有する。2019年7月よりPwC Japanグループのサイバーセキュリティ Co-Leaderを務める。
メールアドレス：taiji.t.ayabe@pwc.com

川本 大亮（かわもと だいすけ）
PwCあらた有限責任監査法人　システム・プロセス・アシュアランス部
パートナー
ITに関するアシュアランスおよびアドバイザリーサービスを日系・外資系企業に提供しており、外部監査、内部監査、US/J-SOXプロジェクト、セキュリティ評価、ITガバナンス、第三者に対する保証と意見表明サービスにおける、ITリスクの発見・評価の経験を豊富に有する。PwCのクラウドセキュリティチームを率い、セキュリティに関する基準の策定、評価、実装について、規制機関およびクライアントを支援してきた。内閣府デジタル市場競争会議のワーキンググループメンバーとして活動。
メールアドレス：daisuke.kawamoto@pwc.com