取締役会レベルのガイド：サイバーセキュリティにおけるリーダーシップ

監督

組織の指導部の最高レベルに当たる取締役会は、サイバーリスクガバナンスに関する究極の説明責任を負うため、この分野における組織の戦略、方針、そして活動を監督する必要がある。取締役会は、特に以下を実施すること：

- 完全な取締役会または特定の取締役会委員会への監督機能の委任を通じて、サイバーリスクおよびレジリエンスに関する究極の責任を負う。
- 組織のサイバーレジリエンス管理能力およびサイバーレジリエンス目標の実装の進捗状況について報告する責任を1人の執行役員に任命する。通常、これには最高情報セキュリティ責任者（CISO）が指名される。この執行役員には、取締役会への定期的なアクセス、十分な権限、主題に関する運用能力、経験、そして当該任務の遂行に必要なリソースが備わっていることを確認する。
- 毎年、組織のリスク許容度を定義して、それが企業戦略とリスク選好度に合致していることを確認する。
- 貴組織のサイバーレジリエンスに関する正式な独立審査が毎年必ず実施されていることを確認する。
- サイバーレジリエンス計画の作成、実装、テスト、そして継続的改善を監督し、組織全体にわたって連携させ、CISO またはアカウンタビリティのあるその他の役員が取締役会に定期的に報告するよう万全を期する。
- 総合的な運用上のリスクにサイバーリスクを完全に統合することを目標に掲げ、組織の総合的な事業戦略、リスク管理、予算編成、そしてリソース配分にサイバーレジリエンスとリスクアセスメントを統合する。第三者リスクを定期的に審査する。
- 上記に関するパフォーマンスを定期的に審査し、継続的な改善を実現できるよう独立した助言を得ることを検討する。

最新情報の入手

取締役会がサイバーリスクを効果的に監督できるかどうかは、主題に関する役員の能力、そして最新情報にかかっている。

- 取締役会に加わる全ての個人が適切かつ最新のスキルと知識を有しており、サイバー脅威が呈するリスクを把握および管理できるよう万全を期する。
- 貴組織の現在および将来的なリスクの露出、関連の規制要件、そしてリスク選好度に関する業界および社会のベンチマークについて、組織の経営陣より定期的な助言を求める。更に、脅威ランドスケープおよび規制環境に関する最新の進展の定期ブリーフィング、サイバーセキュリティにおけるベストプラクティスを実践している同僚およびリーダーとの共同計画および訪問、またガバナンスとレポートに関する取締役会レベルの意見交換に従事する。
- 経営陣には、取締役会議中の常設の議案としてのサイバーリスク、脅威、およびイベントについて、定量化された分かりやすい報告を行う責任を課す。
- サプライチェーンの脆弱性、共通の依存関係、そして情報共有におけるギャップなど、進行中の体系的な課題に関連した進展について経営陣およびその他の関連職員と定期的に確認する。

基調の打ち出し

取締役会は上級管理職と共に、組織のコアバリュー、リスク文化、そしてサイバーレジリエンスに関する期待を設定し、模範となる必要がある。

- あらゆる職位の職員が、各自の重要な責任を認識して、組織のサイバーレジリエンスを確保する組織文化を推進する。模範を示すこと。
- 貴組織のリスク文化の醸成および維持における経営陣の役割を監督する。リスク文化が安全性および健全性に及ぼす影響を考慮した上でその推進、監視、そして評価を行い、必要に応じて変更する。
- 全ての従業員が誠実に行動し、貴組織内外で観察したコンプライアンス違反を速やかにエスカレーションすることを求めている点を明確に伝える。

サイバーリスクガバナンスの基本

以下の質問群に「はい」と回答できることを確認すること：

1. 貴組織は、**関連の法定および規制要件を満たしていますか?**
2. 貴組織は、**サイバーエクスポージャーを定量化して、その財政的レジリエンスをテストしましたか？**
3. 貴組織は、サイバーエクスポージャーが合意済みのリスク選好度内に収まるよう、**改善策**を配備していますか？
4. 取締役会は、経営陣が提供する組織のサイバーレジリエンスに関して簡潔、明晰、かつ実用的な情報の定期的な協議を行っていますか？
5. 貴組織が配備しているインシデントレスポンス計画では、取締役会レベルを含めて最近予行演習を行いましたか？
6. サイバーリスク管理を担当する主要人物の役割は明確であり、3つの防衛線と連携していますか？
7. 貴組織のサイバーリスクポスチャに対する独立検証および保証を取得しましたか？