

# CEO レベル向けガイド：サイバーセキュリティにおけるリーダーシップ

## ガバナンス

貴組織のサイバーセキュリティは、トップマネジメントに始まり、トップマネジメントに終わります。CEO と取締役会はリスクに対する理解を維持し、組織のサイバーセキュリティ活動および職員に関する究極のアカウンタビリティおよび責任を引き受ける必要があります。以下を実施してください：

- 最高情報セキュリティ責任者 (CISO) が存在しない場合は、当該責任者を任命する。また、リソースが限定されている場合は、CISO の機能を果たす人物を組織内で任命する。
- CISO またはその他の技術職員との協力の下、国際的、全国的、また業界の基準およびガイドラインを用いて、組織の具体的なサイバーリスクに合わせてカスタマイズされたサイバーセキュリティ戦略およびフレームワークを確立して維持する。
- 組織のサイバーセキュリティの実装および管理を担当する従業員の役割と責任を明確に示す。
  - CISO との協力の下、全ての職位の職員を対象に適正なサイバーセキュリティの役割とアクセス権を特定する。
  - コミュニケーションとコラボレーションを監督し、全体論的なサイバーセキュリティ管理が行われるよう万全を期する。これは特に、サイバーセキュリティに関する責任が組織内の複数の従業員または部署によって共有されている場合に当てはまる（情報セキュリティ、リスク、そしてテクノロジーなどの異種の垂直関係など）。
- CISO には、ご自分と取締役会に対して適宜脅威について伝えることの可能な、明確な直通のコミュニケーションラインが設けられていることを確認する。
- 上級管理職へのブリーフィングを行えるよう、CISO またはその他の技術職員を定期的に招待する。
- 組織のセキュリティポリシー、基準、施行メカニズム、そして手順が全てのチームおよびラインオブビジネスを跨いで統一されていることを確認する。

## リスクアセスメントおよび管理

強固なサイバーセキュリティウェアネスおよびレジリエンスは、継続的なリスクベース分析によって左右されます。貴組織のサイバーセキュリティを改善するには、以下を実施してください：

- 貴組織の広範なリスク管理およびガバナンスプロセスにおいて、サイバーセキュリティリスクアセスメントおよび管理を確立する。CISO またはその他の技術職員との協力の下、以下を伴うリスクアセスメントの実施計画を立てる：
  - 組織のアセットおよびそれぞれのテクノロジー依存の度合いの解説
  - 組織の成熟度、またアセットのテクノロジー依存度に関連した固有のリスクのアセスメント
  - 組織が希望する成熟度の判断
  - 組織のリスク優先度リストにおけるサイバーセキュリティ脅威の位置づけ
  - サイバーセキュリティの現状と目標とする状態のギャップの特定
  - 成熟度の達成および維持に向けた計画の実装
  - セキュリティへの投資資金の評価および割当て、ならびに既存のギャップへの対処
  - 組織のサイバーセキュリティの成熟度、リスク、目標の継続的な再評価
  - 第三者ペネトレーションテストまたはレッドチームの利用を検討する。
  - サイバー保険の購入といった安全対策の検討
- リスクアセスメントプロセスにおいて従業員の取り組みを主導し、組織全体の時宜を得たレスポンスを促進する。
- 主要ステークホルダーおよび取締役会を含めた経営陣による監督を目的に、リスクアセスメントの結果を分析および提示する。
- 組織において望ましいサイバーセキュリティレジリエンスを維持または増大させるため、あらゆる変更点を監督する。これには、適切な予算編成の下でサイバーセキュリティの向上を目的に、無理のない、組織のリスクに比例した行動を取ることが含まれる。
- 継続的な監視のパフォーマンスを監督して、進化し続けるサイバーリスクに機敏かつ敏捷に対処する。

## 組織文化

貴組織のサイバーセキュリティは、一度きりのプロセスでなければ、数人の従業員の仕事でもありません。つまり、あらゆるビジネス上の判断において考慮すべき要因であると共に、全ての従業員が固守すべき慣行なのです。組織内で継続的かつ全体論的なサイバーセキュリティを奨励するには、以下を実施してください：

- リーダーシップチームとサイバーセキュリティに関する協議を始め、サイバーリスク管理を担当する職員と定期的に連絡を取る。
- サイバーセキュリティトレーニングを全ての従業員オンボーディングの一部にして、全員が貴組織のサイバーセキュリティポリシーの最新情報を把握し、これへの遵守に合意した文書に署名すると共に、IT部署またはその他の技術職員はベストプラクティスに関するブリーフィングを受けるよう万全を期する。
- 全ての職員の長期および短期的なセキュリティ面での責任に関して、繰り返し行われるサイバーセキュリティトレーニングを設定する。
- 貴組織が潜在的なベンダーを評価し、第三者とデータを共有する際は、必ずサイバーセキュリティを考慮するよう万全を期する。
- 合併および買収を検討する際は、組織のサイバーセキュリティアセスメントを組込む。
- 毎年、貴組織のサイバーセキュリティポリシーを見直す。
- 組織内および信頼できる取引先において、サイバーセキュリティの脅威およびインシデントに関する自発的な情報共有を推奨する。
- 最初からセキュリティ上の懸念および計画を組み入れたイノベーションを生み出す。