情報セキュリティ

基本的な考え方・ガバナンス

情報セキュリティは重要リスクとして事業計画に組み込まれており、取締役会と監査委員会は、情報セキュリティを含むすべての重要な企業リスクを監督しています。取締役会と執行役は、グループ全体のエンタープライズ・リスク・マネジメントを運営しており、情報セキュリティはその中核となる分野の一つです。地域・組織それぞれのリスクマネジメントは執行役の指示に基づき、事業計画における重点施策を各事業・各機能長がリスクアセスメントを踏まえて実施しています。執行役のうち、CAOは情報セキュリティの分野における執行責任を担い、CISO（チーフインフォメーションセキュリティオフィサー）はその委任を受けて業務執行のガバナンスを強化しています。情報セキュリティの状況は、CAOからグループ経営執行会議および取締役会に定期的に報告されています。

推進体制

事業に関わる情報セキュリティの適切な管理・保護を確実に実施するため、CISOを設置した体制を整備し、責任を明確にしています。CISOが指揮し、各地域や4つの情報セキュリティ領域を包括するグローバルガバナンス体制の下、情報セキュリティの管理・確保に取り組んでいます。

4つの情報セキュリティ領域	定義
情報セキュリティガバナンスおよび戦略	情報セキュリティのリスクマネジメントおよび戦略の策定を行う
プロダクトセキュリティ	サプライチェーンを含む製品ライフサイクル全般においてセキュリティを保証する
エンタープライズ情報セキュリティ	サイバーセキュリティ・ITセキュリティ・物理的セキュリティを含む、 エンタープライズ情報セキュリティを保証する
データプロテクション	適切なデータクラシフィケーションと、プライバシー要件を含むコンプライアンス義務に沿った リスクコントロールプロセスの業務への組み込みにより、資産損傷リスクマネジメントを保証する

取り組み（マネジメント）

情報セキュリティリスクマネジメント

4つの情報セキュリティ領域を踏まえたアセスメントの実施、分析、計画策定、実施、レビューといったPDCAサイクルを必要な階層に応じて実施しています。アセスメントでは、国内外の監督省庁、情報セキュリティに関わる政府機関・独立関係機関・業界団体・脅威インテリジェンスベンダー等、複数の第三者視点の情報を取り込むとともに、グローバルな自社状況の把握に努めています。また、分析したリスク事象については効果的な対応策を策定するため、適切なリスク分類を行い、自社による取り組みや関連機関との連携、リスク保証等多面的な検討を行っています。

リスク管理プロセス

脆弱性を評価するための模擬攻撃を含む第三者評価や、グローバルに情報セキュリティインシデントのモニタリングを実施し、結果に応じたリスク対処を行っています。

リスク対策

インシデントレスポンス：ITセキュリティに関するインシデントは、グローバルルールを明確化し、CISO直下に設置されたグローバル情報セキュリティガバナンス委員会で状況に応じてインシデントに関する情報共有を行うとともに、インシデントレスポンス体制の有効性を維持するための訓練を行っています。昨今のサイバー攻撃などを踏まえ、インシデント対応の実施計画について常時必要な更新を行い、グローバルな情報セキュリティ対応を図っています。プロダクトセキュリティについては、製品に関する脅威・脆弱性情報を収集し、セキュリティリスクを分析する体制を構築し、早期のセキュリティ対策に努めています。データプロテクションについては、関連法規制に加え、コンプライアンス・リスクコントロールといった観点から適切なデータ重要度分類とそれに見合った管理手法の導入を図り、適切な保護を行っています。

BCP計画：万一インシデントが発生した場合でも業務への影響を最小とするため、全社および各機能・部門において最重要業務や情報資産を洗い出し、それらを維持・保護するための、緊急時体制や業務手順の整備を進めています。

情報セキュリティ教育：eラーニング等を活用した教育、情報セキュリティ方針やインシデントに関する報告プロセスの周知を全地域で行っています。

情報セキュリティ
https://www.olympus.co.jp/csr/governance/security/