コーポレートガバナンス

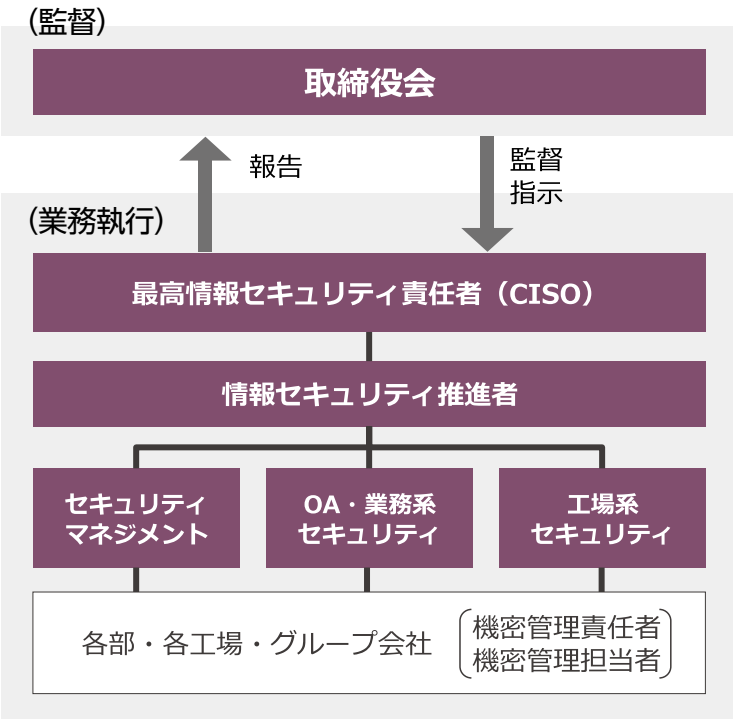
情報セキュリティ

■ 基本的な考え方

当社はお客さま、取引先から預かった情報および当社が保有する営業秘密など重要な情報資産を保有しているほか、近年ではリモート業務や工場設備のネットワーク化などが進展しています。年々高まるサイバー攻撃などの脅威や情報漏洩などから情報資産を保護し、正常な事業活動の継続により、製品を安定供給することは企業の責務であり、重要な経営課題との認識に立ち、情報セキュリティ対策に取り組んでいます。

■ 推進体制

トヨタグループ共通のオールトヨタセキュリティガイドライン(ATSG)などに基づき、最高情報セキュリティ責任者(CISO)のもと、グループ一体で組織的かつ継続的に情報セキュリティの維持・向上ができる体制を整備し、グローバルで同レベルのセキュリティが確保できるよう活動を行っています。
CISOはグループ全体での情報セキュリティ・情報資産保護に関する全体を統括し、セキュリティマネジメント、OS・業務系セキュリティ、工場系セキュリティの各組織が企画立案、推進、監査、支援を行っています。取締役会は毎年2回、CISOから進捗や課題などの報告を受けることで監督機能を果たしています。



具体的な取り組み事例

ATSG※に基づいた セキュリティ点検・監査

グループ全体で継続的に情報セキュリティの取り組み状況を点検し、情報セキュリティの継続的な維持・向上に努めています。
本年度は最新バージョン(Ver 8.1) 対応に向け、グループ各社とも取り組みを強化しています。

※ATSG:オールトヨタセキュリティガイドライン

電子メールによるサイバー攻撃

近年ますます複雑化、巧妙化が進むサイバー攻撃の多くは電子メールからのウィルス感染とされており、対策の強化が急務です。当社でも外部からの不審メールに対しては、防御システム導入などの技術的対策と、従業員への標的型メール訓練の実施や教育などの人的対策を実施することで、サイバーインシデントの発生防止に取り組んでいます。

セキュリティインシデント訓練

万が一、セキュリティインシデントが発生した際に被害や業務への影響を最小限に抑えるため、セキュリティインシデント訓練を実施しています。事前に具体的なリスクシナリオを策定し、実際の場面と同じように時系列で体験することで、サイバー攻撃を受けた際の対処やシステムの早期復旧手順、システムが使えない状態でも業務を継続するための役割分担などの有効性を検証・改善し、組織的な事故対応能力と不測の事態への応用力を高めています。