コンプライアンス

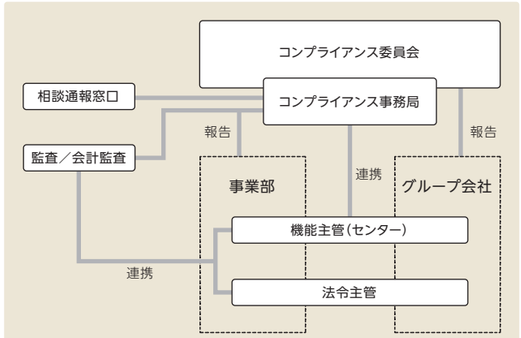
経営理念において「社会の一員として、法と倫理を遵守し、自然・地域と共生する企業をめざす」ことを宣言し、社会の期待に応えることを含めてコンプライアンス活動を進めています。

推進体制・仕組み

コンプライアンスに関する重要な施策などを検討するために社長を委員長とするコンプライアンス委員会を設置しています。また、日常の活動を支えるためにコンプライアンス統括部署のみならず、法令主管部署および各部にコンプライアンス管理責任者／管理担当者を設置することで、職場に適した活動を継続的に行うことができるよう取り組んでいます。

	予防	発見対処
事業部長	文化・風土、方針	調査・再発防止策構築
部門長	コミュニケーション、教育、方針	モニタリング、調査・再発防止策構築
機能主管（センター）、法令主管	各部方針支援、教育	モニタリング支援、調査・再発防止策構築

■組織・体制図



具体的な取り組み

コンプライアンス強調月間活動

毎月10月に実施する「コンプライアンス強調月間活動」では、コンプライアンス意識の維持および向上を図っています。職場でコンプライアンスについて討議する機会のほか、PC起動時のメッセージ、社内報や役員講話、DVD上映会などを行っています。

グループコンプライアンスへの取り組み

コンプライアンス統括部署や法令主管部署が主体となり、国内・海外子会社と連携を図り、各社の状況や環境に応じた体制整備や啓発活動を行っています。

社員行動指針

個人の尊重や社会のルール遵守などを定めた社員行動指針を、社員のコンプライアンス意識の啓発に活用しています。

東海理化イズム

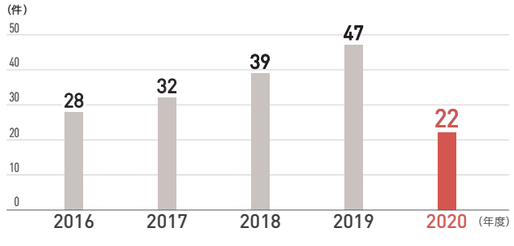
2021年4月、創業者等の想いをまとめ、わかりやすく解説を加えた「先人の言葉」を編纂しました。また、東海理化グループが長年にわたり培ってきた、そして今後も大切にしていくべき価値観を込め、私たちが考えて行動する際の道標（みちしるべ）とする「考動宣言」を策定しました。この両者をまとめて「東海理化イズム」と称し、自分たちの意識と行動を変容させ、より深く、より早く、仕事を遂行し、社会の信頼と期待に応えるための、拠り所としています。

相談通報

社内の問題を早期に発見し、解決するために、社内および社外に相談通報窓口を設置しています。社内の相談通報窓口は、問題をできる限り広く、かつ早期に吸い上げることができるよう、本社、各工場および労働組合の各所に設置するとともに、名称を「なんでも相談窓口」とし、窓口の敷居を低くする工夫をしています。また、社内の窓口には相談しづらいと感じる社員が相談自体を躊躇することがないよう、「コンプライアンス・コール」として、社外弁護士事務所に相談通報窓口を設置しています。当然のことながら、相談者が特定されることがないように秘密厳守を徹底しています。

以下のグラフのとおり、毎年一定数の相談があり、問題の早期解決に結びつけています。

■相談通報件数



情報セキュリティ

機密漏えいの防止、情報の外部からの攻撃に対する防御が事業活動には不可欠と考えています。

当社のみならず取引先の情報は適切な管理・取り扱いをすべき資産であるとの認識に基づき、情報セキュリティ体制を整備しています。

基本的な考え方

当社では、「社員行動指針」に「機密情報は、規則に従って厳重に管理し、漏えいの防止につとめます。」と定め、各部に機密管理責任者、機密情報取扱者を置き、職場でのミーティングや自主点検を実施することで機密管理意識の向上につとめています。

また、従来の機密性に加え、完全性、可用性を確保するために情報セキュリティポリシーおよび規程を制定。

従来の規程、要領、手引き類を見直しました。

情報セキュリティポリシーの制定

2020年3月にCISO（情報セキュリティ最高責任者）名で情報セキュリティポリシーを制定しました。

■情報セキュリティCIA図

情報セキュリティポリシー

1. 情報セキュリティを重要な経営課題として捉え、情報セキュリティの管理体制を構築したうえで、情報セキュリティ活動に継続して取り組みます。
2. 情報セキュリティリスクを評価・分析し、人的・組織的・技術的・物理的に適切なセキュリティ対策を実施します。
3. 情報セキュリティについての教育および訓練を継続的に実施し、全ての社員の情報セキュリティレベルの更なる向上につとめます。
4. 情報セキュリティインシデントが発生した際には、関係各位に迅速に報告したうえで、被害の更なる拡大を抑制するよう初期対応を実施するとともに、原因を究明し、適切な再発防止策を講じます。
5. 管理体制やルールの遵守状況、対策の有効性等、情報セキュリティに係る取り組み全般を定期的に点検し、継続的な是正・改善活動を実施します。

脆弱性監視・インシデント対応要領制定

昨年度制定した情報セキュリティポリシー・規程に基づき、車両サイバーセキュリティの国際法規である国連WP29 Cyber Security Regulationおよび国際規格のISO21434へ準拠するため、従来の総務・情報システム部門に加え、設計・品質部門、工場部門を含めた全社体制により、インシデントを未然に防ぎ、発生時の被害を最小限にする組織を構築。

■SIRT®組織図 ※セキュリティインシデント対応チーム