ガバナンス | コーポレートガバナンス

基本的な考え方

適切な経営執行体制を確保し、企業業績・企業価値・社会的信用性を高めるために、コーポレートガバナンス強化を重要な経営課題と位置づけています。

コーポレートガバナンス体制

当社は、執行役員制度を導入しており、取締役会および監査役会の監視・監督のもと、執行役員において重要な業務執行を行っています。

取締役会

現在、8名で構成されており、定款および取締役会規程などの関連規程に基づき、経営上の業務執行の基本事項について決定するとともに、その執行を管理しています。

取締役会は原則として毎月開催されており、迅速な意思決定を図るとともに、取締役間の緊密かつ闊達な議論を促進しています。また、複数の代表取締役を設け、各取締役の業務分掌を明確にすることで、偏向的な意思決定がなされない体制としています。

監査役会

社外監査役2名を含む3名で構成される監査役会を設置しています。監査役は取締役会など社内の重要な諸会議に出席する他、業務執行状況の聴取を通じて、取締役の職務の執行状況を監査しています。

執行役員

執行役員は、取締役会の基本的事項の意思決定および関連規程上の決裁権限に基づき、重要な権能を所管する各組織を率いて業務を執行することで、効率的な業務運営を実現しています。また、執行役員から定期的に自らの領域について管掌する取締役に対する業務報告の場が設けられており、適時適切な監督体制が機能するよう設計されています。

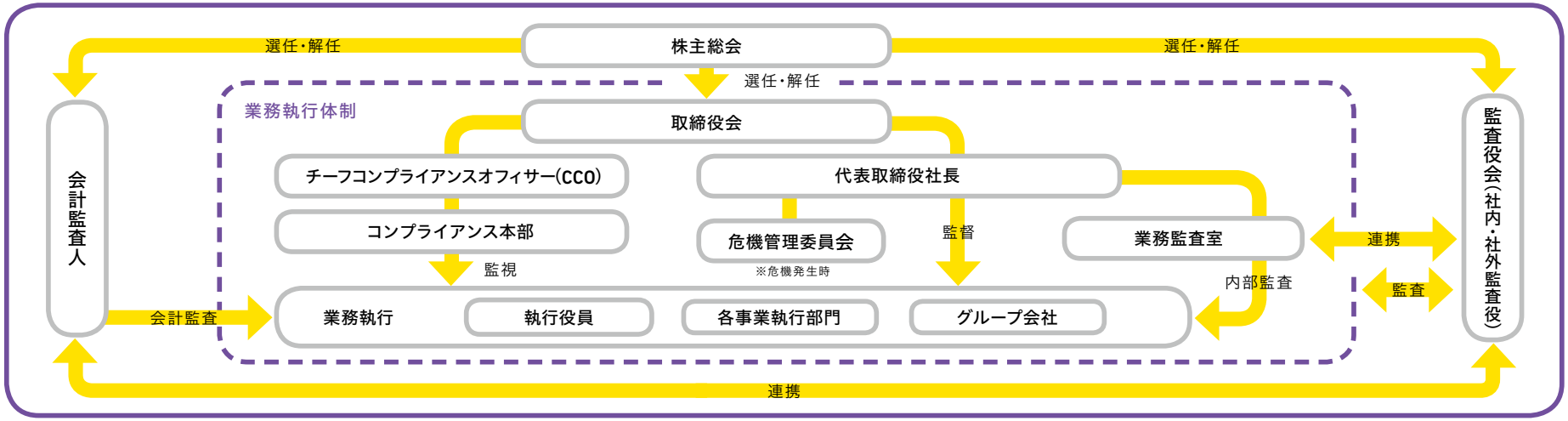
内部統制システム

当社は、職務の執行内容を法令および定款に適合させるため、さまざまな施策を行っています。

当社の事業は、事業本部制のもと、各事業の特性に応じた柔軟な業務運営体制としている一方、本社部門を中心としてグループ一貫とした統制を図るため、基幹組織規程および決裁権限規定などを定め、各組織・分掌・権限を明確にし、これらに基づいた運営体制を構築しています。各部門における業務執行およびレポーティング、ならびに、経営層における意思決定・点検や各部門とのコミュニケーションが確実に行われるようレベルに応じた意思決定や報告の場を定期的に設けています。

グループ会社においては、「関連会社管理規程」を制定し、業務運営ルールを明確にするとともに、必要に応じて会計監査および業務監査を実施しています。

コーポレートガバナンス体系図(組織系統図)



ガバナンス | コンプライアンス

基本的な考え方

企業としての社会的責任を果たし、お客さまの期待に応えていくためには、法令遵守はもちろんのこと、社員が企業の一員としての社会的責任を意識することが必要不可欠です。当社では「コンプライアンス遵守」を会社方針と定め、法令を守ることにとどまらず、社員一人ひとりが高い倫理観をもって行動することで、コンプライアンス徹底に努めています。

推進体制

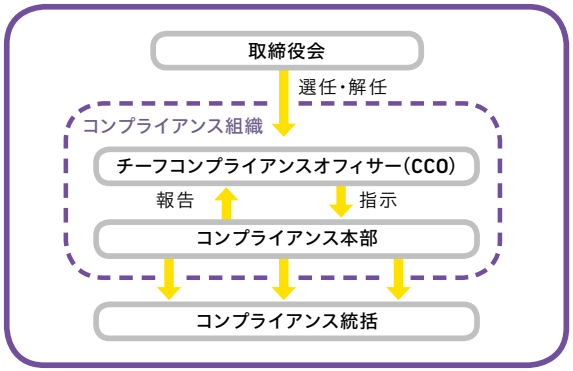
当社では、取締役および執行役員から独立した権限を有するチーフコンプライアンスオフィサー(CCO)がコンプライアンス本部を統括し、コンプライアンスに関わる事項の施策・実施を行っています。CCOを中心にコンプライアンス本部と一体となって、グローバル全体での連携強化を図りつつ、コンプライアンス活動を推進しています。

コンプライアンス違反が生じた場合、CCOが対応責任者としてコンプライアンス本部を指揮して対応にあたります。その影響度に応じ、CCOは本社に対策委員会を設置し、一元的に対応します。

コンプライアンス組織を定めたプログラムは、CCOによる定期的な見直しによって、継続的な改善を図っています。また、コンプライアンス本部において、年1回のグローバルコンプライアンス評価会議を開催しています。

CCOは、コンプライアンス本部における定期的なリスクアセスメントを通じて、特に力を入れるべき分野を指定し、その基本方針に基づき、各領域を統括するコンプライアンスオフィサーを任命しています。これらのコンプライアンスオフィサーとコンプライアンス事務局が連携し、四半期ごとに分科会を開催しています。分科会では、コンプライアンスに関する事項に加え、各領域で発生し得るさまざまな課題やリスクについても意見交換を行い、組織全体での健全な経営とリスク管理の徹底を図っています。また、各分野における最重要事項への対応方針としてコンプライアンスポリシーを策定し、これをグローバルに展開。すべてのイノアックグループ会社に対して、このポリシーの遵守を義務付けることで、国際的な事業運営においても一貫したガバナンスを実現しています。

体制図



コンプライアンス研修の実施

各構成員が遵守すべき、回避すべきことを理解し、実際の業務に落とし込むためには、体系的かつ継続的なコンプライアンス研修が必須と考えています。

「まもる」プロジェクトの取り組みとして、各重要領域に応じた研修項目を整理したうえで、全役職員が受講すべきもの、ステージに応じて受講すべきもの、職種に応じて受講すべきものなどに区分しています。これに基づき、全社必須研修、各ステージの節目となる定期研修(新入社員研修・中途社員研修・海外赴任候補者研修・基幹職研修などにおけるコンプライアンス研修)を実施しています。また、各地域・事業部の特性に応じてコンプライアンス研修を個別に実施しています。

全社必須研修においては、まず行動指針の受講を第一とし、その中で、具体的に排除すべき行動態様として、腐敗行為や反社会的勢力との付き合いなどを列挙しています。その他重要法令、リスクの高い領域については、別途研修枠組みを設け、実施しています。

ガバナンス | コンプライアンス

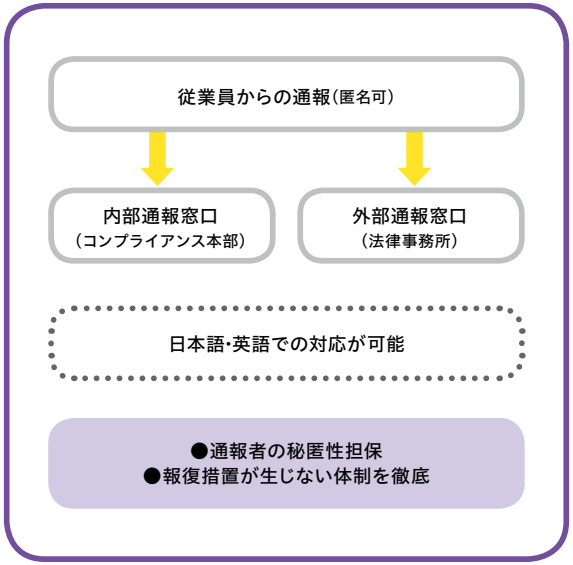
内部通報制度の整備

コンプライアンス違反またはその恐れがある事象について、イノアックグループに従事するすべての者が相談または通報することができる、内部通報窓口を設置しています。

通報窓口は、内部（コンプライアンス本部）および外部（法律事務所）に設けており、日本語のみならず英語での対応も可能です。

関連規程に基づき、通報者の秘匿性は確保され、また通報したことに対する報復措置が生じない体制を徹底しています。

内部通報窓口について



まもるPJの推進

健全な企業運営、コンプライアンス遵守を徹底するため、グループ構成員の誰もが気軽に声をあげることができる風土づくりをすべきと考えております。そのため、あえてコンプライアンスやインテグリティといったカタカナではなく、よりわかりやすくポジティブなイメージを創出するため、「まもる/Mamoru」を合言葉とした取り組みを推進しています。この「まもる」はMamoruとしてそのままグローバルに統一的に展開されており、以下の３つのフレーズを基本精神としています。

❶ルールをまもる　❷仲間をまもる　❸自分をまもる

「まもる/Mamoru」は、先述の内部通報制度の活用のみならず、各個人が業務に際して少しでも疑問を感じたとき、自分や仲間を「まもる」ためにも、いつでもコンプライアンス本部や周りの人に相談することを奨励しています。また、このプロジェクトの一環として、全社員および業務に基づいて指定された者については、指定された「まもる」べきものをより具体的に伝えるため、後述のとおりコンプライアンス研修をブラッシュアップし、定期的な見直しをしています。

「まもる」という言葉は、そのまま経営トップからのメッセージ、コンプライアンスポリシーや窓口とともに世界中のイノアック拠点に届けられており、イノアックグループ内のイントラネットにおいてすべての役職員に公開され、いつでも閲覧が可能です。

イノアックグループの構成員間の風通しをよくすることで、より透明性のある、企業価値を高めることのできる土壌を整備します。

継続的な啓発活動

「まもる」を合言葉に、各コンプライアンスオフィサーから、直接全従業員に対して自らが所管する領域に関して「まもる」べきことを直接伝えることを継続して行っています。

現在は、定期的に発行される社内報に「まもる」の連載枠を準備し、毎回違うオフィサーが情報発信をしています。2024年から、CCOをはじめ、人事・品質・調達など、継続的に掲載しています。

まもる
mamoru

ガバナンス | 情報セキュリティ

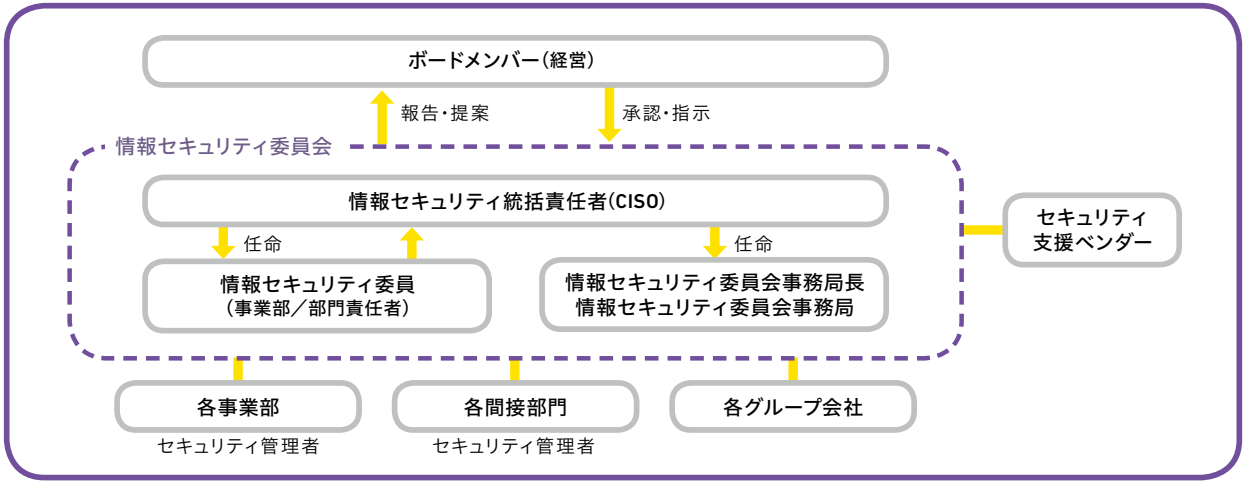
基本的な考え方

当社が取り扱う情報資産が重要な経営資源・資産であるとの認識のもと、安定した製品およびサービスの提供を行います。また、情報資産の機密性・完全性・可用性を確保するために、組織的かつ継続的に情報セキュリティリスクを特定し、適切な管理策を講じるものとします。さらに、グローバルな事業展開にともない、各国および各地域の法規制や文化的背景を考慮し、包括的な情報セキュリティポリシーを策定しています。

推進体制

当社では2022年9月に情報セキュリティ委員会を設立しました。サイバーインシデント発生の低減および対応措置の整備を進めつつ、グローバル全体への展開を目指して活動しています。

体制図(平時)



役割

情報セキュリティ統括責任者(CISO):
情報セキュリティ施策の決定権限を有し全責任を負う。

情報セキュリティ委員会事務局長:
情報セキュリティ委員会の運営の責任を負う。

情報セキュリティ委員会事務局:
情報セキュリティ施策の検討・導入を行う。

情報セキュリティ委員:
各部門の情報セキュリティ施策実施の責任を負う。

情報セキュリティ管理者:
各部門の情報セキュリティ施策実施を行う。

活動内容

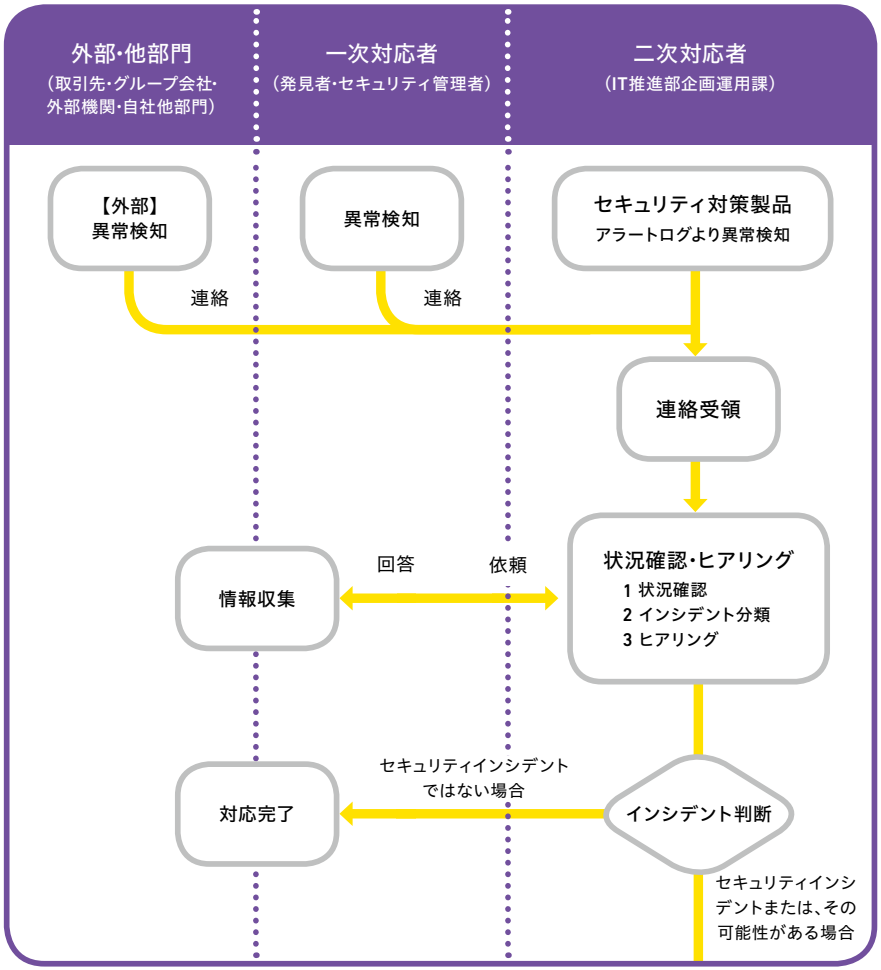
- セキュリティインシデント予防のため社内教育を最低2回/年実施、入社時教育を実施
- 社内規程・ガイドラインの整備
- システム導入時の審査フロー制定
- 情報の機密性に応じた管理ルールの制定と運用
- セキュリティインシデント発生時に迅速な対応が行えるインシデント対応フローの作成と訓練の実施
- セキュリティインシデント発生時の業務継続プラン作成
- ログ相関分析ツール・脆弱性診断ツールによるセキュリティインシデント防御策実施
- 緊急時連絡網の整備
- サプライチェーンの情報セキュリティ実施状況の把握
- 海外グループ会社への情報セキュリティ強化活動の推進

ガバナンス | 情報セキュリティ

インシデント対応

事故レベル3を「取引先をはじめとする外部ステークホルダーへの影響がある重大なインシデント」とし「危機管理規程」および情報セキュリティ委員会によって定められた有事の情報セキュリティ管理体制に基づいて対応を実施しています。

インシデント対応フロー（抜粋）



活動目標・実績

活動目標	2024年　実績
2026年3月までにサイバーセキュリティガイドラインV2.2 の「LV1・LV2」項目について100%達成	Lv1・Lv2 97%達成
重要な情報を取り扱うサプライヤーの情報セキュリティ強化対策状況の把握と推進	特に重要なサプライヤーでの情報セキュリティ対策状況に関する調査実施
製造現場含めた全従業員への教育実施	全社員を対象とした「情報管理」教育を実施
クラウドサービス評価基準実装	事業活動に関わる主要なクラウドサービスについての評価を実施

個人情報保護

事業活動を通じて取得・管理する個人情報の保護を最重要課題の一つと位置づけています。お客さまや従業員のプライバシーを尊重し、安全かつ適正な情報管理を徹底することで、信頼される企業としての責任を果たしていきます。

個人情報の取り扱いに関しては、個人情報保護規定に則り以下の原則を遵守しています。

個人情報の取り扱いの原則

法令・規範の遵守	詳しくはWEBの「個人情報の保護」をご覧ください。(https://www.inoac.co.jp/privacypolicy/)
利用目的の明確化	
適切な管理と保護	
第三者提供の制限	
従業員教育と意識向上	全社員を対象とした「情報管理」教育を実施