リスクマネジメント

オカムラグループは、企業活動に関わるさまざまなリスクを想定し、必要な対策を実施しています。

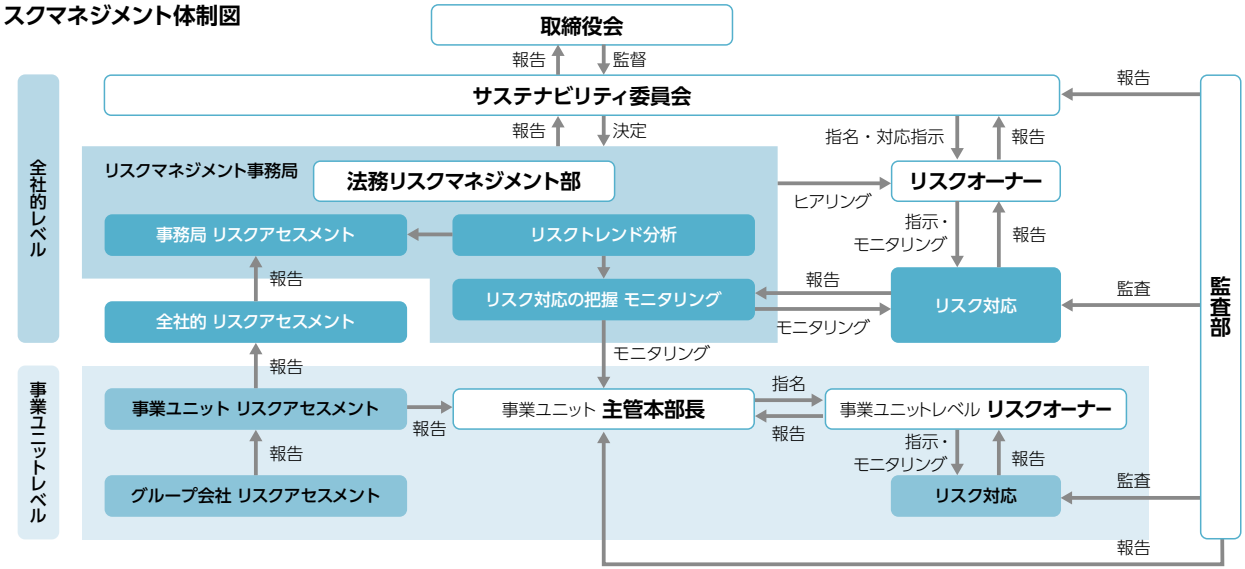
リスクマネジメント体制

オカムラグループは、事業目的の達成に影響を及ぼす可能性（好ましい影響・好ましくない影響の双方を含む）をリスクと認識し、リスクの特定、分析および評価を行った上で、リスクを合理的にコントロールしてリスクがもたらす損失の最小化または機会の最大化を図るよう、組織的に活動しています。
また、リスクに係る組織的な活動であるリスクマネジメントを、グループのサステナビリティ活動と有機的に結びつけて、リスクマネジメントの有効性の向上を図るため、サステナビリティ委員会において、オカムラグループのリスクマネジメントに関する各種事項の決定ならびに有効性評価および改善指導を行っています。オカムラグループでは、こうした体制の整備や運用などリスクマネジメントに関わる基本的な事項を、「リスクマネジメント規程」として定めています。（参照 ▶P.15）

リスクマネジメント体制における各役割と内容

各役割	具体的な内容
サステナビリティ委員会	オカムラグループのリスクマネジメントに関する基本方針および全社的なリスクに係る重点対応リスク・対応策・リスクオーナーの決定、ならびにリスクマネジメントの有効性評価等を実施し、重要事項を取締役会に報告しています。
リスクマネジメント事務局	法務リスクマネジメント部長が事務局長を務め、法務リスクマネジメント部、サステナビリティ推進部、経営企画部、総務部を構成員として、オカムラグループのリスクマネジメントの運営を支援・推進しています。
全社的レベルのリスクマネジメント	当社全体またはオカムラグループに影響が及ぶことが想定される事態に対して、サステナビリティ委員会を決定機関としてリスクマネジメントを実施しています。
事業ユニットレベルのリスクマネジメント	当社の事業本部およびグループ会社を総称したオカムラグループ内における事業活動の責任単位を事業ユニットとしており、事業本部の執行役員を主管本部長としています。事業本部またはグループ会社で対応が可能な事態には、事業ユニットの主管本部長を責任者としてリスクマネジメントを実施しています。
リスクオーナー	リスクごとに、リスクを効果的にコントロールする活動責任と活動内容・結果についての説明責任を持つ責任者をリスクオーナーとして定めています。リスクオーナーは、事業目的・業績目標に照らして適切なリスク対応策を選択・適用する権限を有しており、リスクへの対応を行っています。

リスクマネジメント体制図



リスクアセスメントプロセス

リスクアセスメントにあたっては、まずリスクを特定し、特定したリスクに対して、発生可能性と影響度の観点からリスクマップを用いて分析した上で評価を行っています。

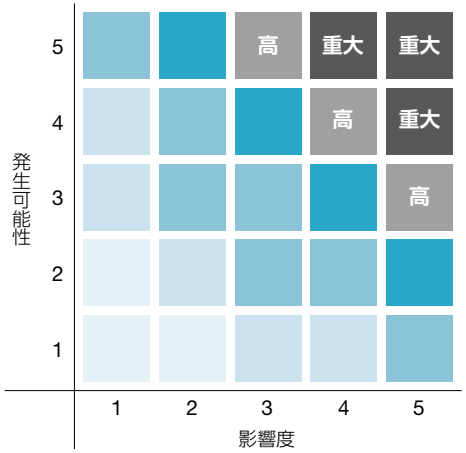
特定されたさまざまなリスクは、大きく「事業環境リスク」「事業戦略リスク」「業務リスク」「金融リスク」「人権・人財・労務リスク」の5つに分類し、さらに中分類・小分類の3つの階層に整理しています。（参照 ▶P.19）

リスクアセスメントは、全社的レベルで年2回、事業ユニットレベルで年1回実施しています。

事業ユニットレベルのリスクアセスメントは、まずグループ会社が自社に係るリスクについて分析・評価を行います。次に、グループ会社のアセスメント結果を踏まえて事業ユニットの主管本部長が事業ユニット単位での重点対応リスクを決定します。

全社レベルのリスクアセスメントは、リスクマネジメント事務局が指定した評価部門が事業ユニットのリスクアセスメントを参考にしつつ一次アセスメントを実施、リスクマネジメント事務局が各評価部門の結果を総合的に検討して再度アセスメントを行います。そのアセスメントによって、リスクマップで「重大」リスク、「高」リスクに位置付けられたリスク、および将来の影響変化予測や社会的責任の重要性を考慮して重要と判断したリスクをサステナビリティ委員会に諮り、同委員会にて全社的な重点対応リスクを決定します。

リスクマップ



重点対応リスク

重点対応リスクとして特定されたものは、各リスクオーナーが顕在化した場合の事業への影響度を分析して対応策を策定し、実行に努めています。その策定にあたっては、短期的・優先的に対応すべきリスクがサステナビリティ委員会で指定されており、その結果が計画に加味されています。

また、リスクオーナーおよびリスクマネジメント事務局は、対応状況をモニタリングし、課題が明らかになった場合には、リスクオーナーがその是正・改善を図っています。

（参照 ▶P.15）

災害対策の強化

オカムラグループでは、生命・身体に危害が及ぶおそれや社会・事業活動に重大な影響を及ぼすおそれのある緊急事態が発生した際の対応を「緊急事態対応規程」として定めるとともに、詳細な手順をマニュアルに定めて、迅速かつ的確な対応により、事態の拡大防止と早期収束を図るよう備えています。そのうち、災害対策としては、災害発生時に全従業員が的確な行動をとり、安全を確保するとともに事業活動への影響を最小限にとどめるため、『災害対応マニュアル』の配布・周知、非常時の情報システムの整備、災害備蓄品の保管、訓練の実施など、総合的な対策を進めています。（関連 ▶P.120）

災害対応マニュアルの配布

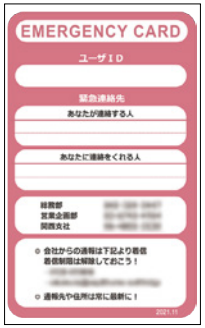
『災害対応マニュアル』では、業務・操業の停止がやむを得ないと判断される自然災害等（大地震、津波、台風、落雷、大雪、大雨、洪水、突風、噴火、その他気候変動による災害）、火災、テロ、感染症等を対象災害と定め、災害発生時における基本姿勢や行動指針、平常時の備えなど、所属長・従業員が取るべき行動を順序立てて記載するとともに、災害対策本部の設置から対策実施の流れを示しています。また、業務継続・停止の判断基準や、従業員が帰宅または職場にとどまる基準を明確化しています。

さらに、職場での災害備蓄品の保管・配布基準を明示するとともに、災害発生時の家族との連絡方法等を紹介し、安否確認を速やかに行えるよう啓発しています。

安否確認システムの構築・運用

災害が発生した際に、従業員の安否状況を迅速に確認するため、安否確認システムを構築・運用しています。震度6弱（首都圏エリアでは震度5強）以上の地震などの災害が発生した場合、発生した地域の全従業員に対して、メールや電話により安否確認の連絡を行います。本システムが有効に機能するよう、毎年2回の定期訓練を行っています。また、システムの使用方法を記載した携帯用の「エマージェンシーカード」を全従業員に配布しています。

『災害対応マニュアル Ver.4』



「エマージェンシーカード」

非常時通信網の整備

災害発生後の停電などにより固定電話・携帯電話が使用できない状況に備えて、主要な拠点に無線機または衛星電話を配備し、通信手段の確保に努めています。さらに、非常時通信網を用いた定期的な通信訓練の実施により、実効性を高めています。

災害備蓄品の保管

大規模災害で交通機関が麻痺し従業員が事務所や工場にとどまる事態を想定し、全国の拠点に3日分の水・食料・簡易トイレのほか、人数分のヘルメットとブランケットを保管するとともに、主要な拠点には非常用電源を配備しています。食料については、1人1日1,300kcal程度を確保できるよう、そのまま食べられるタイプのご飯、副菜等を配備しており、食物アレルギー物質不使用食品を全体の2割程度用意しています。

感染症対策

感染症の罹患は本人の健康にとって重大な問題であり、感染の拡大は企業活動、さらには社会全体にも大きな影響をもたらすリスクを伴っています。オカムラでは、季節性感染症の予防接種や海外赴任者と帯同家族を対象とした予防接種を行うとともに、啓発活動などを通じて従業員の感染予防に取り組んでいます。（詳細 ▶P.102）

秘密情報管理

オカムラグループでは、「秘密情報管理規則」を定め、電子データを含む全ての秘密情報に関する定義、管理方法、秘密保持義務（社外公開・目的外使用の禁止）について規定しています。

さらに、第三者から開示を受けた情報の厳格な管理義務や規則違反に対する罰則を設け、適切な管理体制を構築しています。

これらの取り組みを通じて、お客さまの情報を安全に保護し、信頼性の高いサービスを提供していきます。

秘密情報管理の取り組み

「秘密情報管理規則」に則り、各部門の所属長を情報管理責任者と定め、部門内の情報管理を総括しています。

情報漏えいが発覚した場合、従業員は「緊急事態対応規程」に基づき速やかに報告する義務があります。さらに、情報セキュリティ事故を伴う情報漏えいについては、CSIRTと連携し、情報漏えい拡大防止の措置をとります。

その他、取引先との間でも秘密情報の保護に関する契約を締結するなど、情報の適切な管理を実施しています。

（参照 ▶ P.137 ）

秘密情報管理に関する教育

オカムラでは、全従業員を対象とした秘密情報保護に関するe-ラーニングを2023年5月に実施し、情報管理についての理解を深めました。

また、情報管理のための台帳、規則の解説およびQ&Aを公開し、社内全体で情報管理の重要性の認識向上、実践に取り組んでいます。

これらの教育活動を通じて、全従業員が情報管理の重要性を理解し、実践することで情報の安全な取り扱いを確保しています。

個人情報保護

オカムラは、個人情報保護の取り組み推進を目的として個人情報管理委員会を設置し、教育活動、現場の監査・指導を実施しています。また、一般財団法人日本情報経済社会推進協会が運営するプライバシーマーク®制度の認定を2006年5月に取得、現在まで更新を続けており、個人情報を適切に取り扱っている事業者として、認定基準に基づく対応の徹底を図っています。

個人情報保護方針
https://www.okamura.co.jp/privacy.html

●EU一般データ保護規則（GDPR*）への対応

EUでは、プライバシー保護を目的とする枠組みとしてEU一般データ保護規則が制定され、2018年5月に施行されました。オカムラグループでは、この規則に従い、対象となる情報を適切に取り扱っています。

＊ GDPR：General Data Protection Regulation

GDPR Compliance
https://www.okamura.com/en-eu/etc/legal-notices/gdpr-compliance/

情報セキュリティ対策

オカムラグループでは、情報システム部門をグループ全体の情報セキュリティ向上の統括・推進役と位置付け、システム基盤であるパソコン、サーバー、ネットワークを中心に、グループ各社のセキュリティ対策および統制指導を行っています。
情報漏えい防止の施策として、パソコン内のデータ暗号化やパソコン操作ログの収集、ウェブサイトのフィルタリングシステムの導入を進めるとともに、従業員への教育・訓練を定期的に行っています。
またシステム利用の個人認証やオフィスへの入退室管理に関しても、適切なセキュリティ対策を実施しています。

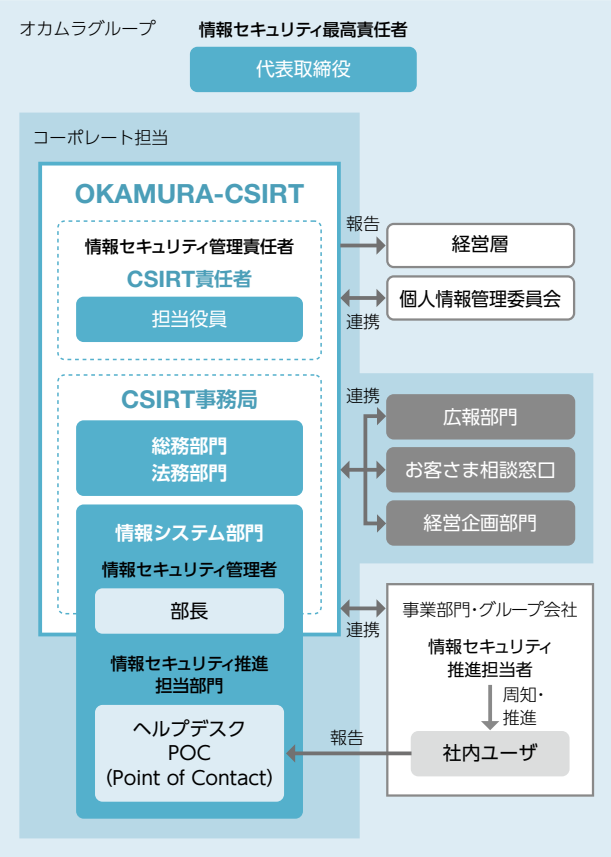
オカムラグループ情報セキュリティ方針および関連規則

オカムラグループでは、情報セキュリティリスクを事業継続における重点対応リスクと位置付け、「オカムラグループ情報セキュリティ方針」を2022年に制定しました。
情報セキュリティ方針に基づき、適切かつ組織的に情報セキュリティ対策を講じることで、情報セキュリティ事故を未然に防止する、または事故発生時の被害を極小化させるため、「情報セキュリティ管理規程」を定めています。さらに、セキュリティインシデント対応のため、「CSIRT憲章」において事前・事後対応の活動を規定しています。
「社内情報システム使用規則」において、従業員・社外常駐者の情報端末、ネットワーク、電子メールシステムなどの適切な使用方法を規定しています。またソーシャルメディア利用に伴うトラブル増加を踏まえ、「ソーシャルメディアガイドライン」を設けています。

情報セキュリティ推進体制

オカムラグループでは、情報セキュリティ事故を未然に防止し、重大な情報セキュリティ事故発生時の影響を最小限に抑えるため、2020年10月にOKAMURA-CSIRT(オカムラ-シーサート)を発足させました。
コーポレート担当役員を責任者として、総務部門、法務部門、情報システム部門が中心となり、広報部門、お客さま相談窓口と連携し、日頃から情報セキュリティ事故を未然に防止するための活動と、情報セキュリティ事故の発生を想定した準備活動を実施しています。
サイバー攻撃に対しては、早期検知の仕組みを導入しており、即時インシデントの管理対応を行います。
またインシデント発生時には、「CSIRT憲章」に則り、CSIRT責任者より深刻度に基づき経営層へ報告を行います。

情報セキュリティに関する体制図

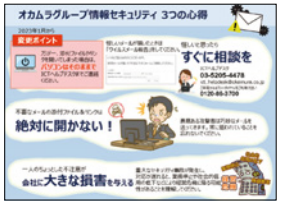


情報セキュリティリスク評価

オカムラグループでは、リスクマネジメント活動の中で、情報セキュリティリスクの評価を実施しています。また経済産業省のサイバーセキュリティ経営ガイドラインに基づき俯瞰的に自己評価を行い、情報セキュリティリスクの分析を組織的・人的・物理的・技術的な観点から行っています。そのリスク分析により、優先順位を明確にし、施策を実施しています。

情報セキュリティに関する教育・訓練

オカムラグループでは、従業員の情報セキュリティ意識の向上を目的に、e-ラーニングによる教育や標的型攻撃メール訓練などを全社的に進めるとともに、イントラネットやパソコン起動時の注意喚起表示により、従業員が日常業務の中で情報セキュリティリスクを意識するための啓発活動を継続的に実施しています。



パソコン起動時の注意喚起表示