

リスクマネジメント

基本的な考え方

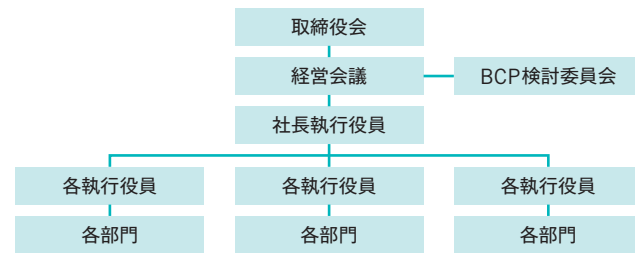
リスクマネジメントは、コンプライアンスとともにコーポレート・ガバナンスを支える基盤であり、切り離せない両輪であるという認識のもと、全従業員に「ミウラグループ企業行動規範」を浸透させ、企業を取り巻くあらゆるリスクに対して公正で適正な対応を進めています。また、危機管理(クライシスマネジメント)については、大規模災害や新型コロナウイルスの流行などの危機事象発生時においても、円滑に業務運営を継続できるよう、BCP※1を策定するなど、迅速かつ適切に対応できる体制を整備するとともに、全従業員への周知に努めています。

※1 BCP (Business Continuity Plan) : 事業継続計画

リスクマネジメント体制

リスク管理については、「リスクマネジメント基本規程」を制定し、当社の経営目標の達成を阻害するさまざまなリスクのうち、特に品質、環境、情報セキュリティ、財務、コンプライアンス、労働災害、災害問題などを主要な対象リスクとして、これらの部門を担当する各執行役員がリスクマネジメント推進者となって、リスク管理の推進と対応策の整備に努めています。

● リスクマネジメント体制図



取締役会は、リスクマネジメント体制に関する、特に重要な事項を決定しています。経営会議は、事業リスク影響評価を行い、リスク対応項目を決定しており、BCP検討委員会は経営会議の諮問機関として設置しています。

社長執行役員をリスクマネジメントの最高責任者とし、リスクマネジメント定例会を年1回開催しています。同定例会は構成メンバーである各部門責任者と事務局(内部統制室)で行い、審議内容は経営会議に報告しています。また、次年度の活動方針の承認も行っています。

リスクマネジメントの取り組み

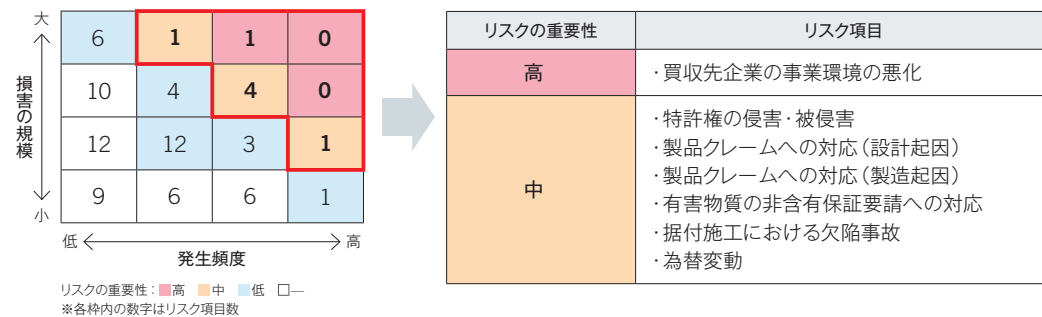
リスクマネジメント定例会において、当年度のリスクマネジメント推進の活動結果を踏まえ、次年度のリスクマネジメント推進の活動方針を策定しています。また、年1回実施しているリスク調査の結果に基づき、ミウラグループのリスクマップを定期的に見直しています。

技術・開発、生産、販売などの各分野においては、品質、労働安全衛生、コンプライアンスなどの観点から、リスク低減に向けたさまざまな取り組みを行っています。

前年度からの継続的な取り組み事項を含め、2020年3月期は期初に策定した活動方針に基づいて施策に取り組みました。重大クレーム発生防止に向けては、関連部署間の連携強化定例会を開催しました。また、労働安全衛生法や産業廃棄物処理法、下請法などについての研修教育や社内周知の実施を行うことで、リスクの低減に努めました。さらには、当社の贈賄防止に関する方針のサプライヤーに対する書面交付や、「インターネットを介したシステム利活用に関する情報セキュリティ要領」の制定、西日本豪雨の水災被害を受けてのBCPの見直しなど、仕組みの整備にも取り組んでいます。

これらの活動結果を踏まえ、2021年3月期は、グループ全体のリスクマネジメント推進や、BCP見直しに伴う製造ラインにおける対策の実施、海外事業のリスクマネジメント体制強化などの取り組みを通じ、引き続きリスクマネジメント体制の強化を進めていきます。

● ミウラグループの主要リスク分布状況(2021年3月期)



情報セキュリティ

お客様から信頼される企業であり続けるためには、お客様からお預かりした情報資産、ならびに当社が保有する情報資産をあらゆる脅威から保護し、適正に管理・運用することが求められます。当社では、「情報管理規程」にて定めている情報セキュリティ対策を実施し、情報資産の保護を最大限に配慮しながら企業活動を展開しています。

り、当社における情報資産の保護、および適切な情報セキュリティ体制を実現することを目的として、2019年5月に「インターネットを介したシステム利活用に関する情報セキュリティ要領」を制定しました。

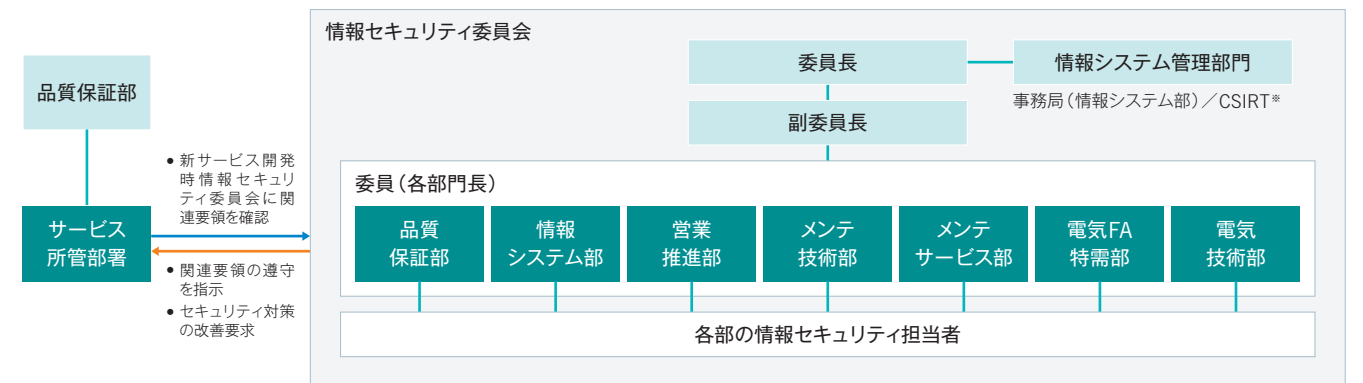
情報セキュリティ体制

当社の情報セキュリティを継続的に維持・強化していくため、情報セキュリティ委員会を設け、全社的なセキュリティマネジメント体制を整えています。情報セキュリティ委員会では、インターネットを活用した製品・サービスについて、企画から製品化の段階にかけてリスクアセスメントを実施し、リスク対応の評価・承認を行っています。2020年3月期は、3件のサービスについて評価・承認を行いました。

「インターネットを介したシステム利活用に関する情報セキュリティ要領」の制定

今後、お客様や従業員に対し利便性が高いサービスや情報を提供していくには、インターネットやクラウドの活用が不可欠となってきています。インターネットを活用したシステムに関する社内規程を定めることによ

● 情報セキュリティ委員会および関係者 体制図



※ CSIRT: Computer Security Incident Response Teamの略で、「コンピュータセキュリティインシデント」に関する報告を受け取り、調査し、対応活動を行う組織体

主な取り組み

当社では、情報セキュリティ対策として「情報管理規程」を定め、セキュリティ管理体制を明確にしており、専門機関によるウェブサイトのセキュリティ診断など、定期的な見直しと対策強化を継続的にを行っています。

また、従業員教育として、情報機器を取り扱う全従業員に対し継続的に情報セキュリティに関する教育・注意喚起を行い、その重要性や、情報の適切な取り扱い・管理について周知徹底を図るほか、教育資料も定期的に見直しています。

事業継続活動

ミウラグループでは、「リスクマネジメント基本規程」のもと、事業活動の継続を脅かすさまざまなリスクへの対策を講じています。特に、ミウラグループの本社・生産機能が集中する四国では、大規模地震などによる大きな被害が予想されることから、BCP基本方針※2に基づき、グループ各社ではBCPを策定し、被災時においてもお客様に安定的に製品・サービスを供給できるよう、グループ全体で取り組んでいます。

※2 BCP基本方針はウェブサイトでご覧いただけます。
<https://www.miuraz.co.jp/corporate/bcp.html>

主な取り組み

オンラインメンテナンスのバックアップシステム

大規模災害などにより愛媛県の本社機能が不全に陥った場合に備え、栃木支店にオンラインメンテナンスのバックアップシステムを設置しています。2020年3月期にはバックアップシステム用の非常用発電機を導入しました。

BCPシステム同時対応

2015年から、災害GIS(地理情報システム)を利用したBCPシステムを運用しています。また、2019年3月期には、それまで一つの災害にしか管理できなかったBCPシステムを同時災害にも対応できるよう改善しました。その結果、2020年3月期に相次いで発生した令和元年佐賀県豪雨災害(8月)、台風19号災害(10月)にも混乱なく対応しました。

医療用機器に対する初動体制への備え

大規模災害が発生した場合などには、法令に基づいて緊急交通路が指定されます。ミウラグループでは、このような通行規制に備え、医療機関からの要請に迅速に対応するために医療用機器の業務に使用する車両を規制除外車両として事前申請しています。