リスクマネジメント

第一三共グループでは、組織の目的・目標の達成を阻害する可能性を有し、かつ事前に想定し得る要因をリスクとして特定し、企業活動に潜在するリスクへの適切な対応（保有、低減、回避、移転）を行うとともに、リスクが顕在化した際の人・社会・企業への影響を最小限に留めるべく、リスクマネジメントを推進しています。

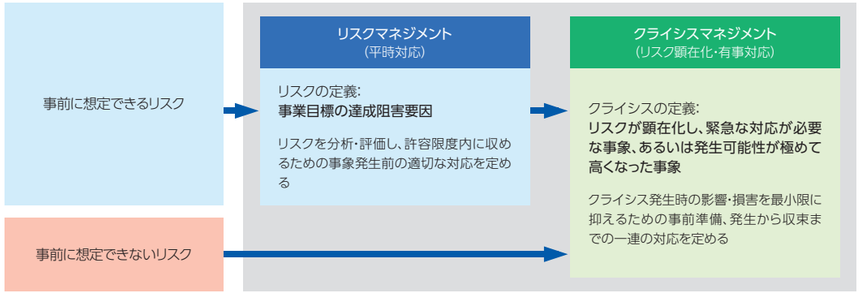
リスクマネジメント

当社グループは、最高財務責任者（CFO）がリスクマネジメント推進責任者として当社グループ全体のリスクマネジメントを統括し、事業計画策定・実行の年次サイクルに合わせたリスクマネジメントを推進しています。

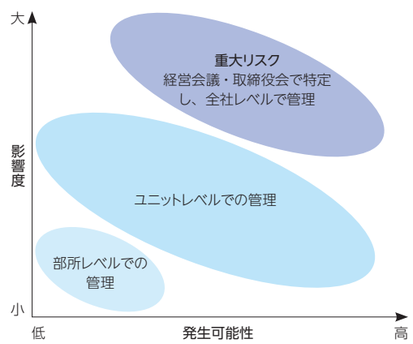
各ユニットにおいてはユニットの責任者が、組織の目的・目標の達成に向け、リスクの抽出、対応策の策定・実行、組織内でのリスクマネジメントに関わる情報提供・教育・啓発等を自律的に実施し、リスクマネジメントを推進しています。

リスクマネジメント事務局では、各ユニットから抽出されたリスクについて、影響度と発生可能性の観点からリスクアセスメントを実施し、企業経営に重大な影響が想定されると評価したリスク項目を、毎年、経営会議および取締役会において重大リスクとして特定します（下図「当社グループにおけるリスクレベル分類の概念図」参照）。さらに特定した重大リスクごとに担当責任者が任命され、関係組織と連携の上、リスク対応策を実行しています。その進捗状況は、年2回のリスクモニタリングを通じて確認され、必要に応じた是正・改善がなされます。重大リスク顕在化の予兆が確認された際は、速やかにリスクマネジメント推進責任者に情報が集約され、CEOに報告される体制としています。

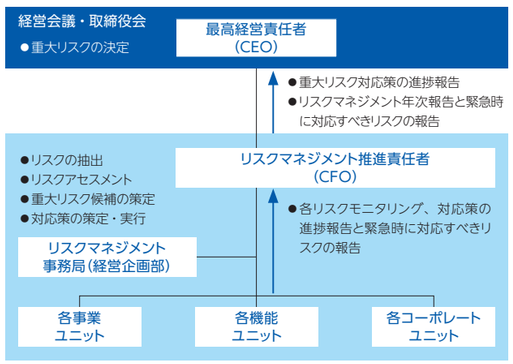
▶リスク・クライシスマネジメントの全体像



▶当社グループにおけるリスクレベル分類の概念図



▶リスクマネジメント体制図



主なリスクとその対応状況

以下は、当社グループの重大リスク、ユニット・部所レベルの管理リスクの中から抽出した「主なリスク」です。抽出にあたっては、投資判断への影響の有無等を考慮しています。

領域	✓重大リスク	リスクの概要	リスクへの対応状況
研究開発・他社とのアライアンス	✓	新薬候補品、特にアストラゼネカ社と提携したトラスツズマブ デルクステカン（DS-8201）、ダトポタマブ デルクステカン（DS-1062）に関する研究開発の中止、承認審査基準の変更等による承認取得不可、研究開発にかかる提携に関する契約条件変更・終了等の可能性	• DS-8201に関してアストラゼネカ社とJoint Executive Committeeを設置し、ビジョンと戦略の策定や進捗管理等を実施 • 当局との継続的なコミュニケーションを通じた薬事リスクの管理・低減
医薬品の副作用や品質問題	✓	医薬品の品質問題や予期せぬ副作用発現による製品回収や発売中止、健康被害に関する賠償責任等に係る多額の費用の発生の可能性	• 国内外の安全管理情報（副作用情報等）の客観的な評価・検討・分析の実施と医療現場への適確な情報提供 • 全社員を対象とした安全管理情報についての研修実施（毎年）
海外における事業展開		海外事業における、当該地域の政治不安、経済情勢の悪化、法規制等への抵触、労使関係等の悪化の可能性	• 海外グループ会社のリスク管理担当者を任命、定期的な情報収集・交換を実施 • 問題発生時には、当該担当者をハブとする現地グループ会社との連携により、迅速に課題解決
製造・仕入れ	✓	当社施設の損壊、社会インフラの障害、技術的な理由等による製造活動や仕入れの遅延・停止等による悪影響の可能性	• 有事の際の速やかな業務復旧、ならびに医療体制維持のための医薬品安定供給および品質確保を可能とする体制の整備 • 生産・物流拠点の分散、自家発電装置の設置 • 主要システムの二重化等、IT基盤の強化
環境・安全		当社社内外の人への化学物質の暴露、土壌汚染、大気汚染等による環境への悪影響や気候変動に伴う気象災害や温暖化等による医薬品のサプライチェーン寸断、製造コスト上昇等が医薬品の安定供給に悪影響を及ぼす可能性	• 規制当局の基準以上の厳格な自主管理基準値の設定と継続的なモニタリング • TCFD（気候変動関連財務情報開示タスクフォース）に沿った情報開示
知的財産権	✓	事業活動が他者の特許権その他の知的財産権に抵触するとして第三者から指摘を受けた場合の事業の断念や係争と、第三者が当社グループの知的財産権を侵害する場合の当社からの訴訟提起の可能性	• 知的財産の創造と保護による価値の最大化とリスクの最小化 • 知的財産係争が発生した場合、社内外の関係者と協力し、事業への影響を最小限にとどめるための体制の整備
訴訟	✓	医薬品の副作用、製造物責任、労務問題、公正取引に関する問題等に関する訴訟の可能性	• 法令、契約、紛争防止・解決等の観点からのリーガルリスク最小化とビジネス機会最大化 • コンプライアンス違反の未然防止策制定
法規制、医療費抑制策等の行政動向	✓	薬価基準の改定、医療制度、健康保険に関する行政施策による事業への悪影響の可能性	• 薬価制度改革や流通改善ガイドラインを踏まえた仕切価格・割戻改定の実施 • 適切な販売契約の設定・実施
法令違反	✓	役員および社員の個人的な不正行為等を含めた重大な法令違反の可能性	• 不適切な活動を早期に発見するための事業活動のモニタリングの実施 • 法規制の遵守・徹底と教育・啓発等による発生防止策の実施
金融市況および為替変動	✓	株式市況の低迷や金利動向、為替相場の変動による不利な影響の可能性	• 政策保有株の削減 • 年金基金資産配分の期中見直し • 為替ヘッジ取引
ITセキュリティおよび情報管理 詳しくは P44参照	✓	ネットワークウイルス感染、サイバー攻撃等によるシステムの休止や個人情報を含む機密情報の漏洩の可能性	• CIO*1とCISO*2の設置による情報分野におけるグローバル組織体制構築 • 情報管理に関する社員研修の実施 • 防御機能、侵害の検知機能と対処機能等のセキュリティシステムの整備 • 情報セキュリティ基盤強化・運用改善
繰延税金資産の回収可能性	✓	課税所得の減少、税制改正等による将来減算一時差異および税務上の繰越欠損金の再評価による悪影響の可能性	• 経営環境変化等を踏まえた将来の課税所得の適宜見直し
人材の確保		採用市場の競争激化等により、高い業務遂行能力や各職務に必要な高度な専門性を持った人材やデジタル人材を十分に確保できない可能性	• 計画的な採用活動の強化、多様なアプローチによる人材確保 • 社内教育プログラムの実施を通じた人材の確保・育成
新型コロナウイルス感染拡大の影響	✓	新型コロナウイルス感染拡大に伴うサプライチェーンでの物資の遅延等による製品安定供給への悪影響ならびに、臨床現場での混乱に伴う現在進行中の開発治験の遅延やプロトコル違反による将来の製品価値の毀損の可能性	• 新型コロナウイルス緊急対策本部の設置 • 医薬品の在庫確保 • 被験者の安全を最優先にした臨床試験の継続・変更

*1 Chief Information Officerの略　*2 Chief Information Security Officerの略。情報管理最高責任者

クライシスマネジメント

当社グループのグローバルクライシスマネジメントポリシーでは、企業活動に潜在するリスクのうち、顕在化し緊急な対応が必要な事象、発生可能性が極めて高くなった事象を総称して「クライシス」と定義しており、その発生による損失の最小化を図ることを目的に、クライシスマネジメントに関わる基本的事項を定めています。

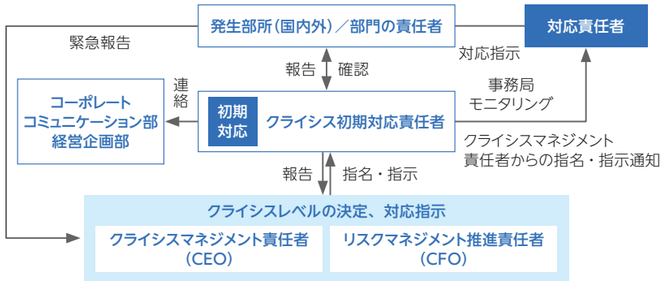
当社グループでは、クライシスの種類（災害・事故、事件・不祥事・法令違反、情報管理に関する問題、製品に関する問題）やクライシスの影響度合いに応じて、機動的な対応を可能とする体制を構築しています（下図「クライシス発生時の初期対応」参照）。報告基準や報告ルートを明確に定め、クライシスマネジメント責任者（CEOまたはCEOが指名した者）、クライシス初期対応責任者（総務・調達部長）を設置し、グローバルに影響が大きく、全社対応の必要性があるクライシスについては、リスクマネジメント推進責任者（CFO）とも当該情報を共有し、迅速かつ的確な初期対応により、事態の拡大防止と初期収束に努めます。また、クライシス収束後は、事後分析により、再発の防止や対応の改善を図ります。

新型コロナウイルス感染症（COVID-19）に対しても、クライシスマネジメント責任者（CEO）をトップとした「新型コロナウイルス緊急対策本部」を早期に立ち上げ、さまざまな部所と連携し、社員の安全はもとより医薬品の安定供給に支障のない対応をとっています。

基本方針

クライシス発生時は、第一三共グループの社員および関係者の生命や地域社会の安全を確保する、生命関連企業の一員としての責任を全うすることを基本に、迅速かつ確実にクライシスマネジメントを展開し、人・社会・企業への影響を最小限に止め、事業の継続や早期復旧を図るべく努力する

▶クライシス発生時の初期対応



事業継続計画（BCP*）

＊ Business Continuity Planの略

当社グループは、事業継続へ影響を及ぼす4つの脅威（自然災害、設備事故、新型インフルエンザ・感染症、システム稼働停止）を対象に事業継続計画（BCP）を定め、有事の際の速やかな業務復旧、ならびに医療体制維持のための医薬品安定供給と品質確保を可能とする体制を整備しています。

- **自然災害、設備事故を想定したBCP**

当社グループでは、東日本大震災での経験を踏まえ、2012年にBCPを刷新し、以降も行政の防災計画改定や社会的要請に基づき、優先して供給する品目や各製造拠点の防災計画を見直す等、脅威が顕在化した際に、より適切に対応できるよう、また、製造や物流の複雑化やグローバル化に耐えうるよう、継続的な改善に努めています。

優先して供給する品目については、多くの患者さんに使用されている薬剤、緊急性のある薬剤、代替品のない薬剤の観点から設定するとともに定期的に見直しを行い、脅威が顕在化した際、必要となる医薬品を継続的かつ適切に供給できる体制を確保しています。

BCP施策としては、設備や物流・在庫・要員、情報といった必要な経営資源に対し、予防策の実施、多様性の確保、支援策の確保、代替策の確保の4つの視点からそれぞれ対策を行っています。

- **新型インフルエンザ行動計画**

当社グループでは、新型インフルエンザウイルスの世界的な大流行（パンデミック）に備え、社員およびその家族の安全を確保し、医薬品の供給を継続することを目的とした「新型インフルエンザ行動計画」を2009年より策定しています。今般の新型コロナウイルス感染症（COVID-19）の発生においては、本計画に準じた弾力的な対応を図っており、そこから得られる知見をもとに、さらに実効性を高めた行動計画へと見直しを行っていきます。

情報管理・セキュリティへの取り組み

近時、高度なサイバー攻撃の急増や各国の関連法令強化等、情報管理に係る環境が大きく変化しています。また、当社グループは他社との協業機会の増加等により、情報管理に関するリスクへの対応を企業活動における重要事項の一つとして捉え、情報管理・セキュリティ体制による対応強化を図るとともに、情報管理に関する規程・セキュリティシステム等の整備に取り組んでいます。

情報管理ガバナンス体制の強化

当社グループでは、安定した製品および情報を顧客に提供するために、ISO/IEC27001を基本としたセキュリティマネジメントシステムの確立をグループ各社で取り組んでいます。

情報分野におけるグローバルな専門機能の統括責任者としてCIOを任命するとともに、機密情報管理、情報セキュリティ対策の推進を担うCISOを任命し、新たなデジタル技術、法規制等に関するポリシー・ルールの整備を進めております。

情報管理関連規程の統一

当社グループ全体の情報管理に対する取り組みを効果的・効率的に実施するために、関連する規程を国内グループ各社共通としました。社員一人ひとりが情報を適切に取り扱うことを目指し、本年4月より、規程類を補完するための社員向けの実運用指針として「情報セキュリティガイドライン」と「情報取扱ガイドライン」の改正を行いました。

サイバーセキュリティへの対応・情報資源を守る

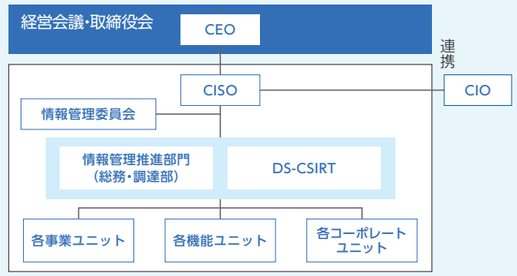
近年増大しているサイバーセキュリティへの脅威に対して適切な対応を行うことを目的とし、CISOのリーダーシップのもとにCSIRT*を設置し、社内だけでなく社会のセキュリティ向上に向け継続的に活動しています。

ITシステムへのサイバー攻撃等への対策強化として、防御機能、検知・対処機能等の情報セキュリティの基盤強化・運用改善を推進し、グローバルでの底上げを図っております。

また、セキュリティ対応・情報資源を守るためには、全ての社員の意識が重要であると考え、各社の状況に合せた社員への情報セキュリティ啓発活動として、情報セキュリティのEラーニングや標的型メール等に対する意識啓発、注意喚起を継続的に実施しています。

＊ Computer Security Incident Response Teamの略。企業等におけるコンピューターセキュリティに関する対応を行う組織

▶情報管理・セキュリティ体制図



情報管理を通じた「企業価値」「事業継続性」の実現に向けて

CISO 古田 弘信

企業価値向上のための情報管理・基盤の整備

さらなる企業価値の向上に向け、情報に対する適切な管理を重要な経営課題として認識し、情報管理に関する基本方針を定めるとともにルール、ガイドライン等を整備し、情報を安心して的確に活用できる仕組みづくりに取り組んでいます。また、定期的な社員教育の実施とクラウド系サービス利用への対応を図ることで、社員一人ひとりの情報リテラシー・活用モラルを向上させ、情報セキュリティを正しく理解できる人材として育成しています。そして、全社や各組織における事業戦略の一環としてDX*を進めていく上で不可欠となる情報セキュリティを確保するため、CIOと連携し、一層の取り組み強化を推進しています。

＊ Digital Transformationの略

サイバーセキュリティ対策を通じた事業継続性

高度なサイバー攻撃の急増等、情報管理に係る社会の変化は激しさを増しています。当社グループは他社との協業機会の増加等により、重要情報が広く社内外に存在する状況であり、これまで以上に厳格な情報管理が求められています。このような状況を踏まえ、当社グループは5つの機能を意識したサイバーセキュリティ対策を強化しており、情報流出等のリスク要因を能動的に把握・対応することで、事業継続性の確保を図っています。

特定―― 情報セキュリティに係る情報収集と脅威の認識
防御―― 脅威の発生可能性の低減
検知―― インシデント発生を早期に発見
対応―― インシデント対応計画の整備とインパクトの低減
復旧―― システム復旧手順の整備

また、当社のCSIRTではサイバー攻撃の脅威に対し、同業・他業種、公的機関などの多様な組織と連携した活動を推進しており、社内のみならず社会のセキュリティ向上にも貢献していきます。