7-4 リスクマネジメント

基本方針

当社グループは、安全と信頼を基盤とした事業継続のため、当社グループの事業活動に関連するリスク要因を正しく認識し、その発生可能性を低下させるための対策および発生した場合の損失を最小限に抑えるための対応について、全社的なリスク管理体制を整備した上で、継続的に検討・実施しています。

推進体制

当社の取締役会は、当社グループの業務執行に重大な影響を与えるリスクの予防と発生した損失の管理のため、危機管理規程、関係会社管理規程などの各種規程を整備し、当社グループ全体に対する横断的なリスク管理体制を整備しています。

当社グループにおける日常の業務遂行に関わる通常のリスク管理は、職務権限規程に基づき各部門が付与された権限の範囲内で適切に行っています。その上で、当社グループの各部門のリスク管理の状況につきましては、管理本部の各部門が専門知識と各業務プロセスに精通した知見を基に検証と確認を行うこととしています。各部門は、問題を発見したときは取締役会に報告することとなっています。

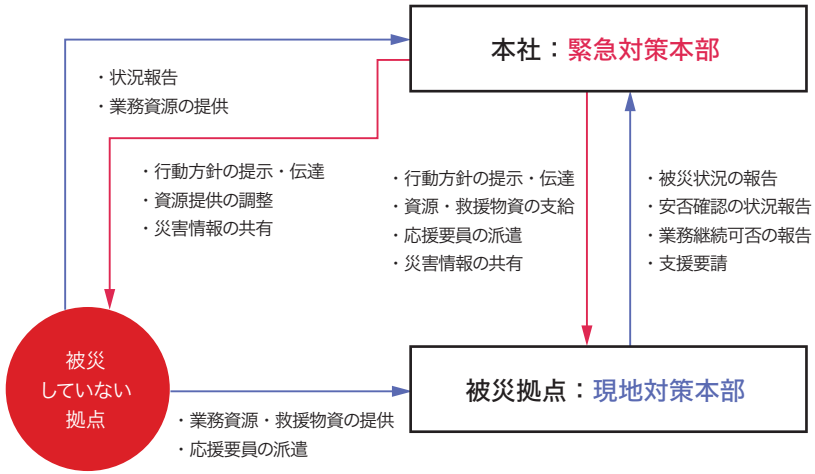
大規模災害等への対応

基本的な考え方

当社グループは、常に市場の期待とニーズを超える製品開発と安定供給を行い、最高水準の信頼性と安全性を確立し、全世界の医療に貢献することで国際的な企業へと飛躍することを目指しています。

当社グループは平常時から大規模災害・パンデミック等のリスクに備えた対策を計画・実施し、有事の際には人命および安全の確保を最優先した上で、被災地域での救援・支援や、製品の安定供給の継続を図ってまいります。

緊急対策本部の役割



<緊急対策本部>

当社グループに災害等の緊急事態が発生した場合には、迅速かつ適切に対応するため、危機管理規程に基づき、代表取締役社長を本部長とする緊急対策本部が統括して危機管理にあたることとしています。一元的な情報伝達体制等を整備することで、従業員や地域社会の安全を守るとともに、安定供給に取り組みます。

BCP（事業継続計画）

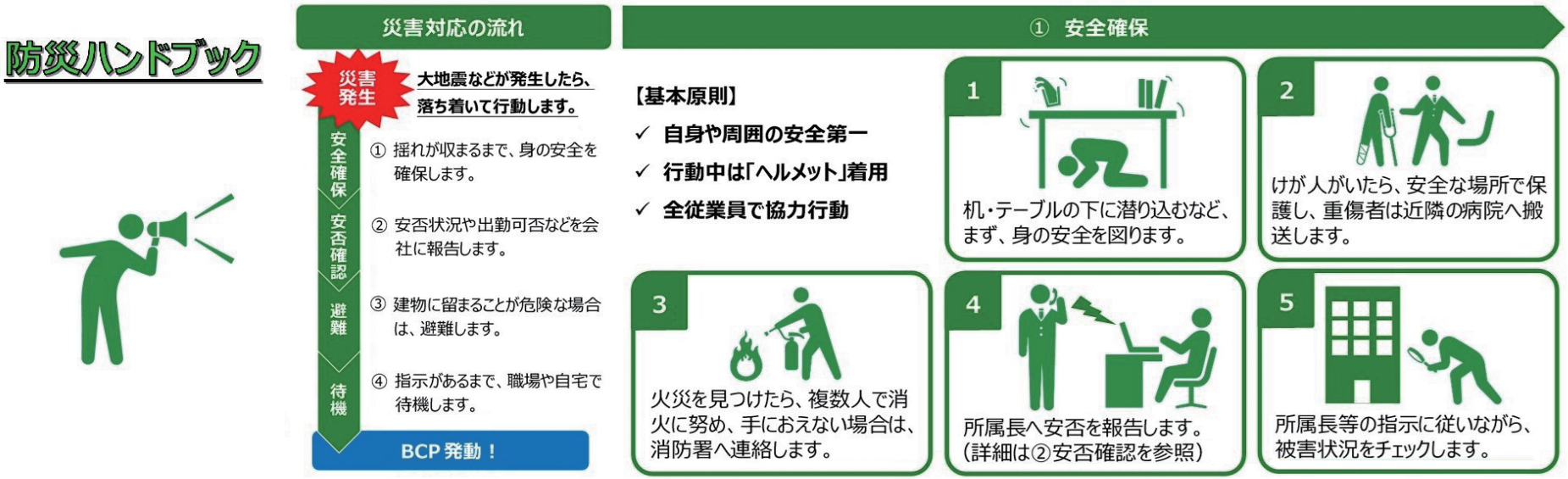
当社グループは、緊急事態が発生した場合のビジネス活動およびお客様への供給体制の継続・早期復旧を目的に「朝日インテックグループBCP（事業継続計画書）」の構築を進めています。有事の際はこれに基づき、優先業務の継続・早期復旧を実現するための作業、企業運営に不可欠となる作業をグループごとに定義し、対応を行っています。

BCP 基本方針

1. 各人の生命・身体の安全確保を最優先に行動する。
2. 被害状況を把握の上、会社の正常な業務活動の早期回復を図り、お客様への影響を最小限とするよう努める。

生産拠点に関するBCP（事業継続計画）

当社グループはBCP（事業継続計画）として、タイ工場、ハノイ工場、セブ工場の3拠点への生産の分散化を進めています。
タイ工場からハノイ工場への生産移管を進めるとともに、ハノイ工場からセブ工場への生産移管を進めています。移管にあたっては、タイ工場やハノイ工場で設計・製作した製造設備や機器・治具等をセブ工場に導入するなどし、安定した製造ラインの構築を実施しています。
当社グループは、患者様の命に関わる製品を世に送り出している医療機器メーカーの使命として、どのような事態においても製品を安定供給できる体制を構築することが求められています。



情報セキュリティ基本方針

❶基本方針

日々深刻化する情報セキュリティリスクに対処すべく、情報セキュリティに関する法令・ガイドライン、その他の社会的規範を遵守した上で、当社のお客様および当社の事業を守るために必要な情報セキュリティ対策を下記の観点に基づいて実施しています。

❷情報セキュリティ管理体制

当社グループでは、情報セキュリティ体制を推進すること、情報セキュリティに関するリスクを管理すること、および組織横断的に各種施策の実施を徹底することを目的として、セキュリティ統括責任者を置き、情報セキュリティに取り組んでいます。

情報セキュリティ強化の取り組み

情報セキュリティ対策の実施

当社グループは「情報セキュリティ規程」を作成し、サイバー攻撃や設備の損壊・通信トラブルによる情報資産の漏えい、改ざん、紛失および情報システム停止等のリスクを低減するため、人的、組織的、技術的対策を実施しています。昨今の巧妙化・多様化する情報セキュリティリスクへ対応すべく定期的に対策の見直しを行い、発生しうるリスクに対し適切に優先度を判断しつつ、継続して対策実施を進めています。

情報セキュリティ教育

当社グループでは、情報セキュリティ教育として入社時に集合研修を実施し、また、E-Learningを活用し定期的なセキュリティ教育コンテンツを配信するなど、倫理観およびセキュリティ意識の醸成を目的とした活動を実施しています。その他、標的型メール攻撃訓練の実施や当社内外を問わず発生したインシデントのうち当社の教訓になると考えられる事象および世間で流行している不審メールやウイルスについての最新の動向などの情報を社内に向けて日常的に発信することで、セキュリティ意識の維持、向上に努めています。今後も、当社グループがこれまで実施してきた情報セキュリティ教育の内容の充実化を図るべく、セキュリティ教育コンテンツの追加や訓練の種類・実施回数の拡充等を継続的に実施いたします。

インシデント対応

当社グループでは、サイバー攻撃やランサムウェア、情報の漏えいなどの発生を監視し遮断する仕組みを導入するとともに、インシデントが発生した際の受け付け、対応支援、および再発防止策の検討など、インシデント対応に必要な体制（CSIRT）を事前に整備しています。被害の拡大や二次被害の発生を抑制するため、迅速かつ効果的なインシデント対応が可能になるよう、必要な体制や手順などを継続的に見直し、当社グループとしてのインシデント対応の能力を継続的に高めています。

内部監査

情報セキュリティの徹底に向けて内部監査を定期的に実施しています。特に個人情報や秘密情報の取り扱いについての監査に重点をおき、改善が必要と認められた場合には改善策の実施が完了するところまでフォローする体制を敷いています。

人的対策

- **情報セキュリティ・インシデント（事故）発生時の対応体制を整備**
  CSIRT(シーサート：Computer Security Incident Response Team)体制を構築し、脆弱性情報などの収集や分析、インシデント発生時の対応、社内外の組織との情報共有や連携する仕組みを整備
- **情報セキュリティ教育の実施**
  全社を対象とした標的型攻撃メール訓練や、インシデントの発生を想定した訓練を実施

技術的対策

- **PC/ サーバセキュリティの強化**
  【コンピュータウイルス対策】全サーバ、PC に対して不審な動きを常に監視し、検知した場合、即遮断できる仕組みを導入
  【バックアップ環境整備】重要なサーバに対して、データ消去や暗号化などされた場合に、データを復旧できる環境を整備
- **インターネットセキュリティの強化**
  【WEB フィルタリング】詐欺サイトなどの不審・悪質な WEB サイトへのアクセスを遮断する仕組みを整備
  【メール対策】不審メールや詐欺メールなどを検知・受信拒否する仕組みを整備
- **ネットワークセキュリティの強化**
  社内ネットワークへの接続について制限する仕組みを整備

ご参考：リスクモデル

想定されるリスク例

投資家の判断に影響を及ぼす可能性のあるリスクのほか、幅広いリスクとして、右のようなものがあります。なお、文中における将来に関する事項は、2025年5月期末時点において、当社グループが判断したもので、7つのサステナビリティの重要課題と関連付けることができます。

		重要課題
①医療機器分野について	法的規制について	安全・安心な製品の供給
	医療制度改革について	安全・安心な製品の供給
	品質管理体制について	安全・安心な製品の供給
	特定製品の依存について	イノベーションを通じた現場の課題解決
	特定地域への売上依存について	リスクマネジメントの強化
	技術革新への対応について	イノベーションを通じた現場の課題解決
	特定取引先からの仕入れについて	サプライチェーンマネジメント
②産業機器分野について	客先仕様であることについて	
	競合状況について	イノベーションを通じた現場の課題解決
③各事業共通事項について	海外事業展開について	リスクマネジメントの強化
	海外生産への依存について	サプライチェーンマネジメント
	原材料価格の高騰について	サプライチェーンマネジメント
	知的財産権について	イノベーションを通じた現場の課題解決
	自然災害や大規模災害などについて	リスクマネジメントの強化
	疫病や感染症による影響について	リスクマネジメントの強化
	気候変動によるリスク	環境負荷低減への取り組み
④全社的な事項について	為替リスクについて	
	保有株式に関するリスクについて	コーポレートガバナンスの強化
	企業買収に関するリスクについて	コーポレートガバナンスの強化
	減損・評価損に係るリスクについて	コーポレートガバナンスの強化
	情報セキュリティ	リスクマネジメントの強化
	人財確保に関わるリスク	グローバル人財基盤の強化
	人権リスク	サプライチェーンマネジメント