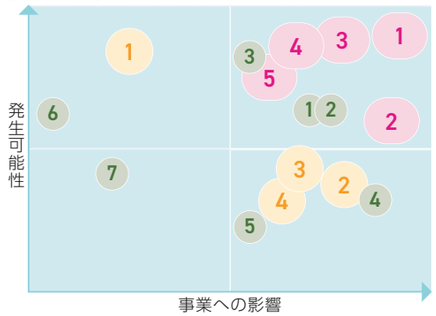
全社重要リスクへの対応

レゾナックでは、CEOが議長を務めるリスクマネジメント委員会を設置し、リスクマネジメント体制やグループの重要リスク、その対応策などについて、トップマネジメントによる組織横断的な審議を行っています。全社の重要リスクテーマについては、リスクマネジメント委員会での検討内容をもとに、2024年6月の経営幹部勉強会で特定、2025年3月の経営幹部勉強会で年次の見直しを行いました。

モニタリングレベル（※）	2025年全社重要リスクテーマ
S	① AI×人材：AIの台頭による人材ポートフォリオの再構築 ② カントリーリスク、経済安全保障 ③ AIによる技術革新と市場変化がもたらすリスク ④ 設備投資の遅れ：高度化・自動化の遅れ New ⑤ サプライチェーンマネジメント（SCM）課題 Aランク▸Sランク
A	① 情報漏洩、サイバー攻撃　③ 環境規制リスク ② 不正・腐敗、コンプライアンス不祥事　④ 人権リスク
B	① 予測困難な市場　⑤ ITインフラ未整備 ② 業界再編　⑥ 国際課税 ③ 品質問題　⑦ 金利変動 ④ 設備の老朽化

（※）**Sランク**
会社運営上の最重要リスク
Aランク
会社目標達成上の重要リスク
Bランク
事業運営上の重要リスク

2025年全社重要リスクヒートマップ

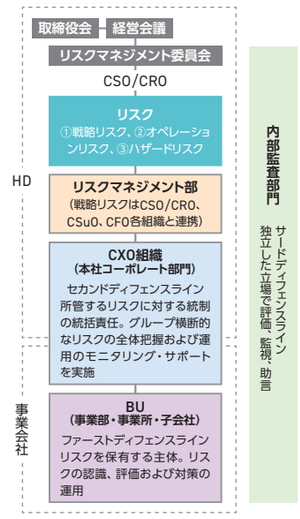


レゾナックのリスクマネジメント体制は、内部統制システムの重要な機能として取締役会で決議され、報告・監視体制を定めています。事業に影響を及ぼす経営上のリスクに総括的、個別的な対処を行うため、当社グループのリスクマネジメント規程において、執行機関や責任部署を設置するとともにISO31000その他の規格に準拠した管理手法を整備しています。

リスク対策の実行においては、ボトムアップでの全社リスク棚卸とトップダウンでの全社重要リスクの特定を組み合わせ、現場目線と経営目線の双方向からのリスクアプローチを行う総合的リスクアセスメントを確立しており、外部環境の変化を反映した仕組みとしています。

全社重要リスクヒートマップ分析において、Aランク以上のリスクテーマを全社重要リスクとし、各リスク対応の"旗振り役"となる推進組織を決定し、対応しています。また、Bランクのリスクテーマは個別リスクとし、各組織にて対応しています。

リスクマネジメント体制



全社重要リスク

ランク	全社重要リスクテーマ	リスク分類	旗振り役／推進組織	具体的なリスク事象
S	AIの台頭による人材ポートフォリオの再編	人事・労務	CHRO	・生産性向上による人員余剰の発生 ・従業員の既存スキル陳腐化
S	カントリーリスク、経済安全保障	事故・災害	CSO/CRO	・各国の自国第一優先政策により、売上減少やサプライチェーン途絶、市場アクセス制限のリスクが上昇 ・軍事衝突による従業員の安全リスクや拠点の資産接収、生産停止・遅延、業務停止・遅延リスクの上昇
S	AIによる技術革新と市場変化がもたらすリスク	経営（事業投資）	CTO	・AIの普及が進むことによる競争力や市場環境の変化に伴う、自社事業実施への影響
S	サプライチェーンの不安定性	調達・物流	CMEO/CQO	・原料輸入元の国で輸出規制が発動され、原材料が入手できなくなる
A	情報漏洩、サイバー攻撃	情報管理	CDIO（IT統括）	・ランサムウェア感染などによる先端技術情報・顧客の個人情報などの窃取、生産システム・基幹システムの停止 ・内部者による意図的な秘密情報の持出
A	不正・腐敗、コンプライアンス不祥事	コンプライアンス	CSuO	・コンプライアンス違反の発生によるステークホルダーからの信頼低下によって生じる取引停止の影響やレピュテーション損失による企業価値の棄損
A	人権リスク	経営（サステナビリティ）	CSuO	・規制の対応遅れによる事業機会の損失：欧州を中心とする新規制の対応遅れによる欧州への出荷・流通停止の影響
A	環境規制			

各全社重要リスクテーマにおいては、リスクシナリオ分析を行い、予防的対策を行っています。Sランクで特定したカントリーリスクについては、売上分析による重点対応地域・事業の特定を行った上で、CXO・BU連携による外部環境リスクのモニタリング継続や地産地消型の生産・供給体制構築を進めることでリスクの最小化に取り組んでいます。

例）カントリーリスクのリスクダッシュボード

ランク	全社重要リスクテーマ	旗振り役組織	リスク事象	モニタリング指標（KRI）
S	カントリーリスク	CSO/CRO	米中の経済安保政策加速によるグローバル市場の混乱	米国、中国の外交政策／産業政策

「サプライチェーンの不安定性」リスクシナリオ

リスクイベント：**米中の経済安保政策（自国保護政策、自国産業育成政策）の加速により、売上減少やサプライチェーン途絶リスクなどが上昇**

注視する政策分類		注視すべきリスクシナリオイベント			当社への主な影響
保護政策	①輸入関税の引き上げ	影響地域	当社業界に影響するリスクシナリオ		
	②資源の輸出入規制の加速	米中・各国	**米国の関税引き上げ**を引き金とした、米中間の関税報復合戦。また、その他各国への波及。	A	（特に対中・対米の）輸出製品の価格競争力低下、売上減少、各国によるサプライチェーン組換の発生
	③先端半導体関連の輸出規制強化	グローバル	デュアルユース規制として、**重要鉱物の輸出規制／販売規制が加速する。**	B	（特に中国からの）原材料調達が途絶し、生産が継続できない
	④貿易協定の見直し				
育成政策	⑤自国産業への支援／国策内製化	中国	**中国への輸出規制**として、半導体とその製造装置・技術だけではなく、**半導体材料にも適用が拡大する。**	C	中国向け輸出売上の減少

対応策／計画

予防的対策（平常時）
- CXO/BU連携による外部環境リスクのモニタリング継続（地政学リスク、トランプ2.0動向など）
- 地産地消型の生産／供給体制構築などによるリスク最小化

※調達リスクの高い購入品目を特定し、対策を推進

事後対策：関係部門による対策チームを構成し、対応を協議／実行する。

対応中の施策例

- 全社配信のカントリーリスクレポート

- 台湾有事退避計画の策定

- 役員シミュレーションを実施
- 人命安全を最優先することを改めて確認した上で、待避計画の策定を決定

▶

対応中
- 人員退避方針（事態緊迫時の行動ワークフロー作成）
- 有事発生時の情報収集
- 現地法人への権限移譲

当社にて発生したセキュリティインシデントについて

最高デジタル情報責任者（CDIO）
能丸 実

2025年5月20日未明に、当社および当社グループの一部サーバーやPC内のファイルが改ざんされる障害が発生しました。その後の調査でランサムウェアを使ったサイバー攻撃と確認したことから、迅速に対応を進めるべく緊急対策本部を立ち上げました。被害拡散を抑えるため、直ちにネットワークの遮断などの措置を行ったため、当社および当社グループ内のシステムが一部使用できなくなり、業務にも停止などの影響が生じました。その後、外部専門家の協力のもと詳細な調査を開始しました。また、警察への被害の届け出や関係省庁との連携などを進めるとともに、関係者の皆さまへの影響を最小限に止めるべく対応を継続して実施しました。

緊急対策を講じた結果、7月4日には、製品供給に支障がないこと、および外部専門家によるマルウェア解析の結果、当社ネットワークとお客さまのネットワークの接続において、感染が広がることはないことが判明しました。

本件において、お取引先さま、関係先の皆さまに多大なるご心配とご迷惑をおかけしましたことを、深くお詫び申し上げます。

今回の原因として、外部の攻撃者が何らかの方法で当社グループのネットワークに侵入し、ランサムウェアを起動させたことを確認しています。今後このようなことを招かないよう、対策を徹底していきます。

2025年5月20日
- ①当社の一部サーバーに対して、外部からの攻撃が確認され、ランサムウェアの感染を確認
- ②直ちに、外部専門家の協力のもと調査を開始し、迅速に対応を進めるべく緊急対策本部を立ち上げ

6月9日
- CDIOを中心とする対策本部に移行

7月4日
- 外部専門家によるマルウェア解析の結果、当社ネットワークとお客さまのネットワークの接続において、感染が広がることはないことを公開

緊急対策実施 ▶ 一過性ではない、再発防止を見据えた長期的な対策

今後1.5年程度で、インシデントに即応可能な体制の構築を目指す。さらに、3年以内には、ランサムウェア以外の高度な脅威についても予測・検知し、高度なセキュリティ体制の確立を目指す。