

マテリアリティの取り組み

リスク管理体制の整備

マテリアリティ

- 全ての有価証券報告書開示リスクについて、主管部署による評価が実施され、優先的に対応すべきリスクが特定されている。
- 優先的に対応すべきリスクが事業に与える影響を低減する。また、低減活動の進捗および残存リスクを管理する。



ガバナンス

マテリアリティ特定背景

リスクを適切に管理すべき主管部署が特定されない、あるいはリスク評価が実施されず優先的に対応すべきリスクが特定されなければ、予期せぬ事態が発生した際に適切な対応が取れず、事業に深刻な影響を及ぼす可能性があります。NIDECグループでは事業に影響を及ぼすリスクをグローバルな視野で中長期的なリスクと日常的なリスクの両方を見据え、事業継続の確保を図っています。そのために、リスク事象の調査・評価を、現状対策の実効性を確認しながら実施する仕組みを整えています。

2023年度の取り組み

リスク主管部署が評価の対象とするリスク事象が、社内外の事業環境の変化や顧客の要請を反映しているかどうかを精査するとともに、リスク評価者の負荷低減を目指して対象リスク事象の絞り込みを実施しました。

今後に向けて

リスク評価で特定された主要リスクについて設定したKRI (Key Risk Indicator) の定期的モニタリングに加え、個別案件の課題と対応策についても取締役会および経営会議にて報告のうえ、NIDECグループ全体でリスク管理活動の効果を検証していきます。

リスク調査・評価活動

図1に示した階層ごとに、事業所長、部門長、その他NIDECグループのリスク管理に係る諮問機関である「リスク管理委員会」で定められた者が、定期的に事業に影響を及ぼすリスク事象の調査・評価を行います。対象とするリスク事象は大きく以下の4つに分類されます。

- 経営戦略リスク
- 事業運営リスク
- ガバナンスリスク
- 偶発的リスク

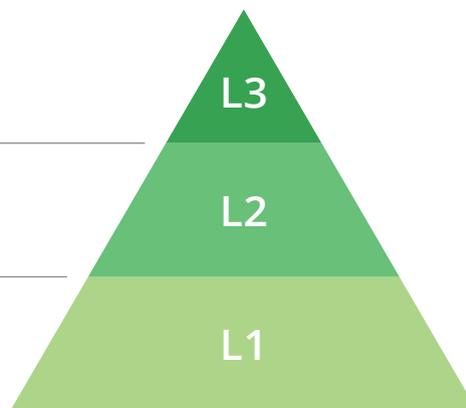
リスク調査・評価にあたっては、現状のリスク管理活動とリスク低減対策の実施状況を確認のうえ、残存リスクのモニタリングを行い、結果を他の階層の施策に相互利用しています。例えば、L2で特定されたリスクについてはL3でも内容を確認し、その中にL3主導で改善しなければならない全グループ共通の課題を発見した場合は適宜L3のリスク管理活動に反映するなど、階層別リスク管理活動を相互に関連づける動きを進めています。

リスク調査・評価活動(図1)

コーポレートレベル
(リスク主管部署)

事業本部レベル

事業所レベル



L = Level (階層)

特に重要なリスク一覧

2023年度にL3で評価の対象となったリスク事象のうち、当社の事業に大きな影響を及ぼすと考えられる「特に重要なリスク」は図2の通りです。その他、事業などのリスクとその対応策の詳細については有価証券報告書 第51期(提出日：2024年6月19日)に記載しています。

リスクレベルはリスク対策実施後の残存リスクに対して、発生の可能性と結果の重大性を5段階に分類したうえで図3のマトリックスにあてはめ、重大・高・中・低の4段階で評価した結果です。

特に重要なリスク(図2)

リスクの分類	リスクの内容	主な対応	リスクレベル
1. 経営戦略リスク			
政治・経済状況の変動に係るリスク	当社の製品が生産・消費される国または地域の予期せぬ景気変動・沈滞、政治・政策動向の悪化	<ul style="list-style-type: none"> 地営地開(現地における営業および開発活動)、地産地消(現地における生産および販売活動)の推進など、地域と一体となった事業活動の推進、事業機会の最大化 事業ポートフォリオの適時確認・見直しによる既存事業のビジネスモデルに対する依存度の低下と事業および組織の新陳代謝の促進による持続可能な企業成長 	高
技術環境・産業構造の変化に係るリスク	技術変遷を背景とした需要の変容、それに呼応する顧客動向の当社の想定を上回る変化	<ul style="list-style-type: none"> 新規商材へのリソース集中投下など、ビジネスポートフォリオ転換の早期化 	高
競合に係るリスク	<ul style="list-style-type: none"> 既存市場の成熟化、技術の陳腐化など市場環境の変化 競争激化、他社の新規参入、競合の戦略変更など競合関係の変化 	<ul style="list-style-type: none"> 研究開発分野への投資の維持・増強、製造能力・販売力・マーケティング力の拡大 新製品のタイムリーな投入 既存製品における収益性の更なる改善 利益性確保のためのコスト削減活動 	高
先行投資に係るリスク	<ul style="list-style-type: none"> 技術革新による設備の陳腐化、滞留在庫、人的余剰 需要の過小評価による設備投資不足 	<ul style="list-style-type: none"> 設備投資の決定過程における必要性・投資回収可能性・投資金額の徹底的な検討 毎月の計画に対する達成度の確認と適切な施策の打ち出しの検討・損失リスクの最小化 陳腐化による経済的価値の棄損の最小化 投資金額の最小化による金額リスクの低減 	高
M&Aに係るリスク	<ul style="list-style-type: none"> 買収した事業の業績悪化、キーパーソンの喪失 事前調査(デュー・ディジジェンス)の不備による損害 	<ul style="list-style-type: none"> 買収対象企業は、当社事業戦略に沿った企業を選定 事前調査を徹底し適正価格で買収 買収後の迅速かつ徹底したPMI 当社の経営理念や経営手法を全従業員に深く浸透させ、当社グループ入りによるシナジー効果を創出しながら、買収対象企業の企業価値を向上してのれん減損リスクを極小化 	重大
2. 事業運営リスク			
高度な専門性を有した人材の採用・保持に係るリスク	新市場に対する高い知見・スキルを持つ人材の不足	<ul style="list-style-type: none"> 3つの人事制度改革(評価制度・等級制度・報酬制度)の段階的導入 専門性の高い人材の採用、幹部人材の確保、育成プロセスの強化 	中

リスクレベル特定マトリックス(図3)

		発生の可能性				
		5 (1年に1回以上)	4 (3年に1回以上)	3 (5年に1回以上)	2 (10年に1回以上)	1 (30年に1回以上)
結果の重大性	5 (事業存続が問われる大問題となる)	重大	重大	重大	重大	高
	4 (事業活動に広域的・長期的影響が出る)	重大	重大	重大	高	中
	3 (事業活動に広域的または長期的影響のいずれか一方の影響が出る)	重大	高	高	中	低
	2 (事業活動に限定的・短期的影響が出る)	高	高	中	低	低
	1 (業務活動に対する影響が分らない程度、または、すぐに解決できる程度)	中	中	低	低	低

情報セキュリティ対策の推進

マテリアリティ

- 重大な情報セキュリティ事故の発生件数をゼロにする。

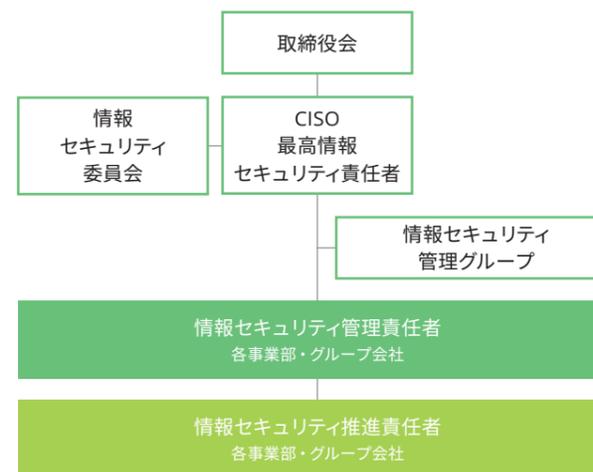


ガバナンス

マテリアリティ特定の背景

NIDECグループは自社で生成・収集するもののほか、取引先などからお預かりするものも含めて事業活動を行なううえで必要な情報を保有しています。そのため、これらの情報資産を適切に保護し、適正に使用することが非常に重要であると認識しています。保護対象には経営情報や技術情報、財務情報、個人情報をはじめとして重要性の高いものがあり、これらが毀損や漏えいした場合には顧客や市場の信頼を失うとともに、自社の競争上の優位性の低下を招き、また法制上のペナルティの対象となる可能性があります。変化・増大する情報セキュリティリスクを把握・評価し、リスクに応じた有効な対策を講じることで、重大なセキュリティ事故の発生防止に取り組んでいきます。

情報セキュリティ体制図



2023年度の取り組み

サイバー攻撃など社外の脅威に備える従来の取り組みに加えて、「内部に潜む脅威」への対策の取り組みを進めました。内部からの情報漏えいの原因の一つに、社員の不注意や社内ルールを軽視した「過失」があります。これによる情報漏えいを防ぐために、自身の不注意やルール

を逸脱した行為が引き起こす結果の重大性を含む教育・注意喚起を繰り返し実施し、その浸透を図りました。また、内部関係者が悪意をもってする行為を抑止・検知する仕組みの導入に取り組みました。2023年度においてはサイバー攻撃などによる重大事故は発生しませんでした。

今後に向けて

2024年度に入って経験したサイバー攻撃を踏まえ、NIDECグループ幹部で構成する情報セキュリティ委員会の指示のもと、NIDECグループ全体において高位かつ均質な情報セキュリティ対策の実現と継続的な改善に取り組んでいきます。

物理的セキュリティの強化

事業所間をネットワークで接続するサイバー空間とは異なり、事業所の内部に区画を設け、その機密性に依拠して許可された者だけが当該区画に入ることができるよう施錠、認証、監視、記録などの機能を備える物理的セキュリティ対策について、これまでは事業所それぞれで取り組む形となっていました。しかしNIDECグループとしての標準的なガイドラインを設けることで、いずれの事業所においても均質なセキュリティの確保を実現します。

インシデント対応

当社グループ内において情報セキュリティ事故が発生した場合の対応について、それにあたる有事の体制(インシデントレスポンスチーム)の設置基準や、そこに参画する組織、責任者の役割、また対応すべき項目と手順を整理し、NIDECグループの標準として整備します。そして、整備した手順に沿った演習や訓練を実施することで、その記載内容の実用性・実効性の検証も行います。これらの活動によりNIDECグループにおいて均質かつ網羅性がありまた遅滞のない有事対応を可能となります。

従来グループ内の各社で実施してきた対策項目についても、その標準化を順次進めることで、NIDECグループ全体でビジネスを支えられる適正な情報セキュリティ管理を実現するための改善を継続していきます。