マテリアリティ12

リスクマネジメントの強化

重要と考える理由

リスクを的確に把握して、その影響を最小化するため事前に対策を講じるリスクマネジメントは、地政学リスクの増大、デジタル変革、気候変動など、企業を取り巻くリスクが多様化する中で、その重要性が高まっています。

また、感染症・伝染病のパンデミック、首都直下地震や南海トラフ巨大地震のような大規模災害、国際紛争や戦争などの有事に備えて、必要な準備や手配をしておくことが、被害の最小化やリスクの軽減につながります。

中長期的な視点で、変化するさまざまなリスクを把握し、経済・環境・社会といった分野で生じる影響を踏まえて、対策を講ずることは、企業の持続的な成長へとつながります。

コミットメント

企業を取り巻くリスクは、急速なテクノロジーの進化やグローバルでの社会・経済情勢の変化などにより、多様化、複雑化しています。こうしたリスクに適切に対応できなければ、顧客や株主などのステークホルダーの信頼を失い、企業の存続にも関わるダメージを受けることにもなりかねません。実効性のあるリスクマネジメント体制の整備は、ますます重要になっています。

ニコングループでは、毎年リスクアセスメントを実施して、全社的な重要リスクの洗い出し、分析・評価を行い、対応状況を定期的にモニタリングしています。また、グループとしてのリスク対応の実効性をより高めるために、内部統制推進体制を強化して、事業活動を健全かつ効率的に運営するために日々の業務の管理ポイントをまとめた「管理標準」を策定しました。今後はその「管理標準」を活用して、内部統制改善プロセスの確立を進めていきます。また、経営環境や事業構造の変化を踏まえつつ、グローバルでのリスク対応力の強化を図るため、効率的かつ柔軟性の高いグループガバナンス体制を整備していきます。

代表取締役 兼 専務執行役員
CRO、経営管理本部長　小田島 匠
※ CRO：Chief Risk Management Officer

【活動方針】

- ニコングループ情報セキュリティ基本方針
- ニコングループ個人情報保護方針

【体制】

- リスク管理委員会
- 品質委員会
- 輸出審査委員会
- コンプライアンス委員会

●2022年度のマテリアリティに対する目標と実績

自己評価　○:達成　△:着手したが未達成

2030年度目標	ニコンとして取り組むべきこと	関連するSDGs	対象範囲	2022年度目標	2022年度実績	自己評価
現状および将来のリスクとインパクトが特定され、体制整備と改善を図るPDCAが運用されている ITインフラの健全な運用と管理、サイバーセキュリティや個人情報保護への対応により、経済的損失と会社レピュテーションの棄損を避けれている	リスクアセアスメントの実施と、高リスク項目の改善指示を行う	―	ニコングループ	リスク把握調査、本社管理部門や監査部門を含めた全社としてのリスク認識の共有と把握	リスク把握調査を実施し、重要リスクに対する対応強化策をまとめ、2023年3月開催のリスク管理委員会に報告	○
	情報セキュリティ(サイバーセキュリティ、個人情報保護)の体制を強化する		ニコングループ	情報セキュリティ(サイバーセキュリティ、個人情報保護)の体制を強化し、適用を受ける各国法令に継続的に対応する	ニコングループ間のグローバルなネットワーク環境をよりセキュアなものとするための施策を計画通り進行 また、適用を受ける各国個人情報保護法令に必要な対応を進めた	○

リスクマネジメント

基本的な考え方

ニコングループでは、ニコンおよびグループ会社の持続的発展を目的に、企業経営に重大な影響を及ぼすあらゆるリスクに対し、適切な対応を図るためのリスクマネジメントを実施しています。

体制

ニコングループでは、経営に重大な影響を及ぼすリスクに対して適切に対応できるよう「リスク管理委員会」を設置しています。本委員会はリスク管理を統括する組織として、代表取締役であるCROを委員長とし、経営委員会メンバーなどを委員、総務部と内部統制推進室を事務局としています。2022年度は、10月と3月の合計2回、委員会を開催しました。

重大リスクに対してより効果的な対応を図るため、重点対象のリスクについて継続的なモニタリングや、機動的な支援ができる体制を構築しています。2023年度は、内部統制改善のプロセス確立や、輸出管理体制の整備、BCMの見直しといったリスクマネジメントの強化に取り組む計画です。

なお、リスク全般についてはリスク管理委員会が管轄していますが、専門的な対応が必要なリスクに対しては、その傘下の品質委員会、輸出審査委員会、コンプライアンス委員会の3つの委員会で対応を図っています。また、サステナビリティの視点から、サステナビリティ委員会でもマテリアリティを中心としたリスクのモニタリングを行っており、リスク委員会と適宜連携し、「環境」「社会・労働」に関するリスクにも対応を図っています。

2022年度のリスク管理委員会の主な活動テーマ

・重点モニター対象会社の進捗＆課題
・内部統制関連（内部統制推進体制構築、管理標準策定）
・2022年度 全社リスク把握調査報告
・係争案件調査結果報告
・各国の個人情報保護法への情報セキュリティ対応

●リスク管理に関わる主な専門委員会

委員会	主な取り扱いリスク
リスク管理委員会	リスク全般
品質委員会*	品質全般
輸出審査委員会*	外為法違反防止、安全保障リスクの管理
コンプライアンス委員会*	コンプライアンス全般
サステナビリティ委員会	サステナビリティ全般、特に環境（気候変動、化学物質管理、水など）、社会・労働（人権など）
生命倫理審査委員会	生命倫理全般

＊リスク管理委員会の傘下委員会

リスクアセスメント

ニコングループでは、地域紛争や感染症などのリスクを含め、自社グループが抱えるリスクを把握するため「リスク把握調査」を実施しています。この調査は、ニコンの部長相当以上および国内・海外グループ会社社長に実施しているもので、調査の結果は、影響規模と発生確率で表す「リスクマップ」の形式とし、リスク管理委員会に報告しています。

2022年度は、リスク把握調査アンケートのリスク分類を現在の経済的・社会的・環境的な観点で主要なリスクに沿って大幅に見直し、リスクの特定に取り組みました。

新型コロナウイルス感染症やロシアのウクライナ侵攻などによる物流の混乱やサプライチェーンの途絶、米中対立などのカントリーリスクにも関連部門と連携してリスク管理体制の整備を進め、リスクの軽減を進めていきます。

関連情報

決算短信では、経営成績・財政状態に関する分析における事業等のリスクを開示しています。

Web 決算短信（2023年3月期 p.06～08）
https://www.jp.nikon.com/company/ir/ir_library/result/pdf/2023/23_4qf_c_j.pdf

気候変動によるニコングループへのリスク（➡ p.073）

BCM*1活動への取り組み

ニコングループでは、大規模災害や感染症などの発生に備えてBCP*2を策定し、見直しています。

2022年2月に起きたロシアのウクライナ侵攻では、侵攻直後から、生産本部や事業部門を中心に関連部門と定期的な状況確認を行い、その後の不測の事態の対応に備えました。

新型コロナウイルス感染症に対しては、在宅勤務やリモートワークを活用、全社的な感染予防を図りながら、事業活動の継続に努めました。

国内ニコングループでは、高い発生確率で想定される「首都直下地震」や「南海トラフ巨大地震」などの大規模地震や、昨今の台風・洪水などの自然災害の甚大化に備えて、非常時の通信ツールを見直し、災害時を想定した通信訓練などの各種訓練を実施しました。

＊1 BCM（Business Continuity Management）：事業継続マネジメント。BCP策定や維持・更新、事前対策の実施、教育・訓練の実施、点検、継続的な改善などを行う平常時からのマネジメント活動。
＊2 BCP（Business Continuity Plan）：事業継続計画。大地震等の自然災害、感染症のまん延など不測の事態が発生しても、重要な事業を中断させない、または中断しても可能な限り短い期間で復旧させるための方針、体制、手順などを示した計画。

情報資産とサイバーセキュリティのリスクマネジメント

情報資産の管理方針

ニコングループでは、保有する情報資産の管理およびセキュリティに関して「ニコングループ情報セキュリティ基本方針」を定め実践しています。本方針に基づき「ニコングループ情報管理規程」などの社内規程を定め、国・地域の状況に応じて、情報資産を適切に保護し業務遂行の適正化および効率化を図っています。これらの規程類は、従業員がいつでも確認できるよう社内ポータルサイトに掲載されています。

Web ニコングループ情報セキュリティ基本方針
https://www.jp.nikon.com/company/sustainability/governance/risk-management/security_policy.pdf

情報管理体制

ニコングループでは、個人情報保護を含む情報管理において代表取締役 兼 社長執行役員を最高責任者と定めるとともに、情報セキュリティマネジメントシステム（ISMS＊）に準拠した業務プロセスを構築しています。この運用においては、代表取締役である情報セキュリティ推進部担当の役員のもと、情報セキュリティ推進部がグループ全体の管理・統括を行い、サイバー攻撃対策をはじめとした情報セキュリティに関する施策の立案や体制整備・維持にも取り組んでいます。

また、ニコングループでは、ニコンの事業部、本部、グループ会社ごとに各組織長を情報管理の責任者と定めており、情報セキュリティ推進部と連携することで、グループ全体を統括的に管理しつつ、それぞれの国・地域の状況にも対応した情報セキュリティの管理体制を整備しています。情報資産リスクの中で重要な案件は、経営委員会メンバーなどで構成される「リスク管理委員会」にてレビューを受けています。

なお、ニコンのヘルスケア事業では、特に厳格な情報管理が要求される医療用の診察・診断支援AIの研究および開発において、ISMSの認証規格であるISO 27001を取得しています。

＊ ISMS：Information Security Management System

情報セキュリティインシデント対応

ニコングループでは、情報セキュリティ事案発生時に、発生現場から直ちに情報セキュリティ推進部へ報告することを義務付けています。情報セキュリティ推進部は、関係部門と協力し、被害や影響を最小限に抑える体制と手順を整え、事業を迅速に再開できるプロセスを確立しています。重大な事案は、情報セキュリティ推進部から担当役員へ迅速に報告しています。また、情報セキュリティ推進部のメンバーに対し、社外の専門家によるインシデント対応時の訓練講習を実施しました。

なお、過去3年間において、罰金、補償金支払いを伴う重大な情報セキュリティ事故はありませんでした。

情報セキュリティ教育

ニコングループでは、情報セキュリティに関する従業員への意識付けおよび実効性の向上のため、入社時研修などで、eラーニングでの情報セキュリティ教育を実施しています。この教育プログラムには、情報管理に関する方針やルールなどに加え、具体的事例も盛り込んでいます。

また、社内規程や会報などで通知した情報セキュリティ施策を分かりやすく解説した教育資料「ニコングループ情報セキュリティハンドブック」を従業員全員がいつでも参照できるようにポータルサイトに掲載しています。このハンドブックを通じて、従業員一人ひとりが情報管理の重要性を理解し、高い意識で規程を遵守できるよう、継続的な教育に取り組んでいます。

2022年度は、例年通り2月を情報セキュリティ月間と定め、社内報で啓発を行い、また国内グループ会社を対象に、eラーニングを実施しました。また、定期入社社員向けには、講師による新人研修を実施しました。海外グループ会社においても、適宜eラーニング、またはその他の手法で情報セキュリティ教育を実施しました。

これらの教育により、従業員への情報セキュリティの徹底を図っています。なお、万が一、従業員が関連規程に違反し、情報漏えい等の事案を発生させた場合には、当該従業員に対し、その所属する会社の就業規則に基づき懲戒処分を行う可能性があります。

情報セキュリティ監査

ニコングループでは、情報セキュリティの徹底に向けて、「ニコングループ情報管理規程」に基づき、内部監査を定期的に実施しています。

2022年度は、国内ニコングループの全部門に対する書面監査を実施し、重要テーマに基づき選定した部門に対して実施監査を行いました。その結果、重大なリスクは発見されませんでした。2023年度も適正に情報セキュリティ対策が実施されていることを確認するため、テーマを定めて監査を行う予定です。

個人情報保護

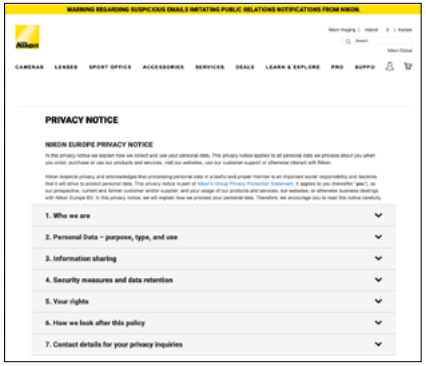
ニコングループでは、プライバシーの尊重、個人情報の適法・適切な取り扱いは重要な社会的責務であると捉え「ニコングループ個人情報保護方針」を定めています。この方針のもと、グループ共通の規程として「ニコングループ個人情報取扱規程」を定め、グループ内に周知するとともに、情報管理体制のもと、この規程に則って個人情報を取り扱っています。

さらに、経営委員会メンバーなどで構成される「リスク管理委員会」の傘下に「個人情報保護部会」を設置し、ニコングループ全体のプライバシーや個人情報に関するリスク管理を行っています。

具体的な取り組みとしては、お客様に対してニコングループ各社のウェブサイトなどを通して関連法令に則ったプライバシーノーティスを提示し個人情報の利用目的、個人情報削除などの個人の権利、個人情報に関する問い合わせ窓口などを通知しています。

また、調達パートナーに対して、個人情報の保護を含めた情報セキュリティを遵守するよう「ニコンCSR調達基準」に定め、要求しています。

Web
ニコングループ個人情報保護方針
https://www.jp.nikon.com/privacy/group/
EU一般データ保護規則(GDPR)に則ったNikon Europe B.V.のPrivacy Notice
https://www.nikon.ie/en_IE/privacy-notice/
ニコンCSR調達基準
https://www.jp.nikon.com/company/corporate/procurement/csr/



EU一般データ保護規則(GDPR)に則ったNikon Europe B.V.のPrivacy Notice(抜粋)

各国法への対応

ニコングループでは、高度な情報セキュリティ管理体制による個人情報の適切な管理を実現すべく、EU一般データ保護規則(GDPR)をはじめとした各国の個人情報保護法を遵法し、違反を未然に防ぐ体制の整備を進めています。

2022年度は、タイの個人情報保護法への対応を進め、タイのグループ会社にてプライバシーノーティスの掲載、その他必要な対応を行いました。アメリカ合衆国カリフォルニア州消費者プライバシー法に基づきプライバシーポリシーの見直しを実施しました。その他の国・地域の個人情報保護関連法令の立法・改正動向などについて、継続的に情報収集を行っています。また、個人情報保護法に関するセミナーを開催し、従業員の啓発を進めました。

2023年度においても、各国・地域の個人情報保護関連法令の立法・改正動向にあわせ、必要な対応を進めていきます。

サイバーセキュリティのインフラ整備とプロセス改善

高度化・巧妙化するサイバー攻撃に対し高い防御力を維持するために、ニコングループでは、サイバー攻撃の早期発見と早期対応のため、グローバルで一括して監視・対応する運用体制の改善・強化を進めています。また、フィッシング詐欺などの電子メールをフィルタリングするシステムの展開も進めています。

このほか、従前の業務プロセスの改善などにも継続的に取り組んでいます。例えば、サイバー攻撃の入り口にもなり得るウェブサイトに対する定期的な脆弱性診断を実施しています。また、製品開発時における情報セキュリティルールに関する設計者教育も定期的に実施しています。