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、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、感染症・伝染病のパンデミックなどに備えて、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、経営環境の変化や急速なテクノロジーの進化、グローバルでの社会・経済などの変化により、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、今後ますます重要になっています。

ニコングループでは、事業部門を主とする第 1 線、管理部門を主とする第 2 線、内部監査部門を主とする第 3 線といったリスク管理における 3 つのディフェンスラインを強化するために人材や体制整備を進めます。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、グループガバナンスの強化、グローバルコンプライアンス体制を整備していきます。

代表取締役 兼 社長執行役員
CRO
徳成 旨亮

【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

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。

戦略

リスク

ニコンの事業環境は、地政学リスクや、インフレ抑制のための各国における政策金利上昇、そして円安といった外部環境の影響を大きく受けています。さらに、中長期的な観点では、被害が甚大化する気候変動などの事業環境の変化に伴うリスクにも適切に対応する必要があります。

ニコンは、経営上の重要リスクを、リスク管理委員会にて選定し、重要リスクについては、関連する部門での対応策や対応状況も踏まえて、リスクの軽減を進めています。

機会

社会情勢や環境の変化に対して、自社における経営上の重要リスクを的確に把握して、優先度をつけて対応することで、ステークホルダーとの双方向のコミュニケーションを積極的に図り、健全な関係の維持、発展に努めています。

戦略

年1回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「リスク把握調査」の結果に加えて、経営陣がみるリスク、調査アンケートから見えてこないリスクなども検討の上で、経営上の重要リスクを選定、対応状況等も鑑みた上で、対応策を講じることで適切なリスク管理を実施していきます。

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（2024年3月期P6～9）
https://www.jp.nikon.com/company/ir/ir_library/result/pdf/2024/24_4qf_c_j.pdf

ガバナンス

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。2023年度は、10月と3月の2回開催しました。

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。2024年度は、高リスクが懸念されるM&Aによりグループ化した子会社のグループガバナンスの強化、グローバルコンプライアンス体制の整備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、リスク管理委員会と連携し、「環境」「社会·労働」に関するリスクにも対応を図っています。

リスクマネジメントの体制としては、3線防衛（第1線：事業部門、第2線：管理部門、第3線：内部監査部門）によるリスクマネジメント体制を推進しています。第1線の事業部門は各種規程とレポートラインを整備し関連のグループ会社を含めた自律的なリスク統制の体制を構築しています。第2線の本社管理部門、海外の拠点統括機能は第1線のリスク統制、アセスメントなどを各々支援します。第3線の経営監査部は業務執行部門から独立した客観的な立場で監査を実施し、第1線、2線による内部統制が機能しているか評価、提言をします。

2023年度のリスク管理委員会の主な活動テーマ

- リスクマネジメントの強化
  （輸出管理体制の整備、BCMの見直し）
- 内部統制の強化
- 重点モニター対象会社の設定とモニタリング
- 係争案件調査結果報告
- 情報セキュリティ関連対応

● 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

リスク管理

ニコングループでは、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、年1回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ます。この調査結果に加えて、経営陣がみるリスク、アンケートから見えてこないリスクなども考察の上で、経営上の重要リスクを選定しています。

選定された重要リスクについては、関連する部門での対応策や対応状況も踏まえて、改善のためにリスク管理委員会の活動方針などに定めて、リスク管理体制の整備、リスクの軽減を進めています。

指標と目標

指標と目標（達成年度）

リスクアセスメントに基づく重要リスクの特定と施策実施の進捗度：100%（毎年度）

▶ **2023年度**

計画

1. 輸出管理体制の最適化支援
2. BCMの見直し

実績

1. 一部グループ会社において現地法令遵守に加え、外為法関連対応を行うなど輸出管理体制を構築
2. BCMとして事業部ごとに中核事業、目標復旧時間、重要業務などの前提条件を確定。基幹システムの洗い出し実施

▶ **2024年度**

計画

1. グループ会社における輸出管理体制の最適化支援
2. 大規模災害BCPおよび国際紛争有事BCMの実効性向上施策の実行（周知・訓練、継続的アップデート）

主な取り組み

リスク管理教育

事業部門やグループ各社が、効率的かつ健全な運営を実現するためのガイダンスとして『管理標準』を策定しました。事業運営にあたって目配りすべき40項目について、概要を示しています。

2023年度は、『管理標準』の発行にあたって全グループ会社の社長および管理部門長を対象とした説明会を開催し、活用方法を周知しました。2024年度も引き続き、新たにグループ会社社長に就任する者を対象として内部統制および『管理標準』の説明を行っていきます。

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。

2023年度は、台湾や朝鮮半島有事など、国際紛争の発生を想定した国際紛争有事の初動対応プランの作成や、

首都直下地震などの大規模災害を想定した主要事業部門のBCPの再点検･アップデートを行い、事業継続のための施策を進めました。

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」などの大規模地震に対する「大規模災害時の行動について」のeラーニングや、災害時を想定した安否確認や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

基本的な考え方

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

戦略

リスク

サイバー攻撃による企業活動の遅延や停止、さらに機密情報や個人情報の窃取、漏洩はニコングループの「信頼」に関するリスクであると認識しています。

機会

情報セキュリティ対策と適切な情報資産管理を実施することで、リスクの低減を図りつつ、ニコングループへの「信頼」の向上にも努めます。

戦略

中期経営計画に基づき、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ています。重点施策については、毎年リスクマップを関連部署と協議し、リソースの集中領域を決定しています。ゼロトラストで施策を進めており、EDRの見直しも行い、欧米含めた監視プラットフォームのグローバル統合を進めています。また、メールセキュリティの監視強化も行いました。

ガバナンス

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(情報セキュリティ推進部担当)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、ネットワークを利用した遠隔診断支援やクラウドによる病理画像の保存・管理サービスなどのデジタル化を軸とした情報サービス領域での事業拡大にともない、医療機関で厳格な管理が求められる被験者や患者の個人情報などの医療情報を取り扱うケースが増加することを踏まえ、2023年12月にISO 27001の取得対象組織を拡大するとともに、クラウドサービスのための情報セキュリティ管理における実践規範であるISO 27017の認証取得と運用を開始し、情報セキュリティマネジメントの徹底を推進しています。

* ISMS：Information Security Management System

リスク管理

世間動向、ニコングループの状況などを総合的に勘案し作成したリスクマップを関連部署と協議し、リソースの集中領域を決定しています。

指標と目標

指標と目標（達成年度）

リスクアセスメントに基づく重要リスクの特定と施策実施の進捗度：100%（毎年度）

▶ 2023年度

計画

適用を受ける各国個人情報保護法令への対応継続

実績

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

▶ 2024年度

計画

サイバーセキュリティの体制強化、製品のサイバーセキュリティ対策を求める各国法令への対応実施

主な取り組み

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。

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。

2023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、メール訓練を実施し、不審メールへの対応の習熟度向上を図りました。

定期入社社員向けには、講師による研修を実施し、キャリア入社社員向けには、eラーニングを実施しています。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、個人情報などの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。

2023年度は、国内ニコングループの全部門に対する書面監査（個人情報の管理等）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

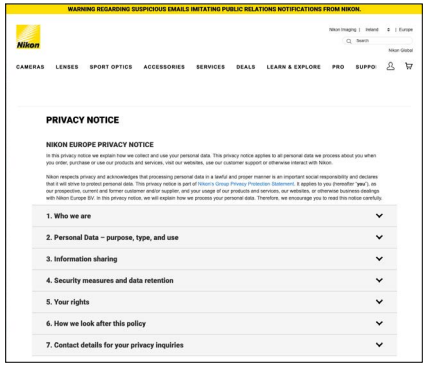
ニコングループでは、プライバシーの尊重、個人情報の適法・適切な取り扱いは重要な社会的責務であると捉え「ニコングループ個人情報保護方針」を定めています。この方針のもと、グループ共通の規程として「ニコングループ個人情報取扱規程」を定め、グループ内に周知するとともに、情報管理体制のもと、この規程に則って個人情報を取り扱っています。

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。

2023年度は、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および下位規則に基づきプライバシーポリシーの修正を実施しました。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。

2024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を展開し、運用しています。

この他、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実施しています。