

マテリアリティ12

リスクマネジメントの強化

ニコングループでは、企業価値を毀損する重要なリスクを特定し、ニコンおよびグループ会社の持続的発展を実現するための積極的なリスクティクと、不正や事故などを未然防止するための適切な対応を図るため、攻めと守りの両方の視点でリスクマネジメントを実施しています。

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
- 内部統制システムの基本方針

体制

- リスク・コンプライアンス委員会
- 輸出審査委員会

● 指標と目標

自己評価：○達成、△一部未達成、計画変更

指標	目標（達成年度）	2024年度計画（アクションプラン）	2024年度実績	自己評価	2025年度計画（アクションプラン）
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）	- グループ会社における輸出管理体制の最適化支援 - 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）	- M&Aで新たにグループ会社となった海外企業の輸出管理と役務提供管理の体制整備や、統括する事業部との連携強化などを実施 2025年1月に大規模災害時の「初動対応訓練」を実施。ITソリューション本部、生産本部（生産グループ会社）とBCM連携に向けた協議を開始	○	- リスクアセスメントのフレームワーク再設計と実行 - 重要リスクの特定と対応方針の検討
		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	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を実施	○	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継続

リスクマネジメント

基本的な考え方

リスクマネジメントでは、地政学リスクの増大やデジタル変革、気候変動などの外部要因だけでなく、中期経営計画の未達といった内部要因も対象としています。多様化するリスクを調査・分析し、影響を予測することで、リスクの回避や低減、適切なリスクテイクを図り、企業としての持続的な成長につなげます。

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、関税の引き上げ、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、市場の大きな変化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。

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が予想されます。

機会

リスクマネジメントは、不正や事故の未然防止などが発生した場合の影響を最低限にとどめるだけでなく、経営戦略を実現するためのリスクテイクの側面も持ち合わせています。

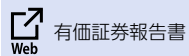
社会情勢や環境の変化に対して、自社における経営上の重要リスクを的確に把握し、優先度を付けて対応することは、経営戦略に沿った事業展開を促し、将来的な利益確保や企業の持続的成長につながります。

戦略

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、社内が考えるリスク、社外が考えるリスクを調査し、経営上の重要リスクを特定した上で、各部門・各社の目標や施策に展開しています。

関連情報

有価証券報告書では、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。



ガバナンス

リスク管理委員会

ニコングループでは、経営に重大な影響をおよ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。本委員会は社長執行役員であるCRO(Chief Risk Officer)を委員長、経営委員会メンバーなどを委員、経営管理部を事務局として年2回開催し、重点対象のリスク

についてモニタリングや、機動的な支援を可能にする体制の構築を図っています。

2025年4月以降は、リスク管理委員会と傘下のコンプライアンス委員会を統合し、「リスク・コンプライアンス委員会」に改称し、コンプライアンスリスクも全社リスク管理の一環として審議していきます。

● 2024年度のリスク管理委員会での主な議題

2024年10月	● 経営委員会重要案件のリスクアセスメント
2025年3月	● 経営委員会重要案件のリスクアセスメント ● 全社リスクマネジメント強化のためのリスク管理委員会・コンプライアンス委員会の統合(2025年4月1日リスク・コンプライアンス委員会として発足) ● 危機発生時の対応強化のため、エスカレーションフローの再整備

リスクマネジメント体制

ニコングループでは、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線で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線では第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線で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、第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。

関連委員会との連携

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、傘下の委

員会およびサステナビリティ委員会をはじめとした委員会、部会と連携を図り、対応を図っています。

● リスク管理に関わる主な専門委員会(2025年4月～)

委員会	主な取り扱いリスク
リスク・コンプライアンス委員会	リスク全般、コンプライアンス全般
品質委員会	品質全般
輸出審査委員会 ^{*1}	外為法違反防止、安全保障リスクの管理
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

^{*1} リスク・コンプライアンス委員会の傘下委員会。

リスク管理

ニコングループでは、当社グループが抱えるリスクを把握するため、リスクアセスメントとして「リスク把握調査」を毎年実施しています。この調査は、当社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、全社的な重要リスクの洗い出しや分析・評価を行い、対応状況をモニタリングしています。調査結果をもとに、回答数や影響が大きいリスクを分析し、かつ社外のリスク認識も加味した「リスク相関図」を作成することで、重要リスクを特定し、取り組みを強化すべき課題の判断をリスク・コンプライアンス委員会にて行っています。

専門的な対応が必要なリスクについては、サステナビリティ委員会、品質委員会、リスク・コンプライアンス委員会

傘下の輸出審査委員会からの情報をもとに、リスク・コンプライアンス委員会が経営の視点から、特に優先して取り組むべきリスク(最優先リスク)を特定し、対応を指示するとともに、その進捗を管理しています。取締役会は、これらの報告を受け、ニコングループ全体のリスクとその管理状況を監督しています。さらに、経営監査部による内部監査においても、リスク管理の妥当性について確認しています。

今後、特定した重要リスクに対する対応を次期中期経営計画に盛り込むとともに、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・コンプライアンス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。

主な取り組み

リスク管理教育

リスクに対する認識、啓発活動のため、ニコングループでは年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対して「リスク把握調査」を実施しています。

また、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作成している「管理標準」を最新の状況に合わせ更新しました。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、2024年度の重点対応項目を各部門で設定した上で、改善策を実施します。

BCM^{*2}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^{*3}を策定し、見直しています。

2024年度は、1月に大規模災害時の「初動対応訓練」を実施し、BCM上の課題を確認、施策に反映しました。

BCPの継続的最適化と、国際紛争有事の初動対応プランのアップデートを引き続き進めていきます。

^{*2} 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。

^{*3} 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。

輸出管理への取り組み

ニコングループでは、国際的な平和および安全の維持を目的として、安全保障貿易管理(輸出管理)に取り組んでいます。経済安全保障や地政学リスクなどを背景に強化される各国の輸出規制に適切に対応するため、2024年度は、グループ会社における輸出管理体制の最適化支援への取り組みを進めました。具体的には、M&Aで新たにグループ会社となった海外企業の輸出管理と役務提供管理の体制整備や、統括する事業部との連携強化などを行い、輸出管理におけるグループガバナンスの強化を図りました。

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。



ニコングループ情報セキュリティ基本方針

戦略

リスク

サイバー攻撃によりシステムの破壊などの被害を被った場合、企業活動の遅延や停止が発生し、売上の低下など財務影響が発生するリスクがあります。また、機密情報や個人情報の窃取・漏えいは、情報管理が不十分であるとの評価につながり、企業として信用を失墜し、損害賠償請求を受けるリスクもあります。

機会

情報セキュリティ対策と情報資産管理を適切に行うことで、サイバー攻撃のリスクの低減が可能になります。これ

により、情報の可用性が高くなるとともに、事業の継続性に貢献することが可能となり、ニコングループへの信頼性向上につながります。

戦略

情報セキュリティ対策と情報資産管理を行い、事業の継続性やニコングループの信頼性の向上に寄与するべく、短期から中長期にかけて以下の活動を進めていきます。

2025年度は、サイバーセキュリティの体制強化や、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などを実施します。

現中期経営計画の達成に向けては、サイバーセキュリティ強化、IT・セキュリティグローバル体制とガバナンス確立を進めます。

そして、2030年のありたい姿の実現に向けては、環境変化と経営戦略に即した全社的リスクマネジメント体制の確立をめざします。

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、社長執行役員のもと、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、情報セキュリティ会議と、経営委員会メンバーなどで構成されるリスク・コンプライアンス委員会(2025年4月改称)にて報告されます。その後、情報セキュリティ推進部が戦略・方針に落とし込み、情報セキュリティ会議とリスク管理委員会に報告します。これらの戦略・方針の目標を情報セキュリティ推進部で定量化し、実績の管理をしています。

* ISMS:Information Security Management System

ヘルスケア事業部での取り組み

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伴い、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。

リスク管理

ニコングループでは、リスクの発生頻度や影響度を考慮したセキュリティリスクマップを作成し、リスクに対して施策を立案・実施します。そして情報セキュリティ会議で施策の有効性評価を行い、来年度の施策に反映しています。

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。

2024年度は、インシデントプロセスに関する文書の改定を行うとともに、インシデント対応の訓練を実施しました。

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。

2024年度は、情報セキュリティ教育プラットフォームの導入を進め、ニコンおよび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。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。

2025年度から、情報セキュリティ教育プラットフォームの海外グループ会社への導入・展開を進めます。

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。

2024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。2025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・コンプライアンス委員会」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。

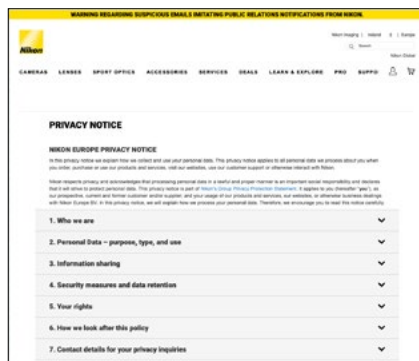
また、調達パートナーに対して、個人情報の保護を含めた情報セキュリティを遵守するよう「ニコンCSR調達基準」に定め、要求しています。



ニコングループ個人情報保護方針

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

ニコンCSR調達基準



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

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ールに関する設計者教育も実施しています。

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・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。

2025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・改正動向に合わせ、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