情報セキュリティとサイバーセキュリティ

基本的な考え方

ニコングループは、保有する情報資産の保護を企業活動の基盤と位置付け、「ニコングループ情報セキュリティ基本方針」を実践しています。本方針に基づく複数の社内規程を整備し、各国・地域の法令や規制に対応した情報管理を推進しています。これら規程類を社内ポータルサイトで常時公開し、定期教育や遵守状況の確認を通じて、運用レベルの維持・改善を図っています。

Web ▶ 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

ニコングループでは、事業の継続性と社会からの信頼性向上に向け、情報セキュリティ対策と情報資産管理を計画的に推進しています。短期から中期にかけては、ゼロトラスト思考に基づくガバナンスとサイバーレジリエンスの向上を図るとともに、AI活用に伴うリスク対応やグローバルなセキュリティ体制の高度化を進めます。長期においては、先制的なリスク管理とセキュリティ文化の定着を全社で推進し、持続的な企業価値向上を支える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、リスクの発生頻度と影響度を評価したセキュリティリスクマップを作成し、優先度に応じた対策を計画・実施しています。これらの対策は情報セキュリティ会議で有効性を評価し、評価結果を来年度以降の施策に反映することで、リスクマネジメントプロセスの強化と継続的改善を実現しています。こうした取り組みにより、グループ全体でリスクを体系的に把握し、組織横断でセキュリティ統制の向上を図っています。

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、情報セキュリティインシデントを「ニコングループ情報管理規程」で明確に定義し、事案発生時には発生部門から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、関係部門と連携し、初動対応から封じ込め、影響調査、復旧までの手順を統一し、被害や影響の最小化と事業の迅速な再開を図っています。重大事案については、担当役員（CISO）へ迅速にエスカレーションし、組織的な判断と対応を行っています。

また、2025年度は、関係部門とのインシデント対応訓練を実施し、対応手順や連絡体制の有効性を確認しました。

なお、過去3年間において、罰金や補償金の支払いを伴う重大な情報セキュリティ事故は発生していません。

情報セキュリティ教育

ニコングループでは、従業員の情報セキュリティ意識の向上と適切な情報管理を実践する能力の強化、入社時研修および定期的なeラーニングによる情報セキュリティ教育を実施しています。教育プログラムでは、情報管理に関する方針やルールに加え、実際の事例を基にしたリスク認識や対応方法を学べる内容としています。

また、社内規程や最新の施策を分かりやすくまとめた教育資料「ニコングループ情報セキュリティハンドブック」を社内ポータルサイトに掲載し、従業員がいつでも参照できる環境を整備しています。これにより、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啓発に取り組んでいます。

2024年度に国内のニコングループに導入した情報セキュリティ教育プラットフォームを、2025年度には海外グループ会社へ順次展開し、グローバルでのeラーニングの定期実施を開始しました。

情報セキュリティ監査

ニコングループでは、情報セキュリティ対策の適切な実施を確認するため、「ニコングループ情報管理規程」に基づく内部監査を定期的に実施しています。

2025年度は、国内の全グループ会社・部門を対象とした書面監査と、重要テーマに基づく選定部門への実地監査を実施し、重大な不適合はないことを確認しました。

2026年度も引き続き重点テーマを設定した監査を行い、対策の運用状況を検証することで、グループ全体での継続的な改善に努めます。

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。「ニコングループ個人情報取扱規程」の遵守状況については、年1回程度、質問票による調査を実施しています。

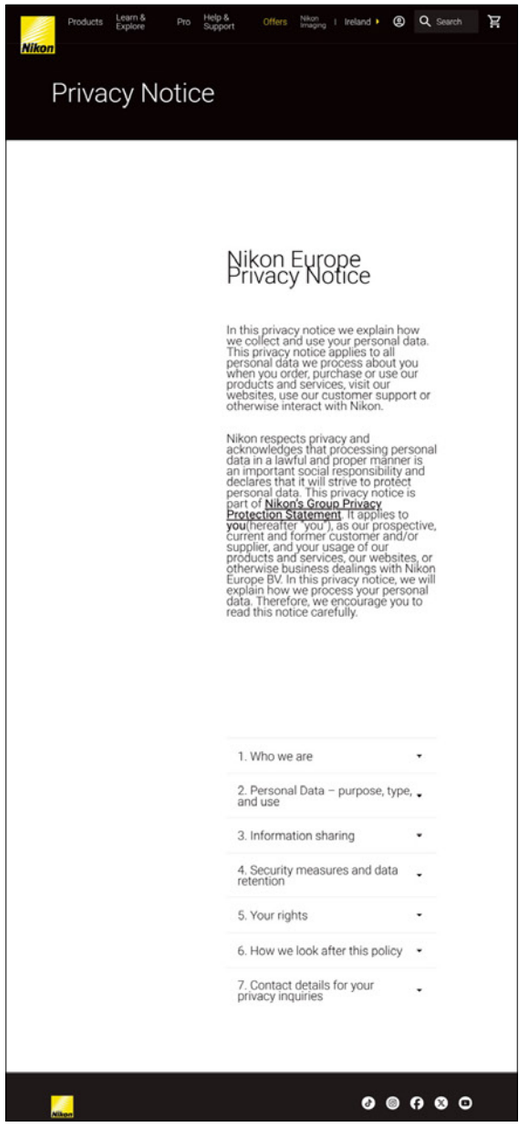
さらに、コンプライアンス部が個人情報領域を所管し、ニコングループ全体のプライバシーや個人情報に関するリスク管理を行っています。

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
- 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

CONTENTS



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・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。

2026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

事業への影響を最小化するサイバーレジリエンス向上のために、ニコングループでは包括的なセキュリティ体制を構築しています。インフラ保護では境界防御と「ゼロトラスト思考」の併用により高度なガバナンスを推進しています。また、外部表面脅威管理として全拠点の公開資産を可視化し、クラウド環境の設定不備も継続的に監視・是正することで情報漏えいの未然防止を図っています。

さらに、製品・サービスでも「セキュリティ・バイ・デザイン」を徹底し、開発初期から安全性を担保するプロセスを強化しています。