情報セキュリティマネジメント

より詳しい情報は、こちらをご覧ください。

基本的な考え方

デジタル技術の活用範囲は様々な分野に及び、情報・データの量が劇的に増加するとともに、その保持・利用の形態は多様化し続けています。そのような事業環境では、情報が不適切に取り扱われてしまうリスクに加え、サイバー攻撃の巧妙化を背景とした情報の漏えいや、サプライチェーンに悪影響を及ぼすリスクが高まっています。NSKグループでは、情報セキュリティマネジメントを重要な経営課題の一つと位置づけ、情報セキュリティ基本方針[※1]を定めるとともに、関連する法規制への対応強化を含む各種リスク低減に取り組んでいます。また、高度化するサイバー攻撃に対し、ネットワーク対策をはじめとする、より強固な仕組みや組織体制の強化に向けた取り組みも推進しています。

※1 NSKグループ 情報セキュリティ基本方針 https://www.nsk.com/jp-ja/information-security/

情報セキュリティ体制

NSKグループではデジタルの力で経営資源を強化し、事業変革に取り組んでいます。デジタル技術の安全な活用を可能とし、デジタル技術とサイバーセキュリティの関連性を考慮した情報セキュリティ強化施策をグローバルに展開していくため、グループ本社である日本精工株式会社デジタル変革本部の下に情報セキュリティ統括部門(ITガバナンス部情報セキュリティ推進グループ)を設置しています。また、情報セキュリティに関するリスクはコーポレートリスク管理体制の下で監督され、取締役会においてもグループ全体の課題の一つとして、情報セキュリティについて討議しています。情報セキュリティ統括部門は、グローバル会議を定期的に開催し、日本、米州、欧州、中国、アセアン・オセアニア、インド、韓国の各地域に設置された情報セキュリティ委員会と強力に連携しながら、NSKグループ全体の情報セキュリティ管理レベルの向上、セキュリティ施策の企画・実行に取り組んでいます。

さらに、サイバー攻撃に対する迅速かつ適切な対応を組織的に行い、被害拡大防止と迅速な復旧を図るための対応体制としてCSIRT[※2]体制を構築し、外部団体である一般社団法人日本シーサート協議会に加盟しています。

※2 Computer Security Incident Response Teamの略で、コンピューターセキュリティに関するインシデントに対処するための組織の総称

情報セキュリティマネジメント強化への取り組み

サイバーセキュリティに関する専門的な団体が策定している、世界的に採用されているガイドライン・フレームワークを活用し、「人・組織」「プロセス」「技術」の3つの観点でバランス良く態勢を構築するとともに、サイバーレジリエンスの考え方を取り入れ、その強化に取り組んでいます。

平時における対策の強化

リスクの把握と評価、迅速な検知と対応によりリスクを低減するため、外部セキュリティ評価サービス等を利用して脆弱性を含めた監視と対策の強化に取り組んでいます。また、情報機器やネットワーク通信などにおける不審な動きや、セキュリティの脅威を把握する技術的施策の推進、検知したインシデント情報を分析し対策を講じるセキュリティオペレーションセンター[※3]による対応など、迅速なインシデント対応を可能にする仕組みを構築しています。また、パソコンを利用する全従業員を対象にした標的型攻撃メール訓練を国内外のグループ会社のシステム管理部門と連携して実施しています。さらに、国内外の従業員を対象とした定期的なeラーニング、役員やシステム管理部門メンバーなどの従業員カテゴリー別研修や入社・海外赴任時などの研修、啓発情報の発信等により、従業員の情報セキュリティに対する意識の維持・向上に取り組んでいます。

※3 サイバー攻撃の検知や分析を行い、対策を講じる専門組織

インシデント対応力の向上

有事におけるインシデント対応力の向上のため、内閣サイバーセキュリティセンターと日本シーサート協議会が連携して開催している、「NISC/NCA連携分野横断的演習」に毎年参加しており、FY2023も演習に参加しました。近年のサプライチェーンへの攻撃を受けるリスクの高まりへの対応として、制御機器のリスク評価と管理、工場におけるインシデント対応訓練の実施など、工場セキュリティ態勢を強化するとともに、取引先への情報セキュリティ点検の実施や、対応水準の向上に向けて取り組んでいます。

また、情報セキュリティ管理システムを活用することで国内外からのセキュリティインシデントに関する情報や報告を適切に分析・管理し、インシデント対応に関する手順や要領を維持・向上し、ナレッジとして活用することを推進しています。