04 サステナビリティ
情報セキュリティ

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、関連する法規制への対応の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。

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も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、デジタル変革本部の下に情報セキュリティ推進室を設置しています。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。情報セキュリティ推進室は、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。

規程類の管理・運用

NSKでは情報セキュリティ基本方針を定めるとともに規程類を整備し、法規制等の新たな施行・改訂や環境変化に応じて見直しや拡充を行っています。また、その周知・教育・啓発および浸透状況の定期的なチェックを通じて、情報セキュリティに関するルールやリスク対策の組織内への徹底を図っています。

■ 主な情報セキュリティ関連規程類

NSKグループ 情報セキュリティ基本方針	NSKグループの情報セキュリティの目指すべき姿（情報セキュリティの取り組み、情報資産の取り扱い、法令・規則・契約への対応、教育、継続的改善）を定めるもの。
NSKグループ 情報セキュリティ管理基準	NSKグループにおける情報セキュリティの最上位規程。情報セキュリティ管理レベルを統一し、向上させるための原則を定めるもの。
NSKグループ 情報セキュリティ管理規定	NSKグループで統一して遵守すべき情報資産の取り扱い方法など、情報資産を守るための対応を定めるもの。

情報セキュリティの取り組み

NSKでは、情報セキュリティマネジメントシステムとして定期的に情報資産の棚卸とリスク評価を実施し、リスク課題があればその対応計画の策定と改善を実行するといったPDCAサイクルを確立し、その結果として国際規格であるISO/IEC27001認証を取得・維持しています。さらに、ドイツの自動車業界において広く採用されるセキュリティ認証であるTISAXについては、顧客の要請に基づき、欧州、中国、日本の計9拠点において認証を取得しています。

サイバー攻撃に対する取り組みとして、インシデント対応における事前準備と検知に基づく迅速な対応によりリスクを低減し、被害発生時の影響を最小化するためのセキュリティインシデント対応態勢を整備しています。また、インシデントレベルの定義と対応手順を定め、インシデントの発生を想定した訓練、およびパソコンを利用する全社員を対象にした標的型攻撃メール訓練を各地域のシステム管理部門と連携して実施しています。さらに、外部専門業者による、インターネット公開システムおよび社内重要システム等に対するセキュリティ評価を実施しています。加えて、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、工場のセキュリティ体制を強化するとともに、お取引先への情報セキュリティ点検を実施しています。

教育・啓発として、日本および海外地域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や入社・海外赴任時などの研修、定期的な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。

より詳しい情報は、こちらをご覧ください。