

セキュリティ強化に向けた具体的な取り組み

プロダクトセキュリティ

リコーグループの「製品・サービス」は、セキュリティを企画・設計段階から確保するセキュリティ・バイ・デザインの実践を国際標準ISO/IEC^{*1} 27034-1に基づき取り組んでいます。脆弱性対策については、国際基準ISO/IEC^{*1} 29147/30111に基づき脆弱性への早期対応を図り、サイバー攻撃リスクに対する注意喚起、脆弱性報告の受付窓口の設置、脆弱性対策情報を提供しています。さらには、各国で強化が進んでいる法規制対応を進めています。

*1 ISO/IEC (International Organization for Standardization/International Electrotechnical Commission):国際標準化機構/国際電気標準会議

コーポレートセキュリティ

リコーグループはサイバーセキュリティ対策をグローバルで推進しています。2013年度よりRICOH-CSIRT (Computer Security Incident Response Team)を組織し、SOC (Security Operation Center)からのインシデント報告、社外CSIRT組織からの情報、セキュリティ情報サイトからの情報をもとに脅威を分析し、迅速かつ最適な対応を主導しています。リコーグループの保有するITシステムを常時監視することで、外部からの不正侵入、内部からの不正利用をいち早く検知し、インシデントの早期対応を実現しています。

ファクトリーセキュリティ

工場ネットワークOT(Operational Technology)を対象とするセキュリティ強化を推進しています。リコーグループでは、各工場が活動の主体となり、セルフアセスメントや第三者アセスメントによる状況把握、課題に対する対策強化活動を実施するとともに、組織によるガバナンスを強化する取り組みを継続的に実施しています。

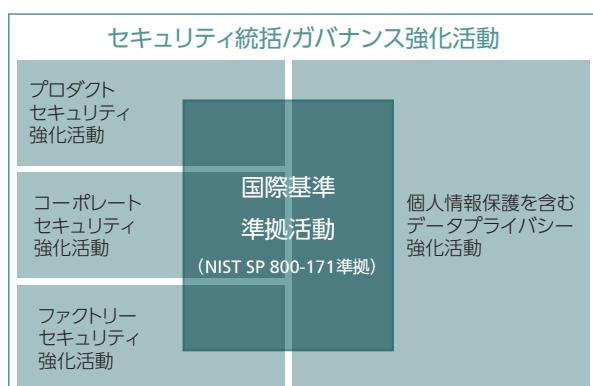
データプライバシーポリシー

デジタル化の進展やビッグデータの利活用の広がりを背景に、データプライバシーや個人情報を含むパーソナルデータの保護への関心が高まっています。リコーグループは、個人情報保護法等の法令に則り、お客様のパーソ

ナルデータ全般に対してデータプライバシーポリシーを定義して情報管理に取り組んでいます。さらに、データビジネス事業を本格始動させ、AI活用による新たな価値を創出し、お客様の成長と課題の解決に貢献していきます。

国際的なセキュリティ基準準拠に向けて

サイバー攻撃の増加と高度化に伴い、その標的は業種を問わず、無差別かつあらゆる産業に拡大しています。リコーグループでは、お客様の情報資産を守ることを第一に配慮したセキュリティ活動を行い、国際的な基準・ガイドラインである、NIST^{*2} SP 800-171への準拠を目指します。この活動は「コーポレート」「プロダクト」「ファクトリー」「データプライバシー」を包括したセキュリティ強化の一環です。リコーグループの「製品・サービス」は、セキュアな「事業環境」やNIST^{*2} SP 800-171に準拠した「事業環境」を目指しているお客様を想定し、NIST^{*2} SP 800-171に必要な機能を搭載した製品を提供していきます。また、リコーグループの「事業環境」においても、お客様の守るべき情報資産を厳格に管理し、保護するため、NIST^{*2} SP 800-171に準拠した施策を継続的に行っていきます。これらセキュリティ強化への取り組みは、リコーグループの「製品・サービス」の導入を検討されるお客様のセキュリティニーズに対応し、情報資産を守ることに貢献し、お客様のビジネスリスクを低減します。



*2 NIST (National Institute of Standards and Technology):米国国立標準技術研究所