情報セキュリティ

基本的な考え方

OKIグループは、事業の成長を支えるIT基盤の整備を進める中で、経営リスクの最小化という観点から、以下の方針に則り情報セキュリティの強化に取り組んでいます。

詳細は、以下Webサイトをご参照ください。
情報セキュリティ基本方針 https://www.oki.com/jp/sustainability/governance/security/policy/index.html
OKIグループ個人情報保護ポリシー https://www.oki.com/jp/privacy/

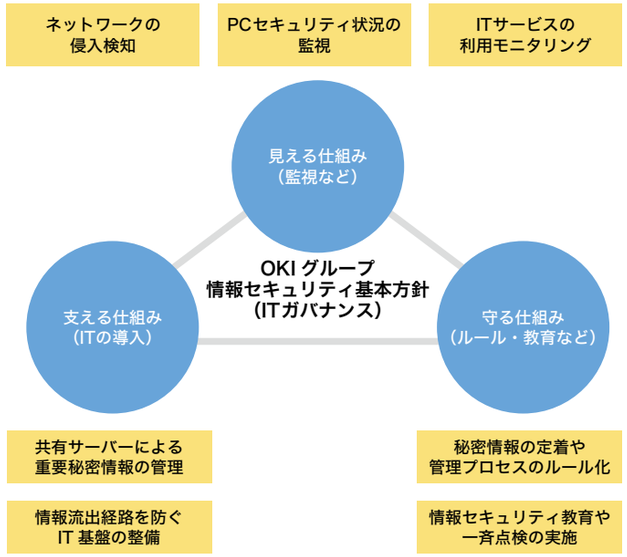
情報セキュリティの取り組み

OKIグループは、事業の成長を支えるIT基盤の整備を進めています。この中で、経営リスクの最小化という観点から取り組んでいるのが情報セキュリティの強化です。リスク管理委員会の定める共通リスクとして「電子情報漏洩」と「サイバー攻撃」を定義し、情報セキュリティ対策が経営として重要な位置づけであることを明示して取り組みを進めています。

情報セキュリティ基本方針に基づき、関連規程や業務ルールの整備を進め、お客様からお預かりしたデータや社内加工データの秘密情報を定義したうえで、それらの取得・作成から廃棄に至る業務プロセスにあわせて規程類や実施細則、ガイドラインを整備しています。

また、グループ横断的に管理する共通リスクとして「電子情報漏洩」と「サイバー攻撃」を定義し、情報セキュリティ基本方針に則り、「見える・支える・守る」施策を幅広く推進するとともに、セキュリティ事故対応専門組織OKI-CSIRT※を設置し、 ISMS（ISO 27001）の仕組みを活用し予防と事故発生時の対応力強化に取り組んでいます。

OKIグループは、システム構築や関連サービス提供における信頼性を高めるため、社内情報システム構築・運用部門やシステム設計・開発部門などで情報セキュリティマネジメントシステム（ISMS）の認証を取得しています。国内グループにおいて、継続してISMS認証の拡大に取り組んでいます。2024年度は



※CSIRT：Computer Security Incident Response Team

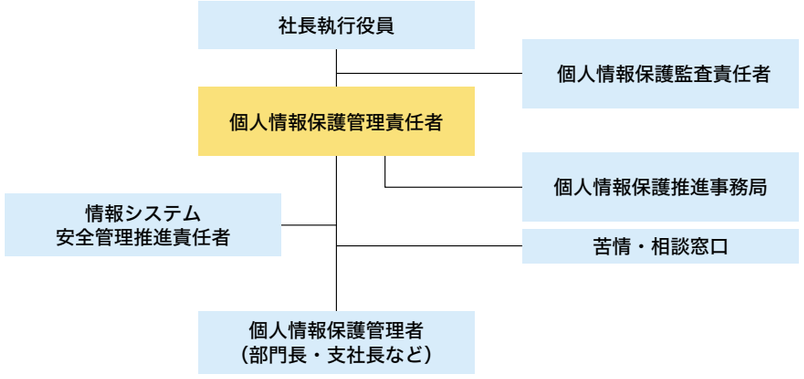
OKIグループにおけるクラウド利用ルールの見直しを行い、より厳格化を図ることで情報セキュリティのさらなる強化に努めました。また、技術的な対策として、社内のセキュリティ監視機能の高度化を行うことで不正アクセス対策の強化を実施しています。

個人情報保護の取り組み

OKIグループは、「個人情報保護ポリシー」に基づき、個人情報保護を徹底しています。また、欧州、アジアなど海外事業地域の個人情報保護関連法規についても規則に則した対応を行っています。なお、グループ各社のWebサイトには、適用される地域や国のプライバシー保護法制やCookie規制に照らしたCookieバナーを導入しています。

2025年6月現在、OKIグループの8社がプライバシーマーク付与認定を受けており、JISQ15001「個人情報保護マネジメントシステム（PMS）－要求事項」に適合した個人情報について適切な保護措置を講じています。プライバシーマーク付与会社では、毎年、各部門の個人情報管理台帳および委託先企業一覧の見直しと委託先企業の評価を行っています。また、各部門においてはPMSの内部監査が実施され、PMSの維持、改善に努めています。この活動は、プライバシーマーク審査機関によるPMSの状況などについての現地審査を2年ごとに受けており、適正であると評価されています。

個人情報保護体制



詳細は、以下Webサイトをご参照ください。
https://www.oki.com/jp/sustainability/governance/security/index.html