情報セキュリティ

基本的な考え方

OKIグループはOKIグループ企業行動憲章・行動規範のもと、情報セキュリティ体制を整備し、お客様および自社の情報の適正管理・保護に努めています。

詳細は、以下Webサイトをご参照ください。
OKIグループ企業行動憲章・行動規範 *https://www.oki.com/global/ja/sustainability/mng/code/*
OKIグループ個人情報保護ポリシー *https://www.oki.com/global/ja/privacy/*

情報セキュリティの取り組み

OKIグループは、事業成長を支えるIT基盤整備の一環として、情報セキュリティの強化を重要な経営課題と位置づけています。リスク・コンプライアンス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。

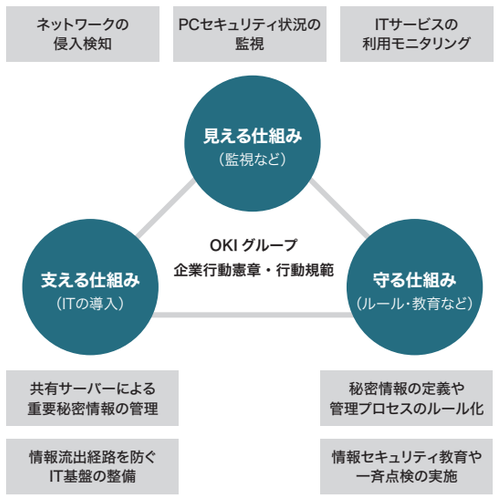
OKIグループ企業行動憲章およびOKIグループ行動規範に基づき、関連規程や業務ルールの整備を進め、お客様からお預かりしたデータや社内加工データの秘密情報を定義したうえで、それらの取得・作成から廃棄に至る業務プロセスにあわせて規程類や実施細則、ガイドラインを整備しています。

また、上記の取り組みのもと、情報セキュリティの運用として「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。

2025年度は、変化するクラウド利用環境や情報セキュリティリスクへの対応力向上を目的として、OKIグループの利用申請制度および運用ルールの継続的な改善を推進し、ガバナンス強化とリスク低減に取り組みました。また、情報セキュリティ対策の強化を通じて、安全かつ適正な利用環境の維持・向上に努めました。

情報セキュリティの3つの仕組み



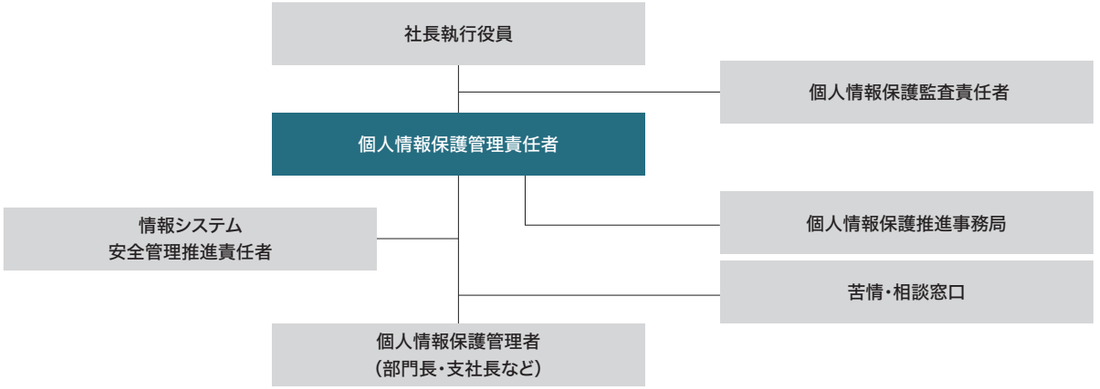
※CSIRT：Computer Security Incident Response Team

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。

2026年6月現在、OKIグループの8社がプライバシーマークを取得しています。認定会社では、プライバシーマーク審査機関によるPMSの運用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（2026年度）



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