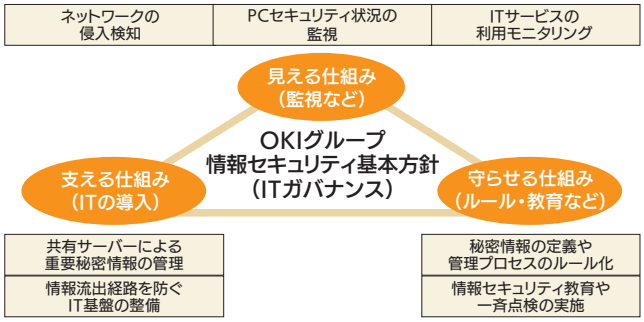
情報セキュリティ

OKIグループは情報セキュリティ基本方針のもと、推進組織である情報セキュリティ委員会を中心とした情報セキュリティ体制を整備しています。活動内容のレビュー（年2回）、情報セキュリティに関わるモニタリングなどを行い、個人情報をはじめとする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。

情報セキュリティの3つの仕組み

OKIグループは下図に示す3つの仕組みを基盤として、PC、ネットワーク、情報システムなどにおける情報セキュリティ対策を幅広く推進しています。



2014年度は、特に内部不正による情報漏洩対策を強化するため、お客様やお取引先の情報を扱うデータベースの管理体制を見直し、個人情報を扱うデータベースについても監視を強化したほか、オンラインストレージサービスの利用制限、およびフリーメール宛てのメール送信制限を実施しました。

OKI-CSIRTによるセキュリティ事故対応力の強化

OKIはセキュリティ事故対応専門組織としてOKI-CSIRT※1（オキ・シーサート）を設置し、日本シーサート協議会や他社CSIRT、関係省庁などの社外組織とも連携して、グループとしてのコンピュータセキュリティ事故予防、事故発生時の対応力強化に取り組んでいます。2014年度は、前年度に続いて標的型メール※2によるサイバー攻撃への対応を強化し、官公庁の職員に成りすましたメールへの対策などを実施しました。

※1　CSIRT：Computer Security Incident Response Team
※2　標的型メール：情報窃取などを目的として、特定の組織や個人に送られる電子メール。

海外拠点における施策の強化

OKIグループは、2008年度より、中国拠点を皮切りに、海外拠点における情報セキュリティ施策を推進しており、2013年度からはアジア/オセアニア地区における施策強化の一環として、情報セキュリティガイドラインの制定やセキュリティ管理者の任命などを実施しています。2014年度はセキュリティ管理ツールの導入により、同地区において社員が使用するPCのセキュリティ状況把握と、これに基づく即時の対応指示を可能としました。

お取引先と課題を共有し改善

OKIは、サプライチェーン全体での情報セキュリティレベル向上をめざし、重要秘密情報を提示しているお取引先を対象に、情報セキュリティ施策への取り組み状況確認を継続的に行っています。これは、OKIが作成したチェックリストに基づいてお取引先が実施したセルフチェックの結果を独自に点数化するもので、OKIとお取引先が課題を共有し、問題点の改善を図っています。2014年度は当社基準における「低評価」のお取引先について課題共有と改善を実施した結果、対象としたすべてのお取引先において「高評価」を達成しました。

ISMS認証の取得

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5社7部門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（2015年6月現在）。2014年度は各取得部門で前年度の規格改訂への対応を進め、2015年度に審査を予定する2部門を除く5部門で新規格への移行を完了しました。

※ ISMS：Information Security Management System

個人情報保護の徹底

OKIグループは、「個人情報保護ポリシー」に基づき、個人情報保護管理責任者のもと、各部門およびグループ企業に個人情報保護管理者をおいて、個人情報保護を徹底しています。適切な保護措置を講ずるため、グループ各社においてプライバシーマークの付与認定取得を推進しており、2015年6月現在、OKIおよびグループの7社がプライバシーマーク付与認定を受けています。

TOPICS　ソーシャルメディアの利用指針を徹底

OKIは、ソーシャルメディアの私的利用に起因する情報漏洩などを未然に防止するため、「OKIグループソーシャルメディア利用ガイド」を策定しました。2014年11月に同ガイドを含む「ソーシャルメディア利用指針」サイトをイントラネットに開設し、社員への周知徹底を図っています。