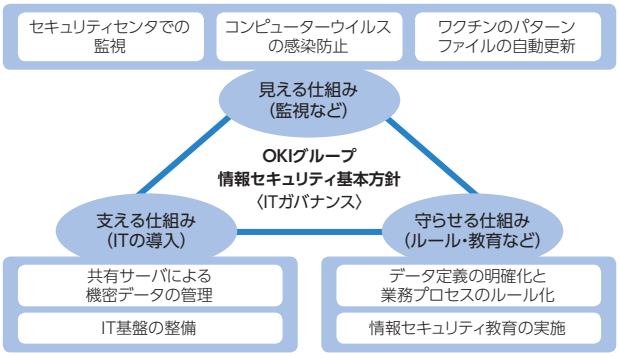
情報セキュリティ

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グループは情報セキュリティに配慮した商品・サービスを提供する企業として、自らの情報セキュリティレベルを高めるため、下図に示す3つの仕組みでセキュリティ対策を推進しています。

2012年度は、「見える仕組み」としてサイバー攻撃などへの監視を強化したことに加え、「支える仕組み」として、OKIのスマートフォン向けクラウドサービス「EXaaS Mobile Deskサービス」を導入し、スマートフォンから社内情報を安全・簡単に閲覧できる環境を整備しました。また「守らせる仕組み」として、グループ各社・各部門における新任の情報セキュリティ施策展開推進責任者／推進者を対象とした集合教育を実施したほか、毎年10月に全従業者を対象に実施している「情報セキュリティ一斉点検」の点検項目を見直し、お客様からお預かりした情報やトレードシークレット、個人情報などの保護についても注意を喚起して、情報管理全般に関する意識向上を図りました。



お取引先における情報セキュリティレベルの向上

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2008年度から継続的に実施しています。これは、OKIが作成したチェックリストに基づいたセルフチェックを実施していただき、回答結果を当社独自に点数化することで、取り組み状況や課題の共有化を図るものです。

2012年度は、これまでの調査において相対的に評価の低かったお取引先について重点的に再チェックを行いました。セルフチェック結果に基づいてOKIとお取引先が課題を共有し、問題点の改善を図った結果、対象の半数において当社基準における「高評価」を達成することができました。

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(NCA)および他社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。

2012年度は、標的型メール※2など増加するサイバー攻撃への対応について、これまで国内で取り組んできた対策を中国のグループ拠点にも展開し、侵入検知の徹底とともに、ウイルスに感染したPCやサーバーからの情報流出経路をブロックする出口対策の強化を図りました。

※1 CSIRT: Computer Security Incident Response Team
※2 標的型メール：サイバー攻撃の一種。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。

ISMS認証の取得を推進

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※)の認証取得に取り組んでいます。2013年6月現在、OKIグループの5社7部門がISMS認証を取得しています。

※ ISMS：Information Security Management System

個人情報保護の徹底

OKIグループは、2004年に制定した「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、コーポレート・営業部門・事業部門・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、2013年6月現在、OKIおよびグループの8社がプライバシーマーク付与認定を受けています。