「ネットワークソリューションのOKI」にふさわしい情報セキュリティ体制を整備、継続的に強化

CIO兼 常務取締役
（情報セキュリティ委員会 委員長）

松下 政好

情報セキュリティは、どんなに設備やシステムを整えても完全ではなく、最終的には個人の意識が重要です。業務で使用するパソコンの容量が飛躍的に増加し、膨大な情報が保管できる今、情報そのものが私たちの「財産」であることを深く認識してもらえるよう、OKIグループ全従業者の感度や意識の向上に継続的に努めていきます。また、業務上のパソコンの役割や必要性を見直し、パソコンで情報を保管しないシンクライアント※の導入を進めたいと考えています。

※シンクライアント ： ユーザが使うコンピュータ端末に必要最小限の処理をさせ、ほとんどの処理をサーバ側に集中させたシステムアーキテクチャ全般のこと。

IT化社会における情報セキュリティの重要性

業務システムの統合化やネットワーク化・モバイル化が企業活動にとって不可欠となった現在、ネットワーク上のセキュリティホールを通じた不正アクセスやコンピュータウイルスによる被害など、新しいリスクが生まれています。例えば独立行政法人情報処理推進機構の統計によれば、ウイルス検出数については減少傾向にあるものの、依然として年間3万4千件以上の被害報告がなされています。またここ数年ではP2P※1ファイル共有ソフトによる情報漏洩が続出しており、企業がこれらのリスクに対応する重要性は高まっています。

OKIグループは、「ネットワークソリューションのOKI」として、情報セキュリティの重要性を早くから認識し、一人ひとりのお客様に安心をお届けするために情報セキュリティ商品・サービスを提供するとともに、自らの情報セキュリティマネジメントに取り組んでいます。2002年度には情報セキュリティ基本方針を制定したほか、社内情報システム構築・運用部門においてISMS※2の認証も取得し、順次情報セキュリティ体制を強化してきました。

しかし、2006年9月、OKIグループ社員の個人所有パソコンからファイル交換ソフト「Winny」によりお客様の個人情報および業務関連情報がネットワーク上へ流出したことが判明。OKIグループではこのことを重く受け止め、再発防止を期して情報漏洩対策のための共通ポリシーを定め、セキュリティ対策のさらなる強化と情報管理の徹底にグループ全体で取り組んでいます。

※1 P2P ： Peer to Peerの略。直接2台のPC間でデータの送受信を行う通信形態。
※2 ISMS ： Information Security Management Systemの略。2005年10月に、ISO27001(ISO/IEC27001:2005)としてISO規格化された。

OKIグループの情報セキュリティの取り組み

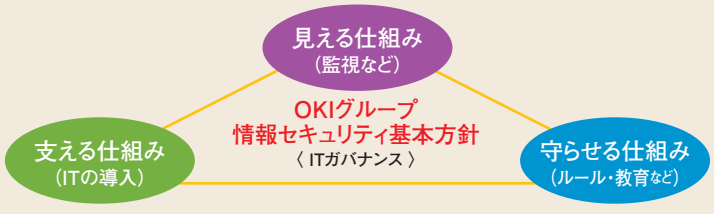
OKIグループは、情報セキュリティを確保するためには、複合的なアプローチが必要だと考え、「OKIグループ情報セキュリティ基本方針」に基づき、下図に示す3つの仕組みでセキュリティ施策を推進しています。

●情報セキュリティの「3つの仕組み」

セキュリティセンタでの監視
「支える仕組み」、「守らせる仕組み」の実施状況、および不正ソフトの導入をセキュリティセンタでの監視により把握

コンピュータウイルスの感染防止
24時間監視を行うサポートセンタを活用して、ウイルスの発生状況を監視し、タイムリーに情報提供

ワクチンのパターンファイルの自動更新
すべてのPC/サーバについてワクチンのパターンファイルの自動更新



共有サーバによる機密データの管理
機密データの保管・アクセス管理のためのOKIグループ共有サーバを設置

IT基盤の整備
●PCからUSBメモリなど可搬記憶媒体への書き込み制限 ●モバイルPCの暗号化 ●個人所有PCのネットワークへの接続制限 ●パスワード管理強化

データ定義の明確化と業務プロセスのルール化
お客様からお預かりしたデータや社内加工データの定義を明確にし、それらの取得・作成から廃棄までの業務プロセスの整備とルール化を行うとともに、関連する規程類を整備

情報セキュリティ教育の実施
●集合教育 ●eラーニング

情報セキュリティ委員会によるグループ管理の徹底

2007年度は情報漏洩対策の全社展開に注力するため、以下に示す活動計画を策定し、実行してきました。

まず、情報漏洩対策の仕組みをOKIグループの情報基盤を利用するすべてのグループ企業、およびそこで働く役員・社員・派遣社員・パートタイマーなどすべての従業者に展開するため、2007年5月、推進組織となる「情報セキュリティ委員会」を設置しました。その後全部門に対する説明会を経て、部門ごとの推進体制構築と計画策定を行い、順次実施しています。(P22参照)

今後も、情報セキュリティの確保と信頼の構築に向けて、OKIグループ一体となって取り組んでいきます。

●2007年度の主な情報セキュリティの取り組み

主な活動内容	作業内容	4	5	6	7	8	9	10	11	12	1	2	3
情報セキュリティ委員会発足	・セキュリティ方針と上期活動計画承認		▼										
全社共通施策の作成	・規程/運用フロー/IT等共通施策の作成		→										
全部門に対して説明会実施	・全部門/会社に対して漏洩対策導入手順、全社共通施策の説明			→	→								
各部門の展開計画作成と実施	・各部門で推進体制、スケジュールの展開計画書作成と実行				→	→	→	→	→	→	→	→	
情報セキュリティポータル設置	・全社共通施策の開示				▼								
情報セキュリティ教育	・全社共通施策をeラーニングで周知							→	→	→			
OKIグループ一斉点検	・施策内容の実施点検							→					
下期情報セキュリティ委員会	・上期実施状況報告/下期活動計画承認							▼					
情報セキュリティ監査	・監査室による情報セキュリティ監査									▼			

社員の声

システムソリューションカンパニー
法人ソリューション本部
鍋山 多恵

法人ソリューション本部は、旅客、鉄道、旅行、流通、各種製造業などさまざまなお客様にITソリューションをご提供しており、多種多様かつ膨大な量の情報を取り扱っています。このためセキュリティ施策を展開するにあたっては、管理すべき情報の再調査を行った上で、部門全体に説明会を実施しました。

施策にはPCから可搬記憶媒体への書き込み制限など、利便性を損ないかねないものも含まれるため、個々人が施策の必要性を理解しないと浸透しません。その点を中心に何度も説明を行ううちに、各員のセキュリティに対する意識レベルが高くなり、施策を推進する一要因となりました。今後も、より安心な情報管理を継続して行うため、体制を整備していきたいと思います。

Column

お客様の「安心」に貢献するセキュリティ関連商品

セキュリティ機能を強化したカラーLEDプリンタ

カラーLEDプリンタC8800dnは、プリントデータや印刷した紙文書からの情報漏洩を防ぐため、非接触ICカードによる認証印刷など、さまざまなセキュリティ機能を搭載することができます。特にハードディスクに蓄積されるプリントデータの暗号化機能を備えた「セキュリティキットタイプA 1」との組み合わせでは、国際的なセキュリティ評価基準ISO/IEC 15408に基づくITセキュリティ認証の評価保証レベル(EAL)3を取得しています。

モバイル機器向けアイリス認証ミドルウェア

「モバイル機器向けアイリス認証ミドルウェア」は、携帯電話、ノートパソコンなどのモバイル機器にアイリス認識※機能を組み込むためのミドルウェアです。盗難・紛失時などの他者による不正使用の防止はもちろん、社外から社内業務システムへのリモートアクセス、モバイル機器を用いた高額電子決済などにおいても、安心・安全な利用者認証を可能にします。

※アイリス認識：人の目のアイリスパターン(虹彩の模様)により個人を認識する技術。間違えて他人を受け入れてしまう確率1/100,000(赤外線カメラを使用すれば1/1,200,000)以下という高精度で、利用者を認証することができる。