富士通の取り組み

ルールと技術の両輪で行う
富士通の情報セキュリティへの取り組み

富士通はICTインフラを担う企業としての社会的責任と、お客様の重要な情報を扱うICTベンダーとしての責任を果たすべく情報セキュリティの推進に取り組んでいる。その特徴はルールと技術の両輪で対策を業務に取り込み、業務を支援する情報セキュリティを追求している点にある。また社内実践や豊富なソリューション実績からさまざまなセキュリティ対策ソリューションを打ち出している。

富士通株式会社
情報セキュリティセンター長
奥原 雅之 氏

富士通グループの指針に基づき情報セキュリティ対策を推進

スマートデバイスやクラウドの普及により、コンピュータを意識することなくその恩恵をいつでもどこでも誰もが享受できる時代が到来しようとしている。富士通は、こうした時代の方向性をいち早く捉え、従来のシステム中心から人が主役となるICT社会のビジョンを提唱。それがヒューマンセントリック・インテリジェントソサエティである。

ビジネスや暮らしのさまざまなシーンにICTが浸透していくヒューマンセントリック・インテリジェントソサエティにおいて、情報セキュリティは一層重要になる。富士通の情報セキュリティに対する取り組みは、ICTインフラを担う社会的な責任と、ICTベンダーとしてお客様への責任の両面を果たすものである。

富士通グループの指針では、「お客様のかけがえのないパートナーとなり、お取引先と共存共栄の関係を築く」とし、その実現において社員に対し機密保持の厳守を求めている。

グループ全体で情報セキュリティを推進する場合、部門やグループ会社によって異なる業界のガイドラインやお客様との契約項目への対応が必要となる。そこで、富士通では情報セキュリティマネジメントを実践するためのひな型として、国内外の基準を採り入れたSMF（セキュリティマネジメントフレームワーク）を各部門やグループ会社に提供（図1）。SMFにより富士通グループ全体での情報セキュリティの基本的な考え方を守りながら、各部門やグループ会社はそれぞれの特徴に合ったマネジメントシステムを構築している。また、各部門から選出された委員が定期的に委員会を開催しSMFをベースにした対策の推進と徹底を図っている。

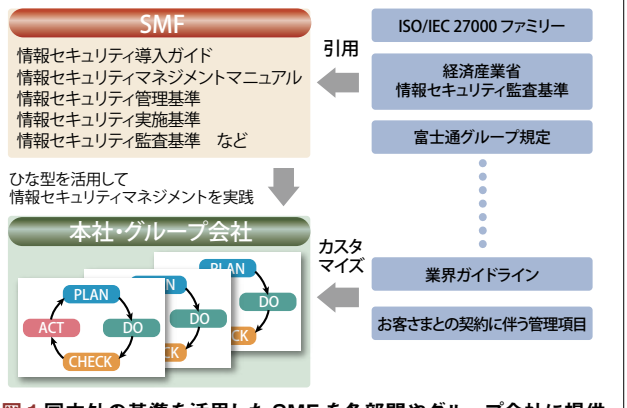

図1 国内外の基準を活用したSMFを各部門やグループ会社に提供

こうした外部基準への対応に加え、具体的な対策ではICTを積極的に活用。例えば、従業員の業務プロセスに着目し、人の注意力に依存する対策をICTに置き換える取り組みを行っている。電子メール誤送信対策、情報セキュリティ対策診断ツールによるパソコン起動時の自動診断、PC暗号化、遠隔指示によりノートパソコンのデータを無効化するリモートデータ消去ソリューションなどを搭載した社内標準パソコンの導入を推進。ルールと技術の両輪を上手くまわし、情報セキュリティ対策を業務の中に組み込み、業務を支援する情報セキュリティを追求している。

運用面を重視し情報セキュリティ管理責任者の育成にも注力

情報セキュリティの取り組みでは運用が重要な鍵となる。富士通では、ルールやツールを導入後、形骸化しないように、SMFを実践する各部門などに情報セキュリティ管理責任者を置き、四半期ごとに状況の報告を義務づけるとともに、情報セキュリティ管理責任者などの人材育成にも力を入れている。

また、運用面では現場の意識向上も欠かせない。情報セキュリティの必要性や施策に対する理解を深める情報提供や啓発活動、eラーニングはもとより、社内SNSにより現場の声も集めている。

最近はスマートデバイスに関する要望が多い。2012年度からは社内規定を一部改定し、スマートデバイスを活用可能にし

た。規定改定の際に重視したのは、スマートデバイスをPCの延長線上として位置付けるということだ。

スマートデバイスの活用条件としてまず社内支給のみとしBYOD(Bring Your Own Device)は許可していない。またセキュアな環境で社内ネットワークにアクセスするためにリモートアクセスサービス「FENICS Ⅱユニバーサルコネクト」を利用。これにより端末紛失時のIDロックなどをいつでも実施できるうえ、利用者の所属や職務に応じて接続時間、接続先などのアクセス制御も容易に行える。さらにメディアに保存するときは暗号化を行い、持ち出しは最小限とするなど、PCと同様にさまざまな規定を組み合わせて情報漏えい対策を強化。紙情報を持ち歩くよりも紛失時の情報漏えいリスクは少ないとも言えるだろう。現在、クラウドサービスとの関連も含めてBYODへの対応も検討している。

標的型メールなど新たな脅威への対応が必要なネットワークセキュリティでは、先端技術をもつ専門部隊が動向分析や対応にあたっている。

標的型サイバー攻撃は情報詐取といった目的を達成するために何度でも攻撃を仕掛けてくる。従来のようにファイアーウォールなどで侵入を阻止するだけでなく、侵入後にどうやってリスクを下げていくかという発想に切り替えることが大切である。富士通では新たな脅威に対し、単一ではなく有効な対策を組み合わせることにポイントを置いている。

情報セキュリティ対策に完璧はない。怖いのは事故の発生が隠蔽され影響が拡大することである。富士通では「ルールが守られていたら現場としての義務は果たされていたとみなす」という企業文化を築いてきた。例えば「不審なメールは開くな」と言っても、何が不審かわからなければ現場は対応できない。不審なメールを見分けるチェック項目といったルール化を行い、万一ウイルスの侵入を許してしまってもセキュリティ事故の報告も含め、ルールが守られていた場合は責任を問わない。情報セキュリティの取り組みにおいて、会社は社員の味方であり、ルールを堅持する社員を守るというメッセージを社員に伝えている。

社内実践や豊富な導入実績を活かしたセキュリティコンサルティング

富士通ではSMFによるセキュリティ対策の考え方や徹底した社内実践、さらにハードウェアからミドルウェア、クラウドサービスまでワンストップで提供しているICTの総合ベンダーとしての豊富な実績を活かしたセキュリティコンサルティングを行っている。

サイバー攻撃など新たな脅威が顕在化してきたことで、情報セキュリティ対策への関心が高まるのに伴い、富士通のセキュリティコンサルティングを導入、検討されるお客様も増えている。さまざまな情報セキュリティ対策の課題に対し、経験豊富なコンサルタントがポリシー策定から情報セキュリティの可視化、監査、ユーザー教育までをサポート(図2)。さらに攻撃段階に合わせた総合的な対策を実現するサイバー攻撃対策やスマートデバイスのセキュアな環境での業務活用を支援するスマートデバイスセキュリティなどお客様のニーズに最適なソリューションを提供している。

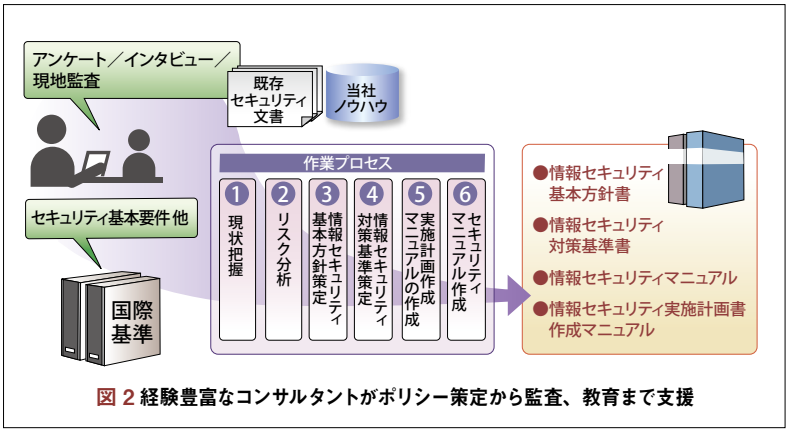

図2 経験豊富なコンサルタントがポリシー策定から監査、教育まで支援

富士通のセキュリティコンサルティングにおいて現在、注力しているのがクラウドを対象にしたコンサルティングだ。クラウド化に伴うセキュリティの課題整理や、ガイドラインの策定などを支援し、お客様企業のセキュリティポリシーに沿ったクラウドサービスの導入をサポートしている。

また富士通のクラウドサービスを安心してご利用いただくために、サイバーテロ、不正利用といったクラウドサービスにおけるセキュリティの脅威に対し、迅速かつ的確に対応する「富士通クラウドCERT」を2010年に設立。富士通クラウドCERTは、脆弱性診断やモニタリングなど情報セキュリティの運用、緊急対応、情報セキュリティマネジメントの3つの役割を担い、グローバル規模でお客様のビジネスを支える。

新たな脅威が次々と登場してくる現在、大切なのは客観的かつ冷静に恐れを抱くことだ。国家を標的とするサイバーテロは、社会的インパクトは大きいが、すべての企業が攻撃対象となるわけではない。脅威や対策に対するアンテナを敏感にしながら、自社に合った情報セキュリティ対策を継続的に実践していく仕組みづくりが重要である。富士通は、情報セキュリティ報告書などにより情報セキュリティの取り組みを公開するとともに、お客様のビジネスを守るためにセキュリティコンサルティングやソリューションの提供にも努めていく。

eふぁみりもあわせてご覧ください!
http://jp.fujitsu.com/family/honbu/family/
巻頭言や事例でのインタビューの様子、IPAから提供されている情報セキュリティのツールなどをご紹介しています。