サイバーセキュリティーへの取組み

原田　融　　濱田　恒生

サイバー攻撃の高度化・巧妙化により、企業や団体からの情報流出事故が続発し、被害が拡大する中、企業はウイルスなどのマルウェア（以降はウイルスと記述する）対策などの従来型の情報セキュリティーから、サイバー攻撃に対応する「サイバーセキュリティー」への転換と整備に関する責任を求められている。本稿では企業の重要な経営課題の一つである、サイバーセキュリティーに関するOKIの取組みと社内ノウハウに基づき提供するセキュリティーソリューションを紹介する。

企業を取り巻くセキュリティーリスクへの対応

サイバー攻撃の増加、被害の拡大に対して、企業は社会的信用の失墜やブランドイメージの毀損、最終的には業績の悪影響へつながる情報セキュリティー事故の与える影響に対して、重要な事業リスクと捉え、サイバーセキュリティーの強化・整備に乗り出している。

経済産業省は独立行政法人 情報処理推進機構とともに、「サイバーセキュリティ経営ガイドライン」を制定し（2015年12月）、企業がサイバーセキュリティーに取り組む指針を示した。本ガイドラインでは、サイバー攻撃から企業を守るために、経営がリスクを認識し、経営のリーダーシップのもとで、サイバーセキュリティーを推進するための3原則、及び経営から情報セキュリティー責任者へ指示すべき重要10項目がまとめられている。

サイバー攻撃に備えて、経営の意思を反映した情報セキュリティー推進体制を整備することが、セキュリティーリスクへの対応のスタートであり、企業の重要な課題でもある。

OKIの情報セキュリティー推進体制

OKIは「情報セキュリティー委員会（委員長：情報責任者）」を中心とした体制のもとで、見える仕組み、支える仕組み、守らせる仕組みの3つの柱で、セキュリティー機関のガイドラインに適合した情報セキュリティー対策を推進し、各事業部と各グループ会社に任命した情報漏洩対策責任者を通して、同一施策（体制、ツール、教育など）をグループ全体へ展開してきた。この推進体制により、情報セキュリティーの均一化と対策の強化を図り、サイバー攻撃などの脅威に備えている。

OKIの3つの柱の具体的な対策内容を以下に述べ、情報セキュリティーにおける基本方針の概念を **図 1**に示す。

（1）見える仕組みとは

- 情報資産の利用や情報セキュリティー対策の実施状況を把握して、情報セキュリティー対策の改善につなげる
- ITサービスの利用状態を監視して、違反行為を検知、防止する

（2）支える仕組みとは

- 重要な秘密情報を集中管理して、適切なアクセス権限やアクセスログの記録により、情報を保護する
- 情報流出経路をブロックし、情報の流出を防止する

（3）守らせる仕組みとは

- 秘密情報を定義し、具体的な管理プロセスの規則を定めて周知する
- 全従業員への情報セキュリティー教育や情報セキュリティー一斉点検などの啓蒙活動を定期的に実施する

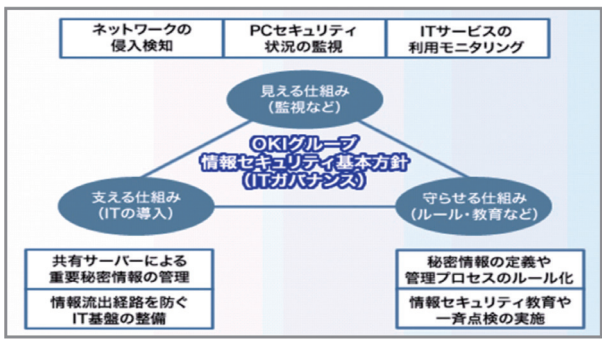

図 1　OKI グループ情報セキュリティ基本方針

また、情報セキュリティーを推進するためには、仕組みや体制の整備に加えて、日々発生する標的型やばらまき型のメール攻撃、ランサムウェア（パソコンやファイルサーバーのファイルを暗号化して身代金を要

求する）や外部からの脆弱性スキャンなどのサイバー攻撃のリスクを分析すること、世の中で発生するセキュリティー事故やセキュリティー機関から入手した脆弱性情報、及びセキュリティーガイドライン改正などの外部環境の変化を捉えること、その結果から、情報セキュリティー対策を改善・強化するためにPDCA管理サイクルを確立し、運用することが重要である。

サイバー攻撃への対策

サイバーセキュリティーで重要なことは、情報を守るためにネットワークとサーバーやパソコンへ適切な対策を講じた上で、IT全体の監視を行い、問題の発生を素早く発見し、原因を分析し、迅速な対策を取ることである。

サイバーセキュリティーへの対策を適切に講じるためには、サイバー攻撃による不正侵入やウイルスのダウンロードを遮断するための「入口対策」、サーバーやパソコンがウイルスに感染しても外部への情報流出を遮断するための「出口対策」、お客様からお預かりした重要な情報の不正な持出しを防止するためのファイルやデータベースのアクセスログ監視などの「不正防止対策」を効果的、かつ多層に配置することが重要である。対策を多層に配置する理由は、たとえば「入口対策」が破られて未知のウイルスが社内ネットワークへ侵入し、パソコンが感染しても、「出口対策」で活動を開始したウイルスの不正サーバーとのアクセスを遮断して、更なるウイルスの侵入や情報の流出を防ぐことが可能になるからである。

OKIが導入している代表的な入口対策、出口対策、不正防止対策の仕組みを以下に述べ、サイバーセキュリティー対策の概要を **図 2**に示す。

（1）入口対策

- ファイアウォール：外部からの不正侵入とDoS攻撃を遮断する
- 侵入検知／防御：外部からの不正なアクセス（スキャン活動など）を検知し、外部からの不正な侵入を遮断する
- メールフィルター：マルウェアやSPAMなどの危険な添付ファイルを除去する
- 振舞い型検知：ウイルス対策ソフトでは検知できない未知のウイルスをサンドボックスで動かしてその挙動からウイルスを検知、遮断する

（2）出口対策

- ファイアウォール：社内からの不正な通信（ウイルスの通信など）を遮断する
- IDS（Intrusion Detection System）/IPS（Intrusion Prevention system）：社内からの不正なアクセス（ウイルスの通信など）を検知、遮断する
- Webフィルター：ウイルスなどによる社内からの不正なサーバーへのアクセスを遮断する

（3）不正防止対策

- ネットワーク接続制御：802.1x認証により、不正な端末のネットワーク接続を遮断する
- 統合認証：Active Directoryの認証により、なりすましを防止する
- DLP（Data Loss Prevention）：可搬記憶媒体の使用制限、重要情報の保護により、情報流出を防止する
- DB監視：DBに対する不正なアクセス（管理者権限の不正利用、未許可の操作など）を監視し、情報流出を防止する

（4）その他の対策

- ウイルス対策：ウイルスを検知し、削除する
- 脆弱性診断：サーバーのOSやミドルウエア、及びWebアプリケーションに潜在的な脆弱性の存在有無を診断する
- セキュリティー事故への対策：事故発生に備え体制を整備し訓練を実施する

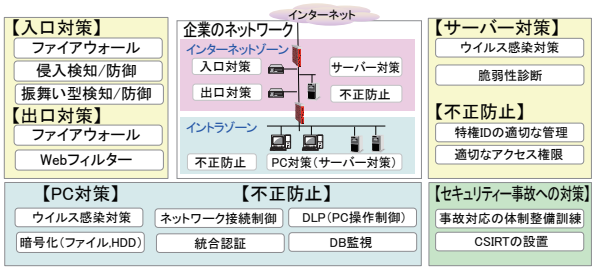

図２　サイバーセキュリティー概念

セキュリティー事故発生への備え

企業はセキュリティー事故の発生に備え、被害拡大の防止と抑制に向けて、コンピュータやネットワーク（特にインターネット）上でセキュリティーの問題が発生した場合に対応する企業内CSIRT（Computer Security Incident Response Team）などの体制を整備しなければならない。

具体的には、社内、及び外部機関との連携を含めた緊急体制の整備、緊急体制を発動する基準、被害拡大を防止するための緊急回避策（たとえばインターネットを停止する基準や方法の準備）、セキュリティー事故を開示する手順や開示すべき内容を定めておくことである。

OKIは2008年に企業内CSIRT「OKI-CSIRT」を構築し、日本シーサート協議会へ加盟している。その目的は、セキュリティー事故が発生した際に「迅速に対応可能な体制の整備」とセキュリティー機関や他企業CSIRTとの「情報共有と連携強化」による、インシデント対応力の向上である。

OKI-CSIRTを構築してから8年間の活動の中で、インシデント対応の基本となる情報セキュリティー監視の強化（侵入検知、ウイルス感染、未知のウイルス侵入、SNSへの情報流出など）と監視結果からインシデントの発生を見える化するなどの仕組みを整備して、多様化するセキュリティーリスクへ対応してきた。

また、インシデント予防活動として、ソフトウェアやネットワーク機器などの脆弱性情報の社内共有や社員への教育・啓蒙活動にも取り組んでいる。

これら、OKI-CSIRT活動の全体イメージを **図 3**に示す。

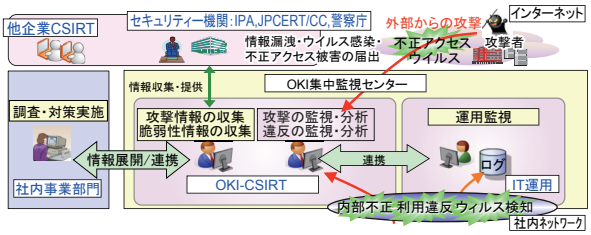

図 3　OKI-CSIRT 活動の全体

OKIが提供する セキュリティーソリューション

OKIは、社内で培ったノウハウを活かしたソリューションとして、情報セキュリティー支援サービスを提供している。その範囲は、**図 4**に示すように「コンサルティング」「脆弱性診断」から「CSIRT構築・運営」「教育サービス」「SOC（Security Operation Center）アウトソーシング」などを視野に入れたトータルサービスである。

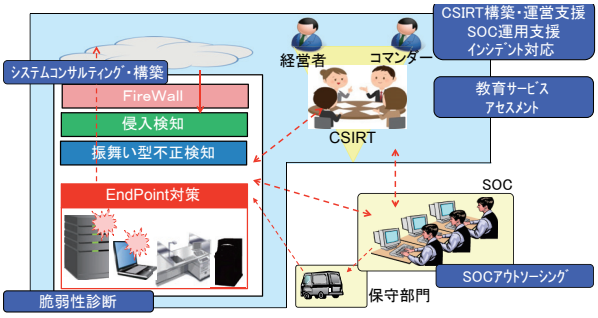

図 4　情報セキュリティー支援サービス

主なサービスの内容を以下に示す。

- **コンサルティング**
  ガバナンス計画やセキュリティー強化のロードマップ策定支援、セキュリティー認証取得や体制構築/改善を支援する。
- 脆弱性診断
  Web診断、ネットワーク診断、モバイル・ワイヤレス環境診断により脆弱性の現状を分析する
- **CSIRT 構築・運営**
  CSIRTのセキュリティー専門組織の構想立案から運用設計までを支援する
- **教育サービス**
  情報セキュリティーの最新動向や事故事例・対策、社内ルールなど、ニーズに合わせて人材育成を支援する
- **SOC アウトソーシング**
  セキュリティー監視センタからのリモート監視により、異常トラフィックやログの解析業務に対応する。また、セキュリティー運用業務の高度化や改善支援を行う

情報セキュリティー支援サービスの 提供ステップ

本サービスは、以下の3段階のステップによりお客様に提供する。

①コンサルティング / アセスメント
お客様の現状を調査/分析し、課題抽出、脆弱性ポイントの洗い出しなど、お客様の現状課題を可視化

②設計 / 構築
分析結果に基づき、体制やアーキテクチャーの見直しなど課題対策を検討、設計/構築を支援

③保守 / 運用
日常の監視・分析、インシデント発生時の調査・対処検討を遠隔、または常駐にて支援

サポートサイクルによる セキュリティー強化

サイバー攻撃は多種多様に日々進化し、セキュリティーリスクを最小限に維持するために、**図 5**に示す情報セキュリティーのサポートサイクルを回し続けることが重要となる。OKIの情報セキュリティー支援サービスは、コンサルティングから構築、運用支援まで、あらゆるフェーズへのサービスを提供することで、継続的なセキュリティー強化を実現する。

図５　情報セキュリティーのサポートサイクル

効率的なサポートサイクルの実現

日々進化する脅威に対抗するには、情報セキュリティーのサポートサイクルをより効率的に回し続けることが求められる。その方法として、社内のシステムに散在するログを分析することで、情報セキュリティにおける改善点を見出すことが有効である。このログ分析をどのように実現するかが、効率的なサポートサイクルの実現につながるものと考えているが、そのためのソリューションとしてSIEM（Security Information and Event Management）と呼ばれる統合ログ管理システムがある。情報セキュリティー支援サービスでは、SIEMの導入を推奨しており、ここに紹介する。

SIEMは、複数のセキュリティーデバイス、データベース、アプリケーションのログ、イベントを収集し一元管理することで、イベントログの可視化、横断的な相関分析、脅威の早期発見、対処を可能とする。SIEMの導入前後の導入効果を**図 6**に示す。

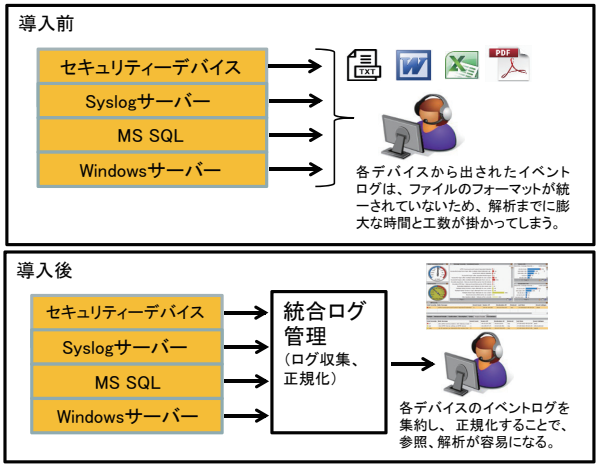

図６　SIEM の導入効果

SIEM導入後のメリットを、以下にまとめる。

- **利便性の向上**
  複数デバイスのイベントログを集約して正規化を行うことで、管理者が容易に参照、解析を実施することが可能となる
- **セキュリティー向上**
  一元管理しているイベントログを常時監視することで不正アクセス、異常な操作などのインシデントを早期発見、迅速に対処可能となる
- **運用工数、コスト削減**
  イベントログに対して常に可視化、相関分析を実施しているので、解析完了までの時間、工数を削減することが可能となる

IoTセキュリティーへの対応

今後、IoTが普及するとあらゆるもの（デバイス）がインターネットへ接続されることになる。それらのデバイスは当然ながらサイバー攻撃などの対象となる。IoTの普及による新たな脅威に対して、総務省と経済産業省は「IoTセキュリティガイドライン」を策定し（2016年7月）、IoT機器やシステム、サービスの提供にあたってのセキュリティーの指針を示した。

OKIはIoTセキュリティーを重要な課題と捉え、ネットワークへ接続するデバイスの増加に伴う膨大なログの効率的な分析や工場の製造機器やセンサーなどの多種多様なデバイスの安全なネットワークへの接続を実現するための技術や製品となる、AI、エッジ、IoT、次世代エンドポイントセキュリティーなどの評価・導入検討を進めている。

おわりに

本稿ではOKIのサイバーセキュリティーの社内の取組みと提供するセキュリティーソリューションを紹介した。OKIは社内で培ったノウハウを活かしたソリューションである情報セキュリティー支援サービスを市場に展開していき、今後普及するIoTへの対応を含めて、お客様が情報通信システムを安心・安全に利用可能なように、これからも挑戦を続ける。 ◆◆

●筆者紹介

原田融：Toru Harada. 情報・技術本部 情報企画部
濱田恒生：Tsuneo Hamada. 情報通信事業本部 新規事業開発室