NEC

企業利益につながる新しいセキュリティソリューション
―協調型セキュリティ「InfoCage」―

日本電気㈱
第一システムソフトウェア事業部
マーケティング・販促グループ
マネージャー　三浦 一樹氏

日本電気㈱
第一システムソフトウェア事業部
マーケティング・販促グループ
主任　辻 貴孝氏

NECの新セキュリティコンセプト「協調型セキュリティ」

近年、多くの企業がセキュリティ対策として、個々のインシデントに対応して様々な投資を続けてきた。しかし、企業を取り巻くセキュリティリスクは多様化しており、しかも守るべき対象と対策が複雑化するなか、従来のようなポイントソリューションの導入による個別対策には限界があり、セキュリティリスクを防ぐことは困難となっている。

一方で、セキュリティを優先するあまり制約ばかりが増え、ビジネス現場においてはITの利便性が低下しているという声もよく聞かれる。これは、よく言われる「セキュリティのCIA（Confidentiality：機密性、Integrity：完全性、Availability：可用性）」のうち、CとIばかりに注力した結果、Aが軽視された状態になったからにほかならない。

NEC第一システムソフトウェア事業部の三浦一樹マネージャーは、「もはや、個別リスクに応じた個々の対策だけでは、情報システムを危険から守ることはできません。すべてのセキュリティリスクを個別対策で防ごうとすると、莫大な手間とコストがかかってしまいます。したがって、部分最適ではなく、全体最適を図るような取組みが必要です。しかも、“やらされ”感の強い“対策”ではなく、ITによる利便性向上、サービス向上のためのセキュリティでなければなりません。そのためNECでは、セキュリティを“対策”と捉えずに、“企業利益につながる活用方式”と位置づけています。しかし、“セキュリティ投資は利益を生まない投資”と言われることがまだまだ多く、その主な原因は、個別対策の集合によるセキュリティマネジメントの不整合にあります。この負のスパイラルから脱却し、安全性と利便性を追求する新しい取組みにより企業価値を高めることが重要です」と語る。

セキュリティへの取組みは、自社に最適なしっかりとしたセキュリティポリシーを策定し、何をどの程度まで守るべきかの優先順位を定めたうえでPDCA（Plan-Do-Check-Action）サイクルを回すことができるマネジメント体制を構築することが重要だ。しかし、複雑化するセキュリティの脅威、利便性を無視した個別セキュリティ対策など、セキュリティマネジメントを行ううえでは様々な課題がある。このような課題を解決し、PDCAサイクルによる効率的なセキュリティマネジメントを行うためには、統一ポリシーのもとリスク要因を可視化し、個別の対策を連携させることで、セキュリティ対策全体の一元管理を実現することが必要だ。

「NECでは、お客様の課題に合わせて個別の対策を行うだけでなく、“フェイルセーフ（fail safe）”の考え方を基軸に、個々の対策間を連携させ、全体としてセキュリティ対策が協調することにより、既存投資の有効活用とセキュリティレベルの向上の両立を実現して企業利益につなげる新しいセキュリティコンセプト“協調型セキュリティ”を提唱し、これに基づくセキュリティソリュー

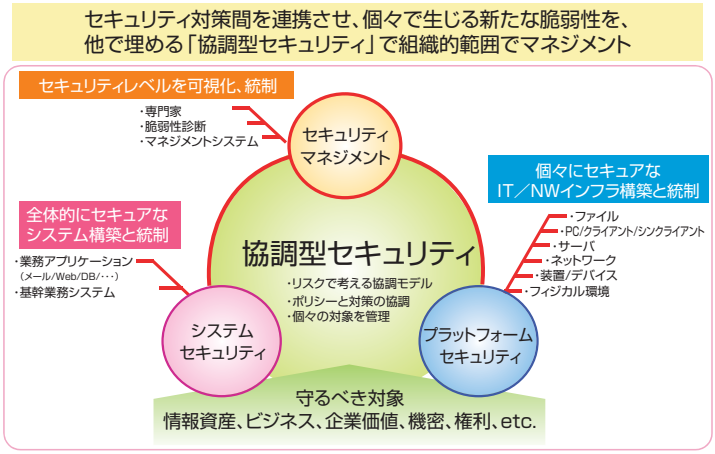

図１　セキュリティの新しい考え方「協調型セキュリティ」

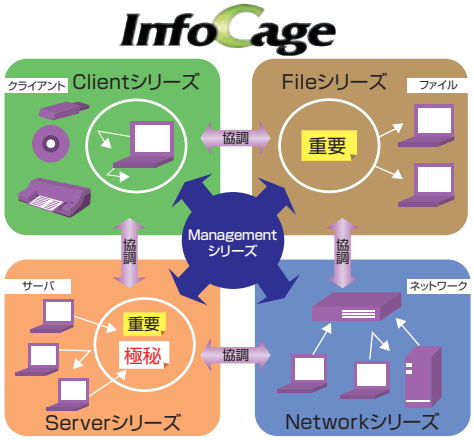

図２　InfoCageの全体像

ションを提供しています。」（辻 貴孝主任）

協調型セキュリティとは、統一したポリシーのもと、PCやサーバ、ネットワーク、ファイルなどそれぞれのセキュリティ機能を相互にかつ自動的に連携させることで、システムのセキュリティを強化するものである。図１に示すように、セキュリティレベルを可視化し統制する「セキュリティマネジメント」を中心に、個々にセキュアなIT/ネットワークインフラの構築と統制を行う「プラットフォームセキュリティ」、全体的にセキュアなシステム構築と統制を行う「システムセキュリティ」の３つ領域で構成しているが、守るべき対象の基軸は情報資産であり、ビジネス、企業価値、機密、権利などである。また、PCやネットワークはその器と位置づけている。

三浦一樹マネージャーは、「協調型セキュリティには、テクノロジーの観点とビジネスの観点の２つのコンセプトがあります」としたうえで、「テクノロジーコンセプトは、セキュリティ対策間を連携・協調させ、個別対策では埋められない新たな脆弱性を、他で埋める“協調型セキュリティ”によって組織的範囲でマネジメントするというものです。もう一つのビジネスコンセプトは、パートナー各社の“連携・協調”によってお互いの強みを活かしてより付加価値の高いものを提供することです。パートナーの選定は、市場でのデファクト製品を中心に行っています」と述べている。

つまり、各領域での対策が協調することにより、複雑化している脅威に動的に対処することを可能にする。各領域での対策を追加していくと、各対策が相互に自律的に協調し、組織全体のセキュリティレベルが向上するという考え方だ。このため、NEC及び市場のデファクト製品を中心に、関連製品間の連携動作によって協調型セキュリティを推進するようにしている。さらにもう一つの特長は、協調型セキュリティは、既存の環境を一新するのではなくて、既存の環境を有効活用しながらポイントごとの機能を順次追加し、さらにPDCAサイクルを回しながら次の対策製品を追加導入することで、セキュリティの投資コストを抑制しつつセキュリティレベルを向上させるという点だ。

「協調型セキュリティ」を具現化する「InfoCageシリーズ」

企業の利益向上に貢献するNECの新しいセキュリティコンセプト「協調型セキュリティ」を実現するソリューションの中核製品として提供されているのが「InfoCage」だ。InfoCageは、図２に示したように、

- PCなどクライアントの暗号化、認証を行う「Clientシリーズ」
- ファイルやコンテンツの暗号化やフォルダ認証を行う「Fileシリーズ」
- サーバからのデータ持ち出しを制御する「Serverシリーズ」
- 持ち込みPCの検知遮断、ネットワーク管理を行う「Networkシリーズ」
- 製品別の管理情報を統合管理する

「Managementシリーズ」の5つのシリーズから構成されている。しかも、図3に示すように、「協調型セキュリティ」のコンセプトに基づき、個々の対策が動的に「協調」することにより、組織全体のセキュリティ向上を実現している。また、各パートナー製品との「協調」により、既存の対策環境を活かしながら、あらゆる脅威に対して必要な対策を段階的に導入することを可能にしている。

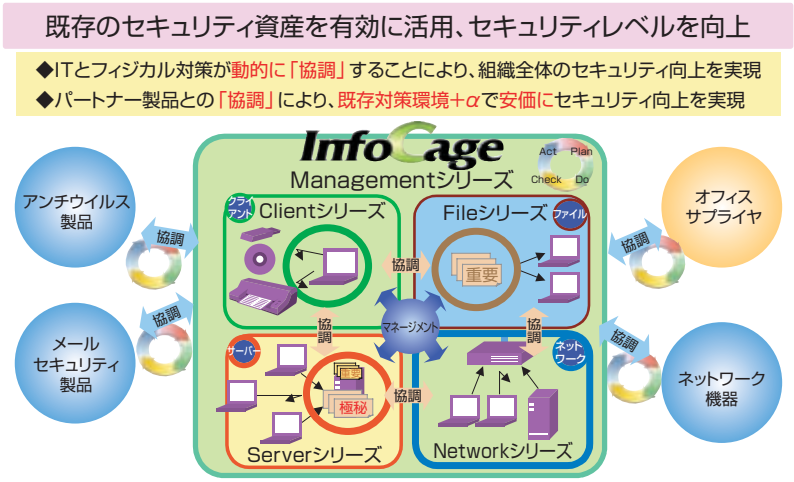

図3　セキュリティレベルを向上するInfoCageの役割

●InfoCage Clientシリーズ

認証強化、暗号化、外部デバイス接続制御や環境固定支援、操作ログ機能などをオールインワンで提供。これにより、盗難・紛失による重要情報の流出や私物USBメモリや社内PCの不正利用など社内に潜む情報漏えいのリスクを軽減。

●InfoCage Fileシリーズ

共有データを社内・社外で積極活用することを前提に、重要な情報へのアクセス権、暗号化、操作監視などの機能を提供。

●InfoCage Serverシリーズ

機密情報が集まるサーバ自体を防御するソリューション。機密情報の持ち出し制限やサーバへのアクセス制御、改ざん検知などの機能を提供。

●InfoCage Networkシリーズ

許可されないPCや問題のあるPCを自動で検知し、自動指示や社内から隔離または排除することにより組織のセキュリティレベルを維持する機能を提供。

●InfoCage Managementシリーズ

コンテンツ、PC、サーバ、ネットワークといった組織内のITコンポネントを網羅的に統合管理し、緊急パッチの公開をはじめ日々変化するセキュリティリスクを可視化することで、継続的なセキュリティマネジメントを実現する機能を提供。

NECの強みを活かしネットワークセキュリティとマネジメントに注力

5つのInfoCageシリーズのうち、現在NECが最も力を入れて取り組んでいるのがInfoCage Networkシリーズと、InfoCage Managementシリーズだ。

●社内ネットワークを安全な状態に保つネットワークセキュリティ

InfoCage Networkシリーズでは、エンドポイントにおけるPCの不正接続を防止する「InfoCage不正接続防止」、ポリシー違反PCをネットワークからの隔離し治療する検疫システムを実現する「InfoCage PC検疫」の2つの製品を提供している。

前者は持ち込みPCの不正接続を防止するもので、社内ネットワークに接続されている機器の情報を集めPC管理台帳を自動作成し、台帳に未登録の不正PCのネットワーク接続を防止する。「InfoCage PC検疫」やパートナー各社の製品と連携することで、より強固なセキュリティシステムを実現する。

なおNECでは、社内ネットワークに持ち込まれた無許可PCからの不正接続を自動検知し、接続を防止するアプライアンス製品「InterSec／NQ30b」（写真1）を提供している。これは、InfoCage不正接続防止Network Agentをプリインストールしたもので、既存のネットワークを変更することなく導入でき、小形・軽量、セットアップも容易といった特長を持つ。

また、後者はセキュリティポリシーを満たさない（パッチ未適用など）

写真1　InterSec/NQ30 bの外観

ポリシー違反PCをネットワークから隔離し、治療するソフトウェアである。様々な機器やソフトと連携して検疫システムを実現する。本年8月には、機能を強化した「InfoCage PC検疫 V2.0」をリリースしている。「InfoCage PC検疫 V2.0」では、①ネットワーク構成やセキュリティ状況の自己診断を始めとする運用管理機能の強化、②マルチレイヤスイッチ「UNIVERGE IP8800シリーズ」との連携による、シンクライアント環境への対応、③SSL -VPN機能を活用したF5ネットワークスジャパン社のFirePassとの連携（エンドポイントセキュリティチェックによる自動識別）を図っている。特に、運用管理機能については、顧客のシステム運用に柔軟に対応できるよう以下のような機能強化を図っている。

(1) 自動診断機能の強化

システム管理者からの要求で自動的に情報採取やアクセス制御を実施する「InfoCageエージェント」が、導入されてないPCを自動検出し、管理されてないPCからの通信をクライアントファイアウォール機能でアクセス制御し、ウイルスやワーム感染からシステムを守る。

(2) 管理サーバの二重化対応

管理サーバを二重化することで、待機系サーバでの業務継続と緊急時のポリシー変更を可能にする。

(3) バックアップ機能の強化

検疫サービスを停止することなく、オンライン自動バックアップを可能とした。これにより、ミッションクリティカルなシステムでの導入も容易にしている。

(4) 猶予期間・有効期間の設定

検疫を実行する猶予期間の設定を可能にしている。すぐにパッチ（修正プログラム）適用できない環境においても柔軟に対応し、業務の継続を可能とする。また社内のセキュリティポリシーを満たしたPCを、社外で利用可能・利用不可能とするための有効期間を設定可能とした。これにより、外出の多い営業システムでの適用を可能にしている。

●効率的なセキュリティマネジメント実現のために

セキュリティ強化にはPDCAの確立が最も重要であり、効率的なセキュリティマネジメントを行うためには、組織の状況に合わせPDCAをいかに回していくかが鍵になる。そのためには、ITを活用した“見える化”と“自動化”によって、セキュリティマネジメントの不整合性をなくし、企業利益につながる効率的な投資を行うことが必要だ。

「協調型セキュリティなら、活用すべき重点レイヤへの部分的導入から始まり、徐々に取り入れて協調のレベルを高めることにより、PDCAを最適な形で回すことが可能になります。また、セキュリティ活用を自動化することで、高度なセキュリティレベルの維持と効率化を図ることができます。協調型セキュリティでは、静的なマネジメントから、見える化・自動化による動的なマネジメントへ段階的に強化することを目指しています。」（辻 貴孝主任）

InfoCage Managementシリーズでは、具体的な製品として、全体システムの見える化、効率的なセキュリティマネジメントの実現を支援する「InfoCageセキュリティリスク管理」を提供している。本製品は、社内のセキュリティリスクを数値で把握でき、管理者が行うセキュリティ管理をサポートするソフトウェアである。主な特長として、①専用ソフト不要のWeb管理画面での可視化、②ポリシー適用指示による徹底、③協調（InfoCageシリーズ製品やパートナー製品との連携）の3点があげられる。

「InfoCageセキュリティリスク管理」を活用することで、社内に接続されているセキュリティ状況を自動で定量化し、管理者はWeb画面で確認するだけで把握することができるので管理が効率的になり、パッチ未適用によるワーム感染などを防ぐことができる。

以上、NECが提唱する「協調型セキュリティ」と具体的な取組みを紹介した。NECグループでは、安全に情報を活用しながら、業務の活性化・競争力の強化につながるセキュアな環境でITを有効活用することを目指し、今後も協調型セキュリティに基づくソリューションの提供に注力していく方針だ。

お問い合わせ先

日本電気㈱
第一システムソフトウェア事業部
TEL：03-3456-3248
E-mail：info@mid.jp.nec.com
URL：http://www.nec.co.jp/security/