ビジネス環境に柔軟に対応する「協調型セキュリティ」

三浦 一樹

要 旨

近年のセキュリティ対策は、オープン化されたITシステムの影響から始まっています。多様化する顧客のシステムに有効的に、そして柔軟にシステム強化を実施するためには、どのようなセキュリティ対策と製品でなければならないのでしょうか？　本稿では、個別製品や個人単位から、全体統制、組織単位でのセキュリティ対策に求められるニーズと課題に対応すべく開発した、「協調型セキュリティ」InfoCageについて説明します。

キーワード

●セキュリティ ●協調型 ●情報漏えい ●流出 ●InfoCage ●WORKS ●安全 ●安心 ●柔軟

1. はじめに

汎用機でビジネスが継続実施・運用されているITシステムは、まだ多くあります。過去のビジネスの大多数は、汎用機で行われています。

NECは個人で楽しむPC-8800シリーズを誕生させ、PC-9800シリーズからビジネスとして利用されるようになり始めました。まだOSは、DOSの時代です。

Microsoft社がWindows3.1を販売し出した頃、TCP/IPの通信ソフトがNECを含めた各ベンダから販売されました。Windows95の発売で、ネットワーク接続は加速化され、当然のようにPCがネットワークに接続される社会になったのです。

PC単体としてネットワーク接続されていない時代は、セキュリティ対策は一般的ではありませんでした。クローズな汎用機やPCは、オペレータ室に配置され、情報漏えいやセキュリティ対策は、オペレータ室への入退管理で実施されています。部屋に入るためには鍵があり、入退には紙媒体である帳簿に記録されてきました。

導入・構築の容易性、低価格な費用の理由から、オープンなITシステムが、本格的にビジネスに導入され稼働し始めた頃、誰もがオープンなITシステムの利便性を感じ始めていました。

一方、利便性を逆手にとったクラッカーは、データを操作することで征服感を楽しんでいました。当初は愉快犯であったクラッカーは、その後、システムには重要データが存在することに気づきます。重要データは売ることができる、つまり、それにより儲けることができるのです。

企業のオープンITシステムに対するセキュリティ対策との戦いが、ここから始まったといえます。

2. セキュリティ対策の現状、求められるニーズと課題

企業のセキュリティ対策、それはインターネットとの接続地点であるゲートウェイでの対策が多く実施されています。

ファイアウォールに始まり、DMZ（非武装地帯）で重要データを保護します。一般的にオープンなITシステムの環境では、重要データはDMZ上に配置され、Webサーバ、メールサーバ、DNSサーバなどが設置されています。Webサーバは、APサーバ層とDBサーバ層に分かれ、アクセスのコントロールとバランシングするのがAPサーバ、重要データを保持するのがDBサーバとなります。

過去のセキュリティの攻撃は、このDMZをターゲットとして狙われてきました。現在ではDMZのサーバを守る対策だけでは十分でありません。その理由は、大きく2つあります。

1) ユビキタス社会（ADSL、無線LAN）の普及
2) 電子メールの普及

これまでの一般的なオープンシステムでは、3層構造のビジネスアプリケーションやWebシステムでの限られたアクセスにより、セキュリティの対策がある程度確保されていました。しかし、ユビキタスなネットワークインフラの普及に伴うPCの移動、電子メールの普及でコンテンツの移動、この要素により、ウイルスやワームの感染の可能性は格段に高くなりました。

ITシステムでのセキュリティ対策は、サーバ、ネットワー

ク、PCクライアントをイメージします。ネットワーク機器を提供するベンダでは、セキュリティ強化した製品が多く開発され、販売されています。PCクライアントには、アンチウイルス製品がバンドルされていることが多くなりました。DMZを守るためにIDS（不正侵入検知）、IDPを導入している企業も多くなりました。しかし、本当にこれでセキュリティ対策は十分なのでしょうか？

これまでのセキュリティ対策はプロフェッショナル中のプロの仕事でしかなかったのかもしれません。ウイルス・ワーム対策を日々実施することで、システム管理者や運用者は多大なる工数とコストが発生していました。IDSの運用においては、インシデントが多く発生しすぎて、ネットワークパケットを監視するには良いが、どのインシデントがシステムへ影響するのか判断するには、豊富な知識が必要とされます。

セキュリティ対策も多様化しているのが現状です。高度なテクニックを駆使するクラッカーと日々戦っているシステム管理者のスキルを向上し続けるには、学習や教育の時間も必要です。

運用を効率化したいシステム管理者にとって、セキュリティ対策は悩みの種です。運用プロセスの見直しには、ITILといったベストプラクティスが発表され、日常的なシステム運用とユーザサポートである「サービスサポート」、長期的な計画と改善の「サービスデリバリ」が存在します。セキュリティは、ITILでは別枠になっており、これがまたシステム管理者を悩ませています。

今、求められるニーズは、容易な導入と運用にあります。また既存システムを変更することなく、セキュリティを強化させることができれば、顧客の資産を無駄にすることなく、ステップアップした、よりセキュアなITシステムを実現できます。

セキュリティ製品を提供するベンダには、得意領域が異なるため、多種多様な製品が顧客のシステムに導入されている場合、管理運用工数が非常にかかります。NECにとっても、この課題を解決することが求められています。

3.「協調型セキュリティ」InfoCageの誕生

単なるポイント的なセキュリティ対策、これらの多種多様なベンダの製品と密連携し、新しいセキュリティ対策ができれば、顧客にとってメリットがあります。既存環境を生かした、セキュリティの向上が実現できるからです。

InfoCageでは、「サーバ」「ネットワーク」「PCクライアント」「ファイル（コンテンツ）」の観点で、ポイントセキュリティ対策製品がラインナップされています（**図1**）。

1. 協調型セキュリティを実現する「InfoCage シリーズ」好評発売中
2.「Networkシリーズ」 PC検疫システムを強化
3.「Fileシリーズ」 ファイル暗号Vista対応

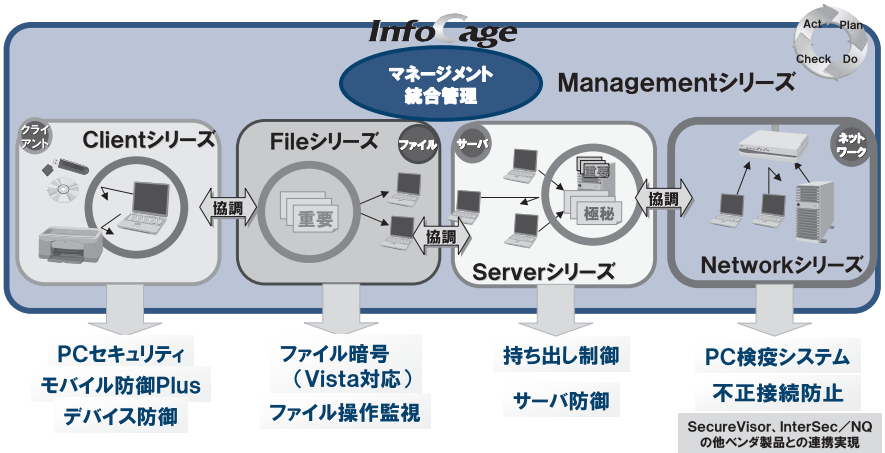

図1　InfoCage体系

市場の状況を考慮すると、アンチウイルス製品をNECが開発することは得策でありません。すでにデファクトであるベンダの製品とは、連携し、協調したITシステムであり、ビジネス環境を継続提供する、これがInfoCageの基本コンセプトです。

「REAL IT PLATFORM」ビジョンの「柔軟」のキーワード、これはInfoCageの「協調型」にも相当します。システムを止めることなく容易に拡張・変更ができる柔軟性。仮想化技術だけでなく、セキュリティ技術も相当するものを、InfoCageでは提供しているのです。

また「REAL IT PLATFORM」の「安心」は、セキュリティ基盤として提供する必要があります。高信頼技術、故障やトラブルなどのシステム稼働停止を回避するのはハードウェアやクラスタリング技術の領域だけでなく、セキュリティにおいてもゼロ・ディフェクト、フェイル・セーフな発想でInfoCage製品に反映されています。

安全なビジネス環境、それは「安心」して利用できるプラットフォーム、運用の複雑さのないシンプルなITシステムなのです。

4.「協調型セキュリティ」の実現例とテクノロジー

「協調型セキュリティ」InfoCageでは、どのような具体的なセキュリティ基盤を提供し、他ベンダとの製品と連携しているのでしょうか？

PCクライアントにおいては、WindowsのOS機能であるファイアウォール、アンチウイルスなどが代表的です。これは市場の導入状況から優先的に考慮したためです。

Microsoft社は、今後もOSのセキュリティ強化をし続け、将来的にはTCP/IPのネットワークと同様に標準機能で、PCクライアントのセキュリティ対策をオールインワンで実施するかもしれません。InfoCageではPCセキュリティといった「認証」「暗号」「ポリシ設定・適用」「追跡ログ」を提供しています。将来的にはMicrosoft社と連携した製品を共同開発する可能性もあります。

ネットワークでは、ネットワーク機器が一番多くあります。ファイアウォールでのOPSECポート遮断や、TCP/IP単位でのセッション切断、これらはIDSの得意とする領域ですが、このIDSを簡易化したのが、InfoCage 不正接続防止（旧名: WebSAM SecureVisor）です。また、ハードウェア・アプライアンス化した製品としては、InterSec/NQ30bが発売されています。

ネットワーク型では、ハブやスイッチ、セグメント単位に設計を実施する場合が多いですが、これらに対応するセンサ部分は、InfoCageが自社開発するだけでなく、各ベンダとの協業により、連携性を深めています。

サーバ型では、機密サーバを徹底的に守ります。Linuxのセキュリティ設定や、SecureOSの発想に近いものです。ネットワークは、その信頼性や継続性のための多重化設定がされていることが多くあります。ネットワークセキュリティ設定に誤りや脆弱点があると、サーバからの情報流出の危険性が高くなります。現在のオープンITシステムである3層構造で考えると、APサーバとDBサーバ間で利用されると、有効的であるといえます。もちろん、PCクライアントとWeb、AP、メールなどのサーバ間での利用も問題ありません。

ファイル（コンテンツ）型は、様々な製品との暗号化において連携できています。InfoCageの暗号化が他ベンダとの製品と連携、協調することで、ファイルなどのコンテンツが外部に流出したとしても、解読できない仕組みになっています。またゲートウェイ形の製品と連携することで、「暗号化されていないデータを外部に出さない」という連携も可能です。

5.「協調型セキュリティ」のゴール

「協調型セキュリティ」InfoCageは、他製品と連携もしくは、他製品の部品の一部として組み込まれます。これは、ITシステムだけの話ではありません。現在のビジネス環境、オフィスにおけるフィジカルなセキュリティ対策にも適用されます。ビルへの入退室や、IDカードによる統合ID管理など、生活の一部として組み込まれ、利用者は意識することなくセキュリティ強化が実施される、これが理想であり、ゴールです。

各種のセキュリティ対策のポイントに対応するInfoCageの各製品は、SOAやSaaSの発想から、ITインフラが整備されれば、アプリケーションをインストールすることなく配布適用され、セキュリティ強化が「REAL IT PLATFORM」として実現できます。これが「協調型セキュリティ」です。

しかし、NECでしかできないような得意分野もあります。統合管理の領域です。各ベンダのセキュリティ製品を、監視し制御する統合管理マネジメント製品により、InfoCageと運用管理WebSAMはさらに協調し、ITシステムの継続した改善と

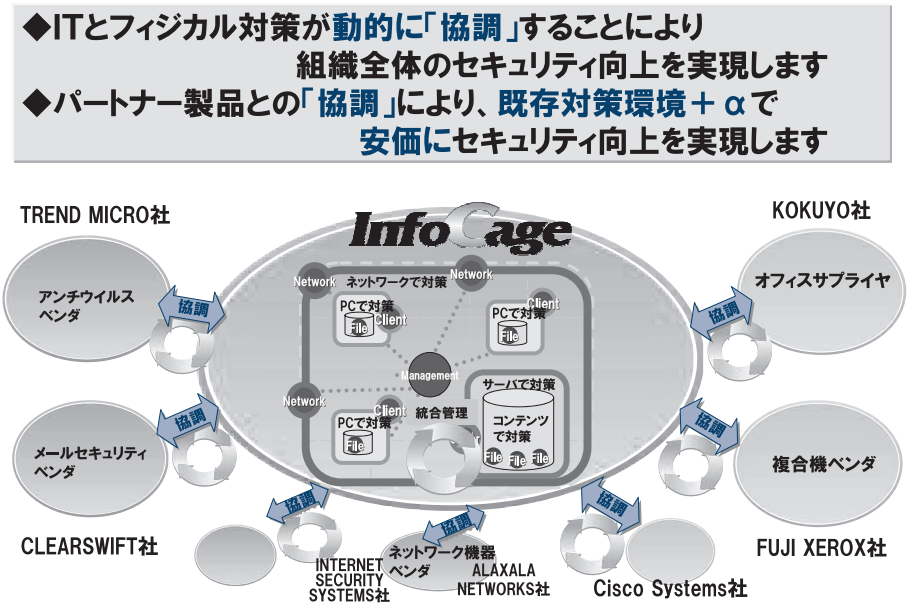

図2 NECの考える「協調型セキュリティ」

「快適」を提供することができるでしょう（**図2**）。

6. まとめ

昨今の内部統制におけるIT全般統制は、運用管理の話題で済まされる傾向が多くあります。セキュリティにもログ追跡できる機能は提供されています。しかし、コンポーネントとして検知し、システム状態の把握と「見える化」、これらの統制の状態から、長期的な改善計画を実施するのは、運用管理だけでなくセキュリティ対策も同様です。

今後NECは、InfoCage WORKSとして、戦略的パートナ製品と密連携し、協調したビジネスモデルを開拓し、新市場へ提供し続けていきます。

「協調型セキュリティ」InfoCageは、「REAL IT PLATFORM」の一部として、「柔軟」「安心」「快適」を提供し、安全なビジネス環境を実現し続けます。

●本論文に関する詳細は下記をご覧ください。

関連URL

http://www.nec.co.jp/cced/infocage/

執筆者プロフィール

三浦 一樹
システムソフトウェア事業本部
第一システムソフトウェア事業部
マネージャー