基盤技術

従来のセキュリティ対策の限界を破る「協調型セキュリティ」

則房 雅也・後藤 淳・森野 淳一
矢野尾 一男・榊 啓・寺崎 浩

要　旨

ブロードバンドネットワーク、持ち運び容易な高性能PC、便利なアプリケーションなど、企業のIT環境が飛躍的に充実するのに合わせて、セキュリティ管理対象と複雑さが飛躍的に増えました。求められる対応の速さは「ゼロ」という言葉が使われるほどに短くなっています。情報とその器が移動するため、静的かつ単一なセキュリティ対策製品ではカバーできない課題が多く出てきています。そこで、今回「協調型セキュリティ」という考え方を導入します。これにより対象領域の異なるセキュリティ製品が連携して機能し、移動する情報と器に対して二重三重のセキュリティ管理を実現し、企業内に高いセキュリティレベルを維持します。これを具現化するのが、新しいInfoCage製品群です。また「協調型セキュリティ」はパートナー製品にも広げ、紙文書や入退管理システムなど、異業種製品とのセキュリティ連携を深めていきます。

キーワード

●協調型セキュリティ　●セキュリティ管理の協調　● InfoCage シリーズ　●パートナー製品との連携

1. はじめに

セキュリティに取り組む必要性は、90年代以降インターネットの利用が企業に浸透するに伴って、企業ユーザの間で広く認識され始めました。十数年を経た今、一般ユーザまで理解する社会的重要テーマとなりましたが、同時に当時では考えられないほど扱うべき管理対象は多岐にわたり複雑になっています。

セキュリティ管理が複雑化する一方で、コンプライアンスに基づく監査や顧客への説明など、適切なセキュリティ管理を行っていることを実証する機会がますます増えていく傾向があります。ここがこれまでと大きく異なる点であり、これからのセキュリティ対策に求められる新しい要件と言えます。

本稿では、これまでのセキュリティ要件の推移と対策の現状を分析し、複雑さを減らし広範囲で一貫性あるセキュリティ管理を実現する「協調型セキュリティ」について論じます。

2. セキュリティ要件の変貌と現状

企業がインターネットにつながった当初、企業ユーザにできることといえば電子メールとファイル転送程度に限られました。その後ウェブ技術が公開されると、ウェブを使った企業情報公開が浸透し、次第に企業活動とインターネット利用は切り離せないものとなりました。企業はインターネットとの境界にファイアウォールを置いてセキュリティ対策とし、VPN(Virtual Private Network)、IDS(Intrusion Detection System)、IPS(Intrusion Prevention System)、アプリケーションごとの対策を行うフィルタリング・ゲートウェイの導入へと対策範囲を広げています。

インターネットを起源としないセキュリティ対策にコンピュータウイルス対策があります。ウイルスの脅威は80年代に存在していましたが、電子メールへの添付ファイルが普及し、すべてのユーザを巻き込んだインターネット時代の脅威となりました。愉快犯的なウイルスは実害を広げるワームへと進化し、ネットワークからPCへ侵入する技術が巧妙になると、スパイウェアやボットといった新たな脅威が現れています。PC上のデータを破壊・改ざんするわけではなく、他のPCを攻撃するとか内部情報を送るという動きをするので、PCユーザが普段気づいていないこともあります。

日本市場で近年特に重要となったセキュリティ対策に情報漏えい対策があります。これまでの多くの対策がネットワークやPCへの攻撃を想定していたのに対し、情報漏えい対策で

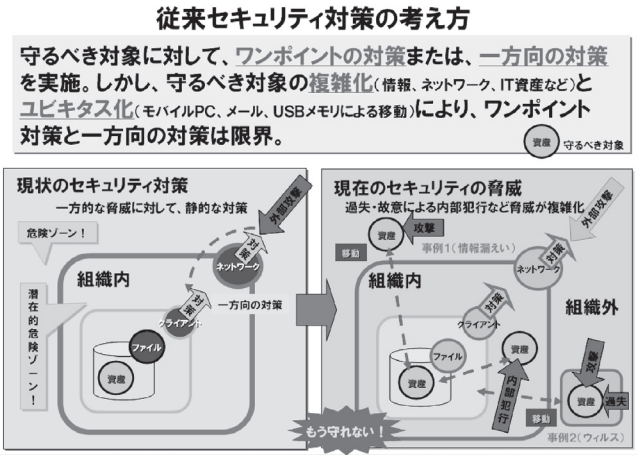

図1　アンバランスなセキュリティ脅威と対策範囲

は内部犯行、内部からの情報送信を管理対象にする必要があり、対策の考え方が本質的に異なってきます。多くの場合、社員が正常なPCやアプリケーションを利用中に漏えいが起こってしまいます。また、データの入ったPCが盗難に遭うことも想定する必要があります。

多くの企業では、これらのセキュリティ対策製品を、そのときどきの課題に合わせて導入してきました。ここにモビリティという要素が加わってきています。ユーザ、PC、情報が一定の場所にとどまることはなく、セキュリティ管理レベルの異なるところへ頻繁、簡単、一瞬にして移動します(**図1**)。

こうしてすぐに変化する管理対象の条件と増え続けるマルチ領域の対策製品間でセキュリティポリシーや機能の一貫性、補完性などを保障することはきわめて難しく、現状ではそれぞれ独立して機能する対策に頼るしかありません。管理対象が移動してセキュリティ管理の境界を越えるとき、予想しなかったセキュリティホールに落ちないように、運用管理者の作業はその複雑さで困難を極めています。

3. 協調型セキュリティとは、その真価

外部からの攻撃を防止する製品と、内部からの犯行を防止する製品では、共通する機能があってもそれぞれ異なる視点で運用管理されます。ユーザ認証、情報アクセスやデータ送信の許し方、ポリシー違反への対応など、それぞれの対策で得られた効果が、PCからネットワークというように管理対象の境界をまたがって情報が動いたとき、セキュリティ管理の脆弱性が生じないとは、実は保障されません。対策製品に十分細かな機能が提供されていても、ポリシー不整合のために管理の抜け道が生じる可能性があります。

たとえば、PC上の対策ソフトだけでデータ送信を制御しても、PC上あるいはユーザで何らかの違反が生じることがあります。スパイウェアが働く場合、ユーザが故意に漏えいを行う場合などです。このとき、途中のファイアウォールでPCからの通信をすべて止めるような対策ができると被害の拡大を防止できます。

「協調型セキュリティ」の考え方は、単一対象に閉じて機能するセキュリティ対策を、周囲の対象まで連携させて動作させることで、単一対象の管理だけでは生じてしまうセキュリティ管理の漏れをふさぐものです。従来の単一対象のセキュリティ対策は、ポリシーで表現された脅威に対する予防措置、その発見と脅威への防御を1つの機能に閉じて実現していました。そのため予防措置が無効化されたり、脅威を発見できても防御機能が無効化された場合、脅威を発見したという結果は有効活用されず、どこか他で用意された対策に頼ることになります。また、脅威を発見する条件も単体では限界があります。協調型セキュリティでは、個々の管理対象で脅威を発見し、それらを組み合わせて判断し、他の管理対象の防御機能にリアルタイムで伝えます。その結果、組織やイントラネットといった広い範囲で一貫性のあるセキュリティ対策を機能させることが可能になります。

対策漏れをふさぐ協調機能Cfは脅威、対策、対策の効果、効果を無効化する条件、脅威の変化で決まります。以下の**表**はその一例を示しています。

協調機能Cfは、セキュリティ対策で共通に実施している機能をまず活用します。**図2**のように、多くのセキュリティ対策は、認証、アクセス制御、証跡の管理を基本としています。信用できる認証、その結果得られたIDを基にしたアクセス制御で、多くの不正利用を防止することが可能です。

企業内IT環境でのセキュリティ管理対象は、「ファイル(コンテンツ)」「PC(クライアント)」「サーバ」「ネットワーク」の4つで現状重要なセキュリティ対策が施されている対象をほぼカバーできます。これら以外に、「紙文書(フィジカル)」「入退ゲート(フィジカル)」「ユーザID(ヒューマン)」といった管理対象が存在します。これらの間でセキュリティ対策を協調させるとき、対策をレイヤー化します。レイヤーの内側には協調動作を電子的に自動化できること、外側には人手を介在するものを位置づけます。もっとも内側には「ファイル」、その

表　脅威、対策、対策の効果、効果の無効化、補う対策の関係

脅威の存在場所	脅威の内容	脅威に対して とられている対策内容	対策が 効果を発揮する条件	対策が 無効にされてしまう場合	Cf: 対策の無効化を 補う方法
PC	ワーム・ウイルスによる情報の拡散	ゲート上でワーム・ウイルスを除去	データが暗号化されていない	シグネチャの無い新種ワーム・ウイルス	①PCの隔離 ②サーバへのアクセス制御
PC	汚染されたPCの持ち込み	PC検疫システムで汚染状況を把握	PCに検疫エージェントを導入	検疫エージェントがとめられる	③ゲート上でワーム・ウイルスを除去 ④PCの隔離
PC、ファイル	ネットワーク経由でファイルを持ち出し	リモートデスクトップなどのプログラム起動禁止	共有情報のアクセス権強化	プログラム名を変更して起動	ファイル暗号化とアクセス権限管理
PC、ファイル	リムーバブルメディアでファイルを持ち出し	外部記憶デバイスへの書き込みは自動的に暗号化	必ずユーザ認証、PCを利用するのは一人	認証が省略される認証済みのPCが悪用される	リムーバブルメディアの切り離し
PC、ファイル	メールにファイルを添付し不用意に送信	重要ファイルの常時暗号化	暗号鍵利用可能範囲での利用	編集作業などファイルを一次的に平文で保存	⑤メールサーバで平文ファイルをフィルタ ⑥PCの通信をロック
サーバ	不正ユーザによる操作	ICカードなど多要素認証の利用	個人に対する認証	カードの共有	認証条件、アクセス管理強化
ネットワーク	WAN上でのデータ盗聴	SSL、IPSECで通信を暗号化	VPNが作れる環境	平文に戻す装置より先の通信管理	ファイルの暗号化

ワーム・ウイルスによる情報の拡散の脅威に対しては、FWやゲートウェイ上でのウイルスの駆除という対策が取られます。しかし、新種の未登録シグネチャのウイルスが発生した場合、対策が有効に機能しません。これには、感染源のPCをネットワークから隔離する追加対策(①)やそのクライアントからサーバへのアクセスを制限することでウイルスの拡散を防止する追加対策(②)が有効です。また、汚染されたPCの持込の脅威に対しては、PC検疫システムによる防御という対策がとられます。しかし、検疫エージェントが停止させられると対策は有効に機能しません。これには、FWやゲートウェイ上でのウイルスの駆除という追加対策(③)や汚染されたPCの通信をゲートウェイで特定し、そのPCを隔離する追加対策(④)などが有効です。ファイルをメールに添付して送ることは日常茶飯事に行われています。PCでファイルを編集すると通常平文でファイルを残せます。これが送信されたときメールサーバで検出して(⑤)、PCでメールを使えないようにすると大きな抑止効果にもなります。

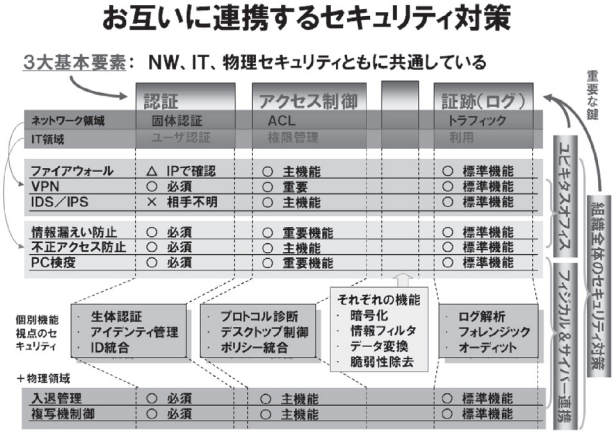

図2　セキュリティ対策の共通項

外に「PC」と「サーバ」、その外に「ネットワーク」があり、「紙文書」「入退ゲート」への対策はその外側に位置づけます。「ヒューマン」はすべてに関係しますが、人手に依存するのでもっとも外側のレイヤーに位置し、セキュリティ対策上は最後の砦といえます。レイヤーの中では、内側で生じた対策漏れは外側でふさがれることになります。

4. 協調型セキュリティの具現化

協調型セキュリティの実現は、「ファイル(コンテンツ)」「PC(クライアント)」「サーバ」「ネットワーク」を対象にした対策製品と、ポリシー管理と協調エンジンを提供する統合管理を揃えたInfoCage製品を中核として、他ベンダーを含む周辺製品との協調型セキュリティ連携を行うことで、フィジカル、ヒューマンといったレイヤーまで協調を実現します(**図3**)。

InfoCageシリーズ製品の間では、統合管理製品を介してダイナミックで密な連携を実現しますが、他ベンダー製品との

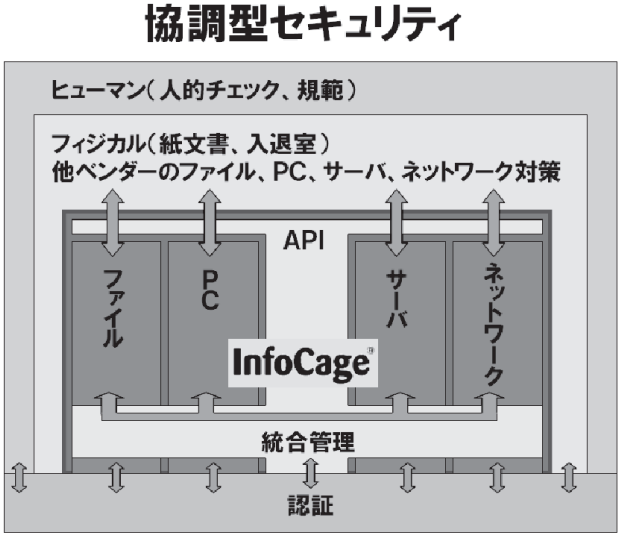

図3　InfoCageを核とした協調型セキュリティ

間は、InfoCageのいずれかの製品がまず協調します。これが基本形となります。たとえば、アンチウイルス製品との協調はInfoCage PCセキュリティ製品の役割です。同様に、ファイアウォールとの協調はInfoCage ネットワークセキュリティ製品が担います。それぞれで協調した結果はInfoCage製品を介して統合管理製品に伝わり、その先の協調内容が他のInfoCage製品に伝えられます。

基本形を超えたより強い協調を他ベンダー製品と行えるように、統合管理製品とのAPIを提供する予定です。たとえば、ファイアウォールでボットのアタックを検出したとき、APIで統合管理製品に通知することで、InfoCageが管理するPCやサーバにボットの対策を行わせるようなことが可能になります。

5. 協調型セキュリティの実現例

協調型セキュリティの実行例を示します(**図4**)。ここでは、暗号化していないファイルを添付して社外にメールで送ることはポリシーで禁止されているとします。このルールを無視して、ファイルを暗号化せずに添付してメールが送信された場合です。

①メールサーバに届いたメールの添付ファイルが暗号化されているかどうかを判断します。
②社外のアドレスに送られるメールに暗号化されていないファイルを見つけたなら、メール転送を止めます。
③InfoCage製品に、止めたことを伝えます。
④統合管理製品に伝わると、関係するInfoCage統合管理に協調の通知が届きます。

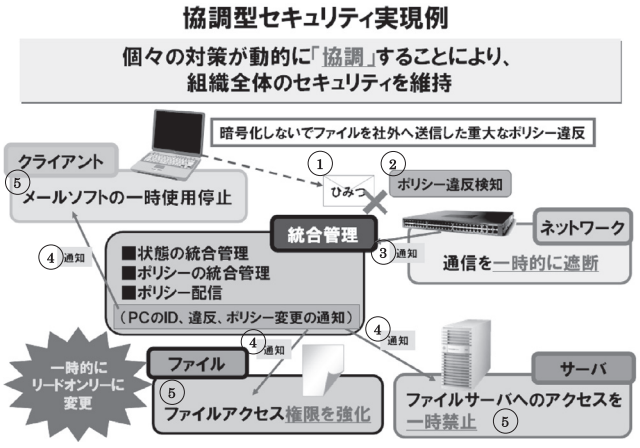

図4　協調型セキュリティで連係動作する例

⑤その結果を受けて、たとえば、
（ア）ネットワーク側でPCからの通信を一時的に遮断する
（イ）ファイルサーバがPCからのアクセスを一時的に拒否する
（ウ）暗号化されたファイルを複合化する権限を一時的に無効にする
（エ）メールクライアントを一時的に起動できないようにする
といった協調的なセキュリティ管理を実行させます。

6. より進んだ協調型セキュリティに向かって

協調型セキュリティは、企業内セキュリティ管理の容易化、広域での高いセキュリティレベルの維持、協調を利用して既存環境を活用した移行がデザインできる、などで企業内セキュリティレベルの向上を行えるものです。より進んだ協調に向けて、2つの大きな方向性があります。1つは、周辺システムとの協調を広げることです。たとえば、

①ファイアウォールとの連携
②IPSとの連携
③NW装置との連携
④アクセス管理装置との連携
⑤PCセキュリティソフトとの連携
⑥複写機との連携
⑦事務機器との連携

などが重要で、これら製品ベンダーとの協調型セキュリティ・パートナープログラムで強化を図っていきます。

もう1つは、一組織を超えて協調型セキュリティを実現することです。同じ企業内でも、場所が異なる場合や、関係会社では異なったセキュリティ管理が行われています。しかし、実際には1つのプロジェクトで、これら別組織の人たちが一緒に仕事をしており、プロジェクトの重要情報を共有し、セキュリティ管理レベルが異なるそれぞれの組織に持ち帰っています。そうなると情報漏えいはどこかセキュリティ管理があまくなったところで起こる可能性が高くなります。

このような組織を超えた協調型セキュリティを実現するためには、まずID管理の協調が鍵になります(**図5**)。ユーザ認証方式はそれぞれで異なっても構いませんが、ユーザのIDは関連付けが管理され、相手先組織で作業するとき、自社に戻って作業するとき、プロジェクト情報はセキュリティ管理レベル

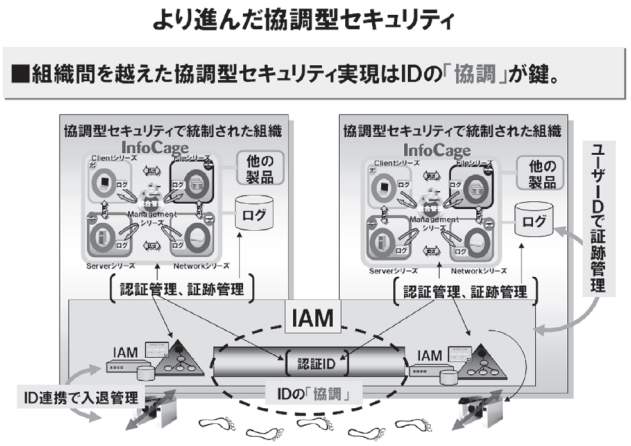

図5　組織にまたがるより進んだ協調型セキュリティ

を落とすことなく扱われ、利用証跡に含まれるIDが同一人物であることを追跡できるようになっていなければなりません。InfoCageシリーズの製品が、IDを相互利用できる機能(IDフェデレーション)を持つIDアクセス管理製品と連携することで、この実現が可能になってきます。

7. まとめ

本稿では、「協調型セキュリティ」の基本的な考え方と実現の方法を説明しました。単製品単機能で管理できるセキュリティには限界があり、脅威や利用条件が変化し個々の対策が無効になる場合が生じても、セキュリティ製品間でセキュリティ管理の協調を実現すると、対策の漏れを他のところで塞ぐことが可能になり、セキュリティ管理のレベルを高く維持管理できます。情報漏えい対策から内部統制へと、同質を求める管理範囲が組織的に広がっており、組織規模でPCやネットワークが協調してセキュリティを維持する方式は時代の要求に合っていると言えます。

協調型セキュリティを企業グループのように複数組織にまたがって適用していくには、ID管理の協調やより多くの情報機器との協調など、協調の範囲を拡張していかなければなりません。これは協調型セキュリティの考え方の重要なポイントになっており、継続して取り組んでいきます。最初は核としてInfoCageの一製品の導入から始まりますが、ステップbyステップで管理範囲を拡張させていき、組織を越えてでもセキュリティ管理を共有していけるようになるのが協調型セキュリティなのです。

執筆者プロフィール

則房 雅也
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
エグゼクティブエキスパート

森野 淳一
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

榊 啓
中央研究所
インターネットシステム研究所

後藤 淳
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
主任

矢野尾 一男
中央研究所
インターネットシステム研究所
主任

寺崎 浩
ソリューション開発研究本部
システム基盤ソフトウェア開発本部
主任