

# ネットワークセキュリティソリューション

吉田 稔\*  
寺沢 茂\*  
山崎 義直\*

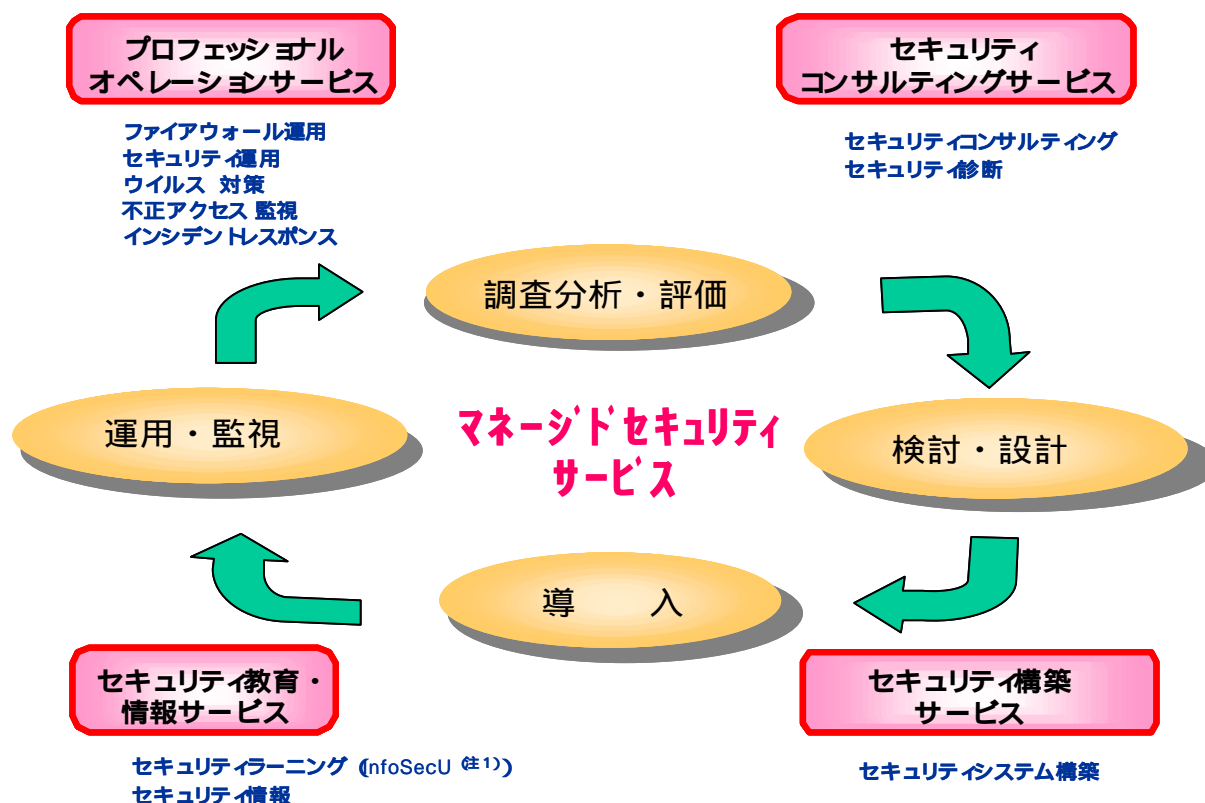
## 要 旨

情報システムはネットワークの発達、とりわけ、インターネットの発展によって、利便性をもつことができた。その一方で、ウイルス、ワームや、サービス不能攻撃 DoS (Denial of Services) 等の不正アクセスの脅威にさらされているのも事実である。過日繁殖した MS-Blaster をみると、対象ソフトウェアの脆弱性の公開から、ワームが現れるまでの時間は以前 (NIMDA は脆弱性公開から 6 ヶ月かかった) に比べ、大きく短縮している (MS-Blaster は 1 ヶ月で出現)。それだけ、迅速な対応が要求されていることがわかる。不正アクセスの手法も多様化し、これらに対応して、情報システムを守らなくてはならない。

ネットワークセキュリティで重要なことはライフサイクルにしたがって、新たな脆弱性、脅威への対応を維持し

ていくことである。これにはネットワークセキュリティの高度な専門技術が必要になる。たとえば、日々、多くのセキュリティ情報を収集し、自社システムに対処が必要か否か、緊急を要するか否かを判断しなくてはならない。これを自社で行うには、要員の確保、育成が必要で、時間とコストがかかる。ところが、脅威は待ってくれない。

このような状況に対し、三菱電機情報ネットワーク(株) (MIND) はお客様に代って、ネットワークセキュリティを実践するサービスを用意している。MIND マネージドセキュリティサービスはネットワークセキュリティのライフサイクル全般をカバーする各種サービスを用意している。



(注1) InfoSecU は、米国RedSiren社の登録商標である。

## MIND マネージドセキュリティサービスの構成

MIND マネージドセキュリティサービスはネットワークセキュリティライフサイクルに対応したサービスを用意している。個々のサービスは互いに関連、連携し、システムのセキュリティという広い視野で提供されている。例えば、不正アクセス監視サービスでは、ファイアウォール情報、パッチ適用情報、セキュリティ診断結果等を考慮して監視を実施している。

## 1. まえがき

企業活動の基盤として、情報システムの重要性はますます高くなっている。情報システムはインターネットの進展やブロードバンド化により、ネットワーク接続され、外部とのインターフェースが増えている。言い換えれば、利便性を享受する反面、リスクに直面していると言える。すなわち、ウイルスやワーム、システムへの不正侵入などのリスクにさらされていることになる。このような攻撃から、情報システムの安定稼働を維持するため、ネットワークセキュリティを抜きにしては、情報システムの“安全”、“安定”は考えられなくなっている。

本稿では2章で、ネットワークセキュリティのライフサイクルについて紹介し、第3章で、ワームを通して得たセキュリティの現状を述べる。第4章ではネットワークセキュリティのソリューションとしてのマネージドセキュリティサービスを紹介する。

## 2. ネットワークセキュリティのライフサイクル

ネットワークセキュリティには4つのフェーズから成るライフサイクルがある(図1)。調査・分析フェーズでは情報システムの現状のリスクを分析し、検討・設計フェーズで、セキュリティシステムを設計する。導入フェーズでは、セキュリティシステムを構築し、実際の運用をスタートさせる。運用監視フェーズでは不正侵入等のチェック、新たな脆弱性を監視し、対処する。そして、新たなリスクに備え、調査・分析フェーズに戻り、ライフサイクルを廻していく。

重要なことは“セキュリティシステムを構築して完了”ではないということである。日々、あらたな脆弱性が公開され、新たなウイルスやワーム、攻撃パターンが生み出されている(図2)。これらに対処していかななくては、構築したセキュリティシステムが役に立たなくなってしまうのである。

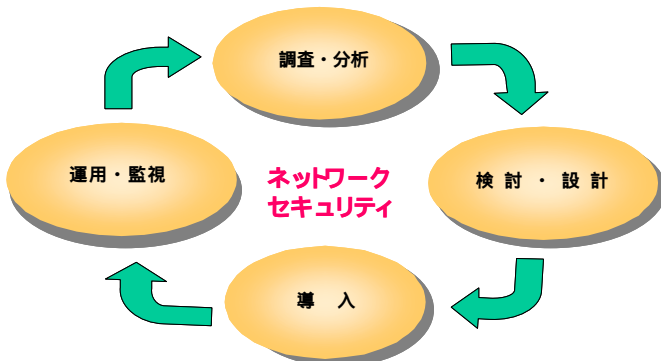
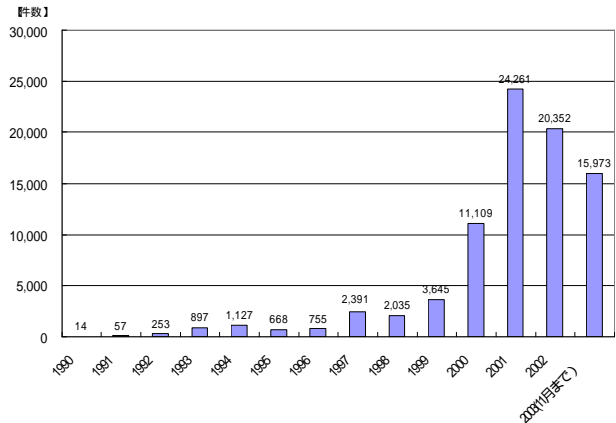


図1 ネットワークセキュリティのライフサイクル



出典：情報処理振興事業協会セキュリティセンター

図2 ウイルス届出件数の推移

## 3. ネットワークセキュリティの現状

### 3.1 MS-Blasterの教えたもの

2003年8月にMS-Blasterと呼ばれるワームが大繁殖した。このワーム騒動は2点の教訓を残している。

#### 3.1.1 脆弱性への迅速な対処

2001年にも、NIMDAというワームの大繁殖があった。NIMDAはMicrosoft IIS<sup>(注2)</sup>の脆弱性を利用したもので、この脆弱性の公開から6ヶ月後にワームが登場している。一方、MS-BlasterはRPC(Remote Procedure Call)の脆弱性を利用したワームで、その脆弱性が公開されてから、わずか1ヶ月余りで登場している。すなわち、脆弱性の公開から、実際に被害がでるまでの時間が1/6に短縮されている。もちろん、今回もこの脆弱性への対処をしていた情報システムには感染の被害はなかった。この事実は、情報システムにとって重要な脆弱性が公開された際には、早い対処が必要であるということを伝えている。これには、日常からセキュリティ情報に注意し、対象となる脆弱性が自システムにあるかどうかを見極め、パッチ適用などの迅速な対処をする必要がある。

#### 3.1.2 内部からの感染

MS-BlasterはRPCの脆弱性を利用したものであるため、ファイアウォールで外部からの侵入は防いでいたにもかかわらず、感染し、被害を受けた企業が多かった。外部からの感染には防御していたが、内部からの感染に対し、無防備だったのである。実際には、外部から持ち込まれたPC、媒体を経由して感染したものである。ネットワークセキュリティでは“内部は安全”という思い込みがあった。内部からの不用意な行動を制御することが必要である。持ち込まれたPCのチェック、不用意に外部からソフトウェアを導入しないことなどはルール化する必要がある。また、

(注2) IISは、米国およびその他の諸国におけるMicrosoft Corporationの登録商標である。

内部からのアクセスにも不正アクセス監視システム IDS (Intrusion Detection System) を置き、監視するなどの対処も効果がある。MS-Blaster の場合は意図した感染ではなかったが、情報漏洩などの事件の70%は内部による犯罪であるという事実にも目を向けるべきである。

### 3.2 運用監視の重要性

上記の例でも解るように、ネットワークセキュリティへの対処は迅速化、対象の拡大へ向かっている。しかし、しっかりしたセキュリティ運用監視をしていれば、防げていることも事実である。ファイアウォールを設置し外部ネットワークとの通信のフィルタリングを行うこと、IDSを導入し不正アクセスを監視すること、セキュリティ情報に注意し、公開された脆弱性には迅速に対処することが肝要である。社内ネットワークへの接続にはウイルスやワームの感染がないことを事前チェックする等々を確実に実施することで、被害は必ず防げるのである。一方、セキュリティ運用監視が不備であるため、情報漏洩やサービス不能攻撃 DoS (Denial of Service) の踏み台にされた場合、社会的な信用とともに、多大な損害を被ることになる。

### 3.3 セキュリティサービスの活用

ネットワークセキュリティのライフサイクルを廻していくには、そのための体制が必要である。例えば、不正アクセス監視システムでアラームが上がった場合、そのアラームが緊急性を要するものか否かを迅速に判断し、対処を決めなくてはならない。また、現在、年間5万件ものセキュリティ情報(脆弱性情報)が公開されている。これらの情報を収集し、理解し、自社システムに必要な情報が否かでふるいにかけ、緊急な対処が必要か否かを判断しなければならない。これらへの対処には、ネットワークセキュリティの専門家かそれに準じるノウハウを持った人材と体制が必要である。これは時間とコストのかかることである。しかし、脅威となるアタックは待ってくれない。このようなネットワークセキュリティの実践を自社でできない場合は、専門家が提供するサービスを利用することによって、質の高い対処を実践することができる。

## 4. マネージドセキュリティサービス

三菱電機情報ネットワーク(MIND)はネットワークセキュリティのライフサイクルをカバーする“マネージドセキュリティサービス”を提供している。以下にその内容を紹介する。

### 4.1 MIND マネージドセキュリティサービスの特長

MIND マネージドセキュリティサービスの特長を以下に示す。マネージドセキュリティサービスは表面に現れた情報だけでなく、その周辺にある様々な情報(機器の設定環境、パッチ情報等)を駆使し、トータルに判断、実施されるものである。また、セキュリティの基本は24時間365

日の運用監視体制である。当然のことながら、セキュリティに休みはない。さらに、常に新しい情報、技術に沿ったセキュリティサービスであることが必要である。そして、サービス提供者自身がネットワークセキュリティの管理がしっかりできていなくてはならない。これらの考えに基づいて MIND マネージドセキュリティサービスは提供されている。

MIND マネージドセキュリティサービスの特長は、次の通りである。

- (1)情報システムの設定環境、状況を考慮し、トータルなセキュリティソリューションを提供する。
- (2)24時間365日の統合運用監視センターを基盤としている。
- (3)米国 RedSiren 社(旧 SRI Consulting)の技術ノウハウを活用したサービスである。
- (4)BS7799-2 及び ISMS 適合性評価制度の認証を受けたセキュリティ管理システムの下で提供される安心できるサービスである。

### 4.2 マネージドセキュリティサービスの紹介

以下にいくつかの特長あるサービスを紹介する。

#### 4.2.1 セキュリティ情報サービス

日々公開されるソフトウェアや各種機器の脆弱性情報をお客様に代って収集し、お客様システムへの影響の有無、緊急性を判断し、その対処を含めて報告するサービスである。緊急の場合は即刻、その内容と外部接続の切断、パッチの適用などの対処をお客様に報告する。緊急性のないものは、月次で報告する。このサービスは表面的なシステム構成を知るだけでは実施できない。お客様システムの動き、情報の流れを知った上で提供される専門家によるサービスである。

#### 4.2.2 監視アラームへの対応

構築したセキュリティ監視システムを使用し、24時間365日、情報システムの異常を検知し、その対処を報告する。その代表的なサービスが不正アクセス監視サービスである。不正アクセス監視サービスでは、監視システムからのアラームへの対応スピードがポイントとなる。IDSはセンサに不正アクセスのパターンを持ち、監視している通信がこのパターンに一致した場合にアラームを上げて通知する。したがって、疑いのあるパターンはすべて、アラームとして通知する。この通知内容と対象システムを考慮してその緊急度を判断しなくてはならない。これは高度の専門技術を必要とする作業である。MIND マネージドセキュリティサービスでは IDS によるセキュリティ監視に二つの技術を加味して対応している。いずれも迅速な判断と対処へのアプローチで、被害の防止、最小化を狙ったサービスである。

一つは不正アクセス防御システム IPS ( Intrusion Prevention System )の導入である。IPS はIDS の機能に加え、様々な異常を検知し、異常パケットの廃棄、セッションリセットなど防御機能も持つシステムである( 図 3 )。急激なトラフィックの増加、異常なアドレスをもつパケット、使用を禁止しているサービスへのアクセス等、設定にしたがって、セキュリティ異常を検知し、即時に対処を行うことができる。

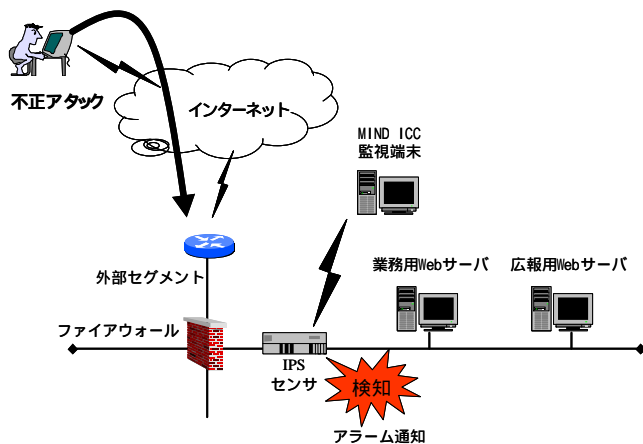


図 3 IPS 導入例

二つ目は相関分析システムの導入である。これはアラームが上がった場合、セキュリティ専門家が行う解析を自動的に行うシステムである。相関分析システムではマネージャがIDSだけでなく、ファイアウォールやサーバのログをリアルタイムに収集している。IDSからアラームが上がると、相関分析システムが関連するファイアウォールのログ、サーバのログを分析し、その危険度を判断する( 図 4 )。危険であると判断した場合にアラームとして通知する。IDSでアラームとなっても、ファイアウォールで廃棄している場合は相関分析の結果、アラームとはなくなる。逆に、サーバで異常パケットを検知していれば、アラームとして、緊急な対処が必要となる。セキュリティ専門家は相関分析の結果を見て、対処を判断し、お客様へ報告を行うことになる。アラームの分析を自動化することで、迅速な判断と対処が可能となる。

#### 4.3 セキュリティ診断サービス

ネットワークシステムのセキュリティレベルは日々の脆弱性公開だけでなく、操作ミスや、不用意な設定変更によって低下する。これをチェックするには定期的なセキュリティ診断が有効である。セキュリティ診断サービスはお客様のシステムに擬似的な攻撃を試みてシステムのセキュリティ度を診断するサービスである。これも単に診断ツールを使用し、その結果を報告するだけでは不十分である。対象システムの構成、情報の流れ、運用を考慮しセキュリティレベルを判断しなくてはならない。

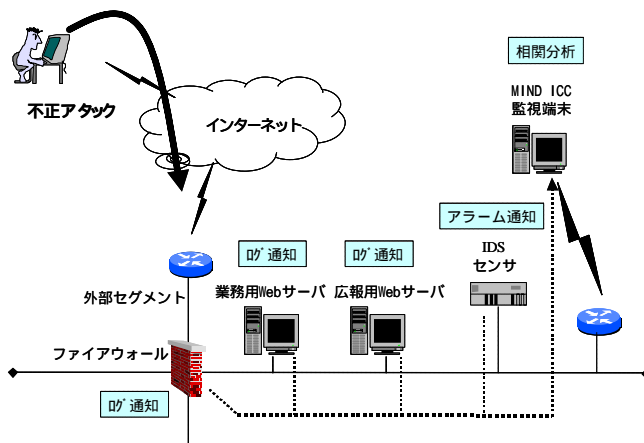


図 4 相関分析システムの構成

従来型の外部からネットワークレベルまでの擬似攻撃を行う診断に加え、Webアプリケーション専用のWebアプリケーション診断が増えている。Webアプリケーションが増えた一方、クロスサイト・スクリプティングなどの不正情報入手手段が既知になっており、アプリケーションレベルでのリスクが増大している。これらの脆弱性をツールだけでなく、ノウハウを持った専門家が診断を実践するサービスである。これにより自社システムのセキュリティレベル、リスクを対処とともに事前を知ることができる。

#### 4.4 セキュリティ教育サービス (e-Learning)

ネットワークセキュリティは一部の人の努力で実現できるものではなく、全員で築き、維持するものである。したがって、各社員の立場に対応したセキュリティ教育が必要である。セキュリティ教育サービス ISU ( Information Security University )は米国 Carnegie Mellon University との提携で生まれた Web システムを使用した教育システムで、利用者のスケジュールに合わせて受講することができる。その理解度のチェックのための修了試験も用意されている。

### 5. むすび

ネットワークセキュリティはますます重要になっていく。しかし、守る情報資産の重要度( 価値 )とかける費用とのバランスが重要である。今後も最新のセキュリティ技術を取り入れ、“安全”、“安心”を少しでも多く提供できるようにサービスの充実を図っていく。