グローバル・システム統合環境における情報セキュリティ管理の課題

法　雲　俊　邑

Ⅰ　はじめに

（1）情報セキュリティ管理の問題点

個人や組織を問わず、さまざまな情報がインターネットを通じて交換されるようになり、そのことが組織体の活動や社会生活に深く浸透することに伴って、情報セキュリティの確保は大変重要な問題となってきた。情報の交換が安全に行われ、情報システムが正常に機能することは、組織体が有効かつ効率的に事業活動を遂行するための前提条件となり、また安全な社会生活を支える基盤条件となるからである。

米国国防総省や各国政府のサイトにハッカーが進入したり、ネット通販企業や銀行から大量の個人情報が漏えいするニュースがしばしば報道されることを考えれば、国際社会においても情報セキュリティ確保の要請は緊急の課題となっている。(1)

このため、わが国にも情報セキュリティ管理基準が制定され、組織体が効果的な情報セキュリティの管理体制を構築し、適切なコントロールを整備、運用するための実践規範を示している。その中で、情報セキュリティ管理は、第一義的には、組織体における必要性と組織体の自己責任において果たされるべきものであることを訴えている。そして、その管理基準が制定された目的は、情報セキュリティ管理の基本的な枠組みと具体的な管理項目を規定することによって、組織体が情報セキュリティ管理体制の構築と、適切なコントロールの整

備・運用を効果的に導入できるように支援することであるとしている。

わが国の情報セキュリティ管理基準[2]は、情報セキュリティに係るマネジメントサイクル確立のための国際標準規格であるISO/IEC 17799:2000（JIS X 5080:2002）をもとにしており、情報資産を保護することや情報セキュリティ管理に関する、マネジメント及びコントロールの項目を規定したものになっている。

また、この管理基準と姉妹編をなす情報セキュリティ監査基準[2]は、それに従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。そして、本管理基準は、ISMS（情報セキュリティマネジメントシステム）適合性評価制度において用いられる適合性評価の尺度と整合するように配慮されたものになっており、組織体における情報システムの管理体制を問う場合、管理基準と監査基準は密接な関係をもっている。[3]

しかしながら、個人のレベルでは、期限切れになったウイルス対策ソフトを年々買い換えることは、ままならない状況である。企業においては、数え切れない台数のサーバや無数のゲートウェイに次々と出てくる新種のウイルスやハッカーに対応したソフトを導入することは容易ではない。

企業で言えば、資金に余裕があれば、取り敢えず対策ソフトを導入するが、以前のソフトとの整合性、メーカーの異なるサーバやゲートウェイとの整合性、無数にあるアプリケーションとの整合性、などは調べられていないのが実態であろう。異常があって原因を追究して初めてそのことに気づくのが本音である。

以下に、情報システムのぜい弱性と脅威の関係、情報システムへの攻撃と不正侵入の例を示してみよう。

（図表１）情報システムのぜい弱性と脅威の関係

ぜい弱性	脅威	攻撃対象
ウイルス対策の不備	ウイルス	サーバ
攻撃に対する対策不備	サーバテロ	サーバ、ソフトウェア全般
アクセスコントロールの不備	不正アクセス	サーバ

セキュリティ教育不足	情報漏えい・改ざん 操作ミス、違法コピー	ソフト・データ・文書の全般
通信データの非暗号化	漏えい・改ざん・消去	データ全般
バックアップ方法の不徹底	バックアップの不備	ソフトウェア、データ
パスワードへの対策不足	なりすまし	サーバ、ソフト全般
メンテナンス不足	システム破壊・故障	ハード・ソフト全般
保管への対策不足	各種の盗難	ハード・ソフト・資産全般

（図表 2）情報システムへの攻撃と不正侵入

攻　撃	内　容
盗聴	無線電波をモニタ、パケットの覗き見
DoS	高トラフィック攻撃によるサーバ機能の低下
DdoS	複数の箇所からの DoS 攻撃
バッファーオバーフロー	サーバ内の RAM メモリを超えるデータを送り管理者権限を搾取
ウイルス	不正プログラムが意図しない動作をする
ワーム	複数の不正アクセスによりサーバに不正侵入し脅威
スパム	本人が望まないメールを大量に送りつける
その他	パスワードなどの不正取得、Web アプリミスによる脅威

情報セキュリティ管理は、情報システムの運用にとって生命線とも言うべき重要性をもつものであるが、実態は前記のような事で、さまざまな理由によってその徹底が尽くし切れていないのが実態のようである。(4)

そこで、本稿では情報セキュリティ管理を、従来とは異なる視点から、合理的に行えるような次世代の ISMS の手法とソフトについて論及し、その解決方法を提示してみたい。

Ⅱ　グローバル・システムおける情報セキュリティの問題点

（1）サプライチェーン（SCM）思考の普及

世界経済のグローバル化、インターネットの普及による EC（電子商取引）市場の拡大、金融資本移動のダイナミック化、等々何を取り上げてもグローバ

ル化と迅速性を指向する社会になりつつある。このような中での、企業の行動は国境を越えた取引も多くなり、それに伴う情報システムも国境を越えたシステム統合が増加している。

そして、コンピュータをインターネットによって結合し、特に、資材や部品の受発注に複数の取引企業間の工場生産サイクルを同期化したタイムリーな取引を行うための、情報交換を行う傾向にある。このようなシステム環境を実現するために、前回の小稿では、「多企業間サプライチェーンにおける情報システム統合の課題」(5) と題して、グローバル化する情報システムの統合に関する課題の解決を論及した。

その要旨はつぎのようである。今日では SCM (Supply Chain Management; サプライチェーン管理) は、物流の供給連鎖のみならず、CAD/CAM 用のソフトやデータ入力の作業工程からも SCM 化への要求が出てくる環境にある。このようにサプライチェーン指向が普及して SCM アプリケーションが、多数の取引企業間でコンピュータネットワークによって結合されて稼働する。もちろんその中には海外の企業や工場も含まれている。

このような環境で問題になるのは、各社の SCM が多種多様なアプリケーションの機能を含んでいると考えられるが、これらをどのように統合するかである。(6)

一つは、多様なアプリケーションのデータベースを統合する方法である。SAP ジャパン社の提供するシステムのように、多種多様なアプリケーション・ソフトのデータベースを統合する機能によって、システムの統合化を実現できる方法である。(7) SAP ジャパン社の提供する SCM システムは、統合プラットフォームとして SAP Net Weaver というツールを利用することにより、さまざまなシステムのマスタを統合することができる。また、それが各種の業務と一貫性をもって統合できる機能がある。これは一種の SOA (Service Oriented Architecture: サービス指向アーキテクチャ) であると説明している。

SAP Net Weaver のような統合プラットフォームをもつシステムであれば、

複数企業がグループウェア方式でソフトウェアを開発する場合にも、容易にサプライチェーン化したSCMシステムで管理することが可能になる。

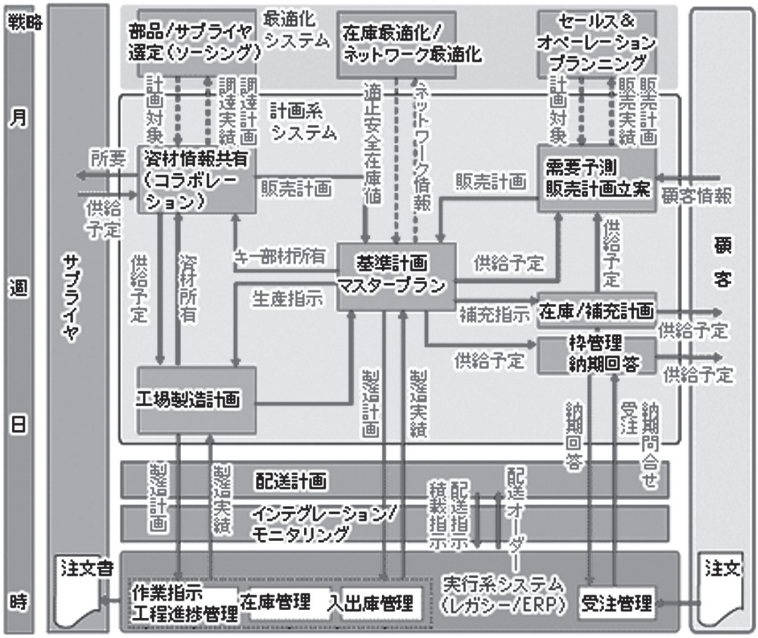
二つには、多種多様なアプリケーション機能をモジュール化してシステムを統合する方法である。i2テクノロジーズ社が提供するシステムのように、多種多様なアプリケーション機能をモジュール化し、システム全体の整合性を図る方法である。つまり、i2テクノロジーズ社のソリューションもERP、SCM、CRMといったモジュールの連携により、業務プロセスの自動化、最適化を進め、それぞれのデータを関連付けることでビジネスの「全体最適」が図れるような、モジュール追加型のシステム構成になっている。(8)

同社の製品はSCM関連ツールを多数用意しており、ユーザー企業の状況に応じて必要なモジュールを組み合わせて提供している。それは、サプライヤーと顧客の間に基準計画マスタープランを中心として、受注・納期管理、在庫管理、工場製造計画、配送計画等のモジュールが互いに連関して相互のデータを更新する構造になっており、サプライヤーから顧客までの過程をサプライチェーンとして連結している。以前は、SCMを製造業における生産活動の合理化という視点で考えてきたが、今日では、顧客や市場の要求の変化に追随して業務プロセスを最適化しようという、デマンド中心指向の考え方に重点を置くようになってきている。

両社の、多様なアプリケーションのデータベースを統合する方法と、多様なアプリケーションのシステムを統合する方法でのソリューションは、ERP、SCM、CRMといったシステムの連携により、業務プロセスの自動化、最適化を進め、それぞれのデータを関連付けることでビジネス全体の最適化を図るための重要なツールになる。このような思考から、先の小論では、多企業間のサプライチェーンにおける情報システム統合の課題について論及し、幾つかの解決ソリューションを提案した。

今日の新たなSCMは、従来の各種の周辺のサブシステムを吸収しているた

（図表３）i2 ソリューションのサポートするビジネスプロセス



出典：i2 テクノロジーズ社、キーマンズ　ネット資料
http://www.keyman.or.jp/3w/prd/91/30001591/?vos=nkeyadww10020747: 2006/02/06

め、受注管理のデータや需要予測のデータを多面的に生産計画に反映させることができ、生産から販売までのシステム化された体制を作るための機能に発展してきたといえるであろう。

しかしながら、このような状況の中で、SCM の情報システムを運用するには、さまざまな危険性があることは容易に予測できる。システムがウイルスやハッカーによって誤動作をしたり、誤データをアウトプットすれば企業経営への影響は大きい。つまり、そのセキュリティ管理ができなければ満足な SCM システムを運用することは不可能になる。また、多企業間の情報交換故に、その責任の所在も不明確になることも考えられる。

（2） グローバル・システムにおける情報セキュリティの問題点

前記では、将来に向けた次世代のグローバルなシステムの統合における問題点について述べて来た。ここでは、グローバル化するシステムを機能させる背景になるセキュリティ管理について検討してみよう。

一般的に、企業内にはさまざまな問題に対して、各種のセキュリティソリューションが導入されている。迷惑メールやハッカーなどの撃退に対応するには個々の問題ごとにそのソフトを導入しないと解決されないからである。しかしながら、ここで問題となるのは自社全体のシステムないしは、連鎖するグローバル化システムが、危険に犯されず正常に稼働しているかどうかをどのように把握するかである。(9)

企業の経営者や担当者、あるいはユーザーは、各種の危険に対応したセキュリティソリューションを導入したのだから、セキュリティレベルは必ず上がっているだろうと期待するのが普通である。しかしながらその実態は、セキュリティシステム任せで把握できないのが偽らざる事実であろう。毎日、各機器やアプリケーションから出される何千万、何十万件という膨大なログ情報から、セキュリティ管理に必要な情報をリアルタイムに抽出できる手間や時間はない。

この深刻な問題に対して悲鳴を上げた米国のユーザー企業が求めた解決方法は、超能力的な分析技術をもったシステム管理者を探すことではなかった。ソフトメーカーに要求したソリューションは、ネットワークに接続されるさまざまなデバイスのデータを、リアルタイムに統合管理するベースソフトであった。そこで開発されたのが SIM（Security Information Management）であり、文字どおりに訳すと「セキュリティ情報マネジメント」である。最近、各種のセキュリティソリューションの管理基盤として開発された SIM は、ネットワークの運用上の問題を解決し、セキュリティマネジメントという観点から重要な存在として認知されるようになり、急速に注目を集めるようになった。

セキュリティ情報を管理すると言うことは、コンピュータにインストール

すれば攻撃を防いでくれるファイアウォールや、IDS（Intrusion Detection System: 侵入検知システム）のように導入すれば、あらゆる攻撃を検知してくれると勘違いされるがそうではない。新しい分野の製品には、しばしば誤解した解釈がなされることがある。(10)

SIM という概念は米国ではすでに数年前から登場しており、今日では数百億円という大きなマーケットになっており、何百種類かの製品が市場で販売されている。しかし、残念ながら日本のセキュリティ管理を見渡すと、ほとんどの技術が米国製品で、日本企業はその販売店になるという後進国である。

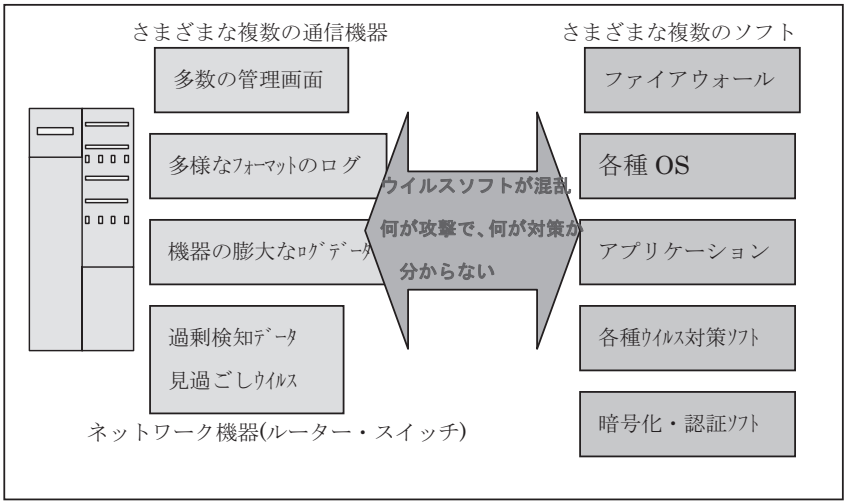
米国では、企業リスクとなる問題が出てくれば、次から次へと新たな対策ソリューションを開発し、提供してきた土壌がある。

このため、ファイアウォールや、IDS、IPS（Intrusion Prevention System: 侵入防止システム）といった侵入検知や防御を目的としたソリューションをはじめ、クライアント PC のセキュリティ対策としてウイルス対策ソフトやパッチマネジメントソリューション、そしてバイオメトリクスやセキュアトークンを利用した個人認証システムなど、さまざまなものが米国で登場し、日本に輸入されてきた。日本でも静脈認証やバイオメトリクス認証の技術は開発されているが、それをセキュリティソフトに組み込んだシステム製品にはなりにくい環境にある。

そして、多くの企業では、セキュリティ・トラブルが起こる度に、各種のソリューションの導入を進め、その防御に対応してきた。その結果、多くの異なる CPU アーキテクチャや無数の業務アプリケーションの中に、多数のセキュリティソフトが混在してインストールされる状況になった。この結果、企業のシステム管理者たちは、各メーカーが提供するセキュリティ管理画面の種類の多さと、その画面から出される警告メッセージ情報の膨大さに、混乱している。

SIM は先にも述べたように、複数の機器のログを集中的に管理する製品をさし、ネットワーク機器に残る大量のログ情報を整理・分析してセキュリティ

（図表４）セキュリティ管理のハードとソフトのクラッシュ



状態を一元的に管理するシステムである。2008 年 4 月に日本版 SOX 法が施行されたことにより、重要情報を扱うシステムのセキュリティに関するログは正確に管理しなければならない。このような理由から、最近の日本でも注目を集めるようになったのである。

III　次世代 SIM の情報セキュリティ管理

（1）　次世代 SIM の情報セキュリティ指向

ネットワーク機器は、セキュリティに関連するさまざまな情報をログとして残すが、外部の攻撃から守るための手がかりもこの情報に含まれている。しかしながら、実際には大量に残されたログ情報の中から役立つ情報を抽出して分析・活用するのは至難の業である。

ここでシステム管理者が、多くの異なる CPU アーキテクチャやネットワークを統合管理することが運用上、大変な困難を伴うものであると言う事情について説明しょう。システム管理者がなぜ苦慮するのかは担当者以外にはなかな

か理解されない。これを理解する手がかりは、その企業の方針として何をチェックするために、セキュリティ対策のアウトプットを要求しているのかを知ることである。

セキュリティへの意識が高く、多くのセキュリティ対策ソリューションを導入している企業では、セキュリティ状況を毎月報告することや、事件が起ったときにはすぐに詳細を報告することをルール化している。そして、たえず各デバイスが出すセキュリティの警告メッセージをチェックしているのである。

しかしながら、そのセキュリティの警告メッセージが、危険を知らせるメッセージとしてIDSから出された場合、

㋐　直ちにIDSの警告メッセージの意味を調べ、サーバのパッチレベルと通過データのスキャン結果を調査して実際にその通信が目的のサーバにどのようなトラブルを与えたか。

㋑　さらに、ファイアウォールのログを調査し、目的のサーバから危険な通信があったかどうかを調べるとともに、サーバのログに異常な形跡がないかなどを調査する。

システム管理の経験がある人なら理解できると思われるが、この調査には非常な労力と時間がかかる。それは何千万件も発生したログの中から必要なログだけを抽出して、事件に関連するログを一つひとつ調べるためである。IDSの警告メッセージ1件だけでもこれだけの作業が発生するのだから、IDSのアラームが月に何百件と発生すれば、どれだけ時間を費やしても足りない程である。徹夜作業でログを解析して、やっと、社内のシステムに不正侵入が見付かり、データが改ざんされたり盗まれていたことが分かっても、後の祭りになるような始末である。(11)

もちろん、システム管理者はこのような危険なログの発見だけではなく、システム上の不具合や基幹システムの運用もやらねばならない。このような難儀を極めるセキュリティ・チェックを容易にできるソフト製品として近年注目され、期待されるようになったのが近年のSIMである。

次に、SIM の主要な機能について検討してみよう。SIM の目的は、セキュリティ状態を一元的にリアルタイムで監視することと、事後的にセキュリティ状態を確認したり報告書等を作成することである。

SIM の一般的な機能は、事前に管理者が登録したネットワーク機器のログをリアルタイムに収集する方法である。ネットワークによって収集する管理の対象は異なるが、通常はファイアウォール、IDS、ルーター、レイヤー３スイッチ、サーバー OS、サーバー・アプリケーションなどが一般的である。

しかしながら、ネットワーク機器が異なればログへのアクセス方法やログのフォーマットはバラバラで、同じ内容の警告がソフトメーカーによって違う名前で呼ばれたりする。したがって SIM は、それぞれの機器に合わせた方法でログを収集し、そのフォーマットを統一する機能がなければならない。主要な機種については、ログの収集やフォーマット変換の方法があらかじめ登録してある。登録されていない機器は、ユーザーがアクセス方法とフォーマットの変換方法を SIM に設定すれば、収集情報として追加できるようになっている。

SIM は、前記のような形で収集したログをリアルタイムに画面上へソース情報として表示し、また、傾向を把握しやすくするためにグラフにして表示する。さらに、関連のある情報をまとめて表示したり、通信異常の発生頻度が急上昇したときに警告メッセージを出すなど、収集したログを分析する機能もある。このような処置によって管理者がトラブルの原因を追求するためにさまざまな画面を見比べる必要はなくなり、見落としも減る。

さらに SIM は、事後に分析したり報告書を作成する時に活用できるように、ログをデータベースに保存する機能ももっている。例えば、セキュリティ上の問題が発見された場合には、ネットワークに接続された各種の機器から検出されたデータに基づいて時間をさかのぼりながらトラブルを確認できる。SIM は統一したフォーマットでログを一元的にデータベースへ蓄積しているので、時間別・アクション別・機器別などのさまざまな切り口で分析できる。また、

月次の報告書を自動生成したり、トラブルに対応した報告データを整える機能もある。セキュリティの現状やトラブル発生時の報告書を作ることが多いセキュリティ担当者には便利な機能である。

上記のようにSIMは、セキュリティ管理者の監視や管理作業を軽減するさまざまな機能を備えており、中でもSIMの持つ分析機能によって、今まで解明できなかった問題も発見されることもある。

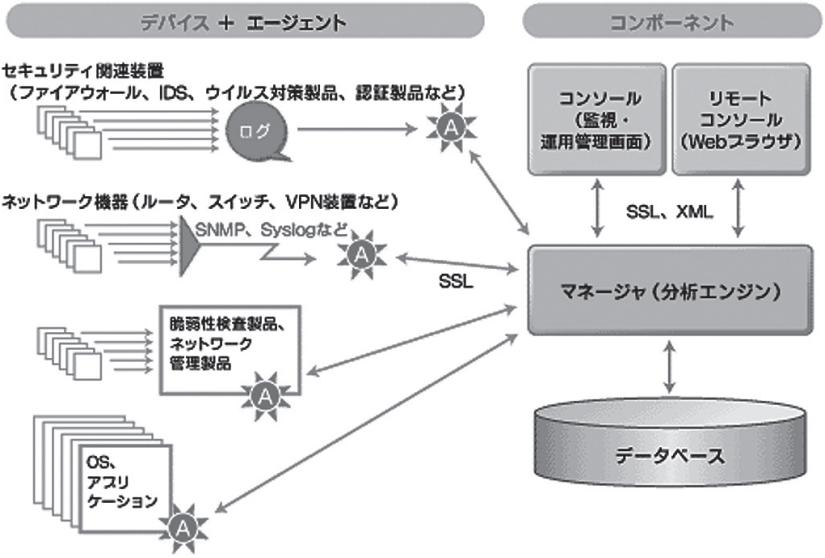
例えばネットワークに接続されたパソコンが、Webサイトからウイルスをダウンロードしたとする。そのウイルスはIDSやファイアウォールが設置されていても、セキュリティ・ホールを通り抜ける新種のウイルスの場合、容易には検出できずにダウンロードされてしまう。

しかしながら、IDSはそのパソコンが「プログラムやデータのようなものをダウンロードした」という情報を記録している。そしてそのパソコンから感染したウイルスが通信を仕掛ければ､ファイアウォールは「通信をブロックした」という情報を記録する。これらの一つひとつのバラバラの情報だけではウイルスに感染したことは判らない。

しかしながら、あるパソコンが「プログラムをダウンロードした」という情報と、そのパソコンの「通信をブロックした」という情報を関連付ければ、パソコンがウイルスに感染して新たな通信を開始しようとしている可能性が高いことがわかる。被害が拡大する前にウイルスの感染を検出できることになる。SIMは、このように複数の情報を関連付ける「相関分析」ができるようになっている。(12)

このような相関分析をするためには、SIMにあらかじめ情報を関連付けるためのルールを教えておく必要がある。SIMの製品は、頻繁に起こりそうな問題についてのルールを出荷時に組み込んでいる。これに加えて、ユーザー固有のネットワークに合わせてルールを変更・追加することも可能である。以上のような方向で、思考される次世代SIMの機能図が下記である。(13)

（図表５）次世代の SIM の機能図



出所：内田 千博、住商エレクトロニクス㈱
http://www.atmarkit.co.jp/fsecurity/special/71sim/sim03.html：2008/10/22

（２） 次世代 SIM の情報セキュリティ管理の機能

前項では、グローバル・システムを稼働するために必要なセキュリティ管理の困難さと、SIM のいくつかのツールを検討してきた。ここでは、グローバルなネットワークを管理するのに必要な次世代 SIM の機能について検討してみよう。

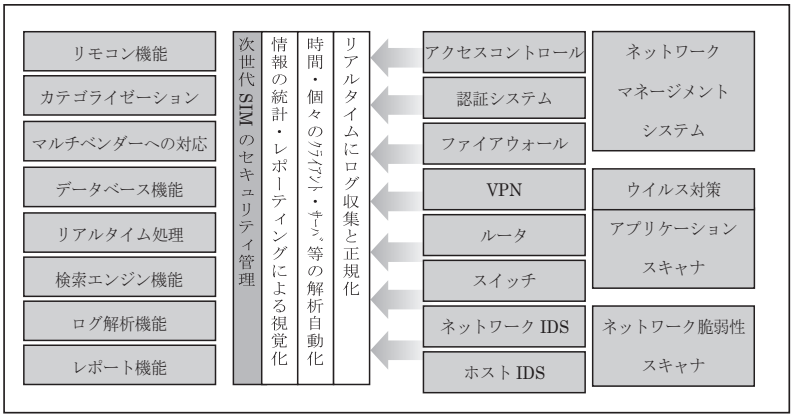
次世代 SIM について検討する前に、従来まで情報システムで対処してきた、攻撃に対するセキュリティ管理の例をまとめて示しておこう。

（図表６）攻撃に対するセキュリティ管理の例

機　能	対策例
抑止機能	セキュリティ・ポリシーの確立と実施の徹底 社内ネットワークの監視
防御機能	アクセス制御、ユーザー認証、パスワードの強化、 暗号化、ディジタル署名、暗号化、ファイアウォール
分析・予測機能	ぜい弱性格査の実施、ソフトウェアのバージョンの最新化 パッチの適用、定期保守の実施、不要アカウントの停止
不正侵入検知機能	不正アクセス侵入検知、稼働状況監視、ログ解析 ウィルスの常駐検査、監視カメラの設置
被害軽減機能	システムの自動切替え、セグメント化、サーバやルーターの二重化
応急処置機能	ログの出力と保存、バックアップデータの保存、ファイル修復対応 インシデント対応（コンティンジェンシプラン）
更新・復元機能	新しいセキュリティ技術の入手、セキュリティ監査の実施

前記の従来までの情報システムで対処してきた、攻撃に対するセキュリティ管理の例を次世代 SIM の機能に対応させた、セキュリティ管理のシステム機能は次のようになる。

（図表７）セキュリティ管理のシステム機能



多企業間のネットワークを運用していくために必要な情報セキュリティの主要なフレームワークの手掛かりが見えてきたと思う。

先にも述べたように、SIM を選定するうえで注意するべき点がある。それは、ベンダーやセキュリティアナリストによって SIM の生い立ちが異なり、コンセプトやその仕様・機能も SIM 製品によって異なるのである。どの製品が良くて最適かということは一概に判定できない。そこで、次世代の SIM と呼ばれる商品は、どのような機能を備えていることが望ましいかについて検討する。以下では、SIM に求められる基本機能を運用の問題点から整理してみよう。

㋐　コンソールとリモートコンソール機能

SIM の監視用インターフェイスとして必要な機能の一つは、システムの操作や管理設定、インターフェイスと関連機器の状態、一連の分析データの表示、統計情報の表示などを行うための機能である。必要に応じてデータベースに保存されているデータの表示などとともに、イベント分析や統計解析の設定や表示も行うと便利である。

また、オペレータが利用するコンソールとは別にリモート監視用のコンソールがあると、現場のオペレータが対応できないセキュリティイベントを責任者が他の場所や社内外からでもリモートで見ながら、アドバイスや簡単な操作を行う機能があれば、タイムリーなセキュリティ管理が可能になる。

㋑　ログフォーマットの統一化とカテゴライゼーション機能

セキュリティの警告を容易に調査するためには、種類の異なるデバイスから様々な形式で出力されるログを SNMP、syslog、SMTP、HTTP などのプロトコルを利用して統一フォーマットに直し（正規化して）、一括管理する必要がある。大きなセキュリティソフトであれば警告メッセージの種類が 2000 ～ 3000 種類あるといわれている。

そしてメッセージ警告は、同じ内容であってもソフトが異なると呼び名が変わり、システム管理者がこの多くの警告メッセージを覚えて対応することは不

可能に近い。このような状況にあることから、IDS から出る警告メッセージをソフトが異なっても共通して理解できるように、変換する必要がある。このようにすれば、多種類のデバイスから出力されるログの関連を調査することも時間が短縮できる。例えば、ファイアウォールと IDS のログから、同じ時間帯で同じ送信元アドレスの通信状況を調査するという作業も時間が短縮され、調査も容易になる。

これを可能にするのがカテゴライゼーションと呼ばれる機能で、SIM が備えるべき特長の一つであり、各種のデバイスの警告メッセージの意味を解釈して誰もが理解できるメッセージに変換する。したがって、社内に複数のソフトの IDS やファイアウォールが設置されていたとしても、この機能があれば、管理者は各種のセキュリティ機器から出される警告メッセージの意味を詳しく覚える必要がなくなる。

㋒　マルチベンダへの対応機能

さまざまなメーカーから出されている各種のセキュリティ機器商品は、エンハンスメント（機能強化／精度向上）を狙った製品を提供するものである。例えば、外部からの攻撃に対して、IDS やサーバのぜい弱性を検出してその精度を上げるものであったり、製品によってはファイアウォールに対して特定通信の遮断命令を自動化する機能をもつものもある。

これをサポートしているシステムは、自社製品のソフトに限定されるケースが多い。このため、システムが小規模な場合には、コンパクトで安価に導入して利用できる。しかしながら、サーバやクライアントの台数が数百・数千台にもなると、ネットワーク規模も大きくなり、小規模なセキュリティソフトでは防御できず、大規模な SIM を導入せざるを得ない。このような場合、マルチベンダに対応した機能をもつ SIM の導入が要求されることになる。

したがって SIM のコンセプトとなる、セキュリティの運用基盤として、デバイスの統合化やネットワーク・セキュリティに関するさまざまな事象に対応

できるような製品が要求されることになる。このように他ベンダー製品とのデータ互換が容易であるように設計されており、リアルタイム性や、高可用性、拡張性が広く求められる。このため、SIM システムは規模が大きくなり高価な製品も多くなるであろう。

㊓　データベースとエージェント機能

セキュリティ管理には、異常や危険を察知するために各デバイスのログデータの収集を行う。ファイアウォールの特定ポートでの異常トラフィック発生、ネットワーク機器の設定変更、業務時間外の重要サーバへのアクセス、緊急度の高いサーバなどはぜい弱性を持つがその数など、把握しておきたい情報も多い。それらの収集方法は、データベースに直接接続したり、前記したように収集したログの統一フォーマット化と意味の解釈（カテゴライゼーション）をし、SIM のデータとしてマネージャに送信する。

データベースでは、マネージャから送られるログの保存と、システム情報などの保存を行う。また、マネージャは、エージェントから送られるログをシステム内のデータベースへ蓄積する一方で、イベント分析、レポート生成、統計解析、トラブルチェック処理など、運用者が求める処理を行う。このような、エージェント（自律的に判断して処理を実行する）とデータベース機能が不可欠である。

㊔　リアルタイム処理

ネットワークの監視規模によっては、ネットワーク機器やセキュリティ機器から送出されるログが 1 日に何万〜数億件に及ぶが、これらをリアルタイムで処理するだけのパフォーマンスがシステムに要求される。つまり、リアルタイムに危険を予知したり、トラブルの発生もできるだけリアルタイムに検知できる必要がある。

セキュリティに関しては、侵入を未然に防いだり、トラブルが起こっても被害を最小に食い止めるような対処など、リアルタイム処理機能が要求される。

最近、フォレンジック（Forensic：法医学の意味だが、ここでは漏えいがあった場合に漏えい者の特定と証拠保全を支援する）システムという製品が出ているが、これはその名のとおりトラブルが発生した後に、データベースの分析をすることによって真相を突き止めるシステムである。

㋕ 原因解明の強力な検索エンジン機能

外部からシステムが何らかの攻撃を受けたと言うことを、セキュリティソフトだけで直接判断することは難しい。どのソフトもログを解析して何らかの事象を把握しその結果、危険の可能性があるという検知しかできない。そして、このような検知データを複数のソフトから収集して組み合わせることによってその信頼性が上がり、危険が断定できる。このように、セキュリティに関する事象は、複数の事象が発生したことを各種のデータを組み合わせて判断してトラブルがあったと確定できる。

しかしながら、各デバイス間で起こった事象の相関関係を分析できるような条件を SIM に初期設定で記述するのは複雑な条件式になる。したがって SIM はこのような条件式の表現をユーザーが簡単に記述できるような機能と、検知データを高速にデータベースから検索できてログ解析できるような機能を備えたエンジンが求められる。

㋖ ログの解析ツール機能

セキュリティの監視・管理とは、「異常を見つける」ことが最も重要な機能である。単なる文字の羅列である大量のログをビジュアル化することによって、個々の事象のみならずネットワーク全体の異常が検知しやすくなる。さまざまな統計関数を使って、いろいろな角度からログを解析し、ビジュアル化して観察できるようになる。その結果、ネットワーク全体のセキュリティ事象の動向が把握でき、トラブルの早期発見につながる。

最近の SIM 機能の一部には、多種類のログフォーマットに対応したログ収集機能とログ解析ツール機能、それをレポート化する機能などの部分的機能を

持つ製品が出てきている。しかしながら、ログ解析ツールはファイアウォールやルーターなどのアクセス解析、サーバなどのイベント解析といった「特定」の用途に限定して設計された製品が主流である。

しかしながら現状では、SIM が得意とするデバイス間の相関分析（Cross correlation）やリアルタイム性に欠ける製品が多いためネットワーク全体の統合管理は難しい。このため、非常に高度な解析機能および視覚的なレポートが作成可能な機能を用意すれば、特定の用途で用いるのにも有用なツールになる。

以上の７点が、SIM に求められる最低限の機能である。

現状の SIM は、それぞれの製品が作られた目的や経緯が異なるため、種類も多く機能もバラバラなものが多い。これらを採用するのであれば、自社のセキュリティ管理方針にどれが合致するかをしっかり把握したうえで、ユーザーのニーズに合う製品を選択していく必要がある。

しかしながら、次世代の SIM 製品は、少なくても最低限で前記したような７点の機能を備えた SIM が求められ、また、そのような方向で充実した製品が出回るようになることを期待したい。

Ⅳ　グローバル・ネットワークの次世代 SIM セキュリティ管理の課題

以上では、今後の企業経営の中で、多企業間や多国間の取引がさらに多くなることを考えて、そのような取引の中で一つの企業の垣根を越え多国籍間で、サプライチエーンの情報ネットワークが多く構築されるであろうことを想定し、そのセキュリティ管理のあり方と SIM 製品がどのような機能をもつべきかを検討してきた。

単なるウエーブレベルではなく、基幹業務を企業と企業の間でネットワーク接続する、また、多国間をまたいで基幹業務のネットワークを接続することは、社内の情報を社外にさらけ出すことに等しい。このような環境の中で、秩序ある情報ネットワーク接続と情報交換を期待するには、第三者的な攻撃をいかに

防御するかが重要な問題になる。

このような場面でセキュリティの管理とトラブルの解決を図るのが、SIM製品である。したがって、そのSIMにどのような機能が必要かについて詳しく述べてきた。ここでは最後に、企業でSIMがどのように利用されるべきかについて述べておこう。

セキュリティ管理にSIMを導入し、業務処理やウエーブ処理を満足に運用していくには、トラブルの予兆を早期に発見して、処理業務に支障をきたさずに解決することが最良の方法である。

しかしながら、そのように解決しない場合は、ログフォーマットの統一化とカテゴライゼーション機能によってSIMデータベースに蓄積されたデータを用いて、原因解明を図る。この場合どのような症状かをSIMコマンドで条件設定し、強力な検索エンジン機能によって関係するデータを抽出するとともに、SIMが原因解明を図ってくれる。

原因の解明に有力な力を発揮するのがログの解析ツール機能である。時間軸を中心にした解析や特定のサーバやクライアントを中心にした解析、あるいは、入退室管理システムの記録などの物理的セキュリティデータを総合的に関連付けて原因の解明を図ることがSIM性能の良否を左右することになる。いずれにしても、トラブル発生時の円滑な調査が重要である。

SIMは情報ネットワーク・セキュリティだけに使われると言う事だけではなく、物理セキュリティ（入退室管理システムの記録など）との融合によるデータ分析もセキュリティ管理の精度を向上させる。例えば、今年４月に三菱東京UFJ銀行であった事件のように、元行員のＡという人が、事前に知り得たＢさんのIDを使ってリモート接続をした（VPN装置のログ記録に残る）場合、これらのデータを照合すれば「なりすまし」行為が検出できる。

また、近年、今注目されているのはRFIDタグを利用するためのミドルウエアである。一昨年のUHF帯の利用解禁で急激な普及が見込まれているRFID（電

子タグ、RFID タグ）の利用により、より高度な SCM を構築することが可能になってきた。RFID を SCM の一部として利用することにより、これまでとは段違いの効率化を実現できる可能性がある。

このような事を考慮すると RFID からの発信データは、SCM のデータとしてのみならず、セキュリティのデータとしても取り込んで関連付ければその管理の精度を飛躍的に向上させることができる。要はさまざまな工夫によって、セキュリティ管理の向上を図る組み合わせも考えることができる。

いずれにしても、次世代 SIM はトラブルの予兆を早期に発見して、処理業務に支障をきたさないように情報システムを守るとともに、そのセキュリティの報告書を作成する機能まで備える必要がある。

また、コンプライアンス管理の一環として、米国では SOX 法（Sarbanes-Oxley Act）という法律が施行され、各社がその実施に苦慮している。この法律は、企業会計や財務報告の透明性・正確性を高めることを目的に作られたものである。財務諸表などを提出する際に、会計システムを含め企業の情報システムに不正なアクセスがあったか否か（データが改ざんされた可能性があるかどうか）を証明しなくてはならない。

重要な情報が入ったサーバや、社内認証システムなどに不審なアクセスがなかったことを、SIM の報告書を用いてレポートしている企業が最近増えている。日本も金融庁が中心となって 2008 年 4 月に日本版 SOX 法が施行された。これによって重要情報を扱うシステムのセキュリティに関するログをきちんと管理しなければならなくなる。そのため、SIM 製品が最近注目を集めている。今後、日本も各企業が厳密なセキュリティ対策を講じていく必要が生じるのは間違いない。

以上で、グローバル化するサプライチエーンの情報ネットワークの普及と安全な運用を前提にして、次世代の「SIM はどのような機能をもつべきか」をテーマに、基本的な方向性を示唆してきた。今後これらのシステムが発展する

うえにおいて、避けられない問題であり、本稿で提起した問題解決と方向をいかに次世代 SIM として製品化するかが大きな課題であり、その実現をメーカーに期待したい。

参考文献

（1）IPA 独立行政法人情報処理推進機構、『情報セキュリティ白書 2009 年』、毎日コミュニケーションズ、2009 年 5 月。

（2） 経済産業省､情報セキュリティ管理基準､(平成 15 年経済産業省告示) を発表したが、http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01.pdf#search=' 情報セキュリティ管理基準 ' : 2009/4/12、経済産業省は、この「情報セキュリティ管理基準」を、ISO/IEC における国際規格化の動きを受け、平成 20 年 7 月 2 日に改正案を発表した。

http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard.pdf : 2009/4/12

（3）また、この（2）の動きに伴って、情報セキュリティ監査基準も、改正案が検討されている。

http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf : 2009/4/12

（4）『情報セキュリティ白書 2009 年』前掲書。法雲俊邑著､『企業情報システム』杉山書店、1995 年　など。

（5）法雲俊邑稿、「多企業間サプライチェーンにおける情報システム統合の課題」、星城大学「研究紀要」第 7 号、平成 21 年 3 月。

（6）法雲俊邑著、『経営工学』オーム出版社、2003 年。

（7） 資料出典：SAP ジャパン社、「SAP NetWeaver のコンポーネントとツール」

http://www.sap.com/japan/platform/netweaver/components/controller/index.epx : 2008/11/10

（８） 出所　キーマンズ　ネット
http://www.keyman.or.jp/3w/prd/91/30001591/?vos=nkeyadww10020747：2006/02/06
（９） http://www.keyman.or.jp/3w/prd/27/10012127/：2006/02/06
(10) 内田 千博、住商エレクトロニクス（株）「SIM で企業のセキュリティを統合管理せよ」@IT アイマーク・アイテイ。
http://www.atmarkit.co.jp/fsecurity/special/71sim/sim03.html：2008/10/22
(11) 同上
(12) 日経 NETWORK、Network キーワード :Itpro、SIM とは。
http://itpro.nikkeibp.co.jp/article/Keyword/20070619/275118/：2009/4/20
(13) 内田 千博、前掲稿。

本稿は星城大学高度ネットワーク社会研究所の研究費助成を受けた、研究の成果である。