

# SIEM 基盤構築に威力を発揮する IBM Tivoli Security Operations Manager (TSOM)

新しいセキュリティ領域として注目を集めるSIEM(Security Information and Event Management)を実現するソフトウェアプラットフォーム「TSOM」が日本IBMよりリリースされた。本稿では、SOCの効率化とコンプライアンス・日本版SOX法対応に有効なTSOMの概要を紹介する。

## ますます重要性が高まる SOC(Security Operation Center)

コンプライアンス（法令遵守）やセキュリティに対する社会的要請、さらには金融商品取引法（日本版SOX法）を踏まえ内部統制強化に向けたセキュリティ基盤強化が求められるなか、安心・安全なICT（Information & Communication Technology）環境の実現が不可欠となっている。

このようななか、企業ネットワークのトラブルは、従来のようなハードウェア障害から、セキュリティに起因する割合が急増している。

日本IBM(株)Netcool営業部の明永康範部長は、「ICT環境は、企業の重要な経営インフラです。企業ネットワークのセキュリティが脅かされている昨今、ネットワーク接続機器の稼働監視や性能監視などを行うNOC（Network Operation Center）、さらにはファイアウォール・不正侵入検知/防御装置（IDS/IPS）の監視やウイルス監視を行い、ログを収集して脅威を分析し、いち早く適切な対策を促すSOC（Security Operation Center）の重要性が急速に高まっています。また、コンプライアンスや日本版SOX法の観点からも、障害

対応のみならずセキュリティ運用を請け負うSOCは極めて重要です。」としたうえで、「しかし現状のSOCの多くは、様々な問題に対して、各々セキュリティソリューションが導入されており、一元化されていないセキュリティ管理システムとなっています。このため、構成するセキュリティ機器や対象サーバが多くなり、各機器やアプリケーションから出される異なるログフォーマット、膨大なログ情報、個々の機器から発生するお互いに独立したイベント検知情報など、なにが本当の問題なのか、なにが本当の攻撃なのかの解析に要する稼働と、センタの管理コストが増大するという大きな課題を抱えています。」と指摘している。

つまり、SOCの重要性が増大する一方で、常時監視、膨大なログ情報の収集・分析を行い、侵入攻撃やサービス不能攻撃等をはじめとするセキュリティ上の脅威に対して迅速な対応を促すSOCの運用上の課題がクローズアップされてきているのだ。

## 注目を集めるSIEM(Security Information and Event Management)

SOCの重要性が高まるなか、上述の問題を解決することが喫緊の課題となっている。このような一元化



日本IBM(株)  
ソフトウェア事業  
Tivoli事業部  
Netcool営業部長  
明永 康範氏

されていないセキュリティ管理システムに起因するSOCが抱える課題を解決するセキュリティ監視・管理の基盤システムとして注目を集めているのがSIEM（Security Information and Event Management；セキュリティ情報管理）ソリューションだ。

米Gartnerは、SIEMとは「SIM」と「SEM」の2つの機能を持つものと定義している。SIM（Security Information Management）は、複数のホストシステムやアプリケーション群及び、セキュリティ機器からのログデータを解析し、セキュリティポリシーとコンプライアンスを支援するレポートを提供するソリューションである。ITセキュリティ、内部監査及びコンプライアンスの活動を支援するために使用される。

これに対しSEM（Security Event Management）は、セキュリティインシデント（事故）への対応を改善するために使用される。セ

セキュリティ機器やネットワーク機器、各サーバシステムからほぼリアルタイムにログデータを収集・処理してセキュリティ・オペレーションのイベント管理を支援する。SEMは、セキュリティ・オペレータに社内外のセキュリティ脅威に対するリアルタイムな検知

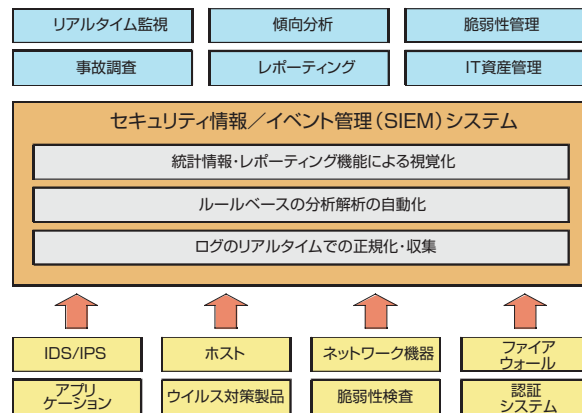


図1 セキュリティ監視・管理の基盤システムとしてのSIEM

機能を提供するソリューションだ。

SIMとSEMの2つの機能を備えたSIEMは、図1に示すようにセキュリティ監視・管理の基盤システムとして最適なソリューションであり、SOCの効率化を促進するだけでなく、コンプライアンス・内部統制強化の観点からも注目を集めている。特に日本版SOX法対策で不可欠なIT全般統制の情報セキュリティ基盤の支援に効果を発揮するソリューションとして注目されている。

SIEMの最大の価値は、オープンであることにある。つまり、マルチベンダー対応の統合的なログの収集・管理・分析機能と膨大なデータを処理する高速性によって、日々の管理業務の中で脅威の有無を明確にし、結果をレポート出力して分かりやすく示すことにある。新しい脅威への対応を含め、膨大かつ多様なログがますます増加し続ける傾向にあることから、SIEMの重要性がより一層高まることが予想される。

以下に、SIEMの活用法を示す。

### ①セキュリティ事故・事件の予兆を発見する

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、緊急度の高い脆弱性を持つサーバ数など、必要な情報がリアルタイムに視覚化できるコンソールで、迅速なセキュリティ事故・事件の予兆を発見する。

### ②セキュリティ事故・事件発生時の円滑な調査

事故・事件発生後の調査の際、ログが散在しては対応が困難である。各種セキュリティ機器のログを統一フォーマットに一元管理できるSIMは、ログを縦断的かつ高速に調査が可能となる。事故・事件発生時の対策としても、有効なソリューションである。

### ③コンプライアンス管理

日本版SOX法により財務諸表などを提出する際に、会計システムを含め企業情報システムに不正なアクセス（データ改ざん）があったかどうかを証明するために、証拠を記録／保管しておき、外部監査へのエビデンスとして提出することが求められている。特に、重要な情報のあ



日本IBM(株)  
ソフトウェア開発  
研究所 システムズ  
マネジメントテクノロジ  
スタッフS/Wエンジニア  
本橋 貴司氏

る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かどうかSIEMを利用してレポートする。

## SIEMを実現するIBM TSOM (Tivoli Security Operations Manager)

日本IBMは、本年1月、セキュリティ監視・管理の基盤システムとして注目を集めるSIEMをカバーするソフトウェア製品「IBM Tivoli Security Operations Manager v3.1」(以下、TSOM v3.1)をリリースした。

「TSOM v3.1は、高度なSIEMを実現するソフトウェアプラットフォームで、オープンであることと、スケーラビリティに優れていることが最大の特長です。ローカライズを行った日本版もリリースする予定ですが、私どもではTSOM v3.1を、障害対応を中心としたネットワーク運用を行うNOCとともに、セキュリティ運用を請け負うSOCの運用の効率化を劇的に向上させる製品として、また日本版SOX法で求められる内部統制強化を支援する製品として、積極的な販売活動を展開していきたいと考えています。」(日本IBM(株) ソフトウェア開発研究所 本橋貴司氏)

TSOMは、SIEMを実現するソリ

SIEM 基盤構築に威力を発揮する IBM Tivoli Security Operations Manager (TSOM)



図2 高度なSIEMを実現するTSOM

ユーシオンとしてすでに米国では多くの導入実績を持つ。TSOMはSIEMに求められる下記の5つの機能要素をすべて有している。

- ① 様々なタイプの複数の機器からログ情報を収集可能である。
- ② 収集したログ情報を保管することが可能である。
- ③ 保管したログ情報からレポート作成が可能である。
- ④ ほぼリアルタイムで相関分析が可能である。
- ⑤ 様々なアクションを結びつけることが可能である。

このようにTSOMは企業のセキュリティ運用の効率と可視性を向上させる、高度なSIEMを実現するソフトウェアプラットフォームとして、全社的なポリシー管理、インシデント管理、リスク緩和機能を一元化し(図2)、以下のサービスを提供する。

- ・ 各種監視対象機器のログをセキュリティ情報イベントとして収集・集約し、標準化し、保存し、レポートを生成

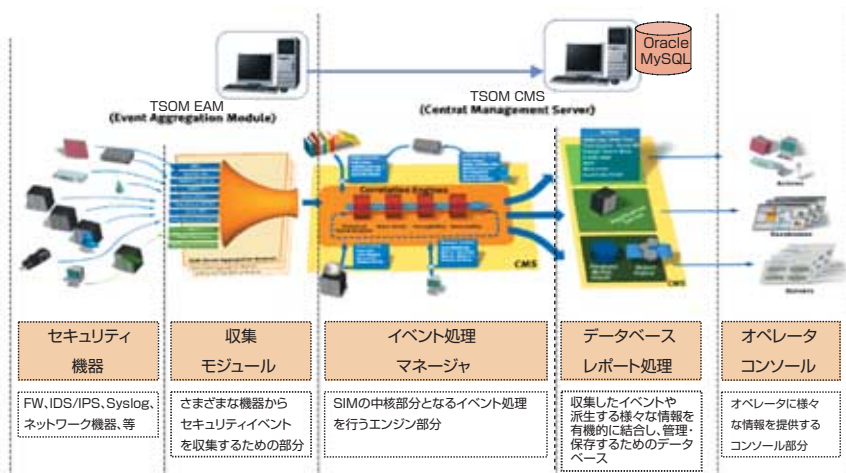


図3 TSOMアーキテクチャ

- ・ セキュリティ情報の相関技術により、包括的なインシデントの認識と管理
- ・ プロアクティブなポリシーの監視と実施
- ・ 様々な規制に対応したレポートテンプレートの提供 (Sarbanes Oxley (US)、GLBA、Privacy等)
- ・ 統合監視システムとの連携

● TSOMアーキテクチャ

図3にTSOMアーキテクチャを示すが、モジュール単位として、EAM (Event Aggregation Module) 及びCMS (Central Management Server) に分けることができ、SIEMに求められる5つの機能要素を効率的・効果的に実現できるようになっている。以下、EAM及びCMSの概要を紹介する。

(1) TSOM EAM

EAMは、様々なベンダーの様々なタイプのセキュリティ機器、OSのシステムログ (Syslog等)、ミドルウェア、アプリケーションからロ

グを収集し、後述するCMSに送信する役割を担っている。EAMでは、マルチベンダー環境下におけるログ収集及び活用を行うために、

- ・ ログフォーマット統一
- ・ ログ内の各行に対するセキュリティ上の意味づけの実施

の2つの機能を実現している。

EAMでは、これら2つの作業を行うために、機器、タイプ、バージョンごとに非常に多くのイベントソースのルールファイルを標準装備している。「TSOMのデバイスサポートリストに入っているセキュリティ機器、OS、ミドルウェア等であれば、EAMをインストールするだけでほぼ自動的にログ情報が収集可能になります。」(本橋貴司氏)

また、EAMの大きな特徴としては、エージェントレス (監視対象機器に特別なプログラム等の仕組みを動作させる必要がない) で取得可能なログについては、できるかぎりエージェントレスで対応しようというポリシーで作られているという点

だ。しかし、例えば Windows System Log 等、エージェントレスで取得できないログに関しては、UCM (Universal Collection Module) と呼ばれるエージェントを対象機器にインストールすることで対応している。

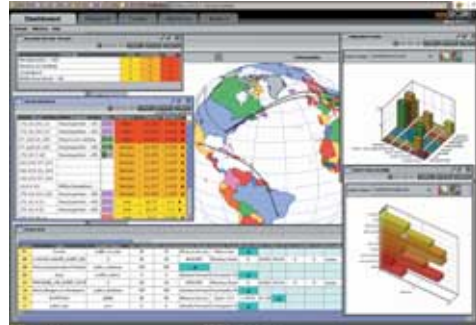


図4 TSOMダッシュボード(例)



図5 TSOMレポートの例

EAMは1台のCMSに対して複数台設置することが可能あり、12台のEAMが各拠点に配備された事例もある。

## (2) TSOM CMS

CMSは、EAMから送信される膨大なログ情報をセキュリティ・イベントとして受信し、リアルタイムでイベント相関分析を行う。また、その結果をストレージ (v3.1ではMySQL、Oracleに対応) に保管するのみならず、各種アクション (e-mailやアラート、スクリプトの起動など) に結びつけたり、ダッシュボード (図4) にリアルタイムで表示したり、保管されたイベントを利用してレポート (図5) を作成することも可能だ。

### ● TSOMの主な特長

以下にTSOMの主な特長を整理して示す。

- ・今日の分散環境のサポートを容易にするスケーラブルなモジュールアーキテクチャ
- ・導入と保守を容易にするイベント集約のためのエージェントレスなアプローチ
- ・統計相関、ルールベース相関、感

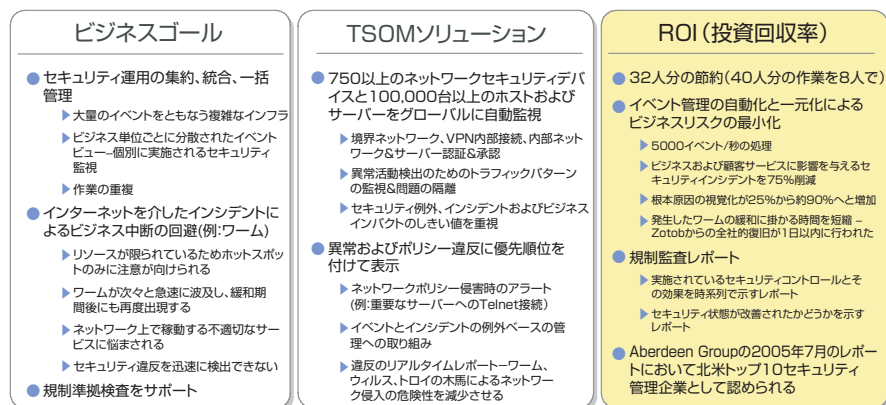


図6 米テレコム企業におけるTSOM導入例

受性相関、脆弱性相関という相互に補完的な4つの相関エンジンを有し、これを使用したリアルタイムのセキュリティ相関情報の分析が可能

- ・高速データ処理を可能にするアーキテクチャ
- ・インテリジェントなインシデント管理ワークフロー
- ・ポリシー及び法規制遵守の自動化
- ・柔軟なデータ解釈を可能にするPowerGrid等の、統合された調査ツール及び機能
- ・セキュリティデバイス、ネットワークデバイス、ホスト、アプリケーションを含むITインフラ全体をカバーするデバイスサポート

## 米テレコム企業での導入例

以上、SIEMを実現するTSOMについて紹介したが、最後に米テレコム企業におけるTSOM導入事例を図6に示す。この企業は、12台のEAMを各拠点に配備し、750以上のネットワークセキュリティデバイスと10万台以上のホスト及びサーバーを監視し、秒間5,000イベントの処理を実現している。

### お問い合わせ先

日本アイ・ビー・エム(株)  
ソフトウェア事業

Tivoli事業部 Netcool営業部

E-mail: netcool@jp.ibm.com

http://www.ibm.com/jp/software/tivoli/