

システム(=ビジネス)を守る統合セキュリティ情報管理ツール 「eTrust Security Command Center」

2月号と4月号で、EIM（エンタープライズ・ITマネジメント）コンセプトに基づくCAの製品戦略と、IT資産に関わるあらゆる情報を統合的に可視化するインテリジェントな分析ツール「Unicenter Asset Intelligence」について紹介した。本連載を締めくくる今回は、企業の重要インフラであるITシステムを守るための包括的セキュリティ・マネジメント・ソリューション群「eTrust」のうち、セキュリティ情報を統合管理する「eTrust Security Command Center (SCC)」を紹介する。eTrust SCCにより、セキュリティイベントを優先度や関連性により絞り込み、重要な情報を見逃さない統合管理機能と対策の自動化により、ビジネスリスクの低減が可能だ。

企業リスクを守るための包括的なセキュリティ・ マネジメント・ソフトウェア「eTrust」

今やITシステムは企業や社会の重要インフラとなっている。ITシステムをセキュリティ・リスクから守ることは、ビジネスを守ることと等価である。ITシステムを守る（ビジネスを守る）ためには、ウイルスや不正侵入のブロック、会社の機密情報流出防止や個人情報保護といった個別のセキュリティ対策を含めた総合的なマネジメントが必要だ。

コンピュータ・アソシエイツ（CA）は、システムを守るための包括的セキュリティ・マネジメント・ソリューション群「eTrust」を提供している。

- ・ eTrustは、
- ・ ウイルスやDos攻撃など外的脅威を防御・管理する「eTrust Threat Management」
- ・ 情報を取り扱うユーザーの特定やサーバへのアクセス制御、ルールを管理する「eTrust Identity and Access Management (IAM)」
- ・ 様々なシステムやアプリケーションから収集した大量のセキュリティ情報を可視化し、適切な判断を迅速に行えるようにする「eTrust Security Information Management (SIM)」

の3つのソリューショングループで構成されている。eTrustはEIM構想の重要なコンポーネントの1つであり、EIMの中核をなすMDBを介して他のコンポーネントとシームレスな統合が可能となっている。EIMでは、ITIL（ITインフラストラクチャー・ライブラリ）でいう3つのPである技術・人・プロセスに加え、セキュリティのプロセスを含めたシステムのマネジメントを実現可能にしている。以下では、eTrust SIMソリューションを中心に紹介する。

セキュリティ情報を集中管理する 「eTrust SIM」ソリューション

本年4月から個人情報保護法が本格施行された。コンプライアンスやビジネスコンティニュイティを維持するためには、現在のようにネットワーク化された複雑な企業環境において、これまでのようなインシデントごとの継ぎ接ぎのセキュリティ対策ではなく、外的・内的脅威を含め包括的に行き届いたセキュリティ対策が不可欠だ。

CAのプロダクトマーケティング部プロダクトマーケティングマネージャーの金子以澄氏はこの理由について、「企業の多くは、アンチウイ

ルス、ファイアウォール、IDS、アクセス制御、情報漏洩といった様々な脅威に対し、ポイントソリューション製品を必要の都度導入してきました。しかし、的確にITシステム全体を管理する視点で見た場合、OSやネットワーク機器を含め、企業内に存在する様々なセキュリティイベントを一元的に管理するとともに、その膨大な情報から関連性や重要度などで優先付けし、問題の根本原因を特定することが重要になります。これらを自動的に行い管理負荷を軽減するとともに、重要なメッセージが膨大なメッセージに埋もれることなく漏れなく対策することが可能になるのです。」と語る。

CAのeTrust SIMソリューションは、様々なセキュリティ・メッセージを統合管理することにより、ITシステム全体のセキュリティを確保するセキュリティ情報の集中管理ソリューションだ。様々なデータの一元化と処理の自動化によって、セキュリティマネジメントの効率化と迅速な問題解決を可能にしている。

セキュリティ情報を統合管理する eTrust Security Command Center

eTrust SIMソリューションの中

核となる製品が、「eTrust Security Command Center (SCC)」である。eTrust SCCは、その名称のとおりセキュリティ監視センターとして、アイデンティティ管理、アクセス管理、スレット(外的脅威)管理といった3つの主要セキュリティ分野を一元管理する製品だ。eTrust SCCにより、企業の全セキュリティ機能の統合、ポータル形式の管理、ビジュアル化が可能になる。eTrust SCCは、昨年開催されたアテネオリンピックのIT管理を担当したアトスオリジン社が採用し、ネットワークへの不正侵入や他のセキュリティ侵害を防止するとともに、競技者や報道機関には安全な環境を提供する統合的なセキュリティ管理に活用された。

eTrust SCCの最大の特長は、CAのeTrustソリューション群はもちろんだ、アンチウイルス、IDS、ファイアウォール、ネットワーク・アプリケーションなど分散しているサードパーティのセキュリティツールや、異なるOSのメッセージ、データベースの監査ログをシームレスに統合管理することができるという点だ。

「あらゆる情報を一元管理するためSDKを使用し追加することも可能な柔軟性を持ち、さらに米国本社ではご要求の多い約130弱の製品に対応するエージェントを提供しています。」(金子以澄氏)ただし、日本市場での製品出荷時には、各ベンダー製品のローカライズされたメッセージの構文解析が必要であり、ご要望により逐次対応していくという。

eTrust SCCは、セキュリティの

イベントメッセージを分析する機能を装備している。メッセージの構文を分解して解析する機能だ。例えば、「ログイン失敗」というイベントが発生した場合、その原因を究明するためにネットワークの経路上の様々なセキュリティツールから上がってくるメッセージをすべて分析し、関連するものを時系列で追っていく。これにより、許可されたコンピュータから単純にパスワードを間違えたために発生したメッセージか、ネットワークを経由して不正にアクセスしてきたのかを判別することを可能にしている。つまり何千、何万というメッセージの中から、本当に緊急で対応しなくてはならないものを見つけ出し、ユーザーに対して対応の優先度を示す機能を提供している。

メッセージの抽出ルールは、スクリプトのような形で記載する必要があるが、CAではeTrust SCCがサポートするツールに関するスクリプトの雛形をWeb上で公開している。また今後は、eTrust SCCにプロセスルールを定義するツール「CleverPath Aion」を組み込む計画もある。これにより、セキュリティツールだけではなく、ユーザーが内製したアプリケーションも含めて、容易にルールを知識ベースとして蓄積することができるので、さらに柔軟に効率的で迅速な対応が可能になる。

セキュリティとシステムの監査情報を 統合管理するeTrust Audit

eTrust SCCと同様、eTrust SIMソリューションの中核製品として、

「eTrust Audit」がある。これは、セキュリティとシステムの監査情報を収集、統合管理するための製品で、eTrust SCCのコンポーネントの一つである。

eTrust Auditは、企業におけるマルチプラットフォームシステム全体から監査情報を収集し、eTrustソリューションをはじめ、様々なサードパーティのセキュリティ製品から収集したイベントデータと統合する。これらの監査情報は、データベースに保管され、eTrust SCCによって影響の関連付けと、ビジネス資産及び情報リソースに対する脆弱性の評価が行われ、対応の優先順位が決められるという仕組みだ。eTrust Auditは、

- ・リアルタイムな監視と情報の収集
- ・柔軟なフィルタリングによるアクションと警告
- ・豊富なグラフ作成の可能なレポート
- ・操作性の高いGUIによる直感的な管理

といった機能を持っている。eTrust Auditは、詳細なアクセスログ、例えばどのリソースに、誰が、どういう端末から、どのプログラムを用い、いつアクセスしたかなどを収集するため、万一不正アクセスが発生した場合でも、アクセスした人物や経路の特定を可能にしている。

●お問い合わせ先●

コンピュータ・アソシエイツ(株)
CAジャパン・ダイレクト
TEL : 0120-702-600
JapanDirect@ca.com
<http://www.caj.co.jp>