4G－5

ネットワークセキュリティにおける運用管理の実現方法

妹尾 徹† 高山 聡一郎†

†(株)日立製作所ソフトウェア事業部

1. はじめに

企業の基幹システムにおいては、ジョブ管理、ネットワーク管理、アプリケーション管理、サービス管理などの様々な運用管理が必要となっている。また e-ビジネスの加速度的な拡大に伴い、ネットワークからの侵入によるWebページの不正書き換えや、機密情報、個人情報の漏洩などの脅威も増大しつつある。

これらの脅威に対抗するため、従来の情報システムに対する運用管理に加え、セキュリティを考慮することが必要となってきている。その際、例えばユーザ情報の管理やイベント監視など、他システムとの整合性を保った形で、統合的にセキュリティ管理を行うことが求められている。

本稿では、ネットワークからの侵入や、企業内の機密情報にへの不正アクセスなどに対抗するセキュリティ管理と、従来からの運用管理との統合について報告する。

2. 不正侵入防止システム

ネットワークからの不正アクセスを防止する一般的な手段は、ファイアウォールを利用して、アクセスを制限することである。しかしながら、近年、不正アクセスの手法は多様化しており、ファイアウォールをすり抜けて企業内ネットワークに侵入する例も報告されている。また、企業内には、複数のファイアウォールが設置されることが一般的であり、これら複数のファイアウォールに対してセキュリティポリシーに基づき適切な設定を行う必要がある。

不正アクセス防止基盤システム[1].[2],[3] は、不正アクセスの検知および対策を行うエージェントと、検知ー対策ルールを管理するマネージャからなり、ファイアウォールが出力するログの監視や、侵入検知ツールなどを用いることにより、ネットワークからの侵入を検知し、コネクションの切断などの対策を、マルチベンダ間で自動的に実行するフレームワークが報告されている。図1．に不正侵入防止システムの概要を示す。

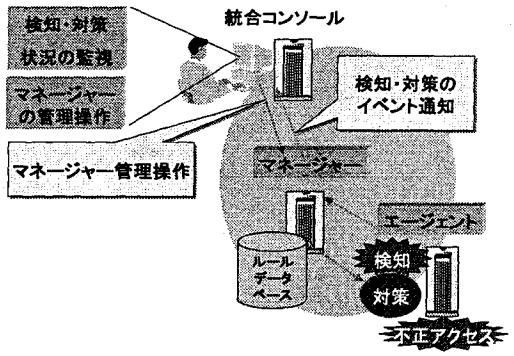

図1．不正侵入防止システムの概要

従来からの運用管理との統合としては、集中的に管理を行っている統合コンソールから不正アクセスの検知、対策状況を監視したり、自動アクションの設定により、オペレータへの自動通報や各種統合システム運用との連携を行うことが可能である。

さらに、統合コンソールからマネージャの機能を呼び出すことにより統合的にマネージャの管理操作を行うことも可能となっている。

3. アクセス制御管理システム

企業のサーバマシンには、財務情報、顧客情報、人事情報など重要な情報が保管されている。これらの情報へのアクセスを制御し、不正アクセスによる情報漏洩、改ざん、破壊を未然に防ぎ、また、WebページやWebアプリケーションへのアクセスを制御するは大変重要である。

アクセス制御間システムは、ファイルやプログラムなど、システム上のリソースへのアクセスや、Webページへのアクセスを所属部門やユーザ毎に制御することを可能とする。その際、ユーザ情報の管理が重要となるが、企業内の全サーバマシンのユーザ情報を各々個別に管理することは大変な労力が必要であり、また退職者や、組織変更時のユーザ情報変更漏れや、サーバマシン間でのユーザ情報の不整合は、セキュリティ上の脅威となりうる。

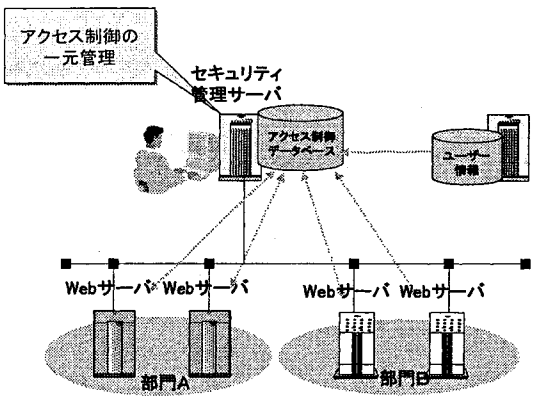

図2．アクセス制御管理システムの構成

図2．にアクセス管理システムの構成を示す。アクセス制御管理システムのユーザ情報管理機能では、既存システムで運用されているユーザ情報を、ディレクトリサーバを使用することにより、全サーバマシンに対して一元的に管理することが可能であり、効率的な管理作業を行うことが可能となっている。

4. まとめと今後の課題

本稿では，セキュリティ管理と従来からの運用管理を統合的に行う方法として不正アクセス防止基盤システムとアクセス制御管理システムについて報告した。これらのシステムでは、(1) 統合コンソールからのイベントの監視、(2) 統合コンソールからの各セキュリティ管理マネージャの管理操作、(3) 従来システムでの資産であるユーザ情報の一元的管理 を統合的に行うことが可能となっている。

本稿で報告したセキュリティ機能以外にもセキュリティ製品として、ウィルス対策やコンテンツフィルタリングなど様々な分野のセキュリティ製品が存在する。また、設計、構築、運用という、システムのライフサイクルを考慮した統合セキュリティ運用管理システム[4]も検討されている。

今後は、統合セキュリティ運用管理として、これらの製品群を統合的に管理する方法を検討していく必要がある。

参考文献

[1] オープンベンダ不正アクセス対策システムにおける統合フレームワークの提案，鳥居他, CSS'99, 1999.10.

[2] オープンベンダ不正アクセス対策システムにおけるモジュール間通信方式の提案，萱島他, CSS'99, 1999.10.

[3] オープンベンダ不正アクセス対策システムにおけるネットワークモニタ実装方式の検討，藤井他, CSS'99, 1999.10.

[4] 統合セキュリティ運用管理システムの実現に向けて，萱島他，情報処理学会全国大会，2001.4.