統合セキュリティ管理システムにおける セキュリティ製品の運用方法

野口順平† 妹尾徹† 浅川知之†
†（株）日立製作所ソフトウェア事業部

１． はじめに

近年のインターネットをベースとする情報システムは企業、学校等の組織だけでなく個人にとっても情報基盤として重要な役割を果たすようになっている。しかし、インターネットは匿名性の保たれたオープンなシステムであるため、Web ページの改ざんやメールシステムに連動するウィルスによる社内文書の流出など、インターネットを利用した悪質な不正行為が過去に多発している。

現在では、これらの不正行為に対する対策としてファイアウォールやウィルス対策製品を導入することは当然のこととなっている。

本稿では、ファイアウォールやウィルス対策製品だけでなく、不正行為を防ぐ様々なセキュリティ製品を統合的に管理し運用するシステムと方法について述べる。２章でセキュリティ製品の運用管理について述べ、３章で複数のセキュリティ製品を統合的に管理するシステムについて述べる。４章でまとめと今後の課題について述べる。

２． セキュリティ運用管理

セキュリティ製品の運用管理は設計、構築、運用の 3 つのフェーズに分けることができる。運用管理はこの 3 つのフェーズを繰り返し行っていくことによりなされる。

２．１．設計フェーズ

設計フェーズではまず、必要となるポリシーを策定し、導入するセキュリティ製品を決定する必要がある。導入するセキュリティ製品には、ファイアウォール、ウィルス対策プログラム、不正侵入検知、アクセス制御など多くのカテゴリがあり一つのセキュリティ製品では必要とするセキュリティポリシーを実現することができないのが現状である。

２．２．構築フェーズ

構築フェーズでは、策定したセキュリティポリシーを実現するために、導入したセキュリティ製品の設定にポリシーを反映する必要がある。このとき、策定したセキュリティポリシーをどの製品で実現するかを明確にし、設定をおこなう。製品ごとに実現できる機能が異なるため、それぞれの製品ごとに設定を行うこととなる。

２．３．運用フェーズ

運用フェーズでは、構築フェーズで設定したおのおのの製品により、セキュリティが正しく維持されているか監視する必要がある。多くの場合は、これまで述べてきたように、セキュリティ製品を複合的に構成することによりシステムのセキュリティを維持していることから、それら全ての製品を監視する必要がある。システムの管理者は外部、又は内部から攻撃を受けた場合に、製品ごとにログ等を見てシステムの異常を判断することになる。

また、不正アクセス等の攻撃の手口は日々複雑・巧妙になっていき、セキュリティホールは日々発見され続けているため、システム管理者は、導入した製品を継続的に監視し続け、必要に応じてセキュリティポリシーを見直す必要がある。

したがって、セキュリティ運用管理では各フェーズを、図１に示すサイクルで回していくことにより、システムのセキュリティを維持することになる。

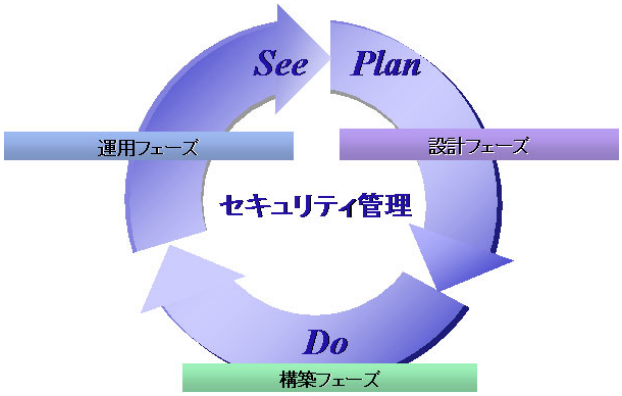

図 1 セキュリティ運用管理サイクル

２．４．セキュリティ運用管理の問題点

現状では構築フェーズと運用フェーズにおいて各製品ごとにポリシーの反映、システムの監視を行う必要がある。個々に製品を運用・管理

することはシステム管理者の負担を増大させ、システム全体の管理コストを増やすだけでなく、障害が発生した場合にタイムリーに調査と対策を行うことが困難となり、システムのセキュリティを維持する上で問題となる。

結果として、セキュリティポリシーにのっとった運用が正しく行われず、システム運用に大きな影響を及ぼす恐れがある[1] [2]。

3． 統合管理システムによる運用方法

今回提案する統合セキュリティ管理システムでは、システムのセキュリティを維持することを容易にし、セキュリティの運用管理サイクルにおける管理者の負担を軽減することを目的としている。

本システムではセキュリティ運用管理において監査支援、一元管理、統合監視の 3 つの機能を提供する。次節以降でその機能の詳細について述べる。

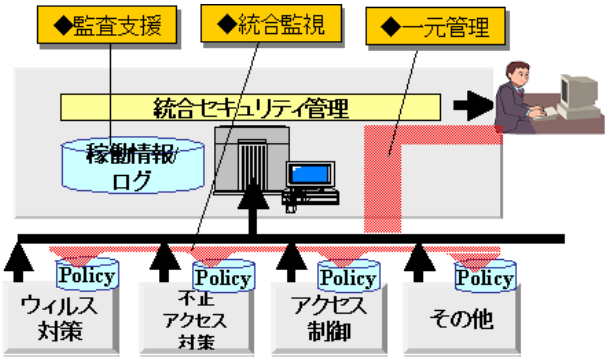

図 2 統合管理システム

3．1．監査支援

管理対象とする全てのセキュリティ製品のログを収集・蓄積し、様々な条件（製品名、期間、製品のカテゴリ等）により検索、並び替え、分類する機能を提供する。この機能により、システムのセキュリティを維持する上で必要となるログのフィルタリング作業と解析作業を大幅に効率化・自動化し、製品ごとではなくシステム全体のセキュリティ監査を容易に行うことが可能となる。

セキュリティ監査は、新たにポリシーを策定する場合にも必要となる作業であるため、設計フェーズにおける負担も軽減できる。

3．2．一元管理

統合セキュリティ管理システムの管理画面からダイレクトに各セキュリティ製品の管理画面を呼び出す機能を提供する。この機能により、各セキュリティ製品のポリシー情報の確認や管理情報のカスタマイズを一元的に行えるため、システム全体として統一的なセキュリティポリシーを策定できる。また、各製品の運用を大幅に省力化・スピードアップすることが可能となる。

個々の製品へポリシーを反映する場合に、統合管理システムからダイレクトに各セキュリティ製品のポリシー設定画面を呼び出せるため、構築フェーズでの負担を軽減できる。

3．3．統合監視

各セキュリティ製品が検知する不正アクセス等のセキュリティイベントを管理者画面より統合的かつリアルタイムに監視する機能を提供する。この機能により、システム管理者は全ての製品が検知するセキュリティイベントを一度に監視でき、どの製品でセキュリティイベントが発生した場合でも即座に対応を取れる。よって、セキュリティ運用管理サイクルの運用フェーズでの負担を軽減できる。

4． まとめと今後の課題

本稿では、複数のセキュリティ製品を統合的に管理するシステムについて述べた。本システムにより、管理対象となる製品のログ収集・蓄積による監査支援、セキュリティ製品のダイレクトな管理者画面の呼び出しによる一元管理、セキュリティ製品の検知するセキュリティイベントの統合監視を行うことが可能となる。

今回提供した機能を用いることにより、システムのセキュリティを維持することを容易にし、またセキュリティサイクルの各フェーズにおいてシステム管理者の負担を軽減できる。

今後は、設計フェーズにおいて策定したセキュリティポリシーをどのように複数のセキュリティ製品に反映させ、各製品のセキュリティレベルを一定に保つかといった構築フェーズにおける統合セキュリティ管理をどのように実現するか検討する必要がある。

参考文献

[1] 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.

[2] 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，妹尾他，情報処理学会全国大会，2001. 9.