統合セキュリティ管理システムによる セキュリティポリシー管理方式

甲斐文幸† 藤岡憲一† 浅川知之† 野口順平† 萱島信‡ 礒川弘実‡
†（株）日立製作所 ソフトウェア事業部 ‡（株）日立製作所 システム開発研究所

1. はじめに

近年，オンラインショッピングや行政の電子化など，インターネットを基盤とした情報システムが我々にとって身近なものとなっている。しかし，その匿名性から，インターネットを利用した不正侵入による Web の改ざんや情報漏洩といった不正行為が多発している。

インターネットを基盤とした情報システムを運用管理する上では，情報システムをこれらの不正行為から守る必要がある。そのため，システムにはファイアウォールや侵入検知システムなど様々なセキュリティ製品が多数導入されている。しかし導入する製品が増えるにつれ，策定したセキュリティポリシーを製品に反映させるための作業が増え，管理者の負担が増大する。そのため，一括して製品の設定をする仕組みが必要となる[2][3]。

本稿では，管理者の負担を軽減することを目的とした，セキュリティポリシーの管理方法について述べる。2 章で複数のセキュリティ製品を統合して管理するシステムについて述べ，3 章で管理者の負担を軽減するセキュリティポリシー管理方式について述べる。最後に 4 章でまとめと今後の課題について述べる。

2. 統合セキュリティ管理システム

現在，システムのセキュリティ製品を統合的に管理するための統合セキュリティ管理システム（図 1）が提案されている[1]。

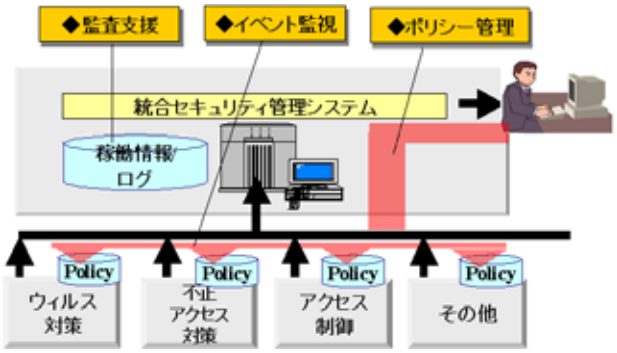

図 1 統合セキュリティ管理システム

2.1. システムの運用方法

このシステムは以下の 3 つの機能を有する。

- **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，含まれるメッセージ等）によるフィルタリングをして管理画面に表示する。これにより，セキュリティ監査の際，管理者の作業が軽減する。
- **イベント監視**
  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にリアルタイムに表示する。これにより，管理者がシステム全体のセキュリティ監視を容易に行える。
- **ポリシー管理**
  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し，策定されたセキュリティポリシーを各製品に反映させることができる。

これらの機能により，一つの管理画面で統合的にセキュリティ管理することができる。

2.2. 問題点

提案されている統合セキュリティ管理システムにおけるポリシー管理では，策定されたセキュリティポリシーを個別に各製品へ反映させる必要がある。これは，セキュリティポリシーを反映させる際に設定の抜け漏れを招き，結果としてシステム全体のセキュリティレベルが低下する。そのため，セキュリティレベルを維持するためのセキュリティポリシーの管理方法を考える必要がある。

3. セキュリティポリシー管理方式

前章で挙げた問題点を解決するために，統合セキュリティ管理システムに継承という考えを組み込み，XML でセキュリティポリシーを管理する方式を提案する。以下，方式の詳細として，ポリシー継承と実際に製品にポリシーを反映させる機能について述べる。

3.1. ポリシー継承

セキュリティ製品をグループ単位（部門など）または製品カテゴリ単位（ファイアウォールや侵入検知システムなど）でまとめ，それぞれのポリシーとなる設定項目および設定値をファイルで管理する。ファイルの形式は W3C によりインターネット標準となっている XML 形式とする。同様に各製品のポリシーとなる設定項目と設定値も XML フ

ァイルで管理する（図 2）。製品などの下位の XML ファイルには，継承を行う上位の XML ファイルの対応を記述しておく。

このように下位の製品群に，システム全体やグループ，製品カテゴリなどの上位で定めたセキュリティポリシーを継承させることで，セキュリティポリシーを各製品に抜け漏れなく反映させることができる。これにより，システム内における各種セキュリティ製品のセキュリティレベルのばらつきがなくなり，システムを安全に保つことができるようになる。

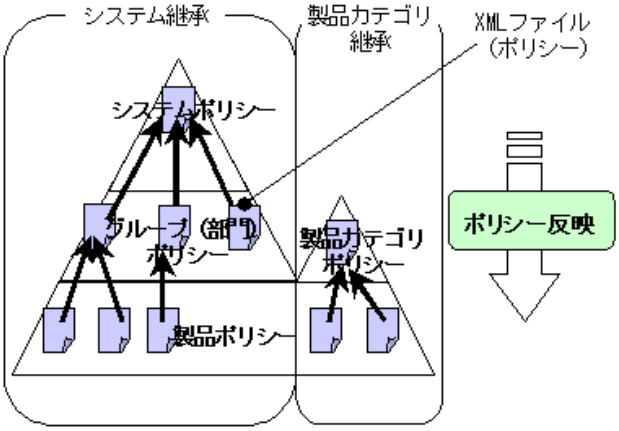

図 2　ポリシー継承

次に具体的に各グループでどのような設定項目を各セキュリティ製品の共通項目とするか選定する。各グループの共通項目は ISO/IEC17799 や ISMS 等の国際セキュリティ標準を基に定めた。例としては，管理者アカウントや，コネクションの設定情報（rlogin や telnet）などの認証系の情報や，セキュリティイベント発生時のメールアラート先などのセキュリティ監査情報がある。

同様に各製品カテゴリの共通項目を選定する。各製品カテゴリの共通項目は複数セキュリティ製品の設定項目の調査を行って定めた。今回はファイアウォールと侵入検知システムに絞り，調査を行った。ファイアウォール製品の場合は，検知するアタックの設定や，サービスを許可するポートの設定などがある。また，侵入検知システムの場合は，SNMP トラップの使用の有無や，ログの採取の有無などがある。実際に製品の設定項目は多数あるが，製品ごとにフォーマットも異なり，共通項目となるのはほんの一部である。今後，標準化が進み共通項目が増えると，製品カテゴリの継承はさらに効果的となる。

3.2. ポリシー収集/配布機能

ポリシーを管理している XML ファイルを編集し，製品やグループに配布する際に，XML ファイルのままでは各製品にポリシーを反映させることができない。そのため，ポリシー収集/配布時には XML のデータを各製品用に変換し各製品を設定する。また，各製品の設定状態を確認したいときには，各製品のデータを XML に変換して収集する（図 3）。

この機能により，製品や，グループのセキュリティポリシーを他の製品やグループに反映させることができ，管理者の負担が軽減する。

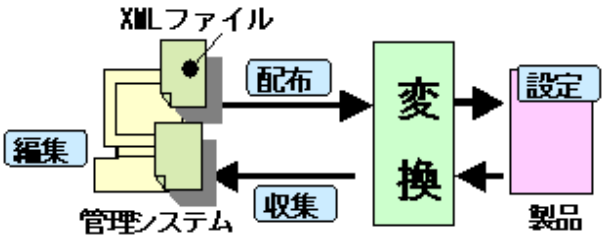

図 3　ポリシー収集/配布

4. まとめと今後の課題

本稿では，セキュリティ製品のポリシー管理方式として，各セキュリティ製品のポリシー設定を XML ファイルで管理し，配布する方式について述べた。本方式を統合セキュリティ管理システムに組み込むことにより，管理者の負担が軽減され，システムのセキュリティレベルの維持を容易にする。

今後の課題としては，製品カテゴリ継承をシステム内に複数設定し，目的に合ったポリシーを反映させるようにすることが挙げられる。また，さらに管理者の負担を軽減するため，検知したセキュリティイベントに対して自動的に製品の設定を変更するような仕組みについて，今後検討していく。

謝辞

本研究は通信・放送機構（TAO）殿の委託研究「インターネットにおける障害情報の自動収集及び復旧支援の研究開発」の成果の一部を含みます。関係各位に感謝いたします。

参考文献

[1] 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，野口他，情報処理学会第 65 回全国大会，2003.3

[2]インターネット障害対策支援システムにおける統合設定機能の設定と実装，笠井他，情報処理学会第 66 回全国大会，2004.3

[3]インターネット障害対策支援システムの提案，萱島他，情報処理学会第 66 回全国大会，2004.3