M-014

ポリシーによるセキュリティ運用管理
A Policy-based Security Management System

岡城 純孝† 松田 勝志†
Sumitaka Okajo Katsushi Matsuda

１．はじめに

インターネットに対する様々な脅威からネットワークを保護するために，ネットワーク全体のセキュリティの一貫性を保ちつつ統一的にセキュリティ施策を実現する方法が求められている．しかし，様々なセキュリティ機能を持った多種多様なセキュリティ機器が存在しているため，それらの設定を統一的に管理することは非常に困難である．そこで，我々は管理者の負担を軽減し設定ミスを防止するため，ポリシーによるセキュリティ運用管理を行うシステムの研究を行っている．

本稿では，機器に依存しないポリシー記述言語と，それで表現したポリシーを分析することによりネットワーク全体のセキュリティ状況の把握や設定の矛盾検出を行う機器設定統合分析システムについて述べる．

２．セキュリティ運用管理における課題

現状のセキュリティ運用管理全般では，以下のような課題がある．

(1) ポリシー表現の不統一
同じ機能を持つセキュリティ機器でも，ベンダや機種，バージョンの違いによってポリシーの記述方法が異なる．

(2) セキュリティ機器の個別管理による一貫性の欠如
異なる機能を持つセキュリティ機器はそれぞれ独立に管理され，正しく連携できているかを確認できない．

(3) 管理者の負担の増大
管理者は，様々なポリシー記述方法を理解し，個々の管理ツールを使い分けながら設定作業を行わなければならず，設定ミスや見落としが発生する可能性が高い．

また、セキュリティ機器の中で最も利用頻度の高いファイアウォール(FW)と侵入検知システム(IDS)の運用管理では，以下のような課題がある．

(4) FW設定の全体像のわかりにくさ
FW のルール設定では，ルールの重なり関係や順序関係が存在するため，設定全体として，どのパケットが通過を許可され，どのパケットが通過を禁止されているのかを把握することが難しく，FW 設定全体の問題点などが見えにくい．

(5) IDS の誤検知
通常，IDS 製品のシグネチャは数百から千を超える数が存在し，それらの設定を対象ネットワークに合わせてうまくチューニングすることは難しい．

３．セキュリティポリシー言語 SCCML

前節の課題（1）および（3）を解決するために，セキュリティ機器に依存しないセキュリティポリシーのモデルおよび記述言語を構築した[1].

3.1 セキュリティ機器動作モデル

まず，セキュリティ機器が持つセキュリティ機能に着目し，その動作と制御されるオブジェクトからなる動作モデルの検討を行った．セキュリティ機能とは，各セキュリティ機器が行う，セキュリティに関する最小単位の処理を指す．例えば，FW ではパケットフィルタリングやアドレス変換がセキュリティ機能に相当する．セキュリティ機器の動作を抽象化して表現することで，機器固有のポリシーの意味と目的の明確化，および類似セキュリティ機器との関連性の明確化を行った．

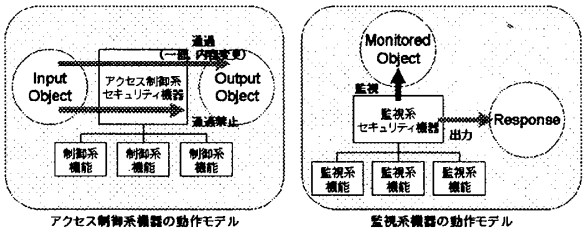

図１ セキュリティ機器の動作モデル

この動作モデルの検討によって，セキュリティ機器をFW に代表されるアクセス制御系機器と，IDS に代表される監視系機器の２つに大別した（図１）．アクセス制御系機器の動作は，

- 入力オブジェクト(InputObject)の通過を許可あるいは拒否する（例：パケットフィルタリング）
- 入力オブジェクト(InputObject)を出力オブジェクト(OutputObject)に変換する（例：アドレス変換）

の２通りに集約できる．また，監視系機器の動作モデルは，

- 監視対象オブジェクト(MonitoredObject)を監視し，該当オブジェクトが検知された場合にはレスポンス(Response)を出力する

で表現できる．

3.2 セキュリティポリシーモデル

次に，それぞれの動作モデルについて，機能の種類，入出力オブジェクトの種類，動作環境の種類などを列挙・整理することでセキュリティポリシーのモデル化を行った（図２）．

アクセス制御系ポリシーには，パケットフィルタリングのように個々のポリシーに優先順位が存在するものがあり，それらをリスト型ポリシーとして規定した．アクセス制御系ポリシーは１つ以上のポリシールールを含む．ポリシールールはセキュリティ機能単位で規定する．例えば，FW のパケットフィルタリング機能のポリシールールは，セキュリティ機能として“パケットフィルタリング”，入力オブジェクトとして“パケットオブジェク

†日本電気株式会社 インターネットシステム研究所

ト”，出力オブジェクトとして“パケットオブジェクト”，動作として“通過許可”あるいは“通過禁止”となる．また，ポリシーごとに条件と責務を規定できる．ポリシーに条件が規定されている場合には，この条件が満足される場合にのみポリシーが評価される．ポリシーに責務が規定されている場合には，ポリシー適用時に責務で規定した処理が実行される．

一方，監視系ポリシーは，例えば，IDS のポリシーは，セキュリティ機能として“パケット監視”，監視対象オブジェクトとして“パケットオブジェクト”，レスポンスとして“アラートオブジェクト”となる．

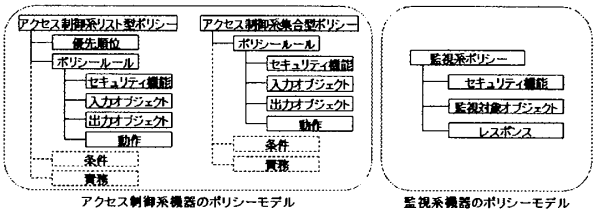

図２ セキュリティポリシーモデル

3.3 SCCML

前述のモデルに基づいて，ポリシー記述言語 SCCML(Security Configuration Coordination Markup Language)を構築した．SCCML は，標準化団体 OASIS が制定した XACML(eXtensible Access Control Markup Language)を拡張した XML 形式の言語である（図３）．

これまでに SCCML を用いて，CheckPoint 社の FW 製品である FireWall-1 や，ISS 社の IDS 製品である NetworkSensor のポリシーを記述できることを確認した．

```
<Policy policyID="contentsSecurity001" policyRuleCombiningAlg="ordered-deny-overrides">
 <PolicyDescription>LANから外部のWebサーバへの接続を許可する</PolicyDescription>
 <PolicyRule policyRuleID="packetFiltering001" effect="permit">
  <PolicyRuleDescription>LANから外部のWebサーバへのアクセス</PolicyRuleDescription>
  <Target>
   <Function>packet_filtering</Function>
   <InputObject>
    <Packet>
     <SrcIP>192.168.1.0/32</SrcIP>
     <SrcPort>any</SrcPort>
     <Protocol>tcp</Protocol>
     <DestIP>0.0.0.0/0</DestIP>
     <DestPort>80</DestPort>
    </Packet>
   </InputObject>
   <Action>accept</Action>
   <OutputObject/>
  </Target>
 </PolicyRule>
 <Obligations fulfillOn="permit">
  <Obligation>
   <Track>long</Track>
  </Obligation>
 </Obligations>
</Policy>
```

図３ SCCML の記述例

４．機器設定統合分析システム

２節の課題（2）～（5）を解決するために，前述の SCCML を用いて記述したセキュリティポリシーを分析することにより，セキュリティ機器を統合的に管理し，管理者の負担を軽減する機器設定統合分析システムを試作した[2]．本システムでは，以下のステップでセキュリティ機器設定の分析を行う．

（1）設定情報の収集

まず，管理対象ネットワークに存在するセキュリティ機器から現在の設定情報を収集する．

（2）ポリシー抽出・言語化

収集した設定情報を SCCML に変換する．

（3）ポリシー分析

次に，ポリシーを分析することにより現在のセキュリティ状況の把握を行う．試作システムでは，

- 削除可能な FW ルールの検出
- パケットの通過／禁止判定を行う FW シミュレータ
- サービスごとの IDS の監視状況の把握

などを実現した．

（4）矛盾検出

続いて，SCCML 中のオブジェクト属性の関連性に基づいてルールを対応付けることにより，異なる機能を持つ機器のポリシー間に存在する矛盾を検出する．試作システムでは，FW ルールと IDS ルールをパケットオブジェクトによって対応付け，さらに FW ルールの動作（通過許可，あるいは通過禁止）と IDS ルールの動作（監視する，あるいは監視しない）を調べることで，

- FW で通過を許可しているのに IDS で監視していない（監視漏れ）
- FW で通過を禁止しているのに IDS で監視している（監視過剰）

という FW と IDS の設定間に存在する２種類の矛盾検出を実現した（図４）．

（5）対処案提示

矛盾が検出された場合には，設定の修正案を提示する．設定の矛盾箇所をピンポイントで特定できるため，具体的な修正案を提示することができる．

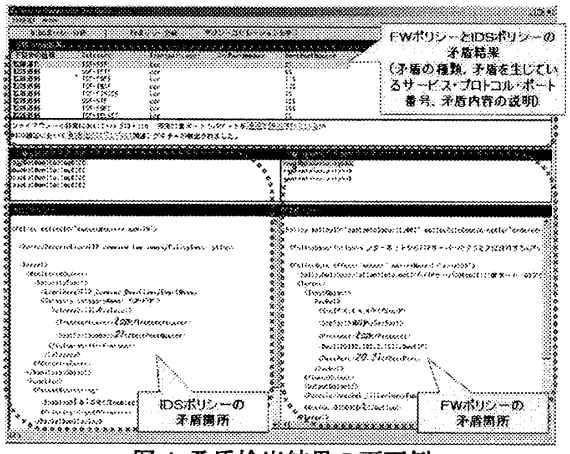

図４ 矛盾検出結果の画面例

FW ルール３個と IDS ルール 1700 個の組み合わせについて矛盾検出の比較実験を行ったところ，システム管理者が手作業で最低でも 170 時間を要したのに対して，試作システムではわずか３分で行えることを確認できた．

５．おわりに

本稿では，セキュリティ運用管理を容易にする，セキュリティポリシー言語 SCCML と、SCCML を用いた機器設定統合分析システムについて述べた．

参考文献

[1]岡城，松田，小川，“セキュリティ運用管理のためのポリシー言語 SCCML”，情報処理学会研究報告，2004-CSEC-27, Vol2004，No.129，pp.89-94(2004).

[2]岡城，松田，小川，“セキュリティ運用管理における機器設定統合分析システム”，情報処理学会研究報告，2005-CSEC-28, Vol2004，No.130，pp.303-308(2005).