社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（53）
2005－CSEC－28（53）
2005／3／23

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

岡城純孝　松田勝志　小川隆一
ＮＥＣインターネットシステム研究所

要旨

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、いろいろな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･管理は非常に複雑である。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、相互に関係する複数のセキュリティ機器から設定情報を抽出し、機器に依存しないポリシー言語に変換して分析を行うことにより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を提案する。また、ファイアウォールと侵入検知システムを分析対象とした試作システムについても述べ、従来方式と比較した場合の本方式の優位性を示す。

An Integrated Security Configuration Analyzing System for Policy-based Security Management

Sumitaka OKAJO, Katsushi MATSUDA and Ryuichi OGAWA

Abstract

In order to protect networks against network security threats, many security components with various security functions have been deployed, and the configuration and management of those components are highly complex. Therefore, we need a policy-based security management system to reduce system administrator's load.

This paper presents a security configuration analyzing system, which can summarize current configurations and find security policy conflicts among the configurations of cooperated devices. The paper also presents a prototype system, which can find conflicts between firewall and NIDS policies. Advantages of the proposed method to existing techniques are clarified by an experiment.

１．はじめに

企業の社外公開サーバの設置によって、ユーザは企業へ２４時間３６５日いつでもどこからでもアクセスしサービスを受けることができるようになった。しかし同時に攻撃者はいつでも攻撃を行うことが可能となり、企業ネットワークには万全なセキュリティ対策が必要となっている。

このような背景から近年、各企業は自身のネットワークを脅威から守るために、様々なベンダから提供される多数のセキュリティ機器やセキュリティ対策ソリューションを併せて運用するようになってきている。しかし、多数のセキュリティ機器の設定項目は膨大な量に上り、それを効果的に分析できるツールが欠けているために、セキュリティ管理者が企業ネットワーク全域に渡ってセキュリティ状況を正確に把握することは非常に困難になっている。

このため、管理者の負担を軽減し設定ミスを防止するセキュリティ運用管理方式が必要とされており、我々はこれを実現するセキュリティポリシー管理基盤の研究を行っている。本稿では、セキュリティ機器から設定情報を抽出し、それら設定情報を分析することによりネットワーク全域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を提案する。

NEC インターネットシステム研究所
Internet Systems Research Laboratories, NEC Corp.

２．セキュリティ運用管理の問題

本節では、セキュリティ運用管理の問題点について述べる。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と IDS（Intrusion Detection System； 侵入検知シス

テム）の運用管理の問題点についても述べる。

２．１．セキュリティ運用管理全般の問題

現在、各企業ではファイアウォール、ウイルス対策ソフト、IDS などのセキュリティ関連のハードウェアやソフトウェアを積極的に導入することによりセキュリティを確保しようとしている。その結果、以下のような問題が深刻化している。

- **セキュリティ機器の個別管理による一貫性の欠如**

個々の機器の設定についてはそれぞれの管理 GUI を利用して比較的簡単に運用管理できるものもある。しかし、同じ機能を持つセキュリティ機器であっても、ベンダやバージョンごとにそれぞれ対応する管理ツールを利用しなければならない。さらに、相互に関係するにもかかわらず異なる機能を持つ機器はそれぞれ独立に管理されており、それらがうまく連携できているか、補完的に動作できているかを確認することができない。このように多数のセキュリティ機器に対して設定変更を間違いなく行うことは非常に難しくなっている。

- **セキュリティ運用管理における管理者負担の増大**

上記のような問題が存在する状況下で、管理者はセキュリティを保つために多くの負担を強いられる。管理者はセキュリティ設定の現状把握や変更のたびに、個々の製品ごとの管理ツールを使い分けながら作業しなければならず、非常に効率が悪い。さらに、相互に関係する機器間の設定において整合性がとれているかどうかについても、管理者の知識や経験に基づいて検査されており、設定ミスや見落としが発生する可能性が高い。

２．２．ファイアウォール運用管理の問題

ファイアウォールの運用管理では以下のような問題点がある。

- **設定の全体像のわかりにくさ**

ファイアウォールでは、個々のパケットごとに細かくルールを設定する必要があり、設定記述自体も同じ形式で表現された多数のルールのリストとなる。また、パケットには IP ドレスやポート番号の範囲、プロトコルの種類などによって重なり関係が存在する。さらに、ルールには順序関係が存在し、通常、ファイアウォールを通過するパケットに対して先頭から順にルールが評価され、そのパケットにマッチする１つのルールが適用されると以降のルールは評価されない。そのため、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、ファイアウォール設定全体の問題点などが見えにくい。

- **設定ミスの発見のしにくさ**

ファイアウォールを通過すべきパケットが通過せずに拒否された場合は、ユーザからクレームが発生するので、この設定ミスは修正され易い。逆に、ファイアウォールを通過してはいけないパケットが通過した場合は、クレームが発生しないので、この設定ミスは気づかれず修正されないことが多い。この種の設定ミスは結果的にセキュリティホールとなってしまう。

２．３．IDS 運用管理の問題

IDS の運用の際には誤検知の問題がある。誤検知には、

- 検知されるはずなのに検知されない(false negative)
- 検知されないはずなのに検知される(false positive)

の２種類がある。これら誤検知の発生をいかに低く抑えるかは、IDS が何を監視し、何を監視しないかの設定に依存する。

しかし、通常の 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。また、シグネチャの名前付けや分類が製品固有の方法で行われているため、IDS を統一的に管理することが難しい。

３．従来研究

３．１．セキュリティ統合管理

前節で述べたような問題を解決する目的で、企業ネットワーク全体の統合管理を行うツールが登場している[1][2]。しかし、これらのツールは１つのコンソールから複数機器の管理 GUI を呼び出したり、複数機器の設定情報を一元管理できたりするにとどまり、異なる機種・機能間の設定矛盾を検出するなどの機能はない。また、ネットワークに存在する脆弱性検査を行うツールも存在する[3][4][5]。しかしこれら脆弱性検査ツールは、製品によって用途や機能にばらつきがあり検査精度が悪い、実環境への影響が大きい、複数機器の連携不備によって生じる脆弱性の検査は行えない、などの問題がある。

３．２．ファイアウォール管理

ファイアウォールポリシーの記述や検証については Jalili らによって、ネットワークトポロジーから独立した高レベルな形式言語によるポリシー記述と、そのポリシー記述を用いて矛盾や対象範囲、脆弱性を発見するための定理証明に基づいた分析ツールが提案されている[6]。

また、Vadim もファイアウォールポリシーを分析するツールを提案しており、「あるルールがそれに続く後のルールのスーパーセットであり、いかなるパケットもマッチしないようなルール(rule shadowing)」を検出可能である[7]。

３．３．IDS 管理

IDS におけるシグネチャの統一管理の問題を解決するため、数多くのセキュリティ関係の組織によって CVE(Common Vulnerability and Exposures)[8]が作成されている。CVE は脆弱性の名称が標準化されたリストである。しかしながら、１つの脆弱性について複数のシグネチャがマッピングされていたり、CVE に登録されていないシグネチャが存在する、などの問題がある。

また、IDS 設定のチューニングについては、管理者の個人的スキルに頼っており、自動的に適切なチューニングを行うような技術はない。

４．機器設定統合分析

従来技術では、相互に関係する複数の機器間の矛盾検出、設定のチューニングなどの問題について解決できていない。これらの問題を解決するため、設定情報から機種に依存しないポリシーを生成し分析することで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提案する。提案システムの概要を図１に示す。

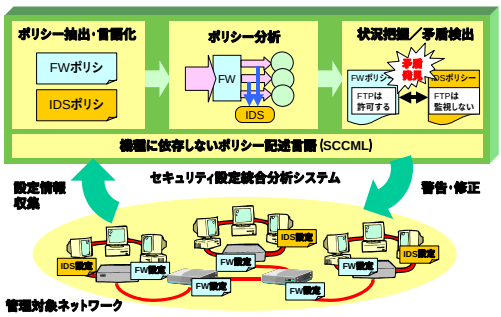

図１ 機器設定統合分析システムの概要

本システムでは、以下のようなステップでセキュリティ機器設定の分析を行う。

（１） 設定情報の抽出とポリシー化

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設定されている設定情報の抽出を行う。そして抽出した設定情報を、機器に依存しないポリシー記述言語である SCCML(Security Configuration Coordinator Markup Language)[9]に変換する。SCCML は、セキュリティ機器が持つセキュリティ機能の動作と、それによって制御されるオブジェクトからなる動作モデルに基づいた記述言語であり、ファイアウォール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ポリシーを統一的に表現可能である（図２参照）。

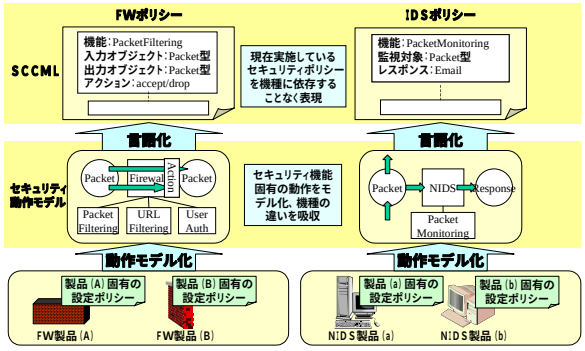

図２ 設定情報の抽出とポリシー化

アクセス制御系機器のポリシーは、

- 入力オブジェクト Input 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 Input を出力オブジェクト Output に変換する（例：アドレス変換）

という２種類の動作モデルに基づいて表現される。また、監視系機器のポリシーは、「監視対象オブジェクト Object を監視し、該当する属性を持つオブジェクトが検知されたときに反応 Response を出力する」という動作モデルに基づいて表現される。図３に SCCML によるパケットフィルタリングポリシーの記述例を示す。図３では、特定のパケットに対するアクション（通過許可あるいは禁止）が表現されている。

これまでに SCCML を用いて、CheckPoint 社のファイアウォール製品である FireWall-1 や、ISS 社の NIDS 製品である NetworkSensor のポリシーを記述できることを確認している。

```
<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>
    </Obligaion>
  </Obligations>
</Policy>
```

図３ SCCML の記述例

（２） ポリシー分析

次に生成された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や設定の矛盾検出を行う。ポリシー分析には、個々のセキュリティ機能のポリシーに対して行う分析と、相互に関係する複数のセキュリティ機能のポリシーに対して行う分析があるが、後者についてはこれまでほとんど研究されていない。本システムでは、SCCML で表現されたポリシーに存在する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、異なる機能についてのポリシー間の統合分析を実現している。本稿では、これをポリシーコリレーション分析と呼ぶ。図４にポリシーコリレーション分析の概略を示す。

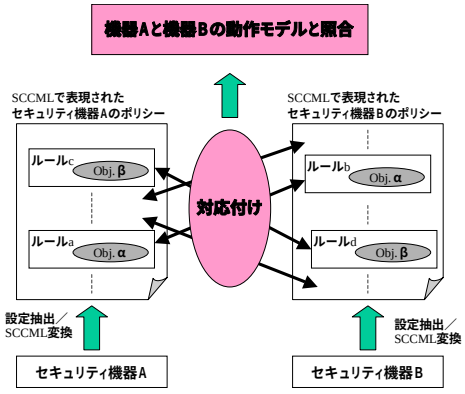

図４ ポリシーコリレーション分析の概要

例えば図４では、異なる機能を持つセキュリティ機器ＡとＢから生成されたポリシーにおいて、Obj. α という同一のオブジェクトの存在によってルール a とルール b を対応付けている。その後、Obj. α を SCCML における機器Ａと機器Ｂとを連携させた動作モデルと照合し、モデル上で Obj. α の流れをシミュレートすることでルール a とルール b の間の矛盾検出を行う。

ポリシーコリレーション分析によって、相互に関連しているにもかかわらず、機能・機種が異なるためにそれぞれ別々に管理されていた機器設定を統合して分析することができる。

（３）修正案提示

ポリシー分析によって矛盾が検出された場合には、それを解消するために、設定の修正案を提示する。本システムの方式では、設定の矛盾箇所をピンポイントに特定可能であるため修正作業が容易になり、管理者の負担を大幅に軽減することができる。

５．試作システム

本節では、ファイアウォール(FW)とネットワーク型 IDS(NIDS)を対象とした、機器設定統合分析の試作システムについて述べる。

５．１．FW ポリシー分析

ＦＷでは、一般にパケットの種類ごとに通過許可あるいは通過禁止の判別をルールとして規定する。そこで本システムでは、各ルールに規定されたパケットをルールの順序関係を加味しながら｛送信元ＩＰアドレス，送信元ポート，宛先ＩＰアドレス，宛先ポート，プロトコル｝からなる５次元空間モデル上に射影し、最終的にこの５次元空間全体を通過許可あるいは通過禁止の２つの領域に分割する。これによってＦＷポリシー全体に対してさまざまな分析が可能となる。図５に FW ポリシー分析の概略を示す。

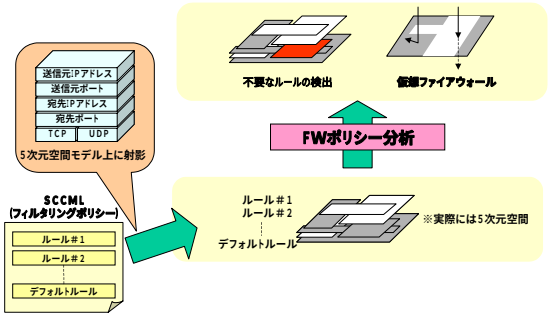

図５ FW ポリシー分析

試作システムでは以下のような機能を実現した。

- **不要なルールの検出**

例えば、図６に示すような２つのルールがあるとする。

(172.16.10.0/24, any, 192.168.100.0/24, any, tcp) : **通過許可**

(172.16.0/24, any, 192.168.100.100, any, tcp) : **通過禁止**

※(送信元IPアドレス, 送信元ポート, 宛先IPアドレス, 宛先ポート, プロトコル) : アクション

図６　FWルールの例

このときＦＷで上から順にルールが評価されるとすると、下のルールは上のルールによって完全に内包されるため、下のルールが発火することはない。つまり下のルールは常に評価されることがないため不要と判断できる。

- **ファイアウォールシミュレータ**

あるパケットがＦＷルール全体と照合された場合に通過領域に含まれるか、禁止領域に含まれるかを判定する。つまり、抽出した設定情報を用いたファイアウォールのシミュレータ機能である。

５．２．NIDS ポリシー分析

NIDS ではどのようなシグネチャを選択して監視を行うか、というルールの集合がポリシーとなる。しかし、シグネチャは攻撃方法や OS の種類など、製品に固有の方法で分類されているため、統一的に監視状況を把握することが難しい。そこで本システムでは、NIDS ポリシーのルールを、シグネチャが実際に監視するサービス（プロトコルとポート番号の組）で分類する。図７に NIDS ポリシー分析の概略を示す。

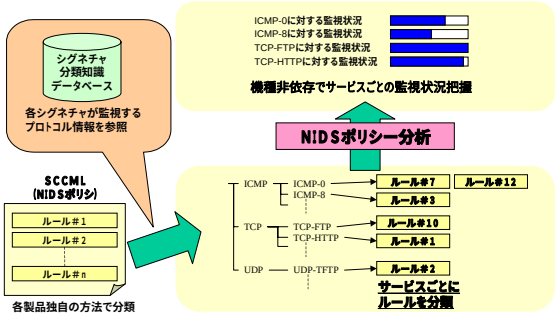

図７　NIDS ポリシー分析

製品固有の方法で分類されたルールをサービスごとに分類するために、シグネチャ分類知識データベースを用いた。各シグネチャが監視しているサービスの情報が格納されたシグネチャ分類知識データベースは、各製品のシグネチャ詳細情報や CVE などを参照して作成した。これによって、機種に依存せず、サービスごとの監視状況を提示する機能を実現した。

５．３．FW-NIDS ポリシーコリレーション分析

ファイアウォールはポリシーに基づいてパケットをフィルタリングする機能を持つが、攻撃の識別は行わない。つまり、ファイアウォールでアクセスを許可した通信を用いた攻撃は防ぐことができない。

NIDS はポリシーに基づいてネットワークを流れるパケットを監視する機能を持つが、防御機能は持たない。さらに NIDS には誤検知の問題がある。

そこで、ファイアウォールでアクセスを許可され、ネットワークを流れる可能性のあるパケットについてのみ NIDS で監視を行う、といった設定になっていれば相互にうまく連携した、矛盾のない設定であるといえる。試作システムでは、この仮説に基づき FW ポリシーと NIDS ポリシーに存在するパケットオブジェクトの関連性に基づいてコリレーション分析を行う。図８に FW-NIDS コリレーション分析の概略を示す。

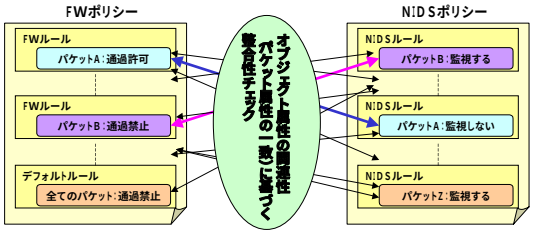

図８　FW-NIDS コリレーション分析

まず、FW ルールと NIDS ルールの対応付けを行う。NIDS ポリシー分析結果からは、各 NIDS ルール（シグネチャ）が監視するプロトコル(tcp, udp あるいは icmp)と、ポート番号や icmp タイプなどのパケット属性が得られる。また、FW ポリシー分析結果からは５次元空間モデルにより通過許可あるいは通過禁止のパケット情報が得られる。このパケット情報には当然、プロトコル、ポート番号ないし icmp タイプのパケット属性も含まれるため、これらのパケット属性について同じ値を持つ FW ルールと NIDS ルールを対応付けることができる。さらに、対応付けられたルールごとに、FW ルール中のアクション（通過許可あるいは通過禁止）と、NIDS ルール中のアクション（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 NIDS で監視していない（監視漏れ状態）
- FW で通過を禁止しているのに NIDS で監視している（監視過剰状態）

という FW と NIDS 間に存在する２種類の矛盾の検出を実現した。図９に試作システムでの実行結果画面例を示す。

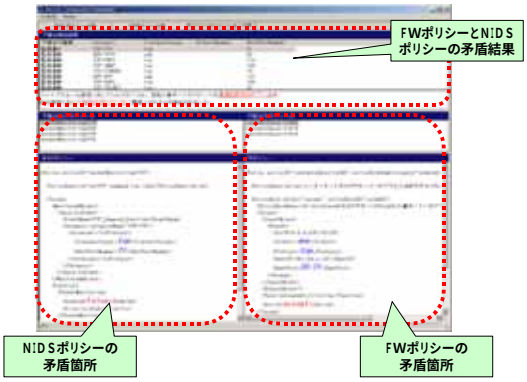

図９ ポリシーコリレーション分析実行結果

さらに、矛盾の原因となるルールをそれぞれのポリシーについてピンポイントで特定することができ、ポリシーの修正案を提示することが可能である。管理者はこの修正案に基づき容易に修正を行うことができる。

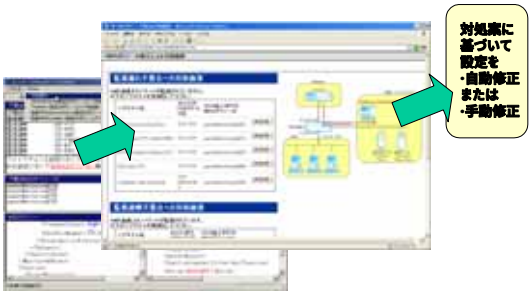

図１０ 対処案提示

６．試作システムの評価

試作システムの効果を確かめるため、FW ポリシーと NIDS ポリシー間の矛盾検出に要する時間コストについて、本システムを用いた場合と手作業による場合との比較実験を行った。図１１に示すような構成を持つネットワークを想定した。

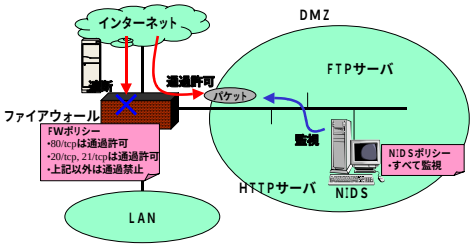

図１１ 想定構成

ファイアウォールポリシーは正しいという仮定のもとで、NIDS ポリシーの 1700 ルールについてファイアウォールポリシーに矛盾しないように修正を行う、つまり HTTP および FTP に関係のないシグネチャを選別することを、FW と IDS の運用管理を行っているシステム管理者に手作業で行ってもらった。すると最低でも 170 時間かかるという結果を得た。一方、本システムでは、それぞれの機器の設定抽出からポリシー間の矛盾検証（シグネチャの選別）まで約 3 分で行えることを確認できた。比較結果を図１２に示す。

方法	検証時間	精度
専門家による手動検査* (膨大な組み合わせ)	× 170時間	○ どこに矛盾があるかわかるが，検査漏れの可能性あり
本方式による検査	◎ 約3分	◎ どこに矛盾があるかがわかり、リアルタイムで対処可能

図１２ 従来方法との比較

７．おわりに

本稿では、セキュリティ機器から設定情報を抽出し、それら設定情報を分析することによりセキュリティ状況の把握や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た。また、ファイアウォールと NIDS の設定統合分析を可能にする試作システムについて述べた。試作システムでは、仮想的なファイアウォール機能を可能とする FW ポリシー分析機能、機種に依存せずにサービスごとの監視状況を提示する NIDS ポリシー分析機能、FW と NIDS 設定間の矛盾検出を行う FW-NIDS ポリシーコリレーション分析機能を実現している。矛盾検出の効率は、人手による場合と比べて 1/1000 のオーダーとなった。

今後は、新しい分析方式や対象機器の拡充について検討を行っていく予定である。

【参考文献】

[1] http://www.hitachi.co.jp/Prod/comp/soft1/jp1/.

[2] http://www.symantec.com/region/jp/ssms/sesa.html.

[3] http://www.isskk.co.jp/product/Internet_Scanner.html

[4] http://www.ncircle.com/index.php?s=products_ip360.

[5] http://www.qualys.com/

[6] Jalili, R., and Rezvani, M, "Specification and Verification of Security Policies in Firewalls", Lecture Notes in Computer Science # 2510, Springer, 2002, pp. 154-163. 2002.

[7] Vadim Kurland, “Firewall Builder”, 11th DFN-CERT Workshop, February 2004.

[8] http://cve.mitre.org/

[9] 岡城純孝，松田勝志，小川隆一，「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).