修士論文要旨

ネットワークセキュリティの統合的管理手法

武智 洋

北陸先端科学技術大学院大学 情報科学研究科

2000年2月15日

キーワード： ネットワークセキュリティ、ポリシー、ネットワークマネージメント.

ネットワークが非常な勢いで普及しつつある中で、ネットワーク管理においてセキュリティ管理を如何に行うかが大きな問題になりつつある。コンピュータウイルスなどのセキュリティ上の脅威も急速に増えつつあり、それらに対応してネットワークの各種設定を維持管理していくことが管理者の負担を増大させている。そのため、多くの組織ではポリシーを定めてそれに基づいてネットワークの運用管理を行なおうとしている。

しかしながら、多くの場合、組織のポリシーは非常に抽象度の高いレベルで記述されており、実際にネットワーク運用に反映するためには、より具体的なレベルの手続きに変更することが必要になる。

企業や大学など一般組織においては、管理者が経験に基づいて、ポリシーの解釈および各種ネットワーク上の機器設定などを行っている。複数ベンダー、様々なハードウェア・ソフトウェアによって構成されるネットワークにおいてすべてのセキュリティ設定を手動で行うことは、非常に優秀な管理者であっても難しいタスクである。

このような理由からポリシーに基づいたネットワーク管理が容易に行える管理手法が必要となってきている。

そこで、本論文では、組織におけるネットワークの各種セキュリティ設定を整合性を保ちつつ運用管理するために、ポリシーに基づいたネットワークの一元管理システムの枠組みを提案する。属性文法に似た手法を用い、ネットワーク上の各機器が構文木のノードになる構文木を構成し属性計算することを特徴とする。属性計算に用いる属性はポリシーから生成されたネットワーク上のサービスを示す属性である。この属性文法的な手法により、ポリシーと実ネットワーク上の機器間の各種対応付けを行う。

では、詳細について順に説明する。まず、この枠組みでは、ネットワークを提供されるサービスの集合であると考え、サービスをポリシーで記述したサービス記述によってネットワークを定義する。ポリシーは以下の要素で構成され、

- **オブジェクト** – サービス提供用資源
- **サブジェクト** – サービス利用者
- **アクション** – サブジェクトのオブジェクトに対する動作
- **制約** – ポリシーが適用される際の条件

『ある制約の中でオブジェクトに対してサブジェクトが何らかの操作（ゴール）を行うことに対して許可または禁止する。』

という記述が行われる。記述されるポリシーは、サブジェクトがアクションを起こそうとする意思を示したものか、あるいは、起こすことができる権限を示したものかに分類される。さらに、アクションがポジティブであるかネガティブであるかで分類され、最終的に以下の 4 種類のポリシーに分類される。

- Positive authorization – 許可
- Negative authorization – 禁止
- Positive motivation – 要求
- Negative motivation – 阻止

これで提供したいネットワークが定義できた。次に、定義したポリシーを実際のネットワーク上に展開するために、ポリシーからサービス属性と属性間の関係を定義した属性評価規則を生成する。

サービス属性は、各サービスに関係していることを示す属性である。先に述べた 4 種類のポリシーのうち、Positive/Negative authorization から生成する。生成するのは以下の 3 つである。

- オブジェクトサービス属性
- ポジティブサブジェクトサービス属性
- ネガティブサブジェクトサービス属性

ポジティブサブジェクトサービス属性は Positive authorization に記述されているサブジェクト、ネガティブサブジェクトサービス属性は Negative authorization に記述されているサブジェクトに与えられる。オブジェクトサービス属性は、そのサービスのオブジェクトに与えられる。

属性評価規則は、各属性間の関係を式で記述したものである。自動生成される属性評価規則としては、サービスが提供されることを保証するための評価式がある。つまり、サービスを利用できるポジティブサブジェクトとサービスを提供するオブジェクトが通信できるように、オブジェクトサービス属性とポジティブサブジェクトサービス属性が互いに交わる必要があることを表現した式である。また、同時にネガティブサブジェクト属性がオブジェクト属性と交わらないことを表現した式も生成される。

ここまでで、実際のネットワーク上にサービスがどのように展開するかを知るための準備が整ったことになる。

次に、実際のネットワークをモデル化したネットワーク構成記述を生成する。ネットワーク構成記述は物理層からアプリケーション層まで5つのレイヤ構造としてモデル化される。これは、各レイヤ毎のアクセス制御機構がサービス属性への制御を独立に行なうことをモデル化するためである。各々のネットワーク機器が持つポートとそれらを結ぶリンクによって記述される。

これら、属性、属性評価式、ネットワーク構成記述から、属性計算が行われ、

- サービスの展開されているネットワーク上の広がり
- サービスに関係しているネットワーク機器

を知ることができる。サービス属性の計算は、ポートとリンクを属性計算の構文木と見立てて、サービス属性が継承あるいは合成されながら、ネットワーク構成記述上を伝搬することで行われる。アクセス制御機構を持つネットワーク機器においてサービス属性が継承あるいは合成されるかは、各ポート間にあるアクセス制御点においてアクセス制御規則または、属性評価規則を評価することによって決まる。

サービス属性の計算によって以下の2つの操作が行える。

- ポリシー違反検出
- アクセス制御規則導出

ポリシー違反検出は、まず、サービス属性を現在設定されているアクセス制御規則で、属性計算する。その後、属性評価式により各ポート上の属性を評価しポリシーに違反を検出する。アクセス制御規則導出は、アクセス制御点において属性評価式を満足するアクセス制御規則を求めることで行なう。

本論文では、サービス記述からアクセス制御規則を導出手法およびポリシー違反の検出手法を提案した。また、ネットワーク層のみのネットワーク構成記述持ったプロトタイプを設計/実装し、内部WWWサービスに対するアクセス規則導出などを行ない、これらの手法の有用性を確認した。また、ポリシーによるセキュリティ管理に関連した各種システムの調査を行い、ポリシーを基にしたセキュリティ管理システムにおいてどのような点が問題となるのかについて議論し、今後の展望として、

- 各種ポリシー表現やポリシーの取り扱い方法
- ポリシーコンフリクト検出
- リファレンスモニターの実現方法

などについて考察した。