6E-1

ネットワーク記述言語の開発とそれによるネットワーク管理

武田 利浩† 佐藤 哲也‡ 平中 幸雄†
山形大学工学部† 山形大学大学院理工学研究科‡

１．はじめに

近年、企業におけるセキュリティー意識の高まりとともに、攻撃を防御する仕組みや、ネットワークを監視するツールに対する需要が増している。そのため、様々な製品が開発され、ネットワークを構成する機器は、複雑化し、マルチベンダ化が進んできている。同じ機能の機器であってもメーカ毎に設定の方法が異なり、固有の知識が求められる。さらに、設計から管理までの統一的な枠組みはなく、それらの設定間の整合性の確認は、管理者の能力に依存しており、保障する方法は無い。

本研究では、ネットワークを構成する機器やサービスを記述できるようなネットワーク記述言語を開発し、ネットワーク管理に応用することを提案する。これにより、ネットワークの設計・設定・管理（監視）を統一的に扱う枠組みが提供でき、管理コストの軽減が期待できる。

２．ネットワーク記述言語

ネットワーク記述言語による記述の対象は、１）設計モデル、２）機器モデル、３）スナップショットの３つである。以下、順に説明する。

１）設計モデル

ネットワークの要求仕様であり、ネットワーク管理者が設計の段階で記述する。ネットワークを構成する機器やサービス、発生する通信の性質を記述する。

２）機器モデル

機器モデルは、個々のネットワーク機器の仕様で、機器を提供するメーカが用意する。

３）スナップショット

運用中のネットワークの現在の状態であり、ネットワークセンサーにより自動的に生成される。

Development of Network Description Language and Its Application to Network Management
†Toshihiro Taketa・Faculty of Engineering, Yamagata University
‡Tetsuya Sato・Graduate School of Science and Engineering, Yamagata University
†Yukio Hiranaka・Faculty of Engineering, Yamagata University

３．ネットワーク管理への応用

従来の方法では、ネットワークの設計・設定・管理は、図１のようになる。設計から管理までの統一的な枠組みはなく、人の経験や能力によって行われている。設計書から個々の機器の設定書を作るには、設定者がネットワークの設計書を理解し、個別の機器の情報の知識を利用して、設定ファイルを書いている。さらに、ネットワークの管理になると、設定を更新しても設計を更新することがなされない場合が多く、設定ファイルにどのような設定がされているかを理解し、ネットワークの仕様をつかみ、各種監視ルーツを設定・運用して管理を行うことになる。

これに対して、本研究では、図２に示すような流れで、これを行う。以下、順に説明する。

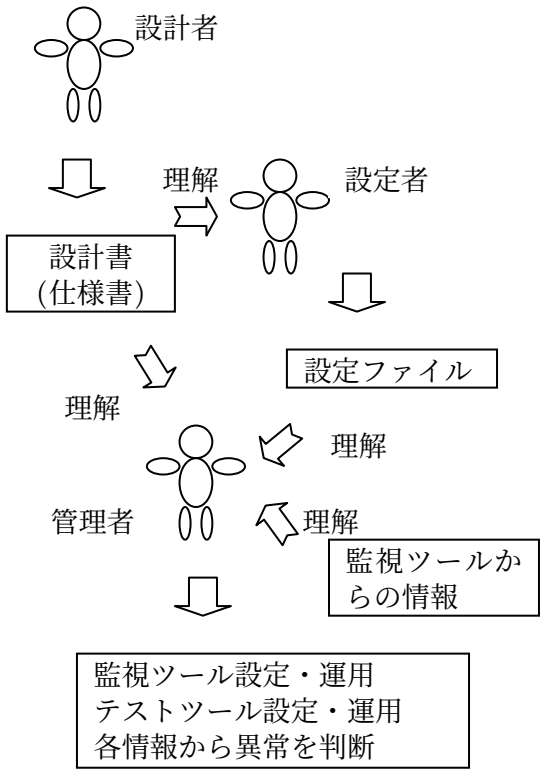

図１　従来の方法での設計・設定・管理の流れ

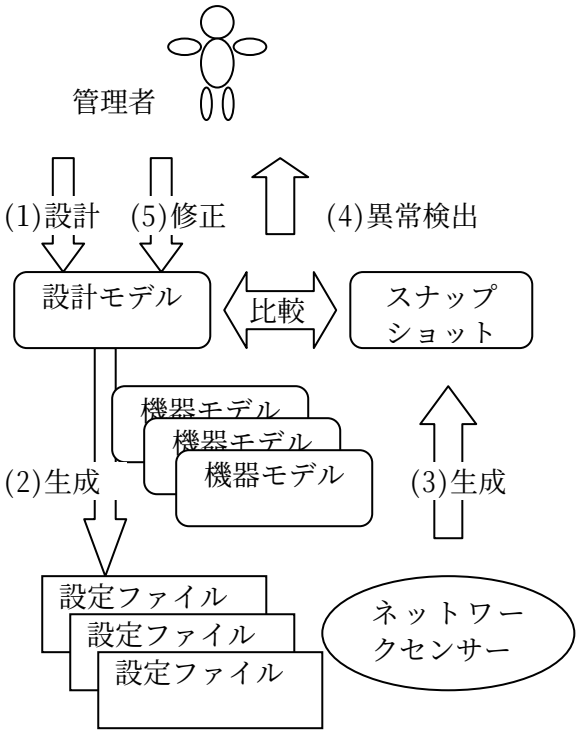

図２　設計・設定・管理の流れ

１）ネットワークの設計

ネットワークの管理者は、構築したいネットワークを設計し、設計モデルを作成する（図２(1)）。この時、個別の機器に依存しない抽象的なモデルを記述する。

２）ネットワークの設定

設計モデルと機器モデルから、個別の機器の設定を機械的に自動生成（図２(2)）し、機器に適応する。

３）ネットワークの管理（監視）

まず、ネットワークセンサーからの出力により、現状のネットワークの状態を表すスナップショットを生成する（図２(3)）。次に、生成したスナップショットと設計モデルの比較から、設計に無い、未知の端末や通信を発見し、異常として検出する（図２(4)）。ここで、検出した異常は、設計時には想定していなかっただけで、正当なものである場合もあり得る。したがって、管理者は、検出した異常について、正当・不正を判断し、設計モデルに反映（図２(5)）させる。

４．期待される効果

企業の内部からの情報漏洩への対策から、不正な端末や不正な通信を監視する仕組みが求められている。また、コスト削減の目的で、IP 電話が積極的に採用されるようになってきているが、想定した通信品質が得られず、通話が途切れるなどの問題が発生する事例が少なくない。

本研究では、ネットワークの仕様記述（設計モデル）とネットワークセンサーにより作成したネットワークの現状（スナップショット）を検証することで、仕様記述にない不正な端末や不正な通信の検出、実際の通信品質が要求を満たしているかの検証を自動的に行うことが可能である。高いセキュリティーとネットワーク管理コストの低減が同時に図れるため、ネットワークの設計や管理コストの軽減が見込まれる。

５．実現方法

設計モデルの記述は、XML(Extensible Markup Language)(1)で、機器モデルの記述は、XSL(Extensible Stylesheet Language)で行う。機器モデルの記述は、設計モデルから実際の設定への変換ルールとして記述される。これまで、XML による設計モデルの記述と XSL による機器モデルの記述を行い、XSLT(XSL Transformations)による設定の生成が可能であることを確認する基礎的な実験を行ってきた。また、ネットワークの状態をモニタするためのネットワークセンサーの準備をほぼ終えており、ネットワークセンサーの出力から、現状のネットワークの仕様記述を生成する機能と、設計モデルとスナップショットとの検証ツールを準備中である。

６．おわりに

ネットワークを構成する機器やサービスを記述できるようなネットワーク記述言語を開発し、ネットワーク管理に応用することを提案した。これにより、ネットワークの設計・設定・管理（監視）を統一的に扱う枠組みが提供でき、管理コストの軽減が期待できる。

今後は、実験的なネットワークでの動作実験を行う予定である。対象とするネットワークの設計モデルを作成し、そこから生成した設定で、ネットワークを構成する機器を設定し、ネットワークセンサーを動作させる。この状態で、不正端末の接続や、不正な通信を行い、これらを検出できることを確認する。さらに、不正な通信ではないが、ネットワーク設計時よりも、負荷の高い通信を発生させ、仕様を上回る通信が発生していることを検出できるかも検証する。

参考文献

(1) XML: http://www.w3.org/XML/