IPv6 ネットワーク運用管理の課題と対応機能の実装

國分 俊介　　三浦 健次郎　　扇谷 篤志　　近藤 誠一
三菱電機株式会社　情報技術総合研究所

1. はじめに

IPv6 プロトコルが主要な OS に実装され、普及環境が整い始めている。IPv6 は広大なアドレス空間を持つことを特長とし、また、RFC2462 に規定されるステートレス方式のアドレス自動設定機能が標準サポートされるなど、ネットワークの接続が容易になっている。このため、企業ネットワークやセンサー・ビル管理等の専用ネットワークでの利用にあたっては、従来の IPv4 ネットワーク運用管理であまり問題にならなかった課題を検討しておく必要がある。

本稿では，企業ネットワーク等で IPv6 ネットワークを運用管理していくための運用管理上の課題を検討し、それを解決する機能を一部実装した結果を報告する。

2. IPv6 ネットワーク運用管理の課題と実装

2.1. アドレス自動発見

まず、ステートレス方式の自動設定方式を採用するネットワークでは、不正利用者に接続されやすいという課題[1]がある。

したがって、従来の IPv4 ネットワーク運用管理ではあまり重視されていなかったクライアント側の管理が重要になってくる。すなわち、接続されたホストインタフェースの（IP アドレス）自動発見・管理機能が重要である。発見機能の実装に当たっては、IPv6 ではアドレス空間が大きいため、一部の IPv4 管理製品等で採用されていた、アドレスの総当たり的検索・検出方法では限界がある。

実装方法はいくつか考えられるが、ステートレス方式では、IPv6 ルータがアドレス設定の基点となるので、ネットワーク管理装置からルータの IPv6MIB（RFC2465 等）を参照して、新規インタフェースのアドレス発見と全体状況を監視する方法を採用し、実装した。

2.2.認証システムとの連携

接続された端末のアドレスを発見するのみでは、正規利用者と不正利用者の区別は困難である。したがって、不正アクセスの監視という観点からは、なんらかの認証システムとの連携がネットワーク運用管理上重要となってくる。

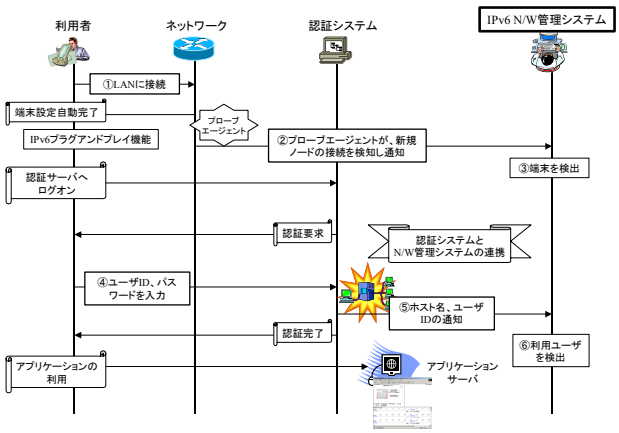

図 1　認証システムとの連携

連携する認証システムの候補としては、次のようなシステムがある。

(1) シングルサインオン認証システム
　WEB アプリケーションのシングルサインオンサーバやドメイン管理用認証サーバによる認証システムである。

(2) IEEE802.1x 認証システム
　現時点では標準化作業が終了していないが、ネットワーク（ポート）接続時に認証を行い、事前に不正利用者を排除するシステムである。

(3) 認証機能付き DHCPv6
　IP アドレス配布時に認証を行う方法で、いくつかの方式が提案されている。ステートフル方式の自動設定を使う場合に有効と考えられる。

今回は、(1)の方式による実装を行った。この場合の自動発見、認証の一連の流れを図 1 に示す。(2)、(3)の認証サーバと連携する場合は、ネットワーク接続時、アドレス取得時の認証処理後に、ネットワーク管理装置と連携し発見処理を行うという流れになると考える。

2.3. 障害検知

IPv6 はアドレス空間が広大であり、AS（Autonomous System：自律システム）に接続されるホストの数も多いと考えられる。このため、中央からのポーリングベース(PING)の障害検出

“The implementation of functions for IPv6 network operation and management”
Information Technology R&D Center, Mitsubishi Electric Corporation.

方法では、ネットワーク管理装置のポーリング負荷が増大するという問題が大きくなる。

したがって、ポーリングエンジンの分散化が重要である。IPv6 のステートレス自動設定方式ではルータが自動設定の基点であるので、ルータに、接続されたホストの状態管理を行うプローブモジュールを実装し、これをネットワーク管理装置と連携させる方法が有効であると考える。

2.4. 位置情報の管理

障害機器の設置場所特定や不正利用者が接続しようとしている場所の特定用途等、位置情報の管理も重要性が増している。

ネットワーク管理装置では標準 MIB（RFC1213 等）を利用し、IP ネットワークの論理的な構成情報を自動的に収集できる。しかし、機器の設置・接続場所について自動的に管理する効果的な実装は少なく、CAD 図面のオブジェクトと自動検出した論理マップ上の IP オブジェクトをリンクして管理する程度であった。

一方、位置情報を自動取得する方法としては、GPS や無線 LAN を用いた方法がある[2]。しかし、GPS では、緯度・経度など絶対位置を取得できる反面、屋内では電波が届かず IP ネットワーク管理用としては利用しづらい。無線 LAN の電波を利用し位置管理する方法は、屋内で使用が可能であるが、複数の無線 LAN アクセスポイントと位置情報管理サーバを事前設置する必要があり大がかりである点、現状では独自実装が多い点が難点である。また、無線 LAN 位置情報管理システムとネットワーク管理システムを連携させる方式については今後の課題であると考える。

今回の実装では、より簡易な位置情報を付加・利用する方式、すなわち、ルータ等の標準 MIB を利用する方式で実装した。本方式は、レイアウト情報をテキスト形式で標準化し、これを MIB として設定・収集した後、物理マップレイアウトに利用する。概要は以下の通りである。

(1) リンクに対する位置情報の設定

位置情報の設定はルータのリンク用標準 MIB を利用する。IPv6 ではネットワーク・スコープの最小単位は“リンクローカル”である。したがって、まず最小単位としての“リンク”の位置情報管理を検討した。

具体的には、ipv6IfDescr（IPv6MIB、RFC 2465）を利用した。ipv6IfDescr はインタフェースについての情報を設定する MIB であり、RFC の定義上フォーマットフリーであるが、この一部を位置情報用として定型化する。

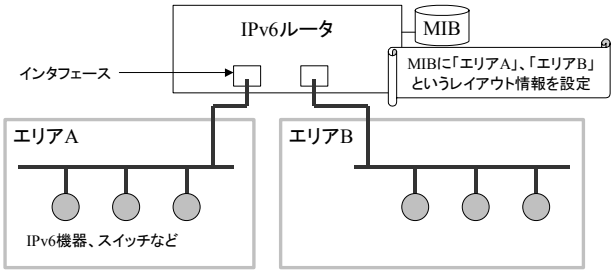

図 2　位置情報の管理

(2) レイアウト情報の定義内容

レイアウト情報の内容は、各インタフェースに接続されている機器が存在する場所を示す定型的な文字列等である。例えば図 2 のように、エリア A に存在する機器がルータのあるインタフェースに接続されている場合、そのルータの MIB（ipv6IfDescr）には「エリア A」を示す位置情報を設定する。

(3) 取得と利用

このようにルータの MIB に位置情報を設定しておけば、IPv6 ルータの各リンクの位置情報を SNMP プロトコルで取得することでリンク位置を集中管理できる。モバイル端末等がどのルータのリンクに接続したかを判断するのは容易であるから、事前に収集したリンク位置情報を参照することで、どの場所にあるリンク上で障害や不正接続がされたのかの判断を迅速化できる。

3. おわりに

本稿では，IPv6 ネットワークの運用管理をしていくための運用管理上の課題を検討し、それを解決する機能について提案を行った。また、一部機能については実装を行った。その結果、IPv4 ネットワークでの運用管理機能とは異なる機能も必要であることがわかった。

今後は残りの機能に関して実装を行い、評価を行っていく。また、IPv4 共存環境も含めたネットワーク管理上の課題も検討していく所存である。

参考文献

[1] 才所、他：IPv4/IPv6 ネットワークにおける不正端末検出システム、情報処理学会第 65 回全国大会講演論文集 5D-5(2003)

[2] 黒崎、他：無線 LAN を利用した位置情報システムの活用、COMPUTER & NETWORK LAN、11 月号(2003)