特定ドメイン管理を実現する為のクラウド型 PBNM 方式

Cloud type of PBNM for Managing a Specific Domain

小田切　和也（Kazuya Odagiri, Ph. D.）
椙山女学園大学　文化情報学部　文化情報学科　准教授
(Associate Professor, Sugiyama Jyogakuen University)
電子情報通信学会　情報処理学会

著書：Strategic Policy-Based Network Management in Contemporary Organizations, Cybertech Publishing (2016 年)　他

研究専門分野：情報ネットワーク　ネットワーク運用管理

あらまし

現在のインターネットは、自律分散型ネットワークであり、統一的に全体が安全・効率的に管理されていない。インターネットの仕組みをあまり理解していない利用者がインターネットに接続する場合､「個人情報の漏洩」、あるいは、「ネットワーク攻撃の踏み台利用」が発生する危険性が高い。一方、インターネット全体をある一定の管理状態に置くための研究は、現在行われていない。その点に対し、ポリシーに基づくネットワーク管理(PBNM)の考え方をインターネット全体に適用して管理する「インターネット PBNM」を長期的視野に立ち推進し、安全・効率的に管理されるインターネットの実現を目指している。4 段階(Step１～４）に分けて研究を進めており、本研究では、第３段階（Step3)としての「特定のドメインを管理するクラウド型 PBNM 方式」を実現の為の研究を行う。

１．研究の目的

本研究は、図１に記載したインターネット PBNM 方式を確立するための長期的な４ステップの研究の中で、第３段階に位置する研究である。図１の左側の（導入前）の図は、インターネット PBNM が導入される前、つまり、通常のインターネットにおけるネットワーク管理状態を模式的に示した図である。現状では、インターネットに接続されるコンピュータ（サーバやクライアント端末）は、個別的な管理状態に置かれ、個々のコンピュータの管理状態が一様ではなく、個人情報の漏洩の発生やネットワーク攻撃の踏み台とされてしまうなどの問題が頻繁に発生する。インターネット PBNM の導入によって、インターネット全域のコンピュータの管理状態がある一定水準に置かれた場合には、図１の右側の（導入後）に示した模式図のような形で、このような問題が、解決、あるいは、改善されることになる。具体的には、クラウド上に保存された提案方式におけるネットワーク通信の制御情報を、各コンピュータに配信・適用することで、各コンピュータ上の通信の出入りをある一定状態に制御することが可能になり、現在のインターネット全体の管理状態を大幅に改善することが可能になる。本研究では、インターネット上のある一定範囲である特定のドメイン（＝複数の組織がそれぞれ保有するネットワークを一纏まりにグループ化した「特定組織ネットワーク群」を、更に複数集めた管理範囲）を管理することが出来るクラウド型の方式の確立を図ることが、本研究の目的である。

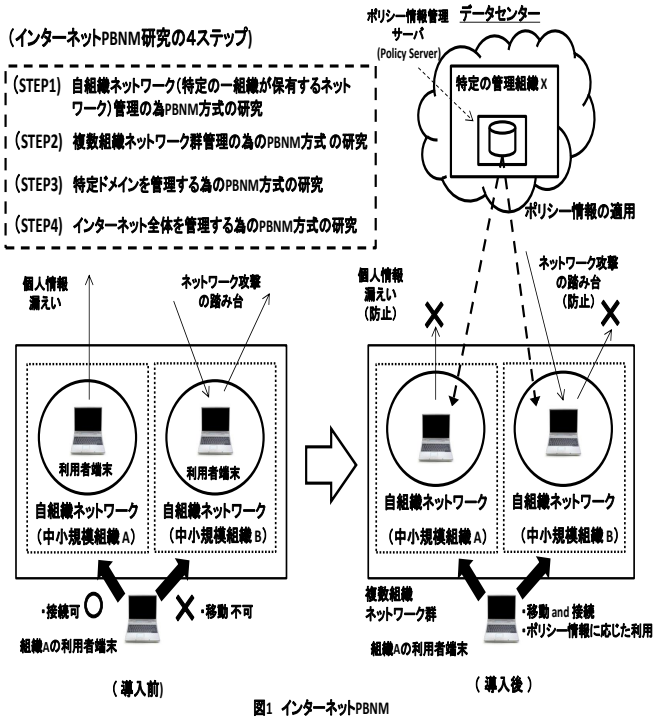

図1 インターネットPBNM

特定ドメイン管理を実現する為のクラウド型 PBNM 方式

Cloud type of PBNM for Managing a Specific Domain

２．研究の背景

既存 PBNM は、自組織のネットワーク・セキュリティポリシーに基づくネットワーク管理を実現する。サーバとクライアントの間の経路上に配置される通信制御機構(PEP)による通信制御(アクセス制御、通信の暗号化、QOS 制御など)を通して自組織ネットワーク全体を管理する。

自組織ネットワークを適用領域とする既存 PBNM は複数の組織で標準化されており、Internet Engineering Task Force(IETF)の PBNM に関係する標準としては、Policy Core Information model (PCIM)、Policy Core LDAP Schema、Common Open Policy Service (COPS)プロトコル、COPS usage for RSVP、COPS usage for Provisioning (COPS-PR)がある。他の組織での標準化の例としては、Distributed Management Task Force (DMTF)で策定された Directory-enabled Network (DEN)、European Telecommunications Standards Institute (ETSI)の Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN) により策定された Resource and Admission Control Subsystem (RACS)や、International Telecommunication Union Telecommunication Standardization Sector (ITU-T)で策定された Resource and Admission Control Functions (RACF)がある。

この既存 PBNM は、理論的には、複数組織ネットワーク群にも拡張可能である。しかしながら、研究論文として報告されておらず、PBNM の技術的構成要素であるアクセス制御[1]や QOS 制御[2]を個別に研究対象として取りあげて、複数組織で利用する為の研究が若干報告されている。複数組織ネットワーク群や特定ドメインに拡張されていない理由は、次に説明する(a)～(c)の理由が考えられるが、本研究と同じ目的・趣旨の研究は見当たらない。

図２に示した既存 PBNM は、PEP をネットワーク経路上に配置する為、ある管理組織が他組織ネットワークを管理しようとする場合、他組織が保有するネットワーク機器を変更する必要があり、(a)機器変更によるコストの発生、(b)既存 PBNM の適用時に発生する

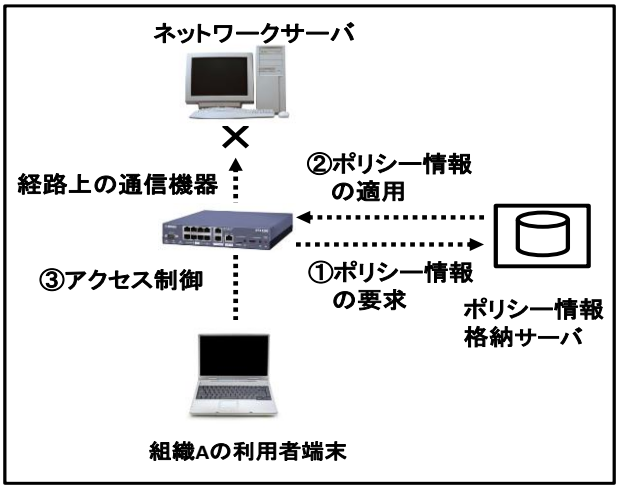

図2　既存PBNM

可能性があるネットワークトポロジ変更、(c)他組織による自組織ネットワーク機器の変更時に問題となるセキュリティポリシーやネットワークポリシー上の制限、という問題点により、機器変更が不可能な場合がある。インターネット全体の管理を前提とする場合は適用対象のネットワーク数が不特定の膨大な数となる為、これらの問題点により、全組織へ導入するのは困難となる。

そこで、図 1 の(Step1)として、「ネットワーク機器の変更が不要な自組織ネットワーク管理の PBNM 方式」を実現する為、ソフトウェア形態の PEP(DACS Client)を物理クライアント・仮想化クライアントに配置する「DACS 方式」を確立した。更に、その研究成果を元に、(Step2)の研究を進めている。具体的には、『特定の管理組織が PBNM の考え方を元に、クライアントの仮想化を前提とする「複数の異なる他組織がそれぞれ保有する LAN や WAN の集まり(複数組織ネットワーク群)」を管理するクラウド型 PBNM 方式』を確立した。

既存 PBNM の適用領域が、何故、複数組織ネットワーク群にまで拡大しないかを検討した結果、前述した(a)～(c)の問題点のうち、特に、(c)の問題点が致命的となっているとの結論に至った。その点を回避すべく、通信制御の制御点である PEP を、ネットワーク経路上からクライアントへ移動させる

特定ドメイン管理を実現する為のクラウド型 PBNM 方式

Cloud type of PBNM for Managing a Specific Domain

方式を発案した。（Step2）の方式は確立した。その成果を元に、本研究では、インターネット PBNM 実現に向けて、更なる提案方式の適用領域拡大を目的とし、（Step3）の研究を進めた。

ネットワーク経路上に PEP を配置する既存方式の場合は、「利用者により共通利用されるネットワーク機器」の変更が困難である可能性が高い。一方、クライアント上に PEP を配置する方式では、PEP を配置するクライアントにソフトウェアをインストールするだけで済む。更に、本方式は、仮想環境を前提とする為、ネットワーク管理者が、クライアントソフトウェアをインストールした「多数の仮想マシン（仮想サーバ上に実現される論理的なクライアントマシン）」を簡単に準備することが出来るため、利用者側では特に何の負担も発生しない。筆者は、PEP のクライアント側への移動が、適用領域の抑制要因を解消し、その結果、適用領域の拡大をもたらし、それが最終的には、インターネット全体にまで波及することになると考えている。（インターネット PBNM 実現への可能性が生まれたと考えている。）

更に、本方式では、クライアント上での通信制御機能の一つとして、Destination NAT(宛先 NAT)による「通信先サーバの変更機能」を備えている。例えば、本方式の通信プロトコルが標準化されて各種クライアント用 OS に標準装備されて本機能が広く一般に普及した場合、この機能によりクライアント上での通信制御に基づく「ネットワークの通信制御方式」が生まれ、現在の『ネットワーク経路上でのルーティング処理を中心とする「既存のネットワークの通信制御方式」』に機能付加する形態で、別の動作原理を持つネットワークが生まれる可能性があると考えている。現在は、図 1 の(STEP4)に記載した「インターネット PBNM」を目指して研究を進めているが、新しい動作原理を持つインターネットの実現が図られる可能性もあると筆者は考えている。その点も念頭に置きながら長期的に研究を推進している。

３．本研究の研究方法や内容等の説明

過去の研究成果を元に、本研究の提案方式を確立した。(a)図 5 に記載した開発・実験環境の構築、(b)方式の明確化、(c)方式実現に必要な方法・機能の要件の明確化、(d)要件の実性現担保の為の機能実験の実施、を行い、(c)の「方法・機能の要件」を図３に示した。

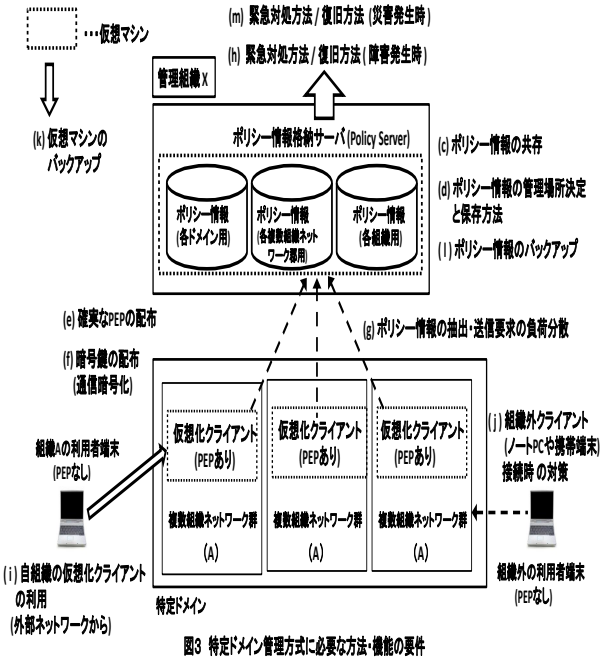

図3 特定ドメイン管理方式に必要な方法・機能の要件

この要件を満たす方式とするために、ユーザ認証の方式とネットワーク通信の制御情報の生成・配付方法（クラウド上の管理サーバにおけるネットワーク通信制御情報の生成・配付方法）を、本提案方式に適合するように機能拡張を行い、特定ドメインを管理する方式の確立を図った。具体的には、以下の 3.1 と 3.2 に記載する形で実装を行い、プロトタイプシステムを開発した。

なお、本提案方式を実際に中小規模組織に適用するための指標を導出するために行われる大規模負荷実験については、現在、実施中であるため、データのご紹介はできないが、実験終了後には、IEEE 関連の国際会議での発表や国際ジャーナル誌での発表を行う予定である。

3.1 ユーザ認証方式

本提案方式に適合するユーザ認証の方法としては、

そのユーザが属する複数組織ネットワーク群のネットワーク管理用の認証サーバに対して認証する方式とした。ユーザ認証の認証情報（ユーザ名・パスワード）がインターネットを経由する形となるので、SSL による暗号化をする形をとった。本提案方式の認証サーバとしては、フリーソフトウェアの OpenLDAP を使用している。その認証サーバに対する認証方法として SSL 対応の認証が行えるので、その機能を使用する形とした。今回は、実験環境内のシステム構築であるので、電子証明書は、自己証明書を利用する形としたが、実際のインターネット環境では、信頼できる認証局の証明書を使用する形にする必要がある。

3.2 ネットワーク通信の制御情報の生成・配付方法

前項に記載したユーザ認証プロセスの後に、各コンピュータに配布するネットワーク通信の制御情報の生成・配布機能が実行されることになる。

この機能の本質的な問題は、あるネットワーク通信が発生した場合に、その通信を制御するための制御情報が、そのユーザ自身が所属する複数ネットワーク群管理のためのものと、そのユーザ自身が実際に接続された別の複数組織ネットワーク群管理のためのものが重複する場合があるので、その部分の制御をどのようにするかという点である。この点については、後者の制御情報を優先して採用することで、この問題点の解決を図った。このような形で、前者と後者のネットワーク制御情報を最終的に一つにまとめることで、各コンピュータに適用する制御情報を生成する。そして、この制御情報を、クラウド上から各コンピュータにインターネットを介する形で配信して適用する。

この制御情報に基づいた形で、ユーザが接続した複数ネットワーク群全体の制御が行われる形となる。

４．将来展望

本提案方式の次の段階では、(Step4) のインターネット全域を管理範囲とするインターネット PBNM に拡張を行う予定である。そして、更に、その先の研究としては、Internet of Things (IOT) や Artificial Intelligence (AI) などの技術を取り入れる形でのサーバーフィジカル型インターネット PBNM への拡張を行う予定である。現在のインターネット PBNM では、各管理範囲に存在する管理者が、提案方式における管理サーバ上に通信制御情報を設定し、その通信制御情報が各コンピュータに送信・反映される形で最終的にインターネット全域が制御される形を想定している。その管理者による制御の部分を自動化するとともに、世界中のインターネットを介して得られる細かな情報を元に制御されるような方式に進化させることで、より柔軟で安全な方式を実現することができると考えている。

また、本研究の提案方式を導入したネットワーク上では、次の図４に示すネットワーク管理手法の創出につながると考えている。

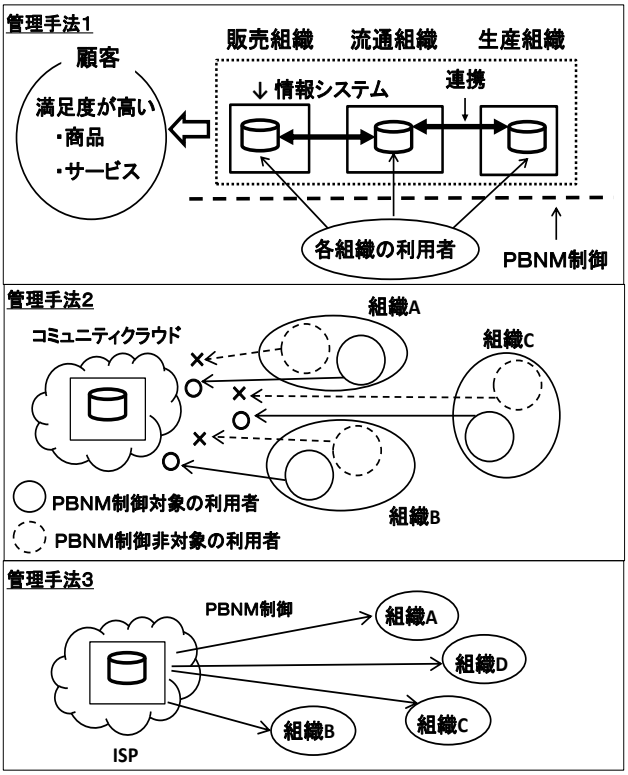

図4 PBNM管理手法

（管理手法 1） Supply Chain Management (SCM)における情報システムのような「複数の組織に跨って構築した情報システム」を守る為に、アクセス元クライアントのネットワークへの接続状態を同一に維持管理する管理手法である。

特定ドメイン管理を実現する為のクラウド型 PBNM 方式

Cloud type of PBNM for Managing a Specific Domain

(管理手法 2)コミュニティクラウド(複数の組織で共通利用されるクラウド)を守る為に、アクセス元の組織のクライアントが属するネットワークへの接続状態を同一に維持管理する管理手法である。

(管理手法 3) Internet Service Provider (ISP)による「ネットワーク・セキュリティの担当者をおけない中小規模の組織」のネットワーク管理手法である。

おわりに

本提案方式の研究は、インターネット PBNM 方式実現のための第３段階（Step3）に位置する研究である。システム要件の検討、プロトタイプシステムの実装、機能実験を行い、提案方式の機能的実現性まで確認を行った。現在、実施中の大規模実験を完了させて、中小規模組織のネットワークが集まる形の複数組織ネットワーク群が更に集まる形の特定ドメインの管理を実際に行うことが出来ることの証明を行う予定である。

参考文献

[1] 市川本浩，河合栄治，藤川和利，砂原秀樹．インターネットにおける組織間システム連携時のアクセス制御に関する考察．情報処理学会 分散システム/インターネット運用技術研究会，2005 年 8 月．

[2] Mohan Baruwal Chhetri,Bao Quoc Vo,Ryszard Kowalczyk.Policy-Based Management of QoS in Service Aggregations,IEEE/ACM International Conference on Cluster, Cloud and Grid Computing,2010.

この研究は、平成２８年度ＳＣＡＴ研究助成の対象として採用され、平成２９～令和１年度に実施されたものです。