クラウド型 PBNM 実現の為のソフトウェアに関する研究

研究代表者　　小田切　和也　　山口大学大学情報機構メディア基盤センター・准教授

1 はじめに

1-1 本研究の位置づけ

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、Policy-based Netwoek Management(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（図 1 の右側）の研究」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。図 1 の 4 ステップで研究を進めており、本研究は(Step1)の最終段階と(Step2)の開始段階の研究である。

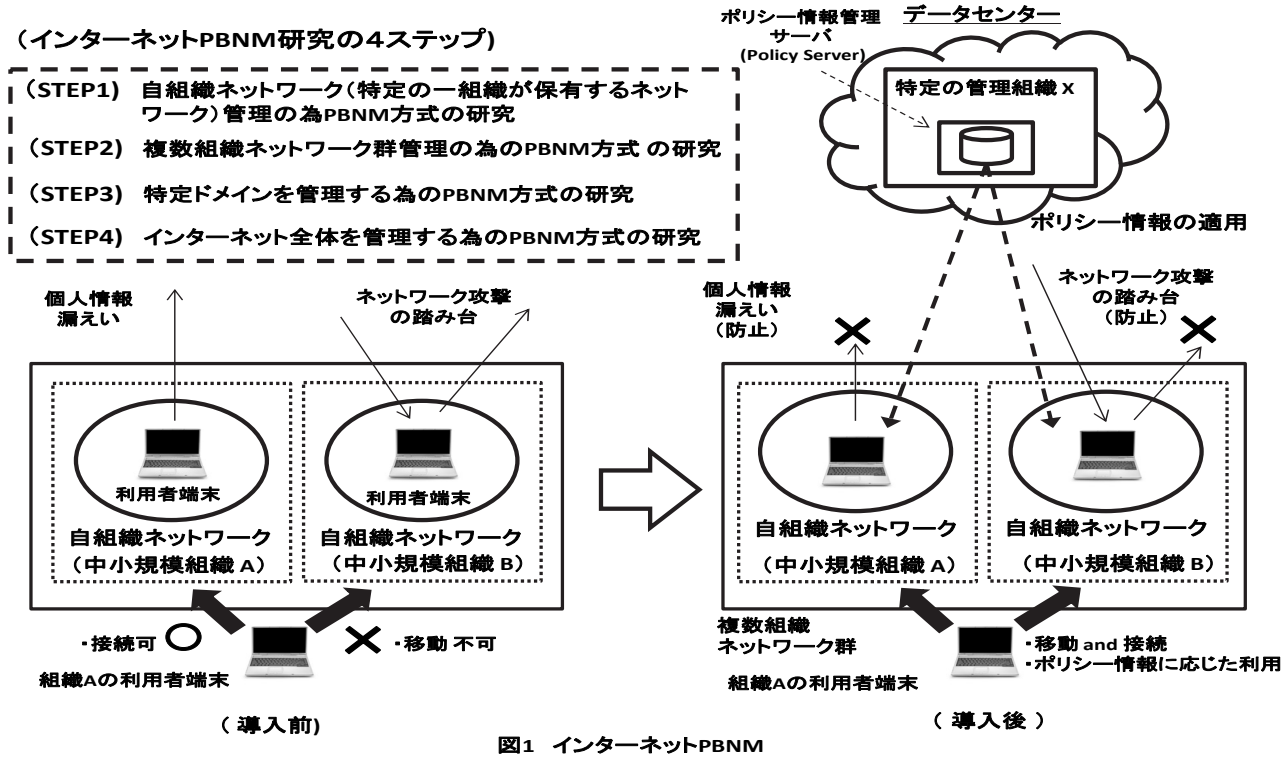

図1　インターネットPBNM

1-2 既存の PBNM

既存の PBNM は､自組織のネットワークポリシーや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ものである(図 2)。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である Policy Enforcement Point(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、ある特定の一組織のネットワーク(自組織ネットワーク)全体を管理する。この既存の PBNM は、複数の組織で標準化されている。

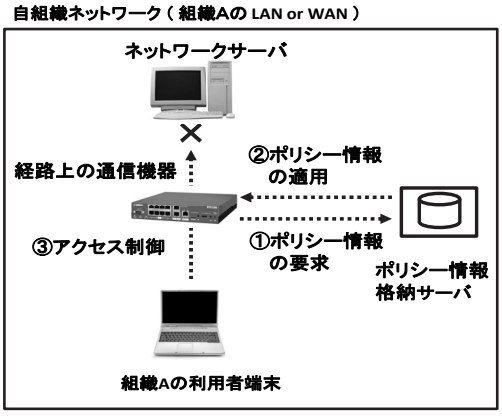

図2　既存PBNM

具体的には、ポリシーサーバに格納される制御情報のモデルとして、ポリシー・コア情報モデル(Policy Core Information model：PCIM)[1]が策定された後、拡張版である PCMIe が策定された。その後、PCIM(e)を、LDAP 形式で記述出来るように、Policy Core LDAP Schema[2]が策定され、ポリシーサーバに格納された制御情報をネットワーク機器に配布するプロトコルとして、Common Open Policy Service (COPS)プロトコル[3]が策定された。そして、COPS プロトコルにおける制御情報の配布方法の違いに対応して、COPS usage for RSVP[4]と COPS usage for Provisioning (COPS-PR)[5]が策定された。前者は、アウトソース方式と呼ばれる配布の方式である。PEP がユーザやクライアントアプリケーションからの通信を検知した後に、Policy Decision Point (PDP)がポリシーに従った判断を行い、その判断結果を、PEP に送信して通信制御が行われる。後者は、プロビジョニング方式と呼ばれる配布の方式である。ユーザやクライアントアプリケーションからの通信が発生する前に、あらかじめシステム管理者やネットワーク管理者が、PEP に対してポリシー情報や PDP の決定を通知しておく方式である。この COPS-PR プロトコルで運ばれるポリシーの形式は、Policy Information Base(PIB)と呼ばれ、Structure of Policy Provisioning Information (SPPI)と呼ばれる構文に基づいて記述される。Request for Comments (RFC)として策定されている PIB には、共通的に利用される Framework Policy Information Base や､QOS 制御の為の Differentiated Services Quality of Service Policy Information Base がある。

また、Distributed Management Task Force (DMTF)では、Directory-enabled Network (DEN)と呼ばれる PBNM のフレームワークが策定されている。具体的には、Lightweight Directory Access Protocol (LDAP)などのディレクトリサービスを使用して構築されるポリシーサーバに、アクセス制御や QOS 制御などに必要な制御情報を格納しておき、それらを LAN 上に分散配置されるネットワーク機器(スイッチやルーターなど)へ配信・適用することで、ネットワーク全体を効率的に管理する。その DEN で用いられる制御情報モデルは、CIM と呼ばれ、そのスキーマ (CIM Schema Version 2.30.0) [6] が公開されている。CIM は、DEN に対応するように拡張が為された後、DEN のフレームワークに組み入れられた。

上記以外の標準としては､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)[7]や、International Telecommunication Union Telecommunication Standardization Sector (ITU-T)で策定された Resource and Admission Control Functions (RACF)[8]がある。

また、最近の PBNM のフレームワークに関係する研究としては、モバイルアドホックネットワークに PBNM を適用する研究やホームエリアネットワークに PBNM を適用する研究、PBNM に対応する Service Level Agreement SLA)管理に関する研究などがある。

1-3 既存方式の研究と問題点・本研究の実施事項

上記の既存の PBNM は、PEP をネットワーク経路上に配置する方式である為、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、その場合、以下の(a)～(c)の問題点が派生する。

(a)機器変更によるコストの発生

(b)既存の PBNM の適用時に発生する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

以上の問題点により、ネットワーク機器の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、特に、(c)の問題点の影響が大きく、全ての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に配置する「DACS 方式」を確立した。

(Step1)における既存の DACS 方式の研究項目は、主に、以下の①～⑥である。

①方式の原理提案 [9]

②Virtual Private Network(VPN)を用いた PEP 非配置の物理クライアントからの通信に対するアクセス制御機能［10］

③物理クライアントの台数増加による処理負荷シミュレーション[11]

④DACS 方式実現の為のソフトウェア開発[12]

⑤WAN 型の自組織ネットワーク管理方式［13］

⑥運用管理システム[14]

これらの研究成果を元に、本研究では、(Step1)の最終段階に位置する研究として、PEP(DACS Client)を仮想クライアントに配置する「DACS 方式」の確立を行った。本研究において、物理クライアントを前提とする方式から仮想クライアントを前提とする方式に移行する理由として、(Step2)の研究で実現予定の方式がクラウド型の方式になる為、その予備的研究的意味合いも含まれる為である。

更に、(Step2)の研究への接続として、クライアントの仮想化を前提とした「複数組織ネットワーク群」の管理方式の検討を行った。具体的には、想定される一部の機能要件の導出・検討などを行った。

1-4 (Step2) における将来展望

参考までに説明すると、(Step2)の研究で、既存の PBNM 研究の適用領域が自組織ネットワークから複数組織ネットワーク群へ拡大し、複数組織を対象とするネットワーク管理でも有効になり、下記に記載した「データセンター用のクラウド型 PBNM 管理手法」(図 3)の創出に繋がると考えている。

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

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、アクセス元の各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

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

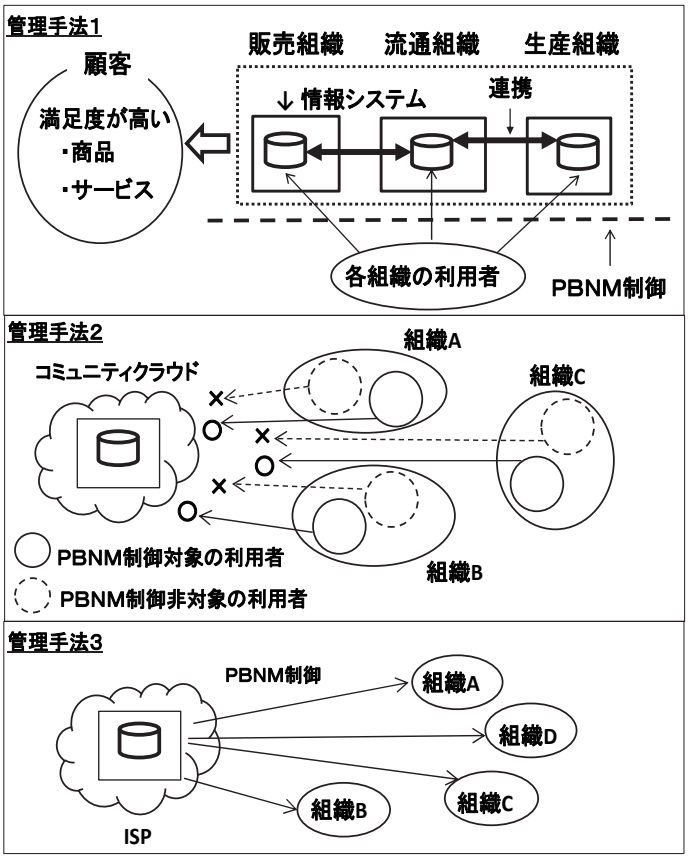

図3 PBNM管理手法

2 クライアントの仮想化を前提とした「自組織ネットワーク全体」の管理方式の確立

2-1 PEP の物理クライアントへの配置により発生する「利用者側の作業コスト」の解消

過去に開発した DACS 方式実現の為のソフトウェアである DACS システムを、仮想環境上で稼働させることで、PEP をクライアントへ配置する為に発生する利用者側の作業コストが不要になることを証明した。具体的には、下記に記載した実験用システムを構築し、機能実験を実施した。実験前は、「仮想環境で DACS システムを稼働させることによる問題点の発生」を想定したが、機能上の問題点は発生しなかった。

(実験システムの概要)

本研究で構築した実験システムの内容を図 4 に示した。VMWare ESXi5.1 を搭載した仮想サーバを 2 台準備し、各仮想サーバを以下の構成とした。

(1) 仮想サーバ 1 (CPU : 2.8GHz 4Core×1 メモリ:16GB)
仮想化基盤ソフトウェア : VMWareESXi5.1
仮想マシン A :
Operating System (CentOS6.5)
DACS Server 用ソフトウェア
仮想マシン B :
Operating System (CentOS6.5)
認証サーバ (OpenLDAP2.4)
仮想マシン C :
Operating System (CentOS6.5)
Windows ドメインサーバ(Samba3.6)
ゲートウェイ仮想ルーター(yatta6.6 : 64bit)

(2) 仮想サーバ 2 (CPU : 2.6GHz 4Core×1 メモリ:16GB)
仮想化基盤ソフトウェア : VMWareESXi5.1
各仮想マシン(5 台) :
Operating System (Windows XP Pro)
DACS Client 用ソフトウェア
ゲートウェイ仮想ルーター(yatta6.6 : 64bit)

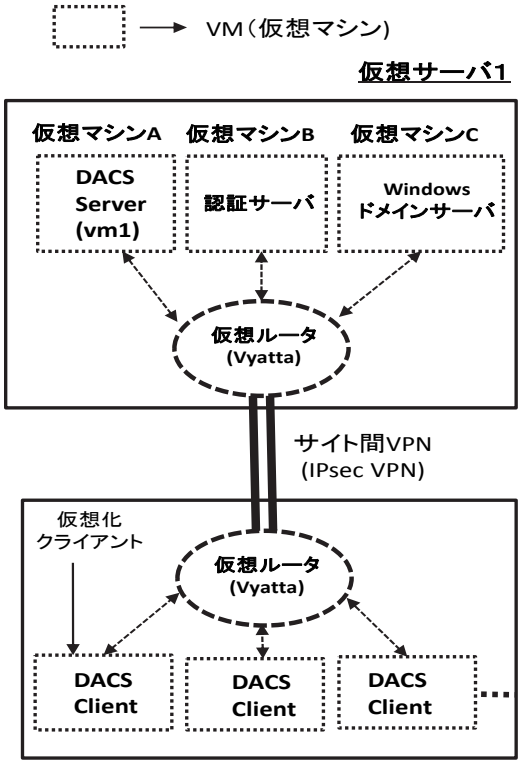

図4 本研究の実験環境

本方式をクラウド環境におけるサービスとして提供することを想定し、各サーバ上に配置した仮想ルーター間を IPsec VPN で接続した環境を準備した。仮想サーバ 1 上に配置された DACS 方式におけるサーバ(DACS Server)を配置し、仮想サーバ 2 上に、各利用者が使用するクライアントマシンに見立てた仮想マシンを配置し、PEP である DACS Client を配置する環境とした。DACS Server と DACS Client は、仮想ルーター間で接続された VPN 経由でポリシー情報の受け渡しを行う。

(機能検証の内容)

図 4 の実験環境を用いて、DACS システムにおける下記(a)(b)の 2 機能についての機能実験を実施した。

(a)ユーザ認証機能

本実験環境では、クライアント側 OS として Windows XP Pro を使用しており、更に、将来的に広く一般に無償公開していく方針を取っている為、フリーソフトウェアによるユーザ認証機構を採用している。具体的には、下記 2 種類のサーバの連携によるユーザ認証機能を使用している為、図 1 の仮想サーバ 2 上の各クライアントと、仮想マシン 1 上の仮想マシン B の間でユーザ認証の処理プロセスが発生する。

・ユーザアカウントの管理を行う為のディレクトリサーバである OpenLDAP サーバ

・Windows ドメインを構築する為の Samba サーバ

(b)ポリシー情報の受け渡し機能

本方式では、(a)のユーザ認証機能の処理プロセスが終了後に、仮想サーバ 2 上の DACS Client と仮想サーバ 1 上の DACS Server 間の連携によるポリシー情報の受け渡しが行われる。

具体的には、以下の 2 ケースの動作実験を行った。クライアント 1 台の場合の動作機能検証と、クライアント複数台による同時アクセスを確認する為の動作機能検証を実施した。

(ケース 1) 仮想サーバ 2 上に仮想マシンを 1 台のみ稼働させる場合

(ケース 2) 仮想サーバ 2 上に仮想マシンを複数台(5 台)稼働させる場合

(機能検証の結果)

(ケース 1)・(ケース 2)共に、機能的な問題は一切発生せずに問題なく稼働した。それにより、従来物理クライアントを前提としていた方式が、仮想クライアントを前提とする環境にも技術的には適用可能であることを実証することが出来た。

但し、実験システムの構築時に、仮想サーバ 2 における仮想マシンを複数準備する際に、特別なツールを使用せずに、VMWareESXi の機能を使用する形で、手作業にて複製を行った。多数のクライアントを複製・管理する場合には簡素化するツールが必要であると判断出来たので、無償公開に備えて、オープンソースのクラウド基盤管理ソフトウェアである OpenStack や CloudStack の調査を進めて､本方式に適合する利用方法を確立する必要がある。この点については、本研究終了後に、別の研究テーマとして進める予定である

2-2 管理可能なクライアント台数の特定実験

(実験方法)

前述の機能実験で使用した実験環境を用いて、DACS Server と DACS Client 間で行われるポリシー情報の受け渡し処理プロセスの同時実行により発生する「DACS Server 側で発生する処理負荷」の測定実験を行った。実験環境の仮想サーバ上の仮想マシンを 100 台に増加させて、10 分間隔で同時に測定対象の処理プロセスを実行し、その時の仮想サーバ 1 上の DACS Server を配置した仮想マシン A 側で発生した処理負荷(CPU 処理速度の最大値)についての測定を実施した。(但し、仮想サーバ 1 の制約により、全ての仮想マシンを配置できなかった為、一部の仮想マシンは、仮想サーバ 2 上に配置した。) 測定方法は、VMWareESXi の標準で装備されているパフォーマンス測定機能を使用した測定を行った。(その時のメモリ使用状況を確認した所、十分な容量が残っており、測定上は問題にはならない点を確認済である。) 測定回数は、10 回実施した。各回の CPU 処理速度の最大値を、下記の表 1 に記載した。全 10 回の測定値の平均値は、55.9MHz となった。

測定回	1	2	3	4	5	6	7	8	9	10
測定値(MHz)	59	58	51	58	59	59	53	51	53	58

表1　DACS Server側における処理負荷測定結果

また、参考までに、VMWareESXi から採取した第 1 回目～5 回目までの CPU 使用率の測定結果のグラフを図 5 に記載した。

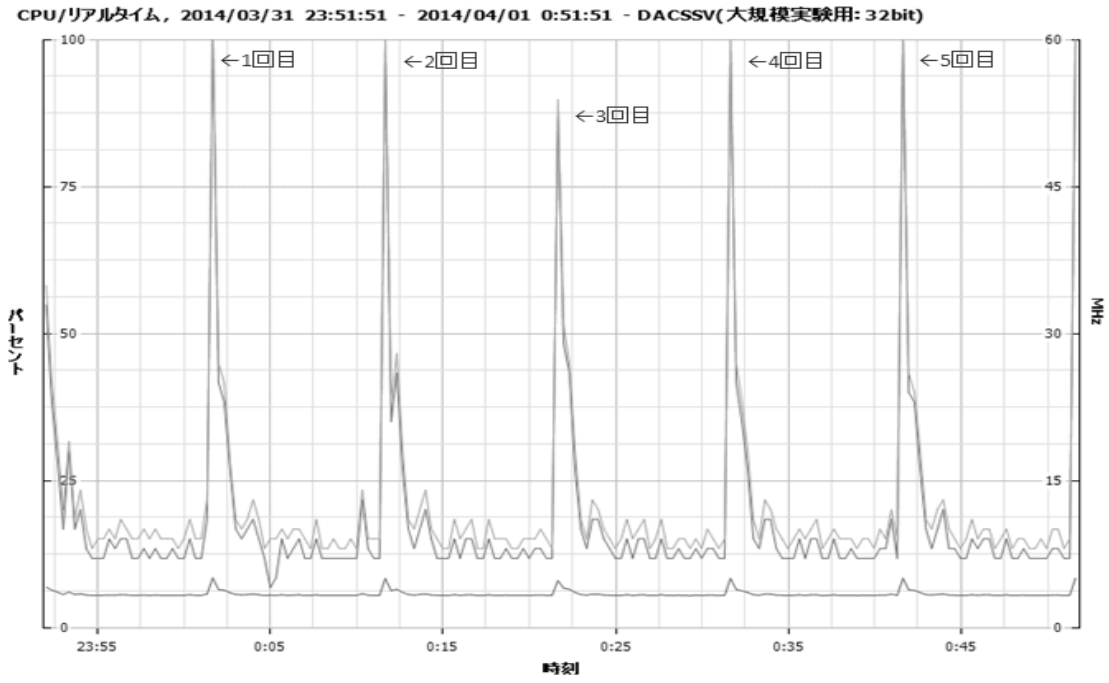

図5 CPU使用率測定結果(1～5回目)

また、第 6 回目～10 回目までの CPU 使用率の測定結果グラフも、図 6 として記載した。

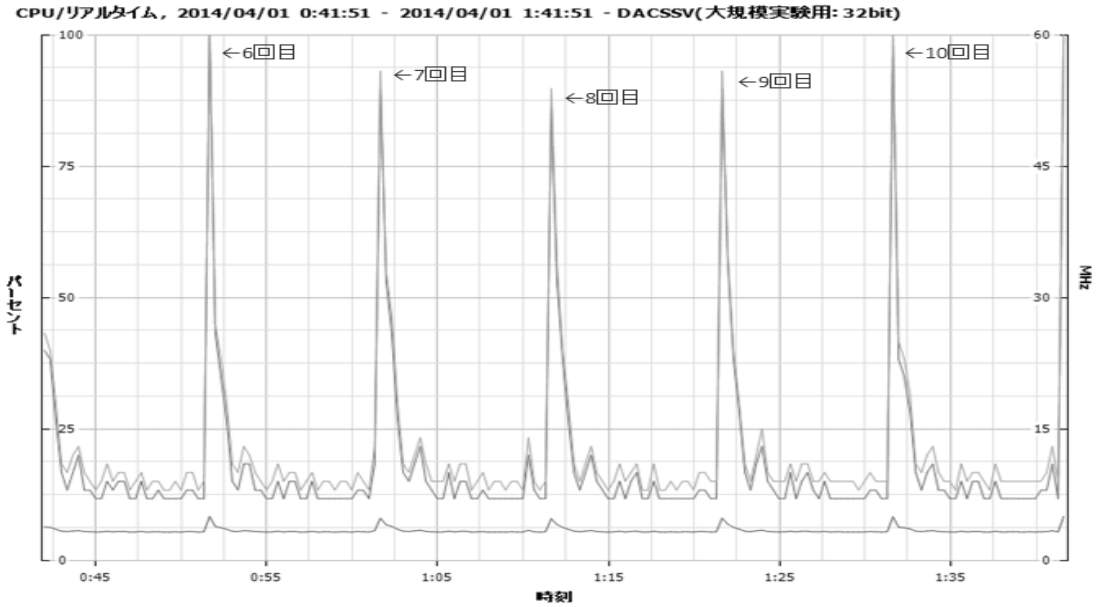

図6 CPU使用率測定結果(6～10回目)

(注) 上記の図 5・6 は、VMware ESXi の画面から採取したハードコピーを元に作成した図である。

上記の実験結果より、クライアント 100 台の条件下で、DACS Server と DACS Client 間で行われるポリシー情報の受け渡し処理プロセスの同時実行により発生する「DACS Server 側で発生する処理負荷」は、56MHz 程度となり、当初考えていたよりも低い値が得られた。この値は、DACS Server を配置した仮想サーバ 1 の CPU(2.8GHz)の約 50 分の 1 である。今回の実験環境は、閉じられた単純なネットワーク構成を取っている為、実際のネットワーク環境との違いはあるものの、理論的には、50×100=5000 台程度のクライアント用仮想マシンからの同時並列的な処理に耐えられることになる。但し、仮想マシン 2 の CPU のコア数を増やした場合には、同条件の実験で得られる CPU 使用率の最大値が上昇することが予想される為、その点については、別途実験環境を整備し、追加実験による検証を行う予定である。更に、可能であれば、上記の 5000 台に出来るだけ近い台数での処理負荷実験も実施したいと考えている。

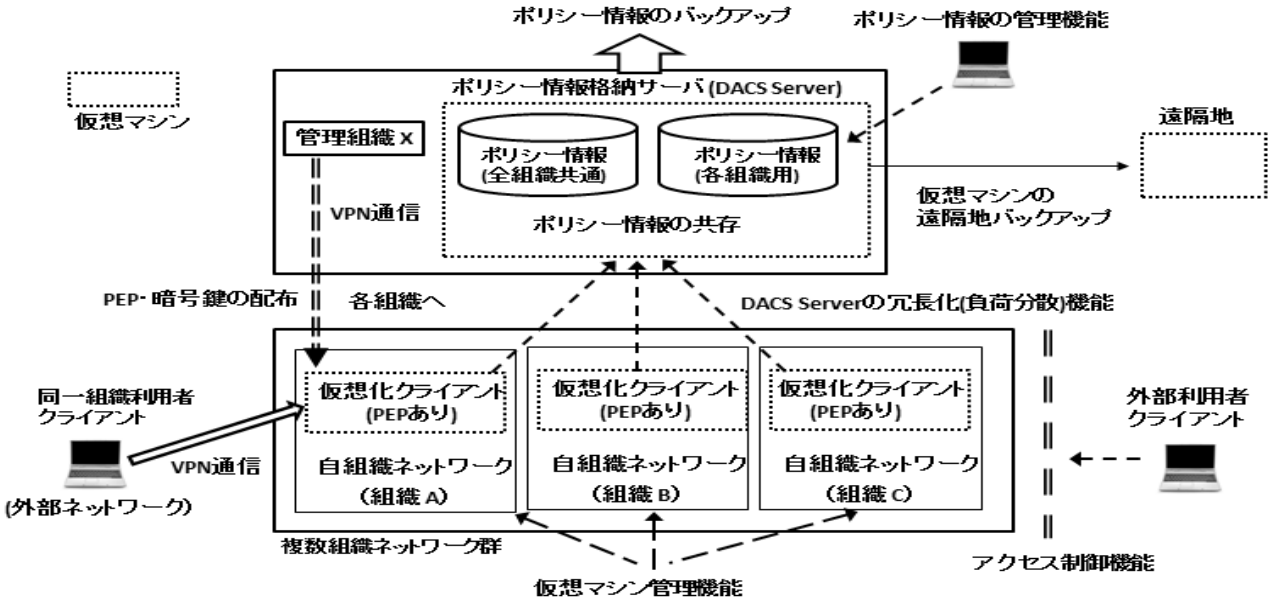

図5 新方式に必要な方法-機能の要件

3 クライアントの仮想化を前提とした「複数組織ネットワーク群」の管理方式の検討

2. の研究と同時並行的に、複数組織ネットワーク群を管理する新方式実現に必要となる方法・機能要件の検討と、下記(1)～(5)に記載した一部の必要機能の導出を行い、実現性を担保する為に必要と思われる技術調査、もしくは、機能実験を実施した。上記図 5 は、新方式実現に必要となる方法・機能要件のイメージ図である。但し、時間的な問題もあり、全ての要素について検討を行った訳ではなく、今後、実験環境を整備して詳細な検討を継続的に実施する予定である。)

(1)複数組織で共通利用出来るポリシー情報の内容・管理機能(バックアップ機能含む)

「ポリシー情報の共存」を行う為には、複数組織で一意に識別出来るユーザ名を決定する必要があるが、その点は、インターネットドメイン名を使用し、例えば、「ユーザ名@ドメイン名」とし、そのユーザ名を含むアカウント情報は、フリーソフトウェアである OpenLDAP を用いて管理する方法を想定している。

(2)ポリシー情報格納サーバである DACS Server の遠隔地バックアップ機能(BCP 対策)

本方式は、仮想化を前提とする方式であるので、バックアップも仮想マシン単位でのバックアップを行い、BCP 対策を行う。仮想マシンによる遠隔バックアップについては、Sceience Information NETwork (SINET)4 を経由する形で、VMWareESXi を使用した技術確認の為の機能実験を行った。具体的には、仮想マシンのスナップショットを毎日遠隔地の VMWareESXi 上に VPN 経由でコピーする実験を 1 ヶ月間実施し、問題なく運用可能であることを確認している。

(3)DACS Server と DACS Client 間の VPN 通信に利用する暗号鍵の配布方式・機能

この点については、以下の 2 通りのケースを検討した。

(ケース 1) DACS Server の冗長化を行わない場合

物理クライアントを前提とする既存の DACS 方式を Wide Area Network 上へ展開する方法の検討[13] を行った際に、VPN を経由する形での暗号鍵の配布方法を検討しており、その方法を適用・拡張する予定である。

(ケース 2) DACS Server の冗長化を行う場合

(6)に記載した仮想アプライアンスの負荷分散装置を用いる場合には、SSL アクセラレーション機能を利用する形での暗号鍵の配布方法を検討する。これについては、(6)の機能を組み込む必要があるので、その際の研究項目とする。当面は、本機能以外の(1)～(5)の機能を優先して、今後の研究を進めていく予定である。

(4)管理対象外クライアント(外部利用者用クライアント)の接続時のアクセス制御機能

過去の研究において、DACS Client を配置していない物理クライアントが、DACS Server にアクセスしてきた場合のアクセス制御法を確立しているので、その方法を適用する予定である。但し、仮想化を前提とする方式とした場合に、その機能の動作検証を行った実績がないので、実験環境を用いた検証が必要となる。検証結果に問題があれば、プログラムの修正、もしくは、別の対処方法の検討を行う。

(5)同一組織利用者による外部ネットワークからの仮想化クライアントの利用方法・機能

これは、具体的には、DACS Client を配置していない物理クライアントを使用する組織内部の利用者が、組織外部のネットワークから DACS Client を配置している仮想マシンへアクセスする方法・機能である。物理クライアントの OS が Windows の場合は、リモートデスクトップ機能を使用することにより、VMWareESXi 上の WindowsOS へアクセス出来る。但し、現時点では、本方式の実験環境を用いた確認までは行えていない。また、物理クライアントとして、他の OS を使用する場合にどのような利用法があるかの調査も含めて、今後、実証実験を行う予定である。

(6)ポリシー情報格納サーバである DACS Server の冗長化(負荷分散)機能

この点については、仮想アプライアンスの負荷分散装置を使用することを想定している。例えば、F5 社の BIG-IP LTM Virtual Edition や Brocad 社の Brocade Virtual ADX のような商用製品がある。可能な限り、商用製品の利用は控えてフリーソフトウェアの活用を考えたいと考えているが、今後、仮想アプライアンスの負荷分散装置に関する調査を継続的に進め、世の中の動向を見極めながら、本機能を組み

込みたいと考えている。但し、当面は、本機能以外の(1)～(5)の機能を優先して、今後の研究を進めていくこととする。

【参考文献】

[1] B. Moore at el., "Policy Core Information Model -- Version 1 Specification", IETF RFC 3060, 2001.

[2] J. Strassner at el., " Policy Core Lightweight Directory Access Protocol (LDAP) Schema", IETF RFC 3703, 2004.

[3] D. Durham at el.,"The COPS (Common Open Policy Service) Protocol", IETF RFC 2748, 2000.

[4] S. Herzog at el.,"COPS usage for RSVP", IETF RFC 2749, 2000.

[5] K. Chan et al.,"COPS Usage for Policy Provisioning (COPS-PR)", IETF RFC 3084, 2001.

[6] CIM Schema: Version 2.30.0, 2011.

[7] ETSI ES 282 003: Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN); Resource and Admission Control Subsystem (RACS); Functional Architecture, June 2006.

[8] ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specifica-tion", April 2006.

[9] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, ”Efficient Network Management System with DACS Scheme：Management with communication control,” Int. Journal of Computer Science and Network Security, Vol.6,No.1, pp30-36,January,2006

[10] Kazuya Odagiri, Rihito Yaegashi, Masaharu Tadauchi, Naohiro Ishii, “Secure DACS Scheme,” Journal of Network and Computer Applications, Elsevier,Vol.31, Issue 4, pp.851-861, November, 2008.

[11] Kazuya Odagiri,Giuseppe De Marco,Rihito Yaegashi,Masaharu Tadauchi,Naohiro Ishii “The Processing Workload Evaluation in two Network Management Models of IP Networks,” Journal of Convergence Information Technology, Volume 4, Number 3, pp.7-16, September 2009.

[12] Kazuya Odagiri, Shougo Shimizu, Rihito Taegashi, Makoto Takizawa, Naohiro Ishii, "DACS System Implementation Method to Realize the Next Generation Policy-based Network Management Scheme," Proc. of Int. Conf. on Advanced Information Networking and Applications (AINA20010), Perth, Australia, IEEE Computer Society, pp.348-354, May, 2010.

[13] Kazuya Odagiri, Shogo Shimizu, Makoto Takizawa, Naohiro Ishii, "Theoretical Suggestion of Policy-Based Wide Area Network Management System (wDACS system part-I)," Proc. of International Conference on Network-Based Information Systems (NBIS2012), pp. 268-275, September, 2012.

[14] Kazuya Odagiri,Shogo Shimizu,Naohiro Ishii, "Technical points in the implementation of the support system for operation and management of DACS system," Proc. of Int. Conf. on Networking and Services (ICNS2013) IEEE Computer Society, pp.16-21, May, 2013.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Theoretical Suggestion of Policy-Based Wide Area Network Management System (wDACS system part-I)	International Journal of Networked and Distributed Computing, Volume 1, Issue 4, pp. 260-269.	2013 年 11 月