様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月　 ５ 日現在

機関番号：３３９０６
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１１３

研究課題名（和文）インターネット管理方式実現に向けた特定ドメインの新規管理手法の確立

研究課題名（英文）Establishment of new management method of specific domain for realizing Internet management system

研究代表者
小田切　和也（Odagiri, Kazuya）

椙山女学園大学・文化情報学部・准教授

研究者番号：３０４４９４９１

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本提案方式の前段階の方式である「複数組織ネットワーク群管理方式」の拡張方式である。この前段階の方式からの主な拡張部分は、ユーザの認証・ポリシー情報の生成・配布の方法の２点である。ユーザ認証方式は、複数の組織がそれぞれ保有するネットワーク群を管理する外部組織を設けて管理する方式とした。ポリシー情報の生成・配布方式は、利用者が所属する複数組織ネットワーク群で管理するポリシー情報と、利用者がノートPC等の移動端末を持って接続した異なる複数組織ネットワーク群で管理するポリシー情報の間でマッチングを行う方式とした。その後、ソフトウェア設計・開発・機能評価・大規模実験による性能評価を実施した。

研究成果の学術的意義や社会的意義
本提案方式の研究により、前段階の「複数組織ネットワーク群管理のための方式」の管理範囲を拡張することが出来るようになった。具体的には、この前段階の方式で管理する範囲が複数独立して存在する場合に、自律分散型で全体を管理する方式を確立した。そのことによって、今後、管理範囲をインターネット全域に拡張するための前段階の準備を整えることができた。

研究成果の概要（英文）：This is an extension of the "multi-organization network group management method" that is the previous step of the proposed method. The two major extensions from the previous method are the method of user authentication and the generation and distribution of policy information. The user authentication method is a method in which an external organization that manages a network group owned by each of a plurality of organizations is provided and managed. Distribution method of the policy information generation is based on the policy information managed by the multiple organizational network groups to which the user belongs and the policy information managed by different multiple organizational network groups to which the user is connected with a mobile terminal such as a laptop PC. The method of matching between the two is adopted. After that, software design and development, function evaluation, performance evaluation by large-scale experiment was conducted.

研究分野：情報ネットワーク

キーワード：ポリシーに基づくネットワーク管理

１．研究開始当初の背景

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」､や「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。そこで､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(Step3)の研究である。

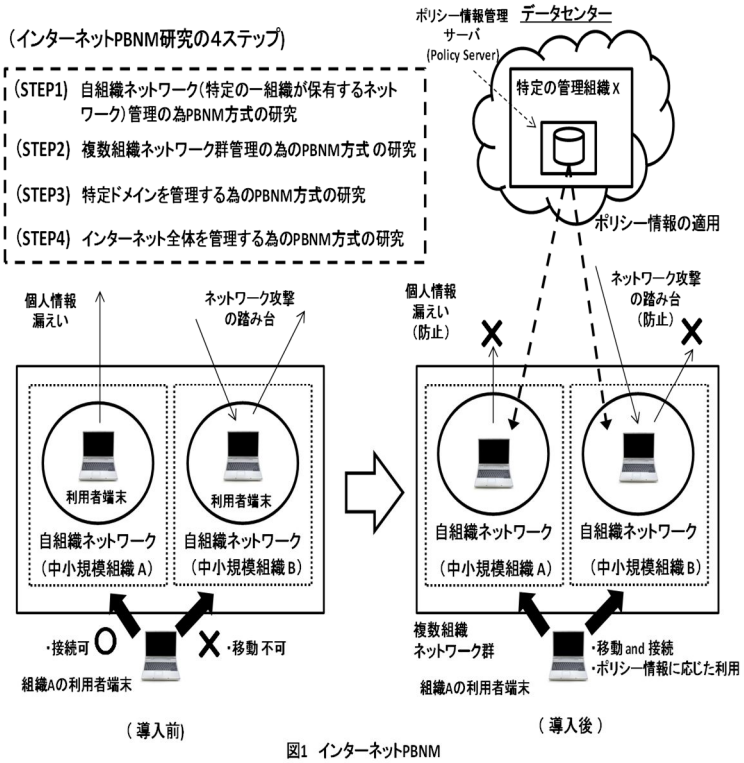

図1 インターネットPBNM

(Step1)に相当する既存 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(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(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。IETF (R. Yavatkar at el. IETF RFC 2753, 2000)や DMTF (DMTF, DSP0123,2002) など複数の組織で標準化されている。この既存 PBNM は、元々、自組織ネットワークを管理する為のものであるが、理論的には、(Step2)に相当する「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。

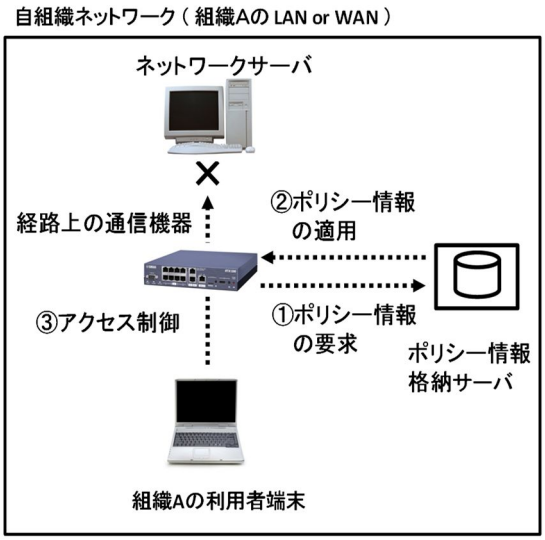

図2　既存PBNM

２．研究の目的

申請者は、これまで第１段階・第２段階の研究を実施し、提案方式の適用領域を、個別組織から複数組織に拡大し、複数組織ネットワーク群管理の為の方式を確立した。本研究では、適用領域を拡大する第３段階の研究である「特定のドメインを管理する目的の研究」を実施した。本研究では、以下の項目を実施した。

(1) 特定ドメインに適用可能な「複数組織ネットワーク群」管理の為のクラウド型 PBNM 方式の明確化
(2) (1)の方法の実現性担保の為のソフトウェア設計・開発・機能評価
(3) 大規模通信負荷実験によるソフトウェア性能評価

３．研究の方法

以下の方法で研究を実施した。

(1) クライアント仮想化を前提とする「特定ドメイン」管理の為のクラウド型 PBNM 方式の明確化

これまでの研究成果を元に、本研究の提案方式を確立する。具体的には、開発・実験環境の構築、方式の明確化、方式実現に必要な方法・機能の要件の明確化、要件の実性現担保の為の機能実験の実施、を行った。

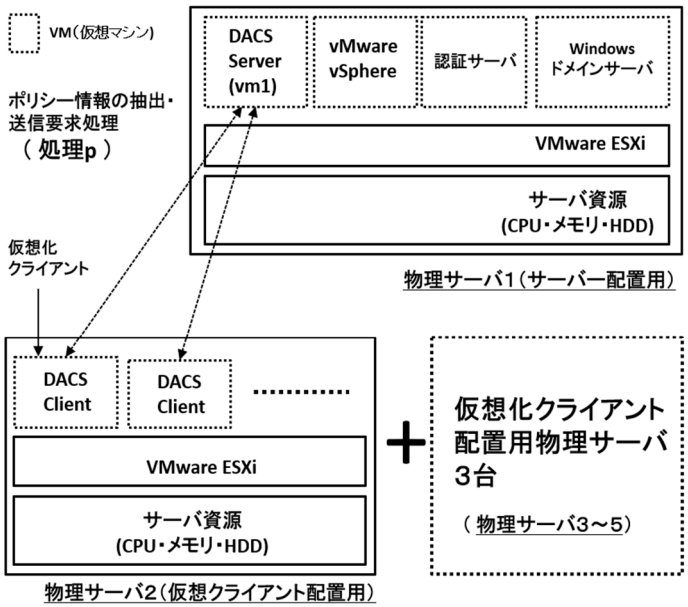

図3 本研究の開発・実験環境

開発環境(図３)として、**VMwareESXi(仮想化基盤用ソフトウェア)**を配置した物理サーバ **5** 台を、特定のドメイン内に属した異なるサブネットに接続し、閉じられた実験用システムを構築する。物理サーバ **1** に **DACS Server(**ポリシー情報管理サーバ**)** を配置し、物理サーバ **2**～**5** に **DACS Client** を配置した「仮想化したクライアント」を配置する。また、各仮想化したクライアントの管理用ツールとして、**VMWare vCenter Server** を活用し、効率的な評価(機能評価、大規模実験による性能評価)環境を整えた。

(2)(1)の管理方式の実現性担保の為のソフトウェア設計・開発・機能評価

(1)で導出した方法・機能の要件をもとに、ソフトウェアの基本・詳細設計を行い、開発と評価を行う。評価は、機能評価を実施する。機能評価は、(1)で明確化した開発要件を元に、予め作成したテスト項目に従って実施した。

開発したソフトウェアは、「将来的なインターネット全体での利用」を見込む為、現在のインターネットで広く普及した技術を用いて開発する。例えば、**Web** の暗号化通信で使用される **HTTPS** プロトコル、暗号化通信の為に必要な暗号鍵をインターネット上で安全に利用する為の **Public Key Infrastracture(PKI)**と呼ばれる公開鍵基盤を利用する形となっている。

(3)大規模実験による性能評価

大規模な性能実験を実施し、仮想環境上で「DACS Server１台で確実に管理可能となるクライアント台数の上限値」を特定した。その後、実験結果の評価を行い、問題点があれば、再度、ソフトウェアの改修を行うこととしたが、特に大きな問題点は発生しなかった。

性能実験の内容：DACS 方式の構造上、処理負荷が最も高い『クライアントへのログイン時に発生する「DACS Client から DACS Server へ発信されるポリシー情報の抽出・送信要求処理(処理p)」』の同時接続数の上限値を特定した。実験のポイントは、下記 2 点である。

- 時刻の同期をとった全クライアントから、スケジューラにより(処理 p)を同時実行し、DACS Server 用の仮想マシン(vm1)の CPU 使用率が 100%となる場合の「vm1 の CPU の処理速度(ps1)」を特定する。同時に、vm1 のメモリ使用状況を監視し、メモリ不足にならないようにする。
- 上記で測定した ps1 の値を減少させながら、それぞれの時点で「vm1 の CPU 使用率が 100%となる場合のクライアント台数」を特定する。(vm1 のメモリ使用状況を監視し、メモリ不足を回避する。)

４．研究成果

(1) クライアント仮想化を前提とする「特定ドメイン」管理の為のクラウド型 PBNM 方式の明確化について

本提案方式の前段階の方式である「複数組織ネットワーク群管理方式」の拡張方式である。そこで、この前段階の方式からの主な拡張部分は、以下の２点である。

(a)ユーザの認証方式

(b)ポリシー情報の生成・配布の方式

(a) ユーザ認証方式
前段階の方式は、複数の組織がそれぞれ保有するネットワーク群を管理する外部組織を設けて管理する方式とした。本提案方式は、その外部組織を管理する組織は設けずに、自律分散型で管理する方式とした。これは、次の段階で、インターネット全域を管理する方式に拡張する為に、管理対象ネットワークが非常に広範囲となるため、重層的管理方式よりも、自律分散型方式が適していると考えたためである。そこで、ユーザ認証方式は、ユーザが属する複数組織ネットワーク群で管理する認証サーバで認証する方式とした。

(b) ポリシー情報の生成・配布方式
ポリシー情報の生成・配布方式は、利用者が所属する複数組織ネットワーク群で管理するポリシー情報と、利用者がノート PC 等の移動端末を持って接続した利用者自身が所属していない複数組織ネットワーク群で管理するポリシー情報の間のマッチングを行う方式とした。具体的には、制御対象の通信に該当するポリシー情報が、双方のポリシー情報の中に含まれる場合は、優先順位付けを行い、優先度の高い方のポリシー情報を優先させる方式とした。原則的には、後者のポリシー情報を優先させる方式としたが、設定を行うことで前者のポリシー情報を優先させることも出来る方式とした。

(2)(1)の管理方式の実現性担保の為のソフトウェア設計・開発・機能評価

上記の(a)(b)の部分を含む全体の試作システムの再設計・開発・機能評価を行った。試作システムの中ではユーザ認証サーバとして OpenLDAP サーバを使用している。この認証サーバに対して、利用者自身が所属する複数組織ネットワーク群以外の複数組織ネットワーク群に接続した場合でも、自分が所属する複数組織ネットワーク群で使用する認証サーバに認証するように機能追加の設計・開発を実施し、機能評価を行った。

また、利用者が所属する複数組織ネットワーク群で管理するポリシー情報と、利用者がノート PC 等の移動端末を持って接続した利用者自身が所属していない複数組織ネットワーク群で管理するポリシー情報について、制御対象の通信に該当するポリシー情報が、双方のポリシー情報の中に含まれる場合は、原則的には、後者のポリシー情報を優先させる方式としたが、設定を行うことで前者のポリシー情報を優先させることも出来るように、再設計・開発・機能評価を実施した。

(3)大規模実験による性能評価
大規模な性能実験を実施し、仮想環境上で「DACS Server 1 台で確実に管理可能となるクライアント台数の上限値」を特定した。

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii	４．巻 Vol.18 No.6
２．論文標題 Load Experiment of the vDACS Scheme to Use between Plural Organizations for Applications to the Small and Medium Size Scale Organization	５．発行年 2018年
３．雑誌名 Int. Journal of Computer Science and Network Security	６．最初と最後の頁 130-138
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii	４．巻 Vol.18 No.11
２．論文標題 Concept of User Authentication Method for the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain	５．発行年 2018年
３．雑誌名 Int. Journal of Computer Science and Network Security	６．最初と最後の頁 68-75
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii	４．巻 Vol.18 No.11
２．論文標題 Concept of Policy Information Decision Method in the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain	５．発行年 2018年
３．雑誌名 Int. Journal of Computer Science and Network Security	６．最初と最後の頁 167-175
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kazuya Odagiri, Shimizu Syogo, Naohiro Ishii	４．巻 17
２．論文標題 Concept of the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain	５．発行年 2017年
３．雑誌名 Int. Journal of Computer Science and Network Security	６．最初と最後の頁 113-119
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii, Makoto Takizawa	4．巻
2．論文標題 9.Consideration of Implementation Method for the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain	5．発行年 2019年
3．雑誌名 eb, Artificial Intelligence and Network Applications	6．最初と最後の頁 44-56
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii	4．巻
2．論文標題 Implementation of Creation and Distribution Processes of DACS rules for the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain	5．発行年 2019年
3．雑誌名 Applied Computing and Information Technology	6．最初と最後の頁 147-164
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii	4．巻 Vol.19,No.6
2．論文標題 35.Consideration of the User Authentication Processes in the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain	5．発行年 2019年
3．雑誌名 International Journal of Computer Science and Network Security	6．最初と最後の頁 158-165
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii	4．巻 Vol.19,No.7
2．論文標題 36.Consideration of Policy Information Decision Processes in the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain	5．発行年 2019年
3．雑誌名 International Journal of Computer Science and Network Security	6．最初と最後の頁 166-174
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　4件）

1．発表者名
Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii, Makoto Takizawa

2．発表標題
Consideration of Policy Information Decision Processes in the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain

3．学会等名
IEEE Advances in Network-Based Information Systems in International Conference on Network-Based Information Systems (NBiS)（国際学会）

4．発表年
2018年

1．発表者名
Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii, Makoto Takizawa

2．発表標題
Concept of User Authentication Method for the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain

3．学会等名
IEEE Int. Conf. on Advanced Information Networking and Applications Workshops (wAINA)（国際学会）

4．発表年
2018年

1．発表者名
Kazuya Odagiri, Shogo Shimizu, Makoto Takizawa, Naohiro Ishii

2．発表標題
Concept of Policy Information Decision Method in the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain

3．学会等名
IEEE Int. Conf. on Computational Science/ Intelligence and Applied Informatics (CSII 2018)（国際学会）

4．発表年
2018年

1．発表者名
Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii, Makoto Takizawa

2．発表標題
Concept of the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain

3．学会等名
Data Engineering and Communication Technologies (Lecture Note) in in Int. Conf. on Broad-Band Wireless Computing, Communication and Applications (BWCCA2017)（国際学会）

4．発表年
2017年

１．発表者名 Kazuya Odagiri, Shogo Shimizu, Naohiro Ishii
２．発表標題 43.Implementation of User Authentication Processes for the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain
３．学会等名 Proc. of IEEE International Conference on Computational Science/Intelligence and Applied Informatics, pp.1-6.
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考