インターネットPBNM導入により実現できる「製造工場における仮想的な工作機械の利用のためのサービス」の提案

小田切　和也（椙山女学園大学文化情報学部）

要旨

著者は，Destination Addressing Control System（DACS）方式と呼ぶネットワーク管理方式を提案し，インターネット全域の管理を実現するために必要なソフトウェアの研究を進めてきた。このDACS方式は，クライアント上だけにソフトウェア形態の通信制御機能を配置し，各クライアントから発信される通信に対する制御を通じて，特定のネットワーク全体を安全かつ効率的に管理する方式である。この方式の管理範囲を拡大していくことで，最終的には，インターネット全域を管理する方式としていきたいと著者は考えている。本論文では，そのDACS方式の有効性を高める目的で，この方式を導入するネットワーク上で実現することが可能であると著者が考えている「製造工場における仮想的な工作機械の利用のためのサービス」についての提案を行う。

キーワード：PBNM，ネットワーク管理，クラウド，アクセス制御，Destination NAT

1. はじめに

現在のインターネットの仕組みは，自律分散型の形態がとられており，統一的に全体が安全・効率的に管理される仕組みにはなっていない。このようなインターネット上には，様々な利用者が存在し，様々な形でインターネットを利用している。そ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して利用する時には，「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くなる。しかしながら，インターネット全域で，そのようなリスクを回避することは，現状では，困難である。そこで，ポリシーに基づくネットワーク管理（PBNM：Policy Based Network Management）の考え方に基づき，インターネット全体を管理する「インターネットPBNM（図1）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。これまでの所，以下の4つのステップで研究を進めている。

（Step1）自組織ネットワーク（特定の一組織が保有するネットワーク）管理の為PBNM方式の研究

（Step2）複数組織ネットワーク群管理の

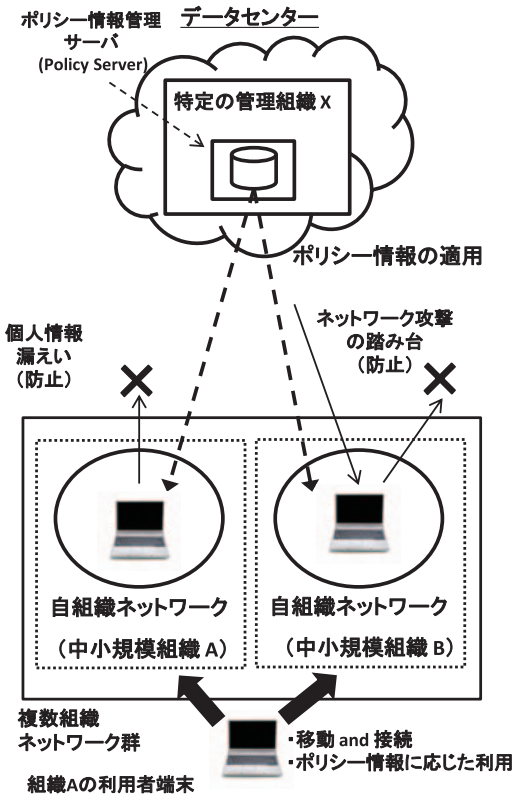

図1　インターネットPBNMのイメージ

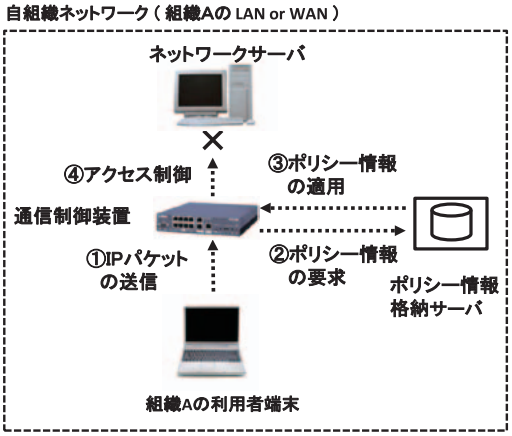

図2　既存PBNM

為のPBNM方式の研究

（Step3）特定ドメインを管理する為のPBNM方式の研究

（Step4）インターネット全体を管理する為のPBNM方式の研究

（Step1）に該当する既存PBNM（図2）は，各組織内で構成員の手によって定められたネットワークポリシーやセキュリティポリシーなどの明文化された方針に基づき，柔軟かつ効率的なネットワーク管理を実現する方式である。その方式の原理は，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能による通信制御（アクセス制御，通信の暗号化，QOS制御など）を通して自組織が保有するネットワーク全体を管理するものである。IETF（R. Yavatkar at el. IETF RFC 2753，2000）やDMTF（DMTF，DSP0123，2002）などの複数の標準化組織で標準化されており，管理対象範囲は，自組織ネットワークである。この方式の原理を，理論的・技術的には，（Step2）の管理対象範囲と同じ範囲である「複数組織ネットワーク群」の管理にも応用できる。しかしながら，様々な理由が推測できるが，そのような趣旨の研究は，見当たらない。PBNMの技術的な個別の構成要素であるアクセス制御技術[1)]やQOS制御技術[2)]を個別に研究対象として取りあげて，複数の組織が個別に保有するネットワークの間で共通利用す

る為の研究が若干報告されているだけである。

そこで，著者は，（Step1）の方式の管理対象範囲，つまり，適用範囲のネットワークを拡大する方向で，（Step2）の研究を推進する。具体的には，適用範囲を，「個別組織のネットワーク」から「複数組織ネットワーク群」に拡大し，複数組織ネットワーク群管理の為の方式とした。現在は，更に適用領域を拡大する（Step3）の研究に相当する「特定のドメインを管理する方式」の研究を推進している。具体的には，インターネットPBNMの実現に向けて，DACS方式で管理される複数組織ネットワーク群（ネットワークグループ）が，インターネット上に多数存在する状況になると想定し，それらのネットワークグループ間を相互に緩やかに連携させることで，管理範囲を拡大することを目指している。インターネットPBNMの確立に向けて，このような形で研究を進めている。しかしながら，その一方で，DACS方式を導入するネットワーク上で実現可能となる新しいサービスの提示も期待されている。そこで，本論文では，著者が考えている新サービスの1例として，産業革命4．0時代に対応する「製造工場における仮想的な工作機械の利用のためのサービス」についての提案を行う。

2．インターネットPBNMの研究

2.1．インターネットPBNM研究推進の動機と関連研究

既存のネットワーク管理に関する研究・技術として，ユーザ認証に関する研究[1)]やサーバ負荷分散などの負荷分散に関する研究[2)]，VPN（Virtual Private Network）[3)]のようなネットワーク仮想化に関する研究，ネットワーク接続時のセキュリティ保証のための検疫ネットワーク[4)]に関する研究など，様々な種類の研究が行われている。しかしながら，これらの研究は，それぞれある特定の個別の目的を実現するためのネットワーク技術に関する研究であり，特定範囲のネットワークを安全かつ効率的に管理することを目的としている研究ではない。特定範囲のネットワークを安全かつ効率的に管理する為のモデルとして，Internet Engineering Task Force（IETF）で示されているPBNMの研究[6) 7) 8) 9)]が存在する。このPBNMの原理は，図3に示された内容のものである。

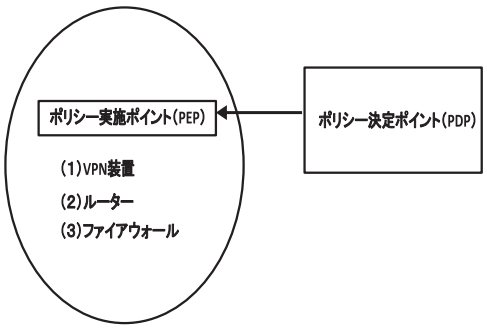

図3　IETFにおけるPBNM

また，このPBNMと同様に，ネットワーク経路上にアクセス制御の為にゲートウェアシステムを用いて利用者単位でアクセス制御するOpengate[5]に関する研究も行われている。（Opengateは，ある国立大学において，学内ネットワークを管理する目的で研究・開発が為されたものである。）これら方式に共通する問題点として，（1）機器変更によるコストの発生，（2）既存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，（3）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，という問題点がある。これらの問題点を克服するPBNM方式を提案し，DACS方式[11) 12)]と呼んでいる。このDACS方式の特徴は，各クライアント上に設けた通信制御機能により，クライアントから発信される通信を制御し，その通信制御を通してネットワーク全体を管理する点である。クライアント上で通信制御を行うという観点で考えると，PBNMの研究の中には，クライアントにソフトウェアを配置してQOS制御する方式の研究[10)]もあるが，これは，ネットワーク全体の管理目的ではなく，あくまでも，QOSに限定されるものである。クライアント上での通信制御を通して，ネットワーク全体を効率的に管理する目的の研究は，DACS方式以外に見当らない。

2.2. DACS方式の説明

本章では，既存のDACS方式の要約を記述する。具体的には，過去に発表した論文[11) 12)]の要約であり，愛知大学の情報メディアセンター紀要[14)]に記載した文章から抜粋したものが中心である。

DACS方式の原理は，ネットワークに接続したクライアントの通信をユーザ，またはクライアント単位で制御することによって，ネットワークシステム全体を管理することである。具体的な制御内容は，通信先サーバを変更する，あるいは，通信を遮断することである。ネットワーク管理者により通信制御情報を管理するサーバ（以下，通信制御情報管理サーバ）に設定された通信制御の為のルール（以下，通信制御ルール）に基づいて制御される。通信先サーバを変更する為には，クライアント上にDestination NATを配備し，通信制御情報管理サーバに定められたルールに従って宛先を変更する。通信を遮断する為には，クライアント上にパケットフィルタリングの仕組みを設けて，同様に通信制御情報管理サーバに定められたルールに従って通信を遮断する。DACS方式では，これらの原理に基づき，以下の基本機能をユーザ，又は，クライアント単位で実現する。

（x） 同一ホスト名に対する通信先サーバ切換
（y） 利用サービス制限
（z） アクセスポート許可

ユーザ単位で通信制御する為には，ユーザ認証サーバと組み合わせることにより，あらかじめ通信制御情報管理サーバに設定されたユーザ単位の通信制御ルールに従ってクライアント上でDestination NATによる宛先変更を行うか，パケットフィルタリングの仕組みにより通信を遮断する。同様に，クライアント単位で通信制御する為には，通信制御情報管理サーバに設定されたIPアドレス単位の通信制御ルールに従い通信制御を行う。それにより，ある特定の場所に設置したクライアントに対する通信制御が可能になる。但し，その通信制御の前提条件として，原則的にはクライアントに固定IPアドレスを設定する必要がある。DHCP環境下においては，ネットワーク単位，あるいは，サブネットワーク単位で接続されたクライアントに同一の制御をすることは可能である。又，通信制御情報管理サーバには，ユーザ，及び，クライアント単位の通信制御ルールが両方設定されている為，そのユーザでログインしたクライアントを制御する為のルールが重複してしまう場合は，ある一定の処理法則に従い優先するルールを決めて通信制御を行う。その処理法則は，組織毎に定められるネットワークポリシーにより決定される。

図4に，DACS方式における基本的なシステム構成の全体像を示す。同図のDACS SV（DACS Server） はDACS方式によるサービスを提供する為に必要なサーバ機能であり，通信制御情報管理サーバの役割も果たす。DACS CL（DACS Client）は，サービスの提供を受ける為に必要なクライアント機能である。又，DACS CTL（DACS Control）は，DACS CLの一部であり，実際に通信を制御する通信制御サービスの役割を果たす。

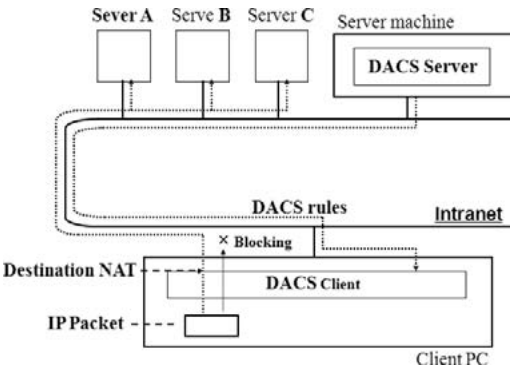

図4　DACS方式の基本システム構成

更に，DACS rulesは，前述した（x）～（z）の3つの基本機能による通信制御の為に必要なルールであり，次の（A）（B）で構成される。（以下の宛先情報X，Y，Zは，IPアドレスとポート番号である。）

（A）（x）の機能を制御する為に，Destination NATに必要となる通信先変更前の宛先情報Xと通信先変更後の宛先情報Y。

（B）（y）（z）の機能を制御する為，パケットフィルタリングで通信の

遮断や許可をする為に必要となる通信の宛先情報Z。

そのDACS rulesは，DACS SVからDACS CLへ送信された後，DACS CLの一部であるDACS CTLに適用される。そして，DACS CTLでは適用直後から通信制御が行われる。ここでは，DACS SVは常時定常状態（運用状態）であり，

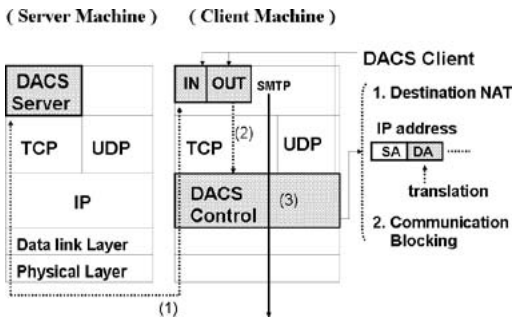

図5　レイヤー設定

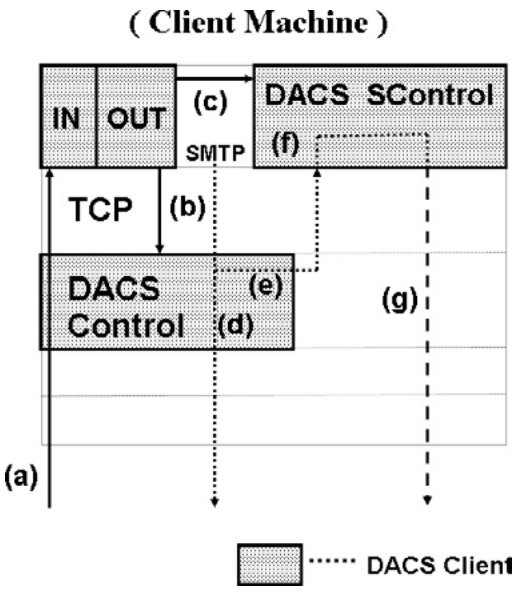

図6　VPN機能

ネットワークの通信が問題なく行える状態であるとの前提のもと，DACS CLの基本的な処理の流れと内容を説明する。また，DACS CLは，クライアントOSの起動・終了処理の一部として起動・終了させる。

また，DACS SV・CL・CTLのレイヤー設定を図5に示す。サーバ，及び，クライアントのアプリケーション層に配置されたDACS SVとDACS CL間でDACS rulesを送受信する。DACS CLは，DACS CTLに対してDACS rulesを適用する。DACS CTLは，ネットワーク層に配置され，Destination NATによる通信先サーバ変更やパケットフィルタリングにより通信を遮断する。

DACS方式は，クライアントに配置したDACS CLで通信を制御する方式である。その為，DACS CLを配置していないクライアントをネットワークに接続する場合，ネットワークサービスを自由に利用出来てしまうという問題点がある。セキュリティポリシーやネットワークポリシーによっては，そのようなクライアントが接続するのを許可する場合もあり得るが，不許可の場合に備えて対処する必要がある。図6に示したように，クライアントから発信される通信をVPN（Virtual Private Network）化出来るように機能拡張し，VPN化されないクライアント，つまり，DACS CLを配置しないクライアントからの通信を遮断出来

るようにして対処する。具体的な仕組みを図6に従って説明する。まず，通信制御開始前に必要な初期化処理を説明すると，(a)のように，DACS SVからDACS rulesがDACS CLに対して送信された後，(b)のようにDACS CTLにDACS rulesが適用されると同時に，(c)のように通信VPN化する機能であるDACS SCTL(DACS SControl)にDACS rulesが適用されて，初期化処理が完了する。そして，(d)のようにクライアントアプリケーションから通信が発信されると，DACS CTLの制御によって，(e)のようにlocalhostへ宛先が変更される。その通信を受け取ったDACS SCTLの制御によって，(f)の部分で通信がVPN化されて，(g)のように，その通信がクライアント外部へ発信される。

現在は，上記したDACS方式の基本原理を用いて，管理範囲を拡張する研究を進めている。

3. 製造工場における仮想的な工作機械の利用のためのサービス

本章では，PBNM方式としてのDACS方式を導入するネットワーク上で実現できると著者が考えているサービスの1例として，製造工場における仮想的な工作機械の利用のためのサービスの提案を行う。

図7に，そのサービスの概要を示した。このサービスを用いることで，例えば，自動車部品加工を行う工場で，各加工機械で加工した個々の部品の寸法の測定データを収集してクラウド上に集め，ビックデータ処理基盤を活用し，各種統計情報として集計することが出来る。それにより，工場の中の「どの機械で，ど

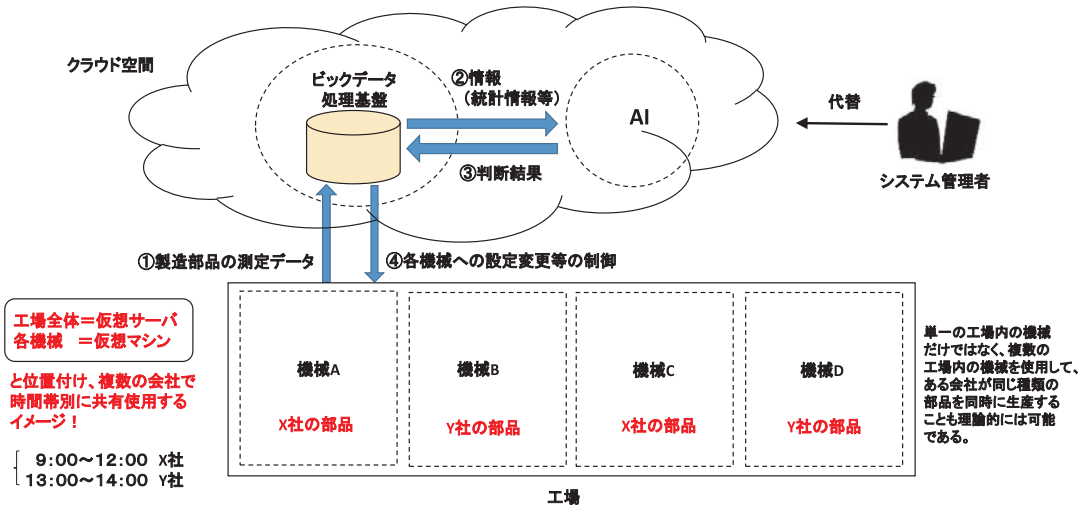

図7　製造工場における仮想的な工作機械の利用のためのサービス

の種類の部品を，どの程度の数生産し，その際の不良品発生率がどの程度になるか」を，ほぼリアルタイムで把握することが可能となる。提案方式による制御により，ネットワーク上の端末としての各々の工作機械から送信される測定データを，会社単位で識別することが出来る為，個々の部品の測定データがどの会社のための部品データなのかを識別することが出来る。生産した部品のサイズにもよるが，例えば，RFID技術し，測定データと実際に生産した部品との間の紐づけを行っておくことで，測定データと部品を取引先に納品することが出来る。

また，その部品データ使用する形で，AIによる制御下で，複数の会社間で工作機械を時間単位で共有し，部品の自動生産を行うことも出来る。その際，例えば，以下のような自動制御が可能である。

（例1）同じ工場内に複数の同じ種類の加工機械が配置されている状態で，各会社（例：X社・Y社）用に個々の加工機械を割り当て，同じ種類の部品の加工を並行して実施し，一方の会社（例：Y社）のその日の必要部品数を作り終えた場合，その会社（Y社）に割り当てられていた加工機械を，もう一方の会社（X社）に割り当て，社用の部品を生産する。

（例2）異なる工場内（例：Z1工場：Z2工場）に複数の同じ種類の加工機械が配置されている状態で，ある会社（X社）用のある部品を生産しているとする。しかしながら，緊急事態が発生し，別の会社（Y社）のための部品（X社と同じ種類の部品）をある一定量（例：Z2工場の半分の数の機械で，2時間あれば生産可能な量）生産する必要が発生し，すぐに生産を行う。

このサービスを実現することにより，例えば，多額の投資を行うことが難しい多数の会社が大規模な工場を建設し，加工機械を共有する形での生産が可能になり，大きなメリットを得ることが出来るようになる。

4. まとめ

本論文では，「製造工場における仮想的な工作機械の利用のためのサービス」についての提案を行った。インターネットPBNMの研究を推進する過程で，著者は，その有効性を提示する必要性を強く感じていたため，今回，新サービスの提案を行うことで，インターネットPBNMの有効性の補強を行うことが出来たと考えている。今後は，提案方式の仕組みに関する研究を継続して進める一方で，提案方式の有効性を高めるために，本論文のように新しいサービス創出に関する研究も進めていく予定である。また，本論文で提案したサービスについても，機会を伺って，実現する方向で研究を進めた

いと考えている。

参考文献

1）若山公威，出路裕介，冷基立，岩田彰，“指紋照合によるリモートユーザ認証方式，”情報処理学会論文誌，Vol.44，No.2，pp.401–404，2003.

2）下川俊彦，木場雄一，中川郁夫，山本文治，吉田紀彦，“広域分散環境におけるDNSと経路情報を利用したサーバ選択機構，”電子情報通信学会論文誌B，Vol.J86-B，No.8，pp.14541462，2003.

3）C. Metz，“The latest in virtual private networks: part I，” IEEE Internet Computing，Vol. 7，No. 1，pp. 87–91，2003.

4）http://www.nec.co.jp/univerge/solution/pack/quarantine/

5）只木進一，江藤博文，渡辺健次，渡辺義明，“利用者移動端末に対応した大規模ネットワークのOpengateによる構築と運用，”情報処理学会論文誌，Vol.46，No.4 pp.922–929，2005.

6）S.Jha，M.Hassan，“Java implementation of policy-based bandwidth management，” Int. J. Network management，John Wiley&Sons，Vol. 13，isuue. 4，pp. 249–258，July，2003.

7）G.M. Prerez，F.G. Skarmeta，S.Zeber，T. Symchych，“Dynamic Policy-Based Network Management for a Secure Coalition Environment，” IEEE Communications Magazine，Vol. 44，issue. 11，pp. 58–64，November，2006.

8）D.C. Verma，“Simplifying Network Administration Using Policy-Based Management，” IEEE Network，Vol. 16，issue. 2，pp. 20–26，March-April，2002.

9）菅野政孝，田中俊介，坂田祐司，小熊慶一郎，白鳥則郎，“情報ネットワークシステムのポリシー制御“PolicyComputing”の適用と実装，”情報処理学会論文誌，Vol. 42，No. 2，2001.

10）H. Chaouchi，P.M. Antunes，“Pre-handover signaling for QOS aware mobility management，” Int. J. of Network management，John Wiley&Sons，Vol. 14，isuue. 6，pp. 367–374，November，2004.

11）K. Odagiri，R. Yaegashi，M. Tadauchi，N. Ishii，“Efficient Network Management System with DACS Scheme: Management with communication control，” Int. J. of Computer Science and Network Security，Vol. 6，No. 1，pp. 30–36，January，2006.

12）K. Odagiri，R. Yaegashi，M. Tadauchi，N. Ishii，“Secure DACS Scheme，” “Journal of Network and Computer Applications，” Elsevier，Vol. 31，No. 4，pp. 851–861，November，2008.

13）K. Odagiri，S. Shimizu，N. Ishii，“Functional Evaluation of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations，” International Journal of Networked and

Distributed Computing (IJNDC), Volume 5, Issue 2, pp. 62–70. April, 2017.
14）小田切和也，“インターネットPBNM 実現に向けたポリシーに基づくドメイン管理方式の実装方法の検討”Vol. 28, No. 1, pp. 45–56, 2018.