マルチメディア通信と分散処理 79－17
（１９９６．１１．１５）

組織間網環境におけるアクセス制御の課題

寺田真敏*1,*3　村山優子*2
情報処理振興事業協会(IPA) 技術センター *1
広島市立大学 情報科学部 *2

ファイアウォール導入による組織内網のセキュリティを確保しつつ、利用上の制約事項を解決するために、『ユーザのネットワーク上での活動範囲を考慮したネットワーク環境』の提供を目的としたアクセス制御機構の検討ならびにプロトタイプ開発を進めている。

本稿では、「組織間網環境におけるアクセス制御方式」として検討・開発を進めてきたプロトタイプシステムにおいて、現在までに明らかとなっているアクセス制御機構と運用管理の課題を提示する。アクセス制御機構の課題としては、ユーザアクセスドメイン間の防御壁の提供、クライアントにおけるユーザ認証情報の保持方法、ファイアウォール多段接続時のアクセス制御の前提条件の低減がある。また、運用管理での課題としては、経路情報とアクセス制御情報の管理、)ユーザ識別子と認証情報の付与、ユーザアクセスドメイン上の情報管理がある。

Problems in Access Control for Inter-Organizational Computer Network Environment

Masato Terada *1,*3　Yuko Murayama *2
Information - Technology Promotion Agency, Japan (IPA) *1
Faculty of Information Sciences, Hiroshima City University *2

We challenge the issue to tackle a problem about access control; how one can provide a transparent network environment to users, while preserving security in each organization with firewalls. We proposed the User Access Domain to provide user-level grouping, and the Access Domain Control Layer to support such user level domain over the organizational networks with firewalls. Based on the proposal, we studied the mechanisms of transparent network environment and route control.
This paper, the outline and problems of the impementation for User Access Domain are presented.

1. はじめに

現在、TCP/IP プロトコル体系に基づいて構成されるインターネットは、単なる終端装置(ホスト)や中間装置(ルータ)から成る網(網間網)としてではなく、組織毎にこれらのシステムが集合し、さらにネットワークを構成する組織間網の形態として運用されつつある。網間網のアーキテクチャは、接続性を重視して作られており、組織間網の形態において考慮しなければならない要因のひとつである組織間のアクセス制御機構が採りいれられてはいない。

組織間網のアーキテクチャで利用できるアクセス制御ツールとしてファイアウォールがある。ファイアウォールは予め決められた基準をもとに、あるデータについては通信を許可するが、他のデータについては通信を拒否するというようなアクセス制御を行う。そのアクセス制御は、主に網や終端装置に対して、アクセスを行う終

*3)　(株)日立製作所より出向中

端装置や利用者を制限するものである。ファイアウォールは、組織間網のアーキテクチャにおいて、組織内網のセキュリティを確保しつつ、インターネットのような組織外網と組織内網との相互接続を行うための接続機能として利用されている。これは、組織が保有する個々のシステムに対する脅威を包括的に減少させるという点で有効なツールである。反面、ファイアウォール導入は、ユーザの利用形態に制約を課している。例えば、分散している職場間での計算機の相互利用や、ひとりのユーザが複数組織に所属している場合の計算機の相互利用に関して、必ずしもユーザの使い勝手が良いものであるとは言えない。

本研究では、ファイアウォール導入による組織内網のセキュリティを確保しつつ、利用上の制約事項を解決するために、『ユーザ(組織・個人)のネットワーク上での活動範囲を考慮したネットワーク環境』の提供を目的としたアクセス制御機構の検討ならびにプロトタイプ開発を進めてきた。

本稿では、「組織間網環境におけるアクセス制御方式」として検討・開発を進めてきたプロトタイプシステムにおいて、現在までに明らかとなっているアクセス制御機構と運用管理の課題を提示する。

2. アクセス制御機構

本節では、本研究で検討を進めているアクセス制御機構について述べる。提案するアクセス制御機構は、ユーザ毎に、利用できる網、終端装置(ホスト)やアプリケーションを制限できる機能を提供する。

2.1 ユーザアクセスドメインとエリア

本研究では、アクセス制御機構を実現するために、「ユーザアクセスドメイン」「エリア」という概念を新たに導入した。

(1)ユーザアクセスドメイン

ネットワーク上に点在する興味の対象であるオブジェクト(サーバマシンなどの物理的な装置など)が、あたかも同じネットワーク上にあるような論理ネットワーキング環境を「論理ネットワーク」と定義する。

「論理ネットワーク」は、ユーザが最終的に利用したいオブジェクトが存在する範囲としてユーザ(組織・個人)毎に「論理ネットワーク」を定義可能とする。本研究では、図 1に示されるように、ユーザ毎に保有する「論理ネットワーク」を「ユーザアクセスドメイン」と定義する。

(2)エリア

「エリア」は、ユーザアクセスドメインの構成要素であり、セキュリティ防御壁として動作するファイアウォールにより分割されたネットワーク資源の範囲である。エリアは同一のセキュリティ方針に基づき制御される範囲と考える。

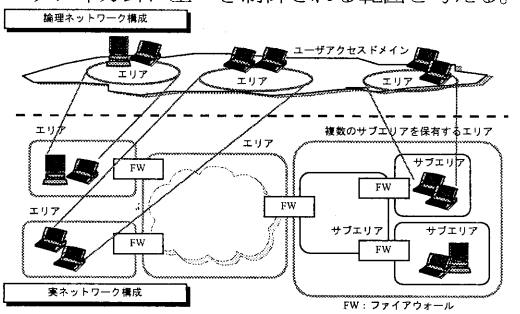

図 1　ユーザアクセスドメインとエリア

2.2 アクセスドメイン制御層

ユーザアクセスドメインを実現する基盤として「アクセスドメイン制御層(ADCL:Access Domain Control Layer)」を導入した。アクセスドメイン制御層とユーザアクセスドメインとの関係は、図 2に示すように、終端、中継装置に配置されたアクセスドメイン制御層がユーザアクセスドメインを形成し、組織間の強固なセキュリティ防御壁と透過的なネットワークサービスの提供を実現する。

アクセスドメイン制御層は、以下の２つの機能を持つ。

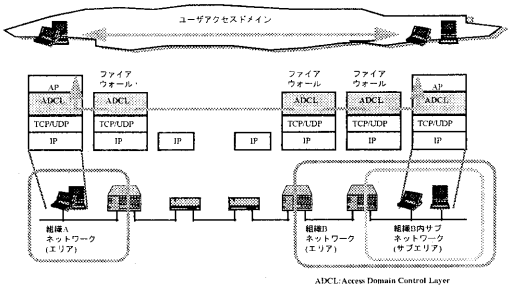

図 2　アクセスドメイン制御層の階層モデル

(1)エリア間の経路制御機能

ユーザに対して透過なネットワークサービスを提供するために、ユーザアクセスドメイン内のエリア間の経路制御を行い、終端装置間の透過的なデータ転送機能を提供する。ADCL は、図 3に示すように終端装置間の透過的な TCP の論理通信路を提供する。また、ADCL が保有する個々のサービス(telnet, ftp 他)、宛先エリアと次送信先情報から構成される経路制御情報テーブルを用いて論理通信路の経路を制御する。

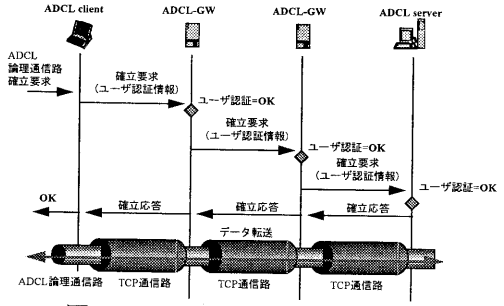

図 3　ADCL の論理通信路の確立

(2)エリアに対するアクセス制御機能

エリアを運用管理する者の運用方針に従い、エリア内に存在するオブジェクトのアクセス制御を行う。すなわち、ネットワーク上で組織・個人がアクセス可能な範囲の制御を行う機能である。図 3に示すように、許可されたユーザが、許可された宛先エリアやサービスに対する接続の場合にのみ、ADCL の論理通信路確立要求パケットを次送信先である ADCL に転送することで制御する。

2.3　プロトタイプ実装方式の概要

本節では、開発中のプロトタイプシステムの概要を述べる。

(1)開発プラットフォーム

SunOS4.1.3

(2)ソフトウェア構成

図 4に示すように、クライアントアプリケーション(ADCL client)側はソケットインタフェース型のライブラリ(adcllib)を提供し、ファイアウォール(ADCL-GW)、サーバアプリケーション(ADCL Server)側には、サーバ(adcld)デーモンを提供する。

(3)サポート機能

(a)透過的なデータ転送

TCP/UDP のデータ転送をサポートする。

(b)エリア間の経路制御

経路制御情報は adcllib、adcld が静的情報として保有する。

ADCLファイアウォール・サーバが保有する経路制御情報

宛先エリア	サービス	次送信先
server.1st.number.com	ftp	adclgw.space.com
cars.edu	http	adclgw.space.com

(c)アクセス制御

アクセス制御情報は、adcld が静的情報として保有する。

ADCLファイアウォール・サーバが保有するアクセス制御情報

ユーザ	送信元エリア	宛先エリア	サービス
Sam	-source color.com	-dest color.edu	-port telnet
Anne	-source mars.space.fr	-dest moon.space.fr	-port http

(d)ユーザ認証

RSA(512 ビット)公開鍵暗号方式と MD5 を用いて、X.509 の 2 方向性厳密認証によりユーザ認証を実施している。なお、ユーザ側の認証情報(RSA 秘密鍵)は、クライアント(adcllib)計算機上の各ユーザのホームディレクトリにファイルとして登録する形態を取っている。

(e)データ暗号化

ユーザ認証時にセション鍵(DES56 ビット)を交換し、このセション鍵を用いてデータ転送時の暗号化を実施する。

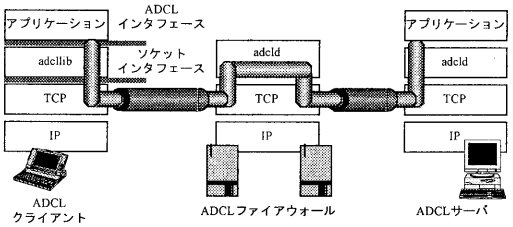

図 4　ADCL 実装方式の概要

3. アクセス制御の課題

「組織間網環境におけるアクセス制御方式」のプロトタイプシステムにおいて、現在までに明らかとなっているアクセス制御機構と運用管理での課題を提示する。

3.1　アクセス制御機構での課題

(1)ユーザアクセスドメイン間の防御壁

ユーザアクセスドメインは、ユーザ毎の論理ネットワークであるが、図 5に示すようにエリア単位でのユーザアクセスドメインの重

なりが起こり得る。開発中のプロトタイプでは、クライアント(adcllib)計算機上の各ユーザのホームディレクトリに、ユーザの認証情報(RSA 秘密鍵)ファイルを登録する形態を取っている。このため、図 6に示すように計算機を複数ユーザで共用している場合には、計算機上でユーザの成りかわりが発生すると、ユーザアクセスドメインの本来の役割が機能しなくなってしまう。

ユーザアクセスドメインの重なりが発生する箇所では、ユーザの認証情報の保持方法も含め、利用形態に応じた防御壁が必要となる。

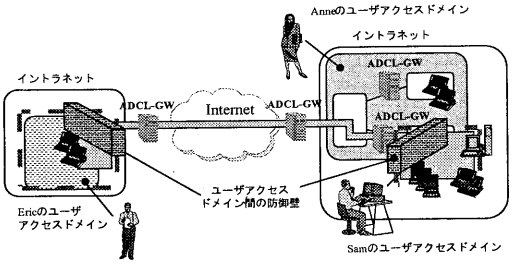

図 5　ユーザアクセスドメインの重なり

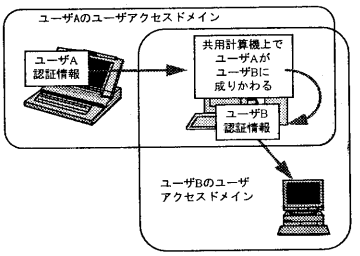

図 6　ユーザの成りかわりの例

(2)クライアントにおけるユーザ認証情報の保持方法

クライアントにおけるユーザ認証情報の保持方法については、上述したユーザアクセスドメインでの重なりが発生した場合に加え、以下の場合を検討しておく必要がある。

(a)クライアントとなる計算機を紛失した場合の対策

(b)異なる組織間にまたがりユーザアクセスドメインを設置し、かつクライアントとなる計算機を常設する場合の対策

いずれの場合も、第 3 者により計算機が不当に取り扱われると、ユーザアクセスドメインの本来の役割が機能しなくなってしまう。

対策方法の 1 つとして、ユーザ認証情報を IC カード等の別ハードウェアに登録するといった物理的なセキュリティ対策を実施することが考えられる。

(3)ファイアウォール多段接続時のアクセス制御

ADCL ファイアウォールのアクセス制御の対象項目は、ユーザ、宛先ホスト(IP アドレス)、宛先サービス(ポート番号)、送信元ホスト、送信元サービスがある。これらのアクセス制御は、図 7に示すような ADCL 論理通信路を確立する確立要求パケットに設定されている情報と、ADCL ファイアウォール・サーバに登録されているアクセス制御情報とを比較することによって実現している。

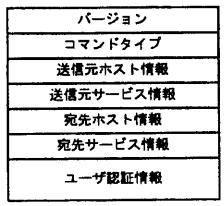

図 7　ADCL 確立要求パケットの形式

現在開発中のプロトタイプでは、ADCL クライアントが確立要求パケットに設定している送信元ホスト、送信元サービスの正しさを確認する手段を提供していない。このため、送信元ホスト、送信元サービスに関するアクセス制御は、クライアントならびに、確立要求パケットを中継する ADCL ファイアウォールを信頼するという稼動条件の下でのアクセス制御となっている。

エリアのセキュリティ方針をよりきめ細かくユーザアクセスドメインに反映するためには、上述のような稼動のための前提条件数を少なくしていく必要がある。

3.2　運用管理での課題

(1)経路情報の管理

プロトタイプシステムでは、小規模なシステム構成を対象として開発を進めており、ADCL ファイアウォールならびにサーバが保有するエリア間の経路情報は静的な情報定義方式を採用している。

今後、大規模なシステム構成を対象とした

経路制御機構を提供していくためには、以下の項目を検討していく必要がある。
(a)分散型の経路情報管理機構
(b)ADCL ファイアウォール障害時の経路迂回機構
(c)経路情報の矛盾により発生する経路ループの検出機構

分散型の経路情報管理機構を実現する方法の1つとして、図 8に示すようなDNS のリソース情報を拡張して経路情報を提供する方法が考えられる。

```
@       IN      SOA     IPA.GO.JP Action\.domains (
20 7200 600 3600000 60)
        NS      AA.IPA.GO.JP.
        NS      BB.IPA.GO.JP.
        MX      10      AA.IPA.GO.JP

        MX      20      BB.IPA.GO.JP
        ADCL    10      AA.IPA.GO.JP
        ADCL    20      BB.IPA.GO.JP
*       ADCL    10      AA.IPA.GO.JP
        ADCL    20      BB.IPA.GO.JP
AA      A       192.218.88.99
        ADCL    10      AA.IPA.GO.JP
BB      A       192.218.88.100
        ADCL    10      BB.IPA.GO.JP
CC      A       192.218.88.101
        ADCL    10      BB.IPA.GO.JP
```

図 8　DNS を用いた経路情報の提供

(2)アクセス制御情報の管理
アクセス制御情報の定義は、経路情報と同様に、ADCL ファイアウォールならびにサーバが保有するアクセス制御情報は静的な情報定義方式を採用している。
ユーザのアクセス制御情報は、ユーザが利用する全ての ADCL ファイアウォール、サーバ上に登録しておく必要がある。このため、プロトタイプシステムでは、各ユーザの定義をグルーピング可能とすることで定義量の低減を図れる仕様としている。
今後、大規模なシステム構成を対象としたアクセス制御機構を提供していくためには、以下の項目を検討していく必要がある。
(a)分散型のアクセス制御情報管理機構
(b)アクセス制御情報の集約化

分散型のアクセス制御情報管理機構を実現する方法の1つとして、図 9に示すようなサブエリアから構成されるエリアの場合、エリアの ADCL ファイアウォールのアクセス制御情報をサブエリアの管理者が管理できる機構が有効であると考えている。

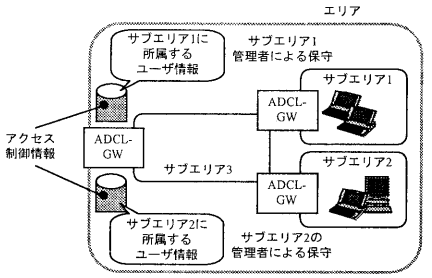

図 9　アクセス制御情報の分散管理

(3)ユーザ識別子と認証情報
同一の組織内でユーザアクセスドメインを構成する場合、このユーザアクセスドメインを利用するユーザは、その組織において一意となる識別子、例えばメールアドレスを付与し、その識別子に対して認証情報を付与することで解決することができるであろう。一方、異なる組織間でユーザアクセスドメインを構成する場合、ユーザ識別子と認証情報の付与は以下の方法が考えられる。
(a)組織毎に個別のユーザ識別子と認証情報を付与し運用する。
(b)主体となる所属組織のユーザ識別子と認証情報を用いて運用する。
(c)主体となる所属組織のユーザ識別子ならびにユーザ識別子の別名、認証情報を用いて運用する。

ユーザ識別子と認証情報の付与については、公開鍵の証明書発行という観点からも検討を行う必要があると考えている。

(4)異なる組織にまたがりユーザアクセスドメインを設置した場合の情報管理
報告者らが提案するアクセス制御方式は、計算機やサービスに対するユーザ毎のアクセス制御機構を提供する。しかし、ユーザアクセスドメイン上を流れる情報に関するアクセス制御機構を実現するまでには至ってはいない。
現行では、ユーザアクセスドメインを異なる組織にまたがって構成した場合、ユーザアクセスドメイン上での情報管理は、ユーザアクセスドメインの利用ユーザにまかせる形態で運用せざるおえない。

4. おわりに

本報告では、まず、報告者らが提案する「組織間網環境におけるアクセス制御方式」の概要と現在開発を進めているプロトタイプシステムの実装方式の仕様について報告した。提案するアクセス制御機構は、ユーザ毎に、利用できる網、終端装置(ホスト)やアプリケーションを制限できる機能を提供する。この提案機構を用いることにより、組織のネットワーク・情報管理者のセキュリティ方針を反映したユーザ毎の論理的なネットワークを提供することを目的としている。

次に開発を進めてきたプロトタイプシステムにおいて、現在までに明らかとなっているアクセス制御機構と運用管理の課題を提示した。

現在までのところ、アクセス制御機構の課題としては、(1)ユーザアクセスドメイン間の防御壁の提供、(2)クライアントにおけるユーザ認証情報の保持方法、(3)ファイアウォール多段接続時のアクセス制御の前提条件の低減がある。また、運用管理での課題としては、(1)経路情報、アクセス制御情報の管理、(2)ユーザ識別子と認証情報の付与、(3)ユーザアクセスドメイン上の情報管理がある。

今後、開発したプロトタイプシステムのセキュリティ面での評価を行うと共に、アクセス制御機構の課題として提示した項目のうち、運用管理を中心に課題解決のための検討を進めていく予定である。

謝辞

本研究は、情報処理振興事業協会技術センターにおける「組織間網環境におけるアクセス制御の研究」プロジェクトとして実施したものである。本プロジェクトを進めるにあたり、有益な助言と協力を頂いたプロジェクトのコンサルティング委員である創価大学 勅使河原 可海 氏、東京電機大学 滝沢 誠 氏、東洋大学 柴田 義孝 氏、北陸先端科学技術大学院大学 岡本 栄司 氏、(株)日立製作所 佐々木 良一 氏、ワーキング委員である高度通信システム研究所 グレン・マンスフィールド氏、東海大学 菊池 浩明 氏、ニチメングラフィックス(株) 田中 啓介 氏、明星大学 渡邊 晶 氏、東京電機大学 立川 敬行 氏、(株)ATR 知能映像通信研究所 江谷 為之氏、日立ソフトウェアエンジニアリング(株) 鮫島吉喜氏ならびに関係者の皆様に深く感謝致します。

参考文献

[1] Ravis S. Sandhu and Pierangela Samarati: "Access Control: Principles and Practice", IEEE Communications Magazine, P40-48 (1994.9)

[2] Daborah Lynn Estrin: "Access to Inter-Organization Computer Networks", MIT (1985)

[3] W.R.Cheswick, S.M.Bellovin: "Firewalls and Internet Security", Addison-Wesley Publishing, 306p (1994)

[4] Marcus J. Ranum: "Thinking about Firewalls", Proceedings of the Second World Conference on Systems and Netowrk Security and Management (1993.4)

[5] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones: "RFC1928: SOCKS Protocol Version 5", (1996.3), ftp://ds.internic.net/rfc/rfc1928.txt

[6] C. Partridge, "RFC974:Mail routing and the domain system", (1986),ftp://ds.internic.net/rfc/rfc974.txt

[7] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "RFC1448: Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)", (1993.5), ftp://ds.internic.net/rfc/rfc1448.txt

[8] 1993 年度 WIDE プロジェクト報告書,WIDE プロジェクト(1993)

[9] 寺田真敏, 芳原誠士, 村山優子：「組織間網環境におけるアクセス制御方式の提案」,マルチメディア通信と分散処理 74-30(1996.1)

[10] 寺田真敏, 芳原誠士, 村山優子：「名前による経路制御における問題点」,マルチメディア通信と分散処理 76-26(1996.5)

[11] 寺田真敏, 芳原誠士, 村山優子：「多段接続ファイアウォールにおけるユーザ認証に関する考察」,マルチメディア通信と分散処理 77-3(1996.7)