

## 組織間網環境におけるアクセス制御方式の提案

寺田真敏\*1,\*3 芳原誠士\*1,\*4 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

現在のインターネットは、組織毎にホストやルータが集合し、さらにネットワークを構成する組織間網の形態として発展しつつある。しかし接続性を重視した網間網のアーキテクチャには、組織間のアクセス制御機構がない。本稿では、組織間網のアーキテクチャにおけるアクセス制御機構のひとつとして、組織として強固なセキュリティの壁を保持しつつ、ユーザにとっては可能な限りセキュリティの壁が見えないようにするための透過なネットワーク環境の構築に関して概要を報告する。透過なネットワーク環境を提供するために、ユーザの活動範囲を定義する“ユーザアクセスドメイン”という概念を与え、網ベースのセキュリティの壁を保持しつつ、ユーザアクセスドメイン環境を提供するために“アクセスドメイン制御層”を導入する。

### Access Control for Inter-Organizational Computer Network Environment

Masato Terada \*1,\*3 Seiji Yoshihara \*1,\*4 Yuko Murayama \*2  
Information - Technology Promotion Agency, Japan (IPA) \*1  
Faculty of Information Sciences, Hiroshima City University \*2

The Internet has evolved to interconnect various networks on an organisational basis, rather than just on a network basis as in its original form. Since the original protocol architecture was motivated to seek out for connectivity, which makes it difficult to incorporate access control. We challenge this issue to tackle a problem; how one can provide a transparent network environment to users, while preserving security in each organisation with firewalls.

We define the User Access Domain to provide user-level grouping, and the Access Domain Control Layer to support such user level domain over the organisational networks with firewalls.

#### 1. はじめに

1970年代後半から始まったTCP/IP (Transmission Control Protocol/Internet Protocol) プロトコル体系による網間網、インターネットは成長を続け、現在では、単なる終端システム(ホスト)や中間システム(ルータ)から成る網というよりも、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なってきた(図1)。網間網のアーキテクチャ自体は、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入れられた形態ではない。

本稿では、現在検討を進めている組織間網のアーキテクチャにおけるアクセス制御機構の構想について、その概要を報告する。

\*3 (株)日立製作所より出向中

\*4 日本電気インフォメーションテクノロジー(株)から出向中

## 2. 既存アクセス制御機構

本節では、既存アクセス制御機構のひとつである「網ベースのアクセス制御(ホスト・ルータから成る集合体を網と捉え、網としてアクセス制御を実施)」と「ホストベースのアクセス制御(個々のホスト・ルータでアクセス制御を実施)」について報告する。

### (1) 網ベースのアクセス制御

網のアクセス制御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他のネットワークへの通信を許可するが、他のデータについては拒否するというような網間のアクセス制御機構として動作するものである。組織間網のアーキテクチャにおいては、主に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網間接続機能として利用されている。

例えば、組織外からの意図的な破壊や進入の阻止や、組織内からの不用意な情報の流出・流入防止を目的とし、外部(インターネット)と組織内との接続点に設置する。また、同一組織内においても、不用意な情報の流出・流入防止や、組織内でアクセス制御に関するポリシーの異なるグループ(網)間で、お互いのポリシーを維持することを目的とし、組織内網の相互接続する接続点に設置される(図2)。

### (2) ホストベースのアクセス制御

ホストベースのアクセス制御は、個々のホストマシンに対してアクセス制御を実施する。また、アクセス制御のための機構は、ホストマシン上に置かれ、ホストマシン自身を直接的に

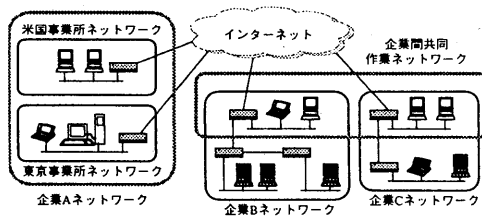


図1 組織間網環境の接続形態

保護する。ホストベースのアクセス制御機構として、パケットをフィルタリングする機能(ホストベースのファイアウォール)等がある。これは、事前に定義された規定に基づいて、どの要求を受け入れて、どの要求を拒絶するかを決定する。

ホストベースのセキュリティは、きめ細かくセキュリティ面での解決策を講じることができ、また網ベースのセキュリティを補完するものである。しかしながら、ホストベースのセキュリティの大きな問題点は、管理する機器の増加に伴い、総合的な保護機能を提供することが複雑化することである。

最良の方法は、網ベースのセキュリティ、ホストベースのセキュリティを組み合わせることにより、相互補完を行うことであると言える。

## 3. アクセス制御機構の概要

本節では、現在検討を進めている組織間網のアーキテクチャにおけるアクセス制御機構の概要を報告する。

### 3.1 解決したい課題

TCP/IP(インターネット)環境における不正行為パターンは著しく変化しており、これまでのパスワードや信頼されたホストを基にした攻撃は影をひそめ、システムの弱点を利用し洗練された侵入プログラムを用いた攻撃が主流になってきている。これに伴い、ホストベースのみのセキュリティ向上だけではなく、ファイアウォール等の網ベースでの防御が攻撃を撃退するのに必要となってきている。

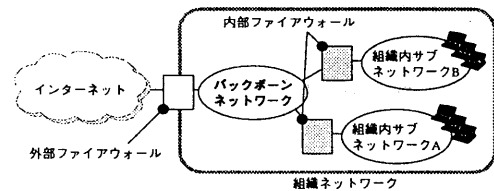


図2 ファイアウォール

組織間網のアーキテクチャにおいて、網ベースのセキュリティ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、ホストベースのセキュリティは個々のシステムを守るという点で、網ベースのセキュリティ施策の導入は有効である。

しかしながら、現在のTCP/IP環境のネットワークアプリケーションは、ファイアウォール等の網ベースのセキュリティを考慮にいれて作成されていないため、ファイアウォールを乗り越えて利用できるアプリケーションが限定されるとき、一人のユーザが複数の組織に所属する場合や職場が分散している場合、個人または部門で保有する情報を効率的に共有できない等の問題が生じている。

例えば、報告者らは、IPAと某社に所属しているが、共通的に利用できるドキュメントやフリーソフトウェアでさえ所属部署毎に別々に保守していかなければならない(図3)。

組織間網のアーキテクチャにおけるアクセス制御機構で解決したい課題は、ファイアウォール等の網ベースのセキュリティ導入による強固なセキュリティの壁を保持しつつ、ユーザにとっては可能な限りファイアウォール等の網ベースのセキュリティが見えないようにするための透過なネットワーク環境、すなわち、組織・個人の活動範囲を考慮したネットワーク環境を提供することにある。

本稿では、このような透過なネットワーク環境を「ネットワーク上に点在するオブジェクト

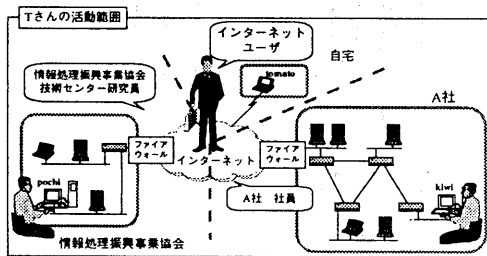


図3 解決したい課題の構成例

(サーバマシン等の物理的な装置、ネットワークアプリケーションサービス等)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ク環境」と定義する。

### 3.2 アクセス制御機構の概要

組織間網のアーキテクチャにおけるアクセス制御機構では、まず、ネットワークにおける組織・個人の活動範囲を定義するため、“ユーザアクセスドメイン(ユーザが透過なネットワークサービスを利用可能な範囲)”という概念を新たに導入する。次に、ファイアウォール等の網ベースのセキュリティ導入による強固なセキュリティの壁を保持しつつ、ユーザアクセスドメイン環境を提供する仕掛けとして、“アクセスドメイン制御層”を導入する。

#### 3.2.1 ユーザアクセスドメイン

ユーザアクセスドメインとは、ユーザが最終的に利用したいオブジェクト(サーバマシン等の物理的な装置、ネットワークアプリケーションサービス等)が存在する範囲である。すなわち、ネットワークにおけるユーザ(組織・個人)の活動範囲であり、またユーザ毎に保有することのできる論理的なネットワークである(図4)。

ユーザアクセスドメインは、以下の特徴を持つ。

- (1)ユーザは、ユーザアクセスドメインに帰属する全てのオブジェクトに対して透過にアクセス可能である。

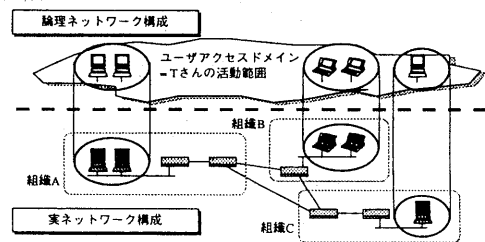


図4 ユーザアクセスドメイン

(2)ユーザアクセスドメインは、ユーザが利用可能な物理的なネットワーク資源の範囲である“エリア”から構成される。

### 3.2.2 エリア

ユーザアクセスドメインの構成要素として、“エリア”という概念を新たに導入した。ここで言う“エリア”とは、ファイアウォール等の網ベースのセキュリティ機構により分割されたネットワーク資源の範囲である。すなわち、分割されたネットワーク資源の集合は、同一のセキュリティポリシーに基づき制御されるものであり、例えば、ファイアウォール等により隔てられた組織が保有するネットワーク資源はひとつのエリアに帰属する(図5)。

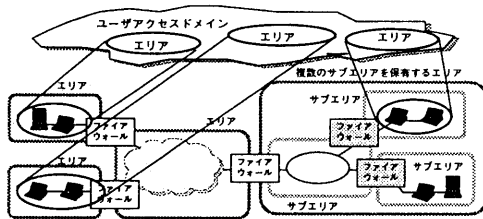


図5 ユーザアクセスドメインとエリア

以上のことから、ユーザアクセスドメインで提

供するユーザに透過なネットワーク環境とは、ユーザが最終的に利用したいオブジェクトが存在するエリアの集合体として再定義することができる。

### 3.2.3 アクセスドメイン制御層

アクセスドメイン制御層(ADCL:Access Domain Control Layer)は、ファイアウォール等の網ベースの強固なセキュリティの壁を保持しつつ、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の通信層である。

#### (1)開放型システム間相互接続モデル

アクセスドメイン制御層はTCP/UDP上位に配置し、トランスポート層のサブレイヤと位置付けた(図6)。これにより、網ベースのアクセス制御(ファイアウォール)におけるトランスポート層ゲートウェイ(図7)と同等のセキュリティ防壁、すなわち、ユーザやネットワークサービスアプリケーションに関するアクセス制御を提供する。また、トランスポート層ゲートウェイとして動作するアクセスドメイン制御層の多段接続により、ユーザに対して透過なネットワークサービス、すなわち、ユーザアクセスドメイン上でのエンドツーエンドのデータ転送を提供する。

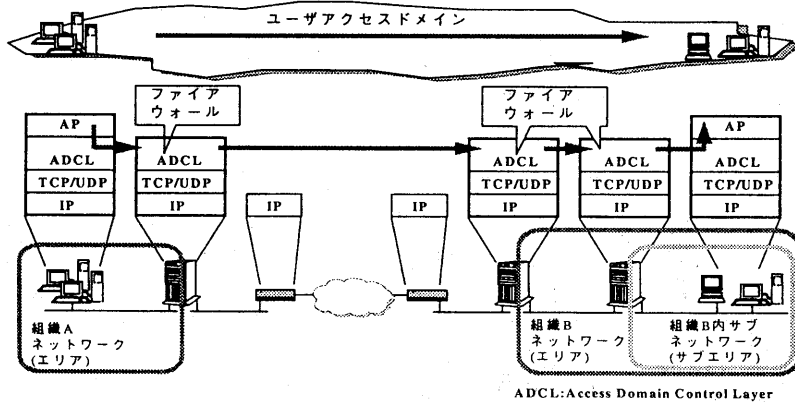


図6 アクセスドメイン制御層

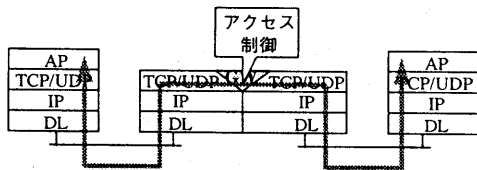


図7 トランスポート層ゲートウェイ

## (2) アクセスドメイン制御層の機能

アクセスドメイン制御層は、以下の2つの機能から構成される。

- ・エリア間の経路制御機能
- ・エリアに対するアクセス制御機能

### (a) 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、エンドツーエンドのデータ転送機能を提供する。

アクセスドメイン制御層における経路制御情報の保有、更新は、アクセスドメイン制御層を有するホスト間の関連を静的に定義する方法と、経路情報の交換によるホスト間の関連を動的に定義する方法等がある。

### (b) 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ポリシーに従い、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。

アクセス制御の対象項目は、ユーザ名、宛先ホスト名(アドレス)、送信元ホスト名(アドレス)、サービス、時刻等がある。

### (i) 網ベースのアクセス制御

エリアの境界におかれたアクセスドメイン制御層は、ユーザ名、サービス等に基づくデータの選択透過型のアクセス制御、すなわち、網ベースのアクセス制御を実施する。これは、現在のファイアウォールの標準構成であるスクリー

ニンド・サブネット、スクリーン・ホスト、デュアルホームゲートウェイにおける要塞ホスト(Bastion Host)にアクセスドメイン制御層を配置することに相当する。

### (ii) ホストベースのアクセス制御

ユーザが最終的に利用したいオブジェクトであるホストにおかれたアクセスドメイン制御層もユーザ名、サービス等に基づくデータの選択透過型のアクセス制御、すなわち、ホストベースのアクセス制御を実施する。

## 3.2.4 稼動環境の要件

本稿で提案するアクセス制御機構は、少なくともアクセスドメイン制御層を有する隣接ホスト間でIP層による直接通信ができる必要がある。このため、パケットフィルタリング等により、アクセスドメイン制御層を有する隣接するホスト間での通信が許可されない場合には、透過なネットワーク環境を提供することはできない。

## 4. プロトタイプシステム開発のアプローチ

現在、以下に示す方向で、アクセスドメイン制御層のプロトタイプシステム開発のための仕様検討を進めている。

エリア間の経路制御機能ならびに、エリアに対するアクセス制御機能により、実ネットワーク上に「ユーザアクセスドメイン」というユーザ毎の論理的なネットワークを構築することができる。この時、複数の「ユーザアクセスドメイン」の制御を考えた場合、網ベースのアクセス制御機構であるファイアウォールから構成された論理バックボーンネットワークを介したエリア間の通信として取り扱うことができる(図8)。

従って、プロトタイプシステム開発では、ファイアウォールから構成された論理バックボーンネットワークにおけるアクセス制御機能と捉え、論理バックボーンネットワークへのアクセス、ネットワーク内のファイアウォール間、さらに宛先ホストへのアクセスに分け、エリア間の経路制御機能ならびに、エリアに対するアク

セス制御機能を実現していく(図9)。

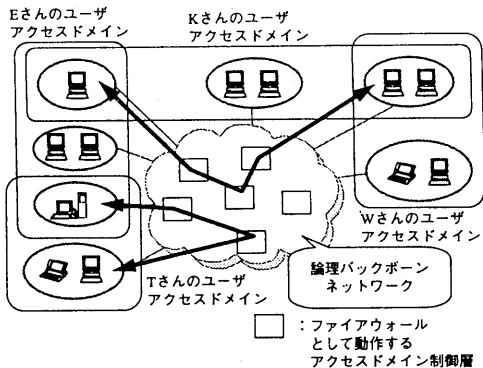


図8 複数ユーザアクセスドメインの制御

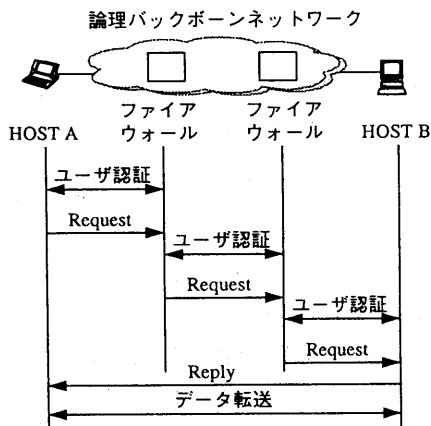


図9 TCP ベースのアプリケーションにおけるユーザ認証

### 5. 結論および今後の課題

本稿では現在検討中の組織間網環境におけるアクセス制御機構についてその概要を報告した。

今後、提案したアクセス制御機構の詳細について検討を進め、プロトタイプシステムの開発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。本研究を進めるにあたって、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 教授、東京電機大学 滝沢 誠 教授、東洋大学 柴田 義孝 助教授、北陸先端科学技術大学院大学 岡本 栄 司 教授、(株)日立製作所 佐々木 良一 氏、ワーキング委員である東海大学 菊池 浩明 氏、ニチメングラフィックス(株) 田中 啓介 氏、日立電線(株) 渡邊 晶 氏、東京電機大学 上川 敬行 氏、富士通関西通信システム(株) 江谷 為之氏、高度通信システム研究所 グレン・マンスフィールド 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]1993 年度 WIDE プロジェクト報告書,WIDE プロジェクト(1993)