組織間網環境におけるアクセス制御方式

寺田真敏[†,☆] 芳原誠士[†,☆☆] 村山優子[††]

インターネットの利用においては，インターネットとの接続性を確保しながら，悪質な侵入者によるシステム破壊等の危険性を回避することが重要な課題となっている．しなしながら，不正なアクセスを防ぐためのアクセス制御は接続性とは相反する技術であり，アクセス制御機構として動作するファイアウォールの存在はユーザの利便性を低下させてしまう場合がある．そこで，本論文では，ネットワーク上でのユーザ活動を支援するために，『ファイアウォール導入による組織としてのセキュリティの壁を保持しつつ，ユーザには可能な限りファイアウォールの存在を見せない透過的なネットワーク環境』の構築を目的としたアクセス制御機構を提案する．アクセス制御機構は，ユーザの利用可能な透過的なネットワーク環境とその範囲を定義するための概念である「ユーザアクセスドメイン」と，透過的な接続機能とアクセス制御機能を兼ね備えた「アクセスドメイン制御層」を用いて実現する．さらに，提案システムに基づき開発したプロトタイプシステムの評価を通じて，本提案方式の有効性を示す．

Access Control for Inter-organizational Computer Network Environment

MASATO TERADA,[†,☆] SEIJI YOSHIHARA[†,☆☆] and YUKO MURAYAMA[††]

Internetworking is becoming the technology platform for a growing range of business uses. When you connect your local network to the Internet, the single most important measure you can take to prevent break-ins is to define a network security policy. In this work, we have examined how one can provide a transparent network, while preserving security policy of organizations by implementing and maintaining strict access control using firewalls. We propose a "User Access Domain (UAD)" to provide user-level grouping, and a "Access Domain Control Layer (ADCL)" to support the user level domain over the organizational networks with firewalls. While the User Access Domain provides the framework for virtual private networks the Access Domain Control Layer provides firewall-transparent TCP/UDP connectivity in what appears to be a seamless logical network spanning the User Access Domain. A proof-of-concept prototype has been developed for evaluation.

1. はじめに

インターネットは，ビジネス分野への普及とともに，企業情報システムのネットワーク基盤の中に取り込まれつつある．これにともない，インターネットとの接続性を確保しながら，悪質な侵入者によるシステム破壊等の危険性を回避することが重要な課題となっている．このような状況にあって，各企業では，企業が保有する計算機やルータをアクセス制御により保護をしながらインターネット接続を進めている．このような接続形態を，組織としてのアクセス制御が行われた後，ネットワークを構成することから組織間網接続と呼ぶこととする．

ネットワークを保護するアクセス制御技術にファイアウォールがある[1)]．ファイアウォールはあらかじ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アクセス制御を行う．しなしながら，不正なアクセスを防ぐためのアクセス制御は接続性とは相反する技術であり，アクセス制御機構として動作するファイアウォールの存在はユーザの利便性を低下させてしまう場合がある．たとえば，ファイアウォールを通過するたびに利用者を確認するためのユーザ認証が必要で

† 情報処理振興事業協会
Information - Technology Promotion Agency, Japan (IPA)
☆ 現在，株式会社日立製作所システム開発研究所
Presently with Systems Development Laboratory, Hitachi Ltd.
☆☆ 現在，日本電気インフォメーションテクノロジー株式会社
Presently with NEC Information Technology Inc.
†† 広島市立大学情報科学部
Faculty of Information Sciences, Hiroshima City University

あったり，ファイアウォールを介して通信することのできる計算機が限定されてしまうなどをあげることができる．これは，以下に示すような接続性や操作性を重視したネットワーク上でのユーザ活動を制限することになってしまう．

- 出張等による移動先から職場に設置された計算機の利用
- 分散している職場間での計算機の相互利用
- 自宅から職場に設置された計算機の利用
- 1人のユーザが複数組織に所属し，所属先に設置された計算機の利用

そこで，本論文では，上記に示すネットワーク上でのユーザ活動を支援するために，『ファイアウォール導入による組織としてのセキュリティの壁を保持しつつ，ユーザには可能な限りファイアウォールの存在を見せない透過的なネットワーク環境』の構築を目的としたアクセス制御機構を提案する．すなわち，不正なアクセスを防ぐアクセス制御の実施と，ユーザの利便性を低下させない接続性の確保を両立させるネットワーク環境の構築を行う．

まず，アクセス制御と接続性という相反する問題を解決するために，ユーザごとに利用可能なネットワークの範囲を制御する「ユーザアクセスドメイン」という概念を導入する．ここで，ユーザとは企業等の組織や利用者個人が該当する．ユーザにとってユーザアクセスドメインは，透過的な接続性の確保されたアクセス可能なネットワーク資源の範囲となる．一方，組織のネットワークやセキュリティ管理者にとってユーザアクセスドメインは，不正なアクセスを防ぐために，許可したユーザだけがファイアウォールを通過して，許可したネットワークサービスのみを利用できるというアクセス制御機構となる．次に，ユーザアクセスドメインを実現するための仕掛けとして，透過的な接続機能とアクセス制御機能を兼ね備えた「アクセスドメイン制御層」を提示する．さらに，提案システムに基づき開発したプロトタイプシステムの評価を通じて，本提案方式の有効性を示す．

以下では，まず，2章で既存ファイアウォールシステムの問題点を示す．次に，3章でアクセス制御機構のアーキテクチャであるユーザアクセスドメインの考え方を示した後，4章でユーザアクセスドメインを実現するアクセスドメイン制御層の機能を示す．5章では開発したプロトタイプシステムの評価を行う．最後に6章で本論文のまとめと今後の課題について述べる．

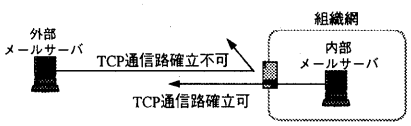
2. 既存のファイアウォールシステムの問題点

本章では，アクセス制御と接続性の見地から，既存のファイアウォール技術を用いてシステムを構築した際の問題点について述べる．

(1) アクセス制御に関する問題

インターネット接続において，企業が保有する計算機やルータを保護するファイアウォール構築技術として，IP（Internet Protocol）層でのパケットフィルタリング[1]技術がある．パケットフィルタリングは，IPパケットの始点と終点IPアドレス，始点と終点ポート番号，さらにTCP（Transmission Control Protocol）通信で使用するフラグ情報を用いて，IPパケットごとにアクセス制御を行う．たとえば，**図1**に示すような構成の場合，電子メールを送信するために，組織網内部の計算機から外部の計算機に対してTCP通信路を確立できるが，外部から組織網内部の計算機に対してTCP通信路は確立できない制御を行う．これにより，組織網内部からインターネットへの接続性を確保するとともに，外部からの不正なアクセスを防ぐ．

しかし，インターネットのビジネス利用への普及とともに，これまで組織網内部からインターネットへのアクセスだけであった利用形態は，インターネット経由で組織網内部の計算機へアクセスしたり，インターネットを介した企業間，組織網間の接続という新たな利用形態へと広がってきている．ここで問題となるのが，インターネット経由で組織網内部へアクセスする場合のアクセス制御である．パケットフィルタリングでは，固定的なIPアドレスを持つ計算機をアクセス制御の対象としている．一方，インターネット接続で一般的に利用されているダイアルアップ接続では，IPアドレス管理とIPアドレス枯渇問題に対処するため，接続時にのみ有効となる一時的なIPアドレス割当て機構を採用している．このため，ダイアルアップ接続



動作	始点IPアドレス	ポート	終点IPアドレス	ポート	フラグ	コメント
許可	内部ホスト	*	*	25		外部のSMTPポートへのパケット
許可	*	25	内部ホスト	*	ACK	外部からの応答
遮断	*	*	*	*		上記条件以外のパケットを遮断

SMTP: Simple Mail Transfer Protocol

図1 パケットフィルタリングによるアクセス制御例
Fig. 1 Access control with packet filtering.

の場合には，パケットフィルタリングを用いたアクセス制御を実施することができない．

また，この問題は，単にパケットフィルタリングによるアクセス制御の問題だけではなく，IPアドレスに依存しないアクセス制御機構の必要性を示唆している．

(2) ユーザの操作性低下に関する問題

企業情報システムのネットワーク化にともない，ネットワーク上でのアクセス制御として，ネットワークを利用するユーザを対象としたアクセス制御の実施が必要とされてきている．これは，アクセス制御の問題で提示したIPアドレスに依存しないアクセス制御機構の必要性と合致する．

ユーザを対象としたアクセス制御には，ファイアウォール構築技術の1つであるアプリケーションゲートウェイを利用することができる[2]．アプリケーションゲートウェイは，ファイアウォールとして動作する計算機上で動作させるデータ中継プログラムであり，データ中継を行う際にIPアドレス，ポート番号のほか，個々のアプリケーションのプロトコルを解釈し，プロトコルに基づいたユーザ認証，利用可能なコマンドの制限等を行う．たとえば，**図2**に示すような遠隔端末接続（telnet）プログラムを用いて，計算機pochiからtomatoにアクセスする場合を考える．ここで，遠隔端末接続（telnet）用のアプリケーションゲートウェイを用いることにより，許可したユーザだけがファイアウォールを通過して，目的とする計算機tomatoにのみ接続するアクセス制御を実施することができる．これは，組織間網環境において，異なる部署間での相互アクセス制御や，インターネット経由での組織網内部の計算機へのアクセス制御において有用である．しかし，図2に示すように，ユーザは経由するすべてのアプリケーションゲートウェイ（kiwi, orange）の明示的な経路指定と，ユーザ認証操作を繰り返す必要がある．このように，アプリケーションゲートウェイはIPアドレスに依存しないアクセス制御機構を提供する反面，ユーザの操作性の低下をもたらす．

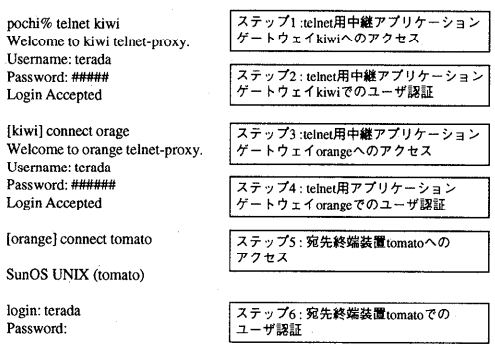


図2 遠隔端末接続（telnet）用アプリケーションゲートウェイによるアクセス制御例

Fig. 2 Access control with telnet application-gateway.

上述のように，組織間網環境のアクセス制御においては，IPアドレスに依存せず，接続性ならびにユーザの操作性を確保するアクセス制御機構が必要不可欠である．

3. アクセス制御機構のアーキテクチャ

本章では，2章で述べた問題を解決し，アクセス制御と接続性を両立させるアーキテクチャについて述べる．

3.1 ユーザアクセスドメインとエリア

本アーキテクチャのための新しい概念を以下に紹介する．

(1) ユーザアクセスドメイン

ネットワーク上に点在するユーザの興味の対象であるオブジェクト，たとえば，サーバマシン等の物理的な装置や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ネットワーキング環境を「論理ネットワーク」と呼ぶ．**図3**に示すような論理ネットワークとは，ユーザに対してセキュリティの壁となるファイアウォールの存在を見せない透過的なネットワーク環境である．また，ユーザの所属や役割に応じたネットワーク資源へのアクセス制限や，不正なアクセスからネットワーク資源を保護するために，本論理ネットワークを組織や個人ユーザごとに構築する．本論文では，**図4**に示すように，ユーザごとに構築した「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

セキュリティの壁となるファイアウォールの役割は，組織のセキュリティ方針に従い，ネットワーク資源を保護するためのアクセス制御を実施することである．このようなセキュリティ方針は，ファイアウォールの

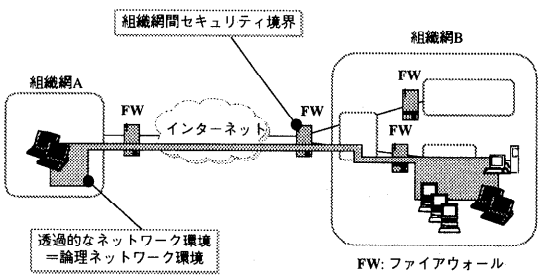


図3 論理ネットワーク

Fig. 3 Logical network.

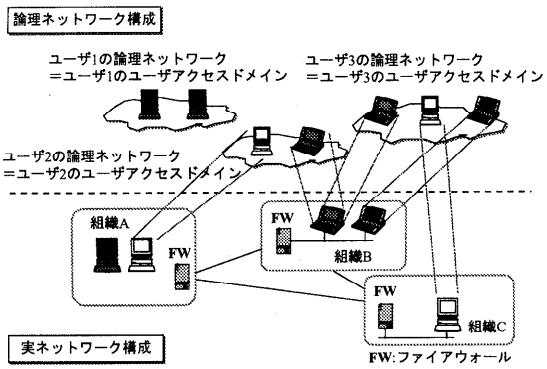


図4 ユーザアクセスドメイン
Fig. 4 User access domain.

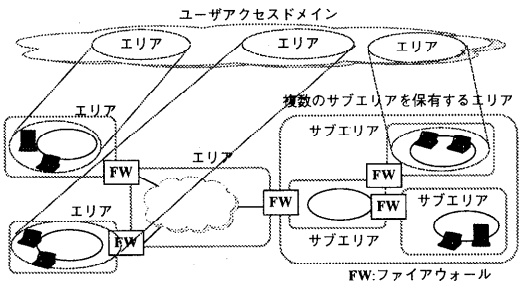


図5 ユーザアクセスドメインとエリアの関連
Fig. 5 Relationship between "user access domain" and "area".

設置場所や，ファイアウォールを用いて保護するネットワーク資源の内容によって異なる．この場合に必要なことは，各組織が保有するセキュリティ方針をユーザアクセスドメインに反映するための機構である．

「エリア」はユーザアクセスドメインの構成要素であり，同一のセキュリティ方針に基づき制御される範囲である．たとえば，**図5** に示すようにファイアウォールにより隔てられた各組織が保有するネットワーク資源は1つのエリアに帰属する．また，階層化したエリアは，上位エリアから下位エリアへとセキュリティ方針が継承されると考える．このようなセキュリティ方針を反映する領域としてエリアという概念を導入し，さらに，ユーザアクセスドメインを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関係付けを行う．これにより，ユーザアクセスドメインが単なる透過的なネットワークとしてだけではなく，各組織が保有するセキュリティ方針を反映したネットワークとしての特性を持たせることができる．

3.2 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，ユーザアクセスドメインを提供するための通信層である．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6** に示すように，終端装置や中継装置上に配置し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する．ここで，アクセスドメイン制御層は，組織間のセキュリティの壁となるファイアウォールとして動作する側面と，透過的なネットワークサービスを提供する側面を兼ね備えた通信層となる．また，アクセスドメイン制御層の配置にあたっては，以下の理由から図6に示すようにTCP/UDP層上位サブレイヤに位置付けた．

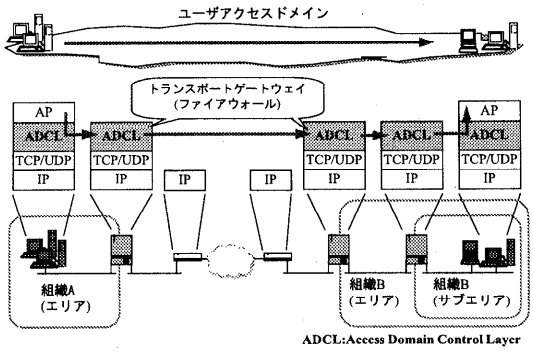


図6 アクセスドメイン制御層の階層モデル
Fig. 6 Layer model of access domain control layer.

- アプリケーションに非依存なセキュリティ防御壁

アクセスドメイン制御層は，ファイアウォール技術の1つであるトランスポートゲートウェイに分類される．TCP/UDP層上位サブレイヤで動作するアクセスドメイン制御層は，アクセスドメイン制御層自身が独自に持つユーザ認証とアクセス制御機構とを用いることにより，アプリケーションに依存しないセキュリティの壁を構築する．これは，どのようなアプリケーションに対しても，エリアが保有するセキュリティ方針をファイアウォールに反映することができる．

- アプリケーションに非依存なデータ中継制御機構

トランスポートゲートウェイ方式に分類されるアクセスドメイン制御層の特徴は，独自のユーザ認証とアクセス制御機構に加え，独自のデータ中継制御機構を持つことにある．これは，IP層での通信を遮断するファイアウォール環境において，ファイアウォールとして動作する計算機上にアクセスドメイン制御層を導入することによりユーザアクセスドメインを構築することができる．さらに，中継という考え方を持たない遠隔端末接続（telnet）やファイル転送（ftp）のようなクライアント・サーバ型のアプリケーション利用環境をユーザアクセスドメイン上に構築しやすいことがあげ

られる．

4. アクセスドメイン制御層の機能

本章では，アクセスドメイン制御層の基本機能であるエリア間の経路制御機能とアクセス制御機能について述べる．エリア間の経路制御機能は，論理ネットワーク上に点在するオブジェクトをあたかも同じネットワーク上にあるような操作性を提供し，アクセス制御機能は,「エリア」の運用管理者のセキュリティ方針に従い「エリア」内に存在するオブジェクトへのアクセス制御を行う．

4.1 エリア間の経路制御機能

エリア間の経路制御機能は，オブジェクト間に透過的な論理通信路を提供するデータ転送と，論理通信路が経由するエリアを決定する．

4.1.1 透過的なデータ転送機能

透過的なデータ転送機能は，ユーザアクセスドメイン上のアプリケーションに対して，TCP と UDP 通信のための透過的な論理通信路を提供する．本項では，TCP と UDP 通信用の透過的な論理通信路の確立手順を示す．

(1) **TCP 転送機能**

TCP 転送機能は，論理ネットワークに接続する計算機間で TCP 通信を用いたデータ転送を提供する．TCP 転送機能は，まず，論理ネットワークに接続する計算機の TCP 通信要求に従い，ADCL 論理通信路と呼ぶコネクション型の論理通信路を終端装置間に確立する．次に，この論理通信路を用いて TCP 通信のデータ転送を行う．ADCL 論理通信路とは，ユーザアクセスドメイン制御層により分断されている TCP の論理通信路を連結接続したコネクション型の論理通信路であり，以下に示す手順で確立を行う（図 **7**）．

(a) ADCL を実装したクライアント（以下，ADCL クライアントと呼ぶ）は，ADCL を実装した中継装置（以下，ADCL-GW と呼ぶ）との間で TCP の論理通信路を確立後，ADCL-GW に対して「ADCL 論理通信路確立要求（ADCL-T 接続要求）」パケットを送信する．

(b) ADCL-GW は，受信パケットに基づき，隣接する ADCL-GW との間で TCP の論理通信路を確立後，受信したパケットを次 ADCL-GW に転送する．

(c) 上記操作を繰り返すことにより，ADCL-GW で分断されていた TCP 論理通信路は，ADCL クライアントと ADCL サーバ間の終端装置間で連結接続した TCP 論理通信路となり，ADCL 論理通信路として構成される．

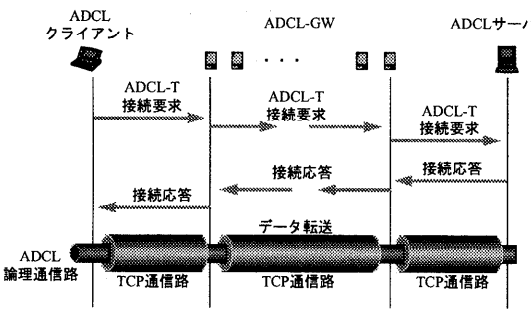


図 7 ADCL の論理通信路の確立
Fig. 7 Establishing ADCL connection.

(2) **UDP 転送機能**

UDP 転送機能は，論理ネットワークに接続する計算機間で UDP 通信を用いたデータ転送を提供する．UDP 転送機能は，まず，論理ネットワークに接続する計算機の UDP 通信要求に従い，ADCL アソシエーションと呼ぶコネクションレス型の論理通信路を終端装置間に確立する．次に，この論理通信路を用いて UDP 通信のデータ転送を行う．ADCL アソシエーションとは，ユーザアクセスドメイン制御層により分断されている UDP のアソシエーションを連結接続したコネクションレス型の論理通信路である．また，ADCL アソシエーション確立における UDP 転送機能の特徴は，ADCL 論理通信路を ADCL アソシエーション用の制御通信路として利用するところにある．UDP 転送機能において，ADCL 論理通信路の役割は以下のとおりである．

- ADCL アソシエーションの存続期間の制御
- ADCL アソシエーションで使用する ADCL-GW 上の UDP データ中継機能（使用ポート番号，アクセス制御等）の制御

ADCL アソシエーションは，以下に示す手順で確立を行う（図 **8**）．

(a) ADCL クライアントは，ADCL-GW との間で TCP の論理通信路を確立後，ADCL-GW に対して「ADCL アソシエーション確立要求（ADCL-U 接続要求）」パケットを送信する．

(b) ADCL-GW は，受信パケットに基づき，ADCL アソシエーション用の UDP データ中継機能の稼動準備を行う．

(c) 隣接する ADCL-GW との間で TCP の論理通信路を確立後，受信したパケットを次 ADCL-GW に転送する．

(d) 上記操作を繰り返すことにより，ADCL-GW で分断されていた UDP アソシエーションは，ADCL-

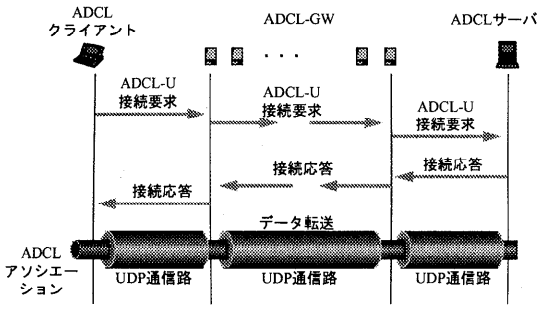


図8 ADCL アソシエーションの確立
Fig. 8 Establishing ADCL association.

GW が提供する UDP データ中継機能を介して，ADCL クライアントと ADCL サーバ間の終端装置間で連結接続した UDP アソシエーションとなり，ADCL アソシエーションとして構成される．

4.1.2 経路制御機能

本項では，論理通信路が経由するエリアを決定する経路制御について述べる．

論理ネットワークに接続する計算機は，宛先エリア内の終端装置に対して ADCL 論理通信路/アソシエーションを確立するために，いくつかの ADCL-GW を経由する．この際使用する ADCL-GW を決定するのがエリア間の経路制御機能であり，ADCL クライアント，ADCL-GW ならびに ADCL サーバが保持するエリア間の経路制御情報を用いて制御する．また，この経路制御機能は，ADCL 独自の機能でありアプリケーションには依存しない．

ADCL の経路制御の対象となる項目は以下のとおりである．

- サービス（ポート番号）
- 宛先エリアと次送信先
- 経路選択の優先度（オプション）

図 9 に示すような経路制御の場合，ADCL-GW adclgw.potato.ad.jp では，組織 tomato.go.jp に置かれた計算機 server.tomato.go.jp に対する ADCL の論理通信路確立要求パケットを受信すると，ADCL-GW が保有する経路制御情報に従い，ADCL-GW adclgw.kiwi.ad.jp にパケットを転送する．

また，エリア間の経路制御で使用する情報は，ADCL クライアント，ADCL-GW ならびに ADCL サーバに対して，以下に示す方法で定義する．なお，5 章のプロトタイプシステムでは，各 ADCL に対してエリア間の経路制御情報を静的に定義することにより，本機能を実現している．

- 各 ADCL への静的なエリア間経路制御情報の定義

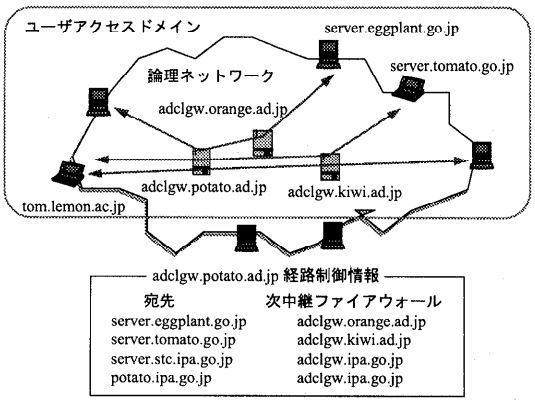


図9 経路制御情報
Fig. 9 Configuration of route control.

- DNS（Domain Name Services）等の経路制御情報提供サーバを用いた情報の定義

4.2 エリア間のアクセス制御機能

本節では，「エリア」運用管理者のセキュリティ方針に従い，「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エリア間のアクセス制御機能について述べる．

4.2.1 アクセス制御情報

エリア間のアクセス制御機能は，各ユーザに対して透過的な接続性を提供する範囲を定義し，各ユーザのユーザアクセスドメインを構成する．また，組織のネットワークやセキュリティ管理者に対しては，許可したユーザだけがファイアウォールを通過して，許可したネットワークサービスのみを利用することのできるアクセス制御機構として動作する．

ADCL のアクセス制御の対象となる項目は以下のとおりである．

- ユーザまたはグループ（組織）
- サービス（ポート番号）
- 宛先エリアと送信元エリア

たとえば，**図 10** のように，ADCL-GW adclgw.potato.ad.jp が保有するアクセス制御情報によれば，ユーザ Sam の場合，telnet サービスを color.com から color.edu との間でのみ利用することができることになり，これがユーザ Sam のユーザアクセスドメインとなる．

4.2.2 アクセス制御機能

本アクセス制御機能は，ADCL 論理通信路/アソシエーションを利用するユーザが正当なユーザであるか否かのユーザ認証操作と，そのユーザが ADCL 論理通信路/アソシエーションを用いて利用できるネット

adelgw.potato.ad.jp アクセス制御情報

ユーザ	送信元	宛先	宛先サービス
Sam	color.com	color.edu	telnet
Anne	mars.space.fr	moon.space.fr	http
Eric	ipa.go.jp	kiwi.ad.jp	ftp

図10 アクセス制御情報
Fig. 10 Configuration of user access control.

ワーク資源へのアクセス制御操作とから構成される．

(1) ユーザ認証操作

ユーザ認証操作は，ADCL 論理通信路/アソシエーション確立を要求するユーザが本人であるか否かの確認であり，X.509[3]に規定された簡易認証または厳密認証を使用する．これらのユーザ認証情報は，ADCL-T/ADCL-U 接続要求パケット内のユーザ認証フィールドに格納する．ADCL-GW ならびに ADCL サーバは，ADCL-T/ADCL-U 接続要求パケット受信時に，受信パケット内のユーザ認証フィールド情報と自身が保持するユーザ認証情報と比較し確認を行う．ユーザ認証情報の一致が確認できた場合，次ステップとなるアクセス制御操作に入る．一致しなかった場合，接続を拒否する ADCL-T/ADCL-U 接続応答を返信後，TCP 論理通信路の切断操作を行い，途中まで確立した ADCL 論理通信路の解放を行う．

(2) アクセス制御操作

アクセス制御操作では，ユーザ認証により確認したユーザに対して，利用可能なネットワーク資源の制限を行う．ADCL-GW ならびに ADCL サーバは，ADCL-T/ADCL-U 接続要求パケット受信時に，受信パケット内の宛先エリアやサービス情報と，自身が保持するアクセス制御情報との比較を行う．接続要求が許可した範囲内にあれば，接続要求パケットを次送信先である ADCL-GW または ADCL サーバに転送する．一方，許可範囲外であれば，**図 11** に示すように，接続を拒否する ADCL-T/ADCL-U 接続応答を返信後，TCP 論理通信路の切断操作を行い，途中まで確立した ADCL 論理通信路の解放を行う．

5. プロトタイプシステムの開発

本章では，提案したユーザアクセスドメインならびにアクセスドメイン制御層を評価するために開発したプロトタイプシステム ADAMS（Access DomAin Management Systems）について述べる．

5.1 特　　徴

開発したプロトタイプシステム ADAMS の特徴は，以下のとおりである．

- TCP 通信に関する透過的なデータ転送

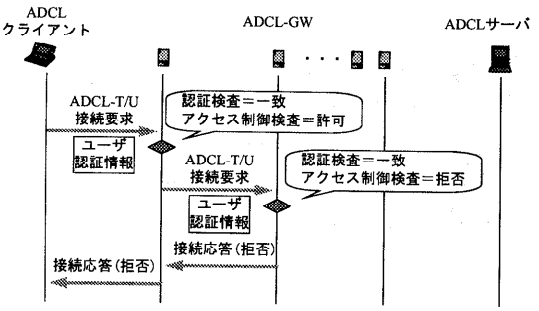


図11 アクセス制御機構
Fig. 11 Mechanism of user access control.

ユーザアクセスドメイン内の終端装置間で TCP 通信に関する透過的なデータ転送を提供する．

- エリア間の経路制御

エリア間の経路制御には，ADCL クライアント，ADCL-GW ならびに ADCL サーバ上に静的に定義したサービス，宛先エリアと次送信先から構成される経路制御情報を用いる．宛先エリアと次送信先情報の記載は，ドメイン名ならびに IP アドレスによる定義を可能としている．なお，経路選択の優先度は支援していない．

- エリア間のアクセス制御

エリア間のアクセス制御には，ADCL-GW ならびに ADCL サーバ上に静的に定義したユーザ，サービス，宛先エリアと送信元エリアから構成されるアクセス制御情報を用いる．宛先エリアと送信元エリア情報の記載には，ドメイン名ならびに IP アドレスによる定義を可能としている．

- ユーザ認証

ADCL 論理通信路の確立を要求する ADCL クライアントの認証機構として，X.509 の簡易認証と厳密認証の両機構を採用した．認証には，ADCL クライアント，ADCL-GW ならびに ADCL サーバ上に静的に定義した認証情報を用いる．

- データ暗号化

ADCL クライアントと ADCL-GW/ADCL サーバ間で ADCL 論理通信路上のデータ暗号化とデータの完全性保証を行う．データ暗号化には DES 56 ビットのセション鍵を，完全性保証には MD5 を使用する．なお，データ暗号化は X.509 に基づく厳密認証使用時に有効となる．

5.2 システムの構成

開発プラットフォームには，SunOS 4.1.3 と Solaris 2.2 を使用した．ソフトウェア構成は，**図 12** に示すように，ADCL クライアント上のアプリケーションに

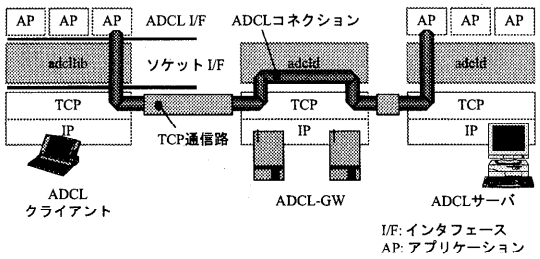


図12 プロトタイプシステム-ADAMS
Fig. 12 Prototype system-ADAMS.

表1 ADCL論理通信路確立時間
Table 1 Establishing time of ADCL connection.

ADCL-GW段数	0	1	2
確立時間（秒）	1.48	1.93	2.53

はソケットインタフェース型のライブラリ（adcllib）を提供し，ADCL-GW，ADCLサーバ上にはサーバデーモン（adcld）を提供する．開発に使用した言語はC言語であり，プログラムサイズは，クライアントライブラリ5Kステップ，サーバプログラム3Kステップである．

ADCLクライアント側では，ADCLクライアント上で動作するアプリケーションを本プロトタイプシステムが提供するライブラリへの移植が必要となる．移植工数を軽減するために，既存ソケットインタフェースからの移植を容易とする関数構成としている．また，ADCLサーバ上のサーバアプリケーションについては，既存のサーバアプリケーションに変更を加えることなく利用可能としている．

5.3 プロトタイプシステムの評価

ワークステーション（SunSparc Classic，SunOS 4.1.3）を用いて，プロトタイプシステムADAMSの評価を行った．評価は，LAN上でのADCL論理通信路の確立時間，ADCLのデータ転送スループットと応答性能の測定に加え，実環境での実験的な利用により行った．結果は，以下のとおりである．

(1) ADCL論理通信路確立時間

本システムを起動し，X.509に基づく厳密認証手順を用いた際のADCL論理通信路が確立されるまでの時間をLAN（10 Mbps）上で実測した．測定値は20回行った平均をとった（**表1** 参照）．通常LAN上でのTCPの論理通信路の確立時間は数十ミリ秒以下である．これに対し，プロトタイプシステムADAMSのADCL論理通信路の確立時間は秒単位となる．また，ADCL-GW段数の増加により速度的な問題は顕著となる．

表2 LAN上でのデータ転送スループット性能
Table 2 Throughput of data transfer on LAN.

ADCL-GW段数	0	1	2
暗号なし（Mbps）	3.34	3.46	3.47
暗号あり（Mbps）	0.83	0.84	1.00

表3 LAN上での応答性能
Table 3 Response of data transfer on LAN.

ADCL-GW段数	0	1	2
暗号なし（packet/sec）	226	207	162
暗号あり（packet/sec）	5.0	5.0	4.5

表4 インターネット上でのデータ転送のスループットと応答性能
Table 4 Throughput and response of data transfer on the Internet.

実験環境	non-ADCL環境	ADCL環境（暗号あり）
スループット性能（Mbps）	0.02	0.02
応答性能（packet/sec）	4.7	1.0

(2) データ転送スループットと応答性能

ネットワーク性能評価測定ツールとして広く利用されているnetperf[4]をadcllib上に移植したadcl-netperfを用いて，データ転送のスループットと応答性能をLAN（10 Mbps）上で実測した．測定値は20回行った平均をとった（**表2**，**表3** 参照）．netperfでは同一パラメータ条件の下で，データ転送のスループット性能は5.5 Mbps，応答性能は470パケット/秒である．adcl-netperfを用いた場合，ADCLでのデータ転送処理がともなうため，データ転送のスループットならびに応答性能の低下は大きい．なお，スループット性能は，ADCL-GW段数の影響を受けずにほぼ一定となっている．

(3) 実環境での実験的な利用

5台のワークステーションから構成されるADAMS実験環境を構築し，adcl-netperfを用いて，データ転送のスループットと応答性能を測定した．ADCLクライアントとADCLサーバ間には3段のADCL-GWが介在しており，3段目と4段目のADCL-GWはインターネットによって相互接続されている．また，比較対象として，インターネットに接続する3段目と4段目の計算機間でADCLを使用しない環境を構築し，netperfを用いた測定を行った（**表4** 参照）．インターネットを介した利用では，ADAMS環境とADCLを使用しない環境での性能上の差異がほとんどないことが明らかとなった．

また，操作性とアクセス制御については，adcllib上に移植した遠隔端末接続（telnet）プログラムadcl-

telnetを用いて評価を行った．実験から，以下の結果が得られた．

- ADAMS環境を利用しない通常操作では目的とする計算機に遠隔端末接続（telnet）するために，最低でも4回のtelnet操作が必要となる．これに対し，ADAMS環境を利用すれば，1回のtelnet操作で目的とする計算機にtelnetログインすることができる．
- telnetログインまでの所要時間は平均して5秒であり，ADAMS環境を利用しない通常操作に比べ，大幅な操作所要時間の短縮が可能となる．
- telnetによる遠隔端末操作の応答性能は，DES 56ビットによるADCL論理通信路暗号化時とADAMS環境を利用しない通常操作時で差異はほとんどない．
- エリア間のユーザ認証操作とアクセス制御操作により，許可したユーザだけがファイアウォールとして動作するADCL-GWを通過し，許可したネットワークサービスのみを利用することができることを確認した．

プロトタイプシステムADAMSを用いた実環境での実験的な利用から，本論文で提案したユーザアクセスドメインならびにユーザアクセスドメイン制御層のアーキテクチャが実現可能であり，インターネットを用いた利用においては，以下の点で十分に実用可能である考える．

- 性能

ADCL論理通信路のデータ暗号通信は，通常操作時に遜色ない性能を提供することができる．

- 操作性

ADCL独自のユーザ認証，アクセス制御とデータ中継制御機構とを利用することにより，通常操作で必要となるユーザ認証操作回数を低減することができる．これにより，操作性の向上を図ることができる．

- アクセス制御

組織のネットワークやセキュリティ管理者に対して，ファイアウォールとして動作するADCL-GWにおいて，ユーザとサービスに基づくアクセス制御機構を提供することができる．

6. おわりに

本論文では，組織間網環境において，ネットワーク上でのユーザの活動を支援するためのアクセス制御機構を提案した．まず，「ユーザアクセスドメイン」と呼ぶ概念を導入し，アクセス制御と接続性という相反する問題を解決するための方向性を示し，次に，透過的な接続機能とアクセス制御機能を兼ね備えた「アクセスドメイン制御層」の機能を提示することで，ユーザアクセスドメインの実現方法を示した．さらに，提案システムに基づき開発したプロトタイプシステムの評価を通じて，**図13**に示されるようなユーザごとにネットワーク，ならびにサービス利用範囲の限定可能な論理ネットワークを構築することができることを示した．

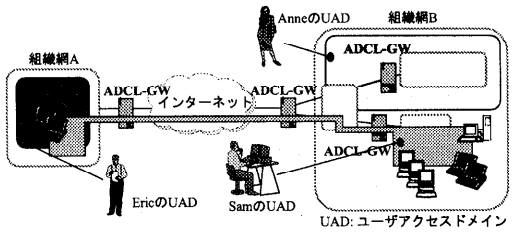


図13 ユーザごとの論理的なネットワーク
Fig. 13 Virtual private network for user.

今後は，プロトタイプシステムADAMSにおけるADCLの経路制御機能，ネットワークセキュリティの評価指針であるレッドブック[5]に従ったアクセス制御機能の評価を行うとともに，UDP通信機能の開発と，各ADCL-GW，ADCLサーバで，静的に定義を行っている経路制御情報，アクセス制御情報とユーザ認証情報を統括管理する機構を検討したいと考えている．

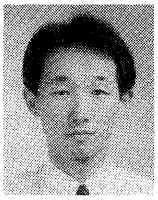
謝辞 本研究は，情報処理振興事業協会技術センターにおける「組織間網環境におけるアクセス制御の研究」プロジェクトとして実施したものである．本プロジェクトを進めるにあたり，有益な助言と協力をいただいたプロジェクトのコンサルティング委員である創価大学勅使河原可海氏，東京電機大学滝沢誠氏，東洋大学柴田義孝氏，北陸先端科学技術大学院大学岡本栄司氏，(株) 日立製作所佐々木良一氏，ワーキング委員である東北大学グレン・マンスフィールド氏，東海大学菊池浩明氏，ニチメングラフィックス（株）田中啓介氏，明星大学渡邊晶氏，東京電機大学立川敬行氏，（株）ATR知能映像通信研究所江谷為之氏，日立ソフトウェアエンジニアリング（株）鮫島吉喜氏，熊谷仁志氏，情報処理振興事業協会古宮誠一氏ならびに関係者の皆様に深く感謝いたします．

参考文献

1) Cheswick, W.R. and Bellovin, S.M.: *Firewalls and Internet Security*, p.306, Addison-Wesley (1994).
2) Ranum, M.J.: Thinking about firewalls, *Proc.*

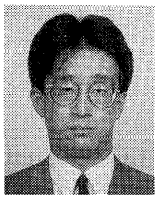
Second World Conference on Systems and Network Security and Management (Apr. 1993).
3) Information technology – Open systems interconnection – The directory: Authentication framework, ITU-T X.509 (Nov. 1993).
4) http://www.cup.hp.com/netperf/NetperfPage.html
5) Department of Defense Trusted Network Interpretation.

(平成 9 年 5 月 12 日受付)
(平成 10 年 1 月 16 日採録)



寺田 真敏（正会員）

昭和 61 年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．平成 6 年 10 月より平成 9 年 11 月まで情報処理振興事業協会技術センター非常勤研究員．現在，(株) 日立製作所システム開発研究所にて，インターネット，ネットワークセキュリティの研究に従事．



芳原 誠士

昭和 62 年広島工業大学工学部電機工学科卒業．同年日本電気市場開発（株）「現日本電気インフォメーションテクノロジー（株)」に入社．平成 6 年 10 月より平成 9 年 11 月まで情報処理振興事業協会技術センター研究員．

村山 優子（正会員）

津田塾大学学芸学部数学科卒業．三菱銀行および横河ヒューレット・パッカード社に勤務．昭和 59 年 University College London 大学院理学部計算機科学科修士課程修了．平成 2 年同大学大学院博士課程修了．Ph.D.（ロンドン大学）．慶應義塾大学環境情報学部非常勤講師を経て，平成 6 年 4 月広島市立大学情報科学部情報工学科講師，現在に至る．インターネット，ネットワークセキュリティの研究に従事．著書「ネットワーク概論」(サイエンス社)．IEEE，ACM，電子情報通信学会，映像情報メディア学会，日本 OR 学会，情報知識学会各会員．