マルチメディア通信と分散処理 77－3
（1996．7．12）

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

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

組織間網環境におけるアクセス制御機構で解決したい課題の１つに、『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』の提供がある。この課題を解決するために、“ユーザアクセスドメイン”、”アクセスドメイン制御層”を導入する方式を提案した。本稿は、その提案に基づき、セキュリティ防御壁としてのファイアウォールの多段接続を対象としたユーザ認証機能の概要を報告する。

User Authentication of Multi-hop Firewalls

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

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 user authentication on multi-hop firewalls.

*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

1. はじめに

本研究では、インターネットを組織毎にホスト、ルータシステムが集合し、さらにネットワークを構成する組織間網の形態として捉え、アクセス制御機構の検討を進めてきた。

報告者らが組織間網の形態におけるアクセス制御機構で解決したい課題の1つに、『ファイアウォールの導入による組織としての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が見えないようにするための透過なネットワーク(論理ネットワーク)環境』、すなわち、『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』の提供がある(図1)。この課題を解決するために、ネットワークにおける組織・個人の活動範囲を定義する概念“ユーザアクセスドメイン(図2)“を導入し、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(図3)”を導入する方式を提案した[6][7]。

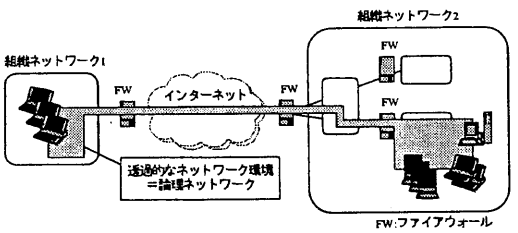

図1　透過的なネットワーク環境

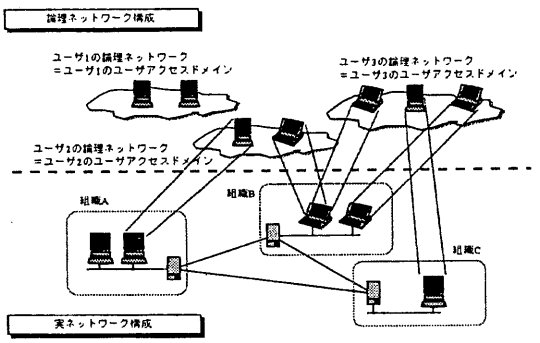

図2　ユーザアクセスドメイン

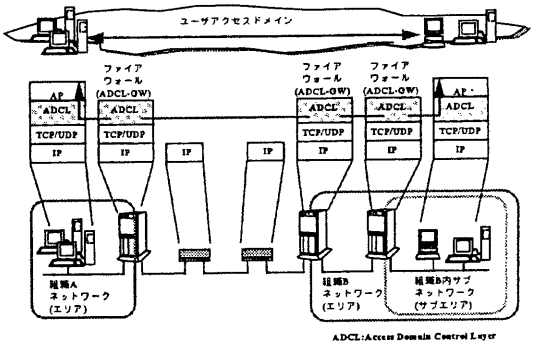

図3　ユーザアクセスドメイン制御層

本稿ではその提案に基づき、組織としての強固なセキュリティの壁を保持する「ユーザ認証機能」の概要と共に、セキュリティ防御壁としてのファイアウォールを多段接続した場合のユーザ認証方式について考察する。

2. 多段接続におけるユーザ認証方式

(1)認証の対象

セキュリティ防御壁として動作するファイアウォールを多段に渡り利用する場合の認証の対象は、以下の3つが考えられる。

(a)隣接間認証

隣接する装置間の相互相手認証を行う(図4)。

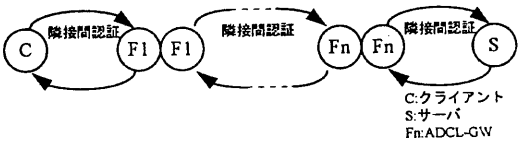

図4　隣接間認証

(b)エリアに対するユーザ認証

該当するエリアを利用するにあたり、そのユーザがアクセス制御の対象として妥当であるか否かを判断するための相手認証を行う(図5)。

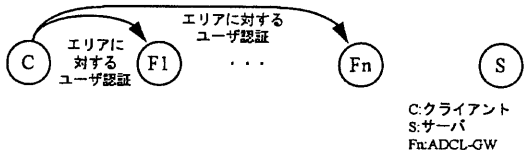

図5　エリアに対するユーザ認証

(c)エンドシステムに対するユーザ認証

該当するサーバを利用するにあたり、そのユーザとサーバ間で相互相手認証を行う(図6)。

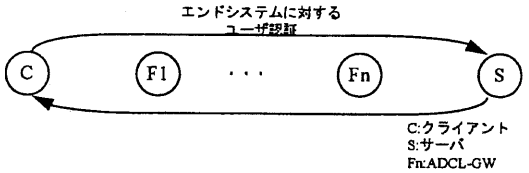

図6　エンドシステムに対するユーザ認証

(2)認証の方式

セキュリティ防御壁として動作するファイアウォールを多段に渡り利用する場合のユーザ認証方式は、以下の2方式に大別することができると考える。

(a)認証委託型

認証委託型とは、送信元から送付されたユーザ認証情報を、中継経路上に存在するファイアウォールADCL-GWで共用する形態である(図7)。この方式の利点は、より少ないメッセージ交換で認証操作を実施できると共に、クライアントは中継経路上のファイアウォール毎のユーザ認証を意識した認証操作が不要となる。欠点は、認証情報が共通であるため、ファイアウォールに不正介在が発生した場合、認証そのものが無力化される可能性が高いことである。

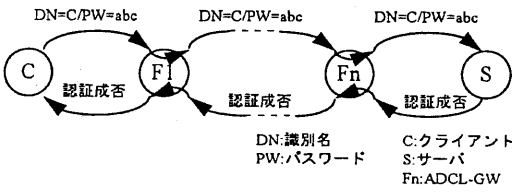

図7　認証委託型による簡易認証手順

(b)個別認証型

個別認証型とは、送信元と各ファイアウォールとして動作するADCL-GW間で個別にユーザ認証を実施する形態である(図8)。この方式は、仮想端末アクセスtelnetを実施する際、異なるパスワードでアクセスをくり返し、目的とする端末にアクセスする形態と類似している。この方式の利点は、認証委託型に比べファイアウォールに不正介在が発生した場合に安全保護性が高いが、認証を実施するためのメッセージ交換が多く、クライアントは中継経路上のファイアウォール毎のユーザ認証を意識した認証操作が必要となる。

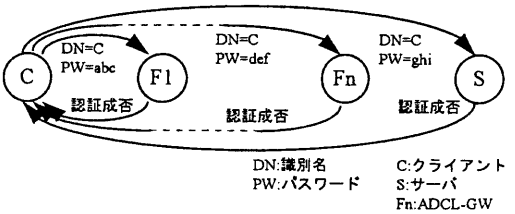

図8　個別認証型による簡易認証手順

3. アクセスドメイン制御層におけるユーザ認証機能

アクセスドメイン制御層(ADCL : Access Domain Control Layer)は、ファイアウォールによる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。アクセスドメイン制御層が提供するユーザ認証機能は、本論理ネットワークを利用するにあたり、そのユーザがアクセス制御の対象として妥当であるか否かを判断するための機能である。

(1)認証委託型の簡易認証方式

セキュアなネットワークであり、かつファイアウォールとして動作するADCL-GWが信頼できる環境で運用されている場合、例えば、同一組織内での利用においては、認証委託型の簡易認証方式が利用可能である。簡易認証は、利用者の識別名、相互に同意されたパスワードを用

いて実現する(図 7,図 9)。

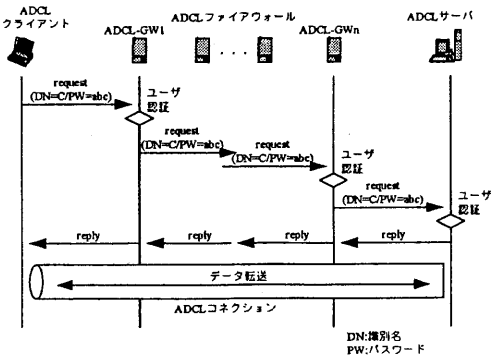

図 9　簡易認証を用いたコネクションの確立

(2)認証委託型の厳密認証方式

組織間にまたがる通信形態の場合や、クライアントがアンセキュアなネットワークに接続している場合には、隣接間の装置の相互相手認証、エリア・エンドシステムに対するユーザ認証により、ネットワーク資源ならびにユーザの安全保護施策が必要である。これは、X.509[9]に示された 2 方向性認証による厳密認証を用いることにより、メッセージ交換を低減した認証委託型の方式て実現することができる(図 10,図 11)。ここで、X{Info}は、利用者 X による署名で、情報 Info に暗号化された要約(一方向性ハッシュ関数によって作成され、暗号化は署名者の秘密鍵を使って行う)が付与されたものである。

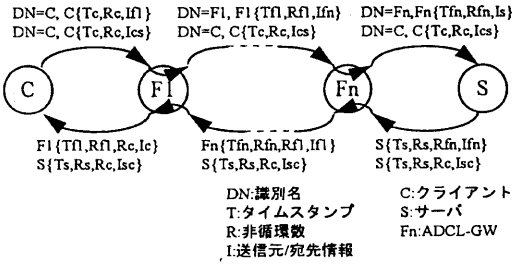

図 10　厳密認証手順概要

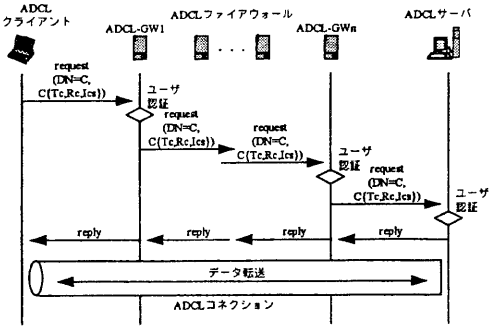

図 11　厳密認証を用いたコネクションの確立

4. 結論および今後の課題

本稿では組織間網環境におけるアクセス制御機構のうち、ユーザ認証機構ついてその概要を報告した。現在、認証委託型の簡易認証方式による ADCL のプロトタイプの実装を完了した。今後、暗号通信機能を持つ認証委託型厳密認証方式による ADCL のプロトタイプの機能設計と実装を行っていく予定である。

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 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、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)
[6]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)
[http://www.ipa.go.jp/STC/ACCESS/index.htm]
[7]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)
[http://www.ipa.go.jp/STC/ACCESS/index.htm]
[8]Poger M. Needham, Micheal D. Schroeder：" Using Encrytion for Autthentication in Large Networks of Computers", Communications of the ACM, Vol.21, Number12 (1978.12)
[9]X.509 ディレクトリ - 認証の枠組み (1988)
[10]SOCKS Protocol Version 5(RFC1928), ftp://ds.internic.net/rfc/rfc1928.txt