監視型認証を用いたネットワーク利用制限装置について

新村　正明*，山下　剛**，國宗　永佳*，不破　泰**

Network Access Control System with Authentication Monitoring

Masaaki Niimura*, Go Yamashita**, Hisayoshi Kunimune*, Yasushi Fuwa**

概要　ネットワークの不正利用を防止するため，いままでネットワークの利用制限を想定せずに運営されてきた大学の教室や公共施設においても，利用制限をかける必要が生じている．本研究では，このようなネットワーク環境においても容易にネットワークの利用制限がかけられるよう，既存のネットワーク環境に影響を与えず，外部認証システムとの連携が不要なネットワーク利用制限装置の開発を行った．特に，外部認証システムを必要としない機能の実現のために，既存の認証システムとの通信を監視することで利用者認証を行う監視型認証方式を提案し，これを実装した利用制限装置による実証試験を行い機能の評価を行った．

1. はじめに

大学の教室や公共の場でネットワークサービスを提供している場合，ある閉じたネットワーク内の利用は無制限に許可をするが，その他のネットワーク領域への接続は大学の教職員や学生，公共の場で許可を受けた人だけに利用を制限する事が必要である．従来利用制限を特に行ってこなかった古いネットワーク設備の教室や公共施設においても，最近の様々なネットワークに関連した問題から，この利用制限をかける必要が緊急に発生してきている．

ここで，ネットワーク利用者を制限する装置を利用制限装置と呼ぶことにする．一般的に利用制限装置はあるネットワークセグメントから他のセグメントへのアクセスを利用者によって制限する装置である．

教室や公共施設，小規模な事業所等でこれまで用いているネットワークに，容易に無理なく利用制限をかけるために利用制限装置に求められる機能として，導入の容易さと管理の容易さがあげられる．

導入の容易さとしては，必要な機材として利用制限装置以外に特別な機器・サービスを要求しないことがあげられる．また，装置の導入によりネットワークアドレスやセグメント等の変更が必要になると，ルータやL3 スイッチ，DHCP 等のネットワークサービスサーバなどネットワーク側の設定にまで影響が及ぶことから，ネットワーク的な設定変更が発生しないことが望ましい．

管理の容易さとしては，利用制限装置の運用管理における主たる要素はユーザ管理であることから，この管理業務を極力減らすことが望ましい．このためには，利用制限装置自身がユーザ管理を行うことによる管理コストは増加をなくすため，既存の別システムにおけるユーザ情報を利用することが望ましい．

本論文は，旧来のネットワークに容易に設置が可能で，以後の管理も容易な利用制限装置についての提案を行い，本装置を試作して実際に大学の環境で利用評価を行うものである．

2. 目的

本研究は，ある閉じたネットワークセグメントからインターネットを含む外部のネットワークへの接続を制限するネットワーク利用制限装置について，いままで利用制限を想定せずに運営されてきたネットワーク環境においても容易に設置が可能なネットワーク利用制限装置の開発を目的とする．

ネットワークの利用制限を行う利用制限装置に必要とされる機能として，

(a) ネットワークの利用制限を行う機能

(b) 利用者の認証を行う機能

の 2 つがある．また，(b)に関しては

(b-1) 利用者を識別するための情報入力

(b-2) 利用者の正当性を確認する認証機能

* 信州大学工学部
Faculty of Engineering, Shinshu University
** 信州大学大学院工学系研究科
Graduate School of Science and Technology, Shinshu University

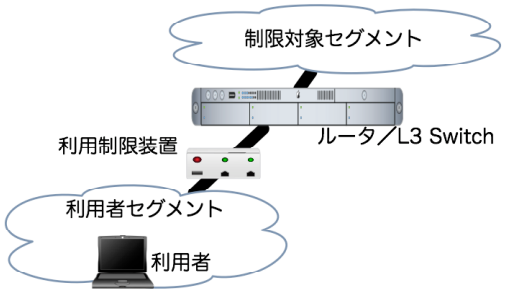

図１　利用制限装置の設置位置

の２つの機能を実現する必要がある．

そこで本研究では，これらの要求項目を上記の目的の範囲内で満足させるために，以下の機能を有するネットワーク利用制限装置の開発を行う．

1) 既存ネットワーク環境に影響を与えない導入
2) 外部認証システムとの連携が不要

以下に，各々の目的について述べる．

2.1 既存ネットワーク環境に影響を与えない導入

(a) のネットワークの利用制限を行うには，通信の許可・遮断の制御を行う必要がある．このため，利用者が存在するネットワークセグメント(以後，利用者セグメントと呼ぶ)と，その外部のネットワークセグメント(以後，制御対象セグメントと呼ぶ)との間に利用制限装置を設置しなければならない．(図 1)

しかし両セグメント間には通常，既設のルータまたはL3 スイッチが存在し，利用者セグメントの管理を行っている．このため，利用者セグメントの出口部分に機器を設置した場合，その機器がルータとして設定されてしまうと，利用者セグメントのサブネットの変更か既存のルータ/L3 スイッチと制御機器間のサブネットの変更のいずれかが必要となる．さらに，この設定変更に対応するために既設のサーバ類(DHCP サーバ等)の設定変更も必要となる場合もある．

そこで，既存のネットワーク環境を変更せずに利用制限装置が導入可能な機能を実現する必要がある．

2.2 外部認証システムとの連携が不要

(b)の利用者の認証を行うには，この認証に必要な情報を利用制限装置が持つか否かにより以下の２つの場合に分けられる．

・装置が利用者情報を保持する場合

利用制限装置がユーザ情報を保持し認証を行う機能を有する場合には，利用制限装置におけるユーザ管理業務(ユーザの追加･削除やパスワード発行)が必要になるため，そのための要員配置等が必要となる．また利用者側にとっても，ネットワーク利用のためのユーザ ID・パスワードといった管理すべき情報の増加という負担を強いることになる．

・外部の認証機能を利用する場合

前節で述べた理由から，利用者の管理を一元化する上でも，利用制限装置自身は認証に必要な情報を持たず，外部の認証機能を利用することが望ましい．このため現在使用されているシステムでは，RADIUS，NIS，Kerberos や LDAP 等の認証システムを利用する方法 [1)-4)]や，利用制限を目的とした専用システムにログインすることにより利用者の認証を行う方式 [5)]等が用いられている．しかしながら，この方式では認証専用システムが必須となる上，その認証システムに認証を委託するための設定が必要となる．特に小規模なサイトでは，電子メールの管理を行う POP サーバや Web サーバ等の基本的なサービスのみが提供されるだけで，前述のような認証専用のシステム自体が存在する例は少なく，何からの専門的な作業が必要となることから簡便な設置は困難である．

そこで，外部の認証システムとの連携を必要としない認証システムを実現する．

3. 提案

本研究では，いままで利用制限を想定せずに運営されてきたネットワーク環境においても，図１に示されるようにネットワークセグメント間に挿入することで容易に設置が可能なネットワーク利用制限装置を実現するために，目的で掲げた機能を実現する以下の手法を提案する．

3.1 既存ネットワーク環境に影響を与えない導入

前節で述べた目的のうち，ネットワークの物理的・論理的構成を変更しない点については，利用制限装置をネットワークのブリッジとして構成することにより既存のネットワークの論理的構成を変更することなく導入が可能である．この方法は，

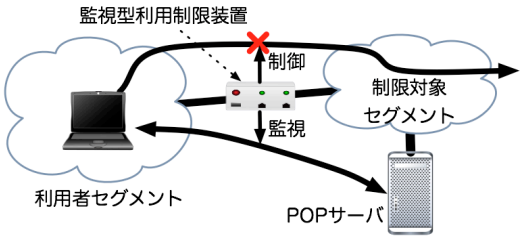

図２　POP プロトコルを監視する方式

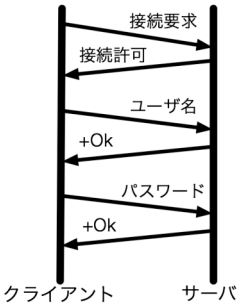

図 3 POP のシーケンス

従来からあるネットワーク利用制限装置においても実現されている方法の１つであり，実現上の問題はない [1)~5)]．特に現在ではネットワーク機器に利用者制限機能を付与した製品も販売されている [6)]．

3.2 外部認証システムとの連携が不要な認証方式

これに対し認証システムに関しては，従来の方式では外部の認証システムとの連携が必要である．これは，目的で述べた

(b-1) 利用者を識別するための情報入力

がネットワーク利用制限装置に対して行われることにより，利用制限装置が利用者を識別するための情報を取得・保持しているのに対して

(b-2) 利用者の正当性を確認する認証機能

を実現するために必要な情報が外部の認証システムに存在するため，利用制限装置が持つ情報と外部の認証システムが持つ情報を照合するための連携が必要となるからである．

しかし，ネットワークの利用制限を行うための認証以外にも，現行のネットワークシステムにおいて提供されるサービスで既に何らかの認証が運用されている場合が多い．たとえば，電子メールシステムにおけるユーザ認証等がその一例である．

そこで，ネットワーク利用制限装置自身が認証を行う方式に代えて，既存のネットワークサービスにおける認証を利用する方式を提案する．具体的には，現行のネットワークサービスで使用されているサーバ=クライアント間の通信を監視し，そこで使用されている認証から利用者が正規ユーザであることの識別を行う．これ以降，このような認証方式を用いた利用制限装置を監視型利用制限装置と呼ぶ．

電子メールシステムを例に説明を行う(図 2)．電子メールシステムでは，ユーザ側のメールクライアント(以後クライアントと略す)とメールを管理するサーバの間でメールの読み出しのために POP と呼ばれるプロトコルを利用している(図 3)．この POP では，メールを読み出す際にパスワードによる認証を行っている．

このプロトコルにおいて，メールを管理するサーバ(以後 POP サーバと略す)が正しいユーザであると認識した場合，サーバから「+Ok 」のレスポンスが送られる．これは，パスワードを暗号化して送信する APOP プロトコルでも同様である．従って，ユーザ認証要求に対して Ok レスポンスが送信されたクライアントは正規ユーザが使用しているものと見なすことができる．

そこで監視型利用制限装置は，まずこの POP サーバ=クライアント間の通信のみを許可し，それ以外の制限対象セグメントとの通信は拒否する．次に POP サーバ=クライアント間の通信を監視し，クライアントからのパスワード送信に対して Ok レスポンスがあった場合に，このクライアントは正規ユーザが利用しているものと判断して，使用ユーザを記憶すると共にネットワークを利用する権限を与える．

この方法は，サーバは制限対象セグメント側にあり，クライアント=サーバ間の通信は監視型利用制限装置が監視できることを前提としている．実際の構成例では，サーバはサーバ室等の制限対象となるセグメントに設置されていることから，このような構成をとることは十分に可能である．

以上は POP を用いた場合について説明したが，他のアプリケーションにおいても，クライアント=サーバ間の通信を監視することで使用ユーザと認証が成功したことが識別できれば，この監視型認

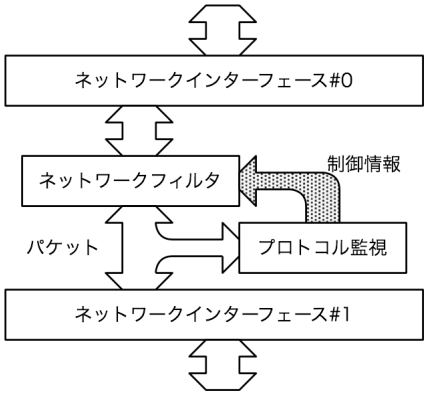

図４　監視型利用制限装置のブロック図

証方式の適用が可能である.

3.3 本認証方式に対する攻撃

本方式は，端末と既存のネットワークサービスシステムとの通信を監視することで認証を行うことから，攻撃方法としては,

・ネットワークサービスシステムへの攻撃
・本利用制限装置自身への攻撃
・端末のなりすまし

が想定される.

ネットワークサービスシステムへの攻撃に関しては，本認証方式による利用制限を使用する・しないにかかわらず，既にネットワークサービスのために運用が行われていることから，このネットワークサービスサーバへの攻撃に対する対処は別途行われるものとして，本研究の対象外とした.

利用制限装置自身に対する攻撃としては，本装置は IP アドレスを持たないブリッジモードとして動作することから，本装置に直接アクセスする攻撃は受けにくいと考えられる．そこで，本装置を通過するパケットの量を増やすDoS攻撃への対応を行った.DoS攻撃への対応については 5.2 節にて評価結果を述べる.

端末のなりすましに関しては，本方式では認証を受けた端末の識別をMACアドレスにより行っていることから，MAC アドレスの偽装によるなりすましが想定される．この対策については，定期的に再認証を強制することで，MAC アドレスの乗っ取りによるなりすましが行われていないことを確認することができる．定期的な再認証については4.3節の切断制御において詳しく述べる.

4. 実装

今回提案する方式の有効性を確認するために，この方式による利用者識別を行う監視型利用制限装置の試作を行った．監視型利用制限装置は図 4 に示すブロックにより構成される.

4.1 接続制御

目的の１つである「既存ネットワーク環境に影響を与えない導入」を実現するために，ネットワークインターフェース #0 #1 間はブリッジモードとして動作させる．この状態ではすべてのパケットが通過してしまうことから，ネットワークフィルタ部により，送信元の IP アドレス/MAC アドレスに基づき転送の可否を決定する.

初期状態では,端末が IP アドレスの取得等に必要となる基本的なサービスプロトコル，例えば ARP， DHCP， DNS を許可する．さらに，認証を含むサービスを受けるために必要な通信も初期状態で許可する.電子メールの例では特定の POP サーバへの POP プロトコルの通信を許可する.

本方式は，既存のネットワークサービスを監視することで認証を行うため，利用制限装置に対して認証のための情報を入力するためのインターフェースを持つ必要がない．このため，監視型利用制限装置自身に IP アドレスを割り当てる必要がなくブリッジモードのみの動作で十分である．これは，既存のネットワーク環境に影響を与えないという目的にも寄与する.

4.2 認証

監視部は，指定されたサービスにおけるクライアント=サーバ間の通信の監視を行う.本方式では既存のサービスにおける認証を監視することから,そのサービスにおけるプロトコルを解釈する機能が求められる．今回の例ではPOPプロトコルについて，クライアント毎にプロトコルの進行状況の監視を行う.

この監視部において，既存のサービスにおける認証が成功したことが確認できた段階で，その端末が有する IP アドレス/MAC アドレスをネットワークフィルタ部に登録し，以後，その端末からの全ての通信を制限対象セグメントに転送する．これにより認証が成功した端末はネットワークの利

用が可能となる.

今回は既存の認証プロトコルとしてPOP認証とHTTP認証(Digest 認証)の2つについて実装を行った

4.2.1 POP・APOP認証

POP 認証については，提案で述べたように，サーバ=クライアント間の通信の監視により使用中のユーザの識別と正規ユーザであることの判別が可能である．しかし，POP サーバにはテスト用アカウントや代表アカウントなど正規ユーザ以外のアカウントも登録されている．そこで簡単なパターンマッチ機能による学生用アカウントの識別や，root，admin 等のよくある代表アカウントの排除等の機能を追加した.

これにより，POP 認証の監視を行う場合には，

・監視対象となるPOPサーバのIPアドレス

・POPサーバで除外するアカウントリスト

等の設定を行う.

また,APOP についてはパスワードの部分が暗号化して送信されるだけであることから，POP の場合とほぼ同様な処理で実装が可能となった.

4.2.2 HTTP認証(Digest認証)

HTTP のプロトコルに規定されている HTTP 認証(Digest 認証)(RFC2617)の監視によるユーザ識別機能を実装した.このプロトコルに関しては,APOPと同じく，パスワードの送信は暗号化されているがユーザ情報と認証結果については平文での確認が可能であるため，POP の場合と同じ方法で使用ユーザの識別と正規ユーザであることの判別が可能である．また設定項目もPOPサーバと同様の設定を可能とした.

4.3 切断制御

本方式は，既存のネットワークサービスにおける認証を監視することでネットワーク利用の可否を決定している．このため，ユーザがネットワークを使わなくなった場合についても同様な方法で検出し，そのクライアントからの通信を拒否する必要がある.

ユーザがネットワークの利用を止めたことを検出する方法については，認証に使用した既存のネットワークサービスにおいてログアウトに相当する機能があれば，そのログアウト操作を検出し，ネットワークの利用を停止させる可能である．しかし,今回の例にあるようなPOPプロトコルでは,メールの読み出し操作を終了する意味でのログアウト操作はあるものの，定期的にメールの受信確認が行われ，その都度ログイン・ログアウト操作が行われることからネットワークの利用を終了することの検出はできない.

そこで，ログアウト操作の確認ができないプロトコルに関しては，最初の認証から一定の期間だけネットワークの利用を許可することとし，それ以降は再度認証を求めることとした.

この一定時間後の再認証については既存のシステムでも使用されている方法であり，Javascript や HTML ファイルの自動再読込機能を利用してユーザがユーザ名・パスワードを再入力する手間を省き利便性の向上を図っている例もある[3]．またPOP による認証は，メールクライアントが定期的にメールの有無を確認することで，メールクライアントを使用している間は自動的に再認証が行われる.

4.4 端末の識別

今回の実装では，MAC アドレスにより端末の識別を行うこととした．これは，前節で述べた一定期間ネットワークの利用を許可する方式を採用したため，IPアドレスにより端末の識別を行った場合，DHCP による IP アドレスの再利用で権限のない端末にネットワークの利用を許可することを防ぐためである．さらに，DHCP による IP アドレスの再利用が行われたことを検知するために，IPアドレスとMACアドレスの組み合わせを追跡する機能を実装した.この実装に関してはDHCPのシーケンスを監視することで IP/MAC の組み合わせを追跡するシステムが提案されているが[2]，本方式ではDHCPが使用されない場合も考慮しARPパケットの監視により実現した.

4.5 ハードウェア構成

監視型利用制限装置は，ネットワークインターフェースを2つ以上有するサーバにより構成される.実装に使用したサーバ機の諸元を表1に示す.

表1　サーバの諸元

CPU	Celeron 2.6GHz
メモリ	512Mbyte
OS	FreeBSD 5.4

実際のネットワーク環境では，ネットワーク機器の管理のために，通常の通信用ネットワークとネットワーク機器管理用のネットワークを VLAN により分離する場合がある．そこで利用制限装置自身も VLAN に対応させ，通常の通信用ネットワークに対して通信制御が行われるようにした．このため，基本 OS として FreeBSD を使用し，ネットワークフィルタとして IPFW を利用した．

5. 評価

5.1 ブロック間連携試験

本システムは，図 4 に示すように，全体の機能を通信の制御を行うネットワークフィルタ部と通信の監視を行う通信監視部に分離して構成している．これは本システムによるパケットロスの発生を極力防ぐため，ネットワークフィルタ部にパケット転送能力等で実績のある既存のシステムを使用したためである．そこで通信監視部からの制御により，外部セグメントとの通信制御が正しく行われることを検証するため，80 人程度を収容する講義室に導入し通信制御の試験運用を行った．

試験運用期間は 10 ヶ月で，のべ人数で約 2200 ユーザに対して実施し，接続制御が正しく行われることを確認した．

5.2 負荷試験

通信監視部に対する負荷試験を行うため，監視型利用制限装置に対して，DoS 攻撃に相当する大量のパケット送信と，認証プロトコルに基づく大量の認証セッションの送信を行う実験を実施した．

図５　DoS 攻撃時の CPU/ネットワーク負荷

DoS 攻撃パケットに関してはネットワークが飽和する程度までパケット送信を行ったがパケットロスは見られなかった．図 5 に MTRG による観測結果を示す．

これは，CPU の性能に依存はするものの，パケットフィルタの機能によりパケットロスが極力抑えられているためである．さらに通信監視部においては，パケットの宛先ポートやペイロード部の先頭文字列等，いくつかの条件で監視対象のパケットであるかの判断を行っていることから，実際のプロトコル解析を行う以前に不要なパケットの判別がつくため，処理量の増加が抑制される．

次に HTTP 認証（Digest 認証）を使用した大量の認証セッションを発行する実験を行ったが，これに関しても監視型利用制限装置でのパケットロスは発生しなかった

原因としては，HTTP サーバ側における Digest 認証処理に要する処理が，本システムの通信監視部の処理よりも大きいことから，本システムにかかる負荷が相対的に低くなるためと考えられる．これは POP サーバにおいても同様であることから，サーバの性能と監視型利用制限装置の性能がアンバランスでない限り，パケットロスが発生することはないと考えられる．

5.3 実証試験

本システムの目的である認証システムを有しない小規模サイトへの簡便な導入と，一般ユーザからの操作性に関する意見を聴取するために，実証試験を行った．

対象として，東和大学に協力をいただき，同校の e-Learning システムが存在するネットワークセグメントの利用権限を制御するシステムとして導入を行った．

1）既存ネットワーク環境に影響を与えない導入

利用制限装置の設置に関しては， e-Learning システムが設置されているサーバ室内において，e-Learning システムのネットワークセグメントにおける最上位の Hub と上位セグメントの Hub の間に設置した．設置は，LAN ケーブルの配線替えだけで完了し，当初の目的通り既存のネットワーク環境を変更することなく設置が完了した．

2）外部認証システムとの連携が不要

認証に関しては，当初は POP の監視による認証を行っていたが，ユーザが必ずしもメールを読む

とは限らないことと,Web ページによる ID/パスワード入力による明示的なログイン操作の方がユーザに対して分かりやすいことから，POP の監視と HTTP 認証の監視を併用することとした．認証システムについては，POP 認証は従来からある POP サーバを使用し，HTTP 認証は e-Learning システムのログインの監視により実現した．

また，実証試験中に監視型利用制限装置のアップデートが発生したが，担当者による操作が可能な範囲内での作業で完了することができた．

6. まとめと今後の課題

ネットワークの利用制限に必要な利用者の認証を既存のネットワークサービスの監視により行う方法の提案と，それを実装した利用制限装置の試作を行った．またその装置の有効性を確認するために実証試験を行った．

実証試験により，本装置が初期の目的を達成していることが確認できた．さらに，利用制限装置がネットワーク的に存在しない構成を取ることが可能となったため，利用制限装置自身に対する攻撃を抑制することが可能となる利点も得られた．

本手法の問題点として，認証に用いる既存のネットワークサービスサーバに対する攻撃への対応がある．本論文では，本方式は既存のネットワークサービスを利用しているだけであることから，このサービスサーバへの攻撃は対象外とした．しかし，いままでは攻撃対象とならなかったサーバが本方式の認証に使用されることで攻撃対象となることも想定されることから，本利用制限装置による保護を検討する必要がある．現在，監視型利用制限装置の利用制限部と監視部を分離し，監視部のみサービスサーバの直前に配置して，サーバの保護を行う方式を検討している．

さらに,サーバ=クライアント間の通信が暗号化通信で行われている場合には監視が困難であるという問題がある．具体的な例としては SSL/TLS による通信路の暗号化である.今回提案した手法は,サーバ=クライアント間で行われる通信内容を監視し認証に成功したかの判断を行っている．このため通信路が暗号化されると，通信内容の監視ができなくなり，認証過程の追跡が困難となる．

この問題に関しては，例えば POP 認証において認証に失敗した場合サーバからセッションの切断が行われる等，TCP セッションの振る舞いなどにより認証が成功したことを検知する方式を検討している．暗号化通信路であっても，通信路を流れるパケットは，通信路を使用するプロトコルに従った動きを行うことから，プロトコルの推移を推測することは可能である．しかし，そのプロトコルを使用するサーバ・クライアントのソフトウェアの種類によりその振る舞いも変化することと，正常な場合のパケット交換と同等なパケットの送出による偽装にも対応しなければならないことから，この手法の有効性に関する検証を進めていく予定である．

参考文献

1) 石橋勇人，坂本晃，山井成良，安倍広多，松浦敏雄 ： 利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式，情報処理学会論文誌，Vol. 42，No. 1,pp.79-88，(2001)．

2) 丸山伸，浅野善男，辻斉，藤井康雄，中村順一 ： 既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築，情報処理研究会報告，99-DSM-14，pp.131-136，(1999)．

3) 渡辺義明，渡辺健次，江藤博文，只木進一 ： 利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発，情報処理学会論文誌，Vol.42，No.12，pp.2802-2809，(2001)．

4) 田島浩一，西村浩二，相原玲二 ：VLAN 選択機能を持つ情報コンセントシステム，情報処理学会研究報告，2001-DSM-22，Vol. 2001，No. 80，pp.25-30，(2001)．

5) 後藤英昭，満保雅浩，静谷啓樹 ： 廉価なスイッチと Secure Shell を利用した安全な情報コンセントの構成方法，電子情報通信学会論文誌，J84-D-I，No.10，pp.1502-1505 (2001)．

6) 日立電線 ：Apresia，http://www.apresia.jp/