ケーブル認証による
アクセス制御システムの提案

神谷　謙吾†　　井上　亮文†　　市村　哲†　　松下　温†

東京工科大学†

1．　はじめに

情報の取得や交換にインターネットが必要不可欠な現在，企業や大学では会議室や教室の机などいたるところに情報コンセントが設置され，LAN やインターネットにどこからでもアクセスが可能になった．しかし，その反面，関係の無い第三者に LAN 内部のリソースに不正にアクセスされる可能性があるため，ユーザやアクセス管理が重要になる．本稿では，LAN ケーブルそのものを固有化して，情報コンセントで認証を行うことでケーブルを挿すだけでユーザ認証ができるシステムを提案する．

2．　現状の問題点

現在，オフィスや大学キャンパスでは部外者の出入りが非常に多く，ゲストのような一時的なユーザにもネットワークへのアクセス環境を提供する必要がある．この際，内部ネットワークへのアクセスを禁止するだけでなく，ゲストに対して，共有プリンタなどの一部の通信を許可しなければならない．このような場所でのアクセス制御方法として MAC アドレスフィルタリングやパスワード認証が行われている．

MAC アドレスフィルタリングでは，NIC（Network Interface Card）に付けられた固有の４８ビットの物理アドレスの MAC アドレスを利用し，登録されている MAC アドレス以外接続できないようにする．しかし，持ち込まれるゲストの PC すべての MAC アドレスを申請してもらい，登録しなくてはならない．さらに本来固有の MAC アドレスは，偽装することが可能であるという問題がある．

パスワード認証では，通信開始時に認証サーバなどにアクセスして，ID とパスワードを入力することによってアクセス制御を行う．そのため，ゲストに認証ソフトや認証サーバの使用方法などを伝えなければならない．

3．　提案システム

提案システムでは，　一時的なユーザへ MAC アドレスの登録やパスワード認証の変わりに，固有の ID を持ったケーブルを貸し出す．そして，情報コンセントでケーブルの ID を認証することで，アクセス可能なリソースを制御する．

例として図 1 では，ケーブル A を使っているゲスト A は，WWW やメールといったインターネットのほかに，ローカルのプリンタなど LAN 内のリソースを利用できる．一方ケーブル B を使っているゲスト B は，インターネットへのアクセスのみに限定される．ID を持たない外部から持ち込んだケーブルは，いずれのリソースも利用することができない．

各ケーブルには利用期限や利用場所などさまざまな条件をつけることができ，指定された部屋だけでの利用や，一定時間が経過したものは無効化することも可能である．

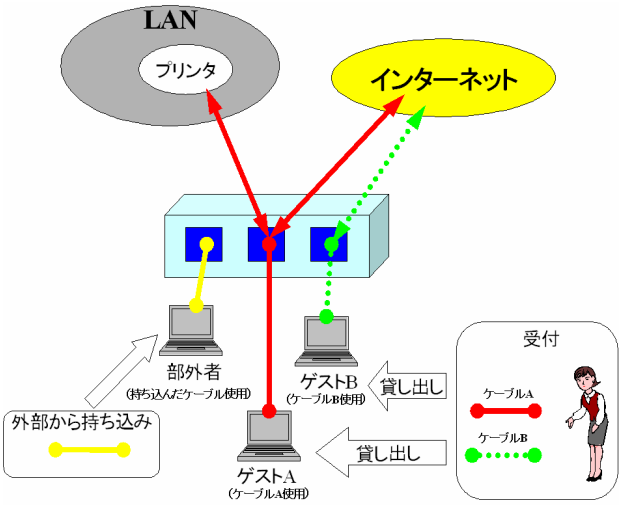

図１　提案システム利用例

User Authentication System with Cable ID
† Kengo Kamiya ,　Akifumi Inoue ,　Satoshi Ichimura ,　Yutaka Matsushita
Tokyo University of Technology

４．　実装

LAN ケーブルには図２のようにコネクタ付近に RFID タグを埋め込むことでケーブルに固有の ID を与える．一方，ケーブルを差し込む LAN コネクタ側にも，図３のようにコネクタの接続部分付近に RFID リーダライタのアンテナが取り付けられている．

RFID タグは，ケーブルを挿した場合のみ読み込めるようにするため，通信距離が理論値で最大 2.4㎜ と短いチップを利用した．このチップは，直径 5㎜，厚さ 1㎜（５円玉の穴に収まるサイズ）であり，容易にケーブルに埋め込むことが可能である．一方，RFID リーダライタは，アンテナが最大で８本まで接続可能である。

アクセス制御を行うために用いるスイッチングハブには外部からシリアルおよび Telnet 通信でコマンドを送ることによって各種機能を制御できる BUFFALO 社製品を使用した．RFID リーダライタは，このスイッチングハブに組み込むことを想定している．

ケーブルによってさまざまなネットワーク接続環境を提供するため，いくつかの情報をタグの ID と関連付けてデータベースに登録している．その例として，利用開始時間，利用終了時間，利用可能場所などがある．

図２ IC タグケーブル

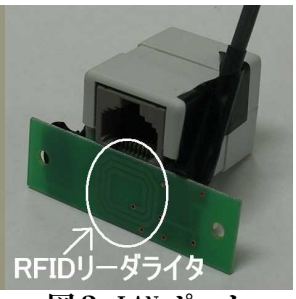

図３ LAN ポート

５．　システムの流れ

システムの流れを図４に示す．なお，初期設定ですべてのポートを通信不可能な状態に設定している．

システムの流れ

① ユーザがケーブルを情報コンセントに挿しこむことで RFID タグの情報が受信可能になる．
② RFID タグの情報をリーダで読み込む．
③ 取得したタグの情報が管理 PC に送信される．
④ 管理 PC は取得したタグの情報からデータベースを参照して利用可能な期間，場所，所属している VLAN グループの情報で接続の可否とネットワークアクセスの利用者に適した設定を判断する．
⑤ 管理 PC はスイッチングハブにコマンドを送り，接続の可否と利用者に合った設定を行う．
⑥ スイッチングハブの設定が反映され，利用者に合ったネットワーク接続環境が提供される．

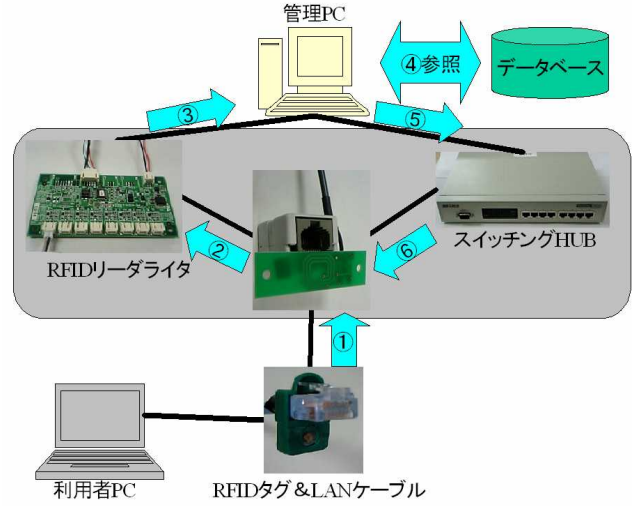

図４　システムの流れ

６．　まとめ

従来のアクセス制御をケーブル認証によってケーブルを挿すだけで簡単に行えるようになった．さらに利用可能な時間帯や場所，アクセス先も制限することができるため，ゲストへのネットワークアクセス環境の提供に適したシステムになった．

今後の課題としては，RFID タグの書き込み領域を利用して電子署名を入れるなど更なるセキュリティの強化やユーザ認証以外への応用が挙げられる．

本稿ではスイッチと PC との接続を念頭においたが，スイッチ同士をこのケーブルで接続することにより，VLAN におけるトランク設定など複雑なネットワーク管理が容易になると考えられる．

謝辞

本研究は日立マクセル(株)の協力による．ここに記して謝意を表す．

参考文献

[1]　日経 BP 社：“無線 IC タグのすべて”：日経 BP 社／日経 BP 出版センター
[2]　RFID について：”RFID テクノロジ”：http://itpro.nikkeibp.co.jp/rfid/
[3]　宮越健，角田浩二：“最新ＬＡＮハンドブック”：株式会社秀和システム
[4]　Gene：“最新ルーティング＆スイッチング”：株式会社秀和システム