RFIDによるアクセス制御機構を持つネットワークスイッチ

井上 亮文　神谷 謙吾　中村 亮太　市村 哲　松下 温
東京工科大学 コンピュータサイエンス学部

Network Cable Authentication System with RFID tags

Akifumi Inoue, Kengo Kamiya, Ryota Nakamura, Satoshi Ichimura
and Yutaka Matsushita
Faculty of Computer Science, Tokyo University of Technology

1　はじめに

企業やキャンパスではイントラネットが急速に普及し，会議室や教室の机などあらゆる場所に情報コンセントが存在するようになっている．一方で，このような遍在化したアクセス環境は，来客や部外者も容易に接続が可能なため，ユーザやアクセス管理が重要となる．実際，近年はこのような外部から持ち込まれるコンピュータによるセキュリティが深刻となっている [1]．本稿では，ネットワークケーブルそのものを情報コンセントで認証することで，これらの手間を軽減する手法について述べる．

2　ケーブル認証機構

2.1　ケーブル及びスイッチの構造

図 1 に，提案手法におけるケーブルとスイッチの構造を示す．ケーブルを認証するために，従来ではコネクタ部分の保護用ラバーブーツがついていた部分に小型のタグを埋め込む．一方，情報コンセント側には，差し込んだ際に上記のタグが接触する位置にリーダーを設置する．情報コンセントを提供するスイッチでは，リーダからタ読み込んだタグの内容に応じて該当ポートにおける通信の可否などを制御する．

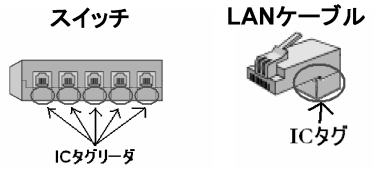

図 1: ケーブルとスイッチの構造

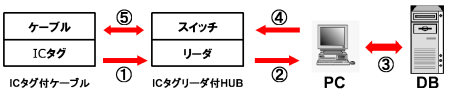

図 2: アクセス制御システムの流れ

2.2　システムの流れ

ケーブル認証機構をネットワークへのアクセス管理に利用した例を図 2 に示す．なお，最初はすべての空きポートが通信不可能な状態に設定されているとする．

1. ユーザがケーブルを情報コンセントに差し込むと，スイッチではその ID をリーダで読み取る．
2. 読み取った情報は，これを管理するコンピュータに送信される．
3. コンピュータではデータベースとタグの情報を照合し，ネットワークの利用可否を判断する．
4. 正当なケーブルと判定された場合，該当するポートの設定が変更される．
5. 通信が可能となる．ケーブルが引き抜かれた場合は，再びポートは通信不可能な状態に戻される．

3　実装

タグ付きケーブル及びリーダ付き情報コンセントのプロトタイプを図 3 に示す．RFID 及びリーダには，日立マクセル社製のものを利用している．このリーダ付きコンセントを，各ポートの通信設定などを制御可能なスイッチ（BUFFALO 社製）の各ポートに取り付けている．

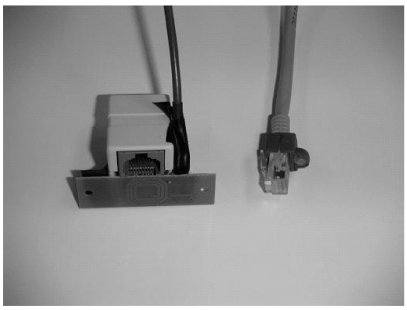

図 3: タグ付きケーブルとリーダー付きコンセント

4 考察

提案手法は単純なポートのアップ・ダウンによるアクセス制御だけでなく，様々なネットワーク管理に応用できると考えている．ここではその例を 2 つ挙げる．

4.1 VLAN 構成への適用

VLAN は同じスイッチ内でサブネットを分割することができるため，セキュリティ的観点や，組織に閉じた情報共有，ブロードキャストパケットの減少による帯域の有効利用といった観点から急速にオフィスでの普及が進んでいる．

通常 VLAN を構成する方法として，各ポートがどの VLAN に属するかを静的に割り振っておくポートベース VLAN，各ポートに接続されるコンピュータの MAC アドレスを用いて動的に構成する MAC ベース VLAN，IP アドレスを用いるサブネットベース VLAN などがある．

ポートベース VLAN では静的に VLAN を割り振ってしまうため，ポートに接続するコンピュータを変更する度に管理者が設定をやり直さなくてはいけない．MAC ベース VLAN では，接続するコンピュータの MAC アドレスをすべて調べておかなくてはいけない．また，ネットワークインタフェースを交換した場合も再設定が必要となる．

提案手法で VLAN を構成する場合，例えばケーブルの色ごとに共通の ID を持つようなタグを埋め込むことで，青色のケーブルを用いたコンピュータ同士はどのポートへ差し込んでも同一の VLAN に属する，といった使い方が可能である．ケーブルに埋め込むタグの ID 管理をしておけば，設定に詳しくないユーザにも直感的に高度なネットワーク設定が可能になる．また，どのコンピュータ同士が VLAN を組んでいるかがケーブルの色で一目瞭然である．

4.2 ゲストへのアクセス環境提供

現在，オフィスやキャンパスでは外部者の出入りが非常に多く，とくに情報系の学会が開催されると，ゲストからネットワークアクセス環境を要求する声が非常に大きい．

ユーザ認証をベースにネットワーク接続を管理するには，ゲスト用アカウントとパスワードを複数管理しておく必要がある．MAC アドレスをベースにするには，持ち込まれるコンピュータすべての MAC アドレスを申請してもらう必要がある．

提案手法では，ゲスト用 ID を持ったケーブルを管理しておき，受付時にこれを手渡す．各情報コンセントでは，ゲスト用ケーブルが差し込まれた場合，外部ネットワークや共有プリンタへの通信は許可した上で，内部ネットワーク・プリンタへのアクセスを禁止するような設定にしておけば，安全で手軽なゲスト環境の構築が可能である．

5 まとめ

本稿では，RFID を用いてケーブルそのものを認証する機構を提案し，より直感的にアクセス制御やネットワーク管理を実現できることを示した．今後の課題として，セキュリティ面の強化，プロトタイプの実装が挙げられる．

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] 佐川 昭宏, 高橋 ひとみ, 斉藤 匡人, 間 博人, 徳田 秀幸, “スイッチ間の連携による内部ネットワークセキュリティ向上機構”, 情報処理学会 第 11 回 DPS ワークショップ, Vol. 2003(19),pp.209–214, 2003.