7R-6

携帯電話を用いたネットワーク認証システム

太田　和宏　　福岡　久雄
松江工業高等専門学校

1.　はじめに

近年，セキュリティ意識の高まりから，数多くの組織がネットワーク認証システムを導入するようになった．その一方で，デジタル家電をはじめとした様々な機器がネットワークに接続されるようになった．

現在，多種多様なネットワーク認証システムが存在するが，それらの大半は認証プロセスを通信主体上で動作させるものである[1)]．しかし，増え続ける様々な機器それぞれに対して，各ネットワーク認証システムに対応した認証プロセスを搭載することは困難であると考える．

この問題に対して，ネットワーク認証において，認証プロセスと通信主体を分離するアプローチが必要と考える．例えば，ケーブル認証[2]は，このようなアプローチと理解することができる．

本稿では，同様の考え方に基づくネットワーク認証システムを，携帯電話をトークンとしても用いるシステムを提案する．

2.　関連技術

井上等によるケーブル認証システム[2)]は，ネットワークケーブルに割り当てられた固有の ID をネットワークポートで識別し，登録された ID からの接続のみを許可する．ネットワークケーブルのコネクタ付近には，ID を保持した RFID タグが埋め込まれている．RFID タグの情報を読み取るには RFID リーダが必要であり，全てのネットワークポートに RFID リーダを設置する必要がある．

3.　提案システム

3.1.　概要

本システムでは，携帯電話をトークンとする．携帯電話の多くは Web サイトへの接続時に，端末固有の識別番号（個体識別番号）を通知できる機能を有する．ユーザは，ネットワーク利用時に特定の Web サイトに接続し，携帯電話の個体識別番号及び利用するネットワークポートを通知する．携帯電話の個体識別番号を認証することで，当該ネットワークポートの利用可否を，所属 VLAN の変更によって制御する．

3.2.　認証処理の流れ

3.2.1. ユーザ登録

ネットワーク利用者は，受付で身分証明書を呈示する．システムは，登録処理毎に無作為に生成した識別符号（処理 ID）を生成する．受付担当者は，処理 ID 及び身分証明書の記載事項及び当該ユーザの利用可能なネットワークポート及び開始/終了日時及び所属できる VLAN をデータベースに登録した上で，使用方法及び登録に必要な URL（処理 ID を含む）をエンコードした QR コードイメージを呈示する．ユーザは，呈示された QR コードイメージを携帯電話でデコードする．携帯電話を用いて当該 URL ページに接続し，個体識別番号及び処理 ID を認証システムに通知する．認証システムは処理 ID をキーに個体識別番号をデータベースに登録する．

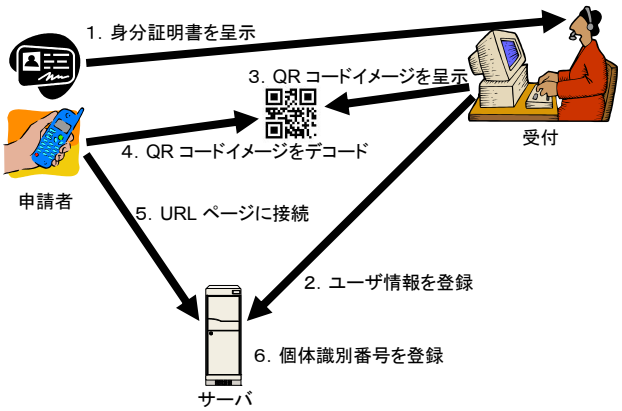

図 1　ユーザ登録

A Network Authentication System using Cellular Phone
Kazuhiro OTA, Hisao FUKUOKA
Matsue National College of Technology

3.2.2. 接続と利用

管理者は，ネットワークポート毎に識別符号（ポート ID）を定める．事前に使用方法及び利用に必要な URL（ポート ID を含む）をエンコードした QR コードイメージを，全てのネットワークポート付近に掲示しておく．

ユーザは，利用するネットワークポート付近に掲示された QR コードイメージを携帯電話でデコードする．携帯電話を用いて当該 URL ページに接続し，個体識別番号及びポート ID を認証システムに通知する．認証システムは，個体識別番号をキーにデータベースを参照し，ユーザが利用を開始するネットワークポート及び日時が許可された範囲内であるかを確認する．許可された範囲内であれば，当該ネットワークポートの状態を変更する為のインタフェースを出力する．ユーザが利用開始の操作（VLAN の選択）を行うと，当該ネットワークポートを通信可能な状態に設定する．

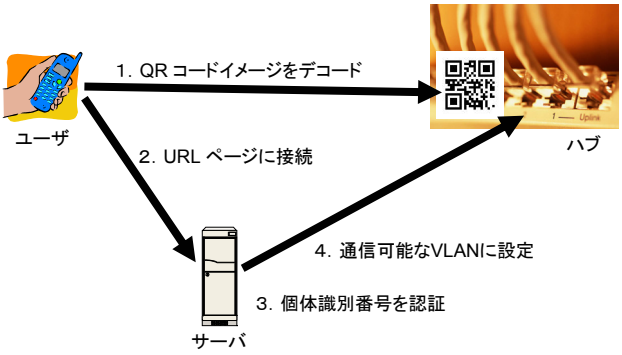

図 2　接続と利用

3.2.3. 利用の終了

ユーザは，利用を終えたいネットワークポート付近に掲示された QR コードイメージを携帯電話でデコードする．当該 URL ページに接続し，個体識別番号及びポート ID を認証システムに通知する．認証システムは，個体識別番号を確認した後，当該ネットワークポートの状態を変更する為のインタフェースを出力する．ユーザが利用終了の操作を行うと，当該ネットワークポートを通信不可能な状態に設定する．

また，日時が許可日時を超えた場合及び linkDown Trap を受信した場合にも当該ネットワークポートを通信不可能な状態に設定する．

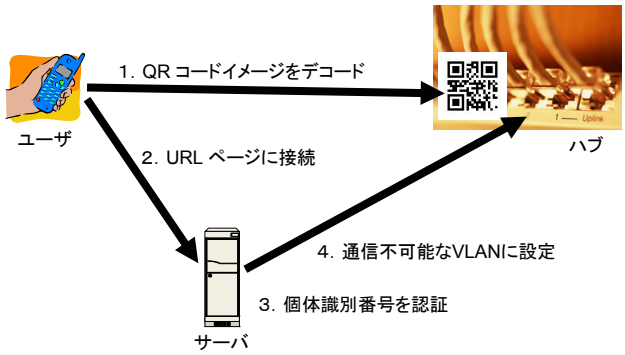

図 3　利用の終了

3.3. 有用性

ケーブル認証では，全てのネットワークポートに RFID リーダを配置する必要がある．本システムでは，RFID リーダの代わりに QR コードイメージが印刷されたシールを使用する．シールは RFID リーダに比べて非常に安価であり，全てのネットワークポートに配置することを考えると，その効果は大きいと考える．

また，ケーブル認証では専用のケーブルを用意しなければならないが，本システムでは通常のケーブルを用いることができる．

トークンとして，コモデティ化している携帯電話を用いることを考え合わせれば，特別に用意すべき物品は QR コードシールのみに限定される．

4.　おわりに

ネットワークに接続される機器は多種多様であることから，認証プロセスを通信主体から分離すべきであるとの考えに従って，携帯電話をトークンとして用いるネットワーク認証システムを提案した．

参考文献

1) Richard E. Smith 著，稲村雄訳：認証技術 パスワードから公開鍵まで，オーム社，東京 (2003)
2) 井上亮文，神谷謙吾，市村哲，松下温：ケーブル認証に基づくネットワーク管理方式，DICOMO 2005，pp. 449-452 (2005)