入退室管理システムに連動したPCのネットワーク接続認証

PC Network Authentication Linked to Entry Control System

大景　聡＊　・　坂谷　洋志＊　・　門田　淳＊　・　數野　浩基＊
Satoshi Okage　Hiroshi Sakatani　Atsushi Kadota　Hiroki Kazuno

PCのネットワーク接続認証時に，従来のIDとパスワードなどの入力だけでなく，入退室管理システムでID所有者の在室を確認して初めてネットワークに接続され，退室時には，ネットワークが切断される認証方法を開発した。

今回開発した方法は，RADIUS（Remote Authentication Dial In User Service）認証プロトコルを使用しているので，RADIUS認証を用いる802.1X認証システムを組み合わせることによって，より安全で多様なネットワークセキュリティーシステムを構築することができる。

The developed authentication method checks the identity of the PC user not only by the input of a user ID and password but also by the presence of the ID owner through the entry control system before authorizing a connection with the network and later disconnecting when the user exits the room.

Because the developed method utilizes the RADIUS (Remote Authentication Dial In User Service) protocol, safer and diversified network security systems can be constructed through combination with a RADIUS-based 802.1X authentication system.

1. ま え が き

2005年4月に施行された個人情報保護法などの影響により，オフィスでのセキュリティー対策へのニーズが高まっている。経済産業省が示すガイドラインにおいても，物理的安全管理措置において入退室（館）管理の実施が求められており，また，技術的安全管理措置においても情報システムへのアクセス制御が求められている。

そのために，ICカードや最近では生体認証などを用いる入退室管理システムが普及し，登録された認証方式で認証された人物だけに対象ゲートの通過を許可したり，入退場の履歴を記録している。

一方，情報システムへのアクセス制御において，ある特定の場所では入退室管理システムにより認証された人物にのみ，アクセスを許可したい場合が考えられる。たとえば，セキュリティーレベルの高いサーバルームでの情報システムの運用が挙げられる。また，社外の人物が在室している可能性のある会議室に社内LANが存在する際に，入室資格がない利用者には，その場所でのネットワークへのアクセスを制限したい場合もある。これらの場合には，入退室管理システムによる入退室情報を用いて情報システムへのアクセスを制限する必要がある。

また，情報システムへのアクセスを許可された人物が，ネットワークに接続したPCを放置したまま，その場所から退室している間に，不正な第三者が情報システムへアクセスしようとした場合に，そのアクセスを制限する必要がある。

今回筆者らは，入退室管理システムによる入退室情報と情報システムへのアクセス制御を組み合わせた認証方法により上記課題を解決し，より安全なネットワークセキュリティーシステムを構築できる装置を開発したので，その開発内容を報告する。

2. 情報システムへのアクセス制御技術

2.1 ネットワークアクセス制御方式

情報システムへの代表的なアクセス制御方式には，①クライアントPC起動アクセス制御方式，②サーバへのアクセス制御方式，③ネットワークアクセス制御方式がある。

①は，情報システム利用者の所有するPC自体の起動に対する制限を設ける。この方式は導入コストが安価であるものの，個々のPCの所有者に設定がゆだねられるため，全PCでの実施の徹底は期待できない。また，②は，情報システムにおける重要な情報を提供する側（サーバ）に認証を設定する。この方式は各サーバ管理者にアクセス制御

＊　新規商品創出技術開発部　設備ネットワークシステム開発部　Installation Network System Development, New Product Technologies Development Department

設定がゆだねられるために，サーバ管理者の技術レベルや知識によってセキュリティー水準に格差が生ずることは避けられない。

一方，③は，情報システムの存在するネットワーク自体へのアクセスに制限を設けるため，認証が成功しなければネットワーク接続ができないという方式であり，すでにIEEEで規定された802.1X認証方式やスイッチングHubのベンダによる独自認証方式が存在している。そこで筆者らは③のネットワークアクセス制御方式のなかの802.1X認証方式を採用して開発を進めた。

2.2　802.1X認証技術

802.1X認証は，有線および無線LANにおけるユーザ認証としてIEEEで規定されたネットワーク接続認証方式である。一般的には，**図1**のようなシステム構成になっており，①ユーザ認証を行うために利用者端末PCに搭載されるサプリカント（supplicant），②サプリカントからの認証要求をRADIUSサーバに転送する認証装置（NAS：Network Access Server），③認証装置経由でサプリカントからの認証要求に対する認証を行うRADIUSサーバから構成される。

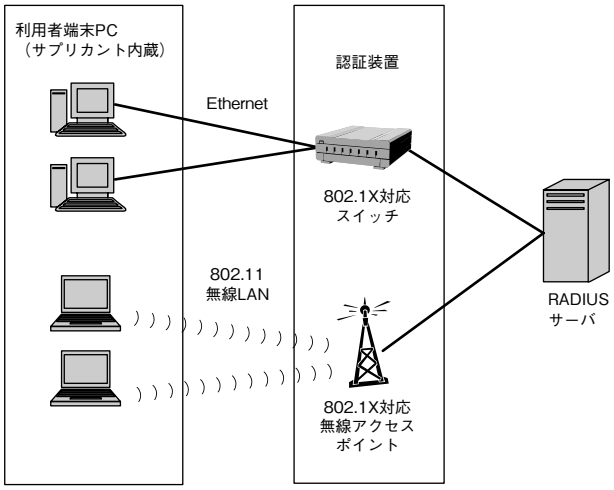

図1　802.1X認証システムの構成図

サプリカントは，認証装置およびRADIUSサーバと情報をやり取りするためのソフトウェアである。

認証装置は，複数サプリカントと無線または有線LANで接続され，RADIUSサーバとサプリカントとの認証処理を中継する中継装置として機能する。

RADIUSサーバは，認証装置との間の認証通信プロトコルとして，RADIUSプロトコルを用いる。RADIUSサーバは，あらかじめユーザ情報を登録することが可能であり，認証要求があった場合，登録情報に基づいて認証処理を行う。認証結果に応じてネットワーク接続の可否をサプリカントに通知する。

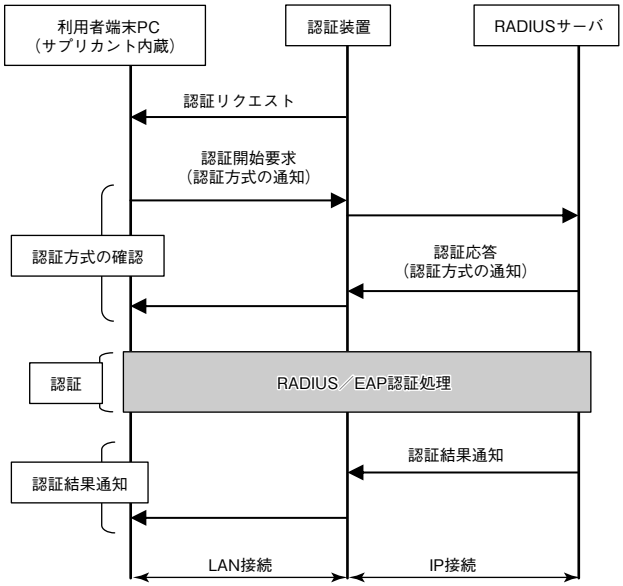

図2　802.1X認証のシーケンス図

図2は802.1X認証のシーケンス図で，認証手順を示している。認証開始のトリガは，基本的に認証装置からサプリカントに対して認証開始のMAC（Media Access Control）フレームが送信されるが，サプリカントから直接認証装置に対して認証要求のMACフレームを送信する場合もある。認証には，ユーザアカウントとパスワード（または電子証明書）が必要であり，サプリカントで入力されたそれらの入力情報は，EAP（Extensible Authentication Protocol）という通信プロトコルにより認証装置に送られる。認証装置は，受信したEAPメッセージをRADIUSパケットに乗せ換えてRADIUSサーバに送信し，RADIUSサーバの認証結果に基づいてサプリカントのネットワーク接続の可否を行う。

認証方式によりフレーム・パケットのやり取りの数は異なるが，認証の流れは大きく3ブロックに分かれており，①認証方式の確認，②認証方式に基づいた認証，③認証結果通知で区別される。

2.2.1　RADIUSプロトコル

RADIUSは，一般的に，ダイアルアップ接続などでユーザ認証を行うことで知られるプロトコルである。

RFC2865により，RADIUSプロトコルは以下のように規定されている。

（1）UDPベースのプロトコルである。
（2）通信状態をもたない。
（3）PPP（Point-to-Point Protocol）認証で用いられるPAP（Password Authentication Protocol）認証とCHAP（Challenge Handshake Authentication Protocol）認証をサポートしている。
（4）50種類以上の属性が用意されており，ベンダ固有の

機能も追加可能である。代表的なRADIUS属性を**表1**に示す。

表1　代表的なRADIUS属性

ID	属性名	説　明
1	User-Name	認証対象のユーザアカウント
4	NAS-IP-Address	認証装置のIPアドレス
5	NAS-Port	認証装置の認証要求対象ポート番号
26	Vendor-Specific	ベンダ固有属性
27	Session-Timeout	認証装置の次回再認証までの間隔
31	Calling-Station-Id	認証装置へ発信した機器の固有ID
32	NAS-Identifier	認証装置の機器名称
33	Proxy-State	RADIUSプロキシによる任意の属性値
61	NAS-Port-Type	着信があった回線の種別(Ethernet，無線LANなど)
79	Message-Authenticator	拡張認証符号(EAP-Message属性使用時必須)
80	EAP-Message	EAPのメッセージ

しかし，PAPは平文でパスワードが送信されること，CHAPはパスワードをハッシュしているが辞書攻撃に強くないことから，これらの認証方式は脆弱とされ，802.1X認証では用いられない。この脆弱性を解決するため，802.1X認証ではPPPを拡張し，認証方式を備えたEAPが使用されている。

2.2.2　EAP

データリンク層での通信プロトコルであるEAPは拡張可能な認証プロトコルという意味で，RFC3579で認証手続きの枠組みを規定されており，**表2**に主なEAP認証方式を示す。

EAPパケットは，IEEEで規定されているように，通信をやり取りするためにEAP-Message属性としてRADIUSプロトコルに定義されている。また，RADIUSパケットの内容を保証するため，認証装置とRADIUSサーバとで共有鍵をもち，HMAC-MD5により算出されたハッシュ値が格納されたMessage-Authenticator属性により，パケットの改ざんの有無を判別する仕組みがある。

EAPのデータをRADIUSパケットに搭載する際には，認証装置がサプリカントから受信したMACフレームよりEAPのデータを取り出し，UDP／IPパケットに乗せ変えてRADIUSサーバに送信する。

表2　主なEAP認証方式

認証方式	説　明
EAP-MD5 (RFC3748で規定)	パスワードをMD5ハッシュで送信する方式。 MD5に弱点があることからあまり使用されない。
EAP-TLS (RFC2716で規定)	サーバ,クライアント双方に電子証明書を用意し,相互に認証を行う。
EAP-TTLS [2)] (Tunneled TLS)	RADIUSサーバ側のサーバ証明書を使用してTLSセッションを確立し，実際の認証はTLSによる暗号化通信路を使用して行う。
EAP-PEAP [3), 4)] (Protected EAP)	RADIUSサーバ側のサーバ証明書を使用してTLSセッションを確立し，実際の認証はTLSによる暗号化通信路のなかでEAP認証方式(一般にEAP-MS-CHAPv2：RFC2759で規定)を使用する。

2.3　RADIUS中継認証技術

RADIUSプロトコルは，サプリカントからの認証要求をいったん受けて，代理でサーバに要求を送信するプロキシの設置を認めている。プロキシを利用することで，複数サプリカントからの認証要求をまとめることや，ユーザごとにRADIUSサーバを切り替えて転送することが可能となる。

RADIUSプロキシにおける必須処理は以下のようになる。

(1) 送信元との共有鍵を用い，RADIUSパケットヘッダ領域の一部であるデータの整合性を保証するための認証符号，およびMessage-Authenticator属性の値によるパケット送信元の認証とパケット改ざん有無の確認を行う。
(2) パケットを転送する際，そのパケットのヘッダ領域に格納されている識別子に対応づけした認証符号を記憶する。
(3) パケット転送先との共有鍵を用い，認証符号およびMessage-Authenticator属性の値を生成し，格納する。
(4) RADIUSプロトコルにおいて，受信パケットの認証符号およびMessage-Authenticator属性の値が不正であった場合，パケットは破棄される。

3.　在室情報と情報システムへのアクセス制御との連携

今回，在室情報と情報システムへのアクセス制御との連携を802.1X認証技術を用いて実現した。

3.1　在室情報によるRADIUS認証中継技術

在室情報と802.1X認証を組み合わせて認証する方式には，RADIUSサーバにその認証方法を組み込む方式と，RADIUSサーバと認証装置との間にRADIUSパケットの転送のみを行うプロキシサーバを置き，その認証方法を組み込む方式が考えられる。

今回開発した方式は，**図3**の構成図のように，後者のプ

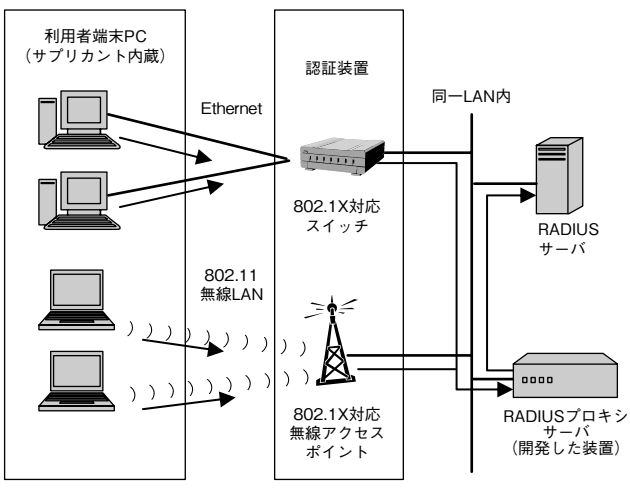

図3　RADIUSプロキシサーバを応用した構成図

ロキシサーバに組み込む方式とした。

この理由は，①既存の802.1X認証システムに追加可能，②RADIUSサーバと切り離すことでユーザ認証設定の簡略化が可能，③頻繁に発生するRADIUSサーバのバージョンアップの影響を受けないといった点である。

3.1.1　在室情報を追加した認証処理

在室情報をネットワーク認証条件に追加する方法として，以下の二つが考えられる。

（1）802.1X認証シーケンスにおける1番目の認証要求に含まれる情報を利用し，在室情報を認証条件に追加する事前認証方式（以下，プレ認証方式と記す）。

（2）802.1X認証シーケンスにおける最後の認証結果をもとに，それまでの認証シーケンスにおける認証情報を利用し，在室情報を認証条件に追加する事後認証方式（以下，ポスト認証方式と記す）。

プレ認証方式およびポスト認証方式の比較を**表3**に示す。

プレ認証方式は，プロキシサーバが認証シーケンス1番目の認証要求パケットを受信したタイミングで，パケットに含まれるユーザアカウントおよび認証装置IPアドレスを利用し，在室情報と比較することで，RADIUSサーバによる認証が開始される前に在室確認が行われる。

一方，ポスト認証方式は，プロキシサーバが認証シーケンス最後のRADIUSサーバによる認証成功応答パケットを受信したタイミングで在室条件を追加する。在室条件が不在の場合は，認証結果を認証拒否に書き換えて認証装置に送信するが，この書換処理には以下のような問題がある。認証方式EAP-PEAPなどは，TLSによる暗号化通信路で認証が行われるため，EAP認証での認証結果がプロキシサーバにより書き換えられた場合，サプリカントはRADIUSサーバと認証シーケンス内で生成したTLS暗号鍵によるパケット認証からデータが改ざんされたことを検知し，認証結果を破棄してしまう。したがって，サプリカントは認証結果を受信できず，正常な認証処理を完了することができない。そのため，認証シーケンス内で行われるTLS暗号化通信路をMan-In-The-Middleを用いて解読し，認証結果を書き換えて再暗号化する必要がある。しかし，TLS暗号化通信路の解読を行う際，認証シーケンスにおける認証情報の記憶管理，公開鍵基盤（PKI：Public Key Infrastructure）によるキー生成，パケットの復号化と暗号化などの処理が必要になるため，メモリーの増加，計算処理の増加に伴ないハードウェアのコストの増大につながる。

以上のことから，プレ認証方式を採用して在室情報を追加した認証を実現している。

表3　プレ認証方式とポスト認証方式の比較

	プレ認証方式	ポスト認証方式
在室確認を行うためのユーザ情報	RADIUS要求パケットに含まれるUser-Name属性またはEAP-Message属性内のIdentityに含まれる。	EAP-PEAP，EAP-TTLS：TLS暗号通信路を解読し，認証結果が格納されたRADIUS応答パケットに含まれる。 EAP-TLS，EAP-MD5：認証結果が格納されたRADIUS応答パケットに含まれる。
不在時のRADIUSサーバへの認証発生	なし	あり
不在時のサプリカントへの認証拒否通知方法	在室情報による認証拒否判断時，Access-Rejectパケットを作成し，認証装置に応答する。	認証結果が成功（Accept）である領域をAccess-Rejectに書き換え，認証装置に応答する。
在室確認処理以外に追加する特別な処理	なし	TLSによる暗号通信路の暗号解読（EAP-PEAP，EAP-TTLSで必要）

3.1.2　プレ認証方式による認証処理

図4は，RADIUSプロキシを応用して，在室情報を認証条件に追加した処理をシーケンス図で表示したものである。

在室情報による認証が行われるRADIUS認証シーケンス1番目のパケットは，EAP-Messageの属性としてEAP-Type＝Identityの値が存在する。その値を検索することで，在室情報を追加した認証許可または認証拒否の認証結果を即座に得ることが可能となる。

認証許可の場合は，認証要求をRADIUSサーバに転送し，通常のユーザアカウント登録による認証を行う。すなわち，RADIUSプロキシサーバと同様の動作を行う。

一方，認証拒否と判断した場合は，即座にRADIUS認証拒否の応答を認証要求元に送信する。認証拒否を送信する際は，RADIUSプロトコルに従ってAccess-Rejectパケットを作成して送信する。

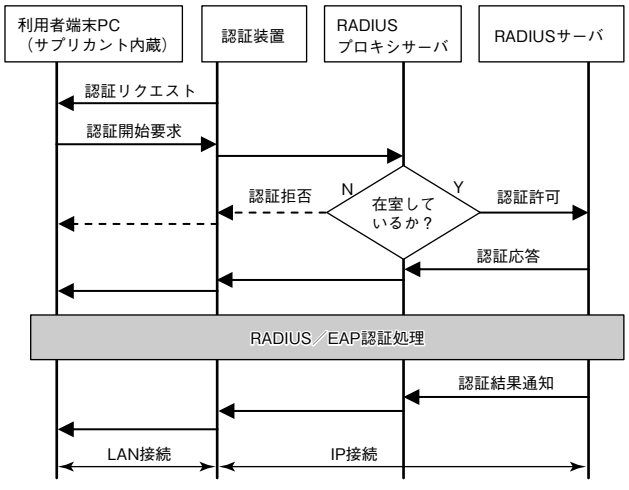

図4　在室情報を組み合わせたシーケンス図

3.1.3　在室情報による認証許可判断

在室情報をもとにした認証許可または拒否の判断は，RADIUS認証におけるユーザアカウントを用いて実現する。

ユーザアカウントは，RADIUS認証要求パケットではUser-Name属性およびEAP-Message属性内のIdentityに含まれる。

RADIUSプロキシサーバ内では，在室情報として入退室管理システムから得られるカード情報をあらかじめ登録し

ておく。そして，取得したユーザアカウントと，対応する在室情報を比較参照することにより，ユーザの認証許可または拒否の判断を行う。

3.1.4　RADIUSプロキシサーバ認証拒否応答規格適合性

一般に認証拒否応答はRADIUSサーバから返却する方法でのみ利用される。しかし今回は，認証拒否の応答をRADIUSプロキシサーバから直接送信する方法を採用するため，規格上の問題の有無を確認する必要がある。

RFC3579（RADIUS Support For Extensible Authentication Protocol）に以下の内容が記載されている。

RADIUS通信は，Access-Acceptパケットもしくは Access-Rejectパケットを受信するまで続く。

（1）Access-Rejectパケットを受信した場合，認証装置はピアからのアクセスを拒否する必要がある。
（2）EAP-Message属性をサポートしないサーバはEAP-Message属性を含む要求にAccess-Rejectを返さなければならない。
（3）RADIUSサーバは，不正なパケットを受信し，致命的エラーが発生した場合，EAP-FailureのEAP-Message属性を含んだAccess-Rejectを送信しなければならない。

したがって，在室情報による認証拒否を「致命的なエラー」と解釈することで，規格上問題なく，認証結果をRADIUSサーバと関係のない箇所から送信することが可能となる。

3.2　入退室管理システムを利用した在室情報の提供

今回開発した装置では，入退室情報を入退室管理システムから取得し，その情報をユーザアカウントを用いて検索しているが，その方法について以下に述べる。

3.2.1　在室管理DB

今回開発した装置は，ユーザから認証要求を受け取ると，その転送可否を判断するにあたり，ネットワークが敷設された部屋におけるそのユーザの在室情報を確認する。その際に参照しているのが在室管理DBである。この在室管理DBでは，本装置が管理しているすべての部屋における入退室状況を集約し，ユーザの在室情報を一括して管理している。**図5**は在室管理DBの基本的な構造を示し，以下ではこれについて説明する。

管理の対象となる部屋の扉にはカードリーダが設置されており，ユーザがそれらの部屋に出入りする際には，カードリーダに自分のカードをかざす必要がある。ユーザがカードをカードリーダにかざすと，その情報は入退室管理システムを介して在室管理DBに送信される。在室管理DBでは，受信した情報をもとに，ユーザ，場所，動作を特定（すなわち，どの部屋に入室したのか，またはどの部屋から退室したのか）をして在室情報として保持する。

3.2.2　認証機能との連携

ここでは在室管理DBが認証要求に対してどのような動作を行うかについて説明する。

ユーザがネットワークにアクセスするために送信した認証要求は，サプリカントが接続されている認証装置を通って装置内の在室管理DBに届く。在室管理DBでは，認証装置のIPアドレスと設置されている部屋はあらかじめ関連づけられているため，ユーザがどの部屋からアクセスを試みているのかを知ることができる。

ここで，認証装置が設置されている部屋と，アクセスを試みているユーザが在室している部屋が一致しない場合には，認証要求は転送しない。

3.2.3　ユーザ情報の設定

今回開発した装置におけるユーザ情報の設定について述べる。

ユーザ情報は，ユーザが入退室管理システムを利用するためのカードの情報と，802.1X認証システムを利用する

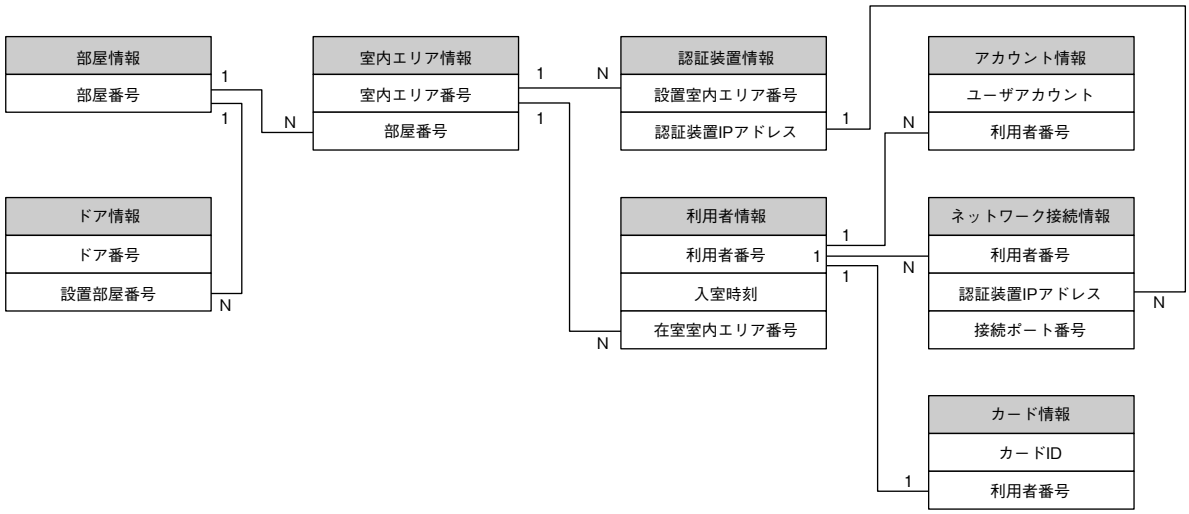

図5　在室管理DB

ためのユーザアカウントの情報が関連づけられた形で在室管理DBに登録される。これにより，ユーザアカウントから在室情報を検索することができる。

今回開発した装置においては，ユーザ情報を所定のcsvファイル形式とし，Webインタフェイス経由でインポート可能としている。

4. 退室時の切断技術

4.1 退室時切断の必要性

3章では，在室情報に基づき認証許可または拒否の判断を行う仕組みについて述べている。しかし，この仕組みによりネットワークにアクセスしようとするユーザの在室情報が確認されるのは，最初に認証要求があったときだけであり，たとえば一度認証許可されたあとに退室したとしても，ネットワークはそのままアクセス可能な状態となっている。すなわち，正規のユーザが退室している間に，不正な第三者がネットワークにアクセスしようとした場合には，それを防ぐことができない。

したがって，このような問題を解決するための対策が必要となる。

4.2 再認証による退室時切断機能

前節に述べたような問題の対策として，今回開発した技術は，ユーザが退室した場合にSNMPを用いて自動的に認証許可を取り消し，ネットワークを切断する機能を追加している。なお，この退室時切断機能が作動するためには，認証装置が802.1X MIBに対応している必要がある。対応していない場合にはこの機能は作動しないため注意が必要である。以下に，SNMPを用いて開発した退室時切断機能の概要を示す。

入退室管理システムからユーザが退室したとの情報を受信すると，まず認証装置から該当ユーザが接続中のポートの状態情報（dot1xAuthPaeState.x，ただし，xは認証装置のポート番号）を取得する。その結果，確かにそのポートがネットワークに接続中であれば，続いてそのポートに接続しているサプリカントについて再認証を行うよう要求（dot1xPaePortReauthenticate.x＝TRUEをセット。ただし，xは認証装置のポート番号）する。すると，3.1.2項で説明したプレ認証方式による認証シーケンスが再度実行され，その時点で該当するユーザは在室していないために認証は拒否されて，ネットワークへのアクセスを切断することができる。以上の処理のシーケンス図を，図6に示す。

5. ネットワーク認証方式の拡張

今回採用した802.1X認証技術は，認証装置のコストダウンのための拡張仕様がある。また，無線LANを利用する場合についても考慮する必要がある。

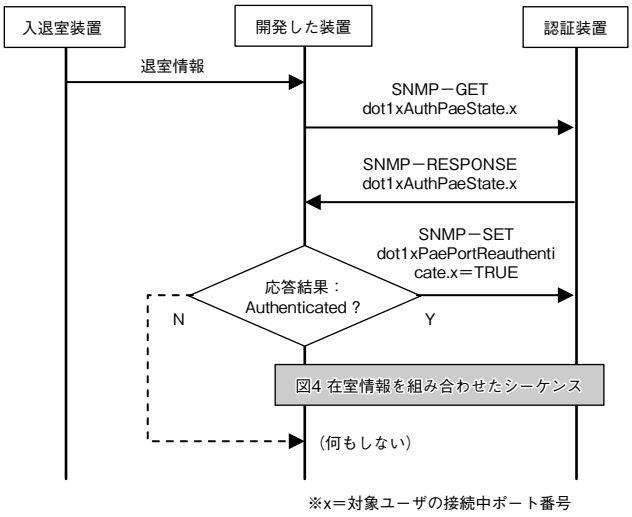

図6　退室時切断動作のシーケンス図

5.1 認証装置による各種認証形態

5.1.1 ポートベース認証

ポートベース認証とは，図7に示すように有線LAN認証装置に装備された各LANポートにサプリカントが1台ずつ接続する構成で認証を行う形態である。したがって，認証装置に装備されたLANポートの数だけ，サプリカントの認証が可能となるので，高価な認証装置にもかかわらずサプリカント利用台数が少ないという問題がある。

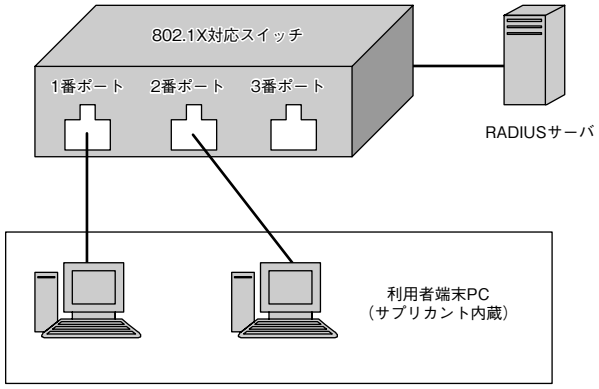

図7　ポートベース認証構成図

5.1.2 MACベース認証

MACベース認証は，図8に示すようにポートベース認証で課題となっていたLANポート対サプリカントが1：1の構成を1：nによる接続に対応した認証形態である。認証装置の任意のLANポートに，802.1X対応の認証装置と比較して，より安価で802.1X未対応のマルチキャストアドレスのMACフレームを通過させることが可能なSwitching hubを接続した構成で，認証装置はサプリカントのMACアドレスをもとに認証状態を制御する。

5.1.3 無線LANによる認証

無線LANによる認証においては，無線アクセスポイン

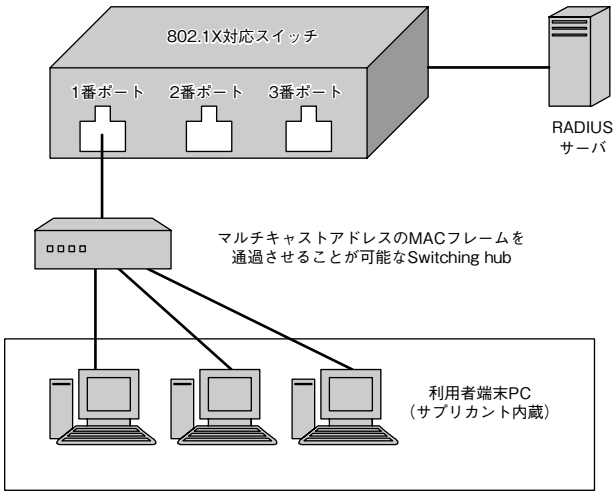

図8　MACベース認証構成図

トが認証装置となる。とくに無線環境では，他のユーザによる通信ポートのなりすましを防止するため，運用上定期的に再認証を行わせることが推奨されている。

認証装置によっては，認証するごとにLANポート番号（仮想ポート番号）を変更する処理機能が実装されている。

5.2　MACベース認証に対応した認証要求識別技術

5.2.1　認証装置IPアドレスおよびポートによる識別方法

認証装置の認証形態がポートベース認証である場合は，ユーザアカウントごとに認証装置IPアドレスと認証成功したLANポート番号から接続箇所を一意に判別可能であるため，認証要求の識別が可能となる。

認証装置IPアドレスは，受信パケットの送信元，またはNAS-IP-Address属性から取得可能である。認証成功したLANポート番号は，NAS-Port属性から取得可能である。

ただし，この制御では，認証装置の一つのLANポートに複数接続するMACベース認証，およびLANポート番号が変化する無線LANによる認証には対応できない。

5.2.2　MACアドレスによる制御方法

MACベース認証および無線LANによる認証でも個々の認証要求を識別可能にするためには，ユーザアカウントごとに，認証要求を行うサプリカントのMACアドレスを直接管理することが必要である。

MACアドレスは，Calling-Station-Id属性から取得可能である。

この技術を応用することでユーザごとのネットワーク接続数も管理することが可能となり，ユーザごとに接続制限を設けるなどの応用が考えられる。

6. あ と が き

PCのネットワーク接続認証時に，従来のIDとパスワードなどの入力だけでなく，入退室管理システムでID所有者の在室を確認して初めてネットワークに接続され，退室時には，ネットワークが切断される認証方法を開発した。

今回開発した方法は，RADIUS認証プロトコルを使用しているので，RADIUS認証を用いる802.1X認証システムを組み合わせることによって，より安全で多様なネットワークセキュリティーシステムを構築することができる。

この技術は，標準通信技術である802.1X認証通信技術およびRADIUS通信技術の規格に合致しており，各種ベンダの提供する802.1X関連応用製品と組み合わせて，各種応用展開が可能である。

＊参 考 文 献

1）Jonatban Hassell：RADIUSユーザ認証セキュリティプロトコル，O'REILLY, p. 19-71, p. 155-190
2）P. Funk, S. Blake-Wilson：EAP Tunneled TLS Authentication Protocol (EAP-TTLS) (February 2002)
3）H. Andersson, S. Josefsson, G. Zorn, D. Simon, A. Palekar：Protected EAP Protocol (PEAP) (February 2002)
4）V. Kamath, A. Palekar, M. Wodrich：Microsoft's PEAP version 0 (Implementation in Windows XP SP1) (October 2002)

◆執 筆 者 紹 介


大景　聡
設備ネットワークシステム開発部


坂谷　洋志
設備ネットワークシステム開発部


門田　淳
設備ネットワークシステム開発部


數野　浩基
設備ネットワークシステム開発部