The Guaranteed Network
いちばん近くで、もっと先へ。

AX シリーズ
認証ソリューションガイド

第 13 版

資料 No. NTS-07-R-015

アラクサラネットワークス株式会社

はじめに

本ガイドは AX シリーズ(AX1200S, AX2200S, AX2400S, AX2500S, AX2300S, AX2600S AX3600S, AX3800S)でサポートしているネットワーク認証機能を用いて、システム構築のための技術情報をシステムエンジニアの方へ提供し、セキュリティの高いシステムの構築と安定稼動を目的として書かれています。RADIUS サーバの設定に関しては、各種 RADIUS サーバ毎に用意した別冊の「RADIUS サーバ設定ガイド」を参照下さい。

AX3800S シリーズについては、AX3600S シリーズと機能差分は無いため本資料では、AX3600S を参照してください。 物理ポート等のコンフィグ差分は製品マニュアルを参照ください。

関連資料

・RADIUS サーバ設定ガイド　Windows Server 2003 編
・RADIUS サーバ設定ガイド　Windows Server 2008 編
・AX シリーズ 認証ソリューションガイド（マルチステップ認証編）
・AX シリーズ 認証ソリューションガイド（RADIUS サーバグループ選択機能編）
・AX シリーズ製品マニュアル（https://www.alaxala.com/jp/techinfo/manual/）
・別冊　Web 認証マニュアル SSL 証明書運用編

本ガイド使用上の注意事項

本ガイドに記載の内容は、弊社が特定の環境において、基本動作や接続動作を確認したものであり、すべての環境で機能・性能・信頼性を保証するものではありません。弊社製品を用いたシステム構築の一助としていただくためのものとご理解いただけますようお願いいたします。

Windows 製品に関する詳細はマイクロソフト株式会社のドキュメント等を参照下さい。

本ガイド作成時の OS ソフトウエアバージョンは以下のようになっております。

AX1230S	Ver1.4.K
AX1240S /AX1250S/AX2200S	Ver2.4.A
AX2400S	Ver11.7.F
AX3600S	Ver11.11
AX2500S/AX2500SE	Ver4.26
AX2300S/AX2600S	Ver2.5

本ガイドの内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上、必要な手続きをおとりください。

なお、不明な場合は、弊社担当営業にお問い合わせ下さい。

商標一覧

・アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および登録商標です。
・Ethernetは、富士フイルムビジネスイノベーション株式会社の登録商標です。
・イーサネットは、富士フイルムビジネスイノベーション株式会社の登録商標です。
・Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
・Windowsは、米国およびその他の国における米国Microsoft Corp. の登録商標です。
・Mac OS Xは、米国およびその他の国におけるApple Inc.の登録商標です。
・そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

使用機器一覧

- AX1230S (Ver1.4.K)
- AX1240S (Ver2.4.A)
- AX2430S (Ver11.7.F)
- AX3630S (Ver11.11)
- AX2530S (Ver3.5)
- Windows Server 2008 R2 Standard
- Windows XP Professional (SP3)
- Windows Vista Ultimate (SP2)
- Windows 7 (SP2)
- Windows 8
- Mac OS X v10.5 Leopard

使用ブラウザ一覧

- Internet Explorer (Version8)
- Internet Explorer (Version9)
- Internet Explorer (Version10)
- Firefox (20.0)
- Safari (3.1.1)

改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	－	2007.7.26.	初版発行	－
第 2 版	－	2007.9.28.	省略	－
第 3 版	－	2007.12.5.	省略	－
第 4 版	－	2008.3.21.	省略	－
第 5 版	－	2008.6.2.	省略	－
第 6 版	－	2008.9.24	省略	－
第 7 版	－	2009.1.30	省略	－
第 8 版	－	2009.5.22	省略	－
第 9 版	－	2009.7.24	1.2.5 章に注意事項 6.2.10 章への参照追加 5 章　構築ノウハウの章を追加 　Web 認証で外部 Web サーバを使用するを追加 6章 注意事項を追加 　Web 認証で SSL を使用する場合の注意事項追加	1.2.5 5 5.1 6 6.2.10
第 10 版	－	2010.1.18	はじめに 　関連資料にマルチステップ編,RADIUS サーバグループ選択機能編を追加 　AX のソフトウェアバージョン更新 1 章ネットワーク認証概要 　RADIUS アトリビュートの解説を修正 　AX-Networker's-Utility(Web 認証画面入替えツール)を追加 2 章　AX シリーズの認証機能サポート一覧 　RADIUS アトリビュートの解説を修正 　表 2.6-1 にポート単位の Web 認証画面選択を追加 　RADIUS サーバグループ選択機能を追加 6 章　注意事項 　URL リダイレクトの負荷対策バージョンを追加 　AX2400S/AX3600S 使用時の同一 VLAN 内の端末移動の変更 　端末移動後の VLAN が変わる場合の再認証の必要性を追加 7 章　運用コマンド 　AX1240S 使用時の RADIUS サーバ状態表示コマンドに変更	はじめに 1.2.4.2 1.5 2.4 2.6 2.9 6.2.2 6.2.4 6.2.7 7.1.1
第 10 版	1	2010.3.26	動的 VLAN(MACVLAN)使用時のレイヤ 2 ハードウェアテーブルの検索方式をオートに設定	3.3.2(1) 3.3.3(1) 3.3.4(1)
第 11 版	－	2011.1.7	はじめに 　AX2500S シリーズを追加、使用機器 Ver 更新 2 章　AX シリーズの認証機能サポート一覧 　AX2500S シリーズを追加 　AX6000S シリーズへダイナミック VLAN を追加 3 章　AX シリーズの認証機能サポート一覧 　AX2500S 構築例の追加 6 章　注意事項 　AX2500S の注意事項を追加（AX1200S シリーズと共通） 7 章　運用コマンド 　AX2500S の運用コマンド追加（AX1200S シリーズと共通） 付録　コンフィグレーション 　　（AX2500S 追加）	はじめに 2 章全般 2.1, 2.6, 2.7 3.3, 3.5 6 章全般 7 章全般

第 12 版		2013.6.28	はじめに 　AX2200S シリーズを追加、使用機器 Ver 更新、AX3800S について AX3600S を参照する記述を追加 1 章 　AX2200S シリーズ追加 　ダイナミック ACL/QoS 認証について追加 　（AX2500S シリーズ） 2 章 　AX2200S シリーズ追加 　AX2500S　エンハンス内容更新(Ver3.1～ Ver3.5) 3 章 　AX2200S シリーズ追加（AX1200S シリーズを参照へ） 　AX2500S　ダイナミック ACL およびトランクポートによる VLANTag 付き認証を追加 4 章 　4.1.3 WindowsXP(SP2)から IEEE802.1X 接続を開始する方法を削除 　Windows7 /Windows 8 の設定例の追加 5 章 　外部 Web サーバ連携において、AX2500S シリーズのエンハンス内容追加　外部 Web サーバコンフィグ指定、外部 Web サーバポーリング、認証成功時に認証前にアクセスしていた URL を自動表示する機能追加 6 章 　IEEE802.1X 注意事項見直し 　（Windows7/Windows8 追加など） 　AX2200S シリーズ追加 　AX2500S　ポートリンクダウン時の認証解除抑止追加 　およびその他見直し 　ダイナミック VLAN において認証成功画面表示に関する注意事項追加 7 章 　AX2200S 追加 　AX2500S は差分がある事を追加	 1 章全般 1.4 2 章全般 2.11 3.1 3.2 3.5 4.1 4.2 5 章全般 6 章全般 7 章全般
第 13 版		2024.9	はじめに 　AX2300S/AX2600S シリーズを追加 1 章 　AX2300S/AX2600S シリーズを追加 2 章 　AX2300S/AX2600S シリーズを追加 6 章 　AX2300S/AX2600S シリーズを追加 7 章 　AX2300S/AX2600S シリーズを追加 付録 B 　外部 Web サーバ入替え用ファイルの AX2300S/AX2600S 用の添付追加	はじめに 1 章全般 2 章全般 6 章全般 7.1 付録 B

目次

1. ネットワーク認証概要

本章では、AX シリーズを用いて、ネットワーク認証を行なうために必要な情報として、1.1 章ネットワーク認証の概要と、1.2 章で AX がサポートする認証方式（IEEE802.1X 認証、Web 認証、MAC 認証）について説明し、1.3 章で AX における認証端末をどの通信インタフェース単位で認証させるか選択する認証モード（ポート単位、動的 VLAN、固定 VLAN）について説明し、1.4 章では検疫システムの概要を説明します。

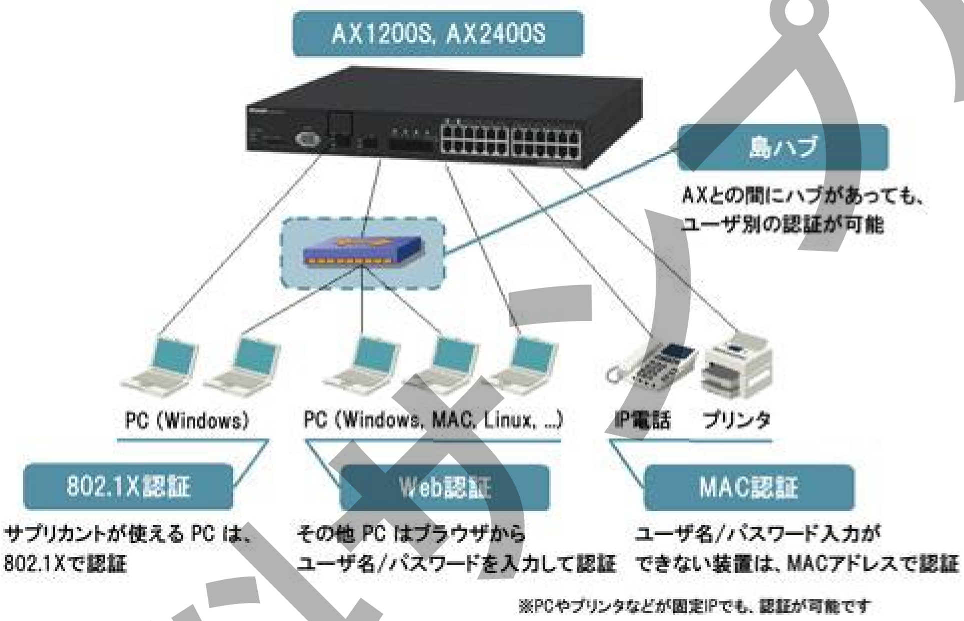

図 1.1-1　アラクサラのトリプル認証

1.1. ネットワーク認証とは

現在、ネットワークは絶えず不正アクセスの脅威にさらされています。従来は外部からのアクセスに対して、ファイアウォール等の装置にて不正アクセスを防いでいましたが、それでも機密情報の漏洩や個人情報の流出事件が多発しました。最近では外部からのアクセスだけでなく、むしろ内部からの不正アクセスが問題となっています。

また、昨今叫ばれている企業の内部統制の必要性から、IT による情報システムによって、業務の管理・記録を残すことも重要となってきています。

そのために、ネットワークにアクセスする際に、アクセスする本人がシステムに登録された正規のユーザであるかを確認する、ネットワーク認証システムが必要とされています。

ネットワーク認証システムによって、以下のことが実現できます。

1) 不特定多数が同時に接続するネットワークにおいて、許可されたユーザに対してのみネットワークサービスを提供することにより、リソースの枯渇を防ぎます。
2) 正規の権限を認められていない情報資源に対して、ネットワークアクセスを許可しないことにより、ネットワークおよび情報システムの安全性を確保します。
3) 情報資源の有効活用および万が一情報漏洩が発生した場合の危機管理という観点から、ネットワークや情報資源の利用状況および利用者の把握を行います。

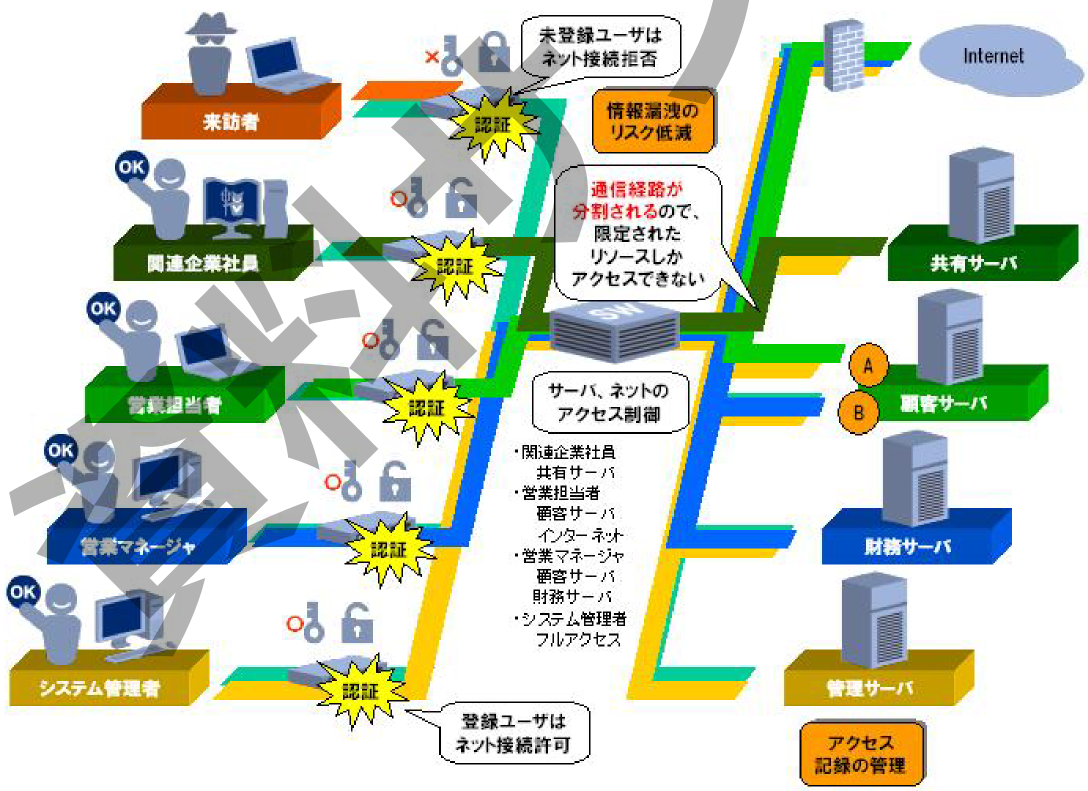

図 1.1-1 ネットワーク認証概要

1.2. 認証方式の特徴およびシステム要素

1.2.1. IEEE802.1X 認証

1.2.1.1. 概要

IEEE802.1X 認証は、アクセス可能なポートからの不正な接続を規制する機能です。バックエンドに認証サーバ(Authentication Server,一般的には RADIUS サーバ)を設置し、認証サーバによる端末(Supplicant)の認証が成功した上で、スイッチ(Authenticator)が通信を許可します。

端末(Supplicant)-スイッチ(Authenticator)間の認証処理に関わる通信は EAP Over LAN(EAPOL)で行います。スイッチ(Authenticator)ー認証サーバ(RADIUS サーバ)間は EAP Over RADIUS プロトコルを使って認証情報を交換します。

構成要素と動作概略を以下に示します。

表 1.2-1 IEEE802.1X 認証の構成要素

項番	構成要素	動作概略
1	Authenticator（スイッチ)	Supplicant のネットワークへのアクセスを制御します。Supplicant と Authentication Server(RADIUS サーバ)の仲介に位置し、相互間の認証シーケンスをトランスペアレントに行います。Supplicant に識別情報を要求し、その情報を認証サーバで確認し、Supplicant に応答をリレーします。Authenticator は、EAP フレームのカプセル化/カプセル化解除、および RADIUS サーバとの対話を処理します。
2	Supplicant(端末)	IEEE802.1X の仕様では、クライアント(端末)は Supplicant といい、IEEE802.1X に準拠するソフト又は OS(Windows XP 等)の搭載が必要です。
3	Authentication Server (RADIUS サーバ)	Supplicant の認証を行います。認証サーバは Supplicant の識別情報を確認し、要求元の Supplicant にサービスへのアクセスを許可すべきかどうかを Authenticator に通知します。

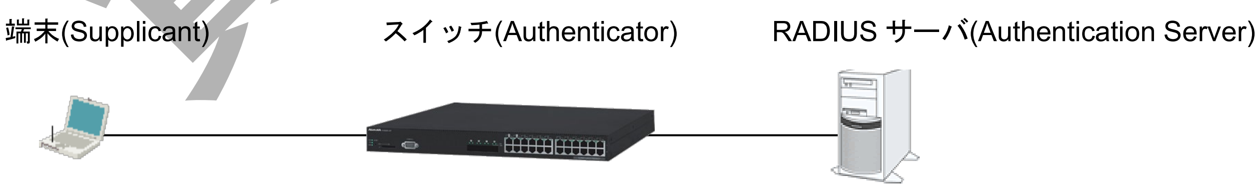

図 1.2-1 IEEE802.1X 認証の構成要素

1.2.1.2. 拡張認証プロトコル(EAP)

EAP(Extensible Authentication Protocol)は複数の認証方式が提案されています。

表 1.2-2 IEEE802.1X の EAP 認証方式

項番	認証方式	特徴
1	EAP-MD5	この方式は、ユーザ ID とパスワードによるクライアント認証であり、電子証明書を必要としないため実装が容易になるというメリットがあります。ただし、クライアントのみを認証する片方向認証であることや、暗号解読による漏洩には脆弱な面もあります。また、Windows XP SP1 以降からは非対応(削除)になりましたが、EAP の実装では MD5 をサポートすることが義務付けられています。
2	PEAP (Protected EAP))	クライアント側ではユーザ ID とパスワードによる認証、認証サーバ側では電子証明書による認証が行われる方式。Cisco-PEAP と MS-PEAP があります。Windows では MS-PEAP を標準で対応しています。
3	EAP-TLS	TLS は、情報を暗号化して安全に送受信するプロトコルで、電子証明書を利用してクライアントと認証サーバの相互認証を行います。電子証明書を使うためセキュリティは高いですが、クライアントと認証サーバの双方で電子証明書の管理が必要となり、PKI 導入基盤が用意されていない場合は使い難いと言われています。なお、Windows が標準で対応しています。
4	EAP-TTLS	MD5 と TLS 双方の利点を併せ持った方式。トンネルを張り認証を行うことでセキュリティを確保します。クライアント側ではユーザ ID とパスワードによる認証を行うことで、導入・管理・運用が TLS と比較して容易だといわれています。また、認証サーバ側では電子証明書が利用されるため、高いセキュリティ性の確保が可能です。ただし、TTLS 対応の Supplicant と認証サーバが必要となります。

暗号強度や鍵生成・配布のプロセスという観点からは、EAP-TLS がもっとも信頼性の高い認証方式となりますが、運用の負荷を考えると PEAP を選択するメリットもあります。

1.2.1.3. EAP 認証シーケンス

EAP のやり取りを以下に示します。

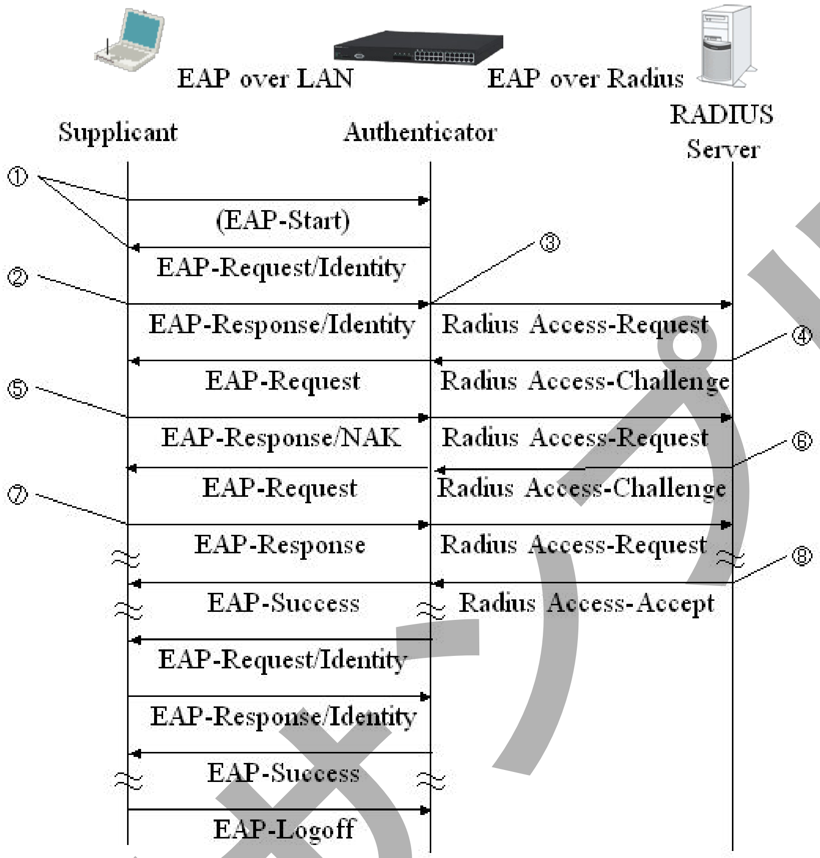

図 1.2-2　EAP 認証シーケンス

1. Supplicant からの EAP-Start または Authenticator からの EAP-Request/Identity によって、EAP シーケンスを開始します。認証は常に EAP-Start から始まらなければいけないというわけではなく、Authenticator は常に EAP-Request/Identity を送信して認証を促すことができます。また、Windows XP はデフォルトの設定では EAP-Start を送信しないため、端末を検知するまでには EAP-Request/Identity の送信間隔を待たなければなりません。
2. Supplicant はユーザ識別子を収集し、Response/Identity メッセージにユーザ識別子を挿入し送信します。
3. Authenticator は Response/Identity を RADIUS Access-Request に変換し、Authentication Server (例では RADIUS Server)に転送します。
4. Authentication Server からは認証チャレンジが発行されます。認証チャレンジは、Authenticator が EAP に変換して Supplicant に転送します。
5. 認証チャレンジを受信した Supplicant は、利用している認証方式と合致している場合は Response を返します。認証方式が合致していなかった場合は、Response/NAK を返します。
6. Authenticator は認証方式が合致するまで、方式を変えて認証チャレンジを再送します。

7. Supplicant は認証方式が合致した場合、Response/(認証タイプ)を返信します。
8. Authentication Server から Accept が返ってくると、Authenticator はポートを開放し、Success の通知を Supplicant に転送します。

1.2.1.4. EAPOL フレームフォーマット

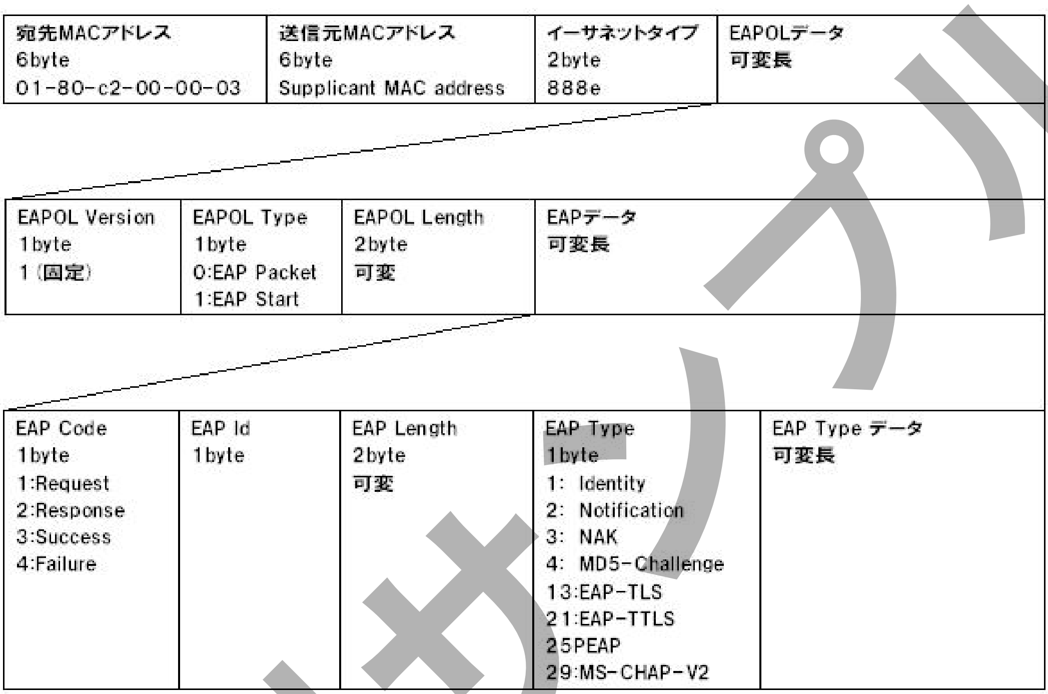

図 1.2-3 IEEE802.1X の EAPOL フレームフォーマット

EAPOL の宛先 MAC アドレスは予約マルチキャストとなっています。このアドレスは他の予約マルチキャストアドレスと同様に、IEEE802.1D では中継しないことを推奨されているため、スイッチによっては廃棄されてしまうことがありますのでご注意下さい。
(IEEE 802.1D-2004 7.12.6 Reserved address)

1.2.2. Web 認証

1.2.2.1. 概要

Web 認証は、Firefox や Internet Explorer などの汎用の Web ブラウザを利用してユーザ ID およびパスワードを使った認証によりユーザを認証し、ユーザが使用する端末の MAC アドレスを使用して認証状態に移行させ、認証後のネットワークへのアクセスを可能にする機能です。

本機能により、端末側に特別なソフトウェアをインストールすることなく、Web ブラウザのみで認証を行うことが可能となります。

クライアントとスイッチ間のプロトコルは基本の http に加え、認証情報を暗号化するための https をサポートしています。

Web 認証では1.3章にて説明する動的 VLAN モードと固定 VLAN モードを選択することができます。

動的 VLAN モードでは、MACVLAN ポートで認証することにより、同一ポート配下でユーザ毎に VLAN を切り替えることが可能です。認証前は認証前 VLAN に接続され認証後に指定された VLAN に切り替えます。また認証前と認証後で VLAN(ネットワーク)切り替わるため、固定 IP の端末は使用できません。

固定 VLAN モードでは、アクセスポートで認証する場合はポート単位で VLAN が固定となります。トランクポートでの認証もサポートしており、この場合 Tag-VLAN で認証が可能です。認証前と認証後の VLAN 切り替えが発生しないので固定 IP 端末の接続が可能となります。固定 VLAN モードでは、認証前には認証専用のアクセスリストに登録された宛先のみ通信可能です。

注）マニュアルでは動的 VLAN の事をダイナミック VLAN と表記している場合があります。

1.2.2.2. Web 認証シーケンス

以下に動的 VLAN モードにおける Web 認証の動作シーケンスについて示します。

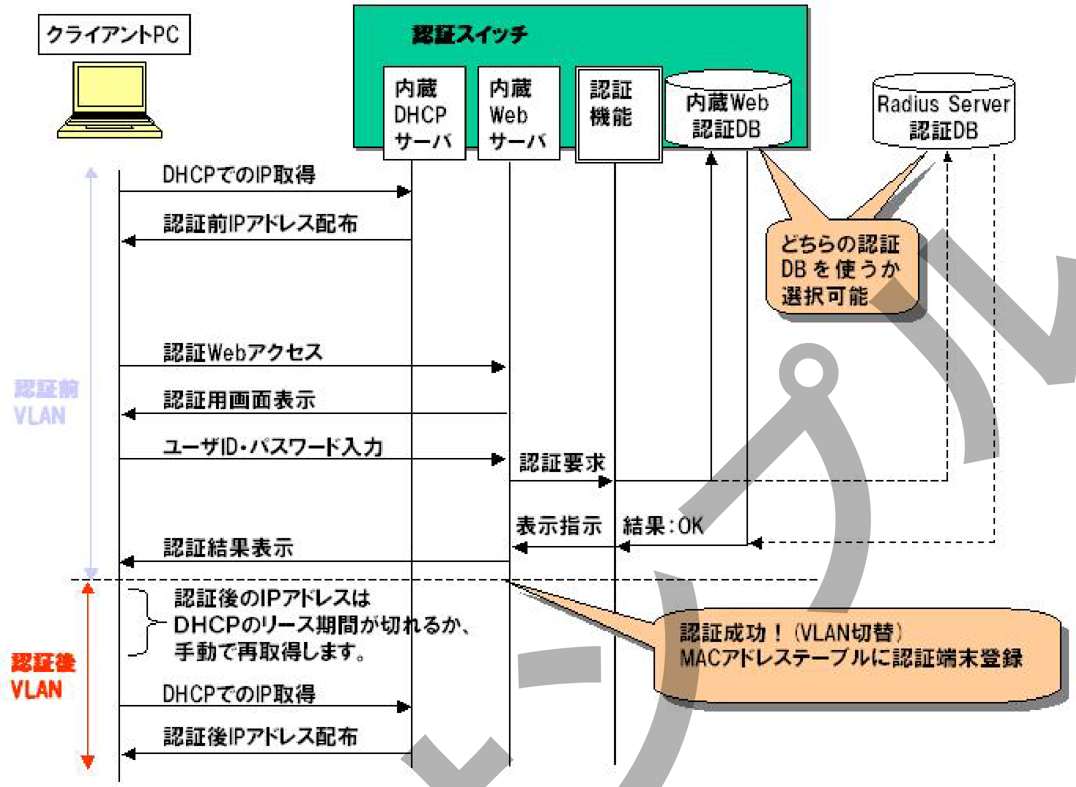

図 1.2-4　動的 VLAN モードにおける Web 認証シーケンス

以下に固定 VLAN モードにおける Web 認証（URL リダイレクト有効時）の動作シーケンスについて示します。

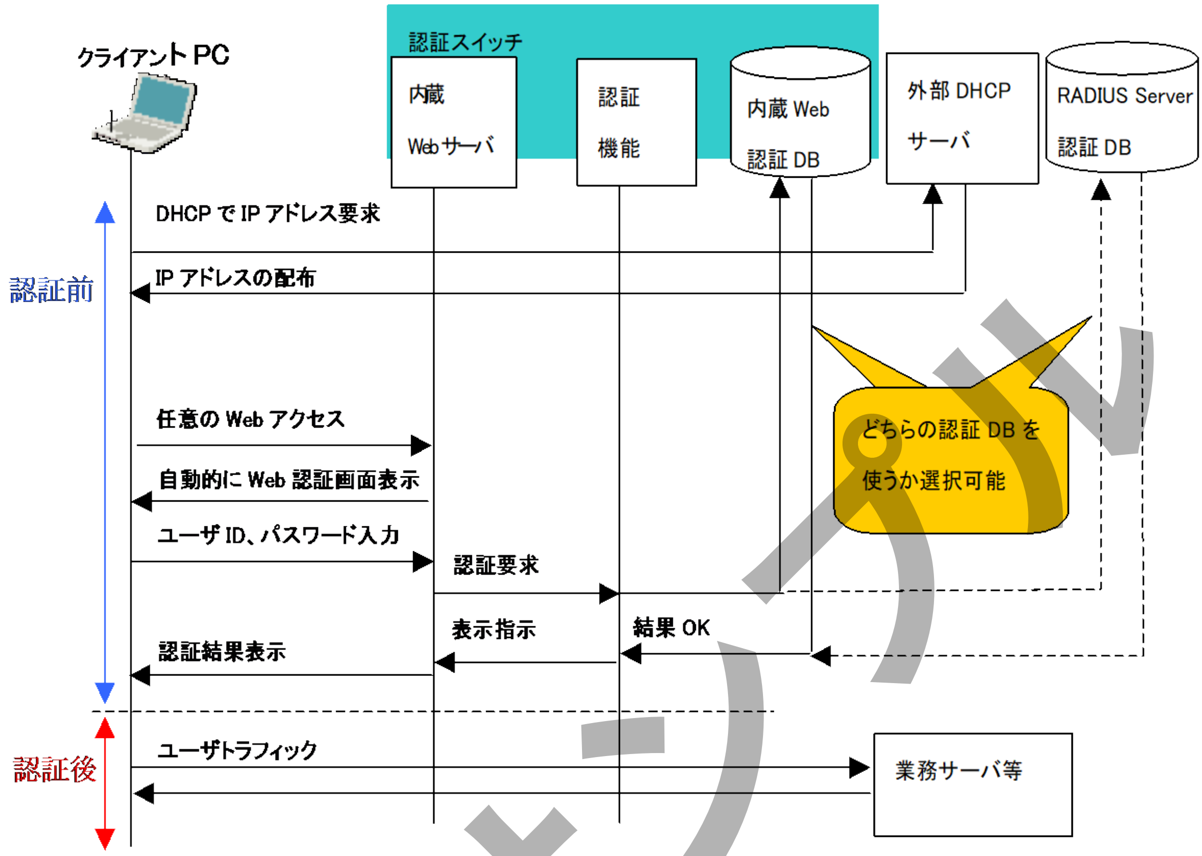

図 1.2-5　固定 VLAN モードにおける Web 認証シーケンス

固定 VLAN モードにおける Web 認証では、IP アドレスは固定および DHCP での配布どちらでも利用可能です。ただし DHCP で IP アドレスを配布する場合には、認証前の PC からの DHCP のトラフィックを許可する設定が必要です。

固定 VLAN では URL リダイレクト機能をサポートしており、認証前の PC から任意の Web アクセスがあった場合、認証画面を自動的に表示することができます。

1.2.3. MAC 認証

1.2.3.1. 概要

ネットワークに繋がる端末は、PC のみとは限りません。近年では PC 以外にプリンタや IP 電話機、ビデオカメラ等の端末もネットワークでの利用が前提となってきています。それらの端末についても、ネットワークの利用状況の管理や、通信する部分を制限するために、端末認証を行う必要があります。

上記の PC 以外の端末では、Web ブラウザや IEEE802.1X の Supplicant 機能を持たないものが多いため、端末から送信されるパケットの送信元 MAC アドレスを使ってユーザを認証する、MAC 認証があります。

しかし、一般的に MAC アドレスは偽装が簡単で、フラッディングしているパケットをキャプチャできると、容易に認証済み MAC アドレスを識別することができるため、認証としての強度は高いものではありません。使用するポートや VLAN、スイッチについて注意が必要となります。

1.2.3.2. MAC 認証シーケンス

以下に MAC 認証時の動作シーケンスを示します。

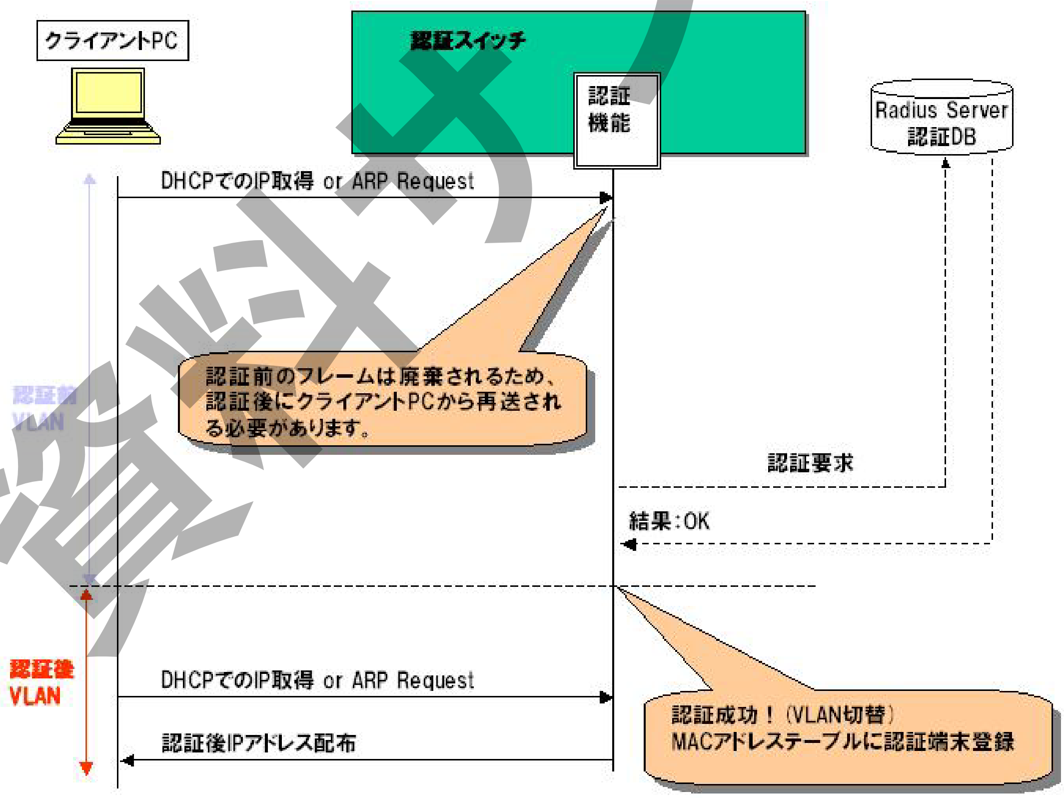

図 1.2-6 MAC 認証シーケンス

1.2.4. RADIUS (Remote Authentication Dial-In User Services)

1.2.4.1. RADIUS 概要

RADIUS(ラディウス)は、ネットワーク資源の利用可否の判断(認証)と、利用の記録(アカウンティング)のためのプロトコルです。その名の示すとおり、元来はダイヤルアップ接続のために開発された認証システムですが、現在はダイヤルアップのみならず、様々なサービスに対して認証とアカウンティングを実現するプロトコルとして幅広く利用されています。クライアントサーバモデルのプロトコルのため、サーバがクライアントに対してサービス停止を行うことは基本的にできません。

RADIUS の基本的な特性は以下のとおりです。

- 認証(Authentication)、承認(Authorization)、アカウンティング(Accounting)　即ち AAA モデルをサポートしています。
- Hop to Hop のセキュリティモデルを採用しています。(信頼関係を持つ AAA サーバ間では要求の転送によって承認を得ることができます。)
- UDP ベースのプロトコルであり、接続開始前にチャレンジ情報のやり取りを行います。
- PAP 認証、CHAP 認証をサポートしています。
- MD5 を利用したパスワード隠蔽の仕組みを備えています。
- 状態情報を持ちません。

RADIUS では認証基盤として自前のデータベースのみならず、外部の Active Directory ドメインサーバなどの LDAP に対応したディレクトリサーバや、NT サーバ、SQL サーバ等と連携することが可能です。これにより、ユーザの管理効率を大幅に向上させることも可能となります。

1.2.4.2.　RADIUS アトリビュート

RADIUS には属性値ペア(AVP: Attribute Value Pair)と呼ばれる登録情報があります。属性値ペアは、属性番号と長さ、属性からなり、属性番号ごとに属性値ペアの値の意味が規定されています。
AX が使用する主な属性名を以下に示します。

表 1.2-3　AX が使用する RADIUS アトリビュート

項番	属性名	Type 値	解説	パケットタイプ
1	User-Name	1	認証されるユーザ名。 MAC 認証の場合は認証端末の送信元 MAC アドレスになります。(小文字 ASCII, "-"区切り)	Request
2	NAS-IP-Address	4	認証要求をしているスイッチの IP アドレス。 AX2300S、AX2600S、AX2400S、AX3600S、AX6000S は、ローカルアドレスが設定されている場合はローカルアドレス、設定されていない場合は送信インタフェースの IP アドレスになります。 AX1200S,AX2200S,AX2500S は、VLAN ID の一番小さな VLAN インタフェースの IP アドレスになります。	Request
3	Service-Type	6	提供するサービスタイプ。Framed(2)固定。	Request Accept
4	Session-Timeout	27	IEEE802.1X 認証の場合は、Supplicant へ送信した EAP-Request に対する応答待ちタイムアウト値。 AX2300S、AX2600S、AX2400S、AX3600S、AX6000S は、項番 5 の Termination-Action が RADIUS-Request(1)に設定されていた場合、以下の値で再認証を行います。 0：再認証は無効 1～60：60 秒で再認証 61～65535：設定された値で再認証 AX1200S,AX2200S,AX2500S はこの属性を参照せず、コンフィグレーションに従います。 （6.1.6章参照）	Challenge Accept
5	Termination-Action	29	再認証時の動作指定。 AX2300S、AX2600S、AX2400S、AX3600S、AX6000S はこの属性が RADIUS-Request(1)に設定されていると、装置で再認証を設定していない場合でも強制的に再認証を行います。 AX1200S,AX2200S,AX2500S はこの属性を参照せず、コンフィグレーションに従います。 （6.1.6章参照）	Accept

項番	属性名	Type 値	解説	パケットタイプ
6	Called-Station-Id	30	スイッチの MAC アドレス(小文字 ASCII、"-"区切り)。AX1230S では未サポート。	Request
7	Calling-Station-Id	31	認証端末の MAC アドレス(小文字 ASCII、"-"区切り)。	Request
8	NAS-Identifier	32	Web認証・MAC認証の場合 固定VLAN モード時に認証端末を収容しているVLAN ID を数字文字列で応答します。 例：VLAN ID 100 の場合 100 ダイナミックVLAN モードおよびIEEE802.1X認証では，コンフィグレーションコマンドhostname で指定された装置名を応答します。	Request
9	NAS-Port-Type	61	スイッチがユーザ認証に使用している物理ポートのタイプ。 IEEE802.1X 認証では Ethernet(15)固定。 Web 認証および MAC 認証では Virtual(5)固定。	Request
10	Tunnel-Type	64	トンネル・タイプ。 動的 VLAN モードでのみ意味を持ちます。 VLAN(13)固定。	Accept
11	Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル。 動的 VLAN モードでのみ意味を持ちます。 IEEE802(6)固定。	Accept
12	Tunnel-Private-Group-ID	81	VLAN を識別する文字列。 動的 VLAN モードでのみ意味を持ちます。 Accept 時は、認証済みの端末に割り当てるVLAN ID になります。 次に示す文字列が対応します。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 (3)"VLAN 名称による割り当て 文字列にスペースを含んではいけません（含めた場合 VLAN 割り当ては失敗します)。 （設定例） VLAN10 の場合 (1)の場合　"10" (2)の場合　"VLAN10" (3)の場合は VLAN に名称を設定することでVLAN 名による VLAN 配布が可能です、たとえば 2 台のスイッチにおいて同一ユーザで所属させたい VLAN 番号が異なる環境でも名称を一致させることで運用可能です。	Accept
13	NAS-Port-Id	87	IEEE802.1X 認証でのみセットされます Supplicant を認証する Authenticator のポートを識別するための文字列。 ポート単位認証："Port x/y" 　固定 VLAN 認証："VLAN x" 　動的 VLAN 認証："DVLAN x" 　（x、y には数字が入る） ただし AX1230S では入りません	Request

1.2.5. CA(Certificate Authority)

CA とは電子的な身分証明書を発行・管理する機関のことであり、認証局、CA 局または CA センターなどと呼ばれています。CA にはパブリック CA とプライベート CA があり、前者は第三者が発行する証明書によりサーバおよび本人性を証明します。後者は企業内などに閉じた範囲で、企業ポリシーに基づいて運用されます。

CA ではユーザの公開鍵の管理や電子証明書を発行し、証明書は、発行者(CA)のみが知る秘密鍵で暗号化された電子署名、ユーザ識別子、ユーザ公開鍵、証明書有効期限等で構成されています。

証明書の発行に関しては、適用する端末認証方式によって差異があります。即ち EAP-TLS ではサーバ証明書およびクライアント証明書の双方をやり取りする必要がありますが、EAP-PEAP、EAP-TTLS ではクライアント証明書は必要ありません。

1) パブリック CA

 外部機関に委託することになるため、信頼性が高く、保守や運用の面でメリットがありますが、証明書の発行にコストが必要となります。特に EAP-TLS を採用する場合はクライアント数分の証明書発行コストがかかることになります。

 また、Web 認証にて HTTPS を行う場合でも、証明書を機器台数分用意することになります。

2) プライベート CA

 パブリック CA とは逆に、証明書の発行コストはかかりませんが、自営システムのため構築・運用・保守のコストがかかります。また、ローカルな証明書になるため、Web 認証で IE を使用した場合は、以下の警告が表示されます。

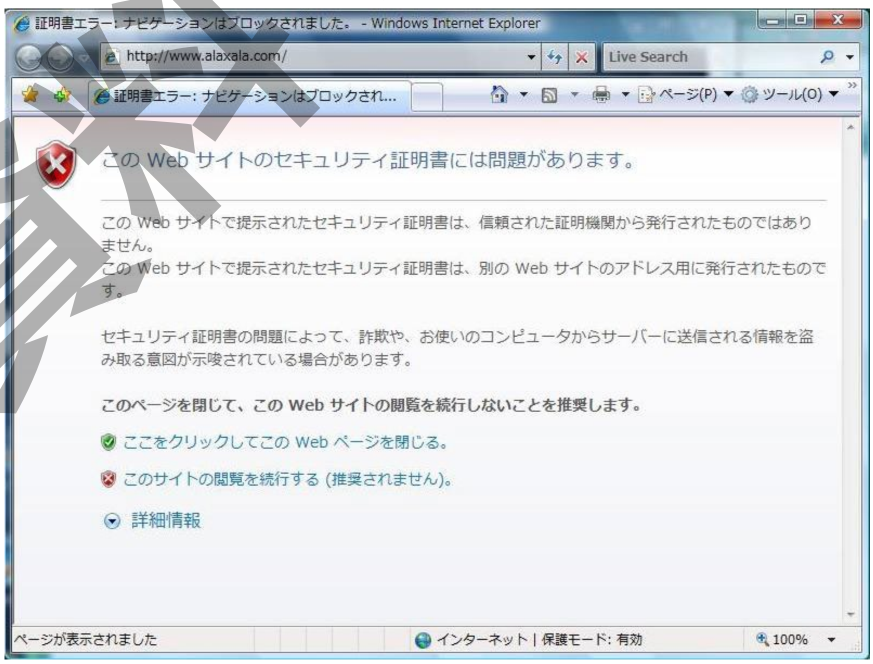

図 1.2-7 Windows の Internet Explorer（IE7 以降 IE8,IE9,IE10）セキュリティ警告画面

AX シリーズでは Web 認証にて https を使用したセキュア認証を実現するため工場出荷時にプライベートの CA から発行されたサーバ証明書がインストールされています。Web 認証で https で認証した場合には証明書エラーが表示されます。回避手段は注意事項**6.2.10**を参照してください。

気になる続きは…

・アラクサラ　インテグレータ会員

または

・ビジネスパートナー様会員

にご登録いただければ、全てをご覧いただけます！

アラクサラ インテグレータ会員またはビジネスパートナー様会員へ登録することで、アラクサラ製品のご利用にあたり役立つ各種資料(システム構築ガイドなど)を全て閲覧することができます。ぜひこの機会にご登録下さい。

アラクサラネットワークス株式会社

〒212-0058
川崎市幸区鹿島田１丁目１番２号 新川崎ツインタワー西棟
https://www.alaxala.com/jp/