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
（マルチステップ認証編）

第 4 版

資料 No. NTS-09-R-010

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（AX1240S/AX1250S/AX2230S および AX2530S）でサポートしている端末認証とユーザ認証を２段階で実施するマルチステップ認証機能を用いた認証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、安全・安心な認証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。

関連資料

・AX シリーズ認証ソリューションガイド
・RADIUS サーバ設定ガイド Windows Server 2008 編
・AX シリーズ製品マニュアル（http://www.alaxala.com/jp/techinfo/manual/index.html）

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。

AX1240S /AX1250S/AX2230S	Ver2.4.A
AX2230S	Ver2.4.A
AX2530S	Ver3.5

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。
・イーサネット、Ethernetは、富士ゼロックス（株）の商品名称です。
・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。
・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

- AX1240S /AX1250S(Ver2.4.A)
- AX2230S(Ver2.4A)
- AX2530S (Ver3.5)
- AX3630S (Ver11.11)
- Windows XP SP3

- Windows Vista SP2
- Windows 7 SP1
- Windows 8
- Windows Server 2008 Standard

改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	―	2009.5.22.	初版発行	―
第 2 版	―	2010.1.18.	使用機器一覧を更新	はじめに
			マルチステップ認証の認証機能の組み合わせを追加 マルチステップ認証基本動作概要の説明を更新	1.1
			第一ステップの認証機能に MAC 認証または IEEE802.1X 認証の選択が可能を追加	1.2
			端末認証追加オプション：dot1x を追加	1.3.1
			認証成功メッセージの RADIUS 属性 Filter-Id と第二ステップで認証必須となる認証機能を更新	1.3.2
			マルチステップ認証ポートでの各認証機能(端末認証追加オプション(dot1x)設定時)を追加	1.4
			マルチステップ認証のシステム構築（固定 VLAN 構成）に IEEE802.1X 認証＋Web 認証を行う C 部署(VLAN300)を追加	3. 3.3.1 3.4.1 3.5
			マルチステップ認証のシステム構築（動的 VLAN 構成）に IEEE802.1X 認証＋Web 認証を行う B 部署(VLAN300)を追加	4. 4.3.1 4.4.1 4.5
			端末認証追加オプション設定した場合の show authenticationmulti-step コマンドの表示例を追加	5.
			端末認証追加オプション(dot1x)設定時の端末移動に関する注意事項を追加	6.5
			構成例のコンフィグレーションに変更	付録 A.
第 3 版	―	2011.1.7	使用機器一覧に AX2530S を追加し使用機器 Ver を更新	はじめに
			AX2530S へのマルチステップ認証のサポートに伴い AX1240S 特有の機能の記述を削除	1
			AX2530S の収容条件を追加	2.1
			固定 VLAN のマルチステップ認証の構築例に AX2530S を追加	3
			動的 VLAN のマルチステップ認証の構築例に AX2530S を追加	4
			AX2530S のコンフィグレーションを追加	付録 A
第 4 版	―	2013.6.28	使用機器一覧に AX2230S を追加し使用機器 Ver を更新	はじめに
			AX2500S の Filter-ID の設定値に/形式の設定について追加	1.3.2
			RADIUS サーバの設定(ダイナミック ACL/QoS 併用時)を追加	1.3.3

			収容条件に AX2230S を追加	2.1
			・AX2230S に関して AX1240S の設定を参照するように追加 ・AX2530S の Filter-ID の設定値に/形式の設定を追加	3 章、4 章

目次

1. マルチステップ認証概要 8

1.1 マルチステップ認証とは 8
1.2 AX シリーズのマルチステップ認証の特徴 11
1.3 AX がサポートするマルチステップ認証 12
1.3.1 認証スイッチの設定 12
1.3.2 RADIUS サーバの設定 14
1.3.3 RADIUS サーバの設定(ダイナミック ACL/QoS 併用時) 15
1.4 マルチステップ認証の各認証機能 16
1.4.1 認証端末の管理と認証解除条件 18

2. AX シリーズの収容条件 19

2.1 収容条件 19

3. マルチステップ認証のシステム構築（固定 VLAN 構成） 20

3.1 概要 20
3.2 マルチステップ認証ネットワーク構成図 21
3.3 構築ポイント 24
3.3.1 AX に関する構築ポイント 24
3.4 AX の設定 26
3.4.1 AX1240S のコンフィグレーション 26
3.4.2 AX2530S のコンフィグレーション 29
3.5 RADIUS サーバの設定 33
3.5.1 ネットワークポリシーの設定 33

4. マルチステップ認証のシステム構築（動的 VLAN 構成） 38

4.1 概要 38
4.2 マルチステップ認証ネットワーク構成図 39
4.3 構築ポイント 42
4.3.1 AX に関する構築ポイント 42
4.4 AX の設定 45
4.4.1 AX1240S のコンフィグレーション 45
4.4.2 AX2530S のコンフィグレーション 49
4.5 RADIUS サーバの設定 53
4.5.1 ネットワークポリシーの設定 53

5. 動作確認 58

5.1 AX シリーズの運用コマンド 58
5.1.1 show authentication multi-step 58

5.1.2 show authentication logging 59
5.1.3 clear dot1x auth-state 59
5.1.4 clear web-authentication auth-state 59
5.1.5 clear mac-authentication auth-state 59

6. 注意事項 60

6.1 マルチステップ認証ポートでのシングル認証に関する注意事項 60
6.2 ユーザ認証許可オプション(permissive)と MAC 認証の設定の注意事項 60
6.2.1 認証対象 MAC アドレスの制限 60
6.2.2 認証再開猶予タイマ 60
6.3 DHCP 使用時の注意事項 60
6.3.1 Native VLAN で IP アドレスを配布しないシステムでの注意事項 60
6.4 ダブルログインによる Web 認証の失敗 60
6.5 端末認証追加オプション(dot1x)設定時の端末移動について 61

7. トラブルシューティング 62

7.1 マルチステップ認証を実行せずシングル認証になる 62
7.2 動的 VLAN モード使用時、認証後 VLAN に移動しない 63

付録 A. コンフィグレーション 64

1. マルチステップ認証概要

1.1 マルチステップ認証とは

従来のシングル認証システムでは、端末認証またはユーザ認証のいずれかひとつ認証が成功すればシステムを利用することができました。そのため、以下のような弱点がありました。

図 1.1-1 シングル認証の弱点

マルチステップ認証では、端末認証とユーザ認証を 2 段階で実施するため、より安全なシステムを構築することが可能となります。

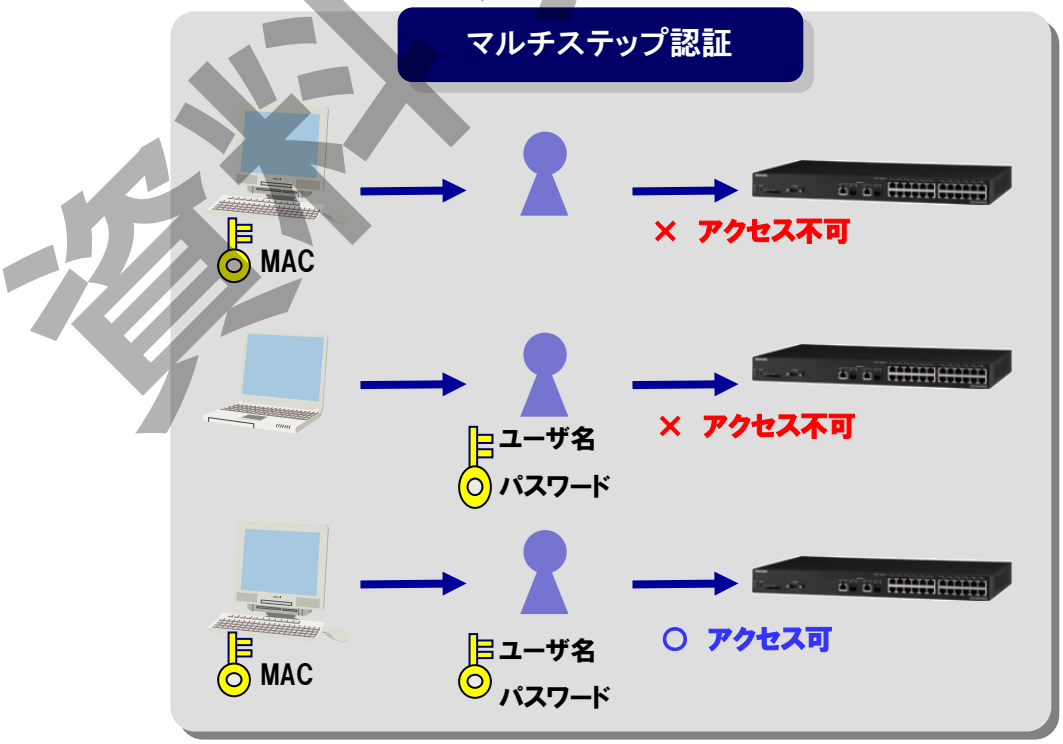


図 1.1-2 マルチステップ認証

AX シリーズでサポートするマルチステップ認証の認証機能の組み合わせは下表となります。

表1.1-1 マルチステップ認証の認証機能の組み合わせ

項番	端末認証（第一ステップ）	ユーザ認証（第二ステップ）
1	MAC 認証	Web 認証
2	MAC 認証	IEEE802.1X 認証
3	IEEE802.1X 認証	Web 認証

以下にマルチステップ認証基本動作概要を示します。

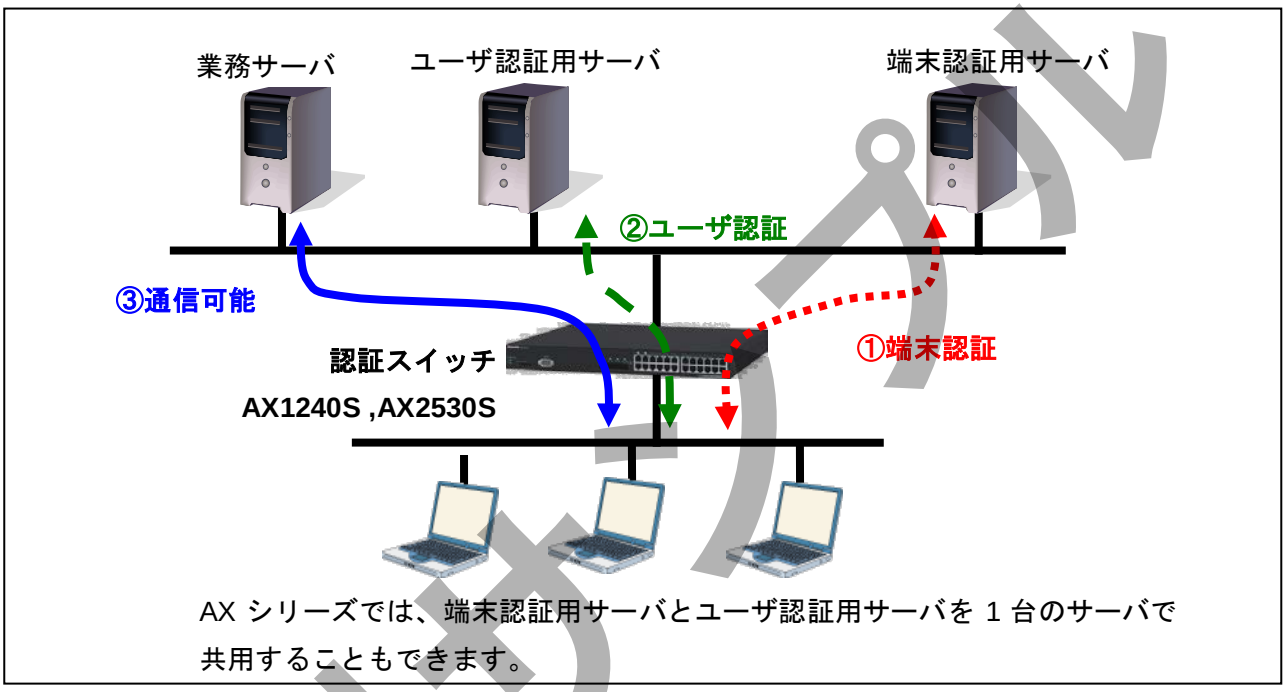


図 1.1-3 マルチステップ認証基本動作概要

① ユーザが端末を起動すると、認証スイッチはユーザのオペレーションなしで端末から送信される任意のパケットまたは、認証開始パケットを検出し認証要求を端末認証用サーバに送信し、端末認証を行います。【第一ステップ】

② ユーザが端末からユーザ認証情報(*1)を送信すると、認証スイッチは端末認証に成功していた場合、端末からのユーザ認証情報をユーザ認証用サーバに送信しユーザ認証を行います。
端末認証に失敗していた場合は、ユーザ認証情報を廃棄します。 【第二ステップ】

③ ユーザ認証に成功した端末は業務サーバとの通信が可能となります。

（*1）：ユーザ ID,パスワードまたは証明書

AX シリーズでは、端末認証はユーザが意識することなく実施(*2)されるため、ユーザ認証のみ実施していたシステムからマルチステップ認証のシステムに拡張する場合、ネットワーク側(認証スイッチ,RADIUS サーバ)の設定変更のみで実現でき、ユーザの端末操作に変更はありません。

(*2)：端末認証を IEEE802.1X 認証とした場合、認証アルゴリズムは証明書を使用する EAP-TLS を推奨します。

AX シリーズのマルチステップ認証は、ポート単位に設定します。また、マルチステップ認証回線でもユーザ認証の必要ないプリンタなどの機器に対しては端末認証のみで認証を許可、ゲストに対してはユーザ認証成功で認証を許可すると共にアクセス範囲を限定(例えば、インターネットのみアクセス可)する設定ができるなど柔軟なシステム構築が可能です。マルチステップ認証システム概要を以下に示します。

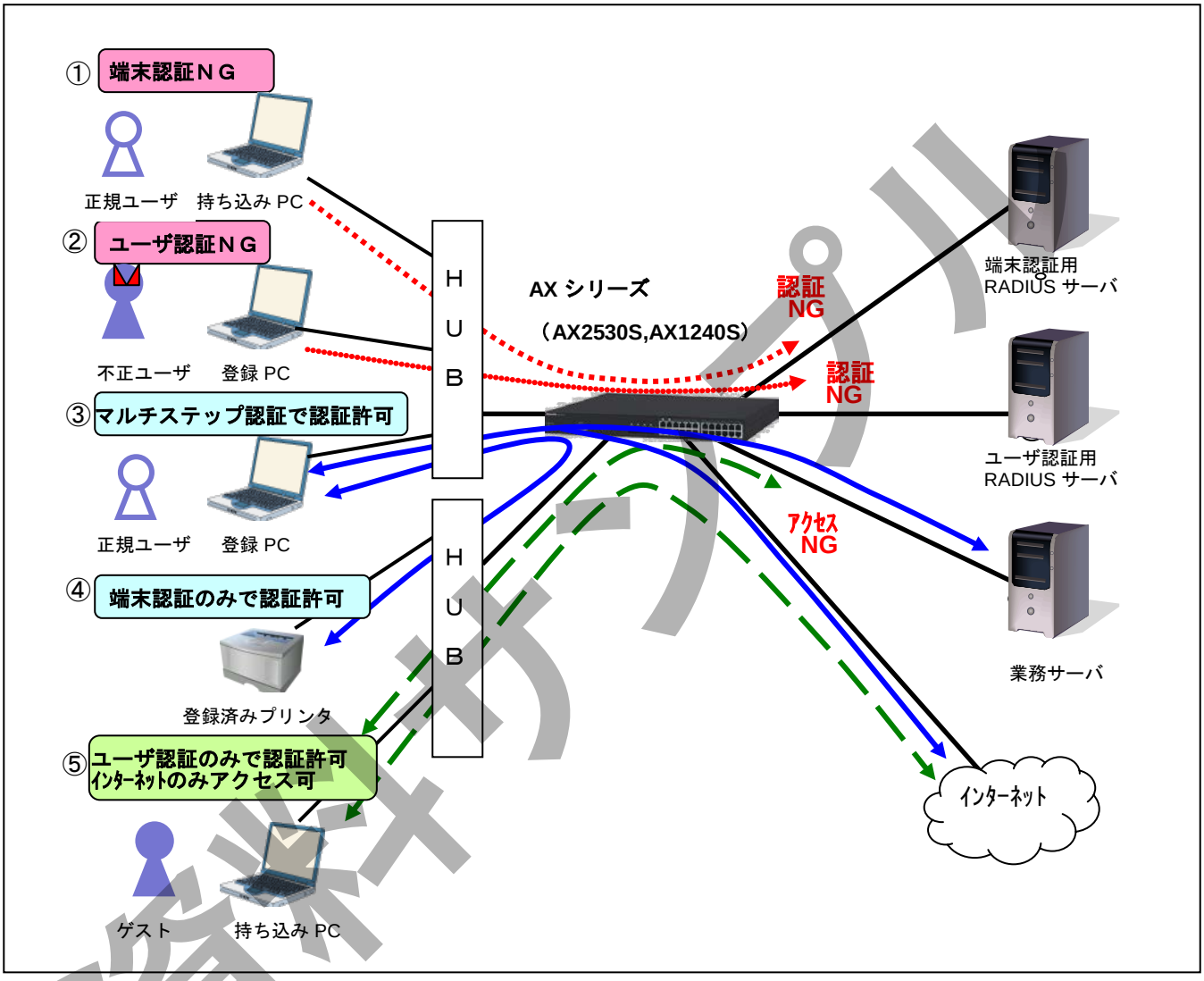


図 1.1-4 マルチステップ認証システム概要

表1.1-2 マルチステップ認証システム概要でのアクセス可否

項番	端末種別	ユーザ種別	アクセス 可否	
			業務サーバ	ｲﾝﾀｰﾈｯﾄ
①	持ち込み PC	正規ユーザ	×	×
②	登録 PC	不正ユーザ	×	×
③	登録 PC	正規ユーザ	○	○
④	登録済みプリンタ	―	○	×
⑤	持ち込み PC	ゲスト	×	○

（凡例）○：アクセス可
×：アクセス不可

1.2 AX シリーズのマルチステップ認証の特徴

AX シリーズのマルチステップ認証の特徴を以下に示します。

（1） 島 HUB 接続でも、ユーザ毎のセキュリティ管理が可能

マルチステップ認証回線でも従来通り IEEE802.1X 認証端末、Web 認証端末および MAC 認証端末を同一ポートで混在できます。これにより島 HUB(＊)経由で複数の認証端末を収容できるためシステム内の認証スイッチの設定台数を抑えることができ、導入コストおよび運用コストが低減され、またレイアウトも柔軟に対応することができます。

＊：IEEE802.1X 認証を島 HUB 経由で行う場合、EAP フレーム透過機能を持った HUB を使用する必要があります。

（2） マルチステップ認証回線でもシングル認証で許可する機能を提供

ユーザ認証許可オプション(permissive)を設定することで、同一ポートでマルチステップ認証を行う正規ユーザ端末とユーザ認証のみ行うゲスト端末との混在が可能です。また、プリンタなど MAC 認証のみ行う機器に対してはシングル認証で認証が可能です。

（3） 固定 VLAN モードと動的 VLAN モードの両方式を提供

固定 VLAN モードと動的 VLAN モードの両方をサポートしています。

各方式の適用

・固定 VLAN モード：既存システムの VLAN 構成を変更することなく認証システムの構築ができます。また、固定 IP 環境で利用可能です。
例えばフロア毎にアクセス制御が異なる環境下で有効な方式です。

・動的 VLAN モード：ユーザ毎に個別に VLAN の設定が可能で、所属する VLAN 毎にサーバへのアクセス許可・遮断設定ができます。
例えばアクセス権限の違うユーザが混在する環境下で有効な方式です。

これによりユーザニーズに合わせた認証システムを柔軟に構築することができます。

（4） 第一ステップの認証機能に MAC 認証または IEEE802.1X 認証の選択が可能

第一ステップの認証機能として従来からサポートしている MAC 認証の他に、証明書を使用し強固なセキュリティを実現できる IEEE802.1X 認証をサポートしました。第一ステップの認証機能に IEEE802.1X 認証を行うかはポート毎に選択することができます。

なお、第一ステップの認証機能を IEEE802.1X 認証とした場合、第二ステップの認証機能は Web 認証となります。

1.3 AX がサポートするマルチステップ認証

マルチステップ認証が動作する認証モードを下表に示します。

表1.3-1 マルチステップ認証が動作する認証モード

項番	マルチステップ認証機能	認証方式	認証モード
1	MAC 認証＋IEEE802.1X 認証	RADIUS 認証	固定 VLAN モード 動的 VLAN モード
2	MAC 認証＋Web 認証	RADIUS 認証	固定 VLAN モード 動的 VLAN モード
3	IEEE802.1X 認証＋Web 認証	RADIUS 認証	固定 VLAN モード 動的 VLAN モード

装置に内蔵した認証用 DB を使用するローカル認証方式では使用できません。また、レガシーモードは使用できません。

1.3.1 認証スイッチの設定

マルチステップ認証を行うために認証スイッチに設定する項目を以下に示します。

（１）マルチステップ認証　　：Authentication multi-step

【説明】マルチステップ認証を行うポートに対し設定します。

（２）ユーザ認証許可オプション：permissive

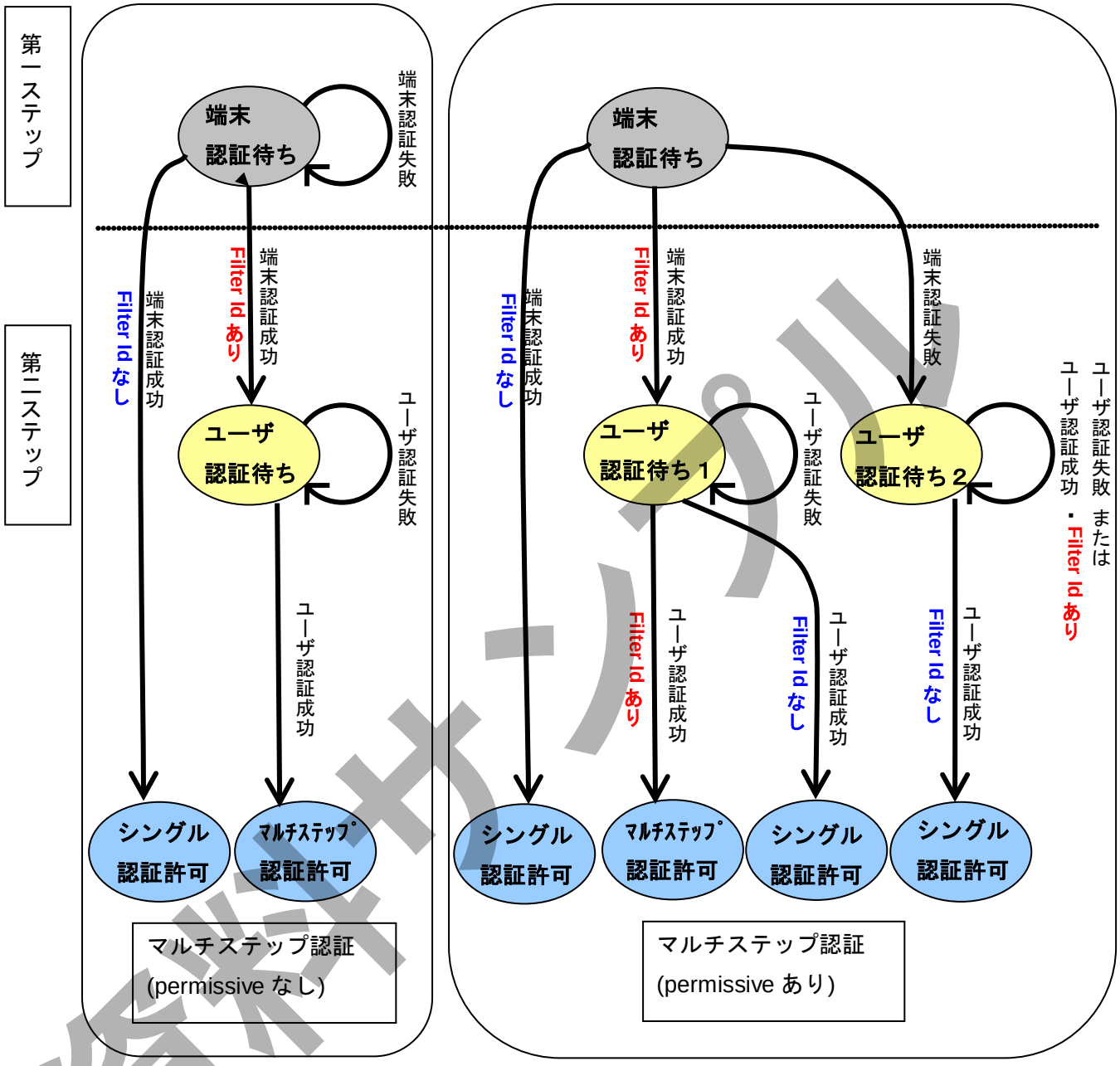
【説明】マルチステップを行うユーザとゲストユーザ(ユーザ認証のみ)が同一ポートに混在する環境で使用します。本オプションを設定すると、端末認証に失敗しても Web 認証入力画面が表示されます。

（３）端末認証追加オプション：dot1x

【説明】第一ステップの認証に IEEE802.1X 認証を使用するポートに設定します。、
但し、ユーザ認証許可オプション(permissive)と端末認証追加オプション(dot1x)は同一ポートに設定することはできません。

その他の設定は各認証機能を使う場合の設定と同じです。

マルチステップ認証回線では、第一ステップとして端末認証を実施します。ユーザ認証許可オプション(permissive)を設定すると端末認証を失敗後、ユーザ認証成功のみでアクセスを許可することができます。Permissive 設定の有無による動作の違いを下図に示します。



（凡例）

：状態　→：発生したイベントおよび条件と遷移先状態の方向

Filter Id については、次項を参照して下さい。

図 1.3-1 マルチステップ認証 permissive 設定による動作の違い

1.3.2 RADIUS サーバの設定

認証スイッチは、マルチステップ認証で必須とする認証機能を RADIUS サーバからの認証成功(Accept)メッセージ内の RADIUS 属性 Filter-Id の文字列で判断します。

RADIUS サーバに設定する RADIUS 属性 Filter-Id の文字列とその結果、認証必須となる認証機能を下表に示します。マルチステップ認証で使用する認証機能に対応する文字列を RADIUS サーバに設定して下さい。

表 1.3-2 認証成功メッセージの RADIUS 属性 Filter-Id と第二ステップで認証必須となる認証機能

項番	RADIUS 属性 Filter-Id の文字列	認証成功メッセージに文字列が入る認証機能	第二ステップで認証必須となる認証機能
1	@@1X-Auth@@ /1X-Auth(*2)	MAC 認証	IEEE802.1X 認証
2	@@Web-Auth@@ /Web-Auth(*2)	MAC 認証，IEEE802.1X 認証	Web 認証
3	@@MultiStep@@ /MultiStep(*2)	MAC 認証，IEEE802.1X 認証	IEEE802.1X 認証(*1)または Web 認証どちらでもよい。

（＊１）: 端末認証追加オプション(dot1x)設定時、第二ステップで行う認証機能は Web 認証のみです。

（＊２）: /形式は AX2500S（Ver3.5）以降のみ指定可能です、ダイナミック ACL/QoS の”/Cass=1～63””指定と併用する場合は必ず/形式としてください。

表 1.3-3 認証成功メッセージの RADIUS 属性 Filter-Id と第一ステップで認証必須となる認証機能

項番	RADIUS 属性 Filter-Id の文字列	認証成功メッセージに文字列が入る認証機能	第一ステップで認証必須となる認証機能
1	@@MAC-Auth@@ /MAC-Auth(*2)	IEEE802.1X 認証，Web 認証 (*1)	MAC 認証

（＊１）: permissive 指定時のユーザ認証側（第 2 段階側）に設定します
permissive 指定時は端末認証側に Filter-ID 指定が無いと MAC 認証でシングル認証許可となります。

（＊２）: /形式は AX2500S（Ver3.5）以降のみ指定可能です、ダイナミック ACL/QoS の”/Cass=1～63””指定と併用する場合は必ず/形式としてください。

1.3.3 RADIUS サーバの設定(ダイナミック ACL/QoS 併用時)

AX2500S Ver3.5 以降でマルチステップ認証とダイナミック ACL/QoS を Filter-ID に併用で設定する場合は、RADIUS サーバの追加アトリビュートの Filter-ID の設定値は表 1.3-2、表 1.3-3に示すように、/形式で指定してください。

ダイナミック ACL/QoS では最終段階の認証が成功した場合にダイナミック ACL のクラス情報を反映します。ダイナミック ACL/QoS を使用する場合は最終段階の認証でクラス情報の配布を行ってください。

たとえば MAC 認証＋Web 認証のマルチステップの場合 2 段階目の Web 認証が終了する前は認証前 ACL が適用され、認証前 ACL ではダイナミック ACL は使用できませんので注意してください。

マルチステップ認証で､ゲスト端末も許可する場合に使用する permissive モードでは 2 段階目においてマルチステップ認証の Filter-ID 指定を行いますので、ダイナミック ACL/Qos と併用する場合においては Filter-ID にマルチステップの指定と Class の指定の両方を併記する必要があります。併記する場合には Radius サーバの追加アトリビュートの Filter-ID に**/MAC-Auth/Class=クラス番号**と指定します。

①マルチステップ permissive モード無し（ゲスト端末無しの環境）所属クラス 20 のユーザの場合

1 段階端末認証のアトリビュート

Filter-ID(11)=/Multistep

2 段階 ユーザ認証のアトリビュート

Filter-ID(11)=/Class=20

②マルチステップ permissive モード（ゲスト端末ありの場合）で社員はクラス２０でゲストはクラス１のとしたい場合

1 段階目の端末認証で登録端末のアトリビュート

Filter-ID(11)=/MultiStep

2 段階目ユーザ認証においてマルチステップ対象のユーザの場合。

Filter-ID(11)=/MAC-Auth/Class=20

2 段階目の認証でゲストユーザで Class 指定のみ配布した意場合。

Filter-ID(11)=/Class=1

マルチステップとの併用するために、RADIUS の Filter-ID の設定について、AX2500S では、/形式の指定が追加になっています。 ダイナミック ACL/QoS の設定に関しては、AX シリーズ認証ソリューションガイド（12 版）以降を参照ください。

1.4 マルチステップ認証の各認証機能

認証スイッチと RADIUS サーバの設定の組み合わせにより、マルチステップ認証の動作が変わります。ユーザ認証許可オプションの有無および RADIUS 属性 Filter-Id の設定毎の各認証機能について**表 1.4-1** に示します。また、端末認証追加オプション(dot1x)設定時の RADIUS 属性 Filter-Id の設定毎の確認認証機能について**表 1.4-2**に示します。

※ **表 1.4-1**,**表 1.4-2**では、Filter-ID に指定する文字列の値を@@形式の例で表現していますが、AX2500S の場合は/形式でも指定できます。

表1.4-1 マルチステップ認証ポートでの各認証機能

項番	コンフィグレーション		端末認証		ユーザ認証		
	マルチステップ認証設定	ユーザ認証許可オプション設定(permissive)	RADIUS 属性 Filter-Id(*1)	MAC 認証	RADIUS 属性 Filter-Id(*1)	IEEE802.1X 認証	Web 認証
1	設定有	設定無	設定無	○	―	―	―
2			@@1X-Auth@@	△	―	◎	―
3			@@Web-Auth@@			―	◎
4			@@MultiStep@@			◎	◎
5		設定有(permissive)	設定無	○	―	―	―
6			―	×	設定無	○	○
7			@@1X-Auth@@	△	設定無	○	―
8			@@Web-Auth@@	△		―	○
9			@@MultiStep@@	△		○	○
10			@@1X-Auth@@	△	@@MAC-Auth@@	◎	―
11			@@Web-Auth@@	△		―	◎
12			@@MultiStep@@	△		◎	◎
13			―	×	@@MAC-Auth@@	▲	▲
14	設定無	―	―	○	―	○	○

(凡例) ◎：端末認証とユーザ認証で許可
○：シングル認証で許可
△ ：端末認証成功でユーザ認証結果待ち(この間通信不可)
▲：ユーザ認証成功だが端末認証失敗の為、認証許可しない
×：認証失敗
―：対象外

＊1：表 1.4-1に記載されていない文字列が設定された場合、Fliter-Id は設定していないのと同様の動作となります。

例とし同一ポートで表 1.4-1の項番 6(ユーザ認証のみで認証成功とするゲスト端末)と項番 12(マルチステップ認証で認証成功とする正規ユーザ端末)を混在させる場合の設定を以下に示します。

認証スイッチ：
・マルチステップ認証(authentication multi-step)を設定
・ユーザ認証許可オプション(permissive)を設定

端末認証用 RADIUS サーバ：
・正規ユーザ端末に対する Fiter-Id に「@@MultiStep@@」と設定

ユーザ認証用 RADIUS サーバ：
・正規ユーザ情報に対する Fiter-Id に「@@MAC-Auth@@」と設定
・ゲストユーザ情報に対しては Fiter-Id を設定しない。

表1.4-2 マルチステップ認証ポートでの各認証機能（端末認証追加オプション(dot1x)設定時）

項番	コンフィグレーション		端末認証 (*1)		ユーザ認証	
	マルチステップ認証設定	端末認証追加オプション設定(dot1x)	RADIUS 属性 Filter-Id(*2)	IEEE 802.1X 認証	RADIUS 属性 Filter-Id(*1)	Web 認証
1	設定有	設定有(dot1x)	設定無	○	ー	ー
2			@@MAC-Auth@@	○	ー	ー
3			@@1X-Auth@@	○	ー	ー
4			@@Web-Auth@@	△		◎
5			@@MultiStep@@	△		◎

(凡例) ◎：端末認証とユーザ認証で許可
○：シングル認証で許可
△：端末認証成功でユーザ認証結果待ち(この間通信不可)
ー：対象外

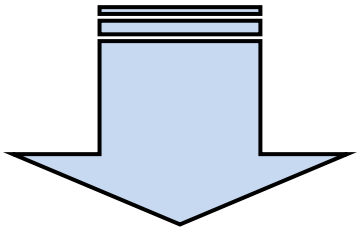
＊１：端末認証追加オプション設定ポートで、第一ステップの認証(端末認証)で MAC 認証を実施する場合は表 1.4-1の項番１～４と同様の動作になります。

＊２：表 1.4-2に記載されていない文字列が設定された場合、Fliter-Id は設定していないのと同様の動作となります。

1.4.1 認証端末の管理と認証解除条件

認証後の端末は、最後に認証した認証機能で管理します。各認証機能の認証解除(ログアウト)条件については、「ソフトウェアマニュアル コンフィグレーションガイド Vol.2」を参照して下さい。

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
川崎市幸区鹿島田一丁目１番２号 新川崎三井ビル西棟
http://www.alaxala.com/