

AX シリーズ ネットワーク・パーティション ソリューションガイド [認証編]

for
the
Guaranteed
Network

資料

第 2 版

はじめに

AX シリーズ ネットワーク・パーティション ソリューションガイド[認証編]は、アラクサラネットワークス社 AX シリーズ AX6700S,AX6600S,AX6300S でサポートしているネットワーク・パーティションと、同 AX シリーズ AX3600S,AX2400S,AX1200S シリーズでサポートしているネットワーク認証機能を組み合わせたシステム構築のための基本的な技術情報をシステムエンジニアの方へ提供し、ネットワーク・パーティションによる各論理ネットワークをネットワーク認証により安全・安心に利用できるシステムの構築とその安定稼働を目的として書かれています。

関連資料

- AX シリーズ ネットワーク・パーティション ソリューションガイド [基本編]
- AX シリーズ ネットワーク・パーティション ソリューションガイド [応用編]
- AX シリーズ 認証ソリューションガイド
- 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 RADIUS サーバ設定ガイド
- AXシリーズ製品マニュアル(<http://www.alaxala.com/jp/techinfo/manual/index.html>)

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて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。

本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX6700S, AX6600S, AX6300S	Ver11.3 (OP-NPAR ライセンス有)
AX3600S, AX2400S	Ver11.2.A
AX1240S	Ver2.2

本資料の内容は、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

本資料を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

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商標登録です。
- Ethernetは、米国Xerox Corp.の商品名称です。
- イーサネットは、富士ゼロックス(株)の商品名称です。
- 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。

改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	—	2009.3.26	初版発行	—
第2版	—	2010.2.19	<p>VRF対応装置にAX6600S追加、認証スイッチをAX1240Sに変更 AX6700S, AX6600S, AX6300S (Ver11. 3対応) および AX1240S (Ver2. 2対応)</p> <p>2章 使用できる認証機能とシステム設計のポイント RADIUSサーバグループ選択機能により複数パーティション を1台に収容した構成を追加 DHCPリレーエージェント機能のエクストラネット対応紹介</p> <p>3章 パーティション個別認証システムの構築例 RADIUSサーバグループ選択機能を利用したネットワーク 構成例を追加(構築のポイント、コンフィグ例など)</p> <p>4章 複数パーティション統合認証システムの構築例 RADIUSおよび認証後DHCPをひとつのサーバに統合し、 認証前DHCPをサーバ側アクセススイッチとしたシステムに 変更</p> <p>5章 注意事項 RADIUSサーバグループ選択機能により、RADIUSとの組み 合わせの条件が緩和される旨を記載</p>	<p>はじめに</p> <p>2. 2. 1</p> <p>2. 2. 2 (2)</p> <p>3. 4, 3. 5</p> <p>4. 1, 4. 2, 4. 3</p> <p>(2)</p>

目次

1. ネットワーク・パーティションと認証.....	5
1.1 ネットワーク・パーティションと認証機能のコラボレーション.....	5
1.2 各機能の分担について.....	6
2. 使用できる認証機能とシステム設計のポイント.....	7
2.1 AXシリーズの認証機能について.....	7
2.2 ネットワークに対する認証スイッチとその他サーバの配置.....	8
3. パーティション個別認証システムの構築例.....	12
3.1 認証スイッチをパーティション毎に置く構成の例.....	12
3.2 認証スイッチをパーティション毎に置く構成での設定ポイント.....	15
3.3 コンフィグレーション例.....	16
3.4 RADIUSサーバグループ選択機能を利用したネットワーク構成.....	22
3.5 RADIUSサーバグループ選択機能を使ったシステムの設定ポイント.....	25
3.6 コンフィグレーション例.....	26
4. 複数パーティション統合認証システムの構築例.....	29
4.1 ネットワーク構成図.....	29
4.2 設定のポイント.....	32
4.3 コンフィグレーション例.....	34
5. 注意事項.....	43
付録： コンフィグレーションファイル.....	44

1. ネットワーク・パーティションと認証

1.1 ネットワーク・パーティションと認証機能のコラボレーション

ネットワーク・パーティションとは「AX シリーズ ネットワーク・パーティション ソリューションガイド[基本編]」で紹介の通り、最小限の物理構成で論理的に独立した複数のネットワークシステムを収容できるシステムソリューションです。その特長の一つとして、論理的に分割された複数ネットワーク間相互で高いセキュリティを提供します。

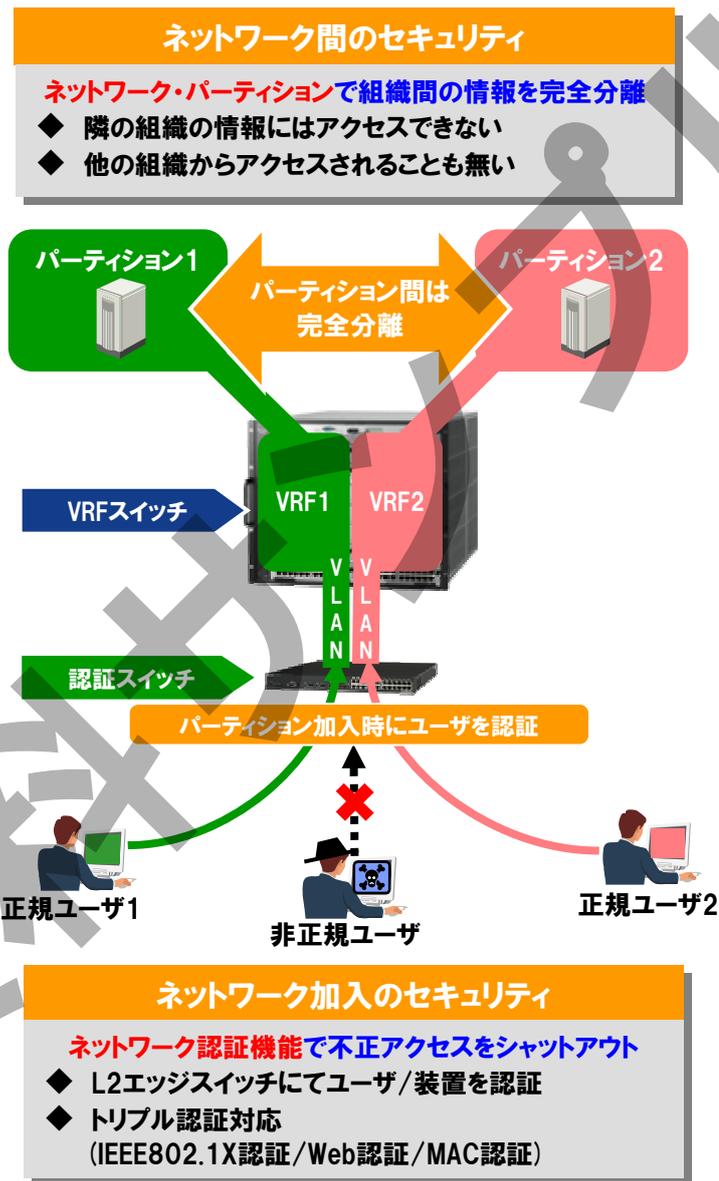


図 1.1-1 パーティション+認証のトータルセキュリティ

さらに AXシリーズには豊富なネットワーク認証機能があります。ネットワークに対し不正なユーザによるアクセスを防ぎ、許可されたユーザのみを加入対象とすることでネットワークの入り口でも安全性を確保するこの機能を組み合わせることにより、ネットワークをトータルでガードできるより強固なシステムを、ローコストかつシンプルな装置構成で実現することが可能となります。

1.2 各機能の分担について

ネットワーク・パーティションは AX6000S ファミリ(AX6700S/AX6600S/AX6300S)の持つ VRF 機能にて実現され、システムとしては L3 コアスイッチの役割を担い、論理的に分離したネットワークを管理します。

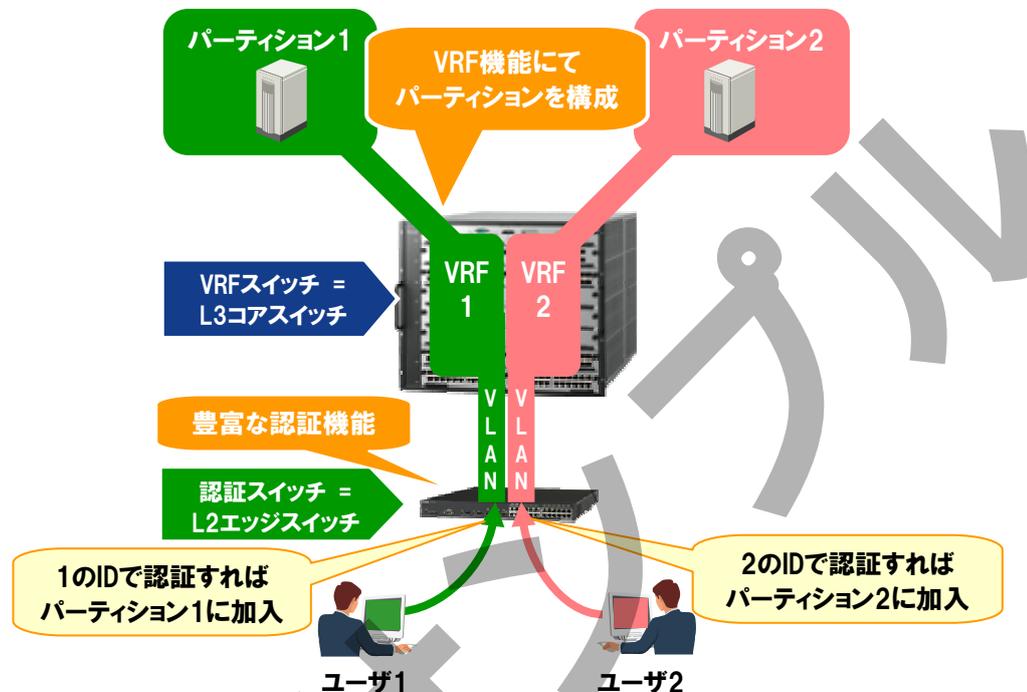


図 1.2-1 VRF 機能と認証機能の分担

一方で、ネットワーク認証ではアクセスエッジに認証スイッチとして AX2400S、AX1200S を利用します。このコンセプトはネットワーク・パーティションを用いたシステムでも同様であり、AX シリーズの持つ豊富な認証機能をそのまま利用できることと合わせて自由度の高いシステム設計が可能です。

さらにネットワーク・パーティションと AX シリーズの認証機能の互いの特長を活かし、同一端末による複数のネットワークへの選択接続なども可能となります。

2. 使用できる認証機能とシステム設計のポイント

ネットワーク・パーティションによるネットワークにて認証システムを構成する際に使用できる認証の方式と、システム設計上気をつけておくべきポイントについて解説します。

2.1 AX シリーズの認証機能について

ネットワーク・パーティションによる論理ネットワークにおいても一般のネットワークシステム同様、認証の機能は接続される認証スイッチの仕様によります。AX シリーズのサポートする認証方式一覧を以下に示します。

表 2.1-1 認証方式

項番	認証方式	認証モード		AX1200S	AX2400S AX3600S	AX6300S(*2) AX6600S(*2) AX6700S(*2)
		固定 VLAN モード	ポート単位 VLAN 単位			
1	IEEE802.1X 認証	固定 VLAN モード	ポート単位	○	○	○
2			VLAN 単位	×	○	○
3		動的 VLAN モード	○	○(*1)	×	
5	Web 認証	固定 VLAN モード		○	○	○
6		動的 VLAN モード		○	○	×
8	MAC 認証	固定 VLAN モード		○	○	○
9		動的 VLAN モード		○	○	×

(凡例) ○:サポート、×:未サポート

- (*1) AX2400S、AX3600S の IEEE802.1X 認証(VLAN 単位認証(動的))は同一装置内で Web 認証または MAC 認証の動的 VLAN モードと併用した場合動的 VLAN モードとして動作します。また装置で IEEE802.1X 認証(VLAN 単位認証(動的))を単独で用いた場合レガシーモードとして動作します。
- (*2) VRF 機能との同時併用はできません。

その他、AX シリーズでサポートされる認証機能の仕様詳細については「[AX シリーズ 認証ソリューションガイド - 2. AX シリーズの認証機能サポート一覧](#)」を参照ください。

2.2 ネットワークに対する認証スイッチとその他サーバの配置

2.2.1 パーティション毎に独立した認証システム

(1) 認証スイッチをパーティション毎に置く一般的な構成

AX シリーズでサポートする認証スイッチでは、参照するデータベースは内蔵のものでも外部参照のものでも一つのネットワークシステムを対象としています。また認証データベースに RADIUS を使用する場合、RADIUS サーバは認証スイッチとの間で通信をおこないます。従ってひとつのパーティションに一組の認証スイッチおよび各種データベースを管理するサーバ群を配置する構成が一般的で分かりやすいシステムとなります。

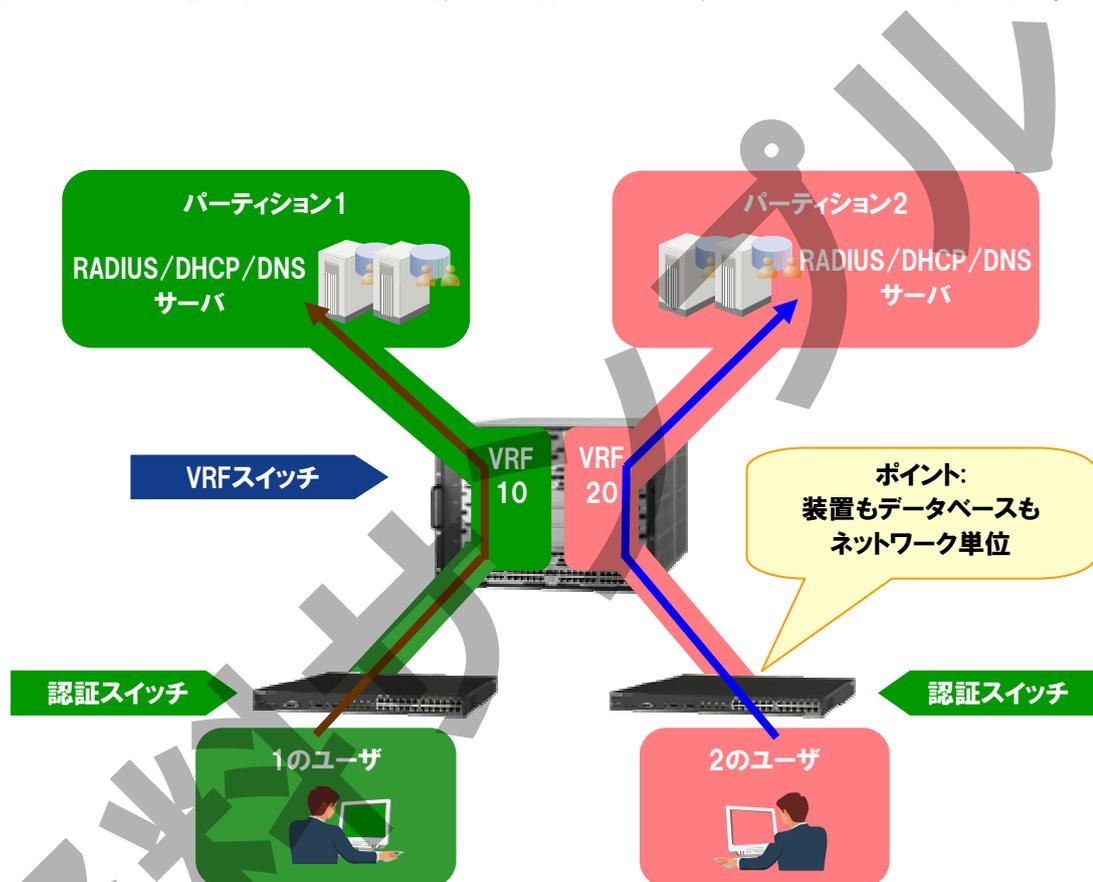


図 2.2-1 ネットワーク単位に認証スイッチを扱う構成

従って、ネットワーク・パーティションのシステムに認証を組み合わせる場合は、各ネットワークでそれぞれ独立した認証システムを持つ構成をまず基本として考えることを推奨いたします。

このようなシステムの構築の一例を [3.1](#) 節にて解説します。

(2) RADIUS サーバグループ選択機能により複数パーティションを1台に収容した構成

先の解説のとおり、RADIUS を使った認証をおこなう場合、認証スイッチは RADIUS サーバと 1 対 1 の組合せとするのが一般的です。

但し、AX1240S(ソフト Ver.2.2 以降)でサポートされる RADIUS サーバグループ選択機能を用いる場合はこの限りではありません。この機能を利用することにより、それぞれ独立した RADIUS サーバにより認証をおこなう各論理ネットワークを最大 4 つまで、一台の認証スイッチに収容することが可能となります。

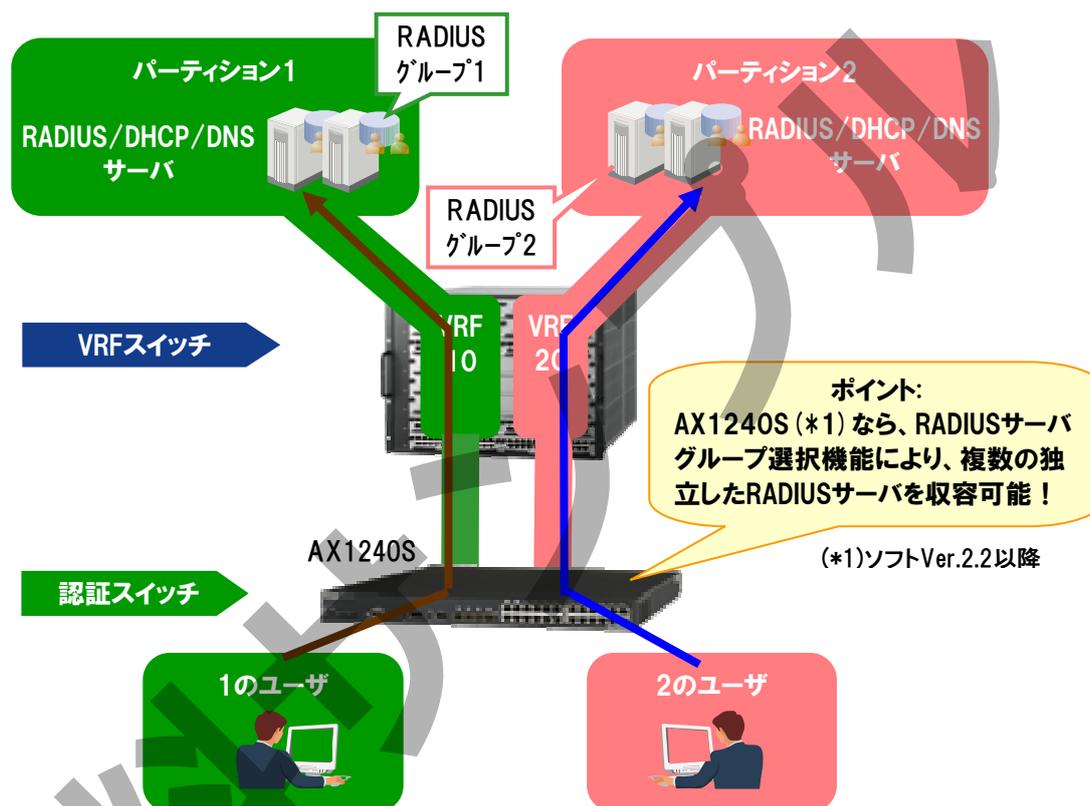


図 2.2-2 AX1240S による複数の RADIUS 認証ネットワークを扱う構成

認証時に参照対象とする RADIUS サーバグループの選択はポート別(IEEE802.1X 認証、Web 認証、MAC 認証)、またはユーザ ID 別(Web 認証のみ)におこなうことが可能です。このため、同一フロアに異なるネットワークが混在するような場合でも、認証スイッチをネットワーク毎に分けることなく、最小限の台数で効率よくシステムを構築することが可能です。

但し認証スイッチでは認証をおこなう VLAN に IP アドレスを与える必要があるため、上記のように 1 台の認証スイッチにて複数ネットワークを扱う場合は共用ネットワークが無い場合でも、異なるネットワーク間での IP アドレスの重複使用は避けて下さい。

こちら、システム構築の一例を [3.2 節](#)にて解説します。

2.2.2 複数パーティションを統合する認証システム

AXシリーズでサポートする認証スイッチには、認証前と認証後で扱う VLAN を切り替える、動的 VLAN 機能があります。この機能を利用し、互いに異なるパーティションにある VLAN を認証前、認証後それぞれに割り当てることにより、1台の認証スイッチで異なるパーティションへのアクセス認証をおこなえ簡単かつ安全にネットワーク単位で認証前後の環境を切替えることができます。

このように、一組の認証システムで複数のパーティションをまとめて扱うシステムを構築するには、以下のような点を考慮すれば容易に実現することが可能です。

(1) RADIUS サーバに関して

一般的な認証スイッチではRADIUSのような認証データベースとは1対1の組合せとなります。従って1台の認証スイッチで複数ネットワークを収容する場合は、RADIUSサーバはその複数ネットワーク分を統合した構成とすることを推奨します。(但し [2.2.1\(2\)](#)で解説のRADIUSサーバグループ選択機能を使用する場合はこの限りではありません。)

その上で、ネットワーク間のセキュリティを保つためにも、統合した RADIUS サーバは、それら各ユーザで利用するネットワークとは独立したパーティションに配置するのが良いでしょう。

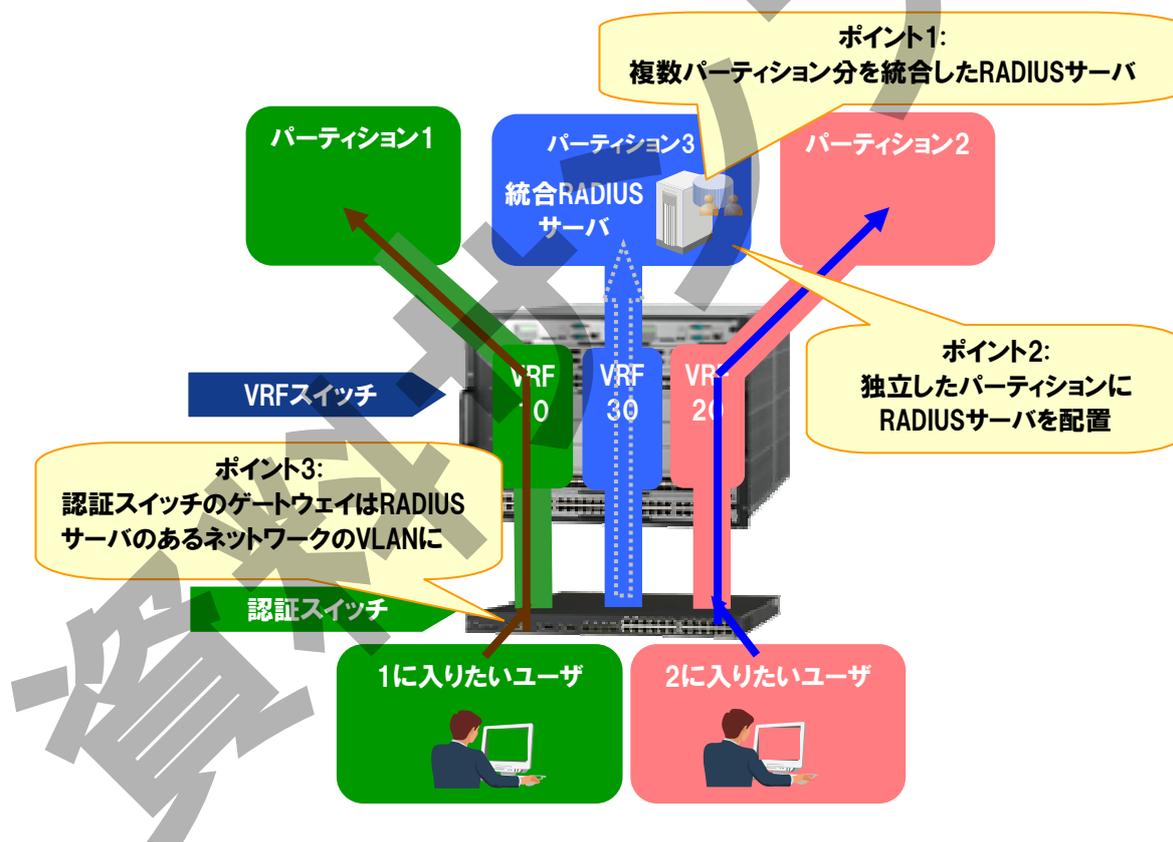


図 2.2-3 複数ネットワークを1台の認証スイッチで扱う構成

RADIUSサーバの属するパーティション(上記パーティション3)はパーティション1,2の共用ネットワークであっても構いませんが、DNSサーバなども統合する場合や管理上の通信等を考慮して共用ネットワークとしておく方が良いでしょう。

DNSに関してはVRFスイッチも認証スイッチも直接関与しないため、端末や他サーバから見えるネットワーク内であればどこに配置しても構いません。

(2) 認証前ネットワークと DHCP サーバに関して

AX シリーズ認証スイッチの持つ動的 VLAN 機能とネットワーク・パーティションの組み合わせにより、簡単かつ安全にネットワーク単位で認証前後の環境を切替えることができます。認証前と認証後の切替はもちろん、認証後のネットワークも複数を選択可能に構成することができ、そのそれぞれのネットワークは論理的に独立していますので、ネットワーク単位でよりセキュアな認証システムを構築できます。

この際の DHCP の扱いについても、パーティション毎に独立して DHCP リレーが可能なため、DHCP サーバをネットワーク個別で独立して扱うことが可能です。また、ソフト Ver.11.2 よりエクストラネット(パーティション間の通信)での DHCP リレーエージェント機能にも対応しました。これにより、各パーティション分を統合した DHCP サーバを構成するということが可能になりました。

特に共用ネットワークなどエクストラネットを構成する場合には IP アドレスを重複しないように構成する必要がありますが、この DHCP リレーエージェント機能の拡張にて DHCP サーバを統合できるようになるため、IP アドレスをシステム全体で一括して管理することが可能となります。

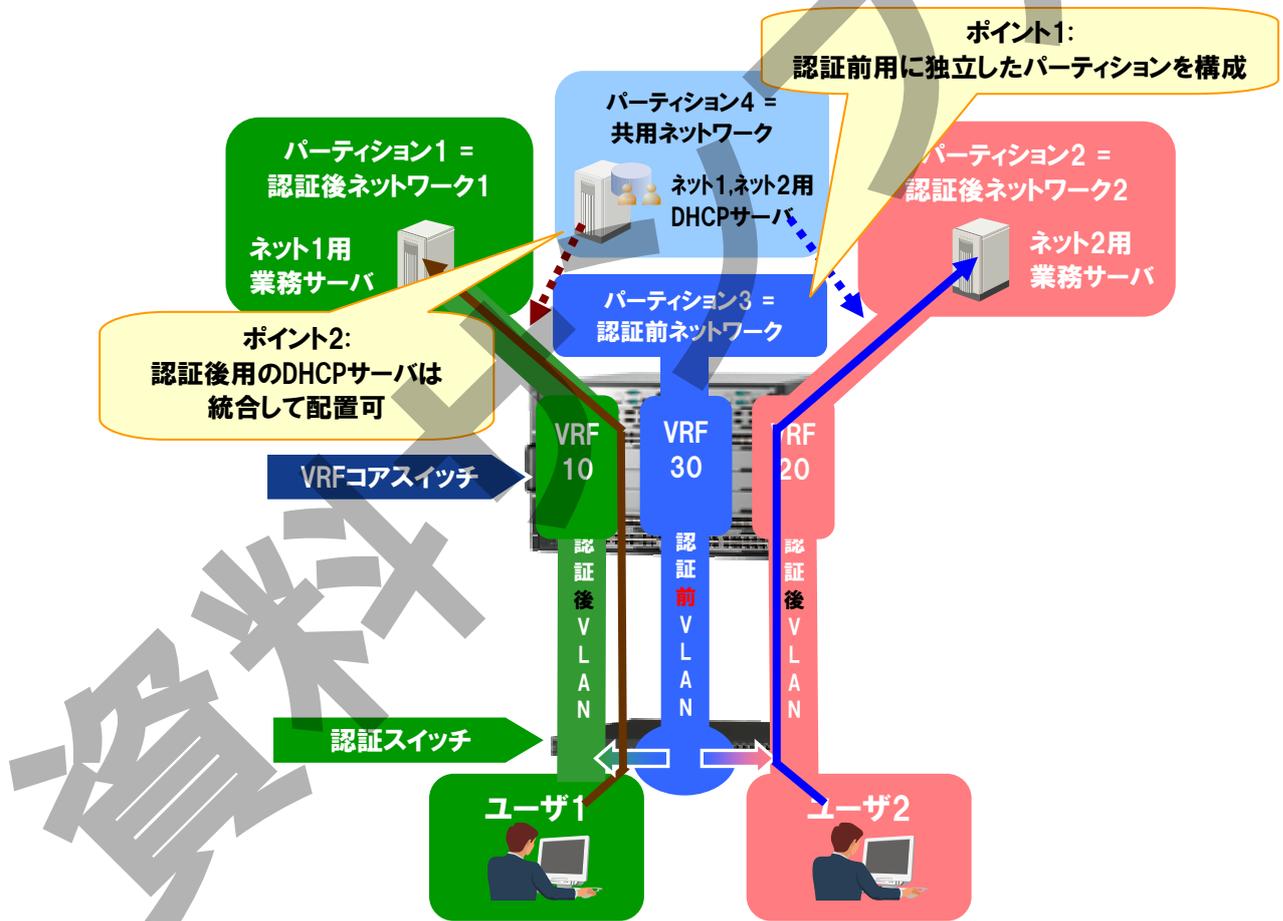
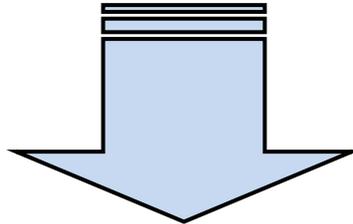


図 2.2-4 認証前ネットワークと DHCP サーバ

但し認証前と認証後では、同じ DHCP サーバを参照させてしまうと認証前後での IP アドレスの切替がおこなわれない場合があります。このため認証前と認証後では DHCP サーバは分けて構成することを推奨します。

またこのような構成においても、認証スイッチでは認証前後の VLAN に IP アドレスを与える必要がある点は同様であるため、1 台の認証スイッチにて複数ネットワークを扱う場合は異なるネットワーク間での IP アドレスの重複使用は避けて下さい。

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/>