

RADIUS サーバ設定ガイド Windows Server 2008 編



第2版

Copyright © 2008,2010 ALAXALA Networks Corporation. All rights reserved.



はじめに

RADIUS サーバ設定ガイド(Windows Server 2008 編)は、アラクサラネットワークス社の AX シリ ーズでサポートしているネットワーク認証機能を用いたシステム構築において、RADIUS サーバに Windows Server 2008 及び Windows Server 2008 R2、クライアント端末に Windows 7 及び Windows Vista を使用する場合の設定方法を示します。

関連資料

- ・AX シリーズ 認証ソリューションガイド
- ・AXシリーズ製品マニュアル(<u>http://www.alaxala.com/jp/techinfo/index.html</u>)

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。

本ガイドは Windows Server 2008 R2 をベースに記述しておりますが、Windows Server 2008 におい ても同様にお使いいただけます。詳細につきましては本文中に示しています。 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

本ガイド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下さい。

商標一覧

- ・アラクサラの名称及びロゴマークは、アラクサラネットワークス株式会社の商標及び登録商標です。
- ・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。
- ・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。

改版	履	歴
----	---	---

版数	rev.	日付	変更内容	変更箇所
初版	—	2008.6.20	初版発行	—
第2版	—	2010.2.17	・使用機器の変更	
			Windows Server 2008 R2 の追加	
			AX3630S,AX2430S(Ver10.7) → (Ver11.2.A)	全体
			AX1230S(Ver1.3.D) \rightarrow AX1240S(Ver2.2)	
			クライアント端末に Windows 7 Professional の追加	
			・AX1230S から AX1240S への装置変更に伴う AX コン	1.2.1
			フィグレーション例の更新。	
			・「1.3 Windows Server 2008 と Windows Server 2008 R2	1.3
			の差分について」を追加	
			・コンピュータ名の変更を「2.2 コンポーネントの追加」	2.1.2
			から「2.1 準備」に移動。	
			・Web サーバ(IIS)の SSL 設定を追加	3.1.3
			誤記および表現を全体的に修正	_

目次

1.	概要	Į	6
	1.1.	概要	6
	1.2.	設定例環境	7
	1.2.	1. 使用機器一覧とAXコンフィグレーション	7
	1.2.	2. 設定例のネットワーク構成図	8
	1.3.	Windows Server 2008 とWindows Server 2008 R2 の差分について	9
2.	Win	dows Server 2008 R2 / Windows Server 2008 の構成	10
	2.1.	準備	10
	2.1.	1. ネットワークアダプタの設定	10
	2.1.	2. コンピュータ名の変更	10
2	2.2.	役割の追加	11
	2.2.	1. Active Directoryのインストール	11
	2.2.	2. Webサーバ(IIS)のインストール	18
	2.2.	3. Active Directory証明書サービスのインストール	21
	2.2.	4. ネットワークポリシーとアクセスサービス(NPS)のインストール	27
	2.2.	5. DHCPサーバのインストール	29
	2.2.	6. インストール内容の確認	34
3.	IEE	E802.1X認証の設定	35
	3.1.	サーバの設定	35
	3.1.	1. ユーザー、グループの作成	35
	3.1.	2. NPSの設定	39
	3.1.	3. Webサーバ(IIS)の設定	52
;	3.2.	クライアント端末の設定	55
	3.2.	1. ドメイン参加	55
	3.2.	2. PEAP設定	58
	3.2.	3. TLS設定	60
	3.3.	IEEE802.1X認証の確認	65
	3.3.	1. サーバでの確認	65
	3.3.	2. AX2430Sでの確認	66
4.	Web	o認証の設定	67
4	4.1.	サーバの設定	67
	4.1.	1. ユーザーの作成	67
	4.1.	2. NPSの設定	70
	4.2.	クライアント端末の設定	76
	4.3.	WEB認証の確認	76

	4.3.1.	クライアントでの確認	76
	4.3.2.	サーバでの確認	77
	4.3.3.	AXでの確認	77
5.	MAC認	証の設定	78
5	5.1. サ-	ーバの設定	78
	5.1.1.	グループポリシーの編集(パスワードのポリシー変更)	78
	5.1.2.	ユーザーの作成	82
	5.1.3.	NPSの設定	86
5	5.2. MA	C認証の確認	86
	5.2.1.	サーバでの確認	86
	5.2.2.	AXでの確認	86

1. 概要

1.1. 概要

本ガイドでは認証スイッチにAX シリーズ、認証端末に Windows 7 と Windows Vista とし、Windows Server 2008 /Windows Server 2008 R2 の NPS を RADIUS サーバ、Active Directory をユーザーデ ータベースとして下記認証方式を使用したネットワーク認証システムを構築するための設定方法を 記載しています。

- ・IEEE802.1X 認証^(※1)(PEAP、TLS)+SSO(Single Sign-On)
- ・Web 認証
- ・MAC 認証

使用方法

本ガイドは、認証方式毎に設定方法を記載しています。目次を参照して、構成する認証方式の項目から設定して下さい。第2章では Windows Server 2008 の「役割」(Windows Server 2003 のコンポーネントに相当します)のインストール方法を記載しています。ここでインストールする役割は Active Directory 証明書サービス(認証局)^(※2)を除き各認証方式で必須となります。

AX のコンフィグレーションに関して本ガイドでは詳細な説明は記載していません。AX の設定は完了 している事を前提にサーバ、クライアントの設定方法を記載しています。各認証方式に関連するコンフ ィグレーションは以下の資料を参照して下さい。

- ・AX シリーズ 製品マニュアル
- ・AX シリーズ 認証ソリューションガイド

Windows Server 2008 とWindows Server 2008 R2 では設定画面のレイアウトやデザインに若干の違いがあります。本ガイドではWindows Server 2008 R2 の設定画面をベースにインストール及び設定方法を示しています。Windows Server 2008 を使用してシステムを構築する場合は「1.3 Windows Server 2008 とWindows Server 2008 R2 の差分について」を参照の上、本文中に記載したWindows Server 2008 の設定手順に従ってください。

^(※1) 本ガイドの IEEE802.1X 認証の設定に関して、サプリカントの端末をドメインに参加させる手順で記載しています。 サプリカント端末をドメインに参加させなくても IEEE802.1X 認証(PEAP、TLS)は構成可能ですが若干手順が異なり ます。

^(※2) IEEE802.1X 認証のみ証明書を発行するため Active Directory 証明書サービス(認証局)のインストールが必要となり ます。また本ガイドでは CA、RADIUS サーバ、Active Directory を一台のサーバにインストールしています。

1.2. 設定例環境

1.2.1. 使用機器一覧と AX コンフィグレーション

使用機器一覧

- > RADIUS $\forall -n$: Windows Server 2008 R2 Standard 、Windows Server 2008 Standard
- ▶ 認証端末: Windows 7 Professional、Windows Vista Ultimate SP1
- > 認証スイッチ: AX1240S(Ver2.2)/ AX2430S(Ver11.2)
- L3switch : AX3630S(Ver11.2)
- ➢ HUB: EAPOL 透過機能有り

AX コンフィグレーション設定例

AX1240S のコンフィグレーション			
hostname "AX1240S"	interface vlan 100		
!	ip address 192.168.100.12 255.255.255.0		
vlan 1	· · · · · · · · · · · · · · · · · · ·		
name "VLAN0001"	interface vlan 200		
!	ip address 192.168.200.12 255.255.255.0		
vlan 30	!		
!	interface vlan 1000		
vlan 100 mac-based	ip address 172.16.0.12 255.255.255.0		
!	!		
vlan 200 mac-based	ip route 0.0.0.0 0.0.0.0 172.16.0.254		
!	!		
vlan 1000	■ip access-list extended "auth"		
!	10 permit udp any any eq bootps		
spanning-tree disable	20 permit udp any any eq bootpc		
spanning-tree mode pvst	■30 permit udp any host 10.51.0.1 eq domain		
!	!		
interface fastethernet 0/1	dot1x system-auth-control		
switchport mode mac-vlan	!		
switchport mac vlan 100,200	mac-authentication system-auth-control		
switchport mac native vlan 30	▲mac-authentication id-format 1		
dot1x port-control auto	mac-authentication password "alaxala"		
dot1x multiple-authentication	!		
dot1x supplicant-detection auto	web-authentication system-auth-control		
web-authentication port	web-authentication ip address 1.1.1.1		
▲mac-authentication port	!		
authentication ip access-group "auth"	service dhcp vlan 30		
authentication arp-relay	■ip dhcp pool "V30"		
!	network 192.168.30.0/24		
~未使用インターフェイスは省略~	■lease 0 0 0 10		
!	default-router 192.168.30.254		
interface gigabitethernet 0/25	dns-server 10.51.0.1		
media-type auto	!		
switchport mode trunk	★radius-server host 10.51.0.1 key "alaxala"		
switchport trunk allowed vlan 30,100,200,1000	★radius-server dead-interval 0		
	!		
interface vlan 1	aaa authentication dot1x default group radius		
	!		
interface vlan 30	▲aaa authentication mac-authentication default group radius		
ip address 192.168.30.12 255.255.255.0	!		
	aaa authentication web-authentication default group radius		
●IEEE802.1X 認証関連コンフィグレーション			
▲MAC 認証関連コンフィグレーション			

★RADIUS サーバ関連のコンフィグレーション(各認証方式共通)

■Web 認証関連コンフィグレーション

※上記コンフィグレーションは AX1240S の設定コンフィグです。同等の設定を AX2430S に定義す る場合は関連資料の「AX 認証ソリューションガイド」を参照して下さい。



1.2.2. 設定例のネットワーク構成図

図 1.2-1 構成図

AX シリーズでは MAC VLAN を使用した動的な VLAN 切り替えを構成しています。認証に成功した端 末は、RADIUS サーバからの VLAN 情報(MAC VLAN の VLAN ID)に従い、動的に VLAN の切り替え を行います。

設定例では、ユーザーID に付属させる各情報について以下のように設定しています。

ユーザーID が所属するグループ名:

認証方式に関わらず、共通にしています(グループ名:SALES)。

認証後に所属させる VLAN:

認証方式によって、分けています。

- ・IEEE802.1X 認証で認証成功→VLAN100
- ・Web 認証と MAC 認証で認証成功→VLAN200

VLAN ID や認証方式による所属 VLAN の振り分けはネットワーク構成に沿って変更して下さい。

1.3. Windows Server 2008 と Windows Server 2008 R2 の差分について

本ガイドを参照して RADIUS サーバを構成する際に Windows Server 2008 と Windows Server 2008 R2 で設定内容や設定画面に差分がある箇所を以下に示します。

(A) 画面表示の違いについて

- 「2.2.1 Active Directory のインストール」
 手順⑤、⑥、⑧、⑩の図にて Windows Server 2008 では一部表示内容が異なります。
 手順⑪の図にて Windows Server 2008 ではフォレストの機能レベルに「Windows Server 2008 R2」
 の選択ができません。
- 「2.2.3 Active Directory 証明書サービスのインストール」
 手順④、④の図にて Windows Server 2008 では選択可能な役割サービスの種類が少なく表示されています。
- 「2.2.5 DHCP サーバのインストール」
 手順⑧の図にて Windows Server 2008 では少し設定画面のデザインが違います。設定項目の違いはありません。

(B) ネットワークアダプタの扱い

複数ネットワークアダプタを持つサーバにインストールして使用する場合、ネットワークアダプタの 状態(ネットワークアダプタが有効か/無効か、ネットワークアダプタのポートがリンクアップしている かダウンしているか)によって以下の違いがあります。

- ・Windows Servre 2008 R2 では 1 つでもリンクダウンしている有効なネットワークアダプタのポート が存在すると Active Directory のインストールが開始できません。
- ・Windows Server 2008 では 1 つでもリンクアップしている有効なネットワークアダプタのポートが存 在すれば Active Directory のインストールは開始できます。

(C) Web サーバの(IIS)の設定について

Windows Server 2008 R2 の「証明書サービスWeb登録」機能を使用してクライアント端末のブラ ウザ経由でユーザー証明書を配布するにはWebサーバ(IIS)でSSLの設定が必須です。Windows Server 2008 を使用する場合はSSLの設定は必須ではありません。本ガイド「3.1.3 Webサーバ(IIS) の設定」にてWindows Server 2008 R2 のWebサーバ(IIS)のSSL設定方法を示しています。

2. Windows Server 2008 R2 / Windows Server 2008 の構成

本章ではWindows server 2008 R2 をRADIUSサーバとして構成するために必要な役割のインストー ル方法を記載しています。以下に本ガイドでインストールする役割を示します。なおWindows Server 2008 をRADIUSサーバとして構成する場合は「1.3 Windows Server 2008 とWindows Server 2008 R2 の差分について」を参照の上本章の手順を行ってください。

- Active Directory ドメイン サービス
- DNS サーバ
- Web サーバ (IIS)
- Active Directory 証明書サービス
- ネットワークポリシーとアクセスサービス (NPS)
- DHCP サーバ

2.1. 準備

2.1.1. ネットワークアダプタの設定

TCP/IPの設定を完了させて下さい。ネットワークアダプタのリンクが上がっていない場合Active Directoryのインストールウィザードを進める事が出来ません。複数のネットワークアダプタが存在する 場合、全てのネットワークアダプタを正しく設定してポートのリンクが上がっている状態にするか、使 用しないネットワークアダプタは無効にして下さい。Windows Server 2008 で構成する場合は使用しな いネットワークアダプタを無効にする必要はありません。詳細は「1.3Windows Server 2008 と Windows Server 2008 R2 の差分について」の(B)を参照してください。

2.1.2. コンピュータ名の変更

本ガイドで必要な上記の役割をインストー ルした後ではサーバのコンピュータ名の変更 が容易にできなくなる為、必要であれば事前 に設定して下さい。

 「スタート」→「コンピュータ」を右クリッ クしてプロパティを開き、システム画面内の 「コンピュータ名、ドメインおよびワークグ ループの設定」の「設定と変更」をクリック する。システムのプロパティ画面にて「変更」 をクリックしてコンピュータ名を変更する。 (本ガイドでは「dc」)設定変更後再起動が 必要です。



2.1-1 コンピュータ名の変更

RADIUS サーバ設定ガイド Windows Server 2008 編(第2版)

2.2. 役割の追加

2.2.1. Active Directory のインストール

ユーザーデータベースに Active Directory を使用します。

 「スタート」→「管理ツール」→「サー バーマネージャ」を起動し、「役割」を選 択、「役割の追加」をクリックする。



図 2.2-1 Active Directory のインストール1

 ②「開始する前に」を確認して「次へ」を クリックする。

※右画面は、各役割の設定画面でその都 度出てきますが内容は同じであるため、 不要な場合は、中段部分にある、「既定で このページを表示しない」にチェックを 入れて下さい。



図 2.2-2 Active Directory のインストール 2

 ③ 「Active Directory ドメインサービス」を 選択、「次へ」をクリックする。

役割の追加ウィザード		X
サーバーの役割の選	産択	
間始する前に サーバーの役割 Active Diectory ドメイン サービス 確認 通行状況 結果	このサーバーにインストールする投製施 1 つ以上型銀化はます。 快数193 	記録時 Control Directory ドメインサードフィ(AD Control Directory ドメインサーシン オットワーク管理者がごれるの情報を使 用できるようになります。AD CO Statistic ローチントロークを理想がごれるの情報を使 用できるようになります。AD CO Statistic ローチントロークになります。AD CO Statistic ローチントローチントローチントローチントローチントローチントローチントローチント
	<前へ(P) 次へ(10> インストール(D) キャンセル

図 2.2-3 Active Directory のインストール 3

※ 右のような「Active Directory ドメインサ ービスに必要な機能を追加しますか?」 のメッセージが表示された場合は「必要 な機能を追加」をクリックしてから「次 へ」をクリックする。(Windows Server 2008 では表示されません。)

役割の追加ウィザード Active Directory ドメイン サービス に Active Directory ドメイン サービス をインストールする W能(E) INET Framework 35.1 の機能 NET Framework 35.1	▲ 必要な機能を迫加しますか? 前に、必要な機能を行ンストールしておく必要があります。 説明 Microsoft NET Framework 35.1 では、NET Framework 20 APIの機能にアブリケンシン 作成別の新しいテクリロジが加かりました。ユー ザーは、戦力的なユーザー インターフェイス。朝 客の個人特報が発意、シームレスで全全な通信 を利用できます。また、さぎさなとジネスプロ セスをモデル化することができます。
	必要な機能を追加(<u>A</u>) キャンセル
① <u>これらの機能が必要な理由</u>	li li

図 2.2-4 Active Directory のインストール 3-1

④ 内容を確認して、「次へ」をクリックする。



図 2.2-5 Active Directory のインストール 4

内容を確認して、「インストール」をクリックする。(Windows Server 2008 では少し表示が異なります)



図 2.2-6 Active Directory のインストール 5

 ⑥ インストールの結果画面、中段部分にある「このウィザードを終了し、Active Directoryドメインサービスインストールウィザード(dcpromo.exe)を起動します。」を選択すると自動的にウィザードが開始される。(Windows Server 2008では少し表示が異なります)



図 2.2-7 Active Directory のインストール 6

⑦ 「次へ」をクリックする。



図 2.2-8 Active Directory のインストール 7

 ⑧ 「次へ」をクリックする。(Windows Server 2008 では少し表示が異なります)



図 2.2-9 Active Directory のインストール 8

⑨「新しいフォレストに新しいドメインを 作成する」を選択、「次へ」をクリックす る。

Active Directory ドメイン サービス イン	ストール ウィザード	
展開の構成の選択 既存のフォレストまたは新しいフォレスト用(こドメイン コントローラを作成できます	ŀ. [
○ 既存のフォレスト(E)		
○ 既存のドメインにドメイン コント	-ローラを追加する(<u>A</u>)	
○ 既存のフォレストに新しいドメイ	(ンを作成する(<u>C</u>)	
このサーバーは新しいドメインの	の最初のドメイン コントローラになりま	t न .
◎ 新しいフォレストに新しいドメインを作	成する(<u>D</u>)	
可能な展開の構成の詳細		
	< 戻る(<u>B</u>)	次へ(N)> キャンセル

図 2.2-10 Active Directory のインストール9

 任意のフォレストルートドメイン名(本 ガイドでは、「example.co.jp」)を入力し、 「次へ」をクリックする。

フォレスト ルート ドメイン名 フォレストの最初のドメインはフォレストのルート ドメインです。その名前は、フォレストの名前です。	
新しいフォレスト ルート ドメインの完全修飾ドメイン名 (FQDN) を入力してください。	
フォレスト ルート ドメインの FQDN(<u>E</u>):	
example.co.jp	
例: corp.contoso.com	
< 戻る(B) 次へ(N) > キャンセル	

図 2.2-11 Active Directory のインストール 10

 (1) 機能レベルを選択し(本ガイドでは 「Windows Server 2008 R2」を選択)、「次 へ」をクリックする。

(Windows Server 2008 は機能レベルに 「Windows Server 2008」を選択してください。)

🖥 Active Directory ドメイン サービス インストール ウィザード	×
フォレストの機能レベルの設定 フォレストの機能レベルを選択してください。	
フォレストの機能レベル(E):	
jwindows Server 2008 R2▼	
Windows Server 2008 R2 フォレストの機能レベルでは、Windows Server 2008 フォレストの機能レニ ベルで使用可能なすべての機能に加えて以下の機能を使用できます。 - こみ箱 これが有効になっている場合。 - Active Directory ドメイン サービスの実行中に、 育能会社にすうプレットを完全に見元できます。 このフォレストで作成されたすべての新しいドメインは、既定で Windows Server 2008 R2 ドメインの 機能レベルで動作します。	
▲ このフォレストには、Windows Server 2008 R2 以降を実行するドメイン コントローラ 一のみ追加できます。	
ドメインとフォレストの機能レベルの詳細	
〈戻る(B) 次へ(N) > キャンオ	비

図 2.2-12 Active Directory のインストール 11

 「DNS サーバー」に、チェックし、「次 へ」をクリックする。

如のドメイン コントローラ オプション	
このドメイン コントローラの追加オブションを選択してください。	
☑ グロー/バル カタログ(Q)	
■ 読み取り専用ドメインコントローラ (RODO)(B)	
注自力or惜幸服(<u>A</u>):	
フォレスト内の最初のドメイン コントローラはグローバル カタログ サーバーでなければならず、 RODC にすることはできません。	<u> </u>
最初のドメイン コントローラに DNS サーバー サービスをインストールすることをお勧めします。	
1	
<u>ドメイン コントローラの追加オブション</u> の詳細	
〈 戻る(<u>B</u>) 次へ(<u>N</u>) >	キャンセル

図 2.2-13 Active Directory のインストール 12

 ・13 質問を確認して問題なければ「はい」を 選択する。



図 2.2-14 Active Directory のインストール 13

vi

① 「データベース」、「ログファイル」、およ び「SYSVOL」の保存先を変更する必要 がなければ「次へ」をクリックする。

🖥 Active Directory ドメイン サービス インストール ウィザード		×
データベース、ログ ファイル、および SYSVOL の場所 Active Directory ドメイン コントローラのデータベース、ログ ファイル、および SYSVOL ルダを指定してください。	を保存するフォ	
より優れたパフォーマンスと回復性を得るには、データベースとログ ファイルを別のボリコ ださい。 データベースのフォルダ(D):	ームに格納してく	
C:#Windows#NTDS	参照(<u>R</u>)	
ログ ファイルのフォルダ(L):		
C:#Windows#NTDS	参照(0)	
SYSVOL フォルダ(S):		-
C:#Windows#SYSVOL	参照(₩)	1
<u>Active Directory ドメイン サービスのファイルの配置</u> の詳細		
< 戻る(B) 次へ(M)	·> ++>	セル

- 図 2.2-15 Active Directory のインストール 14
- 15 任意の復元パスワードを入力、「次へ」を クリックする。



- 図 2.2-16 Active Directory のインストール 15
- 16 設定した内容を確認し「次へ」をクリッ クするとインストールが開始される。 (Windows Server 2008 では少し表示が 異なります)



図 2.2-17 Active Directory のインストール 16

 「完了」をクリックしてサーバを再起動 する。



図 2.2-18 Active Directory のインストール 17

2.2.2. Web サーバ (IIS) のインストール

Web からの証明書発行機能を利用するために、Active Directory 証明書サービス(認証局)をインストールする前に IIS をインストールします。

Active Directory 証明書サービスをインストールしない場合または、本サーバをその他の目的で Web サーバにしない場合は必要ありません。

 「スタート」→「管理ツール」→「サー バーマネージャ」を起動し、「役割フォル ダ」を選択、「役割の追加」をクリックす る。

n 12 an 12 an Carllin Marcard	5120 mm	
校期 税設 12時 株式	サーバーにインストールされている必要的正常性をあ示し、没想や機能も追加	ecimieley.
5 BC 18-19	○ 段割の概要	2 役割の概要へルブ
	 	in terreturne in terreturne
	▲ DNS サーバー ○ Active Directory ドメイン サービス	AD DS 187
	ディレクトリデータを格納し、ユーザーログオン処理、認知、ディレクトリ検索など、ユーザー	とドメインの通信を管理します。
	© 123104X18	Contraction Active Directory ドンイン サービス に 料約
	- かセージ あし シスシム サービス = 酸が実行中、2 酸が伴生 ▲ イベト 表述 24 時間に 4 感の驚音 (ペト, 29 酸の薄弱 (ペト ○ 食が料 – デン - 後秋人・2 トール 57 円 マオ	Di date-Poniste
	(0104)-02 1100 0AP-00101049	2 役割サービスを許録
	Active Directory 154/ン 22小ローライジストール構築 UROE 用D 留理 インストールを用していません IRS サーバー インストールを用ていません ICジード同時 インストールを用ていません ICジード同時 インストールを用ていません 留電アール インストールを用いていません	
	1898 Action Discoury ドメイン、エントロージを使用すると、サーバーでディレクドリーデージを構 ダリン処理、2回該、ディインドリ検索など、ユーザーとドメインの場合を管理することがでい	約し、ユーザー ロ きます。
	C BUTTER THE REAL PROPERTY AND	

図 2.2-19 Web サーバ(IIS)のインストール1

 ② 「Web サーバ (IIS)」にチェックを入れ 「次へ」をクリックする。



図 2.2-20 Web サーバ(IIS)のインストール 2

※Windows Server 2008 では②の手順でチェ ックボックスを入れると同時に、下記の「役 割の追加ウィザード」が現れるので、「必要な 機能を追加」を選択、「次へ」をクリックする。



図 2.2-21 Web サーバ(IIS)のインストール 2-1

③ 内容を確認し、「次へ」をクリックする。



図 2.2-22 Web サーバ(IIS)のインストール 3

④ 他に追加する必要がなければ、「次へ」を クリックする。

役割の追加ウィザード		×
役割サービスの選邦	R	
開始をする前に サーバーの検測 Web サーバー(IIS)	Web サーバー (IS) にインストールする役割サービスを選択 (没割サービス/B) Web サーバー U 割りな、フテッツ U 割りな、フラッツ U 割りな、レクション D コリケ いっし、利用 U 割り、レクション U 割り、レクション U 割り、レクション U コリケ いっし U コリケ いっし <th>1995 1995 1995 1997 199</th>	1995 1995 1995 1997 199

図 2.2-23 Web サーバ(IIS)のインストール 4

内容を確認し、「インストール」をクリックする。



図 2.2-24 Web サーバ(IIS)のインストール 5

⑥ インストールの結果を確認し、「閉じる」をクリックする。



図 2.2-25 Web サーバ(IIS)のインストール 6

2.2.3. Active Directory 証明書サービスのインストール

IEEE802.1X 認証で PEAP を使用する場合にはサーバ証明書、TLS の場合にはサーバ証明書とユーザ ー証明書が必要です。これらの証明書を発行する Active Directory 証明書サービスのインストール手順 を以下に示します。

Active Directory 証明書サービスを別サーバで構成することも可能ですが、本ガイドではドメインコン ローラと同一のサーバに Active Directory 証明書サービスをインストールする手順を記載しています。 なお、IEEE802.1X 認証を行わない場合は、Active Directory 証明書サービスをインストールする必要は ありません。

 「スタート」→「管理ツール」→「サー バーマネージャ」を起動し、「役割フォル ダ」を選択、「役割の追加」をクリックす る。



図 2.2-26 Active Directory 証明書サービスのインストール 1

「Active Directory 証明書サービス」にチェックを入れて、「次へ」をクリックする。



図 2.2-27 Active Directory 証明書サービスのインストール 2

③ 内容を確認し、「次へ」をクリックする。



図 2.2-28 Active Directory 証明書サービスのインストール3

④ 「役割サービスの選択」にて、「証明機関」
 と「証明機関 Web 登録」にチェックを入れ「次へ」をクリックする。(Windows Server 2008 では少し表示が異なります)

役割の追加ウィザード		×
後割サービスの選択	3	
開始する前に サーバーの役割 AD OS を当サービス セットアップの種類 の必要す に登場す のみの登録 配容キー 電号化 CA の名前 者の期間 証明書データペース Web サーバト(IIIS) 役割サービス 確認 通行代応兄 記具	Active Directory 証明書サービス にインストールする(含割サービスを連訳してください: 注明) 夏明 夏明 夏明 夏明 夏日期開催) Web 登録 夏日期開催) Web 登録 夏日期間 Web 登録 夏日期意の全球 アーボーに発展していたったった。 アーボーに発展していたった。 アーボーに発展していたった。 ア・ボーに発展していたった。 ア・ボーに発展していたった。 ア・ボーに発展していたった。 ア・ボーに発展していたった。 ア・ボーに発展していたった。 ア・ボード ア・ボード ア・ボード ア・ボード ア・ボード ア・ボード ア・ボード ア・ボー ア・ボー ア ア	
	<前へ(2) (茶へ(2)) イシストール(2) キャンセル	

図 2.2-29 Active Directory 証明書サービスのインストール 4

⑤ ④の手順で、証明機関 Web 登録にチェ ックを入れると、「役割の追加」ウィザー ドが出てくるので、「必要な役割サービス を追加」を選択、「次へ」をクリックする。



図 2.2-30 Active Directory 証明書サービスのインストール5

⑥ 「エンタープライズ」をチェックして、「次へ」をクリックする。



図 2.2-31 Active Directory 証明書サービスのインストール 6

 「ルート CA」をチェックして、「次へ」 をクリックする。



図 2.2-32 Active Directory 証明書サービスのインストール7

⑧ 「新しい秘密キーを作成する」をチェックして、「次へ」をクリックする。



図 2.2-33 Active Directory 証明書サービスのインストール8

変更する必要がなければ、「次へ」をクリックする。

役割の追加ウィザード		×
CA の暗号化を構	着成	
門防治する前に サーバーの役割 AD CS (発射サービス セットアップの種類 CA の種類 地営地トー 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本	No.N.R. かーキりたりてした。 発行する 2000年の日本に合った地グル 1921年 いー・ジン ブロンパター (Aver State 2000年7月) No.N.R. そのために 2000年 1000日 100000000	
	<前へ(P) 法へ(A) > インストール() キャンセル	

図 2.2-34 Active Directory 証明書サービスのインストール 9

「この CA の共通名」を確認し、変更する必要がなければ、「次へ」をクリックする。

CA 名を構成 CD CA を 施成 CD CA を 施防 Cの CA を 施防 Cの CA を 施防 Cの CA を 施防	利する共通名を入力します。この名前は、CAで発行されるすべての証明書に付加されます。譜別名 自動的に生成されますが、変更できます。
開始する前に この CA を調知	別する共通名を入力します。この名前は、CA で発行されるすべての証明書に付加されます。識別名 自動的に生成されますが、変更で考ます。
サーバーの没計 のサラィックスは AD CS この CA の共う パ交割サービス この CA の共う セントックブの確如 ごろ CA の共う セントップブの確如 ごろ CA の共う モントップブの確如 ごろ Packan モントップブのでののの 「の Packan モントップブのでののの 「の Packan モントップブのでののの 「の Packan モントップブのでののの 「の Packan モントップジーン 「の Packan ビントップジーン 「の Packan ビントップジーン 「の Packan ビントップシーシン 「の Packan ビン 「の Packan	8名(G): -CA (>921(D): DCC=co.DC=p 21_−(P): -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp -DC=CADC=example.DC=co.DC=jp

図 2.2-35 Active Directory 証明書サービスのインストール 10

 有効期間に変更する必要がなければ、「次 へ」をクリックする。



図 2.2-36 Active Directory 証明書サービスのインストール 11

変更する必要がなければ、「次へ」をクリックする。



図 2.2-37 Active Directory 証明書サービスのインストール 12

確認し問題がなければ、「次へ」をクリックする。



図 2.2-38 Active Directory 証明書サービスのインストール 13

 ④ 追加の必要がなければ、「次へ」をクリッ クする。(Windows Server 2008 では少し 表示が異なります)



図 2.2-39 Active Directory 証明書サービスのインストール 14

 内容を確認し問題がなければ、「インスト ール」をクリックする。



図 2.2-40 Active Directory 証明書サービスのインストール 15

インストールの結果を確認し、「閉じる」
 をクリックする。



図 2.2-41 Active Directory 証明書サービスのインストール 16

- 2.2.4. ネットワークポリシーとアクセスサービス (NPS) のインストール
- 「スタート」→「管理ツール」→「サー バーマネージャ」を起動し、「役割フォル ダ」を選択し、「役割の追加」を選択する。



 「ネットワークポリシーとアクセスサー ビス」にチェックを入れて、「次へ」をク リックする。



図 2.2-43 NPS のインストール 2

③ 内容を確認し「次へ」をクリックする。



図 2.2-44 NPS のインストール 3

④ 「ネットワークポリシーサービス」にチェックを入れて、「次へ」をクリックする。



内容を確認し、「インストール」をクリックする。



⑥ インストールの結果を確認し、「閉じる」 をクリックする。



図 2.2-47 NPS のインストール 6

2.2.5. DHCP サーバのインストール

本ガイドでは、クライアント端末の IP アドレスの設定に DHCP を使用する構成となっています。ここでは DHCP サーバのインストールと設定方法を記載しています。

※既に他の DHCP サーバ等が動作している場合、3.1.1 DHCP サーバのインストールは省いて下さい。

 「スタート」→「管理ツール」→「サー バーマネージャ」を起動し、「役割フォル ダ」を選択し、「役割の追加」を選択する。



図 2.2-48 DHCP サーバのインストール1

「DHCP サーバー」にチェックを入れて、
 「次へ」をクリックする。



図 2.2-49 DHCP サーバのインストール 2

③ 内容を確認し、「次へ」をクリックする。



④ 設定を行うセグメントが選択されている ことを確認し、「次へ」をクリックする。

役割の追加ウィザード		×
ネットワーク接続バ	インディングの選択	
開始する前に サーバーの役割 DHOP サーバー ネットワーク地球のインテイング IPv4 DNS 設定 DHOP スコーフ DHOP Xスコーフ DHOP Xスコーフ DHOP Xスコーフ DHOP Xスコーフ DHOP Xスコース DHOP X Xコース DHOP X X Xコース DHOP X X X X X X X X X X X X X X X X X X X	静的 IP アドレスを持つスクトワーク接続が 1 つじ人上 使出たれました。1 つのスクトワーク接続は、1 つの分離された む ワトロ クライアンドム サービスを提供する ために 使用できます。 この DOP サーバーで ウライアントへのサービス 提供のために 使用する ネットワーク接続を選択して だだい。 ネットワーク接続 (2) P アドレス P アドレス 10 510.1 Pv4	
	詳細 名 記 ・ ローカル エリア接続 ネットワーク アダプター・ ローカル エリア接続 神理アドレス・ 00-19-B9-E3-17-28 < (前へ(2) 次へ(<u>い</u>)> イシストード以び キャンセル]

図 2.2-51 DHCP サーバのインストール 4

 「親ドメイン名」と「優先 DNS サーバーの IPv4 アドレス」を確認して、「次へ」 をクリックする。



図 2.2-52 DHCP サーバのインストール 5

⑥ 「IPv4 WINS サーバー設定の指定」で、
 変更する必要がなければ、「次へ」をクリックする。

役割の追加ウィザード	×
IPv4 WINS サーバ	一般定の指定
間始する前に サーバーの投影 DHOP サーバー キットワーン抽扱してクライング IP-4 DNS 設定 DHOP スワーブ DHOP オスープ DHOP オスープ DHOP オスープ DHOP オスープ DHOP オスープ DHOP オスープ IP-4 DNS 設定 DHOP オスープ IP-4 DNS 設定 III(行いた 記県	24(アンパボア アドレスを DKP サーバーから 取得する場、WBC サーバーの P アドレス 20 DKP オフショ 24 クイアンドに 健康 そきます。ここで 確定には 設立に ひゃう を使用するウイアンドに 嫌用されます。 (* このネットワーク上のアウリーシェムに WPOS が 必要(3) の このネットワーク上のアウリーン 24 には WPOS が 必要(3) の たくりークト このアウリウーン 24 には WPOS が 心要(3) の たり やく には 55 さ うくび スロンゴ かど明にないます。これらの WPOS サーバー (4, この の 20 ケーバーの P アドレス(2) (* WPOS サーバーの P アドレス(3)
	<前へ(D) 法へ(N) > インストール(D) キャンセル

図 2.2-53 DHCP サーバのインストール 6

 「DHCP スコープの追加または編集」画 面にて右上の「追加」をクリックする。

	役割の追加ウィザード		×
開始する前に サーバーの検討 DHCP サーバーの検討 DHCP サーバーの検討 EP4 0K5 助定 DHCP サーバーの検討 EP4 0K5 MCC DHCP サーバーの検討 EP4 0K5 MCC DHCP 0K5 0K5 DHCP サーバーの検討 EP4 0K5 MCC DHCP 0K5 0K5 DHCP 0K5	INCP 73-700	自加または編集	
	間続する前に サーバーの役割 DHOP サーバー ネットワーク採用しバインディング IPv4 DHS 設定 CHSP スシーブ DHOP 40 ステートレスモード IPv6 DHS 設定 DHOP サーバーの承認 超望 道行状況 総単	スコープは、シャリクークで使用可能とおり下したの範囲です。スコープが作いたされるまで、DHCP サーバーは アンドンないライアンドは送与するとごができません。 スコープス 通知(4) 「 「アンドンの範囲」 通知(4) 「 「日本 アンドンの範囲」 通知(4) 「 「日本 アンドンの範囲」 通知(4) 「 「日本 中ンドーズの範囲」 通知(4) 「 「日本 中ンドーズの範囲」 「日本 中ンドーズ フロパライ 「 スコープの通知の意味は選択すると、そのスコープのプロパライが表示されます。 スコープの通知の意味面 「コープの通知の意味面」 く 第へ(19) パシストーッドの」	

図 2.2-54 DHCP サーバのインストール7

 ⑧ ネットワーク環境に合わせた DHCP 設定 を入力し、「このスコープをアクティブ化 する」にチェックが入っているのを確認 し、「OK」をクリックする。(本ガイドで は右図の様に設定しています)

(Windows Server 2008 では少し表示が 異なります)

スコープの追加	X
スコープとは、ネットワークで使用可能な DHCP サーバーは IP アドレスをクライア	↓ IP アドレスの範囲です。スコープが作成されるまで、 プントに配布することができません。
- DHCP サーバーの構成設定 スコープ名(S):	VLAN100
開始 IP アドレス(<u>T</u>):	192.168.100.100
終了 IP アドレス(<u>E</u>):	192.168.100.200
サブネットの種類(B):	ワイヤード(有線 - リース期間は 8日)
✓ このスコープをアクティブ化する(A)	
└─DHCP クライアントに伝達する構成設	定
サブネット マスク(<u>U</u>):	255.255.255.0
デフォルト ゲートウェイ (オプション) (D):	192.168.100.254
	OK キャンセル

図 2.2-55 DHCP サーバのインストール 8

⑨ 内容が反映されていることを確認し、「次 へ」をクリックする。



図 2.2-56 DHCP サーバのインストール 9

10 「このサーバーに対する DHCPv6 ステー トレスモードを無効にする」にチェック を入れ、「次へ」をクリックする。



図 2.2-57 DHCP サーバのインストール 10

「DHCP サーバーの承認」 画面で、「現在 (11)の資格情報を使用する」を選択して、「次 へ」をクリックする。



図 2.2-58 DHCP サーバのインストール 11

設定した内容を確認し、「インストール」
 をクリックする。



図 2.2-59 DHCP サーバのインストール 12

インストールの結果を確認して、「閉じる」をクリックする。



図 2.2-60 DHCP サーバのインストール 13

※ インストールウィザードにてスコープを1つ作成しました。

スコープを追加作成する場合、「スタート」→「管理ツール」→「DHCP」を開き、新しいス コープウィザードを再度実行して下さい。

また既存のスコープを右クリックしてプロパティを開く事により、詳細なオプションを設定 する事が可能です。

2.2.6. インストール内容の確認

サーバーマネージャ画面にて、追加した各役割が存在することを確認します。



図 2.2-61 インストールの確認

以上で、Windows Server 2008 R2 を RAIDUS サーバとして使用するために必要な役割のインストール は完了です。

3. IEEE802.1X 認証の設定

本ガイドにて設定する認証方式は EAP-TLS、EAP-PEAP です。またサプリカントでは Windows ドメ インに参加し SSO(Single Sign-On)を構成する方法を記載しています。

3.1. サーバの設定

3.1.1. ユーザー、グループの作成

 「サーバーマネージャー」→「役割」→ 「Active Directory ドメインサービス」→ 「Active Directory ユーザーとコンピュー タ」から作成したドメインを展開し、 「Users」を右クリックして「新規作成」 →「ユーザー」を選択する。

サーバー マネージャ					
ファー{ノレ(F) 陳作(A) 表:	i(V) ΛJIJ(H)				
• • 2 🖬 X 🗈	X 🛛 A 🕞 🛛 🖷				
、サーバー マネージャ (DC)		Users 20 @0t#30+	うト [フィルタ アクティブ]		12/1
- 😰 絵劇		(5.6) 9920	1918	1	Users
(a) (a) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	P440 サージス wg ユーザー・エンピュータ [DCea wg ユーザー・エンピー マーザー・エンピュータ [DCea wg ユーザー・エンピー マーザー・エンピー マーザー・エンピー マーザー マー	Skill 1983 S. Advances of 20. """" S. Advances of 20. """ S. Advances of 20. """ S. Carl Advances """	L247 L247 L247 L247 L247 L257 L25 L25		berr berr
Louis did - bil down i store				A1 4	40

図 3.1-1 ユーザーグループの設定1

- ウィザードが開始されたら、下記の値を
 入力し、「次へ」をクリックする。
- ・姓:任意(本ガイドでは、「user1」)
- •フルネーム:任意

(姓を入力すると同時に反映される)

・ユーザーログオン名:任意
 (姓と同一にする)

新しいオブジェクト - ユーザー	•	×
🤱 作成先:	example.co.jp/Users	
救生(<u>し</u>):	user1	
名(<u>F</u>):	イニシャル(1):	
フル ネーム(<u>A</u>):	user1	
ユーザー ログオン名(<u>U</u>) user1	@example.co.jp	
ユーザー ログオン名 (W	indows 2000 より前)(<u>W</u>):	
EXAMPLE¥	user1	
		_
	< 戻る(B) 次へ(N) > キャンセル	

図 3.1-2 ユーザーグループの設定 2

 パスワードを入力し、「次へ」をクリック する。

新しいオブジェクト - ユーザー	×
🙎 作成先: example.co.jp/Users	
パスワード(P): パスワードの確認入力(<u>C</u>):	
, □ ユーザーは次回ログオン時にパスワード変更が必要(M) □ ユーザーはパスワードを変更できない(S)	
ア パスワードを無期限にする(₩) アカウントは無効(0)	
< 戻る(B) 次へ(N) >	キャンセル

図 3.1-3 ユーザーグループの設定3

④ 確認し、「完了」をクリックする。

新しいオブジェクト - ユーザー	×
🤱 作成先: example.co.jp/Users	
[完了] をクリックすると、 次のオブジェクトが作成されます:	
フル ネーム: user1	<u> </u>
ユーザー ログオン名: user1@example.co.jp	
パスワードを無期限にする	
	T
)	
< 戻る(<u>B</u>)	キャンセル

図 3.1-4 ユーザーグループの設定 4

⑤ グループの作成 画面左の「Users」を右クリックして「新 規作成」→「グループ」を選択する。



図 3.1-5 ユーザーグループの設定 5
⑥ グループ名(本ガイドでは、「SALES」)を入力し、「OK」をクリックする。

新しいオブジェクト - グループ	×	
经作成先: example.co.jp/Users		
グループ名(<u>A</u>):		
SALES		
グループ名 (Windows 2000 以前)(W):		
SALES		
「グループのスコープ」		
○ ドメイン ローカル(②) ○ セキュリティ(S)		
 グローバル(G) 配布(D) 		
OK キャンセル		
図 3.1-6 ユーザーグループの設定 6		

 ⑦ サーバーマネージャ画面にて、先程作成 したユーザー(user1)を選択し、右クリ ックしてプロパティを開く。プロパティ 画面にて「所属するグループ」タブを選 択し、「追加」をクリックする。

user1ወታዐパティ <u>? ×</u>			
環境 セッション リモート制御 ターミナル サービスのブロファイル COM+ フリガナ 全般 住所 アカウント ブロファイル 電話 組織 所属するグループ ダイヤルイン			
所属するグループ(M):			
名前 Active Directory ドメイン サービス フォルダ			
Domain Users example.co.jp/Users			
<u>〔〕〕置力の〔〕〕〕</u>			
プライマリ グループ: Domain Users			
ブライマリ グループの設定(S) グライマリ グループの設定(S) がない場合は、プライマリ グループを変更する 必要はありません。			
OK キャンセル 適用(<u>A</u>) ヘルプ			
図 3.1-7 ユーザーグループの設定7			

 ⑧ グループの選択画面にて、選択するオブ ジェクト名に先程作成したグループ名 (本ガイドでは「SALES」)を入力し、「名 前の確認」をクリックして、「OK」をク リックする。

<u>? ×</u>
オブジェクトの種類(の)
場所(<u>L</u>)
名前の確認(<u>C</u>)
++>\tell

図 3.1-8 ユーザーグループの設定8

⑨ 「所属するグループ」内に指定したグル ープが追加されている事を確認する。



図 3.1-9 ユーザーグループの設定 9

 プロパティ画面にて「ダイヤルイン」タ ブを選択し、「リモートアクセス許可」を 「アクセス許可」にチェック、「OK」を クリックする。

user10วิธฺ/วิรา
□ 環境 セッション リモート制御 ターミナル サービスのプロファイル COM+ フリガナ 全般 住所 アカウント プロファイル 電話 組織 所属するグループ ダイヤルイン
リモートアクセス許可
○ アクセスを許可(W)
○ アクセスを拒否(D)
○ NPS ネットワーク ポリシーでアクセスを制御(P)
○ 発信者番号を確認(⊻):
「コールバック オブション
○ 呼び出し元による設定 (ルーディングビリモート アクセス サービスのみ入当)
○ 市に次の電話番号にコールハック①:
- 「 静的 IP アドレスを割り当てる(1)
このダイヤルイン接続に対して有効にする IP アド レスを定義してください。
□ 静的ルートを適用(图)
このダイヤルイン接続に対して有効にするルートを定 静的ルート(U) 義してください。
OK キャンセル 道用(A) ヘルプ

図 3.1-10 ユーザーグループの設定 10

3.1.2. NPS の設定

(1) サーバの登録

「スタート」→「管理ツール」→「ネットワークポリシーサーバー」を開く。
 左画面の「NPS(ローカル)」を右クリックし、「Active Directory にサーバを登録」
 をクリックする。



図 3.1-11 NPS の設定 1

 下記メッセージが表示される。「OK」を クリックする。 ネットワーク ポリシー サーバー

NPS が Active Directory のユーザーを認証できるようにするには、NPS を実行しているコンピュータがユーザーのダイヤルイン プロパティをドメインから読み取る権限を持っている必要があります。
ユーザーのダイヤルイン プロパティを example.co.jp ドメインから読み取る権限をこのコンピュータに与えますか?

OK キャンセル

図 3.1-12 NPS の設定 2

 下記メッセージが表示される。「OK」を クリックする。



図 3.1-13 NPS の設定 3

(2) RADIUS クライアントの作成

 「サーバーマネージャ」→「役割」→「ネ ットワークポリシーとアクセスサービ ス」→「NPS (ローカル)」→「RADIUS クライアントとサーバー」→「RADIUS クライアント」を右クリックし、「新規」 を選択する。

1.サーバー マネージャー	_ [] X
ファイル(F) 操作(A) 表示(V) ヘルプ(H)	
🍬 🔿 🔁 🖬 📓 🖬	
● 10年 ● 104	時代 RADERS タフ. ▲ 新規 一覧位立2. 表示 → 後時50後. 译 へルブ
図 3.1-14 RADIUS クライアントの設定 1	

- ② 新規 RAIDUS クライアント画面にて、下記3項目を入力して、「OK」をクリックする。
 ・フレンドリ名:任意のフレンドリ名
 - (本ガイドでは、「AX24」)
 - •アドレス:認証スイッチの IP アドレス (本ガイドでは、「172.16.0.11」)
 - ・共有シークレット:認証スイッチにて 設定したシークレットキー

(本ガイドでは「alaxala」)

新しい RADIUS クライアント	×
設定 詳細設定	
▼ この RADIUS クライアントを有効にする(E)	
■ 既存のテンプレートを選択する(1):	
v	
- 名前とアドレス	
AX24	
アドレス (IP または DNS)(<u>D</u>):	
172.16.0.11 確認(少	
共有シークレット 既存の共有シークレット テンプレートを選択(M)	
共有シークレットを直接入力する場合は [手動] をクリックし、自動で生成する場合は [生成] をクリックします。ここに指定した共有シークレットを、RADIUS クライアントの構 成時にも指定する必要があります。共有シークレットでは大文字と小文字が区別され ます。	
● 手動(U) ○ 生成(G)	
共有シークレット(S):	
共有シークレットの確認入力(②):	
OK キャンセル	

図 3.1-15 RADIUS クライアントの設定 2

(3) ネットワークポリシーの作成

- ネットワークポリシーの作成手順を以下に示します。
 - (a) <u>条件の設定</u>
 - (b) <u>認証方法の構成</u>
 - (c) <u>設定の構成</u>
 - (d) <u>ネットワークポリシーの確認</u>
- (a) 条件の設定
- 「サーバーマネージャ」→「役割」→「ネ ットワークポリシーとアクセスサービ ス」→「NPS(ローカル)」→「ポリシ ー」→「ネットワークポリシー」を右ク リックし、「新規」をクリックする。



 ④ 任意のポリシー名(本ガイドでは 「802.1xSALES」)を入力、必要に応じ てネットワークアクセスサーバーの種 類を選択し、「次へ」をクリックする。



図 3.1-17 条件の設定 2

③ NAS ポートの種類

「条件の指定」画面にて右下「追加」を クリックし、「条件の選択」画面にて 「NAS ポートの種類」を選択し、「追加」 をクリックする。

条件の選択	×
条件を選択し、[追加] をクリックします。	
被野電素 ID 検呼電素 ID の条件には、ネットワーク アクセス サーバー (NAS) の電話番号を文字列です 旗が電素 ID の条件には、ネットワーク アクセス サーバー (NAS) の電話番号を文字列です 旗ができます。	指定します。パターン マッチングの ▲
NAS ID NAS ID の条件は、ネットワーク アクセス サーバー (NAS) の名前である文字列を指定しま て NAS 名を指定できます。	す。パターン マッチ構文を使用し
NAS IPv4 アドレス NAS IP アドレスの条件は、NAS の IP アドレスである文字列を指定します。パターン マッチ を指定できます。	構文を使用して IP ネットワーク
NAS IPv6 アドレス NAS IPv6 アドレスの条件は、NAS の IPv6 アドレスである文字列を指定します。パターン トワークを指定できます。	マッチ構文を使用して IPv6 ネッ
№5 ホートの使知の条件は、アナログ電話回線、ISDN、トンネルまたは仮想フライベート いス、あよびイーサネット、入イッチなど、アクセス、クライアントが使用するメディアの優調を指定	ネットワーク、IEEE 802.11 ワイヤ
	追加(D) キャンセル



- 1

 ④ NAS ポートの種類画面にて、一般的な 802.1X 接続トンネルの種類の中から 「Ethernet」をチェックして、「OK」を クリックする。

NAS ホートの種類 🛛 🗡 🗡		
このポリシーに一致するために必要なアクセス メディアの種類を指定します。 一般的なダイヤルアップおよび VPN トンネルの種類(D)		
Async (Modem) ISDN Sync Sync (T1 Line)		
Virtual (VPN) 一般的な 802.1X 接続トンネルの種類(≥)		
Ethernet FDDI Token Ring Wireless - IEEE 802.11		
その他(T) ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation ADSL-DMT - Asymmetric DSL Discrete Multi-Tone Async (Modem)		
OK キャンセル		

図 3.1-19 条件の設定 4

 条件欄に「条件=NAS ポートの種類、 値=Ethernet」が追加されていることを 確認する。

新しいネットワーク ポリシー
条件の指定 揺続要求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。少なども 1 つの条件が必 要です。
条件(<u>C</u>):
条件 値
🤝 NAS ポートの種類 Ethernet
条件の見9月 NAS ボートの種類の条件は、アナログ電話回線、ISDN、トンネルまたは仮想プライベート ネットワーク、IEEE 802.11 ワイヤレス、およびイーサ ネット スイッチなど、アクセス クライアントが使用するメディアの種類を指定します。
<u>道加(D).</u> 編集(E). 削除(E)
前へ(P) 次へ(N) 完了(F) キャンセル
図 3 4 30 冬州の弐中 5

図 3.1-20 条件の設定 5

⑥ Windows グループ

さらに「条件の指定」画面で「追加」を クリックし、条件の選択画面にて 「Windows グループ」を選択し、「追加」 をクリックする。

촜	作の選択	×
	条件を選択し、「追加」をクリックします。	
	グループ	
	Windows グループ Windows グループの条件は、接続ユーザーまたは接続コンピュータが選択されたグループのいずれかに所属している必要が あるととを指定します。	
	コンピュータグループ コンピュータグループの条件は、接続するコンピュータが選択したグループのいずれかに届している必要があることを指定しま	
	ユーザーグループ ユーザーグループの条件は、接続ユーザーが選択されたグループのいずれかに所属している必要があることを指定します。	
	HCAP	
	ロケーショングループ HGAP ロケーショングループの条件には、このポリシーに一致するために必要な HCAP (Host Oredential Authorization Protocol ロケーショングループを指定します。HCAP プロトコルは、NFS と一部のサード パーティ製ネットワーク アクセス サーバー (NAS) との間の通信で使用されます。この条件を使用する前に NAS のドキュメントを参照してください。	•
	<u> 這知(D)</u> キャンセ	JL



 ⑦ Windows グループ画面にて「グループ の追加」をクリックする。
 グループの選択画面にて、選択するグル ープ名を入力し「名前の確認」をクリッ クして、「OK」をクリックする。

グループ の選択	<u>? ×</u>	
オブジェクトの種類を選択してください(<u>S</u>): グループ	オブジェクトの種類(<u>O</u>)	
場所を指定してください(<u>F)</u> : example.co.jp	場所(」)	
選択するオブジェクト名を入力してください (例)(E): SALES	名前の確認(<u>C</u>)	
网。4.00 名供办訊中,2		

図 3.1-22 条件の設定 7

⑧ Windows グループ画面にて、選択した グループが追加されていることを確認 し、「OK」をクリックする。

Windows グルー	プ		X
このポリシーに一	・致するために必要なグループ	メンバシップを指定(<u>S</u>)	
グループ EXAMPLE¥S	ALES		-
[グループの追加(<u>U</u>)	〕 削除(<u>M)</u> OK キャンセル	

図 3.1-23 条件の設定 8

 条件欄に「条件=Windows グループ、 値=選択したグループ名」が追加されて いることを確認し、「次へ」をクリック する。



⑦ アクセス許可の指定
 「アクセスを許可する」をチェックして、
 「次へ」をクリックする。

新しいネットワー	りポリシー	×
	アクセス許可の指定 接続要求がこのポリシーに一致する場合に、ネットワーク アクセスを許可するかまたは拒否するかを構成します。	
 アクセスを許 クライアントの アクセスを拒 クライアントの 	・可する(Δ))接続試行がこのポリシーの条件に一致する場合、アクセスを許可します。)否する(D))接続試行がこのポリシーの条件に一致する場合、アクセスを拒否します。	
「 ユーザー ダー クライアントの	イヤルイン プロパティ (NFS ポリシーよりも優先をれる) によってアクセスを判断する(S))接続時行がこのポリシーの条件に一致する場合、ユーザー ダイヤルイン プロパティに応じてアクセスを許可または拒否します。	
	前へ(P)	

図 3.1-25 条件の設定 10

(b) 認証方法の構成

ここでは、RADIUS サーバで認証許可する EAP の種類の設定を行います。 使用する EAP の種類(①PEAP、②TLS)によって手順を進めて下さい。PEAP と TLS の両方を許 可する場合は、①、②の手順両方を実施して下さい。

① PEAP の場合

「追加」をクリックし、EAP の追加画面 で「Microsoft:保護された EAP (PEAP)」 を選択し、OK。

EAP の種類に追加された「Microsoft : 保 護された EAP (PEAP)」を選択し、「編 集」をクリックする。

保護された EAP プロパティの編集画面 にて、該当するサーバ証明書が選択され ている事を確認し、「OK」で閉じる。

※ 保護された EAP プロパティの編集画面が表示されない場合、Active Directory 証明書サービスからサーバ証明書の取得に失敗しているか、もしくはサーバ証明書が発行されていない可能性があります。

新しいキットワーク ポリラー 認証方法の構成 接続要求が、のポリラーの条件を満たすたがに必要な認証 提該指定する必要があります。税格要求ポリラーは、 を LAP を指定する必要があります。税格要求ポリラーは、	メ 方法を、1つ以上指定してください。EAP IZEEには、EAP の または VPNを開閉する場合は、接続要求ポリシーに存譲され ネットワーク ポリシーの記録証録定よりも優先されます。
EAP の種類は、NPS とクライアントとの間で、表示されている順序でネゴシェー EAP の種 類(T): Microsoft (保護された EAP (PEAP)	とれます。 正へ移動(U) 下へ移動(W) (Paまれた CaD 1016-2016年
注助加(D) 編集(E) 削除(R) セキュリティレベルの低い認証方法: ✓ Microsoft 暗号化認証が一ジョン 2 (MS-CHAP v2\\/) ジ / パスワードの規範が切れた後も、ユーザー(プ\/スワードの変更を許可す 「「「「「「「スワードの規範が切れた後も、ユーザー(プ\/スワードの変更を許可す 「「「「「「「」」」、「」、「スワードの変更を許可す 「「「「「」」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」	またないたことAF / 20/574/0/=3-6
	<u></u>

図 3.1-26 認証方法の構成1

TLS の場合

「追加」をクリックし、EAP の追加画面 で「Microsoft:スマートカードまたはそ の他の証明書」を選択し、OK。 EAP の種類に追加された「Microsoft:ス マートカードまたはその他の証明書」を 選択し、「編集」をクリック。 スマートカードまたはほかの証明書のプ ロパティ画面にて、該当するサーバ証明 書が選択されている事を確認し「OK」を クリックする。



③ EAP の種類に追加されていることを確認し、「次へ」をクリックする。
 (本ガイドでは以下のように EAP の種類に PEAP と TLS の両方許可する設定としています。)

新しいネットワー	-ク ポリシー <u>×</u>
	認証方法の構成 接続要求がこのポリシーの条件を満たすために必要な認証方法を、1 つ以上指定してください。EAP 認証には、EAP の 種類を指定する必要があります。NAP を使用する 802.1X または VPN を展開する場合は、接続要求ポリシーに1条膜され た EAP を指定する必要があります。接続要求ポリシーは、ネットワーク ポリシーの認証設定よりも優先されます。
EAP の種類は	、NPS とクライアントとの間で、表示されている順序でネゴシェートされます。 (T):
Microsoft 7	マートカードまたはその他の証 担明書 集錬された EAP (PEAP) 「下へ移動(近)
 追加(D)- セキュリティし マ パスワー マ パスワー マ パスワー 暗号化認 ご 暗号化認 ご 暗号化認 ご 認証方法: □ ンピュー5 	福東(印) 前形代化 レベルの低い認証方法: 明号化に認証バージュン2 (MS-CHAP v2)(y) ードの期限が切れた後も、ユーザー(こパスワードの変更を許可する(出) 暗号化に認証(MS-CHAP)(y) ードの期限が切れた後も、ユーザー(こパスワードの変更を許可する(z) 証(CHAP)(2) ハマにないな認証(PAP, SPAP)(S) をネイジェートセず(こクライアントに接続を許可する(L) ターの正常性チェックのみを実行する(M)
	前へ(P) 次へ(W) 完了(B) キャンセル

図 3.1-28 認証方法の構成 3

4 制約の構成
 必要な設定がある

必要な設定がある場合は設定し、「次へ」 をクリックする。

新しいネットワーク ポリシー	×.
制約は、接続要求 合、NPS は接続要 さい。	が一致する必要がある、ネットワーク ポリシーの追加パラメータです。接続要求が制約と一致しない場 求を自動的に拒否します。制約はオプションです。制約を構成しない場合は、じたへ」をクリックしてくだ
このネットワーク ポリシーの制約を構 すべての制約が接続要求に一致した	ちします。 (い場合、ネットワーク アクセスは拒否されます。
 1985): 1985) 2745ルタイムアウト 29ションタイムアウト 20ションタイムアウト 20日本語名の単の 20日本語名の単の 20日本語名の単の 21日本語名の単の 22日本語名の単の 	サーバーがアイドル状態になってから接続が切断されるまでの最大時間を分単位で指定します
	前へ(2) 次へ(1) 完了(2) キャンセル

図 3.1-29 認証方法の構成 4

(c) 設定の構成

ここでは、下記3つの認証後アトリビュートの設定を行います。固定 VLAN モードの場合は、本手順を省略して下さい。

- Tunnel-Medium-Type = "802"
- ・Tunnel-Pvt-Group-ID="100"(認証後 VLAN ID)
- Tunnel-Type= "VLAN"
- ① 「追加」をクリックする。

新しいネットワーク ポリシー	×
設定の構成 ポリシーのすべてのネッ	トワーク ボリシー条件および制造が一致した場合、NPS は接続要求に対して設定を適用します。
このネットワークボリシーの設定を構成し 条件と制約が接続要求に一致してアク	ょす。 セスガは中可される場合、この設定が通用されます。
RADILS 置性 後期 二 ペング回海 キャワークアウセス保護 ● NAP 登曲目 型 拡張状状態 ルーティングビリモートアクセス ご マルチリンクおよび茶城 (EAFI)当てフトコルル (EAFI)当てフトコルル 日 アイルタ ご IP 設定	追加腐性を RADIUS クライアントに達信するには、標準 RADIUS 歴性を選択し、[編集] を切っりします。腐性を補成しないと、腐性は RADIUS クライアントに逆信されません。必要 を腐性については、RADIUS クライアントのドキュメントを参照してください。 雷性(I): 名前 信 Framed-Protocol PPP Service-Type Framed 道知(D)_ 編末(日) 可珍(日)
	前へ(P) 法へ(N) 完了(P) キャンセル

図 3.1-30 設定の構成1

 標準 RADIUS 属性の追加画面にて 「Tunnel-Medium-Type」を選択し、「追 加」をクリックする。

標準 RADIUS 属性の追加	×
属性を設定に追加するには、属性を選択し、[追加] をクリックしてください。	
独自または定義済みのベンダ固有属性を追加するには、このダイアログ ボックスを開けて [ベンダ固有] を選択し、 [Ji 加] をグリックしてください。	
アクセスの種類(I):	
রু বিশ্ব	
■性(E): 名前 Turnel-Client=Endpt Turnel-Password Turnel-Preference Turnel-Preference Turnel-Server-Auth-ID Turnel-Server-Auth-ID	1
」 説明: 複数のトランスポートで運用できるブロトコル (L2TP など) のトンネルを作成するときに使うトランスポート メディアを指定 します。	
<u>追加(A)</u> 開じる(C)	

図 3.1-31 設定の構成 2

③ 属性の情報画面にて「追加」をクリック し、「802.1x で一般的に使用する」にチ ェックし、「802」を選択して、「OK」を クリックする。

属性の情報	×
属性名: Tunnel-Medium-Type	
属性の番号: 65	
属性の形式: Enumerator	
属性值:	
● 802.1×で一般的に使用する(M)	
802 (includes all 802 media plus Ethernet canonical format)	•
 その他(Q) 	
	-
OKキャンセル	,

図 3.1-32 設定の構成 3

 ④ 属性の情報画面にて、「ベンダ= RADIUS Standard、値=802」が追加されていることを確認し、「OK」をクリックする。

属性の情報	×
属性名: Tunnel-Medium-Type	
周性の番号: 65	
属性の形式: Enumerator	
属性値(<u>T</u>):	
ベンダー「値」	追加(<u>A</u>)
RADIUS Standard 802 (includes all 802 media plus	編集(E)
	削除(<u>R</u>)
	上へ移動(山)
	下へ移動(D)
OK	キャンセル

図 3.1-33 設定の構成 4

⑤ 「追加」をクリックし、標準 RADIUS
 属 性 の 追 加 画 面 に て
 「Tunnel-Pvt-Group-ID」を選択し、「追
 加」をクリックする。

標準 RADIUS 属性の追加	×
属性を設定に追加するには、属性を選択し、[追加] をクリックしてください。	
独自または定義済みのベンダ固有属性を追加するには、このダイアログ ボックスを閉じて [ベンダ固有] を選択し、「自加」をクリックしてください。	
アクセスの種業(I):	
বন্দের 🔽	
周性(B): 名前 Tunnel-Password Tunnel-Preference Tunnel-Server-Auth-ID Tunnel-Server-Endpt	
Tunnel-Type	J
[災□月:	
トンネル セッションのグループ ID を指定します。	
_ 注意力((<u>A</u>) 開いる(<u>C</u>)	

図 3.1-34 設定の構成5

⑥ 属性の情報画面にて「追加」をクリック
 し、認証後の VLAN ID(本ガイドでは
 「100」)を入力して、「OK」をクリック
 する。

属性の情報	×
属性名: Tunnel-Pvt-Group-ID	
属性の番号: 81	
属性の形式: OctetString	
入力する値の形式(<u>E)</u> : ⓒ 文字列(<u>S</u>) 〇 16 進数(<u>H</u>)	
100	
	OK キャンセル

図 3.1-35 設定の構成6

 ⑦ 属性の情報画面にて、「ベンダ= RADIUS Standard、値=100」が追加されていることを確認し、「OK」をクリックする。

属性の情報	×
属性名: Tunnel-Pvt-Group-ID	
属性の番号: 81	
属性の形式: OctetString	
属性値(<u>T</u>):	
ベンダー 値	追加(<u>A</u>)
RADIUS Standard 100	編集(<u>E</u>)
	削除(<u>R</u>)
	上へ移動(山)
	下へ移動(D)
ОК	キャンセル

図 3.1-36 設定の構成7

 ⑧ 標準 RADIUS 属性の追加画面にて 「Tunnel-Type」を選択し、「追加」をク リックする。

標準 RADIUS 属性の追加	×
属性を設定に追加するには、属性を選択し、[追加] をクリックしてください。	
独自または定義済みのベンダ固有属性を追加するには、このダイアログ ボックスを閉じて [ベンダ固有] を選択し、 6自 加] をクリックしてください。	
アクセスの種業類(工):	
বশ্ব	
居性(B): 名前 Tunnel-Password Tunnel-Preference Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Server-Endpt Tunnel-Type ▼	
使用されるトンネリング プロトコルを指定します。	
〕追加(<u>A</u>) 閉じる(©)	

図 3.1-37 設定の構成 8

⑨ 属性の情報画面にて「追加」をクリックし、「802.1x で一般的に使用する」をチェックし、「Virtual LANs(VLAN)」を選択して、「OK」をクリックする。

属性の情報	×
属性名: Tunnel-Type	
属性の番号: 64	
属性の形式: Enumerator	
属性值:	
○ ダイヤルアップまたは VPN で一般的に使用する(C)	
くなし>	~
○ 802.1×で一般的に使用する(M)	
Virtual LANs (VLAN)	-
○ その他(Q)	
くなし>	~
OK **>	ยม
図 3.1-38 設定の構成 9	

 属性の情報画面にて、「ベンダ= RADIUS Standard、値=Virtual LANs (VLAN)」が追加されていることを確認 し、「OK」をクリックする。

属性の情報				×
属性名: Tunnel-Type				
属性の番号: 64				
属性の形式: Enumerator				
属性値(<u>T</u>):				
ベンダ	値		追加(<u>A</u>)	
RADIUS Standard	Virtual LANs (VLAN)		編集(E)	
			削除(<u>R</u>)	
			上へ移動(山)	
			 下へ移動(<u>D</u>)	
		OK	الطريحية [
		OK	<u>+77771</u>] [
		· 4 ++ 1	-	

図 3.1-39 設定の構成 10

追加したアトリビュートが反映されていることを確認し、「次へ」をクリックする。



① 新しいネットワークポリシーの内容を
 確認して、「完了」をクリックする。

しいネットワーク ポリシー	×
「「「」「」「」「」「」」「」」「」」「」」「」」「」」「」」」「」」」「	-りポリシーの完了
次のネットワーク ポリシーが正常に作り 802.1×SALES	成されました:
ポリシー条件:	
条件 値	
NAS ポートの種類 イーサネット	
Windows グループ EXAMPLE¥SA	LES
L	
ポリシー設定:	
[条件	値
認証方法	EAP または MS-CHAP v1 または MS-CHAP v1 (パスワードの期限が切れた後、フ
アクセス許可	アカヤスを許可する
非進抑クライアントの更新	True
NAP CASE	完全なネットワークアクセスを許可する
Framed-Protocol	PPP
Service-Type	Framed
このワイサードを閉じるには、「完了」を	クリックし (イだき()。
	前へ(P) 次へ(h) 完了(E) キャンセル
	図 3 1-41 設定の構成 12

- (d) ネットワークポリシーの確認
- サーバーマネージャ画面にて、新しいポ リシーが反映されていることを確認す る。

サンドーマネンジー(CC) マンド・マンジー(CC) マンド・マンジー(CC) マンジー(CC) マンジー(CC)	<u>ワークネー</u> 新一覧の立う。 売売 最新の体。 小ルブ

図 3.1-42 ネットワークポリシーの確認

3.1.3. Web サーバ(IIS)の設定

IEEE802.1X 認証に TLS を使用する場合クライアント端末にユーザーの証明書が必要です。本ガイド ではクライアント端末からのユーザー証明書取得方法として Web サーバ(IIS)の「証明書サービス Web 登録」機能を使用します。これによりクライアント端末はブラウザを用いて CA からユーザー証明書を発 行してもらうことが可能となります。

Windows Sever 2008 R2 の「証明書サービス Web 登録」でユーザー証明書を取得する場合、HTTPS でのアクセスが必須となっています。「証明書サービス Web 登録」機能自体は必要な役割をインストールした時点で動作していますが、ここでは本サービスが SSL を使用して動作するように設定する手順を以下に示します。

なお本設定は IEEE802.1X 認証の EAP の種類に TLS を使用し、且つ Web サーバ(IIS) を Windows Server 2008 R2 にて構築する場合のみ必要です。Web サーバ(IIS) を Windows Server 2008 で構築する場合は本設定を行わなくても HTTP アクセスによるユーザー証明書の取得が可能です。

 「スタート」→「管理ツール」→「サー バーマネージャー」を開く。左画面の「役 割」を展開し、「Web サーバ(IIS)」を展 開し「インターネットインフォメーショ ンサービス(IIS)マネージャー」を選択 してください。



図 3.1-43 Web サーバ(IIS)の設定 1

 (2)「接続」画面を展開して「Default Web Site」を右クリックして「バインドの編集」 をクリックしてください。



図 3.1-44 Web サーバ (IIS) の設定 2

- ③ 「サイトバインド」の画面で「追加」を クリックし「サイトバインドの追加」画 面を以下のように入力してください。入 力後「閉じる」をクリックしてください。
 - 種類:"HTTPS"を選択
 - IP アドレス: "未使用の IP アドレス すべて"を選択
 - ポート:443を指定
 - SSL 証明書:サーバー証明書 (本ガイドでは "dc.example.co.jp")
 を選択

サイト バインド			?×
種類 ホスト名 オ	R—К IP 7КИХ	バインド 通	3力D(A)
http 8	U *	桶	扁集(E)
		ļ.	训除余(R)
		1	b照(B)
•		Þ	
		E E E E E E E E E E E E E E E E E E E	月じる(C)
サイトバインドの追加		<u>?</u> ×	
種類(T): IP アドレス(I):	, , , , , , , , , , , , , , , , , , ,	°−ト(0):	
https ▼ 未使用の IP .		443	
ホスト名(H):			
」 SSL 証明書(S):			
dc.example.co.jp	表示	i(V)	
	ОК	キャンセル	

図 3.1-45 Web サーバ (IIS) の設定 3

④ 接続画面の「Default Web Site」を展開し
 「Cert Srv」を選択、「/CertSrv ホーム」
 画面の「SSL 設定」をダブルクリックし
 てください。



図 3.1-46 Web サーバ(IIS)の設定 4

⑤「SSL 設定」画面にて「SSL が必要」をチ ェックし、「クライアント証明書」の項目 は「無視」をチェックしてください。

SSL 設定
このページでは、Web サイトまたはアプリケーションの SSL 設定を変更することができます。
✓ SSL が必要(Q)
クライアント証明書:
⊙ 無視(1)
〇 受理(<u>A</u>)
〇 必要(<u>B</u>)

図 3.1-47 Web サーバ(IIS)の設定 5

※設定は以上です。「Default Web Site」を選択し画面右にある Web サイトの管理から「再起動」 をクリックしてください。以上で「証明書サービス Web 登録」機能は SSL で動作します。

3.2. クライアント端末の設定

本項目では、Windows OS に標準搭載されているサプリカント(IEEE802.1X 認証クライアント)の 設定方法について示します。Windows 7、Windows Vista 共に設定内容や手順に大きな違いはありませ ん。そのため本ガイドでは Windows 7 の設定画面にそって手順を示し、差分がある箇所のみ Windows 7、 Windows Vista 両方の設定方法を示しています。

3.2.1. ドメイン参加

本ガイドでは、ユーザー、コンピュータをドメインにて一元管理する構成で認証を実施しています。 なお、ワークグループ構成でも IEEE802.1X 認証を行うことは可能です。

- (1) 事前準備
 - サーバ(ドメインコントローラ)と通信が可能なネットワークに、対象のクライアント端末を 接続する。
 - TCP/IP の設定を行う。IP アドレス、ネットマスク、およびデフォルトゲートウェイの設定を 行う。優先 DNS サーバにはドメインコントローラの IP アドレスを指定する。
 - ドメインコントローラへ PING を実行して通信可能であることを確認する。
 また、DNS 設定の確認として、ドメイン名指定での PING も実行する。

(2) ドメイン参加手順

 「スタート」→「コンピュータ」を右クリ ックして「プロパティ」を選択、「コンピ ュータの基本的な情報の表示」にて画面右 にある「設定の変更」をクリックして「シ ステムのプロパティ画面」を表示して下さ い。さらに「システムのプロパティ画面内 の」「変更」をクリックして下さい

システムのプロパティ	
コンピューター名 ハードウェア	詳細設定 システムの保護 リモート
(人) 次の情報は、この	コンピューターをネットワーク上で識別するために使われます。
コンピューターの説明(<u>D</u>):	
	例: "キッチンのコンピューター"、"仕事用コンピューター"
フル コンピューター名:	nts-PC
ワークグループ:	WORKGROUP
ドメインまたはワークグループにき するには [ネットワーク ID] をク!	参加するためのウィザードを使用 ネットワーク ID(<u>N</u>)… リックしてください。
コンピューター名を変更したりド 更]をクリックしてください。	メインに参加したりするには「変」 変更(<u>C</u>)
	適用(A)

図 3.2-1 ドメイン参加1

② 「コンピュータ名/ドメイン名の変更」 画面の「次のメンバ」にて「ドメイン」 にチェックし、ドメイン名を入力。「詳細」 をクリックする。



図 3.2-2 ドメイン参加 2

③「DNS サフィックスと NetBIOS コンピュータ名」画面にて「このコンピュータのプライマリ DNS サフィックス」にドメイン名を入力し、「OK」をクリックして画面を閉じる。

DNS サフィックスと NetBIOS コンピューター名
このコンピューターのプライマリ DNS サフィックス(<u>P</u>): example.co.jp
☑ ドメインのメンバーシップが変更されるときにプライマリ DNS サフィックスを変更する(○) NetBIOS コンピューター名(<u>N</u>): NTS-PC
この名前は、古いコンピューターやサービスとの相互運用に使用されます。
OK ++>+211

図 3.2-3 ドメイン参加3

- ④ まもなく下記の画面が表示される。
 <u>3.1.1</u>で作成したユーザー名およびパス ワードを入力し「OK」をクリックする。
 - ※ 下記の画面が表示されない場合、ドメインコントロ ーラとの接続性を確認して下さい。



 端末のドメイン参加が許可された場合、 下記のメッセージが表示される。「OK」 をクリックして画面を閉じると、再起動 が促されます。



図 3.2-5 ドメイン参加5

 ⑥ 再起動後端末のログオンプロンプト画面 にて、ログオン先のドメイン名を確認し (本ガイドでは「EXAMPLE」)、<u>3.1.1</u>で 作成したユーザー名およびパスワードを 入力してログオンする。

user1
••••••
ログオン先: EXAMPLE 別のドメインにログオンするには
ユーザーの切り替え(₩)
図 3.2-6 ドメイン参加 6

(3) 確認方法

CA の証明書を取得している事を確認します。

 「スタート」→「コントロールパネル」→ 「インターネットオプション」を開き、「コ ンテンツ」タブを選択して「証明書」をク リックする。(カテゴリ表示されている場 合は一覧表示に変更すると「インターネッ トオプション」のアイコンが表示されま す。)

証明書画面にて「信頼されたルート証明機 関 」 タ ブ を 選 択 し 、「 発 行 者 = example-DC-CA (CA)」の証明書を確認 する。

			QC1W2981176 167	RC4 040 9E1 17E
発行先	発行者	有効期限	フレンドリ名	
🔄 Class 3 Public Pri	Class 3 Public Primar	2028/08/	VeriSign Class 3.	
🔄 Class 3 Public Pri	Class 3 Public Primar	2004/01/	VeriSign Class 3.	
🔄 Copyright (c) 1997	Copyright (c) 1997 Mi	1999/12/	Microsoft Timest.	
example-DC-CA	example-DC-CA	2015/01/	30	
Microsoft Authenti	Microsoft Authentico	2000/01/	Microsoft Authe	
Microsoft Root Cer	Microsoft Root Certifi	2020/12/	Microsoft Root	
NO LIABILITY ACC	NO LIABILITY ACCE	2004/01/	VeriSign Time St.	
ンポート(D) [エクスポー 明書の目的 すべて>	- ト(E)) 前時(B)]		〕詳細設定 表示(𝒴)

図 3.2-7 CA 証明書の確認

3.2.2. PEAP 設定

本項目では、PEAP を使用した IEEE802.1X 認証の設定方法を示します。 なお、本ガイドでは PEAP-MSCHAPv2 を使用した SSO(Single Sign-On)構成で認証を実施しています。

- ※今回作成したドメインユーザー(本ガイドでは "user1")には IEEE802.1X 認証の設定を変更する権限が無いため一度ログオフしてください。次にこのコンピュータの管理者権限のあるユーザーでドメイン(本ガイドでは "example.co.jp")ではなくこのコンピュータにログオンしてください。
- 「スタート」→「コントロールパネル」
 →「ネットワークと共有センター」→「ア ダプター設定の変更」を開き、該当する ネットワーク接続を右クリックして「プ ロパティ」を開く。
 プロパティ画面にて「認証」タブを選択

し、「IEEE802.1X 認証を有効にする」に チェックを入れ、EAPの種類に 「Microsoft : 保護された EAP(PEAP)」を 選択、「設定」をクリックする。



図 3.2-8 PEAP の設定 1 (Windows Vista)

Windows 7
ローカル エリア接続のプロパティ
ネットワーク 認証
このイーサネット アダプターに認証済みのネットワーク アクセスを提供するに は、このオプションを選択してください。
▼ IEEE 802.1× 認証を有効にする(N)
ネットワークの認証方法の選択(M):
Microsoft 保護された EAP (PEAP) ◆ 設定(S)
□ ログオンするたびに、この接続用の資格情報を使用する(<u>B</u>)
☑ 承認されていないネットワーク アクセスにフォールバックする(E)
追加の設定(D)
OK キャンセル

図 3.2-9 PEAP の設定 1 (Windows 7)

 保護された EAP のプロパティ画面にて 「サーバの証明書を検証する」にチェッ クし、「信頼されたルート証明機関」の 中から「example-DC-CA」をチェックす る。

「認証方法を選択する」の中から「セキ ュリティで保護されたパスワード (EAP-MSCHAPv2)」を選択し、「構成」 をクリックする。

保護された FAP のプロパ	Windows Vista	×
接続のための認証方法	×=T→7ΛΛ	
● ▼ サーハーの証明書を作	(teiliga(<u>v</u>)	
	.9 8/2/	
信頼されたルート証明機	期(<u>R</u>):	
Class 3 Public Prin	mary Certification Authority	
GTE Cyber Trust G	ilobal Root	
Microsoft Root Au	thority rtificate Authority	
Thawte Timestamp	bing CA	
□ I □ 新しいサーバーまたは ない(P)	は信頼された証明機関を承認するようユ	ーザーに求め
認証方法を選択する(<u>S</u>):		
セキュリティで保護されたパ	スワード (EAP-MSCHAP v2) 🛛 💌	構成(<u>C</u>)
✓ すはやい再接続を有効 ● 検疫のチェックを有効に	する(Q) する(Q)	
□ サーバーに暗号化バイン	ッドの TLV がない場合は切断する(<u>D</u>)	
	ОК	*+>>セル
₩ 3.2-10 PF	APの設定 2 (Wind	owe Vieta)
保護された EAP のプロ人	Windows 7	x
保護された EAP のプロ	Windows 7	×
保護された EAP のプロ人 接続のための認証方法: マサーバーの証明書を相	Windows 7	
保護された EAP のプロ・ 接続のための認証方法: 「サーバーの証明書を相 」次のサーバーに接続	Windows 7 髪証する(▽) する(○):	,
保護された EAP のプロ人 接続のための認証方法: ジサーバーの証明書を相 二次のサーバーに接続 信頼されたルート証明根	Windows 7 (型) 検証する(型) する(型): (関)(R):	
保護された EAP のプロ・ 接続のための認証方法: マサーバーの証明書を相 二次のサーバーに接続 信頼されたルート証明機 Class 3 Public Prin Coss 3 Public Prin	Windows 7 錠証する(V) する(Q): 瞬間(R): mary Certification Authority	×.
保護された EAP のプロ 接続のための認証方法: マサーバーの証明書を相 二次のサーバーに接続 信頼されたルート証明機 Class 3 Public Prii マ example-DC-CA Microsoft Root Au	Windows 7 能正する(父) 학중(①): 問題(凡): mary Certification Authority thority	
保護された EAP のプロ 接続のための認証方法: ダサーバーの証明書を相 二次のサーバーに接続 信頼されたルート証明機 Class 3 Public Prii ダ example-DC-CA Microsoft Root Au Microsoft Root Ce Thawte Timestamp	Windows 7 能正する(少) する(少): 構築(氏): mary Certification Authority thority thority thority ping CA	
保護された EAP のプロ 接続のための認証方法 マサーバーの証明書を称 次のサーバーに接続 信頼されたルート証明機 Class 3 Public Pri マ example-DC-CA Microsoft Root Au Microsoft Root Au	Windows 7 全証する(V) する(Q): 開設(<u>R</u>): mary Certification Authority thority rtificate Authority prince CA	
保護された EAP のプロ・ 接続のための認証方法 マサーバーの証明書を称 は知されたルート証明機 Class 3 Public Pri マ example-DC-CA Microsoft Root Au Microsoft Root Au Microsoft Root Au Microsoft Root Au	Windows 7 検証する(父) する(Q): 開駅(<u>R</u>): mary Certification Authority thority rtificate Authority sing CA 信頼された証明機関を承認するようユ	-Ÿ-(с求めない(P)
保護された EAP のプロ 接続のための認証方法: 『サーバーの証明書を利 』次のサーバーに接続 (言頼されたルート証明機 (言頼されたルート証明機 (言頼されたルート証明機 (言頼されたルート証明機 「Class 3 Public Prin マ example-DC-CA Microsoft Root Au Microsoft Root Au Microsoft Root Ce Thawte Timestamp … 新しいサーバーまたは 認証方法を選択する(S):	Windows 7 種証する(公) する(Q): 構題(E): mary Certification Authority thority rtificate Authority oing CA 信頼された証明規関を承認するようユ・	-ザ-(с求めない(P)
保護された EAP のプロ 接続のための認証方法: マサーバーの証明書を私 (注頼されたルート証明概 Class 3 Public Pri マexample-DC-CA Microsoft Root Au Microsoft Au	Windows 7 雑証する(少) する(少): 期間(R): mary Certification Authority thority rtificate Authority ining CA 信筆頼された証即用振開を承認するようユ・ スワード (EAP-MSCHAP v2)	-ザーに求めない(P) 構成(C)
保護された EAP のプロ・ 接続のための認証方法 「サーバーの証明書を利 」次のサーバーに接続 「信頼されたルート証明機 「Class 3 Public Prii マ example-DC-CA Microsoft Root Au Microsoft Root Au Microsoft Root Ce Thawte Timestamp 新しいサーバーまたは 認証方法を選択する(S): セキュリティで(保護されたバ マ 高速再接続を有効にす ネットワーク アクセス(保護 サーバーに暗号化)バイン	Windows 7 線証する(公) する(Q): 線関(E): mary Certification Authority thority rtificate Authority comparison of the second secon	-ザー(c求めない(P) 構成(C)
保護された EAP のプロ・ 接続のための認証方法: マサーバーの証明書を称 (注頼されたルート証明概 Class 3 Public Pri マ example-DC-CA Microsoft Root Au Microsoft Au Microsoft Root Au Microsoft	Windows 7 雑証する(少) する(少): 構題(E): mary Certification Authority thority rtificate Authority ining CA 信筆積された証即用振開を承認するようユ・ ネワード (EAP-MSCHAP v2) る(E) 養を強制する(N) ドの TLV がない場合(は切断する(D) する(2)	-ザーに求めない(P) 構成(C)
保護された EAP のプロ 接続のための認証方法: ● サーバーの証明書を相 ○ ホのサーバーに接続 (信頼されたルート証明機 ○ はない 3 Public Prii ○ example-DC-CA Microsoft Root Au Microsoft Root Au Microsoft Root Ce □ Thawte Timestamp ■ 新しいサーバーまたは 認証方法を選択する(S): セキュリティで「保護されたパ ○ 満速再接続を有効にす ネットワーク アクセス(保書 サーバーに暗号(ヒバイン) ID プライバシーを有効に	Windows 7 類正する(型) する(型): #関(E): mary Certification Authority thority rtificate Authority ping CA (言頼された証明月規関を承認でするようユ・ (注頼された証明月規関を承認でするようユ・ (注頼された証明月規関を承認でするようユ・ (注頼された証明月規関を承認でするようユ・ (注意見) などの「LV がない場合(は切断する(D) する(D) のK	 × -ザー(こ求めない(P) 構成(C) キャンセル

図 3.2-11 PEAP の設定 2 (Windows 7)

 ③ EAP MSCHAPv2 のプロパティ画面にて 「Windows のログオン名とパスワード (およびドメインがある場合はドメイン)を自動的に使う」をチェックして 「OK」をクリックし、プロパティ画面を 閉じる。



図 3.2-12 PEAP の設定 3

3.2.3. TLS 設定

本項目では、TLS を使用した Windows 標準搭載 IEEE802.1X 認証の設定方法を示します。 なお、本ガイドでは認証端末におけるユーザー証明書の取得方法に、「証明書サービス Web 登録」機能 を使用しています。

- (1) ユーザー証明書のダウンロード
- サーバとの通信が可能なネットワークにクライアント端末を接続する。 Internet Explorer を起動し「https://サーバのホスト名/certsrv/」に Web アクセスする。なお RADIUS サーバに Windows Server 2008 を使用している場合は「http://サーバのホスト名 /certsrv/」に Web アクセスする。

(本ガイドでのサーバのホスト名は "dc.example.co.jp"です。)

認証画面が表示されたら、<u>3.1.1</u>で作成 したユーザー名およびパスワードを入 カしログオンする。

☆ お気に入り 68 兆	2) おすすのサイト ▼ 創 Web スライス ギャラ… ▼ 6) * ○ 扁 * ページ(P) * セーフティ(5)	・ ツール(0)・ 👔
U IRIET.		. , ,,,(0) + 1
	Windows セキュリティ	
	dc.example.co.jp へ接続しています。	
	User1	
	Exactly Example	
	□ 資格情報を記録する	
	OK キャンセル	

図 3.2-13 TLS の設定 1

 Microsoft Active Directory 証明書サービ ス画面が表示される。

「タスクの選択」より「証明書を要求す る」をクリックする。

CX + WHOMS INTERNE DECK		
e nttps://dc.example.co.jp/certsrv/	• 🛗 😫 • X 🖓 Bing	
👌 お気に入り 🛛 🎭 🔊 おすすのサイト 🍷 🖉 Web スライス ギャラ 🍷		
Microsoft Active Directory 証明書サービス		フティ(<u>S</u>) • ツール(<u>Q</u>) •
Microsoft Active Directory 証明書サービス example-DO-CA		*-
10C7		
シューマ	更要する いっとせんです 1部目また体目して いっと トでけれのつっぜっけ	ぶあわた白 直を増空止さ
0.メッセージに署名したり、メッセージを暗号化したり、要求した証明書の種	類によってほかのセキュリティタスクを実行したりすることができます。	1008/CE91240/10/
Cの Web サイトを使って証明機関 (CA) 証明書、証明書チェーン、または証	「明書失効リスト (CRL)をダウンロードしたり、保留中の要求の状態を表示	示することもできます。
Active Directory 証明書サービスに関する詳しい情報は、次を参照してくだ	さい: Active Directory 証明書サービスドキュメント	
9.7.5の週祝 : 1回月書を要求する		
保留中の証明書の要求の状態		

図 3.2-14 TLS の設定 2

 ③ 「証明書の要求」で、「ユーザー証明書」 をクリックする。

Microsoft Active Directory IEMB19-E.X - Windows Sitemet Explorer		
e Mtgs. Https://dc.example.co.jp/cartary/cartross.asp	• 🔒 🖯 + 🛠 🖓 Bing)
👷 お気に入り 🖙 (注) おすずのサイト 🔹 (400 スライス ギャラー・	6554 C	
愛 Microsoft Active Directory 証明書サービス	A • ■ • ○	(S) • 𝒴¬𝑘(Q) • (S)
Microsoft Active Directory 印用書サービス scample=DD-CA		1-1
証明書の要求		
国明書の種類の選択 ユーザー提明書		
証明書の要求の詳細設定を送信する。		
ージが表示されました	● インターネット 保護モード: 開助	Fa * # 100%

図 3.2-15 TLS の設定 3

④「Web アクセスの確認」 画面が表示されま すので「はい」をクリックする。



図 3.2-16 TLS の設定 4

⑤ 「送信」をクリックする。



図 3.2-17 TLS の設定 5

⑥ 下記の警告が表示されるが「はい」をク リックする。



図 3.2-18 TLS の設定 6

 「この証明書のインストール」をクリッ クする。



⑧ ユーザー証明書のインストール完了。

€ Microsoft Active Directory 証明書サービス - Windows Internet Explorer		- 0 - X-
🕒 🕗 🔹 https://dc.example.co.jp/certsrv/certrmpn.asp	• 🔒 🖻 ↔ 🗙 🖓 Bing	ρ •
🚖 お気に入り 🛛 🎪 🔊 おすすめサイト 🔻 🔊 Web スライス ギャラ 👻		
Wicrosoft Active Directory 証明書サービス	■ ● ■ ○ ● ■ ページ(P) ■ セーフテ	(5)・ ツール(2)・ 🚷・
Microsoft Active Directory 証明書サービス example-DC-CA		A=#
インストールされた証明書		
新しい証明書は正しくインストールされました。		
ページが表示されました	 インターネット 保護モード: 無効 	√2 ▼ ₹ 100% ▼

図 3.2-20 TLS の設定 8

⑨ 「スタート」→「コントロールパネル」
 →「インターネットオプション」を開き、
 「コンテンツ」タブを選択して「証明書」
 をクリックする。

証明書画面にて「個人」タブを選択し、
 「発行者=example-DC-CA(CA)、発行
 先=ユーザー名」が追加されていること
 を確認する。

证明書	-	10.0 m	(Income Ten	-	×
目的(<u>N</u>):		<বস্মহ>			•
個人	ほかの人 中間	調証明機関 信頼された川	レート証明機関 信約	頼された発行元	信頼されない発行元
発行	i先	発行者	有効期限	フレンドリ名	
ER U	iser 1	example-DC-CA	2011/01/	〈なし〉	
「インボ・	-MQ] [I2	スポート(<u>E</u>) 削除()	R)		言非希出版文定(<u>A</u>)
一証明書	:の目的 	売フリールの/日本 トニノ			
喧方化	J71 N Y AT L	、 電子メールの1未渡、クライ	アント記名曲		表示())
[TFI]書(の詳細について表	示します。			問!:ろ(0)
					19710-00(07

図 3.2-21 TLS の設定 9

(2) TLS 設定手順

今回作成したドメインユーザー(本ガイドでは "user1")には IEEE802.1X 認証の設定を変更する権限 が無いため一度ログオフしてください。次にこのコンピュータの管理者権限のあるユーザーでドメイン (本ガイドでは "example.co.jp")ではなくこのコンピュータにログオンしてください。

① 「スタート」→「コントロールパネル」
 →「ネットワークと共有センター」→「ア
 ダプターの設定の変更」を開き、該当する
 ネットワーク接続を右クリックして「プロ
 パティ」を開く。

プロパティ画面にて「認証」タブを選択し、 「IEEE802.1X 認証を有効にする」にチェ ックを入れ、EAP の種類に「Microsoft: ス マートカードまたはその他の証明書」を選 択、「設定」をクリックする。

Windows Vista Windows Vista
ネットワーク 認証 共有
このイーサネット アダプタに、認証済みのネットワーク アクセスを提供するに は、このオプションを選択してください。
▼ IEEE 802.1× 認証を有効にする(N)
ネットワーク認証方法を選択してください(<u>M</u>):
Microsoft: スマート カードまたはその他 ▼ 設定(S)
□ このネットワークへの)大回接続時のため(こ、ユーザー情報をキャッ シュする(©)

図 3.2-22 TLS の設定 10 (Windows Vista)

Windows 7
□□ ーカル エリア接続の > □ / / / 1 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
ネットワーク 認証
このイーサネット アダプターに認証正済みのネットワーク アクセスを提供するに は、このオプションを選択してください。 「 IEEE 802.1X 認証を有効にする(N)
ネットワークの認証方法の選択(M):
Microsoft スイートカートまたしての他の証明者 ▼ まえたしら) ログオンするたびに、この接続用の資格情報を使用する(B)
▼ 承認されていないネットワーク アクセス(こフォールバックする(E)
追加の設定(D)
 OK キャンセル

図 3.2-23 TLS の設定 10 (Windows 7)

スマートカードまたはほかの証明書のプロパティ画面にて、接続のための認証方法に「このコンピュータの証明書を使う」を選択する。「サーバーの証明書を検証する」にチェックし、「信頼されたルート証明機関」の中から「example-DC-CA」をチェックし、「OK」をクリックして画面を閉じる。

Windows Vista					
スマートカードまたはその心の証明者のノロハティ					
接続のための認証方法: ○ 自分のスマートカードを使う(S) ③ このコンピュータの証明書を使う(C) ▼ 単純な証明書の選択を使う(推奨)(M)					
- ▼ サーバーの証明書を検証する(⊻)					
□ 次のサーバー(注接続する(<u>0</u>):					
信頼されたルート証明機関(尺):					
Class 3 Public Primary Certification Authority					
GTE CyberTrust Global Root					
Microsoft Root Authority					
Thawte Timestamping CA					
」 証明書を表示する(<u>E</u>)					
□ 新しいサーバーまたは信頼された証明機関を承認するようユーザーに求め ない(P)					
OK キャンセル					

図 3.2-24 TLS の設定 11 (Windows Vista)

Windows 7
スマートカードまたはその他の証明書のプロパティ
接続のための認証方法: 自分のスマートカードを使う(S) このコンピューターの証明書を使う(C) 単純な証明書の選択を使う(推奨)(M) サーバーの証明書を検証する(V) 次のサーバー(に接続する(Q):
信頼されたルート証明採開(氏): ○ Class 3 Public Primary Certification Authority ② example=DO-CA ○ Microsoft Root Authority ○ Microsoft Root Certificate Authority ○ Thawte Timestamping CA
証明書を表示する(E) 新しいサーバーまたは信頼された証明機関を承認するようユーザーに求めない(P)
□ この接続で別のユーザー名を使う(<u>D</u>)
OK キャンセル

図 3.2-25 TLS の設定 11 (Windows 7)

RADIUS サーバ設定ガイド Windows Server 2008 編(第2版)

3.3. IEEE802.1X 認証の確認

3.3.1. サーバでの確認

全ての設定が完了しクライアント端末を認証スイッチに接続して IEEE802.1X 認証を行ってください。

「サーバーマネージャ」→「診断」→「イベ ントビューア」→「カスタムビュー」→「サ ーバーの役割」→「ネットワークポリシーと アクセスサービス」の NPS ログを確認する ことができます。

認証プロバイ 認証サーバー 認証サーバー	ダー: Windows -: dc.example	.co.jp	-	
EAP の種類 EAP の種類 MSCHAP v2) アカウントのt	: N 2990aD ID: -	icrosoft: セキュリティで保護さ	れたパスワード (EAP- 	
グの名前(M): -ス(S): (ペント ID(E): >ペリ(L): 2−ザー(U): †ペコード(O): 羊細情春報(I):	セキュリティ Microsoft Windows s 6278 情報 N/A 情報報 <u>イベントログのヘルプ</u>	ecurity ε ログの日付(D): タスクのカテゴリ(Y): キーワード(K): コンピューター(R):	2010/01/14 19:02:59 ネットワーク ポリシー サーバー 成功の 話査 dc <i>e</i> xample.co.jp	
コピー(P)			EE 17	

ネットワークボ 認証プロパイ5 認証サーバー・ 認証加の種類 EAPの種類 アカウントのセッ リース(S)・ イベント ID(E)・ レベル(L)・ ユーザー(U)・ オペコード(O)・ 詳細情報(D)・	リシー名: 	802.1XSAL 2example.co.jp AP Microsoft - Vindows security a <u>Vindows security a</u>	ES スマート カードまた() ログの日(寸(D): タスクのカテゴリ(Y): キーワード(K): コンピューター(R):	▲ その他の証明書 2010/01/14 18:58:36 ネットワーク ポリシー サーバ・ 成功の話査 dc example co.jp	•
---	-----------	--	--	---	---

図 3.3-2 サーバログ (TLS)

3.3.2. AX2430S での確認

AX2430S の show dot1x vlan dynamic detail コマンドにて、IEEE802.1X 認証に成功しているユーザ 一情報を確認することができます。

🧕 COM3:9600baud - Tera	Term VT				- • ×
ファイル(F) 編集(E) 設定	(S) コントロール(C)) ウィンドウ(W) /	へルプ(H)		
show dot1x vlan dynam Date 2010/01/14 19:13 VLAN(Dynamic)	mic detail 1:15 UTC				*
AccessControl : Mult Status : Supplicants : 1 / TxTimer(s) : ReAuthSuccess : 2 SuppDetection : Auto VLAN(s): 100,200	tiple-Auth 1 / 256 / 30 0	PortCon Last EA ReAuthM ReAuthI ReAuthF	trol : Auto POL : 001e. Node : Enabl Timer(s): 259 Tail : 2	c965.ea0c e / 300	
Supplicants MAC	Status SessionTime(s) VLAN(Dynamic)	AuthState Date/Time Supplicants : 1	BackEndState	ReAuthSuccess	
001e.c965.ea0c	Authorized 41	Authenticated 2010/01/14 19:	Idle 10:34		
					-

3.3-3 show dot1x vlan dynamic detail

4. Web 認証の設定

4.1. サーバの設定

4.1.1. ユーザーの作成

Web 認証用のユーザーを作成します。ユーザーID、パスワードが6文字以上でないとAX にて受け 付けない事に留意して下さい。

 「サーバーマネージャ」→「Active Directory ドメインサービス」→「Active Directory ユーザーとコンピュータ」を開 き、作成したドメインを展開して「Users」 を右クリックし、「新規作成」→「ユーザ ー」を選択する。

サーバーマネージャー(DC) Users 22個のオブジェント [2013/2-アクティブ]	建作
P 1028 Advise Directory 75/2 91-221 Advise Directory 75/2 91-22 Advise Directory 75/2 Advise Directory 75/2 91-22 Advise Directory 75/2 A	Uters 1804PD



- ウィザードが開始されたら、下記の値を 入力し、「次へ」をクリックする。
- ・姓:任意(本ガイドでは、「webuser1」)
- ・フルネーム:任意

(姓を入力すると同時に反映される)

・ユーザーログオン名:任意
 (姓と同一にする)

新しいオ	ブジェクト	・- ユーザー					×
2	5	作成先:	example.co.jp	o/Users			
ţ)生(<u>L</u>):		webuser1				
:	名(<u>F</u>):				イニシャル(D:		
	フル ネーム	.(<u>A</u>):	webuser1				
	ューザーロ	グオン名(山):					
	webuser1			@example.	co.jp	•	
2	ユーザーロ	グオン名 (Wir	dows 2000 ්	:り前)(<u>₩</u>):			
	EXAMPLI	E¥		webuser1			
				く戻る(日)	;次へ(<u>N</u>) >	キャンセル	,

図 4.1-2 Web 認証用ユーザーの作成 2

 パスワードを入力して「完了」をクリッ クする。



④ 作成したユーザー (webuser1)を選択し、
 右クリックしてプロパティを開く。プロ
 パティ画面にて「所属するグループ」タ
 ブを選択し、「追加」をクリックする。

図 4.1-3 Web 認証用ユーザーの作成 3

webuser1ወプロパティ <u>? ×</u>
環境 セッション リモート制御 ターミナル サービスのプロファイル COM+ フリガナ 全般 住所 アカウント プロファイル 電話 組織 所属するグループ ダイヤルイン
所属するグループ(M):
名前 Active Directory ドメイン サービス フォルダ
Domain Users example.co.jp/Users
追加(<u>D</u>) 肖明徐(<u>R</u>)
プライマリ グループ: Domain Users
プライマリ グループの設定(S) Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。
OK キャンセル 適用(A) ヘルプ

図 4.1-4 Web 認証用ユーザーの作成 4

⑤ グループの選択画面にて、選択するオブジェクト名に 3.1.1 で作成したグループ名(SALES)を入力して「名前の確認」をクリックし、「OK」をクリックする。

グループ の選択		? X
オブジェクトの種類を選択してください(S): グループ または ビルトイン セキュリティ プリンシパル	オブジェクトの種	類(<u>0</u>)
場所を指定してください(<u>F</u>): example.co.jp		
選択するオブジェクト名を入力してください(<u>例)(E)</u> : SALES		20)
詳細設定(<u>A</u>)	OK \$42	

図 4.1-5 Web 認証用ユーザーの作成 5

⑥ 所属するグループ内に指定したグループ が追加されている事を確認する。

webuser1のプロパティ	<u>? ×</u>
環境 セッション 全般 住所 アカ「	リモート制御 ターミナル サービスのプロファイル COM+ フリガナ ウント フロファイル 電話 組織 所属するグループ ダイヤルイン
所属するグループ(M):	
名前	Active Directory ドメイン サービス フォルダ
Domain Users	example.co.jp/Users
	肖·J际(<u>E)</u>
プライマリ グループ:	Domain Users
ブライマリ グループ	D設定(5) Macintosh クライアントまたは POSDX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。
	OK キャンセル 適用(A) ヘルプ

図 4.1-6 Web 認証用ユーザーの作成 6

 次に「ダイヤルイン」タブを選択し、「リ モートアクセス許可」を「アクセス許可」 にチェック、「OK」をクリックする。

webuser10לםאדי איז איז איז איז איז איז איז איז איז אי
環境 セッション リモート制御 ターミナル サービスのプロファイル COM+ フリガナ 全般 住所 アカウント プロファイル 電話 組織 所属するグループ ダイヤルイン
「リモート アクセス許可
 アクセスを許可(W)
 アクセスを拒否(D)
○ NPS ネットワーク ポリシーでアクセスを制御(P)
□ 発信者番号を確認(V):
- コールバック オブション
⊡ ールバックしない(©)
○ 呼び出し元による設定 (ルーティングとリモート アクセス サービスのみ)(S)
○ 常に次の電話番号にコールバック(Y):
「 #865 TD フビレフナ実的 出アス(Y)
「月初り」「アドレスで書い」ヨービンリー このガイヤルインは接続に対して有効にする IP アド
しえを定義してください。
このダイヤルイン接続に対して有効にするルートを定
義してください。
OK キャンセル 適用(A) ヘルブ

図 4.1-7 Web 認証用ユーザーの作成7

RADIUS サーバ設定ガイド Windows Server 2008 編(第2版)

4.1.2. NPS の設定

※RADIUS クライアントの設定をする。

RADIUSクライアントの設定に関しては 3.1.2.(2)を参照して下さい。

 「サーバーマネージャ」→「役割」→「ネ ットワークポリシーとアクセスサービ ス」→「NPS (ローカル)」→「ポリシー」 →「ネットワークポリシー」を右クリッ クし、「新規」をクリックする。



図 4.1-8 NPS の設定1

 任意のポリシー名(本ガイドでは、「Web 認証 SALES」)を入力し、「次へ」をクリ ックする。

新しいネットワーク ポリシー	×
ネットワークポリシー名と接続の種類 ネットワークポリシーの名前およびポリシーを適用	の指定 する接続の種類を指定できます。
ポリシー 名(<u>A</u>): [Web認証SALES]	
ネットワーク接続の方法 NPS に接続要求を送信するネットワークアクセスサーバーの種類 ペンダー図有1を指定することができますが、どちらも必須ではありま 802.1X ワイヤレスアクセスポイントの場合は、「未指定」を選択して	を選択してください。ネットワーク アクセス、サーバーの種類を選択するか、[せん。ネットワーク アクセス、サーバーが 802.1X 認証スイッチまたは ください。
ネットワークアクセスサーバーの種類(5): Unspecified	3
	前へ(P) 次へ(N) 完了(F) キャンセル
図 4.1-9 N	PS の設定 2

3 条件の指定

「追加」をクリックする。



図 4.1-10 NPS の設定 3

 ④ 条件の選択画面にて、「NAS ポートの種 類」を選択し、「追加」をクリックする。

条件の	選択	×
条件有	を選択し、「追加」をクリックします。	
6	● 独野総末 ID 漆阿端末 ID の条件には、ネットワーク アクセス サーバー (NAS) の電話番号を文字列で指定します。パターン マッチングの 構文を役用して市外局番を指定できます。	•
2	NAS ID) > NAS ID の条件は、ネットワーク アクセス サーバー (NAS)の名前である文字列を指定します。パターン マッチ構文を使用し ■ て NAS 名を指定できます。	
7	NAS IP-VF アドレス NAS IP アドレスの条件は、NAS の IP アドレスである文字列を指定します。パターン マッチ構文を使用して IP ネットワーク を指定できます。	
2	NAS IP-6 アドレス NAS IP-6 アドレスの条件は、NAS の IP-6 アドレスである文字列を指定します。パターン マッチ構文を使用して IP-6 ネッ トワークを指定できます。	
Ż	・ NKS ホートの種類 NAS ホートの種類の条件は、アナログ電話回線、ISON、ドンネルまたは仮想プライベート、ネットワーク、IEEE 802.11 ワイヤ レス、あとびイーサネット スイッチなど、アグセス、ジライアントが使用するメディアの種類も指定します。	-
		L I

図 4.1-11 NPS の設定 4

 S NAS ポートの種類画面にて、「仮想 (VPN)」をチェックし、「OK」をクリッ クする。

NAS ボートの種類	×
このポリシーに一致するために必要なアクセス メディアの種類を指定します。 一般的なダイヤルアップおよび VPN トンネルの種類(<u>D</u>)	
Async (Modem) ISDN Sync	
✓ Virtual (VPN)	
一般的な 802.1X 接続トンネルの種類(X)	
Ethernet FDDI Token Ring Wireless - IEEE 802.11	
その他(<u>T</u>)	
ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation ADSL-DMT - Asymmetric DSL Discrete Multi-Tone Async (Modem)	
OKキャンセル	

図 4.1-12 NPS の設定 5

⑥ 条件一覧に「条件=NAS ポートの種類、
 値=Virtual (VPN)」が追加されていることを確認し、「追加」をクリックする。

新しいネットワー	ク ポリシー	×
	条件の指定 接続要求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。少なくとも 1 つの条件が必要です。 要です。	
条件(<u>C</u>):		
条件	值	
	−r∪y∰zk¥ virtuai∖vriv	
条件の説明 NAS ポートの ネット スイッチが	種類の条件は、アナログ電話回線。EDN、トンネルまたは原理プライベート ネットワーク、IEEE 802.11 ワイヤレス、およびイーサ スと、アクセス クライアントが使用するメディアの種類を指定します。 	•
	_ 前へ(2) _ 法へ(2) _ 元了(5) _ キャンセル	

図 4.1-13 NPS の設定 6

 ⑦ 条件の選択画面にて、「Windows グルー プ」を選択し、「追加」をクリックする。

条件の選択	×
条件を選択し、〔追加〕をクリックします。	
<u> グループ</u>	_
Windows グループの条件は、接続ユーザーまたは接続コンピュータが選択されたグループのいずれかに所属している必要があることを指定します。	
コンピュータヴループ コンピュータ グループの条件は、接続するコンピュータが選択したグループのいずれかに属している必要があることを指定しま	
ユーザーグループ ユーザーグループの条件は、接続ユーザーが選択されたグループのいずれかに所属している必要があることを指定します。	
HCAP	
ロケーショングループ HCAP ロケーショングループの条件には、このポリシーに一致するために必要な HCAP (Host Oredential Authorization HCAP ロケーショングループを指定します。HCAP プロトコルは、NFS と一部のサード パーティ製ネットワーク アクセス サーバー (NAS) との間の通信で使用されます。この条件を使用する前に NAS のドキュメントを参照してください。	V
注意加(D) キャンセル	v

図 4.1-14 NPS の設定 7

⑧ Windows グループ画面にて、「グループ の追加」をクリックする。

Windows ヴループ	×
このポリシーに一致するために必要なグループ メンバシップを指定(S)	
	_
グループ	
ガル	
5777 5 (5)(<u>2)(1)(2</u>)	-
OK キャンセル	

図 4.1-15 NPS の設定 8
⑨ グループの選択画面にて、選択するグル ープ名を入力して「名前の確認」をクリ ックする、「OK」をクリックする。

グループ の選択	<u>? ×</u>
オブジェクトの種類を選択してください(S):	
グループ	オブジェクトの種類(の)
場所を指定してください(E):	
example.co.jp	場所(<u>L</u>)
選択するオブジェクト名を入力してください(<u>例)(E</u>):	
SALES	名前の確認(C)
· · · · · · · · · · · · · · · · · · ·	
	OK キャンセル



 Windows グループ画面にて、選択したグ ループが追加されていることを確認し、 「OK」をクリックする。

Windows グループ	×
このおいいこ(ニュを)オスため(この声など)エニゴ いっぱいっぱた地空(の)	
このパックーに二致するに見たる要なケルークラクパクタイを目れたの	
グループ	
EXAMPLE¥SALES	
ガループの注意的(1.) 質問金(2.6)	-1
OK キャンセ,	11
	_

図 4.1-17 NPS の設定 10

 条件一覧に「条件=Windows グループ、 値=選択したグループ名」が追加されて いることを確認し、「次へ」をクリックす る。

2000 D 2 2 200 2		
	の指定 見求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。少なくとも 1 つの条件が 。	吃
条件(<u>C</u>):		
条件	値	
🤝 NAS ポートの種類	Virtual (VPN)	
🕵 Windows グルー:	2 EXAMPLE¥SALES	
(4 o 1400		
と件の説明: indows グループの条 す。	件は、接続ユーザーまたは接続コンピューターが選択されたグループのいずれかに所属している必要があることを指う	ĒU
&件の説明 Imdows グルーブの楽 す。	件は、接続ユーザーまたは接続コンピューターが選択されたグループのいずれかに所属している必要があることを指う 適加(D) 編集(E) 育明家(E	EL)

図 4.1-18 NPS の設定 11

⑦ アクセス許可の指定
 「アクセスを許可する」にチェックして、
 「次へ」をクリックする。



図 4.1-19 NPS の設定 12

認証方法の構成

「暗号化されていない認証(PAP、SPAP)」 にチェックして、「次へ」をクリックする。 接続要求ポリシーのヘルプトピックが 表示された場合は「いいえ」で先に進め てください。

新しいネットワー	-ク ポリシー
	認証方法の構成 接続審求が、のポリンーの条件を読むすたがに必要な認証方法を、1 つむ上指定して代えい、EAP 認証には、EAP 経営を指定する必要があります。NAP を使用する 8021X または VPN 実展開する場合は、接続要求ポリンーに経緯 だ EAP を指定する必要があります。接続要求ポリシーは、ネットワーク ポリシーの認証設定よりも優先されます。
EAP の種類は、	、NPS とクライアントとの間で、表示されている順序でネゴシエートされます。
EAP の種類(D:
道加(<u>A</u>) セキュリティ レ Microsoft	▲東(日) 用原作日 バルの低い認証方法: 暗号(LIZE)バージョン2(KG-CHAP V2X)) にの問題が用いてきた、このようには「日本」のので用意が見てきたり
□ Microsoft □ パスワー □ 暗号化認	電子に設定している。 ADDAS TODAC ADDAS ADDAS
 ▶ 暗号化され ▶ 認証方法 ■ コンピュータ 	していない認証(PAP、SPAPI(S) をネゴンエートセッピクライアンドに掃続を許可する(L) の正常性チェックのみを実行する(E)
	- 前へ(P) 次へ(Y) - 元了(E) キャンセル

図 4.1-20 NPS の設定 13

④ 制約の構成
 必要な設定がある場合は設定し、「次へ」
 をクリックする。



図 4.1-21 NPS の設定 14

※設定の構成

IEEE802.1X認証の手順と同じ。(3.1.2.(3)(c)を参照)

(1) 新しいネットワークポリシーの完了
 設定した内容を確認し、「完了」をクリックする。



 (16) サーバーマネージャ画面にて、ネットワ ークポリシー一覧に「Web 認証」が追加 されていることを確認する。

↓ サーバーマネージャー (0C)	ネットワーク ポリシー		操作
		ケーと、2050ユーザーが3キリワーン(3株成 またを) 555度(555月の) またを) アンセンの後述1150 (255) 2000年1150 (255) 2000 (255) 2000 (25	25/10-0 おりりー ドル ・「気のないたい ホリーク おりりー ドル ・「気のないたい ホリーク ホーー ・
	設定 - 法の設定が場開られます 設定 値 設定 値 設計 一 設計 一 設計 アクセス3447358 お湯男やクライアンの世界 Tota NAF 後期 デビネス3470-0 7 Framed-Protocol PP Sprive-Tron Framed	2022 (PAP, SPAP)	-

図 4.1-23 NPS の設定 16

4.2. クライアント端末の設定

クライアント端末の設定は特にありません。ブラウザが使用できることを確認してから認証ポ ートに接続してください。

4.3. WEB 認証の確認

4.3.1. クライアントでの確認

 クライアント端末のブラウザから Web 認証専用 IP アドレスに HTTP アクセス すると Web 認証画面が表示されます。 Web 認証用に作成したユーザーとその パスワードを入力し「Login」をクリック する。(本ガイドでは User ID = "webuser1")



図 4.3-1 Web 認証の確認 1

 「Login success」と認証成功画面が表示 される。

		The set of Miner as Characteria d	0.00
Google G+	東京 中参 Ø D マ ロ フックマークマ Ø	フロック数:0 🌍 チェック 🔹 🍎 次に通信 🕶 🌽)) RE
* * 6			!) ▼ ③ ツール(0) ▼
	Login succe	55	
	Login Time 2008/05/2	29 19.06.23 UTC	
	Logout Time 2008/05/2	29 20.06:23 UTC	
	close		
		All Rights Reserved, Copyright (C) 2006–2008 ALAX	ALA Networks Corp.
ページが表示されました		🕝 🚨 インターネット 保護モード: 無効	100% •

図 4.3-2 Web 認証の確認 2

4.3.2. サーバでの確認

「サーバーマネージャ」→「診断」→「イベ ントビューア」→「カスタムビュー」→「サ ーバーの役割」→「ネットワークポリシーと アクセスサービス」で、NPS のログを確認す ることができます。

接続要求ポ ネットワーク: 認証チロバイ 認証サーバい 認証の種類 EAPの種類 アカウントの1	/2; Use Windows authentication for all users ↓ (9)3; WebIXIESALES : Windows dcexample.co.jp PAP - ŷ∋ŷ ID: - ↓	
ソース(<u>S</u>):	Microsoft Windows security a ログの日付(<u>D</u>): 2010/01/15 16:58:05	
イベント ID(<u>E</u>):	6278 タスクのカテゴリ(<u>Y</u>): ネットワーク ポリシー サーバー	
ν~ν.μ(<u>L</u>):	情報 キーワード(<u>K</u>): 成功の監査	
ユーザー(U):	N/A コンピューター(<u>R</u>): dc.example.co.jp	
オペコード(0):	情報	
副羊糸田竹青幸服(I):	イベント ログのヘルプ	

図 4.3-3 サーバログ(Web 認証)

4.3.3. AX での確認

AXの show web-authentication login コマンドにて、Web 認証に成功しているユーザー情報を確認することができます。

COM3:9600baud	- Tera Term VT			
ファイル(F) 編集(E)) 設定(S) コントロール	(0) ウィンドウ(W)	へルプ(H)	
RR2 F triple		- 49 B	tan.	2
AX2430S# sh web- Date 2010/01/15 Total user count	-authentication log 16:57:04 UTC	ļin		8)
F Username	I II II II			
VLAN MAC ac	ddress Login t	ime	Limit time	
webuser1 100 001e.c	c965.ea0c 2010/01	./15 16:55:03 UI	C 00:57:59	
odified by operat	or at Tue Jan 12-1	7:14:27 2010 wi	th version 11.2	
e "AX2430S"				
"VLAN0001"				-

図 4.3-4 show web-authentication login

RADIUS サーバ設定ガイド Windows Server 2008 編(第2版)

5. MAC 認証の設定

5.1. サーバの設定

AXのMAC認証で使用するユーザーを作成する場合、パスワードの設定について2通りの方法があります。

(1) ユーザーID、パスワードにクライアント端末の MAC アドレスを使用する。

Active Directory を構成した場合、「パスワードは複雑さの要件を満たす必要がある」というグループ ポリシーが適用されるためユーザーの作成ができません。そのためグループポリシーの編集が必要と なります。

(2) 装置単位で MAC 認証のパスワードを統一する。

AX のコンフィグレーションコマンド(mac-authentication password)を使用します。

構築する環境に応じてパスワードの設定方法を選択して下さい。

5.1.1. グループポリシーの編集(パスワードのポリシー変更)

MAC 認証のパスワードに端末の MAC アドレスを使用する場合、グループポリシーを編集する方法を 示します。本ガイドでは、デフォルトドメインポリシーを編集する手順を記載しています。

 「スタート」→「プログラムとファイル の検索」に「MMC」と入力して、MMC (Microsoft Management Console)を起 動する。

コンソール1の画面にて、「ファイル」→ 「スナップインの追加と削除」をクリッ クする。

スナップインの追加と削除画面にて、「グ ループポリシー管理エディタ」を選択し 「追加」をクリックする。

スナップインの追加と利除 コンピュータで利用できるスナップインからこのコンソールに使用するスナップイン どの拡張を有効にするかを構成できます。 利用できるスナップイン(S): スナップイン ▲ ペーパークシュートル	を選択したり、選択したスナップインを構成したりでき 選択されたスナップイン(E): 「コンソール ルート	× ます。拡張可能なスナップインでは、
日イペント ピューア 「ノンターネット インフォメーション サービス (IES) マネー・ コニンターブライズ PKI 「グルーブ オパシー オブジェクト エディタ 「グルーブ オパシー ングモック GPO エディタ 「グルーブ オパシー つぎ理 「グルーブ オパシーの管理 「グルーブ オパシーの管理 」 「グルーブ オパシーの管理 」	L	<u>- 削除</u> (1) <u>- 上へ移動(1)</u> 下へ移動(1)
説明 このスナップインでは、Active Directory のサイト、ドメイン、組織単位 (OU) ます。 	にリンクされた、またはコンピュータに格納されたグルー	ブ ポリシー オブジェクトを編集でき OK キャンセル

図 5.1-1 MAC 認証の設定 1

 「グループポリシーウィザード」の選択 画面にて、「参照」をクリックする。

グループ ボリシー オブジェクトの選択	×
グルーブ ポリシー ウィザードの開始	
	グループ ポリシー オブジェクトは Active Directory またはローカル コン ビューダに格納できます。 グループ ポリシー オブジェクトを選択するには、【参照】をクリックしてくだ さい。 グループ ポリシー オブジェクト: [
	参照(B)_ 「コマンド ラインから起動したときに、 グループ ポリシー スナップインの フォーカスを変更できるようにする(A) ごれば、コンソールを保存した場合にのみ適用されます。
	< 戻る(B) 完了 キャンセル

図 5.1-2 MAC 認証の設定 2

 グループポリシーオブジェクトの参照画 面にて「Default Domain Policy」を選択 し、「OK」をクリックする。

グループ ポリシー オブジェクトの参照	<u>? ×</u>
ドメイン/OU サイト すべて)	
場所(D: デexample.co.jp 🛛 🗾 🖄 📑 💌	
名前 ドメイン	
Comain Controllers example.co.jp	
OK ¥	ャンセル

図 5.1-3 MAC 認証の設定 3

④ グループポリシーオブジェクトが
 「Default Domain Policy」に変更された
 事を確認し、「完了」をクリックする。

グルーフ ボリシー オブジェクトの選択 グルーフ ボリシー ウノザードの間絶	×
ערע ערע איז איזעאין אייע	
	バリーブ ポロシー オブジャカト(† Active Directory キキ(†ローカリーア)
	ジルージ パッシー オリシュシャル Active Directory arctall ーカル コン ピュータに格納できます。
	グループ ポリシー オブジェクトを選択する(こは、【参照】 をクリックしてくだ さい。
	グループ ポリシー オブジェクト: Default Domain Policy
	参照(<u>B</u>)
	□ コマンド ラインから起動したときに、 グループ ポリシー スナップインの フォーカスを変更できるようにする(A) これは、 コンソールを保存した場合にのみ 適用されます。
	< 戻る(B) (第7) キャンセル

図 5.1-4 MAC 認証の設定 4

⑤ コンソール1の左画面にて、「コンソール ルート」→「Default domain Policy」→「コ ンピュータの構成」→「ポリシー」→ 「Windowsの設定」→「セキュリティの 設定」→「アカウントポリシー」→「パ スワードのポリシー」と展開し、右画面 の「パスワードは、複雑さの要件を満た す必要がある」を選択し、右クリックで 「プロパティ」を開く。

隔コンソール1 - ロンソール ルート¥Default Domain Policy [C	C.example.co.jp] ポリシー¥コンピュータの構成料	イポリシー¥Windows の)設定¥セ <u>ーロメ</u>
藩 ファイル(E) 操作(A) 表示(Y) お気に入り(Q) ウィンドウ(W)	ヘルプ(円)		_ 8 ×
(= =) 2 📰 🗙 🗉 🗟 🛛 🖬			
א-אעב 📔	ポリシー ^	ポリシー設定	操作
🖃 🧾 Default Domain Policy [DCexample.co.jp] ポリシー	📖 パスワードの長さ	7 文字以上	パスワードのボ 🔺
	以前 パスワードの変更禁止期間	18	16.718/1
	1000 パスワードの有効期間	42 日	100分第111 •
田 UVP/IPの設定	1000パスワードの履歴を記録する	24 🖸	パスワードは、 🔺
スカリプト (スタートアップ/シャットダウン)	「「「パスワートは、後継との要件を満たり必要がある」 「「「「「「「「「「「「「」」」」」」」、「「「「」」」、「「」」、「」」、	何劝	他の操作 ▶
🗉 🚡 セキュリティの設定	100 暗ち1とを70と戻せる4人感じ71スワートを1米1子…	無刈	12007001
🖂 🧾 アカウント ポリシー			
🧾 パスワードのポリシー			
アカウント ロックアウトのポリシー			
E i kerberos ////~			
田 二 イベルログ			
🗉 🔂 制限されたグループ			
🗉 📑 システム サービス			
E			
🗉 🚰 ファイル システム			
III III ワイヤード (有線) ネットワーク(IEEE 80)			
田 == ゼキュリティが気動性された Windows ノア1 「 クットローク ロフト フクージュ ポリシー			
■ ポリビン シッスドマホーンマ パッシ ■ 12 ワイヤレス ネットワーク (TEFE 80211) ポ			
■ ○ 公開キーのポリシー			
■ ≦ ソフトウェアの制限のポリシー			
 IP セキュリティ ポリシー (Active Directo - 			
		<u> </u>	



⑥ 「無効」を選択して、「OK」をクリック する。

バスワートは、複雑さの要件を満たす必要があるのフロバティ	Υ×
セキュリティ ポリシーの設定 説明	
パスワードは、複雑さの要件を満たす必要がある	
☑ このポリシーの設定を定義する(D):	
○ 有効(E)	
● 無効(S)	
OK キャンセル 適用(A)

図 5.1-6 MAC 認証の設定 6

 ⑦ 「パスワードは、複雑さの要件を満たす 必要がある」が無効になっている事を確 認し、コンソール1を閉じる。



図 5.1-7 MAC 認証の設定 7

 ⑧ ポリシーの変更を反映させるためコマン ドプロンプトを開き、「gpupdate」コマン ドを投入する。 もしくはサーバを再起動する。

🖬 管理者፡ ጋマンド プロンプト	
Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	
C:¥Users¥Administrator.DC>gpupdate ポリシーを最新の情報に更新しています	
ユーザー ボリシーの更新が正常に完了しました。 コンビューター ボリシーの更新が正常に完了しました。	
C:¥Users¥Administrator.DC>	-

図 5.1-8 MAC 認証の設定 8

5.1.2. ユーザーの作成

本項目では Active Directory に MAC 認証用のユーザーを作成します。AX1200S シリーズは初期値の MAC アドレス設定形式はユーザー名とパスワードが 00-01-02-03-04-05 の形式となりますが、コンフィ グレーションコマンド (mac-authentication id-format) で 000102030405 や 00:01:02:03:04:05 などの 形式及び英字の大文字小文字が変更可能となっています。

AX2400S,AX3600S シリーズでは MAC アドレスは"-"や":"等の記号を含まない **000102030405** の 16 進数 12 桁(英字は小文字)の形式で登録して下さい。

AX1200S と AX2400S シリーズ混在環境では AX1200S 側のコンフィグレーションで **000102030405** の 16 進 12 桁(英字は小文字)の形式に統一して下さい。

 ⑨ 「スタート」→「管理ツール」→「サー バーマネージャ」→「役割」→「Active Directory ドメインサービス」→「Active Directory ユーザーとコンピュータ」を開 き、作成したドメインを展開して「Users」 を右クリックし、「新規作成」→「ユーザ ー」を選択する。

サーバー マネージャー (DC)	Users 23 価のオブジェクト じっつ	ターアウティブコ	除作
副 税割 □ 🍕 Artica Disartasy Kuld's 林山村7	名約 種類	1698	Users
Athe Director ユーザーご Athe Director ユーザーご Athe Director ユーザーご Athe Director ユーザーご Athe Director Dir	e δ Administrator 29"- g Administrator 29"- B Administrator 29"- B Control FOL: 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0	エンピューシー/ドドイン研究 こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト このかかーズの広い/ドビスト 日本のサービスに対し着望。 しかどうサービスに対し着望。 しかどうサービスとの回知。 ドゲインの管理書 ドゲインの管理書 ドゲインの管理書 ドゲインの管理書 ビストンのサービスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト こののカーズの広い/ドビスト	(BLORRT

図 5.1-9 MAC 認証の設定 9

- ① ウィザードが開始されたら、下記の値を 入力し、「次へ」をクリックする。
- 姓:認証したい端末の MAC アドレス
- ・フルネーム:任意
 (姓を入力すると同時に反映される)
 ・ユーザーログオン名:

認証端末の MAC アドレス

新しいオブジェクト - ユーザー	X
🦰 作成先: exam	ple.co.jp/Users
效生(<u>L</u>): 001	9b97d46c7
名(<u>F</u>):	イニジャルΦ:
フル ネーム(<u>A</u>): 001	9b97d46c7
ユーザー ログオン名(<u>U</u>):	
コーザー ログオン名 (Windows	2000より前)(<u>W):</u>
EXAMPLE¥	0019b97d46c7
	< 戻る(日) 次へ(N) > キャンセル



 パスワードを入力し、「次へ」をクリック する。

新しいオブジェクト - ユーザー	×
人 作成先: example.co.jp/Users	
パスワード(P): ●●●●●●●●●●●●●●● パスワードの確認入力(©): ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	
□ ユーザーは次回ログオン#キにパスワード変更が必要(M) □ ユーザーはパスワードを変更できない(S)	
✓ パスワードを無期限にする(W) アカウントは無効(Q)	
< 戻る(B) 次へ(N) > キャ	ンセル

図 5.1-11 MAC 認証の設定 11

12 「完了」をクリックする。

新しいオブジェクト - ユーザー	×
作成先: example.co.jp/Users	
[完了] をクリックすると、次のオブジェクトが作成されます:	
フル ネーム: 0019b97d46c7	A
ユーザー ログオン名: 0019b97d46c7@example.co.jp	
パスワードを無期限にする	
	-
1	
< 戻る(B) (三元7	キャンセル

図 5.1-12 MAC 認証の設定 12

 第 先程作成したユーザー(MAC 認証用のユ ーザー)を選択し、右クリックしてプロ パティを開く。 プロパティ画面にて「所属するグループ」 タブを選択し、「追加」をクリックする。

001ec965ea0cのプロパティ <u>? × </u>
ダイヤルイン 環境 セッション リモート制御 リモートデスクトップ サービスのプロファイル 個人用仮想デスクトップ COM+ フリガナ 全般 住所 アカウント プロファイル 電話 所属されている組織 所属するグループ
所属するグループ(M):
名前 Active Directory ドメイン サービス フォルダー
プライマリ グループ: Domain Users
OK キャンセル 通用(A) ヘルブ

図 5.1-13 MAC 認証の設定 13

 ④ グループの選択画面にて、選択するオブ ジェクト名に 3.1.1 で作成したグループ 名を入力して「名前の確認」をクリック し、「OK」をクリックする。

グループ の選択	<u>? ×</u>
オブジェクトの種類を選択してください(S):	
グループ または ビルトイン セキュリティ プリンシパル	オブジェクトの種類(<u>O</u>)
場所を指定してたさい(上): example.co.jp	
) *** ********************************	
SALES	名前の確認(C)
詳細設定(<u>A</u>)	OK キャンセル

図 5.1-14 MAC 認証の設定 14

「所属するグループ」内に指定したグル
 ープが追加されている事を確認する。

001ec965ea0cのプロパティ <u>? ×</u>
ダイヤルイン 環境 セッション リモート制御 リ リモートデスクトップサービスのプロファイル 個人用仮想デスクトップ COM+ フリガナ 全般 住所 アカウント プロファイル 電話 所属されている組織 所属するグループ
所属するグループ(M): 名前 Active Directory ドメイン サービス フォルダー Domain Users example.co.jp/Users SALES example.co.jp/Users
 プライマリ グループ: Domain Users プライマリ グループの設定(S) 必要はありませ Auo
OK キャンセル 適用(A) ヘルブ

図 5.1-15 MAC 認証の設定 15

 ① プロパティ画面にて「ダイヤルイン」タ ブを選択し、「リモートアクセス許可」を 「アクセス許可」にチェック、「OK」を クリックする。

0019b97d46c7のプロパティ <u>?</u>	×
□ 環境 セッション リモート制御 ターミナル サービスのプロファイル COM+ フリガ: 全般 住所 アカウント プロファイル 電話 組織 所属するグループ ダイヤルイ	+1 ン1
リモート アクセス許可	
● アクセスを許可(W)	
 アクセスを拒否(D) 	
○ NPS ネットワーク ポリシーでアクセスを制御(P)	
□ 発信者番号を確認(<u>V</u>):	
_ コールバック オブション	
⊡ールバックしない(©)	
○ 呼び出し元による設定 (ルーティングとリモート アクセス サービスのみ)(S)	
○ 常に次の電話番号にコールバック(Y):	
このダイヤルイン接続に対して有効にする IP アド #865 m マドロ コイエン 1	
レスを定義してください。	
「「静的ルートを適用(R)	
このダイヤルイン接続に対して有効にするルートを定 静的ルート(リ)	
戦してんどい。	
OK きャンセル適用(<u>A</u>) へルプ	

図 5.1-16 MAC 認証の設定 16

5.1.3. NPS の設定

MAC認証でのNPSの設定は、Web認証での設定(<u>4.1.2</u>章)と全く同じです。わかりやすくする為に、 ポリシー名変更を行うことを推奨します。

5.2. MAC 認証の確認

5.2.1. サーバでの確認

「サーバーマネージャ」→「診断」→「イ ベントビューア」→「カスタムビュー」→ 「サーバーの役割」→「ネットワークポリ シーとアクセスサービス」で、NPSのログ を確認することができます。

● イベント プロパティ - イベン 「全般」 詳細	· 6278, Microsoft Windows security auditing.	×
E23mtの詳細: 接続要求ポリシー名 ネットワークポリシー 認知証プロパイダー 認知証サーバー: 認知証サーバー: 認知証サーバー: 認知証サーバー: 認知証サーバー: 認知証サーバー: 記知証サーバー: 記知証サーバー: 記知証サーバー: 記知証サーバー: 記知証サーバー: 記知証サーバー: 記知証サーバー: 記述サーン: () () () () () () () () () () () () ()	は は は は は は は は は は は は は は	٠
ログの名前(M): ソース(S): イベント ID(E): レベル(L): ユーザー(U): オペコード(Q): 詳細情報(Q):	セキュリティ Microsoft Windows security a ログの日付(D): 2010/01/15 17:22:15 6278 タスクのカテゴリ(Y): ネットワーク ポリシー サーバー 情報 キーワード(<u>K</u>): 成功の話査 N/A コンピューター(<u>B</u>): dc.example.co.jp 情報 <u>イペント ログのヘルプ</u>	•
<u>」ピー(P)</u>	開にる	5(<u>C</u>)

図 5.2-1 サーバログ (MAC 認証)

5.2.2. AX での確認

AX2430Sの show mac-authentication login コマンドにて、MAC 認証に成功しているユーザー情報 を確認することができます。

COM3:9600baud - Tera Tera Tera Tera Tera Tera Tera Tera	erm VT	11(0) ウィンドウ(W)			
AX24305# show mac-auth	entication	1 login			
Total client counts:1	08 010				And the second second
F MAC address Por 001e.c965.ea0c 0/1 AX2430S#	t VLAN 100	Login time 2010/01/15 17:1	9:13 UTC in	mit time finity	Mode ² Dynamic

☑ 5.2-2 show mac-authentication login



2010年2月17日 第2版 発行

アラクサラネットワークス株式会社 ネットワークテクニカルサポート

〒212-0058 川崎市幸区鹿島田 890 番地 新川崎三井ビル西棟 http://www.alaxala.com/