

RADIUS サーバ設定ガイド Windows Server 2012 編



初版

Copyright © 2015, ALAXALA Networks Corporation. All rights reserved.



はじめに

RADIUS サーバ設定ガイド(Windows Server 2012 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 2012 及び Windows Server 2012 R2、クライアント端末に Windows 8 及び Windows 8.1 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 2012 をベースに記述しておりますが、Windows Server 2012R2 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

本製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国輸出管理規制など外国 の関連法規をご確認の上、必要な手続きをお取り下さい。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

- ・Ethernetは、富士ゼロックス(株)の登録商標です。
- ・イーサネットは、富士ゼロックス(株)の登録商標です。
- ・Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- ・Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- ・Windows Server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	-	2015.2.13	初版発行	—

目次

1.		概要	Ę		. 6
	1.	1.	概要	<u>.</u>	. 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	2.	設定例のネットワーク構成図	. 8
	1.	3.	Win	dows Server 2012 と Windows Server 2012 R2 の差分について	. 9
2.		Win	dow	s Server 2012 / Windows Server 2012R2 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	2.	コンピュータ名の変更	10
	2.	2.	役割	」の追加	11
		2.2.	1.	Active Directory のインストール	11
		2.2.2	2.	Web サーバ(IIS)のインストール	18
		2.2.3	3.	Active Directory 証明書サービス(AD CS)のインストール	20
		2.2.4	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
		2.2.0	6.	インストール内容の確認	33
3.		IEEI	E802	2.1X 認証の設定	34
	3.	1.	サー	-バの設定	34
		3.1.	1.	ユーザー、グループの作成	34
		3.1.2	2.	NPS の設定	39
		3.1.3	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.	IEEE802.1X 認証の有効化	55
		3.2.2	2.	ドメイン参加	56
		3.2.3	3.	PEAP 設定	60
		3.2.4	4.	TLS 設定	62
	3.	3.	IEE	E802.1X 認証の確認	68
		3.3.	1.	サーバでの確認	68
		3.3.2	2.	AX スイッチでの確認	69
4.		Web	っ 認言	正の設定	70
	4.	1.	サー	-バの設定	70
		4.1.	1.	ユーザーの作成	70
		4.1.2	2.	NPS の設定	74
	4.	2.	クラ	・イアント端末の設定	80

80
80
81
81
82
82
82
85
89
89
89 89

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 8、Windows 8.1 とし、Windows Server 2012 /Windows Server 2012 R2 のネットワークポリシーサーバー(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 2012 での「役割」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おりません。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

^(※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 2012 Standard 、Windows Server 2012R2 Standard
- > 認証端末: Windows 8 Enterprise、Windows 8.1 Enterprise update
- > 認証スイッチ: AX1240S (Ver2.4) / AX2530S (Ver4.0.A)
- ▶ L3スイッチ: AX3640S (Ver11.11.A)
- ➢ HUB: EAPOL 透過機能有り

AX コンフィグレーション設定例

AX12403 01 2	7170-737
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
!	Í
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
1	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
1	!
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 ■Web 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)

٦

※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 AX2530S 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 2012 と Windows Server 2012 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、Windows Server 2012 と Windows Server 2012 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⑪の図にて Windows Server 2012 ではフォレストおよびドメインの機能レベルに「Windows Server 2012 R2」の選択ができません。

2. Windows Server 2012 / Windows Server 2012R2 の構成

本章では Windows Server 2012 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 2012R2 を RADIUS サーバとして構成する場合は「1.3 Windows Server 2012 と Windows Server 2012R2 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

少なくとも 1 つのネットワークアダプタの TCP/IP の設定を完了させ、リンクアップ状態としてくだ さい。またその際 DNS クライアントの設定も必ずおこなってください。ネットワークアダプタのリン クが上がっていなかったり、DNS が使用できる状態になっていないと Active Directory サービスの構成 が出来ません(以下 2.2.1 ⑬前提条件のチェックで失敗します)。

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。

 Windows ロゴキーを押すか、チャームから[ス タート]を選択しスタートのタイル画面を表 示→「コントロールパネル」→「システム」 を選択→「コンピュータ名、ドメインおよび ワークグループの設定」から設定の変更をク リックしてシステムのプロパティ画面を開き 「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-2012」)設定変 更後は再起動が必要です。



2.1-1 コンピュータ名の変更

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。

1 windows ロゴキーを押し[スタート画面]
 →「サーバーマネージャー」を起動し、「管
 理」から「役割と機能の追加」をクリックする。



図 2.2-1 Active Directory のインストール1

 (2) 「役割と機能の追加ウィザード」での「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

 「インストールの種類の選択」は「役割 ベースまたは機能ベースのインストー ル」のまま「次へ」をクリックする。



図 2.2-3 Active Directory のインストール 3

 ④ 「対象サーバーの選択」では「サーバー プールからサーバーを選択」で、自サー バーが表示および選択されていることを 確認し、「次へ」をクリック。



図 2.2-4 Active Directory のインストール 4

 「サーバーの役割の選択」で「Active Directory ドメインサービス」を選択する。



図 2.2-5 Active Directory のインストール 5

※ 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「管理 ツールを含める(存在する場合)」にチェッ クが入った状態のまま「機能の追加」を クリックする。



図 2.2-6 Active Directory のインストール 6

 ⑥ 「Active Directory ドメインサービス」に チェックが入っていることを確認し「次 へ」をクリック。



図 2.2-7 Active Directory のインストール7

⑦ 「機能の選択」では何も選択せずそのま ま「次へ」をクリック。



図 2.2-8 Active Directory のインストール 8

「Active Directory ドメインサービス」の (8) 画面を確認し、「次へ」をクリック。



図 2.2-9 Active Directory のインストール9

⑨ 「インストールオプションの確認」を確 認し「インストール」をクリック。

※「必要に応じて対象サーバーを自動的 に再起動する」のチェックは入れても入 れなくても良いが、チェックを入れると 右のような警告画面が表示される。



図 2.2-10 Active Directory のインストール 10

(10) インストールが開始され、「インストール の進行状況」で進行の状況が表示される。 インストールが終了したら、右のように その旨が表示される。



 この後「閉じる」もしくは「次へ」で役割と機能の追加ウィザードを閉じても良いが、その場合サーバーマネージャに Active Directory ドメインサービスの構成を促す通知が表示される。

	Ŧ	ーバーマネージャー	
€⊙- "ダ	ッシュボード	• 🕲 I 🍢	管理(M) 9−ル(T) 表示(V) ヘルプ
■ ダッシュポード	▲ 原節後構成 □	[<u>972</u>] X	
■ ローカル サーバー ■■ すべてのサーバー	DC-2012 で Active Din が必要です このサーバーをドメイン コンオ	ectory Fメイン サービス の構成 ・ローラーに算機する	カル サーバーの構成
間 AD DS 闘 ファイル サービスと記憶	1 機能のインストール 構成が必要です。dc-201 しました。 役割と機能の追加	12 でインストールが正常に完了	:機能の追加 するサーバーの追加
	タスクの加挙相		ー グループの作成
	詳細情報(L)		非表示
	役割とサーバー 役割の数:2	グループ サーバー グループの数:1 サ	-バーの合計数: 1

図 2.2-12 Active Directory のインストール 12

10 10もしくは10で、「このサーバーをドメインコントローラーに昇格する」をクリックすると、「Active Directory ドメインサービス構成ウィザード」が実行される。

()	Active Directory	・ドメイン サービス構成ウィザード	
配置構成			ターゲット サーバー dc-2012
公式成成 ドメインコンドローラーオブ 当近オブランン パス オブラーズのの税認 前提是作のチェック インストール 私語	配価値作を選択してにさい ● 既存のドメインにドメイン ● 新しいドメインを既存の ○ 新しいフォレストを通知可 この操作のドメイン情報を描 ドメイン(Q): この操作を実行するには典料 < 資格情報が指定されていい	1 コントローラーを追加する(D) フルストロン語加する(E) F8(E) 定してください * 各情報を指定してください ません>	選択(<u>s</u>)
	詳細 配置構成		
		< 前へ(P) 次へ(N) >	-(>21-1(I) =+>204

図 2.2-13 Active Directoryの構成1

 「配置操作を選択してください」で「新 しいフォレストを追加する」を選択し、
 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 て「次へ」をクリック。



図 2.2-14 Active Directoryの構成 2

 (1) 「ドメインコントローラーオプション」 でフォレストおよびルートドメインの機 能レベル、ドメインコントローラーの機 能、復元時のパスワードをそれぞれ設定 し(本ガイドではフォレストおよびドメ インの機能レベルに「Windows Server 2012」を選択、DNS サーバーはチェック 入ったままとします)「次へ」をクリック する。



図 2.2-15 Active Directoryの構成3

① DNS サーバーの役割をインストールして
 いない場合、右図のような警告が出ます
 が、確認して「次へ」。



図 2.2-16 Active Directoryの構成4

16 「追加オプション」はそのまま「次へ」



図 2.2-17 Active Directoryの構成5

「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。



18 設定した内容を確認し「次へ」をクリック。



図 2.2-19 Active Directory の構成7

① 前提条件のチェックがおこなわれ、チェ ックに合格するとインストール可能にな りますが、チェック結果に警告が表示さ れることもあるので確認の上「インスト ール」をクリックします。

インストール終了後は自動的に再起動さ れます。



図 2.2-20 Active Directory の構成 8

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。

- 「サーバーマネージャー」の「管理」から「役割と機能の追加」をクリックして役割と機能の追加ウィザードを起動し、「インストールの種類」に「役割ベースまたは機能ベースのインストール」を選択→「対象サーバの選択」に自身のサーバ(デフォルトで選択済み)を選択→「サーバの役割の選択」で「Webサーバ(IIS)」にチェックを入れ「次へ」をクリックする。
- (2)「機能の選択」では何も選択せずそのま ま「次へ」をクリック。



図 2.2-21 Web サーバ(IIS)のインストール1



図 2.2-22 Web サーバ(IIS)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 2.2-23 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。



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。



2.2.3. Active Directory 証明書サービス(AD CS)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。

「サーバーマネージャー」の「管理」から「役割と機能の追加」をクリックして役割と機能の追加ウィザードを起動し、「インストールの種類」に「役割ベースまたは機能ベースのインストール」を選択→「対象サーバの選択」に自身のサーバ(デフォルトで選択済み)を選択→「サーバの役割の選択」で「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 AD CS のインストール1

 (2) 「機能の選択」では何も選択せずそのま ま「次へ」をクリック。



図 2.2-28 AD CS のインストール 2

 「Active Directory 証明書サービス」では 内容を確認し「次へ」をクリック。



図 2.2-29 AD CS のインストール 3

④ 「役割サービスの選択」では、「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。



図 2.2-30 AD CS のインストール 4

⑤ 「インストールオプションの確認」では 内容を確認し、「インストール」をクリッ クする。 必要に応じて対象サーバーを自動的に再 起動するにもチェックを入れる。



図 2.2-31 AD CS のインストール5

⑥ インストールが開始され、インストールの進行状況」で進行の状況が表示される。 インストールが終了したら、右のようにその旨が表示される。



 ⑦「閉じる」もしくは「次へ」で役割と機能の追加ウィザードを閉じても良いが、 その場合サーバーマネージャに Active Directory 証明書サービスの構成を促す 通知が表示される。





 ⑧ ⑥もしくは⑦で「対象サーバーに Active Directory 証明書サービスを構成する」を クリックすると、「AD CS の構成ウィザ ード」が実行される



図 2.2-34 AD CS の構成 1

 ⑨ 「役割サービス」では、「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。



 「セットアップの種類」では「エンター プライズ」をチェックして、「次へ」をク リックする。



 「CA の種類」では「ルート CA」をチェ ックして、「次へ」をクリックする。



図 2.2-37 AD CS の構成 4

「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。



CA の暗号化形式で変更する必要がなければ、「次へ」をクリックする。

0=	AD CS の構成		-	
CA の暗号化) dc-2012.exan	甘象サーバー nple.co.jp
資格情報 役割サービス セットアップの種類	暗号化オプションを指定してください 暗号化プル(19-の連訳(<u>C</u>):		キ−長(<u>K</u>):	
CAの種類	RSA#Microsoft Software Key Storage Provider	+	2048	
NDEX+- 昭子化 CA名 有効期間 証明書データペース 確認 当行状況 社堂	この CA が9時行された証明書の書名に使用する/しらえ 7ル302 5HA256 5HA354 5HA512 5HA512 MPD CA が秘密キーにアクセスするときに、管理者による操作を許可	スムを選択 	(H);	
	暗号化の詳細 (1111年1月1日) (1111年1月1日)		- 携成(C)	Jan 1991

「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。



図 2.2-40 AD CS の構成 7

 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 2.2-41 AD CS の構成 8

変更する必要がなければ、「次へ」をクリックする。



図 2.2-42 AD CS の構成 9

確認し問題がなければ、「構成」をクリックする。



図 2.2-43 AD CS の構成 10

インストールの結果を確認し、「閉じる」
 をクリックする。



図 2.2-44 AD CS の構成 11

- 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
- 「サーバーマネージャー」の「管理」から「役割と機能の追加」をクリックして役割と機能の追加ウィザードを起動し、「インストールの種類」に「役割ベースまたは機能ベースのインストール」を選択→「対象サーバの選択」に自身のサーバ(デフォルトで選択済み)を選択→「サーバの役割の選択」で「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 2.2-45 NPS のインストール1

 (2)「機能の選択」では何も選択せずそのま ま「次へ」をクリックする。



図 2.2-46 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 2.2-47 NPS のインストール 3

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



図 2.2-48 NPS のインストール 4

 「インストール内容を確認し、「インストー ル」をクリックする。



図 2.2-49 NPS 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 2.2-50 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、以下 DHCP サーバのインストールは省いて下さい。

「サーバーマネージャー」の「管理」から「役割と機能の追加」をクリックして役割と機能の追加ウィザードを起動し、「インストールの種類」に「役割ベースまたは機能ベースのインストール」を選択→「対象サーバの選択」に自身のサーバ(デフォルトで選択済み)を選択→「サーバの役割の選択」で「DHCPサーバー」にチェックを入れて、「次へ」をクリックする。



図 2.2-51 DHCP サーバのインストール1

 (2)「機能の選択」では何も選択せずそのま ま「次へ」をクリックする。



図 2.2-52 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。



図 2.2-53 DHCP サーバのインストール 3

④ インストール内容を確認し、「インストー ル」をクリックする。



- 図 2.2-54 DHCP サーバのインストール 3
- ⑤ インストールが開始され、インストールの進行状況」で進行の状況が表示される。 インストールが終了したら、右のようにその旨が表示される。



図 2.2-55 DHCP サーバのインストール 3

⑥ 「閉じる」で役割と機能の追加ウィザー ドを閉じても良いが、その場合サーバー マネージャに DHCP サーバーの構成を促 す通知が表示される。



図 2.2-56 DHCP サーバのインストール 3

 ⑦ ⑥もしくは⑦で「DHCP サーバー構成を 完了する」をクリックすると、「DHCP イ ンストール後の構成ウィザード」が実行 される。「説明」画面では内容を確認し「次 へ」をクリックする。

a ()	DHCP インストール後の構成ウイザード
説明	
28明 承認 第9	ターヴット コンピューター上の DHCP サーバーの構成を完了するために、次の手機が実行されます: DHCP サーバー管理の単任用に、次のセキュリティ グループを作成します。 - DHCP Administrators - DHCP Users ターダット コンピューター上の DHCP サーバーを承認します (Fメイン参加の場合)。
	< 前へ(P) (文へ(b) > コミット) キャンセル

図 2.2-57 DHCP サーバのインストール後の構成1

⑧ 「承認」画面で、「以下ユーザーの資格情報を使用する」を選択して、「コミット」をクリックする。

説明	AD DS のこの DHCP サーバーを承認するための美格情報を指定します。
10.60	④ 以下のユーザーの機格情報を使用する(U)
	ユーザー名: EXAMPLE¥Administrator
	○ 代藝藝格達勝F使用する(S)
	ユーザー名: 指定(E)
	○ AD 承認をスキップする(K)

図 2.2-58 DHCP サーバのインストール後の構成 2

 ⑨ 要約を確認し、「閉じる」をクリックする。
 以上で DHCP サーバのインストールは終 了です。

5) 9)	DHCP インストール後の構成ウィザード
要約	インストール後の構成手機の状態が下に示されます:
27966 要约	セキュリティブループの作成
	(四)

図 2.2-59 DHCP サーバのインストール後の構成 3

DHCP スコープを作成する場合は、「サーバーマネージャー」→「ツール」→「DHCP」を開き、サーバ名以下の IPv4 または IPv6 を右クリックして「新しいスコープ」を選択し、新し いスコープウィザードを実行して下さい。

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のダッシュボード画面にて、追加した各役割が存在することを確認します。



図 2.2-60 インストールの確認

以上で、Windows Server 2012 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」→「ツール」
 →「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。

I		al manual a		0
Active Din 分子され 本部のの 本 本 本 の の の の の の の の の の の の の	actory ユーザーとコンと たクエリ le.co.jp tin nputers nain Controllers eignSecurityPrincip laged Service Acco	名前 Builtin Computers Domain Co ForeignSec Managed S Users	 22(デナー コンデナー 32(デナー 32(デナー 32(デナー 32(デナー 32(デナー 32(デナー 32(デナー 32(デナー 	設明 Default container for Default container for Default container for Default container for Default container for
Ur ·	制御の委任(E) 検索(I)			
	新規作成(N)		コンピューター	
	すべてのタスク(K)	•	連絡先	
	最新の情報に更新	i(F)	グループ	
	プロパティ(R)		InetOrgPerson	
	へルプ(H)		msImaging-PSP MSMQ キュー エイ プロッター	s 1772
			2-4-	
			#モフォルダー	

図 3.1-1 ユーザーの設定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)

姓(<u>L</u>):	user1	
名(E):		1=371
フル ネーム(<u>A</u>):	user1	
ユーザー ログオン名(<u>U</u>):	
user1		Commente en la
user1		@example.co.jp v
T-0- 0001000	<u>o</u>).	

図 3.1-2 ユーザーの設定 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: ex	ample.co.jp/Users	
パスワード(<u>P</u>):	•••••	
パスワードの確認入力(C):	•••••	
□ ユーザーは次回ログオン時に	バスワード変更が必要(<u>M</u>)	
□ユーザーはパスワードを変更	できない(<u>S</u>)	
☑ パスワードを無期限にする(⊻	D	
アカウントは無効(<u>0</u>)		
	< 戻る(B) 次へ(N) > キャ	ンセル

図 3.1-3 ユーザーの設定 3

④ 確認し、「完了」をクリックする。

		新しいオブジ	ェクト - ユ	l-ザ-		x
8	作成先:	example.co.jp	/Users			
[完了]	をクリックすると、ス	次のオブジェクトが平定成	ianat:			
フル ネ・ ユーザ- パスワ-	−ム: user1 - ログオン名: u: -ドを無期限にす	er1@example.co 3	ьjp			< >>
			< 戻る(旦)	完了	+ †?	75H

図 3.1-4 ユーザーの設定 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。

(n m) 🖄 🛛		0 0 0 0 0	1 3 2 11 7 2	36	
Active Dire 保存され 常常 exampl 意 の Built 意 Com 意 Dom 意 Fore 意 Man	ctory ユーザーとコンと たウエリ e.co.jp in puters iain Controllers ignSecurityPrincip aged Service Acco	名前 Administra Allowed R 建 Cert Publis 建 Coneable 建 Denied RO 建 DHCP Adm 建 DHCP Users	種類 説明 ユーザー コンピュ セキュリティグル・・・このグバ セキュリティグル・・・このグバ セキュリティグル・・・このグバ セキュリティグル・・・このグバ セキュリティグル・・・・このグバ セキュリティグル・・・・ロHCP セキュリティグル・・・・ロHCP	サー/ドメインの管 レーブのメンバーは, レーブの、ドメイン ユ レーブの、ドメイン ユ サービスに対し管 サービスに対し続	
User	S 制御の受任(E) 検索(I),	-	セキュリティ グル DNS セキュリティ グル DHCP セキュリティ グル ドメイン コンピューター	管理者グループ サーバーなどのほか の管理者	
1	すべてのタスク(K)		連絡先	15942	
	表示(V)		グループ		
	最新の情報に更新 一覧のエクスポー	新(F) h(L)	InetOrgPerson msImaging-PSPs	- 管理者 バーは、	
	プロパティ(R)		MSMQ キュー エイリアス	パーは下	
	へルプ(H)		2-11-	K-122	
		Read-only	共有フォルダー	バーは	

図 3.1-5 グループの設定 1

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。

グループ名(A):	
SALES	
グループ名 (Windows 2000 よりす	前)(<u>W</u>):
SALES	
グループのスコープ	グループの種類
○ Fメイン □-カル(<u>0</u>)	 セキュリティ(S)
● グローバル(G)	〇 配布(D)
○ ユニバーサル(U)	

図 3.1-6 グループの設定 2
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。

			user1のプロ	コパティ		3)
ダイヤルイン 環境		龟	セッション		リモート制御	
IJŦ	リモート デスクトップ サービスのプロファイル		CC	-MC+	フリガナ	
全般	般 住所 アカウント プロファイル		プロファイル	電話	組織	所属するグルーフ
所属す	るグループ(<u>M</u>):				
名前		Active Di	rectory FX1	ンサービス	フォルダー	1
Dom	nain Users	example.	.co.jp/Users			
追加 プライマ プライマ	ロ(D) マリ グループ: (マリ グループ	剤除(<u>B</u>) Domain の設定(<u>S</u>)) Users Macintosh ケーションがな る必要はあり	クライアントま いい場合は、ご ません。	たは POS プライマリ グ	IX 対応のアプリ ループを変更す

図 3.1-7 グループの設定3

 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。

グループ の選択	? X
オブシェクトの種類の選択(<u>S</u>):	
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(Q)
場所の指定(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 (例)(E):	
SALES	名前の確認(<u>C</u>)
詳細設定(<u>A</u>)	OK キャンセル

図 3.1-8 グループの設定4

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。

		1	user1のプロ	コパティ		- T	
ダイ	ヤルイン	環境	t I	セッション	/	リモート制御	
リモ	ート デスクトッ	プサービスのフ	カファイル	0	OM+	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	
所属す	るグループ(M):					
名前		Active Dir	rectory FX1	ンサービス	フォルダー	1	
Dom	ain Users	example.	co.jp/Users				
SALE	S	example.	co.jp/Users				
追加	0 <u>(D</u>)	削除(<u>B</u>)					
プライマ	リ ヴループ: マリ グループ	Domain (D設定(<u>S</u>)	Jsers Macintosh ケーションがな る必要はあり	クライアント い場合は、 ません。	または POS プライマリ グ	IX 対応のアプリ ループを変更す	

図 3.1-9 グループの設定5

 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。

			user1のプロ	コパティ		? *
IJŦ	ートデスクト	ップ サービスの	プロファイル	c	OM+	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	環境	1	セッション		リモート制御
UE-	トアクセス許	可 <u></u>				
(• P	クセスを許可	(<u>W</u>)				
CP	クセスを拒否	(<u>D</u>)				
C N	PS ネットワー	-ク ポリシーでフ	アクセスを制御(」	<u>P)</u>		
「発	信者番号を	確認(⊻):				
ע-ב	バック オプシ	32		1		
(•]	ールバックした	361(<u>C</u>)				
C吗	び出し元に	よる設定 (ルー	ティングとリモー	アクセス・	サービスのみ	•)(<u>S</u>)
の常	に次の電話	番号にコールバ	「ック <u>(Y</u>):			
	的 IP アドレ	スを割り当てる	(I)			
この	ダイヤルインA を定義してくA	妾続に対して有 ださい。	防にする IP ア	۴ fi	的 IP アド	UZ(I)
日静	的ルートを通	图用(<u>R</u>) —				
この! 義し	ダイヤルインオ	<u> </u> 衰続に対して有	効にするルート	を定	静的儿	-h(<u>u)</u>
		OK	キャンセル		適用(<u>A</u>)	へルプ

図 3.1-10 グループの設定 6

3.1.2. NPS の設定

(1) サーバの登録

 「サーバーマネージャー」→「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。



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」→「ツール」→ 「ネットワークポリシーサーバー」から、 「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。



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(T):
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):
なし 🗸
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(<u>S</u>):
•••••
共有シークレットの確認入力(Q): ●●●●●●●●
 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) 認証方法の構成
- (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」→「ツール」→
 「ネットワークポリシーサーバー」から、
 「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 3.1-16 条件の設定 1

 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。

1	新しし ネットワーク ポリシー	x
ネットワーク ポリシー名と接 ネットワーク ポリシーの名前およびおり	続の種類の指定 19ーを適用する接続の登録を指定できます。	
ポリシー名(A):		
ペットノーマオ時級の方法・ いからに構成要求を送信するネットワークアクセスサー ペンター回転しも接定することができますが、どちらも必 802.1X ワイヤレスアクセスポイントの場合は、構造な 802.1X ワイヤレスアクセスポイントの場合は、構造な	バーの種類を選択してください。ネットワークアクセス サーバーの 満では称りません。ネットワークアクセス サーバーが 802.1X 認識 にし を選択してください。	種類を選択するか、[注入イッチまたは
 ネットワークアクセスサーバーの増加(S): 指定なし。 		
○ ペンダー間有公 10 同 日 日 一 受 一		

図 3.1-17 条件の設定 2

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。

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 T NAS 名も描述できます。	
21	NAS IP-4 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 参加工できます。	
2	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 マッチ構文を使用して IPv6 ネッ ドワーンを指定できず。	
X	NAS ボートの接張 NAS ボートの推振の条件は、アナログ電話回線、500k、レスルまたは原語プライベート、ネットワーク、EEE 00211ワイヤー 12、14月47 ーサスト、ストラダムと、79代ス、グライアン/加快用するシダイアの推調を指定します。	

図 3.1-18 条件の設定 3

 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 「イーサネット」をチェックして、「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>)
□ ISDN 同期 □ 仮想 (VPN) □ 同期 (T1 回線) □ 非同期 (干デム)
一般的な 802.1X 接続トンネルの種類(X)
FDDI
✓ イーサネット
U9470X - IEEE 802.11
その他(工)
ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation ADSL-DMT - Asymmetric DSL Discrete Multi-Tone G.3 Fax
 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=イーサネット」が追加されていることを確認する。

		新しんマット	ワーク ポリシー			
》条 · 杨	わ指定 要求に対してこのネット	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。
件(<u>C</u>):						
条件	値 #5 /_++>。	ale :				
牛の説明						
牛の説明 S ポートの種類の3 小 スイッチなど、アク	新作は、アナログ電話版 地スクライアントが使う	回線、ISDN、トンネルま 用するメディアの種類を打	たは仮想プライベー 留定します。	ኑ ネ ットワーク、 IE	EE 802.11 ワイヤレ	ኢ. ክሬሀተ-
件の証明 ら ポートの種類の5 トト スイッチなど、アク	新作は、アナログ電話の 地スクライアントが使う	回線、ISDN、トンネルま 用するメディアの種類を引	たは原想プライベー 設定します。	ት ネットワーク、 IE	EE 802.11 ワイヤレ	ኢ ክ ሬሀ1–
牛のは見明 8 ポートの種類の5 ト スイッチなど、アク	新作は、アナログ電話で やな、クライアントが使う	回線、ISDN、トンネルま 用するメティアの種類を打	たは仮想プライベー 留定します。	ト ネットワーク、IE 	EE 802.11 ワイヤル 編集(<u>E</u>)	ス、わよびイー 和IDR(<u>R</u>)
牛の説明 S ポートの推調の ト スイッチなど、ア	新作は、アナログ電話的 セスクライアントが使う	回線、ISDN、トンネルま 用するメディアの種類短	たは反想75イベー 都定します。	ት ネットワーク、IE ነይክው(፬)	EE 802.11 ワイヤレ 編集(<u>E</u>)	ス、わよびイー 和助(<u>B</u>)
牛の説明 ら ポートの種類の3 ト スイッチなど、アク	新作は、アナログ電話に たったうくアントが使う	回線、ISDN、トンネルま 用するメディアの種類性	たは仮想75イベー 第年(ます。	ト ネットワーク、IE 「適加KD)。	EE 802.11 ワイヤレ 編集(g).	ス、およびイー 単成家(<u>B</u>)
キの見明 S ポートの種類の: ト スイッチなど、アク	5(件は、アナログ電気に わえ クライアントが使う	回線、ISDN、トンネルま 用するメディアの推進を引	たは反想フライベー 第定します。	ト ネットワーク、IE 注意加(①)	EE 802.11 ワイヤレ 編集(5).	2. 8404- NBK(B)

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。

条件の選択	×
件を選択し、「自加」をクリックします。	
ループ	^
Windows グループ Mindows グループの条件は、接換ユーザーまたは接換コンピューターが確認されたグループのに可れなに得容してい があることを指定します。	8409 E
コンピューターグループ レーコンピューター グループの条件は、接続するコンピューターが選択したグループのいずれかに開している必要があること します。	を指定
ユーザーグループ ユーザーグループの条件は、接続ユーザーが確認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(CAP	.はす。
ロケーショングループ HAAP ロケーショングループの条件には、このボジーに一般するために必要な、HOAP (Host Credential Authoris Frontocol ロケージョングループを指定します。HIGAP、20トン以後、NFS と一部のサード パーティ製ネットワークア・	ation カセス ー

図 3.1-21 条件の設定 6

 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	?
オブジェクトの種類の選択(S):		
グループ		オブジェクトの種類(0).
島所の指定(F):		- 20 Iu
example.co.jp		場所(L)
example.co.jp 催択するオブジェクト名を入力し SALES	てください (<u>例)(E</u>):	場所(L) 名前の確認(C)

図 3.1-22 条件の設定 7

 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(こ一致するため)こ必要なグループ メンバーシップを指定(S)	
グループ EXAMPLE¥SALES	
グループの注動(U) のK ギャン	1011 1011

図 3.1-23 条件の設定 8

 9 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。



図 3.1-24 条件の設定 9

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。

新しいネットワークポリシー
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はたは指否するかを構成します。
 ● アクセスを計可する(A) クライアントの損耗就行がこのポリシーの条件に一致する場合、アクセスを計可します。 ● アクセスを拒否する(D) グライアントの損耗就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 ダイヤルイン プロパティ (NPS ポリシーム)の後先をれる) によってアクセスを判断する(S) グライアントの損耗就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(2) 次へ(3) 元7(5) キャンセル

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。

1歳でしていたい。EAP 2021には、EAP の推 第5人前会は、1線再算まれのジービに保護された の記述目的定よりも通用されます。
EAP の追加 また法(A): textext textext



- ② 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。

部立方法の構成 構築家が広のボジーの各件を表たすたれ 調整教室でも正確があります。NPF を使用す EAP を教室でも正確があります。補成要求者	- 近要な10日5方法を、1 つと る 800 IX またば VPN を開 105 ー は、ネットワーり ポリ5	上版家してCKSL、EAP ISE 変化を場合は、接続版家市の	ELCE EAP の後 シービド語をいた の時まれた EAB プロパランの時代	
EAP の種類は、NPS とクライアントとの間で、表示されている様が EAP の種類(1): 「Monsoin」(編集F1)と EAP (FEAP)	Follow	クライアンドに対して、サーバ 要求ポパシーにおいて、保護 れます。	ーがその ID の証明をするための証明書を継択して たわた SAP のために構成された証明書は、この証	(1520)。 藤橋 料書より優先さ
	TABLE	証明書の発行先(1):	dc-2012.example.co.jp	¥
	10 m	フレンドパ名:	dc-2012.example.co.jp	
		9/78:	example-DC-2012-CA-1	
ABTRATOL ABTRATOL AND		WINNES:	2015/10/29 16:48:39	
セキュリティレベムの低い認識方法 ※Messeet 暗年1120日/一ジン 2016-CHAP ×2000 ※1120R468915015284、ユーザーC/2027-R50定意時有する00 ※1120R468915015284、ユーザーC/2027-R50定意時有する00 ■件に2025 (value1x)00		 ○ 高速再接続を有効にす。 □ 増号化リ(インドがないか) EAP の種類(T) 	ð(F) 5イアントとの課題を記述する(C)	
		SESTATION MORTH	t/J-F (EAP-MSCHAP v2)	(U)
□増増化ERLTLIGL/2022年(PAP, SPAPIES) □2025元をネゴンエートせずにクライアンドに補助相等すする □コンピューターの正常性チェックのみを実行する(M)	υ			(D) (D)
		通加(A) 編	CK Allek(R) OK	40/04

図 3.1-27 認証方法の構成(PEAP) 2

③ 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。



図 3.1-28 認証方法の構成(TLS)1

 ④ 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。

スマートカ	コードまたはその他の証明書のプロパティ	x
このサーバーは、接続が完了 書を選択してください。	する前に呼び出し側に識別されます。識別の証拠として使う	証明
証明書の発行先(<u>I</u>):	dc-2012.example.co.jp	~
フレンドリ名:	dc-2012.example.co.jp	
発行者:	example-DC-2012-CA-1	
有効期限:	2015/10/29 16:48:39	
	OK キャンセノ	L

図 3.1-29 認証方法の構成(TLS) 2

⑤ 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			
	認証方法の構成 接続要求がこのポジーの条件を満たすために必要な認証方法を、I つビ上指定してください。EAP 認証には、EAP の相 路を指定する必要がかります。NAP を使用する。802.1X またば VPN を展開する場合は、接続要求ポリシーに保護された EAP を指定する必要が多ります。構成要求ポリシーは、ネットワーク ポリシーの認証証拠定よりも優先されます。			
EAP の種類は、 EAP の種類(Microsoft 保 Microsoft ス	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。 D: 機された EAP (PEAP) マート カードまたはその他の証明書 下へ行動(公)			
 適加(D) セキュリティレ Microsoft 11 ダイスワー・ 増売くに認知 増売くに認知 増売くに認知 環境証の法あ コンピュータ 	編集(E) ● 郵販(E) ペルの値にV起話方法: 信号が認証パージル2(MS-CHAP v2/_0) ドの期間がが切れた後も、ユーザーにパスワードの定置を許可する(J) 管子に記述(MS-CHAP)(2) RO期間が切れた後も、ユーザーにパスワードの定置を許可する(J) ていない認証(PAP、SPAP)(5) にはい認証(PAP、SPAP)(5) にはい認証(FAP、SPAP)(5) にはいただたうイアントに接続を許可する(L) -の正常性チェックのみを実行する(M)			
	前へ(<u>P)</u> 次へ(<u>M)</u> 完了(E) キャンセル			
	図 3.1-30 認証方法の構成 3			

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。

	新しいネットワークポリシー	×
おおうの構成 おおく、接続要す 合、NFS は接続 しい このネットワーク ポシーの単版注意 すべての単版が建設要式に一致し	たが一致する必要がある。ネットワークボリシーの追加パラメーターです。福格要求 東京を自動的に相否します。朝鮮のはオプションです。朝鮮のを構成しない場合は、し い成します。 ない場合、ネットワーク アクセスは拒否されます。	が創約と一致しない場 kへ】をクリックしてくださ
 (1) (1) (2) (2)<td>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離 す。 □ 最大アイドル時間が経過したら切断する(<u>D</u>) 1 合</td><td>位で指定しま</td>	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離 す。 □ 最大アイドル時間が経過したら切断する(<u>D</u>) 1 合	位で指定しま
	前へ(2) 沈へ(12) 売了(5)	本心也儿

図 3.1-31 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ボリシー
設定の構成 ポリシーのすべて のネットワーク ポリシーの設定を に件と利約が用続要求に一致し	のネッ! 毎成し	ドワーク ポッシー条件および制約が一致した場合、NPS は接続要求に対して設定を運用します ます。 とてが許可される場合、この設定が適用されます。
R定(S): RADILS 居性	~	治療療持を Dannic htt/では小逆使せた小牛 接後 Dannic 属性を避け、()産生)
	Ξ	をかったします。新生産病点」など、新生は「RADBIS クライアントに適性されません。必要 な新生については、RADBUS クライアントのドキュメントを参照してください。 新生し 名称 値 Framed Protocol PPP Service-Type Framed
 ・嶋号化 IP 設定 	~	1850(D) 編集(E) 目標(E)

図 3.1-32 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	x			
属性を設定にご追加するには、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ー団有爾性を追加するには、このダイアログ ボックスを開じて 【ベンダー団有】を選択し、 「意加」をクリックしてください。				
アクセスの種類(工):				
v 57/F				
届性(日):				
名前				
Tunnel-Assignment-ID				
Tunnel-Client-Auth-ID				
Tunnel-Client-Endpt				
Tunnel-Medium-Type				
Tunnel-Password				
Tunnel-Preference	~			
110月				
代数のハランスホートで通用できるフロトコル(L21P など)のトンネルを1kbxするときに使うトランスホート メディアを指定 します。				
<u> う首加(A)</u> 開じる(<u>C</u>)]			

図 3.1-33 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	x
腐性名: Tunnel-Medium-Type	
属性の番号: 65	
属性の形式: Enumerator	
属性値: ● 802.1× で一般的に使用する(<u>M</u>)	
802 (includes all 802 media plus Ethernet canonical format)	~
○ その他(Q)	
(ない)	~
OK ++>>t	μ

図 3.1-34 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	x
属性名: Tunnel-Medium-Type	
属性の番号: 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 Et	編集(<u>E</u>)
	肖邶余(<u>R</u>)
	上へ移動(山)
	下へ移動(<u>D</u>)
ОК	キャンセル

図 3.1-35 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ペンダー回有需性を追加するには、このダイアログ ポックスを開けて [ペンダー固有] を選択し、 DÉJMI をクリックしてください。
アクセスの種類(工):
v
兩性(B) :
名前
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
1400
17 ¹ /1
トンネル セッションのグループ ID を指定します。
追加(<u>A</u>) 閉じる(<u>C</u>)

図 3.1-36 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	x
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(E): ① 文字列(S) ① 16 進数(H)		
100		
	OK キャンセ	JL

図 3.1-37 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	x
属性名: Tunnel-Pvt-Group-1	D	
属性の番号: 81		
属性の形式: OctetString		
届性値(<u>T</u>):		
ベンダー	値	追加(<u>A</u>)
RADIUS Standard	100	編集(<u>E</u>)
		肖邶余(<u>R</u>)
		上へ移動(山)
		下へ移動(<u>D</u>)
	ОК	キャンセル

図 3.1-38 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	×
層性を設定に追加するには、層性を選択し、「追加」をクリックしてください。	
注自または定義済みのベンダー固有需性を追加するには、このダイアログ ポックスを開じて [ベンダー固有] を選択し、 [5回加] をクリックしてください。	
アクセスの種類(1):	
বন্দ	
属性(12)	
名前	1
Tunnel-Password	
Tunnel-Preference	
Tunnel-Pvt-Group-ID	
Tunnel-Server-Auth-ID	
Tunnel-Server-Endpt	
Tunnel-Type	
۲ الت	
1.00	
1.R°A:	
使用されるトンネリング ブロトコルを指定します。	
追加(A) 閉じる(C)	

図 3.1-39 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	
属性値: ○ ダイヤルアップまたは VPN で一般的に使用する(<u>C</u>)	
〈ない〉 ~	
● 802.1× で一般的に使用する(M)	
Virtual LANs (VLAN)]
○ その他(<u>0</u>)	
〈なし〉 🗸	1
OK キャンセル	

図 3.1-40 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	x
屬性名: Tunnel-Type	
属性の番号: 64	
属性の形式: Enumerator	
属性値(<u>T</u>):	
ベンダー 値	追加(<u>A</u>)
RADIUS Standard Virtual LANs (VLAN)	編集(<u>E</u>)
	肖耶余(<u>R</u>)
	上へ移動(山)
	下へ移動(<u>D</u>)
ОК	キャンセル

図 3.1-41 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。



図 3.1-42 設定の構成 11

12 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。

カポリシーの完了
Shalt:
5
112
値 EAP またば MS-CHAP v1または MS-CHAP v1 のなワードの期間が切れた後、ユーザー
値 EAPまたは MSCHAP v1または MSCHAP v1 パスワードの期間が均れた後、ユーザニ アクセスを許可する Ten
値 EAP または MS-CHAP v1 または MS-CHAP v1 パスワードの期間がわれた後、ユーザー アクセンをお可する Tue 第全なシットワーク マクヤフ ちなまでする。
値 EAP またば MSCHAP v1またば MSCHAP v1 (パスワードの時間がわりれた後、ユーザー アクセスを許可する Tuae 完全なネットワーク アクセスを許可する PPP

図 3.1-43 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。



図 3.1-44 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 Server 2012 および Windows Server 2012R2 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 2012 または Windows Server 2012R2 にて構築する場合に必要となります。

「サーバーマネージャー」→「ツール」
 →「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 3.1-45 Web サーバ(IIS)の設定1

 「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 3.1-46 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。

「サイドバインドの追加」設定項目

- 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-2012.example.co.jp")を選択

			ታ ተጉ //	インド		
種類 ホス州 http	5 7	f(−ト IP : 30 *	PFUZ	バインド情報		追加(A) 編集(<u>6</u>) 相降(<u>8</u>) 参照(<u>8</u>)
						親じる(丘)
		ţ	オトバイン	ドの追加		? X
種類(工):	IP	アドレス(1)			ポート(0):	
https	< ▶	使用の IP	アドレスすべて		v 443	
ホスト名(日):						
ホスト名(旦):						
ホスト名(<u>H</u>): サーバー名 SSL 証明書(表示を要求す <u>F</u>):	<u>ଟି(N)</u>				
ホスト名(日): サーバー名 SSL 証明書(dc-2012.ext	表示を要求す E): ample.co.jp	ō(<u>N</u>)			逼択(<u>L</u>)	表示(⊻)
ホスト名(日): ロ サーバー名 SSL 証明書(dc-2012.ext	表示を要求す E): ample.co.jp	₹(<u>N</u>)		~ [遥択(<u>L</u>)	表示(⊻)

図 3.1-47 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。

0	インターネット インフォメーション サービス (115) マネージャー	
🛞 🙆 🧳 + DC-2012 + H	11 + Default Web Site + CertSiv +	1 () () () () () () () () () (
ファイル(E) 表示(Y) ヘルプ(H)		N1
##E ・ 日 名 後、 ・ 25-ト ページ	⑦ /CertSrv ホーム フィルター: ・ 〒 株市(G) ・ □ 耳へて表示(A) グループ化:	日本 時間を開く 図 エクスプローラー
Q OC-2012 (EXAMPLENADMini	15 RP HTTP 254/201 HTTP 256/25- MDHE 0485	アウセンド可の構成 「
	SSL 設定 IF- バーシ FOLONUDBE IV/FF- TVE2d E52-16 D/FEB EBB EXE0F42/01 FML/ABRIN/- EMP EXE0F42/01 TR EMP EXE0F42/01 FR EMP EXE0F42/01 FR EMP EXE0F42/01 FR EMP EXE0F42/01	 ▲ **443 (http://98 ■ P#882 ● ヘルプ オンテインへルプ
< # 5	第4117-0- 回 14802-124 シンデング 22-	

図 3.1-48 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。



図 3.1-49 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。

6 6 A . n	インターネット インフォメーション サービス (115) マネージャー	= 0 x
です(A/E) 表示(V) へはガ(H)	AT . REPORT NEW DIG	and the second second
7744E 8m(2) AU7(E) st 	Default Web Site ホーム Уки	 単合 エクスプレーラー アウセスドモリの単単点… アイトの単気 パイクド 基本型を アカケーSakの表示 通常なんがりの表示 通信なんがりの表示 単位と Web サイトの参照 ● 信息 ● 信息 Web サイトの参照 ● 信息 ● パックスの表示 ● 信息 ● パックスの表示 ● パックスの表示 ● パックスの表示 ● パックスの表示 ● パックスの表示
C	1 HIGE1- 10 7070/E1-	
清燥元了 		9 <u>2</u>

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 8、Windows 8.1 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 8 の設定画面にそって手順を示し、差分がある箇所のみ Windows 8、 Windows 8.1 両方の設定方法を示しています。なお Windows 7 および Windows Vista での設定方法につ いては「RADIUS サーバ設定ガイド(Windows Server 2008 編)」を参照下さい。

3.2.1. IEEE802.1X 認証の有効化

Windows 8 および Windows 8.1 など、クライアント向け Windows OS では IEEE802.1X 認証は既定 で無効になっています。ネットワーク接続での「イーサネット」のプロパティで、「認証」タブが無い 場合は、以下の手順にて有効にして下さい。

 「デスクトップ」からチャームの「設 定」→「コントロールパネル」を開き、 「管理ツール」を選択します。

	1 × 1		シュートカット ワール	管理ツール		
77-11	ホーム 共有	表示	管理			~
00	- † 🕅 « 🕫 ٨	てのコントロ	ール パネル項目 → 管理ツール	~ C	管理ツールの検索	ρ,
* 83	まに入り	名明		更新日時	推动	サイズ
	ダウンロード	M 15	CSI 4251-9-	2012/07/26 5:22	5a-hthet	2 KB
	テスクトップ		DBC データ ソース (32 ドット)	2012/07/26 5:29	シュートカット	2 KB
50.	最近表示した場所	F 0	DBC データ ソース (64 ビット)	2012/07/26 5:25	ショートカット	2 KB
		W N	indows PowerShell (x86)	2012/07/26 17:11	ショートカット	3 KB
1 54	ブラリ	(eff W	indows PowerShell ISE (x86)	2012/07/26 5:20	シュートカット	2 KB
	ドキュメント	W Ker	indows PowerShell ISE	2012/07/26 5:20	シュートカット	2 KB
1	ピクチャ	W de	Indows Xモリ診断	2012/07/26 5:17	ショートカット	2 KB
8	ビデオ	開化	マント ビューアー	2012/07/26 5:20	シュートカット	2 KB
1 1	ミュージック	Ph C	ッターネット インフォメーション サービス (IIS 2012/07/26 5:15	ショートカット	2.KB
		100 20	ビューターの管理	2012/07/26 5:19	ショートカット	2 KB
1 32	ピューター	(A) = 1	ボーネント サービス	2012/07/26 5:22	シュートカット	2 KB
■ ローカル ディスク (C:)		(e) サ	-ビス	2012/07/26 5:19	ショートカット	2 KB
		100 2	ステム構成	2012/07/26 5:18	Samhdarh	2.KB
9 70	トワーク	12 5	ステム情報	2012/07/26 5:18	シュートカット	2 KB
		10 2	キュリティが強化された Windows ファー	7 2012/07/26 5:29	ショートカット	2 KB
		1 47	ひ スケジューラ	2012/07/26 5:20	5-9ートカット	2 KB
		(E. 7.	マスク クリーンアップ	2012/07/26 5:22	シュートカット	2 KB
		100 FT	らイブのテフラグと最適化	2012/07/26 5:18	シュートカット	2 KB
		10	フォーマンス モニター	2012/07/26 5:17	ショートカット	2 KB
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ノース モニター	2012/07/26 5:17	シュートカット	2 KB
		i D-	ーカル セキュリティ ポリシー	2012/07/26 5:19	ショートカット	2 KB
		(in ED	剛の管理	2012/07/26 5:29	ショートカット	2 KB
22.(E)(D)		1010 1 12	V'D			Real

図 3.2-1 IEEE802.1X 認証の有効化1

 管理ツールの「サービス」を実行し、 サービスの名前「Wired AutoConfig」 をダブルクリック。

T=(11/E) (B/E(A))	#=00 ar=00		58V				
J71/I(E) 操作(A)	8(示(型) へいつ(日)						
🕈 🏟 🔟 🗐 🗐 🖉							
🔍 サービス (ローカル)	○ サービス (ローカル)						
	Wired AutoConfig	名航		說明	状態	スタートアップの種類	ログオン
		Q Windows	Firewall	Win	実行中	自動	Local
	サービスの開始	Q Windows	Font Cache Se	共通	実行中	自動	Local
		Q Windows	Image Acquisit	7.4	実行中	手動	Local
	說明:	Q Windows	Installer	Win		手動	Local
	Wired AutoConfig (DOT3SVC) #-	Q Windows	Management I	7A.	実行中	自動	Local
	とんは、イーサネットインターフェイスに対して 1000 800 11 約日を実行します。 課	Q Windows	Media Player N	7-100		平動	Netw.
	在のワイヤードネットワーク展開が	Q Windows	Modules Installer	Win		手動	Local
	802.1X 認証を強制する場合、	😪 Windows	Process Activa	Win	実行中	手動	Local
	DOT35VC サービスは、レイヤー 2 接続	Windows	Remote Manag	Win		手動	Netw.
	認識などであり、シークリン・人へのアッセスの	C Windows	Search	771	実行中	自動(遅延開始)	Local
	802.1X 認証を強制しないワイヤードネッ	C Windows	Store Service (Win		手動(トリガー開始)	Local
	トワークには、DOT3SVC サービスによる影	Q Windows	Time	70h	東行中	手動(トリガー開始)	Local
	客はありません。	🛱 Windows	Update	Win		手動(ドリガー開始)	Local
		G WinHTTP	Web Proxy Aut	Win	寅行中	手動	Local
		Q Wired Au	toConfig	Witan		自動	Local
		WLAN AU	toConfig	WL	実行中	自動	Local
		🔍 WMI Perf	ormance Adapter	Win		手動	Local
		🔍 Workstati	ion	SM	実行中	自動	Netw.
		S World Wit	de Web Publishi	12	実行中	自動	Local
		WWAN A	utoConfig	ZØ		手動	Local
		<					>

図 3.2-2 IEEE802.1X 認証の有効化 2

「全般」タブ内のスタートアップの種類を「自動」、サービスの状態を「開始」とするとサービスが起動します。その後「OK」をクリックします。

(ローカル	コンピューター) Wired AutoConfig のプロパティ	×
全般 ログオン	回復 依存關係	
サービス名:	dot3svc	
表示名:	Wired AutoConfig	
説明:	Wired AutoConfig (DOT3SVC) サービスは、イーサネット , インターフェイスに対して IEEE 802.1X 認証を実行します。	~
実行ファイルのパス: C:¥Windows¥sy	; /stem32¥svchost.exe -k LocalSystemNetworkRestricte	ed
スタートアップの 種類(<u>E</u>):	自動	~
<u>サービスのスタートア</u>	<u>ップ オプションの構成の詳細</u> を表示します	
サービスの状態:	停止	
開始(<u>S</u>)	停止(<u>T</u>) 一時停止(<u>P</u>) 再開(<u>R</u>)	
ここでサービスを開始	台するときに適用する開始パラメーターを指定してください。	
開始パラメーター(<u>N</u>	1):	
	OK キャンセル 適用(<u>A)</u>

図 3.2-3 IEEE802.1X 認証の有効化 3

3.2.2. 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
- 「デスクトップ」からチャームの「設定」
 →「コントロールパネル」→「システム」
 よりシステムウインドウを表示させ、「コ
 ンピュータ名、ドメインおよびワークグル
 ープの設定」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



図 3.2-4 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。

コンビューター名/ドメイン名の変更
このコンピューターの名前とメンバーシップを変更できます。変更により、ネット ワーク リソースへのアクセスに影響する場合があります。
コンピューター名(⊆):
nts-win8
フル コンピューター名: nts-win8
≣羊細(<u>M</u>)
所属するグループ
 ドメイン(D):
example.co.jp
○ ワークグループ(W):
WORKGROUP
ОК ‡ т>1211
図 3.2-5 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 Ne	tBIOS 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	र(<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(<u>C</u>)	
NetBIOS コンピューター名(N):			
NTS-WIN8			
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。		

3.2-6 ドメイン参加3

Windows セキュリティ

ドメインに参加するためのアクセス許可のあるアカウントの名前とパスワードを入力して

図 3.2-7 ドメイン参加4

OK

キャンセル

×

コンピューター名/ドメイン名の変更

user1

・・・・・・・ ドメイン: example.co.jp

ください。

- ④ まもなく右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。
 - ※ 右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、 右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。
- コンピューター名/ドメイン名の変更 i example.co.jp ドメインへようこそ。

図 3.2-8 ドメイン参加5

ロクオン画面にて、←矢 デーを選択し、ログオン 全確認し(本ガイドでは <u>3.1.1</u>で作成したユーザ ワードを入力してログオ



図 3.2-9 ドメイン参加6

⑥ 再起動後端末のログオン画面にて、←矢 印から他のユーザーを選択し、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。

(3) 確認方法

CA の証明書を取得している事を確認します。

「デスクトップ」からチャームの「設定」
→「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-2012-CA (CA)」の証明書を
確認する。

5			証明書				
目的(<u>N</u>): <ずべて>							
個人	ほかの人	中間証明機関	信頼されたルート証明機関	信頼され	北発行元	信頼されない発行元	1
発行 中CC 中CC 中CC 中CC 中CC 中CC 中CC 中CC 中CC 中C	洗 :lass 3 Pub :opyright ()igiCert As example-D example-D xample-D wample-D Microsoft A	blic Primary C, c) 1997 Micro sured ID Roo NTS-SV1-CA C1-CA C-2012-CA C-2012-CA-1 uthenticode(t cot Authority	発行者 Class 3 Public Primary Copyright (c) 1997 Mi DigiCert Assured ID R example-1NTS-SV1-C example-DC1-CA example-DC-2012-CA example-DC-2012-CA Microsoft Authenticod Microsoft Root Authenticod	/ Cer cros toot CA CA -1 le(tm	有効期限 2004/0 1999/1 2031/1 2018/0 2015/1 2019/1 2019/1 2019/1 2020/1	フレンドリ名 VeriSign Class Microsoft Tim DigiCert くなし> くなし> くなし> くなし> くなし> くなし> くなし>	< >
インボー 証明書 <すべ	・ト(I) の目的 て>	エクスポート(E)	創除(2)			詳細設定 表示(<u>V</u>)	(A)
证明書	の詳細につい	て表示します。				閉じる()	⊇)

図 3.2-10 CA 証明書の確認

RADIUS サーバ設定ガイド Windows Server 2012 編(初版)

3.2.3. 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 限が無いため一度サインアウトしてください。次にドメインユーザー(本ガイドでは "user1 ")で はなくこのコンピュータの管理者権限のあるローカルユーザーでサインインしてください。
- チャームの「設定」→「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。

🖞 イーサネット onboardのプロパティ	×
ネットワーク 認証 共有	
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 802.1X 認証を有効にする(<u>N</u>) ネットワークの認証方法の選択(<u>M</u>): Microsoft: 保護された EAP (PEAP) ✓ 設定(<u>S</u>) □ 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>R</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(<u>D</u>)	
ОК ‡ тУТИ	

図 3.2-11 PEAP の設定 1

 保護された EAP のプロパティ画面にて 「証明書を検証してサーバーの ID 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-2012-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 EAP のプロパティ	×
接続のための認証方法:	
☑ 証明書を検証してサーバーの ID を検証する(V)	
 次のサーバーに接続する (例: srv1、srv2、.*¥.srv3¥.com)(<u>0</u>): 	
信頼されたルート証明機関(<u>R</u>):	
Class 3 Public Primary Certification Authority	
DigiCert Assured ID Root CA	
example-DC1-CA	
✓ example-DC-2012-CA	
example-DC-2012-CA-1	
Microsoft Root Authority	
<	
接続前の通知(工):	
サーバー名またはルート証明書が指定されなかった場合にユーザーに通知します >	
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>)	
✓ 高速再接続を有効にする(F)	
□ ネットワーク アクセス保護を強制する(N)	
□ サーバーに暗号化バインドの TLV がない場合は切断する(D)	
□ ID プライバシーを有効にする(I)	
OK キャンセル	
	_

図 3.2-12 PEAP の設定 2

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。



3.2.4. 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。 (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。



図 3.2-14 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。

	0 + 8 2 C Strengt Later Streets	
Nizosoft Active Directory URB/84-P2 example-DC-2	12-04-1	
1377		-
ーーー・ Neb ブラウザー、電子メール クライアント、またはほかのプログラ D、メッセージに署名したり、メッセージを昭号化したり、要求し、	山の証明書を要求する Web サイトです。証明書を使用して Web 上でほか。 た証明書の増加によってほかのゼキュリティ タスタを実行したりすることができ ます	カユーザーがあなた白身を識別) 。
30 Web サイトを使って証明稿間 (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	大観を表示することもでさます。
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	
単物量を使まれる 登録での記録教育の基本の状態 CA 証料書、証明書チェーン、または CRL のグウンロード		

図 3.2-15 TLS の設定 2

 「証明書の要求」で、「ユーザー証明書」 をクリックする。



図 3.2-16 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。

	Web アクセスの確認	×
4	この Web サイトはユーザーの代わりにデジタル証明書の操作を実行します。 https://dc-2012.example.co.jp/certsrv/certrqbi.asp?type=0 ユーザーの代わりにデジタル証明書を操作できるのは、既知の Web サイトだけに 制限する必要があります。 この操作を許可しますか?	
	(おい(Y)) (はい(Y))	

図 3.2-17 TLS の設定 4

⑤ 「送信」をクリックする。



図 3.2-18 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。



⑦ 「この証明書のインストール」をクリッ

クする。

😥 🖉 https://do-2012.example.co.jp/cartars/continuh.asp : D + 🖨 🗄 C 🦪 Microsoft Active Directo X	(n. a.
znsoff Active Directory 証明書サービス example-DC-2012-CA-1	4
非常は発行されました	
和次語明書は要求者に発行されました	
20原明書の12ストール	
広義の保存	
(CHOMP)	

図 3.2-20 TLS の設定 7

⑧ ユーザー証明書のインストール完了。

G (g) https://dc.dll/example.co.gc.antini/continipinale/ (A + e E G) (g) Meropolt Active Directo /	0.0
Alkrosoft Active Directory EMIRT9-EX example-DC-2012-CA-1	
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。	

図 3.2-21 TLS の設定 8

 ⑨ チャームの「設定」→「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-2012-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。

					証明書				
的(N):		<	রুশ্ব>						
国人	ほかの人	中間語	明機関	信頼されたル	一卜証明機	関信頼され	れた発行元	信頼され	はい発行元
発行	先		発行者	I		有効期限	フレンドリ	名	
- u	ser1		exam	ple-DC-2012	2-CA	2015/1	<なし>		
ンボー	►(<u>I</u>)	エクスポー	►(<u>E</u>)	削除(图)				詳細設定(点)
ンポー	ト(I)]	エクスポー	ŀ(<u>E</u>)	削除(R)				詳細設定(A)
(ンポー 正明書) 暗号化	ト(I) り目的 ファイル シス	エクスポー テム, 電	ト(E)	削除(R の保護, クライ))				詳細設定(A)
(ンボー 正明書) 暗号化	ト(I) の目的 ファイル シス	エクスポー テム, 電	ト(E) チメール	削除(R の保護, クライ)) P>ト認証				詳細設定(<u>A</u>) 表示(<u>Y</u>)
(ンボー 正明書) 暗号化	ト(I) つ目的 ファイル シス	エクスポー テム,電	ト(<u>E</u>) 子メ−ルペ ∓す	削除(<u>R</u> D保護, クライ))				詳細設定(<u>A</u>) 表示(<u>X</u>)

図 3.2-22 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 が無いため一度サインアウトしてください。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サインインしてください。

 ① チャームの「設定」→「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。

ローサネット onboardのプロパティ
ネットワーク 認証 共有
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、このオブションを選択してください。 ▼ IEEE 802.1X 認証を有効にする(N)
Nicrosoft: スマート カードまたはその他の証明書 ∨ 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>R</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(<u>D</u>)
OK キャンセル

図 3.2-23 TLS の設定 10

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-2012-CA」をチェックし、「OK」をクリックして画面を閉じる。

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) 	
✓ 証明書を検証してサーバーの ID を検証する(⊻) □ 次のサーバーに接続する (例: srv1、srv2、.*¥.srv3¥.com)(<u>0</u>):	
信頼されたルート証明機関(<u>R</u>): Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA example1-NTS-SV1-CA example-DC1-CA vexample-DC-2012-CA example-DC-2012-CA-1 Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority 2010	
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(D) OK キャンセル	

図 3.2-24 TLS の設定 11 (Windows Vista)

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ー」→「ツール」→「イ ベントビューア」→「カスタムビュー」→ 「ServerRoles」→「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。

認証の詳細 接続要求オ ネットワーク 認証プロパー 認証サーバ 認証サーバ 認証サーバ	10シー名 刺シー名 (ダー: Win 〜 dc- ■ ■■	すべての3 802.1XS/ dows 2012.example.c 1P	ユーザーに Windows 記 ALES co.jp	四至後用	
EAP の種類 MSCHAP v2)	0	Microsof	t セキュリティで保護さ	れたパスワード (EAP-	
アカウントの	セッション ID:	17.2			1
検疫情報 :				~	14
ログの名前(<u>M</u>)	セキュリティ				
ソース(S)	Microsoft Wir	dows security	∉ ログの日付(型)	2014/11/10 14:33:45	
イベント ID(E):	6278		タスクのカテゴリ(ゾ)	ネットワーク ポリシー サーバー	
LYCH(L):	信報		キーワード(K):	成功の話 ネットワークボリシー +	サーバ
ユーザー(山):	N/A		コンピューター(B):	dc-2012.example.co.jp	-
オペコード(0):	信奉程				
詳念對情報8(1)	1121-050	ハルブ			

図 3.3-1 サーバログ (PEAP)

RADIUS クライアンド クライアンド クライアント	Dフレンドリ名: IP アドレス:	AX1240S 172.16.0.12	2	
12日初の単体制 接続要求オ ネットワーク 12日アロル 12日アロル 12日の種類 EAPの種類 アカウントの	Uジー名 ポリシー名 (ダー. W マ. dd ■ E ■ むりつコン ID:	すべてのユーザーに Windows II 802 IVSALES indows - 2012example.co.jp AP Microsoft スマートカードまたは -	な正を使用 目 その他の証明書	
3グの名前(M):	セキュリティ			
ノース(<u>S</u>)	Microsoft V	Vindows security & ログの日付(D):	2014/12/11 11:58:11	
(ベント ID(<u>E</u>):	6278	タスクのカテゴリ(ゾ)	ネットワーク ポリシー サー	-71-
rkh(D)	估報	キーワード(K):	成功の監査	
ユーザー(山):	N/A	コンピューター(B):	dc-2012.example.co.jp	
オペコード(<u>0</u>):	情報			
筆る影響業家の	イベントロジ	あへルプ		

図 3.3-2 サーバログ (TLS)

3.3.2. AX スイッチでの確認

show dot1x port xx detail コマンドにて、IEEE802.1X 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。

🖉 COM1 - Tera Term VT				- 0 X
File Edit Setup Control Window	Help			
AX1240S# show dot1x port 0/1 detai	p1			~
Date 2014/12/11 16:46:04 JST				
Port 0/1 (Dynamic)				
AccessControl : Multiple-Auth	PortCor	itrol : Auto		
Status :	Last EA	POL : 001e.0	965.de05	
Supplicants : 1 / 1 / 64	ReAuth	Node : Disabl	le	
TxTimer : 30	ReAuthT	imer : 3600		
ReAuthSuccess : 0	ReAuthF	ail : 2		
SuppDetection : Auto				
VLAN(s): 30,100,200				
Supplicants MAC F Status	AuthState	BackEndState	ReAuthSuccess	
SessionTime(s	<pre>) Date/Time </pre>		SubState	
[VLAN 100] Port(Dynamic)	Supplicants : 1	La contra		
001e.c965.de05 Authorized	Authenticated	Idle	0	
262	2014/12/11 16:	41:43	Full	
AV12405#				
AX12405# AX12405#				
AA12405#				

図 3.3-3 show dot1x port 0/1 detail (AX1240S にて実行)

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 スイッチ 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ー」→「ツール」 →「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。

Active Di @ @ @### @ @ @ @ @ @ @ @ @ @ @ @	rectory ユーザーとコンビ れたケエリ ple.co.jp littin mputers reignSecurityPrincip maged Service Acco com 制御の発任(E) 検索(() 報気役作成(N) すべてのタスタ(K)	名前 Allowed R Cert Publis Cort Publis Cortenable Denied RO Denied RO DHCP Adm DHCP Adm DHCP Adm	個数 ユーザー セキュリティグリー・・・・ セキュリティグリー・・・ セキュリティグリー・・ セキュリティグリー・・ セキュリティグリー・・ セキュリティグリー・・ セキュリティグリー・・ セキュリティグリー・・ セキュリティグリー・・ セキュリティグリー・ ・ セキュリティグリー・ ・ セキュリティグー ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	世期 コンピューター/ドメインの管 このガルーブのメンバーは このガルーブのメンバーはチ このガルーブのシンバーはチ ログリーブのメンバーは DHCP サービスに対し管 DHCP サービスに対し置 DHCP サービスに対して DHCP サーブーなどのほか Ex.2の留理理 DT-クス DFンイン	
	表示(V) 最新の情報に更新 一覧のエクスポート プロパティ(R)	• (L)	グループ InetOrgPerson msImaging-PS MSMQ キュー エィ プロンター	ゲー 力管理者 シバーは、 シバーはド	
	Contraction of the second		1.101	p+1 2/10)	

図 4.1-1 Web 認証用ユーザーの作成 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、「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)

姓(<u>L</u>):	webuser1			
名(E):			1=3711	
フル ネーム(<u>A</u>):	webuser1			
ユーザー ログオン名(!	<u></u>):			
webuser1		@exam	ple.co.jp	~
ユーザー ログオン名(Windows 2000	より前)(<u>W</u>):		
		Junehusen	-1	

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「次へ」、内容を確認して「完了」をクリックする。

8	作成先:	example.	.co.jp/Use	rs	
[完了] をク	リックすると、ガ	Rのオブジェクト	が作成されま	च:	
<i>Jルネ−L</i> ユ−ザー [パスワード	1: webuser ログオン名: w を無期限にす	ı ebuser1@e> 3	kample.co.	jp	~
					~

図 4.1-3 Web 認証用ユーザーの作成 3

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。

ダー	イヤルイン	環境	竟	セッション	/	リモート制御
IJŦ	デスクト	ップサービスの	プロファイル	0	OM+	フリガナ
全般	住所	アカウント	プロファイル	電話	組織	所属するグルーフ
所属す	るグループ(1	4):				
名前		Active Di	irectory ドメイ	ンサービス	フォルダー	
Dom	nain Users	example	.co.jp/Users			
- 14						
追加	۵(<u>D</u>)	削除(<u>R</u>))			
追た プライマ プライマ	¤(⊵)… ™ グループ: (マリグルーン	剤除(B) Domain の設定(S)) Users Macintosh ケーションがな る必要はあり:	クライアント い場合は、 ません。	または POS プライマリ グ	IX 対応のアプリ ループを変更す

 グループの選択画面にて、選択するオブ ジェクト名に <u>3.1.1</u>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の選択(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(Q)
島所の指定(E):	
example.co.jp	場所(<u>L</u>)
雛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>)
詳細設定(A)	ОК <i>‡</i> †>/2/L

- 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。

19-	イヤルイン	環境	ê l	セッション	>	リモート制御
IJŦ	ートデスクトッ	プサービスの	プロファイル	0	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
所属す	るグループ(<u>M</u>):				
名前		Active Di	rectory FX4	シサービス	フォルダー	
Dom	nain Users	example	.co.jp/Users			
SAL	ES	example	.co.jp/Users			
追加	u(D)	削除(R)				
追加	п <u>(D</u>)	削除(<u>B</u>))			
追加 プライマ	ロ <u>(D</u>) アリ グループ:	削除(<u>R</u>) Domain) Users			
追加 プライマ プライマ	ロ(D) ロ グループ: (マリ グループ)	剤除(B) Domain の設定(S)) Users Macintosh ケーションがた る必要はあり	クライアント い場合は、 ません。	または POS プライマリ り	IX 対応のアプリ ループを変更す
<u>追</u> 力 プライマ プライマ	ロ(D) ツ グループ: (マリ グループ	削除(<u>B</u>) Domain の設定(<u>S</u>)) Users Macintosh ケーションがな る必要はあり	クライアント たい場合は、 ません。	または POS プライマリク	IX 対応のアプリ ループを変更す

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。

IJŦ	ートデスクト	ップ サービスの	プロファイル	0	OM+	フリガナ
全般	住所	アカウント	プロファイル	電話	組織	所属するグルーフ
ダイ	イヤルイン	環境	ŧ	セッション	/	リモート制御
リモー で ア C N 下 発 C コール C 写	ト アクセス許 クセスを許可 クセスを拒否 PS ネットワー 信者番番号を バック オプシ ールバックしれ び出し元にし、 なったの事話	可 (<u>(</u> (<u>(</u>)) -ク ポリシーで7 確認(⊻): ヨン ヨン 3い(<u>C</u>) よる設定 (ルー 番号(□)-ル/)	Pクセスを制御 ティングとリモー Cwp(Y):	(E)	サービスのみ	•)(<u>S</u>)
一日 静	i的 IP アドレ ダイヤルインA を定義してくJ i的ルートを通	ルスを割り当てる 登続に対して有 ださい。 範用(<u>R)</u>	ら(I) 「効にする IP)	アド 前	和 IP アド	-Z(I)
この/ 義し	ダイヤルインオ	妾続に対して有	対にするルート	·を定	静的儿	- t(<u>u</u>)

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 2012 編(初版)

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」→「ツール」→
 「ネットワークポリシーサーバー」から、
 「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

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

	新しんネットリークホリシー	
ネットワークス ネットワーク ポリシ	ドリシー名と接続の種類の指定 ーの名前およびポリシーを適用する接続の種類を指定できます。	0
ポリシー名(A): WebE7FFSALES		
NPS に接続要求を送信するネット ペンダー回知」を指定することがで 802.1X ワイヤレス アウセス ポイン/	ワークアクセスサーバーの種類を選択してください。ネットワークア まますが、どちらも必須ではありません。ネットワークアクセスサー/ の場合は、1階定なし」を選択してください。	ウセス サーバーの種類を選択するか、[「一が 802.1X 認証入イッチまたは
播定なし	A Ban The	
0 ベンダー固有(1)		
(14 (QC)		

図 4.1-9 NPS 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。



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。



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=仮想(VPN)」が追加されていること を確認し、「追加」をクリックする。



図 4.1-13 NPS の設定 6

 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	
:件を選択し、「自加」をクリックします。	_
ブループ	
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ーが確認されたグループのいずれがに所属している必要があることを指定します。	2
コンピューターグループ コンピューターグループの条件は、接続するコンピューターが選択したグループのいずれかに置している必要があることを指定 します。	ł
ユーザークループ ユーザークループの条件は、接続ユーザーが確認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。 iOAP	
9 HOAP ロケーショングループ Protocol ロケーショングループの条件には、このボルンーに一般するために必要な HOAP (Host Oredential Authorization Protocol ロケーショングループを指定します。HOAP フロトコルは、NPS と一部のサードバーディ観光をレフンプアのセス	
imbo(D)*+	ンセル

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 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 メンバーシップを指定(S)	
グループ	
ガル	
	1211

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	? ×
オブジェクトの種類の選択(<u>S</u>):	
グループ	オブジェクトの種類(Q)
島所の指定(<u>E</u>):	
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 (例)(E):	
SALES	名前の確認(<u>C</u>)

図 4.1-16 NPS の設定 9

 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 メンバーシップを指定(<u>S</u>)	
グループ EXAMPLE¥SALES	
ヴループの追加(U) ド 『 ド 除 (M) OK キャンセル	

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。



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

13 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 接続要求が、のポジーの条件を満たすために必要な認証方法を、1つじし指定して(ださい。EAP 1 調を指定する必要があります。NAP を使用する SB2 DX または VPN を原用する場合は、接続要求者 EAP を指定する必要があります。接続要求ポジシーは、ネットワークポジラーの認証認定よりも優先され	恐証には、EAP の種 句シーに保護された れまず。
EAP の種類に	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):	
	下へ移動(室)	
1回20(D)- セキュリティ Microsoft 1/200- 開発に認 デ暗号化認 デ暗号化認 ご暗号化認 ご言がはユー・		
	前へ(b) 法へ(b) 完了(E)	年的地址

図 4.1-20 NPS の設定 13

⑭ 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。

	新しいネットワーク ポリシー
おおの構成 おおの構成 おお、	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ーです。福焼要求が相称と一致しない場 実現を自動的に拒否します。例約はオプションです。海豚方を構成しない場合は、したへ」をクリックしてくださ 成します。 ない場合、ネットワーク アクセスは拒否されます。
 (15) アイトル シイムアウト セッション ダイムアウト 油料学様末 ID 日付は3年初の和政 NAS ポートの建築 	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 ■ 最大アイドル特徴が経過したら切断する(①) ■
	前へ(2) 決へ(3) 売了(5) キャンセル

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)

⑤ 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
	ークポリシーー覧に「Web 認証」が追加
	されていることを確認する。



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")

	0.04		
C C Muth://TTTT	0 ° ° C	×	n x w
	LOGIN		
	Please enter your ID and password.		
	user ID [webuar 1		
	password	*	
	Logn		
	LOGOUT		
	Prease push the following button.		
	LUIGUI		
		0	W-1
ř.			synchronizes in 1417 775

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。

🔶 🕒 🖉 http://1.1.1.1/ogi-bin/Login.ogi	.P - EC Ø	2 M (
	Lo gin success		
	Lagin,Time 2014/11/11 1: Lagout Time 2014/11/11 14	35311 JET 45311 JET	
	clean		
	LOGOUT		
	Please push the following t	button.	
	Logout		

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ー」→「ツール」→「イ ベントビューア」→「カスタムビュー」→ 「ServerRoles」→「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。



図 4.3-3 サーバログ (Web 認証)

4.3.3. AX スイッチでの確認

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。



図 4.3-4 show web-authentication login (AX1240S にて実行)

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。

 「サーバーマネージャー」→「ツール」 →「グループポリシーの管理」から「グ ループポリシーの管理」を開き、「グルー プポリシーの管理」→「フォレス ト:example.co.jp」→「ドメイン」-「example.co.jp」→「グループポリシー オブジェクト」と展開し、「Default Domain Policy」を右クリックし「編集」 を選択、グループポリシー管理エディタ ーを起動する。

	グループオ	13-0	管理			0
□ ファイル(F) 操作(A) 表示(V) ウインドウ(V	W) ヘルプ(H)					- 8
Shーブポルシーの管理 A 「ブルンスト example.co.jp A 「アルンスト example.co.jp A 「 アルンスト A 「 Pr4ン A 「 Pr4 A 「 Pr4	Default Domain Polic スコープ III植 設定 書 リンク 表示するリンクの場所(L):	¥ ⊈ [10	example.co.	p.		
 Domain Controllers グループポリシー オブラコント Default Domain Controllers Default Domain Policy 		1 200	20010309671100 勝利 いい見	s9(1): リンクの有効化 はい	/17 example.co.jp	
5 3 XML 24/2- 5 3 X9-9- GPO 5 3 941	GPO (DRUB)(G)	•				
渡 ヴループ ポルシーのモデル作成 同 ヴループ ポルシーの結果	バックアップから違元(R) だックアップから違元(R) 設定のインポート(I) レポートの発存(S)		# -ザーあよびコンビュ・	ターにのみ適用される	F7(S):	1
	表示(V) ここから新しいウィンドウ(W)	•	•			
	コピー(C) 削除(D) 名用の変更(M)					
	最新の情報に更新(F) へしプ(H)	R	Bk(R)	70/(7+(P)	1	
	20 GPO UZRO WMI 741	ターにリン	クされています(W);			
c 0 3	<\$U>			*	職((0)	

図 5.1-1 MAC 認証の設定 1

②「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」を選択し、右画面の「複雑さの 要件を満たす必要があるパスワード」を 右クリックし「プロパティ」を開く。

JP1ル(F) 操作(A) 表示(V) ヘルノ(H)	
🕈 🌩 🙇 🔟 🗙 🖾 😼 🚺 🗂		
▲ エンピューターの構成 ▲ ① ポリシー ト ○ ソフトウェアの設定 ▲ ○ Windows の設定 ト ○ 名前解決ポリシー スクリプト (スタートアップ/シー スクリプト (スタートアップ/シー	ポルシー (2) パスフードの長さ (2) パスフードの広葉単止時間 (2) パスフードの電整を記録する (2) 峰利化を元に戻せなが載でパスワードを保存する	ポリシー設定 6 文字以上 1 日 0 24 回 類功
▲ 通 アカウント ポリシー	職権対さの要件を満たす必要があるパスワード	プロパティ(R)
▶ 11 パスワードのポリシー		ヘルプ(H)
 □ C→加, 例シー □ C→加, 例シー ■ C→加, 例シー ■ 利益にため/0-ブ ■ 利益にため/0-ブ ■ システム ひーくス □ ンイレード (特徴) ネット □ ンイレード (特徴) ネット □ ローレース (本村) ステム □ ローレス キャレつー ■ ログレース キャレつー ■ ログレース キャレつー ■ ログレース キャレー ■ ログレース キャレー ■ ログレース キャレー ■ ログレース オット ■ ログレース オット ■ ログレース オット ■ ログレース オット 		

図 5.1-2 MAC 認証の設定 5

 「無効」を選択して、「OK」をクリック する。

複雑さの要件を満たす必要があるパスワードのプロパティ ? ×
セキュリティ ポリシーの設定 説明
複雑さの要件を満たす必要があるパスワード
✓このボリシーの設定を定義する(D):
○ 有効(E)
● 無効(S)
OK キャンセル 運用(A)

図 5.1-3 MAC 認証の設定 6

 ④ 「複雑さの要件を満たす必要があるパス ワード」が無効になっている事を確認し、 グループポリシー管理エディターを閉じ る。



図 5.1-4 MAC 認証の設定 7

 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。

2	管理者: コマンド プロンプト	_ D X
Microsoft Windows [Ve (c) 2012 Microsoft Co	ersion 6.2.9200] orporation. All rights reserved.	~ =
C:¥Users¥Administrato ボリシーを最新の情報(or>spupdate こ更新しています	
コンビューター ボリシ ユーザー ボリシーの更	ーの更新が正常に完了しました。 新が正常に完了しました。	
C:¥Users¥Administrato	or> <u>∎</u>	
		~

図 5.1-5 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, AX2200S, AX2500S 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, AX2200S, AX2500S と AX2400S, AX3600S シリーズ混在環境では AX1200S, AX2200, AX2500S 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 (mac-authentication id-format 1) に統一して下さい。

⑥ 「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。

(n nþ	2 🖂 🖌 🗋 🗙 🕻		0 1 3 2 2 7	1 🖻 🕏	
Active Active Active A A A A A A A A A A A A A A A A A A A	e Directory ユーザーとコンと 存されたクエリ ample.co.jp Builtin Computers Domain Controllers ForeignSecurityPrincip Managed Service Acco	名前 名前 総 Allow 総 Cert 総 Clone 総 Denix 総 DHCS	福泉 nistra ユーザー ed R セキュリティグル Publis セキュリティグル able セキュリティグル dt RO セキュリティグル Adm セキュリティグル Adm セキュリティグル	設現 コンピューター/ドメインの管 このゲルーブのメンバーは、 このゲルーブのメンバーはテ このゲルーブのメンバーはテ ログループのシンバーは、 DHCP サーンスに対し着 DHCP サーンスに対し着	
	制御の雲任(E) 検索(I)		mins セキュリティ グル date セキュリティ グル	DNS 管理者グループ DHCP サーバーなどのほか	
	すべてのタスク(K)		連絡先	べてのワークス	
	表示(V)	,	グループ	ザスト	
	最新の情報に更新(F) 一覧のエクスポート(L).		InetOrgPerson msImaging-PSPs	ローザー イズの管理者 のメンバーは、	
	プロ/(ティ(R)		MSMQ #1- 11/07	のメンバーはド	
	へルプ(H)		ユーザー	ー/ドメインへの	
		100	tt Wite I de	The off the	

図 5.1-6 MAC 認証の設定 9

- ⑦ 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

姓(上):	00001111	2222	
名(E):		イニシャル	
フル ネーム(<u>A</u>):	NTS-DPC	02	
ユーザー ログオン名(<u>u</u>):		
000011112222		@example.co.jp	~
ユーザー ログオン名	(Windows 2000	より前)(<u>W</u>):	
EXAMPLE¥		000011112222	1

図 5.1-7 MAC 認証の設定 10

 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	X
🤱 作成先: example	.co.jp/Users	
パスワード(P):		
□ ユーザーは次回ログオン時にパスワー	F変更が必要(<u>M</u>)	
□ ユーザーはパスワードを変更できない	(<u>5</u>)	
□ アカウントは無効(<u>0</u>)		
	< 戻る(旦) 次へ(N) >	キャンセル

図 5.1-8 MAC 認証の設定 11

⑨ 「完了」をクリックする。

		新しいオブ	ジェクト - ユ-	ザー	
8	作成先:	example.co.j)/Users		
[完了]	をクリックすると、2	欠のオブジェクトが4年5	載されます:		
ユーザ- パスワ-	- ログオン名: 00	00011112222@e	kample.co.jp	(Ň
					~

図 5.1-9 MAC 認証の設定 12

 ① 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。

ダイヤルイン リモート デスク 全般 住所 所属するグループ(環境 トップ サービスのご アカウント	^見	+7w3.a			
リモート デスク 全般 住所 所属するグループ(トップ サービスの: アカウント	プロファイル	L//2/	/	リモート制御	
全般 住所 所属するグループ(アカウント		C	OM+	フリガナ	
所属するグループ(住所 アカウント プロファイル 電話 組織		カウント プロファイル 電話 組織 所属する		所属するグループ
	<u>M</u>):					
名前	Active Di	rectory ドメイ	ンサービス	フォルダー		
Domain User	s example.	.co.jp/Users				
追加(<u>D</u>) プライマリ グループ	削除(<u>R</u>) : Domain	Users Macintosh	5-イアント	または POS		

図 5.1-10 MAC 認証の設定 13

 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 の選打	R ?)
オブジェクトの種類の選択(<u>S</u>):	
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(Q)
場所の指定(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 (例)(E):	
SALES	名前の確認(<u>C</u>)
詳細設定(<u>A</u>)	OK キャンセル

図 5.1-11 MAC 認証の設定 14

① 「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。

		NTS	S-DPC020	のプロパティ	(?	•
ダイ	ヤルイン	環境		セッション		リモー	卜制御	1
リモ	リモート デスクトップ サービスのフ		クトップ サービスのプロファイル COM+		-MC+	フリガナ		-
全般	般住所フ		プロファイル	電話	組織	所属	するグリ	レープ
所属す	るグループ(<u>M</u>)):						
名前		Active Dir	ectory FX-	ンサービス	フォルダー			1
Dom	ain Users	example.	co.jp/Users					
SALE	S	example.	co.jp/Users					
追加 プライマ プライ	ロ(D) リグループ: マリグループの	削除(<u>R</u>) Domain (D設定(S)	Jsers Macintosh ケーションがな る必要はあり	クライアントす い場合は、ご ません。	たは POS プライマリ グ	IX 対応0 ループを1	のアプリ	

図 5.1-12 MAC 認証の設定 15

 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。

リモ	ートデスクト	ップ サービスの	プロファイル	0	OM+	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
与一	イヤルイン	環境	兒	セッション	>	リモート制御
リモー	ト アクセス許	可				
• P	クセスを許可	(<u>W</u>)				
CP	クセスを拒否	5(<u>D</u>)				
CN	PS ネ ットワ-	ークボリシーでフ	アクセスを制御(E)		
「発	信者番号を	(確認(⊻):				
コール	バック オブシ	e>		· ·		
• 1	ールバックした	\$U\(<u>C</u>)				
CB	が出し元に	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	+)(<u>S</u>)
0 \$	に次の電話	番号にコール/	(ック <u>(Y</u>):			
「前	略り IP アドレ	ノスを割り当てる	ō(<u>I</u>)			
このレス	ダイヤルインオ を定義してく	接続に対して有 ださい。	I効にする IP ア	۴	的 IP アト	UZ(I)
「前	的ルートを追	^{園用(<u>R</u>)}				
	ダイヤルインオ	接続に対して有	「効にするルート	を定	静的儿	-+(<u>U</u>)
この 義し	cuccos					

図 5.1-13 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ー」→「ツール」→ 「イベントビューア」→「カスタムビュー」 →「ServerRoles」→「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。



図 5.2-1 サーバログ (MAC 認証)

5.2.2. AX スイッチでの確認

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。



図 5.2-2 show mac-authentication login (AX1240S にて実行)



2015 年 2 月 13 日 初版 発行 資料 No. NTS-14-R-030

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