RADIUS サーバ設定ガイド
Windows Server 2008 編

for the Guaranteed Network

第2版

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（http://www.alaxala.com/jp/techinfo/index.html）

本ガイド使用上の注意事項

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

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	ー	2008.6.20	初版発行	ー
第 2 版	ー	2010.2.17	・使用機器の変更 Windows Server 2008 R2 の追加 AX3630S,AX2430S(Ver10.7) → (Ver11.2.A) AX1230S(Ver1.3.D) → AX1240S(Ver2.2) クライアント端末に Windows 7 Professional の追加	全体
			・AX1230S から AX1240S への装置変更に伴う AX コンフィグレーション例の更新。	1.2.1
			・「1.3 Windows Server 2008 と Windows Server 2008 R2 の差分について」を追加	1.3
			・コンピュータ名の変更を「2.2 コンポーネントの追加」から「2.1 準備」に移動。	2.1.2
			・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	ー

目次

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

※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

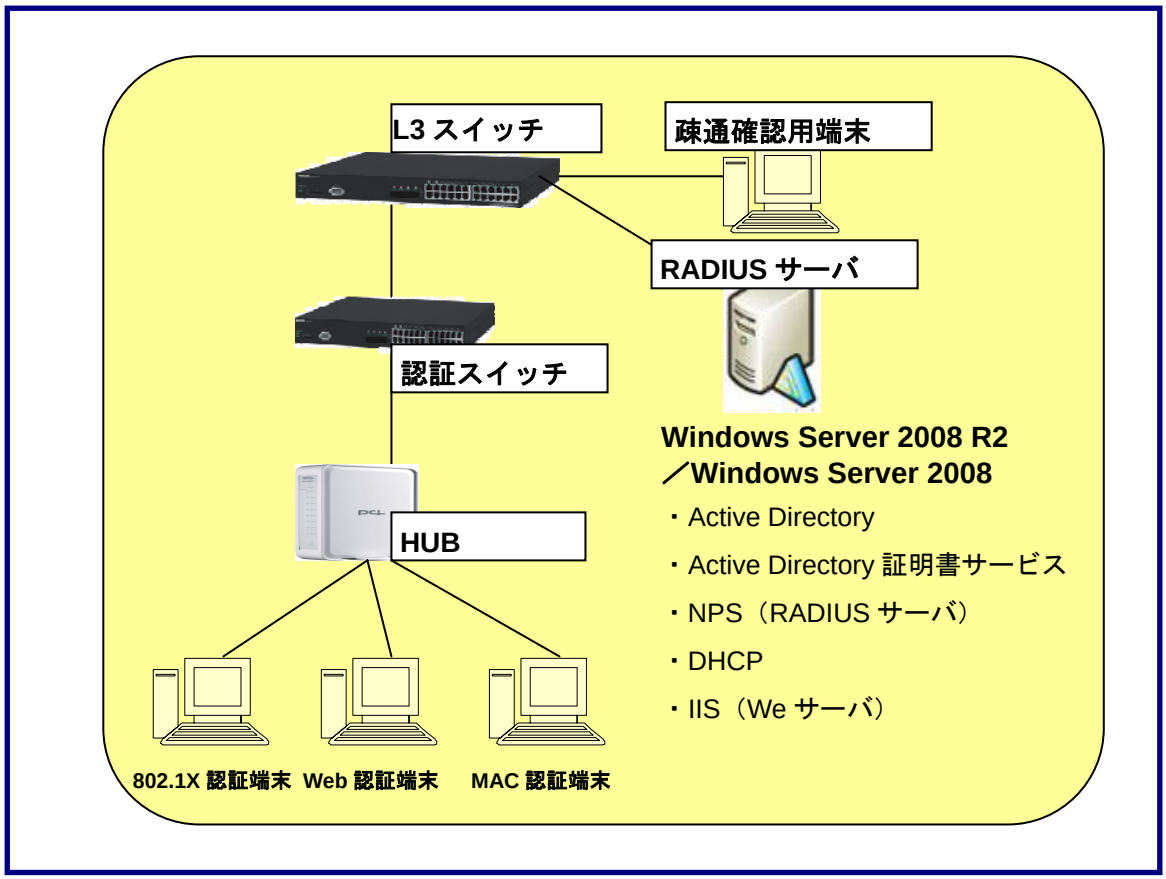


図 1.2-1 構成図

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、⑯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、⑭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

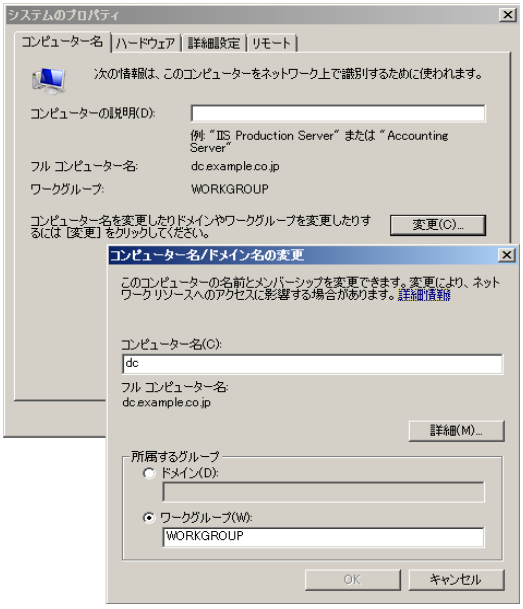
2.1.1. ネットワークアダプタの設定

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。

① 「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

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 「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。

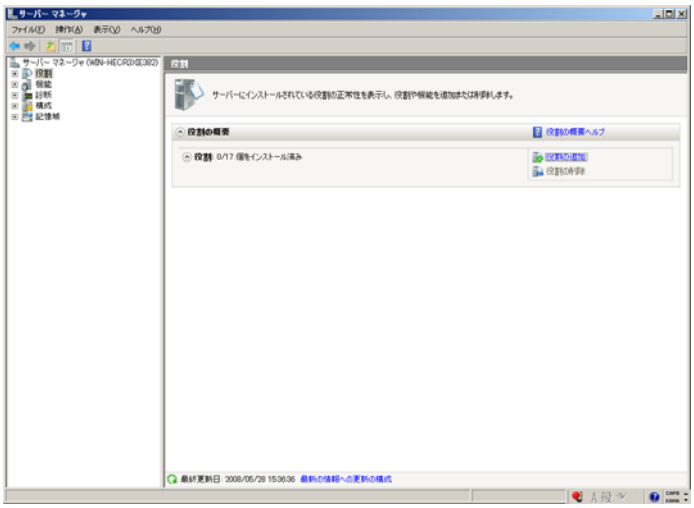


図 2.2-1 Active Directory のインストール 1

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。

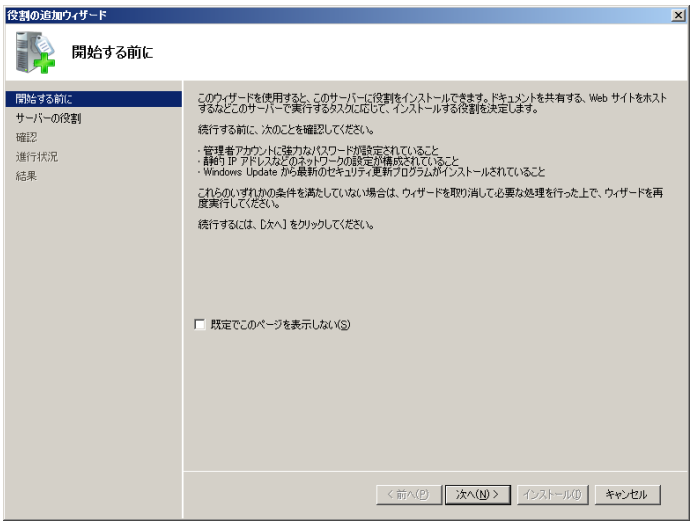


図 2.2-2 Active Directory のインストール 2

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

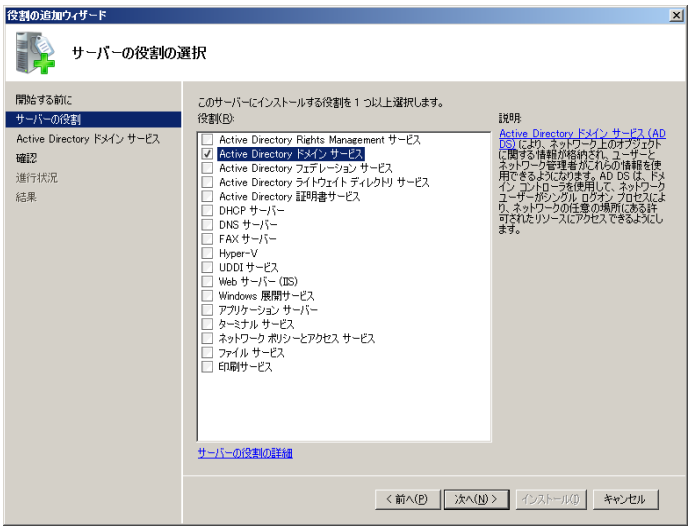


図 2.2-3 Active Directory のインストール 3

※ 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。）

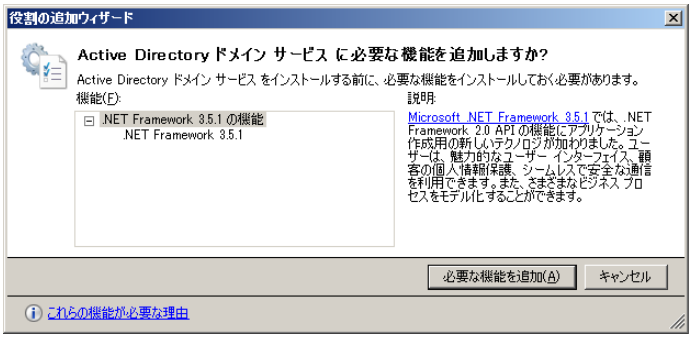


図 2.2-4 Active Directory のインストール 3-1

④ 内容を確認して、「次へ」をクリックする。

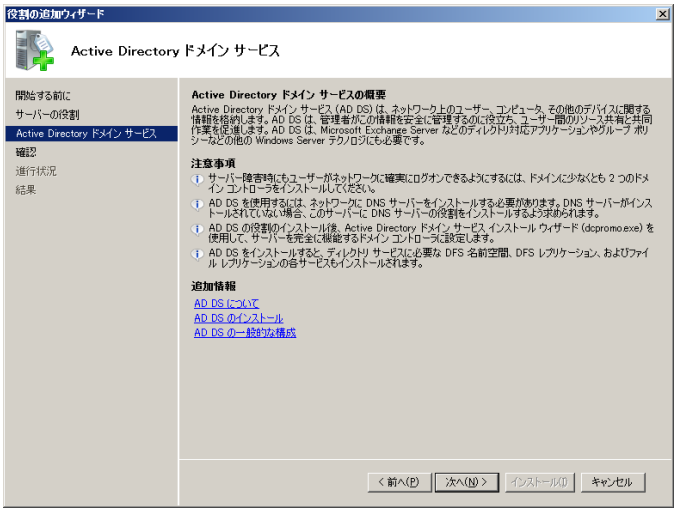


図 2.2-5 Active Directory のインストール 4

⑤ 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）

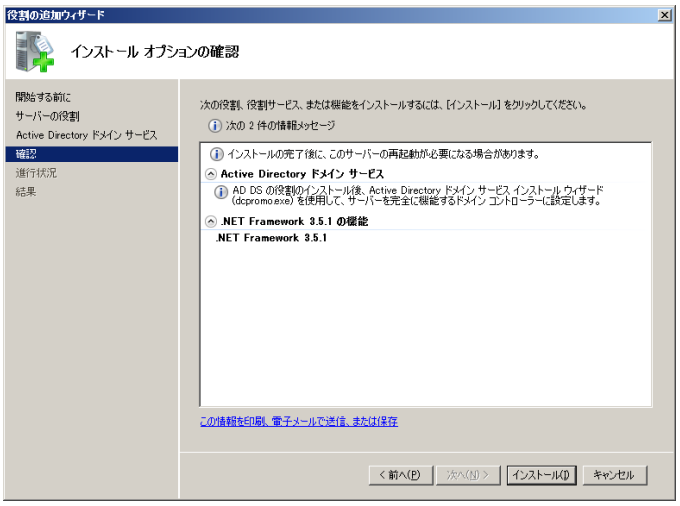


図 2.2-6 Active Directory のインストール 5

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）

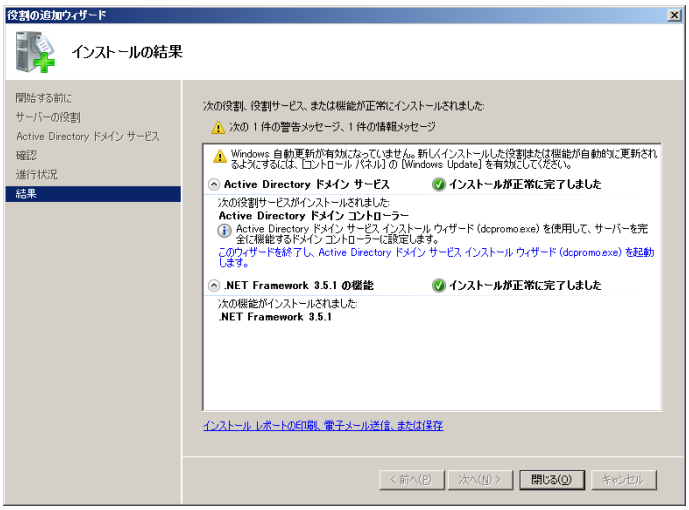


図 2.2-7 Active Directory のインストール 6

⑦ 「次へ」をクリックする。

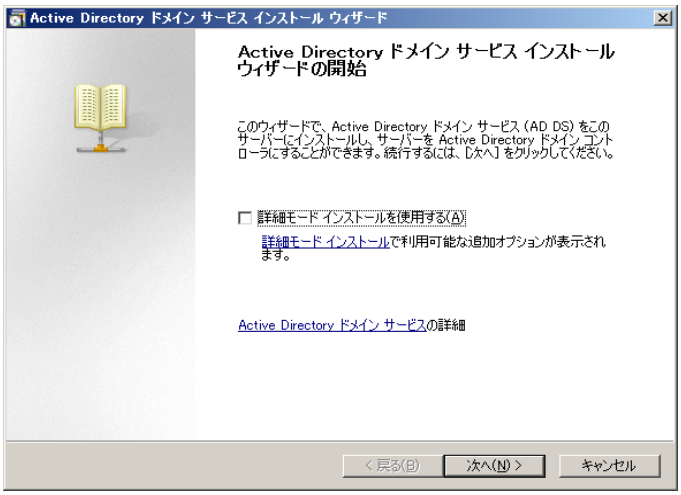


図 2.2-8 Active Directory のインストール 7

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）

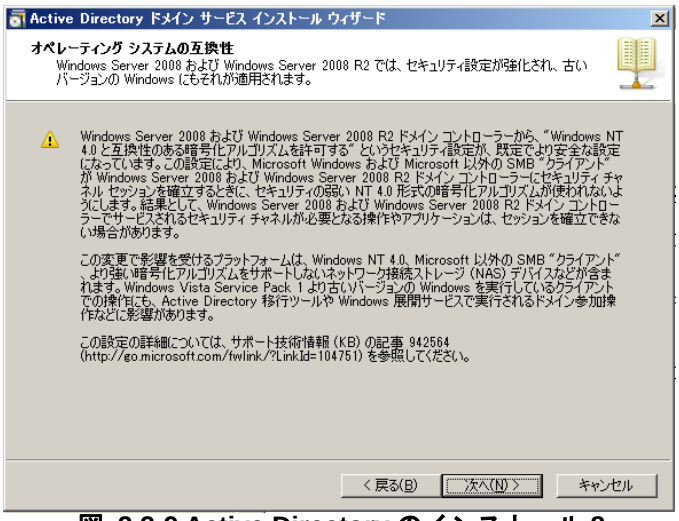


図 2.2-9 Active Directory のインストール 8

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。

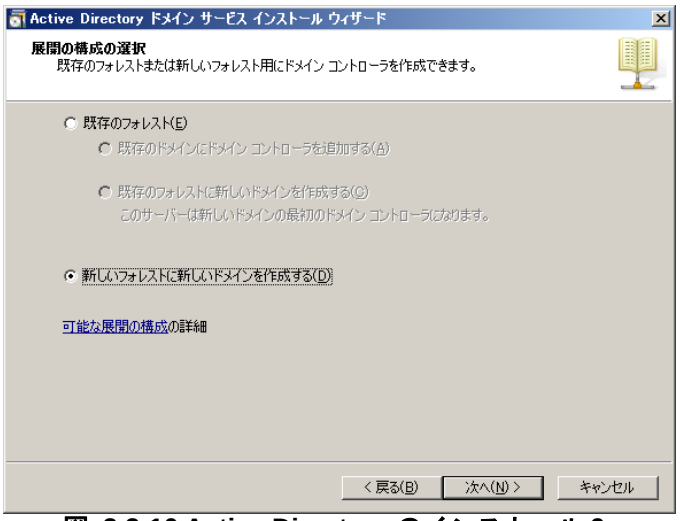


図 2.2-10 Active Directory のインストール 9

⑩ 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。

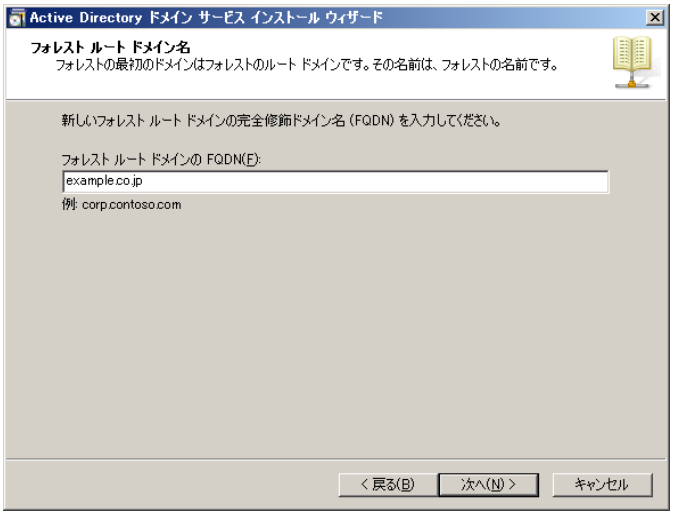


図 2.2-11 Active Directory のインストール 10

⑪ 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。）

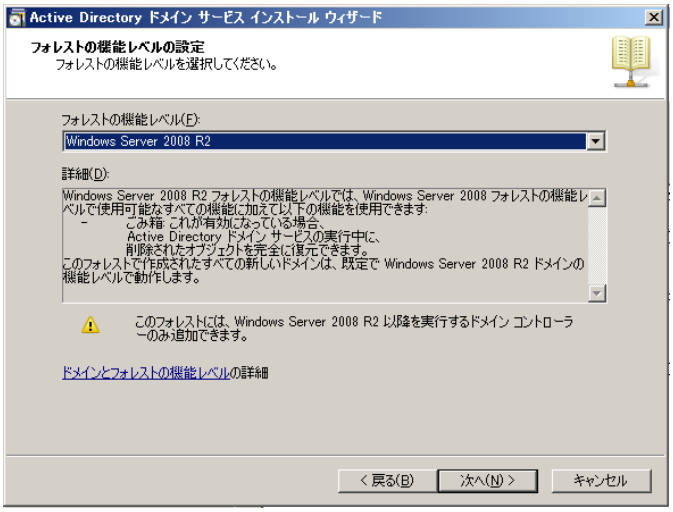


図 2.2-12 Active Directory のインストール 11

⑫ 「DNS サーバー」に、チェックし、「次へ」をクリックする。

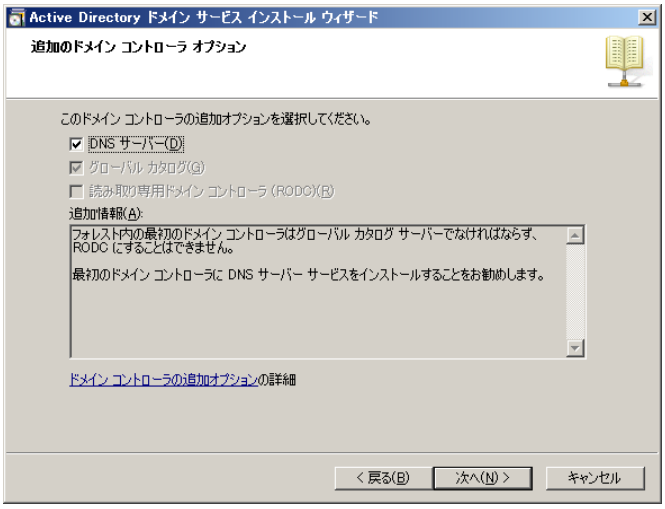


図 2.2-13 Active Directory のインストール 12

⑬ 質問を確認して問題なければ「はい」を選択する。

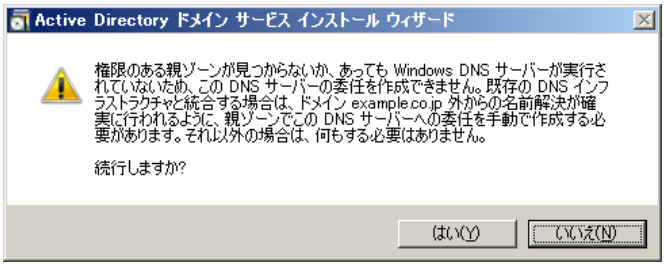


図 2.2-14 Active Directory のインストール 13

⑭ 「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。

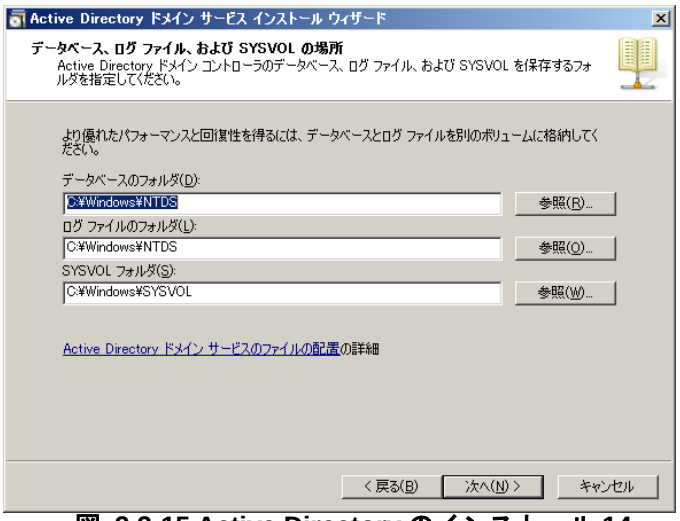


図 2.2-15 Active Directory のインストール 14

⑮ 任意の復元パスワードを入力、「次へ」をクリックする。

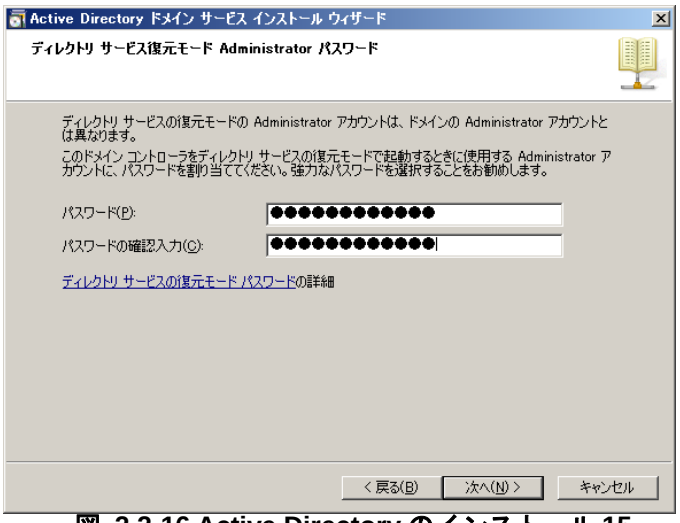


図 2.2-16 Active Directory のインストール 15

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）

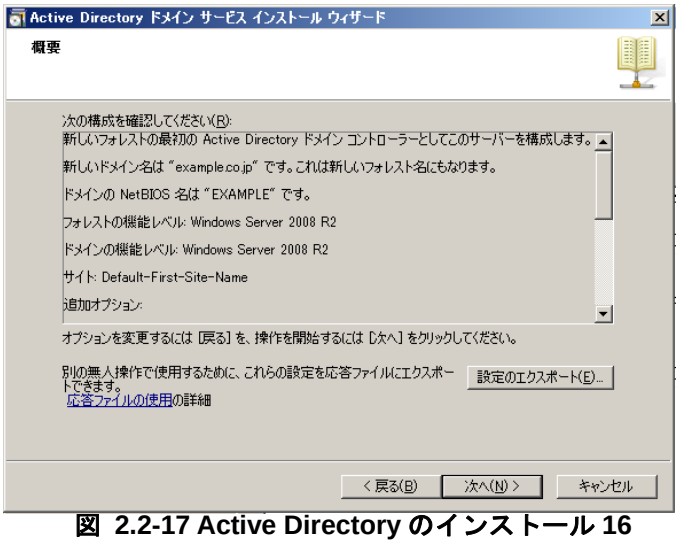


図 2.2-17 Active Directory のインストール 16

⑰ 「完了」をクリックしてサーバを再起動する。

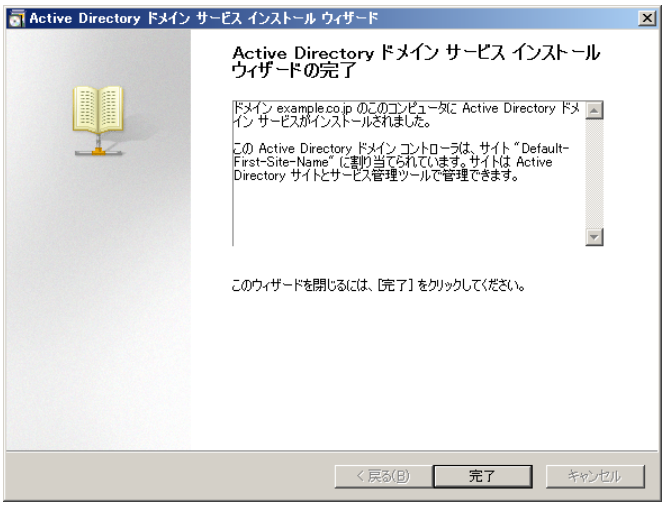


図 2.2-18 Active Directory のインストール 17

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。

① 「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。

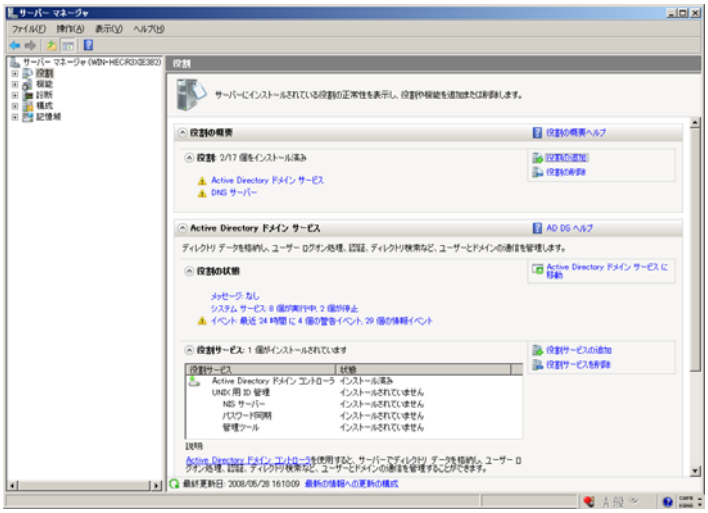


図 2.2-19 Web サーバ(IIS)のインストール 1

② 「Web サーバ（IIS）」にチェックを入れ「次へ」をクリックする。

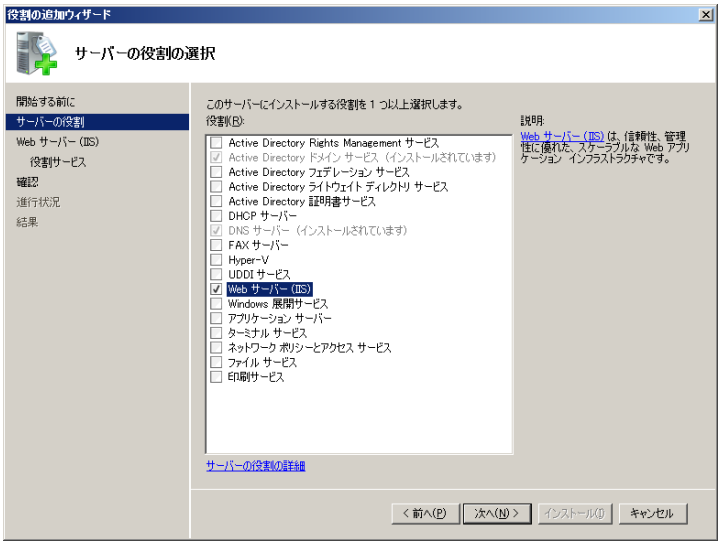


図 2.2-20 Web サーバ(IIS)のインストール 2

※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。

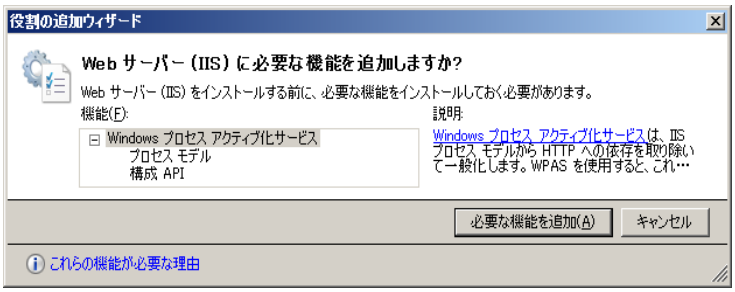


図 2.2-21 Web サーバ(IIS)のインストール 2-1

③ 内容を確認し、「次へ」をクリックする。

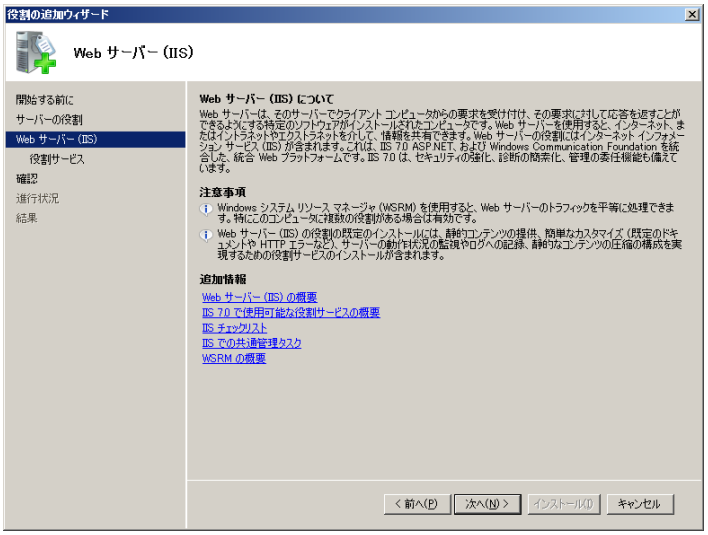


図 2.2-22 Web サーバ(IIS)のインストール 3

④ 他に追加する必要がなければ、「次へ」をクリックする。

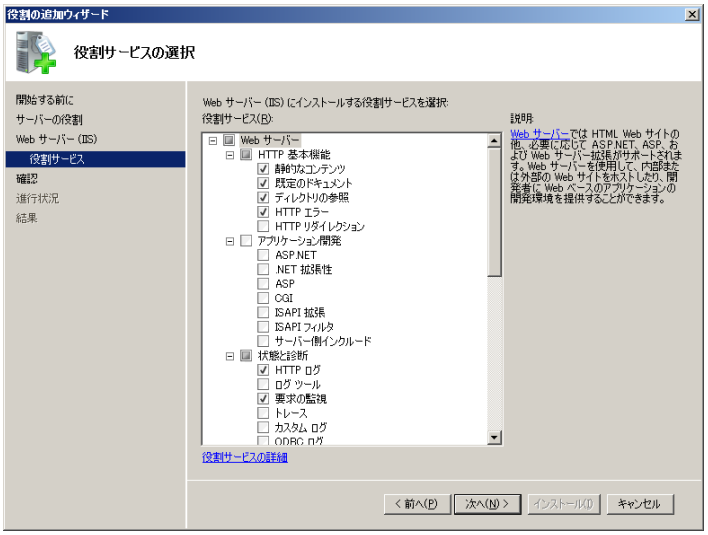


図 2.2-23 Web サーバ(IIS)のインストール 4

⑤ 内容を確認し、「インストール」をクリックする。

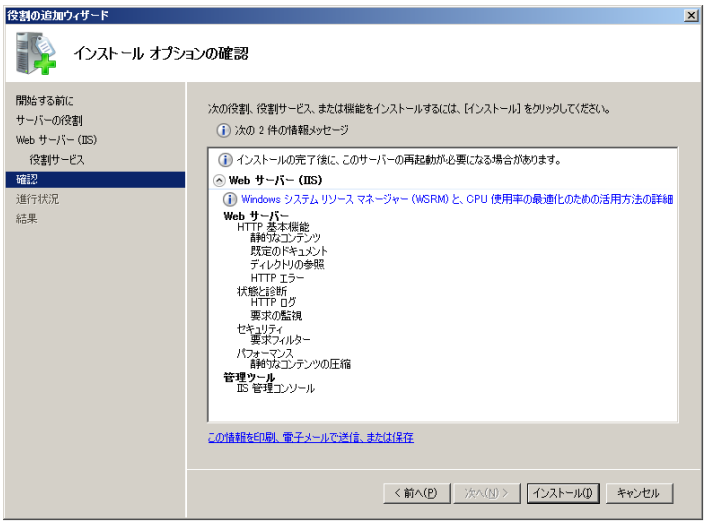


図 2.2-24 Web サーバ(IIS)のインストール 5

⑥ インストールの結果を確認し、「閉じる」をクリックする。

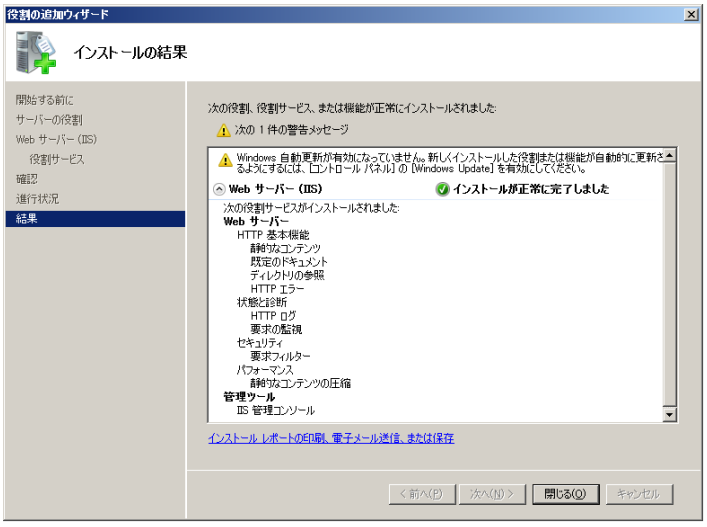


図 2.2-25 Web サーバ(IIS)のインストール 6

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ト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。

① 「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。

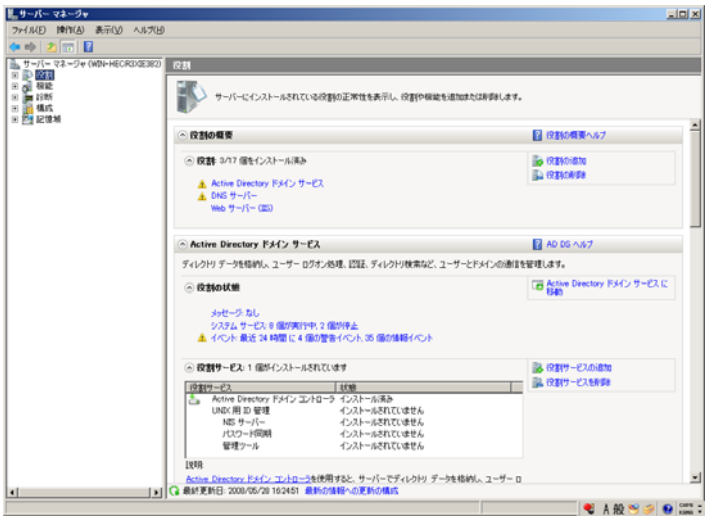


図 2.2-26 Active Directory 証明書サービスのインストール 1

② 「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。

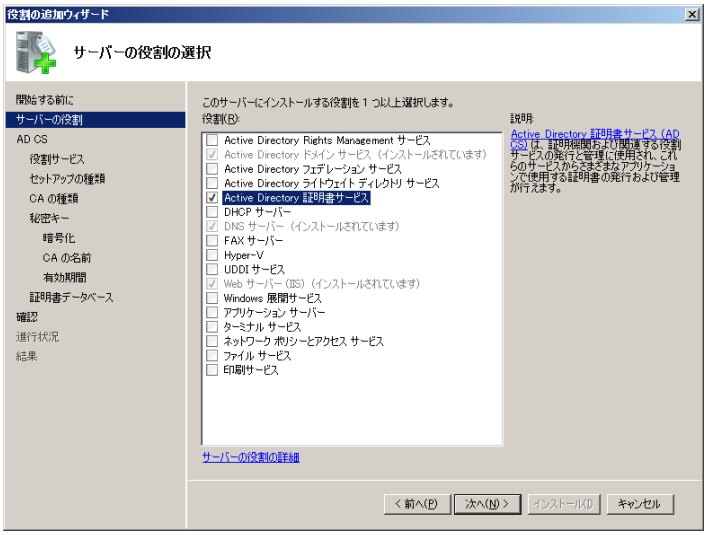


図 2.2-27 Active Directory 証明書サービスのインストール 2

③ 内容を確認し、「次へ」をクリックする。

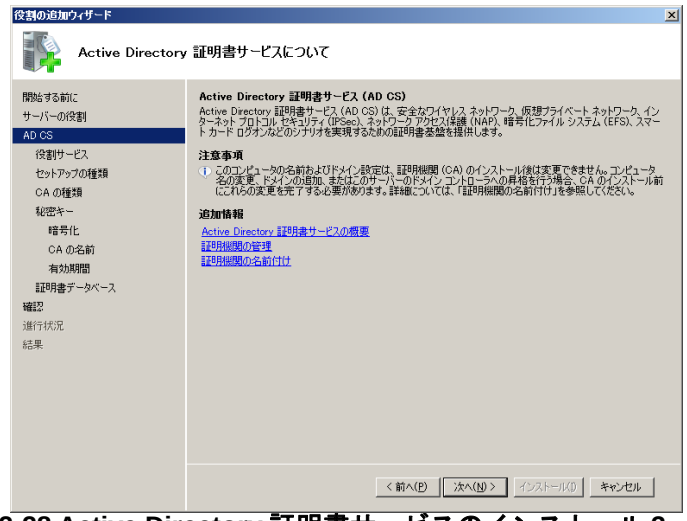


図 2.2-28 Active Directory 証明書サービスのインストール 3

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）

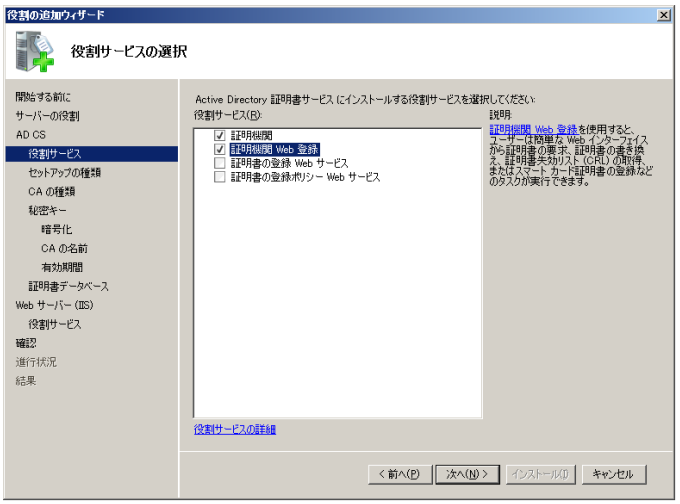


図 2.2-29 Active Directory 証明書サービスのインストール 4

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。

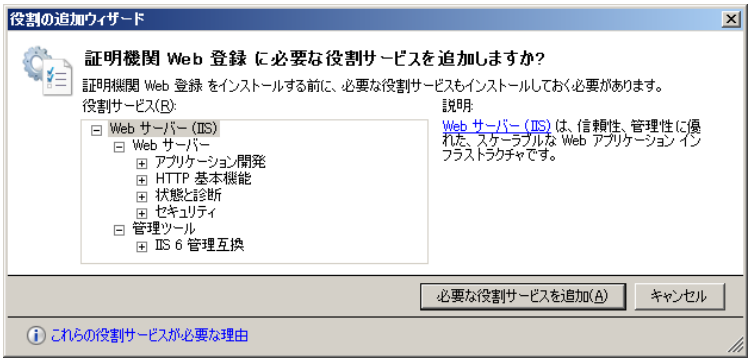


図 2.2-30 Active Directory 証明書サービスのインストール 5

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。

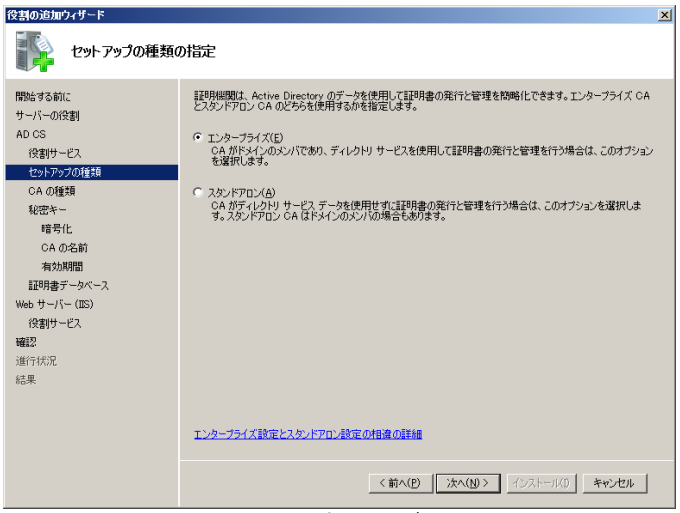


図 2.2-31 Active Directory 証明書サービスのインストール 6

⑦ 「ルート CA」をチェックして、「次へ」をクリックする。

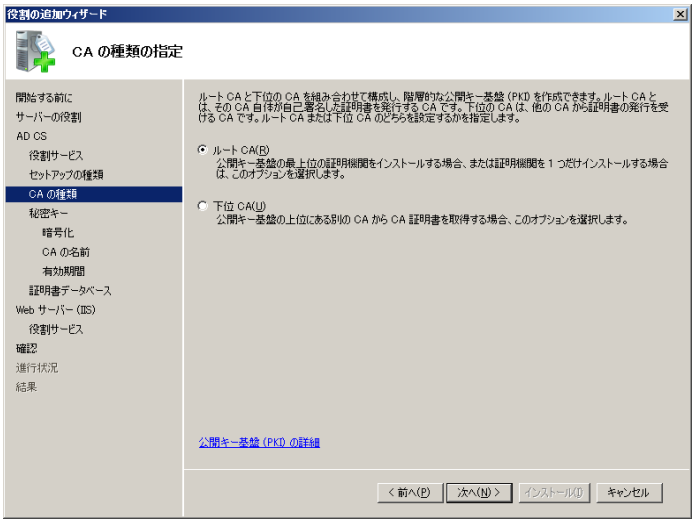


図 2.2-32 Active Directory 証明書サービスのインストール 7

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。

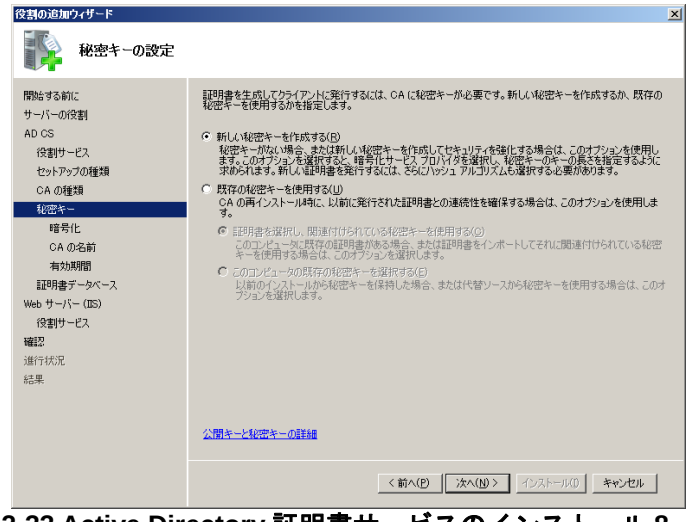


図 2.2-33 Active Directory 証明書サービスのインストール 8

⑨ 変更する必要がなければ、「次へ」をクリックする。

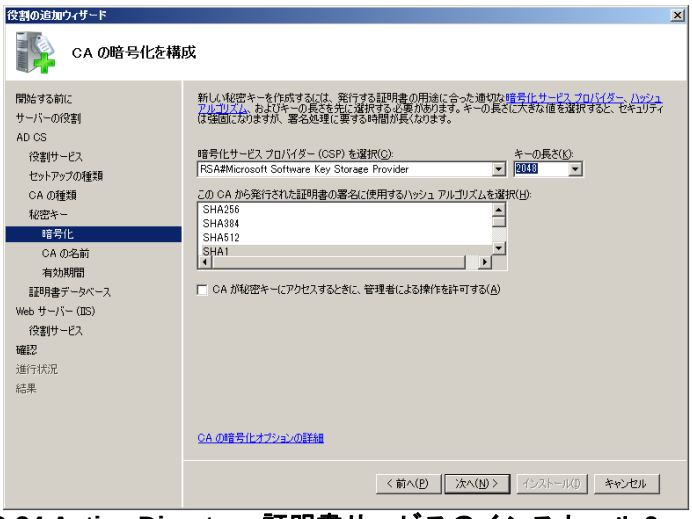


図 2.2-34 Active Directory 証明書サービスのインストール 9

⑩ 「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。

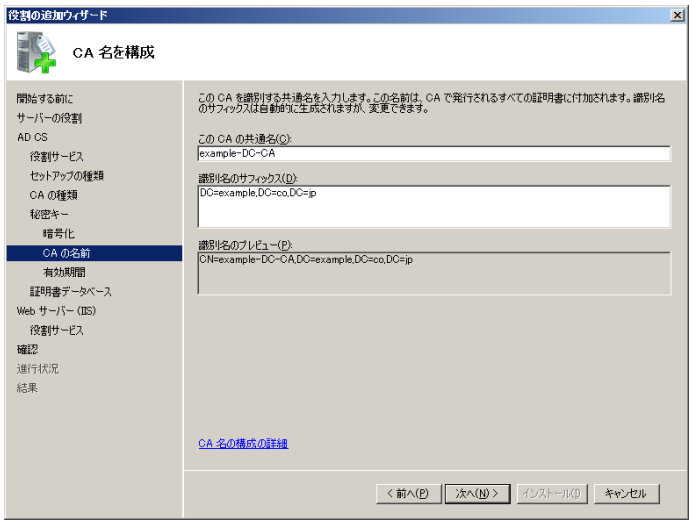


図 2.2-35 Active Directory 証明書サービスのインストール 10

⑪ 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。

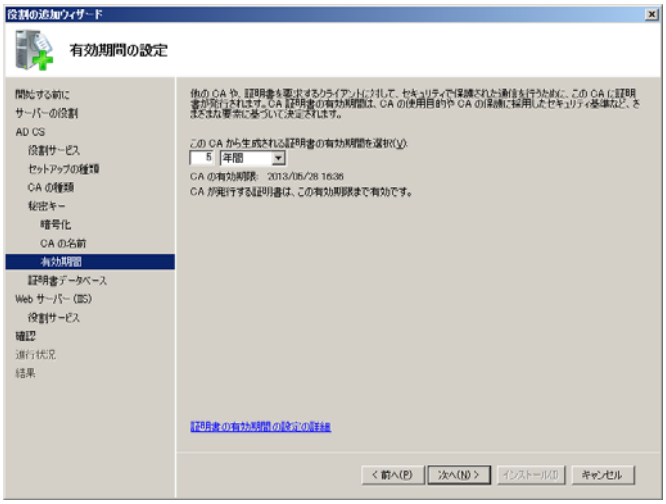


図 2.2-36 Active Directory 証明書サービスのインストール 11

⑫ 変更する必要がなければ、「次へ」をクリックする。

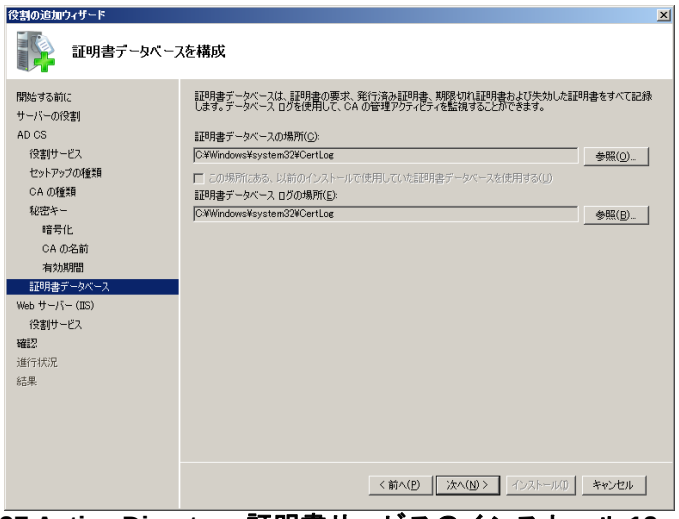


図 2.2-37 Active Directory 証明書サービスのインストール 12

⑬ 確認し問題がなければ、「次へ」をクリックする。

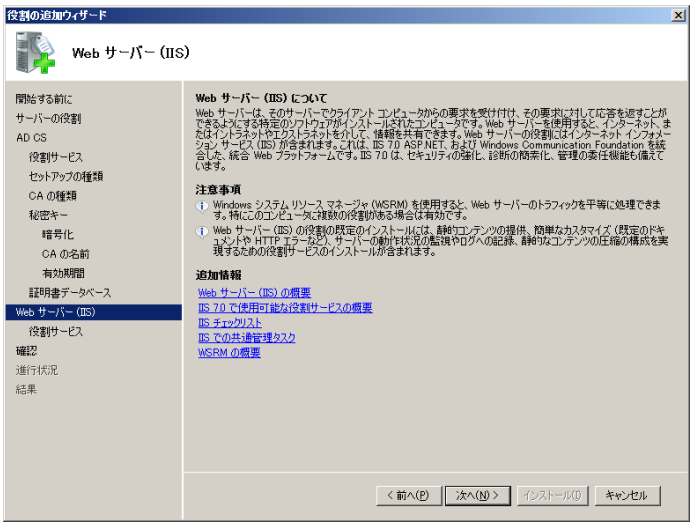


図 2.2-38 Active Directory 証明書サービスのインストール 13

⑭ 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)

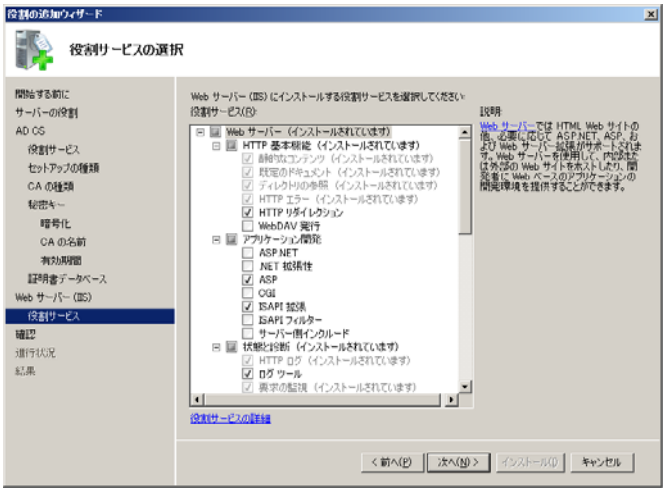


図 2.2-39 Active Directory 証明書サービスのインストール 14

⑮ 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。

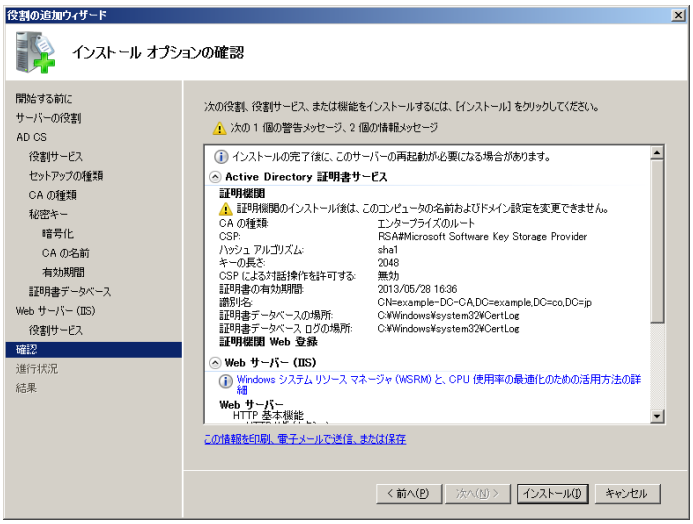


図 2.2-40 Active Directory 証明書サービスのインストール 15

⑯ インストールの結果を確認し、｢閉じる」をクリックする。

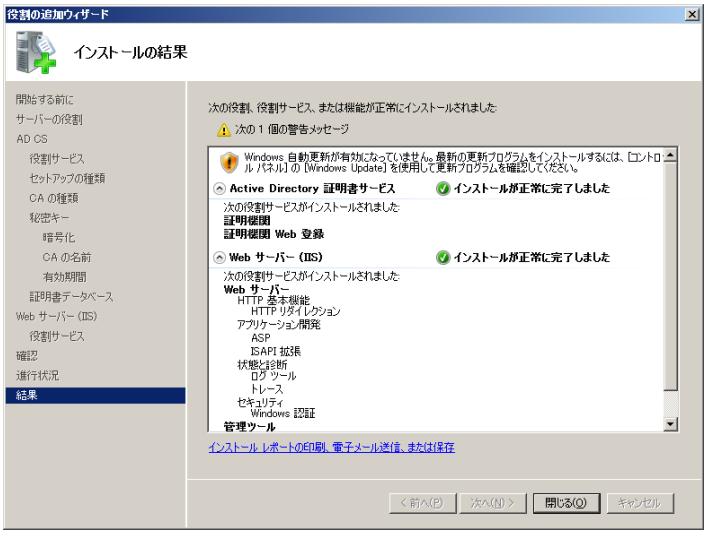


図 2.2-41 Active Directory 証明書サービスのインストール 16

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

① 「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 2.2-42 NPS のインストール 1

② 「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。

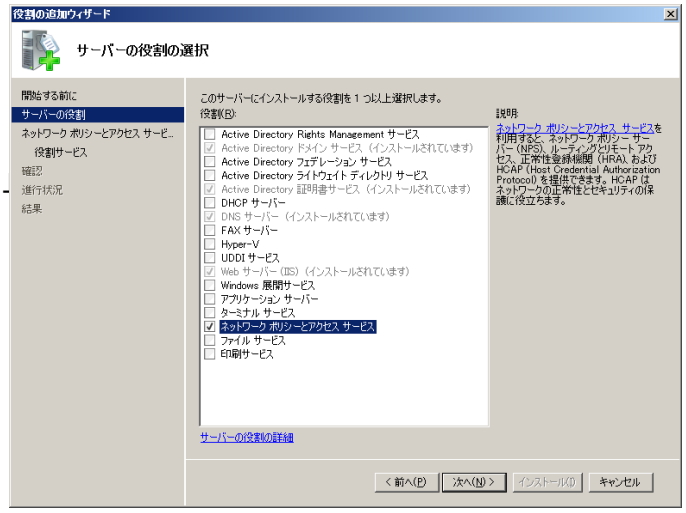


図 2.2-43 NPS のインストール 2

③ 内容を確認し「次へ」をクリックする。

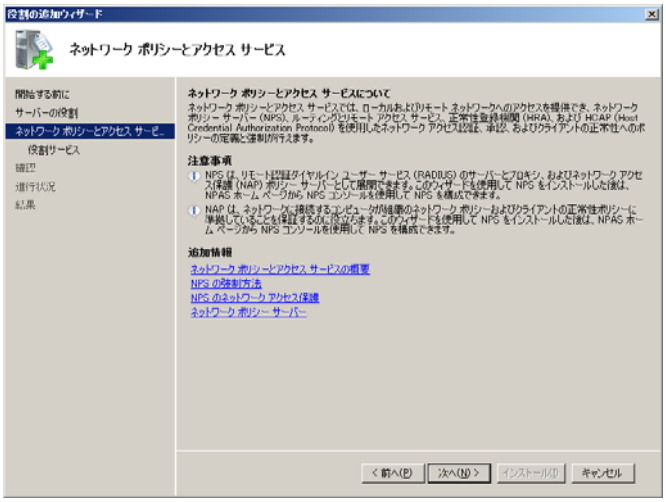


図 2.2-44 NPS のインストール 3

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。

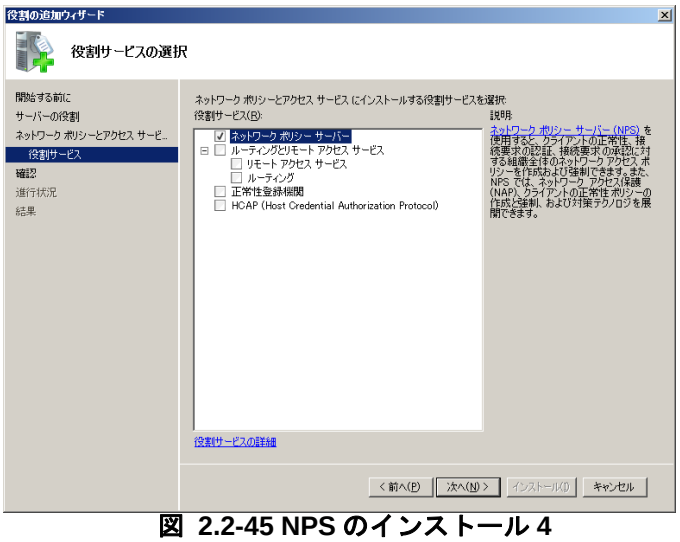


図 2.2-45 NPS のインストール 4

⑤ 内容を確認し、「インストール」をクリックする。

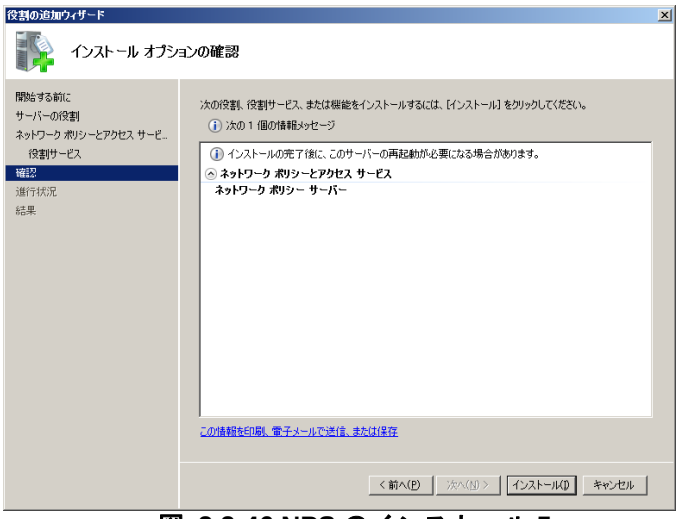


図 2.2-46 NPS のインストール 5

⑥ インストールの結果を確認し、「閉じる」をクリックする。

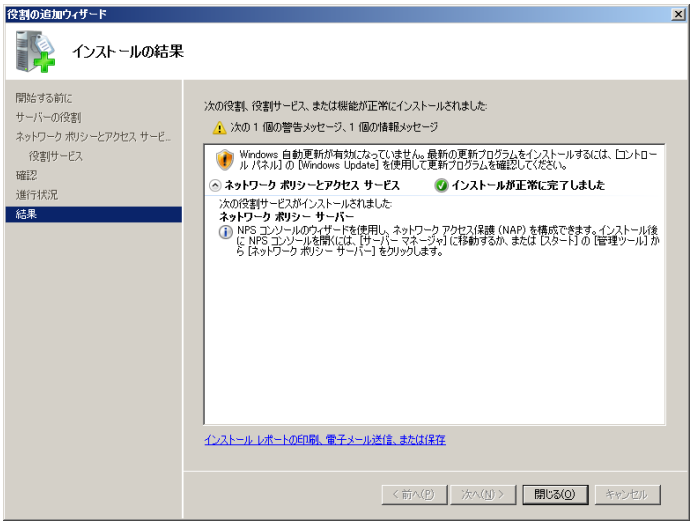


図 2.2-47 NPS のインストール 6

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。

① 「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。

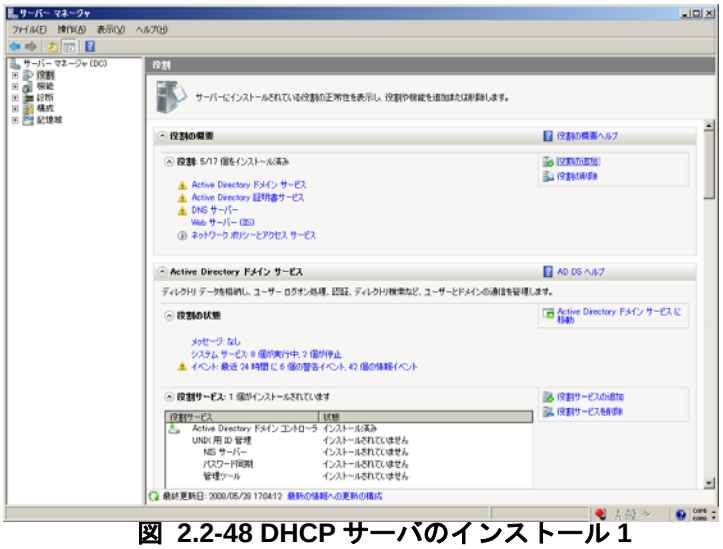


図 2.2-48 DHCP サーバのインストール 1

② 「DHCP サーバー」にチェックを入れて、「次へ」をクリックする。

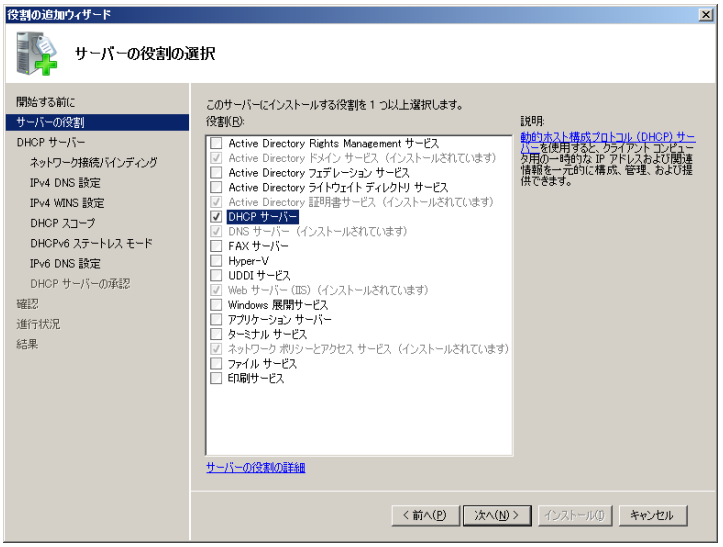


図 2.2-49 DHCP サーバのインストール 2

③ 内容を確認し、「次へ」をクリックする。

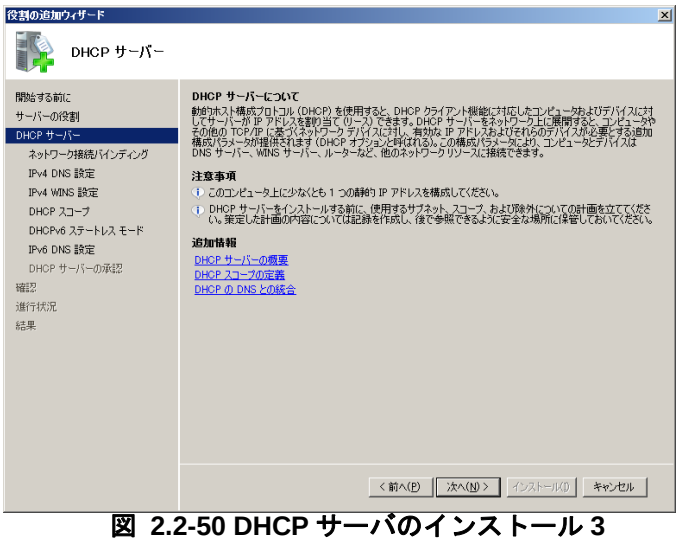


図 2.2-50 DHCP サーバのインストール 3

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。

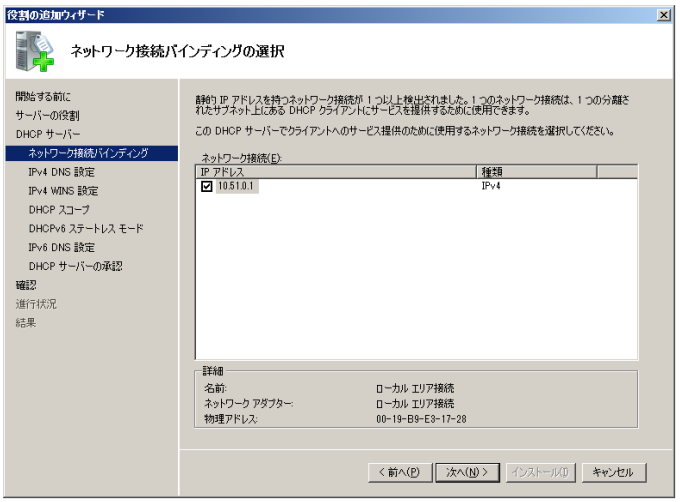


図 2.2-51 DHCP サーバのインストール 4

⑤ 「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。

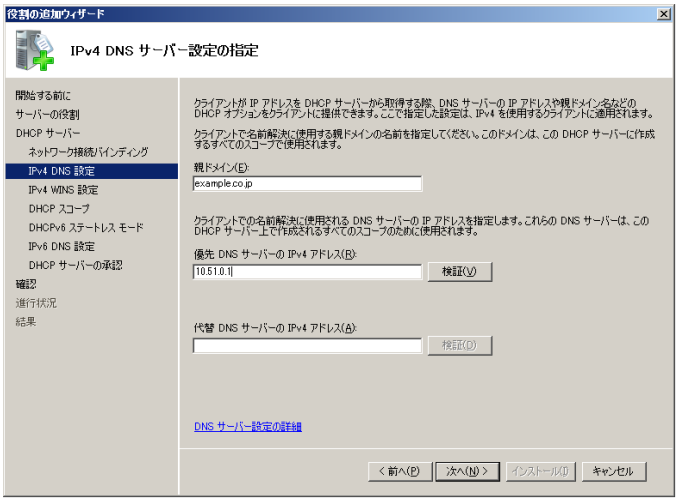


図 2.2-52 DHCP サーバのインストール 5

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。

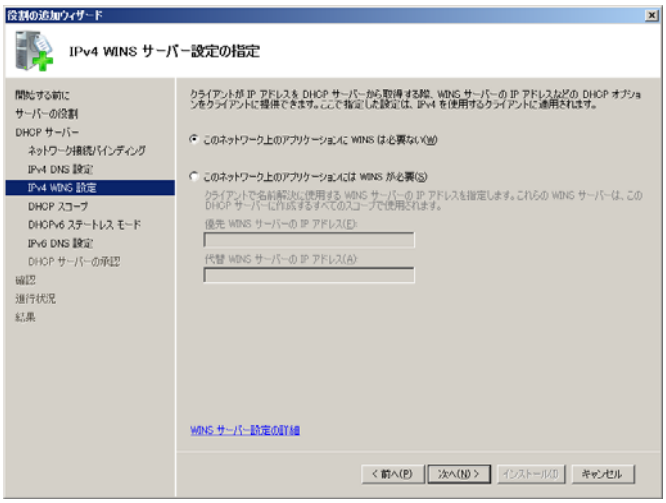


図 2.2-53 DHCP サーバのインストール 6

⑦ 「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。

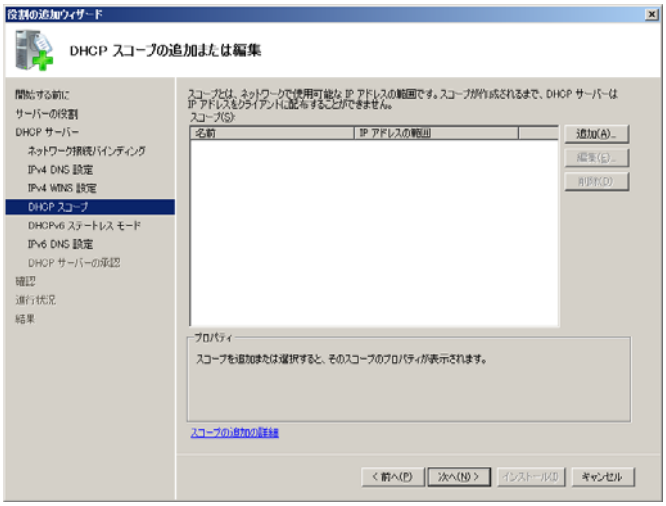


図 2.2-54 DHCP サーバのインストール 7

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）

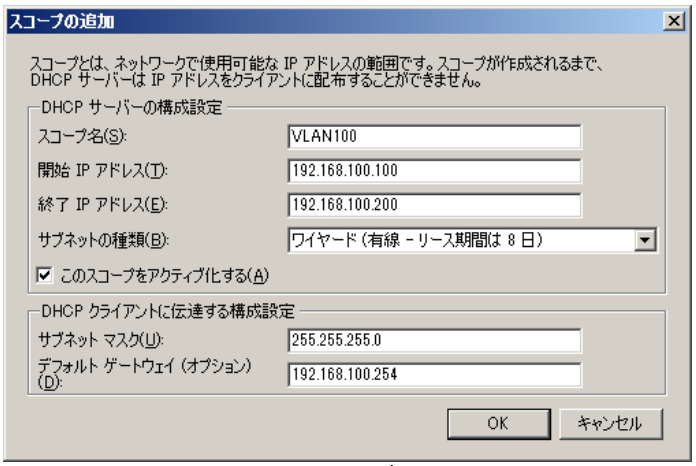


図 2.2-55 DHCP サーバのインストール 8

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。

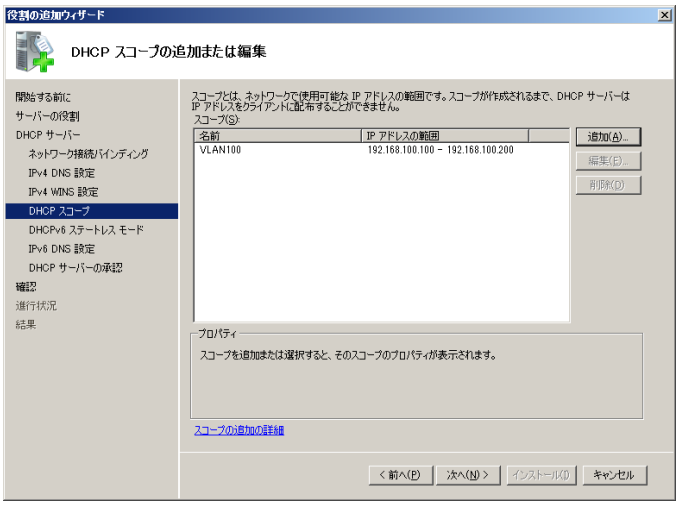


図 2.2-56 DHCP サーバのインストール 9

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。

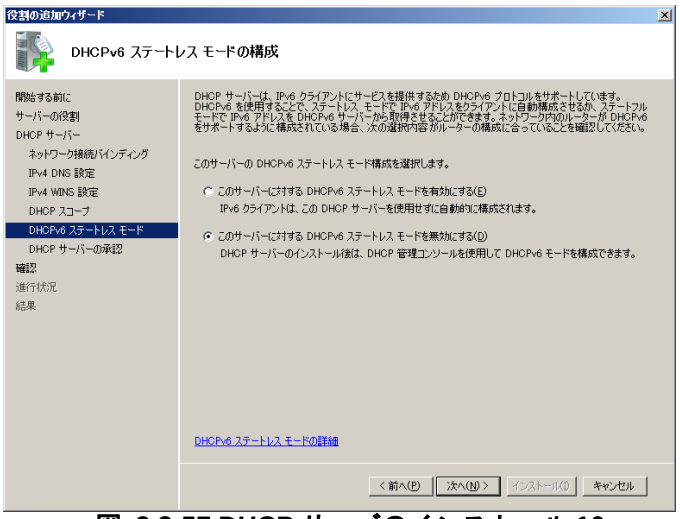


図 2.2-57 DHCP サーバのインストール 10

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

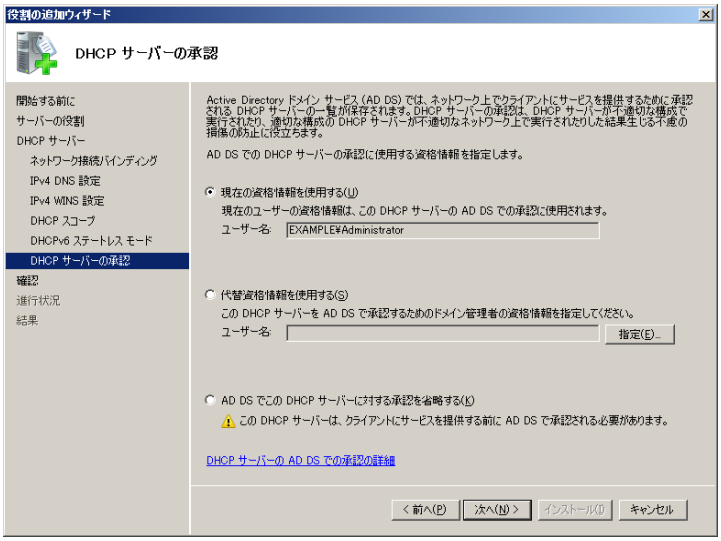


図 2.2-58 DHCP サーバのインストール 11

⑫ 設定した内容を確認し、「インストール」をクリックする。

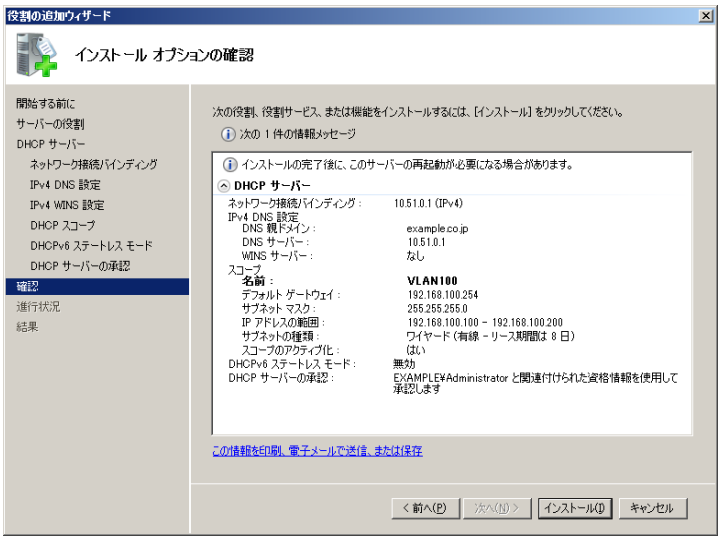


図 2.2-59 DHCP サーバのインストール 12

⑬ インストールの結果を確認して、「閉じる」をクリックする。

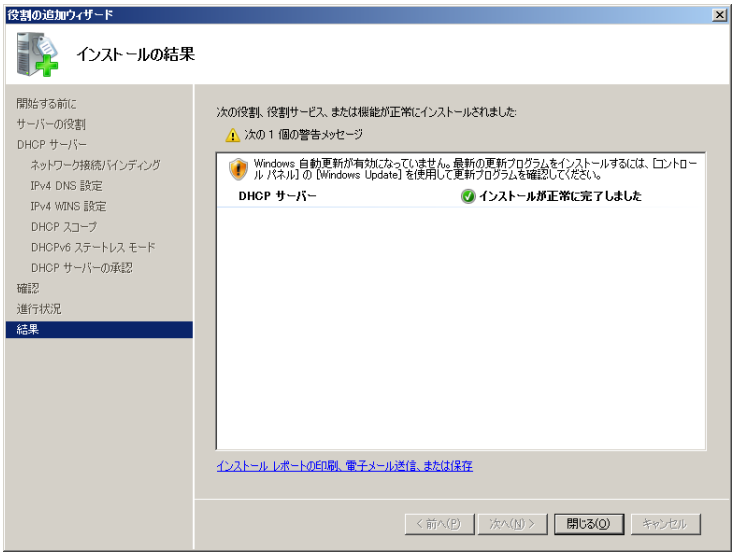


図 2.2-60 DHCP サーバのインストール 13

※ 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。

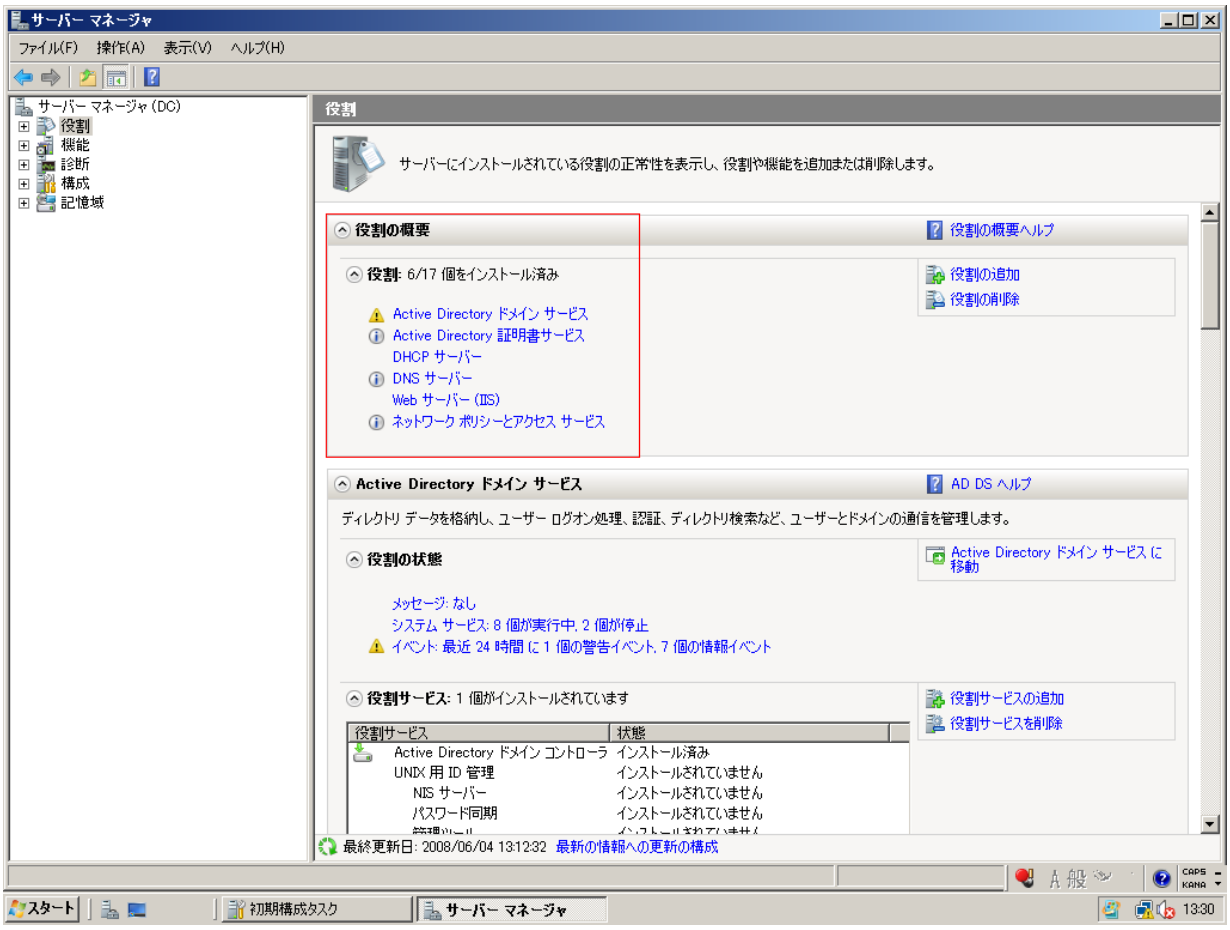


図 2.2-61 インストールの確認

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

① 「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。

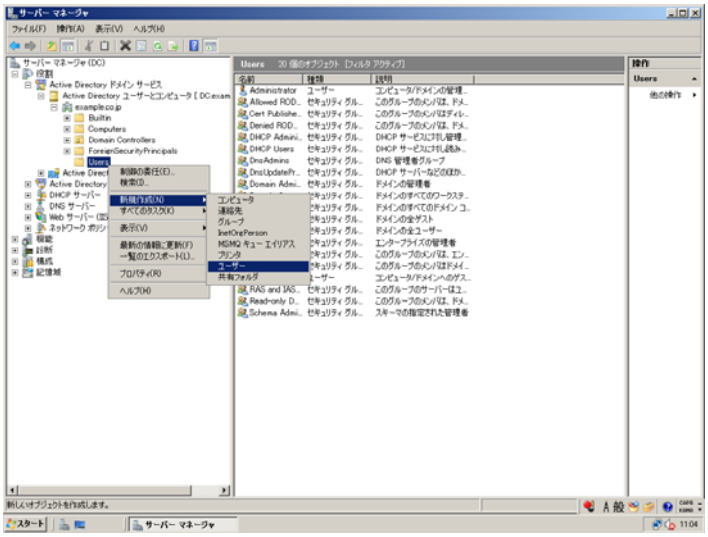


図 3.1-1 ユーザーグループの設定 1

② 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）

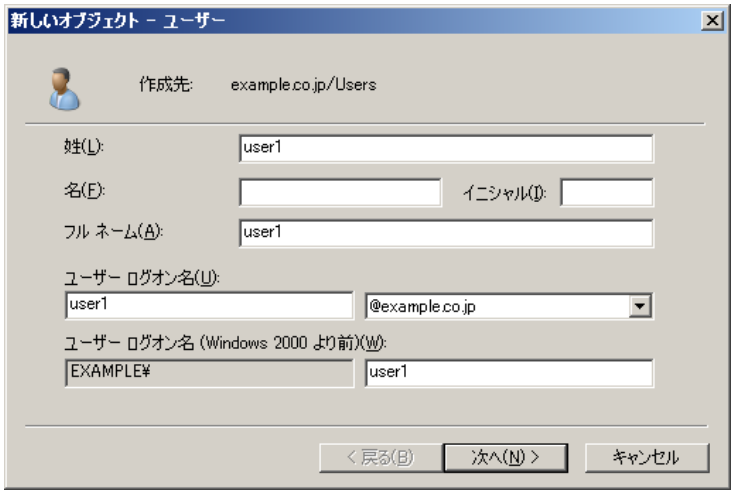


図 3.1-2 ユーザーグループの設定 2

③ パスワードを入力し、「次へ」をクリックする。

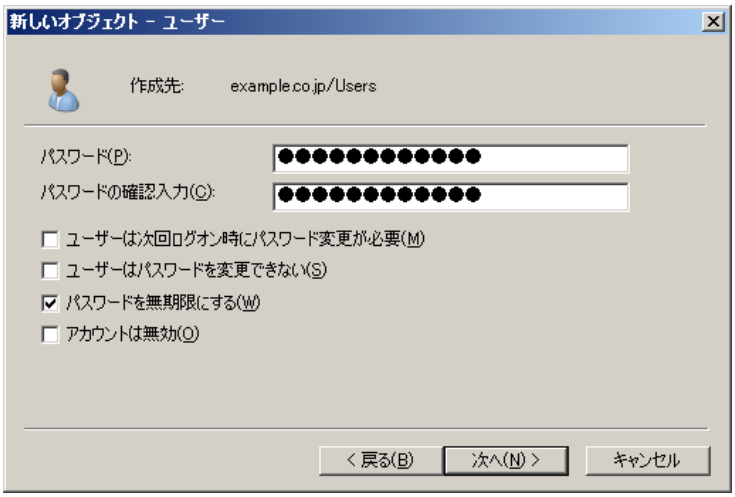


図 3.1-3 ユーザーグループの設定 3

④ 確認し、「完了」をクリックする。

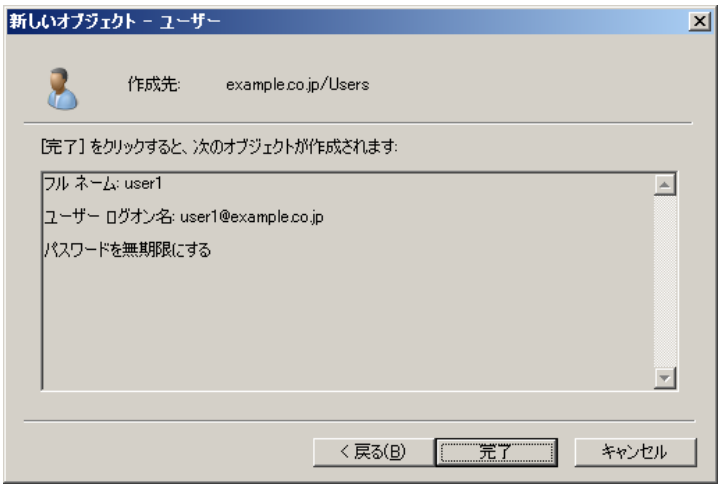


図 3.1-4 ユーザーグループの設定 4

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。

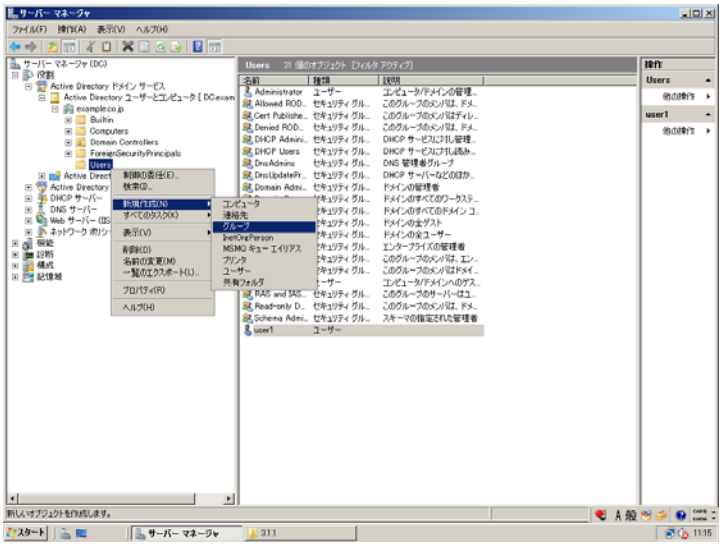


図 3.1-5 ユーザーグループの設定 5

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。

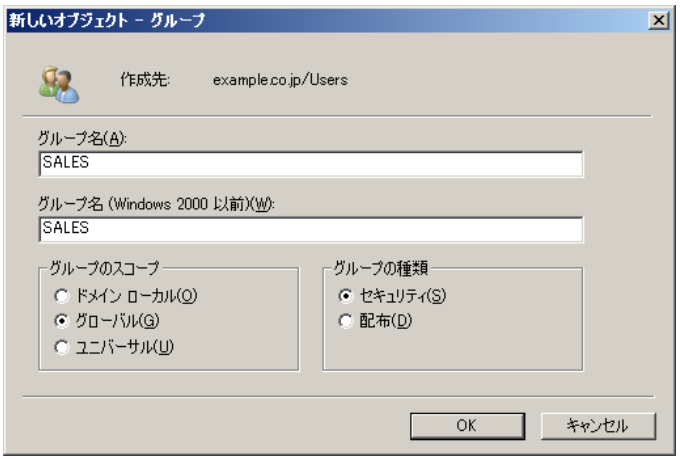


図 3.1-6 ユーザーグループの設定 6

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。

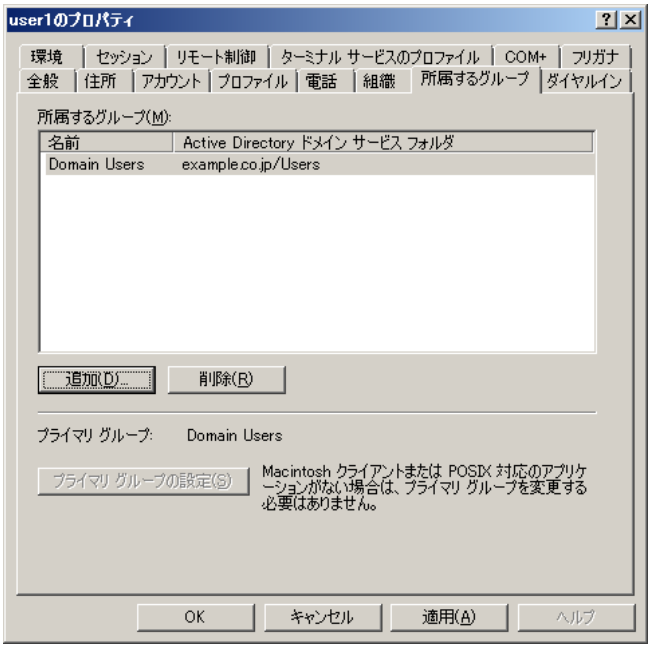


図 3.1-7 ユーザーグループの設定 7

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。

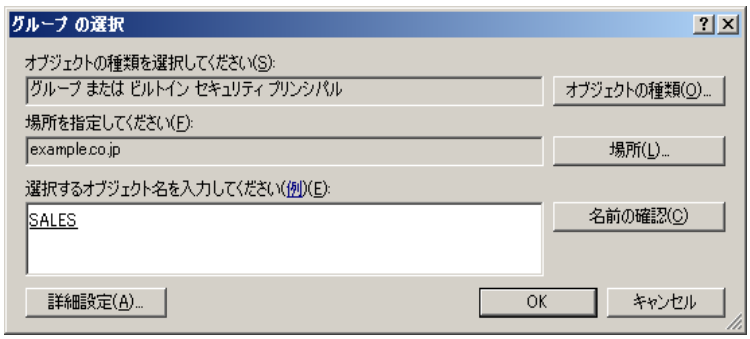


図 3.1-8 ユーザーグループの設定 8

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。

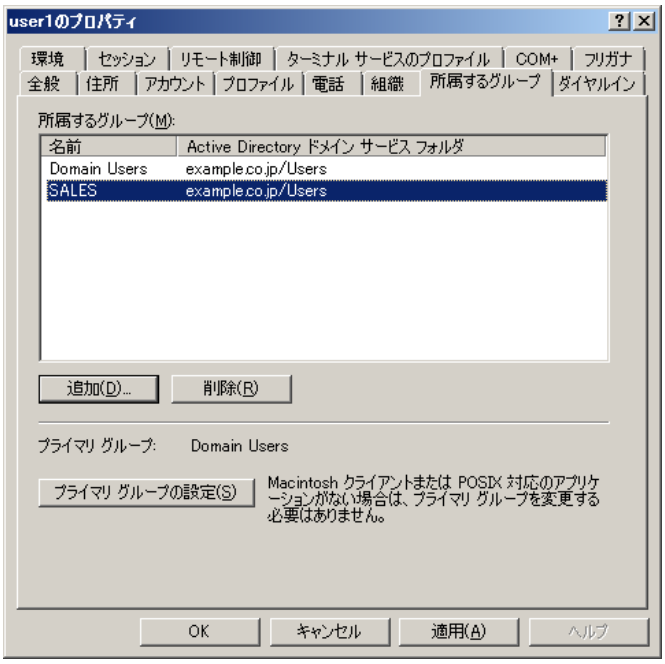


図 3.1-9 ユーザーグループの設定 9

⑩ 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。

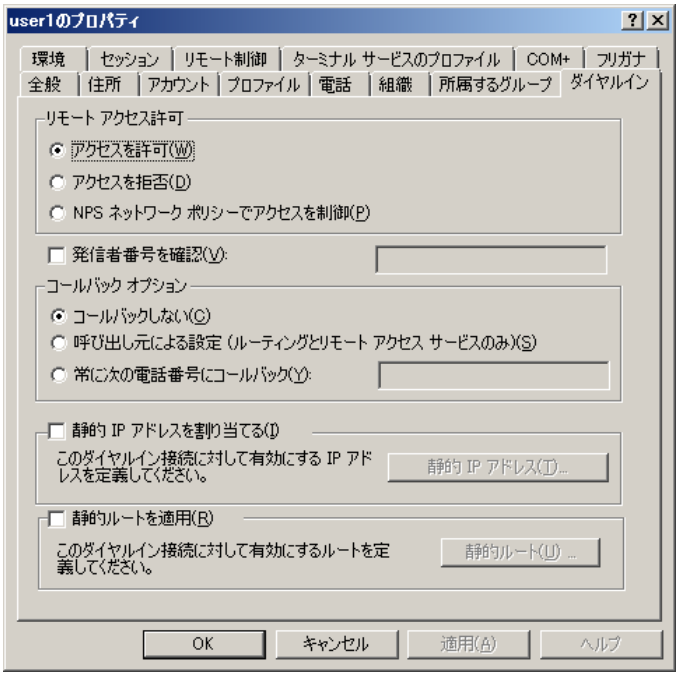


図 3.1-10 ユーザーグループの設定 10

3.1.2. NPS の設定

（1） サーバの登録

① 「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。

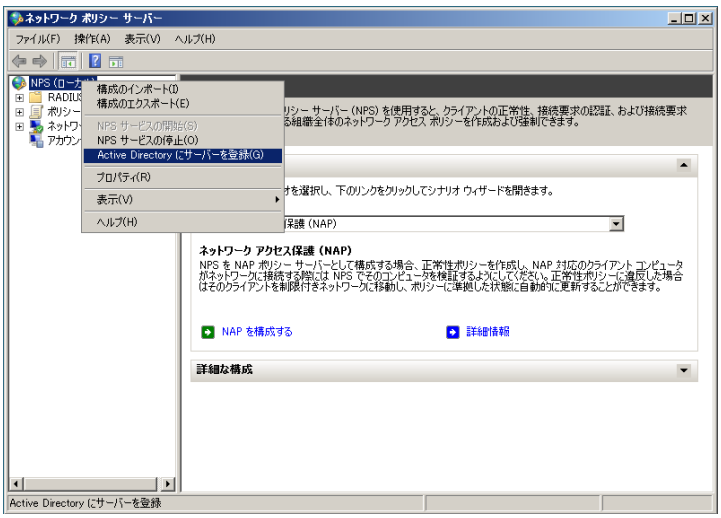


図 3.1-11 NPS の設定 1

② 下記メッセージが表示される。「OK」をクリックする。

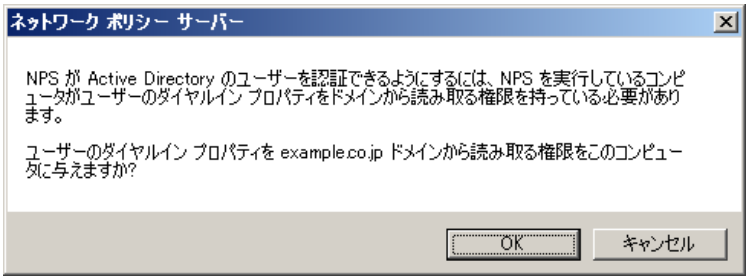


図 3.1-12 NPS の設定 2

③ 下記メッセージが表示される。「OK」をクリックする。

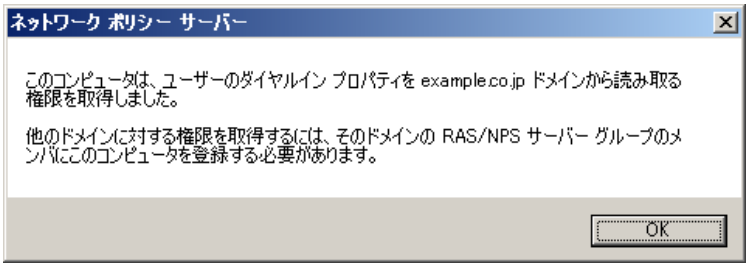


図 3.1-13 NPS の設定 3

（２） RADIUS クライアントの作成

① 「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。

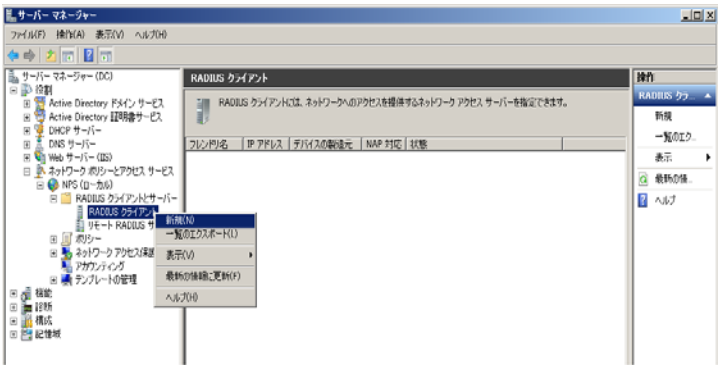


図 3.1-14 RADIUS クライアントの設定 1

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」）

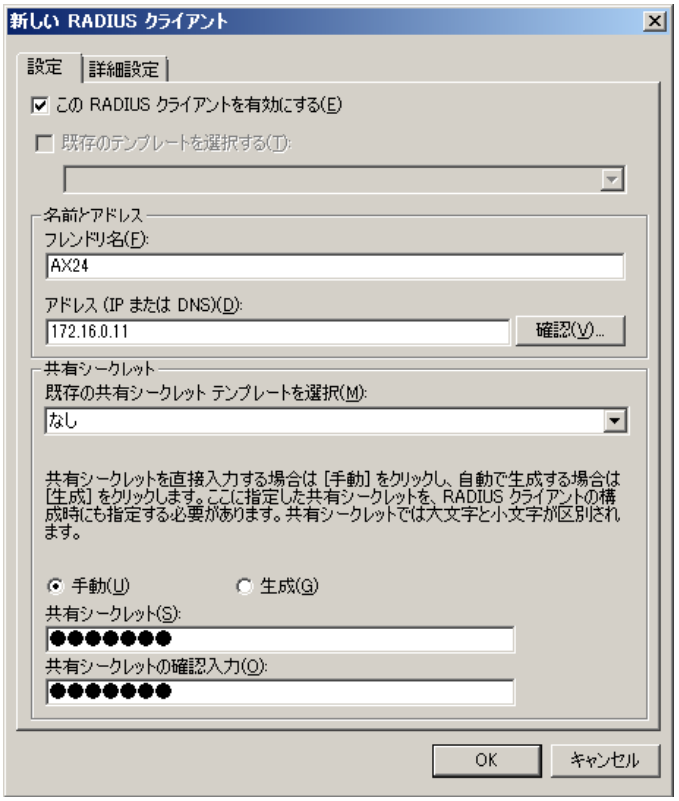


図 3.1-15 RADIUS クライアントの設定 2

（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） 条件の設定
（b） 認証方法の構成
（c） 設定の構成
（d） ネットワークポリシーの確認

（a） 条件の設定

① 「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。

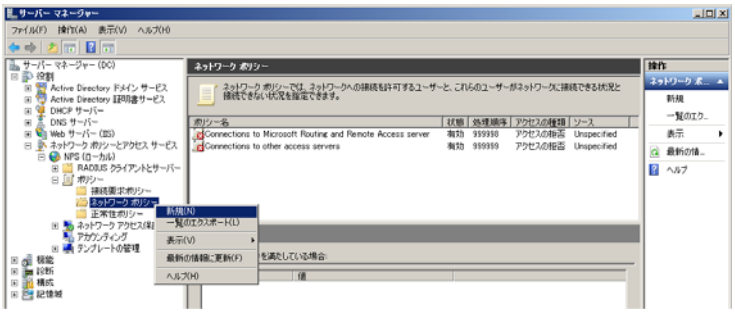


図 3.1-16 条件の設定 1

② 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。

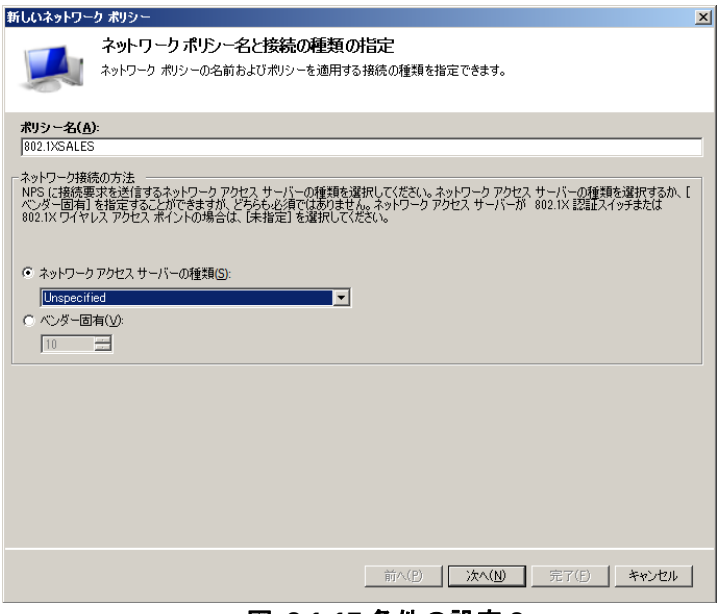


図 3.1-17 条件の設定 2

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。

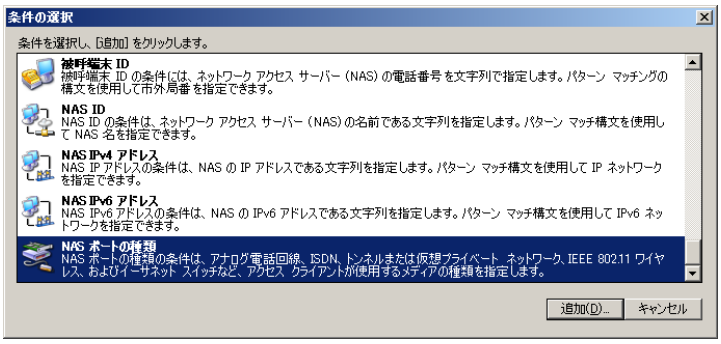


図 3.1-18 条件の設定 3

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「Ethernet」をチェックして、「OK」をクリックする。

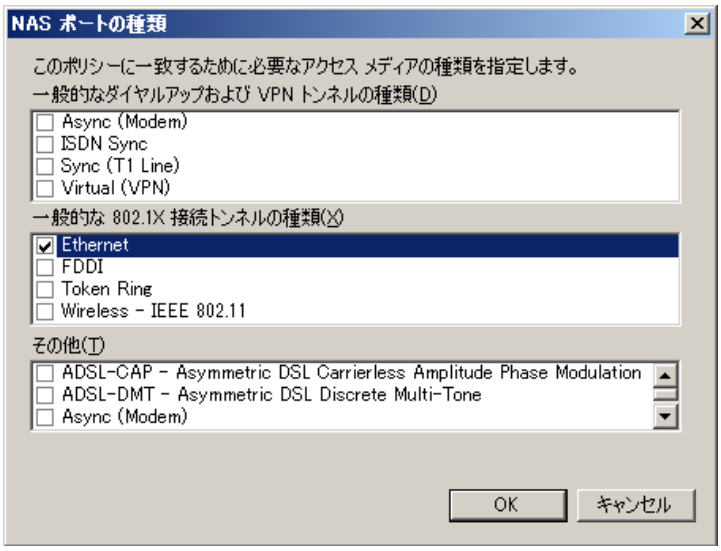


図 3.1-19 条件の設定 4

⑤ 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。

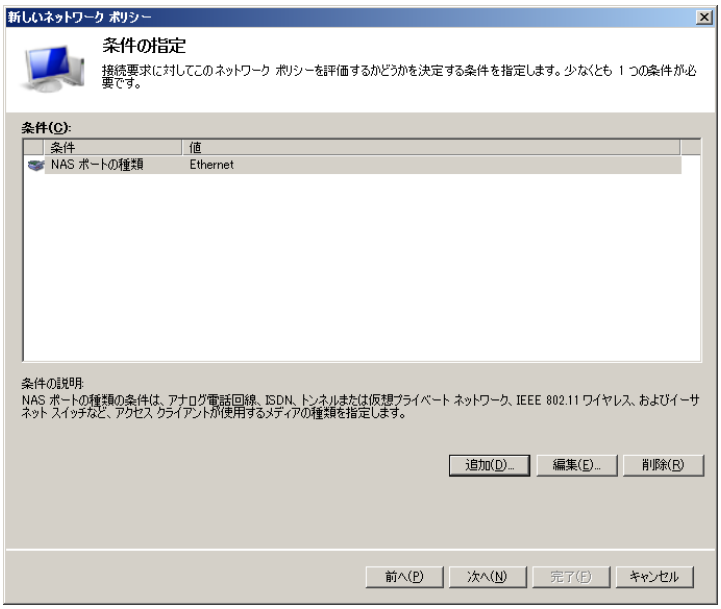


図 3.1-20 条件の設定 5

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。

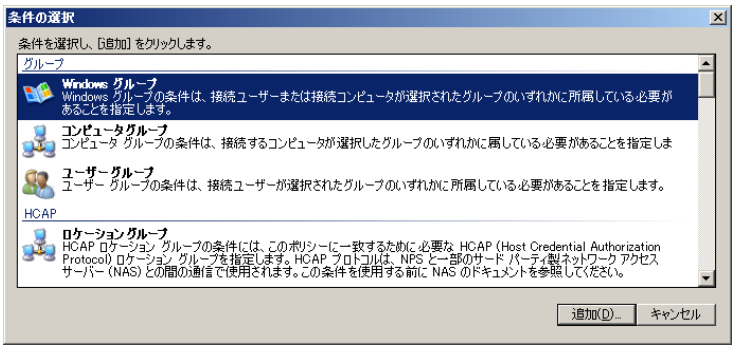


図 3.1-21 条件の設定 6

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。

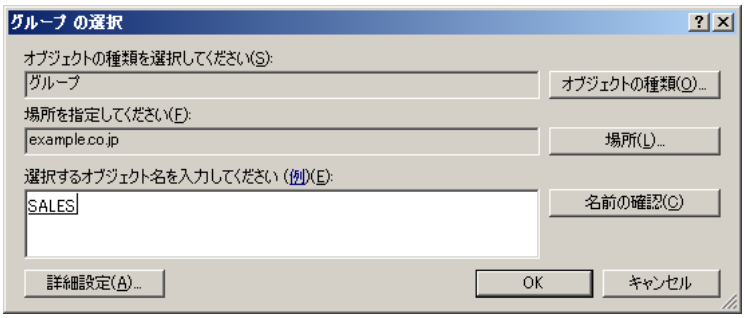


図 3.1-22 条件の設定 7

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。

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。

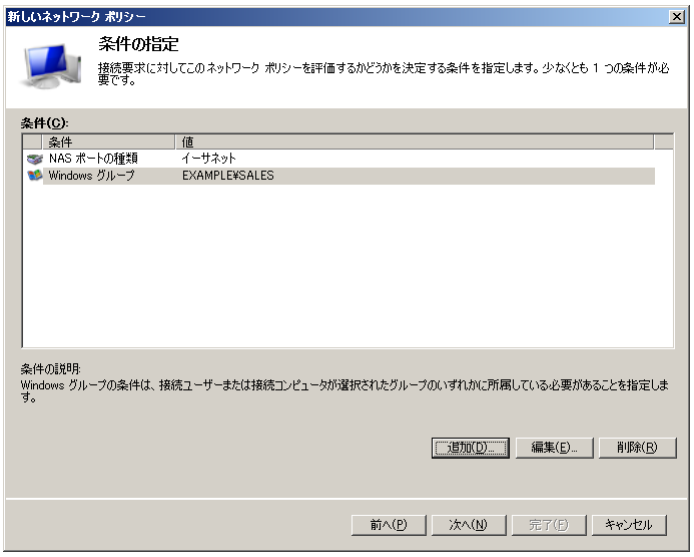


図 3.1-24 条件の設定 9

⑩ 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。

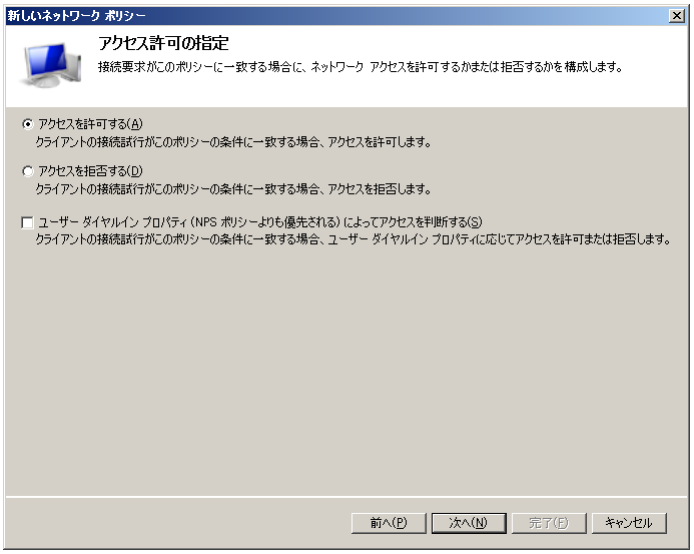


図 3.1-25 条件の設定 10

（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。

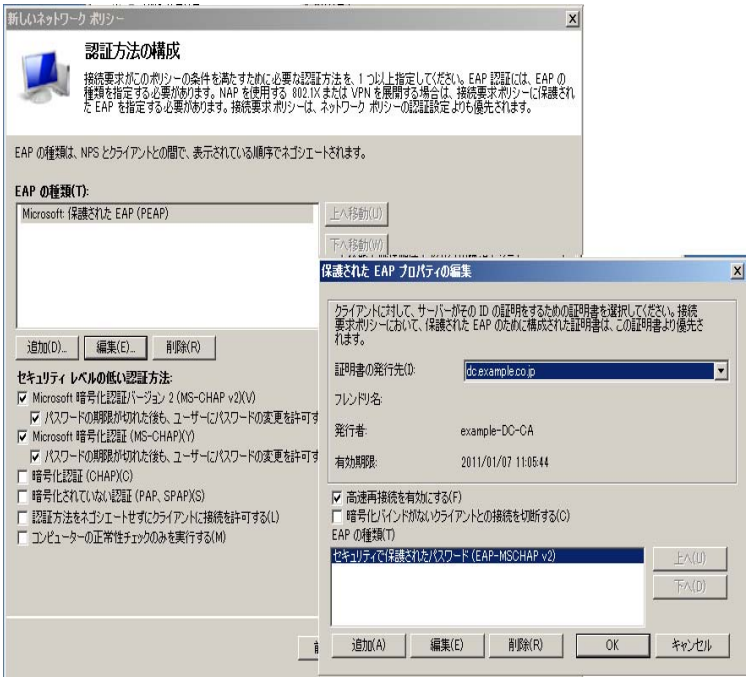


図 3.1-26 認証方法の構成 1

② 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。

図 3.1-27 認証方法の構成 2

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。）

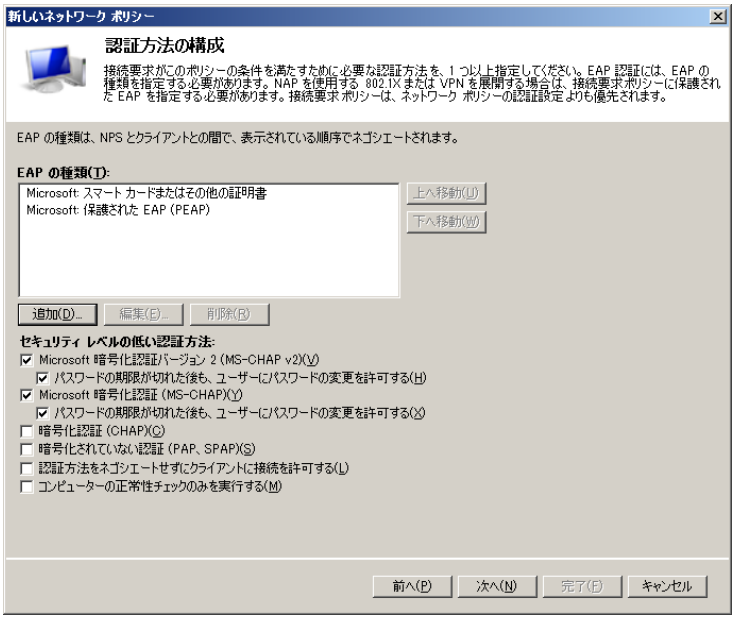


図 3.1-28 認証方法の構成 3

④ 制約の構成

必要な設定がある場合は設定し、「次へ」をクリックする。

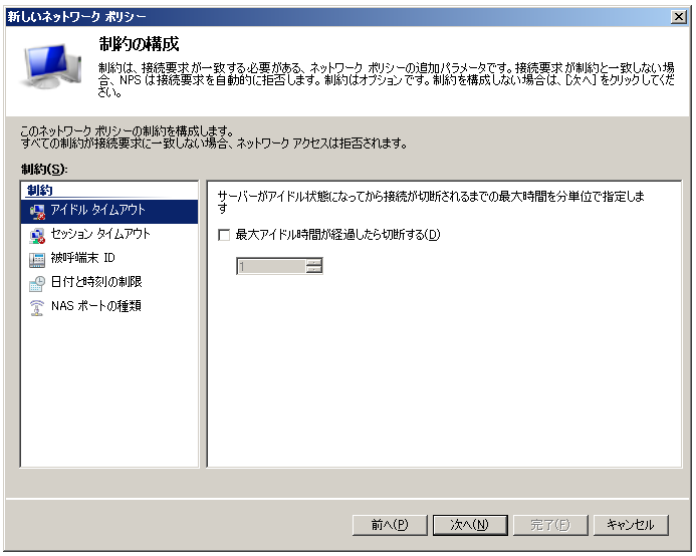


図 3.1-29 認証方法の構成 4

（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。

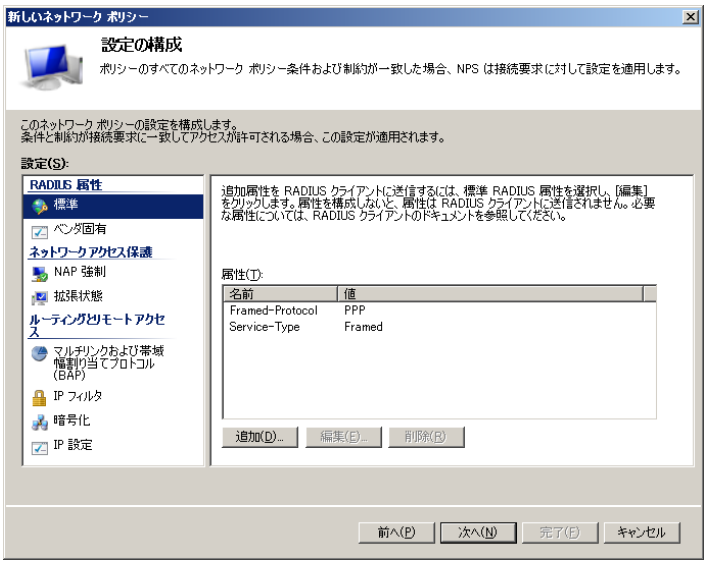


図 3.1-30 設定の構成 1

② 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。

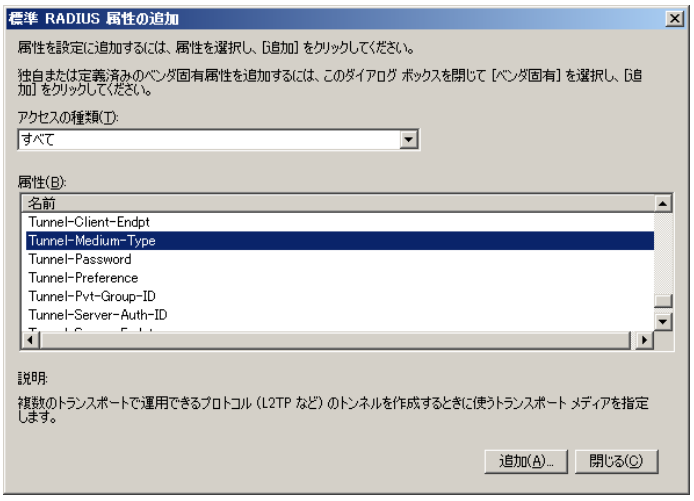


図 3.1-31 設定の構成 2

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。

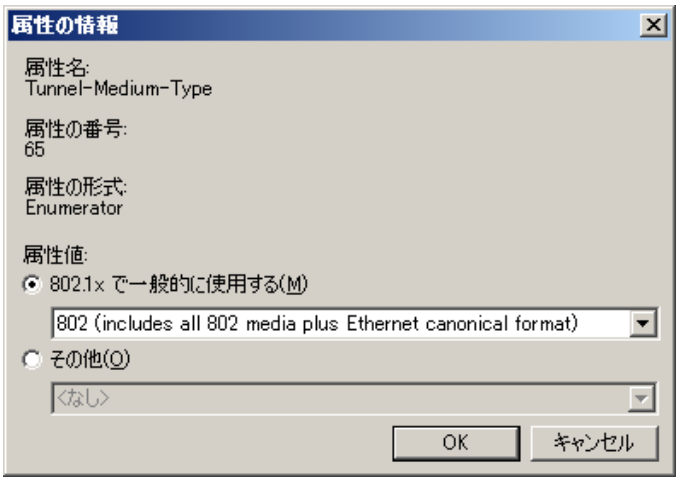


図 3.1-32 設定の構成 3

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。

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。

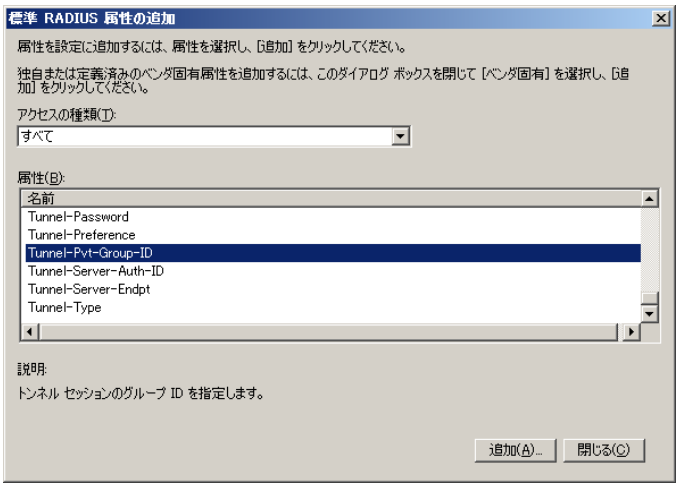


図 3.1-34 設定の構成 5

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。

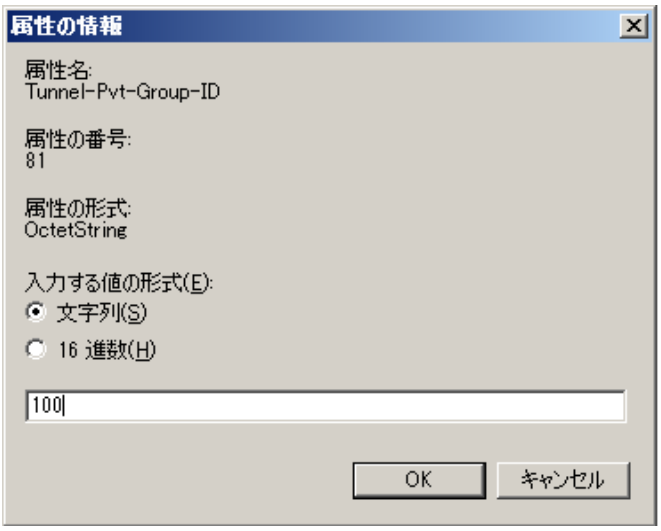


図 3.1-35 設定の構成 6

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。

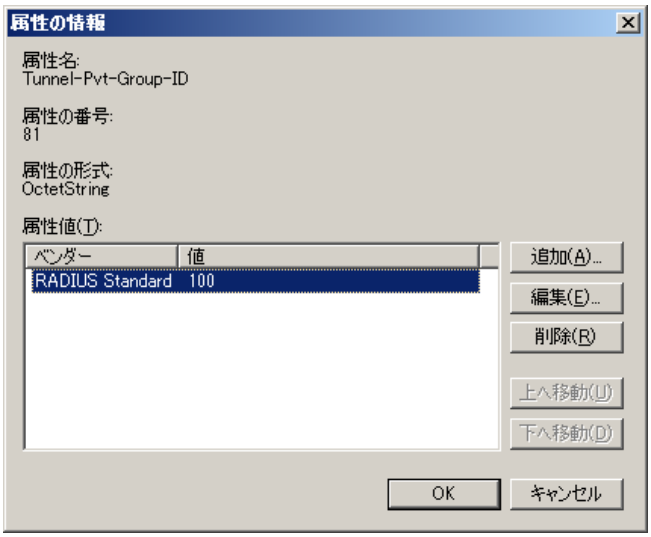


図 3.1-36 設定の構成 7

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。

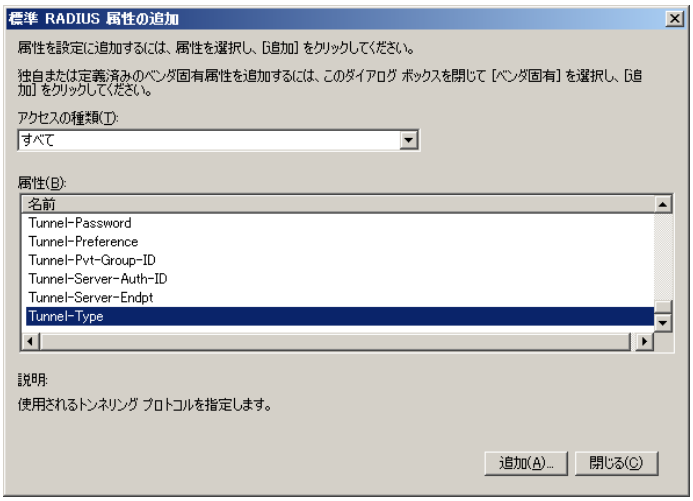


図 3.1-37 設定の構成 8

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。

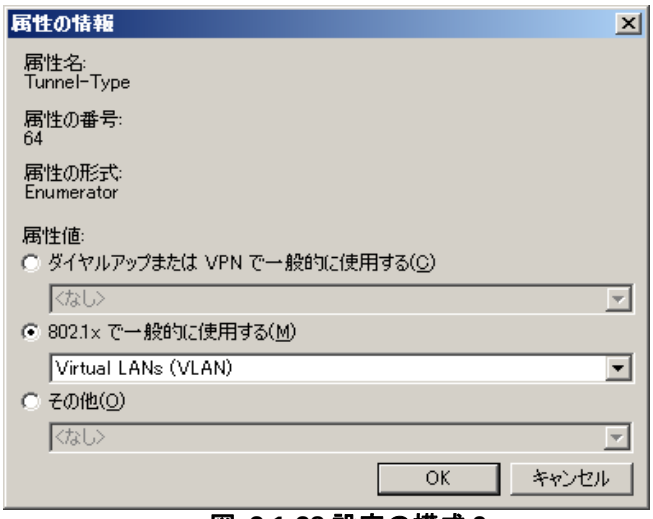


図 3.1-38 設定の構成 9

⑩ 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。

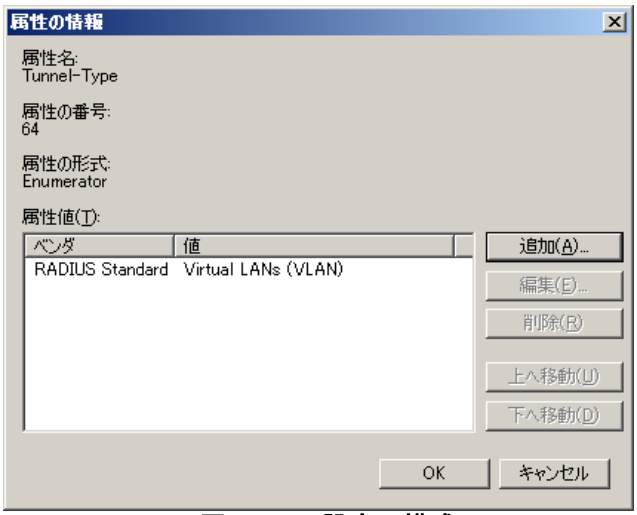


図 3.1-39 設定の構成 10

⑪ 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。

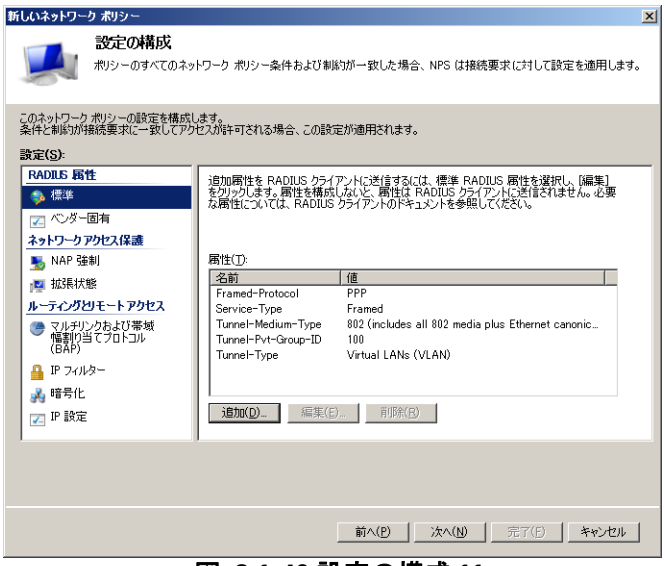


図 3.1-40 設定の構成 11

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。

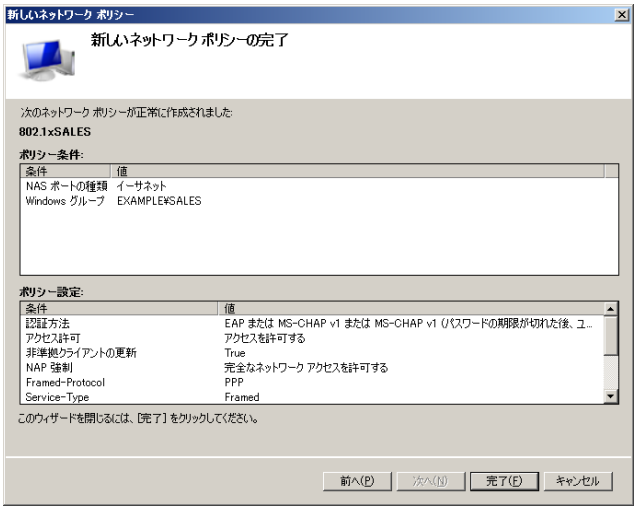


図 3.1-41 設定の構成 12

（d） ネットワークポリシーの確認

① 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。

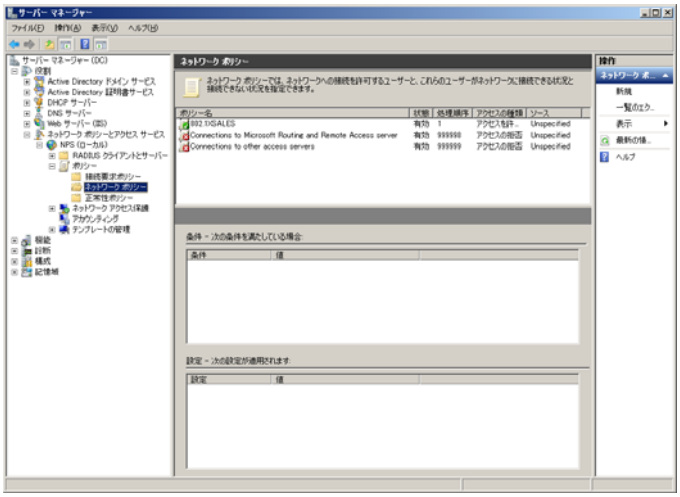


図 3.1-42 ネットワークポリシーの確認

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。

① 「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。

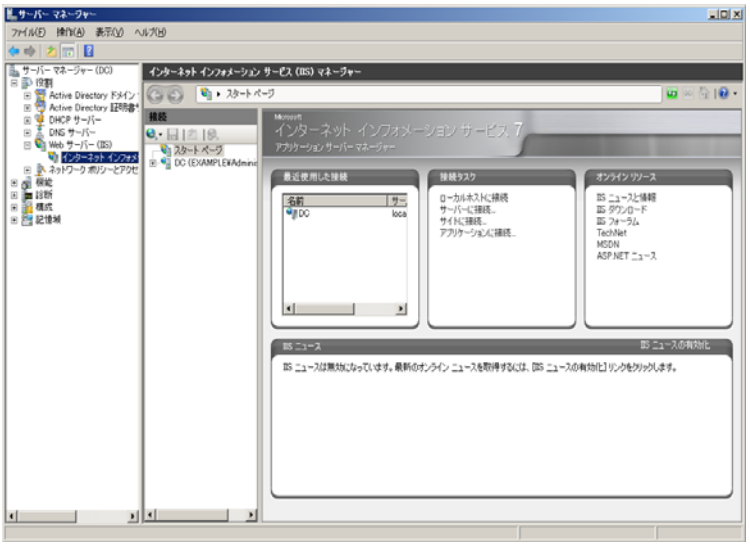


図 3.1-43 Web サーバ（IIS）の設定 1

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。

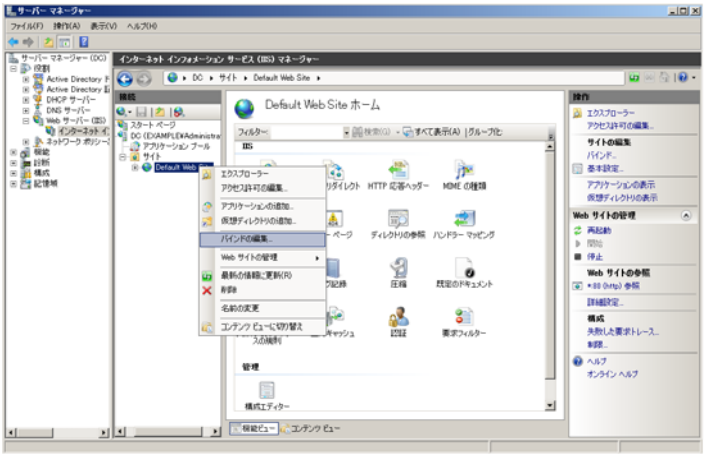


図 3.1-44 Web サーバ（IIS）の設定 2

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

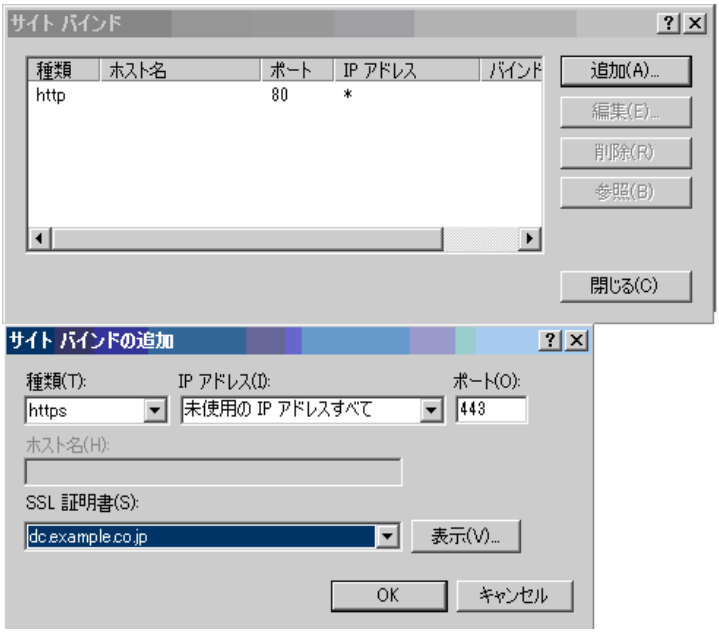


図 3.1-45 Web サーバ（IIS）の設定 3

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。

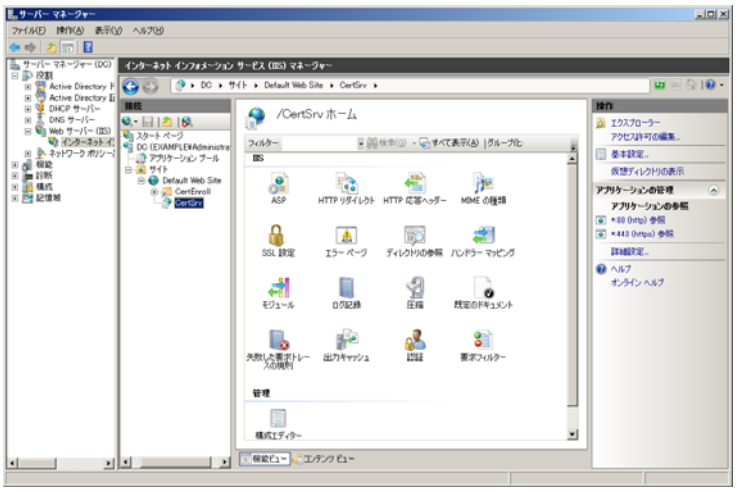


図 3.1-46 Web サーバ（IIS）の設定 4

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。

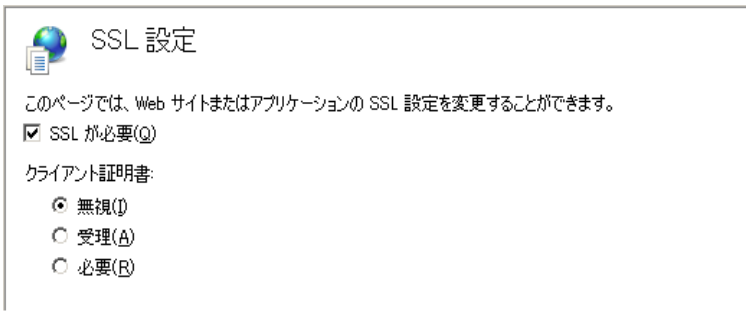


図 3.1-47 Web サーバ（IIS）の設定 5

※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

① 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。

② 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。

③ 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

① 「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

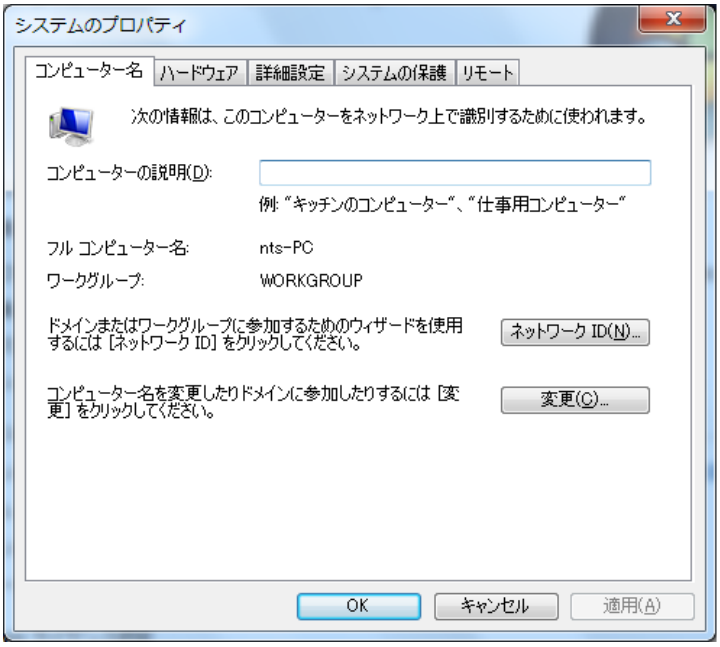


図 3.2-1 ドメイン参加 1

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。

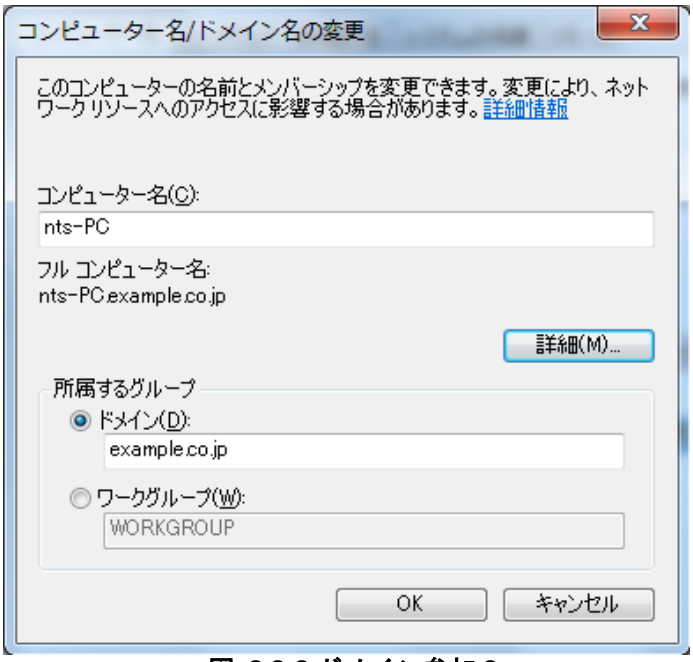


図 3.2-2 ドメイン参加 2

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。

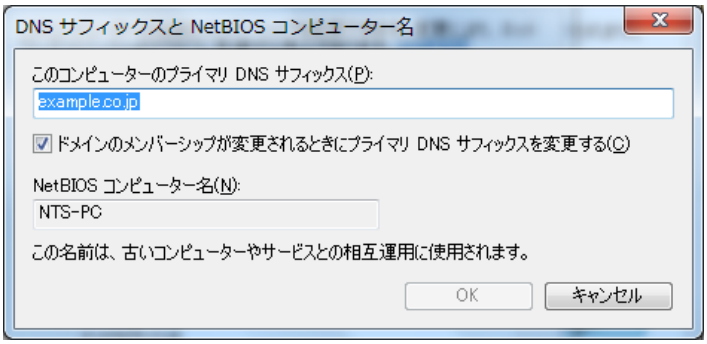


図 3.2-3 ドメイン参加 3

④ まもなく下記の画面が表示される。
3.1.1 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。

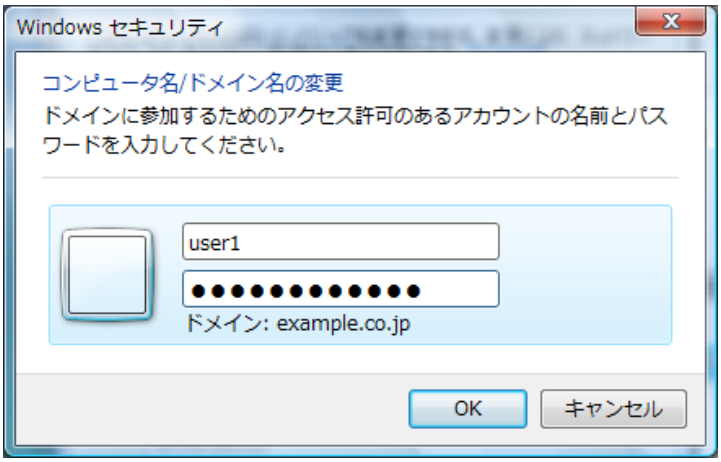


図 3.2-4 ドメイン参加 4

⑤ 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。

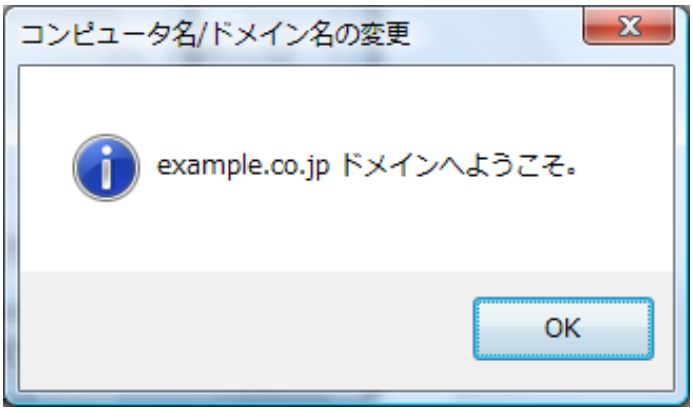


図 3.2-5 ドメイン参加 5

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」）、3.1.1 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。

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。

① 「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。

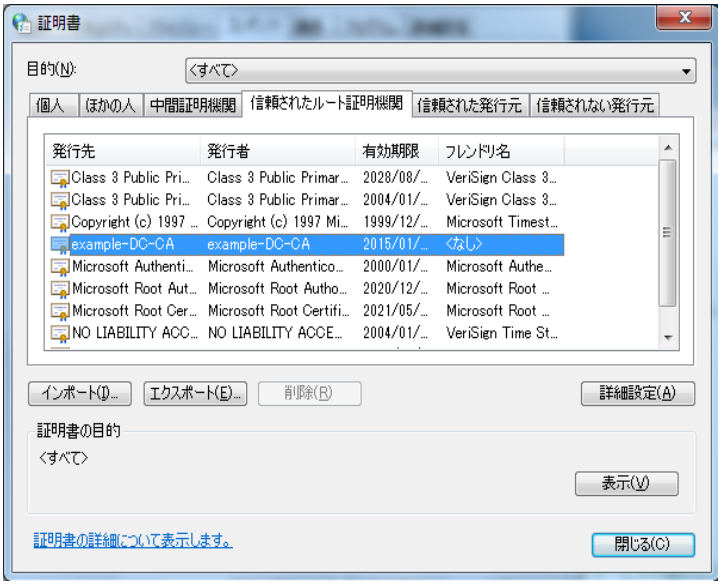


図 3.2-7 CA 証明書の確認

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。

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。

Windows Vista

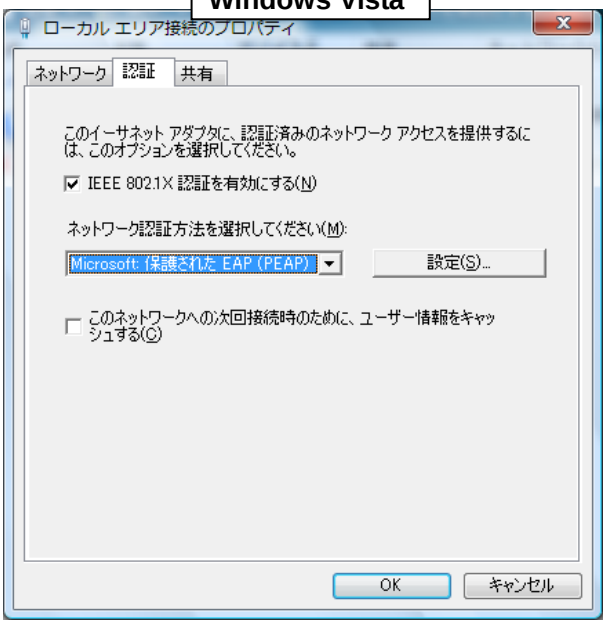


図 3.2-8 PEAP の設定 1 (Windows Vista)

Windows 7

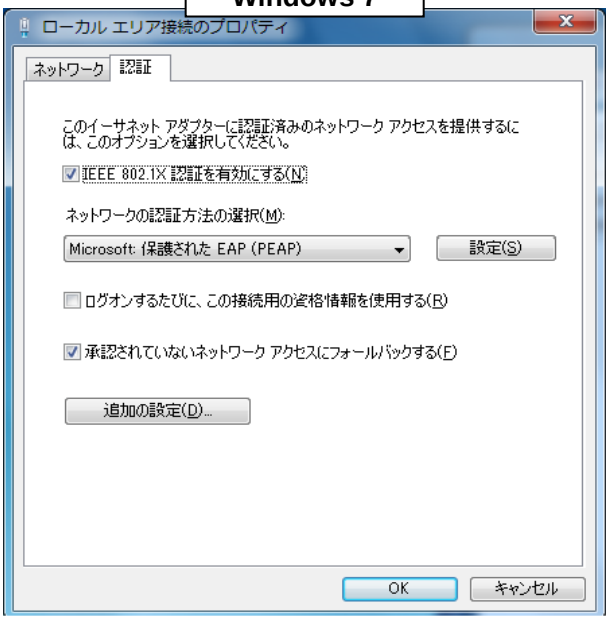


図 3.2-9 PEAP の設定 1 (Windows 7)

② 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。

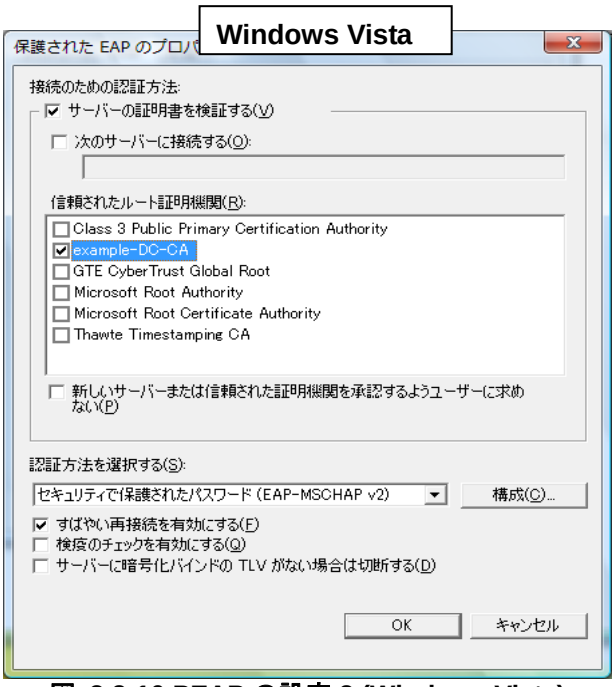


図 3.2-10 PEAP の設定 2 (Windows Vista)

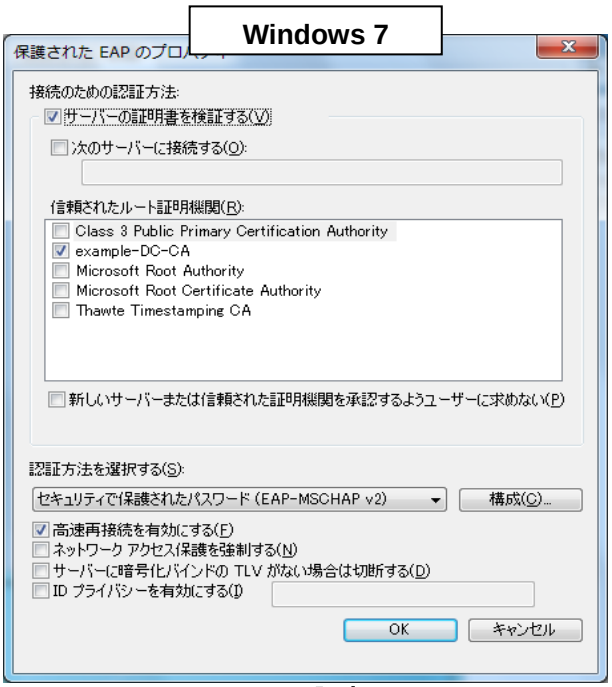


図 3.2-11 PEAP の設定 2 (Windows 7)

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。

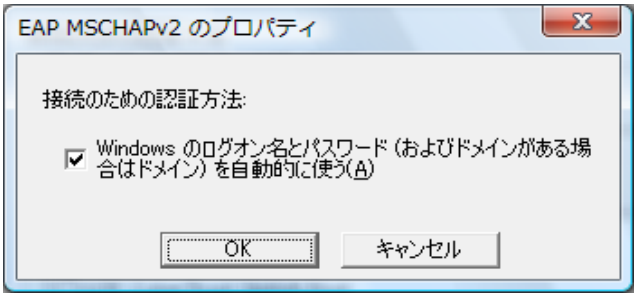


図 3.2-12 PEAP の設定 3

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

① 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、3.1.1 で作成したユーザー名およびパスワードを入力しログオンする。

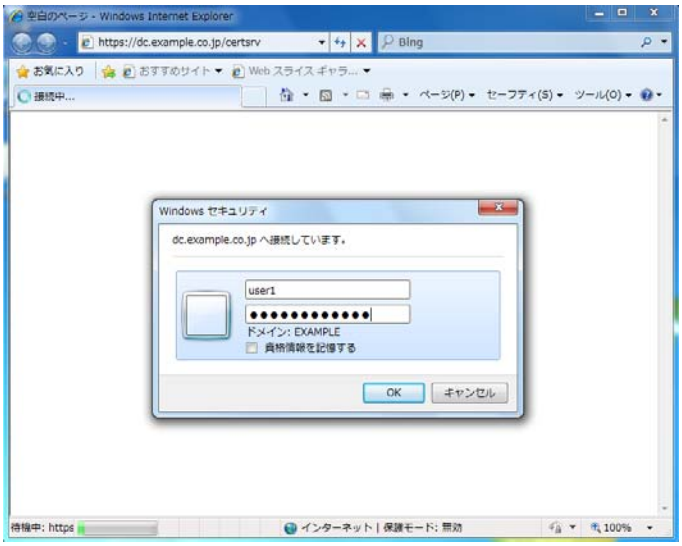


図 3.2-13 TLS の設定 1

② 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。

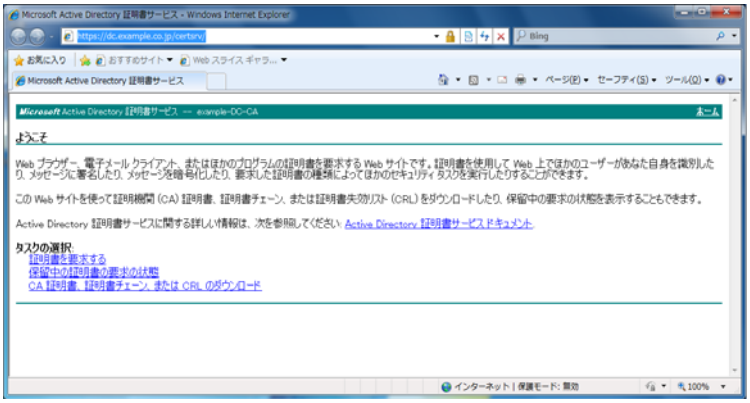


図 3.2-14 TLS の設定 2

③ 「証明書の要求」で、「ユーザー証明書」をクリックする。

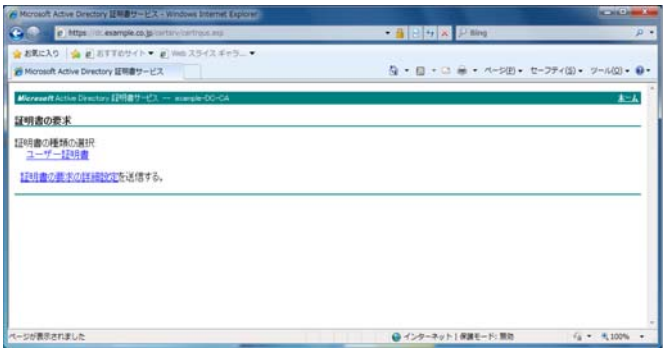


図 3.2-15 TLS の設定 3

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。

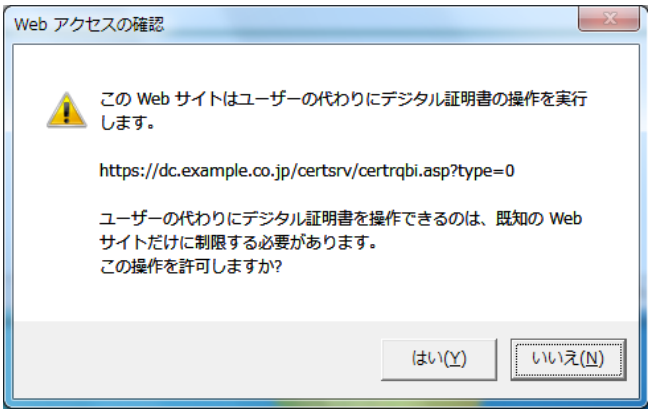


図 3.2-16 TLS の設定 4

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。

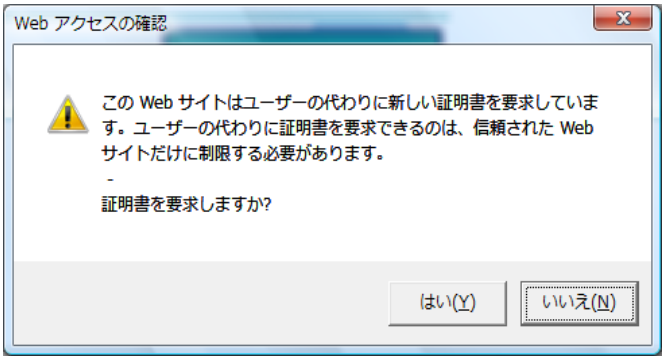


図 3.2-18 TLS の設定 6

⑦ 「この証明書のインストール」をクリックする。

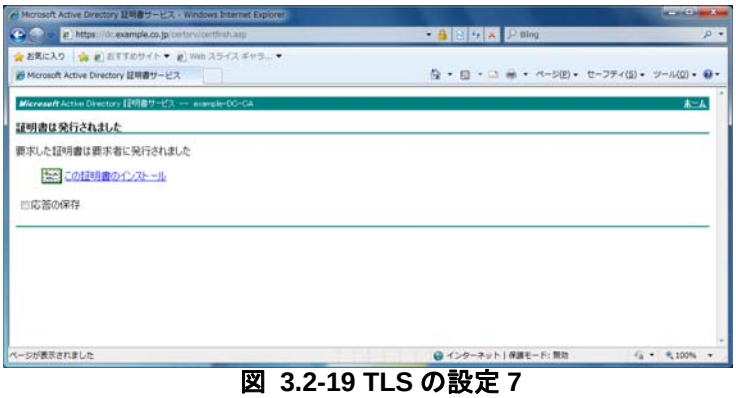


図 3.2-19 TLS の設定 7

⑧ ユーザー証明書のインストール完了。

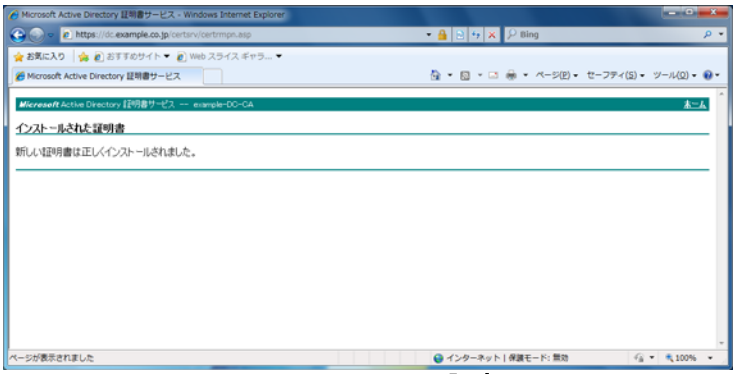


図 3.2-20 TLS の設定 8

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。

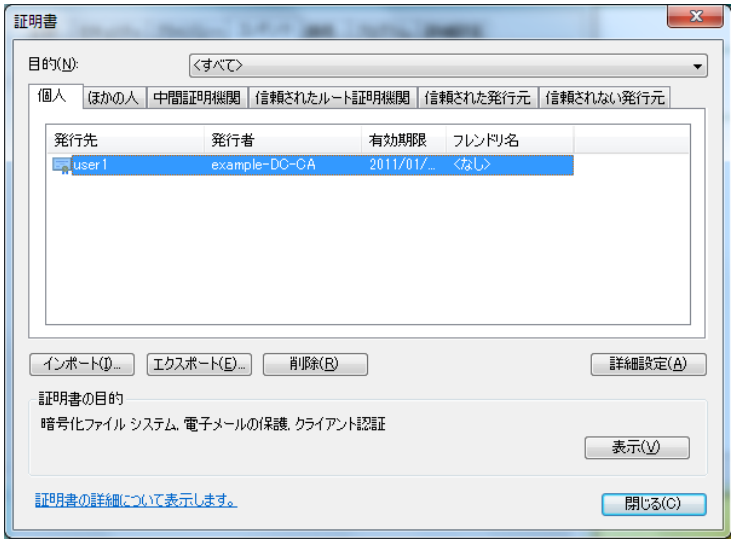


図 3.2-21 TLS の設定 9

（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。

⑩ 「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。

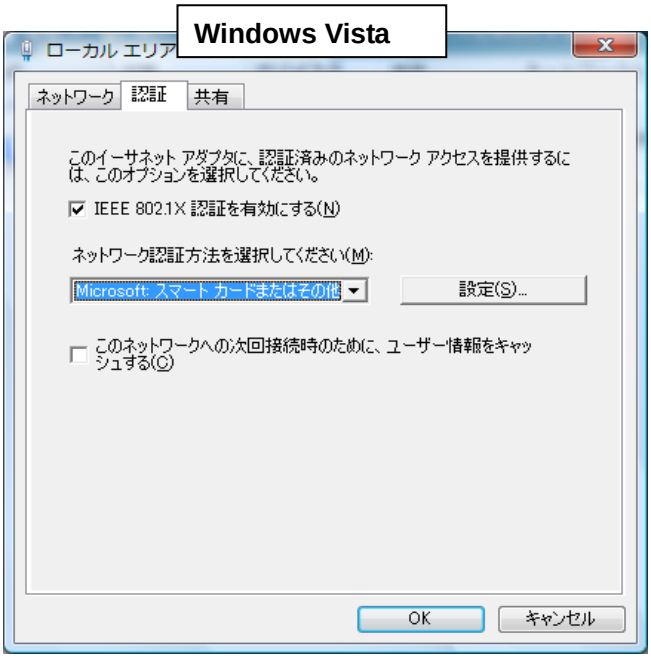


図 3.2-22 TLS の設定 10 (Windows Vista)

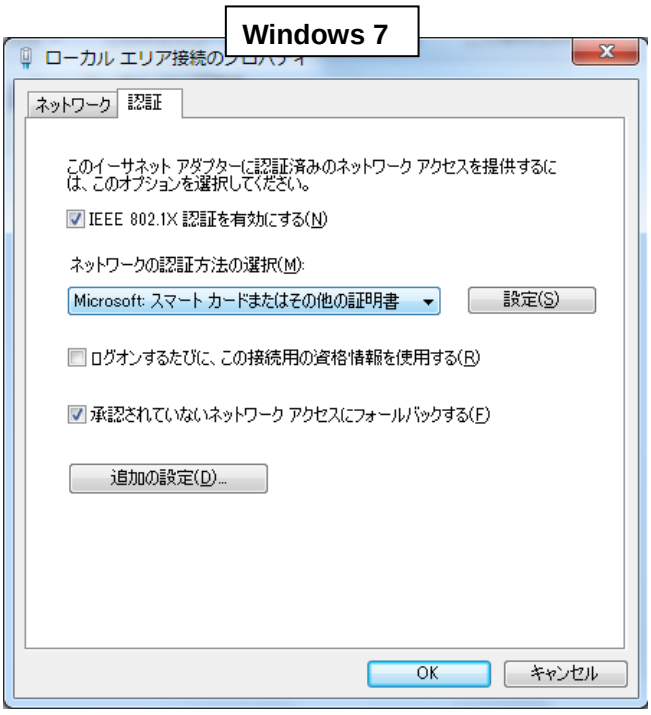


図 3.2-23 TLS の設定 10 (Windows 7)

⑪ 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。

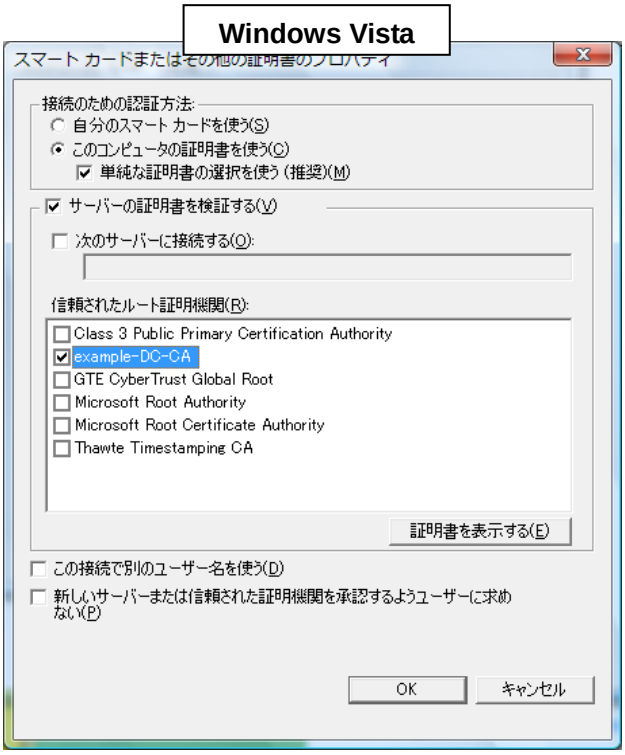


図 3.2-24 TLS の設定 11 (Windows Vista)

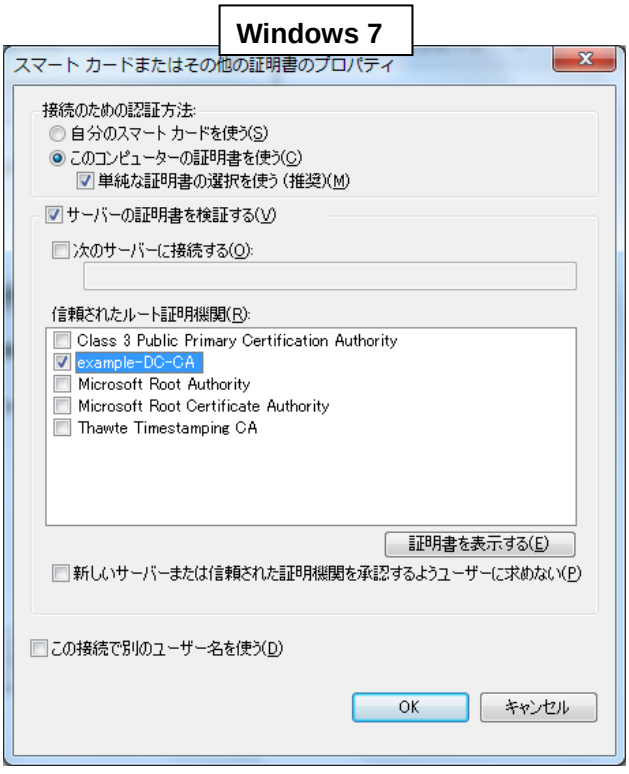


図 3.2-25 TLS の設定 11 (Windows 7)

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。

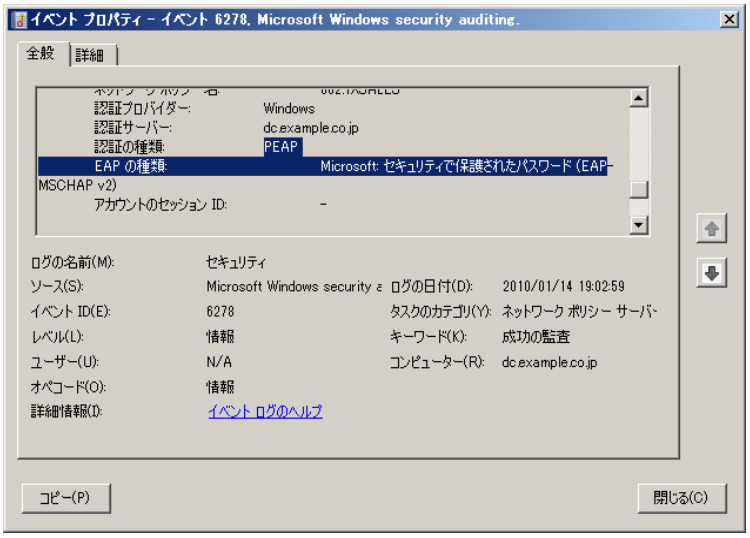


図 3.3-1 サーバログ（PEAP）

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ー情報を確認することができます。

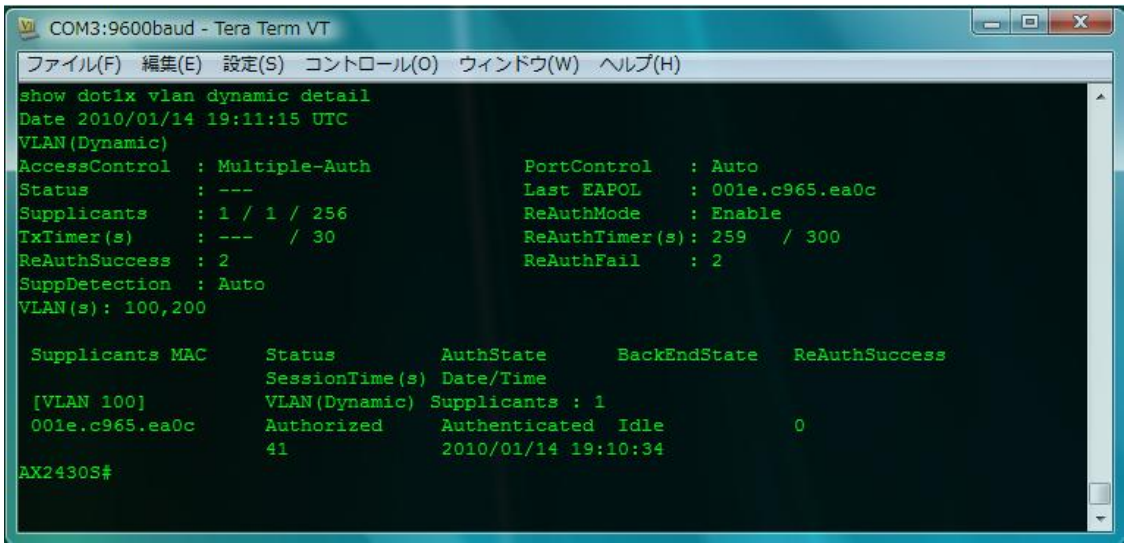


図 3.3-3 show dot1x vlan dynamic detail

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。

① 「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。

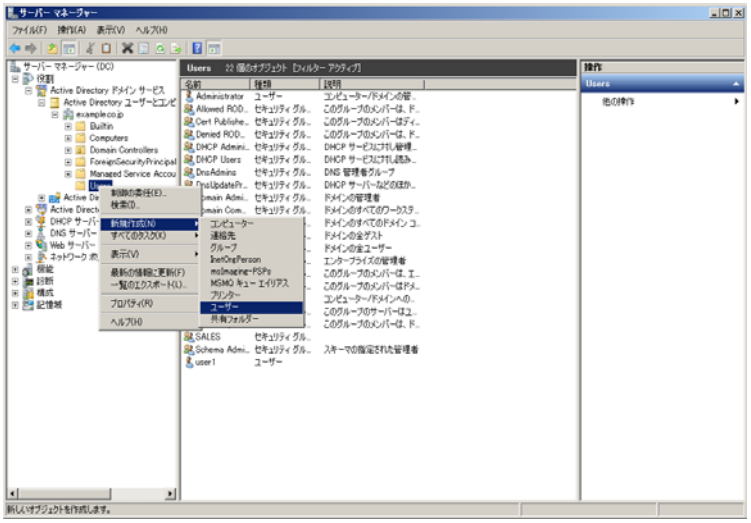


図 4.1-1 Web 認証用ユーザーの作成 1

② 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）

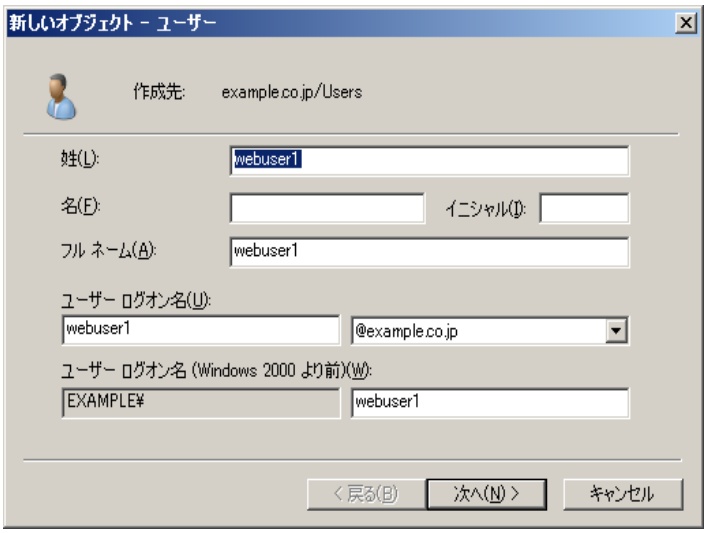


図 4.1-2 Web 認証用ユーザーの作成 2

③ パスワードを入力して「完了」をクリックする。

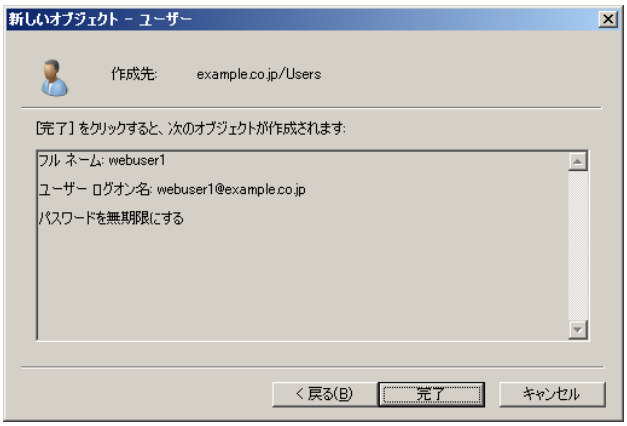


図 4.1-3 Web 認証用ユーザーの作成 3

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。

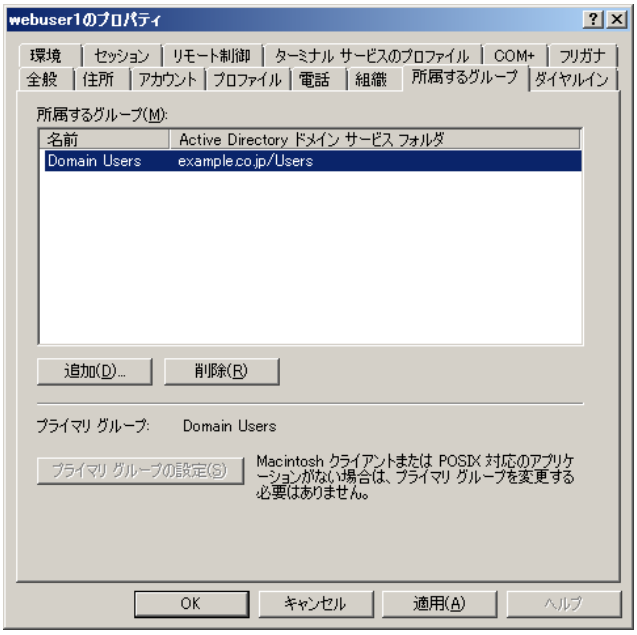


図 4.1-4 Web 認証用ユーザーの作成 4

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。

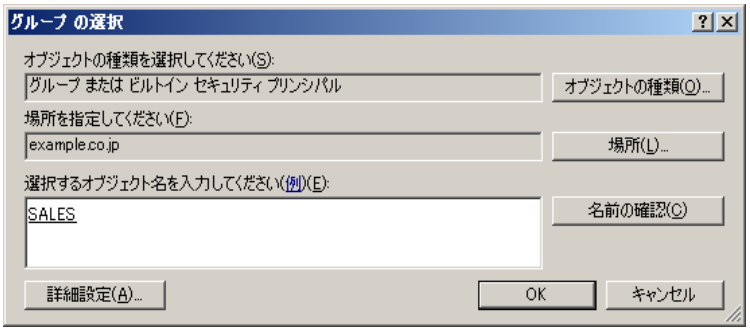


図 4.1-5 Web 認証用ユーザーの作成 5

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。

図 4.1-6 Web 認証用ユーザーの作成 6

⑦ 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。

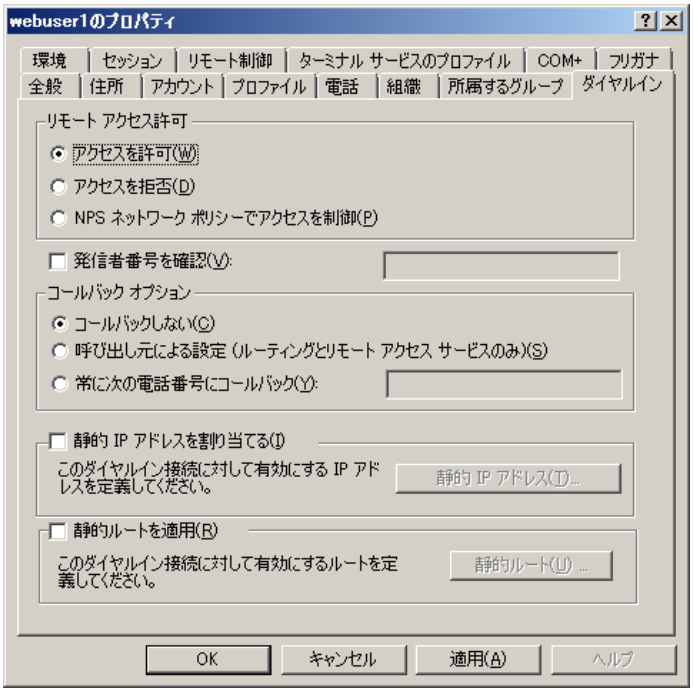


図 4.1-7 Web 認証用ユーザーの作成 7

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。

① 「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。

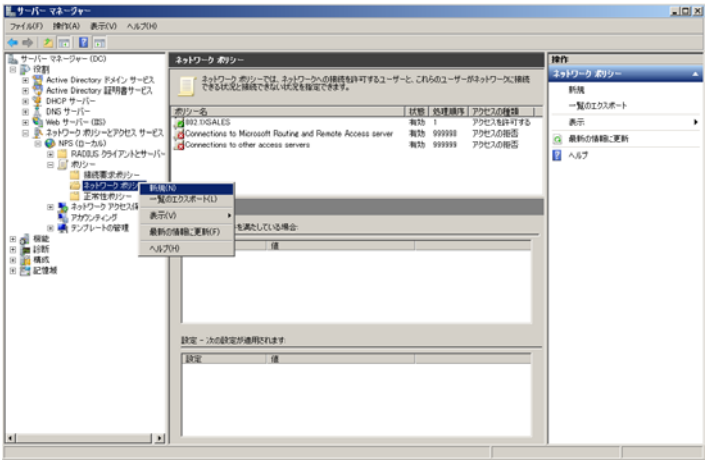


図 4.1-8 NPS の設定 1

② 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。

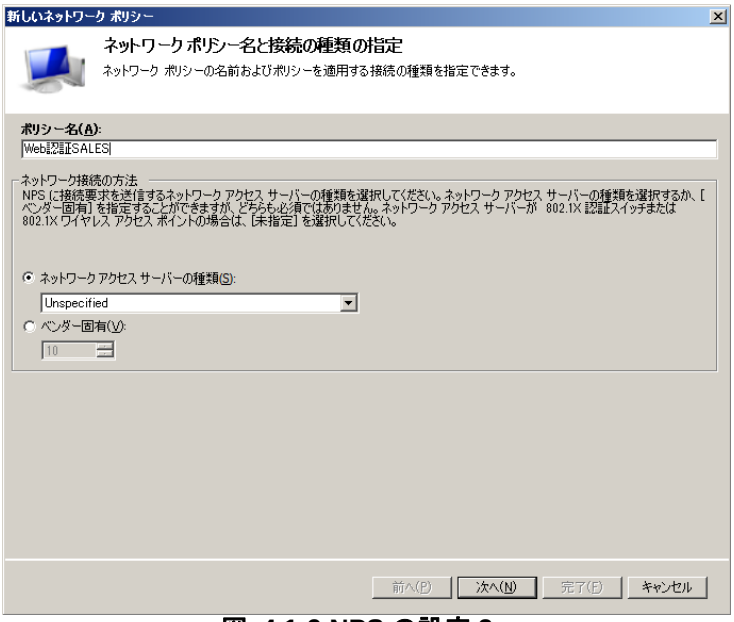


図 4.1-9 NPS の設定 2

③ 条件の指定
「追加」をクリックする。

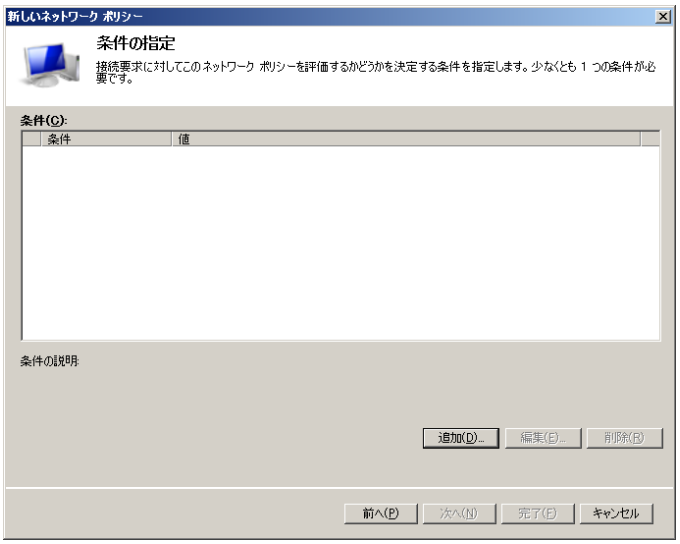


図 4.1-10 NPS の設定 3

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。

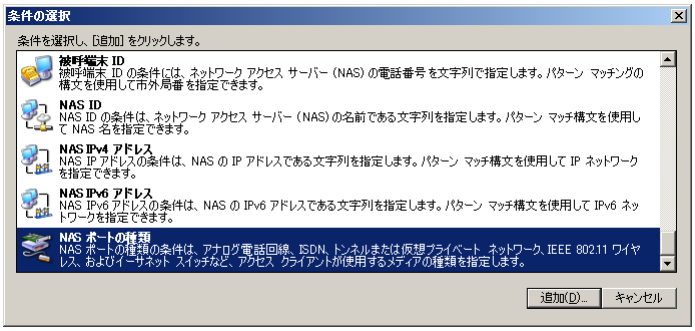


図 4.1-11 NPS の設定 4

⑤ 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。

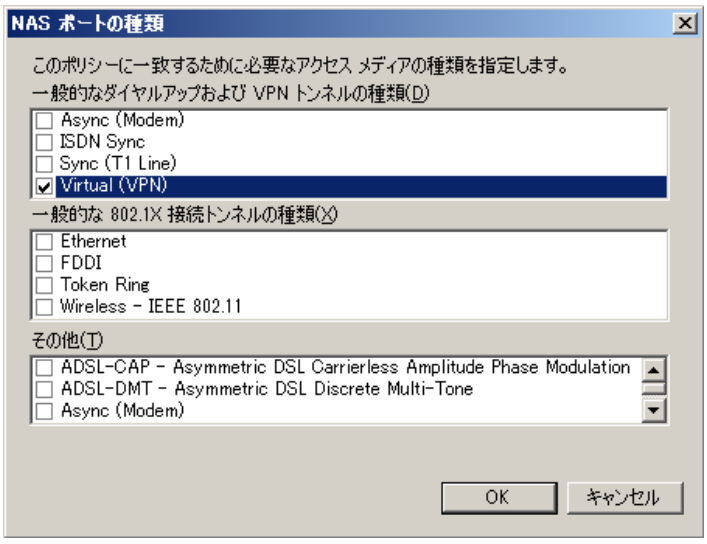


図 4.1-12 NPS の設定 5

⑥ 条件一覧に「条件＝NAS ポートの種類、値＝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。

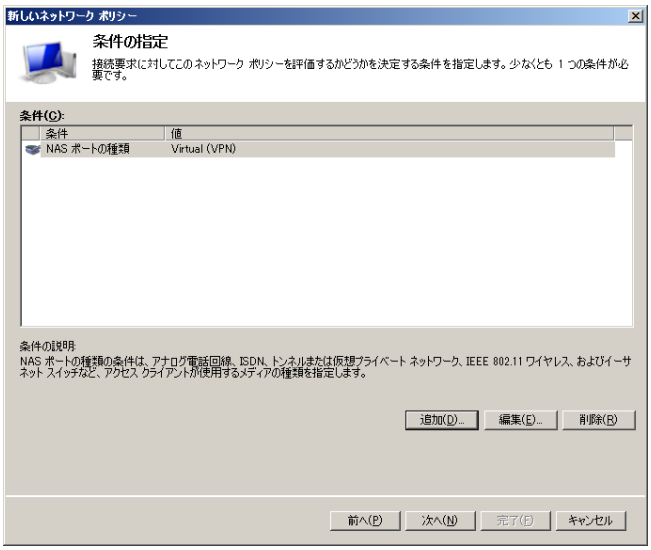


図 4.1-13 NPS の設定 6

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。

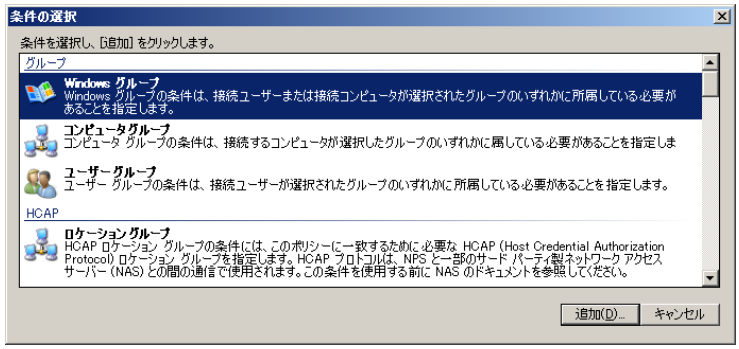


図 4.1-14 NPS の設定 7

⑧ Windows グループ画面にて、「グループの追加」をクリックする。

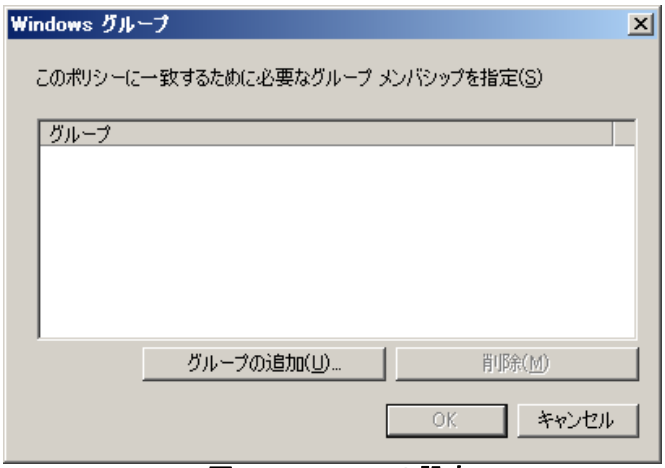


図 4.1-15 NPS の設定 8

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。

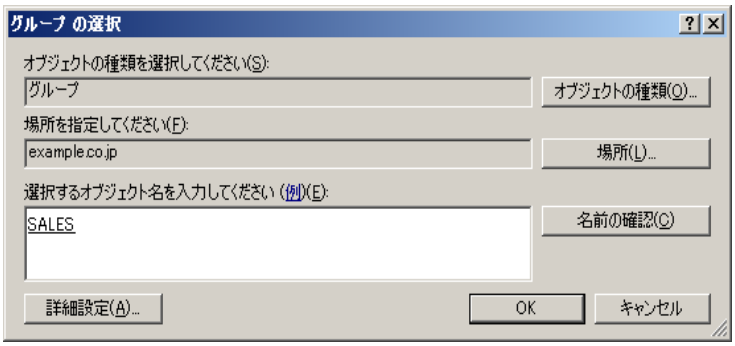


図 4.1-16 NPS の設定 9

⑩ 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。

図 4.1-17 NPS の設定 10

⑪ 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。

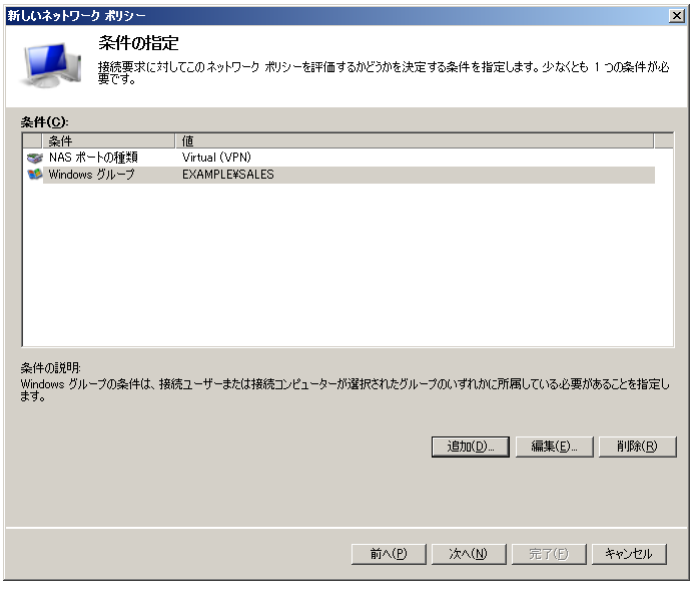


図 4.1-18 NPS の設定 11

⑫ 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。

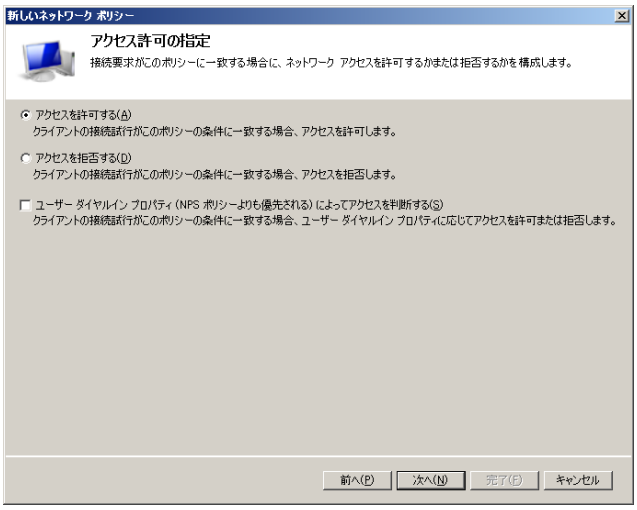


図 4.1-19 NPS の設定 12

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。

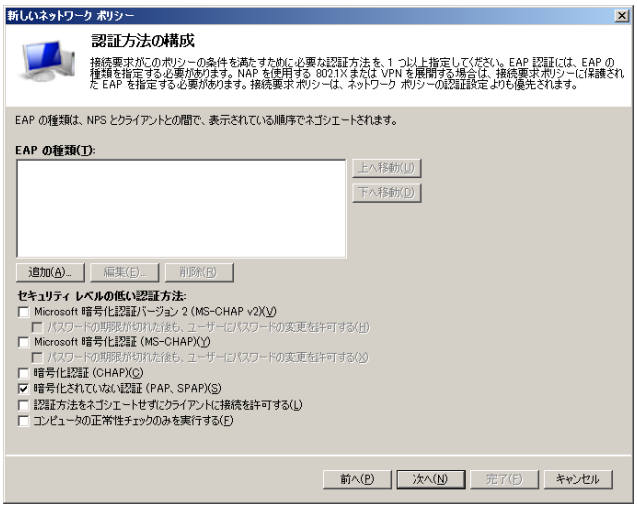


図 4.1-20 NPS の設定 13

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。

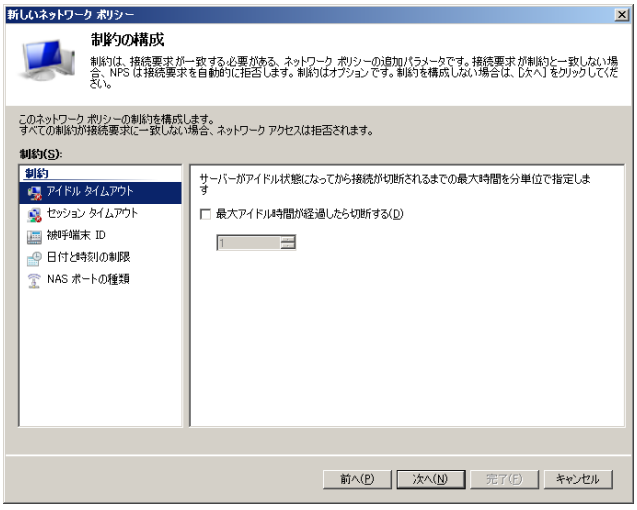


図 4.1-21 NPS の設定 14

※設定の構成

IEEE802.1X認証の手順と同じ。（**3.1.2.（３）（c）**を参照）

⑮ 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。

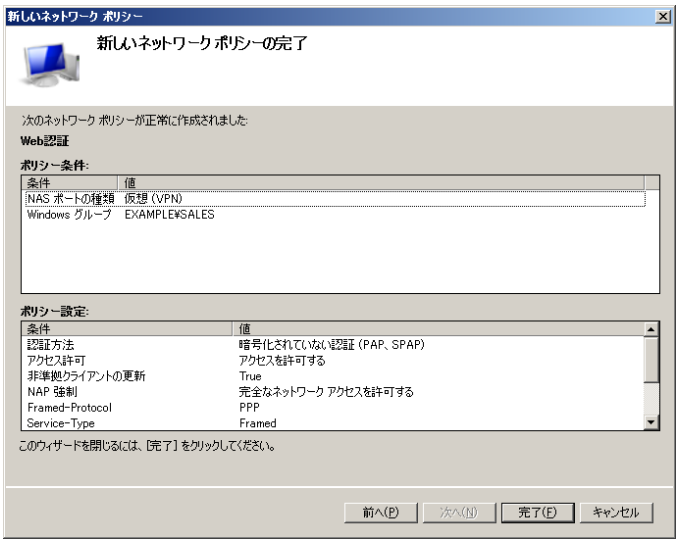


図 4.1-22 NPS の設定 15

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。

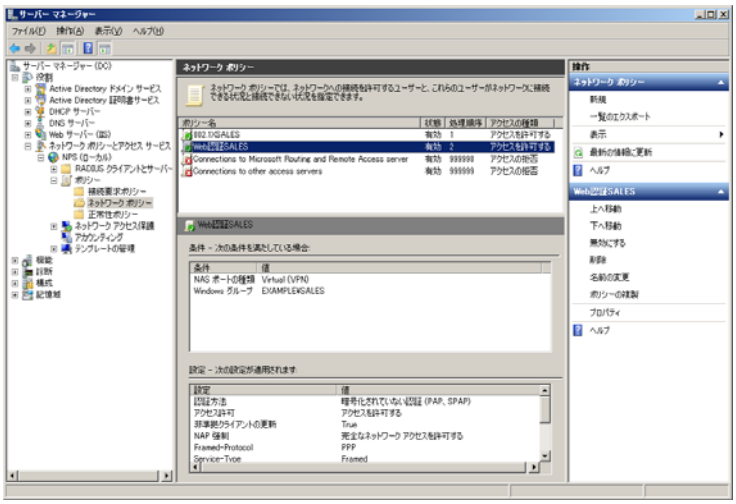


図 4.1-23 NPS の設定 16

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

① 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”）

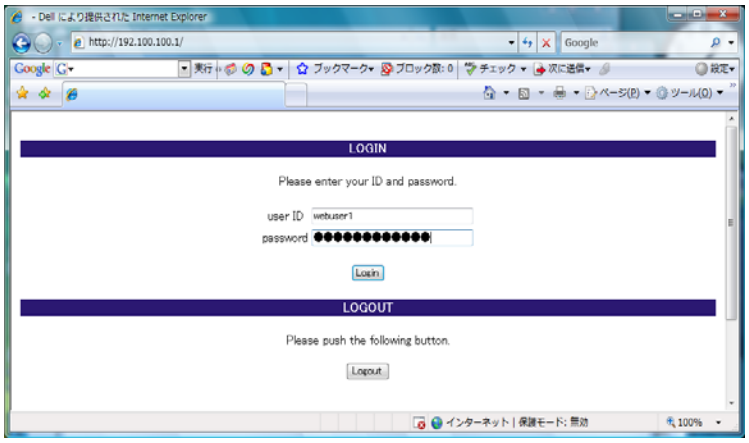


図 4.3-1 Web 認証の確認 1

② 「Login success」と認証成功画面が表示される。

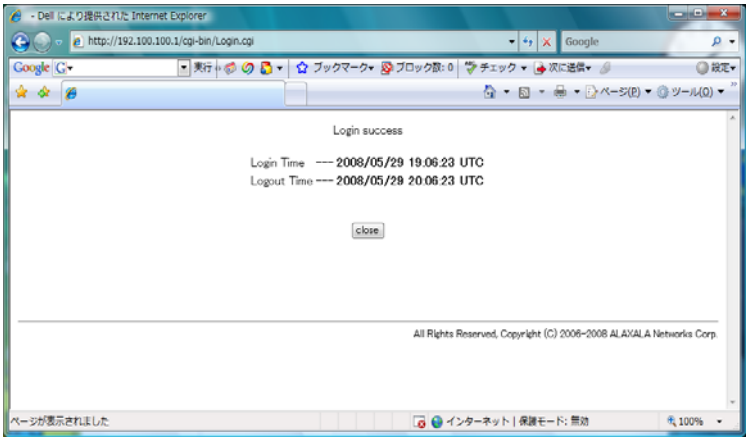


図 4.3-2 Web 認証の確認 2

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。

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。

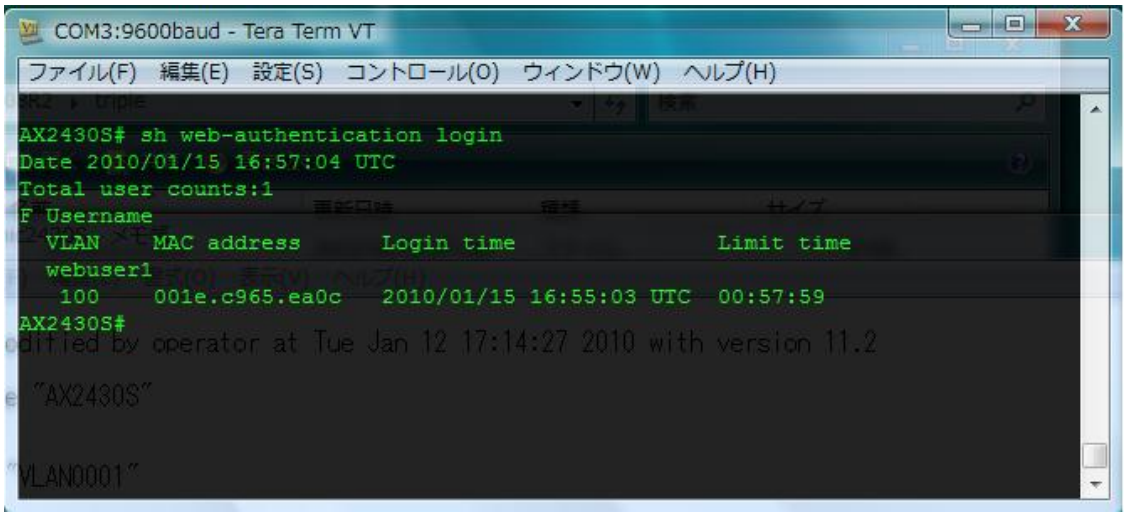


図 4.3-4 show web-authentication login

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。

① 「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。

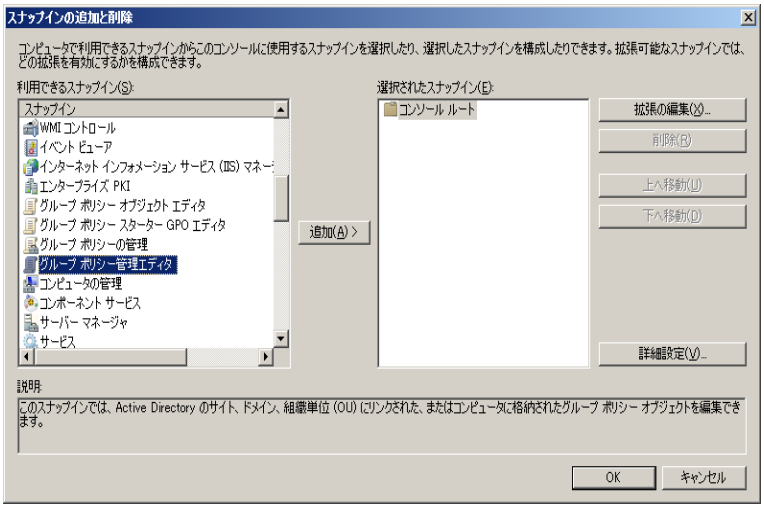


図 5.1-1 MAC 認証の設定 1

② 「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。

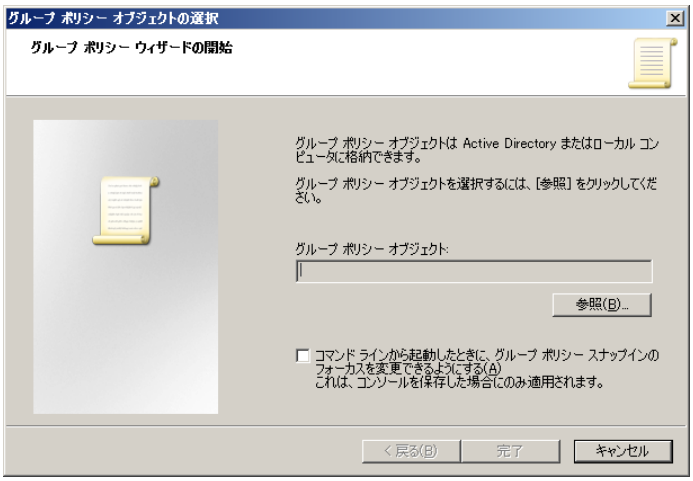


図 5.1-2 MAC 認証の設定 2

③ 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。

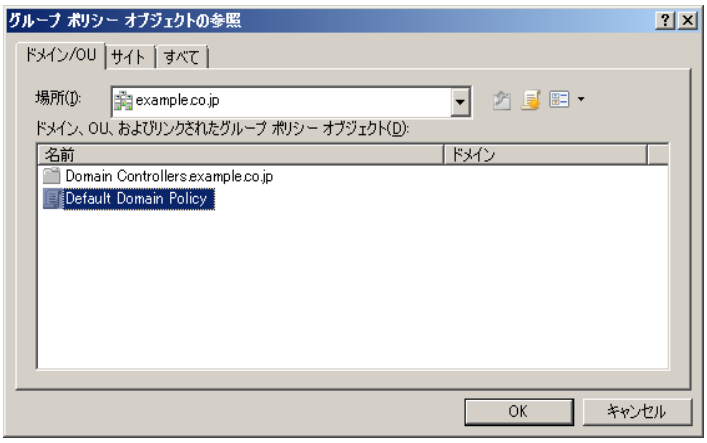


図 5.1-3 MAC 認証の設定 3

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。

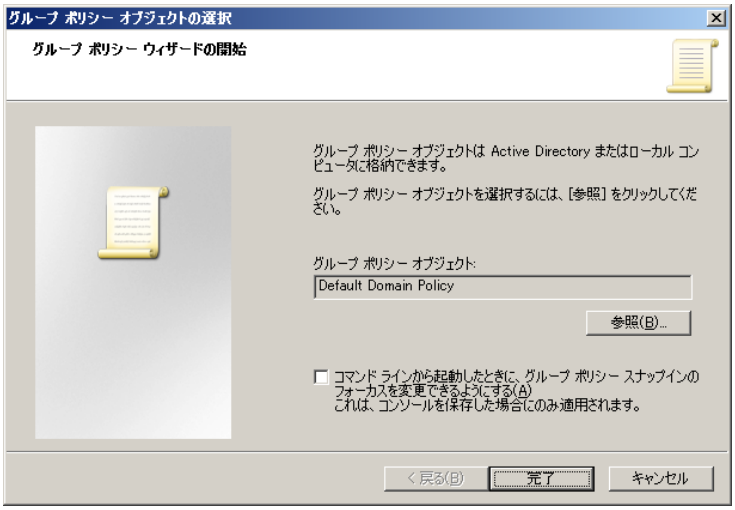


図 5.1-4 MAC 認証の設定 4

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。

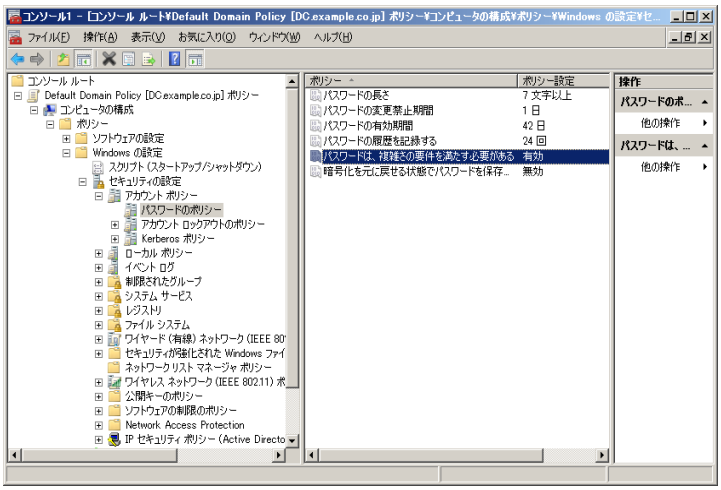


図 5.1-5 MAC 認証の設定 5

⑥ 「無効」を選択して、「OK」をクリックする。

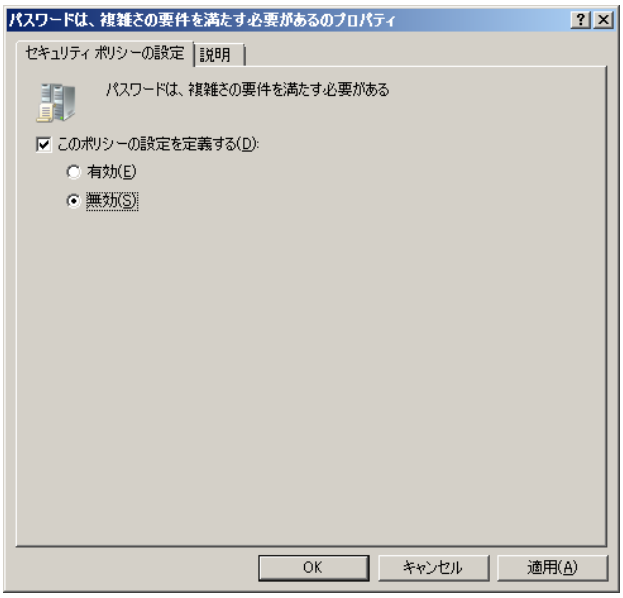


図 5.1-6 MAC 認証の設定 6

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。

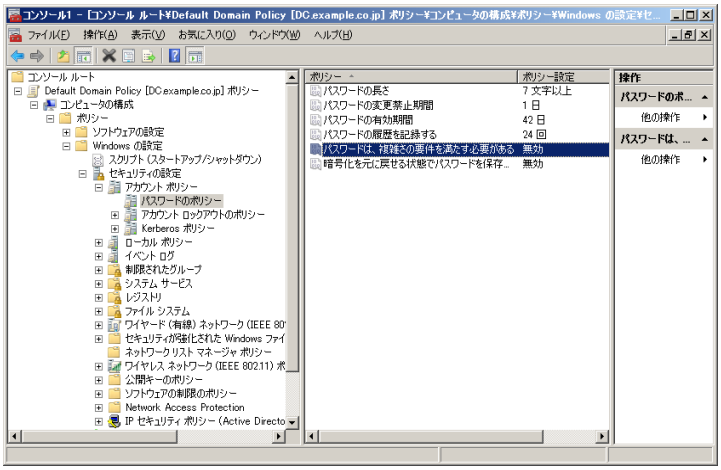


図 5.1-7 MAC 認証の設定 7

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。

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。

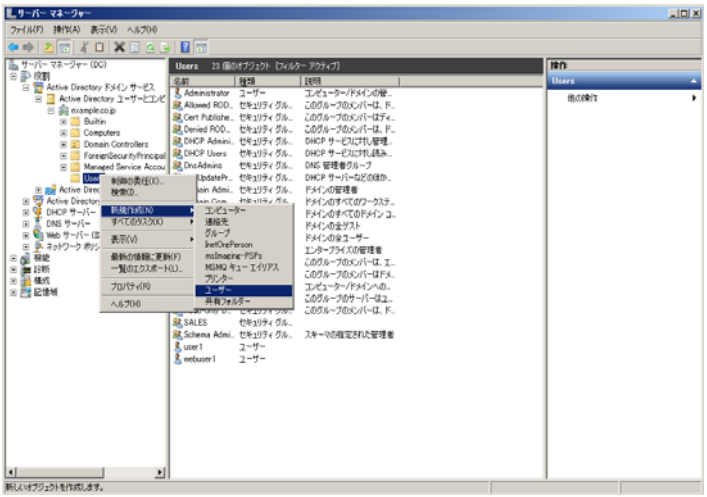


図 5.1-9 MAC 認証の設定 9

⑩ 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

図 5.1-10 MAC 認証の設定 10

⑪ パスワードを入力し、「次へ」をクリックする。

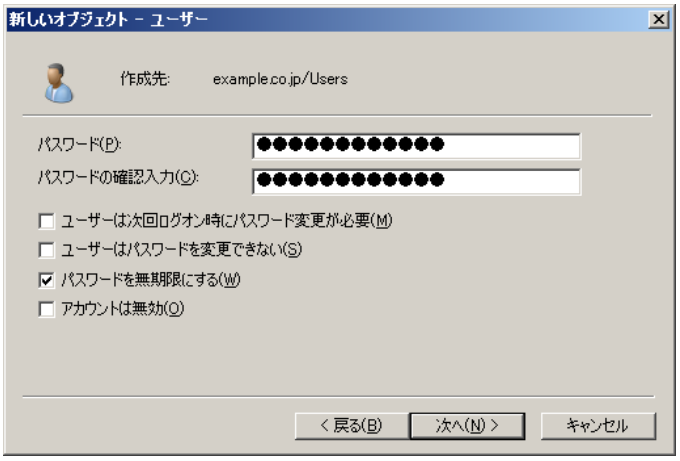


図 5.1-11 MAC 認証の設定 11

⑫ 「完了」をクリックする。

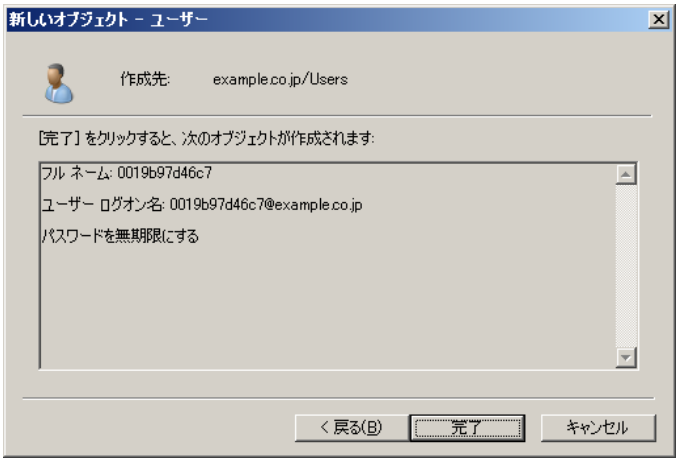


図 5.1-12 MAC 認証の設定 12

⑬ 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。

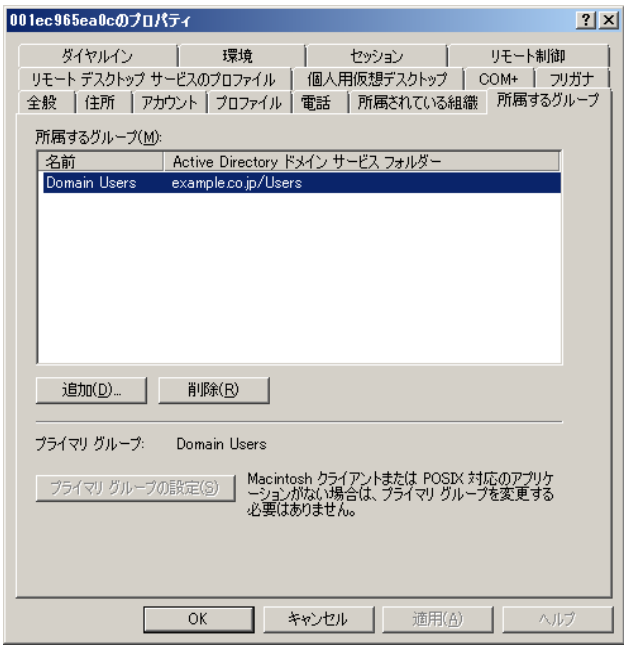


図 5.1-13 MAC 認証の設定 13

⑭ 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。

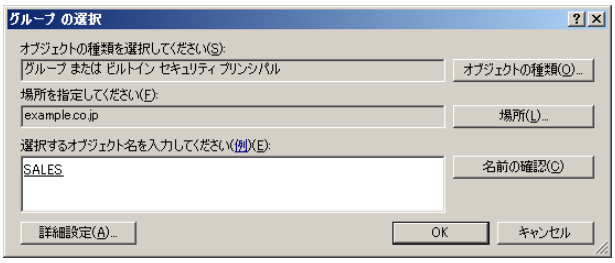


図 5.1-14 MAC 認証の設定 14

⑮ 「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。

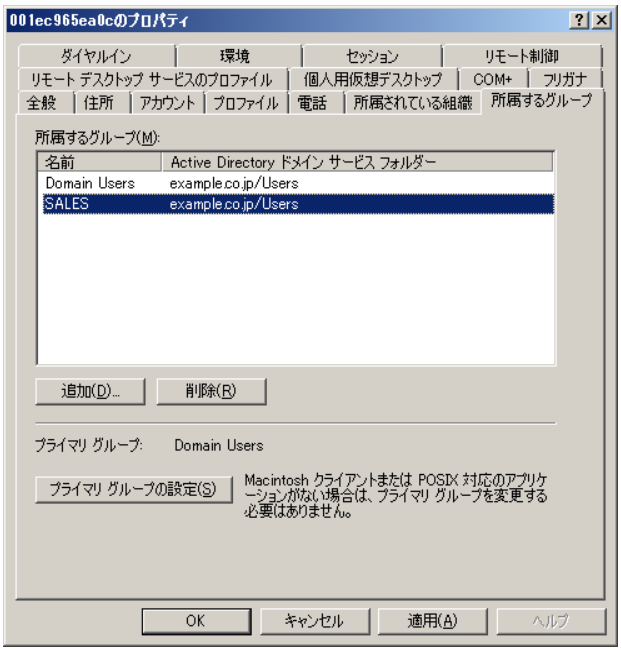


図 5.1-15 MAC 認証の設定 15

⑯ 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。

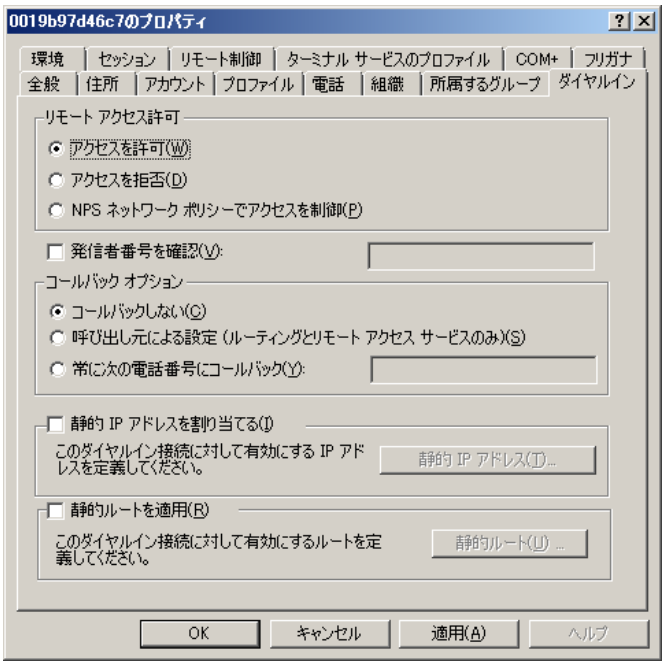


図 5.1-16 MAC 認証の設定 16

5.1.3. NPS の設定

MAC認証でのNPSの設定は、Web認証での設定（4.1.2 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。

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。

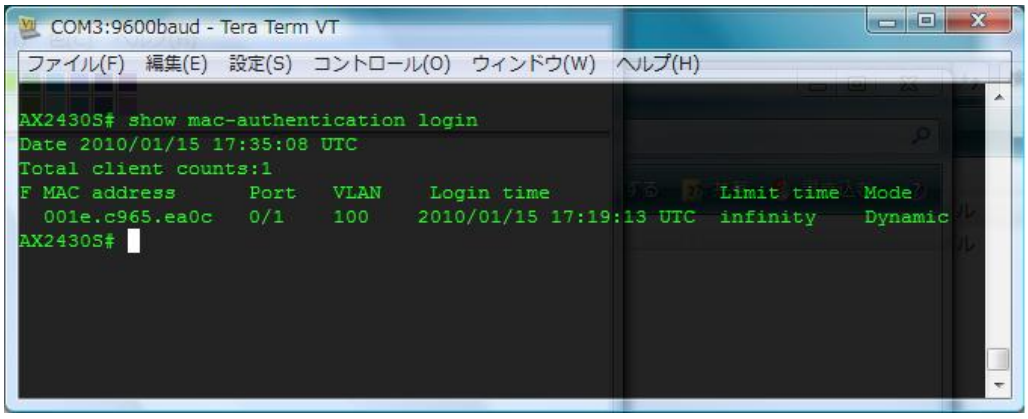


図 5.2-2 show mac-authentication login

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/