

~テスト環境での IPSec NAP の強制~



伊藤忠テクノソリューションズ株式会社





# 目 次

はじめに	
Network Access Protection とは	2
IPSec 構成の NAP	2
テスト環境	3
テスト環境論理図	3
環境作成手順	
ドメインコントローラの作成	
グループの作成	5
ルート CA の構築	5
CA 設定	5
テンプレートの複製	5
組織単位(OU)の構築	
デフォルトドメインポリシーの編集	
自動登録設定	
NPS のインストールと構成	
概要	
Windows Server 2008 のインストール	
NPS の役割のインストール	
役割の追加ウィザード	
下位 CA の構成	
正常性登録機関の設定	
ネットワークポリシーサーバーの設定	21
クライアントの設定	24
グループポリシーによる IPSec の強制	
組織単位への移動	
グループポリシーの適用	
動作確認	
おわりに	



#### 免責事項

本書は伊藤忠テクノソリューションズ株式会社が行った Microsoft Windows Server 2008 に関する様々な検証をもとに記述したものです。

本書は検証における結果をもとに記述していますが、その動作や手順は限られた検証環 境での動作であり、他の検証環境や実環境における動作を明示的にも暗示的にも保証 するものではありません。

また、本書の内容によりいかなる損害が発生した場合においても伊藤忠テクノソリューションズ株式会社はその責任を負いません。

本書に記載された製品名、ロゴ等は各社の商標、登録商標、もしくはトレードマークです。



# はじめに

伊藤忠テクノソリューションズ株式会社は 2007 年から 2008 年にかけて Microsoft Windows Server 2008 に関する検証を実施しました。

製品候補版の段階から数々の検証を実施し、製品発売前に Windows Server 2008 という Microsoftの次期サーバーOS について理解を深め、製品の発売と同時に構築作業が実施でき るようにすることを目的としています。

最終的には RTM 版での動作確認を行っています。

本書は、様々な検証の中で実際に作業した結果をもとに、Network Access Protection(NAP)を IPSec 構成で実装する場合の手順を示したものです。

Network Access Protection(NAP)には様々な構成パターンが存在しますが、IPSec 以外の設定 手順に関してはそれぞれの設定手順書を参照してください。

本書の手順に従い作業を行うことで、IPSecを利用したNAPを構成することができますが、この 手順書の通りに作業した場合、各種の設定項目はデフォルトのままであり、追加の設定が必要 になる場合があります。

また、本書は Active Directory 環境や Windows Server 2008 に関して一通りの知識を持った人を対象に記述されています。

そのため、本書は IPSec を利用した NAP を構成する手順を示すことが目的であり、その前提と なる Windows Server 2008 のインストールや Active Directory の構築方法に関しては記載しま せん。

必要に応じて別途技術資料を参照してください。

本書の内容は Windows Server 2008 Enterprise Edition (x64) を利用して行った検証結果をも とに記載されています。本書内で特に記載がない限り、Windows Server 2008 と記述されている 場合は Windows Server 2008 Enterprise Edition (x64)を指します。





# Network Access Protection とは

Network Access Protection(NAP)は Microsoft の最新サーバーOS Windows Server 2008 に搭載されたネットワーク検疫機能です。

NAP を利用することでセキュリティレベルの低いクライアント PC を社内ネットワークから分離することができます。

NAP には実現方法が5つ用意されており、それぞれに特徴があります。

- -DHCP
- •IP Sec
- •VPN
- •802.1X
- TS Gateway

本書ではソフトウェアレベルで実現可能で、且つセキュリティレベルを保てる IPSec を利用した NAP を実現するための手順を扱います。

### IPSec 構成の NAP

IPSec は通信を暗号化する技術です。IPSec を利用して NAP を構成すると以下のように動作します。

セキュリティポリシーに準拠していると判断された場合には正常性登録機関より証明書が発行 されます。これにより暗号化通信が可能になります。

セキュリティポリシーに準拠していないと判断された場合には証明書は発行されません。このため、このクライアントは暗号化通信ができません。

ある段階でセキュリティポリシーに準拠しなくなったと判断された場合には証明書が削除され、 暗号化通信ができなくなります。

全社的に IPSec を導入し暗号化通信を強制することによって、セキュリティポリシーに準拠して いないクライアントは他のコンピュータと通信できなくなり、社内ネットワークのセキュリティを保 つことができます。

その他の方法に関してはそれぞれの設定手順書を参照してください。

NAPを設定するうえで必要となる各種の用語等に関しては本書では解説しません。必要に応じて各種の技術資料を参照してください。





# テスト環境

## テスト環境論理図

本書は以下の環境を想定しています。



本書の中では上記のマシン名やドメイン名を利用して手順を説明しています。

実際にNAP環境を構築する際にはご自身の環境に合わせて名前やIPアドレスを変更してください。

本書では割愛していますが、必要に応じて WSUS や FCS といったセキュリティを保つためのサ ーバーを構成してください。

### 環境作成手順

NAP のテスト環境を作成するためには、最低限 4 つの役割のサーバーをセットアップする必要 があります。

#### ドメインコントローラ(DC)

Windows Server 2008 が動作している DC01 を使用します。DC01 をドメインコントローラとして Active Directory ドメインサービスと DNS サービスを構成します。

注) NAP 環境においては Active Directory ドメインサービスは必須ではありません。しか しながら、Active Directory ドメインサービスを用いることで、コンピュータのグループに よるアクセス管理やユーザーグループによるアクセス管理など、よりセキュアに使用す ることができます。なお使用する Active Directory ドメインサービスは、Windows Server 2008 でなくてもかまいません。Windows Server 2003 でも使用可能です。



# **ネットワークポリシーサーバーサービス(NPS)** Windows Server 2008 が動作している NPS01 を使用します。NPS01 にネットワークポリシーサー バーサービスを構成します。

### Active Directory 証明書サービス(ルート CA) ドメインコントローラに Active Directory 証明書サービスをインストールし、エンタープライズルー ト CA として構成します。

#### Active Directory 証明書サービス(下位 CA)

ネットワークポリシーサーバーに Active Directory 証明書サービスをインストールし、スタンドア ロンの下位 CA として構成します。

また、NAPを動作させるにはクライアント側の設定も必要です。

#### クライアントの設定

Windows Vista が動作しているクライアント上で NAP クライアントを構成します。

これらのサーバー、クライアントの設定を順次行うことで NAP が動作し、正常性が確認されたク ライアントのみが社内ネットワークに接続できるようになります。

# ドメインコントローラの作成

DC01 に Windows Server 2008 をインストールして次の役割を与えます。 Domain28.local という Active Directory のドメインコントローラ Domain28.local という DNS ドメインの DNS サーバー

手順の概略は次のとおりです。

Windows Server 2008 Enterprise Edition をインストールする TCP/IP の構成を行う Active Directory ドメインサービスをインストールする DCPROMO コマンドを実行して、ドメインコントローラに昇格させる (DNS サービスは同時にインストールする)

ドメインコントローラの作成に関する詳細手順は、ここでは省略します。



# グループの作成

NPS01 をメンバとするためのグループを作成します。 NPS01 がドメインに参加した段階でこのグループのメンバに追加します。

## ルート CA の構築

DC01 に Active Directory 証明書サービスの役割を追加します。 追加の際にエンタープライズのルート CA としてインストールします。

Active Directory 証明書サービスのインストール方法に関してはここでは省略します。

#### CA 設定

「スタート」-「管理ツール」-「証明機関」を選択し証明機関コンソールを開きます。		
CA 名を右クリックし「プロパティ」を表示します。		
「ポリシーモジュール」タブを選択 します。 「プロパティ」ボタンをクリックしま す。	domain28-D001-CAのプロパティ         【1)           証明書マネージャ         登録エージェント         監査         回該エージェント         ゼキュリティ           全級         ポリシーモジュール         終了モジュール         加速機械能         記憶域           アウティブ ポリシー モジュールの説明         名称:         小の回見田         日本           名称:         Windows 既定         日本         日本         日本           129月         アンターブライズを見てんり、ドアロン用に         証明書の要求をどう地達するかを指定します。         パージョン:         60           著作権         の Microsoft Corporation All onts reserved.         ブロパティ(P)_         選択(S)_	
「証明書テンプレートに操作が設 定されている場合はそれに従 い、・・・」を選択し「OK」ボタンをク リックします。	OK     キャンセル     酒田(府)     ヘルプ       プロパティ     ・<	

### テンプレートの複製



「スタート」-「管理ツール」-「証明機関」を選択し証明機関コンソールを開きます。		
CA 名をクリックして展開し「証明書テ	- -ンプレート」を右クリックし「管理」を選択します。	
証明書テンプレートコンソールで 「ワークステーションの認証」を右	■ 王明吉テンプレート コンソール フィイル(F) 皆作(A) 表示(A) ヘルプ(H) 今 中 □ □ □ ● 図 □	
クリックし「テンプレートの複製」を クリックします。	□ 課時書デンプレート(000)     アンパレートを完全、     単小のサポートを知ている 0. パーラ。(日、 3)     「日本     「日本     日本     日本	
	[このテンブルートを巻に、Windows Server 2003, Enterprise Edition CA をサホートするテンプ	
「テンフレートの複製」画面で 「Windows Server 2008 Enterprise Edition」を選択し「OK」ボタンをク リックします。	テンプレートの複製  EIの用書テンプレートは詳細プロパティを指定して作成することもできます。ただし、すべての Windows CA ですべての証明書デンプレート プロパティがサポートされるわけではありませ ん。複製する証明書デンプレートの Windows Server パージョン (サポートする最低限の CA) を選択していたとい。	
	<ul> <li>○ Windows Server 2003 Enterprise Edition(2)</li> <li>○ Windows Server 2008 Enterprise Edition(S)</li> <li>証明書テンプレートの各種パージョンの詳細を表示します。</li> </ul>	
「新しいテンプレートのプロパティ」 の「全般」タブにて「テンプレートの 表示名」を入力します。 (ここでは"SHA"としています) 期間はデフォルトのままで構いま せん。 「Active Directory の証明書を発 行する」にチェックを入れます。	新しいランフレートのプロパティ     X       発行の要件     優先するテンブレート     拡張     セキュリティ       全般     要求処理     暗号化     サブジェクト名       デンブレート表示名(L)     SHA       高小のサポートされている。     GA     Windows Server 2008       このタブで変更を適用すると、以降、テンブレート名を変更することができなくなります。       デンブレート名(T):       SHA       有効期間(V):     更新期間(R):       1     年     6       2     ✓ Active Directory の証明書を発行する(P)       「Active Directory (ご重視する証明書がある場合、自動的に再登録しない(D)       「スマートカート証明書の自動更新で、新しいキーを作成できない場合は既存の       「     キャンセル       通用(A)     ヘルブ	
* 加張」ダブに ビーア ブリグ ージョン ポリシー」を選択し「編集」ボタン をクリックします。		



「アフリケーションホリシーの拡張	アブリケーション ポリシーの拡張の編集
の編集」画面で「追加」ボタンをク	アプリケーションのポリシーで、証明書がどのように使われるかを定義 します。
リックします。	77-41 Jan 2
	<b>追加(A)</b> 編集(E) 育耶余(R)
	「重要な拡張として登録する(M)
	OK ++vJzh
「アプリケーションポリシーの追	
	アナリケーションのポリシーの追加
加」画面で初焼」ホタンをワリソフ	アプリケーションのポリシー(Windows 2000 では拡張キー便用法と呼ばれていました)では 証明書がどのように使われるかを定義します。このテンプレートで発行された証明書の有効 と思えた意味でするアプリケードのの世界してま想用して体影し
しまり。	18月1日1日には19月1日のアンシューンヨンのボウンーに加速す(していたこという)
	アプリケーション ポリシー(A): 「CTL の使用
	IP セギュリティ IKE 中間
	IP セキュリティ ユーサー IP セキュリティ 法端システム KDC 1910
	Microsoft タイム スタンプ Microsoft 信頼リストの署名
	IOUSP 著名 OEM Windows システム コンボーネントの確認 Windows システム コンボーネントの確認
	Windows ハードウェアドライバの確認で カーネルモードのコード署名
	新規(N)
「新しいアプリケーションのポリシ	
	新しいアプリケーションのポリシー
	新しいアプリケーション ポリシーの名前を入力して、必要に応じてオブジェクトの識別子を変更 してください。
は SHA ル、オノシェクトの識別	名前(N):
子に ~1.3.6.1.4.1.311.47.1.1 ぞ人	00001 ナーマジェクト の時日(三/(の))
カします。	1361413114711
何回か「OK」をクリックしテンプレ	
ートのプロパティ画面に戻ります。	
	deficiency and the second se
	王服   要求処理   電方に   57510F名       発行の要件   優先するテンプレート   拡張 セキュリティ
一ノを追加し、「自動登録」の許	グループ名またはユーザー名(G)
可を与える。「OK」をクリック「新し	Authenticated Users
いテンプレートのプロパティ」画面	Domain Admins (DOMAIN28¥Domain Admins)     A Domain Computers (DOMAIN28¥Domain Computers)
を閉じ、「証明書テンプレートコン	& Enterprise Admins (DOMAIN28¥Enterprise Admins)
ソール」画面を閉じます。	(UUMAIN28#NPS)     (Bhn/D)     (BiRe/D)
	<u>メロルパン</u> NPS のアクセク2誌面(P) ジェロ オホホート
	読み取り 書き込み ロー・
	特殊なアクセス許可または詳細設定を表示するには、「詳細設 詳細設定(V) 定]をクリックしてください。
	アクセス制御史アクセス計可の詳細を表示します。
	· · · · · · · · · · · · · · · · · · ·
	OK 「キャンセル」 適用(A) ヘルプ 1





### 組織単位(OU)の構築

クライアントを所属させるための組織単位と NPS01 を所属させるための組織単位を作成します。

クライアント用	IPSec-Secure
ネットワークポリシーサーバー用	IPSec-Boundary

# デフォルトドメインポリシーの編集

デフォルトドメインポリシーを編集し、証明書の自動登録を設定します。

#### 自動登録設定

```
「スタート」-「管理ツール」-「グループポリシーの管理」を開き、デフォルトドメインポリシー
を編集します。
```





NPS01 にて "gpupdate /force" コマンドを実行し、ポリシーを適用します。



# NPS のインストールと構成

#### 概要

ネットワークポリシーサーバー(NPS)を動作させるには Windows Server 2008 が動作している必要があります。

手順の概略は次の通りです。

Windows Server 2008 Enterprise Edition をインストールする TCP/IP の構成を行う domain28.local ドメインに参加する ネットワークポリシーサーバーサービスをインストールする Active Directory 証明書サービスをインストールする Active Directory 証明書サービスを構成する NPS を構成する

以下、手順の詳細を記述します。

### Windows Server 2008 のインストール

コンピュータの電源を入れ Windows Server 2008 Enterprise Edition の DVD を入れます。 画面の指示に従ってインストールを進めます。

インストールが完了したら、Windows にログオンして「ネットワーク接続の管理」から「ローカルエ リア接続」のプロパティを開きます。

Internet Protocol Version 6(TCP/IPv6)のチェックボックスを外します。(本書の手順では IPv6 は使用しません)

Internet Protocol Version 4(TCP/IPv4)のプロパティを開いて、IP アドレス、サブネットマスク、 デフォルトゲートウェイ、優先 DNS を設定して、OK をクリックして画面を閉じます。

ドメインコントローラに ping を実行してレスポンスが正常なことを確認します。

domain28.localドメインに参加して、再起動します。

※OS のインストール、TCP/IP の設定、ドメインへの参加方法の詳細に関しては、Microsoft その他から提供されている技術文書を参照してください。



# NPS の役割のインストール

NPSとCAの役割をNPS01にインストールします。

NPSとCAは別々にインストールすることも可能ですが、本書では同時にインストールする手順を示します。

#### 役割の追加ウィザード

「スタート」をクリックして「管理ツ	₩-8-33-55		
ール」-「サーバーマネージャー」	7かん(日) 操作(合) 表示(公)	~s709 <sup>1</sup> 2	2002
を起動します。	□ サーバーマネージャ(LH00) 日 ● 12月 日 単 12月	サーバー マネージャ (1H02)	
	<ul> <li>※</li> <li>%</li> <li>%</li></ul>	このサーバーの状態の増集の取得、最上位の管理タスクの実行、サーバーの役割や4	#始の適加または単築を行います。 
		◇ サーバーの概要	■ サーバーの概要へルフ
		<ul> <li>・コンピュータ基幅</li> <li>フル エンピュータ名</li> <li>LH02.win2008.local</li> </ul>	● システムプロパティの変更 を キットワーク接続の表示
		ドメイン wir2008.kcal ローカル TUPHRE 2 192198282. Pv6 (株計)	\$ 9t-17X/1970/MMX
		リモート デスクトップ. 有効	
		「ログオン特にこのエンソールを表示しない(Q)	
		<ul> <li>セキュリティ情報</li> </ul>	● Windows ファイアウォールの表示 作 単独立の行い人の単純
		Windows ファイアウォール: 利力) Windows Update: 未構成	42 新しい投影の確認 使われた対応の研究
		更新プログラムの最終確認日時:なし 更新プログラムの最終インストール日 なし	To IE ESC の株式
		193 IE セキュリティ強化の構成 (ESC): 管理者に対して有効 コー・ザーに対して有効	
		▲ 2 2 30 4 2 3 4 3 4 3 4 3 4 3 4 3 4 3 4 3 4 3 4	■ 没料の概要へルフ
		<ul> <li>         ・         ・         ・</li></ul>	■ 0080008880
		○ 最終更新日: 2007/10/31 18:39:08 最新の情報への更新の構成	♥ A 般 😒 🌮 😥 🛤 :
「役割の戦要」を展開しく「役割の	■サーバーマネージャ ファイド(F) 19(7(4) 第三(1)	A 8-100	
追加」をクリックします。「次へ」を			
クリックします。			151 47
	回 <mark>通 格</mark> 成 回 些 記憶地		
		<ul> <li>(交話の概要)</li> <li>(交話) 0/17 信をインストール活み</li> </ul>	■ 投稿の概要へルフ 添 投稿の追加
			🗿 (938608458
			R.
		()最終更新日: 2007/10/31 1839.08 最新の連続への更新の構成	
			♥ A 般 😁 🌮 😖 🚥 :
「役割の追加ウィザード」が起動	役割の追加ウィザード		×
するので「次へ」をクリック」ます	開始する	前に	
1 200 C 32 1200 C 32			
	開始する前に サーバーの役割	このウィザードを使用すると、このサーバーに役割をインストー。 するなどこのサーバーで実行するタス久に応じて、インストール	ルできます。ドキュメントを共有する、Web サイトをホスト する役割を決定します。
	曜12	続行する前に、次のことを確認してください。 ・ 辞理書でかかいに話わたパスワードが設定されていること	
	1進(17)(元) 結果	・静谷 IP アドレスなどのネットワークの設定が構成されている ・Windows Update から最新のセキュリティ更新プログラムが	こと インスキールされていること
		これらのいずれかの条件を満たしていない場合は、ウィザード 度実行してください。	を取り消して必要な処理を行った上で、ウィザードを再
		統行するには、D欠へ]をクリックしてください。	
		□ 既定でこのページを表示しない(S)	
		< 前へ( <u>P</u> )	ホヘ(N)> インストール() キャンセル



「サーバーの役割の選択」ページ 💽 サーバーの役割の選択 が開くので「Active Directory 証明 20サーバー(ビインストールす為代容制を1 つた人上端択(ます。 使意報の: ▲ Arite Directory Rohrts Management サーゼス ▲ Arite Directory Rohr サーゼス ▲ Arite Directory Rohr サーゼス ▲ Arite Directory Rohr サービス ▲ Arite Directory Rohr サービス ▲ Arite Directory Rohr サービス ④ Arite Directory Rohr サービス ● Arite Directory Rohr サービス ● Director サービス ● Arite Directory Rohr サービス ● Arite Directory Rohr サービス ● Director サービス ● Director サービス ● Director サービス ● Directory Directory Port No. ■ Directory Directory Directory Port No. ■ Directory Director 書サービス」と「ネットワークポリシ 開始する前に サーバーの没割 ーとアクセスサービス」にチェック atra ネットワーク ポリシーとアクセス サービスを 利用有ると、ネットワーク ポリシー サー パー(NFS)、レーディグ ジレーモートアク せて、 正常性登録機関(HFA)、および HCAP (Hot Credentia) Autorization Protocol を提出できます。HCAP は ネットワークの正常性とセキュリティの保 識に役立つます。 役割サービス を入れて「次へ」をクリックします AD C 役割サービス セットアップの種類 CA の種類 秘密社 暗号化 CA の名前 証明書の要求 証明書データベース 確認 進行状況 結果 R サーバーの役割の詳細 <前へ(P) 次へ(N) / インストール(D) キャンセル 「ネットワークポリシーとアクセスサービス」に関する説明が表示されます。「次へ」をクリックし ます。 「役割サービスの選択」ページで 後割サービスの選択 「ネットワークポリシーサーバー」 と「正常性登録機関」にチェックを ネットワーク ポリシーとアクセス サービス ロールする役割サービスを選択 役割サービス(R): 説明 開始する前に サーバーの役割 ネットワーク ポパン 入れます。「次へ」をクリックしま ネッドワーク ボリシー サーバー ルーティングとリモート アクセス サービス ローリモート アクセス サービス ロールーティング ーとアクセス サービ. 正常性登録機関では、クライアントから の正常性要求を含む証明書の要求が 検証され、そのクライアントの正常性状 態に基づいて証明書が発行されます。 役割サービス す。 証明機関 □ ルーティング ✓ HCAP (Host Credential Authorization Protocol) 認証要件 サーバー認証証明書 AD 0 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA の名前 証明書の要求 証明書データベース Web サーバー (IIS) R 役割サービス 役割サービスの詳細 進行状況 結果 〈前へ(P) 次へ(N)〉 インストール(D) キャンセル 必要な役割を追加するように促されますので「必要な役割を追加」をクリックします。 「正常性登録期間とともに使用す 正常性登録機関と共に使用する証明機関を選択する る証明機関を選択する」ページで 「HRA コンソールを使用して、後で 開始する前に この正常性登録機関には、1 つ以上の証明機関(CA)を関連付ける必要があります。 1年19日99日に 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.. CA を選択する」を選択して「次 ○ HRA サーバーに対して正常性証明書を発行するため、ローカル CA をインストールする(C) このコンピュータから CA が見つかりませんでした。このオプションを選択すると、新しい CA をローカルにインストールできます。 役割サービス へ」をクリックします。 証明機関 既存のリモート CA を使用する(U) 既存の CA を使用することを選択する場合、その CA は正常性証明書発行専用である必要があります。 認証要件 サーバー認識証明書 道択... AD C ● HRA コンソールを使用して、後で CA を選択する(S) 役割サービス セットアップの種類 CA の種類 ① この CA を構成するまでは、NAP クライアントコンピューダに対して正常性証明書を発行できません。 秘密キー 暗号化 CAの名前 証明書の要求 証明書データベー: R Web サーバー (IIS) 役割サービス 確認 正常性証明書の HRA を介した発行の詳細 進行状況 結果 <前へ(P) 次へ(N)> インストール(0) キャンセル







「セットアップの種類の指定」ペー	1×11××=/00/1/2/1	
ジで「スタンドアロン」を選択して	12ットアップの種類	の指定
「次へ」をクリックします。	開始にする前に サーバーの役割 ネトワーク ポリラーとアクセス サービー (2019年世 モス 室町時間間 2021要件 サーバーに2021年明書 AD CS (役割サービス センドンタンの任和	証明機関は、Active Directory のデーケを使用して証明書の案行と管理を物略化できます。エンタープライズ CA と20メンドアロン CA のどうなを使用するかを指定します。 「エンタープライズ(E) CA かくいくいのメンバであり、ディレンドサービスを使用して証明書の案行と管理を行う場合は、このオフション を選択します。 「アンクトリン(A) CA がティレンドロン(A) CA がティレンドロン(A) CA がティレンドロン(A) CA がティレンドロン(A) CA がティレンドロン(A) CA がティレンドロン(A) CA がティン(A) CA がティン(A) CA がティン(A) CA がティン(A) CA がティン(A) CA がティン(A) CA がたいの(A) CA がたいいの(A) CA がたいの(A) CA がたいの(
	C A の種類 秘密本ー 暗号化 C A の名前 証明音の要求 証明音の要求 経営明サージス 役割サージス 確認 進行状況 結果	<u>エンカープライズ設定とスタンドアロン設定の指摘の詳細</u> < 新へ(P) 法へ(N) インストールの キャンセル
「CA の種類の指定」ページで「下 位 CA」を選択して「次へ」をクリッ	<b>「「」</b> CA の種類の指定	2
クします。	開始まする前に サーバーの役割 ネットワックポリシーとアクセスサーと。 役割サービス 証明明細 に経営業件 サーバー22証証明書 AD CS 役割サービス セットアックの種類 CA の延知 名の広を一	<ul> <li>ルート CAと下位の CA を組み 合わせて構成し、限制的な公開と一巻進(PKD を行成のできます。ルート CAと は、その CA 自体が自己意义に互相引きを指行する CA です。FDD CA は、他の CA がら証明書の発行を空 ける CA です。ルート CA Stati Fib CA のどうを設定するかを指定します。</li> <li>ルート CAR 2.100 - 大幅や 一条線の長上のの正式的できた シストールする場合、または証明報酬を1 つだけインストールする場合 は、このサラシュンを発明を1</li> <li>下位 CA(D) 公開キー委集の上位にある影响 CA から CA 証明書を取得する場合、このオラションを選択します。</li> </ul>
		入 公開キー茶館 (PKD の詳細 <新へ(P) 「次へ(M)> イシストールの 年齢させル
「秘密キーの設定」ページで「新し い秘密キーを作成する」を選択し	秘密キーの設定	
て「次へ」をクリックします。	Phile する前に サーバーの(2割) ネッドワーウ ポリシーとアクセス サーど 役割サービス 証明時間 に容証業件 サーバー記証証明書 AD CS 役割サービス セッドアップの種類 AG の種類 報号化	<ul> <li>記録書を主成してひろいアレイに発行するよばな、なんにない、ホールを要です。新しい地密キーを作成するか、既存の 税名キーモの用するがな話をついます。</li> <li>* 新しい地密キーを作成するにP</li> <li>型空キーパルない場合、または新しい地密キーを作成してビネリティを語してきる場合は、このブラシュンを使用し ないたいです。ないない、地容キーを作成してビネリティを語してきる場合は、このブラシュンを使用し ないたいです。ないないない、地容キーを行われていたなごのかった。</li> <li>* 新しいに定キーを使用する(2) の時インストール体に、し対い定時をひたまであるとかえのため、または、このオラシュンを使用します。</li> <li>* 日時またな深い、問題は付かれているなどキーを使用する(2) このシールークに気付れているなどキーを使用する(2) このシールークに気付れているなどキーを使用する(2) このシールークに気付れているなどキーを使用する(2) このシールークに気付れているなどキーを使用する(2) このシールークに見得られた。************************************</li></ul>
	C & 内 名前 証明者の要求 証明者データベース Web サーバー(TES) 役割サービス 確認 当時1代況 結果	く前へ(P) (次へ(N)) イシストールの キャンセル



「CA の暗号化を構成」ページでけ		
何も変更せず「次へ」をクリックし	日本 CA の暗号化を構	БŬ
ます。	開始する新に サーバーの役割	新しい秘密を一を作成するには、発行する証明書の用途に合った遺伝は連 <u>発化サービスプロパイズ、パレジュア</u> ルコリズム、およりキーの長を使じ通知状況する必要があります。キーの長さに大きな信を選択すると、セキュリティは 強固におりますが、暑谷処理に要する時間が長くなります。
	ネットワーク ポリシーとアクセス サービ 役割サービス	暗号化サービス フロバイダ (CSP) を確保(C): キーの長さ(K) ESA#Microsoft Software, Key Storage Provider マレ 1003 マ
	設計事件 設計要件 サーバージョンデステル日本	
	AD CS 役割サービス	md2 md4 md5
	セットアップの種類 CA の種類	CSPから提供された強力な秘密キー(実績保能を使用する(U) (CA が秘密キー(ごかセスするたび)に管理者(こよる操作が必要な場合があります)
	秘密キー 暗号化 04 の名前	
	証明書の要求 証明書データベース	
	Web サーバー (IIS) 役割サービス	
	118422 )進行(状況 結果	
		< 81~(M) JA~(N)> 10/1-1/10 440004
「CA 名を構成」ページで CA の共 」 通名を入力します。 デフォルトで	了。 CA 名を構成	
はドメイン名とコンピュータ名を使	開始する前に サーバーの役割	この CA を撮影する共通会を入力します。この名前は、CA で発行されるすべての証明書に付加されます。識別名 のサフィックスは自動的に生成されますが、変更できます。
った CA 名が作成されます。 適切に入力したら「次へ」をクリッ	ネットワーク ポリシーとアクセス サービ 役割サービス	<u>この</u> CA の共通者(C) domain28-NP501-CA
りします。	証明機関 認証要件	識別P&のサフィックス(D): DC=domain28,DC=local
	リーハーscalaradine AD CS 役割サービス	 接別になのプレビュー(P): 「Nu-turnering AND/20 (20 D/2-turner/20 D/2-turne)
	セットアップの種類 CA の種類	
	秘密キー 暗号化	
	<b>証明書の要求</b> 証明書データベース	<i>[</i> ₹
	Web サーバー (IIS) 役割サービス	
	曜12 進行状況 結果	
		(BIAU) XAAN) 49XH-JKU **7774
「親CAからの証明書を要求」ページで「朝CAからの証明書の要求」ペー	親 CA からの証明	
信する」を選択し、「参照」ボタンを	開始する前に	この下位 CA の証明書をネットワーク内の親 CA に直接要求することも、要求をファイルに保存して後で親 CA に
クリックします。	サーバーの役割 ネットワーク ポパシーとアクセス サービ	121日することもできます (* 親 CA (注記明書の要求を送信する(E)
	役割サービス 証明規規関 認証原件	参照の単位(0) ○ CA の名前 C コンピュータ名 親 CA DC01 domain28 localWdomain28-DC01-CA 参照(B)
	サーバー記録調明書 AD CS	○ 証明書の要求をファイルに保存し、後から手動で親 CA (ご送信する(V): ファイル名: ○3NPS01.doman28.local.doman28-NPS01-CA.reg 参照(円).
	役割サービス セットアップの種類	① この CA を運用可能な状態にするには、親 CA から手動で証明書を取得する必要があります。
	UN UNE 秘密キー 暗号化	
	CA の名前 証明者の要求	R.
	証明書データベース Web サーバー (IIS)	
	12書9) -CA 確認 進行状況	
	結果	<(前へ(P) 次へ(N)> イジストールの キャンセル
「証明機関の選択」画面が表示さ	証明機関の選択	
れるので、適切なルート CA を選	使用する証明機関 (CA)	を選択してください(S)
ボして「UK」をクリックします。 「親CAからの証明書を要求」ペー	domain28-CA01-C	A CA01 domain28 local
ジに戻ったら「次へ」をクリックしま	uormain28-DCUT-C	
<b>च</b> .		
	2	
		OK キャンセル



「証明書テータヘースの構成」へ ージでは何も変更せずに「次へ」	証明書データベー	スを構成
をクリックします。	開始する新に サーバーの改著引 ネットワークボジッーとアクセス・サービー、 没到サービス 証明機関 さな証明者 カーバーで注意証明書 AD CS 後週サービス センドアック20種類 をごやー に たみの名前 証明者の要求 <b>正辺時者の</b> 要求 <b>正辺時者の</b> 要求 <b>正辺時者の</b> 要求 <b>正辺時者の</b> 要求 <b>正辺時者の</b> 要求	【明書デーケベーンは、経営時金の要求、取行液み経時金、調整な計量時金をおくた知いた経時金をすべて記録 「記号表 デーケベースの注意(1)(2) 「ごの情報に必ら、以前のイシストールで(使用していた証明金データベースを使用する(い) 証号書データベース ログの地類(f)(2) [○WWindown¥oystemの2WCentlog ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
「Web サーバー」に関する説明が 表示されるので、内容を確認し	Web サーバー (II	s)
「次へ」をクリックします。	間時なる前に サーバーの役割 ネットワーク ポッシーとアクセス サービ 役割サービス 正明時間 記証要件 サーバー22証証明時 AD CS 役割サービス セットアップの種類 AD RT にないたい 証明音の要求 証明音の実示 証明音の大いて 注明中ごス 後期サービス 確認 :	Web サーバーは、そのサーバーであったアナーングは、一切かの電力を繋行けて、その置かに引してに等を過ごっかが、 なられてきないたいであった。 なられてきないたいですが、したいたいたいで、 なられてきないたいでは、したいたいで、 なられてきないたいでは、 ならないたいでは、 ならないたいでする。 なられていでする。 なられていたいでする。 なられていたいでする。 なられていたいです。 なられていたいでする。 なられていたいでする。 なられていたいでする。 なられていたいでする。 なられていたいでする。 なられていたいです。 なられていたいです。 なられていたいです。 なられていでする。 なられていたいでする。 なられていたいでする。 なられていたいです。 なられていたいでする。 なられていたいでする。 なられていたいでです。 なられていたいでです。 なられていでです。 なられていで
「役割サーヒスの選択」ページで		
は必要な役割が自動的に選択されています。何も変更せず「次 へ」をクリックします。		ty





以上で NPS と CA がインストールされました。



# 下位 CA の構成

IPSec 用の証明書を発行するための証明機関の構成を行います。

│ NPS01 にて「スタート」-「管理ツー	ル」ー「証明機関」を開きます。	
CA 名を右クリックし「プロパティ」	■certsry - 証明機関(ローカル)¥domain28-NPS01-CA]	
を表示します。	77-(JUE) 操作(A) 表示(V) <>Ju7(H)	
	記録98888 (ローカル)     名前     名	
	(1) (1) (1) (1) (1) (1) (1) (1) (1)	
	最新の情報に更新(F)	
	一覧のエクスボート(U)	
	VIF2(H) 2	
	違択した項目のプロパティ ダイアログ ボックスを開きます。	
「プロパティ」画面で「ポリシーモ	domain28-NPS01-CAのプロパティ ?! ×	
ジュール」タブをクリックし、「プロ	証明書マネージャ   登録エージェント   監査   回復エージェント   セキュリティ   全般 ポリシー モジュール   終了モジュール   拡張機能   記憶域	
パティ」ボタンをクリックします。	「アクティブ ポリシー モジュールの説明	
	名前: Windows 既定	
	説明: エンターブライズおよびスタンドアロン用に 証明書の要求をどう処理するかを指定します。	
	/バージョン・ 60	
	著作権: © Microsoft Corporation. All reserved.	
	54	
	OK キャンセル 通用(A) ヘルプ	
「ニンプレートに撮佐が記字され		
	要求の処理	
	Windows 際空地にノーエジュール/1 この CA が際空でどの下述に部用事の更要な施	
小ダンをクリックします。	理するかを制御します。	
	証明書の要求を受信した場合の操作	
	○ 管理者が調証明書を発行するまで、証明書の要求状態を保留にする(S)	
	○ 証明書テンプレートに操作が設定されている場合はそれに従い、設定されて (パイ)場合は自動的に正明書を発行する(F)	
	N	
円匹割と近9メツセーンかる示    キャキキのティート		
これよりので、Active Directory	変更を有効にするには、Active Directory 証明書サービスを再起動する必要があります。	
□		
] व.	ОК	
円 円 ∪ UA 名を石クリックし ノロハナ	イ」と衣示しより。	





これで、下位 CA の設定は完了です。

#### 正常性登録機関の設定

正常性登録機関の設定を行います。

「ファイル名を指定して実行」から mmc を起動します。	
「スナップインの追加と削除」で	フナップインの合わせる開始
「正常性登録機関」を追加しま	コンピュータで利用できるスキップインからこのコンソールに使用するスナップインを選択したり、選択したスナップインを構成したりできます。拡張可能なスナップインでは
	というねられをで有いたとうらかでを知られてきます。 利用できるスナップイン(S) 選択されたスナップイン(E)
9 0	2.ナップイン パンダ ▲ 描述表の編集(20). 国ルーティングとリモート アクセー Microsoft Corpor.
	Fight ユーザーとガループ Microsoft Corpor      IDStrip      BC検媒エクスプローラ Microsoft Corpor      IDStrip            IDStr
	「 最大本と記憶域の管理 Microsoft Corpor  ・ 上へ移動(U)  ・ 上へ移動(U)  ・ 上へ移動(U)  ・ 上へ移動(U)  ・ しへ移動(U)  ・ しん移動(U)  ・ しんや  ・
	プロージャ Microsoft Corpor_ 通知のAl > 通知のAl > 通知のAl > 通知のAl >
	副語明書 Microsoft Corpor 回語明書 Vブレート Microsoft Corpor
	④信頼性とパフォーマンス モニ Microsoft Corpor   一 信頼性キータ Microsoft Corpor
	「正計性登録機関 Microsoft Corpor  詳細設定(V)
	і Хава Пара Пара Пара Пара Пара Пара Пара Пар
	正常性望録機関の設定を構成、管理します。
「ローカルコンピュータ・・・」を選択	正常性登録機関
$\int \tau \left[ OK \right] \pi \left[ \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \right] \pi \left[ \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2}$	このスキッブインで管理するものを避択してください。
	○ ローカル コンピュータ (このコンソールを実行しているコンピュータ)(L)
	C 他のコンピュータ(A) 参照(W)
	C 構成ファイル(F)
	ファイルの#4%間 このオブションを選択すると、コンパューカには設定を適用しないで、ファイル形式に構成を設定
	Ceals(20089.
	<ul> <li>3mU(1771)(N)</li> <li>名前(M):</li> <li>参照(R)</li> </ul>
	<b>場所(T)</b> : 間((P)
	C 既存のファイル(E)
「正労性祭録機問」を展開「証明機	
	ほうで ノフノノしみり。 2011 - リービリコーナね ブレスム 座部レナナ リコーナム ブ
i 証明 () () () () () () () () () () () () ()	zolocal かりストされているか確認します。リストされて
いない場合には以下の手順を実行し	<b>ノ</b> ます。



機関を追加]をクリックします。           「証明機関の追加」画面で「参照]           「証明機関の追加」画面で「参照]           ポタンをクリックします。           「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。           「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。           「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。           「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。           「証明機関の選択」」画面で NPS01 を選択し「OK」ボタンをクリックします。           「証明機関目でもクリックし「プロパ ティ」を表示します。           「証明機関目でもクリックし「プロパ ティ」を表示します。           「この」」           「この」」」           「ごの」」」           「ごの」」」           「この」」」           「この」」」           「ごの」」」           「ごの」」」           「ごの」」」           「ごの」」」           「ごの」」」           「ごの」」」」           「この」」」」           「ごの」」」」           「ごの」」」」           「ごの」」」」           「この」」」」           「この」」」」           「この」」」」           「ごの」」」」           「この」」」」           「この」」」」           「この」」」」           「この」」」」           「この」」」           「この」」」」」           「この」」」」」」」」」           「この」」」」」」」」」」」」」	「証明機関」で右クリックし「証明	コンソール1 - ロンソールルードす正常性な登録機関(ローカルコンピュータ)Y証明機関     コンソールルードす正常性な登録機関(ローカルコンピュータ)Y証明機関     コンリール1 - レース     コンリール1 - レース     コンリール1 - レース
「証明機関の追加」画面で「参照」         「証明機関の選加」画面で「参照」         「証明機関の選択」画面で、参照」         「証明機関の選択」画面で、参照」         「証明機関の選択」画面で、参照」         「証明機関の選択」画面で、PSOI         を選択し「OK」ボタンをクリックします。         「ごの問題」、こので、「「「」」」         「証明機関の選択」画面で、「参照」         「証明機関の選択」画面で、「参照」         「正明機関の選択」画面で、PSOI         「正明機関の選択」のは、「「」」」         「「」」」」         「」」」」         「」」」」         「」」」」」         「」」」」」         「」」」」」」         「」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」	機関を追加」をクリックします。	
「証明機関の追加」画面で「参照」       第5000000000000000000000000000000000000		コンジールルート     正行性登録機関     新WNFS01 domain28.locaWdomain21     証明確問
「証明機関の追加」画面で「参照」 ボタンをクリックします。         ************************************		■ ● 東京水 プロパティ(R) ・
「証明機関の追加」画面で「参照」 ボタンをクリックします。         「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。           「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。         「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。           「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。         「「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。           「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。         「「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。           「「証明機関」でもカリックし「プロ・パ ティ」を表示します。         「「「」」」」           「「」」」」         「」」」」」           「」」」」         「」」」」」           「」」」」         「」」」」」           「」」」」         「」」」」」           「」」」」」         「」」」」」           「」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」		表示(い) まっこう ( まっこう) 表示 ・
「証明機関の追加」画面で「参照記         「ごいろのののになっていた」」         「「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」」         「ごいろのののになっていた」         「ごいろのののになっていた」         「ごいろのののになっていた」         「ごいろののののになっていた」         「ごいろのののになっていた」         「ごいろのののののののののののののののののののののののののののののののののののの		最新の情報に更新(F) 一覧のエクスポート(U)(0) 最新の情報に、
「証明機関の追加」画面で「参照」 ボタンをクリックします。       「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。         「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。       「「証明機関」で右クリックし「プロ・ ティ」を表示します。         「証明機関」で右クリックし「プロ・ ティ」を表示します。       「「ご」」」」」         「記明機関」で右クリックし「プロ・ ティ」を表示します。       「「ご」」」」」」         「こ」」」」       「「ご」」」」」」         「ご」」」」」」」       「「ご」」」」」」」」」」         「ご」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」		ヘルプ(H) ■ 一覧の192末 ■ 0.1.7
「証明機関の追加」画面で「参照」 ボタンをクリックします。「証明機関の選加」画面で NPS01 を選択し「OK」ボタンをクリックします。「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。「証明機関」で右クリックし「プロパ ティ」を表示します。「証明機関」で右クリックし「プロパ ティ」を表示します。「スタンドアロン証明機関を使用 すっ」を選択し「OK」ボタンをクリ シング「スタンドアロン証明機関を使用 すっ」を選択し「OK」ボタンをクリ シング「スタンドアロン証明機関を使用 すっ」を選択し「OK」ボタンをクリ シング「スタンドアロン証明機関を使用 すっ」を選択し「OK」ボタンをクリ シング「スタンドアロン証明機関を使用 すっ」を選択し「OK」ボタンをクリ ・ 		
「証明機関の追加」画面で「参照」 ボタンをクリックします。       「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。         「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。       「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックします。         「証明機関」で右クリックし「プロパ ティ」を表示します。       「ごちちちちちちちます」         「ごの日本ます」       「ごちちちちちちちちちちちちちちちちちちちちちちちちちちちちちちちちちちちち		
「証明機関の追加」画面で「参照」 ボタンをクリックします。       「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックしま す。       「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックしま す。         「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックしま す。       「「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックしま す。       「「証明機関」で右クリックし「プロパ ティ」を表示します。         「「証明機関」で右クリックし「プロパ ティ」を表示します。       「「証明機関」で右クリックし」「プロパ ティ」を表示します。       「「証明機関」で右クリック」「プロパ ティ」を表示します。		
TAS > 50 (2007) - 2003 - 100 - 2004     TERMENDER - 2004 - 100     TERMENDER - 2004 - 100 - 2004     TERMENDER - 2004 - 2004 - 2004 - 2004     TERMENDE	「証明機関の追加」画面で「参昭」	
「証明機関の選択」画面で、NPS01 を選択し「OK」ボタンをクリックします。            「証明機関」で右クリックし「プロパ ティ」を表示します。	ボタンをクリックします。	副日の構築の万百万円 正常性重要操縦関(HRA)から有効な証明書登録要求を送信する、証明機
「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックしま す。       「「正明機関」で右クリックし「プロパ ティ」を表示します。       「「「証明機関」で右クリックし「プロパ ティ」を表示します。         「証明機関」で右クリックし「プロパ ティ」を表示します。       「「「10000000000000000000000000000000000		間の名前を入力してたさい。 参照(R)
IIII 明機関の選択」画面で NPSOI を選択し「OK」ボタンをクリックし す。		
「証明機関の選択」画面で NPS0I を選択し「OK」ボタンをクリックしま。                「証明機関」で右クリックし「プロパ ティ」を表示します。               「証明機関」で右クリックし「プロパ ティ」を表示します。               「ごの」 <ul> <li>「新田明機関」で右クリックし「プロパ ティ」を表示します。</li> </ul> 「この」 <ul> <li>「新田明機関」で右クリックし「プロパ ティ」を表示します。</li> </ul> <ul> <li>「「新田明機関を使用 する」を選択し「OK」ボタンをわり、</li> <li>「「「「」」」」</li> <li>「「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> </ul> 「「なっ」をないた」         「「」」」」」 <ul> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」」</li> </ul> <ul> <li>「」」」」</li> <li>「」」」」」</li> <li>「」」」」」</li> <li>「」」」」</li> <li>「」」」</li> <li>「」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」」</li> <li>「」」」</li></ul>		HRAで使用する証明書サーバーとして選択しないでください。
「証明機関の選択」画面で NPSOI を選択し「OK」ボタンをクリックしま す。       「「日日間に100 年年 「「証明機関」で右クリックし「プロパ ティ」を表示します。       「「100 日日 100 日 100 日日 100 日 100 日 100 日 100 日 100 日日 100 日 100		OK #1021
「証明機関の選択」画面で NPS01 を選択し「OK」ボタンをクリックしま す。 「証明機関」で右クリックし「プロパ ティ」を表示します。 「証明機関」で右クリックし「プロパ ティ」を表示します。 「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。		
ど選択し「OK」ボタンをクリックしま       1000 5000 0000 000000000000000000000000	「証明機関の選択」画面で NPS01	記明様則の選択 ? X
9 °       D000000000000000000000000000000000000	を選択し「OK」ホタンをクリックしま す	12:H3 5 3 8 10 4 8 10 4 20 8 H C ( X < C ( X ) )
「証明機関」で右クリックし「プロパ ティ」を表示します。	<b>9</b> o	adomain28-DC01-CA DC01 domain28.local
I 証明機関」で右クリックし「プロパ っ」を表示します。		
マイルクレーマン         「証明機関」で右クリックし「プロパ ティ」を表示します。         ジールクレーマン         ジーレアン         ジールクレーマン         ジーレアン		
「証明機関」で右クリックし「プロパ ティ」を表示します。		OK
ティ」を表示します。          ディ」を表示します。 <tbody< th=""><th>「証明機関」で右クリックし「プロパ</th><th></th></tbody<>	「証明機関」で右クリックし「プロパ	
「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。       ()))         ())       ())	ティ」を表示します。	
「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。       ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		□ 小正并性登纬组版 新WNS01 domain/28.local#domain/2.1 □ 小正子性登纬组版 新WNS01 domain/28.local#domain/2.1 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
この時代は92,99(0)       第第第         *数0232*+03.       第約04.         *数0232*+03.       第約04.         *数0232*+03.       第302.         *10150000000000000000000000000000000000		
「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。          「現場類のグロ/5~/ アロ/5*の原示         「現場類のグロ/5~/ アロ/5*の原示             「日間         ・ 0.2012         ・ 1.2012 <th></th> <th>ここから新しいウィンドグ(W) また 最新の信頼に更新(F) ここから新し</th>		ここから新しいウィンドグ(W) また 最新の信頼に更新(F) ここから新し
「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。       ************************************		- 覧のエクスホート(L) へルプ(H) - 覧のエク
「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。		עלידער איזער א איזער איזער איזע
「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。 <ul></ul>		※ 再販 回 プロパティー
「スタンドアロン証明機関を使用 する」を選択し「OK」ボタンをクリッ クします。		・         ・
する」を選択し「OK」ボタンをクリッ クします。	「スタンドアロン証明機関を使用	
クします。 サーバーが利用不可と識別はれたときの要求の間隔(分)XN) この正常性登録機関によって承認された証明書の有効期際(C): 「「日間」」 ・ スタンドアロン証明機関を使用する(S) 「 オリシー OID を有効にする(C) 認知が一切のと有効にする(C) 認知が単純証明書デンブレード(N) 「 クリア> 広谷学校証明書デンブレード(N) 「 クリア> 」	する」を選択し「OK」ボタンをクリッ	
J     この正常性登録機関間によって承認された証明書の有効期限(C):       「     時間       「     時間       ・     スタンドアロン語明機関を使用する(S)       「     ポッシー OID を有効にする(O)       ・     エンターブライズ証明機関を使用する(E)       ビ乙証済み準地証明書デンブレード(U):         ベクリア >        ビスシンブレード(Y):	クします。	サーバーが利用不可と識別されたときの要求の間隔(分)NN
この正常性登録機関によって承認された証明書の有効期限(C):		3
□     □		この正常性登録規関によって承認された証明書の有効期限(C):
<ul> <li>「ポリシー OID を有対にする(O)</li> <li>「エンターブライズ証型明線関連使用する(E)</li> <li>記録正済み 準純証明常書テンプレート(U):</li> <li>「</li> <li>(</li> <li>(<th></th><th></th></li></ul>		
		「ポリシー OID を有効にする(0)
< 2012 > ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		・ エレターブオース MEP 4960 (21だけ) 9 3 (と) 認知道 ネタングレート(し):
< 2007 > ▼		トクリアシー 匿名準拠認明書テンプレート(Y):
<u>OK</u> <u>キャンセル</u> 通用(A)		<u>OK</u> <u></u> キャンセル 通用(A)



#### ネットワークポリシーサーバーの設定

NAP を提供するためのポリシーサーバーを構成します。

まずはウィザードを利用して必要なポリシーを作成し、その後、セキュリティ正常性検証ツール を設定します。

#### AD への登録

スタートをクリックして「管理ツール」-「ネットワークポリシーサーバー」をクリックします。	
「NPS(ローカル)」を右クリックし、「Active Directory にサーバーを登録」をクリックします。	

#### NAP 構成ウィザード

「NAP で使用するネットワーク接	NAP を構成する X
売方法の選択」ページが開いた ら、「ネットワーク接続の方法」で	NAP CT使用 9 るイットリーク接続方法の選択
プルダウンから「正常性登録機関 HRA)を使用する IPSec」を選択し	<b>ネットワーク接続の方法:</b> NAP 対応クライアントコンピュータ用にネットワークに展開するネットワーク接続方法を選択してください(L) 作時なれたポリントは、ロスマットワーク接続の種類にのみ動作します。追加のネットワーク接続方法のポリシーを作成
ます。「ポリシー名」には自動的に	9 らにしは、ワイサートを用成果(TUCいたこい。 正治性登録規関 (HRA)を使用する IPsec
NAP IPSec と HRA」か入ります。 「次へ」をクリックします。	<b>ポリシー名:</b> このウィザードで作成されるポリシーには、下記の文字列的名前の一部として使用されます(T) このまま使用することも、変更することもできます。
	NAP IPsec と HRA 追加要件:
	● NAP をセットアップするには、追加のアクションを実行する必要があります。下のリンクをクリックして、追加の NAP 要件を表示してください。 <u> 遠加要目+(U)</u>
	N
	い 前へ(P)
	NAP を構成する X
ーの指定」ページでは特に何も設 定せず、「次へ」をクリックします。	HRA を実行する NAP 強制サーバーの指定
	RADIUS クライアントは、ネットワーク アクセス サーバーであり、クライアント コンピューダではありません。ローカル コンピューダで HRA を実行している場合、この手順を省略して じべいをがっかします。
	リモート HRA サーバーを RADIUS ウライアントとして通知するには、し飯加」をワックします。通知するすべてのリ モート HRA サーバーで、 RADIUS ウライアンドしている連載があります。とたい、リート HRA-NPS サーバーは、接続 要求をこの NPS サーバー(ローカル コンピュータ)に転送する必要があります。
	RADIUS クライアント(G):
	R
	554/00 ( 564/00 ) = = 7/0 ( 410 APU )



「ユーザーグループとコンピュータ   グループの構成」ページでも、今   回特に設定を行わないので、「次   ヘ」をクリックします。	NAP を構成する × ユーザーグループとコンピュータグループの構成
	コンピュータのクレーフに対してからたを行うまたは社会する場合は、ロンピュータクルーフルビクループを追加しま す。ユーザーののループに対してからたを行うまたは社会する場合は、ローザークループのに分ん す。このポリシーに対し、コンピュータグループとコーザーグループの両方を構成できます。 グループを選択しないと、このポリシーはすべてのユーザーに適用されます。 コンピュータグループ:
	K
	<u>前へ(P)</u> 次へ(N) 完了(F) キャンセル
「NAP 正常性ポリシーの定義」ペ	NAP を構成する
ージではデフォルト設定を確認します。テストのために「クライアン	NAP 正常性ポリシーの定義
トコンビュータの自動修復を有効 にする」のチェックをはずします。	インストール本れているシステム正常性検証シールの一覧です(S) この正常性まれジーで強制するシステム正常性検証シールだけを選択してください。 名前
	Windows セキュリティ正常性検証ツール
	■  ア クライアントコンピュータの自動修復を有効にする(E) 道理尺にた場合、正常性有りシーに準絶していないを助にネッドワークへのフル・アクセスを拒否された NAP 対応クラ イアントコンピュータムの 開催サージーメのクリンドウマ ア軍計のクラムを取得てきます。
	選択しない場合、非準拠の NAP 対応クライアント コンピュータは自動的に更新されず、手動で更新されるまで 完全なネットワーク アクセスは得られません。
	₽ ₽
	前へ(P)   次へ(N) 完了(F)   キャンセル
	11AD + 48-49-17
「 NAP 強制ポリシーおよび RADIUS クライアント構成の完了」 ページで「完了」をクリックして、ウ ィザードを終了します。	NAF をあみする AP 強制ポリシーおよび RADIUS クライアント構成の完了
	:次のボリシーが正常に作成され、次の RADIUS クライアントが正常に構成されました。 <ul> <li>・既定のブラウザで構成の詳細を表示するには、「構成の詳細」をクリックしてださい。</li> <li>・構成を変更するには、「新八」をクリックしてださい。</li> <li>・構成を変更するには、「新八」をクリックしてださい。</li> </ul>
	正常性ポリシー NAP Free と HRA 準拠 NAP Free と HRA 準拠 猪袋要求ポリシー: NAP Free と HRA ネットワーク ポリシー: NAP Free と HRA 準拠 NAP Free と HRA 非準拠
	<u>前へ(P)</u> 次へ(N) 完了(F) キャンセル

ウィザードが完了し、5つのポリシーが作成されました。

正常性ポリシー

NAP IPSec と HRA 準拠



NAP IPSec と HRA 非準拠

接続要求ポリシー NAP IPSec と HRA

ネットワークポリシー

NAP IPSecとHRA 準拠

NAP IPSecとHRA 非準拠

#### セキュリティ正常性検証ツールの設定

のコンソールで「NAP(ローカル)」					
を展開し、「ネットワークアクセス 保護」-「システム正常性検証ツー ル」クリックします。右ペインで 「Windows セキュリティ正常性検 証ツール」をダブルクリックしてプ ロパティを表示させます。	NPS (10-5/h)         ●         > 2/5/L 正常性検証ソール (5/NV)では、NAP 対応25/(アントンビュータンと変お設定性推定できます。SNV           PADUE 5 /5 / アント         ●         ※         ● <t< th=""></t<>				
	・         ・				
「Windows セキュリティ正常性検証ッ をクリックします。	ノールのプロパティ」ダイアログが表示されるので「構成」				
「Windows セキュリティ正常性検 証ツール」ダイアログが表示され るので「Windows Vista」タブで「フ ァイアウォール」と「自動更新」だ けチェックを入れた状態にして 「OK」をクリックしてダイアログを 閉じます。	Windows 位もリティを活住とヨシール         ウ」           Windows Vita [Windows Xiz]         UT CodE電話を見用して、Windows セキュリティを素性を経営シール わりンーも定義します。ここで違原した作品により、ネットワーンに接続するウライアント コンビューシの原件が定義され ます。           11 Edata [Line   Windows セキュリティを素性を経営シール わりンーも定義します。ここで違原した作品により、ネットワーンに接続するウライアント コンビューシの原件が定義され ます。         「           12 F 2 かけつ フリまれました(ア・ア・ア・ボードを定義します。ここで違原した作品により、ネットワーンに接続するウライアント コンビューシの原件が定義され ます。         「           12 F 2 かけつ フリまれました(ア・ア・ア・ボードを行んが)         「           12 F 2 かけつ ア・ボードを行んが(加)         「           12 F 2 かけの ア・ブレンドを行んが(加)         「           12 F 2 かけつ アンビントのアンドントのアンドンたを発展する(20)         [           12 F 2 かけで たい         「           12 F 2 かけつ ア・ブレンドを行いて クリント・ボード たい ア・ブレンドン たい ア・ブレンドン たい				
再び「Windows セキュリティ正常性検 をクリックしてダイアログを閉じます。	証ツールのプロパティ」のダイアログに戻るので、「OK」				

「ネットワークポリシーサーバー」のコンソールを終了します。これで、ネットワークポリシーサー バーの設定は完了です。



#### クライアントの設定

クライアントの設定を行います。

Windows Vista に管理権限のあるアカウントでログオンします。





アドレスを追加する前に「すべてサ	新しい信頼されたサーバー グループ	X
ーバーの確認(https)を必要とす	サーバーの追加	
る」のチェックボックスを OFF にしま	クライアントに信頼させる正常性登録機関の URL を追加してください(L)	
す。		ieto(A)
「完了」ボタンをクリックします。	信頼されたサーバー(S): URL http://nps01.domain28.local/domainhra/hcsrvext.dll http://nps01.domain28.local/nondomainhra/hcsrvext.dll	[上へ移動(U)] [下へ移動(D)]
	<	
	前へ(P) 次へ(N) 完了(F)	48 **>t211

「コンピュータの管理」-「サービス」から「Network Access Protection Agent」のプロパティを表示 して「全般」タブで「スタートアップの種類」を「自動」にし、「開始」ボタンをクリックしてサービスを 開始させます。

クライアントの設定が完了しました。

# グループポリシーによる IPSec の強制

IPSec を強制するため、グループポリシーを設定します。

ドメインコントローラにて「グループホ	ポリシー管理ツール」を起動します。
グループポリシーを新規に SecureF	Policy という名前で作成します。
「コンピュータの構成」-「ポリシ ー」-「Windows の設定」-「セキ コリティが強化された Windows フ	
エリアィか強化された Windows フ ァイアウォール」ー「セキュリティ が強化された Windows ファイアウ ォール LDAP」まで展開します。 「接続セキュリティの規則」で右ク リックし「新しい規則」をクリックし ます。	TUL-2-40構成     TUL-40構成     TUL-40構成     TUL-40構成     TUL-40構成     TUL-40構成     TUL-40/構成     TUL-40/H     TUL-40



「規則の種類」画面で「分離」を選	🐭 新規の接続セキュリティの無	則ウィザード 🛛 🗴	
択し「次へ」をクリックします。	規則の種類		
	1年成する接続のセキュリティの現象	112200	
	<ul> <li>規則の種類</li> </ul>	作成する接続セキュリティの規則の種類を選択してください。	
	● 要件	6 UM	
	<ul> <li>認証方法</li> <li>プロファイル</li> </ul>	* 5788(1) ドメインのメンバシップや正常性の状態などの認証基準に基づいて接続を制限します。	
	<ul> <li>名前</li> </ul>	○ 記録の除外(A) 指定したコンピュータからの接続を認証しません。	
		○サーバー間(S) 指定したコンピュータ間の接続を認証します。	
		○ トンネル(T) ゲードウェイ コンピューク間の接信を認証します。	
		たえきム(C) サンド/ (1498)	
		注意: 接続性性コリティ規則は、認識の実行される方法と特期を指定しますが、接続を許可しま	
		されの特徴ではキャリラムには、支目書かには201日の7月19日21FのACは 9。 規則の経験の詳細を表示しませ	
		_<床約(B): 3本へ(N)>	
「要件」画面で「受信接続の認証	新規の接続セキュリティの規	関ウィザ〜ド▼	
を必須とし、送信接続に対して認	要件		
証を要求する」を選択し「次へ」を	この規則に一致する接続の認証	の要件を指定してください。	
ことをかりる」を送水し、水、」と クリックします	スプラン: ● 規則の種類	どのような条件で認証を実行しますか?	
	<ul> <li>● 要件</li> <li>● 認証方法</li> </ul>	⑦ 受信接続と送信接続に対して認証を要求する(R) 可能な場合は認証を要行しますが、認証な必須ではありません。	
	<ul> <li>ブロファイル</li> <li>名前</li> </ul>	⑦ 受信操続の認証を必須とし、送信操続に対して認証を要求する(E)	
		受信接続には認証が必要です。送信接続では可能な限り認証が実行されますが、認証は 必須ではありません。	
		○ 受信接続と逆信接続の22証を要求する(0) 受信接続と逆信接続のいずれにも認証が必要です。	
		認証要件の詳細を表示します	
		R.	
		< 戻る(B) (次へ(N)> キャンセル	
「認証方法」画面で「コンピュータ			
	部所規の接続でキュリティの展 認証方法	與II/7寸~下 <u>X</u>	
	規則に一致する接続に対して行き	23認証方法を指定してください。	
「参照」ホタンをクリックしルート	ステップ: - ###########	どの認証方法を使用しますか?	
CA を選択します。	<ul> <li>● 要件</li> </ul>	○ 既定(0)	
「正常性証明書のみを受け入れ	<ul> <li>認証方法</li> <li>ブロファイリ</li> </ul>	プロファイルのプロパティで指定された32話を方法を使用します。	
る」にチェックを入れ「次へ」をクリ	<ul> <li>ノロノアバル</li> <li>名前</li> </ul>	C コンピュータとユーザー(Ketheros VS)(C) ドメインに参加しているユーザーとコンピュータが必須抵抗に通信を制限します。受信と送信 規則で特定のユーザーやコンピュータを承認するとき、ID 情報を提供します。	
ックします。		C コンピュータ (Kerberos V5)(O) ドメイン(全参加しているコンピュータからの現状に)通信含制限します。受信と送信規則で特定のコンピューの存在記名であた。10 情報を提供します。	
		⑦ コンピュータ証明書(T) この証明相関(CA)から発行された証明書を持つコンピュータからの接流に過信を制限しま	
		す。 CAの名前 DC=local, DC=domain28, CN=domain28-DC01-CA 参照(R)	
		ご 正常性証明者のみを受け入れる(H)   ご 詳細設定(A)	
		10人タムの1 巻目と 2 巻目のは28話時定を指定します。 <u> カスタイズ</u>	
		< 電気(R)    (大へ(M) > ) またいたれ、	



「ブロファイル」画面ですべての項	新規の接続セキュリティの規則ウィザード			
日にチェックを入れ「次へ」をクロ	วํตวราม			
	この規則が適用されるプロファイルを指定してください。			
ックします。	<b>ステップ</b> :			
	• 要件			
	<ul> <li></li></ul>			
	● プロファイル			
	<ul> <li>名前</li> <li>フライベート(P)</li> <li>コンピュータがフライベートネットワークの場所に接続しているときに適用されます。</li> </ul>			
	ズ パブリック(D)			
	コンピュータがパブリックネットワークの場所に接続しているときに適用されます。			
	プロファイルの詳細を表示します			
	N			
「名前」画面で Secure Rule と入	● ビ油の物料をといこの加加点 ポード			
	2前			
カし「元」」ホタンをクリックしま	この規則の名前と説明を指定してください。			
<del>.</del>				
<b>7</b> o	A 392- ##RI/058+10			
	· 7500001200			
	<ul> <li> 認識方法</li> <li> 名前</li> </ul>			
	Jロファイル     Secure Rule			
	● 名前			
	記号用(オブション):			
	× .			
	〈戻る(B) 完了(F) キャンセル			
作成されたポリシーを	夏 グループ ポリシーの管理			
IPSec-Seure 組織単位に割り当	🗢 🔿 🖄 📷 🗈  📽 🔯 🖉 📅			
アキオ	IPSec-Secure IPSec-Secure			
しまり。	<ul> <li>□ △ フォレスド doman28.local</li> <li>□ ○ ○ ドレイン</li> <li>□ □ ○ 下レイド</li> <li>□ □ ○ 下レイン</li> <li>□ □ ○ ○ ドレイン</li> </ul>			
	日 論 domain28.local リンクの順序 ^ GPO (強制 リンクの有効化 GPO の状態 WMI 7-7)			
	Elevant Domain 会 1 Mar SecurePolicy (八 ほい 有効 なし     Elevant Domain Controll			
	E Broker-Boundary			
	SecurePolicy			
	BoundaryPol			
	i≣ Default Dom			
	SecurePolicy			
	世 WMI フィルタ 世 2月 2月 - 夕一 QPO			
	🗷 🏨 サイト			
	愛 クルーフ ポリシーのモデル(         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			
	<u>لا</u>			

ネットワークポリシーサーバーに割り当てるためのグループポリシーを作成します。

ドメインコントローラーにて「グループポリシー管理ツール」を起動します。
グループポリシーを新規に BoundaryPolicy という名前で作成します。







「籾証士は」両面で「ついピュータ			
' 認証力法」回由 (' コノビユーダ	■ 新規の接続セキュリティの規則ウィザード 認知に方注		
訨明書」を選択します。	規則に一致する接続に対して行なう認証方法を指定してください。		
「参照」ボタンをクリックしルート	ステップ		
	<ul> <li>規則の種類</li> </ul>	どの認識方法を使用しますか?	
CA を選択しま9。	● 要件	○ 既定(D)	
「正常性証明書のみを受け入れ	<ul> <li>認証方法</li> <li>ブロファイル</li> </ul>	プロファイルのプロパティで指定された認証方法を使用します。	
る」にチェックを入れ「次へ」をクリ	<ul> <li>名前</li> </ul>	(* コンピューダンモリーゲー(Montones VS)(C) ドメイバニを知いているユーザーとコンピューがから初期後に通信を範疇します。受信と送信 規則で特定のユーザーやコンピュータを承認するとき、ID 情報を提供します。	
ックします。		○ コンピュータ (Karberos VS)(O) ドメイルに参加しているコンピュータからの建築に)動きを制限します。受信と送信規則で特定のコンピュータを承認するとき、D 情報を提供します。	
		コンピュータ証明表(T)     この証明機関(CA) から発行された証明書を持つコンピュータからの接続に過信を制限しま     す。	
		CAの名前 DC=local DC=domain28.CN=domain28-DC01-CA 参照(R) ア 正常性証明書のあを受け入れる(H)	
		C 詳細設定(A) カスタムの1番目と2番目の認識設定を指定します。 カスタマイズ カスクマイズ	
		記録方法の詳細を表示します	
		く 戻る(B) 次へ(10) 年代ンセル	
「プロファイル」画面ですべての頂			
	新規の接続セキュリティの: プロコッイル。	規則ウィザ−ド 区	
目にチェックを入れ「次へ」をクリ	この規則が適用されるプロファイ	ルを指定してください。	
ックします。	ステップ		
	● 規則の種類	この規則はいつ適用しますか?	
	● 要件	E hi h m	
	<ul> <li>認証方法</li> <li>ゴロコイル</li> </ul>	▶ トメイン(D) コンピュータがその企業ドメインに接続しているときに適用されます。	
	<ul> <li>20000000</li> <li>名前</li> </ul>	▼ プライベート(P)	
		コンビューションジョイヘート ネットワーンの場所に接続しているときに適用されます。	
		コンピュータがパブリックネットワークの場所に接続しているときに適用されます。	
		2077イルの詳細を表示します (夏3(8) (次へのり) キャンフル	
「名前」画面で Boundary Rule と	* 私知の技体わた。113、の		
入力し「完了」ボタンをクリックしま	名前この規則の名前と説明を指定し	77(52%)	
<b>व</b> .	ステップ		
	<ul> <li>規則の種類</li> <li>更供</li> </ul>		
	· xiT • 認証方法	名前	
	לולדלםל	Boundary Rule	
	● 名前	説明 (オブション):	
		《戻&(B) 元(h) 并约包ル	



作成されたポリシーを	夏ダルーナポリシーの管理
	三 ファイル(F) 操作(A) 表示(V) ウィンドウ(W) ヘルヴ(H)
IPSec-Boundary 組織単位に割り	🗢 🔿 📩 💼 🖻 🖬
	IPSec-Boundary
白しまり。	□ A フォレスト domain28.local リンクされたグループ ポリシー オブジェクト グループ ポリシーの継承   委任
	<ul> <li>回 論 tomain28.local</li> <li>リンクの順序 (GPO)</li> <li>G#制 リンクの有効化 (GPOの状態 WML 74/)</li> </ul>
	📓 Default Domain 👌 1 🔊 BoundaryPolicy い はい 有効 なし
	BoundaryPol
	E IPSec-Secure
	SecurePolicy 7
	BoundaryPol
	Default Dom     Default Dom     Default Dom
	田 👺 WMI フィルタ
	= = = = <del>2 − − GPO</del>
	■ 91ト - ジリート ポリシーのモデルイ
	田 🚉 グループ ポリシーの結果

### 組織単位への移動

ドメインコントローラにて Active Directory ユーザーとコンピュータを開きます。 クライアントコンピュータを IPSec-Secure 組織単位に移動します。 ネットワークポリシーサーバー(NPS01)を IPSec-Boundary 組織単位に移動します。

### グループポリシーの適用

クライアント PC 及びネットワークポリシーサーバーで gpupdate /force コマンドを実行します。

以上ですべての設定が完了しました。



# 動作確認

本書の手順では、正常性検証ツールの設定として Windows ファイアウォールと自動更新を選択 しています。

IPSec を利用した NAP の場合、健全な状態では暗号化通信に利用する証明書が発行されます。 Windows ファイアウォールや自動更新が無効に設定されていると検疫ネットワークに隔離され ることになりますが、IPSec を利用した NAP の場合、実際には証明書が発行されず、IPSec での 暗号化通信が強制されているコンピュータとは通信ができなく、結果として隔離されたことにな ります。

本書の手順ではクライアント PC は IPSec を強制し、NPS は IPSec を要求はするが必須ではな いという設定です。また、DC に関しては何の制御も行っていません。よって、不健全な状態であ ってもクライアントから NPS や DC には通信することができますが、クライアント PC 同士の通信 は行えません。

正常な状態では以下の図のように各クライアントに証明書が発行されます。



この状態ならば DC01 はもちろん、NPS01 やクライアント PC 同士で通信が可能です。 ping コマンド等で通信状態を確認してください。

Windows ファイアウォールを無効にするとセキュリティポリシーに準拠していないと判断され証明書は自動的に削除されます。



<ul> <li>□ンソール1 - [コン!</li> <li>□アイル(F) 操作(</li> <li>(本) ● (タ) (ホ)</li> </ul>	ノール ルー A) 表示(	ト¥証明書 (ロー; V) お気に入り(	カル コンピュータ)¥個人¥証明 (0) ウィンドウ(W) ヘルプ	書] (H)	- 8 x
	発行先	್ このビューにま	発行者 表示する項目はありません。		<mark>操作</mark> 証明書 ▲ 他の操作 →
✓ III → ストア個人には1個の	< 正明書があ	 ります。		•	

この状態ではクライアント PC 同士の通信はできません。ping コマンド等で確認してください。 しかし、NPS01 には通信できます。ですからクライアントが修復され、セキュリティポリシーに準 拠するようになれば、再度証明書を要求し、発行してもらう事が可能です。

自動修復が有効な状態では、Windows ファイアウォールを無効にしただけでは、即時に有効に 変更されます。



# おわりに

ここまで見てきたように、Network Access Protection(NAP)を利用すると、セキュリティレベルの 低いマシンを社内 LAN から分離し、全社的なレベルを維持することができます。

NAP には様々な構成方法がありますが、本書で取り上げた IPSec 構成は通信そのものを暗号 化する方法であり、通信を傍受されたとしても解読できないというセキュリティレベルの高い構 成です。

ただ、IPSec 構成ではポリシーを適用する範囲を適切に設定しないと正しく通信できなくなる恐 れがあります。守るべきものと守らなくてもいいものを明確にし、ネットワーク全体を意識した設 定を検討する必要があります。

NAP にはいくつかの方式があります。本書で取り上げた IPSec の方式も含め、「とりあえずは DHCP で、順次 802.1X に」という段階導入も考慮、検討してください。

Windows Server 2008 のグループポリシーでは IPSec の設定と Windows ファイアウォールの設 定が統合されました。本書では動作確認のために Windows ファイアウォールを OFF にする都合 上 IPSec のみを有効にしていますが、実環境では Windows ファイアウォールもポリシーで制御 することが多くなると思います。このあたりも検討してください。

平成 20 年 2 月作成

伊藤忠テクノソリューションズ株式会社 IT エンジニアリング室 プラットフォーム技術部 Windows 技術課

