





伊藤忠テクノソリューションズ株式会社



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 製品候補版(RC0 及び RC1)に関する様々な検証をもとに記述したものです。製品化前の 段階での検証であり、製品出荷時に仕様が変更になり、本書の内容と相違が発生する可 能性があります。

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。





目 次

はじめに	
Network Access Protection とは	2
DHCP 構成	2
テスト環境	
テスト環境論理図	
環境作成手順	
ドメインコントローラの作成	
NPS のインストールと構成	5
概要	5
Windows Server 2008 RC1 のインストール	5
NPSとDHCPの役割のインストール	
役割の追加ウィザード	
DHCP サービスの構成	
ネットワークポリシーサーバーの設定	11
AD への登録	
クライアントの設定	14
動作確認	
おわりに	
付録 NPSとDHCPの分離構成	
インストール手順	
NAP 構成ウィザード	
DHCP サーバーの設定	
RADIUS Proxy の設定	



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 に関する検証を製品候補版(RC0 及び RC1)を利用して実施しました。

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。

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 DHCP 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、DHCP 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、DHCP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 DHCP 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 RC1 (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 RC1 (x64)を指します。





Network Access Protection とは

Network Access Protection(NAP)は Microsoft の次期 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

本書では一番手軽に導入できるであろう DHCP を利用した NAP を実現するための手順を扱い ます。

DHCP 構成

DHCP を利用して NAP を構成する場合、DHCP サーバーがクライアントの状態に応じて IP アドレスとサブネットマスクの組み合わせ、さらに静的ルーティングを利用して、修復サーバー以外には接続できないように制御します。

VLANのようにサブネットを変更するわけではなく、静的ルーティングを利用して接続できるサーバーを制御します。

Windows Server 2008 だけあれば構成することができ、他のネットワーク機器等に依存しないため、NAPの基本的な動作を確認する際に役に立ちます。

ネットワークポリシーサーバー(NPS)と DHCP サーバーは分離することも可能ですが、本書では より構築が容易な同居構成の手順を示します。 (分離構成の手順は付録に記載)

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3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 RC1 が動作している LH01 を使用します。LH01 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 RC1 が動作している LH02 を使用します。LH02 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。

DHCP サービス

NPS 用の LH02 に DHCP サービスを同居させます。 NAP 用の DHCP サービスは Windows Server 2008 で構築する必要があります。

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、DHCP クライアントと 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

LH01 に Windows Server 2008 RC1 をインストールして次の役割を与えます。 Win2008.local という Active Directory のドメインコントローラ Win2008.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 RC1 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) 必要に応じて Active Directory でユーザー作成や、GPO を構成する

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。



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 RC1 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 RC1 をインストールする TCP/IP の構成を行う win2008.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 DHCP サービスをインストールする DHCP 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 RC1 のインストール

コンピュータの電源を入れ Windows Server 2008 Enterprise Edition RC1 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。

win2008.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 と DHCP の役割のインストール

NPSとDHCPの役割をLH02にインストールします。

NPSとDHCP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

「Start」をクリックして「管理ツー	1 0 d. 23 de		
ル」-「サーバーマネージャー」を	2H(A(2) 101(A) AT(2) AA7(3)	9 it	
記動します。		- パー マネージャ (LH02)	
	H D D D D D D D D D D D D D D D D D D D	507-//-00380480494. #LE09849330497. 7-//-0038748800	anaeciananerik var.
	1	9-K-048	1 7-/5-00RAN7
		③ コンピュータ毎報 75 コンピュータ& U402 wieQ008.bcal	(第 システム プロパラ «の定更) (型 ネットワーク接続の表示)
		P.54()/ we2000.local n=his_tryPlane_2 192160.202 (hist dath)	100 19E-1- 97201-970484
		リモート ダスクトック 和助	
	1 1	70595 ID 78441-002-6100211-70061 「 05が146にのエバーホをあ示しない(2)	
			Windows 7r (P?s=50@3
	1 1	Windows 7+179+16 和助 Windows Update 单键版	49 \$14,492509240985
		東新プログラムの最終端回日時 なし 実新プログラムの最終インストール日 なし	THE R ESC ONLY
	1 1	1月 E セキュッティ語(2の用AL (ESC) 登録者につりして自た5 コーポージェアン アルマト	
		Diade	DOMMERS
		■ B23 0/7 (B±(>2)	D-039-040 +1
	0	ANDING CONTRACTOR SOLES IN ALTER A	● 人般 🍽 🍜 😖 🛄 :
「役割の概要」を展開して「役割	L9-1-72-9+		.D.X
の追加」をクリックします。「次	- 2+(4位) 10(1(4) 単元(3) へルス(4) ◆ 10) 20 111 日	0	
へ」をクリックします。	= 0-0(- ∀20+0.H02) (7) = 0 001 = 0 001		
	10 10 10 10 10 10 10 10 10 10 10 10 10 1	ターバーにインストールされているの意味な正常なも示し、の意作機能を追加または非常い。	t7.
	10	R2648	R 030084.57
		● 森林 0.77 保トインストール(薬)	ille regenerate
	1		Pa .
	1		
	1		
	1		
	1		
	1 1		
	1 1		
	a	NBORSO-SIMPARE SORE INVOLVES BRITE	1 45 KD 10 10 10 10 10 10 10 10 10 10 10 10 10
			• A 102 • • • • • •
「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」をクリックします	🔛 開始する前に		
	4.2 1		
	開始する前に サーバーの役割	このワイサードを使用すると、このサーバーに投動をインストールでき するなどこのサーバーで実行するタスクに応じて、インストールする行	はす。ドキュメントを共有する、Web サイトをホスト は割を決定します。
	· 1012	統行する新に、次のことを確認としてくたさい。 ・管理者アカウンドに強力なパスワードが設定されていること	
	結果	 動的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こと Windows Update から最新のセキュリティ更新プログラムがインス 	ちールされていること %
		これらのいずれかの染件を満たしていない場合は、ウィザードを取 度実行していたとい。	が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大ヘ」をクリックしてください。	
		厂 既定でこのページを表示しない(S)	
		catern II a	n(N)) ///Zh=n/p tonsition
		CIRCUP.	10/10/10/14/20



「サーバーの役割の選択」ペー 役割の追加ウィザート 🙀 サーバーの役割の選択 ジが開くので「DHCP サーバー」 と「ネットワークポリシーとアクセ 開始する前に このサーバーにインストールする役割後 1 つ以上選択します。 役割(B) は Pio う Vieto、 サーバーの役割 ネットワーク ポリシーとアクセス サービー 役割サーム スサービス」にチェックを入れて NED: Active Directory Rights Management サービス Active Directory ドメイン サービス Active Directory フォブレーション サービス Active Directory ジャーション サービス Active Directory ジャージス Directory 正明書サービス 1895 動的大人と構成プロトロル(OHCP)サー 人」を使用すると、グライアントコンピュー グ用の一時的な IP アドレスおよび関連 情報を一元的に構成、管理、および理 (目で表す。 「次へ」をクリックします HCP サ ネットワーク接続バインディ IPv4 DNS I的定 IPv4 WINS IRTE DNS サーバー FAX サーバー UDDI サービス Web サーバー (IIS) Windows SharePoi R DHCP 23 DHOPV6 Jモートレス モード IPv6 DNS 設定 Web サーバー (LEs) Windows SharePoint S Windows 展開サービス アプリケーション サーバー ターミナル サービス int Services DHOP サーバーの承担 1912 ターミナル サービ ネットワーク ポリ ファイル サービス 印刷サービス ーとアクセス サービス 進行状況 結果 サーバーの没来の詳細 <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。 役割の追加ウィザード 「役割サービスの選択」ページ 後割サービスの選択 で「ネットワークポリシーサーバ ー」にチェックを入れます。「次 キットワーク ポリシーとアクセス サービス にインスト (注射サービス(E) - スタリタークホッリンーサーズ。 - パー・ティングシリシート アクセス サービス - ジェート アクセス サービス - 正式計算者を確認 - HCAP (Host Credential Authorization Pr 開始する約に ・「京割サービスを選択 サーバーの役割 ネットワーク ポリシーとアクセス サービー へ」をクリックします。 100円 あり<u>ワーク ポリン・サーバー(IFE)</u>を 使用すなど、ウイアントの正常性、種 の業界本の記述は、種植業界でからいとし、 する結構主体のネットワークアウセス。本 リン・書作杯およりは事創でを含まった。 NPS では、ネットワーン、アンセス体験 個できます。 個できます。 役割サービス DHCP サーバー ネットワーク接続バインディング ネットワーク課題/パンディング IPv4 DNS 設定 IPv4 WIN5 設定 DHOP スコープ DHOPv6 ステートレス モード IPv6 DNS 設定 tial Authorization Pro DHCP サーバーの承認 確認 進行状況 結果 役割サービスの詳細 く前へ(P) 次へ(N)> インストール(D) キャンセル 「DHCP サーバー」に関する説明が表示されます。「次へ」をクリックします。 役割の追加ウィザード 「ネットワーク接続バインディン ネットワーク接続バインディングの選択 グの選択」ページで DHCP サー ビスのために使用するネットワ 開始する前に 動約 IP アドレスを持つネットワーク接続が 1 ついしと検出送れました。1 つのネットワーク接続は、1 つの分離さ れたサブネット上にある DHOP クライアントにサービスを提供するために使用できます。 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 ーク接続が持つ「IP アドレス」を この DHOP サーバーでクライアントへのサービス提供のために使用するネットワーク接続を選択してください。 選択して「次へ」をクリックしま 役割サービス DHCP サーバー ネットワーク接続(<u>6)</u> IP アドレス IP 192168282 種類 す。 ネットワーク接続 IPv4 DNS IRE IPv4 WING RE DHCP 23-7 DHCPv6 ステートレス モード IPv6 DNS L的定 DHOP サーバーの承担 12177 递行状况 纪果 ITIE ローカル エリア接続 2 Broadcom BCM5700C NetXfreme II GigE (NDIS VBD クラ イアント) む 名前: ネットワーク アダプタ 00-1C-C4-BC-DB-94 物理アドレス <約へ(P) 法へ(N) インストール(D) キャンセル



「IPv4 DNS サーバー設定の指 定」ページで親ドメインボックス	の我の2007/7-1	
に「win2008.local」、優先 DNS サ ーバーボックスに IP アドレスを 入力して「次へ」をクリックしま す。入力が終わったら「検証」ボ タンをクリックして「有効」と表示 されたら「次へ」をクリックしま す。	間始する前に サーバーの役割 ネットワークカリンーとアクセスサーと- (役割サーセス) DHCP サーバー ネットワーク時代(インディング Pr4 VBG 設定 DHCP カーブー DHCP カーブー DHCP カーブーの単位 HHCP スコージ UHCP ガーバーの単位 MHCP MHCP MHCP MHCP	クタイアンドボッスをDACは サーバーがたが同様する際。DAS サーバーの PT アドレスト欄 ドインをおどの DACF オンシュルをクイアンドに 接続できます。ここで有意した気を加え、このドメインは、この DACP サーバーCPH 35 マイアントで その新潟を12 (明1978) F A インの名前 物面 定して たまか、このドメインは、この DACP サーバーCPH 35 (明 F A イン2) PP イク20 Recall PP イク20 Recall クタイアント ドロクス (新潟に) (明 F R 2 C OA) PP インクション (日本) PP インクシ
		<前へ(2) 次へ(3) 32ストール(3) キャンセル
IPv4 WINS サーハー設定の指 定 ページで「このネットワーク	1231の30109ィザード IPv4 WINS サー	「一設定の指定
上のアプリケーションに WINS は 必要ない」が選択されているの を確認して、「次へ」をクリックし ます。	開始する新に サーバーの原料 ネットワークス 利少っとアクセス サービュ 没まサービス したい サーバー ネットワーク 利約・大学 ハング でん DNS 設定 ロイトロ スコープ DNG DNG スコープ DNG DNG スコープ DNG DNG スコープ DNG DNG スコードス モード HP-G DNS 設定 DNG TP サーバーの承担 ME2 通行 状況 表示	クライアンドボル アドレスを DHCP サーバーから取得する際、WINS サーバーの IP アドレスなどの DHCP オブジョ >を3075アンド 通信できます。ここで 指定 ULA 該定は IF 4 を使用するクライアンドに 通用されます。 「 このキットワーク上のアガリケーシェンに WINS は 必要ない VLA 「 このキットワーク上のアガリケーションに WINS は 必要ない VLA 「 このキットワーク上のアガリケーションに WINS が 必要(5) クティアンドンドを構成されます。これらの WINS サーバーの IP アドレス指定によす。これらの WINS サーバーの IC 2000 (人気 WINS サーバーの IP アドレス(D) 「 「 WINS サーバーの IP アドレス(D)
		<u> WDS: 9-17-18-00 (260</u>
		<第への (X(30) - パンストーバロ (キャンセル)
「DHCP スコープの追加または編集	 しページが表示	
「スコープの追加」ダイアログが	入コープの追加	×
表示されるので、スコープ名、 開始 IP アドレス、終了 IP アドレ ス、サブネットマスクを入力して (デフォルトゲートウェイはオプ ション)サブネットの種類を確認 したら、「OK」をクリックします。	スコープとは、ネットワークで使用可能 DHGP サーバーは PP アドレスを少す スコープを(G) 間応 PP ドレス(D) 終了 PP ドレス(D) サブネット マスス(U) デフォルト サードウォイ (オブッルンX(D) サブネットの機能(B) 「2 このスコープをアウライブ化する(A)	な P アドレスの範囲です。20-7月9時だれるまで、 アント 記載 時 など D できません。 「 フイヤード(物語 - リース制物1 6 日) ・ OK キャンセル
入力したスコープが反映されて	役割の追加ウィザード	×
いれは、「次へ」をクリックしま す。	DHCP 73-70)	色加または編集
	間時する前に サーバーの22割 ネットワーク用ジーとアクセスサーと- 投影サービス Dice サーバー ネットワーク接続以インディング IP-4 DIS 語定 DISP 201-27 DifCPA 27-1-12 モード IP-4 DIS 語定 DISP 201-7 DifCPA 27-1-12 モード IP-4 DIS 語言	スコープないおからつって使用可能なと思うを見いたの解剖です。スコープが1985を13.56で、DHOP ゲーバーは サアドバスを行うたいただ用するととかできない。 スコープない 「のゆ 192100.201 - 192100.20254 ほぼ(ど) よりかくの してい うり フロパライ スコープを追加めたは違訳すると、そのスコープのプロパラィが表示されます。
		<u>~</u>





以上で NPS と DHCP がインストールされました。



DHCP サービスの構成

NAP を使用するため必要な設定を DHCP サービスに対して行います。

スタートをクリックして「管理ツール	」「DHCP」をクリックします。
「DHCP」コンソールが開いたら、 「LH02.win2008.local」を展開して 次に「IPv4」を展開します。 スコープを右クリックして「プロパ ティ」をクリックします。 「スコープのプロパティ」が表示 されたら「ネットワークアクセス 保護」タブを開いて、「ネットワー クアクセス保護設定」の項目か ら「このスコープに対して有効に する」を選択し「既定のネットワ ークアクセス保護プロファイル」 を選択して「OK」をクリックして 画面を閉じます。	スコープ【192.168.280.0] пар.0711/57 21× 全般 DNS ネットワーク アクセス/保護 ここでは、このスコープに対するネットワーク アクセス/保護設定をセットアップできます。 ネットワーク アクセス/保護設定 ・ このスコープに対して不効にする(N) ・ 既定のネットワーク アクセス/保護設定 ・ のスコープに対して不効にする(N) ・ 既定のネットワーク アクセス/保護対応 ・ ごのスコープに対して不効にする(N) ・ このスコープに対して無効にする(P) ・ このスコープに対して無効にする(P) ・ このスコープに対して無効にする(P) ・ このスコープに対して無効にする(P)
スコープオプションに「既定のネット 「スコープオプション」を右クリックし	>ワークアクセス保護クラス」を追加します。 ♪て「オプションの構成」をクリックします。
「スコープオプション」の画面が 表示されたら「詳細設定」タブを 開いて「ユーザークラス」で「既 定のネットワークアクセス保護ク ラス」を選択します。 「006 DNS サーバー」にチェック を入れ、データ入力の欄にドメイ ンコントローラ(DNS)の IP アドレ スを入力します。	スコープ オブジョン 空 メ ズ 金秋 詳細記定 ペンダ クラス(い): DHCP 標準オブジョン ユーザー クラス(U): 既定のネットワーク アクセス保護クラス 1月時可能なオブジョン マ 1月時可能なオブジョン マ 1000 DNS サーバー ホーム サーバー 1000 DNS サーバー ホーム サーバー 1000 DNS サーバー ボークラーアドマ 1010 DNS サーバー ボークラーアドマ 102 DNS サーバー ボークサーバー 102 DNS サーバー ボーク・ 102 DNS サーバー ボーク・ 102 DNS サーバー ボーク・ 102 DNS サーバー ボーク・ 102 DNS ローバー ボーク・ 102 DNS ローバー
「015 DNSドメイン名」にチェック を入れて、データ入力の欄に文 字 列 と し て 「restricted.win2008.local」を入 力します。	スコーナ オナション 21 × 金統 詳細設定 ペンダ クラス(い): DHCP 標準オプション ユーザー クラス(U): (既定のネットワーク アクセス保護クラス、マ 副用可能なオプション 1014 メリット ダンプ ファイル 〇のち DNS ドメイン名 クライアント解マー 〇のち DNS ドメイン名 クライアント解マー マニマニ キ *** ・ データ入力 ・ アデータ入力 ・ 「restricted win2008 local ・
入力が完了したら、「OK」をクリック	して画面を閉じます。

これで、DHCP サーバーの設定は完了です。



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

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。			
「ネットワークポリシーサーバー」の)コンソールが開いたら「NAP(ローカル)」をクリックしま		
す。			
右ペインで「ネットワークアクセス保	護(NAP)を選択し、「NAP を構成する」をクリックしウィザ		
ードを起動します			
「NAP で使用するネットワーク接	NAP を構成する		
続方法の選択」ページが開いた	NAP で使用するネットワーク接続方法の選択		
ら、「ネットワーク接続の方法」で			
プルダウンから「動的ホスト構成			
プロトコル (DHCP)を選択しま	イッチワーン構成の力が。 NAF 対応で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) 作成されたポリシーはこのネ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		
す。「ポリシー名」には自動的に	するには、ウィザードを再度実行してください。		
「NAP DHCP」が入ります 「次	動的ホスト構成プロトコル (DHCP)		
ヘッタクリックします	ポリシー名: このウィ <u>サードで作</u> 氏され <u>るポリシー</u> には、下記の文字列が名前の一部として使用されます(T)		
.]27770878	このまま使用することも、変更することもできます。 NAP DHCPI		
	NAP をごやたかシックるには、1回加切アクションを実行する必要かめります。下のリンクをクリックして、1回加切 NAP 要当を表示してださい。 当つの思想(1))		
「DHCP サーバーサービスを実行す	る NAP 強制サーバーの指定」ページでは特に何も設定		
せず、「次へ」をクリックします。			
「DHCP スコープの指定」ページでは、今回特に設定を行わないので、「次へ」をクリックしま			
す。			
「ユーザーグループとコンピュータク	「ループの構成」ページでも、今回特に設定を行わないの		
で、「次へ」をクリックします。			
「NAP 修復サーバーグループおよび URL の指定」ページでも今回特に設定を行わないの			
で、「次へ」をクリックします。			





ウィザードが完了し、6つのポリシーが作成されました。

正常性ポリシー

NAP DHCP 準拠

NAP DHCP 非準拠

接続要求ポリシー

NAP DHCP

- ネットワークポリシー
 - NAP DHCP 準拠
 - NAP DHCP 非準拠
 - NAP DHCP 未対応

セキュリティ正常性検証ツールの設定



「ネットワークポリシーサーバ ー」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。	
「Windows セキュリティ正常性検証 をクリックします。 「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。	
をクリックしてダイアログを閉じます	(夜証) — ルックロバ (1) のタイ / ログに戻るので、 (0K) - 。

「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

最後に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。



「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。

これで一通り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。また、自動修復のオプションも有効になっています。

よって、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とし て隔離され、自動修復された後に通常のネットワークに接続されます。

正常な状態では ipconfig の結果は以下のとおりです。

画 管理者: コマンド プロンプト	<u> </u>
C:¥Users¥Administrator>ipconfig	
Windows IP 構成	
イーサネット アダブタ ローカル エリア接続: 接続固有の DNS サフィックス : win2008.local IPv4 アドレス : 192.168.28.100 サブネット マスク : 255.255.255.0 デフォルト ゲートウェイ	
Tunnel adapter ローカル エリア接続* 6:	
接続固有の DNS サフィックス : win2008.local リンクローカル IPv6 アドレス : fe80::5efe:192.168.28.100%10 デフォルト ゲートウェイ :	
C:¥Users¥Administrator>	
	_

Windowsファイアウォールを無効にした場合、ポリシーに合致しないと判断され、検疫ネットワークに隔離されます。

その状態で ipconfig を実行すると、以下のようになります。

■ 管理者: コマンド プロンプト	- 🗆 🗙
Microsoft Windows [Version 6.0.6000] Copyright (c) 2006 Microsoft Corporation. All rights reserved.	<u>^</u>
C:¥Users¥Administrator>ipconfig	
Windows IP 構成	
イーサネット アダブタ ローカル エリア接続:	
接続固有の DNS サフィックス : restricted.win2008.local IPv4 アドレス : 182.168.28.100 サブネット マスク : 255.255.255.255 デフォルト ゲートウェイ :	
Tunnel adapter ローカル エリア接続* 9:	
接続固有の DNS サフィックス : restricted.win2008.local リンクローカル IPv6 アドレス : fe80::5efe:192.168.28.100%18 デフォルト ゲートウェイ :	
C:¥Users¥Administrator>	
	-

サブネットマスクが 255.255.255 となっています。

これにより、自分以外のマシンとはそのままでは通信できない状態です。

この状態では修復サーバーへの静的ルートのみが設定されており、必要に応じてウィルスのパ



ターンファイルを更新したり、Windows Update でパッチを最新にすることができます。

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 DHCP 構成が最も導入が容易で、 入門編とも言える構成です。

ただ、DHCP 構成には限界があるのも事実ですので、他の方式への移行も検討する必要があります。

NAP の場合は他の方式への移行もスムーズに行えるため、「とりあえずは DHCP で、順次 802.1X に」という段階導入も可能です。

そのあたりも実環境への展開時には考慮、検討してください。

平成 20 年 1 月 作成 平成 20 年 2 月 改訂

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





付録 NPSとDHCPの分離構成

ここでは NPS と DHCP を別筐体で運用するための手順を示します。

分離構成と言っても完全には分離できません。認証を行うNPSとDHCPは分離できるのですが、 DHCP だけでは NPS に認証要求を渡せません。そこで、DHCP サーバーに NPS をインストール し、RADIUS Proxy として NPS に要求を転送するように設定します。

インストール手順

LH02 が NPS、LH03 が DHCP という環境の場合の手順は以下の通りです。

LH02 に NPS をインストール NAP 構成ウィザードでポリシーを作成 LH03 に NPS と DHCP をインストール DHCP を設定 LH03 の NPS で転送用の接続要求ポリシーを作成

インストールそのものは同居構成の時と同じです。ただ、LH02 では NPS のみを選択し、LH03 で NPS と DHCP の 2 つを選択するという点だけ注意してください。



ウィザードの中の「DHCP サー バーサービスを実行する NAP 強制サーバーの指定」ページで RADIUS クライアントとして LH03 を定義します。	NAP を構成する 区 DHCP サーパー を実行する NAP 強制サーパーの指定 Participation 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 コンピュータではありません。ローカル コンピュータで DHCP サーバーを実行している場合、この手順を省略して けべいを オーバーのではあっますべての リモート DHCP サーバーを NADUS クライアントとにき知ってんに、自知の をグリックします。追加するすべての リモート DHCP サーバーを NAPUS ウライアントとにきかります。そのに、PHC や DHCP NE サーバーであ、	
	前へ(2) 	



DHCP サーバーの IP アドレスと 共有シークレットを入力します。	新規 RADIUS クライアント
作成された PNDUS クライマント	
のプロパティを開き、「RADIUS	LH08のプロパ ラ 7 × ×
クライアントが NAP に対応して	☞ この RADIUS クライアントを有効にする(E)
いる」をチェックします。	フレンドリ名(E): [LH03 アドレス (IP または DNSX(D): [1921662283 ・ 力能対応 RADIUS グライアント用の RADIUS 標準を指定するか、一覧から RADIUS グラ イアント ペンダ名選択してください。 ペンダ名(M): [RADIUS Standard] ・ ・ 共有シークリットを直接入力する場合は (手動) をリックし、自動で生成する場合は (生成) をジョンはます。ここに指定に共有シークレットや名、RADIUS グライアントが RADIES (14年前) をジークレットの違いた式中シークレットでは大文字を小文字が区別されます。 ・ ・ <t< th=""></t<>

DHCP サーバーの設定

DHCP サーバーの設定は同居構成と全く同じです。

RADIUS Proxy の設定

LH03の NPSの設定で LH02 へ要求を転送するための設定を行います。

「リモート RADIUS サーバーグル ープ」を新規に作成します。	新し(リモート RADIUS サーバー グループ グループ名(G): RADIUS サーバー: RADIUS サーバー: 像先順位 重み	▶ 3唐如(O) 新課集(E) 肖印即代(R)
	ОК	**>セル



IP アトレスを週切に入力しま	RADIUS サーバーの追加
」す。	
	アドレス 認証/アカウンティング 負荷分散
	追加する RADIUS サーバーの名前または IP アドレスを入力してください。
	++, 17, 7°%
	192168282
	OK キャンセル 適用(A)
「認証/アカウンティング」タブに	
て NAP 構成ウィザードを実行し	RADIUS サーバーの追加 X
	アドレス認証/アカウンティング 負荷分散
に除に入力したのと向し共有シ	記録本一ト(U): 1812
ークレットを入力します。	共有シークレット(S): *******
	共有シークレットの確認入力(C): ########
	□ 要求はメッセージ認証属性を含んでいる必要がある(R)
	アカウノイング アカウトティング ボート(T) 1913
	I State C / JF J J 1 J 5 (C) = 0 (J + 1 / J + 1 /
	共有シークレット(H):
	共有シークレットの確認入力(0):
	▼ ネットワーク アクセス サーバーの開始と/停止の通知をこのサーバーに転送する(F)
	OK キャンセル 適用(A)
「按续两步步心。」去乾坤に作	新しい接続要求ポリシー X
「技術安水小リンー」を新規に作	接続要求ポリシー名と接続の種類の指定
成します。	接続要求ポリシーの名前およびポリシーを追用する接続の種類を指定できます。
	ポリシー名(A): Proxid
	* ネットワーク接続の方法
	NPS に構築要求を逆信するネットワーク アクセス サーバーの種類を選択してください。ネットワーク アクセス サーバーの種類を選択するか、 [へこが因素]を指定することができます。
	ネットワークアクセスサーバーの種類(S): ホーバーの種類(S): ホーパーの種類(S): ホーパーの ホーの
	Unspecified
	○ へび週期(V):
	前へ(?) 次へ(N) 完了(?) 年+2-世ル
すべての要求を転送するだけたの	で ネットワークアクセスサーバーの種類け指定する必要
フ ヽこい女小で和心りのにいるい	マンドション ノノノンピハン ハ の性友は旧たりの必女
かめりません。	





これで分離構成での設定は完了です。 同居構成と同様の動作確認を行ってください。

