



Challenging Tomorrow's Changes

Windows Server 2008

NAP 設定手順書 IPsec 編

～テスト環境での IPsec NAP の強制～



Windows Server® 2008

伊藤忠テクノソリューションズ株式会社

目 次

はじめに.....	1
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	3
ドメインコントローラの作成.....	4
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.....	8
デフォルトドメインポリシーの編集.....	8
自動登録設定	8
NPS のインストールと構成	10
概要	10
Windows Server 2008 のインストール	10
NPS の役割のインストール	11
役割の追加ウィザード	11
下位 CA の構成.....	18
正常性登録機関の設定	19
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	25
組織単位への移動.....	30
グループポリシーの適用	30
動作確認.....	31
おわりに.....	33

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る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。

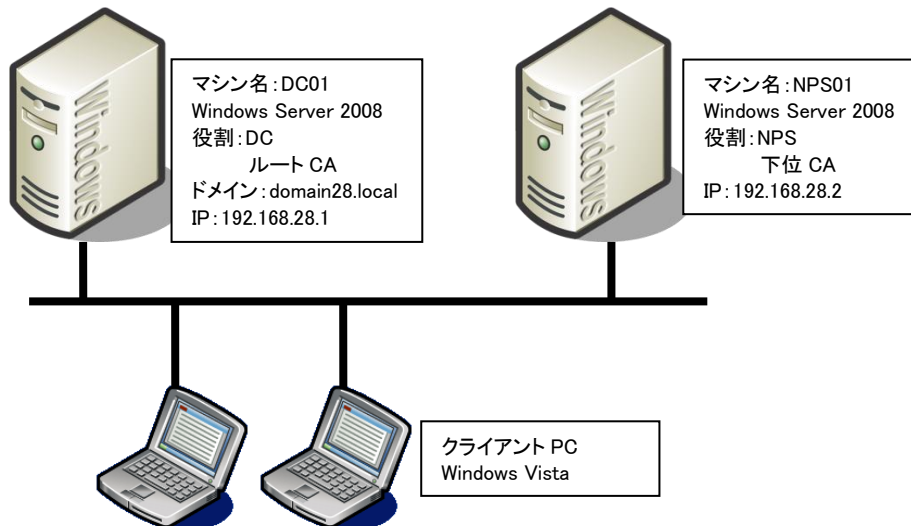
その他の方法に関してはそれぞれの設定手順書を参照してください。

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

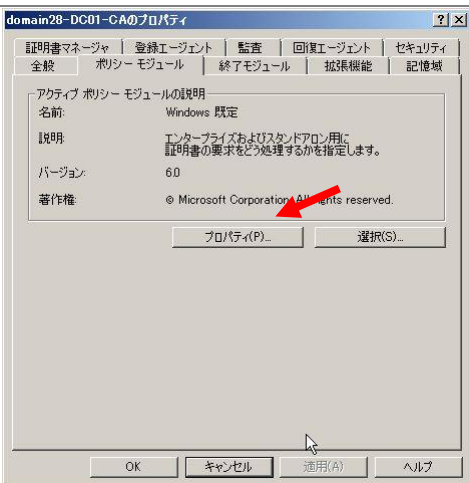

- NPS01 をメンバとするためのグループを作成します。
- NPS01 がドメインに参加した段階でこのグループのメンバに追加します。

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

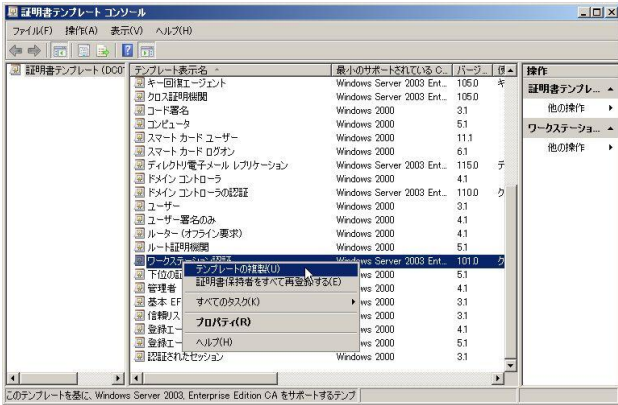
<p>「スタート」-「管理ツール」-「証明機関」を選択し証明機関コンソールを開きます。</p>	
<p>CA 名を右クリックし「プロパティ」を表示します。</p>	
<p>「ポリシーモジュール」タブを選択します。 「プロパティ」ボタンをクリックします。</p>	
<p>「証明書テンプレートに操作が設定されている場合はそれに従い、・・・」を選択し「OK」ボタンをクリックします。</p>	

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。

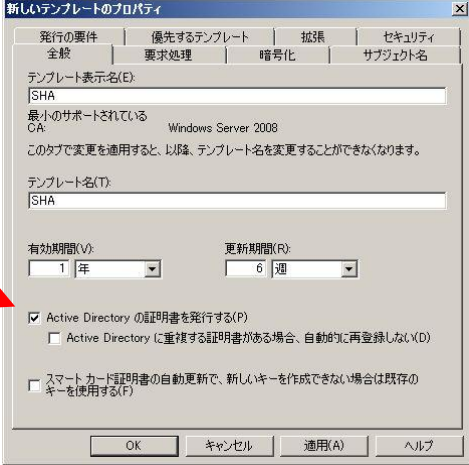
証明書テンプレートコンソールで「ワークステーションの認証」を右クリックし「テンプレートの複製」をクリックします。



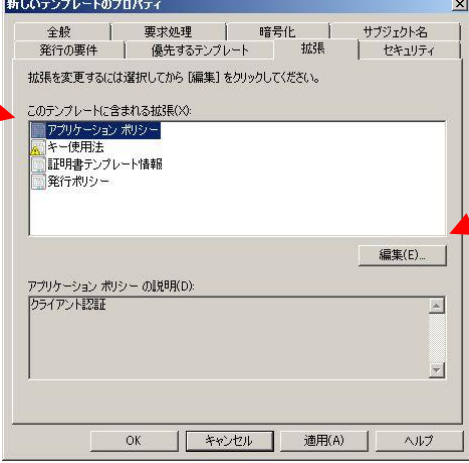
「テンプレートの複製」画面で「Windows Server 2008 Enterprise Edition」を選択し「OK」ボタンをクリックします。




「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。



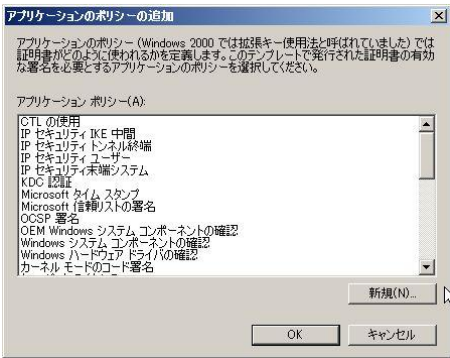
「拡張」タブにて「アプリケーションポリシー」を選択し「編集」ボタンをクリックします。




「アプリケーションポリシーの拡張の編集」画面で「追加」ボタンをクリックします。



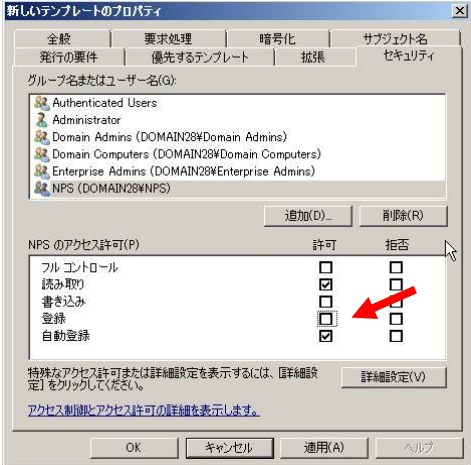
「アプリケーションポリシーの追加」画面で「新規」ボタンをクリックします。



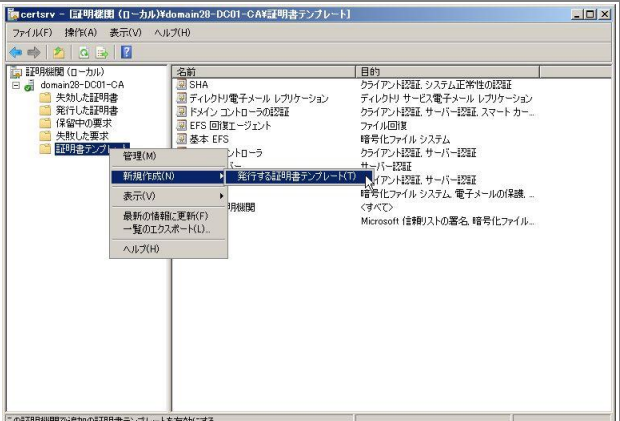
「新しいアプリケーションのポリシー」画面で名前を入力(ここでは "SHA")し、オブジェクトの識別子に "1.3.6.1.4.1.311.47.1.1" を入力します。何回か「OK」をクリックしテンプレートのプロパティ画面に戻ります。



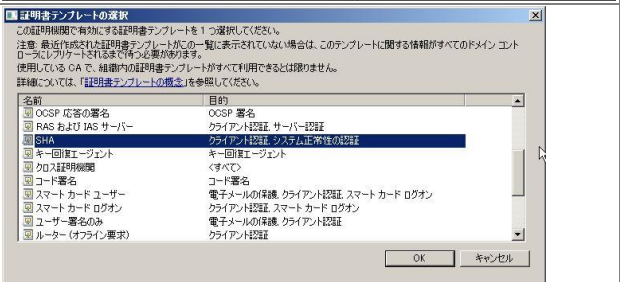
「セキュリティ」タブにて NPS01(NPS)をメンバーとするグループを追加し、「自動登録」の許可を与える。「OK」をクリック「新しいテンプレートのプロパティ」画面を閉じ、「証明書テンプレートコンソール」画面を閉じます。



証明機関コンソールにて「証明書テンプレート」を右クリックし、「新規作成」→「発行する証明書テンプレート」をクリックします。



先程複製したテンプレート(ここでは SHA)を選択し「OK」をクリックします。



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

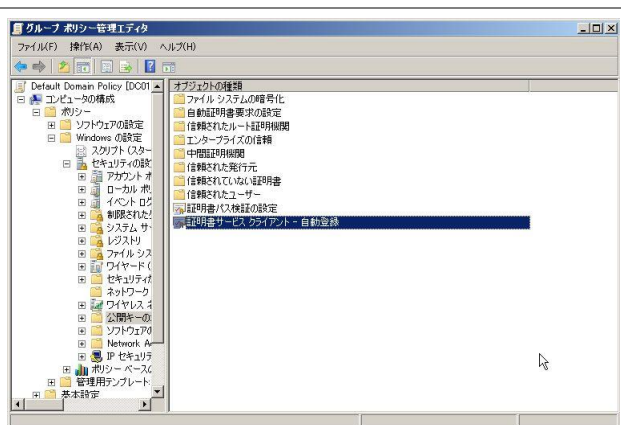
デフォルトドメインポリシーの編集

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。

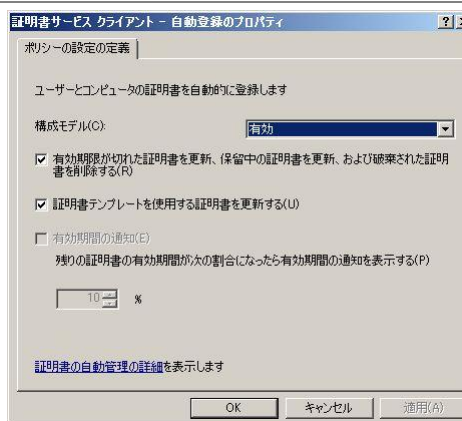
自動登録設定

「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。

「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」-「公開キーのポリシー」を開きます。
右ペインで「証明書サービスクライアント-自動登録」をダブルクリックします。



構成モデル: 有効
「有効期限が...」ON
「証明書テンプレート...」ON



「OK」をクリックしてデフォルトドメインポリシーの編集を終了します。

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。

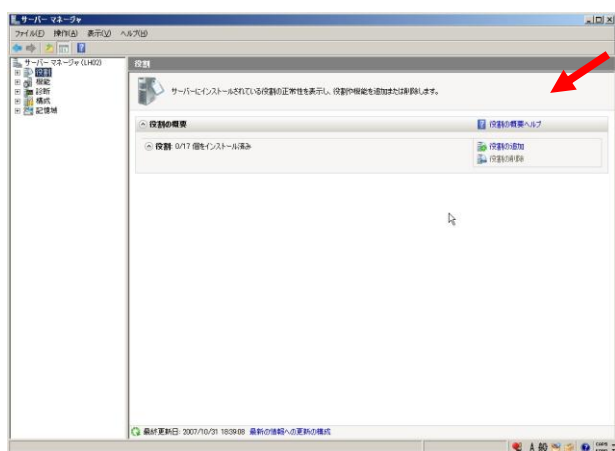
NPS と CA は別々にインストールすることも可能ですが、本書では同時にインストールする手順を示します。

役割の追加ウィザード

「スタート」をクリックして「管理ツール」-「サーバーマネージャー」を起動します。



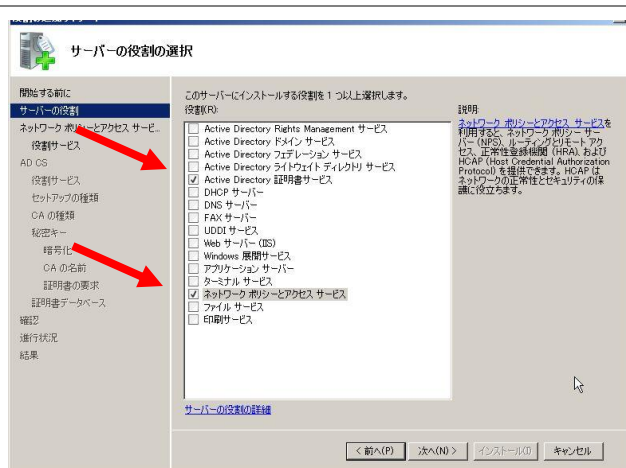
「役割の概要」を展開して「役割の追加」をクリックします。「次へ」をクリックします。



「役割の追加ウィザード」が起動するので「次へ」をクリックします

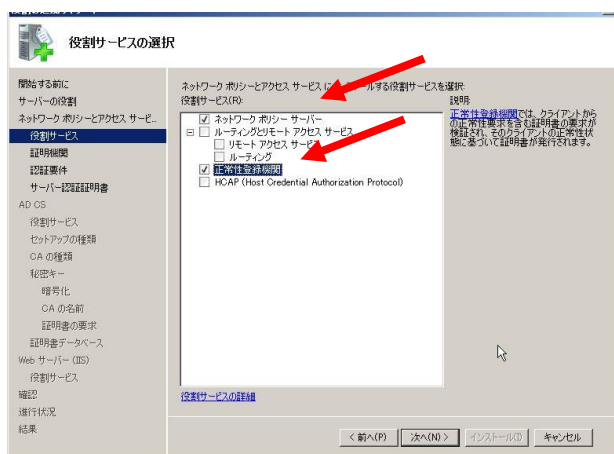


「サーバーの役割の選択」ページが開くので「Active Directory 証明書サービス」と「ネットワークポリシーとアクセスサービス」にチェックを入れて「次へ」をクリックします



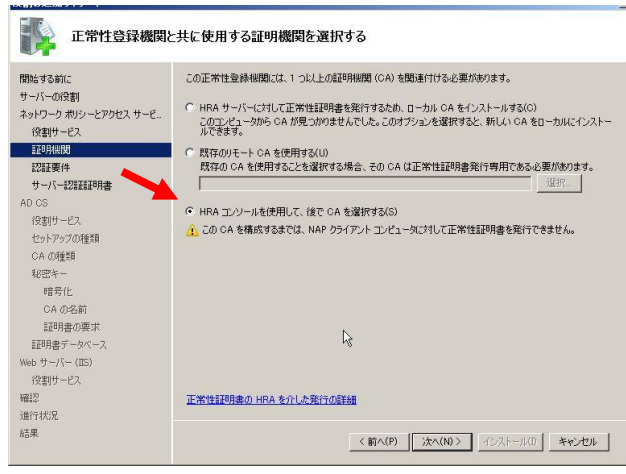
「ネットワークポリシーとアクセスサービス」に関する説明が表示されます。「次へ」をクリックします。

「役割サービスの選択」ページで「ネットワークポリシーサーバー」と「正常性登録機関」にチェックを入れます。「次へ」をクリックします。



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 CA を選択する」を選択して「次へ」をクリックします。



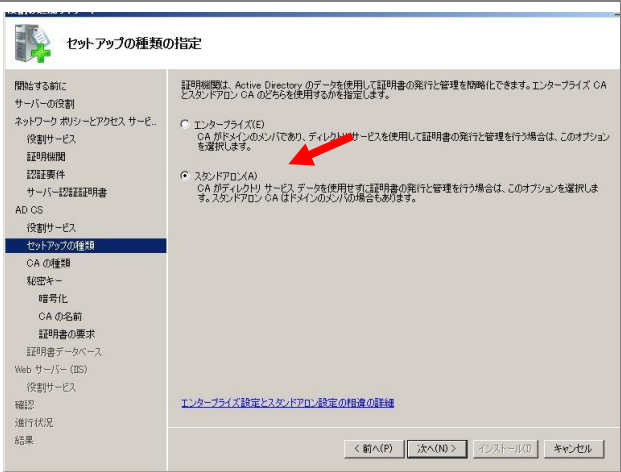
「正常性登録機関の認証要件を選択」ページで「いいえ、匿名による正常性証明書の要求を受け付けます」を選択して「次へ」をクリックします。

「SSL 暗号化用のサーバー認証証明書を選択」ページで「SSL を使用しない、または SSL 暗号化の証明書を後で選択する」を選択して「次へ」をクリックします。

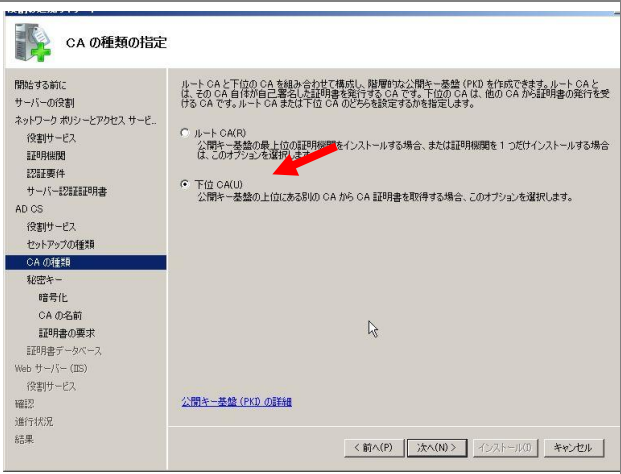
「Active Directory 証明書サービス」に関する説明が表示されるので確認して「次へ」をクリックします。

「役割サービスの選択」ページで「証明機関」にチェックを入れ「次へ」をクリックします。

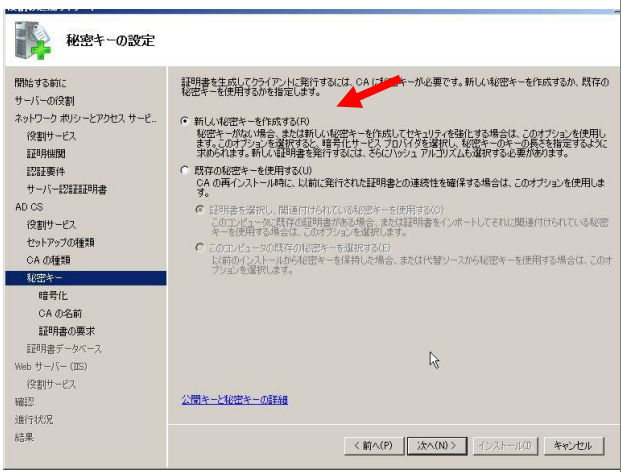
「セットアップの種類」ページで「スタンドアロン」を選択して「次へ」をクリックします。



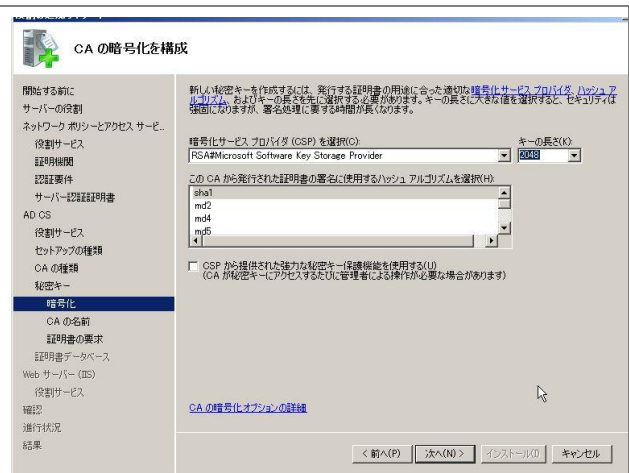
「CA の種類」ページで「下位 CA」を選択して「次へ」をクリックします。



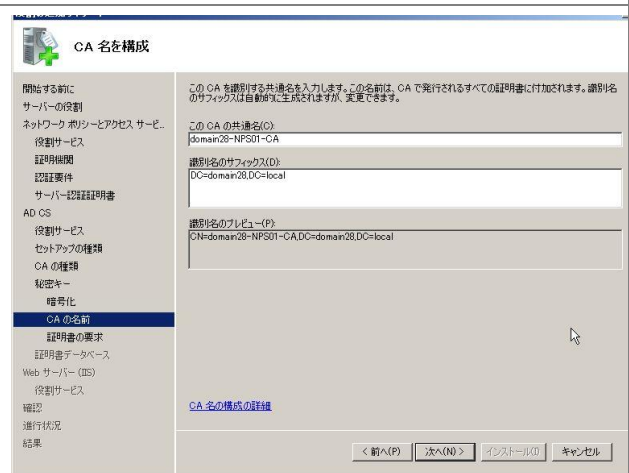
「秘密キーの設定」ページで「新しい秘密キーを作成する」を選択して「次へ」をクリックします。



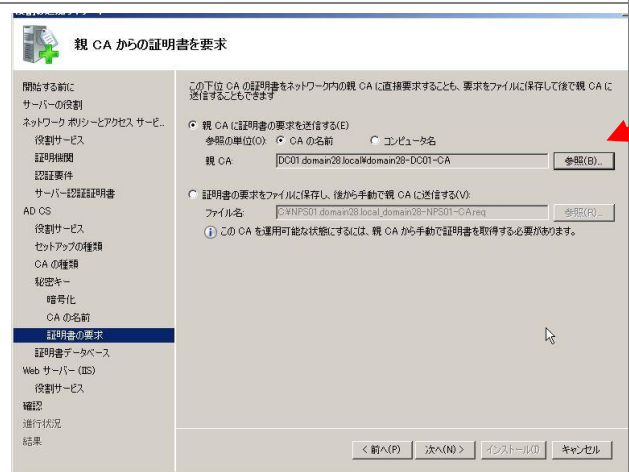
「CA の暗号化を構成」ページでは何も変更せず「次へ」をクリックします。



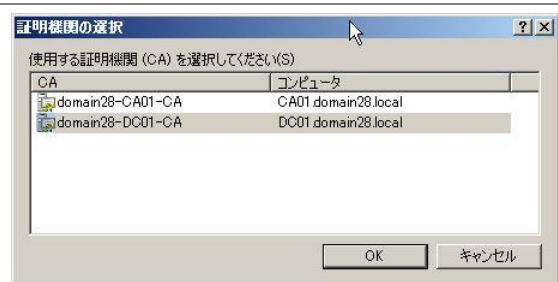
「CA 名を構成」ページで CA の共通名を入力します。デフォルトではドメイン名とコンピュータ名を使った CA 名が作成されます。適切に入力したら「次へ」をクリックします。



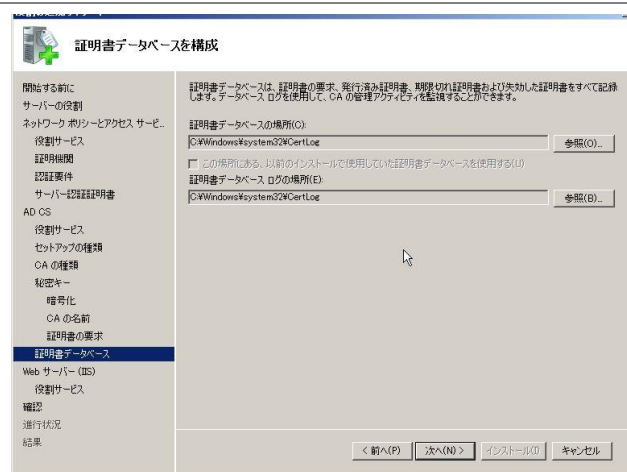
「親 CA からの証明書を要求」ページで「親 CA に証明書の要求を送信する」を選択し、「参照」ボタンをクリックします。



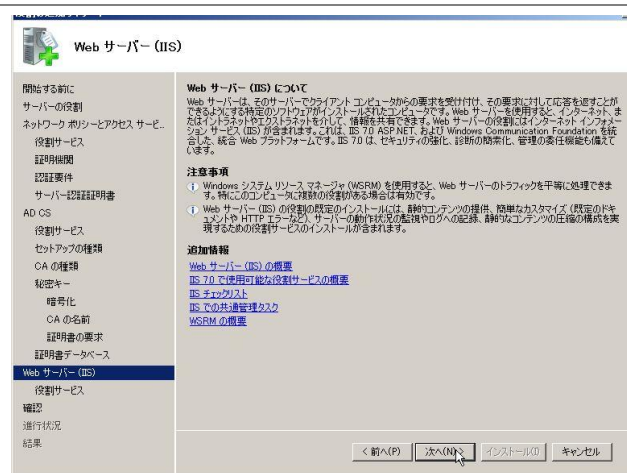
「証明機関の選択」画面が表示されるので、適切なルート CA を選択して「OK」をクリックします。「親 CA からの証明書を要求」ページに戻ったら「次へ」をクリックします。



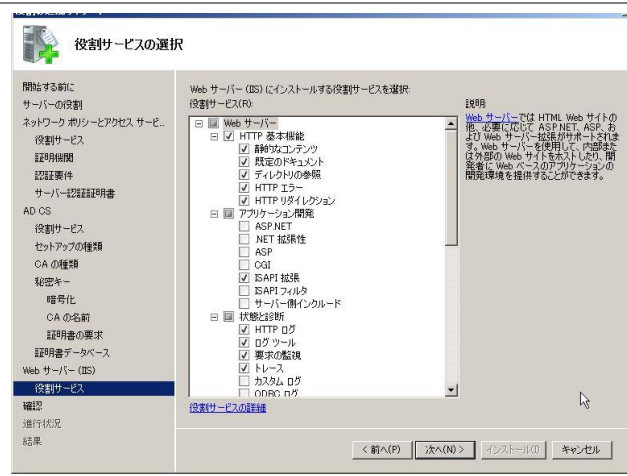
「証明書データベースの構成」ページでは何も変更せずに「次へ」をクリックします。



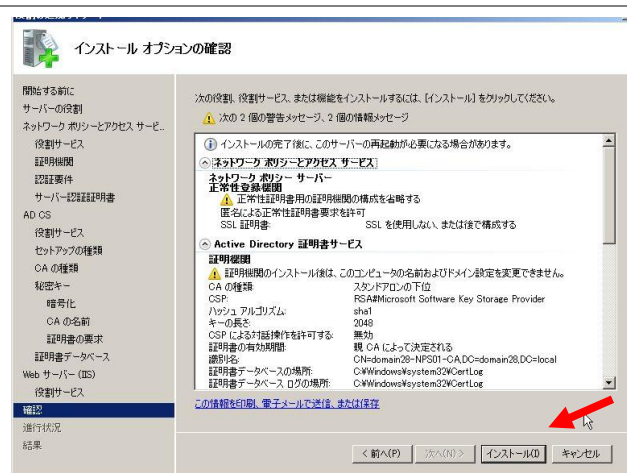
「Web サーバー」に関する説明が表示されるので、内容を確認し「次へ」をクリックします。



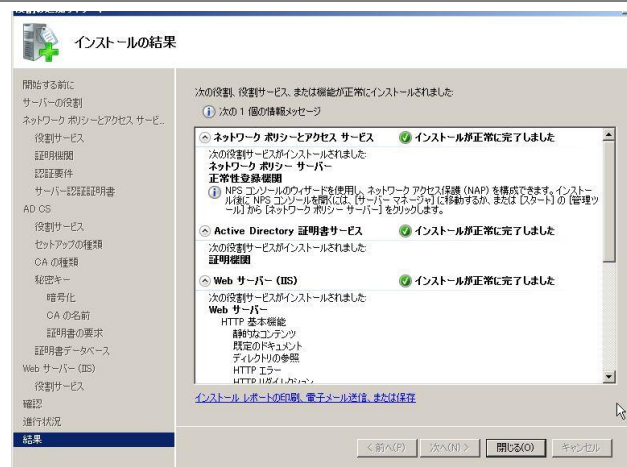
「役割サービスの選択」ページでは必要な役割が自動的に選択されています。何も変更せず「次へ」をクリックします。



インストールする内容が表示されますので、確認し「インストール」ボタンをクリックします。
インストールが開始されます。



完了すると結果が表示されます。

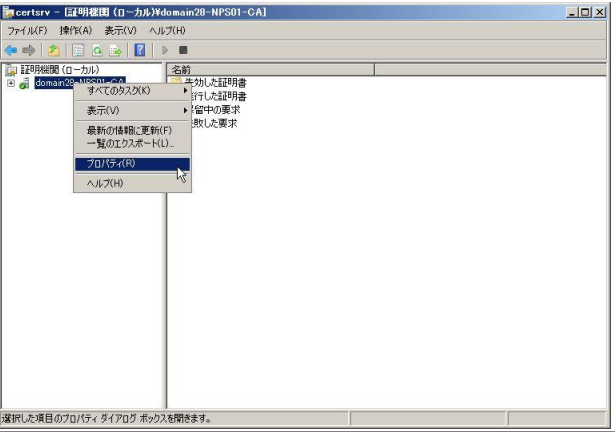
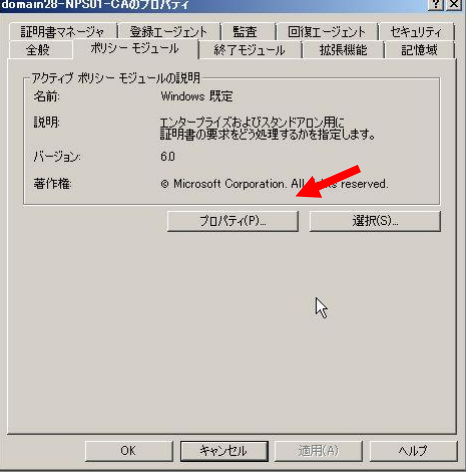
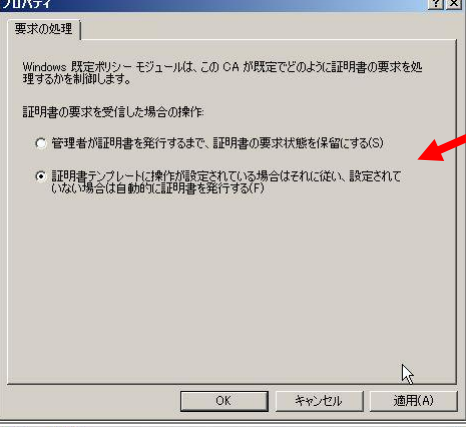



「インストールの結果」画面でインストールが正常に完了したことを確認したら、「閉じる」をクリックして、「役割の追加ウィザード」を終了します。続いて「サーバーマネージャー」も閉じます。

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。

<p>NPS01 にて「スタート」-「管理ツール」-「証明機関」を開きます。</p> <p>CA 名を右クリックし「プロパティ」を表示します。</p>	
<p>「プロパティ」画面で「ポリシーモジュール」タブをクリックし、「プロパティ」ボタンをクリックします。</p>	
<p>「テンプレートに操作が設定されている場合は…」を選択し「OK」ボタンをクリックします。</p>	
<p>再起動を促すメッセージが表示されますので、Active Directory 証明書サービスを再起動します。</p>	
<p>再び CA 名を右クリックし「プロパティ」を表示します。</p>	

「セキュリティ」タブをクリックし NETWORK SERVICE を追加します。
NETWORK SERVICE にすべての権限を許可します。

「OK」ボタンをクリックしてプロパティを閉じます。

これで、下位 CA の設定は完了です。

正常性登録機関の設定

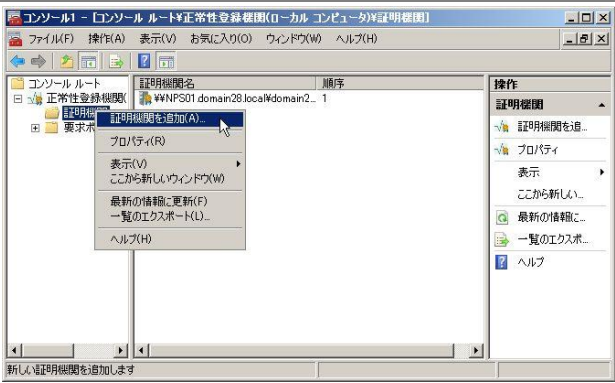
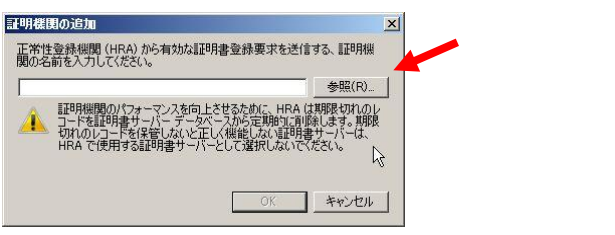


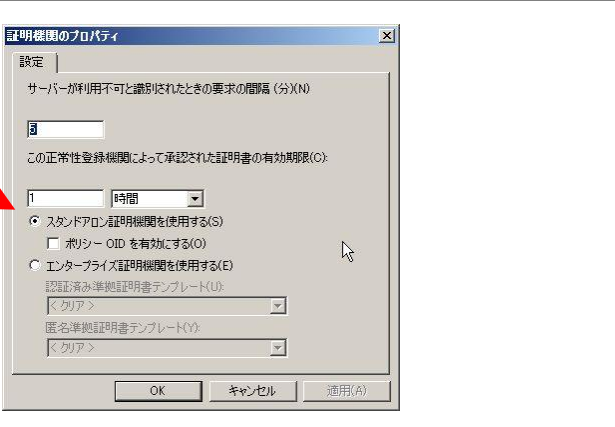
正常性登録機関の設定を行います。

「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「正常性登録機関」を追加します。

「ローカルコンピュータ...」を選択して「OK」ボタンをクリックします。

「正常性登録機関」を展開し「証明機関」をクリックします。
証明機関名として ¥\$NPS01.domain28.local がリ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ます。

<p>「証明機関」で右クリックし「証明機関を追加」をクリックします。</p>	
<p>「証明機関の追加」画面で「参照」ボタンをクリックします。</p>	
<p>「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。</p>	
<p>「証明機関」で右クリックし「プロパティ」を表示します。</p>	
<p>「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。</p>	

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。

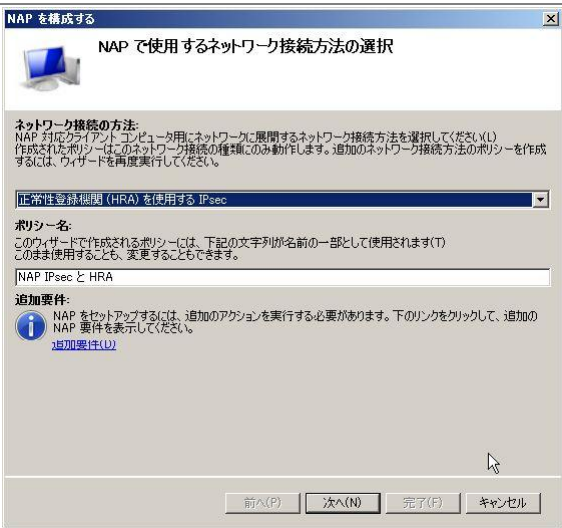
AD への登録

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。

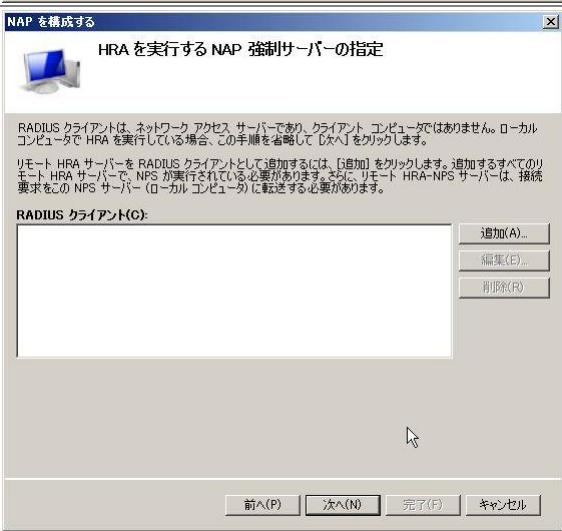
NAP 構成ウィザード

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続方法の選択」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」を選択します。「ポリシー名」には自動的に「NAP IPsec と HRA」が入ります。「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」ページでは特に何も設定せず、「次へ」をクリックします。



<p>「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、「次へ」をクリックします。</p>	
<p>「NAP 正常性ポリシーの定義」ページではデフォルト設定を確認します。テストのために「クライアントコンピ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。</p>	
<p>「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。</p>	

ウィザードが完了し、5つのポリシーが作成されました。

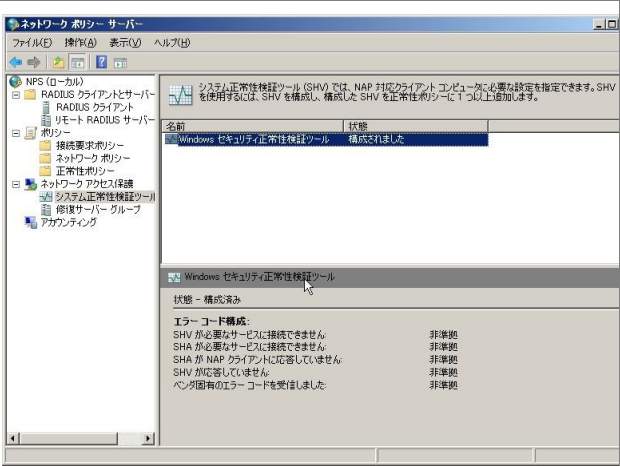
正常性ポリシー

NAP IPsec と HRA 準拠

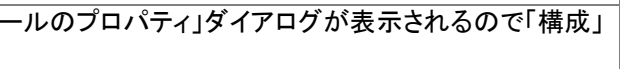
- NAP IPsec と HRA 非準拠
- 接続要求ポリシー
 - NAP IPsec と HRA
- ネットワークポリシー
 - NAP IPsec と HRA 準拠
 - NAP IPsec と HRA 非準拠

セキュリティ正常性検証ツールの設定

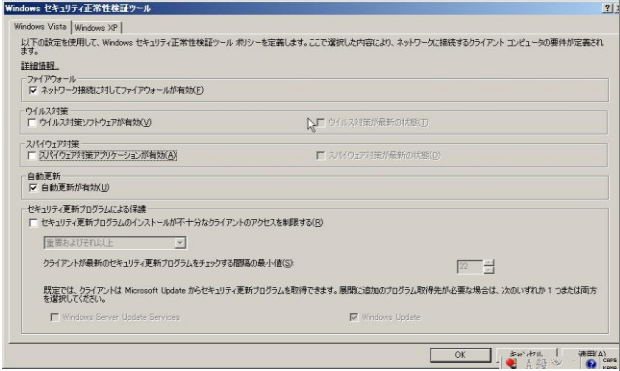
「ネットワークポリシーサーバー」のコンソールで「NAP(ローカル)」を展開し、「ネットワークアクセス保護」-「システム正常性検証ツール」をクリックします。右ペインで「Windows セキュリティ正常性検証ツール」をダブルクリックしてプロパティを表示させます。



「Windows セキュリティ正常性検証ツールのプロパティ」ダイアログが表示されるので「構成」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。



再び「Windows セキュリティ正常性検証ツールのプロパティ」のダイアログに戻るので、「OK」をクリックしてダイアログを閉じます。

「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

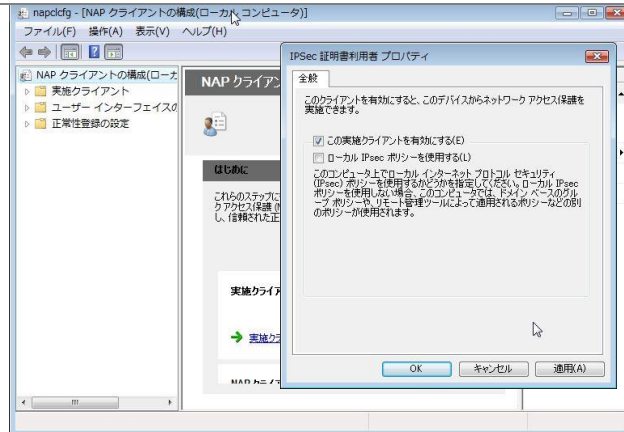
クライアントの設定を行います。

Windows Vista に管理権限のあるアカウントでログオンします。

「スタート」-「すべてのプログラム」-「アクセサリ」-「ファイル名を指定して実行」をクリックします。
「NAPCLCFG.MSC」と入力して「OK」をクリックします。

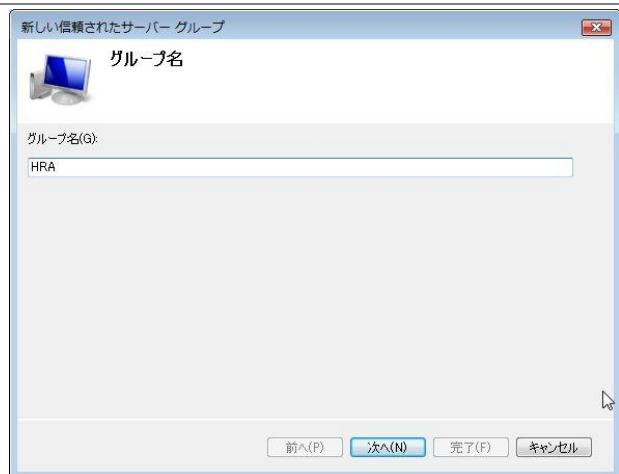
「NAPCLCFG - NAP クライアントの構成(ローカルコンピュータ)」コンソールが開きます。「実施クライアント」をクリックし、右ペインに表示される項目のうち「IPsec 証明書利用者」選択して「プロパティ」を表示します。

「IPsec 証明書利用者プロパティ」ダイアログが表示されたら「この実施クライアントを有効にする」にチェックを入れて、「OK」をクリックしてダイアログを閉じます。



「正常性登録の設定」-「信頼されたサーバーグループ」を右クリックし、「新規」をクリックします。

「グループ名」を入力し、「次へ」をクリックします。

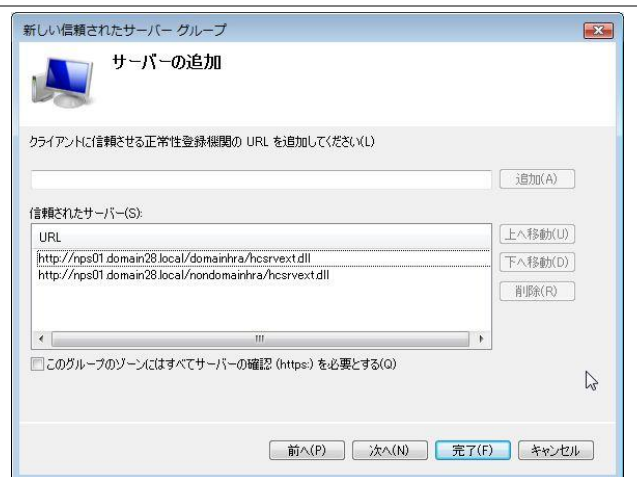


以下の 2 つの URL を追加します。

<http://nps01.domain28.local/domainhra/hcsrvext.dll>

<http://nps01.nondomain28.local/domainhra/hcsrvext.dll>

アドレスを追加する前に「すべてサーバーの確認(https)を必要とする」のチェックボックスを OFF にします。
「完了」ボタンをクリックします。



コンソールを終了します。

「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。

クライアントの設定が完了しました。

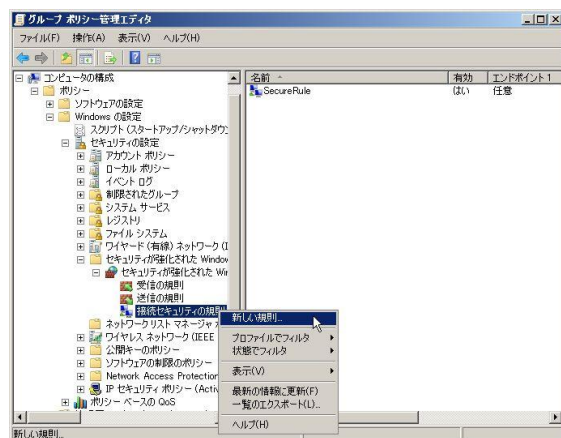
グループポリシーによる IPsec の強制

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 SecurePolicy 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」-「セキュリティが強化された Windows ファイアウォール」-「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。



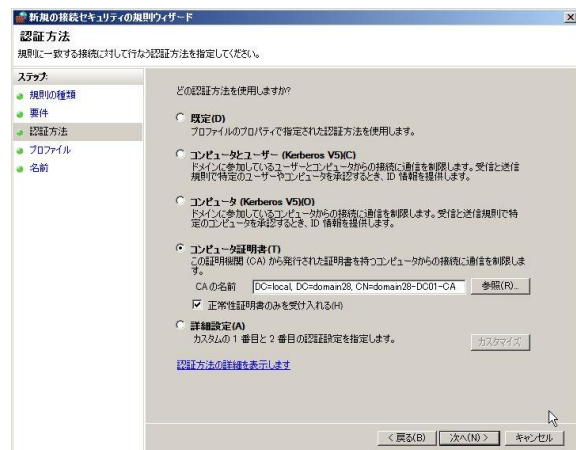
「規則の種類」画面で「分離」を選択し「次へ」をクリックします。



「要件」画面で「受信接続の認証を必須とし、送信接続に対して認証を要求する」を選択し「次へ」をクリックします。



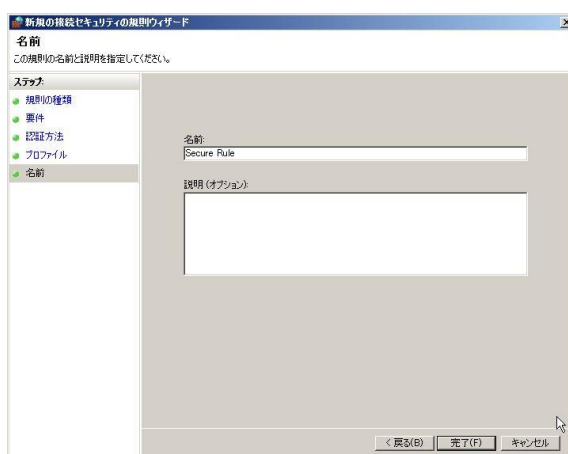
「認証方法」画面で「コンピュータ証明書」を選択します。「参照」ボタンをクリックしルートCAを選択します。「正常性証明書のみを受け入れる」にチェックを入れ「次へ」をクリックします。



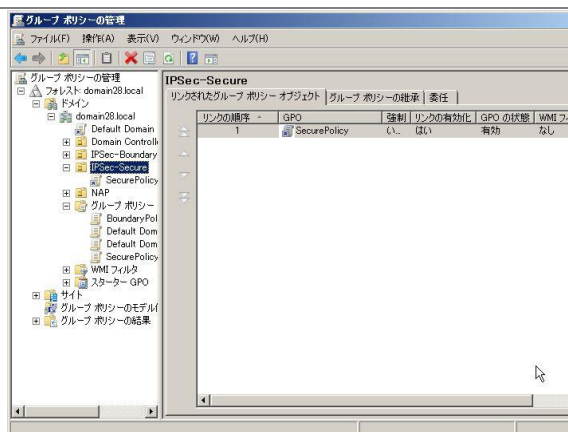
「プロファイル」画面ですべての項目にチェックを入れ「次へ」をクリックします。



「名前」画面で Secure Rule と入力し「完了」ボタンをクリックします。



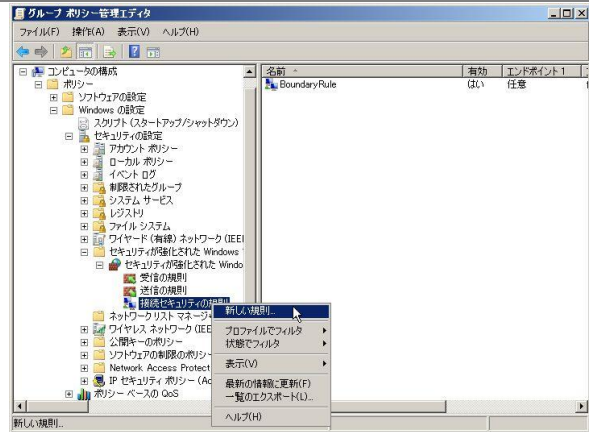
作成されたポリシーを IPSec-Secure 組織単位に割り当てます。



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。

「コンピュータの構成」-「ポリシー」-「Windows の設定」-「セキュリティが強化された Windows ファイアウォール」-「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。



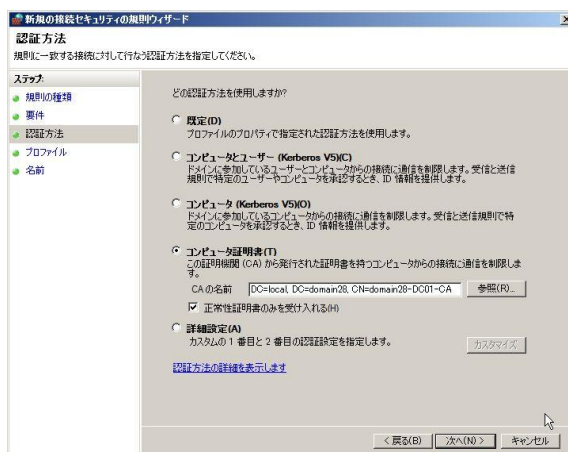
「規則の種類」画面で「分離」を選択し「次へ」をクリックします。



「要件」画面で「受信接続と送信接続に対して認証を要求する」を選択し「次へ」をクリックします。



「認証方法」画面で「コンピュータ証明書」を選択します。
「参照」ボタンをクリックしルートCAを選択します。
「正常性証明書のみを受け入れる」にチェックを入れ「次へ」をクリックします。



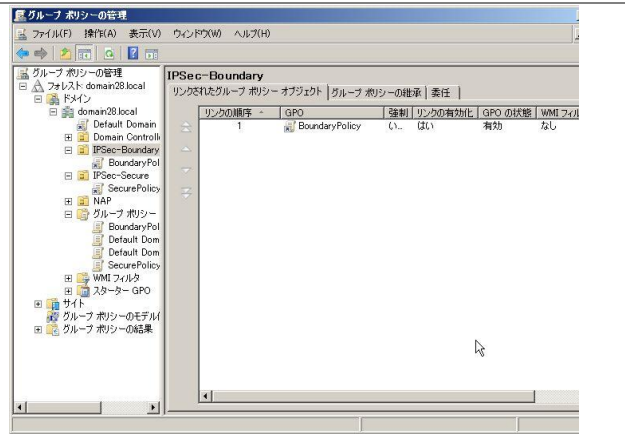
「プロファイル」画面ですべての項目にチェックを入れ「次へ」をクリックします。



「名前」画面で Boundary Rule と入力し「完了」ボタンをクリックします。



作成されたポリシーを
IPSec-Boundary 組織単位に割り
当てます。



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。

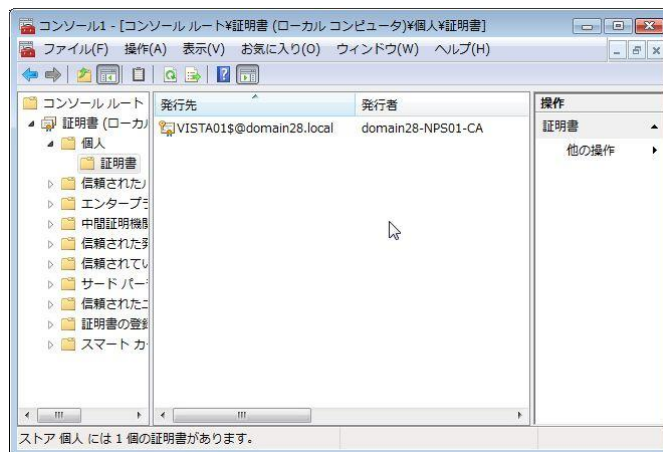
動作確認

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となりますが、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となります。

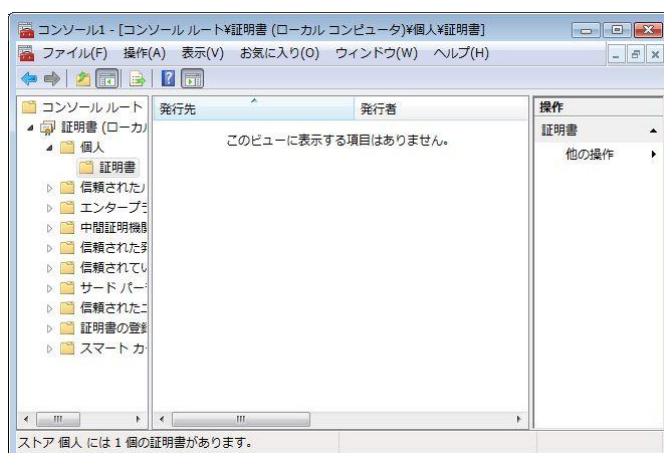
本書の手順ではクライアント PC は IPsec を強制し、NPS は IPsec を要求はするが必須ではないという設定です。また、DC に関しては何の制御も行っていない。よって、不健全な状態であってもクライアントから NPS や DC には通信することができますが、クライアント PC 同士の通信は行えません。

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。



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

CTC

Challenging Tomorrow's Changes