

Windows Server 2008
NAP 設定手順書 802.1X 編

～テスト環境での 802.1X NAP の強制～



Windows Server® 2008

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)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、製品出荷時に仕様に変更になり、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.....	1
Network Access Protection とは	2
802.1X とは	2
テスト環境.....	3
テスト環境論理図	3
検証シナリオ	3
環境作成手順	4
準備作業.....	5
ドメインコントローラの作成.....	5
組織単位の作成.....	5
ユーザーグループの作成.....	5
証明書サービスのインストール	6
役割の追加ウィザード	6
DHCP サービスのインストール	6
NPS のインストールと構成	7
概要	7
Windows Server 2008 RC0 のインストール	7
証明書の取得	8
NPS の役割のインストール	8
役割の追加ウィザード	8
ネットワークポリシーサーバーの設定	11
AD への登録.....	11
NAP 構成ウィザード.....	11
セキュリティ正常性検証ツールの設定	16
ネットワークデバイスの設定	17
クライアントの設定	18
NAP クライアントの設定.....	18
サービスの起動.....	18
ネットワークのプロパティの設定.....	19
動作確認.....	20
おわりに.....	22
付録 グループポリシー.....	24
ワイヤード(有線)ネットワーク(IEEE802.3)ポリシー	24
PEAP - ユーザー認証	24
TLS - コンピュータ認証.....	26
ワイヤレスネットワーク(IEEE802.11)ポリシー	27
PEAP - ユーザー認証	28
Network Access Protection	30
実施クライアント	30
付録 スイッチの構成	31

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)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 802.1X 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、802.1X 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、802.1X 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。同様にスイッチやアクセスポイントといったネットワークデバイス、更には 802.1X の概念やそれらの 802.1X 設定方法に関して一通りの知識を持った人が対象です。

本書は 802.1X 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、ネットワークデバイスの詳細な設定方法に関しては記載しません。特にネットワークデバイスの設定に関してはメーカーや機種毎にコマンドや設定方法が異なるため、特定の例を記載するにとどめます。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 RC0 (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 RC0 (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

本書では最もセキュリティレベルが高いと言われている 802.1X を利用した NAP を実現するための手順を扱います。

802.1X とは

802.1X はスイッチやアクセスポイントといったネットワークデバイスと RADIUS サーバーが連携し、特定のポリシーに準拠したユーザーもしくはコンピュータのみをネットワークに接続させる技術です。ポリシーに準拠している場合にはスイッチのポートを開け、準拠していない場合にはポートを閉じるという動作になります。

これにより、ドメインに参加していないクライアント、いわゆる持ち込み PC を社内 LAN に接続させないといった制御が可能になります。

802.1X ではユーザー認証とコンピュータ認証のいずれかが利用できます。また、認証の方式として PEAP と呼ばれるパスワードを利用する方法と TLS と呼ばれる証明書を利用する方法があります。

これらを組み合わせてネットワークへのアクセス許可/拒否を制御します。

ポリシーの条件にはいくつかの項目が指定できますが、例えば「無線で接続し、且つ特定の AD 上の特定のグループに所属しているコンピュータ」という指定ができます。

Windows Server 2008 のネットワークポリシーサーバーは Windows Server 2003 のインターネット認証サービスの機能を拡張させたもので、802.1X 用の RADIUS サーバーとしても動作します。

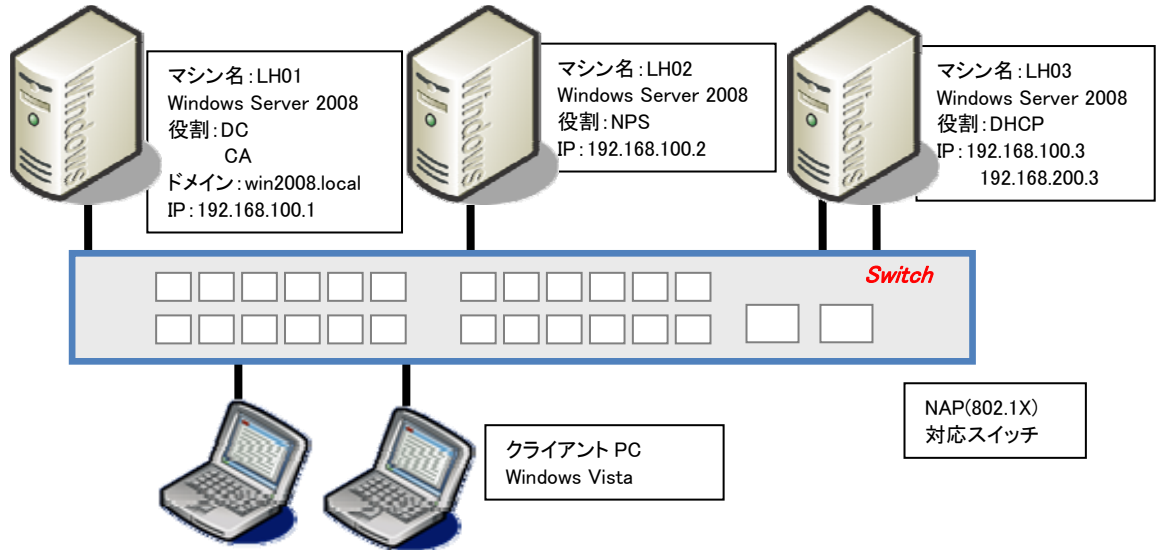
NAP で 802.1X を利用するとウイルス対策のパターンファイルが古い、ファイアウォールが無効になっているといった場合にスイッチ側でそのポートを閉じることができます。また、ほとんどの 802.1X 対応スイッチは動的 VLAN に対応しており、セキュリティレベルの低い PC を異なる VLAN に所属させることができ、社内 LAN のセキュリティレベルを維持しつつ、該当 PC を修復(パターンファイルを最新に更新する等)することが可能になります。

802.1X 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。

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築してください。

検証シナリオ

NAP(802.1X)に対応したスイッチに有線でサーバー、クライアント共に接続します。

802.1X を利用して動的に VLAN を切り替え、正常性のチェックで許可されたクライアント PC のみが正常な VLAN にアサインされ、問題のあるクライアント PC には検疫用 VLAN がアサインされます。

正常な VLAN と検疫用 VLAN はそれぞれ異なったセグメントにあり、DHCP サーバーからそれぞれのセグメント用の IP アドレスを取得します。

Windows ファイアウォールを無効にした段階で検疫ネットワークに隔離され、有効に戻した段階で社内 LAN に接続されることを確認します。

本書では PEAP を利用したユーザー認証の手順を示します。

環境作成手順

802.1X 構成の 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 RC0 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。

ネットワークポリシーサーバーサービス(NPS)

Windows Server 2008 RC0 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。

証明書サービス(CA)

ドメインコントローラである LH01 に証明書サービスをインストールします。RADIUS サーバー(NPS)に証明書を発行します。

更に、クライアントの状態に応じて異なったセグメントに所属させるため、それぞれのセグメントに DHCP サーバーを配置するか、2つのスコープを持つ DHCP サーバーを構築します。

DHCP サービス

Windows Server 2008 RC0 が動作している LH03 に DHCP サービスを構成します。NIC を複数構成し、それぞれのセグメントに対して IP アドレスをリースさせます。

NAP(802.1X)対応スイッチ

NAP もしくは 802.1X に対応したネットワークデバイス(スイッチ)が必要です。動的 VLAN を設定し、クライアントの状態に応じて VLAN を変更させます。

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、スイッチ、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。

準備作業

NAP を構成するための準備作業を行います。

ドメインコントローラの作成

LH01 に Windows Server 2008 RC0 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 RC0 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。

組織単位の作成

新規に組織単位(OU)を作成し、検疫を実施するコンピュータをその組織単位に移動させます。

ユーザーグループの作成

グループを作成し、ネットワークに対するアクセスを許可するユーザーをグループに所属させます。

証明書サービスのインストール

LH01 に証明書サービスをインストールします。

役割の追加ウィザード

役割の追加ウィザードを利用して「Active Directory 証明書サービス」をインストールします。

証明機関は企業の要件に従って構成することになりますが、ここではエンタープライズルート CA として構成するものとします。

また、必要に応じてグループポリシーを用いて証明書を自動登録するように設定します。

証明書サービスのインストールに関する詳細はここでは省略します。

DHCP サービスのインストール

LH03 に DHCP サービスをインストールします。

Windows Server 2008 の DHCP サービスでなくとも 2 つのセグメントに対してそれぞれ IP アドレスをリースできる DHCP サーバーならばかまいません。

もしくはそれぞれのセグメントに DHCP サーバーを配置します。

DHCP サービスのインストールに関する詳細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)の役割を動作させるには Windows Server 2008 RC0 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 RC0 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
- 証明書を取得する
- 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
- NPS を構成する

以下、手順の詳細を記述します。

Windows Server 2008 RC0 のインストール

コンピュータの電源を入れ Windows Server 2008 Enterprise Edition RC0 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 を適切に設定し、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。

証明書の取得

LH02 でコンピュータ証明書(サーバー証明書)を取得します。

証明書の取得方法は証明機関の構築方法やグループポリシーの設定によって異なりますが、エンタープライズルート CA が構築され、グループポリシーで自動登録が有効に設定されていれば、ドメインに参加し、グループポリシーが適用された段階で証明書が取得されています。自動的に取得されていない場合には証明機関に要求し、証明書を取得してください。

証明書の取得方法に関する詳細は省略します。

NPS の役割のインストール

NPS の役割を LH02 にインストールします。

役割の追加ウィザード

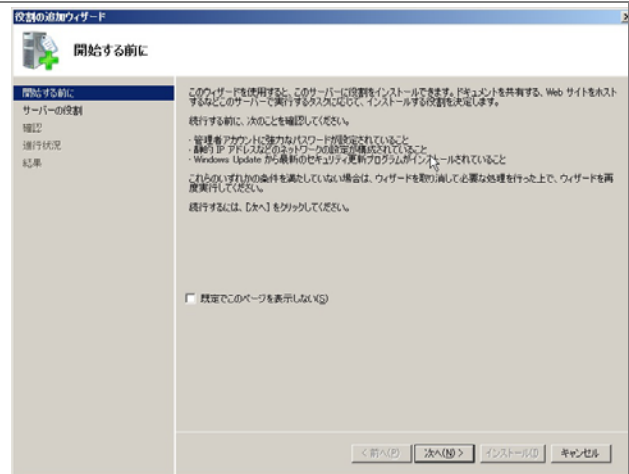
「Start」をクリックして「管理ツール」-「サーバーマネージャー」を起動します。



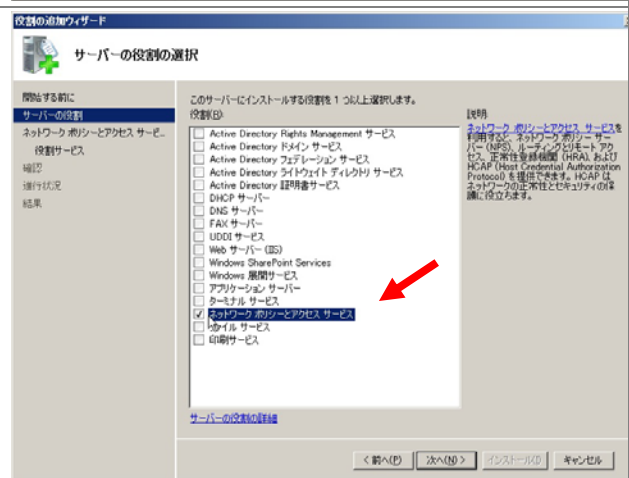
「役割の概要」を展開して「役割の追加」をクリックします。「次へ」をクリックします。



「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。

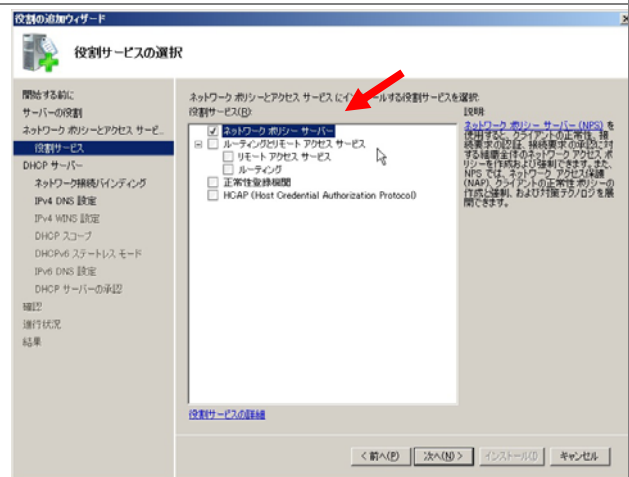


「サーバーの役割の選択」ページが開くので「ネットワークポリシーとアクセスサービス」にチェックを入れて「次へ」をクリックします

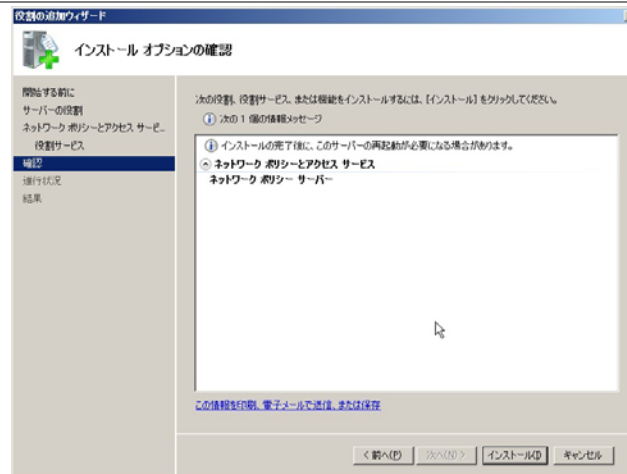


「ネットワークポリシーとアクセスサービス」に関する説明が表示されます。「次へ」をクリックします。

「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」にチェックを入れます。「次へ」をクリックします。



「インストールオプションの確認」ページで内容を確認して問題がなければ、「インストール」ボタンをクリックします。



「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 がインストールされました。

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

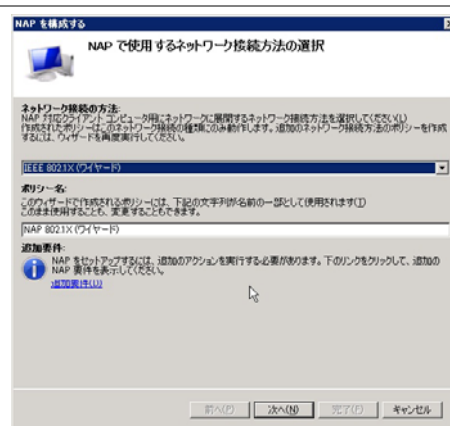
スタートをクリックして「管理ツール」-「ネットワークポリシーサーバー」をクリックします。「NPS(ローカル)」を右クリックし、「Active Directory にサーバーを登録」をクリックします。

NAP 構成ウィザード

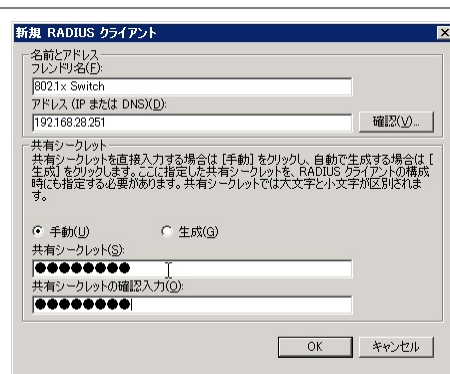
スタートをクリックして「管理ツール」-「ネットワークポリシーサーバー」をクリックします。「ネットワークポリシーサーバー」のコンソールが開いたら「NAP(ローカル)」をクリックします。右ペインで「ネットワークアクセス保護(NAP)」を選択し、「NAP を構成する」をクリックしウィザードを起動します

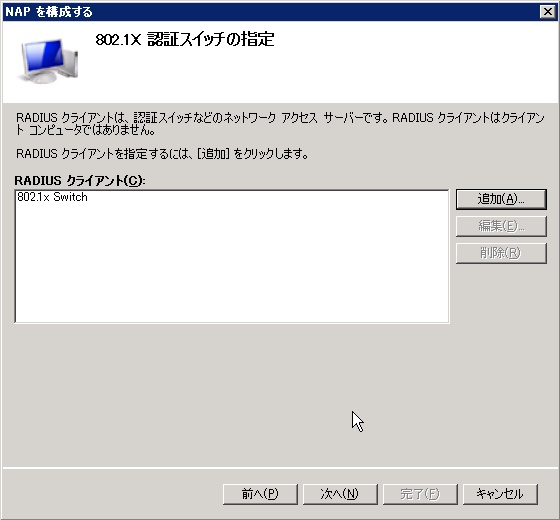
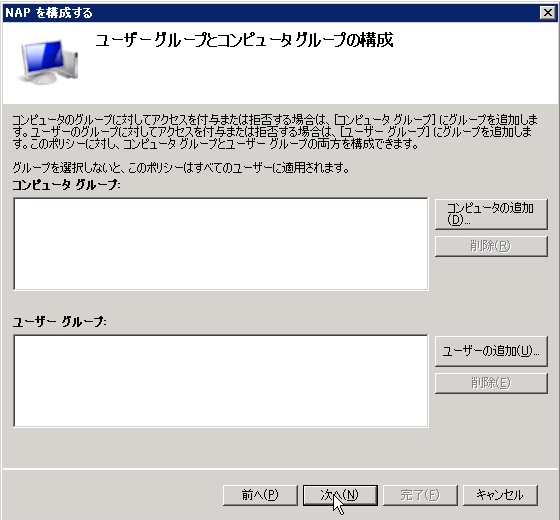
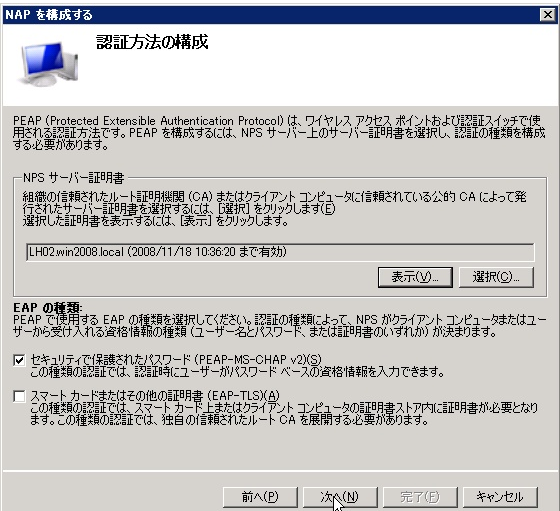


「NAP で使用するネットワーク接続方法の選択」ページが開いたら、「ネットワーク接続の方法」でプルダウンから「IEEE 802.1X(ワイヤード)」を選択します。「ポリシー名」には自動的に「NAP 802.1X(ワイヤード)」が入ります。必要に応じてポリシー名を変更し、「次へ」をクリックします。

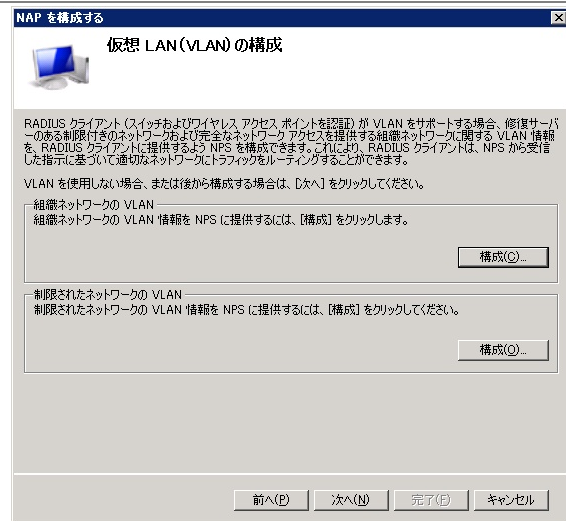


「802.1X 認証スイッチの指定」ページで「追加」ボタンをクリックすると「新規 RADIUS クライアント」の画面が開きます。識別のためのネットワークデバイスの名前(任意)とIPアドレス、更に共有シークレットを入力し、「OK」をクリックします。



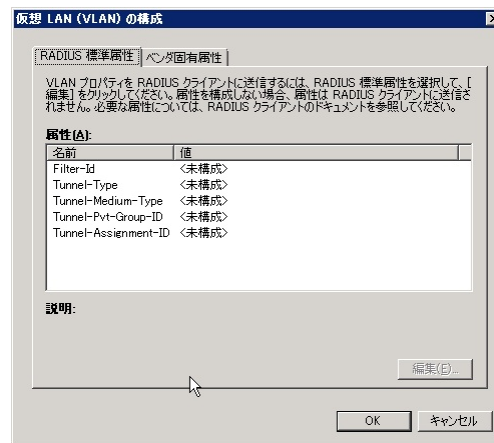
<p>「802.1X 認証スイッチの指定」ページに戻ったら「次へ」をクリックします。</p>	
<p>「ユーザーグループとコンピュータグループの構成」ページで必要に応じてアクセス許可を与えるグループを指定し、「次へ」をクリックします。</p>	
<p>「認証方式の構成」ページで NPS サーバー証明書が正しく表示されていることを確認します。EAP の種類として「セキュリティで保護されたパスワード (PEAP-MS-CHAP v2)」のみにチェックを入れ、「次へ」をクリックします。</p>	

「仮想 LAN(VLAN)の構成」ページで「組織ネットワークの VLAN」の「構成」ボタンをクリックし、検疫をパスしたコンピュータに対して与える属性(アトリビュート)を指定します。

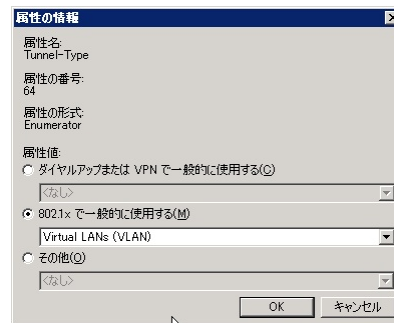


「仮想 LAN(VLAN)の構成」画面で「Tunnel-Type」を選択し、「編集」ボタンをクリックします。

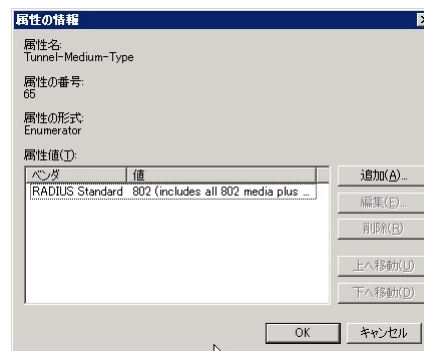
注) 以下の手順は一般的に VLANID をネットワークデバイスに渡すための手順です。ネットワークデバイスによっては異なる属性(アトリビュート)が必要な場合がありますので、ネットワークデバイスの説明書を参照してください。



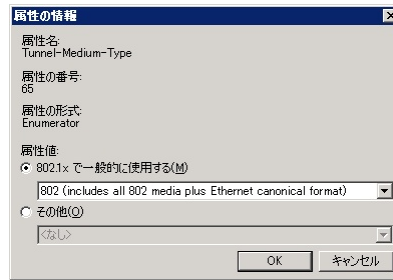
「属性の情報」画面で「802.1X で一般的に使用する」を選択し、プルダウンから「Virtual LANs(VLAN)」を選択し、「OK」をクリックします。



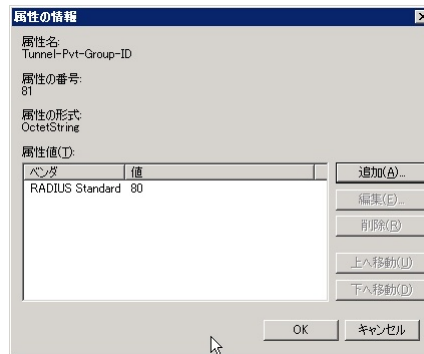
同様に「Tunnel-Medium-Type」を選択し、「編集ボタン」をクリックします。「属性の情報」画面で「追加」ボタンをクリックします。



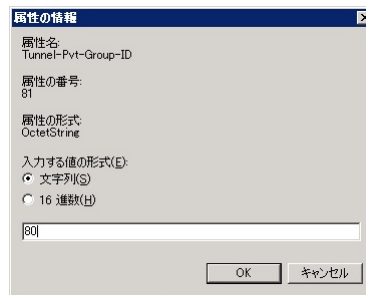
「802.1X で一般的に使用する」を選択し、プルダウンから「802(include all 802 ...)」を選択し、「OK」をクリックします。「属性の情報」画面に戻ったら「OK」をクリックします。



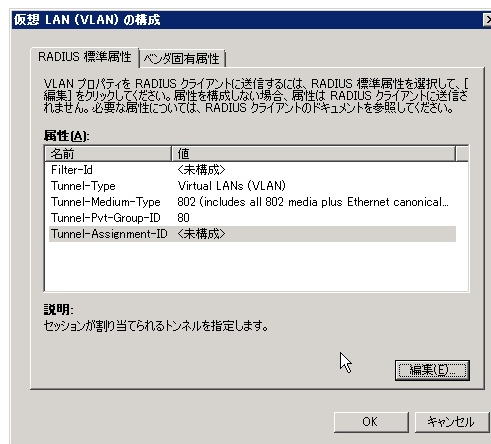
更に、「Tunnel-Pvt-Group-ID」を選択し、「編集」ボタンをクリックします。「属性の情報」画面で「追加」ボタンをクリックします。



「入力する値の形式」で「文字列」を選択し、テキストボックスに組織ネットワーク VLAN(正常なネットワーク)の VLANID の番号(画面では 80)を入力し、「OK」をクリックします。「属性の情報」画面に戻ったら「OK」をクリックします。



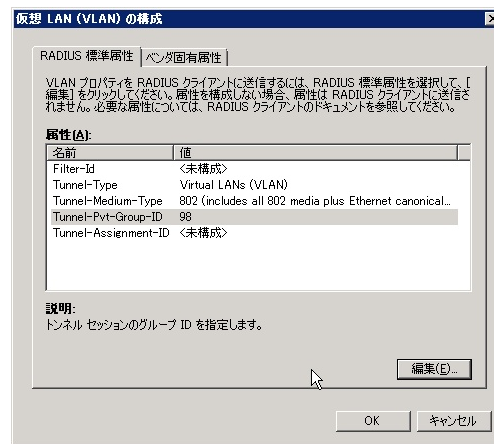
「仮想 LAN(VLAN)の構成」画面に戻ったら「OK」をクリックします。



「仮想 LAN(VLAN)の構成」ページに戻ります。

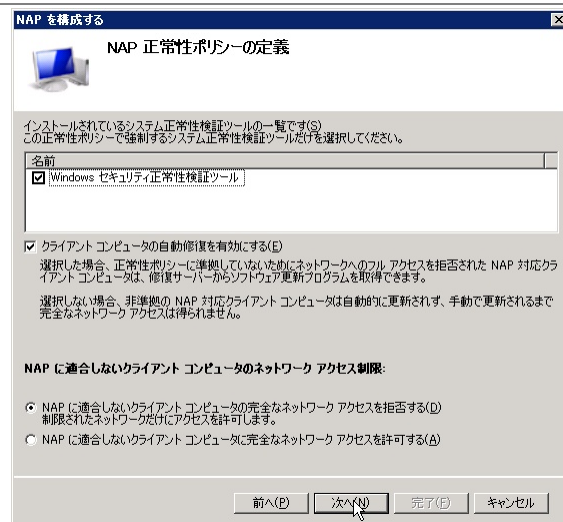
同様に「制限されたネットワークの VLAN」の「構成」ボタンをクリックし、検疫ゾーン用の VLANID を設定します。

※手順は「組織ネットワークの VLAN」を構成する手順と同じです。

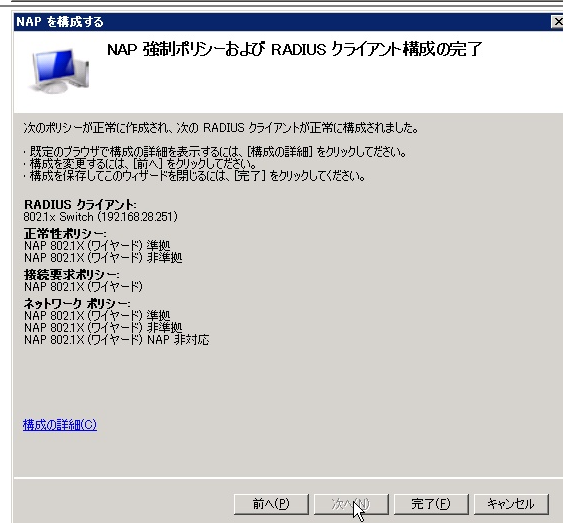


VLAN の設定が終わったら「次へ」をクリックします。

「NAP 正常性ポリシーの定義」ページで「Windows セキュリティ正常性検証ツール」のチェックボックスが ON になっていることを確認します。また「NAP に適合しないクライアントコンピュータの完全なネットワークアクセスを拒否する(制限されたネットワークだけにアクセスを許可します)」を選択し、「次へ」をクリックします。



「NAP 強制ポリシーおよび RADIUS クライアント構成の完了」ページが表示され、自動的に作成されるポリシーを確認し、「完了」ボタンをクリックします。



ウィザードが完了し、6 つのポリシーと RADIUS クライアント設定が作成されました。

正常性ポリシー

- NAP 802.1X(ワイヤード)準拠
- NAP 802.1X(ワイヤード)非準拠

接続要求ポリシー

NAP 802.1X(ワイヤード)

ネットワークポリシー

NAP 802.1X(ワイヤード)準拠

NAP 802.1X(ワイヤード)非準拠

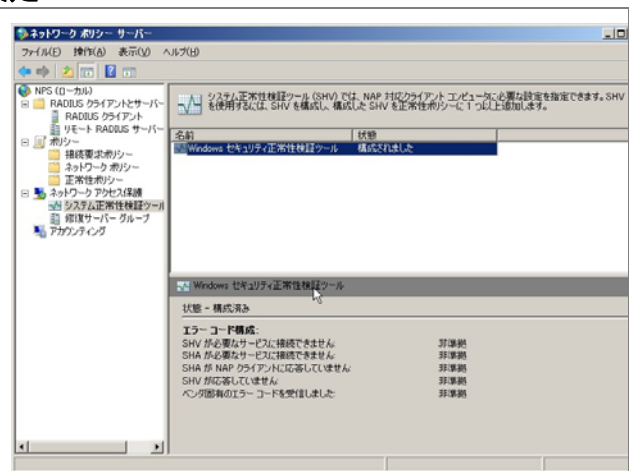
NAP 802.1X(ワイヤード)未対応

RADIUS クライアント

802.1X Switch(フレンドリ名)

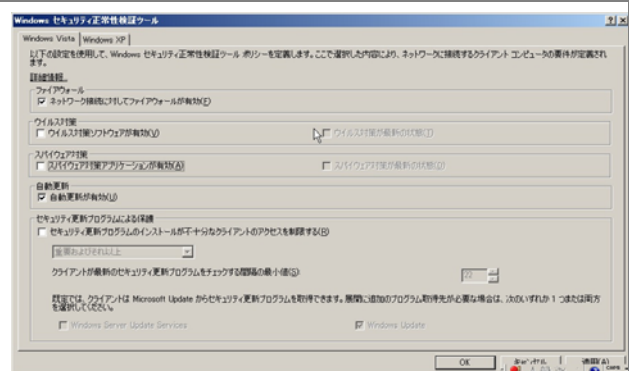
セキュリティ正常性検証ツールの設定

「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。

ネットワークデバイスの設定

ネットワークデバイス側で受け取った属性に応じて VLAN を動的に変更させる設定を行います。

上記の手順で NPS を設定した場合、正常なクライアントの場合には 80 が、セキュリティレベルの低いクライアントの場合には 98 が VLANID として渡されるので、それぞれの VLAN を割り当てます。

一般的に動的 VLAN に対応しているネットワークデバイスは VLANID を認識します。

しかし、ネットワークデバイスによっては特定の属性によりステータスを変化させ、結果として VLAN を変更させるようなものも存在します。

設定方法はネットワークデバイスのメーカーや機種により異なりますので、ここでは記述しません。それぞれの説明書及び付録を参照してください。

クライアントの設定

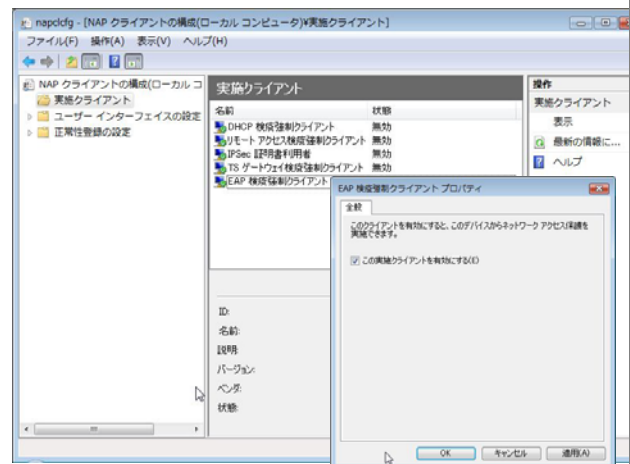
最後にクライアントの設定を行います。

NAP クライアントの設定

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「EAP 検疫強制クライアント」を選択して「プロパティ」を表示します。
「EAP 検疫強制クライアントプロパティ」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。



コンソールを終了します。

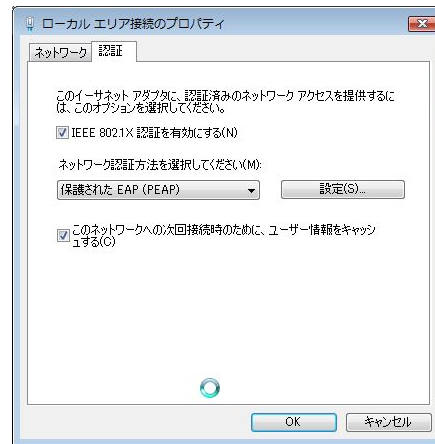
※グループポリシーを利用して制御する事も可能です。

サービスの起動

「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。

ネットワークのプロパティの設定

ローカルエリア接続のプロパティを表示させ、「認証」タブをクリックします。
 「IEEE802.1X 認証を有効にする」のチェックボックスを ON にします。
 「保護された EAP(PEAP)」を選択し、「設定」ボタンをクリックします。



「保護された EAP のプロパティ」の画面で以下の設定を行います。

- ・「サーバーの証明書を検証する」のチェックボックスを ON
- ・LH01 に構築した証明機関のチェックボックスを ON
- ・「検疫のチェックを有効にする」のチェックボックスを ON
- ・「セキュリティで保護されたパスワード (EAP-MSCHAP v2)」を選択



「OK」をクリックしてネットワークの設定を終了します。

※グループポリシーを利用して制御する事も可能です。

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に隔離され、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。

```

C:\Users\Administrator> ipconfig

Windows IP 構成

イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . . . . :
   IPv4 アドレス . . . . . : 192.168.28.61
   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 . . . . . :
   リンクローカル IPv6 アドレス . . . . . : fe80::5efe:192.168.28.61%16
   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。

```

C:\Users\Administrator> ipconfig

Windows IP 構成

イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . . . . :
   IPv4 アドレス . . . . . : 192.168.98.63
   サブネット マスク . . . . . : 255.255.255.0
   デフォルト ゲートウェイ . . . . . : 192.168.98.254

Tunnel adapter ローカル エリア接続* 6:

   接続固有の DNS サフィックス . . . . . :
   リンクローカル IPv6 アドレス . . . . . : fe80::5efe:192.168.98.63%16
   デフォルト ゲートウェイ . . . . . :

C:\Users\Administrator>
  
```

異なるセグメントの IP が割り当てられています。

修復ゾーンのセグメントに配置、もしくは適切にルーティングされた修復サーバーに接続し、必要に応じてウィルスのパターンファイルの更新や、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 802.1X 構成が最もセキュリティレベルが高いと言える構成です。

802.1X の方法是对应するスイッチ類が必要になり、導入には大量のネットワーク機器をリプレイスする必要があるかもしれません。

ただ、これらの機器には様々な機能が備わっている場合が多いので、本書で取り上げた 802.1X の制御だけでなく、MAC アドレス認証等を利用して NAP に対応していないクライアントの制御を行う事も可能です。

ネットワークデバイスの特定の機能の利用も検討してください。

本書では PEAP を利用したユーザー認証の手順を記述していますが、TLS の方式やコンピュータ認証も利用できます。

また、無線 LAN でも 802.1X が利用可能です。

Windows Server 2008 のドメインで Windows Vista をクライアントとして利用している場合にはグループポリシーで 802.1X 関連の設定が制御できます。

特にコンピュータ認証を行いたい場合にはクライアント側には設定箇所がありません。グループポリシーでは制御が可能です。

NAP は複数の方式で実装できますが、802.1X の構成の場合にはネットワークデバイスの交換や設定作業も必要になります。「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ので、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 グループポリシー

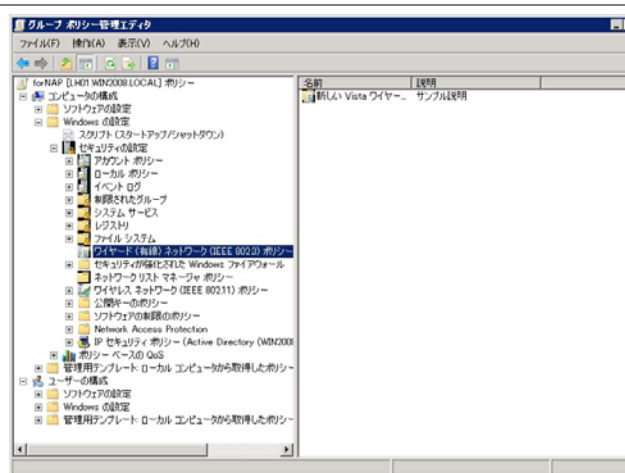
クライアントの 802.1X に関するネットワーク設定をグループポリシーで制御する場合の設定例を記載します。(一例として記載します。環境に応じて変更してください。)

ワイヤード(有線)ネットワーク(IEEE802.3)ポリシー

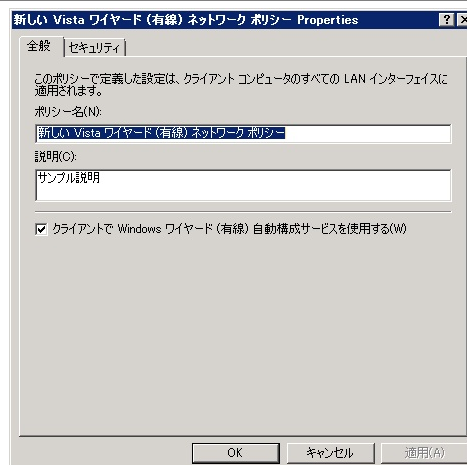
Windows Server 2008 のドメインでは有線用の 802.1X 設定をポリシーで制御できます。ただし、有線に関して設定できるのは Vista のみです。

PEAP - ユーザー認証

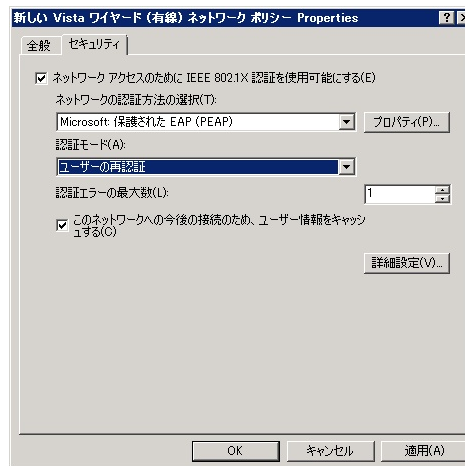
有線用のポリシーを作成します。



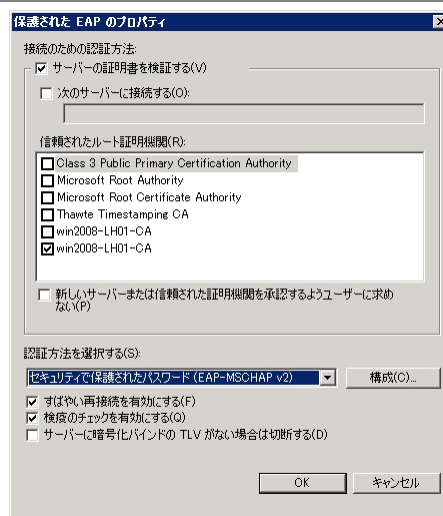
ポリシー名は任意です。



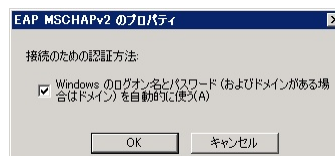
認証の種類として「PEAP」、モードは「ユーザーの再認証」を選択します。



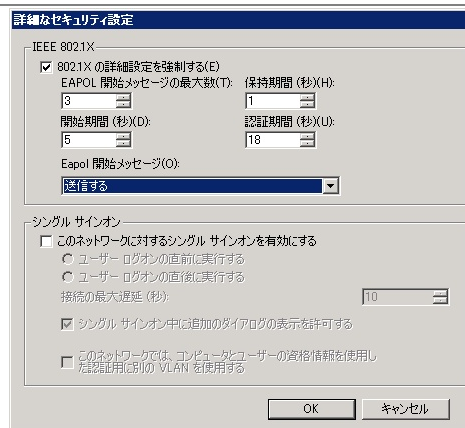
認証方法は「セキュリティで保護されたパスワード」を選択します。「検疫のチェックを有効にする」のチェックボックスを ON にします。(必須)



「構成」ボタンをクリックすると、パスワード入力の自動化を設定できます。

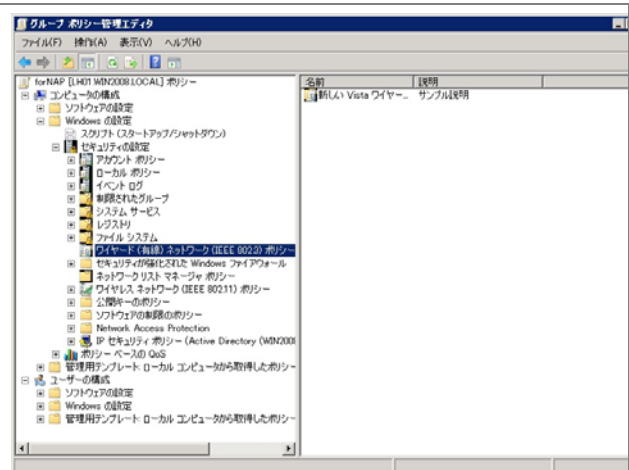


PEAP のプロパティとして 802.1X の詳細設定ができます。

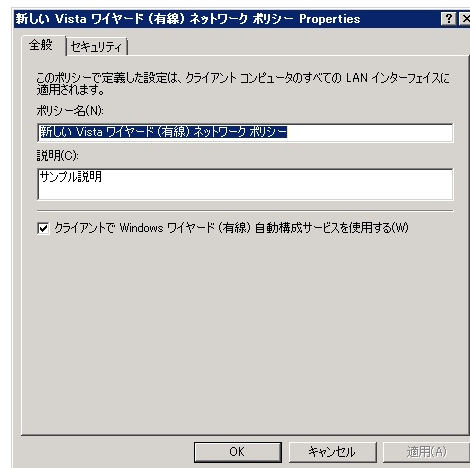


TLS - コンピュータ認証

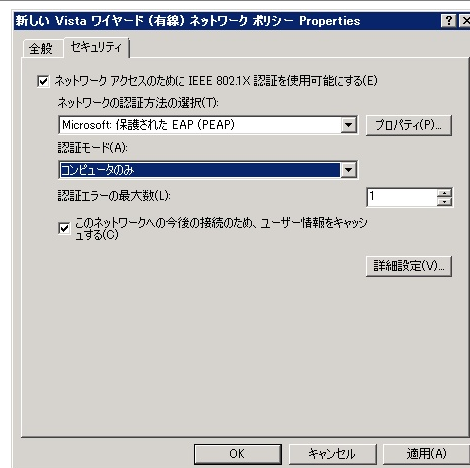
有線用のポリシーを作成します。

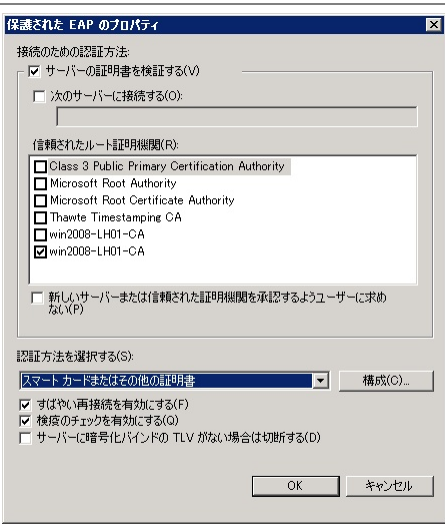

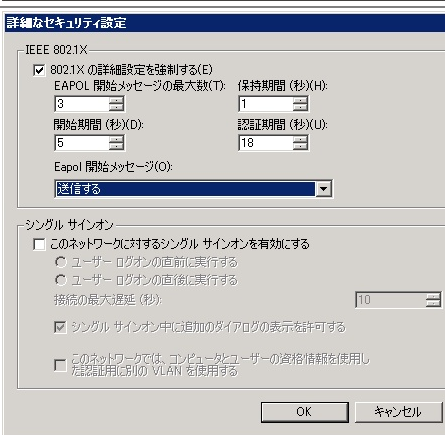


ポリシー名は任意です。



認証の種類として「PEAP」を、モードとして「コンピュータのみ」を選択します。



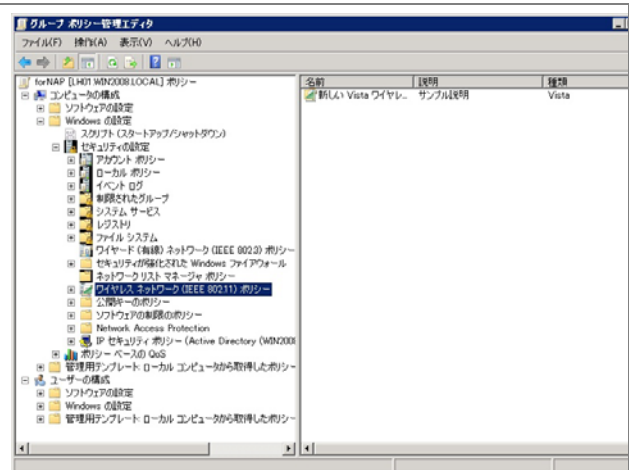
<p>認証方法で「スマートカードまたはその他の証明書」を選択します。 「検疫のチェックを有効にする」のチェックボックスを ON にします。 (必須)</p>	
<p>適切な証明書を選択します。</p>	
<p>PEAP のプロパティとして 802.1X の詳細設定ができます。</p>	

ワイヤレスネットワーク(IEEE802.11)ポリシー

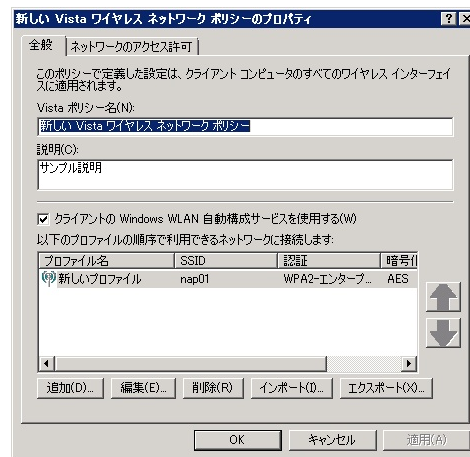
無線接続の際の 802.1X 設定をポリシーで制御できます。

PEAP - ユーザー認証

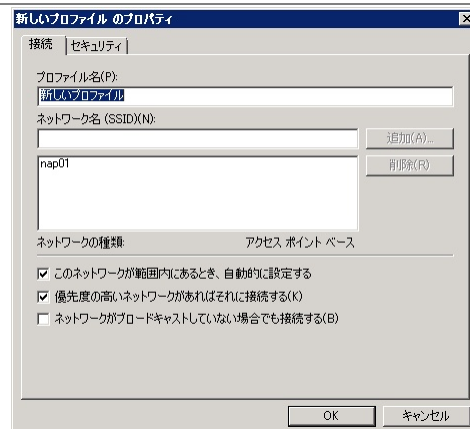
無線用のポリシーを作成します。



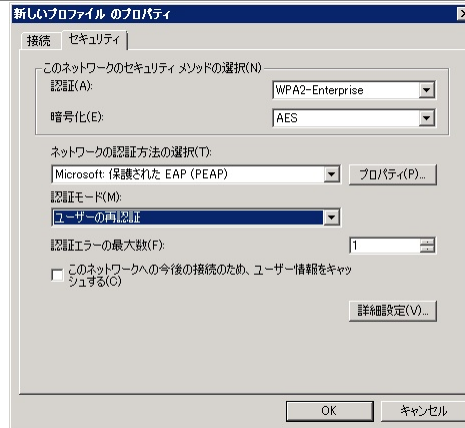
ポリシー名は任意です。



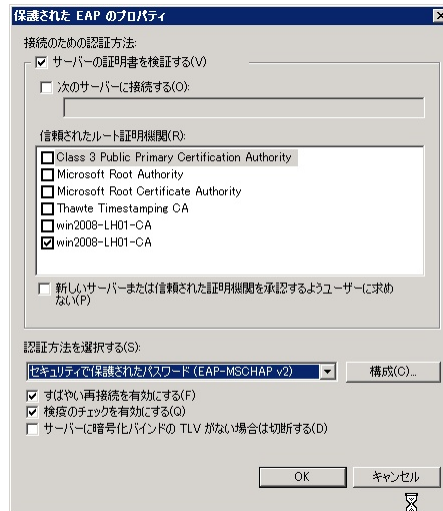
無線用のプロファイルを作成します。



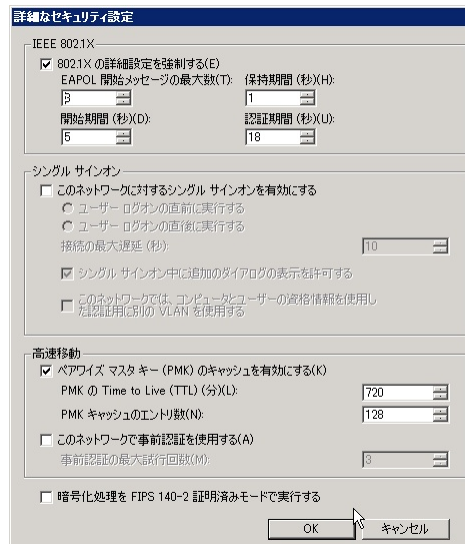
以下の設定を行います。
 認証の種類: WPA2-Enterprise
 暗号化の方式: AES
 ネットワーク認証方法: PEAP
 認証モード: ユーザーの再認証

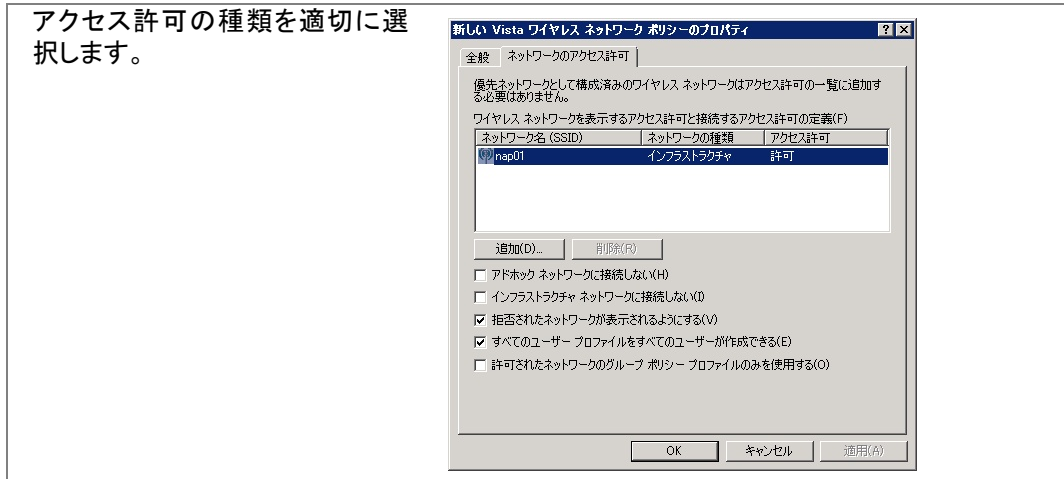


認証方法は「セキュリティで保護されたパスワード」を選択します。「検疫のチェックを有効にする」のチェックボックスを ON にします。(必須)



PEAP のプロパティとして 802.1X の詳細設定ができます。



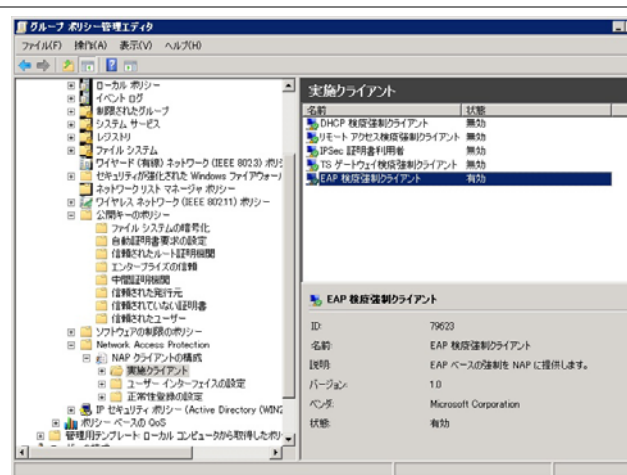


Network Access Protection

Windows Server 2008 のドメインではグループポリシーで Network Access Protection(NAP)のクライアント設定を制御できます。

実施クライアント

グループポリシーの「実施クライアント」を開きます。



802.1X 構成の NAP を利用する場合は「EAP 検疫強制のクライアント」を有効にします。



付録 スイッチの構成

ネットワークデバイスの設定は、メーカー、機種により様々です。
 ここでは一例として検証を実施した際のスイッチの設定例を記載します。

Alaxala AX2430S (Ver.10.6)
<p>ポート VLAN の設定</p> <pre>(config)# vlan 1 (config-vlan)# state active (config)# vlan 10 (config-vlan)# name NativeVLAN (config)# vlan 1000 (config-vlan)# name ManagedVLAN</pre> <p>MAC VLAN の設定</p> <pre>(config)# vlan 30 mac-based (config-vlan)# name QuarantineVLAN (config)# vlan 20 mac-based (config-vlan)# name OkVLAN</pre> <p>物理ポートの設定</p> <pre>(config)# interface range fastethernet 0/1-32 (config-if-range)# switchport mode mac-vlan (config-if-range)# switchport mac vlan 20,30 (config-if-range)# switchport mac native vlan 10 (config)# interface range gigabitethernet 0/1-4 (config-if-range)# media-type rj45 (config)# interface range fastethernet 0/33-40 (config-if-range)# switchport mode access (config-if-range)# switchport vlan 1 (config)# interface range gigabitethernet 0/48 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 1,20,30,1000</pre> <p>インタフェースの設定</p> <pre>(config)# interface vlan 1000 (config-if)# ip address 192.168.0.1 255.255.255.0</pre> <p>RADIUS サーバの設定</p> <pre>(config)# radius-server host 192.168.28.2 key "alaxala"</pre> <p>スタティックルートの設定</p> <pre>(config)# ip default-gateway 192.168.0.254</pre> <p>アクセスリストの設定</p> <pre>(config)# ip access-list extended VLAN10 (config-ext-nacl)# deny ip any any (config)# interface vlan 10 (config-if)# ip access-group VLAN10 in</pre> <p>RADIUS の設定</p> <pre>(config)# aaa authentication dot1x default group radius (config)# aaa authorization network default group radius</pre> <p>動的 VLAN 認証の設定</p>

```
(config)# dot1x vlan dynamic radius-vlan 20,30
(config)# dot1x vlan dynamic enable
(config)# dot1x vlan dynamic reauthentication
(config)# dot1x vlan dynamic timeout reauth-period 360
(config)# dot1x vlan dynamic supplicant-detection disable
(config)# dot1x system-auth-control
```

ARUBA 800 (3.1.1.7 (w/PEF License))

Setup Dialog による設定

```
System name: aruba800
VLAN 1 interface IP address: 192.168.28.250
VLAN 1 interface subnet mask: 255.255.255.0
IP Default gateway: 192.168.28.254
Switch Role: master
Country code: JP
Time Zone: JST+9:0
Ports shutdown: no
```

VLAN の設定

```
vlan 48
vlan 68
vlan 88
vlan 108
```

インターフェースの設定

```
interface vlan 1
    ip address 192.168.28.250 255.255.255.0

interface vlan 108
    ip address 192.168.108.254 255.255.255.0
    ip helper-address 192.168.28.3
    operstate up

interface vlan 48
    ip address 192.168.48.254 255.255.255.0
    ip helper-address 192.168.28.3
    operstate up

interface vlan 68
    ip address 192.168.68.254 255.255.255.0
    ip helper-address 192.168.28.3
    operstate up

interface vlan 88
    ip address 192.168.88.254 255.255.255.0
    ip helper-address 192.168.28.3
    operstate up
```

RADIUS サーバの設定

```
aaa authentication-server radius "lh02"
    host 192.168.28.2
    key 2d5e3ad1a7073b507b23815455e8193b
    nas-identifier "aruba800"
    nas-ip 192.168.28.250
```

```
aaa server-group "radius01"
auth-server lh02
```

AAA プロファイルの設定

```
aaa profile "nap01-aaa"
authentication-dot1x "default"
dot1x-server-group "radius01"
```

SSID プロファイルの設定

```
wlan ssid-profile "nap01-ssid"
essid "nap01"
opmode wpa2-aes
```

Virtual AP の設定

```
wlan virtual-ap "nap01-ap"
ssid-profile "nap01-ssid"
vlan 108
aaa-profile "nap01-aaa"
```

AP Group の設定

```
ap-group "group01"
virtual-ap "nap01-ap"
```

ロールとポリシーの設定

```
user-role compliant
vlan 48
session-acl allowall
!
user-role non_compliant
vlan 68
session-acl allowall
!
user-role non_nap
vlan 88
session-acl allowall
```

STP を無効に設定

```
no spanning-tree
```