

~テスト環境での 802.1X NAP の強制~



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)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	
802.1X とは	2
テスト環境	
テスト環境論理図	
検証シナリオ	
環境作成手順	
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	
役割の追加ウィザード	
DHCP サービスのインストール	
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	
NPS の役割のインストール	
役割の追加ウィザード	
ネットワークポリシーサーバーの設定	
AD への登録	
NAP 構成ウィザード	
セキュリティ正常性検証ツールの設定	
ネットワークデバイスの設定	
クライアントの設定	
NAP クライアントの設定	
サービスの起動	
ネットワークのプロパティの設定	
動作確認	
おわりに	
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	
ワイヤレスネットワーク(IEEE802.11)ボリシー	
PEAP - ユーザー認証	
Network Access Protection	
実施クライアント	
付録 スイッチの構成	



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 RCO (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 RCO (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を利用するとウィ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 RCO 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 RCO 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 RCO 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しての詳細は省略します。

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





「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	
	(学校・学を前に サーバーの(注新 編注 (通行状況) 紀平:	このウイゲード気候用すると、このサーバーに回動をインストールできます。ドキュンシトを共有する、Web サイトをホスト するなどこのサーバーで使用すなスクなだして、インストールを含め着きを実施します。 またするすめに、かんじと地味認いてない。 ・ ・ 「読得者 サウクン」は変わないなり、一般的な方式ないことと ・ 「Webwen Usebate が一般時的にをおうっだ用りつうう」がインストールだれていること これらいって計れていた時代やも読んしていない場合は、ウィザードを取り消して必要なな速を行った上で、ウィザードを再 販売行してくだだか。 認得すするには、これへ」を分ックしてください。
		「 展前でたのページを表示しない(S) (前へ(2) (次へ(B)) イシストーバの 年齢が出来
	-	
「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	役割の追加ウィザード 「「「」」 サーパーの役割の	選択
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- します。	開始する新に サーバーの位日 ネットワーカ ポシートアウセス サーミー 後期 デージス 場に 通行状況 総果 ービス」に関する	このサーバービインストールするの理解1 つとし上選択します。 (文解日) 【V# これたいを Detectory Fighds Management サービス したいた Detectory Fighds Management サービス Detectory Fighds Management Hangement Management Hangement
「役割サービスの選択」ページで	役割の追加ウィザード	
「ネットワークポリシーサーバー」	御 役割サービスの選	R
にチェックを入れます。「次へ」を クリックします。	間始する時に サーバーの(78) ネットワーク 赤りワーとアクセス サービー ゼロサービス DHCP サーバー ネットワーク時時時 (10) ディング サーダ ONS 間空 DHCP 4 ステード レットの INS 間空 DHCP 4 ステード レットの INS 間空 DHCP サーバーの中起2 幅空 調査(1式) 元	Apt/ワークス(1) ドサマシス(2) ドサマシス(2) Log 2 23-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20)-07 (20) 3-52-27 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (20)-07 (
		役割サービスの詳細
		<10.00 x0.00



「インストールオプションの確認」	役割の追加ウィザード	
ページで内容を確認して問題が	1ンストール オプショ	心の確認
なければ、「インストール」ボタン をクリックします。	間始する新に サーバーの位割 ネットワークボルジーとアクセスサービ。 役割サービス 増行がえ見 総系	 (カの93)、役割サービス、または繊維をインストールするには、{/ンストール]をグラウルではだが、 (ナンストールの第二年に、このサーバーの再記曲が必要になる場合がかります。 (ホートリーク ボリシーとアクセス サービス ネットワーク ボリシー サーバー
		4
		この情報を印刷、電子メールで送信、または保存
		<#A(P)
「インストールの結果」画面でインスト リックして、「役割の追加ウィザード」 す。	ールが正常に5 を終了します。約	宅了したことを確認したら、「閉じる」をク 乱いて「サーバーマネージャー」も閉じま

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





「802.1X 認証スイッチの指定」へ	NAP を構成する
ージに戻ったら「次へ」をクリックし	802.1X 認証スイッチの指定
ます。	
	RADIUS クライアントは、認証スイッチなどのネットワーク アクセス サーバーです。RADIUS クライアントはクライアン ト コンピュータではありません。
	RADIUS クライアントを指定するには、[追加] をクリックします。
	RADIUS クライアント(<u>C</u>):
	802.1× Switch
	[編集(1)]
	\mathbf{k}
	<u>前へ(P)</u> <u>汰へ(N)</u> <u>完て(E)</u> <u>キャンセル</u>
「ユーザーグループとコンピュータ	NAP を構成する X
グループの構成」ページで必要に	ユーザーグループとコンピュータグループの構成
ウルッの構成」、シモジタに	
ーフを指定し、「次へ」をクリックし	コンピュータのグループに対してアクセスを付与または拒否する場合は、ロンピュータグループ」にグループを追加しま
ます。	す。ユーリーのグループに対してアクセスを行うまでは担合するの場合は、ユニットーグループにクループを追加します。このポリシーに対し、コンピュータグループとユーザー 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 ガリーゴ・
	באני איי איי איי איי איי איי איי איי איי
	コーザー ガループ・
	<u></u>
「認証方式の構成」ページで NPS	NAP を構成する
サーバー証明書が正しく表示され	認証方法の構成
ていることを確認します。	
	PEAP (Protected Extensible Authentication Protocol)は、ワイヤレスアクセスポイントおよび認証スイッチで使用される認証方法です。PEAP を構成する(には、NPS サーバー上のサーバー証明書を選択し、認証の種類を構成
休護されたハスリート	する必要がめります。
(PEAP-MS-CHAP v2)」のみにチ	NPS サーバー証明書
ェックを入れ、「次へ」をクリックし	行きれたサーバー証明書を選択するには、「選択」をクリックします(E) 選択した証明書を選択するには、「選択」をクリックします(E) 選択した証明書を選択するには、「表示」をクリックします。
ます。	
	PHO2 WIN2000,000 (2000/11/10 10:30:20 まで有効)) 表示(V) 違扼(C)
	EAP の種類
	FEAF CU実用する EAF の種類を運択してんたい。認識の種類によって、NPS がのライアントコンピュータまたはユーザーから受け入れる資格情報の種類(ユーザー名とパスワード、または証明書のいずれか)が決まります。
	✓ セキュリティで保護されたパスワード (PEAP-MS-CHAP v2)(S) この確認角部項目では「取取損益にコーザーがパスワード パーコの必約がは超な 3 力でキャオ
	CVILLARValdelLCIX adelLCICL フレンソフロ・ハンンジョイスンンジョンフレビスタッ。
	この種類の認証では、スマートカード上またはクライアントコンピュータの証明書ストア内に証明書が必要となり ます。この種類の認証では、独自の信頼されたルート CA を展開する必要があります。



「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。	NAP を結成する 文 仮想 LAN (VLAN) の構成 このある朝鮮(村名のような、ビューターングレスアクセス、ポイントを認証) が VLAN をサポートする場合、修課サーバ - のある朝鮮(村名のように、ビューターングレンスアクセス、ポイントを認証) が VLAN をサポートする場合、修課サーバ - のある朝鮮(村名のように、ビューターングレンス) 不らい (日本) ないのい (日本) ないのい (日本) ないのい (日本) ないのい (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本)
「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。 主)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	反想 LAN (VLAN) の構成 X RADIUS 標準顕性 ペンタ回有男性 // ペンタ回有男性 // ペンタ回有男性 // ペンタ回有男性 // ペンタ回方 (1) 大学な、男性な RADIUS クライアントに注信するには、RADIUS 標準男性を選択して、「 福美国家 クリックルでだだい。 RADIUS クライアントに注信するには、RADIUS クライアントには、RADIUS クライアントロビス 作業になる RADIUS クライアントロビス 作業になる RADIUS クライアントロビス 作業になる RADIUS クライアントロビス 不信の (RADIUS クライアントロビス RADIUS クライアントロビス RADIUS クライアントロビス RADIUS RAD
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。	シロボ 編集(E)… OK キャンセル
「属性の情報」画面で「802.1X で ー般的に使用する」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。	国性名: Tunnel-Type 図 周性の形式: Enumeator 周性の形式 Solution: マー級的に使用する(C) びるしン ✓ で 約21xで一級的に使用する(M) ✓ Virtual LANs (VLAN) ▼ でるの他(Q) ✓ OK キャンセル
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。	歴世の特徴



「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。	EttOth程 区 歴史2: Tunnel-Medium-Type 属性の番号: 6 属性の形式: Enumerator 陽性値 6 802.1x で一般的に使用する(M) [902 (includes all 802 media plus Ethernet canonical format) [902 (includes all 802 media plus Ethernet canonical format)] ○ その他(Q)
	(ない) OK キャンセル
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。	F住の特報 F性名: Tunnel-Pxt-Group-ID F性の形式: OcteRSting Ft位(f): RADIUS Standard 80 FADIUS Standard 80 FARMU(J) FARMU(J) FARMU(J) FARMU(J) FARMU(J) FARMU(J) FARMU(J) FARMU(J)
「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。	時性の情報 ▼ 歴性名: Tunnel-Pvt-Group-ID 野性の番号: 81 野性の形式: OctelString 入力する他の形式:(E): で 文字列(S) 「 16 浅磁気(H) [S0]
「仮想 LAN(VLAN)の構成」画面に 戻ったら「OK」をクリックします。	反切 LAN (VLAN) の構成 ▼ RADIUS 標準編性 ペング回有腐性 VLAN プロパライを RADIUS クライアントに送信されない場合、開性は RADIUS クライアンドに送信される 必要な場面については、RADIUS クライアントのドキュメントを参照してただい。 審査 価 Filter-1d <未構成> Tunnel-Type Withia LANs (VLAN) Tunnel-Program 000000000000000000000000000000000000
「仮想 LAN(VLAN)の構成」ページに	戻ります。





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



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」ー「すべてのプログラム」ー「゙	アクセサリ」-「ファ	イル名を指え	定して実行」をク	リックしま
す。				
「NAPCLCFG.MSC」と入力して「OK」を	をクリックします。			
「NAPCLCFG – NAP クライアント	in napcidg - [NAP クライアントの構成()	ローカル コンピュータ)¥実施ク	ライアント]	
の構成(ローカルコンピュータ)」コ	ファイル(F) 操作(A) 表示(V) ヘル	プ(H)		
ンソールが開きます。「実施クライ	 ・ ・ ・	etative is an annual		10.41
アント」をクリックし、右ペインに表	ご 実施クライアント	実」絶クラ1 アント 名前	状態	実施クライアント
示される項目のうち「EAP 検疫強	▶ 🎬 正常性登録の設定	50HCP 検疫強制クライアント 50リモート アクセス検疫強制クラ	無効 イアント 無効	表示 ④ 最新の情報に
制クライアント」選択して「プロパ		DPSec 証明書利用者 TS ゲートウェイ検疫法制クライ	無効 イアント 無効	2 117
ティーを表示します。		SEAP (0)2 SEAP (EAP 検疫強制クライアント プロパティ 全校	
「EAP 検疫強制クライアントプロパ			このクライアントを有効にすると、このデバイスから4 実施できます。	・ットワーク アクセス/実績を
ティレダイアログが表示されたら			図 この実施クライアントを有効にする(ℓ)	
「この実施クライアントを有効にす				
$\Delta_{1} (C + T_{1}) / \Delta_{2} (C + T_{1}) / \Delta_{2$		ID: :名約:		
		1988		
	6	N-912		
		状態		
		1	D OK **	
			.,	

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	♀ ローカルエリア接続のプロパティ
します。	ネットワーク 認証
「IFEE8021X 認証を有効にする」	このイーサネット アダプタに、認証済みのネットワーク アクセスを提供する(こ
	は、このオプションを選択してください。
のテェックホックスを ON にしま	✓ IEEE 802.1× 認識で有効にする(N)
	ネットワーク認証方法を選択してください(M):
「保護された EAP(PEAP)」を選択	(米額された EAP (PEAP) ▼
し、「設定」ボタンをクリックしま	▼このネットワークへの)次回接続時のために、ユーザー情報をキャッシ
す。	-19900
	O
	OK キャンセル
「保護された EAP のプロパティ」の	保護された EAP のプロパティ
画面で以下の設定を行います。	接続のための認証方法
・「サーバーの証明書を検証す	▼サーバーの調理明書を検証する(V)
るIのチェックボックスを ON	□ 〉次のサーバー(ご接続する(0))
	(言理語された)ルート語TB月4期間(R):
	Class 3 Public Primary Certification Authority
エックホックスを UN	Microsoft Root Authority
・「検疫のチェックを有効にする」	Thavite Timestamping CA In the second secon
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	□ 新ししいサーバーまたは信頼された間正明根関を承認でするようユーザーに求めな (V(P)
選択	
	認証方法を選択する(S)
	【セキュリティで保護されたパスワード (EAP-MSCHAP v2) ▼ 【構成(C)】
	 ✓ すはたい再接続を有効にする(F) ✓ 検疫のチェックを有効にする(Q)
	□サーバーに暗号化バインドの TLV がない場合は切断する(D)
	OK (#w`d?ll)
「OK」をクリックしてネットワークの設定	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。

m 管理者: コマンド プロンプト	_ 🗆 🗙
C:¥Users¥Administrator≻ipconfig	^
∜indows 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 : 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>_	
k	
	•

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。

國 管理者: コマンド プロンプト	<u>- 🗆 ×</u>
C:¥Users¥Administrator>ipconfig	
Nindows IP 構成	
イーサネット アダプタ ローカル エリア接続:	
接続国有の DNS サフィックス: IP∨4 アドレス: 192.168.98.63 サブネット マスク: 255.255.05 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>	
\mathbf{k}	

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 の方法は対応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。







認証の種類として「PEAP」、モード	新し() Vista ワイヤード (有線) ネットワーク ポリシー Properties ? ×
は「ユーザーの再認証」を選択し	全般 セキュリティ
ます。	▼ ネットワーク アクセスのために IEEE 802.1X 認証を使用可能にする(E)
	ネットワークの認証方法の選択(T): Microsoft: 保護された EAP (PEAP) フロパティ(P)
	12811 - H(A):
	□ <u>□</u>
	このネットワークへの今後の接続のため、ユーザー情報をキャッシュ コ オス(イ) コ オス(イ)
	- 2.2、2、2
認証方法は「セキュリティで保護	保護された EAP のプロパティ X
されたパスワード」を選択します。	接続のための認証方法:
「検疫のチェックを有効にする」の	□ 次のサーバーに接続する(O):
ナエックホックスを ON にします。	(音楽系文1) た-11、一人専び日日御月(12)
(必須)	Class Primary Certification Authority
	Increase the contract of
	☐ win2008-LH01-CA ☑ win2008-LH01-CA
	□ 新しいサーバーまたは1番和された温祉の外域内を水気29 るようエーサーによめ) ない、(P)
	12証方法を選択する(S):
	セキュリティで保護されたパスワード (EAP-MSCHAP v2) 構成(C)
	▼ 検疫のチェックを有効にする(Q) □ サーバーに暗号化パインドの TLV がない場合は切断する(D)
「構成」ボタンをクリックすると、パ	FAP MSCHAPy2 加力パティ X
スワード入力の自動化を設定でき	1986のかかの1970万方法:
ます。	✓ Windows のログオン名とパスワード (およびドメインがある場 会けドメイン) 本自動的に使う((本))
PEAP のプロパティとして 802.1X	詳細なセキュリティ設定
の詳細設定ができます。	- IEEE 802.1X
	EAPOL開始シッセージの最大致(T): (米特期間(物)(H): 3 当 1 当
	開始4期間(秒)(D): 認証期間(秒)(U): 5 11 18 11
	Eapol 開始メッセージ(0): [法信司る
	このネットワークに対するシングル サインオンを有効にする ごっ サーロジオンの直前に実行する
	C ユーザーログオンの直後に実行する 接続の最大遅延(秒). 10 ──
	シングル サインオン中に追加のダイアログの表示を許可する
	■ このネットワークでは、コンピュークとユーザーの)資格情報を使用し た認証用に別の VLAN を使用する



有線用のポリシーを作成します。	重 グループ ポリシー管理エディタ
	ファイル(F) 操作(A) 表示(V) ヘルプ(H)
	● WARE (10) 使用 ● WARE (10) (10) ● WARE <t< th=""></t<>
	全数 セキュリティ このポリシーで定義した設定は、クライアントコンピュータのすべての LAN インターフェイスに 適用なれます。 ポリシー名(い): 「加入してYBLEのこだなード(有語)」ぶつトワークポリシー 見見用(C): サンプル見想用 ▽ クライアントで Windows ワイヤード (有線) 自動構成サービスを使用する(W)
	OK キャンセル 適用(A)
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。	新しい Vista ワイヤード (有線) ネットワーク ポリシー Properties ? × 全般 セキュリティ マ ネットワーク アクセスのために IEEE 802.1X 認証を使用可能にする(E) ネットワークの202証方法の選択(T): Microsoft (昇級された EAP (PEAP) ジビュージの35 ジビュージの35 ジビュージのの今後の接続のため、ユーザー情報をキャッシュオる(C) 詳細観史定(い). ロボットワークへの今後の接続のため、ユーザー情報をキャッシュオる(C) 詳細観史定(い). ロボークシーへの今後の接続のため、ユーザー情報をキャッシュオる(C)



認証方法で「スマートカードまた	保護された EAP のプロパティ X
はその他の証明書」を選択しま	接続のための認証方法:
す。	レダ サーバー(J単体内害を使証する(V) ブンパー(J単体内害を使証する(V) ブンパー(J単体内害を使証する(O):
「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。	信頼されたルレト語IDFA(機関(R):
(必須)	Class 3 Public Primary Certification Authority
	Microsoft Root Certificate Authority Thawte Timestamping CA
	Win2008-LH01-CA Win2008-LH01-CA Win2008-LH01-CA
	□ 新しいサーバーまたは信頼された証明規関を承認なるようユーザーに求めない(XP)
	初期工会にためなってい
	ままれの2008年(199000) スマートカードまたはその他の証明書
	「 サーバー(ご暗号化/パインドの TLV がない場合は切断する(D)
	OK #v>t2//
適切な証明書を選択します。	スマート カードまたはその他の証明書のプロパティ
	- 接続のための認証方法:
	で このコンピュータの評明書を使う(C) 「このコンピュータの評明書を使う(C)
	▶ 単地はる面の者のと思う(者を)(を)(を)(を)(を)(を)(を)(を)(を)(を)(を)(を)(を)(を
	「)次のサーバーに接続する(0):
	TarRe<1 <i>UZIV</i> ← hallenHikiRig(HV): □Class 3 Public Primary Certification Authority
	☐ Microsoft Root Authority ☐ Microsoft Root Certificate Authority
	Thawte Timestamping CA
	☑ win2008-LH01-CA
	<u> 正明書を表示する(E)</u>
	□ この接続におりのユーザー名を使べい) □ 新しいサーバーまたは信頼された証明用機関を承認するようユーザー(に求め)
	/46/KF/
	OK #*>tz#
PEAP のプロパティとして 802.1X	詳細なセキュリティ設定
の詳細設定ができます。	- IEEE 802.1× 「 「 802.1× の詳細設定を強制する(E)
	EAPOL 開始メッセージの最大数(T): (保持期間(秒)(H): 3 三 1 三
	開始期間(秒)(D): 認証期間(秒)(U):
	0
	送信する ▼
	- シングル サインオン
	○ ユーザーログオンの直前に実行する ○ ユーザーログオンの直前に実行する
	○ ユーリーロンクク加ビ(気に夹)(す)の 接続の最大遅延(秒): 10 量
	▶ シングル サインオン中に追加のダイアログの表示を許可する
	□ このネットワークでは、コンピュータンコーザーの資格情報を使用し た認識研に別の VLAN を使用する
	 ОК #ө ⁵ ,471,

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。



ボリシー名は任意です。 ボリシー名は任意です。 	無線用のポリシーを作成します。	■ グルーフ ポリシー管理エディタ
ボリシー名は任意です。 ビングロクション ビングロクション ビングロクション 第8線用のブロファイルを作成しま す。 ビングロクション ビングロクション ビングロクション ビングロクション 第3000000000000000000000000000000000000		ファイル(F) 操作(A) 表示(V) ヘルプ(H)
ボリシー名は任意です。 「シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シークション・シーション・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・シー・		
ボリシー名は任意です。 ドレット・シーンの「「「」」」」」 ボリシー名は任意です。 ドレット・シーンの「「」」」」」 ボリシー名は任意です。 ドレット・シーンの「「」」」」」 ボリシー名は任意です。 ドレット・シーンの「「」」」」」 ボリシー名は任意です。 ドレット・シーンの「「」」」」 ボリシー名は任意です。 ドレット・シーンの「「」」」」 ボリシー名は任意です。 ドレット・シーンの「「」」」」 ボリシー名は任意です。 ドレット・シーンの「「」」」」 ボリット・シーンの「「」」」」 「」」」 ボリット・シーンの「」」」」 「」」」 ボリット・シーンの「」」」」 「」」」 ボリット・シーンの「」」」」 「」」」 ボリット・シーンの「」」」」 「」」」」 ボリット・シーンの「」」」」 「」」」」 ボリット・シーンの「」」」」 「」」」」 ボリット・シーンの「」」」」 「」」」」」 ボリット・シーンの「」」」」 「」」」」」 ボリット・シーンの「」」」」」 「」」」」」 ボリット・シーンの「」」」」」 「」」」」」 ボリット・シーンの「」」」」 「」」」」」 ボリット・シーンの「」」」」」 「」」」」」」 ボリット・シーンの「」」」」」 「」」」」」」 ボリット・シーンの「」」」」」 「」」」」」 ボリット・シーンの「」」」」」 「」」」」」 ボリット・シーンの「」」」」」 「」」」」」 ボリット・シーンの「」」」」」 「」」」」」 ボリット・シーンの「」」」」」 「」」」」」 「」」」」」」」 「」」」」」」」」		■ 「「「「「「「」」(10) 「「「」」(10) 「「」」(10) 「 ■ ■ コンピュータの構成 □ 」」」(10) 「「」」(10) 「 ■ 「」」」」」」」」」」」 ● 「」」」」」」」」 ● 「」」」」」」 ● 「」」」」 ● 「」」」 ● 「」」」」 ● 「」」」 ● 「」」」」 ● 「」」」」 ● 「」」」」 ● 「」」」」 ● 「」」」」 ● 「」」」 ● 「」」 ● 「」」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」 ● 「」 ● 「」」 ● 「」」 ● 「」 ● 「」」 ● 「」」 ● 「」」 ● 「」 ● 「」 ● 「」」 ● 「」」 ● 「」 ● 「」」 ● 「」」 ● 「」」 ● 「」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」 ● 「」」 ● 「」」 ● 「」 ● 「 ● 「」 ● 「 ● 「 ● 「 ● 「
ポリシー名は任意です。 ************************************		H 2777FPalleta H Windows 6月8年
ボリシー名は任意です。 アレーション・シーンの時代の中の時代の中の時代の中の時代の中の時代の中の時代の中の時代の中の時代の		スクリフト (スタートアップ/ジャットダウン)
####################################		※ 開 アカウント ボリシー マング ウカント ボリシー
####################################		● □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
# With and State St		回 d 制限されたグループ 回 3 システム サービス
# Water State S		B 2 レジスPJ B 2 ファイル システム
####################################		10 ワイヤード (有線) ネットワーク (IEEE 0023) ボリシー
#With State of the state		ネットワークリストマネージャ ポリシー
####00********************************		■ 2011 10 4 1975 - 0 1222 2021 1 2057 -
第世史学生の1998年の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の		Symptometry (1999) Berlin Receives Protection
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		 ・
ボリシー名は任意です。 「いいにつりついたいまた」、カリンーのフリン・マーレー・ション・マールのシークリン・マール・ション・マールのシークリン・マール・ション・マールのシークリン・マール・ション・マール・ション・マール・ション・マール・ション・マール・マール・マー・マール・マール・マール・マール・マール・マール・マール・		B 〇 管理用デンブレート ローカル コンピュータから取得したボリシー 日 4. ユーザーの構成
ポリシー名は任意です。		
ポリシー名は任意です。 パレ Vesta 04 Vesta 44 Vest 44 24 - 20 04 VC 007 4 Vest 44 2- 20 04 VC 004 4 2- 20 04 VC 007 4 Vest 4- 20 04 VC 000 4		田 管理用デンプレート ローカル コンピュータから取得したポリシー
ポリシー名は任意です。 「しい いに ワイレス えり シーの おり シーの カリト (***) ジージー ひの アクセン ほう い ラー ハウ アクレス い い い い い い い い い い い い い い い い い い い		
ポリシー名は任意です。 ドレン Viela 0/4 Vb 2 3-b17 - 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 / 0.70 /		
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) <t< td=""><td>ポリシー名は任意です。</td><td>新しい Vista ワイヤレス ネットワーク ポリシーのプロパティ ? 🔽</td></t<>	ポリシー名は任意です。	新しい Vista ワイヤレス ネットワーク ポリシーのプロパティ ? 🔽
コーンですべいとないです。 コーンですべいとないですべいないからくてのワイヤレス インターフェイ いないかすべてのワイヤレス インターフェイ いないかすべてのワイヤレス インターフェイ いちいう こうない いたいの いたい いたい いたい いたい いたい いたい いたい いたい い		全般 スットワーカのアクセス許可
####################################		
Web かどうーきがと 3時間のご 19点(2) 17.71 1480月 マ クライアントロ、Windows WLAN 目動構成サービスを使用する(W) レマロファイルの崩壊で(F)明できるネットワーンに接続します: プロファイルを作成しま 18万(0): 18月のプロファイルを作成しま クビ キャンセル 18月のパロファイルを作成しま クロファイルを作成しま クロファイルを作成しま 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100%		このパリシーに定義した設定は、リライアンドコンビュータのすべてのワイヤレスインターフェイ スに適用されます。
第二日本税(1995年1995年39月20日日) 第二日本税(1995年1995年3月20日日日) 第二日本税(1995年1995年3月20日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		Vista ポリシー名(N):
調査時のご サンプバル登明 サンプバル登明 マングングングのWerdows WLAN 自動構成サービスを使用するWO 以下のブワングバルの順等で利用できるネットワージに構成しま: リロングイル 「マングイル2」 丁ロン 「マングイル2」 丁ロン 「マングイル2」 「日本 「マングーンの オャンシンル 「日本 アクロンティート 「日本 「日本 「日本 「日本 「日本 アクロンティート 「日本 「日本 「日本 「日本 「日本 「日本 「マングーンの 「日本 「日本 「日本 「ロンディーン 「日本 「日本 「日本		新しい Vista ワイヤレス ネットワーク ポリシー
アクライアントのWindows WLAN 自動構成サービスを使用する(W) 以下のプロファイルのMBでや川間できるトックーンは接します: 「************************************		説中期(C): + 1、プル語は日
マクライアントのWindows WLAN 自動構成サービスを使用する(W) 以下のフロファイルの随時で利用できるネットワーグに接続します。 「クロファイルを 「「クライアンル」 nsp01 WFA2:::ンターフ_AES 」 10000 編集(E) 110000 編集(E) 1100000 (I) 1100000 (I) 1100000 (I) 11000000 (I) 110000000 (I) 110000000000 (I) 110000000000000000 (I) 1100000000000000000000000000000000000		
() シフリンクイルの間のかいのい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		
コンティルを SDD WPA2-エンタース AES (*) 新しいフロファイル **** **** **** 通知(0)_ 編集(E)_ 新政(R) 1/2/#-K(O_ 0K **** **** **** 1 1 1 **** **** 1 1 1 1 **** **** ● **** **** **** ***** ***** ● **** ***** ******* ********* ● ************************************		▼ ジンイアンドの WINDOWS WEAN 目動時間がって人を使用する(W) 以下のプロファイルの順序で利用できるネットワークに接続します。
(学新しいフロファイル nap01 WPA2-Tンターク AES 通知(0)_ 編集(E)_ 副原除(R) 12:ボート(0 エクスポート(0 0K キャンセル 通用(A) (Bit Ux10)アイルのクロノティー のクロノティー のクロノティー のクロノティー のクロノティー のクロノティー のクロノティー アクスポート(0 0K キャンセル 通用(A) (Bit Ux10)アイル のクロノティー のクロノティー のクロノティー のクロノティー のクロノティー アクスポート(0 0F キャンセル 通用(A) (Bit Ux10)アイル のクロノティー のクロノティー のクロノティー (Sit D) (N): 100000 100000 100000 1000000 100000 100000 1000000 100000 100000 100000000 100000 100000 10000000000 1000000 1000000 100000000000 100000000 10000000 1000000000000000000000000000000000000		プロファイル名 SSID 認証 暗号(
#線用のプロファイルを作成しま す。 OK キャンセル 述の円(A) #線用のプロファイルを作成しま す。 INCASTOPACH. 05 OLDSA OK キャンセル 述の円(A) 「なんシロクタイル 05 OLDSA INCASTOPACH. 05 OLDSA JUDY 10 - 50 (1000) INCASTOPACH. 05 OLDSA JUDY 10 - 50 (1000) INCASTOPACH. 05 OLDSA JUDY 10 - 50 (1000) INTER(A) INTER(A) INTER(A) JUDY 10 - 50 (1000) INTER(A)		(空新しいプロファイル nap01 WPA2-エンターブ AES
# ###(E)###(E)####(E)##########		
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		
通知(D) 編集(E). 前隊(R) インボード(D). エクスボード(D). 0K キャンセル 0K セキュリティー 0K ロー 0K		
○K キャンセル 適用(か) ● ● ● ● す。 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		
○K キャンセル 通用(A) 無線用のプロファイルを作成しま す。 「したゴロファイルを作成しま す。 C 第続 [セキュリティ] フロファイル名(P) [第6.52075740] ネットワークな (SSID)(N): 「通加(A)」 「同P(R) 「回りワークの種類 アクセス ポイント ベース マ このネットワークが種類「いたあたき、自動的に設定する マ 優先度の高い ネットワークがきればそれに接続する(K) 「 ネットワークがプロードキャストしていない場合でも接続する(B)		
無線用のプロファイルを作成しま す。 近いゴロファイルを作成しま 事様「世キュリティ」 フロファイル名(P) 第005/107974/J 区 「コロファイル名(P) 第005/107974/J 35///0.40/- 第第第「世キュリティ」 「コロファイル名(P) 第005/107974/J 35///0.40/- 第第第(P) 「コロファイル名(P) 第005/107974/J 第第第(P) 35///0.40/- 「コロファイル名(P) 第005/107974/J 第第第(P) 35///0.40/- 35///0.40/- 「コロアイル名(P) 「第第(P) 35///0.40/- 35///0.40/- 「コロアイル名(P) 「第第(P) 35///0.40/- 35///0.40/- 「コロアイル名(P) 「第1004/P) 35///0.40/- 35///0.40/- 「コロアイル名(P) 「第104/P) 第10//P) 35///0.40/- 「コロアイル名(P) 「日本の名(P) 第10//P) 35///0.40/- 「コロアイル名(P) 「日本の名(P) 「日本の名(P) 35///0.40/- 「コロアイル名(P) 「日本の名(P) 10///0.40/-		 OK キャンヤル 適用(A)
無線用のプロファイルを作成します。 す。 ・ ・ ・		
境然 世をユリティ] プロファイル-&(P): プロファイル-&(P): プロファイル->>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	無線用のプロファイルを作成しま	新しいプロファイル のプロパティ
プロファイル-&(P) 満しなうロラテイル ネットワーク名(SSID)(N) 「ap01 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 」 「 」 「 」 「 」 「 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 』 」 』 」 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』 』	d_	接続 セキュリティ
第1日のショーラアポリ ネットワーク名(SSID(N) 「ap01 第10年(不) ネットワークの種類 アクセス ポイント ベース マ このネットワークの種類 アクセス ポイント ベース マ このネットワークが範囲内にあるとき、自動的に設定する マ 優先度の高いネットワークがあればそれば後続する(K) 「 ネットワークがブロードキャストしていない場合でも接続する(B)	. 0	プロファイル名(P):
ネットワーク名 (SSID)(N). j目加(A) î回の(A) î回の(A) î回の(A) î回の(A) î回の(A) î回の(A) î回の(A) î回の(A) ? ?		新しいプロファイル
nap01 前野奈(F) ネットワークの種類 アクセス、ポイント ベース マ このネットワークが範囲内にあるとき、自動的いに設定する マ 優先度の高いネットワークが参ればそれに接続する(K) 「ネットワークがプロードキャストしていない場合でも接続する(E)		ネットワーク名 (SSID)(N):
nap01 可が多(F) ネットワークの種類 アクセス ポイント ベース マ このネットワークが範囲内にあるとき、自動的りに設定する マ マ 優先度の高いネットワークがあればそれに接続する(K) 「ネットワークがプロードキャストしていない場合でも接続する(E)		
ネットワークの種類 アクセス ポイント ベース ✓ このネットワークが範囲内にあるとき、自動的1に設定する ✓ 優先度の高いネットワークがあればそれに接続する(K) □ ネットワークがプロードキャストしていない場合でも接続する(B)		nap01
ネットワークの種類 アクセス ポイント ベース マ このネットワークが範囲内にあるとき、自動的に設定する マ 優先度の高いネットワークがあればそれに接続する(K) ロ ネットワークがブロードキャストしていない場合でも接続する(B)		
ネットワークの種類 アクセス ポイント ベース レ このネットワークが範囲内にあるとき、自動的に設定する レ 優先度の高いネットワークがあればそれに接続する(K) レ ネットワークがブロードキャストしていない場合でも接続する(B)		
 ✓ このネットワークが範囲内にあるとき、自動的りに設定する ✓ 優先度の高いネットワークがあればそれに接続する(K) □ ネットワークがブロードキャストしていない場合でも接続する(B) 		ネットワークの種業時 アクセス ポイント ベース
 ✓ 優先度の高いネットワークがあればそれに接続する(K) □ ネットワークがブロードキャストしていない場合でも接続する(B) 		▶ このネットワークが範囲内にあるとき、自動的に設定する
□ ネットワークがブロードキャストしていないり易合でも接続する(B)		✓ 優先度の高いネットワークがあればそれに接続する(K)
		□ ネットワークがブロードキャストしていない場合でも接続する(B)



以下の設定を行います。 認証の種類:WPA2-Enterplise 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	新しいプロファイルのプロパティ × 接続 セキュリティ - 「読続」セキュリティ、シソッドの違抗(N) - 「記載(A): WPA2-Enterprise 暗号化(E): AES ネッドワークの記録方法の違択(T): Microsoft (保護された EAP (PEAP) 「記載モード(M): マーサーの両記録
	IZ証エラーの最大数(F): 「
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)	保護された EAP のプロパライ ▼ 接続のための辺辺正方法: 「サーバーの証明書を検証する(V) 「次切サーバーに接続する(O): 「 「信頼花れたルート証明規閲(R): [Class 3 Public Primary Certification Authority] ● Increaseft Root Authority ● ● Microsoft Root Certificate Authority ● ● Win2008-LH01-CA ● ● Win2007-Win348 ●
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





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)

ポート VLAN の設定 (config)# vlan 1 (config-vlan)# state active (config)# vlan 10 (config-vlan)# name NativeVLAN (config)# vlan 1000 (config-vlan)# name ManagedVLAN

MAC VLAN の設定 (config)# vlan 30 mac-based (config-vlan)# name QuarantineVLAN (config)# vlan 20 mac-based (config-vlan)# name OkVLAN

物理ポートの設定 (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

インタフェースの設定 (config)# interface vlan 1000 (config-if)# ip address 192.168.0.1 255.255.255.0

RADIUS サーバの設定 (config)# radius-server host 192.168.28.2 key "alaxala"

スタティックルートの設定 (config)# ip default-gateway 192.168.0.254

アクセスリストの設定 (config)# ip access-list extended VLAN10 (config-ext-nacl)# deny ip any any (config)# interface vlan 10 (config-if)# ip access-group VLAN10 in

RADIUS の設定 (config)# aaa authentication dot1x default group radius (config)# aaa authorization network default group radius

動的 VLAN 認証の設定



(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	
interiace vian i	
Ip address 192.108.28.200 200.200.200.0	
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

