





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 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。





目 次

はじめに	1
Network Access Protection とは	2
TS Gateway 構成	2
テスト環境	3
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	4
ターミナルサーバーの作成	5
TS Gateway のインストールと構成	6
概要	6
Windows Server 2008 のインストール	6
TS GatewayとNPS の役割のインストール	
役割の追加ウィザード	
TS Gateway の構成	
ネットワークポリシーサーバーの設定	13
AD への登録	13
クライアントの設定	17
動作確認	21
おわりに	
付録 構成の検討	



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 版で動作を確認しています。

本書は、様々な検証の中で実際に作業した結果をもとに、TS Gateway 経由で接続する際に Network Access Protection(NAP)を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、TS Gateway 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、TS Gateway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 TS Gateway 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

本書ではリモートアクセスの際にセキュリティレベルを保つための TS Gateway を利用した NAP を実現するための手順を扱います。

TS Gateway 構成

TS Gateway は Windows Server 2008 の新機能で安全にリモートアクセスを実現するための機 能です。リモートデスクトップ接続を SSL でカプセリングすることでファイアウォールの外からの アクセスを可能にしています。

この TS Gateway での接続時に NAP を利用することで、セキュリティレベルの低い PC からの接続を排除することができます。

この機能により、自宅から安全に社内にリモートデスクトップ接続でき、社内リソースへアクセスできます。

機器構成には様々なパターンが想定されますが、本書では基本となる TS Gateway とネットワ ークポリシーサーバー(NPS)を同居させる構成での手順を示します。

また、TS Gateway は SSL 通信を行うため、証明書が必要です。本書では自己発行の証明書を 使う方法を示します。

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、必要に応じてウィルス対策や自動更新といったセキュリティを保つための機能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"DC"を使用します。"DC"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 単体で考えた場合 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。



TS Gateway サービス

Windows Server 2008 が動作している"TSG"を使用します。TS Gateway は Windows Server 2008 で構築する必要があります。

ネットワークポリシーサーバーサービス(NPS) TS Gateway が稼働している"TSG"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。

ターミナルサービス

Windows Server 2008 が動作している"TS"を使用します。クライアントが実際に接続するサーバーです。

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。リモートデスクトップ接続の際に TS Gateway を指定します。

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 を利用した TS Gateway 経由の接続が行え、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

"DC"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) 必要に応じて Active Directory でユーザー作成や、GPO を構成する



OS のインストール方法、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。

ターミナルサーバーの作成

"TS"に Windows Server 2008 をインストールしてドメインに参加させます。 "TS"にターミナルサービスの役割を与えます。 アクセス権を適切に設定します。

OS のインストール方法、ターミナルサーバーの作成に関する詳細手順は、ここでは省略します。

※必ずしもターミナルサーバーが Windows Server 2008 である必要はありません。 Windows Server 2003 のターミナルサービスにも接続できます。 その場合にはクライアント側のリモートデスクトップ接続のネットワーク認証に関す る設定を適切に行う必要があります。



TS Gateway のインストールと構成

概要

TS Gateway 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 TS Gateway をインストールする ネットワークポリシーサービスをインストールする TS Gateway を構成する ネットワークポリシーサービスを構成する

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。

さらにネットワークカードを増設し、外部接続用の IP アドレスを構成します。 本書の環境では以下のようなネットワーク構成になります。

社内用ネットワーク IP アドレス : 192.168.28.4 サブネットマスク : 255.255.255.0



デフォルトゲートウェイ:192.168.28.254 DNS:192.168.28.1

外部アクセス用ネットワーク IP アドレス:192.168.1.4 サブネットマスク:255.255.255.0 デフォルトゲートウェイ:なし DNS:なし

なお、ルーティングは不要です。

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。



TS Gateway と NPS の役割のインストール

TS Gateway とNPS の役割を"TSG"にインストールします。

TS Gateway をインストールすると自動的に NPS も選択されます。

手順は以下の通りです。

役割の追加ウィザード













役割の追加ウィザート 「TS ゲートウェイの TS RAP を 下シュート マンデート マンチャン TS RAP を作成 作成」ページで「ユーザーがネ ットワーク上の任意のコンピュ 開始する前に ユーザーが、のTSゲードウェイサーバー毎日で有続をできるネットワークリソースを指定する以は、T<u>S PAP を</u>作 気する心理があります。「変更したユーザーブループのメリルだけが、このリソースへの理読を指すでくます。TS RAP のユーザーを増取した5、TS RAP の名前を付け、ユーサーが発読できるネッドワークリソースを指定する 必要があります。 サーバーの役割 ターミナル サービス ータに接続できるようにする」を 選択し、「次へ」をクリックしま 役割サービス サーバー認証証明書 承認ホリシー TS RAP の名前を入力(E) [TS_RAP_01 す。 TS ゲートウェイのユーザー グ この TS RAP を使用してアクセス可能なコンピュータを指定 、ユーザーが次のグループのコンピュータを指定: 、ユーザーが次のグループのコンピュータにのみ接続できるようにする(U) TS RAP トワーク ポリシーとアク マニザーがネットワーク上の任意のコンピューダに接続できるようにする(W) このオジョンを確認すると、サモートデスクトゥブ経由でアクセス可能な任意のコンピューダにコーザーが接続で きるよどになります。 役割サービス Web サーバー (IIS) 役割サービス 確12 通行状况 ※接続できるターミナルサーバ ーを限定することも可能で R TS RAP OPERTO IT IS す。 く前へ(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 👔 役割サービスの選択 で「ネットワークポリシーサーバ 一」のみにチェックが入っている 開始する約に ネットワーク ポリシーとアクセス サービス にインストーン 役割サービス(E) いまりサービスを選び 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 ことを確認し、「次へ」をクリック キットワーク ボジー サーバー (NPS) 1 使用すると、クライアントの正常性、特 経費家の記242、複紙要求の承認にで する種類を1をのネットワーク アクセス イ リシーを1作成および注創できます。また NPS では、ネットワーク アクセス保護 サービス します。 役割サービス \triangleright DHCP サーバー 正常性型绿相関 HCAP (Hose (NAP)、クライアントの正常性ポリシーの 作成と基制、および対策テクノロジを展 間で失ます。 ネットワーク接続バインディング IPv4 DNS L的定 IPv4 WINS L的定 DHOP 23-7 DHOPv6 ステートレス モード IPv6 DNS 脱定 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 <前へ(P) 次へ(N)> インストール(D) キャンセル 「Web 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。 インストールする役割の詳細が表示されますが、何も変更せず「次へ」をクリックします。 役割の追加ウィザード 「インストールオプションの確 1ンストール オブションの確認 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」 開始する前に 次の役割、役割サービス、または機能をインストールするには、「インストール」をクリックしてください。 をクリックします。 サーバーの(役割) ターミナル サービス ③ 次の 2 個の情報メッセージ 役割サービス サーバーIZIIIIII明書 (1) インストールの完了後に、このサーバーの両記動が必要になる場合があります。 ターミナル サービス TS ゲートウェイ サーバー証明書: 接続承認ポリシー 名前: 承認約シー 自己署名入りの証明書を作成 TS ゲートウェイのユーザー グ. TS_CAP_01 パスワード Administrators, DOMAIN28#Do 名前: 認証方法: アクセスが平可されたグループ: リンース承認ポリシー 名前: アクセスを許可する対象: TS CAP TS RAP ネットワーク ボリシーとアクセス サービ. 役割サービス TS_RAP_01 ネットワーク上の任意のコンピュータ Web サーバー (ES) ◇ ネットワーク ポリシーとアクセス サービス ネットワーク ポリシー サーバー 役割サービス ネット・シーク ホッシー マーハー ● Web サーバー(IIS) ① Windows システム リソース マネージャ (WSRM) と、OPU 使用率の最適化のための活用方法のIIT 種 確認 結果 Web サーバー HTTP 基本相能 都特なコンテンツ R -この情報を印刷、電子メールで送信、または保存 <約へ(P) ※へ(20)> インストール(D) キャンセル 「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 TS Gateway と NPS がインストールされました。



TS Gateway の構成

TS Gateway の初期設定を行います。

スタートをクリックして「管理ツール」-「ターミナルサービス」-「TS ゲートウェイマネージャ」を			
<u></u>			
サーバー名を右クリックし、プロパラ 「SSL 証明書」タブで「SSL 暗号 化用の自己署名証明書を作成 する」を選択し、「証明書の作 成」ボタンをクリックします。	- イを表示します。 TSG プロパティ 全級 SSL 証明書 TS CAP ストア サーバー ファーム [監査 SSL プリッジ] TS ゲートウェイ サーバーと接続テクライアントの間のなっトワージ通信をセキュリティで保護す るには、Secure Sockets Layer (SSL) 証明書が必要です。 ・ 次の証明書が TSG にインストールされています 発行売 TSG domain28 local 発行元 TSG domain28 local アレッシュージョン・シューシールされています 正明書の作成(E)_ で SSL 暗号化用の既存の証明書を選択する (推奨)(S) TS ゲートウェイ サーバー TSG で使用可能なサーバー証明書を表示するには、証証明書 の参照1をジリックして(ださい。 正明書の参照(W)_		
「自己署名証明書の作成」画面	IS ゲードウェイの証明論の詳細を表示します。 OK キャンセル 道用(点) 自己署名品ぞ明書の作成 21 ×1		
でクライアントからアクセスされ るときに使用する適切な名前 (FQDN)を入力します。	証明書の名面 次の共通名 (CN) で自己署名証明書を作成する [tag.domain:23 internet		
ファイルの保存先を確認し、 ート証明書を格納する」のチェッ クが入っていることを確認して 「OK」ボタンをクリックします。	auf9月前辺3821 カライヤントからこの TS ゲートウェイ サーバーに接続するには、そのルート国時書を手動でウライアントに配布す など要が扱わます。ルートは世界戦に大のライレンドルに経済することをお勧助します: C ¥Users¥administator DOMAIN/28¥Documents アケイル名 C ¥Users¥administator DOMAIN/28¥Documents¥TSG.cer 基即得書を影りの場所に格納するには、[参照]をグリックして影りの場所を選択してください。 ア ルート版IP用書を格約する(S) TS ゲードウェイの証明書の詳細を表示します。		
	OK ++>ZU		
証明書が作成された旨のメッセ ージが表示されるので「OK」をク リックします。	TS ゲートウェイ X TS ゲートウェイ(によって自己署名証明書が正しく作成されました。証明書は次の ファイルに格納だれます。 C×Users¥odministrator DOMAIN28¥Documents¥TSG.cer OK		
「OK」をクリックしてプロパティを閉じます。			

これで、TS Gateway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「ネットワークアクヤス係	ミ護(NAP)を選択し、「NAP を構成する」をクリックしウィザ
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
続方法の選択パージが開いた	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「ターミナルサー	ት _ግ ነርር. ከ ጀም ውታ ነት
ビスゲートウェイ(TS ゲートウェ	↑クアレーン教徒のの方法・ NAP 対応の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
インを選択します。「ポリシー名」	するには、ウィザードを再度実行してください。
には自動的に「NAP TS ゲートウ	[ጶーミナル サービス ゲートウェイ (TS ゲートウェイ)
エイ」が入ります。「次へ」をクリ	オリシー名: このウィザードで作成されるポリシーには、下記の文字列が名前の一部として使用されます(T)
ックします。	このままだH19のことも、東足9のこともにきます。 NAP TS ゲードウェイ
	追加要件: NAP をセットアップする(ゴニー)含tmのアケッコンを実行する。必要指本がます。 下のリンクをクリックリーアー)含tmの
	NAP 裏任を表示してください。 当の要任(U)
	k
	前へ(P) 先7(F) キャンセル
「TS ゲートウェイを実行する	- NAP を構成する X
NAP 強制サーバーの指定」ペー	TS ゲートウェイを実行する NAP 強制サーバーの指定
ジでは特に何も設定せず、「次	
へ」をクリックします。	TS ゲードウェイ がローカル マンピュータ 上でのみ実行されている場合は、「次へ」 あクリックします。 TS ゲードウェイ
	が1 台以上のリモート コンピュータ上で実行されている場合は、「追加」をクリックし、谷リモート TS ゲートウェイ サーバーを追加します。
	TS ゲートウェイ サーバー:
	前時余(四)
	Ν
	r/2
	前へ(P) 次へ(N) 完了(F) キャンセル



「クライアントデバイスのリダイレ クトと認証方法の構成」ページ で適切なリダイレクト設定を行い ます	NAP を構成する × シライアント デバイスのリダイレクトと認証方法の構成
ま9。 認証方法は「パスワードを許可」 のみがチェックされている状態 を確認し、「次へ」をクリックしま す。	 下5 ゲートウィイ経由では継続するウライアントにオレクライアントデバイスのリダイレクトを有効にするか無効にできるか = ブパイスのリダイレクトは、信頼なれジモート、クライアントについてのみ無効してきます。 = ブパイスのリダイレクトは、信頼なれジモート、クライアントについてのみ無効してきます。 = ブパイス リダイレクトは、信頼なれジモート、クライアントについてのか用がしてきます。 = ブパイス リダイレクト 「リモート クライアント上のすべてのデバイスのリダイレクトを無効にする(D) 「リモート クライアント上のすべてのデバイスのリダイレクトを無効にする(D) 「リモート クライアント上のすべてのデバイスの増加のリダイレクトを無効にする(D) 「リモート クライアント上のすべてのデバイスの増加のリダイレクトを無効にする(D) 「リモート クライアント上のすべてのデバイスのリダイレクトを無効にする(D) 「リモート クライアント」とのすべてのデバイスのリダイレクトを無効にする(D) 「リモート クライアント」との次のデバイスの増加のリダイレクトを無効にする(S) 「レディイク) 「レディイク) 「ジワブル ディト(C) 「ジワブル ディト(C) 「ジワブル ディト(C) 「シブワブル ディト(C) 「シブート クラトをおもす(M) 「ハスワートを計す(M) 「ハスワートを計す(M)
	<u> 前へ(P)</u> <u> 次へ(N)</u> 元ア(F) <u> キャンセル</u>
「ユーザーグループとコンピュー タグループの構成」ページでは TS Gateway 経由でアクセスを 許可するユーザーグループを指 定し、「次へ」をクリックします。	NAP を結成する × ユーザーグループとコンピュータグループの構成 ・ アーザーグループ、またはオブションでコンピュータグループにアクセスを許可する場合は、「自知」をグリックし、目がの グループを指定します。 ・ コンピュータグループ:(オブションでコンピュータグループにアクセスを許可する場合は、「自知」をグリックし、目がの グループを指定します。 ・ コンピュータグループ:(オブション) ・ コンピュータグループ:(オブション) ・ コーザーグループ:(4ズ狗) ・ DOMAIN284Domain Users ・ ユーザーの追加(U) ・
	<u>前へ(P)</u> <u>次へ(N)</u> <u>売了(F)</u> <u>キャンセル</u>
「NAP 正常性ボリシーの定義」 ページではデフォルト設定のま ま「次へ」をクリックします。	NAP を構成する XAP を構成する XAP を構成する XAP 正常性ポリシーの定義 インストールされているシステム正常性検証ツールの一覧です(S) Cの正常性ポリシーで強制するシステム正常性検証ツールだけを選択してください。 Sán X
	L ₃
	NAP に適合しないクライアント コンピュータのネットワーク アクセス制限: の リモート デュクトップを実行していスカーミナル サーバーキキバナ・ピューカル ハルトニノマ・ル マクトゥッキルホイレキオ
	C リモート デスクトップを実行しているターミナル サーバーまたはコンピュータへのクライアント アクセスを許可します。
	<u> 前へ(P)</u> <u> 次へ(N)</u> 完了(F) <u> キャンセル</u>



「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	NAP を構成する NAP 強制ポリシーおよび RADIUS クライアント構成の完了	X
て、ウィザードを終了します。	次のポリシーが正常に作成され、次の RADIUS クライアントが正常に構成されました。 ・ 既定のブラウザで構成の単純色を表示するには、構成の単純目をクリックしてださい。 ・ 相応気変更するには、加入「をクリックしてださい。 ・ 本構充気化学してのウイザードを閉じるには、した了」をクリックしてください。 ・ まな化ポリシー: ・ 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	
	NAP IS ゲードクロイ ス トワーク 水りうー: NAP IS ゲードウエイ 非単純 NAP IS ゲードウェイ NAP 非対応:	
	4.種点式の直接報(○) []]	\$
		*ンセル

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 TS ゲートウェイ準拠
- NAP TS ゲートウェイ非準拠

接続要求ポリシー

NAP TS ゲートウェイ

ネットワークポリシー

- NAP TS ゲートウェイ準拠
- NAP TS ゲートウェイ非準拠
- NAP TS ゲートウェイ未対応

セキュリティ正常性検証ツールの設定

「ネットロークポリシーサーバ			
	多ネットワーク ポリシー サーバー	_0×	
ー」のコンソールで「NAP(ローカ	77イルE 操作A 表示(2) ヘルプ(B)		
」 い 」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。		 2. 単ム投資を指定できます。SHV 人上通知します。 	
	<u>ار ا</u>		
「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	Windows 102319742あれは1219-か ()メ Windows Veta [windows 20] () とびて後辺を使用して、Windows 104319742米世報日ワールボリンーを定義します。ここで選邦した内容により、ホットワールで提供するウェイアント コンピューシの原件が定義され また。 () EXEMPLE () アンドプロサール () アメリカワロール () アメリカロール () アメリカロール () アメリカロール ()
「ファイアワオール」と「自動更 新」だけチェックを入れた状態に	
	- 2014年2月1日 「2014年2月1日第7月9月-1日、本時期度合」 「2014年2月1日第7月1日日の日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本
していて」をノリノノレてメイノロ	自動更新 〒 自動更新が執動(1)
クを閉じます。	
	α α α α α α α α α α α α α α
再び「Windows セキュリティ正常性材	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

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。

「ファイル名を指定して実行」に regedit と入力し、レジストリエディタを起動します。					
以下のキーを変更します。 HKEY_LOCAL_MACHINE ¥SOFTOWARE ¥Microsoft ¥Terminal Server Client ¥TrustedGateways					
名前:GatewayFQDN	び レジストリエディタ ファイル(F) 編集(E) 表示(V) お	気に入り(A) ヘルプ	(н)		- • •
種類:REG_MULTI_SZ データ: <ts fqdn="" gateway="" の=""></ts>	TristeGateways TristeGateways TristeGateways Trig Transaction Server TV System Services uDRM URAP Device Host Virtual Machine VirtualStudio WAB WBEM Windowsi	名明 会明 会)(版定) 図 Contrway FQD	相助 REG_SZ REG_MULTI_SZ	データ (他の脱充なし) tsg.domain28.internet	
※レジストリに TS Gateway の FQDN が記載されていないと 接続できません。	Windows Defender Windows Desitop Search Windows Media Device Manager II Windows Media Device Manager II Windows Media Player NSS Windows Messaging Subsystem Windows Resaging Subsystem Windows Resaging Subsystem Windows Resaging Subsystem Windows Messaging Subsystem Windows Messagin	NEWSOFTWAREWMIC	rosoft¥⊺erminal Serve	er Client∔TrustedGateways	



TS Gatewayの設定中に作成した自己署名証明書を何らかの方法でクライアントPC にコピー					
します。 証明書をダブルクリックして開きます。					
「証明書のインストール」をクリッ					
クします。					
	□ 1973年の前報 この CA ルート証明書は信頼されていません。信頼を有効にするには				
	この証明書を信頼されたルート証明確則のストアにインストールしてくた さい。				
	発行先: tsg.domain28.internet				
	発行者: tsg.domain28.internet				
	有效期間 2008/03/02 から 2008/09/01				
	ОК				
証明書のインポートウィザードが開き	始されますので、「次へ」をクリックします。				
「証明書ストア」の選択画面で	□ 証明書のインボート ウィザード				
「証明書をすべて次のストアに配	証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。				
直する」を選択し、「参照」ホタン をクリック」 ます					
	 ● 証明書の種類に基づいて、自動的に証明書ストアを選択する(U) 				
	◎ 証明書をすべて)太のストア(:配置する(P) 証明書をフトア。				
	(言類されたルート語取用規則) 参照(R)				
	N				
	1月月末入トアの詳細を表示します しま				
│ │「信頼されたルート証田機関↓を					
選択し「OK」をクリックします。	証明書ストアの選択				
	(使用する編集の用書人トノを)離れてしてたといいで)				
	- 18人 - 10日 - 1110 - 110				
	- - - - - - - - - - - - - -				
	- 18和C40C0 Nat				
	OK #+>セル				
ウィザードを続けると 信頼されたル					
「OK」をクリックします。					
さらに続けると正しくインストールされ	れた旨が表示されます。				
ファイル名を指定して実行から mmc を起動します。					



「ファイル」-「スナップインの追加 と削除」を選び、「証明書」-「ユ	************************************			
ーサー」と「証明書」-「コンビュー タ(ローカル)」を追加します。	□ コン・ホルート ● 目初時書 (U-カル) エビュージ	名前 〇田印書 - 現石のユーザー 〇田印書 ゆったら コンピュージ		
「証明書-現在のユーザー」の信頼されたルート証明機関内に格納された TS Gateway の証 明書をコピーし、「証明書(ローカルコンピュータ)の信頼されたルート証明機関内に貼り付け ます。				

必要に応じてクライアントの hosts ファイルを編集し、TS Gateway の FQDN に対して名前解決 が行えるように設定します。

これで一通りの設定が完了しました。

クライアントが TS Gateway を経由してターミナルサーバーに接続するには以下の手順を実行します。









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。

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ターミナルサーバーに 接続できません。



すべての条件をクリアしていれば正しくターミナルサーバーに接続できます。

NAP を利用した TS Gateway 接続の場合、接続時に正常性のチェックを行っています。 接続中にファイアウォールを無効に変更しても接続が切断されるわけではありません。



おわりに

ここまで見てきたように、TS Gateway と 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が社内 LAN に接続することを防ぐことができます。

NAPには様々な構成方法がありますが、本書で取り上げたTS Gateway構成はNAPの構成方法の一つというよりはTS Gatewayの拡張といえる方法です。

よって、その他の NAP とは考え方も異なり、「修復する」という考え方はありません。あくまでも TS Gateway を利用して社内にアクセスする際に最低限のセキュリティレベルをクリアしたクライ アントだけにアクセスを制限するための機能です。

TS Gateway と NAP を連携させるにはクライアント側で行う作業が非常に多く、「手軽に」接続で きるものではありません。よってリモートアクセスが必要で且つこれだけの設定が行えるユーザ 一のみに接続を許可することになります。

社内ネットワークを守るための NAP として全社的に 802.1X 構成や IP Sec 構成の NAP を導入 しつつ、さらに社外からのアクセスの際にも TS Gateway と NAP を組み合わせて穴を作らないと いう考え方で全体を検討してください。

平成20年3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



付録 構成の検討

本書では検証環境でTS Gatewayの動作を確認することを目的に、シンプルな構成での設定手順を示しています。

しかしながら、実環境ではこのようなシンプルな構成は考えにくいと思われます。

例えば下記のような構成ならば現実的な構成に近いと思われます。



しかしながらこの構成の場合は様々な注意点が存在します。

・ドメインへの参加

TS Gateway で NAP を利用する場合、ユーザーグループでの制御が必須になります。 TS Gateway が DMZ に配置された場合、ワークグループ環境での運用がほとんどと思われま すが、この場合にはドメインのユーザー、グループでアクセスを制御できません。 逆にドメインに参加させた場合には攻撃を受けた場合のリスクが高くなります。

・RADIUS プロキシ



NPS には RADIUS プロキシの機能があり、社内のドメインに参加している NPS に RADIUS 要求を転送し、認証させる方法も検討する必要があります。

しかしながら、この構成での設定は非常に複雑であり、実現は困難です。

・アカウントの二重管理

結果的に上記の例では TS Gateway のマシン上で NPS も動作させ、NAP 構成ウィザードを 利用して TS Gateway と NAP を連携させることになります。

この場合、TS Gateway に対するアクセス許可を TS Gateway のローカルユーザー/グループ で制御し、最終的に接続するターミナルサーバーに対するアクセス許可はドメインのユーザ ー/グループで行うことになります。

つまり、アカウントを二重に管理する必要があります。

·証明書

クライアント側に信頼されたルート証明書が存在しないと SSL 通信が行えません。公的な証明機関からの証明書の取得を検討してください。

·名前解決

インターネット経由で接続するためには公開された DNS 上にホスト名が登録されている必要 があります。

ここで取り上げた例の他にも様々な構成パターンが存在します。それぞれに長所と短所、さら に葉注意点が存在しますので、実際の環境を考慮し、最適な構成を選択してください。

