

Windows Server 2008 NAP 設定手順書 TS Gateway 編

～テスト環境での TS Gateway 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 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	3
環境作成手順	3
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	8
役割の追加ウィザード	8
TS Gateway の構成.....	12
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.....	22
付録 構成の検討.....	23

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 でカプセル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。

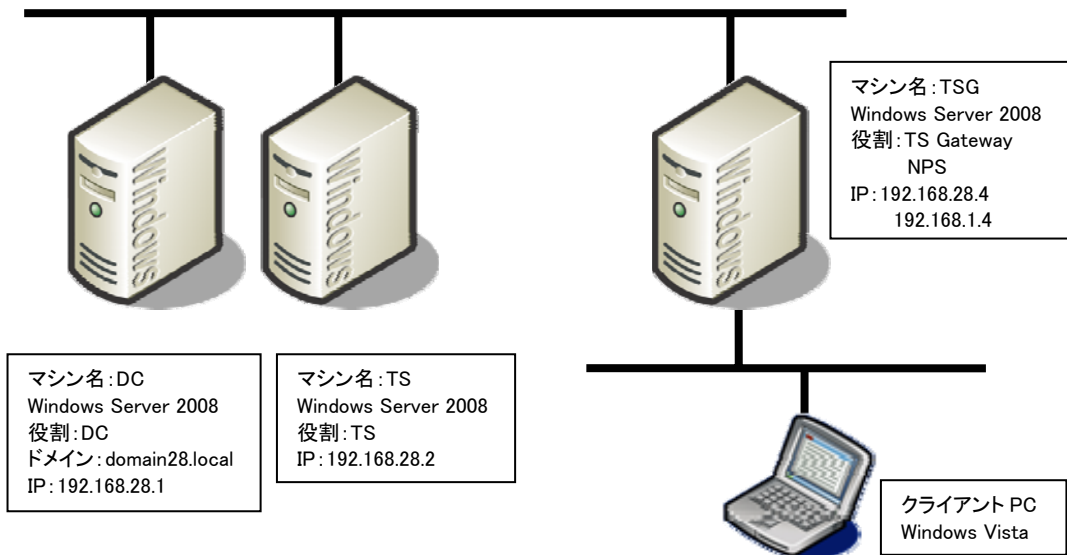
その他の方法に関してはそれぞれの設定手順書を参照してください。

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。

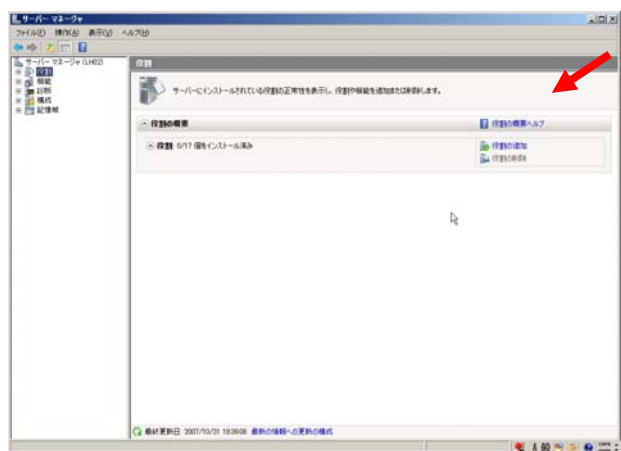
手順は以下の通りです。

役割の追加ウィザード

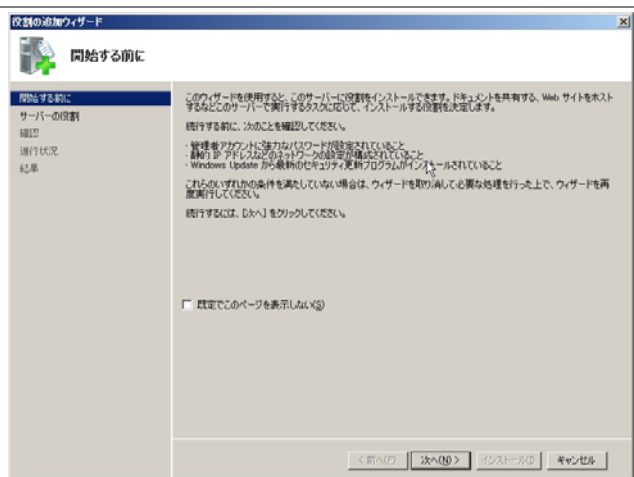
「Start」をクリックして「管理ツール」-「サーバーマネージャー」を起動します。



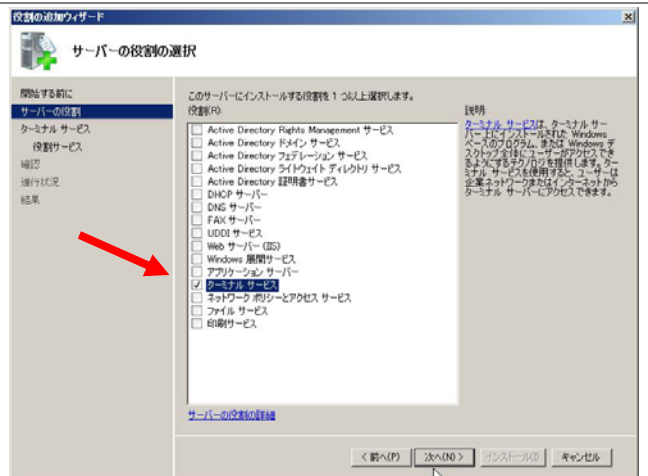
「役割の概要」を展開して「役割の追加」をクリックします。「次へ」をクリックします。



「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

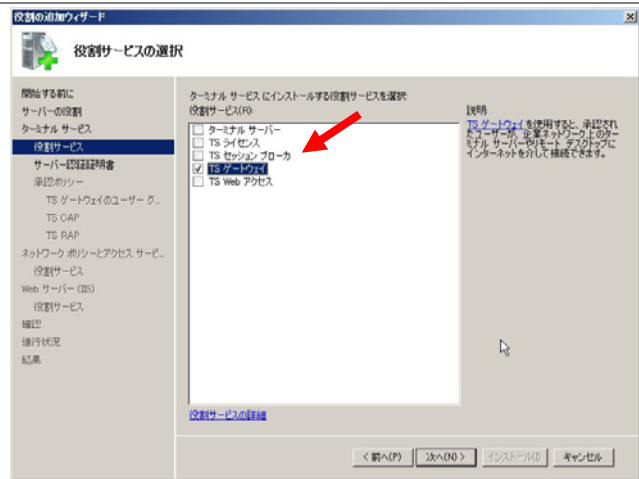


「サーバーの役割の選択」ページが開くので「ターミナルサービス」にチェックを入れて「次へ」をクリックします

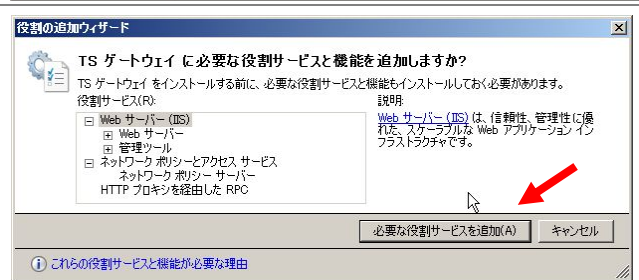


「ターミナルサービス」に関する説明が表示されます。「次へ」をクリックします。

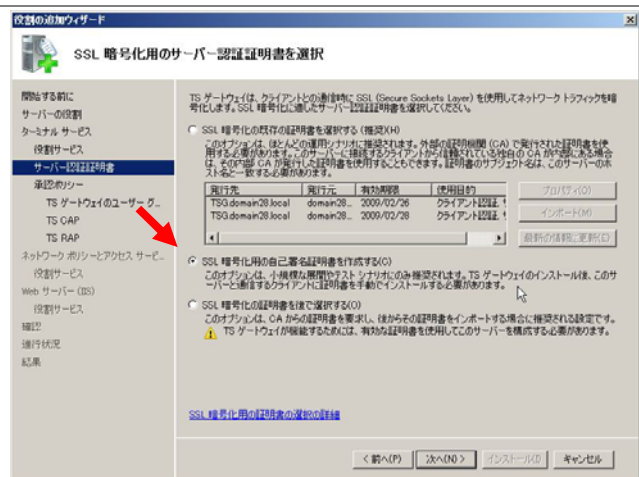
「TS ゲートウェイ」を選択します。

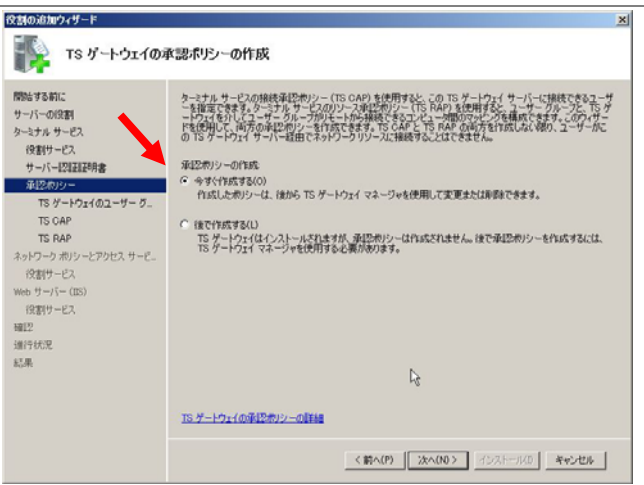
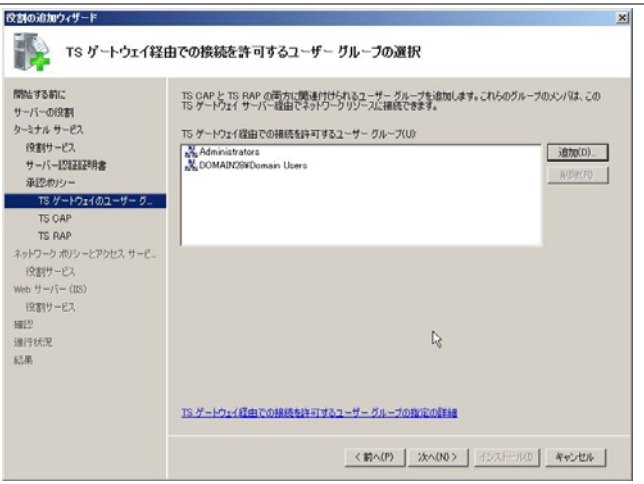
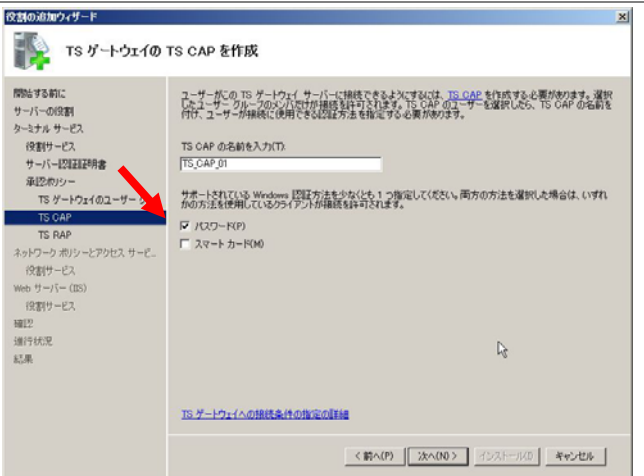


TS ゲートウェイに必要なサービスを同時にインストールするか尋ねてきますので、そのまま「必要な役割サービスを追加」をクリックします。



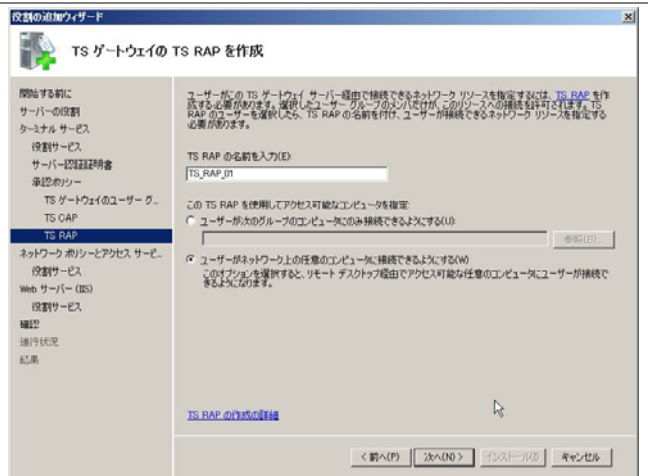
「SSL 暗号化用の自己署名証明書を作成する」を選択し、「次へ」をクリックします。



<p>「TS ゲートウェイの承認ポリシーの作成」ページにて「今すぐ作成する」を選択し、「次へ」をクリックします。</p>	
<p>「TS ゲートウェイ経由での接続を許可するユーザーグループの選択」ページで適切なグループを追加します。</p>	
<p>「TS ゲートウェイの TS CAP を作成」ページで「パスワード」のみが選択されていることを確認し、「次へ」をクリックします。</p>	

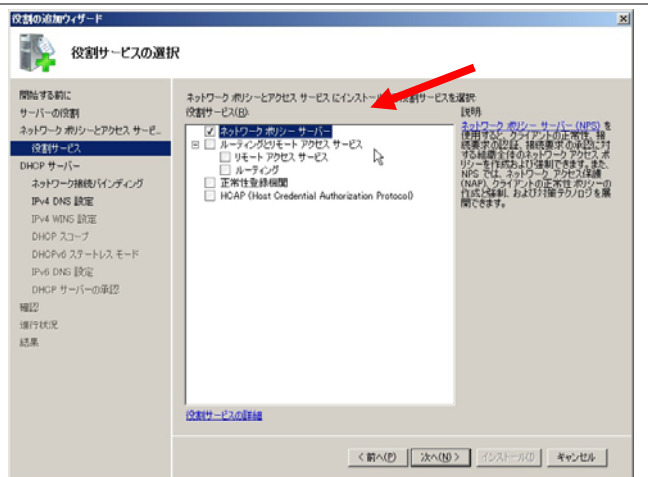
「TS ゲートウェイの TS RAP を作成」ページで「ユーザーがネットワーク上の任意のコンピュータに接続できるようにする」を選択し、「次へ」をクリックします。

※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。



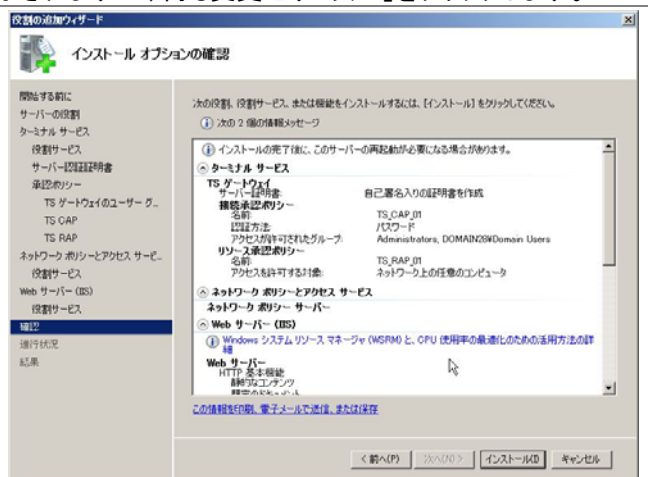
「ネットワークポリシーとアクセスサービス」に関する説明が表示されます。「次へ」をクリックします。

「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」のみにチェックが入っていることを確認し、「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。

「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」をクリックします。

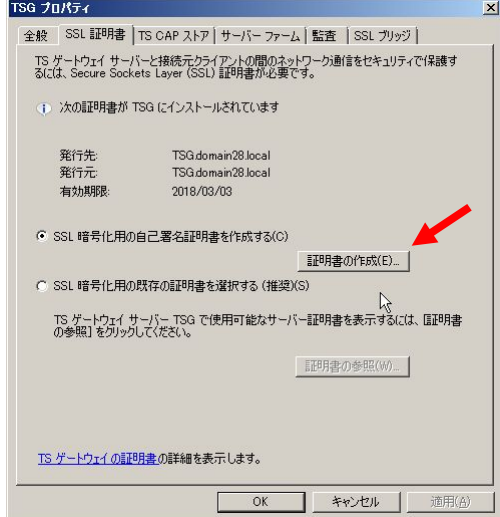
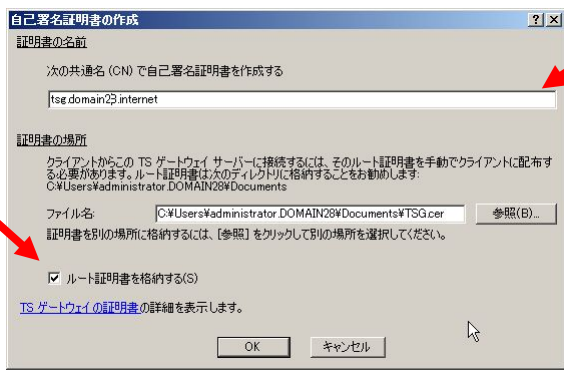



「インストールの結果」画面でインストールが正常に完了したことを確認したら、「閉じる」をクリックして、「役割の追加ウィザード」を終了します。続いて「サーバーマネージャー」も閉じます。

以上で 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。

<p>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」をクリックします。</p>	
<p>サーバー名を右クリックし、プロパティを表示します。</p>	
<p>「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。</p>	
<p>「自己署名証明書の作成」画面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。ファイルの保存先を確認し、「ル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。</p>	
<p>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。</p>	
<p>「OK」をクリックしてプロパティを閉じます。</p>	

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。

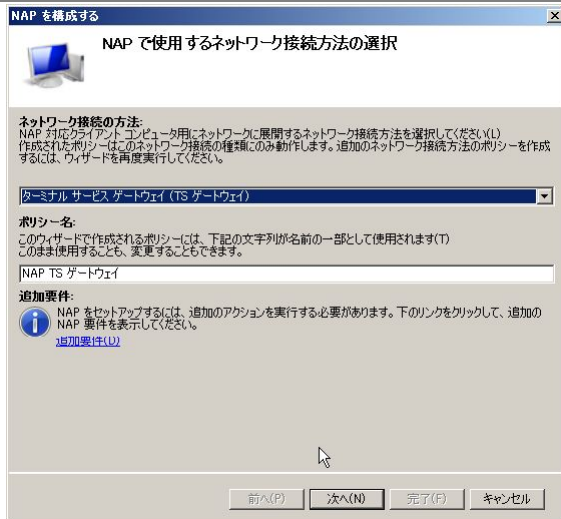
AD への登録

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。

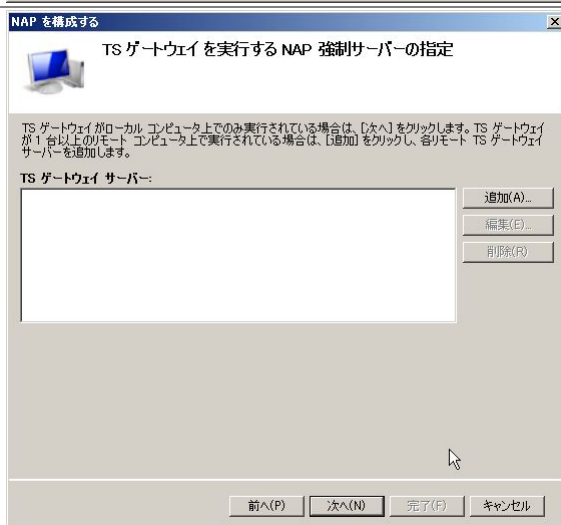
NAP 構成ウィザード

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「ターミナルサービスゲートウェイ(TS ゲートウェイ)」を選択します。「ポリシー名」には自動的に「NAP TS ゲートウェイ」が入ります。「次へ」をクリックします。



「TS ゲートウェイを実行する 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。



「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。
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。



NAP を構成する

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

TS ゲートウェイ経由で接続するクライアントは、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するかを指定し、接続時のクライアントが使用できる認証方法を 1 つ以上選択します。セキュリティ警告

- デバイスのリダイレクトは、信頼されたリモート クライアントについてのみ無効にできます。
- スマート カードとパスワードの認証を両方選択した場合、どちらか 1 つを接続に使用できます。

デバイスリダイレクト

- 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有効にする(E)
- スマート カード以外の、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 クライアント上の次のデバイスの種類のリダイレクトを無効にする(S)
 - ドライブ(R)
 - クラップボード(C)
 - フロッピー(F)
 - シリアル ポート(L)
 - サポートされているプラグ アンドプレイ デバイス(G)

認証方法

- スマート カードを許可(M)
- パスワードを許可(W)

前へ(P) 次へ(N) 完了(F) キャンセル

「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 を構成する

ユーザーグループとコンピュータグループの構成

ユーザー グループ、またはオプ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、[追加] をクリックし、目的のグループを指定します。

コンピュータ グループ: (オプション)

コンピュータの追加(D)...
削除(R)

ユーザー グループ: (必須)

DOMAIN20\Domain Users
ユーザーの追加(U)...
削除(E)

前へ(P) 次へ(N) 完了(F) キャンセル

「NAP 正常性ポリシーの定義」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

NAP 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)
こ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。

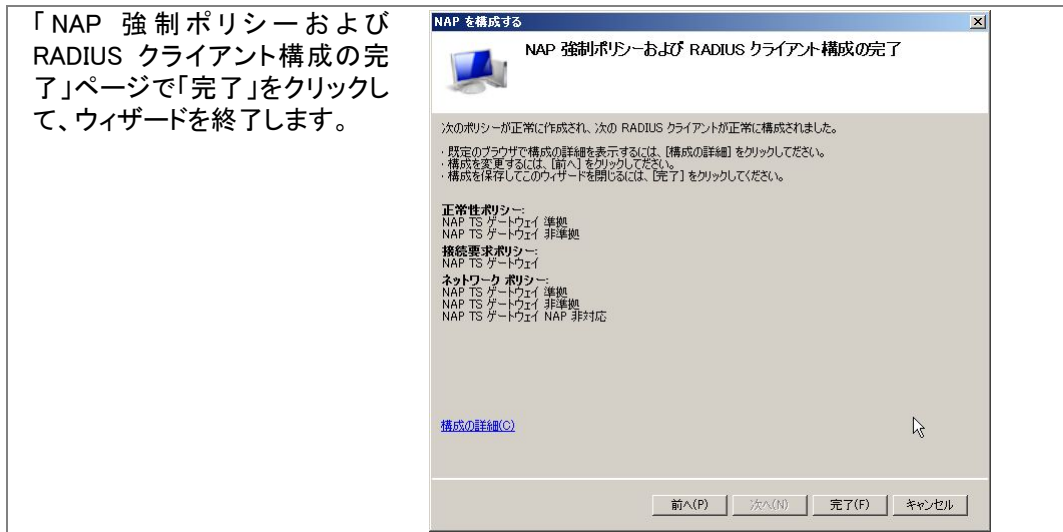
名前

- Windows セキュリティ正常性検証ツール

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:

- 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 アクセスを拒否します。
- 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。

前へ(P) 次へ(N) 完了(F) キャンセル



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

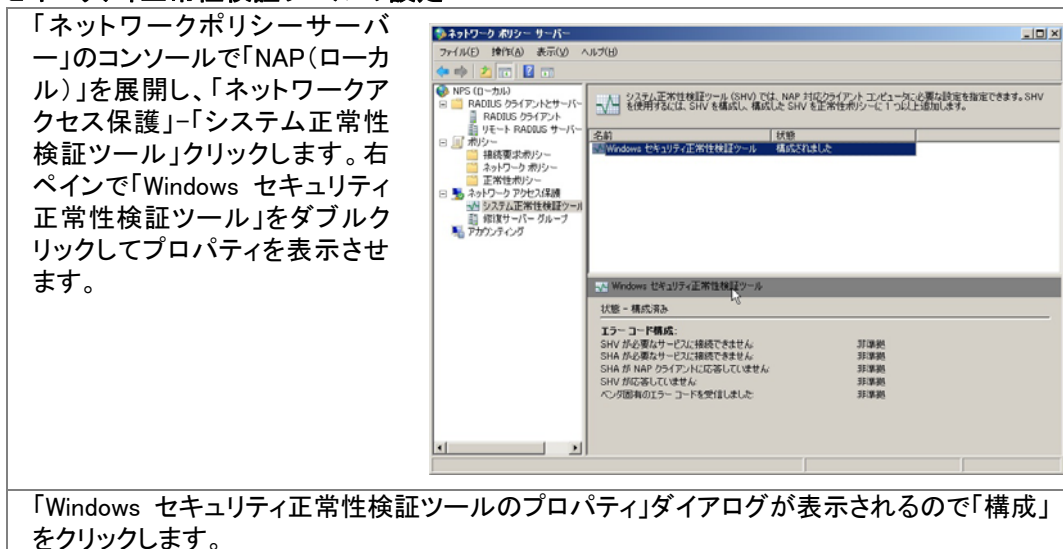
接続要求ポリシー

- NAP TS ゲートウェイ

ネットワークポリシー

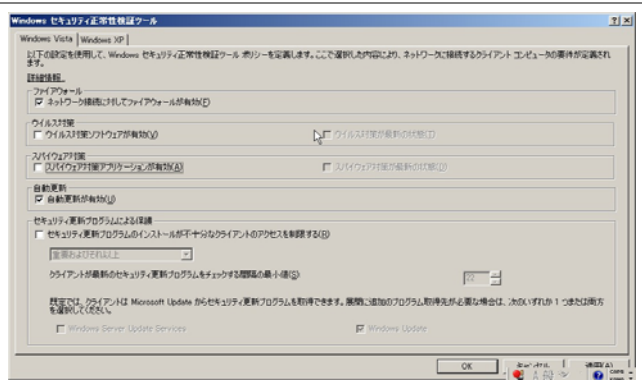
- NAP TS ゲートウェイ準拠
- NAP TS ゲートウェイ非準拠
- NAP TS ゲートウェイ未対応

セキュリティ正常性検証ツールの設定



「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。

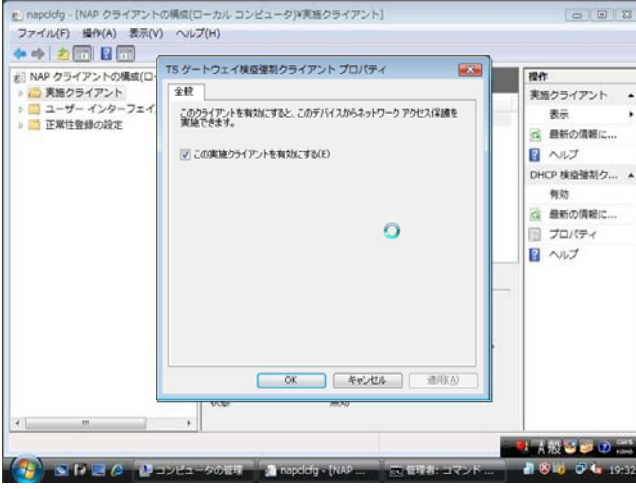
クライアントの設定

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。

「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「TS ゲートウェイ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。
「TS ゲートウェイ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。

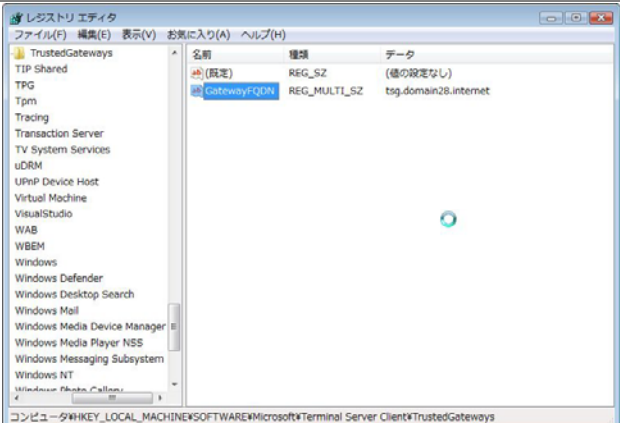
「コンピュータの管理」-「サービス」から「Network Access Protection Agent」のプロパティを表示して「全般」タブで「スタートアップの種類」を「自動」にし、「開始」ボタンをクリックしてサービスを開始させます。

「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
¥SOFTWARE
¥Microsoft
¥Terminal Server Client
¥TrustedGateways

名前: GatewayFQDN
種類: REG_MULTI_SZ
データ: <TS Gateway の FQDN>

※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。



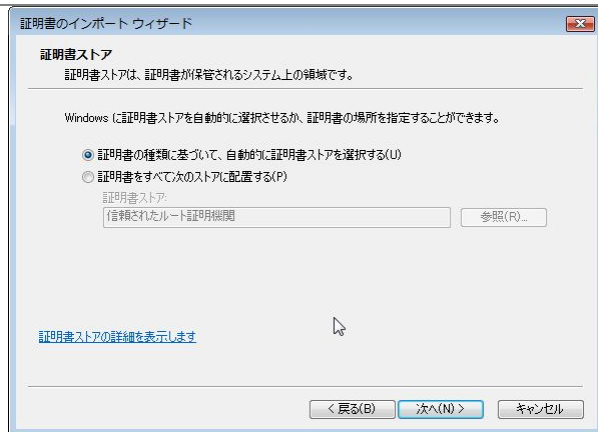
TS Gateway の設定中に作成した自己署名証明書を何らかの方法でクライアント PC にコピーします。
証明書をダブルクリックして開きます。

「証明書のインストール」をクリックします。

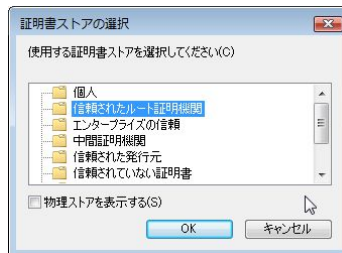


証明書のインポートウィザードが開始されますので、「次へ」をクリックします。

「証明書ストア」の選択画面で「証明書をすべて次のストアに配置する」を選択し、「参照」ボタンをクリックします。



「信頼されたルート証明機関」を選択し「OK」をクリックします。

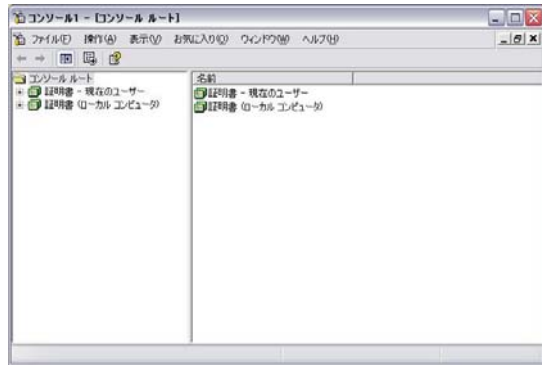


ウィザードを続けると、信頼されたルートとしてインストールしていいか確認されますので、「OK」をクリックします。

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」-「ユーザー」と「証明書」-「コンピュータ(ローカル)」を追加します。



「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。

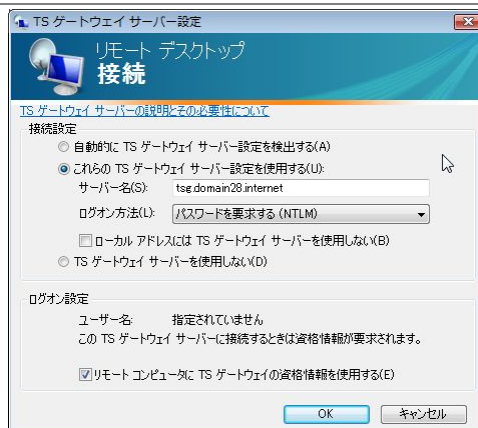
これで一通りの設定が完了しました。

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。

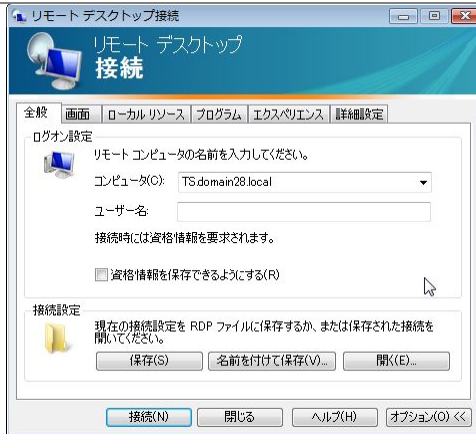
「スタート」メニューから「リモートデスクトップ接続」を起動します。
「オプション」ボタンをクリックし、「詳細設定」タブを選択します。
「任意の場所から接続する」欄にある「設定」ボタンをクリックします。

「TSゲートウェイ設定」画面が表示されます。
「これらの TS ゲートウェイサーバー設定を使用する」を選択し、サーバー名に TS Gateway の FQDN を入力します。
「OK」ボタンをクリックします。

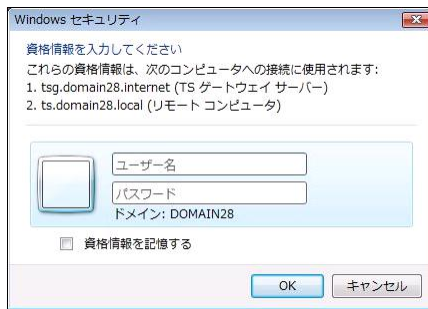
※証明書と同じ名前を指定しないと接続できません。
レジストリに記載した名前と同じでないと接続できません。



「リモートデスクトップ接続」画面に戻りますので、接続するターミナルサーバーのコンピュータ名を入力し、「接続」ボタンをクリックします。



適切なユーザー名とパスワードを入力します。

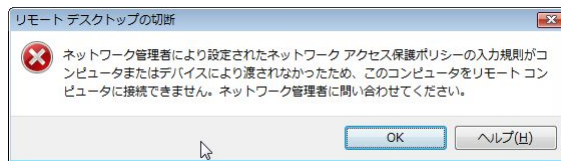


ターミナルサーバーに接続されます。

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ー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

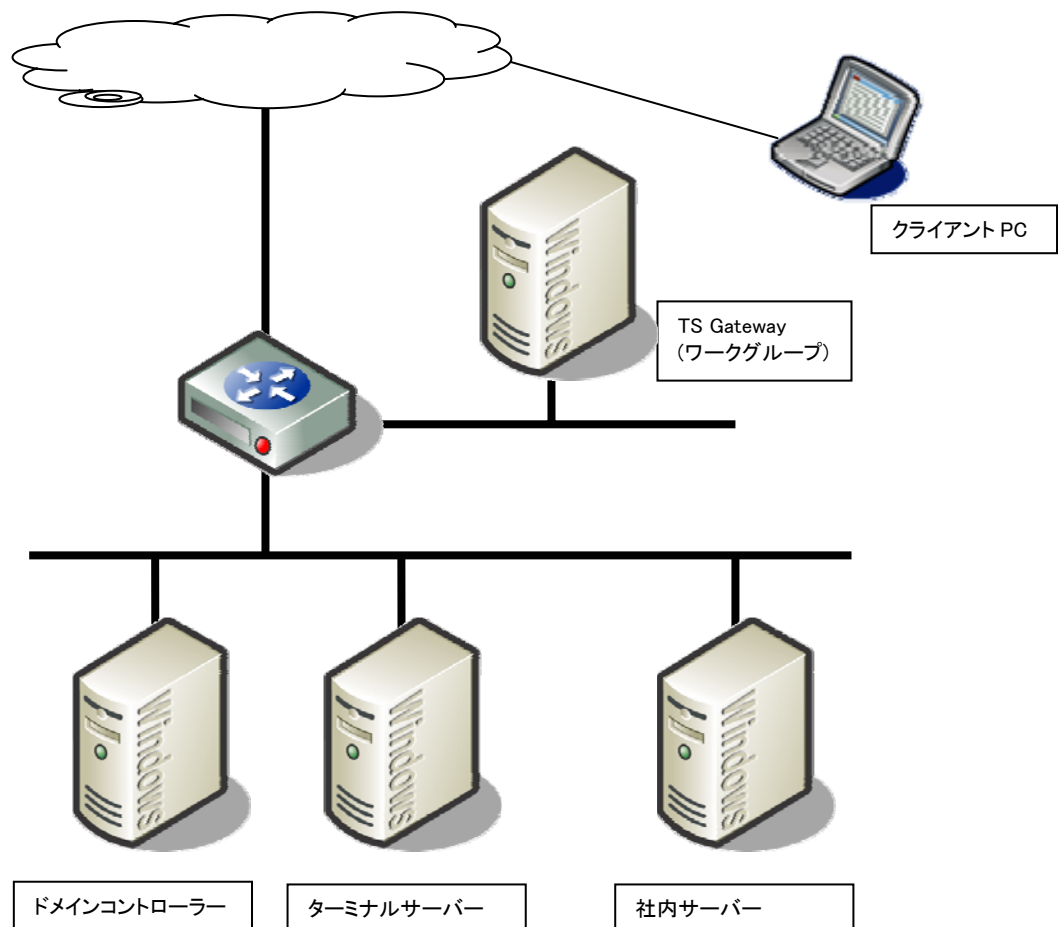
伊藤忠テクノソリューションズ株式会社
IT エンジニアリング室
プラットフォーム技術部
Windows 技術課

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。

CTC

Challenging Tomorrow's Changes