最終更新 2011/03/10

IP アドレスおよびサービスの構成

IPv6 及び IPv4 の構成

DHCP の構成

ルーティング

IPSec

名前解決の構成

DNS サーバー構成

DNS ゾーン

ゾーンの作成

DNS レコード

DNS の管理と監視

クライアントコンピュータの名前解決

ネットワークアクセスの構成

リモートアクセス

RADIUS サーバーの構成

ネットワークアクセス保護（NPA）

- NPS の構成
- NAP クライアントの構成
- DHCP 強制
- VPN 強制
- IPSec の強制
- 802.1x 強制

無線 LAN

ファイアウォール設定

ファイル及び印刷サービスの構成

ファイルサーバー構成

共有フォルダのシャドウコピー

DFS（Distributed File System）構成

バックアップ及び復元

ディスククォータ管理

印刷サービスの監視及び構成

ネットワークインフトラクチャの監視及び管理

Windows Server Update Services サーバー設定を構成

システム状態データを収集する

イベントログを監視する

ネットワークデータを収集する

Windows Server 2008 R2 新機能

DirectAccess

R2 での新機能には「※R2」マーク有り

■IP アドレスおよびサービスの構成

IPv6 及び IPv4 の構成

16 ビットずつ 16 進数に変換し：で区切る。先頭の 0 は省略可能。連続した 0000 は 1 回に限り::で省略可能。

（通常） FFEC:0001:0000:0000:0000:0A12:0000:0001

（省略） FFEC:　1:　　:A12:　0:　1

Windows Server 2003 以降で対応。WindowsXP で IPv6 を使うには、コマンドプロンプトで「ipv6 install」を行う。

前半の 64bit がネットワーク部、後半 64bit がホスト部だが、

IPv4 と同様に CIDR 形式でネットワーク部とホスト部を任意のプレフィックス長で分離可能。

(例)2001::90D3:2F3B:2AA:FF:FE28:9C5A の IP アドレスにおける 59bit のネットワークプレフィックスの求め方

2F3B が、49～64bit 部分であることが解る。2 進数に分解すると、0010 1111 0010 1011

青文字部分までが 59bit でネットワークプレフィックスとなる。16 進数に戻すと、2F20 になる。

最終的な表記　2001::90D3:2F20:2AA:FF:FE28:9C5A/59

同一サブネット内のアドレス解決にマルチキャストによる近隣要請メッセージを使用する。

これは IPv4 の ARP（Adress Resolution Protocol：アドレス解決プロトコル）の機能。

通信	説明
ユニキャスト	1 対 1 の通信。IPv4 と同じ
マルチキャスト	特定グループに所属するホストに対して送信する IP アドレス。FF00::/8
エニーキャスト	別々のサーバーで同じ IP アドレスを設定することで、一番距離が近いホストへ通信する

IP アドレス		説明
ﾙｰﾌﾟﾊﾞｯｸｱﾄﾞﾚｽ	::1	自分自身を指す。IPv4 では、127.0.0.1
ｸﾞﾛｰﾊﾞﾙﾕﾆｷｬｽﾄｱﾄﾞﾚｽ	200::/3	インターネットにアクセスする際に使用される
ﾘﾝｸﾛｰｶﾙｱﾄﾞﾚｽ	FE80::/10	自動構成される IP アドレスでルーティングされない（インターネット接続できない）IPv4 の場合は DHCP 失敗時に付与される 169.254.0.0/16 ・同じサブネット上のホストとの通信においてのみ利用するアドレス ・IPv6 ホストでは必ず付与される。 ・通常、Stateless Address Auto Configuration にて作成される
ｻｲﾄﾛｰｶﾙｱﾄﾞﾚｽ	FEC0::/10	IPv4 のプライベートアドレスに該当。現在は廃止されている
ﾕﾆｰｸﾛｰｶﾙﾕﾆｷｬｽﾄｱﾄﾞﾚｽ	FC00::/8 FD00::/8	IPv4 のプライベートアドレスに該当。組織内部の通信に限定

IPv4 上で IPv6 をサポートする技術

技術	説明
6over4	IP マルチキャストを用いて IPv4 ネットワーク上で IPv6 通信をトンネリングする
6to4	IP を用いて IPv4 ネットワーク上で IPv6 通信をトンネリングする。 NAT が存在する場合の動作は保証されていない。 IPv6⇔IPv4 の通信を確立する為には、宛先まで 6to4 ルータでルーティングさせなければならない

IPv6 自動ﾄﾝﾈﾘﾝｸﾞ	IPv4 互換アドレスを用いて IPv4 ホスト間で IPv6 通信を行う
ISATAP	IP を用いて IPv4 ネットワーク上で IPv6 通信をトンネリングする。 6to4 と異なり IPv4 ネットワークに辿り着く前に ISATAP ルータを入れるだけでよい
PortProxy	IPv4 アドレスへの通信を IPv6 アドレスに変換したり、その逆を行う
Teredo	UDP を用いて IPv4 ネットワーク上で IPv6 をトンネリングする。 NAT が存在する場合の動作も保証されている

IPv4 の構成

クラス	グローバルアドレス範囲	プライベートアドレス範囲
A	1.0.0.0 ～ 126.255.255.255	10.0.0.0 ～ 10.255.255.255
B	128.0.0.0 ～ 191.255.255.255	172.16.0.0 ～ 172.31.255.255
C	192.0.0.0 ～ 223.255.255.255	192.168.0.0 ～ 192.168.255.255
D	224.0.0.0～239.0.0.0	IP マルチキャスト用に予約されている
E	240.0.0.0～247.0.0.0	調査研究用に予約されている

IP アドレスが設定される優先順位の流れ

① 静的 IP アドレスの構成

② DHCP サーバーによる動的 IP アドレス設定

③ 代替構成が存在していれば、その IP アドレスが設定される。※

④ APIPA による IP アドレス構成（リンクローカルアドレス FE80::/10 169.254.0.0/16）

※代替構成は動的構成にしている場合のみ、TCP/IP プロパティのタブに「代替構成」タブが表示され設定できる

DHCP の構成

AD に参加しているサーバー上で、DHCP サーバーを起動させるには DHCP サーバーの承認（承認済みとして AD 内に登録する）が必要。スタンドアロンサーバーの場合は不要（承認自体ができない）

承認は Enterprise Admin 権限を持つ管理者が管理ツール「DHCP」にて行うことができる。

承認は AD にて行われる為、DHCP サーバーはドメインのメンバ（DC かメンバサーバ）である必要がある。

PXE や BOOTP や等のネットワークブートでも DHCP から IP アドレスを取得できる。

スコープ種類	説明
スコープ	特定サブネットのクライアントに割り当てる IP アドレスの範囲。 スコープの設定後「スコープ」を右クリックし[アクティブ化]を行うことで有効になる。 2 台の DHCP で冗長構成した場合､同じスコープを設定後､重複のアドレスを払い出さないように 80/20 or 50/50 の割合でアドレスを除外する。

分割スコープ ※R2	2 台の DHCP で同じスコープを共有し、分割の割合を決める。 1 台の DHCP サーバーが使用不可能になった場合、別のサーバーが機能を代行する。 構成台数は 2 台で行い Pv4 でのみ使用可能。 設定したスコープを右クリック、[詳細設定]⇒[分割スコープ]
ｽｰﾊﾟｰｽｺｰﾌﾟ	DHCP のスコープをまとめて 1 つの論理的なスコープとして定義する
ﾏﾙﾁｷｬｽﾄｽｺｰﾌﾟ	マルチキャストアドレスを動的に配布する。グループ単位で同じマルチキャストアドレスを付与。 ビデオ会議などで A 会議室に参加しているクライアントに同じマルチキャストアドレスを付与等
予約	MAC アドレス（ハイフンなしで指定）に対応したクライアントに特定の IP アドレスを割り振る。 複数の DHCP サーバーを立てた場合、全ての DHCP サーバーで同じ予約アドレスを指定する必要がある

オプション構成

DHCP サーバーが IP アドレスとサブネット以外にクライアントに割り当てる値。

オプション	説明
003 ルーター	デフォルトゲートウェイの IP アドレス
006 DNS サーバー	ネットワーク上のクライアントが利用可能な DNS サーバーの IP アドレス
015 DNS ドメイン名	クライアントが名前解決で使用する接続専用の DNS サフィックス
046 WINS/NBT サーバー	WINS サーバーの IP アドレス
046 WINS/NBT ﾉｰﾄﾞﾀｲﾌﾟ	NETBIOS 名前解決の種類。1=ブロードキャスト　2=ピア　4=混合　8=ハイブリッド

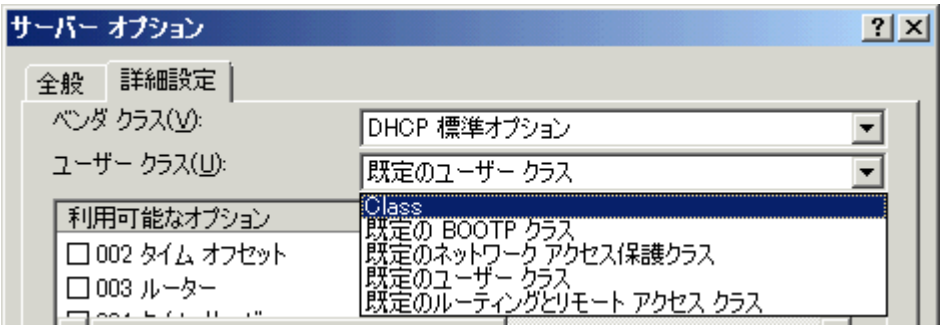
IPv4 or 6 を右クリックし[既定のオプション設定]を編集することでオリジナルのオプション構成も作成可能

適用優先順位	説明（DHCP 管理ツールの左ペイン選択箇所）
クライアント	クライアント端末での設定（静的に IP アドレスやゲートウェイを設定している）
サーバーレベル	DHCP サーバーのすべての DHCP クライアントに割り当てられる（サーバーオプション）
スコープレベル	スコープ全ての DHCP クライアントに割り当てられる（スコープオプション）
クラスレベル	特定のユーザークラスに定義された DHCP クライアントに割り当てられる
予約クライアントレベル	予約設定された 1 台の DHCP クライアントに割り当てられる（予約で作成した項目）

ユーザークラスの作成方法

ユーザークラスは管理ツール「DHCP」から IPv4 か IPv6 を右クリックし[ユーザークラスの定義]から作成する。

DHCP オプション割り当て時、[詳細設定]タブのユーザークラスのプルダウンから作成したユーザー定義が選択可能になる。



DHCP クライアント側で、ipconfig /setclassid "LAN の名称" ユーザークラス名称　を実行する

フィルタ設定

指定した MAC アドレス（ワイルドカード使用可能）のクライアントに対し DHCP サービスを許可、拒否の設定を定義する

DHCP リレーエージェント

DHCP クライアントは IP アドレスを取得する為、最初にブロードキャストを行うが、ブロードキャストは別セグメントへ転送されない為、DHCP サーバーが同一サブネット内でないと IP アドレスの取得が行えない。
DHCP リレーエージェントを使用することで DHCP サーバーが別サブネットにある場合でも IP アドレスが取得可能になる。
RFC1542 準拠しているルータを使うことでも DHCP ブロードキャストを他のセグメントへ転送でき IP アドレスの取得が可能。
DHCP サーバー自体を DHCP リレーエージェントにはできない（同じポート番号を使用する為）

① 「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰとｱｸｾｽｻｰﾋﾞｽ」役割から[ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽｻｰﾋﾞｽ]サービスを追加
② 管理ツール「ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽ」を起動し、サーバー名で右クリック、[ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽの構成と有効化]を選択するとウィザードが起動する。
③ 構成画面で「カスタム構成」を選択、カスタム構成画面から[LAN ルーティング]を選択し、サービスを起動させる
④ 適切な IP ﾊﾞｰｼﾞｮﾝを展開し全般を右ｸﾘｯｸ、[新しいﾙｰﾃｨﾝｸﾞﾌﾟﾛﾄｺﾙ]を選択し[DHCP ﾘﾚｰｴｰｼﾞｪﾝﾄ]を追加する
⑤ 「DHCP ﾘﾚｰｴｰｼﾞｪﾝﾄ」を右クリックし[新しいｲﾝﾀｰﾌｪｰｽ]を選択し、ｸﾗｲｱﾝﾄから DHCP を受け付けるｲﾝﾀｰﾌｪｰｽを選択する
⑥ 「DHCP ﾘﾚｰｴｰｼﾞｪﾝﾄ」のプロパティから転送先の DHCP サーバーの IP アドレスを設定する

DHCP の管理

DHCP データベースの肥大化を解消するには、DHCP サービスを停止した状態で、jetpack コマンドにてコンパクト化する。

```
jetpack %systemroot%¥system32¥dhcp¥dhcp.mdb 一時ファイル名.mdb
```

コンパクト化されたファイルが作成されるので、作成されたファイルを dhcp.mdb に変更する

DHCP データーベースのバックアップは既定でバックアップディレクトリに 60 分毎に自動的にバックアップされている。
復元を行った際は DHCP データベースの整合性を取ることが推奨される。
既に払い出されている IP が DB に反映されてない場合、重複で IP を払い出してしまうため。

管理ツール「DHCP」から「IPv4」のプロパティを開き、[詳細設定]タブの[検出回数]の数値を入力することで、
払い出す予定の IP に[検出回数]で指定した回数 ping が失敗した場合のみ払い出しを行う。

ipconfig コマンド

オプション	説明
/release	指定した NIC の DHCP サーバから取得した IP アドレスを解放（省略時は全部の NIC）
/renew	指定した NIC に DHCP サーバから IP アドレスを取得する（省略時は全部の NIC）
/registerdns	DHCP サーバからの IP アドレスのリースを更新し、動的(A と PTR レコード)更新も行う
/setclassid	新しいクラス ID をアダプタに設定する
/displaydns	DNS リゾルバキャッシュの表示
/flushdns	DNS リゾルバキャッシュの消去

netsh コマンド

netsh interface { ipv4|ipv6 } { show|set|add } interface [Idx|IF 名] [ｵﾌﾟｼｮﾝ={ enable|disable }]

オプション	説明
advertise	自動構成情報を送信設定
managedaddress	IP アドレスの情報を送信設定（ルータ側で IP アドレスの自動構成を行っている場合は無効にする）

otherstateful	DNS サーバーなどその他（IP アドレス以外）の構成情報の送信設定

タスクの例	コマンド例
ﾈｯﾄﾜｰｸ構成表示	netsh interface ipv4 show interface　※NIC の Idx 確認
静的 IP ｱﾄﾞﾚｽ設定	netsh interface ipv4 set address "Idx | 名前" static　IP ｱﾄﾞﾚｽ　ｻﾌﾞﾈｯﾄ　ﾃﾞﾌｫﾙﾄｹﾞｰﾄｳｪｲ
DNS サーバー設定	netsh interface ipv4 add dnsserver name="Idx or 名前" address=DNS ｻｰﾊﾞｰ IP ｱﾄﾞﾚｽ index=INDEX 番号　※DNS サーバーを設定する毎に 1 からカウントアップさせていく

Server Core

GUI を持たない必要最低限の役割のみ提供される。APS の役割追加、Power Shell は動作しない

タスク	コマンド
サーバー名変更	netdom renamecomputer ｺﾝﾋﾟｭｰﾀ名 /newname:ｺﾝﾋﾟｭｰﾀ名
サーバーライセンス認証 リモートでの認証	slmgr.vbs -ato　※ローカルでのライセンス認証、成功時は何も表示されない cscript %systemroot%¥system32¥slmgr.vbs ｻｰﾊﾞｰ名 ﾕｰｻﾞｰ名 ﾊﾟｽﾜｰﾄﾞ:-ato
ドメインに参加させる	netdom join ｺﾝﾋﾟｭｰﾀ名 /domain:ﾄﾞﾒｲﾝ名 /user:ﾕｰｻﾞｰ名 /password:* ※ﾕｰｻﾞｰ名はドメインに参加させる為のアクセス許可があるユーザーを指定
Administrators ｸﾞﾙｰﾌﾟに追加	net localgroup administrators /add ﾄﾞﾒｲﾝ名¥ﾕｰｻﾞｰ名
役割の追加	start /w ocsetup 役割名称 [/uninstall] oclist コマンドにて Server Core で利用可能な役割・機能の一覧を表示する（Server Core インストールを行った場合のみ使用可能） ※R2 から dism コマンドで管理もできるようになった
Active Directory の役割追加	Dcpromo /unattend:無人ｾｯﾄｱｯﾌﾟﾌｧｲﾙ名　※GUI が使えない為、無人ｾｯﾄｱｯﾌﾟが必要
ﾘﾓｰﾄからの MMC 接続許可	netsh firewall set service remoteadmin enable
ﾘﾓｰﾄﾃﾞｽｸﾄｯﾌﾟでの接続許可	cscript %systemroot%¥system32¥scregedit.wsf /ar 0
ﾘﾓｰﾄ接続許可	サーバー　　：winrm quickconfig　でリモート接続許可を行う。 クライアント：winrm get uri -r　でサーバーに接続する

インストール可能な役割	ocsetup での役割名称
AD LDS	DirectoryServices-ADAM-ServerCore
DHCP サーバー	DHCPServerCore
DNS サーバー	DNS-Server-Core-Role
ファイルアプリケーションサービス 分散ファイルシステムサービス DFS（分散ファイルシステム）レプリケーション NFS（Network File System）用サービス	FRS-Infrastructure DFSN-Server DFSR-Infrastructure-ServerEdition ServerForNFS-Base ClientForNFS-Base
印刷サービス LPD(ラインプリンタデーモン)サービス	Printing-ServerCore-Role Printing-LPDPrintService
ストリーミングメディアサービス	MediaServer
WEB サービス	IIS-WebServer

ルーティング

Windows2008 では RIPv2 のみサポートされる。RIPv2 では、VLSM 及び認証がサポートされている。

管理ツール「ルーティングとリモートアクセス」の「全般」を右クリックし、

[新しいルーティングプロトコルの追加]から RIP バージョン 2 のプロトコルをインストール可能。

用途	コマンド	
ﾙｰﾃｨﾝｸﾞﾃｰﾌﾞﾙ表示	route print	
ﾙｰﾃｨﾝｸﾞ追加	route -p add 宛先 mask ｻﾌﾞﾈｯﾄﾏｽｸ ｹﾞｰﾄｳｪｲｱﾄﾞﾚｽ metric ﾒﾄﾘｯｸ if ｲﾝﾀｰﾌｪｰｽ	
	-p	レジストリに書き込む。再起動しても設定が消えない
	宛先	宛先ネットワークを指定。デフォルトルートの場合は 0.0.0.0 を指定する
	ｻﾌﾞﾈｯﾄﾏｽｸ	宛先ネットワークに対するネットマスク指定。省略時は 255.255.255.255
	ｹﾞｰﾄｳｪｲｱﾄﾞﾚｽ	次のルーターのアドレスを指定。ローカルに直接指定されたアドレスの場合はサブネットに接続されている自分自身の IF の IP アドレスを指定する
	ﾒﾄﾘｯｸ	ルートに対するコストを 1～32767 から指定
	ｲﾝﾀｰﾌｪｰｽ	宛先に到達できる IF 用の INDEX（route print で確認）を指定する。省略時はｹﾞｰﾄｳｪｲｱﾄﾞﾚｽに基づいて決定する
	(例)route -p add 192.168.11.0 mask 255.255.255.0 192.168.12.1 192.168.11.0/24 のパケットは 192.168.12.1 へ転送される	

IPSec を構成する

完全性の確保（改ざんの防止）、送信元の認証（なりすまし防止）、機密性の確保（暗号化）を提供する。

セキュリティプロトコル	実装されているセキュリティ
AH：Authentication Header	完全性の確保、送信元の認証
ESP：Encapusulating Security Payload	完全性の確保、送信元の認証、機密性の確保

IPSec は実際に通信する前に通信するコンピュータと IKE プロトコルを使用してネゴシエーションを行う。

その結果 SA（Security Association）が確立され、認証方法、暗号化アルゴリズム、鍵の情報など共有し通信を行う。

相手との認証方法	説明
Kerberos V5 認証	同じフォレスト内のコンピュータ間で IPSec を行う場合、特別な構成なしで実装できる。 ただしドメインに参加してないクライアントでは使用できない
事前共有キー	管理者が設定するランダムな文字列で通信を行うコンピュータ間でパスワードとして使用。 Active Directory 環境がなくても使用可能だが、IPSec ポリシーにクリアテキストとして保存されるので一番セキュリティが低い
証明書	認証局から IPSec 通信に使用する証明書を発行し、それを使用する一番強固なセキュリティ。 AD 環境がなくても使用可能だが発行された証明書をインストールする作業などがある為、一番作業負担が高い

IP セキュリティポリシー

IPSec 通信を行うには、Active Directory のグループポリシーを利用する。

「グループポリシー管理エディタ」から[コンピュータの構成] - [ポリシー] - [Windows の設定] - [セキュリティの設定]

[IP セキュリティポリシー]にて以下の何れかの割り当てを IPSec を行う双方のコンピュータに適用する

ポリシー名	説明
クライアント（応答のみ）	通信相手が IPSec を要求してこない限り IPSec の通信は行わない
サーバー（ｾｷｭﾘﾃｨが必要）	通信相手に IPSec の要求を行い、相手が応答した場合は IPSec、応答しない場合は通常の通信
ｾｷｭﾘﾃｨで保護されたｻｰﾊﾞｰ	通信相手に IPSec の要求を行い、相手が応答した場合は IPSec、応答しない場合は通信を切断

※スタンドアロンの場合、ローカルポリシーの[IP セキュリティポリシー]にて設定を行う

■名前解決の構成

DNS サーバー構成

Active Directory 環境には必須のサービス。DNS クエリとは DNS サーバーに対して送信される名前解決要求のこと。

DNS クエリ	クエリの内容と、問い合わせに対する結果のパターン
再帰クエリ	DNS クライアントが DNS サーバーに対して行うクエリ。クエリの結果をクライアントに返す義務がある DNS サーバーにフォワーダが設定されている場合、DNS サーバーが他の DNS サーバーに再帰クエリを投げる。
反復クエリ	再帰クエリを受け取った DNS サーバーが他の DNS サーバーに対して行うクエリ

権限の**ある** DNS サーバー（要求されたゾーンを保持している DNS サーバー）は、
クライアントからの要求に対して、レコードを調査し応答を返す。目的のレコードがない場合は、否定応答を返す。
権限の**ない** DNS サーバー（要求されたゾーンを保持していない DNS サーバー）は、
解決できないクエリに対してフォワーダの設定がされていればフォワーダ（DNS サーバー）に再帰クエリを転送する。
フォワーダが設定されていない場合はルートヒントを参照し、DNS ツリーを辿りながら権限のあるサーバーに辿り着く。

ルートヒント

ルートサーバーの IP アドレス一覧が記載されたファイル。（%SystemRoot%¥system32¥dns¥cache.dns）
ルート(.)ゾーンが構成されている DNS サーバーの場合、ルートヒントは無効になる。
企業内ネットワークにおいて各名前解決に外部のインターネットを使わない場合、ルートヒントを企業内ネットワークの IP アドレスに変更することで名前解決が社内ドメインに限定されセキュリティ向上に繋がる。

キャッシュ専用サーバー

他の DNS サーバーから返ってきた結果をキャッシュに保存する。次回同じ問い合わせがあった場合、外部へ問い合わせを行わずキャッシュから直ぐに応答を返す。キャッシュ保存時間は TTL にて設定。
存在しない DNS サーバーの結果もネガティブキャッシュとして残る（既定は 15 分）
DNS サービスをインストールした初期状態はゾーンを持ってない為、この状態でフォワーダを設定すればキャッシュ専用サーバーとなる。

フォワーダ

通常自身で解決できなかった DNS クエリはルートサーバーへ反復クエリを投げるが、フォワーダが設定された DNS サーバーでは、指定した他の DNS サーバーに再帰クエリとして転送する。転送先の DNS サーバーをフォワーダと言う。
再帰クエリを受け取ったフォワーダがルートサーバーに反復クエリを投げて名前解決を行う。
フォワーダを設定した DNS サーバーではルートヒントを保持できない。
ルートヒントを設定するとフォワーダが機能しない。
フォワーダが設定された DNS サーバーは再帰クエリを受け取った時のみフォワーダへ転送する。

各拠点の DNS サーバーがそれぞれインターネット側の DNS サーバーに反復クエリを繰り返す再帰クエリを行うと、

DNS システム全体として効率が悪い、本社拠点間の WAN 回線帯域幅を圧迫する、セキュリティが低下するなど問題がある。
各拠点では再帰クエリを行わず、インターネット側の DNS サーバーに転送させ、
その DNS サーバーに対してのみ再帰クエリを行わせることで上記の問題を回避することが出来る。

「DNS マネージャ」を起動し、「サーバー名」プロパティの[フォワーダ]タブにて設定する。
[フォワーダが利用可能な場合にルートヒントを使用する]のチェックがオン（排他モード）とオフ（非排他モード）

モード	フォワーダが DNS クエリを解決できない場合の動作
ON ：排他モード	ルートヒントを使用せず DNS クエリの発行者にクエリの失敗を返す（反復クエリを行わない）
OFF：非排他モード	ルートヒントを利用して自身で名前解決を行おうとする。ルートサーバーに反復クエリを行う

日本語の意味と逆になっているが、表記の誤りであり Microsoft の文書にも記載がある

dnscmd サーバ名 /ResetForwarders マスタ IP アドレス [/Timeout 時間] [/Slave | /NoSlave]

サーバー名	DNS サーバー名を入力。ローカルの DNS サーバーの場合は「.」で良い
マスタ IP アドレス	クエリの転送先となる DNS サーバー（フォワーダとなる DNS サーバー） 複数指定の場合はスペースで区切る
/Timeout 時間(秒)	転送クエリがタイムアウトになるまでの時間。デフォルトは 5 秒
/Slave | /NoSlave	フォワーダを排他（非排他）モードにする

フォワーダを使用するシナリオ

内部 DNS サーバーと外部 DNS サーバーの分離

内部 DNS サーバーはインターネット側の名前解決を行わず、
外部向けの DNS サーバーに全て転送することで、セキュリティを高める。

本社・支店間の DNS トラフィック軽減

支店の DNS サーバーをキャッシュ専用 DNS サーバーに設定することで、本社・支店間のトラフィックを軽減する。
ゾーン設定を行わずフォワーダ設定のみ行うことで再帰クエリを行わないキャッシュ専用サーバーとなる。

条件付きフォワーダ

クエリで指定しているドメイン名に直接転送先 DNS サーバーを指定する。
「DNS マネージャ」を起動し、「条件付きフォワーダ」を右クリックから[新規条件付きフォワーダ]で追加を行う。
DNS ドメインに名前解決したいクエリのドメイン名。IP アドレスに転送先フォワーダの IP アドレスを入力する。
条件付きフォワーダは Active Directory に保存することが可能。(/DsFowarder)
dnscmd サーバ名 /ZoneAdd フォワード先ゾーン名 { /Forwarder | /DsForwarder } フォワーダ先 DNS サーバー

DNS ゾーン

ゾーンとはドメインの情報を格納する DNS データベースの単位で、1 ドメインの情報だけを格納することも複数ドメインの情報を 1 つのゾーンファイルで管理することも可能。ゾーン転送はゾーンファイル単位で行う。

ゾーン転送

ゾーンに格納された情報を別のサーバーに複製する動作のこと。

ゾーンの種類	説明

プライマリゾーン	オリジナルのゾーン情報を保持。読み書き可能。 Active Directory 統合ゾーンにすることで、AD に情報を格納できる
セカンダリゾーン	ゾーン情報の転送元サーバーから取得したコピーを保持。読み取り専用。 情報はファイルに格納される。%Systemroot%¥system32¥dns¥ゾーン名.dns

ゾーン転送の制御を行うのは SOA レコードで、現在のプライマリゾーンを保持しているサーバーなどの情報がある

情報	説明
シリアル番号	ゾーンファイルの更新世代を示す番号。ゾーン内のリソースレコードが更新される度にカウントアップしゾーン転送先サーバーが最新のリソースレコードを保持しているか判断する
プライマリサーバー	ゾーンのプライマリ DNS のホスト名
責任者	ゾーン管理者の電子メールを記述。@の替わりに.を使う
更新間隔	セカンダリサーバーがマスタサーバーに SOA を問い合わせる間隔。既定値は 15 分。 シリアル番号が最新でない場合は、マスタサーバにゾーン転送を要求する
再試行間隔	ゾーン転送に失敗した際に再試行するまでの待機時間。既定値は 10 分
期限	更新間隔に達してもゾーン転送が行われない場合、「期限」を過ぎたローカルのゾーンファイルを「信頼できないデータ」とし、このゾーンに対するクエリに応答しなくなる。既定値は 24 時間
最小 TTL	新しくレコードを作成した際に既定で設定されている TTL 値。レコード作成時に変更可能
このﾚｺｰﾄﾞの TTL	SOA レコード自身の TTL 値

ゾーン転送の仕組み	説明
完全ゾーン転送	ゾーンデータベースを全てコピーする。フルゾーン転送、AXFR とも呼ばれる
増分ゾーン転送	ゾーンデータベースの変更分だけコピーする。インクリメントゾーン転送、IXFR とも呼ばれる

ゾーン転送方法	説明
更新間隔がトリガ	セカンダリサーバーが更新間隔に達したらマスタサーバーにクエリ要求を出す。 プライマリサーバーは SOA クエリの応答。セカンダリは SOA のシリアル番号を比較。 シリアル番号が最新でなければ更新要求、最新であればこの時点で終了。
通知がトリガ	プライマリサーバがレコードが更新されたことをセカンダリサーバーに通知する。 通知を受け取ったセカンダリサーバーが更新を要求する。 「DNS マネージャ」より「ゾーン」のプロパティ[ゾーン転送]タブ[通知]にて設定する。 [ネームサーバー]タブに記載されている DNS サーバーか[任意に指定した DNS サーバー]か選択する

手動でのゾーン転送	説明（「DNS」より[セカンダリゾーン]を右クリック、転送方法を選択する）
マスタから転送	セカンダリサーバーで SOA のシリアル番号を比較し、最新でなければ IXFR のゾーン転送を行う dnscmd DNSｻｰﾊﾞｰ /ZoneRefresh 更新するｾｶﾝﾀﾞﾘｿﾞｰﾝ名
マスタから再読み込み	ゾーンの SOA レコードのシリアル番号に関係なくマスタサーバーから AXFR のゾーン転送を行う コマンドによる AXFR のゾーン転送はできない

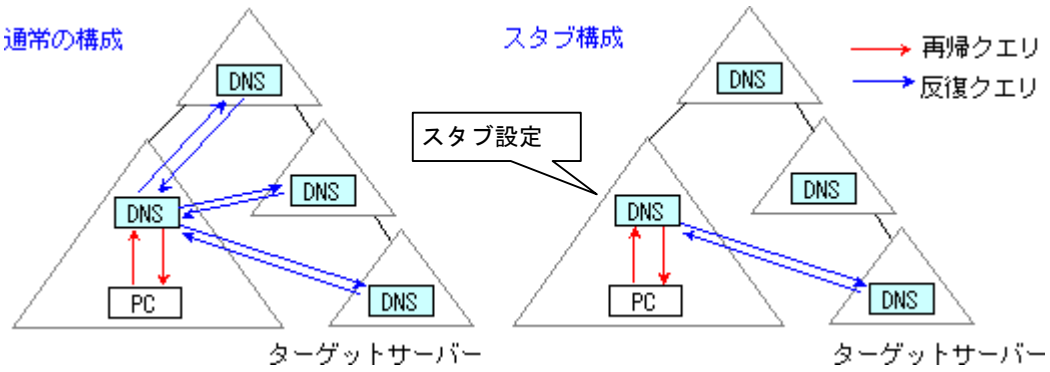
ゾーン転送の許可	説明（「DNS マネージャ」より「ゾーン」のプロパティ[ゾーン転送]タブ）

すべてのサーバー	ゾーン転送要求があれば全てのセカンダリサーバーに対してゾーン転送を許可 dnscmd DNS ｻｰﾊﾞｰ /ZoneResetSecondaries ｿﾞｰﾝ名 **/NonSecure** 通知ｵﾌﾟｼｮﾝ 転送を許可しない場合は /NoXfr 通知ｵﾌﾟｼｮﾝは /NoNotify | /Notify | /NotifyList IP ｱﾄﾞﾚｽ から選択する
ﾈｰﾑｻｰﾊﾞｰﾀﾌﾞの一覧にあるｻｰﾊﾞｰのみ	[ネームサーバー]タブのサーバー一覧登録されている DNS サーバーのみゾーン転送を許可。 「通知」の設定もこの DNS サーバーが対象になるので手動で登録作業が不要になる dnscmd DNS ｻｰﾊﾞｰ /ZoneResetSecondaries ｿﾞｰﾝ名 **/SecureNs** 通知ｵﾌﾟｼｮﾝ
次のサーバーのみ	[ゾーン転送]タブで指定された DNS サーバーのみゾーン転送を許可 dnscmd DNS ｻｰﾊﾞｰ /ZoneResetSecondaries ｿﾞｰﾝ名 **/SecureList** ｻｰﾊﾞｰ名 通知ｵﾌﾟｼｮﾝ

スタブゾーン

スタブゾーンを設定すると相手先のゾーンから、SOA、NS、グルーA レコード(DNS サーバーの A レコード)をゾーン転送によりコピーする。これらは相手の DNS サーバーを識別するために必要なレコードのみ。

スタブ設定を行うことでターゲットサーバーの SOA/NS/グルーA レコードがコピーされるる為、
ルートサーバーを経由せず、直接ターゲットサーバーが存在する DNS サーバーにクエリを送信できる。



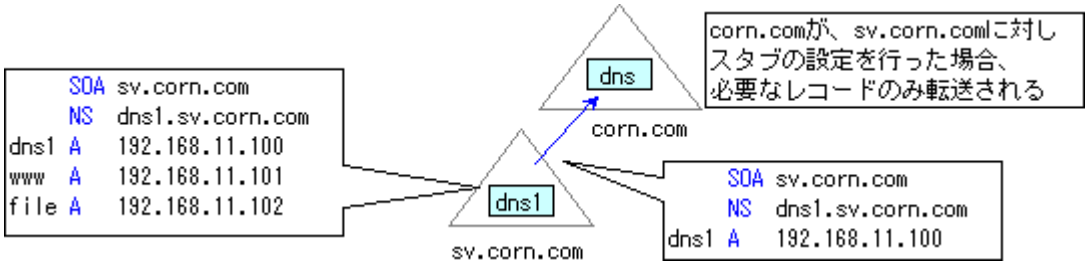
似たような動きとして条件付きフォワーダがあるが違いは以下の通り。
スタブは**反復クエリを送信**し自身で再帰処理を担当する為、自身に負荷が掛かる。
条件付きフォワーダは**再帰クエリを送信**する為、相手先のサーバーに負荷が掛かる。

子ドメインに対するスタブの設定

親ドメイン（corn.com とする）が管理する子ドメイン（sv.corn.com とする）の DNS サーバーに変更（名称変更等）があった場合、子ドメイン(sv.corn.com)管理者が親ドメイン(corn.com)に対して、新しい DNS サーバーへの修正依頼が必要。

修正しない場合、co.jp に対して古い DNS サーバーへ名前解決を依頼する為、
その DNS サーバーが既に名前変更や削除されていた場合、名前解決が失敗してしまう。

親ドメイン(corn.com)が子ドメイン(sv.corn.com)に対するスタブを設定すると、子ドメイン(sv.corn.com)の SOA、NS、グルーA レコードが自動的に転送される為、子ドメイン側で DNS サーバーの変更があった場合でも、スタブはマスターサーバと定期的に通信を行い自動的にゾーンを最新の状態に更新する。



ゾーンの作成

DnsCmd　DNS サーバー名　/ZoneAdd　ゾーン名　ゾーン種類　[オプション]

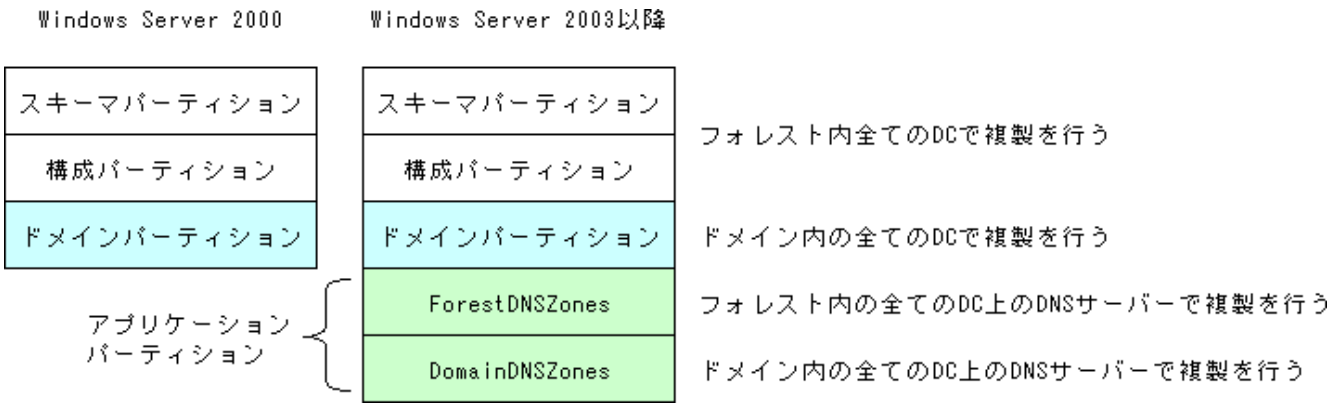
ゾーン種類	説明
/DsPrimary	Active Directory 統合プライマリゾーン。/dp オプションにて複製範囲を指定可能
/Primary	プライマリゾーン
/Secondary ﾏｽﾀ IP ｱﾄﾞﾚｽ	セカンダリゾーン。マスタ IP アドレスは複数指定可能
/Stub ﾏｽﾀ IP ｱﾄﾞﾚｽ	スタブゾーンの作成。マスタ IP アドレスは複数指定可能
/DsStub ﾏｽﾀ IP ｱﾄﾞﾚｽ	Active Directory 統合スタブゾーン作成。マスタ IP アドレスは複数指定可能
/Forwarder ﾏｽﾀ IP ｱﾄﾞﾚｽ	条件付きフォワーダの設定
/DsForwarder ﾏｽﾀ IP ｱﾄﾞﾚｽ	DC 上の DNS サーバーで条件付きフォワーダを設定。 フォレストまたはドメイン内の全ての DC 上の DNS サーバーに設定が複製される

オプション	説明
/file ﾌｧｲﾙ名	ゾーンファイル名
/load	既存ファイルを読み込む。指定しない場合は既定のゾーンレコードを作成
/a 管理者名	プライマリゾーンのみゾーン管理者のメールアドレスを指定可能
/dp FQDN	/DsPrimary を指定した場合のみ指定可能。格納先によりゾーン情報の複製範囲が変わる レコードが格納されるディレクトリパーティションを指定。完全修正ドメイン名を入力
/dp /domain	アプリケーションパーティションの DomainDnsZones に格納
/dp /forest	アプリケーションパーティションの ForestDnsZones に格納
/dp /legacy	ドメインパーティションに格納

標準ゾーンと Active Directory 統合ゾーン

標準ゾーン	ゾーン情報はファイルに保存。%SystemRoot%¥system32¥dns¥～.dns DNS サーバーがゾーン情報の複製を制御し、シングルマスタ複製を行う
Active Directory 統合ゾーン	Active Directory データベースに保存される為、DNS サーバーは DC である事が必須。 Active Directory 統合ゾーン同士で動的更新が可能。 ゾーン複製は Active Directory 標準の複製プロセスが使用されマルチマスタで行う。 セカンダリゾーンは Active Directory 統合ゾーンにはできない（スタブゾーンは可能）

Active Directory 統合ゾーンの保存場所と複製



ドメインパーティションの情報は同じドメイン内の全てのコントローラに複製されることから以下の問題があった。

- ドメインが異なると Active Directory 統合ゾーンによる複製ができない
- DNS サーバーでないドメインコントローラーにも DNS 情報が複製される

単一ラベル名前解決のためのゾーン

単一ラベルとは DNS サフィックスを伴わない単あるホスト名のこと。

WIN2008.example.com という FQDN に対して、WIN2008 が単一ラベルとなる。

単一ラベルの名前解決に「GlobalNames ゾーン」を使用する。WINS サーバーを立てずに単一ラベルの名前解決が可能。

LLMNR とは異なりサブネットを越えての名前解決が可能。

GlobalNames ゾーンは動的更新をサポートしない為、動的に IP アドレスが変わるコンピュータの単一名前解決は対象外。

GlobalNames ゾーンを使用した単一ラベルの名前解決の流れ。

① ドメインサフィックス検索リフトが設定されていれば、その順序でホスト名の後ろにドメイン名サフィックスを追加してクエリを行う。追加されていなければ自身が所属しているドメイン名を追加して DNS サーバーにクエリを行う。

② ①で名前解決が失敗した場合、単一ラベルでの名前解決を要求する。

③ GlobalNames ゾーンが有効になっていれば、GlobalNames ゾーンにて名前解決を行う。

④ ③で名前解決が失敗した場合、LLMNR や、NetBIOS 名前解決を試みる

GlobalNames ゾーンの作成方法

① 前方参照ゾーンに「GlobalNames」という名前のゾーンを作成する

② CNAME または A レコードを追加する

③ dnscmd ｻｰﾊﾞｰ名 /config /enableglobalnamessupport 1 を実行し有効にする

レジストリを直接編集することでも有効にできる。

動的更新

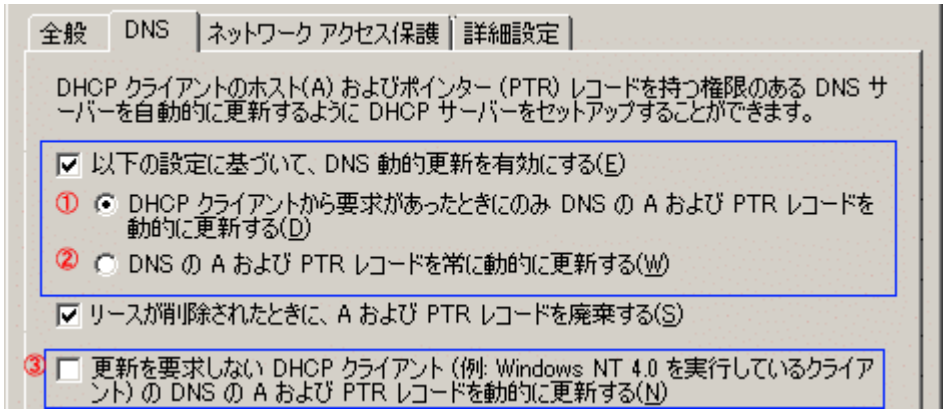
DNS サーバーが動的更新のメッセージを受け付けて DNS ゾーンのリソースコードを動的に作成すること。

DNS サーバーへの動的更新の対象は IP アドレスが動的に変化する DHCP クライアント。

クライアントでは「TCP/IP 詳細設定」の[DNS]タブから[この接続のアドレスを DNS 登録する]にチェックを入れる。

DHCP サーバーでは「DHCP 管理コンソール」より「IP バージョン」のプロパティを開き[DNS]タブにて設定する。

[以下の設定に基づいて、DNS 動的更新を有効にする]にチェックを入れ、以下のどちらかをチェックする。



① DHCP クライアント自身が A レコードを登録し、DHCP サーバーが PTR レコードを登録する

② DHCP クライアントからの動的更新は行われず、DHCP サーバーが A レコード、PTR レコードを登録する

③ DHCP クライアントが UNIX の場合、この設定にしないと動的更新が行えない（DHCP オプション 81 サポートしてない為）

DHCP を 2 台で運用し同じスコープを割り当てた場合、以下の追加設定が必要。

- DHCP サーバーのコンピュータアカウントを DnsUpdateProxy グローバルグループメンバにする
- 動的更新用のﾕｰｻﾞｰを作成し、そのﾕｰｻﾞｰの権限で動的更新を行う（ﾄﾞﾒｲﾝﾒﾝﾊﾞのみ動的更新を許可する場合に必要）
  [詳細設定]タブの[資格情報]から動的更新用のユーザーが作成できる

DNS サーバーでは「DNS マネージャ」より対象ゾーンのプロパティを開き[全般]タブの[動的更新]から選択する

なし	動的更新を受け付けない
非ｾｷｭﾘﾃｨ保護およびｾｷｭﾘﾃｨ保護	すべての DNS クライアントの動的更新を受け付ける
セキュリティ保護のみ	Active Directory で認証されたコンピュータからの動的更新のみ受け付ける Active Directory 統合ゾーンの場合のみ選択可能

DNS レコード

DnsCmd　DNS サーバー名　{ /RecordAdd | /RecordDelete }　ゾーン名　ノード名　RR 種類　RR データ

RR 種類	説明
A	ホスト名と IP アドレスを対応付ける （例） dnscmd . /RecordAdd corn.com PC1 A 192.168.11.11 PC1　IN　A　192.168.10.11
PTR	IP アドレスからホスト名を調べる。IP アドレスを逆に並び替えて最後に検索するドメイン名を付与 IPv4 は 5.11.168.192.in-addr.arpa、IPv6 は、1.0.～略.08FF.ip6.int という PTR レコードを検索 （追加例） dnscmd . /Recordadd　11.168.192.in-addr.arpa 101 PTR corn.com （削除例） dnscmd . /RecordDelete 11.168.192.in-addr.arpa 101 PTR corn.com
CNAME	ホストに別名を付ける。設定するには別名と A レコードをリンクさせる
NS	DNS サーバーのホスト名を登録。NS レコードによってそのドメインの DNS サーバーを認知する
HINFO	目的のコンピュータの情報（CPU や OS）を記述する

MX	メール送信先ドメインのメールサーバー識別する IN MX 10 mail1.example.jp. IN MX 20 mail2.example.jp. mail1 IN A 192.168.10.10 mail2 IN A 192.168.10.11 優先順位は 1～65535 の値が入力可能で、小さい方を優先してメールサーバーとして使用する 同じ値を設定した場合はロードバランシングされる
SRV	サービスに対するポート番号や、処理優先順位を指定することができる。 【書式】_Service._Proto.Name TTL Class SRV Priority Weight Port Target _ftp._tcp.example.jp. IN SRV 1 1 21 server01.example.jp _ftp._tcp.example.jp. IN SRV 1 2 21 server02.example.jp Target には必ず A レコードで IP アドレスが指定されている必要がある。 プライオリティが同じ場合は、Weight の割合でロードバランシングされる。 Active Directory を使用する際には必須のレコードで AD インストール時に自動で作成される。 Netlogon サービスを再起動することでも必要な SRV レコードの作成が行われる。 ログオン時に DC やグローバルカタログサーバーの検索するために使用する。
WINLOOKUP	DNS サーバーで名前解決できなかった DNS クエリを指定した IP アドレス（WINS サーバー）に転送する。 この時、WINS サーバーへは FQDN 名のうちノード名のみ転送する（ws2008.local.com の場合 ws2008） 「DNS マネージャ」から該当サーバーのプロパティを開き[WINS]タブから設定を行う。 WINLOOKUP は MS 独自レコードの為、サードパーティの DNS がセカンダリサーバーになっている場合、 ゾーン転送時にレコード認識できずにエラーになる可能性がある。 [ﾚｺｰﾄﾞをﾚﾌﾟﾘｹｰﾄしない]にチェックを入れることで当該レコードのゾーン転送を行わないようにする

DNS の管理と監視

DNS サーバーを運用していくと古いレコードが削除されずに残り、DNS データベースの容量が大きくなることで、
古いレコードがクエリとして返されたり、ゾーン転送量が多くなる為、エージングと清掃を行う必要がある。

エージング	古いリソースレコードを DNS データベースから削除するかを判別するプロセス。 エージング期間は、非更新間隔＋更新間隔
清掃	古いリソースレコードを DNS データベースから削除するプロセス。 エージング期間中、一切の更新が行われてないレコードを削除する

非更新間隔	DNS サーバーが UPDATE のみ受け付ける期間。タイムスタンプの更新を受け付けない期間を設けることにより属性値の変更を防ぎ、不要なレプリケーショントラフィックを抑えることを目的に設定する
更新間隔	DNS サーバーが UPDATE 及び REFRESH を受け付ける期間。

DNS クライアントが DNS サーバーに対して行う更新プロセス

REFRESH	内容の更新を伴わないタイムスタンプのみの更新。24 時間毎、または再起動したタイミングで発生
UPDATE	内容の変更を伴う更新

エージングの設定

Active Directory 統合ゾーンではサーバー単位での設定が可能。

「DNS マネージャ」から「DNS サーバー」を右クリック[すべてのゾーンに対しエージング/清掃を設定する]を選択する。

標準プライマリゾーンの場合は、ゾーン単位で、ゾーンのプロパティから[全般]タブの「エージング」から設定する。

静的レコードを削除対象にするにはレコードのプロパティから[古くなったらこのﾚｺｰﾄﾞを削除する]にチェックを入れる。※

※表示メニューから[詳細]を選択した場合のみ設定項目が表示される

清掃の設定

「DNS マネージャ」から「DNS サーバー」のプロパティを開き[詳細設定]タブを選択する

清掃プロセスが起動する間隔を設定する。(既定では 7 日)

今すぐに清掃プロセスを実行する

「DNS マネージャ」から DNS サーバーを選択し右クリックから「古いリソースレコードの清掃」を選択。

サーバーキャッシュの消去

「DNS マネージャ」の「表示」メニューから[詳細]にチェックを入れることでキャッシュが表示される。

リソースレコードの表示内容も増え、Time to Live(TTL)の設定変更が可能になる。

キャッシュの消去は、DNS サーバーを右クリックし「キャッシュの消去」を選択する。

TTL は DNS サーバー及び、DNS クライアントにレコードがキャッシュされる期間。

DNS クライアントにキャッシュが残っていれば DNS サーバーへの問い合わせはしなくて済む。

dnscmd　DNS ｻｰﾊﾞｰ名　ｵﾌﾟｼｮﾝ

オプション	説明
/StartScavenging	清掃プロセスの実行
/ClearCache	DNS サーバーキャッシュの消去
/EnumZone	DNS サーバーで構成されているゾーンの一覧を表示
/ZoneInfo ｿﾞｰﾝ名	DNS サーバーのゾーン情報を表示
/ZoneExport ｿﾞｰﾝ名 ﾌｧｲﾙ名	ゾーン情報をファイルに出力する

nslookup [ｵﾌﾟｼｮﾝ] [検索対象] [DNS ｻｰﾊﾞｰ名]

オプション(対話ﾓｰﾄﾞ)	説明
set all	現在の設定を表示
set domain=ﾄﾞﾒｲﾝ名	既定の DNS ドメイン名を指定した名前に変更する。 set domain=co.jp として、yahoo を検索した場合、自動で yahoo.co.jp になる
server DNS サーバー	問い合わせ先の DNS サーバーを指定する。省略時は自ドメインの DNS サーバーを使用
set type=ﾚｺｰﾄﾞﾀｲﾌﾟ	問い合わせるレコードタイプを変更する (既定は A)
set d2	デバッグモードにする

※非対話モードの場合、set の変わりに、ハイフンを指定する。

(例) nslookup -type=PTR 10.0.168.192.in-addr.arpa 192.168.11.1

トラストアンカー　※R2

リモート DNS サーバーから受信したセキュア DNS (DNSSEC) 応答を検証するために使用。

署名された DNS 応答を検証するにはトラストアンカーを DNSKEY 形式の公開キーとして構成する。

DNS サーバーのプロパティにて設定する。

クライアントコンピュータの名前解決

名前解決の順序は①DNS リゾルバキャッシュ（HOSTS 含む） ②DNS ③GlobalNames ゾーン ④LLMNR ⑤NetBIOS

DNS リゾルバキャッシュ（クライアント DNS キャッシュとも呼ばれる）は

DNS サーバーから返されたレコードを一定期間（TTL によって異なる）メモリに保存する。

ipconfig /displaydns	DNS リゾルバキャッシュの表示
ipconfig /flushdns	DNS リゾルバキャッシュの消去

LLMNR（Link-local Multicast Name Resolusion）

IPv6 と IPv4 ホストの両方が DNS サーバーを使用しなくても同一サブネットであれば名前解決が可能な新しいプロトコル。

Windows Vista、Windows Server 2008 以降で利用可能で既定で有効になっている。

LLMNR 対応ホストはクエリをサブネット内の LLMNR 対応ホストがリッスンしているマルチキャストで送信する。

そしてクエリで指定された名前の所有者が応答を返す。UDP ポートの 5355 を使用する。

バージョン	宛先 IP	宛先 MAC
IPv4	224.0.0.254	01-00-5E-00-00-FC
IPv6	FF02::1:3	33-33-00-01-00-03

NetBIOS

名前解決は以下の順だがノードタイプの設定を変更することで、この順序を変更することが可能

①NetBIOS 各キャッシュ ②WINS ③ブロードキャスト ④LMHOSTS

NetBIOS 各キャッシュ	一度名前解決を行った応答を一定期間メモリに保存する仕組み（デフォルトの TTL は 10 分） NetBIOS のキャッシュ参照 nbtstat -c キャッシュの消去 nbtstat -R
WINS	NetBIOS においてホスト名解決の DNS サーバーに相当するコンポーネント
LMHOSTS	IP アドレスとそれに対応した NetBIOS コンピュータ名で静的な名前登録を行うことができる

LMHOSTS で定義済みのキーワード

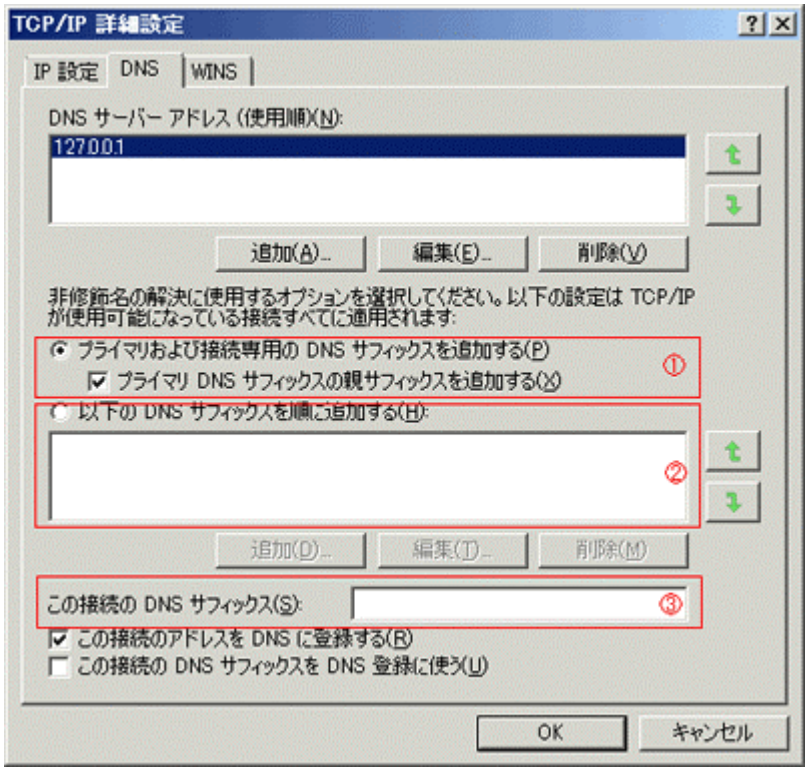
定義	説明
#PRE	NetBIOS キャッシュに永続的なエントリとして事前に読み込んでおくことが可能 （例） 182.102.93.122 CORN #PRE
#INCLUDE	ローカルの LMHOSTS ではなくリモートの LMHOSTS ファイルを読み込む （例） #INCLUDE ¥¥WS2008¥Public¥LMHOSTS
#BEGIN_ALTERNATE #END_ALTERNATE	リモート LMHOSTS ファイルに冗長性を持たせる。この 2 行の間で#INCLUDE したファイルは最初に INCLUDE したファイルが読み込めない場合、2 つ目に INCLUDE したファイルを読み込む

NetBIOS ノードタイプ

NetBIOS 名前解決で使用する手段や、その順序を決定する設定項目で DHCP のオプション設定等で変更可能

タイプ	名前解決の順序	タイプ	名前解決の順序
B ノード	ブロードキャスト	M ノード	ブロードキャスト ⇒ WINS
P ノード	WINS	H ノード	WINS ⇒ ブロードキャスト （Windows Server2008 のデフォルト）

サフィックスの検索順序



ﾌﾟﾗｲﾏﾘおよび接続専用の DNS ｻﾌｨｯｸｽを追加する

単一ﾗﾍﾞﾙのﾎｽﾄ名指定が行われた場合、

ﾌﾟﾗｲﾏﾘ DNS ｻﾌｨｯｸｽと接続固有のｻﾌｨｯｸｽを

後ろにつけて FQDN にして名前解決を行う。

ﾌﾟﾗｲﾏﾘ DNS ｻﾌｨｯｸｽは「ｼｽﾃﾑﾌﾟﾛﾊﾟﾃｨ」⇒「ｺﾝﾋﾟｭｰﾀ名」⇒変更⇒詳細にて設定

接続固有のｻﾌｨｯｸｽは③で追加する

[ﾌﾟﾗｲﾏﾘ DNS ｻﾌｨｯｸｽの親ｻﾌｨｯｸｽを追加する]

にﾁｪｯｸを入れるとﾌﾟﾗｲﾏﾘ DNS ｻﾌｨｯｸｽを付けての名前解決に失敗した場合、

ｻﾌｨｯｸｽの先頭ﾗﾍﾞﾙを 1 つ減らして再度名前解決を試みる。それも失敗すれば更に 1 つ減らして名前解決を試みる。以降この動作を繰り返す。上位のドメインを外す動作をデボルブという

[以下の DNS サフィックスの親サフィックスを追加する]を選択した場合、プライマリ DNS サフィックスや接続固有のサフィックスで指定したドメインは無視され、このドメイン検索リストに表示されている順序で名前解決を行う

サフィックスが追加されるプロセス

① DNS クライアントはホスト名にプライマリ DNS サフィックスを追加して DNS サーバーにクエリを送る

② 解決できない場合は、ホスト名に接続固有の DNS サフィックスを追加して DNS サーバーにクエリを送る

③ ②でも解決できない場合、プライマリ DNS サフィックスの親サフィックスをホスト名に追加して DNS サーバーにクエリを送り、それでも解決できない場合は、更にその親サフィックスという順序で 2 ドメインになるまで繰り返す。

④ ドメインサフィックス検索リスト（図の②）を使用していた場合は、検索リストにある順番にサフィックスを追加して名前解決を試みる。

サフィックス名前解決の例として以下の設定がある DNS クライアントがあるとする

プライマリ DNS サフィックス：sales.south.nwtraders.com　接続固有のサフィックス：contoso.con

図の①の設定にチェックが入ってるものとする。

Server1 で名前解決を行おうとすると、Server1.sales.south.nwtraders.com　Server1.contoso.con

Server1.south.nwtraders.com　Server1.nwtraders.com　の順序で

2 ドメイン（デボルブレベルが 2）になるまで名前解決を行う。

R2 以降のデボルブ動作

FRD（Forest Root Domain）までしかデボルブ動作を行わなくなった。

- ADDS フォレストルートドメインのラベルの数が 1 つの場合またはプライマリ DNS サフィックスの末尾にフォレストルートドメインが付加されていない場合、デボルブは無効になる
- プライマリ DNS サフィックスの末尾にフォレストルートドメインが付加されている場合、デボルブレベルはフォレストルートドメインのラベルの数になる

上記例の場合、FRD が south.nwtraders.com の場合、Server1.south.nwtraders.com　の名前解決までしか行わない。

グループポリシーを使用したクライアント管理

[コンピュータの構成] - [ポリシー] - [管理者テンプレート] - [ネットワーク] - [DNS クライアント]

プライマリ DNS サフィックスのデボルブレベル

デボルブレベルを変更する。未構成（既定値）は 2

修正複数ラベル名への DNS サフィックスの追加を許可する

web1.east のようにドットを含むが DNS サフィックスを全て指定してないものを非修正ラベルと言う。

web1.east で名前解決が失敗した場合、既定ではその後ろに DNS サフィックスを追加して名前解決を行わない。

この設定を有効にすることで、失敗した場合、DNS サフィックスを追加して名前解決を行うようになる

マルチキャスト名前解決をオフにする

Windows Vista 以降はデフォルトで LLMNR がサポートされてるが使用したくない場合はこの設定を有効にする

■ネットワークアクセスの構成

リモートアクセス

ダイアルアップや、VPN（Virtural Private Network）を使用するには、

役割「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰとｱｸｾｽｻｰﾋﾞｽ」内にある「ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽｻｰﾋﾞｽ（RRAS）」サービスを追加する。

インストール直後は無効化されている為、管理ツール「ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽ」を起動し、

「ホスト名」を右クリックし「ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽの構成と有効化」を選択するとｾｯﾄｱｯﾌﾟｳｨｻﾞｰﾄﾞが起動する。

ウィザード	説明
構成	ﾘﾓｰﾄｱｸｾｽ（ﾀﾞｲﾔﾙｱｯﾌﾟまたは VPN）を選択することでﾘﾓｰﾄｱｸｾｽｻｰﾊﾞｰ構成となる
ﾘﾓｰﾄｱｸｾｽ	受信可能な接続を選択する。「VPN」と「ダイヤルアップ」のどちらか、または両方
IP ｱﾄﾞﾚｽ割り当て	リモートクライアントに IP アドレスを割り当てる方法を選択する 自動：RRAS ｻｰﾊﾞが企業内の DHCP ｻｰﾊﾞから IP ｱﾄﾞﾚｽを取得し、それをﾘﾓｰﾄｸﾗｲｱﾝﾄに割り当てる 指定したｱﾄﾞﾚｽ範囲：RRAS ｻｰﾊﾞがﾘﾓｰﾄｸﾗｲｱﾝﾄに対し IP ｱﾄﾞﾚｽを割り当てる
複数のﾘﾓｰﾄｱｸｾｽｻｰﾊﾞｰの管理	リモートクライアントの認証をﾘﾓｰﾄｱｸｾｽｻｰﾊﾞｰで行うか、RADIUS サーバーにて行うか選択する

RRAS がリモートアクセスクライアントを Active Directory ドメインユーザーアカウントで認証する場合、

AD にある「RAS and IAS Servers」セキュリティグループにﾘﾓｰﾄｱｸｾｽｻｰﾊﾞｰのｺﾝﾋﾟｭｰﾀｱｶｳﾝﾄを追加する必要がある。

追加することで RRAS がユーザーアカウントの[ダイヤルイン]プロパティを参照できるようになる。

ドメイン管理者権限があるユーザーが RRAS 構成をインストールを行った場合は自動でこのメンバーに追加される。

AD がインストールされていないメンバサーバーの場合はローカルアカウントでユーザー認証が可能。

上記のローカル認証または、RADIUS サーバーに認証要求を転送する場合はこのメンバーに追加する必要はない。

リモートアクセスの認証

管理ツール[ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽｻｰﾋﾞｽ]から左ペインの「ｻｰﾊﾞｰ名（ﾛｰｶﾙ）」のプロパティを表示。

[セキュリティ]タブの「認証方法」にてユーザー認証を設定する

認証方法	ユーザー名とパスワードにて認証を行う

PAP	ユーザーとパスワードを暗号化せず平文で送信する
CHAP	ユーザーとパスワードを暗号化して送るが強度が高くない
MS-CHAP	マイクロソフトが CHAP を拡張した認証プロトコルでバージョン 1 と 2 がある
認証方法	証明書による認証を行うプロトコル
EAP	リモートアクセスクライアントと認証を行うサーバー間の様々な拡張認証方式を利用するための枠組みを定義しており、Windows Server 2008 では以下の認証方式に対対応している。 EAP-TLS（Extensible Authentication Protocol-Transport Layer Security） サーバー認証及び、ユーザー認証（正しいユーザーかどうかの確認）を証明書によって認証する。 クライアント側で使用する証明書はインストールまたは、スマートカードを利用する
PEAP	PEAP クライアントとサーバー間の暗号化を行い、PEAP と組み合わせが可能な他の認証プロトコルに対して追加のセキュリティを提供する。ワイヤレスネットワークでのみ利用可能。 PEAP には「PEAP-EAP-MS-CHAP v2」と「PEAP-EAP-TLS」がある
PEAP-EAP-MS-CHAP v2 認証サーバーにサーバー認証（正しいサーバーかどうかの確認）の為のサーバー証明書をインストールし、 ユーザー認証（正しいユーザーかどうかの確認）にはユーザー名とパスワードを使用する。 クライアント側にはサーバー証明書の正当性を確認する為に、 サーバー証明書を発行した発行元 CA（認証局）やルート CA の証明書をインストールしておく必要がある	
PEAP-EAP-TLS EAP-TLS を使用する PEAP で RRAS が標準でサポートする認証方式で最もセキュリティが高い。スマートカード認証が可能	

クライアント⇔サーバー間で複数の認証が利用できる場合、最も高いセキュリティの認証が自動的に選択される

リモートアクセスプロトコル

ダイヤルアップサーバーとして利用する場合、クライアントの接続には PPP を使用する。

VPN サーバーとして使う場合は、PPTP、L2TP、SSTP の何れかの VPN プロトコルを使用する。

ﾌﾟﾛﾄｺﾙ	説明
PPTP	クライアントと VPN サーバーとの間に VPN トンネルの制御コネクションを TCP 1723 ポートにて PPTP トンネルを確立し、PPP フレームを GRE でカプセル化したものを使用する。 GRE は IP プロトコル番号 47 を使用する。 暗号化機能が元々付与してないことから、MPPE と MS-CHAP を組み合わせて暗号化を行っている。 ユーザー名と、パスワードを用いた認証しか対応していない
L2TP	ユーザーデータに PPP ヘッダー、L2TP ヘッダーを付与し、さらに UDP ヘッダーと新しい IP ヘッダーを付与する。UDP 1701 ポートが使用される。暗号化は IPSec にて行う。 コンピュータの認証方式は、証明書か、事前共有キーのどちらかを利用できる。 事前共有キーの場合、サーバー側とクライアント側にて同じキーを設定しておく必要がある。 ｻｰﾊﾞｰ　「ﾙｰﾃｨﾝｸﾞ とﾘﾓｰﾄｱｸｾｽ」にてｻｰﾊﾞｰのﾌﾟﾛﾊﾟﾃｨ[ｾｷｭﾘﾃｨ]ﾀﾌﾞの「ｶｽﾀﾑ IPSec ﾎﾟﾘｼｰ～」をﾁｪｯｸ ｸﾗｲｱﾝﾄ　VPN 接続ﾌﾟﾛﾊﾟﾃｨの[ﾈｯﾄﾜｰｸ]ﾀﾌﾞから IPSec 設定
SSTP	VPN トンネル制御及びユーザーデータ送受信共に HTTPS（TCP 443 ポート）のみを使用する。 ユーザーの IP パケットを PPP でカプセル化し、さらにそのデータを SSL を使用してカプセル化する。 VPN サーバーがお互いの所属するネットワークを仮想的に接続する拠点間 VPN には対応していない

	PPTP	L2TP	SSTP

ユーザー認証	○	○	○
ｺﾝﾋﾟｭｰﾀ認証	×	コンピュータ証明書 or 事前共有キー	サーバー証明書
暗号化	○（MPPE＋MS-CHAP）	○（IPSec）	○（https）
改ざん防止	×	○（IPSec）	○（https）
ポート IP ﾌﾟﾛﾄｺﾙ番号	TCP 1723 IP 47	L2TP　　UDP 1701 IPSec IKE：UDP 500　ESP：IP 50	TCP 443
証明書	使用しない	証明書を選択した場合、VPN サーバー及びクライアント双方に必要	VPN サーバー側にサーバー証明書が必要
サポート OS	Windows 2000 以前	Windows 2000 以降	サーバーは Windows 2008 クライアントは Vista SP1 以降
RFC 文書番号	2637	L2TP：2661　L2TP/IPSec：3193	規定されていない

VPN サーバーへの接続

Windows Vista で VPN サーバーに接続する手順

① コントロールパネルから「ネットワークとインターネット」⇒「ネットワークと共有センター」を開く

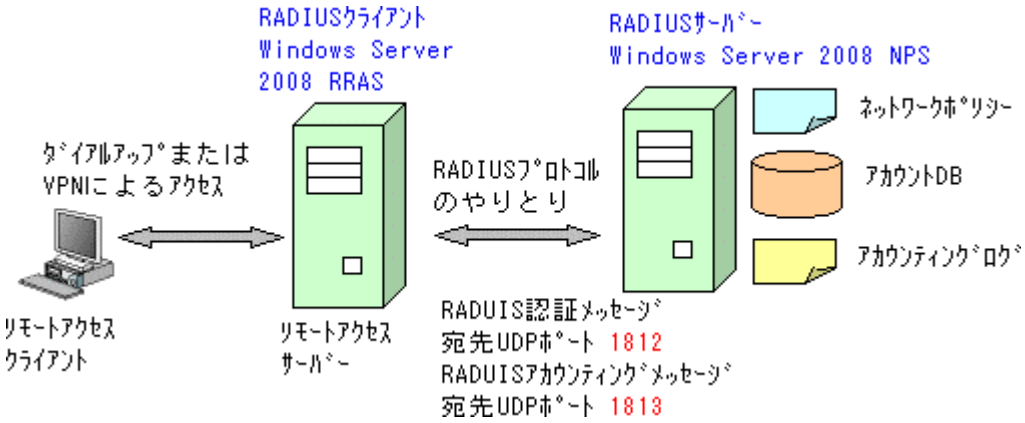
② 「接続またはネットワークのセットアップ」をクリックし接続オプションで「職場に接続します」を選択

③ 必要な情報を入力し接続を作成した後は「ネットワークと共有センター」にある VPN 接続の為のアイコンをクリックすることで VPN 接続が行える。リモートアクセスの接続のためのアイコンを右クリックしプロパティから VNP プロトコルや認証方法を変更できる

RADIUS サーバーの構成

認証、承認、アカウンティングの一元管理を行う。ダイアルアップ接続、VPN 接続、IEEE 802.x、NAP で使用される。

RADIUS サーバーを構成するには「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰとｱｸｾｽｻｰﾋﾞｽ」の役割から「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」ｻｰﾋﾞｽを追加することで、RADIUS サーバー及び、RADIUS クライアントの両方がインストールされる



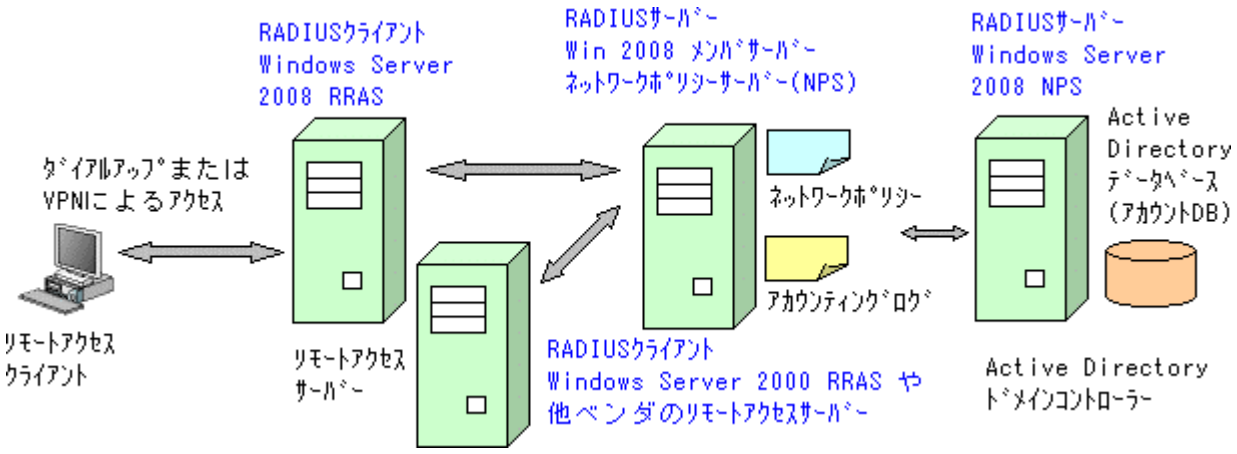
RRAS：ルーティングとリモートアクセスサービス

NPS　：ネットワークポリシーサーバー

複数の RADIUS クライアントで 1 台以上の RADIUS サーバーを共有することで認証の一元管理が可能になる。

Active Directory に登録されているユーザーアカウントで認証する場合、RADIUS サーバーを Active Directory ドメインコントローラかメンバサーバとして構成し、RAS and IAS Servers ｾｷｭﾘﾃｨｸﾞﾙｰﾌﾟにコンピュータを登録する必要がある

管理ツール「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」から「NPS(ﾛｰｶﾙ)」を右クリック[Active Directory にｻｰﾊﾞｰを登録]にて登録。



リモートアクセスサーバーは Active Directory のドメインコントローラやメンバサーバーにする必要なく、RADIUS クライアントの機能のみサポートしていれば良く DMZ 領域に配置するリモートアクセスサーバーをドメインから分離できる事で、ドメインコントローラとメンバサーバーとの間で必要とされる様々なトラフィックを FW で許可する必要がなくなる。

RADIUS サーバー（NPS）側での RADIUS クライアント（RRAS サーバ）の指定

管理ツール「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」から[RADIUS ｸﾗｲｱﾝﾄとｻｰﾊﾞｰ]-[RADIUS ｸﾗｲｱﾝﾄ]を右クリックし[新規 RADIUS ｸﾗｲｱﾝﾄ]

要素	説明
フレンドリ名	この構成を識別するためのタイトルを入力する
アドレス	RADIUS クライアントとなるリモートアクセスサーバーの IP アドレスかホスト名を入力
共有シークレット	RADIUS サーバーと RADIUS クライアントが正しい相手かどうかお互いに判断する為のパスワード文字列で両者に同じ物を設定しておく

RADIUS クライアント（RRAS サーバ）側での設定

・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して**ない**場合

管理ツール「ﾙｰﾃｨﾝｸﾞとﾘﾓｰﾄｱｸｾｽ」から「ｻｰﾊﾞｰ名(ﾛｰｶﾙ)」のプロパティから[ｾｷｭﾘﾃｨ]タブを表示。

認証プロバイダを RADIUS 認証にする。

[構成]ボタンから[追加]をクリック。[サーバー名]に RADIUS サーバーの IP アドレス又はホスト名を入力。

[共有シークレット]に RADIUS サーバーと同じパスワードを入力。

・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して**いる**場合

管理ツール「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」から設定を行う。

[RADIUS ｸﾗｲｱﾝﾄとｻｰﾊﾞｰ] - [ﾘﾓｰﾄ RADIUS ｻｰﾊﾞｰｸﾞﾙｰﾌﾟ]からﾘﾓｰﾄの RADIUS ｻｰﾊﾞｰを指定する。

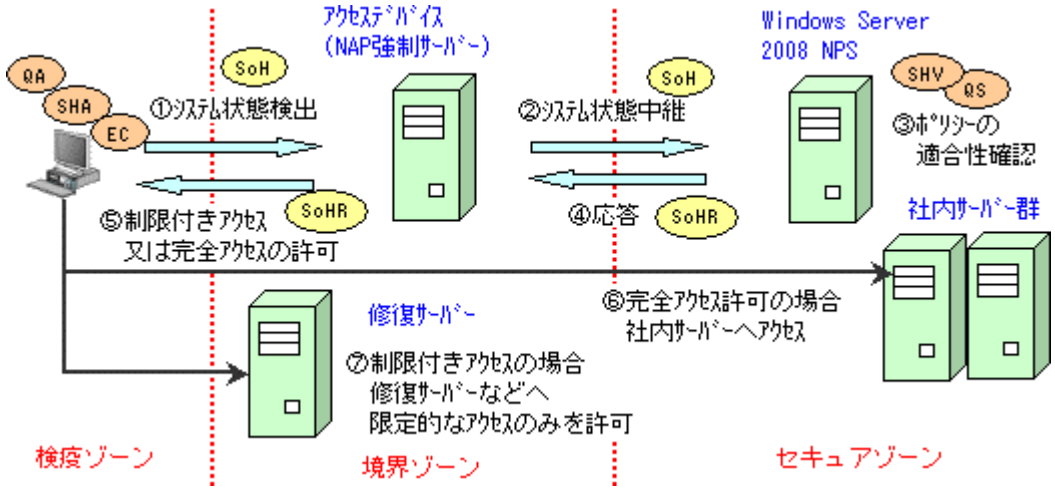
複数指定することで負荷分散させることが可能。負荷分散は優先度及び重み付けにて決定される

ネットワークアクセス保護（NPA）

企業のセキュリティ要件に適合しないコンピュータを社内ネットワークから隔離することで、

社内ネットワークを安全な状態に保つ為の機能。

NAP の動作



NAP 実施環境の要素	説明
NAP クライアント	NAP による検疫対象となるクライアント。 クライアントには NAP クライアントとしての機能が有効化されている必要がある
ネットワーク ポリシーサーバー	事前にクライアントに対するポリシーと、「ポリシーに準拠」「ポリシーに非準拠」「NAP に非対応」の時の動作（適切な NAP 構成）を定義しておく（RADIUS サーバーとして構成する）
修復サーバー	ポリシーに非準拠のクライアントはネットワークから隔離するだけでは、いつまでもポリシーに準拠することが出来ない。ポリシーに適合させるために必要なセキュリティ更新プログラムを提供する WSUS サーバーなどに対してアクセスのみを許可するように構成されたサーバー
アクセスデバイス (NAP 強制サーバー)	NAP クライアントと NPS との間にある機器のこと（NAP を強制するサーバー） NPS とのやりとりは RADIUS ﾌﾟﾛﾄｺﾙで行うので、RADIUS プロキシとして構成する必要がある

検疫ゾーン	NAP 非対応や非準拠、または検疫中のクライアントが配置されるゾーン
境界ゾーン	検疫ゾーンからもセキュアゾーンからもアクセス可能なゾーン
セキュアゾーン	社内サーバーなどのセキュリティで保護されるべきサーバーがあるゾーン

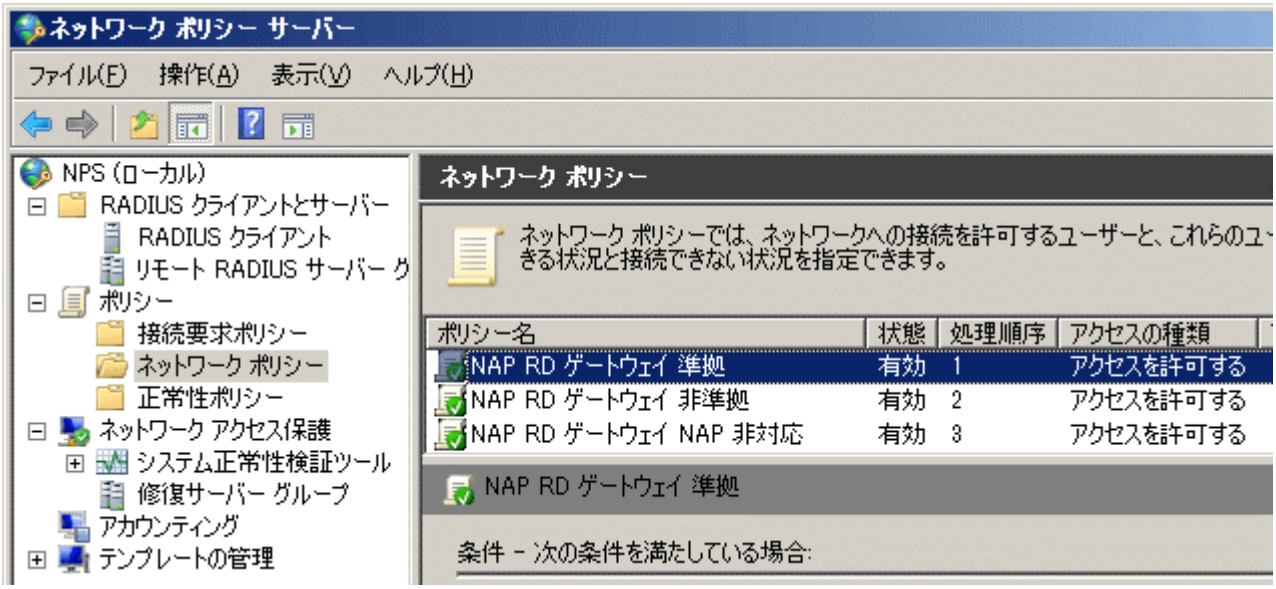
NAP ｺﾝﾎﾟｰﾈﾝﾄ	説明
SHA	システム正常性エージェント（System Health Agent） クライアントの状態を検査しポリシーに適合しているかを検証
QA	検出エージェント（Quarantine Agent） SHA から渡された状態情報をキャッシュ及び一覧化し実施クライアント（EC）に渡す
EC	実施クライアント（Enforcement Client） ポリシー準拠に基づいてクライアントに対しアクセスを完全に許可、制限付きで許可などの動作を強制するコンポーネント。ES に正常性ステートメント（SoH）を送信する
ES	NAP 強制サーバー（Enforcement Server） EC から受け取った SoH を SHV に転送する。QS より受け取った SoHR を EC へ転送する
SHV	システム正常性検出エージェント（System Health Validator） SoH を評価しアクセス可否情報を含む正常性ステートメント応答（SoHR）を QS に渡す
QS	検疫サーバー（Quarantine Server） SoHR を RADIUS プロトコルを使用して ES に送信する

NAP 実施方法	説明
DHCP NAP	アクセスデバイスとして Windows Server 2008 の DHCP サーバーを配置し、DHCP クライアントに対して NAP を実施。DHCP サーバーから IP アドレスを取得しようとした時に NAP を強制する。 アクセスデバイスである DHCP NAP 実施サーバーと NAP サーバーは同じコンピュータに構成することも異なるコンピュータに構成することも可能。 ポリシーに準拠/非準拠により異なる DHCP オプションやサブネットをリースする
VPN NAP	アクセスデバイスとして Windows Server 2008 の RRAS サーバーを配置し VPN 接続時に NAP を強制。 RRAS と NPS は異なるサーバーに構成することも同じサーバーに構成することも可能。 ポリシーに準拠してないクライアントにはパケットフィルタにより限定的なアクセスにする
IPSec NAP	社内サーバーのアクセスに IPSec を強制する。 ポリシーに準拠してないクライアントには IPSec 通信が必要なネットワークにアクセスできない
IEEE 802.1x NAP	アクセスデバイスとして 802.1x に対応したスイッチやワイヤレスアクセスポイントを配置する。 有線 LAN/無線 LAN クライアントが 802.1x を用いてネットワークにアクセスしようとした時に NAP を強制。ポリシーに準じてないクライアントは異なる VLAN に隔離するなどが行える
ﾀｰﾐﾅﾙｻｰﾋﾞｽ ｹﾞｰﾄｳｪｲ NAP	TS ゲートウェイはリモートデスクトッププロトコルを HTTPS でカプセル化して通信する為に使用される。NAP ポリシーに準拠したクライアントのみ TS サーバーへのアクセスを許可する等の制御が可能

NPS の構成

ポリシーが有効化される範囲を定義する「条件」と有効化された際の制限事項となる「制約」や「設定」がある。

ネットワークポリシーは処理順序で評価され「条件」に合致した場合、以降のポリシーは評価されない。



ポリシー	説明
接続要求ﾎﾟﾘｼｰ	NAP のアクセスデバイスから受信した接続要求をローカル認証にするか、RADIUS サーバーに転送するかを指定する。時間やユーザーの条件により認証を振り分けることができる

ﾈｯﾄﾜｰｸﾎﾟﾘｼｰ	条件を満たした場合にアクセスを許可するか、拒否するか定義する。 [ﾕｰｻﾞｰﾀﾞｲｱﾙｲﾝﾌﾟﾛﾊﾟﾃｨによってｱｸｾｽを判断する]にﾁｪｯｸした場合、 ﾄﾞﾒｲﾝﾕｰｻﾞｰのﾌﾟﾛﾊﾟﾃｨにある[ﾀﾞｲｱﾙｲﾝ]ﾀﾌﾞの設定が優先される。 さらに認証方法と制約、設定を定義する。 設定の定義では、アクセス許可時の動作を定義（NAP 強制や暗号化など）する。 NAP 強制⇒ 完全なﾈｯﾄﾜｰｸｱｸｾｽを許可、時間で許可、制限付きｱｸｾを許可の何れか 暗号化 ⇒ 通信の暗号化を指定する
正常性ﾎﾟﾘｼｰ	セキュリティ正常性検出ツール（SHV）のポリシーに準拠してるか、非準拠となっているかのポリシーを作成する。ここで定義したポリシーはネットワークポリシーの条件で使用可能
ｼｽﾃﾑ正常性検出ﾂｰﾙ	Windows ファイアウォール、ウィルス対策ソフトウェアなどのチェックをポリシー条約に指定できる。 ここで定義したポリシーは正常性ポリシーの条件で使用する

NAP クライアントの構成

以下の設定を有効にすることで、NAP 強制を行うことが可能になる。

各 NAP クライアントで個別に有効化（napclcfg.msc）もできるが AD 環境であればグループポリシーが使用できる。

① セキュリティセンターの有効化

[コンピュータの構成]-[ポリシー]-[管理者テンプレート]-[Windows コンポーネント]-[セキュリティセンター]

② Network Access Protection Agent サービスの有効化

[コンピュータの構成]-[ポリシー]-[Windows の設定]-[セキュリティの設定]-[システムサービス]から

「Network Access Protection Agent」を開き「このポリシー設定を定義する」を選択しサービスを「自動」にする

③ 実施クライアントの有効化

[コンピュータの構成]-[ポリシー]-[Windows の設定]-[セキュリティの設定]-[Network Access Protection]

[NTP クライアントの構成]-[実施クライアント]を選択。対象の実施クライアントを右クリックし「有効」にする。

クライアントの種類は、DHCP 強制、VPN 強制、IPSec 強制、TS ゲートウェイ強制、EAP 強制

DHCP 強制

管理ﾂｰﾙ「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」から[NPS(ﾛｰｶﾙ)]を選択し右ペインの「NAP を構成する」をｸﾘｯｸ[動的ﾎｽﾄ構成ﾌﾟﾛﾄｺﾙ]を選択

構成ウィザード	説明
DHCP ｻｰﾊﾞｰを実行する NAP 強制ｻｰﾊﾞｰの指定	NPS と DHCP が別々のｺﾝﾋﾟｭｰﾀの場合、RADIUS ｸﾗｲｱﾝﾄを追加する。 この場合、DHCP ｻｰﾊﾞｰ側にも NPS をｲﾝｽﾄｰﾙし、DHCP ｻｰﾊﾞｰ側の NPS を RADIUS ﾌﾟﾛｷｼとして構成する
DHCP スコープ	NAP で使用するスコープを指定。省略時は全ての NAP 有効スコープにポリシーが適用される
NAP 修復ｸﾞﾙｰﾌﾟ および URL の指定	修復サーバーグループは NAP 非準拠クライアントに対して NAP ポリシーに準拠する手順を提供するサーバー。また正常性ポリシーに準拠される方法についてのヘルプの WEB ページを指定する
NAP 正常性ポリシー	NAP クライアントの設定をポリシーに準拠するように強制的に変更する場合、 [クライアントコンピュータの自動修復を有効にする]のチェックを入れる。

DHCP サーバーのスコープで NAP を有効化

管理ツール「DHCP」を起動し[サーバー名]-[IPv4]から目的のスコープのプロパティを開く。

[ネットワークアクセス保護]タブから、[このスコープに対して有効にする]を選択する。

ポリシーに非準拠のクライアントは、IP アドレスがスコープ範囲内でリリースされるがサブネットが 255.255.255.255 となりデフォルトゲートウェイもない。結果として他ホストへの通信ができない。しかしながら IP は手動で変更できてしまう

ポリシーに非準拠のスコープオプションは[スコープオプション]を右クリック[オプション構成]を選択

[詳細設定]タブのユーザークラスで[規定のネットワークアクセス保護クラス]にて構成する。

VPN 強制

管理ﾂｰﾙ「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」から[NPS(ﾛｰｶﾙ)]を選択し右ペインの「NAP を構成する」をｸﾘｯｸ[仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ]

構成ウィザード	説明
VPN ｻｰﾊﾞｰを実行する NAP 強制ｻｰﾊﾞｰの指定	NPS と NAP VPN が別々のコンピュータの場合､RADIUS クライアントを追加する。 この場合､RRAS サーバー側にも RADUIS サーバーとして NPS を指定する必要がある
認証方法	EAP の種類を選択。EAP-TLS、PEAP-EAP-TLS を使用する場合、AD 証明書サービスの構成も含め PKI 環境が必要。PEAP-EAP-MS-CHAP v2 はサーバー証明書を NPS にインストールする必要がある

VPN クライアント側の認証設定（PEAP-EAP-MS-CHAP v2）

[スタート]-[ネットワーク]-[ネットワーク共有センター]-[ネットワーク接続の管理]から VPN アイコンのプロパティ

[セキュリティ]タブで[詳細(カスタム)]を選択し[設定]をクリック

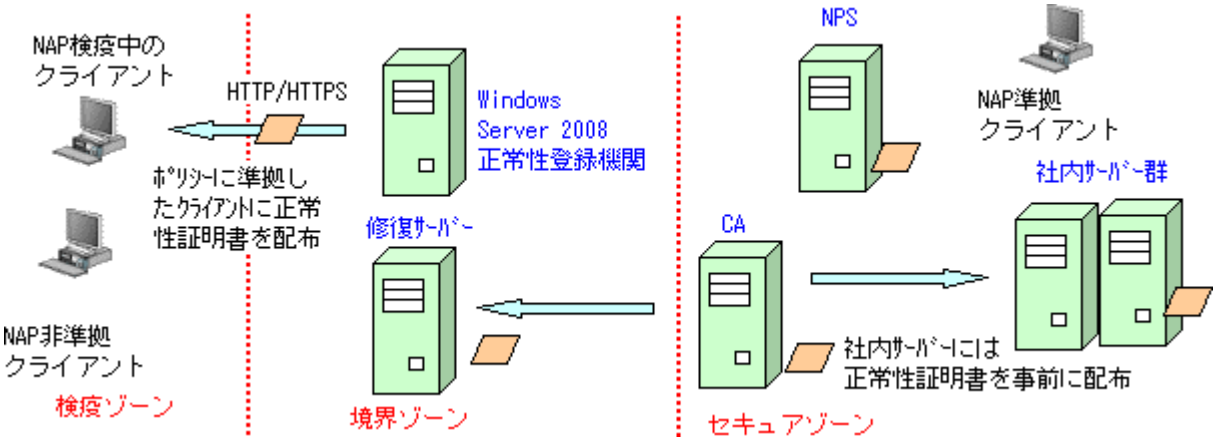
[拡張認証プロトコルを使う(EAP)]オプションを選択、[保護された EAP(PEAP)(暗号化は有効)]を選択し[プロパティ]

サーバー証明書を検証する、すばやい再接続を有効化する、検疫のチェックを有効にするの 3 つにチェックを入れる

IPSec の強制

NAP ﾎﾟﾘｼｰに準拠した NAP ｸﾗｲｱﾝﾄは、正常性登録期間から正常証明書が配布され社内ｻｰﾊﾞｰと IPSec 通信が可能になる。

NAP ｸﾗｲｱﾝﾄは、継続的に自身の正常性を確認し準拠しなくなった場合、正常性証明書を削除し IPSec 通信ができなくなる。



IPSec NAP を実施するには、以下の設定が必要

設定	説明
ｾｷｭｱｿﾞｰﾝ、境界ｿﾞｰﾝのｺﾝﾋﾟｭｰﾀに正常証明証を配布	社内サーバーに IPSec 通信のための正常性証明書を配布する
IPSec ポリシーを設定	正常性証明書を使って IPSec 通信を行うように以下の IPSec ポリシーを設定する。 ｾｷｭｱｿﾞｰﾝのｻｰﾊﾞｰ：正常性証明書を用いた IPSec 通信を必須にする 境界ｿﾞｰﾝのｻｰﾊﾞｰ：正常性証明書を用いた通信と IPSec を使用しない通信を許可 NAP ｸﾗｲｱﾝﾄ：通信相手から IPSec を要求された場合に IPsec 通信で応答する

NAP ｸﾗｲｱﾝﾄのための正常性登録機関と CA を設定	NAP クライアントに対して正常性証明書を配布する為に正常性登録機関と CA を設定する。 正常性登録機関は IPSec NAP におけるアクセスデバイスで NAP ポリシーに準拠しているクライアントの変わりに正常性証明書の要求を CA に送信する
NAP ポリシーを作成	DHCP NAP や VPN NAP と同様に IPSec NAP を有効化し、NPS ポリシーを定義する
NAP クライアントの構成	IPSec NAP クライアントとして必要な設定を行う

CA と正常登録機関を同じコンピュータにインストールする設定例

[ネットワークポリシーとアクセスサービス]の役割から[正常性登録機関]を追加する。

[HRA サーバーに対して正常証明書を発行するため、ローカル CA をインストールする]を選択する。

セットアップウィザードが起動するので適切なものを選んでインストールする。

正常性登録機関と CA インストール後の設定

[サーバーマネージャ]-[役割]-[ネットワークポリシーとアクセスサービス]-[正常性登録機関]から

[証明機関]を右クリックし、[証明機関を追加]にて[参照]をクリックし適切な CA を追加する。

[スタート]-[管理ツール]-[証明機関]から[CA 名]を右クリックしプロパティを開く

[ポリシーモジュール]タブのプロパティから、[証明書テンプレートに操作が設定されている場合はそれに従い、設定されていない場合は自動的に証明書を発行する]を選択する

IPSec NAP を NPS で構成する

管理ツール「ネットワークポリシーサーバー」から「NPS(ローカル)」を選択。右ペインの[NAP を構成する]をクリック。

[正常性登録期間 (HRA) を使用する IPSec]を選択し、NAP を構成する。

NAP クライアントの構成

[グループポリシー管理エディタ]で[コンピュータの構成]-[ポリシー]-[Windows 設定]-[セキュリティの設定]

[Network Access Protection]-[NAP クライアント構成]-[実施クライアント]から[IPSec 証明書利用者]を有効にする

[NAP クライアント構成]-[正常性登録の設定]-[信頼されたグループ]を右クリックし[新規]を選択する

サーバー追加で、以下のように URL を登録する。https を使用する場合は https で開始、https を必要するにチェックする

http://<正常性登録機関のサーバー名>/domainhra/hcsrvext.dll

http://<正常性登録機関のサーバー名>/nodomainhra/hcsrvext.dll

802.1x 強制

管理ﾂｰﾙ「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」から[NPS(ﾛｰｶﾙ)]を選択し右ペインの「NAP を構成する」をｸﾘｯｸ[IEEE 802.1X]を選択

構成ウィザード	説明
802.1X 認証ｽｲｯﾁの指定	スイッチなどの 802.1x 対応機器を指定 機器側でもこの NPS を RADIUS サーバーとして指定する必要がある
認証方法の構成	サーバー証明書の選択と、EAP 認証の種類を選択する
仮想 LAN (VLAN)	組織ネットワークの VLAN に、ポリシーに準拠した VLAN ID の設定 制限されたネットワークの VLAN に、ポリシーに準拠しない VLAN ID の設定 それぞれ「構成」ボタンから設定を行うが機器により必要な属性が異なる場合がある

組織ﾈｯﾄﾜｰｸ VLAN 構成	「Tunnel-Type」を選択して「編集」⇒属性の追加で「802.1x で一般的に使用する」を選択 「Tunnel-Medium-Type」を選択、属性追加で「802.1x で一般的に使用する」を選択 「Tunnel-Pvt-Group-ID」を選択、属性追加で、VLAN ID を入力する
制限されたﾈｯﾄﾜｰｸの VLAN	上記と同じ要領で設定を行う

NAP クライアントの構成

[スタート]-[ネットワーク]から、[ネットワーク共有センター]をクリック。

[ネットワーク接続の管理]をクリック、[ローカル接続]のプロパティの[認証]タブ※にて以下の設定を行う。

※認証タブを表示するにはクライアントで[Wired AutoConfig]サービスが有効化されている必要がある

[IEEE 802.1x 認証を有効にする]を選択。[保護された EAP（PEAP）]を選択。

[保護された EAP のプロパティ]で以下の設定を有効にする。

[サーバー証明書を検証する]にチェック。

[認証方法を選択する]で[セキュリティ保護されたパスワード（EAP-MSCHAP v2）]を選択。

[検疫のチェックを有効にする]にチェック。

無線 LAN

標準化	規格	最大速度	使用電波
1997 年	802.11	1/2Mbps	赤外線 / 2.4GHz
1999 年	802.11b	11Mbps	2.4GHz
2003 年	802.11g	54Mbps	2.4GHz
1999 年	802.11a	54Mbps	5GHz
2009 年	802.11n	600Mbps	2.4GHz/5GHz 帯の

Wi-Fi ロゴは、無線 LAN 機器の相互接続性を認証されたことを示す

アドホックモードは、無線 LAN クライアント同士が直接通信する。アクセスポイントは不要。

インフラストラクチャモードは、アクセスポイントを経由して各コンピュータが通信を行う。

無線 LAN セキュリティ

暗号化	説明
WEP	暗号キーの長さは 64bit または 128bit にて暗号化。暗号化アルゴリズムは「RC4」
WPA-TKIP	従来の SSID と WEP キーに加えて、ユーザ認証機能を備えた点や、暗号鍵を一定時間毎に自動的に更新する「TKIP」と呼ばれる暗号化プロトコルを採用する。暗号化アルゴリズムは「RC4」 WPA-PSK：認証サーバを使用せずパスフレーズにて認証を行う（個人向け） 802.1x ：認証サーバを使用して認証を行う（企業向け）
WPA-AES	暗号化アルゴリズムにより強固な「AES」を採用した WPA。AES の鍵長は 128、192、256 ビットから選択
WPA2	CCMP というデータの改ざんを検知する機能が実装されている

802.1x を使用した無線 LAN 認証

802.1x はユーザーの認証及び暗号化の為の動的なキーの生成と配送を行う仕組みを提供する規格で 3 つの要素で構成。

認証サーバー	認証を行うサーバー。802.1x では RADIUS サーバーを使用
オーセンティケータ	802.1x に対応したネットワーク機器

サプリカント	認証される側。つまりクライアント側に必要なソフトウェア

認証サーバーは、管理ツール「ﾈｯﾄﾜｰｸﾎﾟﾘｼｰｻｰﾊﾞｰ」から[NPS（ﾛｰｶﾙ）]を選択し右ペインのドロップダウンリストから、

[802.1x ﾜｲﾔﾚｽ接続またはﾜｲﾔｰﾄﾞ（有線）接続用の RADIUS ｻｰﾊﾞｰ]を選択し[802.1x を構成]をクリックし構成を行う。

ワイヤレスのグループポリシー

クライアントが利用できる無線 LAN の認証方法やアクセスポイントを一元管理するには

[グループポリシーの管理]にて以下のポリシーを作成し割り当てたい OU（組織単位）にリンクさせる。

[ｸﾞﾙｰﾌﾟ管理ﾎﾟﾘｼｰ管理ｴﾃﾞｨﾀ]-[ｺﾝﾋﾟｭｰﾀの構成]-[ﾎﾟﾘｼｰ]-[Windows の設定]-[ｾｷｭﾘﾃｨ]-

[ﾜｲﾔﾚｽﾈｯﾄﾜｰｸ（IEEE802.11）ﾎﾟﾘｼｰ]を右ｸﾘｯｸし、[新しい Windows XP ﾎﾟﾘｼｰ作成]を選択する。

ファイアウォール設定

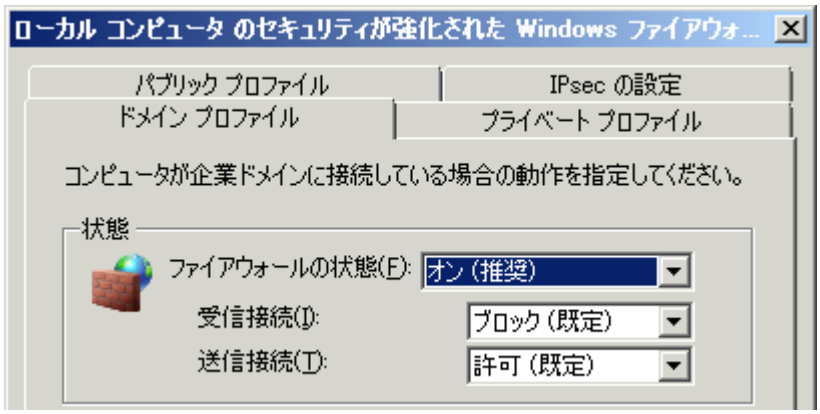
管理ツールのセキュリティが強化された Windows ファイアウォールには 3 つのプロファイルが存在する。

ネットワークの状況により自動的に 1 つのプロファイルが選択される。

プロファイル	説明
ドメイン	コンピュータが AD ドメインに参加しており、DNS サーバーとの通信が可能なときに適用
プライベート	ドメインがないネットワークにコンピュータが接続するときに適用
パブリック	保護されてないネットワークに接続する際に適用。最も厳しい規則が適用される

管理ツール[ﾛｰｶﾙｺﾝﾋﾟｭｰﾀのｾｷｭﾘﾃｨが強化された Windows ﾌｧｲｱｳｫｰﾙ]のプロパティから、ファイアウォールの動作を指定する。

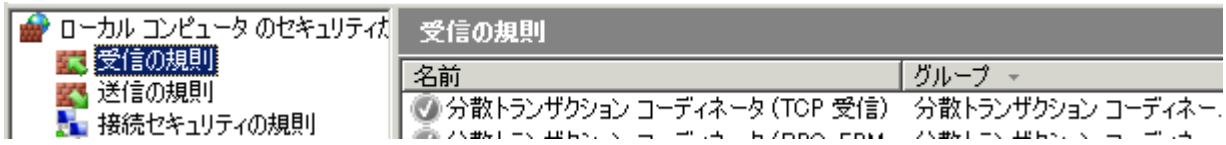
ブロック	「接続を許可する」として作成された規則以外、全ての接続をブロックする
すべての接続をﾌﾞﾛｯｸ	規則の有無に関わらず、接続を全てブロックする
許可	「接続をブロックする」として作成された規則以外以外、全ての接続を許可する



規則の作成

管理ツールの[受信の規則]や[送信の規則]を右クリックし[新規の規則]を選択して作成する。

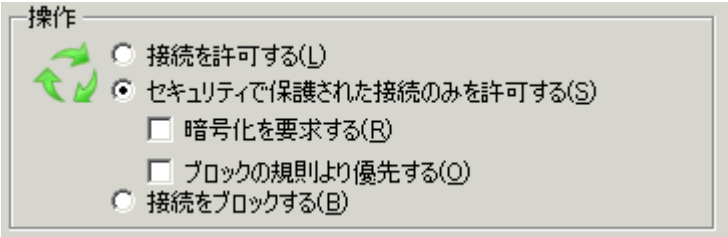
プログラムやポート番号によるフィルタリングを行う。



プロトコル	ポート番号	プロトコル	ポート番号	プロトコル	ポート番号
Telnet	TCP：23	SMNP	TCP：25	Kerberos	TCP/UDP：88

DNS	TCP/UDP：53	RDP	TCP：3389	SMB	TCP：139/445
HTTP	TCP：80	HTTPS	TCP：443	LDAP	TCP：389

受信の規則や送信の規則の[全般]タブの操作にて[ｾｷｭﾘﾃｨで保護された接続のみ許可する]を選択すると、IPSec 認証された接続のみ許可することが可能。[接続を許可する]の場合は、IPSec 認証しない接続も許可される



接続セキュリティの規則

コンピュータ単位で IPSec 認証の構成を簡単に設定することが出来る。

[接続セキュリティの規則]を右クリックし[新しい規則]を選択する

規則の種類	説明
分離	IPSec トランスポートモードによるポリシーを作成（ホスト間での IPSecVPN）
認証の除外	IPSec 通信から除外するためのポリシーを作成する。 IP アドレスやサブネット、アドレス範囲、事前定義されたコンピュータセット等を用いて除外範囲を指定
サーバー間	指定したコンピュータ間に対する IPSec トランスポートモードのポリシーを作成。 IP アドレスやサブネット、アドレス範囲、事前定義されたコンピュータセット等を用いて除外範囲を指定
トンネル	IPSec トンネルモードの IPSec ポリシーを作成（ゲートウェイコンピュータ（ルータ）間での IPsecVPN）
カスタム	カスタム条件で IPSec ポリシーを作成

認証の除外以外を選択した場合は[要件]で以下の何れかを選択する

要件	
受信接続と送信接続に対して 認証を要求する	送受信接続に対して IPSec 通信を要求するが IPSec 通信ができない場合、通常の通信を**行う**
受信接続の認証を必須とし、 送信接続に対して認証を要求する	受信接続に対して IPSec 通信を必須とし、IPSec できない場合は通信を**行わない** 送信接続において IPSec 通信ができない場合、通常の通信を**行う**
受信接続と送信接続の 認証を要求する	送受信に接続に対して IPSec 通信を必須とし、 IPSec 通信ができない場合、通信を**行わない**

監視

[ファイアウォール]にて処理されたログ、[セキュリティアソシエーション]（SA）にて IPSec を確立しているコンピュータの状態が確認できる。またセキュリティアソシアーションでは、メインモードとクイックモードがある。

メインモードではコンピュータ間でキー生成情報を交換する為のセキュアなトンネルを確立しているコンピュータ。

クイックモードでは、実際にパケット交換されているコンピュータの情報が確認できる。

グループポリシーによる一元管理

[ｺﾝﾋﾟｭｰﾀ構成]-[ﾎﾟﾘｼｰ]-[Windows の設定]-[ｾｷｭﾘﾃｨの設定]-[ｾｷｭﾘﾃｨが強化された Windows ﾌｧｲｱｳｫｰﾙ]-[ｾｷｭﾘﾃｨが強化された Windows ﾌｧｲｱｳｫｰﾙ-LDAP://～]の設定から上記のポリシーが全て設定可能。

ここでポリシーを作成し特定の OU に GPO リンクすれば一括でポリシーの管理ができる

■ファイル及び印刷サービスの構成

ファイルサーバー構成

管理ツール[共有と記憶域の管理]にて共有設定の一元管理が可能。

共有設定はフォルダのプロパティにある共有・セキュリティのタブにて設定を行う。

許可の種類	説明
共有アクセス許可	フォルダプロパティの[共有]タブの[詳細な共有]→[アクセス許可]から設定 ネットワーク経由でアクセスするユーザーのみ適用される
NTFS アクセス許可	[セキュリティ]タブにて共有アクセスより細かな設定が行え、ファイルに対しても設定できる ネットワーク経由でアクセスするユーザーだけではなくローカルユーザーにも適用される

ネットワーク経由でアクセスする場合、最初に共有アクセスが評価され拒否されなければ、NTFS アクセス許可を評価する

共有アクセス許可	許可することで、可能になる操作
ﾌﾙｺﾝﾄﾛｰﾙ	全ての操作
変更	ファイルの表示、実行、追加、削除。アクセス権の変更は不可
読み取り	ファイルの表示、実行

NTFS アクセス許可	許可することで、可能になる操作
ﾌﾙｺﾝﾄﾛｰﾙ	全ての操作
変更	既存ファイルの内容変更。新規作成、削除は不可
読み取りと実行	ファイルの表示、実行
ﾌｫﾙﾀﾞの内容の一覧表示	フォルダ内のファイルの表示とプログラムの実行。フォルダにだけ表示される属性
読み取り	ファイルの表示のみ。実行は不可
書き込み	ファイルの新規作成、内容変更。削除は不可
特殊なｱｸｾｽ許可	上記に含まれない特殊なアクセス許可を設定する

[変更]や[書き込み]を拒否すると、アクセス自体ができなくなる。

所有者のみファイル削除可能にするには、ファイルの作成者を示す CREATE OWNER アカウントにフルコントロールの権限を付与すれば良い。Authenticated Users、Everyone は全てのユーザーやグループを示すアカウント。

共有アクセスと NTFS アクセスの設定を一度に行いたい場合は、

フォルダを右クリックし[共有]または、プロパティの[共有]タブの[共有]から設定を行う。

アクセス許可レベル	共有アクセス許可	NTFS アクセス許可
閲覧者	読み取り	読み取りと実行
投稿者	変更	変更
共同所有者	フルコントロール	フルコントロール
所有者	フルコントロール	フルコントロール、所有者※

※通常フォルダの所有者は作成したユーザーだが、NTFS における所有者にはアクセス許可がない場合でもアクセス許可の変更する権限がある

共有アクセス許可同士、または NTFS アクセス許可同士の許可は**累積**される。拒否がある場合は拒否が優先される。

共有アクセスと NTFS アクセスの組み合わせの場合、最終的なアクセス許可は**共通部分のみ許可**される。

共有アクセスに Group1[読み取り]、NTFS アクセスに Group2[フルコントロール]となっているディレクトリに Group1 と Group2 に所属しているユーザーがアクセスした場合、[読み取り]しか行えない

アクセスベースの列挙

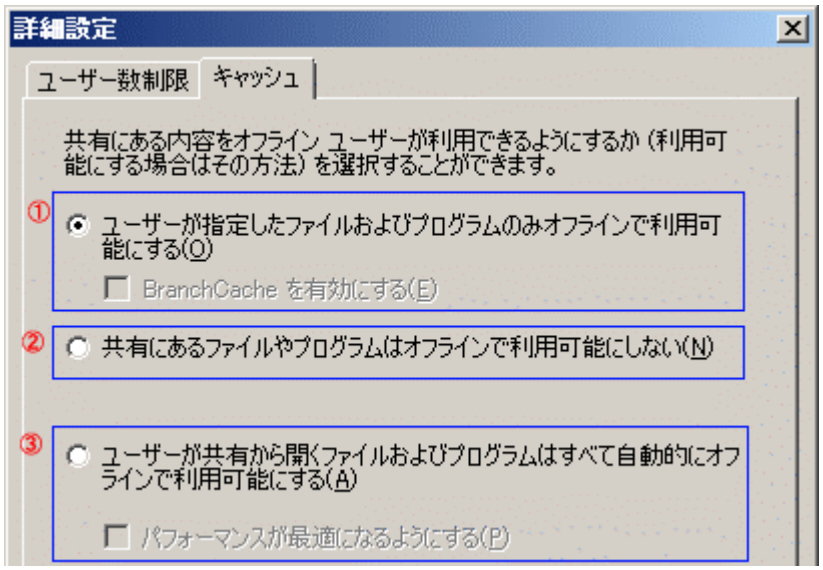
共有フォルダをネットワーク経由で参照した場合、アクセス権のないファイルやフォルダを表示させない機能。

管理ツール[共有と記憶域の管理]から共有フォルダのプロパティを開き、[共有]タブの[詳細設計]をクリック。

[ユーザー数制限]タブに[アクセスベースの列挙を有効にする]のチェックボタンがある

オフラインフォルダ

[共有と記憶域の管理]から共有フォルダのプロパティから[共有]タブ[詳細設計]をクリック。[キャッシュ]タブにて設定



① ネットワークに接続していないときにアクセスするファイルまたはプログラムを自分で指定する必要がある

② オフラインフォルダの使用を許可しない

③ 共有フォルダ内にあるファイルまたはプログラムを開くとキャッシュされオフラインで使用可能になる

[ﾊﾟﾌｫｰﾏﾝｽが最適になるようにする]にチェックを入れると、EXE、DLL などはアクセスしなくても自動的にキャッシュされるようになる（Windows Vista 以降では意味がない）

BranchCache とはキャッシュされたオフラインファイルを他のコンピュータで更に利用可能にしたもの。※R2

動作モード	説明
分散キャッシュ	クライアントとして使用している Windows 7／Windows Server 2008 R2 だけでお互いにデータをキャッシュしてやり取りするモード。50 台程度までのネットワークに向いている
ホスト型キャッシュ	リモートからアクセスしたコンテンツはキャッシュ専用サーバーにコピーされ、各クライアントはキャッシュ専用サーバーからコンテンツを参照する

共有フォルダのシャドウコピー

ある時点でのファイルやフォルダのスナップショットのこと。

シャドウコピーは HDD のプロパティ[シャドウコピー]タブから設定する。パーティション単位でしか行えない。

シャドウコピーを有効にするとフォルダプロパティの[以前のバージョン]から

スナップショットされている時間でのファイルを復元可能になる。過去のバージョンは 64 個まで保存される。

vssadmin　オプション

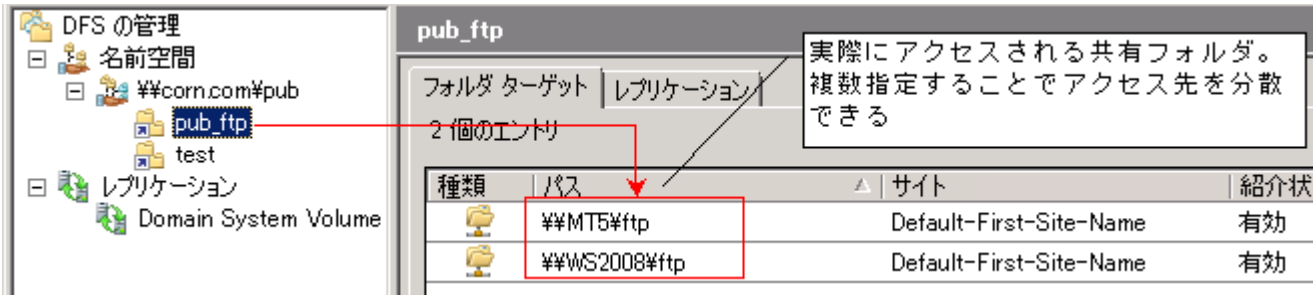
オプション	説明
Add ShadowStorage	シャドウコピーを保存する記憶域を指定 （例）vssadmin Add ShadowStorage /For=C: /On=D: /MaxSize=900MB
Delete ShadowStorage	シャドウコピー記憶域の関連づけを削除 （例）vssadmin Delete ShadowStorage /For=C: /On=D:
Create Shadow	新しいシャドウコピーを作成（例）vssadmin Create Shadow /For=C: /AutoRetry=2
Delete Shadows	既存のシャドウコピーを削除（例）vssadmin Delete Shadows /For=C: /Oldest

List Shadows	シャドウコピーの一覧表示
List ShadowStorage	シャドウコピー記憶域の関連づけ一覧表示
Revert Shadow	シャドウコピーを復元。スナップショット時点までの状態に戻る
Query Reverts	シャドウコピー復元操作の進行状況を表示

DFS（Distributed File System）構成

複数のファイルサーバーの共有フォルダに対し、仮想的な共有フォルダのツリーをユーザーに提供する。

DFS 名前空間に作成されたターゲットを持つフォルダにアクセスするとターゲットとなる別の共有フォルダに自動的にリダイレクトされる。名前空間のフォルダには複数のターゲットを割り当てることもできる



DFS 名前空間	説明
名前空間のパス	ドメインベースの名前空間では「¥¥ドメイン名¥ルート名」 スタンドアロンの名前空間では「¥¥サーバー名¥ルート名」と表記。
名前空間サーバー	DFS 名前空間を保存するサーバー
名前空間ルート	DFS 開始ポイント。インストールすると「C¥DFSRoots¥」に作成される
フォルダ	リンク先であるフォルダターゲットを持つものと、通常のフォルダの両方を配置可能

ドメインベースの名前空間

Active Directory 必須。名前空間サーバーにドメイン名を指定している為、

名前空間を変更してもユーザーが指定する UNC（ネットワーク上のリソースを示す表記規則）に変更はない。

フォールトトレラントな名前空間（1 つの名前空間を複数の名前空間サーバーに格納する機能）をサポートする。

名前空間サーバーは、同じドメインのドメインコントローラか、メンバサーバーのみ追加可能。

左記 2 つのサーバーそれぞれにフォルダターゲットが作成される為、どちらかがダウンしても該当のフォルダへアクセス可能。

名前空間サーバーはサイトの近い方が使用される

スタンドアロンの名前空間

Active Directory 不要。名前空間サーバーが変更されると UNC も変更する。

Active Directory 環境であれば、DFS レプリケーションは可能。

DFS のインストールと名前空間の構成

「ファイルサービス」の役割から[分散ファイルシステム]サービス追加

自動で「C¥DFSRoots¥<ルート名>」の共有フォルダが読み取り専用で作成される。

管理ツール「DFS の管理」から各種設定（フォルダや名前空間サーバーの追加等）が行える。

DFS レプリケーションの構成

ドメイン環境の場合、同じフォルダに関連付けられたフォルダのターゲット間でレプリケーション設定が行える。

DFS レプリケーション（ブロック単位で変更のみレプリケート）もサポート。

ターゲットのフォルダはそれぞれ別の名前空間サーバーの必要がある。

初期複製時、レプリケーショングループのメンバとプライマリメンバで同じファイルがあった場合、

プライマリメンバのファイルが優先される。トポロジは以下の 2 つより選択する。

トポロジ	説明
ハブおよびスポーク	3 つ以上のレプリケーションメンバがいる時に選択可能。中心となるフォルダターゲット（ハブ）に他のフォルダターゲット（スポーク）が接続し、ハブ⇔スポーク間でレプリケート
フルメッシュ	すべてのフォルダターゲットがレプリケーショングループの全メンバとレプリケートする。メンバが多くなるとトポロジが複雑になる為、10 以下の場合にのみ使用することを推奨

アクセスベースの列挙

DFS 空間でアクセスベースの列挙を使用するには以下の設定が必要

① Active Directory の機能レベルが「Windows Server 2008」

② dfsutil property abde enable [¥¥ドメイン DFD¥DFS ルート]にて DFS ルートの ABE 設定

③ dfsutil property acl deny コマンドにて表示を拒否するアクセス許可の設定

バックアップ及び復元

- 機能の追加にて「Windows Server バックアップ」をインストールする必要がある
- バックアップ対象は NTFS フォーマットのみ。FAT フォーマットはバックアップできない
- ドライブ単位でのバックアップをサポート。フォルダ単位ではできない
- バックアップ先は、NTFS のローカル HDD、DVD メディア、リムーバブルをサポート
- テープや別ネットワークの共有フォルダへのバックアップはできない
- 完全バックアップと、増分バックアップに対応
- ネットワーク経由で別のコンピュータのバックアップを行う場合、管理対象となるコンピュータに「Windows Server バックアップ」機能がインストールされてる必要がある。
- [操作]⇒[別のコンピュータへの接続]にてリモートコンピュータのバックアップが行える

Windows Server 2003 など従来のバックアップ（NTBackup.exe）とは次の違いがある

バックアップ対象	ボリューム単位で指定。フォルダやファイル単位は不可。復元はフォルダ・ファイル単位可能
バックアップ方式	完全バックアップと増分バックアップに対応
バックアップ先	ディスク、共有フォルダ、DVD など。テープデバイスはサポートしていない
バックアップデータ形式	VSS のスナップショットとディスクのブロックレベルでのバックアップ技術を採用。バックアップ対象のボリュームをディスクイメージとして取得し VHD ファイルに格納する

wbadmin オプション

オプション	説明
enable bacukup	デイリーバックアップスケジュールを有効にする。disable で無効

start backup	１回限りのﾊﾞｯｸｱｯﾌﾟを実行。ﾊﾟﾗﾒｰﾀなしで実行するとﾃﾞｲﾘｰﾊﾞｯｸｱｯﾌﾟｽｹｼﾞｭｰﾙの設定を利用してﾊﾞｯｸｱｯﾌﾟする。-allcritical を付与すると OS のｺﾝﾎﾟｰﾈﾝﾄが存在する重要なﾎﾞﾘｭｰﾑをﾊﾞｯｸｱｯﾌﾟ対象として指定することができる
start recovery	復元の実行
stop job	実行中のバックアップ、回復オペレーションを停止する
get versions	回復可能なバックアップデータのバージョン番号を一覧表示する
get status	現在実行しているバックアップまたは回復操作の状況を表示する
start systemstatebackup	システム状態のみバックアップを行う。-backuptarget:f: でＦドライブにバックアップ
start systemstaterecovery	システム状態のみ復元する

バックアップからの復元

管理ツール[Windows Server バックアップ]から[操作]-[回復]を選択し復元を行う。

回復の種類は、[ファイルおよびフォルダ]、[アプリケーション]、[ボリューム]から選択可能。

回復オプション指定では、ファイルや、フォルダの復元先や、セキュリティ設定の復元するかの設定を行う。

サーバーの復元には、Windows Server 2008 のインストールディスクと、バックアップファイルが格納されているディスクが必要。インストールディスクでコンピュータを起動後、「システム回復オプション」にアクセスし「Windows Complete PC 復元」を選択する。

ディスククォータ管理

クォータ	説明
ユーザー単位	役割や機能追加なしに設定可能。ボリュームに対して設定し、ユーザー単位で使用量の制限などを行う ボリュームのプロパティ「クォータ」から各種設定を行う
フォルダ単位	フォルダに対してクォータを割り当てる。ユーザー単位での制限はできない。 閾値に達した際に大きいサイズのファイルや、クォータ使用率をレポートとして保存できる。 レポートを電子メールで送信することも可能 「ファイルサービス」役割の[ファイルサーバーリソースマネージャ]サービスが必要

フォルダ単位のディスククォータ

管理ツール「ファイルサーバーリソースマネージャ」にてクォータの割り当てを行う。

閾値はクォータテンプレート（既定で 6 つ作成されている）を使用するか「カスタムプロパティ」にて都度作成する。

クォータ作成の項目

項目	説明
クォータのパス	クォータを接待するフォルダを指定
パスにクォータを作成する	クォータパスにクォータを割り当てる場合に選択
規定と新規のｻﾌﾞﾌｫﾙﾀﾞに自動でﾃﾝﾌﾟﾚｰﾄ適用とｸｫｰﾀ設定を行う	クォータパス内の既定および新規サブフォルダに自動的にクォータの設定を割り当てる場合に選択
ｸｫｰﾀﾃﾝﾌﾟﾚｰﾄからﾌﾟﾛﾊﾟﾃｨを取得する	既存のテンプレートを選択してクォータを設定する
ｶｽﾀﾑｸｫｰﾀのﾌﾟﾛﾊﾟﾃｨを定義する	テンプレートを使わずに個別にフォルダに対してクォータを設定する

クォータテンプレートのプロパティ項目

プロパティ	説明
テンプレート名	クォータテンプレート名
制限	クォータ閾値を指定。単位として、KB、MB、GB、TB が選択できる
ハードクォータ ソフトクォータ	制限を超えるとデータの保存ができない 制限を超えてもデータの保存が可能（ハードかソフトかどちらか一方を選択する）
通知のしきい値	指定した閾値（%）に達したときのアクションを指定

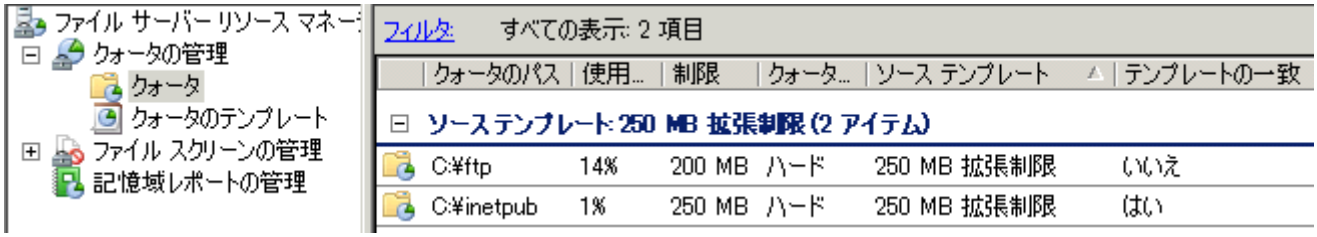
コマンドラインでクォータの管理を制御するには、dirquota コマンドを使用する

（例）dirquota quota list　設定されているクォータを一覧表示できる

テンプレートを変更した時のポップアップ

元のテンプレートに一致する取得したクォータのみにテンプレートを適用する

クォータテンプレートを使用してクォータを設定した後、プロパティにてクォータの値を変更した場合、管理ツールに表示されるテンプレートの一致が「いいえ」になる。この「いいえ」となったクォータは変更せず、テンプレートと完全に一致しているクォータのみ変更を反映させる場合に選択する



取得したクォータすべてのテンプレートを適用する

変更したテンプレートを使用して作成された既存のすべてのクォータを変更する

取得したクォータにテンプレートを適用しない

既定のクォータに変更を反映させない

ファイルスクリーンの管理

使用量ではなく、ファイルの拡張子により書き込みを禁止させる機能。

ファイルグループにて特定拡張子のグループを作成し、そのグループにファイルスクリーンを適用する。

[ファイルスクリーンの例外]を設定すると、親フォルダの設定より優先される。

C:¥ftp　　← ファイルスクリーンで拡張子.avi の保存が禁止されているとする

C:¥ftp¥move　← ファイルスクリーンの例外で、拡張子.avi を許可すると、このフォルダに対しては保存可能になる

move フォルダに特定ユーザーのみ「変更」の権限を付与することで、特定ユーザーのみ.avi が保存可能になる

記憶域レポート管理

閾値を超えた場合ではなく定期的にフォルダの使用状況のレポートを作成できる。

レポート作成されるスケジュールや、メールへの送信なども可能。Storrept コマンドでも設定可能。

ファイル管理タスク　※R2

ファイルの有効期限タスクを設定し、条件に一致したファイルを指定のフォルダに移動させることが出来る。

条件は分類管理ツリーにある**分類プロパティ**及び、**分類規則**から独自の条件を作成できる。

ファイルの場所、分類プロパティ、時間等に基づき、ファイルにコマンドやスクリプトを自動実行できる。

印刷サービスの監視及び構成

ネットワークを経由して複数のコンピュータでプリンタを共有できるようにするためのサーバ機能。
役割や機能の追加を行わなくてもプリントサーバーとして動作するが「印刷サービス」役割の[プリントサーバー]サービスをインストールすることで管理ツール「印刷の管理」にて複数プリントサーバーやプリンタの管理などが行える。
[LPD サービス]サービスをインストールすることで LPR サービスを利用している UNIX 等がプリンタを使用できるようになる。
[LRP ポートモニタ]の機能をインストールすると UNIX ベースのプリンタに出力することが可能になる

プリンタのプロパティ項目

[共有]タブ	説明
このプリンタを共有する	プリンタ共有の有効・無効を設定
ディレクトリに表示する	Active Directory にプリンタを公開することで、クライアントが[Active Directory 検索]を行うことで安易にプリンタを見つけることができる
追加ドライバ	共有プリンタに接続するクライアントに自動手配布するドライバを追加する

クライアント側はネットワークから目的のプリンタ見つけ、右クリックから「接続」を行うことで自動的にドライバがダウンロードされプリントサーバーに印刷要求を出すことができるようになる

[セキュリティ]タブではプリンタのアクセス許可を設定する。

グループまたはユーザー	既定の許可項目	対象
Eveyone	印刷	全てのユーザー
CREATE OWNER	ドキュメントの管理	印刷要求を行ったユーザー
administrator と Administrators	印刷、ドキュメントの管理、プリンタの管理	管理者

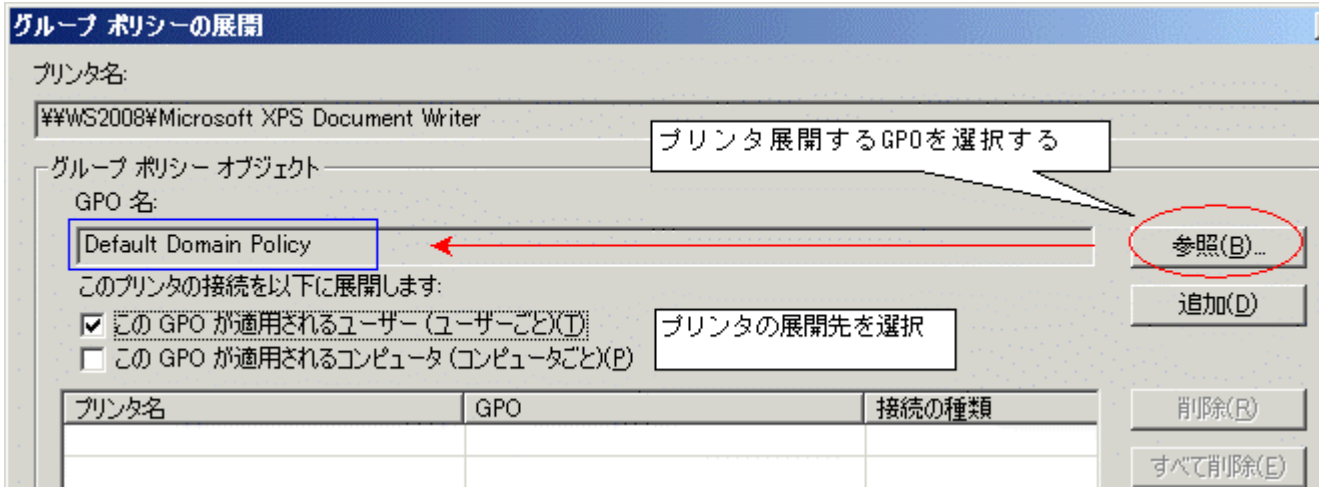
設定項目	説明
印刷	印刷が行える
このプリンタの管理	プリンタのプロパティ変更や、キューイングを制御できる
ドキュメントの管理	印刷プリンタのキューイングを制御できる

グループポリシーを使用したプリンタの展開

グループポリシーを使用してドメインのユーザーやコンピュータに共有プリンタへのプリンタ設定を自動展開できる。
自動展開できる単位は、[サイト/OU]、[ドメイン]、[すべて]の何れか。
展開されたユーザーまたはコンピュータには[プリンタと FAX]内にプリンタが表示されるようになる。

同じプリンタを追加し、異なるプロパティを設定したうえでプリンタの展開を行えば、
ユーザー毎にプリンタの設定（白黒印刷、カラー印刷など）を振り分けることが可能。

管理ツール[印刷の管理]より対象プリンタを右クリック[グループポリシーの展開]を選択。
[参照]からプリンタを展開させたい GPO を選択し、展開先をチェック後、[追加]を押下する



Windows XP 以前の端末にグループポリシーを用いてクライアントにプリンタの接続を展開するにはスタートアップスクリプトか、ログオンスクリプトに「PushPrinterConnections.exe」ユーティリティを追加する必要がある

カスタムフィルタ

特定の条件に一致するプリンタをリアルタイムにフィルタ表示できる。

フィルタ条件に一致した時の動作としてメール送信やスクリプトの実行なども指定可能。

フィルタ	説明
すべてのプリンタ	すべてのプリンタを表示
すべてのドライバ	すべてのドライバを表示
ジョブのあるプリンタ	プリンタのキュー内に印刷ジョブが１つ以上あるプリンタを表示
準備ができてないプリンタ	プリンタキューの状態が[準備完了]以外のステータスのプリンタを表示

ジョブのあるプリンタ、準備ができていないプリンタは右クリックのプロパティから、

フィルタ条件のカスタマイズができる。フィールド、条件、値を組み合わせてフィルタ条件を絞り込む。

準備ができてないプリンタのカスタム条件は「フィールド：キューの状態」、「条件：完全一致しない」、「値：準備完了」

■ネットワークインフトラクチャの監視及び管理

Windows Server Update Services サーバー設定を構成

WSUS は無料のアドオンツールで MicroSoft 社からダウンロードする。

WSUS3.0 をインストールするには、以下のコンポーネントが必要。また圧縮ドライブにインストールはできない

① インターネットインフォメーションサービス（IIS）

　└ ASP.NET / Windows 認証 / 静的なコンテンツの圧縮 / IIS6 メタベース互換 のコンポネート追加

② バックグラウンドインテリジェント転送サービス（BITS）

③ .NET Framework2.0 SP1 と .NET Framework2.0 SP1 日本語 Language Pack

④ MMC3.0

⑤ Report Viewer 2005 SP1 と Report Viewer 2005 日本語 Language Pack

②～④は OS 標準の為、実際は①と⑤をインストールする。

WSUS3.0 のインストール時、更新プログラムの保存場所や、クライアントの更新状態を管理する為の DB を指定する。

ｵﾌﾟｼｮﾝで設定可能項目	説明
更新先とプロキシサーバー	更新プログラムの取得先を選択する。WEB ページ、WSUS サーバーのどちらか。 WSUS サーバーから取得する場合、アップストリームサーバーのレプリカがチェック可能

製品とクラス	ダウンロードする更新プログラムの種類を指定する
更新ﾌｧｲﾙと更新言語	更新プログラムの保存方法や、DL 対象とする言語を指定
同期スケジュール	更新プログラムをダウンロードするスケジュールを指定
自動承認	条件に一致した製品とクラスの更新プログラムを自動的に承認のステータスにする
コンピュータ	新規に登録されたコンピュータが割り当てられるグループ決定方法
ｻｰﾊﾞｰｸﾘｰﾝｱｯﾌﾟｳｨｻﾞｰﾄﾞ	使用してない更新プログラムを削除する
ロールアップのレポート	更新プログラム適用情報をアップストリームサーバーに送信するか、しないかの設定 レプリカのダウンロードサーバーのみ指定可能
電子メール通知	新しい更新プログラムが同期された時のメール送信を設定
個人用設定	レプリカサーバーからロールアップされた情報を、どこまで表示するか設定

クライアント側の設定

gpedit.msc コマンドにて「ローカルグループポリシーエディタ」を開き

[ｺﾝﾋﾟｭｰﾀの構成]-[管理用ﾃﾝﾌﾟﾚｰﾄ]-[Windows ｺﾝﾎﾟｰﾈﾝﾄ]-[Windows Update]から

「自動更新を構成する」及び「ｲﾝﾄﾗﾈｯﾄの Microsoft 更新サービスの場所を指定する」を有効にする。

ドメインメンバの場合は「グループポリシー」にて一括管理を行える。

[ｺﾝﾋﾟｭｰﾀの構成]-[ﾎﾟﾘｼｰ]-[管理用ﾃﾝﾌﾟﾚｰﾄ]-[Windows ｺﾝﾎﾟｰﾈﾝﾄ]-[Windows Update]

自動更新を構成する

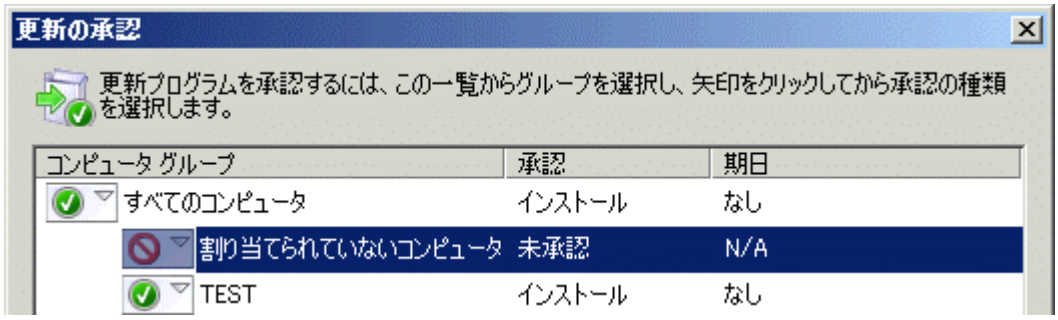
自動更新構成	説明
2.ﾀﾞｳﾝﾛｰﾄﾞとｲﾝｽﾄｰﾙを通知	更新プログラムを DL する前とｲﾝｽﾄｰﾙする前にメッセージをユーザーに通知
3.自動ﾀﾞｳﾝﾛｰﾄﾞしｲﾝｽﾄｰﾙを通知	更新プログラムの DL は自動で行われ、インストール前に通知する
4.自動ﾀﾞｳﾝﾛｰﾄﾞしｲﾝｽﾄｰﾙ日時を指定	更新プログラムの DL は自動で行われ、指定した日時にインストールされる
5.ﾛｰｶﾙ管理者の設定選択を許可	WSUS クライアントの管理者ユーザーがコントロールパネルの[自動更新]でオプションを設定することを許可する

イントラネットの Microsoft 更新サービスの場所を指定する

設定	説明
更新を検出するためのｲﾝﾄﾗﾈｯﾄの更新ｻｰﾋﾞｽを指定する	クライアントが更新プログラムを DL する WSUS サーバーを指定
ｲﾝﾄﾗﾈｯﾄ統計サーバーの指定	更新プログラム適用状態を報告するサーバーを指定

更新プログラムの承認

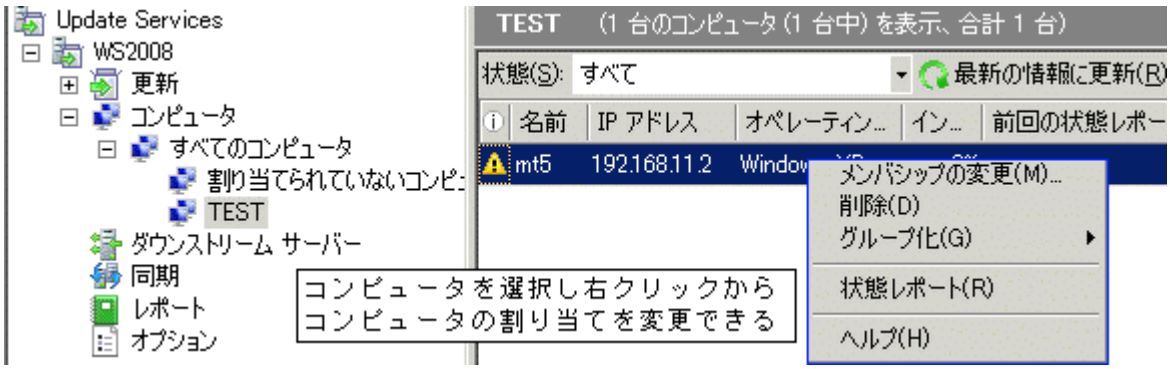
更新したいプログラムを右クリックし「承認」をクリックし、適用したいコンピュータグループを選択する。



[コンピュータ]-[すべてのコンピュータ]から右クリックし、[コンピュータの追加]で新規グループを作成し、

[割り当てられていないコンピュータ]から任意のコンピュータを選択し[メンバシップの変更]が可能。

コンピュータの一覧はクライアント側の設定を行っているコンピュータのみ表示される



ブラウザ経由での Windows Update を禁止する

グループポリシーにてクライアントに WSUS を設定しても IE から Windows Update は行える。

これを制限するには、グループポリシーから[Windows Update へのリンクとアクセスを削除する]と

[Windows Update のすべての機能へのアクセスを削除する]を有効にする。

リモート管理

WSUS3.0 のインストール時のモードにて「管理コンソールのみ」を選択すればリモートで WSUS サーバーを管理できる。

WSUS 管理ツールから[Update Services]を右クリックし、[サーバーに接続]を選択する。

その際、ポート番号のプルダウンを 80 から 443 にするか、SSL を使用するにチェックを入れることで通信を暗号化できる。

SSL を使用するには WSUS サーバー側に SSL 用のサーバー証明書がインストールされている必要がある。

WSUS サーバーのチェーン化

WEB から更新プログラムを DL し管理する WSUS サーバー（アップストリームサーバー）を構成し、

アップストリームサーバーから更新プログラムを DL し管理する WSUS サーバー（ダウンストリームサーバー）の構成。

ダウンストリームサーバーを構成するには WSUS 管理ツールのオプションから[更新先およびプロキシサーバー]を選択し、

「別の Windows Server Update Services サーバーから同期します」を選択しアップストリームサーバーの URL を入力する。

通常は、各ダウンストリームサーバーでそれぞれ承認作業を行う必要がある。

アップストリームサーバーの承認情報を引き継ぎダウンストリームサーバーで承認の管理を行いたくない場合は、

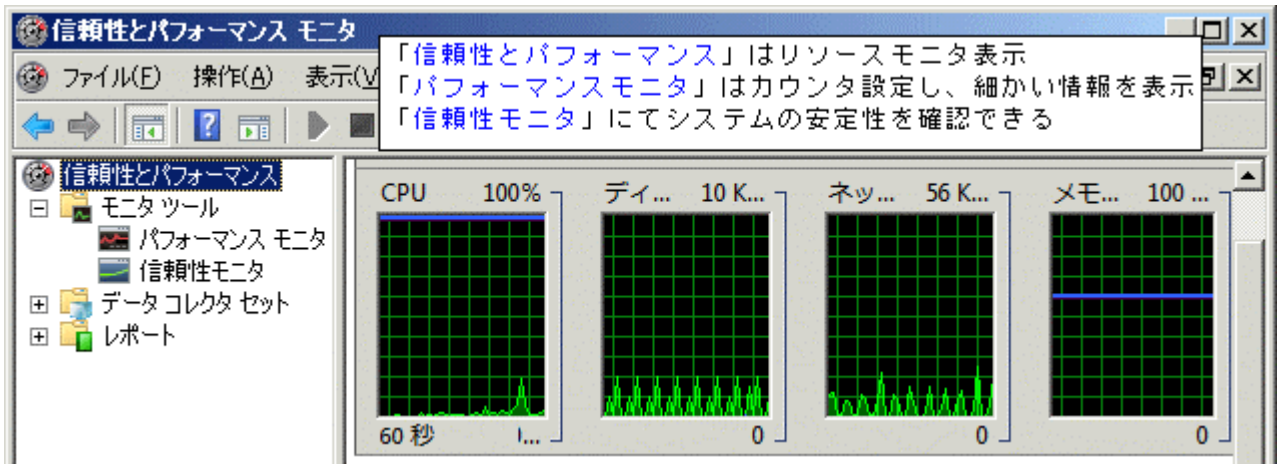
「このサーバーはアップストリームサーバーのレプリカです」のチェックを入れる

Wsusutil コマンド

C:¥Program Files¥Update Services¥Tools ディレクトリに格納されている

ｵﾌﾟｼｮﾝ	説明
checkhealth	WSUS サーバーの稼働状態や検出要件などのチェックを行いイベントログに記録する
reset	DB のすべての更新メタデータ行にファイルシステムに格納されている対応する更新ファイルが含まれている事を確認する。更新ファイルが不足していたり壊れていた場合、更新ファイルをもう一度 DL する
deleteunneededrevisions	不必要な更新プログラムの改訂版の更新メタデータを、データベースから削除する

システム状態データを収集する



データコレクタセットで、取得したいカウンタ値を設定し、開始を行うことでパフォーマンスモニタの情報をファイルに保存できる。当該ファイルをローカルで確認することで細かいリソースの診断が可能。

信頼性モニタでは以下の３つのカテゴリにてシステムの稼働状況を確認できる

システム安定性グラフ	数値が 10 に近い程、システムが安定していることを示す。 イベントログのエラーや警告によってこの数値が決まる
カテゴリ毎の情報一覧	ｿﾌﾄｳｪｱのｲﾝｽﾄｰﾙまたはｱﾝｲﾝｽﾄｰﾙ、ｱﾌﾟﾘｹｰｼｮﾝｴﾗｰ、ﾊｰﾄﾞｳｪｱｴﾗｰ、Windows ｴﾗｰ、その他のｴﾗｰ の 5 つのカテゴリごとにシステム安全性に影響を与えたイベントを表示
安全性レポート	発生したイベント毎の具体的な内容

情報収集のエージェント

信頼性モニタはスケジュールされた RACAgent タスクによって提供されるデータを使用する。

既定では有効になっているが、無効になっていると信頼性モニタが使用できない。有効化の手順は以下の通り。

管理ツール[タスクスケジューラ]を起動。コンソールツリーから[RAC]を選択し右クリック。

「表示」⇒「非表示になっているタスクを表示する」で中央ペインに表示された RACAgent を右クリックし「有効」

リモートコンピュータの情報表示

[信頼性とパフォーマンス]を右クリックし「別のコンピュータへの接続」を選択する。

リモートコンピュータ側で「リモートレジストリサービス（Remote Registry)」が実行されている必要がある。

イベントログを監視する

Wevtutil ツールにて、イベント ログおよび発行元に関する情報の取得、イベント マニフェストのインストールおよびアンインストール、クエリの実行、ログのエクスポートアーカイブおよびクリアが可能。

従来のイベントビューワから改善された点

カスタムビュー	条件にマッチしたものだけを表示する独自のビューを作成する
Windows ログ	システムログ、アプリケーションログ、セキュリティログなど従来形式で表示
ｱﾌﾟﾘｹｰｼｮﾝとｻｰﾋﾞｽﾛｸﾞ	サービスやアプリケーション毎にイベントが表示される
イベントのサマリー	過去 1 時間、24 時間、7 日間のイベントサマリー（エラー回数など）が表示

イベントログとタスクの連動

右ペインに表示されるメニュー（リリースバージョンとカスタムか Windows のログを選択しているかで表示が異なる）から
そのイベントが書き込まれた場合に、指定のプログラムを実行、電子メールを送信、ポップアップを表示の何れかのアクション
を設定できる。設定したアクションはタスクスケジューラに登録される

VER	カスタムビュー	Windows ログ	条件
R1	タスクをこのカスタムビューに添付 タスクをこのイベントに添付	タスクをこのカスタムビューに添付 タスクをこのイベントに添付	ログが書き込まれた時 当該イベントが書き込まれた時
R2	このカスタムビューにタスクを設定 このイベントにタスクを設定	このログにタスクを設定 このイベントにタスクを設定	ログが書き込まれた時 当該イベントが書き込まれた時

特定のカスタムビューを選択した状態で、「タスクをこのカスタムビューに添付」から設定を行った場合、
そのカスタムビューにログが書き込まれたら、設定したアクションが実行されるようになる。
同様に「タスクをこのイベントに添付」で設定した場合は、そのイベント内容が書き込まれた場合に実行される。

イベントサブスクリプション

複数のリモートコンピュータからイベントのコピーを収集してローカルコンピュータに格納する機能のこと。

①ソースコンピュータと、コレクタコンピュータでそれぞれ以下のコマンドを実行する

winrm quickconfig	ソースコンピュータで実行
wecutil qc	コレクタコンピュータで実行

②各ソースコンピュータのローカル administrators グループにコレクタコンピュータのコンピュータアカウントを追加
GUI ツールまたは、net localgroup Administrators /add ﾄﾞﾒｲﾝ名¥ｺﾝﾋﾟｭｰﾀ名$　で追加する
※最後の $ は追加するのがユーザーではなくコンピュータであることを示す

③コレクタコンピュータでサブスクリプションを作成する（サブスクリプションを選択し、右クリック）

プロパティ	説明
サブスクリプション名	サブスクリプション設定を識別する名前
宛先ログ	ソースコンピュータから収集したイベントを表示するイベントビューワの場所を指定 既定では「転送されたイベント」に格納される
サブスクリプションの種類とソースコンピュータ	コレクタ側から情報を収集（コレクタによる開始）か、ソースコンピュータ側が情報を送信（ソースコンピュータによる開始）するか選択する。
コンピュータの選択	ログの収集元となるソースコンピュータを選択する
収集するイベント	収集するイベントの条件を設定する

サブスクリプションを実装するには「Windows イベントコレクターサービス」が実行されている必要がある

ネットワークデータを収集する

Microsoft Network Monitor を DL しインストールする。以降、Ver3.4 をベースに説明。

フィルタなしのキャプチャー

「New Capture」ボタンを押下するとキャプチャー用の画面が開く。Start を押下するとキャプチャーが実行される

フィルタを適用する

「Capture Settings」ボタンを押下し、フィルタの条件を追加する。

（例）IPv4.SourceAddress == 192.168.11.14　※AND や OR にて複数条件も追加可能。

「Load Filtter」からテンプレートや、自分で作成したフィルタを読み込める。

P-Mode でのキャプチャ

既定ではローカルコンピュータと他のコンピュータとの通信トラフィックをキャプチャするが、

P-Mode（プロミスモード）に設定すると他のコンピュータ同士の通信も含めて全てキャプチャすることができる。

「Select network adapters captuer」画面から対象の LAN にチェックを入れ、プロパティから P-Mode のチェックを入れる。

キャプチャしたパケットの表示

「Display Filter」画面にフィルタ条件を追加し「Apply」で適用する。

パケットキャプチャーされた項目を右クリックし「Add Selected Value to Display Filter」を選択して追加もできる。

「Save As」にて「Displayed frames」を選択して保存することでフィルタ条件のパケットのみ保存される。

カラムの追加

Frame Summary の「Colums」から「Choose Colums」を選択することで表示するカラムをカスタマイズ可能。

IP アドレスを任意のホスト名で表示する

Frame Summary の「Aliases」から「Manage Aliases」を選択し「New」ボタンから IP アドレスとホスト名を設定する。

コマンドラインでのキャプチャー

Network Monitor をインストールすることで使用可能になる。

nmcap オプション

オプション	説明
/network　NIC 名	キャプチャー対象のネットワークアダプタを指定。（例）"ローカル エリア接続" や *
/capture ﾌﾟﾛﾄｺﾙ名	キャプチャー条件を指定するフレームフィルタ。（例）tcp udp icmp dns Ipv4 SMB など (条件 and 条件)のように繋げることが可能
/file ﾌｧｲﾙ名	キャプチャーを保存するファイル名を指定
/startwhen /time	キャプチャ開始時刻。（例）19:00 04/11/2011
/stopwhen /timeafter	キャプチャ開始後からの終了時間。（例）30 min
/inputcapture	保存したキャプチャーファイルを読み込む

■Windows Server 2008 R2 新機能

Direct Access

社外に持ち出したモバイル PC をインターネットに接続するだけで、社内ネットワークと同様の環境を実現する仕組み。

DirectAccess クライアントは、IPSec over IPv6 トンネルを通して社内ネットワークに IPv6 でアクセスする。

クライアント PC が IPv4 でインターネットに接続している場合、DirectAccess サーバへの IPv6 接続には 6to4 および Teredo が使われる

VPN との違い

① インターネットに接続するだけで、自動で社内ネットワークに接続

② セットアップは自動で完了。グループポリシーベースの設定

③ イントラネットへのアクセスとインターネットへのアクセスの分離

Direct Access の接続プロセス

Direct Access クライアントがインターネットに接続すると、管理者が指定したイントラネット Web サーバーに接続する。
Web サーバーに接続できれば社内、接続できなければ社外（インターネット接続）と判断する

Direct Access サーバーへの接続（以下の 4 つのパターンを自動的に選択して接続する）

接続形態	パターン	適用される IPv6
IPv6	IPv6 アドレスが割り振られた場合	そのまま踏襲
6to4	パブリック IPv4 アドレスが割り振られた場合	2002::/16
Teredo	プライベート IPv4 アドレスが割り振られた場合	2001:0000::/32
IP-HTTPS	ファイアウォールによって、6to4 や Teredo がブロックされている場合	2002::/16

DirectAccess サーバーへの接続を試み、IPSec のサーバー認証、クライアント認証を経て
IPSec over IPv6 のセキュアなトンネル（IPv6 および IP プロトコル番号 50 の ESP を使用）を構築。
このトンネルを用いて社内のイントラネットとシームレスな通信を行うことができる。

6to4 は IPv6 パケットを IPv4 パケットでカプセル化（IP プロトコル番号 41 を使用）して、
リモートの IPv6 ネットワークに接続する

Teredo は IPv6 トラフィックを IPv4 でトンネリングするテクノロジであるが、プライベート IPv4 アドレスから NAT 経由で接続することを可能にするために、UDP データグラム（UDP ポート 3544）を使用して IPv6 パケットをカプセル化する

必要な要件

- クライアントは Windows 7 Enterprise、Ultimate（ドメイン参加済み）
- 2 つの物理 NIC。NIC の一方は社内のプライベートネットワークに接続され、もう一方はパブリックな IP アドレスでインターネットに接続されていること
- インターネット接続側の NIC には、連続した 2 つのパブリック IPv4 アドレスを割り当てること
- Active Directory 証明書サービスによるエンタープライズ PKI が展開されていること
- Windows Server 2008 SP2 以降の DC と DNS が 1 台（スマートカードを使用する場合は 2008 R2）が存在すること

Direct Access サーバーの構築

[機能追加]より[DirectAccess 管理コンソール]をインストールし、管理コンソールから以下を設定する。

設定項目	設定内容
DirectAccess クライアント	サーバーに接続するクライアント
DirectAccess サーバー	NIC、証明書
インフラストラクチャサーバ	DC、DNS
アプリケーションサーバー	接続先となるサーバー

IP-HTTPS で接続ができない（名前解決ができない）対応

DirectAccess サーバーの外部 FQDN と社内の Active Directory のドメイン名が同じ場合、
DirectAccess サーバーのパブリックな IPv4 アドレスを正しく名前解決できなくなる。
DirectAccess の設定を行う際に、社内ドメインに名前解決を依頼する為、社内の DNS にレコードが存在する場合、
その IP アドレスが返却され、存在しない場合はエラーになってしまう。
解決するには、適用されている DirectAccess の設定（NRPT: 名前解決ポリシーテーブル）を手動で編集する必要がある