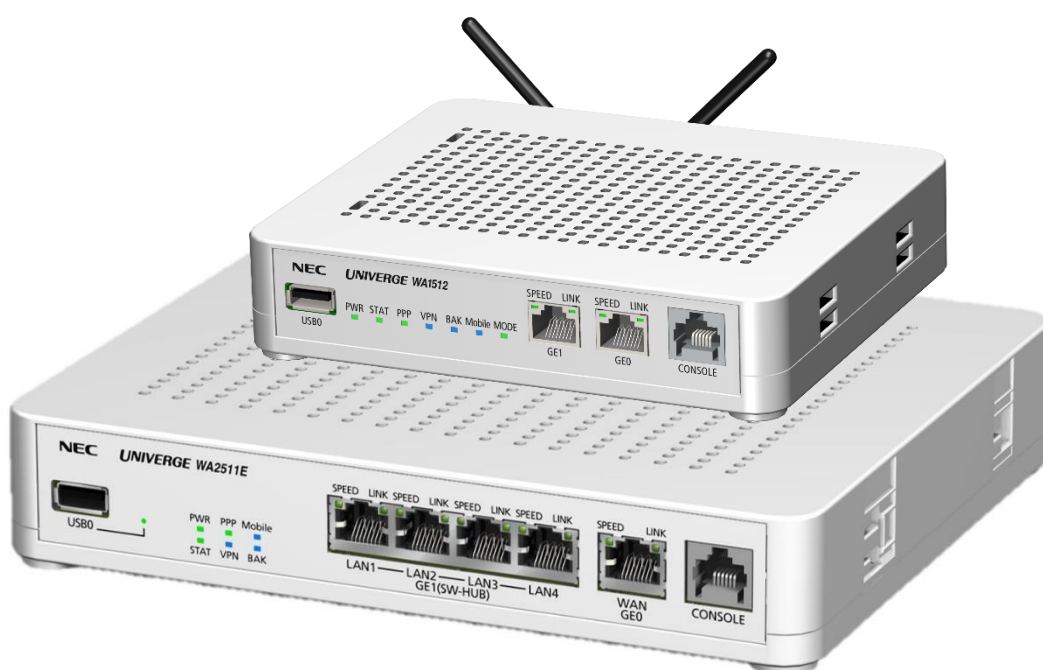




ワイヤレスアダプタ/ワイヤレス VPN ルータ **UNIVERGE WA シリーズ**



ダイナミック VPN 設定ガイド 第 8.6 版

ご注意

ご使用の前にこのマニュアルをよくお読みの上で、正しくお使いください。
お読みになったあとは、いつでもご覧になれる場所に必ず保管してください。

はじめに

このたびはワイヤレスアダプタ/ワイヤレス VPN ルータ UNIVERGE WA シリーズ（以降、WA シリーズあるいは単に WA と記載する場合があります）をお買い上げ頂きありがとうございます。

このマニュアルでは、ダイナミック VPN 機能 (Version 8.6 からサポート) を他機種 (※) 間で接続する場合や NAT/NAPT 環境で接続する場合の設定方法について説明します。

※ 本書では他機種の対向装置として NEC VPN 対応高速アクセスルータ UNIVERGE IX シリーズ（以降、IX シリーズあるいは単に IX と記載する場合があります）と Cisco 800 シリーズ ルータ を対象とします。

※ Cisco 800 シリーズ ルータ のコンフィグ設定は、Cisco 881 サービス統合型ルータ での確認結果を基に記載しております。（以降、Cisoco シリーズあるいは単に Cisco と記載する場合があります）

なお、このマニュアルでは、パソコンおよびネットワークについて基本的な操作や設定ができる方を対象に説明しています。パソコンの操作や一般的なネットワークの設定については、お使いの製品のマニュアルや市販の書籍等をご覧ください。

ご注意

- (1) 本マニュアルの内容の一部または全部を無断で転載することは禁止されています。
- (2) 本マニュアルの内容については、将来予告なしに変更することがあります。
- (3) 本マニュアルは内容について万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきのことがありましたら、ご一報くださいますようお願い致します。
- (4) 運用した結果については、(3) 項にかかわらずいかなる責任も負いかねますので、あらかじめご了承ください。

販売終了機種のご案内

UNIVERGE WA シリーズにおいて、以下の機種は販売を終了しております。

後継機種をご導入いただくよう、ご検討をお願いします。

詳細は製品ホームページをご確認ください。

・販売終了機種

WA1020 / WA2020 / WA2021 / WA100-AP /

WA1511-DL01 / WA2611-AP-DL02

・製品ホームページ

<https://jpn.nec.com/univerge/wa/index.html>

- UNIVERGE®は日本電気株式会社の登録商標です。
- NetMeister\ネットマイスターは、NEC プラットフォームズ株式会社の登録商標です。
- 本紙に掲載された社名、製品名は各社の商標または登録商標です。
- 本製品（ソフトウェア含む）は日本国内仕様であり、外国の規制等には準拠していません。
- 本製品は日本国外で使用された場合、当社は一切責任を負いかねます。また、当社は本製品に関し、海外での保守サービス及び技術サポート等を行っていません。
- 本製品の輸出（非居住者への役務提供等を含む）に際しては、外国為替及び外国貿易法等、関連する輸出管理法令等をご確認の上、必要な手続きをお取り下さい。
- 本紙に掲載された製品の色は、印刷の都合上、実際のものとは多少異なることがあります。また、改良のため予告なく形状、仕様を変更することがあります。

【 もくじ 】

はじめに.....	i
1. IX シリーズと接続する場合の設定.....	1-1
1.1. Web-GUI での設定	1-1
1.1.1. IX シリーズをセンタとする場合.....	1-1
1.1.2. WA シリーズをセンタとする場合.....	1-7
1.2. CLI コマンドでの設定	1-13
1.2.1. IX シリーズをセンタとする場合.....	1-13
1.2.2. WA シリーズをセンタとする場合.....	1-22
2. Cisco と接続する場合の設定.....	2-1
2.1. CLI コマンドでの設定	2-1
2.1.1. Cisco をセンタとする場合	2-1
2.1.2. WA シリーズをセンタとする場合.....	2-10
2.2. Web-GUI での設定(WA シリーズのみ)	2-17
2.2.1. Cisco をセンタとする場合	2-17
2.2.2. WA シリーズをセンタとする場合.....	2-19
2.3. IKEv1 を使用する場合	2-21
2.3.1. Cisco 側	2-21
2.3.2. WA シリーズ側	2-21
2.4. トンネルモードを使用する場合	2-21
2.4.1. Cisco 側	2-22
2.4.2. WA シリーズ側	2-22
3. NAT/NAPT 環境での設定.....	3-1
3.1. NAT/NAPT ルータ配下の拠点の NHRP 登録.....	3-1
3.2. NAT/NAPT ルータ配下の拠点との間のトンネル構築.....	3-2
3.2.1. デフォルト設定例.....	3-3
3.3. 1 つの NAPT ルータ配下に複数の拠点を配置した場合の動作.....	3-6

1. IX シリーズと接続する場合の設定

WA シリーズと IX シリーズをダイナミック VPN で接続する場合の、Web-GUI/CLI コマンドそれぞれの設定方法について記載します。

1.1. Web-GUI での設定

WA シリーズと IX シリーズどちらも Web-GUI で設定を行う場合の設定方法について、IX シリーズをセンタとする場合と、WA シリーズをセンタとする場合をそれぞれ記載します。

IX シリーズについては、「かんたん設定」と「詳細設定」で入力画面に差が無いため、「かんたん設定」の画面での設定について記載します。

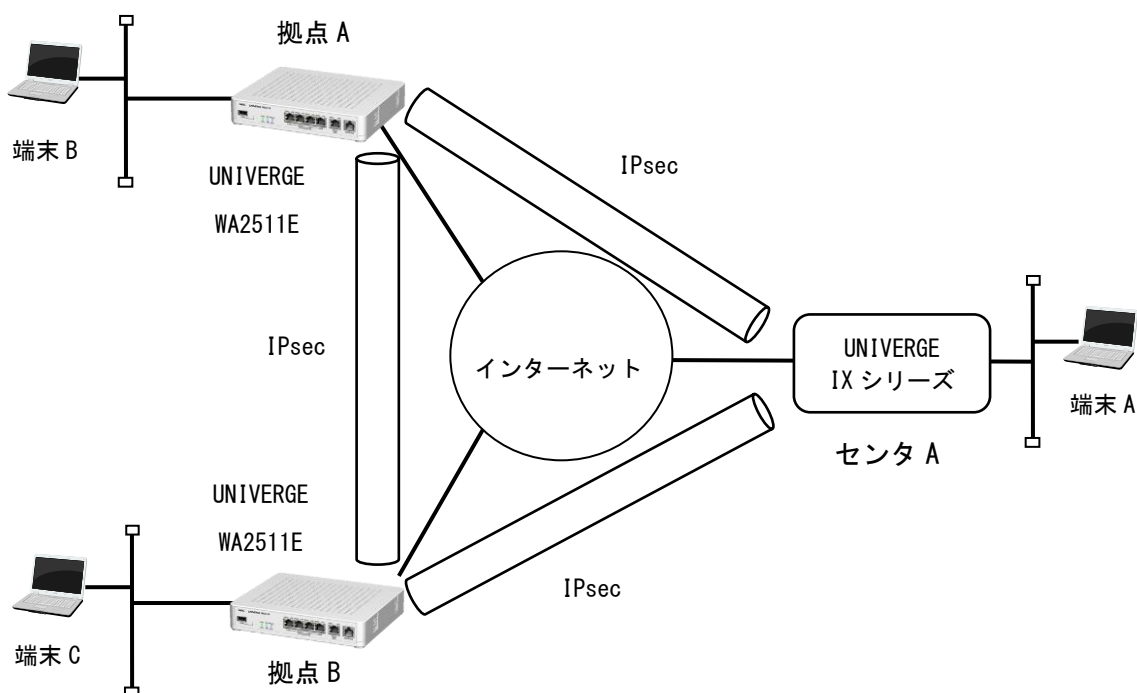
WA シリーズは「かんたん設定」と「装置設定」で入力画面の項目に差分があるため、両方の画面での設定について記載します。

1.1.1. IX シリーズをセンタとする場合

本章では IX シリーズをセンタ、WA シリーズを拠点とする場合の設定方法を記載します。

1.1.1.1. 接続構成例

IX シリーズをセンタとしたときの接続構成例です。



1.1.1.2. IX シリーズ側の設定

IX シリーズの設定画面は以下の通りです。

VPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

ダイナミックVPNの設定

2 拠点間通信でもセンタが必要です。いずれかの拠点で必ずセンタを選択してください。
タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
パスワード		すべての拠点で共通のパスワードを設定してください。 <input type="text"/> 文字列(半角英数字)を入力してください。

画面の各入力項目と、設定反映後の設定値は以下の通りです。

<入力項目説明>

項目名	説明
タイプ	拠点/センタのどちらで設定するかを選択します。 本章では IX シリーズをセンタとするため、センタを選択します。
パスワード	IKE の事前共有鍵を設定します。 WA シリーズを含む全ての拠点/センタで同じ内容とする必要があります。

<反映後の設定値> ※ダイナミック VPN に関連する箇所のみ抜粋

!
ikev2 authentication psk id ipv4 169.254.255.254 key char dmvpn-password
!
!
!
route-map web-dmvpn-map permit 10
match interface GigaEthernet2.0
!
route-map web-dmvpn-map-tunnel0.0 permit 10
set ip next-hop 169.254.255.254
!
ppp profile web-ppp-gigaethernet0.1
authentication myname test-user
authentication password test-user test-password
!
router bgp 65535
timers 5 15
address-family ipv4 unicast
redistribute connected route-map web-dmvpn-map
peer-group web-dmvpn-group-tunnel0.0 remote-as 65535
listen range 169.254.0.0/16

```

    connect-interval 10
    route-reflector-client
    address-family ipv4 route-map web-dmvpn-map-tunnel0.0 out
!
interface GigaEthernet0.1
    description WAN1
    encapsulation pppoe
    auto-connect
    ppp binding web-ppp-gigaethernet0.1
    ip address ipcp
    ip tcp adjust-mss auto
    ip napt enable
    ip napt hairpinning
    ip napt static GigaEthernet0.1 50
    ip napt static GigaEthernet0.1 udp 500
    ip napt static GigaEthernet0.1 udp 4500
    no shutdown
!
interface Tunnel0.0
    description DynamicVPN
    tunnel mode mgre ipsec-ikev2
    ip address 169.254.255.254/16
    ip tcp adjust-mss auto
    ikev2 child-pfs 2048-bit
    ikev2 child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
    ikev2 child-proposal integrity sha2-512 sha2-384 sha2-256
    ikev2 dpd interval 10
    ikev2 local-authentication psk id ipv4 169.254.255.254
    ikev2 nat-traversal keepalive 20
    ikev2 outgoing-interface GigaEthernet0.1 auto
    ikev2 sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
    ikev2 sa-proposal integrity sha2-512 sha2-384 sha2-256
    ikev2 sa-proposal dh 2048-bit
    ikev2 sa-proposal prf sha2-512 sha2-384 sha2-256
    ikev2 ipsec-mode transport
    ikev2 peer any authentication psk
    no shutdown
!
web-console system information
    o wizard easy-inet-vpn-pppoe
    o wan1 GigaEthernet0.1
    o lan1 GigaEthernet2.0

```

※ IX シリーズの Web-GUI では、センタのプロトコルアドレス (Tunnel インタフェースの IP アドレス) を設定する項目は無く、169.254.255.254/16 が設定されます。

1.1.1.3. WA シリーズ側の設定(かんたん設定)

WA シリーズのかんたん設定の設定画面は以下の通りです。

かんたん設定:VPNの設定

	現在の設定	設定の変更
接続形態		<input type="radio"/> サイト間VPN <input checked="" type="radio"/> ダイナミックVPN <input type="radio"/> L2TPv2/IPsec

ダイナミックVPNの設定

※拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ <small>※この拠点やセンタと常にIPアドレスは設定しないで行ってください。</small> <input type="button" value="IPアドレスを入力してください"/>
mGREのIPアドレス		<input checked="" type="radio"/> IKEv2 <input type="radio"/> IKEv1(メイン) <input type="radio"/> IKEv1(アグレッシブ)
IKEバージョン		<input checked="" type="radio"/> mGREのIPアドレス(プロトコルアドレス) <input type="radio"/> WAN側のIPアドレス(NBMAアドレス) <small>※すべての拠点で共通の事前共有鍵を設定してください。</small> <input type="button" value="事前共有鍵を入力してください"/>
IKEのIDに使用するアドレス		
事前共有鍵		
IKE SA 暗号化アルゴリズム		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> DES-CBC
IKE SA 認証アルゴリズム		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
IKE SA 暗号化アルゴリズム		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
IKE SA 認証アルゴリズム		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> DES-CBC
OnSite SA 暗号化アルゴリズム		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
OnSite SA 認証アルゴリズム		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> DES-CBC
NAT/NAPT設定下の拠点との間のVPN接続条件		<small>※本機がNAT/NAPTデバイス設定下の拠点の場合のみ有効な設定です。</small> <small>※この拠点とNAT/NAPT設定下の拠点との間のVPN接続が可能です。通信できません。</small> <input type="radio"/> 両側の拠点がNAT/NAPT設定下の場合のみ許可 <input type="radio"/> センタ側のWANに設定されているIPアドレスまたはドメイン名を入力してください。 <input type="button" value="IPアドレスまたはIPアドレスを入力してください"/>
センタ側のWAN側のIPアドレス		<input type="button" value="IPアドレスを入力してください"/>
センタ側のmGREのIPアドレス		<input type="button" value="IPアドレスを入力してください"/>

上記の画面の各入力項目と、Web-GUI でセンタとして設定を行った IX シリーズと接続するための設定値は以下の通りです。

<入力項目説明>

項目名	説明	IX シリーズと接続するための設定値
タイプ	拠点/センタのどちらで設定するかを選択します。	本章では IX シリーズをセンタとするため、WA シリーズでは拠点を選択します。
mGRE の IP アドレス	WA シリーズのプロトコルアドレス (mGRE0.0 インタフェースの IP アドレス) を設定します。	IX シリーズのプロトコルアドレス (169.254.255.254/16) と同じネットワークかつ、重複しない IP アドレス (169.254.0.1/16 など) を設定します。
IKE バージョン	ダイナミック VPN で使用する IKE のバージョンを選択します。	IX シリーズのダイナミック VPN 機能は IKEv2 のみサポートしているため、WA シリーズ側も IKEv2 を選択します。
IKE の ID に使用するアドレス	IKE の ID にプロトコルアドレス (mGRE インタフェースの IP アドレス) と、NBMA アドレス (WAN 側インタフェースのアドレス) のどちらを使用するか選択します。	IX シリーズは IKE の ID にプロトコルアドレスを使用するため、mGRE の IP アドレス (プロトコルアドレス) を選択します。
事前共有鍵	IKE の事前共有鍵を設定します。	IX シリーズ側に設定した事前共有鍵と同じ設定値とする必要があるため、IX シリーズの Web-GUI の「パスワード」と同じ内容を設定します。

IKE SA 暗号化 アルゴリズム	IKE SA 暗号化アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」を使用する設定が行われます。WA シリーズ側は、「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」のいずれかを選択することで、IX シリーズと接続可能となります。
IKE SA 認証アルゴリズム	IKE SA 認証アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「SHA2(512bits)」、「SHA2(384bits)」、「SHA2(256bits)」を使用する設定が行われます。WA シリーズ側は、「SHA2(256bits)」を選択することで、IX シリーズと接続可能となります。
IKE SA PRF アルゴリズム	IKE SA PRF アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「SHA2(512bits)」、「SHA2(384bits)」、「SHA2(256bits)」を使用する設定が行われます。WA シリーズ側は、「SHA2(256bits)」を選択することで、IX シリーズと接続可能となります。
Child SA 暗号化アルゴリズム	Child SA 暗号化アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」を使用する設定が行われます。WA シリーズ側は、「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」のいずれかを選択することで、IX シリーズと接続可能となります。
Child SA 認証アルゴリズム	Child SA 認証アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「SHA2(512bits)」、「SHA2(384bits)」、「SHA2(256bits)」を使用する設定が行われます。WA シリーズ側は、「SHA2(256bits)」を選択することで、IX シリーズと接続可能となります。
NAT/NAPT 配下の拠点との間の VPN 接続条件	NAT/NAPT 配下の拠点がとの VPN 接続について、片側が NAT/NAPT の場合のみ接続可能とするか、両側が NAT の場合も接続可能とするかを選択します。	IX シリーズの動作は、WA シリーズで「片側の拠点が NAT/NAPT の場合のみ許容」を選択した場合と同様です。WA シリーズ側も IX と同様の動作とするために片側の拠点が NAT/NAPT の場合のみ許容」を選択します。
センタ装置の WAN 側の IP アドレス	センタ装置の NBMA アドレスを設定します。	センタとして使用する IX シリーズの WAN 側インタフェース(web-console system information の wan1 のインタフェース)の IP アドレス、または FQDN を設定します。
センタ装置の mGRE の IP アドレス	センタ装置のプロトコルアドレスを設定します。	センタとして使用する IX シリーズのプロトコルアドレスである 169.254.255.254/16 を設定します。

1.1.1.4. WA シリーズ側の設定(装置設定)

WA シリーズの装置設定の設定画面は以下の通りです。

	現在の設定	設定の変更
タイプ ?		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
WAN側インタフェース ?		<input checked="" type="radio"/> GigaEthernet0/0 <input type="radio"/> PPPoE0 <input type="radio"/> PPPoE1 <input type="radio"/> MobileEthernet0/0 <input type="radio"/> Serial0
LAN側インタフェース ?		<input checked="" type="checkbox"/> GigaEthernet1/0 <input type="checkbox"/> WirelessEthernet0/0 <input type="checkbox"/> WirelessEthernet0/1 <input type="checkbox"/> WirelessEthernet0/2 <input type="checkbox"/> WirelessEthernet0/3
mGREのIPアドレス ?		<input type="text" value="192.168.1.1"/> <input type="button" value="IPアドレスを入力してください。"/>
IPv6バージョン ?		<input checked="" type="radio"/> IPv6 <input type="radio"/> IPv6(メイン) <input type="radio"/> IPv6(アプレッシュ)
IPv6のIPに使用するアドレス ?		<input checked="" type="radio"/> mGREのIPアドレス(プロトコルアドレス) <input type="radio"/> WAN側のIPアドレス(NBMAアドレス)
事前共有鍵 ?		<input type="text" value="1234567890123456789012345678901234"/> <input type="button" value="文字列(半角)を入力してください。"/>
IKE SA 暗号化アルゴリズム ?		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> 3DES-CBC
IKE SA 認証アルゴリズム ?		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
IKE SA PRFアルゴリズム ?		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
Onike SA 暗号化アルゴリズム ?		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> 3DES-CBC
Onike SA 認証アルゴリズム ?		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
NAT/NAPT配下の 拠点との間の VPN接続条件 ?		<input checked="" type="radio"/> 片側の拠点がNAT/NAPT配下の場合のみ許容 <input type="radio"/> 両側の拠点がNAT配下の場合も許容
センタ側 のIPアドレス ?		<input type="text" value="192.168.1.1"/> <input type="button" value="IPアドレスまたはIP/GDMを入力してください。"/>
センタ側 のmGREの IPアドレス ?		<input type="text" value="192.168.1.1"/> <input type="button" value="IPアドレスを入力してください。"/>

上記の画面の各入力項目の内、装置設定固有の項目について、Web-GUI でセンタとして設定を行った IX シリーズと接続するための設定値を以下に記載します。(かんたん設定と共通の項目については、1.1.1.3 章をご参照ください。)

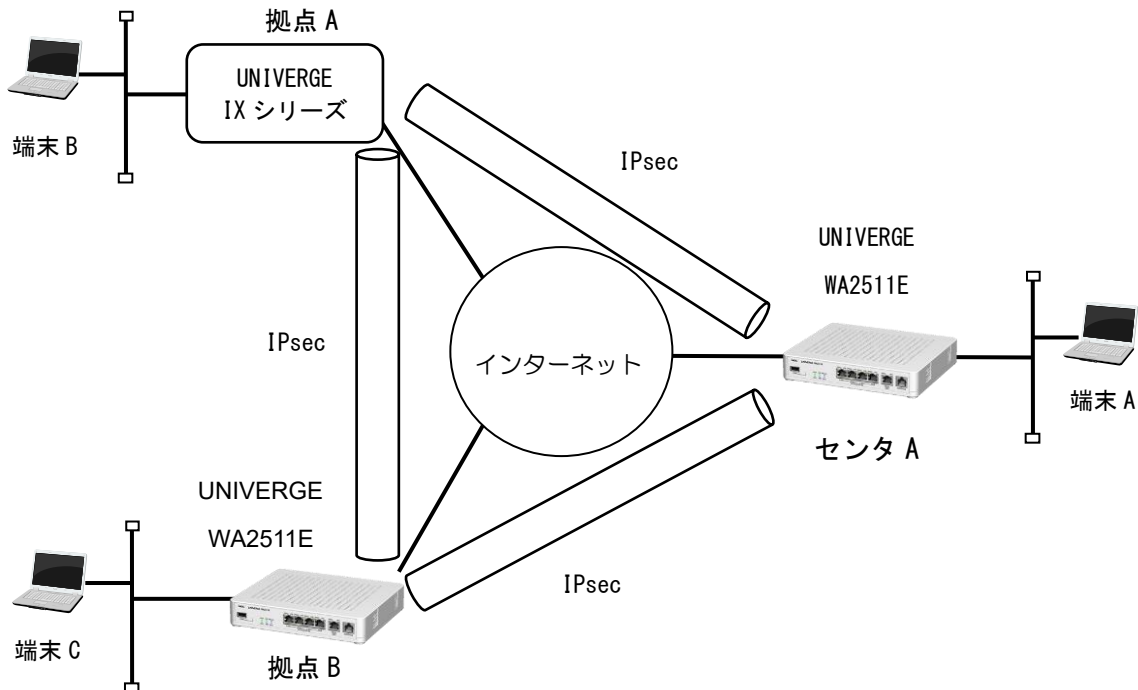
項目名	説明	IX シリーズと接続するための設定値
WAN 側インタフェース	ダイナミック VPN で使用する WAN 側のインタフェースを選択します。	IX シリーズの WAN 側インタフェースと接続可能なインタフェースを選択してください。 選択したインタフェースの詳細は「有線回線」や「モバイル回線」の設定画面で設定を行ってください。
LAN 側インタフェース	ダイナミック VPN で使用する LAN 側のインタフェースを選択します。	どのインタフェースを選択しても IX シリーズとの接続に影響はありません。

1.1.2. WA シリーズをセンタとする場合

本章では WA シリーズをセンタ、IX シリーズを拠点とする場合の設定方法を記載します。

1.1.2.1. 接続構成例

WA シリーズをセンタとしたときの接続構成例です。



1.1.2.2. IX シリーズ側の設定

IX シリーズ側の設定画面は以下の通りです。

VPNを設定します。

	現在の設定	設定の変更
接続種別		<input checked="" type="radio"/> ダイナミックVPN

ダイナミックVPNの設定

2 拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。

タイプや拠点番号を変更すると、LAN側IPアドレスが変更されます。

	現在の設定	設定の変更
タイプ		<input checked="" type="radio"/> 拠点 <input type="radio"/> センタ
拠点番号		他の拠点と同じ番号は設定しないでください。 1
パスワード		すべての拠点で共通のパスワードを設定してください。 文字列(半角英数字)を入力してください。
センタWAN側IPアドレス		センタ装置のWANに設定されているIPアドレスまたはドメイン名を入力してください。 入力形式が不正です。

画面の各入力項目と、設定反映後の設定値は以下の通りです。

<入力項目説明>

項目名	説明
タイプ	拠点/センタのどちらで設定するかを選択します。 本章では WA シリーズをセンタとするため、IX シリーズでは拠点を選択します。
拠点番号	プロトコルアドレス (Tunnel インタフェースの IP アドレス) の下位 8bit を設定する項目で、本項目で選択した値が 169.254.0.X/16 の X の部分に適用されます。 例として 1 選択した場合は、プロトコルアドレスには 169.254.0.1/16 が設定されます。
パスワード	IKE の事前共有鍵を設定します。 WA シリーズを含む全ての拠点/センタで同じ内容とする必要があります。
センタ WAN 側 IP アドレス	WA シリーズ側の DMVPN で使用する WAN 側インタフェースの IP アドレス、または FQDN を設定します。

<反映後の設定値> ※ダイナミック VPN に関連する箇所のみ抜粋

```

!
nhrp local GigaEthernet2.0
!
ikev2 authentication psk id ipv4 169.254.0.1 key char dmvpn-password
!
!
!
route-map web-dmvpn-map permit 10
  match interface GigaEthernet2.0
!
ppp profile web-ppp-gigaethernet0.1
  authentication myname test-user
  authentication password test-user test-password
!
router bgp 65535
  timers 5 15
  neighbor 169.254.255.254 remote-as 65535
  neighbor 169.254.255.254 connect-interval 10
  address-family ipv4 unicast
    redistribute connected route-map web-dmvpn-map
!
interface GigaEthernet2.0
  description LAN1
  ip address 192.168.1.254/24
  http-server ip enable
  no shutdown
!
interface GigaEthernet0.1
  description WAN1
  encapsulation pppoe
  auto-connect
  ppp binding web-ppp-gigaethernet0.1
  ip address ipcp
  ip tcp adjust-mss auto
  ip napt enable

```

```

ip napt hairpinning
ip napt static GigaEthernet0.1 50
ip napt static GigaEthernet0.1 udp 500
ip napt static GigaEthernet0.1 udp 4500
no shutdown
!
interface Tunnel0.0
description DynamicVPN_#1
tunnel mode mgre ipsec-ikev2
ip address 169.254.0.1/16
ip tcp adjust-mss auto
nhrp nhs 169.254.255.254/16 nbma 203.113.0.100
ikev2 child-pfs 2048-bit
ikev2 child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
ikev2 child-proposal integrity sha2-512 sha2-384 sha2-256
ikev2 dpd interval 10
ikev2 local-authentication psk id ipv4 169.254.0.1
ikev2 nat-traversal keepalive 20
ikev2 outgoing-interface GigaEthernet0.1 auto
ikev2 sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
ikev2 sa-proposal integrity sha2-512 sha2-384 sha2-256
ikev2 sa-proposal dh 2048-bit
ikev2 sa-proposal prf sha2-512 sha2-384 sha2-256
ikev2 ipsec-mode transport
ikev2 peer any authentication psk
no shutdown
!
web-console system information
o wizard easy-inet-vpn-pppoe
o wan1 GigaEthernet0.1
o lan1 GigaEthernet2.0

```

1.1.2.3. WA シリーズ側の設定(かんたん設定)

WA シリーズのかんたん設定の設定画面は以下の通りです。

かんたん設定:VPNの設定

	現在の設定	設定の変更
接続形態		<input type="radio"/> サイト間VPN <input checked="" type="radio"/> ダイナミックVPN <input type="radio"/> L2TPv2/IPsec

ダイナミックVPNの設定

2拠点間通信でもセンタは必要です。いずれかの拠点で必ずセンタを選択してください。

	現在の設定	設定の変更
タイプ		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ 他の拠点やセンタと同じIPアドレスは設定しないでください。 IPアドレスを入力してください。 [設定]
mGREのIPアドレス		
IKEバージョン		<input checked="" type="radio"/> IKEv2 <input type="radio"/> IKEv1(メイン) <input type="radio"/> IKEv1(アプレッシュ)
IKEのIDに使用するアドレス		<input checked="" type="radio"/> mGREのIPアドレス(プロトコルアドレス) <input type="radio"/> WAN側のIPアドレス(NBMAアドレス) すべての拠点で共通の事前共有鍵を設定してください。
事前共有鍵		文字列(半角)を入力してください。
IKE SA 暗号化アルゴリズム		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(192bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> 3DES-CBC
IKE SA 認証アルゴリズム		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
IKE SA PDPアルゴリズム		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
Child SA 暗号化アルゴリズム		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(192bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> 3DES-CBC
Child SA 認証アルゴリズム		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5

[戻る] [次へ]

上記の画面の各入力項目と、Web-GUI で拠点として設定を行った IX シリーズと接続するための設定値は以下の通りです。

項目名	説明	IX シリーズと接続するための設定値
タイプ	拠点/センタのどちらで設定するかを選択します。	本章では WA シリーズをセンタとするため、センタを選択します。
mGRE の IP アドレス	WA シリーズのプロトコルアドレス(mGRE 0.0 インタフェースの IP アドレス)を設定します。	IX シリーズのプロトコルアドレス(169.254.0.X/16)と同じネットワークかつ、重複しない IP アドレス(169.254.255.254/16 など)を設定します。
IKE バージョン	ダイナミック VPN で使用する IKE のバージョンを選択します。	IX シリーズのダイナミック VPN 機能は IKEv2 のみサポートしているため、WA シリーズ側も IKEv2 を選択します。
IKE の ID に使用するアドレス	IKE の ID にプロトコルアドレス(mGRE インタフェースの IP アドレス)と、NBMA アドレス(WAN 側インタフェースのアドレス)のどちらを使用するか選択します。	IX シリーズは IKE の ID にプロトコルアドレスを使用するため、mGRE の IP アドレス(プロトコルアドレス)を選択します。
事前共有鍵	IKE の事前共有鍵を設定します。	IX シリーズ側に設定した事前共有鍵と同じ設定値とする必要があるため、IX シリーズの Web-GUI の「パスワード」と同じ内容を設定します。
IKE SA 暗号化アルゴリズム	IKE SA 暗号化アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」を使用する設定が行われます。WA シリーズ側は、「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」のいずれかを選択することで、IX シリーズと接続可能となります。

IKE SA 認証アルゴリズム	IKE SA 認証アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「SHA2(512bits)」、「SHA2(384bits)」、「SHA2(256bits)」を使用する設定が行われます。 WA シリーズ側は、「SHA2(256bits)」を選択することで、IX シリーズと接続可能となります。
IKE SA PRF アルゴリズム	IKE SA PRF アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「SHA2(512bits)」、「SHA2(384bits)」、「SHA2(256bits)」を使用する設定が行われます。 WA シリーズ側は、「SHA2(256bits)」を選択することで、IX シリーズと接続可能となります。
Child SA 暗号化アルゴリズム	Child SA 暗号化アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」を使用する設定が行われます。 WA シリーズ側は、「AES-CBC(256bits)」、「AES-CBC(192bits)」、「AES-CBC(128bits)」のいずれかを選択することで、IX シリーズと接続可能となります。
Child SA 認証アルゴリズム	Child SA 認証アルゴリズムを選択します。	IX シリーズのダイナミック VPN の Web-GUI では「SHA2(512bits)」、「SHA2(384bits)」、「SHA2(256bits)」を使用する設定が行われます。 WA シリーズ側は、「SHA2(256bits)」を選択することで、IX シリーズと接続可能となります。

1.1.2.4. WA シリーズ側の設定(装置設定)

WA シリーズの装置設定の設定画面は以下の通りです。

	現在の設定	設定の変更
タイプ 2		<input type="radio"/> 拠点 <input checked="" type="radio"/> センタ
WAN側インタフェース 2		<input checked="" type="radio"/> GigaEthernet0/0 <input type="radio"/> PPPE0/0 <input type="radio"/> PPPE1 <input type="radio"/> MobileEthernet0/0 <input type="radio"/> Serial0
LAN側インタフェース 2		<input checked="" type="checkbox"/> GigaEthernet1/0 <input type="checkbox"/> WirelessEthernet0/0 <input type="checkbox"/> WirelessEthernet0/1 <input type="checkbox"/> WirelessEthernet0/2 <input type="checkbox"/> WirelessEthernet0/3
uGREのIPアドレス 2		<input type="text"/> IPアドレスを入力してください。
GREバージョン 2		<input checked="" type="radio"/> GREv2 <input type="radio"/> GREv1(メイン) <input type="radio"/> GREv1(アラレッシュ)
GREのIDに使用するアドレス 2		<input checked="" type="radio"/> uGREのアドレス(プロトコルアドレス) <input type="radio"/> WAN側のIPアドレス(NBMAアドレス)
事前共有鍵 2		<input type="text"/> 文字列(半角)を入力してください。
IKE SA 暗号化アルゴリズム 2		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(192bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> 3DES-CBC
IKE SA 認証アルゴリズム 2		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
IKE SA PDPアルゴリズム 2		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5
Child SA 暗号化アルゴリズム 2		<input checked="" type="radio"/> AES-CBC(256bits) <input type="radio"/> AES-CBC(192bits) <input type="radio"/> AES-CBC(128bits) <input type="radio"/> 3DES-CBC
Child SA 認証アルゴリズム 2		<input checked="" type="radio"/> SHA2(256bits) <input type="radio"/> SHA1 <input type="radio"/> MD5

[戻る](#) [設定・保存](#) [削除](#)

上記の画面の各入力項目の内、装置設定固有の項目について、Web-GUI で拠点として設定を行った IX シリーズと接続するための設定値を以下に記載します。(かんたん設定と共通の項目については、1.1.2.3 章をご参照ください。)

項目名	説明	IX シリーズと接続するための設定値
WAN 側インタフェース	ダイナミック VPN で使用する WAN 側のインタフェースを選択します。	IX シリーズの WAN 側インタフェースと接続可能なインタフェースを選択してください。 選択したインタフェースの詳細は「有線回線」や「モバイル回線」の設定画面で設定を行ってください。
LAN 側インタフェース	ダイナミック VPN で使用する LAN 側のインタフェースを選択します。	どのインタフェースを選択しても IX シリーズとの接続に影響はありません。

1.2. CLI コマンドでの設定

1.2.1. IX シリーズをセンタとする場合

本章では IX シリーズと接続するために WA シリーズに必要な CLI コマンドの設定例を記載いたします。

1.2.1.1. IX シリーズ側の設定例

```
!  
ikev2 authentication psk id ipv4 169.254.0.100 key char dmvpn-password  
!  
!  
!  
route-map dmvpn-map permit 10  
  match interface GigaEthernet2.0  
!  
route-map dmvpn-map-tunnel0.0 permit 10  
  set ip next-hop 169.254.0.100  
!  
router bgp 65535  
  timers 5 15  
  address-family ipv4 unicast  
    redistribute connected route-map dmvpn-map  
  peer-group web-dmvpn-group-tunnel0.0 remote-as 65535  
    listen range 169.254.0.0/24  
    connect-interval 10  
    route-reflector-client  
    address-family ipv4 route-map dmvpn-map-tunnel0.0 out  
!  
interface GigaEthernet0.0  
  ip address 203.113.0.100/24  
  no shutdown  
!  
interface GigaEthernet2.0  
  ip address 192.168.0.254/24  
  no shutdown  
!  
interface Tunnel0.0  
  tunnel mode mgre ipsec-ikev2  
  ip address 169.254.0.100/24  
  ikev2 child-pfs 2048-bit  
  ikev2 child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128  
  ikev2 child-proposal integrity sha2-512 sha2-384 sha2-256  
  ikev2 dpd interval 10  
  ikev2 local-authentication psk id ipv4 169.254.255.254  
  ikev2 nat-traversal keepalive 20  
  ikev2 outgoing-interface GigaEthernet0.0 auto  
  ikev2 sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128  
  ikev2 sa-proposal integrity sha2-512 sha2-384 sha2-256  
  ikev2 sa-proposal dh 2048-bit
```

```
ikev2 sa-proposal prf sha2-512 sha2-384 sha2-256
ikev2 ipsec-mode transport
ikev2 peer any authentication psk
no shutdown
!
```

1.2.1.2. WA シリーズ側の設定例

```
!
route-map dmvpn-map permit 10
  match interface GigaEthernet1.0
!
interface GigaEthernet0.0
  ip address 203.113.0.1/24
  ikev2 binding ikev2-prof1
  :
  ikev2 binding ikev2-prof16
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.1.254/24
  no shutdown
!
interface mGRE0.0
  gre source GigaEthernet0.0
  nhrp nhs 169.254.0.100/24 nbma 203.113.0.100
  ip address 169.254.0.1/24
  no shutdown
!
!
ip route 169.254.0.0/24 mGRE0.0
!
router bgp 65535
  timers 5 15
  neighbor 169.254.0.100 remote-as 65535
  neighbor 169.254.0.100 connect-interval 10
  address-family ipv4 unicast
    redistribute connected route-map dmvpn-map
!
ikev2 profile ikev2-prof1
  peer any
!
:
!
ikev2 profile ikev2-prof16
  peer any
!
ikev2 default-profile
  ipsec-mode transport
  source-address GigaEthernet0.0
  local-authentication psk plain dmvpn-password
```

```
local-id address 169.254.0.1
dpd interval 10
nat-traversal enable keepalive 20
sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
sa-proposal integrity sha2-256
sa-proposal prf sha2-256
sa-proposal dh 2048-bit
ignore tsi-payload
child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
child-proposal integrity sha2-256
child-pfs 2048-bit
!
nhrp local GigaEthernet1.0
!
```

1.2.1.3. WA シリーズの設定の説明

1.2.1.3.1. WAN 側インタフェースの設定

ダイナミック VPN の WAN 側のインタフェースは、IKEv2 プロファイルの設定が可能なインタフェースであれば、どのインタフェースでの使用可能です。

1. 2. 1. 2 章の設定例では、IX シリーズの GigaEthernet0.0(※)と同じネットワークアドレスを設定した GigaEthernet0.0 を、ダイナミック VPN の WAN 側インタフェースとして使用する設定を記載しています。

※ 上記は IX シリーズ側に 1. 2. 1. 1 章の設定を行った場合で記載しています。IX シリーズ側の設定を Web-GUI で行った場合は、web-console system information の wan1 のインタフェースと通信可能なインタフェースを、WA シリーズの WAN 側インタフェースとして設定してください。

1.2.1.3.2. LAN 側インタフェースの設定

ダイナミック VPN の LAN 側として使用するインタフェースは、nhrip local コマンドで設定することができます。

1. 2. 1. 2 章の設定例では、GigaEthernet1.0 を LAN 側インタフェースとして使用する設定を記載しています。

LAN 側インタフェースの設定は拠点間トンネルの生成に必要な設定です。nhrip local コマンドで設定したインタフェースのネットワークを宛先とするパケットをトリガとして、拠点間トンネルを生成することができますようになります。

1.2.1.3.3. mGRE インタフェースの設定

ダイナミック VPN 機能では、mGRE インタフェースを使用することで GRE over IPsec の複数対地接続を行います。

1. 2. 2. 1 章の設定例で mGRE0.0 インタフェースに対して行っている各設定の詳細を以下に記載します。

設定コマンド	説明
gre source GigaEthernet0.0	GRE カプセル化後の Outer IP ヘッダの送信元 IP アドレスを設定するコマンドです。設定例では、WAN 側インタフェースとして使用する GigaEthernet0.0 の IP アドレスを設定しています。 ※ 設定を省略した場合、mGRE トンネルの宛先へのルーティングから最適なインタフェースを選択し、そのインタフェースの IP アドレスを使用しますが、設定例は GigaEthernet0.0 のみ使用する想定の設定のため、明示的に GigaEthernet0.0 を設定しています。

nhp nhs 169.254.0.100/24 nbma 203.113.0.100	<p>センタ装置である IX シリーズのプロトコルアドレス (Tunnel インタフェースの IP アドレス) と、NBMA アドレス (WAN 側インタフェースの IP アドレス) を設定します。</p> <p>※ NBMA アドレスは IP アドレスの他、FQDN を設定することも可能です。</p> <p>※ IX シリーズの設定を Web-GUI で行った場合、左記の「169.254.0.100/24」の箇所は「169.254.255.254/16」を設定してください。また、「203.113.0.100」の箇所は web-console system information の wan1 のインタフェースの IP アドレス、または FQDN を設定してください。</p>
ip address 169.254.0.1/24	<p>センタ装置である IX シリーズのプロトコルアドレス (Tunnel インタフェースの IP アドレス) と同じネットワーク、かつ重複しない IP アドレスを設定します。</p> <p>1.2.1.1 章の IX シリーズの設定例では、プロトコルアドレスに 169.254.0.100/24 を設定しているため、WA シリーズ側は 169.254.0.0/24 のネットワークで、169.254.0.100 と重複しない 169.254.0.1/24 を設定しています。</p> <p>※ IX シリーズ側の設定を Web-GUI で行った場合、IX シリーズのプロトコルアドレスは 169.254.255.254/16 となりますので、169.254.255.254/16 と同じネットワークかつ、重複しない IP アドレス (169.254.0.1/16 など) を設定してください。</p>
no dmvpn ike-id (デフォルト設定値)	<p>IX シリーズのダイナミック VPN では IKE の ID にプロトコルアドレス (Tunnel インタフェースの IP アドレス) を使用します。</p> <p>このため、WA シリーズ側も同様に、IKE の ID にプロトコルアドレスを使用する設定とする必要があります。WA シリーズのコンフィグでは、デフォルトで ID にプロトコルアドレスを使用する設定となっておりますので、dmvpn ike-id コマンドの設定値はデフォルト設定値のままとする必要があります。</p>
no nhp enable-ack-with-nat (デフォルト設定値)	<p>WA シリーズに nhp enable-ack-with-nat コマンドを設定しない場合の NAT/NAPT 配下の拠点装置の動作は、IX シリーズと同様となります。このため、IX シリーズと接続する場合は、nhp enable-ack-with-nat コマンドを設定せず、デフォルト設定値のままとします。</p>

1.2.1.3.4. IKEv2 の設定

IX シリーズとのダイナミック VPN 接続は、IKEv2 のトランスポートモードを使用する必要があります。

1.2.1.2 章の設定例の内、IKEv2 に関連する各設定の詳細を以下に記載します。

設定コマンド	説明
interface GigaEthernet0.0 ikev2 binding ikev2-prof1 : ikev2 binding ikev2-prof16	<p>WAN 側インタフェースにダイナミック VPN で使用する IKEv2 プロファイルを必要数分設定します。</p> <p>設定例では、1 つの mGRE インタフェースでの最大接続数 (16) 分の IKEv2 プロファイルを設定しています。</p> <p>IX シリーズのダイナミック VPN 機能は IKEv2 のみサポートしているため、IKEv1 の IPsec プロファイルを使用して IX シリーズと接続することはできません。</p>

ikev2 profile ikev2-profX peer any	ダイナミック VPN 機能では peer の設定を any または any ipv6 とする必要があります。 設定例では WAN 側インタフェースは IPv4 のため、peer any を設定しています。
ikev2 default-profile	WAN 側インタフェースに設定する全ての IKEv2 プロファイルで共通する設定 (peer 以外) は IKEv2 デフォルトプロファイルで設定することが可能です。 (IKEv2 デフォルトプロファイルを使用することで、CLI コマンドの設定数を少なくすることができます。) なお、IKEv2 デフォルトプロファイルを使用せず、各 IKEv2 プロファイルにそれぞれ同じ設定を行う方法でも、設定例と同様の設定が可能です。
ipsec-mode transport	IX シリーズのダイナミック VPN 機能はトランスポートモードのみサポートしているため、WA シリーズ側もトランスポートモードを設定します。
source-address GigaEthernet0.0	Child-SA を確立するソースインタフェースを設定します。 Child-SA は WAN 側インタフェース間で生成するため、WAN 側インタフェースの IP アドレスを設定します。
local-authentication psk plain dmvpn-password	ダイナミック VPN 機能では、全センタ/装置で同じ事前共有鍵を使用する必要があります。 このため、local-authentication コマンドでは IX シリーズ側と同じ事前共有鍵を設定してください。 IX シリーズ側の対象の設定は、1.2.1.1 章の設定例の場合は、以下が該当します。 ikev2 authentication psk id ipv4 169.254.0.100 key char dmvpn-password Ver. 8.6 以降の WA シリーズでは、remote-authentication コマンドの設定を省略することで、local-authentication コマンドと同じ設定値を remote-authentication でも使用することが可能です。
local-id address 169.254.0.1	IX シリーズと接続する場合、local-id には自装置のプロトコルアドレス (mGRE インタフェースの IP アドレス) を設定する必要があります。 local-id の設定を省略した場合でも、IKE ネゴシエーションのイニシエータとなる場合は、自動で自装置のプロトコルアドレスを使用しますが、ダイナミック VPN の拠点装置はレスポндаにもなり得るため、local-id を明示的に設定することが推奨されます。
nat-traversal enable keepalive 20	他のセンタ/拠点との間に NAT/NAPT デバイスを配置する場合、nat-traversal enable コマンドの設定が必要となります。NAT/NAPT デバイスを配置しない構成で、nat-traversal enable コマンドを設定しても、接続性に影響は有りません。

sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128	IX シリーズの Tunnel インタフェースの ikev2 sa-proposal enc コマンドと一致する暗号化アルゴリズムを設定してください。 1. 2. 1. 1 章の設定例の場合、IX シリーズ側は aes-cbc-256、aes-cbc-192、aes-cbc-128 の 3 種を設定しておりますので、WA シリーズ側は aes-cbc-256、aes-cbc-192、aes-cbc-128 のいずれかを必ず設定する必要があります。 設定例のように全て設定し、3 種から自動で暗号化アルゴリズムを選択する設定とすることも可能です。 ※ IX シリーズ側の設定を Web-GUI で行った場合、 「aes-cbc-256 aes-cbc-192 aes-cbc-128」が設定されますので、WA シリーズ側は「aes-cbc-256」、 「aes-cbc-192」、「aes-cbc-128」のいずれかを含む設定を行ってください。
sa-proposal integrity sha2-256	IX シリーズの Tunnel インタフェースの ikev2 sa-proposal integrity コマンドと一致する認証アルゴリズムを設定してください。 1. 2. 1. 1 章の設定例の場合、IX シリーズ側は sha2-512 sha2-384 sha2-256 の 3 種を設定しておりますが、WA シリーズではこれら 3 種の内、sha2-256 のみ設定可能ですので、1. 2. 1. 1 章の設定の IX シリーズと接続する場合は、sha2-256 を設定してください。 ※ IX シリーズ側の設定を Web-GUI で行った場合、 「sha2-512 sha2-384 sha2-256」が設定されますので、WA シリーズ側は「sha2-256」含む設定を行ってください。
sa-proposal prf sha2-256	IX シリーズの Tunnel インタフェースの ikev2 sa-proposal prf コマンドと一致する PRF アルゴリズムを設定してください。 1. 2. 1. 1 章の設定例の場合、IX シリーズ側は sha2-512 sha2-384 sha2-256 の 3 種を設定しておりますが、WA シリーズではこれら 3 種の内、sha2-256 のみ設定可能ですので、1. 2. 1. 1 章の設定の IX シリーズと接続する場合は、sha2-256 を設定してください。 ※ IX シリーズ側の設定を Web-GUI で行った場合、 「sha2-512 sha2-384 sha2-256」が設定されますので、WA シリーズ側は「sha2-256」含む設定を行ってください。
sa-proposal dh 2048-bit	IX シリーズの Tunnel インタフェースの ikev2 sa-proposal dh と同じ DH グループを設定してください。 ※ IX シリーズ側の設定を Web-GUI で行った場合、 「2048-bit」が設定されますので、WA シリーズ側も「2048-bit」を設定してください。
ignore tsi-payload	IX シリーズとの間に NAT/NAPT デバイスを配置する場合、WA シリーズ側に ignore tsi-payload コマンドの設定が必要となります。 本コマンドは NAT-T の場合のみ適用される設定のため、NAT/NAPT デバイスを配置しない構成で設定しても、接続性に影響は有りません。

child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128	<p>IX シリーズの Tunnel インタフェースの ikev2 child-proposal enc コマンドと一致する暗号化アルゴリズムを設定してください。</p> <p>1. 2. 1. 1 章の設定例の場合、IX シリーズ側は aes-cbc-256、aes-cbc-192、aes-cbc-128 の 3 種を設定しておりますので、WA シリーズ側は aes-cbc-256、aes-cbc-192、aes-cbc-128 のいずれかを必ず設定する必要があります。</p> <p>設定例のように全て設定し、3 種から自動で暗号化アルゴリズムを選択する設定とすることも可能です。</p> <p>※ IX シリーズ側の設定を Web-GUI で行った場合、「aes-cbc-256 aes-cbc-192 aes-cbc-128」が設定されますので、WA シリーズ側は「aes-cbc-256」、「aes-cbc-192」、「aes-cbc-128」のいずれかを含む設定を行ってください。</p>
child-proposal integrity sha2-256	<p>IX シリーズの Tunnel インタフェースの ikev2 child-proposal integrity コマンドと一致する認証アルゴリズムを設定してください。</p> <p>1. 2. 1. 1 章の設定例の場合、IX シリーズ側は sha2-512 sha2-384 sha2-256 の 3 種を設定しておりますが、WA シリーズではこれら 3 種の内、sha2-256 のみ設定可能ですので、1. 2. 1. 1 章の設定の IX シリーズと接続する場合は、sha2-256 を設定してください。</p> <p>※ IX シリーズ側の設定を Web-GUI で行った場合、「sha2-512 sha2-384 sha2-256」が設定されますので、WA シリーズ側は「sha2-256」含む設定を行ってください。</p>
child-pfs 2048-bit	<p>IX シリーズの Tunnel インタフェースの ikev2 child-pfs と同じ PFS を設定してください。</p> <p>※ IX シリーズ側の設定を Web-GUI で行った場合、「2048-bit」が設定されますので、WA シリーズ側も「2048-bit」を設定してください。</p>

1.2.1.3.5. BGP の設定

1. 2. 2. 1 章の設定例の内、BGP に関連する各設定の詳細を以下に記載します。

設定コマンド	説明
route-map dmvpn-map permit 10 match interface GigaEthernet1.0	BGP で他のセンタ/拠点に LAN 側のネットワークアドレスを通知するために、1. 2. 1. 3. 2 章で nhrp local コマンドで設定したインタフェース指定で route-map を作成します。
ip route 169.254.0.0/24 mGRE0.0	<p>BGP のパケットを、mGRE0.0 インタフェース経由でダイナミック VPN のトンネルを通過させるためのルーティング設定です。プロトコルアドレスのネットワークアドレスを設定してください。</p> <p>※ IX シリーズの設定を Web-GUI で行った場合、プロトコルアドレスのネットワークアドレスは「169.254.0.0/16」となりますので、「ip route 169.254.0.0/16 mGRE0.0」としてください。</p>

<pre>router bgp 65535</pre>	<p>BGP の設定を行います。 AS 番号は全センタ/拠点で同じ番号(1.2.1.1 章の router bgp の番号)を設定してください。</p> <p>※ IX シリーズの設定を Web-GUI で行った場合、IX シリーズ側の AS 番号は 65535 となります。</p>
<pre>neighbor 169.254.0.100 remote-as 65535</pre>	<p>BGP のネイバーとして、センタの IX シリーズのプロトコルアドレスを設定します。 AS 番号は 1.2.1.1 章の router bgp の番号(=自装置と同じ番号)を設定してください。</p> <p>※ IX シリーズの設定を Web-GUI で行った場合、左記の「169.254.0.100」の箇所は「169.254.255.254」を設定してください。</p> <p>※ IX シリーズの設定を Web-GUI で行った場合、IX シリーズ側の AS 番号は 65535 となります。</p>
<pre>address-family ipv4 unicast redistribute connected route-map dmvpn-map</pre>	<p>BGP で他センタ/拠点に通知するネットワークアドレスを設定します。 設定例では LAN 側のインタフェース指定で作成した route-map を対象としていますが、network コマンドでネットワークアドレスを直接設定することも可能です。</p>

1.2.2. WA シリーズをセンタとする場合

1.2.2.1. WA シリーズ側の設定例

```
!  
route-map dmvpn-map permit 10  
  match interface GigaEthernet1.0  
!  
interface GigaEthernet0.0  
  ip address 203.113.0.100/24  
  ikev2 binding ikev2-prof1  
  :  
  ikev2 binding ikev2-prof16  
  no shutdown  
!  
interface GigaEthernet1.0  
  ip address 192.168.0.254/24  
  no shutdown  
!  
interface mGRE0.0  
  gre source GigaEthernet0.0  
  ip address 169.254.0.100/24  
  no shutdown  
!  
!  
ip route 169.254.0.0/24 mGRE0.0  
!  
router bgp 65535  
  timers 5 15  
  cluster-id 169.254.0.100  
  connect-interval 10  
  address-family ipv4 unicast  
    dmvpn next-hop-self  
    redistribute connected route-map dmvpn-map  
!  
ikev2 profile ikev2-prof1  
  peer any  
!  
  :  
!  
ikev2 profile ikev2-prof16  
  peer any  
!  
ikev2 default-profile  
  ipsec-mode transport  
  source-address GigaEthernet0.0  
  local-authentication psk plain dmvpn-password  
  local-id address 169.254.0.100  
  dpd interval 10  
  nat-traversal enable keepalive 20  
  sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
```

```
sa-proposal integrity sha2-256
sa-proposal prf sha2-256
sa-proposal dh 2048-bit
ignore tsi-payload
child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
child-proposal integrity sha2-256
child-pfs 2048-bit
!
```

1.2.2.2. IX シリーズ側の設定例

```
!
nhrp local GigaEthernet2.0
!
ikev2 authentication psk id ipv4 169.254.0.1 key char dmvpn-password
!
!
!
route-map dmvpn-map permit 10
  match interface GigaEthernet2.0
!
router bgp 65535
  timers 5 15
  neighbor 169.254.0.100 remote-as 65535
  neighbor 169.254.0.100 connect-interval 10
  address-family ipv4 unicast
    redistribute connected route-map dmvpn-map
!
interface GigaEthernet0.0
  ip address 203.113.0.1/24
  no shutdown
!
interface GigaEthernet2.0
  ip address 192.168.1.254/24
  no shutdown
!
interface Tunnel0.0
  description DynamicVPN_#1
  tunnel mode mgre ipsec-ikev2
  ip address 169.254.0.1/24
  ip tcp adjust-mss auto
nhrp nhs 169.254.0.100/24 nbma 203.113.0.100
ikev2 child-pfs 2048-bit
ikev2 child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
ikev2 child-proposal integrity sha2-512 sha2-384 sha2-256
ikev2 dpd interval 10
ikev2 local-authentication psk id ipv4 169.254.0.1
ikev2 nat-traversal keepalive 20
ikev2 outgoing-interface GigaEthernet0.1 auto
ikev2 sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
ikev2 sa-proposal integrity sha2-512 sha2-384 sha2-256
```

```
ikev2 sa-proposal dh 2048-bit
ikev2 sa-proposal prf sha2-512 sha2-384 sha2-256
ikev2 ipsec-mode transport
ikev2 peer any authentication psk
no shutdown
```

```
!
```

1.2.2.3. WA シリーズの設定の説明

1.2.2.3.1. WAN 側インタフェースの設定

ダイナミック VPN の WAN 側のインタフェースは、IKEv2 プロファイルの設定が可能なインタフェースであれば、どのインタフェースでの使用可能です。

1. 2. 2. 1 章の設定例では、IX シリーズの GigaEthernet0.0 と同じネットワークアドレスを設定した GigaEthernet0.0 を、ダイナミック VPN の WAN 側インタフェースとして使用する設定を記載しています。

※ 上記は IX シリーズ側に 1. 2. 2. 2 章の設定を行った場合で記載しています。IX シリーズ側の設定を Web-GUI で行った場合は、web-console system information の wan1 のインタフェースと通信可能なインタフェースを、WA シリーズの WAN 側インタフェースとして設定してください。

1.2.2.3.2. LAN 側インタフェースの設定

ダイナミック VPN のセンタは NHRP 解決要求を受信（配下拠点への転送のための経由点としての受信を除く）することは無いため、nhrp local コマンドで LAN 側インタフェースを設定する必要はありません。

LAN 側インタフェースのネットワークアドレスをルーティング情報として配下拠点に通知するための設定は 1. 2. 2. 3. 5 章の BGP の設定をご参照ください。

1.2.2.3.3. mGRE インタフェースの設定

ダイナミック VPN 機能では、mGRE インタフェースを使用することで GRE over IPsec の複数対地接続を行います。

1. 2. 1. 2 章の設定例で mGRE0.0 インタフェースに対して行っている各設定の詳細を以下に記載します。

設定コマンド	説明
gre source GigaEthernet0.0	1. 2. 1. 3. 3 章と同様のため、詳細は 1. 2. 1. 3. 3 章をご参照ください。
no nhrp nhs	自身がセンタ装置のため、nhrp nhs コマンドの設定は不要です。
ip address 169.254.0.100/24	拠点装置である IX シリーズのプロトコルアドレス (Tunnel インタフェースの IP アドレス) と同じネットワーク、かつ重複しない IP アドレスを設定します。 1. 2. 1. 3. 3 章と同様のため、詳細は 1. 2. 1. 3. 3 章をご参照ください。 ※ IX シリーズ側の設定を Web-GUI で行った場合、IX シリーズのプロトコルアドレスは 169.254.0.X/16 となりますので、169.254.0.X/16 と同じネットワークかつ、重複しない IP アドレス (169.254.255.254/16 など) を設定してください。
no dmvpn ike-id (デフォルト設定値)	1. 2. 1. 3. 3 章と同様のため、詳細は 1. 2. 1. 3. 3 章をご参照ください。
no nhrp enable-ack-with-nat (デフォルト設定値)	センタ装置は nhrp enable-ack-with-nat コマンドは設定有無で動作に変化がありませんので、設定は不要です。

1.2.2.3.4. IKEv2 の設定

WA シリーズがセンタの場合も、IKEv2 の設定は 1.2.1.3.4 章の拠点の場合の設定をほぼそのまま使用できます。

本章では 1.2.1.3.4 章と設定値の異なるコマンドについてのみ記載いたします。

設定コマンド	説明
local-id address 169.254.0.100	1.2.1.3.4 章に記載の通り、local-id には自装置のプロトコルアドレス (mGRE インタフェースの IP アドレス) を設定します。1.2.2.1 章の設定例では mGRE0.0 インタフェースの IP アドレスを 169.254.0.100 としているため、local-id にも 169.254.0.100 を設定します。
ignore tsi-payload	ignore tsi-payload コマンドは、NAT/NAPT 配下の WA シリーズが NAT/NAPT 外部の IX シリーズと接続するために必要な設定のため、WA シリーズをセンタとして使用する場合は設定不要ですが、設定を行っても接続性に影響は有りません。

- ※ IX シリーズ側の設定を Web-GUI で行った場合、SA、Child-SA の暗号化アルゴリズムには「aes-cbc-256 aes-cbc-192 aes-cbc-128」が設定されますので、WA シリーズ側は「aes-cbc-256」、「aes-cbc-192」、「aes-cbc-128」のいずれかを含む設定を行ってください。
- ※ IX シリーズ側の設定を Web-GUI で行った場合、SA、Child-SA の認証アルゴリズムや PRF アルゴリズムには「sha2-512 sha2-384 sha2-256」が設定されますので、WA シリーズ側は「sha2-256」含む設定を行ってください。
- ※ IX シリーズ側の設定を Web-GUI で行った場合、sa-proposal の dh や chide-pfs には「2048-bit」が設定されますので、WA シリーズ側も「2048-bit」を設定してください。

1.2.2.3.5. BGP の設定

1.2.1.1 章の IX シリーズの設定例では、ダイナミック VPN 網内の各センタ/拠点間でのルーティングの設定に BGP を使用する設定を行っています。

1.2.1.2 章の設定例の内、BGP に関連する各設定の詳細を以下に記載します。

設定コマンド	説明
route-map dmvpn-map permit 10 match interface GigaEthernet1.0	1.2.1.3.5 章と同様のため、詳細は 1.2.1.3.5 章をご参照ください。
ip route 169.254.0.0/24 mGRE0.0	1.2.1.3.5 章と同様のため、詳細は 1.2.1.3.5 章をご参照ください。
router bgp 65535	1.2.1.3.5 章と同様のため、詳細は 1.2.1.3.5 章をご参照ください。
cluster-id 169.254.0.100	ルートリフレクタのクラスタ ID を設定します。 設定例ではセンタ装置のプロトコルアドレスを設定していますが、どのような設定値でも問題はありません。

<pre>address-family ipv4 unicast dmvpn next-hop-self</pre>	<p>配下拠点から通知されたルーティング情報を他の拠点にアドバタイズする際に、ネクストホップをセンタ装置のプロトコルアドレスに変更するための設定です。</p> <p>配下拠点の LAN 側インタフェースが複数ある場合に、LAN 側インタフェース数分のショートカットルート生成を可能とするために、センタ装置に本コマンドの設定が必要となります。</p> <p>本コマンドを設定しない場合、配下拠点から通知されたルーティング情報が、そのまま他の拠点にアドバタイズされるため、宛先拠点毎に生成可能なショートカットルートが 1 つずつのみ(※)となります。</p> <p>※ 配下拠点から通知されたルーティング情報がそのままアドバタイズされた場合、ルーティング情報のネクストホップは宛先拠点のプロトコルアドレスとなります。このため、LAN を複数持つ拠点が宛先の場合、いずれか 1 つの LAN 宛で拠点間トンネルを生成済であれば、他の LAN 宛のパケットは NHRP 解決を行わずに宛先拠点に転送可能となります。</p> <p>センタに dmvpn next-hop-self を設定することで、ルーティング情報のネクストホップがセンタとなるため、全ての LAN 宛のパケットが NHRP 解決の対象(ショートカットルート生成前はセンタ経由での転送となるため)とすることが可能となります。</p>
<pre>redistribute connected route-map dmvpn-map</pre>	<p>1.2.1.3.5 章と同様のため、詳細は 1.2.1.3.5 章をご参照ください。</p>

2. Cisco と接続する場合の設定

WA シリーズと Cisco をダイナミック VPN で接続する場合の、CLI コマンド/Web-GUI (WA シリーズのみ) それぞれの設定方法について記載します。

※ 本章の Cisco 側の設定は Cisco 881 を対象とした内容です。

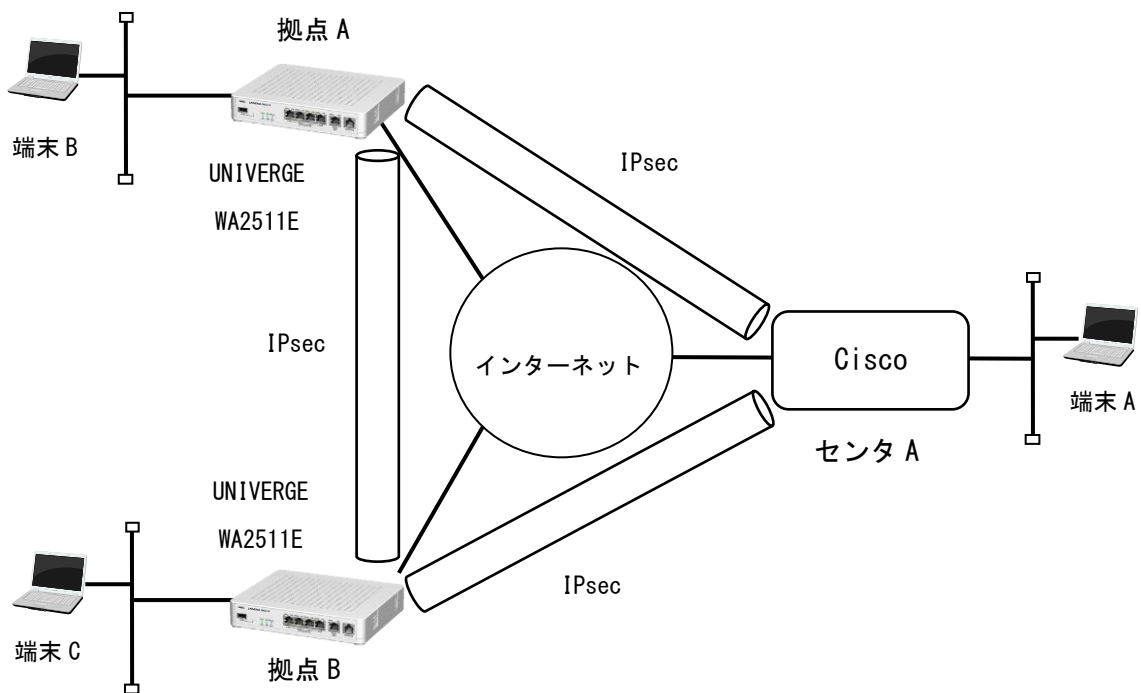
2.1. CLI コマンドでの設定

本章では Cisco と接続するために WA シリーズに必要な CLI コマンドの設定例を記載いたします。

2.1.1. Cisco をセンタとする場合

2.1.1.1. 接続構成例

Cisco をセンタとしたときの接続構成例です。



2.1.1.2. Cisco 側の設定例

```
crypto ikev2 proposal cisco-ikev2-prop
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy cisco-ikev2-pol
  proposal cisco-ikev2-prop
!
crypto ikev2 keyring cisco-ikev2-keyring
  peer dmpn-node
    address 0.0.0.0 0.0.0.0
    pre-shared-key dmpn-password
!
!
crypto ikev2 profile cisco-ikev2-profile
  match identity remote address 203.113.0.0 255.255.255.0
  match identity remote address 169.254.1.0 255.255.255.0
  authentication remote pre-share
  authentication local pre-share
  keyring local cisco-ikev2-keyring
!
crypto ipsec transform-set cisco-ts esp-aes 256 esp-sha256-hmac
  mode transport
!
crypto ipsec profile cisco-ipsec-ikev2
  set transform-set cisco-ts
  set ikev2-profile cisco-ikev2-profile
!
interface Tunnel0
  ip address 169.254.1.200 255.255.255.0
  no ip redirects
  ip nhrp map multicast dynamic
  ip nhrp network-id 9
  ip nhrp redirect
  tunnel source FastEthernet4
  tunnel mode gre multipoint
  tunnel protection ipsec profile cisco-ipsec-ikev2
!
interface FastEthernet0
  no ip address
!
interface FastEthernet1
  no ip address
!
interface FastEthernet2
  no ip address
!
interface FastEthernet3
  no ip address
```

```
!  
interface FastEthernet4  
  ip address 203.113.0.200 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface Vlan1  
  ip address 192.168.10.1 255.255.255.0  
!  
router bgp 65535  
  bgp log-neighbor-changes  
  bgp listen range 169.254.1.0/24 peer-group dmvpn-group  
  neighbor dmvpn-group peer-group  
  neighbor dmvpn-group remote-as 65535  
  !  
  address-family ipv4  
    redistribute connected route-map dmvpn-map  
    neighbor dmvpn-group activate  
    neighbor dmvpn-group route-reflector-client  
  exit-address-family  
  !  
  !  
  route-map dmvpn-map permit 10  
    match interface Vlan1  
  !
```

2.1.1.3. WA シリーズ側の設定例

```
route-map dmvpn-map permit 10
  match interface GigaEthernet1.0
!
!
interface GigaEthernet0.0
  ip address 203.113.0.1/24
  ikev2 binding ikev2-prof1
  :
  ikev2 binding ikev2-prof16
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.1.1/24
  no shutdown
!
!
interface mGRE0.0
  gre source GigaEthernet0.0
  nhrp nhs 169.254.1.200/24 nbma 203.113.0.200
  dmvpn ike-id nbma-address
  ip address 169.254.1.1/24
  no shutdown
!
ip route 169.254.1.0/24 mGRE0.0
!
router bgp 65535
  neighbor 169.254.1.200 remote-as 65535
  address-family ipv4 unicast
    redistribute connected route-map dmvpn-map
!
ikev2 profile ikev2-prof1
  peer any
!
  :
!
ikev2 profile ikev2-prof16
  peer any
!
ikev2 default-profile
  ipsec-mode transport
  source-address GigaEthernet0.0
  local-authentication psk plain dmvpn-password
  sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
  sa-proposal integrity sha2-256
  sa-proposal prf sha2-256
  sa-lifetime 28800
  sa-proposal dh 2048-bit
  ignore config-payload
  child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
```

```
child-proposal integrity sha2-256
child-lifetime 28800
child-pfs 2048-bit
upper-layer-protocol 47
!
nhrp local GigaEthernet1.0
!
```

2.1.1.4. WA シリーズの設定の説明

2.1.1.4.1. WAN 側インタフェースの設定

ダイナミック VPN の WAN 側のインタフェースは、IKEv2 プロファイルの設定が可能なインタフェースであれば、どのインタフェースでの使用可能です。2. 1. 1. 3 章の設定例では、Cisco の FastEthernet4 と同じネットワークアドレスを設定した GigaEthernet0.0 を、ダイナミック VPN の WAN 側インタフェースとして使用する設定を記載しています。

2.1.1.4.2. LAN 側インタフェースの設定

ダイナミック VPN の LAN 側として使用するインタフェースは、nhrp local コマンドで設定することができます。2. 1. 1. 3 章の設定例では、GigaEthernet1.0 を LAN 側インタフェースとして使用する設定を記載しています。

LAN 側インタフェースの設定は拠点間トンネルの生成に必要な設定です。nhrp local コマンドで設定したインタフェースのネットワークを宛先とするパケットをトリガとして、拠点間トンネルを生成することができるようになります。

2.1.1.4.3. mGRE インタフェースの設定

ダイナミック VPN 機能では、mGRE インタフェースを使用することで GRE over IPsec の複数対地接続を行います。

2. 1. 1. 3 章の設定例で mGRE0.0 インタフェースに対して行っている各設定の詳細を以下に記載します。

設定コマンド	説明
gre source GigaEthernet0.0	GRE カプセル化後の Outer IP ヘッダの送信元 IP アドレスを設定するコマンドです。設定例では、WAN 側インタフェースとして使用する GigaEthernet0.0 の IP アドレスを設定しています。 ※ 設定を省略した場合、mGRE トンネルの宛先へのルーティングから最適なインタフェースを選択し、インタフェースの IP アドレスを使用しますが、設定例は GigaEthernet0.0 のみ使用する設定のため、明示的に GigaEthernet0.0 を設定しています。
nhrp nhs 169.254.1.200/24 nbma 203.113.0.200	センタ装置である Cisco のプロトコルアドレス (Tunnel インタフェースの IP アドレス) と、NBMA アドレス (WAN 側インタフェースの IP アドレス) を設定します。 ※ NBMA アドレスは IP アドレスの他、FQDN を設定することも可能です。
ip address 169.254.1.1/24	センタ装置である Cisco のプロトコルアドレス (Tunnel インタフェースの IP アドレス) と同じネットワーク、かつ重複しない IP アドレスを設定します。 2. 1. 1. 2 章の Cisco の設定例では、プロトコルアドレスに 169.254.1.200/24 を設定しているため、WA シリーズ側は 169.254.1.0/24 のネットワークで、169.254.1.200 と重複しない 169.254.1.1/24 を設定しています。

dmvpn ike-id nbma-address	Cisco のダイナミック VPN では IKE ネゴシエーションの ID に NBMA アドレス (WAN 側インタフェースの IP アドレス) を使用します。このため、WA シリーズ側も同様に、IKE ネゴシエーション ID に NBMA アドレスを使用する設定とする必要があります。
---------------------------	--

2.1.1.4.4. IKEv2 の設定

Cisco とのダイナミック VPN 接続は、IKEv2/IKEv1、トランスポートモード/トンネルモードのどれを使用しても可能ですが、本書では IX シリーズとの接続と同様に IKEv2 のトランスポートモードを例として記載します。

2.1.1.3 章の設定例の内、IKEv2 に関連する各設定の詳細を以下に記載します。

設定コマンド	説明
interface GigaEthernet0.0 ikev2 binding ikev2-prof1 : ikev2 binding ikev2-prof16	WAN 側インタフェースにダイナミック VPN で使用する IKEv2 プロファイルを必要数分設定します。 設定例では、1 つの mGRE インタフェースでの最大接続数 (16) 分の IKEv2 プロファイルを設定しています。
ikev2 profile ikev2-profX peer any	ダイナミック VPN 機能では peer の設定を any または any ipv6 とする必要があります。 設定例では WAN 側インタフェースは IPv4 のため、peer any を設定しています。
ikev2 default-profile	WAN 側インタフェースに設定する全ての IKEv2 プロファイルで共通する設定 (peer 以外) は IKEv2 デフォルトプロファイルで設定することが可能です。 (IKEv2 デフォルトプロファイルを使用することで、CLI コマンドの設定数を少なくすることができます。) なお、IKEv2 デフォルトプロファイルを使用せず、各 IKEv2 プロファイルにそれぞれ同じ設定を行う方法でも、設定例と同様の設定が可能です。
ipsec-mode transport	本書では GRE over IPsec で一般に用いられるトランスポートモードを設定します。
source-address GigaEthernet0.0	Child-SA を確立するソースインタフェースを設定します。 Child-SA は WAN 側インタフェース間で生成するため、WAN 側インタフェースの IP アドレスを設定します。
local-authentication psk plain dmvpn-password	ダイナミック VPN 機能では、全センタ/装置で同じ事前共有鍵を使用する必要があります。 このため、local-authentication コマンドでは IX シリーズ側と同じ事前共有鍵を設定してください。 Cisco の対象の設定は、2.1.1.2 章の設定例の場合は、以下が該当します。 crypto ikev2 keyring cisco-ikev2-keyring peer dmvpn-node address 0.0.0.0 0.0.0.0 pre-shared-key dmvpn-password

no local-id	Cisco と接続する場合、local-id には自装置の NBMA アドレス (WAN 側インタフェースの IP アドレス) を設定する必要があります。 WA シリーズは local-id の設定を省略すると、local-id に WAN 側インタフェースの IP アドレスを使用します。WAN 側インタフェースの IP アドレスを直接設定することも可能ですが、WAN 側インタフェースは DHCP や IPCP など動的に IP アドレスを取得するケースもあるため、local-id の設定を省略が推奨です。
sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128	Cisco の crypto ikev2 proposal の encryption と同じ暗号化アルゴリズムを含む設定を行います。
sa-proposal integrity sha2-256	Cisco の crypto ikev2 proposal の integrity と同じ認証アルゴリズムを設定します。
sa-proposal prf sha2-256	同上。
ignore config-payload	Cisco は IKE ネゴシエーションの際、ISAKMP のパケットに Config ペイロードを設定します。 WA シリーズはデフォルト設定では、未対応のペイロードを受信すると IKE ネゴシエーション NG とするため、ignore config-payload コマンドにより、Config ペイロードを受信しても無視する設定を行います。 なお、WA シリーズ側に ignore config-payload の設定を行わず、Cisco 側に no config-exchange request を設定 (Cisco が Config ペイロードを設定しないように設定) することでも接続可能です。
child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128	Cisco の crypto ikev2 proposal の encryption と同じ暗号化アルゴリズムを含む設定を行います。
child-proposal integrity sha2-256	Cisco の crypto ikev2 proposal の integrity と同じ認証アルゴリズムを設定します。
upper-layer-protocol 47	Cisco と接続するためには、トラフィックセクタの上位プロトコル番号に 47 (=GRE) を設定する必要があります。

2.1.1.4.5. BGP の設定

2.1.1.2 章の IX シリーズの設定例では、ダイナミック VPN 網内の各センタ/拠点間でのルーティングの設定に BGP を使用する設定を行っています。

2.1.1.3 章の設定例の内、BGP に関連する各設定の詳細を以下に記載します。

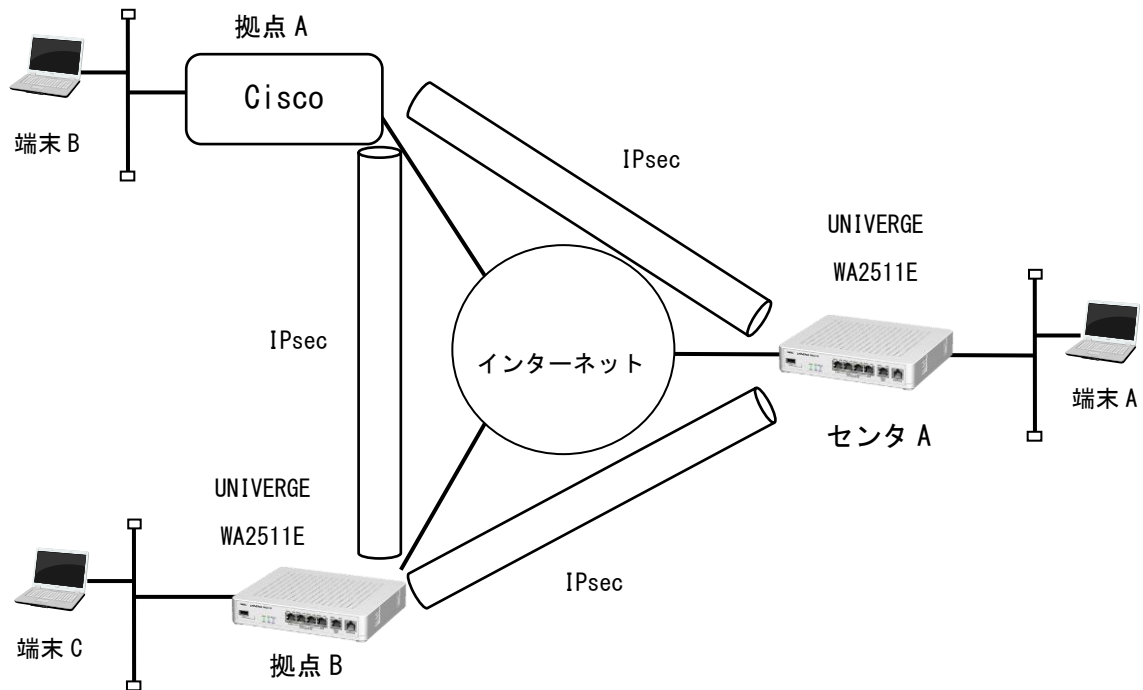
設定コマンド	説明
route-map dmvpn-map permit 10 match interface GigaEthernet1.0	BGP で他のセンタ/拠点に LAN 側のネットワークアドレスを通知するために、1.2.1.3.2 章で nhrp local コマンドで設定したインタフェース指定で route-map を作成します。
ip route 169.254.1.0/24 mGRE0.0	BGP のパケットを、mGRE0.0 インタフェースを経由でダイナミック VPN のトンネルを通過させるためのルーティング設定です。 プロトコルアドレスのネットワークアドレスを設定してください。
router bgp 65535	BGP の設定を行います。 AS 番号は全センタ/拠点で同じ番号 (2.1.1.2 章の router bgp の番号) を設定してください。

<pre>neighbor 169.254.1.200 remote-as 65535</pre>	<p>BGP のネイバーとして、センタの Cisco のプロトコルアドレスを設定します。</p> <p>AS 番号は 2.1.1.2 章の router bgp の番号 (= 自装置と同じ番号) を設定してください。</p>
<pre>address-family ipv4 unicast redistribute connected route-map dmvpn-map</pre>	<p>BGP で他センタ/拠点に通知するネットワークアドレスを設定します。</p> <p>設定例では LAN 側のインタフェース指定で作成した route-map を対象としていますが、network コマンドでネットワークアドレスを直接設定することも可能です。</p>

2.1.2. WA シリーズをセンタとする場合

2.1.2.1. 接続構成例

WA シリーズをセンタとしたときの接続構成例です。



2.1.2.2. Cisco 側の設定例

```
crypto ikev2 proposal cisco-ikev2-prop
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy cisco-ikev2-pol
  proposal cisco-ikev2-prop
!
crypto ikev2 keyring cisco-ikev2-keyring
  peer dmvpn-node
    address 0.0.0.0 0.0.0.0
    pre-shared-key dmvpn-password
!
!
crypto ikev2 profile cisco-ikev2-profile
  match identity remote address 203.113.0.0 255.255.255.0
  authentication remote pre-share
  authentication local pre-share
  keyring local cisco-ikev2-keyring
!
crypto ipsec transform-set cisco-ts esp-aes 256 esp-sha256-hmac
  mode transport
!
crypto ipsec profile cisco-ipsec-ikev2
  set transform-set cisco-ts
  set ikev2-profile cisco-ikev2-profile
!
interface Tunnel0
  ip address 169.254.1.200 255.255.255.0
  no ip redirects
  ip nhrp map 169.254.1.1 203.113.0.1
  ip nhrp multicast 203.113.0.1
  ip nhrp network-id 9
  ip nhrp nhs 169.254.1.1
  ip nhrp registration no-unique
  ip nhrp shortcut
  tunnel source FastEthernet4
  tunnel mode gre multipoint
  tunnel protection ipsec profile cisco-ipsec-ikev2
!
interface FastEthernet0
  no ip address
!
interface FastEthernet1
  no ip address
!
interface FastEthernet2
  no ip address
```

```
!  
interface FastEthernet3  
  no ip address  
!  
interface FastEthernet4  
  ip address 203.113.0.200 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface Vlan1  
  ip address 192.168.10.1 255.255.255.0  
!  
router bgp 65535  
  bgp log-neighbor-changes  
  neighbor 169.254.1.1 remote-as 65535  
  neighbor 169.254.1.1 update-source Tunnel0  
  !  
  address-family ipv4  
    redistribute connected route-map dmvpn-map  
    neighbor 169.254.1.1 activate  
  exit-address-family  
  !  
  !  
  route-map dmvpn-map permit 10  
    match interface Vlan1 FastEthernet0  
  !
```

2.1.2.3. WA シリーズ側の設定例

```
!  
route-map dmvpn-map permit 10  
  match interface GigaEthernet1.0  
!  
interface GigaEthernet0.0  
  ip address 203.113.0.1/24  
  ikev2 binding ikev2-prof1  
  :  
  ikev2 binding ikev2-prof16  
  no shutdown  
!  
interface GigaEthernet1.0  
  ip address 192.168.1.1/24  
  no shutdown  
!  
interface mGRE0.0  
  gre source GigaEthernet0.0  
  dmvpn ike-id nbma-address  
  ip address 169.254.1.1/24  
  no shutdown  
!  
!  
ip route 169.254.1.0/24 mGRE0.0  
!  
router bgp 65535  
  timers 5 15  
  cluster-id 169.254.1.1  
  connect-interval 10  
  address-family ipv4 unicast  
    dmvpn next-hop-self  
  redistribute connected route-map dmvpn-map  
!  
ikev2 profile ikev2-prof1  
  peer any  
!  
  :  
!  
ikev2 profile ikev2-prof16  
  peer any  
!  
ikev2 default-profile  
  ipsec-mode transport  
  source-address GigaEthernet0.0  
  local-authentication psk plain dmvpn-password  
  dpd interval 10  
  nat-traversal enable keepalive 20  
  sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128  
  sa-proposal integrity sha2-256  
  sa-proposal prf sha2-256
```

```
sa-proposal dh 2048-bit
ignore config-payload
child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
child-proposal integrity sha2-256
child-pfs 2048-bit
```

!

2.1.2.4. WA シリーズの設定の説明

2.1.2.4.1. WAN 側インタフェースの設定

ダイナミック VPN の WAN 側のインタフェースは、IKEv2 プロファイルの設定が可能なインタフェースであれば、どのインタフェースでの使用可能です。2. 1. 2. 3 章の設定例では、Ciaso の FastEthernet4 と同じネットワークアドレスを設定した GigaEthernet0.0 を、ダイナミック VPN の WAN 側インタフェースとして使用する設定を記載しています。

2.1.2.4.2. LAN 側インタフェースの設定

ダイナミック VPN のセンタは NHRP 解決要求を受信（配下拠点への転送のための経由点としての受信を除く）することは無いため、nhrp local コマンドで LAN 側インタフェースを設定する必要はありません。

LAN 側インタフェースのネットワークアドレスをルーティング情報として配下拠点に通知するための設定は 2. 1. 2. 4. 5 章の BGP の設定をご参照ください。

2.1.2.4.3. mGRE インタフェースの設定

ダイナミック VPN 機能では、mGRE インタフェースを使用することで GRE over IPsec の複数対地接続を行います。

2. 1. 2. 3 章の設定例で mGRE0.0 インタフェースに対して行っている各設定の詳細を以下に記載します。

設定コマンド	説明
gre source GigaEthernet0.0	2. 1. 1. 4. 3 章と同様のため、詳細は 2. 1. 1. 4. 3 章をご参照ください。
no nhrp nhs	自身がセンタ装置のため、nhrp nhs コマンドの設定は不要です。
ip address 169.254.1.1/24	拠点装置である Cisco のプロトコルアドレス (Tunnel インタフェースの IP アドレス) と同じネットワーク、かつ重複しない IP アドレスを設定します。 2. 1. 1. 4. 3 章と同様のため、詳細は 2. 1. 1. 4. 3 章をご参照ください。
dmvpn ike-id nbma-address	2. 1. 1. 4. 3 章と同様のため、詳細は 2. 1. 1. 4. 3 章をご参照ください。

2.1.2.4.4. IKEv2 の設定

WA シリーズがセンタの場合も、IKEv2 の設定は 2.1.1.4.4 章の拠点の場合の設定をそのまま使用できます。

2.1.2.4.5. BGP の設定

2.1.2.3 章の設定例の内、BGP に関連する各設定の詳細を以下に記載します。

設定コマンド	説明
route-map dmvpn-map permit 10 match interface GigaEthernet1.0	2.1.1.4.5 章と同様のため、詳細は 2.1.1.4.5 章をご参照ください。
ip route 169.254.1.0/24 mGRE0.0	2.1.1.4.5 章と同様のため、詳細は 2.1.1.4.5 章をご参照ください。
router bgp 65535	2.1.1.4.5 章と同様のため、詳細は 2.1.1.4.5 章をご参照ください。
cluster-id 169.254.1.1	ルートリフレクタのクラスタ ID を設定します。 設定例ではセンタ装置のプロトコルアドレスを設定していますが、どのような設定値でも問題はありません。
address-family ipv4 unicast dmvpn next-hop-self	配下拠点から通知されたルーティング情報を他の拠点にアドバタイズする際に、ネクストホップをセンタ装置のプロトコルアドレスに変更するための設定です。 配下拠点の LAN 側インタフェースが複数ある場合に、LAN 側インタフェース数分のショートカットルート生成を可能とするために、センタ装置に本コマンドの設定が必要となります。 本コマンドを設定しない場合、配下拠点から通知されたルーティング情報が、そのまま他の拠点にアドバタイズされるため、宛先拠点毎に生成可能なショートカットルートが1つずつのみ(※)となります。 ※ 配下拠点から通知されたルーティング情報がそのままアドバタイズされた場合、ルーティング情報のネクストホップは宛先拠点のプロトコルアドレスとなります。このため、LAN を複数持つ拠点が宛先の場合、いずれか1つの LAN 宛で拠点間トンネルを生成済であれば、他の LAN 宛のパケットは NHRP 解決を行わずに宛先拠点に転送可能となります。 センタに dmvpn next-hop-self を設定することで、ルーティング情報のネクストホップがセンタとなるため、全ての LAN 宛のパケットが NHRP 解決の対象(ショートカットルート生成前はセンタ経由での転送となるため)とすることが可能となります。
redistribute connected route-map dmvpn-map	2.1.1.4.5 章と同様のため、詳細は 2.1.1.4.5 章をご参照ください。

2.2. Web-GUI での設定 (WA シリーズのみ)

2.2.1. Cisco をセンタとする場合

2.2.1.1. かんたん設定

かんたん設定の画面の各入力項目と、センタとして設定を行った Cisco と接続するための設定値は以下の通りです。

項目名	説明	Cisco と接続するための設定値
タイプ	拠点/センタのどちらで設定するかを選択します。	本章では WA シリーズを拠点とするため、拠点を選択します。
mGRE の IP アドレス	WA シリーズの Protocol アドレス (mGRE 0.0 インタフェースの IP アドレス) を設定します。	Cisco の Tunnel インタフェースの IP アドレスと同じネットワークで、重複しない IP アドレス (169.254.1.1/24 など) を設定します。
IKE バージョン	ダイナミック VPN で使用する IKE のバージョンを選択します。	Cisco は IKEv2/IKEv1 どちらもサポートしておりますが、本書では代表して IKEv2 を設定します。
IKE の ID に使用するアドレス	IKE の ID に Protocol アドレス (mGRE インタフェースの IP アドレス) と、NBMA アドレス (WAN 側インタフェースのアドレス) のどちらを使用するか選択します。	Cisco は IKE の ID に NBMA アドレスを使用するため、WAN 側の IP アドレス (NBMA アドレス) を選択します。
事前共有鍵	IKE の事前共有鍵を設定します。	Cisco 側に設定した事前共有鍵と同じ設定値とする必要があるため、Cisco の pre-shared-key と同じ内容を設定します。
IKE SA 暗号化アルゴリズム	IKE SA 暗号化アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の encryption と同じ暗号化アルゴリズムを設定します。
IKE SA 認証アルゴリズム	IKE SA 認証アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の integrity と同じ認証アルゴリズムを設定します。
IKE SA PRF アルゴリズム	IKE SA PRF アルゴリズムを選択します。	同上。
Child SA 暗号化アルゴリズム	Child SA 暗号化アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の encryption と同じ暗号化アルゴリズムを設定します。
Child SA 認証アルゴリズム	Child SA 認証アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の integrity と同じ認証アルゴリズムを設定します。
NAT/NAPT 配下の拠点との間の VPN 接続条件	NAT/NAPT 配下の拠点がどの VPN 接続について、片側が NAT/NAPT の場合のみ接続可能とするか、両側が NAT の場合も接続可能とするかを選択します。	NAT 配下の拠点、かつ宛先の拠点が同じ NAT 配下でない場合、本項目はどちらを設定しても Cisco との接続性に影響はありません。

センタ装置の WAN 側の IP アドレス	センタ装置の NBMA アドレスを設定します。	センタとして使用する Cisco の WAN 側インタフェース (設定例では FastEthernet4) の IP アドレス、または FQDN を設定します。
センタ装置の mGRE の IP アドレス	センタ装置の プロトコルアドレスを設定します。	センタとして使用する Cisco の プロトコルアドレス (Tunnel インタフェースの IP アドレス) である 169.254.1.200/24 を設定します。

2.2.1.2. 装置設定

装置設定の画面の各入力項目の内、装置設定固有の項目について、センタとして設定を行った Cisco と接続するための設定値を以下に記載します。(かんたん設定と共通の項目については、2.2.1.1 章をご参照ください。)

項目名	説明	Cisco と接続するための設定値
WAN 側インタフェース	ダイナミック VPN で使用する WAN 側のインタフェースを選択します。	Cisco の WAN 側インタフェースと接続可能なインタフェースを選択してください。 選択したインタフェースの詳細は「有線回線」や「モバイル回線」の設定画面で設定を行ってください。
LAN 側インタフェース	ダイナミック VPN で使用する LAN 側のインタフェースを選択します。	どのインタフェースを選択しても Cisco との接続に影響はありません。

2.2.2. WA シリーズをセンタとする場合

2.2.2.1. かんたん設定

かんたん設定の画面の各入力項目と、拠点として設定を行った Cisco と接続するための設定値は以下の通りです。

項目名	説明	Cisco と接続するための設定値
タイプ	拠点/センタのどちらで設定するかを選択します。	本章では WA シリーズをセンタとするため、センタを選択します。
mGRE の IP アドレス	WA シリーズのプロトコルアドレス (mGRE0.0 インタフェースの IP アドレス) を設定します。	Cisco の Tunnel インタフェースの IP アドレスと同じネットワークで、重複しない IP アドレス (169.254.1.1/24 など) を設定します。
IKE バージョン	ダイナミック VPN で使用する IKE のバージョンを選択します。	Cisco は IKEv2/IKEv1 どちらもサポートしておりますが、本書では代表して IKEv2 を設定します。
IKE の ID に使用するアドレス	IKE の ID にプロトコルアドレス (mGRE インタフェースの IP アドレス) と、NBMA アドレス (WAN 側インタフェースのアドレス) のどちらを使用するか選択します。	Cisco は IKE の ID に NBMA アドレスを使用するため、WAN 側の IP アドレス (NBMA アドレス) を選択します。
事前共有鍵	IKE の事前共有鍵を設定します。	Cisco 側に設定した事前共有鍵と同じ設定値とする必要があるため、Cisco の pre-shared-key と同じ内容を設定します。
IKE SA 暗号化アルゴリズム	IKE SA 暗号化アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の encryption と同じ暗号化アルゴリズムを設定します。
IKE SA 認証アルゴリズム	IKE SA 認証アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の integrity と同じ認証アルゴリズムを設定します。
IKE SA PRF アルゴリズム	IKE SA PRF アルゴリズムを選択します。	同上。
Child SA 暗号化アルゴリズム	Child SA 暗号化アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の encryption と同じ暗号化アルゴリズムを設定します。
Child SA 認証アルゴリズム	Child SA 認証アルゴリズムを選択します。	Cisco の crypto ikev2 proposal の integrity と同じ認証アルゴリズムを設定します。

2.2.2.2. 装置設定

装置設定の画面の各入力項目の内、装置設定固有の項目について、拠点として設定を行った Cisco と接続するための設定値を以下に記載します。(かんたん設定と共通の項目については、2.2.2.1 章をご参照ください。)

項目名	説明	Cisco と接続するための設定値
WAN 側インタフェース	ダイナミック VPN で使用する WAN 側のインタフェースを選択します。	Cisco の WAN 側インタフェースと接続可能なインタフェースを選択してください。 選択したインタフェースの詳細は「有線回線」や「モバイル回線」の設定画面で設定を行ってください。
LAN 側インタフェース	ダイナミック VPN で使用する LAN 側のインタフェースを選択します。	どのインタフェースを選択しても Cisco との接続に影響はありません。

2.3. IKEv1 を使用する場合

Cisco と IKEv1 を使用してダイナミック VPN 接続を行うための設定について記載します。

設定項目の大半は IKE バージョンによる設定値の差分がありませんので、本章では IKEv2 を使用する場合 (2.1 章、および 2.2 章) との差分点を中心に記載いたします。

2.3.1. Cisco 側

Cisco で IKEv1 を使用する場合の設定例 (2.1 章の IKEv2 の場合との差分点のみ) は以下の通りです。

```
crypto isakmp policy 1 ★ crypto ikev2 proposal/policy/keyring/profile に該当
encr aes 256
authentication pre-share
group 14
crypto isakmp key dmvpn-password address 0.0.0.0
!
crypto ipsec transform-set cisco-ts esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile cisco-ipsec-ikev1
set transform-set cisco-ts ★ set ikev2-profile は不要
!
interface Tunnel0
:
tunnel protection ipsec profile cisco-ipsec-ikev1
!
```

2.3.2. WA シリーズ側

- 鍵交換タイプはメインモードを使用してください、Web-GUI では「IKE バージョン」で「IKEv1 (メイン)」を選択、CLI コマンドでは `ike policy` の `mode` に `main` を設定してください。
- 暗号化アルゴリズム/認証アルゴリズムは Cisco 側の設定と一致するものを設定してください。2.3.1 章の設定例の場合、Web-GUI では「AES-CBC (256bits)」と「SHA1」を選択、CLI コマンドの場合では、`ike proposal` は `aes256-cbc` と `hmac-sha1` を、`ipsec proposal` は `aes256-cbc` と `hmac-sha1-96` を設定してください。
- 事前共有鍵は Cisco の `crypto isakmp key` と同じ設定値を全てのセンタ/拠点で使用してください。(IKEv2 の場合と同様)
- IKEv2 と同様、IKE の ID に NBMA アドレスを使用する設定を行ってください。Web-GUI では「IKE の ID に使用するアドレス」で「NBMA アドレス (WAN 側インタフェースのアドレス)」を選択、CLI コマンドでは `mGRE インタフェースコンフィグ` で `dmvpn ike-id nbma-address` を設定してください。
- IKE フェーズ 2 の ID の上位プロトコル番号に 47 (=GRE) を設定する必要があります。Web-GUI では特定の設定項目は無く自動で設定されますが、CLI コマンドでは `ipsec policy` の `upper-layer-protocol` に 47 を設定してください。

2.4. トンネルモードを使用する場合

Cisco と IKEv1 を使用してダイナミック VPN 接続を行うための設定について記載します。

設定項目の大半は IPsec カプセル化モードによる設定値の差分がありませんので、本章ではトランスポートモードを使用する場合 (2.1 章、および 2.2 章) との差分点を中心に記載いたします。

2.4.1. Cisco 側

Cisco でトンネルモードを使用する場合の設定例(2.1 章、2.3 章のトランスポートモードの場合との差分点のみ)は以下の通りです。

```
crypto ipsec transform-set cisco-ts esp-aes 256 esp-sha-hmac
mode tunnel ★ mode に tunnel を設定
!
```

2.4.2. WA シリーズ側

- Web-GUI ではトンネルモードの設定を行うことはできません。トンネルモードを使用する場合は CLI コマンドで設定してください。
- トンネルモードを使用する場合は、接続するトンネル数(対向装置数)分の IPsec インタフェースを用意し、mGRE インタフェースの gre outgoint-interface コマンドで使用する全ての IPsec インタフェースを設定してください。
- ikev2 profile の ipsec-mode や、ipsec profile の mode に tunnel を設定してください。
- IKEv1 を使用する場合は ike policy の mode に main を設定してください。
- 暗号化アルゴリズム/認証アルゴリズムは Cisco 側の設定と一致するものを設定してください。(トランスポートモードと同様)
- 事前共有鍵は Cisco の crypto isakmp key と同じ設定値を全てのセンタ/拠点で使用してください。(トランスポートモードと同様)
- トランスポートモードと同様、IKE の ID に NBMA アドレスを使用するために、mGRE インタフェースコンフィグで dmvpn ike-id nbma-address を設定してください。
- トランスポートモードと同様、IKEv2 のトラフィックセクタや IKEv1 の IKE フェーズ 2 の ID の上位プロトコル番号に 47(=GRE)を設定する必要があります。ikev2 profile や ipsec policy の upper-layer-protocol に 47 を設定してください。

※ 上記では IKEv2 の場合の設定方法を「ikev2 profile」としてありますが、ikev2 default-profile や IPsec インタフェースの ikev2 コマンドで設定することも可能です。

3. NAT/NAPT 環境での設定

WA シリーズのダイナミック VPN 機能では、IPsec のカプセル化モードがトランスポートモードの場合に限り、拠点 NAT/NAPT ルータの配下に配置することが可能です。

注意

CG-NAT を利用した環境では、各拠点の NAT 変換後の IP アドレスが同一になることがあり、その場合は、ダイナミック VPN 機能を利用することができません。

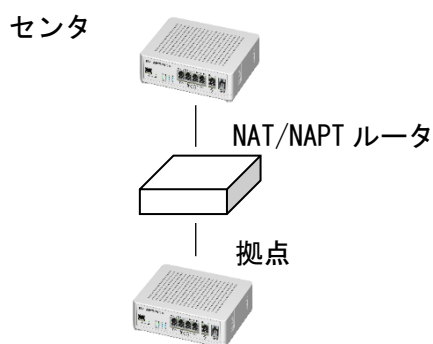
ダイナミック VPN 機能を利用する場合、拠点毎にユニークな IP アドレスである必要があります。

3.1. NAT/NAPT ルータ配下の拠点の NHRP 登録

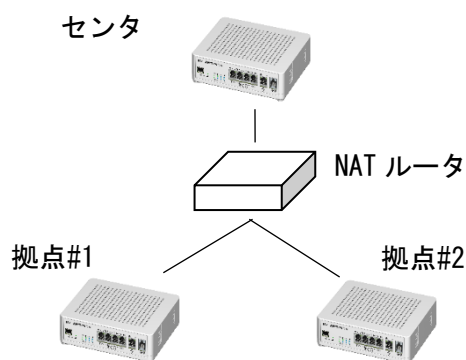
WA シリーズのダイナミック VPN 機能では、NAT/NAPT ルータ外部のセンタに、NAT/NAPT ルータの配下の拠点を NHRP 登録することが可能です。

ただし、1 つの NAPT ルータ配下に複数の拠点を配置する構成では、各拠点の NAPT 変換後の IP アドレスが同一となるため、1 拠点のみ NHRP 登録が可能です。

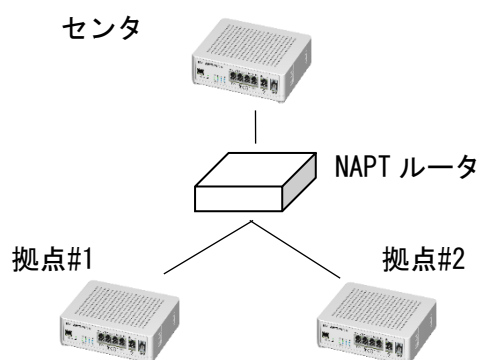
【拠点の NHRP 登録が可能】



【拠点#1/拠点#2 どちらも NHRP 登録が可能】



【拠点#1/拠点#2 のどちらかのみ NHRP 登録が可能】

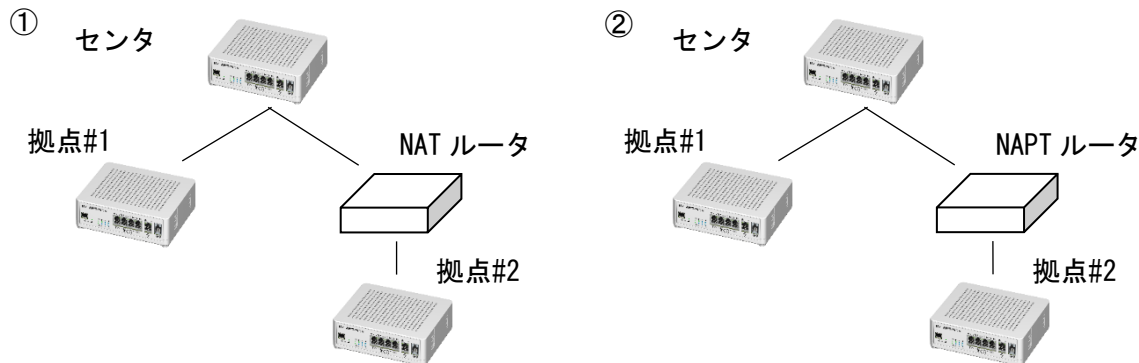


3.2. NAT/NAPT ルータ配下の拠点との間のトンネル構築

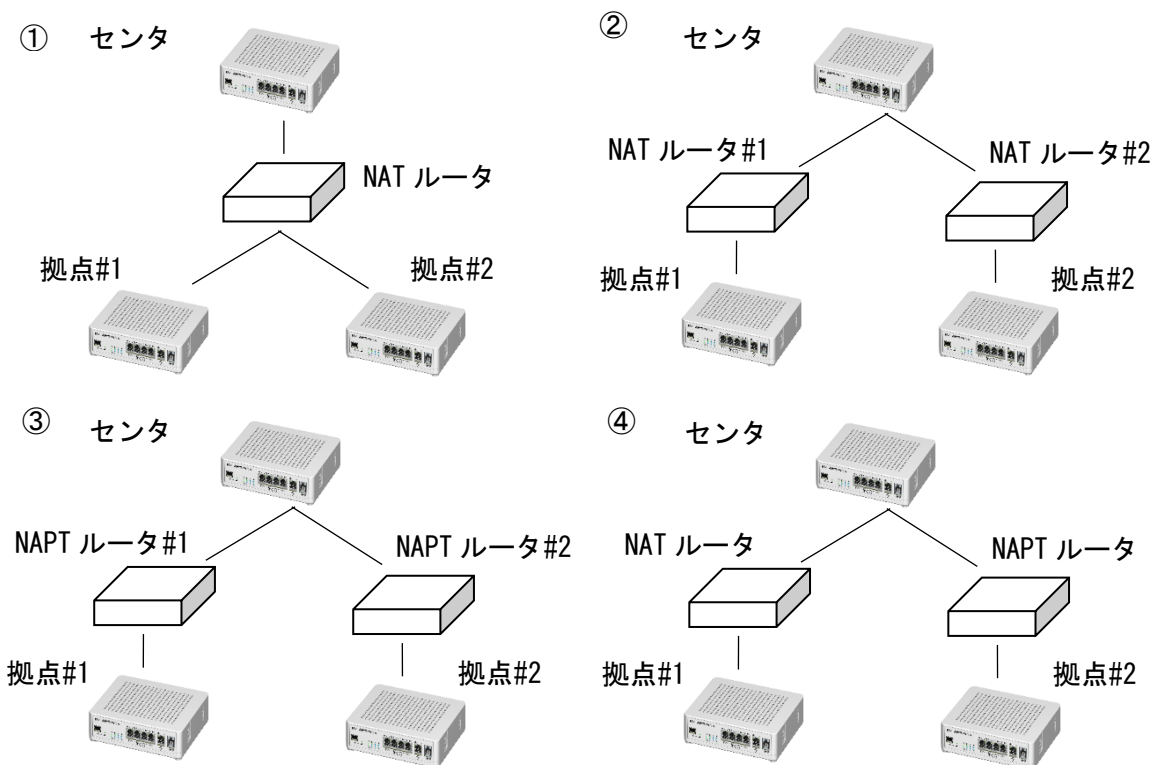
WA シリーズのダイナミック VPN 機能では、一部の構成を除き、NAT/NAPT ルータの配下の拠点との間の拠点間トンネルの構築が可能です。

デフォルト設定の場合に拠点間トンネルの構築が可能な構成と不可の構成は以下の通りです。拠点間トンネルの構築が不可の構成では、拠点間トンネルの構築を抑止してセンタ経由での通信となります。

【デフォルト設定で拠点間トンネルを構築可能な構成】



【デフォルト設定で拠点間トンネルの構築が不可能な構成】



上記の拠点間トンネルを構築可能な構成について、先に拠点#2→拠点#1 への方向の拠点間トンネルを生成済の場合に限り、拠点#1→拠点#2 への方向の拠点間トンネルの生成が可能となります。

拠点#2→拠点#1 への方向の拠点間トンネルが無い状態で、拠点#1→拠点#2 へパケット送信を行っても拠点間トンネルは生成されません。

上記の拠点間トンネルを構築可能な構成にて、拠点#1⇔拠点#2 間の双方向の通信で拠点間トンネルを生成する場合、拠点#2→拠点#1 への方向はすぐに拠点間トンネルを生成しますが、拠点#1→拠点#2 への方向は最初の 5 秒～3 分は拠点間トンネルを生成せずにセンタ経由での通信となります。5 秒～3 分後に拠点#1→拠点#2 への方向のパケット送信を行うと、双方向で拠点間での直接通信が可能となります。

3.2.1. デフォルト設定例

```
[センタ]
!
route-map dmvpn-map permit 10
  match interface GigaEthernet1.0
!
interface GigaEthernet0.0
  ip address 10.1.1.100/24
  ip tcp adjust-mss auto
  ikev2 binding ikev2-prof1
  ikev2 binding ikev2-prof2
  ip napt enable
  ip napt reserve esp
  ip napt reserve udp 500
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.0.254/24
  no shutdown
!
interface mGRE0.0
  gre source GigaEthernet0.0
  ip address 169.254.0.100/24
  ip tcp adjust-mss auto
  no shutdown
!
ip route default 10.1.1.254
ip route 169.254.0.0/24 mGRE0.0
!
router bgp 65534
  cluster-id 169.254.0.100
  address-family ipv4 unicast
    dmvpn next-hop-self
    redistribute connected route-map dmvpn-map
!
ikev2 profile ikev2-prof1
  peer any
!
ikev2 profile ikev2-prof2
  peer any
!
ikev2 default-profile
  ipsec-mode transport
  source-address GigaEthernet0.0
  dpd interval 10
  local-authentication psk plain dmvpn-password
  local-id address 169.254.0.100
!

[拠点]
!
route-map dmvpn-map permit 10
  match interface GigaEthernet1.0
!
interface GigaEthernet1.0
```



```

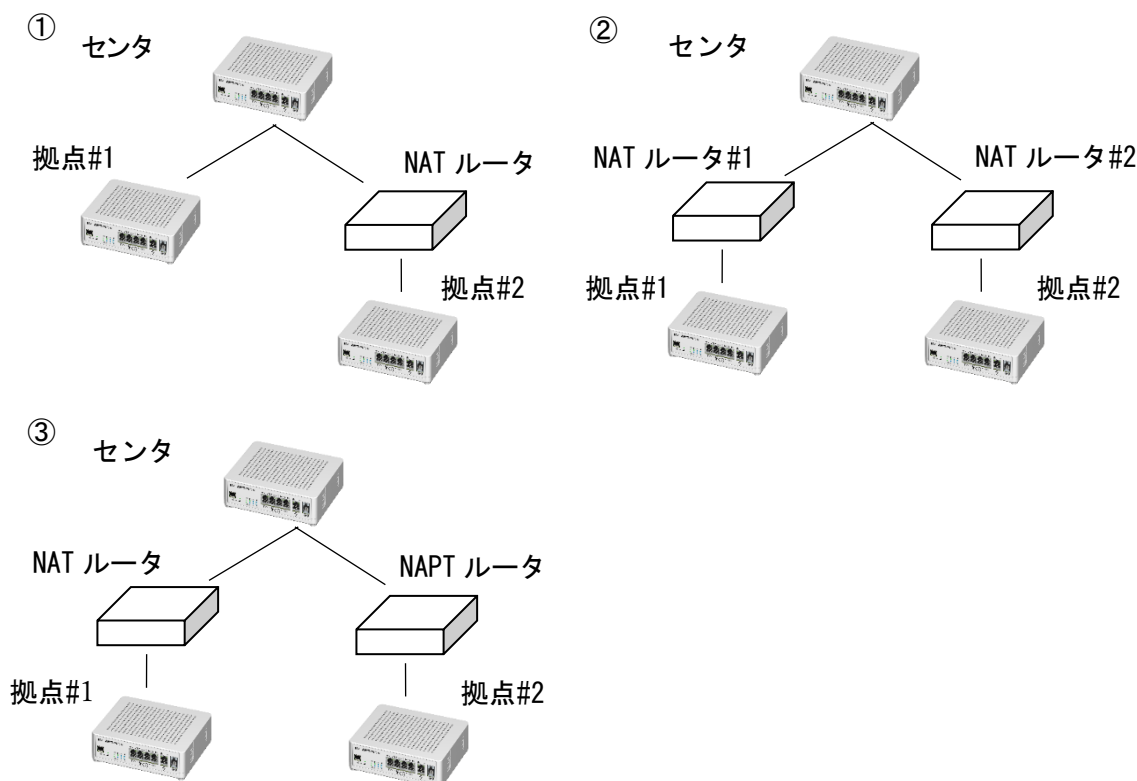
ip address 192.168.2.254/24
no shutdown
!
interface MobileEthernet0.0
ip address dhcp
ip tcp adjust-mss auto
ikev2 binding ikev2-prof1
ikev2 binding ikev2-prof2
ip napt enable
ip napt reserve esp
ip napt reserve udp 500
mobile id IP example.net
auto-connect
no shutdown
!
interface mGRE0.0
gre source MobileEthernet0.0
nhp nhs 169.254.0.100/24 nbma 10.1.1.100
ip address 169.254.0.2/24
ip tcp adjust-mss auto
no shutdown
!
ip route 169.254.0.0/24 mGRE0.0
ip route default dhcp MobileEthernet0.0
!
router bgp 65534
neighbor 169.254.0.100 remote-as 65534
address-family ipv4 unicast
redistribute connected route-map dmvpn-map
!
ikev2 profile ikev2-prof1
peer any
!
ikev2 profile ikev2-prof2
peer any
!
ikev2 default-profile
ipsec-mode transport
source-address MobileEthernet0.0
dpd interval 10
local-authentication psk plain dmvpn-password
local-id address 169.254.0.2
!
nhp local GigaEthernet1.0
!

```

デフォルト設定で拠点間トンネルの構築が不可の構成の内、一部の構成は、NAT ルータ配下の拠点に `nhrp enable-ack-with-nat` コマンドを設定することで、拠点間トンネルの構築が可能となります。

コマンド	内容
<code>nhrp enable-ack-with-nat</code>	NAT ルータ配下に配置された拠点が NHRP 解決要求に対して ACK 応答を返すための設定になります。 (mGRE インタフェースコンフィグモード)

【`nhrp enable-ack-with-nat` 設定で拠点間トンネルを構築が可能となる構成】



片側が NAT ルータ配下、片側が NAT/NAPT 無しの構成(上記の図の①)については、`nhrp enable-ack-with-nat` コマンドの設定を行わなくても双方向で拠点間の直接通信が可能です。NAT ルータ配下の拠点(拠点#2)に `nhrp enable-ack-with-nat` コマンドを設定すると、拠点#1⇄拠点#2間で双方向の通信で拠点間トンネルを生成する場合に、すぐに双方向で拠点間の直接通信が可能となります。

両側が NAT ルータ配下の構成(上記の図の②)について、両側の拠点(拠点#1 と 拠点#2)の双方に `nhrp enable-ack-with-nat` コマンドを設定することで、双方向で拠点間の直接通信が可能となります。どちらか一方の拠点に `nhrp enable-ack-with-nat` コマンドを設定した場合も双方向で拠点間の直接通信が可能となりますが、デフォルト設定で拠点間トンネルを構築可能な構成と同様の状態(※)となります。

片側が NAT ルータ配下、片側が NAPT ルータ配下の構成(上記の図の③)については、NAT ルータ配下の拠点(拠点#1)に `nhrp enable-ack-with-nat` コマンドを設定することで、双方向で拠点間の直接通信が可能となります。この場合、デフォルト設定で拠点間トンネルを構築可能な構成と同様の状態(※)となります。

なお、NAPT ルータ配下の拠点(拠点#2)に `nhrp enable-ack-with-nat` コマンドを設定した場合、拠点間の通信が不可となることがあります。

※拠点#1 のみ `nhrp enable-ack-with-nat` コマンドを設定した場合、拠点#2→拠点#1 への方の拠点間トンネルは無条件で生成可能となりますが、拠点#1→拠点#2 への方の拠点間トンネルは、先に拠点#2→拠点#1 への方の拠点間トンネルを生成済の場合に限り生成可能となります。(拠点#1⇄拠点#2 間の双方向の通信で拠点間トンネルを生成する場合の動作もデフォルト設定で拠点間トンネルを構築可能な構成と同様となります。)

3.3. 1 つの NAPT ルータ配下に複数の拠点を設置した場合の動作

ダイナミック VPN 機能では、1 つの NAPT ルータ配下に複数の拠点を配置する構成をサポートしていませんが、1 つの NAPT ルータ配下の複数の拠点から NHRP 登録を行った場合、以下のような動作となります。

➤ センタ⇄拠点間の通信

同じ NAPT ルータ配下の拠点の内、最後に NHRP 登録を行った拠点のみ、センタとの間の通信が可能です。

その他の拠点では、拠点から送信したパケットはセンタに到達可能ですが、センタから拠点への送信パケットは、全て最後に NHRP 登録を行った拠点に転送され、本来の宛先の拠点に到達することができません。

ユーザパケットだけではなく、NHRP のパケットや BGP4 のパケットも同様ですので、センタ⇄拠点間のトンネルの更新や、BGP4 でのルーティング情報の共有を行うことができません。

➤ 拠点間の通信

同じ NAPT ルータ配下の拠点間は、センタ経由での通信、直接通信のどちらも行うことができません。

NAT/NAPT 無しの拠点や他の NAT/NAPT ルータ配下の拠点との通信は、最後に NHRP 登録を行った拠点のみセンタ経由での通信が可能です。拠点間で直接通信を行うことはできません。

その他の拠点では、NAT/NAPT 無しの拠点や他の NAT/NAPT ルータ配下の拠点宛の送信パケットは宛先の拠点に到達可能ですが、NAT/NAPT 無しの拠点や他の NAT/NAPT ルータ配下の拠点からの送信パケットは、センタからの転送先が全て最後に NHRP 登録を行った拠点となり、本来の宛先の拠点に到達することができません。また、センタから本来の宛先の拠点に転送されないため、NHRP 解決による拠点間トンネルの構築を行うこともできません。

UNIVERGE WA シリーズ
ダイナミック VPN 設定ガイド

GVT-189668-001-00

2022 年 1 月 第 8.6 版

日本電気株式会社
NECプラットフォームズ株式会社
(禁無断複製)

©NEC Corporation 2009-2022
©NEC Platforms, Ltd. 2009-2022