NDA 対象文書

技術仕様書（接続 IF 仕様書）

WAN 側接続パラメータを説明した資料　および　試験項目表

NTTPC

2021/12/06

1 目次

2 用語

語句（ABC、あいうえお順）	説明
BGPIP	BGP neighbor の IP アドレス。
CPE	各拠点の ONU に結線するルータ。自営ネットワーク接続装置とも呼ぶ。本書仕様を満たす接続を実現する装置。
CPE ホスト名	DNS サーバに登録される CPE FQDN のホスト名のこと。
DDNS	Dynamic DNS。動的に割り当てられる NTT 東日本・NTT 西日本 NGN 区間の IPv6 アドレスと、その FQDN の対応を、動的に登録・管理する仕組み
DDNS サーバ	CPE からのアドレス通知を受ける DynamicDNS サーバ。正しい通知を受けて更新がある場合 DNS サーバを更新する。東日本と西日本にそれぞれ 1 つ用意される。
DNS サーバ	本サービス用に用意される DNS サーバ。GW と CPE の AAAA レコードと、CPE の PTR レコードを持つ。東日本と西日本にそれぞれ 1 つ用意される。
FQDN	本サービス接続に使われる Fully Qualified Domain Name
GW	NTTPC ネットワーク網に存在し、CPE からの IPv6 IPSEC および IPv4 BGP 接続を終端する装置。Main/Back で 2 つ提供される（GW-1,GW-2）。GW-1,GW-2 の 2 つの間では東西分散はされない。
HGW	Home Gateway。NTT 東日本・NTT 西日本が設置するひかり電話ルータ。
NGN	本書では NTT 東日本・NTT 西日本「フレッツ 光ネクスト」網のこと
OGW	Office Gateway。ひかり電話 A(エース)利用時に NTT 東日本・NTT 西日本が設置するひかり電話ルータ。
TEP	Tunnel End Point。CPE からの IPSEC 接続の GW 側終端点アドレスまたは FQDN。IPSEC SA を確立する peer のこと。 GW-1 では TEP1、GW-2 では TEP2 とも表記される。
VNE	Virtual Network Enabler。IPoE 接続事業者。2018 年時点ではインターネットマルチフィード株式会社（以降 IMF）となる。
拠点通番	当社が拠点に対してユニークに付与する数値。CPE ホスト名とこの通番が一致した場合、DDNS サーバは CPE からのアドレス通知を受領する。
ステージング環境	当社が提供する CPE 接続性試験環境。NTT 西日本区域からは利用できない。
ステージング GW	ステージング環境に用意する GW。
東西分散	CPE からの IPSEC と BGP を終端する GW を NTT 東日本区域と NTT 西日本区域に分けること。

保守番号	拠点毎に付与する NTTPC 管理番号。設備側設定は本保守番号単位にユニークとなる。NTT 東日本・NTT 西日本を跨がない場所移転時でも変更される場合がある。
パートナー事業者	「IPoE インターネットサービス CPE コラボレーション」を契約した SIer、装置ベンダー、通信事業者等のこと。

3 本書について

WAN 側接続パラメータを説明した資料　および　試験項目表となります。

サービス提供内容の詳細は利用規約または卸契約書、サービス仕様書に記載します。

3.1 接続について当社の実施範囲

利用規約または卸契約書、サービス仕様書も参照してください。

・本サービスにおいて当社は以下を行いません。

1. 顧客 NW 設計・管理維持
2. CPE の購入・配送・設定・設置・開通試験・VersionUP・設定変更・監視・切り分け・交換・回収・廃棄・物品管理等の現地物品に関わるすべての業務
3. NTT フレッツ回線の申し込み・現調・現地作業日程調整・立ち会い・HGW 及び OGW の設置設定・廃止等の NTT 回線に関わるすべての業務
4. ユーザ通信試験の立ち会い

・当社は以下を行います。

1. GW の動作正常性確認
2. ステージング GW に接続された当社が管理する CPE1 台の IPv4 over IPv6 IPSEC と IPv4 BGP 動作正常性確認。

3.2 パートナー事業者の実施内容

利用規約または卸契約書、サービス仕様書も参照してください。

ステージング環境において、論理接続図の通り IPSEC および BGP 接続がそれぞれ確立していることを確認する。

以下項目を実施することにより確認できます。

1. IPSEC Peer(FQDN または IPv4 アドレス)への Ping 疎通応答があること
   ※ *応答がない場合は WAN 接続または設定が未完了。*
2. （CPE の Loopback アドレスを送信元とした）BGPIP への Ping 疎通応答があること
   ※ *論理接続図の紫色の線を通る Ping。応答がない場合は IPSEC が未確立。*
3. BGP neighbor 確立の確認と、経路送受信の確認
4. LAN 内からの Ping 疎通確認
5. Ping 疎通確認の長期(24 時間)安定化試験

3.2.1 禁止事項

ステージング環境または実ユーザ環境において以下を実施することはできません。

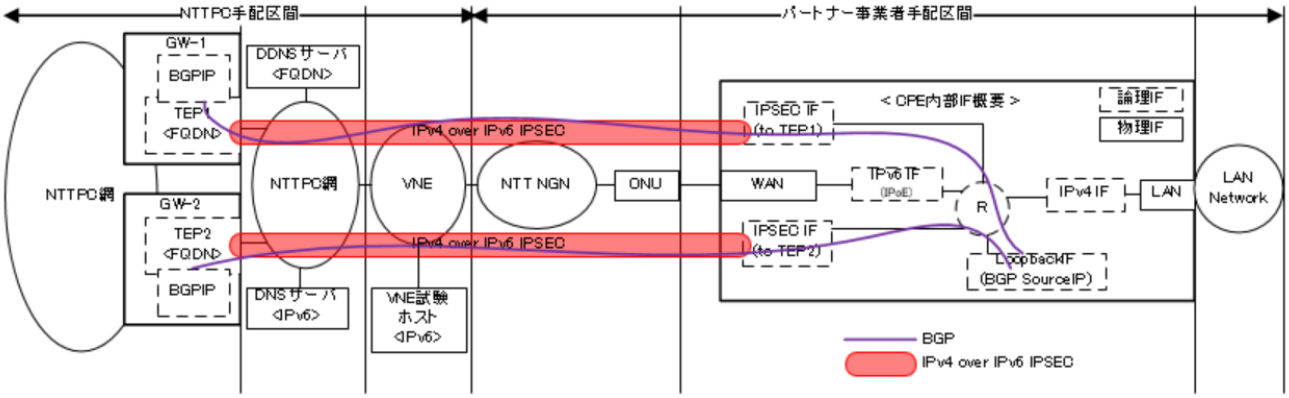
1. 測定器等を用いた負荷試験
2. GW2 つのうち、片側の IPSEC や BGP を意図的に確立させない行為の継続。
3. DNS サーバ、DDNS サーバの本サービス用途以外での利用
4. 当社または VNE 設備への IF 仕様書外のパケット、BGP メッセージの送信
5. VNE 試験ホスト、TEP、BGP neighbor、DNS サーバ、DDNS サーバ等当社設備への継続的な監視パケットの送信
6. 同一の IPv6 アドレスにて、複数の FQDN を DDNS 通知すること（※IPSEC 確立に DNS の正引きおよび逆引きレコードを利用するため）
7. 上記以外に当社が異常と検知した行為

4　IF 仕様および設定例

IPv4 over IPv6 IPSEC、DDNS、BGP についての IF 仕様および設定例

4.1　接続論理図

GW から CPE の内部 IF までの論理接続図と論理接続図内の各パラメータ。



種別	西日本	東日本
DDNS サーバ FQDN	＜削除＞	＜削除＞
DNS サーバ IPv6 アドレス	＜削除＞	＜削除＞
TEP1, TEP2	＜削除＞	
BGPIP	＜削除＞	
CPE FQDN	＜削除＞	＜削除＞
CPE WAN 側 IPv6 アドレス	＜削除＞	＜削除＞
CPE LAN 側 IP と NW アドレス	＜削除＞	
CPE Loopback アドレス	＜削除＞	

4.2　技術要素

本書規定の接続を実現するため、以下 4 つの設定または実装が必要です。

設定	詳細説明章	ページ
WAN 側 IF の IPv6 設定	5.1 IPv6 について	9
DDNS 設定	5.2 IPv6 区間 DNS および DDNS	11
IPv4 over IPv6 IPSEC 設定	5.3 IPSEC 機能	12
BGP 設定	5.4 BGP-4	14

4.3　接続設定例

参考資料として別冊を参照してください。

5 各技術要素

5.1 IPv6 について

VNE および NTT 東日本・NTT 西日本地域区間では IPv6 通信となります。

5.1.1 付与されるアドレス

CPE には以下の VNE の Prefix の中から、/64 の Prefix が付与されます。変更される場合があります。

■NTT 東日本地域

	完全表記	省略表記
Prefix	＜削除＞	＜削除＞
Network start	＜削除＞	＜削除＞
Network end	＜削除＞	＜削除＞
Netmask	＜削除＞	＜削除＞

■NTT 西日本地域

Prefix	＜削除＞	＜削除＞
Network start	＜削除＞	＜削除＞
Network end	＜削除＞	＜削除＞
Netmask	＜削除＞	＜削除＞

CPE は NDP に基づき、ICMPv6 Type=134 Router Advertisement(以降、RA)メッセージが WAN 側 IF に送信されることを期待するよう設定します。

RA メッセージの Prefix Information から WAN 側 IPv6 アドレスの Prefix 部分をセットし、Default Gateway も RA メッセージの送信元に自動的にセットするよう設定します。

【参考】InterfaceID は CPE 機種により固定設定も可能な場合があります。故障交換時でも IPv6 アドレスを変えないことができます。

5.1.2フレッツ・光ネクスト IPv6 仕様

NGN 区間については NTT 東の技術参考資料 「IP 通信網サービスのインタフェース」第三分冊 または、NTT 西の技術参考資料「IP 通信網サービス（フレッツシリーズ＜光ネクスト、光ライト、光 WiFi アクセス編＞）」の「フレッツ 光ネクスト」の箇所を参照してください。
https://www.ntt-east.co.jp/gisanshi/
https://www.ntt-west.co.jp/info/gisanshi/

「通信機器は Preferred Lifetime が 0 でないアドレスを所持している場合は、Preferred Lifetime が 0 ではないアドレスの利用を推奨します。」とあるため、アドレス選択基準を Lifetime が最長の物を利用するようにして、推奨動作を実現してください。

IPv6 Prefix は NTT 東日本・NTT 西日本の都合により変わる可能性があります。WAN 側アドレスが PPPoE のように IP1 固定ではありません。

5.1.3 フレッツ・v6 オプション

本サービスはフレッツ・v6 オプション契約がないと利用出来ません。具体的には本サービスで採用する VNE 事業者の IPv6 プレフィックスが付与できません。
http://flets.com/v6option/
東日本はデフォルト有効となっていますが、平成 24 年 5 月以前の回線では有効になっていません。
http://www.ntt-east.co.jp/release/detail/20120528_01.html
西日本はデフォルト有効ではありません。工事費は無料となっています。
http://www.ntt-west.co.jp/news/1205/120528a.html

5.1.4 その他注意点

IPv6 区間のフィルタはパートナー事業者にて検討ください。NTTPC ネットワークからの到達性の担保を行うため、2001:2c0:7::/48 からのアクセスは許容してください。

ひかり電話を利用する場合、NTT 東日本・NTT 西日本より貸与される Home Gateway または Office Gateway が ONU との間に存在するようになります。HGW および OGW は ONU と一体型である場合もあります。

HGW や OGW を利用する場合には、HGW や OGW の設定が必要になる場合があります。
「IPv6 ファイアウォール機能」にて、「無効に変更」または「送信元 2001:2c0:7::/48 の許可」が必要です。
【参考】以下 URL 等を参考にしてください。
http://ybb.softbank.jp/support/connect/hikari/router/ipv6packet.php

5.2 IPv6 区間 DNS および DDNS

本サービスでは DDNS の仕組みを利用して、CPE の IPv6 アドレスを FQDN で疎通可能としています。DDNS サーバアドレスは FQDN で提供されます。DDNS サーバの FQDN を解決するため DNS サーバを提供します。

GW は CPE の DNS レコード情報を利用して IPSEC 接続を確立しようとします。DDNS による CPE の FQDN 登録ができていない場合、IPSEC 接続が確立しません。

DDNS サーバと DNS サーバは東西分散も行っています。CPE から参照する先の DNS サーバは NTT 東日本・NTT 西日本で分かれます。

種別	西日本	東日本
TEP1,TEP2	＜削除＞	
DDNS FQDN	＜削除＞	＜削除＞
DNS サーバ IPv6 アドレス	＜削除＞	＜削除＞
CPE FQDN	＜削除＞	＜削除＞

DNS サーバへの DNS クエリーが高頻度であった場合、その接続元をフィルタする場合があります。

DDNS サーバへのアドレス通知が高頻度であった場合、その接続元をフィルタする場合があります。

5.2.1 DDNS サーバへ通知する構文

CPE は自動的に WAN 側 NGN IPoE 区間の IPv6 アドレスを DDNS サーバに通知する仕組みを内蔵する必要があります。

DDNS サーバに通知する構文は以下の通り

プロトコル	HTTP GET
ポート	＜削除＞
構文	/gw_config.cgi?cmd=add&host=<CPE ホスト名>&cpe_env=<シリアル>_kinfo=<拠点通番>&tep1=<TEP1>&tep2=<TEP2> ※<>は可変値です。シリアルは必須ではありませんが、空白にはできません。
認証	BASIC 認証を行います。ID/PW は別途提示されます。
応答コード	200：正常（登録完了） 401：構文エラー 403：BASIC 認証エラー
Full Request URI 例	以下、東日本の場合。<>は可変値です。 ＜削除＞

起動時、およびアドレス変更時以外では 24 時間以上の周期でアドレス通知を行うことを許容します。

BASIC 認証、構文および構文内の拠点通番、TEP1、TEP2 がすべて正しくないと、200 応答（登録完了）とはなりません。

5.3 IPSEC 機能

CPE は各 GW の TEP と FQDN 設定で IKE 接続する必要があります。将来的に IPv6 アドレスが変更される場合があるため、IPv6 アドレス設定の IKE 設定の場合の接続性は保証しません。

5.3.1MTU・フラグメント処理

不要なフラグメント処理が発生しないように、以降記載する IPSEC パラメータを参考に IPSECIF に MTU を設定してください。IPv4 TCP MSS 値を IPSECIF 側の MTU に合わせては調整することを推奨します。
上位送出側回線種別とそのパートナー事業者用意 CPE 設定次第で、GW からは IPv6 Fragment パケットが送出される場合があります。

CPE 側から IPoE 区間で IPv6 Fragment パケットを送出した場合、一部のパケットが GW に到達しない場合があります。

5.3.2 GW との IPSEC パラメータ

SA の管理方式	Continuous-channel SA 型を推奨
利用する SA	最後に作成された最新の SA を利用すること
フラグメント処理	Pre-Fragment を推奨
Anti-Replay	OFF

■Phase-1

IKE Version	1
Exchange Mode	Main Mode
ID Type	ID_IPV6_ADDR
Encryption Algorithm	AES256-CBC
Hash Algorithm	HMAC-SHA-1-96
Authentication Method	Preshare（保守番号毎に 30 文字で用意される）
Diffe-Hellman 方式	Group14(2048bit MODP)
SA life type	second
SA life duration	14400
Soft Rekey	life duration - 540sec 以上 3600sec 以下とすること

	Initiator、Responder に関わらず、また、Phase-1 単体でも Rekey すること
IKE keepalive	RFC3706。間隔は 10sec 以上。通信中は抑制することを推奨。GW は CPE からの keepalive に応答はするが、keepalive 送付はしない。

■Phase-2

Exchange Mode	Quick Mode
ID Type	IP_IPV4_SUBNET
Local ID	0.0.0.0/0
Remote ID	0.0.0.0/0
Transform	ESP_AES256-CBC
Encapsulation Mode	Tunnel
Hash Algorithm	HMAC-SHA-1-96
PFS	Enable
Differs-Hellman 方式	Group14(2048bit MODP)
SA life type	second
SA life duration	7200
Anti-Reply Detect	off
Soft Rekey	life duration - 540sec 以上 1800sec 以下とすること

5.3.3 Notify Messages

Status Types では INITIAL-CONTACT をサポートしています。
GW は INITIAL-CONTACT を受信した場合は、自分の持っている全ての IPSEC SA を削除します。

5.3.4 その他 IPSEC 注意点

全拠点一斉に IKE 再接続しても、確立までには数分かかる場合があります。
最終的に確立した最新の SA を利用しますが、IKE 折衝が輻輳する状態では、IPSEC 通信は確立しても通信できません。
Rekey の IKE 衝突しないために、CPE 側で Soft Rekey 値を変更して CPE から Rekey するよう設定してください。

5.4 BGP-4

確立した Main/Back2 つの IPv6 IPSEC トンネルの中で、それぞれ IPv4 BGP 接続を行います。

5.4.1 サポートしている RFC

RFC1771 A Border Gateway Protocol 4 (BGP4)
RFC2918 Route Refresh Capability for BGP-4

5.4.2 BGP-4 パラメータ

AS 番号	
CPE 側ローカル AS 番号	65100
GW-1 (Main 側) AS 番号	65001
GW-2 (Back 側) AS 番号	65002
CPE パラメータ	
配信経路・属性	・当社が払い出した GlobalIP 経路 ・Loopback アドレス経路を配信しないこと ・GW-1 から受信した経路及び GW-2 から受信した経路を GW-1 と GW-2 に配信しないこと ・GW-1 と GW-2 に同一の経路・属性を配信すること ・AS_PATH 属性は 65100 1 つのみにすること
Router ID	Loopback アドレス
BGP SourceIP	Loopback アドレス
Timer 値	Keepalive : 10 秒以上 Hold Timer : 30 秒以上 TCP 再接続 Timer : 10 秒以上
Capability	IPv4 Unicast : 必須 Route-refresh : 推奨
GW パラメータ	
GW-1 (Main 側) 配信経路	0.0.0.0/0
GW-1 (Main 側) 配信 Path 属性	・AS_PATH 属性を利用して Main/Back 経路をコントールします。 ・装置仕様により以下の 2 種類のうち、いずれかの AS_PATH の経路を配信します。 ・65001 のみ ・GW の保持する 0.0.0.0/0 の AS_PATH に 65001 を 1 個 Prepend したもの ・設備都合により上記の AS_PATH からさらに Prepend/Remove する場合があります。
GW-1 (Main 側) 受信経路	当社が払い出した GlobalIP 経路

GW-2（Back 側）配信経路	0.0.0.0/0
GW-2（Back 側）配信 Path 属性	・AS_PATH 属性を利用して Main/Back 経路をコントールします。 ・装置仕様により以下の 2 種類のうち、いずれかの AS_PATH の経路を配信します。 ・65002 65002 ・GW の保持する 0.0.0.0/0 の AS_PATH に 65002 を 2 個 Prepend したもの ・設備都合により上記の AS_PATH からさらに Prepend/Remove する場合があります。
GW-2（Back 側）受信経路	当社が払い出した GlobalIP 経路

5.4.3その他 BGP 注意点

CPE 側で Cisco 社独自の WEIGHT 属性や LOCAL_PREF 属性を用いて GW-1 か GW-2 かの PATH 選択を変えないでください。PATH 選択は GW 側の AS PATH 属性で決定するように設定してください。

GW-1 と GW-2 で配信経路を分けて、PATH 冗長を実現する構成は組めません。

全拠点一斉に BGP 再接続した場合、確立までに数分かかる場合があります。

6 履歴

日付	内容
2019/02/07	initial beta release
2019/09/03	用語を ABC 順に並び替え。表記方法の一部修正 3「本サービスの概要」を「本書について」という名前に変更して説明を追加 その他修正
2021/06/23	試験表を削除 SIV コラボの記載を削除
2021/12/06	用語 Update。パートナー事業者の実施内容の記載を更新。接続論理図更新。その他文言修正。