TTC仕様書
Technical Specification

TS-1017

NGN 上の SIP-VPN 通信方式に関するインタフェース技術仕様

Technical Specification on SIP VPN connection over NGN

第 1.0 版

2011 年 11 月 16 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　次

<参考>

1. 国際勧告等の関連

本標準技術仕様に関する国際勧告はない。

2. 改版の履歴

版数	制定日	改版内容
第 1.0 版	2011 年 11 月 16 日	制定

3. 参照文書

3.1. 規準参照文書

[1] "NGN NNI シグナリングプロファイル プロトコルセット 1（NGN NNI Signalling Profile）", TTC 標準 JT-Q3401 第 2.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

[2] "NGN UNI シグナリングプロファイル プロトコルセット 1（NGN UNI Signalling Profile）", TTC 標準 JT-Q3402 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

[3] "NGN における SDP メディアネゴシエーションに関するインタフェース技術レポート", TTC 技術レポート TR-1020 第 1.0 版, 2009 年 5 月

[4] "NAT 越えでの IKE ネゴシエーション（Negotiation of NAT-Traversal in the IKE）", TTC 標準 JF-IETF-RFC3947 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[5] "IPsec ESP パケットの UDP カプセル化（UDP Encapsulation of IPsec ESP Packets）", TTC 標準 JF-IETF-RFC3948 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[6] "IP のカプセル化セキュリティペイロード（IP Encapsulating Security Payload (ESP)）", TTC 標準 JF-IETF-RFC4303 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[7] "ユーザ データグラム プロトコル（UDP）", TTC 標準 JF-IETF-RFC768 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[8] "インターネット プロトコル（IP）", TTC 標準 JF-IETF-RFC791 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[9] "トランスミッション コントロール プロトコル（TCP）", TTC 標準 JF-IETF-RFC793 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[10] "インターネット プロトコル バージョン 6（IPv6）仕様", TTC 標準 JF-IETF-RFC2460 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[11] "STUN – UDP の簡易な NAT トラバーサル方式（STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", TTC 標準 JF-IETF-RFC3489 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[12] "インターネット鍵交換（IKEv2）プロトコル（Internet Key Exchange Protocol Version 2 (IKEv2)）", TTC 標準 JF-IETF-RFC5996 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[13] "セッション記述プロトコル（SDP）上での TLS を用いたメディアトランスポート（Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)）", TTC 標準 JF-IETF-RFC4572 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[14] "ICE: オファー・アンサープロトコルにおける NAT トラバーサルのためのプロトコル（Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", TTC 標準 JF-IETF-RFC5245 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

[15] "セッション記述プロトコル（SDP）における IKE のメディア記述（Media Description for IKE in the Session Description Protocol (SDP)）", TTC 標準 JF-IETF-RFC6193 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2011 年 11 月

4. 工業所有権

TTC の「工業所有権等の実施の権利に係る確認書」の提出状況は、TTC ホームページで公開されている。

5. 技術仕様策定部門

信号制御専門委員会

1　概要

1.1　本仕様の適用範囲

本仕様は、JT-Q3402[2]に規定されるUNI 、及びJT-Q3401[1]に規定されるNNIにおいて、本仕様で規定されるSIP-VPN通信方式を提供するNGNのインタフェース、及びSIP-VPN端末に適用される。

1.2　本仕様の目的と規定

本仕様は、SIP/SDP を用いて NGN 上に IPsec パスを確立する手順に関して、網及び端末が従うべき動作について規定するものである。なお、当該手順を用いた通信について、本仕様では「SIP-VPN 通信」と呼び、SIP-VPN 通信を行う端末を「SIP-VPN 端末」と呼ぶ。

網及び端末に関して実装条件として選択可能である項目は、本仕様中に括弧（【 】）にて示し、付録Iに表形式にて記載する。

1.3　本仕様の規定内容

本仕様は、1.1節の適用範囲において、SIP-VPN通信を適切に行うために、SIP-VPN端末とNGNが満たすべき要求条件、及び接続インタフェース条件を規定する。

本仕様の構成は以下の通りである。

本文	SIP-VPN 通信手順
付属資料 A	SIP-VPN 通信に網及び端末が対応する場合における、JT-Q3402（UNI）と JT-Q3401（NNI）に対するオプション項目選択
付録 I	SIP-VPN 通信に関するオプション項目表
付録 II	SIP-VPN 通信のシーケンスとメッセージ例

2　用語

本仕様に関する用語は、JT-Q3401[1]及びJT-Q3402[2]に準拠する。

SIP-VPN に関連する用語として、以下に示す略語を使用する。

CP	Configuration Payload
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESP	IP Encapsulating Security Payload
IKE	Internet Key Exchange
IPsec	Security Architecture for the Internet Protocol
PFS	Perfect Forward Security
SA	Security Association
VPN	Virtual Private Network

また、SIP-VPN の動作を示すため、以下に示す用語を定義し、本仕様中にて使用する。

アウター	IPsec トンネルの外側のこと。
インナー	IPsec トンネルの内側のこと。
IKE イニシエータ	IPsecパス確立に際して、IKEのinitiator[11]となる側の端末のこと。
IKE レスポンダ	IPsecパス確立に際して、IKEのresponder[11]となる側の端末のこと。

VPN クライアント	SIP-VPN 端末のうち、VPN サーバが提供するネットワーク空間に参加する側の端末のこと。IKE のネゴシエーション時には、IKE イニシエータとなる。
VPN サーバ	SIP-VPN 端末のうち、VPN のネットワーク空間を提供する側の端末のこと。IKE のネゴシエーション時には、IKE レスポンダとなる。
逆方向接続	VPN サーバ側が発端末となる接続形式のこと。
順方向接続	VPN クライアント側が発端末となる接続形式のこと。
着端末	SIP ダイアログの確立に際して、Initial INVITE を受信する側の端末のこと。
発端末	SIP ダイアログの確立に際して、Initial INVITE を送信する側の端末のこと。

3　SIP-VPNの概要

本章では、SIP-VPN のアーキテクチャとプロトコル構成を示す。

3.1　端末の役割

SIP-VPN 通信では、NGN に接続される 2 つの端末間で SIP を用いてセッション確立を行い、両端末間で IPsec を用いた VPN を確立する。片側の端末が VPN のネットワーク空間を提供し、もう一方の端末が相手方から提供されたネットワーク空間に参加する。このため、端末の役割や動作は非対称である。

本仕様では、SIP-VPN 端末のうち、VPN のネットワーク空間を提供する側の端末を「VPN サーバ」、VPN サーバのネットワーク空間に参加する側の端末を「VPN クライアント」と呼ぶこととする。

3.2　通信形態

SIP-VPN 端末は、NGN に UNI を介して接続される。SIP-VPN 端末間で、SIP/SDP を用いた呼制御を行い、IPsec（IKE、ESP）のペイロードを UDP でカプセル化（UDP encapsulation）し、メディアとして送受信することによって、両端末間で VPN を確立するものである。

図 3-1に、SIP-VPN 通信の形態を示す。

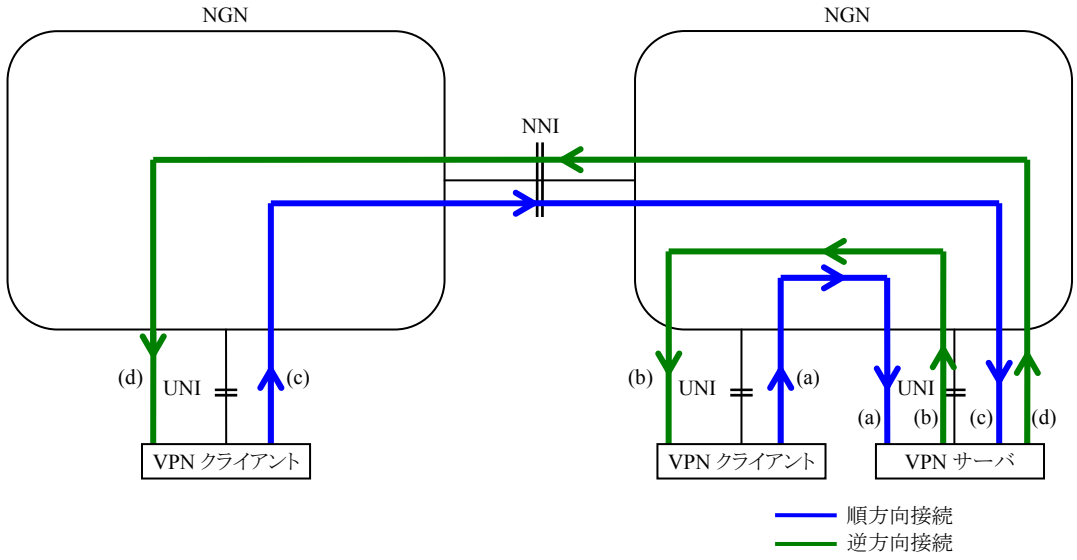


図3-1／TS-1017　本仕様で規定する SIP-VPN 通信の形態

SIP-VPN 端末間の接続は、単一の NGN のみを経由して接続されても（図 3-1の a 及び b の接続）、NNI を通り複数の NGN を経由して接続されても（同 c 及び d の接続）よい。

また、呼接続については、VPN クライアントから発信しても（図 3-1の a 及び c の接続）、VPN サーバ側から発信しても（図 3-1の b 及び d の接続）よい。本仕様では、VPN クライアント側から発信する形態の接続を「順方向接続」、VPN サーバ側から発信する形態の接続を「逆方向接続」と呼ぶこととする。逆方向接続の用途としては、課金上の都合によるコールバック接続や、サーバ側からのプッシュ配信などが想定される。

本仕様では、上記 4 種類の接続形態（図 3-1の a、b、c 及び d）の接続を規定対象とする。なお、SIP-VPN 端末は、順方向接続と逆方向接続の少なくともいずれかに対応する。【付表 I-C-1 項番 1～2、付表 I-S-

1 項番 1～2】

3.3　プロトコル構成

SIP-VPN通信を行う場合の、インタフェース規定点（UNI/NNI）におけるプロトコルの一覧を、OSI参照モデルに準拠する形にて 表 3-1に示す。本仕様中で特に言及がない項目に関しては、表 3-1に示す各種勧告類の規定に従う。

なお、OSI 参照モデルにおける第 2 層（データリンク層）と第 1 層（物理層）については、本仕様の規定範囲外である。

表 3-1／TS-1017　プロトコル構成

レイヤ		使用プロトコル		
		セッション制御	メディア	
			IPsec 接続制御	IPsec 接続
7	アプリケーション	SIP/SDP： TTC JT-Q3402[2] TTC JT-Q3401[1] TTC TR-1020[3] TTC JF-IETF-RFC6193[15] TTC JF-IETF-RFC4572[13]	IKE： TTC JF-IETF-RFC5996[12] TTC JF-IETF-RFC3947[4]	ESP: TTC JF-IETF-RFC4303[6] TTC JF-IETF-RFC3948[5]
6	プレゼンテーション			
5	セッション			
4	トランスポート	UDP： TTC JF-IETF-RFC768[7] TCP： TTC JF-IETF-RFC793[9]	UDP： TTC JF-IETF-RFC768[7]	
3	ネットワーク	IPv4： RFC791[8] IPv6： RFC2460[10]		

3.3.1　ネットワーク層プロトコル

SIP-VPN 端末は、アウター、インナー、それぞれ少なくとも IPv4 と IPv6 のいずれかのネットワーク層プロトコルに対応する。【付表 I-C-3 項番 1～4、付表 I-S-3 項番 1～4】

3.3.2　SIP/SDP

SIP-VPN通信のセッション制御に用いるSIP/SDPの仕様に関しては、UNIはJT-Q3402 に、NNIはJT-Q3401に、メディアのネゴシエーション条件はTR-1020 に従い、SIP-VPNに固有の条件はRFC6193[15]に従う。また、SIP-VPNを利用する場合におけるJT-Q3402 及びJT-Q3401 のオプション項目の選択条件を、付属資料Aに示す。

3.3.3　IKE

SIP-VPN通信のIPsec接続制御には、IKEv2[11][4]を使用する。

3.3.4　ESP

SIP-VPN通信のIPsec接続には、ESP[6]をUDPカプセル化 [5]した信号を使用し、トンネルモード（tunnel mode）の仕様に従う。

3.4　認証

SIP-VPN 通信では、IKE を用いた IPsec 確立手順において、VPN サーバが VPN クライアントの認証を行い、不正な VPN 接続を防ぐ。本仕様では、この認証手順として、パスワード認証と共有鍵認証の手順を定める。端末は少なくともいずれかの認証手順に対応する。【付表 I-C-2 項番 1～2、付表 I-S-2 項番 1～2】

3.4.1　パスワード認証

IKE の EAP-MD5 認証を用いて、VPN クライアントが VPN サーバにユーザ名とパスワードを通知し、VPN サーバ側ではこれらを用いて IKE のイニシエータ認証を行う手順である。

VPN サーバ側は自身の証明書として、自己署名証明書を用いる。

3.4.2　共有鍵認証

VPN クライアント、VPN サーバ間で共通の事前共有鍵（PSK）を用いて認証を行う手順である。

VPN サーバ側は、受信した SDP オファーに設定された PSK を用いて IKE イニシエータ認証を行う。

4　通信手順

SIP-VPN通信の手順はRFC6193[15]に従うが、本章では接続、切断、キープアライブに関する手順の詳細条件を示す。

4.1　接続

SIP/SDPを用いてVPN端末間でSIPセッションを確立し、IKE確立（SA確立）・認証・端末コンフィギュレーションを行った後、IPsecによる通信を開始する。ICE[14]及びSTUN[11]は使用しない。

4.1.1　接続時の信号条件（SIP）

順方向接続を行う場合は VPN クライアントが発端末、逆方向接続を行う場合は VPN サーバが発端末となり、Initial INVITE リクエストを送信する。

4.1.2　接続時の信号条件（SDP）

SIP-VPN 端末は、オファー・アンサーとも、SDP には media description を 1 つのみ設定する。また、受信した SDP に media description が 2 つ以上設定されている場合は、エラー応答（488 Not Acceptable Here）を返すこととし、仮に一部の media description が SIP-VPN 通信で使用されるものと同様の記載内容であっても、接続を受け入れてはならない。

本節及び従属節に、media description 内の詳細な設定条件を示す。

4.1.2.1　ペイロード形式

RFC6193[15]に規定される 2 種類のペイロードのうち、ESPパケットをUDPカプセリングして送受信を行うペイロードである、application/ike-esp-udpencapを使用する（fmtにはike-esp-udpencapと記載する）。ESPパケットの直接送受信を行うapplication/ike-espは使用しない。

4.1.2.2　ポート番号

SIP-VPN 端末は、オファー・アンサーの SDP とも、m=行の port には IKE と、UDP カプセル化 ESP で待ち受けるポート番号（典型的には 4500）を設定する。

ただし、SIP-VPN端末は、網から受信するオファー・アンサーのSDPに、4500 以外のポート番号が設定された場合にもIPsecによる通信が行えなければならない。このとき、SIP-VPN端末はRFC6193[15]の 5.4 節に従い、受信したSDPに記載されるポート番号に対してUDPカプセル化IKEとUDPカプセル化ESPの通信を行う。

4.1.2.3　b=AS行

SIP-VPN 端末は、SIP-VPN で使用する帯域を網に対して明示的に指定する場合、b=AS 行を使用する。このとき、b=AS 行で指定する値は、アウターの帯域であり、かつ IP ヘッダや UDP ヘッダを含むレイヤ 3 の帯域であることに留意する。

4.1.2.4　a=ike-setup行

RFC6193[15]に従い、a=ike-setup行には、IKEイニシエータとなる予定のSIP-VPN端末がactiveを、IKEレス

ポンダとなる予定のSIP-VPN端末がpassiveを指定する。従って、発端末か着端末かに関わらず、VPNクライアントがactiveを、VPNサーバがpassiveを指定する。

なお、VPN クライアントとしての能力しか具備しない SIP-VPN 端末が a=ike-setup 行に active を指定された SDP を持つ Initial INVITE リクエストを受信した場合、逆に VPN サーバとしての能力しか具備しない SIP-VPN 端末が a=ike-setup 行に passive を指定された SDP を持つ Initial INVITE リクエストを受信した場合は、SDP の内容に従った通信が不可能であることから、エラーレスポンス（488 Not Acceptable Here）による応答を行う。

4.1.2.5 a=fingerprint行

3.4.1節に示すパスワード認証を使用する場合、VPNサーバはRFC4572[13]に従いa=fingerprint行を設定し、自らの自己署名証明書のダイジェストを記載する。

なお、3.4.2節に示す共有鍵認証のみを使用するSIP-VPN端末がa=fingerprint行を設定されたSDPを持つInitial INVITEリクエストを受信した場合は、相手端末が共有鍵認証以外の認証手順を要求していると解釈されることから、エラーレスポンス（488 Not Acceptable here）による応答を行う。

4.1.2.6 a=psk-fingerprint行

3.4.2節に示す共有鍵認証を使用する場合は、VPNクライアント、VPNサーバともに、RFC4572[13]に従い、a=psk-fingerprint行を設定し、事前共有鍵のダイジェストを記載する。

なお、3.4.1節に示すパスワード認証のみを使用するSIP-VPN端末がa=psk-fingerprint行を設定されたSDPを持つInitial INVITEリクエストを受信した場合は、相手端末がパスワード認証以外の認証手順を要求していると解釈されることから、エラーレスポンス（488 Not Acceptable Here）による応答を行う。

4.1.3 端末コンフィギュレーション

SIP-VPN 端末は、相互接続性確保のため、IKE を用いた IPsec 確立手順中で CP を用いたインナーのコンフィギュレーションを行う能力を有しなければならない。

4.1.3.1 VPNクライアント

VPNクライアントは、3.4.1節に示すパスワード認証を使用する場合、CPを利用したコンフィギュレーション能力を有していなければならない。インナーでのIPv4 を用いた通信に対応する場合には、INTERNAL_IP4_ADDRESS、INTERNAL_IP4_DNS、INTERNAL_IP4_SUBNETを、インナーでのIPv6 を用いた通信に対応する場合には、INTERNAL_IP6_ADDRESS、INTERNAL_IP6_DNS、INTERNAL_IP6_SUBNETに、それぞれ対応する。

ただし、個々の SIP-VPN 通信時に各 CP を利用するか否かは、VPN クライアントの設定によるものとする。

また、VPN サーバが提供する VPN ネットワーク空間の設定によっては、要求したパラメータに応答が返されないことに留意する。例えば、IPv6 の VPN ネットワーク空間を提供しない VPN サーバからは、INTERNAL_IP6_ADDRESS 等の IPv6 関連パラメータは返されず、DNS が VPN ネットワーク空間に存在しない場合は INTERNAL_IP4_DNS 等の DNS 関連パラメータは返されない。

4.1.3.2 VPNサーバ

VPNサーバは、3.4.1節に示すパスワード認証を使用する場合、CPを利用したコンフィギュレーション能

力を有していなければならない。IPv4 のVPNネットワーク空間を提供する場合には、VPNクライアントからINTERNAL_IP4_ADDRESS、INTERNAL_IP4_DNS、INTERNAL_IP4_SUBNETの各パラメータを要求された場合に、VPNネットワーク空間に関する情報を応答する。また、IPv6 のVPNネットワーク空間を提供する場合には、INTERNAL_IP6_ADDRESS、INTERNAL_IP6_DNS、INTERNAL_IP6_SUBNETの各パラメータを要求された場合に、VPNネットワーク空間に関する情報を応答する。

4.2 切断

IPsec の SA 削除（INFORMATIONAL リクエストによる delete 要求）を実施した後、SIP の BYE リクエストを送信し SIP セッションを解放する。

ただし、SA が存在する状態で BYE リクエストを受信した場合、または SA 削除のリクエストに対して応答を得られない場合、SIP-VPN 端末は SA 削除完了を待たず SIP の BYE リクエストを送信して良い。このとき、自端末内で SIP-VPN に使用していた SA は速やかに削除すること。

BYE リクエスト送信前に SA 削除を行うのは、以下の理由による。

切断時に BYE リクエストを送信すると、網により SIP-VPN 端末間でのメディアパスが削除され、UDP カプセル化 IKE や UDP カプセル化 ESP のパケットを疎通することが不可能となる場合がある。しかし、IKE や ESP のプロトコル層が通信断を認識できるまでしばらく時間を要することから、ユーザビリティ上の問題が発生する可能性がある。

4.3 キープアライブ

SIP セッションの更新に関しては、JT-Q3402 及び JT-Q3401 に従う。

SIP-VPN端末は、SAの更新をRFC5996[12]に従い、ReKeyを利用した手順を行う。このとき、PFSはOFFとする。なお、将来的なセキュリティ向上を鑑み、VPNサーバはPFSがONのSA更新手順にも対応していることが推奨される。

付属資料A　　UNI/NNI オプション項目選択

（本付属資料は仕様の一部である。）

A.1　概要

本付属資料は、SIP-VPN 通信を行うために必要となる、UNI/NNI のオプション項目選択のパターンを示す。

A.2　UNI オプション項目選択

JT-Q3402 の付録 i に記載されているオプション項目選択表のうち、SIP-VPN 通信に関連する項目について選択パターンを示す。

灰色背景部分が選択する項目を、ゴシック体の下線部分が関連する特記事項の内容を示す。SIP-VPN 通信を行う場合、網及び端末は下表の選択内容に従う。

付表 1-14／JT-Q3402 メディア

項番	項目	UNI の条件	端末の選択	関連項目 参照章節等	特記事項	備考
2	データ通信（m=application、m=data 等）	許容する	利用する場合がある	10.3.1 節 / 表 10-8	【許容するメディア種別（SDP の m=行）を決定する】 →application を許容する 《端末が利用する場合はメディア種別を記載する》 →application を利用する	
			利用しない			
		許容しない	利用しない			

付表 1-16／JT-Q3402 コーデックリストに含めるコーデック／データ通信用プロトコル

項番	項目	UNI の条件	端末の選択	関連項目 参照章節等	特記事項	備考
3	データ通信	許容する	利用する	8.1 節	【許容する場合はプロトコル名を記載する】 →application/ike-esp-udpencap を許容する 《端末が利用する場合はプロトコル名を記載する》 →application/ike-esp-udpencap を利用する	
			利用しない			
		許容しない	利用しない			

付表 1-22／JT-Q3402 メディアのネゴシエーション

項番	項目	UNI の条件	端末の選択	関連項目 参照章節等	特記事項	備考
4	オプションで規定する SDP 行 ［端末が送信］	利用する	－	10.3.1 節 表 10-8	【利用する SDP 行を記載する】 →a=ike-setup 行、a=fingerprint 行、a=psk-fingerprint 行を利用する 《送信する SDP 行を記載する》 →a=ike-setup 行、a=fingerprint 行、a=psk-fingerprint 行を送信する	
		利用しない	－			
5	オプションで規定する SDP 行 ［端末が受信］	利用する	－	10.3.1 節 表 10-8	【利用する SDP 行を記載する】 →a=ike-setup 行、a=fingerprint 行、a=psk-fingerprint 行を利用する 《受信をサポートする SDP 行を記載する》 →a=ike-setup 行、a=fingerprint 行、a=psk-fingerprint 行の受信に対応する	
		利用しない	－			

A.3 NNI オプション項目選択

JT-Q3401 の付録 iv に記載されているオプション選択表のうち、SIP-VPN 通信に関連する項目について選択パターンを示す。

灰色背景部分が選択する項目を、ゴシック体の下線部分が関連する特記事項の内容を示す。SIP-VPN 通信を NGN 間の NNI を越えて行う場合、網は下表の選択内容に従う。

付表 iv-6／JT-Q3401 SDP

	項目	網間での利用条件	関連項目	特記事項	備考
1	オプションで規定する SDP 行	利用する	10.3 節 表 10-7	【利用する SDP 行を決定する】 →a=ike-setup 行、a=fingerprint 行、a=psk-fingerprint 行を利用する	
		利用しない			

付表 iv-7／JT-Q3401 メディア

	項目	網間での利用条件	関連項目	特記事項	備考
2	データ通信（m=application、m=data 等）	利用する	10.3 節 表 10-7	【利用するメディア種別（SDP の m=行）を決定する】 →application を利用する	
		利用しない			

付表 iv-8／JT-Q3401 コーデックリストに含めるコーデック

	項目	網間での利用条件	関連項目	特記事項	備考
3	データ通信	含める	8 章	【プロトコル名を決定する】 →application/ike-esp-udpencap を利用する	
		含めない			

付録I　　SIP-VPN オプション項目表

（本付録は参考資料であり、仕様ではない。）

I.1　概要

本付録に示すオプション項目表は、UNI を介して NGN に接続する SIP-VPN 端末、及び NNI を介して相互に接続する NGN が SIP-VPN の相互接続性を高めるために、本仕様の本文、付属資料および付録において網が運用ポリシーにより選択可能なオプション項目、及び端末実装上で選択可能なオプション項目を抜き出して表にしたものである。網及び端末は、各項目について選択することができる。

本項目表中の各項目の詳細内容に関しては、関連する章節を「関連項目」欄に示すので参照されたい。

本表では、それぞれの項目の競合条件については、記載を行っていないことに注意が必要である。

なお、本文と本オプション項目表に、齟齬が存在した場合は本文の記載が適用される。

I.2　オプション項目の抽出ポリシー

オプション項目として、インタフェース仕様の観点と、端末実装の観点から項目を抽出した。

インタフェース仕様に関しては、下記の観点から抽出を行っている。

・UNI（JT-Q3402）を介する、SIP-VPN 端末の接続性を高める観点

・NNI（JT-Q3401）を介する、SIP-VPN 通信を円滑に行う観点

端末実装に関しては、下記の観点から抽出を行っている。

・VPN クライアントについて、本仕様で対応機能を選択可能とした項目の明確化

・VPN サーバについて、本仕様で対応機能を選択可能とした項目の明確化

なお、本文及び付属資料でサポートが必須となっている項目については、選択可能な項目ではないことから、オプション項目表に記載していない。

I.3　オプション項目表のフォーマット

オプション項目表のフォーマットと見方について付表 i-1 及び付表 i-2 に記載する。

I.3.1　インタフェース仕様（NNI）

付表 i-1／TS-1017　フォーマット例（NNI）

項番	項目	網間での利用条件	関連項目	特記事項	備考
1	－	－	－	－	－

項目:　オプション項目を示す。

網間での利用条件:　網間で選択可能なパターンを示す。

関連項目:　各オプション項目が、TS-1017 本文、付属資料及び付録のいずれの章節に関連するか示す。

特記事項:　「網間での利用条件」欄に加えて決定すべきオプション項目を示す。

なお、付表 i-1 では、本標準に NNI に関するオプション項目が存在しないため、記載内容は「－」とする。

I.3.2　インタフェース仕様（UNI）

付表 i-2／TS-1017　フォーマット例（UNI）

項番	項目	UNI の条件		端末の選択	関連項目 参照章節等	特記事項	備考
1	－	－	－	－	－	－	－
			－	－			

項目:　オプション項目を示す。
UNI の条件:　網が、UNI の条件として選択可能なパターンを示す。
端末の条件:　網の選択に対して、端末が選択可能なパターンを示す。
関連項目:　各オプション項目が、TS-1017 本文、付属資料及び付録のいずれの章節に関連するか示す。
特記事項:　「UNI の条件」、および「端末の選択」欄に加えて決定すべきオプション項目を示す。
なお、「UNI の条件」に関する特記事項を【】内に、「端末の選択」に関する特記事項を《》内に示す。

なお、付表 i-2 では、本標準に UNI に関するオプション項目が存在しないため、記載内容は「－」とする。

I.3.3　機能（VPN クライアント、VPN サーバ）

付表 i-3／TS-1017 フォーマット例（VPN クライアント）

	項目	機能の条件	関連項目	特記事項	備考
1	パスワード認証	サポートする	3.4節		
		サポートしない			
2	共有鍵認証	サポートする	3.4節		
		サポートしない			

項目:　オプション項目を示す。
機能の条件:　端末が具備する機能の条件として選択可能なパターンを示す。
関連項目:　各オプション項目が、TS-1017 本文、付属資料及び付録のいずれの章節に関連するか示す。
特記事項:　「機能の条件」欄に加えて決定すべきオプション項目を示す。

I.4　オプション項目表（インタフェース仕様）

I.4.1　UNI

UNI に関して、SIP-VPN 通信に固有のオプション項目はない。

I.4.2　NNI

NNI に関して、SIP-VPN 通信に固有のオプション項目はない。

I.5　オプション項目表（機能）

I.5.1　VPN クライアント

VPN クライアントの機能に関するオプション項目表を、付表 I-C-1 から I-C-2 に示す。

付表 I-C-1／TS-1017　発着信（VPN クライアント）

	項目	機能の条件	関連項目	特記事項	備考
1	発端末動作	サポートする	3.2節		
		サポートしない			
2	着端末動作	サポートする	3.2節		
		サポートしない			

付表 I-C-2／TS-1017　認証手順（VPN クライアント）

	項目	機能の条件	関連項目	特記事項	備考
1	パスワード認証	サポートする	3.4節		
		サポートしない			
2	共有鍵認証	サポートする	3.4節		
		サポートしない			

付表 I-C-3／TS-1017　IP バージョン（VPN クライアント）

	項目	機能の条件	関連項目	特記事項	備考
1	アウターの IPv4	サポートする	3.3.1節		
		サポートしない			
2	アウターの IPv6	サポートする	3.3.1節		
		サポートしない			
3	インナーの IPv4	サポートする	3.3.1節		
		サポートしない			
4	インナーの IPv6	サポートする	3.3.1節		
		サポートしない			

I.5.2　VPN サーバ

VPN サーバの機能に関するオプション項目表を、付表 I-S-1 に示す。

付表 I-S-1／TS-1017　発着信（VPN サーバ）

	項目	機能の条件	関連項目	特記事項	備考
1	発端末動作	サポートする	3.2節		
		サポートしない			
2	着端末動作	サポートする	3.2節		
		サポートしない			

付表 I-S-2／TS-1017 認証手順（VPN サーバ）

	項目	機能の条件	関連項目	特記事項	備考
1	パスワード認証	サポートする	3.4節		
		サポートしない			
2	共有鍵認証	サポートする	3.4節		
		サポートしない			

付表 I-S-3／TS-1017 IP バージョン（VPN サーバ）

	項目	機能の条件	関連項目	特記事項	備考
1	アウターの IPv4	サポートする	3.3.1節		
		サポートしない			
2	アウターの IPv6	サポートする	3.3.1節		
		サポートしない			
3	インナーの IPv4	サポートする	3.3.1節		
		サポートしない			
4	インナーの IPv6	サポートする	3.3.1節		
		サポートしない			

付録II　　シーケンス・メッセージ例

（本付録は参考資料であり、仕様ではない。）

本付録では、SIP-VPN 通信におけるシーケンス例及びメッセージ例について記載する。

本付録で記載したメッセージ例は、あくまで実装時の参考の位置づけであり、NGN のサービス内容や端末の機能により、適宜変更が必要となる場合がある。また、本付録の内容によって通信の接続性や品質を保証するものではない。

II.1　シーケンス・メッセージ例

本節では、表 II-1 に示すパターンについて、シーケンス例及びメッセージ例を記載する。

表 II-1：シーケンス・メッセージ例一覧

No.	シーケンス名	対応する章節
1	順方向接続（パスワード認証）	II.1.1
2	順方向接続（共有鍵認証）	II.1.2
3	切断	II.1.3
4	キープアライブ（SA 更新）	II.1.4

なお、本節の例では、SIP-UA や網の情報について、表 II-2 のような前提を置いて記載する。

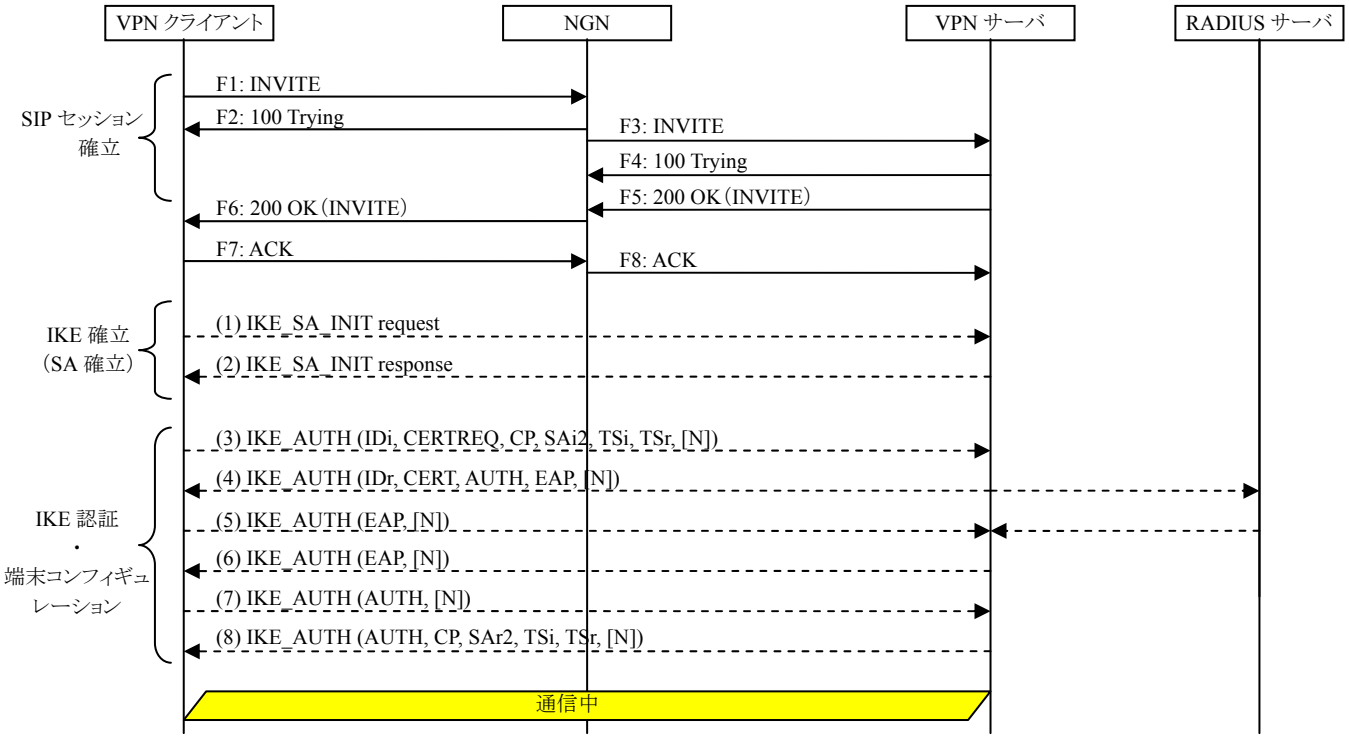
表 II-2：シーケンス・メッセージ例におけるアドレス等の設定

項目		設定内容
VPN クライアント	TEL-URI	tel:0311111111;phone-context=example.ne.jp
	SIP-URI	sip:0311111111@example.ne.jp
	IPv6 アドレス	2001:db8:1234:5678:acde:48ff:fe01:1
VPN サーバ	SIP ドメイン	example.ne.jp
	TEL-URI	tel:0322222222;phone-context=example.ne.jp
	SIP-URI	sip:0322222222@example.ne.jp
	IPv6 アドレス	2001:db8:1234:5678:acde:48ff:fe02:2
網	IPv6 アドレス（VPN クライアント側、SIP）	2001:db8::1
	IPv6 アドレス（VPN クライアント側、メディア）	2001:db8::11
	IPv6 アドレス（VPN サーバ側、SIP）	2001:db8::2
	IPv6 アドレス（VPN サーバ側、メディア）	2001:db8::22

II.1.1　順方向接続（パスワード認証）

順方向接続でパスワード認証を行う際のシーケンス例を付図 II-1 に示す。

シーケンス中では VPN サーバと RADIUS サーバを異なる機能部として記載しているが、実装上は RADIUS サーバ機能が VPN サーバ内に具備されていても良い。



付図 II-1／TS-1017　順方向接続（パスワード認証）

F1: INVITE

```
INVITE tel:0322222222;phone-context=example.ne.jp SIP/2.0
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:1]:5060;branch=z9hG4bK11
111111-11111111
Route: <sip:[2001:db8::1];lr>,<sip:s-cscf.example.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example.ne.jp>
From: <sip:0311111112@example.ne.jp>;tag=1234abcd
Call-ID: qwertyuiop111111@[2001:db8:1234:5678:acde:48ff:fe01:1]
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@[2001:db8:1234:4567:acde:48ff:fe01:1]:5060>
Allow: INVITE,ACK,BYE,CANCEL,UPDATE
Supported: timer
Session-Expires: 300
P-Preferred-Identity: <sip:0311111112@example.ne.jp>
Privacy: none
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82664419472 82664419472 IN IP6 2001:db8:1234:5678:48ff:fe01:1
s=-
c=IN IP6 2001:db8:1234:5678:48ff:fe01:1
t=0 0
m=application 4500 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:active
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:1]:5060;branch=z9hG4bK11
111111-11111111
To: <tel:0322222222;phone-context=example.ne.jp>
From: <sip:0311111111@example.ne.jp>;tag=1234abcd
Call-ID: qwertyuiop111111@[2001:db8:1234:5678:acde:48ff:fe01:1]
CSeq: 1 INVITE
Content-Length: 0
```

F3: INVITE

```
INVITE sip:contact@[2001:db8:1234:5678:acde:48ff:fe02:2] SIP/2.0
Via: SIP/2.0/UDP [2001:db8::2]:5060;branch=z9hG4bK22222222-22222222
Record-Route: <sip:[2001:db8::2];lr>
Max-Forwards: 64
To: <sip:0322222222@example.ne.jp>
From: <sip:0311111112@example.ne.jp>;tag=2345efgh
Call-ID: qwertyuiop222222@[2001:db8::2]
CSeq: 100 INVITE
Contact: <sip:asdfghj@[2001:db8::2]:5060>
Allow: INVITE,ACK,BYE,CANCEL,UPDATE
Supported: timer
Session-Expires: 300
P-Asserted-Identity: "0311111111"<sip:0311111111@example.ne.jp>,"0311111111"
<tel:0311111111;phone-context=example.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0322222222@example.ne.jp>
Content-Type: application/sdp
```

```
Content-Length: 162

v=0
o=- 82664419472 82664419472 IN IP6 2001:db8::22
s=-
c=IN IP6 2001:db8::22
t=0 0
m=application 22222 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:active
```

F4: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [2001:db8::2]:5060;branch=z9hG4bK22222222-22222222
To: <sip:0322222222@example.ne.jp>
From: <sip:0311111111@example.ne.jp>;tag=2345efgh
Call-ID: qwertyuiop222222@[2001:db8::2]
CSeq: 100 INVITE
Content-Length: 0
```

F5: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8::2]:5060;branch=z9hG4bK22222222-22222222
Record-Route: <sip:[2001:db8::2];lr>
To: <sip:0322222222@example.ne.jp>;tag=9876zyxw
From: <sip:0311111111@example.ne.jp>;tag=2345efgh
Call-ID: qwertyuiop222222@[2001:db8::2]
CSeq: 100 INVITE
Contact: <sip:[2001:db8::2]:5060>
Allow: INVITE,ACK,BYE,CANCEL,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 289

v=0
o=- 82917391739 82917391739 IN IP6 2001:db8:1234:5678:acde:48ff:fe02:2
s=-
c=IN IP6 2001:db8:1234:4567:acde:48ff:fe02:2
t=0 0
m=application 4500 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:passive
a=fingerprint:SHA-1 52:B6:5D:FA:BF:8A:8A:DB:7B:78:49:21:2C:AB:86:71:DC:9D:1C
:65
```

F6: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:1]:5060;branch=z9hG4bK11
111111-11111111
Record-Route: <sip:[2001:db8::1];lr>
To: <tel:0322222222;phone-context=example.ne.jp>;tag=8765vuts
From: <sip:0311111111@example.ne.jp>;tag=1234abcd
Call-ID: qwertyuiop111111@[2001:db8:1234:5678:acde:48ff:fe01:1]
CSeq: 1 INVITE
Contact: <sip:[2001:db8::1]:5060>
Allow: INVITE,ACK,BYE,CANCEL,UPDATE
Require: timer
```

```
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 244

v=0
o=- 82917391739 82917391739 IN IP6 2001:db8::11
s=-
c=IN IP6 2001:db8::11
t=0 0
m=application 11111 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:passive
a=fingerprint:SHA-1 52:B6:5D:FA:BF:8A:8A:DB:7B:78:49:21:2C:AB:86:71:DC:9D:1C
:65
```

F7: ACK

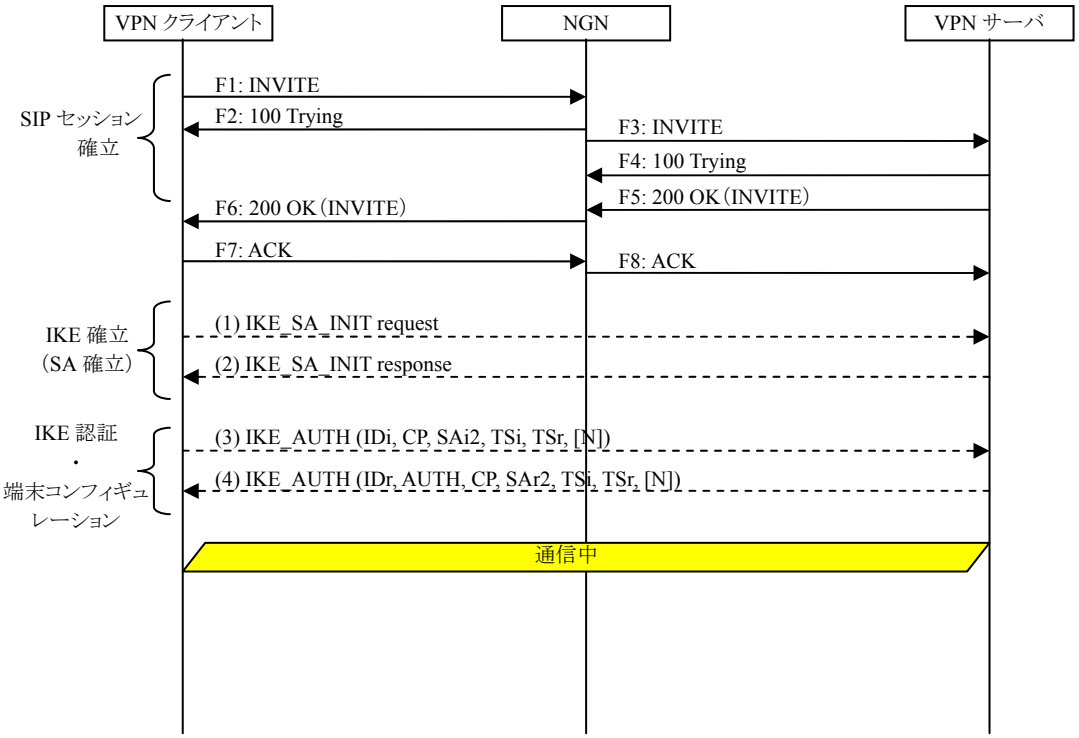
```
ACK sip:[2001:db8::1]:5060 SIP/2.0
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:1]:5060;branch=z9hG4bK11
111111-11111112
Route: <sip:[2001:db8::1];lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example.ne.jp>;tag=8765vuts
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd
Call-ID: qwertyuiop111111@[2001:db8:1234:5678:acde:48ff:fe01:1]
CSeq: 1 ACK
Content-Length: 0
```

F8: ACK

```
ACK sip:[2001:db8:1234:5678:acde:48ff:fe02:2]:5060 SIP/2.0
Via: SIP/2.0/UDP [2001:db8::2]:5060;branch=z9hG4bK22222222-22222223
Max-Forwards: 64
To: <sip:0322222222@example.ne.jp>;tag=9876zyxw
From: <sip:0311111111@example.ne.jp>;tag=2345efgh
Call-ID: qwertyuiop222222@[2001:db8::2]
CSeq: 100 ACK
Content-Length: 0
```

II.1.2　順方向接続（共有鍵認証）

順方向接続で共有鍵認証を行う際のシーケンス例を付図 II-2 に示す。



付図 II-2／TS-1017　順方向接続（共有鍵認証）

F1: INVITE

```
（SIP信号部分はII.1.1節のF1と同様であるため省略）

v=0
o=- 82664419472 82664419472 IN IP6 2001:db8:1234:5678:48ff:fe01:1
s=-
c=IN IP6 2001:db8:1234:5678:48ff:fe01:1
t=0 0
m=application 4500 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:active
a=psk-fingerprint:SHA-1 F5:02:66:86:6B:94:DC:37:C9:1E:2F:08:53:9A:00:F9:24:C
A:9D:86
```

F2: 100 Trying

（II.1.1節のF2 と同様であるため省略）

F3: INVITE

```
（SIP信号部分はII.1.1節のF3と同様であるため省略）

v=0
```

```
o=- 82664419472 82664419472 IN IP6 2001:db8::22
s=-
c=IN IP6 2001:db8::22
t=0 0
m=application 22222 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:active
a=psk-fingerprint:SHA-1 F5:02:66:86:6B:94:DC:37:C9:1E:2F:08:53:9A:00:F9:24:C
A:9D:86
```

F4: 100 Trying

（II.1.1節のF4 と同様であるため省略）

F5: 200 OK (INVITE)

```
（SIP信号部分はII.1.1節のF5と同様であるため省略）

v=0
o=- 82917391739 82917391739 IN IP6 2001:db8:1234:5678:acde:48ff:fe02:2
s=-
c=IN IP6 2001:db8:1234:4567:acde:48ff:fe02:2
t=0 0
m=application 4500 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:passive
a=psk-fingerprint:SHA-1 78:94:03:35:AD:EC:91:30:51:59:0D:13:24:E3:AF:4E:AF:9
2:1C:6F
```

F6: 200 OK (INVITE)

```
（SIP信号部分はII.1.1節のF6と同様であるため省略）

v=0
o=- 82917391739 82917391739 IN IP6 2001:db8::11
s=-
c=IN IP6 2001:db8::11
t=0 0
m=application 11111 udp ike-esp-udpencap
b=AS:1000
a=ike-setup:passive
a=psk-fingerprint:SHA-1 78:94:03:35:AD:EC:91:30:51:59:0D:13:24:E3:AF:4E:AF:9
2:1C:6F
```

F7: ACK

（II.1.1節のF7 と同様であるため省略）

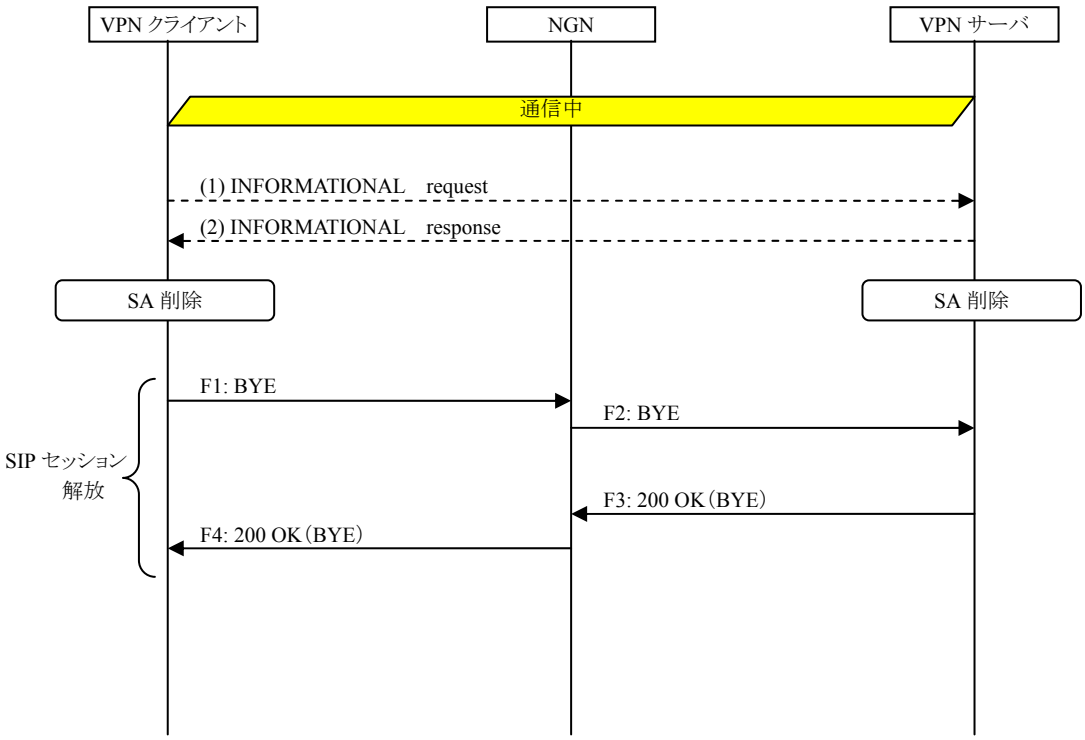
F8: ACK

（II.1.1節のF8 と同様であるため省略）

II.1.3　切断

切断を行う際のシーケンス例を付図 II-3 に示す。

SIP の BYE リクエストを送信する前に、IPsec のアソシエーションを解放する。



付図 II-3／TS-1017　切断

F1: BYE

```
BYE sip:[2001:db8::1]:5060 SIP/2.0
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:1]:5060;branch=z9hG4bK11
111111-11111113
Route: <sip:[2001:db8::1];lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example.ne.jp>;tag=8765vuts
From: <sip:0311111111@example.ne.jp>;tag=1234abcd
Call-ID: qwertyuiop111111@[2001:db8:1234:5678:acde:48ff:fe01:1]
CSeq: 3 BYE
Content-Length: 0
```

F2: BYE

```
BYE sip:[2001:db8:1234:5678:acde:48ff:fe02:2] SIP/2.0
Via: SIP/2.0/UDP [2001:db8::2]:5060;branch=z9hG4bK22222222-22222224
Max-Forwards: 64
To: <sip:0322222222@example.ne.jp>;tag=9876zyxw
From: <sip:0311111111@example.ne.jp>;tag=2345efgh
Call-ID: qwertyuiop222222@[2001:db8::2]
CSeq: 103 BYE
Content-Length: 0
```

F3: 200 OK（BYE）

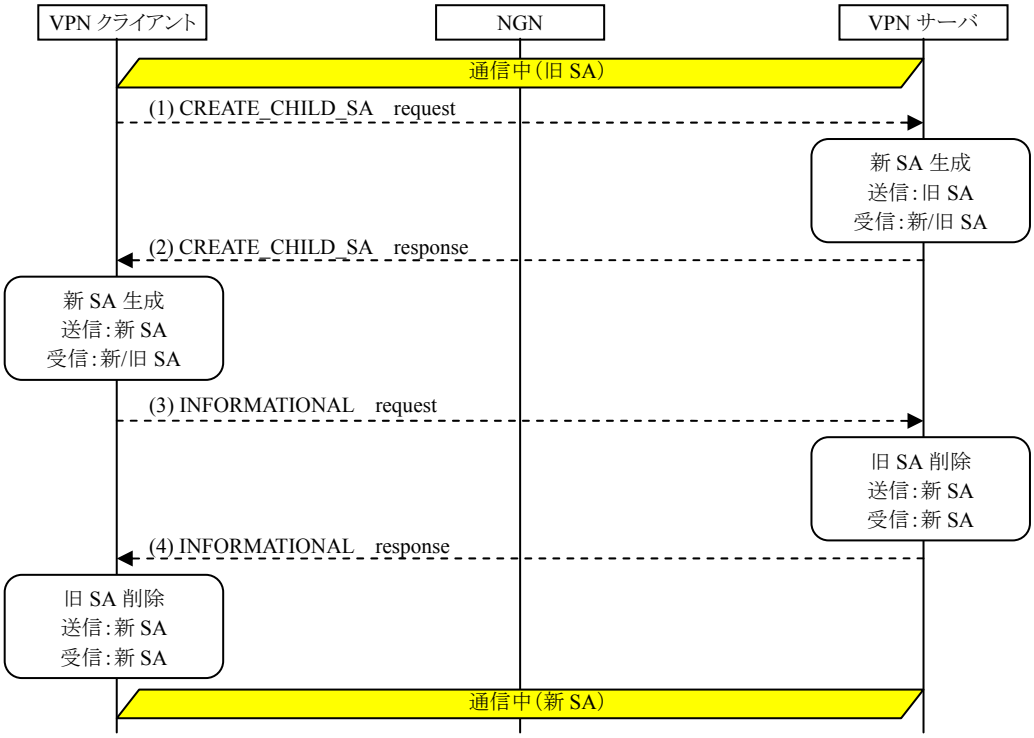
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8::2]:5060;branch=z9hG4bK22222222-22222224
To: <sip:0322222222@example.ne.jp>;tag=9876zyxw
From: <sip:0311111111@example.ne.jp>;tag=2345efgh
Call-ID: qwertyuiop222222@[2001:db8::2]
CSeq: 103 BYE
Content-Length: 0
```

F4: 200 OK（BYE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:1]:5060;branch=z9hG4bK11
111111-11111113
To: <tel:0322222222;phone-context=example.ne.jp>;tag=8765vuts
From: <sip:0311111111@example.ne.jp>;tag=1234abcd
Call-ID: qwertyuiop111111@[2001:db8:1234:5678:acde:48ff:fe01:1]
CSeq: 3 BYE
Content-Length: 0
```

II.1.4　キープアライブ（SA 更新）

キープアライブ（SA 更新）を行う際のシーケンス例を付図 II-4 に示す。



付図 II-4／TS-1017　キープアライブ（SA 更新）