TTC標準
Standard

JT-Q3402

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 (Protocol Set 1)）

第 3.0 版

2015 年 5 月 21 日

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

本標準は、2008 年 1 月に勧告化が承認された ITU-T 勧告 Q.3402 に準拠している。

2. 上記の勧告等に対する追加項目等

2. 1 オプション選択項目

なし

2. 2 ナショナルマター項目

なし

2. 3 その他

(1) 本標準は、上記 ITU-T 勧告に対し、内容を補足するために下記の事項を付属資料/付録として追加している。

(a) 国内の NGN 事業者網に UNI を介して接続する SIP 端末の接続性を高めるため、JT-Q3402 本文をベースドキュメントとした規定の明確化やオプション項目の明確化。

本標準の本文に対し、TTC として規定の明確化を行う項目を、本文の章節と対応付けて表形式で一覧とし、付属資料として記述している。したがって、本文と付属資料で記載が重複している箇所については、付属資料の規定に従う。（付属資料 a）

(b) 発信者番号の通知に関する事項。（付属資料 b）

(c) 端末登録に関する事項。（付属資料 c)

(d) SIP の能力交換に関する事項。（付属資料 d）

(e) SDP の設定及びメディアの扱いに関する事項。（付属資料 e）

(f) 輻輳の防止及び抑制への考慮に関する事項。（付属資料 f）

(g) 帯域制御に関する事項。（付属資料 g）

(h) SIP メッセージの設定内容について明確化。（付属資料 h）

(i) 音声端末の動作に関する規定。（付属資料 i）

(j) 本文、付属/付録資料の全体を含むオプション項目の一覧。（付録 i）

(k) レスポンスコードの用法に関するガイドライン。（付録 ii）

(l) SDP 記述を用いた品質クラスとの対応付け方式。（付録 iii）

(m) セキュリティに関する考慮事項。（付録 iv）

(n) SCF アドレスの取得手順。（付録 v）

(o) 各 SIP メッセージ及びヘッダに関する信号規定表。（付録 vi）

(p) 接続シーケンス例。（付録 vii)

2. 4 現勧告との章立て構成比較表

上記国際勧告との章立て構成の相違はない。

3. 改版の履歴

版数	制定日	改版内容
第 1.0 版	2009 年 5 月 27 日	制定
第 2.0 版	2011 年 5 月 31 日	帯域制御に関する記載の修正（JT-Y1221 を参照）等
第 3.0 版	2015 年 5 月 21 日	CUG/PNP に関する参照を追加等

4. 工業所有権

本標準に関わる「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ホームページで御覧になれます。

5. 標準策定部門

信号制御専門委員会

1. 本標準の範囲

本標準は、サービス層プロファイル、すなわちユーザと網の間の SIP/SDP インタフェースに関する記述と RTP などのトランスポート層プロファイルを規定する。

NGN UNI シグナリングプロファイルのプロトコルセット 1 として、本標準は、VoIP、マルチメディア電話、DTMF、T.38 FAX、マルチメディア呼出音、着信音、アナウンスを含むマルチメディア(音声、ビデオ、ならびにデータ)を対象とする。

本標準は、SIP 宅内ゲートウェイ、SIP 電話及び SIP IP-PBX といった全ての端末種別を対象とする。
そのため、以下に示す UNI を規定する。

- PSTN/ISDN 端末もしくは IP 電話が接続される SIP 宅内ゲートウェイと、サービス提供事業者の間。
- SIP 電話（IMS ベースの SIP 仕様が実装されたソフトフォンまたはハードフォン）と、サービス提供事業者の間。
- SIP IP-PBX（プロキシまたは B2BUA）と、サービス提供事業者の間。

2. 参考文献

以下の参照文書に含まれる規定は、本標準で引用されることによって、本標準の規定を構成する。これらの参照文書は、本標準が制定された際、ここに提示する版が有効であった。全ての参照文書は将来改訂されることを考慮し、本標準のすべての利用者には、以下の参照文書の最新版を適用する可能性を調査することが推奨される。現在有効な ITU-T 勧告のリストは、正式に出版されている。

本標準内の参照文書は、参照によって単独の TTC 標準とみなされるわけではない。

2.1. ITU 勧告、TTC 標準及び ISO/IEC 標準規格

[TR-1014] "NGN アーキテクチャの概要(General overview of NGN architecture)", TTC 技術レポート TR-1014 第 1 版，情報通信技術委員会(The Telecommunication Technology Committee)，2006 年 6 月

[T.38] "IP ネットワーク上のリアルタイムグループ 3 ファクシミリ通信手順 (Procedures for real-time Group 3 facsimile communication over IP networks)", TTC 標準 JT-T38 第 6 版,情報通信技術委員会(The Telecommunication Technology Committee)，2008 年 5 月

[T.140] ITU-T 勧告 T.140, "Protocol for multimedia application text conversation", 1998

[G.711] "音声周波数帯域信号の PCM 符号化方式(Pulse Code Modulation (PCM) of Voice Frequencies)",TTC 標準 JT-G711 第 4 版,情報通信技術委員会(The Telecommunication Technology Committee)，2001 年 4 月

[G.722] "64kbit/s 以下の 7kHz オーディオ符号化方式(7 kHz Audio Coding within 64 kbit/s)",TTC 標準 JT-G722 第 2.2 版,情報通信技術委員会(The Telecommunication Technology Committee)，2004 年 6 月

[G.722.1] "フレーム消失の少ないシステムにおけるハンズフリー用途向け 7kHz 帯域 24 および 32kbit/s オーディオ符号化方式(7kHz Audio-coding at 24 and 32 kbit/s for Hands Free Operation in Systems with Low Frame Loss)",TTC 標準 JT-G722.1 第 4 版,情報通信技術委員会(The Telecommunication Technology Committee)，2005 年 11 月

[G.722.2] "適応マルチレート広帯域（AMR-WB）方式を用いた 16kbit/s 程度の広帯域音声符号化 (WIDEBAND CODING OF SPEECH AT AROUND 16 KBIT/S USING ADAPTIVE MULTI-RATE

WIDEBAND (AMR-WB))",TTC 標準 JT-G722.2 第 3.3 版,情報通信技術委員会(The Telecommunication Technology Committee), 2007 年 5 月

[G.726] "40,32,24,16kbit/s 適応差分パルス符号変調方式(40,32,24,16kbit/s Adaptive Differential Pulse code Modulation (ADPCM))",TTC 標準 JT-G726 第 2.1 版,情報通信技術委員会(The Telecommunication Technology Committee), 2005 年 6 月

[G.729] "8kbit/s CS-ACELP を用いた音声符号化方式(Coding of Speech at 8kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP))",TTC 標準 JT-G729 第 6.1 版,情報通信技術委員会(The Telecommunication Technology Committee), 2006 年 11 月

[G.729A] ITU-T 勧告 G.729 Annex A, "Reduced complexity 8 kbit/s CS-ACELP speech codec", 1996

[G.729.1] "JT-G729 ベースのエンベデッド可変ビットレート符号化: JT-G729 とビット列互換な 8-32kbit/s スケーラブル広帯域符号化(G.729 based Embedded Variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729)",TTC 標準 JT-G729.1 第 1 版,情報通信技術委員会(The Telecommunication Technology Committee), 2007 年 3 月

[H.263] "低ビットレート通信用ビデオ符号化方式(Video Coding For Low Bitrate Communication), TTC 標準 JT-H263 第 3.2 版,情報通信技術委員会 (The Telecommunication Technology Committee), 2005 年 6 月

[H.264] "オーディオビジュアルサービス全般のための高度ビデオ符号化方式(ADVANCED VIDEO CODING FOR GENERIC AUDIOVISUAL SERVICES), TTC 標準 JT-H264 第 4.0 版,情報通信技術委員会 (The Telecommunication Technology Committee), 2006 年 8 月

[ISO/IEC 14496-2] ISO/IEC 14496-2 (2004), Information technology -- Coding of audio-visual objects -- Part 2: Visual

[ISO/IEC 14496-3] ISO/IEC 14496-3 (2005), Information technology -- Coding of audio-visual objects -- Part 3: Audio

2.2. TTC で簡略標準化された IETF 文書

2.2.1. サービス層シグナリング規定文書

[RFC 2046] "多目的インターネットメール拡張(MIME)パート2:メディア型式(Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types) ",TTC標準JF-IETF-RFC2046 第1版, 情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月

[RFC 2327] "SDP:セッション記述プロトコル (Session Description Protocol)",TTC標準 JF-IETF-RFC2327,情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月

[RFC 2617] "HTTP 認証方式：ベーシックアクセス認証とダイジェスト・アクセス認証(HTTP Authentication: Basic and Digest Access Authentication)",TTC標準 JF-IETF-RFC2617,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 2976] "セッション開始プロトコル（SIP）INFOメソッド (The SIP INFO Method)",TTC標準 JF-IETF-RFC2976,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3261] "SIP:セッション開始プロトコル(Session Initiation Protocol) ",TTC標準JF-IETF-RFC3261 第1版, 情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月.

[RFC 3262] "セッション開始プロトコル（SIP）における暫定レスポンスの信頼性(Reliability of Provisional Responses in SIP)",TTC標準 JF-IETF-RFC3262 第1版, 情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月.

[RFC 3263] "SIPサーバ情報の取得手順(Session Initiation Protocol (SIP): Locating SIP Servers)",TTC標準 JF-IETF-RFC3263 第1版, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3264] "セッション記述プロトコル（SDP）を使ったオファー/アンサーモデル(An Offer/Answer model with SDP)",TTC標準 JF-IETF-RFC3264 第1版,情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月.

[RFC 3265] "セッション開始プロトコル(SIP)特有のイベント通知(Session Initiation Protocol (SIP)-Specific Event Notification)",TTC標準 JF-IETF-RFC3265 第1版,情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月.

[RFC 3310] "AKAを利用する場合のHTTPダイジェスト認証方式(Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA))",TTC標準 JF-IETF-RFC3310, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3311] "セッション開始プロトコル（SIP）UPDATEメソッド（The Session Initiation Protocol UPDATE Method） ",TTC標準 JF-IETF-RFC3311, 情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月

[RFC 3312] "リソース管理とセッション開始プロトコル（SIP）の統合(Integration of Resource Management and Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3312,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3313] "メディア認証に関するSIPの拡張 (Private Session Initiation Protocol (SIP) Extensions for Media Authorization)",TTC標準 JF-IETF-RFC3313, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3320] "信号圧縮方式（SigComp） (Signaling Compression (SigComp))",TTC標準 JF-IETF-RFC3320, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3323] "セッション開始プロトコル（SIP）のためのプライバシー機構 (A Privacy Mechanism for the Session Initiation Protocol (SIP)) ", TTC標準 JF-IETF-RFC3323,情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月

[RFC 3324] "網付与ID情報のための短期的な要求条件(Short Term Requirements for Network Asserted Identity)", TTC標準 JF-IETF-RFC 3324第1版, 情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月.

[RFC 3325] "トラストドメイン内の網付与ID情報のためのセッション開始プロトコル（SIP）へのプライベート拡張 (Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks) ",TTC標準 JF-IETF-RFC3325,情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月

[RFC 3326] "セッション開始プロトコル（SIP）のためのReasonヘッダフィールド (The Reason Header Field for the Session Initiation Protocol (SIP)) ",TTC標準 JF-IETF-RFC3326,情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月

[RFC 3327] "隣接していないコンタクトを登録するためのセッション開始プロトコル（SIP）の拡張ヘッダフィールド(Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts) ",TTC 標準 JF-IETF-RFC3327, 情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月

[RFC 3329] "SIPにおけるセキュリティ能力交換方式(Security Mechanism Agreement for the Session Initiation Protocol (SIP)) ",TTC標準 JF-IETF-RFC3329,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3388] "SDPにおけるメディア行のグループ化(Grouping of Media Lines in the Session Description Protocol (SDP))",TTC標準 JF-IETF-RFC3388,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3420] "インターネットのメディア型式 message/sipfrag(Internet Media Type message/sipfrag)",TTC標準 JF-IETF-RFC3420,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3428] "インスタントメッセージのためのセッション開始プロトコル（SIP）"（Session Initiation Protocol (SIP) Extension for Instant Messaging）, TTC標準 JF-IETF-RFC3428, 情報通信技術委員会(The Telecommunication Technology Committee), 2006年9月

[RFC 3455] "3GPPのためのセッション開始プロトコル（SIP）のプライベートヘッダ（P-Header）拡張(Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)), TTC 標準 JF-IETF-RFC3455, 情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月

[RFC 3485] "信号圧縮方式（SigComp）のSIP/SDP用静的辞書(The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)) ", TTC標準 JF-IETF-RFC3485,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3486] "SIPにおける信号圧縮方式(Compressing the Session Initiation Protocol(SIP))", TTC標準 JF-IETF-RFC3486,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3515] "セッション開始プロトコル（SIP）Referメソッド (The Session Initiation Protocol (SIP) Refer Method)", TTC 標準 JF-IETF-RFC3515, 情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月

[RFC 3524] "SDPにおけるSRFグループ指定によるリソース予約の共有(Mapping of Media Streams to Resource Reservation Flows)",TTC 標準 JF-IETF-RFC3524, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3556] "RTCP帯域指定を行うためのSDP記述方式(Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth)",TTC標準 JF-IETF-RFC3556,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3581] "NAPT存在下でレスポンスの対称ルーチングを行うためのSIP拡張(An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing)",TTC標準 JF-IETF-RFC3581,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3608] "登録時のサービスルート検出のためのセッション開始プロトコル（SIP）拡張ヘッダフィールド(Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration)",TTC標準 JF-IETF-RFC3608,情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月.

[RFC 3680] "登録のためのセッション開始プロトコル（SIP）イベントパッケージ(A Session Initiation Protocol (SIP) Event Package for Registrations)",TTC標準 JF-IETF-RFC3680,情報通信技術委員会 (The Telecommunication Technology Committee), 2007年3月.

[RFC 3725] "SIPにおける第三者呼制御（3pcc）手順(Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3725,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3824] "セッション開始プロトコル（SIP）におけるE.164番号の利用(Using E.164 numbers with the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3824,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3840] "セッション開始プロトコル(SIP)におけるUA能力の通知(Indicating User Agent Capabilities in the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3840,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月

[RFC 3841] "セッション開始プロトコル(SIP)の為の発信者プレファレンス(Caller Preferences for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3841,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3842] "メッセージ状態通知およびメッセージウェイティング通知のためのSIPイベントパッケージ(A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3842,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3853] "SIPにおけるS/MIMEでのAES利用(S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3853,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3856] "プレゼンス通知のためのSIPイベントパッケージ(A Presence Event Package for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3856,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3857] "ウォッチャー情報通知のためのSIPイベントパッケージ(A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3857,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3858] "ウォッチャー情報のためのXMLベース形式(An Extensible Markup Language (XML) Based Format for Watcher Information)",TTC標準 JF-IETF-RFC3858,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3859] "プレゼンス共通プロファイル（CPP）(Common Profile for Presence (CPP))",TTC標準 JF-IETF-RFC3859,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3860] "インスタントメッセージ共通プロファイル（CPIM）(Common Profile for Instant Messaging (CPIM))",TTC標準 JF-IETF-RFC3860,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3861] "インスタントメッセージとプレゼンスにおけるアドレス解決方式(Address Resolution for Instant Messaging and Presence)",TTC標準JF-IETF-RFC3861,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3862] "CPIM： メッセージ形式(Common Presence and Instant Messaging (CPIM): Message Format)",TTC標準 JF-IETF-RFC3862,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3863] "プレゼンス情報データ形式(PIDF) (Presence Information Data Format (PIDF))",TTC標準 JF-IETF-RFC3863,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 3891] "セッション開始プロトコル (SIP) Replacesヘッダ (The Session Initiation Protocol (SIP) "Replaces" Header)", TTC標準 JF-IETF-RFC3891,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月

[RFC 3892] "セッション開始プロトコル (SIP) Referred-Byメカニズム (The Session Initiation Protocol (SIP) Referred-By Mechanism)",TTC標準 JF-IETF-RFC3892, 情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月.

[RFC 3903] "イベント状態発行のためのセッション開始プロトコル (SIP) 拡張 (Session Initiation Protocol (SIP) Extension for Event State Publication)",TTC標準 JF-IETF-RFC3903,情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月.

[RFC 3911] "セッション開始プロトコル (SIP) Joinヘッダ(The Session Initiation Protocol (SIP) "Join" Header)",TTC標準 JF-IETF-RFC3911,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3959] "セッション開始プロトコル(SIP)の為の早期セッション特性型式(The Early Session Disposition Type for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3959,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3960] "セッション開始プロトコル(SIP)におけるアーリーメディアおよび呼出音生成 (Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC3960,情報通信技術委員会(The Telecommunication Technology Committee), 2006年8月.

[RFC 3966] "電話番号のためのtel URI(The tel URI for Telephone Numbers)",TTC標準 JF-IETF-RFC3966,情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月.

[RFC 3994] "インスタントメッセージでの通信中におけるメッセージ作成中状態の通知(Indication of Message Composition for Instant Messaging)", TTC標準 JF-IETF-RFC3994, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4028] "セッション開始プロトコル (SIP) におけるセッションタイマ (Session Timers in the Session Initiation Protcol (SIP)",TTC標準JF-IETF-RFC4028,情報通信技術委員会(The Telecommunication Technology Committee), 2005年8月

[RFC 4032] "セッション開始プロトコル(SIP)のプレコンディション・フレームワークの更新(Update to the Session Initiation Protocol (SIP) Preconditions Framework)",TTC標準 JF-IETF-RFC4032,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 4145] "セッション記述プロトコル(SDP)におけるTCPベースのメディアトランスポート(TCP-Based Media Transport in the Session Description Protocol (SDP))", TTC標準 JF-IETF-RFC4145, 情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月.

[RFC 4168] "SIPにおけるSCTPの利用方式(The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC4168,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 4235] "セッション開始プロトコル(SIP)の為のINVITE送出ダイアログ・イベント・パッケージ(An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC4235,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 4244] "リクエスト履歴情報のためのセッション開始プロトコル(SIP)への拡張 (An Extension to the Session Initiation Protocol (SIP) for Request History Information)", TTC標準 JF-IETF-RFC4244, 情報通信技術委員会(The Telecommunication Technology Committee), 2006年8月

[RFC 4320] "非INVITEトランザクションに関する課題を解決するための修正(Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction)",TTC標準 JF-IETF-RFC4320,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 4412] "セッション開始プロトコル(SIP)の為の通信リソースのプライオリティ(Communications Resource Priority for the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC4412,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月

[RFC 4458] "ボイスメールおよび音声応答システム(IVR)などのアプリケーションのためのセッション開始プロトコル(SIP)URI (Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR))", TTC標準 JF-IETF-RFC4458, 情報通信技術委員会(The Telecommunication Technology Committee), 2006年8月.

[RFC 4480] "RPID： プレゼンス情報データ形式（PIDF）の拡張(RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF))",TTC標準 JF-IETF-RFC4480, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 4483] "セッション開始プロトコル(SIP)メッセージにおけるコンテンツ間接参照メカニズム(A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages)",TTC標準 JF-IETF-RFC4483,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 4566] "SDP：セッション記述プロトコル(SDP: Session Description Protocol)",TTC標準 JF-IETF-RFC4566,情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月.

[RFC 4575] "会議状態通知のためのSIPイベントパッケージ(A Session Initiation Protocol (SIP) Event Package for Conference State)",TTC標準 JF-IETF-RFC4575, 情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4579] "会議におけるSIPのisfocusフィーチャーを用いた呼制御手順(Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents)",TTC標準 JF-IETF-RFC4579,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4583] "BFCPストリームのSDP記述方式(Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams)",TTC標準 JF-IETF-RFC4583,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4662] "リソースリスト通知のためのSIPイベント通知の拡張(A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists)",TTC標準 JF-IETF-RFC4662,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4715] "tel URIのためのISDNサブアドレスエンコード形式 (The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI)",TTC標準 JF-IETF-RFC4715,情報通信技術委員会(The Telecommunication Technology Committee), 2007年3月.

[RFC 4730] "キー押下に関するスティミュラスな通知（KPML）のためのSIPイベントパッケージ(A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML))",TTC標準 JF-IETF-RFC4730,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 5031] "緊急呼等に関するサービスURNの規定(A Uniform Resource Name (URN) for Emergency and Other Well-Known Services)",TTC標準 JF-IETF-RFC5031,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月

[RFC 5049] "SIPへの信号圧縮方式（SigComp）の適用(Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC5049,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 5079] "SIPにおける匿名リクエストの拒否(Rejecting Anonymous Requests in the Session Initiation Protocol (SIP))",TTC標準 JF-IETF-RFC5079,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

.

2.2.2. トランスポート層規定文書

[RFC 3016] "MPEG-4 Audio/VisualストリームのRTPペイロード形式(RTP Payload Format for MPEG-4 Audio/Visual Streams)",TTC標準 JF-IETF-RFC3016,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3047] "ITU-T勧告 G.722.1のRTPペイロード形式(RTP Payload Format for ITU-T Recommendation G.722.1)",TTC標準JF-IETF-RFC3047,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3267] "AMR及びAMR-WB音声コーデックの為のRTPペイロード形式と蓄積形式(Real-time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs)",TTC標準 JF-IETF-RFC3267,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3389] "コンフォートノイズの為のRTPペイロード(RTP Payload for Comfort Noise)",TTC標準 JF-IETF-RFC3389,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 3550] "RTP: リアルタイムアプリケーションのためのトランスポートプロトコル(RTP: A Transport Protocol for Real-Time Applications)",TTC標準 JF-IETF-STD64,情報通信技術委員会(The Telecommunication Technology Committee), 2005年5月.

[RFC 3551] "最小限の制御による音声とビデオ会議のためのRTPプロファイル(RTP Profile for Audio and Video Conferences with Minimal Control)",TTC標準 JF-IETF-STD65,情報通信技術委員会(The Telecommunication Technology Committee), 2005年6月.

[RFC 3558] "EVRCとSMVのRTPペイロード形式(RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV))",TTC標準 JF-IETF-RFC3558,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3611] "RTCPの拡張レポート（XR）パケット形式(RTP Control Protocol Extended Reports (RTCP XR))",TTC標準 JF-IETF-RFC3611,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3711] "セキュアリアルタイムトランスポートプロトコル(SRTP) (The Secure Real-time Transport Protocol (SRTP))",TTC標準 JF-IETF-RFC3711,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 3984] "H.264ビデオのためのRTPペイロードフォーマット(RTP Payload Format for H.264 Video)",TTC標準 JF-IETF-RFC3984,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4103] "テキスト対話の為のRTPペイロード(RTP Payload for Text Conversation)",TTC標準 JF-IETF-RFC4103,情報通信技術委員会(The Telecommunication Technology Committee), 2007年11月.

[RFC 4348] "VMR-WBのRTPペイロード形式(Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec)",TTC標準 JF-IETF-RFC4348,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4629] "ITU-T勧告H.263のRTPペイロード形式(RTP Payload Format for ITU-T Rec. H.263 Video)",TTC標準 JF-IETF-RFC4629,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4733] "DTMFディジット、電話トーン、電話信号のためのRTPペイロード(RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals)",TTC標準 JF-IETF-RFC4733,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

[RFC 4749] "G.729.1のRTPペイロード形式(RTP Payload Format for the G.729.1 Audio Codec)",TTC標準 JF-IETF-RFC4749,情報通信技術委員会(The Telecommunication Technology Committee), 2008年3月.

2.3. ETSI 文書

[EN 301 703] ETSI EN 301 703 V7.0.2 (1999-12), Digital cellular telecommunications system (Phase 2+); Adaptive Multi-Rate (AMR); Speech processing functions; General description (GSM 06.71 version 7.0.2 Release 1998)

2.4. その他の文書

[TIA-127] TIA-127-A, Enhanced Variable Rate Codec (EVRC) Speech Option 3 for Wideband Spread Spectrum Digital Systems (May 2004)

[TIA-1016] TIA-1016-A, Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB), Service Options 62 and 63 for Spread Spectrum Systems (January 2006)

3. 用語と定義

SIP と SDP に関する特有な用語については、[RFC 3261]、[RFC 3264]、[RFC 2327] 及び [RFC 4566]が参照されなければならない。NGN に関する特有な用語については、[TR-1014]が参照されなければならない。本標準で追加使用される用語を以下に記す：

3.1. 推奨コーデックリスト

推奨コーデックリストは UNI 上で交換される SIP/SDP メッセージで網がユーザに示すべきコーデックを含む。

(注) : 推奨コーデックリストの目的は、単に網が UNI のユーザに推奨するコーデックを示すことであり、推奨コーデックリストはリストに示されたコーデックの全てを実装することを端末に推奨するものではない。

3.2. EUF

エンドユーザ機能(EUF)は、従来の端末と NGN 端末の両方のエンドユーザ装置、および私設網を含む。エンドユーザ装置は移動体もしくは固定端末のいずれでも良い。NGN に接続する EUF の持つエンドユーザインタフェースは物理及び機能(制御)インタフェースの両方によってサポートされる。

3.3. SCF

サービス制御機能（SCF）は、マルチメディアセッションを確立、監視、サポート、そして解放し、またユーザが利用する複数のサービスの相互作用を管理する。

3.4. SIP B2BUA

バック-トゥ-バック ユーザエージェント(B2BUA)は、SIP ユーザエージェントクライアント(UAC)とユーザエージェントサーバ (UAS)を結合したものである。

(注) IETF は、B2BUA を[RFC 3261]において「バック・トゥ・バック ユーザエージェント(B2BUA)とは、リクエストを受け取り、ユーザエージェントサーバ(UAS)としてそれを処理する論理的なエンティティである。リクエストにどのように答えるべきか決定するためにユーザエージェントクライアント(UAC)として動作し、リクエストを生成する。プロキシサーバとは違い、ダイアログの状態を保持し、それが確立したダイアログ上で送られるすべてのリクエストに関与しなければならない。UAC と UAS が結合されたものなので、その動作に関する明示的な定義は必要とされない。」と定義している。(UAC の動作と UAS の動作は[RFC 3261]で定義されている。) B2BUA はメッセージを送信する前に新規リクエストとして再形成する。

4. 略語

本標準内では以下の略語が使用される。

3GPP	3rd-Generation Partnership Project
AKA	Authentification and Key Agreement
AMR	Adaptive Multirate (codec)
AMR NB	AMR Narrowband
AMR WB	AMR Wideband
B2BUA	Back-to-Back User Agent
CSC-FE	Call Session Control Functional Entity
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DTMF	Dual-Tone Multifrequency
EUF	End-User Functions
EVRC	Enhanced Variable Rate Codec
FQDN	Fully Qualified Domain Name
GRUU	Globally Routable User Agent URIs
HTTP	Hypertext Transfer Protocol
IBC-FE	Interconnection Border gateway Control Functional Entity
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP PBX	IP Private Branch eXchange
ISDN	Integrated Services Digital Network
ISO/IEC	International Standardization Organization/International Electrotechnical Commission
ISUP	ISDN User Part
ITU-T	International Telecommunication Union-Telecommunication
IVR	Interactive Voice Response
KPML	Key Press Stimulus
MIME	Multi-purpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
NAT	Network Address Translation
NGN	Next Generation Network
NGN-TE	NGN Terminal Equipment
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RGW	Residential Gateway
RTCP	RTP Control Protocol
RTCP XR	RTCP eXtended Reports
RTP	Real-Time Transport Protocol
SCF	Service Control Functions
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol

SIPS	Session Initiation Protocol Secure
SMV	Selectable Mode Vocoders
SRTP	Secure Real-time Transport Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UNI	User-to-Network Interface
URI	Universal Resource Identifier
VMR-WB	Variable-Rate Multi-Mode Wideband
VoIP	Voice over IP

5. 参照モデル

[TR-1014]に定義される UNI インタフェースが、NGN アーキテクチャにおいて本標準が対象とする範囲である。

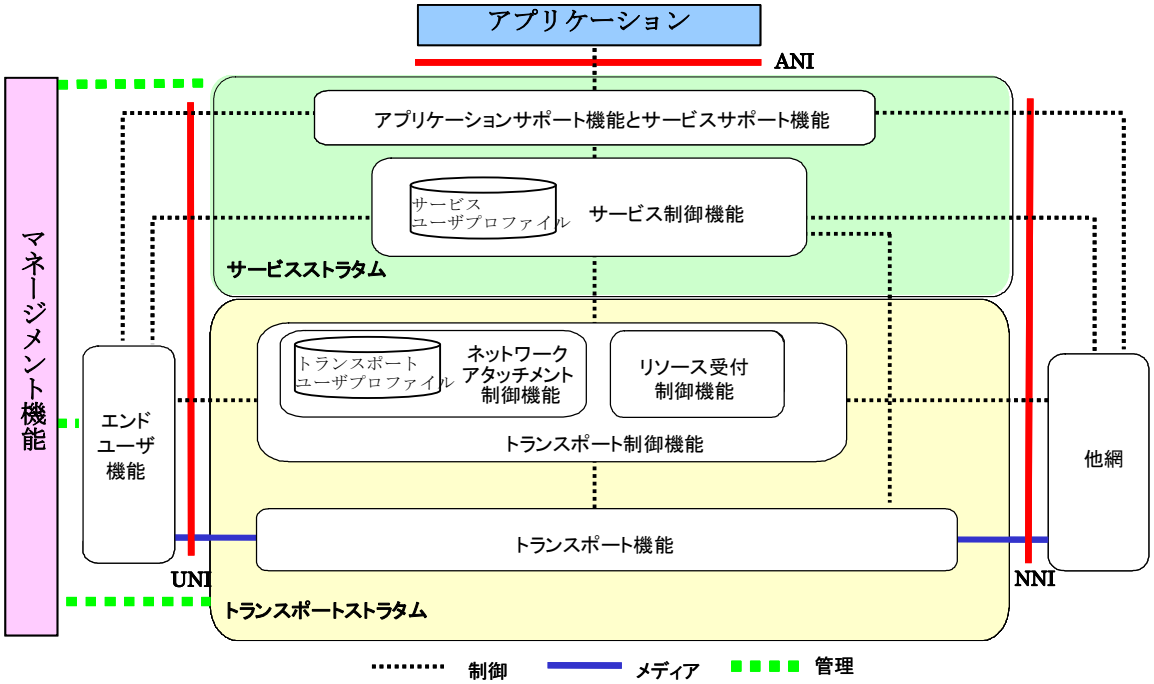


図 5-1／JT-Q3402　NGN アーキテクチャにおける本標準が対象とするインタフェース　（ITU-T Q.3402）

図 5-2、図 5-3及び図 5-4は、EUF の範囲内の端末種別についての想定概要を図示する。

図 5-2は、SIP 宅内ゲートウェイを通じてサービス提供事業者に接続する PSTN/ISDN 端末と IP 電話のための概要を示す。

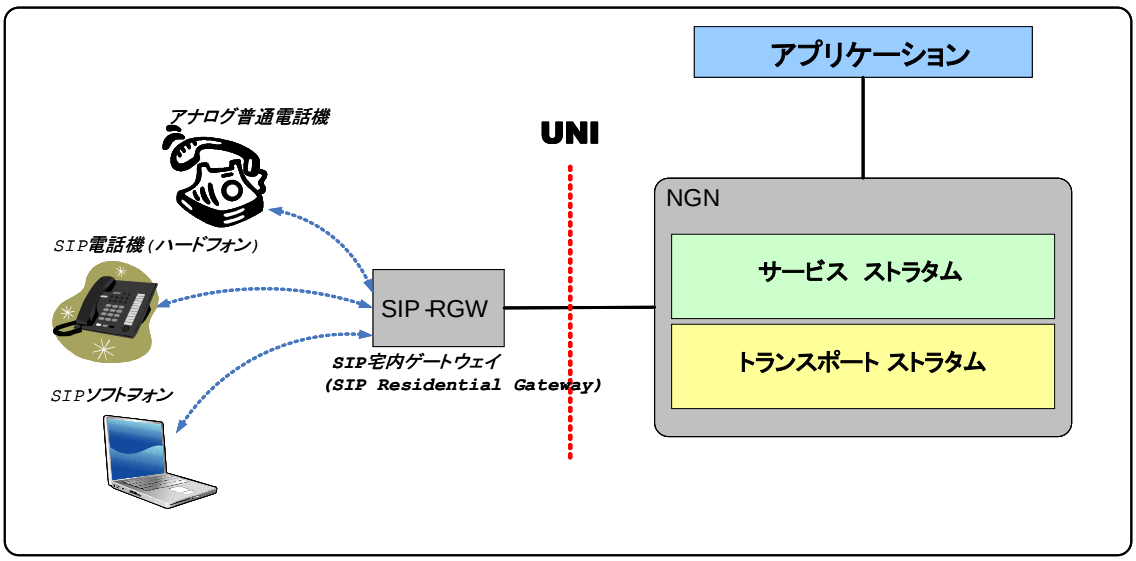


図 5-2／JT-Q3402　SIP 宅内ゲートウェイのための概要　（ITU-T Q.3402）

図 5-3は、サービス提供事業者に直接接続する IMS ベースの SIP 端末のための概要を示す。

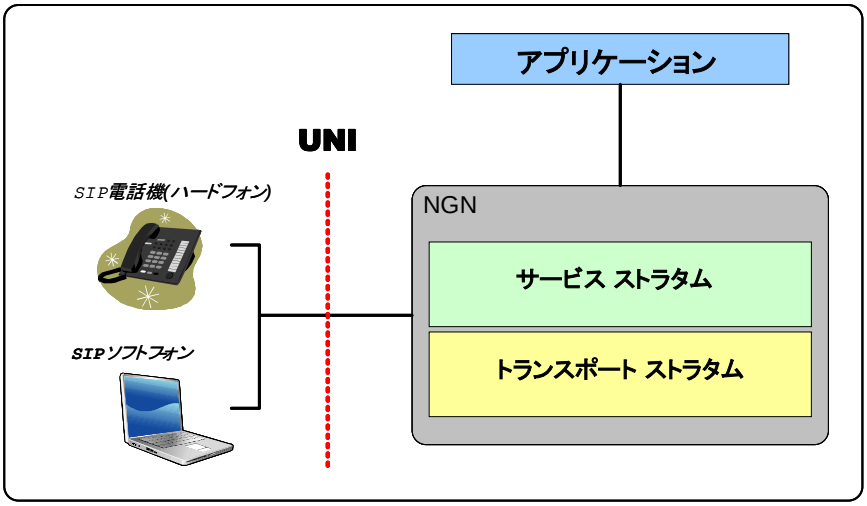


図 5-3／JT-Q3402　IMS ベースの SIP 端末のための概要　（ITU-T Q.3402）

図 5-4は、SIP IP PBX を通じてサービス提供事業者に接続する SIP 端末のための概要を示す。

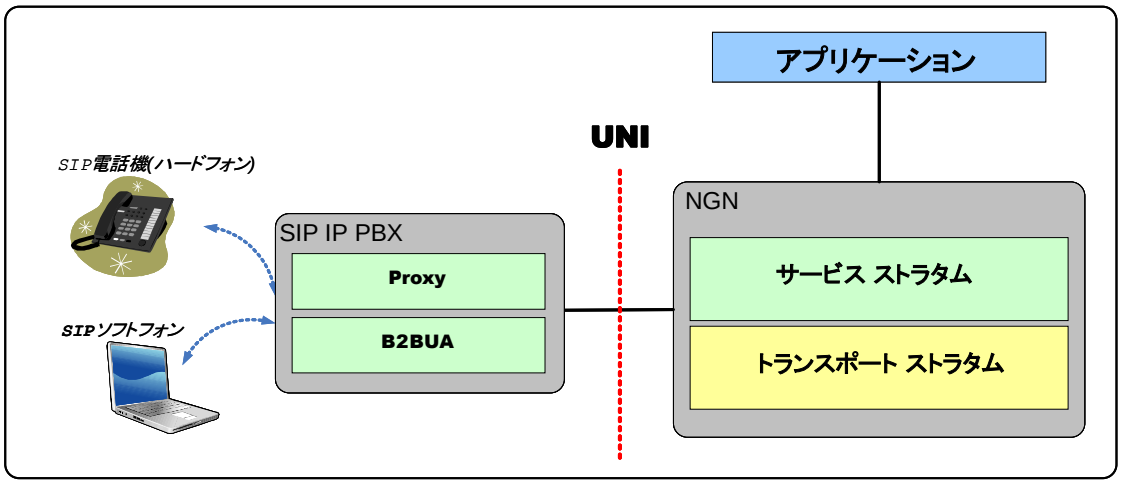


図 5-4／JT-Q3402　SIP IP-PBX のための概要　（ITU-T Q.3402）

6.　想定事項

本標準は、以下の想定項目に基づく。

1. セッション制御に SIP/SDP を使用する。
2. 音声及び映像の転送に RTP または SRTP を使用する。データアプリケーションを利用する場合、その他のトランスポートプロトコルを使用しても良い。

7.　SIP セッションにて利用可能なメディア

7.1.　メディアパケットに関する考慮事項

以下の事項は、SIP を使用して UNI 上で確立された全てのメディアセッションに適用される。

a) 発信側 EUF

- INVITE に対する 2xx レスポンスに含まれる SDP アンサー受信以降、メディアパケットを送信しなければならない。

- アーリーダイアログが設定されている場合、INVITE に対する 1xx レスポンスに含まれる最初の SDP アンサーの受信後、すぐにメディアパケットを送信しても良い。事業者網はポリシーとして、従量制課金が採用されている場合では、サービスの不正利用を回避するために、最終 SDP ネゴシエーションが行われるまで、発信元からのメディアパケットを通さないことを選択する場合がある。
- SDP オファーを含む INVITE を送信後、メディアパケットを受信する準備をしなければならない。

b) 着信側 EUF

- SDP を含む INVITE に対する 2xx レスポンスを送信後、メディアパケットを送信しなければならない。
- INVITE に対する 2xx レスポンスを送信後、メディアパケットを受信する準備をしなければならない。

c) [RFC3261]に従い、ダイアログの終了後、メディアフローは停止されなければならない。

d) UNI 上にメディアパケットが流れていなくても、EUF もしくは事業者網は SIP セッションを終了してはならない。ただし、SDP のネゴシエーションによってメディアフローの状態がアクティブの場合、ある一定期間の UNI 上のメディアパケット消失は、SIP セッションを終了する理由となる場合がある。

(注) ある一定期間の UNI 上のメディアパケット消失は、障害によるということが確かな場合のみ、SIP セッションを終了する理由となる場合がある。

7.2. メディアストリームの追加・削除

UNI 上で確立されたメディアセッションは、発信側と着信側の間の SDP ネゴシエーションにより、1 種類のメディア形式（音声等)、または複数のメディアストリームとして異なるメディア形式 (音声と映像等)で開始する。通信期間中は、任意のメディアストリームの追加、削除が可能である。

8. コーデック

8.1. コーデックリスト

NGN の周辺にあるエンティティ（例えば NGN-TE）やメディアを終端する網装置は、エンド・トゥ・エンドのメディアセッションを確立するために、コーデックのネゴシエーションを行う機能を持つ必要がある。

NGN は、ネットワークからの推奨コーデックリストの範囲内でエンド・トゥ・エンドのネゴシエーションを許容しなければならない。また、そのネットワークポリシーに基づいて、推奨コーデックリストにないコーデックを許容しても良い。

(注 1) 本標準は、コーデックのネゴシエーションができない場合の手順を提供しない。

(注 2) NGN は、相互接続性を促進し、異なる事業者網間におけるコーデック変換の数を制限し、網リソースを有効利用するために、ユーザに推奨コーデックリストを提示することが望ましい。UNI 上で交換される SIP/SDP メッセージは、この推奨コーデックリスト内のひとつ以上のコーデックの使用希望を通知する。

推奨コーデックリストにないコーデックを含むメッセージや、推奨コーデックリストに含まれるコーデックを持たないメッセージの処理方法は、ネットワークポリシーに依存する。すなわち、推奨コ

ーデックリストにないコーデックの使用を許容する網もあれば、拒否する網もある場合がある。

本標準における推奨コーデックリストに関する記述は、端末が推奨コーデックリスト内の全コーデックをサポートしなければならないということを意味するものではない。また、事業者網がコーデック変換を目的として実装しなければならないコーデックを規定するものでもない。

SIP/SDP オファーが推奨コーデックリストに適合していても、コーデックネゴシエーションが成功するとは限らない。

(注 3) ネットワークポリシーにより UNI 上で利用できないコーデックがある場合には、注 2 に記述のとおり、ユーザにコーデックを推奨することが望ましい。そのような推奨が不可能な場合、推奨コーデックリストは G.711 A/μ law[G711]を含まなければならない。

(注 4) NGN は、音声通信を行うために、推奨コーデックリストに G.711A-law またはμ-law を含まなければならない。

ネットワークポリシーに基づき、推奨コーデックリスト内のいずれのコーデックが使用されても良い。ただし、推奨コーデックリストは AMR NB [EN 301 703]、EVRC [TIA-127]、G.729 [G.729]、G.729A [G.729A]、G.722.1 [G.722.1]、G.726 [G.726]および MPEG-4 Audio [ISO/IEC14496-3]を含むことが推奨される。

より高品位な音声サービスの提供を可能にするために、推奨コーデックリストは AMR-WB [G.722.2]、VMR-WB [TIA-1016]、G.722 [G.722]、G.729.1 [G.729.1]等の広帯域コーデックを含むことが強く推奨される。

聴覚に障がいのあるユーザをサポートするために、推奨コーデックリストは T.140 [T.140]を含むことが推奨される。既存 PSTN/ISDN と相互接続する場合、T.140 [T.140]は G.711 A/μ law [G/.711]上で伝達されるために変換されることが推奨される。

映像通信のために、推奨コーデックリストは、H.263 [H.263]、H.264 [H.264]及び MPEG-4 Visual [ISO/IEC 14496-2]を含むことが推奨される。

データ通信のために、事業者網がユーザに推奨するデータアプリケーションを示すことが推奨される。

(注 5) 個々のセッションに対して、エンド・トゥ・エンドのコーデックのネゴシエーションに関する可視性を持つ CSC-FE、アプリケーションサーバや IBC-FE のような呼制御信号装置は、エンドポイント間のコーデック変換の必要性を判定する場合があり、またコーデック変換を開始する場合がある。

(注 6) コーデック変換は可能な限り避けられるべきであるが、相互接続性を促進するために（例えば、エンドポイントにサポートされるコーデックが推奨コーデックリストにあるが、共通のコーデックが検出されない場合）、事業者網はコーデック変換をサポートする場合がある。

ただし、本標準における推奨コーデックリストに関する記述は、事業者網がコーデック変換を目的として実装しなければならないコーデックを規定するものではない。

8.2. パケット化

パケット化サイズが、端末間、網装置間、端末－網装置間のコーデックのネゴシエーションで選択されない、またはネットワークポリシーで推奨されない場合、G.711 の音声符号化には 10ms の音声パケット化サンプリングサイズが使用されるべきである。10ms という値は、ネットワーク運用下でのエンド・トゥ・エンドの遅延のバランスを取るための最適値として推奨されている。

ネットワークポリシーによってより大きい値が推奨される場合がある、ということが認識されている。そのような場合、20ms の値が推奨される。事業者網は、例えば 60ms のような、超えるべきではないパケット化サイズの上限に関するポリシーを持つべきである、ということも認識されている。

(注) パケット化サイズが、端末間、網装置間、端末－網装置間のコーデックのネゴシエーションによって選択される場合、本標準は選択される値に関して規定しない。

9. ルーチングとアドレス方式

表 9-1に、UNI でサポートされなければならない URI フォーマットを記載する。
その他のフォーマットは使用されても良い。

表9-1／JT-Q3402　URI フォーマット　（ITU-T Q.3402）

SIP URI	sip:userinfo@hostport;uri-parameters　(注 1)
	説明：”userinfo”,”hostport” 及び ”uri-parameters”は[RFC3261]の 25 章に基づき設定する。 ”userinfo”は国際 E.164 番号もしくは国内番号を含む。
	参照文書：[RFC 3261],[RFC 3966]
tel URI	tel:telephone-subscriber
	説明：telephone-subscriber は国際 E.164 番号もしくは国内番号を含む。
	参照文書：[RFC 3966]
注 1	“hostport”は、ドメイン名もしくは IP アドレスを含む。 また、“hostport”は port 番号を含んでも良い。

REGISTER メソッドにおいては、[RFC 3261]に規定されるように、Request-URI の SIP URI は”@”を含む”userinfo”を含んではならない。

10. サービス層シグナリングプロファイル

10.1. サポートする RFC 文書

表10-1／JT-Q3402　UNI における M/O/C コードの説明　（ITU-T Q.3402）

コード	コード名	定義内容
M	Mandatory	UNI は、リストされた RFC に準拠しなければならない。必須とされる RFC のエレメントの処理に関する詳細情報は、以下の当該従属節を参照のこと。
O	Optional	UNI は、リストされた RFC に準拠しても良い。
C	Conditional	UNI は、リストされた RFC について、コンテキストに基づき条件的に準拠しなければならない。必須とされる RFC の記述内容の処理に関するコンテキストは、以下の当該従属節を参照のこと。

表10-2／JT-Q3402　UNI でサポートする RFC　（ITU-T Q.3402）

種別	RFC 番号	タイトル	EUF	SCF
アイデンティティとプライバシー	RFC 3323	"A Privacy Mechanism for the Session Initiation Protocol (SIP)"	M (注 1)	M
	RFC 3324	Short Term Requirements for Network Asserted Identity	M (注 1)	M
	RFC 3325	"Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks"	M (注 1)	M
URI	RFC 3966	"The tel URI for Telephone Numbers"	M (注 2)	M (注 2)

	RFC 4715	The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI	O	O
	RFC 3824	Using E.164 numbers with the Session Initiation Protocol (SIP)	C1	C1
	RFC 4458	”Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)”	C2	C2
	RFC 5031	A Uniform Resource Name (URN) for Emergency and Other Well-Known Services	O	O
SIP と SIP 拡張	RFC 3261	"SIP: Session Initiation Protocol"	M	M
	RFC 3262	"Reliability of provisional responses in Session Initiation Protocol (SIP)"	C3	M
	RFC 3263	“Session Initiation Protocol (SIP): Locating SIP Servers"	C4	C4
	RFC 3264	"An Offer/Answer Model with Session Description Protocol (SDP)"	M	M
	RFC 3265	"Session Initiation Protocol (SIP) Specific Event Notification"	C5	C5
	RFC 3310	"Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"	C6	C6
	RFC 3311	"The Session Initiation Protocol (SIP) UPDATE method"	M (注 3)	M (注 3)
	RFC 3312	"Integration of resource management and Session Initiation Protocol (SIP)"	O	O
	RFC 3326	"The Reason Header Field for the Session Initiation Protocol (SIP)"	O	O
	RFC 3327	"Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts"	O	O
	RFC 3313	"Private Session Initiation Protocol (SIP) Extensions for Media Authorization"	O	O
	RFC 3320	"Signaling Compression (SigComp)"	O	O
	RFC 3515	"The Session Initiation Protocol (SIP) REFER method"	C7	C7
	RFC 3581	"An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing"	C8	C8
	RFC 3891	"The Session Initiation Protocol (SIP) "Replaces" Header"	C7	C7
	RFC 3892	"The Session Initiation Protocol (SIP) Referred-By Mechanism"	C7	C7
	RFC 4244	"An Extension to the Session Initiation Protocol for Request History Information"	C9 (注 4)	C9 (注 4)
	RFC 3959	The Early Session Disposition Type for the Session Initiation Protocol (SIP)	O	O
	RFC 3960	Early Media and Ringback Tone Generation in the Session Initiation Protocol	C10	C10
	RFC 3842	"A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)"	C11	C11
	RFC 4028	"Session Timers in the Session Initiation Protocol (SIP)"	M	M
	RFC 3725	“Best Current Practices for Third Party Call Control (3pcc)in the Session Initiation Protocol (SIP)”	O	O
	RFC 4730	“A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)”	O	O

	RFC 2617	"HTTP Authentication: Basic and Digest Access Authentication"	O (注 5)	O (注 5)
	RFC 2976	"The SIP INFO method"	O	O
	RFC 3911	"The Session Initiation Protocol (SIP) "Join" Header"	O	O
	RFC 3840	"Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"	O	O
	RFC 3841	"Caller Preferences for the Session Initiation Protocol (SIP)"	O	O
	RFC 3608	"Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration"	O	O
	RFC 3680	"A Session Initiation Protocol (SIP) Event Package for Registrations"	O	O
	RFC 3329	"Security Mechanism Agreement for the Session Initiation Protocol (SIP)"	O	O
	RFC 3455	"Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)"	O	O
	RFC 3485	"The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)"	O	O
	RFC 3486	"Compressing the Session Initiation Protocol (SIP)"	O	O
	RFC 3853	S/MIME AES Requirement for SIP	O	O
	RFC 4320	Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) non-INVITE Transaction	O (注 6)	O (注 6)
	RFC 4412	Communications Resource Priority for the Session Initiation Protocol (SIP)	O	O
	RFC 4483	A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages	O	O
	RFC 4032	"Update to the Session Initiation Protocol (SIP) Preconditions Framework"	O	O
	RFC 4235	An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP)	O	O
	RFC 4168	The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)	O	O
	RFC 5079	Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)	O	O
	RFC 5049	Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)	O	O
メディア記述	RFC 2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	O	O
	RFC 3388	"Grouping of Media Lines in Session Description Protocol"	O	O
	RFC 3420	"Internet Media Type message/sipfrag"	O	O
	RFC 3524	Mapping of Media Streams to Resource Reservation Flows	O	O
	RFC 3556	"Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth"	O	O
	RFC 4145	TCP-Based Media Transport in the Session Description Protocol (SDP)	O	O
	RFC 4566	"SDP: Session Description Protocol"	M (注 7)	M (注 7)

	RFC 4583	Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams	O	O
カンファレンス(会議機能)	RFC 4575	"A Session Initiation Protocol (SIP) Event Package for Conference State"	C12	C12
	RFC 4579	Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents	C13	C13
インスタントメッセージ	RFC 3428	"Session Initiation Protocol (SIP) Extension for Instant Messaging"	C14	C14
	RFC 3860	Common Profile for Instant Messaging (CPIM)	O	O
	RFC 3861	"Address Resolution for Instant Messaging and Presence"	O	O
	RFC 3862	Common Presence and Instant Messaging (CPIM): Message Format	O	O
	RFC 3994	Indication of Message Composition for Instant Messaging	O	O
プレゼンス	RFC 3903	"An Event State Publication Extension to the Session Initiation Protocol (SIP)"	C15	C15
	RFC 3856	"A Presence Event Package for the Session Initiation Protocol (SIP)"	C15	C15
	RFC 3857	"A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)"	O	O
	RFC 3858	An Extensible Markup Language (XML) Based Format for Watcher Information	O	O
	RFC 3859	Common Profile for Presence (CPP)	O	O
	RFC 3863	“Presence Information Data Format”	O	O
	RFC 4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)	O	O
	RFC 4662	"A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists"	O	O

C1:[RFC 3824]は、ENUM において、SIP-URI のフォーマットに対するガイドラインを使う場合に必須である。

C2:[RFC 4458]は、IVR を提供する場合に必須である。

C3:[RFC 3262]は、暫定応答の信頼性が要求される場合に必須である。

C4:[RFC 3263]は、管理された事業者網において、事前設定された端末装置もしくはアウトバンドプロキシのアドレスが登録期間に受信される場合、必須ではないが、その他の場合に必須である。

C5:[RFC 3265]は、メッセージウェイト通知のような、イベント通知が要求される場合に必須である。

C6:[RFC 3310]は、移動体ユーザ端末において必須である。一方、固定回線端末においては任意である。

C7:[RFC 3515]、[RFC 3891] 及び[RFC3892]は、参照を行うリクエストが要求される場合に必須である。

C8:[RFC 3581]は、NAT トラバーサルが要求される場合に必須である。

C9:[RFC 4244]は、呼転送が要求され、呼転送関連の情報が UNI を通じて伝達される場合に必須である。

C10:[RFC 3960]の 3 章は、P-early media ヘッダがサポートされている場合を除き、アナウンスの授受に関する、必須の指示に利用される場合に必須である。

C11:[RFC 3842]は、ボイスメール数の通知のようなメッセージ通知が要求される場合に必須である。

C12:[RFC 4575]は、会議機能が要求される場合に必須である。

C13:[RFC 4579] は、会議機能を利用する場合、会議機能のための規範的な RFC をサポートする方法を明確化するために必須である。

C14:[RFC 3428]は、インスタントメッセージが要求される場合に必須である。

C15:[RFC 3903]及び[RFC 3856]は、プレゼンス機能が要求される場合に必須である。

(注 1)　企業網に対し、[RFC 3323],[RFC 3324]及び[RFC 3325]をサポートすることは任意である。

(注 2) SIP URI がサポートされる場合でも、[RFC 3966]は、SIP URI における[E.164]ベースの userinfo 部のために必須である。

(注 3)　EUF 及び SCF は、[RFC 3311]に従わなければならない。Initial INVITE が確立する前にパラメータを更新するためには、UPDATE を使用しなければならない。Initial INVITE の確立後にパラメータを更新するためには、re-INVITE もしくは UPDATE を使用しなければならない。

UPDATE の使用条件は、ユーザが Allow ヘッダフィールドにて UPDATE のサポートを示していることである。相手側ユーザが新規オファーを受け付けるか拒否するかの選択を制限する意図がある場合、UPDATE を使用するべきである。

相手側ユーザが新規オファーを受け付けるか拒否するかを選択する機会を許容する意図がある場合、re-INVITE を使用するべきである。相手側が UPDATE をサポートしない場合、re-INVITE を使用しなければならない。

(注 4)　[RFC 4244]の代わりに、[RFC4458]が、一部の既存 SIP 実装でサポートされる。

(注 5)　ベーシック認証手順は使用してはならない。

(注 6) [RFC 4320]は、非 INVITE トランザクションを取り扱うために実装されることが推奨される。

(注 7) 例えば、m=data のような、[RFC 2327]のみに規定される規定事項が使用される場合、[RFC 2327]はサポートされなければならない。

10.2. SIP プロファイル

10.2.1. RFC3261 に基づく SIP プロファイル

本従属節は、UNI インタフェースにおける EUF 及び SCF が利用する SIP プロファイルを定義する。本従属節は、[RFC 3261]とその章番号の振り方に対応するよう構成されている。本従属節の番号は、4 桁目（すなわち、10.2.1.x の x）が[RFC 3261]の章番号と一致するように番号が振られている。また従属節のタイトルは[RFC 3261]の章タイトルと一致している。

本従属節は、[RFC 3261]に基づく実装に関して、一連の拡張および制限を定義する。

本標準で特に記述されない限り、EUF 及び SCF は[RFC 3261]に従って動作しなければならない。

10.2.1.1. Introduction

[RFC 3261]の 1 章はインフォメーショナル。

10.2.1.2. Overview of SIP Functionality

[RFC 3261]の 2 章はインフォメーショナル。

10.2.1.3. Terminology

[RFC 3261]の 3 章はインフォメーショナル。

10.2.1.4. Overview of Operation

[RFC 3261]の 4 章はインフォメーショナル。

10.2.1.5. Structure of the Protocol

[RFC 3261]の 5 章にあるプロトコルの構成はインフォメーショナル。

10.2.1.6. Definitions

[RFC 3261]の 6 章は、SIP に特別な意味を持つ用語を定義する。追加の定義用語は、本標準の3章で参照可能である。

本標準の利用者は、本従属節中の“クライアント”という用語は、UAC およびプロキシ両方を対象とすることに留意すること。

10.2.1.7. SIP Messages

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 7 章に従い SIP プロファイルを設定しなければならない。

10.2.1.7.1. Requests

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 7.1 章に従い SIP プロファイルを設定しなければならない。EUF 及び SCF は、INVITE、ACK、CANCEL 及び BYE をサポートしなければならない。

SCF は、UPDATE 及び PRACK をサポートしなければならない。EUF は UPDATE をサポートしなければならず、暫定応答の信頼性が要求される場合は、PRACK もサポートしなければならない。

EUF は REGISTER メソッドの送信をサポートしなければならない。SCF は REGISTER メソッドの受信をサポートしなければならない。OPTIONS メソッドはサポートされても良い。

Request-URI は、[RFC 3261]に既定される SIP URI、または[RFC 3966]に既定される tel URI でなければならない。SIPS URI フォーマットはサポートされても良い。

基本電話呼のための Initial INVITE の Request-URI は、tel URI もしくは SIP URI の telephone-subscriber 構文情報要素 （ユーザがダイヤルした電話番号）を用いて、着信ユーザを識別しなければならない。Request-URI が SIP URI の時、Request-URI のホスト部によって、SCF またはそのメッセージが送られるエンティティが特定できなければならない。

基本電話呼に関連するその他の（Initial INVITE 以外の）リクエストに設定される Request-URI は、Contact ヘッダで与えられる IP アドレスまたは FQDN を用いて、対象となるホストを識別しなければならない。

Request-URI のホスト部は通常、受信サーバのホスト名のひとつと一致する。ただし、受信された INVITE の Request-URI が一致しなければ、サーバは保持する翻訳情報や事前にプロビジョニングされたポリシー情報に基づき、リクエストを他のエンティティに中継するべきである。

(注) REGISTER における Request-URI は、[RFC3261]に規定されるように、”@”を含む”userinfo”を含んではならない。

10.2.1.7.2. Responses

EUF 及び SCF は、[RFC 3261]の 7.2 章に従い、SIP プロファイルを設定しなければならない。

10.2.1.7.3. Header Fields

EUF 及び SCF は、[RFC 3261]の 7.3 章に従い、SIP プロファイルを設定しなければならない。

10.2.1.7.4. Bodies

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 7.4 章に従い SIP プロファイルを設定しなければならない。

10.2.1.7.4.1 Message Body Types

EUF と SCF は、本従属節での記述を除き、[RFC 3261]の 7.4.1 章に従い、SIP プロファイルを設定しなければならない。

EUF と SCF は、メッセージボディタイプ"application/sdp"をサポートする SIP プロファイルを設定しなければならず、その他のメッセージボディタイプはサポートされても良い。

メッセージボディタイプ"application/sdp"は、INVITE メソッド、UPDATE メソッド、INVITE および UPDATE メソッドに対する失敗ではないレスポンスにおいてサポートされなければならない。

メッセージボディタイプ"application/sdp"は、H.323 網とのインタワークを許容する、また第三者呼制御（3PCC）を行なうサービスをサポートするために、PRACK メソッド、PRACK メソッドに対する失敗ではないレスポンスにおいてサポートされるべきである。

メッセージボディタイプ"application/sdp"は、上記のメソッドに対する 488(Not Acceptable Here)のようなエラーレスポンスでサポートされる場合がある。

10.2.1.7.4.2 Message Body Length

EUF 及び SCF は、[RFC 3261]の 7.4.2 章に従い、SIP プロファイルを設定しなければならない。

10.2.1.7.5. Framing SIP Messages

EUF と SCF は、[RFC 3261]の 7.5 章に従い、SIP プロファイルを設定しなければならない。

10.2.1.8. General User Agent Behaviour

本従属節および配下の従属節は、EUF が UAC または UAS として、SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ適用する。

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 8 章に従い動作しなければならない。

単一の呼に対する複数同時のメディアストリームのサポートは任意である。

本従属節で定義される動作は、ダイアログ外のリクエストおよびレスポンスにのみ適用されるということに留意すること。ダイアログ内の動作は、本標準の10.2.1.12節で定義される。

10.2.1.8.1. UAC Behaviour

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 8.1 節に従い動作しなければならない。

10.2.1.8.1.1. Generating the Request

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 8.1.1 節に従い動作しなければならない。

リクエスト内の Request-URI は、着信ユーザのアドレスを含む。これは通常、電話番号であるが、一般的な SIP URI であっても良い。 リクエスト内の From および To フィールドは、発信側ユーザのプライバシーを保護するランダムな文字列を含む場合がある。

利用できる各種ヘッダフィールド値の詳細については、10.2.1.20節を参照のこと。

10.2.1.8.1.2. Sending the Request

EUF 及び SCF は、[RFC 3261]の 8.1.2 章に従い動作しなければならない。

10.2.1.8.1.3. Processing Responses

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 8.1.3 章に従い動作しなければならない。

SIP 認証が要求される場合、EUF 及び SCF は、[RFC3261]の 8.1.3.5 章に従い、401(Unauthorized)による SIP 認証手順をサポートしなければならない。

407 (Proxy Authentication Required)による SIP 認証手順のサポートは任意である。サポートされる場合、[RFC 3261]の 8.1.3.5 章の規定に従う。

420 (Bad Extension) 受信時に使用される SIP リトライ手順のサポートは任意である。サポートされる場合、[RFC 3261]の 8.1.3.5 章の規定に従う。

10.2.1.8.2. UAS Behaviour

EUF 及び SCF は、[RFC 3261]の 8.2 章に従い動作しなければならない。

10.2.1.8.3. Redirect Servers

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 8.3 章に従い動作しなければならない。

SCF は、リダイレクトサーバ機能を提供しなくても良い。ただし、限られた数の INVITE リクエストに対して、リダイレクトサーバ機能を提供し、リダイレクションを起動する場合がある。リダイレクション数を制限する理由は、UNI 上の SIP 信号トラヒックとリダイレクションに付随する処理の複雑性を管理するためである。Max-Forwards ヘッダ（本標準の10.2.1.20節参照）は、全 SIP リクエストで必須であり、リクエストが宛先に向かう過程で取ることができるホップ数を制限する役割を果たす。リダイレクション機能がサポートされる場合、SCF は、[RFC 3261]の 8.3 章に従う。

3xx レスポンスコードは、事業者網、または INVITE メッセージを受信する後位網で起こる場合があるリダイレクションをサポートするために、事業者網のポリシーまたは加入オプションに基づき UNI でサポートされる場合がある。

10.2.1.9. Cancelling a Request

本従属節および配下の従属節では、プロキシに特有な処理は SCF が SIP プロキシとして動作する場合のみ、UA に特有な処理は EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ、そしてレジストラサーバに特有な処理は SCF がレジストラサーバとして動作する場合のみ適用する。

EUF 及び SCF は、[RFC 3261]の 9 章に従い動作しなければならない。

10.2.1.10. Registrations

本従属節および配下の従属節では、プロキシに特有な処理は SCF が SIP プロキシとして動作する場合のみ、UA に特有な処理は EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ、そしてレジストラサーバに特有な処理は SCF がレジストラサーバとして動作する場合のみ適用する。

EUF 及び SCF は、[RFC3261]の 10 章に従い動作をしなければならない。

10.2.1.11. Querying for Capabilities

本従属節および配下の従属節では、プロキシに特有な処理は SCF が SIP プロキシとして動作する場合のみ、

UA に特有な処理は EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ、そしてレジストラサーバに特有な処理は SCF がレジストラサーバとして動作する場合のみ適用する。

能力問い合わせのサポートは任意である。サポートされる場合、[RFC 3261]の 11 章に従う。

10.2.1.12. Dialogs

本従属節および配下の従属節は、EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ適用する。

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 12 章に従い動作しなければならない。

10.2.1.12.1. Creation of a Dialog

SIPS URI のサポートは任意である。サポートする場合、[RFC 3261]の 12.1 章に従う。

10.2.1.12.2. Requests within a Dialog

SIPS URI のサポートは任意である。サポートする場合、[RFC 3261]の 12.2 章に従う。

10.2.1.12.3. Termination of a Dialog

EUF 及び SCF は、[RFC 3261]の 12.3 章に従い動作しなければならない。

10.2.1.13. Initiating a Session

本従属節および配下の従属節は、EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ適用する。

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 13 章に従い動作しなければならない。

Initial INVITE 送信側の EUF は、Initial INVITE にメッセージボディタイプ"application/sdp"を可能な限り含むべきである。

SDP オファー無しの Initial INVITE のサポートは、H.323 網との相互接続を許容する、また第三者呼制御（3PCC）を行なうサービスをサポートするために推奨される。

コーデック選択をサポートするために、

- Initial INVITE が SDP オファーを含むとき、SDP アンサーは INVITE への信頼性のある暫定レスポンス（例えば信頼性を持って送信された 183-Session-Progress）か、または INVITE への非失敗最終レスポンス（例えば 2xx）に含まれても良い。SDP アンサーが信頼性のある暫定レスポンスに含まれない場合、非失敗最終レスポンスに含まれなければならない。非失敗最終レスポンスが SDP アンサーを含んでいる場合、同じ値の SDP が INVITE に対する信頼性のない非失敗暫定レスポンスに設定される場合がある。
- Initial INVITE が SDP オファーを含まないとき、最初の SDP オファーは INVITE への最初の信頼性のある暫定レスポンスに含まれなければならない。これは、含まる場合は信頼性を持って送信される最初の 18x 応答（例えば信頼性を持って送信された 180-Ringing）、含まれない場合は INVITE への非失敗最終レスポンス（例えば 2xx）にある。最初の SDP オファーが信頼性のある暫定応答に含まれる場合、SDP アンサーはこの応答の到着確認を行なう PRACK メッセージに含まれなければならない。最初の SDP オファーが INVITE への非失敗最終レスポンス（例えば 2xx）に含まれる場合、SDP アンサーはこの応答の到着確認を行なう ACK メッセージに含まれなければならない。

10.2.1.14. Modifying an Existing Session

本従属節および配下の従属節は、EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ適用する。

EUF 及び SCF は、本従属節の記述を除き、[RFC 3261]の 14 章に従い動作しなければならない。

re-INVITE または UPDATE メソッドに含まれる新規に受信した SDP オファーへの SDP アンサー構築時、転送プレーンを制御する SCF 及び EUF は、最初の SDP のネゴシエーション手順で取り決められた受信 IP アドレスやポート番号を変更するべきでない。

10.2.1.15. Terminating a Session

本従属節および配下の従属節は、EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ適用する。

EUF 及び SCF は、[RFC 3261]の 15 章に従い動作しなければならない。

10.2.1.16. Proxy Behaviour

本従属節および配下の従属節は、SCF が SIP プロキシとして動作する場合のみ適用する。

SCF は、本従属節での記述を除き、[RFC 3261]の 16 章に従い動作しなければならない。

単一の呼に対する複数同時メディアストリームのサポートは任意である。

10.2.1.17. Transactions

本従属節および配下の従属節では、プロキシに特有な処理は SCF が SIP プロキシとして動作する場合のみ、UA に特有な処理は EUF が UAC または UAS として、また SCF が B2BUA またはリダイレクトサーバとして動作する場合のみ、そしてレジストラサーバに特有な処理は SCF がレジストラサーバとして動作する場合のみ適用する。

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 17 章に従い動作しなければならない。

EUF 及び SCF は、ユーザに対するダイアログが既に存在し、新規 INVITE がそのダイアログの一部でない場合、そのユーザへの INVITE リクエストにエラーコード 486（Busy Here）を返す場合がある。

10.2.1.18. Transport

EUF 及び SCF は、[RFC 3261]の 18 章に従い動作しなければならない。ただし、[RFC 3261]の 18 章と不整合がある場合は本標準の12章が常に優先される。

10.2.1.19. Common Message Components

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 19 章に従い SIP プロファイルを設定しなければならない。

SIPS URI のサポートは任意である。サポートされる場合、[RFC 3261]の 19.1.1 章の規定に従う。

10.2.1.20. Header Fields

EUF 及び SCF は、本従属節での記述を除き、[RFC 3261]の 20 章に従い SIP プロファイルを設定しなければならない。

配下の従属節に、[RFC 3261]で定義される SIP ヘッダが列挙され、EUF 及び SCF でそれらをサポートするための要求条件が規定される。

10.2.1.20.1. Accept

Accept ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.1 章の規定に従う。

10.2.1.20.2. Accept-Encoding

Accept-Encoding ヘッダのサポートは任意である。サポートされる場合、以下の記述を除き、[RFC 3261]の 20.2 章の規定に従う。

Accept-Encoding ヘッダは、EUF 及び SCF によって使用される場合がある。"identity"はサポートされなければならず、その他のエンコーディング値はサポートされても良い。

10.2.1.20.3. Accept-Language

Accept-Language ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.3 章の規定に従う。

10.2.1.20.4. Alert-Info

Alert-Info ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.4 章の規定に従う。

[RFC 3261]の 20.4 章に記述があるように、Alert-Info ヘッダの利用に伴うセキュリティリスクが存在することに留意すること。

10.2.1.20.5. Allow

Allow ヘッダは、以下の記述を除き、[RFC 3261]の 20.5 章の規定通りにサポートされなければならない。

Allow ヘッダは、Initial INVITE および Initial INVITE への 2xx レスポンスに存在しなければならない。

ヘッダ値は、サポートされるメソッドを全て（例えば、INVITE、ACK、CANCEL、BYE、UPDATE および PRACK）を列挙しなければならない。

ただし、EUF 及び SCF は Allow ヘッダフィールドが無いメッセージの受信に対して備える必要がある。

EUF 及び SCF は、Initial INVITE 及び Initial INVITE に対する 2xx レスポンスに Allow ヘッダが存在しない場合でも呼制御を継続するべきである。

10.2.1.20.6. Authentication-Info

Authentication-Info ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.6 章の規定に従う。

10.2.1.20.7. Authorization

SIP 認証が要求される場合、[RFC3261]の 20.7 章に従い、EUF は Authorization ヘッダの送信をサポートしなければならず、SCF は Authorization ヘッダの受信をサポートしなければならない。

EUF における Authrization ヘッダの送受信両方のサポート、また、SCF における Authorization ヘッダ送信のサポートは任意である。サポートされる場合、[RFC 3261]の 20.7 章の規定に従う。

10.2.1.20.8. Call-ID

Call-ID ヘッダは、以下の記述を除き、[RFC 3261]の 20.8 章の規定通りにサポートされなければならない。

Call-ID 値は、[RFC 3261]の 8.1.1.4 章に記述の通りグローバルに一意でなければならず、また[RFC 3323]の 4.1 章に記述の通り、プライバシー保護のために、Call-ID に IP アドレスやホスト名を記載する代わりに適切な長さのランダム値（リクエストの From ヘッダのための'tag'として使われる値が再利用されるかもしれない）を使用すべきである。発信側ユーザがプライバシーを要求する場合、発信側 EUF はプライバシーが保護された Call-ID を使用するべきである。

10.2.1.20.9. Call-Info

Call-Info ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.9 章の規定に従う。

[RFC 3261]の 20.9 章に記述があるように、Call-Info ヘッダの利用に伴うセキュリティリスクが存在することに留意すること。

10.2.1.20.10. Contact

Contact ヘッダは、以下の記述を除き、[RFC 3261]の 20.10 章の規定通りにサポートされなければならない。

EUF 及び SCF は、INVITE リクエスト、信頼性のある暫定応答および INVITE リクエストへの 2xx レスポンス内の Contact ヘッダが SIP URI を持つように SIP プロファイルを設定しなければならない。その他の種類の URI のサポートは任意である。

ユーザがプライバシーを要求する時、Contact ヘッダはいかなるドメイン名も含むべきではなく、代わりに IP アドレス形式が使用されるべきである。複数の網インタフェースを持つシステムでは、（単一の）IP アドレス形式の使用はシステム全体の信頼性を低下させ得ることに留意するべきである。複数のインタフェースが存在し信頼性が懸念される場合は、IP アドレス形式の使用を控えることが適切な代替案であると考えられる。

EUF 及び SCF は、INVITE リクエストへの 3xx レスポンスの Contact ヘッダが有効な SIP URI または tel URI を持つように SIP プロファイルを設定しなければならない。新しい宛先が電話番号の場合、本標準の10.2.1.7.1節の記述通りに、新しい宛先の電話番号を持つ SIP URI または tel URI を含まなければならない。その他の種類の URI のサポートは任意である。

10.2.1.20.11. Content-Disposition

Content-Disposition ヘッダのサポートは任意である。サポートされる場合、以下の記述を除き、[RFC 3261]の 20.11 章の規定に従う。

Content-Disposition ヘッダは、EUF 及び SCF によって使用される場合がある。"session"はサポートされなければならず、その他の値はサポートされても良い。

[RFC 3959]に定義されるアプリケーションサーバモデルにより、アーリーメディアが提供される場合、Content-Disposition ヘッダは、[RFC 3959]に規定されているように、" early-session "を含まなければならない。メッセージボディタイプ"application/sdp"の初期値は"session"、一方その他全てのメッセージボディタイプ（"message/sipfrag"等）の初期値は"render"であることに留意すること。初期値を望まない場合は、Content-Disposition ヘッダを含まなければならない。

10.2.1.20.12. Content-Encoding

Content-Encoding ヘッダのサポートは任意である。サポートされる場合、以下の記述を除き、[RFC 3261]の 20.12 章の規定に従う。

Content-Encoding ヘッダは EUF 及び SCF によって使用される場合がある。"identity"はサポートされなければならず、その他のエンコーディング値はサポートされても良い。

10.2.1.20.13. Content-Language

Content-Language ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.13 章の規定に従う。

10.2.1.20.14. Content-Length

Content-Length ヘッダは、[RFC 3261]の 20.14 章の規定通りにサポートされなければならない。

10.2.1.20.15. Content-Type

Content-Type ヘッダは、以下の記述を除き、[RFC 3261]の 20.15 章の規定通りにサポートされなければならない。

"application/sdp"はサポートされなければならず、その他の値はサポートされても良い。

[RFC 3959]に定義されるアプリケーションサーバモデルにより、アーリーメディアが提供される場合、様々なセッション形式 (通常のセッションと early セッションなど) を指定するため、[RFC 2046]に規定されているようにコンテンツ型式"multipart/mixed"はサポートされなければならない。各コンテンツ型式は、本ヘッダにおいて"boundary"tag の使用により、その指定内容を囲む。

10.2.1.20.16. CSeq

CSeq ヘッダは、[RFC 3261]の 20.16 章の規定通りにサポートされなければならない。

10.2.1.20.17. Date

Date ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.17 章の規定に従う。

10.2.1.20.18. Error-Info

Error-Info ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.18 章の規定に従う。

[RFC 3261]の 20.18 章に記述があるように、Error-Info ヘッダの利用に伴うセキュリティリスクが存在することに留意すること。

10.2.1.20.19. Expires

Expires ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.19 章の規定に従う。

10.2.1.20.20. From

From ヘッダは、以下の記述を除き、[RFC 3261]の 20.20 章の規定通りにサポートされなければならない。

ユーザプライバシーのサポートのため、SCF は From ヘッダが許容する内容を制限する。

セッション開始者がプライバシーを要求する時、EUF は以下の規則に従って From ヘッダを生成するべきである。

- display-name は"Anonymous"でも良い。
- addr-spec は userinfo に識別子"anonymous"を含まなければならない。
- addr-spec は匿名ホスト名"anonymous.invalid"を含まなければならない。

10.2.1.20.21. In-Reply-To

In-Reply-To ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.21 章の規定に従う。

10.2.1.20.22. Max-Forwards

EUF での Max-Forwards ヘッダ受信のサポートは任意である。サポートされる場合、[RFC 3261]の 20.22 章の規定に従う。EUF は Max-Forwards ヘッダの送信を、[RFC3261]の 20.22 章に従いサポートしなければならない。

SCF は、以下の記述を除き、[RFC 3261]の 20.22 章の規定通りに Max-Forwards ヘッダをサポートしなければならない。

SCF 内の B2BUA がリクエストを転送する時、入 Max-Forwards 値から 1 を引いた値に等しい Max-Forwards 値を使用しなければならない。

10.2.1.20.23. Min-Expires

[RFC3261]の 20.23 章に従い、EUF は Min-Expires ヘッダの受信をサポートしなければならず、SCF は Min-Expires ヘッダの送信をサポートしなければならない。

EUF から SCF 方向への Min-Expires ヘッダは適用不可である。

10.2.1.20.24. MIME-Version

MIME-Version ヘッダのサポートは任意である。サポートされる場合、以下の記述を除き、[RFC 3261]の 20.24 章の規定に従う。

バージョン値"1.0"はサポートされなければならず、その他のバージョン値はサポートされても良い。

10.2.1.20.25. Organization

Organization ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.25 章の規定に従う。

10.2.1.20.26. Priority

Priority ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.26 章の規定に従う。

このヘッダを利用するエンティティに対し、セキュリティ上の悪影響があることに留意すること。

10.2.1.20.27. Proxy-Authenticate

EUF での Proxy-Authenticate ヘッダの受信のサポート、SCF での Proxy-Authenticate ヘッダの送信のサポートは任意である。

サポートされる場合、[RFC 3261]の 20.27 章の規定に従う。

EUF から SCF 方向への Proxy-Authenticate ヘッダは適用不可である。

10.2.1.20.28. Proxy-Authorization

EUF での Proxy-Authorization ヘッダの送信のサポート、SCF での Proxy-Authorization ヘッダの受信のサポートは任意である。サポートされる場合、[RFC 3261]の 20.28 章の規定に従う。

SCF から EUF 方向への Proxy-Authorization ヘッダは適用不可である。

10.2.1.20.29. Proxy-Require

SCF は、Proxy-Require ヘッダの受信をサポートしなければならない。EUF での Proxy-Require ヘッダの送受信両方のサポート、SCF での Proxy-Require ヘッダの送信のサポートは任意である。

サポートされる場合、以下の記述を除き、[RFC 3261]の 20.29 章の規定に従う。

"privacy"は[RFC3323]に従いサポートされなければならず、その他の option-tag 値はサポートされても良い。

10.2.1.20.30. Record-Route

Record-Route ヘッダは、[RFC 3261]の 20.30 章の規定通りにサポートされなければならない。

10.2.1.20.31. Reply-To

Reply-To ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.31 章の規定に従う。

10.2.1.20.32. Require

Require ヘッダは、以下の記述を除き、[RFC 3261]の 20.32 章の規定通りにサポートされなければならない。

"timer" は、[RFC 4028]に従い、EUF 及び SCF によってサポートされなければならない。

"100rel" は、[RFC 3262]に従い、EUF は暫定応答の信頼性が要求される場合にサポートしなければならず、SCF はサポートしなければならない。その他の option-tag 値はサポートされても良い。

[RFC 3959]に定義されるアプリケーションサーバモデルにより、アーリーメディアが提供され、UAC がアーリーメディアの要求の処理をサポートすることを UAS に期待する場合、Require ヘッダは[RFC 3959]に規定されるように、"early-session"を含まなければならない。

10.2.1.20.33. Retry-After

Retry-After ヘッダのサポートは任意である。サポートされる場合、以下の記述を除き、[RFC 3261]の 20.33 章の規定に従う。

REGISTER リクエストの送信後、EUF は Retry-After ヘッダを伴ったエラーレスポンスを受信する場合がある。そのような場合、Retry-After ヘッダに指定される時間が経過した後にリクエストを再送信することが推奨される。

10.2.1.20.34. Route

[RFC3261]の 20.34 章に従い、EUF は Route ヘッダの送信をサポートしなければならず、SCF は Route ヘッダの受信をサポートしなければならない。

SCF から EUF 方向への Route ヘッダは適用不可である。

10.2.1.20.35. Server

Server ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.35 章の規定に従う。

10.2.1.20.36. Subject

Subject ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.36 章の規定に従う。

10.2.1.20.37. Supported

Supported ヘッダは、以下の記述を除き、[RFC 3261]の 20.37 章の規定通りにサポートされなければならない。

"timer"は、[RFC4028]に従いサポートしなければならない。

"100rel" は、[RFC3262]に従い、EUF は暫定応答の信頼性が要求される場合にサポートしなければならず、SCF はサポートしなければならない。その他の option-tag 値はサポートされても良い。

[RFC 3959]に定義されるアプリケーションサーバモデルにより、アーリーメディアが提供される場合、Supported ヘッダは、[RFC 3959]に規定されるように、"early-session"を含まなければならない。

10.2.1.20.38. Timestamp

Timestamp ヘッダのサポートは任意である。サポートされる場合、以下の記述を除き、[RFC 3261]の 20.38 章の規定に従う。

EUF 及び SCF はリクエストで Timestamp ヘッダを送信する場合がある。受信される際、このヘッダは[RFC 3261]の 20.38 章の記述に従って処理されなければならない。

10.2.1.20.39. To

To ヘッダは、以下の記述を除き、[RFC 3261]の 20.39 章の規定通りにサポートされなければならない。

ユーザプライバシーのサポートのため､EUF 及び SCF は To ヘッダに設定する内容を制限しても良い｡通常、To ヘッダは SIP URI または tel URI でダイヤル番号を示す。この情報はエンド・トゥ・エンドで重要であり、発信者の位置に関する情報、例えば企業、ローカル、長距離、または国際かを明かす場合もある。

発信側がプライバシーを要求する場合、EUF 及び SCF は、以下の規則に従って To ヘッダを生成しても良い。

- display-name は存在してはならない。
- 国際電話番号が使用される場合、addr-spec の userinfo 部は、国番号を含む完全な E.164 番号を含まなければならない。
- addr-spec のホスト部は、匿名ホスト名"anonymous.invalid"を含まなければならない。

発信側によって匿名性が要求されない場合、またユーザが電話番号をダイヤルした場合、To ヘッダはダイヤル番号を持つ SIP URI または tel URI を含むべきである。

10.2.1.20.40. Unsupported

Unsupported ヘッダは、[RFC 3261]の 20.40 章の規定通りにサポートされなければならない。

10.2.1.20.41. User-Agent

User-Agent ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.41 章の規定に従う。

10.2.1.20.42. Via

Via ヘッダは、[RFC 3261]の 20.42 章の規定通りにサポートされなければならない。

10.2.1.20.43. Warning

Warning ヘッダのサポートは任意である。サポートされる場合、[RFC 3261]の 20.43 章の規定に従う。

10.2.1.20.44. WWW-Authenticate

SIP 認証が要求される場合、[RFC 3261]の 20.44 章に従い、EUF は WWW-Authenticate ヘッダの受信をサポートしなければならず、SCF は WWW-Authenticate ヘッダの送信をサポートしなければならない。

EUF での WWW-Authenticate ヘッダの送信のサポート及び、SCF での WWW-Authenticate ヘッダの受信のサポートは任意である。サポートされる場合、[RFC3261]の 20.44 章の規定に従う。

10.2.1.21. Response Codes

EUF 及び SCF は、[RFC 3261]の 21 章に従い SIP プロファイルを設定しなければならない。

10.2.1.22. Usage of HTTP Authentication

HTTP Authentication のサポートは任意である。サポートされる場合、[RFC 3261]の 22 章の規定に従う。

10.2.1.23. S/MIME

S/MIME のサポートは任意である。使用される場合、[RFC 3261]の 23 章の規定に従う。

10.2.1.24. Examples

[RFC 3261]の 24 章はインフォメーショナルである。

10.2.1.25. Augmented BNF for the SIP Protocol

EUF 及び SCF は、[RFC 3261]の 25 章に従い SIP プロファイルを設定しなければならない。

10.2.2. RFC3261 の拡張に関する SIP プロファイル

本従属節は、10.1 節に列挙されている、[RFC 3261]以外でサポートが必須の RFC で定義される拡張メソッド、ヘッダ、そしてレスポンスコードを規定する。RFC のサポートが任意の場合、それらの RFC で定義されるメソッド、ヘッダ、そしてレスポンスコードのサポートも任意となるため、個別に記述しない。

10.2.2.1. 拡張メソッド

SCF は、UPDATE 及び PRACK をサポートしなければならない。EUF は UPDATE をサポートしなければならず、信頼性のある暫定応答が要求される場合は、PRACK もサポートしなければならない。

10.2.2.1.1. UPDATE

EUF 及び SCF は、[RFC 3311]に規定されるように UPDATE をサポートしなければならない。

Initial INVITE の確立前にセッションパラメータを更新するためには、UPDATE が使用されなければならない。Initial INVITE の確立後は、re-INVITE または UPDATE を使用しても良い。セッションパラメータの更新には re-INVITE を利用することを推奨する。

特に、通信中は、様々なメディアの追加、削除は、UPDATE の代わりに、SDP オファー/アンサー手順に従って、変更された SDP プロファイルを含む新しいメディア記述を備えた re-INVITE を使用して実行されるべきである。

10.2.2.1.2. PRACK

SCF は、[RFC3262]に従い PRACK メソッドをサポートしなければならない。

信頼性のある暫定応答が要求される場合、EUF は、[RFC 3262]に規定されるように PRACK メソッドをサポートしなければならない。送信側の EUF が、信頼性のある暫定応答を保証するために、"100rel"を伴った Require ヘッダを含むイニシャルリクエストを送信する場合、受信側の EUF は暫定応答に"100rel "を伴った Require ヘッダを含めなければならない。100 Trying 以外の暫定応答が"100rel"を伴った Require ヘッダを含んでいる場合、送信側の EUF は[RFC 3262]に従い、PRACK を返送しなければならない。

送信側の EUF が "100rel"を伴った Supported ヘッダを含むイニシャルリクエストを送信した場合、受信側の EUF は、INVITE に対し、100 Trying 以外のいかなる暫定応答も信頼性を持って送信して良い。100 Trying 以外の暫定応答中の Require ヘッダが"early-session"または"precondition"を含む場合、Supported ヘッダフィールドに"100rel "を含まなければならない。

10.2.2.2. 拡張ヘッダ

10.2.2.2.1. Min-SE

Min-SE ヘッダフィールドは、delta-second 単位で、セッション間隔の最小値を通知する。

EUF での Min-SE ヘッダの送信のサポートは任意である。サポートされる場合、[RFC 4028]の規定に従う。EUF は[RFC 4028]に従い Min-SE ヘッダの受信をサポートしなければならない。

SCF は、[RFC 4028]に従い Min-SE ヘッダをサポートしなければならない。

10.2.2.2.2. P-Asserted-Identity

P-Asserted-Identity ヘッダフィールドは認証による検証を経て、SIP メッセージを送信するユーザのアイデンティティを信頼できる SIP エンティティ間で伝達するために使用される。

[RFC 3325]に従い、EUF は P-Asserted-Identity ヘッダの受信をサポートしなければならず、SCF は P-Asserted-Identity ヘッダの送信をサポートしなければならない。

EUF から SCF 方向への P-Asserted-Identity ヘッダは適用不可である。

10.2.2.2.3. P-Preferred-Identity

P-Preferred-Identity ヘッダフィールドは、UA が信頼できるプロキシに対して、P-Asserted-Identity ヘッダフィールドに設定したいアイデンティティを通知するために使用される。

EUF での P-Preferred-Identity ヘッダの送信のサポートは任意である。サポートされる場合、[RFC 3325]の規定に従わなければならない。

SCF は[RFC 3325]に従い P-Prefered-Idenitty ヘッダの受信をサポートしなければならない。

SCF から EUF 方向の P-Preferred-Identity ヘッダは、適用不可である。

10.2.2.2.4. Privacy

Privacy ヘッダは、UA がメッセージに一定のプライバシーを要求することを可能にする。

EUF は Privacy ヘッダの受信をサポートしなければならず、SCF は Privacy ヘッダの送受信の両方をサポートしなければならない。EUF での Privacy ヘッダの送信のサポートは任意である。サポートされる場合、以下の記述を除き、[RFC 3323]の規定通りにサポートされなければならない。

プライバシーオプションの"id"の適用はサポートされなければならない。その他のプライバシーオプションは、事業者網のポリシーまたは加入オプションに基づきサポートされても良い。

10.2.2.2.5. RAck

RAck ヘッダは、信頼性のある暫定応答をサポートするために、PRACK リクエストで送信される。

[RFC 3262]に規定されるように、暫定応答の信頼性が要求される場合、EUF は RAck ヘッダをサポートしなければならず、また SCF は[RFC 3262]に従ってサポートしなければならない。

10.2.2.2.6. RSeq

RSeq ヘッダは、暫定応答において、それらを信頼性を持って送信するため使用される。

[RFC 3262]に規定されるように、暫定応答の信頼性が要求される場合、EUF は RSeq ヘッダをサポートしなければならず、また SCF は[RFC 3262]に従ってサポートしなければならない。

10.2.2.2.7. Session-Expires

Session-Expires ヘッダフィールドは、SIP セッションのセッション間隔を伝達する。

Session-Expires ヘッダは、[RFC 4028]の規定通りにサポートされなければならない。

10.2.2.3. 拡張レスポンスコード

10.2.2.3.1. 422 (Session Interval Too Small)

EUF での 422 (Session Interval Too Small)の送信のサポートは任意である。サポートする場合、[RFC 4028]の規定通りにサポートしなければならない。

EUF は、[RFC 4028]に従い 422 (Session Interval Too Small)の受信をサポートしなければならない。

SCF は、[RFC 4028]に従い 422 (Session Interval Too Small)をサポートしなければならない。

10.2.3. SIP メソッド及びヘッダの概要

以下の SIP メソッドおよびヘッダのサポートは、表 10-3,表 10-4 ,表 10-5 および表 10-6の規定通りに、必須、任意または適用不可である。

提示されている SIP メソッドまたはヘッダの送受信のサポートとは、メソッドまたはヘッダが UNI 上の SIP メッセージに設定される場合があることを意味し、UNI 上の SIP メッセージに、そのヘッダが常に存在することを意味するものではない。

(注)レスポンスのサポートに関する情報については、[RFC 3261]を参照のこと。

表10-3／JT-Q3402　RFC 3261 メソッド　（ITU-T Q.3402）

メソッド	EUF->SCF		SCF->EUF		参照先
	EUF 送信	SCF 受信	SCF 送信	EUF 受信	
ACK	M	M	M	M	10.2.1.7.1 を参照
BYE	M	M	M	M	10.2.1.7.1 を参照
CANCEL	M	M	M	M	10.2.1.7.1 を参照
INVITE	M	M	M	M	10.2.1.7.1 を参照
OPTIONS	O	O	O	O	10.2.1.7.1 を参照
REGISTER	M	M	N/A	N/A	10.2.1.7.1 を参照

表10-4／JT-Q3402　拡張メソッド　（ITU-T Q.3402）

メソッド	EUF->SCF		SCF->EUF		参照先	RFC
	EUF 送信	SCF 受信	SCF 送信	EUF 受信		
PRACK	C	M	M	C	10.2.1.7.1 を参照	RFC 3262
UPDATE	M	M	M	M	10.2.1.7.1 を参照	RFC 3311

C:信頼性のある暫定応答が要求される場合に必須である。

表10-5／JT-Q3402　RFC3261 ヘッダ　（ITU-T Q.3402）

ヘッダ	EUF->SCF		SCF->EUF		参照先
	EUF 送信	SCF 受信	SCF 送信	EUF 受信	
Accept	O	O	O	O	10.2.1.20.1 節を参照
Accept-Encoding	O	O	O	O	10.2.1.20.2 節を参照
Accept-Language	O	O	O	O	10.2.1.20.3 節を参照
Alert-Info	O	O	O	O	10.2.1.20.4 節を参照
Allow	M	M	M	M	10.2.1.20.5 節を参照
Authentication-Info	O	O	O	O	10.2.1.20.6 節を参照
Authorization	C	C	O	O	10.2.1.20.7 節を参照
Call-ID	M	M	M	M	10.2.1.20.8 節を参照
Call-Info	O	O	O	O	10.2.1.20.9 節を参照
Contact	M	M	M	M	10.2.1.20.10 節を参照
Content-Disposition	O	O	O	O	10.2.1.20.11 節を参照
Content-Encoding	O	O	O	O	10.2.1.20.12 節を参照
Content-Language	O	O	O	O	10.2.1.20.13 節を参照
Content-Length	M	M	M	M	10.2.1.20.14 節を参照
Content-Type	M	M	M	M	10.2.1.20.15 節を参照
CSeq	M	M	M	M	10.2.1.20.16 節を参照
Date	O	O	O	O	10.2.1.20.17 節を参照
Error-Info	O	O	O	O	10.2.1.20.18 節を参照
Expires	O	O	O	O	10.2.1.20.19 節を参照
From	M	M	M	M	10.2.1.20.20 節を参照
In-Reply-To	O	O	O	O	10.2.1.20.21 節を参照
Max-Forwards	M	M	M	O	10.2.1.20.22 節を参照
Min-Expires	N/A	N/A	M	M	10.2.1.20.23 節を参照
MIME-Version	O	O	O	O	10.2.1.20.24 節を参照
Organization	O	O	O	O	10.2.1.20.25 節を参照
Priority	O	O	O	O	10.2.1.20.26 節を参照
Proxy-Authenticate	N/A	N/A	O	O	10.2.1.20.27 節を参照
Proxy-Authorization	O	O	N/A	N/A	10.2.1.20.28 節を参照
Proxy-Require	O	M	O	O	10.2.1.20.29 節を参照
Record-Route	M	M	M	M	10.2.1.20.30 節を参照
Reply-To	O	O	O	O	10.2.1.20.31 節を参照
Require	M	M	M	M	10.2.1.20.32 節を参照
Retry-After	O	O	O	O	10.2.1.20.33 節を参照
Route	M	M	N/A	N/A	10.2.1.20.34 節を参照
Server	O	O	O	O	10.2.1.20.35 節を参照
Subject	O	O	O	O	10.2.1.20.36 節を参照

ヘッダ	EUF->SCF		SCF->EUF		参照先
	EUF 送信	SCF 受信	SCF 送信	EUF 受信	
Supported	M	M	M	M	10.2.1.20.37 節を参照
Timestamp	O	O	O	O	10.2.1.20.38 節を参照
To	M	M	M	M	10.2.1.20.39 節を参照
Unsupported	M	M	M	M	10.2.1.20.40 節を参照
User-Agent	O	O	O	O	10.2.1.20.41 節を参照
Via	M	M	M	M	10.2.1.20.42 節を参照
Warning	O	O	O	O	10.2.1.20.43 節を参照
WWW-Authenticate	O	O	C	C	10.2.1.20.44 節を参照

C: SIP 認証が要求される場合に必須である。

表10-6／JT-Q3402　拡張ヘッダ　（ITU-T Q.3402）

ヘッダ	EUF->SCF		SCF->EUF		参照先	RFC
	EUF 送信	SCF 受信	SCF 送信	EUF 受信		
Min-SE	O	M	M	M	10.2.2.2.1 節を参照	RFC 4028
P-Asserted-Identity	N/A	N/A	M	M	10.2.2.2.2 節を参照	RFC 3325
P-Preferred-Identity	O	M	N/A	N/A	10.2.2.2.3 節を参照	RFC 3325
Privacy	O	M	M	M	10.2.2.2.4 節を参照	RFC 3323
RAck	C	M	M	C	10.2.2.2.5 節を参照	RFC 3262
RSeq	C	M	M	C	10.2.2.2.6 節を参照	RFC 3262
Session-Expires	M	M	M	M	10.2.2.2.7 節を参照	RFC 4028

C: 暫定応答の信頼性が要求される場合に必須である。

上記の表における、M、O、C 及び N/A は、以下の意味を持つ：

表10-7／JT-Q3402　表 10-3,10-4,10-5 および 10-6 におけるコードの説明　（ITU-T Q.3402）

コード	コード名	EUF->SCF		SCF->EUF	
		EUF 送信	SCF 受信	SCF 送信	EUF 受信
M	Mandatory	能力はサポートされなければならない。 EUF は要求される場合、送信可能でなければならない。	能力はサポートされなければならない。 UNI での SCF における SIP メッセージまたはヘッダの受信のサポートとは、UNI から受信される場合に、このメッセージまたはヘッダが期待する処理をしなければならないことを意味する。 着側網内の網装置またはこの網	能力はサポートされなければならない。 UNI での SCF における SIP メッセージまたはヘッダの送信のサポートとは、網内から受信した場合に、このメッセージまたはヘッダを UNI へ送信しなければならないことを意味する。 着側網内の網装置またはこの網	能力はサポートされなければならない。 要求されている情報が適用不可能な場合、処理は継続されるべきではない。（適切な切断/解放処理が行なわれるべきである。）しかしながら、初期値が決定されている時、処理は初期値を使用して行なわれる。

コード	コード名	EUF->SCF		SCF->EUF	
		EUF 送信	SCF 受信	SCF 送信	EUF 受信
			に接続されているユーザ装置が、このメッセージやヘッダをサポートしなければならないことを意図するのではない。 要求されている情報が適用不可能な場合、処理は継続されるべきではない。（適切な切断/解放処理が行なわれるべきである。） しかしながら、初期値が決定されている場合、処理は初期値を使用して行なわれる。	に接続されるユーザ装置が、このメッセージやヘッダをサポートしなければならないことを意図するのではない。	
O	Optional	能力は UNI での EUF でサポートされて良いし、サポートされなくても良い。 これは実装にて選択可能である。	能力は UNI での SCF でサポートされて良いし、サポートされなくても良い。 これは実装にて選択可能である。 可能であれば、送信側の EUF が期待する処理が実行されるべきである。 EUF が期待する処理が実行されない時、受信された内容は無視され、処理を継続するべきである。	能力は UNI での SCF でサポートされて良いし、サポートされなくても良い。 これは実装にて選択可能である。	送信側の EUF に同じ。 可能であれば、送信側の SCF が期待する処理が実行されるべきである。 . SCF が期待する処理が実行されない時、受信された内容は無視され、処理を継続するべきである。
C<integer>	Conditional	機能の要求条件("M","O")は、その他の任意または条件付き項目に依存している。 <整数>は条件付きを表す記号である。	送信側の EUF に同じ。	送信側の EUF に同じ。	送信側の EUF に同じ。
N/A	Not Applicable	能力の使用は不可能である。サポート欄への回答は要求されない。	送信側の EUF に同じ。	送信側の EUF に同じ。	送信側の EUF に同じ。

10.3. SDP プロファイル

10.3.1. SDP の用法

本従属節は、EUF 及び SCF で使用する SDP プロファイルを定義する。[RFC 2327]および[RFC 4566]に基づく実装の一連の拡張および制限もまた定義する。

表 10-8における、M、O および C は、表 10-7と同様の意味を持つ。

表10-8／JT-Q3402　使用する SDP プロファイル　（ITU-T Q.3402）

項目	EUF->SCF		SCF->EUF	
	EUF 送信	SCF 受信	SCF 送信	EUF 受信
Session description				
v= (protocol version)	M	M	M	M
o= (owner/creator and session identifier)	M	M	M	M
s= (session name)	M	M	M	M
i= (session information)	O	M	O	M
u= (URI of description)	O	O	O	O
e= (email address)	O	O	O	O
p= (phone number)	O	O	O	O
c= (connection information)	C1	M	C1	M
b= (bandwidth information)	O	M	O	M
Time description (one or more per description)				
t= (time the session is active)	M	M	M	M
r= (zero or more repeat times)	O	O	O	O
Session level description (continue)				
z= (time zone adjustments)	O	O	O	O
k= (encryption key)	O	O	O	O
a= (zero or more session attribute lines)	O	M	O	M
Media description (zero or more per description)				
m= (media name and transport address)	C2	M	C2	M
i= (media title)	O	O	O	O
c= (connection information)	C1, C2	M	C1, C2	M
b= (bandwidth information)	O	M	O	M
k= (encryption key)	O	O	O	O
a= (zero or more media attribute lines) (Note)	O	M	O	M

C1:セッション記述とメディア記述のうち、少なくともひとつのc=行が実装されなければならない。

C2:メディア記述を実装する場合、m=行とc=行はいずれも実装しなければならない。
(注) 映像セッションを起動する場合、映像のセッション記述は[RFC2429/4629]のように各コーデック規定形式を定義するRFCの規定に従ってSDPのa行のfmtpフィールドを記述するべきである。フレームレートはa行の"framerate"に記述しても良い。この場合、"framerate"のフィールド値はfmtpフィールド内に記述されたフレームレートと同じでなければならない。

(注) この表 10-8は、表 10-7に記述の通り実装の観点から記述されている。例えば、メディア記述部の c=行が実装されているとしても、特定の SIP/SDP メッセージの中の全てのメディア記述が c=行を含むことを意味するのではない。c=行がセッション記述部に含まれる時、メディア記述部の c=行は含まれない場合がある。

メディアセッションが UNI 上でビデオを利用する場合、メディア型式"video"がサポートされなければならない。本標準の表 10-8に規定されるメディア記述(メディアコーデックとその属性及び属性値等)は、ビデオ接続を開始するために SIP/SDP メッセージで交換される。

10.3.2. 能力交換

SDP アンサーを送信時、受け付けたメディアタイプ毎に、アンサー側の EUF は、受信した SDP オファーの希望するメディア型式の中から、サポートする第一優先のメディア型式のみ選択するべきである。

メディア形式"telephone-event"については例外である。それは、"telephone-event"を使用する場合、SDP アンサーに含まれるためである。

11. トランスポート層プロファイル

11.1. サポートする RFC

表 11-1における、M および O は、本標準の 10.1 節の定義と同様の意味を持つ。

表11-1／JT-Q3402　サポートするトランスポート層 RFC　（ITU-T Q.3402）

参照RFC	タイトル	EUF	SCF
RFC 3016 [RFC 3016]	RTP Payload Format for MPEG-4 Audio/Visual Streams	O	O
RFC 3047 [RFC 3047]	RTP Payload Format for ITU-T Recommendation G.722.1	O	O
RFC 3267 [RFC 3267]	Real-time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs	O	O
RFC 3389 [RFC 3389]	RTP Payload for Comfort Noise	O (注1)	O (注1)
RFC 3550 [RFC 3550]	RTP: A Transport Protocol for Real-Time Applications	M	M
RFC 3551 [RFC 3551]	RTP Profile for Audio and Video Conferences with Minimal Control	M	M
RFC 3558 [RFC 3558]	RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)	O	O
RFC 3611 [RFC 3611]	RTP Control Protocol Extended Reports (RTCP XR)	O	O
RFC 3711 [RFC 3711]	The Secure Real-time Transport Protocol (SRTP)	O	O
RFC 3984 [RFC 3984]	RTP Payload Format for H.264 Video	O	O
RFC 4103 [RFC 4103]	RTP Payload for Text Conversation	O	O
RFC 4348 [RFC 4348]	Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec	O	O
RFC 4629 [RFC 4629]	RTP Payload Format for ITU-T Rec. H.263 Video	O	O
RFC 4733 [RFC 4733]	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	M (注 2)	M (注 2)
RFC 4749 [RFC 4749]	RTP Payload Format for the G.729.1 Audio Codec	O	O
T.38 [T.38]	Procedures for real-time Group 3 facsimile communication over IP networks	O	O

(注 1) G.711 [G.711]および G.726 [G.726] のようなそれ自体では本来コンフォートノイズをサポートしないコーデックと共に使用するため。

(注 2) G.711 [G.711]が使用される時、[RFC 4733]は必須ではない。

以下のリストは、表 11-1に記載されたプロトコルより低位レイヤのプロトコルの代表的な例を示す。
低位レイヤに他のプロトコルをサポートしても良い。

- IETF RFC 768 (08/1980): User Datagram Protocol
- IETF RFC 791 (09/1981): Internet Protocol
- IETF RFC 792 (09/1981): Internet Control Message Protocol
- IETF RFC 793 (09/1981): Transmission Control Protocol
- IETF RFC 826 (11/1982): An Ethernet Address Resolution Protocol – or – Converting Network Protocol Address to 48bit Ethernet Address for Transmission on Ethernet Hardware
- IETF RFC 2460 (12/1998): Internet Protocol, Version 6 (IPv6) Specification
- IETF RFC 2461 (12/1998): Neighbor Discovery for IP Version 6 (IPv6)
- IETF RFC 2463 (12/1998): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- IEEE Std 802.3-2005 (12/2005): Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications - Media Access Control Parameters, Physical Layers and Management Parameters for subscriber access networks
- ISO/IEC 8877:1992 (12/1992): Information technology - Telecommunications and information exchange between systems - Interface connector and contact assignments for ISDN Basic Access Interface located at reference points S and T

11.2. DTMF トーンの処理

UA を含む SCF 及び EUF は、DTMF イベントを転送するために、[RFC 4733]の特定部をサポートしなければならない。G.711[G.711]が使用される時、[RFC 4733] は必須でなくても良い。

一方は RTP オーディオで、もう一方は非 RTP オーディオで動作する装置に関し、特有の要件がある。

これらは RTP 側からの[RFC 4733]のペイロードを検出し、非 RTP 側で DTMF オーディオトーンを生成可能でなければならない。逆に、それらは非 RTP 側からの DTMF オーディオトーンを検出し、RTP 側で[RFC 4733]ペイロードを生成しなければならず、インバンド・オーディオから DTMF トーンを除去するべきである。

12. 呼制御信号転送方式

UNI は、デフォルトの転送方式として UDP 上で SIP を転送するべきである。
ただし、例えば、メッセージサイズが大きい場合、TCP または SCTP 上で SIP を転送しても良い。

セキュリティのために、TLS 上で SIP を転送しても良い。

13. IP プロトコルバージョン

事業者網は IPv4 をサポートしなければならない。 また、事業者網は IPv6 をサポートしても良い。

EUF は IPv4 をサポートしなければならず、EUF は IPv6 をサポートしても良い。但し、EUF が IPv4 のみをサポートする事業者網に接続することが想定されない場合、EUF は IPv6 のみサポートしても良い。

14. セキュリティ考察

呼制御信号はセキュアであるべきであり、メディアはセキュアであっても良い。

付録 I.　　コールフロー例

（本付録は参考資料であり、仕様ではない。）

本付録におけるフロー例は、UNIを通じた発信側UAと着信側UA間のメディアセッションの確立とセッション解放に関する参考例を提示するものである。本付録のシナリオは、 UAがメディアセッションを確立するために SIP メッセージを交換して、異なる事業者網を経由して接続されるケースに基づいている。

本付録は、UA間の基本的な音声通話サービスの成功呼と不成功呼の呼設定と呼解放の参考例を提示する。

これらのシナリオには、NNI に相当する事業者網間の呼制御は含まれていないことに留意すること。

I.1.　SIP セッション確立の成功例

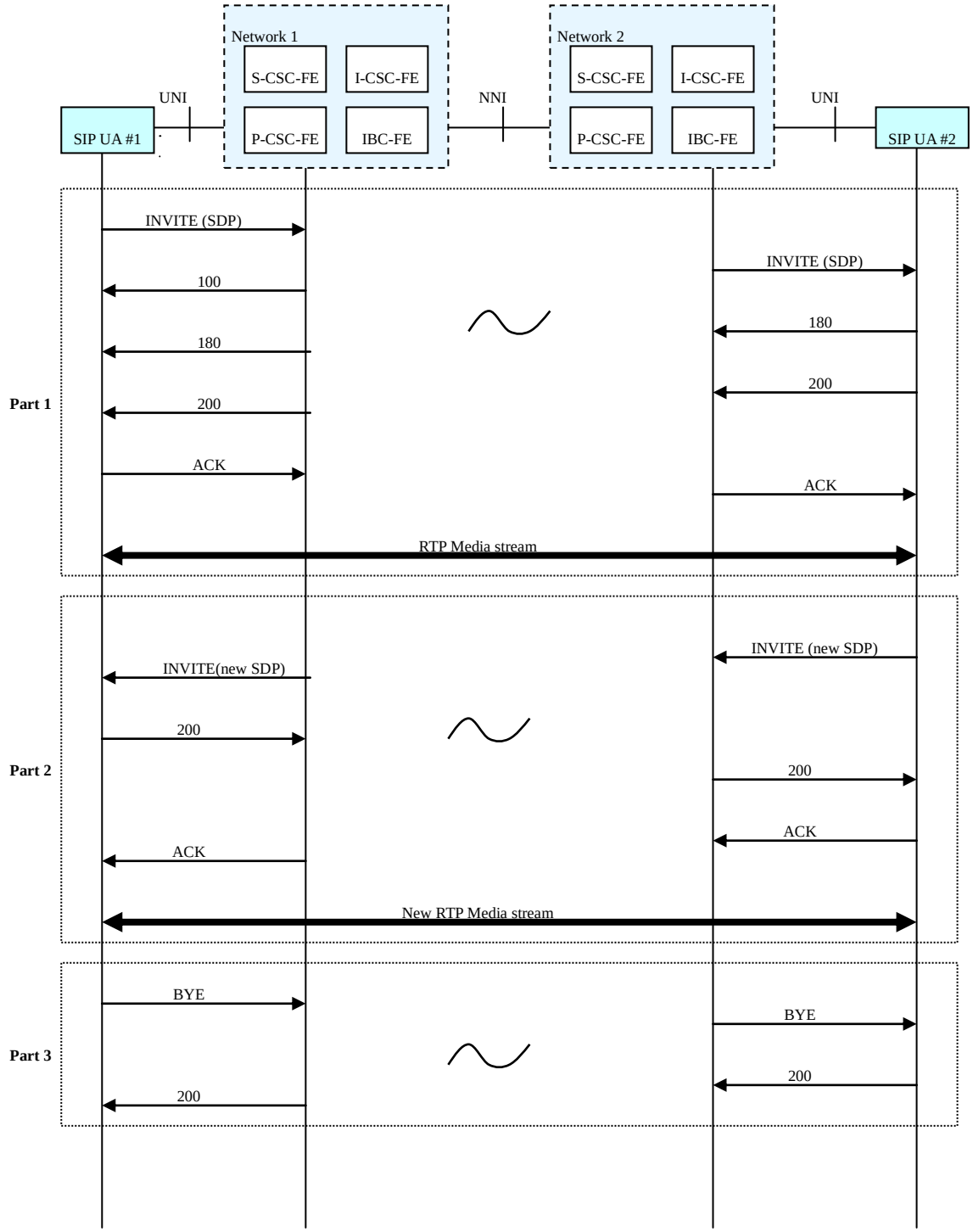
本従属節は、異なる事業者網に接続するUA#1とUA#2間の基本呼の成功例のフローを提示する。

付図 I-1では、Part 1（呼の確立）、Part 2（Re-INVITEによる再確立）、Part 3（呼の開放）の3つのパートにてサービス・シナリオの例を提示する。

付図 I-1のPart 1は、UA#1がSDPにセッションパラメータを記述したINVITEメッセージをUA#2に送信する様子を示す。セッション間で使用されるメディアタイプ(即ち、オーディオ、ビデオ等)に応じて、特定のメディアパラメータ及び値がUA間で交渉されるべきである。ACKメッセージの交換後、呼はUA#1とUA#2間で確立される。

付図 I-1のPart 2は、2つのUA間のメディアセッション確立後、re-INVITEを使用して、呼が再確立する様子を示す。本例においては、着信側のUAが、メディアセッションを再生成するために、SDPに新規のセッション記述を伴ったINVITEメッセージを発信側UAに送信する。これらの処理は、Part 1で示すように初期に確立したセッションに対する、新規のメディアタイプの追加、もしくあらゆるメディアタイプの削除を可能にする。

最後に、付図 I-1のPart 3で示すように、UA#1は、終話するところで、セッションを解放するために、BYEメッセージをUA#2に送信する。本例では、UA#2が200レスポンスメッセージをUA#1に送信するとき、セッションは削除される。



付図 I-1／JT-Q3402　SIP セッション確立の成功例　（ITU-T Q.3402）

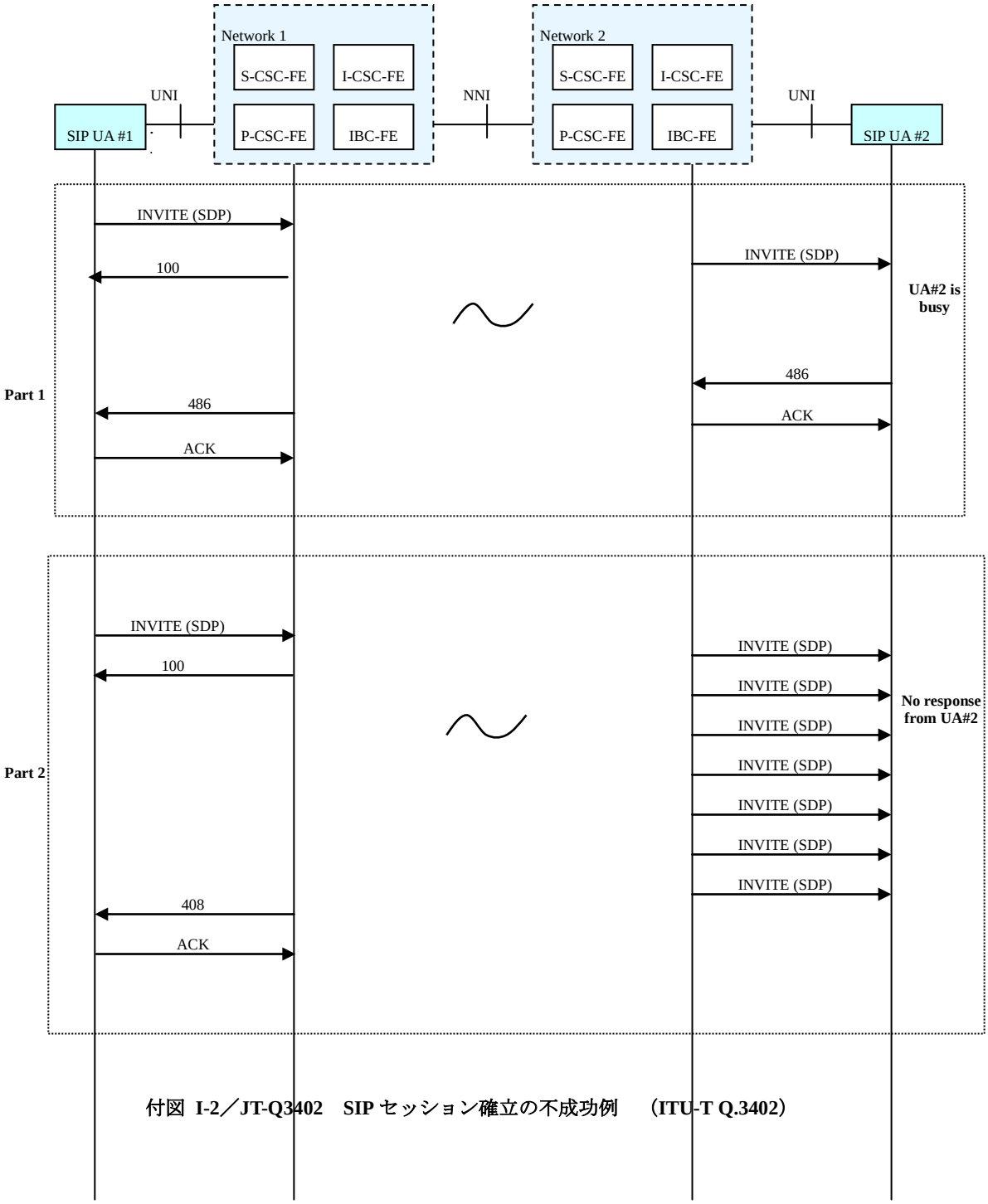
I.2. SIP セッション確立の不成功例

本従属節は、異なる事業者網に接続するUA#1とUA#2間の基本サービスの不成功例のフローを提示する。

付図 I-2は、話中と無応答による、特定のサービス不成功例を記す。

付図 I-2のPart 1は、発信側のUA(即ち、UA#1)から、INVITEメッセージを受信する時、着信側のUA(即ち、UA#2)が話中である様子を示す。従って、UA#1に486レスポンスメッセージを送信する。必然的に、メディアセッションは両者間で確立していない。

付図 I-2のPart 2は、UA#1からINVITEメッセージを受信する時、UA#2から応答が無いため、呼設定が失敗する様子を示す。INVITEメッセージは、UA#2に6回再送信されることに留意すること。この後、UA#1は、網から408レスポンスメッセージを受信する。

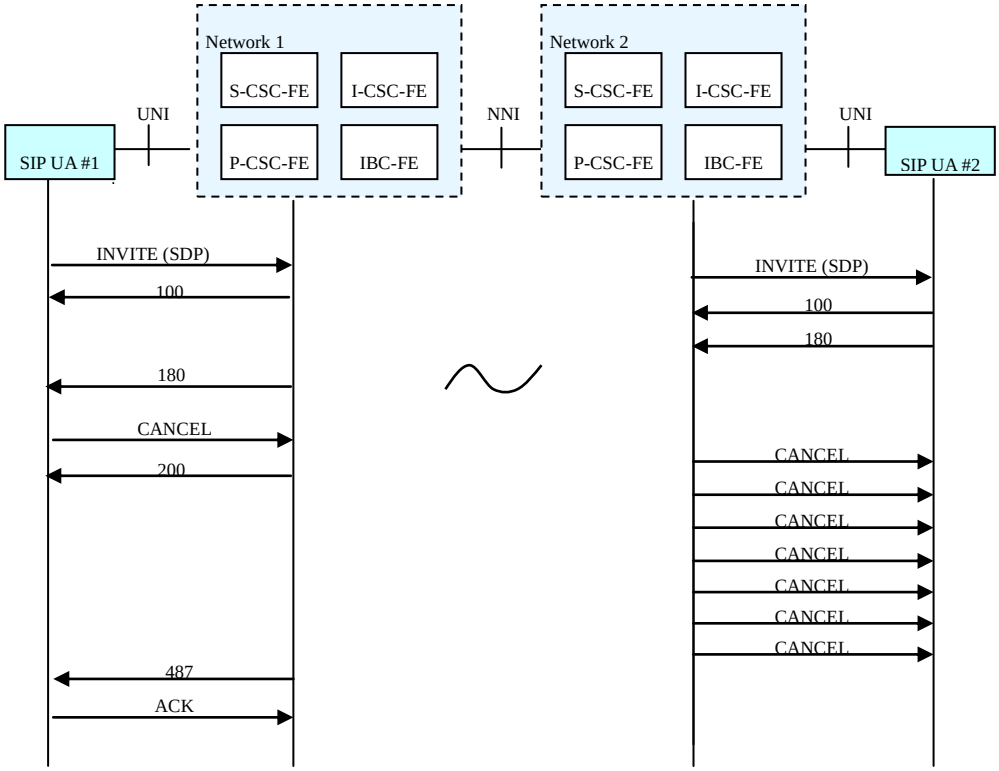


付図 I-2／JT-Q3402　SIP セッション確立の不成功例　（ITU-T Q.3402）

I.3.　キャンセル呼に対する無応答による不成功例

付図 I-3は、異なる事業者網に接続する UA#1 と UA#2 間のサービスの不成功例を提示する。

UA#1 は、UA#2 と呼を開始するために INVITE メッセージを送信する。UA#1 は、UA#2 からの 180 レスポンスを受信後、呼を断念する。UA#1 は呼設定を取り消すため、CANCEL メッセージを送信するが、UA#2 からは無応答である。この状況は UA#2 が突発的な電源断に陥ったかネットワークから切断された場合に起こるかもしれない。

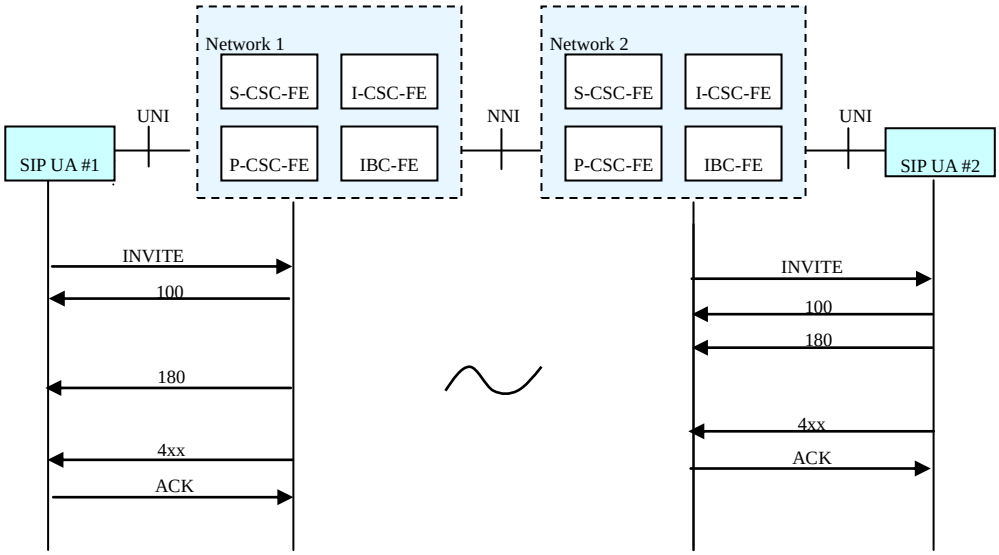


付図 I-3／JT-Q3402　キャンセル呼に対する無応答の不成功例　（ITU-T Q.3402）

I.4.　呼設定の不成功例

付図 I-4は、異なる事業者網に接続する UA#1 と UA#2 間のサービスの不成功例を提示する。

UA#1 は、UA#2 と呼を開始するために INVITE メッセージを送信する。着信先は成功裏に呼び出されるが、UA#2 は 4xx(Client-Error)レスポンスメッセージを送信することにより、呼を拒否した。この状況は UA#2 が発信元を識別し、電話に出ない判断をした場合に起こるかもしれない。



付図 I-4／JT-Q3402　呼設定の不成功例　（ITU-T Q.3402）

15. 関連技術文献

– [b-ETSI ES 282 007], Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture

– [b-ETSI TS 182 006], Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)

– [b-ETSI ES 283 003], Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]

– [b-3GPP TS24.229], 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3

付属資料 a.　JT-Q3402 本文に対する規定の明確化項目およびオプション項目

（本付属資料は仕様の一部である。）

a.1.　概要

本付属資料は、JT-Q3402 本文に規定されるアーキテクチャにおいて NGN に UNI を介して接続する SIP 端末の接続性を高めるため、JT-Q3402 本文をベースドキュメントとした規定の明確化や、オプション項目の明確化を行う。

a.2.　参考文献

本付属資料で参照する参考文献を以下に示す。

[RFC4585]　"RTCP をベースとしたフィードバックのための拡張 RTP プロファイル（RTP/AVPF）(Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF))", TTC 標準 JF-IETF-RFC4585 第 1.0 版, 2008 年 3 月

[RFC5104]　"フィードバックを伴う RTP AV プロファイル（AVPF）のコーデック制御イメージ(Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF))", TTC 標準 JF-IETF-RFC5104 第 1.0 版, 2008 年 3 月

[RFC5407]　"SIP における準正常状態のコールフロー例(Example calls flows of race conditions in the Session Initiation Protocol (SIP))", TTC 標準 JF-IETF-RFC5407 第 1.1 版, 2009 年 11 月

a.3.　規定の明確化項目およびオプション項目

JT-Q3402 本文をベースドキュメントとして、TTC で規定を明確化する項目、およびオプション項目を付表 a-1 に示す。なお、表に記載のない章節については、規定の明確化項目がベースドキュメントどおりであることを意味する。また、付属資料 a～付属資料 i、および付録 i～付録 viiで記載されるオプション項目は付表 a-1 に記述していない。付属資料、および付録も含めたオプション項目表は、付録 iを参照のこと。

付表 a-1／JT-Q3402　規定の明確化項目およびオプション項目

JT-Q3402 本文の参照節		規定の明確化項目	オプション項目	備考
項番	項目			
2.	参考文献	ベースドキュメントに加え、本標準で必要な参考文献を個別の付属資料や付録に記載する。	－	
5	参照モデル	EUF が音声電話端末である場合は、付属資料 iの規定に従う。	－	
6.	想定事項	2. 音声及び映像の転送に SRTP は使用しない。	－	
7.1	メディアパケットに関する考慮事項	ベースドキュメントどおり。	INVITE への 1xx レスポンスに SDP アンサーが含まれていた場合における、発信側端末からのメディアパケット送信（付表 1-25 項番 1） Initial INVITE に対する最終 SDP ネゴシエーションが行われる前のメディアパケットの扱い（付表 1-25 項番 2）	
8.1	コーデックリスト	音声のコーデックリストには、G.711μ-law を必ず含める。 コーデックリストに含まれるコ	G.711μ-law 以外で、コーデックリストに含めるコーデック（付表 1-16 項番 1～3）	

		ーデックを SDP オファーに設定した場合においても、事業者のポリシーによりエンド・トゥ・エンドのネゴシエーションとならない場合がある。 コーデックリストに含まれないコーデックは、SDP オファーに設定しない。		
8.2	パケット化周期	G.711μ-law を用いる場合のパケット化周期について、付属資料i.2.1節の規定に従う。	－	
9.	ルーチングとアドレス形式	国内番号を用いる場合の URI 形式について、付属資料b.6節の規定に従う。 サブアドレスについて、付属資料b.7節の規定に従う。	REGISTER を除く既存ダイアログ外リクエストの Request-URI 形式（付表 1-20 項番 1～2）	
10.1	サポートする RFC	RFC2976，RFC3388，RFC3725，RFC3824，RFC3853，RFC3861，RFC3959，RFC3960，RFC4168，RFC4244，RFC4412，RFC4458，RFC5031， draft-levy-sip-diversion-08 は使用しない。 RFC3313 に規定される P-Media-Authorization ヘッダは、SCF から EUF 方向のみ適用可能とする。 RFC3326 に規定される Reason ヘッダの扱いについて、付属資料f.3.1節の規定に従う。 RFC3327 に規定される path 拡張機能について、付属資料c.3節の規定に従う。なお、Path ヘッダは SCF から EUF 方向のレスポンスにのみ適用される。 RFC3329 に規定される Security-Client、Security-Verify ヘッダは EUF から SCF 方向のリクエストに、また Security-Server ヘッダは SCF から EUF 方向のレスポンスにのみ適用可能とする。 RFC3455 に規定されるヘッダのうち、P-Associated-URI ヘッダと P-Called-Party-ID ヘッダを、付属資料 bの規定に従い利用する。 P-Charging-Vector ヘッダ、P-Charging-Function-Addresses 、P-Visited-Network-ID ヘッダは利用しない。 P-Access-Network-Info ヘッダは、EUF から SCF 方向の SIP 信号にのみ適用される。 RFC3608 に規定される	各 RFC に関連し、以下の項目がオプション項目となる。 【RFC2046】 MIME Multipart の利用（付表 1-10 項番 1～4） 【RFC3310, RFC2617, RFC3329】 端末の認証手順（付表 1-11 項番 1～2） セキュリティ能力交換機能（sec-agree）の利用（付表 1-7 項番 8） 【RFC3262】 暫定応答の信頼性確保機能（100rel）の利用（付表 1-7 項番 2） 【RFC3265】 SUBSCRIBE メソッド、および NOTIFY メソッドの利用（付表 1-2 項番 10～15） 【RFC3311】 UPDATE による SDP オファー（付表 1-23 項番 1, 2, 5, 6） アーリーダイアログにおけるメディア変更（付表 1-23 項番 1～2） 【RFC3312, RFC4032】 確立前帯域確保機能（precondition）の利用（付表 1-7 項番 5） 【RFC3313】 P-Media-Authorization ヘッダの利用（付表 1-17 項番 1） 【RFC3320, RFC3485,	

		Service-Route ヘッダの扱いについて、付属資料c.3節に従う。 RFC3680 に規定される登録イベントについて、付属資料c.6節に従う。 注）RFC をサポートすることは、その RFC の記述内容に従うことであって、全てのセッションにおいてその能力を利用することを意味するものではない。	RFC3486, RFC5049】 SigComp の利用（付表 1-5 項番 1） 【RFC3388, RFC3524】 メディアのグループ化（付表 1-18 項番 1） 【RFC3428】 MESSAGE メソッドの利用（付表 1-2 項番 2～5） 【RFC3515, RFC3892】 REFER メソッドの利用（付表 1-2 項番 6～9） 【RFC3556】 RTCP 帯域指定の利用（付表 1-13 項番 4） 【RFC3581】 UNI 下部での Hosted NAT の許容（付表 1-6 項番 1） 【RFC3840, RFC3841】 端末能力通知機能（pref）の利用（付表 1-7 項番 6） 【RFC3891】 ダイアログ置換機能（replaces）の利用（付表 1-7 項番 3） 【RFC3903】 PUBLISH メソッドの利用（付表 1-2 項番 16～19） 【RFC3911】 会議セッション参加機能（join）の利用（付表 1-7 項番 4） 【RFC4028】 UPDATE メソッドによるセッション更新（付表 1-8 項番 1）	
10.2.1.7	SIP Messages	SIP メッセージの設定最大長について、付属資料 hの規定に従う。	－	
10.2.1.7.1	Requests	OPTIONS メソッドは利用しない。 SIPS-URI は利用しない。	－	
10.2.1.7.4.1	Message Body Types	ベースドキュメントどおり。	PRACK および PRACK に対する 200OK への SDP の設定（付表 1-22 項番 2～3）	
10.2.1.8.1.3.	Processing Responses	ベースドキュメントどおり。	端末の認証手順（付表 1-11 項番 1～2）	
10.2.1.8.3	Redirect Servers	ベースドキュメントどおり。なお、3xx レスポンスは REGISTER を除く既存ダイアログ外リクエストに適用可能とする。	3xx レスポンスによるリダイレクト機能の利用（付表 1-12 項番 1～2）	

10.2.1.10	Registrations	端末登録の手順に関して付属資料 cの規定に従う。また、端末登録時の輻輳制御に関して付属資料f.2節の規定に従う。	端末登録の有無及び手順（付表 1-2 項番 1、付表 1-11 項番 1、付表 1-24 項番 1～5）	
10.2.1.11	Querying for Capabilities	能力問い合わせはサポートしない。	－	
10.2.1.12.1	Creation of a Dialog	SIPS-URI は利用しない。	－	
10.2.1.12.2	Requests within a Dialog	SIPS-URI は利用しない。	－	
10.2.1.13	Initiating a Session	Initial INVITE には、有効なメディアを記載した SDP オファーを含むこととする。 （2xx/ACK での SDP ネゴシエーションは利用しない） 発信時の輻輳制御に関して付属資料f.3節の規定に従う。		
10.2.1.14	Modifying an Existing Session	re-INVITE を用いる場合、SDP オファーは INVITE リクエストに設定する。	ダイアログ確立後のメディア変更（付表 1-23 項番 3～6）	
10.2.1.17	Transactions	SIP 信号の信号交差等による準正常状態時における処理は、[RFC5407]に従う。なお、 当該文書は 2 つの SIP-UA 間におけるシーケンスを記載しているが、UNI に適用するに際して、網及び端末の間におけるシーケンスとして読み替える。	－	
10.2.1.19	Common Message Components	SIPS-URI は利用しない。	－	
10.2.1.20.7	Authorization	Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用する。	－	
10.2.1.20.11	Content-Disposition	Content-Disposition ヘッダのパラメータには、初期値のみ設定可能とする。 RFC3959 に定義されるアプリケーションサーバモデルは利用しない。	－	
10.2.1.20.27	Proxy-Authenticate	Proxy-Authenticate ヘッダは SCF が EUF からの REGISTER を除く既存ダイアログ外リクエストを認証する際の 407 レスポンスに限り利用する。	－	
10.2.1.20.28	Proxy-Authorization	Proxy-Authorization ヘッダは SCF が EUF からの REGISTER を除く既存ダイアログ外リクエストを認証する際に限り利用する。	－	
10.2.1.20.29	Proxy-Require	Proxy-Require ヘッダは EUF から SCF 方向にのみ適用する。	－	
10.2.1.20.24	MIME-Version	“1.0”のみをサポートする。	－	
10.2.1.20.32	Require	RFC3959 に定義されるアプリケーションサーバモデルは利用しない。	timer、100rel、およびその他 SIP オプションタグの利用(付表 1-7 項番 1～9)	
10.2.1.20.33	Retry-After	輻輳抑制のため、Retry-After ヘッダに関して付属資料f.2.1節に示す動作を行う。	－	
10.2.1.20.34	Route	pre-existing ルートに関して、付属資料c.3節の規定に従う。	－	

10.2.1.20.44	WWW-Authenticate	WWW-Authenticate ヘッダは SCF が EUF からの REGISTER リクエストを認証する際の 401 レスポンスに限り利用する。	－	
10.2.1.23	S/MIME	INVITE に関わる呼処理信号で SDP 情報を扱う場合においては、S/MIME を利用しない。	－	
10.2.2.1	拡張メソッド	UPDATE 及び PRACK リクエストの利用について、付属資料 d の規定に従う。	－	
10.2.2.2.2	P-Asserted-Identity	REGISTER を除く既存ダイアログ外リクエストでのみ P-Asserted-Identity ヘッダを利用する。 発信者番号通知について、付属資料 bの規定に従う。	－	
10.2.2.2.3	P-Preferred-Identity	REGISTER を除く既存ダイアログ外リクエストでのみ P-Preferred-Identity ヘッダを利用する。 発信者番号通知について、付属資料 bの規定に従う。	－	
10.2.2.2.4	Privacy	REGISTER を除く既存ダイアログ外リクエストでのみ Privacy ヘッダを利用する。 利用可能なプライバシーオプションは”id”と”none”のみとする。 発信者番号通知について、付属資料 bの規定に従う。	－	
10.2.3	Summary of SIP methods and headers	OPTIONS は利用しない。	利用するメソッド（付表 1-2 項番 1～21）	
10.3.1	SDP の用法	SDP の扱いについて、付属資料 e の規定に従う。 b=行で指定する帯域値に関して、付属資料 gの規定に従う。	利用する SDP 行（付表 1-22 項番 4～5） メディアで利用する IP バージョン（付表 1-3 項番 3） 映像(m=video)およびデータ通信(m=application, m=data 等)の利用（付表 1-14 項番 1～2） メディアにおける TCP の利用 [RFC4145]（付表 1-14 項番 3）	
11.1	サポートする RFC	ベースドキュメントどおり。なお、RTCP を用いたフィードバック機能（RTP/AVPF）[RFC4585] [RFC5104]を利用可能とする。	RTCP を用いたフィードバック機能の利用（付表 1-19 項番 1～2）	
12	呼制御信号転送方式	SIP 信号の送受信には、UDP もしくは TCP をトランスポートプロトコルとして使用する。セキュリティのため TLS を使用してもよい。	呼制御信号に利用するレイヤ 4 プロトコル種別（付表 1-4 項番 1～3）	
13	IP プロトコルバージョン	ベースドキュメントどおり。なお、IPv4/IPv6 のフォールバックに関する留意事項として付属資料e.4.1節を参照する。	呼制御信号に利用するレイヤ 3 プロトコル種別（付表 1-3 項番 1～4）	

付属資料 b.　発信者番号通知と関連ヘッダ

（本付属資料は仕様の一部である。）

b.1.　概要

本付属資料では、発信者番号及び非通知理由の通知に関する手順、それに用いるヘッダ（P-Preferred-Identity、P-Asserted-Identity、Privacy、From）と Request-URI、及び関連する網付与ユーザ ID 通知に用いるヘッダ（P-Associated-URI）と、着信対象の通知に用いるヘッダ（P-Called-Party-ID）について明確化する。

b.2.　参考文献

本付属資料で参照する参考文献を以下に示す。

[TS-1008]　"発着サブアドレス情報転送サービスに関する技術仕様", TTC 仕様書 TS-1008 第 2 版, 情報通信技術委員会(The Telecommunication Technology Committee), 2014 年 10 月

b.3.　網付与ユーザ ID

NGN において、認証等を経て網で付与される（端末から提示された場合には検証される）、ユーザのアイデンティティに関する情報（当該端末へ着信可能な E.164 番号を用いて構成される SIP-URI 等）であり、発信者 ID 等に用いられる。b.7節に示すように、発端末が設定したサブアドレス情報も付与される場合がある。

網付与ユーザ ID の具体的な URI 形式は、b.6節に示す。

b.3.1.　端末登録時の通知

網は端末に網付与ユーザ ID を通知するため、端末登録に REGISTER リクエストを用いる場合、その 200 OK レスポンスに P-Associated-URI ヘッダ[RFC3455]を設定する場合がある。【付表 1-24 項番 3】

P-Associated-URI ヘッダには、当該端末に割り当てられた網付与ユーザ ID を示す URI が記載される。複数の網付与ユーザ ID が記載されている場合は、端末は最初の URI をデフォルトの網付与ユーザ ID として認識する。

b.4.　発信者番号の取り扱い

発信者番号（以下、発信者 ID）情報の通知は、JF-IETF-RFC3323[RFC3323]、JF-IETF-RFC3324[RFC3324]、JF-IETF-RFC3325[RFC3325]に基づいて、網付与ユーザ ID 及び通知／非通知情報を伝達することにより実現する。発信者 ID 通知／非通知の対象となるのは、UNI で送受信可能なリクエストのうち、REGISTER 以外の既存ダイアログ外リクエストである。

発信者 ID 情報の通知は、大きく分けて 4 段階で行われる。

1) 発端末が、選択する発信者 ID 情報（P-Preferred-Identity）と、通知／非通知の希望（Privacy）を網に伝え、接続先を指示（Request-URI）し、発信する。
2) 発加入者を収容する網は、端末が選択した発信者 ID の検証及び正規化を行い、また当該加入者に関するデフォルトの通知／非通知設定等を考慮し、網内及び NNI で伝達する発信者 ID 情報を決定する。
3) 着加入者を収容する網は、通知／非通知の情報と、着加入者に関する発信者 ID 情報通知契約等を考慮して、着端末へ通知する発信者 ID 情報を決定する。
4) 着端末は、着信時に網から発信者 ID 情報を通知される。

本付属資料では、段階1)及び2)を発信条件としてb.4.1節に、段階3)及び4)を着信条件としてb.4.2節に示す。

b.4.1. 発信条件

b.4.1.1. 発信者 ID の選択

端末は、発信者 ID の通知／非通知に関わらず、発信者 ID としての使用を希望する網付与ユーザ ID があるならば、その網付与ユーザ ID を既存ダイアログ外リクエストの P-Preferred-Identity ヘッダに設定する。b.3.1 節に示す手順で網付与ユーザ ID が通知されている場合は、P-Associated-URI ヘッダに記載されている URI のいずれかを選択し、P-Preferred-Identity ヘッダに記載する。

網は、P-Preferred-Identity ヘッダに設定された SIP-URI を発信者 ID として扱う。ただし、P-Preferred-Identity ヘッダが設定されていない場合、または P-Preferred-Identity ヘッダに設定されている URI が、発端末に割り当てられた網付与ユーザ ID でない場合は、P-Preferred-Identity ヘッダにデフォルトの網付与ユーザ ID が設定されたものと同等として扱う。

b.4.1.2. 発信者 ID 通知／非通知の設定

端末が送信する既存ダイアログ外リクエストについて、発信者 ID 通知／非通知は Privacy ヘッダ[RFC3325]と 186/184 プリフィックスの 2 種類の手順を用いて要求される。

- Privacy ヘッダに"none"を設定することにより発信者 ID 通知を要求し、"id"を設定することにより非通知を要求することができる。端末は、発信者 ID 通知／非通知の設定項目を有しており、かつユーザがその設定を行った場合に限り、Privacy ヘッダを設定する。
- Request-URI が国内電話番号から構成される URI である場合は、186 プリフィックスが設定されている場合に発信者 ID 通知が指定され、184 プリフィックスが設定されている場合に非通知が指定されたことになる。この 186/184 プリフィックスの設定は、ダイヤルするユーザに委ねられなければならず、端末が自動的にこれらのプリフィックスを付与するような動作を行ってはならない。

Privacy ヘッダの設定と 186/184 プリフィックスの設定は独立である。

端末は、Privacy に"id"を設定した場合は、From ヘッダの SIP-URI に <sip:anonymous@anonymous.invalid> を設定する。それ以外の場合は、P-Preferred-Identity ヘッダと同一の URI を設定する。

上記のヘッダ類に設定する内容を、付表 b-1 に示す。

付表 b-1／JT-Q3402　番号通知に関連するヘッダ類の設定条件

フィールド	Privacy ヘッダ		
	none	id	ヘッダなし
Request-URI の user 部もしくは telephone-subscriber 部	ユーザがダイヤルした番号 （186/184 プリフィックスがダイヤルされた場合も、そのまま設定する）		
P-Preferred-Identity ヘッダ	発信者の網付与ユーザ ID		
To ヘッダの URI	Request-URI と同値		
From ヘッダの name-addr	P-Preferred-Identity ヘッダを設定する場合、P-Preferred-Identity ヘッダに設定された URI と同値	<sip:anonymous@anonymous.invalid>	P-Preferred-Identity ヘッダを設定する場合、P-Preferred-Identity ヘッダに設定された URI と同値

網は、Privacy ヘッダと 186/184 プリフィックスの設定、及び当該発加入者に関するデフォルトの発信者 ID 通知／非通知の設定に従い、発信者 ID 通知／非通知を選択する。

- Request-URI に記述される電話番号の先頭に 186/184 プリフィックスが設定されている場合、Privacy ヘッダの設定内容に関わらず、186 が設定されている場合は発信者 ID 通知、184 が設定されている場合は発信者 ID 非通知として扱う。
- Privacy ヘッダの設定も、186/184 プリフィックスの設定もない場合は、当該発加入者に関するデフォルトの発信者 ID 通知／非通知の設定に従う。
- 184 プリフィックスが設定されていない場合、緊急発呼時には Privacy ヘッダの設定内容に関わらず、発信者 ID 通知として扱う。

上記の Privacy ヘッダ設定、186/184 プリフィックス設定、及びデフォルトの発信者 ID 通知／非通知設定との優先関係を付表 b-2 及び付表 b-3 に図示する。

付表 b-2／JT-Q3402　一般呼における発信者 ID 通知／非通知選択条件

		宛先番号のプリフィックス		
		186	184	プリフィックスなし
Privacy	none	発信者 ID 通知	発信者 ID 非通知	発信者 ID 通知
	id			発信者 ID 非通知
	ヘッダなし			発ユーザ毎に管理された網のデフォルト値に従う

付表 b-3／JT-Q3402　緊急呼における網の発信者 ID 通知／非通知選択条件

		宛先番号のプリフィックス		
		186	184	プリフィックスなし
Privacy	none	発信者 ID 通知	発信者 ID 非通知	発信者 ID 通知
	id			
	ヘッダなし			

発信者 ID が非通知の場合の非通知理由は、付表 b-4 に示される理由のうち、"Anonymous"（ユーザ拒否のため通知不可）が選択される。

b.4.2.　着信条件

着加入者に関する、着側の発信者 ID の通知／非通知の設定に従い、着信時のヘッダ条件が異なる。

b.4.2.1.　発信者 ID や非通知理由が通知される場合

網から受信した既存ダイアログ外リクエストに Privacy ヘッダが設定され、発信者 ID や非通知理由の通知が行われる。

Privacy ヘッダに"none"が設定されている場合、発信者 ID が P-Asserted-Identity ヘッダで通知される。P-Asserted-Identity ヘッダには SIP-URI のみが設定されるか、SIP-URI と TEL-URI の両方が設定される。

Privacy ヘッダに"id"が設定されている場合、発信者 ID は P-Asserted-Identity ヘッダで通知されない。代わりに、From ヘッダの display-name に非通知理由が設定される。発信者 ID が通知されない場合は、非通知理由として付表 b-4 に示される形式で表示内容（意味）が提供される場合がある。ただし、付表 b-4 に示されるような形式でない場合は、非通知理由は提供されていない。

付表 b-4／JT-Q3402　非通知理由

受信内容(*1)(*2)	表示内容（意味）
Anonymous	ユーザ拒否のため通知不可
Coin line/payphone	公衆電話発信のため通知不可
Interaction with other service	サービス競合のため通知不可
Unavailable	サービス提供不可のため通知不可

(*1)　二重引用符号（ダブルクォーテーションマーク）で囲まれる場合がある。
(*2)　本表の記載する文字列の後ろに任意の文字列が続く場合がある。

b.4.2.1.1.　発信者 ID の表示

端末は、P-Asserted-Identity ヘッダで通知された発信者 ID に関して、下記の優先度で表示を行う。

1) P-Asserted-Identity ヘッダに SIP-URI と TEL-URI の両方が設定されている場合は、TEL-URI を優先して表示する。
2) P-Asserted-Identity ヘッダの URI に display-name が設定されている場合は、addr-spec よりも display-name を優先して表示する。

display-name が設定されていない場合に、SIP-URI の user 部や TEL-URI の local-number-digits 部または global-number-digits 部を表示する場合、当該箇所が付表 b-5 の受信内容に示す文字列である場合は、それぞれに対応する表示内容（意味）を表示する。

付表 b-5／JT-Q3402　発信者電話番号表示内容

受信内容(*1)	表示内容（意味）
数字のみ	受信した数字列
「+81」から始まり、+以降が数字のみ	「+81」を削除し、先頭に「0」を付与した数字列
「+」から始まり、+以降が全て数字で、+の次が「81」ではない。	「+」を削除し、先頭に「010」を付与した数字列

(*1)　display-name として使用する場合は二重引用符号（ダブルクォーテーションマーク）で囲まれる場合がある。

b.4.2.2.　発信者 ID や非通知理由が通知されない場合

Privacy ヘッダ、P-Asserted-Identity ヘッダが設定されず、From ヘッダの display-name にも非通知理由を示す文字列は設定されない。

b.5.　着信対象の通知

網は、着端末に対して送信する既存ダイアログ外リクエストに、P-Called-Party-ID ヘッダ[RFC3455]を付与し、着信対象の網付与ユーザ ID を示す URI を設定する場合がある。

端末は、複数の網付与ユーザ ID が割り当てられている場合に、いずれの網付与ユーザ ID に対する着信かを識別するために、P-Called-Party-ID ヘッダを用いる。なお、P-Called-Party-ID ヘッダが設定されていない場合は、デフォルトの網付与ユーザ ID に対する着信であると認識すべきである。

b.6.　国内電話番号を用いる場合の URI 形式

網付与ユーザ ID、及び Request-URI に国内電話番号を用いる場合の用いる URI 形式を示す。国内番号以外を用いる URI 形式は、使用してもよい。【付表 1-20 項番 1】

網付与ユーザ ID には、SIP-URI または TEL-URI を使用し、各ユーザには網付与ユーザ ID として 1 つ以上

の SIP-URI が割り当てられる。Request-URI には、SIP-URI もしくは TEL-URI を使用する。

また、b.7節に示すサブアドレスが設定される場合がある。

b.6.1. user 部・local-number-digits 部

SIP-URI では国内番号の数字列を user 部に記述し、TEL-URI では国内番号の数字列を local-number-digits 部に記述する。ただし、user 部及び local-number-digits 部に、visual-separator に該当する文字は用いない。

Request-URI の場合は、user 部及び local-number-digits 部には、ユーザがダイヤルした数字列をそのまま設定する。網付与ユーザ ID の場合は、国内プリフィックスで開始される全桁の電話番号を設定する。

b.6.2. hostport 部・context の descriptor 部

SIP-URI の hostport 部、及び TEL-URI の context の descriptor 部は、網が定めるドメイン名もしくはホスト名（IP アドレス形式を含む）とする。【付表 1-20 項番 2】

b.7. サブアドレス

網が管理するユーザに対して、JJ-90.10 で規定される相互接続インタフェースを通した ISUP 網で提供可能なサブアドレス情報の転送によって実現可能なサービスと同等のサービスを提供することがある。【付表 1-9 項番 1～2】

本付属資料では、サブアドレス情報の処理を行う網及び端末において、サブアドレス情報の送受を適切に行うために満たすべき条件のうち、[TS-1008]との差分となる SIP 信号のサブアドレス情報の条件を記述する。その他の条件は、[TS-1008]の UNI の規定に従う。

b.7.1. サブアドレス情報

b.7.1.1. サブアドレス情報の内容

サブアドレス情報の内容は、0 から 9 までの数字 19 桁以内の数字列とする。詳細は、[RFC4715] および [TS-1008] に基づく。

b.7.1.2. サブアドレス情報のフォーマット

サブアドレス情報は、SIP 信号のすべてのリクエスト／レスポンスを対象とし、発信元を示すヘッダ（From、P-Preferred-Identity、P-Asserted-Identity）および着信先を示すヘッダ（To、P-Called-Party-ID）および Request URI における、SIP URI の user 部または TEL URI の中の、セミコロン(;)および"isub="に続く数字列として設定される。

付属資料 c.　端末登録

（本付属資料は仕様の一部である。）

c.1.　概要

本付属資料では、端末登録に関して規定を行う。

c.2.　網側アドレスの取得

網は端末に対して、SCF の IP アドレス及びポート番号を通知する手段を提供する。網は、DHCP/DHCPv6 や事前設定、またはアクセス回線に依存するその他の手順を提供する。【付表 1-24 項番 2】

端末は、取得した IP アドレス及びポート番号に対して SIP 信号の送信を行う。

c.3.　登録

端末は登録したい Contact アドレスを設定した REGISTER リクエストを網に送信することで登録を行う。Contact アドレスへの q パラメータの設定条件について、網で定める場合がある。【付表 1-24 項番 6】

端末が Contact アドレスの expires パラメータ、もしくは Expires ヘッダに設定する値は網で定める場合がある。【付表 1-24 項番 4】

c.3.1.　path 拡張機能と Service-Route ヘッダ

網は、path 拡張機能と Service-Route ヘッダを用いた pre-existing ルートの提供を行う場合がある。【付表 1 1-7 項番 7、付表 1-24 項番 1】

網から pre-existing ルートの提供が行われる場合、端末は、JF-IETF-RFC3327[RFC3327]で規定される path 拡張機能を Supported ヘッダで表明し、REGISTER リクエストを送信する。端末登録が成功した場合、網は 200 OK レスポンスに Service-Route ヘッダ[RFC3608]を設定し、pre-existing ルートの第 2hop 以降の SIP-URI を通知する。

c.3.2.　pre-existing ルート

c.3.1節に示す手順を用いた pre-existing ルートの提供が行われる場合、端末はc.2節で提供されるアドレスを記載し loose-routing を指定する SIP-URI を第 1hop とし、c.3.1節の手順で提供された pre-existing ルートで提供されるアドレスを第 2hop 以降とする pre-existing ルートとし、REGISTER を除く既存ダイアログ外リクエスト送信時に Route ヘッダに指定する。なお、REGISTER リクエストに対しては、pre-existing ルートは提供されない。

c.3.3.　網で保持されるアドレス形式との差分

網に登録される Contact アドレスは、端末が REGISTER リクエストに設定した Contact アドレスと差異が生じる場合がある。端末は Contact アドレスの URI を照合する場合に留意しなければならない。

- 網が認識しない URI パラメータについては保持されない場合がある。
- hostport 部において SIP のデフォルトの port 番号（5060）を指定していたとしても、網には port 番号の指定がない形式の Contact アドレスとして保持される場合がある。また逆に、port 番号を指定していなかったとしても、網にはデフォルトの port 番号（5060）が指定されている形式の Contact アドレスとして保持される場合がある。

c.4. 更新

端末は網より登録または更新完了である 200(OK)レスポンスを受信した場合には、その Contact ヘッダに含まれる、当該端末が REGISTER リクエストで要求した Contact アドレスとそれに対する expires パラメータ、もしくは Expires ヘッダで指定された保持期限（Z 秒）を記録する。

更新のタイミング(T 秒)は保持期限（Z 秒）を過ぎるまでの間かつ、頻繁な REGISTER リクエストの送信が起こらないように、例えば保持期限（Z 秒）の 0.x 倍として、かつ再送時間を考慮し保持期限の残りが JF-IETF-RFC3261[RFC3261]において規定される Timer F（= 32 秒）より多く残っているような動作としなければならない。なお、更新のタイミングに関しては網で定める場合がある。【付表 1-24 項番 5】

c.5. 削除

端末は、突然の電源断や、装置シャットダウン時におけるシーケンス異常などを考慮し、装置起動時においては、起動後に行われる登録動作前に、自身が登録する全ての Contact アドレスを削除すべきである。なお、その際の削除については、何らかの形で以前に登録したロケーション情報を確実に削除できることを保証できない場合は、Contact アドレスに * を、Expires ヘッダに 0 を指定する REGISTER リクエストを送信する、全指定削除で行うべきである。

c.5.1. 端末停止時・IP アドレス変更時の考慮

端末は、例えば再起動や IP アドレス変更時、もしくはアプリケーション終了時（ソフトフォンの場合）等には、網に登録する Contact アドレスを削除ないし更新すべきである。

c.6. 登録イベント

網は、端末の登録状態が未登録状態へ変化したことを端末へ通知する、JF-IETF-RFC3680[RFC3680]で規定される登録イベント（reg イベント）機能を提供する場合がある。【付表 1-24 項番 8】

端末が、端末登録後に登録状態が変化した通知を受けたい場合、登録イベントパッケージの機能を利用して、通知を受けることができる。

c.6.1. 登録イベントの購読

網が管理する端末の登録状態が未登録状態へと変化した通知を受ける場合、端末は登録後に SUBSCRIBE リクエストに登録イベントを設定し、網へ登録状態変更通知の購読を要求する。網が登録状態変更通知を提供している場合は、JF-IETF-RFC3265[RFC3265]で規定する手順に従い購読を受け付け、NOTIFY リクエストに登録状態の情報を設定し端末へ通知する。

c.6.2. 登録イベントの通知

端末の登録状態が未登録状態へと変化した場合、網は登録通知予約を行っている端末に対して、NOTIFY リクエストに未登録状態の情報を設定し通知する。

付属資料 d.　　SIP 能力交換

（本付属資料は仕様の一部である。）

d.1.　概要

本付属資料は、SIP 信号に関する能力交換の手順について規定する。

d.2.　送信可能メソッド

本標準で必ず利用可能であるメソッド（INVITE、ACK、BYE、CANCEL）以外のメソッドについて、網が端末の送信を許容する場合に、利用可否を判断する能力交換の手順について示す。

d.2.1.　UPDATE

端末は、送信する Initial INVITE リクエスト及び INVITE リクエストに対する 18x/2xx レスポンスに Allow ヘッダを設定し、UPDATE を記載することで、UPDATE リクエストの受信能力を表明する。

また端末は、Initial INVITE リクエストまたは最後に受信した 18x/2xx レスポンスに Allow ヘッダが設定されており、かつ当該ヘッダに UPDATE が記載されている場合は、UPDATE リクエストの送信が許容される。なお、Early ダイアログにおいては、UPDATE リクエスト送信前に PRACK リクエストのトランザクションが完了している必要がある。

d.2.2.　PRACK

端末は、受信した 1xx（≠100(Trying)）レスポンスに Require ヘッダが設定され、かつ 100rel が記載されている場合に、当該レスポンスに対して PRACK を送信する。

d.3.　拡張機能

拡張機能について、利用可否を判断する能力交換の手順について示す。

d.3.1.　セッションタイマ機能（timer）

端末は、INVITE リクエスト及び UPDATE リクエスト送信時に Supported ヘッダに timer を設定することにより、本機能のサポートを網に伝える（INVITE リクエスト及び UPDATE リクエストに Require ヘッダを設定して timer を記述してはならない）。

d.3.2.　暫定応答の信頼性確保機能（100rel）

端末は、INVITE リクエスト送信時に Supported ヘッダに 100rel を設定することにより、本機能のサポートを網に伝える（INVITE リクエストに Require ヘッダを設定して 100rel を記述してはならない）。

端末は、送信した INVITE リクエストに対して Require ヘッダに 100rel が設定された 1xx レスポンス（≠100(Trying)）を受信した場合、当該レスポンスに限り 100rel 拡張機能を有効とし、PRACK リクエストの送信を行う。

付属資料 e.　　SDP とメディアの扱い

（本付属資料は仕様の一部である。）

e.1.　概要

本付属資料は、JF-IETF-RFC4566[RFC4566]及び JF-IETF-RFC3264[RFC3264]を補足し、SDP を用いたメディア確立及びメディアの変更に関して規定する。

e.2.　メディアの変更要求の判断

e.2.1.　SDP の受信

SDP を含んだ re-INVITE リクエストもしくは UPDATE リクエストを受信した場合､以前のメディア確立／変更の際に受信していたオファーまたはアンサーの SDP に記載されていた o=行の sess-version の値と比較し、異なっている場合に限りメディアの変更要求と判断する。

メディアの変更要求に対してその変更内容を実行できない場合には、488(Not Acceptable Here)レスポンスを返送するが、既存のセッションの終了処理を行わず、その扱いはセッション変更要求をした側の端末の判断に委ねることとする。

e.2.2.　SDP の送信

複数コーデックを記載してオファー（メディアとして RTP を使用し、m=行の fmt 部に複数の payload type を記載したオファー）を行った場合、アンサーで一部のコーデックのみが選択される。その後、当該端末がセッション更新などメディアの変更要求を行わない re-INVITE または UPDATE リクエストを送信する場合は、JF-IETF-RFC4028[RFC4028]の 7.4 節に記載の通り、o=行の sess-version の値を変更せず、またそれに伴い、JF-IETF-RFC3264[RFC3264]の 8 章に記載の通り、sess-version 以外の SDP の内容に関しても変更しない。なお、UPDATE リクエストを用いてセッション更新を行う場合は JF-IETF-RFC4028[RFC4028]の 7.4 節に従い、SDP を設定しないことが推奨される。

e.3.　ペイロードタイプ

メディアとして RTP を使用する場合、m=行の fmt 部に指定する RTP のペイロードタイプ番号としては、JF-IETF-STD65[RFC3551]に静的な対応付けが行われているコーデックに関しては、当該番号を用いる。例えば、G.711 μ-law の場合は、fmt 部に 0 を使用することとする。

また、コーデックの規定によりダイナミックペイロードタイプを用いてコーデックを指定し、アンサーとして当該コーデックを選択する場合において、アンサーの m=行にオファーと同一のダイナミックペイロードタイプを設定する。

なお、m=行の fmt 部に設定できるコーデックの最大数は、網によって指定される場合がある。【付表 1-21 項番 3】

e.4.　フォールバック手順

e.4.1.　IP バージョンの不一致

端末は、Initial INVITE を受信した際に、要求された IPv6 による通信が不可と判断した場合には、warn-code として 300(Incompatible network protocol)もしくは 301(Incompatible network address formats)が設定された Warning ヘッダを含む 488(Not Acceptable Here)レスポンスを返却すべきである。

端末は、送信した Initial INVITE リクエストに対して warn-code が 300(Incompatible network protocol)もしくは 301(Incompatible network address formats)の Warning ヘッダを含む 488(Not Acceptable here)レスポンスを受信

する場合がある。IPv6 を用いて発信した場合に上記のレスポンスを受信した場合、IPv6 を用いた通信が不可能と解釈して、IPv4 によるフォールバックを試みてもよい。ただし、フォールバックした呼に対し、上記レスポンスを受信してもさらなる再発信はしないこととする。

e.4.2. メディア種別の不一致

受信した SDP に対応可能でないメディア種別が設定されている場合においては、端末は 488(Not Acceptable Here)レスポンスを返送する。端末は 488 レスポンスの Warning ヘッダに warn-code として 304(Media type not available)を設定する。

付属資料 f.　　輻輳の防止・抑制

（本付属資料は仕様の一部である。）

f.1.　概要

本付属資料は、輻輳を防止または抑制するために網及び端末が行うべき動作について規定する。

f.2.　端末登録時における輻輳抑制への考慮

網が UNI において端末登録（REGISTER）を必須とする場合、当該網の全てのユーザが定期的に REGISTER 信号を送信することとなるため、網は定常的に多量の信号を処理する負荷が生じる。このため、端末登録に際しては網に不必要な負荷をかけないよう、端末側の動作に考慮が必要である。

f.2.1.　エラーレスポンス受信時の扱い

端末は、送信した REGISTER リクエストに対して Retry-After ヘッダを含むエラーレスポンス（4xx – 6xx レスポンス: JF-IETF-RFC3261[RFC3261]では 404(Not Found)レスポンス、413(Request Entity Too Large)レスポンス、480(Temporary Unavailable)レスポンス、486(Busy Here)レスポンス、500(Server Internal Error)レスポンス、503(Service Unavailable)レスポンス、600(Busy Everywhere)レスポンス、603(Decline)レスポンス）を受信する場合がある。この場合、輻輳状態等、網に何らかの問題が発生している可能性があるため、さらなる輻輳を避けるべく Retry-After ヘッダによって指定された時間後に端末登録を再試行する（指定時間後に REGISTER リクエストを再送したとしても再度エラーレスポンスを受信することも考慮する）。

Retry-After ヘッダを含まないエラーレスポンスを受信した場合にも、同様の理由により、適切な時間が経過後に端末登録の再試行を行う（ただし、401(Unauthorized)レスポンスの受信時を除く）。

f.2.2.　無応答時の扱い

端末は、送信した REGISTER リクエストに対して、SIP 信号の再送タイムアウトが発生しレスポンスを受信できない場合がある。また、SIP のアプリケーションレイヤより下位のレイヤにおいてエラーとなる場合（ICMP によるエラー通知等）もある。このような場合は、端末は適切な時間が経過した後に、端末登録の再試行を行う。【付表 1-24 項番 7】

f.2.3.　複数 Contact アドレス登録における留意事項

端末登録動作による網の不必要な負荷を防止するために、例えば 1 つの端末が複数の AoR を管理している場合や、複数の Contact アドレスを網に登録する必要がある場合において、複数の REGISTER リクエストを送信する場合などには、端末は短い時間に連続して REGISTER リクエストを送信しないよう考慮すべきである。

f.2.4.　ユーザ名またはパスワードの誤り

端末は、Authorization ヘッダを含んだ REGISTER リクエストに対して、網から 401(Unauthorized)レスポンスを受信した場合、WWW-Authenticate ヘッダの stale パラメータの値が TRUE であった場合を除き、同一のユーザ名とパスワードを用いた端末登録の再試行を行わず、不必要な REGISTER リクエストの送信を避けるようにすべきである。

f.2.5.　一時的障害時の端末再登録

端末が何らかの原因で一時的に SIP メッセージの送受信ができない状況を検出した場合には、その原因が

取り除かれ SIP メッセージの送受信が可能になったときに、端末自身の Contact アドレスの変更有無や、登録の保持期限に関わらず、速やかに端末登録の更新や再登録を行うような考慮をすべきである。

ただし、アクセスネットワークにおける広域障害の一斉復旧を契機として端末登録動作が一斉に行われることによる網の輻輳や、一時的障害の断続的な繰り返しによる端末登録の不要な繰り返しを避けるために、障害復旧後の REGISTER リクエストの送信は、ある適切な時間内で統計的に一様となる時間だけ待った後に行うような考慮をするべきである。なお、網が無応答の場合に REGISTER リクエストを再送する間隔に関しては、網により規定される場合がある。【付表 1-24 項番 7】

f.3. 発信時における輻輳抑制への考慮

輻輳状態にあり呼損が生じているような網に対して、端末からさらに繰り返し発信（REGISTER 以外の既存ダイアログ外リクエスト送信）が行われると、輻輳がより悪化する恐れがある。このため、呼損とする際に網が輻輳状態にあることを端末に通知する手順と、端末が網から通知された情報をユーザに対して通知する手順を規定し、網からユーザに対して輻輳状態にあることを通知することによって、ユーザの再発信行動そのものを抑制することを図る。

また、発信時のエラーレスポンスに対して端末が無制限に発信の再試行を行い、輻輳の原因となることのないよう、発信の再試行条件を規定する。

f.3.1. 輻輳通知

網の信号輻輳を回避するために、網が端末に対して送信するエラーレスポンスによる輻輳等の情報通知、及び当該エラーレスポンスに対する端末での対応について記載する。

f.3.1.1. 網から端末への通知

網が、輻輳等により端末からのいかなるリクエストについてもサービスを提供できない場合、端末から受信したリクエストに対して、Reason ヘッダ（protocol が Q850、protocol-cause が 42（交換機輻輳））を含む 503(Service Unavailable)レスポンスが送信され、網がサービスを提供できない状態であることが通知される。また、網から輻輳以外の理由により Reason ヘッダ（protocol が Q850、protocol-cause が 42）を含むレスポンスが端末に送信されることはない。

なお、f.3.2.1節で示す付加情報の通知が、本節で示す輻輳通知に合わせて行われる場合がある。

f.3.1.2. 端末からユーザへの通知

端末は、Reason[RFC3326]ヘッダ（protocol に Q850、protocol-cause に 42（交換機輻輳））が設定された 503(Service Unavailable)レスポンスを受信した場合、網が輻輳等によりいかなるリクエストについてもサービスを提供できない状態であると認識し、ユーザにその旨を通知するための可視表示、あるいは端末に内蔵する輻輳通知のためのガイダンスや輻輳を示す信号音など、可聴音の生成などを行う。また、自動再発信など、その後の自動動作を行ってはならない。

なお、f.3.2.1節で示す付加情報の通知が同時に行われた場合は、f.3.2.1節で示す付加情報の表示を優先して行う。

f.3.2. 付加情報の通知

Warning ヘッダを用いて、網から端末へ付加的な情報を通知する手順を示す。

f.3.2.1. 網から端末への通知

網は、エラー時等においてユーザに対して付加情報を提供したい場合に、端末に返すレスポンスメッセージに Warning ヘッダを付与し、warn-code として 399(Miscellaneous warning)を設定することで、warn-text に任意のテキスト情報を埋め込み端末へ通知することができる。また、網はユーザへの通知を意図する情報が含まれている場合を除き、warn-code が 399 である Warning ヘッダを設定したレスポンスを端末に送信してはならない。

f.3.2.2. 端末からユーザへの通知

端末は、warn-code が 399 である Warning ヘッダが設定されたレスポンスを受信した場合、当該のテキスト情報をユーザに通知すべきである。端末がテキスト情報の可視表示を可能とする場合は、積極的に当該情報を表示することでユーザに提供すべきである。また、端末が可聴音の生成を可能とする場合には、当該情報を読み上げる等の実装も検討されるべきである。

f.3.3. ユーザ名またはパスワードの誤り

端末は、送信したリクエストに対して網から Proxy-Authenticate ヘッダを含んだ 407(Proxy Authentication Required)レスポンスを受信した場合、Proxy-Authenticate ヘッダの stale パラメータが TRUE であるか、またはこれまでに受信をしていない realm パラメータが設定された WWW-Authenticate ヘッダもしくは Proxy-Authenticate ヘッダが存在した場合を除き、同一のユーザ名とパスワードを用いてリクエストを再度送信すべきではない。

付属資料 g.　　帯域制御

（本付属資料は仕様の一部である。）

g.1.　概要

本付属資料は、NGN の特徴である帯域制御機能に関して、シグナリング手順、及びトランスポート層プロトコルとの関係について、JT-Y1221[Y.1221]を参照し規定する。

以下では、TR-1014[TR-1014]に示されるリソース受付制御機能（RACF）を用いた方式によって帯域制御が行われることを前提として記述を行っているが、網内の実装に関しては他の方式を用いて実現することも許容される。ただし、その場合でも、UNI においては本付属資料の規定に従った帯域制御機能を提供し、当該機能で要求された帯域を網内に確保することが求められる。

g.2.　参考文献

本付属資料で参照する参考文献を以下に示す。

[Y.1221]　"IP ネットワークにおけるトラヒック制御と輻輳制御方式 (Traffic control and congestion control in IP based networks)", TTC 標準 JT-Y1221 第 2 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2013 年 2 月

[Y.1540]　ITU-T 勧告 Y.1540, "Internet protocol data communication service – IP packet transfer and availability performance parameters", 2007

[Y.1541]　ITU-T 勧告 Y.1541, "Network performance objectives for IP-based services ", 2007

[RFC2474]　"IPv4 及び IPv6 ヘッダにおける DS フィールドの規定", TTC 標準 JF-IETF-RFC2474 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

[RFC2475]　"DiffServ 実現のためのアーキテクチャ", TTC 標準 JF-IETF-RFC2475 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

g.3.　NGN における帯域制御の仕組み

JT-Y1221 の付属資料 a に従う。また、JT-Y1221 の付属資料 a を UNI に適用する際の補足規定、及びオプション項目を下記に示す。

- JT-Y1221 の a.2.3 節に示される、一次比例の関係を適用せず個別にトークンバケットサイズを設定する場合の値については、網で定める。【付表 1-13 項番 1】
- UNI におけるレート係数の値のうち、JT-Y1221 に示される品質クラスαについては、JT-Y1221 の a.2.5.1 節に従う。その他の品質クラスに適用される値については、網で定める。網で定める値は、g.5節に示す品質クラスによって異なる可能性がある。【付表 1-13 項番 2】。

g.4.　SIP/SDP に関する規定

JT-Y1221 の付属資料 a に従う。また、JT-Y1221 の付属資料 a を UNI に適用する際の補足規定、及びオプション項目を下記に示す。

- JT-Y1221 の a.2.2 節に従い、トークンバケット速度は SDP の b=行で指定された値とする。ただし、

音声通信においては、網がコーデックに対して個別のトークンバケット速度を定め、b=行を用いた端末からの申告に代わって適用してもよい。【付表 1-13 項番 3】

- b=RR 行及び b=RS 行の利用可否は網で定める。【付表 1-13 項番 4】
- b=RR 行及び b=RS 行が指定されない場合における RTCP の帯域として、JT-Y1221 の a.2.2.1 節に記載される推奨値である RTP 帯域の 5%以外とする場合は、網で別途定める。【付表 1-13 項番 5】

g.5. 品質クラス

JT-Y1221 の a.1.4 節及びその従属節に示されるように、NGN では、異なる条件を持つ複数のサービスを同一の網で同時に提供する。

例えば、Web ブラウザなどによる http 通信と、0AJ の IP 電話を同時に提供する場合、それぞれのサービスに提供される QoS（Quality of Service）は一般に異なっている。

この QoS にはサービスにより固有のさまざまな要素があるが、本付属資料では、IP パケットの転送品質に関して扱う。具体的には、Y.1540[Y.1540]に示される、IP Packet Transfer Delay（IPTD : 以下「遅延」）、IP packet Delay Variation（IPDV：以下「ゆらぎ」）、IP packet Loss Ratio（IPLR：以下「損失率」）を扱う。また、これら「遅延」「ゆらぎ」「損失率」の組によって定義される IP パケットの転送品質を、品質クラスと呼ぶこととする。なお、提供する品質クラスは網で定める。【付表 1-13 項番 6】

g.5.1. 複数の品質クラスの提供と DiffServ

NGN では、品質クラス毎に網のリソースを割り当て、かつサービス毎に品質クラスを割り当てることによって、サービスに応じた品質クラスの提供が可能となる。例えば、g.5節の例であれば、Web ブラウザの http 通信には、遅延・ゆらぎ・損失率が保証されないベストエフォート通信としての品質クラスを、また 0AJ の IP 電話の通信には、遅延・ゆらぎ・損失率が保証される品質クラスを、それぞれ割り当てることになる。

各品質クラスで定めた条件を満たすためには、それぞれの通信で用いられる IP パケットが属する品質クラスが NGN のアクセス網及びコア網で識別され、各品質クラスに応じた扱いを受ける必要がある。そのために、NGN では Y.1221[Y.1221] Appendix III に従い、DiffServ[RFC2474][RFC2475]を用いて、IP パケットの DSCP 値を用いた転送の優先度付けを行う。なお、UNI に適用する具体的な DiffServ の DSCP 値については、網で定める。【付表 1-13 項番 7】

g.5.2. DSCP 値の付与

NGN のエンド・トゥ・エンドの品質クラスを提供するため、UNI-UNI、UNI-NNI の通信の全域にわたって、IP パケットの優先制御が必要である。このため、IP パケットへの DSCP 値の付与は、端末及び網によって下記のように行う。

- UNI 区間における優先制御を適切に行うため、端末は網へ IP パケットを送信する際に、DSCP 値を設定する。
- 網内における優先制御を適切に行うため、網は、端末から受信した IP パケットを網内に取り込む際に、DSCP 値を再設定してもよい。

付属資料 h.　SIP メッセージの文字列長と設定値の範囲

（本付属資料は仕様の一部である。）

h.1.　概要

本付属資料は、SIP 及び SDP に関して、文字列の最大長や設定値の範囲について明確化する。

h.2.　各種最大長と設定値の範囲

端末が網から受信して正常に処理を行えなければならない条件（端末の受信条件）を示す。端末は本付属資料に示す条件より高い受信能力を具備してもよい。端末から網への送信が許容される信号条件についても受信能力の条件と同様とするが、網は異なる条件を定めてもよい。また、網は本節に示す条件に追加して、またはより詳細化して、受信条件と送信条件を定めてもよい。【付表 1-21 項番 1～2】

なお、本付属資料に特段の記載がない文字列長や設定値の範囲については、本標準が参照する各参照文献に従う。

h.2.1.　SIP

SIP に関して、各種最大長及び設定値の範囲を、推奨条件とともに付表 h-1 に示す。各項目の説明には、明確化のため JF-IETF-RFC3261[RFC3261]の 25.1 節に示される ABNF 文法中のフィールド名を使用している。

付表 h-1／JT-Q3402　SIP に関する文字列長・設定値条件

項目		文字列長・設定値条件	備考
全般	SIP メッセージの 1 行あたりの文字列長（Request-Line, Status-Line, message-header）	行末（CR+LF）を含め 255 バイト以下	
ダイアログ・ルート管理	Via の段数（via-parm の個数）	10Hop 以下	
	Via の branch（via-branch）の文字列長	z9hG4bK を含め 128 バイト以下	
	To/From tag（tag-param の token）の文字列長	128 バイト以下	
	Call-ID（callid）の文字列長	128 バイト以下	
	Route Set を構成する URI の個数	10Hop 以下	
	Record-Route の 1 つの URI（rec-route）の文字列長	128 バイト以下	
	Contact アドレス（contact-param）の文字列長	128 バイト以下	
発着 URI	発信先 URI（Reqiuest-URI）の文字列長	128 バイト以下	
	P-Preferred-Identity 及び P-Asserted-Identity の 1 つの URI の文字列長	128 バイト以下	
端末登録	REGISTER 先の SIP-URI（REGISTER リクエストの Request-URI）	32 バイト以下	
	HTTP Digest 認証時の realm の文字列長	64 バイト以下	
	HTTP Digest 認証時のユーザ名の文字列長	32 バイト以下	
	HTTP Digest 認証時のパスワードの文字列長	32 バイト以下	

h.2.2.　SDP

SDP に関して、各種最大長及び設定値の範囲を、推奨条件とともに付表 h-2 に示す。各項目の説明には、明確化のため JF-IETF-RFC4566[RFC4566]の 9 章に示される ABNF 文法中のフィールド名を使用している。

付表 h-2／JT-Q3402　SDP に関する文字列長・設定値条件

項目		文字列長・設定値条件	備考
全般	SDP の 1 行あたりの文字列長	行末（CR+LF）を含め 255 バイト以下	
	SDP（session-description）の長さ	1000 バイト以下（UDP 使用時）	
o=	o=行の username の文字列長	64 バイト以下	
	o=行の sess-id の値の範囲	63 ビット非負整数（0～2^{63}-1）	JF-IETF-RFC3264[RFC3264] 5 章
	o=行の sess-version の値の範囲	63 ビット非負整数（0～2^{63}-1）	
s=	s=行の text の文字列長	64 バイト以下	

付属資料 i.　音声端末の動作に関する規定

（本付属資料は仕様の一部である。）

i.1.　概要

本付属資料では、NGN 端末のうち、特に電話端末やテレビ電話端末などに特有の動作に関して規定する。

i.2.　コーデック

JT-G711[G711]に規定される G.711μ-law（64kbit/s）のサポートを必須とする。また、デコード処理としては、JT-G711 付録 1 に規定される PLC（Packet Loss Concealment）機能を備えることが望ましい。

i.2.1.　パケット化周期

端末は、G.711μ-law を SDP のネゴシエーションに含める場合は、G.711μ-law のパケット化周期として 20ms への対応を必須とする。

SDP オファー時に G.711μ-law に対して a=ptime 行を設定する場合は、パケット化周期として 20ms を設定することが推奨される。a=ptime 行の設定条件と、パケット化周期として指定する値は、網により規定される場合がある。【付表 1-15 項番 1, 2】

SDP アンサー時に G.711μ-law に対して a=ptime 行を設定する場合は、オファーの a=ptime 行に設定されたパケット化周期を指定する。ただし、オファーに a=ptime 行が設定されていない場合は、20ms を設定する。a=ptime 行の設定条件は、網により規定される場合がある。【付表 1-15 項番 1】

i.3.　切断時の動作

切断時においては、SIP 信号のシーケンスとしては、CANCEL リクエストの再送状態や、Initial INVITE リクエストに対する最終レスポンス未受信、200(OK)レスポンス受信にともなう BYE リクエストの再送状態などの状態が考えられるが、いずれの場合においても、新規の発着呼に伴う新たな Initial INVITE リクエストの送受信を並行して処理可能とする。

i.3.1.　CANCEL/BYE リクエスト送信

端末はユーザからの切断要求（オンフックやアプリケーション終了時等）等により途中放棄を行うために CANCEL リクエストを送信した場合は、CANCEL リクエストに対する 2xx レスポンスを未受信であっても、また CANCEL リクエストに対する 2xx レスポンス受信後 Initial INVITE リクエストに対する最終レスポンス未受信であっても、それらのトランザクションはタイマ内で保持及び処理継続したまま、その間においてユーザより新規発信要求があった場合は、次 INVITE トランザクションを生成し新たな Initial INVITE リクエストを送信できなければならない。

端末が通話中にユーザリソースの終話を検出した際に、BYE リクエスト未受信であれば自ら当該ダイアログを解放する BYE リクエストを送信し、ダイアログ／メディア／ユーザリソースの解放を行う。なお、BYE トランザクションの状態（BYE リクエストの再送状態や、エラーレスポンス受信状態）に関わらず、新規発着呼のための Initial INVITE リクエスト送受信を可能とする。

i.3.2.　CANCEL/BYE リクエスト受信（最終応答前）

端末が Initial INVITE リクエストに対する最終レスポンスを送信していない状態で CANCEL リクエストもしくは BYE リクエストを受信した場合は、当該リクエスト及び Initial INVITE リクエストへのレスポンスを送信の上で、ユーザリソース呼出の停止／解放処理を行う。この場合、ACK リクエスト未受信による

487(Request Terminated)レスポンス再送中であっても、新規発着呼のための Initial INVITE リクエスト送受信は並行して処理できなければならない。

端末が通話中において BYE リクエストを受信した場合、BYE リクエストに対するレスポンスを送信するとともに、ユーザリソースに対しては BusyTone を送出するかもしくはそれに準じた動作を行う。

i.3.3. CANCEL リクエスト受信（最終応答後）

端末は着信時に、Initial INVITE リクエストに対して、2xx レスポンスを送信後、ACK リクエストを受信するまでの間に、その INVITE トランザクションやダイアログに対する CANCEL リクエストを受信した場合、ユーザリソースに対しては CANCEL リクエスト受信を契機として端末から Busy Tone を送出（もしくはそれに準じた動作）することにより発側切断であることを通知すべきである。

上記、200(OK)レスポンス送信後の CANCEL リクエスト受信の際に、ACK リクエスト未受信による 200(OK)レスポンス再送中や、ACK リクエスト受信後の BYE リクエスト未受信などの状態であっても、新規発着呼のための Initial INVITE リクエスト送受信は並行して処理できなければならない。

i.3.4. 3xx レスポンス受信

端末が Initial INVITE リクエストに対して 3xx レスポンスを受信し、当該レスポンスに含まれる Contact ヘッダで指定される宛先へ Initial INVITE リクエストを送信しない場合は、3xx レスポンス受信と同時に発呼を停止しユーザに Busy Tone などを聴取させ発信不可である旨を通知する。

i.3.5. 4xx-6xx レスポンス受信

端末が Initial INVITE リクエストに対して 4xx-6xx レスポンスを受信し、認証のための再送信やフォールバック（SDP 等の信号条件を変更した再発呼）を行わない場合は、4xx-6xx レスポンス受信と同時に発呼を停止しユーザに BusyTone などを聴取させ発信不可である旨を通知する。

特に、f.3.1.1節及びf.3.2.1節に示す形式の 503 レスポンスを受信した場合は、f.3.1.2節及びf.3.2.2節に従い輻輳抑制のためユーザにその旨を通知する。

i.3.6. 4xx-6xx レスポンス送信

端末は、Initial-INVITE リクエストに対して 4xx-6xx レスポンスを送信した場合、ACK リクエスト待ちの状態においてもユーザリソースが新規発着信処理可能である状態であれば、Initial INVITE リクエスト送受信を並行して処理できなければならない。

i.4. 呼出音の生成とダイアログ管理

i.4.1. 18x レスポンス送信

端末は、precondition 拡張機能を利用しない場合、1xx（≠100(Trying)）レスポンスについてはユーザ呼出中状態であることを判断せずに送信してはならず（例：ユーザリソースが 2W アナログインタフェースであり、ダイヤルインシーケンスを前提としている場合の、ユーザ（PBX 等）からの内線指定受信完了信号を受信するまでの間や、ナンバーディスプレイシーケンスを前提としている場合の、情報受信端末からの受信完了信号を受信するまでの間など）、またユーザ呼出中状態を判断でき次第送信する必要がある。

端末による 1xx レスポンス送信への設定 SDP 許容／非許容は、網により規定される。【付表 1-22 項番 1】

i.4.2. 18x レスポンス受信

i.4.2.1. 呼出中音の再生

SDP を含む 1xx(≠100(Trying)) レスポンスを以前に受信していない状態にて、SDP を含まない 180(Ringing) レスポンスを受信した場合には、その時点より呼出中音は自身の音源により生成しなければならない。以降同一ダイアログにおいて、どの 1xx レスポンスを受信してもそれに SDP が含まれない限り、呼出中音生成を継続しなければならず（つまり呼出中音の再生をやり直してはならない）、もし SDP が含まれている場合には、i.4.2.2節に従いメディアパスを接続して網からの音源を再生しなければならない。

i.4.2.2. Early メディアの再生

端末は SDP が設定された 1xx レスポンスを受信した場合には、パスを接続することにより Early メディアを確立できなければならない。以降同一ダイアログにおいて、どの 1xx レスポンスを受信しても、その SDP 有無にかかわらず、受信メディアの再生を継続しなければならない（つまりメディアの張り替え処理を行ってはならない）。

i.4.2.2.1. UPDATE リクエストによるメディア変更

UPDATE リクエストによる網からのオファーで指定されたメディアの変更が自身において可能であれば、適切なアンサーを含んだ 200(OK)レスポンスを返送するとともにメディア変更を行い、指定されたメディア変更が不可能な場合には 488(Not Acceptable Here)レスポンスを返す必要がある。ただし、488(Not Acceptable Here)レスポンスを返送後に端末側からは既存のセッションの終了処理を行わないこととする。

端末による Early 段階での UPDATE 送出の許容／非許容は、網により規定される。【付表 1-23 項番 1】

i.4.2.2.2. 複数ダイアログとメディアの管理

端末は、Initial INVITE リクエストに対して網から複数の 1xx（≠100(Trying)）レスポンスを受信する可能性がある。よって端末は 1 つの Initial INVITE リクエスト送信に対して、既存ダイアログ（既に複数確立している場合もある）に加えてそれまでに受信したものとは異なる To-tag を含むレスポンスを受信することで複数のダイアログが確立される場合を想定した動作を実施しなければならない。

また、複数のダイアログは、それぞれに対応した異なるメディアを持つ場合も想定した動作を実施しなければならない。

上記を考慮した発側端末の処理として、最低限の実装範囲と実装が望ましい範囲について付表 i-1 に示す。

付表 i-1／JT-Q3402　複数ダイアログとメディアの管理（発側 SIP 端末）

	既存ダイアログ	新ダイアログ	処理内容
①	Early ダイアログ	Early ダイアログ	・SDP の有無や内容等の条件でユーザインタフェース処理上どちらを優先するかのポリシーを持つことができる。但し、100rel を利用する場合には 2xx レスポンスにアンサーが含まれない場合も想定されるため、全てのメディア情報を保持しておくか、もしくは BYE リクエストを送信して明示的に Early ダイアログを終了することが望ましい。特に判断可能な条件がない場合には、新ダイアログの方を優先させる。(無応答時転送などの場合を考慮)

i.4.3. 2xx レスポンス受信

端末が 2xx レスポンスを受信した際には、当該レスポンス受信前に同一ダイアログに属する 1xx 信号によりアンサーを受信していた場合には、2xx レスポンスに含まれる SDP の内容は、それまでに確立しているメディアの内容と同一であると期待し、無視する。2xx レスポンスを受信する前にアンサーを受信していない

場合には、2xx レスポンスに含まれるアンサーによりセッション確立の処理を行う。

i.4.3.1. 複数ダイアログとメディアの管理

端末は、Initial INVITE リクエストに対して網から複数の 2xx レスポンスを受信する可能性がある。よって端末は 1 つの Initial INVITE リクエスト送信に対して、既存ダイアログ（既に複数確立している場合もある）に加えてそれまでに受信したものとは異なる To-tag を含むレスポンスを受信することで複数のダイアログが確立される場合を想定した動作を実施しなければならない。

また、複数のダイアログは、それぞれに対応した異なるメディアを持つ場合も想定した動作を実施しなければならない。

上記を考慮した発側端末の処理として、最低限の実装範囲と実装が望ましい範囲について付表 i-2 に示す。

付表 i-2／JT-Q3402　複数ダイアログとメディアの管理（発側 SIP 端末）

	既存ダイアログ	新ダイアログ	処理内容
①	Early ダイアログ	Confirmed ダイアログ	・Confirmed ダイアログの内容にメディアを変更する。Early ダイアログに関しては BYE リクエストを送信して明示的に Early ダイアログを終了するか、64×T1 後にその内容を破棄する。
②	Confirmed ダイアログ	Confirmed ダイアログ	・SDP 等の条件でどちらを優先するのか(もしくは同時に保持するのか)のポリシーを持つことができる。いずれかを選択する場合においては、明示的に他のダイアログを BYE リクエストにより解放することが望ましい。(単に ACK リクエストを返送しない場合には、2xx レスポンスの再送が生じる)

i.5. メディアの変更

i.5.1. IP アドレス・ポート番号

IP アドレスまたはポート番号（もしくは両方）を変更するメディアの変更要求に対しては、端末は変更に対応する能力を具備していなければならない。

付属資料 j.　　CUG/PNP

（本付属資料は仕様の一部である。）

j.1.　参考文献

[TS-1018]　"CUG/PNP に関するインタフェース技術仕様", TTC 仕様書 TS-1018 第 2.0 版, 情報通信技術委員会(The Telecommunication Technology Committee), 2015 年 3 月

j.2.　UNI 条件

CUG/PNP を提供する場合の、UNI インタフェース条件は、[TS-1018]に従う。

付録 i.　　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.　はじめに

本オプション項目表は、NGN に UNI を介して接続する SIP 端末の接続性を高めるために、JT-Q3402 本文、付属資料および付録における事業者が運用ポリシーにより選択可能なオプション項目を抜き出して表としたものである。事業者は各項目に関して UNI の条件を選択することができ、また端末は UNI の条件として許容される範囲内において動作を選択することができる。

本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、次の観点から項目の抽出を行っている。

UNI を介して接続する SIP 端末の接続性を高める観点からオプション項目を抽出し、見やすいように項目分類を行った。

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 1-1 に記載する。

付表 1-1／JT-Q3402　フォーマット例

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	IPv4	IPv4 による接続を提供する	端末は IPv4 による接続機能を具備する	IPv4 で接続する場合がある	13 章		
			端末は IPv4 による接続機能を具備しても良い	IPv4 で接続する場合がある			
				IPv4 で接続しない			

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。
端末の選択：　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、JT-Q3402 本文、付属資料および付録のどの章節に関連するかを示す。
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について示す。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。

i.4.　オプション項目表

オプション項目表を付表 1-2～付表 1-25 に示す。なお、本文および付属資料でサポート必須となっている項目は各表に明記していない。

付表 1-2／JT-Q3402　SIP メソッド

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	REGISTER ［端末が送信］	端末は REGISTER で 端末登録を行う	－	10.2.1.10 節 10.2.3節	【REGISTER を利用する場合は、Contact アドレスの種別・個数について記載する】	
		端末は REGISTER で 端末登録を行わない	－			
2	MESSAGE（既存ダイアログ外） ［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3428 10.2.3節	《端末が送信する場合は Content-Type とメッセージボディの形式を記載する》	
			送信しない			
		許容しない	送信しない			
3	MESSAGE（既存ダイアログ外） ［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3428 10.2.3節	《端末が受信機能を具備する場合は Content-Type とメッセージボディの形式を記載する》	
		端末は受信機能を 具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
4	MESSAGE（既存ダイアログ内） ［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3428 10.2.3節	《端末が送信する場合は Content-Type とメッセージボディの形式を記載する》	
			送信しない			
		許容しない	送信しない			
5	MESSAGE（既存ダイアログ内） ［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3428 10.2.3節	《端末が受信機能を具備する場合は Content-Type とメッセージボディの形式を記載する》	
		端末は受信機能を 具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
6	REFER（既存ダイアログ外） ［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3515 10.2.3節		
			送信しない			
		許容しない	送信しない			
7	REFER（既存ダイアログ外） ［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3515 10.2.3節		
		端末は受信機能を 具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
8	REFER（既存ダイアログ内） ［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3515 10.2.3節		
			送信しない			
		許容しない	送信しない			
9	REFER（既存ダイアログ内） ［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3515 10.2.3節		
		端末は受信機能を 具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
10	SUBSCRIBE（INVITE ダイアログ外） ［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3265 10.2.3節	《端末が送信する場合はイベント名を記載する》	
			送信しない			
		許容しない	送信しない			
11	SUBSCRIBE（INVITE ダイアログ外）	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3265 10.2.3節	《端末が受信機能を具備する場合はイベント名を記載する》	
		端末は受信機能を 具備しなくても良い	受信機能を具備する			

	［端末が受信］		受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
12	SUBSCRIBE（INVITE ダイアログ内）［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3265 10.2.3節	《端末が送信する場合はイベント名を記載する》	
			送信しない			
		許容しない	送信しない			
13	SUBSCRIBE（INVITE ダイアログ内）［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3265 10.2.3節	《端末が受信機能を具備する場合はイベント名を記載する》	
		端末は受信機能を具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
14	NOTIFY［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3265 10.2.3節	《端末が送信する場合はイベント名を記載する》	
			送信しない			
		許容しない	送信しない			
15	NOTIFY［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3265 10.2.3節	《端末が受信機能を具備する場合はイベント名を記載する》	
		端末は受信機能を具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
16	PUBLISH（INVITE ダイアログ外）［端末が送信］	許容する	送信する場合がある	10.1 節 表 10-2 / RFC3903 10.2.3節	《端末が送信する場合はイベント名を記載する》	
			送信しない			
		許容しない	送信しない			
17	PUBLISH（INVITE ダイアログ外）［端末が受信］	端末は受信機能を具備する	－	10.1 節 表 10-2 / RFC3903 10.2.3節	《端末が受信機能を具備する場合はイベント名を記載する》	
		端末は受信機能を具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
18	PUBLISH（INVITE ダイアログ内）［端末が送信］	許容する	送信する場合がある	10.1 節 表 10-2 / RFC3903 10.2.3節	《端末が送信する場合はイベント名を記載する》	
			送信しない			
		許容しない	送信しない			
19	PUBLISH（INVITE ダイアログ内）［端末が受信］	端末は受信機能を具備する	－	10.1 節 表 10-2 / RFC3903 10.2.3節	《端末が受信機能を具備する場合はイベント名を記載する》	
		端末は受信機能を具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
20	その他のメソッド［端末が送信］	許容する	送信する場合がある	10.2.3節	【網が利用を許容する場合はメソッド名を記載する】 《端末が送信する場合はメソッド名を記載する》	
			送信しない			
		許容しない	送信しない			
21	その他のメソッ	端末は受信機能を具備する	－	10.2.3節	【網が端末に受信機	

	ド ［端末が受信］	端末は受信機能を 具備しなくても良い	受信機能を具備する		能を求める場合はメソッド名を記載する】 《端末が受信機能を具備する場合はイベント名を記載する》	
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			

付表 1-3／JT-Q3402　IP バージョン・IP 拡張機能

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	IPv4	IPv4 による接続を提供する	端末は IPv4 による接続機能を具備する	IPv4 で接続する場合がある	13章		
			端末は IPv4 による接続機能を具備しても良い	IPv4 で接続する場合がある			
				IPv4 で接続しない			
2	IPv6	IPv6 による接続を提供する	端末は IPv6 による接続機能を具備する	IPv6 で接続する場合がある	13章		
			端末は IPv6 による接続機能を具備しなくても良い	IPv6 で接続する場合がある			
				IPv6 で接続しない			
		IPv6 による接続を提供しない	端末は IPv6 で接続を行わない	－			
3	呼制御信号とメディアの IP バージョン	同一の IP バージョンのみ許容する		同一の IP バージョンを利用する	13章		
		同一または異なる IP バージョンを許容する		同一の IP バージョンを利用する			
				同一または異なる IP バージョンを利用する			
4	呼制御信号への IPsec の適用	IPsec による接続を提供する	端末は IPsec による接続機能を具備し、必ず利用する	－	13章	【IPsec による接続を提供する場合は条件を記載する】	
			端末は IPsec による接続機能を具備しなくても良い	IPsec で接続する場合がある			
				IPsec で接続しない			
		IPsec による接続を提供しない	端末は IPsec で接続を行わない	－			

付表 1-4／JT-Q3402　呼制御信号に利用するレイヤ 4 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
1	UDP	UDP による接続を提供する	端末は UDP による接続機能を具備する	UDP で接続する場合がある	12章	【送信または受信にデフォルト（5060 番）以外のポート番号を使用する場合は記載する】	
			端末は UDP による接続機能を具	UDP で接続する場合がある			

			備しなくても良い	UDP で接続を行わない			
		UDP による接続を提供しない	端末は UDP で接続を行わない	－			
2	TCP（TLS なし）	TCP による接続を提供する	端末は TCP による接続機能を具備する	TCP で接続する場合がある	12章	【待ち受けにデフォルト（5060 番）以外のポート番号を使用する場合は記載する】	
			端末は TCP による接続機能を具備しなくても良い	TCP で接続する場合がある			
				TCP で接続を行わない			
		TCP による接続を提供しない	端末は TCP で接続を行わない	－			
3	TCP（TLS あり）	TLS による接続を提供する※1	端末は TLS による接続機能を具備する	TLS で接続する場合がある	12章	【待ち受けにデフォルト（5061 番）以外のポート番号を使用する場合は記載する】	
			端末は TLS による接続機能を具備しなくても良い	TLS で接続する場合がある			
				TLS で接続を行わない			
		TLS による接続を提供しない	端末は TLS で接続を行わない	－			

※1 TLS による接続を利用する場合に認証を行う場合は、付表 1-11 項番 1～2 において認証手順として HTTP Digest 認証を選択する。

付表 1-5／JT-Q3402 SigComp

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	SigComp の利用	全セッションで利用する	端末は本機能を具備し、全てのメッセージで本機能を用いて送受信を行う	－	10.1節 表 10-2 / RFC3320 表 10-2 / RFC3485 表 10-2 / RFC3486 表 10-2 / RFC5049		
		必要に応じて個々のセッションで利用する	端末は本機能用いた信号の受信機能を有する	本機能を利用して信号を送信する場合がある			
				本機能を利用した信号の送信は行わない			
		利用しない	端末は本機能を用いた信号の送信を行わず、受信時は破棄する	－			

付表 1-6／JT-Q3402 Hosted NAT

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	UNI 下部（ユーザ宅内）における Hosted NAT の許容	許容する	Hosted NAT を設置する	10.1 節 表 10-2 / RFC3581		
			Hosted NAT を設置しない			
		許容しない	Hosted NAT を設置しない			

付表 1-7／JT-Q3402　SIP オプションタグ

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	セッションタイマ機能（timer）	全セッションで利用する	端末は本機能を具備し※1、要求に応じ※2、表明し※3、表明があれば要求する※4	－	10.2.1.20.32 節	【セッションのタイムアウト時間を定める場合は delta-seconds 値を記載する】	
		必要に応じて個々のセッションで利用する	端末は本機能を具備し、要求に応じる	表明し、表明があれば要求する			
				表明しない場合や要求しない場合がある			
2	暫定応答の信頼性確保機能（100rel）	全セッションで利用する	端末は本機能を具備し、表明し、要求に応じ、表明があれば要求する	－	10.1 節 表 10-2 / RFC3262 10.2.1.20.32 節		
		必要に応じて個々のセッションで利用する	端末は本機能を具備し、要求に応じる	表明し、表明があれば要求する			
				表明・要求する場合がある			
			端末は本機能を具備しなくても良い	表明し、表明があれば要求する			
				表明・要求する場合がある			
3	ダイアログ置換機能（replaces）	必要に応じて個々のセッションで利用する	端末は本機能を具備し、要求に応じる	表明・要求する場合がある	10.1 節 表 10-2 / RFC3891		
				表明・要求しない			
			端末は本機能を具備しなくても良い	表明・要求する場合がある			
				表明・要求しない			
		利用しない	端末は本機能を表明・要求せず、要求を拒否する※5	－			
4	会議セッション参加機能（join）	必要に応じて個々のセッションで利用する	端末は本機能を具備し、要求に応じる	表明・要求する場合がある	10.1 節 表 10-2 / RFC3911		
				表明・要求しない			
			端末は本機能を具備しなくても良い	表明・要求する場合がある			
				表明・要求しない			
		利用しない	端末は本機能を表明・要求せず、要求を拒否する	－			
5	確立前帯域確保機能（precondition）	必要に応じて個々のセッションで利用する	端末は本機能を具備し、要求に応じる	表明・要求する場合がある	10.1 節 表 10-2 / RFC3312 表 10-2 / RFC4032		
				表明・要求しない			
			端末は本機能を具備しなくても良い	表明・要求する場合がある			
				表明・要求しない			
		利用しない	端末は本機能を表明・要求せず、要求を拒否する	－			
6	端末能力通知機能（pref）	必要に応じて個々のセッションで利用する	端末は本機能を具備し、要求に応じる	表明・要求する場合がある	10.1 節 表 10-2 / RFC3840 表 10-2 / RFC3841		
				表明・要求しない			
			端末は本機能を具備しなくても	表明・要求する場合がある			

			良い	表明・要求しない			
		利用しない	端末は本機能を表明・要求せず、要求を拒否する	－			
7	REGISTER 経路記録機能（path）	利用する	端末は本機能を具備し、端末登録時に必ず表明する	－	10.1 節 表 10-2 / RFC3327		
		利用しない	端末は本機能を表明しない	－			
8	セキュリティ能力交換機能（sec-agree）	利用する	端末は本機能を具備し、必ず要求する	－	10.1 節 表 10-2 / RFC3329	【利用する場合は、セキュリティ能力を記載する】 《利用する場合は、端末が具備するセキュリティ機能を記載する》	
		利用しない	端末は本機能を要求しない	－			
9	その他の SIP オプションタグ	必要に応じて個々のセッションで利用する	端末は網の規定に従い当該機能を具備する	－	10.2.1.20.32節	【利用する場合は、SIP オプションタグ名と利用条件を決定する】	
			端末は当該機能を具備しなくても良い				
		利用しない	端末はその他の機能を表明・要求せず、要求を拒否する	－			

※1 機能を「具備する」とは、端末が当該機能を実装していることを示す（機能が発現することを必ずしも意味しない）。
※2 機能の「要求に応じる」とは、Require ヘッダで指定された場合に、当該機能を発現させることを意味する。
※3 機能を「表明する」とは、当該機能を具備していることを Supported ヘッダで示すことを意味する。
※4 機能を「要求する」とは、当該機能の発現を要求することを Require ヘッダで示すことを意味する。
※5 機能の「要求を拒否する」とは、リクエストの Require ヘッダで要求された場合に、420 レスポンスを返しリクエストを受け付けないことを意味する。

付表 1-8／JT-Q3402　timer

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	UPDATE メソッドによるセッション更新	利用する	端末は本機能を具備し、可能ならば利用する	－	10.1節 表 10-2 / RFC4028		
		利用しない	端末は UPDATE でセッション更新を行わない	－			

付表 1-9／JT-Q3402　サブアドレス

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	発サブアドレス	発サブアドレス機能を提供する	端末は着信時の発サブアドレス受信機能を具備する	発信時に発サブアドレスを使用する場合がある	付属資料b.7節		
				発信時に発サブアドレスを使用しない			
		発サブアドレス機能を提供しない	端末は発サブアドレスを使用せず、受信した場合は無視する	－			

2	着サブアドレス	着サブアドレス機能を提供する	端末は着信時の着サブアドレス受信機能を具備する	発信時に着サブアドレスを使用する場合がある	付属資料b.7節		
				発信時に着サブアドレスを使用しない			
		着サブアドレス機能を提供しない	端末は着サブアドレスを使用せず、受信した場合は無視する	－			

付表 1-10／JT-Q3402　MIME Multipart

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	INVITE リクエストでの MIME Multipart の利用［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC2046	《端末が送信する場合は Multipart の内容を記載する》	
			送信しない			
		許容しない	送信しない			
2	INVITE リクエストでの MIME Multipart の利用［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC2046	【端末が受信機能を具備する Multipart の内容を記載する】 《端末が受信機能を具備する Multipart の内容を記載する》	
		端末は受信機能を具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
3	MESSAGE リクエストでの MIME Multipart の利用［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC2046	《端末が送信する場合は Multipart の内容を記載する》	
			送信しない			
		許容しない	送信しない			
4	MESSAGE リクエストでの MIME Multipart の利用［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC2046	【端末が受信機能を具備する Multipart の内容を記載する】 《端末が受信機能を具備する Multipart の内容を記載する》	
		端末は受信機能を具備しなくても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			

付表 1-11／JT-Q3402　認証

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	認証 （REGISTER）	HTTP Digest 認証を実施する	端末は HTTP Digest 認証機能を具備する	－	10.1節 表 10-2 / RFC2617 表 10-2 / RFC3310 表 10-2 / RFC3329		
		AKA 認証を実施する※1	端末は AKA 認証機能を具備する	－			
		実施しない（アクセス回線に基づく認証を実施する）	－	－			

2	認証（REGISTER 以外の既存ダイアログ外リクエスト）	HTTP Digest 認証を実施する	端末は HTTP Digest 認証機能を具備する	－	10.1節 表 10-2 / RFC2617 表 10-2 / RFC3310 表 10-2 / RFC3329		
		AKA 認証を実施する※1	端末は AKA 認証機能を具備する	－			
		実施しない（アクセス回線に基づく認証を実施する）	－	－			

※1 AKA 認証を実施する場合、付表 1-3 項番 4 で IPsec による接続を提供する必要がある。

付表 1-12／JT-Q3402　リダイレクション

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
1	3xx レスポンスによるリダイレクションの利用［端末が送信］	リダイレクション機能を提供する	送信する場合がある	10.2.1.8.3節	【リダイレクションを許容する場合はメソッドとレスポンスコードを記載する】	
			送信しない			
		リダイレクション機能を提供しない	送信しない			
2	3xx レスポンスによるリダイレクションの利用［端末が受信］	端末は 3xx 受信時にリダイレクションを行う	－	10.2.1.8.3節	【リダイレクションを許容する場合はメソッドとレスポンスコードを記載する】	
		端末は 3xx 受信時にリダイレクションを行わない	－			

付表 1-13／JT-Q3402　帯域制御

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	トークンバケットサイズの個別指定	指定する		－	付属資料g.3節	【指定する場合は、上限値・下限値を定める】	
		指定しない		－			
2	レート係数	品質クラス毎にレート係数を規定する		－	付属資料g.3節	【レート係数の値を決定する】	
		単一のレート係数を規定する		－			
3	コーデックに対応づけたトークンバケット速度	利用する		－	付属資料g.3節	【利用する場合は、コーデック毎の条件を示す】	
		利用しない		－			
4	b=RR／b=RS を用いた RTCP 帯域指定	利用する	端末は b=RR／b=RS の受信機能を具備する	利用する	付属資料g.4節		
				利用しない			
			端末は b=RR／b=RS を受信時に無視してもよい	利用しない			
		利用しない	端末は b=RR／b=RS を受信時に無視する	利用しない			
5	b=RR／b=RS 未指定時の RTCP 帯域	RTP 帯域の 5%とする		－	10.1節 表 10-2 / RFC3556 付属資料g.4節	【5%以外の帯域を利用する場合は、帯域の決定方法を示す】	
		5%以外の値を利用する		－			
6	品質クラス	複数の品質クラスを提供する		－	付属資料g.5節	【品質クラスを規定する場合は、各要素について記載する】 《端末は利用する品質クラスを記載する》	
		単一の品質クラスを提供する		－			
7	品質クラス毎の	規定する		－	付属資料g.5.1節	【DSCP 値を規定する	

	DSCP 値	規定しない	－		場合は記載する】	

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
1	映像（m=video）	許容する	利用する場合がある	10.3.1節 / 表 10-8		
			利用しない			
		許容しない	利用しない			
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】 《端末が利用する場合はメディア種別を記載する》	
			利用しない			
		許容しない	利用しない			
3	メディアの TCP 接続	許容する	オファーする場合がある	10.3.1節 / 表 10-8	【TCP を許容するメディア種別（SDP の m=行）及び proto 部を決定する】 《端末が利用する場合はメディア種別及び proto 部を記載する》	
			オファーしない			
		許容しない	オファーしない			

付表 1-15／JT-Q3402　G.711μ-law 利用時の条件

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	G.711μ-law を利用する場合の a=ptime 行の設定	必須とする	設定する	付属資料i.2.1節		
		必須としない	設定する			
			設定しない			
2	G.711μ-law をオファーする場合のパケット化周期	20ms のみ許容する	－	付属資料i.2.1節	【20ms 以外を許容する場合は、許容するパケット化周期を記載する】	
		20ms 以外を許容する	－			

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
1	G.711 μ-law 以外の音声帯域コーデック	G.711 μ-law 以外の音声帯域コーデックを許容する	G.711 μ-law 以外の音声帯域コーデックを利用する	8.1節	【G.711 μ-law 以外のコーデックを許容する場合は記載する】 《端末が G.711 μ-law 以外のコーデックを利用する場合は記載する》	
			G.711 μ-law 以外の音声帯域コーデックを利用しない			
		G.711 μ-law 以外の音声帯域コーデックを許容しない	G.711 μ-law 以外の音声帯域コーデックを利用しない			
2	映像コーデック	許容する	利用する	8.1節	【許容する場合はコ	

			利用しない		ーデック名を記載する】 《端末が利用する場合はコーデック名を記載する》	
		許容しない	利用しない			
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】 《端末が利用する場合はプロトコル名を記載する》	
			利用しない			
		許容しない	利用しない			

付表 1-17／JT-Q3402　メディア関連の SIP ヘッダ

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	P-Media-Authorization ヘッダ	利用する	端末は受信能力を具備する	送信しない	10.1節 表 10-2 / RFC3313		
			端末は受信能力を具備しなくてもよい	送信せず、受信した場合はヘッダの内容に従い動作する			
				送信せず、受信した場合は無視する			
		利用しない	端末は送信せず、受信した場合は無視する	－			

付表 1-18／JT-Q3402　メディアのグループ化

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	メディアのグループ化 （a=group 行、a=mid 行）	利用する	端末は受信能力を具備する	送信する場合がある	10.1節 表 10-2 / RFC3388 表 10-2 / RFC3524	【利用する場合は利用可能なセマンティクスを記載する】 《端末が利用する場合は、利用するセマンティクスを記載する》	
				送信しない			
			端末は受信能力を具備しなくてもよい	送信する場合がある			
				送信しない			
		利用しない	端末は受信した場合は無視する	送信しない			

付表 1-19／JT-Q3402　RTCP を用いたフィードバック制御

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	RTCP を用いたフィードバック制御のための RTCP パケット（RTPFB、PSFB）	許容する	－	利用する場合がある	11.1節	《端末が利用する場合はフィードバックの方式を記載する》	
				利用しない			
		許容しない	端末は受信した場合は無視する	利用しない			
2	RTCP を用いたフィードバック制御のための SDP	許容する	－	利用する場合がある	11.1節	《端末が利用する場合はフィードバックの方式を記載する》	
				利用しない			

	記述（RTP/AVPF）の利用	許容しない	端末は受信した場合は適切なエラーレスポンスを返す	利用しない			

付表 1-20／JT-Q3402　URI 形式

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	国内番号以外を用いる Request-URI 形式（REGISTER を除く既存ダイアログ外リクエスト）	許容する	利用する場合がある	9 章 付属資料 b.6 節	【許容する場合は URI 形式を記載する】 《利用する URI 形式を記載する》	
			利用しない			
		許容しない	利用しない			
2	国内番号利用時における、SIP-URI の hostport 部、及び TEL-URI の context の descriptor 部	ドメインを指定	－	9 章 付属資料 b.6.2 節	【ドメイン名または IP アドレスを示す】	
		IP アドレスを指定	－			

付表 1-21／JT-Q3402　SIP/SDP の文字列長や設定値の範囲

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	付属資料 hに規定していない，SIP に関する文字列長・設定値条件	設定する	－	付属資料h.2.1節	【設定する場合は具体的な送信条件／受信条件を示す】	
		設定しない	－			
2	付属資料 hに規定していない，SDP に関する文字列長・設定値条件	設定する	－	付属資料h.2.2節	【設定する場合は具体的な送信条件／受信条件を示す】	
		設定しない	－			
3	m=行の fmt 部に設定できるペイロードタイプの数	網で最大数を規定する	－	付属資料e.3節	【最大数を規定する場合は値を記載する】 《端末がオファーする場合に fmt 部に記述する最大のペイロード数を記載する》	
		網で最大数を規定しない	－			

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
1	1xx レスポンスへの SDP 設定［端末が送信］	許容する	設定する場合がある	付属資料 g.4.1 節		
			送信しない			
		許容しない	送信しない			

2	PRACK リクエストによる SDP オファー［端末が送信］	許容する	設定する場合がある	10.2.1.7.4.1 節		
			設定しない			
		許容しない	設定しない			
3	PRACK リクエストによる SDP オファー［端末が受信］	端末は受信能力を具備する	－	10.2.1.7.4.1 節		
		端末は受信能力を具備しなくてもよい	受信能力を具備する			
			受信能力を具備しない			
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】《送信する SDP 行を記載する》	
		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】《受信をサポートする SDP 行を記載する》	
		利用しない	－			

付表 1-23／JT-Q3402　メディア変更

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	アーリーダイアログでのメディア変更［端末が送信］	許容する	送信する場合がある	10.1節 表 10-2 / RFC3311		
			送信しない			
		許容しない	送信しない			
2	アーリーダイアログでのメディア変更［端末が受信］	端末は受信機能を具備する	－	10.1節 表 10-2 / RFC3311		
		端末は受信機能を具備しても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
3	re-INVITE によるダイアログ確立後のメディア変更［端末が送信］	許容する	送信する場合がある	10.2.1.14節		
			送信しない			
		許容しない	送信しない			
4	re-INVITE によるダイアログ確立後のメディア変更［端末が受信］	端末は受信機能を具備する	－	10.2.1.14節		
		端末は受信機能を具備しても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			
		端末は受信した場合は適切なエラーレスポンスを返す	－			
5	UPDATE によるダイアログ確立後のメディア変更［端末が送信］	許容する	送信する場合がある	10.2.1.14節		
			送信しない			
		許容しない	送信しない			
6	UPDATE によるダイアログ確立後のメディア変更［端末が受信］	端末は受信機能を具備する	－	10.2.1.14節		
		端末は受信機能を具備しても良い	受信機能を具備する			
			受信した場合は適切なエラーレスポンスを返す			

		端末は受信した場合は適切なエラーレスポンスを返す	－			

付表 1-24／JT-Q3402　端末登録

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	端末登録時の pre-existing ルート提供（ Service-Route ヘッダ）※1	提供する	端末は提供される pre-existing ルートを利用する	－	付属資料c.3.1節		
		提供しない	端末は pre-existing ルートを設定しない	－			
2	網側アドレスの取得	DHCP/DHCPv6 により、網側の IP アドレス/ポート番号を提供する		－	付属資料c.2節	【DHCP と事前設定以外の場合は手順を記載する】	
		端末に網側の IP アドレス/ポート番号を事前設定する		－			
		上記以外の方法により、IP アドレス/ポート番号を提供する		－			
3	REGISTER 時の網付与ユーザ ID の通知（ P-Associated-URI ヘッダの利用）	通知する場合がある		通知を受けた場合は受信した SIP-URI を利用する	付属資料b.3.1節	【通知する場合は条件を記載する】	
		通知しない		－			
4	端末登録時の Contact の expires パラメータ値、もしくは Expires ヘッダの設定値	網で固定値を定める		指定された値を設定する	付属資料c.3節	【固定値を定める場合は値を記載する】	
		網では固定値を定めない		任意値を設定する			
				設定しない			
5	更新時の Contact の expires パラメータ値、もしくは Expires ヘッダの設定値	網で規定する		指定された値を設定する	付属資料c.4節	【計算式もしくは固定値を定める場合は記載する】	
		網で規定しない		任意値を設定する			
				設定しない			
6	Contact アドレスへの q パラメータの設定	許容する		設定する	付属資料c.3節	【網で許容する場合は設定条件を記載する】	
				設定しない			
		許容しない		設定しない			
7	網が無応答の場合に REGISTER リクエストを送信する間隔	網で規定する		指定された値で送信する	付属資料f.2.5節	【網で規定する場合は間隔を記載する】《網で規定されない場合は端末の送信間隔を記載する》	
		網で規定しない		端末の実装に従い送信する			
8	端末の登録状態通知（reg イベント）機能	提供する		登録通知を購読する場合がある	付属資料c.6節		
				登録通知の購読は行わない			
		提供しない		登録通知の購読は行わない			

※1　本手順を利用するためには、付表 1-7 項番 7 の端末能力通知機能（path）を利用する必要がある。

付表 1-25／JT-Q3402　RTP パケットの送受信

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	SDP アンサーを	送信を開始する	－	7.1節		

	含む INVITE の 1xx レスポンス受信時における端末の RTP 送信動作	送信を開始してもよい	送信する			
			送信しない			
		送信を開始しない	－			
2	Initial INVITE に対する最終 SDP ネゴシエーションが行われる前のメディアパケットの扱い	端末に送信を開始する場合がある	－	7.1節		
		端末に送信を開始しない	－			

付表 1-26／JT-Q3402　CUG/PNP

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	CUG/PNP	提供する	利用する	付属資料 j		
			利用しない			
		提供しない	利用しない			

付録 ii.　　レスポンスコードの用途

（本付録は参考資料であり、仕様ではない。）

ii.1.　はじめに

NGN は、音声通信以外にもメッセージ通信やデータ通信など、多様な通信形態で用いられる。従来の音声通信においては、接続失敗時には網からの音声ガイダンスをユーザに聴取させるだけであったが、メッセージ通信やデータ通信などにおいては、音声ガイダンスではなく SIP のレスポンスコードをもとにユーザへ通知することが必要となる。また、音声通信を行う端末であっても、ソフトフォンをはじめ画面表示能力を有する高機能な端末では、レスポンスコードに応じて、ユーザにエラー理由の画面表示を行うことがより望ましいと考えられる。

端末が SIP のレスポンスコードをもとにエラー理由を適切に表示するためには、レスポンスコードの意味する情報が、網及び端末で一致している必要がある。しかし、JF-IETF-RFC3261[RFC3261]が示すレスポンスコードの定義は、実際に NGN での通信において生起する事象そのものを表現しているわけではないため、具体例との対応付けにゆらぎが生じ、ユーザへの適切な表示が行えなくなる可能性がある。

このため、本付録では、レスポンスコードの利用法の具体例を示すことにより、レスポンスコードの意味づけを解釈する助けとする。ただし、本付録に示す以外のレスポンスコードの利用法も網により許容される場合がある。

ii.2.　4xx 系レスポンス

ii.2.1.　403 Forbidden

網は、端末が指定した発信先が当該加入者に許容されていない場合など、加入者ないし端末からのアクセスが許容されないリソースへの接続が行われようとした場合に、403(Forbidden)応答を返す。

端末は、着信時に発信者 ID の内容から判断して着信拒否を行う場合に、403(Forbidden)で応答する。また、403(Forbidden)を受信した場合は、網または着側端末によって着信が拒否された（「接続拒否」）と解釈すべきである。

ii.2.2.　404 Not Found

網は、指定された加入者が存在しない場合や、加入者までのルーチングが不可能である場合、また発信先番号列が長すぎる場合など Request-URI が不適切な場合は、音声ガイダンスを提供する代わりに 404(Not Found)で応答してもよい。

端末は、網から指定されたサブアドレスでの着信を受け付ける端末が存在しない場合に、404(Not Found)で応答する。また、404(Not Found)を受信した場合は、発信先が不適切であった（「欠番または宛先なし」）と解釈すべきである。

ii.2.3.　410 Gone

網は、発信先として指定された加入者が異なる URI に変更されているが、端末に対してリダイレクションの指示は行わない場合は、音声ガイダンスで移転した旨を通知する代わりに、410(Gone)で応答してもよい。また、それ以外の場合に 410(Gone)を返すべきではない。

端末は、移転と混同することがないよう、不必要に 410(Gone)を返すべきではない。410(Gone)を受信した場合は、発信先が移転したなど URI が変更された（「移転」）と解釈すべきである。

ii.2.4. 433 Anonymity Disallowed

非通知呼に対して着信を拒否するサービスを提供する網は、当該サービスにより着信を拒否する場合、音声ガイダンスを提供する代わりに JF-IETF-RFC5079[RFC5079]で規定される 433(Anonymity Disallowed)で応答してもよい。

端末は、発信者 ID が非通知であることを理由として着信拒否を行う場合に、433(Anonymity Disallowed)で応答する。また、433(Anonymity Disallowed)を受信した場合は、非通知であることを理由に着信を拒否された（「非通知拒否」）と解釈すべきである。

ii.2.5. 480 Temporarily Unavailable

網は、指定された加入者が存在するが、端末外れなどの理由で通信不可能である場合（端末が未登録または登録の有効期限が切れている場合等）に、音声ガイダンスを提供する代わりに 480(Temporarily Unavailable)で応答してもよい。

端末は、480(Temporarily Unavailable)を受信した場合は、着側端末が端末外れなど一時的に着信不可能な状態（「端末不在」）であると解釈すべきである。

ii.2.6. 486 Busy Here

網は、発側加入者または着側加入者に許容されるセッション数を超えて呼接続が行われようとした場合に、486(Busy Here)で応答する。

端末は、着信した端末が既に他の通信を行っているために着信不可である場合に、486(Busy Here)で応答する。また、486(Busy Here)を受信した場合は、呼接続に必要な網または着側端末のセッション数が不足している（「話中」）と解釈すべきである。INVITE リクエストの他、MESSAGE や SUBSCRIBE、REGISTER などのリクエストに対しても 486(Busy Here)が返される可能性について留意すべきである。

ii.2.7. 487 Request Terminated

網は、発信中で未確立の呼を終了する場合に、端末から CANCEL リクエストを受信しているか否かに関わらず、487(Request Terminated)で応答してよい。一定時間以上にわたり呼び出し中の状態が続いた場合や、ガイダンスを終了する場合等が該当する。

端末は、487(Request Terminated)を受信した場合は、上記のような事象が生じたと解釈すべきである。

ii.2.8. 488 Not Acceptable Here

網は、端末から送信された INVITE または UPDATE リクエストに設定された SDP の内容が受け付けられない（当該 SDP に指定されたメディア種別やコーデック、帯域、IP アドレス種別等での通信が不可能である）場合、488(Not Acceptable Here)で応答する。また、それ以外の場合に 488(Not Acceptable Here)を返すべきではない。

端末は､受信した INVITE または UPDATE リクエストに設定された SDP の内容が受け付けられない場合、488(Not Acceptable Here)で応答する。それ以外の場合に 488(Not Acceptable Here)を返すべきではない。また、488(Not Acceptable Here)を受信した場合は、網または着側端末が SDP を受け入れなかったと解釈すべきである。

ii.3. 5xx 系レスポンス

ii.3.1. 503 Service Unavailable

網は、輻輳状態または故障状態など、端末に対してサービスを提供できない状態である場合、付属資料 f

に示すように、503(Service Unavailable)応答を返す。

端末は、網の輻輳や故障と混同することがないよう、不必要に 503(Service Unavailable)を返すべきではない。また、503(Service Unavailable)を受信した場合は、付属資料 fに示すように動作する。

付録 iii.　SDP 記述を用いた品質クラスとの対応付け方式

（本付録は参考資料であり、仕様ではない。）

iii.1.　概要

本付録では、付属資料 gに規定される品質クラスを決定するために、SDP のメディア記述内容から品質クラスを対応づける方式を例として示す。ただし、UNI における QoS クラスの関連づけ方式は、本付録で示す例に限定されない。

iii.2.　考え方

網が複数の品質クラスを提供している場合、メディアの性質に合わせて適切な品質クラスを選択する必要がある。メディアは SDP で記述されることから、1 つの実現方式として、この SDP の記述内容からメディアの性質を読み取り、暗黙的なルールによって品質クラスへの対応付けを行う方式が考えられる。

IP パケットの転送品質に関連するメディアの性質としては、メディアの種別と、方向性がある。

メディアの種別とは、音声（m=audio）か、映像（m=video）か、データ（m=application 等）か、という通信の種類であり、SDP では m=行の proto で示される。

音声に関しては（0AJ で求められる品質を提供する等の理由により）、遅延・ゆらぎ・損失率ともに低くすることが望ましい。映像に関しても、音声とのリップシンクを考慮すれば、音声と同等の遅延・ゆらぎ・損失率とすることが望ましいと考えられる。一方で、データ通信に関しては、一般には遅延やゆらぎは音声や映像ほど低くすることが求められない。損失率に関しても、データ通信の場合は再送により回復できる場合が多い。このように、メディアの種別について考慮すると、音声や映像は高い優先度で、データに関してはそれらよりも低い優先度の品質クラスを割り当てることが適切と思われる。

メディアの方向性とは、通信が双方向（a=sendrecv）か、片方向（a=recvonly / a=sendonly）か、という通信の種類であり、SDP では方向属性で示される。

双方向通信（音声電話やテレビ電話など）では、通信の相手から受けた情報を元に応答を返すまでの時間として、網内の遅延が直接的に実感されてしまう。一方で片方向通信（ストリーミングなど）では通信の相手から受信するのみ、ないし通信の相手に送信するのみであるため、網内の遅延が見えづらい。従って、双方向通信は高い優先度で、片方向通信はそれよりも低い優先度の品質クラスを割り当てることが適切と思われる。

iii.3.　対応付けの例

メディアの種別と方向性に基づき、SDP のメディア記述の内容から各メディアを QoS クラスに対応づける例を示す。

iii.3.1.　SDP

種別が音声（m=audio）や映像（m=video）のメディアは高い優先度で、データ（m=application）のメディアは低い優先度とする。また、優先度が高い音声や映像のメディアに関しては、メディアの方向属性が双方向（a=sendrecv）の場合により高い優先度を、片方向（a=recvonly / a=sendonly）の場合には双方向よりも低い優先度とする。

上記の対応付けにより、SDP 記述から 3 種類の品質クラスが選択される（付表 2-1）。

付表 2-1／JT-Q3402　SDP 記述と品質クラスの対応付けの例

品質クラス	メディアの SDP 記述		サービス例
	種別	方向属性	
最優先クラス	音声（m=audio） 映像（m=video）	双方向 （a=sendrecv）	音声電話、テレビ電話
高優先クラス	音声（m=audio） 映像（m=video）	片方向 （a=recvonly / a=sendonly）	映像ストリーミング
優先クラス	データ （m=application）	双方向または片方向 （a=sendrecv / a=recvonly / a=sendonly）	データ配信、機器の遠隔制御

なお、品質が要求されない通信のために、付表 2-1 に示す優先クラスよりも下の品質クラスとして、SIP/SDP を用いたリソース受付制御を行わないベストエフォートクラスを設定することを想定している。

付録 iv.　セキュリティ

（本付録は参考資料であり、仕様ではない。）

iv.1.　概要

本付録では、UNI におけるセキュリティに関して、14章で示される要求条件を満たす上で有効と期待されるソリューション例について示す。

iv.2.　UNI における必要条件

UNI においては、下記の事項がセキュリティの観点から考慮されるべきである。

1) 改竄の防止
UNI を通じて通信する SIP 信号が第三者によって改竄されないこと。

2) なりすまし（Spoofing）の防止
端末が受信する SIP 信号がなりすましでなく確実に SIP トラストドメインから送信されていること。

3) ユーザ情報の秘匿
ユーザを特定する情報が、不必要に対向する端末に通知されないこと。

iv.3.　ソリューション例

iv.3.1.　発 IP アドレスの限定

なりすましの防止のため、例えば以下のように発 IP アドレスを限定する処理が有効と期待される。

- 端末が受信する SIP 信号で発 IP アドレスが網のバウンダリ（群）であるパケットは確実に網のバウンダリ（群）からのパケットであることが保証されるよう、UNI において何らかの手段によるパケットのフィルタリングを行う（発 IP アドレスのなりすましの防止）。
- 端末は受信する SIP 信号の発 IP アドレスが事前に設定した網のバウンダリ（群）のアドレスと一致する場合にのみ正当な SIP トラストドメインからの着信と判断し、接続を受け付ける。

iv.3.2.　利用ポートの限定

なりすましの防止のため、例えば以下のように利用ポートを限定する処理が有効と期待される。

- 端末が SIP 信号の送受信で使用するポート番号を特定のポートに限定する。
- 端末が受信するパケットで着ポート番号が前項で定めた特定のポートであるものは確実に網のバウンダリ（群）からのパケットであることが保証されるよう、UNI において何らかの手段によるパケットのフィルタリングを行う（他からの特定ポートの利用防止）。

なお、この場合、上記の特定ポートは別の用途で利用できなくなることに留意されるべきである。

iv.3.3.　Contact ヘッダのランダム化（端末登録時）

端末が SIP トラストドメイン以外から SIP 信号を直接受信する可能性がある網構成の場合、端末は登録時に指定する Contact アドレスの user 部を、以下に示す理由のとおり、容易に第三者に推測されない任意のラ

ンダムな文字列とすることが推奨される。

- 端末は既存ダイアログ外リクエスト受信時に、その Request-URI と登録した Contact アドレスの比較を行うことで着信信号の正当性判断を行うが、この Contact アドレスとしてユーザ名や自身の電話番号などの容易に第三者に推測され得る値を用いた場合には、SIP トラストドメインを介さない不正な既存ダイアログ外リクエストによるいたずら呼被害を受ける可能性が高くなるため。
- DHCP や PPPoE といった IP アドレスを自動取得するような網構成で、取得のたびに端末の IP アドレスが変更される場合は、端末に予期せぬ障害（停電等）が発生した場合にも、網は当該 Contact アドレスを保持し続けることになる。このような状況下において、当該 IP アドレスが別の端末に払い出されてしまった場合、本来は予期せぬ障害が発生した端末に送信されるべきリクエストが、異なる端末に送信される事態が発生し得るが、端末が既存ダイアログ外リクエスト受信時に user 部の一致検証を行うことにより、表面上の誤着信動作を予防することが可能であるため。

iv.3.4. Contact ヘッダのランダム化（発信時）

端末が SIP トラストドメイン以外から SIP 信号を直接受信する可能性がある網構成の場合、端末は既存ダイアログ外リクエストに設定する Contact アドレスの値に、第三者に容易に推測できないユニークな user 部を生成することが望ましい。また、当該端末が端末登録時に REGISTER リクエストに設定した Contact アドレスとは user 部が異なった文字列とすることが望ましい。ただし、同一ダイアログ内における後続のトランザクションで文字列を変更しない。

iv.3.5. ヘッダ透過転送に関する留意事項

端末が設定した SIP/SDP 情報は、網でフィルタリングや書き換えが行われず、着側の UNI や NNI へ通知される可能性があるため、付属資料 b に示したヘッダ以外の SIP ヘッダや、SDP 構成要素などにユーザ情報に相当する文字列を設定すべきではない。

付録 v.　　SCF アドレスの取得

（本付録は参考資料であり、仕様ではない。）

v.1.　概要

本付録では、付属資料c.3節に規定される端末登録において、SCF のアドレスを取得するための手順を例として示す。ただし、SCF のアドレスを取得する手順は、本付録で示す例に限定されない。

v.2.　参考文献

本付録で参照する参考文献を以下に示す。

[RFC2131]　"動的なホスト設定プロトコル", TTC 標準 JF-IETF-RFC2131 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

[RFC3315]　"IPv6 における動的なホスト設定プロトコル", TTC 標準 JF-IETF-RFC3315 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

[RFC3319]　"SIP サーバ情報取得のための DHCPv6 オプション", TTC 標準 JF-IETF-RFC3319 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

[RFC3361]　"SIP サーバ情報取得のための DHCP オプション", TTC 標準 JF-IETF-RFC3361 第 1.0 版, 情報通信技術委員会（The Telecommunication Technology Committee）, 2009 年 5 月

v.3.　DHCP/DHCPv6

網が IPv4 による接続を提供する場合、IPv4 端末に対して DHCP[RFC2131]を用いる手順を提供する。DHCP を用いる場合、端末はオプション 120[RFC3361]を要求することで、SCF の IPv4 アドレス及びポート番号が提供される。オプション 120 の要求に対してドメイン一覧が返された場合は、さらに JF-IETF-RFC3263[RFC3263]に規定される手順に従い、DNS を用いて IPv4 アドレス及びポート番号を解決する必要がある。

網が IPv6 による接続を提供する場合、IPv6 端末に対して DHCPv6[RFC3315]を用いる手順を提供する。DHCPv6 を用いる場合、端末はオプション 22[RFC3319]またはオプション 21[RFC3319]を要求することで、SCF の IPv6 アドレス及びポート番号が提供される。オプション 21 でドメイン一覧が返された場合は、さらに JF-IETF-RFC3263[RFC3263]に規定される手順に従い、DNS を用いて IPv6 アドレス及びポート番号を解決する必要がある。

v.4.　端末の事前設定

端末には、事前設定により、SCF の IP アドレス及びポート番号を設定する。

付録 vi.　　SIP メッセージとヘッダ情報

（本付録は参考資料であり、仕様ではない。）

本付録では各々の SIP メソッドについて、リクエストメッセージおよびレスポンスメッセージのヘッダ情報の設定条件について、ダイナミックビューにより記載している。

vi.1.　ダイナミックビューとスタティックビュー

vi.1.1.　スタティックビュー

3GPP の TS24.229 の付属資料 A 等に見られるような各ヘッダの適用条件について「送信側」「受信側」の SIP エンティティでの機能具備を M（Mandatory）や O（Optional）などとして記載したものをスタティックビュー（Static View）による表現形式という。

スタティックビューでは、インタフェース規定点の両側の SIP エンティティが、当該のヘッダ情報を理解しているか、つまりは、内容を把握し RFC 等に規定のとおりに動作する機能が具備されているかという観点で M（Mandatory）や O（Optional）が分類される。従って、M（Mandatory）だからといって、必ずしも SIP メッセージ内で当該ヘッダが記述されるわけではないという特徴を有する。

vi.1.2.　ダイナミックビュー

RFC3261 等の RFC で書かれている各ヘッダの適用条件表では､スタティックビューのような｢送信側」「受信側」という適用区分は存在しておらず、SIP エンティティ間のインタフェース上の信号として、まさに現れるか、情報項目として存在するか、という観点で M（Mandatory）や O（Optional）が表現されており、これをダイナミックビュー（Dynamic View）という。

ダイナミックビューでは、インタフェース規定点で当該ヘッダが存在するかという情報の出現（appearance）可否が書かれ、M（Mandatory）であれば、当該のヘッダは、当該のメッセージに必ず記述されなくてはならない。

vi.1.3.　本付録でのダイナミックビューの採用について

本付録ではインタフェースに係わる規定の明確化であることを念頭にダイナミックビューによる表現を用いることとする。

vi.1.4.　本付録内の表における条件コードの定義

各表の「RFC」および「本書の規定」の列に記載される条件コードの定義は、RFC3261 と同等である。

付表 6-1／JT-Q3402　条件コードの定義

条件コード	定義
m	当該のヘッダフィールドは、必須である。リクエストメッセージ中の必須のヘッダフィールドは存在していなくてはならず、また、リクエストメッセージを受ける UAS 側で理解され得なくてはならない。同じくレスポンスメッセージ中の必須のヘッダフィールドは存在していなくてはならず、また、レスポンスメッセージを処理する UAC 側で理解され得なくてはならない。
m*	当該のヘッダフィールドは、メッセージ中に存在するべきである。しかし、メッセージを受け取るクライアントもしくはサーバは、当該のヘッダフィールドが存在しない場合にも備えておかなくてはならない。なお、事業者により"m"または"o"とする明確化が行われる場合がある。
t	当該のヘッダフィールドは、メッセージ中に存在するべきである。しかし、メッセージを受け取るクライアントもしくはサーバは、当該のヘッダフィールドが存在しない場合にも備えておかなくてはならない。 なお、SIP メッセージのトランスポートレイヤーに TCP を利用する場合、当該のヘッダフィードは必須であり、送信されなくてはならない。
o	当該のヘッダフィールドは選択的である。選択的とは、当該のヘッダフィールドは、リクエストやレスポンスメッセージに存在しても良い。また当該のヘッダフィールドがリクエストやレスポンスメッセージ内に存在した場合には、RFC に従い受信側で理解され、対応する動作が行われなければならない。なお、事業者により"m"または"－"とする明確化が行われる場合がある。 （注）ただし、特に規定される場合、当該のヘッダフィールドがリクエストやレスポンスメッセージ内に存在した場合でも無視することが許容される。これらの規定については適用条件欄および備考欄に注記される。当該のヘッダフィールドに係わるオプション項目を選択している場合、当該のヘッダフィールドはオプション項目に記載の規定に従う。
－	当該のヘッダフィールドは適用されない。適用されない当該のヘッダフィールドは、リクエストやレスポンスメッセージ内に存在してはならない。
c	当該のヘッダフィールドの適用は、メッセージの文脈による。 （注）本書では、適用条件欄にヘッダフィールドの適用に関する条件を記載することで、RFC で「c」と既定されているヘッダフィールド以外を「c」と記載することは行っていない。本書での「c」については、信号の文脈上で当該のヘッダフィールドが必要になる場合があるということを示す。なお、事業者により"m"または"－"とする明確化が行われる場合がある。 なお、信号を利用するものの条件として、設定が必要になるヘッダフィールドについては、RFC での規定を尊重しつつ、適用条件欄および備考欄に注記される。
*	当該のヘッダフィールドは、メッセージボディ部が存在する場合に適用され存在しなくてはならない。

vi.2. ACK

本メッセージは、INVITE リクエストに対する最終レスポンスを得た場合に、順方向に転送される。

vi.2.1. ACK リクエストメッセージでサポートされるヘッダ

付表 6-2／JT-Q3402 Supported headers within the ACK request

メッセージ種別： リクエスト

Method： ACK

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Allow-Events	RFC3265	o	o	o	c2（付表 1-2 項番 10～15）	c2（付表 1-2 項番 10～15）	
Authorization	RFC3261	o	－	－	c3	c3	
Call-ID	RFC3261	m	m	m			
Contact	RFC3261	o	o	o			
Content-Disposition	RFC3261	o	－	－	c4	c4	
Content-Encoding	RFC3261	o	－	－	c4	c4	
Content-Language	RFC3261	o	－	－	c4	c4	
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	－	－	c4	c4	
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	－	－	c4	c4	
P-Media-Authorization	RFC3313	o	－	－	c5	c6	
Privacy	RFC3323	o	－	－	c7	c7	
Proxy-Authorization	RFC3261	o	o	－	c8（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」の場合）	c9	
			－	－	c8（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」以外の場合）	c9	
Reason	RFC3326	o	o	o			（注 1）
Record-Route	RFC3261	o	o	o			（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Route	RFC3261	c	c	－		c10	
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261	o	－	－	c4	c4	

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7 項番 6）

c2: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）

c3: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c4: 付属資料a.3の付表 a-1の 10.2.1.13 により ACK による SDP ネゴシエーションは行わないためメッセージボディを利用しない。

c5: 付属資料a.3の付表 a-1の 10.1 により EUF から SCF 方向では利用されない。

c6: 付属資料a.3の付表 a-1の 10.2.1.13 により ACK による SDP ネゴシエーションは行わないため、P-Media-Authorization ヘッダを用いた認証トークンの通知も行われない。

c7: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c8: REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）

c9: 本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。

c10: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.2.2. ACK レスポンスメッセージでサポートされるヘッダ

ACK リクエストメッセージ対するレスポンスメッセージは規定されない。

vi.3. BYE

本メッセージは、要求された呼が開始された後(アーリーダイアログ又はダイアログ確立後)、切断時に用いる。

vi.3.1. BYE リクエストメッセージでサポートされるヘッダ

付表 6-3／JT-Q3402 Supported headers within the BYE request

メッセージ種別： リクエスト

Method： BYE

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o	c2（付表 1-2 項番 10～15）	c2（付表 1-2 項番 10～15）	
Authorization	RFC3261	o	－	－	c3	c3	
Call-ID	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			（注 1）
Content-Encoding	RFC3261	o	o	o			（注 1）
Content-Language	RFC3261	o	o	o			（注 1）
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			（注 1）
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			（注 1）
P-Access-Network-Info	RFC3455	o	o	－		c4	（注 1）
P-Asserted-Identity	RFC3325	o	－	－	c5	c5	
P-Charging-Function-Addresses	RFC3455	o	－	－	c6	c6	
P-Charging-Vector	RFC3455	o	－	－	c6	c6	
P-Preferred-Identity	RFC3325	o	－	－	c7	c7	
Privacy	RFC3323	o	－	－	c8	c8	
Proxy-Authorization	RFC3261	o	o	－	c9（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」の場合）	c10	
			－	－	c9（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」以外の場合）	c10	
Proxy-Require	RFC3261	o	o	－		c11	
Reason	RFC3326	o	o	o			（注 1）
Record-Route	RFC3261	o	o	o			（注 1）
Referred-By	RFC3892	o	o	o	c12（付表 1-2 項番 6～9）	c12（付表 1-2 項番 6～9）	（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	c	c	c			
Route	RFC3261	c	c	－		c13	
Security-Client	RFC3329	o	o	－	c14（付表 1-11 項番 1～2、付表 1-4 項番 3）	c15	
Security-Verify	RFC3329	o	o	－	c14（付表 1-11 項番 1～2、付表 1-4 項番 3）	c15	
Supported	RFC3261	o	o	o			（注 1）
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			

メッセージボディ	RFC3261	o	o	o			（注 1）

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）

c3: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c4: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c5: 付属資料a.3の付表 a-1の 10.2.2.2.2 により P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c6: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。

c7: 付属資料a.3の付表 a-1の 10.2.2.2.3 により P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c8: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c9: REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）

c10: 本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。

c11: 付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。

c12: REFER を利用した結果として Referred-By ヘッダが用いられることがある。（付表 1-2 項番 6～9） REFER が UNI で利用可能な場合は、当該ヘッダの情報は有効に扱われるかもしれない。また REFER を用いた結果として Referred-By ヘッダが利用されることについて保証されるものではない。

c13: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

c14 AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c15: 付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.3.2.　BYE レスポンスメッセージでサポートされるヘッダ

付表 6-4／JT-Q3402　Supported headers within the BYE response

メッセージ種別：　レスポンス

Method：　BYE

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	415	RFC3261	c	c	c			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o	c1（付表 1-2 項番 10～15）	c1（付表 1-2 項番 10～15）	
Authentication-Info	2xx	RFC3261	o	－	－	c2	c2	
Call-ID		RFC3261	m	m	m			
Contact	3xx	RFC3261	o	－	－	c3	c3	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			（注 1）
Content-Encoding		RFC3261	o	o	o			（注 1）
Content-Language		RFC3261	o	o	o			（注 1）
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			（注 1）
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455	o	o	－		c4	（注 1）
P-Asserted-Identity		RFC3325	o	－	－	c5	c5	
P-Charging-Function-Addresses		RFC3455	o	－	－	c6	c6	
P-Charging-Vector		RFC3455	o	－	－	c6	c6	
P-Preferred-Identity		RFC3325	o	－	－	c7	c7	
Privacy		RFC3323	o	－	－	c8	c8	
Proxy-Authenticate	401	RFC3261	o	－	－	c9	c10	
Proxy-Authenticate	407	RFC3261	m	－	m	c9		
Reason		RFC3326	o	o	o			（注 1）
Record-Route	18x 2xx	RFC3261	o	o	o			（注 1）
Require		RFC3261	c	c	c			（注 1）
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
Security-Server	421 494	RFC3329	o	－	o	c11	c12（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
Supported	2xx	RFC3261	o	o	o			（注 1）
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c13	c13	

WWW-Authenticate	407	RFC3261	o	－	－	c13	c13	
メッセージボディ		RFC3261	o	o	o			（注 1）

c1:	SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）
c2:	対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。
c3:	付属資料a.3の付表 a-1の 10.2.1.8.3 により 3xx レスポンスを用いたリダイレクトは利用しない。
c4:	付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c5:	付属資料a.3の付表 a-1の 10.2.2.2.2 により P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c6:	付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info、P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c7:	付属資料a.3の付表 a-1の 10.2.2.2.3 により P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外リクエストにのみ適用される。
c8:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c9:	本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、401/407 レスポンス自体を利用しない。
c10:	付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは 401 レスポンスでは利用しない。すなわち、401 レスポンス自体を利用しない。
c11:	付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。
c12:	AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c13:	付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401/407 レスポンス自体を利用しない。
注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.4. CANCEL

本メッセージは、要求された呼が確立される前の発側からの切断時に用いる。

vi.4.1. CANCEL リクエストメッセージでサポートされるヘッダ

付表 6-5／JT-Q3402 Supported headers within the CANCEL request

メッセージ種別： リクエスト

Method： CANCEL

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Authorization	RFC3261	o	－	－	c2	c2	
Call-ID	RFC3261	m	m	m			
Content-Length	RFC3261	t	t	t			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
Privacy	RFC3323	o	－	－	c3	c3	
Reason	RFC3326	o	o	o			（注 1）
Record-Route	RFC3261	o	o	o			（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Route	RFC3261	c	c	－		c4	
Supported	RFC3261	o	o	o			（注 1）
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c3: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c4: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.4.2. CANCEL レスポンスメッセージでサポートされるヘッダ

付表 6-6／JT-Q3402 Supported headers within the CANCEL response

メッセージ種別： レスポンス

Method： CANCEL

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Call-ID		RFC3261	m	m	m			
Content-Length		RFC3261	t	t	t			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
From		RFC3261	m	m	m			
Privacy		RFC3323	o	－	－	c1	c1	
Proxy-Authenticate	401	RFC3261	o	－	－	c2	c2	
Reason		RFC3326	o	o	o			（注 1）
Record-Route	18x 2xx	RFC3261	o	o	o			（注 1）
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
Server		RFC3261	o	o	o			（注 1）
Supported	2xx	RFC3261	o	o	o			（注 1）
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）

c1: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c2: 付属資料a.3の付表 a-1の 10.2.1.20.27 により、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されず、SCF から EUF 方向の 401 レスポンスでも利用されない。すなわち、401 レスポンス自体を利用しない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.5. INVITE

本メッセージは、呼を開始するために利用される。

vi.5.1. INVITE リクエストメッセージでサポートされるヘッダ

付表 6-7／JT-Q3402 Supported headers within the INVITE request

メッセージ種別： リクエスト

Method： INVITE

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Alert-Info	RFC3261	o	o	o			（注 1）
Allow	RFC3261	o	m* / o	m* / o	c2	c2	
Allow-Events	RFC3265	o	o	o	c3（付表 1-2 項番 10～15）	c3（付表 1-2 項番 10～15）	
Authorization	RFC3261	o	－	－	c4	c4	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			（注 1）
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
Expires	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
In-Reply-To	RFC3261	o	o	o			（注 1）
Join	RFC3911	o	o	o	c5（付表 1-7 項番 4 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	c5（付表 1-7 項番 4 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	
			－	－	c5（付表 1-7 項番 4 で UNI 条件が「利用しない」の場合）	c5（付表 1-7 項番 4 で UNI 条件が「利用しない」の場合）	
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o	c6	c6	
Min-SE	RFC4028	o	o	o	c7	c7	
Organization	RFC3261	o	o	o			（注 1）
P-Access-Network-Info	RFC3455	o	o	－		c8	（注 1）
P-Asserted-Identity	RFC3325	o	－	o / －	c9	c9	
P-Called-Party-ID	RFC3455	o	－	o / －	c10	c10	
P-Charging-Function-Addresses	RFC3455	o	－	－	c11	c11	
P-Charging-Vector	RFC3455	o	－	－	c11	c11	
P-Media-Authorization	RFC3313	o	－	o	c12	c13（付表 1-17 項番 1 で UNI 条件が「利用する」の場合）	
			－	－	c12	c13（付表 1-17 項番 1 で UNI 条件が「利用しない」の場合）	
P-Preferred-Identity	RFC3325	o	o / －	－	c14	c14	
P-Visited-Network-ID	RFC3455	o	－	－	c11	c11	
Priority	RFC3261	o	o	o			（注 1）
Privacy	RFC3323	o	o / －	o / －	c15	c15	
Proxy-Authorization	RFC3261	o	o	－	c16（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」の場合）	c17	

			－	－	c16（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」以外の場合）	c17	
Proxy-Require	RFC3261	o	o	－		c18	
Reason	RFC3326	o	－ / o	－ / o	（注 2）	（注 2）	（注 1）
Record-Route	RFC3261	o	o	o			
Referred-By	RFC3892	o	o	o	c19（付表 1-2 項番 6～9）	c19（付表 1-2 項番 6～9）	
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Replaces	RFC3891	o	o	o	c20（付表 1-7 項番 3 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	c20（付表 1-7 項番 3 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	
			－	－	c21（付表 1-7 項番 3 で UNI 条件が「利用しない」の場合）	c21（付表 1-7 項番 3 で UNI 条件が「利用しない」の場合）	
Reply-To	RFC3261	o	o	o			（注 1）
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	c	c	c	c22	c22	
Route	RFC3261	c	m / c	－	c23（付表 1-24 項番 1 で UNI 条件が「利用する」の場合）	c24	
			－ / c	－	c23（付表 1-24 項番 1 で UNI 条件が「利用しない」の場合）	c24	
Security-Client	RFC3329	o	o	－	c24（付表 1-11 項番 1～2、付表 1-4 項番 3）	c25	
Security-Verify	RFC3329	o	o	－	c24（付表 1-11 項番 1～2、付表 1-4 項番 3）	c25	
Session-Expires	RFC4028	o	m	m	c7（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	c7（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	
			o	o	c7（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	c7（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	
Subject	RFC3261	o	o	o			（注 1）
Supported	RFC3261	m*	m*	m*	c21	c21	
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261	o	m	m	c26	c26	

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7 項番 6）

c2: 本文 10.2.1.20.5 より、Initial INVITE では Allow ヘッダの設定が必要。（ただし設定されない Initial INVITE を受信した場合もエラーとしない）

c3: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）

c4: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c5: 会議セッション参加機能（join）が UNI で利用可能な場合に当該ヘッダを利用することができる。（付表 1-7 項番 4）

c6: メッセージボディに MIME Multipart が利用される場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-10 項番 1～2）

c7: 本文 10.2.2.2.1 および 10.2.2.2.7 より、当該のヘッダを規定どおりに利用しなければならない。Session-Timer を利用する場合は、少なくとも Session-Expires ヘッダへの値（delta-seconds）の設定が必要になる。

c8: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c9: 付属資料a.3の付表 a-1の 10.2.2.2.2 及び付属資料 bにより、P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の伝達を行う。（Initial INVITE には設定可能であるが、re-INVITE には設定しない。）

c10: 付属資料 bにより、P-Called-Party-ID ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、着信対象の通知を行う。（Initial INVITE には設定可能であるが、re-INVITE には設定しない。）

c11: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses、P-Visited-Network-ID ヘッダは利用しない。

c12: 付属資料a.3の付表 a-1の 10.1 により EUF から SCF 方向では利用されない。

c13:	メッセージボディが設定され P-Media-Authorization ヘッダによる認証トークンの通知が行われる場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-17 項番 1）
c14:	付属資料a.3の付表 a-1の 10.2.2.2.3 及び付属資料 bにより、P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで EUF から SCF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、EUF が通知を要求する発信者情報の伝達を行う。（Initial INVITE には設定可能であるが、re-INVITE には設定しない。）
c15:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の通知/非通知情報を伝達する。（Initial INVITE には設定可能であるが、re-INVITE には設定しない。）
c16:	REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）
c17:	本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。
c18:	本文 10.2.1.20.29 節より、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。
c19:	REFER を利用した結果として Referred-By ヘッダが用いられることがある。（付表 1-2 項番 6～9） REFER が UNI で利用可能な場合は、当該ヘッダの情報は有効に扱われるかもしれない。また REFER を用いた結果として Referred-By ヘッダが利用されることについて保証されるものではない。
c20:	ダイアログ置換機能（replaces）が UNI で利用可能な場合に当該ヘッダを利用することができる。（付表 1-7 項番 3）
c21:	本文 10.2.1.20.32 および 10.2.1.20.37 より、"timer"については、Require ヘッダ及び Supported ヘッダに文脈上で設定する必要がある。（"timer"はその文脈上、Initial INVITE 及び re-INVITE の Supported ヘッダに設定されるべきである。）
c22:	pre-existing ルート機能が UNI で利用される場合に Initial INVITE では Route ヘッダの設定が必要。（付表 1-24 項番 1）
c23:	本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。
c24:	AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c25:	付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。
c26:	付属資料a.3の付表 a-1の 10.2.1.13 および 10.2.1.14 より、INVITE リクエストのボディ部に SDP オファーを記述する。
注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。
注 2	Reason ヘッダは、RFC3326 により規定されるが、規定では既存ダイアログ内の全てのリクエスト、CANCEL、全てのレスポンスに適用可能となっている。したがって、re-INVITE では利用可能であるが、Initial INVITE での利用はできない。

vi.5.2. INVITE レスポンスメッセージでサポートされるヘッダ

付表 6-8／JT-Q3402 Supported headers within the INVITE response

メッセージ種別： レスポンス

Method： INVITE

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	2xx	RFC3261	o	o	o			
Accept	415	RFC3261	c	c	c			
Accept-Encoding	2xx	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	2xx	RFC3261	o	o	o			
Accept-Language	415	RFC3261	c	c	c			
Alert-Info	180	RFC3261	o	o	o			（注 1）
Allow	2xx	RFC3261	m*	m*	m*			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o	c1（付表 1-2 項番 10～15）	c1（付表 1-2 項番 10～15）	
Authentication-Info	2xx	RFC3261	o	－	－	c2	c2	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			（注 1）
Contact	1xx	RFC3261	o	o	o	c3	c3	
Contact	2xx	RFC3261	m	m	m			
Contact	3xx	RFC3261	o	o	o			（注 2）
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
Expires		RFC3261	o	o	o			（注 1）
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o	c4	c4	
Min-SE	422	RFC4028	m	m	m	c5（付表 1-7 項番 1）	c5（付表 1-7 項番 1）	
Organization		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455	o	o	－		c6	（注 1）
P-Asserted-Identity		RFC3325	o	－	－	c7	c7	
P-Charging-Function-Addresses		RFC3455	o	－	－	c8	c8	
P-Charging-Vector		RFC3455	o	－	－	c8	c8	
P-Media-Authorization	101-199	RFC3313	o	－	o	c9	c10（付表 1-17 項番 1 で UNI 条件が「利用する」の場合）	
				－	－	c9	c10（付表 1-17 項番 1 で UNI 条件が「利用しない」の場合）	
P-Media-Authorization	2xx	RFC3313	o	－	o	c9		
P-Preferred-Identity		RFC3325	o	－	－	c11	c11	
Privacy		RFC3323	o	－	－	c12	c12	
Proxy-Authenticate	401	RFC3261	o	－	－	c13	c14	
Proxy-Authenticate	407	RFC3261	m	－	m	c13		
Reason		RFC3326	o	o	o			（注 1）
Record-Route	18x 2xx	RFC3261	o	o	o	c3	c3	
Reply-To		RFC3261	o	o	o			（注 1）
Require		RFC3261	c	c	c	c3, c5	c3, c5	
Retry-After	404	RFC3261	o	o	o			（注 1）

	413 480 486							
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
RSeq	1xx	RFC3262	o	o	o	c3	c3	
Security-Server	421 494	RFC3329	o	－	o	c15	c16（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
Session-Expires	2xx	RFC4028	o	m	m	c5（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	c5（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	
				o	o	c5（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	c5（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	
Supported	2xx	RFC3261	m*	m*	m*			
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning	488	RFC3261	o	o	o	c17	c17	
Warning	他	RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c18	c18	
WWW-Authenticate	407	RFC3261	o	－	－	c18	c18	
メッセージボディ		RFC3261	o	o	o			

c1: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）

c2: 対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。

c3: 本文 10.2.2.2.6 より、信頼性のある暫定応答を行う場合には、Require ヘッダへの"100rel"の設定および RSeq ヘッダの設定が必要になる。また、後続の PRACK リクエストを受け付けるために Contact ヘッダの設定が必要になる。INVITE リクエストの 2xx レスポンスに Record-Route ヘッダが設定される場合は、信頼性のある暫定応答にも同一内容の Record-Route ヘッダが設定されるべきである。

c4: メッセージボディに MIME Multipart が利用される場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-10 項番 1～2）

c5: 本文 10.2.1.20.32、10.2.2.1 および 10.2.2.2.7 より、当該のヘッダを規定どおりに利用しなければならない。Session-Timer を利用する場合には、少なくとも Session-Expires ヘッダへの値（delta-seconds）の設定が必要になる。さらに Refresher を"uac"とする場合は Require ヘッダへの"timer"の設定が必要になる。（付表 1-7 項番 1）

c6: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c7: 付属資料a.3の付表 a-1の 10.2.2.2.2 により P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c8: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。

c9: 付属資料a.3の付表 a-1の 10.1 により EUF から SCF 方向では利用されない。

c10: メッセージボディが設定され P-Media-Authorization ヘッダによる認証トークンの通知が行われる場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-17 項番 1）

c11: 付属資料a.3の付表 a-1の 10.2.2.2.3 により P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c12: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c13: 本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、401/407 レスポンス自体を利用しない。

c14: 付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは 401 レスポンスでは利用しない。

c15: 付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。

c16: AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c17: 付属資料a.3の付表 a-1の 13 および付属資料 eより、488(Not Acceptable Here)レスポンスに Warning ヘッダを設定し、付属資料 e の設定値を用いることで、IP バージョンやメディア種別の不一致を通知することが可能である。

c18: 付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401/407 レスポンス自体を利用しない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

注 2　本文 10.2.1.8.3 より、3xx レスポンスによるリダイレクション機能については、UNI で利用可能な場合に当該ヘッダの情報が有効に取り扱われる。（付表 1-12 項番 1～2）

vi.6. MESSAGE

本メッセージは、ステートレスなショートメッセージサービスに用いられる。MESSAGE は特定ダイアログに関連せず使用することが可能である。

vi.6.1. MESSAGE リクエストメッセージでサポートされるヘッダ

付表 6-9／JT-Q3402 Supported headers within the MESSAGE request

メッセージ種別： リクエスト

Method： MESSAGE

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Allow	RFC3261	o	o	o			
Authorization	RFC3261	o	－	－	c2	c2	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			（注 1）
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
Expires	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
In-Reply-To	RFC3261	o	o	o			（注 1）
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261		o	o	c3	c3	
Organization	RFC3261	o	o	o			（注 1）
P-Access-Network-Info	RFC3455	o	o	－		c4	（注 1）
P-Asserted-Identity	RFC3325		－	o / －	c5	c5	
P-Called-Party-ID	RFC3455	o	－	o / －	c6	c6	
P-Charging-Function-Addresses	RFC3455	o	－	－	c7	c7	
P-Charging-Vector	RFC3455	o	－	－	c7	c7	
P-Preferred-Identity	RFC3325		o / －	－	c8	c8	
P-Visited-Network-ID	RFC3455	o	－	－	c7	c7	
Priority	RFC3261	o	o	o			（注 1）
Privacy	RFC3323	o	o / －	o / －	c9	c9	
Proxy-Authorization	RFC3261	o	o	－	c10（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」の場合）	c11	
			－	－	c10（付表 1-11 項番 2 で UNI 条件が「HTTP Digest 認証を実施する」以外の場合）	c11	
Proxy-Require	RFC3261	o	o	－		c12	
Reason	RFC3326	o	－ / o	－ / o	（注 2）	（注 2）	（注 1）
Referred-By	RFC3892		o	o	c13（付表 1-2 項番 6～9）	c13（付表 1-2 項番 6～9）	（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Reply-To	RFC3261	o	o	o			（注 1）
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	c	c	c			
Route	RFC3261	c	m / c	－	c14（付表 1-24 項番 1 で UNI 条件が「利用する」の場合）	c15	
			－ / c	－	c14（付表 1-24 項番 1 で UNI 条件が「利用しない」の場合）	c15	
Security-Client	RFC3329	o	o	－	c16（付表 1-11 項番 1～2、付表 1-4 項番 3）	c17	

Security-Verify	RFC3329	o	o	－	c16（付表 1-11 項番 1～2、付表 1-4 項番 3）	c17	
Subject	RFC3261	o	o	o			（注 1）
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261		o	o			

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c3: メッセージボディに MIME Multipart が利用される場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-10 項番 3～4）

c4: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c5: 付属資料a.3の付表 a-1の 10.2.2.2.2 及び付属資料 bにより、P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の伝達を行う。（既存ダイアログ外の MESSAGE リクエストには設定可能であるが、既存ダイアログ内の MESSAGE リクエストには設定しない。）

c6: 付属資料 bにより、P-Called-Party-ID ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、着信対象の通知を行う。（既存ダイアログ外の MESSAGE リクエストには設定可能であるが、既存ダイアログ内の MESSAGE リクエストには設定しない。）

c7: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses、P-Visited-Network-ID ヘッダは利用しない。

c8: 付属資料a.3の付表 a-1の 10.2.2.2.3 及び付属資料 bにより、P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで EUF から SCF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、EUF が通知を要求する発信者情報の伝達を行う。（Initial INVITE には設定可能であるが、re-INVITE には設定しない。）

c9: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の通知/非通知情報を伝達する。（既存ダイアログ外の MESSAGE リクエストには設定可能であるが、既存ダイアログ内の MESSAGE リクエストには設定しない。）

c10: REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）

c11: 本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。

c12: 付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。

c13: REFER を利用した結果として Referred-By ヘッダが用いられることがある。（付表 1-2 項番 6～9） REFER が UNI で利用可能な場合は、当該ヘッダの情報は有効に扱われるかもしれない。また REFER を用いた結果として Referred-By ヘッダが利用されることについて保証されるものではない。

c14: pre-existing ルート機能が UNI で利用される場合に既存ダイアログ外の MESSAGE リクエストでは Route ヘッダの設定が必要。（付表 1-24 項番 1）

c15: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

c16: AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c17: 付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

注 2 Reason ヘッダは、RFC3326 により規定されるが、規定では既存ダイアログ内の全てのリクエスト、CANCEL、全てのレスポンスに適用可能となっている。したがって、既存ダイアログ内の MESSAGE リクエストでは利用可能であるが、既存ダイアログ外の MESSAGE リクエストでの利用はできない。

vi.6.2. MESSAGE レスポンスメッセージでサポートされるヘッダ

付表 6-10／JT-Q3402 Supported headers within the MESSAGE response

メッセージ種別： レスポンス

Method： MASSAGE

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	415	RFC3261	m*	m*	m*			
Accept-Encoding	415	RFC3261	m*	m*	m*			
Accept-Language	415	RFC3261	m*	m*	m*			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Authentication-Info	2xx	RFC3261	o	－	－	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			（注 1）
Contact	3xx	RFC3261	o	o	o			（注 2）
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			（注 1）
Content-Encoding		RFC3261	o	o	o			（注 1）
Content-Language		RFC3261	o	o	o			（注 1）
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			（注 1）
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
Expires		RFC3261	o	o	o			（注 1）
From		RFC3261	m	m	m			
MIME-Version	4xx-6xx	RFC3261		o	o	c2	c2	（注 1）
Organization		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455	o	o	－		c3	（注 1）
P-Charging-Function-Addresses		RFC3455	o	－	－	c4	c4	
P-Charging-Vector		RFC3455	o	－	－	c4	c4	
Privacy		RFC3323	o	－	－	c5	c5	
Proxy-Authenticate	401	RFC3261	o	－	－	c6	c7	
Proxy-Authenticate	407	RFC3261	m	－	m	c6		
Reason		RFC3326	o	o	o			（注 1）
Reply-To		RFC3261	o	o	o			（注 1）
Require		RFC3261	c	c	c			（注 1）
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
Security-Server	421 494	RFC3329	o	－	o	c8	c9（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	（注 3）	（注 3）	
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c10	c10	
WWW-Authenticate	407	RFC3261	o	－	－	c10	c10	

メッセージボディ	2xx-3xx	RFC3261	－	－	－			
メッセージボディ	4xx-6xx	RFC3261	o	o	o			（注 1）

c1: 対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。
c2: メッセージボディに MIME Multipart が利用される場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-10 項番 3～4）
c3: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c4: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c5: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c6: 本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、401/407 レスポンス自体を利用しない。
c7: 付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは 401 レスポンスでは利用しない。
c8: 付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。
c9: AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c10: 付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401/407 レスポンス自体を利用しない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。
注 2 本文 10.2.1.8.3 より、3xx レスポンスによるリダイレクション機能については、UNI で利用可能な場合に当該ヘッダの情報が有効に取り扱われる。（付表 1-12 項番 1～2）
注 3 RFC3903 の規定は"o"であるが、RFC3261 に準じ Unsupported は"m"とする。

vi.7. NOTIFY

本メッセージは、イベントサブスクリプション（イベントダイアログ）内で、イベントに関連する情報の通知に用いられる。NOTIFY は特定イベントサブスクリプションに関連付けて使用する。

イベントサブスクリプションは、SUBSCRIBE メソッド、REFER メソッド、その他インプリシットな利用法に基づいて確立される。

vi.7.1. NOTIFY リクエストメッセージでサポートされるヘッダ

付表 6-11／JT-Q3402 Supported headers within the NOTIFY request

メッセージ種別： リクエスト

Method： NOTIFY

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7項番 6）	c1（付表 1-7項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o			
Authorization	RFC3261	o	－	－	c2	c2	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261		－	－	（注 2）	（注 2）	
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
Event	RFC3265	m	m	m			
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
P-Access-Network-Info	RFC3455	o	o	－		c3	（注 1）
P-Asserted-Identity	RFC3325	o	－	－	c4	c4	
P-Charging-Function-Addresses	RFC3455	o	－	－	c5	c5	
P-Charging-Vector	RFC3455	o	－	－	c5	c5	
P-Preferred-Identity	RFC3325	o	－	－	c6	c6	
Privacy	RFC3323	o	－	－	c7	c7	
Proxy-Authorization	RFC3261	o	o	－	c8（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」の場合）	c9	
			－	－	c8（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」以外の場合）	c9	
Proxy-Require	RFC3261	o	o	－		c10	
Reason	RFC3326	o	o	o			（注 1）
Record-Route	RFC3261	o	o	o			（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	o	o	o			
Route	RFC3261	c	c	－		c11	
Security-Client	RFC3329	o	o	－	c12（付表 1-11 項番 1～2、付表 1-4 項番 3）	c13	
Security-Verify	RFC3329	o	o	－	c12（付表 1-11 項番 1～2、付表 1-4 項番 3）	c13	
Subscription-State	RFC3265	m	m	m			

Supported	RFC3261	o	o	o			
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
Warning	RFC3261	o	o	o			（注 1）
メッセージボディ	RFC3261		o	o	（注 3）	（注 3）	

c1:	端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7 項番 6）
c2:	付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。
c3:	付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c4:	付属資料a.3の付表 a-1の 10.2.2.2.2 により P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c5:	付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c6:	付属資料a.3の付表 a-1の 10.2.2.2.3 により P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外リクエストにのみ適用される。
c7:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。（NOTIFY はサブスクリプション（ダイアログ相当）内で用いられるため本ヘッダは適用されない。）
c8:	REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）
c9:	本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。
c10:	付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。
c11:	本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。
c12:	AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c13:	付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。
注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。
注 2	Call-Info は信号発信者の付加的な情報を示すものであるが、NOTIFY への適用は RFC 等に記載がなく、NOTIFY で本ヘッダを利用した場合のリアクションについても定義し難い。RFC3261 では Call-Info へのセキュリティリスクも指摘されているため、不用意な利用は避けるべきである。
注 3	追加情報が存在する場合利用される。フォーマットなどは、Content-Type に依存する。

vi.7.2.　NOTIFY レスポンスメッセージでサポートされるヘッダ

付表 6-12／JT-Q3402　Supported headers within the NOTIFY response

メッセージ種別：　レスポンス

Method：　NOTIFY

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	415	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	o	o	o			
Accept-Language	415	RFC3261	o	o	o			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o			
Allow-Events	489	RFC3265	m	m	m			
Authentication-Info	2xx	RFC3261	o	－	－	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261		－	－	（注 2）	（注 2）	
Contact	1xx	RFC3261	o	o	o			
Contact	2xx	RFC3261	o	o	o			
Contact	3xx	RFC3261	m	－	－	c2	c2	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			（注 1）
Content-Encoding		RFC3261	o	o	o			（注 1）
Content-Language		RFC3261	o	o	o			（注 1）
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			（注 1）
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455	o	o	－		c3	（注 1）
P-Asserted-Identity		RFC3325	o	－	－	c4	c4	
P-Charging-Function-Addresses		RFC3455	o	－	－	c5	c5	
P-Charging-Vector		RFC3455	o	－	－	c5	c5	
P-Preferred-Identity		RFC3325	o	－	－	c6	c6	
Privacy		RFC3323	o	－	－	c7	c7	
Proxy-Authenticate	407	RFC3261	m	－	m	c8		
Reason		RFC3326	o	o	o			（注 1）
Record-Route	2xx 401 484	RFC3261	o	o	o			（注 1）
Require		RFC3261	o	o	o			
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
RSeq	1xx	RFC3261	o	－	－	（注 3）	（注 3）	
Security-Server	421 494	RFC3329	o	－	－	c9	c10（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			

Unsupported	420	RFC3261	o	m	m	（注 4）	（注 4）	
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c11	c11	
メッセージボディ		RFC3261		o	o	（注 5）	（注 5）	（注 1）

c1: 対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。

c2: 付属資料a.3の付表 a-1の 10.2.1.8.3 により 3xx レスポンスを用いたリダイレクトは利用しない。

c3: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c4: 付属資料a.3の付表 a-1の 10.2.2.2.2 により P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c5: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。

c6: 付属資料a.3の付表 a-1の 10.2.2.2.3 により P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外リクエストにのみ適用される。

c7: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c8: 本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、407 レスポンス自体を利用しない。

c9: 付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。

c10: AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c11: 付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401 レスポンス自体を利用しない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

注 2 Call-Info は信号発信者の付加的な情報を示すものであるが、NOTIFY への適用は RFC 等に記載がなく、NOTIFY で本ヘッダを利用した場合のリアクションについても定義し難い。RFC3261 では Call-Info へのセキュリティリスクも指摘されているため、不用意な利用は避けるべきである。

注 3 NOTIFY で 100rel オプション（PRACK）を利用することはないとする。

注 4 RFC3265 の規定は"o"であるが、RFC3261 に準じ Unsupported は"m"とする。

注 5 通知情報が存在する場合利用される。フォーマットなどは、Content-Type に依存する。

vi.8. PRACK

本メッセージは、呼の確立において信頼性のある暫定応答メッセージ(100rel)を提供する場合に用いられる。

vi.8.1. PRACK リクエストメッセージでサポートされるヘッダ

付表 6-13／JT-Q3402 Supported headers within the PRACK request

メッセージ種別： リクエスト

Method： PRACK

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o	c2（付表 1-2 項番 10～15）	c2（付表 1-2 項番 10～15）	
Authorization	RFC3261	o	－	－	c3	c3	
Call-ID	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
P-Access-Network-Info	RFC3455	o	o	－		c4	（注 1）
P-Charging-Function-Addresses	RFC3455	o	－	－	c5	c5	
P-Charging-Vector	RFC3455	o	－	－	c5	c5	
P-Media-Authorization	RFC3313	o	－	o	c6	c7	
Privacy	RFC3323	o	－	－	c8	c8	
Proxy-Authorization	RFC3261	o	o	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」の場合）	c10	
			－	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」以外の場合）	c10	
Proxy-Require	RFC3261	o	o	－		c11	
RAck	RFC3262	m	m	m			
Reason	RFC3326	o	o	o			（注 1）
Record-Route	RFC3261	o	o	o			（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	c	c	c			
Route	RFC3261	c	c	－		c12	
Supported	RFC3261	o	o	o			（注 1）
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261		o	o	c13（付表 1-22 項番 2～3）	c13（付表 1-22 項番 2～3）	

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）

c3: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c4:	付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c5:	付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c6:	付属資料a.3の付表 a-1の 10.1 により EUF から SCF 方向では利用されない。
c7:	PRACK による SDP オファーが行われる場合に当該ヘッダの情報は有効に扱われる。（付表 1-22 項番 3）
c8:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c9:	REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）
c10:	本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。
c11:	付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。
c12:	本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。
c13:	本文 10.2.1.7.4.1 より、PRACK でのメッセージボディ部については、サポートされるべきとある。ボディ部での SDP 設定が UNI で利用可能な場合にメッセージボディの情報は有効に取り扱われる。（付表 1-22 項番 2～3）
注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.8.2. PRACK レスポンスメッセージでサポートされるヘッダ

付表 6-14／JT-Q3402 Supported headers within the PRACK response

メッセージ種別： レスポンス

Method： PRACK

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				SCF 送信	EUF 送信	EUF 送信	SCF 送信	
Accept	415	RFC3261	c	c	c			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o	c1（付表 1-2 項番 10～15）	c1（付表 1-2 項番 10～15）	
Authentication-Info	2xx	RFC3261	o	－	－	c2	c2	
Call-ID		RFC3261	m	m	m			
Contact	3xx	RFC3261	o	－	－	c3	c3	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
P-Access-Network-Info		RFC3455	o	o	－		c4	（注 1）
P-Charging-Function-Addresses		RFC3455	o	－	－	c5	c5	
P-Charging-Vector		RFC3455	o	－	－	c5	c5	
P-Media-Authorization	2xx	RFC3313	o	－	o	c6	c7	
Privacy		RFC3323	o	－	－	c8	c8	
Proxy-Authenticate	401	RFC3261	o	－	－	c9	c10	
Proxy-Authenticate	407	RFC3261	m	－	m	c9		
Reason		RFC3326	o	o	o			（注 1）
Record-Route	18x 2xx	RFC3261	o	o	o			（注 1）
Require		RFC3261	c	c	c			
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
Server		RFC3261	o	o	o			（注 1）
Supported	2xx	RFC3261	o	o	o			（注 1）
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c11	c11	
メッセージボディ		RFC3261		o	o	c12	c12	

c1: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）

c2: 対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。

c3:	付属資料a.3の付表 a-1の 10.2.1.8.3 により 3xx レスポンスを用いたリダイレクトは利用しない。
c4:	付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c5:	付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c6:	付属資料a.3の付表 a-1の 10.1 により EUF から SCF 方向では利用されない。
c7:	PRACK による SDP オファーが行われる場合に当該ヘッダの情報は有効に扱われる。（付表 1-22 項番 3）
c8:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c9:	本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、401/407 レスポンス自体を利用しない。
c10:	付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは 401 レスポンスでは利用しない。
c11:	付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401 レスポンス自体を利用しない。
c12:	本文 10.2.1.7.4.1 より、PRACK でのメッセージボディ部については、サポートされるべきとある。ボディ部での SDP 設定が UNI で利用可能な場合にメッセージボディの情報は有効に取り扱われる。（付表 1-22 項番 2～3）
注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.9. PUBLISH

本メッセージは、プレゼンス情報などの購読される情報を、新規に発行または更新する場合に用いられる。

vi.9.1. PUBLISH リクエストメッセージでサポートされるヘッダ

付表 6-15／JT-Q3402 Supported headers within the PUBLISH request

メッセージ種別： リクエスト

Method： PUBLISH

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o	c2（付表 1-2 項番 10～15）	c2（付表 1-2 項番 10～15）	
Authorization	RFC3261	o	－	－	c3	c3	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			（注 1）
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
Event	RFC3265	m	m	m			
Expires	RFC3261	o	o	o			
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Organization	RFC3261	o	o	o			（注 1）
P-Access-Network-Info	RFC3455		o	－		c4	（注 1）
P-Asserted-Identity	RFC3325		－	o / －	c5	c5	
P-Called-Party-ID	RFC3455		－	o / －	c6	c6	
P-Charging-Function-Addresses	RFC3455		－	－	c7	c7	
P-Charging-Vector	RFC3455		－	－	c7	c7	
P-Preferred-Identity	RFC3325		o / －	－	c8	c8	
P-Visited-Network-ID	RFC3455		－	－	c7	c7	
Priority	RFC3261	o	o	o			（注 1）
Privacy	RFC3323		o / －	o / －	c9	c9	
Proxy-Authorization	RFC3261	o	o	－	c10（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」の場合）	c11	
			－	－	c10（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」以外の場合）	c11	
Proxy-Require	RFC3261	o	o	－		c12	
Reason	RFC3326	o	－ / o	－ / o	（注 2）	（注 2）	（注 1）
Referred-By	RFC3892		o	o	c13（付表 1-2 項番 6～9）	c13（付表 1-2 項番 6～9）	（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	o	o	o			
Route	RFC3261	c	m / c	－	c14（付表 1-24 項番 1 で UNI 条件が「利用する」の場合）	c15	
			－ / c	－	c14（付表 1-24 項番 1 で UNI 条件が「利用しない」の場合）	c15	

Security-Client	RFC3329		o	―	c16（付表 1-11 項番 1～2、付表 1-4 項番 3）	c17	
Security-Verify	RFC3329		o	―	c16（付表 1-11 項番 1～2、付表 1-4 項番 3）	c17	
SIP-If-Match	RFC3261	o	o	o			
Subject	RFC3261	o	o	o			（注 1）
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261		o	o			

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）

c3: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c4: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c5: 付属資料a.3の付表 a-1の 10.2.2.2.2 及び付属資料 bにより、P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の伝達を行う。（INVITE ダイアログ外の PUBLISH リクエストには設定可能であるが、INVITE ダイアログ内の PUBLISH リクエストには設定しない。）

c6: 付属資料 bにより、P-Called-Party-ID ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、着信対象の通知を行う。（INVITE ダイアログ外の PUBLISH リクエストには設定可能であるが、INVITE ダイアログ内の PUBLISH リクエストには設定しない。）

c7: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses、P-Visited-Network-ID ヘッダは利用しない。

c8: 付属資料a.3の付表 a-1の 10.2.2.2.3 及び付属資料 bにより、P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで EUF から SCF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、EUF が通知を要求する発信者情報の伝達を行う。（INVITE ダイアログ外の PUBLISH リクエストには設定可能であるが、INVITE ダイアログ内の PUBLISH リクエストには設定しない。）

c9: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の通知/非通知情報を伝達する。（INVITE ダイアログ外の PUBLISH リクエストには設定可能であるが、INVITE ダイアログ内の PUBLISH リクエストには設定しない。）

c10: REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）

c11: 本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。

c12: 付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。

c13: REFER を利用した結果として Referred-By ヘッダが用いられることがある。（付表 1-2 項番 6～9） REFER が UNI で利用可能な場合は、当該ヘッダの情報は有効に扱われるかもしれない。また REFER を用いた結果として Referred-By ヘッダが利用されることについて保証されるものではない。

c14: pre-existing ルート機能が UNI で利用される場合に INVITE ダイアログ外の PUBLISH リクエストでは Route ヘッダの設定が必要。（付表 1-24 項番 1）

c15: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

c16: AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c17: 付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

注 2 Reason ヘッダは、RFC3326 により規定されるが、規定では既存ダイアログ内の全てのリクエスト、CANCEL、全てのレスポンスに適用可能となっている。したがって、INVITE ダイアログ内の PUBLISH リクエストでは利用可能であるが、INVITE ダイアログ外の PUBLISH リクエストでの利用はできない。

vi.9.2.　PUBLISH レスポンスメッセージでサポートされるヘッダ

付表 6-16／JT-Q3402　Supported headers within the PUBLISH response

メッセージ種別：　レスポンス

Method：　PUBLISH

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	415	RFC3261	m*	m*	m*			
Accept-Encoding	415	RFC3261	m*	m*	m*			
Accept-Language	415	RFC3261	m*	m*	m*			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Allow-Events	489	RFC3261	m	m	m			
Authentication-Info	2xx	RFC3261	o	－	－	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			（注 1）
Contact	3xx	RFC3261	o	o	o			（注 2）
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			（注 1）
Content-Encoding		RFC3261	o	o	o			（注 1）
Content-Language		RFC3261	o	o	o			（注 1）
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			（注 1）
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
Expires	2xx	RFC3261	m	m	m			
Expires	他	RFC3261	o	o	o			
From		RFC3261	m	m	m			
Min-Expires	423	RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			（注 1）
Organization		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455		o	－		c2	（注 1）
P-Charging-Function-Addresses		RFC3455		－	－	c3	c3	
P-Charging-Vector		RFC3455		－	－	c3	c3	
Privacy		RFC3323		－	－	c4	c4	
Proxy-Authenticate	401	RFC3261	o	－	－	c5	c6	
Proxy-Authenticate	407	RFC3261	m	－	m	c5		
Reason		RFC3326	o	o	o			（注 1）
Require		RFC3261	o	o	o			
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
Security-Server	421 494	RFC3329		－	o	c7	c8（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
SIP-ETag	2xx	RFC3261	m	m	m			
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	（注 3）		
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）

WWW-Authenticate	401	RFC3261	m	－	－	c9	c9	
WWW-Authenticate	407	RFC3261	o	－	－	c9	c9	
メッセージボディ		RFC3261		o	o			（注 1）

c1:	対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。
c2:	付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c3:	付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c4:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c5:	本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、401/407 レスポンス自体を利用しない。
c6:	付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは 401 レスポンスでは利用しない。
c7:	付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。
c8:	AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c9:	付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401/407 レスポンス自体を利用しない。

注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。
注 2	本文 10.2.1.8.3 より、3xx レスポンスによるリダイレクション機能については、UNI で利用可能な場合に当該ヘッダの情報が有効に取り扱われる。（付表 1-12 項番 1～2）
注 3	RFC3903 の規定は"o"であるが、RFC3261 に準じ Unsupported は"m"とする。

vi.10. REFER

本メッセージは、既存ダイアログ内もしくは既存ダイアログ外で用いられ、本メッセージの受信者に対して、Refer-To で指定する発信等の行動を行うよう依頼するために用いられる。

vi.10.1. REFER リクエストメッセージでサポートされるヘッダ

付表 6-17／JT-Q3402　Supported headers within the REFER request

メッセージ種別：　リクエスト

Method：　REFER

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265		o	o	（注 2）	（注 2）	
Authorization	RFC3261	o	－	－	c2	c2	
Call-ID	RFC3261	m	m	m			
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	o	t	t	（注 3）		
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
Expires	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Organization	RFC3261	o	o	o			（注 1）
P-Access-Network-Info	RFC3455	o	o	－		c3	（注 1）
P-Asserted-Identity	RFC3325	o	－	o / －	c4	c4	
P-Called-Party-ID	RFC3455	o	－	o / －	c5	c5	
P-Charging-Function-Addresses	RFC3455	o	－	－	c6	c6	
P-Charging-Vector	RFC3455	o	－	－	c6	c6	
P-Preferred-Identity	RFC3325	o	o / －	－	c7	c7	
P-Visited-Network-ID	RFC3455	o	－	－	c6	c6	
Privacy	RFC3323	o	o / －	o / －	c8	c8	
Proxy-Authorization	RFC3261	o	o	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」の場合）	c10	
			－	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」以外の場合）	c10	
Proxy-Require	RFC3261	o	o	－		c11	
Reason	RFC3326	o	－ / o	－ / o	（注 4）	（注 4）	（注 1）
Record-Route	RFC3261	o	o	o			
Refer-To	RFC3515	m	m	m			
Referred-By	RFC3892		o	o	c12（付表 1-2 項番 6～9）	c12（付表 1-2 項番 6～9）	
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	c	c	c			
Route	RFC3261	c	m / c	－	c13（付表 1-24 項番 1 で UNI 条件が「利用する」の場合）	c14	
			－ / c	－	c13（付表 1-24 項番 1 で UNI 条件が「利用しない」の場合）	c14	

Security-Client	RFC3329		o	－	c15（付表 1-11 項番 1～2、付表 1-4 項番 3）	c16	
Security-Verify	RFC3329		o	－	c15（付表 1-11 項番 1～2、付表 1-4 項番 3）	c16	
Supported	RFC3261	o	o	o			
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261		o	o	（注 5）	（注 5）	

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c3: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c4: 付属資料a.3の付表 a-1の 10.2.2.2.2 及び付属資料 bにより、P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の伝達を行う。（既存ダイアログ外の REFER では設定可能であるが、既存ダイアログ内の REFER では設定しない。）

c5: 付属資料 bにより、P-Called-Party-ID ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、着信対象の通知を行う。（既存ダイアログ外の REFER では設定可能であるが、既存ダイアログ内の REFER には設定しない。）

c6: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses、P-Visited-Network-ID ヘッダは利用しない。

c7: 付属資料a.3の付表 a-1の 10.2.2.2.3 及び付属資料 bにより、P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで EUF から SCF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、EUF が通知を要求する発信者情報の伝達を行う。（既存ダイアログ外の REFER では設定可能であるが、既存ダイアログ内の REFER では設定しない。）

c8: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の通知/非通知情報を伝達する。（既存ダイアログ外の REFER リクエストでは設定可能であるが、既存ダイアログ内での REFER リクエストでは設定しない。）

c9: REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）

c10: 本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。

c11: 付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。

c12: REFER を利用した結果として Referred-By ヘッダが用いられることがある。（付表 1-2 項番 6～9） REFER が UNI で利用可能な場合は、当該ヘッダの情報は有効に扱われるかもしれない。また REFER を用いた結果として Referred-By ヘッダが利用されることについて保証されるものではない。

c13: pre-existing ルート機能が UNI で利用される場合に既存ダイアログ外の REFER リクエストでは Route ヘッダの設定が必要。（付表 1-24 項番 1）

c14: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

c15: AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c16: 付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

注 2 REFER を送信した UA は、"refer"イベントオプションをサポートしていると考えられ、当該情報が設定される可能性があるので、RFC 上の規約は無いが、オプションと表記。

注 3 RFC3515 の規定は"o"であるが、RFC3261 に準じ Content-Length は"t"とする。

注 4 Reason ヘッダは、RFC3326 により規定されるが、規定では既存ダイアログ内の全てのリクエスト、CANCEL、全てのレスポンスに適用可能となっている。したがって、既存ダイアログ内の REFER では利用可能であるが、既存ダイアログ外の REFER での利用はできない。

注 5 通知情報が存在する場合利用される。フォーマットなどは、Content-Type に依存する。

vi.10.2. REFER レスポンスメッセージでサポートされるヘッダ

付表 6-18／JT-Q3402　Supported headers within the REFER response

メッセージ種別：　レスポンス

Method：　REFER

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	415	RFC3261	c	c	c			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Allow-Events		RFC3265		o	o	（注 2）	（注 2）	
Authentication-Info	2xx	RFC3261	o	－	－	c1	c1	
Call-ID		RFC3261	m	m	m			
Contact	2xx	RFC3261	m	m	m			
Contact	3xx-6xx	RFC3261	o	o	o			（注 3）
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	o	t	t	（注 4）	（注 4）	
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	3xx-6xx	RFC3261	o	o	o			（注 1）
Expires		RFC3261	o	o	o			
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
Organization		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455	o	o	－		c2	（注 1）
P-Asserted-Identity		RFC3325	o	－	－	c3	c3	
P-Charging-Function-Addresses		RFC3455	o	－	－	c4	c4	
P-Charging-Vector		RFC3455	o	－	－	c4	c4	
P-Preferred-Identity		RFC3325	o	－	－	c5	c5	
Privacy		RFC3323	o	－	－	c6	c6	
Proxy-Authenticate	401	RFC3261	o	－	－	c7	c8	
Proxy-Authenticate	407	RFC3261	m	－	m	c7		
Reason		RFC3326	o	o	o			（注 1）
Record-Route	18x 2xx	RFC3261	o	o	o			
Require		RFC3261	c	c	c			
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
Security-Server	421 494	RFC3329		－	o	c9	c10（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	（注 5）	（注 5）	
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			

Warning		RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c11	c11	
WWW-Authenticate	407	RFC3261	o	－	－	c11	c11	
メッセージボディ		RFC3261		o	o	（注 6）	（注 6）	

c1:	対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。
c2:	付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c3:	付属資料a.3の付表 a-1の 10.2.2.2.2 により P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c4:	付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c5:	付属資料a.3の付表 a-1の 10.2.2.2.3 により P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外リクエストにのみ適用される。
c6:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c7:	本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、401/407 レスポンス自体を利用しない。
c8:	付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは 401 レスポンスでは利用しない。
c9:	付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。
c10:	AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c11:	付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401/407 レスポンス自体を利用しない。

注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。
注 2	REFER を受信した UA は、"refer"イベントオプションをサポートしていると考えられ、当該情報が設定される可能性があるので、RFC 上の規約は無いが、オプションと表記。
注 3	本文 10.2.1.8.3 より、3xx レスポンスによるリダイレクション機能については、UNI で利用可能な場合に当該ヘッダの情報が有効に取り扱われる。（付表 1-12 項番 1～2）
注 4	RFC3515 の規定は"o"であるが、RFC3261 に準じ Content-Length は"t"とする。
注 5	RFC3515 の規定は"o"であるが、RFC3261 に準じ Unsupported は"m"とする。
注 6	通知情報が存在する場合利用される。フォーマットなどは、Content-Type に依存する。

vi.11. REGISTER

本メッセージは、端末の登録・削除または登録の更新を行うために用いられる。

vi.11.1. REGISTER リクエストメッセージでサポートされるヘッダ

付表 6-19／JT-Q3402　Supported headers within the REGISTER request

メッセージ種別：　リクエスト

Method：　REGISTER

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o				
Accept-Encoding	RFC3261	o	o				
Accept-Language	RFC3261	o	o				
Allow	RFC3261	o	o				
Allow-Events	RFC3265	o	o		c1		
Authorization	RFC3261	o	o		c2（付表 1-11 項番 1 で UNI 条件が「実施しない」以外の場合）		
			―		c2（付表 1-11 項番 1 で UNI 条件が「実施しない」の場合）		
Call-ID	RFC3261	m	m				
Call-Info	RFC3261	o	o				（注 1）
Contact	RFC3261	o	o				
Content-Disposition	RFC3261	o	o				（注 1）
Content-Encoding	RFC3261	o	o				（注 1）
Content-Language	RFC3261	o	o				（注 1）
Content-Length	RFC3261	t	t				
Content-Type	RFC3261	*	*				（注 1）
CSeq	RFC3261	m	m				
Date	RFC3261	o	o				（注 1）
Expires	RFC3261	o	o				
From	RFC3261	m	m				
Max-Forwards	RFC3261	m	m				
MIME-Version	RFC3261	o	o				（注 1）
Organization	RFC3261	o	o				（注 1）
P-Access-Network-Info	RFC3455	o	o				（注 1）
P-Charging-Function-Addresses	RFC3455	o	―		c3		
P-Charging-Vector	RFC3455	o	―		c3		
P-Visited-Network-ID	RFC3455	o	―		c3		
Path	RFC3327	o	―		c4		
Privacy	RFC3323	o	―		c5		
Proxy-Authorization	RFC3261	o	―		c6		
Proxy-Require	RFC3261	o	o				
Referred-By	RFC3892	o	o		c7（付表 1-2 項番 6～9）		（注 1）
Request-Disposition	RFC3841	o	o		c8（付表 1-7 項番 6）		
Require	RFC3261	c	c				
Route	RFC3261	c	―		c9		
Security-Client	RFC3329	o	o		c10（付表 1-11 項番 1～2、付表 1-4 項番 3）		
Security-Verify	RFC3329	o	o		c11（付表 1-11 項番 1～2、付表 1-4 項番 3）		
Supported	RFC3261	o	o		c12		
Timestamp	RFC3261	o	o				（注 1）
To	RFC3261	m	m				
User-Agent	RFC3261	o	o				（注 1）
Via	RFC3261	m	m				
メッセージボディ	RFC3261	o	o				（注 1）

c1:	端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）
c2:	REGISTER リクエストに対して HTTP Digest 認証または AKA 認証が行われる場合に利用される。（付表 1-11 項番 1）
c3:	付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses、P-Visited-Network-ID ヘッダは利用しない。
c4:	付属資料a.3の付表 a-1の 10.1 により Path ヘッダは、EUF から SCF 方向のリクエストには適用されない。
c5:	付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c6:	付属資料a.3の付表 a-1の 10.2.1.20.28 により Proxy-Authorization ヘッダは、REGISTER リクエストには適用されない。
c7:	REFER を利用した結果として Referred-By ヘッダが用いられることがある。（付表 1-2 項番 6～9） REFER が UNI で利用可能な場合は、当該ヘッダの情報は有効に扱われるかもしれない。また REFER を用いた結果として Referred-By ヘッダが利用されることについて保証されるものではない。
c8:	端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）
c9:	付属資料a.3の付表 a-1の 10.2.1.20.34 及び付属資料c.3.2により、REGISTER リクエストに pre-existing ルートは提供されない。
c10:	付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c11:	REGISTER 経路記録機能（path）を利用する場合は"path"を記載する必要がある。（付表 1-24 項番 1）
注 1	EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.11.2. REGISTER レスポンスメッセージでサポートされるヘッダ

付表 6-20／JT-Q3402　Supported headers within the REGISTER response

メッセージ種別：　レスポンス

Method：　REGISTER

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	2xx	RFC3261	o		o			
Accept	415	RFC3261	c		c			
Accept-Encoding	2xx	RFC3261	o		o			
Accept-Encoding	415	RFC3261	c		c			
Accept-Language	2xx	RFC3261	o		o			
Accept-Language	415	RFC3261	c		c			
Allow	2xx	RFC3261	o		o			
Allow	405	RFC3261	m		m			
Allow	他	RFC3261	o		o			
Allow-Events	2xx	RFC3265	o		o		c1（付表 1-2 項番 10～15）	
Authentication-Info	2xx	RFC3261	o		o			
Call-ID		RFC3261	m		m			
Call-Info		RFC3261	o		o			
Contact	2xx	RFC3261	o		o			
Contact	3xx	RFC3261	o		－		c2	
Contact	485	RFC3261	o		o			
Content-Disposition		RFC3261	o		o			
Content-Encoding		RFC3261	o		o			
Content-Language		RFC3261	o		o			
Content-Length		RFC3261	t		t			
Content-Type		RFC3261	*		*			
CSeq		RFC3261	m		m			
Date		RFC3261	o		o			
Error-Info	300-699	RFC3261	o		o			
Expires		RFC3261	o		o			
From		RFC3261	m		m			
Min-Expires	423	RFC3261	m		m			
MIME-Version		RFC3261	o		o			
Organization		RFC3261	o		o			
P-Access-Network-Info		RFC3455	o		－		c3	
P-Associated-URI	2xx	RFC3455	o		o		c4（付表 1-24 項番 3 の UNI 条件が「通知する場合がある」の場合）	
					－		c4（付表 1-24 項番 3 の UNI 条件が「通知しない」の場合）	
P-Charging-Function-Addresses		RFC3455	o		－		c5	
P-Charging-Vector		RFC3455	o		－		c5	
Path	2xx	RFC3327	o		o			
Privacy		RFC3323	o		－		c6	
Proxy-Authenticate	401	RFC3261	o		－		c7	
Proxy-Authenticate	407	RFC3261	m		－		c7	
Reason		RFC3326	o		o			
Require		RFC3261	c		c			
Retry-After	404 413 480 486	RFC3261	o		o			
Retry-After	500 503	RFC3261	o		o			
Retry-After	600 603	RFC3261	o		o			

Security-Server	421 494	RFC3329	o		o		c8（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Service-Route	2xx	RFC3608	o		o		c9（付表 1-24 項番 1 の UNI 条件が「提供する」の場合）	
					－		c9（付表 1-24 項番 1 の UNI 条件が「提供しない」の場合）	
Server		RFC3261	o		o			
Supported	2xx	RFC3261	o		o			
Timestamp		RFC3261	o		o			
To		RFC3261	m		m			
Unsupported	420	RFC3261	m		m			
User-Agent		RFC3261	o		o			
Via		RFC3261	m		m			
Warning		RFC3261	o		o			
WWW-Authenticate	401	RFC3261	m		m			
WWW-Authenticate	407	RFC3261	o		o			
メッセージボディ		RFC3261	o		o			

c1: SUBSCRIBE/NOTIFY が UNI で利用可能な場合に当該ヘッダの情報は有効に取り扱われる。（付表 1-2 項番 10～15）
c2: 付属資料a.3の付表 a-1の 10.2.1.8.3 により 3xx レスポンスを用いたリダイレクトは利用しない。
c3: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。
c4: P-Associated-URI ヘッダを用いた網付与ユーザ ID の通知が行われる場合に利用される。（付表 1-24 項番 3）
c5: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。
c6: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。
c7: 付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは REGISTER リクエストでは利用しない。
c8: 付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは AKA 認証または呼制御信号の TLS 接続が利用される場合に適用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）
c9: pre-existing ルート機能が UNI で利用される場合に設定が必要。（付表 1-24 項番 1）

vi.12. SUBSCRIBE

本メッセージは、イベントサブスクリプション（イベントダイアログ）を形成するために用いられる。

vi.12.1. SUBSCRIBE リクエストメッセージでサポートされるヘッダ

付表 6-21／JT-Q3402　Supported headers within the SUBSCRIBE request

メッセージ種別：　リクエスト

Method：　SUBSCRIBE

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o			
Authorization	RFC3261	o	－	－	c2	c2	
Call-ID	RFC3261	m	m	m			
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
Event	RFC3265	m	m	m			
Expires	RFC3261	o	o	o			
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Organization	RFC3261	o	o	o			（注 1）
P-Access-Network-Info	RFC3455	o	o	－		c3	（注 1）
P-Asserted-Identity	RFC3325	o	－	o / －	c4	c4	
P-Called-Party-ID	RFC3455	o	－	o / －	c5	c5	
P-Charging-Function-Addresses	RFC3455	o	－	－	c6	c6	
P-Charging-Vector	RFC3455	o	－	－	c6	c6	
P-Preferred-Identity	RFC3325	o	o / －	－	c7	c7	
P-Visited-Network-ID	RFC3455	o	－	－	c6	c6	
Priority	RFC3261	o	o	o			（注 1）
Privacy	RFC3323	o	o / －	o / －	c8	c8	
Proxy-Authorization	RFC3261	o	o	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」の場合）	c10	
			－	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」以外の場合）	c10	
Proxy-Require	RFC3261	o	o	－		c11	
Reason	RFC3326	o	－ / o	－ / o	（注 2）	（注 2）	（注 1）
Record-Route	RFC3261	o	o	o			
Referred-By	RFC3892	o	o	o	c12（付表 1-2 項番 6～9）	c12（付表 1-2 項番 6～9）	
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	o	o	o			
Route	RFC3261	c	m / c	－	c13（付表 1-24 項番 1 で UNI 条件が「利用する」の場合）	c14	
			－ / c	－	c13（付表 1-24 項番 1 で UNI 条件が「利用しない」の場合）	c14	

Security-Client	RFC3329	o	o	－	c15（付表 1-11 項番 1～2、付表 1-4 項番 3）	c16	
Security-Verify	RFC3329	o	o	－	c15（付表 1-11 項番 1～2、付表 1-4 項番 3）	c16	
Supported	RFC3261	o	o	o			
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261		o	o	（注 3）	（注 3）	

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c3: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c4: 付属資料a.3の付表 a-1の 10.2.2.2.2 及び付属資料 bにより、P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の伝達を行う。（Initial SUBSCRIBE には設定可能であるが、re-SUBSCRIBE には設定しない。）

c5: 付属資料 bにより、P-Called-Party-ID ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで SCF から EUF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、着信対象の通知を行う。（INVITE ダイアログ外の Initial SUBSCRIBE には設定可能であるが、INVITE ダイアログ内の SUBSCRIBE リクエストまたは既存サブスクリプション内の re-SUBSCRIBE には設定しない。）

c6: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses、P-Visited-Network-ID ヘッダは利用しない。

c7: 付属資料a.3の付表 a-1の 10.2.2.2.3 及び付属資料 bにより、P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストで EUF から SCF 方向の信号にのみ設定可能（既存ダイアログ内では用いない）であり、EUF が通知を要求する発信者情報の伝達を行う。（Initial SUBSCRIBE には設定可能であるが、re-SUBSCRIBE には設定しない。）

c8: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ設定可能（既存ダイアログ内では用いない）であり、発信者情報の通知/非通知情報を伝達する。（INVITE ダイアログ外の Initial SUBSCRIBE には設定可能であるが、INVITE ダイアログ内の SUBSCRIBE リクエストまたは既存サブスクリプション内の re-SUBSCRIBE には設定しない。）

c9: REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）

c10: 本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。

c11: 付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。

c12: REFER を利用した結果として Referred-By ヘッダが用いられることがある。（付表 1-2 項番 6～9） REFER が UNI で利用可能な場合は、当該ヘッダの情報は有効に扱われるかもしれない。また REFER を用いた結果として Referred-By ヘッダが利用されることについて保証されるものではない。

c13: pre-existing ルート機能が UNI で利用される場合に INVITE ダイアログ外の Initial SUBSCRIBE では Route ヘッダの設定が必要。（付表 1-24 項番 1）

c14: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

c15: AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c16: 付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

注 2 Reason ヘッダは、RFC3326 により規定されるが、規定では既存ダイアログ内の全てのリクエスト、CANCEL、全てのレスポンスに適用可能となっている。したがって、INVITE ダイアログ内の SUBSCRIBE リクエストまたは既存サブスクリプション内の re-SUBSCRIBE では利用可能であるが、INVITE ダイアログ外の Initial SUBSCRIBE での利用はできない。

注 3 通知情報が存在する場合利用される。フォーマットなどは、Content-Type に依存する。

vi.12.2. SUBSCRIBE レスポンスメッセージでサポートされるヘッダ

付表 6-22／JT-Q3402　Supported headers within the SUBSCRIBE response

メッセージ種別：　レスポンス

Method：　SUBSCRIBE

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	415	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	o	o	o			
Accept-Language	415	RFC3261	o	o	o			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Allow-Events	489	RFC3265	m	m	m			
Authentication-Info	2xx	RFC3261	o	－	－	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261		－	－	（注 2）	（注 2）	
Contact	1xx	RFC3261	o	o	o			
Contact	2xx	RFC3261	m	m	m			
Contact	3xx	RFC3261	m	m	m			（注 3）
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
Expires	2xx	RFC3261	m	m	m			
From		RFC3261	m	m	m			
Min-Expires	423	RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
Organization		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455	o	o	－		c3	（注 1）
P-Asserted-Identity		RFC3325	o	－	－	c4	c4	
P-Charging-Function-Addresses		RFC3455	o	－	－	c5	c5	
P-Charging-Vector		RFC3455	o	－	－	c5	c5	
P-Preferred-Identity		RFC3325	o	－	－	c6	c6	
Privacy		RFC3323	o	－	－	c2	c2	
Proxy-Authenticate	407	RFC3261	m	－	m	c7		
Reason		RFC3326	o	o	o			（注 1）
Record-Route	2xx 401 484	RFC3261	o	o	o			
Require		RFC3261	o	o	o			
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
RSeq	1xx	RFC3262	o	－	－	（注 4）	（注 4）	
Security-Server	421 494	RFC3329	o	－	－	c8	c9（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			（注 1）

To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	（注 5）	（注 5）	
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c10	c10	
メッセージボディ		RFC3261		o	o	（注 6）	（注 6）	

c1: 対応するリクエストで Authorization ヘッダが利用されないため、Authentication-Info ヘッダによる認証情報の更新も行われない。

c2: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c3: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c4: 付属資料a.3の付表 a-1の 10.2.2.2.2 により P-Asserted-Identity ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c5: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。

c6: 付属資料a.3の付表 a-1の 10.2.2.2.3 により P-Preferred-Identity ヘッダは、REGISTER を除く既存ダイアログ外リクエストにのみ適用される。

c7: 本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、407 レスポンス自体を利用しない。

c8: 付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。

c9: AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c10: 付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401 レスポンス自体を利用しない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

注 2 Call-Info は信号発信者の付加的な情報を示すものであるが、SUBSCRIBE への適用は RFC 等に記載がなく、SUBSCRIBE で本ヘッダを利用した場合のリアクションについても定義し難い。RFC3261 では Call-Info へのセキュリティリスクも指摘されているため、不用意な利用は避けるべきである。

注 3 本文 10.2.1.8.3 より、3xx レスポンスによるリダイレクション機能については、UNI で利用可能な場合に当該ヘッダの情報が有効に取り扱われる。（付表 1-12 項番 1～2）

注 4 SUBSCRIBE で 100rel オプション（PRACK）を利用することはないとする。

注 5 RFC3265 の規定は"o"であるが、RFC3261 に準じ Unsupported は"m"とする。

注 6 通知情報が存在する場合利用される。フォーマットなどは、Content-Type に依存する。

vi.13. UPDATE

本メッセージは、呼のリフレッシュ（Session-Timer）、および通話中にメディアストリームの設定情報の変更に用いられる。

vi.13.1. UPDATE リクエストメッセージでサポートされるヘッダ

付表 6-23／JT-Q3402　Supported headers within the UPDATE request

メッセージ種別：　リクエスト

Method：　UPDATE

情報要素	参照	RFC	本書の規定		適用条件		備考
			EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Authorization	RFC3261	o	－	－	c2	c2	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			（注 1）
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			（注 1）
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Min-SE	RFC4028	o	o	o	c3	c3	
Organization	RFC3261	o	o	o			（注 1）
P-Access-Network-Info	RFC3455	o	o	－		c4	（注 1）
P-Charging-Function-Addresses	RFC3455	o	－	－	c5	c5	
P-Charging-Vector	RFC3455	o	－	－	c5	c5	
P-Media-Authorization	RFC3313	o	－	o	c6	c7	
Privacy	RFC3323	o	－	－	c8	c8	
Proxy-Authorization	RFC3261	o	o	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」の場合）	c10	
			－	－	c9（付表 1-11 項番 2 が「HTTP Digest 認証を実施する」以外の場合）	c10	
Proxy-Require	RFC3261	o	o	－		c11	
Reason	RFC3326	o	o	o			（注 1）
Record-Route	RFC3261	o	o	o			（注 1）
Reject-Contact	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Request-Disposition	RFC3841	o	o	o	c1（付表 1-7 項番 6）	c1（付表 1-7 項番 6）	
Require	RFC3261	c	c	c	c12	c12	
Route	RFC3261	c	c	－		c13	
Security-Client	RFC3329	o	o	－	c14（付表 1-11 項番 1～2、付表 1-4 項番 3）	c15	
Security-Verify	RFC3329	o	o	－	c14（付表 1-11 項番 1～2、付表 1-4 項番 3）	c15	
Session-Expires	RFC4028	o	m	m	c3（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	c3（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	

			o	o	c3（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	c3（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	
Supported	RFC3261	o	o	o	c12	c12	
Timestamp	RFC3261	o	o	o			（注 1）
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			（注 1）
Via	RFC3261	m	m	m			
メッセージボディ	RFC3261	o	o	o			

c1: 端末能力通知機能 Caller Preferences（pref タグ）が UNI で利用可能な場合に当該ヘッダの情報は有効に扱われる。（付表 1-7項番 6）

c2: 付属資料a.3の付表 a-1の 10.2.1.20.7 により、Authorization ヘッダは SCF が EUF からの REGISTER リクエストを認証する際に限り利用される。

c3: 本文 10.2.2.2.1 および 10.2.2.2.7 より、当該のヘッダを規定どおりに利用しなければならない。Session-Timer を利用する場合は、少なくとも Session-Expires ヘッダへの値（delta-seconds）の設定が必要になる。

c4: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c5: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。

c6: 付属資料a.3の付表 a-1の 10.1 により EUF から SCF 方向では利用されない。

c7: UPDATE による SDP オファーが行われる場合に当該ヘッダの情報は有効に扱われる。（付表 1-23 項番 6）

c8: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c9: REGISTER 以外の既存ダイアログ外リクエストに対して HTTP Digest 認証が実施される場合に利用される。（付表 1-11 項番 2）

c10: 本文 10.2.1.20.28 節より、SCF から EUF 方向への Proxy-Authorization ヘッダは利用されない。

c11: 付属資料a.3の付表 a-1の 10.2.1.20.29 により、SCF から EUF 方向への Proxy-Require ヘッダは利用されない。

c12: 本文 10.2.1.20.32 および 10.2.1.20.37 より、"timer"については、Require ヘッダ及び Supported ヘッダに文脈上で設定する必要がある。（"timer"はその文脈上、UPDATE リクエストの Supported ヘッダに設定されるべきである。）

c13: 本文 10.2.1.20.34 節より、SCF から EUF 方向への Route ヘッダは利用されない。

c14: AKA 認証または呼制御信号の TLS 接続が利用される場合に有効に扱われる。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c15: 付属資料a.3の付表 a-1の 10.1 により Security-Client、Security-Verify ヘッダは SCF から EUF 方向のリクエストには適用されない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

vi.13.2. UPDATE レスポンスメッセージでサポートされるヘッダ

付表 6-24／JT-Q3402　Supported headers within the UPDATE response

メッセージ種別：　レスポンス

Method：　UPDATE

情報要素	適用	参照	RFC	本書の規定		適用条件		備考
				EUF 送信	SCF 送信	EUF 送信	SCF 送信	
Accept	2xx	RFC3261	o	o	o			
Accept	415	RFC3261	c	c	c			
Accept-Encoding	2xx	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	2xx	RFC3261	o	o	o			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	他	RFC3261	o	o	o			
Authentication-Info	2xx	RFC3261	o	－	－	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			（注 1）
Contact	1xx	RFC3261	o	o	o			
Contact	2xx	RFC3261	m	m	m			
Contact	3xx	RFC3261	o	－	－	c2	c2	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			（注 1）
Error-Info	300-699	RFC3261	o	o	o			（注 1）
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
Min-SE	422	RFC4028	m	m	m	c3（付表 1-7 項番 1）	c3（付表 1-7 項番 1）	
Organization		RFC3261	o	o	o			（注 1）
P-Access-Network-Info		RFC3455	o	o	－		c4	（注 1）
P-Charging-Function-Addresses		RFC3455	o	－	－	c5	c5	
P-Charging-Vector		RFC3455	o	－	－	c5	c5	
P-Media-Authorization	2xx	RFC3313	o	－	o	c6	c7	
Privacy		RFC3323	o	－	－	c8	c8	
Proxy-Authenticate	401	RFC3261	o	－	－	c9	c10	
Proxy-Authenticate	407	RFC3261	m	－	m	c9		
Reason		RFC3326	o	o	o			（注 1）
Record-Route	18x 2xx	RFC3261	o	o	o			（注 1）
Require		RFC3261	c	c	c	c3	c3	
Retry-After	404 413 480 486	RFC3261	o	o	o			（注 1）
Retry-After	500 503	RFC3261	o	o	o			（注 1）
Retry-After	600 603	RFC3261	o	o	o			（注 1）
Security-Server	421 494	RFC3329	o	－	o	c11	c12（付表 1-11 項番 1～2、付表 1-4 項番 3）	
Server		RFC3261	o	o	o			（注 1）
Session-Expires	2xx	RFC4028	o	m	m	c3（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	c3（付表 1-7 項番 1 で UNI 条件が「全セッションで利用する」の場合）	

				o	o	c3（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	c3（付表 1-7 項番 1 で UNI 条件が「必要に応じて個々のセッションで利用する」の場合）	
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			（注 1）
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			（注 1）
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			（注 1）
WWW-Authenticate	401	RFC3261	m	－	－	c13	c13	
WWW-Authenticate	407	RFC3261	o	－	－	c13	c13	
メッセージボディ		RFC3261		o	o			

c1: 対応するリクエストで Authorization ヘッダが利用されないため､Authentication-Info ヘッダによる認証情報の更新も行われない。

c2: 付属資料a.3の付表 a-1の 10.2.1.8.3 により 3xx レスポンスを用いたリダイレクトは利用しない。

c3: 本文 10.2.1.20.32、10.2.2.1 および 10.2.2.2.7 より、当該のヘッダを規定どおりに利用しなければならない。Session-Timer を利用する場合には、少なくとも Session-Expires ヘッダへの値（delta-seconds）の設定が必要になる。さらに Refresher を"uac"とする場合は Require ヘッダへの"timer"の設定が必要になる。（付表 1-7 項番 1）

c4: 付属資料a.3の付表 a-1の 10.1 により P-Access-Network-Info ヘッダは EUF から SCF 方向の SIP 信号にのみ適用可能である。

c5: 付属資料a.3の付表 a-1の 10.1 により P-Charging-Vector、P-Charging-Function-Addresses ヘッダは利用しない。

c6: 付属資料a.3の付表 a-1の 10.1 により EUF から SCF 方向では利用されない。

c7: UPDATE による SDP オファーが行われる場合に当該ヘッダの情報は有効に扱われる。（付表 1-23 項番 6）

c8: 付属資料a.3の付表 a-1の 10.2.2.2.4 により Privacy ヘッダは、REGISTER を除く既存ダイアログ外のリクエストにのみ適用される。

c9: 本文 10.2.1.20.27 節より、EUF から SCF 方向への Proxy-Authenticate ヘッダは利用されない。すなわち、401/407 レスポンス自体を利用しない。

c10: 付属資料a.3の付表 a-1の 10.2.1.20.27 により Proxy-Authenticate ヘッダは 401 レスポンスでは利用しない。

c11: 付属資料a.3の付表 a-1の 10.1 により Security-Server ヘッダは EUF から SCF 方向のレスポンスには適用されない。

c12: AKA 認証または呼制御信号の TLS 接続が利用される場合に利用される。（付表 1-11 項番 1～2、付表 1-4 項番 3）

c13: 付属資料a.3の付表 a-1の 10.2.1.20.44 により WWW-Authenticate ヘッダは、REGISTER リクエストの認証にのみ適用される。すなわち、401/407 レスポンス自体を利用しない。

注 1 EUF が送信する信号に指定した場合に SCF が期待通りの動作を行うか／行う能力を提供するかは、NGN 事業者のポリシーに委ねられる。

付録 vii.　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 呼接続において代表的な発着信に関わる呼接続シーケンス例を記載する。

本章で記載したシーケンス例は、あくまで実装時の参考の位置づけであり、各事業者のサービス内容や端末の機能により、本付録の記載シーケンスと異なる動作が必要となる場合がある。また、本シーケンス例の内容によって、通信の接続性や品質を保証するものではない。

付表 7-1／JT-Q3402　掲載シーケンス例一覧

No.	シーケンス名	対応する章節・図
1	端末登録（回線に基づく認証）	付録 vii.1.1
2	端末登録（HTTP Digest 認証）	付録 vii.1.2
3	端末削除（回線に基づく認証）	付録 vii.1.3
4	発信～切断（IPv4、timer・100rel 利用、G.711 μ-law）	付録 vii.1.4
5	発信～切断（IPv4、timer・100rel 利用、G.711 μ-law、HTTP Digest 認証）	付録 vii.1.5
6	着信～切断（IPv4、timer・100rel 利用、G.711 μ-law）	付録 vii.1.6
7	途中放棄	付録 vii.1.7
8	着側ビジー	付録 vii.1.8
9	ガイダンス聴取	付録 vii.1.9
10	ガイダンス聴取後接続（UPDATE 利用）	付録 vii.1.10
11	MESSAGE 送信（IPv6）	付録 vii.1.11
12	MESSAGE 着信（IPv6）	付録 vii.1.12
13	登録イベントの購読	付録 vii.1.13
14	登録イベントの通知（端末登録の削除）	付録 vii.1.14

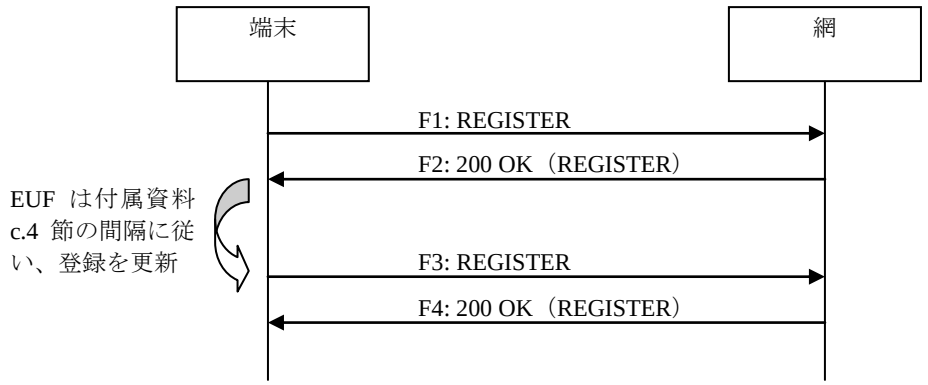
vii.1. シーケンス例

vii.1.1. 端末登録（回線に基づく認証）

網が端末の REGISTER を必須とし、端末の認証をアクセス回線に基づいて行う場合のシーケンス例を示す。Contact アドレスとして IPv4 及び IPv6 アドレスを 1 つずつ使用し、IPv4 の UDP で REGISTER を行っている。網は Service-Route ヘッダで pre-existing ルートを、P-Associated-URI ヘッダで利用可能な網付与ユーザ ID を通知している。

なお、下記の例をはじめ端末登録の例では、端末登録時の From ヘッダ・To ヘッダに指定する URI として vii.1.4節等に示す発信者番号の例と同様に電話番号を用いた SIP-URI を記載しているが、NGN 事業者のポリシーにより電話番号を用いて構成されない SIP-URI を用いる場合があることについて留意する必要がある。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP）： 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345　　IP（SIP）： 192.0.1.10, 2001:db8::1



付図 7-1／JT-Q3402　端末登録（回線に基づく認証）

F1: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F2: 200 OK（REGISTER）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe01:2345]
>;expires=3600
```

```
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

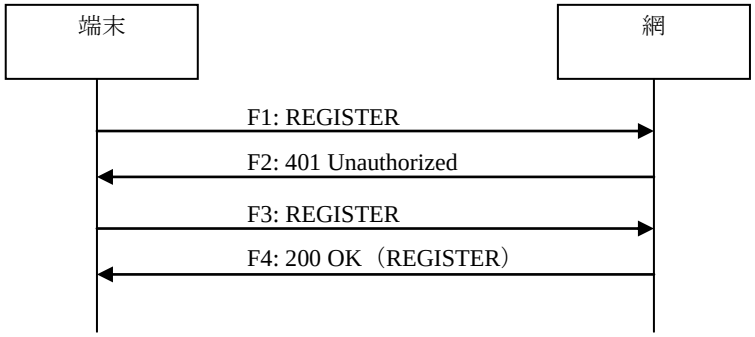
F4: 200 OK（REGISTER）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe01:2345]
>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

vii.1.2. 端末登録（HTTP Digest 認証）

vii.1.1とは異なり、網が端末の認証を HTTP Digest 認証を用いて行う場合のシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP）： 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345　　IP（SIP）： 192.0.1.10, 2001:db8::1



付図 7-2／JT-Q3402　端末登録（HTTP Digest 認証）

F1: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F2: 401 Unauthorized

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop11111111@192.0.1.1
CSeq: 1 REGISTER
Supported: path
WWW-Authenticate: Digest realm="example1.ne.jp",nonce="M5vIfYzRWDkD3E-iFxCJBfk8c68JXm5s
",algorithm=MD5
Content-Length: 0
```

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abce-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
```

```
Expires: 3600
Supported: path
Authorization: Digest realm="example1.ne.jp",nonce="M5vIfYzRWDkD3E-iFxCJBfk8c68JXm5s",uri=
"sip:example1.ne.jp",username="0311111111",response="70849961c8f5513ca19cbfc44c147c35",algorith
m=MD5
Content-Length: 0
```

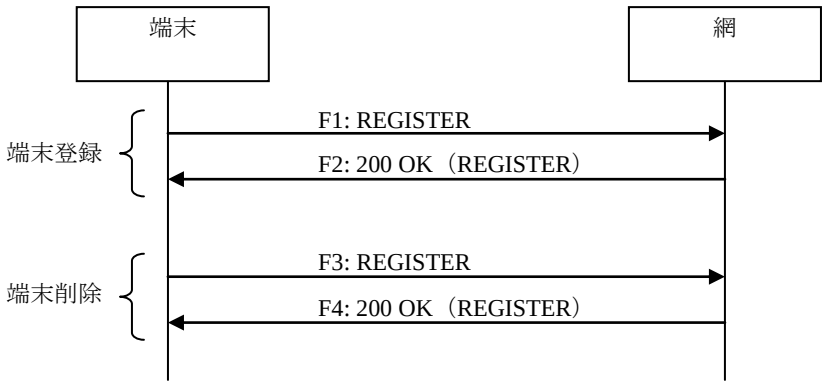
F4: 200 OK（REGISTER）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxv-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abce-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:fe01:2345]
>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

vii.1.3. 端末削除（回線に基づく認証）

vii.1.1と同一のオプション項目表選択条件下で、端末が電源投入時などに、端末の古い登録内容が網に残っている場合を想定し、端末の登録を削除する場合のシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP）： 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345　　IP（SIP）： 192.0.1.10, 2001:db8::1



付図 7-3／JT-Q3402　端末削除（回線に基づく認証）

F1～F2: 付録vii.1.1節と同一のため省略

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: *
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 0
Supported: path
Content-Length: 0
```

F4: 200 OK（REGISTER）

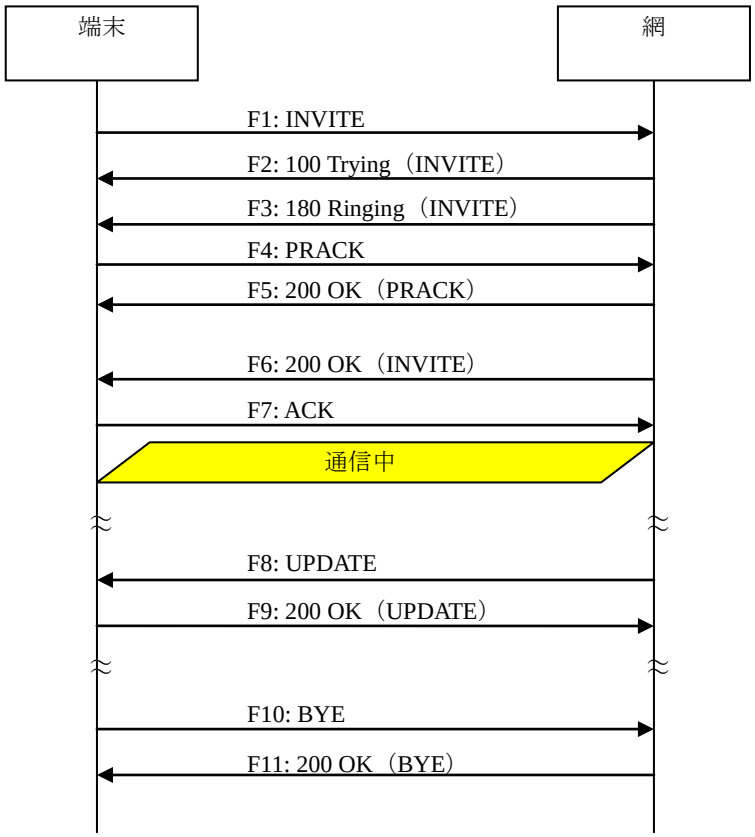
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

vii.1.4. 発信～切断（IPv4、timer・100rel 利用、G.711 μ-law）

発着ともに timer と 100rel の拡張機能を使用する場合の、発側における呼接続シーケンス例を示す。呼制御及びメディア信号には IPv4 を使用し、呼制御では UDP を、メディアでは音声として G.711 μ-law を使用している。セッション更新を UPDATE で実施し、最後に BYE で切断動作（発側切断）を行っている。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP/RTP）： 192.0.1.1

IP（SIP） ：192.0.1.10
IP（RTP） ：192.0.1.11



付図 7-4／JT-Q3402　発信～切断（IPv4、timer・100rel 利用、G.711 μ-law）（回線に基づく認証）

F1: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
```

```
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK（PRACK）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
Content-Length: 0
```

F6: 200 OK（INVITE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK（UPDATE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
```

```
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

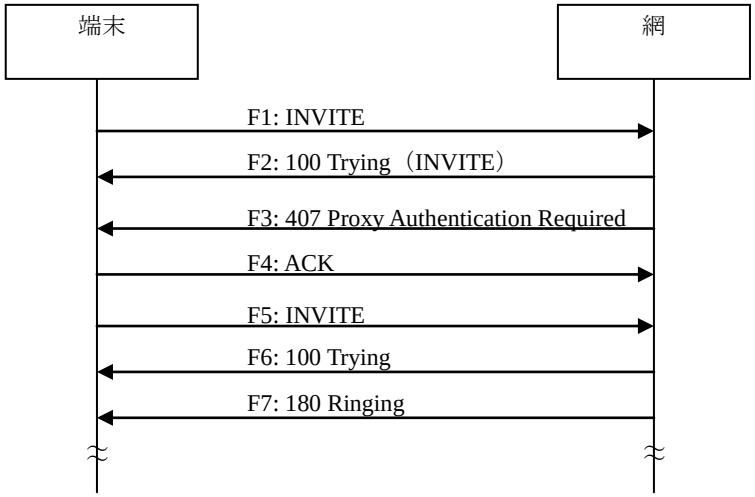
F11: 200 OK（BYE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

vii.1.5. 発信～切断（IPv4、timer・100rel 利用、G.711 μ-law、HTTP Digest 認証）

vii.1.4節と異なり、INVITE 信号に対して HTTP Digest 認証を行う場合のシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112　　IP（SIP） ：192.0.1.10
IP（SIP/RTP）： 192.0.1.1　　IP（RTP） ：192.0.1.11



付図 7-5／JT-Q3402　発信～切断（IPv4、timer・100rel 利用、G.711 μ-law）（HTTP Digest 認証）

F1: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
```

```
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F3: 407 Proxy Authentication Required

```
SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Proxy-Authenticate: Digest realm="example1.ne.jp",nonce="rBqRaPCEcljUN-VQ9wS97fgQHOs9Ig4k
",algorithm=MD5
Content-Length: 0
```

F4: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK2345678-11111121
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

F5: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Proxy-Authorization: Digest username="0311111111",realm="example1.ne.jp",nonce="rBqRaPCEcljU
N-VQ9wS97fgQHOs9Ig4k",uri="tel:0322222222;phone-context=example1.ne.jp",response="0cd3f053fe2
295036b73613dce5b2fa3",algorithm=MD5
Contact: <sip:xcvbnmz@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419518 82664419518 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F6: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Content-Length: 0
```

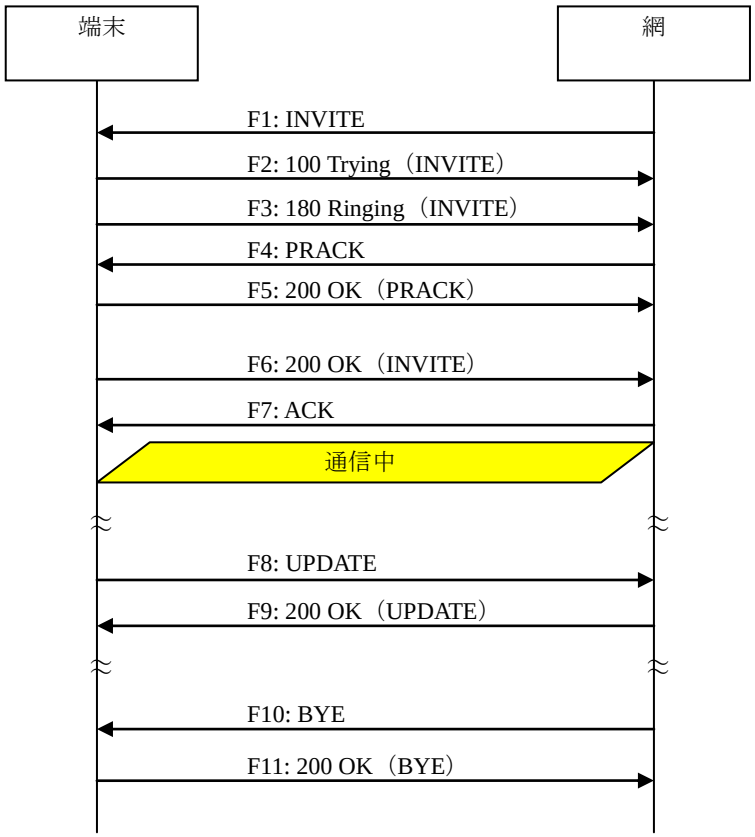
F7: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101021
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

vii.1.6. 着信～切断（IPv4、timer・100rel 利用、G.711 μ-law）

vii.1.4節と同一のオプション項目表選択条件下で、着側のシーケンス例を示す。網から着信後、UPDATE でセッション更新を行った後に、BYE で切断（着側切断）を行っている。網は着側端末に対して、P-Asserted-Identity ヘッダで発信者 ID 情報の通知を、P-Called-Party-ID ヘッダで着信対象の通知を行っている。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP/RTP）： 192.0.1.1
IP（SIP） ：192.0.1.10
IP（RTP） ：192.0.1.11



付図 7-6／JT-Q3402 着信～切断（IPv4、timer・100rel 利用、G.711 μ-law）

F1: INVITE

```
INVITE sip:qwertyui@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:03122222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:lkjhgfds@192.0.1.10>
P-Asserted-Identity: "0322222223" <sip:0322222223@example1.ne.jp>,"0322222223" <tel:0322222223;phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0311111112@example1.ne.jp>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 197
```

```
v=0
o=- 82664482616 82664482616 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 40000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
To: <sip:0311111112@example1.ne.jp>
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK（PRACK）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
Content-Length: 0
```

F6: 200 OK（INVITE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 30000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101022
Max-Forwards: 70
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:lkjhgfds@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
Max-Forwards: 70
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK（UPDATE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:lkjhgfds@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
```

```
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
Max-Forwards: 70
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

F11: 200 OK（BYE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

vii.1.7. 途中放棄（呼び出し中切断）

vii.1.4節と同一のオプション項目表選択条件下で、発側から途中放棄（呼び出し中切断）を行う場合のシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112　　IP（SIP） ：192.0.1.10
IP（SIP/RTP）： 192.0.1.1　　IP（RTP） ：192.0.1.11

付図 7-7／JT-Q3402　途中放棄（呼び出し中切断）

F1～F5 は付録vii.1.4節と同一であるため、省略する。

F6: CANCEL

```
CANCEL tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F7: 200 OK（CANCEL）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F8: 487 Request Terminated

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

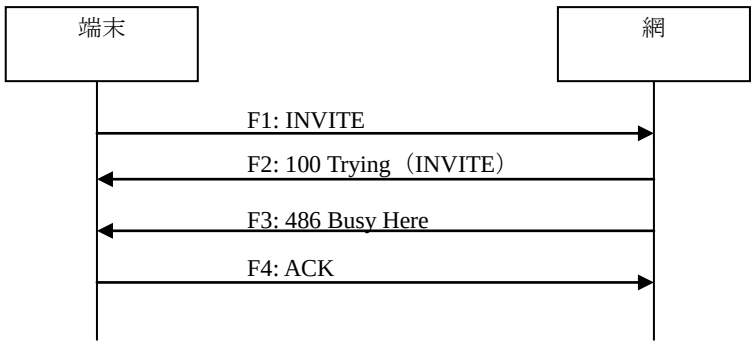
F9: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.8. 着側ビジー

vii.1.4節と同一のオプション項目表選択条件下で、着信先がビジー（空きセッション不足）であった場合のシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112　　IP（SIP） ：192.0.1.10
IP（SIP/RTP）： 192.0.1.1　　IP（RTP） ：192.0.1.11



付図 7-8／JT-Q3402　着側ビジー

F1～F2 は付録vii.1.4節と同一であるため、省略する。

F3: 486 Busy Here

```
SIP/2.0 486 Busy Here
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

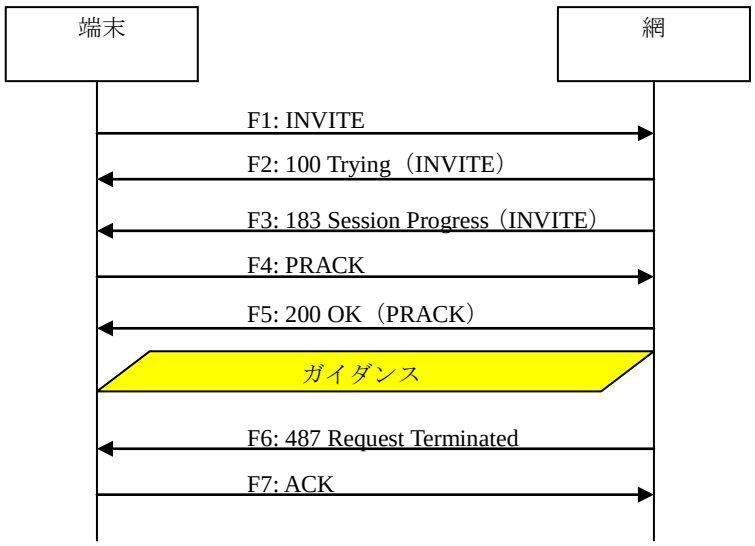
F4: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.9. ガイダンス聴取

vii.1.4節と同一のオプション項目表選択条件下で、網から音声ガイダンスが提供された後に切断されるシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP/RTP）： 192.0.1.1
IP（SIP） ：192.0.1.10
IP（RTP） ：192.0.1.11



付図 7-9／JT-Q3402　ガイダンス聴取

F1～F2 は付録vii.1.4節と同一であるため、省略する。

F3: 183 Session Progress（INVITE）

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F4～F5 は付録vii.1.4節と同一であるため、省略する。

F6: 487 Request Terminated

```
SIP/2.0 487 Request Terminated
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F7: ACK

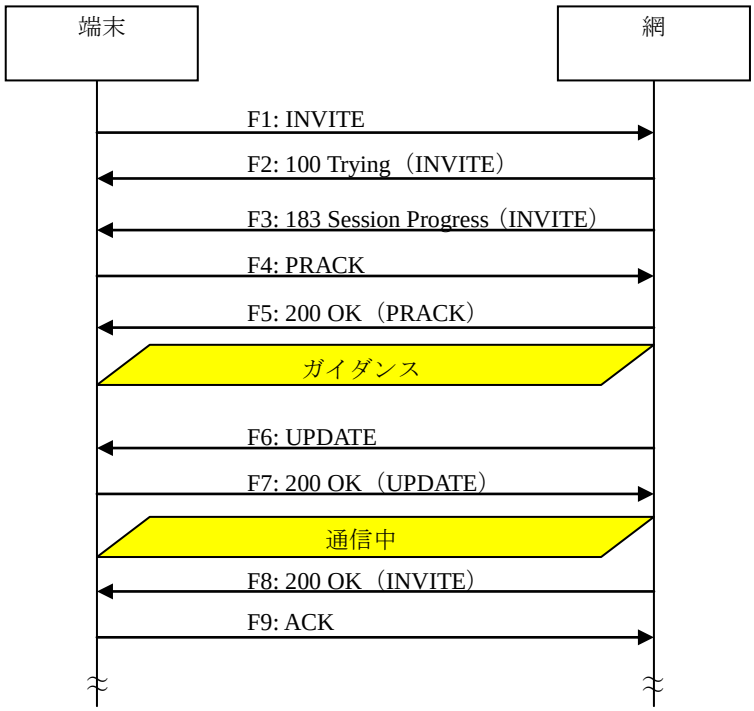
```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.10. ガイダンス聴取後接続（UPDATE 利用）

vii.1.9節と同様のシーケンスで網からガイダンスが提供された後、最終着信者に接続されて通信が行われる場合のシーケンス例を示す。ガイダンスから最終着信者への切り替えに際しては、Early ダイアログ中での UPDATE リクエストが利用されている。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP/RTP）： 192.0.1.1

IP（SIP） ：192.0.1.10
IP（RTP） ：192.0.1.11, 192.0.1.12



付図 7-10／JT-Q3402　ガイダンス聴取

F1～F5 は付録vii.1.9節と同一であるため、省略する。

F6: UPDATE

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Content-Length: 197

v=0
o=- 82917391739 82917391740 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.12
t=0 0
m=audio 21000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

```
a=ptime:20
```

F7: 200 OK（UPDATE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222222@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F8: 200 OK（INVITE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Length: 0
```

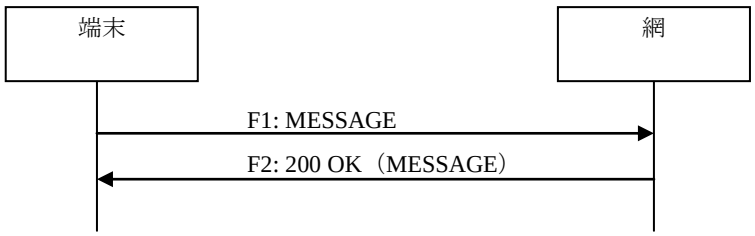
F9: ACK

```
ACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.11. MESSAGE 送信（IPv6 利用）

MESSAGE リクエストを用いて短いテキストメッセージを送信するシーケンス例を示す。IPv6 の UDP で SIP 信号の送受信を行っている。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP/RTP）： 2001:db8:1234:5678:acde:48ff:fe01:2345　　IP（SIP） ：2001:db8::1



付図 7-11／JT-Q3402　MESSAGE 送信（IPv6 利用）

F1: MESSAGE

```
MESSAGE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:2345]:5060;branch=z9hG4bK12345678-111111
31
Route: <sip:[2001:db8::1];lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
Call-ID: qwertyuiop111113@[2001:db8:1234:5678:acde:48ff:fe01:2345]
CSeq: 1001 MESSAGE
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Content-Type: text/plain;charset=utf-8
Content-Length: 13

foo bar baz
```

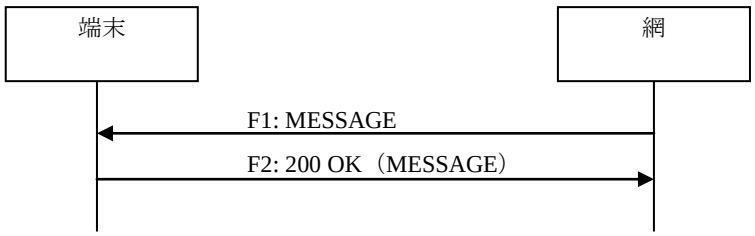
F6: 200 OK（MESSAGE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:2345]:5060;branch=z9hG4bK12345678-111111
31
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101030
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
Call-ID: qwertyuiop111113@[2001:db8:1234:5678:acde:48ff:fe01:2345]
CSeq: 1001 MESSAGE
Content-Length: 0
```

vii.1.12. MESSAGE 着信（IPv6 利用）

MESSAGE リクエストを用いて短いテキストメッセージを受信するシーケンス例を示す。IPv6 の UDP で SIP 信号の送受信を行っている。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP/RTP）： 2001:db8:1234:5678:acde:48ff:fe01:2345　　IP（SIP） ：2001:db8::1



付図 7-12／JT-Q3402　MESSAGE 着信（IPv6 利用）

F1: MESSAGE

```
MESSAGE sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345] SIP/2.0
Via: SIP/2.0/UDP [2001:db8::1]:5060;branch=z9hG4bK87654321-10101030
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:03122222223@example1.ne.jp>;tag=9876zyxw-10101030
Call-ID: poiuytrewq101030@[2001:db8::1]
CSeq: 2001 MESSAGE
P-Asserted-Identity: "0322222223" <sip:0322222223@example1.ne.jp>,"0322222223" <tel:032222222
3;phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0311111112@example1.ne.jp>
Content-Type: text/plain;charset=utf-8
Content-Length: 13

foo bar baz
```

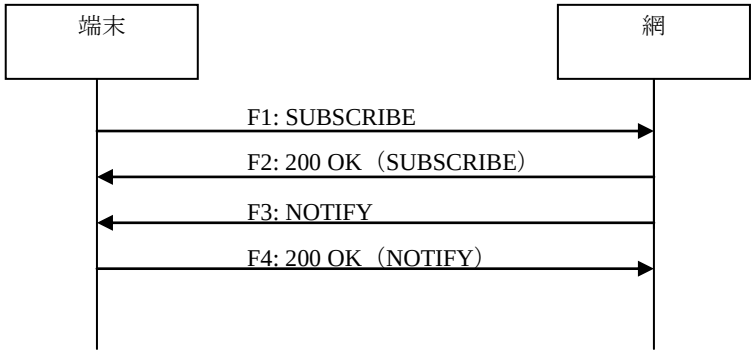
F6: 200 OK（MESSAGE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8::1]:5060;branch=z9hG4bK87654321-10101030
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101030
Call-ID: poiuytrewq101030@[2001:db8::1]
CSeq: 2001 MESSAGE
Content-Length: 0
```

vii.1.13. 登録イベントの購読

付属資料c.6に記載される登録（reg）イベントを購読（SUBSCRIBE）する場合のシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112　　IP（SIP） ：192.0.1.10
IP（SIP/RTP）： 192.0.1.1　　IP（RTP） ：192.0.1.11



付図 7-13／JT-Q3402　登録イベントの購読

F1: SUBSCRIBE

```
SUBSCRIBE sip:0311111111@example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111141
Max-Forwards: 70
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp>
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 1 SUBSCRIBE
Contact: <sip:wertyuio@192.0.1.1>
P-Preferred-Identity: <sip:0311111111@example1.ne.jp>
Privacy: none
Event: reg
Expires: 3600
Accept: application/reginfo+xml
Content-Length: 0
```

F2: 200 OK（SUBSCRIBE）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060; branch=z9hG4bK12345678-11111141
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 1 SUBSCRIBE
Contact: <sip:oiuytrew@192.0.1.10>
Event: reg
Expires: 3600
Content-Length: 0
```

F3: NOTIFY

```
NOTIFY sip:wertyuio@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101040
Max-Forwards: 69
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
```

```
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Contact: <sip:oiuytrew@192.0.1.10>
Subscription-State: active;expires=3600
Event: reg
Expires: 3600
Content-Type: application/reginfo+xml
Content-Length: 741

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
                    version="1" state="full">
  <registration aor="sip:0311111111@example1.ne.jp" id="a7" state="active">
    <contact id="76" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="sip:0311111112@example1.ne.jp" id="a8" state="active">
    <contact id="77" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="tel:+81311111111" id="a9" state="active">
    <contact id="78" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
</reginfo>
```

F4: 200 OK（NOTIFY）

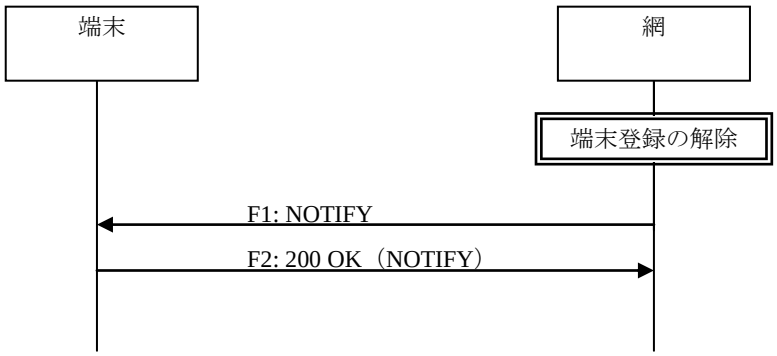
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101040
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Content-Length: 0
```

vii.1.14. 登録イベントの通知（端末登録の削除）

vii.1.13節で購読を行った登録イベントで、網側で端末登録の解除が行われた際に NOTIFY リクエストで端末に通知される場合のシーケンス例を示す。

SIP ドメイン： example1.ne.jp
TEL： 03-1111-1111, 03-1111-1112
IP（SIP/RTP）： 192.0.1.1

IP（SIP） ：192.0.1.10
IP（RTP） ：192.0.1.11



付図 7-14／JT-Q3402　登録イベントの通知

F1: NOTIFY

```
NOTIFY sip:wertyuio@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101041
Max-Forwards: 69
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Contact: <sip:oiuytrew@192.0.1.10>
Subscription-State: terminated
Event: reg
Expires: 3600
Content-Type: application/reginfo+xml
Content-Length: 758

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
                version="1" state="full">
  <registration aor="sip:0311111111@example1.ne.jp" id="a7" state="active">
    <contact id="76" state="terminated" event="deactivated">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="sip:0311111112@example1.ne.jp" id="a8" state="active">
    <contact id="77" state="terminated" event="deactivated ">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="tel:+81311111111" id="a9" state="active">
    <contact id="78" state="terminated" event="deactivated ">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
</reginfo>
```

F2: 200 OK（NOTIFY）

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101041
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Content-Length: 0
```