

JJ-22.11

企業 SIP 網に接続する SIP 端末⇔サーバ間 基本接続インタフェース技術仕様

Basic connection interface technical specifications between
SIP terminal <=> Servers linked to a Private SIP network

第 2.1 版

2016 年 6 月 9 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

本書は、一般社団法人情報通信技術委員会が著作権を保有しています。
内容の一部又は全部を一般社団法人情報通信技術委員会の許諾を得ることなく複製、転載、改変、転用及びネットワーク上での送信、配布を行うことを禁止します。

目次

<参考>.....	7
1. 概説.....	9
1.1. 本標準の適用範囲.....	9
1.1.1. 基本接続形態.....	9
1.2. 本標準の目的と規定.....	10
1.3. 本標準の内容.....	10
1.3.1. 本標準策定の背景と位置づけについて.....	10
1.3.2. 想定する接続相手.....	11
1.3.3. フィールドの条件.....	11
1.3.4. 設定選択オプション.....	11
1.3.5. 本標準の位置づけ.....	11
1.3.6. B2BUA での、UAC、UAS の考え方.....	12
1.4. 用語.....	13
2. 各種定義.....	14
2.1. 表における定義.....	14
3. 下位レイヤ.....	14
4. ロケーション情報登録動作.....	14
4.1. REGISTER リクエスト送受信.....	14
4.1.1. 基本動作.....	14
4.1.2. Request-URI.....	15
4.1.3. REGISTER リクエストヘッダ.....	15
4.1.4. 登録.....	17
4.1.5. 削除.....	17
4.1.6. 更新.....	18
4.1.7. 確認.....	18
4.2. 認証.....	18
4.2.1. 401 (Unauthorized) レスポンス送受信.....	19
4.2.2. 認証 REGISTER リクエスト送信.....	19
4.3. 2xx レスポンス送受信.....	20
4.3.1. 基本動作.....	20
4.3.2. 登録に対する 2xx レスポンス送受信.....	20
4.3.3. 削除に対する 2xx レスポンス受信.....	21
4.3.4. 更新に対する 2xx レスポンス送受信.....	21
4.3.5. 確認に対する 2xx レスポンス送受信.....	21
4.3.6. ロケーション情報の正当性検証における留意事項.....	21
4.4. 3xx/4xx/5xx/6xx レスポンス送受信.....	21
4.4.1. 基本動作.....	21
4.5. 輻輳抑制への考慮.....	22
4.5.1. ロケーション情報登録動作失敗時のリトライに関する留意事項.....	22
4.5.2. 複数 REGISTER における留意事項.....	22
4.5.3. 一時的障害発生時における留意事項.....	22

5.	Initial INVITE リクエスト送信	23
5.1.	Initial INVITE リクエスト送信	23
5.1.1.	基本動作.....	23
5.1.2.	Request-URI.....	23
5.1.3.	AoR (From ヘッダ)	24
5.1.4.	認証.....	24
5.2.	1xx レスポンス受信.....	26
5.2.1.	基本動作.....	26
5.2.2.	呼出中音の再生と Early メディア	27
5.2.3.	複数ダイアログとメディアの管理	28
5.3.	2xx レスポンス受信.....	28
5.3.1.	基本動作.....	28
5.3.2.	複数ダイアログとメディアの管理	28
5.4.	3xx レスポンス受信.....	29
5.4.1.	基本動作.....	29
5.4.2.	ACK リクエスト送信.....	29
5.5.	4xx/5xx/6xx レスポンス受信.....	29
5.5.1.	基本動作.....	29
5.5.2.	ACK リクエスト送信.....	29
5.6.	途中放棄	29
5.6.1.	CANCEL リクエスト送信	29
5.6.2.	信号／処理衝突に関する留意事項	30
5.7.	留意事項	30
5.7.1.	輻輳制御への考慮.....	30
5.7.2.	リクエストの Contact ヘッダの値.....	30
5.7.3.	INVITE リクエストのリトライ	30
6.	Initial INVITE リクエスト受信	30
6.1.	Initial INVITE リクエスト受信.....	30
6.1.1.	基本動作.....	30
6.1.2.	Request-URI.....	31
6.2.	1xx レスポンス送信.....	31
6.2.1.	基本動作.....	31
6.2.2.	180(Ringing)レスポンス	31
6.3.	2xx レスポンス送信.....	32
6.3.1.	基本動作.....	32
6.4.	3xx レスポンス送信.....	32
6.5.	4xx/5xx/6xx レスポンス送信.....	32
6.6.	エラーレスポンスに対する ACK リクエスト受信.....	32
6.7.	途中放棄	32
6.7.1.	CANCEL/BYE リクエスト受信	32
6.7.2.	信号／処理衝突に関する留意事項	33
6.8.	その他留意事項	33
6.8.1.	レスポンスの Contact ヘッダの値.....	33

7.	リモートターゲット	33
7.1.	基本動作	33
7.2.	発呼側リモートターゲット	33
7.3.	着呼側リモートターゲット	34
8.	100rel 拡張機能	34
8.1.	能力交換	34
8.2.	1xx レスポンス送信	34
8.3.	PRACK リクエスト送信	34
9.	セッションタイム拡張機能	34
9.1.	能力交換	35
9.2.	セッションリフレッシュリクエスト	35
9.2.1.	re-INVITE リクエスト	35
9.2.2.	UPDATE リクエスト	35
9.3.	リフレッシャー決定	36
9.3.1.	セッション確立時	36
9.3.2.	セッション更新時	36
9.4.	セッションタイム値と Min-SE 値	37
9.4.1.	発呼側/リフレッシャー側	37
9.4.2.	着呼側/非リフレッシャー側	37
9.5.	セッションの更新	37
9.5.1.	リフレッシャー側	37
9.5.2.	非リフレッシャー側	37
9.5.3.	メディア変更にともなうリクエスト送信	38
9.6.	セッションリフレッシュ失敗時	38
10.	メディア確立	38
10.1.	コーデック	38
10.2.	SDP	38
10.2.1.	オファー/アンサーによるメディア確立	38
10.2.2.	メディア変更要求受信	40
10.2.3.	メディア変更要求送信	40
10.2.4.	re-INVITE トランザクションにおける留意事項	40
11.	呼切断	41
11.1.	BYE リクエスト送信	41
11.2.	BYE リクエスト受信	41
12.	付加機能	41
12.1.	番号通知/非通知	41
12.1.1.	Initial INVITE リクエストの設定規則	41
12.1.2.	ヘッダ透過転送に関する留意事項	42
12.2.	発信者番号表示	42
12.2.1.	方式 1 発信者番号表示	43
12.2.2.	方式 2 発信者番号表示	43
13.	SIP 関連信号フォーマット	44
13.1.	基本信号フォーマット	44

13.1.1.	SIP リクエスト信号.....	44
13.1.2.	SIP レスポンス信号.....	44
13.1.3.	SDP.....	52
13.2.	動的変数共通条件	52
13.2.1.	SIP 端末設定・保持情報の実装値条件.....	52
13.2.2.	SIP 端末変数値条件.....	53
13.3.	SIP リクエスト信号.....	54
13.3.1.	ACK リクエスト (2xx レスポンス時)	54
13.3.2.	ACK リクエスト (3xx/4xx/5xx/6xx レスポンス時)	56
13.3.3.	BYE リクエスト	57
13.3.4.	CANCEL リクエスト.....	58
13.3.5.	Initial INVITE リクエスト.....	59
13.3.6.	PRACK リクエスト	60
13.3.7.	re-INVITE リクエスト.....	62
13.3.8.	REGISTER リクエスト	64
13.3.9.	UPDATE リクエスト	65
13.4.	SIP レスポンス信号.....	66
13.4.1.	BYE リクエストに対するレスポンス.....	66
13.4.2.	CANCEL リクエストに対するレスポンス.....	69
13.4.3.	Initial INVITE リクエストに対するレスポンス.....	70
13.4.4.	PRACK リクエストに対するレスポンス.....	72
13.4.5.	re-INVITE リクエストに対するレスポンス	74
13.4.6.	REGISTER リクエストに対するレスポンス.....	76
13.4.7.	UPDATE リクエストに対するレスポンス.....	78
付録 i.	シーケンス例	80
i.1	REGISTER 登録.....	81
i.2	REGISTER 指定削除.....	83
i.3	REGISTER 全指定削除.....	85
i.4	接続シーケンス 1 (発着 100rel 動作、発着 timer 動作、発着 UPDATE 動作)	87
i.5	接続シーケンス 2 (発着 100rel 未動作、発着 timer 動作、発着 UPDATE 未動作)	96
i.6	接続シーケンス 3 (発着 100rel 未動作、発着 timer 未動作、発着 UPDATE 未動作)	106
i.7	接続シーケンス 4 (INVITE 認証つき)	112

<参考>

1. 国際勧告等の関連

本標準に関する国際勧告はない。

2. 改版の履歴

版数	制定日	改版内容
第 1.0 版	2013 年 5 月 23 日	初版制定
第 1.1 版	2013 年 6 月 13 日	誤記訂正
第 2.0 版	2014 年 5 月 22 日	認証機能追加
第 2.1 版	2016 年 6 月 9 日	図 1.1 の誤記訂正

3. 参照文書

3.1. 規準参照文書

- [1] "SIP:セッション開始プロトコル(SIP: 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.
- [2] "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.
- [3] "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.
- [4] "セッション開始プロトコル(SIP)UPDATE メソッド" (The Session Initiation Protocol UPDATE Method, JF-IETF-RFC3311, 情報通信技術委員会(The Telecommunication Technology Committee), 2005 年 6 月.
- [5] "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 第 1 版, 情報通信技術委員会(The Telecommunication Technology Committee), 2005 年 6 月.
- [6] "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.
- [7] "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 第 1 版, 情報通信技術委員会(The Telecommunication Technology Committee), 2005 年 6 月.
- [8] "電話番号のための tel URI(The tel URI for Telephone Numbers)", TTC 標準 JF-IETF-RFC3966 第 1 版, 情報通信技術委員会(The Telecommunication Technology Committee), 2005 年 6 月.
- [9] "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.
- [10] "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 6 月.
- [11] "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.

- [12] " PULSE CODE MODULATION (PCM) OF VOICE FREQUENCIES ", ITU-T Recommendation G.711, ITU-T, 1998.
- [13] “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 Protocol(SIP) , JF-IETF-RFC4028, 情報通信技術委員会(The Telecommunication Technology Committee), 2005年8月.
- [14] “DTMF デジタル、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), JF-IETF-RFC2833, 情報通信技術委員会(The Telecommunication Technology Committee), 2006年6月.
- [15] “企業 SIP 網間における相互接続インタフェース”(Technical Specifications on Inter-connection Interface between Private SIP Networks)、JJ-22.01 情報通信技術委員会 (The Telecommunication Technology Committee), 2007年12月.

3.2. 非規準参照文書

- [16] "Session Initiation Protocol (SIP)に関する技術レポート", TR-1007, 情報通信技術委員会 (The Telecommunication Technology Committee), 2003年3月

4. 工業所有権

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

5. 標準策定部門

企業ネットワーク専門委員会

1. 概説

1.1. 本標準の適用範囲

本標準は、JJ-22.01[15]に規定されるフレームワーク標準の網接続アーキテクチャにおいて、私設総合サービス網交換機(PINX)と SIP 端末間（インターフェース E）の推奨仕様を規定するものである。

また、インタフェース B を経由して接続される端末が、本標準の範囲を超えた能力を保持することを妨げるものではない。但し、その場合においても本標準に準拠する端末との接続性について考慮することが望ましい。

1.1.1. 基本接続形態

本標準は、図 1.1 で示す企業 SIP 網相互接続モデルに規定されるインタフェース E に適用可能な管理された企業 SIP 網との接続インタフェースの条件を示す。本インタフェースの規定を遵守できるインタフェースを有する企業 SIP 網に関して、

本標準では“管理された企業 SIP 網”と呼ぶ。以下企業 SIP 網と表記する場合は、“管理された企業 SIP 網”であることを前提とする。

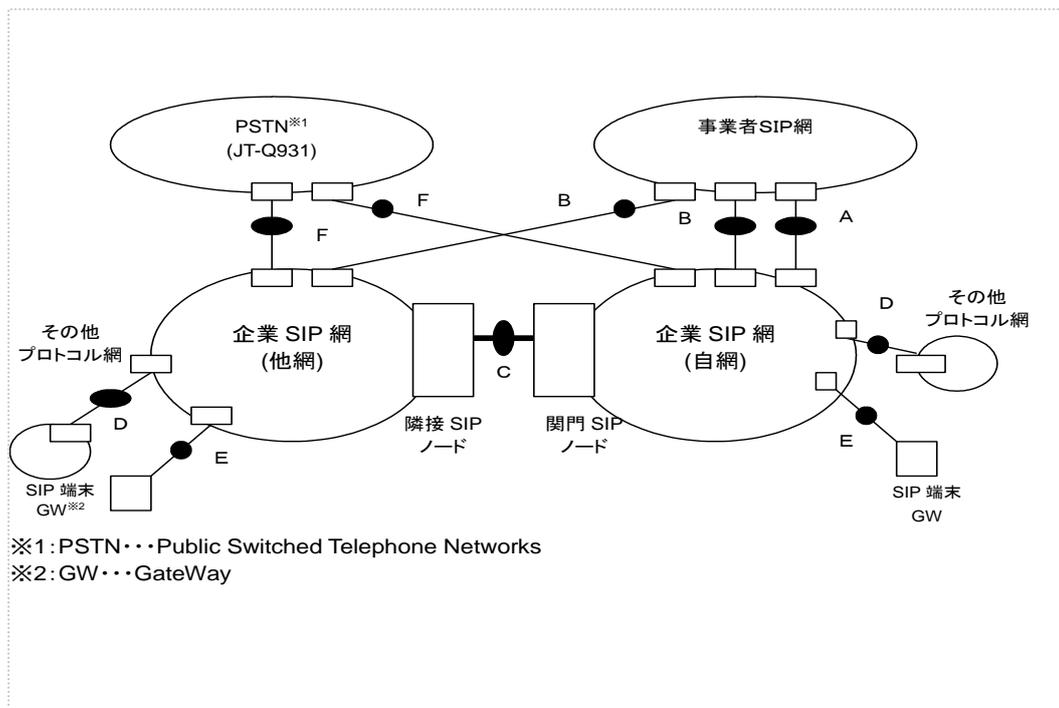


図 1.1 企業 SIP 網相互接続モデル

1.2. 本標準の目的と規定

本標準では、私設総合サービス網交換機(PINX)及び SIP 端末の実装に際して、

- 接続条件に関わる規定の解釈を一意とすることで、実装可能な標準とする。
- SIP 網を介した私設総合サービス網交換機(PINX)と SIP 端末との接続において、共通的に適用することが可能な標準とする。
- 本規定の範囲を超えるまたは、厳密に本規定を遵守していない SIP UA との接続性にも最大限配慮した標準とする。

ことを目的に以下の規定を行う。

- 呼制御信号条件及び登録信号条件として、JF-IETF-RFC3261[1]で規定される SIP 及びその拡張規定の用法に関する事項
- 音声のメディア条件として、メディア能力条件、SDP 及び RTP に関する事項¹
- その他の呼接続動作及び登録動作に関わる SIP サーバ及び SIP 端末の動作に関する事項

1.3. 本標準の内容

本仕様の本文では、主として以下の事項について規定を行う。

- 私設総合サービス網交換機(PINX)と SIP 端末は、B2BUA で接続されることを前提とし、SIP 網を介した私設総合サービス網交換機(PINX)に接続するための動作規定として、ロケーション登録時の動作(4章)、発信時の動作(5章)、着信時の動作(6章)、呼切断時の動作(11章)について規定する。また、必要となるレコードルートの処理(7章)についても規定を行う。
- 実装が必要となる、機能拡張として 100rel(8章)とセッションタイマ(9章)の詳細動作について規定する。
- 音声呼を確立するためのオファー/アンサーモデルに必要な動作(10章)について規定する。
- 付加サービスに関する動作規定として、発信時及び着信時における発信者番号表示に関する動作(12章)について規定する。
- メッセージのフォーマットに関する規定(13章)を行う。
- シーケンス例を記載(付録 i)する。

1.3.1. 本標準策定の背景と位置づけについて

1.3.1.1. 概要

本付録は、本標準策定の背景および技術基準策定における判断基準について記述する。

1.3.1.2. 本標準策定の背景

本標準策定時点において、日本国内では私設総合サービス網交換機(PINX)と SIP 端末間の規定が無かった。このため、本標準策定においては、本標準に準拠する端末同士が、それらが接続できる能力を持った私設総合サービス網交換機(PINX)を介して接続することだけを想定した規定ではなく、本標準に準拠する端末同士が、策定時点で既にサービス提供されている私設総合サービス網交換機(PINX)を介して接続する場合や、さらには接続する私設総合サービス網交換機(PINX)だけでなく相手端末が策定時点で既にサービ

¹ 音声以外のメディアをサポートしている SIP UA との接続性にも配慮しなければならない。

ス提供されている場合においても、それら私設総合サービス網交換機 (PINX) 及び端末との間で、基本的な音声呼の接続が可能となるような共通の技術標準を策定することを目的として策定を行った。

1.3.1.3. 技術規準策定における判断基準

上記の本標準策定の背景に基づいて、技術規準策定における判断基準として特に留意されるべき事項を以下に記述する。

1.3.2. 想定する接続相手

本標準の動作は、原則として IETF で定められる RFC 文書の規定内容に違反しないように定められる。ただし、本標準の適用対象となる端末は、接続相手 (SIP 網または端末) が必ずしも IETF 等で規定される技術規定の動作に従っていない場合でも、実際に存在するものであれば、RFC 文書等の規定に違反しない範囲で接続が可能となるように本標準の技術規準を定めている。

1.3.3. フィールドの条件

本標準では、RFC 文書の規定の範囲を超えて SIP メッセージのフィールドに関するフォーマット条件を限定している場合がある。その中でも、送信条件と受信条件が異なる規定となっているものが存在することに留意する必要がある。そのような規定とした主な理由は、1.3.1.2 節で記載したように本標準に準拠する端末が接続する SIP 網及び相手端末における動作仕様を一意に特定できないことにより、想定する接続相手への送信条件と想定する接続相手からの受信条件のそれぞれにおける要求条件に差分が存在するからである。送信条件としては、実際に存在する接続相手が受入れ可能となるように、より厳格な規定を行い、受信条件としては、実際に存在する接続相手が送信する可能性のあるメッセージを受入れ可能となるように、より緩やかな規定を行うことで、より確実な接続性を確保することを目的としている。

1.3.4. 設定選択オプション

本標準の適用対象となる端末の動作において、動作を一意に決定するのではなく、いくつかの設定可能な選択項目としている場合がある。そのような規定となる理由は、接続する私設総合サービス網交換機 (PINX) や相手側端末のポリシーにより、ある私設総合サービス網交換機 (PINX) では接続やサービスの保証のために動作 A を要求し、別の私設総合サービス網交換機 (PINX) では別の動作 B を要求するような動作規定が存在するためであり、このような動作規定については、動作 A と動作 B を端末において設定などにより選択が可能であることを条件とした項目としている。なお、選択の方法については、本標準では範囲外とし、言及しない。

1.3.5. 本標準の位置づけ

本標準は、既に存在する私設総合サービス網交換機 (PINX) や多様な音声端末との接続が可能となるような技術規準として定められる。なお、本標準の規定については、国内における SIP を利用し音声接続を行うことを目的とした端末における最低限の条件を満たす基準仕様として参照されることが期待される。

1.3.6. B2BUA での、UAC、UAS の考え方

本標準は、図 1.2 で示す B2BUA 接続モデルに規定される UAC、UAS の考え方を前提とする。

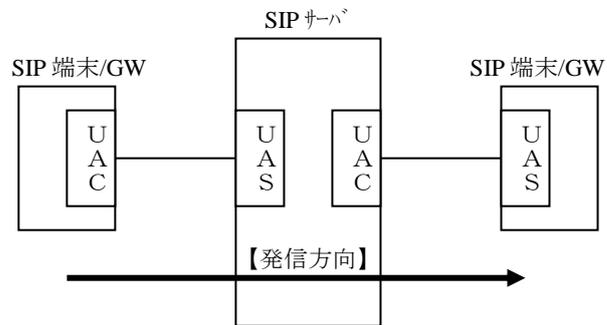


図 1.2 B2BUA 接続モデル

1.4. 用語

本標準で使用する用語について定義する。

AoR	:	私設総合サービス網交換機(PINX)が電話番号と紐付けて管理している SIP URI 形式の文字列。Address of Record の略。
re-INVITE	:	存在するダイアログ内で送信される INVITE リクエストメッセージ。
オファー	:	JF-IETF-RFC3264[3]で規定される SDP オファー/アンサーモデルにおいて、オファー(offer)となる SDP
アンサー	:	JF-IETF-RFC3264[3]で規定される SDP オファー/アンサーモデルにおいて、アンサー(answer)となる SDP
SIP サーバアドレス	:	SIP 端末がセッション確立のための SIP メッセージ送受信を行う SIP プロキシサーバのアドレス。FQDN(Fully Qualified Domain Name)形式または、IPv4 アドレス形式で与えられる。 及び、特定の AoR に対して Initial INVITE リクエストをフォローアップするために必要なロケーション情報を、私設総合サービス網交換機(PINX)が SIP 端末からの動的な Register 登録により受け付けるための SIP サーバのアドレス。FQDN 形式または、IPv4 アドレス形式で与えられる。
SIP 端末	:	SIP を介して私設総合サービス網交換機(PINX)と接続し、音声通信を行うために、SIP のユーザ・エージェントを実装した端末設備等の総称である。
SIP UA	:	私設総合サービス網内に存在する、一般的な SIP のユーザ・エージェント。
認証リクエスト	:	HTTP Digest 方式等による認証結果を設定した Authorization もしくは Proxy-Authorization ヘッダが付与されたリクエスト
パスワード	:	HTTP Digest 方式による認証を行う場合のユーザ名に対応するパスワード文字列
ユーザ	:	SIP 端末の利用者（人間または、電話機など接続される他の端末設備）や、SIP UA の制御を司る上位アプリケーションなどの総称。
ユーザ名	:	HTTP Digest 方式による認証を行う場合のユーザ名の文字列
ユーザリソース	:	SIP 端末の内部において、SIP 上での呼制御や音声メディアの送受信をユーザに提供するためのリソースの総称（例：2Wアナログ電話機を接続する宅内GWにおいては、2Wアナログインタフェースを指す）。
ロケーション情報	:	ある瞬間において特定の AoR に対する SIP 網上の SIP UA としての位置情報。SIP URI 形式で表現されており、SIP メッセージを送信する宛先としての IPv4 アドレス、ポート番号を含む。

2. 各種定義

2.1. 表における定義

本規定に記載される表中において共通で使用する規定タイプの定義を表 2-1 にて規定する。

表 2-1/JJ-22.11 表における規定タイプの定義

コード	コード名	意味
m	mandatory	この機能がサポートされている必要がある。 ここで“必須 (mandatory)”という言葉の意味することは、参照される規定を機能として有しているということである。必須とされているからといって必ず常に発現するというのではなく、参照する文書で規定される動作に従い、必要とされる場合に発現される必要があることを示している。 例えば、送信パラメータとして、このコードが指定されていた場合においては、常にそのパラメータが含まれていることを意味せず、参照文書の規定に従って必要な場合に含められることを意味している(動的な適用要求条件)。
o	optional	能力のサポートは、実装に依存しており、サポートされるかもしれないし、サポートされないかもしれない。
n/a	not applicable	この機能のサポート条件は、意味を持たない。(対応する機能を規定する標準を示す)サポート列は省略してよい。
x	prohibited (excluded)	この機能は、使用が許されない。
c <integer>	conditional	機能のサポート条件(m,o,n/a,x)は、他の選択可能な条件(c<数字>で示される)に依存している。
o.<integer>	qualified optional	同じ<数字>の中から排他的に選択可能なオプションであることを示す。
i	irrelevant	本標準の範囲外であることを示す。ベースとなる仕様が別の標準に立脚している場合などでは別の場合でも有用なケースもある。

3. 下位レイヤ

SIP メッセージの送受信は UDP/IPv4 とする。この規定は TCP、TLS、IPv6 等の使用を妨げるものではない。

4. ロケーション情報登録動作

本章では、REGISTER メソッドによる SIP サーバ及び、SIP 端末のロケーション情報登録動作を規定する²。

4.1. REGISTER リクエスト送受信

4.1.1. 基本動作

SIP 端末は自身が保持する特定の AoR に対するロケーション情報を自身が属する私設総合サービス網交換機(PINX)に登録すべく、その私設総合サービス網交換機(PINX)に存在する SIP サーバを宛先とした REGISTER リクエストを、SIP サーバに送信する。登録されたロケーション情報は、その AoR に対して着信があった場合に私設総合サービス網交換機(PINX)にてロケーション解決に使用され、そのロケーション情報宛に Initial INVITE がフォワーディングされる。

²ロケーション情報の解決に REGISTER メソッドを用いない私設総合サービス網交換機(PINX)との接続においては、本章の規定は適用されない。

送信した REGISTER リクエストに対して 401(Unauthorized)レスポンスを受信した場合には、4.2 節に従って認証処理を行う必要がある。

また、SIP サーバは、SIP 端末からの REGISTER リクエストを受信した場合、4.2 節に従った認証処理により、登録可能と判断した場合は当該 SIP 端末の各種情報(AoR など)を登録し、200(OK)レスポンスを送信する。その後、当該 AoR に対して着信があった場合に、そのロケーション情報宛に Initial INVITE を送信する。

4.1.2. Request-URI

REGISTER リクエストの Request-URI は SIP URI 形式で構成する。なお、SIP URI 形式以外での Request-URI の構成は本規定の範囲を超える。

Request-URI は以下のとおり構成する。

Request-uri = "sip:" host [:port] [uri-parameters]

表 4-1 / JJ-22.11 REGISTER リクエスト送信時の Request-URI 構成要素

構成要素	参照	種別 (送信側)	備考
host	[1]	m	一般的には SIP サーバアドレス (AoR の host 文字列とは異なるかもしれない) を用いることが想定される
port	[1]	cl	
uri-parameters	[1]	o	省略可能。詳細な規定は本規定の範囲を超える
cl:5060 を使用する場合は"o"、5060 以外を使用する場合は"m"			

4.1.3. REGISTER リクエストヘッダ

4.1.3.1. 必須ヘッダの扱い

JF-IETF-RFC3261[1] 20 章の Table 2 及び Table 3 で REGISTER リクエストにおいて必須の設定であるヘッダに関して SIP 端末に対して要求される設定条件を表 4-2 に示す。

表 4-2/JJ-22.11 REGISTER リクエスト送出時の必須ヘッダ値設定

ヘッダ	値	補足
To	ロケーション情報登録動作を行う対象の AoR (SIP URI) を指定する。	
From	ロケーション情報登録動作を行う対象の AoR (SIP URL) を指定する (この場合 To ヘッダと同じ)。	設定変更により、ロケーション情報登録動作を行う対象の AoR とは異なる第三者の AoR を設定できる機能を有してもよい ³ 。
Call-ID	<Global-Unique-ID>	過去のロケーション情報登録動作と同一 Call-ID を用いたロケーション情報登録動作を行う場合、CSeq の値をそのときよりも大きく設定していない REGISTER リクエストは許容されないことに留意する。(例えば SIP 端末のリポート時などに以前と同一 Call-ID、且つ CSeq をインクリメントしていない場合は SIP サーバにて許容されない)。
Via	<via-param>	JF-IETF-RFC3261[1]に従う。
CSeq	<整数値 LWS Method >	JF-IETF-RFC3261[1]に従う。整数値は 32-bit 符合なし整数で表記可能な値。
Max-Forwards	70	JF-IETF-RFC3261[1]に従う。

4.1.3.2. Contact ヘッダの扱い

ロケーション情報である REGISTER リクエストの Contact ヘッダの設定条件について表 4-3 に記載する(但し、全登録ロケーション情報を削除するために用いる“*”に関する条件については 4.1.5 節に記述し、ロケーション情報確認時の扱いについては 4.1.7 節に記述する。)

Contact ヘッダで指定するロケーション情報の userinfo 部は以下に示す理由のとおり、容易に他者に推測されない任意のランダムな英数文字列を 0 節に従う条件で設定することが望ましい⁴。

- DHCP などを用いた IP アドレスを自動取得するような SIP 端末の場合、予期せぬ障害 (停電等) が発生した場合に、ロケーション情報を削除するための REGISTER リクエストを送信できないため、SIP サーバ側では当該ロケーション情報を保持しつづけることになる。このような状況下において、当該 IP アドレスが別の SIP 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 SIP 端末に受信されるべき Initial INVITE リクエストが、新たに同一の IP アドレスを取得した SIP 端末に受信される事態が発生しうるが、Initial INVITE リクエスト受信時に userinfo 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なため

³ ロケーション情報登録動作を行う対象の AoR とは異なる第三者の AoR であった場合、それを許容するか否かは私設総合サービス網交換機(PINX)のポリシーにより異なることに留意する。

⁴ Contact ヘッダで指定するロケーション情報への userinfo 部の設定有無及びその内容については、各私設総合サービス網交換機(PINX)にて本標準を超えた内容が定義されるかもしれない。

表 4-3 / JJ-22.11 REGISTER リクエストの Contact ヘッダのパラメータ値

Parameter	値	種別 (送信側)	補足
displayname	なし	o	
addr-spec	SIP-URI	m	SIP-URI 形式以外は本規定対象外とする
userinfo	文字列	m	任意の文字列を設定する。設定値は JF-IETF-RFC3261[1]に従う。
host	IPv4address 形式	m	Ipv4address 形式以外 (Ipv6reference、hostname 等)は本規定対象外とする。
port	パラメータなし、もしくは数値。	c1	省略した場合には、Initial INVITE リクエストの受信用ポートが 5060 となる。
user-param	パラメータなし、もしくは "phone"か"ip"	o	設定されている場合は SIP サーバによってはパラメータが無視される可能性があることに留意する。
transport-param	パラメータなし	o	UDP 以外は本規定対象外とする。設定されている場合は SIP サーバによってはパラメータが無視される可能性があることに留意する。
maddr-param	パラメータなし	x	
headers	パラメータなし	x	
other URI パラメータ	パラメータなし	x	
q パラメータ (c-p-q)	パラメータなし、もしくは 0~1 までの小数点 3 桁までの数字を表す文字列	o	使用方法については、私設総合サービス網交換機(PINX)により異なる。
expires パラメータ ⁵ (c-p-expires)	パラメータなし、0~4294967295	o	許容する形式以外の場合には SIP サーバによってはメッセージが許容されない、もしくはパラメータが無視されることに留意する。また、パラメータなしの場合には、SIP サーバのポリシーにより値が異なる可能性があることに留意する。 ⁶
contact-extension	パラメータなし	n/a	

c1: 5060 を使用する場合は o、5060 以外を使用する場合は m

4.1.4. 登録

SIP 端末は自身が保持する AoR に対して、ロケーション情報として登録したい情報を Contact ヘッダに設定した REGISTER リクエストを SIP サーバアドレス宛に送信することで登録を行う。なお、Expires パラメータもしくは Expires ヘッダを設定する場合は、その内容は表 4-3 に従う。

また、SIP サーバは、SIP 端末より受信する REGISTER リクエストを元にロケーション情報を登録する。

4.1.5. 削除

SIP 端末は自身が保持する AoR に対して、以前に SIP サーバに登録していたロケーション情報のうち、指定したロケーション情報のみの削除（指定削除）または、全てのロケーション情報の削除（全削除）を行う目的において SIP サーバに削除 REGISTER を送信する。

SIP 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、装置起動時には、起動後に行われる登録動作前に、自身が管理する AoR に対する全ロケーション情報を削除するべきである。なお、その際の削除については、何らかの形で以前に自身が登録したロケーション情報を確

⁵ なお、Expires ヘッダについてもその内容は本規定と同様とする。

⁶ 私設総合サービス網交換機(PINX)により推奨値が指定される場合がある。

実に削除できることを保証できない場合は、全指定削除で行うべきである。

また、SIP サーバは、SIP 端末より受信する削除 REGISTER リクエストを元にロケーション情報を削除する。

4.1.5.1. 指定削除

SIP 端末は自身が保持する AoR にバインディングされる特定のロケーション情報のみを削除する場合は、そのロケーション情報を設定した Contact ヘッダの expires パラメータもしくは Expires ヘッダを 0 に設定した REGISTER リクエストを SIP サーバに送信する。SIP サーバでは当該 AoR に対してバインディングされている全ロケーション情報のうち、Contact ヘッダに指定されたロケーション情報のみがバインディングから削除される。

4.1.5.2. 全指定削除

SIP 端末は自身が保持する AoR にバインディングされる全ロケーション情報を削除する場合は、Contact ヘッダに "*" を設定し、且つ Expires ヘッダに 0 を設定した REGISTER リクエストを SIP サーバに送信する。SIP サーバでは当該 AoR に対してバインディングされている全ロケーション情報が削除される。

4.1.5.3. ロケーション情報削除に関する留意事項

SIP 端末は自身が保持する AoR に対して、自身が SIP サーバに登録したロケーション情報を通常は管理可能であるが、例えば、当該 SIP 端末がアプリケーション終了する場合や、再起動や IP アドレス保持期限などにより自身の IP アドレスが変わる可能性がある動的 IP アドレス割当の環境にて動作している場合においては、SIP 端末が能動的に SIP サーバに対してロケーション情報の削除、更新を行わない限り、SIP サーバにおいて正確なロケーション情報が管理できなくなる可能性があるため、ロケーション情報の削除/更新を行うべきである。

4.1.6. 更新

SIP 端末は自身が保持する AoR に対して以前 SIP サーバに登録していたロケーション情報について、その際に決定した保持期限内にロケーション情報及び保持期限の更新を行うために、SIP サーバに対して、既に登録している当該ロケーション情報を Contact ヘッダに設定した更新 REGISTER リクエストを送信する。なお、Expires パラメータもしくは Expires ヘッダを設定する場合は、その内容は表 4-3 に従う。

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 倍などのロジックで、且つ再送時間を考慮し保持期限の残りが JF-IETF-RFC3261[1]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。

また、SIP サーバは、ロケーション情報登録時に決定した保持期限内にロケーション情報の更新が無い場合は、ロケーション情報の削除を行う。

4.1.7. 確認

SIP 端末は自身が保持する AoR に対して、以前に SIP サーバに登録していたロケーション情報及びその保持期限を確認する必要がある場合には、SIP サーバに対して、Contact ヘッダを設定しない確認 REGISTER リクエストを送信することができる。

4.2. 認証

SIP 端末が SIP サーバに REGISTER リクエストを送信した際に、SIP サーバより 401 (Unauthorized) レス

ポンスを受信した場合には、WWW-Authenticate ヘッダにて指示される認証方式により認証手順を行う。認証方式は HTTP Digest 方式を使用する。

4.2.1. 401 (Unauthorized) レスポンス送受信

SIP 端末が SIP サーバに REGISTER リクエストを送信した際に、SIP サーバより 401 (Unauthorized) レスポンスを受信した場合には、WWW-Authenticate ヘッダにて指示される認証方式により認証手順を行う。WWW-Authenticate ヘッダの扱いを 表 4-4 に記載する。

表 4-4/JJ-22.11 401 (Unauthorized) レスポンスの WWW-Authenticate ヘッダの扱い

ディレクティブ	値	種別 (受信側)	補足
nonce	<nonce>	m	
realm	<realm>	m	realm の文字列。
domain	<domain>	o	domain の文字列。
opaque	<opaque>	m	二重引用符号のみの空文字、もしくは 32 文字以下の任意の文字列
stale	TRUE、もしくは FALSE	m	<p>【TRUE】 送信した REGISTER リクエストに含まれる Authorization ヘッダの nonce パラメータの値が、SIP サーバ管理上、有効期限切れ、もしくは不正 nonce であった場合であるため、401 (Unauthorized) レスポンスで受信した nonce 値で再度認証手順を実行する。</p> <p>【FALSE】 送信した REGISTER リクエストに Authorization ヘッダが含まれていない (即ち新規認証) 場合は、認証手順に従い認証リクエスト (REGISTER) を送信する。Authorization ヘッダが含まれている場合は、Authorization ヘッダの username パラメータに設定された値や、response パラメータが SIP サーバにて不正と判断されたとして、何らかの方法にてユーザに通知する。</p>
algorithm	MD5	o	
qop-options	auth、auth-int	m	
その他パラメータ	-	o	無視をする。アプリケーションにて使用する場合はこの限りでない。

※ 鍵括弧 (“<”及び“>”) で囲まれたものについては、状況/設定に応じて適切な値が SIP レジストラサーバより通知される。

4.2.2. 認証 REGISTER リクエスト送信

SIP 端末が 401 (Unauthorized) レスポンスを受信した後、指定された認証手順によりユーザ名、パスワードを指定した Authorization ヘッダを含んだ REGISTER リクエストを SIP サーバに送信する。Authorization ヘッダの扱いを表 4-5 に記載する。

なお、REGISTER リクエストに設定する Call-ID ヘッダの値は 401 (Unauthorized) レスポンスで受信したものと同値とし、CSeq の値は 1 インクリメントする。

表 4-5 / JJ-22.11 認証リクエスト (REGISTER) にて送信する Authorization ヘッダの扱い

ディレクティブ	値	種別 (送信側)	補足
username	<username>	m	認証に使用するユーザ名を設定する。
nonce	受信した WWW-Authenticate ヘッダからのコピー	m	401 (Unauthorized) レスポンスで受信した値と同一の値を設定する。
realm	受信した WWW-Authenticate ヘッダからのコピー	m	401 (Unauthorized) レスポンスで受信した値と同一の値を設定する。
uri	Request-URI と同値	m	
response	<response>	m	401 (Unauthorized) レスポンスの WWW-Authenticate ヘッダで指定された algorithm でパスワードより算出した値を設定する。
opaque	受信した WWW-Authenticate ヘッダからのコピー	m	401 (Unauthorized) レスポンスで受信した値と同一の値を設定する。
algorithm	MD5	o	401 (Unauthorized) レスポンスで受信した値と同一の値を設定する。
cnonce	端末にて任意に生成した値	m	401 (Unauthorized) レスポンスで受信した WWW-Authenticate ヘッダにて qop-options が設定されている場合にのみ設定する。
nonce-count	認証リクエストの送信回数の 16 進表現	m	401 (Unauthorized) レスポンスで受信した WWW-Authenticate ヘッダにて qop-options が設定されている場合にのみ設定する。
message-qop		m	401 (Unauthorized) レスポンスで受信した WWW-Authenticate ヘッダにて qop-options が設定されている場合にのみ設定する。(*1) 設定する場合は 401 (Unauthorized) レスポンスで受信した値と同一の値を設定する。
その他パラメータ	-	o	設定しない。アプリケーションにて使用する場合はこの限りでない。

(*1) 401 (Unauthorized) レスポンスで受信した WWW-Authenticate ヘッダにて qop-options が設定されていない場合には、message-qop を設定してはいけない。

4.3. 2xx レスポンス送受信

4.3.1. 基本動作

SIP サーバは、SIP 端末より REGISTER リクエスト要求を受信した場合、REGISTER リクエストの登録/削除/更新/確認要求のいずれかのロケーション情報操作を行い、SIP 端末に対して 2xx レスポンスを送信する。

SIP 端末は送信した REGISTER リクエストに対する 2xx レスポンス受信により、REGISTER リクエストで要求した登録/削除/更新/確認のいずれかのロケーション情報登録動作が完了したものと判断する。各それぞれの要求内容での 2xx レスポンス受信時の動作を次節より記載する。

4.3.2. 登録に対する 2xx レスポンス送受信

SIP サーバは、SIP 端末より REGISTER リクエストの登録要求を受信した場合、Contact ヘッダに含まれるロケーション情報を登録し、expires パラメータ、もしくは Expires ヘッダで保持期限 (Z 秒) を指定した 200(OK)レスポンスを送信する。

SIP 端末は SIP サーバより登録完了である 200(OK)レスポンスを受信した場合には、その Contact ヘッダに含まれる自身が追加要求したロケーション情報とそれに対する 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。

SIP 端末が SIP サーバに送信したロケーション情報と、SIP サーバより 200(OK)レスポンスの Contact ヘッダにて受信した登録された URI との比較処理の留意事項については 4.3.6 節にて記載する。

4.3.3. 削除に対する 2xx レスポンス受信

SIP サーバは、SIP 端末より REGISTER リクエストの削除要求を受信した場合、該当するロケーション情報を削除するとともに、SIP 端末に対し 200(OK)レスポンスを送信する。

SIP 端末は SIP サーバより削除完了である 200(OK)レスポンスを受信した場合には、SIP サーバにて当該ロケーション情報が削除されたと判断する。

4.3.4. 更新に対する 2xx レスポンス送受信

SIP サーバは、SIP 端末より REGISTER リクエストの更新要求を受信した場合、Contact ヘッダに含まれる情報を更新し、expires パラメータ、もしくは Expires ヘッダで保持期限（Z秒）を指定した 200(OK)レスポンスを送信する。

SIP 端末は SIP サーバより更新完了である 200(OK)レスポンスを受信した場合には、その Contact ヘッダに含まれる自身が更新要求したロケーション情報とそれに対する 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。

SIP 端末が SIP サーバに送信したロケーション情報と、SIP サーバより 200(OK)レスポンスの Contact ヘッダにて受信した登録された URI との比較処理の留意事項については 4.3.6 節にて記載する。

4.3.5. 確認に対する 2xx レスポンス送受信

SIP サーバは、SIP 端末より Contact ヘッダを設定しない確認 REGISTER リクエストを受信した場合、各ロケーション情報と、それに対する expires パラメータを含む Contact ヘッダ、もしくは保持期限が設定された expires ヘッダを含む 200(OK)レスポンスを送信する。

SIP 端末は SIP サーバより確認完了である 200(OK)レスポンスを受信した場合には、その Contact ヘッダに含まれる各ロケーション情報とそれに対する expires パラメータ、もしくは expires ヘッダで指定された保持期限の検証が可能となる。検証後の動作については本規定外とする。

4.3.6. ロケーション情報の正当性検証における留意事項

追加、更新、削除、確認において、SIP 端末は自身が送信した REGISTER リクエストの Contact ヘッダに含まれるロケーション情報と、SIP サーバからの 200(OK)レスポンスにて受信した Contact ヘッダに含まれるロケーション情報とを比較検証する場合は、SIP サーバが認識しないパラメータについてはロケーション情報に含めて保持しない場合があることに留意し、URI パラメータを比較対照とすべきでない。アプリケーションにて使用するパラメータのように特別に必要とする場合はこの限りではない。

4.4. 3xx/4xx/5xx/6xx レスポンス送受信

4.4.1. 基本動作

SIP サーバは、SIP 端末より REGISTER リクエスト要求を受信し各種処理を実施する際に、種々の条件により処理ができない場合、表 13-4 に従ったレスポンスを SIP 端末へ送信する。

SIP 端末は受信したレスポンスを表 13-4 に従い処理する。必要であれば 4.5.1 節に従ったリトライを行う。

4.5. 輻輳抑制への考慮

4.5.1. ロケーション情報登録動作失敗時のリトライに関する留意事項

SIP サーバは、SIP 端末より REGISTER リクエスト要求を受信した時、サーバが輻輳状態等、私設総合サービス網交換機(PINX)に何らかの問題が発生している場合は、さらなる輻輳を避ける目的で 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[1]では 404(Not Found)レスポンス, 413(Request Entity Too Large)レスポンス, 480(Temporarily 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) を送信する。

SIP 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を受信する可能性がある。この場合、SIP サーバが輻輳状態等、私設総合サービス網交換機(PINX)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リクエスト再送を行うことが望ましい (指定時間後に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は、同様の理由により、適切な時間が経過後にリクエスト再送を行うことが望ましい (但し、401 (Unauthorized) レスポンスの受信時を除く)。

また、SIP アプリケーションレイヤより下位においてエラーとなった場合 (ICMP エラー通知やメッセージ再送タイムアウト等) も同様に、適切な時間が経過後にロケーション情報登録動作のリトライを行うことが望ましい。

4.5.2. 複数 REGISTER における留意事項

ロケーション情報登録動作による SIP サーバの不必要な輻輳を防止するために、例えば 1 つの SIP 端末が複数の AoR を管理している場合や、複数のロケーション情報を SIP サーバに登録する必要がある場合において、複数の REGISTER リクエストを一度に送信する場合などには、SIP 端末では短い時間に連続した REGISTER リクエストの送信を制限することを考慮するべきである。

また、Authorization ヘッダを含んだ REGISTER リクエストに対して、SIP サーバから 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 REGISTER リクエストの再送を行わず、不必要な REGISTER リクエストの送信を避けるようにするべきである。

4.5.3. 一時的障害発生時における留意事項

SIP 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、SIP 端末自身のロケーション情報の変更有無や、登録保持期限に関わらず、すみやかにバインディングの更新もしくはバインディングの確認 (登録が削除されていた場合には引き続き登録処理) を行うような考慮をすべきである。

但し、アクセスネットワークにおける広域障害の一斉復旧による一斉のロケーション情報登録動作による SIP サーバの処理輻輳や、一時的障害の断続的な繰り返しによるロケーション情報登録動作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。

5. Initial INVITE リクエスト送信

5.1. Initial INVITE リクエスト送信

5.1.1. 基本動作

SIP 端末は、ユーザからの発呼要求にともない、SIP サーバアドレスを宛先とする Initial INVITE リクエストを送信する。また、SIP サーバは発呼側 SIP 端末からの発呼要求にともない、着呼側 SIP 端末アドレスを宛先とする Initial INVITE リクエストを送信する。なお、以前の呼に関する SIP 上のトランザクションまたはダイアログが正常に終了していない状態においてユーザからの発呼要求があった場合についても、現在処理中の SIP シーケンスとは独立して Initial INVITE リクエストの送信処理を可能とする方が望ましい。

Initial INVITE リクエストにはオファーを含める必要があるが、オプションとしてサーバから着信端末への Initial INVITE にはオファーを含めない方式でも良い。また、送信した Initial INVITE リクエストに対して 407 (Proxy Authentication Required) レスポンスを受信した場合には、5.1.4 節に従って認証処理を行う必要がある。PINX は B2BUA で接続されるため、401(Unauthorized)を使う場合もある。この場合、端末は REGISTER での認証動作と同じく 4.2 節に記載されている WWW-Authenticate ヘッダに従って認証手順に対応できる事が望ましい。

option-tag で規定される SIP 拡張機能の利用については、Supported ヘッダに実装する拡張機能の文字列 ("100rel" など) を設定する。Require ヘッダや、Proxy-Require ヘッダを用いた場合には、全てまたは一部の呼接続パターンにおいて呼接続が不可能となる原因となりうることに留意する必要がある。本規定では、"100rel" 及び、"timer" の規定を行っており、それぞれの拡張機能用法の詳細は、それぞれ 8 節及び 9 節に記載する。

5.1.2. Request-URI

Initial INVITE リクエストの Request-URI は SIP URI 形式で構成する。なお、SIPS URI などのその他の URI 形式での Request-URI の構成は本規定の範囲を超える。

Request-URI は以下のとおり構成する。

```
Request-uri      =      "sip:" user"@ " host [ :port ] [ uri-parameters ]
```

表 5-1/JJ-22.11 Initial INVITE リクエスト送信時の Request-URI 構成要素

構成要素	値	種別 (送信側)	備考
user	DIGIT	m	一般的にはユーザダイヤル番号に相当する文字列。
host	Ipv4address、もしくは hostname 形式	m	一般的には SIP サーバアドレス、又は、SIP UA アドレス (AoR の host 文字列とは異なるかもしれない) を用いることが想定される
port		c1	
uri-parameters		o	
c1:5060 を使用する場合は”o”、5060 以外を使用する場合は”m” ⁷			

5.1.3. AoR (From ヘッダ)

From ヘッダの addr-spec には、AoR または匿名 URI のいずれかを設定する。AoR と匿名 URI の選択については、12.1 節に記載する。

AoR の user 部は 13.2.1 節に示す条件で任意の文字列⁸を設定可能とする。

5.1.4. 認証

SIP 端末が SIP サーバに Initial INVITE リクエストを送信した場合、SIP サーバは発呼側 SIP 端末を認証しても良い。認証の結果、Initial INVITE リクエストを拒否する場合は、SIP サーバより 407 (Proxy Authentication Required) レスポンスを受信した場合には、Proxy-Authenticate ヘッダにて指示される認証方式により認証手順を行う。認証方式は HTTP Digest 方式を使用する。

5.1.4.1. 407 (Proxy Authentication Required) レスポンス受信

SIP 端末が SIP サーバに Initial INVITE リクエストを送信した際に、SIP サーバより 407 (Proxy Authentication Required) レスポンスを受信した場合には、Proxy-Authenticate ヘッダにて指示される認証方式により認証手順を行う。受信した Proxy-Authenticate ヘッダの扱いを表 5-2 に記載する。

⁷ 使用するポート番号を私設総合サービス網交換機(PINX)により指定されるかもしれない。

⁸ AoR の user 部は私設総合サービス網交換機(PINX)のポリシーにより、telephone-subscriber とは限らないことに留意する必要がある。

表 5-2/JJ-22.11 407(Proxy Authentication Required)レスポンスにて受信する Proxy-Authenticate ヘッダの扱い

ディレクティブ	値	種別 (受信側)	補足
nonce	<nonce>	m	
realm	<realm>	m	realm の文字列。
domain	<domain>	o	domain の文字列。
opaque	<opaque>	m	二重引用符号のみの空文字、もしくは 32 文字以下の任意の文字列
stale	TRUE、もしくは FALSE	m	<p>【TRUE】 送信した Initial INVITE リクエストに含まれる Proxy-Authentication ヘッダの nonce パラメータの値が、SIP サーバ管理上、有効期限切れ、もしくは不正 nonce であった場合であるため、407 で受信した nonce 値で再度認証手順を実行する。</p> <p>【FALSE】 送信した Initial INVITE リクエストに Proxy-Authentication ヘッダが含まれていない（即ち新規認証）場合は、認証手順に従い認証 REGISTER リクエストを送信する。Proxy-Authentication ヘッダが含まれている場合は、Proxy-Authentication ヘッダの username パラメータに設定された値や、response パラメータが SIP サーバにて不正と判断されたとして、何らかの方法にてユーザに通知する。</p>
algorithm	MD5	o	
qop-options	auth、auth-int	m	
その他パラメータ	-	o	無視をする。アプリケーションにて使用する場合はこの限りでない。

※ 鍵括弧 (“<”及び“>”) で囲まれたものについては、状況/設定に応じて適切な値が SIP サーバより通知される。

5.1.4.2. 認証 Initial INVITE リクエスト送信

407(Proxy Authentication Required)レスポンスを受信した後、指定された認証手順によりユーザ名、パスワードを指定した Proxy-AuthORIZATION ヘッダを含んだ Initial INVITE リクエストを SIP サーバに送信する。Proxy-AuthORIZATION ヘッダの扱いを表 5-3 に記載する。

なお、認証 Initial INVITE リクエストに設定する Call-ID ヘッダの値は 407(Proxy Authentication Required)レスポンスで受信したものと同値とし、CSeq の値は 1 インクリメントする。

表 5-3 / JJ-22.11 認証 Initial INVITE にて送信する Proxy-Authorization ヘッダの扱い

ディレクティブ	値	種別 (送信側)	補足
username	<username>	m	認証に使用するユーザ名を設定する。
nonce	受信した Proxy-Authenticate ヘッダからのコピー	m	407(Proxy Authentication Required)レスポンスで受信した値と同一の値を設定する。
realm	受信した Proxy-Authenticate ヘッダからのコピー	m	407(Proxy Authentication Required)レスポンスで受信した値と同一の値を設定する。
uri	Request-URI と同値	m	
response	<response>	m	407(Proxy Authentication Required)レスポンスの Proxy-Authenticate ヘッダで指定された algorithm でパスワードより算出した値を設定する。
opaque	受信した Proxy-Authenticate ヘッダからのコピー	m	407(Proxy Authentication Required)レスポンスで受信した値と同一の値を設定する。
algorithm	MD5	o	407(Proxy Authentication Required)レスポンスで受信した値と同一の値を設定する。
cnonce	端末にて任意に生成した値	m	407(Proxy Authentication Required)レスポンスで受信した Proxy-Authenticate ヘッダにて qop-options が設定されている場合にのみ設定する。
nonce-count	認証リクエストの送信回数の16進表現	m	407(Proxy Authentication Required)レスポンスで受信した Proxy-Authenticate ヘッダにて qop-options が設定されている場合にのみ設定する。
message-qop		m	407(Proxy Authentication Required)レスポンスで受信した Proxy-Authenticate ヘッダにて qop-options が設定されている場合にのみ設定する。(*1) 設定する場合は 407(Proxy Authentication Required)レスポンスで受信した値と同一の値を設定する。
その他パラメータ	-	o	設定しない。アプリケーションにて使用する場合はこの限りでない。

(*1) 407(Proxy Authentication Required)レスポンスで受信した Proxy-Authenticate ヘッダにて qop-options が設定されていない場合には、message-qop を設定してはいけない。

5.2. 1xx レスポンス受信

5.2.1. 基本動作

送信した Initial INVITE リクエストに対して最終レスポンスを受信するまでの間に、1つも 1xx レスポンスを受信しない場合、1つもしくは複数の 1xx レスポンスを受信する場合のいずれについても受信した SIP レスポンスに応じた処理を行う。また、1xx レスポンスを受信した場合、Initial INVITE リクエストの再送を停止し、最終レスポンスの受信を待たなければならない。

1xx レスポンスに SDP が含まれている場合及び、180(Ringing)レスポンスの受信との関係については、5.2.2 節に記載する。

To ヘッダに tag パラメータが設定された 1xx (≠100(Trying)) レスポンスを受信した場合には、Early ダイ

アログを確立する。To ヘッダに tag パラメータが含まれてない場合においても受信した SIP レスポンス信号に応じた処理を行う必要がある。

また、100(Trying)レスポンスを除く 1xx レスポンスには送信した Initial INVITE リクエストの Supported ヘッダの内容に応じて、Require ヘッダが設定されている場合がある。ここでは、Supported ヘッダに設定した option-tag は必ずしも Require ヘッダに設定されているとは限らず、また、Require ヘッダそのものが存在しないかもしれないことに留意する必要がある、その場合には当該の SIP 拡張機能を使わずにセッション確立できなくてはならない。本規定では”100rel”の規定を行っており、その拡張機能用法の詳細は 8 節に記載する。

5.2.2. 呼出中音の再生と Early メディア

5.2.2.1. 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 (≠100(Trying)) 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、5.2.2.2 節に従いメディアパスを接続して着側からの音源を再生しなければならない。

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 を含む 1xx レスポンスを受信した場合には、5.2.2.2 節に従いメディアパスを接続して着側からの音源を再生しなければならない。

5.2.2.2. Early メディア

5.2.2.2.1. 基本動作

SIP 端末は SDP が設定された 1xx (≠100(Trying)) レスポンスを受信した場合にはそのレスポンスが 100rel 拡張機能の動作有無に関わらずアンサーと解釈し、パスを接続することにより Early メディアを確立できないなければならない。これは全ての 1xx (≠100(Trying)) レスポンスが信頼性を持って転送されるわけではない (私設総合サービス網交換機(PINX)が転送する全ての 1xx (≠100(Trying)) レスポンスに、100rel 拡張機能が動作されるわけではない) ことに留意し、最初に受信した SDP を含む 1xx (≠100(Trying)) レスポンス (当該レスポンスが信頼性を持つ持たないに関わらず) の SDP をアンサーと解釈してセッション確立の処理を行い両方向の音声パスを接続する。

SDP が設定された 1xx (≠100(Trying)) レスポンスを受信した場合には、以前と異なる SDP を含む 1xx (≠100(Trying)) レスポンスを受信した場合には、受信メディアの張り替え処理を行っても良い。

5.2.2.2.2. UPDATE メソッドによるセッション変更

Initial INVITE リクエストの Allow ヘッダに UPDATE を含め、且つ、100rel 拡張機能が動作する信頼性を持った 1xx (≠100(Trying)) レスポンスによりアンサーを受信した (最初のオファー/アンサーが完了後) 場合においては、最終レスポンス受信までに着側からのオファーを含む UPDATE リクエストを受信する可能性を考慮しなければならない。つまり、UPDATE メソッドによる着側からのオファーで指定されたセッション内容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セッション内容の変更を行い、指定されたセッションの変更が不可能な場合には 488 (Not Acceptable Here) 等のレスポンスを返送する必要がある。但し、488 (Not Acceptable Here) 等のレスポンスを返信する際においては、既存のセッションの終了処理を行わず、その扱いはメディア変更要求をした SIP UA 側の判断に委ねることとする。

5.2.3. 複数ダイアログとメディアの管理

SIP サーバは、自身が Initial INVITE リクエストをフォーキングした場合、複数の着側 SIP 端末からの 1xx(≠100(Trying))レスポンスを受信する可能性がある。よって SIP サーバは UAC として、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することが望ましい。

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することが望ましい。

上記を考慮した SIP サーバの処理として、最低限の実装範囲と実装が望ましい範囲について表 5-4 に示す。

表 5-4 / JJ-22.11 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	・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)

5.3. 2xx レスポンス受信

5.3.1. 基本動作

SIP 端末は最初に受信した 2xx レスポンスにより confirmed ダイアログを確立する。その 2xx レスポンスに To ヘッダに tag が含まれていない場合には To ヘッダの tag を null として扱い confirmed ダイアログを確立できなければならない（過去に To ヘッダに tag を含んだ 1xx(≠100(Trying))レスポンスを受信していた場合には 5.3.2 節に従う）。

SIP 端末が 2xx レスポンスを受信した際には、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ものとする。

5.3.2. 複数ダイアログとメディアの管理

SIP サーバは、自身が Initial INVITE リクエストをフォーキングした場合、複数の着側 SIP UA からの 2xx レスポンスを受信する可能性がある。よって SIP サーバは UAC として、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することが望ましい。

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することが望ましい。

上記を考慮した発側 SIP 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表 5-5 に示す。

表 5-5 / JJ-22.11 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	<ul style="list-style-type: none"> Confirmed ダイアログの内容にセッションを変更する。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	<ul style="list-style-type: none"> 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)

5.4. 3xx レスポンス受信

5.4.1. 基本動作

3xx レスポンスを受信した場合には、そのレスポンスが自身の属する私設総合サービス網交換機 (PINX)からのものであること、かつセキュリティ上のリスクがないことが確認されない限り、メッセージに含まれる Contact ヘッダで指定される宛先へ Initial INVITE リクエストを転送してはならず、3xx レスポンスを受信と同時に発呼を停止しユーザに Busy Tone などで発信不可である旨を通知する。

5.4.2. ACK リクエスト送信

JF-IETF-RFC3261[1]に従い通常のエラーレスポンスに対する ACK リクエスト送信と同様の処理を行う。

5.5. 4xx/5xx/6xx レスポンス受信

5.5.1. 基本動作

SIP サーバ及び、SIP 端末は受信したレスポンスを表 13-2 に従い処理する。受信したレスポンスコード及びリーズンプレーズ、ヘッダ類の情報を上位のアプリケーションに渡し、JF-IETF-RFC3261[1]に従い ACK リクエストを返送して Initial INVITE リクエストのトランザクションを終了する。

- ・ 413 (Request Entity Too Large) レスポンス、415 (Unsupported Media Type) レスポンス、416 (Unsupported URI Scheme) レスポンス、420 (Bad Extension) レスポンスの各レスポンスを受信した場合には、JF-IETF-RFC3261[1] 8.1.3.5 節に従いリクエストの内容を修正してリトライする機能を有していてもよい。
- ・ 422 (Session Interval Too Small) レスポンスを受信した場合には、9 節の動作規定に従う。

5.5.2. ACK リクエスト送信

JF-IETF-RFC3261[1]に従い通常のエラーレスポンスに対する ACK リクエスト送信と同様の処理を行う。

5.6. 途中放棄

5.6.1. CANCEL リクエスト送信

SIP サーバ及び、SIP 端末は 1xx レスポンス受信後最終レスポンス未受信状態において、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)や、呼出中タイムアウトなどにより、途中放棄する場合には Initial INVITE リクエストに対する CANCEL リクエストを JF-IETF-RFC3261[1]に従って送信する。

なお、Initial INVITE リクエストに対する 1xx レスポンス未受信の状態において、ユーザリソース側での当該呼に対する途中放棄を検出した場合は JF-IETF-RFC3261[1]上 CANCEL リクエストを送出してはならない為、Initial INVITE の再送処理を停止するが、トランザクションタイムアウトまで Initial INVITE トランザクションを保持し、その間に INVITE リクエストに対する 1xx レスポンスを受信した場合は、その後

CANCEL リクエストを送信し、INVITE リクエストに対するエラーレスポンスを受信した場合は 5.5 節に従い処理を行う。また、INVITE リクエストに対する 2xx レスポンスを受信した場合は、5.3 節に従い処理を行う。

5.6.2. 信号／処理衝突に関する留意事項

CANCEL リクエスト送信後、当該 Initial INVITE リクエストに対する 2xx レスポンスを受信した場合は、SIP サーバ及び、SIP 端末は ACK リクエストを送信し、ダイアログを確立させた後、BYE リクエストを送出することにより当該ダイアログを終了させる必要がある。

SIP メッセージ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保持が考えられるが、いずれの場合においても、新規の発着呼にともなう新たな Initial INVITE リクエストの送受信を並行して処理可能とする方が望ましい。

5.7. 留意事項

5.7.1. 輻輳制御への考慮

SIP 端末 (SIP サーバ) からの INVITE リクエスト送信による SIP サーバ (SIP 端末) の不必要な輻輳を防止するために、SIP 端末 (SIP サーバ) では短い時間に連続したリクエストの送信を制限する機能を持つべきである。

また、Proxy-Authenticate ヘッダを含んだ SIP サーバからの 407 (Proxy Authentication Required) レスポンスに対して、Proxy-Authenticate ヘッダの stale パラメータが TRUE であった場合、またはこれまでに受信していない 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再送するべきではない。

5.7.2. リクエストの Contact ヘッダの値

INVITE リクエストで設定する Contact ヘッダの値である local target host は、そのダイアログ内における自身宛リクエストの宛先であるため、第三者に容易に推測できないユニークな userinfo 部を生成することが望ましい。また、当該 SIP 端末がロケーション情報登録時に、REGISTER リクエストに含めた Contact ヘッダの値とは userinfo 部が異なった値とすることが望ましい。但し、同一ダイアログ内における後続のトランザクションで値を変更しない。

なお、SIP 端末が期待するダイアログ内における受信リクエストの Request-URI は、特別な理由がない限り期待する値と異なる Request-URI を含むリクエストは破棄されるべきである。

5.7.3. INVITE リクエストのリトライ

SIP サーバは受信した INVITE 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を返送する可能性がある。この場合、私設総合サービス網交換機(PINX)の処理輻輳等、私設総合サービス網交換機(PINX)に何らかの問題が発生している可能性があるため、Retry - Afterヘッダによって指定された時間内には同じ Request-URI に対する INVITE リクエストの送信をリトライしないようにすべきである。

6. Initial INVITE リクエスト受信

6.1. Initial INVITE リクエスト受信

6.1.1. 基本動作

SIP サーバ及び、SIP 端末は To ヘッダに tag パラメータのない INVITE リクエストを受信した場合、Initial INVITE リクエストの受信と判断する。当該 Initial INVITE リクエストが 6.1.2 節で記載する Request-URI のチ

チェックにより自信宛と判断された場合、100(Trying)レスポンスを返信し着信処理を行う。

なお、以前の呼に関する SIP 上のトランザクションまたはダイアログが正常に終了していない状態において Initial INVITE リクエストを受信した場合についても、現在処理中の SIP シーケンスとは独立して Initial INVITE リクエストの受信処理を可能とする方が望ましい。

6.1.2. Request-URI

SIP サーバは、自身が認識しているロケーション情報と、以下に示す条件により比較することにより、同値と判断される Request-URI であった場合にのみ、正常に処理すべき着信呼と判断するのが望ましい。

SIP 端末は受信した Initial INVITE リクエストの Request-URI を、自身がロケーション情報登録動作時に REGISTER リクエストの Contact ヘッダに指定したロケーション情報と、以下に示す条件により比較することにより、同値と判断される Request-URI であった場合にのみ、正常に処理すべき着信呼と判断するのが望ましい。

- ロケーション情報登録動作時に SIP 端末が設定した Contact ヘッダの URI の userinfo 部及び host 部と同値であること。
- SIP サーバが認識しない URI パラメータについてはロケーション情報に含めて保持しない場合があることに留意し、URI パラメータを比較対照とするべきでない。
- hostport において port 番号を指定していたとしても、Initial INVITE リクエストの Request-URI にその port が hostport に指定されるとは限らないため、Request-URI の hostport にて指定される port の照合は行うべきでない。

6.2. 1xx レスポンス送信

6.2.1. 基本動作

Initial INVITE リクエストの受信後すぐに 1xx レスポンス(≠100(Trying))または、最終レスポンスを送信できない場合、不要な Initial INVITE リクエストの再送を防ぐために、100(Trying)レスポンスを送信すべきである。

100(Trying)レスポンスを除く 1xx レスポンスを送信する場合には、0 節にもとづく tag パラメータを生成し、To ヘッダに付与することにより、Early ダイアログを確立させなければならない。また、引き続き 1xx レスポンスを送信する場合、ここで生成したものと同値な tag パラメータを To ヘッダに付与しなければならない。

100(Trying)レスポンスを除く 1 または複数の 1xx レスポンスを送信する場合、受信した Initial INVITE リクエストの Supported ヘッダに含まれる option-tag の SIP 拡張機能に対応している場合、送信する全ての 1xx レスポンスの Require ヘッダに当該 option-tag を設定する。なお、受信した Initial INVITE リクエストに Supported ヘッダそのものが存在しない場合や、対応している option-tag が Supported ヘッダに設定されていない場合には、上記 Require ヘッダを設定してはならず、当該の SIP 拡張機能を用いずにセッション確立できなくてはならない。本規定では”100rel”の規定を行っており、その SIP 拡張機能の詳細は 8 章に記載する。

6.2.2. 180(Ringing)レスポンス

180(Ringing)レスポンスについては、5.2.2 節に記載するとおり、発呼側の SIP 端末が受信した場合に特別な処理を行うことを考慮し、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ケンスを前提としている場合、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。

6.3. 2xx レスポンス送信

6.3.1. 基本動作

ユーザからの応答時に 2xx レスポンスを送信し、confirmed ダイアログを確立するものとする。early メディアを確立していない場合には、2xx レスポンスにアンサーを含めるものとする。

受信した Initial INVITE リクエストの Supported ヘッダに含まれる option-tag の SIP 拡張機能に対応している場合、送信する 2xx レスポンスの Require ヘッダにセッション確立後に使用する SIP 拡張機能に対応する当該 option-tag を設定する。なお、受信した Initial INVITE リクエストに Supported ヘッダそのものが存在しない場合や、対応している option-tag が Supported ヘッダに設定されていない場合には、上記 Require ヘッダを設定してはならず、当該の SIP 拡張機能を用いずにセッション確立できなくてはならない。本規定では”セッションタイマ”の規定を行っており、その拡張機能用法の詳細は 9 章に記載する。

6.4. 3xx レスポンス送信

SIP 端末は、3xx レスポンスはセキュリティ上のリスクがないことが確認されない限り、送信してはならない。

6.5. 4xx/5xx/6xx レスポンス送信

SIP サーバ及び、SIP 端末は、ユーザ話中や、空き回線なしなどの何らかの理由により受信した Initial INVITE リクエストに対するセッション確立処理が継続できないと判断した場合には、4xx/5xx/6xx レスポンスのうち、適切なレスポンスコードのエラーレスポンスを送信する。

エラーレスポンス送信後、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、SIP 端末は Initial INVITE リクエスト送受信を並行して処理を可能とする方が望ましい。

6.6. エラーレスポンスに対する ACK リクエスト受信

SIP サーバ及び、SIP 端末はエラーレスポンス送信後、その応答である ACK リクエストを受信するが、その際のトランザクションマッチングの 1 つとして、ACK リクエストの Request-URI を Initial INVITE の Request-URI と比較を行う場合は、信号の認識性・接続性を考慮し URI パラメータを対象としないことが望ましい。

6.7. 途中放棄

受信した Initial INVITE リクエストに対して、1xx レスポンスを送信後から、最終レスポンス送信に対応する ACK リクエストを受信するまでの間は、Initial INVITE リクエストに対する CANCEL リクエストもしくは、確立させた Early ダイアログに対応する BYE リクエストを受信する可能性がある（発側 SIP UA からの途中放棄）。

6.7.1. CANCEL/BYE リクエスト受信

CANCEL リクエストもしくは BYE リクエスト受信時点において、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場合は、受信した CANCEL リクエストに対する 2xx レスポンス、もしくは

BYE リクエストに対応する 2xx レスポンスを返信するとともに、Initial INVITE リクエストに対応する 487(Request Terminated)レスポンスを送信し、ユーザリソース呼出の停止／解放処理を行う。既に 1xx(≠100(Trying))レスポンスの送信により Early ダイアログを確立していた場合、ここで送信する SIP レスポンスメッセージには、それと同一の To-tag パラメータを設定しなければならない。なお、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を可能とする方が望ましい。

6.7.2. 信号／処理衝突に関する留意事項

SIP サーバ及び、着側 SIP 端末は 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、SIP 上は発側 SIP UA からの ACK リクエスト、及びその後の BYE リクエストの受信待ちとなるが、応答した着側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着側 SIP 端末の場合には 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を可能とする方が望ましい。

6.8. その他留意事項

6.8.1. レスポンスの Contact ヘッダの値

INVITE リクエストに対する 1xx(≠100(Trying))及び 2xx レスポンスで設定する Contact ヘッダの値である local target host は、そのダイアログ内における自身宛リクエストの宛先であるため、第三者に容易に推測できないユニークな userinfo 部を生成することが望ましい。また、当該 SIP 端末がロケーション情報登録時に REGISTER リクエストに含めた Contact ヘッダの値とは userinfo 部が異なった値とすることが望ましい。但し、同一ダイアログ内における後続のトランザクションで値を変更しない。

なお、SIP サーバ及び、SIP 端末が期待するダイアログ内における受信リクエストの Request-URI は、特別な理由がない限り期待する値と異なる Request-URI を含むリクエストは破棄されるべきである。

7. リモートターゲット

ダイアログ中に送信する SIP リクエストメッセージの構成における、リモートターゲットについて考慮が必要な事項について以下に記載する。

7.1. 基本動作

SIP 端末は、SIP 端末がダイアログ中に送信する SIP リクエストメッセージの Request-URI は以下のとおり構成する。

-Request-URI にはリモートターゲットを設定する。

上記のとおり構成した SIP リクエストメッセージを隣接ルート(一番上位に設定した Route ヘッダ)を宛先として送信する。

7.2. 発呼側リモートターゲット

Initial INVITE リクエストで接続相手の SIP UA から受信する Contact ヘッダの URI と同値とする。ダイアログ確立後に異なる URI を受信した場合は、当該ダイアログのリモートターゲットを新しく受信したものに上書きを行う。

7.3. 着呼側リモートターゲット

1xx レスポンス、UPDATE リクエスト、及び 200(OK)レスポンスで接続相手の SIP UA から受信する Contact ヘッダの URI と同値とする。ダイアログ確立後に異なる URI を受信した場合は、当該ダイアログのリモートターゲットを新しく受信したものに上書きを行う。

8. 100rel 拡張機能

SIP 端末は、1xx レスポンスの送達保証を行うために、JF-IETF-RFC3262[2]で規定される 100rel の拡張機能を実装していることが望ましい。また、設定により、本機能の利用を停止することが可能であることが必要である⁹。

8.1. 能力交換

発呼側 SIP 端末は Initial 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着側 SIP UA に伝え、実際の利用要否は着側 SIP UA に委ねる (Initial INVITE リクエストに Require ヘッダを設定してはいけない)。

着呼側 SIP 端末は受信した Initial INVITE リクエストの Supported ヘッダに 100rel が設定されている場合のみ、100rel 拡張機能動作を行うことが可能である。

8.2. 1xx レスポンス送信

着呼側 SIP 端末は、受信した Initial INVITE リクエストの Supported ヘッダに 100rel が設定されている場合にも、送信する全ての 1xx レスポンス (≠100(Trying)) の Require ヘッダに 100rel を設定するとともに、RSeq ヘッダを設定する。1xx レスポンス (≠100(Trying)) に対応する PRACK リクエストを受信するまで、JF-IETF-RFC3262[2]にしたがい再送を行う。PRACK リクエストを受信した場合、RAck ヘッダの method、CSeq-num、response-num の検証を行ない、送信した 1xx レスポンス (≠100(Trying)) に対する PRACK リクエストであることを確認できた場合は PRACK リクエストに対する 200(OK)レスポンスを送信する。1xx レスポンス (≠100(Trying)) 再送タイマがタイムアウトするまでに PRACK リクエストを受信しない場合は、Initial INVITE リクエストに対して 500(Server Internal Error)レスポンスを送信し、Initial INVITE リクエストトランザクションを終了させる。

着呼側 SIP 端末が複数の 1xx レスポンス (≠100(Trying)) を送信する必要がある場合においては、先に送信した 1xx レスポンス (≠100(Trying)) に対する PRACK リクエストを受信までは、次の 1xx レスポンス (≠100(Trying)) は送信するべきではない。

8.3. PRACK リクエスト送信

Require ヘッダに 100rel が設定された 1xx レスポンス (≠100(Trying)) を発呼側 SIP 端末が受信した場合、RAck ヘッダを設定した PRACK リクエストを送信する。PRACK リクエストを送信した発呼側 SIP 端末は、最終レスポンスを受信するまで JF-IETF-RFC3262[2]にしたがい PRACK リクエストの再送を行う。なお、PRACK リクエストに対する最終レスポンスを受信する前に RSeq がインクリメントされた 1xx レスポンス (≠100(Trying)) を受信時は新たな 1xx レスポンスとして 100rel 拡張機能動作を実施する。

9. セッションタイマ拡張機能

準正常時のセッション解放の検出を行うために JF-IETF-RFC4028[13]で規定されるセッションタイマ拡張機能を実装していることが必要である。また、設定により、本機能の利用を停止することが可能であるこ

⁹ 本拡張機能は接続を行う私設総合サービス網交換機(PINX)において機能の使用停止が指示される場合がある。

とが必要である¹⁰。

9.1. 能力交換

発呼側 SIP 端末は Initial INVITE 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着側 SIP UA に伝え、実際の利用要否は着側 SIP UA に委ねる (Initial INVITE リクエストに Require ヘッダを設定してはいけない)。セッションタイマ起動有無については、200(OK)レスポンスの Require ヘッダへの”timer”設定有無により判断を行い、受信しない場合はセッションタイマを起動しない。着呼側 SIP 端末は受信した Initial INVITE リクエストに Session-Expires ヘッダが設定されている場合にセッションタイマ起動を行う。なお、Supported ヘッダに timer が設定されている場合にのみ、送信する 200(OK)レスポンスの Require ヘッダに timer を設定する。

上記は、セッションリフレッシュリクエストのトランザクションにおいても同様とする。

9.2. セッションリフレッシュリクエスト

セッションリフレッシュリクエストとして送信する SIP リクエストとしては、re-INVITE リクエストもしくは UPDATE リクエストを用いる。SIP 端末の実装としては、UPDATE リクエストの送受信を行える機能を実装していることが必要である。具体的には自身が送信する Allow ヘッダに”UPDATE”を設定する能力を有すること、及び自身がリフレッシャーとなる場合において、9.2.1 節及び 9.2.2 節に記載するセッション確立時の接続相手 SIP UA との間での Allow ヘッダによる能力交換にもとづくリフレッシュ動作が可能であることが必要である。また、設定により、セッションリフレッシュリクエストとして UPDATE リクエストを用いずに、re INVITE リクエストのみを用いるような能力交換を可能とすることもあわせて必要である¹¹。

9.2.1. re-INVITE リクエスト

セッション確立時に接続相手の SIP UA との間で Allow ヘッダの交換により、UPDATE リクエストを利用できない場合 (Initial INVITE リクエストまたは、200(OK)レスポンスにおける Allow ヘッダに UPDATE が含まれていない場合) は re-INVITE リクエストを利用する。re-INVITE リクエスト及び 200(OK)レスポンスには SDP の設定を行わなければならない。

9.2.2. UPDATE リクエスト

セッション確立時に接続相手の SIP UA との間で Allow ヘッダの交換により、UPDATE リクエストを利用できる場合 (Initial INVITE リクエストまたは、200(OK)レスポンスにおける Allow ヘッダに UPDATE が含まれている場合) は UPDATE リクエストを利用する。セッションリフレッシュを目的とした UPDATE リクエスト/レスポンスにおいては、SDP の設定を行わないことが推奨される。なお、接続相手の SIP UA から受信し Allow ヘッダに UPDATE が設定されていた場合においても、re-INVITE を用いたセッションリフレッシュリクエストを受信することについても考慮が必要である。

¹⁰ 本拡張機能は接続を行う私設総合サービス網交換機(PINX)において機能の使用停止が指示される場合がある。機能停止が指定される場合、本章に記載された動作を SIP 端末は行わない。

¹¹ UPDATE リクエストの使用は接続を行う私設総合サービス網交換機(PINX)において使用停止が指示される場合がある。

9.3. リフレッシャー決定

9.3.1. セッション確立時

9.3.1.1. 発呼側 SIP 端末

発呼側 SIP 端末は Initial INVITE リクエストの Session-Expires ヘッダには `refresher` パラメータを設定せず、リフレッシャーの選択を着側 SIP UA の処理に任せることが推奨される。受信した 200(OK)レスポンスの Session-Expires ヘッダに `refresher=uac` と設定されていれば、次回セッションリフレッシュリクエストを送信する立場（リフレッシャー）と認識し、`refresher=uas` と設定されていれば、セッションタイム満了までにセッションリフレッシュリクエストの受信を待つ立場（非リフレッシャー）と認識する。なお、発呼側 SIP 端末が Initial-INVITE の Session-Expires ヘッダに `refresher` パラメータを設定する場合には、200(OK)レスポンスで受信する Session-Expires ヘッダの `refresher` パラメータで受信する値が異なるケースにおいて受信した内容で動作する必要がある。

9.3.1.2. 着呼側 SIP 端末

受信した Initial INVITE リクエストの Session-Expires ヘッダに `refresher=uas` と設定されていれば、次回セッションリフレッシュリクエストを送信する立場（リフレッシャー）と認識し、`refresher=uac` と設定されていれば、セッションタイム満了までにセッションリフレッシュリクエストの受信を待つ立場（非リフレッシャー）と認識する。送信する 200(OK)レスポンスの Session-Expires ヘッダには受信した `refresher` パラメータの値をそのままコピーする。

着呼側 SIP 端末が受信した Initial INVITE リクエストに Supported ヘッダが存在し且つ”timer”が含まれている場合において、Session-Expires ヘッダに `refresher` パラメータが存在しない場合は、送信する 200(OK)レスポンスの Session-Expires ヘッダに `refresher=uas` もしくは `uac` と設定する。

着呼側 SIP 端末が受信した Initial INVITE リクエストに Supported ヘッダが存在しないまたは”timer”が含まれていない場合において、`refresher` パラメータのない Session-Expires ヘッダを受信した場合においては着呼側 SIP 端末が送信する 200(OK)レスポンスの Session-Expires ヘッダには `refresher=uas` と設定し、自身がリフレッシャーとして動作する。

9.3.2. セッション更新時

9.3.2.1. リフレッシャー側

セッション確立時に自身がリフレッシャーとしてセッション確立した場合は、Session-Expires ヘッダに `refresher=uac` と設定したセッションリフレッシュリクエストを送信する。

9.3.2.2. 非リフレッシャー側

受信したセッションリフレッシュリクエストの Session-Expires ヘッダに `refresher=uas` と設定されていれば、次回セッションリフレッシュリクエストを送信する立場（リフレッシャー）と認識し、`refresher=uac` と設定されていれば、セッションタイム満了までにセッションリフレッシュリクエストの受信を待つ立場（非リフレッシャー）と認識する。送信する 200(OK)レスポンスの Session-Expires ヘッダには受信した `refresher` パラメータの値をそのままコピーする。

受信したセッションリフレッシュリクエストに Supported ヘッダが存在し且つ”timer”が含まれている場合において、Session-Expires ヘッダに `refresher` パラメータが存在しない場合は、送信する 200(OK)レスポンスの Session-Expires ヘッダに `refresher=uas` もしくは `uac` と設定する。

9.4. セッションタイマ値と Min-SE 値

9.4.1. 発呼側/リフレッシャー側

Initial INVITE リクエスト/セッションリフレッシュリクエストにおける Session-Expires ヘッダの”delta-seconds”に設定する値を変更できるような実装が望ましい¹²。ここで設定した値は、Min-SEヘッダの設定に違反しない限り、SIPサーバにて値を変更することがある。また、Min-SEヘッダは設定しないことが望ましいが、設定する場合にはその値を変更できるような実装が望ましい¹³。

Initial INVITE リクエスト/セッションリフレッシュリクエストに対して、Min-SEヘッダが設定された422(Session Interval Too Small)レスポンスを受信した場合、受信した Min-SEヘッダを含めかつ、受信した Min-SEヘッダの値を Session-Expiresヘッダに設定した Initial INVITE リクエストを用いて、ユーザリソースに影響を与えることなくセッション確立動作を継続する方が望ましい。

なお、リトライした Initial INVITE リクエスト/セッションリフレッシュリクエストに対してさらに422(Session Interval Too Small)レスポンスを受信したとしても、同様に再度リトライを行い、それまでの間に送受信した Min-SEヘッダの値も含めて最も大きい値を、ダイアログ確立時にダイアログ内の Min-SE値として用いるために記憶しておく。

200(OK)レスポンスで受信した Session-Expiresヘッダの”delta-seconds”値をもって、セッションタイマを設定/開始する。

9.4.2. 着呼側/非リフレッシャー側

受信した Initial INVITE リクエスト/セッションリフレッシュリクエストの Session-Expiresヘッダの値を200(OK)レスポンスの Session-Expiresヘッダに設定する。

受信した Initial INVITE リクエストの Supportedヘッダに timer が設定されており、Session-Expiresヘッダの値が自身が設定しうるセッションタイマ値として小さすぎる場合は、自身がセッションタイマ値として設定しうる最小の値を、Min-SEヘッダに設定した422(Session Interval Too Small)レスポンスを送信する。

200(OK)レスポンス送信とともに、Session-Expiresヘッダに設定した値をもって、セッションタイマを設定/開始するとともに、受信した Initial INVITE リクエストに Min-SEヘッダが含まれていれば、それまでの間に送受信した Min-SEヘッダの値も含めて最も大きい値をダイアログ内の Min-SE値として記憶しておく。

9.5. セッションの更新

9.5.1. リフレッシャー側

リフレッシャーは、当該ダイアログにおけるセッションタイマが直前のセッションリフレッシュリクエストの送受信時に決定したセッションタイマ値（未だ当該ダイアログにおけるセッションリフレッシュリクエストの送受信を行っていない場合は、セッション確立時に決定したセッションタイマ値）の半分¹⁴を経過した時点で、セッションリフレッシュリクエストを送信する。200(OK)レスポンス受信とともに、Session-Expiresヘッダで受信した値をもって、セッションタイマを再設定/開始する。

なお、リフレッシャー側が Session-Expiresヘッダを含む re-INVITE リクエストもしくは UPDATE リクエストを受信した場合においてもセッションリフレッシュリクエストと認識し、非リフレッシャーのケースと同様の処理を行わなければならない。

9.5.2. 非リフレッシャー側

当該ダイアログにおけるセッションタイマが満了するまでの間に、当該ダイアログに該当する

¹² 接続する私設総合サービス網交換機(PINX)に応じて規定する値が異なることに留意する必要がある。

¹³ 接続する私設総合サービス網交換機(PINX)に応じた規定値以下を設定する必要がある。

¹⁴ 接続する私設総合サービス網交換機(PINX)に応じて規定する値が異なることに留意する必要がある。

Session-Expires ヘッダを含む UPDATE リクエストまたは re-INVITE リクエストを受信した場合、これをセッションリフレッシュリクエストの受信と判断する。200(OK)レスポンス送信とともに、Session-Expires ヘッダに設定した値をもって、セッションタイマを再設定/開始する。

9.5.3. メディア変更にともなうリクエスト送信

セッションタイマが動作している場合においては、Confirmed ダイアログ確立後にメディア変更をともなう re-INVITE リクエストもしくは UPDATE リクエストを送信する場合においても、セッションリフレッシュリクエストとしての動作を行わなければならない。

9.6. セッションリフレッシュ失敗時

リフレッシャー側 SIP 端末は、セッションリフレッシュリクエストの再送タイムアウトや、408(Request Timeout)レスポンスもしくは 481(Call/Transaction Does Not Exist)レスポンス受信の際には JF-IETF-RFC3261[1] の 12.2.1.2 節に従い BYE リクエストを送信し呼を開放する。408(Request Timeout)レスポンス及び 481(Call/Transaction Does Not Exist)レスポンス以外のエラーレスポンス受信の際は、リフレッシャー側 SIP 端末は JF-IETF-RFC3261[1]の各レスポンスコード受信時の規定に従い動作する。但し 422(Session Interval Too Small)レスポンス受信-時は本文 9.4.1 節の Initial INVITE における 422(Session Interval Too Small)レスポンス受信時の動作と同様に動作する。

もしくは、リフレッシャー側 SIP 端末はセッションリフレッシュリクエストの再送タイムアウトや 422(Session Interval Too Small)レスポンス以外のレスポンスを受信時には、ユーザリソースや上位アプリからの切断指示がない限り、セッションタイマが満了する 10 秒前まではセッションを継続した後、強制的に当該ダイアログに対して BYE リクエストを送信し、ユーザリソースへの BusyTone 送出（もしくはそれと同等の処理）を行う動作であってもよい。

非リフレッシャー側 SIP UA はセッションタイマが満了する 32 秒前もしくはセッションタイマ値の 3 分の 1 の値が 32 秒より小さければその値前までにセッションリフレッシュリクエストを受信しなかった場合、その時点で強制的に当該ダイアログに対して BYE リクエストを送信し、ユーザリソースへの BusyTone 送出（もしくはそれと同等の処理）を行う。もしくは本動作はセッションタイマが満了する 10 秒前もしくはセッションタイマ値の 3 分の 1 の値が 10 秒より小さければその値前であってもよい。

10. メディア確立

10.1. コーデック

ITU-T 勧告 G.711 μ -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、G.711 Appendix I 相当の PLC(Packet Loss Concealment)機能を備えることが望ましい。なお、その他のコーデックをサポートしている場合においては、優先するコーデックの選択や特定コーデックのみ選択などが設定により指定可能であることが望ましい¹⁵。

10.2. SDP

10.2.1. オファー/アンサーによるメディア確立

JF-IETF-RFC3264[3]にもとづくオファー/アンサーの交換によりメディアを確立する。なお、SDP の改行コードについては、送信時には CRLF を設定しなければならず、受信時も CRLF を処理しなくてはならない。

セッション確立時のオファーは Initial INVITE（又は、200(OK)）リクエストに含めて送信し、同一ダイアログ内におけるアンサーの受信は、1xx (\neq 100(Trying)) レスポンスにより受信した SDP または、200(OK)（又

¹⁵ どのコーデックを最優先として扱うかは私設総合サービス網交換機(PINX)により定義される。

は、ACK) レスポンスにより受信した SDP のいずれか早く受信したものにより確定する。なお、100rel 拡張機能未動作時においても、1xx (≠100(Trying)) レスポンスにて受信した SDP はアンサーとして処理できなければいけない。複数ダイアログに対して SDP を 1xx/2xx レスポンスにて複数回を受信した場合の処理については、5.3.2 節を参照する。

SIP レスポンスメッセージの経路での喪失や SIP メッセージと RTP パケットが経由するルートの違いにより、発側 SIP 端末は相手からのアンサー受信前に相手からの RTP を受け取る場合がある。この場合、可能でありかつ必要ならば、ジッタバッファの調整などを行うとともに、ユーザリソースへのパス接続を行っても構わない。また、同様の理由により、アンサーを送信した SIP 端末は、送信した RTP パケットに対して ICMP Unreachable を受信する可能性があるが、これを無視してダイアログ/メディアを継続する。

メディアは、SDP の交換による c=行、m=行及び a=行にもとづき RTP/RTCP により送受信するが、RTCP を受信できないことにより切断処理を行ってはならない (実際には RTCP を送信しない接続相手 SIP UA の存在も考慮する)。

受信した SDP に対応可能なコーデックが設定されていない場合においては、SIP 端末は JF-IETF-RFC3261[1]に従い 488(Not Acceptable Here)レスポンスを返送する。SIP 端末は 488 レスポンスの Warning ヘッダに 304 を設定し、また、対応可能なコーデックをメッセージボディに設定することが出来る。

Initial INVITE リクエストに含めるオファーの構成は以下のとおりとする。

- ◆ m=行には、サポートするコーデックの中で定義された優先順位¹⁶、もしくは特定コーデックのみにて fmt list に設定する。なお G711 に対応する fmt list の値は 0 を使用することとする。m=行に設定できるコーデックの数は、私設総合サービス網交換機(PINX)によって指定される場合がある。
- ◆ a=inactive、a=sendonly、a=recvonly の属性は設定しない。また、G711 において a=ptime を設定する場合は 20ms が推奨される¹⁷。
- ◆ Media Description パートを複数繰り返さない。
- ◆ その他、省略可能な行は省略する。

また、アンサーの構成は以下のとおりとする。

- ◆ m=行には、受信したオファーの m=行に複数のコーデックが示されていた場合、自身がサポートするコーデックと比較し、定義された選択方法により決定されたコーデックを fmt list に設定する。選択方法はオファーで受信した優先順位に従う場合と、SIP 端末に定義されているコーデック優先順位に従い決定する場合などが考えられる¹⁸。この優先順位に従いコーデックを一つ選択し、アンサーとして設定する。なお、DTMF の送信に JF-IETF-RFC2833[1]で規定される telephone-event を使用する場合は、選択したコーデックの他に telephone-event も同時に設定する。
- ◆ m=行が複数存在するオファーを受信した場合は、受信した m=行を削除することなく、利用できないまたは、利用しないコーデックが fmt list に示されている m=行の port に”0”を設定する方が望ましい。また、セッションリフレッシュリクエストとして、re-INVITE リクエストを送信しなければならない場合に、ここで構成したアンサーと同じものを送信しなければならないことに留意する。

¹⁶ 複数コーデックの機能を有する場合の優先度は私設総合サービス網交換機(PINX)により指定される。

¹⁷ 私設総合サービス網交換機(PINX)により他の値についても許容されるかもしれない。

¹⁸ 複数コーデックの機能を有する場合の優先度は私設総合サービス網交換機(PINX)により指定される。

- ◆ a=inactive、a=sendonly、a=recvonly の属性をオファーで受信した場合には、指定に従い a=行を設定する。これらの属性に対応していない場合は 488(Not Acceptable Here)レスポンスを返送する方が望ましい。但し、既存のセッションの終了処理を行わず、その扱いはメディア変更要求をした SIP UA 側の判断に委ねることとする。また、a=ptime を設定する場合は、オファーで受信した値と合せるかまたは、オファーで受信していない場合は 20ms を推奨とする。
- ◆ オファーの m=行で、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、アンサーとして該当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ことを私設総合サービス網交換機(PINX)によって指定される可能性がある。また、a=行の設定についても、オファーと同一値を設定することを私設総合サービス網交換機(PINX)によって指定される可能性がある。
- ◆ その他、省略可能な行は省略する。

10.2.2. メディア変更要求受信

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、オファーにおける o=行の version の値を確立済みのメディア確立/変更の際に受信していたオファーまたは、アンサーにおける o=行の version の値と比較し、異なっている場合はメディア変更要求と判断する。この場合、メディア確立時と同様にアンサーを構成し、変更内容に応じたメディア再確立を行う。なお、前回自身が送信したオファーまたは、アンサーと変更のない場合は o=行の version を変更してはならない。

メディア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) 等の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、その扱いはメディア変更要求をした SIP UA 側の判断に委ねることとする。なお、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変更要求受信に対しては、SIP 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。

10.2.3. メディア変更要求送信

メディア変更要求を行う場合¹⁹は、以前に送信した SDP における o=行の version を 1 インクリメントし、re-INVITE リクエストもしくは UPDATE リクエストに設定しオファーを行う。なおダイアログが確立した状態且つセッションタイム拡張機能が動作している場合においては、本文 9 章に記載する動作に従う必要がある。

ダイアログが確立している状態においてメディア変更要求に対して UAS にてその変更内容が実行できないと判断された場合には 488 (Not Acceptable Here) 等のレスポンスを受信する可能性があるが、セッション継続を望む場合において、セッションタイム拡張機能が当該ダイアログにて動作している場合には本文 9 章に記載する動作に従う必要がある。

10.2.4. re-INVITE トランザクションにおける留意事項

セッションタイム拡張機能（本文 9 章参照）におけるセッションリフレッシュ動作などで行われる re-INVITE トランザクションによるメディア変更をとまなわないオファー/アンサーの送受信における留意事項を記載する。

複数コーデックをサポートしているオファーを Initial INVITE リクエストに含めていた場合、その SIP UA

¹⁹ メディア変更要求を行ってもよいかどうかは接続する私設総合サービス網交換機(PINX)により定義される。

が送出する re-INVITE トランザクションにおけるオファーまたは、アンサーの m=行には、メディア確立時に受信したアンサーで選択されたコーデックのみを fmt list に含めることとする。この際、SDP 内容の変更をしていることになるが、実質的に接続相手の SIP UA に対してメディア変更要求をとまなう必要がないため、o=行の version を変更しないこととする。

また、複数コーデックをサポートするオファーを Initial INVITE リクエストで受信していた場合は、その SIP UA から受信する re-INVITE トランザクションにおけるオファーまたは、アンサーが以下のいずれの条件であっても、問題なくオファー/アンサーが完了したものと判断し、正常にセッションリフレッシュできるように考慮する。

- ◆ o=行の version がインクリメントされかつ、m=行の fmt list がメディア確立時に受信したアンサーで選択されたコーデックのみに変更されている
- ◆ Initial INVITE リクエストで受信したオファーと全く同じ (m=行の fmt list に複数のコーデックが含まれている)
- ◆ o=行の version はインクリメントされていないが、m=行の fmt list はメディア確立時のアンサーで選択されたコーデックのみに変更されている

11. 呼切断

11.1. BYE リクエスト送信

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に該当する 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方が望ましい。

11.2. BYE リクエスト受信

通話中に当該ダイアログに該当する BYE リクエストを受信した場合、200(OK)レスポンスを送信するとともに、ダイアログ/メディアの解放を行う。ユーザリソースに対しては、BYE リクエスト受信を契機として、BusyTone を送出するかもしくはそれに準じた動作を行う。

12. 付加機能

12.1. 番号通知/非通知

12.1.1. Initial INVITE リクエストの設定規則

発番号通知/非通知の制御のために、SIP 端末において Initial INVITE リクエスト送信時に適切な設定を行わなければならない。JF-IETF-RFC3323[5]/JF-IETF-RFC3325[7]に規定される方式を用いる(方式 1)ことにより私設総合サービス網交換機(PINX)に通知するか、ユーザダイヤル番号をそのまま Initial INVITE リクエストに設定する(方式 2)かのいずれかの方式を用いる。方式 1 における Initial INVITE リクエストへの設定条件を表 12-1 に、方式 2 における Initial INVITE リクエストへの設定条件を表 12-2 にそれぞれ記載する。なお、本 2 つの方式については設定により選択可能であることが望ましい。

表 12-1/JJ-22.11 方式1 発信時における番号通知に関するヘッダ設定条件

フィールド	通知時	非通知時	備考
Privacyヘッダ	none	id	
P-Preferred-Id entityヘッダ	<AoR>	<AoR>	通知時は設定しなくてもよい。
P-Asserted-Identityヘッダ	<ul style="list-style-type: none"> • sip_URIのDISPLAYNAME (非通知理由文字列) • tel_URIのDISPLAYNAME (数字情報) 	none	
Fromヘッダのname-addr	<AoR>	<sip:anonymous@anonymous.in valid>	
FromヘッダのDisplay-name	付加しても良い。(Userinfo部と同じ)	<sip:anonymous@anonymous.in valid>	
Request-URIのuserinfo部	電話番号	電話番号	184/186は設定しない。
Toヘッダのuserinfo部	Request-URIと同じ	Request-URIと同じ	184/186は設定しない。

表 12-2/JJ-22.11 方式2 発信時における番号通知に関するヘッダ設定条件

フィールド	通知時	非通知時	備考
Privacyヘッダ	—	—	設定してはいけない。
P-Preferred-Id entityヘッダ	—	—	設定してはいけない。
Fromヘッダのname-addr	<AoR>	<A o R >	
FromヘッダのDisplay-name	付加しても良い。(Userinfo部と同じ)	付加しても良い。(Userinfo部と同じ)	
Request-URIのuserinfo部	(186)電話番号	(184)電話番号	184/186をユーザからダイヤルされた場合は電話番号の先頭に設定。
Toヘッダのuserinfo部	Request-URIと同じ	Request-URIと同じ	184/186をユーザからダイヤルされた場合は電話番号の先頭に設定。

12.1.2. ヘッダ透過転送に関する留意事項

SIPサーバでは、不明なヘッダ情報等を着側SIPUAまで透過に転送する可能性があるため、12.1.1節に示したヘッダ以外のSIPヘッダ(但し、Proxy-Authorizationヘッダにおけるusernameを除く)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しない方が望ましい。²⁰

12.2. 発信者番号表示

受信したInitial INVITEリクエストのP-Asserted-Identityヘッダ/Privacyヘッダ/Fromヘッダの設定内容に応じて着信ユーザに表示する発信者情報の判断を以下の判定論理により行う。²¹

²⁰ 受信時の条件については、12.1.1節に示すヘッダに発信者を示す情報が設定されるかもしれない。

²¹ 但し、別の設定方式が私設総合サービス網交換機(PINX)により指定される場合がある。

12.2.1. 方式 1 発信者番号表示

SIPサーバは、Privacyヘッダにidが設定されている場合、P-Asserted-Identityヘッダは設定してはいけない。また、Privacyヘッダにnoneが設定されている場合、あるいはPrivacyヘッダが設定されていない場合は、P-Asserted-Identityヘッダは設定するべきである。

① P-Asserted-Identityヘッダ

- P-Asserted-Identityヘッダが設定されている場合は②へ
- P-Asserted-Identityヘッダが設定されていない場合は④へ

② P-Asserted-Identityヘッダの sip URI の DISPLAYNAME

- 表 12-3 のいずれかの条件に合致すれば、表 12-3 の”表示内容（意味）”欄に相当する内容を表示
- 表 12-3 の条件に合致しない場合は③へ

③P-Asserted-Identityヘッダの tel_URI の DISPLAYNAME

- 受信した数字列を表示

④Privacyヘッダ

- idが設定されている場合⑦へ
- noneが設定されている、あるいはヘッダが設定されていない場合⑤へ

⑤Fromヘッダの-DISPLAYNAME

- DISPLAYNAMEが有る場合、受信した文字列を表示
- DISPLAYNAMEが無い場合⑥へ

⑥Fromのuserinfo部

- userinfoで受信した文字列を表示

⑦FromのDISPLAYNAME

- 表 12-3 のいずれかの条件に合致すれば、表 12-3 の”表示内容（意味）”欄に相当する内容を表示。
- 表 12-3 の条件に合致しない場合、「サービス提供不可のため通知不可」に相当する内容を表示。

12.2.2. 方式 2 発信者番号表示

Fromヘッダの“display-name”又は“userinfo”部に、“anonymous”の設定があれば非通知と判断する。“anonymous”以外の非通知理由（表 12-3 参照）の表示については考慮しても良い。

Fromヘッダの“display-name”又は“userinfo”部に、“anonymous”の設定がなければ通知と判断し、Fromヘッダの“display-name”又は、“userinfo”部から発信者番号情報を抽出し表示する。尚、発信者番号情報内に数字以外が設定されていた場合は、端末の条件により発信者番号情報の中から表示可能な情報のみを選択して表示しても良い。

表 12-3/JJ-22.11 非通知理由表示内容

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）で囲まれるかもしれない。

(*2) 本表の記載する文字列の後ろに任意の文字列が続くかもしれない。

13. SIP 関連信号フォーマット

各 SIP メッセージ(リクエスト、レスポンス)に対し、関連する SIP ヘッダやその他の構成要素のリストを表形式で示す。

13.1. 基本信号フォーマット

13.1.1. SIP リクエスト信号

本規定が扱う SIP リクエスト信号の一覧を表 13-1 に示す。

表 13-1/JJ-22.11 SIP リクエスト信号一覧

SIP リクエスト信号	参照	種別 (送信側)	種別 (受信側)	備考
ACK	[1]	m	m	
BYE	[1]	m	m	
CANCEL	[1]	m	m	
Initial INVITE	[1]	m	m	
PRACK	[2]	c1	m	
re-INVITE	[1]	m	m	
REGISTER	[1]	x(サーバ) c2(端末)	m(サーバ) i(端末)	
UPDATE	[4]	c3	m	
その他リクエスト		i	i	

c1: Initial INVITE の Supported ヘッダに"100rel"を設定した場合は"m"、設定しない場合は"x"
c2: ロケーション情報登録動作が必要な場合"m"、必要でない場合"x"
c3: セッションの更新に UPDATE を使用する場合は"m"、UPDATE を使用しない場合"x"

13.1.2. SIP レスポンス信号

表 13-1 にて記載する各 SIP リクエストに対する本規定が扱う SIP レスポンス信号の一覧を表に示す。但し、SIP レスポンス信号受信時には JF-IETF-RFC3261[1]8.1.3.2 節を最低限サポートしなければならない。

表 13-2/JJ-22.11 INVITE リクエストに対する SIP レスポンス信号一覧

種別	SIP レスポンス信号		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考	
	コード	フレーズ					
1xx	100	Trying	[1]	m	m		
	180	Ringing	[1]	m	m		
	181	Call Is Being Forwarded	[1]	o	o		
	182	Queued	[1]	o	o		
	183	Session Progress	[1]	o	o		
	他			i	i		
2xx	200	OK	[1]	m	m		
	他		[1]	i	i		
3xx	300	Multiple Choices	[1]	o	o		
	301	Moved Permanently	[1]	o	o		
	302	Moved Temporarily	[1]	o	o		
	305	Use Proxy	[1]	o	o		
	380	Alternative Service	[1]	o	o		
	他		[1]	i	i		
4xx	400	Bad Request	[1]	o	o		
	401	Unauthorized	[1]	x(端末) o(サーバ)	o(端末) i(サーバ)	※3	
	402	Payment Required	[1]	o	o		
	403	Forbidden	[1]	o	o		
	404	Not Found	[1]	o	o		
	405	Method Not Allowed	[1]	o	o		
	406	Not Acceptable	[1]	o	o		
	407	Proxy Authentication Required	[1]	x(端末) m(サーバ)	m(端末) i(サーバ)		
	408	Request Timeout	[1]	o	o		
	410	Gone	[1]	o	o		
	413	Request Entity Too Large	[1]	o	o		
	414	Request-URI Too Long	[1]	o	o		
	415	Unsupported Media Type	[1]	o	o		
	416	Unsupported URI Scheme	[1]	o	o		
	420	Bad Extension	[1]	o	o	表 13-13(proxy-required)と関連。	
	421	Extension Required	[1]	x	o		
	422	Session Interval Too Small	[13]	m	m		
	423	Interval Too Brief	[1]	n/a	i		
	480	Temporarily Unavailable	[1]	o	o		
	481	Call/Transaction Does Not Exist	[1]	o	o		
	482	Loop Detected	[1]	o	o		
	483	Too Many Hops	[1]	o	o		
	484	Address Incomplete	[1]	o	o		
	485	Ambiguous	[1]	o	o		
	486	Busy Here	[1]	m	m		
	487	Request Terminated	[1]	m	m		
	488	Not Acceptable Here	[1]	m	m		
	491	Request Pending	[1]	o	o		
	493	Undecipherable	[1]	o	o		
	他		[1]	i	i		
	5xx	500	Server Internal Error	[1]	o	o	
		501	Not Implemented	[1]	o	o	
502		Bad Gateway	[1]	o	o		
503		Service Unavailable	[1]	o	o		
504		Server Time-out	[1]	o	o		
505		Version Not Supported	[1]	o	o		
513		Message Too Large	[1]	o	o		
他			[1]	i	i		
6xx	600	Busy Everywhere	[1]	o	o		
	603	Decline	[1]	o	o		
	604	Does Not Exist Anywhere	[1]	o	o		
	606	Not Acceptable	[1]	o	o		
	他		[1]	i	i		

c1: そのレスポンスが自身の属する SIP サーバからのものであることの確証がとれ、且つセキュリティ上のリスクがないことが確認される場合”o”、確認されない場合”x”

※1. INVITE を受信して、レスポンスを送信する側

※2. INVITE を送信して、エラーを受信する側

※3 B2BUA 方式の SIP サーバで利用される場合がある。端末は 407 認証と双方の認証に対応することが望ましい。

表 13-3/JJ-22.11 UPDATE リクエストに対する SIP レスポンス信号一覧

SIP レスポンス信号			参照	種別 (送信側) ※1	種別 (受信側) ※2	備考	
種別	コード	フレーズ					
1xx	100	Trying	[1][4]	x	o		
	180	Ringing	[1][4]	x	o		
	181	Call Is Being Forwarded	[1][4]	x	o		
	182	Queued	[1][4]	x	o		
	183	Session Progress	[1][4]	x	o		
	他		[1][4]	i	i		
2xx	200	OK	[1][4]	m	m		
	他		[1][4]	i	i		
3xx	300	Multiple Choices	[1][4]	x	i		
	301	Moved Permanently	[1][4]	x	i		
	302	Moved Temporarily	[1][4]	x	i		
	305	Use Proxy	[1][4]	x	i		
	380	Alternative Service	[1][4]	x	i		
	他		[1][4]	i	i		
4xx	400	Bad Request	[1][4]	o	o		
	401	Unauthorized	[1][4]	o	o		
	402	Payment Required	[1][4]	o	o		
	403	Forbidden	[1][4]	o	o		
	404	Not Found	[1][4]	o	o		
	405	Method Not Allowed	[1][4]	o	o		
	406	Not Acceptable	[1][4]	o	o		
	407	Proxy Authentication Required	[1][4]	x(端末) o(サーバ)	o(端末) x(サーバ)	※3	
	408	Request Timeout	[1][4]	o	o		
	410	Gone	[1][4]	o	o		
	413	Request Entity Too Large	[1][4]	o	o		
	414	Request-URI Too Long	[1][4]	o	o		
	415	Unsupported Media Type	[1][4]	o	o		
	416	Unsupported URI Scheme	[1][4]	o	o		
	420	Bad Extension	[1][4]	o	o		
	421	Extension Required	[1][4]	x	o		
	422	Session Interval Too Small	[4][13]	m	m		
	423	Interval Too Brief	[1][4]	n/a	i		
	480	Temporarily Unavailable	[1][4]	o	o		
	481	Call/Transaction Does Not Exist	[1][4]	o	o		
	482	Loop Detected	[1][4]	o	o		
	483	Too Many Hops	[1][4]	o	o		
	484	Address Incomplete	[1][4]	o	o		
	485	Ambiguous	[1][4]	o	o		
	486	Busy Here	[1][4]	o	o		
	487	Request Terminated	[1][4]	o	o		
	488	Not Acceptable Here	[1][4]	m	m		
	491	Request Pending	[1][4]	o	o		
	493	Undecipherable	[1][4]	o	o		
	他		[1][4]	i	i		
	5xx	500	Server Internal Error	[1][4]	o	o	
		501	Not Implemented	[1][4]	o	o	
		502	Bad Gateway	[1][4]	o	o	
503		Service Unavailable	[1][4]	o	o		
504		Server Time-out	[1][4]	o	o		
505		Version Not Supported	[1][4]	o	o		
513		Message Too Large	[1][4]	o	o		
他			[1][4]	i	i		
6xx		600	Busy Everywhere	[1][4]	o	o	
	603	Decline	[1][4]	o	o		
	604	Does Not Exist Anywhere	[1][4]	o	o		
	606	Not Acceptable	[1][4]	o	o		
他		[1][4]	i	i			

※1.UPDATEを受信して、レスポンスを送信する側
※2.UPDATEを送信して、エラーを受信する側
※3.UPDATEにおける認証は非推奨とする

表 13-4/JJ-22.11 REGISTER リクエストに対する SIP レスポンス信号一覧

種別	SIP レスポンス信号		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考
	コード	フレーズ				
1xx	100	Trying	[1]	x	o	
	180	Ringing	[1]	x	o	
	181	Call Is Being Forwarded	[1]	x	o	
	182	Queued	[1]	x	o	
	183	Session Progress	[1]	x	o	
	他		[1]	i	i	
2xx	200	OK	[1]	m	m	
	他		[1]	o	o	
3xx	300	Multiple Choices	[1]	c1	c1	
	301	Moved Permanently	[1]	c1	c1	
	302	Moved Temporarily	[1]	c1	c1	
	305	Use Proxy	[1]	c1	c1	
	380	Alternative Service	[1]	c1	c1	
	他		[1]	i	i	
4xx	400	Bad Request	[1]	o	o	
	401	Unauthorized	[1]	端末 : n/a サーバ : m	端末 : m サーバ : x	
	402	Payment Required	[1]	o	o	
	403	Forbidden	[1]	o	o	
	404	Not Found	[1]	o	o	
	405	Method Not Allowed	[1]	o	o	
	406	Not Acceptable	[1]	o	o	
	407	Proxy Authentication Required	[1]	o	o	
	408	Request Timeout	[1]	o	o	
	410	Gone	[1]	o	o	
	413	Request Entity Too Large	[1]	o	o	
	414	Request-URI Too Long	[1]	o	o	
	415	Unsupported Media Type	[1]	o	o	
	416	Unsupported URI Scheme	[1]	o	o	
	420	Bad Extension	[1]	o	o	
	421	Extension Required	[1]	o	o	
	422	Session Interval Too Small	[13]	n/a	n/a	
	423	Interval Too Brief	[1]	m	m	
	480	Temporarily Unavailable	[1]	o	o	
	481	Call/Transaction Does Not Exist	[1]	o	o	
	482	Loop Detected	[1]	o	o	
	483	Too Many Hops	[1]	o	o	
	484	Address Incomplete	[1]	o	o	
	485	Ambiguous	[1]	o	o	
	486	Busy Here	[1]	o	o	
	487	Request Terminated	[1]	o	o	
	488	Not Acceptable Here	[1]	o	o	
	491	Request Pending	[1]	o	o	
	493	Undecipherable	[1]	o	o	
	他		[1]	i	i	
5xx	500	Server Internal Error	[1]	o	o	
	501	Not Implemented	[1]	o	o	
	502	Bad Gateway	[1]	o	o	
	503	Service Unavailable	[1]	o	o	
	504	Server Time-out	[1]	o	o	
	505	Version Not Supported	[1]	o	o	
	513	Message Too Large	[1]	o	o	
	他		[1]	i	i	
6xx	600	Busy Everywhere	[1]	n/a	n/a	
	603	Decline	[1]	n/a	n/a	
	604	Does Not Exist Anywhere	[1]	n/a	n/a	
	606	Not Acceptable	[1]	n/a	n/a	
	他		[1]	i	i	

c1: そのレスポンスが自身の属する SIP サーバ又は端末からのものであることの確証がとれ、且つセキュリティ上のリスクがないことが確認される場合”o”、確認されない場合”x”

※1. REGISTER を受信するサーバ側を規定する為、端末側は“n/a”となる。

※2. REGISTER を送信する端末側

表 13-5/JJ-22.11 CANCEL、PRACK、BYE リクエストに対する SIP レスポンス信号一覧

種別	SIP レスポンス信号		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考	
	コード	フレーズ					
1xx	100	Trying	[1][2]	x	o		
	180	Ringing	[1][2]	x	o		
	181	Call Is Being Forwarded	[1][2]	x	o		
	182	Queued	[1][2]	x	o		
	183	Session Progress	[1][2]	x	o		
	他		[1][2]	i	i		
2xx	200	OK	[1][2]	m	m		
	他		[1][2]	i	i		
3xx	300	Multiple Choices	[1][2]	x	i		
	301	Moved Permanently	[1][2]	x	i		
	302	Moved Temporarily	[1][2]	x	i		
	305	Use Proxy	[1][2]	x	i		
	380	Alternative Service	[1][2]	x	i		
	他		[1][2]	i	i		
4xx	400	Bad Request	[1][2]	o	o		
	401	Unauthorized	[1][2]	x	o		
	402	Payment Required	[1][2]	o	o		
	403	Forbidden	[1][2]	o	o		
	404	Not Found	[1][2]	o	o		
	405	Method Not Allowed	[1][2]	o	o		
	406	Not Acceptable	[1][2]	o	o		
	407	Proxy Authentication Required	[1][2]	x(端末) o(サ-バ [®])	o(端末) x(サ-バ [®])	※3	
	408	Request Timeout	[1][2]	o	o		
	410	Gone	[1][2]	o	o		
	413	Request Entity Too Large	[1][2]	o	o		
	414	Request-URI Too Long	[1][2]	o	o		
	415	Unsupported Media Type	[1][2]	o	o		
	416	Unsupported URI Scheme	[1][2]	o	o		
	420	Bad Extension	[1][2]	o	o		
	421	Extension Required	[1][2]	o	o		
	422	Session Interval Too Small	[13][2]	n/a	n/a		
	423	Interval Too Brief	[1][2]	n/a	o		
	480	Temporarily Unavailable	[1][2]	o	o		
	481	Call/Transaction Does Not Exist	[1][2]	o	o		
	482	Loop Detected	[1][2]	o	o		
	483	Too Many Hops	[1][2]	o	o		
	484	Address Incomplete	[1][2]	o	o		
	485	Ambiguous	[1][2]	o	o		
	486	Busy Here	[1][2]	o	o		
	487	Request Terminated	[1][2]	o	o		
	488	Not Acceptable Here	[1][2]	o	o		
	491	Request Pending	[1][2]	o	o		
	493	Undecipherable	[1][2]	o	o		
	他		[1][2]	i	i		
	5xx	500	Server Internal Error	[1][2]	o	o	
		501	Not Implemented	[1][2]	o	o	
502		Bad Gateway	[1][2]	o	o		
503		Service Unavailable	[1][2]	o	o		
504		Server Time-out	[1][2]	o	o		
505		Version Not Supported	[1][2]	o	o		
513		Message Too Large	[1][2]	o	o		
他			[1][2]	i	i		
6xx	600	Busy Everywhere	[1][2]	o	o		
	603	Decline	[1][2]	o	o		
	604	Does Not Exist Anywhere	[1][2]	o	o		
	606	Not Acceptable	[1][2]	o	o		
	他		[1][2]	i	i		

- ※1. CANCEL などを受信して、レスポンスを送信する側
- ※2. CANCEL などを送信して、エラーを受信する側
- ※3. CANCEL などにおける認証は非推奨とする

13.1.3. SDP

本規定が扱う SDP の各フィールド一覧を表 13-6 にて記載する。

表 13-6/JJ-22.11 SDP

項目	参照	規定タイプ (送信側)	規定タイプ (受信側)	備考 (参照節など)	
Session description	v=	[9]	m	m	“0”固定
	o=	[9]	m	m	
	s=	[9]	m	m	
	i=	[9]	o	o	
	u=	[9]	o	o	
	e=	[9]	o	o	
	p=	[9]	o	o	
	c=	[9]	m	m	
	b=	[9]	o	o	
	z=	[9]	o	o	
	k=	[9]	o	o	
a=	[9]	o	o	送受信指定	
Time description	t=	[9]	m	m	
	r=	[9]	o	o	
Media description	m=	[9]	m	m	
	i=	[9]	o	o	
	c=	[9]	o	o	
	b=	[9]	o	o	
	k=	[9]	o	o	
a=	[9]	m	m		

13.2. 動的変数共通条件

13.2.1. SIP 端末設定・保持情報の実装値条件

SIP 端末は私設総合サービス網交換機(PINX)に接続する上で、接続する対象サーバのアドレスや自身の AoR 等さまざまなユーザ情報を設定・保持するが、その中でも最低限必要となりうる情報について、レンジ等の設定・保持上の必要実装条件を表 13-7 に記載する。

表 13-7/JJ-22.11 設定・保持情報の実装条件

設定項目	最低実装要件	備考
SIP サーバアドレスの文字数	<ul style="list-style-type: none"> ・ IPv4 アドレス形式 ・ FQDN 形式：最低 32 文字までは対応可能であること 	
SIP レジストラサーバアドレスの文字数	<ul style="list-style-type: none"> ・ IPv4 アドレス形式 ・ FQDN 形式：最低 32 文字までは対応可能であること 	私設総合サービス網交換機(PINX)によっては INVITE リクエストの送信先である SIP サーバと REGISTER リクエストの送信先である SIP レジストラサーバ筐体が別であるため、SIP サーバアドレスとはフィールドを別とする。
AoR の文字数	<ul style="list-style-type: none"> ・ user 部：英数文字列。最低 16 文字までは対応可能であること ・ host 部：英数文字列。最低 32 文字までは対応可能であること。 	

ユーザ名の文字数	英数文字列。最低 16 文字までは対応可能であること	HTTP Digest 認証用ユーザ名
パスワードの文字数	英数文字列。最低 16 文字までは対応可能であること。	HTTP Digest 認証用パスワード

13.2.2. SIP 端末変数値条件

SIP 端末の実装等により動的に設定される文字列など、設定条件が変動する変動要素に関して、SIP 端末の実装として自身がその設定値の作成主体となる場合の作成可能な文字数の最大値及び、自身がその設定値の作成主体ではないが、接続相手から受信して正常に接続処理を行わなければならない文字数の受信能力の最低値を表 13-8 に示す。

表 13-8/JJ-22.11 SIP 端末変数値条件

変動要素の送受信条件変動要素	送受信時条件	備考
SIP ヘッダ 1 行あたりの文字数	最大 255 Byte 以下 (CRLF を含む)	生成時には複数 uri により SIP ヘッダ 1 行あたりの文字数が 255Byte を超える場合はヘッダを複数行に分割する。 例 Record-Route、Route、Via 等
realm の文字数	—	
Via-branch の文字数	最大 32Byte	
local uri の文字数	【user 部】 最大 16Byte 【host 部】 最大 31Byte	Initial INVITE リクエストの From ヘッダに設定する uri
remote uri の文字数	【user 部】 最大 16Byte 【host 部】 最大 31Byte	Initial INVITE リクエストの To ヘッダに設定する uri
To/From tag の文字数	最大 32 Byte 以下	
Call-ID の文字数	最大 64 Byte 以下	
CSeq ヘッダのシーケンス番号	初期値として、1 以上最大 999900 以下 ※32 bit Unsigned Integer の表現範囲	
RSeq ヘッダのシーケンス番号	初期値として、最大 999900 以下 ※32 bit Unsigned Integer の表現範囲	
ロケーション情報の文字数	user 部：最大 16 Byte 以下 全体：最大 64 Byte 以下	REGISTER リクエストの Contact ヘッダに設定する SIP URI
remote target の文字数	user 部：最大 16 Byte 以下 全体：最大 64 Byte 以下	自身が Initial INVITE リクエストまたは、1xx/2xx レスポンスの Contact ヘッダに設定する uri (REGISTER リクエストの Contact ヘッダに設定する uri も同条件とする)
rec-route1 あたりの文字数	— 最大 28Byte	送信条件は受信条件に従う。

変動要素の送受信条件変動要素	送受信時条件	備考
SDP o= 行 username の文字数	最大 10 Byte 以下	接続する私設総合サービス網交換機 (PINX) に応じて規定する値が異なることに留意する必要がある。
SDP o= 行 session id の文字数	初期値として、最大 999900 以下 ※32 bit Unsigned Integer の表現範囲	
SDP o= 行 version の値	初期値として、最大 999900 以下 ※32 bit Unsigned Integer の表現範囲	
SDP s= 行 session name の文字数	最大 10 Byte 以下	接続する私設総合サービス網交換機 (PINX) に応じて規定する値が異なることに留意する必要がある。

13.3. SIP リクエスト信号

本規定が扱う各 SIP リクエスト信号 (表 13-1 参照) における各ヘッダー一覧を記載する。

13.3.1. ACK リクエスト (2xx レスポンス時)

Initial INVITE リクエスト及び re-INVITE リクエストに対する最終レスポンスが 2xx レスポンスであった場合の ACK リクエストにおける各ヘッダー一覧を表 13-9 に記載する。

表 13-9 / JJ-22.11 ACK リクエスト (2xx レスポンス時) 設定

項目		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (本文書内の参照節など)
Request Line	Method	[1]	m	m	
	Request-URI	[1]	m	m	5.1.2 節及び、6.1.2 節を参照
	SIP-Version	[1]	m	m	“SIP/2.0”の固定値
Message Header	Authorization	[1]	o	o	
	Call-ID	[1]	m	m	
	Contact	[1]	o	o	
	Content-Disposition	[1]	x	o	
	Content-Encoding	[1]	x	o	
	Content-Language	[1]	x	o	
	Content-Length	[1]	m	o	
	Content-Type	[1]	o	o	
	CSeq	[1]	m	m	
	Date	[1]	o	o	
	From	[1]	m	m	
	Max-Forwards	[1]	m	o	
	MIME-Version	[1]	o	o	
	Privacy	[5]	x	o	
	Proxy-Authorization	[1]	o	o	
	Record-Route	[1]	x	o	
	Route	[1]	o	o	
	Timestamp	[1]	o	o	
	To	[1]	m	m	
	User-Agent	[1]	o	o	
Via	[1]	m	m		
その他			i	i	
SDP		[9]	o	o	

※1. 2xx を受信して、ACK を送信する側
 ※2. 2xx を送信して、ACK を受信する側

13.3.2. ACK リクエスト (3xx/4xx/5xx/6xx レスポンス時)

表 13-10 / JJ-22.11 ACK リクエスト (3xx/4xx/5xx/6xx レスポンス時) 設定

項目		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)
Request Line	Method	[1]	m	m	
	Request-URI	[1]	m	m	INVITE の Request-URI と同値
	SIP-Version	[1]	m	m	“SIP/2.0”の固定値
Message Header	Authorization	[1]	o	o	
	Call-ID	[1]	m	m	
	Contact	[1]	o	o	
	Content-Disposition	[1]	x	o	
	Content-Encoding	[1]	x	o	
	Content-Language	[1]	x	o	
	Content-Length	[1]	m	o	
	Content-Type	[1]	x	o	
	CSeq	[1]	m	m	
	Date	[1]	o	o	
	From	[1]	m	m	
	Max-Forwards	[1]	m	o	
	MIME-Version	[1]	x	o	
	Privacy	[5]	x	o	
	Proxy-Authorization	[1]	o	o	
	Record-Route	[1]	x	o	
	Route	[1]	x	o	
	Timestamp	[1]	o	o	
	To	[1]	m	m	
	User-Agent	[1]	o	o	
Via	[1]	m	m	Branch-id は INVITE のものと同値。	
その他			i	i	
SDP		[9]	x	o	

※1. 3xx/4XX/5XX/6XX を受信して、ACK を送信する側
 ※2. 3xx/4XX/5XX/6XX を送信して、ACK を受信する側

13.3.3. BYE リクエスト

表 13-11/JJ-22.11 BYE リクエスト設定

項目	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
Request Line	Method	[1]	m	m	
	Request-URI	[1]	m	m	Record-Routing の動作に従う (33 章を参照)
	SIP-Version	[1]	m	m	“SIP/2.0”の固定値
Message Header	Accept	[1]	o	o	
	Accept-Encoding	[1]	o	o	
	Accept-Language	[1]	o	o	
	Allow	[1]	o	o	
	Authorization	[1]	x	o	
	Call-ID	[1]	m	m	
	Content-Disposition	[1]	x	o	
	Content-Encoding	[1]	x	o	
	Content-Language	[1]	x	o	
	Content-Length	[1]	m	o	
	Content-Type	[1]	x	o	
	CSeq	[1]	m	m	
	Date	[1]	o	o	
	From	[1]	m	m	
	Max-Forwards	[1]	m	o	
	MIME-Version	[1]	x	o	
	P-Asserted-Identity	[7]	x	o	
	P-Preferred-Identity	[7]	x	o	
	Privacy	[5]	x	o	
	Proxy-Authorization	[1]	o	o	
	Proxy-Require	[1]	x	o	
	Record-Route	[1]	x	o	
	Require	[1]	x	o	
	Route	[1]	o	o	
Supported	[1]	o	o		
Timestamp	[1]	o	o		
To	[1]	m	m		
User-Agent	[1]	o	o		
Via	[1]	m	m		
その他		i	i		
SDP	[9]	x	o		

※1. BYE を送信する側
 ※2. BYE を受信する側

13.3.4. CANCEL リクエスト

表 13-12 / JJ-22.11 CANCEL リクエスト設定

項目		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)
Request Line	Method	[1]	m	m	
	Request-URI	[1]	m	m	INVITE と同じ値を設定
	SIP-Version	[1]	m	m	“SIP/2.0”の固定値
Message Header	Authorization	[1]	x	o	
	Call-ID	[1]	m	m	
	Content-Length	[1]	m	o	
	CSeq	[1]	m	m	
	Date	[1]	o	o	
	From	[1]	m	m	
	Max-Forwards	[1]	m	o	
	Privacy	[5]	x	o	
	Record-Route	[1]	x	o	
	Route	[1]	x	o	
	Supported	[1]	o	o	
	Timestamp	[1]	o	o	
	To	[1]	m	m	
	User-Agent	[1]	o	o	
	Via	[1]	m	m	
その他			i	i	
SDP		[9]	x	o	
※1. CANCEL を送信する側 ※2. CANCEL を受信する側					

13.3.5. Initial INVITE リクエスト

表 13-13 / JJ-22.11 Initial INVITE リクエスト設定

項目		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)
Request Line	Method	[1]	m	m	
	Request-URI	[1]	m	m	
	SIP-Version	[1]	m	m	“SIP/2.0”の固定値
Message Header	Accept	[1]	o	o	
	Accept-Encoding	[1]	o	o	
	Accept-Language	[1]	o	o	
	Alert-Info	[1]	o	o	
	Allow	[1]	o	c1	送信時、100rel 拡張機能を使用する場合は”PRACK“を挿入し、UPDATE メソッドを使用する場合は”UPDATE”を挿入する。
	Authorization	[1]	o	o	
	Call-ID	[1]	m	m	
	Call-Info	[1]	o	o	
	Contact	[1]	m	m	
	Content-Disposition	[1]	x	o	
	Content-Encoding	[1]	x	o	
	Content-Language	[1]	x	o	
	Content-Length	[1]	m	o	
	Content-Type	[1]	m	m	
	CSeq	[1]	m	m	
	Date	[1]	o	o	
	Expires	[1]	o	o	
	From	[1]	m	m	
	In-Reply-To	[1]	o	o	
	Max-Forwards	[1]	m	o	
	MIME-Version	[1]	x	o	
	Min-SE	[13]	c2	c3	
	Organization	[1]	o	o	
	P-Asserted-Identity	[7]	c8	c8	
	P-Preferred-Identity	[7]	c8	c8	
	Priority	[1]	o	o	
	Privacy	[5][7]	c4	c4	
	Proxy-Authorization	[1]	o	o	
Proxy-Require	[1]	x(端末) o(サーバ)	o	表 13-2(420)と関連。	
Record-Route	[1]	x	o		
Reply-To	[1]	o	o		
Require	[1]	x	o		

	Route	[1]	x	o	
	Session-Expires	[13]	c5	c6	
	Subject	[1]	o	o	
	Supported	[1][2] [13]	c7	c7	
	Timestamp	[1]	o	o	
	To	[1]	m	m	
	User-Agent	[1]	o	o	
	Via	[1]	m	m	
	その他		i	i	
SDP		[9]	m	m	サーバから着側端末へ送信される Initial INVITE にはオファーを含めなくても良い。

c1: UPDATE メソッドを使用する場合”m”,使用しない場合”o”
c2: セッションタイム拡張機能を使用しかつ同じ発信要求(同一 Call-ID) で以前に 422(Session Interval Too Small)レスポンスを受信している場合”m”、セッションタイム拡張機能を使用しかつ同じ発信要求(同一 Call-ID) で以前に 422(Session Interval Too Small)レスポンスを受信していない場合”o”、セッションタイム拡張機能を使用しない場合”x”
c3: セッションタイム拡張機能を使用する場合”m”、使用しない場合”o”
c4: 表 12-1 を使用する場合”m”、表 12-2 を使用する場合”x”
c5: セッションタイム拡張機能を使用する場合”m”、セッションタイム拡張機能を使用しない場合”x”
c6: セッションタイム拡張機能を使用する場合”m”、セッションタイム拡張機能を使用しない場合”o”
c7: 100rel 拡張機能もしくはセッションタイム拡張機能を使用する場合”m”,使用しない場合”i”
c8: 表 12-1 を使用する場合”m”、表 12-2 を使用する場合”x”

※1. Initial INVITE を送信する側
※2. Initial INVITE を受信する側

13.3.6. PRACK リクエスト

表 13-14 / JJ-22.11 PRACK リクエスト設定

項目		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)
Request Line	Method	[1][2]	m	m	
	Request-URI	[1] [2]	m	m	Record-Routing の動作に従う (7 節を参照)
	SIP-Version	[1] [2]	m	m	“SIP/2.0”の固定値
Message HeaderR	Accept	[1] [2]	o	o	
	Accept-Encoding	[1] [2]	o	o	
	Accept-Language	[1] [2]	o	o	
	Allow	[1] [2]	o	o	
	Authorization	[1] [2]	x	o	
	Call-ID	[1] [2]	m	m	
	Content-Disposition	[1] [2]	x	o	
	Content-Encoding	[1] [2]	x	o	
	Content-Language	[1] [2]	x	o	
	Content-Length	[1] [2]	m	o	
Content-Type	[1] [2]	x	o		

CSeq	[1] [2]	m	m	
Date	[1] [2]	o	o	
From	[1] [2]	m	m	
Max-Forwards	[1] [2]	m	o	
MIME-Version	[1] [2]	x	o	
Privacy	[2][5]	x	o	
Proxy-Authorization	[1] [2]	o	o	
Proxy-Require	[1] [2]	x	o	
Record-Route	[1] [2]	x	o	
Require	[1] [2]	x	o	
Route	[1] [2]	o	o	
RAck	[1] [2]	m	m	
Supported	[1] [2]	o	o	
Timestamp	[1] [2]	o	o	
To	[1] [2]	m	m	
User-Agent	[1] [2]	o	o	
Via	[1] [2]	m	m	
その他		i	i	
SDP	[9]	x	o	

※1. PRACK を送信する側
※2. PRACK を受信する側

13.3.7. re-INVITE リクエスト

表 13-15/JJ-22.11 re-INVITE リクエスト設定

項目	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
Request Line	Method	[1]	m	m	
	Request-URI	[1]	m	m	Record-Routing の動作に従う (7 章を参照)
	SIP-Version	[1]	m	m	“SIP/2.0”の固定値
Message Header	Accept	[1]	o	o	
	Accept-Encoding	[1]	o	o	
	Accept-Language	[1]	o	o	
	Alert-Info	[1]	o	o	
	Allow	[1]	o	o	送信時、UPDATE メソッドを使用する場合は”UPDATE”を挿入する。
	Authorization	[1]	x	o	
	Call-ID	[1]	m	m	
	Call-Info	[1]	o	o	
	Contact	[1]	m	m	
	Content-Disposition	[1]	x	o	
	Content-Encoding	[1]	x	o	
	Content-Language	[1]	x	o	
	Content-Length	[1]	m	o	
	Content-Type	[1]	m	m	
	CSeq	[1]	m	m	
	Date	[1]	o	o	
	Expires	[1]	o	o	
	From	[1]	m	m	
	In-Reply-To	[1]	o	o	
	Max-Forwards	[1]	m	o	
	MIME-Version	[1]	x	o	
	Min-SE	[13]	c2	c3	
	Organization	[1]	o	o	
	P-Asserted-Identity	[7]	x	o	
	P-Preferred-Identity	[7]	x	o	
	Priority	[1]	o	o	
	Privacy	[5]	x	o	
Proxy-Authorization	[1]	o	o		
Proxy-Require	[1]	x	o		
Record-Route	[1]	x	o		
Reply-To	[1]	o	o		
Require	[1]	x	o		

Route	[1]	o	o	
Session-Expires	[13]	c4	c3	
Subject	[1]	o	o	
Supported	[1] [13]	c5	c5	
Timestamp	[1]	o	o	
To	[1]	m	m	
User-Agent	[1]	o	o	
Via	[1]	m	m	
その他		i	i	
SDP	[9]	o	m	本文 10 章参照

- c1: UPDATE メソッドを使用する場合”m”,使用しない場合”o”
- c2: セッションタイム拡張機能を使用しかつ同一ダイアログ内で以前に 422(Session Interval Too Small)レスポンス、もしくはセッションリフレッシュリクエスト(INVITE/UPDATE)にて Min-SE ヘッダを受信している場合”m”、セッションタイム拡張機能を使用しかつ同一ダイアログ内で以前に 422(Session Interval Too Small)レスポンス、もしくはセッションリフレッシュリクエスト(INVITE/UPDATE)にて Min-SE ヘッダを受信していない場合”o”、セッションタイム拡張機能を使用しない場合”x”
- c3: セッションタイム拡張機能を使用する場合”m”、使用しない場合”o”
- c4: セッションタイム拡張機能を使用する場合”m”、使用しない場合”x”
- c5: セッションタイム拡張機能を使用する場合”m”,使用しない場合”i”

※1. re-INVITE を送信する側
 ※2. re-INVITE を受信する側

13.3.8. REGISTER リクエスト

表 13-16 / JJ-22.11 REGISTER リクエスト設定

項目	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
Request Line	Method	[1]	m	m	
	Request-URI	[1]	m	m	
	SIP-Version	[1]	m	m	“SIP/2.0”の固定値
Message Header	Accept	[1]	o	o	
	Accept-Encoding	[1]	o	o	
	Accept-Language	[1]	o	o	
	Allow	[1]	o	o	
	Authorization	[1]	c1	c3	
	Call-ID	[1]	m	m	
	Call-Info	[1]	o	o	
	Contact	[1]	c2	m	
	Content-Disposition	[1]	x	x	
	Content-Encoding	[1]	x	x	
	Content-Language	[1]	x	x	
	Content-Length	[1]	m	o	
	Content-Type	[1]	x	x	
	CSeq	[1]	m	m	
	Date	[1]	o	o	
	Expires	[1]	o	o	
	From	[1]	m	m	
	Max-Forwards	[1]	m	o	
	MIME-Version	[1]	x	x	
	Organization	[1]	o	o	
	Privacy	[5]	x	o	
	Proxy-Authorization	[1]	x	x	
	Proxy-Require	[1]	x	o	
Require	[1]	x	o		
Route	[1]	x	o		
Supported	[1]	o	o		
Timestamp	[1]	o	o		
To	[1]	m	m		
User-Agent	[1]	o	o		
Via	[1]	m	m		
その他	[1]	i	i		
SDP	[9]	x	x		

c1: 401(Unauthorized)レスポンスにより認証要求受信後にリクエストを送信する場合”m”、左記以外”x”
 c2: 本文 4.1.7 節に記載されるロケーション情報確認時”x”、左記以外の場合”m”
 c3: 401(Unauthorized)レスポンス送信後にリクエストを受信する場合”m”、左記以外”x”

※1.REGISTER を送信する側（端末側）

※2.REGISTER を受信する側（サーバ側（端末は REGISTER を受信しない））

13.3.9. UPDATE リクエスト

表 13-17/JJ-22.11 UPDATE リクエスト設定

項目		参照	種別 (送信側) ※1	種別 (受信側) ※2	備考（参照節など）
Request Line	Method	[1][4]	m	m	
	Request-URI	[1][4]	m	m	Record-Routing の動作に従う（節を参照）
	SIP-Version	[1][4]	m	m	“SIP/2.0”の固定値
Message Header	Accept	[1][4]	o	o	
	Accept-Encoding	[1][4]	o	o	
	Accept-Language	[1][4]	o	o	
	Allow	[1][4]	o	o	
	Authorization	[1][4]	x	o	
	Call-ID	[1][4]	m	m	
	Call-Info	[1][4]	o	o	
	Contact	[1][4]	m	m	
	Content-Disposition	[1][4]	x	o	
	Content-Encoding	[1][4]	x	o	
	Content-Language	[1][4]	x	o	
	Content-Length	[1][4]	m	o	
	Content-Type	[1][4]	o	o	
	CSeq	[1][4]	m	m	
	Date	[1][4]	o	o	
	From	[1][4]	m	m	
	Max-Forwards	[1][4]	m	o	
	MIME-Version	[1][4]	x	o	
	Min-SE	[4] [13]	c1	c2	
	Organization	[1][4]	o	o	
Privacy	[4][5]	x	o		
Proxy-Authorization	[1][4]	o	o		
Proxy-Require	[1][4]	x	o		
Record-Route	[1][4]	x	o		
Require	[1][4]	x	o		
Route	[1][4]	o	o		

Session-Expires	[4] [13]	c3	c2	
Supported	[1][4] [13]	c4	c4	
Timestamp	[1][4]	o	o	
To	[1][4]	m	m	
User-Agent	[1][4]	o	o	
Via	[1][4]	m	m	
その他		i	i	
SDP	[9]	o	m	

c1: セッションタイム拡張機能を使用しかつ同一ダイアログ内で以前に 422(Session Interval Too Small)レスポンス、もしくはセッションリフレッシュリクエスト(INVITE/UPDATE)にて Min-SE ヘッダを受信している場合”m”、セッションタイム拡張機能を使用しかつ同一ダイアログ内で以前に 422(Session Interval Too Small)レスポンス、もしくはセッションリフレッシュリクエスト(INVITE/UPDATE)にて Min-SE ヘッダを受信していない場合”o”、セッションタイム拡張機能を使用しない場合”x”

c2: セッションタイム拡張機能を使用する場合”m”、使用しない場合”o”

c3: セッションタイム拡張機能を使用する場合”m”、使用しない場合”x”

c4: セッションタイム拡張機能を使用する場合”m”、使用しない場合”i”

※1.UPDATE を送信する側
 ※2.UPDATE を受信する側

13.4. SIP レスポンス信号

本規定が扱う各 SIP リクエスト信号 (表 13-1 参照) に対する各レスポンス信号におけるヘッダ一覧を記載する。

13.4.1. BYE リクエストに対するレスポンス

表 13-18/JJ-22.11 BYE リクエストに対するレスポンス設定

項目	status-Code	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
status-Line	SIP-Version	全 code	[1]	m	m	“SIP/2.0”の固定値
	Status-Code	全 code	[1]	m	m	
	Reason-Phrase	全 code	[1]	m	o	
Message Header	Accept	415	[1]	m	o	
	Accept-Encoding	415	[1]	m	o	
	Accept-Language	415	[1]	m	o	
	Allow	1xx,2xx	[1]	o	o	
	Allow	300~699	[1]	o	o	
	Allow	405	[1]	m	o	
	Authentication-Info	2xx	[1]	o	o	
	Call-ID	全 code	[1]	m	m	
	Contact	3xx 485	[1]	o	o	
	Content-Disposition	全 code	[1]	x	o	
	Content-Encoding	全 code	[1]	x	o	
	Content-Language	全 code	[1]	x	o	
	Content-Length	全 code	[1]	m	o	
	Content-Type	全 code	[1]	x	o	
	CSeq	全 code	[1]	m	m	
	Date	全 code	[1]	o	o	
	Error-Info	300-699	[1]	o	o	
	From	全 code	[1]	m	m	
	MIME-Version	全 code	[1]	x	o	
	P-Asserted-Identity	全 code	[7]	x	o	
	P-Preferred-Identity	全 code	[7]	x	o	
	Privacy		[5]	x	o	
	Proxy-Authenticate	401	[1]	x(端末) o(サーバ)	o(端末) x(サーバ)	BYE での認証は非推奨とする
	Proxy-Authenticate	407	[1]	x(端末) o(サーバ)	o(端末) x(サーバ)	BYE での認証は非推奨とする
	Record-Route	2xx, 18x	[1]	x	o	
	Require	全 code	[1]	x	o	
	Retry-After	404,413,480,486, 500,503, 600,603	[1]	o	o	
	Server	全 code	[1]	o	o	
Supported	2xx	[1]	o	o		
Timestamp	全 code	[1]	o	o		
To	全 code	[1]	m	m		
Unsupported	420	[1]	m	o		

User-Agent	全 code	[1]	o	o	
Via	全 code	[1]	m	m	
Warning	全 code	[1]	o	o	
www-Authenticate	401	[1]	x(端末) o(サーバ)	o(端末) x(サーバ)	BYE での認証は非推奨とする
	407		x	o(端末) x(サーバ)	
その他			i	i	
SDP		[9]	x	o	
※1. BYEを受信してレスポンスを送信する側 ※2. BYEを送信してレスポンスを受信する側					

13.4.2. CANCEL リクエストに対するレスポンス

表 13-19/JJ-22.11 CANCEL リクエストに対するレスポンス設定

項目	status-Code	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
status-Line	SIP-Version	全 code	[1]	m	m	“SIP/2.0”の固定値
	Status-Code	全 code	[1]	m	m	
	Reason-Phrase	全 code	[1]	m	o	
Message Header	Call-ID	全 code	[1]	m	m	
	Content-Length	全 code	[1]	m	o	
	CSeq	全 code	[1]	m	m	
	Date	全 code	[1]	o	o	
	Error-Info	300-699	[1]	o	o	
	From	全 code	[1]	m	m	
	Proxy-Authenticate	401	[1]	x(端末) o(サーバ)	o(端末) x(サーバ)	CANCEL での認証は非推奨とする
	Privacy	全 code	[5]	x	o	
	Record-Route	2xx, 18x	[1]	x	o	
	Retry-After	404,413,480,486, 500,503, 600,603	[1]	o	o	
	Server	全 code	[1]	o	o	
	Supported	2xx	[1]	o	o	
	Timestamp	全 code	[1]	o	o	
	To	全 code	[1]	m	m	
	User-Agent	全 code	[1]	o	o	
Via	全 code	[1]	m	m		
Warning	全 code	[1]	o	o		
その他			i	i		
SDP		[9]	x	o		

※1.CANCEL を受信してレスポンスを送信する側
 ※2.CANCEL を送信してレスポンスを受信する側

13.4.3. Initial INVITE リクエストに対するレスポンス

表 13-20/JJ-22.11 Initial INVITE リクエストに対するレスポンス設定

項目	Status-Code	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
status-Line	SIP-Version	全 code	[1]	m	m	“SIP/2.0”の固定値
	Status-Code	全 code	[1]	m	m	
	Reason-Phrase	全 code	[1]	m	o	
Message Header	Accept	2xx	[1]	o	o	
	Accept	415	[1]	m	o	
	Accept-Encoding	2xx	[1]	o	o	
	Accept-Encoding	415	[1]	m	o	
	Accept-Language	2xx	[1]	o	o	
	Accept-Language	415	[1]	m	o	
	Alert-Info	180	[1]	o	o	
	Allow	1xx,2xx	[1]	o	c1	送信時、100rel 拡張機能を使用する場合は”PRACK“を挿入し、UPDATE メソッドを使用する場合は”UPDATE”を挿入する。
	Allow	300~699	[1]	o	o	
	Allow	405	[1]	m	o	
	Authentication-Info	2xx	[1]	o	o	
	Call-ID	全 code	[1]	m	m	
	Call-Info	全 code	[1]	o	o	
	Contact	1xx,	[1]	c2	c2	
		2xx	[1]	m	m	
	Contact	300-699	[1]	o	o	
	Contact	485	[1]	o	o	
	Content-Disposition	全 code	[1]	x	o	
	Content-Encoding	全 code	[1]	x	o	
	Content-Language	全 code	[1]	x	o	
	Content-Length	全 code	[1]	m	o	
	Content-Type	1xx	[1]	o	m	企業網ではアーリーメディア対応
	Content-Type	2xx	[1]	m	m	
	Content-Type	300-699	[1]	x	o	
	CSeq	全 code	[1]	m	m	
	Date	全 code	[1]	o	o	
	Error-Info	300-699	[1]	o	o	
Expires	全 code	[1]	o	o		
From	全 code	[1]	m	m		
MIME-Version	全 code	[1]	x	o		
Min-SE	422	[13]	m	m		

Organization	全 code	[1]	o	o	
P-Asserted-Identity		[7]	x	o	
P-Preferred-Identity		[7]	x	o	
Privacy		[5][7]	x	o	
Proxy-Authenticate	401	[1]	x(端末) o(サーバ)	o(端末) x(サーバ)	
Proxy-Authenticate	407	[1]	x(端末) m(サーバ)	m(端末) x(サーバ)	
Record-Route	2xx,18x	[1]	o	o	
Reply-To	全 code	[1]	o	o	
Require	1xx	[1][2]	c3	c4	
Require	2xx	[1] [13]	c5	c6	
Require	300-699	[1]	x	o	
Retry-After	404,413,480,486,500,503,600,603	[1]	o	o	
RSeq	1xx	[1][2]	c3	c4	
Server	全 code	[1]	o	o	
Session-Expires	2xx	[13]	c7	c6	
Supported	2xx	[1]	c6	i	
Timestamp	全 code	[1]	o	o	
To	全 code	[1]	m	m	
User-Agent	全 code	[1]	o	o	
Unsupported	420	[1]	m	o	
Via	全 code	[1]	m	m	
Warning	全 code	[1]	o	o	
WWW-Authenticate	401	[1]	x(端末) m(サーバ)	m(端末) x(サーバ)	
	407		x	o(端末) x(サーバ)	
	その他	全 code		i	i
SDP	1xx	[9]	o	m	
	2xx	[9]	m	m	
	3xx/4xx/5xx/6xx	[9]	x	o	

c1: 100rel 拡張機能もしくは UPDATE メソッドを使用する場合”m”,使用しない場合”o”

c2: 100rel 拡張機能を使用する場合”m”,使用しない場合”o”

c3: 100rel 拡張機能を使用し、且つ受信した INVITE リクエストに Supported ヘッダがあり”100rel”が設定されていた場合”m”,左記以外”x”

c4: 100rel 拡張機能を使用する場合”m”,使用しない場合”i”

c5: セッションタイム拡張機能を使用し、且つ受信した INVITE リクエストに Supported ヘッダがあり”timer”が設定されていた場合”m”,左記以外”x”

c6: セッションタイム拡張機能を使用する場合”m”,使用しない場合”i”

c7: セッションタイム拡張機能を使用し、且つ受信した INVITE リクエストに Session-Expires ヘッダが設定されていた場合”m”,左記以外”x”

※1.Initial INVITE リクエストを受信して、レスポンスを送信する側

※2.Initial INVITE リクエストを送信して、レスポンスを受信する側

13.4.4. PRACK リクエストに対するレスポンス

表 13-21/JJ-22.11 PRACK リクエストに対するレスポンス設定

項目	Status-Code	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
status-Line	SIP-Version	全 code	[1][2]	m	m	“SIP/2.0”の固定値
	Status-Code	全 code	[1][2]	m	m	
	Reason-Phrase	全 code	[1][2]	m	o	
Message-HeaderR	Accept	415	[1][2]	m	o	
	Accept-Encoding	415	[1][2]	m	o	
	Accept-Language	415	[1][2]	m	o	
	Allow	全 code	[1][2]	o	o	
	Authentication-Info	2xx	[1][2]	o	o	
	Call-ID	全 code	[1][2]	m	m	
	Contact	3xx 485	[1][2]	o	o	
	Content-Disposition	全 code	[1][2]	x	o	
	Content-Encoding	全 code	[1][2]	x	o	
	Content-Language	全 code	[1][2]	x	o	
	Content-Length	全 code	[1][2]	m	o	
	Content-Type	全 code	[1][2]	x	o	
	CSeq	全 code	[1][2]	m	m	
	Date	全 code	[1][2]	o	o	
	Error-Info	300-699	[1][2]	o	o	
	From	全 code	[1][2]	m	m	
	MIME-Version	全 code	[1][2]	x	o	
	Privacy	全 code	[5]	x	o	
	Proxy-Authenticate	401	[1][2]	x(端末) o(サーバ)	o(端末) x(サーバ)	PRACK での認証は非推奨とする
	Proxy-Authenticate	407	[1][2]	x(端末) o(サーバ)	o(端末) x(サーバ)	PRACK での認証は非推奨とする
	Record-Route	2xx,18x	[1][2]	x	o	
	Require	全 code	[1][2]	x	o	
	Retry-After	404,413,480,486,500,503,600,603	[1][2]	o	o	
	Server	全 code	[1][2]	o	o	
Supported	2xx	[1][2]	o	o		
Timestamp	全 code	[1][2]	o	o		
To	全 code	[1][2]	m	m		

Unsupported	420	[1][2]	m	o	
User-Agent	全 code	[1][2]	o	o	
Via	全 code	[1][2]	m	m	
WWW-Authenticate	401	[1][2]	x(端末) o(サーバ)	o(端末) x(サーバ)	PRACK での認証は非推奨とする
	407		x	o(端末) x(サーバ)	
その他	全 code		i	i	
SDP	全 code	[9]	x	o	

※1.PRACK リクエストを受信して、レスポンスを送信する側
 ※2.PRACK リクエストを送信して、レスポンスを受信する側

13.4.5. re-INVITE リクエストに対するレスポンス

表 13-22/JJ-22.11 re-INVITE リクエストに対するレスポンス設定

項目	Status-Code	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
status-Line	SIP-Version	全 code	[1]	m	m	“SIP/2.0”の固定値
	Status-Code	全 code	[1]	m	m	
	Reason-Phrase	全 code	[1]	m	o	
Message Header]	Accept	2xx	[1]	o	o	
	Accept	415	[1]	m	o	
	Accept-Encoding	2xx	[1]	o	o	
	Accept-Encoding	415	[1]	m	o	
	Accept-Language	2xx	[1]	o	o	
	Accept-Language	415	[1]	m	o	
	Alert-Info	180	[1]	o	o	
	Allow	2xx	[1]	o	c1	送信時、UPDATE メソッドを使用する場合は”UPDATE”を挿入する。
	Allow	300～699	[1]	o	o	
	Allow	405	[1]	m	o	
	Authentication-Info	2xx	[1]	o	o	
	Call-ID	全 code	[1]	m	m	
	Call-Info	全 code	[1]	o	o	
	Contact	2xx	[1]	m	m	
	Contact	300-699	[1]	o	o	
	Contact	485	[1]	o	o	
	Content-Disposition	全 code	[1]	x	o	
	Content-Encoding	全 code	[1]	x	o	
	Content-Language	全 code	[1]	x	o	
	Content-Length	全 code	[1]	m	o	
	Content-Type	2xx	[1]	m	m	
	Content-Type	300-699	[1]	x	o	
	CSeq	全 code	[1]	m	m	
	Date	全 code	[1]	o	o	
	Error-Info	300-699	[1]	o	o	
	Expires	全 code	[1]	o	o	
	From	全 code	[1]	m	m	
MIME-Version	全 code	[1]	x	o		
Min-SE	422	[13]	m	m		
Organization	全 code	[1]	o	o		
P-Asserted-Identity	全 code	[7]	x	o		

P-Preferred-Identity	全 code	[7]	x	o	
Privacy	全 code	[5]	x	o	
Proxy-Authenticate	401	[1]	x(端末) o(サーバ)	o(端末) x(サーバ)	re-INVITE での認証は非推奨とする
Proxy-Authenticate	407	[1]	x(端末) m(サーバ)	m(端末) x(サーバ)	re-INVITE での認証は非推奨とする
Record-Route	2xx	[1]	x	o	
Reply-To	全 code	[1]	o	o	
Require	2xx	[1] [13]	c2	c3	
Require	300-699	[1]	x	o	
Retry-After	404,413, 480,486, 500,503, 600,603	[1]	o	o	
Server	全 code	[1]	o	o	
Session-Expires	2xx	[1] [13]	c4	c3	
Supported	2xx	[1] [13]	c3	i	
Timestamp	全 code	[1]	o	o	
To	全 code	[1]	m	m	
User-Agent	全 code	[1]	o	o	
Unsupported	420	[1]	m	o	
Via	全 code	[1]	m	m	
Warning	全 code	[1]	o	o	
WWW-Authenticate	401	[1]	x(端末) m(サーバ)	m(端末) x(サーバ)	re-INVITE での認証は非推奨とする
	407		x	o(端末) x(サーバ)	
	その他	全 code		I	i
SDP	2xx	[9]	m	m	
	3xx/4xx/ 5xx/6xx	[9]	x	o	

c1: UPDATE メソッドを使用する場合”m”,使用しない場合”o”

c2: セッションタイム拡張機能を使用し、且つ受信した re-INVITE リクエストに Supported ヘッダがあり”timer”が設定されていた場合”m”、左記以外”i”

c3: セッションタイム拡張機能を使用する場合”m”、使用しない場合”i”

c4: セッションタイム拡張機能を使用し、且つ受信した re-INVITE リクエストに Session-Expires ヘッダが設定されていた場合”m”、左記以外”x”

※1.re-INVITE リクエストを受信して、レスポンスを送信する側

※2.re-INVITE リクエストを送信して、レスポンスを受信する側

13.4.6. REGISTER リクエストに対するレスポンス

表 13-23/JJ-22.11 REGISTER リクエストに対するレスポンス設定

項目	Status-Code	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
status-Line	SIP-Version	全 code	[1]	m	m	“SIP/2.0”の固定値
	Status-Code	全 code	[1]	m	m	
	Reason-Phrase	全 code	[1]	m	o	
Message Header	Accept	2xx	[1]	o	o	
	Accept	415	[1]	o	o	
	Accept-Encoding	2xx	[1]	o	o	
	Accept-Encoding	415	[1]	o	o	
	Accept-Language	2xx	[1]	o	o	
	Accept-Language	415	[1]	o	o	
	Allow	全 code	[1]	o	o	
	Authentication-Info	2xx	[1]	o	o	
	Call-ID	全 code	[1]	m	m	
	Call-Info	全 code	[1]	o	o	
	Contact	2xx,	[1]	m	m	
	Contact	3xx	[1]	o	o	
	Contact	485	[1]	o	o	
	Content-Disposition	全 code	[1]	x	o	
	Content-Encoding	全 code	[1]	x	o	
	Content-Language	全 code	[1]	x	o	
	Content-Length	全 code	[1]	m	o	
	Content-Type	全 code	[1]	x	o	
	CSeq	全 code	[1]	m	m	
	Date	全 code	[1]	o	o	
	Error-Info	300-699	[1]	o	o	
	Expires	全 code	[1]	m	m	
	From	全 code	[1]	m	m	
Min-Expires	423	[13]	m	m		
MIME-Version	全 code	[1]	x	o		
Organization	全 code	[1]	o	o		

Privacy		[5]	o	o	
Proxy-Authenticate	401 407	[1]	x	x	
Require	全 code	[1]	o	o	
Retry-After	404,413,480,486, 500,503, 600,603	[1]	o	o	
Server	全 code	[1]	o	o	
Supported	2xx	[1]	o	o	
Timestamp	全 code	[1]	o	o	
To	全 code	[1]	m	m	
Unsupported	420	[1]	o	o	
User-Agent	全 code	[1]	o	o	
Via	全 code	[1]	m	m	
Warning	全 code	[1]	o	o	
WWW-Authenticate	401	[1]	m	m	
WWW-Authenticate	407	[1]	x	x	
その他	全 code		i	i	
SDP	全 code	[9]	x	x	

※1.REGISTER リクエストを受信して、レスポンスを送信する側（サーバ側）
 ※2.REGISTER リクエストを送信して、レスポンスを受信する側（端末側）

13.4.7. UPDATE リクエストに対するレスポンス

表 13-24/ JJ-22.11 UPDATE リクエストに対するレスポンス設定

項目	Status-Code	参照	種別 (送信側) ※1	種別 (受信側) ※2	備考 (参照節など)	
status-Line	SIP-Version	全 code	[1][4]	m	m	“SIP/2.0”の固定値
	Status-Code	全 code	[1][4]	m	m	
	Reason-Phrase	全 code	[1][4]	m	o	
Message Header	Accept	2xx	[1][4]	o	o	
	Accept	415	[1][4]	m	o	
	Accept-Encoding	2xx	[1][4]	o	o	
	Accept-Encoding	415	[1][4]	m	o	
	Accept-Language	2xx	[1][4]	o	o	
	Accept-Language	415	[1][4]	m	o	
	Allow	2xx	[1][4]	o	c1	
	Allow	300～699	[1][4]	o	o	
	Allow	405	[1][4]	m	o	
	Authentication-Info	2xx	[1][4]	o	o	
	Call-ID	全 code	[1][4]	m	m	
	Call-Info	全 code	[1][4]	o	o	
	Contact	2xx	[1][4]	m	m	
	Contact	300-699	[1][4]	o	o	
	Contact	485	[1][4]	o	o	
	Content-Disposition	全 code	[1][4]	x	o	
	Content-Encoding	全 code	[1][4]	x	o	
	Content-Language	全 code	[1][4]	x	o	
	Content-Length	全 code	[1][4]	m	o	
	Content-Type	2xx	[1][4]	c2	c3	
	Content-Type	300-699	[1][4]	x	o	
	CSeq	全 code	[1][4]	m	m	
	Date	全 code	[1][4]	o	o	
	Error-Info	300-699	[1][4]	o	o	
	From	全 code	[1][4]	m	m	
	MIME-Version	全 code	[1][4]	x	o	
	Min-SE	422	[13]	m	m	
	Organization	全 code	[1][4]	o	o	
	Privacy	全 code	[5]	x	o	
	Proxy-Authenticate	401	[1][4]	x(端末) m(サーバ)	m(端末) x(サーバ)	UPDATE での認証は非推奨とする
Proxy-Authenticate	407	[1][4]	x(端末) o(サーバ)	o(端末) x(サーバ)	UPDATE での認証は非推奨とする	
Record-Route	2xx	[1][4]	x	o		

Reply-To	全 code	[1][4]	o	o	
Require	2xx	[1][4] [13]	c4	c5	
Require	300-699	[1][4]	x	o	
Retry-After	404,413, 480,486, 500,503, 600,603	[1][4]	o	o	
Server	全 code	[1][4]	o	o	
Session-Expires	2xx	[13]	c6	c5	
Supported	2xx	[1][4]	c5	i	
Timestamp	全 code	[1][4]	o	o	
To	全 code	[1][4]	m	m	
User-Agent	全 code	[1][4]	o	o	
Unsupported	420	[1][4]	m	o	
Via	全 code	[1][4]	m	m	
Warning	全 code	[1][4]	o	o	
WWW-Authenticate	401	[1][4]	x(端末) m(サーバ)	m(端末) x(サーバ)	UPDATE での認証は非推奨とする
	407		x	o(端末) x(サーバ)	
その他	全 code		i	i	
SDP	2xx	[9]	c1	c7	
	3xx/4xx/ 5xx/6xx	[9]	x	o	

c1: ・セッション変更の場合は”m”。

・リフレッシュの場合は”o”。

c1: 受信した UPDATE リクエストに SDP が含まれている場合”m”、左記以外”o”

c2: 送信した UPDATE リクエストに SDP を含んでいた場合”m”、左記以外”o”

c3: セッションタイマ拡張機能を使用し、且つ受信した UPDATE リクエストに Supported ヘッダがあり”timer”が設定されていた場合”m”、左記以外”i”

c4: セッションタイマ拡張機能を使用する場合”m”、使用しない場合”i”

c5: セッションタイマ拡張機能を使用し、且つ受信した UPDATE リクエストに Session-Expires ヘッダが設定されていた場合”m”、左記以外”i”

c6: 送信した UPDATE リクエストに SDP を含んでいた場合”m”、左記以外”o”

※1.UPDATE リクエストを受信して、レスポンスを送信する側

※2.UPDATE リクエストを送信して、レスポンスを受信する側

付録 i. シーケンス例

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付けであり、私設総合サービス網交換機 (PINX) のサービス内容や端末の機能により、適宜変更が必要となる場合がある。また、本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。

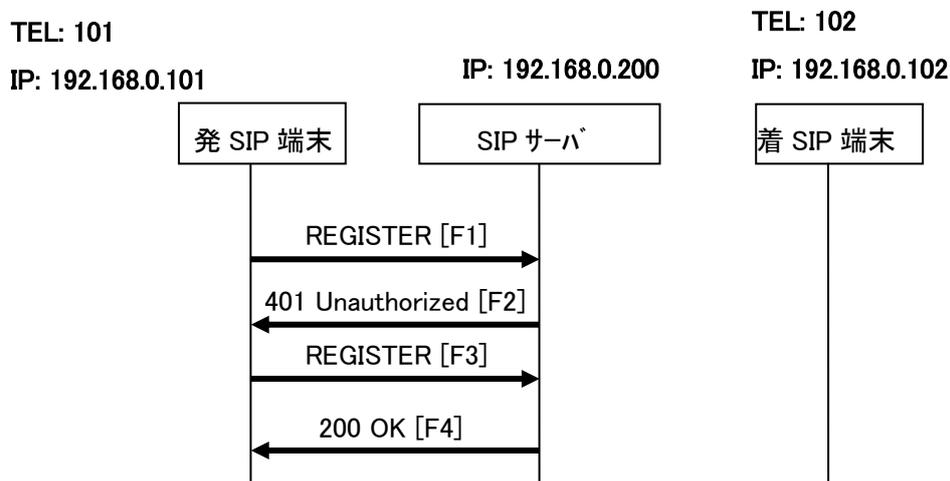
付表 i -1 / JJ-22.11 掲載シーケンス例一覧

No	シーケンス名	備考
1	REGISTER 登録	付図 i -1
2	REGISTER 指定削除	付図 i -2
3	REGISTER 全指定削除	付図 i -3
4	接続シーケンス 1 (発着 100rel 動作、発着 timer 動作、発着 UPDATE 動作)	付図 i -4
5	接続シーケンス 2 (発着 100rel 未動作、発着 timer 動作、発着 UPDATE 未動作)	付図 i -5
6	接続シーケンス 3 (発着 100rel 未動作、発着 timer 未動作、発着 UPDATE 未動作)	付図 i -6
7	接続シーケンス 4 (INVITE 認証付)	付図 i -7

i.1 REGISTER 登録

REGISTER 登録シーケンス例を付図 i-1 に示す。

なお、レジストレーション・サーバ機能は SIP サーバに具備されているものとする。また、各メッセージ例を付記する。



付図 i -1/JJ-22.11 REGISTER 登録

メッセージ詳細例

F1 REGISTER

```
REGISTER sip:192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs394ec0a4f
Max-Forwards: 70
Call-ID: 0477e902-e4630c1887cc3437bb900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3516156121
To: <sip:101@192.168.0.200>
CSeq: 1 REGISTER
Allow: INVITE,ACK,CANCEL,BYE,UPDATE
Contact: <sip:101@192.168.0.101:5060>
Expires: 3600
Content-Length: 0
```

F2 401 Unauthorized

```
Status-Line: SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs394ec0a4f
Call-ID: 0477e902-e4630c1887cc3437bb900080f0bf882c@192.168.0.101
```

From: <sip: 101@192.168.0.200>;tag=3516156121
To: <sip: 101@192.168.0.200>;tag=1387512496
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="RegisteredUsers",
 nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",algorithm=MD5
Content-Length: 0

F3 REGISTER

Request-Line: REGISTER sip:192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsf15debb70
Max-Forwards: 70
Call-ID: 0477e902-e4630c1887cc3437bb900080f0bf882c@192.168.0.101
From: <sip: 101@192.168.0.200>;tag=3516156121
To: <sip: 101@192.168.0.200>
CSeq: 2 REGISTER
Authorization: Digest realm="RegisteredUsers",nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",
 algorithm=MD5,uri="sip:192.168.0.200:5060",username="360",
 response="997c057f45c34b61bda81f2e0c16745b"
Contact: <sip:101@192.168.0.101:5060>
Expires: 3600
Content-Length: 0

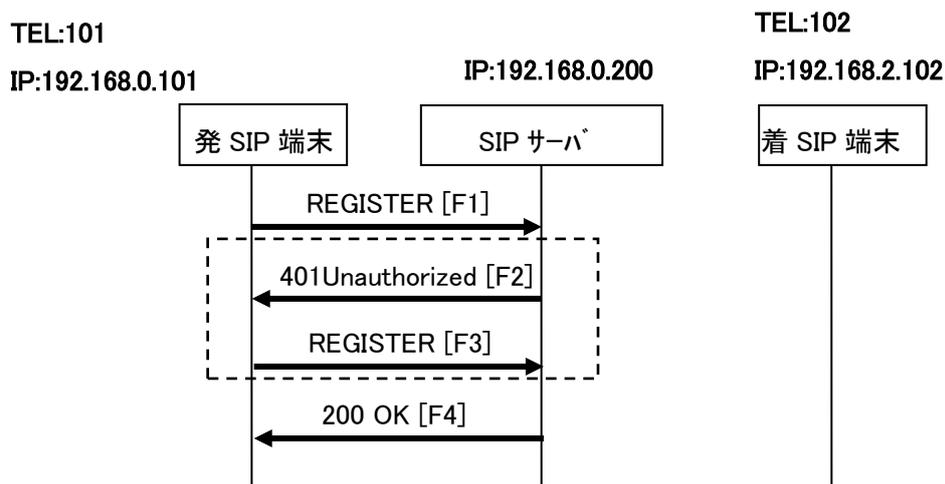
F4 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsf15debb70
Call-ID: 0477e902-e4630c1887cc3437bb900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3516156121
To: <sip:101@192.168.0.200>;tag=1591016740
CSeq: 2 REGISTER
Contact: <sip:101@192.168.0.101:5060>;expires=3600
Expires: 3600
Content-Length: 0

i.2 REGISTER 指定削除

REGISTER 登録されたコンタクト情報を指定削除するシーケンス例（認証シーケンスは省略）を付図 i-2 に示す。[F2]および[F3]は REGISTER 認証を用いる場合のシーケンスであり、装置によっては省略可能。

なお、レジストレーション・サーバ機能は SIP サーバに具備されているものとする。また、各メッセージ例を付記する。



付図 i -2/JJ-22.11 REGISTER 指定削除

メッセージ詳細例

F1 REGISTER

```
Request-Line: REGISTER sip:192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa4120f
Max-Forwards: 70
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>
CSeq: 1 REGISTER
Contact: <sip:101@192.168.0.101:5060>
Expires: 0
Content-Length: 0
```

F2 401 Unauthorized

```
Status-Line: SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa4120f
```

From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>;tag=1755
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="RegisteredUsers", nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",
algorithm=MD5
Expires: 0
Content-Length: 0

F3 REGISTER

Request-Line: REGISTER sip:192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa41200
Max-Forwards: 70
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>
CSeq: 2 REGISTER
Authorization: Digest realm="RegisteredUsers",nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",
algorithm=MD5,uri="sip:192.168.0.200:5060",username="360",
response="997c057f45c34b61bda81f2e0c16745b"
Contact: <**sip: 101@192.168.0. 101:5060**>
Expires: 0
Content-Length: 0

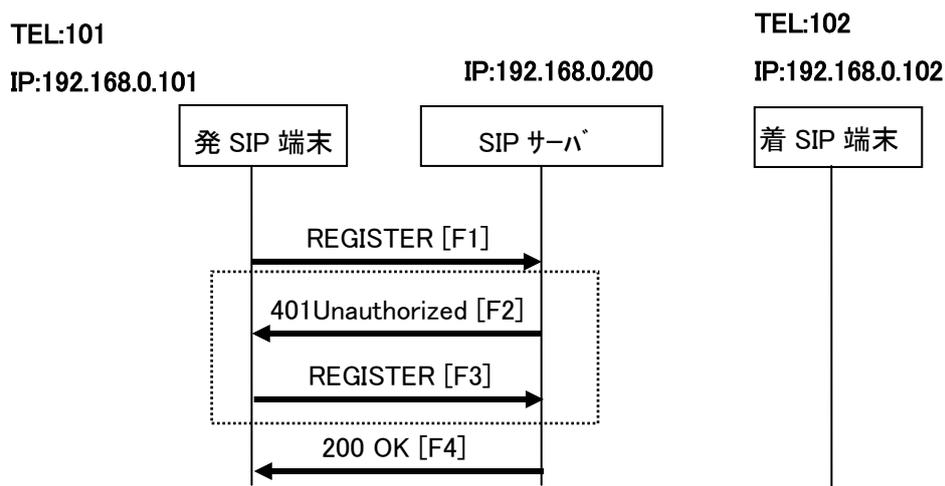
F4 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa41200
From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>;tag=1750
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
CSeq: 2 REGISTER
Expires: 0
Contact: <**sip: 101@192.168.0. 101:5060**>
Content-Length: 0

i.3 REGISTER 全指定削除

REGISTER 登録されたコンタクト情報を全指定削除するシーケンス例（認証シーケンスは省略）を付図 i-3 に示す。[F2]および[F3]は REGISTER 認証を用いる場合のシーケンスであり、装置によっては省略可能。

なお、レジストレーション・サーバ機能は SIP サーバに具備されているものとする。また、各メッセージ例を付記する。



付図 i -3/JJ-22.11 REGISTER 全指定削除

メッセージ詳細例

F1 REGISTER

```
Request-Line: REGISTER sip:192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa4120f
Max-Forwards: 70
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>
CSeq: 1 REGISTER
Contact: *
Expires: 0
Content-Length: 0
```

F2 401 Unauthorized

```
Status-Line: SIP/2.0 401 Unauthorized
```

Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa4120f
From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>;tag=1755
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="RegisteredUsers",
 nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",algorithm=MD5
Expires: 0
Content-Length: 0

F3 REGISTER

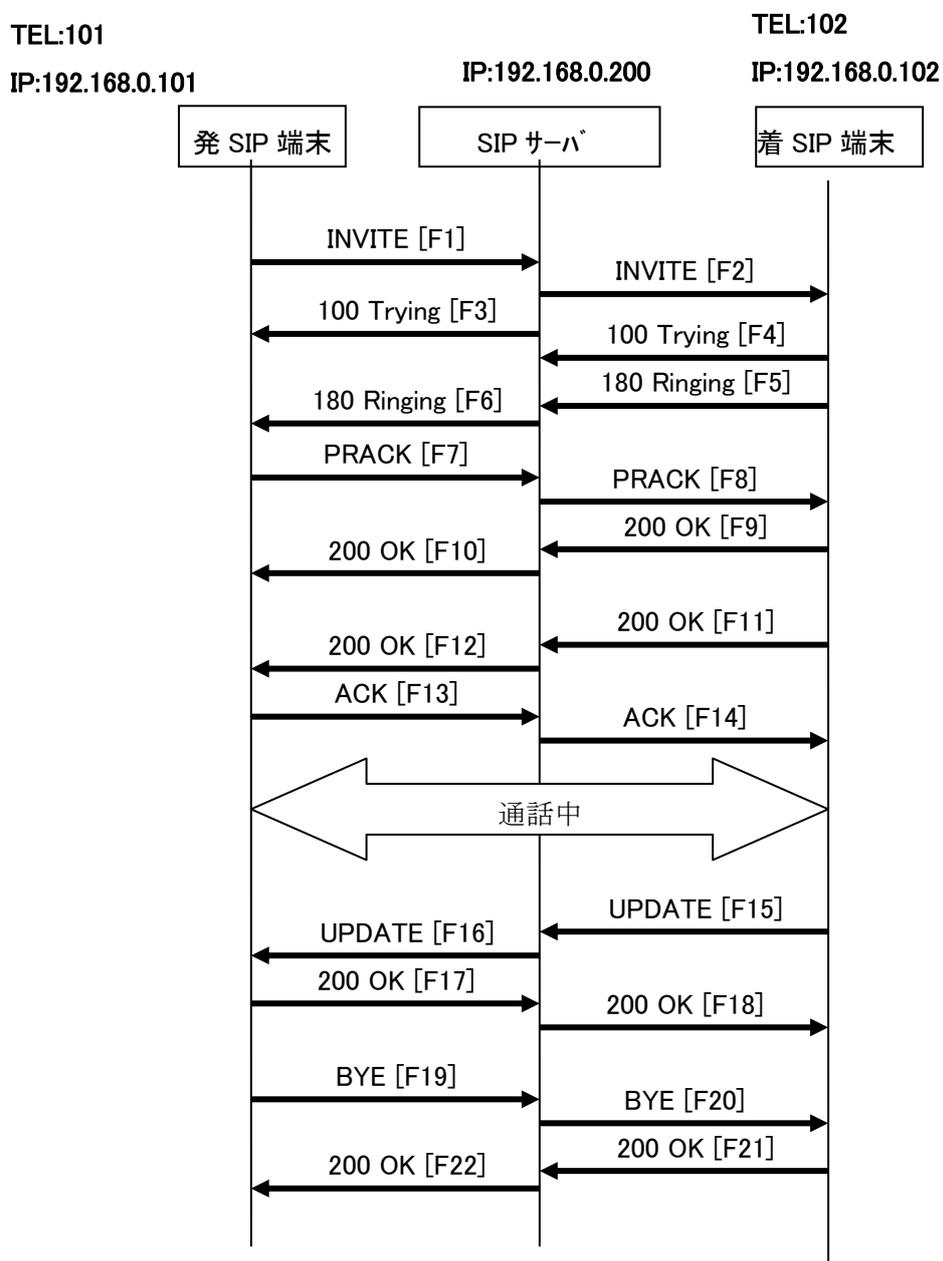
Request-Line: REGISTER sip:192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa41200
Max-Forwards: 70
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>
CSeq: 2 REGISTER
Authorization: Digest realm="RegisteredUsers",nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",
 algorithm=MD5,uri="sip:192.168.0.200:5060",username="360",
 response="997c057f45c34b61bda81f2e0c16745b"
Contact: *
Expires: 0
Content-Length: 0

F4 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs31aa41200
From: <sip:101@192.168.0.200>;tag=181520611
To: <sip:101@192.168.0.200>;tag=1750
Call-ID: 2bb87709-e8c60d1828f0b900c89e0080f0e8b136@192.168.0.101
CSeq: 2 REGISTER
Expires: 0
Contact: *
Content-Length: 0

i.4 接続シーケンス 1 (発着 100rel 動作、発着 timer 動作、発着 UPDATE 動作)

発着 100rel 動作、発着 timer 動作、発着 UPDATE 動作時の呼接続シーケンス例 (認証シーケンスは省略) を付図 i-4 に示す。また、各メッセージ例を付記する。



付図 i-4/JJ-22.11 接続シーケンス 1

メッセージ詳細例

F1 INVITE

Request-Line: INVITE sip:102@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsdaef515f
Max-Forwards: 70
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE
Supported: 100rel,timer
Contact: <sip:101@192.168.0.101:5060>
Session-Expires: 180
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 4 4 IN IP4 192.168.0.101
s= -
c= IN IP4 192.168.0.101
t= 0 0
m= audio 8014 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F2 INVITE

Request-Line: INVITE sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560127171000623
From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>
Content-Type: application/sdp
Call-ID: 14241-72f0b6@192.168.0.200
CSeq: 1 INVITE
Contact: <sip:101@192.168.0.200:5060>
Max-Forwards: 70
Content-Length: 118
Supported: 100rel, timer
Allow: ACK,BYE,CANCEL,INVITE,PRACK,UPDATE
Session-Expires: 180
v= 0
o= - 5 7 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0

m= audio 20000 RTP/AVP 0
a= rtpmap:0 PCMU/8000

F3 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsdaef515f
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
CSeq: 2 INVITE
Content-Length: 0

F4 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560127171000623
Call-ID: 14241-72f0b6@192.168.0.200
From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>
CSeq: 1 INVITE
Content-Length: 0

F5 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560127171000623
Call-ID: 14241-72f0b6@192.168.0.200
From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>;tag=4244609427
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE
Supported: 100rel,timer
Contact: <sip:102@192.168.0.102:5060>
Require: 100rel
RSeq: 1
Content-Length: 0

F6 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsdaeaf515f
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>;tag=6627
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
CSeq: 2 INVITE
Contact: <sip:102@192.168.0.200:5060>
Content-Length: 0
Allow: ACK,BYE,CANCEL,INVITE,PRACK,UPDATE
Supported: 100rel, timer
Require: 100rel
RSeq: 1

F7 PRACK

Request-Line: PRACK sip:102@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs4eaecf6ef
Max-Forwards: 70
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>;tag=6627
CSeq: 3 PRACK
RAck: 1 2 INVITE
Content-Length: 0

F8 PRACK

Request-Line: PRACK sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560127265000726
From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>;tag=4244609427
Call-ID: 14241-72f0b6@192.168.0.200
CSeq: 2 PRACK
RAck: 1 1 INVITE
Max-Forwards: 70
Content-Length: 0

F9 200 OK

Status-Line: SIP/2.0 200 OK

Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560127265000726
Call-ID: 14241-72f0b6@192.168.0.200
From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>;tag=4244609427
CSeq: 2 PRACK
Content-Length: 0

F10 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs4eaecf6ef
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>;tag=6627
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
CSeq: 3 PRACK
Content-Length: 0

F11 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560127171000623
Call-ID: 14241-72f0b6@192.168.0.200
From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>;tag=4244609427
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE
Supported: 100rel, timer
Contact: <sip:102@192.168.0.102:5060>
Require: timer
Session-Expires: 180;refresher=uas
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 2 2 IN IP4 192.168.0.102
s= -
c= IN IP4 192.168.0.102
t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F12 200 OK

Status-Line: SIP/2.0 200 OK
Content-Type: application/sdp
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsdaef515f
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>;tag=6627
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
CSeq: 2 INVITE
Contact: <sip:102@192.168.0.200:5060>
Content-Length: 129
Allow: ACK,BYE,CANCEL,INVITE,PRACK,UPDATE
Supported: 100rel, timer
Session-Expires: 180;refresher=uas
v= 0
o= - 5 7 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 20000 RTP/AVP 0
a= rtpmap:0 PCMU/8000

F13 ACK

Request-Line: ACK sip:102@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs746ab01df
Max-Forwards: 70
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>;tag=6627
CSeq: 2 ACK
Content-Length: 0

F14 ACK

Request-Line: ACK sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560129359000727
Max-Forwards: 70
Call-ID: 14241-72f0b6@192.168.0.200
From: <sip:101@192.168.0.200>;tag=1967

To: <sip:102@192.168.0.200>;tag=4244609427
CSeq: 1 ACK
Content-Length: 0

F15 UPDATE

Request-Line: UPDATE sip:101@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKsd8c80456f
Max-Forwards: 70
Call-ID: 14241-72f0b6@192.168.0.200
From: <sip:102@192.168.0.200>;tag=4244609427
To: <sip:101@192.168.0.200>;tag=1967
CSeq: 1 UPDATE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE
Supported: timer
Contact: <sip:102@192.168.0.102:5060>
Session-Expires: 180;refresher=uac
Content-Length: 0

F16 UPDATE

Request-Line: UPDATE sip:101@192.168.0.101:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560082718000749
From: <sip:102@192.168.0.200>;tag=6627
To: <sip:101@192.168.0.200>;tag=3471845493
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
CSeq: 2 UPDATE
Contact: <sip:102@192.168.0.200:5060>
Max-Forwards: 70
Content-Length: 0
Supported: timer
Session-Expires: 180;refresher=uac
Allow: ACK,BYE,CANCEL,INVITE,PRACK,UPDATE

F17 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560082718000749
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
From: <sip:102@192.168.0.200>;tag=6627

To: <sip:101@192.168.0.200>;tag=3471845493
CSeq: 2 UPDATE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE
Supported: timer
Contact: <sip:101@192.168.0.101:5060>
Require: timer
Session-Expires: 180;refresher=uac
Content-Length: 0

F18 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKsd8c80456f
From: <sip:102@192.168.0.200>;tag=4244609427
To: <sip:101@192.168.0.200>;tag=1967
Call-ID: 14241-72f0b6@192.168.0.200
CSeq: 1 UPDATE
Contact: <sip:101@192.168.0.200:5060>
Content-Length: 0
Supported: timer
Require: timer
Session-Expires: 180;refresher=uac
Allow: ACK,BYE,CANCEL,INVITE,PRACK,UPDATE

F19 BYE

Request-Line: BYE sip:102@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsde9dd08cf
Max-Forwards: 70
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>;tag=6627
CSeq: 4 BYE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE
Content-Length: 0

F20 BYE

Request-Line: BYE sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560222421000012

From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>;tag=4244609427
Call-ID: 14241-72f0b6@192.168.0.200
CSeq: 3 BYE
Max-Forwards: 70
Content-Length: 0

F21 200 OK

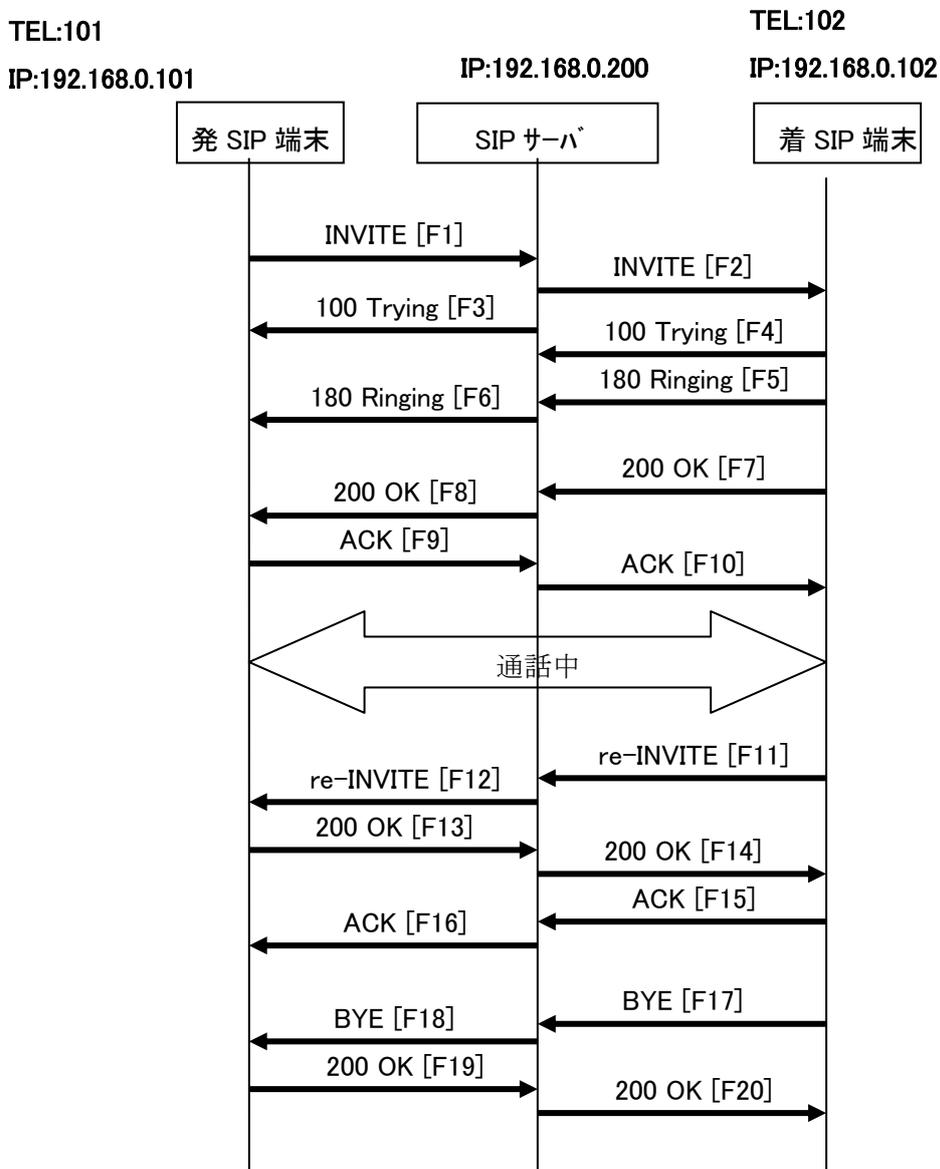
Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560222421000012
Call-ID: 14241-72f0b6@192.168.0.200
From: <sip:101@192.168.0.200>;tag=1967
To: <sip:102@192.168.0.200>;tag=4244609427
CSeq: 3 BYE
Content-Length: 0

F22 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKsde9dd08cf
From: <sip:101@192.168.0.200>;tag=3471845493
To: <sip:102@192.168.0.200>;tag=6627
Call-ID: d63b14f7-c8cf0d18ca17fd7bd29e0080f0e8b136@192.168.0.101
CSeq: 4 BYE
Content-Length: 0

i.5 接続シーケンス 2 (発着 100rel 未動作、発着 timer 動作、発着 UPDATE 未動作)

発着 100rel 未動作、発着 timer 動作、発着 UPDATE 未動作時の呼接続シーケンス例 (認証シーケンスは省略) を付図 i -5 に示す。また、各メッセージ例を付記する。



付図 i -5/JJ-22.11 接続シーケンス 2

メッセージ詳細例

F1 INVITE

Request-Line: INVITE sip:102@192.168.0.200:5060 SIP/2.0
 Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
 Max-Forwards: 70

Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Supported: timer
Contact: <sip:101@192.168.0.101:5060>
Session-Expires: 180
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 1 1 IN IP4 192.168.0.101
s= -
c= IN IP4 192.168.0.101
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F2 INVITE

Request-Line: INVITE sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Supported: timer
Contact: <sip:101@192.168.0.200:5060>
Session-Expires: 180;refresher=uas
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 1 1 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F3 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>
CSeq: 2 INVITE
Content-Length: 0

F4 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>
CSeq: 1 INVITE
Content-Length: 0

F5 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.102:5060>
Content-Length: 0

F6 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927

To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.200:5060>
Content-Length: 0

F7 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Supported: timer
Contact: <sip:102@192.168.0.102:5060>
Require: timer
Session-Expires: 180;refresher=uas
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 9 9 IN IP4 192.168.0.102
s= -
c= IN IP4 192.168.0.102
t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F8 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Supported: timer
Contact: <sip:102@192.168.0.200:5060>

Require: timer
Session-Expires: 180;refresher=uas
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 0 0 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F9 ACK

Request-Line: ACK sip:102@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs79da021cf
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 ACK
Content-Length: 0

F10 ACK

Request-Line: ACK sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs0f1f33c6f
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 1 ACK
Content-Length: 0

F11 re-INVITE

Request-Line: INVITE sip:101@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKs6804a07af

Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:102@192.168.0.200>;tag=1690348044
To: <sip:101@192.168.0.200>;tag=2138050867
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Supported: timer
Contact: <sip:102@192.168.0.102:5060>
Session-Expires: 180;refresher=uac
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 9 9 IN IP4 192.168.0.102
s= -
c= IN IP4 192.168.0.102
t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F12 re-INVITE

Request-Line: INVITE sip:101@192.168.0.101:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560485109000305
From: <sip:102@192.168.0.200>;tag=1499443485
To: <sip:101@192.168.0.200>;tag=3492213927
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
CSeq: 3 INVITE
Contact: <sip:102@192.168.0.200:5060>
Max-Forwards: 70
Content-Length: 117
Supported: timer
Session-Expires: 180;refresher=uac
Allow: ACK,BYE,CANCEL,INVITE
Content-Type: application/sdp
v= 0
o= - 0 0 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200

t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000

F13 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560485109000305
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:102@192.168.0.200>;tag=1499443485
To: <sip:101@192.168.0.200>;tag=3492213927
CSeq: 3 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Supported: timer
Contact: <sip:101@192.168.0.101:5060>
Require: timer
Session-Expires: 180;refresher=uac
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 1 1 IN IP4 192.168.0.101
s= -
c= IN IP4 192.168.0.101
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F14 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKs6804a07af
From: <sip:102@192.168.0.200>;tag=1690348044
To: <sip:101@192.168.0.200>;tag=2138050867
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
CSeq: 2 INVITE
Contact: <sip:101@192.168.0.200:5060>
Content-Length: 117

Supported: timer
Require: timer
Session-Expires: 180;refresher=uac
Allow: ACK,BYE,CANCEL,INVITE
Content-Type: application/sdp
v= 0
o= - 1 1 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000

F15 ACK

Request-Line: ACK sip:101@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKse2d8891cf
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:102@192.168.0.200>;tag=1690348044
To: <sip:101@192.168.0.200>;tag=2138050867
CSeq: 2 ACK
Content-Length: 0

F16 ACK

Request-Line: ACK sip:101@192.168.0.101:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bK1350560485171000817
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:102@192.168.0.200>;tag=1499443485
To: <sip:101@192.168.0.200>;tag=3492213927
CSeq: 3 ACK
Content-Length: 0

F17 BYE

Request-Line: BYE sip:101@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKs55e58646f
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:102@192.168.0.200>;tag=1690348044
To: <sip:101@192.168.0.200>;tag=2138050867
CSeq: 3 BYE
Allow: INVITE,ACK,CANCEL,BYE
Content-Length: 0

F18 BYE

Request-Line: BYE sip:101@192.168.0.101:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKsd9287acef
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:102@192.168.0.200>;tag=1499443485
To: <sip:101@192.168.0.200>;tag=3492213927
CSeq: 4 BYE
Allow: INVITE,ACK,CANCEL,BYE
Content-Length: 0

F19 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKsd9287acef
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:102@192.168.0.200>;tag=1499443485
To: <sip:101@192.168.0.200>;tag=3492213927
CSeq: 4 BYE
Content-Length: 0

F20 200 OK

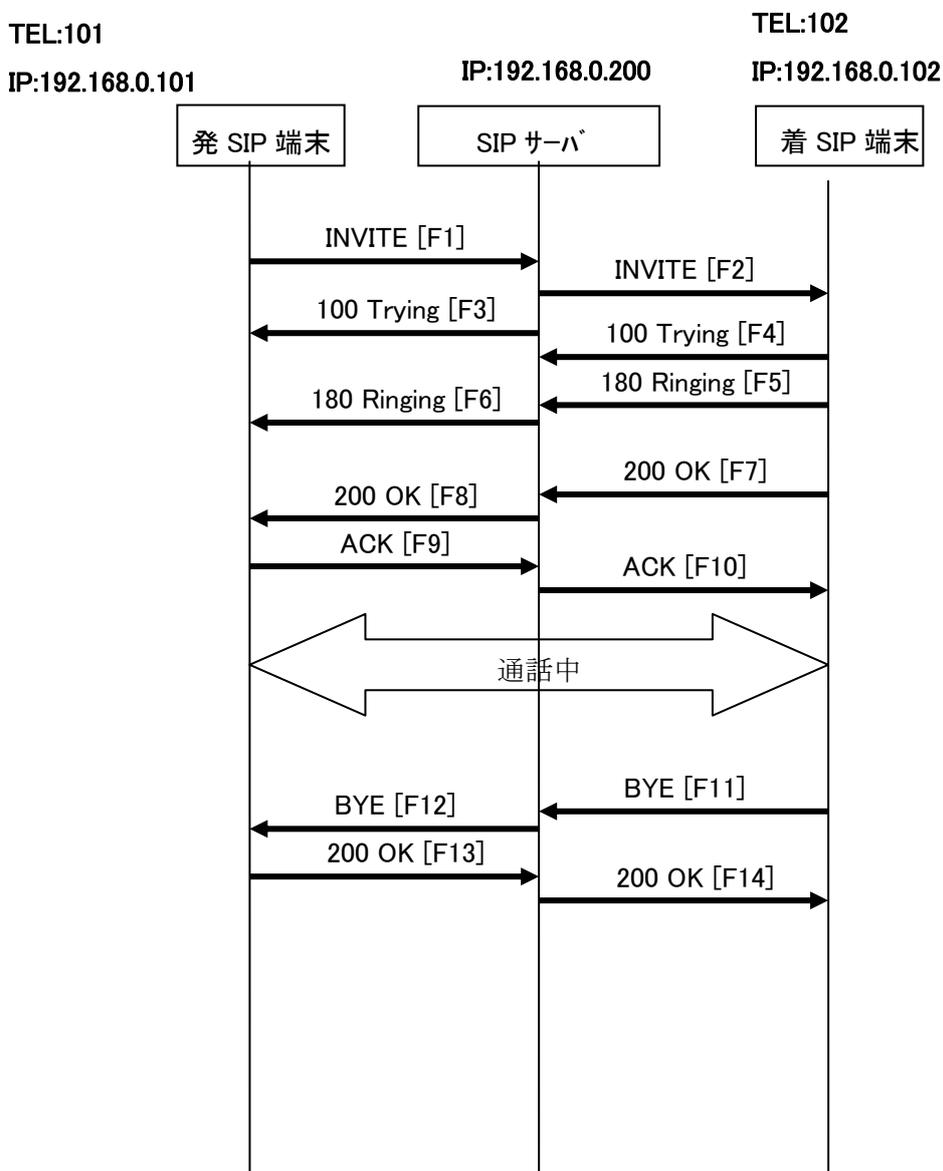
Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKs55e58646f
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:102@192.168.0.200>;tag=1690348044
To: <sip:101@192.168.0.200>;tag=2138050867

CSeq: 3 BYE

Content-Length: 0

i.6 接続シーケンス 3 (発着 100rel 未動作、発着 timer 未動作、発着 UPDATE 未動作)

発着 100rel 未動作、発着 timer 未動作、発着 UPDATE 未動作時の呼接続シーケンス例 (認証シーケンスは省略) を付図 i-6 に示す。また、各メッセージ例を付記する。



付図 i -6/JJ-22.11 接続シーケンス 3

メッセージ詳細例

F1 INVITE

Request-Line: INVITE sip:102@192.168.0.200:5060 SIP/2.0
 Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f

Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:101@192.168.0.101:5060>
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 1 1 IN IP4 192.168.0.101
s= -
c= IN IP4 192.168.0.101
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F2 INVITE

Request-Line: INVITE sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:101@192.168.0.200:5060>
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 1 1 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F3 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>
CSeq: 2 INVITE
Content-Length: 0

F4 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>
CSeq: 1 INVITE
Content-Length: 0

F5 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.102:5060>
Content-Length: 0

F6 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 INVITE

Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.200:5060>
Content-Length: 0

F7 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.102:5060>
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 9 9 IN IP4 192.168.0.102
s= -
c= IN IP4 192.168.0.102
t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F8 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.200:5060>
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 0 0 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200

t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F9 ACK

Request-Line: ACK sip:102@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs79da021cf
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 ACK
Content-Length: 0

F10 ACK

Request-Line: ACK sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs0f1f33c6f
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 1 ACK
Content-Length: 0

F11 BYE

Request-Line: BYE sip:101@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKs55e58646f
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:102@192.168.0.200>;tag=1690348044
To: <sip:101@192.168.0.200>;tag=2138050867
CSeq: 3 BYE
Allow: INVITE,ACK,CANCEL,BYE
Content-Length: 0

F12 BYE

Request-Line: BYE sip:101@192.168.0.101:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKsd9287acef
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:102@192.168.0.200>;tag=1499443485
To: <sip:101@192.168.0.200>;tag=3492213927
CSeq: 4 BYE
Allow: INVITE,ACK,CANCEL,BYE
Content-Length: 0

F13 200 OK

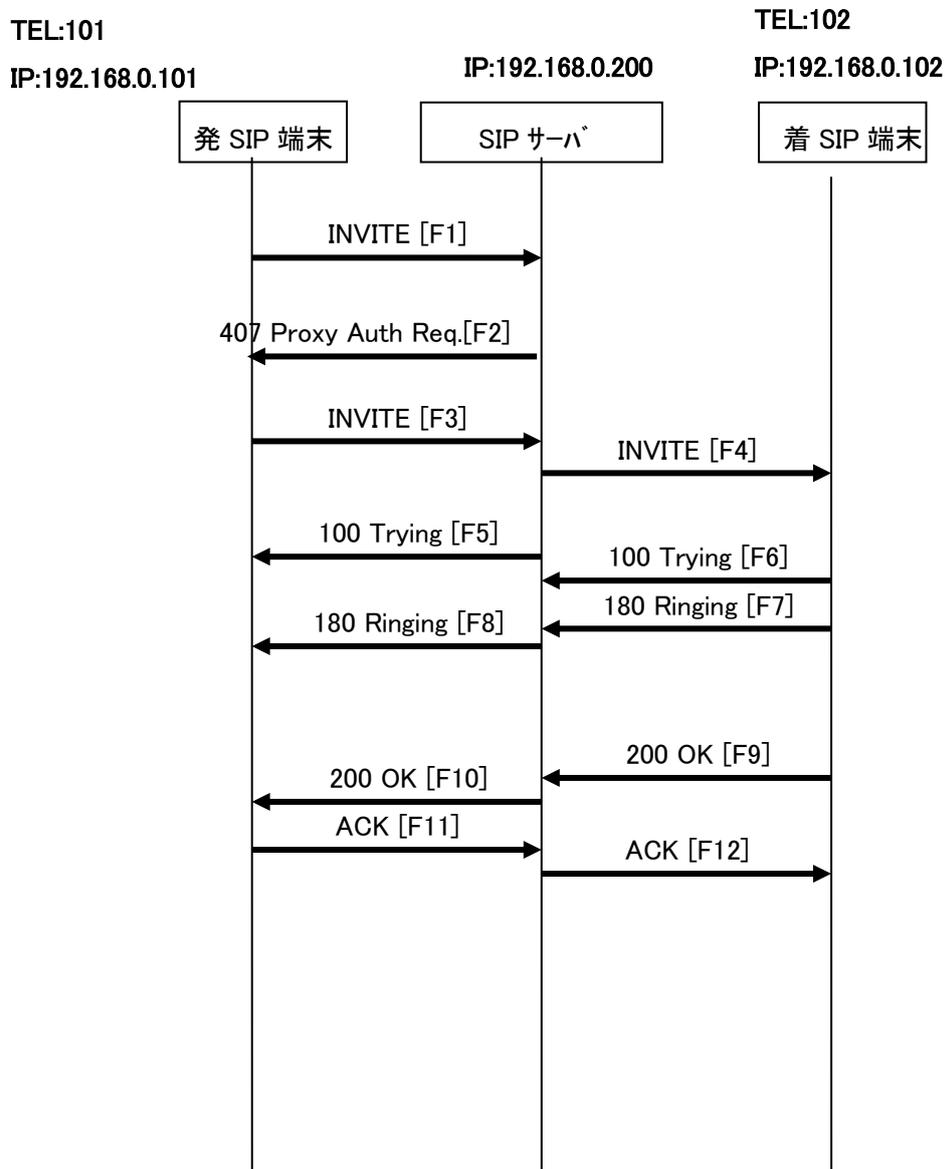
Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKsd9287acef
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:102@192.168.0.200>;tag=1499443485
To: <sip:101@192.168.0.200>;tag=3492213927
CSeq: 4 BYE
Content-Length: 0

F14 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.102:5060;branch=z9hG4bKs55e58646f
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:102@192.168.0.200>;tag=1690348044
To: <sip:101@192.168.0.200>;tag=2138050867
CSeq: 3 BYE
Content-Length: 0

i.7 接続シーケンス 4 (INVITE 認証つき)

INVITE 認証を求めるパターンについて、付図 i-7 に示す。また、各メッセージ例を付記する。



付図 i -7/JJ-22.11 接続シーケンス 4

メッセージ詳細例

F1 INVITE

```
Request-Line: INVITE sip:102@192.168.0.200:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
```

To: <sip:102@192.168.0.200>
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:101@192.168.0.101:5060>
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 1 1 IN IP4 192.168.0.101
s= -
c= IN IP4 192.168.0.101
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F2 407 Proxy Authentication Required

Status-Line: SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/UDP 192.168.0.101:5060;branch=z9hG4bKs5f404d71f
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>;tag=1755
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
CSeq: 1 INVITE
WWW-Authenticate: Digest realm="RegisteredUsers", nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",
algorithm=MD5
Content-Length: 0

F3 INVITE

Request-Line: INVITE sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch=z9hG4bKs4afd31eff
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>;tag=3492213927
To: <sip:102@192.168.0.200>
CSeq: 2 INVITE
Authorization: Digest realm="RegisteredUsers",nonce="6ddab56bd7ae5dba75ebd6ac58b163c7",
algorithm=MD5,uri="sip:192.168.0.200:5060",username="360",
response="997c057f45c34b61bda81f2e0c16745b"
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:101@192.168.0.101:5060>
Content-Type: application/sdp

Content-Length: 129

v= 0
o= - 1 1 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F4 INVITE

Request-Line: INVITE sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch= z9hG4bKs4afd31e0f
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>
CSeq: 3 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:101@192.168.0.200:5060>
Content-Type: application/sdp
Content-Length: 129

v= 0
o= - 1 1 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 8026 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F5 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.101:5060;branch= z9hG4bKs4afd31eff
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>; tag=3492213927
To: <sip:102@192.168.0.200>
CSeq: 2 INVITE
Content-Length: 0

F6 100 Trying

Status-Line: SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.0.200:5060;branch= z9hG4bKs4afd31e0f
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>
CSeq: 3 INVITE
Content-Length: 0

F7 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.200:5060;branch= z9hG4bKs4afd31e0f
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 3 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.102:5060>
Content-Length: 0

F8 180 Ringing

Status-Line: SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.0.101:5060;branch= z9hG4bKs4afd31eff
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>; tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.200:5060>
Content-Length: 0

F9 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.200:5060;branch= z9hG4bKs4afd31e0f

Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 3 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.102:5060>
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 9 9 IN IP4 192.168.0.102
s= -
c= IN IP4 192.168.0.102
t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F10 200 OK

Status-Line: SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.101:5060;branch= z9hG4bKs4afd31eff
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>; tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 INVITE
Allow: INVITE,ACK,CANCEL,BYE
Contact: <sip:102@192.168.0.200:5060>
Content-Type: application/sdp
Content-Length: 129
v= 0
o= - 0 0 IN IP4 192.168.0.200
s= -
c= IN IP4 192.168.0.200
t= 0 0
m= audio 8016 RTP/AVP 0
a= rtpmap:0 PCMU/8000
a=ptime:20

F11 ACK

Request-Line: ACK sip:102@192.168.0.200:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.0.101:5060;branch= z9hG4bKs4afd31eff
Max-Forwards: 70
Call-ID: 23b7c294-ff640c1884a2be60bd900080f0bf882c@192.168.0.101
From: <sip:101@192.168.0.200>; tag=3492213927
To: <sip:102@192.168.0.200>;tag=1499443485
CSeq: 2 ACK
Content-Length: 0

F12 ACK

Request-Line: ACK sip:102@192.168.0.102:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.200:5060;branch= z9hG4bKs4afd31e0f
Max-Forwards: 70
Call-ID: 7803534a-8f5135187dbc755589860080f0b27810@192.168.0.200
From: <sip:101@192.168.0.200>;tag=2138050867
To: <sip:102@192.168.0.200>;tag=1690348044
CSeq: 1 ACK
Content-Length: 0