TTC標準
Standard

JJ-90.21

事業者 SIP 網に関するフレームワーク技術仕様

Technical Specification of the framework on Provider's SIP Networks

第 1 版

2005 年 6 月 2 日

社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

目　次

<参考>

1. 国際勧告などとの関連

特になし。

2. 改版履歴

版数	制定日	改版内容
第 1.0 版	2005 年 6 月 2 日	初版制定 (TS-1003 第 1 版を改訂)

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 Technologies 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 the Session Initiation Protocol (SIP))", TTC 標準 JF-IETF-RFC3262 第 1 版, 情報通信技術委員会(The Telecommunication Technologies 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 the Session Description Protocol (SDP))", TTC 標準 JF-IETF-RFC3264 第 1 版, 情報通信技術委員会(The Telecommunication Technologies Committee), 2005 年 6 月.

[4] "SDP: セッション記述プロトコル" (SDP: Session Description Protocol), TTC 標準 JF-IETF-RFC2327 第 1 版, 情報通信技術委員会(The Telecommunication Technologies 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 Technologies Committee), 2005 年 6 月.

[6] Zimmerer, E., Peterson, J., Vemuri, A., Ong, L., Audet, F., Watson, M. and M. Zonoun, "MIME media types for ISUP and QSIG objects", RFC 3204, Internet Engineering Task Force (IETF), December 2001.

[7] "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 Technologies Committee), 2005 年 6 月.

[8] Postel, J., "User Datagram Protocol", RFC 768/STD 6, Internet Engineering Task Force (IETF), August 1980
Postel, J., "Internet Protocol", RFC 791/STD 7, Internet Engineering Task Force (IETF), September 1981

[9] Freed, N. and Borenstein, N., "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, Internet Engineering Task Force (IETF), November 1996

[10] "相互接続共通インタフェース仕様 (Inter-Carrier Interface based on ISUP)", TTC 標準 JJ-90.10 第 6 版, 情報通信技術委員会(The Telecommunication Technologies Committee), 2003 年 4 月

[11] "SIP-TTC ISUP 信号方式相互接続に関する技術仕様 (Technical Specification on SIP to TTC ISUP Interworking)", TTC 標準 JF-IETF-RFC3398 第 1 版, 情報通信技術委員会(The Telecommunication Technologies Committee), 2005 年 6 月

[12] International Telecommunications Union, "The International Public Telecommunications Numbering Plan", [13]

ITU-T Recommendation E.164, ITU-T, 1997.

3.2. 非規準参照文書

[14] Postel, J., "Transmission Control Protocol", RFC 793/STD 7, Internet Engineering Task Force (IETF), September 1981

[15] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, Internet Engineering Task Force (IETF), January 1999

[16] Stewart, R., Xiw, Q., Aharp, C., Schwarzbauer. H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, Internet Engineering Task Force (IETF), October 2000

[17] Camarillo, G. and H. Schulzrinne, "Early Media and Ringback Tone Generation in the Session Initiation Protocol (SIP)", RFC 3960, Internet Engineering Task Force (IETF), December 2004

[18] Rosenberg, J., Peterson, J., Schulzrinne, H. and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", RFC 3725/BCP 85, Internet Engineering Task Force (IETF), Internet Engineering Task Force, April 2004

[19] Johnston, A., Sparks, R., Cunnigham, C., Donovan, S. and K. Summers, "Session Initiation Protocol Service Examples", draft-ietf-sipping-service-examples-08, Internet Engineering Task Force (IETF), Work in Progress, March 2005.

[20] Mahy, R., Biggs, B. and R. Dean, "The Session Initiation Protocol (SIP) "Replaces" Header", RFC 3891, Internet Engineering Task Force (IETF), September 2004.

[21] Mahy, R. and D. Petrie, "The Session Initiation Protocol (SIP) "Join" Header", RFC 3911, Internet Engineering Task Force (IETF), October 2004.

[22] Peterson, J., "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format", RFC 3893, Internet Engineering Task Force (IETF), September 2004.

[23] Sparks, R., "Internet Media Type message/sipfrag", RFC 3420, Internet Engineering Task Force (IETF), November 2002.

[24] Rosenberg, J., Schulzrinne, H. and R. Mahy, "An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP)", draft-ietf-sipping-dialog-package-05, Internet Engineering Task Force (IETF), Work In Progress, November 2004.

[25] Willis, D. and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", RFC 3327, Internet Engineering Task Force (IETF), December 2002

[26] Willis, D. and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration", RFC 3608, Internet Engineering Task Force (IETF), October 2003

[27] International Telecommunications Union, "Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service," ITU-T Recommendation H.323, 2003.

[28] Andreasen, F. and B. Foster, "Media Gateway Control Protocol (MGCP) Version 1.0", RFC 3435, Internet Engineering Task Force (IETF), January 2003

[29] "Session Initiation Protocol (SIP)に関する技術レポート", TTC 技術レポート TR-1007, 情報通信技術委員会(The Telecommunication Technologies 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

信号制御専門委員会

1. 概要

1.1. 本仕様の適用範囲

本仕様は、JJ-90.10 [10]の規定に基づいて相互接続を行っている事業者が提供する網との間で、網間インタフェースを経由して呼が接続される可能性があり、かつSIP (JF-IETF-RFC3261 [1])により他網およびユーザ端末と接続する網(事業者SIP網)に適用される。また、規定対象とする呼の範囲についてはJJ-90.10 による相互接続インタフェースを経由して実際に接続される呼だけではなく、事業者SIP網を通したSIP端末間の接続等についても含むものとする。

本仕様におけるメディアの規定に関してはJJ-90.10 [10]で規定される網との間における音声呼の接続のみを適用範囲とし[1]、端末間のメディアについての規定は本仕様の範囲外とする。また、SIPの呼制御信号の規定に関しては最終的に呼接続するインタワーク網の組合わせによらず適用される[2]。

また、本仕様は本仕様で記述される内容に事業者 SIP 網の能力を限定するものではなく、事業者間の合意や SIP に関連する各標準に沿った形で拡張機能を利用することを制限するものではない。特定のインタフェースに関わる詳細仕様や、事業者 SIP 網として基本呼接続に加えて提供されるサービスに関する規定は、本仕様をベースとして、本仕様とは別の文書により規定される

1.2. 本仕様の目的と規定

- 本仕様は、事業者 SIP 網に関連したインタフェースやサービス仕様を規定するためのアーキテクチャやモデルなどのフレームワークを規定する。
- 本仕様は、呼制御信号条件として、事業者 SIP 網が他の事業者 SIP 網と接続する場合における、JF-IETF-RFC3261 [1]で規定される SIP およびその拡張規定に関して共通的に適用される信号処理条件を規定する。
- 本仕様は、事業者 SIP 網が満たすべき条件として、事業者 SIP 網を経由して生起する呼による輻輳の波及防止機能の具備等、特に既存網を含めた相互接続をする網を防護するためのセキュリティ条件および輻輳制御条件を規定する。また同じく、事業者 SIP 網が将来の拡張を含めた相互接続性の向上を確保するために考慮すべき要件について規定する。
- 本仕様は、音声等のメディア条件として、ISUP 網との音声呼の接続を保証するための事業者 SIP 網に位置する MGC/MG (Media Gateway Controller/Media Gateway)でサポートするメディア能力条件を規定する。事業者 SIP 網を経由して確立する SIP UA (User Agent)間のセッションのメディア条件については特に制限しない。

1.3. 本仕様の内容

本仕様は、1.1節の適用範囲において網間接続を行うために事業者SIP網が満たすべき要求条件および接続インタフェース条件を規定する。本仕様の構成は以下の通りである。

---

[1] 今後の検討や適用されるインタフェースの増加によっては、メディアに関する適用範囲を拡大するかもしれない。

[2] 事業者のポリシーにより、インタワークする網やプロトコルによりSIPの動作を異なるように扱うことを制限するものではない。

・ 本文: 対象となる接続モデルおよび用語の定義を規定する。また、事業者 SIP 網が満たす要件等について規定を行う。また、ISUP 網との音声呼の接続を保証するための事業者 SIP 網に位置するノードでサポートするメディア能力条件を規定する。

・ 付録: 本文に対する次の参考情報を記載する。

- 事業者 SIP 網における SIP メッセージの透過性についての留意点(付録 i)
- SIP UA のメディア能力(付録 ii)
- SIP メディア能力に関する一般的な性質(付録 iii)
- 事業者 SIP 網が管理するユーザが利用する SIP UA で動的に IP アドレスを取得する場合の留意点(付録 iv)
- From ヘッダの SIP URI のなりすましや一意性の確保に関するガイドラインについて(付録 v)

1.4. 用語

本仕様の本文および付録において使用される主な用語の定義を示す。なお、本仕様のJF-IETF-RFC3261[1]に関連する用語については、基本的にTR-1007 [29]の付属資料 1 の用法に従う。

<事業者 SIP 網>

ある事業者の一定の管理下に置かれたSIPノードからなり、SIPのメッセージを転送し、バウンダリとなるSIPノードを通して外部の網や端末類とセッションを確立する網であり、JJ-90.10 [10]で規定される相互接続を行っている電気通信事業者の提供する網に、自網の接続インタフェースもしくは他網を介して直接的もしくは間接的に接続される可能性がある網。本標準の規定の対象となる網。

<SIP ノード>

SIPのメッセージを受信および送信する網上のエンティティ。JF-IETF-RFC3261 [1]におけるSIP UAの機能を有するノード(SIP端末, B2BUA, MGC等を含む)もしくはSIPプロキシサーバの機能を有するノード (ステートフルもしくはステートレス)を指す。なお、物理的に同一のSIPノードが呼によって、論理的にはSIP UAとして動作することもあれば、SIPプロキシサーバとして動作することもある。

<セッション>

接続インタフェースを介したSIPメッセージによるSDP (Session Description Protocol) [4]の交換により確立される音声等のメディアストリーム。

<呼>

接続インタフェースを介したInitial `INVITE`リクエストから始まるSIPメッセージの交換により管理されるエンドポイントおよび網の関係および状態。

<Initial INVITE リクエスト>

呼およびそれに結び付けられたセッションを確立するために送信される`INVITE`リクエストで、`To-tag`パラメータのない`To`ヘッダを含んでいることでサーバ側で認識される。

<入接続呼>

SIPを利用する接続インタフェースに対して適用され、当該接続インタフェースを通してInitial `INVITE`リクエストが他網から自事業者SIP網の方向に送信される場合の呼。

<出接続呼>

SIPを利用する接続インタフェースに対して適用され、当該接続インタフェースを通してInitial `INVITE`リクエストが自事業者SIP網から他網の方向に送信される場合の呼。

<セッション管理 SIP メッセージ>

Initial INVITEリクエストおよびそれに対する100 (Trying) レスポンス以外の1xx、もしくは2xxレスポンスにより確立したダイアログ内で送受されるSIPメッセージ(リクエストおよびそれに対するレスポンス)の総称。re-INVITE(Toヘッダに To-tagパラメータを含むINVITE)メッセージ、PRACKメッセージ、UPDATEメッセージ、BYEメッセージ、等が含まれる。

<隣接 SIP ノード>

他事業者SIP網に存在し、自事業者SIP網との間でインタフェースA (図 1)を介して直接SIPメッセージを送受するSIPノード。

<関門 SIP ノード>

自事業者SIP網内に存在し、他事業者SIP網との間でインタフェースA (図 1)を介して直接SIPメッセージを送受するSIPノード。

<バウンダリ>

自事業者 SIP 網(自網)と他網(端末類を含む)との境界に位置する自網側の信号ノードもしくはノード群

<MGC>

Media Gateway Controller。本標準においては、事業者 SIP 網に存在し、SIP と ISUP をインタワークする信号ノードである SIP UA のこと。

<MG>

Media Gateway。本標準においては、事業者 SIP 網に存在し、MGC からの制御により IP 上の音声メディアストリームと回線交換網の回線との間で音声パスを確立するノード。本文書内で MGC/MG と記述する場合には、MGC と MG は物理的に別のエンティティであってもよいし、同じエンティティであってもよい。

<匿名 URI>

URI情報を匿名化したい場合に利用するURI。具体的な形式はJF-IETF-RFC3323 [5]で推奨される形式 <sip:anonymous@anonymous.invalid> となる。

<事業者 SIP 網が管理するユーザ>

事業者 SIP 網のバウンダリにおいて呼の生起者を事業者 SIP 網が責任を持って特定する必要があるユーザ。

<接続インタフェース>

事業者SIP網が他網またはユーザとの間に有する呼制御信号に関する論理的な接続点。本文書においては呼制御信号として使用するプロトコルやカテゴリー(ユーザ接続インタフェースもしくはネットワーク接続インタフェース)により、その種別をラベル付けして使用する(表 1参照)。

<ユーザ接続インタフェース>

事業者SIP網と事業者SIP網が管理するユーザとの間の接続インタフェースのカテゴリー。事業者SIP網相互接続モデル(図 1)におけるインタフェースBはこのカテゴリーに含まれる。また、事業者SIP網相互接続モデルにおけるインタフェースAおよびインタフェースCは、呼の生起者の特定の責任は接続インタフェース以遠の網に求められるため、このカテゴリーには含まれない。その他の今後規定する接続インタフェース種別についてはその内容によりこのカテゴリーに含まれるかもしれないし、その他プロトコル網、もしくは以遠の網において呼の生起者の特定が行われるのであれば、このカテゴリーには含まれない。

<ネットワーク接続インタフェース>

ユーザ接続インタフェース以外の接続インタフェースのカテゴリー。

2. 相互接続モデル

2.1. アーキテクチャモデル

本標準で参照する相互接続アーキテクチャモデルについて図 1に示す。

本標準の対象となる事業者SIP網は自網が有するインタフェースCまたは、自網と接続する事業者SIP網(他網)が有するインタフェースCを通してJJ-90.10 [10]で規定される相互接続網と接続される能力を有しているものとする。

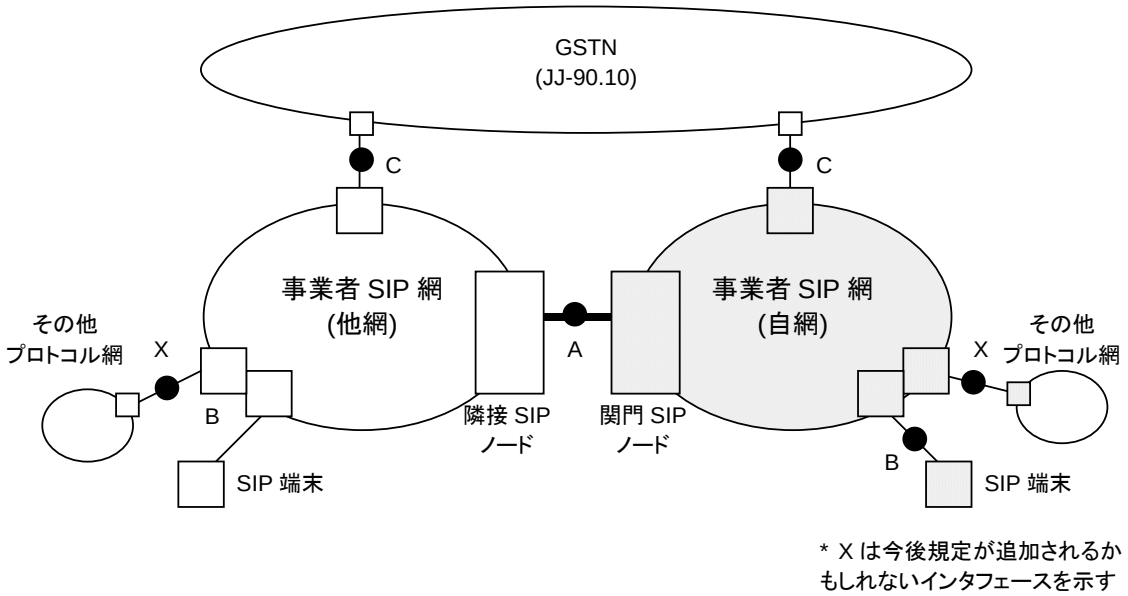


図 1／JJ-90.21　事業者 SIP 網相互接続モデル

表 1／JJ-90.21　相互接続モデルにおける接続インタフェース規定

インターフェース	プロトコル	バウンダリ	カテゴリー
A	SIP	SIP プロキシ等	ネットワーク
B	SIP	SIP アウトバウンドプロキシ等	ユーザ
C	ISUP	MGC	ネットワーク

なお、表 1に挙げた以外の接続インタフェース種別[3]については、必要時に種別を増やしていくことを想定し、その規定については本標準もしくは別の参照資料によって規定することとする。

2.2. コールモデル

本標準の対象となるコールモデルのパターンを表 2に示す[4]。

---

[3] 具体的な例を挙げるとすれば、ITU-T H.323 [27]やMGCP (Media Gateway Control Protocol) (RFC 3435 [28]) が挙げられる。

[4] インタフェースAを経由せず、SIP信号が 1 つの事業者SIP網に閉じる場合や、インタフェースC-インタフ

なお、インタフェース A を通して他事業者 SIP 網発信元インタフェースおよび他事業者 SIP 網着信先インタフェースまでの間にさらに別の事業者 SIP 網がインタフェース A によって経由される場合についてもスコープに含まれるものとする。
また、インタフェース X が新たに規定される場合、インタフェース X のコールモデル上の位置付けはインタフェース B に準じるものとするが、例外規定がある場合には新規規定時に明示する。

表 2／JJ-90.21　相互接続モデルにおけるコールモデル

	他事業者 SIP 網発信元インタフェース	事業者 SIP 網入インタフェース	事業者 SIP 網出インタフェース	他事業者 SIP 網着信先インタフェース
1.	B (または X)	A	C	-
2.	B (または X)	A	B (または X)	-
3.	B (または X)	A	A	C
4.	B (または X)	A	A	B (または X)
5.	C	A	B (または X)	-
6.	C	A	A	B (または X)
7.	-	B (または X)	A	C
8.	-	B (または X)	A	B (または X)
9.	-	C	A	B (または X)

3.　事業者 SIP 網に関する要求条件

3.1.　メッセージに関する要求条件

3.1.1. SIP メッセージの透過性

事業者SIP網を通して、インタフェースA-インタフェースA間、インタフェースA-インタフェースB間でSIPメッセージを交換し、呼およびセッションの確立をする能力を有する場合、種々のSIPにおける機能や将来の拡張性も含めた相互接続性に関してSIPメッセージの情報透過性(付録 i参照)の保証の程度と有無とが重要な要件となる。したがって、事業者SIP網においては、SIPメッセージの情報透過性について付録 iの各項目に基づき、適切な内容を必要に応じて相互接続先への提示を行うこととする。
なお、事業者 SIP 網が提供するサービスや接続構成により、同一のインタフェースにおいても情報透過性に関して一意に定まるとは限らないことに留意されるべきである。

3.1.2. SIP 拡張機能のサポートについて

事業者SIP網を通した呼における拡張機能利用のネゴシエーションの将来的な動作を保証するため、事業者SIP網内でJF-IETF-RFC3261 [1]に規定されるSIPプロキシサーバの動作とは異なる処理を行うノードが存在する場合については、未認識のものを含めて`option-tag`[5]で指定される拡張機能の実現に当該ノードの処理動作が影響を与えないということが確実に保証できない場合(以下、未サポート`option-tag`と記述)、以下の点について事業者SIP網として留意が必要である[6]。

ェースA-インタフェースCのコールパターンを含まない。

[5] SIP拡張機能の`option-tag`のリストは現在、http://www.iana.org/assignments/sip-parameters のページの`option-tag`のパートに記載されている。

[6] 新規拡張機能が規定された場合に、SIPノードの処理動作がその拡張に影響がないことが確認できれば、同新規`option-tag`に対して本節で規定した処理を行わないようにすることができるようにするべきであ

なお、事業者SIP網内の全てのSIPノードがJF-IETF-RFC3261 [1]に規定されるSIPプロキシサーバの処理動作に従うのであれば、下記の処理を行う必要はない。

- 受信したSIPリクエストに含まれるRequireヘッダが未サポートoption-tagを含む場合、事業者SIP網からは同SIPリクエストに対して未サポートoption-tagをUnsupportedヘッダに含んだ420 (Bad Extension)レスポンスを返送するべきである。また、Proxy-Requireヘッダについても同様である。
- 受信したSIPリクエストおよび2xxレスポンスに含まれるSupportedヘッダが未サポートoption-tagを含む場合、事業者SIP網では転送するメッセージに含めるSupportedヘッダに未サポートoption-tagを含めるべきではない。
- 受信した421 (Extension Required)レスポンス[7]に含まれるRequireヘッダが未サポートoption-tagを含む場合、事業者SIP網でエラーレスポンスを前位に転送する場合には421 (Extension Required)レスポンスをそのまま転送せず、Requireヘッダを含まない400 (Bad Request)等のレスポンスで転送するべきである。[8]

3.1.3. 未認識ヘッダ/パラメータの処理について

事業者SIP網内においては、将来における拡張性の確保のために、未認識ヘッダや未認識のヘッダパラメータを受信した場合において、SIPメッセージを次ホップへ転送する場合においては、当該ヘッダやヘッダパラメータが存在しなかったものとして処理を継続することが望ましい[9]。また、SIP UAとして動作する場合においても、当該ヘッダやヘッダパラメータの内容を無視して処理を継続することが望ましい。

3.1.4. SIP リクエストのメッセージサイズについて

次ホップへのSIPリクエストの送信に利用可能なトランスポートがUDPのみである場合等においては、IPレイヤにおける多数のフラグメンテーションの影響で網輻輳やノード輻輳が懸念される。左記の問題点を回避するため、一定の上限を超えるフラグメンテーションの発生が想定されるような場合には事業者SIP網においては次ホップへのSIPリクエストの転送を拒否してもよい。その場合のレスポンスとしては、513 (Message Too Large)レスポンスを使用することが望ましい。また、事業者SIP網からメッセージサイズを理由としてエラーレスポンスを返送する場合においては、事業者SIP網においてその事実を検知できる

る。

[7] RFC 3261 ではUASが421 (Extension Required)レスポンスを返送し、特定の拡張機能のサポートを要求することは推奨されていない。

[8] 421 (Extension Required)レスポンスを転送した場合、UACで指定のoption-tagを付加して再送するとSIPノードは420 (Bad Extension)レスポンスを返送、指定のoption-tagなしで再送すると421 (Extension Required)レスポンスを受信するという繰り返しを避けるためである。

[9] SIPプロキシサーバとして動作するのであれば、通常透過転送を行う。ただし、網が提供するサービスにおいて必要である場合や、当該ヘッダもしくはヘッダパラメータが明らかに相互接続性に影響を与えることが事前に明確になっている場合等においては事業者SIP網のポリシーとして削除してもよい。その際においては3.1.1節および3.1.2節に留意し、その内容に従って処理動作について明確化すること。

ようにするべきである[10]。
また、インタフェースAのバウンダリにおいては、JF-IETF-RFC3261 [1] 18.1.1 節で言及されている少なくとも 1300 バイトまでのメッセージについては処理できなくてはならない。
なお、SIP UA はフラグメント化された SIP パケットの受信が可能であることが強く推奨される。

3.1.5. 1xx レスポンスの送達保証について

SIPを利用して呼を接続する場合において、1xxレスポンスが何らかの理由で転送時の経路で消失した場合、着信側ユーザの呼出中を示す呼出音や網が生成するアナウンスを発信側ユーザへ伝えることができなくなる可能性がある。したがって、他網と相互接続した場合も含めて、GSTNと接続する可能性のある事業者SIP網の呼においては、1xxレスポンスを確実に転送するための対策が取られるべきである。SIPのプロトコル上においてはJF-IETF-RFC3262 [2]で規定される100relのオプションにより実現することが可能であるが、メッセージ転送の全ての経路でTCPなどの信頼性のあるトランスポートが保証されるなど、100relオプション以外の別の手段により実現されていてもよい。

3.2. 発ユーザの特定

事業者SIP網においては事業者SIP網が管理するユーザからのユーザ接続インタフェースを通した信号を元に送信するInitial INVITEリクエストについてはその送信契機となった呼を生起したユーザが特定可能であること。
また、ネットワーク接続インタフェースを通した入接続呼に関しては、その接続インタフェースによって接続される網において、もしくはそれ以遠の網において確実に呼を生起したユーザが特定可能であること。

3.3. メディアに関する要求条件

3.3.1. インタフェース C のバウンダリの IP 側メディア条件

事業者SIP網がインタフェースCを持ち、インタフェースAを通してSIPメッセージを交換し、GSTNとの間でセッションの確立を行う場合、インタフェースCのバウンダリであるMGC/MGは最低限表 3のメディア能力プロファイルをサポートしていることが期待される。また、MGC/MGはJF-IETF-RFC3261 [1]やJF-IETF-RFC3264 [3]で規定されるSIPのネゴシエーション能力を有していなくてはならない。
なお、MGC/MGは表 3のメディア能力プロファイルで示される以上の能力を有しているかもしれない。

表 3／JJ-90.21　インタフェース C のバウンダリの最低保証メディア能力プロファイル

	大項目	小項目	プロファイル
1-1	SDP 能力要素(送信)	受信 IP アドレス	IPv4, Unicast
1-2		ポート番号	ウェルノウンポート以外の任意
1-3		コーデック	G.711 μ Law をサポートする
1-4		帯域	-
1-5		パケット間隔	20 もしくは指定なし
1-6		方向	sendrecvもしくは付与しない

[10] メッセージサイズの想定する上限を超える条件を確認し、必要があればメッセージサイズの上限を増やす等の対策を取ることが想定される。

	大項目	小項目	プロファイル
2-1	SDP 能力要素(受信)	受信 IP アドレス	IPv4, Unicast
2-2		ポート番号	ウェルノウンポート以外の任意
2-3		コーデック	G.711 μ Law はサポートする
2-4		帯域	-
2-5		パケット間隔	20 もしくは指定なし (20ms 間隔はサポートする)
2-6		方向	sendrecvもしくは指定なし
3-1	SDP 能力要素特殊値 (送信)	受信IPアドレス (c=行: 0.0.0.0)	送信しない
3-2		ポート番号 (m=行: 0)	送信しない
3-3		帯域 (b=行: 0)	送信しない
4-1	SDP 能力要素特殊値 (受信)	受信IPアドレス (c=行: 0.0.0.0)	受信時に処理できないかもしれない
4-2		ポート番号 (m=行: 0)	受信を期待しない (本文書 ISUP との相互接続の範囲では複数メディアを同時に確立しない)
4-3		帯域 (b=行: 0)	受信を期待しない
5-1	SDP 形式	マルチパート MIME ボディ (オファー)	送信しない
5-2		マルチパート MIME ボディ (アンサー)	送信しない
5-3		m=行なしSDP (オファー)	送信しない
5-4		複数m=行SDP (オファー)	送信しない
5-5		複数 PT (アンサー)	送信しない
6-1	SDP 形式 (受信)	マルチパート MIME ボディ (オファー)	受信可能 (ただし、multipart/mixedでapplication/sdp以外の認識できないContent-Typeに対応するContent-Dispositionヘッダのhandlingパラメータがoptionalである場合)
6-2		マルチパート MIME ボディ (アンサー)	受信可能 (ただし、multipart/mixedでapplication/sdp以外の認識できないContent-Typeに対応するContent-Dispositionヘッダのhandlingパラメータがoptionalである場合)
6-3		m=行なしSDP (オファー)	受信しないかもしれない (その場合にはエラーレスポンス返送)
6-4		複数m=行SDP (オファー)	受信しないかもしれない (ただし、サポートできるm=行が存在する場合、受信可能であることが望ましい)
6-5		複数 PT (アンサー)	単一の PT しかサポートしないかもしれない。
7-1	Early Media (180/Media/Alert-Info)	受信/受信/受信	a.(呼出音) / b.(受信メディア再生) (b.は事業者SIP網内の信頼できかつメディアの再生を期待するノードからのメディアであることが判断可能であるときのみ再生してもよい[11])
7-2		受信/受信/未受信	同上
7-3		受信/未受信/受信	a.(呼出音)
7-4		受信/未受信/未受信	a.(呼出音)
7-5		未受信/受信/未受信	d.(無音)

[11] JF-IETF-RFC3398 [11] 付録i参照

	大項目	小項目	プロファイル
8-1	発信時確立手順 (オファー/アンサー)	INVITE/2xx	対応する
8-2		INVITE/1xx (100rel)	対応する
8-3		2xx/ACK	対応しない (SDPなしのINVITEリクエストを送信しない)
8-4		1xx(100rel)/PRACK	対応しない (SDPなしのINVITEリクエストを送信しない)
9-1	着信時確立手順 (オファー/アンサー)	INVITE/2xx	対応する
9-2		INVITE/1xx (100rel)	対応する
9-3		2xx/ACK	対応しないかもしれない
9-4		1xx(100rel)/PRACK	対応しないかもしれない
10-1	複数ダイアログ処理 (既存/新)	Early/Early	-
10-2		Early/Confirm	Confirm ダイアログの方を優先する
10-3		Confirm/Confirm	先の Confirm ダイアログの方を優先する
11-1	セッション変更要求送信 (State/リクエスト)	Confirmed/re-INVITE	送信しない
11-2		Confirmed/UPDATE	送信しない
11-3		Early/UPDATE (UAS)	送信されるかもしれない
11-4		Early/UPDATE (UAC)	送信しない
11-5		Early/PRACK	送信しない
12-1	セッション変更要求受信 (State/リクエスト)	Confirmed/re-INVITE	変更内容が可能であれば処理する
12-2		Confirmed/UPDATE	変更内容が可能であれば処理する (Allowヘッダに UPDATEを含めた場合のみ)
12-3		Early/UPDATE (UAS)	処理しないかもしれない
12-4		Early/UPDATE (UAC)	処理しないかもしれない
12-5		Early/PRACK	処理しないかもしれない
13-1	セッション変更内容 (送信)	受信 IP アドレス	送信しない
13-2		受信ポート番号	送信しない
13-3		ペイロードタイプ変更	送信しない
13-4		ペイロードタイプ削除	送信しない
13-5		メディア追加	送信しない
13-6		メディア削除	送信しない
13-7		方向	送信しない
13-8		受信パケット間隔	送信しない
14-1	セッション変更内容 (受信)	受信 IP アドレス	変更しないかもしれない (変更可能であるべき)
14-2		受信ポート番号	変更しないかもしれない
14-3		ペイロードタイプ変更	変更しないかもしれない
14-4		ペイロードタイプ削除	変更しないかもしれない
14-5		メディア追加	変更しないかもしれない
14-6		メディア削除	変更しないかもしれない
14-7		方向	変更しないかもしれない
14-8		受信パケット間隔	変更しないかもしれない

3.4. セキュリティに関する要求条件

事業者 SIP 網において以下の要求条件が満たされること。

3.4.1. メッセージプライバシー

事業者 SIP 網内においては、第三者によってメッセージの内容を見られたり改竄されたりすることがないこと。

3.5. 輻輳制御に関する要求条件

事業者 SIP 網において以下の要求条件が満たされること。

3.5.1. 輻輳波及の防止機能について

出接続呼において、輻輳の波及を防止するために自動もしくは手動にて輻輳の原因となっているある一定の条件に当てはまるInitial `INVITE`リクエストの転送を接続先の事業者もしくは自身の判断により制限することが可能であること。

3.5.2. 特定ユーザからの発信停止機能について

ユーザ接続インタフェースからの不正な発信または不必要に多量な発信による網輻輳の波及を防止するために、原因となっている事業者SIP網が管理するユーザからのInitial `INVITE`リクエストの転送を事後に運用措置により停止することが可能であること。

3.5.3. 単一ユーザからの同時接続試行呼数/接続呼数の上限について

ユーザ接続インタフェースからの事業者 SIP 網が管理する(単一の)ユーザからの出接続呼による網輻輳を発生させないようにするために単一ユーザからの同時接続試行呼数/接続呼数に関して事前に有限な上限を設定することが可能であること。

4. インタフェース A に関する規定

4.1. インタフェース A に関する規定範囲

本章の以下の節において、2章に規定される相互接続モデルにおけるインタフェースAに関する規定について記述する。

なお、本章で規定される接続インタフェース条件は当該呼がJJ-90.10 [10]で規定される網との間でセッションを確立する場合だけではなく、その他の接続パターン(SIP UA間の接続等)においても適用される。

4.2. 接続インタフェース要求条件

本節では、インタフェース A に関するネットワークレイヤ以上の基本接続要求条件について規定する。

なお、本節に明記する要求条件以外のプロトコル[12]についてはその利用を排除するものではなく、事業者間の合意に基づき使用してもよい。

ただし、DoS 攻撃による処理異常や発アドレスの偽装などによる不正なメッセージを処理することがないようネットワークレイヤ以下のレイヤにおいてセキュリティ上の考慮がなされていること。

4.2.1. ネットワークレイヤインタフェース

Internet Protocol (IP) Version4 (IPv4) (RFC 791/STD 7) [8]をサポートすること。Internet Protocol (IP) Version6 (IPv6)の利用について妨げるものではない。

---

[12] Internet Protocol Version6 (IPv6)、Transmission Control Protocol (TCP) [14], Transport Layer Security (TLS) [15], Stream Control Transmission Protocol (SCTP) [16]等

4.2.2. トランスポートレイヤインタフェース

User Datagram Protocol (UDP) (RFC 768/STD 6 [8])をサポートすること。また、Transmission Control Protocol (TCP)についてもサポートしていることが望ましい。また、事業者SIP網間でメッセージのセキュリティ上の問題を解決するために両社の合意に基づきTLSを利用することを妨げるものではない。

4.2.3. アプリケーションインタフェース

Session Initiation Protocol (SIP) v2.0 (JF-IETF-RFC3261 [1])を使用する。

4.3. SIP メッセージ要求条件

4.3.1. 必須ヘッダ設定条件

表 4にInitial INVITEリクエストに設定される必須ヘッダの値設定について示す。

表 4／JJ-90.21 Initial INVITE リクエストの必須ヘッダ値設定

ヘッダ	入接続呼 (受信)	出接続呼 (送信)
To	JF-IETF-RFC3261 [1]のフォーマットに従う値を許容すること。tagパラメータが付与されていないことによりInitial INVITEであることを認識する。	JF-IETF-RFC3261 [1]のフォーマットに従うこと。tagパラメータは付与されてないこと。
From	JF-IETF-RFC3261 [1]のフォーマットに従う値を許容すること。tagパラメータが付与されていることを前提としてよい。	JF-IETF-RFC3261 [1]のフォーマットに従うこと。
Contact	JF-IETF-RFC3261 [1]のフォーマットに従う値を許容すること。	JF-IETF-RFC3261 [1]のフォーマットに従うこと。
Call-ID	JF-IETF-RFC3261 [1]のフォーマットに従う値を許容すること。	JF-IETF-RFC3261 [1]のフォーマットに従うこと。
CSeq	JF-IETF-RFC3261 [1]のフォーマットに従う値を許容すること。	JF-IETF-RFC3261 [1]のフォーマットに従うこと。
Via	JF-IETF-RFC3261 [1]のフォーマットに従う値を許容すること。	JF-IETF-RFC3261 [1]のフォーマットに従うこと。
Max-Forward	JF-IETF-RFC3261 [1]のフォーマットに従う値を許容すること。	JF-IETF-RFC3261 [1]のフォーマットに従うこと。

4.3.2. メッセージルーティングに関するヘッダフィールド

関門 SIP ノードから隣接 SIP ノードへの SIP メッセージにおける、セッション確立後に転送される SIP リクエストの隣接 SIP ノードから関門 SIP ノードへのホップバイホップのメッセージルーティングのための宛先を示す SIP URI 形式のヘッダフィールドについての要求条件を示す。

<要求条件>

- hostport部がメッセージを送出する関門SIPノードのIPアドレス形式[13]であること。ただし、maddrパラメータが設定される場合を除く。
- maddrパラメータが設定される場合、maddrパラメータが上記条件を満たすこと。

[13] IPv4 の場合はABNFで、IPv4address = 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT の形式で示される。

- port部を設定してもよい (5060 以外のポート番号も許容する)
- transportパラメータは設定しなくてもよい
- lrパラメータ[14]等その他のパラメータは必要があれば設定してもよい[15]
- 上記hostport部で指定するアドレスが隣接SIPノードから到達可能であること

<適用されるヘッダフィールド>

- SIPリクエストの先頭の Record-Routeヘッダのrec-route
- (関門SIPノードがSIP UAの場合でRecord-Routeヘッダを設定しない場合) SIPリクエストのContactヘッダのhostport部
- 100 (Trying) レスポンス以外の1xxまたは2xxレスポンスのRecord-Routeヘッダのrec-route (すなわち、対応するリクエストを隣接SIPノードから受信して後位へ転送したときに設定したRecord-Routeヘッダ)
- (関門SIPノードがSIP UAの場合でRecord-Routeヘッダを設定しない場合) 100 (Trying) レスポンス以外の1xxまたは2xxレスポンスのContactヘッダのhostport部

4.3.3. セッション管理 SIP メッセージに関する要求条件

セッション管理SIPメッセージに関しては、Routeヘッダの内容に従いダイアログ内で転送されること。

4.4. 接続先 URI 指定方式

Initial INVITEリクエストのRequest-URIの設定について次のように規定する。

4.4.1. user 部

出接続呼および入接続呼の宛先がE.164 番号形式で指定可能な電話番号である場合、そのInitial INVITEリクエストのRequest-URIのSIP URIのuser部には基本的にはJF-IETF-RFC3966 [7] のABNFで規定されるtel URIのglobal-number-digitsのフォーマットを使用することを推奨する。また、visual-separatorの利用は推奨されない。JJ-90.10 [10]で規定される着信先番号に対応するフォーマットについて表 5に示す。

なお、global-number-digitsにパラメータ部(セミコロン(;)以降)が含まれる場合、それぞれのセミコロンの次がm-で始まっているものでない限りその内容が認識できない場合においても処理を継続できなくてはいけない。

表 5 ／JJ-90.21 Request-URI の user 部の設定

フォーマット	条件	用途
+ 国番号 国内番号	国番号は 81 以外、最大 15 桁	国際網着信
+81ABCDEFGHJ	A および B は 0 以外	地域固定電話着信, IP 電話着信 (カテゴリ A)
+81A0CDEFGHJK	A=2,7,8,9,C は 0 以外	移動体･PHS･無線呼出し(ポケベル)着信
+8150CDEFGHJK	C は 0 以外	IP 電話着信 (カテゴリ B)

[14] ただし、lrパラメータを挿入した場合においてもstrict-routingにも対応しているべきである。

[15] 受信したパラメータは透過転送しなくてはならない。

本推奨規定は、事業者SIP網間での合意により番号形式以外も含めて表 5以外のフォーマットを利用することを妨げるものではない。なお、表 5に記述するフォーマットの内容を含めて、別に規定されてインタフェースAに適用される接続インタフェース規定技術仕様でuser部のフォーマットの規定が定められるかもしれない。

4.4.2. hostport 部

出接続呼におけるInitial `INVITE`リクエストの`hostport`部は、隣接SIPノードの属するドメイン名もしくはホスト名(IPアドレス形式[16]を含む)を設定する。
したがって、入接続呼におけるInitial `INVITE`リクエストの`hostport`部は、関門SIPノードの属するドメイン名もしくはホスト名(IPアドレス形式[17]を含む)を設定されていることを期待する。

4.4.3. オプション URI パラメータ部

オプション URI パラメータは処理上無視する。

4.5. セキュリティ要求条件

事業者 SIP 網間のインタフェース A において以下の要求条件が満たされること。

4.5.1. メッセージプライバシー

接続インタフェースにおいては、第三者からメッセージの内容を見られたり改竄されたりすることがないこと。
接続インタフェースにおいて受信されるメッセージは確実に期待する信頼する他事業者 SIP 網からのメッセージであることが保証され、なりすまし等により不正な発信者からのメッセージを受信し処理することがないこと。

4.5.2. From ヘッダの正当性の確保

事業者SIP網からインタフェースAを通して送出するInitial `INVITE`リクエストの`From`ヘッダのURIは、Initial `INVITE`リクエストの生成者とは異なる他ユーザを示すURIではないこと、つまり他ユーザへのなりすましが行われないようにすること。
なお、他事業者SIP網からインタフェースAを通して受信するInitial `INVITE`リクエストの`From`ヘッダのURIは他事業者SIP網が本文書の上記の内容に従っていれば、なりすましはないものとみなすことができる。

以上

---

[16] ABNFでは、`IPv4address = 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT`

[17] ABNFでは、`IPv4address = 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT`

付録 i.　　SIP 網における情報透過(Transparency)について

i.1.　本付録の目的

JF-IETF-RFC3261 [1]で規定される動作に従ったSIPプロキシサーバからなる網を通して 2 つのSIP UAがSIPメッセージを交換し、実質的なセッションを確立する場合、メッセージ内の情報は基本的には経由するSIPプロキシサーバを通してSIP UA間で透過転送される。したがって、JF-IETF-RFC3261 [1]で規定される機能および関連するSIPの拡張機能の実現においては、基本的に網での情報透過(Transparency)を前提としている。ただし、実際の網への実装においては様々な理由から情報透過の性質が保持されない場合が存在し、その場合には潜在的な制約条件が存在する。

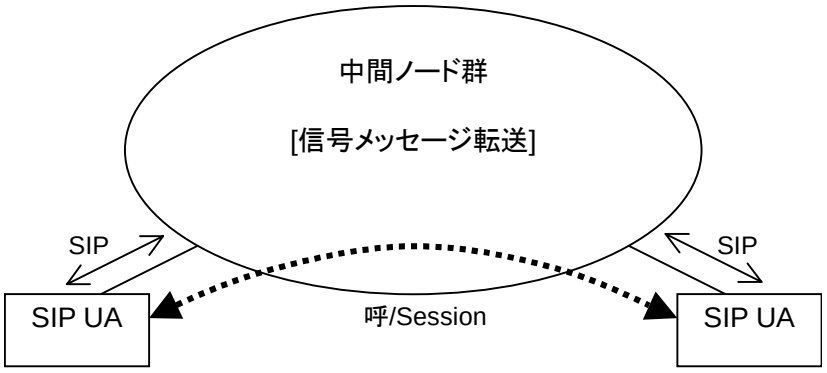
本付録では、情報透過の性質のタイプを分類し、その影響について考察し、本文書で規定される事業者 SIP 網に要求される条件、もしくは事業者 SIP 網が接続する網に対して提示する条件を整理する等にあたって参照される内容を記述する。

なお、本付録の内容は、情報透過の性質の保持に関わる代表的な事項を含んでいるが、決して全ての事項が網羅されているわけではないことに留意するべきである。

i.2.　概要

本付録においては次のようなモデルを想定する。また、用語については本文で記述される内容を採用する。

発側のSIP UAがInitial `INVITE`リクエストを送出し、それが契機となり中間ノード群を通して実質的な通話を確立する着側のSIP UAへInitial `INVITE`リクエストが送信される(付図ｉ)。着側のSIP UAは`To`ヘッダに`tag`パラメータを含むレスポンスを返送することでSIPダイアログが確立したと認識し、発側のSIP UAは`To`ヘッダに`tag`パラメータを含むレスポンスを受信することでSIPダイアログが確立したと認識する。また、確立したセッションがIP網上のRTPの場合、SIP UA間で直接IPパケットのやりとりを行うかもしれないし、中間ノード群の中でIPレイヤとしては一度以上終端されて中継されているかもしれない。



付図ｉ／JJ-90.21　SIP セッションにおけるメッセージ交換

本付録では、i.3節にJF-IETF-RFC3261 [1]で規定されるSIPプロキシサーバのみで構成される中間ノード群を通った場合には保証されるが、ある種のノードにおいては保証されないかもしれない情報透過について主なものを挙げ、i.4節において、情報透過が保持されないことによる制約条件について整理する。

なお、本付録の中では、SIP UAは付図ｉの実質的な通話を行う両端のSIP UAを指すこととする。また、中間ノードという用語により、付図ｉの任意のノード(SIPノードかもしれないし、それ以外のノードである

かもしれない)を指すこととする。

i.3. 情報透過

本節の各節において、括弧内の文はJF-IETF-RFC3261 [1]で規定されるSIP Proxyだけで構成される網であればSIP UA間で保証される処理内容を示す。続く内容がある場合は、括弧内の文の内容を補足するものである。
また、各節の最後に括弧の内容と異なる動作となることが発生すると想定される例を記述する。

i.3.1. ダイアログ情報透過

「SIP UA間でダイアログ[18]に関する情報が透過転送され、同じダイアログ情報を共有している[19]」

<想定される情報透過されない例>

- `Call-ID`ヘッダの値を引き継がない完全なB2BUAが中間ノードとして存在する。
- Forkや中間ノードによる順次サーチ等により複数の異なる`To-tag`を含むレスポンスを受信する場合に中間ノードが修正する (元とは異なる`tag`を利用)。
- `To-tag`や`From-tag`がないメッセージに対して、中間ノードが付与する (`To-tag`の利用/非利用の違い)。

i.3.2. メッセージ情報透過

「ダイアログ内の SIP メッセージはメソッドに依らずダイアログの相手の SIP UA まで転送される」

JF-IETF-RFC3261 0においては、ダイアログ内のメッセージについては、Record Routeの機能に従って動作をする限りにおいて、中間ノードを経由して相手まで転送される。また、Record Routeが行われない場合は中間ノードを介さずに直接メッセージが交換される。なお、転送された後にSIP UAで`405 (Method Not Allowed)` レスポンス等でエラーレスポンスを返送される可能性は当然存在する。
なお、Record Routeの機能に従っている場合でも、`Proxy-Require`ヘッダを含む場合には中間ノードでエラーレスポンスを`420 (Bad Extension)` レスポンスのエラーレスポンスを返送するかもしれない。

<想定される情報透過されない例>

- 中間ノードが単純な`INVITE/ACK/CANCEL - BYE`のみをサポートしており、その他のメソッドの転送をサポートしていない。
- 中間ノードがRTPも終端している場合で、セッション変更のための`UPDATE`リクエストや`re-INVITE`リクエストを吸収し転送しない。

i.3.3. CSeq 番号情報透過

「`CSeq`番号はSIP UA間で透過転送される」

---

[18] Call-ID, ローカルtag, リモートtagの組みで一意に決定される。

[19] 厳密にはi.3.4節のヘッダ情報透過の内容に含まれるかもしれないが、特別な意味を持つものとして特に区別をしている。

中間ノードがSIP UAからのリクエスト送出を契機とせずに、中間ノード自身がリクエストメッセージを生成する場合、Initial INVITEリクエストのCSeq番号が一致していたとしても途中で一致しない状況となる。

<想定される情報透過されない例>

- CSeq番号を引き継がない完全なB2BUAが中間ノードとして存在する。
- 中間ノードがセッション終了のためBYEリクエストを送出する。
- 中間ノードがセッション管理のためUPDATEリクエスト、re-INVITEリクエストを送出する。
- 中間ノードがセッション変更のためUPDATEリクエスト、re-INVITEリクエストを送出する。

i.3.4. ヘッダ情報透過

「JF-IETF-RFC3261 [1]Table2 および Table3、およびその他の拡張メソッドや拡張ヘッダを規定する RFC において同内容に相当する表において proxy 欄が m もしくは d となっているもの以外(未認識ヘッダを含む)については SIP UA 間でヘッダは透過転送される」

<想定される情報透過されない例>

- 特定のヘッダのみを透過転送する中間ノードが存在する。
- 特定のヘッダを編集する中間ノードが存在する。
- 未認識ヘッダを透過転送しない中間ノードが存在する。

i.3.5. セッション情報透過

「SDPの内容はSIP UA間で透過転送される[20]」

<想定される情報透過されない例>

- NAPT等を経由してRTPセッションを確立させるため、アドレス情報(c=行)やポート番号(m=行)を変換する中間ノードとセッション中継ノードが存在する。
- 網で許容するコーデック等のセッション情報を制限するため、能力情報の一部(m=行のペイロードタイプ等)を削除する中間ノードが存在する。

i.3.6. メッセージボディ情報透過

「メッセージボディはメソッドに依らず SIP UA 間で透過転送される」

<想定される情報透過されない例>

- 網で転送を許容する情報を制限するため、メッセージボディの削除やmultipart/mixedの一部を削除する中間ノードが存在する。
- メッセージの長さをハンドリング可能な長さとするためメッセージボディを削除する中間ノードが存在する。

---

[20] 厳密にはi.3.6節メッセージボディ情報透過の内容に含まれるかもしれないが、特別な意味を持つものとして特に区別をしている。

i.3.7. トポロジー情報透過

「SIPメッセージのルーティングのためにSIPプロキシサーバで付与されるヘッダ(Via, Route, Record-Route, Path (RFC 3327 [25]), Service-Route (RFC 3608 [26])ヘッダ21等)は付与された後、SIP UAまで透過転送される」

<想定される情報透過されない例>

- ルーティング情報についても完全に分離して処理する B2BUA が中間ノードとして存在する。
- 事業者 SIP 網のノードの数や配置に関する情報を外部から隠蔽するためのノードが中間ノードとして存在する。

i.4. 透過転送非保持に伴う制約

i.3節の各節に挙げたSIPにおける透過転送の特性のネットワークでの非保持による影響、制約について記述する。ただし、全ての考えうる影響および制約について網羅的に記述するものではないことに留意するべきである。

i.4.1. ダイアログ情報透過

<ダイアログ情報を利用した処理時の異常>

通信を行うSIP UA間で共通のダイアログ情報を保持していることを前提にした処理において期待した動作結果が得られなくなる。具体例としては、現在IETFにおいて検討中であるReplacesヘッダ (RFC 3891 [20])やJoinヘッダ (RFC 3911 [21])の利用が考えられるAttended Transfer, Call park, Call Pickup, 3-way Conference - 3ｒｄ Party Join, Single Line Extensionなどのシーケンスが実現できなくなる可能性が生じる[22]。

これらの拡張に対しても対応が可能なように途中でヘッダの値を書き換えることも不可能ではないが、実装上の難易度や今後の未知の拡張に対する対応において問題が生じる可能性がある。多くの場合にはoption-tagが設定されることが想定されるため、未知のoption-tagを含むSupportedヘッダから転送時に削除することで対応することは可能かもしれないが、本来のSIP UA間の機能拡張性を損なう可能性がある。

また、検討中のdialog event package (draft-ietf-sipping-dialog-package-05 [24])について様々な場面での利用が想定され、UA間でのダイアログの同一性が保証されない環境で利用した場合には問題となる可能性がある。

<aib 利用時の問題>

SIPメッセージのメッセージボディにsignatureによるID情報を含めるAuthenticated Identity Body (AIB) (RFC 3893 [22])を利用する場合、Replay ProtectionのためCall-IDヘッダの値がsignatureの計算に含まれる可能性があるため、Call-IDヘッダの値に変更があった場合、AIBの情報が正当に扱われない可能性がある。

---

[21] Path, Service-RouteヘッダはREGISTERリクエストでのみの使用が想定されているため、呼の確立のための信号のみを考える場合には利用されない。

[22] ここで挙げたサービスのシーケンス例がインターネットドラフト draft-ietf-sipping-service-examples-07 [19]に記載されている。

<ログ情報比較上の問題>

ダイアログの透過性を保持しない中間ノードを経由した場合に、SIP ノードおよび SIP UA 間でのログ情報を比較する場合に、中間ノードにおけるマッピング情報がない場合には対応するログを参照することが難しくなる場合が想定される。

i.4.2. メッセージ情報透過

<メッセージ不透過による拡張機能への影響>

SIPリクエストがダイアログ内で転送されない場合、当該メッセージを利用したSIP UA間のサービスが実現できなくなる可能性がある。Allowヘッダ等を該当する中間ノードで修正することで、転送されないメソッドのSIPリクエスト自体の送出をなくすことでエラーとなることは防止することは可能であるが、機能の利用は制限される可能性がある。

i.4.3. CSeq 番号情報透過

<aib 利用時の問題>

SIPメッセージのメッセージボディにsignatureによるID情報を含めるAuthenticated Identity Body (AIB) (RFC 3893 [22])を利用する場合、Replay ProtectionのためCSeqヘッダの値がsignatureの計算に含まれる可能性があるため、CSeqヘッダの値に変更があった場合、AIBの情報が正当に扱われない可能性がある。

<100rel オプション利用時等の問題>

JF-IETF-RFC3262 [2]で規定されるReliable Provisional Response (100rel)をSIP UA間で利用する場合に、RAｃｋヘッダにCSeq番号がコピーされた値が含まれることになるため、適切な考慮がない場合には正常な処理がSIP UA間で行われない。

JF-IETF-RFC3262 [2]に特化した対応は可能であるが、今後のSIPの拡張機能においてCSeqヘッダの値を別のヘッダ等で利用するものが出て来ない保証はなく、新規拡張機能に対してセッションを確立するSIP UAだけがサポートしているだけでは正常に処理が行われない可能性がある。

i.4.4. ヘッダ情報透過

<ヘッダ不透過による拡張機能への影響>

ヘッダが透過転送されない場合、当該ヘッダを利用した拡張機能が正常に動作しない可能性がある。

i.4.5. セッション情報透過

<セッション能力交換への影響>

SDP の能力交換に関する情報が透過転送されない場合、SIP UA 間で持っているセッション能力よりも低い能力でセッションが確立される可能性や、本来確立可能な能力を持っているにも関わらず、セッションが確立できない可能性がある。

i.4.6. メッセージボディ情報透過

<メッセージボディ不透過による拡張機能への影響>

メッセージボディが透過転送されない場合、当該メッセージボディを利用した情報の交換が行われない可能性がある。

i.4.7. トポロジー情報透過

<aib 利用時の問題>

SIPメッセージのメッセージボディにsignatureによるID情報を含めるAuthenticated Identity Body (AIB) (RFC 3893 [22])を利用する場合、`Contact`ヘッダの値がsignatureの計算に含まれるため、`Contact`ヘッダの値に変更があった場合、AIBの情報が正当に扱われない可能性がある。

付録 ii.　　SIP UA のメディア能力について

ii.1.　概要

SIP (JF-IETF-RFC3261 [1])におけるメディアセッションはオファー/アンサーと呼ばれるモデル(JF-IETF-RFC3264 [3])に基づいてSIPメッセージ上のSDP (Session Description Protocol: JF-IETF-RFC2327 [4])の交換により確立/管理される。本付録では、SDP受信時の処理能力について議論をするにあたっての考慮すべき事項についてまとめる。

本付録の内容は参照するRFC (JF-IETF-RFC3264 [3]およびJF-IETF-RFC2327 0)に基づく場合に想定される動作について記述している。

本付録の前提条件としては、SDP の交換により“ユニキャスト”の“RTP”メディアストリームを確立する場合を想定するものとする。

ii.2.　SDP 能力要素

付表 ii -1に主なSDPの要素について示す。なお、全ての要素について網羅的に列挙しているわけではないことに留意すること。

また、付表 ii -2に各要素の内、ゼロ値など特殊な意味を持つ値が存在する場合について挙げる。

付表 ii -1／JJ-90.21　SDP 能力要素

	内容	SDP 要素	補足
①	受信 IP アドレス	c=行	Session 部にあっても Media 部にあっても処理可能であること。
②	ポート番号	m=行	
③	コーデック	m=行および a=rtpmap	a=rtpmapがない静的なペイロードタイプにも対応可能であること。
④	帯域	b=行	
⑤	パケット間隔	a=ptime	送信側はptimeの値に従うべきではあるが、受信側はその他のパケット間隔であっても受信可能であるべき。
⑥	方向	a=行	inactive/sendrecv/sendonly/recvonly

付表 ii -2／JJ-90.21　SDP 能力要素の特殊値

	内容	SDP 要素	特殊値	意味	補足
①	受信 IP アドレス	c=行	0.0.0.0	メディアの保留	Obsoleteされた RFC 2543 での規定で JF-IETF-RFC3264[3]では利用を推奨しない。(direction 属性で指定を推奨)
②	ポート番号	m=行	0	メディアの拒否/削除	
③	帯域	b=行	0	メディア受信拒否	RTCP も受信されない。

機器実装の能力の表現としては、付表 ii -1および付表 ii -2のSDP能力要素について、送信する可能性の有無と受信した場合の処理動作について定める必要がある。なお、ここで送信/受信はSDPのオファー/アンサーとは独立でSDPの送受信のことを指す。ただし、オファー/アンサーで特記するべき差異がある場合には、その内容を記載するべきである。

ii.3. SDP 形式

ii.3.1. マルチパート MIME ボディ (オファーまたはアンサー)

multipart/mixedのMIME ボディを受信し、各partをSIP UAが処理可能かContent-Dispositionヘッダのhandlingパラメータがoptionalである場合に、含まれるSDPを正常に処理可能であるべきである。なお、処理できる能力がない場合には、415 (Unsupported Media Type) レスポンスを送信し、Acceptヘッダにサポート可能なタイプ(application/sdp等)のみを含めなくてはならない。

ii.3.2. m=行なし SDP (オファー)

m=行なしの(Initial) オファーであるSDPを受信した場合に、m=行なしのアンサーであるSDPを返送可能であること。Third Party Call Control (RFC 3725 [18])の最初のINVITEリクエストで用いられる場合がある。また、この場合には通常re-INVITEリクエストもしくはUPDATEリクエストによりm=行の追加が行われることが期待される。

ii.3.3. 複数 m=行 SDP (オファー)

複数のm=行を含むSDPを受けた場合に、対応できるm=行以外はポート番号を 0 に設定したアンサーを返送できること。

ii.3.4. 複数ペイロードタイプ受信 (アンサー)

複数ペイロードタイプ値をm=行に対応可能なペイロードタイプとして含めたオファーを送信した場合、複数のペイロードタイプ値をm=行に含んだアンサーを受信することがある。この場合、複数のペイロードタイプをひとつのセッション内で自由に切替えることができることを意味するため、切替えが出来ない場合にはre-INVITEリクエストもしくはUPDATEリクエストによって、実際に使用を希望するペイロードタイプ値のみを含めたSDPを再度オファーしなくてはならない。

付表 ii -3／JJ-90.21　SDP の形式について

	SDP	オファー/アンサー	補足
①	マルチパート MIME ボディ	オファー	415レスポンスを受信した場合には、その内容と自身のポリシーに従いリトライできるべき。
②		アンサー	マルチパート MIME が認識できない、もしくはhandling=optionalではないContent Typeを含む場合には 415 レスポンスに適切なAcceptヘッダを含めて返送しなくてはならない。
③	m=行なしSDP	オファー	3pcc (RFC 3725 [18])で利用される可能性あり
④	複数m=行SDP	オファー	Video 能力を持つ端末等から送出される可能性あり。
⑤	複数ペイロードタイプ受信	アンサー	複数ペイロードタイプを送信しない場合には受信することはない。

ii.4. Early メディアおよびローカル呼出音

Earlyメディアとローカル呼出音に関しては、JF-IETF-RFC3960 [17]において、一般的なルールが記述されており、180 (Ringing)レスポンスの受信とEarlyメディア(RTPパケット)の受信の有無によって、どのような処理を行うべきかについて言及されている。

また、Alert-Infoヘッダが180 (Ringing)レスポンスに含まれている場合には、その内容によってはAlert-Infoヘッダの値から得られる情報をローカル呼出音として利用してもよい。したがって、ローカル呼出音の送出能力を持ったSIP UAの処理動作としては次のパターンが想定される。

a. ローカル呼出音を利用する。
b. 受信したメディアを再生する。
c. Alert-Infoヘッダで示すリソースへアクセスし再生する。
d. 音は再生しない。

付表 ii -4に180 (Ringing)レスポンスの受信、Earlyメディアの受信、Alert-Infoヘッダの受信、のそれぞれのパターンとその処理選択の実装の可能性について示す。

付表 ii -4／JJ-90.21　Early メディアおよびローカル呼出音

	180	Media	Alert-Info	処理内容 (選択)	補足
①	受信	受信	受信	a. / b. / c.	0においてはb.をポリシーの例として挙げているが、PSTN GWなどにおいては、2xxレスポンス受信前のメディアの再生を行わない等のポリシーとなる可能性がある。
②	受信	受信	未受信	a. / b.	
③	受信	未受信	受信	a. / c.	
④	受信	未受信	未受信	a.	
⑤	未受信	受信	未受信	b. / d.	①/②と同様。

ii.5.　セッション確立

Initial INVITEトランザクションにおけるセッションの確立においては、オファーとアンサーの交換手順においていくつかのパターンが存在する。

ii.5.1.　発信時 (Initial INVITE リクエスト送信時)

付表 ii -5に発信時に現状想定し得るInitial INVITEトランザクションによるセッション確立の手順を示す。なお、相手オファーについては自身がSDPを含まないInitial INVITEリクエストを送信しない限り生じない。

付表 ii -5／JJ-90.21　発信時のセッション確立手順

	タイプ	オファー	アンサー	補足
①	自身オファー	INVITE	2xx	最も標準的
②		INVITE	1xx (100rel)	100relサポート時
③	相手オファー	2xx	ACK	Initial INVITEにオファーがない場合対応必須
④		1xx (100rel)	PRACK	Initial INVITEにオファーがない場合かつ100relサポート時必須

ii.5.2.　着信時 (Initial INVITE リクエスト受信時)

エラー! 参照元が見つかりません。に着信時に現状想定し得るInitial INVITEトランザクションによるセッション確立の手順を示す。オファーであるSDPを含まないINVITEリクエストを受信する状況としては、Third Party Call Control (RFC 3725 [18])等が想定される。

付表 ii -6／JJ-90.21　着信時のセッション確立手順

	タイプ	オファー	アンサー	補足
①	相手オファー	INVITE	2xx	最も標準的
②		INVITE	1xx (100rel)	100relサポート時対応必須 (2xxレスポンスにアンサー SDPはないかもしれない)
③	自身オファー	2xx	ACK	Initial INVITEにオファーがない場合必須(もしくはエラー切断)
④		1xx (100rel)	PRACK	Initial INVITEにオファーがない場合でReliable 1xxレスポンス送信時必須

ii.6.　複数ダイアログ処理

SIP UAがInitial INVITEリクエストを送出した場合、既存ダイアログに加えてそれまでに受信したものとは異なるTo-tagを含むレスポンスを受信することで複数のダイアログが確立される可能性がある。また、既存ダイアログは既に複数確立している可能性もある。複数のダイアログは、それぞれに対応するメディアを持つため、ポリシーに基づき適切な処理を必要とする。

付表 ii -7／JJ-90.21　複数ダイアログの処理

	既存ダイアログ	新ダイアログ	必要な処理
①	Early ダイアログ	Early ダイアログ	SDPの有無や内容等の条件でユーザインタフェース処理上どちらを優先するかのポリシーを持つことができる。ただし、100relを利用する場合には2xxレスポンスにアンサーが含まれない場合も想定されるため、全てのセッション情報を保持しておくか、もしくはBYEリクエストを送信して明示的にEarlyダイアログを終了することが望ましい。特に判断可能な条件がない場合には、新ダイアログの方を優先させることを推奨する。(無応答時転送などの場合を考慮)
②	Early ダイアログ	Confirmed ダイアログ	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。
③	Confirmed ダイアログ	Confirmed ダイアログ	SDP等の条件でどちらを優先するのか(もしくは同時に保持するのか)のポリシーを持つことができる。いずれかを選択する場合においては、明示的に他のダイアログをBYEリクエストにより解放することが望ましい。(単にACKリクエストを返送しない場合には、2xxレスポンスの再送が生じる)

ii.7.　セッション変更

セッションの変更は、変更されたSDPを含むSIPリクエストを送信することで要求する。変更内容がSIPリクエスト受信側で受け入れられる場合には、2xxレスポンスにアンサーであるSDPを含めて返送する。また、変更内容がSIPリクエスト受信側で受け入れられなかった場合には、488 (Not Acceptable Here)レスポンスを返送しなくてはならず、かつ変更要求時に保持していたセッションおよびダイアログはそのまま保持していなくてはならない。

ii.7.1.　変更要求送信

付表 ii -8にセッション変更を要求する場合の想定される種別を示す。

なお、実装においてはダイアログ確立後のセッション変更を含むオファーに対してエラーレスポンスを受けた場合に、不必要にセッションを終了しないような考慮がされるべきである。

付表 ii -8／JJ-90.21　セッション変更要求送信種別

	State	リクエスト	処理内容
①	Confirmed	re-INVITE	Confirmed ダイアログに対して変更を行う。
②		UPDATE	Confirmed ダイアログに対して変更を行う。ただし、相手側からのメッセージにUPDATEを含むAllowヘッダが含まれている場合に限る。
③	Early	UPDATE (UAS)	Early ダイアログに対して、INVITEトランザクションのUAS側からセッションを変更する場合
④		UPDATE (UAC)	Early ダイアログに対して、INVITEトランザクションのUAC側からセッションを変更する場合
⑤		PRACK	Early ダイアログに対して、INVITEトランザクションのUAC側からセッションを変更する場合。 * PRACKリクエストの2xxレスポンスにアンサーがない場合には、セッションの変更が失敗したもの(オファーが認識されなかった)と解釈して処理継続を行うような実装をするべきかもしれない。

ii.7.2.　変更要求受信

付表 ii -9にセッション変更要求を受信する場合の種別と、その受信条件や変更不可時の処理について示す。

付表 ii -9／JJ-90.21　セッション変更要求受信種別

	State	リクエスト	受信条件	変更不可時処理
①	Confirmed	re-INVITE	通常受信する可能性がある。	488レスポンス
②		UPDATE	AllowヘッダにUPDATEを含めなければ受信しない	488レスポンス
③	Early	UPDATE (UAS)	INVITEリクエストのAllowヘッダにUPDATEを含めなければ受信しない	488レスポンス
④		UPDATE (UAC)	Reliable 1xxレスポンスのAllowヘッダにUPDATEを含めなければ受信しない	488レスポンス
⑤		PRACK	100relモードでなければ、受信しない	488レスポンス

ii.7.3.　変更内容

付表 ii -10に主なセッション変更の内容を挙げる。

付表ⅱ-10／JJ-90.21　セッション変更内容

	変更要素	変更内容	補足 (用途等)
①	受信 IP アドレス	c=行のIPアドレスを変更する。	端末が移動する場合などが想定される。その場合にはContactヘッダの変更も併せて行われることが想定される。
②	受信ポート番号	m=行のポート番号を変更する。	IP アドレスの変更等と併せて行われる場合が想定される。
③	ペイロードタイプ変更	m=行のペイロードタイプ（およびa=rtpmapの内容)を変更する。	コーデックの変更などが想定される。
④	ペイロードタイプ削除	m=行の使用しないペイロードタイプを削除する。	アンサーで複数のペイロードタイプが返信された場合で、通信中に動的にRTP上でのペイロードタイプの変更ができない場合に、1つにするなどの場合が想定される。
⑤	メディア追加	m=行を追加する。	ビデオ通信や、その他のアプリケーションストリームの追加等が想定される。
⑥	メディア削除	m=行のポート番号を０とする。	
⑦	方向	a=inactive/sendonly/recvonly/sendrecvを変更する。	保留などを行う場合に、変更することが想定される。
⑧	受信パケット間隔	a=ptimeを変更する。	

付録 iii.　　SIP メディア能力プロファイル

iii.1.　SIP メディア能力プロファイルについて

本付録では付録 iiの内容に基づいて、メディアを扱うSIP UA(群)のメディア処理に関する能力を記述するためのプロファイルを規定する。メディア能力を記述するための唯一の方式ではないが、共通的な能力比較や確認のためのツールとして利用されることを目的としている。

iii.2.　SIP メディア能力プロファイル

付表 iii-1にメディアプロファイルの記述フォーマットを示す。

付表 iii-1／JJ-90.21　SIP メディア能力プロファイル

	大項目	小項目	プロファイル指定形式	参照
1-1	SDP 能力要素(送信)	受信 IP アドレス	IPv4/IPv6, Unicast/Multicast, 指定可能なアドレス範囲等を記述。	ii.2節 付表 ii-1
1-2		ポート番号	指定しうる値の範囲を記述。	
1-3		コーデック	サポートするコーデックを記述。	
1-4		帯域	指定しうる値の範囲を記述。ただし付与しない場合は「付与しない」と記述。	
1-5		パケット間隔	同上	
1-6		方向	同上	
2-1	SDP 能力要素(受信)	受信 IP アドレス	IPv4/IPv6, Unicast/Multicast, 対応可能なアドレス範囲を記述。	
2-2		ポート番号	対応可能範囲について記述。	
2-3		コーデック	サポートするコーデックについて記述。	
2-4		帯域	対応可能範囲について記述。また、指定されない場合の処理について記述。	
2-5		パケット間隔	同上	
2-6		方向	同上	
3-1	SDP 能力要素特殊値 (送信)	受信IPアドレス (c=行: 0.0.0.0)	送信有無および送信契機条件について記述	ii.2節 付表 ii-2
3-2		ポート番号 (m=行: 0)	同上	
3-3		帯域 (b=行: 0)	同上	
4-1	SDP 能力要素特殊値 (受信)	受信IPアドレス (c=行: 0.0.0.0)	受信時処理内容および条件について記述。	
4-2		ポート番号 (m=行: 0)	同上	
4-3		帯域 (b=行: 0)	同上	
5-1	SDP 形式 (送信)	マルチパート MIME ボディ (オファー)	送信有無について記述。送信する場合には、その契機と条件について記述。	ii.3節 付表 ii-3
5-2		マルチパート MIME ボディ (アンサー)	同上	
5-3		m=行なしSDP (オファー)	同上	
5-4		複数m=行SDP (オファー)	同上	
5-5		複数ペイロードタイプ (アンサー)	同上	

	大項目	小項目	プロファイル指定形式	参照
6-1	SDP 形式 (受信)	マルチパート MIME ボディ (オファー)	受信時処理内容および条件について記述。	
6-2		マルチパート MIME ボディ (アンサー)	同上	
6-3		m=行なしSDP (オファー)	同上	
6-4		複数m=行SDP (オファー)	同上	
6-5		複数ペイロードタイプ (アンサー)	同上	
7-1	Early Media (180/Media/Alert-Info)	受信/受信/受信	基本的に a., b. または c. から処理内容を選択記述。その他の場合について処理内容を具体的に記述。	ii.4節 付表 ii-4
7-2		受信/受信/未受信	基本選択肢が a. / b.である以外は同上。	
7-3		受信/未受信/受信	基本選択肢が a. / c. である以外は同上。	
7-4		受信/未受信/未受信	基本選択肢が a. である以外は同上。	
7-5		未受信/受信/未受信	基本選択肢が b. / d. である以外は同上。	
8-1	発信時確立手順 (オファー/アンサー)	INVITE/2xx	対応有無について記述。条件がある場合には明記する。	ii.5.1節 付表 ii-5
8-2		INVITE/1xx (100rel)	同上	
8-3		2xx/ACK	同上 (SDPを含まないINVITE送出有無について記述)	
8-4		1xx(100rel)/PRACK	同上 (SDPを含まないINVITE送出有無について記述)	
9-1	着信時確立手順 (オファー/アンサー)	INVITE/2xx	対応有無について記述。条件がある場合には明記する。	ii.5.2節 付表 ii-6
9-2		INVITE/1xx (100rel)	同上	
9-3		2xx/ACK	同上 (SDPを含まないINVITE受信時処理について明記)	
9-4		1xx(100rel)/PRACK	同上 (SDPを含まないINVITE受信時処理について明記)	
10-1	複数ダイアログ処理 (既存/新)	Early/Early	処理内容について記述。	ii.6節 付表 ii-7
10-2		Early/Confirm	同上	
10-3		Confirm/Confirm	同上	
11-1	セッション変更要求送信 (State/リクエスト)	Confirmed/re-INVITE	送信有無について記述。送信する場合にはその契機と条件について記述。	ii.7.1節 付表 ii-8
11-2		Confirmed/UPDATE	同上	
11-3		Early/UPDATE (UAS)	同上	
11-4		Early/UPDATE (UAC)	同上	
11-5		Early/PRACK	同上	
12-1	セッション変更要求受信 (State/リクエスト)	Confirmed/re-INVITE	受信可否およびその条件について記述。受信拒否する場合にはセッション継続有無を含めて処理内容を記述。	ii.7.2節 付表 ii-9
12-2		Confirmed/UPDATE	同上	
12-3		Early/UPDATE (UAS)	同上	
12-4		Early/UPDATE (UAC)	同上	
12-5		Early/PRACK	同上	

	大項目	小項目	プロファイル指定形式	参照
13-1	セッション変更内容 (送信)	受信 IP アドレス	変更要求送信有無について記述。送信する場合には、その契機と条件について記述。	ii.7.3節 付表 ii-10
13-2		受信ポート番号	同上	
13-3		ペイロードタイプ変更	同上	
13-4		ペイロードタイプ削除	同上	
13-5		メディア追加	同上	
13-6		メディア削除	同上	
13-7		方向	同上	
13-8		受信パケット間隔	同上	
14-1	セッション変更内容 (受信)	受信 IP アドレス	変更可否(ステート)	ii.7.3節 付表 ii-10
14-2		受信ポート番号	変更可否(ステート)	
14-3		ペイロードタイプ変更	変更可否(ステート)	
14-4		ペイロードタイプ削除	変更可否(ステート)	
14-5		メディア追加	変更可否(ステート)	
14-6		メディア削除	変更可否(ステート)	
14-7		方向	変更可否(ステート)	
14-8		受信パケット間隔	変更可否(ステート)	

付録 iv.　　動的 IP アドレスを利用する SIP 端末の留意点

iv.1.　動的 IP アドレス利用時の問題点

SIPの端末においては、JF-IETF-RFC3261 [1]で規定されるREGISTERメッセージを利用して動的にレジストラサーバに対してAoRとContactアドレス(URI)のバインディングを登録する機構を用いることが一般的に利用されている。

その際にレジストラサーバでのバインディングは一般的にはソフトステートであるため、登録を行った端末の実際の動的 IP アドレスが解放され、別の端末に割振られた後であっても当該 AoR に対する呼は、その(古い)バインディングにしたがって処理が行われることとなる。この場合には、次のような問題点が生じることになる。

<通信の事実/着信メッセージ内容の漏洩>

当該 AoR 宛のメッセージが第三者に転送されることから、呼の生起者から当該 AoR の保持者へ着信があったという事実が第三者に対して漏洩する可能性がある。

また、SIP メッセージの内容が漏洩することにより、SIP メッセージに含まれる秘密であるかもしれない内容が第三者に漏洩する可能性がある。

<予期しないメッセージの受信>

動的に割当てられた IP アドレスがある別の AoR のバインディングとしてレジストラサーバに残っている場合、別の AoR 宛の着信メッセージを受信することがある。

iv.2.　動的 IP アドレス利用時の端末の推奨動作

動的IPアドレスの払出しとレジストラサーバに登録されるバインディングの内容を統合的に網側で管理が可能であれば、iv.1節の問題点を網側だけの処理で解消することは可能かもしれないが、一般的に網に統合的な管理を要求するものではない。この条件の下においては問題点の解消のために事業者SIP網が管理するユーザが利用する動的IPアドレスを割当てるSIP UA (以下、単にSIP UAとする)は下記の動作を行うことが有効である。

<バインディングの期間の制限>

SIP UAは動的に得たIPアドレスを利用している場合、動的IPアドレスの払出期限を超えてREGISTERリクエストで登録するバインディングの期間を設定しない。(IPアドレス払出期限の延長を行うか、払出期限内のバインディングの期間を設定する)

<バインディングの明示的削除>

SIP UAが(アプリケーション終了等で)着信待受けを終了する場合には、自身がレジストラサーバに対して登録を行ったContactヘッダを指定し、かつ同Contactヘッダのexpiresパラメータ値もしくはExpiresヘッダを0に設定したREGISTERリクエストを利用してバインディングを削除する。また、アプリケーションや機器の再起動などの後に、以前に自身が登録したバインディングを想定可能な場合には、同様に以前に自身が登録したバインディングを明示的に削除する。

なお、Contactヘッダに“*”を指定したREGISTERリクエストの利用は、同ユーザ(同一AoR)の別のSIP UAに関する登録についても削除してしまう可能性があるため、ひとつのAoRに対して複数のバインディングを保持することが想定されるような可能性がある場合には留意が必要である。

<着信メッセージの Request-URI の確認>

SIP UAはSIPメッセージの処理の可否を受信したパケットの受信ポート番号だけで判断するのではなく、SIPリクエストのRequest-URIの値を確認し、自身が期待する値のものであるもののみに限定する(例えば、

自身がREGISTERメッセージのContactヘッダで登録したURI)。このように処理することでSIP UAは動的アドレスの払出期間を過ぎてレジストラサーバに残ってしまったバインディングによる予期しない着信による呼出しを避けることができる。
また、SIP UAがインターネット上にある場合、期待しないRequest-URIを含むメッセージを無視することがIP上の任意のSIPアプリケーションのIPアドレスを探索するようなソフトウェアからの攻撃を避けるためには有効である。

付録 v.　　From ヘッダの SIP URI について

v.1.　本付録の目的

本文の4.5.2節において、インタフェースAにおけるFromヘッダの正当性の確保として、他ユーザへのなりすましが行われないことが要求条件として挙げられているが、本付録において複数の事業者SIP網間において異なるユーザが同じSIP URIを保有しないことなどを保証するためのガイドラインを記載する。

v.2.　匿名 URI

匿名URI (`sip:anonymous@anonymous.invalid`)は全ての事業者SIP網において特定のユーザに対して設定されないことが保証されるため、特定のユーザを指定しない場合においては匿名URIを利用することが推奨される。

事業者SIP網毎に匿名性を示すURI (例: `sip:anonymous@ttc.or.jp`)を利用し、特定のユーザに対して設定されないように管理することは許容されるが、事業者に関する匿名性が失われる可能性があることに留意するべきである。

v.3.　SIP URI

v.3.1.　host 部

`host`部が`hostname`形式を取る場合には事業者SIP網を管理する事業者が利用する権限を持つICANNが管理するTLDもしくはccTLDをルートとする正当なドメイン名もしくはサーバ名とする。この場合、事業者SIP網を管理する事業者が他事業者から運用を委任されたドメイン名もしくはサーバ名を含むこととする。

`host`部が`IPv4address`形式を取る場合には、事業者SIP網を管理する事業者が保有する固定IPアドレスとし、端末等に割振られる動的なIPアドレスを用いないこと。

v.3.2.　user 部

`user`部は、事業者SIP網を管理する事業者が、同事業者SIP網が管理するユーザに対してSIP URIを割り振る場合、指定した`hostname`部に対して一意となるように指定するものとする。`user`部のフォーマットに関しては、一意であることとJF-IETF-RFC3261 [1]で規定されているABNF (Augmented Backus-Naur Form)に従う限りにおいて制限はない。

また、事業者SIP網が管理するユーザではなく他網から受信する信号メッセージによって`From`ヘッダを生成する場合においては、バウンダリが設定するSIP URIの`hostname`部に対してuser部の設定について実際の発信者が異なる場合に同じ値を生成しないような値を選んで設定しなくてはならない。例えば、他網との接続がISUPの場合(インタフェースC)、E.164 番号の文字列を選択することで左記の条件を満たすことが可能である。