TTC技術レポート
Technical Report

TR-1013

H.323 マルチメディアシステムの NAT 越え及びファイアウォール越えに関する要求条件

Technical Report: Requirements for Network Address Translator and Firewall Traversal of H.323 Multimedia Systems

第 1 版

2006 年 10 月 4 日制定

社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　次

0. はじめに

本技術レポートは、ITU Technical Paper “Requirements for Network Address Translator and Firewall Traversal of H.323 Systems” を和訳し訳注を加えて、H.323 システムにおけるファイアウォール／NAT 越え問題に対する参考技術情報のため、纏めたものである。

作成担当：メディア符号化専門委員会　マルチメディアシステム SWG

ITU-T技術文書
H.323マルチメディアシステムの
NAT越え及びファイアウォール越えに関する要求条件

概要

本技術文書の目的は、H.323 マルチメディアシステムにおいて Network Address Translator (NAT)越え及びファイアウォール越えを実現する仕組みが考慮すべき一般的な要求条件を示すことである。また、本文書では、NAT やファイアウォールの利用形態に関してサービスプロバイダ型ネットワーク構成をとる場合と企業ネットワーク型構成をとる場合における H.323 マルチメディアシステムの様々な利用シナリオを定義する。

更新履歴

本文書は、2005 年 7 月 26 日から同年 8 月 5 日にジュネーブで開催された ITU-T 第 16 研究委員会の会合において承認された“Requirements for Network Address Translator and Firewall Traversal of H.323 Systems”の ITU-T Technical Paper（技術文書）第一版である。

概要

H.323 マルチメディアシステムが使用される IP ネットワークにおいて、グローバルユニークな IPv4 アドレスの枯渇対策として、またそれに加え、外部レルムから内部レルムへのアクセスを防止する付加的なセキュリティ手段としても、ネットワークアドレス変換(Network Address Translator, NAT)は急速に普及してきている。

そのため、H.323 のエンドポイントやゲートキーパーは、一つ以上の NAT により隔てられた異なるレルムに配置された場合、内部 IPv4 アドレスが当該レルム外で使用できないため、セッションが NAT を通過しようとする場合、障害にぶつかることになる。このような場合、NAT は、ペイロードに格納されたアドレスを使用して動作する H.323 プロトコルを破綻させ、あるレルム内に配置されたプライベートアドレスを持つ H.323 エンドポイントやゲートキーパーがレルム外のエンティティと全く通信できないといった状況を引き起こす。

H.323 マルチメディアシステムが直面する NAT 越えやファイアウォール越えの問題を解決するため、本技術文書では、サービスプロバイダ型ネットワーク構成と企業ネットワーク型構成の双方をターゲットとし、それらネットワーク構成における一般的要求条件を定義する。あらゆる NAT 越え方式やファイアウォール越え方式は本文書で規定した要求条件を考慮すべきである。

1. 範囲

本文書は、サービスプロバイダ型ネットワーク構成かもしくは企業ネットワーク型構成で使用される H.323 マルチメディアシステムの NAT 越えに関する要求条件を規定する。H.323 マルチメディアシステムの NAT 越えには、H.323 のシグナリングとメディアストリーム（例えば、音声やビデオの Real-time Transport Protocol (RTP)ストリーム）の双方が関連する。

本文書では、単に NAT といえば、IETF RFC3022 で規定されているトラディショナル NAT を意味するものとする。その他の種類の NAT は本文書の対象外である。本文書では、複数レベルのレルムにおいてそれぞれのレベルに NAT が存在するような場合も扱う。

通常、ファイアウォールは NAT と関連ある役割を担う。NAT 自身もファイアウォールの一形態である。具体的には、NAT は、内向きの通信を、それに先立って対応する外向きの通信が行われた場合を除き阻止する。一方で、ファイアウォールは、パケットが通過できるかどうかに関するポリシーを事実上無制限に設定できる。これは、いわゆるファイアウォール越えの方法が、ファイアウォールポリシー次第で、機能することもあるし、機能しないこともあるということを意味する。そのため、ファイアウォールポリシーが所望の機能に悪影響を与えない範囲であれば、本文書で示す要求条件をファイアウォール越え方式に対して適用することも可能である。

2. 参考文献

[1] H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communication systems

[2] H.235, Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals

[3] H.245, Control protocol for multimedia communication

[4] H.323, Packet-based multimedia communications systems

[5] IETF RFC 768 (1980), User Datagram Protocol

[6] IETF RFC 791 (1981), Internet protocol

[7] IETF RFC 793 (1981), Transmission control protocol

[8] IETF RFC 3550 , RTP: A Transport Protocol for Real-Time Applications

[9] IETF RFC 2663, IP Network Address Translator (NAT) Terminology and Considerations.

[10] IETF RFC 2979, Behaviour of and Requirements for Internet Firewalls.

[11] IETF RFC 3022, Traditional IP Network Address Translator

[12] IETF RFC 3304 (2002), Middlebox Communications (midcom) Protocol Requirements.

[13] IETF RFC 3489 (2003), STUN - Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NATs)

3. 略語

ALG	アプリケーション・レベル・ゲートウェイ(Application Level Gateway)
E-GK	企業ネットワークの GK (Enterprise GK)
FW	ファイアウォール(Firewall)
GK	ゲートキーパー(Gatekeeper)
GW	ゲートウェイ(Gateway)
IP	インターネットプロトコル(Internet Protocol)
MC	多地点コントローラ(Multipoint Controller)
MCU	多地点会議制御ユニット(Multipoint Control Unit)
MP	多地点プロセッサ(Multipoint Processor)
NAT	ネットワークアドレス変換(Network Address Translator)
PC	パーソナルコンピュータ(Personal Computer)
RTP	リアルタイム転送プロトコル(Real-time Transport Protocol)
S-GK	サービスプロバイダの GK (Service Provider GK)
TCP	伝送制御プロトコル(Transmission Control Protocol)
UDP	ユーザデータグラムプロトコル(User Datagram Protocol)

4. 用語定義

4.1. ゲートキーパー(Gatekeeper)

H.323 の定義によると、ゲートキーパー(Gatekeeper, GK)は、H.323 エンティティであり、ネットワーク上にあって、H.323 の端末、ゲートウェイ、 MCU に対しアドレス変換やネットワークへのアクセス制御の機能を提供する。また、ゲートキーパーは、端末、ゲートウェイ、MCU に対し、帯域管理やゲートウェイ探索などのサービスを提供する場合がある。

4.2. ゲートウェイ(Gateway)

H.323 の定義によると、H.323 ゲートウェイ(Gateway, GW)は、ネットワークのエンドポイントであり、パケット型ネットワーク上の H.323 端末と回線交換型ネットワーク上の他の ITU 端末とのリアルタイム双方向通信を取り持つか、他の H.323 ゲートウェイへのリアルタイム双方向通信をサポートする。ここで、“他の ITU 端末”には、H.310（ATM）、H.320（ISDN）、H.321（ATM 上の H.320）、H.322（QoS 保証 LAN）、H.324（GSTN を想定した勧告全般、H.324/M として知られるモバイルアプリケーション用の Annex C、H.324/I として知られる ISDN 用の Annex D）、V.70（DSVD, Digital Simultaneous Voice and Data）などの各勧告に準拠する端末が含まれるものとする。

4.3. H.323 エンティティ(H.323 entity)

H.323 の定義によると、H.323 エンティティは H.323 システム構成要素であり、端末、ゲートウェイ、ゲートキーパー、MC、MP、MCU のいずれかである。

4.4. エンドポイント(Endpoint)

H.323 では、エンドポイントは、H.323 の端末、ゲートウェイ、MCU のいずれかであると定義されている。エンドポイントは発呼も着呼もできる。また、エンドポイントは、情報ストリームを生成したり終端したりする。

4.5. ネットワークアドレス変換(Network Address Translation)

RFC2663 によると、ネットワークアドレス変換(network address translation)は、公衆網と私設網の間でアドレスやポート番号の対応付けを提供するサービスである。ネットワークアドレス変換により、私設網内のホストは外部ネットワーク上の相手と透過的に通信することが可能となり、その逆もまた可能となる。

4.6. トラディショナル NAT (Traditional NAT)

トラディショナル NAT では、セッションは私設網から外部へ向けての一方向に限られる。逆方向のセッションは、事前に選択されたホストへの静的マッピングを用いることで、例外的に許可することができる。ベーシック NAT や NAPT (Network Address Port Translation)は、いずれもトラディショナル NAT の変形である。これらについては RFC2663 参照。

4.7. アプリケーション・レベル・ゲートウェイ(Application Level Gateway)

アプリケーション・レベル・ゲートウェイ(Application Level Gateway, ALG)は、H.323 アプリケーションに特化したネットワークアドレス変換を行うものである。（RFC2663 参照）

4.8. レルム(Realm)

RFC2663 の定義によると、アドレスレルム(address realm)は、アドレスがエンティティに対し一意に割り当てられており、それによりエンティティへとデータグラムをルーティングできると認められるネットワーク領域のことである。ネットワーク領域内部で使用されるルーティングプロトコルは、ネットワークアドレスが割り振られたエンティティへのルート検索に対して責任を持つ。本文書で扱う NAT は IPv4 環境に限定する。IPv6 環境など他のネットワーク環境における NAT の使用は本文書では扱わない。

4.9. ゾーン(Zone)

H.323 では、ゾーン(Zone)は、一つのゲートキーパーが管理する全ての端末、ゲートウェイ(GW)、多地点会議制御ユニット(MCU)の集まりであると定義されている。よって、一つのゾーンはただ一つのゲートキーパーを持つ。ゾーンはネットワークトポロジーに依存せず、一つのゾーンがルータやその他の装置で接続された複数のネットワークセグメントに跨ることもある。ゾーン内に NAT が存在する場合、そのゾーンは二つ以上のレルムで構成されることになるだろう。

4.10. NAT オペレーションモード(NAT Operation Mode)

RFC3489 では、NAT のオペレーションモードを、フルコーン(Full Cone)、制限コーン(Restricted Cone)、ポート制限コーン(Port Restricted Cone)、対称(Symmetric)の 4 種類に分類している。それぞれの定義は以下の通りである。

- フルコーン：フルコーン NAT は、同一の内部 IP アドレス及びポート番号からのパケットを、常に同一の外部 IP アドレス及びポート番号に対応付ける。更に、任意の外部ホストは、内部ホストが対応付けられた外部アドレスにパケットを送ることで、その内部ホストにパケットを届けることができる。
- 制限コーン：制限コーン NAT は、同一の内部 IP アドレス及びポート番号からのパケットを、常に同一の外部 IP アドレス及びポート番号に対応付ける。ただし、フルコーン NAT と異なり、外部ホストが内部ホストにパケットを送信できるのは、それに先立って内部ホストが外部ホストの IP アドレスに向けてパケットを送信した場合に限られる。

- ポート制限コーン：ポート制限コーン NAT は、制限コーン NAT に類似するが、制限にポート番号が含まれる。具体的に言うと、外部ホストが送信元 IP アドレス X 及び送信元ポート番号 P で内部ホストにパケットを送信できるのは、それに先立って内部ホストが IP アドレス X 及びポート番号 P に向けてパケットを送信した場合に限られる。
- 対称：対称 NAT は、同一の内部 IP アドレス及びポート番号から特定の宛先 IP アドレス及びポート番号へのパケットを、常に同一の外部 IP アドレス及びポート番号に対応付ける。この場合、同一ホストが同一の送信元アドレス及び送信元ポート番号でパケットを送信しても、宛先が異なるならば、異なる対応付けがなされる。更に、内部ホストからのパケットを受信する外部ホストのみが UDP パケットをその内部ホストへと返送できる。

5. 規則

本文書では、「しなければならない／するべきである／してもよい」は、全て拘束力のない表現である。これらの要求条件は、全て参考推奨であり、実装に必須では無いからである。

6. H.323 マルチメディアシステムにおける NAT 越えの課題

6.1. NAT の一般的な効果

6.1.1 パケットとペイロード間の不整合アドレス

H.323 プロトコルは、セッションの確立メッセージにアドレスとポート情報を埋め込んでいる。NAT は IP パッケージの中のアドレスに関連する情報の変換を実行する際に、送信元 IP アドレス、及び／または、ポートを外部 IP アドレス、及び／または、ポートに変換する。この場合、H.245 メッセージのようなペイロードに含まれている IP アドレスとポートは、IP パケットの送信元 IP アドレスとポートに整合しなくなる。そのため、受信者が正しく送信者に返信する事が出来ず、送信者と受信者の間のメディアセッションの確立が失敗することになる。

6.1.2 NAT 構成の複雑性

ある NAT モードにおいては、NAT 越えメカニズムが成功するかも知れないが、別の NAT モードでは失敗する可能性がある。特に複数レベルのレルムにおいて、NAT の各レベルが異なるモードで動作する可能性がある。この場合、1 つ以上のレベルの NAT の支配下にある場合、NAT 越えメカニズムは失敗する可能性がある。

6.2. ファイアウォール機能の一般的な効果

6.2.1 ポートの動的割り当て

H.323 マルチメディアシステムでは、メディアのための伝送ポートは動的に割り当てられ、ファイアウォールを通過する H.245 メッセージに含まれて交換される。もし、ファイアウォールが伝送ポートを知らなかった場合、メディアストリームはファイアウォールに達した時点でブロックされる。

6.2.2 ファイアウォールのセキュリティポリシー

通常、ファイアウォールは、出て行くパケットは通過を許可されており、入ってくるパケットは拒否するべきであると見なしている。

そのため、外側のレルムの H.323 エンドポイントから、内側のエンドポイントのレルムに向けて発呼されたセッションは、ブロックされる。従って、内側の H.323 エンドポイントは、外側のエンドポイントと通信することができない。外側の H.323 エンドポイントが内側の呼を受信することを可能とするためには、全ての外側の IP アドレスを利用できるようにし、外側のレルムから、内側のレルムにアクセスを許可するような幾つかの特別なポリシーをファイアウォールに構築しなければならない。その結果、内側のレルムを幾つかの潜在的なセキュリティリスクにさらす事になる。

7. H.323 マルチメディアシステムの NAT 越え

H.323 マルチメディアシステムは、サービスプロバイダ型ネットワークワーク構成か、企業ネットワーク型構成で使用することができる。サービスプロバイダ型ネットワーク構成では、GK はサービスプロバイダによって提供され、制御される。企業ネットワーク型構成では、GK は、企業によって提供され、制御される。

本文書では、E-GK は、企業ネットワークの GK を意味し、S-GK は、サービスプロバイダの GK を意味する。

7.1. サービスプロバイダ型ネットワーク構成で使用される NAT/FW

7.1.1 グローバル固有の登録アドレスを持つレルムにおける GK

グローバル固有な IPv4 アドレスの消費を最小にするため、H.323 端末は、通常、プライベートアドレスを持つレルムに設置される。レルムの出口で NAT はアドレス、及び、ポート変換機能を提供するために設置される。プライベートアドレスを持つレルムは、一つのレベル、または、複数レベルのレルムになっても良い。プライベートアドレスが複数レベルのレルムであるシナリオの場合、H.323 端末を、どのレベルのレルムに設置しても良い。加えて、H.323 端末をグローバル固有な登録アドレスを持つレルム内に設置しても良い。

サービスプロバイダ型ネットワーク構成では、サービスプロバイダによって提供されたゲートキーパー、ゲートウェイ、MCU は、通常、グローバル固有な登録アドレスを持つレルム内に置かれ、ファイアウォールの背後に設置される。このネットワーク構成を図 1 に図示する。シナリオの詳細は、8.1.1 項に記述する。

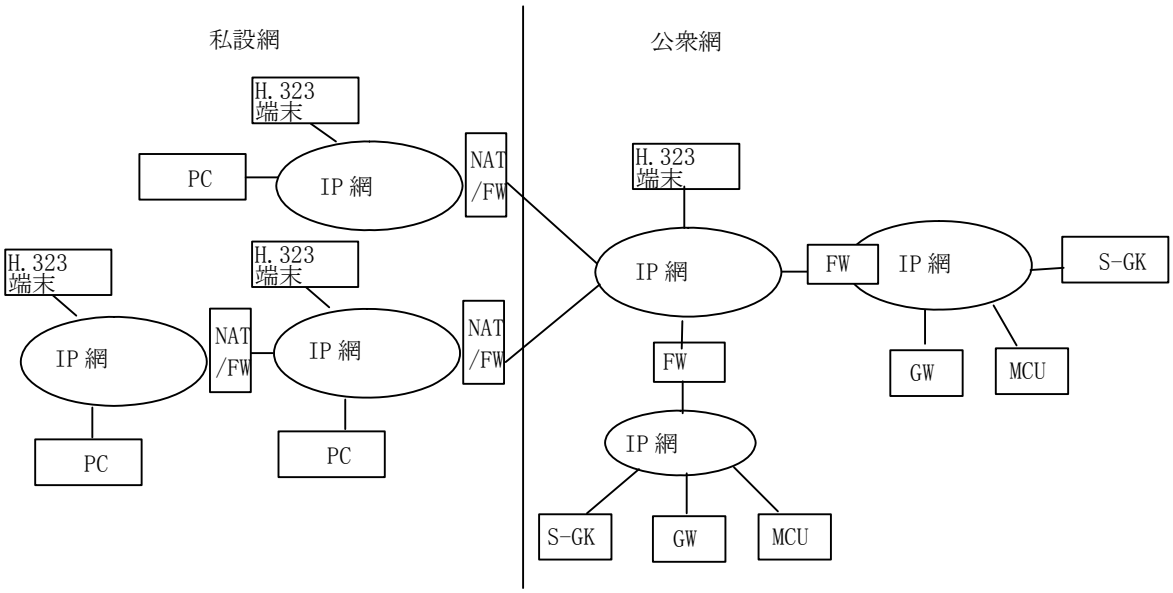

図 1. サービスプロバイダ型ネットワーク構成における H.323 マルチメディアシステム
（公衆網に GK を設置）

7.1.2 プライベートアドレスを持つレルムにおける GK

ある場合においてゲートキーパー、ゲートウェイ、MCU はプライベートアドレスを持つレルム内に設置し、セキュリティの考慮のため、図 2 に示すように、ファイアウォール機能を持つ NAT の背後に設置することができる。

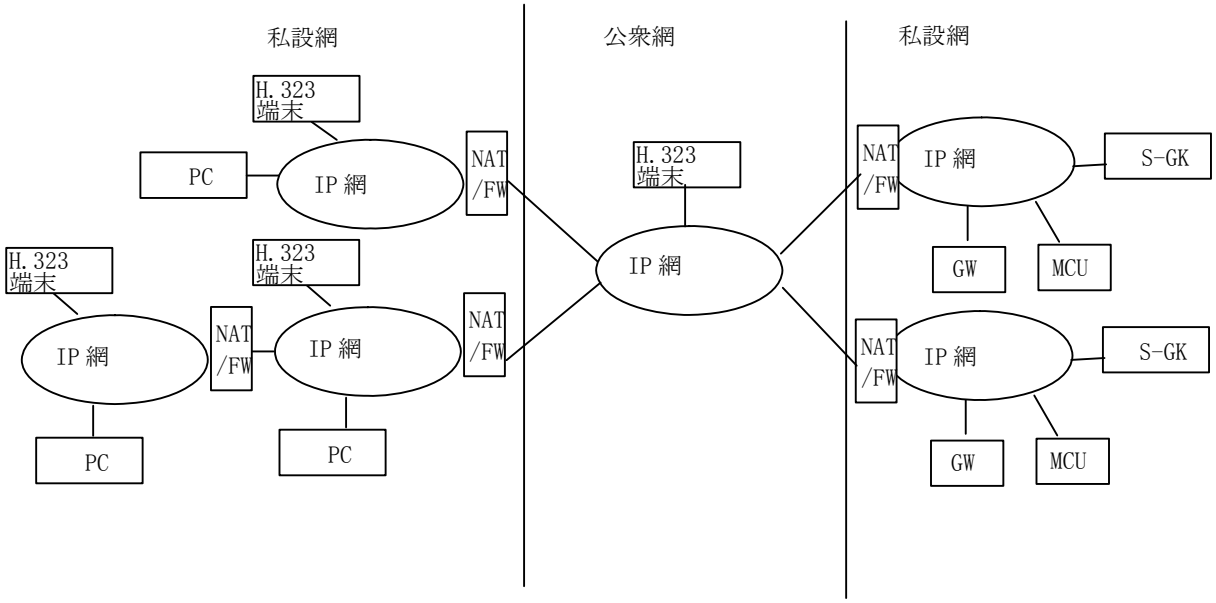

図 2. サービスプロバイダ型ネットワーク構成における H.323 マルチメディアシステム
（私設網に GK を設置）

7.2. 企業ネットワーク型構成で使用される NAT/FW

7.2.1 企業によって提供される GK

企業ネットワーク型構成では、企業レルムの全体は、プライベートアドレスを持つ一つ以上のレルムからなる。場合によっては、企業レルムは、複数レベルのレルムであっても良い。これらの企業レルムは、パブリックアドレスを持つレルムに接続されている。NAT は、アドレス、及び、ポート変換機能を実現するために異なるレルムの境界に配置されるべきである。

企業網全体にわたって H.323 マルチメディアサービスを提供するため、H.323 エンドポイント、及び、企業の GK は、図 3 に図示するとおり、企業レルムに設置されている。

この場合、企業の GK は企業レルムに設置しても良い。もし、企業の H.323 エンドポイントが同じ企業内の H.323 エンドポイントに発呼した場合、それらの端末は、企業の GK によって相互に接続される。もし、企業 H323 エンドポイントが、企業レルム外の H.323 エンドポイントに発呼した場合、企業の GK はサービスプロバイダの GK に接続される。

企業ネットワーク型構成のためのシナリオの詳細は、8.2 節で定義される。

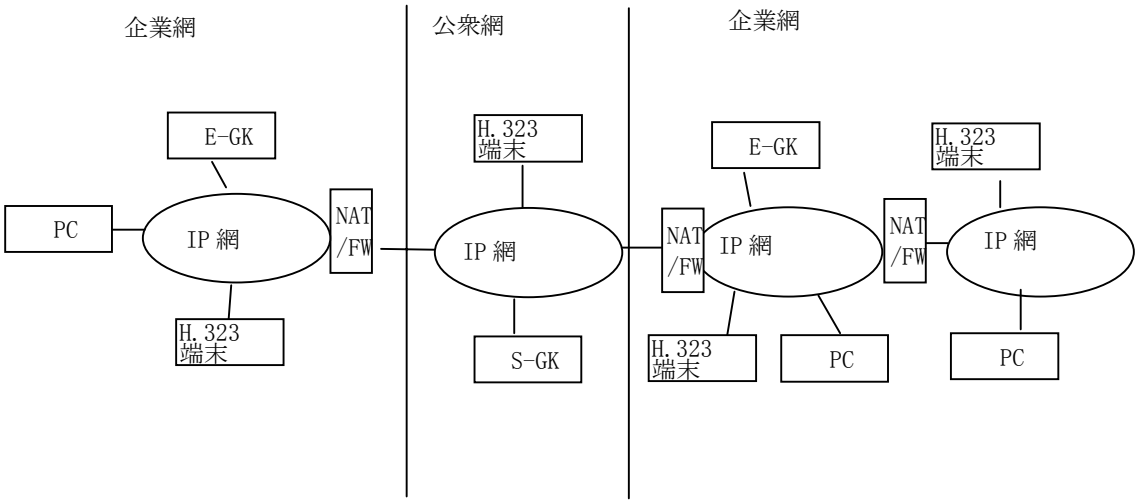

図 3. 企業ネットワーク型構成における H.323 マルチメディアシステム

企業ネットワーク型構成では、企業の H.323 エンドポイントは、公衆網からアクセスする場合など、企業レルムから企業レルムの外側に移動する事ができる。（図 4 参照）

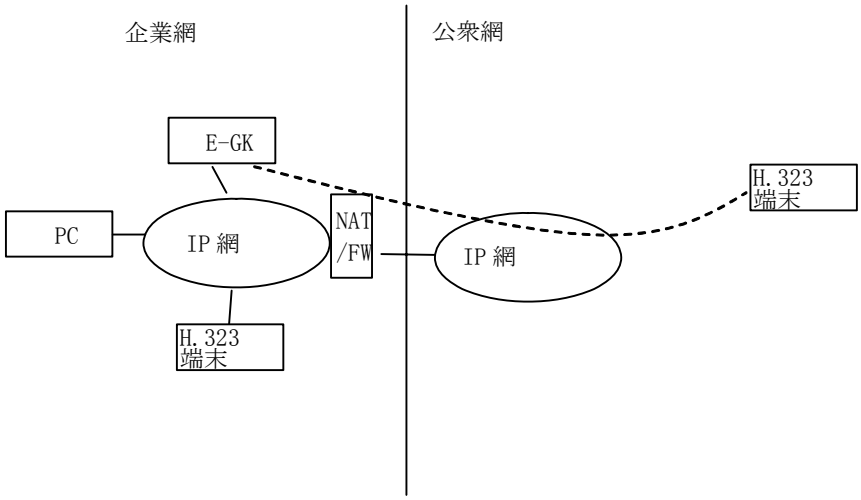

図 4. 企業ネットワーク型構成における H.323 マルチメディアシステム
（外側のレルムからのアクセス）

7.2.2　　サービスプロバイダによって提供される仮想 GK

時として、企業では、そのレルム内に GK を持たない場合がある。しかし、図 5 に図示されるようにサービスプロバイダレルム内の GK を仮想企業 GK として使用することができる。

この企業ネットワーク型構成の利用は、本文書の範囲外である。

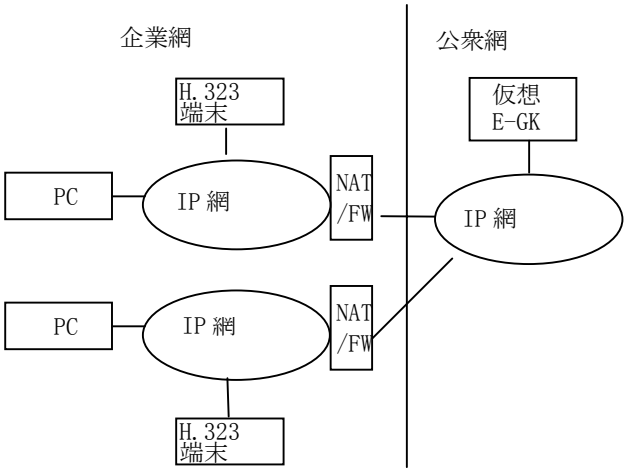

図 5. 企業ネットワーク型構成における H.323 マルチメディアシステムのための仮想 GK

8. H.323 マルチメディアシステムのシナリオ

8.1. サービスプロバイダ型ネットワーク構成のシナリオ

8.1.1 GK がグローバル固有の登録アドレスを持つレルムにある場合のシナリオ

この節では、サービスプロバイダ GK がグローバル固有のアドレスを持つレルムに位置しているときにおけるサービスプロバイダ型ネットワーク構成の可能なすべてのシナリオを扱っている。

サービスプロバイダシナリオ 1 を図 6 に示しており、そこでは H.323 エンドポイントはプライベートアドレスを割り振られた同一のレルムに存在する。このシナリオでは、各 H.323 エンドポイントは発呼者または被呼者として動作することができる。

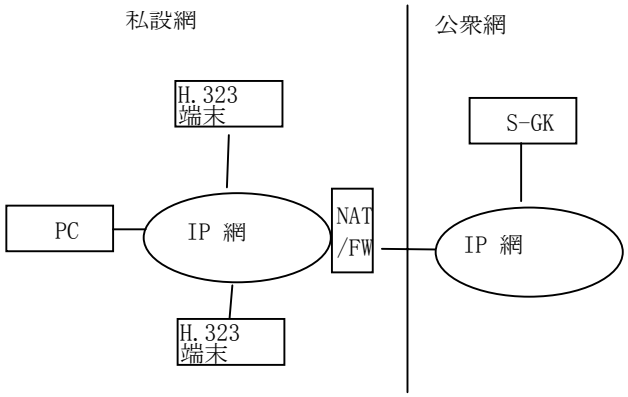

図 6 - サービスプロバイダシナリオ 1

サービスプロバイダシナリオ 2 を図 7 に示す。H.323 エンドポイントはプライベートアドレスを持つ 2 つの異なったレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは発呼者または被呼者として動作することができる。

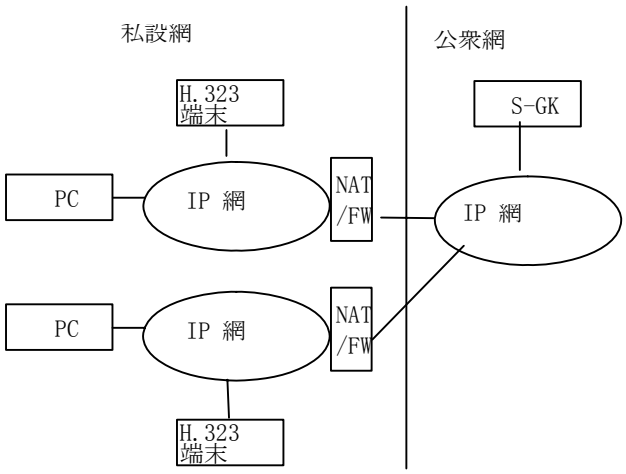

図 7 - サービスプロバイダシナリオ 2

サービスプロバイダシナリオ 3 を図 8 に示す。H.323 エンドポイントはプライベートアドレスを持つレルムに置かれ、別の H.323 エンドポイントはパブリックアドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは発呼者または被呼者として動作することができる。

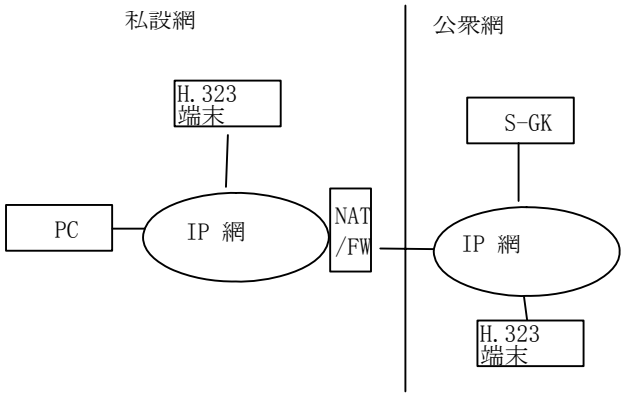

図 8 - サービスプロバイダシナリオ 3

サービスプロバイダシナリオ 4 を図 9 に示す。H.323 エンドポイントは、プライベートアドレスを持つ複数レベルの同一レルムに置かれる。このシナリオでは、各 H.323 エンドポイントは発呼者または被呼者として動作することができる。

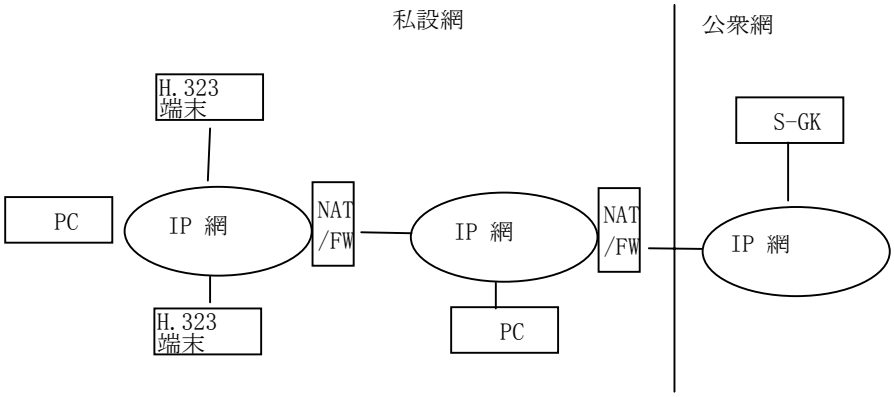

図 9 - サービスプロバイダシナリオ 4

サービスプロバイダシナリオ 5 を図 10 に示す。H.323 エンドポイントはプライベートアドレスを持つ、複数レベルの異なったレルムに置かれる。このシナリオでは H.323 エンドポイントは発呼者または被呼者として動作することができる。

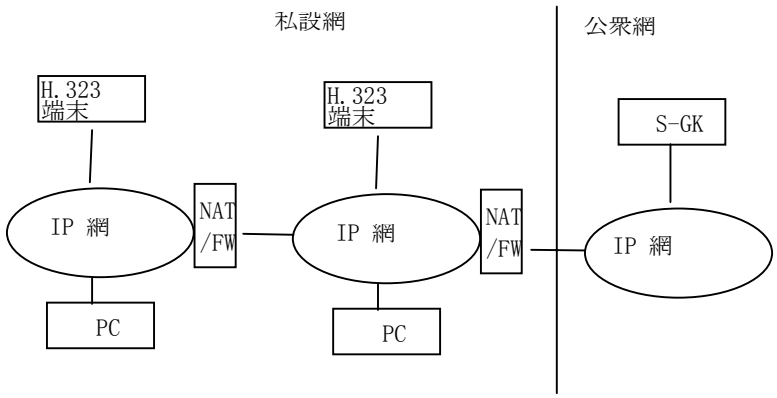

図 10 - サービスプロバイダシナリオ 5

サービスプロバイダシナリオ 6 を図 11 に示す。H.323 エンドポイントはプライベートアドレスを持つ複数レベルのレルムに置かれ、もう一方の H.323 エンドポイントはプライベートアドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは発呼者または被呼者として動作することができる。

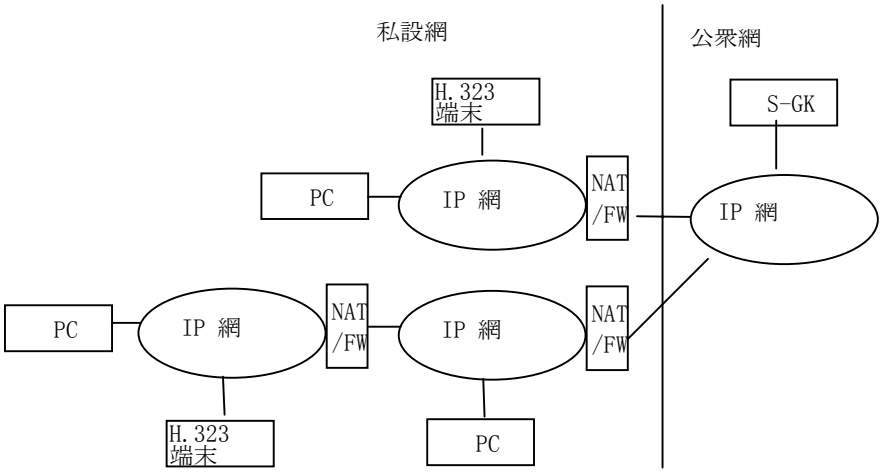

図 11 - サービスプロバイダシナリオ 6

サービスプロバイダシナリオ 7 を図 12 に示す。H.323 エンドポイントはプライベートアドレスを持つ複数レベルのレル

ムに置かれ、もう一方の H.323 エンドポイントはパブリックアドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは発呼者または被呼者として動作することができる。

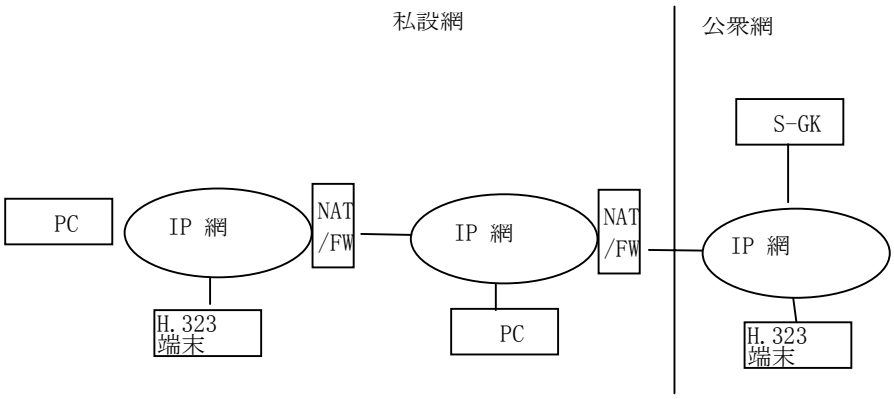

図 12 – サービスプロバイダシナリオ 7

8.1.2　GK がプライベートアドレスを持つレルムにある場合のシナリオ

サービスプロバイダの GK がプライベートアドレスを持つレルムにある場合については、H.323 マルチメディアシステムの企業ネットワーク型構成と同じである。それゆえにこの場合は企業ネットワークレルム内に企業の GK を持つ企業ネットワーク型構成を参考にすることができる。

8.2.　企業ネットワーク型構成のシナリオ

8.2.1　企業ネットワーク GK のシナリオ

この節では、企業ネットワーク型構成で可能な全てのシナリオを記述している。企業ネットワークレルム内の H.323 エンドポイントは、企業ネットワークレルム内にある企業 GK に接続されている。サービスプロバイダ GK を通じて、企業ネットワークレルム内の H.323 エンドポイントは、企業ネットワークレルム外の H.323 エンドポイントと相互接続することができる。

企業ネットワーク型構成シナリオ 1 を、図 13 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

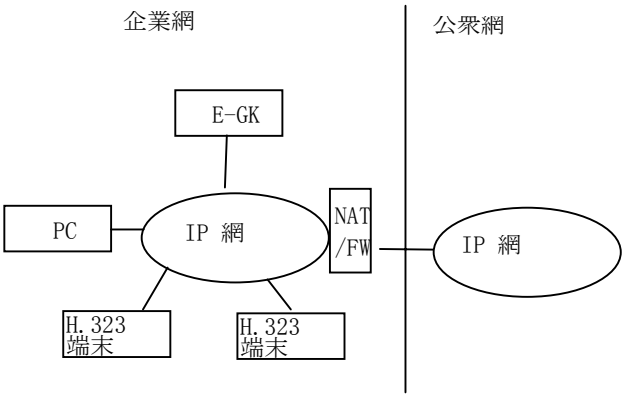

図 13 -企業ネットワーク型構成シナリオ 1

企業ネットワーク型構成シナリオ 2 を、図 14 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ同じレルムに置かれる。もう一方の H.323 エンドポイントはプライベートアドレスを持つ別のレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

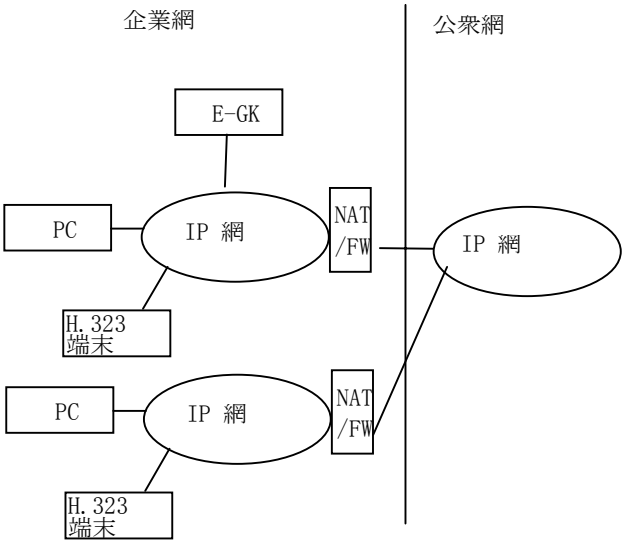

図 14 -企業ネットワーク型構成シナリオ 2

企業ネットワーク型構成シナリオ 3 を、図 15 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ同じレルムに置かれる。もう一方の H.323 エンドポイントと企業 GK はプライベートアドレスを持つ別のレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

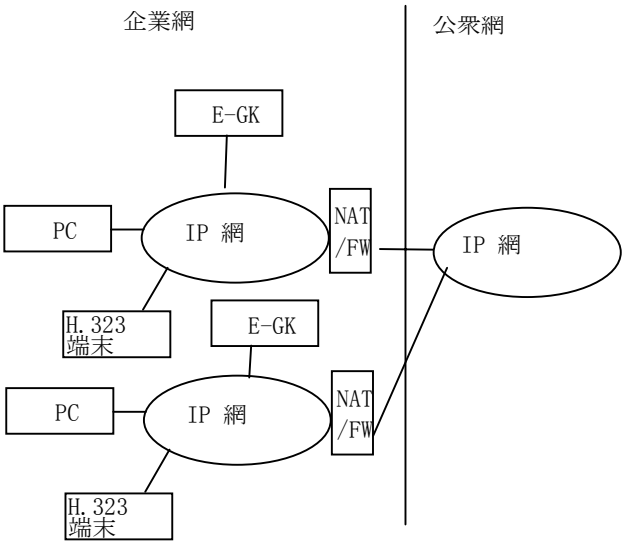

図 15 -企業ネットワーク型構成シナリオ 3

企業ネットワーク型構成シナリオ 4 を、図 16 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ同じレルムに置かれる。もう一方の H.323 エンドポイントとサービスプロバイダ GK はグローバル固有の登録アドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

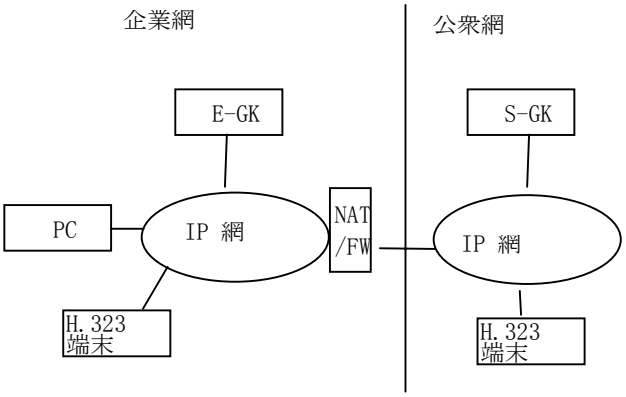

図 16 -企業ネットワーク型構成シナリオ 4

企業ネットワーク型構成シナリオ 5 を、図 17 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ、異なったレルムに置かれる。もう一方の H.323 エンドポイントとサービスプロバイダ GK はグローバル固有の登録アドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

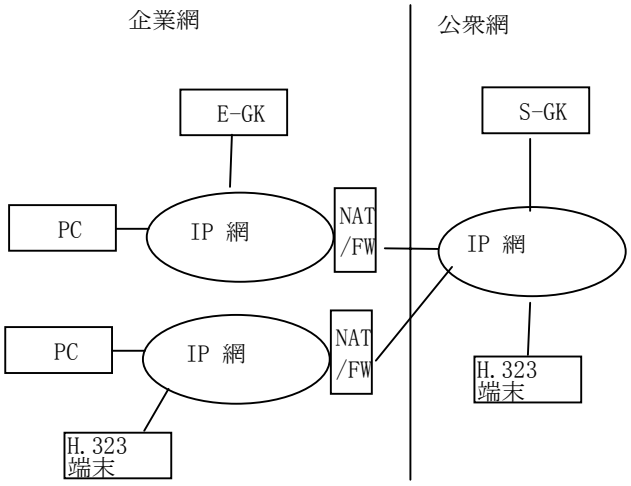

図 17 -企業ネットワーク型構成シナリオ 5

企業ネットワーク型構成シナリオ 6 を、図 18 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ複数レベルの企業ネットワークレルムに置かれる。もう一方の H.323 エンドポイントとサービスプロバイダ GK はグローバル固有の登録アドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

H.323 エンドポイント間の相互接続は、企業 GK 及びサービスプロバイダ GK によって実現される。

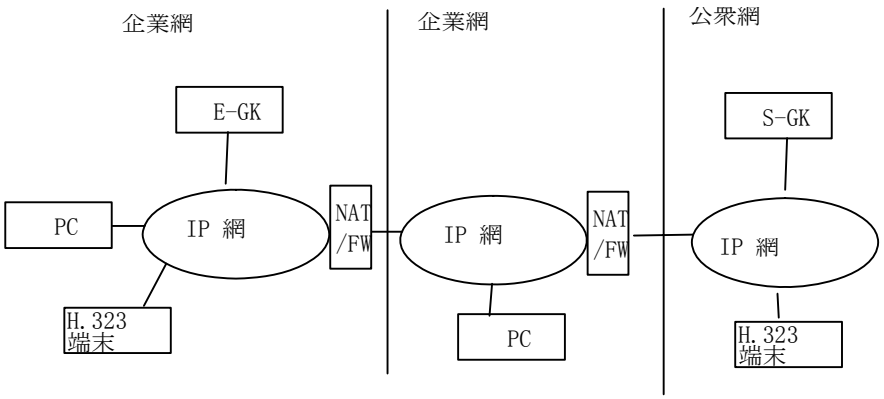

図 18 -企業ネットワーク型構成シナリオ 6

企業ネットワーク型構成シナリオ 7 を、図 19 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ異なった複数レベルの企業ネットワークレルムに置かれる。もう一方のサービスプロバイダ GK と H.323 エンドポイントはグローバル固有の登録アドレスを持つレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

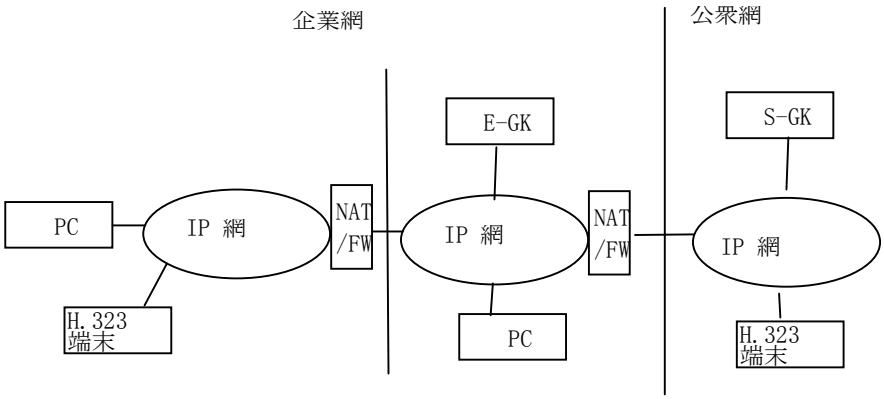

図 19 -企業ネットワーク型構成シナリオ 7

企業ネットワーク型構成シナリオ 8 を、図 20 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ企業ネットワークレルムに置かれる。もう一方の H.323 エンドポイントは異なった複数レベルのレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

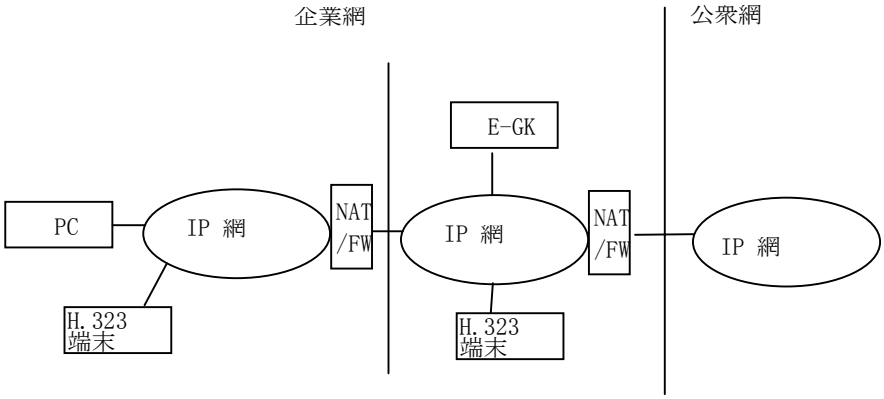

図 20 – 企業ネットワーク型構成シナリオ 8

企業ネットワーク型構成シナリオ 9 を、図 21 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ企業ネットワークレルムに置かれる。もう一方の H.323 エンドポイントと企業 GK は異なった複数レベルのレルムに置かれる。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

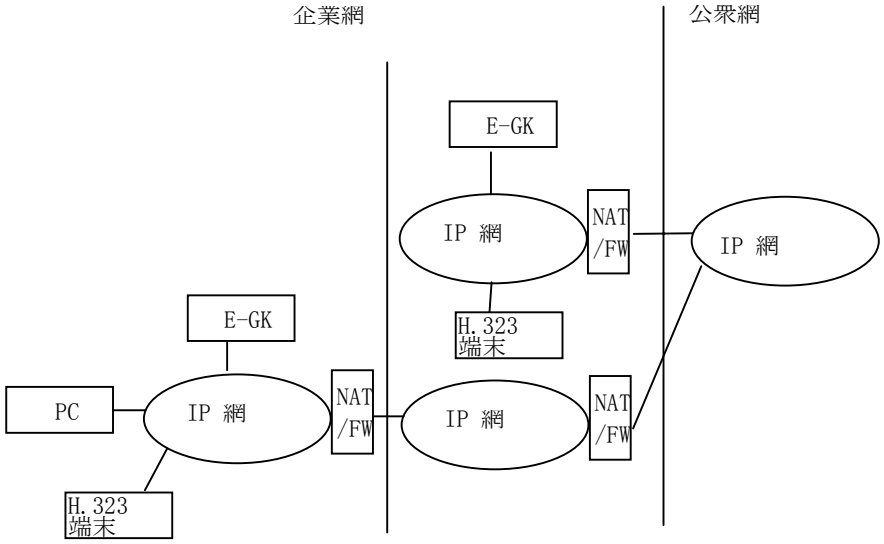

図 21 -企業ネットワーク型構成シナリオ 9

企業ネットワーク型構成シナリオ 10 を、図 22 に示す。H.323 エンドポイントと企業 GK はプライベートアドレスを持つ企業ネットワークレルムに置かれる。もう一方の H.323 エンドポイントは、企業ネットワークレルムの外に移動している。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

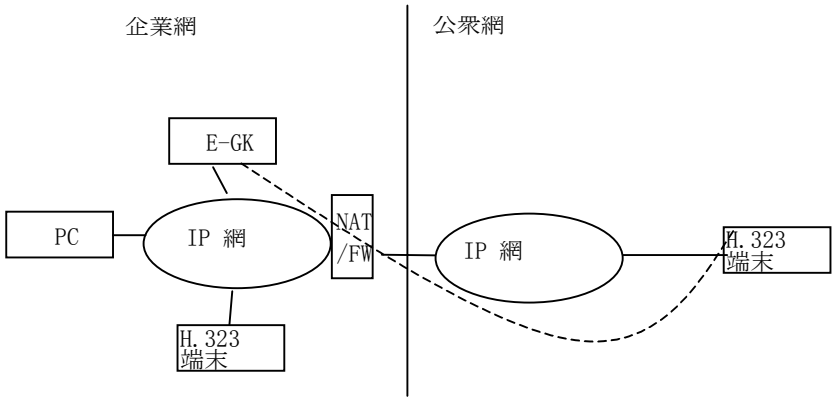

図 22 -企業ネットワーク型構成シナリオ 10

企業ネットワーク型構成シナリオ 11 を、図 23 に示す。企業 GK はプライベートアドレスを持つレルムに置かれる。H.323 エンドポイントは、企業ネットワークの外のレルムに移動している。もう一方の H.323 エンドポイントとサービスプロバイダ GK はグローバル固有の登録アドレスを持つレルムのような、サービスプロバイダのレルム内にある。このシナリオでは、各 H.323 エンドポイントは、発呼者または被呼者として動作することができる。

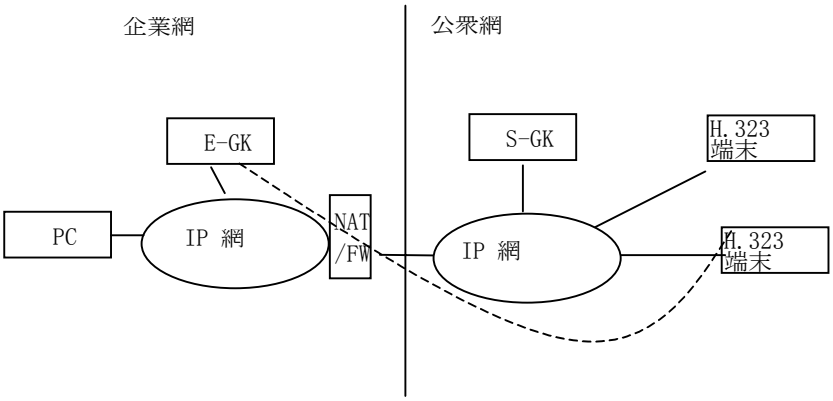

図 23 -企業ネットワーク型構成シナリオ 11

8.2.2　仮想 GK がサービスプロバイダにより提供される場合のシナリオ

仮想 GK がサービスプロバイダにより提供される場合の企業ネットワーク型構成のシナリオは、この文書の範囲外である。

9.　H.323 マルチメディアシステムのための NAT 越え要求条件

9.1.　一般的要求条件

以下の要求条件が、8 章に定義された NAT 越えシナリオ全てに適用される。

a) H.323 マルチメディアシステムのための NAT 越えは、可能な限り、複数レベルの NAT 越えを考慮すべきであることを推奨する。

b) 8 章で述べられた全てのネットワーク型構成におけるそれぞれの H.323 エンドポイントは、発呼者あるいは被呼者のいずれでも動作可能であるべきである。

c) H.323 マルチメディアシステムのための NAT 越え方式は、プライベートアドレスを持つレルムの GK と、グローバル固有の登録アドレスを持つレルムの GK の両方を考慮すべきであることを推奨する。異なった NAT 越え方式は、H.323 マルチメディアシステムにおいて共存すべきである。

d) 異なった NAT 越え方式は、同一レルムの境界で共存すべきである。

e) NAT 越え方式は、どの NAT 操作モードをサポートするのか明らかにすべきである。

9.1.1　サービスプロバイダ型ネットワーク構成のための一般的要求条件

9.1 節の要求条件に追加して、以下の要求条件をサービスプロバイダ型ネットワーク構成に考慮すべきである。

a) H.323 マルチメディアシステムのための NAT 越えは、可能な限り、8.1 節で述べられた全てのシナリオの考慮を推奨する。

9.1.2　企業ネットワーク型構成のための一般的要求条件

9.1 節の要求条件に追加して、以下の要求条件を企業ネットワーク型構成に考慮すべきである。

a) 企業ネットワークレルムにおける GK は、企業ネットワークレルムにおける H.323 マルチメディアサービスをサポートすべきである。

b) 企業ネットワークレルム内の H.323 エンドポイントと企業ネットワークレルム外の H.323 エンドポイントは、企業ネ

ットワーク GK とサービスプロバイダ GK 間で相互接続しなければならない。
c) H.323 マルチメディアシステムのための NAT 越えは、8.2 節で描かれた全てのシナリオを考慮すべきである。
d) 企業ネットワーク H.323 エンドポイントを企業ネットワークレルム外に移動することができる。そのため、企業ネットワーク H.323 エンドポイントは、外側から企業ネットワークレルムにアクセスすることができる。

9.2. H.323 マルチメディアシステムにおける機能エンティティの要求条件

9.2.1 H.323 エンドポイントのための要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、ソフトウェアアップグレードや、セキュリティや QoS ポリシーの変更など、H.323 エンドポイントに求められる変更を明示すべきである。

9.2.2 GK のための要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、ソフトウェアアップグレードや、セキュリティや QoS ポリシーの変更などの、H.323 エンドポイントに求められる変更を明示すべきである。

9.2.3 NAT のための要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、4 つの NAT 操作モード全てを可能な限り考慮すべきで、どの NAT 操作モードがふさわしいかを指示すべきである。
b) H.323 マルチメディアシステムのための NAT 越え方式は、トラディショナル NAT において求められる変更を（例えばソフトウェアアップグレード）を明示すべきである。
c) NAT は、シグナリングメッセージやメディアストリームの通過を可能にするために、対応するポリシーに従いプロビジョニングを行ってもよい。

9.3. シグナリングとメディアストリームの要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、シグナリングとメディアストリームの通過を一緒に考慮すべきである。
b) H.323 マルチメディアシステムのための NAT 越え方式は、ITU-T H.323v3、H.245v7、H.225.0v4、H.235v3 以降のものをサポートしなければならない。H.323、H.245、H.225.0、H.235 のそれ以降のどのバージョンでもサポートしてよい。
c) H.323 マルチメディアシステムのための NAT 越えを可能にするプロトコル拡張は、ITU-T H.323、H.225.0、H.245、H.235 の規定に基づき、矛盾がないようにしなければならない。
d) もし H.323 エンドポイントが同一レルム内にあり、あるいは複数レベルレルムの同一レベル内にあるならば、マルチメディアストリームは H.323 エンドポイント間で直接流すか、NAT を経由して渡すかのどちらかが可能である。
e) もし H.323 エンドポイントが異なったレルム内にあるか、複数レベルレルムの異なったレベル内にあるならば、H.323 エンドポイント間のマルチメディアストリームは、NAT 経由で渡さなければならない。

9.4. パフォーマンスと QoS の要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、NAT パフォーマンスの低下をできるだけ少なくするなど、NAT パフォーマンスへの影響を考慮すべきであることを推奨する。

b) H.323 マルチメディアシステムのための NAT 越え方式は、H.323 マルチメディアシステムにおける QoS の低下をできるだけ少なくするなど、H.323 マルチメディアシステムにおける QoS への影響を考慮すべきであることを推奨する。

9.5. セキュリティの要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、サービスプロバイダ型ネットワーク構成と企業ネットワーク型構成の両方について H.323 マルチメディアシステムのセキュリティを低下させるべきではない。
b) NAT 越え方式は、自身で H.323 マルチメディアシステム用のセキュリティを提供すべきである。
c) （IPsec のような）ネットワークレイヤのその他のセキュリティ方式を持つ H.323 マルチメディアシステムに関する NAT 越え方式の要求条件は、本文書の範囲外である。

9.6. ネットワーク管理システムの要求条件

a) サービスプロバイダ型ネットワーク構成において、H.323 マルチメディアシステムのための NAT 越え方式は、元々ある H.323 マルチメディアシステムのためのネットワーク管理方式に影響を及ぼすべきでない。
b) 企業ネットワーク型構成における H.323 マルチメディアシステムのためのネットワーク管理は、本文書の範囲外である。

9.7. 信頼性の要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、NAT 越えを必要としないネットワーク部分の信頼性を低下させるべきではない。
b) NAT 越えに関わるネットワーク部分について、H.323 マルチメディアシステムのための NAT 越え方式は、信頼性の低下をできるだけ少なくすべきである。

9.8. 課金の要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、H.323 エンドポイントの課金情報の収集を妨げるべきではない。注：H.323 マルチメディアシステムのための課金情報の収集方式は本文書の範囲外である。

9.9. サービス提供の要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、サービス提供の能力を低下させるべきでなく、そのため、与えられた H.323 ゾーンにおいて提供された既存サービス全てをサポートすべきである。

9.10. 他の通過方式と共存する要求条件

a) サービスプロバイダや企業ネットワークは、そのネットワークに 2 つ以上の NAT 越え方式を配置してもよい。そのため、異なった NAT 越え方式が同じネットワークに共存できることが望ましい。
b) しかしながら、より良い相互接続性や管理のしやすさのために、サービスプロバイダや企業は、そのネットワークに共存する異なった NAT 越えの方式数を最小限にすることが推奨である。

9.11. モビリティの要求条件

a) H.323 マルチメディアシステムのための NAT 越え方式は、H.323 エンドポイントのモビリティ能力において負の影響を最小限にする考慮を払うべきである。