TTC技術レポート
Technical Report

TR-1012

H.323 システムの ファイアウォール/NAT 越え問題に 関する技術レポート

Technical Report: Firewall and NAT Traversal Problems in H.323 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 “Firewall and NAT Traversal Problems in H.323 Systems” を和訳し注を加えて、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システムのファイアウォール/NAT越え問題

概要

本技術文書は、現在の IP ネットワークにファイアウォール（FW）及び NAT (Network Address Translator)装置が存在することにより H.323 システムに引き起こされる問題点を分析する。
本文書は、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」で定義されるシナリオ及び ITU-T 第 16 研究委員会で研究されたシナリオについて言及し、各シナリオに関連する FW/NAT 越え問題を特定しようと試みるものである。

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 ITU-T 技術文書“Firewall and NAT Traversal Problems in H.323 Systems ”の第一版である。

概要

本技術文書では、H.323 システムにおいて現在の IP ネットワークに FW、NAT 装置が存在することにより引き起こされる問題について分析し、各シナリオに関連する FW/NAT 越え問題を特定しようと試みるものである。

1. 範囲

本技術文書では、H.323 システムにおいて現在の IP ネットワークに FW、NAT 装置が存在することにより引き起こされる問題について分析する。本文書は、ITU-T 技術文書 “Requirements for Network Address Translator and Firewall Traversal of H.323 Multimedia Systems（H.323 マルチメディアシステムのネットワークアドレス変換、ファイアウォール越えのための要求条件）”で定義され、SG16 において検討されたシナリオを対象に、各シナリオに関連する FW/NAT 越え問題を特定しようと試みるものである。

2. 参照

[1] TTC 標準 JT-H323 パケットに基づくマルチメディア通信システム
ITU-T Recommendation H.323 (2003), Packet-based multimedia communications systems.

[2] TTC 標準 JT-H225.0 パケットに基づくマルチメディア通信システム のためのシグナリングプロトコル とメディア信号のパケット化
ITU-T Recommendation H.225.0 (2003), Call signalling protocols and media stream packetization for packet-based multimedia communication systems.

[3] ITU-T Recommendation H.460.17 (2005), *Using H.225.0 call signalling connection as transport for H.323 RAS messages*.

[4] IETF RFC 3489(1999), *STUN - Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NATs)*

[5] ITU-T Technical Paper TP-H.323-Req.NATFW (2005-08) “Requirements for Network Address Translator and Firewall Traversal of H.323 Systems”

3. 略語

ALG	アプリケーションレベルゲートウェイ（Application Level Gateway）
EP	エンドポイント（Endpoint）
FW	ファイアウォール（Firewall）
GK	ゲートキーパー（Gatekeeper）
IP	インターネットプロトコル（Internet Protocol）
NAT	ネットワークアドレス変換（Network Address Translator）
PER	ASN.1 圧縮符号化規則(PER)（ASN.1 Packed Encoding Rules）
SCTP	ストリーム制御転送プロトコル（Stream Control Transmission Protocol）
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. 文書の骨子

H.323 に存在する FW/NAT 越え問題は、H.323 が TCP/IP プロトコルを使用する方法、及び、FW と NAT 装置の実装方法に起因する。

本文書は、既存の FW、NAT 装置、及び、NAT 及び／または FW を一緒に接続することで作られた装置のタイプについての記述から始める。

その次に本文書では、H.323 プロトコルを機能させるために要求される TCP/UDP/IP 動作の分析を続ける。いくつかの

H.323 動作モードについて分析する。

その後、本文書では、異なる FW/NAT トポロジーにおいて H.323 システムによって使用される特定の IP 動作に関連する問題について議論する。

最終セクションでは、“要求条件文書”に記載されたシナリオをリストにし、各シナリオを本文書に記載する FW/NAT トポロジーにマッピングする。

本文書は UDP と TCP の H.323 利用を分析するものであり、SCTP の利用は継続検討である。

5. NAT 装置のタイプ、NAT 装置のネスト

ネットワークアドレス変換（NAT）装置は、内部、及び、外部ネットワーク間を通過する IP パケットの送信元、または、送信先 IP アドレスを変更するネットワーク要素である。NAT 装置の主たる目的は、外部ネットワークのアドレススペースで内部ネットワークを表現するために必要な IP アドレス数を低下させることである。NAT 装置は、また、セキュリティの特定のレベルを達成するため、トポロジー隠蔽装置としても使用する。

RFC3489 によると NAT 装置は、以下のように分類することができる。

- フルコーン：フルコーン NAT は、同じ内部 IP アドレスとポートからの全ての要求を同じ外部 IP アドレスとポートにマッピングするものである。更に外部ホストは、マッピングされた外部アドレスにパケットを送信することで内部ホストにパケットを送信することができる。
- 制限コーン：制限コーン NAT は、同じ内部 IP アドレスとポートからの全ての要求を同じ外部 IP アドレスとポートにマッピングするものである。フルコーン NAT との違いとして、内部ホストから外部ホストに対して前回送信した場合のみ外部ホストは内部ホストにパケットを送信することができる。
- ポート制限コーン：ポート制限コーン NAT は、制限コーン NAT と似ているが、制限としてポート番号が含まれる。特に内部ホストが前回 IP アドレス X、ポート P にパケットを送信した場合のみ、外部ホストは、送信元 IP アドレス X、送信元ポート P を持つパケットを送信することができる。
- 対称：対称 NAT は、同じ内部 IP アドレス、ポートから特定の送信先 IP アドレス、ポートへの全ての要求を同じ外部 IP アドレス、ポートにマッピングするものである。同じホストが同じ送信元アドレス、ポートを持つが異なる送信先を持つパケットを送信する場合、異なるマッピングが使用される。更に、パケットを受信した外部ホストのみが内部ホストに対して UDP パケットを返送することができる。

ネットワークによっては幾つかの NAT 装置によって分割されていることもある。これらの NAT 装置が、ある装置の外部ネットワークが別の装置の内部ネットワークとなるような方法で接続され、全ての通信装置が最も内側の内部ネットワークの内側と最も外側の外部ネットワークの外側に位置している場合、NAT 装置の全てのチェーンは、前述したタイプの一つに属している単一の NAT 装置としてみることができる。

図 1 に 2 つのネストした NAT の振る舞いについて図示している。その結果、図からは一連の多数の NAT 装置は、一つの NAT 装置として振舞うことがわかる。

		内部			
		フルコーン	**制限コーン**	**ポート制限コーン**	**対称**
外部	**フルコーン**	フルコーン	制限コーン	ポート制限コーン	対称
	制限コーン	制限コーン	制限コーン	ポート制限コーン	対称
	ポート制限コーン	ポート制限コーン	ポート制限コーン	ポート制限コーン	対称
	対称	対称	対称	対称	対称

図 1: 2 つの NAT 装置のネストと合成された振る舞い

6. FW 装置と FW 装置のネスト

FW 装置の機能の一つは、パケットフィルタとしての働きである。FW は各々のパケットを検査し、その後、

- パケットを変更せずに他方に通過させる
- 完全にパケットを落とす。もしくは、
- ある方法でパケットそのものを処理する

FW は、典型的にはパケットの 5-タプル（プロトコル値、送信元・送信先 IP アドレス、送信元・送信先ポート番号）に関する決定に基づいている。

複数の FW に関連する事として、連続して接続された幾つかの FW は、一つの新たな装置を生成する。そして、（FW の全てのチェーンを通じて通信を行う装置の観点からすれば、）その装置は決定規則のセットを組み合わせた FW として振舞う。

6.1. アプリケーションレベルゲートウェイ (ALG)

幾つかの FW は、特定のプロトコルのロジックを実装し、その規則に従ってパケットをフィルタし、変換する。具体的には、H.323ALG は、H.323 パケットを解釈し、そして H.323 パケットから集められた情報に従って FW ルールを変更する。NAT 機能を実装し、H.323 ALG として動作する FW 装置は、H.323 パケット中の（PER 構造で埋め込まれた）アドレスを内部値から外部値に変更することができる。

H.323 ALG は、同じ FW/NAT 越え解決法が使用される場合における FW/NAT 越え問題の幾つかを解決するものの、別のタイプの FW 越え解決法に併せて使用される場合には、実際には付加的な問題を引き起こす場合がある。

7. H.323 マルチメディアシステムにおける IP 通信種別

この章で解析を行う目的のため、H.323 システムは 2 つの H.323 EP と 1 つあるいは 2 つの GK から構成されていると仮定する。もし 1 つの GK のみを利用しているならば、両方の EP を制御する。もし 2 つの GK が利用されているならば、各々の EP は自分自身の GK によって制御される。同様の仮定は、[5]によってなされている。

H.323 は、いくつかの異なった動作モードを利用することができる。例えば H.245 トンネル対個別チャネル伝送、H.225.0 の TCP 対 AnnexE（UDP）伝送、呼シグナリングの直接対 GK 経由型伝送など。異なった動作モードは、異なった FW/NAT 越え問題を引き起こす。

この節では、H.323 システムが利用するさまざまな種類の通信（IP 動作）を一覧にしている。3 つの異なった場合を示す。

- 最大の場合：すべての H.323 の動作モードがサポートされている。
- 最小の場合：FW/NAT にもっとも相性のよいモードのみがサポートされている。（すなわち、H.460.17 の持続性のある TCP や H.245 トンネル含んだ GK 経由型呼シグナリング）
- 典型的な場合：現在最も広く利用されているモードである RAS over UDP と H.245 が分離されている GK 経由の H.225.0 over TCP。

7.1. 最大の場合

H.323 標準は、H.323 エンティティ間に以下の種別の通信を必要とする。

- EP と EP 自身の GK 間
- EP と相手の GK 間
- GK と GK 間
- EP と EP 間

ネットワーク内の FW/NAT に対する、GK と EP の相対的配置に依存し、1 つ以上の種別の通信が問題となる可能性がある。

注：ITU-T Technical Paper には記述がないが、UDP データグラム送信あるいは TCP 接続確立に関わる H.323 メッセージの例を（）内に記す。図番は H.323 v6 (2006 年 6 月承認)を参照。

7.1.1 EP と自身の GK 間の通信

以下の基本的な TCP/IP 動作は、通常 H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。（以下のリストの well-known の意味は IANA で定義され、FW 機器では既知であり、known a-priori は何らかの外部手段で利用しようとしている機器に知られているという意味であるが、FW 機器では必ずしも知られているとは限らない。）

- EP から GK の well-known アドレスにマルチキャスト UDP データグラムを送信する（Figure 23/H.323 の GRQ）。
- EP から GK の known a-priori アドレスにユニキャスト UDP データグラムを送信する（Figure 24/H.323 の RRQ）。
- EP から GK によって設定された GK のアドレスにユニキャスト UDP データグラムを送信する（Figure 36/H.323 の ARQ(1)、アドレスは Figure 23/H.323 の GCF で付与済み）。
- GK から EP によって設定された EP のアドレスにユニキャスト UDP データグラムを送信する（Figure 36/H.323 の ACF/ARJ(2)）。
- EP から GK で設定された GK のアドレスに TCP 接続を確立する（Figure 38/H.323 の Setup(3)を送るための TCP 接続確立）。
- GK から EP で設定された EP のアドレスに TCP 接続を確立する（Figure 37/H.323 の Setup(14)を送るための TCP 接続確立、アドレスは EP2 が GK2 に登録時 RRQ で付与済み）。

7.1.2 EP と相手側の GK との通信

以下の基本的な TCP/IP 動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- EP から自らの GK によって設定された相手先 GK のアドレスに TCP 接続を確立する（Figure 37/H.323 の Setup(13)を送るための TCP 接続確立、アドレスは Figure 37 の Facility(7)で付与済み）。
- 相手先 GK から EP によって設定された自らののアドレスに TCP 接続を確立する（Figure 38/H.323 の Setup(4)を送るための TCP 接続確立、アドレスは Figure 38 の ACF(2)で付与済み）。

7.1.3 GK 間の通信

以下の基本的な TCP/IP 動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- Well-known アドレスへのマルチキャスト UDP データグラムを送信する（Figure 40/H.323 の LRQ(2)）。
- Known a-priori アドレスにユニキャスト UDP データグラムを送信する（Figure 40/H.323 の LCF(3)）。
- GK が受け入れた接続によって設定されたアドレスに TCP 接続を確立する（Figure 39/H.323 の Setup(10)を送るための TCP 接続確立）。

7.1.4 EP 間の通信

以下の基本的な TCP/IP 動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- 受信している EP が設定したアドレスにユニキャスト UDP データグラムを送信する（Figures 36-40/H.323 には表されていない音声、映像、データ情報）。
- 接続を受け付けた EP によって設定されたアドレスに TCP 接続を確立する（Figure 36/H.323 の Setup(3)を送るための TCP 接続確立）。

7.2. 最小の場合

前の章では、すべての可能な H.323 動作モードを実装するのに必要な通信種別を定義している。すべてのエンティティが、FW/NAT で最も親和性の高い H.323 モード（以前定義した）をサポートしている環境内では、より小さいセットの IP 動作で十分である。この節ではそのような最小限のセットを定義する。H.323 標準は、H.323 のエンティティ間で少なくとも以下のような通信種別を必要とする。

- EP と自身の GK 間
- GK と GK 間
- EP と EP 間

7.2.1 EP と自身の GK 間の通信

以下の基本的な TCP/IP の動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- EP から GK で設定されたアドレスの GK に対して TCP 接続を確立する。

7.2.2 GK 間の通信

以下の基本的な TCP/IP の動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- GK が接続受付を行なったアドレスに TCP 接続を確立する。

7.2.3 EP 間の通信

以下の基本的な TCP/IP の動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- 受信 EP によって設定されたアドレスに対しユニキャスト UDP データグラムを送信する。

7.3. 典型的な場合

最も広く採用されている H.323 ネットワークは、エンティティ間における以下の種別の通信を利用している。

- EP と自身の GK 間
- GK と GK 間
- EP と EP 間

7.3.1 EP と自身の GK 間の通信

以下の基本的な TCP/IP の動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- EP から known a-priori アドレスの GK へユニキャスト UDP データグラムを送信する。
- EP から GK へ、GK によって設定されたアドレス宛にユニキャスト UDP データグラムを送信する。
- GK から EP へ、EP によって設定されたアドレス宛にユニキャスト UDP データグラムを送信する。
- EP から GK へ、GK によって設定されたアドレス宛に TCP 接続を確立する。
- GK から EP へ、EP によって設定されたアドレス宛に TCP 接続を確立する。

7.3.2 GK 間の通信

以下の基本的な TCP/IP の動作は H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- GK が接続受付を行った GK が設定するアドレスに対して TCP 接続を確立する。

7.3.3 EP 間の通信

以下の基本的な TCP/IP の動作は、H.323 エンティティによって行われ、FW/NAT 越え問題のテーマになると思われる。

- 受信側 EP によって設定されたアドレスに対してユニキャスト UDP データグラムを送信する。
- 接続受付を行う EP によって設定されたアドレスに対して TCP 接続を確立する。

8. H.323 システムにおける FW/NAT 装置によって引き起こされる問題

8.1. 一般的な問題

8.1.1 トポロジの発見

本文書において記述されるように、2 つの通信エンティティ間でいくつかの可能な FW/NAT トポロジが存在する。異なったトポロジは違った問題を生じ、結果としてトポロジ発見機構を必要とするかもしれない。FW/NAT 越え問題の解決には、通信エンティティ間の FW/NAT トポロジ発見のための手段を提供すべきである。
そのような発見の結果は、次のような情報を含むべきである。

- 通信パスにおける NAT 装置の存在とそれらの種別
- 通信パスにおける FW 装置の存在
- 通信パスにおける H.323 ALG の存在

8.1.2 動的ポート割り当て

ファイアウォールの主要な役割は、正当なトラフィックのみを許容することによってネットワークのトラフィックを制限することである。H.323 プロトコルは、その機能のいくつかにおいて動的ポート割り当てを使用し、H.323 装置は 65536 個のうちの任意の UDP ポートと TCP ポートを使用しても良い。これが、H.323 非認識 FW 装置による H.323 パケットだけをフィルタリングするという規則の定義を不可能にしている。FW/NAT 越えソリューションは、H.323 非認識 FW による他のプロトコルパケットをフィルタリングすることに影響を及ぼすことなく、H.323 トラフィックを可能・不可能にする FW の構成を許容すべきである。

8.1.3 仲介装置の使用に関する問題

FW/NAT 越えを解決するには一般的に、H.323 仲介装置の使用が含まれる。ある特定の問題を解決するとは言え、そのようなソリューションでは他の問題がしばしば引き起こされる。本節はこれらの問題を議論する。

8.1.3.1 H.323 ALG 関連問題

H.323 ALG は、H.323 標準によって定義されていないエンティティである。これは、ある状況におけるその振る舞いが

分からない、もしくは予測できないものであることを意味する。
例えば、ファイアウォールに設置された H.323 ALG の後ろに位置する H.323 エンティティがその（H.323 エンティティの）外部アドレスを（例えば STUN プロトコルを使用して）発見し、H.323 メッセージ中にそのアドレスを使用すると仮定しよう。そのようなメッセージを受信する ALG は普通、内部アドレスを外部アドレスに変換する。外部アドレスを受信する時、ALG の振る舞いがどうあるべきということが定義されていない。

8.1.3.2 セキュリティに関連する問題

仲介装置は、H.323 メッセージ中にあるトランスポートアドレスの変更を必要とするかもしれない。これは、通信中の H.323 エンティティが H.235 完全性保護機構を使用していれば、問題を引き起こす場合がある。この場合、すべての仲介装置は、アドレスが変更された後にメッセージをデジタル署名できなければならない（言い換えると、全ての仲介装置が信頼されるエンティティでなければならないことを意味する）。

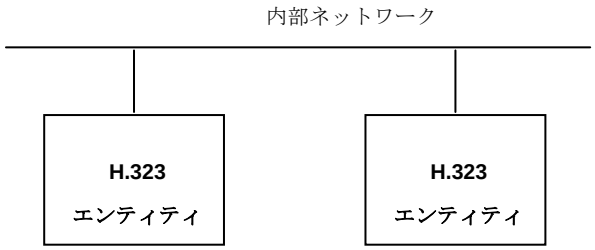
8.1.3.3 QoS に関連する問題

メディア通信パス上の全ての仲介エンティティは、メディアの遅延やジッタの付加を引き起こし、パケットロスの確率を増大する。仲介装置の選択がまずければ、メディアパケットが隣の部屋に戻るために地球を一周する状況を引き起こしうるということである。

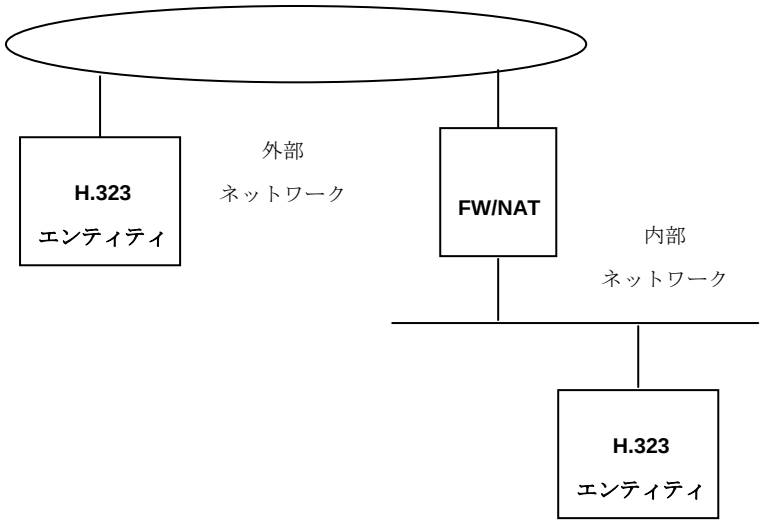
8.2. FW/NAT トポロジに特化した問題

次の 3 つの FW/NAT トポロジが通信中の 2 つの H.323 エンティティ間に起こりそうである。

- 直接接続：2 つの H.323 エンティティ間に FW/NAT 装置は存在しない。
  訳注： 下記の図は、訳者が追加したもので、原文には含まれない。

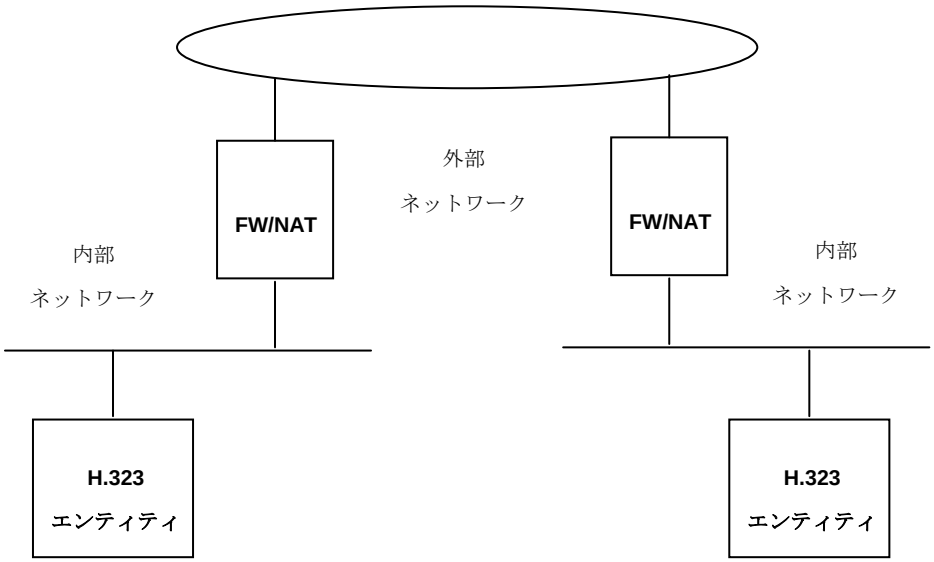


- FW/NAT 装置：（1 つ前の外部ネットワークが次の内部ネットワークに接続する）同じ方向の 1 つ以上の FW/NAT 装置が、2 つの H.323 エンティティ間のパス上に存在する。
  訳注： 下記の図は、訳者が追加したもので、原文には含まれない。



- ヘッドツーヘッド FW/NAT（head to head FW/NAT）：2 つの H.323 エンティティそれぞれが 1 つ以上の FW/NAT 装置の後ろに位置する。これら FW/NAT 装置は同じ外部ネットワークに接続されている。

  訳注： 下記の図は、訳者が追加したもので、原文には含まれない。



直接接続は文字通り（直接接続を発見することの問題を除いて）どの FW/NAT 越え問題も引き起こさない。

次節は、FW/NAT 装置を含む他のトポロジー2 つに関連する問題を描いている。それぞれのトポロジーは、そのようなトポロジーの中で固有の IP 操作を行うことの問題の記述を含む。ここでは、（上述の）「典型的な H.323 事例」に必要となる IP 操作のみを議論する。

8.2.1 2 つの H.323 通信エンティティ間の FW/NAT 装置

8.2.1.1 既知の外部アドレスへのユニキャスト UDP データグラムの送信

この操作は、NAT 変換に関連するどんな既知の問題をも引き起こさない。

FW 越えに対しては、その操作は指定された宛先アドレスとの通信が許可されていることを必要とする。そのようなアドレスが既知であるという考慮を取り入れると、これは特別な問題を何も引き起こさないはずである。

8.2.1.2 外部の相手先によって与えられたアドレスへのユニキャスト UDP データグラムの送信

この操作は、NAT 変換に関連するどの問題も引き起こさない。

FW 越えに対しては、その操作は指定された宛先アドレスとの通信が許可されていることを必要とする。そのようなアドレスが動的に相手先によって割り当てられ、アドレスが取得できる値を制限する規則を定義する標準がない点を考慮すると、この種の通信は FW 越え問題を引き起こす。

8.2.1.3 外部エンティティによって与えられた動的アドレスに確立した TCP 接続

外部エンティティへの TCP 接続の確立は、分かっている NAT 装置問題を引き起こさない。そのような接続を維持するには、NAT 装置に定義されるバインディングの期限切れ時間よりは頻繁にその接続上で何らかのネットワーク活動を必要とする。TCP キープアライブ機構の使用はこの問題を解決するものの、H.323 においてはこの機構の使用を指定したり推奨したりしてはいない。

FW 越えに対しては、この操作は、上記の動的アドレスを含むどの操作とも同じ種の問題を引き起こす。

8.2.1.4　既知の内部アドレスへのユニキャスト UDP データグラムの送信

フルコーン NAT 装置と静的アドレス対応付けを許容する NAT 装置のみは、この種の操作を可能にする。その他の NAT 装置は、この操作先立ち、反対の方向に UDP データグラムを送信しなければならない。

FW 越えに対しては、その操作は指定された内部宛先アドレスとの通信が許可されていることを必要とする。そのようなアドレスが既知であるという考慮を取り入れると、これは更なる問題をも引き起こさないはずである。

8.2.1.5　相手先によって与えられた内部アドレスへのユニキャスト UDP データグラムの送信

NAT 装置は、この操作の前に、（使用された NAT 装置の種別に依存した）UDP データグラムを内部アドレスから外部アドレスへ送信することを必要とする。H.323 におけるこの種の操作を使用する多くの場合において（例えば、RAS メッセージや RTP/RTCP メッセージなど）、そのような先行メッセージを特定することができる。不幸にも、H.323 は到着メッセージの UDP/IP レベルのアドレスの使用を禁止し、その代わりとして対応する H.323 レベルフィールドの使用を必須としている。H.323 はまた、この問題をさらに複雑にする点として、RAS と RTP/RTCP パケットを送受信するために異なったアドレスの使用を許可している。

内部アドレスに長時間 UDP データグラムを送出するには、内部アドレスから UDP データグラムを定期的に外部アドレスに送信しなければならない。

FW 越えに対しては、この操作は上記の動的アドレスを含むどの操作とも同じ種の問題を引き起こす。

8.2.1.6　内部エンティティによって与えられた動的アドレスへの TCP 接続の確立

この操作は普通、NAT 装置によって無効化される。

FW 越えに対しては、この操作は上記の動的アドレスを含むどの操作とも同じ種の問題を引き起こす。

8.2.2　2 つの H.323 通信エンティティ間におけるヘッドツーヘッド FW/NAT 装置

8.2.2.1　既知のアドレスへのユニキャスト UDP データグラム送信

この操作は、初めの NAT 装置における外部ネットワークへと、次に 2 番目の NAT 装置における内部ネットワークへの、UDP データグラムの送信を含む。これまで記述されているように、そのような操作は、もし 2 番目の NAT 装置がフルコーン NAT 装置であるか、あるいは静的なアドレス対応付けを許していれば、可能となる。

双方の FW 越えは、コンフィギュレーションの問題であり、また、アドレスが既知であることを考慮に入れる問題である。故に、この構成は新たな問題を引き起こすはずはない。

8.2.2.2　相手先によって与えられたアドレスへのユニキャスト UDP データグラム送信

この操作は、最初の NAT 装置における外部ネットワークへと、次に 2 番目の NAT 装置における内部ネットワークへの、UDP データグラムの送出を含む。動的内部アドレスへ UDP データグラムを送出することは、8.2.1.5 節で議論したような問題を引き起こす。

2 番目の NAT 装置（外部ネットワークから内部ネットワークへの方向に通過する NAT 装置）がフルコーン NAT 装置ではない場合、ヘッドツーヘッド NAT を通して直接の UDP 通信は不可能である。この場合における UDP 通信の唯一知られた方法は外部ネットワークに位置した仲介エンティティの使用である。

FW 越えに対しては、この操作は、上記の動的アドレスを含む他の操作とも同じ種の問題を引き起こす。

8.2.2.3　エンティティ間の TCP 接続の確立

この操作は普通、外部ネットワークから内部ネットワークへの方向において、NAT 装置によって無効化される。

FW 越えに対しては、その操作は上記の動的アドレスを含む他の操作とも同じ種の問題を引き起こす。

9. H.323 マルチメディアシステムにおけるシナリオ

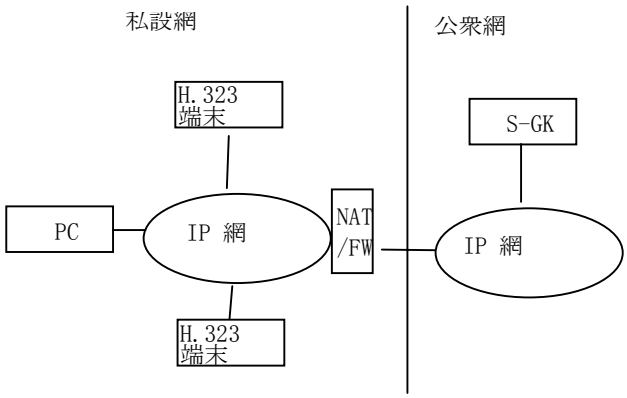
次節は[5]で提供されているシナリオのリストをベースにしている。それぞれのシナリオに対し特定の H.323 エンティティペア間での通信で 8.2 節のどの FW/NAT 越えトポロジーが使用されるかを述べる。

9.1. サービスプロバイダ型ネットワーク構成でのシナリオ

9.1.1 シナリオ 1 – エンドポイントはプライベートアドレスを持った同一のドメイン内にある

EP から GK は FW/NAT 経由 （EP - 内部、 GK - 外部）

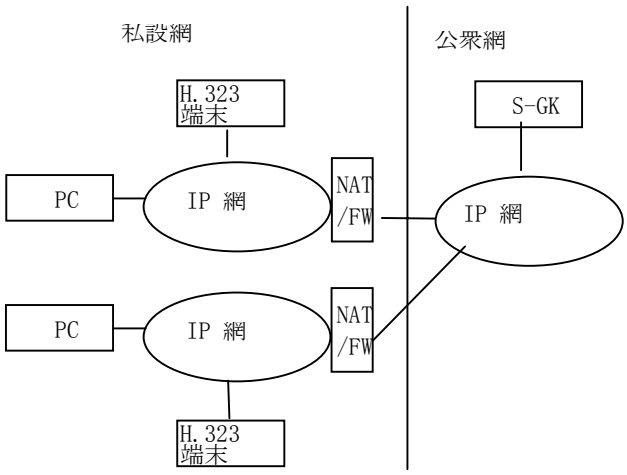
EP から EP は 直接接続



9.1.2 シナリオ 2 – エンドポイントはプライベートアドレスを持った異なるドメイン内にある

EP から GK は FW/NAT 経由 （EP は内部、 GK は外部）

EP から EP は２つのヘッドツーヘッド FW/NAT 経由

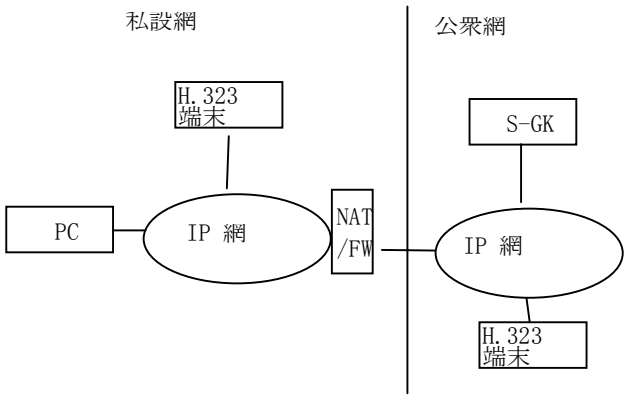


9.1.3 シナリオ 3 – 一方のエンドポイントはパブリックアドレスアドレスを持ち、もう一方のエンドポイントはプライベートアドレスを持つ

EP1 から GK は FW/NAT 経由（EP は内部、GK は外部）

EP2 から GK は直接接続

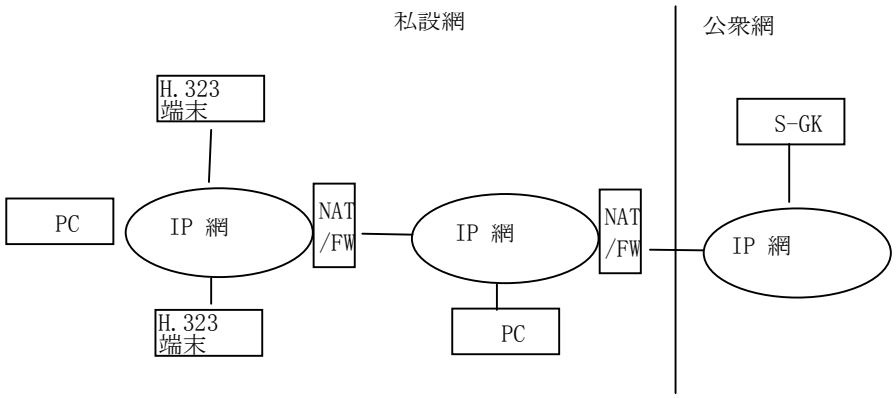
EP から EP は FW/NAT 経由



9.1.4 シナリオ 4 - 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ある場合

EP から GK は FW/NAT 経由 （EP は内部、GK はパブリック）

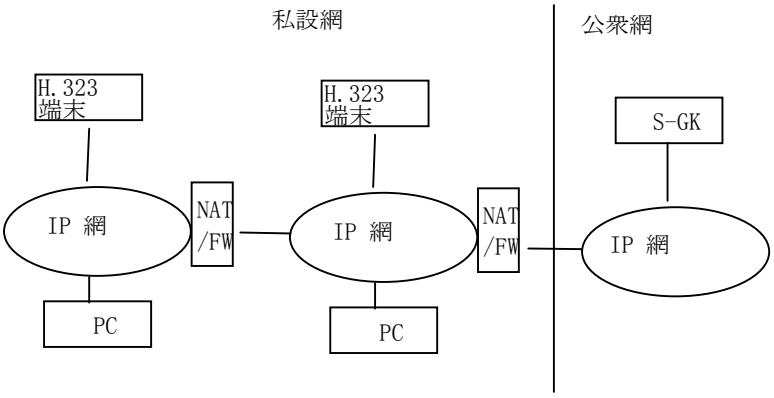
EP から EP は直接接続



9.1.5 シナリオ 5 - エンドポイントはプライベートアドレスを持ち、異なった複数レベルのレルムにある場合

EP から GK は FW/NAT 経由（EP は内部、GK は外部）

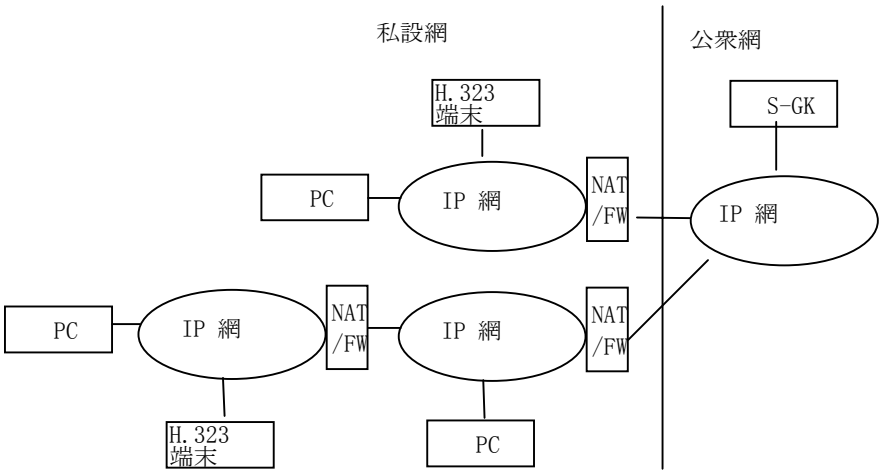
EP から EP は FW/NAT 経由



9.1.6　　シナリオ 6 – 一方の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レルムにあり、もう一方の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ある。

EP から GK は FW/NAT 経由（EP は内部、GK は外部）

EP から EP は 2 つの FW/NAT ヘッドツーヘッド

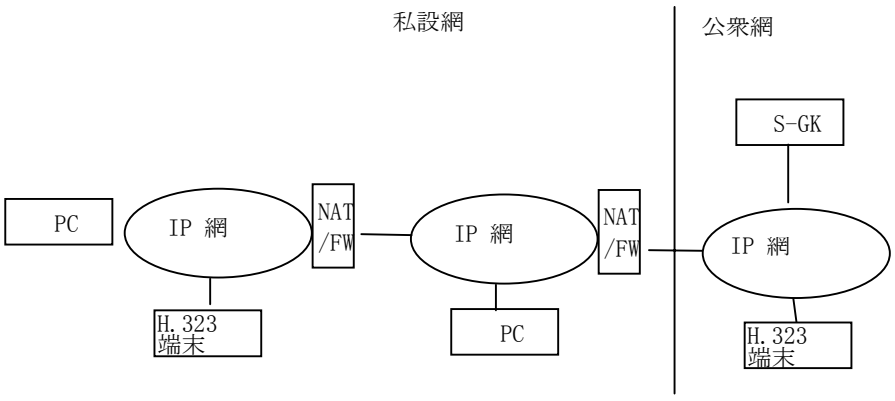


9.1.7　　シナリオ 7 - 一方のエンドポイントはプライベートアドレスを持つ複数レベルレルムにあり、もう一方のエンドポイントはパブリックアドレスを持つレルムにある。

EP1 から GK は FW/NAT 経由（EP は内部、GK は外部）

EP2 から GK は直接接続

EP から EP は FW/NAT 経由

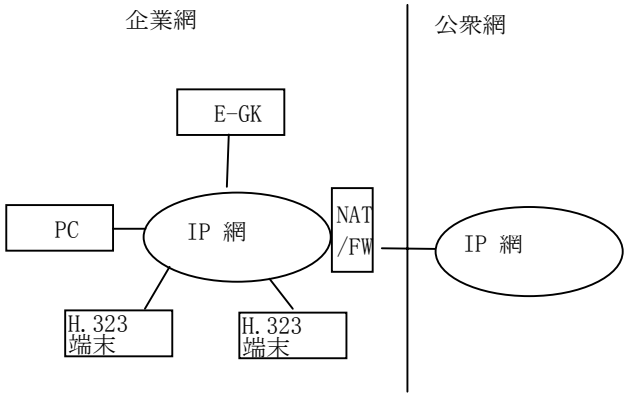


9.2.　企業ネットワーク構成のシナリオ

9.2.1　　シナリオ 1 - エンドポイントと GK はプライベートアドレスを持つレルムにある

EP から GK は直接接続

EP から EP は直接接続

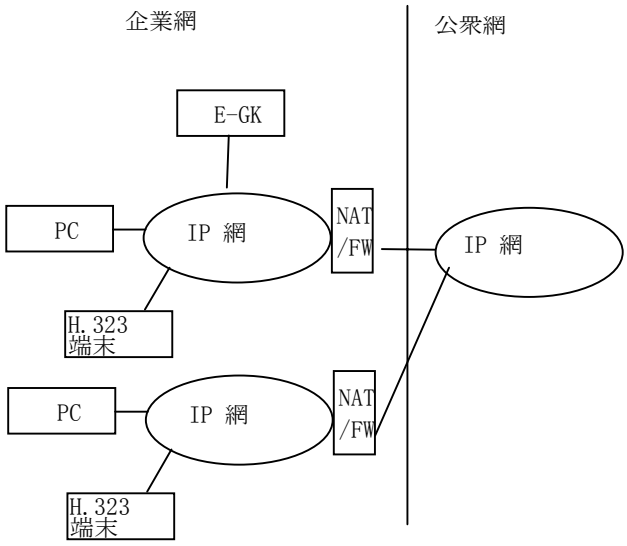


9.2.2　シナリオ 2 - 一方のエンドポイントと GK はプライベートアドレスを持つ同じレルムにあり、もう一方のエンドポイントはプライベートアドレスを持つ別のレルムにある

EP1 から GK はヘッドツーヘッド FW/NAT 経由

EP2 から GK は直接接続

EP から EP はヘッドツーヘッド FW/NAT 経由

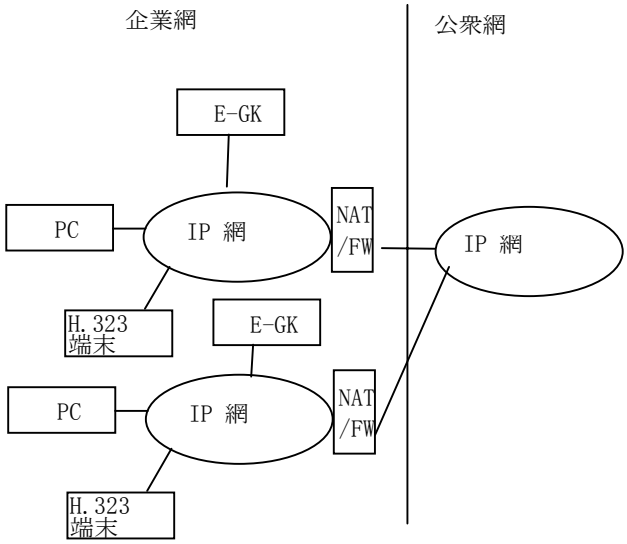


9.2.3　シナリオ 3 -一方のエンドポイントとその GK はプライベートアドレスを持つ同じレルムにあり、もう一方のエンドポイントとその GK はプライベートアドレスを持つ別のレルムにある。

EP から GK は直接接続

GK から GK はヘッドツーヘッド FW/NAT 経由

EP から EP はヘッドツーヘッド FW/NAT 経由



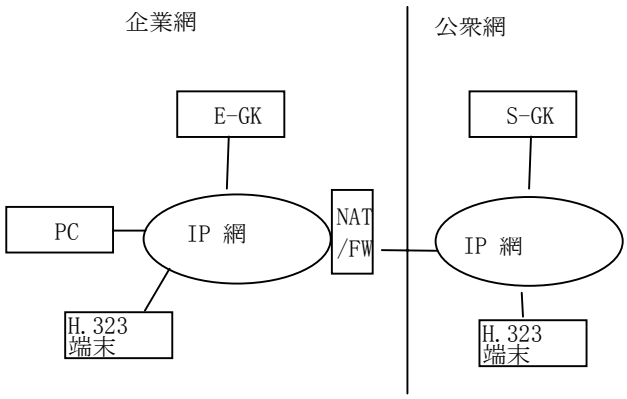
9.2.4　シナリオ 4 -一方のエンドポイントとその GK はプライベートアドレスを持つ同じレルムにあり、もう一方のエンドポイントとその GK はパブリックアドレスを持つレルムにある

EP1 から GK1 は直接接続

EP2 から GK2 は直接接続

GK から GK は FW/NAT 経由

EP から EP は FW/NAT 経由



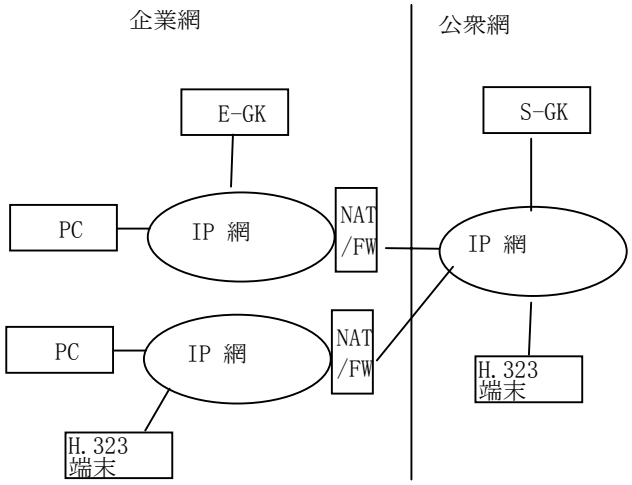
9.2.5　シナリオ 5 - 一方のエンドポイントとその GK はプライベートアドレスの異なったレルムにあり、もう一方のエンドポイントとその GK はグローバルでユニークな登録アドレスを持つレルムにある

EP1 から GK1 はヘッドツーヘッド FW/NAT 経由

EP2 から GK2 は 直接接続

GK から GK は FW/NAT 経由

EP から EP は FW/NAT 経由



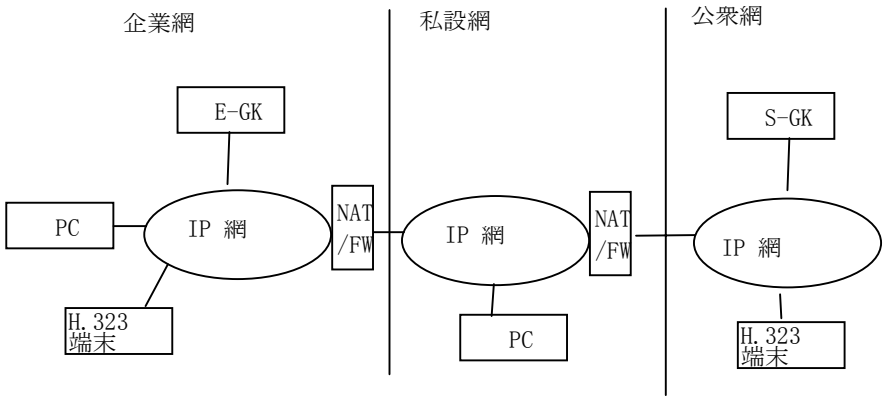
9.2.6　**シナリオ 6 -一方のエンドポイントとその GK はプライベートアドレスを持つ複数レベルレルムにあり、もう一方のエンドポイントとその GK はグローバルでユニークな登録アドレスを持つレルムにある。**

EP1 から GK1 は直接接続

EP2 から GK2 は直接接続

GK から GK は FW/NAT 経由

EP から EP は FW/NAT 経由



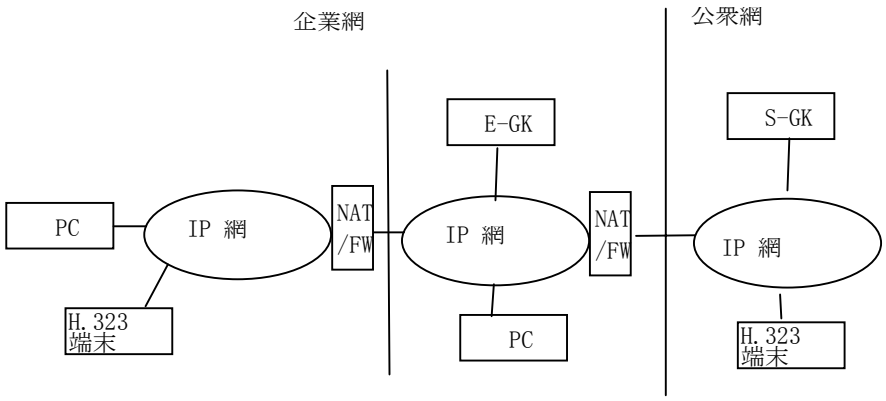
9.2.7　**シナリオ 7 -一方のエンドポイントとその GK はプライベートアドレスを持つ異なる複数レベルレルムにあり、もう一方のエンドポイントとその GK はグローバルでユニークな登録アドレスを持つレルムにある。**

EP1 から GK は FW/NAT 経由 （EP は内部、GK は外部）

EP2 から GK2 は直接接続

GK から GK は FW/NAT 経由

EP から EP は FW/NAT 経由

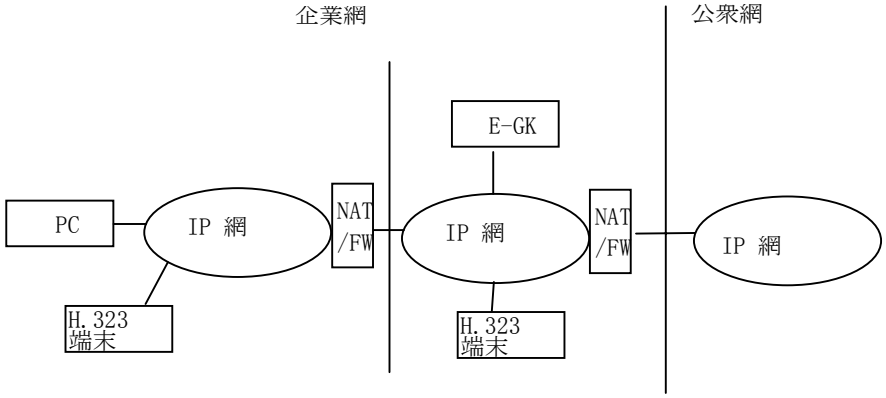


9.2.8　**シナリオ 8 –一方のエンドポイントと GK がプライベートアドレスを持つレルムにあり、もう一方のエンドポイントは異なる複数レベルのレルムにある。**

EP1 から GK は FW/NAT 経由（EP は内部、GK は外部）

EP2 から GK は直接接続

EP から EP は FW/NAT 経由



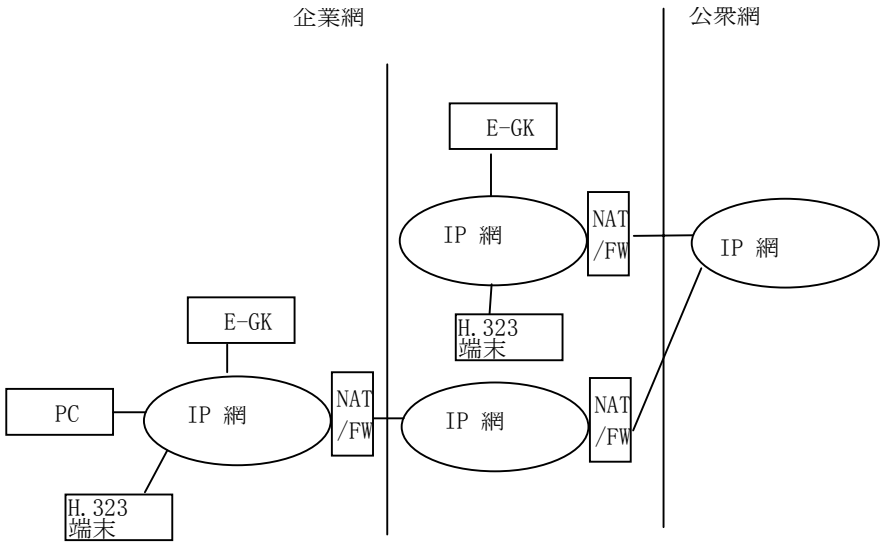
9.2.9　**シナリオ 9 –一方のエンドポイントとその GK はプライベートアドレスを持つレルムにあり、もう一方のエンドポイントとその GK は異なる複数レベルのレルムにある。**

EP1 から GK1 は直接接続

EP2 から GK2 は直接接続

GK から GK はヘッドツーヘッド FW/NAT 経由

EP から EP はヘッドツーヘッド FW/NAT 経由

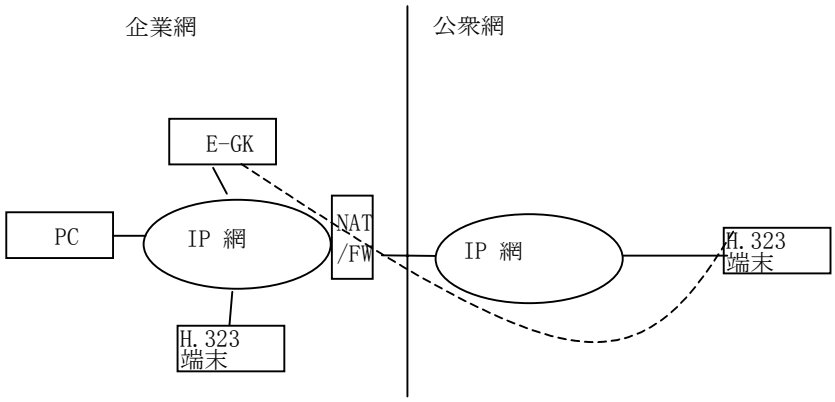


9.2.10　**シナリオ 10-一方のエンドポイントとその GK はプライベートアドレスを持つレルムにあり、もう一方のエンドポイントは企業ネットワークレルムの外に移動している。**

EP1 から GK は直接接続

EP2 から GK は FW/NAT 経由　（GK は内部、EP は外部）

EP から EP は FW/NAT 経由



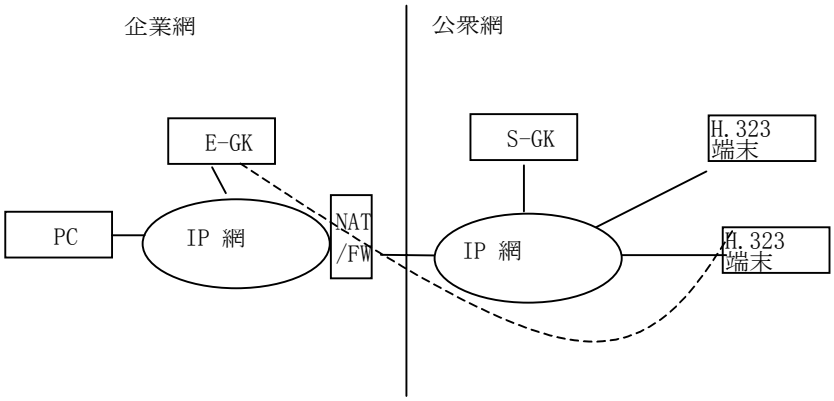
9.2.11　**シナリオ 11 –一方のエンドポイントは企業ネットワークの外のレルムに移動していて、その GK はプライベートアドレスを持つレルムにあり、もう一方のエンドポイントとその GK はグローバルでユニークな登録アドレスを持つレルムにある。**

EP1 から GK1 は直接接続

EP2 から GK2 は FW/NAT 経由　（GK は内部、EP は外部）

GK から GK は FW/NAT 経由

EP から EP は直接接続


企業網
公衆網
E-GK
S-GK
H.323
端末
PC
IP 網
NAT
/FW
IP 網
H.323
端末