ファイアウォールを通過できる IP 電話

伊藤　将志　　渡邊　晃
名城大学理工学部

1.　はじめに

近年ブロードバンドの普及により，ネットワーク伝送容量が大幅に増加し，IP 電話の実用レベルの品質保証が可能になった．更に，2002 年秋から“050-”の事業者受付が開始され，従来の電話からの受信を可能にした．それ以降多くの ISP が低額固定料金である IP 電話サービスを提供するようになり，IP 電話の普及は著しく進んでいる．

しかし，この普及に伴い VoIP の様々な課題が浮かび上がってきた．問題になるのは，ファイアウォール，NAT，プロキシなどの存在により通信が制限されることである．既存の VoIP ではこれらによって生じる問題に完全に対応できず，ファイアウォールを設置している企業では外部との通話ができない．

本稿では，既存の VoIP 技術である SIP を利用し，プライベートネットワークの内部と外部に配置した２台のリレーエージェント同士の通信を HTTP でトンネルすることにより，課題を解決するシステムを提案し，その詳細について説明する．

2.　既存技術とその課題

2.1.　SIP の課題

SIP では，図１のように左側の SIP プロキシが端末からダイアルのメッセージを受け取ると，通信先の SIP プロキシの IP アドレスを DNS で取得するという手順をとる．しかし，相手のドメインに NAT が存在する場合

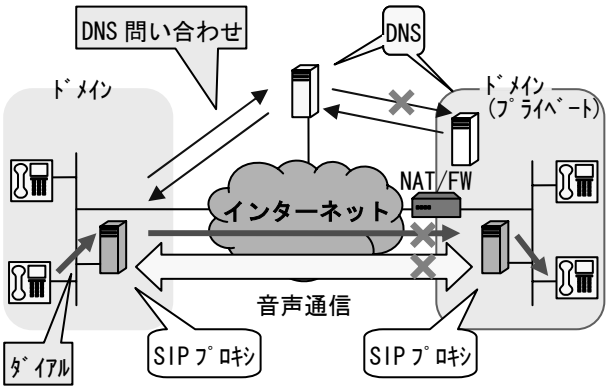

図１．SIP による NAT/FW の問題

“Proposal of voice over IP system passing through Firewall”
Masashi Ito & Akira Watanabe
Faculty of Science and Technology, Meijo University

には，通話相手の IP アドレスが外部から特定不可能なため，外部からのダイアルができない．また，特定のポート番号や IP アドレスのパケットをフィルタリングするファイアウォールが存在する場合もある．企業などのファイアウォールは多くの場合 HTTP で使用する 80 番ポートなどの必要以外のポート番号を通過させないため，SIP による IP 電話を実装する場合，ファイアウォールの設定を変更しなければならない．これはセキュリティ低下に繋がるなどの障害があり， SIP による通信を困難なものにしている．

2.2.　既存の解決システム

このような制限の多いネットワーク環境において外部と通話するための技術は既にいくつか存在している．

HCAP では HTTP のダウンロード機能を利用して NAT を通過し，80 番ポートによりファイアウォールを通過することが可能である[1]．しかし，音声端末それぞれに HCAP という専用プロトコルを導入する必要があり，またファイアウォールの非武装地帯（DMZ）上に特殊なサーバを設置しなければならず，そこへ組織内の複数の端末が常時接続するためファイアウォールに不要な負荷がかかる．

また Skype は 80 番ポートを利用した独自アプリケーションによりファイアウォールを通過する．ユーザエージェントからグローバル環境上のサーバに TCP 接続をしておき，端末間のダイアルや音声をサーバが中継するという方式であり，NAT を通過することもできる．しかし，80 番ポートを独自アプリケーションで使用しているため，HTTP プロキシを通過することができず，セキュリティ的にも信頼性が低い．

3.　提案システム

3.1.　提案システムの原理

本提案システムでは図２のようにプライベートネットワークの内側と外側に中継機能を持った HRA（ハーフリレーエージェント）と呼ぶ装置を設置する．この２つの装置はダイアルの際，あわせて１つの仮装的な SIP プロキシとしての機能を持つと共に音声を中継する機能を持つ．

２台の HRA はダイアルのメッセージや音声ストリームを HTTP に埋め込み、ダウンロードやアップロードに

よりデータのやり取りをすることによって，ファイアウォールや NAT を通過する．プライベートネットワークの内側に設置する HRA は DMZ などのセグメントに置く必要はなく電話端末と同じ位置に設置するだけでよい．HRA のうちプライベートネットワーク内部に設置するものを HRA クライアント，インターネットに設置する HRA を HRA サーバと呼ぶ．

本提案システムでは，前述のような既存技術の課題に対し，既存のファイアウォールシステムに影響を与えない上，音声端末も標準の IP 電話対応のものを使用することができる．ファイアウォール上を流れるのは外部と内部の HRA 同士の 1 対 1 の通信のみのため，ファイアウォール上に無駄なトラヒックが発生しない．

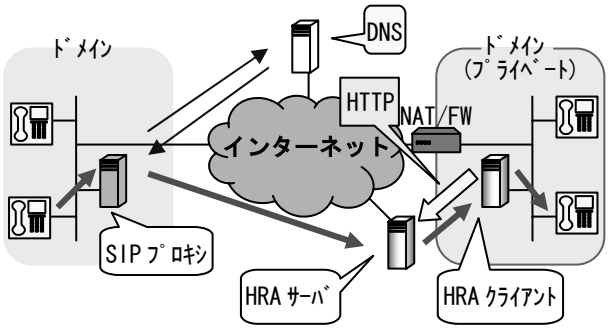

図２．HRA による解決法

3.2. 動作概要

本提案システムの基本動作は図３のように，まず内部の HRA クライアントが外部の HRA サーバに対して，あらかじめ GET メソッドを発行しておく．その後，HRA サーバから定期的に HRA クライアントに向けて通信を行い，HRA 間の接続を維持する．このようにして HRA クライアントはプライベートな IP アドレスを持ちながらも，外部からの着呼を受けることのできる状態になる．音声ストリームも同様に GET メソッドにより，ダウンロードされる．また，内部の端末からのダイアル情報を持つメッセージや音声ストリームは POST メソッドにより，HRA サーバへアップロードされ，HRA サーバにより外部に送信される．

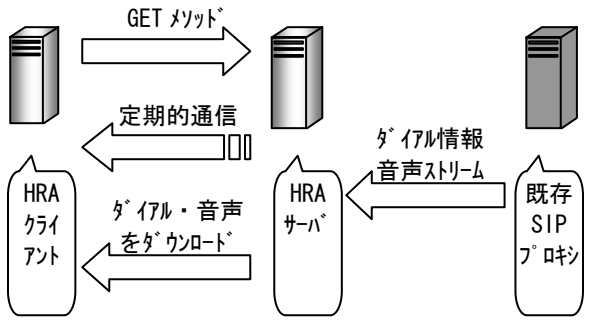

図３．HTTP によるダイアル・音声の中継

4. 評価

本提案システムの利点を確認するために，複数の既存 IP 電話システムを調査した．ダイアルとシステムの導入の簡易さ，システムを構成する機器によるディレイについて考察し，それぞれの項目で比較を行った結果を表１に示す．

表１．IP 電話システムの比較

	FW 通過	NAT 通過	ﾌﾟﾛｷｼ 通過	SIP との互換	公衆網との互換	ﾃﾞｨﾚｲ	導入
Linphone	×	×	×	◎	◎	◎	◎
HCAP	◎	◎	◎	×	×	△	○
Skype	◎	◎	×	×	×	△	○
提案システム	◎	◎	◎	○	○	△	◎

既存の SIP 技術を利用した IP 電話としてフリーソフトである Linphone をあげた．Linphone ではファイアウォールや NAT などは通過できないが，音声ストリームには UDP を利用するので，ディレイは少ない．

また，HCAP や Skype では独自のダイアル方法を利用しているため，SIP との互換性はない．

提案システムのダイアル方式では，ファイアウォール，NAT，プロキシを通過できる上， SIP との互換性は高い．また通常の IP 電話端末が使用でき，内部ネットワークに HRA を設置するだけでよいので，導入が容易である．しかし，HTTP を用いてリレーエージェントを通過するために，ディレイに関しては UDP を利用した既存の VoIP よりは劣化すると考えられる．

5. おわりに

本稿では，ファイアウォールを通過することのできる新しいシステムを提案し，その詳細について説明した．また，既存の VoIP と提案システムを比較し，提案システムの利点について考察した．

今後は提案システムの実装を行い，性能の測定結果を既存技術と具体的に比較をする．また，通信する相手が同じように NAT・ファイアウォールの存在する環境であった場合の通信方法についても検討を行っていく．

参考文献

[1]宮内信二“多様な環境で利用できるインターネットプロトコル”情報処理学会論文誌 Vol.44 No.3
[2]登大遊“SoftEther による Ethernet の仮想トンネリング通信”
[3]千村保文，村田利文“SIP 教科書”IDG ジャパン
[4] J. Rosenberg,et all”SIP: Session Initiation Protocol”IETF RFC3261(2002.6)