企業ネットワークにおける IPv6 アドレスの隠蔽方式

久保敷　透*，寺澤　圭史，鈴木　秀和，渡邊　晃(名城大学)

Researches on a Conceal Method of IPv6 Addresses in Enterprise Networks

Toru Kuboshiki, Keiji Terazawa, Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．はじめに

インターネットの普及に伴い IPv4 アドレスが枯渇し，IPv6 アドレスへの移行が必須と言われている．IPv6 では，すべての端末に対してグローバルなアドレスが割り当てられるため，企業ネットワーク内のアドレスが外部に見えてしまうという課題がある．この問題を解決するため，IPv6 アドレスを隠蔽し，企業ネットワークの構造を予測出来なくするための方式を提案する．

２．サイトローカルアドレスと匿名アドレス

IPv6 では，IPv4 プライベートアドレスに対応するアドレスとしてサイトローカルアドレスが定義されていた．しかし，サイトローカルアドレスはエンドエンドの通信を阻害するとして廃止が決まっており，使用は推奨されていない[1]．そこで内部端末を匿名化する技術として，匿名アドレス[2]が定義されているが，インタフェース ID だけを匿名化するため，企業ネットワークの構造までは隠蔽することができないという課題がある．

３．　提案方式

上記の問題を解決するための方式として 2 通りのアプローチを提案する．

(1)　ゲートウェイ方式

内部ネットワークの境界にあるゲートウェイ（以下 GW）において，内部ネットワークに置かれている端末のアドレスを任意のアドレスで書き換えることで，内部ネットワークを隠蔽する．

Fig.1 にゲートウェイ方式の概要を示す. 内部端末 A が外部端末 C へ通信を開始する場合，送信元アドレス A，宛先アドレス C として通信を開始する．このとき GW は送信元アドレスを任意のアドレス X1 に書き換え, 変換テーブルを生成する．

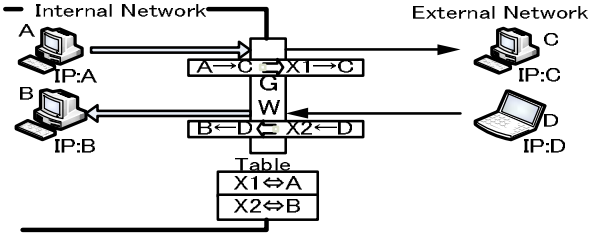


Fig.1. Gateway method

外部からの通信開始に関しては，内部端末があらかじめ GW に内部のアドレスと任意のアドレスの関係を登録しておくことにより実現が可能である．端末 D が DNS を介して端末 B のアドレスを X2 として認識し，X2 宛てのパケットが GW に到着する．GW では登録済みのテーブルに従い X2 を B に変換する．

(2)　エンドノード方式

端末が IPv6 アドレスを通常のアドレスと，外部通信用の任意のアドレスの 2 つのアドレスを持つ．通信相手が内部端末か外部端末かによって使用するアドレスを選択する．

Fig.2 にエンドノード方式を示す．内部端末には，通常のアドレス A，B と，任意のアドレス X1，X2 の 2 つのアドレスをそれぞれ割り当てる．内部端末 A が通信を開始する際に，通信相手が内部端末であればアドレス A を送信元アドレとして選択する．通信相手が外部端末である場合は，アドレス X1 を送信元アドレスとする．この場合，中継ルータはパケットの送信元アドレスから端末 A の位置を登録していく．外部端末からの通信開始に関しては，内部端末が DDNS 登録をする際のパケットを用いて，中継ルータが送信元アドレスを登録しておくことにより実現可能である．

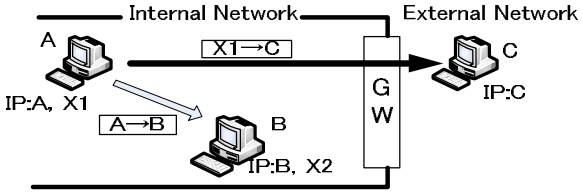


Fig.2. End node method

４．　まとめ

企業ネットワークにおいて，内部ネットワークのアドレスを隠蔽する方式について提案した．ゲートウェイ方式では，ゲートウェイのみの改造で良いが，IP アドレスを直接扱うアプリケーションでは GW での対応が必要である．エンドノード方式では，端末とルータへの改造が必要である．今後は，2 通りの方式について更に検討を進める．

文　献

[1] C. Huitema, B. Carpenter “Deprecating Site Local Address” RFC3879 September 2004

[2] T. Narten, R. Draves “Privacy Extensions for Stateless Address Autoconfigration in IPv6” RFC3041 January 2002

企業ネットワークにおける IPv6アドレスの隠蔽方式

名城大学理工学部
久保敷透　寺澤圭史　鈴木秀和　渡邊　晃

研究背景

- IPv4アドレスの枯渇
  - 短期解決策
    - プライベートアドレスやCIDRの使用
  - 長期解決策
    - IPv6アドレスへの移行
- IPv6アドレスのセキュリティ
  - IPv6ではNATを使用せずすべての端末に一意なアドレスが割り当てられる
  - 端末の特定やネットワーク構造の予測をされる可能性がある

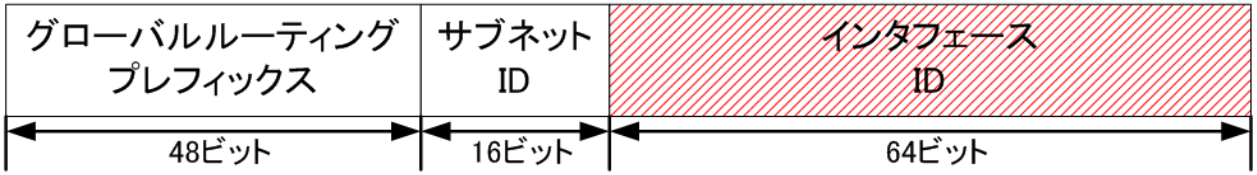
IPv6アドレスを隠す方法の検討

CIDR: Classless Inter-Domain Routing
NAT: Network Address Translation

既存技術

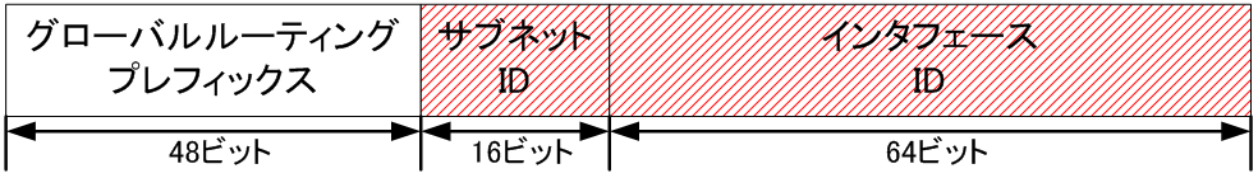
- サイトローカルアドレス(RFC3513)
  - プライベートIPv4アドレスと同様のアドレス
  - サイトローカルアドレスはRFC3879により廃止が決定（アドレスの重複、NATを助長する可能性）

- 匿名アドレス(RFC3041)
  - 下位64ビットのインタフェースIDを匿名化
  - サブネットIDによりネットワーク構造が予測される



提案方式

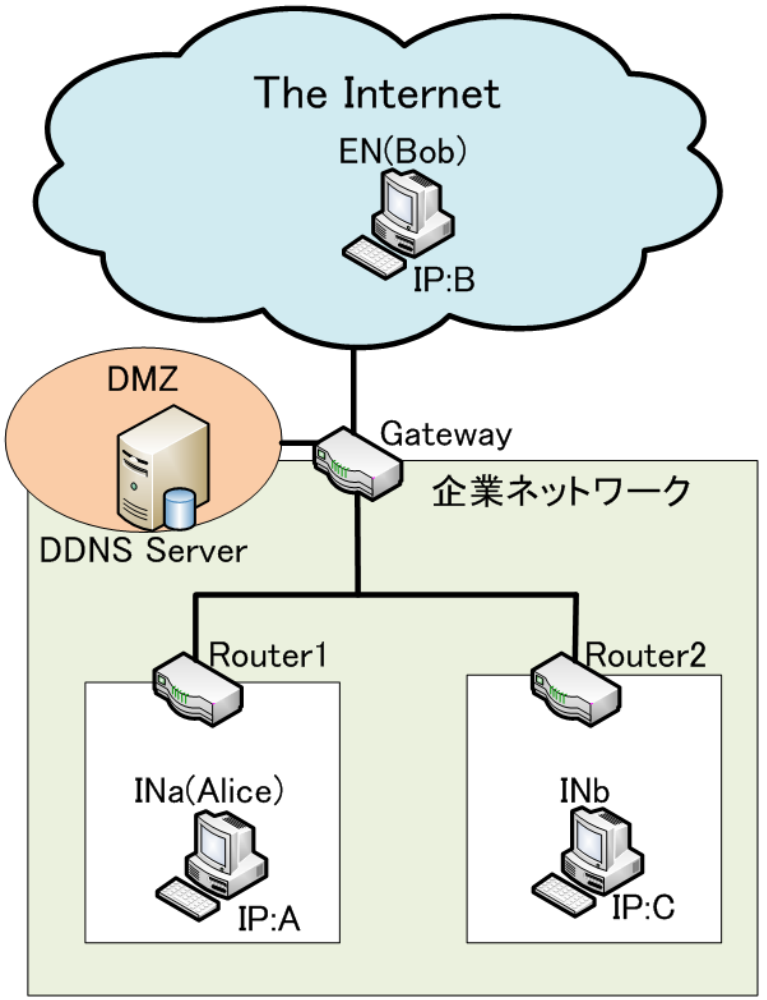
- IPv6アドレスにおいて企業ネットワークの内部構造を隠蔽する
  - IPv6アドレスの下位80ビット（サブネットIDまで）を匿名化
  - これを隠蔽アドレスと呼ぶ



- 提案方式
  - ゲートウェイ方式
  - エンドノード方式

ネットワーク構成

- ネットワーク構成
  - 内部端末：INa,INb
  - 外部端末：EN
  - Router1,Router2
  - Gateway
  - DDNS Server

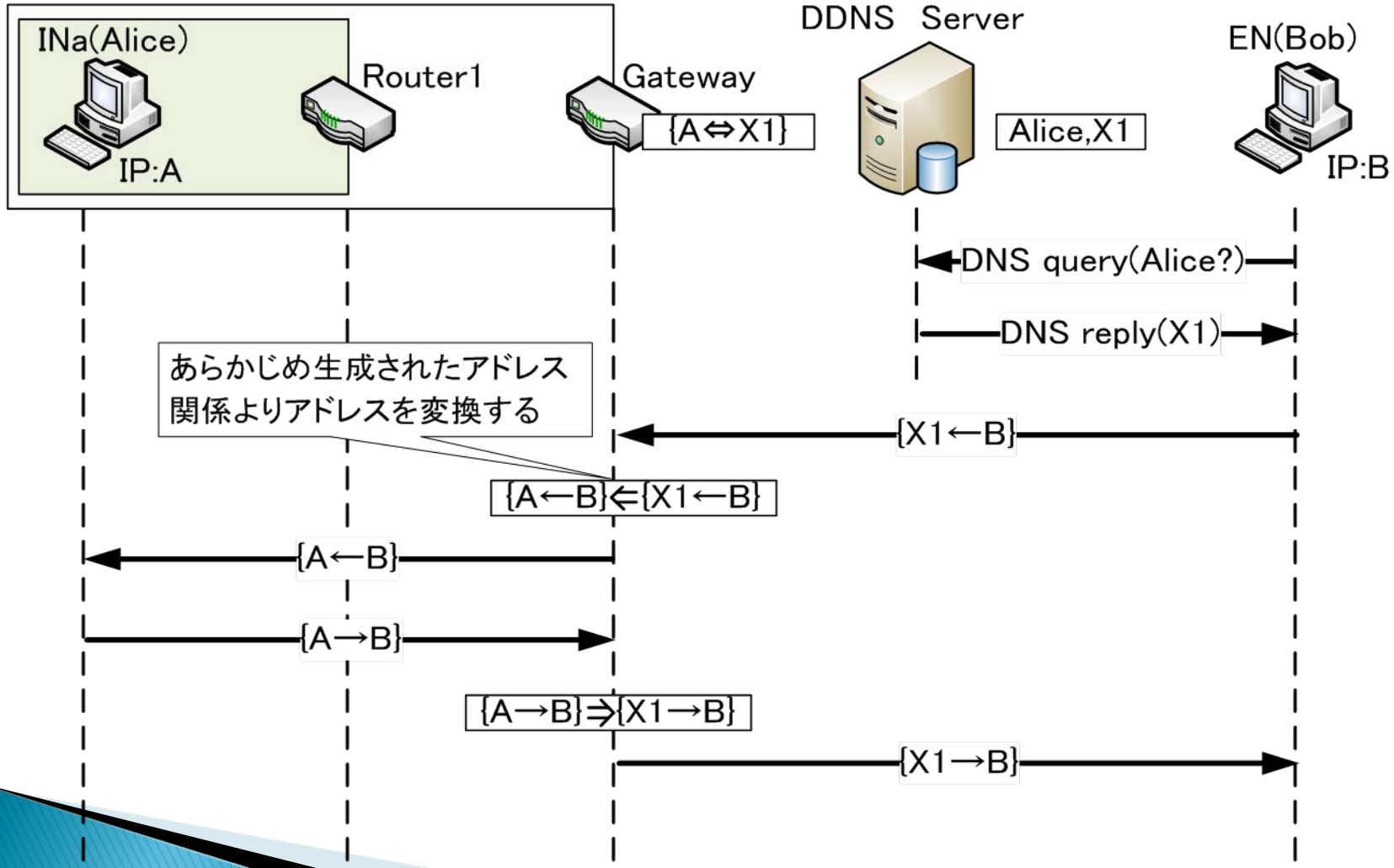


IN: Internal Node EN: External Node
DDNS: Dynamic DNS
DMZ: DeMilitarized Zone

ゲートウェイ方式

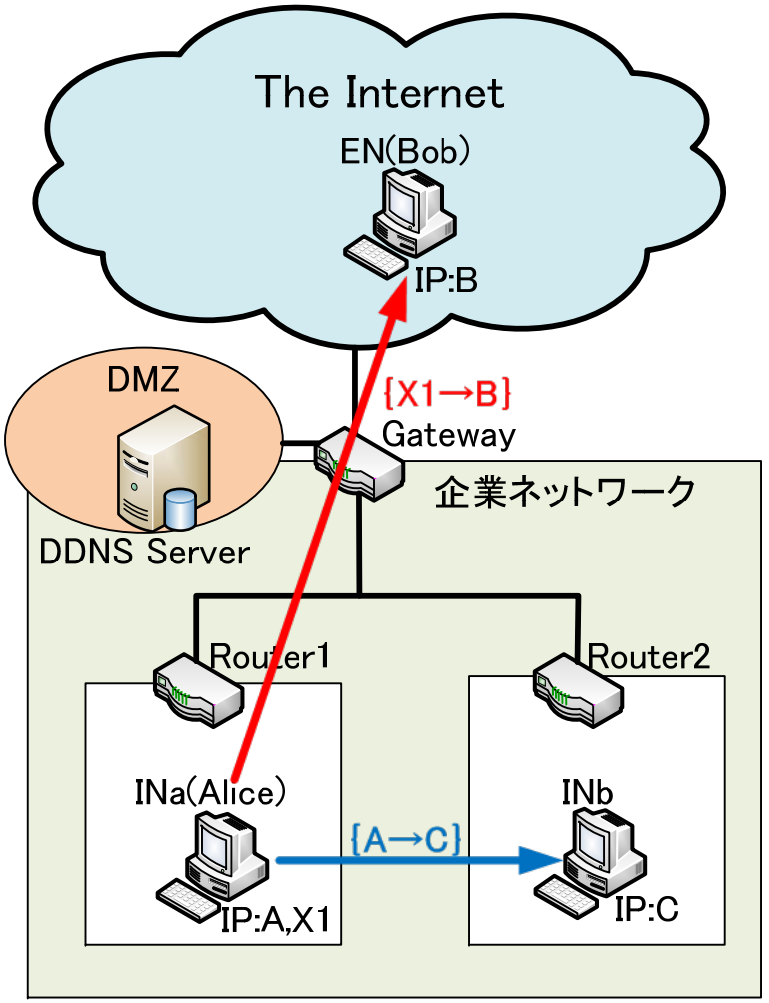
- ゲートウェイ方式
  - ゲートウェイによって内部ネットワークのアドレスを隠蔽
  - 隠蔽アドレスをゲートウェイで生成し実アドレスを隠蔽アドレスに変換する
- 事前準備
  - あらかじめゲートウェイへ実アドレスと隠蔽アドレスの関係を登録しておく必要がある

ゲートウェイ方式（外部→内部）

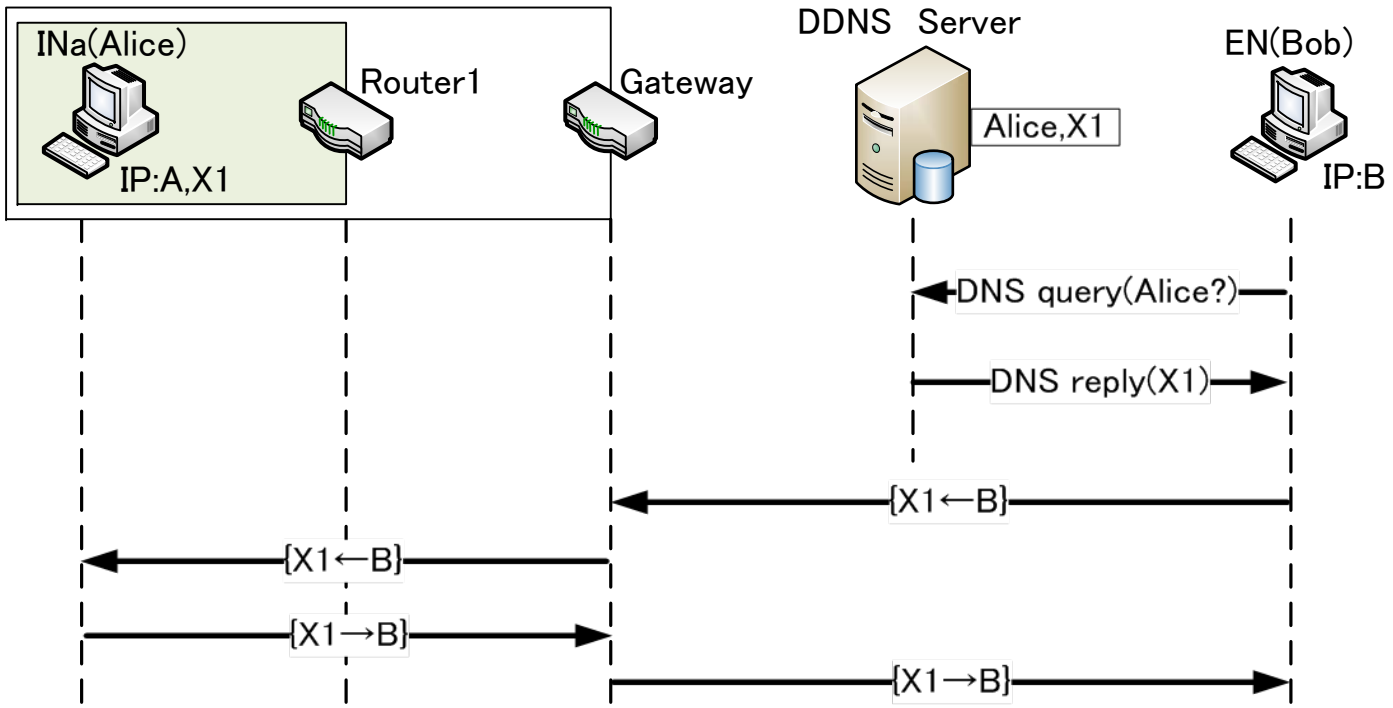


エンドノード方式

- エンドノード方式
  - 端末は実アドレスと隠蔽アドレスの2つを持ち通信相手によって使い分ける
  - 内部との通信
    - 実アドレスAを使用する
  - 外部との通信
    - 隠蔽アドレスX1を使用する



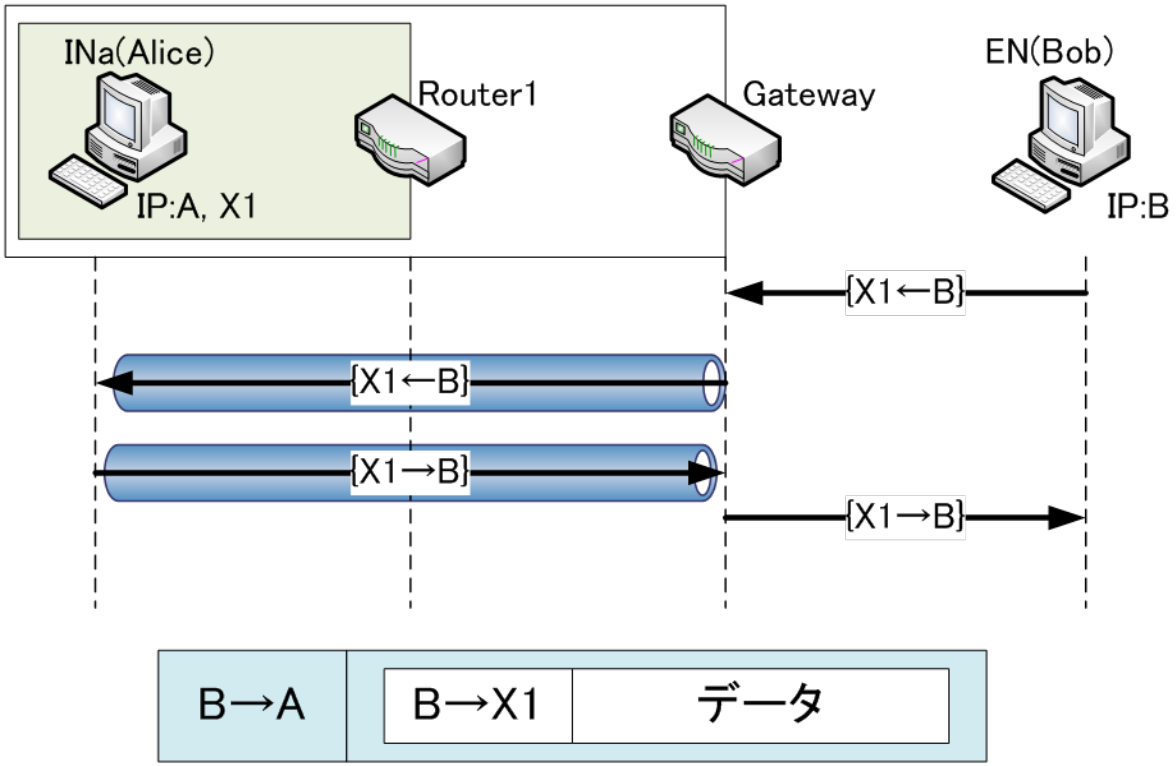
エンドノード方式（外部→内部）



- 外部端末との通信
  - 外部からのパケットは、隠蔽アドレスを用いているためルーティングすることができない。そのため端末まで届くようにする必要がある

エンドノード方式のルーティング

- カプセル化
  - 端末からゲートウェイまでを実アドレスでカプセル化する



提案方式の比較

	改造箇所	管理負荷	アプリケーション
ゲートウェイ方式	ゲートウェイ、端末	△	△
エンドノード方式	端末、ゲートウェイ	△	○

- 管理負荷
  - どちらの方式においてもゲートウェイですべての端末のアドレス関係を管理する必要がある
- アプリケーション
  - ゲートウェイ方式ではIPアドレスを埋め込むアプリケーションの対応が必要

まとめ

- 提案方式
  - IPv6アドレスにおいて企業ネットワークの構造を隠蔽する方式の提案
- 今後の課題
  - アドレスの生成方法
  - エンドノード方式におけるアドレス選択やルーティング方法

付録　匿名アドレス生成方法

- ハッシュ関数を使用しハッシュ値の上位64ビットをインタフェースIDに割り当て、上位64ビットを履歴バッファとして記憶する