

2005 年 IPv6 移行ガイドライン

大企業ネットワークにおける IP 電話導入のケーススタディ

2005 年 3 月

IPv6 普及・高度化推進協議会

移行 WG 大企業・自治体・SOHO SWG

想定ケース

ここでは、ある大企業における IPv6 による IP 電話の導入事例を取り上げます。

B社は、国内の従業員数が全国で 10,000 人、国内のグループ会社従業員数は合計 7,000 人、海外法人の従業員数は 5,000 人という規模の企業です。WAN サービスについては、国内・海外ともに IP-VPN を利用しています。そのネットワーク構成 (VPN 構成) は、本社を中心としたツリー型となっています。B社では、アドレス衝突を避けるために、各部門で NAT 機器を設置しています。海外の大規模拠点についても、本社と接続する形となっています。そして海外の拠点間は、大規模拠点を中心にツリー型の構成となっています。インターネット接続に関しては、国内の拠点については、本社を経由しています。海外の拠点については、本社ではなく海外の大規模拠点を經由してインターネットにつながるようになっています。

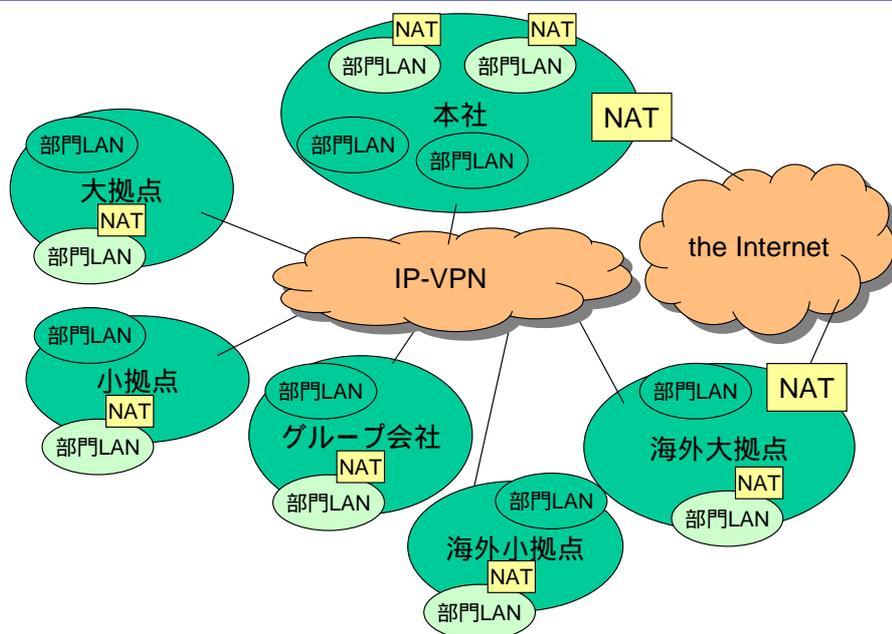


想定ケース

- 大企業ネットワークを以下のように想定
 - ◆ 親会社は国内の従業員数は合計10,000人
 - ◆ 国内グループ会社の従業員数は、合計7000人
 - ◆ 海外法人の従業員数の合計は、5000人
 - ◆ WANサービスは国内、海外共にIP-VPNを使用
 - ◆ ネットワーク構成は、本社を中心とするツリー型構成
 - ◆ 各部門毎にアドレス衝突を避けるためのNAT機器を設置
 - ◆ 海外大規模拠点は本社と接続
 - 海外のネットワーク構成は、大規模拠点を中心とするツリー型構成
 - ◆ The Internet接続
 - 国内の各拠点は、本社経由で接続
 - 海外の拠点は海外大規模拠点経由で接続

	拠点数	従業員/拠点	合計
本社	1	5000	5000
大規模拠点	5	700	3500
小規模拠点	15	100	1500
		小計	10000
国内グループ会社	10	700	7000
海外大規模拠点	5	700	3500
海外小規模拠点	15	100	1500
		小計	12000
		合計	22000

ネットワーク概念図



3

IPv6PC Transition WG Enterprise SWG

B 社ネットワークにおけるモチベーションと問題点

B 社における IPv6 での VoIP 導入の背景として、導入前における同社のネットワークの状況を考えてみます。

B 社では、ネットワークを社内の部門統合や分離、M&A による事業規模の拡大に対応させる必要があります。こうした対応を進める上での問題点として、以下が挙げられます。

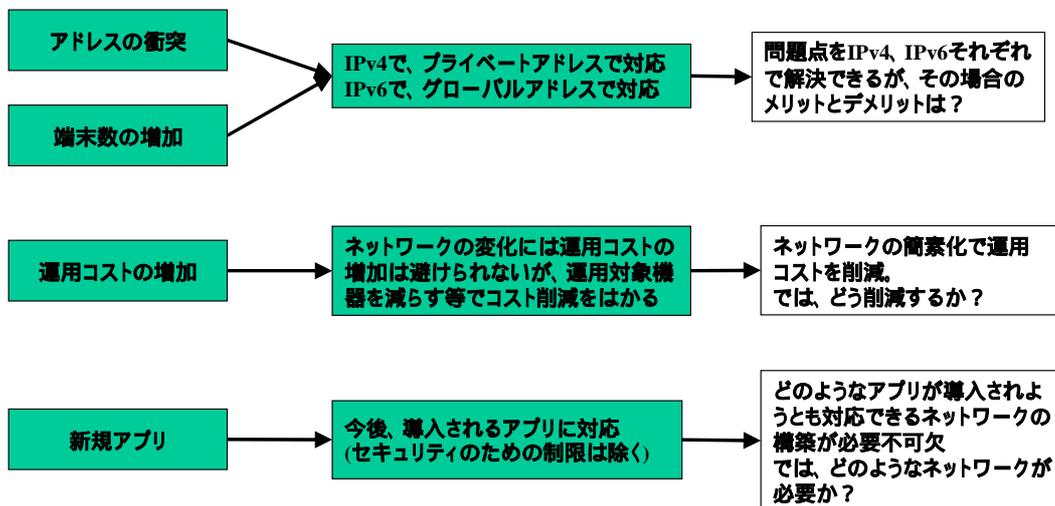
- ・ IPv4 で構築されたプライベートアドレスが、企業統合で生じるプライベートアドレスの衝突
- ・ PC だけでなく、今後予想される無線 LAN 電話導入等による端末の増加 (= サブネット設計の複雑化)
- ・ 導入される機器が多くなり、ネットワーク管理運用費用の増加

投資効果や、今後の技術動向、サービス動向等も踏まえ、これらについての解決策を検討する必要があります。その際、アドレス問題に起因している項目が多いので、まずこの問題を解決する

ことを考えます。

まず、プライベートアドレスの衝突や端末数の増加については、IPv4、IPv6 のどちらでも解決策はありますが、それぞれのメリット、デメリットを考慮する必要があります。運用コストの増加については、ネットワークの簡素化で対応できる可能性があります。問題はどうすればこれが実現できるかにあります。また、将来のアプリケーションへの対応についても、ネットワークとしての対応をどのように行うかが焦点となります。

解決方針



IPv4 で考える限り、継ぎ接ぎのネットワークになる可能性が高いこと、使用アプリケーションが限定される可能性が高いこと、そしてネットワーク管理対象が増えることで、管理コストが増加する可能性が高いこと、が考えられます。

では、まずアドレスの衝突や端末数の増加の問題を考えましょう。

IPv4 の場合、具体的な対応策としては、以下の 4 つの選択肢があります。

- ・ NAT を使い続ける
- ・ プライベートアドレスのアドレスレンジが拠点間で衝突するのを回避するため、その都度アドレスの再割り振りを行う
- ・ アドレスレンジの変更を避ける代わりに、ネットマスクを変更する
- ・ セカンダリアドレスを利用する

これら IPv4 における 4 つの選択肢と IPv6 の利用のそれぞれのメリット、デメリットは下の表のとおりです。IPv4 における方法は、いずれも当座の解決策にはなるものの、ネットワークの複雑化を招き、将来を考えると拡張性が限定されてしまうことが懸念されます。一方、IPv6 ではシンプルなネットワーク構成が可能で、発展性に優れていると考えられます。



IPv4とIPv6の比較

IPv4とIPv6、それぞれで対応したときのメリットとデメリット

	方法	メリット	デメリット
IPv4	NAT	NAT装置を設置、またはルータにNAT機能をさせることで簡単・安価に対応できる	NATより先のネットワーク状況が把握しにくく、集中管理ができない。 アプリによっては、使用できないものがある。 運用対象の増加
	Renumber	再構築することで、管理しやすいネットワークを構築できる	ネットワークの見直しが必要になり、再設定作業、移行作業に伴う、コストが発生する。 今後導入するアプリによっては、再度ネットワーク見直しが発生する可能性がある
	ネットマスクを変更	Renumberしたときと同じような現象になる	
	セカンダリアドレス	NATを導入したときと同じような現象になる	
IPv6	アドレス取得	アドレス枯渇に対応でき、ネットワークにscalabilityを持たせることができる。簡潔なネットワークの構築が可能	IPv6対応のネットワーク構築が必要になる。 現状では使用できないアプリが存在する

IPv4で対応した場合、その場限りの構築は可能だが、必ず行き詰まり、構築コストも継続して発生する可能性はある。しかし、ネットワークをIPv6対応することで、今後の行き詰まりはIPv4で構築した場合に比べて少ないと考えられる

IPv6 におけるセキュリティ上の考慮点

ただし、IPv6 で企業ネットワークを構築する場合には、セキュリティに関して事前に十分考慮する必要があります。IPv4 とは異なる考え方や新たな対策が必要となる面もあります。IPv6 ネットワークでは、以下の点に留意してセキュリティ対策を行うべきです。

ファイアウォール(企業境界ファイアウォール)

インターネットと社内ネットワークの境界に配置されるファイアウォールは、基本的に次のポリシーに基づいて運用すべきです。

- ・ DMZ とインターネット間の IPv6 ルーティング許可
- ・ DMZ と社内網の IPv6 ルーティング許可

- ・ 社内網とインターネットの IPv6 ルーティング不許可

踏み台防止(DMZ 内サーバ)

DMZ 内のサーバでは、プロキシを禁止し、セキュリティ侵害の踏み台になることを防ぐべきです。

DMZ 内サーバおよび社内向けサーバのウイルス対策

これらサーバに対し、ウイルススキャンデータの設定を行います。

社内向けサーバセグメント用ルータにおける不正アクセス防止

IPv4 については NAT(DNS はスタティック NAT)を設定します。フィルタリングに関しては、このセグメントでは IPv6 SIP のみを許可します。

部門ルータにおける不正アクセス防止

IPv6 の帯域を一定に制限することも考慮します。

部門ファイアウォール

部門レベルのファイアウォール設定は、IPv4 については従来通りです。一方、IPv6 については、状況に応じて、すべての通信を許可するか、SIP および指定ポート番号のみを許可するかを選択します。

一般 PC

社内の一般的な PC 端末に関しては、パーソナルファイアウォールを導入し、SIP 電話関連アプリケーションの許可を指定します。ウイルススキャンも実行します。端末を特定するため、IPv6 のアドレス管理に関しては、匿名アドレスの利用を禁止し、EUI-64 に基づくアドレスを利用します。

運用コスト増大および新規アプリケーションへの対応

3 つの主な課題のうち、最初の課題であるアドレス衝突や端末数の増大に関しては、すでに検討しました。それでは残りの 2 つの課題、つまり運用コストの増大、そしてアプリケーションの対応についてはどうでしょうか。

運用コストに関しては、ネットワークが拡大すれば、ネットワーク構成も複雑化する傾向にあることは否定できません。しかし、管理対象機器をできるだけ減らす努力をすることで、その複雑化傾向を抑えることが可能です。特に NAT を減らすことによって、管理負荷を軽減できる可能性が生

まれます。

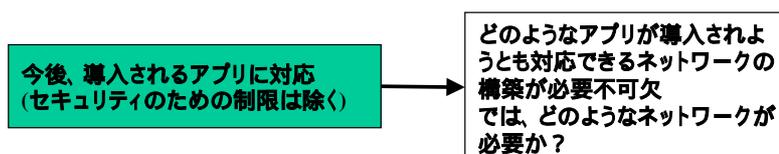
もう 1 つのアプリケーションへの対応についてですが、今後社内でも利用される可能性のあるアプリケーションに幅広く対応できるようなネットワークインフラを構築するには、基本的にできるだけプライベートアドレスの利用を避け、グローバルアドレスを利用するほうが有利であると指摘することができます。



その他の考慮点



- 簡素化するためには、管理対象機器を少なくする必要がある。余計な機器は使用しない
- 継ぎ接ぎでネットワーク構築を行ったために使用したNATを外すことで管理対象機器を少なくできる



- どのようなアプリにも対応するには、プライベートアドレスよりも、グローバルアドレスでネットワーク構築を行った方がよい

VoIP 構築に関する IPv4 と IPv6 のコスト比較

以上のことから、VoIP についても、何となく IPv6 で構築した方がよさそうだという感じはしてくるかと思います。しかし、本当に IPv6 で構築したほうがコストは安くなるのでしょうか。

それでは、B社のネットワークにおいて、VoIP を新規に導入すると仮定した場合の、IPv4 と IPv6 のコストを比較してみましょう。

B社では、IPv4 ネットワークは既に構築済みで、コア系ルータ/スイッチは約 125 台、その他のルータ/スイッチとしては約 4300 台が導入されています。IPv6 を利用する場合、IPv6 化する必要のあるネットワーク機器は、コア系のルータやスイッチの約 125 台です。IPv4 ネットワークはす

で構築されていますが、VoIP 用にアドレスの払い出し等の構築費は発生します。また、SIP 端末は、ソフトフォンとハードフォンを 1:1 の比率で配布します。VoIP を IPv4 で構築する際は、ネットワークに NAT で構築されている部分があるので、SIP セッションを保持できる装置 (SIP-NAT) が必要となります。

VoIP 構築に関する初期コストとして必要になるのは、おもに SIP サーバ、IPv4 で構築した場合の SIP-NAT、そして SIP 端末 (ソフトフォン、ハードフォン) です。

各種構築費については、IPv4 で構築した場合、VoIP ネットワーク費用、SIP 構築費用、そして SIP-NAT の構築費用がかかります。一方、IPv6 で構築した場合、IPv4 で発生した費用に、ネットワークの IPv6 化費用が必要になります。

ランニングコストとしては、各機器の保守費用、運用監視費用が発生します。

これらの要素を実際に試算すると、下のグラフのような結果となります。

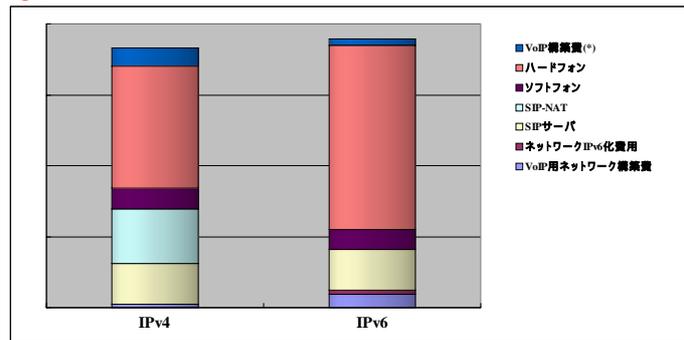
初期コストに関しては、IPv6 の場合、IPv4 と比較してネットワークの IPv6 化費用が発生し、ハードフォンについては IPv6 対応の機種が限定されることから、調達費用が大きく増加します。その一方で、SIP-NAT を購入する費用が要らなくなります。

結論として、初期コストについては IPv6 のほうがかかるものの、あまり差は見られません。ランニングコストに関しては、SIP-NAT の運用・保守費の分だけ IPv6 のほうが低くなります。結果として、今回の試算では、導入後 1 年以内に IPv6 による総コストが IPv4 による総コストを下回る結果が出ました。

コスト比較

初期コスト

IPv4の方がIPv6と比較して初期コストは安くなりそうだが、差はあまり見られない



(*)SIPサーバ構築、IP-NAT構築費用

ランニングコスト

IPv4とIPv6の差分はSIP-NATの運用保守費になる

今回のケーススタディでは、コスト回収は1年以内に可能になる

結論

今回のケーススタディでは、既存のネットワークを持っている大企業が、様々な理由でネットワーク更改を行うタイミングで、VoIPのようなセッション保持が必要なアプリケーションの導入を図る際に遭遇する問題を考えました。

構築済みのネットワークを前提にしてこうしたアプリケーションの導入を進めていくと、様々な問題が発生します。代表的な問題としては、アドレスの重複問題や、端末数の増加等によるアドレスアサインポリシーの行き詰まりが挙げられます。

さらに、IPv4とIPv6で、それぞれVoIPを構築した際の概算コスト比較を行いました。コスト的にさほど差は見られませんでした。

ネットワーク運用者からは見えないコストが発生することも否定できないので、その部分は導入対象となる各社によって違いがあると思われます。その部分が一番大切ですが、ケースによる差異が大きいため、今回のコスト比較には加えませんでした。

しかし、上記のコスト比較からは、IPv4とIPv6には差がないため、IPv6への移行についてはコスト的には問題ないように思われます。

今後のネットワーク動向を考えると、IPv6に移行していくことは避けられません。まずは小さな規模でもいいので、IPv6化に関し、様々な検証や構築見積を進めていくべきだと考えられます。

移行WG 大企業・自治体セグメント 検討メンバ

(敬称略)

SWG チェア

月岡(日立)

阪内(NEC)

メンバ

荒野(インテックネットコア)

伊藤(キヤノン)

猪俣(富士通)

及川(マイクロソフト)

太田(NTT 東日本)

大平(リコー)

加藤(NTT)

金山(インテック W&G)

国武(RINT)

鈴木(日立)

橘(あにあにどっとこむ)

田付(NEC)

徳重(NTT コミュニケーションズ)

中井(NTT コミュニケーションズ)

中原(NEC)

西田(リコー)

白田(日立)

橋本(MRI)

廣海(インテックネットコア)

山崎(NTT コミュニケーションズ)

山本(NTT 東日本)

吉岡(トヨタ IT 開発センタ)

移行WG SOHOセグメント 検討メンバ

(敬称略)

SWG チェア

猪俣(富士通)

阪内(NEC)

月岡(日立)

メンバ

荒野(インテックネットコア)

中井(NTT コミュニケーションズ)

中原(NEC)

金海(NEC)

大平(リコー)

伊藤(キヤノン)

山本(清水建設)

吉岡(トヨタ)

尾崎(富士通)

お問い合わせ先

本ガイドラインに関するお問い合わせは、以下のアドレスまでメールでご連絡下さい。
IPv6 普及・高度化推進協議会移行WG / e-mail: wg-dp-comment@v6pc.jp