IPv4 アドレスの枯渇時に生じる諸課題に適切に対処するための手順書

平成２５年１０月

目次

1　背景・目的

Carrier Grade NAT（CGN）を利用したIPv4アドレスの共有環境やIPv4/IPv6共存環境に関しては、運用、情報セキュリティ対策等に係るノウハウが十分に蓄積・共有されておらず、これまでの情報セキュリティ対策が機能しなくなる等の問題や、ISPの規模によって、必要とされる機器や機器の配置に相違があることが考えられる。

このため、IPv4アドレスの共有環境やIPv4/IPv6共存環境における情報セキュリティ対策等に必要な調査・検証を行い、IPv4/IPv6インターネットサービスに関わる事業者等が、IPv4アドレスの枯渇時に生じる諸課題に適切に対処できるよう手順書としてまとめた。

2　手順書

2.1　対象者

IPv6 環境を既に導入している企業や、IPv4 環境のみで事業を行っている企業も含め、IPv4 枯渇への対策が必要と考えられる通信事業者、ISP、ASP、コンテンツ・アプリケーション提供者、データセンタ事業者、通信機器メーカを対象とした。

2.2　手順書の策定

2.2.1　IPv4アドレス共有環境及びIPv4/IPv6共存環境における情報セキュリティ対策等に係る解説

（1） IPv4 アドレス共有環境及び IPv4/IPv6 共存環境における情報セキュリティ対策に係る課題

インターネット上に存在するサーバ側から見ると、CGN配下のクライアントの送信元IPアドレスはCGNのグローバルIPアドレスとなる。そのため、インターネット上でサービスを行うサーバでは、CGN配下のクライアントからの通信はCGNからの通信として扱われる。

一般的にAccess Control List（ACL）を用いたフィルタリングを行う場合、サーバではIPアドレスをベースとしてフィルタリングを行う。CGN配下のあるクライアントからの通信に対してフィルタリングを行うと、フィルタリングされたグローバルIPアドレスを共有している CGN 配下のクライアントすべてからサーバへの通信が不可能となってしまう。

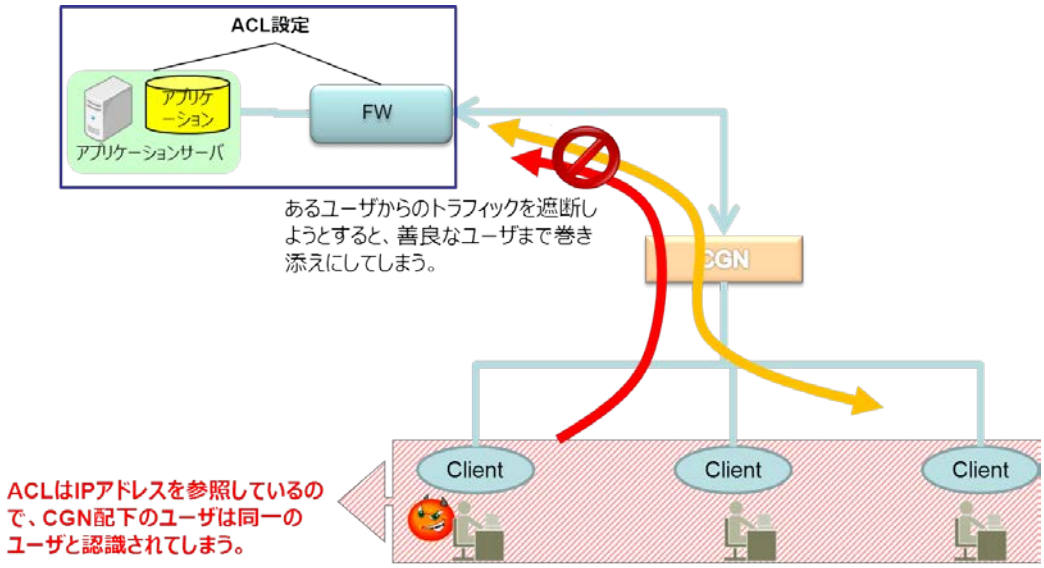


図 2.2-1　CGN 導入下での情報セキュリティ対策に係る課題

CGN の LAN にあるクライアントからの通信が、CGN からの通信として扱われることを利用した攻撃も考えられる。インターネットに存在する攻撃者が、送信元 IP アドレスを CGN の IP アドレスと詐称し、送信元 IP アドレスベースのファイアウォールを利用しているサーバへ攻撃を行うと、CGN の IP アドレスがフィルタリングされてしまう。それによって、攻撃に用いられた IP アドレスを共有している CGN の LAN に存在するクライアントすべてからサーバへの通信が不可能となってしまうという課題がある。

（2） 洗い出された課題に対する対策

IP アドレスを利用しクライアントを識別する ACL 等のフィルタリングに代わる新たな対策を講じる必要がある。

クライアントを識別する方法としては、例えば TCP ポート番号の利用が考えられるが、複数ユーザが同一のポート番号を使用することもあるので、ユーザ特定が困難である。また、IPv4 プライベートアドレスをクライアントの識別に利用した場合も、DHCP でアドレスを振られる可能性があり、毎回アドレスが変更すると管理が困難となる。MAC アドレス情報も CGN は保持しないため利用は不可である。

上記以外でクライアントを識別する方法として、現在 CGN の LAN からインターネットに向かう通信上においてクライアントの識別子を含む情報を付与することにより、識別を行う方法が提案されている。識別子はホスト ID[1]と呼ばれ、CGN の IPv4 プライベートアドレスや IPv6 フローラベルなどが用いられる。

図 2.2-2 は、ホスト ID を付与した場合、サーバから見た CGN の LAN にあるクライア

[1] http://tools.ietf.org/html/draft-boucadair-intarea-nat-reveal-analysis-04

ントからの通信の様子である。

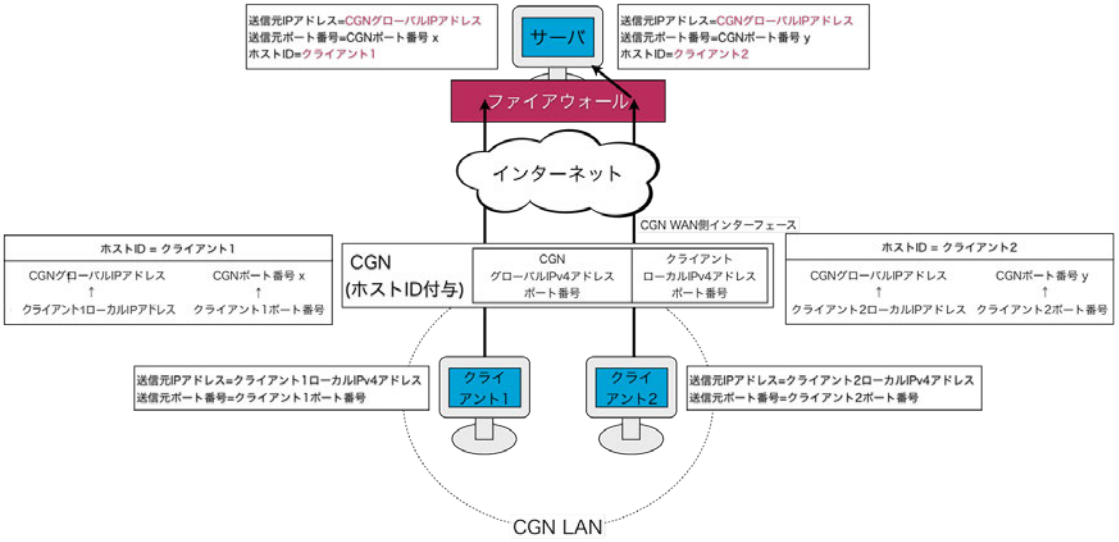


図 2.2-2　サーバから見たCGNのプライベートネットワークにあるクライアントからの通信（ホストIDを付与した場合）

CGN の LAN にあるクライアント１とクライアント２の通信は、CGN によって送信元 IP アドレスが CGN のグローバル IP アドレスに変換されている。CGN はインターネットへ送り出すパケットに対し、ホスト ID を付与している。そのため、インターネット上に存在するサーバはホスト ID を参照することによって、クライアント１の通信とクライアント２の通信を識別することが可能である。ホスト ID を用いたフィルタを書くことによって、従来のフィルタのようにグローバル IP アドレスを共有している複数のクライアント全てをフィルタリングすることなく、クライアントごとにフィルタリングを行うことが可能になると考えられる。

ホスト ID をどのヘッダのフィールドに埋め込むかについては複数の案がある。IP 層より上位の層でホスト ID を埋め込むものは、そのプロトコルを用いた通信でしか用いることが出来ない。例えば、TCP ヘッダのオプションにホスト ID を埋め込む方法が提案されているが、この方法では UDP を用いた通信においてホスト ID を埋め込むことが出来ない。汎用的にホスト ID を使うためには、IP ヘッダにホスト ID を埋め込む必要がある。IP ヘッダにホスト ID を埋め込む方法としては、IP オプションにホスト ID を埋め込む方法と、IP ヘッダの識別子フィールドにホスト ID を埋め込む方法が提案されている。

本検証では、ホスト ID を IP オプションに埋め込む方法を用いる。それによって、パケットがどのようにフィルタリングされるか検証を行う。また、CGN の WAN に存在する攻撃者が、CGN になりすまして攻撃を行う場合、ホスト ID がどのように作用するのか、検証を行う。

(ア) ホスト ID の有用性

以下の方法を用い、ホスト ID の有用性について検証した。

(A) CGN 配下の LAN から行われる攻撃

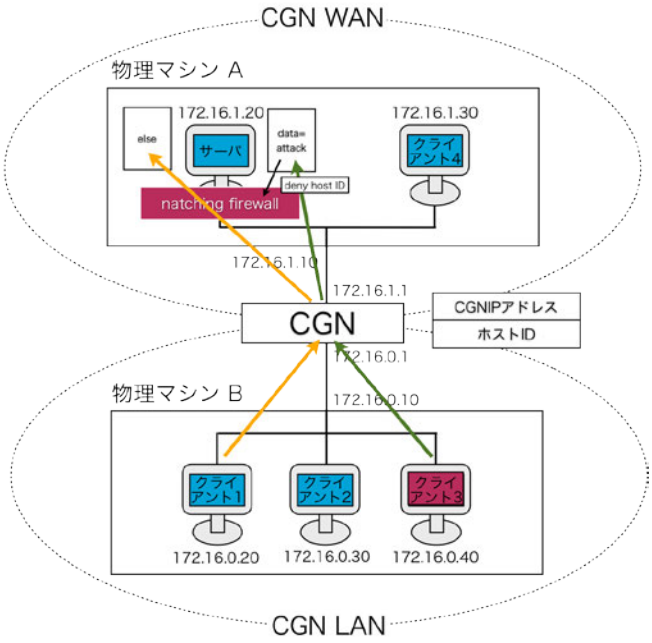


図 2.2-3　CGN 配下の LAN からの攻撃（送信元 IP アドレス）

CGN には 2 台の物理マシンが接続され、それぞれのマシンの中には Kernel-based Virtual Machine（KVM）を用いて複数の仮想マシンを立ち上げる。物理マシン A には、サーバとクライアント 4 が設置され、CGN の WAN 環境（インターネット）として設定される。物理マシン B には、クライアント 3 台（クライアント 1、クライアント 2、クライアント 3）が設置され、CGN の LAN 環境として設定される。ホスト ID は一般的に用いられている方法ではないため、ホスト ID を用いた検証を行うために 2 つのツールを用意した。1 つは、ホスト ID を参照してフィルタリングを行うホスト ID 処理機能付き firewall（以下、本稿においてのみ便宜上、natching firewall とする）である。もう 1 つは CGN の LAN からインターネットへ転送されるパケットの IP オプションにホスト ID を付与する機能を持つソフトウェア CGN、StarPorte[2]である。本検証では、ファイアウォールに natching firewall を用い、CGN に StarPorte を用いて検証を行う。

[2] 本稿においては、IPv4/IPv6 ともフルルートのトランジットの提供を受け、 インターネットへの接続性を確保している大規模検証用ネットワークを指す。

CGN の同一 LAN 内にあるクライアント（CGN にぶら下がっているクライアントが利用するグローバル IP アドレスは全て同一となる）のうち、ある一人のクライアントからインターネットに存在するサーバに攻撃をする。CGN ではクライアントごとにホスト ID を付与する機能があるため、その機能を実行し、挙動を検証した。

その結果、サーバにおいて、CGN 配下の LAN に存在するクライアントの判別が可能となり、ホスト ID を用いてフィルタリングを行うことによって、フィルタリングしたい対象（図 2.2-3 におけるクライアント 3）に的確にフィルタリングすることが出来た。

(B) CGN の IP アドレスを用いホスト ID を付与した通信を行うクライアントからの攻撃

仮に CGN の WAN に存在する攻撃者（図 2.2-4 におけるクライアント 4)、つまり送信元 IP アドレスを CGN の WAN 側のインターフェースに付けられた IP アドレスとし、IP オプションにクライアント 1 のホスト ID を付与し、attack を仕掛けた場合においてもホスト ID を利用したフィルタリングが有効であるか検証を実施した。

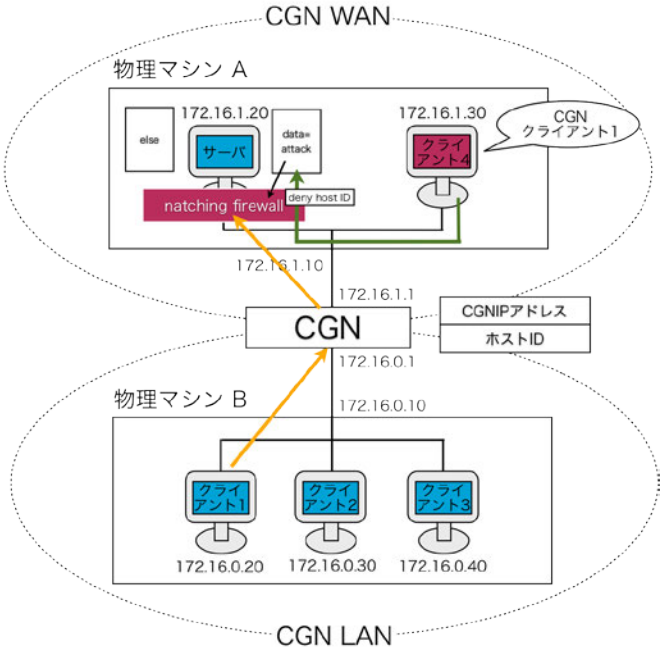


図 2.2-4　送信元 IP アドレスを CGN の IP アドレスと詐称したクライアントから行われる攻撃

検証の結果、CGN の IP アドレスを用いホスト ID を付与した通信を行うクライアントからの攻撃においても、CGN の IP アドレスとホスト ID の組み合わせが合わなけれ

ば、攻撃として効力を発揮しないことが明らかとなった。

上記(A)、(B)の結果より、CGN 配下のフィルタリング方法としてホスト ID の付与が有用であることが示された。

ただし、実際のインターネットにおいて、IP オプションにホスト ID を付与する方法は使用することが難しい。インターネットにおけるルータやファイアウォールの中には、RFC において定義されていない IP オプションを発見した場合、パケットを通過させないものが存在する。そのため、ホスト ID を付与したパケットをインターネットに送信した場合、通信できない場合が多く発生する。ホスト ID を実際に用いる場合、RFC での定義やオペレータへの周知が必要となる。

(イ) 最適なログ管理

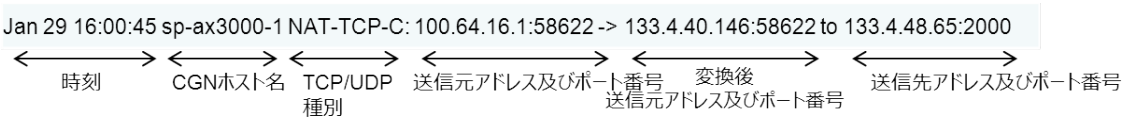
ACL を用いたフィルタリングが使えなくなることにより、情報セキュリティが確保されないという課題に対して、ホスト ID を利用したセキュリティ対策の有用性が示されたが、これによりこれまでは主に IP アドレスのログを管理すれば問題なかったものが、IP アドレスだけでなく、ホスト ID やユーザのソースポート番号等もログをとらなければならなくなり、管理すべきログ情報が膨大となる。

このため、実際のログ情報について、実証により具体的なデータ量を把握するとともに、不必要なログの削減やログ形式の工夫によるログのデータ量の削減効果について検証を実施した。

(A) ログ項目について

≪一般的なログ形式≫

以下のログによって、NAT によるソースアドレスの変換が行われたことを表す。



≪ログ生成タイミング≫

ログ生成のタイミングは、機器の実装に依存するが、以下の 4 つのタイミングがある。

① NAT テーブルの割当・消去

② データ通信の開始・終了

今回の検証では、IP アドレス及びポート番号を全てダイナミックマッピングとしたため、ユーザの通信発生ごとに NAT テーブルの割当とデータ通信の開始のログが生成され、通信が終了するとデータ通信終了と NAT テーブル消去のログが生成される。

≪ログ形式≫

ログの形式として、以下の 3 つの形式がある。

① ASCII 形式

② Compact 形式

③ バイナリ形式

Compact 形式とは、IP アドレス及びポート番号の形式を 16 進数表記にするなど、表記上の工夫によってログデータ量を削減する方法である。

また、バイナリ形式は、情報を損なわずに最もデータ量を削減できるフォーマットであるが、実際の格納形式については機器依存となる。

以上を踏まえ、基本設定及び以下の 4 つの場合を考慮し、ログのデータ量を計測した。

≪計測するログのパターン≫

・基本設定：Full Logging：

全ての下記ログを取得する。

⑴NAT テーブルの割当・消去

⑵データ通信の開始・終了

⑶送信先アドレス及びポート情報

・Case 1：Compact Option：

IP アドレス及びポート番号の形式を 16 進数表記にするなど、表記上の工夫によってログデータ量を削減する。

・Case 2：Remove include-destination：

⑶送信先アドレス及びポート情報を取得しない

・Case 3：Remove Log-session：

⑵データ通信の開始・終了情報を取得しない

・Case 4：Case 1+Case 2+Case 3：

上記の 3 つの手法を組み合わせた場合

(B) 検証結果

以下の表は、ユーザ規模 1.6 万人のうち 25%のユーザが 400 セッションの通信を”1 回”行ったと仮定した際のログデータ量等について表している。ログ対象・形式ごとに計測したログサイズ及び基本設定のログサイズを 100%としたときのそれぞれの

Case におけるログサイズ率について、表 2.2-1 に示す。

表 2.2-1　ログ対象・形式ごとに計測したログサイズ及び基本設定のログサイズを 100%としたときのそれぞれの Case におけるログサイズ率

	ログ対象・形式	Log Size	Ratio
基本設定	Full Logging	720MB	100%
Case 1	Compact Option	564MB	78%
Case 2	Remove include-destination	690MB	96%
Case 3	Remove Log-session	317MB	44%
Case 4	Case 1+Case 2+Case 3	229MB	32%

(C) 考察

≪どのようなログが必要不可欠か≫

あるユーザが特定の NAT テーブルの割当を受けている状態で、他のユーザが同一の NAT テーブル割当を用いて通信を行うケースは無いため、NAT テーブルの割当から消去までの期間が該当ユーザと特定できる期間と考えれば、NAT テーブルの割当と消去のログがあれば十分である。

上記のことから、表 2.2-1 Case3 において削減したデータ通信開始・終了の情報は、ユーザの特定に必須ではない。

以上を踏まえ、IP アドレス及びポート番号を全てダイナミックにアサインした場合に、情報セキュリティを確保するための必須ログを表 2.2-2 に示す。

表 2.2-2　IP アドレス及びポート番号を全てダイナミックにアサインした場合に、情報セキュリティを確保するための必須ログ

必須か否か	ログの種類
○	NAT テーブルの割当
×	データ通信の開始
×	データ通信の終了
○	NAT テーブルの消去

≪ユーザを特定するのに必須なログ項目はどれか≫

表 2.2-1 Case2 によって削減した送信先 IP アドレス及びポート番号については、申

告するコンテンツサーバ側が送信元のポート番号を記録していない限り、ユーザの特定に必要となる。図 2.2.6 は、CGN が通信先サーバ情報を保持していることによって、コンテンツサーバ側が送信元のポートを記録していない場合も、ユーザの特定が可能であることを図示している。しかし、異なるユーザが同じ通信先に通信しているケースも想定できるため、それらを区別するために、NAT のログに正確な時刻を記載し、サーバ側が申告している時刻と突き合わせなければならない。多くのケースでは、以上の特定は有効に働くと思われるが、異なるユーザが同一サーバにほぼ同一時刻にアクセスするようなケースでは、NAT ログ上は両者の区別をすることはできない。

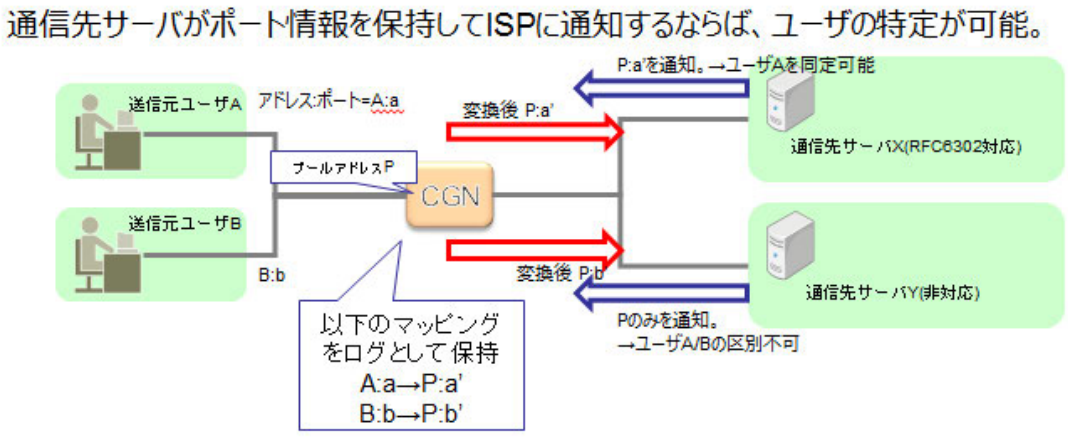


図 2.2-5　通信先サーバが送信元ポートを保持している場合

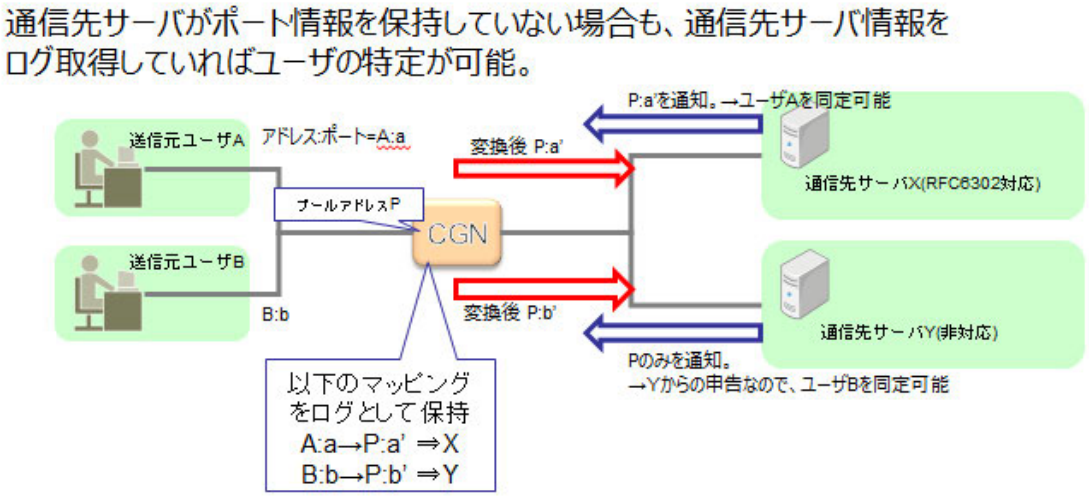


図 2.2-6　CGN が通信先サーバ情報を保持している場合

[rfc6302]において、通信先ホスト側にてアクセス元の IP アドレスだけでなくポート

番号を取得すべきと記載されており、その対応が行われている場合には不要であるが、必ずしも対応ができているとは考えないほうがよいと思われる。

また送信先 IP アドレス及びポート情報を CGN で取得すべきでない理由として[draft-ietf-behave-lsn-requirements-10]では privacy issue およびログの削減が理由として挙げられているが、ログの削減については、検証結果（表 2.2-1 Case2 参照）から大幅な効果が見込めない（96%）ことがわかっている。

privacy issue についても、ユーザ保護の観点から、ポート情報等を取得することで確実に（IP アドレスレベルという留保はあるが)ユーザの特定ができるために、通信先ログは取得した方がよいものと思われる。

しかし、IETF では現在も送信先 IP アドレス及びポート番号をユーザを特定するための必須ログとすべきかどうかが議論されており(2013 年 7 月現在)、一部の CGN では取得することをオプションとして選択できる実装となっているが、取得すべきかどうかについては、今後の議論の動向をしっかりと見極める必要がある。

以上の検証結果は、IP アドレス及びポート番号について全てダイナミックマッピングをした結果であり、ユーザ通信ごとにログの記録が必須であった。さらなるログ削減については、ユーザとアサインするポート番号を一意に事前に対応させることによって、ログを取得する必要性が変わる。方法は以下の二通りが考えられる。

① 静的マッピング

上述のとおり、ユーザとアサインするポート番号を事前に対応させる。このことにより、NAT 後の IP アドレスとポート番号から、NAT ログに頼らずユーザ特定ができるため、NAT テーブルの割当・消去のログは一切取る必要がなくなる。ただし、通信元ポート番号を記録しないサーバからの申告に対応するためには、データ通信の開始・終了のログに基づいて、通信先の IP アドレスを記録しなければならない点には注意が必要である。

② ポートブロックアロケーション

静的マッピングとダイナミックマッピングの中間にあたる手法である。

ユーザの通信ごとに 1 つのポートではなく、複数のポートブロックをまとめて割り当てを行う。ユーザの次の通信は割り当てられたブロック内のポートで通信を行う。このことによって、どのポートブロックが割り当てられたかというログを残せばよいことになるため、ポートブロックのサイズの分だけログの量を減らすことができる。

また、ユーザの通信が全て終了した時点でポートブロックを解放し、次のユーザに割り当てることができるので、効率的な利用が可能となる。また、多量のポートを利用する場合も 2 つ目以降のポートブロックを割り当てれば良く、ポート数の上

限も柔軟に変更することができる。この方法においても、場合によっては通信先の IP アドレスを記録しなければならない点には注意が必要である。

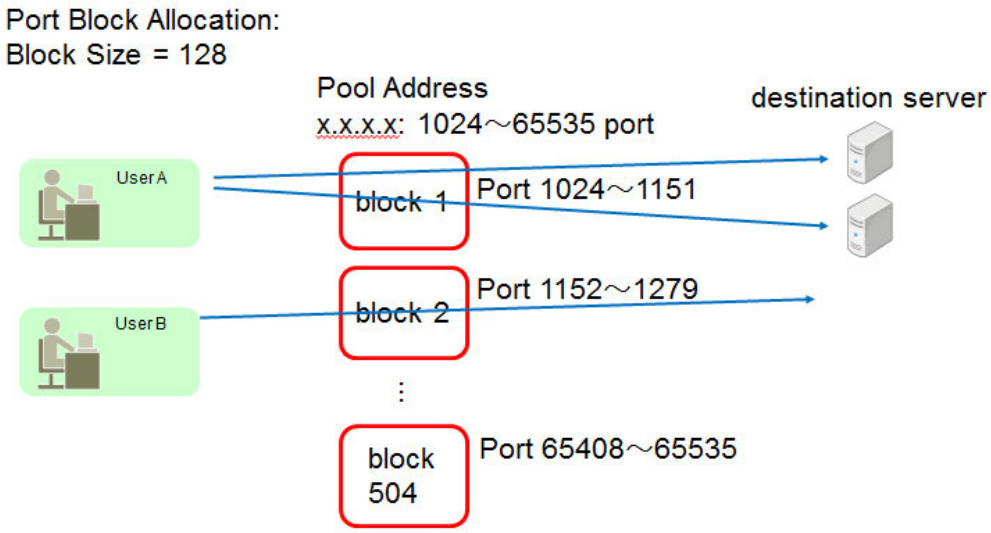


図 2.2-7　ポートブロックアロケーション

図 2.2-7 はポートブロックアロケーションを図示したものである。各ユーザは、pool address の中の決められたサイズのポート範囲(この場合では 128 ポート)を、動的に割り当てられる。一度割り当てを受けたユーザは、そのブロックを一貫して用いることになるので、ポートの割当ごとではなく、ポートブロックの割当ごとに記録をすれば、ユーザの特定が可能となる。また、利用ポート数が多いユーザの場合には、1 ユーザが複数のブロックを利用したとしても問題はない。

2.2.2 推奨対応

検証結果を元に、いくつかのモデルに類型化されたネットワークの設計や運用の方針、機器選定の方針などを明確化し、問題となるであろう課題に対して、どのように対応すべきか推奨案としてまとめた。

≪機器選定方針≫

CGN 機器の選定にあたり、基準となるキャパシティ(収容限界)は以下の 3 点である。

(A) スループット(Throughput)

(B) 同時セッション数(MCS:Max Concurrent Sessions)

(C) セッション到着率(CPS:Connections Per Sec)

これらは、それぞれが独立ではなく、CGN 機器に対して複合的な負荷となる。

そのため、メーカの公称値（カタログ値）は特定の条件下においてそれぞれ達成された値であり、実網トラフィックにおいては各負荷が合計されるので、実際の収容限界値がカタログ値を下回る可能性が高い点については、実環境で検証を行うことを推奨する。

今回の検証においては、StarBED[3]にてユーザをエミュレーションした実網に近い負荷を与えることによって、実際の性能値がカタログ値を下回っていることが確認された。

ただし、実際の性能値を一つの目安として、後述するように最適な適応箇所に CGN 機器を配置することによって、実性能に合わせた設計・導入が可能であることも確認された。

(A) スループット(Through put)

機器全体としての転送性能を示す。

現状は 1G-Ether および 10G-Ether の IF を持つ CGN 機器が各社主力であるが、各 IF ではなく、全 IF のトラフィックの合計値としての性能上限がある。

機器のアーキテクチャ依存であるが、ALG(Application Level Gateway)の ON/OFF によって、CPU を通るパスにトラフィックの処理が変わる可能性があるため、転送性能に影響を与える可能性がある。

(B) 同時セッション数(MCS:Max Concurrent Sessions)

CGN 機器の NAT テーブルに保持されるレコード数の上限を表す。

多くの CGN 機器では、NAT テーブルを格納するメモリ領域の限界値がカタログ値

---

[3]独立行政法人情報通信研究機構（NICT）の北陸 StarBED 技術センターが運営する世界最大規模のエミュレーション基盤

として記載されている。

TCP/UDP/ICMP で別々に管理されている場合もあれば合計値である場合もある。

保持されるレコード数は、NAT テーブル保持時間に依存する概念である。

なぜなら、データ通信終了後も、アプリケーションの挙動を担保するために一定時間 NAT テーブルを保持するからである。

REQ-8（巻末[1]参照） に記載されている通り、TCP のセッションを管理しているものについては、TCP の RST または FIN が観測されたら NAT テーブルを解放してよいが、RST または FIN が観測されていない TCP セッションや、UDP、ICMP の通信については、一定時間 NAT テーブルを保持すべきである。

また、Full Cone NAT の場合、外部からの通信を一定時間待ち受けるため、Full Cone NAT のテーブルについても一定時間保持すべきである。

これらの NAT テーブル保持時間は time out 値を、設定可能な機器を選定することが望ましい。

NAT テーブル溢れを抑えるために time out 値を短くすることは有効であるが、実際に行う際にはアプリケーションの挙動を阻害しないか注意深く行う必要がある。

すでに実トラフィックの流れている区間に対し、最大の同時セッション数を見積もることは非常に難しい。理論的には、以下のようになる。

<式>

同時セッション数 = 契約数 × Active ユーザ率(%) × 1(Active)ユーザ当たりの平均セッション数

<定義>

契約ユーザ：当該 ISP に契約しており、潜在的に CGN 区間を通過する可能性のある契約数

Active ユーザ：該当期間に実際にトラフィックを流している契約ユーザ数

平均セッション数：1Active ユーザ当たりの NAT テーブル上のレコード数を表す。

最大同時セッション：トラフィックの最繁時間帯(夜 9 時～1 時)での値を見積もる。

今回の検証では、仮に

- 最大 Active ユーザ率(%) = 25%
- 1 ユーザ当たりのセッション数= 400

として、1 万ユーザの場合は最大 100 万セッションとして見積もった（巻末[2]参照）。

ISP 毎のポリシによって Active ユーザ率は異なると思われるが、上記の仮定において、今回の検証では、10 万ユーザ規模であれば 1 台の CGN 機器で収容が可能であることが示された。

(C) セッション到達率(CPS :Connections Per Sec)

同様に、すでに実トラフィックの流れている区間に対し、CPS の値を見積もること

は非常に難しい。冗長化時にスタンバイ側の機器に突然トラフィックが流れるようなケース(※1)では、CPS 性能が律速となるため、障害時の影響を最小化するために CPS の高い性能を持つ機器を選択すべきである。

(※1)今回の検証では、スタンバイ機器ともセッション同期を行った上で切り替えを行ったが、実際にはセッション同期が行えない機器やそのような状況が存在する。

≪設計検討項目≫

設計時に検討すべき項目は以下の 9 点である。

(1) プールアドレス設計
(2) Shared Address 設計
(3) ポート割り当て手法設計
    a. 動的割り当て (Dynamic Allocation)
    b. PBA (Port Block Allocation)
    c. 静的割り当て (Static Allocation)
(4) time out 値設計
(5) EIM/EIF(Full Cone)設計
(6) hairpining 設計
(7) ALG 設計
(8) ログ設計
(9) ログサーバ台数/サーバ冗長化設計

上記の検討項目で機能を満たさない場合は、機器選定からやり直しする必要があるだろう。

(1)プールアドレス設計

十分な数のプールアドレスを用意しなければアドレスプールが枯渇し、ユーザの新規通信が阻害されてしまう。

CGN 機器は、NAT テーブルが用意できない場合はそのパケットをドロップし、送信元に ICMP エラー(Host Unreachable)を返す。([1] REQ-11)

必要なプールアドレス数については以下のように設計する(動的割り当ての場合)。
例えば、今回の以下の設定に従った場合、

- Active ユーザ率(%) = 25%
- 1 ユーザ当たりのセッション数(session/人) = 400

1 万ユーザを対象とした場合、最大 100 万セッションとなるので、各プール IP アドレスあたり約 32000 ポートが利用できるとした場合(※2)、

1,000,000 (session) / 32000 (port) = 31.25 (個)

となる。

1 万ユーザに対してプールアドレスとして 32 個(=/28)アドレスを用意すればよいことになる。この時のアドレス集約効率は、

10000 (人) / 32 (個) = 312.5 倍

となる。

(※2) [rfc4787]において、NAT の動作として Well Known Port(0～1023)以外のポート(1024～65535)が利用できると定義されているが、ここではエフェメラルポートとして Linux では 32768～61000、IANA 提言では 49152～65535 となっていることから、32768 以降のポートは問題なく利用できるものと考え約 32000 ポートとした。

プールアドレス帯については、今後の拡張性を考え、必ずしも連続したアドレス帯でなくても追加できるような機器が良い。(cf. [1] REQ-3)

また、上記 REQ-3 についてはプールアドレス数について上限が無いほうが良いとあるが、実際には機器によっては上限があるため、十分なプールアドレス数を保持できる機器を選定すべきである。

(2)Shared Address 設計

ユーザに実際に割り当てるアドレスを設計する。

特に問題がなければ[RFC6598]に従い、100.64.0.0/10 空間を利用すべきであろう。これは既存の[RFC1918]に従うプライベートアドレス空間(10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)との重複を避けるためである。

CGN 装置を複数設置して Shared Address ドメインが複数に別れる場合には、Shared Address を全顧客に対して固有に割り振るか、重複を許すかについては、各事業者の設計ポリシに委ねられる。100.64.0.0/10 空間は約 419 万個の IP アドレスを含むため、多くの事業者にとってはユニークな割り振りで問題は無いと思われる。

(3)ポート割り当て手法設計

ユーザにどのようにポートを割り当てるかについては、大きく分けて以下の 3 つの手法がある。

- 動的割り当て (Dynamic Allocation)
- PBA (Port Block Allocation)
- 静的割り当て (Static Allocation)

これらの選択は、プールアドレス設計、ログ設計およびセキュリティ対応と深く関連する項目である。

一般に、アドレス利用の効率性とログ管理の問題の 2 点から見たそれぞれの手法の利点・欠点は以下の通りである。

表 2.2-3　アドレス利用の効率性とログ管理の問題から見たそれぞれの手法の利点・欠点

	動的割り当て (Dynamic Allocation)	PBA (Port Block Allocation)	静的割り当て (Fixed Allocation)
効率	◎	○	×
ログ	×	○	◎

以下にそれぞれの手法についての詳細を記載するので、設計の際の参考にされたい。

a.動的割り当て（Dynamic Allocation）

-NAT 集約効率について

動的割り当てを選んだときのプールアドレス数の設計および集約効率については、(1)で記述した通りである。

- ログについて

動的に割り当てを行うため、NAT テーブルの割当・解放について記録する必要がある。そのため、ログの量は非常に膨大になる。

ログの量の問題については(8)にて記述する。

- ユーザごとのポート上限数について

動的割り当てによって柔軟にユーザに IP アドレスの割当を行うことができるが、特定ユーザによるポートの占有により他ユーザの通信を阻害できてしまうという問題がある。そのため、ユーザごとのポート上限数を設定できる機器が望ましい。

検証結果より、各アプリケーションについて 100 程度のセッションが発生することから、複数端末が同一 CPE 配下にある状況を考慮して、1000 ポート程度を目安としてキャップすることが良いと思われる。

- IP address/Port selection

NAT 変換後のソースポートについて、どのポートを選択するかという問題は実装に任されている。NAT プールに複数 IP アドレスを設定した場合、どのプールアドレスを選択するかという問題も同様である。

攻撃者にとって容易に推測可能なポートを利用することの危険性が[RFC6056]において指摘されているため、特に問題がなければ、IP アドレスおよびポート番号についてランダムに選択するものが良いと思われる。

b. PBA (Port Block Allocation)

PBA は、予め決められた個数のポートブロックを動的にユーザに割り当てる方法である。動的割り当てと同様に NAT 集約効率が高く、なおかつログの量が削減できる。

-NAT 集約効率について

ポートブロックのサイズの設計については、現状で最適値というものは無い。

例えば、検証より 1 アプリケーションあたりのセッション数が 100 程度であったことから、仮にポートブロックのサイズを 100 とする。

以下の 2 つのユーザがいた場合、

ユーザ A:60 セッション

ユーザ B:120 セッション

ユーザ A は 1 ブロックを利用することになる。この時に、60 ポートは有効利用されるが、残り 40 ポートはユーザ A が完全に通信を終了するまで死蔵されることになる。ユーザ B は 2 ブロックを利用することになる。この時、120 ポートは有効利用されるが、同様に残り 80 ポートは B 用に予約されるので他ユーザには利用されない。

このように利用されないポートが生じるので、動的割り当てと比較すると集約効率は悪くなってしまう。

また、モバイルのアプリケーションのように、キープアライブを発し続け、いつまでもセッション残るような通信があることがわかっており、その少量セッションのために一つのブロックがアサインされ続けてしまうという問題も懸念される。

-ログについて

上記の例に従うと、NAT ログの量については、動的割り当てでは 180 個の割当について全て記録する必要があるが、PBA では A に 1 ブロック、B に 2 ブロックの 3 ブロックの割当の記録だけで十分であるため、劇的に削減することが可能である。

- ユーザごとのポート上限数について

動的割り当てと同様に、1000 ポート程度を目安としてキャップすることが良いと思われる。

- IP address/Port selection

ポートブロックが割り当てられるため、攻撃者にとって、利用されるポートレンジが特定できてしまう。

ブロック内のどのポートを利用するか、複数ブロック利用するときにどのブロックを利用するかについては、ランダムに選択するものが良いと思われる。

c.静的割り当て（Static Allocation）

静的割り当てはユーザに決められた数のポートを割り当てるため、動的割り当てや PBA に比較すると NAT 集約効率が悪いが、ログを取得する必要がなくなるというメ

リットがある。
　ただし、割り当ての対応について設定をする必要があり、統一的なルールで記述できない場合は、設定ファイルの量が膨大になってしまうという問題が発生する場合がある。

-NAT 集約効率について
　比較のため、動的割り当てと同様に 1 万ユーザでの場合で考える。
　1 ユーザ当たりに割り当てるセッション数については、最大値を割り当てておかないと、通信ができなくなってしまうため、1 ユーザ当たり 1000 ポート割り当てとする。
　10000 (ユーザ) × 1000 (session) = 10,000,000 (session)
のポート確保が必要となる。
　各プール IP アドレスあたり約 32000 ポートが利用できるとした場合、
　10,000,000 (session) / 32000 (port) = 312.5 (個)
となる。
　1 万ユーザに対してプールアドレスとして 312 個(1.2C)アドレスを用意すればよいことになる。
　この時のアドレス集約効率は、
　10000 (人) / 312 (個) = 32 倍
となる。
　このように、NAT による集約効率は動的割り当ての場合よりも 1 桁ほど悪くなる。

-ログについて
　静的割り当てのため、どのユーザがどのアドレス及びポート帯に割り当てるかについて、記録する必要がない。

- ユーザごとのポート上限数について
　1 ユーザごとの割当がポート上限数になる。そのため、十分と思われる数の割当が必要となる。ポートの割当数がサービスレベルに直結するため、ポート割り当て数に差をつけて、サービスレベルを分けた段階サービスを提供できる可能性もある。

- IP address/Port selection
　静的割り当てのため、攻撃者にとって、利用されるアドレスレンジが特定できてしまう。ブロック内のどのポートを利用するかについては、ランダムにするのが良いと思われる。

(4)time out 値設計

機器選定方針において記載した通り、TCP のセッションをきちんと管理しているものについては、TCP の RST または FIN が観測されたら NAT テーブルを解放してよいが、RST または FIN が観測されていない TCP セッションや、UDP、ICMP の通信については、一定時間 NAT テーブルを保持すべきである。

また、Full Cone NAT の場合、外部からの通信を一定時間待ち受けるため、Full Cone NAT のテーブルについても一定時間保持すべきである。

これらの time out 値についてはプロトコルごとに変更可能であることが望ましい。特に、今回検証した機器については、ICMP および DNS トラフィックの time out 値については短く設計されており、ポートの再利用が早かったが、その点が性能面によい影響を与えていた。

time out 値が変更可能であることによって、プロトコルの特性に合せて CGN 機器の最適化が可能である。

(5)EIM/EIF(Full Cone)設計

EIM(Endpoint Independent Mapping)とは、通信先が異なっていても、同一の送信元 IP アドレス及びポートに対しては同一のプール IP アドレス及びポートを割り当てる挙動である。

EIF(Endpoint Independent Filtering)とは、EIM によって作成された NAT テーブルにおけるプール IP アドレス及びポート向けの通信は、外部のどのホストからの通信でも受け入れる挙動である。

EIM かつ EIF であるとき、Full Cone NAT と呼ばれる。

Full Cone NAT は NAT テーブルが作成されていれば外部の全ての宛先からの通信を受け入れるため、P2P 通信が可能となる。

CGN 機器にとっては最も透過性が高く望ましい挙動と言える。

網設計として P2P 通信を望まない場合には、EIM/EIF を選択的に disable にできる機器が望ましい。今回検証した機器では、0-1023 の well known port については EIM/EIF が disable にされていたが、well known port では主にサーバ-クライアント型の通信のため、問題ないと考えられる。

なお、該当機器では、Full Cone テーブルは TCP セッション終了の後も保持されるため、通常の NAT テーブルと別に保存される（タイムアウト時間を独立に管理するため）。一般のインターネットトラフィックの半分以上は TCP/80 番通信（サーバクライアント型）のため、CGN 機器のリソースを無駄使いしないためにも、上記の設定（上段の EIM/EIF の disable に関する設定）が良いと考えられる。

(6)hairpining 設計

hairpining は、CGN 機器配下のクライアント間で、グローバルアドレスを介した折り

返し通信が可能であることである。

hairpining がサポートされていないと、ユーザ間の折り返し通信ができなくなってしまうため、折り返し通信を想定したネットワーク設計をする場合には、そのような CGN 機器は選定すべきではない。

(7)ALG 設計

ALG(Application Level Gateway)の種類が多く、また ON/OFF を選択できる機器を選定すべきである。CGN 機器の透過性という意味では、可能な限り全ての ALG を有効化することが望ましい。しかし、ALG の有効化によって性能面でのインパクトがあることから、実際に有効化するかについては、負荷状況に応じた判断が必要である。

また、検証結果より ALG の有効性が確認されたが、

- アプリケーション側の対応によって解決可能なもの(FTP passive mode, IPsec NAT traversal, TURN など)
- セキュリティ上脆弱性の発見されたプロトコル(PPTP)

については必ずしも有効化の必要はないと思われる。

(8) ログ設計

事業者には、abuse 対応等のため申告に基づいてユーザを特定するケースがある。そのために必要なのは、従来は、通信元 IP アドレスとタイムスタンプであった。

IP アドレスの払い出しを行うサーバ(Radius や DHCP)のログによって、該当時間における IP アドレスと認証情報を突合することによってユーザの特定が(※IP アドレスレベルという留保において)可能であった。

※対象のユーザが Tor 等のソフトによって接続経路の匿名化を行っている場合は、
最終的なユーザ特定は別問題となる。

しかし、CGN によって IP アドレスを共有するケースでは、通信先のホストからの申告と NAT 変換のログを突合する必要が出てくる。

検証結果より、動的割り当てをしている場合には NAT テーブルの割当・消去のタイミングで、下記のログを取得することが推奨される。

- 送信元 IP アドレス及びポート
- NAT 変換後 送信元 IP アドレス及びポート番号
- 送信先 IP アドレス及びポート番号
- Timestamp

ASCII 形式の場合、このログは 1 レコードで約 120 byte となる。

送信先 IP アドレス及びポート番号については、取らなかった場合でもログ削減量がわずかであることと、port overlapping 実施の場合には必須となるので、取得することを推奨とした。

ログの形式として、以下の 3 つの形式がある。

- ASCII 形式
- Compact 形式
- バイナリ形式

Compact 形式とは、表記上の工夫(16 進数利用)によってログの量を減らす手法である。どの方法も情報としては同じものであるが、どのような形式で保存するかの違いである。

例えば、Compact 形式は ASCII 形式と比較しログの量を約 80%にできることが検証で確認された。ログ保存の選定については、CGN 機器および各事業者の NMS(network management system)に依存するため、ここでは特に指定しない。

-RFC6302 対応について

[RFC6302]において、アドレス共有技術に関わる問題として「IP アドレスだけではユーザが特定できなくなること」が指摘されている。解決するアプローチの一つが、通信先のサーバや FW においてアクセスしてきた送信元のポート情報(および正確なタイムスタンプ)を取る方法である。ISP ではなくコンテンツ側の協力が必要であるため、必ずしもすべての申告が IP アドレス+ポート で行われるようになるわけではない。

CGN を運用している ISP に対して、IP アドレスのみで abuse の申告が来た場合、動的割り当ての場合、通信宛先もログに含めておかなければ、ユーザの同定ができない。また、静的割り当ての場合においても、通信宛先のログを全て保存しておかなければならない。

静的割り当ての場合、多くの事業者はログを取得しないと思われるが、その場合は RFC6302 に準拠のサーバからの abuse 申告だけに対応することができる、

(9)ログサーバ台数/サーバ冗長化設計

検証結果より、1.6 万ユーザ規模 ISP において、一番厳しい条件において 100GB/day のログが生成されることがわかった。

abuse 対応を目的としているため、これらのログの取り逃しを避けるように設計しなければならない。そのため、CGN 機器としては、ログサーバを冗長化し複数の宛先へ送ることができるものを選択することが望ましい。また、ログサーバとのコネクションが無い場合には一時的に CGN 本体へ保存できる動作が望ましい。ログサーバからは目的のユーザ情報を迅速に取り出せるようなシステムであることが望ましい。

以上の 9 点の検討により CGN 本体(および周辺システム)の設計はほぼ完了である。CGN は NAT 変換という重要な役割を網内において行うことから、SPOF(Single Point of Failure)となる可能性がある。そのため、2.2.3 対応手順および 2.2.4 機器構成にて CGN 自身において可能な HA 構成を検討し、設置個所を設計する。

2.2.3　　対応手順

2.2.2 項で挙げている推奨対応の対応手順を、特に IPv4 のみのネットワークを IPv4/IPv6 デュアルスタックへと変更することを主眼において具体的にまとめた。

IPv4 アドレスを複数ユーザでシェアする方法は潜在的にいくつもの問題を引き起こす。具体的には、アプリケーションへの影響、事業者の管理の複雑化、セキュリティへの影響などである。これらの問題を回避する永続的な方法は IPv6 化である。しかし、短期的には IPv4 の引き続きの需要によって、CGN などの IPv4 共有手法が必要とされる。IPv6 普及によって、IPv4 共有手法による問題は軽減される。例えば、CGN の性能面に対して総セッションや CPS が影響を与えるが、IPv6 普及によって IPv4 のセッション数は減少する。IPv6 通信が増えるほど、CGN を通る IPv4 通信は減少し、ユーザ一人当たりのセッション数も減少する。また、ユーザで共有するグローバルアドレス数も減少する。結果として、IPv4 アドレスのセッション上限によるアプリケーションへの影響は軽減され、管理コストの問題やセキュリティの問題も軽減されるだろう。この効果は、IPv4 共有技術と IPv6 を同時に提供することで生じるものである。このため、既存の IPv4 のみのネットワークに対して、CGN と同時に IPv6 を提供する方法を推奨対応として、対応手順を記載する。

なお、実際のネットワーク構成については、以下の例よりも複雑であり、事業者個別の事情もある。あくまで例としての構成であるが、基本的な考え方としては広く用いることができる事例となるように注意を払い提示した。

≪CGN のトラフィック分離について≫

既存のネットワークでは IPv4 通信と IPv6 通信がすでにデュアルスタックで混在している場合がある。この場合、CGN を導入するにあたって、CGN が「NAT 機能とは別に、グローバルの IPv4 および IPv6 をルーティング可能であること」によって、ネットワークのアーキテクチャに対する影響が抑えられ、柔軟な設計が可能となる。

NAT 対象としない IPv4 通信(例えば、固定 IP アドレス払い出しを受けているユーザ)の通信が混在している場合、CGN によって選択的に NAT 対象と NAT 対象外を区別し、NAT 対象外のトラフィックについても転送可能であることが望ましい。また、NAT 対象ホストと NAT 対象外ホスト間の折り返し通信についても hairpining 処理が可能であることが必須となる。

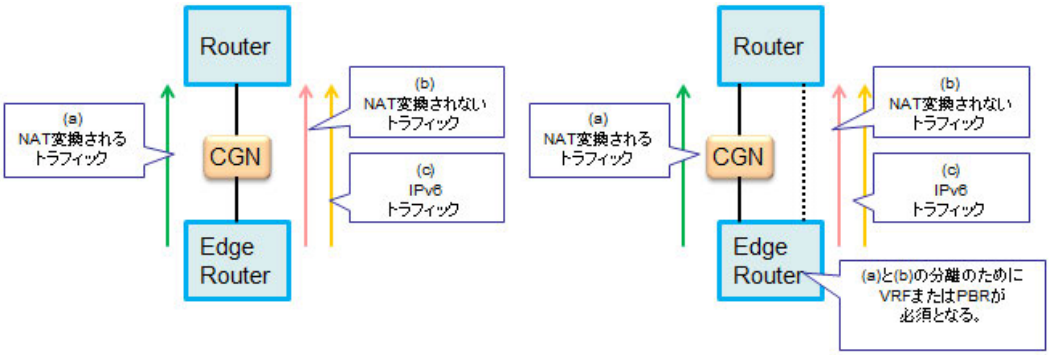


図 2.2-8　CGN のトラフィック分離

ただし、CGN と無関係なトラフィックが CGN を流れてしまうことにより、CGN の性能限界に達し、重要サービスへの影響が懸念されるケースも想定される。そのため、CGN の負荷を軽減するため、IPv6 トラフィックおよび NAT 対象外トラフィックを CGN からバイパスさせる設計も有効である。

NAT 対象と NAT 対象外の IPv4 通信を CGN 以外の機器のルーティングによって分ける場合には、NAT 配下のルータにて VRF(Virtual Routing and Forwarding)や PBR(policy based routing)が必要となる（巻末[4]参照）。

上記の VRF や PBR を実施しているルータよりもさらに下部に折り返しのルーティングが可能なルータがある場合には、NAT 対象ユーザが NAT 対象外ユーザに CGN を通らずに直接通信してしまうため、混在の場合は NAT 対象ユーザの折り返し通信は必ず CGN まで到達するように設計しなければならない点に注意が必要である。ただし、ユーザ間の折り返し通信を許容しない設計の場合にはその限りではない。

≪CGN のルーティング機能について≫

Shared IPv4 アドレス（100.64.0.0/10)を割り当てられたユーザは、必ず CGN を通信とならなければいけないため、CGN は SPOF(Single Point of Failure)となりうる。そのため、HA(High Availability)構成を取るためには、動的ルーティングが可能であることが最低限必要である。しかし、現在の CGN 機器の一部は十分なルーティング機能を持っているとは言い難い。CGN の処理性能が向上しているため、ISP のよりコアなネットワークへの適用ができるようになって来ている。しかし、例えば BGP(Border Gateway Protocol)によるルーティングが実装されていないと、適用箇所が制限されると共に、既存のネットワークへの大きな変更が必要となる。

また、動的ルーティングによる冗長パスへの切り替えが発生したときに、NAT の状態を切り替え先の CGN にハンドオーバーしなければならない。このため、CGN 機器は動的ルーティング機能と HA 機能を組み合わせた実装となっていることが望ましい。

≪DNS の配置について≫

DNS の配置について、検証の結果より、以下の 2 つのパターンを推奨する。

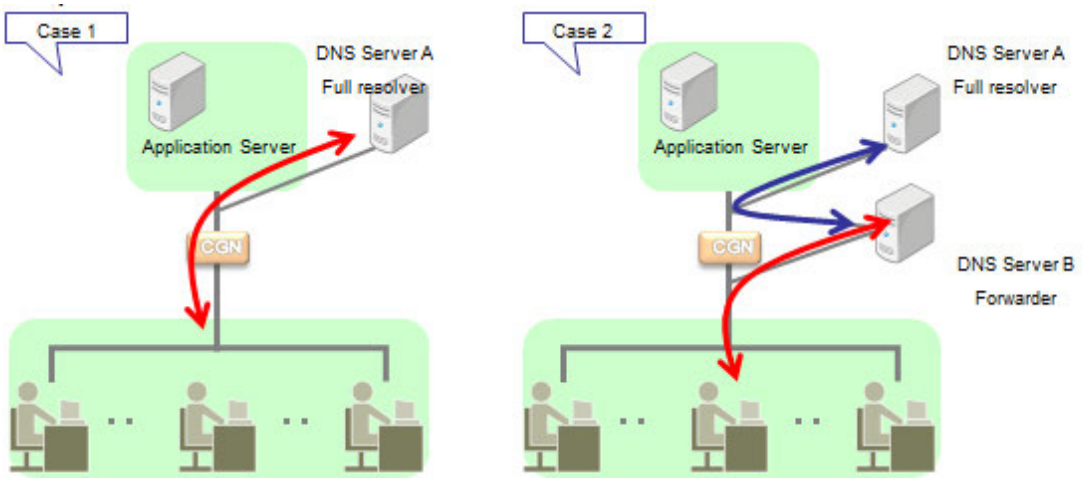


図 2.2-9　DNS サーバの推奨配置

CGN 側で、DNS トラフィックの NAT　time out 値を小さくすることで性能への影響を限定的にすることが示された。しかし、CGN への影響を極力抑えたいという事業者にとっては、DNS クエリが CGN を通らない設計とする方が望ましい場合もあると考える。

以上より、CGN の導入について、表 2.2-4 に示した 2 つのポリシを持った事業者を想定する。

表 2.2-4　想定事業者

	事業者 A	事業者 B
IPv4Global および IPv6 トラフィック	CGN を通過	CGN 以外の機器で分離
動的ルーティング	CGN で可能	CGN 以外の機器で実施
DNS クエリ	bypass しない	bypass する

イメージとしては、事業者 A の使用する CGN のほうがより多機能であると想定する。

≪既存ネットワークについて≫

既存ネットワークを持っている事業者として主に中小規模 ISP～大規模 ISP を想定する。日本のネットワークの特性としてアクセス網が事業分離されているため、ISP はアクセス網との相互接続点(POI: Point of Interface)よりも上位に CGN を設置する。各県に配置された POI からコアネットワークへのトラフィックの集約の仕方として、

(1) エッジ終端型配置

(2) コア終端型配置

の 2 通りがある。図 2.2-10 に示した構成を想定の既存ネットワークとする。

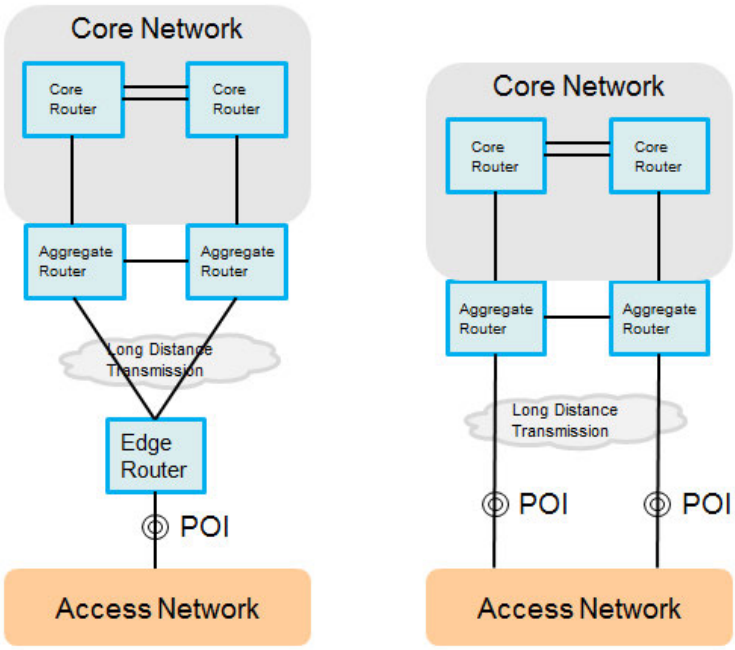


図 2.2-10　想定の既存ネットワーク

(1) エッジ終端型ネットワークへの CGN の導入事例（事業者 A）

事業者 A の場合は、Edge Router を CGN に置き換えることによって既存のトポロジーを変更することなく導入することが可能である。

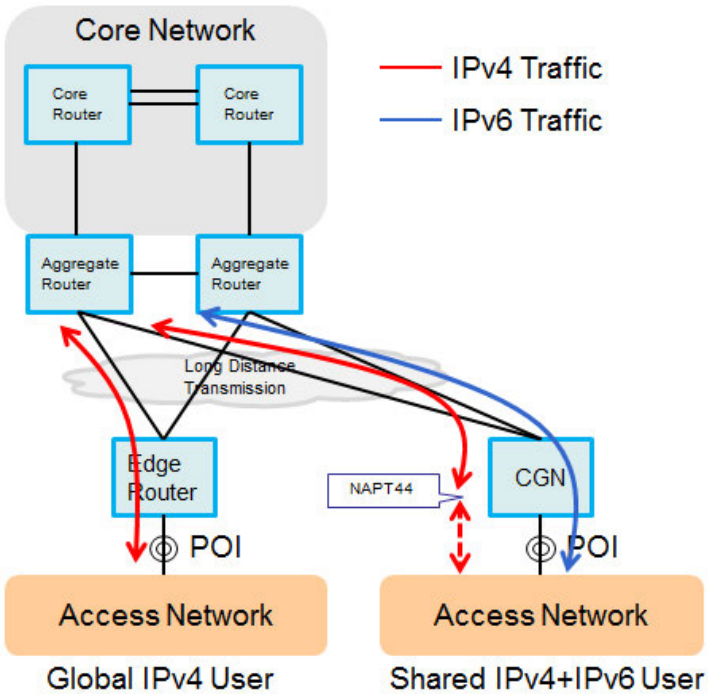


図 2.2-11　エッジ終端型ネットワークへの CGN の導入事例(事業者 A)

CGN の適応区間は 1GigabitEthernet 区間とする。元からシングル構成区間であることから、CGN が HA 構成を取る必要は少ない。CGN で動的ルーティングが可能であることから、アクセス網との接続は Static 接続だけでなく BGP 接続も可能である。本事例では、CGN から上位ネットワークへの接続は IGP による冗長化をしていることから、CGN による IGP の設定および冗長化ができることが条件となる。DNS トラフィックはバイパスされずに CGN を通ることから、DNS クエリに対する NAT テーブルのアサインは time out 値を短くする対策をしていることが望ましい。

以上の特徴を持つ CGN の POI を新規に作ることによって、既存ユーザのスムーズな移行が可能である。ユーザに割り振るアドレスを Shared Address に変更し、アクセス網内で CGN 用 POI への接続に変更することでサービス継続が可能である。上記の図では CGN ユーザのみの POI として書いているが、既存ユーザも CGN でルーティングが可能であれば、既存ユーザと CGN ユーザを同時収容できるため、高価な長距離伝送パスを有効利用することができる。また、IPv6 についても、強いて CGN 上を通過する必要はないが、可能性として図示した。

(2) エッジ終端型ネットワークへの CGN の導入事例（事業者 B）

事業者 B の場合は、CGN のルーティング機能が制限されていることから、POI に直接の接続は不可能である。その替り、Edge Router の機能を利用し、NAT 対象トラフィックと NAT 対象外トラフィックを分離して CGN を接続する。

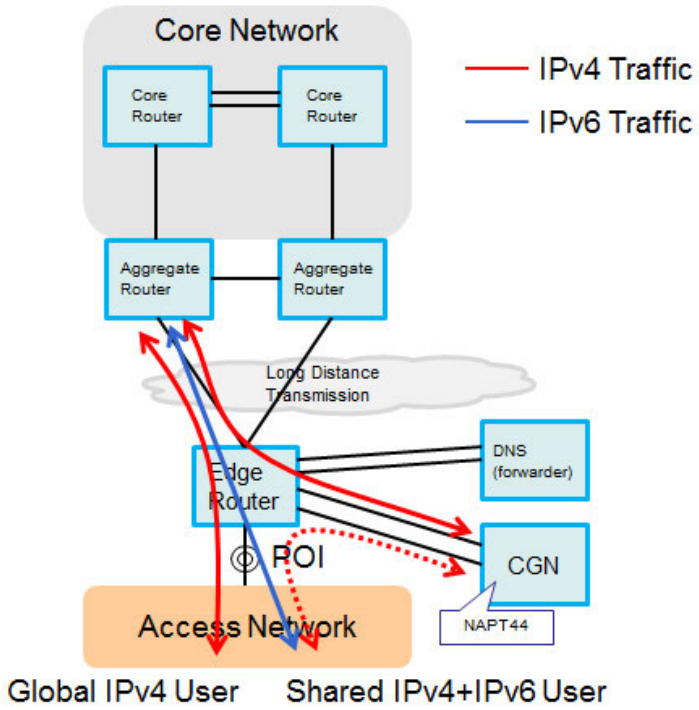


図 2.2-12　エッジ終端型ネットワークへの CGN の導入事例(事業者 B)

トラフィックの分離には、同一の POI 回線に NAT 対象通信と NAT 対象外通信が混ざる場合には Edge Router でソースアドレスルーティングが必要となる。POI 回線がわかれている場合には VRF によって分離可能である。既存のルータが PBR や VRF の機能を有していない場合は、新規ルータへのリプレースが必要となる。

また、DNS について、グローバルと Shared Address の両方のセグメントに接続することによって、CGN を通らない構成とすることが可能である。ただし、DNS サーバがエッジルータごとに必要となるため、CGN ごとに機器の追加が必要となる。また、DNS サーバが地域に分散されることによって管理コストも増大する。

CGN を接続した後は、Shared IPv4 アドレスを配布したユーザについてのみ CGN 向けの通信とすることによって、ユーザを順次収容変更していくことが可能である。グローバル IPv4 トラフィックおよび IPv6 トラフィックと、Shared IPv4 トラフィックが明示的に分かれているため、オペレーション的にわかりやすい構成であるが、PBR を用いた場合にはトラブルシュートが複雑になる傾向がある（PBR 経路はルーティングテーブル上に現れないため)。

(3) コア終端型ネットワークへの CGN の導入事例(事業者 C)

CGN の規模としては。10GigbitEthernet の IF を持ち、10 万ユーザ程度を収容できるものを想定する。

事業者 C の場合、同様に既存のルータの置き換えを検討する。CGN にルーティング機能(特に BGP 機能)があり、なおかつ NAT 対象外のトラフィックのルーティングが可能であれば、図 2.2-13 のような構成が可能である。

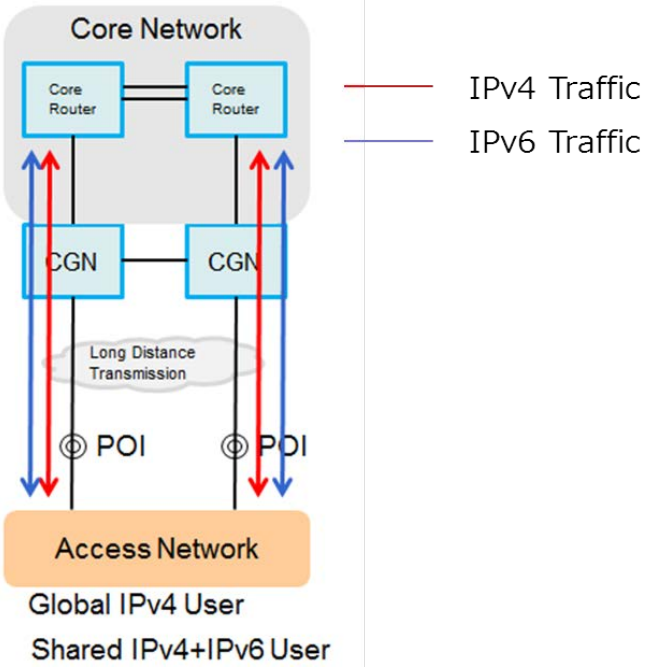


図 2.2-13　コア終端型ネットワークへの CGN の導入-1 事例(事業者 C)

ただし、CGN 対象トラフィックの流れについては注意が必要である。まず、アクセス網からの上りトラフィックについて、0 系/1 系のどちらを流れるかがアクセス網事業者の都合によって操作される点である。この場合 CGN のどちらも通る可能性があるため、Active/Active で運用できる CGN であり、なおかつ NAT テーブルの同期ができなければならない(下りトラフィックが非対称通信である可能性があるため)。HA の実装としてこのような構成が可能な CGN でなければ導入できない。

また、図 2.2-14 のようにエッジの収容ルータの上位に CGN を配置する方法がある。自らのコントロール下においてトラフィックの流れを制御することができるので、CGN を Active/Standby で運用することが可能である。ただし、動的ルーティングによるトラフィックの切り替えによって、Standby 系の CGN に急激のトラフィックが流れ込む際の CGN 性能の担保(通信断時間の見積もり)が必要とされるだろう。また、2 台の CGN 同士が協調(NAT テーブルの同期)ができない場合には、ルーティング側で、いかなる障害のケースに対しても非対称通信とならないように設計する必要がある。

また、CGN が layer3 装置として動作するため、既存のルーティングに影響を与えてしまう。特に、IGP および iBGP の設計に大きな変更が加わる。

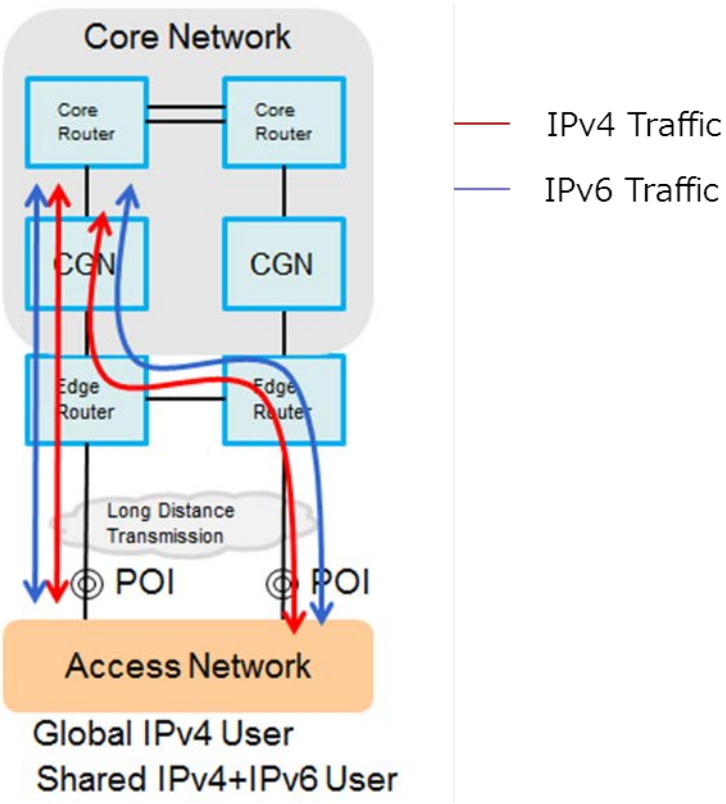


図 2.2-14　コア終端型ネットワークへの CGN の導入-2 事例(事業者 C)

(4) コア終端型ネットワークへの CGN の導入事例(事業者 D)

事業者 D の場合で、既存の NW 構成になるべく影響を与えないような構成を考える。

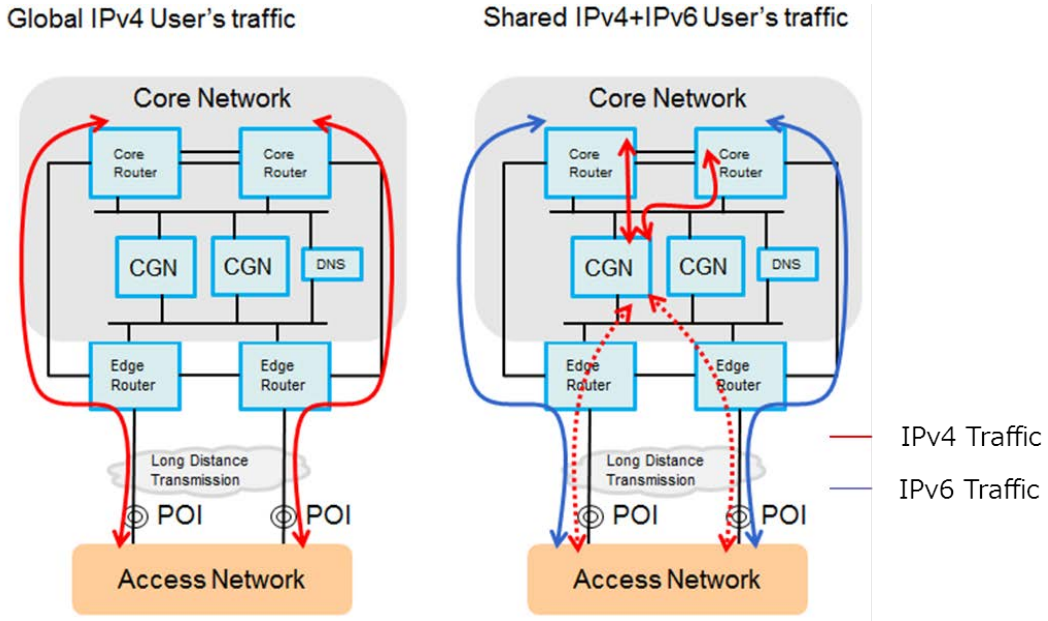


図 2.2-15　コア終端型ネットワークへの CGN の導入-1 事例(事業者 D)

Edge Router と Core Router の間に新たに CGN を通るネットワークを構築する。このネットワークは既存の回線とは別に構築する。CGN 自身が動的ルーティング機能を持たない仮定であることから、動的ルーティングには参加しない。CGN の規模としては 10 万ユーザを超える収容が想定されることから、CGN の HA 構成が必須となる。そのため、ここでは VRRP(Virtual Router Redundancy Protocol)用いて冗長化しているものとする。そのため、L2SW も新たに必要になる。

Shared IPv4 アドレスを配布したユーザについてのみ CGN 向けの通信とすることによって、ユーザを順次収容変更していくことが可能である。

また、コアルータの IF 単価が高価な場合や、エッジルータとコアルータ間の回線が高価な場合には、図 2.2-16 に示した構成によって、既存ネットワーク(Global IPv4)のトラフィックと Shared IPv4 トラフィックおよび IPv6 トラフィックを重畳できる。

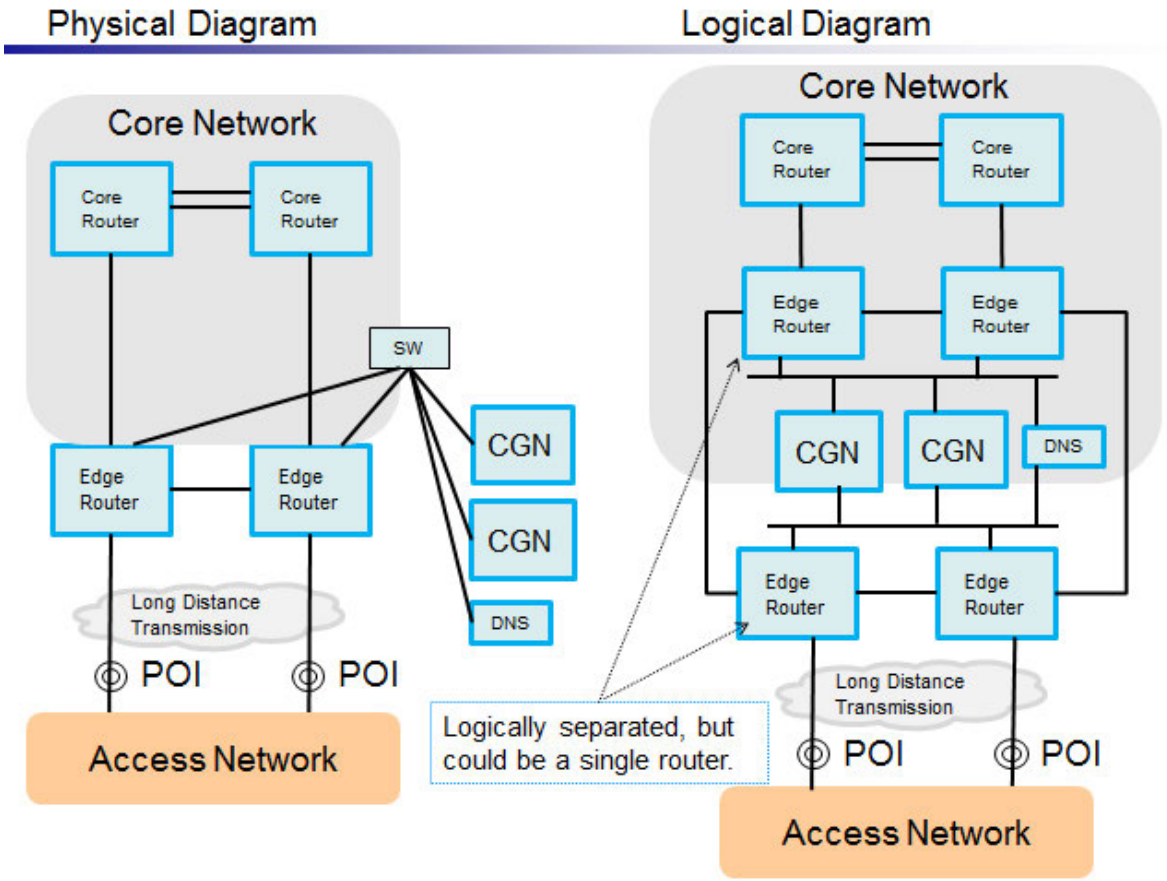


図 2.2-16　コア終端型 NW への CGN の導入-2 事例(事業者 B)

また、これらの構成は、DNS トラフィックのバイパスも可能である。論理ルータを用いたこの構成は、StarBED での検証環境にて実際に構築し、疎通の確認および CGN の切り替えによる HA 動作の確認がされている。

各事業者においては、これらの構成および、前節で示した CGN の設計を参考に、ネットワーク設計が可能である。また、自身の事業における(今後の)Shared IPv4 アドレスユーザ数を見積もることで、適応箇所および CGN の規模を検討することができる。CGN を適用するために、機器の追加や、周囲のルータのリプレースが必要となる可能性はあるが、既存のネットワーク設備を極力利用し、トラフィックの重畳効果を期待することで、ユーザのスムーズな移行が可能である。また、Shared IPv4 アドレスと同時に IPv6 アドレスを利用させることで、CGN への依存を次第に減らしていくことができるネットワーク設計にすることが重要である。なぜなら CGN は、IPv4 枯渇に対する永続的な解決策ではなく、IPv6 化が最終的な解決策だからである。

2.2.4　　機器構成

検証した結果を元に、対象となる ISP や ASP などの規模に合わせた最適な機器構成をまとめ、具体的な例と機器設定、運用方法を含めた例を示した。

（1） 小規模（顧客：1 万人）

顧客規模から考えて、小規模な事業者として地域密着した ISP を想定する。

(ア) 最適な機器構成（推奨機器、配置等）

規模が小さいため、顧客収容ルータ/コアルータ/トランジットルータからなるシンプルな構成であると考えられる。ルータ数が少なくトラフィックが集中しているので、収容ルータを CGN に置き換える構成を推奨構成とする。網内には顧客にサービスを提供しているサーバ群(メールサーバ・DNS サーバなど)があり、網内を全て Shared Address に変更することは現実的ではないため、CGN はトランジット側ではなく、可能な限りエッジに近いところに配置するものとする。ただし、複数回線を集約する役目も同時に持つため、収容 IF を十分持つものを選定することが望ましい。

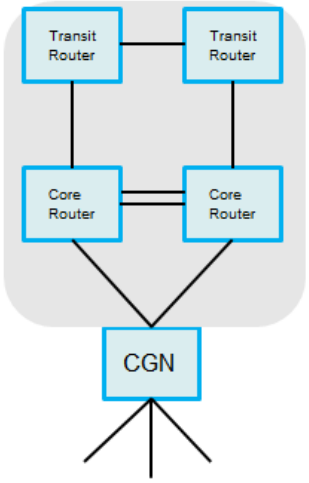


図 2.2-17　最適な機器構成（小規模）

推奨機器: AX2500～（A10 ネットワークス）, ASR1001～(Cisco), SRX650～(Juniper) など。

(イ) 機器設定

各設計項目について、規模に合わせて以下のような設計例で config を示す。

表 2.2-5　Config 例（小規模）

設計項目	設計検討	config 例(A10)
(1) プールアドレス設計	－Active ユーザ率(%) = 25% －1 ユーザ当たりのセッション数(session/ユーザ) = 400 とすると、10000 ユーザに対して最大同時 100 万セッション程度と予想される。 1 pool address あたり 32000 ポートの利用を想定すると、32 アドレス程度用意すればよいことになる。	ip nat pool [poolname] 133.4.0.0 133.4.0.31 netmask /27　lsn
(2) Shared Address 設計	100.64.0.0/10 空間を利用し、ユーザに配布する。	class-list [classname] 100.64.0.0 /10 lsn-lid 1
(3) ポート割り当て手法設計	アドレスの追加取得が難しいため、アドレス圧縮効率の高い動的割り当てを採用する。ユーザ数がそこまで多くないので、NAT ログを全て取得できるサーバを用意することが可能とする。 ユーザごとに利用可能なポート上限数を以下のように設定する。 TCP = 1000port UDP = 1000port ICMP = 100identifier	lsn-lid 1 source-nat-pool [poolname] user-quota udp 1000 user-quota tcp 1000 user-quota icmp 100
(4) time out 値設計	以下の設定とする。 TCP time out= 300(sec) UDP time out = 300(sec) ICMP time out = 2(sec) TCP SYN time out = 60(sec) DNS time out = 3(sec) Full Cone time out = 2(min)	(以下は default の設定) ip nat translation tcp-timeout 300 ip nat translation udp-timeout 300 ip nat translation icmp-timeout 300 ip nat translation syn-timeout 300 ip nat translation service-timeout udp 53 fast ip nat translation service-timeout tcp 53 fast ip nat lsn stun-timeout 2
(5) EIM/EIF(Full Cone)設計	全てのポートで Full Cone 動作であるとする。	ip nat lsn full-cone enable
(6) hairpining	hairpin 通信が可能であるとする。	(default)

設計項目	設計検討	config 例(A10)
設計		
(7) ALG 設計	可能な限り全ての ALG を ON にする。	ip nat lsn alg esp enable ip nat lsn alg ftp enable ip nat lsn alg pptp enable ip nat lsn alg rstp enable ip nat lsn alg sip enable ip nat lsn alg tftp enable
(8) ログ設計	以下の項目を取得する(abuse 対応のため通信先情報も取得することとする。) - 送信元 IP アドレス及びポート - NAT 変換後 送信元 IP アドレス及びポート - 送信先 IP アドレス及びポート - Timestamp log format は可読性のために、ascii format で取得する。	ip nat template logging [templatename] include-destination format default
(9) ログサーバ台数/サーバ冗長化設計	syslog server にて NAT ログを取得する。2 台のサーバで分散してログを取得する。	slb server [name01] [IPaddress] port 514 udp slb server [name02] [IPaddress] port 514 udp slb service-group [groupname] udp member [name01]:514 member [name02]:514

(ウ) 運用方法

NAT 対象ユーザへ徐々に切り替えを行う。

セッション数が徐々に増えていくため、time out 値・セッション上限・プールアドレス数は、ユーザ状況に合わせて変更が可能である。

NAT ログ取得量が徐々に増えていくため、ログサーバのログ量の予測をしながら調整が可能である。

帯域に加えて、NAT セッション数について監視項目とし、安定運用を目指す。abuse 申告があった場合には、自社の認証サーバのログと NAT ログを突合し、エンドユーザを特定する。

（2） 中規模（顧客：10 万人）

顧客規模から考えて、全国面を持つ中規模の ISP を想定する。

(ア) 最適な機器構成

各エリアから集約されるトラフィックを少数セットの CGN で集約できるようにする。また、HA 構成を必須とする。規模の大きな構成となるため、性能の高い CGN が要求される。DNS について、CGN を通らない構成とする。ログの取得について、規模が大きいので動的割り当ては現実的ではないため、ポートを固定的に割り当てる手法を用いることとする。

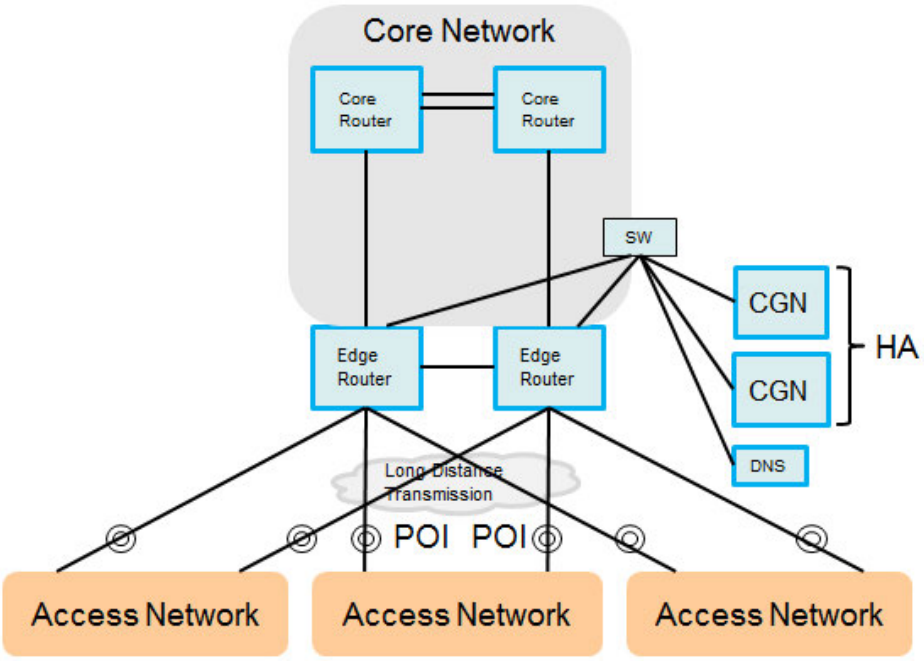


図 2.2-18 最適な機器構成（中規模）

推奨機器: AX5200～ (A10 ネットワークス), CRS1～(Cisco), SRX3000～(Juniper) など。

(イ) 機器設定

表 2.2-6 Config 例（中規模）

設計項目	設計検討	config 例(A10)
(1) プールアドレス設計	固定割り当てのため、1 ユーザあたり固定的にポートを割り当てる。 2 の乗数となるように整理し、131072(2^17)ユーザに対し、1024(2^10)ポートを割り当てる。1 プールアドレスあたり 32768(2^15)ポート利用とすると、プールアドレスとして、2^27/2^15=2^12(4096)アドレス用意すれ	fixed-nat inside 100.64.0.0 100.65.255.255 netmask /15 nat 133.4.32.0 133.4.47.255 netmask /20 usable-nat-ports 32768 65535 ports-per-user 1024 ha-group-id 1

設計項目	設計検討	config 例(A10)
	ばよい。	
(2) Shared Address 設計	100.64.0.0/10 空間内の、10.64.0.0/15 アドレス(131072 ユーザ分)を利用する。	(上記)
(3) ポート割り当て手法設計	上記のように固定割り当てとする。 ユーザごとに利用可能なポート上限数は 1024 ポートとなる。	(上記)
(4) time out 値設計	以下の設定とする。 TCP time out = 300(sec) UDP time out = 300(sec) ICMP time out = 2(sec) TCP SYN time out = 60(sec) DNS time out = 3(sec) Full Cone time out = 2(min)	(以下は default の設定) ip nat translation tcp-timeout 300 ip nat translation udp-timeout 300 ip nat translation icmp-timeout 300 ip nat translation syn-timeout 300 ip nat translation service-timeout udp 53 fast ip nat translation service-timeout tcp 53 fast ip nat lsn stun-timeout 2
(5) EIM/EIF(Full Cone)設計	ポートの利用を削減するために、1024 以降のポートのみで Full Cone 動作であるとする。	ip nat lsn full-cone default
(6) hairpining 設計	hairpin 通信が可能であるとする。	(default)
(7) ALG 設計	可能な限り全ての ALG を ON にする。	ip nat lsn alg esp enable ip nat lsn alg ftp enable ip nat lsn alg pptp enable ip nat lsn alg rstp enable ip nat lsn alg sip enable ip nat lsn alg tftp enable
(8) ログ設計	Fixed-nat の port range 割り当てログのみ取得する。セッションごとのログはログ量削減のために取得しない。	ip nat template logging [templatename] log fixed-nat-all log fixed-nat-user-ports

設計項目	設計検討	config 例(A10)
(9) ログサーバ台数/サーバ冗長化設計	syslog server にて NAT ログを取得する。2 台のサーバで分散してログを取得する。	slb server [name01] [IPaddress] port 514 udp slb server [name02] [IPaddress] port 514 udp slb service-group [groupname] udp member [name01]:514 member [name02]:514
HA 設定	VIP を用いた HA 構成とする。	!AX-1 ha id 1 ha group 1 priority 100 ha interface ethernet * ha conn-mirror ip 10.200.1.2 ha preemption-enable floating-ip 133.4.16.4 ha-group 1 floating-ip 100.100.0.4 ha-group 1 !AX-2 ha id 2 ha group 1 priority 101 ha interface ethernet * ha conn-mirror ip 10.200.1.1 ha preemption-enable floating-ip 133.4.16.4 ha-group 1 floating-ip 100.100.0.4 ha-group 1

(ウ) 運用方法

エッジルータで CGN セグメントへ NAT 対象トラフィックを分離する。これによって、徐々に切り替えが可能である。abuse 申告に対しては、IP アドレスとポートを合わせて連絡が来たものに対して、ポートレンジ割り当てのログを見ることでユーザの同定が可能である。HA 構成では、NAT テーブルの同期を常に行い、ルーティング切り替え発生の際にも、断無く継続できる構成となるようにする。

（3） 大規模（顧客：100 万人）

顧客規模から考えて、全国面を持つ大規模の ISP を想定する。

(ア) 最適な機器構成

CGN 機器の現状の性能面を鑑みて、前述の中規模ユーザ程度のエリアに分割して、エリアごとに CGN 機器を導入する形が理想である。

(イ) 機器設定

小規模 ISP・中規模 ISP の場合の組み合わせとなるため、省略する。

(ウ) 運用方法

エリアごとの CGN 導入になるため、サービスの全国展開は時間をかけたものになると想定される。CGN および DNS サーバが複数分散するため、統合的な運用方法の構築が重要である。機器コストに対して、運用コスト・保守コストの割合が上昇する。abuse 対応でデータベースの突合する場合には、効率よく探索できるシステム設計をすることが重要である。

最後に、大規模を想定した最適な機器構成、また機器設定例をそれぞれ図 2.2-19、および表 2.2-7 から表 2.2-13 に示す。

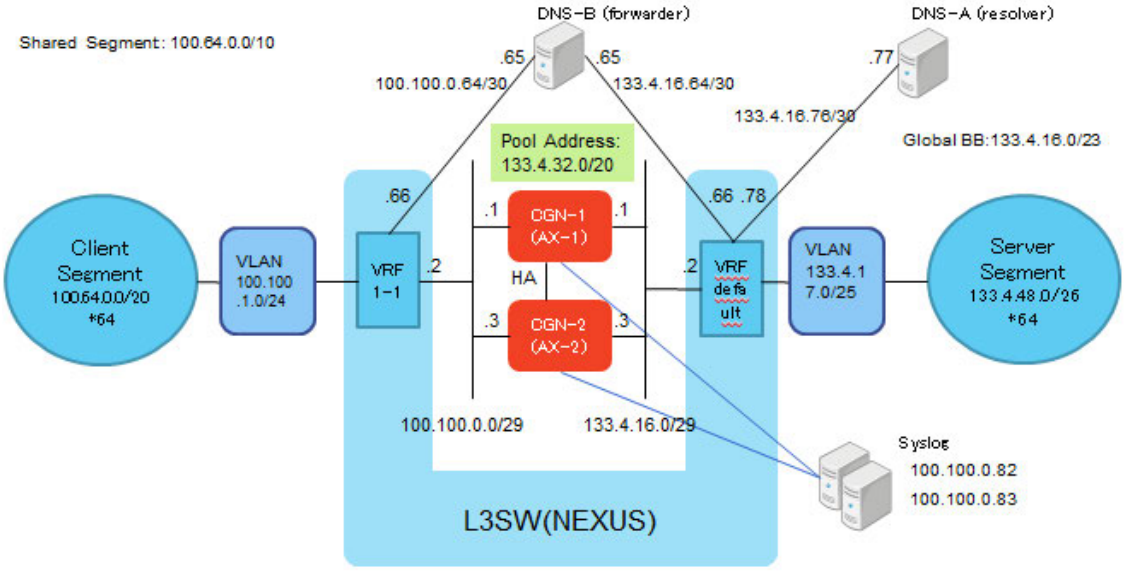


図 2.2-19　最適な機器構成（大規模）

表 2.2-7　AS3000-1(Active) config 例

```
ha id 1
hostname sp-ax3000-1
!
clock timezone Asia/Tokyo
!
!
system resource-usage l4-session-count 67108864
system resource-usage nat-pool-addr-count 4000
!
!
!
vlan 2801
 tagged ethernet 19 to 20
 router-interface ve 2801
 name "SHARED"
!
vlan 2806
 tagged ethernet 19 to 20
 router-interface ve 2806
 name "GLOBAL"
!
vlan 2840
 tagged ethernet 2 to 3
 router-interface ve 2840
 name "STORAGE"
!
vlan 2850
 untagged ethernet 4
 router-interface ve 2850
 name "HA_LINK"
!
class-list starclass
 100.64.0.0 /10 lsn-lid 1
!
interface management
```

```
 ip address 10.10.0.103 255.255.0.0
 ip control-apps-use-mgmt-port
!
interface ethernet 2
 lacp trunk 3 mode active
!
interface ethernet 3
 lacp trunk 3 mode active
!
interface ethernet 19
 lacp trunk 1 mode active
!
interface ethernet 20
 lacp trunk 1 mode active
!
interface ve 2801
 ip address 100.100.0.1 255.255.255.248
 ip nat inside
 !
interface ve 2806
 ip address 133.4.16.1 255.255.255.248
 ip nat outside
!
interface ve 2840
 ip address 100.100.0.81 255.255.255.248
!
interface ve 2850
 ip address 10.200.1.1 255.255.255.252
!
ip route 100.64.0.0 /10 100.100.0.2
ip route 133.4.0.0 /16 133.4.16.2
ip route 0.0.0.0 /0 133.4.16.2
!
!
ha group 1 priority 100
ha interface ethernet 4
```

```
ha conn-mirror ip 10.200.1.2
!
ha preemption-enable
!
floating-ip 133.4.16.4 ha-group 1
floating-ip 100.100.0.4 ha-group 1
!
!
!
!
ip nat pool starpool01 133.4.32.0 133.4.33.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool02 133.4.34.0 133.4.35.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool03 133.4.36.0 133.4.37.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool04 133.4.38.0 133.4.39.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool05 133.4.40.0 133.4.41.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool06 133.4.42.0 133.4.43.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool07 133.4.44.0 133.4.45.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool08 133.4.46.0 133.4.47.159 netmask /23   ha-group-id 1 lsn
!
ip nat pool-group starpools ha-group-id 1
  member starpool01
  member starpool02
  member starpool03
  member starpool04
  member starpool05
  member starpool06
  member starpool07
  member starpool08
!
!
!
!
!
ip nat inside source class-list starclass
!
!
```

```
ip nat template logging starlog01
ip nat template logging startemplate01
!
!
lsn-lid 1
 source-nat-pool starpools
!
!
!
!
slb server starsyslog03 100.100.0.83
    no health-check
    port 514    udp
          no health-check
!
slb server starsyslog02 100.100.0.82
    no health-check
    port 514    udp
          no health-check
!
slb service-group starsyslogs udp
      member starsyslog02:514
      member starsyslog03:514
!
!
!
!
ip nat template logging startemplate01
 include-destination
 service-group starsyslogs
!
!
ip nat lsn logging default-template startemplate01
snmp-server enable
snmp-server community read public remote default
!
```

```
!
!
enable-core
!
terminal idle-timeout 0
!
end
```

表 2.2-8　AX3000-2(Standby) config 例

```
ha id 2
hostname sp-ax3000-2
!
clock timezone Asia/Tokyo
!
!
system resource-usage l4-session-count 67108864
system resource-usage nat-pool-addr-count 4000
!
!
!
vlan 2801
 tagged ethernet 19 to 20
 router-interface ve 2801
 name "SHARED"
!
vlan 2806
 tagged ethernet 19 to 20
 router-interface ve 2806
 name "GLOBAL"
!
vlan 2840
 tagged ethernet 2 to 3
 router-interface ve 2840
 name "STORAGE"
```

```
!
vlan 2850
 untagged ethernet 4
 router-interface ve 2850
 name "HA_LINK"
!
class-list starclass
 100.64.0.0 /10 lsn-lid 1
!
interface management
 ip address 10.10.0.104 255.255.0.0
 ip control-apps-use-mgmt-port
!
interface ethernet 2
 lacp trunk 3 mode active
!
interface ethernet 3
 lacp trunk 3 mode active
!
interface ethernet 19
 lacp trunk 1 mode active
!
interface ethernet 20
 lacp trunk 1 mode active
!
interface ve 2801
 ip address 100.100.0.3 255.255.255.248
 ip nat inside
 !
interface ve 2806
 ip address 133.4.16.3 255.255.255.248
 ip nat outside
!
interface ve 2840
 ip address 100.100.0.84 255.255.255.248
!
```

```
interface ve 2850
 ip address 10.200.1.2 255.255.255.252
!
ip route 100.64.0.0 /10 100.100.0.2
ip route 133.4.0.0 /16 133.4.16.2
ip route 0.0.0.0 /0 133.4.16.2
!
!
ha group 1 priority 99
ha interface ethernet 4
ha conn-mirror ip 10.200.1.1
!
ha preemption-enable
!
floating-ip 133.4.16.4 ha-group 1
floating-ip 100.100.0.4 ha-group 1
!
!
!
!
ip nat pool starpool01 133.4.32.0 133.4.33.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool02 133.4.34.0 133.4.35.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool03 133.4.36.0 133.4.37.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool04 133.4.38.0 133.4.39.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool05 133.4.40.0 133.4.41.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool06 133.4.42.0 133.4.43.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool07 133.4.44.0 133.4.45.255 netmask /23   ha-group-id 1 lsn
ip nat pool starpool08 133.4.46.0 133.4.47.159 netmask /23   ha-group-id 1 lsn
!
ip nat pool-group starpools ha-group-id 1
 member starpool01
 member starpool02
 member starpool03
 member starpool04
 member starpool05
 member starpool06
```

```
 member starpool07
 member starpool08
!
!
!
!
!
!
ip nat inside source class-list starclass
!
!
ip nat template logging starlog01
ip nat template logging startemplate01
!
!
lsn-lid 1
 source-nat-pool starpools
!
!
!
!
slb server starsyslog03 100.100.0.83
    no health-check
    port 514   udp
         no health-check
!
slb server starsyslog02 100.100.0.82
    no health-check
    port 514   udp
         no health-check
!
slb service-group starsyslogs udp
      member starsyslog02:514
      member starsyslog03:514
!
!
```

```
!
ip nat template logging startemplate01
 facility local1
 include-destination
 service-group starsyslogs
!
!
ip nat lsn logging default-template startemplate01
snmp-server enable
snmp-server community read public remote default
!
!
!
enable-core
!
terminal idle-timeout 0
!
end
```

表 2.2-9　L3SW(NEXUS) config 例

```
version 6.0(2)

vrf context management
vrf context vrf1-1
   ip route 0.0.0.0/0 100.100.0.4
   ip route 100.64.0.0/10 Null0
   ip route 100.64.0.0/20 100.100.1.1
   ip route 100.64.16.0/20 100.100.1.2
   ip route 100.64.32.0/20 100.100.1.3
   ip route 100.64.48.0/20 100.100.1.4
   ip route 100.64.64.0/20 100.100.1.5
   ip route 100.64.80.0/20 100.100.1.6
   ip route 100.64.96.0/20 100.100.1.7
   ip route 100.64.112.0/20 100.100.1.8
   ip route 100.64.128.0/20 100.100.1.9
```

```
ip route 100.64.144.0/20 100.100.1.10
ip route 100.64.160.0/20 100.100.1.11
ip route 100.64.176.0/20 100.100.1.12
ip route 100.64.192.0/20 100.100.1.13
ip route 100.64.208.0/20 100.100.1.14
ip route 100.64.224.0/20 100.100.1.15
ip route 100.64.240.0/20 100.100.1.16
ip route 100.65.0.0/20 100.100.1.17
ip route 100.65.16.0/20 100.100.1.18
ip route 100.65.32.0/20 100.100.1.19
ip route 100.65.48.0/20 100.100.1.20
ip route 100.65.64.0/20 100.100.1.21
ip route 100.65.80.0/20 100.100.1.22
ip route 100.65.96.0/20 100.100.1.23
ip route 100.65.112.0/20 100.100.1.24
ip route 100.65.128.0/20 100.100.1.25
ip route 100.65.144.0/20 100.100.1.26
ip route 100.65.160.0/20 100.100.1.27
ip route 100.65.176.0/20 100.100.1.28
ip route 100.65.192.0/20 100.100.1.29
ip route 100.65.208.0/20 100.100.1.30
ip route 100.65.224.0/20 100.100.1.31
ip route 100.65.240.0/20 100.100.1.32
ip route 100.66.0.0/20 100.100.1.33
ip route 100.66.16.0/20 100.100.1.34
ip route 100.66.32.0/20 100.100.1.35
ip route 100.66.48.0/20 100.100.1.36
ip route 100.66.64.0/20 100.100.1.37
ip route 100.66.80.0/20 100.100.1.38
ip route 100.66.96.0/20 100.100.1.39
ip route 100.66.112.0/20 100.100.1.40
ip route 100.66.128.0/20 100.100.1.41
ip route 100.66.144.0/20 100.100.1.42
ip route 100.66.160.0/20 100.100.1.43
ip route 100.66.176.0/20 100.100.1.44
ip route 100.66.192.0/20 100.100.1.45
```

```
   ip route 100.66.208.0/20 100.100.1.46
   ip route 100.66.224.0/20 100.100.1.47
   ip route 100.66.240.0/20 100.100.1.48
   ip route 100.67.0.0/20 100.100.1.49
   ip route 100.67.16.0/20 100.100.1.50
   ip route 100.67.32.0/20 100.100.1.51
   ip route 100.67.48.0/20 100.100.1.52
   ip route 100.67.64.0/20 100.100.1.53
   ip route 100.67.80.0/20 100.100.1.54
   ip route 100.67.96.0/20 100.100.1.55
   ip route 100.67.112.0/20 100.100.1.56
   ip route 100.67.128.0/20 100.100.1.57
   ip route 100.67.144.0/20 100.100.1.58
   ip route 100.67.160.0/20 100.100.1.59
   ip route 100.67.176.0/20 100.100.1.60
   ip route 100.67.192.0/20 100.100.1.61
   ip route 100.67.208.0/20 100.100.1.62
   ip route 100.67.224.0/20 100.100.1.63
   ip route 100.67.240.0/20 100.100.1.64
vlan 1
vlan 2801
   name SP-StarBED-2801
vlan 2806
   name SP-StarBED-2806
vlan 2821
   name SP-StarBED-2821
vlan 2843
   name SP-P2P-DNS-planB-shared
vlan 2844
   name SP-P2P-DNS-planB-global
vlan 2845
   name SP-P2P-DNS-planA
vlan 3781
   name SP-P2P-TYOG1-KMQA2

interface Vlan2801
```

```
   description To:CGN-1
   no shutdown
   vrf member vrf1-1
   no ip redirects
   ip address 100.100.0.2/29
   ip unreachables

interface Vlan2806
   description To:CGN-1
   no shutdown
   no ip redirects
   ip address 133.4.16.2/29
   ip unreachables
   ip ospf passive-interface
   ip router ospf 55384 area 0.0.0.0

interface Vlan2821
   no shutdown
   no ip redirects
   ip address 133.4.17.126/25
   ip unreachables
   ip ospf passive-interface
   ip router ospf 55384 area 0.0.0.0

interface Vlan2843
   description To:DNS-planB-shared
   no shutdown
   vrf member vrf1-1
   no ip redirects
   ip address 100.100.0.66/30
   ip unreachables

interface Vlan2844
   description To:DNS-planB-global
   no shutdown
   no ip redirects
```

```
   ip address 133.4.16.66/30
   ip unreachables

interface Vlan2845
   description To:DNS-planA
   no shutdown
   no ip redirects
   ip address 133.4.16.78/30
   ip unreachables

interface Vlan3781
   description To:TYO-RT-G01
   no shutdown
   mtu 9000
   ip access-group INCOMING-ACL in
   no ip redirects
   ip address 133.4.0.46/30
   ip unreachables
   ipv6 address use-link-local-only
   no ipv6 redirects
   ipv6 unreachables
   ip ospf cost 100
   ip router ospf 55384 area 0.0.0.0
   ospfv3 cost 100
   ipv6 router ospfv3 55384 area 0.0.0.0

interface port-channel1
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 2801-2810,2821-2825
   switchport trunk allowed vlan add 2843-2845,3781
   logging event port link-status
   logging event port trunk-status



interface Ethernet4/25
```

```
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 2801-2810,2821-2825
   switchport trunk allowed vlan add 2843-2845,3781
   logging event port link-status
   logging event port trunk-status
   channel-group 1 mode active
   no shutdown

interface Ethernet4/27
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 2801-2810,2821-2825
   switchport trunk allowed vlan add 2843-2845,3781
   logging event port link-status
   logging event port trunk-status
   channel-group 1 mode active
   no shutdown

interface Ethernet4/29
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 2801-2810,2821-2825
   switchport trunk allowed vlan add 2843-2845,3781
   logging event port link-status
   logging event port trunk-status
   channel-group 1 mode active
   no shutdown

interface Ethernet4/31
   switchport
   switchport mode trunk
   switchport trunk allowed vlan 2801-2810,2821-2825
   switchport trunk allowed vlan add 2843-2845,3781
   logging event port link-status
   logging event port trunk-status
```

```
   channel-group 1 mode active
   no shutdown

interface loopback0
   ip address 133.4.0.4/32
   ip unreachables
   ipv6 address 2001:df0:2ee::4/128
   ipv6 unreachables
   ip ospf advertise-subnet
   ip router ospf 55384 area 0.0.0.0
   ipv6 router ospfv3 55384 area 0.0.0.0

router ospf 55384
   router-id 133.4.0.4
   redistribute static route-map redist-static-to-ospf
router ospfv3 55384
   router-id 133.4.0.4
   graceful-restart

ip route 133.4.32.0/20 133.4.16.4
ip route 133.4.48.0/26 133.4.17.1
ip route 133.4.48.64/26 133.4.17.2
ip route 133.4.48.128/26 133.4.17.3
ip route 133.4.48.192/26 133.4.17.4
ip route 133.4.49.0/26 133.4.17.5
ip route 133.4.49.64/26 133.4.17.6
ip route 133.4.49.128/26 133.4.17.7
ip route 133.4.49.192/26 133.4.17.8
ip route 133.4.50.0/26 133.4.17.9
ip route 133.4.50.64/26 133.4.17.10
ip route 133.4.50.128/26 133.4.17.11
ip route 133.4.50.192/26 133.4.17.12
ip route 133.4.51.0/26 133.4.17.13
ip route 133.4.51.64/26 133.4.17.14
ip route 133.4.51.128/26 133.4.17.15
ip route 133.4.51.192/26 133.4.17.16
```

```
ip route 133.4.52.0/26 133.4.17.17
ip route 133.4.52.64/26 133.4.17.18
ip route 133.4.52.128/26 133.4.17.19
ip route 133.4.52.192/26 133.4.17.20
ip route 133.4.53.0/26 133.4.17.21
ip route 133.4.53.64/26 133.4.17.22
ip route 133.4.53.128/26 133.4.17.23
ip route 133.4.53.192/26 133.4.17.24
ip route 133.4.54.0/26 133.4.17.25
ip route 133.4.54.64/26 133.4.17.26
ip route 133.4.54.128/26 133.4.17.27
ip route 133.4.54.192/26 133.4.17.28
ip route 133.4.55.0/26 133.4.17.29
ip route 133.4.55.64/26 133.4.17.30
ip route 133.4.55.128/26 133.4.17.31
ip route 133.4.55.192/26 133.4.17.32
ip route 133.4.56.0/26 133.4.17.33
ip route 133.4.56.64/26 133.4.17.34
ip route 133.4.56.128/26 133.4.17.35
ip route 133.4.56.192/26 133.4.17.36
ip route 133.4.57.0/26 133.4.17.37
ip route 133.4.57.64/26 133.4.17.38
ip route 133.4.57.128/26 133.4.17.39
ip route 133.4.57.192/26 133.4.17.40
ip route 133.4.58.0/26 133.4.17.41
ip route 133.4.58.64/26 133.4.17.42
ip route 133.4.58.128/26 133.4.17.43
ip route 133.4.58.192/26 133.4.17.44
ip route 133.4.59.0/26 133.4.17.45
ip route 133.4.59.64/26 133.4.17.46
ip route 133.4.59.128/26 133.4.17.47
ip route 133.4.59.192/26 133.4.17.48
ip route 133.4.60.0/26 133.4.17.49
ip route 133.4.60.64/26 133.4.17.50
ip route 133.4.60.128/26 133.4.17.51
ip route 133.4.60.192/26 133.4.17.52
```

```
ip route 133.4.61.0/26 133.4.17.53
ip route 133.4.61.64/26 133.4.17.54
ip route 133.4.61.128/26 133.4.17.55
ip route 133.4.61.192/26 133.4.17.56
ip route 133.4.62.0/26 133.4.17.57
ip route 133.4.62.64/26 133.4.17.58
ip route 133.4.62.128/26 133.4.17.59
ip route 133.4.62.192/26 133.4.17.60
ip route 133.4.63.0/26 133.4.17.61
ip route 133.4.63.64/26 133.4.17.62
ip route 133.4.63.128/26 133.4.17.63
ip route 133.4.63.192/26 133.4.17.64
```

表 2.2-10　Syslog server /etc/rsyslog.d/ax.conf

```
# for AX3000 syslog
#   AX3000's default is:
#     minimum severity level = 7(debugging)
#     facility = local0
local0.*            /mnt/sdb/log/ax.log
local1.*            /mnt/sdb/log/ax2.log
```

表 2.2-11　DNS server (forwarder) /etc/unbound/unbound.conf

```
# Unbound configuration file for Debian.
#
# See the unbound.conf(5) man page.
#
# See /usr/share/doc/unbound/examples/unbound.conf for a commented
# reference config file.

server:
        # The following line will configure unbound to perform cryptographic
        # DNSSEC validation using the root trust anchor.
        verbosity: 1
        #auto-trust-anchor-file: "/var/lib/unbound/root.key"
        do-ip4: yes
        do-ip6: no
```

```
    do-tcp: yes
    do-udp: yes

    num-threads: 1

    access-control: 127.0.0.0/8 allow
    access-control: 100.64.0.0/10 allow
    access-control: 133.4.0.0/18 allow

    hide-identity: yes
    hide-version: yes
    interface: 100.100.0.65
    interface: 127.0.0.1


forward-zone:
        name: "orz."
        forward-addr: 133.4.16.77

forward-zone:
        name: "4.133.in-addr.arpa."
        forward-addr: 133.4.16.77

forward-zone:
name: "."
forward-addr: 133.4.16.77
```

表 2.2-12　DNS server (resolver) /etc/bind/named.conf.orz

```
// prime the server with knowledge of the root servers
zone "orz" {
        type master;
        file "/etc/bind/master/orz.zone";
};

zone "48.4.133.in-addr.arpa" {
        type master;
```

```
        file "/etc/bind/master/48.4.133.zone";
};

zone "49.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/49.4.133.zone";
};

zone "50.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/50.4.133.zone";
};

zone "51.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/51.4.133.zone";
};

zone "52.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/52.4.133.zone";
};

zone "53.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/53.4.133.zone";
};

zone "54.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/54.4.133.zone";
};

zone "55.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/55.4.133.zone";
```

```
};

zone "56.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/56.4.133.zone";
};

zone "57.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/57.4.133.zone";
};

zone "58.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/58.4.133.zone";
};

zone "59.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/59.4.133.zone";
};

zone "60.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/60.4.133.zone";
};

zone "61.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/61.4.133.zone";
};

zone "62.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/62.4.133.zone";
};
```

```
zone "63.4.133.in-addr.arpa" {
        type master;
        file "/etc/bind/master/63.4.133.zone";
};
```

表 2.2-13　DNS server (resolver) /etc/bind/master/orz.zone　(逆引き file は省略)

```
$TTL    86400
@       IN      SOA     ns.orz. ns.orz. (
                        20130212
                        3600
                        900
                        3600000
                        86400
                )
                NS      ns.orz.

ns              A       10.10.0.211

$GENERATE       0-255   133.4.48.$      A       133.4.48.$
$GENERATE       0-255   133.4.49.$      A       133.4.49.$
$GENERATE       0-255   133.4.50.$      A       133.4.50.$
$GENERATE       0-255   133.4.51.$      A       133.4.51.$
$GENERATE       0-255   133.4.52.$      A       133.4.52.$
$GENERATE       0-255   133.4.53.$      A       133.4.53.$
$GENERATE       0-255   133.4.54.$      A       133.4.54.$
$GENERATE       0-255   133.4.55.$      A       133.4.55.$
$GENERATE       0-255   133.4.56.$      A       133.4.56.$
$GENERATE       0-255   133.4.57.$      A       133.4.57.$
$GENERATE       0-255   133.4.58.$      A       133.4.58.$
$GENERATE       0-255   133.4.59.$      A       133.4.59.$
$GENERATE       0-255   133.4.60.$      A       133.4.60.$
$GENERATE       0-255   133.4.61.$      A       133.4.61.$
$GENERATE       0-255   133.4.62.$      A       133.4.62.$
$GENERATE       0-255   133.4.63.$      A       133.4.63.$
```

2.2.5　　その他必要と思われる項目

その他 IPv4 枯渇における課題や対策について必要と思われる事項をまとめた。

（1）セッション数制限における課題

CGN が持つ NAT 技術は、IPv4 アドレス及びポート番号を複数の利用者で共同利用することから、利用者間の公平性確保のために、ISP において 1 ユーザ当たりの TCP（あるいは UDP）の同時セッション数を制限する必要がある。TCP には 2 バイト（16 ビット）のポート番号空間があり、一つのグローバル IP アドレス当たり、最大 64K（2^{16}、すなわち 65,536）個のセッションを生成できる。1024～65535 番のハイポートと呼ばれるポート番号の中でも、32K 以上のポートを利用すると、セキュリティ上問題があると認識されているため、32K 個のポートだけをソースポートとして使用することとなる。そのため、仮に一つの IP アドレスを複数のユーザで共有すると、使える TCP セッションは約 32,000 個のセッションをユーザ数で等分することになるが、昨今のウェブアプリケーション等の中には、多数のセッションを同時利用するものもあり、一人のユーザが同時に何セッションまで利用可能かどうかは、単純にユーザ数で等分するわけにはいかず、制限によってはユーザに多大な影響を与える可能性があった。そのため、CGN を導入した場合における 1 利用者当たりの必要なセッション数の目安（ウェブサイトの閲覧に支障が生じない範囲、ウェブアプリケーションの品質を低下させない範囲）、ポート利用の効率性を上げる方法を実証により明らかにした。

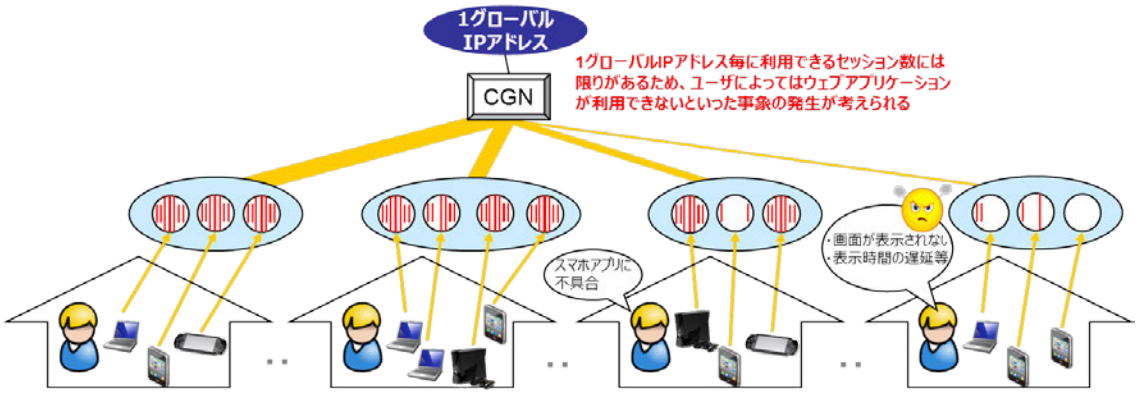


図 2.2-20　CGN 導入下におけるセッション数制限に係る課題

（2）セッション数制限の諸課題に関する対策

検証結果より、1ユーザ当たりのセッション数を1000セッション程度以下に制限することが望ましい。

1人のPCから発生する同時セッション数は100セッション程度以下であることが検証より明らかとなったが、一般家庭においても複数端末が同じCPEルータの下に接続されることを考えると、額面通り1ユーザ当たりの最大セッション数を100に制限すると、家庭内の複数機器で競合を起こすことが考えられる。

そのため、1ユーザ当たりのセッション数を1000セッション程度以下に制限することによって、特定ユーザによるセッションの食いつぶしを避けつつ(=公平利用)、多くのアプリケーションにとって問題の無い動作となることが想定できる。

ただし、上記は1ユーザに固定的に1000セッション割り当てることを意味するものではない。

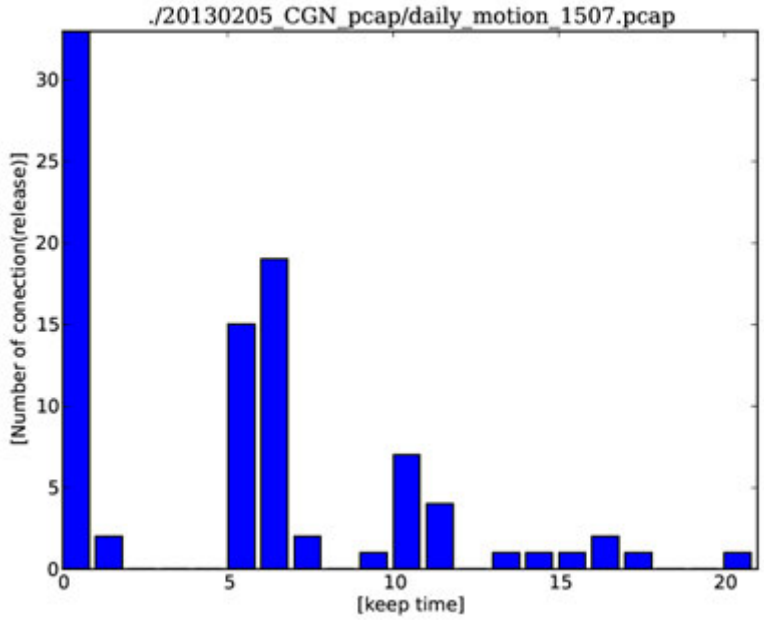


図 2.2-21　セッション数と継続時間の関係

図2.2-21は、セッション数の多かった代表的な通信において、セッションの継続時間をヒストグラムによってあらわしたものであるが、長期的なセッションが常に発生しているわけではなく、短期的なセッションが多いことがわかる。そのため、ユーザに固定的にセッション数を割り当ててしまうと、グローバルアドレスの有効利用(NAT 効率)の低下を招く恐れがある。この点においては、ユーザには動的にセッションを割り当てることが推奨される。

≪ポートアサイン手法と利用効率について≫

[1] REQ-13 において、CGN のポート割り当てスキームについては、ポート利用効率性を最大化すべきと要請されている。

ポート利用効率性について、Port Overlapping 手法について述べる

(ア) Port Overlapping

動的割り当てによっても、プールアドレスが足りなくなるように真に困窮した場合には、さらに効率的な利用方法として Port Overlapping（巻末 [3]参照）がある。送信先が異なる場合には、図 2.2-22 のように同じプールアドレスとポートに変換したとしても、通信が可能である。

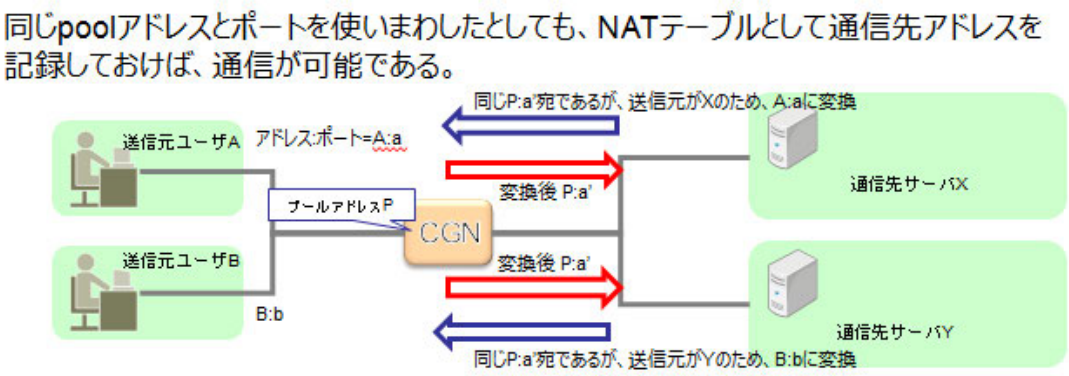


図 2.2-22　Port Overlapping

これにより、ポートの再利用が可能になり、少ないプールアドレスを有効活用できる。Port Overlapping は、CPE での NAT にはすでに利用されている手法である。この手法は、原理的に「静的割り当て」や「ポートブロックアロケーション」では利用できない。

また、第 3 者からの返りのパケットを受け入れることができないため、Full Cone NAT ではなくなる。そのため、Server-Client 型の通信に於いてのみ用いることができる。

3　参考文献

[1]　[I-D.ietf-behave-lsn-requirements]

Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", draft-ietf-behave-lsn-requirements-10 (work in progress), December 2012.

http://tools.ietf.org/html/draft-ietf-behave-lsn-requirements-10

[2]　[CGN_Viability]

Alcock, S., "Research into the Viability of Service-Provider NAT", 2008, <http://www.wand.net.nz/~salcock/someisp/flow_counting/result_page.html>.

[3] [draft-penno-behave-rfc4787-5382 -5508-bis-04]

Penno, R., Perreault, S., Kamiset, S., Boucadair, M., and K. Naito, "Network Address Translation (NAT) Behavioral Requirements Updates", draft-penno-behave-rfc4787-5382-5508-bis-04 (work in progress), January 2013.

[4] [draft-ietf-opsawg-lsn-deployment-02]

Victor Kuarsingh, John Cianfaran, CGN Deployment with BGP/MPLS IP VPNs”
draft-ietf-opsawg-lsn-deployment-02
http://tools.ietf.org/html/draft-ietf-opsawg-lsn-deployment-02