FUJITSU Hybrid IT Service FJcloud-O IaaS

IPCOM VA2 スタートガイド

Version 2.7

FUJITSU LIMITED

まえがき

本書の目的

本書は、FUJITSU Hybrid IT Service FJcloud-O IaaS（以降、IaaS）– IPCOM VA2（以下、IPCOM VA2 と言います)のインストール手順および、IaaS 上での設定手順例について記載しております。本書の記載内容に沿って IPCOM VA2 をご利用ください。

本書は、西日本第 3 リージョン、東日本第 3 リージョンを対象としています。

本書の読者

本書は、IPCOM VA2 をご利用になる方を対象としています。本書のご利用にあたり、基本的な IaaS の操作方法、ネットワークの知識を有していることを前提としております。あらかじめご了承ください。

本書の適用製品

本書の内容は以下の製品に適用されます。

- IPCOM VA2 1300 LS (EX)
- IPCOM VA2 1300 SC
- IPCOM VA2 2500 LS (SSL)
- IPCOM VA2 2500 SC

本書における語句の定義

本書で使用される語句の定義を下表に示します。

語句	定義の説明
IPCOM VA2 (アイピーコム ブイエーツー)	FUJITSU Hybrid IT Service FJcloud-O IaaS – IPCOM VA2 の略称です。
IaaS	FUJITSU Hybrid IT Service FJcloud-O IaaS の略称です。
Primary	IPCOM VA2 の装置二重化機能を有効にした場合の現用装置(プライマリー)です。
Secondary	IPCOM VA2 の装置二重化機能を有効にした場合の待機装置(セカンダリ)です。
仮想 IP アドレス	負荷分散対象のサーバ群を束ねる終端のアドレスとして IPCOM VA2 に定義する IP アドレスです。
代表 IP アドレス	2 台の IPCOM VA2 で共有するため、割り当てる IP アドレスです。冗長切り替え後に片方の IPCOM VA2 に引き継がれます。
ダミーポート	仮想 IP アドレス、代表 IP アドレスに対応する IaaS 上のポートです。IPCOM VA2 へのアタッチは不要です。
ライセンスキー	IPCOM VA2 のライセンスキーです。申し込み完了後、当社からお客様へ通知されます。
LB	ロードバランサー(Load Balancer)の略称です。
Lan	IPCOM VA2 のネットワークインターフェースの名称です。

語句	定義の説明
物理インターフェース	本書では、IaaS のポートに紐づく IPCOM VA2 のインターフェースを示します。

マニュアル体系

本書は IPCOM VA2 の設定に関する初期段階の説明を記載しております。 IPCOM VA2 の機能詳細は、本書と同 Web ページに掲載の製品マニュアルをご覧ください。下表に製品マニュアルの種類と目的・用途を示します。
IPCOM VA2 1300 LS(EX)、IPCOM VA2 1300 SC と IPCOM VA2 2500 LS(SSL)、IPCOM VA2 2500 SC とで参照する製品マニュアルが異なりますので、ご注意ください。

マニュアル名称	目的・用途
IPCOM VA2 シリーズマニュアル体系と読み方	マニュアルの構成と読み方、対象読者と前提知識、マニュアルで使用する名称や略称、マークの説明、コピーライトおよび商標などについて説明しています。 はじめに必ずお読みください。
IPCOM VA2 シリーズ VA2 ユーザーズガイド (*1)	IPCOM VA2 が提供する機能、IPCOM EX シリーズとの機能差分などについて説明しています。IPCOM VA2 を操作する前にこのマニュアルをよく読み、書かれている留意点や注意事項を十分に理解してください。
IPCOM EX シリーズユーザーズガイド (*1)(*2)	IPCOM EX シリーズの機能、導入、運用および本装置を使用するにあたって留意すべき点について解説したものです。
IPCOM EX シリーズ事例集(*2)	IPCOM EX シリーズの導入例の解説、および一般的な構成定義の例を紹介しています。
IPCOM EX シリーズコンソールリファレンスガイド (*2)	IPCOM EX シリーズの Web コンソールの基本操作および画面の詳細について説明しています。
IPCOM EX シリーズコマンドリファレンスガイド(*2)	IPCOM EX シリーズのコマンドの基本操作および各コマンドの機能について詳細に説明しています。
IPCOM EX シリーズ保守ガイド(*2)	IPCOM EX シリーズのメンテナンス方法やトラブル発生時の対処方法について説明しています。また、表示されるメッセージについて解説しています。

(*1) 該当マニュアルに記載されている機能対応一覧は IaaS に適用されません。詳細は 1 章を参照ください。

(*2) IPCOM VA2 シリーズは、IPCOM EX シリーズの仮想アプライアンス版であり、ソフトウェア仕様部分は共通であるため、IPCOM EX シリーズのマニュアルのうちソフトウェアに関するものを参照するようにしています。

輸出管理規制

本書を輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、 必要な手続きをおとりください。

IPCOM VA2 の使用条件について

IPCOM VA2 をご使用いただくにあたり、ライセンス条項に同意いただく必要がございます。IPCOM VA2 をご使用の前に、以下の Web ページに掲載のライセンス条項をお読みいただき、同意のうえ IPCOM VA2 をご使用ください。

IPCOM VA2 の使用に関するライセンス条項
https://jp.fujitsu.com/solutions/cloud/fjcloud/-o/document/pdf/ipcom-covenant.pdf

お願い

- 本資料の無断複製、転載を禁じます。
- 本資料は仕様変更等により予告なく内容を変更する場合がございます。あらかじめご注意願います。
- 本書に記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。

変更履歴

版数	更新日	変更箇所	概要
1.0	2018 年 6 月 25 日	初版作成	
1.1	2018 年 7 月 30 日	IPCOM VA2 1300 LS(EX)の記載追加 IPCOM VA2 1300 SC の記載追加	機能追加対応
1.2	2018 年 8 月 20 日	2.3 留意事項 No.13 を追記 3.2 仮想ルータの作成 の手順変更	IPCOM 冗長化構成時に必要な手順を変更し、サポートデスク側でのカスタマイズが必要になる旨の留意事項、注意書きを追加
1.3	2018 年 10 月 18 日	留意事項 項番 1	誤記修正
		留意事項 項番 14 の記載追加 7 章、14 章のコマンド例	IPCOM VA2 の mtu 値を 8950 に設定する記載を追加
1.4	2018 年 11 月 22 日	2.2 IPCOM VA2 設定の流れ	説明文の追記
		6.1 ルーティング許可の設定	allowed_address_pairs 設定内容の変更
		8.1 ファイアーウォールの設定	logging collection-level に関する説明を追記
		9.1 負荷分散機能の設定(LS primary)	負荷分散用の仮想 IP アドレスに関する説明の追記
		10.2 IPCOM VA2 LS の各代表 IP に対するポートを作成	ポート生成時のパラメータ変更
		12.1 IPCOM VA2 SC ファイアーウォールの設定	logging collection-level に関する説明を追記 誤記修正
		14.2【LS】IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当	グローバル IP アドレスの割当時のパラメータ変更
1.5	2018 年 12 月 20 日	留意事項 項番 13 の削除 3.2 仮想ルータの作成 の手順変更	仕様改善に伴い、IPCOM 冗長化構成時のサポートデスク側でのカスタマイズが不要になったため、関連記載を削除
		3.2 仮想ルータの作成 3.4 セキュリティグループの作成 10.2 IPCOM VA2 LS の各代表 IP に対応するポートを作成 10.3 メタデータ通信用の設定	コマンド例の curl パラメータの指定内容および一部の実行結果例を変更

		14.2 【LS】IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当	
		3.2 仮想ルータの作成 8.1 ファイアーウォールの設定 10.1 外部通信設定/secondary への LB 設定の同期 14.2【LS】IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当	誤記修正
1.6	2019 年 3 月 20 日	本書における語句の定義 10.2 IPCOM VA2 LS の各代表 IP に対応するダミーポートを作成 14.2【LS】IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当	用語に「ダミーポート」を追加
		まえがき	誤記訂正。製品マニュアルのパスワードに関する記載の削除
		第 1 章 IPCOM VA2 の概要、機能一覧	記載内容の改善。IPCOM VA2 の仕様の明確化
		2.1 IPCOM VA2 の使用手順について	記載内容の改善。申請メールの必要事項の詳細化
		2.3 留意事項 No.13 7.2 インターフェースと冗長化設定(LS primary) 7.4 インターフェースと冗長化設定(LS secondary) 11.2 インターフェース設定(SC)	記載内容の改善。mtu 値の設定理由の明確化
		2.3 留意事項 No.14	記載内容の改善。フレーバー変更のサポート有無の明確化
		6.1 ルーティング許可の設定	記載内容の改善。ルーティング許可対象の IP アドレスの明確化
		7.2 インターフェースと冗長化設定(LS primary) 7.4 インターフェースと冗長化設定(LS secondary) 付録 A：【設定事例】IPCOM VA2 LS の running-config	誤記訂正。動作に影響を及ぼさない auto-negotiation 設定の記載を削除。
		10.3 メタデータ通信用の設定	誤記訂正。スタティックルーティングの設定内容の修正
		14.3 【LS】IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当	誤記訂正。図表番号の訂正
		付録 C：IaaS 上の IPCOM VA2 の未サポート機	記載内容の改善。IPCOM

		能 付録 D：IPCOM VA2 および IaaS の構成 付録 E：IPCOM VA2 と IaaS の通信設定	VA の仕様の明確化
1.7	2019 年 5 月 23 日	2.3 留意事項 No.13 7.2 インターフェースと冗長化設定(LS primary) 7.4 インターフェースと冗長化設定(LS secondary) 11.2 インターフェース設定(SC) E-7 MTU 値の設定	記載内容の改善。用語統一および MTU 値の設定条件を追記
		C-1-13 運用管理/保守機能	記載内容の改善。リアルタイム・モニタを非サポートに変更
1.8	2020 年 3 月 17 日	2.1 IPCOM VA2 の使用手順について	ライセンスキーの入手手順を変更
1.9	2020 年 5 月 20 日	2.3 留意事項 メタデータ通信の設定について	記載内容の改善。仮想ルータのファイアーウォールの設定内容を変更
2.0	2020 年 7 月 16 日	2.3 留意事項	記載内容の改善。 アンチアフィニティ機能に関する記載の見直し
		3.4 セキュリティグループの作成	記載内容の改善。 推奨ルールの冗長化機能使用時の記載の見直し
		E-7 MTU 値の設定	記載内容の改善。 MTU に関する記載の見直し
2.1	2020 年 9 月 16 日	2.3 留意事項 4.1 【LS】IPCOM VA2 の作成(LS primary) 4.2 【LS】IPCOM VA2 の作成(LS secondary) 4.3 【SC】IPCOM VA2 の作成(SC)	対応する仮想サーバタイプを追加
2.2	2020 年 11 月 16 日	2.3 留意事項 項番 14	機能改善。 仮想サーバリサイズのサポート化
		2.3 留意事項 メタデータ通信の設定について 10.3 メタデータ通信用の設定	メタデータ通信の設定内容の改善。(10.3 章を削除)
		2.3 留意事項 項番 15 第 3 章【共通設定】環境準備 [注意] 3.2 仮想ルータの作成［注意］ E-1 通信設定の概要 (4)冗長化構成	設定内容の改善。 冗長化構成の IPCOM に接続されたサブネットに仮想ルータを接続する必要がある旨を追記

2.3	2021 年 1 月 14 日	第 4 章 【LS/SC】仮想サーバの作成 第 5 章 【LS/SC】ライセンス登録	記載内容の改善。 コマンド例にある不要なパラメタ"availability_zone"を削除
2.4	2021 年 4 月 19 日	5.3 【LS】追加ボリュームの作成およびアタッチ(LS primary) 5.4 【LS】追加ボリュームの作成およびアタッチ(LS secondary) 5.8 【SC】追加ボリュームの作成およびアタッチ(SC)	誤記訂正 追加ボリュームの種別の内容を修正
2.5	2021 年 7 月 16 日	3.4 セキュリティグループの作成	記載内容の改善。 セキュリティグループの利用に関する注意書きを追記
		14.1 仮想ルータのファイアーウォールルールの設定	記載内容の改善。 ファイアーウォールの設定例を見直し、図 14-1 の修正と注意書きを追加
		E-8 セキュリティグループのステートフル・ステートレスの設定	付録 E-8 を追加
2.6	2021 年 9 月 15 日	2.4 本書で作成するシステム構成	記載内容の改善。 通信設定の仕様、推奨値の参照先：付録 E を追加
		3.4 セキュリティグループの作成	記載内容の改善。 注意書きの記載内容の見直し
		E-1 通信設定の概要 (2) サーバ負荷分散機能	記載内容の改善。 サポート構成に関する記載を追加
		本資料全体	文言統一。 文面内の「FW」を「ファイアーウォール」に統一
2.7	2023 年 9 月 13 日	3.4 セキュリティグループの作成 E-8 セキュリティグループのステートレス設定	記載内容の改善。 ステートレスセキュリティグループの表現を改善

目次

第 1 章　IPCOM VA2 の概要、機能一覧

FUJITSU Hybrid IT Service FJcloud-O IaaS – IPCOM VA2 は、FUJITSU Hybrid IT Service FJcloud-O IaaS 上で動作する仮想アプライアンスソフトウェアであり、インターネットやイントラネットとシステム（サーバやアプリケーション）を接続するシステムフロントで必要となるさまざまなトラフィック制御機能やセキュリティ機能を持っています。

1.1 提供機能

IaaS 上の IPCOM VA2 は、FUJITSU Network IPCOM シリーズの仮想アプライアンスソフトウェア製品をベースに、IaaS 上で動作するよう対応したものです。IaaS 上の IPCOM VA2 において未サポートとなる機能につきましては、以下をご確認ください。

- 付録 C：IaaS 上の IPCOM VA2 の未サポート機能

本書の記載以外の、FUJITSU Network IPCOM シリーズの仮想アプライアンスソフトウェア製品との共通機能、および、各マニュアルの参照関係につきましては、以下をご確認ください。

- IPCOM VA2 シリーズマニュアル体系と読み方
- IPCOM VA2 シリーズ VA2 ユーザーズガイド
- IPCOM EX シリーズユーザーズガイド
- IPCOM EX シリーズ事例集
- IPCOM EX シリーズコンソールリファレンスガイド
- IPCOM EX シリーズコマンドリファレンスガイド
- IPCOM EX シリーズ保守ガイド

IaaS 上の IPCOM VA2 をご使用いただく上での前提知識および基本的な仕様、設定確認箇所につきましては、以下をご確認ください。

- 付録 D：IPCOM VA2 および IaaS の構成
- 付録 E：IPCOM VA2 と IaaS の通信設定

1.2 ソフトウェアオプション

IaaS 上の IPCOM VA2 で利用可能なソフトウェアオプションを以下に示します。

表 1-1：IaaS 上の IPCOM VA2 で利用可能なソフトウェアオプション

製品名	利用可能なソフトウェアオプション	備考
IPCOM VA2 1300 LS (EX)	『WAF オプション』	
IPCOM VA2 1300 SC	なし	
IPCOM VA2 2500 LS (SSL)	『SSL アクセラレーターオプション』	
IPCOM VA2 2500 SC	なし	

第 2 章 IPCOM VA2 ご利用の流れ

本章では、IPCOM VA2 をご利用いただくための作業の流れや留意点について説明します。

2.1 IPCOM VA2 の使用手順について

IPCOM VA2 を使用するためにはライセンスキーが必要となります。ライセンスキーを入手する際は、以下の申請内容を記載し、ヘルプデスクまでご連絡ください。

<ライセンスキー払い出しの申請内容>

- 契約番号
- ライセンスキー払い出し希望日　※ライセンスキーの払い出しは最短で 2 営業日が必要となります
- IPCOM 種別
  - IPCOM VA2 1300 LS(EX)
  - IPCOM VA2 1300 SC
  - IPCOM VA2 2500 LS(SSL)
  - IPCOM VA2 2500 SC

［注意］

ライセンスキーを入力するまでは IPCOM VA2 を配備しても使用できません（コマンド入力等が受け付けられません）。
配備した時点から課金が開始となるため、配備する前に必ずライセンスキーの使用申請を行うようお願いいたします。

2.2 IPCOM VA2 設定の流れ

本書では、IPCOM VA2 を含むシステムの作成を事例として、IPCOM VA2 の設定方法を説明します。図 2-1 に設定の流れの全体を示します。

図 2-1：IPCOM VA2 設定の流れ

IPCOM VA2 の構成によって、以下の章を参照して下さい。

・クラスタ構成(IPCOM VA2 LS)；4/5/6/7/8/9/10/14 章

・シングル構成(IPCOM VA2 SC)；4/5/11/12/13/14 章

2.3 留意事項

作業を始める前に表２-1 の留意事項をよくお読みください。

表 2-1：留意事項(1/2)

項番	留意事項	該当する章番号
1	仮想サーバタイプは IPCOM VA2 1300 ; S3-1, S4-1S / IPCOM VA2 2500 ; C3-4, C4-4S を指定してください (IaaS プライベートリソースサービス専有仮想サーバをご利用の場合は、IPCOM VA2 1300 ; S3-1.d, S4-1S.d / IPCOM VA2 2500 ; C3-4.d, C4-4S.d を指定してください)。該当以外の仮想サーバタイプを指定した場合、IPCOM VA2 の動作は保証しておりません。また、オートスケールには対応しておりません。	4 章
2	IPCOM VA2 に割り当てるディスクボリュームは初回 boot 時に/dev/vda に 2GB、その後の追加設定で/dev/vdb に 100GB 割り当てます。それ以外のサイズを指定した場合、IPCOM VA2 の動作は保証しておりません。また、ボリュームのリサイズや追加アタッチには対応しておりません。	5 章
3	IPCOM VA2 の冗長化機能はマルチ AZ 構成では使用できません。	なし
4	冗長化構成の IPCOM VA2 の仮想サーバを作成する際、異なるホスト上で動作するよう、アンチアフィニティ機能を設定してください。また、IPCOM VA2 に繋がっているサブネット上の仮想サーバは、アンチアフィニティ機能の設定を推奨します。	4 章
5	セキュリティレベル向上のため、ライセンス登録後は必ず admin ユーザーのパスワード設定を実施してください。また、admin パスワードを設定するまでリモートアクセス(IPCOM VA2 の機能による SSH や GUI へのアクセス)は許可しないでください。	7 章,11 章
6	IPCOM VA2 を経由する通信を行う仮想サーバはキーペアのインポートやホスト名の取得のために次頁の内容を実施する必要があります。設定は本設定手順に沿って行えば実施できます。(*1)	10 章
7	IPCOM VA2 はキーペアには対応しておりません。そのため、キーペアを割り当てててもキーを用いてログインすることはできません。	3 章
8	IPCOM VA2 は仮想サーバインポートおよび仮想サーバエクスポートには対応しておりません。	なし
9	IPCOM VA2 はスナップショット機能には対応しておりません。	なし
10	作成済みの IPCOM VA2 から、仮想サーバイメージを作成することはできません。	なし
11	SDK-WEBよりダウンロードしたモジュールは、IPCOM VX2上での動作のみサポートしています。IaaSインフラ上にて、SDK-WEBよりダウンロードしたモジュールによるインストールおよびアップデートを実施しないでください。	なし
12	WebアクセラレーションおよびHTTP Keep-Alive負荷分散を使用する場合、分散対象のWebサーバのHTTPのKeep Alive設定を有効にしてください。 上記機能を使用しない場合、Keep Alive設定を無効にしてください。 詳細は、「IPCOM EX シリーズユーザーズガイド」 2-6-4-4 コンテンツ単位の負荷分散を参照してください。	なし

表 2-1：留意事項(2/2)

項番	留意事項	該当する章番号
13	MTU値は、付録E：IPCOM VA2とIaaSの通信設定のE-7 MTU値の設定を参考に設定してください。	7 章、14 章
14	IPCOM VA2の仮想サーバは、仮想サーバリサイズ(仮想サーバタイプの変更)に対応しています。当留意事項の項番1を確認したうえで、以下のいずれかの手順で実施してください。 ・ポータルサイトで「仮想サーバリサイズ」、「リサイズ/マイグレーション確定」の実行 ・Resize Server API、Confirm Resized Server APIの実行 また、仮想サーバリサイズを実施する際、事前にIPCOM VA2を停止状態(poweroffコマンドまたはWebコンソール画面からの停止)にしてください。 ※プライベートリソースサービスの利用が可能です。 ※東日本第1/第2、西日本第1/第2リージョンのIPCOM VA2の仮想サーバリサイズは未サポート(サポート予定無し)になりますのでご注意ください。	なし
15	下記構成の場合、IPCOMに接続するサブネットに仮想ルータを接続する必要があります。仮想ネットワークを構築する際はご注意ください。 ・IPCOMを冗長化構成にする場合 (サブネットに仮想ルータが無い場合、通信性能に影響がでる可能性があります) ・IPCOMに接続されるサブネット上の仮想サーバでメタデータ通信が必要な場合	3 章

(*1)留意事項 6 の詳細：メタデータ通信の設定について

メタデータ通信とは、仮想サーバを起動するときにIaaSが提供する特別なサーバ(メタデータプロキシ)からキーペアのキーや仮想サーバのホスト名などのデータを取得するための通信を指します。

IPCOM に接続するサブネット上の仮想サーバよりメタデータ通信を行う場合、サブネットに仮想ルータを接続してください。仮想サーバのデフォルトルートやサブネットの GatewayIP、HOST_ROUTES の NextHop は、仮想ルータもしくは IPCOM VA2 のいずれかを指定してください。

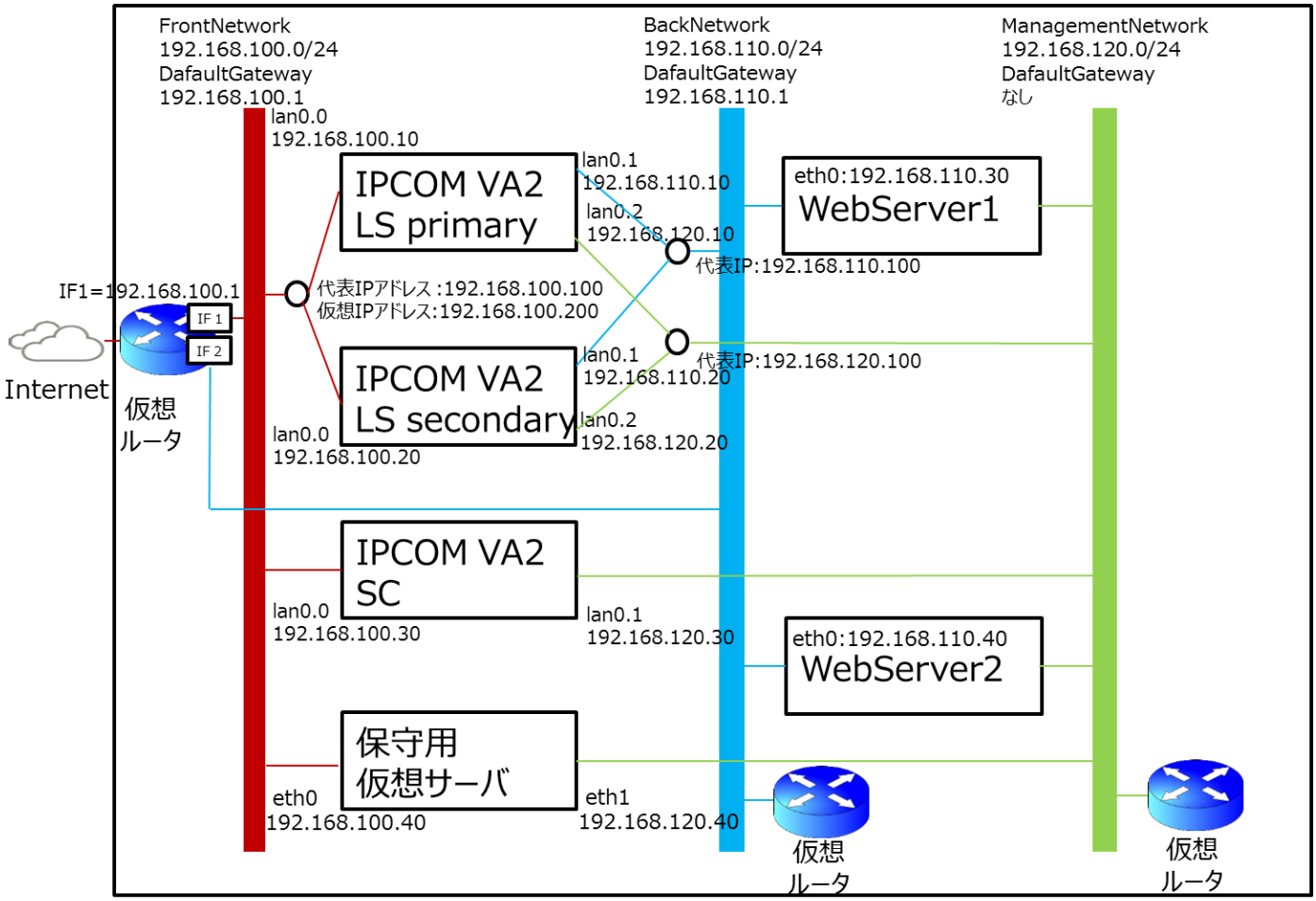
2.4 本書で作成するシステム構成

以降の章では、IaaS 上で IPCOM VA2 を含んだシステムの設定方法を事例として紹介しております。本事例を参考にし、構築を行ってください。図 2-3 に、本書で作成するシステム構成を示します。

本マニュアルに記載した事例以外の構成に関しては、IPCOM EX シリーズ事例集ならびに IaaS マニュアルを参照ください。また、通信設定に関する仕様や推奨値については、付録 E：IPCOM VA2 と IaaS の通信設定 をご確認ください。

API で使用するエンドポイントや変数について、以降の説明では下記の表記をしております。エンドポイントについては IaaS マニュアルをご参照ください。

- $COMPUTE：compute サービスのエンドポイント
- $NETWORK：ネットワークサービスのエンドポイント
- $OS_AUTH_TOKEN：取得した API のトークン
- $PROJECT_ID ：設定するプロジェクトの ID



※保守用仮想サーバは IPCOM VA2 メンテナンスの用途を想定しております。

※IPCOM VA2 SC は本事例において DNS サーバとしての事例を紹介しております。

図 2-3：IaaS 上の IPCOM VA2 を含むシステム構成

本章では、IPCOM VA2 作成前に必要となる環境準備作業について説明します。

［注意］

下記構成の場合、IPCOM に接続するサブネットに仮想ルータを接続する必要があります。仮想ネットワークを構築する際はご注意ください。

- **IPCOM を冗長化構成にする場合(サブネットに仮想ルータが無い場合、通信性能に影響がでる可能性があります)**
- **IPCOM に接続されるサブネット上の仮想サーバでメタデータ通信が必要な場合**

3.1 仮想ネットワークの作成

システムで利用するプライベートネットワークを作成します。

① 仮想ネットワークを作成します。操作は API で行ってください。(図 3-1)

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=frontNetwork ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .

※1  名前は任意で指定してください。
※2  ipcom のテナント ID で指定してください。
```

実行結果例

```
{
"network": {
   "id": "0261afcc-cc9e-4f3d-a76b-8189d3206f60",
   "shared": false,
   "status": "ACTIVE",
   "subnets": [],
   "name": "net-internet",
   "router:external": false,
   "project_id": "7338b034a37749ffb8b912bb0b064705",
   "tenant_id": "7338b034a37749ffb8b912bb0b064705",
   "admin_state_up": true
 }
}
```

図 3-1：仮想ネットワーク作成画面

② Subnet、Gateway の設定を行います。(図 3-2)

コマンド例

```
[root@K5-Host ]# CIDR=192.168.100.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=frontSubnet ※2
[root@K5-Host ]# NETWORK_ID=作成した仮想ネットワークの ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'"}}' | jq .
```

※1 サブネットアドレスで指定してください。
※2 名前は任意で指定してください。
※3 作成した仮想ネットワークの ID で指定してください。
※4 ipcom のテナント ID で指定してください。

実行結果例


```
{
"network": {
   "id": "0261afcc-cc9e-4f3d-a76b-8189d3206f60",
   "shared": false,
   "status": "ACTIVE",
   "subnets": [],
   "name": "net-internet",
   "router:external": false,
   "project_id": "7338b034a37749ffb8b912bb0b064705",
   "tenant_id": "7338b034a37749ffb8b912bb0b064705",
   "admin_state_up": true
 }
}
```


図 3-2：サブネット、ゲートウェイの設定例

③ 外部インターネット接続を行う場合、DNS を設定します。(図 3-3)

コマンド例

```
[root@K5-Host ]# SUBNET_ID=作成した Subnet の ID  ※1
[root@K5-Host ]# DNS=DNS の ip address  ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets/$SUBNET_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"dns_nameservers":["'$DNS'"]}}' | jq .
```

※1 作成した仮想 Subnet の ID で指定してください。
※2 DNS の ip address で指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2018-06-22T08:54:23Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
    "dns_nameservers": [
```

```
      "133.162.192.9",
      "133.162.192.10"
    ],
    "host_routes": [],
    "revision_number": 2,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "b08bfdcf-5d7a-4708-839b-aecf90f3757b",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "7916efee-b8e0-4ff6-86e6-7605cccbeca0",
    "gateway_ip": "133.162.193.9",
    "project_id": "48c51d33bd4f4891858bcf5163847787",
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.100.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "test-sub",
    "enable_dhcp": false,
    "network_id": "3cbbbaf6-7d9a-4427-a3c4-a1383565d6c1",
    "tenant_id": "48c51d33bd4f4891858bcf5163847787",
    "created_at": "2018-06-22T08:54:23Z",
    "ip_version": 4,
    "nuagenet": "be1458c7-24d8-42ec-a2f1-db66e9939b00"
  }
}
```


図 3-3：DNS 設定例

上記の手順で、図 2-3 のシステム構成に従い、3 つプライベートネットワークを作成します。

[ネットワーク例]

- FrontNetwork
  - NetworkAddress :192.168.100.0
  - GatewayIP :192.168.100.1
- BackNetwork
  - NetworkAddress :192.168.110.0
  - GatewayIP :192.168.110.1
- ManagementNetwork
  - NetworkAddress :192.168.120.0
  - GatewayIP :なし

3.2 仮想ルータの作成

外部接続用の仮想ルータを作成します。

① 仮想ルータを作成します。操作は API で行ってください。(図 3-4)

コマンド例

```
[root@K5-Host ]# ROUTER_NAME=Ext-Router ※1
[root@K5-Host ]# TENANT_ID=テナントの ID  ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/routers -X POST -H "X-Auth-Token:$OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"router": {"name": "'$ROUTER_NAME'", "tenant_id": "'$TENANT_ID'"}}' | jq .
```

※1 名前は任意で指定してください。
※2 ipcom のテナント ID で指定してください。

実行結果例


```
{
    "router": {
        "admin_state_up": true,
        "created_at": "2018-04-27T01:18:27Z",
        "description": "",
        "ecmp_count": 1,
        "external_gateway_info": null,
        "id": "eadbf3a1-5ffa-42cd-ba95-6609bd357df3",
        "name": "Ext-Router",
        "nuage_backhaul_rd": "65534:23913",
        "nuage_backhaul_rt": "65534:30733",
        "nuage_backhaul_vnid": 10993991,
        "nuage_underlay": "off",
        "project_id": "7338b034a37749ffb8b912bb0b064705",
        "rd": "65534:35697",
        "revision_number": 1,
        "routes": [],
        "rt": "65534:16038",
        "status": "ACTIVE",
        "tags": [],
        "tenant_id": "7338b034a37749ffb8b912bb0b064705",
        "updated_at": "2018-04-27T01:18:27Z"
    }
}
```


図 3-4：仮想ルータの作成例

② 仮想ルータを作成後、インターフェースの作成および仮想ルータへのアタッチを行います。仮想ルータのインターフェースは以下のように API で作成します。

■インターフェース 1 の作成 (図 3-5)

- サブネット：FrontNetwork に所属するサブネット
- IP アドレス：任意(ゲートウェイ IP を推奨します)

コマンド例

```
[root@K5-Host ]# PORT_NAME=FrontSubnetRouterPort ※1
[root@K5-Host ]# NETWORK_ID="FrontNetwork の ID"
[root@K5-Host ]# SUBNET_ID="FrontNetwork のサブネット ID"
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.100.1 ※2
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port":{"network_id": "'$NETWORK_ID'", "name": "'$PORT_NAME'", "fixed_ips":
[{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}]}}' | jq .
```

※1 【任意】名前は任意で指定してください。
※2 【任意】ポートの IP アドレスは任意です。（ゲートウェイ IP を推奨します）

実行結果例


```
{
    "port": {
        "admin_state_up": true,
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "created_at": "2018-04-27T01:23:41Z",
        "description": "",
        "device_id": "",
        "device_owner": "",
        "extra_dhcp_opts": [],
        "fixed_ips": [
            {
                "ip_address": "192.168.100.1",
                "subnet_id": "ca18f920-3578-48d9-833e-9c9bf56e0cd5"
            }
        ],
        "id": "366fcbe2-edf9-4319-ba26-7ec658b78205",
        "mac_address": "fa:16:3e:ac:bc:bd",
        "name": "",
        "network_id": "b4b6a1e0-6f13-4ad1-8402-d76721e155ac",
        "nuage_floatingip": null,
        "nuage_policy_groups": null,
        "nuage_redirect_targets": [],
        "port_security_enabled": true,
        "project_id": "7338b034a37749ffb8b912bb0b064705",
        "revision_number": 5,
        "security_groups": [
            "ad2b8385-c8a0-4eec-a29d-dcd0ed54fc66"
        ],
        "status": "DOWN",
        "tags": [],
        "tenant_id": "7338b034a37749ffb8b912bb0b064705",
        "updated_at": "2018-04-27T01:23:42Z"
    }
```

```
}
```

図 3-5：FrontNetwork 用のインターフェース 1 の作成例

■ インターフェース 1 を仮想ルータにアタッチします。(図 3-6)

コマンド例

```
[root@K5-Host ~]# ROUTER_ID="作成した仮想ルータの ID"
[root@K5-Host ~]# PORT_ID="作成したインターフェース 1 の ID"
[root@K5-Host ~]# curl -s $NETWORK/v2.0/routers/$ROUTER_ID/add_router_interface -X PUT -H "X-Auth-Token:
$OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port_id": "'$PORT_ID'" }' | jq .
```

実行結果例

```
{
    "id": "eadbf3a1-5ffa-42cd-ba95-6609bd357df3",
    "network_id": "b4b6a1e0-6f13-4ad1-8402-d76721e155ac",
    "port_id": "366fcbe2-edf9-4319-ba26-7ec658b78205",
    "subnet_id": "ca18f920-3578-48d9-833e-9c9bf56e0cd5",
    "subnet_ids": [
        "ca18f920-3578-48d9-833e-9c9bf56e0cd5"
    ],
    "tenant_id": "7338b034a37749ffb8b912bb0b064705"
}
```

図 3-6：FrontNetwork 用のインターフェース 1 を仮想ルータにアタッチ

■ インターフェース 2 の作成 (図 3-7)

- サブネット：BackNetwork に所属するサブネット
- IP アドレス：任意(ゲートウェイ IP を推奨します)

※インターフェース 2 は WebServer がメタデータプロキシと通信するために必要となるため必ず設定してください。

コマンド例

```
[root@K5-Host ]# PORT_NAME=BackSubnetRouterPort ※1
[root@K5-Host ]# NETWORK_ID="BackNetwork の ID"
[root@K5-Host ]# SUBNET_ID="BackNetwork のサブネット ID"
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.110.1 ※2
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port":{"network_id": "'$NETWORK_ID'", "name": "'$PORT_NAME'", "fixed_ips":
[{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}]}}' | jq .
```

※1 【任意】名前は任意で指定してください。
※2 【任意】ポートの IP アドレスは任意です。(ゲートウェイ IP を推奨します)

実行結果例

```
{
    "port": {
        "admin_state_up": true,
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "created_at": "2018-04-27T01:31:55Z",
```

```
        "description": "",
        "device_id": "",
        "device_owner": "",
        "extra_dhcp_opts": [],
        "fixed_ips": [
            {
                "ip_address": "192.168.110.1",
                "subnet_id": "fcc8bf68-5ebe-4b9e-b206-6b50c55788e0"
            }
        ],
        "id": "f1ac4297-9e6a-4d92-8430-5008eedcd801",
        "mac_address": "fa:16:3e:47:68:08",
        "name": "",
        "network_id": "4eb676c5-070f-4d28-b8d1-f6c395f16eaf",
        "nuage_floatingip": null,
        "nuage_policy_groups": null,
        "nuage_redirect_targets": [],
        "port_security_enabled": true,
        "project_id": "7338b034a37749ffb8b912bb0b064705",
        "revision_number": 5,
        "security_groups": [
            "ad2b8385-c8a0-4eec-a29d-dcd0ed54fc66"
        ],
        "status": "DOWN",
        "tags": [],
        "tenant_id": "7338b034a37749ffb8b912bb0b064705",
        "updated_at": "2018-04-27T01:31:55Z"
    }
}
```


図 3-7： BackNetwork 用のインターフェース 2 の作成例

■ インターフェース 2 を仮想ルータにアタッチします。(図 3-8)

コマンド例

```
[root@K5-Host ~]# ROUTER_ID="仮想ルータの ID"
[root@K5-Host ~]# PORT_ID="インターフェース 2 の ID"
[root@K5-Host ~]# curl -s $NETWORK/v2.0/routers/$ROUTER_ID/add_router_interface -X PUT -H "X-Auth-Token:
$OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port_id": "'$PORT_ID'"  }' | jq .
```

実行結果例


```
{
  "subnet_id": "5582755b-8480-4ccf-baac-3c2ddfc74ea7",
  "tenant_id": "a6a7fe34a4e6447d8487ea8225db64c4",
  "port_id": "99472b16-feb6-45a4-9678-376eb160a311",
  "id": "758dc549-2020-4492-b0ef-994eafca9447",
  "availability_zone": "jp-east-1a"
}
```


図 3-8：BacktNetwork 用のインターフェース 2 を仮想ルータにアタッチ

③ 仮想ルータ経由でインターネットにアクセスするため、仮想ルータのゲートウェイ設定で外部仮想ネットワークを設定します。

(図 3-9)

コマンド例

```
[root@K5-Host ~]# ROUTER_ID="作成した仮想ルータの ID"
[root@K5-Host ~]# EXT_NET_ID="グローバル IP ネットワークの ID" ※1
[root@K5-Host ~]# curl -s $NETWORK/v2.0/routers/$ROUTER_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"router": {"external_gateway_info": {"network_id": "'$EXT_NET_ID'"}}}' | jq .

※1 本例では inf_az1_ext-net02 を指定します。
```

実行結果例

```
{
  "router": {
    "status": "ACTIVE",
    "external_gateway_info": {
      "network_id": "6516b3b1-1c8c-46da-8bc5-c12f4602817c",
      "enable_snat": true
    },
    "name": "Ext-Router",
    "admin_state_up": true,
    "tenant_id": "a6a7fe34a4e6447d8487ea8225db64c4",
    "routes": [],
    "id": "758dc549-2020-4492-b0ef-994eafca9447",
    "availability_zone": "jp-stg1a"
  }
}
```

図 3-9：仮想ルータのゲートウェイ設定で外部仮想ネットワークを設定

[注意]

下記構成の場合、IPCOM に接続するサブネットに仮想ルータを接続する必要があります。前述の①、②の手順を参考に仮想ルータを作成し、ManagementNetwork のサブネットに接続してください。

- **IPCOM を冗長化構成にする場合(サブネットに仮想ルータが無い場合、通信性能に影響がでる可能性があります)**
- **IPCOM に接続されるサブネット上の仮想サーバでメタデータ通信が必要な場合**

3.3 キーペアについて

IPCOM VA2 はキーペアに対応していないため、作成したキーペアを利用して、ログインはできません。

そのため、キーペアは割り当てをしなくて構いません。

3.4 セキュリティグループの作成

IPCOM のセキュリティグループ

IPCOM に設定するセキュリティグループは**ステートレス・セキュリティグループ**をご利用ください。
特に冗長構成で IPCOM を構築する場合においては、ステートフル・セキュリティグループを利用すると装置切り替えが発生した際に長期間通信不可となる重大な通信障害に繋がる可能性があります。
※手動による運用切り替え操作、オートフェイルオーバによる切り替わりなど状況によらず装置切り替え全般を指します。

ステートレス・セキュリティグループの利用については、以下をご確認ください。

- IaaS ドキュメント・ツール類 クラウドデザインパターン・実装サンプル集
  + ネットワーク基本
    + ステートレスセキュリティグループ［東日本／西日本リージョン 3 向け］

IPCOM VA2 の冗長切り替え時の通信影響については、以下をご確認ください。

- IPCOM EX シリーズ ユーザーズガイド
  + A.4 装置切り替え時のエンド間の通信への影響

また、仮想ルータのファイアーウォールサービスとステートレス・セキュリティグループを併用した場合、特定の条件下で TCP 通信が切断される場合があります。対処方法として、以下のどれかの設定(複数可)を推奨します。

- 仮想ルータのファイアーウォールに逆方向ルールを追加する
  ※IPCOM 冗長構成で仮想ルータのファイアーウォールを利用する場合に必要な設定になります。
- TCP コネクションが切断されても短時間でリトライするよう、クライアント側のタイムアウト値を調整する
- 仮想ルータのファイアーウォールサービスを使用せず、IPCOM のファイアーウォールサービスを使用する

詳細は以下をご確認ください。

- IaaS ドキュメント・ツール類 機能説明書
  + ネットワーク [東日本第 3／西日本第 3]
    + ファイアーウォールサービス
      + ファイアーウォールサービスとステートレス・セキュリティグループの組み合わせ

IPCOM VA2 のセキュリティグループを作成します。API で以下を実施してください。

① IPCOM VA2 用のセキュリティグループを作成します。(図 3-10)

コマンド例

```
[root@K5-Host ~]# SG_NAME=ipcom-va2-SG        ※1
[root@K5-Host ~]# SG_STATEFUL=false           ※2
[root@K5-Host ~]# curl -s $NETWORK/v2.0/security-groups -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"security_group": {"name": "'$SG_NAME'", "stateful": "'$SG_STATEFUL'"}}'
| jq .
```

※1　【任意】名前は任意で指定してください。
※2　「false」を指定してください。ステートレスとして設定されます。

実行結果例


```
{
  "security_group": {
    "tenant_id": "77b97024974140cf921bb40834a383d0",
    "description": "",
    "name": "ipcom-va2-SG",
    "security_group_rules": [
      {
        "remote_group_id": null,
        "direction": "egress",
        "remote_ip_prefix": null,
        "protocol": null,
        "ethertype": "IPv6",
        "port_range_max": null,
        "security_group_id": "80b6deee-c4a8-4c33-805c-daf15c11786a",
        "port_range_min": null,
        "tenant_id": "77b97024974140cf921bb40834a383d0",
        "id": "6b19ca09-cf4b-4b68-b8e7-117dc2db73e7"
      },
      {
        "remote_group_id": null,
        "direction": "egress",
        "remote_ip_prefix": null,
        "protocol": null,
        "ethertype": "IPv4",
        "port_range_max": null,
        "security_group_id": "80b6deee-c4a8-4c33-805c-daf15c11786a",
        "port_range_min": null,
        "tenant_id": "77b97024974140cf921bb40834a383d0",
        "id": "b611e02f-dff0-413d-80a5-5e5b3fdfa7bb"
      }
    ],
    "id": "80b6deee-c4a8-4c33-805c-daf15c11786a"
  }
}
```


図 3-10: IPCOM VA2 用のセキュリティグループを作成

② 作成したセキュリティグループのルールを定義します。APIで以下を実施してください。IPCOM VA2は内部でファイアーウォールの設定を行うため、本例では以下の推奨ルールを設定しております。

【推奨ルール】
egress IPv6 - (全許可)
egress IPv4 – (全許可)
ingress IPv4 icmp 0.0.0.0/0 (全許可)
ingress IPv4 tcp 1-65535 0.0.0.0/0(全許可)
ingress IPv4 udp 1-65535 0.0.0.0/0(全許可)
ingress IPv4 112 (VRRP) 0.0.0.0/0(全許可)
※112(VRRP)は冗長化機能を使用する場合許可をしてください。また、「egress IPv4 – (全許可)」を設定しない場合、「egress IPv4 112 (VRRP) 0.0.0.0/0(全許可)」を設定してください。
※IPCOM VA2 内部でファイアーウォール機能を有しているため、セキュリティグループはすべて許可します。

■ tcpをすべて許可するルールを作成し、適用します。（図 3-11）

コマンド例

```
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=tcp
[root@K5-HOST ]# MIN_PORT_NUM=1
[root@K5-HOST ]# MAX_PORT_NUM=65535
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'","port_range_min": '$MIN_PORT_NUM',"port_range_max": '$MAX_PORT_NUM',"protocol": "'$PROTCOL'","remote_ip_prefix": "'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

実行結果例

```
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "ingress",
    "protocol": "tcp",
    "ethertype": "IPv4",
    "port_range_max": 65535,
    "security_group_id": "80b6deee-c4a8-4c33-805c-daf15c11786a",
    "tenant_id": "77b97024974140cf921bb40834a383d0",
    "port_range_min": 1,
    "remote_ip_prefix": "0.0.0.0/0",
    "id": "688a124f-d2d8-433f-9c50-0670c1f4fabc"
  }
}
```

図 3-11:tcp 許可ルールを作成

■ udpをすべて許可するルールを作成し、適用します。(図 3-12)

コマンド例

```
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=udp
[root@K5-HOST ]# MIN_PORT_NUM=1
```

```
[root@K5-HOST ]# MAX_PORT_NUM=65535
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'","port_range_min":
'$MIN_PORT_NUM',"port_range_max": '$MAX_PORT_NUM',"protocol": "'$PROTCOL'","remote_ip_prefix":
"'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

実行結果例


```
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "ingress",
    "protocol": "udp",
    "ethertype": "IPv4",
    "port_range_max": 65535,
    "security_group_id": "80b6deee-c4a8-4c33-805c-daf15c11786a",
    "tenant_id": "77b97024974140cf921bb40834a383d0",
    "port_range_min": 1,
    "remote_ip_prefix": "0.0.0.0/0",
    "id": "a3401741-7ae4-4fd2-bbca-ff8a373ef7bc"
  }
}
```


図 3-12:udp 許可ルールを作成

■ icmp をすべて許可するルールを作成し、適用します。(図 3-13)

コマンド例

```
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=icmp
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'","protocol":
"'$PROTCOL'","remote_ip_prefix": "'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

実行結果例


```
{
  "security_group_rule": {
  "remote_group_id": null,
  "direction": "ingress",
  "protocol": "icmp",
  "ethertype": "IPv4",
  "port_range_max": null,
  "security_group_id": "80b6deee-c4a8-4c33-805c-daf15c11786a",
  "tenant_id": "77b97024974140cf921bb40834a383d0",
  "port_range_min": null,
  "remote_ip_prefix": "0.0.0.0/0",
  "id": "becf6ee7-a63c-459e-89e8-58b728da9c50"
}
```


図 3-13：icmp 許可ルールを作成

■ VRRP を許可するルールを作成し、適用します。(冗長化機能を利用時の場合、作成)(図 3-14)

コマンド例

```
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=112 ※1
```

```
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'","protocol": "'$PROTOCOL'","remote_ip_prefix": "'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

※1 VRRP のプロトコル番号は 112 です。

実行結果例


```
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "ingress",
    "protocol": 112,
    "ethertype": "IPv4",
    "port_range_max": null,
    "security_group_id": "80b6deee-c4a8-4c33-805c-daf15c11786a",
    "tenant_id": "77b97024974140cf921bb40834a383d0",
    "port_range_min": null,
    "remote_ip_prefix": "0.0.0.0/0",
    "id": "41e802e6-c883-4f4f-b71d-ed74d3778712"
  }
}
```


図 3-14：VRRP 許可ルールを作成

3.5 アンチアフィニティの設定

IPCOM VA2 が冗長構成を組む場合は、異なるホスト上で動作するよう配置するために、アンチアフィニティの設定を行います。(図 3-15)

コマンド例

```
[root@K5-Host ]# NAME=IPCOM_VA2_ServerGr
[root@K5-Host ]# POLICY="anti-affinity"
[root@K5-Host ]# curl -s  $COMPUTE/v2/$PROJECT_ID/os-server-groups -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN"
-H "Content-Type:application/json" -d '{"server_group":{ "name": "'$NAME'", "policies": [ "'$POLICY'" ]}}'  |
jq .
```

実行結果例

```
{
  "server_group": {
    "members": [],
    "metadata": {},
    "id": "4a8bd960-688b-474f-83f9-e1ae72bf6cf6",
    "policies": [
      "anti-affinity"
    ],
    "name": "IPCOM_VA2_ServerGr"
  }
}
```

図 3-15：アンチアフィニティの設定

第 4 章 【LS/SC】仮想サーバの作成

本章では、IPCOM VA2 および関連する仮想サーバの作成手順について説明します。

［注意］

本章および次章の IPCOM VA2 仮想サーバの構築は、必ず記載されている手順どおりに実施してください。
トラブルや手順ミス等で継続できない場合、構築中の VA2 仮想サーバを破棄した上で本章からやり直してください。

4.1 【LS】IPCOM VA2 の作成(LS primary)

IPCOM VA2 LS の primary を作成します。アンチアフィニティで作成するので、API で実行してください。(図 4-1)

コマンド例

```
[root@K5-Host ~]# VM_NAME=IPCOM_VA2_LS_primary ※1
[root@K5-Host ~]# IMAGE_REF_ID=“IPCOM VA2 LS の ImageID”
[root@K5-Host ~]# FLAVOR_ID=“IPCOM VA2 LS の FlavorID” ※2
[root@K5-Host ~]# VOL_SIZE=2 ※3
[root@K5-Host ~]# DEVICE_NAME=/dev/vda ※4
[root@K5-Host ~]# SOURCE=image ※5
[root@K5-Host ~]# DESTINATION=volume ※6
[root@K5-Host ~]# ISDELETE=true ※7
[root@K5-Host ~]# INSTANCE_MAX=1 ※8
[root@K5-Host ~]# INSTANCE_MIN=1 ※9
[root@K5-Host ~]# NETWORK_ID1=“FrontNetwork の ID”
[root@K5-Host ~]# NETWORK_ID2=“BackNetwork の ID”
[root@K5-Host ~]# NETWORK_ID3=“ManagementNetwork の ID”
[root@K5-Host ~]# SG_NAME=“「SecurityGroup の作成で作成した」グループ名”
[root@K5-Host ~]# GROUP_ID=“アンチアフィニティの設定で作成したグループ ID” ※10
[root@K5-Host ~]# curl -k $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "imageRef": "", "flavorRef":
"'$FLAVOR_ID'","block_device_mapping_v2":[ {"boot_index": "0", "uuid":"'$IMAGE_REF_ID'", "volume_size":
"'$VOL_SIZE'", "device_name": "'$DEVICE_NAME'", "source_type": "'$SOURCE'", "destination_type":
"'$DESTINATION'", "delete_on_termination": "'$ISDELETE'"} ], "max_count": '$INSTANCE_MAX', "min_count":
'$INSTANCE_MIN', "networks": [{"uuid": "'$NETWORK_ID1'"},{"uuid": "'$NETWORK_ID2'"},{"uuid":
"'$NETWORK_ID3'"}], "security_groups": [{"name": "'$SG_NAME'"}]},"os:scheduler_hints": {"group":
"'$GROUP_ID'"}}'

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 【任意】名前は任意で指定してください。
※2 【固定】仮想サーバタイプ ID は、下記を選択してください。
    IPCOM VA2 1300 ; S3-1, S4-1S の ID(専有仮想サーバの場合、S3-1.d, S4-1S.d の ID)
    IPCOM VA2 2500 ; C3-4, C4-4S の ID(専有仮想サーバの場合、C3-4.d, C4-4S.d の ID)
※3 【固定】初回起動時のボリュームは 2GB 固定です。
※4 【固定】
※5 【固定】
※6 【固定】
※7 【任意】IPCOM VA2 の削除時にボリュームも削除する場合は指定してください。
※8 【固定】
```

※9 【固定】
※10 【任意】冗長構成を組む場合は、指定してください。

図 4-1: IPCOM VA2 の作成(LS primary)

4.2 【LS】IPCOM VA2 の作成(LS secondary)

IPCOM VA2 LS の secondary を作成します。アンチアフィニティで作成するので、API で実行してください。(図 4-2)

コマンド例

```
[root@K5-Host ~]# VM_NAME=IPCOM_VA2_LS_secondary ※1
[root@K5-Host ~]# IMAGE_REF_ID=“IPCOM VA2 LS の ImageID”
[root@K5-Host ~]# FLAVOR_ID=“IPCOM VA2 LS の FlavorID” ※2
[root@K5-Host ~]# VOL_SIZE=2 ※3
[root@K5-Host ~]# DEVICE_NAME=/dev/vda ※4
[root@K5-Host ~]# SOURCE=image ※5
[root@K5-Host ~]# DESTINATION=volume ※6
[root@K5-Host ~]# ISDELETE=true ※7
[root@K5-Host ~]# INSTANCE_MAX=1 ※8
[root@K5-Host ~]# INSTANCE_MIN=1 ※9
[root@K5-Host ~]# NETWORK_ID1=“FrontNetwork の ID”
[root@K5-Host ~]# NETWORK_ID2=“BackNetwork の ID”
[root@K5-Host ~]# NETWORK_ID3=“ManagementNetwork の ID”
[root@K5-Host ~]# SG_NAME=“「SecurityGroup の作成で作成した」グループ名”
[root@K5-Host ~]# GROUP_ID=“アンチアフィニティの設定で作成したグループ ID” ※10
[root@K5-Host ~]# curl -k $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "imageRef": "", "flavorRef":
"'$FLAVOR_ID'","block_device_mapping_v2":[ {"boot_index": "0", "uuid":"'$IMAGE_REF_ID'", "volume_size":
"'$VOL_SIZE'", "device_name": "'$DEVICE_NAME'", "source_type": "'$SOURCE'", "destination_type":
"'$DESTINATION'", "delete_on_termination": "'$ISDELETE'"} ], "max_count": '$INSTANCE_MAX', "min_count":
'$INSTANCE_MIN', "networks": [{"uuid": "'$NETWORK_ID1'"},{"uuid": "'$NETWORK_ID2'"},{"uuid":
"'$NETWORK_ID3'"}], "security_groups": [{"name": "'$SG_NAME'"}]},"os:scheduler_hints": {"group":
"'$GROUP_ID'"}}'

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 【任意】名前は任意で指定してください。
※2 【固定】仮想サーバタイプ ID は、下記を選択してください。
    IPCOM VA2 1300 ; S3-1, S4-1S の ID（専有仮想サーバの場合、S3-1.d, S4-1S.d の ID）
    IPCOM VA2 2500 ; C3-4, C4-4S の ID（専有仮想サーバの場合、C3-4.d, C4-4S.d の ID）
※3 【固定】初回起動時のボリュームは 2GB 固定です。
※4 【固定】
※5 【固定】
※6 【固定】
※7 【任意】IPCOM VA2 の削除時にボリュームも削除する場合は指定してください。
※8 【固定】
※9 【固定】
※10 【任意】冗長構成を組む場合は、指定してください。
```

図 4-2: IPCOM VA2 の作成(LS secondary)

4.3 【SC】IPCOM VA2 の作成(SC)

IPCOM VA2 SC を作成します。アンチアフィニティで作成するので、API で実行してください。(図 4-3)

コマンド例

```
[root@K5-Host ~]# VM_NAME=IPCOM_VA2_SC ※1
[root@K5-Host ~]# IMAGE_REF_ID=“IPCOM VA2 SC の ImageID”
[root@K5-Host ~]# FLAVOR_ID=“IPCOM VA2 LS の FlavorID” ※2
[root@K5-Host ~]# VOL_SIZE=2 ※3
[root@K5-Host ~]# DEVICE_NAME=/dev/vda ※4
[root@K5-Host ~]# SOURCE=image ※5
[root@K5-Host ~]# DESTINATION=volume ※6
[root@K5-Host ~]# ISDELETE=true ※7
[root@K5-Host ~]# INSTANCE_MAX=1 ※8
[root@K5-Host ~]# INSTANCE_MIN=1 ※9
[root@K5-Host ~]# NETWORK_ID1=“FrontNetwork の ID”
[root@K5-Host ~]# NETWORK_ID2=“ManagementNetwork の ID”
[root@K5-Host ~]# SG_NAME=“セキュリティグループ名”
[root@K5-Host ~]# GROUP_ID=“「アンチアフィニティの設定で」作成したグループ ID”
[root@K5-Host ~]# curl -k $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "imageRef": "", "flavorRef":
"'$FLAVOR_ID'","block_device_mapping_v2":[ {"boot_index": "0", "uuid":"'$IMAGE_REF_ID'", "volume_size":
"'$VOL_SIZE'", "device_name": "'$DEVICE_NAME'", "source_type": "'$SOURCE'", "destination_type":
"'$DESTINATION'", "delete_on_termination": "'$ISDELETE'"} ], "max_count": '$INSTANCE_MAX', "min_count":
'$INSTANCE_MIN', "networks": [{"uuid": "'$NETWORK_ID1'"},{"uuid": "'$NETWORK_ID2'"}], "security_groups":
[{"name": "'$SG_NAME'"}]},"os:scheduler_hints": {"group": "'$GROUP_ID'"}}'

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 【任意】名前は任意で指定してください。
※2 【固定】仮想サーバタイプ ID は、下記を選択してください。
    IPCOM VA2 1300 ; S3-1, S4-1S の ID（専有仮想サーバの場合、S3-1.d, S4-1S.d の ID）
    IPCOM VA2 2500 ; C3-4, C4-4S の ID（専有仮想サーバの場合、C3-4.d, C4-4S.d の ID）
※3 【固定】初回起動時のボリュームは 2GB 固定です。
※4 【固定】
※5 【固定】
※6 【固定】
※7 【任意】IPCOM VA2 の削除時にボリュームも削除する場合は指定してください。
※8 【固定】
※9 【固定】
※10 【任意】冗長構成を組む場合は、指定してください。
```

図 4-3: IPCOM VA2 の作成(SC)

4.4 負荷分散対象仮想サーバの作成

負荷分散対象の仮想サーバ(WebServer1、WebServer2)を作成します。(図 4-4)

以下は WebServer1 の作成例です。同様に WebServer2 も作成してください。※の部分以外はお客様の任意の値となります。

コマンド例

```
[root@K5-Host ~]# VM_NAME=WebServer1
[root@K5-Host ~]# IMAGE_REF_ID=“WebServer として利用したい任意の Image の ID”
[root@K5-Host ~]# FLAVOR_ID=“仮想サーバスペック ID 例 C3-2: 9719437f-0542-49b8-80d1-c89194f5bc52”
[root@K5-Host ~]# VOL_SIZE=“ボリュームサイズ(GB)”
[root@K5-Host ~]# DEVICE_NAME=/dev/vda
[root@K5-Host ~]# SOURCE=image
[root@K5-Host ~]# DESTINATION=volume
[root@K5-Host ~]# ISDELETE=true
[root@K5-Host ~]# KEYNAME=“キー名”
[root@K5-Host ~]# INSTANCE_MAX=1
[root@K5-Host ~]# INSTANCE_MIN=1
[root@K5-Host ~]# NETWORK_ID1=“BackNetwork の ID” ※1
[root@K5-Host ~]# NETWORK_ID2=“ManagementNetwork の ID” ※2
[root@K5-Host ~]# SG_NAME=“セキュリティグループ名”
[root@K5-Host ~]# GROUP_ID=“「アンチアフィニティの設定で」作成したグループ ID” ※3
[root@K5-Host ~]# curl -k $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "imageRef": "", "flavorRef": "'$FLAVOR_ID'","block_device_mapping_v2":[ {"boot_index": "0", "uuid":"'$IMAGE_REF_ID'", "volume_size": "'$VOL_SIZE'", "device_name": "'$DEVICE_NAME'", "source_type": "'$SOURCE'", "destination_type": "'$DESTINATION'", "delete_on_termination": "'$ISDELETE'"} ], "key_name": "'$KEYNAME'", "max_count": '$INSTANCE_MAX', "min_count": '$INSTANCE_MIN', "networks": [{"uuid": "'$NETWORK_ID1'"},{"uuid": "'$NETWORK_ID2'"}], "security_groups": [{"name": "'$SG_NAME'"}]},"os:scheduler_hints": {"group": "'$GROUP_ID'"}}'

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 前手順で作成した BackNetwork を指定してください。
※2 前手順で作成した ManagementNetwork を指定してください。
※3 前手順で作成したサーバグループを指定してください。
```

図 4-4: 負荷分散対象の仮想サーバの作成

4.5 保守用仮想サーバの作成

保守用の仮想サーバを作成します。以下は保守用仮想サーバの作成例です。※の部分以外はお客様の任意の値となります。

コマンド例と実行結果例

```
[root@K5-Host ~]# VM_NAME=MngVM
[root@K5-Host ~]# IMAGE_REF_ID=“イメージ ID”
[root@K5-Host ~]# FLAVOR_ID=“仮想サーバスペック ID”
[root@K5-Host ~]# VOL_SIZE=“ボリュームサイズ(GB)”
[root@K5-Host ~]# DEVICE_NAME=/dev/vda
[root@K5-Host ~]# SOURCE=image
[root@K5-Host ~]# DESTINATION=volume
[root@K5-Host ~]# ISDELETE=true
[root@K5-Host ~]# KEYNAME=“キーペアのキー名”
[root@K5-Host ~]# INSTANCE_MAX=1
[root@K5-Host ~]# INSTANCE_MIN=1
[root@K5-Host ~]# NETWORK_ID1=“FrontNetwork の ID” ※1
[root@K5-Host ~]# NETWORK_ID2=“ManagementNetwork の ID” ※2
[root@K5-Host ~]# SG_NAME=“セキュリティグループ名”
[root@K5-Host ~]# GROUP_ID=“「アンチアフィニティの設定」で作成したグループ ID” ※3
[root@K5-Host ~]# curl -k $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "imageRef": "", "flavorRef":
"'$FLAVOR_ID'","block_device_mapping_v2":[ {"boot_index": "0", "uuid":"'$IMAGE_REF_ID'", "volume_size":
"'$VOL_SIZE'", "device_name": "'$DEVICE_NAME'", "source_type": "'$SOURCE'", "destination_type":
"'$DESTINATION'", "delete_on_termination": "'$ISDELETE'"} ], "key_name": "'$KEYNAME'", "max_count":
'$INSTANCE_MAX', "min_count": '$INSTANCE_MIN', "networks": [{"uuid": "'$NETWORK_ID1'"},{"uuid":
"'$NETWORK_ID2'"}], "security_groups": [{"name": "'$SG_NAME'"}]},"os:scheduler_hints": {"group":
"'$GROUP_ID'"}}'

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 前手順で作成した FrontNetwork を指定してください。
※2 前手順で作成した ManagementNetwork を指定してください。
※3 前手順で作成したサーバグループを指定してください。
```

図 4-5: 保守用仮想サーバの作成

第 5 章 【LS/SC】ライセンス登録

本章では、IPCOM VA2 に対してライセンスを登録する手順を説明します。

5.1 【LS】IPCOM VA2 LS にリモートコンソールログイン

IPCOM VA2 LS にリモートコンソールログインし、以降の作業を実施します。

[注意]

リモートコンソール以外のリモートログイン(SSH、GUI)はデフォルトで無効です。セキュリティの観点から、7 章「ホスト名とパスワードの設定」にてお客様自身でパスワードを設定するまで、リモートログインの許可は行わないでください。

IaaS ポータルで対象の仮想サーバのアクションでリモートコンソールを指定し、リモートコンソールでログインします。(図 5-1,5-2)

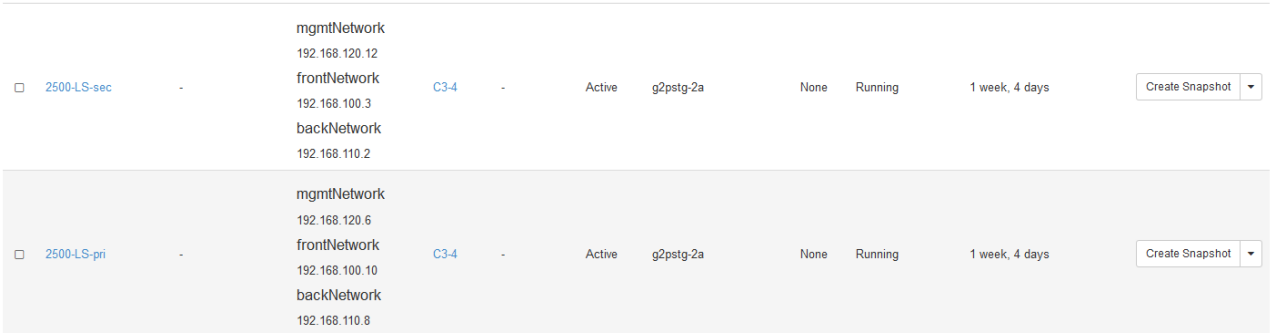


図 5-1：リモートコンソールへログイン

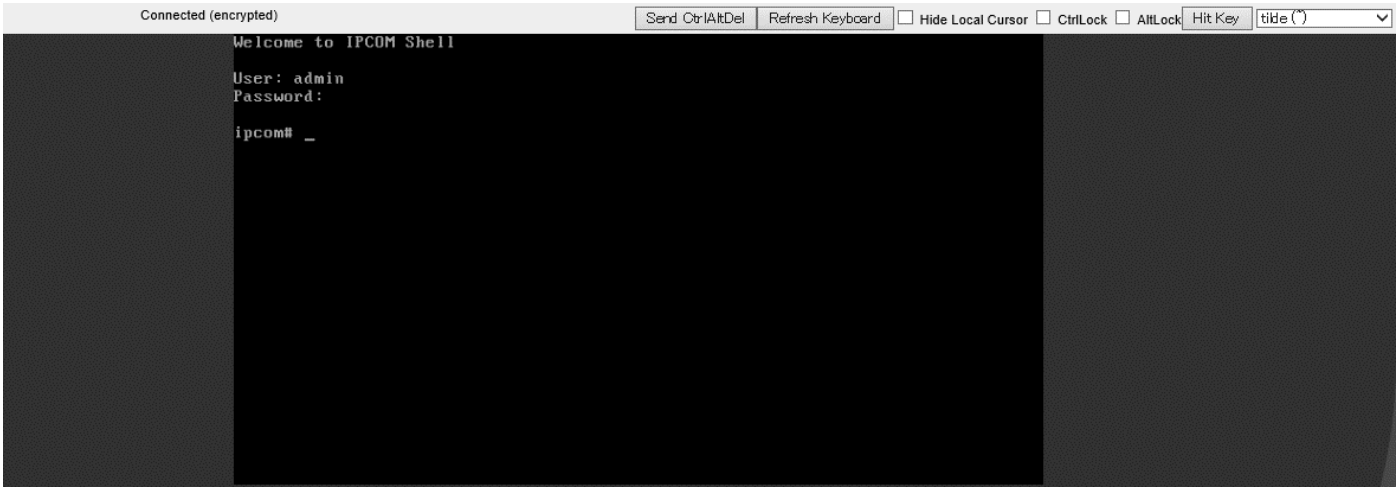


図 5-2：リモートコンソールへログイン後の画面

5.2【LS】IPCOM VA2 LS のライセンスキー登録

IPCOM VA2 LS 2 台にそれぞれリモートコンソールでログイン後、ライセンスキーを登録します。(図 5-3)

コマンド例
User: admin Password:(初期パスワードはデフォルトで設定されていないためそのままエンターキーを押下してください。) ipcom# license key 〈ライセンスキー〉 ipcom# poweroff ※1 ※1　ライセンスキー登録後、IPCOM VA2 をシャットダウンします。 ※本操作は Primary、Secondary それぞれ実施してください。

図 5-3：IPCOM VA2 LS のライセンス登録

[注意]

以降、「5.4【LS】追加ボリュームの作成およびアタッチ(secondary)」が完了するまで、IPCOM VA2 の再起動を行わないでください。追加ボリュームへのアタッチができなくなります。

5.3【LS】追加ボリュームの作成およびアタッチ(LS primary)

Primary 側の IPCOM VA2 LS のシステム用ボリュームを作成し、アタッチします。

① 以下の値でストレージを primary のシステムボリュームとして 1 つ作成してください。(図 5-4)

- 種別：M2 または M2.d (専有ブロックストレージ機能専用)
- 容量：100GB(固定)
- ストレージソース：空のボリューム

※その他の値については任意です

コマンド例

```
[root@K5-Host ]# NAME=ipcom_va2_LS_pri_vol ※1
[root@K5-Host ]# SIZE=100 ※2
[root@K5-Host ]# curl -X POST -s $BLOCKSTORAGE/v2/$PROJECT_ID/volumes -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"volume":{"name": "'$NAME'", "size": "'$SIZE'"}}' | jq .
```

※1 名前は任意です。
※2 ボリュームサイズは 100GB 固定です。

実行結果例

```
{
  "volume": {
    "status": "creating",
    "user_id": "cf29bf6ba54f479e93ba7938961d7b01",
    "attachments": [],
    "links": [
      {
        "href":
"http://10.3.0.201/v2/77b97024974140cf921bb40834a383d0/volumes/b5872d8a-a6fa-446e-91b6-3cff5f448e1c",
        "rel": "self"
      },
      {
        "href":
"http://10.3.0.201/77b97024974140cf921bb40834a383d0/volumes/b5872d8a-a6fa-446e-91b6-3cff5f448e1c",
        "rel": "bookmark"
      }
    ],
    "availability_zone": "jp-east-1a",
    "bootable": "false",
    "encrypted": false,
    "created_at": "2017-04-21T00:47:14.991210",
    "description": null,
    "volume_type": "M2",
    "name": "ipcom_va2_LS_pri_vol",
    "source_volid": null,
    "snapshot_id": null,
    "metadata": {
      "readonly": "False"
    },
    "id": "b5872d8a-a6fa-446e-91b6-3cff5f448e1c",
    "size": 100
  }
}
```

図 5-4：システムボリューム作成(LS primary 側)

② ストレージ作成完了後、停止している IPCOM VA2 LS の primary にアタッチしてください。(図 5-5)

コマンド例

```
[root@K5-Host ]# DEVICE=/dev/vdb
[root@K5-Host ]# SERVER_ID="IPCOM VA2 LS primary のサーバ ID"
[root@K5-Host ]# VOLUME_ID="①で作成したボリュームの ID"
[root@K5-Host ]# curl -s -X POST $COMPUTE/v2/$TENANT_ID/servers/$SERVER_ID/os-volume_attachments -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"volumeAttachment": {"volumeId": "'$VOLUME_ID'","device": "'$DEVICE'"}}' | jq .
```

実行結果例

```
{
  "volumeAttachment": {
    "device": "/dev/vdb",
    "serverId": "eaf95c2a-8995-45c7-9915-0dd3acc79a44",
    "id": "b5872d8a-a6fa-446e-91b6-3cff5f448e1c",
    "volumeId": "b5872d8a-a6fa-446e-91b6-3cff5f448e1c"
  }
}
```

図 5-5：システムボリュームのアタッチ(LS primary 側)

5.4 【LS】追加ボリュームの作成およびアタッチ(LS secondary)

primary 側と同様に、secondary 側 IPCOM VA2 LS のシステム用ボリュームを作成し、アタッチします。

① 以下の値でストレージを secondary のシステムボリュームとして 1 つ作成してください。(図 5-6)

- 種別：M2 または M2.d (専有ブロックストレージ機能専用)
- 容量：100GB(固定)
- ストレージソース：空のボリューム

※その他の値については任意です

コマンド例

```
[root@K5-Host ]# NAME=ipcom_va2_LS_sco_vol ※1
[root@K5-Host ]# SIZE=100 ※2
[root@K5-Host ]# curl -X POST -s $BLOCKSTORAGE/v2/$PROJECT_ID/volumes -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"volume":{"name": "'$NAME'", "size": "'$SIZE'"}}' | jq .
```

※1 名前は任意です。
※2 ボリュームサイズは 100GB 固定です。

実行結果例


```
{
  "volume": {
    "status": "creating",
    "user_id": "cf29bf6ba54f479e93ba7938961d7b01",
    "attachments": [],
    "links": [
      {
        "href":
"http://10.3.0.201/v2/77b97024974140cf921bb40834a383d0/volumes/ff82504e-30fc-41dc-b6ee-66556db66318",
        "rel": "self"
      },
      {
        "href":
"http://10.3.0.201/77b97024974140cf921bb40834a383d0/volumes/ff82504e-30fc-41dc-b6ee-66556db66318",
        "rel": "bookmark"
      }
    ],
    "availability_zone": "jp-east-1a",
    "bootable": "false",
    "encrypted": false,
    "created_at": "2017-04-21T00:55:41.336729",
    "description": null,
    "volume_type": "M2",
    "name": "ipcom_va2_LS_sco_vol",
    "source_volid": null,
    "snapshot_id": null,
    "metadata": {
      "readonly": "False"
    },
    "id": "ff82504e-30fc-41dc-b6ee-66556db66318",
    "size": 100
  }
}
```


図 5-6：システムボリューム作成(LS secondary 側)

② ストレージ作成完了後、停止している IPCOM VA2 の secondary にアタッチしてください。(図 5-7)

コマンド例

```
[root@K5-Host ~]# DEVICE=/dev/vdb
[root@K5-Host ~]# SERVER_ID="IPCOM VA2 LS secondary のサーバ ID"
[root@K5-Host ~]# VOLUME_ID="①で作成したボリュームの ID"
[root@K5-Host ~]# curl -s -X POST $COMPUTE/v2/$TENANT_ID/servers/$SERVER_ID/os-volume_attachments -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"volumeAttachment": {"volumeId": "'$VOLUME_ID'","device": "'$DEVICE'"}}' | jq .
```

実行結果例

```
{
  "volumeAttachment": {
    "device": "/dev/vdb",
    "serverId": "28c8d1c1-7866-466b-acf6-b5d69e8b0317",
    "id": "ff8250d4e-30fc-41dc-b6ee-66556db66318",
    "volumeId": "ff8250d4e-30fc-41dc-b6ee-66556db66318"
  }
}
```

図 5-7：システムボリュームのアタッチ(LS secondary 側)

5.5【LS】IPCOM VA2 LS の起動

停止している IPCOM VA2 LS を起動します。(図 5-8)

IPCOM VA2 の起動は①primary、②secondary の順番に実施してください。

ライセンス登録後の起動は boot 時にディスクフォーマットをするため、起動に 5 分程度かかります。

図 5-8：IPCOM VA2 の起動

ここからは IPCOM VA2 SC に対してライセンス登録を行います。

5.6 【SC】IPCOM VA2 SC にリモートコンソールログイン

IPCOM VA2 SC にリモートコンソールログインし、以降の作業を実施します。

[注意]

リモートコンソール以外のリモートログイン(SSH、GUI)はデフォルトで無効です。セキュリティの観点から、12 章「ホスト名とパスワードの設定」にてお客様自身でパスワードを設定するまで、リモートログインの許可は行わないでください。

IaaS ポータルで対象の仮想サーバのアクションでリモートコンソールを指定し、リモートコンソールでログインします。(図 5-9,5-10)

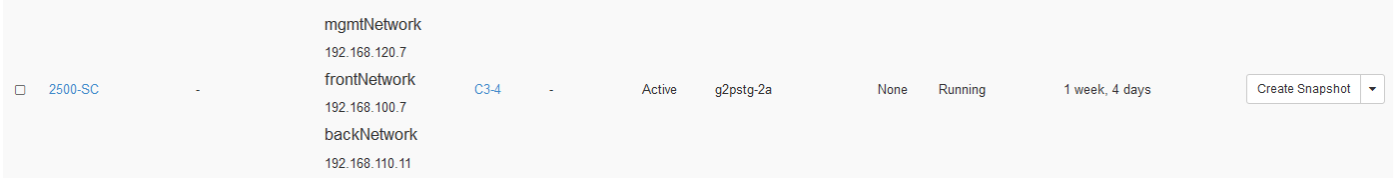


図 5-9：リモートコンソールでログイン

図 5-10：リモートコンソールでログイン後の画面

5.7【SC】IPCOM VA2 SC のライセンスキー登録

IPCOM VA2 SC にリモートコンソールでログイン後、ライセンスキーを登録します。(図 5-11)

コマンド例
User: admin Password:(初期パスワードはデフォルトで設定されていないためそのままエンターキーを押下してください。) ipcom# license key〈ライセンスキー〉 ipcom# poweroff ※1 ※1 ライセンスキー登録後、IPCOM VA2 SC をシャットダウンします

図 5-11：IPCOM VA2 SC のライセンス登録

[注意]

以降、「5.8【SC】追加ボリュームの作成およびアタッチ(SC)」が完了するまで、IPCOM VA2 の再起動を行わないでください。追加ボリュームへのアタッチができなくなります。

5.8【SC】追加ボリュームの作成およびアタッチ(SC)

IPCOM VA2 SC のシステム用ボリュームを作成し、アタッチします。

① 以下の値でストレージを IPCOM VA2 SC のシステムボリュームとして 1 つ作成してください。(図 5-12)

- 種別：M2 または M2.d (専有ブロックストレージ機能専用)
- 容量：100GB(固定)
- ストレージソース：空のボリューム

※その他の値については任意です

コマンド例

```
[root@K5-Host ]# NAME=ipcom_va2_LS_SC_vol ※1
[root@K5-Host ]# SIZE=100 ※2
[root@K5-Host ]# curl -X POST -s $BLOCKSTORAGE/v2/$PROJECT_ID/volumes -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"volume":{"name": "'$NAME'", "size": "'$SIZE'"}}' | jq .
```

※1 名前は任意です。
※2 ボリュームサイズは 100GB 固定です。

実行結果例

```
{
  "volume": {
    "status": "creating",
    "user_id": "cf29bf6ba54f479e93ba7938961d7b01",
    "attachments": [],
    "links": [
      {
        "href":
"http://10.3.0.201/v2/77b97024974140cf921bb40834a383d0/volumes/e9a9f4e5-56f4-4436-b77f-84f5e6eeebc7",
        "rel": "self"
      },
      {
        "href":
"http://10.3.0.201/77b97024974140cf921bb40834a383d0/volumes/e9a9f4e5-56f4-4436-b77f-84f5e6eeebc7",
        "rel": "bookmark"
      }
    ],
    "availability_zone": "jp-east-1a",
    "bootable": "false",
    "encrypted": false,
    "created_at": "2017-04-21T01:36:51.325182",
    "description": null,
    "volume_type": "M2",
    "name": "ipcom_va2_SC_vol",
    "source_volid": null,
    "snapshot_id": null,
    "metadata": {
      "readonly": "False"
    },
    "id": "e9a9f4e5-56f4-4436-b77f-84f5e6eeebc7",
    "size": 100
  }
}
```

図 5-12：システムボリューム作成(SC)

② ストレージ作成完了後、停止している IPCOM VA2 SC にアタッチしてください。(図 5-13)

コマンド例

```
[root@K5-Host ]# DEVICE=/dev/vdb
[root@K5-Host ]# SERVER_ID="IPCOM VA2 SC のサーバ ID"
[root@K5-Host ]# VOLUME_ID="①で作成したボリュームの ID"
[root@K5-Host ]# curl -s -X POST $COMPUTE/v2/$TENANT_ID/servers/$SERVER_ID/os-volume_attachments -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"volumeAttachment": {"volumeId": "'$VOLUME_ID'","device": "'$DEVICE'"}}' | jq .
```

実行結果例

```
{
  "volumeAttachment": {
    "device": "/dev/vdb",
    "serverId": "d8d4295a-c689-432b-866d-c6ef07f09d14",
    "id": "e9a9f4e5-56f4-4436-b77f-84f5e6eeebc7",
    "volumeId": "e9a9f4e5-56f4-4436-b77f-84f5e6eeebc7"
  }
}
```

図 5-13：システムボリュームのアタッチ(SC)

5.9【SC】IPCOM VA2 SC の起動

停止している IPCOM VA2 SC を起動します。(図 5-14)

ライセンス登録後の起動は boot 時にディスクフォーマットをするため、起動に 5 分程度かかります。

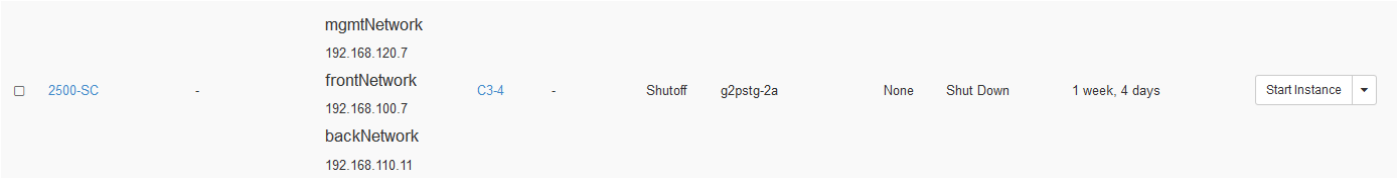


図 5-14：IPCOM VA2 SC の起動

第 6 章 【LS】ルーティング許可の設定

本章では、IPCOM VA2 をルータとして利用する場合の設定について説明します。
本例では IPCOM VA2 LS がルーティングを実行するため、LS2 台に対して設定する例を記載しております。

6.1 ルーティング許可の設定

API を利用し、作成した IPCOM VA2 のポートすべてに対してルーティングを許可する設定を行います。

本設定を行わない場合、IPCOM VA2 のルータ機能が正常に動作しないため、必ず本設定を実施してください。

本例のルーティング許可の設定パラメータ値は、「東日本第 1/第 2、西日本第 1/第 2 リージョン」向けの設定パラメータとは一部異なります。詳細は、以下の (1) LS primary への設定(図 6-1)、(2) LS secondary への設定(図 6-2) を参照してください。

(1) LS primary への設定(図 6-1)

コマンド例

```
[root@K5-Host ]# PORT_ID= “FrontNetwork のポート ID”
[root@K5-Host ]# PORT_address1= “0.0.0.0/0”   ※1
[root@K5-Host ]# PORT_address2= “FrontNetwork の代表 IP アドレス”   ※1
[root@K5-Host ]# PORT_address3= “FrontNetwork の仮想 IP アドレス”   ※1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address": "'$PORT_address1'"},{"ip_address": "'$PORT_address2'"},{"ip_address": "'$PORT_address3'"}]}}' | jq .

[root@K5-Host ]# PORT_ID= “BackNetwork のポート ID”
[root@K5-Host ]# PORT_address1 = “0.0.0.0/0”   ※1
[root@K5-Host ]# PORT_address2 = “BackNetwork の代表 IP アドレス”   ※1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address": "'$PORT_address1'"},{"ip_address": "'$PORT_address2'"}]}}' | jq .

[root@K5-Host ]# PORT_ID= “ManagementNetwork のポート ID”
[root@K5-Host ]# PORT_address1 = “0.0.0.0/0”   ※1
[root@K5-Host ]# PORT_address2 = “ManagementNetwork の代表 IP アドレス”   ※1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":{"allowed_address_pairs":  [{"ip_address":  "'$PORT_address1'"},{"ip_address": "'$PORT_address2'"}]}}' | jq .
```

※1　このパラメータの内容は「東日本第 1/第 2,西日本第 1/第 2 リージョン」向けのスタートガイドと異なります。「東日本第 3,西日本第 3 リージョン」では上記の内容で設定して下さい。

図 6-1：IPCOM VA2 LS primary へのルーティング許可の設定

(2) LS secondary への設定(図 6-2)

コマンド例

```
[root@K5-Host ]# PORT_ID= “FrontNetwork のポート ID”
[root@K5-Host ]# PORT_address1= “0.0.0.0/0”   ※1
[root@K5-Host ]# PORT_address2= “FrontNetwork の代表 IP アドレス”   ※1
[root@K5-Host ]# PORT_address3= “FrontNetwork の仮想 IP アドレス”   ※1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address": "'$PORT_address1'"},{"ip_address":
"'$PORT_address2'"},{"ip_address": "'$PORT_address3'"}]}}' | jq .

[root@K5-Host ]# PORT_ID= “BackNetwork のポート ID”
[root@K5-Host ]# PORT_address1 = “0.0.0.0/0”   ※1
[root@K5-Host ]# PORT_address2 = “BackNetwork の代表 IP アドレス”   ※1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address": "'$PORT_address1'"},{"ip_address":
"'$PORT_address2'"}]}}' | jq .

[root@K5-Host ]# PORT_ID= “ManagementNetwork のポート ID”
[root@K5-Host ]# PORT_address1 = “0.0.0.0/0”   ※1
[root@K5-Host ]# PORT_address2 = “ManagementNetwork の代表 IP アドレス”   ※1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json"   -d   '{"port":{"allowed_address_pairs":   [{"ip_address":   "'$PORT_address1'"},{"ip_address":
"'$PORT_address2'"}]}}' | jq .
```

※1　このパラメータの内容は「東日本第 1/第 2,西日本第 1/第 2 リージョン」向けのスタートガイドと異なります。「東日本第 3,西日本第 3 リージョン」では上記の内容で設定して下さい。

図 6-2：IPCOM VA2 LS secondary へのルーティング許可の設定

第 7 章 【LS】IPCOM VA2 LS の初期設定

本章では、IPCOM VA2 の初期設定や、冗長化構成の設定について説明します。

7.1 ホスト名とパスワードの設定(LS primary)

LS primary の IPCOM VA2 にリモートコンソールログインをしてホスト名とパスワードを設定します。(図 7-1)

[注意]

admin パスワード設定は必ず実施してください。またリモートアクセス許可は admin パスワード設定後に実施してください。

コマンド例

```
ipcom# configure
ipcom(config)# load running-config
ipcom(edit)# user admin
ipcom(edit-user)# password “任意の password” ※1
ipcom(edit-user)# exit
ipcom(edit)# hostname vipcom-pri vipcom-sco ※2
ipcom(edit)#  user-role remote
ipcom(edit-user-role)# match user admin ※3
ipcom(edit-user-role)# exit
ipcom(edit)# commit force-update
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):y

※1  パスワードは簡単に推測されない文字列を設定してください。(8 文字以上かつ英数字記号を混在した文字列を推奨)
※2  ホスト名は以下の順番で指定してください。
     hostname “primary のホスト名” “secondary のホスト名”
※3  パスワードを設定したため、admin ユーザーの remote アクセスを許可します。
```

図 7-1：ホスト名とパスワードの設定(LS primary)

[SSH 接続時の留意点]

ライセンス登録前に保守用の仮想サーバ等から IPCOM VA2 へ SSH ログインを試みていた場合、ライセンス登録後に同じ仮想サーバから SSH ログインすると以下のような表示が出力されます。本表示が出た場合、ログインを試みたユーザーの「/ユーザー名/.ssh/known_hosts」の該当の IP アドレス(本例では 192.168.100.10)の行を削除してください。

表示例

```
[root@mngvm k5user]# ssh admin@192.168.100.10
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
30:b6:0f:bd:04:d8:bd:7b:66:4c:38:9f:b8:d4:e9:e0.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending RSA key in /root/.ssh/known_hosts:3
RSA host key for 192.168.100.10 has changed and you have requested strict checking.
Host key verification failed.
```

図 7-2：ライセンス登録後の SSH ログイン時の留意事項

7.2 インターフェースと冗長化設定(LS primary)

LS primary の IPCOM VA2 のインターフェースと冗長化の設定を行います。(図 7-3)

コマンド例

```
vipcom-pri> admin
vipcom-pri# configure
vipcom-pri(config)# load running-config
vipcom-pri(edit)# protect checksum-inspection disable ※1
vipcom-pri(edit)# cluster mode primary
vipcom-pri(edit)# cluster id 1  ※2
vipcom-pri(edit)# cluster secret-key vipcom ※3
vipcom-pri(edit)# interface lan0.0
vipcom-pri(edit-if)# ip address 192.168.100.100 255.255.255.0 ※4
vipcom-pri(edit-if)# ip address primary 192.168.100.10 ※5
vipcom-pri(edit-if)# ip address secondary 192.168.100.20 ※6
vipcom-pri(edit-if)# description IPCOM-VA2-front-net ※7
vipcom-pri(edit-if)# mtu 8950 ※8
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 10 ※9
vipcom-pri(edit-if)# exit

vipcom-pri(edit)# interface lan0.1
vipcom-pri(edit-if)# ip address 192.168.110.100 255.255.255.0
vipcom-pri(edit-if)# ip address primary 192.168.110.10 ※10
vipcom-pri(edit-if)# ip address secondary 192.168.110.20 ※11
vipcom-pri(edit-if)# description IPCOM-VA2-back-net ※12
vipcom-pri(edit-if)# mtu 8950 ※13
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 20 ※14
vipcom-pri(edit-if)# exit

vipcom-pri(edit)#  interface lan0.2
vipcom-pri(edit-if)# ip address 192.168.120.100 255.255.255.0 ※15
vipcom-pri(edit-if)# ip address primary 192.168.120.10 ※16
vipcom-pri(edit-if)# ip address secondary 192.168.120.20 ※17
vipcom-pri(edit-if)# description IPCOM-VA2-management-net ※18
vipcom-pri(edit-if)# mtu 8950 ※19
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 30 ※20
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# ip route 0.0.0.0/0 192.168.100.1 distance 2  ※21
vipcom-pri(edit)# save startup-config
Do you overwrite  “startup-config”  by the current configuration? (y|[n]):y
vipcom-pri(edit)# reset
Restarting of the system disconnects all communications. Are you sure?(y|[n]):y

※1  パケットのチェックを行う機能は K5 上では使用しないでください。予期せぬ動作が起こる場合があります。
※2  id は primary、secondary で同一 id を設定してください。
※3  secret-key は primary、secondary で同一の値を設定してください。
※4  代表 IP アドレスを設定
※5  K5 で割当された primary の FrontNetwork 側の IP アドレスを指定してください
※6  K5 で割当された secondary の FrontNetwork 側の IP アドレスを指定してください
※7  説明文のため任意です
```

※8　IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※9　lan0.0 の vrid は primary、secondary で同じ値を設定してください。
※10 K5 で割当された primary の BackNetwork 側の IP アドレスを指定してください
※11 K5 で割当された secondary の BackNetwork 側の IP アドレスを指定してください
※12 説明文のため任意です
※13 IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※14 lan0.1 の vrid は primary、secondary で同じ値を設定してください。
※15 代表 IP アドレスを設定
※16 K5 で割当された primary の Management　Network 側 IP アドレスを指定してください
※17 K5 で割当された secondary の Management Network 側の IP アドレスを指定してください
※18 説明文のため任意です
※19 IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※20 lan0.2 の vrid は primary、secondary で同じ値を設定してください。
※21 仮想ルータのインターフェースをデフォルトゲートウェイに設定します。

図 7-3：インターフェースと冗長化設定(LS primary)

7.3 ホスト名とパスワードの設定(LS secondary)

LS secondary の IPCOM VA2 にリモートコンソールログインをしてホスト名とパスワードを設定します。(図 7-4)

コマンド例

```
ipcom# configure
ipcom(config)# load running-config
ipcom(edit)# user admin
ipcom(edit-user)# password “任意の password” ※1
ipcom(edit-user)# exit
ipcom(edit)# hostname vipcom-pri vipcom-sco ※2
ipcom(edit)#  user-role remote
ipcom(edit-user-role)# match user admin ※3
ipcom(edit-user-role)# exit
ipcom(edit)# commit force-update
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):y

※1 パスワードは簡単に推測されない文字列を設定してください。(8 文字以上かつ英数字記号を混在した文字列を推奨)
※2 ホスト名は以下の順番で記載してください。
    hostname “primary のホスト名” “secondary のホスト名”
※3 パスワードを設定したため、admin ユーザーの remote アクセスを許可します。
```

図 7-4：ホスト名とパスワードの設定(LS secondary)

7.4 インターフェースと冗長化設定(LS secondary)

LS secondary の IPCOM VA2 のインターフェースと冗長化の設定を行います。(図 7-5)

コマンド例

```
vipcom-pri(edit)# protect checksum-inspection disable ※1
vipcom-pri(edit)# cluster mode secondary
vipcom-pri(edit)# cluster id 1  ※2
vipcom-pri(edit)# cluster secret-key vipcom※3
vipcom-pri(edit)# interface lan0.0
vipcom-pri(edit-if)# ip address 192.168.100.100 255.255.255.0 ※4
vipcom-pri(edit-if)# ip address primary 192.168.100.10 ※5
vipcom-pri(edit-if)# ip address secondary 192.168.100.20 ※6
vipcom-pri(edit-if)# description IPCOM-VA2-front-net ※7
vipcom-pri(edit-if)# mtu 8950 ※8
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 10 ※9
vipcom-pri(edit-if)# exit

vipcom-pri(edit)# interface lan0.1
vipcom-pri(edit-if)# ip address 192.168.110.100 255.255.255.0
vipcom-pri(edit-if)# ip address primary 192.168.110.10 ※10
vipcom-pri(edit-if)# ip address secondary 192.168.110.20 ※11
vipcom-pri(edit-if)# description IPCOM-VA2-back-net ※12
vipcom-pri(edit-if)# mtu 8950 ※13
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 20 ※14
vipcom-pri(edit-if)# exit

vipcom-pri(edit)#  interface lan0.2
vipcom-pri(edit-if)# ip address 192.168.120.100 255.255.255.0 ※15
vipcom-pri(edit-if)# ip address primary 192.168.120.10 ※16
vipcom-pri(edit-if)# ip address secondary 192.168.120.20 ※17
vipcom-pri(edit-if)# description IPCOM-VA2-management-net ※18
vipcom-pri(edit-if)# mtu 8950 ※19
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 30 ※20
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# ip route 0.0.0.0/0 192.168.100.1 distance 2  ※21
vipcom-pri(edit)# save startup-config
Do you overwrite "startup-config" by the current configuration? (y|[n]):y
vipcom-pri(edit)# reset
Restarting of the system disconnects all communications. Are you sure?(y|[n]):y

※1  パケットのチェックを行う機能は K5 上では使用しないでください。予期せぬ動作が起こる場合があります。
※2  id は primary、secondary で同一 id を設定してください。
※3  secret-key は primary、secondary で同一の値を設定してください。
※4  代表 IP アドレスを設定
※5  K5 で割当された primary の FrontNetwork 側の IP アドレスを指定してください
※6  K5 で割当された secondary の FrontNetwork 側の IP アドレスを指定してください
※7  説明文のため任意です
※8  IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※9  lan0.0 の vrid は primary、secondary で同じ値を設定してください。
※10 K5 で割当された primary の BackNetwork 側の IP アドレスを指定してください
```

※11 K5 で割当された secondary の BackNetwork 側の IP アドレスを指定してください
※12 説明文のため任意です。
※13 IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※14 lan0.1 の vrid は primary、secondary で同じ値を設定してください。
※15 代表 IP アドレスを設定
※16 K5 で割当された primary の Management Network 側の IP アドレスを指定してください
※17 K5 で割当された secondary の Management Network 側の IP アドレスを指定してください
※18 説明文のため任意です
※19 IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※20 lan0.2 の vrid は primary、secondary で同じ値を設定してください。
※21 仮想ルータのインターフェースをデフォルトゲートウェイに設定します。

図 7-5：インターフェースと冗長化設定(LS secondary)

7.5 冗長化設定の確認

primary または secondary で IPCOM VA2 の冗長化設定が正しく設定できているか確認します。

IPCOM VA2 に SSH ログインして以下のコマンドを実行し、対向ノードを正しく認識しているか確認します。(図 7-6)

※本作業は primary/secondary どちらでも実施可能です

コマンド例

```
vipcom-pri> admin
vipcom-pri# show cluster
```

実行結果例

```
MAC/IP Address Information:
--------------------  -----------------  ---------------
Interface             MAC Address        IP Address
--------------------  -----------------  ---------------
lan0.0      Delegate  00:00:5e:00:01:0a  192.168.100.100
lan0.0      Local     fa:16:3e:d9:66:15  192.168.100.10
lan0.0      Peer      fa:16:3e:e0:8d:5b  192.168.100.20
--------------------  -----------------  ---------------
lan0.1      Delegate  00:00:5e:00:01:14  192.168.110.100
lan0.1      Local     fa:16:3e:b1:ac:f8  192.168.200.10
lan0.1      Peer      fa:16:3e:c9:22:2e  192.168.200.20
--------------------  -----------------  ---------------
lan0.2      Delegate  00:00:5e:00:01:1e  192.168.120.100
lan0.2      Local     fa:16:3e:45:d0:c9  192.168.120.10
lan0.2      Peer      fa:16:3e:94:b9:aa  192.168.120.20
--------------------  -----------------  ---------------
```

【確認ポイント】
Local と Peer の IP/MAC アドレスが正しく表示されているかご確認ください。
表示されていない場合、セキュリティグループの設定で VRRP(112)が許可されていない可能性があります。セキュリティグループが正しく設定されていることをご確認ください。

図 7-6：冗長化設定の確認

第 8 章 【LS】IPCOM VA2 LS のファイアーウォール機能の設定

本章では、IPCOM VA2 LS におけるファイアーウォールの設定手順を説明します。

8.1 ファイアーウォールの設定

ファイアーウォールを設定するため、primary 側 IPCOM VA2 LS でルール作成およびインターフェースへのルール設定を行います。

本設定例では、FrontNetwork と BackNetwork に http(80)・https(443)・dns(53)の許可、また BackNetwork のみ負荷分散対象の仮想サーバを監視するため icmp の許可、ManagemantNetwork には保守用仮想サーバからの SSH アクセスのみ許可します。

① primary 側 IPCOM VA2 でファイアーウォールのルールを作成します。(図 8-1)

コマンド例

```
vipcom-pri> admin
vipcom-pri# con
vipcom-pri(config)# load running-config
vipcom-pri(edit)# access-control default-deny※1
vipcom-pri(edit)# no access-control configuration ※2
All the definitions for the access control map are deleted if the access control
rule is changed to enable. Are you sure?(y|[n]):y
vipcom-pri(edit)# class-map match-any web-access ※3
vipcom-pri(edit-cmap)# match destination-port 80/tcp
vipcom-pri(edit-cmap)# match destination-port 443/tcp
vipcom-pri(edit-cmap)# exit
vipcom-pri(edit)# class-map match-all ping-moniter ※4
vipcom-pri(edit-cmap)# match icmp ping
vipcom-pri(edit-cmap)# exit
vipcom-pri(edit)# class-map match-all dns-access ※5
vipcom-pri(edit-cmap)# match destination-port 53/udp
vipcom-pri(edit-cmap)# exit
vipcom-pri(edit)# class-map match-all mng-access ※6
vipcom-pri(edit-cmap)# match destination-port 22/tcp
vipcom-pri(edit-cmap)# match source-address ip 192.168.120.30 ※7
vipcom-pri(edit-cmap)# exit
vipcom-pri(edit)# class-map match-all webconsole-access ※8
vipcom-pri(edit-cmap)# match destination-port 82/tcp
vipcom-pri(edit-cmap)# match source-address ip 192.168.120.30 ※9
vipcom-pri(edit-cmap)# exit

※1 rule に該当しないものはすべて破棄します。
※2 access control rule を有効にします。
※3 HTTP(80)、HTTPS(443)をルールに指定します。
※4 icmp(ping)をルールに指定
※5 DNS(53)をルールに指定
※6 保守用仮想サーバから SSH アクセスを許可するようルールに指定します
※7 保守用仮想サーバの Management Network の IP アドレスを指定します。
※8 IPCOM VA2 の GUI(82 番ポート)へアクセスするルールを指定します。
※9 保守用仮想サーバからのアクセスのみ許可します。
```

図 8-1：ファイアーウォールルール作成

② 作成したファイアーウォールのルールをインターフェースに指定します。(図 8-2)

コマンド例

```
vipcom-pri(edit)# interface lan0.0
vipcom-pri(edit-if)# rule access 100 in web-access accept audit-session-normal audit-match-normal ※1
vipcom-pri(edit-if)# rule access 110 out web-access accept audit-session-normal audit-match-normal ※2
vipcom-pri(edit-if)# rule access 120 out dns-access  accept audit-session-normal audit-match-normal ※3
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# interface lan0.1
vipcom-pri(edit-if)# rule access 100 in web-access accept audit-session-normal audit-match-normal ※4
vipcom-pri(edit-if)# rule access 110 out web-access accept audit-session-normal audit-match-normal ※5
vipcom-pri(edit-if)# rule access 120 in dns-access  accept audit-session-normal audit-match-normal ※6
vipcom-pri(edit-if)# rule access 130 out ping-moniter accept audit-session-normal audit-match-normal ※7
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# interface lan0.2
vipcom-pri(edit-if)# rule access 100 in mng-access accept audit-session-normal audit-match-normal ※8
vipcom-pri(edit-if)# rule access 110 in webconsole-access accept audit-session-normal audit-match-normal ※9
vipcom-pri(edit-if)# rule access 120 out any accept audit-session-normal audit-match-normal ※10
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# commit
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):n
vipcom-pri(edit)# exit
vipcom-pri(config)#exit

※1  インバウンドの web アクセス許可
※2  アウトバウンドの web アクセス許可
※3  アウトバウンドへの DNS アクセス許可
※4  インバウンドの web アクセス許可
※5  アウトバウンドの web アクセス許可
※6  インバウンドの DNS アクセス許可
※7  アウトバウンドの icmp(ping)を許可
※8  保守用仮想サーバからの SSH アクセス許可
※9  保守用仮想サーバからの WebConsole(82)許可
※10  アウトバウンドはすべて許可
```

図 8-2：ファイアーウォールのルールをインターフェースに適用

rule access コマンドにて audit-session-noramal / audit-match-normal 設定したログを出力する際には、logging collection-level コマンドにてログレベルを設定して下さい。なお、詳細については、以下のマニュアルを参照して下さい。

IPCOM EX シリーズコマンドリファレンスガイド

2.1.2.12 logging collection-level

2.16.2.6.1 rule access

8.2 ファイアーウォールの設定を secondary に同期

primary で設定したコンフィグを secondary に同期します。(図 8-3)

コマンド例
vipcom-pri# sync cluster primary-to-secondary This System: primary primary (2017/01/25(Wed)16:44:42) -> secondary(2017/01/24(Tue)18:27:11) Are you sure? (y|[n]):y

図 8-3：ファイアーウォールの設定を secondary に同期

第 9 章 【LS】IPCOM VA2 LS の負荷分散機能の設定

本章では、IPCOM VA2 の負荷分散機能の設定手順を説明します。

9.1 負荷分散機能の設定(LS primary)

primary 側 IPCOM VA2 LS で負荷分散ルールを作成します。

secondary 側 IPCOM VA2 LS の負荷分散機能設定は、次章の手順内で secondary への同期により行われます。

① 負荷分散機能のルールを設定します。primary の IPCOM VA2 で以下を実施してください。(図 9-1)

コマンド例

```
vipcom-pri# con
vipcom-pri(config)# load running-config
vipcom-pri(edit)# slb real-server web-server1  ※1
vipcom-pri(edit-slb-real)# distribution-address 192.168.110.30 ※2
vipcom-pri(edit-slb-real)# exit
vipcom-pri(edit)# slb real-server web-server2  ※3
vipcom-pri(edit-slb-real)# distribution-address 192.168.110.40 ※4
vipcom-pri(edit-slb-real)# exit

※1 負荷分散対象の登録をします。web-server1 の部分は任意の名前です。
※2 WebServer1 の BackNetwork 側の IP アドレスを指定してください。
※3 負荷分散対象の登録をします。web-server2 の部分は任意の名前です。
※4 WebServer2 の BackNetwork 側の IP アドレスを指定してください。
```

図 9-1：負荷分散対象の登録

② 負荷分散機能のルール(HTTP)を設定します。primary の IPCOM VA2 LS で以下を実施してください。(図 9-2)

コマンド例

```
vipcom-pri(edit)# slb-rule 100
vipcom-pri(edit-slb-rule)# virtual-server 192.168.100.200 80/tcp ※1
vipcom-pri(edit-slb-rule)# transit-mode round-trip
vipcom-pri(edit-slb-rule)# transfer-mode ip-address
vipcom-pri(edit-slb-rule)# distribution-rule 100 ※2
vipcom-pri(edit-dist-rule)# class-map any
vipcom-pri(edit-dist-rule)# distribution-mode round-robin ※3
vipcom-pri(edit-dist-rule)# persistence mode http-session cookie ipcom
vipcom-pri(edit-dist-rule)# persistence guarantee-time 180
vipcom-pri(edit-dist-rule)# persistence cookie-mode persistent-cookie 1800
vipcom-pri(edit-dist-rule)# monitor level application
vipcom-pri(edit-dist-rule)# monitor level ping ※4
vipcom-pri(edit-dist-rule)# monitor check-interval 60
vipcom-pri(edit-dist-rule)# monitor check-timeout 10000
vipcom-pri(edit-dist-rule)# real-server web-server1 ※5
vipcom-pri(edit-dist-rule-real)# port-map virtual 80 real 80 ※6
vipcom-pri(edit-dist-rule-real)# exit
vipcom-pri(edit-dist-rule)# real-server web-server2 ※7
vipcom-pri(edit-dist-rule-real)# port-map virtual 80 real 80
vipcom-pri(edit-dist-rule-real)# exit
```

```
vipcom-pri(edit-dist-rule)# exit
vipcom-pri(edit-slb-rule)# exit
```

※1 負荷分散用の仮想 IP アドレス登録をします。本設定例では FrontNetwork 内の IP アドレスを指定します。負荷分散用の仮想 IP アドレスは、本装置の物理インターフェースまたは仮想インターフェースの IP アドレスと重複しないように設定する必要があります。
※2 ID は任意の数値です。
※3 本設定例では、負荷分散方式はラウンドロビンで設定します。
※4 本事例では ping によるサーバ監視を設定します。ping の設定ではアプリケーションのダウン検知はされないため、お客様のシステムに合わせて、ヘルスチェックのルールを設定してください。
※5 負荷分散設定①で設定した負荷分散対象を指定します。
※6 HTTP(80)を受けた場合、そのまま HTTP で分散します。
※7 負荷分散設定①で設定した負荷分散対象を指定します。

図 9-2：負荷分散対象ルールの登録(HTTP)

③ 負荷分散機能のルール(HTTPS)を設定します。primary の IPCOM VA2 で以下を実施してください。(図 9-3)

コマンド例

```
vipcom-pri(edit)# slb-rule 200
vipcom-pri(edit-slb-rule)# virtual-server 192.168.100.200 443/tcp ※1
vipcom-pri(edit-slb-rule)# transit-mode round-trip
vipcom-pri(edit-slb-rule)# transfer-mode ip-address
vipcom-pri(edit-slb-rule)# distribution-rule 100 ※2
vipcom-pri(edit-dist-rule)# class-map any
vipcom-pri(edit-dist-rule)# distribution-mode round-robin ※3
vipcom-pri(edit-dist-rule)# persistence mode node
vipcom-pri(edit-dist-rule)# persistence guarantee-time 180
vipcom-pri(edit-dist-rule)# persistence cookie-mode persistent-cookie 1800
vipcom-pri(edit-dist-rule)# monitor level application
vipcom-pri(edit-dist-rule)# monitor level ping ※4
vipcom-pri(edit-dist-rule)# monitor check-interval 60
vipcom-pri(edit-dist-rule)# monitor check-timeout 10000
vipcom-pri(edit-dist-rule)# real-server web-server1 ※5
vipcom-pri(edit-dist-rule-real)# port-map virtual 443 real 443 ※6
vipcom-pri(edit-dist-rule-real)# exit
vipcom-pri(edit-dist-rule)# real-server web-server2 ※7
vipcom-pri(edit-dist-rule-real)# port-map virtual 443 real 443
vipcom-pri(edit-dist-rule-real)# exit
vipcom-pri(edit-dist-rule)# exit
vipcom-pri(edit-slb-rule)# exit
```

※1 負荷分散用の仮想 IP アドレス登録をします。本設定例では FrontNetwork 内の IP アドレスを指定します。負荷分散用の仮想 IP アドレスは、本装置の物理インターフェースまたは仮想インターフェースの IP アドレスと重複しないように設定する必要があります。
※2 ID は任意の数値です。
※3 本設定例では、負荷分散方式はラウンドロビンで設定します。
※4 ping による監視を行います。
※5 負荷分散設定①で設定した負荷分散対象を指定します。
※6 HTTPS(443)を受けた場合、そのまま HTTPS で分散します。
※7 負荷分散設定①で設定した負荷分散対象を指定します。

図 9-3 負荷分散対象ルールの登録(HTTPS)

第 10 章 【LS】IPCOM VA2 LS の外部通信設定

本章では、IPCOM VA2 LS が外部と通信するために必要な設定について説明します。

10.1 外部通信設定/secondary への LB 設定の同期

primary で参照先 DNS サーバの設定や NAT の設定を行い、ここまでの設定を secondary 側に同期します。(図 10-1)コマンド例

```
vipcom-pri(edit)# dns-server primary ipv4 133.162.193.9 ※1
vipcom-pri(edit)# dns-server secondary ipv4 133.162.193.10 ※1
vipcom-pri(edit)# class-map match-all web-server ※2
vipcom-pri(edit-cmap)# match source-address ip 192.168.110.0/24 ※3
vipcom-pri(edit-cmap)# exit
vipcom-pri(edit)# host-group snapt ※4
vipcom-pri(edit-host-group)# host ipv4 192.168.110.0/24 ※5
vipcom-pri(edit-host-group)# exit
vipcom-pri(edit)# class-map match-any server ※6
vipcom-pri(edit-cmap)# match destination-address host-group snapt ※7
vipcom-pri(edit-cmap)# exit
vipcom-pri(edit)# class-map match-all get-metadata  ※8
vipcom-pri(edit-cmap)# match source-address ip 192.168.110.0/24 ※9
vipcom-pri(edit-cmap)# match destination-address ip 169.254.169.254 ※10
vipcom-pri(edit-cmap)# exit
vipcom-pri(edit)# interface lan0.1
vipcom-pri(edit-if)# rule src-napt 10 ipv4 server to auto 10000-20000 ※11
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# interface lan0.0
vipcom-pri(edit-if)# rule src-napt 10 ipv4 web-server to 192.168.100.200 10000-20000 ※12
vipcom-pri(edit-if)# rule no-src-nat get-metadata ※13
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# commit
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):y
vipcom-pri(edit)# exit
vipcom-pri(config)# exit
vipcom-pri# sync cluster primary-to-secondary ※14
This System: primary
primary (2017/01/25(Wed)16:44:42) -> secondary(2017/01/24(Tue)18:27:11)
Are you sure? (y|[n]):y
```

※1 参照先 DNS サーバのアドレスを指定します。
※2 NAT の対象となるグループを設定します。
※3 BackNetwork の NW アドレスを指定します。
※4 ホストグループを設定します。
※5 BackNetwork の NW アドレスを指定します。
※6 NAT の対象となるグループを設定します。
※7 ホストグループを指定します。
※8 メタデータ取得の際必須となる設定です。
※9 BackNetwork の NW アドレスを指定します。
※10 メタデータプロキシのアドレス(169.254.169.254)を指定してください。

※11 WebServer からの戻りの通信を IPCOM にするために SRC-NAPT を設定します。
※12 外部接続するために SRC-NAPT を設定します。アドレスは仮想 IP アドレスを指定します。
※13 メタデータ通信のために NAT を解除します。本設定を行わない場合、BackNetwork に所属する仮想サーバがキーペアの取得等を行えなくなるため、必ず設定してください。
※14 primary から secondary にコンフィグを同期します。

図 10-1：外部通信設定/secondary への LB 設定の同期

10.2 IPCOM VA2 LS の各代表 IP に対応するダミーポートを作成

ポート生成時の設定パラメータ値は、「東日本第 1/第 2、西日本第 1/第 2 リージョン」向けの設定パラメータとは一部異なります。
詳細は、以下の 図 10-2：IPCOM VA2 LS の各代表 IP に対応するダミーポートを作成 を参照してください。

代表 IP がプロジェクト内で別の仮想サーバで使用されないようにダミーポートを作成します。(図 10-2)

コマンド例

```
[root@K5-Host ]# PORT_NAME=FrontShareIP
[root@K5-Host ]# NETWORK_ID= “FrontNetwork の ID”
[root@K5-Host ]# SUBNET_ID= “FrontNetwork のサブネット ID”
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.100.100 ※1
[root@K5-Host ]# SG_ID= “「SecurityGroup の作成」で作成した SecuriryGroup”
[root@K5-Host ]# DEVICE_OWNER="nuage:vip"  ※4
[root@K5-Host  ]#  curl  -X  POST  -s  $NETWORK/v2.0/ports  -H  "Content-Type:application/json"  -H
"Accept:application/json" -H "X-Auth-Token: $OS_AUTH_TOKEN " -d '{"port": {"network_id":"'$NETWORK_ID'",
"name":  "'$PORT_NAME'","admin_state_up":  true,"fixed_ips":  [{"ip_address":
"'$FIXED_IP_ADDRESS'","subnet_id":"'$SUBNET_ID'"}],"security_groups":  ["'$SG_ID'"],"device_owner":
"'$DEVICE_OWNER'" }}' | jq .

[root@K5-Host ]# PORT_NAME=BackShareIP
[root@K5-Host ]# NETWORK_ID= “BackNetwork の ID”
[root@K5-Host ]# SUBNET_ID= “BackNetwork のサブネット ID”
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.110.100 ※2
[root@K5-Host ]# SG_ID= “「SecurityGroup の作成」で作成した SecuriryGroup”
[root@K5-Host ]# DEVICE_OWNER="nuage:vip"  ※4
[root@K5-Host  ]#  curl  -X  POST  -s  $NETWORK/v2.0/ports  -H  "Content-Type:application/json"  -H
"Accept:application/json" -H "X-Auth-Token: $OS_AUTH_TOKEN " -d '{"port": {"network_id":"'$NETWORK_ID'",
"name":  "'$PORT_NAME'","admin_state_up":  true,"fixed_ips":  [{"ip_address":
"'$FIXED_IP_ADDRESS'","subnet_id":"'$SUBNET_ID'"}],"security_groups":  ["'$SG_ID'"],"device_owner":
"'$DEVICE_OWNER'" }}' | jq .

[root@K5-Host ]# PORT_NAME=ManagementShareIP
[root@K5-Host ]# NETWORK_ID= “managementNetwork の ID”
[root@K5-Host ]# SUBNET_ID= “ManagementNetwork のサブネット ID”
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.120.100 ※3
[root@K5-Host ]# SG_ID=「SecurityGroup の作成」で作成した SecuriryGroup”
[root@K5-Host ]# DEVICE_OWNER="nuage:vip"  ※4
[root@K5-Host  ]#  curl  -X  POST  -s  $NETWORK/v2.0/ports  -H  "Content-Type:application/json"  -H
"Accept:application/json" -H "X-Auth-Token: $OS_AUTH_TOKEN " -d '{"port": {"network_id":"'$NETWORK_ID'",
"name":  "'$PORT_NAME'","admin_state_up":  true,"fixed_ips":  [{"ip_address":
"'$FIXED_IP_ADDRESS'","subnet_id":"'$SUBNET_ID'"}],"security_groups":  ["'$SG_ID'"],"device_owner":
"'$DEVICE_OWNER'" }}' | jq .

※1 FrontNetwork 側の IPCOM VA2 の代表 IP アドレス
※2 BackNetwork 側の IPCOM VA2 の代表 IP アドレス
※3 FrontNetwork 側の IPCOM VA2 の代表 IP アドレス
※4 このパラメータは「東日本第 1/第 2,西日本第 1/第 2 リージョン」向けのスタートガイドと異なり、「東日本第 3,西日本第 3 リージョン」では必須のパラメータになります。
```

図 10-2：IPCOM VA2 LS の各代表 IP に対応するダミーポートを作成

第 11 章 【SC】IPCOM VA2 SC の初期設定

本章では、IPCOM VA2 SC の初期設定について説明します。

11.1 ホスト名とパスワードの設定(SC)

IPCOM VA2 SC にリモートコンソールログインをしてホスト名とパスワードを設定します。(図 11-1)

※本設定以降は SSH でログインし、操作できます。

コマンド例

```
ipcom# configure
ipcom(config)# load running-config
ipcom(edit)# user admin
ipcom(edit-user)# password “任意の password” ※1
ipcom(edit-user)# exit
ipcom(edit)# hostname vipcom-sc ※2
ipcom(edit)#  user-role remote
ipcom(edit-user-role)# match user admin ※3
ipcom(edit-user-role)# exit
ipcom(edit)# commit force-update
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):y
vipcom-sc(edit)# exit
vipcom-sc(config)# exit

※1 パスワードは簡単に推測されない文字列を設定してください。(8 文字以上かつ英数字記号を混在した文字列を推奨)
※2 ホスト名は任意です。
※3 パスワードを設定したため、admin ユーザーの remote アクセスを許可します。
```

図 11-1：ホスト名とパスワードの設定(SC)

11.2 インターフェース設定(SC)

IPCOM VA2 SC のインターフェースの設定を行います。(図 11-2)

コマンド例

```
vipcom-sc> admin
vipcom-sc# configure
vipcom-sc(config)# load running-config
vipcom-sc(edit)# protect checksum-inspection disable ※1
vipcom-sc(edit)# interface lan0.0
vipcom-sc(edit-if)# ip address 192.168.100.30 255.255.255.0 ※2
vipcom-sc(edit-if)# description IPCOM-VA2-SC-front-net ※3
vipcom-sc(edit-if)# mtu 8950 ※4
vipcom-sc(edit-if)# exit
vipcom-sc(edit)# interface lan0.1
vipcom-sc(edit-if)# ip address 192.168.120.30 255.255.255.0 ※5
vipcom-sc(edit-if)# description IPCOM-VA2-SC-management-net ※6
vipcom-sc(edit-if)# mtu 8950 ※7
vipcom-sc(edit-if)# exit
vipcom-sc(edit)# ip route 0.0.0.0/0 192.168.100.1 distance 2 ※8
vipcom-sc(edit)# commit
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):y

※1 パケットのチェックを行う機能は K5 上では使用しないでください。予期せぬ動作が起こる場合があります。
※2 K5 で割当された FrontNetwork 側の IP アドレスを指定してください
※3 説明文のため任意です
※4 IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※5 K5 で割当された ManagementNetwork 側の IP アドレスを指定してください
※6 説明文のため任意です。
※7 IPCOM VA2 の MTU 値は、付録 E：IPCOM VA2 と IaaS の通信設定の E-7 MTU 値の設定を参考に設定してください。
※8 仮想ルータのインターフェースをデフォルトゲートウェイに設定します。
```

図 11-2：ホスト名とパスワードの設定(SC)

第 12 章 【SC】IPCOM VA2 SC のファイアーウォール機能の設定

本章では、IPCOM VA2 SC におけるファイアーウォールの設定手順を説明します。

12.1 IPCOM VA2 SC ファイアーウォールの設定

ファイアーウォールを設定するため、IPCOM VA2 SC でルール作成およびインターフェースへのルール設定を行います。
本設定例では、FrontNetwork に dns(53)の許可、ManagemantNetwork には保守用仮想サーバからの SSH、WebConsole アクセスのみ許可します。

① IPCOM VA2 SC でファイアーウォールのルールを作成します。(図 12-1)

コマンド例

```
vipcom-sc> admin
vipcom-sc# con
vipcom-sc(config)# load running-config
vipcom-sc(edit)# access-control default-deny ※1
vipcom-sc(edit)# no access-control configuration ※2
All the definitions for the access control map are deleted if the access control rule is changed to enable. Are
you sure?(y|[n]):y
vipcom-sc(edit)# class-map match-any dns-access ※3
vipcom-sc(edit-cmap)# match destination-port 53/udp
vipcom-sc(edit-cmap)# match destination-port 53/tcp
vipcom-sc(edit-cmap)# exit
vipcom-sc(edit)# class-map match-all mng-access ※4
vipcom-sc(edit-cmap)# match destination-port 22/tcp
vipcom-sc(edit-cmap)# match source-address ip 192.168.120.30
vipcom-sc(edit-cmap)# exit
vipcom-sc(edit)# class-map match-all webconsole-access ※5
vipcom-sc(edit-cmap)# match destination-port 82/tcp
vipcom-sc(edit-cmap)# match source-address ip 192.168.120.30
vipcom-sc(edit-cmap)# exit
vipcom-sc(edit)#

※1 rule に該当しないものはすべて破棄します。
※2 access control rule を有効にします。
※3 DNS(53)をルールに指定
※4 保守用仮想サーバからのみ SSH アクセスを許可するようルールに指定します
※5 保守用仮想サーバからのみ IPCOM VA2 の GUI(82 番ポート)へアクセス許可するルールを指定します。
```

図 12-1：IPCOM VA2 SC ファイアーウォールのルールの作成

② 作成したファイアーウォールのルールをインターフェースに指定します。(図 12-2)

コマンド例

```
vipcom-sc(edit)# interface lan0.0
vipcom-sc(edit-if)# rule access 100 in dns-access accept audit-session-normal audit-match-normal ※1
vipcom-sc(edit-if)# rule access 110 out dns-access accept audit-session-normal audit-match-normal ※2
vipcom-sc(edit-if)# exit
vipcom-sc(edit)# interface lan0.1
vipcom-sc(edit-if)# rule access 100 in mng-access accept audit-session-normal audit-match-normal ※3
vipcom-sc(edit-if)# rule access 110 in webconsole-access accept audit-session-normal audit-match-normal ※4
vipcom-sc(edit-if)# rule access 120 out any accept audit-session-normal audit-match-normal ※5
vipcom-sc(edit-if)# exit
vipcom-sc(edit)# commit
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):y

※1 インバウンドの web アクセス許可
※2 アウトバウンドの web アクセス許可
※3 保守用仮想サーバからの SSH アクセス許可
※4 保守用仮想サーバからの WebConsole(82)許可
※5 アウトバウンドはすべて許可
```

図 12-2：IPCOM VA2 SC ファイアーウォールのルールをインターフェースに適用

rule access コマンドにて audit-session-noramal / audit-match-normal 設定したログを出力する際には、logging collection-level コマンドにてログレベルを設定して下さい。なお、詳細については、以下のマニュアルを参照して下さい。

IPCOM EX シリーズコマンドリファレンスガイド

2.1.2.12 logging collection-level

2.16.2.6.1 rule access

第 13 章 【SC】IPCOM VA2 SC の DNS 機能の設定

本章では、IPCOM VA2 SC における DNS 機能の設定手順を説明します。

13.1 DNS の設定

DNS を設定するため、IPCOM VA2 SC で DNS ゾーンとレコードの設定を行います。本例では「ipcom-va2.com」という名前のゾーンを作成しております。(図 13-1)

コマンド例

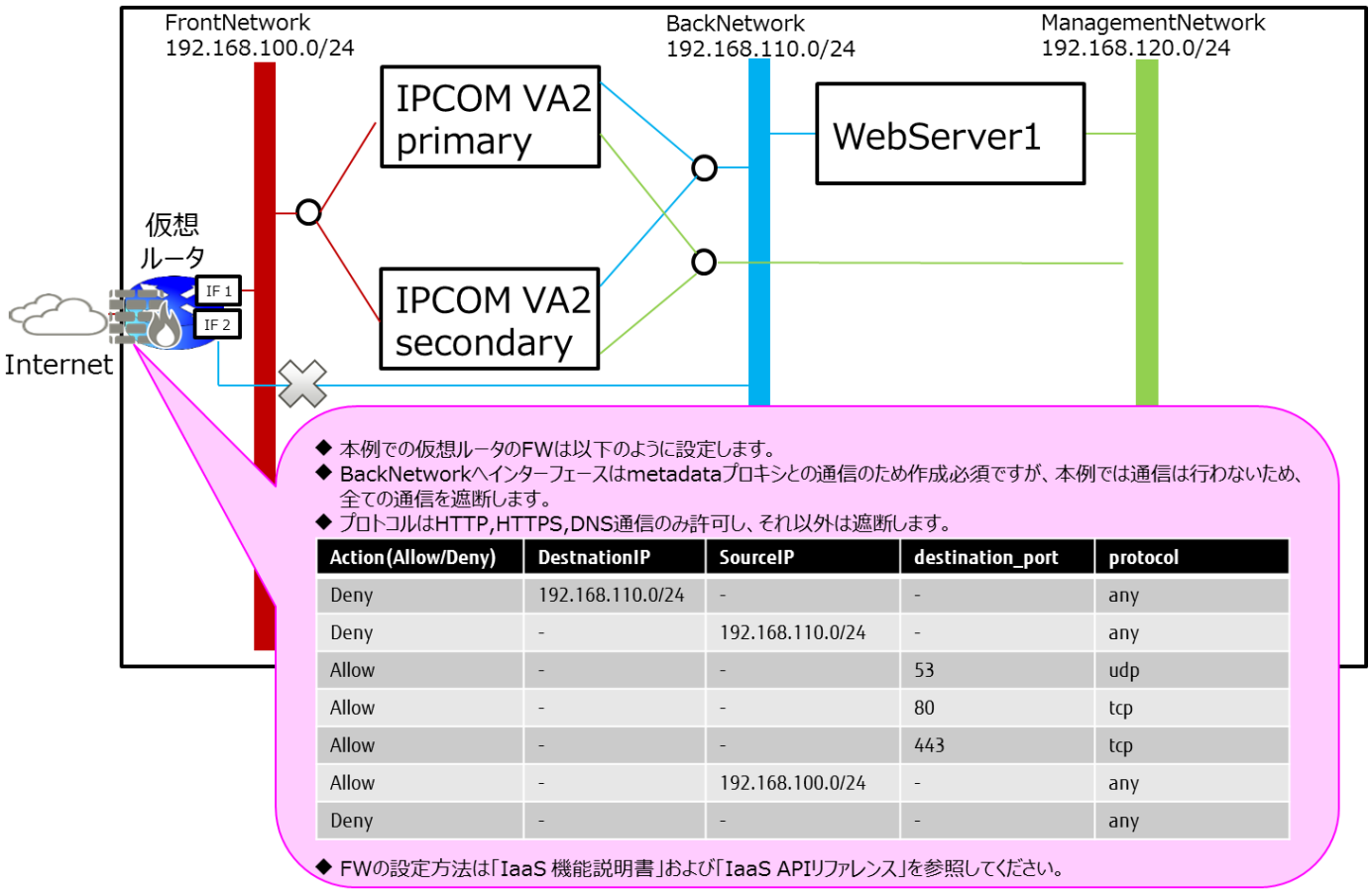
```
vipcom-sc> admin
vipcom-sc# con
vipcom-sc(config)# load running-config
vipcom-sc(edit)# dns-server-config
vipcom-sc(edit-dns-server)# zone ipcom-va2.com ※1
Register new zone. OK?([y]|n):y
vipcom-sc(edit-dns-server-zone)# type master ※2
vipcom-sc(edit-dns-server-zone)# soa-data all 20170427 10800 3600 604800 86400 600 master ipcom-va2.com.※3
vipcom-sc(edit-dns-server-zone)# host dns NS ※4
vipcom-sc(edit-dns-server-zone)# name-server dns ※4
vipcom-sc(edit-dns-server-zone)# host-ip-address dns 192.168.100.30 ※5
vipcom-sc(edit-dns-server-zone)# host webserver A ※6
vipcom-sc(edit-dns-server-zone)# host-ip-address webserver 192.168.100.200 ※7
vipcom-sc(edit-dns-server-zone)# exit
vipcom-sc(edit-dns-server)# exit
vipcom-sc(edit)# commit
Do you overwrite "running-config" by the current configuration? (y|[n]):y
Do you update "startup-config" for the restarting system? (y|[n]):y

※1 DNS のゾーンを指定します。今回は「ipcom-va2.com」という名前のゾーンを作成します。
※2 マスターの DNS として登録します。
※3 SOA を設定します(パラメータ詳細は IPCOM のコマンドマニュアル参照)。
※4 NamaServer を定義します。
※5 DNS 自身の名前解決ルールを定義します。本例では SC の FrontNetwork 側のインターフェースを指定します。
※6 WebServer の A レコードを定義します。
※7 本例では IPCOM VA2 LS の仮想 IP アドレスを指定します。
```

図 13-1：IPCOM VA2 SC DNS サーバの設定

14.1 仮想ルータのファイアーウォールルールの設定

仮想ルータのファイアーウォールのルールは下記に示した通り設定して下さい。



◆ 本例での仮想ルータのFWは以下のように設定します。
◆ BackNetworkへインターフェースはmetadataプロキシとの通信のため作成必須ですが、本例では通信は行わないため、全ての通信を遮断します。
◆ プロトコルはHTTP,HTTPS,DNS通信のみ許可し、それ以外は遮断します。

Action(Allow/Deny)	DestnationIP	SourceIP	destination_port	protocol
Deny	192.168.110.0/24	-	-	any
Deny	-	192.168.110.0/24	-	any
Allow	-	-	53	udp
Allow	-	-	80	tcp
Allow	-	-	443	tcp
Allow	-	192.168.100.0/24	-	any
Deny	-	-	-	any

◆ FWの設定方法は「IaaS 機能説明書」および「IaaS APIリファレンス」を参照してください。

図 14-1：IaaS 上の仮想ルータのファイアーウォール設定

［注意］

冗長構成の IPCOM VA2 で仮想ルータのファイアーウォールを利用した通信を行う場合、双方向の通信を許可するファイアーウォールルールが必要です。

14.2【LS】IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当

IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当し、IPCOM VA2 LS の運用を開始します。(図 14-2)

グローバル IP アドレスの割当時の設定パラメータ値は、「東日本第 1/第 2、西日本第 1/第 2 リージョン」向けの設定パラメータとは一部異なります。詳細は、以下の 図 14-2：IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当 を参照してください。

コマンド例

```
[root@K5-Host ]# PORT_NAME=ipcom_va2_virtual_server
[root@K5-Host ]# NETWORK_ID= “FrontNetwork の ID”
[root@K5-Host ]# SUBNET_ID= “FrontNetwork のサブネット ID”
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.100.200 ※1
[root@K5-Host ]# SG_ID= “「SecurityGroup の作成」で作成した SecuriryGroupID”
[root@K5-Host ]# DEVICE_OWNER="nuage:vip"  ※2

# 仮想 IP アドレス(virtualserver のポートのアドレス)のダミーポートを作成
[root@K5-Host ]# curl -X POST -s $NETWORK/v2.0/ports -H "Content-Type:application/json" -H
"Accept:application/json" -H "X-Auth-Token: $OS_AUTH_TOKEN " -d '{"port": {"network_id":"'$NETWORK_ID'",
"name": "'$PORT_NAME'","admin_state_up": true,"fixed_ips": [{"ip_address":
"'$FIXED_IP_ADDRESS'","subnet_id":"'$SUBNET_ID'"}],"security_groups": ["'$SG_ID'"],"device_owner":
"'$DEVICE_OWNER'" }}' | jq .

# 作成したポート(virtualserver のポートのアドレス)にグローバル IP アドレスを割当
[root@K5-Host ]# NETWORK_ID= “グローバル IP ネットワークの ID”
[root@K5-Host ]# VM_PORT_ID= “新規作成したポートの ID”
curl -s $NETWORK/v2.0/floatingips -X POST -H "X-Auth-Token:$OS_AUTH_TOKEN" -H "Content-Type:application/json"
-d '{"floatingip":{"floating_network_id":"'$NETWORK_ID'", "port_id":"'$VM_PORT_ID'"}}' | jq .
```

※上記設定を完了後、WebServer の参照先 DNS サーバやデフォルトゲートウェイの設定を確認し、インターネットからグローバル IP アドレスにアクセスし、疎通を確認して LS の設定は完了です。

※1 「負荷分散機能の設定」で定義した負荷分散用の仮想 IP アドレス

※2 このパラメータは「東日本第 1/第 2,西日本第 1/第 2 リージョン」向けのスタートガイドと異なり、「東日本第 3,西日本第 3 リージョン」では必須のパラメータになります。

図 14-2：IPCOM VA2 LS の仮想 IP アドレスにグローバル IP アドレスを割当

14.3【SC】IPCOM VA2 SC の FrontNetwork 側の IP アドレスにグローバル IP アドレスを割当

IaaS ポータルで IPCOM VA2 SC の FrontNetwork 側の IP アドレスにグローバル IP アドレスを割当し、IPCOM VA2 SC の運用を開始します。(図 14-3)

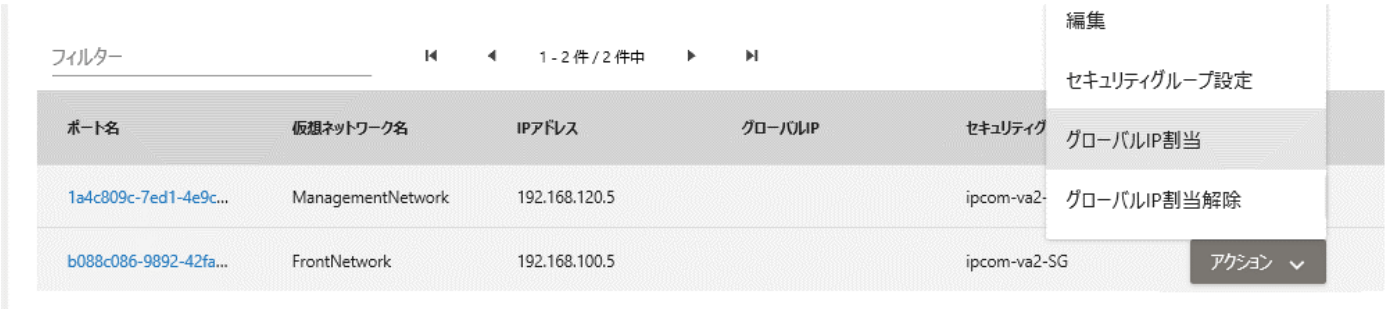


図 14-3：IPCOM VA2 SC の FrontNetwork 側の IP アドレスにグローバル IP アドレスを割当

以上で本書における導入事例の説明は終了です。

付録 A：【設定事例】IPCOM VA2 LS の running-config

本書の手順に従い設定を行った場合の LS のコンフィグ(running-config コマンド実行結果)を以下に示します。
※running-config コマンドの詳細は IPCOM EX シリーズコマンドリファレンスガイドをご参照ください。

running-config コマンドの実行結果
dns-server primary ipv4 133.162.193.9 dns-server secondary ipv4 133.162.193.10 hostname vipcom-pri vipcom-sco fixup protocol dns 53/udp fixup protocol ftp 21/tcp fixup protocol http 80-83/tcp fixup protocol http 8080-8083/tcp fixup protocol https 443/tcp cluster mode primary cluster id 1 cluster secret-key vipcom access-control default-deny access-control audit session-normal match-normal protect checksum-inspection disable interface lan0.0 　ip address 192.168.100.100 255.255.255.0 　ip address primary 192.168.100.10 　ip address secondary 192.168.100.20 　description IPCOM-VA2-front-net 　mtu 8950 　ip-routing 　rule src-napt 10 ipv4 web-server to 192.168.100.200 10000-20000 　rule no-src-nat get-metadata 　rule access 100 in web-access accept audit-session-normal audit-match-normal 　rule access 110 out web-access accept audit-session-normal audit-match-normal 　rule access 120 out dns-access accept audit-session-normal audit-match-normal 　cluster sync-interface 　cluster vrid 10 ! interface lan0.1 　ip address 192.168.110.100 255.255.255.0 　ip address primary 192.168.110.10 　ip address secondary 192.168.110.20 　description IPCOM-VA2-back-net 　mtu 8950 　ip-routing 　rule src-napt 10 ipv4 server to auto 10000-20000 　rule access 100 in web-access accept audit-session-normal audit-match-normal 　rule access 110 out web-access accept audit-session-normal audit-match-normal 　rule access 120 in dns-access accept audit-session-normal audit-match-normal 　rule access 130 out ping-moniter accept audit-session-normal audit-match-normal

```
    cluster sync-interface
    cluster vrid 20
!
interface lan0.2
    ip address 192.168.120.100 255.255.255.0
    ip address primary 192.168.120.10
    ip address secondary 192.168.120.20
    description IPCOM-VA2-management-net
    mtu 8950
    ip-routing
    rule access 100 in mng-access accept audit-session-normal audit-match-normal
    rule access 110 in webconsole-access accept audit-session-normal audit-match-normal
    rule access 120 out any accept audit-session-normal audit-match-normal
    cluster sync-interface
    cluster vrid 30
!
ip route 0.0.0.0/0 192.168.100.1 distance 2
slb real-server web-server1
    distribution-address 192.168.110.30
!
slb real-server web-server2
    distribution-address 192.168.110.40
!
slb-rule 100
    virtual-server 192.168.100.200 80/tcp
    transit-mode round-trip
    transfer-mode ip-address
    distribution-rule 100
        class-map any
        distribution-mode round-robin
        persistence mode http-session cookie ipcom
        persistence guarantee-time 180
        persistence cookie-mode persistent-cookie 1800
        monitor level application
        monitor level ping
        monitor check-interval 60
        monitor check-timeout 10000
        real-server web-server1
            port-map virtual 80 real 80
        !
        real-server web-server2
            port-map virtual 80 real 80
        !
    !
!
slb-rule 200
    virtual-server 192.168.100.200 443/tcp
    transit-mode round-trip
    transfer-mode ip-address
    distribution-rule 100
```

```
        class-map any
        distribution-mode round-robin
        persistence mode node
        persistence guarantee-time 180
        persistence cookie-mode persistent-cookie 1800
        monitor level application
        monitor level ping
        monitor check-interval 60
        monitor check-timeout 10000
        real-server web-server1
            port-map virtual 443 real 443
        !
        real-server web-server2
            port-map virtual 443 real 443
        !
    !
!
class-map match-all any
    match any
!
class-map match-all dns-access
    match destination-port 53/udp
!
class-map match-all get-metadata
    match source-address ip 192.168.110.0/24
    match destination-address ip 169.254.169.254
!
class-map match-all mng-access
    match destination-port 22/tcp
    match source-address ip 192.168.120.40
!
class-map match-all ping-moniter
    match icmp ping
!
class-map match-any server
    match destination-address host-group snapt
!
class-map match-any web-access
    match destination-port 80/tcp
    match destination-port 443/tcp
!
class-map match-all web-server
    match source-address ip 192.168.110.0/24
!
class-map match-all webconsole-access
    match destination-port 82/tcp
    match source-address ip 192.168.120.40
!
host-group snapt
    host ipv4 192.168.110.0/24
```

```
!
user-role administrator
     description "Default user role"
     display-name "IPCOM administrators"
     match user admin
!
user-role remote
     description "Default user role"
     display-name "IPCOM access via network"
     match user admin
!
user-role user
     description "Default user role"
     display-name "IPCOM operators"
!
user admin
     valid
     secret-password 000180b918874ade72ba
     authentication pap
     description "Default user"
     display-name "IPCOM administrator"
!
```

付録 B：【設定事例】IPCOM VA2 SC の running-config

本書の手順に従い設定を行った場合の SC のコンフィグ(running-config コマンド実行結果)を以下に示します。
※running-config コマンドの詳細は IPCOM EX シリーズコマンドリファレンスガイドをご参照ください。

running-config コマンドの実行結果

```
hostname vipcom-sc
fixup protocol dns 53/udp
fixup protocol ftp 21/tcp
fixup protocol http 80-83/tcp
fixup protocol http 8080-8083/tcp
fixup protocol https 443/tcp
dns-server-config
    zone ipcom-va2.com 0
        type master
        soa-data expire 604800
        soa-data max-cache-ttl 86400
        soa-data max-ncache-ttl 600
        soa-data person-domain ipcom-va2.com.
        soa-data person-user master
        soa-data refresh 10800
        soa-data retry 3600
        soa-data serial 20170427
        host dns NS
        host webserver A
        host-ip-address dns 192.168.100.30
        host-ip-address webserver 192.168.100.200
        name-servers dns
    !
!
access-control default-deny
access-control audit session-normal match-normal
protect checksum-inspection disable
interface lan0.0
    ip address 192.168.100.30 255.255.255.0
    description IPCOM-VA2-SC-front-net
    mtu 8950
    rule access 100 in dns-access accept audit-session-normal audit-match-normal
    rule access 110 out dns-access accept audit-session-normal audit-match-normal
!
interface lan0.1
    ip address 192.168.120.30 255.255.255.0
    description IPCOM-VA2-SC-management-net
    mtu 8950
    rule access 100 in mng-access accept audit-session-normal audit-match-normal
    rule access 110 in webconsole-access accept audit-session-normal audit-match-normal
    rule access 120 out any accept audit-session-normal audit-match-normal
```

```
!
ip route 0.0.0.0/0 192.168.100.1 distance 2
class-map match-all any
     match any
!
class-map match-any dns-access
     match destination-port 53/tcp
     match destination-port 53/udp
!
class-map match-all mng-access
     match destination-port 22/tcp
     match source-address ip 192.168.120.40
!
class-map match-all webconsole-access
     match destination-port 82/tcp
     match source-address ip 192.168.120.40
!
user-role administrator
     description "Default user role"
     display-name "IPCOM administrators"
     match user admin
!
user-role remote
     description "Default user role"
     display-name "IPCOM access via network"
     match user admin
!
user-role user
     description "Default user role"
     display-name "IPCOM operators"
!
user admin
     valid
     secret-password 0001cd5d29e805d6fa4b15550e812fea47d6
     authentication pap
     description "Default user"
     display-name "IPCOM administrator"
!
```

付録 C：IaaS 上の IPCOM VA2 の未サポート機能

C-1 未サポート機能一覧

IPCOM VA2 シリーズ VA2 ユーザーズガイドの「1-2-1 提供機能」で記載されている提供機能のうち、IaaS 上で未サポートの機能を以下に記載します。

C-1-1 レイヤ 2 中継機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
VLAN	ポート VLAN	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
	MAC-VLAN	
	tagVLAN	
	VLAN 間レイヤ 2 中継	
	VLAN パススルー	
	802.1p タグ優先度	

C-1-2 レイヤ 3 中継機能(IPv6)

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
ルーティング(IPv6)	RA	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
	スタティック	
	RIPng	
MTU	IP フラグメント	
	MTU 長変更	
フィルタリング(IPv6)	送受信 IPv6 アドレス	
	IP flow label	
	TCP src/dst port	
	TCP syn/ack	
	UDP src/dst port	
レイヤ 3 中継機能 On/Off		

C-1-3 サーバ負荷分散

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
配置方法・動作モード	並列型ブリッジ	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
サーバ分散方式	最小サーバ負荷	
	最小 FNA LU 数	
故障監視(監視方式)	負荷計測エージェント監視	
VMware View 負荷分散機能		

C-1-4 リンク負荷分散

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
リンクアグリゲーション		IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
アウトバウンドトラフィック制御		
インバウンドトラフィック制御		
ルータ監視/ ルート監視/SLA 監視		
バックアップリンク制御		
VPN(IPsec) 連携分散		
センター自動切り替え		
障害復旧時の自動切り戻し		
グレースフルシャットダウン		
分散単位	ノード単位	
	セッション単位	
	固定	
	あて先 IP アドレス単位/ 送信元 IP アドレス + あて先 IP アドレス単位/ 送信元サブネット単位	
分散方式	帯域幅ベース・ラウンドロビン	
	最小利用帯域幅	
	最小コネクション	

C-1-5 IPS 機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能			説明
シグネチャー型 IPS	動作モード	ブリッジモード	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
		ルータモード	
	シグネチャーベースの侵入検知/遮断		
	シグネチャーのダウンロード		
	検知ポリシーの作成(ゾーンルールの編集と保存)		
	検知ポリシーのバックアップとリストア		
	侵入情報の保存と解析(エビデンスの収集と保存、解析)	検知イベントログ	
		検知イベントのメール送信(通知)	
		攻撃検知パケットの保存/参照	
		攻撃統計情報の保存と集計	
		攻撃状態監視/表示	
	シグネチャー更新/IPS ライセンスのイベント通知		
	セッションログ(標準形式/WELF 形式)		

C-1-6 Web コンテンツ・フィルタリング機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
URL データベース	業務不適カテゴリ	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
	一般カテゴリ	
	カスタムカテゴリ	
動作モード	プロキシモード	
	透過モード	
	透過モード(接続先 IP アドレス隠蔽モード)	

C-1-7 アンチウィルス機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
プロトコル	SMTP	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
	POP3	
	HTTP	
	FTP	
動作モード	プロキシモード	
	透過モード	
	透過モード(接続先 IP アドレス隠蔽モード)	
ウィルスパターンファイルのアップデート	自動	
	手動	
スパムメール対策	SMTP	
	POP3	

C-1-8 アドレス変換機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能	説明
ダイナミックポート・アプリケーション対応	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。

C-1-9 IPsec-VPN 機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

<table>
<tr><th colspan="4">機能</th><th>説明</th></tr>
<tr><td colspan="2">IPsec 動作モード</td><td colspan="2">トンネルモード</td><td rowspan="20">IaaS 上の IPCOM VA2 で左記機能は、未サポートです。</td></tr>
<tr><td rowspan="2">セキュリティタイプ</td><td colspan="3">AH(リプレイ防御機能)</td></tr>
<tr><td colspan="3">ESP(リプレイ防御機能)</td></tr>
<tr><td rowspan="3">暗号アルゴリズム</td><td colspan="3">DES</td></tr>
<tr><td colspan="3">3DES</td></tr>
<tr><td colspan="3">AES(128/192/256)</td></tr>
<tr><td rowspan="3">認証アルゴリズム</td><td colspan="3">MD5</td></tr>
<tr><td colspan="3">SHA1</td></tr>
<tr><td colspan="3">SHA2(256/384/512)</td></tr>
<tr><td colspan="4">ポリシーベース IPsec-VPN</td></tr>
<tr><td colspan="4">Hub and Spoke 中継</td></tr>
<tr><td colspan="4">IP フラグメント</td></tr>
<tr><td colspan="4">IPsec トンネル分析(リンク負荷分散連携)</td></tr>
<tr><td colspan="4">IPsec マルチホーミング</td></tr>
<tr><td colspan="4">パス MTU ディスカバリ/MSS 書き換え</td></tr>
<tr><td colspan="4">障害時の SA 自動復旧</td></tr>
<tr><td colspan="4">ダイナミックネットワークのサポート</td></tr>
<tr><td colspan="4">Commit ビット</td></tr>
<tr><td colspan="4">セキュリティパラメータ設定の簡略化</td></tr>
<tr><td colspan="4">同時接続最大数制限</td></tr>
<tr><td colspan="4">NAT トラバーサル</td></tr>
<tr><td colspan="4">ファイアウォール連携</td></tr>
<tr><td rowspan="8">鍵管理機能</td><td rowspan="2">鍵交換</td><td>Manual</td></tr>
<tr><td>IKE</td></tr>
<tr><td rowspan="2">IKE 認証方式</td><td>Pre-shared Key</td></tr>
<tr><td>Digital signature</td></tr>
<tr><td>IKE Phase1 モード</td><td>Main mod</td></tr>
<tr><td>IKE Phase2 モード</td><td>Aggressive mode</td></tr>
<tr><td>Diffie Hellman(DH)</td><td>Quick mode</td></tr>
<tr><td>PFS</td><td>Group 1,2,5,14</td></tr>
</table>

C-1-10 L2TP/IPsec 機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
認証機能	接続認証	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
	ユーザ認証	
	パスワード変換機能	
監視機能	L2TP キープアライブ機能	
	無通信監視機能	
	最大セッション時間監視機能	
	セッション数超過/警告通知機能	
ファイアウォール連携		
アドレス変換連携		
IPsec-VPN 連携		
アンチウィルス機能連携		
Web コンテンツ・フィルタリング機能連携		
VPN タグマッピング機能		

C-1-11 SSL-VPN 機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
アクセス方式	HTTP リバースプロキシ	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
	ポートフォワーディング(Java/Active-X)	
	L2 フォワーディング(Java/Active-X)	
ポータル	Web ブラウザサービス	
	Windows ファイルサービス	
	WebFTP サービス	
	ブックマーク	
	クライアントマネージャ	
	カスタマイズ	
	リンク	
	テンプレートによる UI カスタマイズ	
ユーザ認証(ユーザ認証機能と連携)		
ユーザ認証 SECUREMATRIX 連携		
アクセス方式	ユーザロールベース	
	リソースベース	
	クライアント監査ベース	
エンドポイントセキュリティ	クライアントチェッカ	
	キャッシュクリーナ	
日英バイリンガル		
アクセスログ(セッションログ)		
仮想 SSL-VPN システム		
ファイアウォール連携		
QoS 制御(帯域制御)連携		
リンク負荷分散連携		
アンチウィルス連携	Web コンテンツフィルタリング連携	

C-1-12 高信頼性機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能	説明
LAN 二重化	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
リンクアグリゲーション	

C-1-13 運用管理/保守機能

IaaS 上の IPCOM VA2 で未サポートとなる機能を以下に示します。

機能		説明
保守機能	リアルタイム・モニタ	IaaS 上の IPCOM VA2 で Web コンソールの運用・保守の画面のモニタ機能は、非サポートです。
	リモート操作ユーティリティ(ipcompass)	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
MIB	MIB-II	IaaS 上の IPCOM VA2 で左記機能は、未サポートです。
	拡張 MIB	

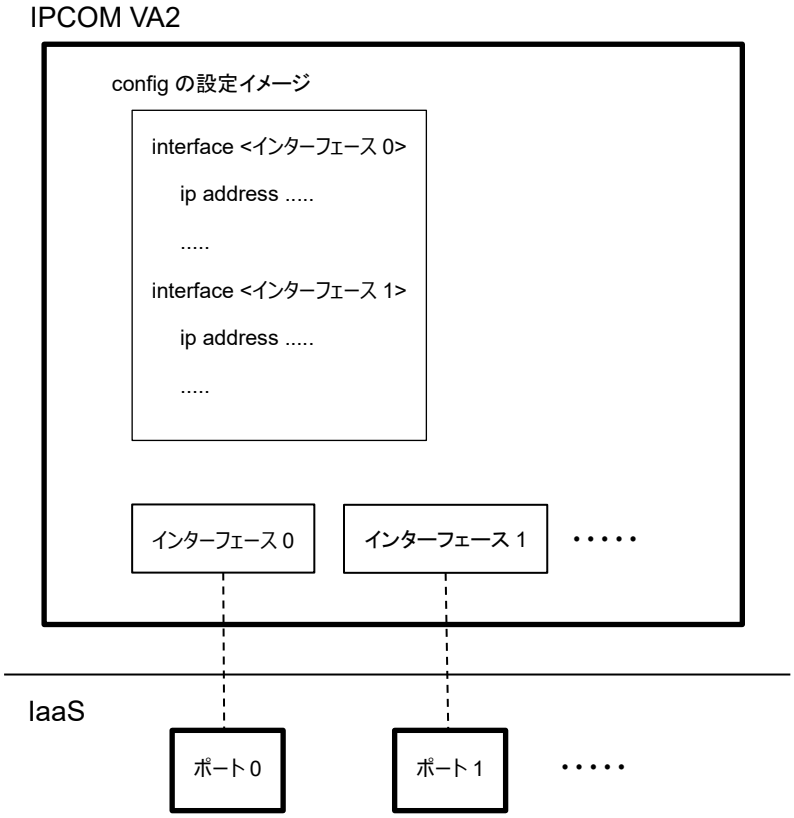
付録 D：IPCOM VA2 および IaaS の構成

D-1 IPCOM VA2 のインターフェースと IaaS のポートの関係

本節では、IPCOM VA2 のインターフェースと IaaS のポートの関係について説明します。IaaS 上の IPCOM VA2 が通信を行うためには、以下の対応付けが正しく設定されている必要があります。

- IPCOM VA2 が認識するインターフェース及びその構成定義
- IaaS のポート

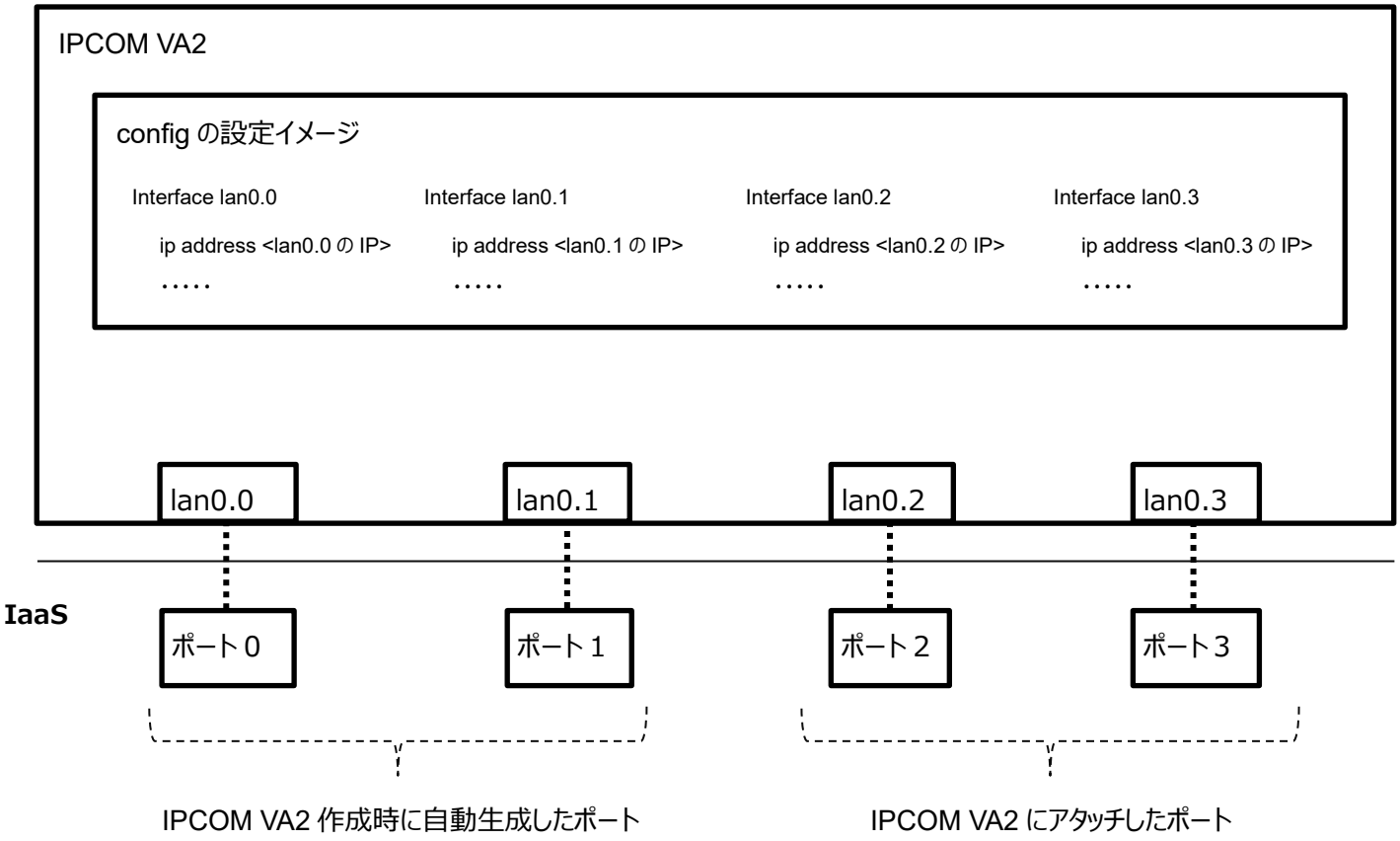
上記の対応付けの仕様を下図に示します。



- IPCOM VA2 では、アタッチされている IaaS のポートをインターフェースとして認識します。
- IPCOM VA2 におけるインターフェースの認識順番は以下の通りです。
  ① IPCOM VA2 作成時に自動生成された IaaS のポート
  ② IPCOM VA2 に対してアタッチした IaaS のポート
- IPCOM VA2 におけるインターフェースは、「lanX.Y」(「X」と「Y」はそれぞれ 0～3 の番号)の形式で扱われます。
- IPCOM VA2 は、前述のインターフェースの認識順番に従って「lan0.0」、「lan0.1」、「lan0.2」、「lan0.3」、「lan1.0」・・・(以降、省略)のようにインターフェースを認識します。
- IPCOM VA2 を設定する際は、config 内のインターフェース構成定義において、前述のインターフェース名と IaaS のポートに対応するネットワーク設定を行う必要があります。
- IPCOM VA2 にアタッチ済の IaaS のポートをデタッチした場合、IaaS の該当ポートに対応するインターフェースを経由した通信が IPCOM VA2 においてできなくなります。

・ IPCOM VA2 にアタッチ済の IaaS のポートをデタッチした後、IPCOM VA2 の再起動を行った場合、該当ポートに対応するインターフェースは IPCOM VA2 では認識されなくなります。その認識されなくなったインターフェースの名前は、後続の認識済のインターフェースに割り当たります。この時、インターフェース名の番号(「lanX.Y」の「X」と「Y」の部分)は順番に割り当たります。例えば「lan0.0」→「lan0.2」のように「lan0.1」を飛び越すような事はありません。
・ IPCOM VA2 が認識するインターフェース数については、IPCOM VA2 シリーズ VA2 ユーザーズガイド 「1-1-1 IPCOM VA2 シリーズのプラットフォーム」の「仮想 LAN インターフェース」を参照してください。

上記仕様の例を以降に示します。本例では、以下の条件により IPCOM VA2 を設定した場合について記載しています。
・ IPCOM VA2 作成時、IaaS の 2 つのポートを自動生成(下図の「ポート 0」「ポート 1」)
・ IPCOM VA2 に対し、2 つのポートをアタッチ(下図の「ポート 2」「ポート 3」)



前述のインターフェースの認識順序の仕様に示した通り、本例では、ポート 0～ポート 3 がそれぞれ lan0.0～lan0.3 として IPCOM VA2 に認識されます。

D-2 ネットワーク構成変更時のインターフェース構成定義変更手順

IPCOM VA2 は、ネットワーク構成変更等に伴うIaaSのポートのアタッチ/デタッチ操作による変更内容を、自動的には認識できません。IPCOM VA2 に対する IaaS のポートのアタッチ/デタッチ操作を行う際は、それに合わせて、以下の手順により IPCOM VA2 のインターフェース構成定義を再設定してください。

なお、本節に記載されているコマンドの実行結果は例です。実際の出力結果とは異なる場合があります。

(1) 構成定義の退避

現在の全インターフェース構成定義の内容を控えてください。次に構成定義を退避します。以下のコマンドを実行してください。ここで控えた内容は、後述のインターフェース構成定義の再設定時に使用します。

```
ipcom# save “任意の退避用ファイル名”
```

(2) インターフェース構成定義の仮設定

全インターフェースの定義を、以下のように仮設定してください。本作業は、後述の手順において、IaaS の各ポートと IPCOM VA2 が認識するインターフェースとの対応を確認するために必要です。

```
ipcom(edit)# interface <仮設定対象のインターフェース>
ipcom(edit-if)# ip address <任意の IP アドレス>
ipcom(edit-if)# exit
```

(3) 現設定を起動時の構成定義に保存

現在の設定を IPCOM VA2 起動時の構成定義に保存します。以下のコマンドを実行してください。

```
ipcom(edit)# save startup-config
```

(4) IPCOM VA2 の停止

IPCOM VA2 を停止します。以下のコマンドを実行してください。

```
ipcom# poweroff
```

(5) IaaS のネットワーク構成変更

IaaS のネットワーク構成変更を行ってください。必要に応じて IPCOM VA2 に対する IaaS のポートのアタッチ/デタッチを行ってください。

(6) IPCOM VA2 の起動

IPCOM VA2 を起動してください。

(7) IPCOM VA2 のインターフェースと IaaS のポートの関係の確認

IPCOM VA2 が認識するインターフェースと IaaS のポートとの関係は、両者の MAC アドレスが一致しているかどうかで判断できます。以下の手順により、全インターフェースと各 IaaS のポートの関係をそれぞれ確認してください。

・IPCOM VA2 が認識する各インターフェースの MAC アドレスを確認する。

```
ipcom# show interface
ipcom# lan0.0       MTU:    1500   <LINKUP>
ipcom#    Type: gigabit ethernet
ipcom#    Description:
ipcom#    MAC address: fa:16:3e:00:d4:0f
ipcom#    IP address: 192.168.10.10/24      Broadcast address: 192.168.10.255
・・・以下略・・
```

・IaaS のポートの MAC アドレスを確認する

IaaS の「5.5.5 List ports」API の実行結果から、該当ポートの MAC アドレスを確認してください。

```
# curl -k -s $NETWORK/v2.0/ports -X GET -H "X-Auth-Token: $OS_AUTH_TOKEN" | jq .
  {
 "ports": [
  {
      ・・・・略・・・・
      "mac_address": "fa:16:3e:00:d4:0f",
      ・・・・略・・・・
   "fixed_ips": [
   {
          "subnet_id": "33f92d78-9a2a-4688-9f4b-4bd467bf8d89",
          "ip_address": "192.168.10.10"
    }
   ],
```

(8) インターフェースの構成定義の変更

前述(7)で確認したインターフェースと IaaS のポートの関係を元に、IPCOM VA2 のインターフェース構成定義を再設定してください。

① MAC アドレスを元に、IaaS のポートに対応するインターフェース名 lanX.Y を特定する。

② IPCOM VA2 のインターフェース構成定義「interface lanX.Y」に対応する IaaS のポートの IP アドレスと構成定義を設定する。

上記設定の際、必要に応じて、(1)で控えたインターフェース構成定義を参照してください。

IaaS のポートの定義と、IPCOM VA2 のインターフェース構成定義が一致している事を確認後、IPCOM VA2 に現在の構成定義を即時反映します。以下のコマンドを実行してください。

```
ipcom(edit)# commit
```

(9) 疎通確認

IPCOM VA2 において、すべてのインターフェースの状態が「LINKUP」になっている事を確認します。以下のコマンドを実行してください。

```
ipcom# show interface
ipcom# lan0.0       MTU:    1500   <LINKUP>
ipcom#     Type: gigabit ethernet
ipcom#     Description:
ipcom#     MAC address: fa:16:3e:00:d4:0f
ipcom#     IP address: 192.168.10.10/24      Broadcast address: 192.168.10.255
・・・以下略・・
```

各インターフェースに対し、外部から通信ができる事を確認してください。

上記手順において、状態が「LINKUP」にならないインターフェースが存在する場合、または、外部からの通信ができないインターフェースが存在する場合、IaaS のポートと IPCOM VA2 のインターフェース構成定義が一致していない可能性があります。前述(7)の手順を行い、インターフェースと IaaS のポートの関係に誤りがないか確認してください。誤りがあった場合、(8)以降の手順を再度実施してください。

付録 E：IPCOM VA2 と IaaS の通信設定

E-1 通信設定の概要

IPCOM VA2 が通信を行う際に必要な通信設定の概要を以下に示します。本節を参照して、通信設定、およびその設定が意図した内容になっていることの確認を実施してください。

(1) 共通設定

IPCOM VA2 に必要な共通設定を下図に示します。

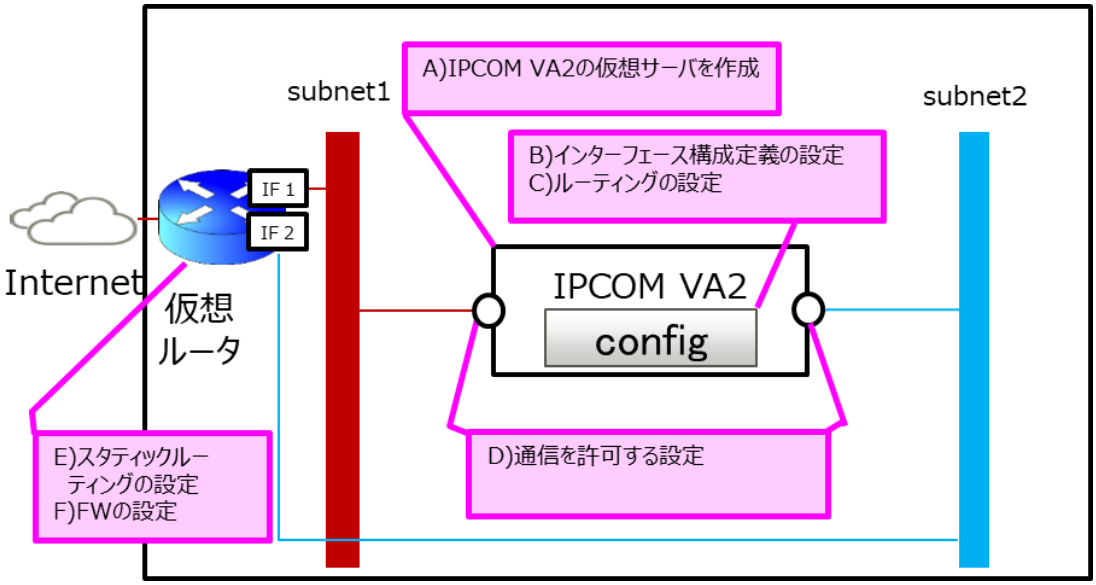


図 E-1-1：IaaS 上の IPCOM VA2 に必要な共通設定

A) IPCOM VA2 の仮想サーバを作成します。詳細は、IaaS API リファレンス（東日本リージョン 3／西日本リージョン 3）の「1.3.2 Create Server」をご確認ください。実行例は、4.1 【LS】IPCOM VA2 の作成(LS primary)をご確認ください。

IPCOM VA2 の仮想サーバを作成した後は、必ず以下の設定を順番に行ってください。

① 「license key」コマンドで、IPCOM VA2 にライセンスを登録してください。実行例は、5.2 【LS】IPCOM VA2 LS のライセンスキー登録をご確認ください。

② 「poweroff」コマンドで、IPCOM VA2 をシャットダウンしてください。

③ IaaS API リファレンス（東日本リージョン 3／西日本リージョン 3）の「2.3.2 Create a volume」API で、追加ボリュームを作成してください。「1.3.49 Attach a volume to an instance」API で、IPCOM VA2 に追加ボリュームをアタッチしてください。実行例は、5.3 【LS】追加ボリュームの作成およびアタッチ(LS primary)をご確認ください。

④ IaaS API リファレンス（東日本リージョン 3／西日本リージョン 3）の「1.3.18 Start Server」API またはポータルサイトより、IPCOM VA2 を起動してください。

⑤ 「user」、「password」、「hostname」の各コマンドで、ユーザー名、パスワード、ホスト名をそれぞれ設定してください。実行例は、7.1 ホスト名とパスワードの設定(LS primary)をご確認ください。

B) インターフェース構成定義を設定します。詳細は、E-4 インターフェース構成定義の設定をご確認ください。実行例は、7.2 インターフェースと冗長化設定(LS primary)をご確認ください。

C) デフォルトゲートウェイおよび静的ルーティングを設定します。詳細は、IPCOM EX シリーズ コマンドリファレンスガイドの「2.25.2.1.6 ip route」をご確認ください。該当設定は、IaaS のサブネットの設定(例：「host_routes」,「gateway_ip」)に対して自動的には反映されません。

D) IaaS のポートに対し、通信許可を設定します。詳細は、E-2 IaaS のポートの通信許可設定をご確認ください。

E) 仮想ルータに対し、必要に応じてスタティックルーティングを追加します。

F) 仮想ルータに対し、ファイアーウォールルールを設定します。詳細は、IaaS 機能仕様書の「6.6 ファイアーウォール」をご確認ください。設定例は、14.1 仮想ルータのファイアーウォールルールの設定 をご確認ください。

(2) サーバ負荷分散機能

サーバ負荷分散機能使用時に必要な設定を下図に示します。IaaS の IPCOM では、通過型ブリッジ(サーバ負荷分散の戻りの通信を IPCOM 経由にする)と IP アドレス変換を組み合わせた構成をサポートしています。IP アドレスやサブネットアドレス範囲を重複した構成(並列型ブリッジの構成、MAC アドレス変換、透過デバイス負荷分散)はサポートしておりません。

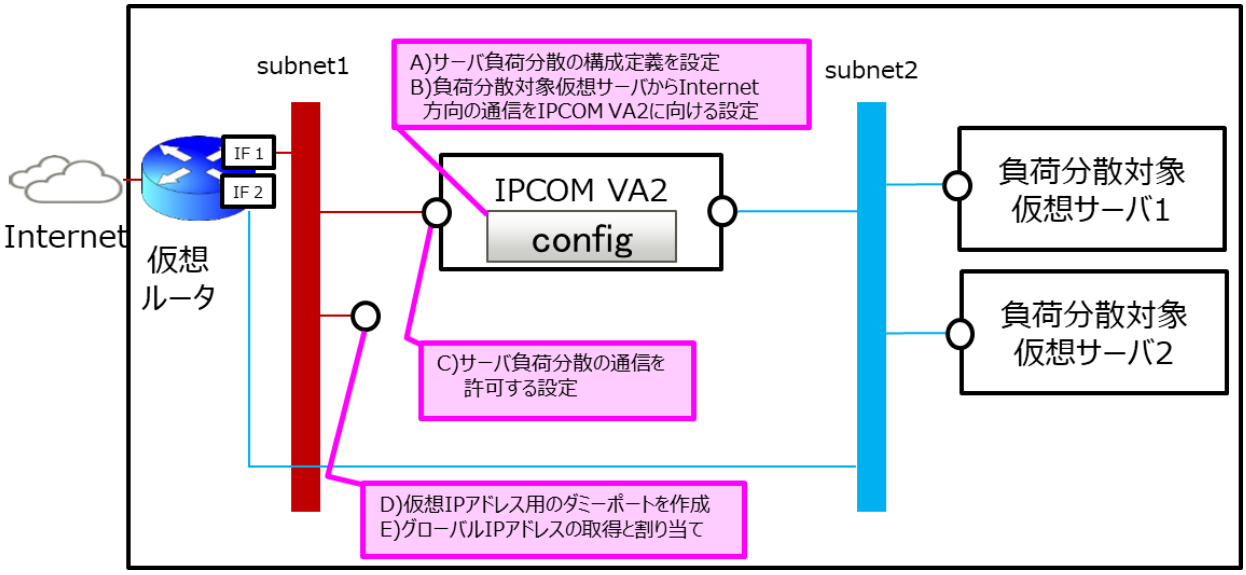


図 E-1-2：IaaS 上のサーバ負荷分散機能使用時に必要な設定

A) 仮想 IP アドレスを指定して、サーバ負荷分散用の構成定義(slb-rule)を設定します。詳細は、IPCOM EX シリーズ ユーザーズガイドの「2-6 サーバ負荷分散機能」、「2-6-9 構成定義情報の設定例」をご確認ください。

B) インターフェース構成定義に、負荷分散対象仮想サーバ向け通信の送信元 IP アドレスを IPCOM VA2 の IP アドレスに変換する設定(src-napt)を行ってください。本設定により、IPCOM VA2 と負荷分散対象仮想サーバの間における通信は以下のようになります。

表 E-1-3：IPCOM VA2 と負荷分散対象仮想サーバ間の通信のあて先および送信元 IP アドレス

通信方向	あて先 IP アドレス	送信元 IP アドレス
IPCOM VA2→負荷分散対象仮想サーバ	負荷分散対象仮想サーバ	IPCOM VA2
負荷分散対象仮想サーバ→IPCOM VA2	IPCOM VA2	負荷分散対象仮想サーバ

C) 物理インターフェースに紐づく IaaS のポートに対し、仮想 IP アドレス向けの通信許可を設定します。詳細は、E-2 IaaS のポートの通信許可設定をご確認ください。

D) 仮想 IP アドレス用のダミーポートを作成します。詳細は、E-3 ダミーポートの作成をご確認ください。

E) Internet から通信を行う場合、仮想 IP アドレスをグローバル IP アドレスに対応づけてください。詳細は、E-5 グローバル IP アドレスの設定をご確認ください。

本設定は、下図のようなワンアーム構成の場合も同様に実施してください。前述の B)を仮想ルータ側のインターフェース構成定義に設定してください。

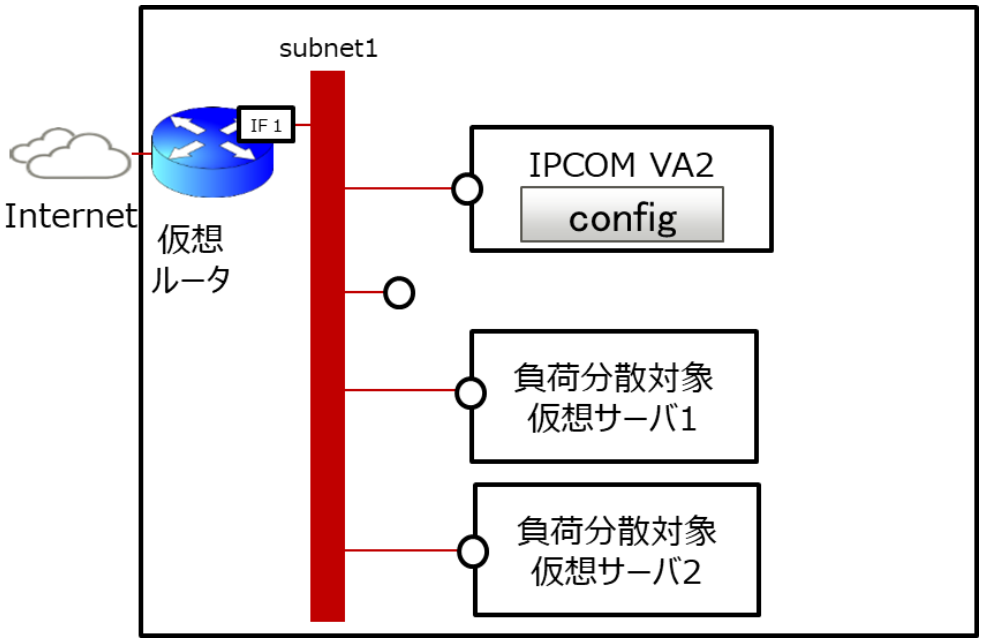


図 E-1-4：IaaS 上の 1 つのサブネットに IPCOM VA2 と負荷分散対象仮想サーバを配置したワンアーム構成

(3) ファイアーウォール機能

ファイアーウォール機能使用時に必要な設定を下図に示します。

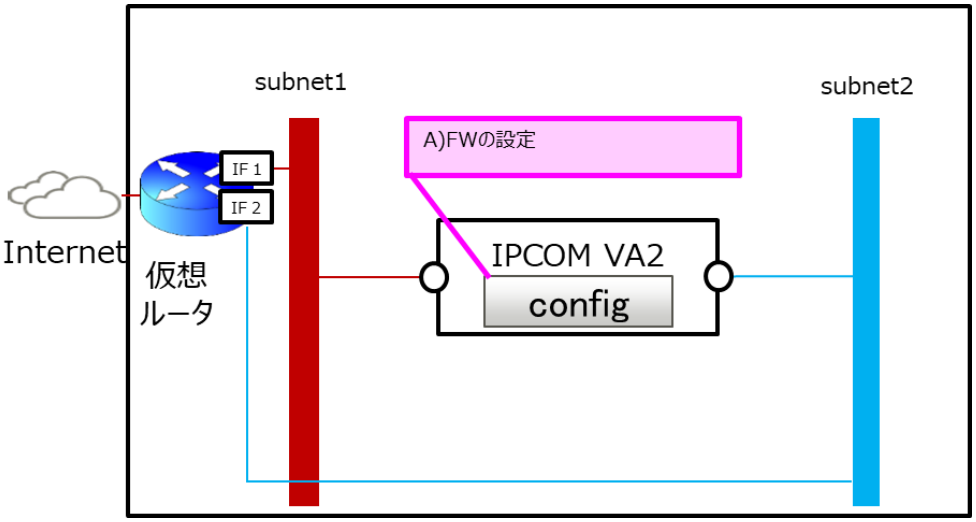


図 E-1-5：IaaS 上のファイアーウォール機能使用時に必要な設定

A) IPCOM VA2 の構成定義にファイアーウォールのルールを設定します。詳細は、IPCOM EX シリーズ ユーザーズガイドの「2-10 ファイアーウォール機能」をご確認ください。

(4) 冗長化構成

冗長化構成に必要な設定を下図に示します。

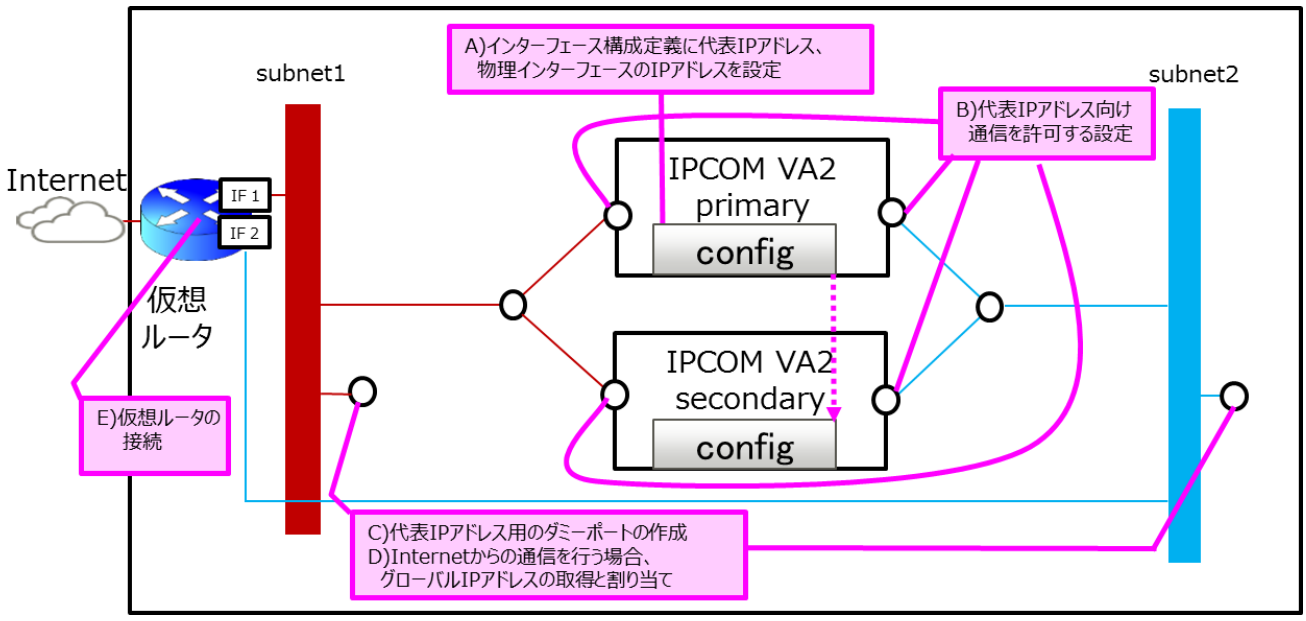


図 E-1-6：IaaS 上の冗長化構成に必要な設定

A) 代表 IP アドレスと Primary/Secondary の物理インターフェースの IP アドレスをインターフェース構成定義に設定します。詳細は、E-4 インターフェース構成定義の設定をご確認ください。

B) 物理インターフェースに紐づく IaaS のポートに対し、代表 IP アドレス向けの通信許可を設定します。詳細は、E-2 IaaS のポートの通信許可設定をご確認ください。

C) 代表 IP アドレス用のダミーポートを作成します。詳細は、E-3 ダミーポートの作成をご確認ください。

D) Internet から代表 IP アドレス向けの通信を行う場合、代表 IP アドレスをグローバル IP アドレスに対応づけてください。詳細は、E-5 グローバル IP アドレスの設定をご確認ください。

E) IPCOM VA2 に接続するサブネットに仮想ルータを接続してください。サブネットに仮想ルータが無い場合、通信性能に影響がでる可能性があります。

E-2 IaaS のポートの通信許可設定

IPCOM VA2 の各物理インターフェースに紐づく IaaS のポートに通信許可(ルーティング許可)を設定します。

IaaS API リファレンス（東日本リージョン 3／西日本リージョン 3）の「5.5.3 Update port」API により、該当ポートに通信許可設定を追加してください。API のパラメータは、以下の形式で指定してください。本 API の実行例は、6.1 ルーティング許可の設定をご確認ください。

表 E-2-1：「5.5.3 Update port」API に指定するパラメータ

パラメータ名	設定内容	備考
allowed_address_pairs ※1	以下の順で IP アドレス("ip_address")を指定します。MAC アドレス(“mac_address”)は指定しないでください。 ① 通信を許可する IP アドレスの範囲(CIDR 形式) ② 代表 IP アドレス(CIDR 形式不可) ※2 ③ 仮想 IP アドレス(CIDR 形式不可) ※2	・シングル構成の場合、②は設定不要です。 ・③の仮想 IP アドレスが複数ある場合、すべて指定してください。

※1「allowed_address_pairs」に指定する通信許可アドレスペア数には上限があります。詳細は、IaaS 機能仕様書の「A.1 制限値」の「ネットワークに関する制限値」にある「ポートに設定可能な通信許可アドレスペア数」をご確認ください。

※2 ②、③の各アドレスを使用した通信を行うためには、IaaS のダミーポートが必要です。詳細は、E-3 ダミーポートの作成をご確認ください。

E-3 ダミーポートの作成

仮想 IP アドレス用、代表 IP アドレス用のダミーポートを作成します。

IaaS API リファレンス（東日本リージョン 3／西日本リージョン 3）の「5.5.6 Create port」API により、ダミーポートを作成してください。API のパラメータは、以下の形式で指定してください。本 API のパラメータに「allowed_address_pairs」は指定しないでください。

表 E-3-1：「5.5.6 Create port」API に指定するパラメータ

名前	設定内容	備考
fixed_ips	仮想 IP アドレス/代表 IP アドレスと対応するサブネットの ID を指定します。	
security_groups	IPCOM VA2 の物理インターフェースに紐づくポートのセキュリティグループの ID を指定します。	
device_owner	"nuage:vip"を指定します。	

E-4 インターフェース構成定義の設定

インターフェース構成定義を設定します。詳細は、IPCOM EX シリーズ コマンドリファレンスガイドの「2.4.2.15 interface」をご確認ください。インターフェース構成定義(interface lanX.Y)に指定する IP アドレスは、以下の形式で指定してください。

IPCOM VA2 の IP アドレスの詳細は、D-1 IPCOM VA2 のインターフェースと IaaS のポートの関係をご確認ください。

表 E-4-1：インターフェース構成定義に設定する IP アドレス

インターフェース構成定義の定義名	設定内容	備考
ip address	冗長化構成の場合、代表 IP アドレスを指定します。 シングル構成の場合、物理インターフェースに紐づく IaaS のポートの IP アドレスを指定します。	
ip address primary	冗長化構成の場合、Primary の物理インターフェースに紐づく IaaS のポートの IP アドレスを指定します。	
ip address secondary	冗長化構成の場合、Secondary の物理インターフェースに紐づく IaaS のポートの IP アドレスを指定します。	

E-5 グローバル IP アドレスの設定

Internet から IPCOM VA2 に通信を行う場合、IPCOM VA2 に設定した IP アドレスをグローバル IP アドレスに対応づけます。1 つの IP アドレスを複数のグローバル IP アドレスに対応づけないでください。

表 E-5-1：グローバル IP アドレスに対応づける IP アドレス

通信	グローバル IP アドレスに対応づける IP アドレス	備考
サーバ負荷分散の通信	仮想 IP アドレス	
冗長化構成時の通信	代表 IP アドレス	
シングル構成時の通信	物理インターフェースの IP アドレス	

E-6 チェックサム値の検査の設定

チェックサム値の検査を行う機能(protect checksum-inspection)を無効にしてください。本機能を有効にした場合、IPCOM VA2 で正常なパケットを破棄してしまうことがあります。

E-7 MTU 値の設定

IaaS 上の IPCOM VA2 の MTU 値は、通信の最適化のため、8950 を推奨しています。

ただし、以下の条件に該当する場合、利用者の環境に沿った最適な MTU 値を設定してください。

(1) インターネットの通信を多用する場合（インターネット通信のパケットサイズは上り下り共に 1500byte になります）

・IPCOM および IPCOM と通信する仮想サーバの MTU を 1500 に統一してください。

(2) IPCOM VA2 経由の通信で、パス MTU ディスカバリが機能せず通信できない場合

・IPCOM および仮想ルータ、仮想サーバで ICMP(code3 type4)の通信許可を設定してください。

(3) 表 E-7-1 の「構成」に示した条件で当該機能を使用する場合

・表 E-7-1 の「MTU 値の設定」に示した値に設定してください。

表 E-7-1：特定機能使用時の MTU 値の設定

構成		MTU 値の設定			
サーバ負荷分散の HTTP Keep Alive 負荷分散または Web アクセラレーション	SSL アクセラレーター	IPCOM のインターフェース		クライアントのインターフェース	負荷分散対象サーバのインターフェース
		クライアント側	負荷分散対象サーバ側		
○	－	8950	8950	8232 以下	8232 以下
○	○	8232	8232	8232 以下	8232 以下
－	○	8950	8950	8950 以下	8950 以下

○：機能を使用する　－：機能を使用しない

E-8 セキュリティグループのステートレス設定

IaaS 上の IPCOM VA2 で使用するポートにおけるステートレスセキュリティグループについて記載します。IPCOM では、ステートレス・セキュリティグループを利用してください。ステートフル・セキュリティグループと比べて以下の特徴があります。

- より高いトランザクション性能を出せる
- より多くのコネクション（対地間接続、同時アクセス）を可能にする
- 冗長切り替え時、切り替え先の IPCOM に既存のコネクションを切断することなく継続的に引き継ぎ可能にする

表 E-8-1：IPCOM のポートにおけるセキュリティグループの設定

通信	下図のポート	推奨設定	説明
仮想ルータのファイアーウォール機能を介した通信があるポート	1 3	ステートレス	・ステートレスを利用する場合、機能説明書のファイアーウォールサービスとステートレス・セキュリティグループの組み合わせのページを確認し、必要に応じて対処してください。機能説明書のファイアーウォールサービス ファイアーウォールルールの作成／変更のヒントに記載されている双方向の通信を許可するファイアーウォールルールを追加済みの場合、上記の確認は不要です。 ・ステートフルを利用する場合、装置切り替え時に通信断が発生する可能性があります。
	2	-	・ダミーポートのセキュリティグループの設定は不要です。設定されていても影響はありません。
仮想ルータのファイアーウォール機能を介した通信がないポート	4	ステートレス	・ステートレスを利用する場合、特に制約はありません。 ・ステートフルを利用する場合、装置切り替え時に通信断が発生する可能性があります。
	5	-	・ダミーポートのセキュリティグループの設定は不要です。設定されていても影響はありません。
	6	-	・ステートレスを利用する場合、特に制約はありません。 ・ステートフルを利用する場合、特に制約はありません。

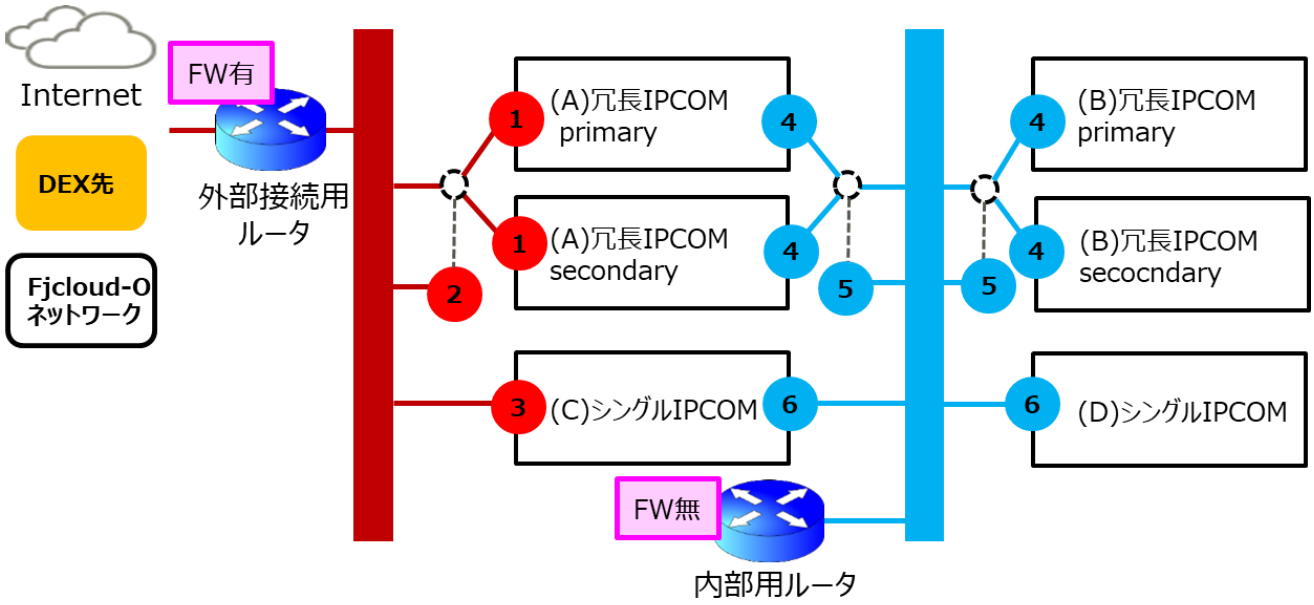


図 E-8-1：IPCOM のポートにおけるセキュリティグループ推奨設定の例

ファイアーウォールサービスとステートレス・セキュリティグループの組み合わせの詳細は、以下のマニュアルをご確認ください。

- IaaS ドキュメント・ツール類 機能説明書
  + ネットワーク [東日本第 3／西日本第 3]
    + ファイアーウォールサービス
      + ファイアーウォールサービスとステートレス・セキュリティグループの組み合わせ

ステートフル・ステートレスの詳細については、以下のマニュアルをご確認ください。

- FUJITSU Hybrid IT Service FJcloud-O 設計・構築ガイド（デザインパターン・実装サンプル集）
  + ステートレスセキュリティグループ［東日本／西日本リージョン 3 向け］

IPCOM の装置切り替えの通信影響については、以下のマニュアルをご確認ください。

- IPCOM EX シリーズ ユーザーズガイド
  + A.4 装置切り替え時のエンド間の通信への影響

FUJITSU Hybrid IT Service FJcloud-O IaaS

IPCOM VA2 スタートガイド 2.7 版

発行日 2023 年 9 月

●本書の内容は、改善のため事前連絡なしに変更することがあります。