FUJITSU Hybrid IT Service FJcloud-O IaaS

IPCOM VE2m スタートガイド

Version 1.4

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 VE2m (以下、IPCOM VE2m 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 VE2m をご利用ください。

本書は、西日本第 1/第 2 リージョン、東日本第 1/第 2 リージョンを対象としています。

本書の読者

本書は、IPCOM VE2m 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 VE2m 100 LS PLUS
- IPCOM VE2m 220 LS
- IPCOM VE2m 220 LS PLUS
- IPCOM VE2m 100 SC
- IPCOM VE2m 220 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 VE2m (アイピーコム ブイイーツーエム)	FUJITSU Hybrid IT Service FJcloud-O IaaS – IPCOM VE2m の略称です。IPCOM VE2 の FUJITSU Hybrid IT Service FJcloud-O IaaS 版派生製品であるため、IPCOM VE2 のドキュメントを参照可能です。なお、IPCOM VE2m と IPCOM VE2 は製品番号上、異なる製品になります。
IaaS	FUJITSU Hybrid IT Service FJcloud-O IaaS の略称です。
Primary	IPCOM VE2m 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)です。
Secondary	IPCOM VE2m 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 VE2m に定義する IP アドレスです。
代表 IP アドレス	2 台の IPCOM VE2m 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 VE2m 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 VE2m へのアタッチは不要です。

語句	定義の説明
ライセンスキー	IPCOM VE2m 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。
FW	ファイアーウォール(FireWall)の略称です。
LAN	IPCOM VE2m のネットワークインターフェースの名称です。
物理インターフェース	本書では、IaaS のポートに紐づく IPCOM VE2m 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 VE2m の設定に関する初期段階の説明を記載しております。 IPCOM VE2m 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。

マニュアル名称	目的・用途
IPCOM VE2 ソフトウェアシリーズ 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 VE2 ソフトウェアシリーズ VE2 ユーザーズガイド	IPCOM VE2 が提供する機能、IPCOM EX2 シリーズとの機能差分などについて説明しています。IPCOM VE2 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 EX2 ソフトウェアシリーズ ユーザーズガイド	IPCOM EX2 ソフトウェアシリーズの機能、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 EX2 ソフトウェアシリーズ 事例集	IPCOM EX2 ソフトウェア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 EX2 ソフトウェアシリーズ コンソールリファレンスガイド	IPCOM EX2 ソフトウェアシリーズの 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 EX2 ソフトウェアシリーズ コマンドリファレンスガイド	IPCOM EX2 ソフトウェア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 EX2 ソフトウェアシリーズ 保守ガイド	IPCOM EX2 ソフトウェア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 VE2m シリーズは、IPCOM EX2 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 EX2 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先としています。

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 VE2m の使用条件について

IPCOM VE2m 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 VE2m 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 VE2m をご使用ください。

IPCOM VE2m 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	2020 年 6 月 15 日	初版作成	
1.1	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
1.2	2021 年 3 月 16 日	5.2【LS】IPCOM VE2m LS のライセンスキー登録 5.7【SC】IPCOM VE2m SC のライセンスキー登録	設定内容の改善。 ライセンス入力後の操作内容を修正
1.3	2022 年 11 月 16	1.2 提供機能	記載内容の改善。 SSL アクセラレーター機能の TLS v1.3 の提供機能の追加
1.4	2024 年 10 月 17 日	付録 D：IPCOM VE2m および IaaS の構成	記載内容の改善。 新しいインタフェースの仕様を追加

目次

第 1 章　IPCOM VE2m の概要、機能一覧

FUJITSU Hybrid IT Service FJcloud-O IaaS – IPCOM VE2m 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 IaaS 上の IPCOM VE2m の製品仕様

IaaS 上の IPCOM VE2m 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。本製品を構成するシリーズは以下のとおりです。

表 1-1 製品の主要なサポート機能

製品名	主要サポート機能	対応する旧製品(VA2)
IPCOM VE2m 100 LS PLUS	サーバ負荷分散機能、WAF	IPCOM VA2 1300 LS (EX)
IPCOM VE2m 220 LS	サーバ負荷分散機能、SSL アクセラレーター機能	IPCOM VA2 2500 LS (SSL)
IPCOM VE2m 220 LS PLUS	サーバ負荷分散機能、SSL アクセラレーター機能、WAF	—
IPCOM VE2m 100 SC	ファイアーウォール機能	IPCOM VA2 1300 SC
IPCOM VE2m 220 SC	ファイアーウォール機能	IPCOM VA2 2500 SC

IaaS 上の IPCOM VE2m 製品が必要とする仮想ハードウェアリソースは以下のとおりです。
仮想マシンのカスタム構成は以下のように設定してください。異なる構成や設定値を選択した場合は、起動に失敗する場合がありますのでご注意ください。

表 1-2 仮想ハードウェアリソース

項目名	VE2m 100	VE2m 220
仮想 CPU 数	1	4
仮想メモリ量	4(GB)	8(GB)
仮想ディスク 1(システムディスク)容量	4(GB)	4(GB)
仮想ディスク 2(拡張ディスク)容量	100(GB)	100(GB)
仮想 LAN インターフェース	最大 8 port	最大 16 port

※1 仮想ディスク 1 は必須です。

※2 仮想ディスク 2 は必須です。

※3 LAN インターフェースの名称は以下のとおりです。本製品の LAN インターフェースは、IPCOM VE2m 起動時に lan0.0 から順番に自動で括りつけが行われます。詳細は、D-1 IPCOM VE2m 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 1-0-1 LAN インターフェース名称

LAN インターフェース		備考
LAN0.	0 ～ 3	IaaS 上の IPCOM VE2m 全シリーズ
LAN1.	0 ～ 3	
LAN2.	0 ～ 3	IaaS 上の IPCOM VE2m 220
LAN3.	0 ～ 3	

1.2 提供機能

IaaS 上の IPCOM VE2m の提供機能について説明します。

1-2-1 レイヤー2 中継機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
ブリッジ(MAC 学習)		●	●	●	●	●
VLAN	ポート VLAN	×	×	×	×	×
	MAC-VLAN	×	×	×	×	×
	tagVLAN	×	×	×	×	×
	VLAN 間レイヤー2 中継	×	×	×	×	×
	VLAN パススルー	×	×	×	×	×
	802.1p タグ優先度	×	×	×	×	×

● : 基本機能 ×: 未サポート

1-2-2 PPPoE クライアント機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能	サポート可否				
	100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
PPPoE マルチセッション	×	×	×	●	●
固定/ 自動/Unnumbered 接続	×	×	×	●	●
接続切断制御	×	×	×	●	●
セッションキープアライブ（監視/ 自動再接続）	×	×	×	●	●
TCP/MSS 値書き換え	×	×	×	●	●
DNS/ ルーティング情報の自動登録	×	×	×	●	●

● : 基本機能 ×: 未サポート

1-2-3 レイヤー3 中継機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
ルーティング(IPv4)	スタティック	●	●	●	●	●
	RIP v1	●	●	●	●	●
	RIP v2 （MD5 認証）	●	●	●	●	●
	OSPFv2	●	●	●	●	●
	BGP4	●	●	●	●	●

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
MTU	IP フラグメント	●	●	●	●	●
	MTU 長変更	●	●	●	●	●
フィルタリング(IPv4)	送受信 IP Address	●	●	●	●	●
	IP Precedence	●	●	●	●	●
	IP ToS	●	●	●	●	●
	Protocol(TCP/UDP/ICMP)	●	●	●	●	●
	ICMP type/code	●	●	●	●	●
	TCP src/dst port	●	●	●	●	●
	TCP syn/ack	●	●	●	●	●
	UDP src/dst port	●	●	●	●	●
レイヤー3 中継機能 On/Off		●	●	●	●	●

● : 基本機能 ×: 未サポート

1-2-4 レイヤー3 中継機能(IPv6)

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
ルーティング(IPv6)	RA	×	×	×	×	×
	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(IPv4)	送受信 IPv6 アドレス	×	×	×	×	×
	IP flow label	×	×	×	×	×
	Protocol(TCP/UDP/ICMPv6)	×	×	×	×	×
	ICMPv6 type/code	×	×	×	×	×
	TCP src/dst port	×	×	×	×	×
	TCP syn/ack	×	×	×	×	×
	UDP src/dst port	×	×	×	×	×
レイヤー3 中継機能 On/Off		×	×	×	×	×

● : 基本機能 ×: 未サポート

1-2-5 サーバ負荷分散機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
配置方法・動作モード	並列型ブリッジ	×	×	×	×	×
	通過型ブリッジ	●	●	●	×	×
	ブリッジ・ルータ	●	●	●	×	×
転送方式	IP アドレス変換	●	●	●	×	×
	MAC アドレス変換	●	●	●	×	×
サーバ分散方式	ラウンドロビン	●	●	●	×	×
	静的な重み付け	●	●	●	×	×
	最小コネクション数	●	●	●	×	×
	最小クライアント数	●	●	●	×	×
	最小サーバ負荷	×	×	×	×	×
	最小データ通信量	●	●	●	×	×
	最小応答時間	●	●	●	×	×
	最小待ちメッセージ数（IIOP 負荷分散）	×	×	×	×	×
	最小通信バッファ使用率（IIOP 負荷分散）	×	×	×	×	×
	最小 FNA LU 数	×	×	×	×	×
コンテンツタイプ負荷分散	URL ベース負荷分散	●	●	●	×	×
	HTTP ヘッダー負荷分散	●	●	●	×	×
Web アクセラレーション		●	●	●	×	×
分散単位	ノード単位	●	●	●	×	×
	コネクション単位	●	●	●	×	×
一意性保証（セッション維持）	cookie	●	●	●	×	×
	URL リライト	●	●	●	×	×
	SSL セッション ID	●	●	●	×	×
	HTTP ヘッダー情報	●	●	●	×	×
	HTTP 認証情報ヘッダー	●	●	●	×	×
故障監視（監視方式）	装置監視方式（レイヤー3）	●	●	●	×	×
	サービス監視方式（レイヤー4）	●	●	●	×	×
	アプリケーション監視（レイヤー7）	●	●	●	×	×
	負荷計測エージェント監視	×	×	×	×	×

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
拡張型故障監視（監視方式）	拡張型サービス監視方式（レイヤー4）	●	●	●	×	×
	拡張型アプリケーション監視方式（レイヤー7）	●	●	●	×	×
故障監視（オプション機能）	URL リダイレクト	●	●	●	×	×
	可変 URL リダイレクト	●	●	●	×	×
	HTTP エラーメッセージ転送	●	●	●	×	×
	コネクションリセット	●	●	●	×	×
セッション・リカバリー		●	●	●	×	×
ポート多重化		●	●	●	×	×
アクセス数の制限	最大コネクション数	●	●	●	×	×
	最大クライアント数	●	●	●	×	×
バックアップサーバ		●	●	●	×	×
クライアントの関連づけ		●	●	●	×	×
サーバ保守制御		●	●	●	×	×
スロースタート制限		●	●	●	×	×
透過デバイス負荷分散		●	●	●	×	×
IIOP 負荷分散		×	×	×	×	×
分散対象パケットの置換機能		●	●	●	×	×
BackToBack 機能		●	●	●	×	×
HTTP Keep-Alive 負荷分散		●	●	●	×	×

● ： 基本機能 ×： 未サポート

1-2-6 QoS 制御（帯域制御）機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
動作モード	ブリッジモード	●	●	●	×	×
	ルータモード	●	●	●	×	×
優先転送		●	●	●	×	×
最低帯域保証		●	●	●	×	×
最大帯域幅（帯域制限）		●	●	●	×	×
仮想回線の階層化		●	●	●	×	×
トラフィック分類	汎用フィルター条件	●	●	●	×	×

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
	ダイナミックポート・アプリケーションの識別・分類	●	●	●	×	×
	メディアタイプの識別・分類	●	●	●	×	×
	ストリーミング・アプリケーションの識別・分類	●	●	●	×	×
	P2P アプリケーションの識別・分類	●	●	●	×	×
	非 IP トラフィックの識別・分類	●	●	●	×	×
均等割り当て	セッション単位	●	●	●	×	×
	ノード単位	●	●	●	×	×
	転送元 IP アドレス単位	●	●	●	×	×
	転送先 IP アドレス単位	●	●	●	×	×
アドミッション制御	拒否/ 破棄/ 受け入れ/ リダイレクト	●	●	●	×	×
	SIP ビジー制御	●	●	●	×	×
パケットサイズの最適化	IP フラグメンティング	●	●	●	×	×
	IP フラグメントの無効化	●	●	●	×	×
	TCP セグメンティング（MSS 値書き換え）	●	●	●	×	×
VLAN ユーザープライオリティ・マーキング		×	×	×	×	×
ToS マーキング（IPv6 Traffic Class マーキング）		×	×	×	×	×
IEEE 802.1Q/ToS マッピング（IPv6 Traffic Class マッピング）		×	×	×	×	×
ポリシースケジューリング		●	●	●	×	×
フェールオーバーマネジメント		●	●	●	×	×
最大キューサイズのカスタマイズ		●	●	●	×	×
帯域仮想専用線		●	●	●	×	×
トラフィックディスカバリ		●	●	●	×	×

● ： 基本機能 ×： 未サポート

1-2-7 リンク負荷分散機能

本製品ではサポートしていません。

1-2-8 クラウドプロキシ機能

本製品ではサポートしていません。

1-2-9 ファイアーウォール機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能			サポート可否				
			100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
動作モード	ブリッジモード		●	●	●	●	●
	ルータモード		●	●	●	●	●
構成定義	アクセス制御ルール		●	●	●	●	●
	アクセス制御マップ		●	●	●	●	●
アクセス制御	汎用フィルター条件		●	●	●	●	●
	ダイナミックポート・アプリケーションの追跡		●	●	●	●	●
	P2P アプリケーションの追跡		●	●	●	●	●
	メディアタイプの追跡		●	●	●	●	●
	ストリーミング・アプリケーションの追跡		●	●	●	●	●
	アクセス制御アクション	受諾(ACCEPT)	●	●	●	●	●
		廃棄(DROP)	●	●	●	●	●
		認証(auth)	×	×	×	×	×
		拒否(REJECT)	●	●	●	●	●
		リダイレクト (REDIRET)	●	●	●	●	●
		無効化 (REMOVE)	●	●	●	●	●
セッションログ（標準形式/WELF 形式）			●	●	●	●	●

● ： 基本機能 ×： 未サポート

1-2-10 IPS 機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能				サポート可否				
				100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
アノマリ型 IPS	動作モード	ブリッジモード		●	●	●	●	●
		ルータモード		●	●	●	●	●
	疑わしいアクセスおよび DoS 攻撃の検出と防御	攻撃防御ルール		●	●	●	●	●
		攻撃防御アクション	廃棄(DROP)	●	●	●	●	●
			ブロック(BLOCK)	●	●	●	●	●
	アクセス数規制	接続元コネクション数制限		●	●	●	●	●

機能			サポート可否				
			100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
		接続先コネクション数制限	●	●	●	●	●
	セッションログ（標準形式/WELF 形式）		●	●	●	●	●
シグネチャー型 IPS	動作モード	ブリッジモード	×	×	×	×	×
		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）		×	×	×	×	×

● ： 基本機能 ×: 未サポート

1-2-11 WAF 機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
動作モード	ブリッジモード	●	×	●	×	×
	ルータモード	●	×	●	×	×
防御動作（アクション）	通過	●	×	●	×	×
	拒否	●	×	●	×	×
	エラーページ応答	●	×	●	×	×

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
	リダイレクト応答	●	×	●	×	×
防御機能	リクエストライン規制	●	×	●	×	×
	HTTP ヘッダー規制	●	×	●	×	×
	メッセージボディ規制	●	×	●	×	×
	パラメーター規制	●	×	●	×	×
	ファイル転送規制	●	×	●	×	×
	改ざん	●	×	●	×	×
	アクセス違反	●	×	●	×	×
	脆弱性攻撃防御	●	×	●	×	×
クローキング（情報隠蔽）	HTTP レスポンスヘッダー	●	×	●	×	×
	HTTP レスポンスのステータスコード	●	×	●	×	×
	HTML コメント	●	×	●	×	×
	クレジットカード番号	●	×	●	×	×
	マイナンバー	●	×	●	×	×
学習		●	×	●	×	×
WAF ログ		●	×	●	×	×
検知イベントのメール通知		●	×	●	×	×
脆弱性レポート		●	×	●	×	×

● ： 基本機能 ×： 未サポート

1-2-12 Web コンテンツ・フィルタリング機能

本製品ではサポートしていません。

1-2-13 アンチウィルス機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
プロトコル	SMTP	×	×	×	×	×
	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 （接続元 IP アドレス隠蔽モード）	×	×	×	×	×
ウィルスパターンフ	自動	×	×	×	×	×

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
ァイルのアップデート						
	手動	×	×	×	×	×
スパムメール対策	SMTP	×	×	×	×	×
	POP3	×	×	×	×	×

● ： 基本機能 ×: 未サポート

1-2-14 標的型攻撃対策連携機能

本製品ではサポートしていません。

1-2-15 アドレス変換機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能	サポート可否				
	100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
送信元 IP アドレス変換(SNAT)	●	●	●	●	●
送信元 IP アドレス/ ポート変換(SNAPT)	●	●	●	●	●
あて先 IP アドレス変換(DNAT)	●	●	●	●	●
あて先 IP アドレス/ ポート変換(DNAPT)	●	●	●	●	●
ダイナミックポート・アプリケーション対応	●※	●※	●※	●※	●※

● ： 基本機能 ×: 未サポート

※通信経路で NAT しない構成で使用する場合に限りサポートします。IaaS 上の仮想ルータは同機能を有していないため、グローバル IP を使用した通信では、使用できません。

1-2-16 ユーザー認証機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
認証パスワード	固定パスワード（PAP 方式）	●	●	●	●	●
	固定パスワード（CHAP 方式）	●	●	●	●	●
	固定パスワード（MS-CHAP-V2 方式）（L2TP/IPsec 時）	×	×	×	×	×
	S/Key ワンタイムパスワード	×	×	×	×	×
	SecurID ワンタイムパスワード	×	×	×	×	×
	X.509 デジタル証明書（SSL-VPN/SSL アクセラレーター時）	×	●	●	×	×

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
	EAP （L2TP/IPsec 時）	×	×	×	×	×
ユーザー認証/管理	ローカル認証	●	●	●	●	●
	RADIUS 連携	●	●	●	●	●
	LDAP	●	●	●	●	●
	TACACS+	●	●	●	●	●
ユーザーの正当性検証		●	●	●	●	●
認証許可条件の検証		●	●	●	●	●
ユーザーロール選択条件の検証		●	●	●	●	●
ユーザーロールベースのアクセス制御		●	●	●	●	●

● ： 基本機能 ×： 未サポート

1-2-17 IPsec-VPN 機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
IPsec 動作モード	トンネルモード	×	×	×	×	×
セキュリティタイプ	AH （リプレイ防御機能）	×	×	×	×	×
	ESP （リプレイ防御機能）	×	×	×	×	×
暗号アルゴリズム	DES	×	×	×	×	×
	3DES	×	×	×	×	×
	AES(128/192/256)	×	×	×	×	×
認証アルゴリズム	MD5	×	×	×	×	×
	SHA1	×	×	×	×	×
	SHA2(256/384/512)	×	×	×	×	×
ポリシーベース IPsec-VPN		×	×	×	×	×
Hub and Spoke 中継		×	×	×	×	×
IP フラグメント		×	×	×	×	×
IPsec トンネル分散（リンク負荷分散連携）		×	×	×	×	×
IPsec マルチホーミング		×	×	×	×	×
パス MTU ディスカバリ/MSS 書き換え		×	×	×	×	×
障害時の SA 自動復旧		×	×	×	×	×
ダイナミックネットワークのサポート		×	×	×	×	×
Commit ビット		×	×	×	×	×
セキュリティパラメーター設定の簡略化		×	×	×	×	×
同時接続最大数制限		×	×	×	×	×
NAT トラバーサル		×	×	×	×	×

機能			サポート可否				
			100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
ファイアーウォール連携			×	×	×	×	×
鍵管理機能	鍵交換	Manual	×	×	×		
		IKE	×	×	×	×	×
	IKE 認証方式	Pre-shared Key	×	×	×	×	×
		Digital signature	×	×	×	×	×
	IKE Phase1 モード	Main mod	×	×	×	×	×
		Aggressive mode	×	×	×	×	×
	IKE Phase2 モード	Quick mode	×	×	×	×	×
	Diffie Hellman (DH)	Group 1, 2, 5, 14	×	×	×	×	×
	PFS		×	×	×	×	×

● ： 基本機能 ×: 未サポート

1-2-18 L2TP/IPsec 機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
認証機能	接続認証	×	×	×	×	×
	ユーザー認証	×	×	×	×	×
	パスワード変更機能	×	×	×	×	×
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	×	×	×	×	×
ファイアーウォール連携		×	×	×	×	×
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		×	×	×	×	×

● ： 基本機能 ×: 未サポート

1-2-19 SSL アクセラレーター機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能			サポート可否				
			100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
プロトコル	SSL v3.0		×	●	●	×	×
	TLS v1.0		×	●	●	×	×
	TLS v1.1		×	●	●	×	×
	TLS v1.2		×	●	●	×	×
	TLS v1.3		×	●	●	×	×
暗号スイート	鍵交換	RSA, ECDHE_RSA ECDHE_ECDSA	×	●	●	×	×
	暗号化	3DES, AES, RC4, AES_GCM ChaCha20-Poly1305	×	●	●	×	×
	ハッシュ	MD5, SHA1, SHA256, SHA384	×	●	●	×	×
サービス中継	HTTPS, SMTPS, NNTPS, LDAPS, TELNETS, IMAPS, POP3S		×	●	●	×	×
HTTP ヘッダー書き換え			×	●	●	×	×
クライアント認証			×	●	●	×	×
セキュアーcookie			×	●	●	×	×

● : 基本機能 ×: 未サポート

1-2-20 SSL-VPN 機能

本製品ではサポートしていません。

1-2-21 HTTP コンテンツ圧縮機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能	サポート可否				
	100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
HTTP 通信	●	●	●	●	●
HTTPS 通信	×	●	●	×	×

● : 基本機能 ×: 未サポート

1-2-22 FNA ルーティング機能

本製品ではサポートしていません。

1-2-23 HTTP ネットワークサービス機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能	サポート可否				
	100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
DHCP サーバ	×	×	×	●	●
DHCP リレーエージェント	×	×	×	●	●
DHCP クライアント	●	●	●	●	●
DNS サーバ	×	×	×	●	●
DNS プロキシ	×	×	×	●	●

● ： 基本機能 ×： 未サポート

1-2-24 ビジュアライザ機能

本製品ではサポートしていません。

1-2-25 認証・検疫ゲートウェイ機能

本製品ではサポートしていません。

1-2-26 高信頼性機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能		サポート可否				
		100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
自動復電		×	×	×	×	×
ホットスタンバイ（監視プロトコル）	VRRP ベースの独自	●	●	●	●	●
ホットスタンバイ（付加機能）	同期データ転送	●	●	●	●	●
	RIP 制御（仮想 IP で RIP 送信）	●	●	●	●	●
	ゲートウェイ・フェールセーフ	●	●	●	●	●
ホットスタンバイ（構成）	2 台冗長構成	●	●	●	●	●
LAN 二重化		×	×	×	×	×
リンクアグリゲーション		×	×	×	×	×
UPS アラーム検知	Network インターフェース	×	×	×	×	×
温度監視		×	×	×	×	×
FAN 監視		×	×	×	×	×
CPU ・メモリ使用率表示		●	●	●	●	●
LAN バイパス（ブリッジモード時）		×	×	×	×	×

機能	サポート可否				
	100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
ローリングアップデート（装置冗長化時）	●	●	●	●	●
装置電源冗長化	×	×	×	×	×

● ： 基本機能 ×: 未サポート

1-2-27 ドメインリスト管理

本製品ではサポートしていません。

1-2-28 運用管理/ 保守機能

本機能で、製品ごとに提供する機能は以下のとおりです。

機能			サポート可否				
			100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
構成定義	構成定義複数世代管理		●	●	●	●	●
	環境定義情報の退避・復元		●	●	●	●	●
	インターフェースの動的定義変更（I/F の変更・追加・削除）		●	●	●	●	●
	コマンドラインインターフェース(CLI)		●	●	●	●	●
	Web コンソール		●	●	●	●	●
コンフィグドライブ			×	×	×	×	×
アラーム表示機能	電源障害アラーム		×	×	×	×	×
	FAN ユニットアラーム		×	×	×	×	×
	吸気温度アラーム		×	×	×	×	×
	装置障害アラーム		×	×	×	×	×
保守 LAN(MNT)			×	×	×	×	×
保守インターフェース	Serial		×	×	×	×	×
	VGA(Local Console)		●	●	●	●	●
	Telnet サーバ		●	●	●	●	●
	SSH サーバ		●	●	●	●	●
	SSH クライアント		●	●	●	●	●
	FTP クライアント		●	●	●	●	●
	TFTP クライアント		●	●	●	●	●
	HTTP サーバ機能		●	●	●	●	●
保守形態	local		●	●	●	●	●
	remote		●	●	●	●	●
	パネル		×	×	×	×	×
UPS LAN			×	×	×	×	×
保守機能	IP ホスト機能	ping	●	●	●	●	●

機能			サポート可否				
			100 LS PLUS	220 LS	220 LS PLUS	100 SC	220 SC
		traceroute	●	●	●	●	●
	NTP クライアント		●	●	●	●	●
	NTP サーバ		●	●	●	●	●
	ログ		●	●	●	●	●
	Syslog 送信（クライアント）		●	●	●	●	●
	イベント通知（メール転送）		●	●	●	●	●
	イベント通知（SNMP trap 転送）		●	●	●	●	●
	イベント通知（ログファイル転送）		●	●	●	●	●
	メモリダンプ/ プロセスダンプ		●	●	●	●	●
	ネットワークトレース		●	●	●	●	●
	ファンクショントレース		●	●	●	●	●
	プロトコルイベントトレース		●	●	●	●	●
	リモートメンテナンス対(REMCS)		×	×	×	×	×
	リアルタイム・モニタ		●	●	●	●	●
	簡易ロギングユーティリティ		×	×	×	×	×
	リモート操作ユーティリティ (ipcompass)		×	×	×	×	×
	ログ解析ツール		●	●	●	●	●
SNMP	SNMPv1		●	●	●	●	●
	SNMPv2c		●	●	●	●	●
	SNMPv3		●	●	●	●	●
MIB	MIB MIB-II		●	●	●	●	●
	拡張 MIB		●	●	●	●	●
統計スナップショット			×	×	×	×	×
セーフモード			×	×	×	×	×

● ： 基本機能 ×： 未サポート

第 2 章 IPCOM VE2m ご利用の流れ

本章では、IPCOM VE2m 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 VE2m の使用手順について

IPCOM VE2m 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 VE2m 100 LS PLUS
  - IPCOM VE2m 220 LS
  - IPCOM VE2m 220 LS PLUS
  - IPCOM VE2m 100 SC
  - IPCOM VE2m 220 SC

［注意］

ライセンスキーを入力するまでは IPCOM VE2m 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 VE2m 設定の流れ

本書では、IPCOM VE2m を含むシステムの作成を事例として、IPCOM VE2m 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。

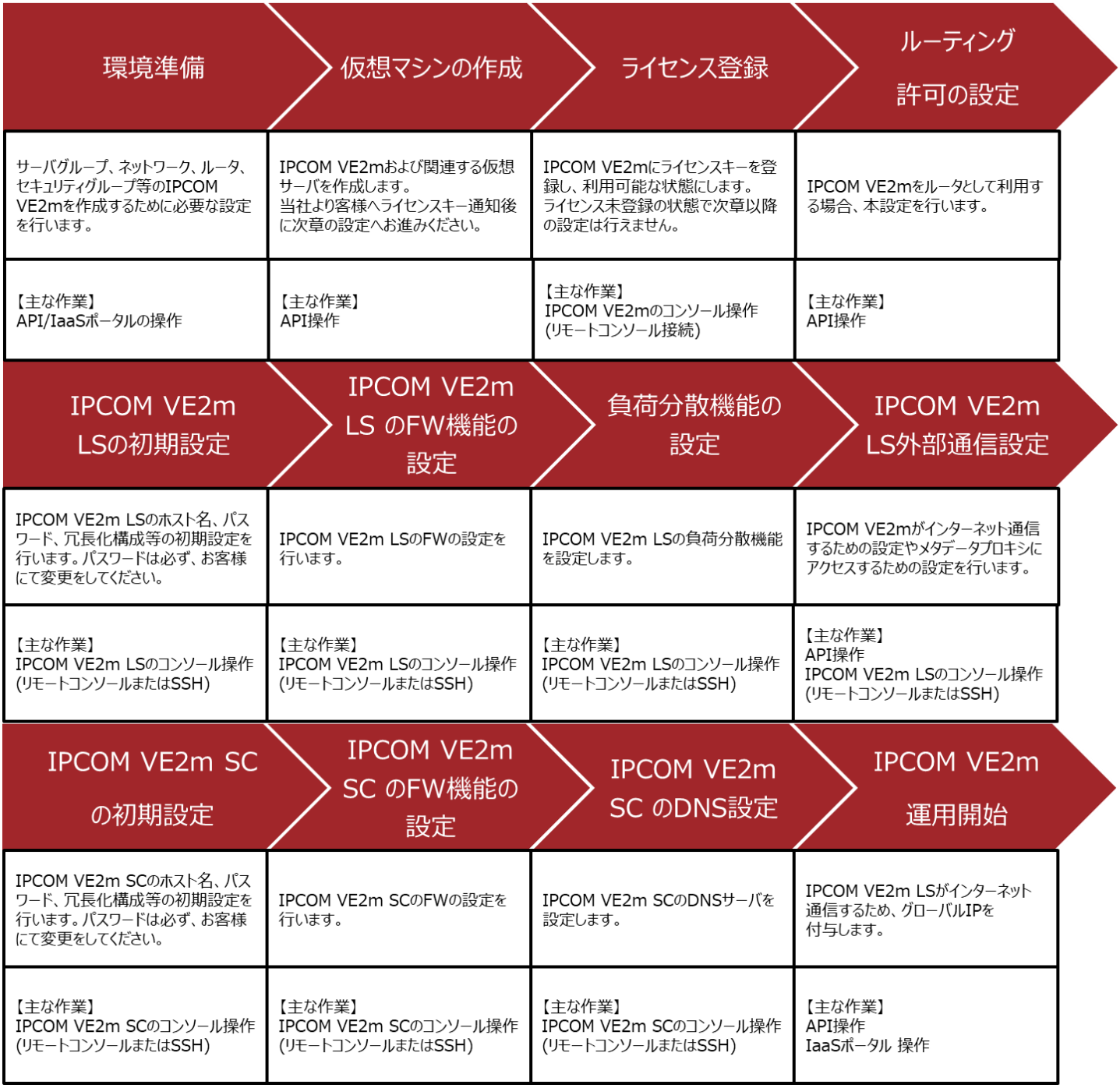


図 2-1：IPCOM VE2m 設定の流れ

IPCOM VE2m 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 VE2m LS)；4/5/6/7/8/9/10/14 章

・シングル構成(IPCOM VE2m 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

項番	留意事項	該当する章番号
1	仮想サーバタイプは IPCOM VE2m 100；S-1 もしくは S2-1/IPCOM 220；C-4 もしくは C2-4 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 VE2m 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 VE2m に割り当てるディスクボリュームは初回 boot 時に/dev/vda に 4GB、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 VE2m 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 VE2m 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 VE2m 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 VE2m 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、admin ユーザーのパスワード設定を必ず実施してください。また、外部接続用の設定はパスワードの設定後に実施してください。	7 章,11 章
6	IPCOM VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m 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、IaaS上での動作をサポートしておりません。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機能および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 EX2 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
13	IPCOM VE2mは、フレーバーの変更に対応していません。	なし

(*1)留意事項 7 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。

BackNetwork 上の仮想サーバがメタデータ通信するために、以下の設定が必要となります。以降の設定に下記の内容が含まれておりますので、必ず設定してください。(図 2-2)

① 仮想ルータと BackNetwork サブネットを接続する

② 仮想ルータにスタティックルーティングを追加する

- destination : BackNetwork の CIDR
- nexthop : IPCOM VE2m LS lan0.0 の IP アドレス

③ 仮想ルータの FW に送信先 IP が BackNetwork のものは全拒否を設定する

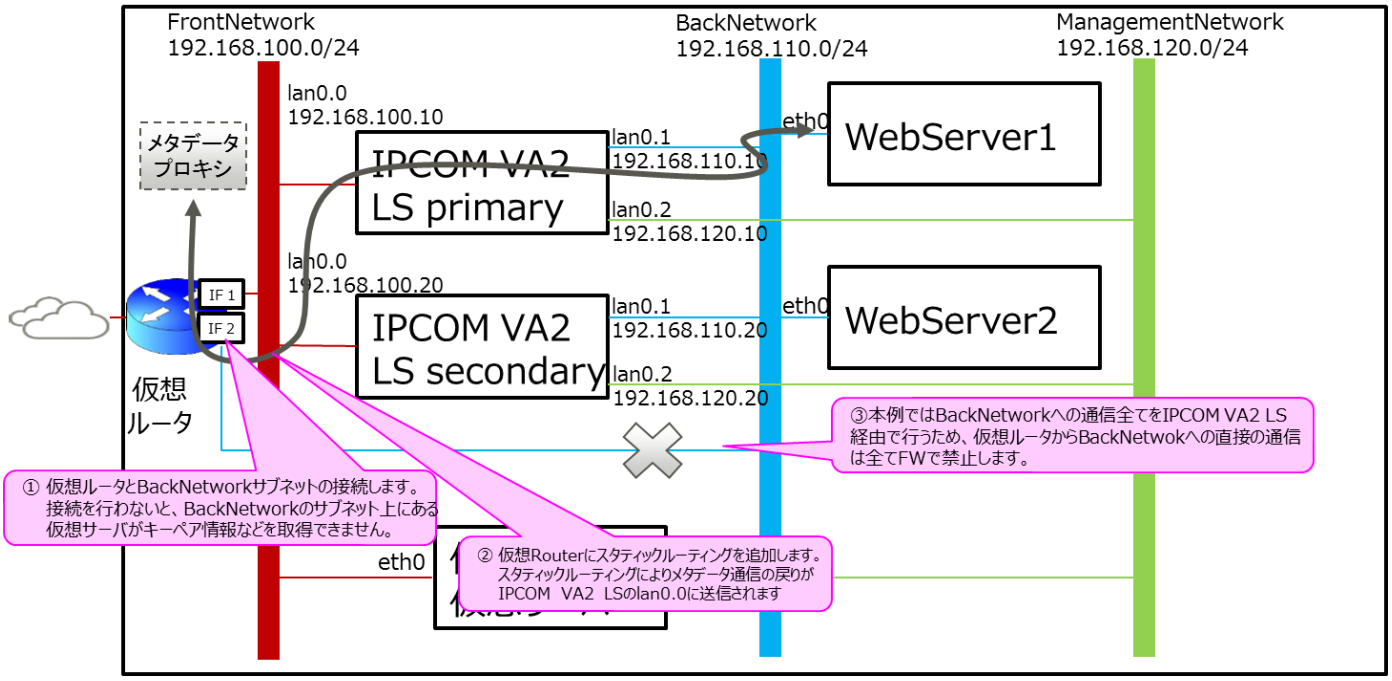


図 2-2：メタデータ通信の設定

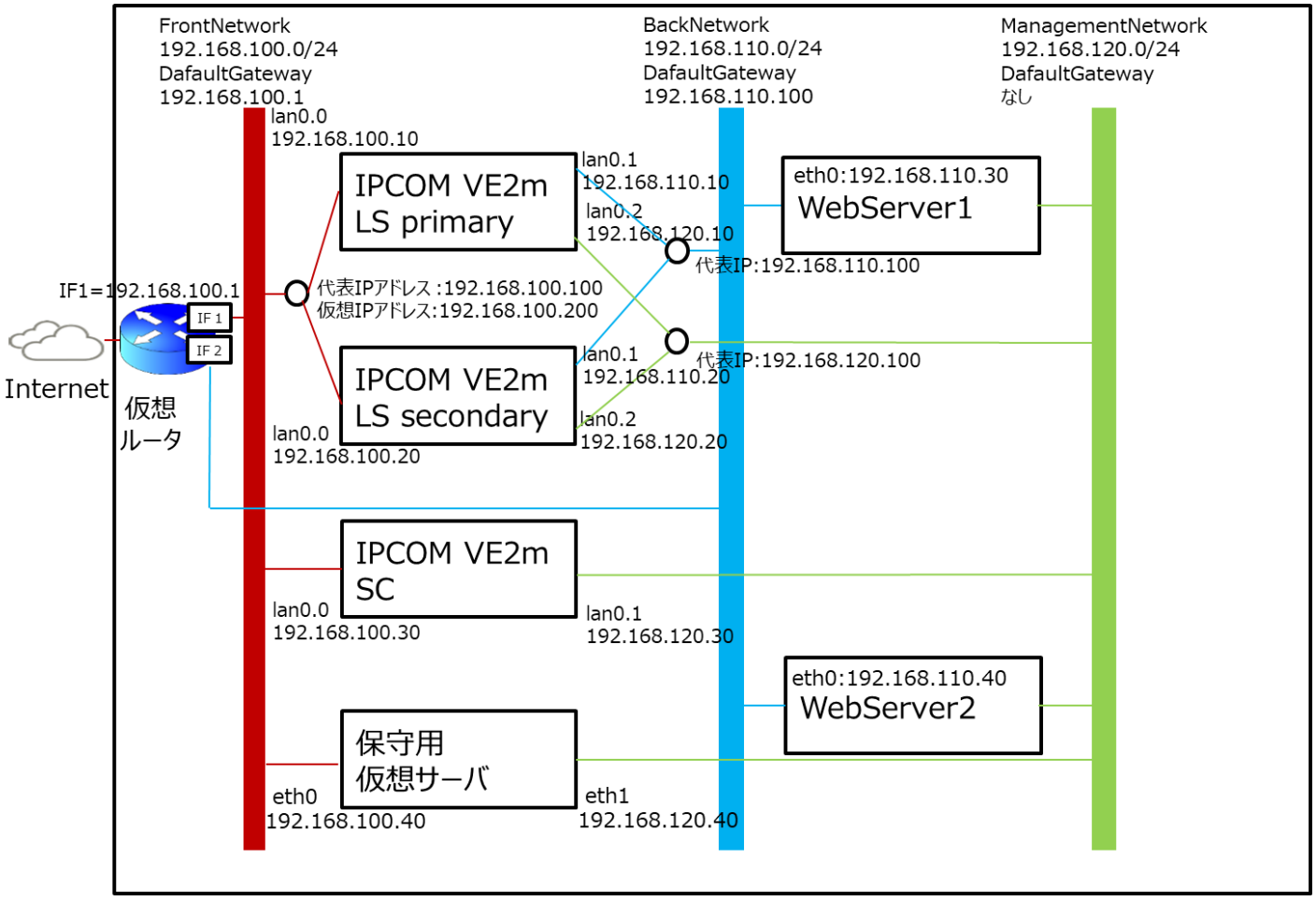
2.4 本書で作成するシステム構成

以降の章では、IaaS 上で IPCOM VE2m 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 EX2 シリーズ事例集ならびに IaaS マニュアルを参照ください。

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 VE2m メンテナンスの用途を想定しております。

※IPCOM VE2m 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 VE2m を含むシステム構成

本章では、IPCOM VE2m 作成前に必要となる環境準備作業について説明します。

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 IaaS ポータルから仮想ネットワーク作成画面まで遷移します。(図 3-1)

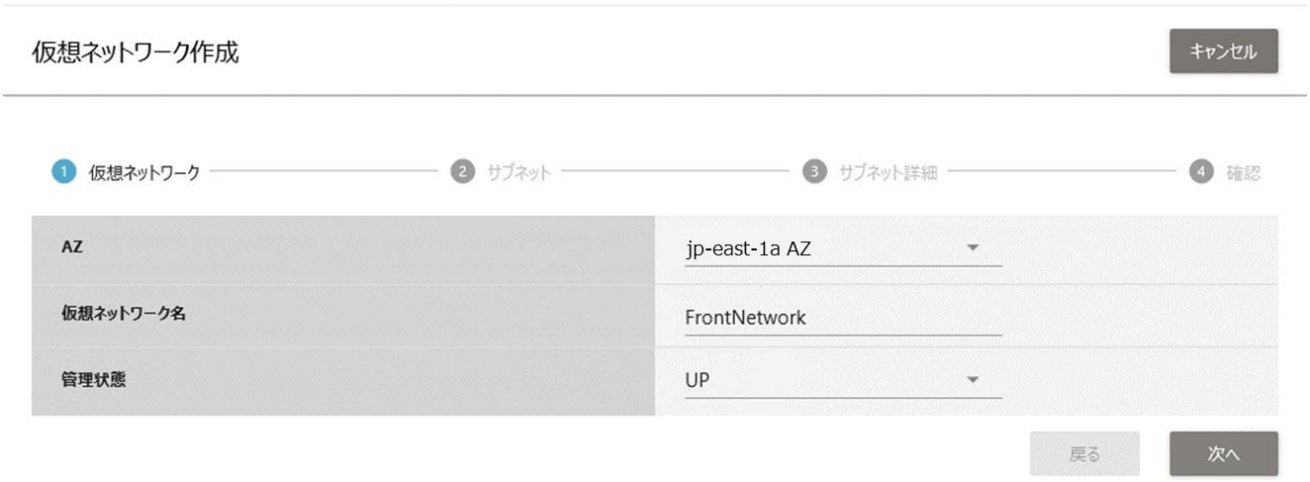


図 3-1：仮想ネットワーク作成画面

② Subnet、Gateway の設定を行います。(図 3-2)

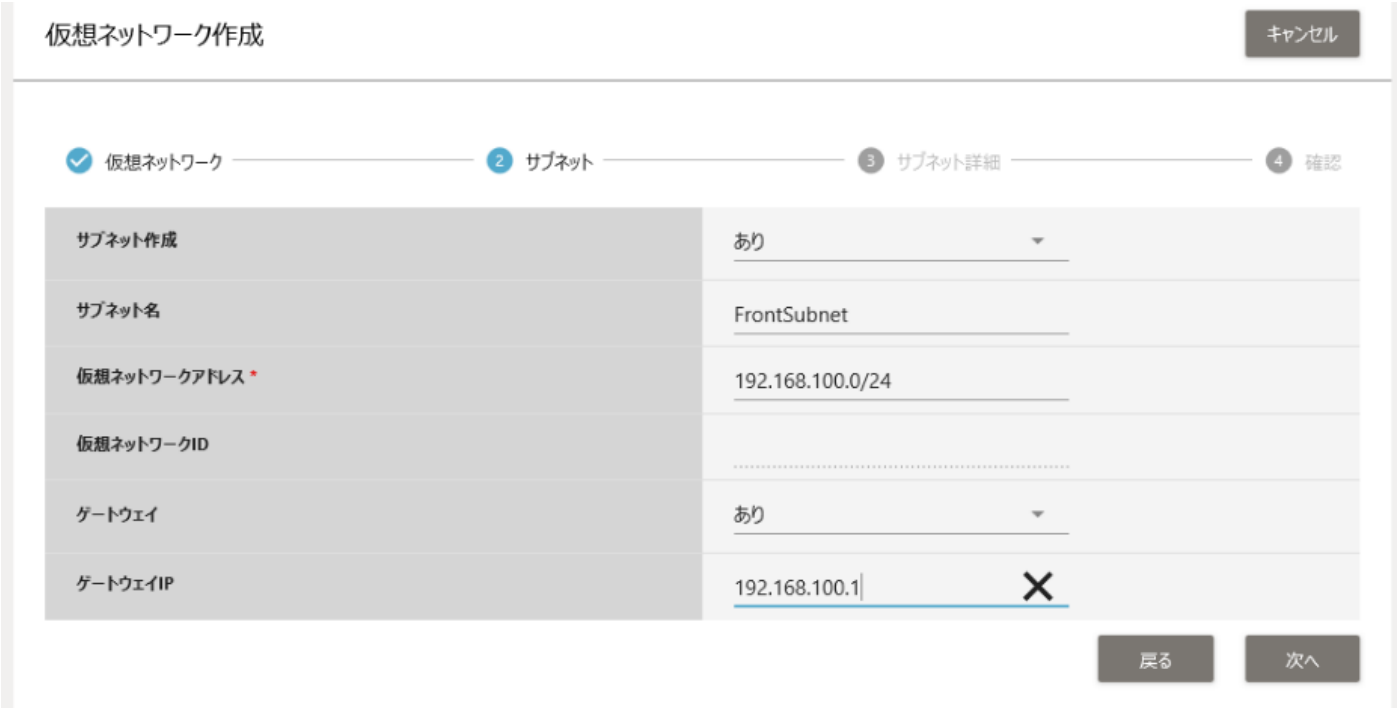


図 3-2：サブネット、ゲートウェイの設定例

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)

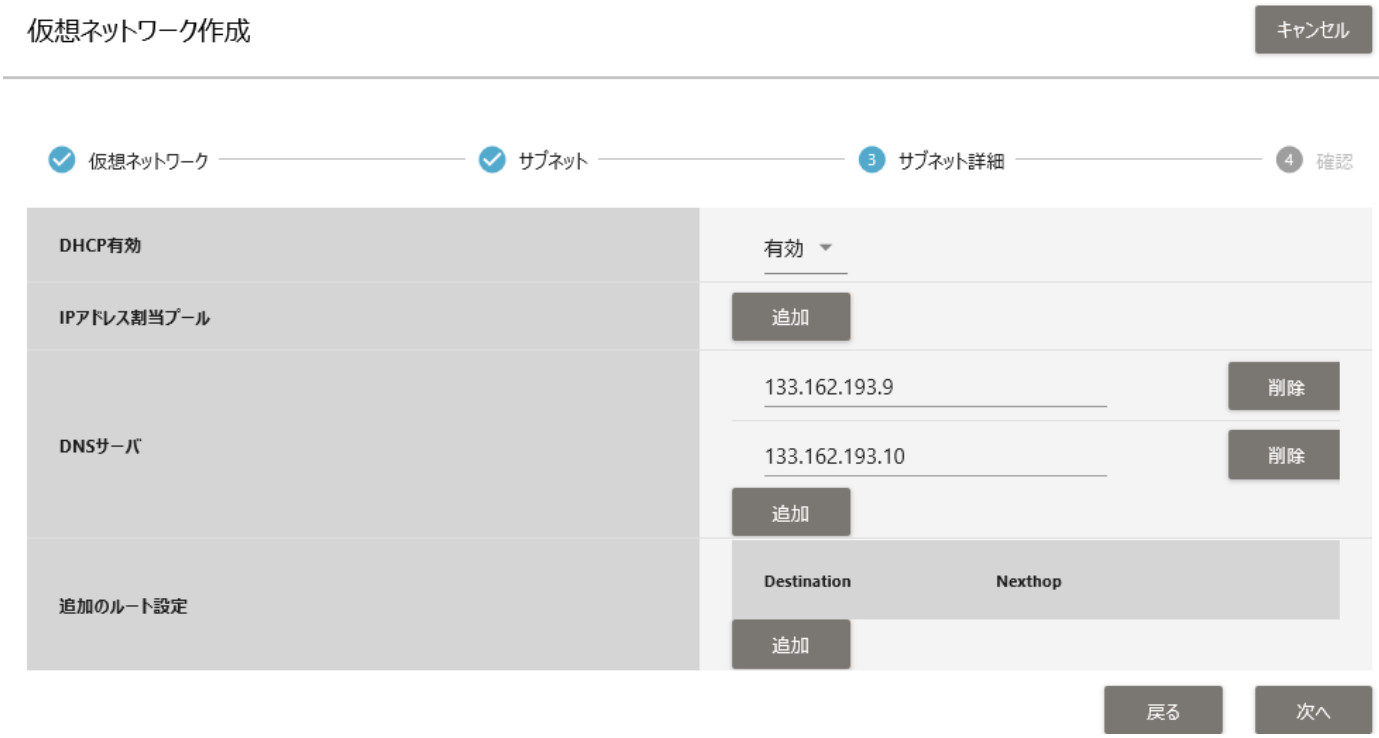


図 3-3：DNS 設定例

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@IaaS-Host ]# ROUTER_NAME=Ext-Router                          ※1
[root@IaaS-Host ]# AZ=jp-east-1a                                   ※2
[root@IaaS-Host ]# curl -Ss $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": "'$TENANT_ID'",
"availability_zone": "'$AZ'"}}' | jq .

※1  名前は任意で指定してください。
※2  作成先の AZ 名を指定してください。
```

実行結果例

```
{
  "router": {
    "status": "ACTIVE",
    "external_gateway_info": null,
    "name": "Ext-Router",
    "admin_state_up": true,
    "tenant_id": "a6a7fe34a4e6447d8487ea8225db64ce4",
    "id": "758dc549-2020-4492-b0ef-994eafca94901",
    "availability_zone": "jp-east-1a"
  }
}
```

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@IaaS-Host ]# PORT_NAME=FrontSubnetRouterPort                 ※1
[root@IaaS-Host ]# NETWORK_ID="FrontNetwork の ID"
[root@IaaS-Host ]# SUBNET_ID="FrontNetwork のサブネット ID"
[root@IaaS-Host ]# FIXED_IP_ADDRESS=192.168.100.1                  ※2
[root@IaaS-Host ]# AZ=jp-east-1a                                   ※3
[root@IaaS-Host ]# curl -Ss $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": "'$PORT_NAME'", "availability_zone":
"'$AZ'", "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）
※3  【任意】作成先の AZ 名を指定してください。
```

実行結果例

```
{
  "port": {
    "status": "DOWN",
```

```
    "name": "FrontSubnetRouterPort",
    "allowed_address_pairs": [],
    "admin_state_up": true,
    "network_id": "0ffaf902-a320-44d7-a9ac-0d3722e71538",
    "tenant_id": "a6a7fe34a4e6447d8487ea8225db64c4",
    "binding:vnic_type": "normal",
    "device_owner": "",
    "mac_address": "fa:16:3e:85:f2:XX",
    "fixed_ips": [
      {
        "subnet_id": "44ad230c-df0c-4cf8-b670-b5abf40a9120",
        "ip_address": "192.168.100.1"
      }
    ],
    "id": "25daf8e8-4340-4aac-bcc9-21c9dcfe7683",
    "security_groups": [
      "a74dbc40-1e75-4f20-a014-133b6c933b17"
    ],
    "device_id": "",
    "availability_zone": "jp-east-1a"
  }
}
```

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@IaaS-Host ~]# ROUTER_ID="作成した仮想ルータの ID"
[root@IaaS-Host ~]# PORT_ID="作成したインターフェース 1 の ID"
[root@IaaS-Host ~]# curl -Ss $NETWORK/v2.0/routers/$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": "44ad230c-df0c-4cf8-b670-b5abf40a9XXX",
  "tenant_id": "a6a7fe34a4e6447d8487ea8225db6XXX",
  "port_id": "25daf8e8-4340-4aac-bcc9-21c9dcfe7XXX",
  "id": "758dc549-2020-4492-b0ef-994eafca9XXX",
  "availability_zone": "jp-east-1a"
}
```

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@IaaS-Host ]# PORT_NAME=BackSubnetRouterPort                    ※1
[root@IaaS-Host ]# NETWORK_ID="BackNetwork の ID"
[root@IaaS-Host ]# SUBNET_ID="BackNetwork のサブネット ID"
[root@IaaS-Host ]# FIXED_IP_ADDRESS=192.168.110.1                    ※2
[root@IaaS-Host ]# AZ=jp-east-1a                                     ※3
```

```
[root@IaaS-Host ]# curl -Ss $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": "'$PORT_NAME'", "availability_zone": "'$AZ'", "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)
※3 【任意】作成先の AZ 名を指定してください。

実行結果例


```
{
  "port": {
    "status": "DOWN",
    "name": "BackSubnetRouterPort",
    "allowed_address_pairs": [],
    "admin_state_up": true,
    "network_id": "58f7f0ed-3b9c-4694-82a1-22326bafad44",
    "tenant_id": "a6a7fe34a4e6447d8487ea8225db64c4",
    "binding:vnic_type": "normal",
    "device_owner": "",
    "mac_address": "fa:16:3e:db:4b:XX",
    "fixed_ips": [
      {
        "subnet_id": "5582755b-8480-4ccf-baac-3c2ddfc74ea7",
        "ip_address": "192.168.110.1"
      }
    ],
    "id": "99472b16-feb6-45a4-9678-376eb160a311",
    "security_groups": [
      "a74dbc40-1e75-4f20-a014-133b6c933b17"
    ],
    "device_id": "",
    "availability_zone": "jp-east-1a"
  }
}
```


図 3-7： BackNetwork 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 3-8)

コマンド例

```
[root@IaaS-Host ~]# ROUTER_ID="仮想ルータの ID"
[root@IaaS-Host ~]# PORT_ID="インターフェース 2 の ID"
[root@IaaS-Host ~]# curl -Ss $NETWORK/v2.0/routers/$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@IaaS-Host ~]# ROUTER_ID="作成した仮想ルータの ID"
[root@IaaS-Host ~]# EXT_NET_ID="グローバル IP ネットワークの ID"              ※1
[root@IaaS-Host ~]# curl -Ss $NETWORK/v2.0/routers/$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'"}}}'

※1　本例では inf_az1_ext-net02 を指定します。
```

実行結果例

```
HTTP/1.1 200 Connection established

HTTP/1.1 200 OK
X-Fcx-Endpoint-Request: EXECUTED_REQ004731206_200
Date: Fri, 14 Apr 2017 14:11:21 GMT
Server: Apache
x-openstack-request-id: req-f69b24b6-3e0d-41fc-a7d0-d5c33ecf78a7
Cache-Control: no-cache
X-Request-Id: 2511c4fa-3e9e-4b25-ba01-c51e39e00124
X-Runtime: 1.491000
Connection: close
Content-Type: application/json;charset=UTF-8
Content-Length: 303

{"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

3.3 キーペアについて

IPCOM VE2m 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 VE2m 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 VE2m 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@IaaS-Host ~]# SG_NAME=ipcom-VE2m-SG                                    ※1
[root@IaaS-Host ~]# curl -Ss $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'"}}'
```

※1 【任意】名前は任意で指定してください。

実行結果例

```
HTTP/1.1 200 Connection established

HTTP/1.1 201 Created
X-Fcx-Endpoint-Request: EXECUTED_REQ010721482_201
Date: Thu, 20 Apr 2017 12:12:05 GMT
Server: Apache
x-openstack-request-id: req-18e2a7fc-6148-40a7-95fd-dd7d59d648d2
Cache-Control: no-cache
X-Request-Id: 81df35d3-58fc-49dd-b6e4-41bb1e58ab4f
X-Runtime: 1.212000
Connection: close
Content-Type: application/json;charset=UTF-8
Content-Length: 822

{"security_group": {"tenant_id": "77b97024974140cf921bb40834a383d0", "description": "", "name": "ipcom-
VE2m-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 VE2m 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 VE2m は内部で FW 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 VE2m 内部で FW 機能を有しているため、セキュリティグループは全て許可します。

■ tcp を全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 -Ss $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 を全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 -Ss $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 を全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 ]# MIN_PORT_NUM=0
[root@K5-HOST ]# MAX_PORT_NUM=255
[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 -Ss $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": "icmp",
  "ethertype": "IPv4",
  "port_range_max": 255,
  "security_group_id": "80b6deee-c4a8-4c33-805c-daf15c11786a",
  "tenant_id": "77b97024974140cf921bb40834a383d0",
  "port_range_min": 0,
  "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 -Ss $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 .

※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 VE2m 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@IaaS-Host ]# NAME=IPCOM_VE2m_ServerGr
[root@IaaS-Host ]# POLICY="anti-affinity"
[root@IaaS-Host ]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ]# curl -Ss $COMPUTE/v2/$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":
[ "'$POLICY'" ], "availability_zone": "'$AZ'"}}' | jq .
```

実行結果例

```
{
  "server_group": {
    "members": [],
    "metadata": {},
    "id": "4a8bd960-688b-474f-83f9-e1ae72bf6cf6",
    "policies": [
      "anti-affinity"
    ],
    "name": "IPCOM_VE2m_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 VE2m 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］

西日本第 1/第 2 リージョン、東日本第 1/第 2 リージョンは、コンフィグドライブに対応していません。コンフィグドライブを指定して IPCOM VE2m 仮想サーバを作成しないでください。
また、セキュリティの観点から、7.1 ホスト名とパスワードの設定(LS primary)にてお客様自身でパスワードを設定するまで、ssh 等でリモートログインできる状態にしないでください。

［注意］

本章および次章の IPCOM VE2m 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 VE2m 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 VE2m の作成(LS primary)

IPCOM VE2m LS の primary を作成します。API で実行してください。(図 4-1)

コマンド例

```
[root@IaaS-Host ~]# VM_NAME=IPCOM_VE2m_LS_primary                              ※1
[root@IaaS-Host ~]# IMAGE_REF_ID="IPCOM VE2m LS の ImageID"
[root@IaaS-Host ~]# FLAVOR_ID=1101                                             ※2
[root@IaaS-Host ~]# VOL_SIZE=4                                                 ※3
[root@IaaS-Host ~]# DEVICE_NAME=/dev/vda                                       ※4
[root@IaaS-Host ~]# SOURCE=image                                               ※5
[root@IaaS-Host ~]# DESTINATION=volume                                         ※6
[root@IaaS-Host ~]# ISDELETE=1                                                 ※7
[root@IaaS-Host ~]# INSTANCE_MAX=1                                             ※8
[root@IaaS-Host ~]# INSTANCE_MIN=1                                             ※9
[root@IaaS-Host ~]# NETWORK_ID1="FrontNetwork の ID"
[root@IaaS-Host ~]# NETWORK_ID2="BackNetwork の ID"
[root@IaaS-Host ~]# NETWORK_ID3="ManagementNetwork の ID"
[root@IaaS-Host ~]# SG_NAME="「SecurityGroup の作成で作成した」グループ名"
[root@IaaS-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@IaaS-Host ~]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ~]# curl -Ss $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "availability_zone": "'$AZ'",
"imageRef": "", "flavorRef": "'$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 は下記を参照ください。
IPCOM VE2m 100 ： 1101(S-1)もしくは 2101(S2-1)いずれかを選択してください。
IPCOM VE2m 220 ： 1303(C-4)もしくは 2303(C2-4)いずれかを選択してください。
※3 【固定】初回起動時のボリュームは 4GB 固定です。
※4 【固定】
※5 【固定】
※6 【固定】
※7 【任意】IPCOM VE2m 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 VE2m の作成(LS primary)

4.2 【LS】IPCOM VE2m の作成(LS secondary)

IPCOM VE2m LS の secondary を作成します。API で実行してください。(図 4-2)

コマンド例

```
[root@IaaS-Host ~]# VM_NAME=IPCOM_VE2m_LS_secondary                              ※1
[root@IaaS-Host ~]# IMAGE_REF_ID="IPCOM VE2m LS の ImageID"
[root@IaaS-Host ~]# FLAVOR_ID=1101                                               ※2
[root@IaaS-Host ~]# VOL_SIZE=4                                                   ※3
[root@IaaS-Host ~]# DEVICE_NAME=/dev/vda                                         ※4
[root@IaaS-Host ~]# SOURCE=image                                                 ※5
[root@IaaS-Host ~]# DESTINATION=volume                                           ※6
[root@IaaS-Host ~]# ISDELETE=1                                                   ※7
[root@IaaS-Host ~]# INSTANCE_MAX=1                                               ※8
[root@IaaS-Host ~]# INSTANCE_MIN=1                                               ※9
[root@IaaS-Host ~]# NETWORK_ID1="FrontNetwork の ID"
[root@IaaS-Host ~]# NETWORK_ID2="BackNetwork の ID"
[root@IaaS-Host ~]# NETWORK_ID3="ManagementNetwork の ID"
[root@IaaS-Host ~]# SG_NAME="「SecurityGroup の作成で作成した」グループ名"
[root@IaaS-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@IaaS-Host ~]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ~]# curl -Ss $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "availability_zone": "'$AZ'",
"imageRef": "", "flavorRef": "'$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、下記を参照ください。
    IPCOM VE2m 100；1101(S-1) もしくは 2101(S2-1)いずれかを選択してください。
    IPCOM VE2m 220；1301(C-4) もしくは 2301(C2-4)いずれかを選択してください。
※3 【固定】初回起動時のボリュームは 4GB 固定です。
※4 【固定】
※5 【固定】
※6 【固定】
※7 【任意】IPCOM VE2m 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 VE2m の作成(LS secondary)

4.3【SC】IPCOM VE2m の作成(SC)

IPCOM VE2m 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@IaaS-Host ~]# VM_NAME=IPCOM_VE2m_SC                                    ※1
[root@IaaS-Host ~]# IMAGE_REF_ID="IPCOM VE2m SC の ImageID"
[root@IaaS-Host ~]# FLAVOR_ID=1101                                           ※2
[root@IaaS-Host ~]# VOL_SIZE=4                                               ※3
[root@IaaS-Host ~]# DEVICE_NAME=/dev/vda                                     ※4
[root@IaaS-Host ~]# SOURCE=image                                             ※5
[root@IaaS-Host ~]# DESTINATION=volume                                       ※6
[root@IaaS-Host ~]# ISDELETE=1                                               ※7
[root@IaaS-Host ~]# INSTANCE_MAX=1                                           ※8
[root@IaaS-Host ~]# INSTANCE_MIN=1                                           ※9
[root@IaaS-Host ~]# NETWORK_ID1="FrontNetwork の ID"
[root@IaaS-Host ~]# NETWORK_ID2="ManagementNetwork の ID"
[root@IaaS-Host ~]# SG_NAME="セキュリティグループ名"
[root@IaaS-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@IaaS-Host ~]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ~]# curl -Ss $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "availability_zone": "'$AZ'",
"imageRef": "", "flavorRef": "'$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、下記を参照ください。
IPCOM VE2m 100；1101(S-1) もしくは 2101(S2-1)いずれかを選択してください。
IPCOM VE2m 220；1301(C-4) もしくは 2301(C2-4)いずれかを選択してください。
※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 VE2m 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 VE2m 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@IaaS-Host ~]# VM_NAME=WebServer1
[root@IaaS-Host ~]# IMAGE_REF_ID="WebServer として利用したい任意の Image の ID"
[root@IaaS-Host ~]# FLAVOR_ID="仮想サーバスペック ID 例 S-1:1101"
[root@IaaS-Host ~]# VOL_SIZE="ボリュームサイズ(GB)"
[root@IaaS-Host ~]# DEVICE_NAME=/dev/vda
[root@IaaS-Host ~]# SOURCE=image
[root@IaaS-Host ~]# DESTINATION=volume
[root@IaaS-Host ~]# ISDELETE=1
[root@IaaS-Host ~]# KEYNAME="キー名"
[root@IaaS-Host ~]# INSTANCE_MAX=1
[root@IaaS-Host ~]# INSTANCE_MIN=1
[root@IaaS-Host ~]# NETWORK_ID1="BackNetwork の ID"                    ※1
[root@IaaS-Host ~]# NETWORK_ID2="ManagementNetwork の ID"              ※2
[root@IaaS-Host ~]# SG_NAME="セキュリティグループ名"
[root@IaaS-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@IaaS-Host ~]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ~]# curl -Ss $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "availability_zone": "'$AZ'",
"imageRef": "", "flavorRef": "'$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。
```

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@IaaS-Host ~]# VM_NAME=MngVM
[root@IaaS-Host ~]# IMAGE_REF_ID="イメージ ID"
[root@IaaS-Host ~]# FLAVOR_ID="仮想サーバスペック ID"
[root@IaaS-Host ~]# VOL_SIZE="ボリュームサイズ(GB) "
[root@IaaS-Host ~]# DEVICE_NAME=/dev/vda
[root@IaaS-Host ~]# SOURCE=image
[root@IaaS-Host ~]# DESTINATION=volume
[root@IaaS-Host ~]# ISDELETE=1
[root@IaaS-Host ~]# KEYNAME="キーペアのキー名"
[root@IaaS-Host ~]# INSTANCE_MAX=1
[root@IaaS-Host ~]# INSTANCE_MIN=1
[root@IaaS-Host ~]# NETWORK_ID1="FrontNetwork の ID"                    ※1
[root@IaaS-Host ~]# NETWORK_ID2="ManagementNetwork の ID"               ※2
[root@IaaS-Host ~]# SG_NAME="セキュリティグループ名"
[root@IaaS-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@IaaS-Host ~]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ~]# curl -Ss $COMPUTE/v2/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "availability_zone": "'$AZ'",
"imageRef": "", "flavorRef": "'$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。
```

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 VE2m 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 VE2m LS にリモートコンソールログイン

IPCOM VE2m 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]

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、ssh 等でリモートログインできる状態にしないでください。

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)

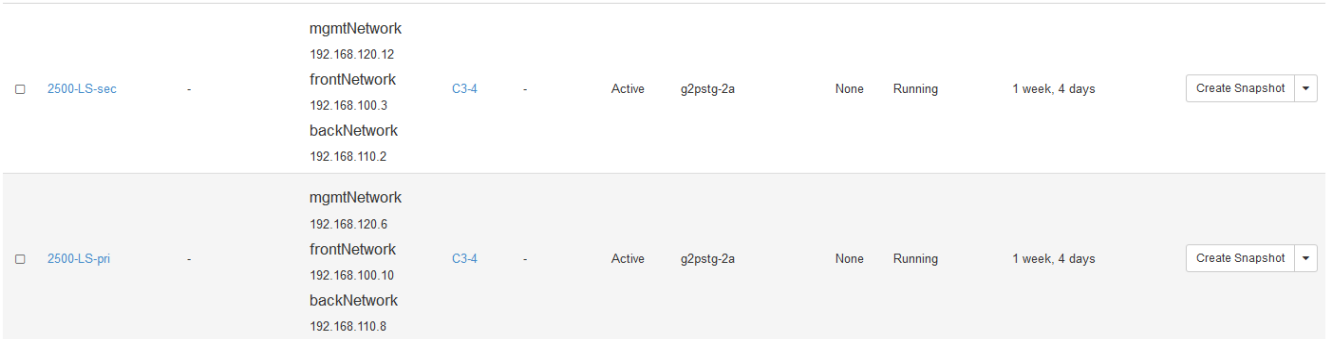


図 5-1：リモートコンソールへログイン

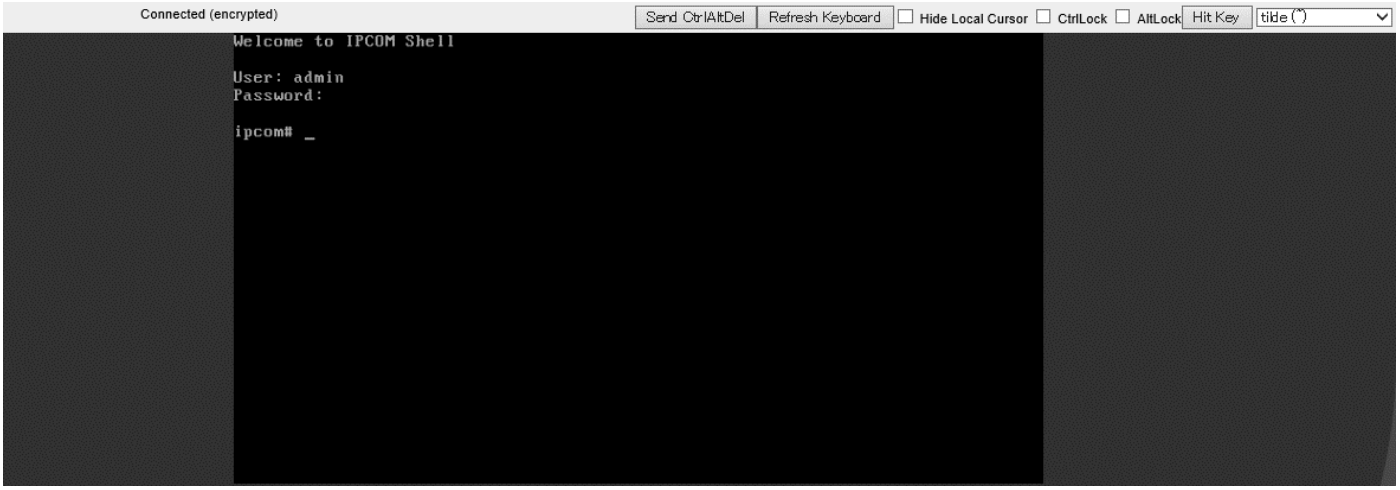


図 5-2：リモートコンソールへログイン後の画面

5.2【LS】IPCOM VE2m LS のライセンスキー登録

IPCOM VE2m 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> The license "VE2-220 LS Software License" is registered. After registering the license, the system will shutdown to activation. Are you sure?(y|[n]):y　※1 Please select either reset or power off.(r|p): p　※2 Broadcast message from root (Tue Feb 11 05:52:52 2020): The system is going down for system halt NOW! <INFO> Wait for a moment until powering off this system. ※1 ライセンスキー登録後、システムのシャットダウンが必要なため、「y」を選択してください。 ※2 パワーオフ「p」を選択してください。 ※本操作は Primary、Secondary それぞれ実施してください。

図 5-3：IPCOM VE2m 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 VE2m 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 VE2m 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：M1
- 容量：100GB(固定)
- ストレージソース：空のボリューム
- AZ：IPCOM VE2m が所属する AZ

※その他の値については任意です

コマンド例

```
[root@IaaS-Host ]# NAME=ipcom_VE2m_LS_pri_vol                                    ※1
[root@IaaS-Host ]# SIZE=100                                                      ※2
[root@IaaS-Host ]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ]# curl -Ss $BLOCKSTORAGE/v2/$PROJECT_ID/volumes -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN"
-H "Content-Type: application/json" -d '{"volume":{"name": "'$NAME'", "size": "'$SIZE'",
"availability_zone": "'$AZ'"}}' | 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": "M1",
    "name": "ipcom_VE2m_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 VE2m LS の primary にアタッチしてください。(図 5-5)

コマンド例

```
[root@IaaS-Host ]# DEVICE=/dev/vdb
[root@IaaS-Host ]# SERVER_ID="IPCOM VE2m LS primary のサーバ ID"
[root@IaaS-Host ]# VOLUME_ID="①で作成したボリュームの ID"
[root@IaaS-Host ]# curl -Ss $COMPUTE/v2/$TENANT_ID/servers/$SERVER_ID/os-volume_attachments -X POST -H "X-
Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"volumeAttachment": {"server_id":
"'$SERVER_ID'","volumeId": "'$VOLUME_ID'","tenant_id": "'$TENANT_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(secondary)

primary 側と同様に、secondary 側 IPCOM VE2m 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：M1
- 容量：100GB(固定)
- ストレージソース：空のボリューム
- AZ：IPCOM VE2m が所属する AZ

※その他の値については任意です

コマンド例

```
[root@IaaS-Host ]# NAME=ipcom_VE2m_LS_sco_vol                                    ※1
[root@IaaS-Host ]# SIZE=100                                                      ※2
[root@IaaS-Host ]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ]# curl -Ss $BLOCKSTORAGE/v2/$PROJECT_ID/volumes -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN"
-H "Content-Type: application/json" -d '{"volume":{"name": "'$NAME'", "size": "'$SIZE'",
"availability_zone": "'$AZ'"}}' | 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": "M1",
    "name": "ipcom_VE2m_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 VE2m の secondary にアタッチしてください。(図 5-7)

コマンド例

```
[root@IaaS-Host ~]# DEVICE=/dev/vdb
[root@IaaS-Host ~]# SERVER_ID="IPCOM VE2m LS secondary のサーバ ID"
[root@IaaS-Host ~]# VOLUME_ID="①で作成したボリュームの ID"
[root@IaaS-Host ~]# curl -Ss $COMPUTE/v2/$TENANT_ID/servers/$SERVER_ID/os-volume_attachments -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"volumeAttachment": {"server_id": "'$SERVER_ID'","volumeId": "'$VOLUME_ID'","tenant_id": "'$TENANT_ID'","device": "'$DEVICE'"}}' | jq .
```

実行結果例

```
{
  "volumeAttachment": {
    "device": "/dev/vdb",
    "serverId": "28c8d1c1-7866-466b-acf6-b5d69e8b0317",
    "id": "ff82504e-30fc-41dc-b6ee-66556db66318",
    "volumeId": "ff82504e-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 VE2m LS の起動

停止している IPCOM VE2m LS を起動します。(図 5-8)

IPCOM VE2m 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。

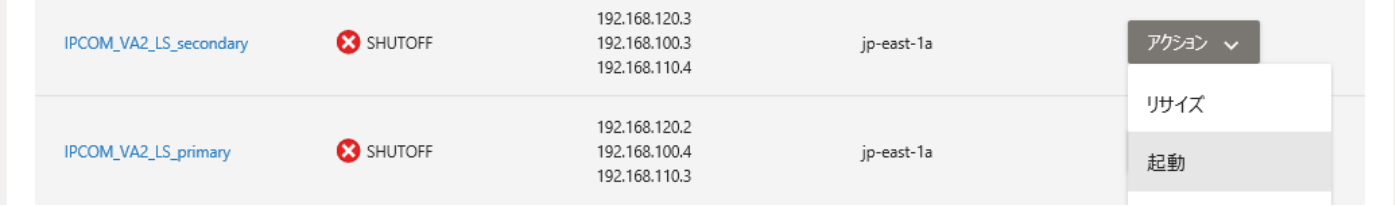


図 5-8：IPCOM VE2m の起動

ここからは IPCOM VE2m SC に対してライセンス登録を行います。

5.6 【SC】IPCOM VE2m SC にリモートコンソールログイン

IPCOM VE2m 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]

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、ssh 等でリモートログインできる状態にしないでください。

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)

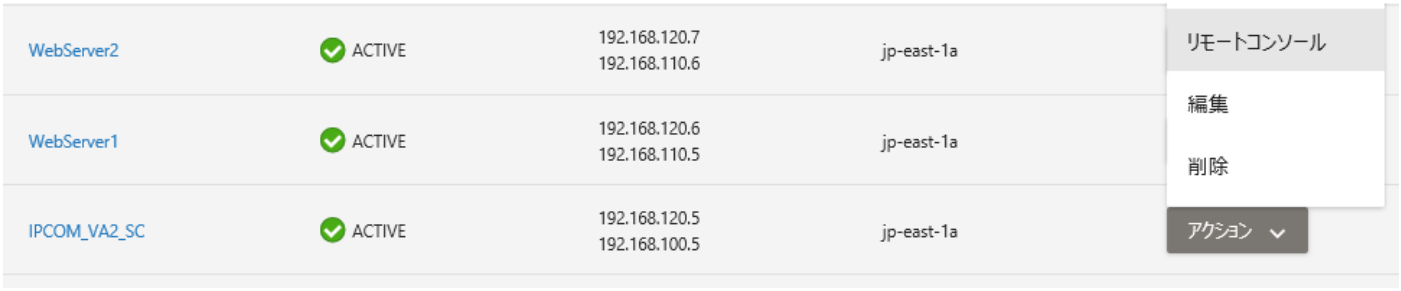


図 5-9：リモートコンソールでログイン

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 VE2m SC のライセンスキー登録

IPCOM VE2m 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> The license "VE2-220 SC Software License" is registered. After registering the license, the system will shutdown to activation. Are you sure?(y|[n]):y　※1 Please select either reset or power off.(r|p): p　※2 Broadcast message from root (Tue Feb 11 05:52:52 2020): The system is going down for system halt NOW! <INFO> Wait for a moment until powering off this system. ※1 ライセンスキー登録後、システムのシャットダウンが必要なため、「y」を選択してください。 ※2 パワーオフ「p」を選択してください。

図 5-11：IPCOM VE2m 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 VE2m 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 VE2m 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 VE2m 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：M1
- 容量：100GB(固定)
- ストレージソース：空のボリューム
- AZ：IPCOM VE2m が所属する AZ

※その他の値については任意です

コマンド例

```
[root@IaaS-Host ]# NAME=ipcom_VE2m_LS_SC_vol                                    ※1
[root@IaaS-Host ]# SIZE=100                                                     ※2
[root@IaaS-Host ]# AZ="作成先の AZ 名 例：jp-east-1a"
[root@IaaS-Host ]# curl -Ss $BLOCKSTORAGE/v2/$PROJECT_ID/volumes -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN"
-H "Content-Type: application/json" -d '{"volume":{"name": "'$NAME'", "size": "'$SIZE'",
"availability_zone": "'$AZ'"}}' | 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": "M1",
    "name": "ipcom_VE2m_LS_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 VE2m SC にアタッチしてください。(図 5-13)

コマンド例

```
[root@IaaS-Host ]# DEVICE=/dev/vdb
[root@IaaS-Host ]# SERVER_ID="IPCOM VE2m SC のサーバ ID"
[root@IaaS-Host ]# VOLUME_ID="①で作成したボリュームの ID"
[root@IaaS-Host ]# curl -Ss -X POST $COMPUTE/v2/$TENANT_ID/servers/$SERVER_ID/os-volume_attachments -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"volumeAttachment": {"server_id": "'$SERVER_ID'","volumeId": "'$VOLUME_ID'","tenant_id": "'$TENANT_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 VE2m SC の起動

停止している IPCOM VE2m 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。

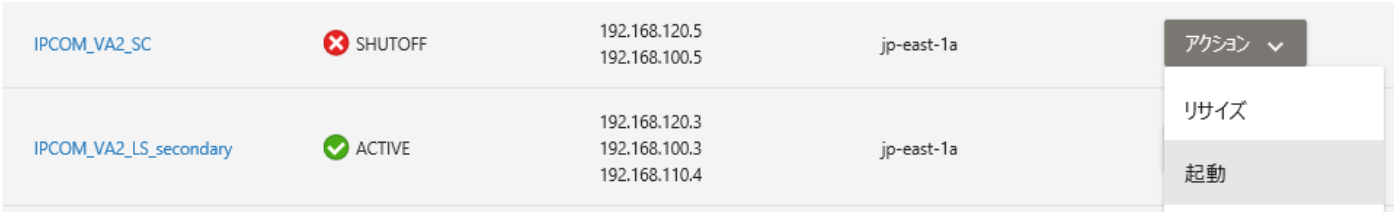


図 5-14：IPCOM VE2m SC の起動

第 6 章 【LS】ルーティング許可の設定

本章では、IPCOM VE2m 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 VE2m 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 VE2m のポート全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 VE2m 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。

(1) LS primary への設定(図 6-1)

コマンド例

```
[root@IaaS-Host ]# PORT_ID="FrontNetwork のポート ID"
[root@IaaS-Host ]# curl -Ss $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address":
"0.0.0.0/1"},{"ip_address": "128.0.0.0/1"}]}}' | jq .

[root@IaaS-Host ]# PORT_ID="BackNetwork のポート ID"
[root@IaaS-Host ]# curl -Ss $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address":
"0.0.0.0/1"},{"ip_address": "128.0.0.0/1"}]}}' | jq .

[root@IaaS-Host ]# PORT_ID="ManagementNetwork のポート ID"
[root@IaaS-Host ]# curl -Ss $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address":
"0.0.0.0/1"},{"ip_address": "128.0.0.0/1"}]}}' | jq .
```

図 6-1：IPCOM VE2m 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@IaaS-Host ]# PORT_ID="FrontNetwork のポート ID"
[root@IaaS-Host ]# curl -Ss $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address":
"0.0.0.0/1"},{"ip_address": "128.0.0.0/1"}]}}' | jq .

[root@IaaS-Host ]# PORT_ID="BackNetwork のポート ID"
[root@IaaS-Host ]# curl -Ss $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address":
"0.0.0.0/1"},{"ip_address": "128.0.0.0/1"}]}}' | jq .

[root@IaaS-Host ]# PORT_ID="ManagementNetwork のポート ID"
[root@IaaS-Host ]# curl -Ss $NETWORK/v2.0/ports/$PORT_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"port":{"allowed_address_pairs": [{"ip_address":
"0.0.0.0/1"},{"ip_address": "128.0.0.0/1"}]}}' | jq .
```

図 6-2：IPCOM VE2m LS secondary へのルーティング許可の設定

第 7 章 【LS】IPCOM VE2m LS の初期設定

本章では、IPCOM VE2m 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 VE2m 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]

セキュリティレベル向上のため、admin ユーザーのパスワード設定(下図※1)を必ず実施してください。また、外部接続用の設定はパスワードの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 VE2m 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 VE2m 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-VE2m-front-net                    ※7
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 10                                     ※8
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                   ※9
vipcom-pri(edit-if)# ip address secondary 192.168.110.20                 ※10
vipcom-pri(edit-if)# description IPCOM-VE2m-back-net                     ※11
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 20                                     ※12
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           ※13
vipcom-pri(edit-if)# ip address primary 192.168.120.10                   ※14
vipcom-pri(edit-if)# ip address secondary 192.168.120.20                 ※15
vipcom-pri(edit-if)# description IPCOM-VE2m-management-net               ※16
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 30                                     ※17
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# ip route 0.0.0.0/0 192.168.100.1 distance 2            ※18
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 IaaS 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 IaaS 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 IaaS 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 lan0.0 の vrid は primary、secondary で同じ値を設定してください。
※9 IaaS 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
※10 IaaS 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

※11 説明文のため任意です
※12 lan0.1 の vrid は primary、secondary で同じ値を設定してください。
※13 代表 IP アドレスを設定
※14 IaaS 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
※15 IaaS 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
※16 説明文のため任意です
※17 lan0.2 の vrid は primary、secondary で同じ値を設定してください。
※18 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 VE2m 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。
※3 hostname "primary のホスト名" "secondary のホスト名"
※4 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 VE2m 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-VE2m-front-net                    ※7
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 10                                     ※8
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                   ※9
vipcom-pri(edit-if)# ip address secondary 192.168.110.20                 ※10
vipcom-pri(edit-if)# description IPCOM-VE2m-back-net                     ※11
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 20                                     ※12
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           ※13
vipcom-pri(edit-if)# ip address primary 192.168.120.10                   ※14
vipcom-pri(edit-if)# ip address secondary 192.168.120.20                 ※15
vipcom-pri(edit-if)# description IPCOM-VE2m-management-net               ※16
vipcom-pri(edit-if)# ip-routing
vipcom-pri(edit-if)# cluster sync-interface
vipcom-pri(edit-if)# cluster vrid 30                                     ※17
vipcom-pri(edit-if)# exit
vipcom-pri(edit)# ip route 0.0.0.0/0 192.168.100.1 distance 2            ※18
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 IaaS 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 IaaS 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 IaaS 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 lan0.0 の vrid は primary、secondary で同じ値を設定してください。
※9 IaaS 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
※10 IaaS 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
※11 説明文のため任意です。
※12 lan0.1 の vrid は primary、secondary で同じ値を設定してください。
※13 代表 IP アドレスを設定

※14 IaaS 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
※15 IaaS 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
※16 説明文のため任意です
※17 lan0.2 の vrid は primary、secondary で同じ値を設定してください。
※18 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 VE2m の冗長化設定が正しく設定できているか確認します。

IPCOM VE2m 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 VE2m LS の FW 機能の設定

本章では、IPCOM VE2m LS における FW の設定手順を説明します。

8.1 FW の設定

FW を設定するため、primary 側 IPCOM VE2m 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 VE2m で FW 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全て破棄します。
※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 VE2m 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：FW ルール作成

② 作成した FW 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 web 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  アウトバウンドは全て許可
```

図 8-2：FW ルールをインターフェースに適用

8.2 FW 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：FW の設定を secondary に同期

第 9 章 【LS】負荷分散機能の設定

本章では、IPCOM VE2m 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 VE2m LS で負荷分散ルールを作成します。

secondary 側 IPCOM VE2m 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 VE2m で以下を実施してください。(図 9-1)

コマンド例

```
vipcom-pri# config
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 VE2m 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。
※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 VE2m 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 200ipcom-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。
※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 VE2m LS の外部通信設定

本章では、IPCOM VE2m 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)# class-map match-all get-metadata                               ※4
vipcom-pri(edit-cmap)# match source-address ip 192.168.110.0/24                  ※5
vipcom-pri(edit-cmap)# match destination-address ip 169.254.169.254              ※6
vipcom-pri(edit-cmap)# 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 ※7
vipcom-pri(edit-if)# rule no-src-nat get-metadata                                ※8
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                                    ※9
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 メタデータ取得の際必須となる設定です。
※5 BackNetwork の NW アドレスを指定します。
※6 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。
※7 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。
※8 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。
※9 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 VE2m LS の各代表 IP に対応するダミーポートを作成

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@IaaS-Host ]# PORT_NAME=FrontShareIP
[root@IaaS-Host ]# NETWORK_ID="FrontNetwork の ID"
[root@IaaS-Host ]# SUBNET_ID="FrontNetwork のサブネット ID"
[root@IaaS-Host ]# FIXED_IP_ADDRESS=192.168.100.100                    ※1
[root@IaaS-Host ]# SG_ID="「SecurityGroup の作成」で作成した SecuriryGroup"
[root@IaaS-Host ]# AZ="IPCOM VE2m が配備されている AZ"
[root@IaaS-Host ]# curl -Ss $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": "'$PORT_NAME'", "availability_zone":
"'$AZ'", "fixed_ips": [{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}],
"security_groups": ["'$SG_ID'"]}}' | jq .
[root@IaaS-Host ]# PORT_NAME=BackShareIP
[root@IaaS-Host ]# NETWORK_ID="BackNetwork の ID"
[root@IaaS-Host ]# SUBNET_ID="BackNetwork のサブネット ID"
[root@IaaS-Host ]# FIXED_IP_ADDRESS=192.168.110.100                    ※2
[root@IaaS-Host ]# SG_ID="「SecurityGroup の作成」で作成した SecuriryGroup"
[root@IaaS-Host ]# AZ="IPCOM VE2m が配備されている AZ"
[root@IaaS-Host ]# curl -Ss $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": "'$PORT_NAME'", "availability_zone":
"'$AZ'", "fixed_ips": [{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}],
"security_groups": ["'$SG_ID'"]}}' | jq .
[root@IaaS-Host ]# PORT_NAME=ManagementShareIP
[root@IaaS-Host ]# NETWORK_ID="managementNetwork の ID"
[root@IaaS-Host ]# SUBNET_ID="ManagementNetwork のサブネット ID"
[root@IaaS-Host ]# FIXED_IP_ADDRESS=192.168.120.100                    ※3
[root@IaaS-Host ]# SG_ID="「SecurityGroup の作成」で作成した SecuriryGroup"
[root@IaaS-Host ]# AZ="IPCOM VE2m が配備されている AZ"
[root@IaaS-Host ]# curl -Ss $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": "'$PORT_NAME'", "availability_zone":
"'$AZ'", "fixed_ips": [{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}],
"security_groups": ["'$SG_ID'"]}}' | jq .

※1  FrontNetwork 側の IPCOM VE2m の代表 IP アドレス
※2  BackNetwork 側の IPCOM VE2m の代表 IP アドレス
※3  FrontNetwork 側の IPCOM VE2m の代表 IP アドレス
```

図 10-2：IPCOM VE2m LS の各代表 IP に対応するダミーポートを作成

10.3 メタデータ通信用の設定

メタデータ(仮想サーバの初期設定用データ)を BackNetwork に所属する仮想サーバが取得できるように設定を行います。

本設定を行わない場合、仮想サーバに対するキーペア情報の登録やホスト名情報の取得ができないため、必ず本設定を実施してください。

仮想ルータにスタティックルーティングを追加します。以下の設定を行う場合の実行例を示します。(図 10-3)
スタティックルーティングの設定は、BackNetwork が属するネットワークの CIDR を以下のように 2 回に分けて設定してください。

【実行例】

- 1 つ目の destnation：192.168.110.0/25　※メタデータを取得する仮想サーバが所属するサブネット
  (本設定例では BackNetwork の CIDR の前半)
- 1 つ目の nexthop　：192.168.100.100　※IPCOM VE2m LS の FrontNetwork 側の代表 IP アドレス

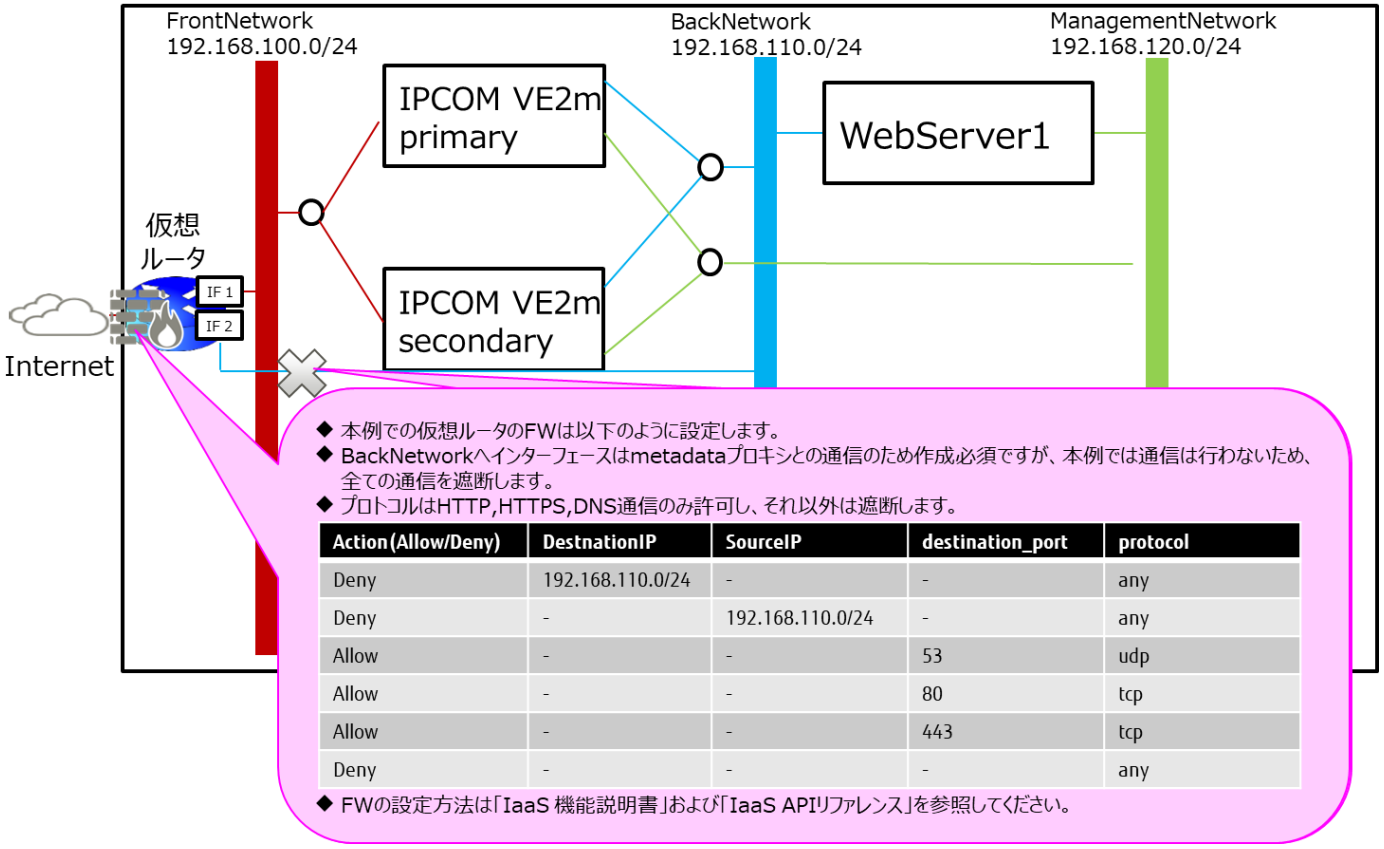
- 2 つ目の destnation：192.168.110.128/25 ※メタデータを取得する仮想サーバが所属するサブネット
  (本設定例では BackNetwork の CIDR の後半)
- 2 つ目の nexthop　：192.168.100.100　※IPCOM VE2m LS の FrontNetwork 側の代表 IP アドレス

コマンド例
ROUTER_ID=6f642eb8-20d5-412c-9973-c53246b85bc6 ROUTES=[{¥"nexthop¥":¥"192.168.100.100¥",¥"destination¥":¥"192.168.110.0/25¥"},{¥"nexthop¥":¥"192.168.100.100¥",¥"destination¥":¥"192.168.110.128/25¥"}] $ curl -Ss $NETWORK/v2.0/routers/$ROUTER_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"router": { "routes": ['$ROUTES'] }}'
実行結果例
{"router":{"status":"ACTIVE","external_gateway_info":null,"name":"endrouter","admin_state_up":true,"tenant_id":"384c0ee7848f442f998b42fa839486f5","routes":[{"nexthop":"192.168.100.100","destination":"192.168.110.0/25"},{"nexthop":"192.168.100.100","destination":"192.168.110.128/25"}],"id":"6f642eb8-20d5-412c-9973-c53246b85bc6","availability_zone":"jp-east-1a"}}

図 10-3：メタデータ通信用の設定

10.4 仮想ルータの FW ルールの設定

本設定例では、仮想ルータの FW ルールは図 10-4 に示したとおり設定してください。



◆ 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
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 10-4：IaaS 上の仮想ルータの FW ルール設定例

10.5 WebServer のデフォルトゲートウェイ設定

BackNetwork のサブネットのルーティング情報を変更し、デフォルトゲートウェイを IPCOM VE2m LS に変更します。(図 10-5)

コマンド例

```
[root@IaaS-Host ]# SUBNET_ID="BackNetwork のサブネット ID"
[root@IaaS-Host ]# HOST_ROUTES={¥"nexthop¥":¥"192.168.110.100(IPCOM VE2m の BackNetwork 側代表
IP)¥",¥"destination¥":¥"0.0.0.0/0¥"}
[root@IaaS-Host ]# curl -Ss $NETWORK/v2.0/subnets/$SUBNET_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"subnet": { "host_routes": ['$HOST_ROUTES'] }}'
HTTP/1.1 200 Connection established

HTTP/1.1 200 OK
X-Fcx-Endpoint-Request: EXECUTED_REQ000104230_200
Date: Mon, 27 Feb 2017 04:27:16 GMT
Server: Apache
x-openstack-request-id: req-8bc1ffa3-f617-4143-bdb8-b34dae741354
Cache-Control: no-cache
X-Request-Id: 90a0480d-e7e5-4bd7-8632-e4b405387e5b
X-Runtime: 0.352000
Connection: close
Content-Type: application/json;charset=UTF-8
Content-Length: 496

{"subnet":{"name":"BackBackNetwork","enable_dhcp":true,"network_id":"702ae944-a86c-4de7-b966-
d4275c052bba","tenant_id":"a6a7fe34a4e6447d8487ea8225db64c4","dns_nameservers":[],"allocation_pools":[{"sta
rt":"192.168.110.2","end":"192.168.110.254"}],"host_routes":[{"nexthop":"192.168.110.100","destination":"0.
0.0.0/0"}],"ip_version":4,"gateway_ip":"192.168.110.1","cidr":"192.168.110.0/24","id":"0a055929-5176-4e2a-
9903-29c89d1c812c","availability_zone":"jp-east-1a"}}
```

図 10-5：WebServer のデフォルトゲートウェイ設定

第 11 章 【SC】IPCOM VE2m SC の初期設定

本章では、IPCOM VE2m 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 VE2m 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 VE2m 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-VE2m-SC-front-net                 ※3
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             ※4
vipcom-sc(edit-if)# description IPCOM-VE2m-SC-management-net            ※5
vipcom-sc(edit-if)# exit
vipcom-sc(edit)# ip route 0.0.0.0/0 192.168.100.1 distance 2             ※6
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 IaaS 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 IaaS 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 IaaS で割当された ManagementNetwork 側の IP アドレスを指定してください
※5 説明文のため任意です。
※6 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 VE2m SC のＦW機能の設定

本章では、IPCOM VE2m SC における FW の設定手順を説明します。

12.1 IPCOM VE2m SC FW の設定

FW を設定するため、IPCOM VE2m 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 VE2m SC で FW 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全て破棄します。
※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 VE2m 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 VE2m SC FW ルールの作成

② 作成した FW 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 アウトバウンドは全て許可
```

図 12-2：IPCOM VE2m SC FW ルールをインターフェースに適用

第 13 章 【SC】IPCOM VE2m SC の DNS 機能の設定

本章では、IPCOM VE2m 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 VE2m SC で DNS ゾーンとレコードの設定を行います。本例では「ipcom-ve2m.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-VE2m.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-VE2m.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-VE2m.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 VE2m LS の仮想 IP アドレスを指定します。
```

図 13-1：IPCOM VE2m SC DNS サーバの設定

第 14 章 【LS/SC】IPCOM VE2m の運用開始

14.1【LS】IPCOM VE2m LS の仮想 IP アドレスにグローバル IP アドレスを割当

IPCOM VE2m 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 VE2m LS の運用を開始します。(図 14-1)

コマンド例

```
[root@IaaS-Host ]# PORT_NAME=ipcom_ve2m_virtual_server
[root@IaaS-Host ]# NETWORK_ID="FrontNetwork の ID"
[root@IaaS-Host ]# SUBNET_ID="FrontNetwork のサブネット ID"
[root@IaaS-Host ]# FIXED_IP_ADDRESS=192.168.100.200                    ※1
[root@IaaS-Host ]# SG_ID="「SecurityGroup の作成」で作成した SecuriryGroupID"
[root@IaaS-Host ]# AZ="IPCOM VE2m が配備されている AZ"

# 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@IaaS-Host ]# curl -Ss $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": "'$PORT_NAME'", "availability_zone":
"'$AZ'", "fixed_ips": [{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}],
"security_groups": ["'$SG_ID'"]}}' | 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@IaaS-Host ]# NETWORK_ID="ext-network の ID"
[root@IaaS-Host ]# VM_PORT_ID="新規作成したポートの ID"
[root@IaaS-Host ]# AZ="IPCOM VE2m が配備されている AZ"
curl -Ss $NETWORK/v2.0/floatingips -X POST -H "X-Auth-Token:$OS_AUTH_TOKEN" -H "Content-
Type:application/json" -d '{"floatingip":{"floating_network_id":"'$NETWORK_ID'", "port_id":"'$VM_PORT_ID'",
"availability_zone": "'$AZ'"}}' | 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(※2)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 WebServer のデフォルトゲートウェイは IPCOM VE2m の BackNetwork 側の代表 IP を指定してください。

図 14-1：IPCOM VE2m LS の仮想 IP アドレスにグローバル IP アドレスを割当

14.2【SC】IPCOM VE2m 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 VE2m 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 VE2m SC の運用を開始します。(図 14-2)

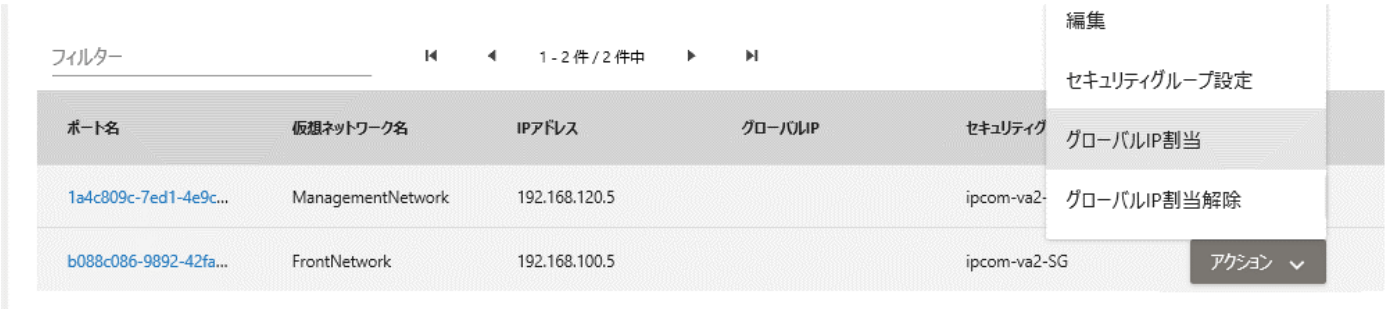


図 14-2：IPCOM VE2m SC の FrontNetwork 側の IP アドレスにグローバル IP アドレスを割当

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 VE2m 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 EX2 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-VE2m-front-net
    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-VE2m-back-net
    ip-routing
    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-VE2m-management-net
    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 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
!
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 VE2m 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 EX2 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-ve2m.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-VE2m.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-VE2m-SC-front-net
    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-VE2m-SC-management-net
    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：コンフィグドライブを指定した IPCOM VE2m 仮想サーバの構築手順

［注意］

西日本第 1/第 2 リージョン、東日本第 1/第 2 リージョンは、コンフィグドライブに対応していません。コンフィグドライブを指定して IPCOM VE2m 仮想サーバを作成しないでください。

また、セキュリティの観点から、お客様自身で admin ユーザーのパスワードを設定するまで、ssh 等でリモートログインできる状態にしないでください。

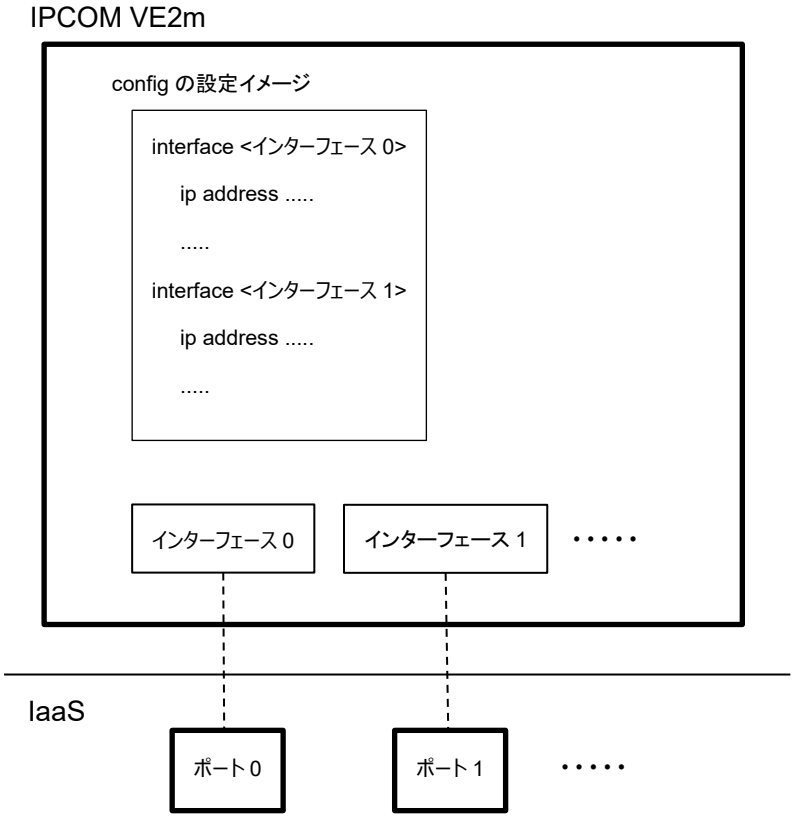
付録 D：IPCOM VE2m および IaaS の構成

D-1 IPCOM VE2m のインターフェースと IaaS のポートの関係

本節では、IPCOM VE2m 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 VE2m 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 VE2m 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

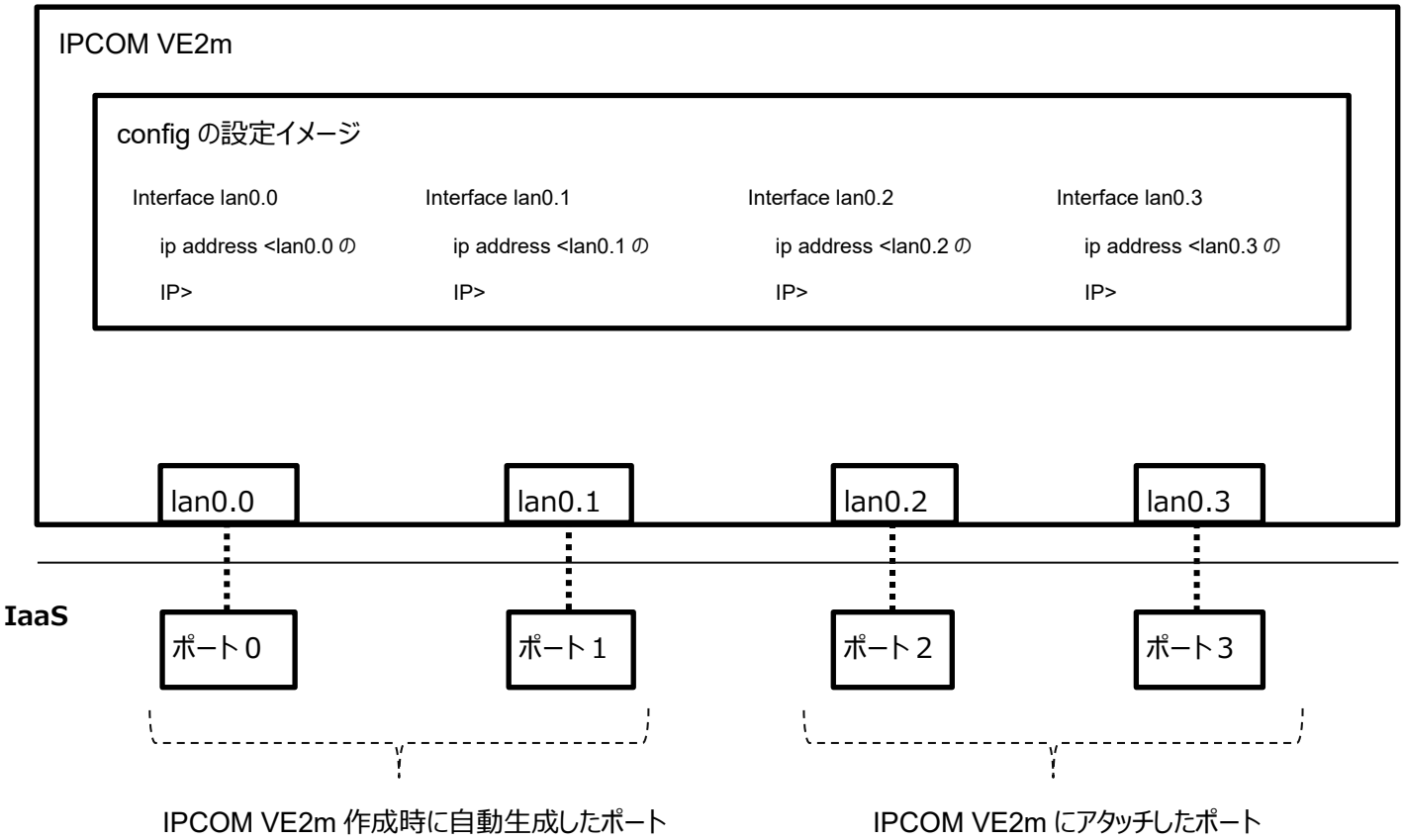
上記の対応付けの仕様を下図に示します。



- IPCOM VE2m 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 VE2m 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 VE2m 作成時に自動生成された IaaS のポート
  ② IPCOM VE2m に対してアタッチした IaaS のポート
- IPCOM VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m においてできなくなります。

・ IPCOM VE2m のファームウェア版数が V01L04NF0401 より前の場合、インタフェースの仕様は以下の通りです。
IPCOM VE2m にアタッチ済の IaaS のポートをデタッチした後、IPCOM VE2m 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 VE2m 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。
ネットワーク構成手順は「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」を参照してください。
・ IPCOM VE2m のファームウェア版数が V01L04NF0401 以降の場合、インタフェースの仕様は IPCOM VE2 シリーズ VE2 ユーザーズガイド 「1-1-1 IPCOM VE2 の製品仕様」を参照してください。
ネットワーク構成手順は「D-3 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(V01L04NF0401 以降)」を参照してください。
・ IPCOM VE2m が認識するインターフェース数については、IPCOM VE2 シリーズ VE2 ユーザーズガイド 「1-1-1 IPCOM VE2 の製品仕様」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 VE2m を設定した場合について記載しています。
・ IPCOM VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m の停止

IPCOM VE2m 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 VE2m 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 VE2m の起動

IPCOM VE2m を起動してください。

(7) IPCOM VE2m のインターフェースと IaaS のポートの関係の確認

IPCOM VE2m 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 VE2m 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
 lan0.0       MTU:    1500   <LINKUP>
   Type: gigabit ethernet
   Description:
   MAC address: fa:16:3e:00:d4:0f
   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 VE2m 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 VE2m 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 VE2m 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 VE2m 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 VE2m において全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
lan0.0        MTU:    1500   <LINKUP>
    Type: gigabit ethernet
    Description:
    MAC address: fa:16:3e:00:d4:0f
    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 VE2m 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。

D-3 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(V01L04NF0401 以降)

IPCOM VE2m 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 VE2m 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 VE2m 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) IPCOM VE2m の停止

IPCOM VE2m を停止します。以下のコマンドを実行してください。

```
ipcom# poweroff
```

(3) 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 VE2m 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。

(4) IPCOM VE2m の起動

IPCOM VE2m を起動してください。

(5) IPCOM VE2m のインターフェースと IaaS のポートの関係の確認

IPCOM VE2m 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 VE2m 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 system resource
CPU : 4
Memory : 7982MB
HDD : PRESENT
HDD size : 100GB
Cipher Card : NO_PRESENT
lan0.0
    driver      : virtio_net
    MAC address: FA:16:3E:00:D4:0F
lan0.1
    driver      : virtio_net
    MAC address: FA:16:3E:78:E1:7E
・・・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"
      }
    ],
```

(6) インターフェースの構成定義の変更

前述(5)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 VE2m 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 VE2m 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。

```
ipcom(edit)# interface <インターフェース名>
ipcom(edit-if)# ip address <IaaS のポートの IP アドレス>
ipcom(edit-if)# exit
```

IaaS のポートの定義と、IPCOM VE2m 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 VE2m 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
```

(7) 疎通確認

IPCOM VE2m において全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
lan0.0        MTU:    1500   <LINKUP>
    Type: gigabit ethernet
    Description:
    MAC address: fa:16:3e:00:d4:0f
    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 VE2m 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(5)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、(6)以降の手順を再度実施してください。

付録 E：IPCOM VE2m と IaaS の通信設定

E-1 通信設定の概要

IPCOM VE2m 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 VE2m に必要な共通設定を下図に示します。

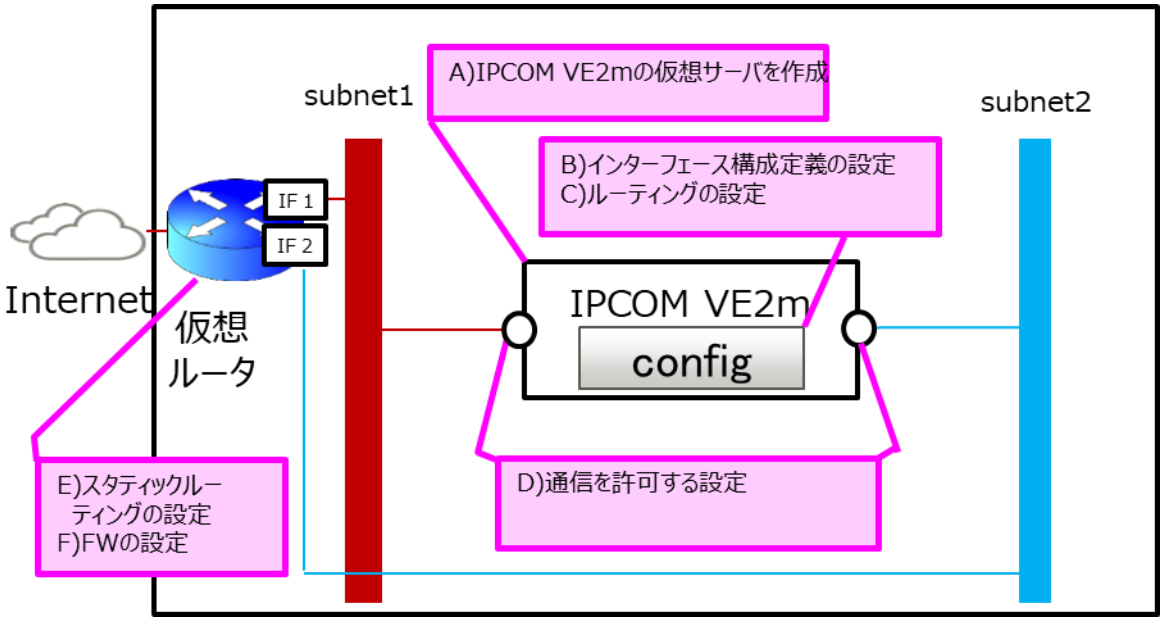


図 E-1-1：IaaS 上の IPCOM VE2m に必要な共通設定

A) IPCOM VE2m の仮想サーバを作成します。詳細は、API リファレンス（Foundation Service 編）（東日本第 1，西日本第 1，西日本第 2）の「1.3.3.17 Create server (1)」をご確認ください。実行例は、4.1 【LS】IPCOM VE2m の作成(LS primary)をご確認ください。

IPCOM VE2m 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 VE2m にライセンスを登録してください。実行例は、5.2 【LS】IPCOM VE2m 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 VE2m をシャットダウンしてください。

③ API リファレンス（Foundation Service 編）（東日本第 1，西日本第 1，西日本第 2）の「5.2.2.6 Create volume (1)」API で、追加ボリュームを作成してください。「1.6.2.3 Attach volume」API で、IPCOM VE2m 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 API リファレンス（Foundation Service 編）（東日本第 1，西日本第 1，西日本第 2）の「1.4.3.7 Start server」API またはポータルサイトより、IPCOM VE2m 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 EX2 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、メタデータ通信のためのスタティックルーティングを追加します。実行例は、10.3 メタデータ通信用の設定をご確認ください。

F) 仮想ルータに対し、FW ルールを設定します。詳細は、IaaS 機能仕様書の「5.6 ファイアーウォール」をご確認ください。設定例は、10.4 仮想ルータの FW 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。

本節では、ワンアーム構成のサーバ負荷分散に対応した設定方法を記載しています。そのため、負荷分散対象仮想サーバから Internet 方向の通信を IPCOM VE2m に向ける設定(下記「B)」)が、本書の事例の 10.5 WebServer のデフォルトゲートウェイ設定と異なりますので、ご注意ください。

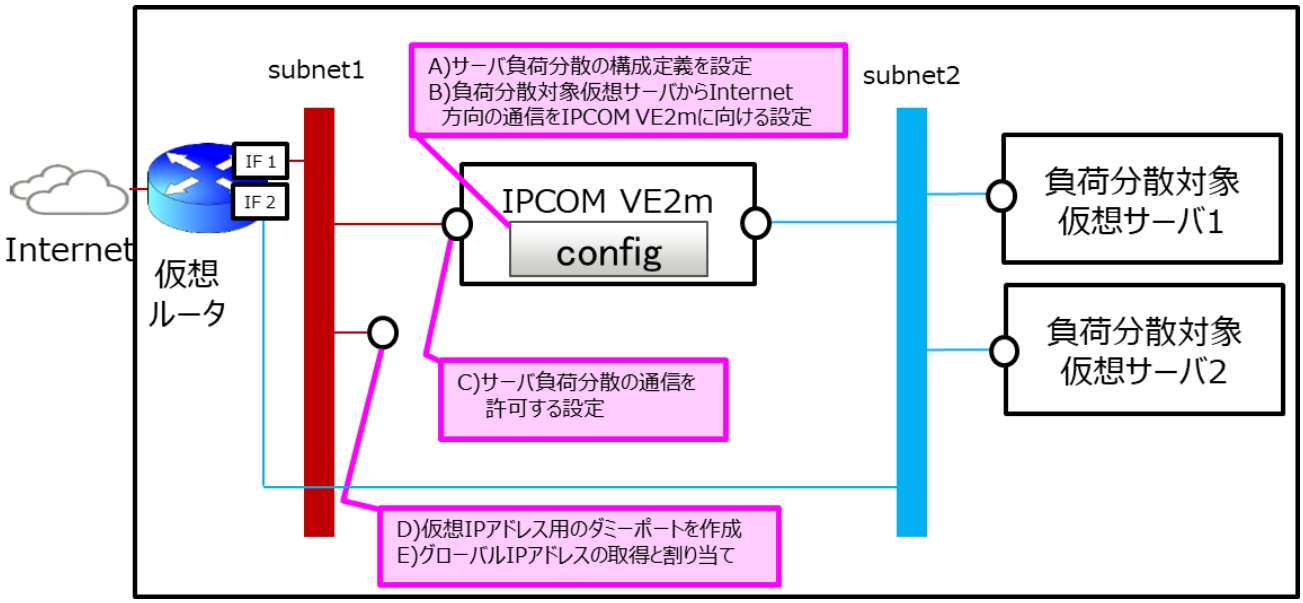


図 E-1-2：IaaS 上のサーバ負荷分散機能使用時に必要な設定

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 EX2 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 VE2m 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 VE2m 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 VE2m と負荷分散対象仮想サーバ間の通信の宛先および送信元 IP アドレス

通信方向	宛先 IP アドレス	送信元 IP アドレス
IPCOM VE2m→負荷分散対象仮想サーバ	負荷分散対象仮想サーバ	IPCOM VE2m
負荷分散対象仮想サーバ→IPCOM VE2m	IPCOM VE2m	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設定してください。前述 B)の設定を仮想ルータ側のインターフェース構成定義に行ってください。

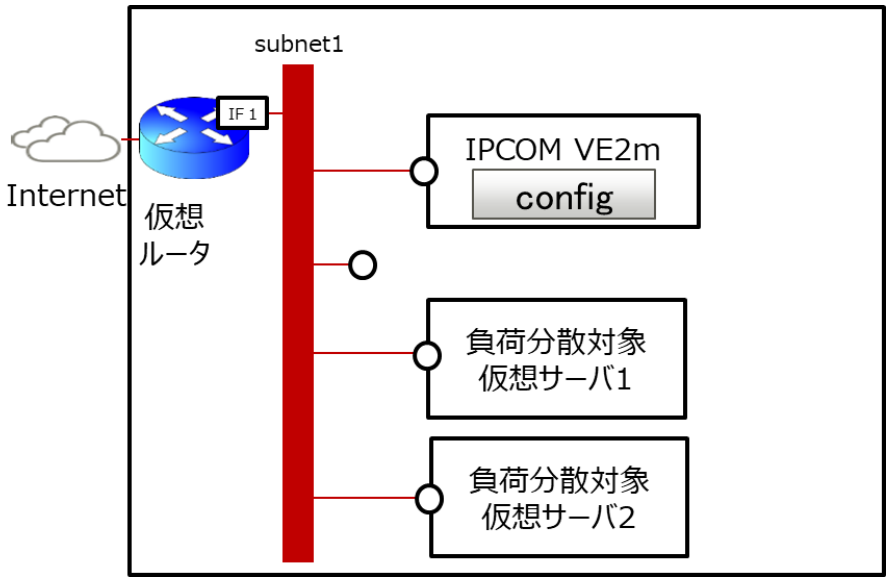


図 E-1-4：IaaS 上の 1 つのサブネットに IPCOM VE2m と負荷分散対象仮想サーバを配置したワンアーム構成

(3) FW 機能

FW 機能使用時に必要な設定を下図に示します。

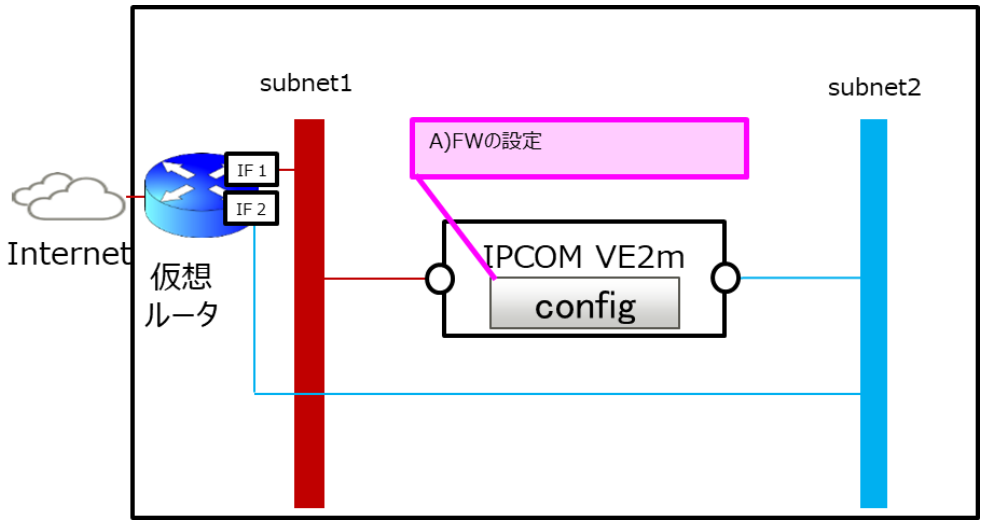


図 E-1-5：IaaS 上の FW 機能使用時に必要な設定

A) IPCOM VE2m の構成定義に FW ルールを設定します。詳細は、IPCOM EX2 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。

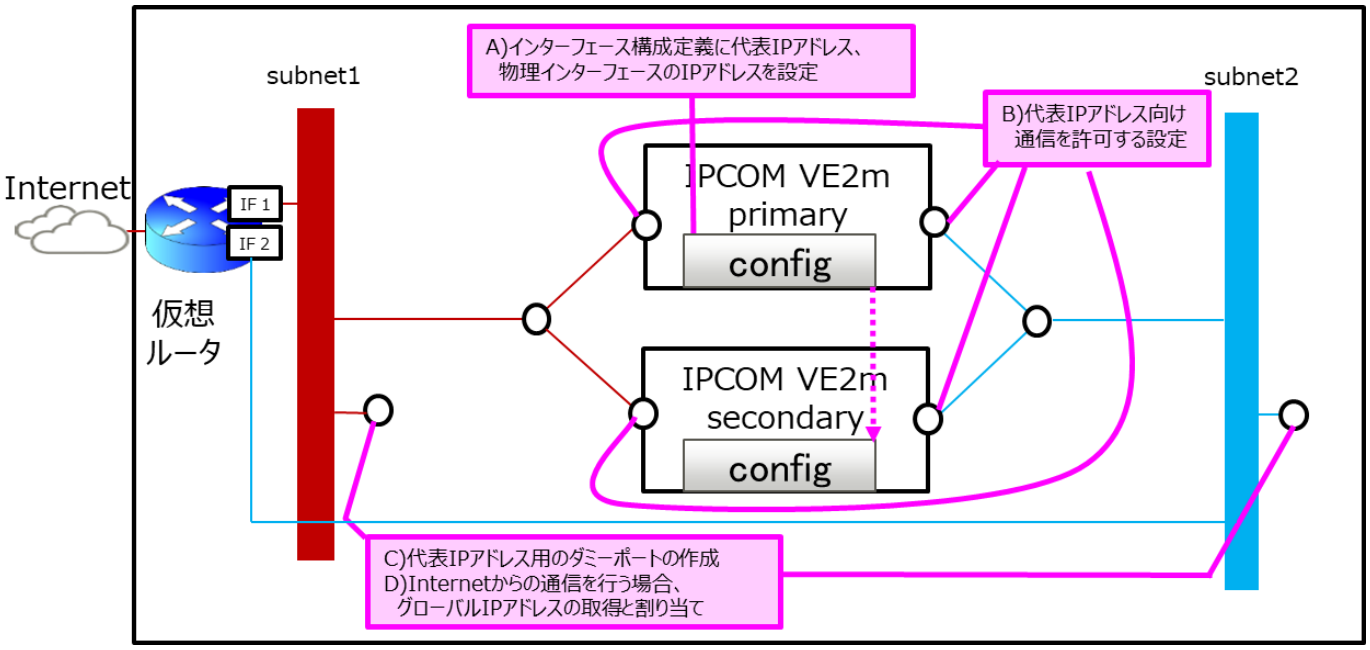


図 E-1-6：IaaS 上の冗長化構成に必要な設定

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-2 IaaS のポートの通信許可設定

IPCOM VE2m 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（Network 編）（東日本第 1，西日本第 1，西日本第 2）の「1.5.2.4 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：「1.5.2.4 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	MAC アドレス(“mac_address”)は指定しないでください。 全通信を許可する場合、"0.0.0.0/1"と"128.0.0.0/1"を指定してください。	

※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。

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（Network 編）（東日本第 1，西日本第 1，西日本第 2）の「1.5.2.2 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。

表 E-3-1：「1.5.2.2 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 VE2m 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。	

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 EX2 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 VE2m の IP アドレスの詳細は、D-1 IPCOM VE2m 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 VE2m に通信を行う場合、IPCOM VE2m 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 VE2m で意図しない破棄が発生してしまうことがあります。

E-7 MTU 値の設定

IaaS 上の IPCOM VE2m の MTU 値は、通信の最適化のため、1500 以下(設定省略時：1500)にしてください。

FUJITSU Hybrid IT Service FJcloud-O IaaS

IPCOM VE2m スタートガイド 1.4 版

発行日 2024 年 10 月