
統合ネットワークサービス
(IPCOM VE2 シリーズ)

V01L06
スタートガイド

はじめに

このたびは、統合ネットワークサービス（IPCOM VE2 シリーズ）をお買い上げいただき、誠にありがとうございます。統合ネットワークサービス（IPCOM VE2 シリーズ）（以降、IPCOM VE2 ソフトウェア、IPCOM VE2 シリーズ、IPCOM VE2、本サービス、本製品、本装置、本ソフトウェア、または仮想マシンと記述する場合があります）は、クラウド上で提供されるサービスであり、インターネットやイントラネットとシステム（サーバー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。

このマニュアルは、本製品をクラウド上で利用するにあたっての導入手順や仕様などについて説明しています。本製品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。

本書をお読みになる前に

本書をお読みになる前に、別冊の「マニュアル体系と読み方」をお読みください。

「マニュアル体系と読み方」では、本製品の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記載しています。

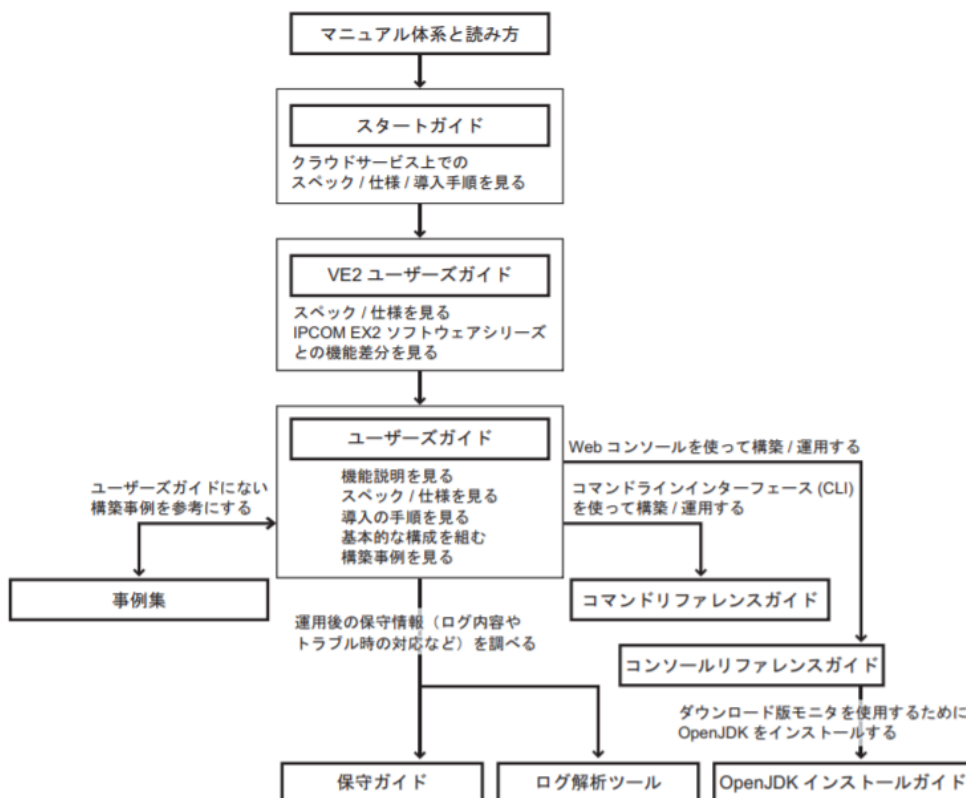
統合ネットワークサービス（IPCOM VE2 シリーズ）は、IPCOM VE2 ソフトウェアシリーズをニフクラ上で提供するサービスであるため、これらのマニュアルを参照しています。本サービスのご利用にあたっては、スタートガイドに記載の仕様や表現が優先されます。

統合ネットワークサービス（IPCOM VE2 シリーズ）のマニュアルには以下のものがあります。

使用する目的に応じてお使いください。

- 統合ネットワークサービス（IPCOM VE2 シリーズ） スタートガイド（本書）
- IPCOM VE2 ソフトウェアシリーズ マニュアル体系と読み方
- IPCOM VE2 ソフトウェアシリーズ VE2 ユーザーズガイド
- 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 事例集
- 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 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 保守ガイド

以下に各マニュアルの関係を示します。



本書の目的と構成

本書の目的と構成及び概要について説明いたします。

本書の目的

本書は、本製品をニフクラ上で利用するにあたっての導入手順や仕様、留意事項について説明したものです。

本書の構成

本書は、以下のような構成になっています。

第 1 章 **IPCOM VE2** とは

本製品の特長について説明しています。

第 2 章 **IPCOM VE2** ご利用の流れ

ニフクラ上で本製品を導入するまでの流れを説明しています。

第 3 章 **IPCOM VE2** の作成

本製品の作成手順について説明しています。

第 4 章 **IPCOM VE2** のライセンス登録

本製品に対してライセンスを登録する手順を説明しています。

第 5 章 **IPCOM VE2** の設定

本製品の各種設定を行う手順を説明しています。

第 6 章 留意事項

本製品を使用するにあたっての留意事項について説明しています。

第 7 章 構成例

本製品が提供する個々の制御機能の構成定義例を元に、構成定義コマンドの使用方法や必要な定義内容について説明しています。

安全にお使い頂くために

本製品を安全に正しくお使いいただくために守って頂きたい重要な情報を記載しています。

セキュリティの確保について

本製品出荷時には、初期導入時の設定を行うためのユーザー（ユーザー名：admin、パスワード：なし）が登録されています。セキュリティ確保のために、運用に入る前にパスワードの設定と IPCOM VE2 への管理者アクセスを信頼できる端末だけに制限する適切なアクセスコントロールを必ず実施してください。

輸出管理規制について

当社のドキュメントには「外国為替および外国貿易管理法」に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

ハイセイフティについて

〔高度な安全性が要求される用途への使用について〕

本製品は、一般事務用、パーソナル用、家庭用、通常の産業などの一般的用途を想定して開発・設計・製造されているものであり、原子力施設での核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムでの運行制御、生命維持のための医療用機器、兵器システムでのミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性をともなう用途（以下「ハイセイフティ用途」という）に使用されるよう開発・設計・製造されたものではありません。お客様は本製品を必要な安全性を確保する措置を施すことなくハイセイフティ用途に使用しないでください。また、お客様がハイセイフティ用途に本製品を使用したことにより発生する、お客様または第三者からのどんな請求または損害賠償に対しても富士通株式会社およびその関連会社は一切責任を負いかねます。

目次

はじめに.....	2
本書をお読みになる前に.....	3
本書の目的と構成.....	4
本書の目的	4
本書の構成	4
安全にお使い頂くために.....	5
セキュリティの確保について	5
輸出管理規制について	5
ハイセイフティについて.....	5
目次	6
1 IPCOM VE2 とは	8
1-1 IPCOM VE2 の特徴	8
1-1-1 IPCOM VE2 の製品仕様.....	8
1-2 IPCOM VE2 の機能	9
1-2-1 提供機能.....	9
2 IPCOM VE2 ご利用の流れ.....	23
2-1 本製品の導入の流れ.....	23
2-1-1 運用ライセンス発行前	23
2-1-2 運用ライセンス発行後	24
3 IPCOMVE2 の作成	27
3-1 サーバーの作成	27
3-2 ディスクの追加.....	33
3-3 NIC の追加	37
3-4 マルチ IP アドレスの追加	42
3-5 サーバーの起動	47
4 IPCOM VE2 の ライセンス登録.....	51
4-1 IPCOM VE2 のライセンス登録	51
5 IPCOM VE2 の設定.....	54
5-1 ホスト名とパスワードの設定.....	54
5-2 IPCOM VE2 への SSH 接続	55
5-3 マルチ IP アドレスの設定	58
5-4 IPCOM VE2 への WEB コンソール接続	60
6 留意事項	62
6-1 初期定義について	62
6-2 コンフィグドライブの留意事項	64
6-2-1 IP アドレス	エラー! ブックマークが定義されていません。

6-2-2 admin ユーザーのリモートアクセス可否	エラー! ブックマークが定義されていません。
7 構成例	65
7-1 インターネット公開	65
7-1-1 インライン（ファイアーウォール/アドレス変換）	エラー! ブックマークが定義されていません。
7-1-2 インライン（SSL アクセラレーター/ サーバー負荷分散）	68
7-1-3 ワンアーム（サーバー負荷分散+Web ア クセレーション）	73
7-1-4 プライベートセグメントを挟んだインライン	76
7-2 イントラネット公開（閉域網 接続）	77
7-2-1 インライン（ファイアーウォール/アドレス変換）	77
7-2-2 インライン（SSL アクセラレーター/ サーバー負荷分散）	80
7-2-3 ワンアーム（サーバー負荷分散+Web ア クセレーション）	83
7-2-4 プライベートセグメントを挟んだインライン	84
7-2-5 プロキシ	85
7-2-6 冗長化(1)サーバーセパレート	86
7-2-7 冗長化(2)マルチゾーン・プライベー トブリッジ	90

1 IPCOM VE2 とは

1 - 1 IPCOM VE2 の特長

本製品は IPCOM VE2 ソフトウェアシリーズ相当の機能を有するサービスです。

本製品は、IPCOM VE2 ソフトウェアシリーズをニフクラ上で提供するサービスです。

本製品は、以下のような特長を持っています。

- 独立性
管理ホスト上で仮想マシンとして動作し、同一の管理ホスト上で動作するほかの IPCOM VE2 に運用面での影響を与えない、高い独立性を実現します。
- サイジングの簡易化
性能・機能・容量に応じてあらかじめ用意されており、サイジングの簡易化を実現します。

1 - 1 - 1 IPCOM VE2 の製品仕様

本製品を構成するシリーズは以下のとおりです。

シリーズ名	主要サポート機能
LS シリーズ	サーバー負荷分散機能、SSL アクセラレーター機能
LS PLUS シリーズ	サーバー負荷分散機能、SSL アクセラレーター機能、WAF 機能
SC シリーズ	ファイアーウォール機能、IPsec-VPN 機能
SC PLUS シリーズ	ファイアーウォール機能、IPsec-VPN 機能、L2TP/IPsec 機能

本書で説明するサポートクラウドサービスは以下のとおりです。

- ニフクラ
- FUJITSU Hybrid IT Service FJcloud-V

本製品が必要とするニフクラでのサーバータイプおよびその他の仮想ハードウェアリソースは以下のとおりです。

項目		VE2-100	VE2-220
サーバータイプ		h2-small4 / e2-small4 / c2-small4 / h2r-small4 / e-small4 / c-small4	h2-large8 / e2-large8 / c2-large8 / h2r-large8 / e2r-large8 / e-large8 / c-large8
増設ディスク (※1)	容量	100GB	
	ディスクタイプ	標準ディスク/高速ディスク [A/B] /フラッシュドライブ/ 標準フラッシュドライブ [A/B] /高速フラッシュドライブ [A/B]	
仮想 LAN インターフェース		最大 8port	
コンソール(VGA)		○	

※1 増設ディスクは必須です。

参照

その他、製品仕様に関する詳細は「VE2 ユーザーズガイド」を参照してください。

ご注意

LS PLUS2 シリーズおよび VE2-200 は、本サービスではサポートしていません。

1 - 2 IPCOM VE2 の機能

本製品が提供する機能一覧を、以下に示します。

1 - 2 - 1 提供機能

ここでは、シリーズごとの提供機能について説明します。なお、ニフクラ上ではクラウドサービスの仕様により一部未サポートになる機能があります。以下の表の " ニフクラ上でのサポート可否 " を参照してください。各機能の詳細は、「ユーザーズガイド」および「VE2 ユーザーズガイド」を参照してください。ニフクラでは、グローバルネットワークとプライベートネットワークで制約が異なるため、機能のサポートの有無をネットワークごとに記載しています。VE2 のインターフェースが、共通グローバルに 1 つでも接続している場合は「グローバル」、プライベート LAN だけに接続している場合は、「プライベート」の項目を参照してください。

1-2-1-1 レイヤー2 中継機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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 ○ : オプション機能 × : 未サポート

※ 管理ホスト側で仮想マシンに対して、タグつきフレームを送受信できない場合は使用できません。

1-2-1-2 PPPoE クライアント機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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 ○ : オプション機能 × : 未サポート

1-2-1-3 レイヤー3 中継機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
ルーティング (IPv4)	スタティック	●	●	●	●	●	●
	RIP v1	●	●	●	●	×	×
	RIP v2 (MD5 認証)	●	●	●	●	×	×
	OSPFv2	●	●	●	●	×	×
	BGP4	●	●	●	●	×	×
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 ○：オプション機能 ×：未サポート

1-2-1-4 レイヤー3 中継機能(IPv6)

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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(IPv6)	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 ○：オプション機能 ×：未サポート

1-2-1-5 サーバー負荷分散機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
配置方法	並列型配置	●※	●※	×	×	×	×
	通過型ワンアーム配置	●	●	×	×	●	●
	通過型配置	●	●	×	×	●	●
転送方式	IP アドレス変換	●	●	×	×	●	●
	MAC アドレス変換	●	●	×	×	●	●
サーバー分散方式	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	●	●	×	×	●	●
	最小サーバー負荷	●	●	×	×	●	●
	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	●	●	×	×	●	●
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ー		●	●	×	×	●	●
クライアントの関連づけ		●	●	×	×	●	●
サーバー保守制御		●	●	×	×	●	●
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 ○：オプション機能 ×：未サポート

※ 並列型配置は、VMware 上では使用できません。

ご注意

グローバル側でのサーバー負荷分散ルールの仮想 IP アドレスにはマルチ IP アドレスを使用する必要があります。

なお、サーバー負荷分散ルールの仮想 IP アドレスは、インターフェース、あて先アドレス変換ルールの変換前アドレス、送信元アドレス変換ルールの変換後アドレスの IP アドレスと異なっている必要があります。

1-2-1-6 QoS 制御(帯域制御)機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LSPLUS	SC	SCPLUS	グローバル	プライベート
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	●	●	×	●	●	●
	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 ○：オプション機能 ×：未サポート

1-2-1-7 リンク負荷分散機能

本製品ではサポートしていません。

1-2-1-8 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。

1-2-1-9 ファイアウォール機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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 (REDIRECT)	●	●	●	●	●

		無効化 (REMOVE)	●	●	●	●	●	●
セッションログ（標準形式/WELF 形式）			●	●	●	●	●	●

●：基本機能 ○：オプション機能 ×：未サポート

1-2-1-10 IPS 機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
				LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
アナマリ型 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		●	●	●	●	●	●
		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 ○：オプション機能 ×：未サポート

1-2-1-11 WAF 機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
動作モード	ブリッジモード	×	●	×	×	×	●
	ルータモード	×	●	×	×	●	●
防御動作	通過	×	●	×	×	●	●

(アクション)	拒否	×	●	×	×	●	●
	エラーページ応答	×	●	×	×	●	●
	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 ○：オプション機能 ×：未サポート

ご注意

グローバル側でインターフェースに設定した IP アドレスと異なる IP アドレスを受信する場合には、ニフクラの「マルチ IP アドレス」を使用する必要があります。

1-2-1-12 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。

1-2-1-13 アンチウイルス機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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）	○	○	○	○	×	×
ウイルスパターンファイルのアップ	自動	○	○	○	○	×	×

ブデット	手動	○	○	○	○	×	×
スパムメール対策	SMTP	○	○	○	○	×	×
	POP3	○	○	○	○	×	×

●：基本機能 ○：オプション機能 ×：未サポート

1-2-1-14 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。

1-2-1-15 アドレス変換機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
	LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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 ○：オプション機能 ×：未サポート

ご注意

グローバル側でインターフェースに設定した IP アドレスと異なる IP アドレスを受信する場合には、ニフクラの「マルチ IP アドレス」を使用する必要があります。あて先アドレス変換ルールの変換前アドレス、送信元アドレス変換ルールの変換後アドレスは、インターフェースの IP アドレス、サーバー負荷分散ルールの仮想 IP アドレスと異なっている必要があります。グローバル側で使用する場合は、ニフクラの「マルチ IP アドレス」を使用し、これらの IP アドレスと異なる IP アドレスを割り当ててください。

あて先アドレス / ポート変換ルールや送信元アドレス / ポート変換ルールでは、インターフェースに割り当てられた IP アドレスを使用できます。

1-2-1-16 ユーザー認証機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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 アクセラレーター時)	●	●	●	●	●	●
	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 ○：オプション機能 ×：未サポート

1-2-1-17 IPsec-VPN 機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
			LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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 トラバース			×	×	●（※1）	●（※1）	●	●
ファイアウォール連携			×	×	●	●	●	●
鍵管理機能	鍵交換	Manual	×	×	●	●	●	●

	IKE 認証方式	IKE	×	×	●	●	●	●
		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 ○：オプション機能 ×：未サポート

※1 IPv6 は未サポート。

1-2-1-18 L2TP/IPsec 機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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 キーブアライブ機能	×	×	×	●	●	●
	無通信監視機能	×	×	×	●	●	●
	最大セッション時間監視機能	×	×	×	●	●	●
	セッション数超過/ 警告通知機能	×	×	×	●	●	●
ファイアウォール連携		×	×	×	●	●	●
アドレス変換連携		×	×	×	●	●	●
IPsec-VPN 連携		×	×	×	●	●	●
アンチウイルス機能連携		×	×	×	○	×	×
Web コンテンツ・フィルタリング機能連携		×	×	×	×	×	×

●：基本機能 ○：オプション機能 ×：未サポート

1-2-1-19 SSL アクセラレーター機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
プロトコル	SSL v3.0	●	●	×	●	●	●
	TLS v1.0	●	●	×	●	●	●
	TLS v1.1	●	●	×	●	●	●
	TLS v1.2	●	●	×	●	●	●

暗号スイート	鍵交換	RSA, ECDHE_RSA	●	●	×	●	●	●
	暗号化	3DES, AES, RC4,AES_GCM	●	●	×	●	●	●
	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-cookie			●	●	×	●	●	●

●：基本機能 ○：オプション機能 ×：未サポート

ご注意

グローバル側でインターフェースに設定した IP アドレスと異なる IP アドレスを受信する場合には、ニフクラの「マルチ IP アドレス」を使用する必要があります。

1-2-1-20 SSL-VPN 機能

本製品ではサポートしていません。

1-2-1-21 HTTP コンテンツ圧縮機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
	LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
HTTP 通信	●	●	●	●	●	●
HTTPS 通信	●	●	×	●	●	●

●：基本機能 ○：オプション機能 ×：未サポート

1-2-1-22 FNA ルーティング機能

本製品ではサポートしていません。

1-2-1-23 ネットワークサービス機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
	LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
DHCP サーバー	×	×	●	●	×	×
DHCP リレーエージェント	×	×	●	●	×	×
DHCP クライアント	●	●	●	●	●	●
DNS サーバー	×	×	●	●	●	●
DNS プロキシ	×	×	●	●	×	×

●：基本機能 ○：オプション機能 ×：未サポート

※ DNS サーバー /DNS プロキシ機能は、PPPoE クライアント機能や DHCP クライアント機能のために簡易的な機能として提供しているもので、本格的に DNS サーバー機能を使用する場合は、外部の DNS サーバーを使用されることを推奨します。

1-2-1-24 ビジュアライザ機能

本製品ではサポートしていません。

1-2-1-25 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。

1-2-1-26 高信頼性機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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)		×	×	×	×	×	×
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 ○ : オプション機能 × : 未サポート

1-2-1-27 ドメインリスト管理

本製品ではサポートしていません。

1-2-1-28 運用管理/保守機能

本機能で、シリーズ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				ニフクラ上でのサポート可否	
		LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
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（※1）		●	●	●	●	●	●
アラーム表示機能（※2）	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)（※3）	●	●	●	●	●	●
	Telnet サーバー	●	●	●	●	●	●
	SSH サーバー	●	●	●	●	●	●
	SSH クライアント	●	●	●	●	●	●
	FTP クライアント	●	●	●	●	●	●
	TFTP クライアント	●	●	●	●	●	●
	HTTP サーバー機能	●	●	●	●	●	●
保守形態	local（※3）	●	●	●	●	●	●
	remote	●	●	●	●	●	●
	パネル	×	×	×	×	×	×
UPS LAN		×	×	×	×	×	×

機能			サポート可否				ニフクラ上でのサポート可否	
			LS	LS PLUS	SC	SC PLUS	グローバル	プライベート
保守機能	IP ホスト機能	ping	●	●	●	●	●	●
		traceroute	●	●	●	●	●	●
	NTP クライアント		●	●	●	●	●	●
	NTP サーバー		●	●	●	●	●	●
	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応 (REMCS) (※4)	×	×	×	×	×	×
	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-II	●	●	●	●	●	●
	拡張 MIB	●	●	●	●	●	●
統計スナップショット		×	×	×	×	×	×
セーフモード		×	×	×	×	×	×

●：基本機能 ○：オプション機能 ×：未サポート

※1 ハイパーバイザーまたはオーケストレーターと連携して、本製品の初期設定を行います。詳細は、

[コンフィグドライブの留意事項](#)を参照してください。

※2 ハードウェア状態は管理ホスト側で監視。

※3 ハイパーバイザー経由でだけ接続可能。

※4 センターへのリモート通報（NST で SNMP-Trap を監視し、通報を行います）は、別途ネットワーク LCM サービスの契約が必要です。

1 - 3 IPCOM VE2 ライセンス

本製品のライセンスについて以下に示します。

- 公開イメージの種類

月額向けイメージは SC/SCP/LS/LSP の 4 種 × 試用/正式の 2 種の合計 8 種を提供します。

- 機種

仮想マシン起動時に、割り当てられたリソースから VE2-100/220 の機種を決定します。

- ライセンス移行

今後は月額ライセンスのみの提供となり、年額ライセンス(既存)の利用者については、月額ライセンスへの移行を推進するため、月額ライセンスで動作している場合を従来通りの表示とします。

2 IPCOM VE2 ご利用の流れ

2 - 1 本製品の導入の流れ

本製品をニフクラで導入する場合の基本的な流れを示します。

2 - 1 - 1 運用ライセンス発行前

作業		
準備	1) 操作用仮想マシンを準備する	コマンドラインインターフェース (CLI) または Web コンソールを使用して、本装置の構成定義を行うために必要な操作用仮想マシン (コマンド操作端末または Web ブラウザ端末) を準備してください。操作用仮想マシンは、プライベートネットワーク (プライベート LAN) に接続してください。または、ニフクラのコンソールを使用して設定してください。
	2) 本製品を準備する	本製品の仮想マシンを作成します。 ニフクラ上の本製品紹介ページから導入ライセンスの発行依頼を行い、導入ライセンスを入手してください。 本製品に必要なハードウェアリソースは、 IPCOM VE2 の製品仕様 を参照してください。また、仮想マシンの作成方法は IPCOMVE2 の作成 を参照してください。 スクリプト機能を利用することで、導入ライセンス登録前の本製品に対して一部の構成定義を設定した状態で起動できます。スクリプト機能での設定方法は サーバーの作成 を参照してください。 初回起動時にリモート接続する場合はスクリプトの利用が必須です。スクリプト機能を使用しない場合の定義は 初期定義について を参照してください。 本製品は操作用仮想マシンと同一のプライベートネットワーク (プライベート LAN) に接続して、以降の導入手順を実施します。
導入・申請	3) 本製品にログインする	本製品に CLI または Web コンソールからログインします。CLI は、telnet や ssh によってリモートで接続、またはニフクラのコンソールから接続します。
	4) 日時を設定する	date コマンドにより、システム日付および時刻を設定します。ライセンスの有効期限が正しく処理されるよう、ライセンス登録前に必ず正しい日時を設定してください。
	5) 導入ライセンス (※1) を登録する	本製品を使用するために必要な導入ライセンスを登録し、再起動します。 IPCOM VE2 のライセンス登録 を参照してください。
	6) オプション製品のライセンスキーを設定する	ライセンスキー設定が必要なソフトウェアオプションをご購入された場合は、license key コマンドまたは Web コンソールを使用して、ライセンスキーを登録します。
	7) 基本設定を行う	本製品を運用するための基本的な項目の定義を行います。アクセス制御ルールやアクセス制御マップのルールを定義しない、またはアクセス制御ルールやアクセス制御マップのルールに一致しない通信は、アクセス制御のデフォルト動作モード省略時、ARP バケットを除いてすべて廃棄となります。
	8) 利用する機能の設定を行う	本製品が提供するサーバー負荷分散、ファイアウォール機能、装置二重化、SSL アクセラレーターなどの構成定義を行います。
	9) 構成定義情報を反映する	7)、8) で設定した構成定義情報を本製品に反映します。
	10) ネットワークの接続状況を確認する	操作用仮想マシンを使用して、本製品が正しくネットワークに接続され、正常に通信が行われるかを確認します。
	11) システムの環境を退避する	操作用仮想マシンを使用して、本製品に設定した構成定義情報や証明書などを外部に退避、保存します。
	12) 運用ライセンスキーの発行を申請する	本製品を導入ライセンスの試用利用期間後も継続運用するために必要な、運用ライセンスキーの発行を申請します。 show ipcom-virtual-machine-id コマンドまたは Web コンソールにより、IPCOM 仮想マシン識別子 (※2) を確認し、下記 URL のフォームより必須事項をご記入の上、お申し込みください。 https://inquiry.nifcloud.com/webeq/pub/cloud/ipcom_ops_auth

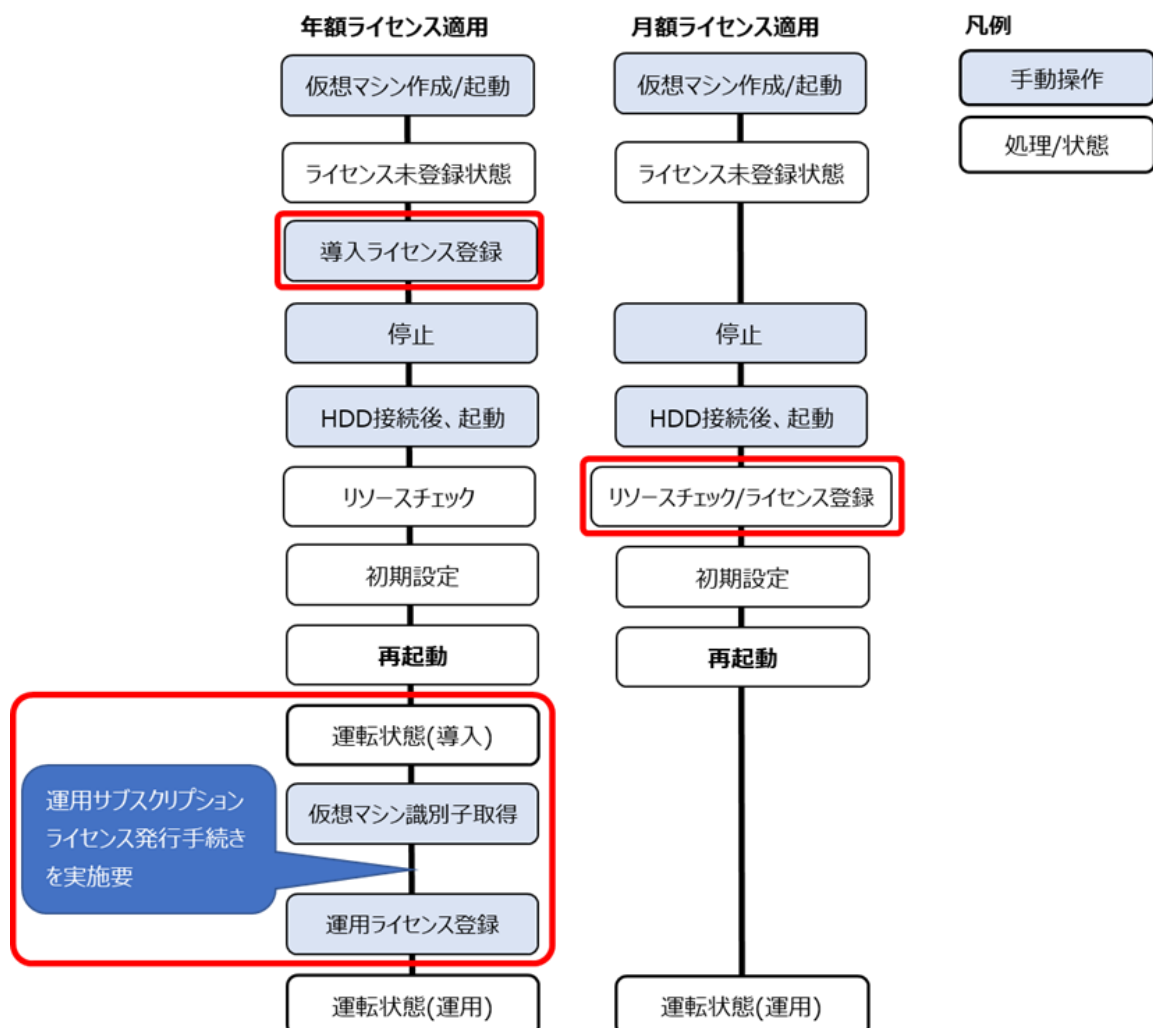
- ※ 1 本ライセンスの試用利用期間は 30 日です。
- ※ 2 IPCOM 仮想マシン識別子は、仮想マシンごとに固有な情報です。

2-1-2 運用ライセンス発行後

作業		
正式運用	13)本製品にログインする	本製品にログインします。CLI または Web コンソールからログインします。リモート接続可能な場合、CLI は、telnet や ssh によってリモートで接続します。 リモート接続できない場合、ニフクラのコンソールで接続します。
	14)運用ライセンスを登録する	本製品を導入ライセンスの試用利用期間後も継続運用するために必要な、運用ライセンスを登録します。 「VE2 ユーザーズガイド」の " 運用サブスクリプションライセンスキーの登録 " を参照してください。

2-1-3 機種変更

アップグレード/ダウングレード方法



機種変更に伴う初期化

仮想マシンへの CPU コア数とメモリ容量の割り当てを変更し、前回起動時と異なる機種に決定した場合、一部の設定情報が初期化されます。

220 から 100 への downgrade 時は諸元が小さくなるため、構成定義情報を初期化します。

また、アップデート・バックアウトなど、機種に依存する情報は、upgrade/downgrade 問わず初期化されます。

VE2 の機種移行により変更後機種における設定情報の初期化有無を以下の表に示します。

変更後機種の初期化の有無： 初期化される : 初期状態の設定に戻る
 初期化されない : 設定状態から変更されない

設定情報	変更後機種の初期化の有無	
	VE2-220 (upgrade)	VE2-100 (downgrade)
バックアウト情報	初期化される	初期化される
アップデート予約	初期化される	初期化される
構成定義情報	初期化されない	初期化される
ユーザー名、パスワード、管理者パスワード（構成定義情報に含む）	初期化されない	初期化される
ファンクショントレース設定情報	初期化されない	初期化されない
SSH 用ホスト鍵（公開鍵と秘密鍵）	初期化されない	初期化されない
SSH コマンド用 known_hosts ファイル （ホスト名とサーバの公開鍵のペアが登録されているファイル）	初期化されない	初期化されない
SSL（Web コンソール）用証明書(ssl-*.crt)	初期化されない	初期化されない
ユーザーが登録、更新した証明書、証明書失効リスト	初期化されない	初期化されない
新規インストール時に登録される CA 証明書	初期化されない	初期化されない
証明書失効リスト（動的にダウンロードしたもの）	初期化されない	初期化されない
証明書の失効確認や公開鍵の使用用途などの証明書の検証条件	初期化されない	初期化されない
SSL アクセラレーターのエラーページファイル	初期化されない	初期化されない
DNS 用のゾーン定義ファイル(*.zone) ※	初期化されない	初期化される
SLB エラーページ(*-slb.html)	初期化されない	初期化されない
アンチウィルスのウィルス検出メッセージ	初期化されない	初期化されない
シグネチャー型 IPS の IPS ポリシー（マスタシグネチャー）	初期化されない	初期化されない
シグネチャー型 IPS の IPS ポリシー（カスタムシグネチャー、検知ポリシー）	初期化されない	初期化されない
シグネチャー型 IPS の IPS ポリシーファイル(ips-policy.xml)	初期化されない	初期化されない
シグネチャー型 IPS のヘルプファイル	初期化されない	初期化されない
WAF グローバルポリシー	初期化されない	初期化される
WAF サイトポリシー	初期化されない	初期化される
WAF 脆弱性レポート	初期化されない	初期化される
WAF 学習データベース	初期化されない	初期化される
WAF 採取パケット	初期化されない	初期化される
WAF 統計情報	初期化されない	初期化される
ライセンス情報	初期化されない	初期化されない
再送ログ	初期化される	初期化される
マスタアプリケーション辞書	初期化されない	初期化されない
import application-dictionary コマンドで、本装置に反映したカスタムアプリケーション辞書	初期化されない	初期化されない
タイムゾーン定義情報	初期化されない	初期化されない
ファームウェア異常時の装置動作設定	初期化されない	初期化されない
復電時の自動電源投入	初期化されない	初期化されない
国/地域別 IP アドレスリスト	初期化されない	初期化されない

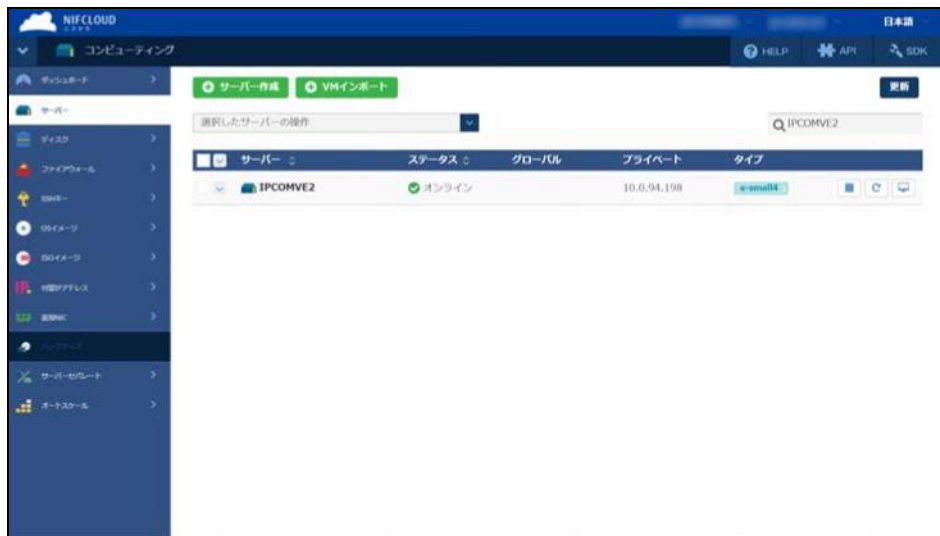
設定情報	変更後機種の初期化の有無	
	VE2-220 (upgrade)	VE2-100 (downgrade)
自動退避された環境定義情報	初期化される	初期化される
ウイルス検出エンジンの更新	初期化されない	初期化されない
アンチウイルスパターンファイル	初期化されない	初期化されない
アンチウイルスの統計情報	初期化されない	初期化されない

3 IPCOMVE2 の作成

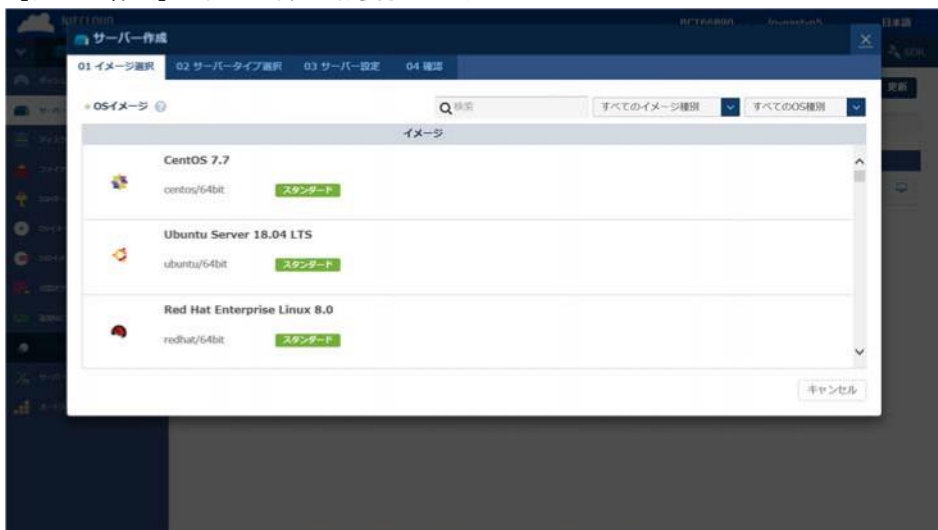
3 - 1 サーバーの作成

サーバーの作成方法について説明します。

1. コントロールパネルの左メニューの「サーバー」を選択し、サーバー一覧を表示します。



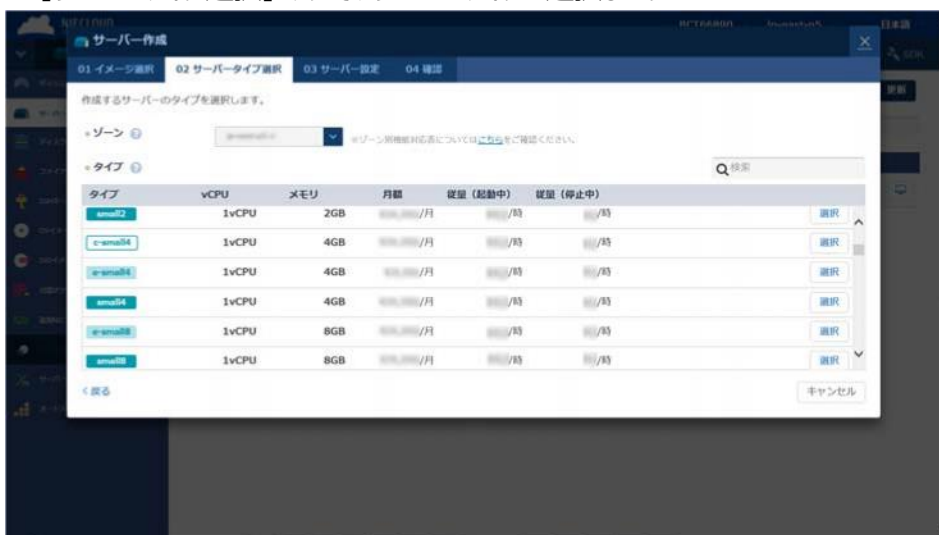
2. 「サーバー作成」ボタンを選択します。
「サーバー作成」ダイアログボックスが表示されます。



3. 「イメージ選択」タブで、OS イメージとして IPCOM VE2 を選択します。



4. 「サーバータイプ選択」タブで、サーバータイプを選択します。



- ゾーン
サーバーを作成するゾーンを指定します。
- タイプ
利用する IPCOM VE2 モデルの vCPU/ メモリに対応するサーバータイプを選択します。

IPCOM VE2 モデル	vCPU	メモリ
IPCOM VE2-100 LS / LS PLUS	1	4GB
IPCOM VE2-220 LS / LS PLUS	4	8GB
IPCOM VE2-100 SC / SC PLUS	1	4GB
IPCOM VE2-220 SC / SC PLUS	4	8GB

IPCOM VE2 の各モデルで選択可能なサーバータイプは、[IPCOM VE2 の製品仕様](#) を参照してください。

5. 「サーバー設定」タブで、サーバーの設定情報を入力します。 情報を入力したあとに、「確認」ボタンを選択します。

- サーバー名
任意の名前を入力します。
- メモ
任意のメモを入力します。
- 料金プラン
料金プランを選択します。
- SSH キー
任意の SSH キーを指定します（IPCOM VE2 では SSH キーによる認証はサポートしていませんが、ニフクラでは指定は必須です）。

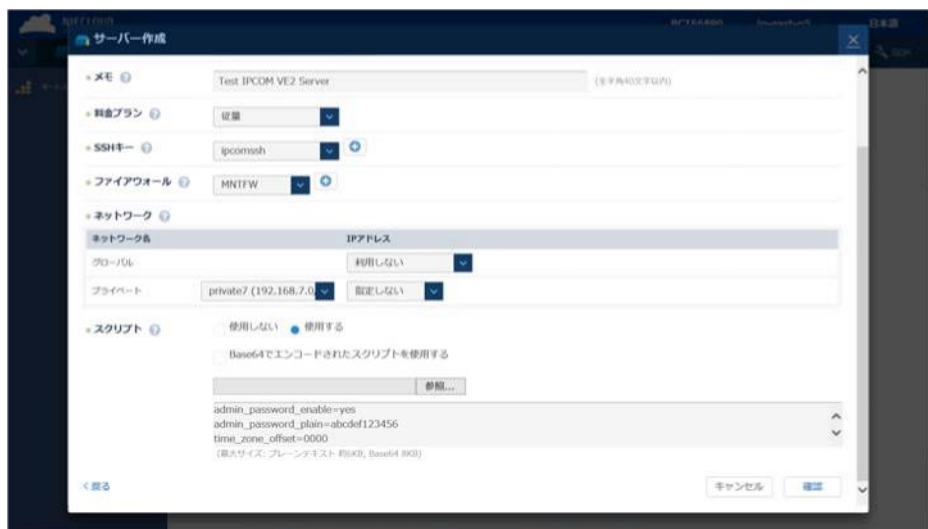
ご注意

IPCOM VE2 SSH サーバー機能では、ユーザー認証はパスワード認証機能だけをサポートします。

- ファイアーウォール
ニフクラが提供するファイアーウォール機能を利用する場合、選択します。ファイアーウォールを設定しないときは、「適用しない」のままとしてください。
- ネットワーク
利用する機能・構成により異なります。[構成例](#)の各機能設定例を参照してください。
 - ーグローバルネットワーク
「自動割り当て」、「付け替え IP アドレス」、「利用しない」から選択します。「利用しない」を選択すると、インターネットからのアクセスはできません。
マルチ IP アドレスを設定する場合は、「自動割り当て」を選択してください。
マルチ IP アドレスの設定については[マルチ IP アドレスの追加](#)を参照してください。
サーバー負荷分散ルール、あて先アドレス変換ルール、送信元アドレス変換ルールでグローバル側の IP アドレスを使用する場合は、マルチ IP アドレスの設定でインターフェースの IP アドレスと異なる IP アドレスを割り当ててください。
 - ープライベートネットワーク
作成済みのプライベート LAN から選択します。IPCOM VE2 では「共通プライベート」を選択しないでください。
 - ープライベートネットワークの IP アドレス
「自動割り当て」、「指定する」、「指定しない」から選択します。
- スクリプト
使用の有無を選択します。

参照

IPCOM VE2 スクリプト使用法は、「IPCOM VE2 ユーザーズガイド」の“コンフィグドライブによる設定”を参照してください。



スクリプトを「使用する」を選択したときは、以下を指定してください。

– 事前にスクリプトをファイルで準備しているときは、そのスクリプトファイルを指定してください。

- Base64 でエンコードされたスクリプトファイルを使用するときは、[Base64 でエンコードされたスクリプトを使用する] をチェックします。
- [参照] ボタンを選択して、スクリプトファイルを指定します。

– スクリプトをファイルで準備していないときは、テキストボックスにスクリプト内容を直接入力してください。

ライセンス登録前のため、設定できる定義には制限があります。この時点では、導入時のライセンス登録や初期設定を行うためにリモートアクセスするのに必要な最低限の定義および一部の運用管理コマンドだけ設定できます。

参照

IPCOM VE2 スクリプトの書式は、「IPCOMVE2 ユーザーズガイド」の“コンフィグドライブによる設定方法とユーザーデータの書式”を参照してください。

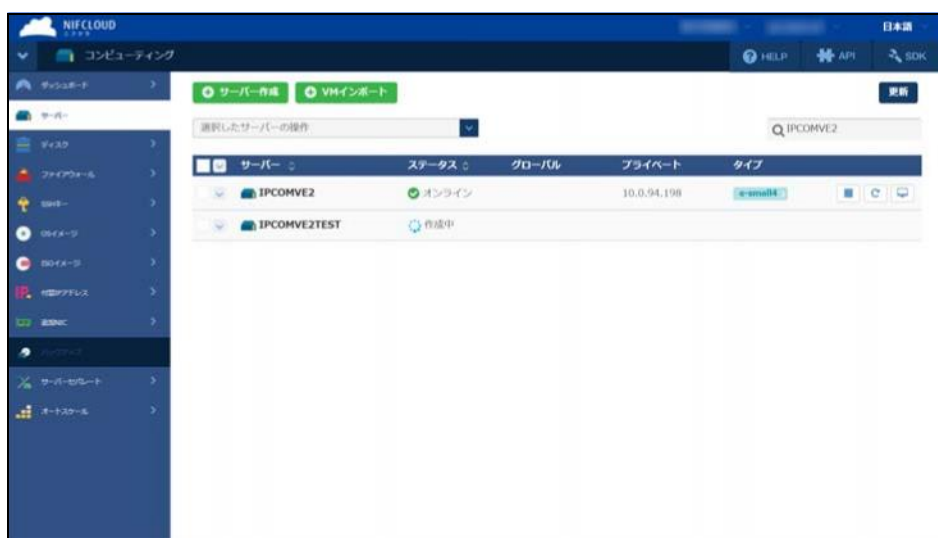
IPCOM VE2 スクリプトの設定項目およびニフクラ固有の注意点は、以下のとおりです。

interface_lanX.Y_addr	DHCP から IP アドレスを取得する場合、auto を設定してください。固定 IP は設定しないでください。
interface_lanX.Y_routers	interface_lanX.Y_addr=auto を指定した場合だけ設定できます。
static_route_addr	必要に応じて、静的ルートを設定してください。
static_route_gateway	必要に応じて、静的ルートを設定してください。
hostname	必要に応じて、ホスト名を設定してください。
admin_password_enable	リモートアクセス有りの構成の場合、セキュリティの観点から必ず設定してください。
admin_password_plain	リモートアクセス有りの構成の場合、セキュリティの観点から必ず設定してください。
admin_remote_login_enable	リモートアクセス有りの構成の場合、yes を設定してください。セキュリティの観点から admin パスワードを必ず設定してください。
time_zone_offset	必要に応じて、タイムゾーンを設定してください。
protect_checksum_inspection_enable	必要に応じて、チェックサム検査を設定してください。

6. 入力情報を確認したあとに、[作成する] ボタンを選択します。



7. サーバー一覧へ戻ります。
作成したサーバーのステータスが、「作成中」から「オンライン」へ遷移するまでお待ちください。



NIFCLOUD

コンピューティング

ヘルプAPISDK

日本語

サーバー作成VMインポート更新

選択したサーバーの操作

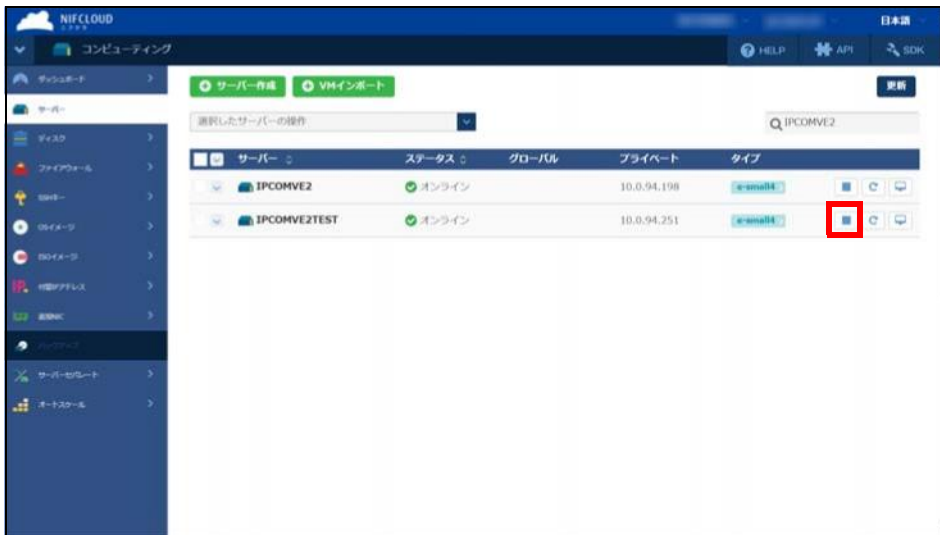
Q IPCOMVE2

サーバー	ステータス	グローバル	プライベート	タイプ
IPCOMVE2	オンライン		10.0.94.198	e-small4
IPCOMVE2TEST	オンライン		10.0.94.251	e-small4

3 - 2 ディスクの追加

ディスクの追加方法について説明します。

1. **サーバーの作成**で作成したサーバーを停止します。
[サーバー停止] ボタンを選択します。

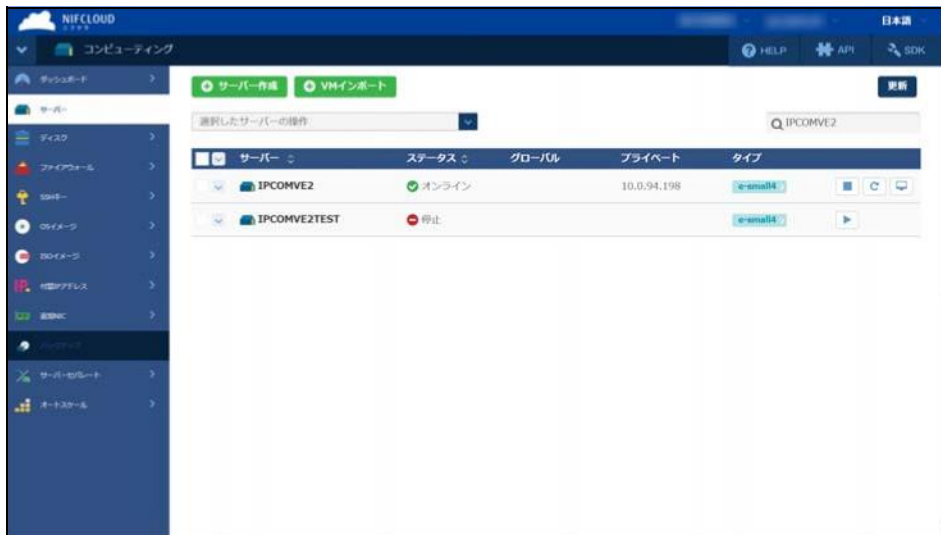


[サーバー停止] ダイアログボックスが表示されます。

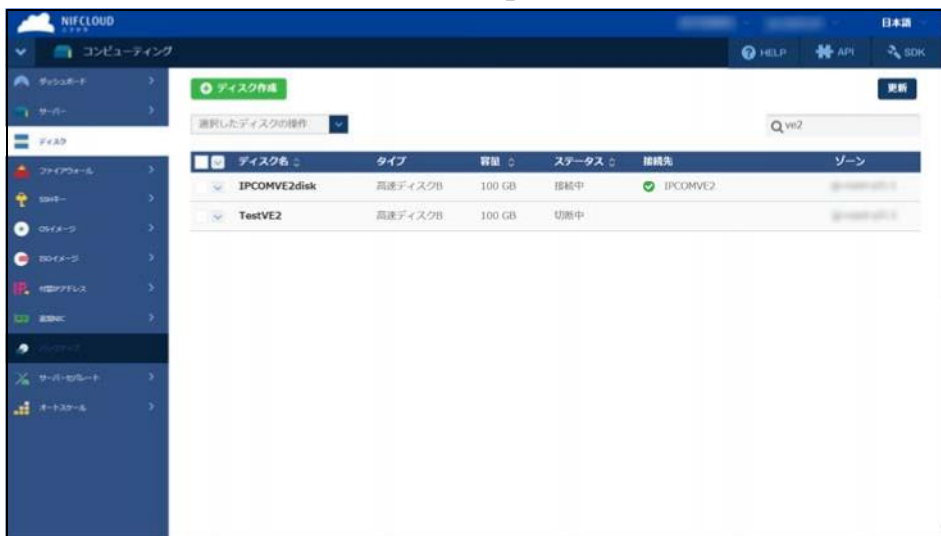
2. [サーバー停止] ダイアログボックスで、[停止する] をチェックして、[OK] ボタンを選択します。



3. サーバー一覧へ戻ります。
停止したサーバーのステータスが、「処理中」から「停止」へ遷移するまでお待ちください。



4. コントロールパネルの左メニューの「ディスク」を選択し、ディスク一覧を表示します。



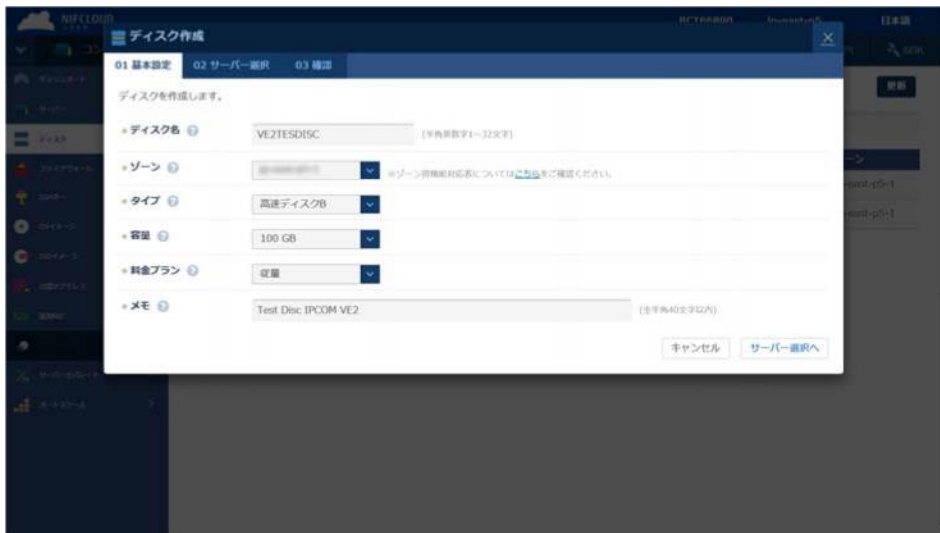
5. 「ディスク作成」ボタンを選択します。

「ディスク作成」ダイアログボックスが表示されます。



6. 「基本設定」タブで、ディスクを作成します。

情報を入力したあとに、「サーバー選択へ」ボタンを選択します。



- ディスク名
任意の名前を入力します。
- ゾーン
サーバーを作成したゾーンを指定します。
- タイプ
ディスクタイプを選択します。
- 容量
ディスク容量を指定します。IPCOM VE2 は「100GB」を指定してください。
- 料金プラン
料金プランを選択します。
- メモ
作成するディスクのメモを入力します。

7. 入力したディスクの情報を確認したあとに、[作成する] ボタンを選択します。



8. 入力したディスクの情報を確認した後に、[作成する] ボタンを選択します。

以下の内容でよろしければ「作成する」ボタンをクリックしてください。

基本設定

ディスク名	VE2TESDISC
ゾーン	ap-northeast-1
タイプ	高速ディスクB
容量	100 GB
料金プラン	従量
メモ	Test Disc IPCOM VE2

基本設定を変更する >

サーバー

サーバー名	タイプ	IPアドレス
IPCOMVE2TEST	ap-northeast-1	

サーバーを変更する >

項目名	単位	数量	小計 (税別)
高速ディスクB 100GB	1台/時	1台	¥1,000/時

※本ページに記載の料金はすべて税別表示価格です。
詳しくは、[料金表の価格表](#)をご覧ください。

戻る キャンセル **作成する**

9. ディスク一覧へ戻ります。

作成したディスクのステータスが「接続中」であることを確認してください。

ディスク名	タイプ	容量	ステータス	接続先	ゾーン
IPCOMVE2disk	高速ディスクB	100 GB	接続中	IPCOMVE2	ap-northeast-1
TestVE2	高速ディスクB	100 GB	切断中		ap-northeast-1
VE2TESDISC	高速ディスクB	100 GB	接続中	IPCOMVE2TEST	ap-northeast-1

3 - 3 NIC の追加

NIC の追加方法について説明します。

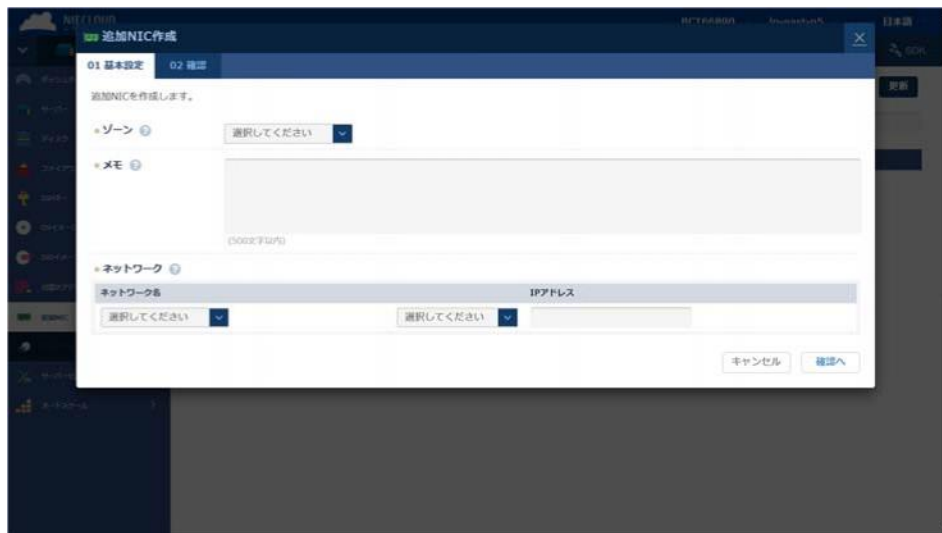
NIC の接続について、以下にご留意ください。

- IPCOM VE2 サーバーの初回起動時に、接続 NIC は lan0.0 から順番に自動で括りつけられます。
- lanX.X は、MAC アドレスで固定化されます。どこかの NIC を切断したときも、自動で lanX.X が前詰めされることはありません。また NIC の追加接続は、lan0.0,lan0.1・・・lan1.0・・・lan1.3 と検索していき、最初の空きポートに接続されます。
- 構成を変更した場合は、IPCOM VE2 コンソール画面から show system resource コマンドを実施して、構成変更後のニフクラ NIC と IPCOM VE2 lanX.X の接続関係を確認してください。

1. コントロールパネルの左メニューの「追加 NIC」を選択し、追加 NIC 一覧を表示します。



2. 「追加 NIC 作成」ボタンを選択します。
追加 NIC 作成ダイアログボックスが表示されます。



3. 「基本設定」タブで追加 NIC を作成します。
情報を入力したあとに、「確認へ」ボタンを選択します。

- ゾーン
サーバーを作成したゾーンを指定します。
- メモ
作成する追加 NIC のメモを入力します。
- ネットワーク
利用する機能・構成により異なります。[構成例](#)の各機能設定例を参照してください。
 - ネットワーク名
作成済みのプライベート LAN から選択します。
 - IP アドレス
「自動割り当て」、「指定する」、「指定しない」から選択します。

4. 入力した追加 NIC の情報を確認したあとに、[作成する] ボタンを選択します。

項目名	単位	数量	小計 (概算)
追加NIC	/月	1	1NIC

- #### 5. 追加 NIC 一覧へ戻ります。
- 作成した追加 NIC のステータスが「利用可能」であることを確認してください。



6. 追加 NIC 一覧から、作成した追加 NIC を選択します。
 左上の「選択した追加 NIC の操作」プルダウンから、「サーバーに設定する」を指定します。



「サーバーに設定する」ダイアログボックスが表示されます。

7. 「サーバー選択」タブで、追加 NIC をサーバーに設定します。
 サーバー一覧から、作成した追加 NIC を設定するサーバーを選択します。
 ディスクの追加の 1. ～ 3. の手順でサーバーは停止しています。サーバーが停止していないときは、同手順でサーバーを停止させてください。
 情報を入力したあとに、「確認へ」ボタンを選択します。



- 再起動方法
「再起動しない」を選択します。

ご注意

「再起動」を選択すると、追加 NIC 設定後にサーバーが自動的に再起動します。サーバーに追加 NIC を複数個設定する場合、ここでは再起動せず、追加 NIC 設定がすべて終了したあとに、サーバーを手動で再起動します。

8. 入力した設定内容を確認したあとに、[サーバーに設定する] ボタンを選択します。



9. 追加 NIC 一覧へ戻ります。 追加 NIC のステータスが「使用中」であることを確認してください。

NIFCLOUD

ニフクラ

BCT66890jp-east-p5日本語

コンピューティングヘルプAPISDK

ダッシュボードサーバーディスクファイアウォールSSMキーOSイメージISOイメージ付帯ソフトウェア監視NIC

サーバー・グループネットワーク

追加NIC作成

更新

選択した追加NICの操作

Q 2/7

NIC ID	ネットワーク名	IPアドレス	ステータス	ゾーン
ni-06xkzj78	private1		使用中	ap-east-1-jp-east-1

3-4 マルチ IP アドレスの追加

マルチ IP アドレスの追加方法について説明します。

マルチ IP アドレスは、複数のグローバル IP アドレスをサーバーへ割り当てることが可能になるサービスです。IPCOM VE2 では、" サーバー 負荷分散 " や " アドレス変換 " の機能で複数のグローバル IP アドレスを設定するときに利用できます。

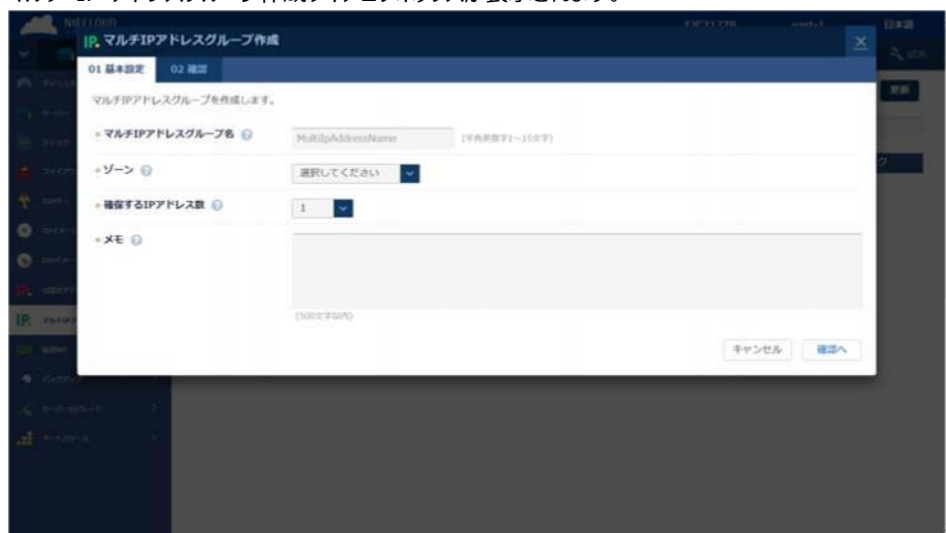
IPCOM VE2 へ複数のグローバル IP アドレスを設定する場合は、以下の手順を実施してください。設定しない場合は、[サーバーの起動](#)の手順を実施してください。

IPCOM VE2 へマルチ IP アドレスを設定する方法は、[マルチ IP アドレスの設定](#)を参照してください。

1. コントロールパネルの左メニューの「マルチ IP アドレス」を選択し、マルチ IP アドレス一覧を表示します。



2. 「マルチ IP アドレスグループ作成」ボタンを選択します。
マルチ IP アドレスグループ作成ダイアログボックスが表示されます。



3. 「基本設定」タブでマルチ IP アドレスグループを作成します。
情報を入力したあとに、「確認へ」ボタンを選択します。

- マルチ IP アドレスグループ名
任意の名前を入力します。
- ゾーン
サーバーを作成したゾーンを指定します。
- 確保する IP アドレス数
確保する IP アドレス数を指定します。
- メモ
任意のメモを入力します。

4. 入力したマルチ IP アドレスグループの情報を確認したあとに、[作成する] ボタンを選択します。

項目名	単価	数量	小計(税別)
マルチIPアドレス	¥1/月	2IPアドレス	¥2/月

5. マルチ IP アドレスグループ一覧へ戻ります。

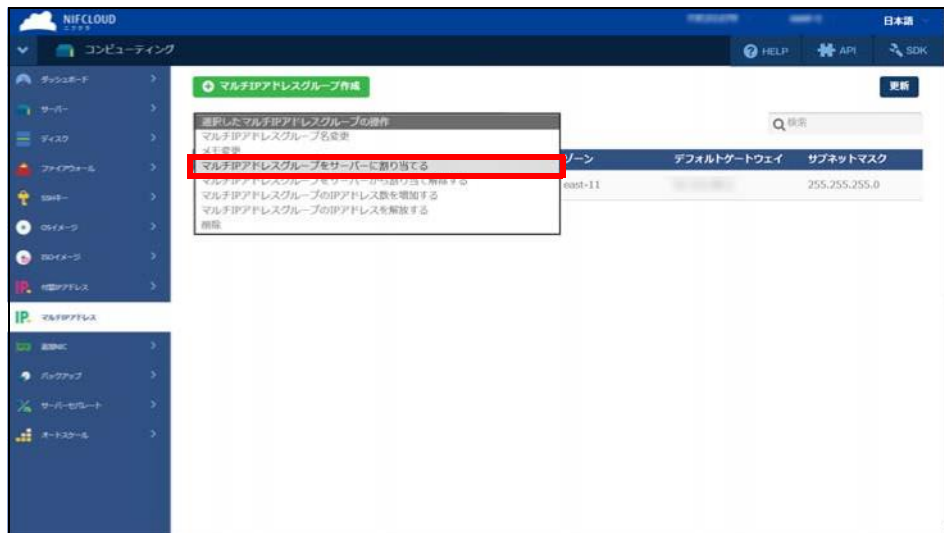
作成したマルチ IP アドレスグループのステータスが「利用可能」であることを確認してください。



6. マルチ IP アドレスグループ一覧から、作成したマルチ IP アドレスグループを選択します。

※**IPCOM が起動している場合は停止させてください。**

左上の「選択したマルチ IP アドレスグループの操作」プルダウンから、「マルチ IP アドレスグループをサーバーに割り当てる」を指定します。



「マルチ IP アドレスグループをサーバーに割り当てる」ダイアログボックスが表示されます。

7. 「サーバー選択」タブで、マルチ IP アドレスグループをサーバーに割り当てます。

サーバー一覧から、作成したマルチ IP アドレスグループを割り当てるサーバーを選択します。

ディスクの追加の 1. ～ 3. の手順でサーバーは停止しています。

情報を入力したあとに、「確認へ」ボタンを選択します。



● 再起動方法

「再起動しない」を選択します。

ご注意

「再起動」を選択すると、マルチ IP アドレスグループ割り当て後にサーバーが自動的に再起動します。
ここでは再起動せず、サーバーの設定がすべて終了したあとに、サーバーを手動で再起動します。

8. 入力した設定内容を確認したあとに、[サーバーに割り当てる] ボタンを選択します。



9. マルチ IP アドレスグループ一覧へ戻ります。

マルチ IP アドレスグループのステータスが「利用可能」であることを確認してください。

VEZESTESTMULTIIP

マルチIPアドレスグループ作成

ヘルプ

API

SDK

日本語

コンピューティング

マルチIPアドレス

仮想マシン

パブリックIP

プライベートIP

ネットワーク

ストレージ

データベース

セキュリティ

監視

開発者ツール

ドキュメント

お問い合わせ

選択したマルチIPアドレスグループの操作

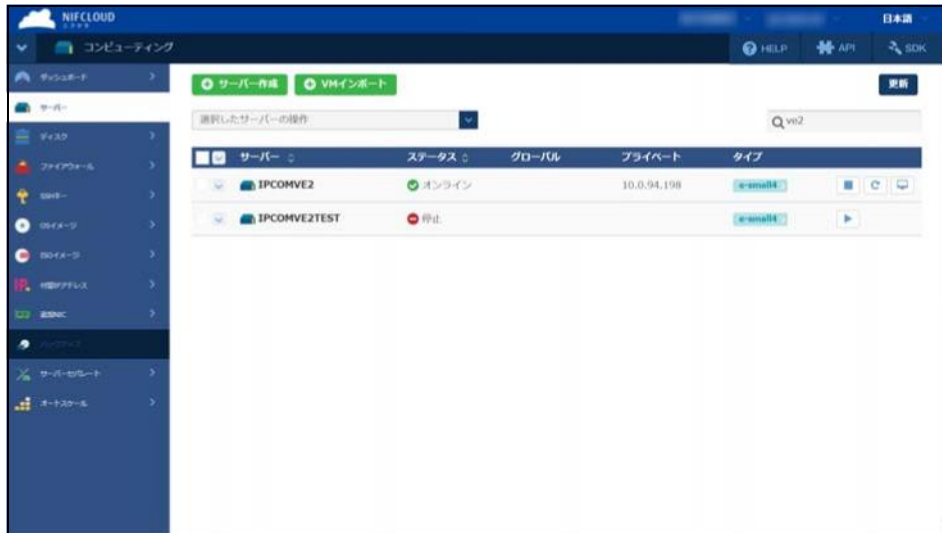
検索

マルチIPアドレスグループ名	ステータス	ゾーン	デフォルトゲートウェイ	サブネットマスク
VEZESTESTMULTIIP	利用可能	us-east-1a	10.0.0.1	255.255.255.0

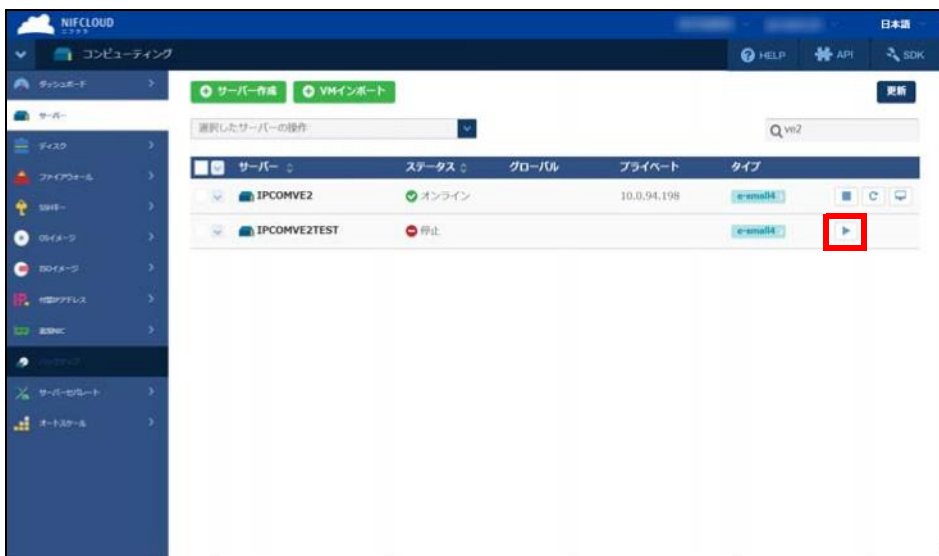
3 - 5 サーバーの起動

サーバーの起動方法について説明します。

1. コントロールパネルの左メニューの「サーバー」を選択し、サーバー一覧を表示します。
サーバーのステータスが、「処理中」から「停止」へ遷移するまでお待ちください。



2. サーバー一覧からサーバーの起動を実行します。
[サーバー起動] ボタンを選択します。



[サーバー起動] ダイアログボックスが表示されます。

3. [サーバー起動] ダイアログボックスで、情報を入力したあとに [起動する] をチェックして、[OK] ボタンを選択します。



● スクリプト

使用の有無を選択します。

IPCOM VE2 スクリプトの使用方法は「IPCOM VE2 ユーザーガイド」の「コンフィグド」ライブによる設定を参照してください。



スクリプトを「使用する」を選択したときは、以下を指定してください。

– 事前にスクリプトをファイルで準備しているときは、そのスクリプトファイルを指定してください。

- Base64 でエンコードされたスクリプトファイルを使用するときは、[Base64 でエンコードされたスクリプトを使用する] をチェックします。
- [参照] ボタンを選択して、スクリプトファイルを指定します。

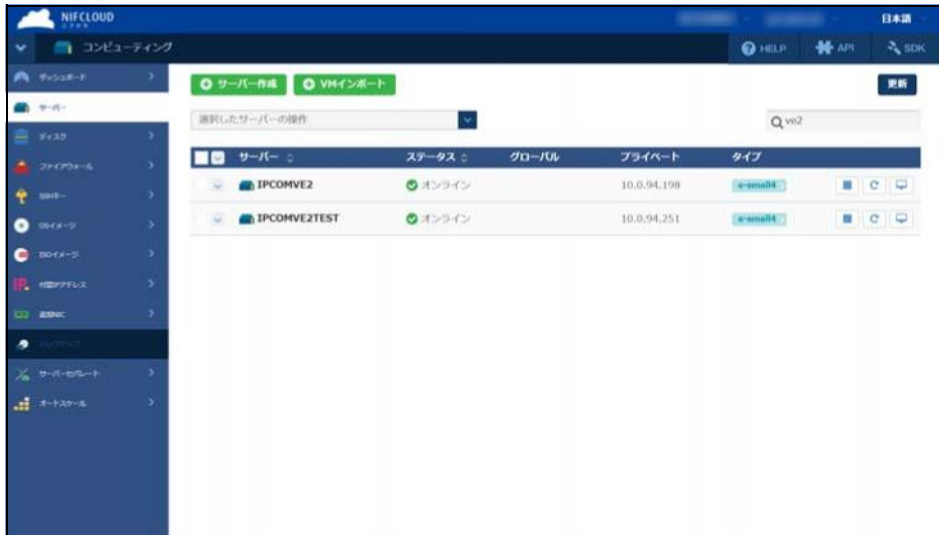
– スクリプトをファイルで準備していないときは、テキストボックスにスクリプト内容を直接入力してください。

参照

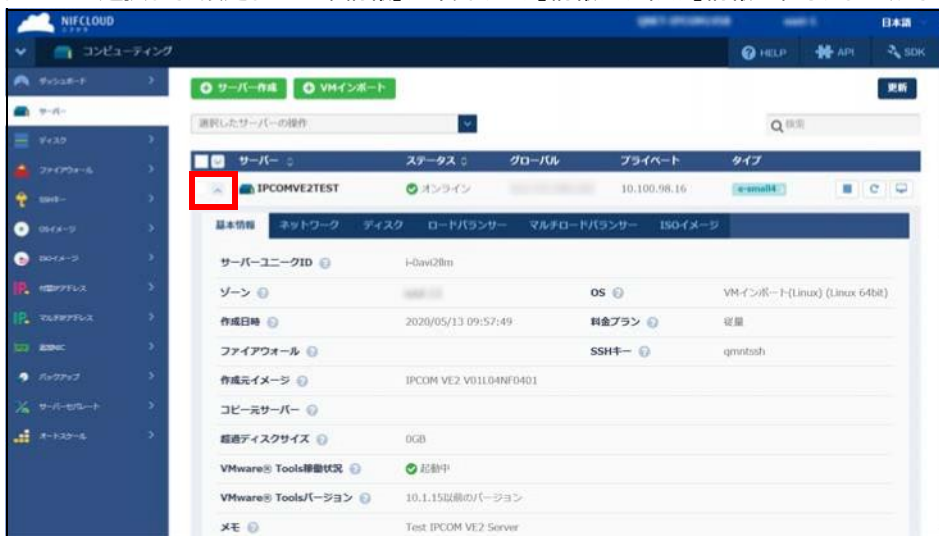
IPCOM VE2 スクリプトの書式は、「IPCOM」

4. サーバー一覧へ戻ります。

起動したサーバーのステータスが、「処理中」から「オンライン」へ遷移するまでお待ちください。



サーバーを選択して、設定した「基本情報」、「ネットワーク」情報、「ディスク」情報を確認することができます。



NIFCLOUD

日本語

ヘルプ API SDK

コンピューティング

サーバー作成 VMインポート

更新

選択したサーバーの操作

サーバー ステータス グローバル プライベート タイプ

IPCOMVE2TEST オンライン 10.0.94.251 e-small4

基本情報 ネットワーク ディスク ロードバランサー マルチロードバランサー ISOイメージ

ネットワーク名	IPアドレス	MACアドレス	NIC ID
高速ネットワーク	10.0.94.251	00:50:56:b3:36:3b	
private1		00:50:56:b3:8e:79	ni-0r16fw80

サーバー

ディスク

ファイアウォール

ロードバランサー

OSイメージ

ISOイメージ

付随ソフトウェア

監視

バックアップ

サーバーセキュリティ

オートスケーリング

NIFCLOUD

日本語

ヘルプ API SDK

コンピューティング

サーバー作成 VMインポート

更新

選択したサーバーの操作

サーバー ステータス グローバル プライベート タイプ

IPCOMVE2TEST オンライン 10.0.94.251 e-small4

基本情報 ネットワーク ディスク ロードバランサー マルチロードバランサー ISOイメージ

ディスク名	タイプ	容量	ディスク接続日時
VE2TESDISC	高速ディスクB	100GB	2020/01/24 15:25:47

サーバー

ディスク

ファイアウォール

ロードバランサー

OSイメージ

ISOイメージ

付随ソフトウェア

監視

バックアップ

サーバーセキュリティ

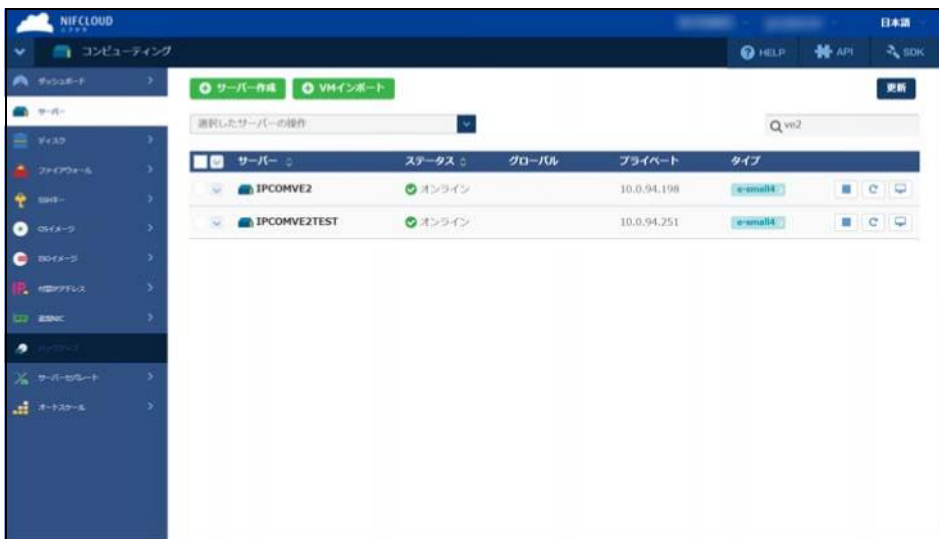
オートスケーリング

4 IPCOM VE2 の ライセンス登録

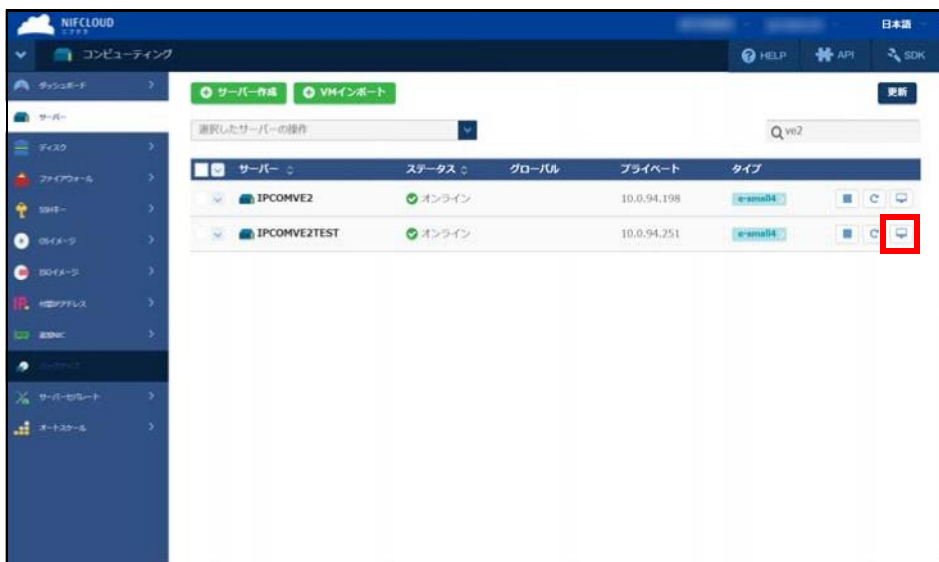
4 - 1 IPCOM VE2 のライセンス登録

IPCOM VE2 のライセンスを登録する方法について説明します。

1. コントロールパネルの左メニューの「サーバー」を選択し、サーバー一覧を表示します。



2. ライセンスを登録するサーバーの「コンソール起動」ボタンを選択します。



[コンソール]ダイアログボックスが表示されます。

3. [コンソール] ダイアログボックスで、[ブラウザから接続する] ボタンを選択します。

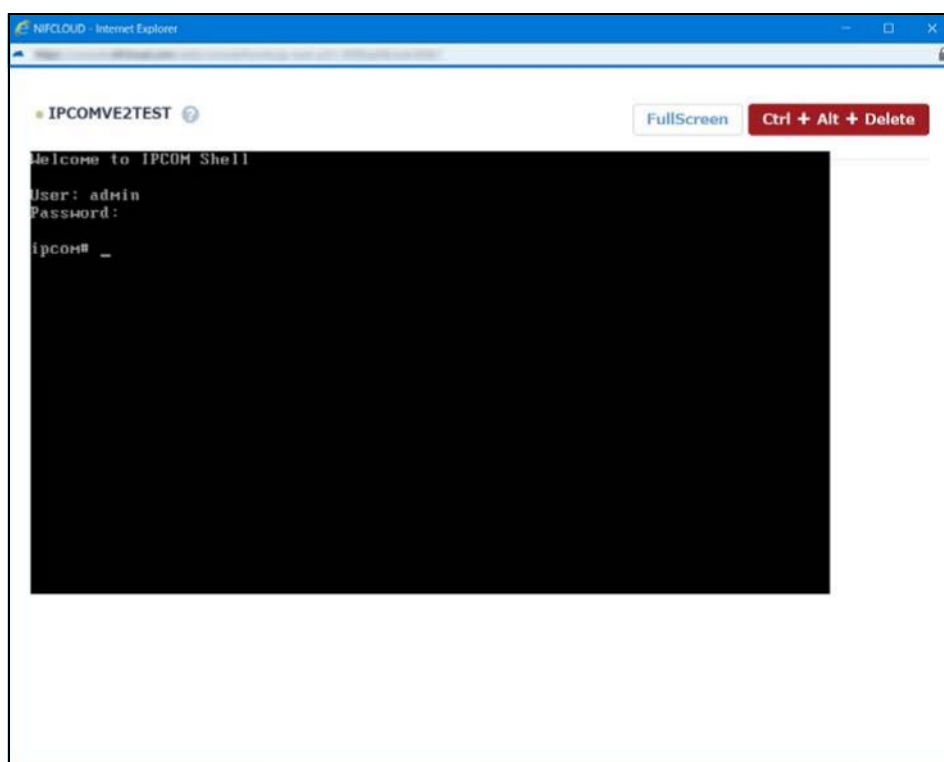


コンソール画面が表示されます。

4. admin ユーザーでログインします。

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 [Enter] キーを押してください。

スクリプトで admin パスワードを設定している場合は、そのパスワードを入力し、ログインしてください。



5. license key コマンドで、IPCOM VE2 導入ライセンスを登録します。

```
ipcom# license key <ライセンスキー>
```

6. IPCOM VE2 を再起動します。

IPCOM VE2 導入ライセンスが反映されます。

再起動 (reset:r) または停止 (power off:p) を選択してください。

停止を選択したときは、コントロールパネルから IPCOM VE2 起動を実施してください。

The license "VE2-100 LS Software License" is registered.

After registering the license, the system will shutdown to activation.

Are you sure?(y:[n]):y

Please select either reset or power off.(r:p): r

<INFO> Wait for a moment until restarting this system.

ipcom#

ご注意

再起動時に追加ディスクが初期化されます。初期化には数分かかりますので、ご注意ください。

Starting HDD format

.....

Finish HDD format Completely.

5 IPCOM VE2 の設定

5 - 1 ホスト名とパスワードの設定

ホスト名とパスワードを設定する方法について説明します。

IPCOM VE2 のコンソールへログインして、ホスト名とパスワードを設定します。

サーバー作成時にスクリプトで「admin_remote_login_enable=yes」と設定した場合も、セキュリティの観点から、ライセンス登録後に admin パスワードを変更することを推奨します。

ご注意

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

1. IPOM VE2 のコンソール画面で、configure コマンドを実行します。

実行例

```
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-ve2 ..... 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. 任意のパスワードを設定します。
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 文字以上で、英数字記号が混在した文字列を推奨）。
2. 任意のホスト名を設定します。
3. パスワードを設定したので、admin ユーザーのリモートアクセスを許可します。

5 - 2 IPCOM VE2 への SSH 接続

IPCOM VE2 へ SSH 接続する方法について説明します。

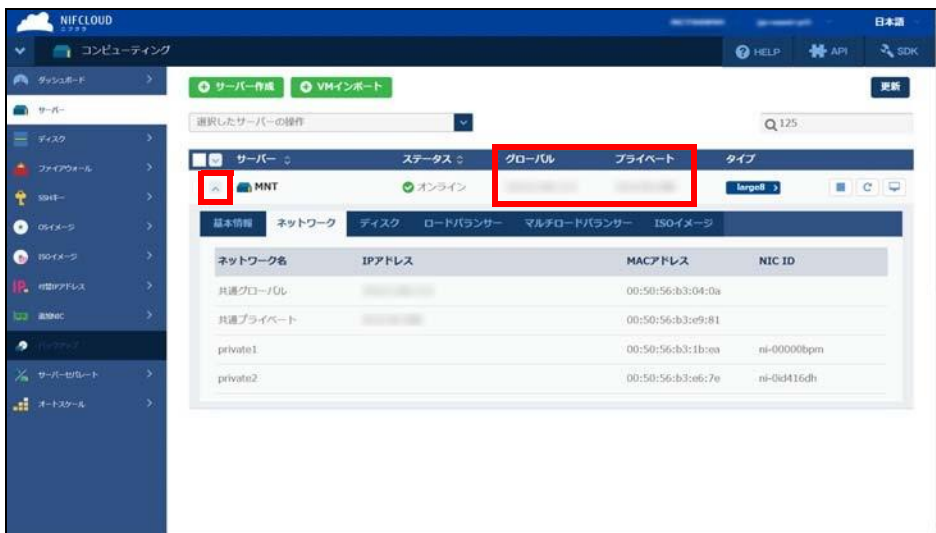
IPCOM VE2 へ SSH 接続します。

TeraTerm などのターミナルソフト（SSH クライアント）を利用して、IPCOM VE2 にログインします。

1. コントロールパネルの左メニューの「サーバー」を選択し、サーバー一覧を表示します。

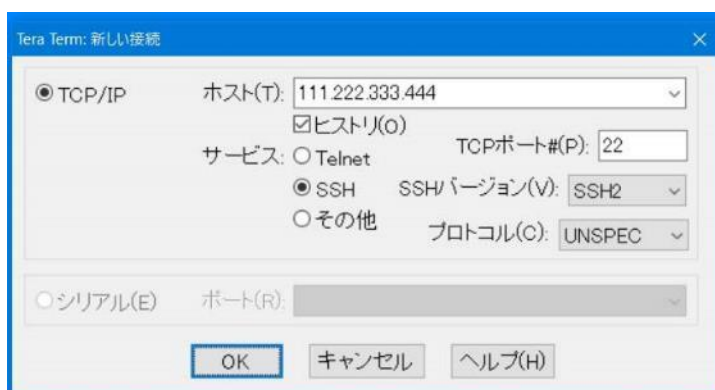
サーバー一覧から、SSH 接続するサーバーの IP アドレスを確認します。

[サーバーの作成](#)の 5. の手順で設定した、グローバルネットワーク、プライベートネットワークの IP アドレスが表示されます。



サーバーの「詳細ボタン」を選択して、設定した「ネットワーク」情報を確認することができます。

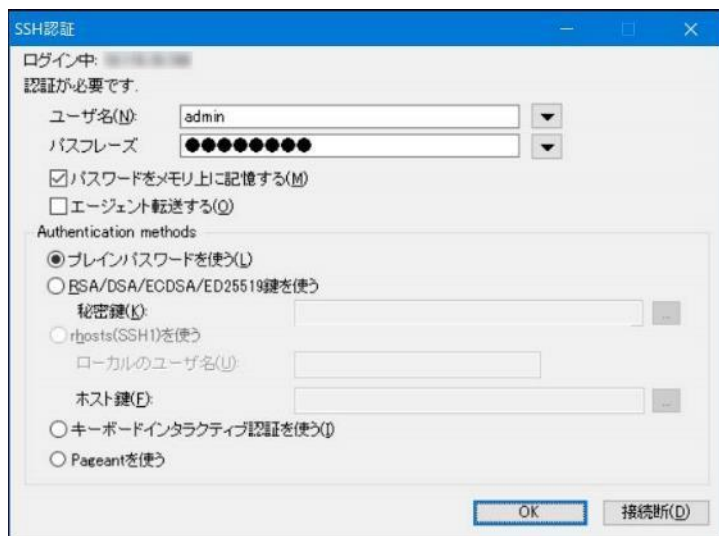
2. TeraTerm を起動し、以下の情報を入力して、[OK] ボタンを選択します。



- ホスト : IPCOM VE2 の IP アドレス（プライベート IP アドレスでの SSH 接続を推奨します）
- TCP ポート # : 22
- サービス : SSH
- SSH バージョン : SSH2

SSH 認証画面が表示されます。

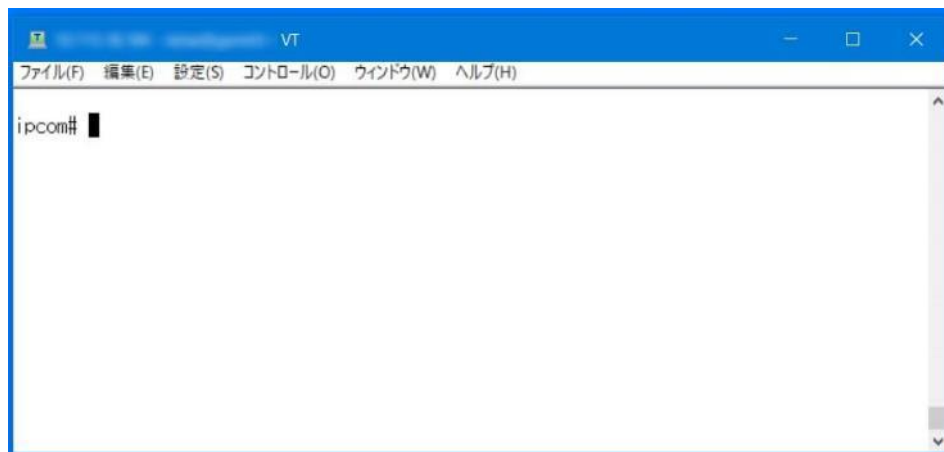
3. SSH 認証画面で、以下の内容を入力して、[OK] ボタンを選択します。



SSH認証画面のスクリーンショット。タイトルバーには「SSH認証」とあり、標準的なWindowsウィンドウの操作ボタン（最小化、最大化、閉じる）が右側に配置されている。ウィンドウ内は「ログイン中:」というステータスと「認証が必要です。」というメッセージで始まる。ユーザー名(N)の入力欄には「admin」が入力されている。パスワード(P)の入力欄には黒い丸が10個表示されている。その下には「パスワードをメモリ上に記憶する(M)」というチェックボックスがオンになっている。さらに「エージェント転送する(O)」というオプションのチェックボックスがある。次に「Authentication methods」のセクションがあり、ここでは「ブレインパスワードを使う(L)」が選択されている。他のオプションには「RSA/DSA/ECDSA/ED25519鍵を使う」、「rhosts(SSH1)を使う」、「ローカルのユーザー名(U)」、「ホスト鍵(F)」、「キーボードインタラクティブ認証を使う(I)」、および「Pageantを使う」がある。画面の右下には「OK」と「接続断(D)」のボタンが配置されている。

- ユーザー名: admin
- パスフレーズ : 設定した admin パスワード
- Authentication methods :「ブレインパスワードを使う」を選択

IPCOM VE2 にログインします。



SSH 接続時の注意点

ライセンス登録前に保守用の仮想マシンなどから IPCOM VE2 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マシンから SSH ログインすると、セキュリティ警告のメッセージが表示されます。これは、ライセンス登録前とライセンス登録後とで、IPCOM VE2 のホスト鍵が変更されることによる現象です。セキュリティ上の問題ではありませんので、以降の対処を実施してください。

Linux 環境の場合

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@localhost user]# 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.

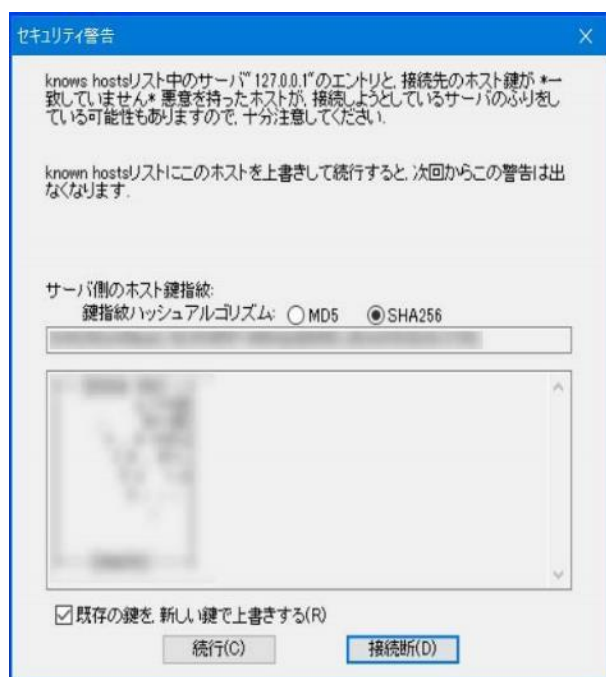
Please contact your system administrator.

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.
```

Windows 環境の場合

本警告画面が表示された場合、[既存の鍵を , 新しい鍵で上書きする] をチェックし、[続行] ボタンを選択してください。

表示例



5 - 3 マルチ IP アドレスの設定

マルチ IP アドレスを設定する方法について説明します。

IPCOM VE2 へ複数のグローバル IP アドレスを設定する場合は、以下の手順を実施してください。

IPCOM VE2 へは、[マルチ IP アドレスの追加](#)の手順で、マルチ IP アドレスグループを割り当てておいてください。

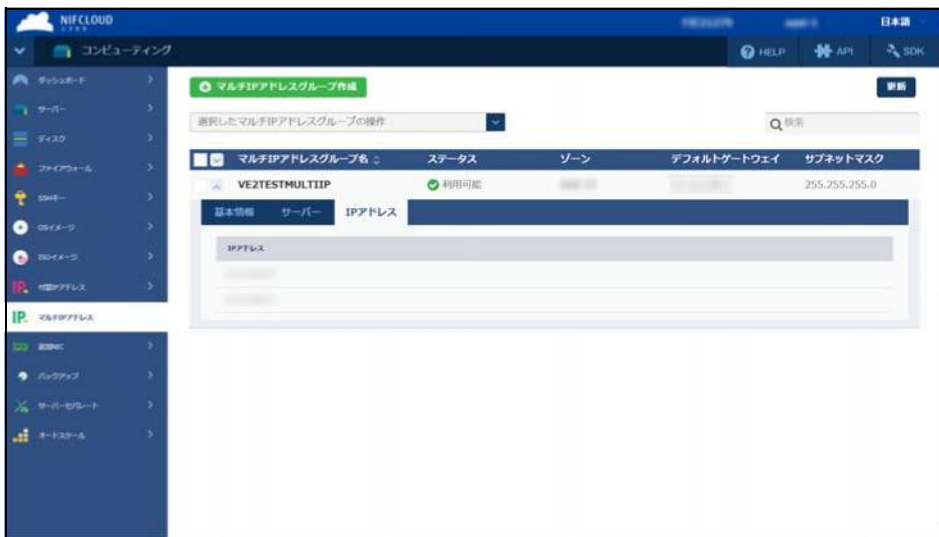
ご注意

- 共通グローバルネットワークに接続されていないサーバーに、マルチ IP アドレスグループを割り当てることはできません。
マルチ IP アドレスを利用する IPCOM VE2 は、グローバルネットワークに「自動割り当て」を指定して作成してください。
- IPCOM VE2 サーバーで利用中であったグローバル IP アドレスは、
マルチ IP アドレスグループの割り当てとともに利用できなくなります。

1. コントロールパネルの左メニューの「マルチ IP アドレス」を選択し、マルチ IP アドレスグループ一覧を表示します。

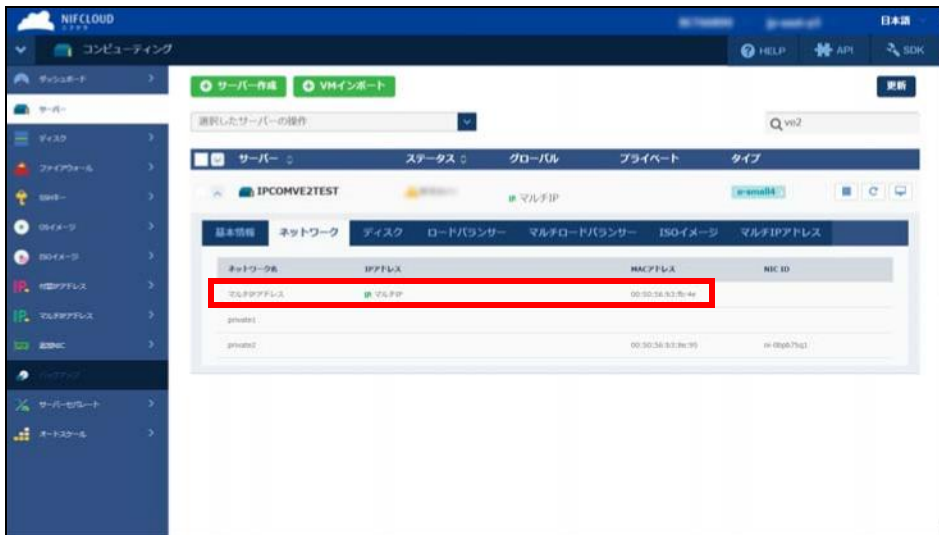
IPCOM VE2 へ割り当てているマルチ IP アドレスグループの「デフォルトゲートウェイ」、「サブネットマスク」を確認します。

マルチ IP アドレスグループの「詳細ボタン」を選択して、割り当てられた「IP アドレス」一覧を確認します。



2. コントロールパネルの左メニューの「サーバー」を選択し、サーバー一覧を表示します。

IPCOM VE2 サーバーの「詳細ボタン」を選択して、マルチ IP アドレス「ネットワーク」情報から MAC アドレスを確認します。



3. IPCOM VE2 へログインします。

プライベートネットワーク側から、またはコンソール画面からログインします。

4. IPCOM VE2 のマルチ IP アドレスが割り当たっているインターフェースを確認します。

show system resource コマンドを実行します。

実行例

```
ipcom# show system resource
CPU          : 1
Memory       : 3949MB
HDD          : NO_PRESENT
Cipher Card  : NO_PRESENT
lan0.0
  driver : vmxnet3
  MAC address: 00:50:56:B3:FB:4E
lan0.1
  driver : vmxnet3
  MAC address: 00:50:56:B3:8E:95
```

2. の MAC アドレスと一致するインターフェースが、マルチ IP アドレスが割り当たっているインターフェースです。

5. IPCOM VE2 へマルチ IP アドレスを静的に割り当てる設定をします。

設定するマルチ IP アドレスは、1. の IP アドレス一覧から任意に選択します。

実際の構成定義設定例は、[インライン（ファイアーウォール/アドレス変換）](#) と [インライン（SSL アクセラレーター/サーバー負荷分散）](#) を参照してください。

5 - 4 IPCOM VE2 への WEB コンソール接続

IPCOM VE2 へ WEB ブラウザを使ってログインする方法について説明します。

1. IPCOM VE2 の IP アドレスを確認してブラウザに入力します。

IPCOM VE2 への SSH 接続 と同様に IPCOM のグローバルネットワークまたはプライベートネットワークの IP アドレスを確認して、アドレス欄に、[https://IP アドレス:82](https://IPアドレス:82) を入力して IPCOM にアクセスします。

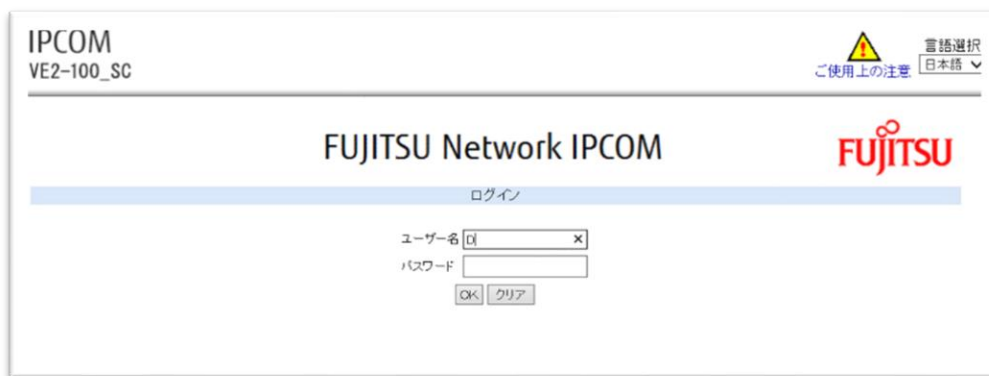
※ニフクラ FW を使っている場合はポート 82/tcp を許可してください。

※ブラウザは Microsoft Edge の Internet Explorer モードをお使いください。

2. 認証情報を入力して認証します。

ユーザー名とパスワードを入力して OK ボタンを押して認証します。

- ユーザー名: admin
- パスフレーズ : 設定した admin パスワード



3. 下記画像が出てくれば WEB コンソールへのログイン完了です。

運用・保守メニュー

- 運用
 - システム状態
 - ダウンロード版モニタ
 - モニタ
 - ライセンス管理
 - 証明書管理
 - シグネチャ型IPS管理
 - アンチウィルス管理
 - アプリケーション辞書管理
 - 国/地域別IPアドレスリスト管理
 - ログインセッション管理
 - コンソール用証明書管理
 - 疎通確認
 - 二重化切り替え
 - 装置の停止・再起動
- 保守
 - 退避と復元
 - ファームウェアの更新
 - メンテナンス情報の採取

システム状態

システム稼働状態

現在日時	2022/01/31(Mon) 15:21:24	設定...
装置起動日時	2021/11/26(Fri)14:56:41	
システム名	IPCOM VE2-100_SC	
装置ID	00VE2100SC####NB75701C01 ##MG110011210001	
ソフトウェアID	00VE2100SC####NB75701C01 ##MG110011210001	
ホスト名	ipcom11	
ファームウェア版数	V01L04 NF0401 B01	
アップグレード 予約中の版数	-	
バックアップ 可能な版数	-	
Startup-config作成日時	2021/12/01(Wed)18:10:14	
Running-config作成日時	2021/12/01(Wed)18:10:14	
CPU使用率	0%	
メモリ使用率	38%	
温度状態	-	
電源状態	-	
消費電力	現在値: - 最大値: -	
装置二重化 状態	装置二重化は定義されていません。	

ネットワーク稼働状態

インターフェース	タイプ	リンク	GW監視
lan0.0	10gigabit ethernet	linkup	-
lan0.1	10gigabit ethernet	linkup	-

オプション構成

リソース割り当て状態

CPU	1
メモリ	3949MB
HDD	あり
HDDサイズ	100GB
拡張カード	なし

登録済みライセンス

The license VE2-100 SC Software License (valid:2022/09/17)
--

ログ情報

エラーログ	最終: 2021-11-26 14:56:39	表示...
メッセージログ	最終: 2022-01-26 11:31:51	表示...

表示の更新

ポーリング間隔 30 秒(初期値)

6 留意事項

6 - 1 初期定義について

初期定義の留意事項について説明します。

本製品の初期定義は、lan0.0、lan0.1 が DHCP で IP アドレスを取得、リモート接続不可の定義になっています。本製品のすべてのシリーズで共通です。

```
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
access-map mng-lan-connection inbound
    rule 10 mng-in-telnet any any telnet
        action accept audit-normal
    !
    rule 20 mng-in-ssh any any ssh
        action accept audit-normal
    !
    rule 30 mng-in-webconsole any any tcp any 82
        action accept audit-normal
    !
    rule 50 mng-in-dhcp-client any any udp any 68
        action accept audit-normal
    !
!
access-control default-deny inbound
access-control audit session-normal match-normal
access-control configuration access-map
protect checksum-inspection enable audit-normal
protect small-ip-frg detect-only audit-normal min-size 400
interface-group mng
    access-map mng-lan-connection
    interface lan0.0
    interface lan0.1
!
```

```
interface lan0.0
    ip address auto
!
interface lan0.1
    ip address auto
!
class-map match-all any
    match any
!
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"
!
user-role user
    description "Default user role"
    display-name "IPCOM operators"
!
user admin authentication pap
    description "Default user"
    display-name "IPCOM administrator"
!
```

ご注意

コンフィグドライブ利用時は、その設定に基づいた定義となります。

詳細は [コンフィグドライブの留意事項](#) を参照してください。

6 - 2 コンフィグドライブの留意事項

コンフィグドライブの留意事項について説明します。

本製品がニフクラ上で動作する際に、コンフィグドライブで値を指定しなかった場合の省略値が、「VE2 ユーザーズガイド」に記載の値と異なる設定項目があります。

なお、本書に記載のない設定項目に関しては同じ省略値ですので、「VE2 ユーザーズガイド」の " コンフィグドライブによる設定 " を参照してください。

IP アドレス

定義	パラメーター	省略値	対応する IPCOM コマンド
iinterface_lanX.Y_addr	{ <A.B.C.D/M> auto }	auto (lan0.0 および lan0.1)	ip address

※ lan0.0 および lan0.1 の定義が省略された場合は auto が設定されますが、その他の lan の定義が省略された場合は設定されません。

admin ユーザーのリモートアクセス可否

定義	パラメーター	省略値	対応する IPCOM コマンド
admin_remote_login_enable	{ yes no }	no	match user admin (user-role remote)

7 構成例

7-1 インターネット公開

インターネット環境から共通グローバルネットワーク経由でニフクラへ接続する構成について説明します。

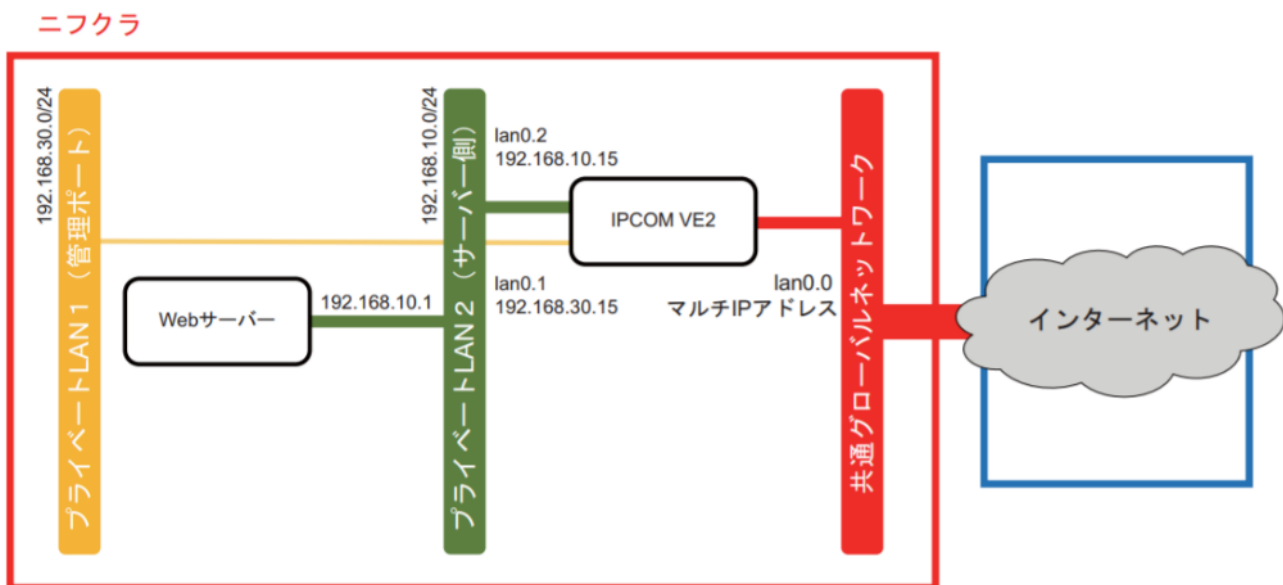
7-1-1 インライン（ファイアーウォール/アドレス変換）

構成例の概要

IPCOM VE2 を、インターネット環境と Web サーバーを配置するプライベート LAN との間に位置します。マルチ IP アドレスを利用して、インターネット側に 2 個のグローバル IP アドレスを設定します。

以下の構成例は、ファイアーウォール機能により、特定のサーバー / サービスへのアクセスだけを許可します。また、アドレス変換機能により、パケットヘッダーに含まれる IP アドレス・ポート番号を、別の IP アドレス・ポート番号へ変換します。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は以下の通りです。

共通グローバル	割り当てられたマルチ IP アドレス(10.0.0.11/24、10.0.0.12/24)を設定
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.10.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (インターネット側)	10.0.0.11/255.255.255.0 (割り当てられたマルチ IP アドレス)
LAN0.1 の IP アドレスとサブネットマスク値 (管理ポート)	192.168.30.15/255.255.255.0
LAN0.2 の IP アドレスとサブネットマスク値 (サーバー側)	192.168.10.15/255.255.255.0

- 共通グローバルネットワーク→プライベート LAN で許可するフィルター条件は、以下のとおりです。

接続元 IP	接続先 IP	接続先ポート	アクション
共通グローバルネットワーク	10.0.0.11 (割り当てられたマルチ IP アドレス)	80/tcp,443/tcp	透過

- 共通グローバルネットワーク→プライベート LAN に対するアドレス変換条件は、以下のとおりです。

変換元 IP ・ポート番号	変換先 IP ・ポート番号
10.0.0.12:80 (割り当てられたマルチ IP アドレス)	192.168.10.1 : 80

IPCOM VE2 構成定義例

【IPCOM VE2 のインターフェースに関する定義】

```
# インターネット側の本装置の IP アドレス定義
ipcom(edit)# interface lan0.0
ipcom(edit-if)# ip address 10.0.0.11 255.255.255.0
ipcom(edit-if)# ip-routing
ipcom(edit-if)# exit

# サーバー側の本装置の IP アドレス定義
ipcom(edit)# interface lan0.2
ipcom(edit-if)# ip address 192.168.10.15 255.255.255.0
ipcom(edit-if)# ip-routing
ipcom(edit-if)# exit

# ファイアウォールのデフォルト動作モードの変更
ipcom(edit)# access-control default-deny

# マルチ IP アドレスグループのデフォルトゲートウェイの設定
ipcom(edit)# ip route 0.0.0.0/0 10.0.0.1
```

【IPCOM VE2 のアクセス制御に関する定義】

```
# アクセス制御ルール定義を有効に設定
ipcom(edit)# no access-map mng-lan-connection inbound
ipcom(edit)# no interface-group mng
ipcom(edit)# access-control configuration rule-access
```

【インターネット側のパケット透過ルールの定義】

フィルター条件の定義

ipcom(edit)# class-map match-all client-side

ipcom(edit-cmap)# match port 80/tcp,443/tcp

ipcom(edit-cmap)# exit

ファイアーウォールの定義

ipcom(edit)# interface lan0.0

ipcom(edit-if)# rule access 10 in client-side accept

ipcom(edit-if)# rule access 10 out client-side accept

ipcom(edit-if)# exit

【サーバー側のパケット透過ルールの定義】

フィルター条件の定義

ipcom(edit)# class-map match-all any

ipcom(edit-cmap)# match any

ipcom(edit-cmap)# exit

制限なし

ipcom(edit)# interface lan0.2

ipcom(edit-if)# rule access 1 in any accept

ipcom(edit-if)# rule access 1 out any accept

ipcom(edit-if)# exit

【インターネット側のアドレス変換の定義】

アドレス変換の定義

ipcom(edit)# interface lan0.0

ipcom(edit-if)# rule dst-napt 10 ipv4 10.0.0.12 80 tcp to 192.168.10.1 80

ipcom(edit-if)# exit

Web サーバーの定義

デフォルトゲートウェイの設定を、IPCOM VE2 のサーバー側インターフェース
(192.168.10.15/24) にします。

7-1-2 インライン（SSL アクセラレーター/ サーバー負荷分散）

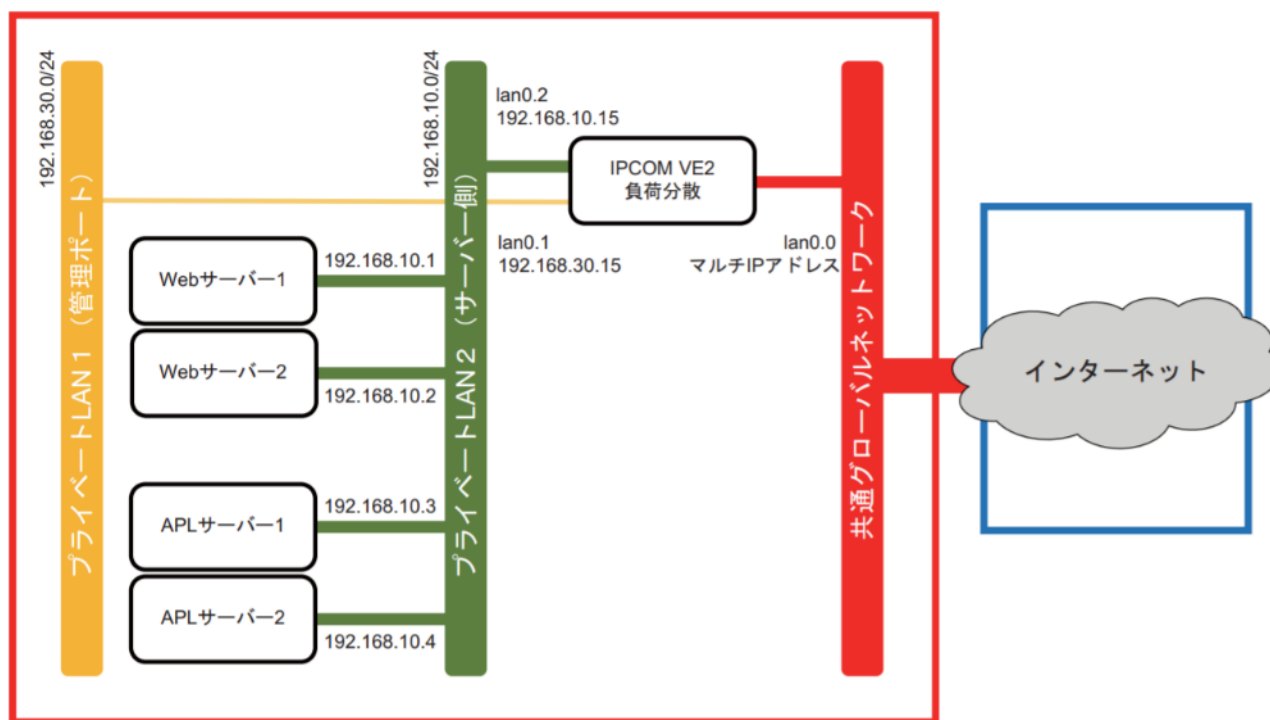
構成例の概要

インターネット上のクライアントからの SSL 通信を、背後の Web サーバーに負荷分散します。また、Web サーバーと APL サーバーを同一サブネットのプライベート LAN 上に配置して、Web サーバーから APL サーバーへの通信に対して、APL サーバーの負荷分散を行います。

マルチ IP アドレスで、インターネット側に 2 個のグローバル IP アドレスを設定します。

ニフクラ/PCOM VE2 構成図

ニフクラ



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	割り当てられたマルチ IP アドレス(10.0.0.11/24、10.0.0.12/24)を設定
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.10.0/24)を設定

PCOM VE2 設定条件

- PCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (インターネット側)	10.0.0.11/255.255.255.0 (割り当てられたマルチ IP アドレス)
LAN0.1 の IP アドレスとサブネットマスク値	192.168.30.15/255.255.255.0

(管理ポート)	
LAN0.2 の IP アドレスとサブネットマスク値 (サーバー側)	192.168.10.15/255.255.255.0

- 分散対象となる Web サーバーは、以下のとおりです。

分散対象サーバーの IP : ポート番号	分散対象サーバー1 192.168.10.1 : 80 分散対象サーバー2 192.168.10.2 : 80
仮想 IP アドレス : 仮想ポート番号	10.0.0.12:443 (割り当てられたマルチ IP アドレス)

- 分散対象となる Web サーバーおよび負荷分散機能の設定条件は、以下のとおりです。

パケットの転送方式	IP アドレス変換
応答経路	通過型配置
分散方法	最小コネクション数
分散の単位	ノード単位
監視パケット送信間隔	60 秒間隔
監視パケット応答待ち時間	10 秒
監視パケットリトライ回数	3 回

- 分散対象となる APL サーバーは、以下のとおりです。

分散対象サーバーの IP : ポート番号	分散対象サーバー1 192.168.10.3 : 80 分散対象サーバー2 192.168.10.4 : 80
仮想 IP アドレス : 仮想ポート番号	192.168.10.100 : 80

- 分散対象となる APL サーバーおよび負荷分散機能の設定条件は、以下のとおりです。

パケットの転送方式	MAC アドレス変換
応答経路	応答経路並列型配置
分散方法	最小コネクション数
分散の単位	ノード単位
監視パケット送信間隔	60 秒間隔
監視パケット応答待ち時間	10 秒
監視パケットリトライ回数	3 回

IPCOM VE2 構成定義例

【IPCOM VE2 のインターフェースに関する定義】

インターネット側の本装置の IP アドレス定義

```
ipcom(edit)# interface lan0.0
```

```
ipcom(edit-if)# ip address 10.0.0.11 255.255.255.0
```

```
ipcom(edit-if)# ip-routing
```

```
ipcom(edit-if)# exit
```

```
ipcom(edit)# interface-group mng
ipcom(edit-if-grp)# no interface lan0.0
ipcom(edit-if-grp)# exit
# サーバ側の本装置の IP アドレス定義
ipcom(edit)# interface lan0.2
ipcom(edit-if)# ip address 192.168.10.15 255.255.255.0
ipcom(edit-if)# ip-routing
ipcom(edit-if)# exit
# ファイアウォールのデフォルト動作モードの変更
ipcom(edit)# access-control default-accept
# マルチ IP アドレスグループのデフォルトゲートウェイの設定
ipcom(edit)# ip route 0.0.0.0/0 10.0.0.1
```

【分散対象 Web サーバリソースの定義】

```
# サーバ 1 の定義
ipcom(edit)# slb real-server WEBSERVER-1
ipcom(edit-slb-real)# distribution-address 192.168.10.1
ipcom(edit-slb-real)# exit
# サーバ 2 の定義
ipcom(edit)# slb real-server WEBSERVER-2
ipcom(edit-slb-real)# distribution-address 192.168.10.2
ipcom(edit-slb-real)# exit
```

【Web サーバ分散ルールの定義】

```
# フィルタ条件の定義
ipcom(edit)# class-map match-all any
ipcom(edit-cmap)# match any
ipcom(edit-cmap)# exit
ipcom(edit)# fixup protocol https 443/tcp
#SSL の分散ルールの定義
ipcom(edit)# slb-rule 100
ipcom(edit-slb-rule)# virtual-server 10.0.0.12 443/tcp
ipcom(edit-slb-rule)# ssl-accelerate decrypted-service 443
ipcom(edit-slb-rule)# transit-mode round-trip
ipcom(edit-slb-rule)# transfer-mode ip-address
# 条件付分散ルールの定義
ipcom(edit-slb-rule)# distribution-rule 100
ipcom(edit-dist-rule)# class-map any
ipcom(edit-dist-rule)# distribution-mode minimum-connection
ipcom(edit-dist-rule)# persistence mode node
ipcom(edit-dist-rule)# monitor level ping
ipcom(edit-dist-rule)# monitor level port
ipcom(edit-dist-rule)# monitor check-interval 60
ipcom(edit-dist-rule)# monitor check-timeout 10000
```

```
ipcom(edit-dist-rule)# monitor retry-times 3
# 分散対象サーバーの定義
ipcom(edit-dist-rule)# real-server WEBSERVER-1
ipcom(edit-dist-rule-real)# port-map virtual 443 real 80
ipcom(edit-dist-rule-real)# access-limit mode connection limit 1000 recover 800
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# real-server WEBSERVER-2
ipcom(edit-dist-rule-real)# port-map virtual 443 real 80
ipcom(edit-dist-rule-real)# access-limit mode connection limit 1000 recover 800
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# exit
ipcom(edit-slb-rule)# exit
ipcom(edit)#
```

【分散対象 APL サーバーリソースの定義】

```
# サーバー 1 の定義
ipcom(edit)# slb real-server APLSERVER-1
ipcom(edit-slb-real)# distribution-address 192.168.10.3
ipcom(edit-slb-real)# exit
# サーバー 2 の定義
ipcom(edit)# slb real-server APLSERVER-2
ipcom(edit-slb-real)# distribution-address 192.168.10.4
ipcom(edit-slb-real)# exit
```

【APL サーバー分散ルールの定義】

```
#HTTP の分散ルールの定義
ipcom(edit)# slb-rule 200
ipcom(edit-slb-rule)# virtual-server 192.168.10.100 80/tcp
ipcom(edit-slb-rule)# transit-mode one-way
ipcom(edit-slb-rule)# transfer-mode mac-address
# 条件付分散ルールの定義
ipcom(edit-slb-rule)# distribution-rule 200
ipcom(edit-dist-rule)# class-map any
ipcom(edit-dist-rule)# distribution-mode minimum-connection
ipcom(edit-dist-rule)# persistence mode node
ipcom(edit-dist-rule)# monitor level ping
ipcom(edit-dist-rule)# monitor level port
ipcom(edit-dist-rule)# monitor check-interval 60
ipcom(edit-dist-rule)# monitor check-timeout 10000
ipcom(edit-dist-rule)# monitor retry-times 3
# 分散対象サーバーの定義
ipcom(edit-dist-rule)# real-server APLSERVER-1
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# real-server APLSERVER-2
```

```
ipcom(edit-dist-rule-real)# exit
```

```
ipcom(edit-dist-rule)# exit
```

```
ipcom(edit-slb-rule)# exit
```

【SSL アクセラレーターの定義】

```
ipcom(edit)# rule ssl-accel server 100
```

```
# 事前に作成のサーバー証明書を設定
```

```
ipcom(edit-ssl-accel)# cert 1
```

```
ipcom(edit-ssl-accel)# protocol tls1.2
```

```
ipcom(edit-ssl-accel)# cipher-suites +DEFAULT +ECDHE_RSA
```

```
ipcom(edit-ssl-accel)# server-address any 443
```

```
ipcom(edit-ssl-accel)# exit
```

```
ipcom(edit)#
```

APl サーバーの設定

サーバー負荷分散機能で MAC アドレス変換を使用する場合、分散対象となる Linux サーバーへ以下の設定を行います。

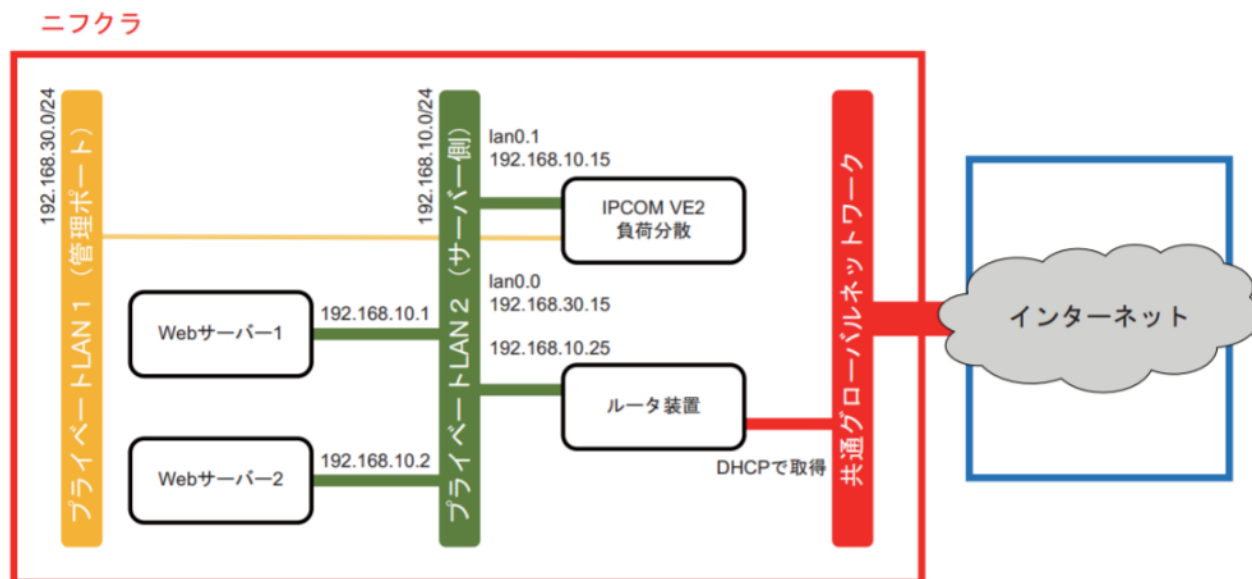
```
iptables -t nat -A PREROUTING -d 192.168.10.100 -j REDIRECT
```


7-1-3 ワンアーム（サーバー負荷分散+Web アクセラレーション）

構成例の概要

インターネット環境のクライアントからの HTTP 通信を、ワンアーム構成で配置された IPCOM VE2 が、同一サブネット内の Web サーバーに負荷分散します。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	自動割り当て、DHCP で取得した IP アドレスを自動設定
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.10.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (管理ポート)	192.168.30.15/255.255.255.0
LAN0.1 の IP アドレスとサブネットマスク値 (サーバー側)	192.168.10.15/255.255.255.0

- 分散対象となる Web サーバーは、以下のとおりです。

分散対象サーバーの IP : ポート番号	分散対象サーバー1 192.168.10.1 : 80 分散対象サーバー2 192.168.10.2 : 80
----------------------	--

仮想 IP アドレス：仮想ポート番号	192.168.10.10：80
--------------------	------------------

- 分散対象となる Web サーバーおよび負荷分散機能の設定条件は、以下のとおりです。

パケットの転送方式	IP アドレス変換
応答経路	通過型配置
分散方法	ラウンドロビン
分散の単位	ノード単位
監視パケット送信間隔	60 秒間隔
監視パケット応答待ち時間	10 秒
監視パケットリトライ回数	3 回

IPCOM VE2 構成定義例

【IPCOM VE2 のインターフェースに関する定義】

```
# サーバー側の本装置の IP アドレス定義
ipcom(edit)# interface lan0.1
ipcom(edit-if)# ip address 192.168.10.15 255.255.255.0
ipcom(edit-if)# ip-routing
ipcom(edit-if)# exit
# ファイアウォールのデフォルト動作モードの変更
ipcom(edit)# access-control default-accept
```

【分散対象 Web サーバーリソースの定義】

```
# サーバー 1 の定義
ipcom(edit)# slb real-server WEBSERVER-1
ipcom(edit-slb-real)# distribution-address 192.168.10.1
ipcom(edit-slb-real)# exit
# サーバー 2 の定義
ipcom(edit)# slb real-server WEBSERVER-2
ipcom(edit-slb-real)# distribution-address 192.168.10.2
ipcom(edit-slb-real)# exit
```

【Web サーバー分散ルールの定義】

```
# フィルター条件の定義
ipcom(edit)# class-map match-all any
ipcom(edit-cmap)# match any
ipcom(edit-cmap)# exit
# HTTP の分散ルールの定義
ipcom(edit)# slb-rule 100
ipcom(edit-slb-rule)# virtual-server 192.168.10.10 80/tcp
```

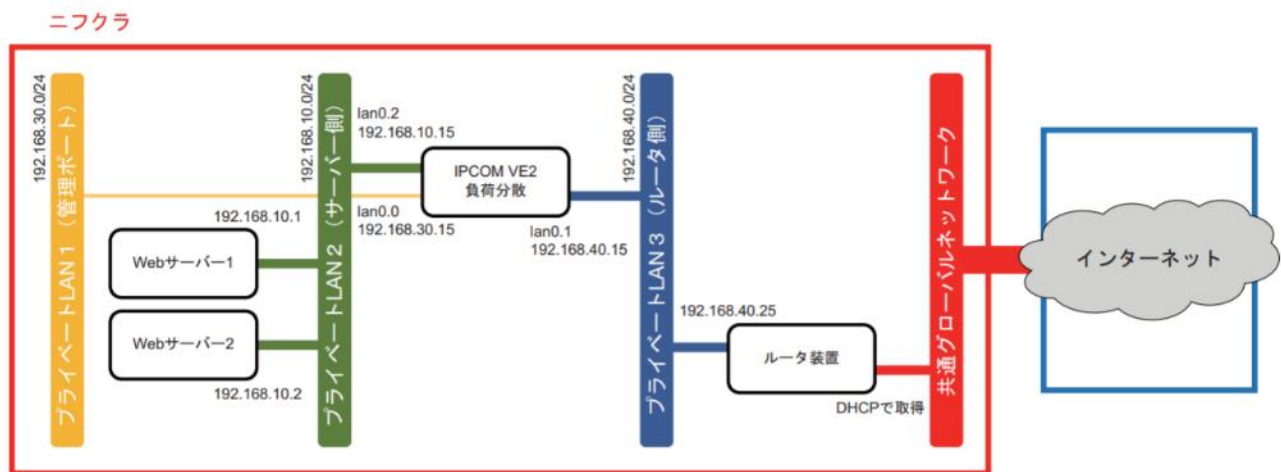
```
ipcom(edit-slb-rule)# transit-mode round-trip
ipcom(edit-slb-rule)# transfer-mode ip-address
#Web アクセラレーション機能を利用
ipcom(edit-slb-rule)# web-accelerate send-client-address
# 条件付分散ルールの定義
ipcom(edit-slb-rule)# distribution-rule 100
ipcom(edit-dist-rule)# class-map any
ipcom(edit-dist-rule)# distribution-mode round-robin
ipcom(edit-dist-rule)# persistence mode node
ipcom(edit-dist-rule)# monitor level ping
ipcom(edit-dist-rule)# monitor level port
ipcom(edit-dist-rule)# monitor check-interval 60
ipcom(edit-dist-rule)# monitor check-timeout 10000
ipcom(edit-dist-rule)# monitor retry-times 3
# 分散対象サーバーの定義
ipcom(edit-dist-rule)# real-server WEBSERVER-1
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# real-server WEBSERVER-2
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# exit
ipcom(editslb-rule)# exit
ipcom(edit)#
```

7-1-4 プライベートセグメントを挟んだインライン

構成例の概要

インライン（SSL アクセラレーター/ サーバー負荷分散）構成の、インターネット環境と IPCOM VE2 を配置するプライベート LAN との間に、プライベート LAN を追加した構成です。ルータ装置の追加配置など、お客様の利用シーンに応じた柔軟な構成が可能です。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	自動割り当て、DHCP で取得した IP アドレスを自動設定
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.10.0/24)を設定
プライベート LAN3	作成したプライベート LAN(192.168.40.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値（管理ポート）	192.168.30.15/255.255.255.0
LAN0.1 の IP アドレスとサブネットマスク値（ルータ側）	192.168.40.15/255.255.255.0
LAN0.2 の IP アドレスとサブネットマスク値（サーバー側）	192.168.10.15/255.255.255.0

7-2 イン트라ネット公開（閉域網 接続）

お客様環境からダイレクトポートまたはプライベートアクセス経由でニフクラへ接続する閉域網の 構成について説明します。

【用語】

- ダイレクトポート
お客様の専用線・閉域網からニフクラへダイレクトに接続するためのサービスです。
- プライベートアクセス
ニフクラから回線事業者の閉域網へのプライベートな接続を提供するサービスです。

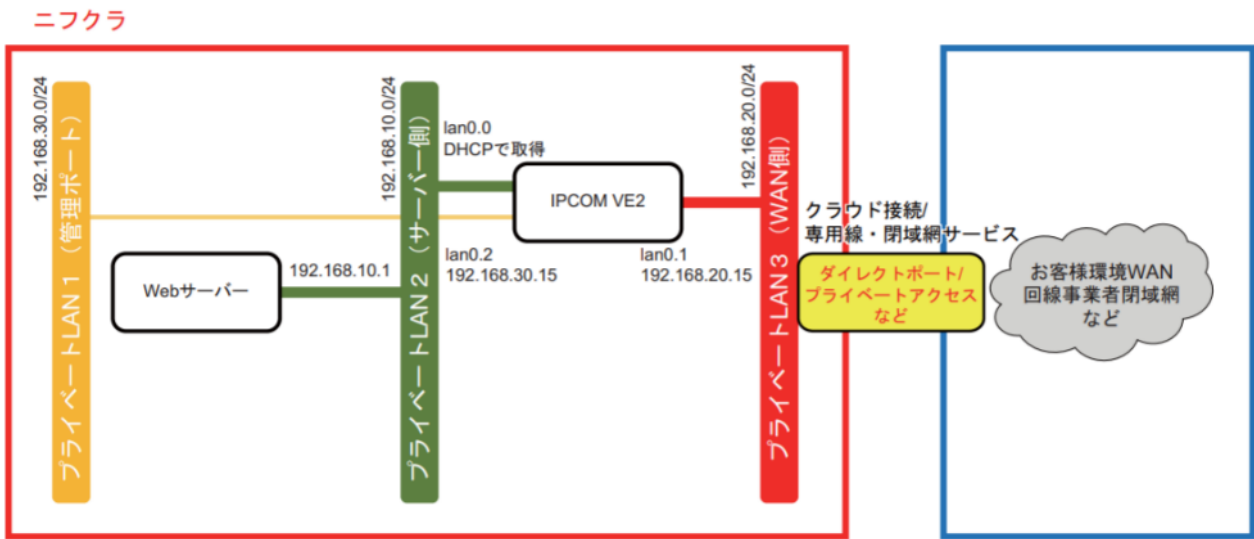
7-2-1 インライン（ファイアーウォール/アドレス変換）

構成例の概要

IPCOM VE2 を、お客様環境と Web サーバーを配置するプライベート LAN との間に配置します。

以下の構成例は、ファイアーウォール機能により、特定のサーバー / サービスへのアクセスだけを許可します。また、アドレス変換機能により、パケットヘッダーに含まれる IP アドレス・ポート番号を、別の IP アドレス・ポート番号へ変換します。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	利用しない
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.10.0/24)を設定
プライベート LAN3	作成したプライベート LAN(192.168.20.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (管理ポート)	192.168.30.15/255.255.255.0
LAN0.1 の IP アドレスとサブネットマスク値 (WAN 側)	192.168.20.15/255.255.255.0
LAN0.2 の IP アドレスとサブネットマスク値 (サーバー側)	192.168.10.15/255.255.255.0

- プライベート LAN (WAN 側) →プライベート LAN (サーバー側) で許可するフィルター条件は、以下のとおりです。

接続元 IP	接続先 IP	接続先ポート	アクション
WAN 側プライベートネットワーク	192.168.20.15	80/tcp,443/tcp	透過

- プライベート LAN (WAN 側) →プライベート LAN (サーバー側) に対するアドレス変換条件は、以下のとおりです。

変換元 IP ・ポート番号	変換先 IP ・ポート番号
192.168.20.10 : 80	192.168.10.1 : 80

IPCOM VE2 構成定義例

【IPCOM VE2 のインターフェースに関する定義】

インターネット側の本装置の IP アドレス定義

```
ipcom(edit)# interface lan0.1
```

```
ipcom(edit-if)# ip address 192.168.20.15 255.255.255.0
```

```
ipcom(edit-if)# ip-routing
```

```
ipcom(edit-if)# exit
```

サーバー側の本装置の IP アドレス定義

```
ipcom(edit)# interface lan0.2
```

```
ipcom(edit-if)# ip address 192.168.10.15 255.255.255.0
```

```
ipcom(edit-if)# ip-routing
```

```
ipcom(edit-if)# exit
```

ファイアーウォールのデフォルト動作モードの変更

```
ipcom(edit)# access-control default-deny
```

【インターネット側のパケット透過ルールの定義】

フィルター条件の定義

```
ipcom(edit)# class-map match-all client-side
```

```
ipcom(edit-cmap)# match port 80/tcp,443/tcp
```

```
ipcom(edit-cmap)# exit
```

ファイアーウォールの定義

```
ipcom(edit)# interface lan0.1
```

```
ipcom(edit-if)# rule access 10 in client-side accept
```

```
ipcom(edit-if)# exit
```

【サーバー側のパケット透過ルールの定義】

```
# フィルター条件の定義
ipcom(edit)# class-map match-all any
ipcom(edit-cmap)# match any
ipcom(edit-cmap)# exit
# 制限なし
ipcom(edit)# interface lan0.2
ipcom(edit-if)# rule access 1 in any accept
ipcom(edit-if)# rule access 1 out any accept
ipcom(edit-if)# exit
```

【インターネット側のアドレス変換の定義】

```
# アドレス変換の定義
ipcom(edit)# interface lan0.1
ipcom(edit-if)# rule dst-napt 10 ipv4 192.168.20.10 80 tcp to 192.168.10.1 80
ipcom(edit-if)# exit
```

Web サーバーの定義

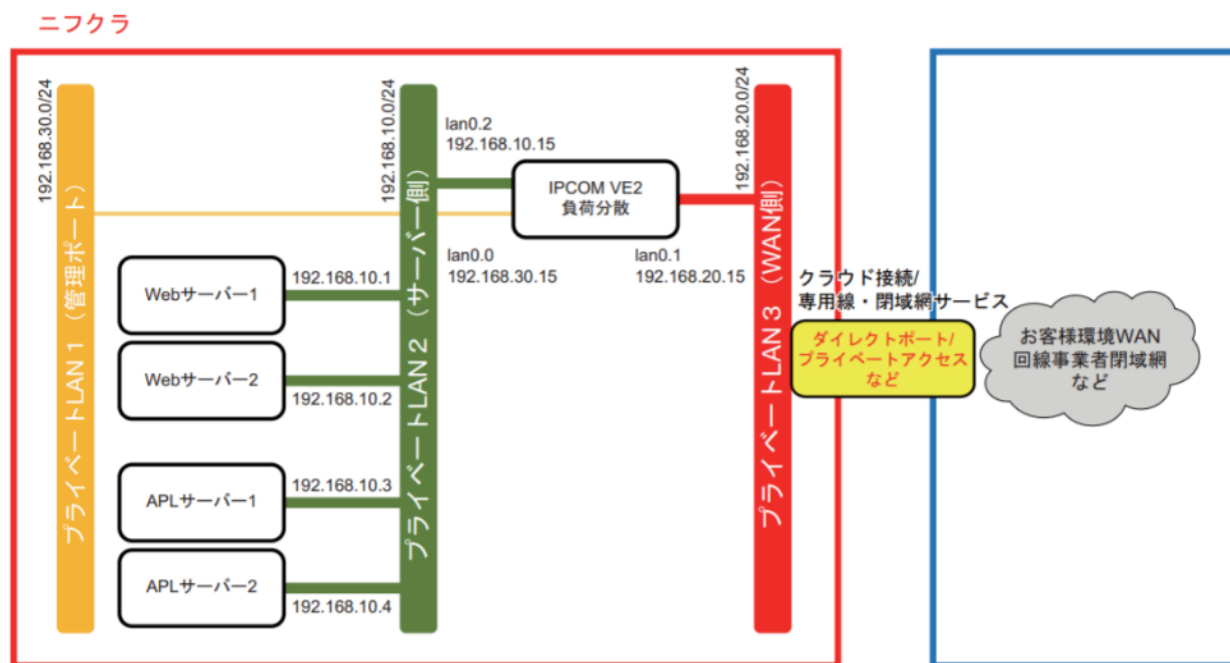
デフォルトゲートウェイの設定を、IPCOM VE2 のサーバー側インターフェース(192.168.10.15/24) にします。

7-2-2 インライン（SSL アクセラレーター/ サーバー負荷分散）

構成例の概要

お客様環境のクライアントからの SSL 通信を、背後の Web サーバーに負荷分散します。また、Web サーバーと APL サーバーを同一サブネットのプライベート LAN 上に配置して、Web サーバーから APL サーバーへの通信に対して、APL サーバーの負荷分散を行います。

ニフクラ/IPCOW VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	利用しない
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.10.0/24)を設定
プライベート LAN3	作成したプライベート LAN(192.168.20.0/24)を設定

IPCOW VE2 設定条件

- IPCOW VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (管理ポート)	192.168.30.15/255.255.255.0
LAN0.1 の IP アドレスとサブネットマスク値 (WAN 側)	192.168.20.15/255.255.255.0
LAN0.2 の IP アドレスとサブネットマスク値 (サーバー側)	192.168.10.15/255.255.255.0

- 分散対象となる Web サーバーは、以下のとおりです。

分散対象サーバーの IP : ポート番号	分散対象サーバー1 192.168.10.1 : 80 分散対象サーバー2 192.168.10.2 : 80
仮想 IP アドレス : 仮想ポート番号	192.168.20.1 : 443

- 分散対象となる Web サーバーおよび負荷分散機能の設定条件は、以下のとおりです。
[インライン \(SSL アクセラレーター/ サーバー負荷分散\)](#) と同じ構成になります。
- 分散対象となる APL サーバーは、以下のとおりです。
[インライン \(SSL アクセラレーター/ サーバー負荷分散\)](#) と同じ構成になります。
- 分散対象となる APL サーバーおよび負荷分散機能の設定条件は、以下のとおりです。
[インライン \(SSL アクセラレーター/ サーバー負荷分散\)](#) と同じ構成になります。

IPCOM VE2 構成定義例

【IPCOM VE2 のインターフェースに関する定義】

```
#WAN 側の本装置の IP アドレス定義
ipcom(edit)# interface lan0.1
ipcom(edit-if)# ip address 192.168.20.15 255.255.255.0
ipcom(edit-if)# ip-routing
ipcom(edit-if)# exit

# サーバー側の本装置の IP アドレス定義
ipcom(edit)# interface lan0.2
ipcom(edit-if)# ip address 192.168.10.15 255.255.255.0
ipcom(edit-if)# ip-routing
ipcom(edit-if)# exit

# ファイアーウォールのデフォルト動作モードの変更
ipcom(edit)# access-control default-accept
```

【分散対象 Web・サーバーリソースの定義】

[インライン \(SSL アクセラレーター/ サーバー負荷分散\)](#) と同じ構成になります。

【Web サーバー分散ルールの定義】

```
# フィルター条件の定義
ipcom(edit)# class-map match-all any
ipcom(edit-cmap)# match any
ipcom(edit-cmap)# exit

ipcom(edit)# fixup protocol https 443/tcp

#SSL の分散ルールの定義
ipcom(edit)# slb-rule 100
ipcom(edit-slb-rule)# virtual-server 192.168.20.1 443/tcp
ipcom(edit-slb-rule)# ssl-accelerate decrypted-service 443
ipcom(edit-slb-rule)# transit-mode round-trip
ipcom(edit-slb-rule)# transfer-mode ip-address

# 条件付分散ルールの定義
ipcom(edit-slb-rule)# distribution-rule 100
ipcom(edit-dist-rule)# class-map any
```

```
ipcom(edit-dist-rule)# distribution-mode minimum-connection
ipcom(edit-dist-rule)# persistence mode node
ipcom(edit-dist-rule)# monitor level ping
ipcom(edit-dist-rule)# monitor level port
ipcom(edit-dist-rule)# monitor check-interval 60
ipcom(edit-dist-rule)# monitor check-timeout 10000
ipcom(edit-dist-rule)# monitor retry-times 3
# 分散対象サーバーの定義
ipcom(edit-dist-rule)# real-server WEBSERVER-1
ipcom(edit-dist-rule-real)# port-map virtual 443 real 80
ipcom(edit-dist-rule-real)# access-limit mode connection limit 1000 recover 800
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# real-server WEBSERVER-2
ipcom(edit-dist-rule-real)# port-map virtual 443 real 80
ipcom(edit-dist-rule-real)# access-limit mode connection limit 1000 recover 800
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# exit
ipcom(edit-slb-rule)# exit
ipcom(edit)#
```

【分散対象 APL サーバーリソースの定義】

[インライン（SSL アクセラレーター/ サーバー負荷分散）](#)と同じ構成になります。

【APL サーバー分散ルールの定義】

[インライン（SSL アクセラレーター/ サーバー負荷分散）](#)と同じ構成になります。

【SSL アクセラレーターの定義】

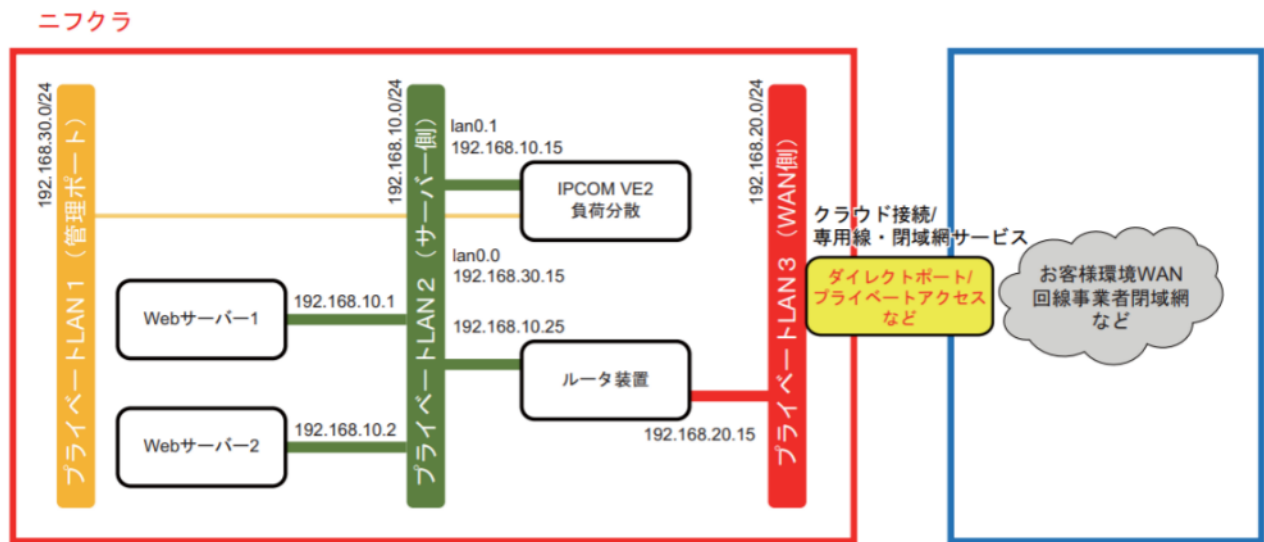
[インライン（SSL アクセラレーター/ サーバー負荷分散）](#)と同じ構成になります。

7-2-3 ワンアーム（サーバー負荷分散+Web アクセラレーション）

構成例の概要

お客様環境のクライアントからの HTTP 通信を、ワンアーム構成で配置された IPCOM VE2 が、同一サブネット内の Web サーバーに負荷分散します。

ニフクラ/IPCOM VE2 構成図



● ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	利用しない
共通プライベート	利用しない
プライベートLAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベートLAN2	作成したプライベート LAN(192.168.10.0/24)を設定
プライベートLAN3	作成したプライベート LAN(192.168.20.0/24)を設定

IPCOM VE2 設定条件

ワンアーム（サーバー負荷分散+WEB アクセラレーション）と同じ構成になります。

IPCOM VE2 構成定義例

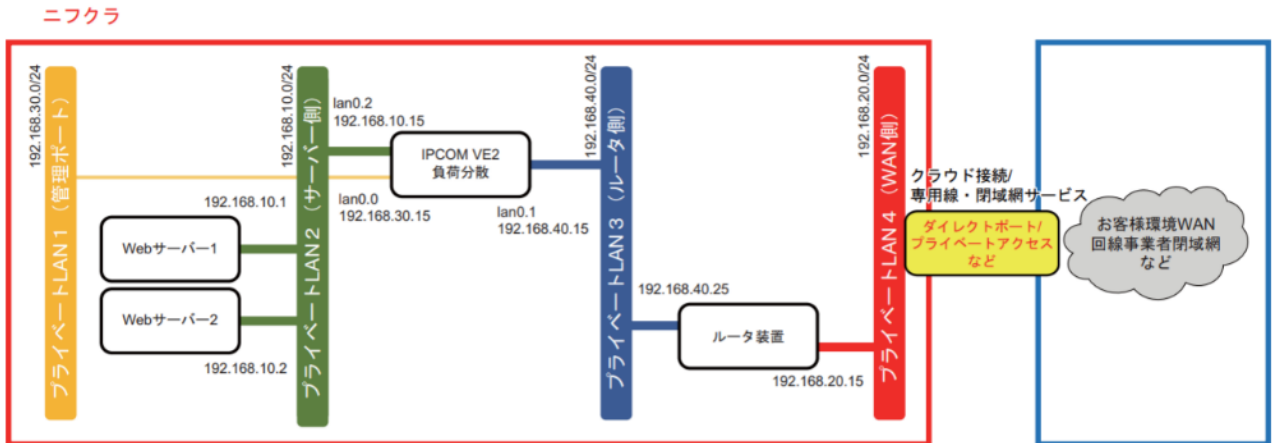
ワンアーム（サーバー負荷分散+WEB アクセラレーション）と同じ構成になります。

7-2-4 プライベートセグメントを挟んだインライン

構成図の概要

インライン（SSL アクセラレーター/ サーバー負荷分散）構成の、お客様環境と IPCOM VE2 サーバーを配置するプライベート LAN との間に、プライベート LAN を追加した構成です。ルータ装置の追加配置など、お客様の利用シーンに応じた柔軟な構成が可能です。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	利用しない
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.10.0/24)を設定
プライベート LAN3	作成したプライベート LAN(192.168.40.0/24)を設定
プライベート LAN4	作成したプライベート LAN(192.168.20.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (管理ポート)	192.168.30.15/255.255.255.0
LAN0.1 の IP アドレスとサブネットマスク値 (ルータ側)	192.168.40.15/255.255.255.0
LAN0.2 の IP アドレスとサブネットマスク値 (サーバー側)	192.168.10.15/255.255.255.0

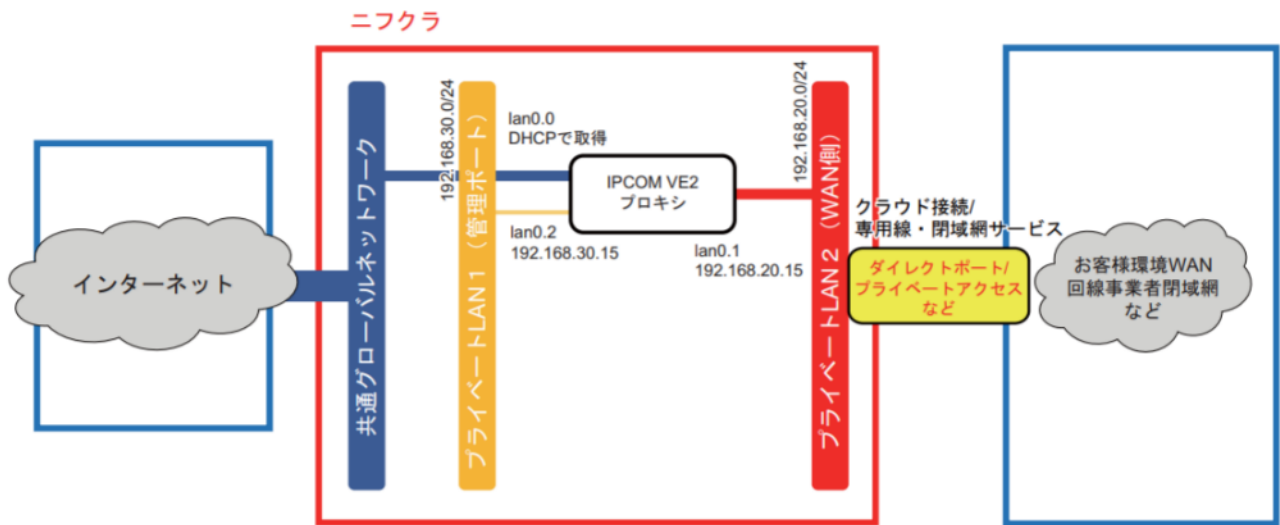
7-2-5 プロキシ

構成例の概要

お客様環境からダイレクトポートまたはプライベートアクセス経由でニフクラへ接続し、そこから共通グローバルネットワーク経由でインターネット環境へ接続する構成です。

お客様環境からインターネット環境へ Web アクセスする環境で、IPCOM VE2 をプロキシサーバーとして動作させ、装置を通過するパケットをアンチウイルス機能に受け渡し、ウイルス検査を行わせる構成例となります。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	自動割り当て、DHCP で取得した IP アドレスを自動設定
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.20.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値（インターネット側）	DHCP で取得
LAN0.1 の IP アドレスとサブネットマスク値（WAN 側）	192.168.20.15/255.255.255.0
LAN0.2 の IP アドレスとサブネットマスク値（管理ポート）	192.168.30.15/255.255.255.0

7-2-6 冗長化(1)サーバーセパレート

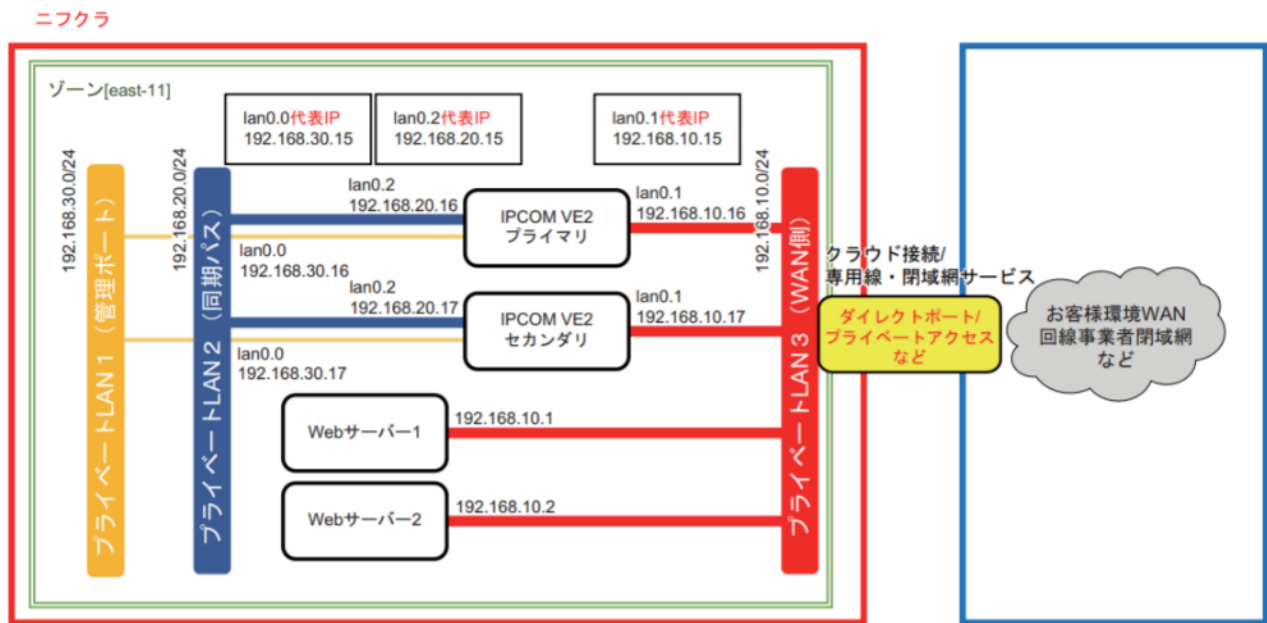
構成例の概要

ニフクラのサーバーセパレート機能を利用する冗長構成です。

サーバーセパレートは、指定したサーバー 2 台を同一ゾーンの異なる物理ホスト上に分離的に配置する機能です。これにより、冗長化用途のサーバーが物理ホスト障害の影響を同時に受ける確率を軽減します。

2 台の IPCOM VE2 を、装置二重化機能（クラスタリング機能）により冗長化します。お客様環境のクライアントからの SSL 通信を、プライマリ装置の IPCOM VE2 が受け取り、背後の Web サーバーに負荷分散処理します。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	利用しない
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.20.0/24)を設定
プライベート LAN3	作成したプライベート LAN(192.168.10.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (管理ポート)	192.168.30.15/255.255.255.0 (代表 IP) 192.168.30.16/255.255.255.0 (プライマリ) 192.168.30.17/255.255.255.0 (セカンダリ)
LAN0.1 の IP アドレスとサブネットマスク値 (WAN 側)	192.168.10.15/255.255.255.0 (代表 IP) 192.168.10.16/255.255.255.0 (プライマリ) 192.168.10.17/255.255.255.0 (セカンダリ)
LAN0.2 の IP アドレスとサブネットマスク値 (同期パス用)	192.168.20.15/255.255.255.0 (代表 IP) 192.168.20.16/255.255.255.0 (プライマリ) 192.168.20.17/255.255.255.0 (セカンダリ)

- 分散対象となる Web サーバーは、以下のとおりです。

分散対象サーバーの IP : ポート番号	分散対象サーバー1 192.168.10.1 : 80 分散対象サーバー2 192.168.10.2 : 80
仮想 IP アドレス : 仮想ポート番号	192.168.10.10 : 443

- 分散対象となる Web サーバーおよび負荷分散機能の設定条件は、以下のとおりです。

パケットの転送方式	IP アドレス変換
応答経路	通過型配置
分散方法	ラウンドロビン
分散の単位	ノード単位
監視パケット送信間隔	60 秒間隔
監視パケット応答待ち時間	10 秒
監視パケットリトライ回数	3 回

IPCOM VE2 構成定義例

【IPCOM VE2 の装置二重化に関する定義】

```
# クラスタの定義
ipcom(edit)# hostname VE2-PRI VE2-SEC
ipcom(edit)# cluster mode primary
ipcom(edit)# cluster id 1
ipcom(edit)# cluster secret-key abcdefgh
```

【IPCOM VE2 のインターフェースに関する定義】

```
# サーバー側の本装置の IP アドレス定義
ipcom(edit)# interface lan0.1
ipcom(edit-if)# ip address 192.168.10.15 255.255.255.0
ipcom(edit-if)# ip address primary 192.168.10.16
ipcom(edit-if)# ip address secondary 192.168.10.17
ipcom(edit-if)# ip-routing
ipcom(edit-if)# cluster vrid 11
ipcom(edit-if)# exit
# 同期パスの本装置の IP アドレス定義
```

```
ipcom(edit)# interface lan0.2
ipcom(edit-if)# ip address 192.168.20.15 255.255.255.0
ipcom(edit-if)# ip address primary 192.168.20.16
ipcom(edit-if)# ip address secondary 192.168.20.17
ipcom(edit-if)# ip-routing
ipcom(edit-if)# cluster sync-interface priority 1
ipcom(edit-if)# cluster vrid 12
ipcom(edit-if)# exit
# ファイアウォールのデフォルト動作モードの変更
ipcom(edit)# access-control default-accept
```

【分散対象 Web サーバリソースの定義】

```
# サーバ 1 の定義
ipcom(edit)# slb real-server WEBSERVER-1
ipcom(edit-slb-real)# distribution-address 192.168.10.1
ipcom(edit-slb-real)# exit
# サーバ 2 の定義
ipcom(edit)# slb real-server WEBSERVER-2
ipcom(edit-slb-real)# distribution-address 192.168.10.2
ipcom(edit-slb-real)# exit
```

【Web サーバ分散ルールの定義】

```
# フィルタ条件の定義
ipcom(edit)# class-map match-all any
ipcom(edit-cmap)# match any
ipcom(edit-cmap)# exit
ipcom(edit)# fixup protocol https 443/tcp
#SSL の分散ルールの定義
ipcom(edit)# slb-rule 100
ipcom(edit-slb-rule)# virtual-server 192.168.10.10 443/tcp
ipcom(edit-slb-rule)# ssl-accelerate decrypted-service 443
ipcom(edit-slb-rule)# transit-mode round-trip
ipcom(edit-slb-rule)# transfer-mode ip-address
# 条件付分散ルールの定義
ipcom(edit-slb-rule)# distribution-rule 100
ipcom(edit-dist-rule)# class-map any
ipcom(edit-dist-rule)# distribution-mode round-robin
ipcom(edit-dist-rule)# persistence mode node
ipcom(edit-dist-rule)# monitor level ping
ipcom(edit-dist-rule)# monitor level port
ipcom(edit-dist-rule)# monitor check-interval 60
ipcom(edit-dist-rule)# monitor check-timeout 10000
ipcom(edit-dist-rule)# monitor retry-times 3
# 分散対象サーバの定義
```



```
ipcom(edit-dist-rule)# real-server WEBSERVER-1
ipcom(edit-dist-rule-real)# port-map virtual 443 real 80
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# real-server WEBSERVER-2
ipcom(edit-dist-rule-real)# port-map virtual 443 real 80
ipcom(edit-dist-rule-real)# exit
ipcom(edit-dist-rule)# exit
ipcom(edit-slb-rule)# exit
ipcom(edit)#
```

【ワンアーム構成のアドレス変換の定義】

```
# フィルター条件の定義
ipcom(edit)# class-map match-all webserver
ipcom(edit-cmap)# match destination-address ipv4 192.168.10.1-192.168.10.2
ipcom(edit-cmap)# exit
# アドレス変換の定義
ipcom(edit)# interface lan0.1
ipcom(edit-if)# rule src-napt 10 ipv4 webserver to 192.168.10.10 1024-65535
ipcom(edit-if)# exit
```

【SSL アクセラレーターの定義】

```
ipcom(edit)# rule ssl-accel server 100
# 事前に作成のサーバー証明書を設定
ipcom(edit-ssl-accel)# cert 1
ipcom(edit-ssl-accel)# protocol tls1.2
ipcom(edit-ssl-accel)# cipher-suites +DEFAULT +ECDHE_RSA
ipcom(edit-ssl-accel)# server-address any 443
ipcom(edit-ssl-accel)# exit
ipcom(edit)# exit
```

7-2-7 冗長化(2)マルチゾーン・プライベートブリッジ

構成例の概要

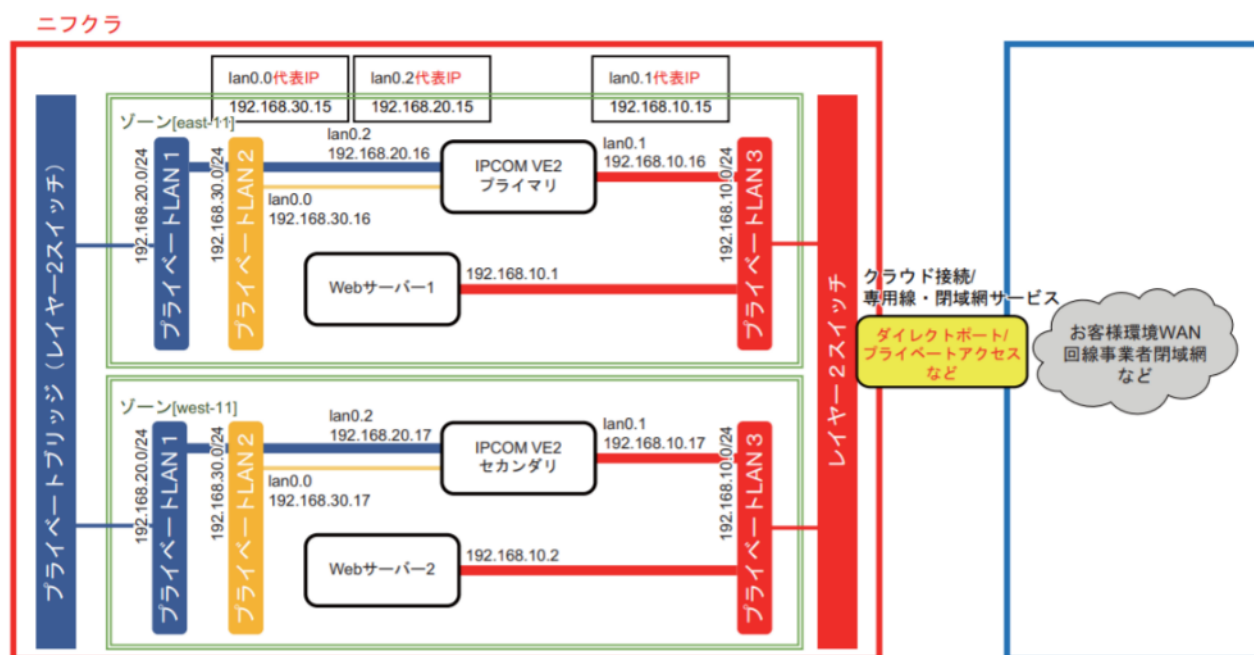
マルチゾーンヘッサー 2 台を分離的に配置し、さらにプライベートブリッジでサーバー 2 台を接続する冗長構成です。

プライベートブリッジは、プライベート LAN 同士をレイヤー2 スwitch接続するネットワークサービスです。

別々のリージョンのゾーンで冗長構成を組むことにより、DR（ディザスタリカバリ）対策になります。

IPCOM VE2 の構成は、プライベートブリッジを経由してサーバー間の同期が行われます。それ以外は、[冗長化\(1\)サーバーセパレーター](#)と同様です。

ニフクラ/IPCOM VE2 構成図



- ニフクラのネットワーク構成は、以下のとおりです。

共通グローバル	利用しない
共通プライベート	利用しない
プライベート LAN1	作成したプライベート LAN(192.168.20.0/24)を設定
プライベート LAN2	作成したプライベート LAN(192.168.30.0/24)を設定
プライベート LAN3	作成したプライベート LAN(192.168.10.0/24)を設定

IPCOM VE2 設定条件

- IPCOM VE2 の IP アドレスとサブネットマスク値は、以下のとおりです。

LAN0.0 の IP アドレスとサブネットマスク値 (管理ポート)	192.168.30.15/255.255.255.0 (代表 IP) 192.168.30.16/255.255.255.0 (プライマリ) 192.168.30.17/255.255.255.0 (セカンダリ)
---------------------------------------	---

LAN0.1 の IP アドレスとサブネットマスク値 (WAN 側)	192.168.10.15/255.255.255.0 (代表 IP)
	192.168.10.16/255.255.255.0 (プライマリ)
	192.168.10.17/255.255.255.0 (セカンダリ)
LAN0.2 の IP アドレスとサブネットマスク値 (プライベートブリッジ側/同期パス用)	192.168.20.15/255.255.255.0 (代表 IP)
	192.168.20.16/255.255.255.0 (プライマリ)
	192.168.20.17/255.255.255.0 (セカンダリ)

そのほかには、[冗長化\(1\)サーバーセパレート](#)と同じ構成になります。