多様なネットワーク環境を提供するネットワークサービス

籾山 奈々子　滝口 敏行　荒久田 博士　清水 昭彦　菅野 洋太郎　水島 一紀

要 旨

ICTシステムでは従来、ネットワーク機器の物理的な制約に縛られることが多くありました。近年では、仮想的なネットワークの利用が広がっています。需要の変動に対応して迅速な利用が可能であることは、変化の速いICTの世界、とりわけクラウドの世界では重要な要件となっています。一方で、ネットワーク機器の能力を最大限に生かせる物理機器への需要も根強いものがあります。NEC Cloud IaaSでは双方のニーズを満たすため、仮想から物理まで幅広いラインアップを用意しています。本稿では、NEC Cloud IaaSで提供している「多様なネットワーク環境を実現するネットワークサービス」の構成について紹介します。

KeyWords　クラウド／SDN／ネットワークサービス／物理アプライアンス／仮想アプライアンス

1. はじめに

クラウドのネットワークには、利用の迅速性・柔軟性とともに、基幹システムにも耐えうる機能性・性能性が求められます。また、クラウドへの移行を容易にし、クラウドを含めた全資産を最大限活用するためには、クラウドだけではなく、ハウジングサービスとの連携、利用者拠点や他データセンターとの接続性も重要となります。

NECが提供するNEC Cloud IaaSのネットワークサービスには、以下の特長・コンセプトがあります。

（1）利用者の要求に応える幅広いラインアップ

（2）外部接続を含めたネットワーク構成の自由度

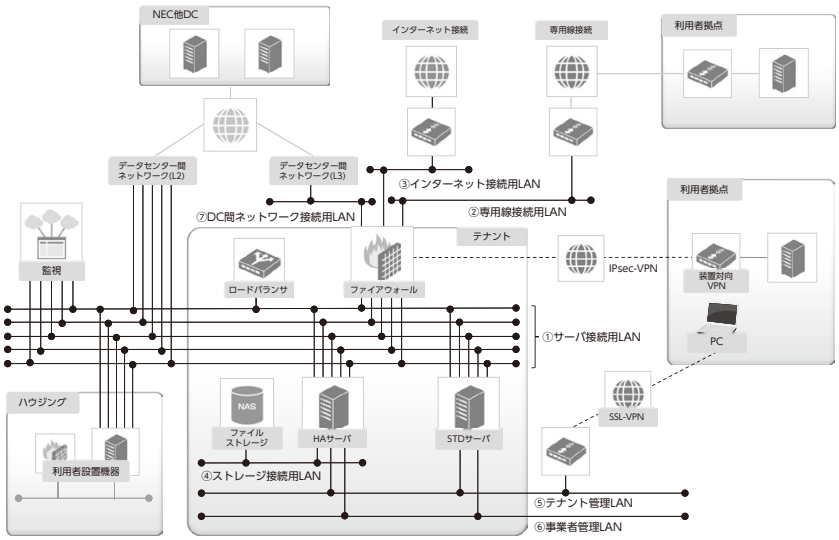

図　NEC Cloud IaaS ネットワーク全体図

(3) 利用者が必要に応じてネットワークリソースを利用できるオンデマンド性

これらコンセプトの実現を目標に、NEC Cloud IaaSは設計・構築されています。

利用者がテナント内で作成できるネットワークの全体構成は図のとおりです。

NEC Cloud IaaSではテナント内のプライベートネットワークのほか、ファイアウォールやロードバランサ、インターネット接続やVPN、専用線接続をはじめとした外部接続サービスなどを提供しています。次章より各種サービスの概要と、それを実現する要素技術について解説します。

2. 基本ネットワーク（仮想LAN）

NEC Cloud IaaSでは、テナントに払い出されるネットワークを「仮想LAN」と総称しています。仮想LANには、サーバや各種ネットワークサービス間を接続してシステムを構成する中心となる「サーバ接続用LAN」をはじめ、外部と接続するための「インターネット接続用LAN」、ファイルストレージと接続するための「ストレージ接続用LAN」などがあります。仮想LANの作成・設定は、利用者によってセルフサービスポータルから実施することが可能です。

NEC Cloud IaaSは、高性能・高信頼の「ハイアベイラビリティ（HA）」と高いコストパフォーマンスの「スタンダード（STD）」の2つのサービスを用意しており、ハイアベイラビリティ（HA）の仮想LANは、弊社製品であるWebSAM vDC AutomationとUNIVERGE PFシリーズを活用し、VTN（Virtual Tenant Netwoek）による通信分離を実現しています。また、スタンダード（STD）の仮想LANには、VXLANを利用しています。VTNはVLANにマッピングされ、更にVXLANにもマッピングされます。これらを活用し、接続性向上とテナント間の通信分離、機密性向上を実現しています。

3. SSL-VPN

利用者がテナント内に作成したサーバを管理するための接続経路として、SSL-VPNを用いたインターネットVPNを提供しています。テナント入会時、SSL-VPN装置に対して、専用のインタフェースと通信ポリシーを自動で生成・設定します。SSL-VPNの有効化・無効化、パスワード変更はセルフサービスポータルから操作可能です。

4. 物理アプライアンス

ネットワークを構成する際に必須となるファイアウォールやロードバランサの機能を、それに特化した物理ハードウェアで提供するネットワークアプライアンスを「物理アプライアンス」と呼んでいます。NEC Cloud IaaSの物理アプライアンスサービスでは、採用している物理ハードウェアが持つ独自機能のなかから、ニーズの高いものを選別して提供しています。これは、物理アプライアンスでも、後述の仮想アプライアンスでも均質なサービスの提供を目標にし、セルフサービスポータルからは同じ操作感でネットワークアプライアンスを利用できるようにしているためです。

4.1 ファイアウォール（物理）

物理アプライアンスのファイアウォールサービスには、共用サービスと専用サービスがあります。共用サービスでは、ファイアウォール機器に論理ファイアウォールを複数稼働させ、利用者ごとに提供しています。専用サービスでは、ファイアウォール機器を1利用者＝1テナントで占有することで、機器の能力を最大限に利用可能です。

利用者によるセルフサービスポータルでのファイアウォールサービス契約を機に、機器に対して論理ファイアウォールの作成や通信ポリシーといった、ファイアウォール利用開始に必要な処理が順に実行されます。利用者がインターネット接続を必要とする場合には、グローバルIPアドレスの払い出しとファイアウォールに対する設定も実行されます。

利用者は払い出されたファイアウォールに対して、通信ポリシーの設定をセルフサービスポータルから行うことができます。

4.2 ロードバランサ（物理）

物理アプライアンスのロードバランササービスにも、共用サービスと専用サービスがあります。共用サービスではロードバランサ機器のリソースを論理分割し、論理リソースを利用者ごとに提供しています。専用サービスでは、ロードバランサ機器を1利用者＝1テナントで占有利用することで、機器の能力を最大限に生かすことができます。

利用者によるセルフサービスポータルでのロードバランササービス契約を機に、機器に対する論理リソース払い出しや

ロードバランサ利用開始に必要な処理が順に実行されます。

利用者は払い出されたロードバランサに対して、仮想サーバ設定・振り分け先サーバ設定・ヘルスチェック設定などをセルフサービスポータルから行うことができます。

5. 仮想アプライアンス

NEC Cloud IaaSでは、弊社のアプライアンス製品「InterSecVM」をベースとして、ファイアウォール及びロードバランサを仮想アプライアンスとして提供しています。仮想アプライアンスは、x86サーバ（汎用機）で動くHypervisor上の仮想マシンとなっています。そのため、高価な物理アプライアンス（専用機）と比較して、安価なコストでの提供が可能となっています。

仮想アプライアンスを操作するためのREST API群を開発し、物理アプライアンスと同等の設定をセルフサービスポータルから実行可能としています。

5.1 ファイアウォール（仮想）

テナント内のプライベートネットワークまたはインターネットからのアクセスに対して、アクセスポリシー制御・ルーティング制御・内向きNAT変換といったファイアウォールとしての基本機能をセルフサービスポータルから利用可能です。利用者によるセルフサービスポータルでの操作が上述のREST API群と連動し、ファイアウォールへ設定が行われます。

5.2 ロードバランサ（仮想）

Round-RobinまたはLeast Connectionsの分散方式で、テナント内の仮想サーバに対するロードバランシング機能を提供しています。また、セッション維持やヘルスチェック機能・SSL暗号化機能など、ロードバランサとしての基本機能も具備しており、これら機能をセルフサービスポータルから利用することが可能です。セルフサービスポータルでの操作が上述のREST API群と連動し、ロードバランサへ設定が行われます。

6. 外部接続サービス

6.1 インターネット接続

サーバに対し、インターネットへの接続機能を提供しています。利用者が柔軟にインターネット接続を利用できるよう、ベストエフォートと帯域保障のメニューを提供しています。ベストエフォートと帯域保障のメニューを組み合わせて利用することも可能です。

サーバがインターネット接続をする際には、帯域制御装置・インターネット接続用スイッチ・ファイアウォールなど、多種多様なネットワーク機器を経由します。これら機器に対して一貫した設定をしなければ、簡易な操作で安心感のあるインターネット接続は実現できません。NEC Cloud IaaSでは、一貫した設定を行うためのロジック及びAPI群を開発しています。これにより、利用者がセルフサービスポータルから行った操作と連動したインターネット接続の自動化を可能としています。

6.2 装置対向VPN

利用者サイトと利用者テナント間をセキュアに接続する手段の1つとして、インターネットを介したVPN接続を可能とするためのVPNゲートウェイ（VPN GW）機能を提供しています。VPN GW機能を、ファイアウォール機能のオプションとして提供することで、VPN通信に対してもセルフサービスポータルから一元的なアクセス制御が可能です。

利用者サイト側で準備するVPN GWに対する制限（ベンダ・製品・アプリケーションなど）をできるだけ排除することを目的に、サイト間VPNの方式として一般的なIPSecを採用しています。

6.3 専用線接続

利用者サイト及びNEC Cloud IaaS側に専用線接続機器を準備いただくことで、利用者サイトとNEC Cloud IaaS間を専用線接続することができます。

6.4 データセンター間ネットワーク接続

NEC Cloud IaaSと弊社の主要データセンターとの間で、ネットワーク接続が可能です。第6章1節のインターネット接続と同様、柔軟にデータセンター間ネットワーク接続を構成できるよう、ベストエフォートと帯域保障のメニューを提供しています。ベストエフォートのメニューと、帯域保障のメニューを組み合わせて利用することも可能です。

接続方針として以下2つのメニューを提供しており、NEC Cloud IaaS内のサーバと対向側データセンターに存在する機器のネットワークアドレスが同じである場合・同じではない場合のどちらでも、接続が可能です。

（1）ブリッジング接続（L2）サービス
（2）ルーティング接続（L3）サービス

7. ハウジング連携サービス

NEC Cloud IaaSを提供しているデータセンターでは、同じ建物の中でハウジングサービスを提供しています。NEC Cloud IaaSの利用者は、ハウジングサービスとNEC Cloud IaaSの双方を利用することが可能です。

ハウジング連携サービスを利用することで、NEC Cloud IaaSとハウジング環境で通信を行うことが可能となります。NEC Cloud IaaSで提供されていない機器・機能を利用者自らハウジング環境に用意し、ハウジング連携サービスを利用いただくことで、より柔軟にNEC Cloud IaaSを利用いただくことができます。

8. ネットワークサービスの自動化

本章では、NEC Cloud IaaSで提供しているネットワークサービスの自動化について述べます。この自動化機能は、前章までで説明したネットワークサービスの払い出し自動化・各サービスのセルフサービスポータル化実現を目指し、開発・構築しました。

NEC Cloud IaaSでは、多種多様なネットワーク機器を利用しています。本稿ではすべてを紹介することはできませんが、弊社のネットワーク・SDN（Software-Defined Networking）製品であるUNIVERGE PFシリーズやQXシリーズ、IXシリーズをはじめ、WebSAM vDC AutomationやInterSecVMを採用しています。OEM製品や他社製品としては、Fortinet社のFortiGateやF5ネットワークス社のBIG-IP、アンリツネットワークス社のPureFlowやCISCO社のルータ・スイッチなどを採用しています。

これら機器は、仕様・設定方式・アクセスプロトコル・実行多重度が異なります。適切なネットワークサービスを実現するためには、機器間で一貫した設定がされているかを管理・制御する必要があります。これらを適切に制御したうえで、ネットワークサービスの払い出し自動化・セルフサービスポータル化を実現するために開発した機能を「SDN自動化機能」と呼んでいます。

SDN自動化機能は、機器ごとに異なる設定方式やアクセスプロトコル、認証方式を隠ぺいするSDK層、SDK層を組み合わせて機器のシーケンスを制御するシーケンス層、複数のシーケンス層を制御して設定を行うためのネットワークサービス層から構成されます。

利用者によるセルフサービスポータルでの操作はネットワークサービス層に引き継がれ、適切な多重度・シーケンスで複数の機器に対する処理が行われます。機器ごとに異なる仕様や設定方式の差は、ここで吸収されます。利用者は共通化されたセルフサービスポータルでのGUI操作をすることで、個別機器への煩雑な設定を実施することなく、ネットワークサービスを利用することができます。

9. おわりに

本稿では、NEC Cloud IaaSで提供している「多様なネットワーク環境を実現するネットワークサービス」について紹介しました。多種多様な機器とSDNを活用し、「幅広いラインアップ」「利用者に対する柔軟なネットワーク構成の解放」「オンデマンド性」を実現しています。今後も、変化の速いICT・クラウドの世界に追従し、利用者の需要に応じたネットワークサービスの拡充・向上に努めます。

執筆者プロフィール

籾山 奈々子
SDN戦略本部

滝口 敏行
SDN戦略本部

荒久田 博士
SDN戦略本部
主任

清水 昭彦
NECソリューションイノベータ
第三ソフトウェア事業部
マネージャー

菅野 洋太郎
NECソリューションイノベータ
UNシステム事業部
マネージャー

水島 一紀
NECソリューションイノベータ
UNシステム事業部
主任

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.67 No.2　ICTシステムを担うこれからのクラウド基盤特集

ICTシステムを担うこれからのクラウド基盤特集によせて
NECのクラウド基盤への取り組み

◇ 特集論文

NEC C&Cクラウド基盤　NEC Cloud IaaSのサービス
マルチ環境統合を実現するポータルサービス
多用途環境に対応するハイブリッド型サーバサービス
多様なネットワーク環境を提供するネットワークサービス
内部統制手法を活用した堅牢なセキュリティサービス
クラウド基盤を支えるデータセンターサービス

NEC C&Cクラウド基盤を支える製品、最新技術
運用の自動化によりトータルコストを最適化する「WebSAM vDC Automation」
運用自動化により効率的な管理を実現する統合運用管理基盤
データセンターのTCO削減に貢献するマイクロモジュラーサーバ及び相変化冷却機構
クラウド環境に適した高信頼基盤を提供するiStorage M5000
データ保存に最適な、優れた圧縮効率と高速性を両立するiStorage HSシリーズ
大規模データセンターの管理自動化をサポートするSDN対応製品 UNIVERGE PFシリーズ
省電力を実現する相変化冷却技術・熱輸送技術

NEC C&Cクラウド基盤の将来技術
低コスト・省電力・低フットプリントを実現するアクセラレータ活用技術
スケールアップにより多種多様なコンピューティングを実現するResource Disaggregated Platform
クラウド環境を対象にしたモデルベース設計支援技術
モデルベースでのサイジングと構成管理によりクラウド上のSIを効率化するクラウド型SI
ビッグデータ分析とクラウド ～異常を見抜くインバリアント分析技術～

導入事例
クラウドで遠隔監視保守システムの安定稼働を実現　全国約1,100基のタワーパーキングの安全を支える
ビジネスの中核を担うシステムをNEC Cloud IaaSへ移行　NECのトータルサポート力を評価
クラウド基盤サービスでグループのIT環境を共通化　ITガバナンスのさらなる強化を目指す

◇ NEC Information

C&Cユーザーフォーラム&iExpo2014
Orchestrating a brighter world　世界の想いを、未来へつなげる。
基調講演
展示会報告

NEWS
2014年度C&C賞表彰式典開催

Vol.67 No.2
(2015年3月)

特集TOP