

Software-Defined Network によるネットワークの刷新

Complete Reform of the Network by Software-Defined Network

池 上 公 也, 江 沢 佳 則

要 約 企業システムのデータセンターへの移行が加速する中で、データセンター事業者やクラウドサービス事業者においては、ますます大規模化、複雑化するネットワークをいかに効率的に統合管理していくかが課題となってきた。

本稿では次世代データセンターネットワーク技術として注目を集めているSDN (Software-Defined Network) の必要性和、その有効性について、要素技術である VXLAN とともに紹介する。また例として実際の製品 (Cisco ACI) を用いてデータセンターネットワークの設計構築のアプローチも解説する。

Abstract While enterprise systems rapidly migrate to datacenters, datacenter and cloud service companies struggle to integrate complicated networks for effective management of the network systems.

In this report, we explain the importance and necessity of SDN (Software-Defined Network) which gathering attention as a next-generation datacenter network technology, and also on VXLAN technology. Finally, we argue the design construction of the datacenter network using a real product (Cisco ACI).

1. は じ め に

2008 年ごろから企業情報システムをクラウド化する動きが主流となり、仮想化技術の進歩は各インフラ業界に波及している。ネットワーク業界も 2012 年ごろから SDN (Software-Defined Network) が注目を浴びており、2013 年には NFV (Network Functions Virtualization) の仕様が公開されるなど相次いで技術変革が起きている。

SDN はソフトウェア操作でネットワークの構成/機能/性能を管理するコンセプトの総称であり対象範囲は広い。本稿では SDN がもたらす技術革新により一つのデータセンターネットワークの設計構築から運用管理までがどのように変わるのかを紹介する。特に対象となるデータセンターネットワーク構築において、その必要性和利便性を認識し有効活用していくための変革ポイントを記述する。

2 章 3 章ではデータセンターデザインの変遷とネットワーク仮想化への課題について、4 章ではネットワーク仮想化の要素技術である VXLAN について解説する。5 章で SDN の概要と 6 章では製品実例として Cisco ACI について、7 章では自動化を実現するオーケストレーターについて解説する。

2. データセンターの転換期

従来のデータセンターでは、サーバー/ストレージ/ネットワークの物理リソース制限を考慮しながら専用の企業システムを構築していた。その後、物理リソースを効率的に有効活用するサーバー仮想化やストレージ仮想化が急速に発展していくなかで、ネットワーク仮想化は追随

ができていない状況にあった。

扱われるデバイスの多様化とアプリケーションの変革とともに年々増大していくデータ通信量と、逐次増加し複雑化するサーバー/ストレージ/ネットワークの変更にいかに対応していくかがデータセンターネットワークの課題である。

主要構成要素であるサーバーやストレージだけではなくネットワークも仮想化技術に統合していくには、データセンター全体を柔軟かつ効率的に統合管理できる SDDC (Software-Defined Data Center) デザインが有効である。

3. ネットワーク仮想化の実現

サーバーやストレージでは、一つの物理デバイス上で複数の仮想領域を作り出すことが容易な環境となったため仮想化導入は増加傾向にある。ネットワーク側の設定も比例して頻度・ボリュームが増大することが見込まれる。

その際にデータセンターネットワークで求められるのは仮想化環境が柔軟かつ安全に構築できる機能を持つことである。本章では、ネットワーク仮想化を実現するにあたって解決しなければならない特有の問題点や課題と、ネットワーク仮想化が求められる要因について記載する。また、ネットワーク仮想化が VXLAN 技術を用いた SDN に至る変遷についても述べる。

3.1 ネットワーク仮想化の要求と課題

いくつかの要因によってネットワークの仮想化技術がなかなか普及せず、柔軟な構成変更や最適化がサーバーやストレージと比べて遅れた。本節ではネットワーク機器を仮想化する必要性や、技術上困難であった点を考察する。

3.1.1 制御機能とデータ転送機能

従来のデータセンターネットワークではコントロールプレーン（制御機能）とデータプレーン（データ転送機能）が各ネットワーク機器内で自立分散的に動作していた。そのためネットワーク運用者は各機器一台一台へコンソール接続や Telnet 接続などでログインしてから各機器の確認をする必要があった。そのため膨大な機器数となるデータセンターネットワークでは管理が難しい傾向があった。

3.1.2 ネットワーク階層モデルと拡張の柔軟性

データセンターネットワークで用いられる 3 階層（コア層・ディストリビュート層・アクセス層）モデルではデバイスの特性考慮と、スパンニングツリープロトコルやルーティングプロトコルなどのプロトコルに依存した作業の煩雑さを都度考慮しながらスケールアップ拡張を行う必要があった。

3.1.3 VLAN スケーラビリティ問題

ネットワークの仮想化が出遅れた理由の一つに VLAN 機能を活用してきたことが挙げられる。一つの物理ネットワーク上に構成できる VLAN 数は 4096 個が限界（VLAN-ID 上限が 12bit のため）という制限があったため、特に多くの VLAN 数が必要となるデータセンターネットワークでは足枷となっていた。

3.1.4 アプリケーションアーキテクチャの変遷による広帯域化

従来のデータセンターでは単一のサーバーに複数のアプリケーションが稼働していた。しかし求められるアプリケーション要件が変わり、単一のアプリケーションを複数のサーバーで稼働させることが増えてきている。そのためサーバー間の通信で必要帯域が増大する傾向にある(図1)。

これはクラウド/ソーシャル/モバイル等のアプリケーションを中心とした技術と利用度合いが急速な成長を遂げながら牽引しているためである。それに伴いサーバーアクセスは1Gから10Gへの移行が選択されるようになり、40Gアップリンク利用など広帯域確保が必須要件として求められてきている。

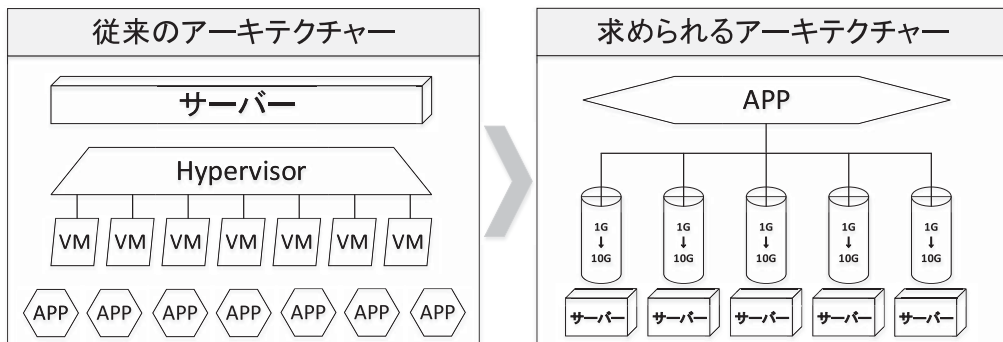


図1 アプリケーションアーキテクチャ変遷

3.2 ネットワーク仮想化の特徴的な要素

ネットワークをソフトウェアで動的に制御するSDNと、物理ネットワークの上に複数の仮想ネットワークを構築するVXLANは、課題を克服するアーキテクチャとして注目を集めている。その根底となるネットワーク仮想化の特徴的な要素を記述する。

3.2.1 制御機能とデータ転送機能の分離

これまでの自律分散型ネットワーク機器では、個々の機器ごとに設定を行い宛先ベースで経路制御を実施していた。ネットワーク仮想化では、個々のネットワーク機器に実装されていたコントロールプレーン（制御機能）を外部デバイスに分離し集約させ、管理者は可視化された各ネットワーク機器を一括管理できるようになった。これはデータセンターに存在する個々の機器に対する管理負荷を軽減する。

そのためネットワーク機器はデータプレーン機能を優先させることができ、コントロールプレーンを簡素化することで設備投資コスト（CAPEX）削減が期待される。またコントロールプレーンでの一元管理ができるという点から、従来かかっていた運用コスト（OPEX）削減も見込める。

3.2.2 ネットワーク階層モデルと拡張への対策

多くのネットワークで用いられてきた3階層（コア層・ディストリビュート層・アクセス層）モデルでは、それぞれの層にあたる機器を上位モデルへリプレイスするスケールアップ方式を

とっていた。しかし機器を横並びに増設していくスケールアウト方式の拡張が可能となったことで、スケールアップ方式に比べてネットワークの停止時間軽減やリプレイスによる通信影響を極小化できる。

3.2.3 作業量増大への対策

仮想化に伴い構成変更が柔軟かつ容易になる反面で、サーバーやストレージの仮想化作業に付随するネットワーク作業が増えてくる。その要件ごとに対象機器を絞り設定作業を行っている。従来のような増設計画ではコストが見合わないことが予見される。ネットワークを仮想化することで効率と安全性を兼ね備えるアーキテクチャーを利用できる。

4. VXLAN (Virtual eXtensible LAN)

2014年の8月にRFC(7348)にて標準化されたVXLANは、従来のVLANが抱える問題を解決するために作られた。仮想のL2ネットワークを物理のL3ネットワーク上に拡張させるトンネリングプロトコルであり、Cisco Nexus/VMware NSX/Nuage VSP/Juniper Contrail/Aristaなどの多くの製品で対応が進んでいる。SDNにおいて仮想ネットワークを実現する要素技術であるVXLANの特徴と機能について紹介する。

4.1 VXLANの登場背景

従来のVLAN技術自体は古い技術であり、ソリューションごとの予約VLANを含めると実質は4096には及ばないVLAN(L2ネットワークセグメント最大)数までという制約問題があった。仮想化技術ではL2ネットワークセグメント識別子の取り扱い数も圧倒的に多くなることから、従来のVLANに内在していた最大の問題を解決するVXLANが標準化された。

4.2 VXLANの特徴

約1600万のセグメンテーションやスケーラビリティとともに、物理構成や既存のセグメントに依存せず利用できるIPモビリティなどを実現できる機能を持つ。Leaf/Spine・3層トポロジー・フルメッシュなど様々なトポロジー展開パターンをサポートするオーバーレイネットワーク技術のコアテクノロジーである。以下の特徴的な技術を用いて大規模なネットワークセグメントを管理することが可能である。

- 1) 元のイーサネットフレームに8byteのVXLAN-Headerを付与
- 2) UDPパケットの中にイーサネットフレームをカプセル化
- 3) VXLAN Network Identifier(VNI)24ビットのIDにて約1600万のVLAN-IDが利用可能
- 4) Virtual Tunnel End Point(VTEP)間でトンネリング

他の手法に比べて既存の物理ネットワーク環境を利用できる点が移行においてもメリットの一つとなっている。SDNコントローラーを用いてVXLAN対応スイッチをVTEP定義し、その間をトンネリングすることで異なるL2ネットワーク(物理またはソフトウェアのスイッチ)を接続させる。つまり従来のVLANで限界値である4096までのセグメントを擬似的にIPネットワークへ透過させることができるのである(図2)。

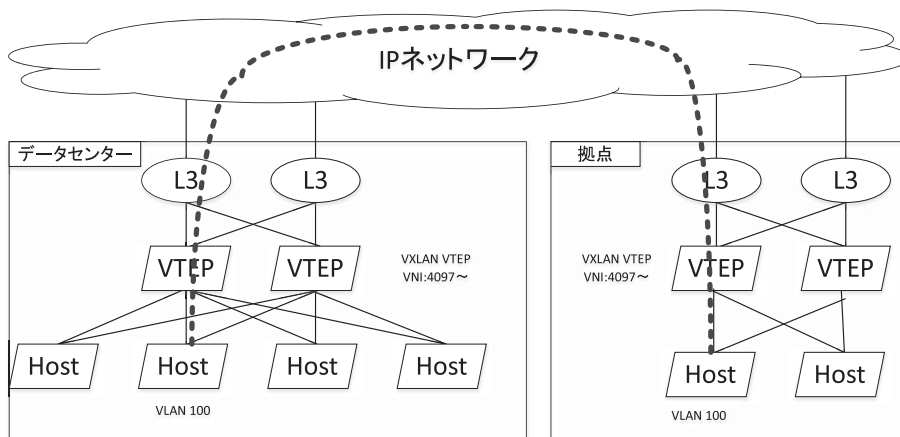


図2 VXLAN の利用イメージ

5. SDN (Software-Defined Network)

SDN とはフレームワークの総称のため定義は困難かつ様々だが、データセンターのように大規模ながらも効率的に複数のテナントを収容させていく状況下で有効な考え方である。そして複雑化されたネットワークをソフトウェアで一括管理して人の手に依らない構築・設定・管理を行う概念のことである。SDN の特徴について紹介する。

5.1 SDN の登場背景

1 台の物理サーバー上に複数の仮想マシンを動作させてリソースを有効活用するサーバー仮想化はコスト低減が期待できて運用管理がしやすい。また利用者にとっても物理サーバーを意識する必要がなくなりモビリティ向上が見込まれる側面も兼ね備えるためによく使われる技術となっている。しかしサーバー側で仮想化を行っても相対するネットワーク側が手動で作業連携を行っているようでは作業工程のボトルネックになってしまう。こうしたギャップを埋めるために SDN が誕生したのである。

5.2 SDN の構成要素

SDN の構成要素は主に 3 種類のレイヤーに分けられる。物理サーバーを集約する「物理スイッチ」または仮想サーバー（仮想マシン）を集約するための「ソフトウェアスイッチ（仮想スイッチ）」が一つ目の構成レイヤーとなる。このスイッチ群のパケット処理方法を制御するためのネットワーク制御・管理ソフトウェアが「SDN コントローラー」と呼ばれる二つ目の構成レイヤーとなる。最後に SDN コントローラー上で「経路計算およびネットワークの論理分割などを実現するアプリケーション」が三つ目の構成レイヤーである。

従来のデータセンターネットワークでは各機器固有の管理ツールを用いて機器 1 台ごとの設定を行っていたが、SDN コントローラーを用いることで管理者は一元管理が可能となる（図3）。

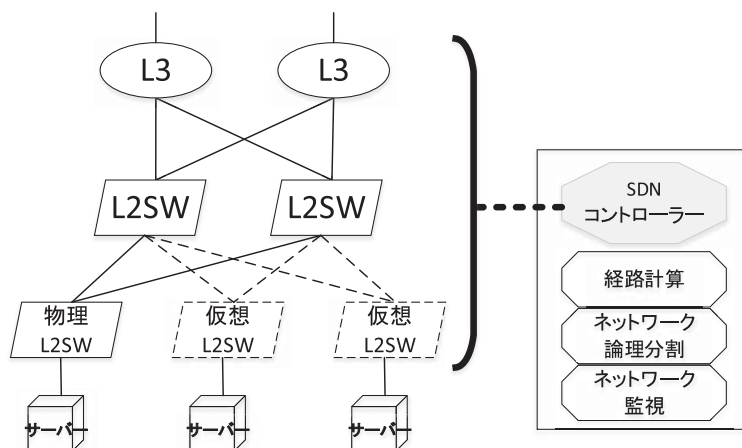


図3 SDN 構成要素

5.3 サウスバンド API とノースバンド API

コントロール（SDN 制御機能）から見て、上流にあたるアプリケーション（機能またはサービス）はノースバンドと呼ばれ、下流にあたるインフラストラクチャー（データ転送機能）はサウスバンドと呼ばれる。ネットワーク内のトラフィック方向を示すノースバンドおよびサウスバンドへのインターフェース操作として API（Application Programming Interface）と呼ばれるソフトウェアが利用される（図4）。

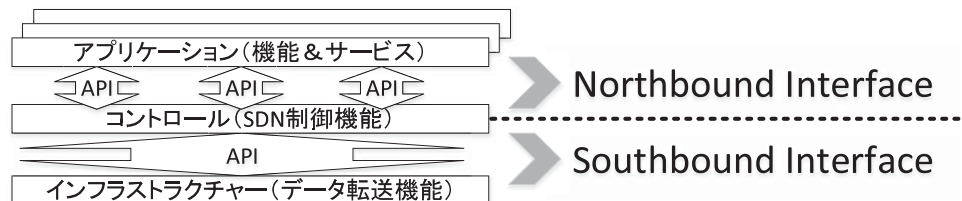


図4 サウスバンド API とノースバンド API

6. Cisco ACI

シスコシステムズ社が提供する ACI（Application Centric Infrastructure）について紹介する。ネットワークの機能や設定を抽象化したプロファイルを用い、アプリケーション視点からポリシーに基づいた自動化を目指すことで、運用・管理を簡素化できる。またデータセンターネットワークの可視化を実現する IaaS 基盤を提供する SDN ソリューションである。

6.1 Cisco ACI の構成要素

Cisco ACI では Spine 層と Leaf 層の 2 階層モデルとなっており、APIC「Application Policy Infrastructure Controller」と呼ばれるコントローラーにて Spine 層と Leaf 層の物理および仮想の両ネットワークを管理する構造となっている。Cisco ACI を構成するネットワーク全体を ACI ファブリックと呼ぶ（図5）。

帯域を増やすには Spine を増強し、サーバー収容数を増やすには Leaf を増設することで容易なスケールアウトが図れる。そのためデータセンターネットワークで一般的な 3 階層モデル

よりも柔軟に増設ができ、スケールアウト時にネットワーク全体への影響を抑えることができるようになった。

データセンタースイッチ「Cisco Nexus 9000」シリーズにて Spine スイッチと Leaf スイッチが提供されており、ACI モードにて 40G のメッシュ接続をさせることで、ファブリックネットワーク上にポリシーベースの VXLAN オーバーレイネットワークを構築する。

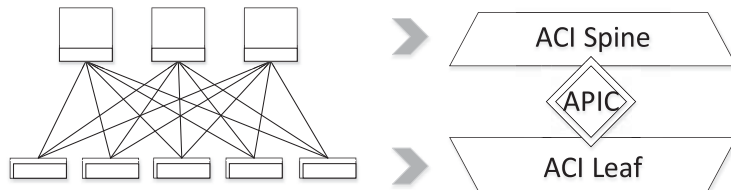


図5 ACI ファブリック

6.2 Cisco ACIの構成方法

テナント内に Application Network Profile を定義し、作成することで ACI ファブリック内の通信が可能となるよう自動化が図れる。具体的には同じ設定ポリシーで扱われるものを EPG（End Point Group）とし、その EPG 間を Contract と呼ばれる接続ルールで結びつけたものである（図6）。

こうして Cisco ACI では必要な通信のみを転送するセキュアな仮想ネットワークを Application Network Profile の単位で簡易に作成できる。

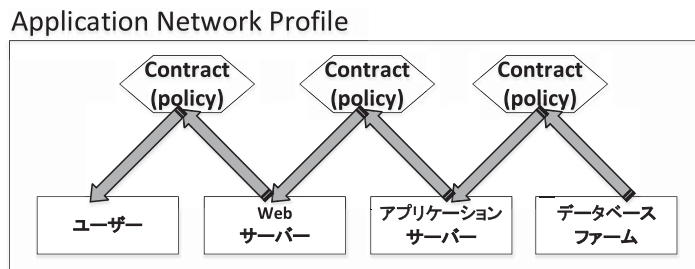


図6 Application Network Profile と Contract の概要

6.3 Cisco ACIの導入による運用変化

アーキテクト・設計・コンピュータ・ストレージ・セキュリティー・ネットワークの要素を定めたポリシーに従って自動化することで、サービスリクエストからアプリケーション稼働までの展開時間を大幅に削減するモデルを構築できる。また ACI ファブリックでは可視化された分析機能があり、ヘルススコアやリソースの利用状況などをアプリケーション・テナント・インフラごとに確認することができる。

従来では管理者が個々のスイッチに Configuration を作成し設定していたが、ACI を用いた場合にスイッチは通信要件が定義されたポリシーを自動で読み込み利用可能となる。

6.4 Cisco ACIの導入アプローチ

既存のネットワークを Cisco ACI で置き換えるのに最も簡単な方法は、既存ネットワークで使用している VLAN を EPG にマッピングすることである。これにより、従来の L2/L3 スイッチと同等の使い方ができる。既存 VLAN と対応する EPG を接続し、既存ネットワークを ACI ファブリックにまで拡張するのである。Cisco ACI 特有のポリシー定義である Application Network Profile の設定をあえて最小限に留めることで、旧来からのネットワーク管理者にも比較的容易に Cisco ACI でネットワーク設計が実施できる。

6.4.1 適用領域と初期構成

Cisco ACI の適用領域としては、データセンターのサーバーファーム、大規模データベース環境、サービスプロバイダーの SaaS・PaaS 環境などが想定されている。また、中規模から大規模な企業ネットワークのサーバーファーム用途にも適用は可能である。

Cisco ACI の初期構成は、Spine スイッチ 2 台、Leaf スイッチ 2 台から構成でき、必要なポート数に応じて Leaf スイッチを増設していくことが簡単にできる。機器構成のサイジングは、Leaf スイッチで必要なポート数を主な目安として機器構成を検討すればよい。

6.4.2 REST API を利用した運用自動化

Cisco ACI が SDN 製品として本領を発揮するのは、APIC に実装されている REST API を用いて、ソフトウェアから直接 Cisco ACI のポリシー定義や運用操作を行うことにある。APIC にはブラウザーベースの GUI があり、通常は GUI を用いて設定操作する。しかしながら運用の自動化、効率化を図るには、REST API を用いて運用操作を行うことになる。REST API は python 言語で独自にプログラミングすることもできるが、オープンソースで用意されている ACI toolkit を用いるのが有効である。ACI toolkit には python 言語のサンプルコードを含むライブラリが多数用意されていて、そのままでも利用できるが、サンプルコードをカスタマイズして実環境に合わせたコードを作成することで、自動化・効率化に大いに役立つのである。ACI toolkit を利用したスクリプトの実行により、テナント作成、ポリシー設定や運用操作を実行する。これをオーケストレーションソフトウェアから自動実行することで、運用の自動化を実現する。

7. オーケストレーションソフトウェア

データセンターネットワークで主軸となる SDx (Software-Defined Anything) 技術を、領域ごとではなくオーケストレーションソフトウェアで統合的に扱う概要を紹介する。

ネットワーク/コンピュータ/ストレージの各 SDx インフラストラクチャー領域をソフトウェアで統合管理するためには、オーケストレーターが必要となる。ソフトウェア管理になることで仮想および物理の各構成機器を扱うことが可能となり、管理画面も可視化されシステムインテグレーションや運用にかかるコストを低減することができる (図 7)。

シスコシステムズ社では紹介した ACI や同社の Cisco UCS サーバーを一元管理できるインフラストラクチャー向けオーケストレーションソフトウェアとして UCS Director も提供している。

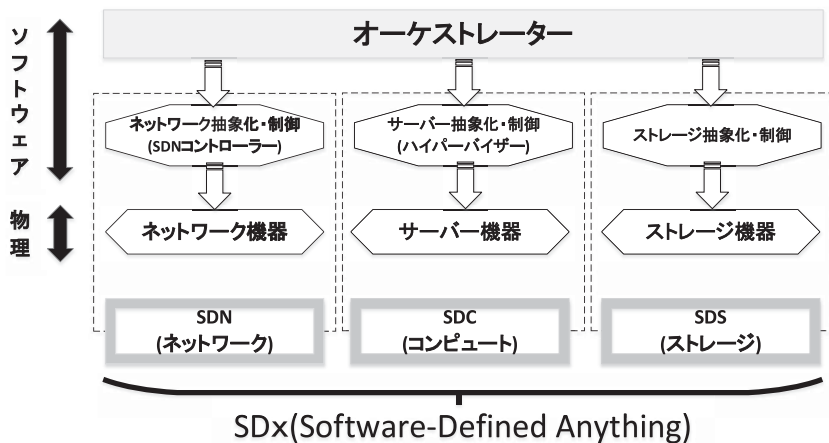


図7 オーケストレーターとSDxの連携概要

8. お わ り に

データセンターネットワークの仮想化への変遷と、SDN 商品の一つとしてシスコシステムズ社の提供する ACI を紹介した。今後は SDN やオーケストレーションソフトウェアとも連携し一つのデータセンター内でより効率的な活用が見込まれる。また複数データセンターのクラウド環境を連携させるような自律型データセンターの必要性が高まっていくことが予想される。

その中でユニアデックスは、次世代データセンターネットワークに必要な様々な SDN 技術の推進に取り組み、データセンターネットワーク管理や運用に悩みを抱えた顧客へアドバンテージを提供していきたい。

-
- 参考文献** [1] データセンター デザイン：IP ネットワーク インフラストラクチャー - Cisco
<http://www.cisco.com/web/JP/solution/netsol/designzone/datacenter/literature/pdf/OL-19225-01-J.pdf> (2015/09/30 アクセス)
- [2] Application Centric Infrastructure (ACI) ユニファイドファブリック - Cisco
http://www.cisco.com/web/JP/solution/datacenter/unified_fabric/app-centric-infrastructure.html (2015/09/30 アクセス)

執筆者紹介 池 上 公 也 (Kimiya Ikegami)

1990 年日本ユニシス(株)入社。UNIX 通信ソフトウェアの開発に携わる。1997 年よりユニアデックス(株)でネットワーク設計業務に従事。キャリアー商用ネットワークやデータセンターネットワークの設計を行う。2011 年よりネットワーク製品技術主管として製品サポート業務にあたる。シスコ認定 CCIE。



江 沢 佳 則 (Yoshinori Ezawa)

2001 年ユニアデックス(株)入社. ネットワークエンジニアとして主にキャリア法人や金融系顧客を中心に設計業務を担当し, 2010 年よりクラウドプロジェクトに参加した. 2013 年よりサーバー設計構築・技術主管に従事しており, データセンターネットワークに関連するサーバービジネス拡大に取り組む.

