データセンターネットワーク
リファレンスガイド

日本データセンター協会

2014 年 1 月

（第 2 版）

目次

１．はじめに

2011 年 3 月に発生した東日本大震災では、ツイッターをはじめとするインターネット上のソーシャルネットワークが人々の安否情報や被害状況確認など、多くの人の役にたったことは記憶に新しいところです。インターネットは情報共有の手段として、もはや人類に必須のものとなり、言い換えれば社会インフラ化したといえます。

インターネットは人やモノをつなぐ有線あるいは無線のネットワーク、およびそれらを制御し情報を蓄える役目を担うデータセンターから構成されています。インターネットが社会インフラ化したことにより、必然的にデータセンターも社会インフラの一つとして認識されるようになってきました。

技術的観点から見ると、近年データセンターは、クラウド化の流れにより仮想化技術の導入が急速に進んでいます。サーバやストレージなどのデータセンターを構成する IT 機器はコモディティ化が進んでおり、仮想化技術を採用することで、サービスを迅速にかつ低価格に提供することが可能となるからです。

一方で、データセンターのネットワークを見てみると、サーバ・ストレージに比べてネットワーク構成のダイナミックな変更が難しい、従来敷設したケーブルが足かせになり、機器の追加が思うように進まない、などの課題が残っています。また、災害対策・ビジネスコンティニュイティの観点から、複数のサイトを接続し、あたかも一つのデータセンターとして扱うことを可能とする広域データセンター構想に対応したネットワーク設計が求められるようになっています。

このような状況を踏まえ、日本データセンター協会・ネットワークワーキンググループでは、これから社会インフラとしてますます重要性が高まるデータセンターにおいて、ネットワークの設計・運用を担当されている方、ネットワークの観点で技術動向を収集されている方、および同事業の意思決定者の方を対象に、データセンターネットワークに関する最新の技術トレンドを網羅的・体系的に通りまとめ、データセンターネットワークリファレンスガイド（本書）としてまとめることにしました。

本書にはネットワークの課題と、これを解決する一般的な解決策が記載されています。解決策が明確となっていない項目については、技術的な課題解決の選択肢とメリット、デメリットとして記載しました。

また、本書は事業者の運営するデータセンターを想定して記載されており、一般企業が運営しているデータセンター（マシンルーム）は想定外となっていますが、今後データセンターを活用する可能性のある企業の方は参考にすべき内容です。

本書をご覧いただくことで、ご自分のデータセンターネットワークの課題を抱えられている方が解決に向けた糸口をつかんでいただくことはもちろん、課題を感じておられない方においても解決すべき課題が見出せる可能性があるため、本書を一度ご覧いただければ幸いです。

日本データセンター協会・ネットワークワーキンググループ一同は、本書が皆様のデータセンターにおいてネットワークの設計・運用を効率的に行うための一助となることを希望します。

日本データセンター協会
ネットワークワーキンググループ一同

２．最新データセンターネットワークの全体像

本章では最新のデータセンターネットワークの全体像を把握することを目的とし、これまで辿ってきたコンピューターシステムの変遷とそれに伴ったデータセンターサービスの種類を整理するとともに、これを受けたデータセンターネットワークの要件と課題について明確化します。

２－１．コンピューターシステムのトポロジーの変遷

(1)メインフレームの時代・・・集中管理・集中処理

現在のコンピューターシステムは、1980 年代に IBM を始めとするメインフレームベンダの台頭が普及の原点と言っていいでしょう。メインフレームとは巨大な１台のコンピューターであり、これを複数のダム端末からタイムシェアリングという技術で共有するシステムです。

また、メインフレームは非常に高価なものであったため、1 台のコンピューター上で複数のソフトウェア・サービスの稼働を可能としていました。これはまさに現在の Hypervisor であり、サーバ仮想化そのものです。実はサーバ仮想化は新しいようで古くからある技術なのです。

(2)Web コンピューティング・クライアントサーバの時代・・・分散管理・分散処理

1990 年代に入ると、UNIX などのオープンシステムの価格性能比が飛躍的に向上し、メインフレームから UNIX へのダウンサイジングの流れがはじまりました。時同じくしてパソコンが急速に普及し Web ブラウザが利用されるようになると、本格的なインターネット時代に入りました。

さらに、インターネットの企業利用が本格化すると、UNIX をサーバ、パソコンをクライアントとして利用し LAN で接続するクライアントサーバモデルのシステム構成が企業で主流となりました。このため、急速に増加したサーバをまとめて収容する必要が出てきたため、現在のデータセンターの原型が生まれました。

このような経緯で、データセンターには複数の物理サーバが設置されるようになりました。

(3)クラウドコンピューティングの時代・・・集中管理・分散処理

その後、2000 年代前半から現在にかけて、サーバコンピューターの価格性能比が飛躍的に向上し、VMware などに代表される Hypervisor 型のサーバ仮想化製品が成熟してきました。ある調査によると、トラフィックやアプリケーションの性質により、サーバファーム(複数のサーバを設置した状態)における個々のサーバ利用率は約 15%であるという統計が出ており、このような多くの利用率の低いサーバが設置されることで、データセンター使用料（電力・空調費など）がかさみ、多くの出費につながることになりました。

従ってデータセンターに設置されるサーバはより効率化が求められるようになり、Hypervisor により物理サーバ上で CPU、メモリー、I/O リソースを複数の仮想マシン(Virtual Machine;VM)で共有するサーバ仮想化が積極的に利用されるようになってきま

した。また、データセンターサービスも高度化し、個々の企業でサーバを購入する形態に加え、サーバリソースもデータセンター事業者で用意するサービスも増えてきました。

このような流れで、いつでも、好きなだけ、必要なサーバリソースが直ちに利用可能となるクラウドコンピューティングが主流になりつつあります。前述の通りクラウドコンピューティングに欠かせない技術の一つとして仮想化が挙げられます。

仮想化によりリソース効率化はもちろん、VM のライブマイグレーション機能などを活用すれば障害やメンテナンスなどにおけるサービスのダウンタイムを最小限に抑えられるようにもなります。クラウドコンピューティングの利用がさらに拡大する環境が整いました。

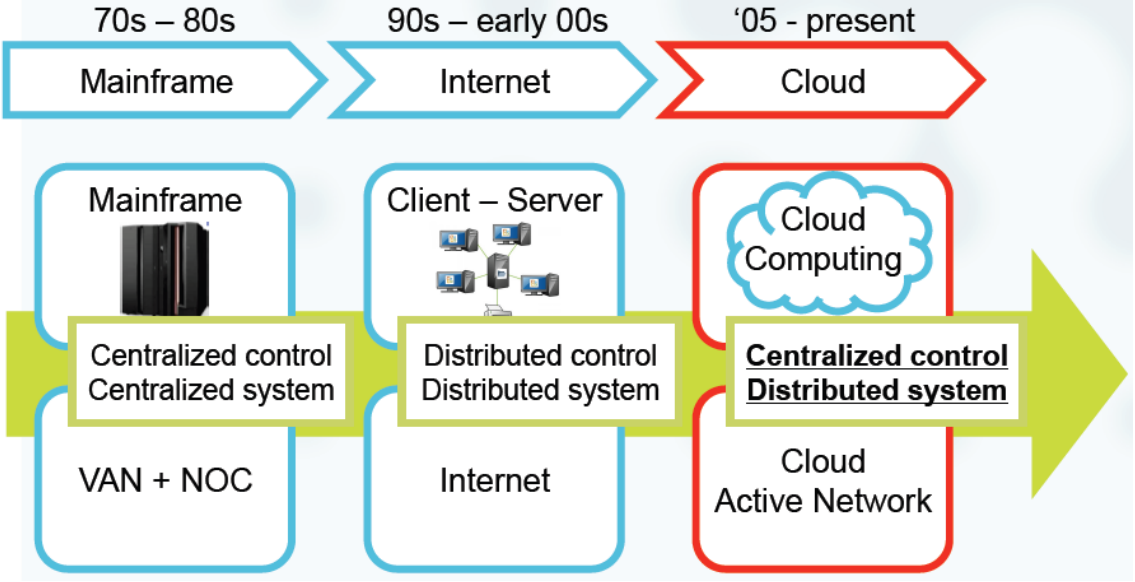


図 2-1　コンピューターシステムの変遷

・　1；2011/12/05 JDCC ネットワーク WG Midokura 社 発表資料より引用

２－２．データセンターサービスの種類

コンピューターシステムのトポロジーの変遷に対応して、データセンターサービスの形態も進化し、現在では下記の通り多様なデータセンターサービスが提供されています。

(1) ハウジングサービス

コロケーションサービスとも呼ばれ、データセンター事業者が敷地内のスペースを契約者に提供し、利用者はそのスペースを利用してシステムの開発や構築を行うことができるサービスです。その他、インターネット接続などのネットワークサービス、電源・空調関連サービス、ラックの運用・監視・保守や緊急対応などのサービスも提供しています。

⑵ホスティングサービス

契約者に対して、サーバの運用・管理などの負担不要でサーバ機能（HDD や CPU）を提供するサービスです。1 台のサーバを複数の利用者で共有するシェアードホスティングサービス、物理的にサーバ機を占有できる形態の占有ホスティングサービスが存在します。

契約者はサーバ自体やラック、電源・空調などの管理を意識せずにサーバ機能を利用できるのが特徴です。

⑶クラウドサービス

全ての機能をまるごとサービスとして提供するクラウドサービスには以下の通り主に 3 つのメニューがあります。

① SaaS(Software as a Service)

サービス利用者はクラウド上でサービスプロバイダが提供するアプリケーションを利用します。

利用者側ではアプリケーションが動作している OS やハードウェア、ネットワーク設定などを行なう必要がなく、すべてサービス提供者側で行います。

② PaaS(Platform as a Service)

サービス利用者はクラウド上でサービスプロバイダが提供するホスティング環境を利用し、サービス利用者自身が用意したアプリケーションを使用します。

SaaS 同様、基本的に利用者で OS やハードウェア、ネットワークのコントロールを行う必要はありませんが、アプリケーション設定や一部の環境設定（アプリケーション　フレームワークなど）が利用できるサービスもあります。

③ IaaS（Infrastructure as a Seivice)

サービス利用者はサーバリソース（vCPU, メモリー, HDD など）やストレージ、ネットワークなどのインフラリソースを自らコントロールし、その上で OS やアプリケーションも含め、任意のソフトウェアを導入することができます。

サービス利用者はクラウド自体の管理を行う必要はありませんが、クラウド上で動作する OS やストレージや一部のネットワークの機能（ロードバランサや FW など）の設定を行う必要があります。

【参考】SaaS, PaaS, IaaS の責任分界点について

サービス提供者と利用者はクラウドシステム上のリソースの管理を共有します。下記の図では各サービスモデルよってクラウド提供者とクラウド利用者がサーバ上のリソースの管理（設定）の範囲を示したものです。それぞれのサービスモデルによって、アプリケーション層、ミドルウェア層、や OS 層まで管理が可能となる範囲が異なります。このように各サービスモデルはそれぞれの階層によって責任分界点が分かれているということが言えます。

サーバ機能のみならず、インフラ部分（ロードバランスやファイアウォール、DNS な

ど)のコントロールやサーバ機能(VM)の移動も柔軟にできるようになっています(IaaS)。また、OS やミドルウェアのプラットフォームが予め組み込まれた形でサービスが提供される PaaS やアプリケーションソフトをサービスとして配布し利用できるようにした SaaS などのサービス形態もあります。

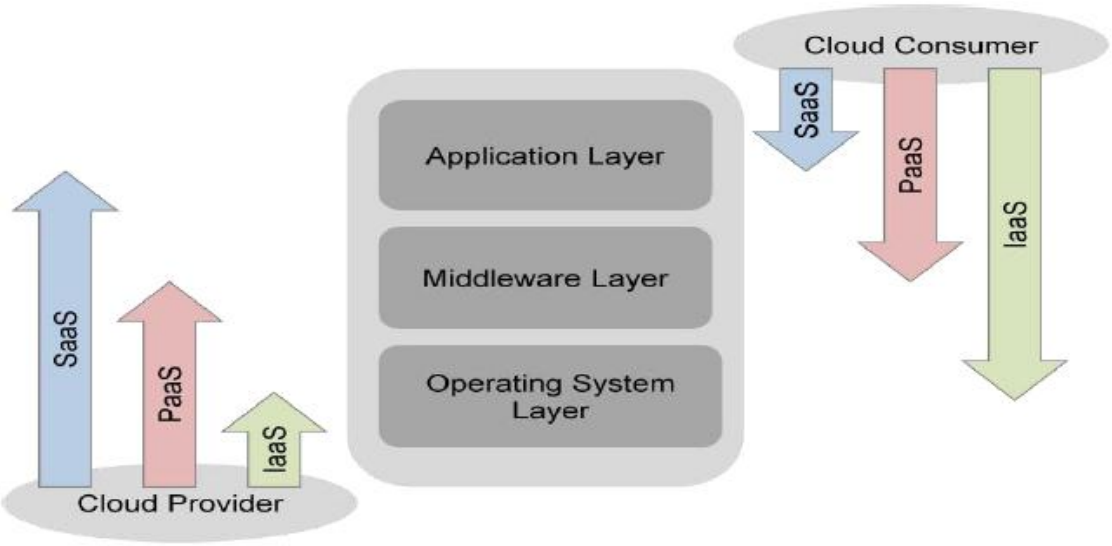


図 2-2　SaaS, PasS, IaaS の責任分界点[1]

[1] NIST 発行" NIST Cloud Computing Reference Architecture"より引用。

２－３．サービス利用者から見たクラウド種別

これまで述べたクラウドサービスを、今度は利用する側の視点で分類します。クラウドサービスには様々な活用形態がありますが、大きく分けてパブリック、プライベート、およびハイブリッドの 3 種類に分けるのが一般的です。

また、それぞれの形態において、クラウドを管理する基盤（ミドルウェア）が必要となり、利用者は ID パスワードなどによる認証を行って当該クラウドを利用することが可能となります。このクラウド基盤はネットワークと直接関係ないため、本書ではあまり触れませんが、効率的な運用を行うための自動化・一元管理、およびセキュアな運用を実現する機能や、課金を行うテナント(顧客)管理機能が求められます。

(1) パブリッククラウド

サービス利用者にとって外部のデータセンター内のサーバから受けるクラウドサービスを「パブリッククラウド」と呼びます。パブリッククラウドでは全てのインフラの管理をサービス提供者側が行います。

利用者は実際に利用したリソースに対して利用料金を支払うという課金方式が一般的

に取られています。特に中小規模の企業、あるいは大企業の部門組織での利用に適しています。

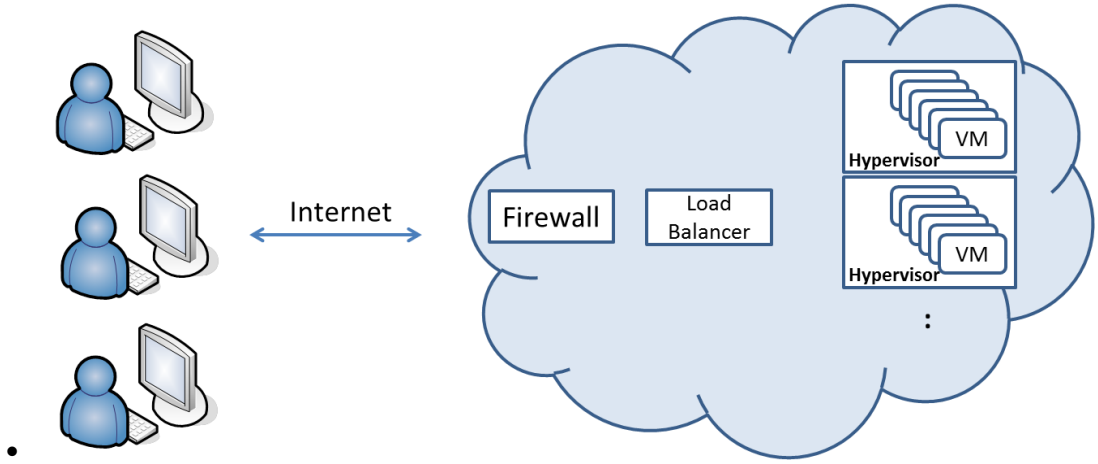


図 2-3a　パブリッククラウド

(2) プライベートクラウド

企業の IT 部門自身が所有するデータセンター内でクラウドサービスを提供するものを「プライベートクラウド」と呼びます。

この形態を取る理由としては、主にセキュリティ面で外部の企業にデータを預けたくないなどや、インフラを自らコントロールしたいなどの理由があります。すなわち、冗長性、拡張性、マイグレーションの面でクラウド技術自体が企業内においても有効であるということが言えます。また、IT 部門は利用状況に応じて、負担部門に費用を請求します。全社・グループ企業間レベルの大規模な企業において、より厳密なコスト管理とサーバリソースの効率化を図ることができます。

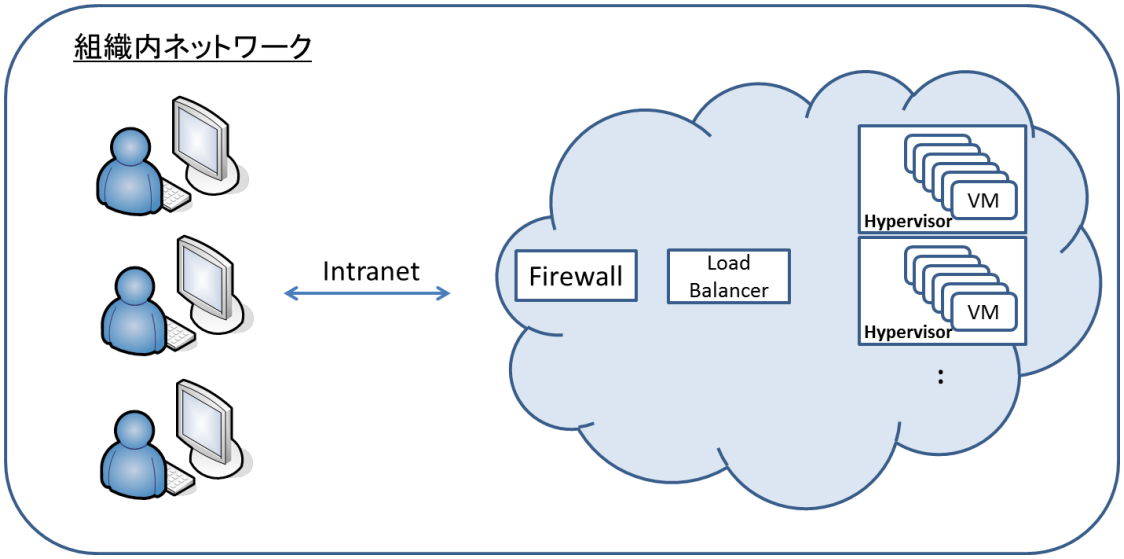


図 2-3b　（オンサイト）プライベートクラウド

(3) ハイブリッドクラウド

パブリッククラウドとプライベートクラウドの特性を必要に応じて使い分け、双方のメリットを最大限に利用したクラウドを「ハイブリッドクラウド」と呼ばれています。
セキュリティ面や柔軟性を求められないサービスにおいてはパブリッククラウドを利用し、個人情報などセキュリティを求められるデータを取り扱う場合はプライベートクラウドを利用するといった使い方が考えられます。

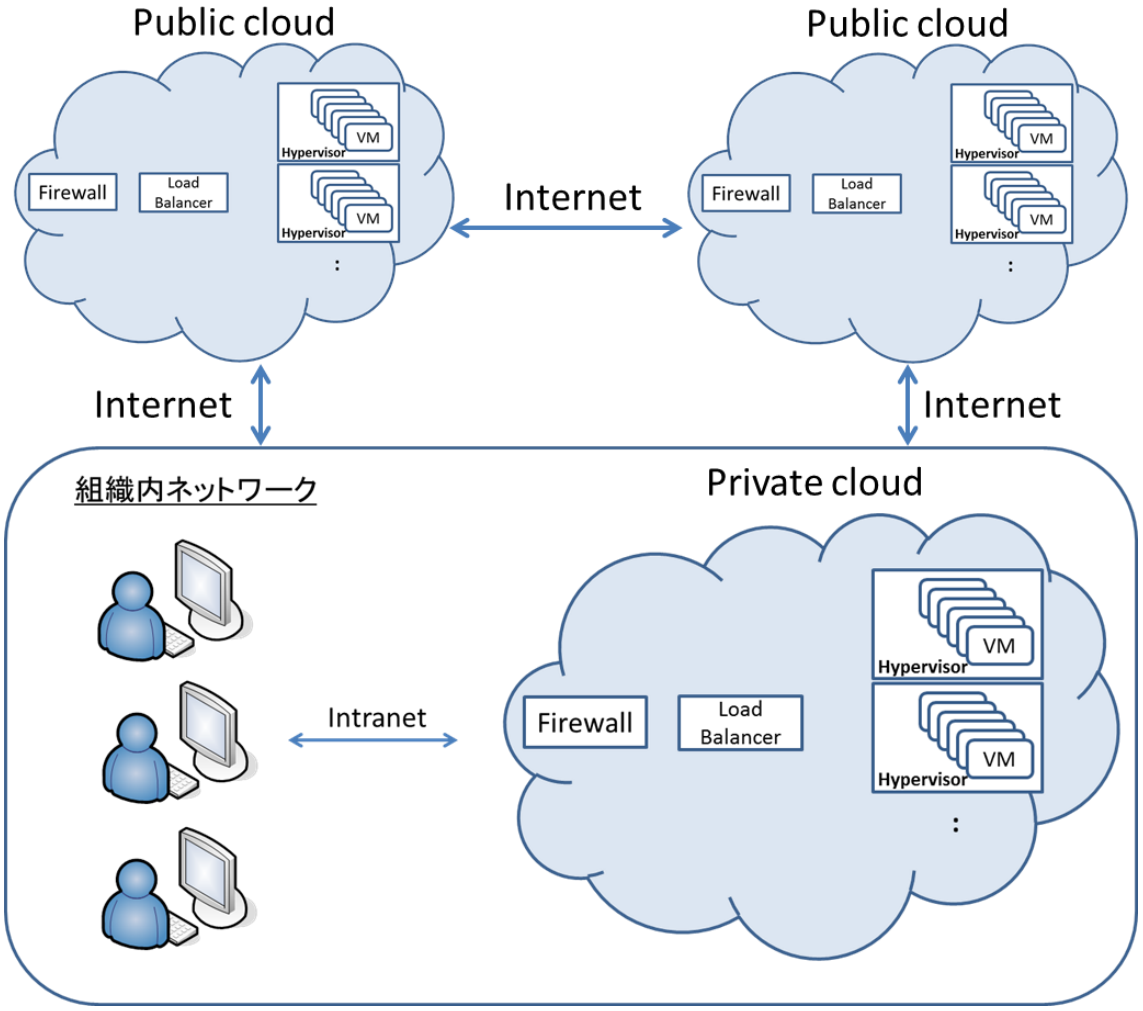


図 2-3c　ハイブリッドクラウド

(4) その他の形態

前述の (1) プライベートクラウドでは、利用者の組織内で構築する「オンサイト」プライベートクラウドとして定義しましたが、プライベートクラウドを外部のクラウド提供者に委託する、「アウトソース」プライベートクラウドのような形態も存在します。

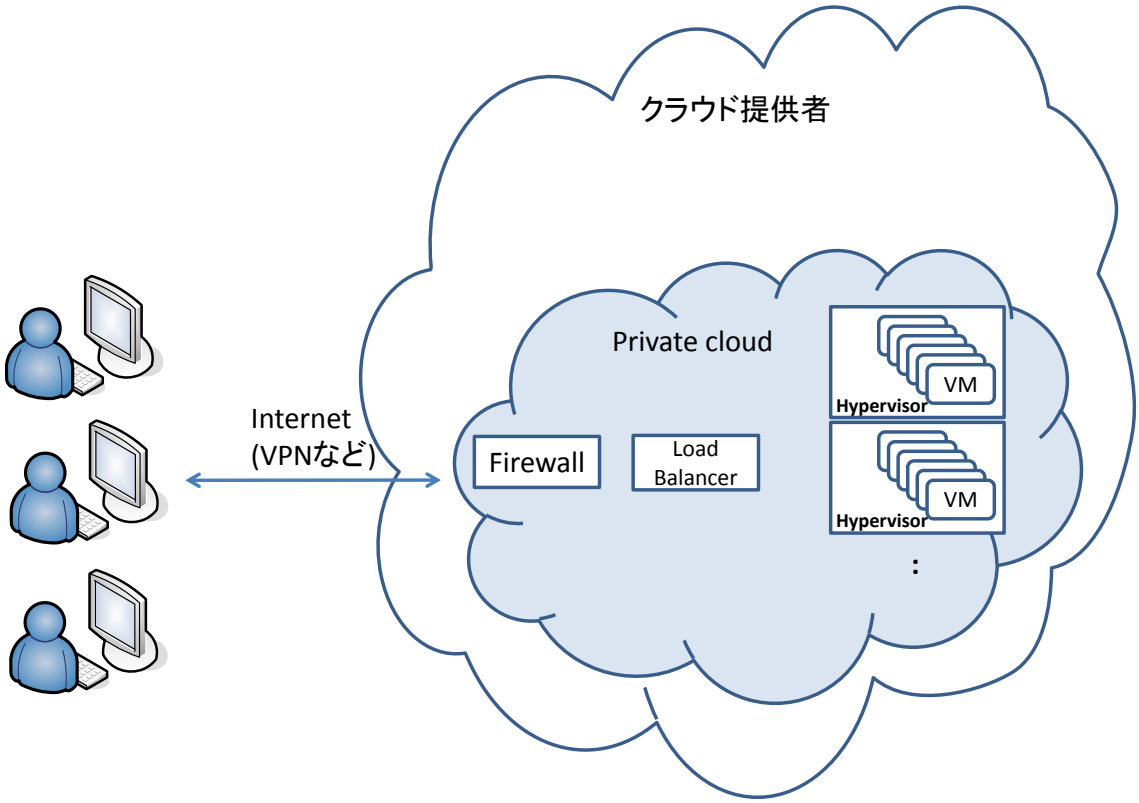


図 2-3d　（アウトソース）プライベートクラウド

２－４．クラウドネットワークに求められる要件

クラウドサービスの提供が一般化した現在では、データセンターにおいて、ネットワーク上で多種多様なサービスが同一プラットフォーム上で提供･運用されることを想定しておく必要があるとともに、様々な利用者により運用がなされることも想定しなければなりません。

ゆえに求められる要件としては、下記が挙げられます。

- ･安定性（可用性）
- ･信頼性
- ･セキュリティ
- ･設定の容易性（最小限の努力での設定）

また、場合によっては下記のような要件も求められます。

- ･サービスに必要なトラフィックを適切に捌くことができる。
- ･DC 内における LAN およびストレージネットワークにおいて低遅延であること。
- ･VM の増減や移動がネットワークに影響を及ぼさないこと。

２－５．データセンターネットワークの課題

前述の通りクラウドサービスの提供を担うデータセンターには、突然の高負荷や、利用者の増減に対応可能なシームレスなサービス拡張や変更とともに、利用者の負担が少ない機能修正や機能追加、負荷に応じた ICT リソースの柔軟な制御を行う必要があります。このような状況において、データセンターネットワークには以下の課題が生じています。

(1)ネットワークの複雑さ

昨今のデータセンターでは、帯域制御装置やファイアウォール、ロードバランサをスイッチで多段に接続した複雑な構成によりサービスを提供しています。その複雑なネットワーク構成をいかに効率的に管理するかが課題となっています。また、障害時にもなかなか障害点にたどり着かず、解決に多くの時間を費やすことも課題です。

(2)サービスプロビジョニングへの対応

急変する市場の声に対応すべく、新たなサービスを迅速に立ち上げる必要が生じるため、この際に物理・仮想サーバや利用者を追加することになります。これにともない、各ネットワーク機器の設定変更をその都度個別に実施することとなりますが、この設定変更をいかに省力化するかが課題となっています。

(3)仮想マシンのマイグレーションへの対応

サーバリソースは仮想化が進み、柔軟に仮想サーバを生成、移動、消去することが可能となりました。ところが、ネットワークの設定変更にはまだ非常に煩雑なオペレーションを経なければなりません。特にサーバ仮想化では、仮想マシンが稼働中に異なる物理サーバに乗り移るライブマイグレーションという機能を実装しているため、ネットワークも動的に設定変更を行う必要がありますが、これに対応するソリューションはまだ未成熟な段階です。

(4)マルチテナント対応

リソースの効率化の観点から、複数利用者が一つの物理リソースを共有するタイプのサービスを提供する場合、マルチテナントと呼ばれる利用者管理も必要になります。ネットワークの観点でマルチテナント管理をセキュアに行う必要があります。

(5)トラフィック予測

従来のネットワークでは、特定用途で利用するサーバあるいはサーバファーム単位で配置しているケースが多いため、トラフィックの流量や傾向をある程度予測することができました。それに対してクラウドの環境では、仮想サーバ単位でトラフィックが発生し、また、動的に仮想サーバがネットワークを移動することにより、トラフィックの予測が難しい状況となっ

てきています。

	従来ネットワーク	クラウドネットワーク
ノード	物理サーバ	仮想サーバ
配置	（ほぼ）固定	流動的
トラフィック傾向	予測しやすい	予測が難しい

(6) ネットワークの継続性（BCP）対策

ネットワークの継続性（BCP）対策として複数のデータセンターを跨ってクラウドを構築する場合、下記のいずれかの方法を検討していく必要があります。

- 利用者が意識せずに適切なデータセンター（サーバ）にトラフィックを誘導する仕組み。
- データセンターでメンテナンスや障害が発生した場合など、データセンター間で仮想サーバを移動する仕組み（ライブマイグレーション）。

３．最新技術動向と具体的なソリューション

本章では前章で整理したデータセンター構内のネットワークの要件と課題に関し、最新技術動向を踏まえながら課題解決に向けたアプローチ手法を解説するとともに、解決策が複数存在する場合には選択肢とメリット、デメリットとして記載します。

本章は以下５つの章から構成されています。

なお、本章に記載の内容はいずれもデータセンター内ネットワークに関するもので、複数のデータセンターをまたがる広域ネットワークについては４章ならびに５章を参照下さい。

３－１．トポロジー
本章で記載するデータセンターネットワークの基本構成を規定しています。

３－２．物理ネットワーク
ケーブルおよびケーブル配線にかかわる項目を記載しています。

３－３．論理ネットワーク
サーバ仮想化に対応するネットワークの仮想化について記載しています。

３－４．運用管理
ITILv3 をベースに標準的なネットワークマネジメントのあり方を記載しています。

３－５．トラフィックマネジメント
急な負荷変動に対応するための技術的なポイントについて記載しています。

３－１．トポロジー

クラウドサービスを提供するデータセンターを構成するトポロジーとしては、下記が挙げられます。

・物理サーバ（Hypervisor、VM）
  - 利用者側サービス（コンテンツ配信サーバなど）
  - サービス提供側サービス（管理系サーバ、クラウドコントロール用サーバ、DB など）
・NW 機器
  - ボーダルータ（Internet 接続部分）
  - コアスイッチ（Aggregate スイッチ）
  - エッジスイッチ（Access 、TOR スイッチとも呼ばれる）
・　アプライアンス、その他
  - ファイアウォール
  - ロードバランサ
  - DNS サーバ（GSLB 機器など）
・　ストレージ

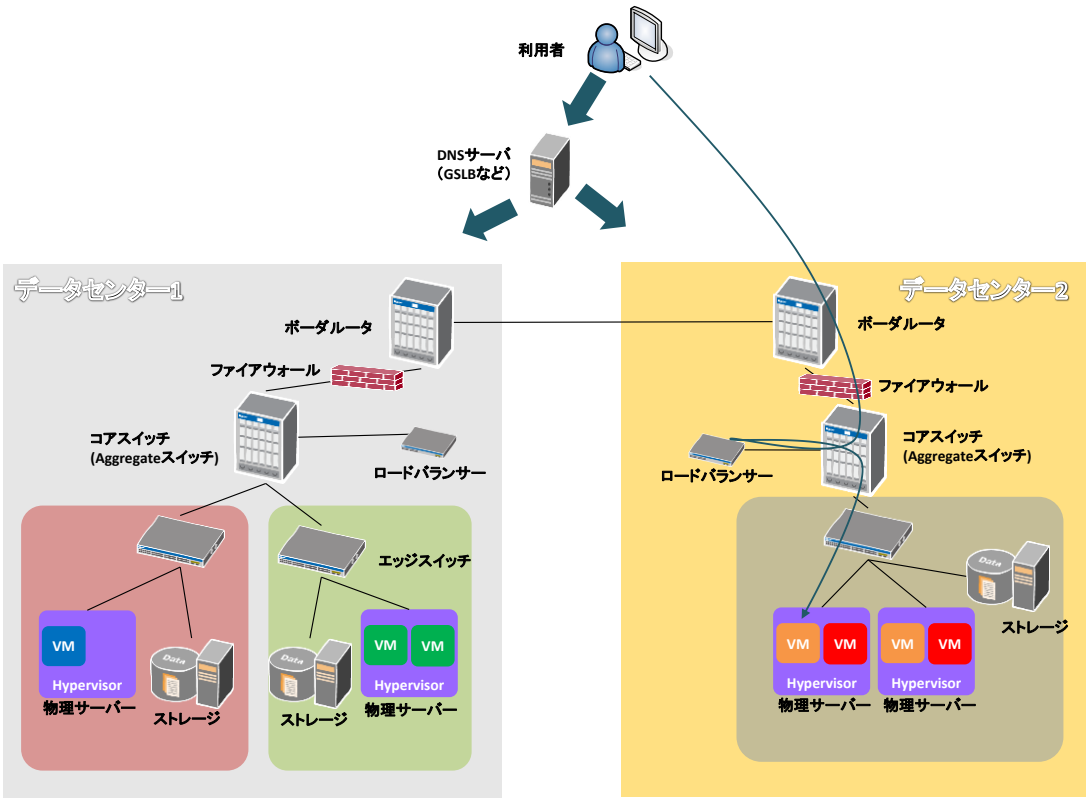


図 3-1　データセンターネットワークの構成要素

３－２．物理ネットワーク

データセンターは更なる環境負荷低減を目指した環境配慮型のデータセンターが多くなってきています。この背景には、省エネルギー、CO2 排出量低減を推進することがデータセンター事業者の社会的責任としての側面を持つようになったことがあげられます。これらを実現するために高性能設備、高効率運用を提供する設備の導入、状況に応じて冷涼な地域に構える、モジュール構造などの採用と同時に空調の省エネルギー化を進めることなどで低 PUE 値を実現していますが、これらを実現する要素の一つにネットワーク機器を接続する LAN ケーブル、その敷設を含めた配線工事（ケーブリング）、設計（デザイン）、施工が関与することから、本章では、配線部材であるケーブル、ケーブル線材などを交え「物理ネットワーク」とし紹介することにします。

３－２－１．配線構成の考え方

データセンターを設計する際、建物や設備だけでなくケーブルインフラを考える事がとても重要です。データセンターに構築されるケーブルインフラに関する代表的な規格は以下の通りになります。

- ISO/IEC 24764
- ANSI/TIA-942
- CENELEC EN 50173-5
- ANSI/BICSI-002

これらの各規格に共通する考え方は、データセンターが提供する機能・サービスを最適化するために、管理区分や構築要件に応じた階層型モデル(サブシステム)を採用している点にあります。階層型モデルは、各サブシステムが独立したケーブルシステムとして構成されるため、トラブル時の影響を限定化しシステム全体の信頼性を高めると共に、移設や増設等を容易に実現する事が出来ます。また、管理ポイントをサブシステム毎に確立するため、運用管理の最適化と効率化を図る事が出来ます。

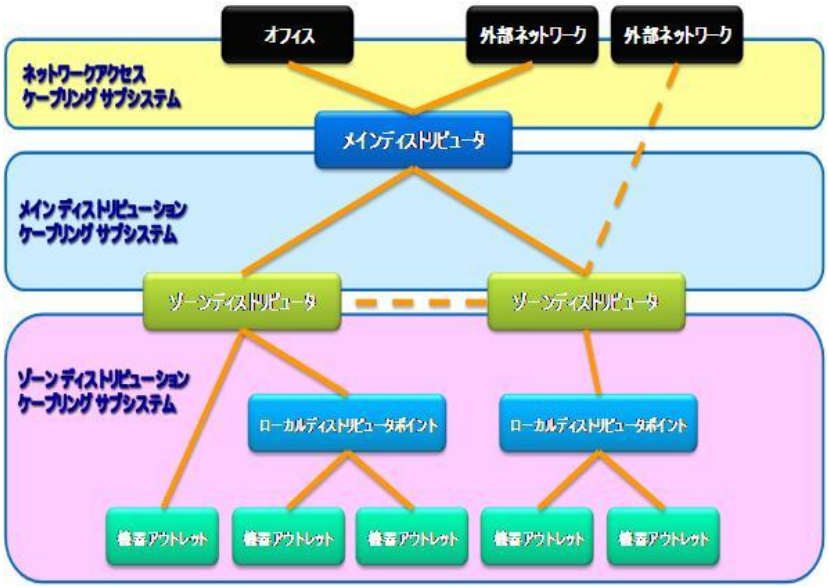
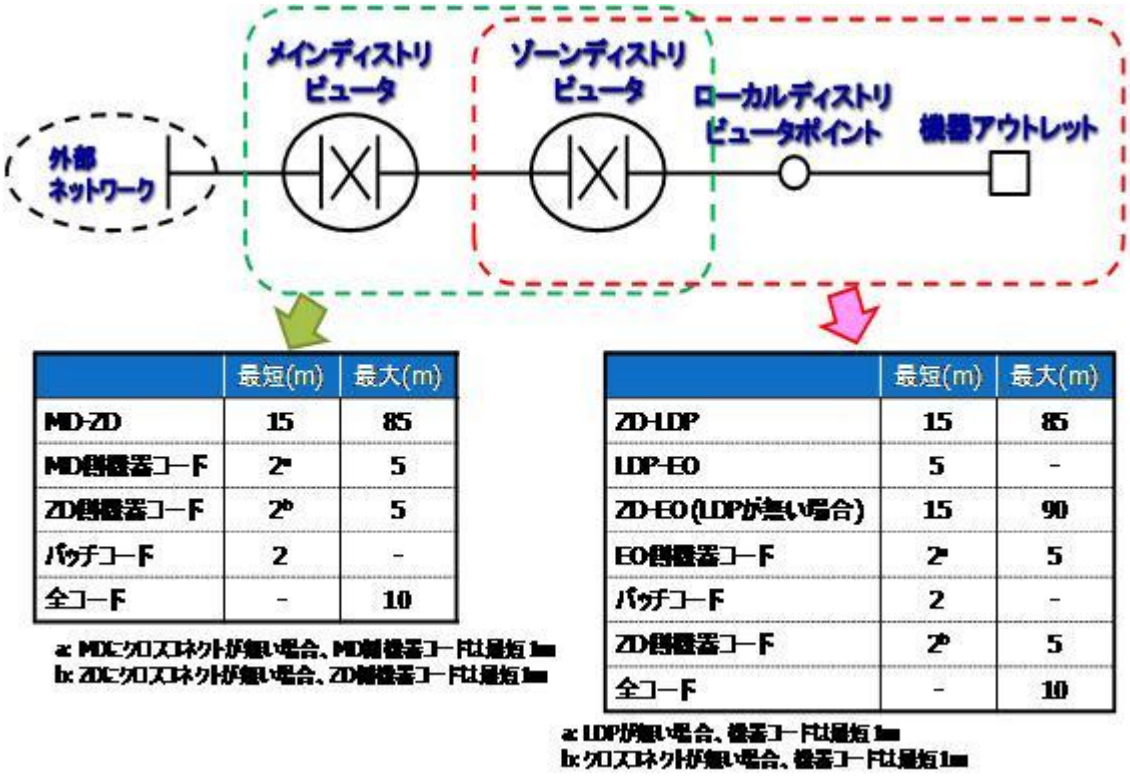


図 3-2a　ISO/IEC 24764 ケーブリングストラクチャモデル

各サブシステム内の配線構成や性能については、ISO/IEC11801 等で規定される要件が求められています。以下の図 3-2b は ISO/IEC 24764 に規定される配線仕様となります。



	最短(m)	最大(m)
MD-ZD	15	85
MD側機器コード	2[a]	5
ZD側機器コード	2[b]	5
パッチコード	2	-
全コード	-	10

a: MDにクロスコネクトが無い場合、MD側機器コードは最短 1m
b: ZDにクロスコネクトが無い場合、ZD側機器コードは最短 1m

	最短(m)	最大(m)
ZD-LDP	15	85
LDP-EO	5	-
ZD-EO (LDPが無い場合)	15	90
EO側機器コード	2[a]	5
パッチコード	2	-
ZD側機器コード	2[b]	5
全コード	-	10

a: LDPが無い場合、機器コードは最短 1m
b: クロスコネクトが無い場合、機器コードは最短1m

図 3-2b ISO/IEC24764 配線仕様

３－２－２．ケーブル･ルートと設置場所の選択

ケーブル･ルートは、ケーブリングと同様にデータセンターのネットワークにおいて重要な物理インフラです。ケーブル･ルートは、配線経路の明確化やケーブルの支持をするためだけではなく、ケーブルの保護をすることも目的の一つに挙げられます。そのため、データセンターに敷設される通信ケーブルは基本的に全て適切なケーブル･ルート上に配線を行う必要があります。ここでは、サーバルーム内のケーブル･ルートのデザインについて解説します。

サーバルーム内の配線ルートは主に架上配線か床下配線が利用されます。どちらを選択するかは、建物の制約、利用方法、サービス、セキュリティポリシー、作業頻度、作業者の熟練度など様々なことを考慮することが必要です。

建築構造的な制約としては、天井高が低く架上にルートを設置できないため床下配線とするケースや、フリーアクセスを使用しない直床式デザインのため架上配線を採用するケースなどがあります。このような、構造的な理由が無い場合、ケーブル･ルートの設置場所はデータセンター事業者の自由となります。以下に、床下配線と架上配線のそれぞれの特徴を紹介します。

(1)床下配線

国内のデータセンター事業者にもっとも多く採用されている床下配線の最大の特徴は、ケーブルが視界に入らないと言う事です。その為、セキュリティ性に優れています。床下配線の場合、フリーアクセスフロアを外さないとケーブルへアクセスができないため、ケーブルへの外的リスクが非常に低くなります。また、第三者が安易に配線を行う事を防ぐ事ができるため、配線品質の維持もしやすくなります。このように、利用者が勝手に配線することやイタズラを防止することが期待できるため、コロケーションエリアに非常に適したケーブル･ルートになります。第三者が容易に配線できないと言う事は、配線品質の維持管理も行いやすくなるため、重要回線や幹線ケーブルの様な一度敷設したらあまり変更のないケーブルを敷設するルートとして適しています。

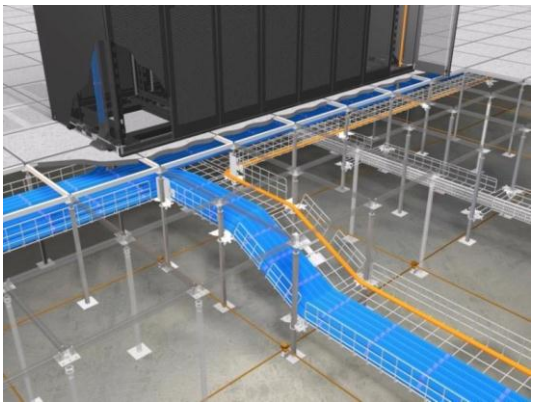


図 3-2c　床下ケーブルルート例

それ以外にも、以下のような場合も適しています。

- アイルキャップの垂れ壁など、ラック上部に障害物があるような場合
- 電源ルートが架上配線の場合
- ラック上部に空調機などの設備が置かれている場合

運用上の注意点としては、作業時の床板開口部への第三者の転落など、作業や運用時に考慮しなくてはならない事があります。エアフローへの影響や配線品質の維持の為、専門家が作業を行う事が望ましいです。

日本国内の場合、キャビネットの前面（Cold Isle 側）に通信ルートを配置する場合が多く見られます。しかし、TIA/EIA ではラック背面（Hot Isle 側）に設置する事を推奨しています。

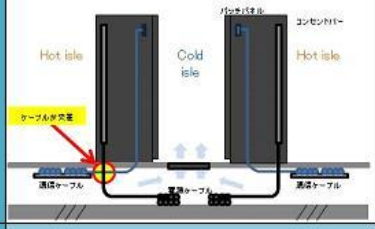
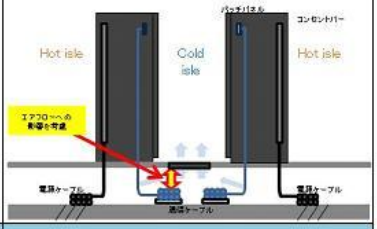
	TIA/EIA	国内DC
通信配線ルート	リア側（Hot Isle） 	フロント側（Cold Isle） 
設置高さ	OA直下（浅い）	スラブ寄り（深い）
特徴	エアフローへの影響を考慮し、通信ルートをラック背面に。また、作業性の確保の為、床板直下の高さに配線	通信ケーブルと電源ケーブルの取り合い的には適切な配置。追加電源、通信ケーブルの増設などの作業時も、施工性が高い。ルートの設置は床吹出し口から遠い位置で敷設することが望ましい。
注意点	ラックの真下で電源ケーブルと通信ケーブルが交差してしまう。ケーブルの保護が必要になる。 本数が多い際には作業性の確保が難しい。	エアフローへの影響を考慮する必要がある。 通信ケーブルが深い位置に敷設されるため、作業時にOA上から手が届きにくくなる。

表 3-2A　床下ケーブルルート比較表

(2)架上配線

最近では、架上配線も多くのデータセンターに採用され始めています。国内データセンター事業者の場合、コロケーションサービスなどの同一エリアを複数の利用者が利用するサービスを提供している場合が多くあります。その為、ケーブルが視界に入る可能性が高い架上配線はセキュリティと言う観点からあまり採用されていませんでした。しかし最近では、床下配線によるエアフローへの影響や床下空間のないデータセンターの出現などから架上配線を採用するデータセンター事業者も増えています。架上配線は、自社のシステムを自社で運用する場合に最適な配線方法です。コロケーションと異なり第三者が立ち入らないため、視界にケーブルが入る事への懸念は無くなります。逆に、作業性が高いためラック間の配線の追加変更をシステム担当者が行う場合などに適しています。その為、CSP 事業者やホスティングサービス、クラウドサービス事業者などでは、多く採用されています。

図 3-2d 架上ケーブルルート例

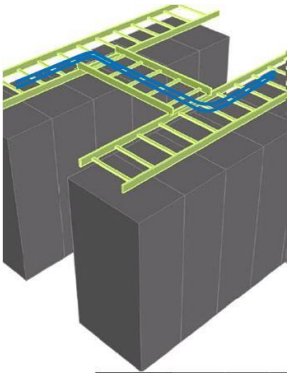


図 3-2e　架上ケーブルルート例

デザインの際には、梁や他の設備との取り合いを注意する必要がありますが、作業性が高いため、一度ルートを構築すれば、ケーブルの敷設は容易になります。ただし、容易な分、整線などを疎かにすると配線品質の低下を招き管理不能な状態になる事もあるため、きちんとしたルールを設ける事が大切です。

	床下配線	架上配線
特徴	直接ケーブルが見えなく、床板を開けないと容易にケーブルへのアクセスができない	床下空調のエアフローへの影響がない。 作業性が高く容易に追加変更が行える
適したケース	・ 追加変更の少ないケーブルの敷設 ・ コロケーションエリアのように多数のユーザーが利用する場所 ・ 天井高が低く架上にルートを設置できない場所 ・ アイルキャッピングなどの垂れ壁による、架間ルート上に障害が多数ある場合 ・ 電源ルートが架上ルートの場合 ・ ラック上部に空調機などの設備が置かれている場合	・ 都度引きや、追加撤去などが頻繁な場合 ・ 特定のユーザーしか出入りしないエリア ・ 床下空間が狭い ・ ケーブル量が多く、床下だとエアフローへの影響が出てしまう場合 ・ システムエンジニアなどが、ケーブルを敷設する事がある場合 ・ 同一架列内でのラック間配線などが多く想定される場合
設置条件	床下空調の場合、床下に400mm以上の有効空間が必要。また、OAフロアの足のピッチや通路幅などにより、ケーブル容量が限られる可能性がある。	ラック上部の空間が450mm以上あることが望ましい。複数階の建物の場合、梁などがあるため、ルート設計において考慮する必要がある。
配線施工性	・ ケーブル敷設作業時、敷設ルートの床板をあける必要があり、DC利用者に対する安全対策が必要となる。また、施工者自身も開口部から足を外しケーブルの上に落下する恐れもある。	・ 架上の場合、最低でも床面から2m以上の高所に敷設されるため、脚立などの足場が必要になる。そのため作業足場からの転落事故の危険が伴う。また、ケーブルが煩雑な状態になった場合、利用者からも見えてしまうため印象がわるくなる。

表 3-2B　ケーブルルート比較表

(3)階層化

サーバルーム内の水平配線で使われるケーブルには、大きく分けて電源ケーブル、ツイストペアなどのメタル系通信ケーブル、光ファイバーケーブルの３種類があります。

これらの電源・通信線の混触防止やケーブル種類、強度、利用方法など様々な状況に応じて階層化をすることで、安全性や作業性、管理性を高める事ができます。

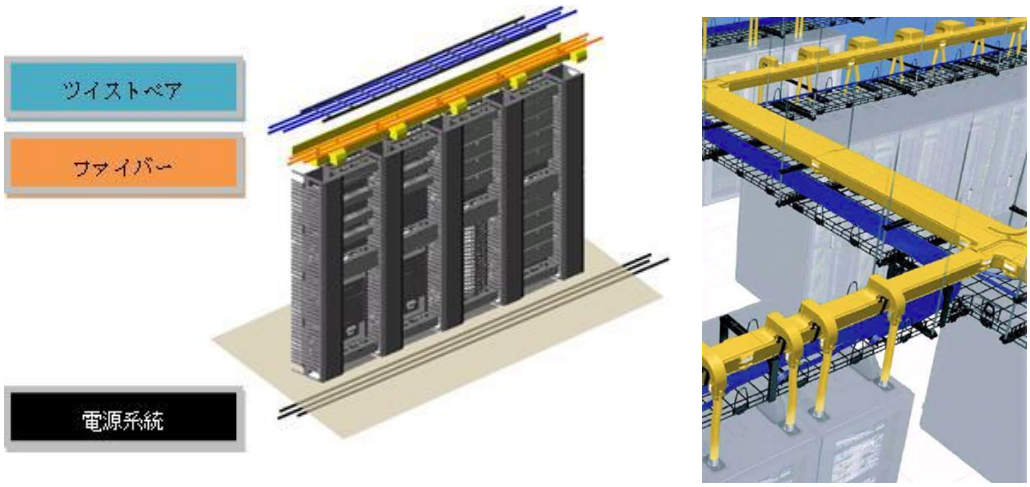


図 3-2f　ケーブルルートの階層化

図 3-2 f は、電線種（電源系、ツイストペア、光ケーブル）毎に階層化した例です。こうする事により、電源と通信系の混色を防止することができます。また、光パッチコードのような外皮がないデリケートな線種でも専用の線路部材を利用したルートを作ることで、パッチコードを用いてラック間配線を容易に行えるようになります。今後、通信速度の増加と共に光ケーブルの利用率が上昇していくデータセンターにおいて、この階層化モデルは非常に有効な方法の一つになります。
この他にもラック間 UTP を都度配線するようなサービス形態の場合、都度引き用のルートを別途で作る事で、作業性や整線性、管理性などを高める事が可能になります。
ケーブル･ルートの階層化は、データセンターのケーブル･ルートデザインに有効な手法となります。

３－２－３．通信ケーブルの種類

データセンターで用いられる通信ケーブルは大別するとメタルケーブルと光ケーブルに分類されます。

(1)メタルケーブルとそのメリット・デメリット

メタルケーブル（UTP 等）は、銅線を撚り合わせたケーブル類であり、LAN では一番使用実績のある伝送媒体です。プラグ付の形態もありますが、一般的には現場でケーブルを配線し、長さを揃えてプラグを取付接続します。
光ケーブルと比べて簡単に配線出来るという特長を有しています。あわせて使用する箇所(需要量)が多く、光ケーブルでは光電変換として光トランシーバを必要とするのに対し、メタルではそのままで良いため安価であり、トータルの配線コストも光ケーブルに比べると安くなるというメリットがあります。
一方、高速伝送を行うことになると、減衰、雑音等の影響もあり、メタルでは 10Gbps で最大 100m（Cat.6A）の伝送距離に対して、光ケーブルファイバーでは最大 40km と 400 倍の差となっています。また、曲げ半径も雑音等の兼ね合いで、Cat.6A では従来の光ケーブルと同等の 30mm の曲げ半径で使用しなければなりません。さらに、銅等を用いているため、光ケーブルに比べて約

10 倍（10Gbps の伝送を行う場合の単位 m 当たりのケーブル重量比）と重く、耐荷重制限等がある DC 等では少なからず影響を及ぼします。また、ケーブル径も約 2.5 倍（10Gbps の伝送を行う場合）太いため、多くの本数をフリーアクセス内に配線してしまうと、エアフローを遮り空調効率を悪化させます。さらに、エイリアンクロストークの影響を受けやすく、昨今の 1Gbps を越える伝送を行う際には、並行して敷設しない等工夫を行う必要があります。また、光ケーブルに比べて消費電力が大きくなる傾向があります。

(2)）光ケーブルとそのメリット・デメリット

光ケーブルはUTP等メタルケーブルに比べて細径･軽量という特長を有しています。そのため、耐荷重等が問題となるデータセンターには効果的です。また、コアとクラッドの屈折率差を利用し、コアの中に光を閉じ込め伝送を行うため、MMF（OM4）で550m、SMFでは数10kmと大容量長距離伝送が可能であることも光ケーブルの大きな特長です。さらに、メタルケーブルのようにエイリアンクロストークを考える必要がない点も優位なところです。

一方で、石英（ガラス）であるため、曲げるとロスが高くなる、曲げ過ぎたり、踏みつけると割れる（折れる）ため、取り扱いはメタルケーブルよりも慎重に行わなければならないという問題もあります。そのため、敷設施工では、光ケーブルをメタルケーブルとは別のルートに配線する、または専用のダクト等に配線して保護する等の工夫がなされていました。また、メタルケーブルは現場にてケーブルを敷設し、コネクタを後から取り付け、設置するのが一般的であるのに対し、光ケーブルは両端末のコネクタがついた状態で敷設されるので、どうしてもある程度の余長が発生し、それが配線ガイドもしくは床下に収容、輻輳及び空調の気流の遮断等の原因になることもあります。さらに、機器類に取り付けるトランシーバも光ケーブル用はメタルケーブル用に比べて高価という問題もあります。

(3)最近の光ケーブル

上記のように光ケーブルは、メリットを有する半面デメリットも多数有しており、データセンターでは未だメタルケーブルが主流で光ケーブルは一部の使用のみという実態があります。しかし、後述のように40GbE、100GbEの規格が制定され、さらなる規格化も検討され、それらは殆どが光ケーブルを主とした規格となっており､光ケーブルの比重が高くなる傾向にあるのは間違いありません。そのため、光トランシーバ等も数量が増えることで使いやすい価格になってくると考えています。

光ケーブルに関しても、デメリットに対する改良検討が行われ、扱い易い光ケーブルが市場に出てきています。例えば、曲げても損失が出にくい、出ないものがITUにてG.657.B3が勧告されました。具体的には、従来は半径30㎜以下には曲げられなかった光ケーブルが、半径5㎜でも損失、ビットエラーが発生せず、また折れません。ただし、従来使用されていた心線対照器が使えなくなるというデメリットも有しています。

また、光ケーブルを保護するコード・ケーブルの材料、構造を工夫することで、局所的に曲げたり、踏んだり、挟んだりしても光ケーブルが破損しないようなものも多数出てきています。さらに、ケーブル材料の工夫で非常に滑りやすい（低摩擦）ケーブルも開発され、容易な敷設作業及び撤去等、輻輳、空調対策に効果があり、運用が行いやすくなってきています。

コネクタにも工夫がなされ､現場にて簡単に組立可能なものが製品化されています。そのため、光ケーブルを所要量敷設し、現地でコネクタを取り付けられるため、余長が最小限で済みます。

また、40GbE、100GbEでインタフェースとして規格化されたMPO/MTPコネクタは、最大24心を一

括接続することが可能なため、非常に狭い管路への敷設も容易であり、かつ施工時間が従来工法に比べて約半減することが出来るようにもなってきています。

上記のような各種改良検討がなされたことで、敷設、運用が非常に良好になりました。

３－２－４．ケーブル･ルートの線路部材

線路部材の選定は､ケーブル･ルートの設計において考慮すべき重要な一つの項目になります。線路部材はケーブルを単に支えるためのものではなく、保護する目的もあるのです。サービスの提供形態や線種によって線路部材を適切に選択する事が重要です。下記に主な線路部材を紹介します。

ケーブルラックの様なサイドウォール（親桁）がある線路部材の場合、サイドウォールを乗り越えるような敷設はケーブルの損傷を招く場合があり､その際は角にカバーなどをつけて保護するなどの考慮が必要になります。最近では通信ケーブルに最適な、サイドウォールをなくしてフルフラットなルートデザインができるタイプのものもあります。複数階構造の建物が多い日本のデータセンターの場合､天井高が低くても自由なルート設計がしやすいフルフラットなルートデザインができるフラットメッシュタイプは非常に有効な線路部材になります。

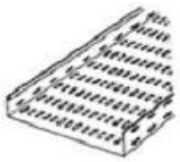
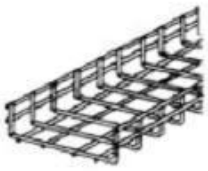
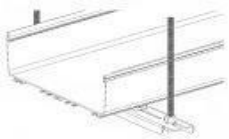
線路部材	適用ケーブル/コード	設置場所	姿図
ケーブルラック	電源ケーブル ・CV、VVF 光ケーブル ・構内・屋外ケーブル UTPケーブル インナーシースケーブル	架上/床下	
ケーブルトレー	電源ケーブル ・VVF 光ケーブル ・構内用（少数芯数） UTPケーブル	架上/床下	
ケーブルトレー （バスケット型）	電源ケーブル ・CV、VVF 光ケーブル ・構内・屋外 UTPケーブル インナーシースケーブル	架上/床下	
ケーブルトレー （ファイバー用）	光パッチコード UTPケーブル	架上/床下	
ケーブルトレー （フラットメッシュ）	電源ケーブル ・CV、VVF 光ケーブル ・構内・屋外 UTPケーブル インナーシースケーブル	架上	

表 3-2D　線路部材とケーブル種適用例

（参考）光コードの敷設

下記図は、光ファイバーのコードとケーブルの断面図になります。ファイバーコードは主にパッチコードとして、ラック内の機器などの接続に用いられます。また、ケーブルは強い外皮があるため、水平配線に利用されます。

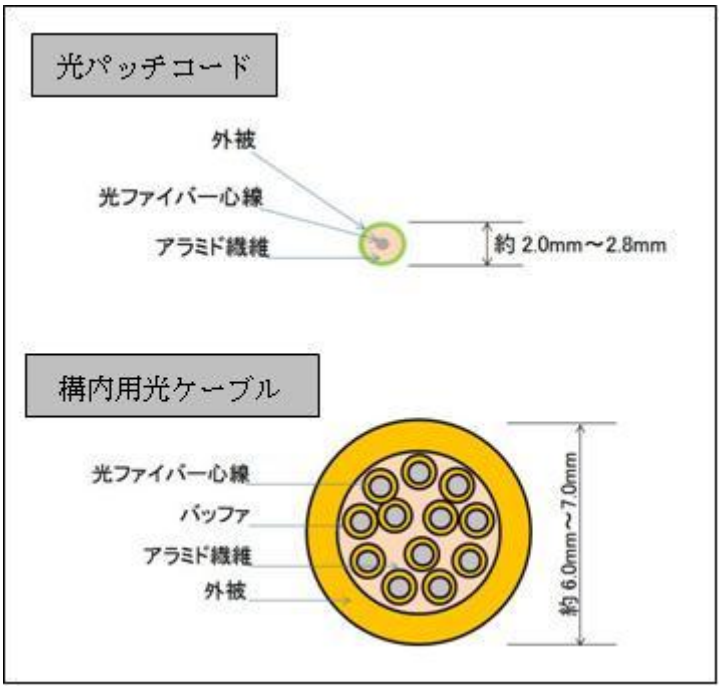


図 3-2h　ケーブルとコードの断面構造

ファイバーコードのように丈夫な外皮が無い柔らかいものは、ケーブルラックに直接配線をすることは適していません。ファイバーコード専用に作られたケーブル･ルートを利用するか、コードではなく外皮のあるケーブルを使用する事を推奨します。止むを得ずケーブルラダーに敷設する場合には、保護をするなどの対応が必要です。また、太く硬いケーブルと細くデリケートなケーブルを混在して敷設すると、キンクや折れによる通信障害などが発生する可能性が高くなります。ケーブル･ルートの適正な選択と､敷設するケーブル種類を考慮しセパレーターや配線位置を離隔するなど適切に配置する事が望まれます。

図 3-2i　光コード用ケーブルトレー

図 3-2j　スパイラルチューブ

３－２－５．ケーブルの整線

(1) ケーブル･ルート上の整線

ケーブル･ルート上にケーブルを布設する際には必ずきれいに配線をする意識を持つ事が大切です。ケーブル･ルート上のケーブルが煩雑になり撤去が困難になってしまい埋め殺しにしてしまうケースがあります。これは、配線作業に対する意識が低いとすぐに陥ってしまう症状です。そして、一度この状態になってしまうと、きれいな整理された状態へ戻すことは非常に困難になります。このようにならないためには、以下の事に注意する事が大切です。

- 常にきれいに配線をするように意識する
  ：この意識が無い場合、どのような対策を行っても煩雑になってしまいます。一度煩雑になると、それ以降も煩雑に配線されてしまいます。きれいな状態を維持し続ける事が大切です。
- 配線方法やルート、包縛方法などのルールを明確化する
  ：共通のルールに則った配線作業を行う事で、均一な品質を維持する事が出来ます。
- 基本的にはパッチパネルを使用し、都度引きは可能な限り行わない
  ：一度敷設したケーブルは可能な限り触らない事が品質維持につながります。
- 止むを得ず都度引きが必要な区間は、都度引き専用のケーブル･ルートをつくる
  ：同一架列内などで都度引きを行う場合、都度引き専用のケーブル･ルートを作る事で既存の配線品質への影響をなくすことができます。
- ケーブルを敷設する作業員を特定する
  ：作業員を特定する事で、配線品質の均一化が図れるだけでなく、雑な配線の抑制になります。
- ケーブル･ルートの階層化を意識したデザインを行う
  ：階層化する事により、管理性や施工性が高まります。
- 余長を意識し、適切な長さのケーブルを使用する。余長が発生してもケーブル･ルート上に丸めたりしない
  ：ケーブル･ルート上での余長の収容は絶対に行ってはいけません。

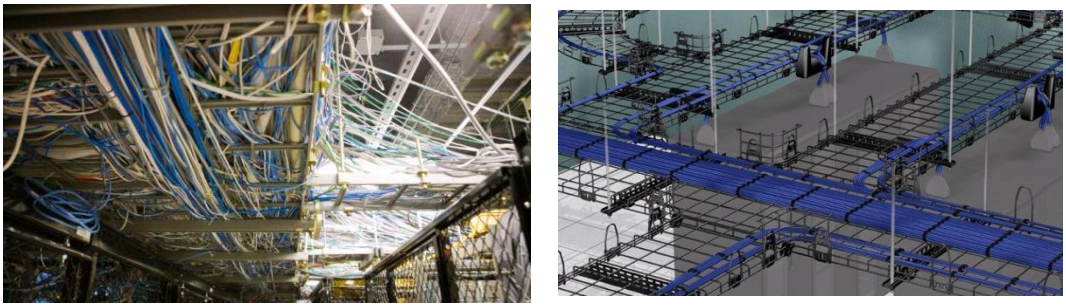


図3-2j　ケーブル･ルート整線例

(2) ラック内の整線

最近では高密度化により、ラック内のケーブルやコードが煩雑になるケースも多く起こっています。特にポート数の多い大型のスイッチ機器や、高密度に搭載した 1U サーバラックなどで起こりやすくなります。まったく同じ構成のラックを、別々の事業者が運用をしても事業者によって煩雑になったり、きれいな状態を維持したりとバラつきが出ます。マネジメント部材もまったく同じにしても差異が出るのは意識の問題が大きくあるのです。ケーブル･ルート同様に先ずは意識を持つ事が重要です。

- 常にきれいに配線をするように意識する
  ：ケーブル･ルート上と同様にこの意識が無いとどのような対策を行っても煩雑になってしまいます。一度煩雑になると、それ以降も煩雑に配線されてしまいます。きれいな状態を維持し続ける事が大切です。
- 適切なケーブルマネジメントの使用
  ：きちんとしたケーブルマネジメント部材を使用する事で、作業性が高まり整理しやすくなります。
- ケーブル量に応じたラックサイズを使用する
  ：ポート数の多い機器や、パッチパネルラックなどの場合、ラックそのもののケーブル容量を超えてしまう場合があります。大型ネットワーク機器などを搭載する場合には、ラックの幅が 800㎜ 以上必要な場合もあります。
- 機器に合わせた配線ルートをルール化する
  ：特にネットワークスイッチの場合、配線ルートを考慮しないとモジュールの交換やファン故障時の対応が困難になってしまう場合があります。ラック内でも、配線ルートのルール化は大切です。
- ラック間の配線は、できる限りパッチパネル経由で配線する
  ：ラックをまたいだ配線で直接機器に接続するとケーブルが煩雑になりやすくなります。特に大型のスイッチなどは、できる限りパッチパネルを経由するような物理構成にすることが大切です。
- パッチコードは、適切な長さの物を使用する
  ：余長はパッチコードでも意識する必要があります。同一ラック内の場合、パッチコードの長さの目安は２～３．５ｍでほとんどが賄えます。長すぎるケーブルは、ラックのケーブル容量の圧迫や巻きだめなど、煩雑になるきっかけになります。

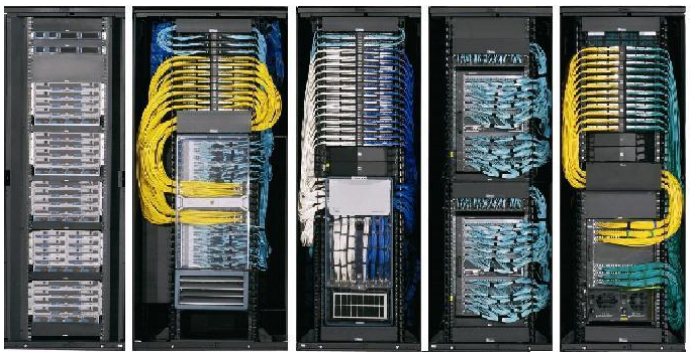


図 3-2k　機器に合わせたケーブルルートのルール化例

３－２－６．ネットワークアーキテクチャと配線

データセンター内でスイッチとサーバを接続する代表的な構成に Top of Rack（ToR）と Middle of Row（MoR）/ End of Row（EoR）があります。下記の図のように、エリア（POD）毎に ToR や EoR などを使い分けて利用する事が可能です。
ToR は柔軟性が非常に高い構成です。サーバラックやストレージラックなどラック単位で仕様を変える事が可能であり、増設もラック単位で可能になります。
E/MoR の場合、集約スイッチが少ないため、ネットワークの設定やポリシーの管理などがしやすいと言われています。また、POD 内の通信は、外部を経由しないで済むため、システム内部での通信が多い場合などには最適です。
サービスやシステムに合わせて ToR や E/MoR を自由に選択する事が可能なように、データセンター全体の階層化をきちんとする事も重要になります。
ここでは、図 3-21 で示す ToR 及び E/MoR デザインと、今後の 40GbE/100GbE への対応を考慮した物理層の構成例を紹介します。

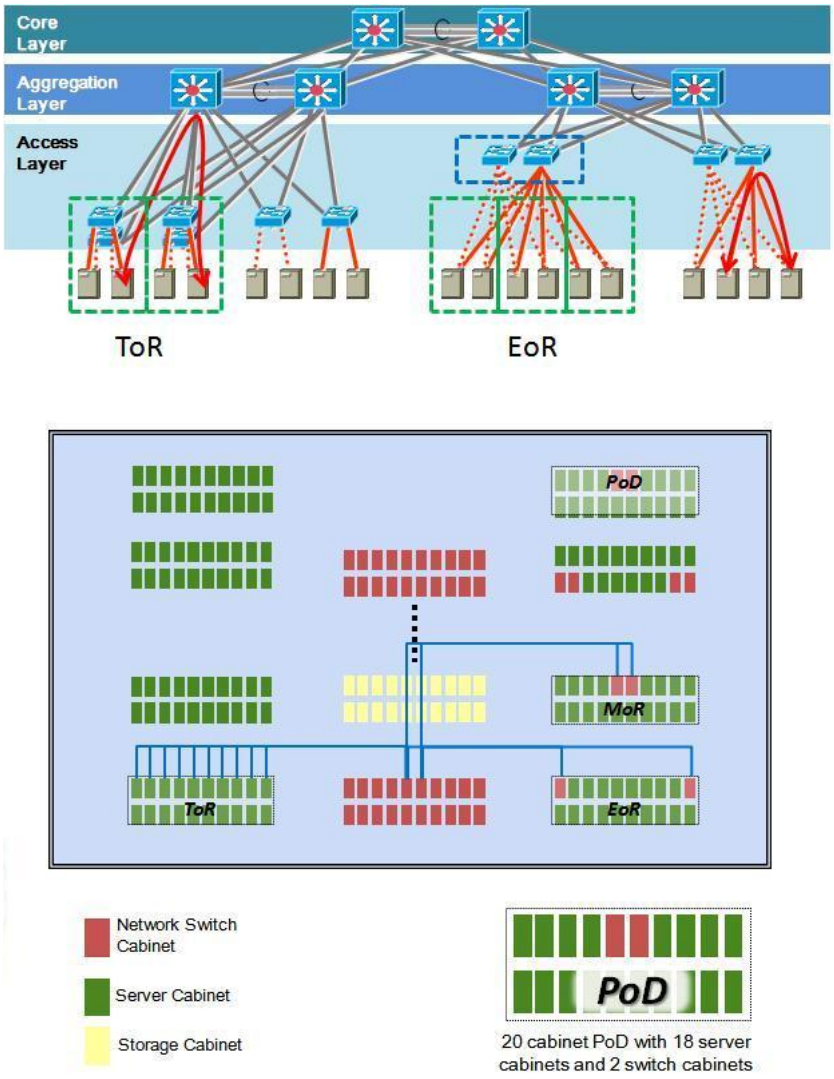


図 3-21　論理層と物理層（POD イメージ）

(1)ToR（Top of Rack）

各サーバラックにスイッチを設置し、ラック内のサーバを収容する構成を ToR（Top of rack）と言います。ToR の最大の特徴は、最小構成単位が１ラックとなることです。これにより、ラック単位でのポリシーの変更が容易になり設計の自由度が高くなります。また増設単位も１ラック単位で可能となるため、データセンターの増設計画や空調の無駄な運転を少なくするなど、物理レベルの運用メリットも高くなります。現在のデータセンターにとって、柔軟性は非常に重要な要求事項となっています。また、多様なサービスへの対応もラック単位で仕様を変えることが容易な ToR デザインは、使い勝手の良い構成となります。モジュール化への対応も、ラック単位で考えることができるので、現在のデータセンターでは多く利用されている構成になっています。また、スイッチ～サーバ間の距離が短いのでケーブルの制限距離が短いメディアを利用することも容易になります。隣接する複数のラックを集約することでスイッチの台数を減らすことも可能です。

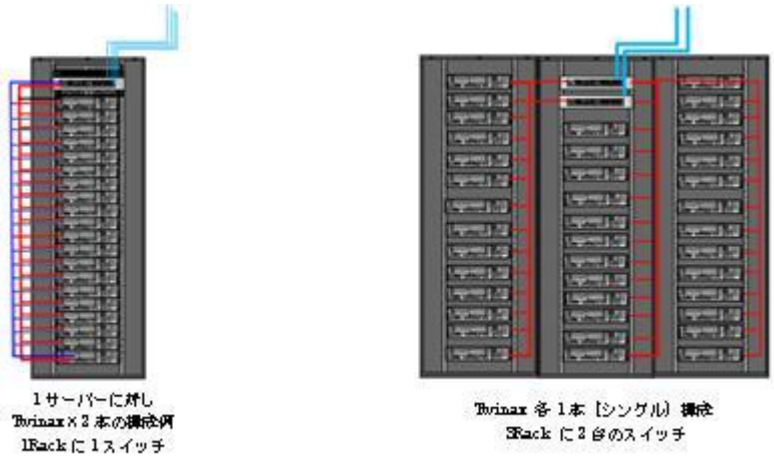


図 3-2m　ToR Rack イメージ

スイッチのアップリンクを 10GbE（Cat6A や OM3/4 LC など）でデザインした場合、40GbE/100GbE への対応のためにはケーブルの変更が必要な場合があります。高速化を視野に入れているデータセンターの場合、OM3/4 -MPO/MTP ケーブルを当初から導入することで物理的な変更を最小限に 40GbE/100GbE への移行が可能となります。10GbE で利用の期間は、MPO/MTP ケーブルを LC に変換するパッチパネルやコードを利用します。

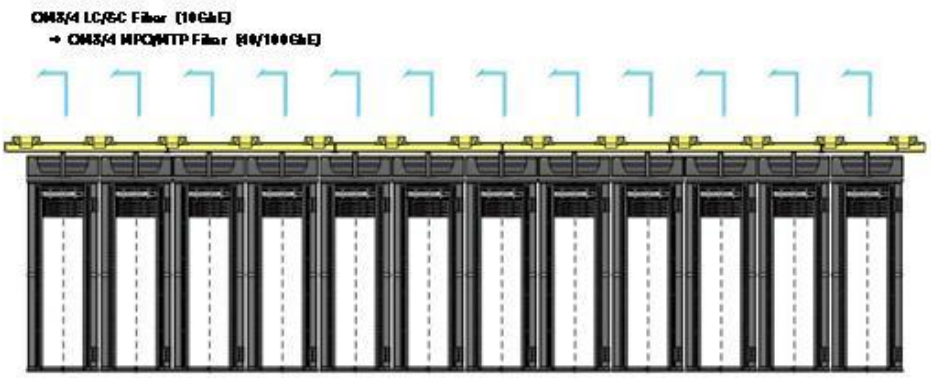


図 3-2n　ToR POD イメージ

(2)EoR (End of row)　/MoR (Middle of row)

POD 毎に集約用の大型スイッチを設置し、POD 内の各機器を集約する構成です。架列の端のラックにスイッチを設置する場合を EoR、中央のラックにスイッチを設置する場合を MoR 呼びます。E/MoR デザインは ToR に比べメリットが低いと言われる場合があります。しかし、POD を一つのシステムと考えたとき、システム内のトラフィックを集約スイッチで折り返せるためクローズされたネットワークとして効率的な運用が可能になります。

ToR 同様モジュールという概念において、POD 単位での拡張性を持つため柔軟性のある構成になります。しかし、サーバの台数に比例して必要なケーブルをスイッチまで配線する作業が発生します。1U や 2U タイプのサーバの場合、台数によってはケーブル本数が非常に多くなる可能性があります。集約台数が多い場合、分散させるために部分的に ToR 同様サーバラックにスイッチを設置し 2 段階(ToR と E/MoR のハイブリッド)構成にすることで回避することができます。また、サーバ～スイッチの距離があるため、ケーブル種類によってはケーブル長が対応できないケースがあります。MoR にすることで、全体の距離を縮めることも可能ですが POD のサイズによってはそれでも届かない場合があります。E/MoR 構成でサーバとの通信速度を 10GbE で行う前提でいる場合、ケーブル長に余裕がある Cat6A もしくはファイバーの使用が一般的となります。
40GbE/100GbE への移行を行う可能性がある場合、ToR と同様にスイッチのアップリンク側のケーブルを 40GbE/100GbE に対応できるケーブルを使用することで物理的な変更を最小限にすることが可能になります。

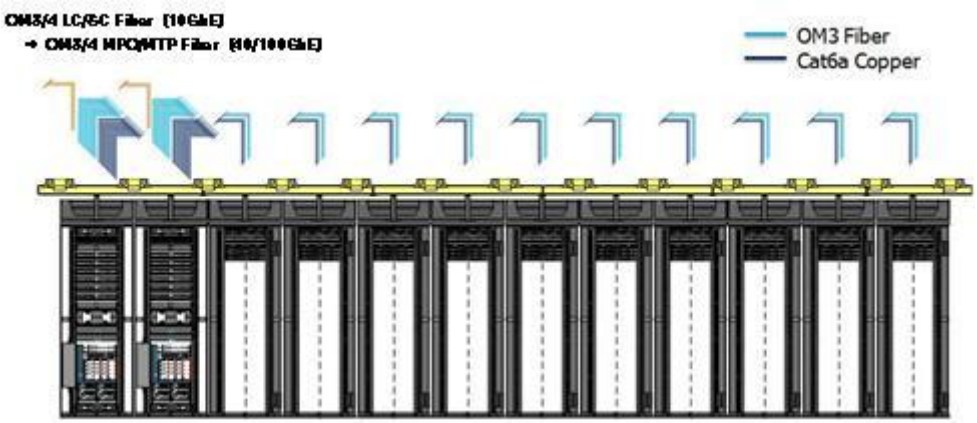


図 3-2o　EoR POD イメージ

(3)ToR、E/MoR の高速化に対する物理的要件

40/100GbE に関する移行方法の物理的概略を説明します。柔軟性がある ToR や E/MoR 構成においても、いざ 40/100GbE への移行を実行しようとした時に、ケーブルが一つの障壁になり移行が困難になるケースがあります。機器やモジュールの変更だけでは対応ができず、ケーブル全体を改修しなくてはならない状況が発生し、長時間サービスを停止しなくてはならなくなることも起こりえます。
40/100GbE に対応するためには今までのケーブリングの考え方とは少し異なる意識を持つ必要があります。1GbE から 10GbE への移行の際は、コネクタもケーブルもそのまま使用することができました。しかし、40/100GbE への移行に関してはコネクタ形状の変更だけではなく、芯数も

変わってきます。今までのケーブルの場合エンクロージャー内でコネクタを付け変えることも可能でしたが、MPO/MTP コネクタは現地で取付る事が難しいため、一般的に両端にコネクタが付けられているケーブルやコードを利用する必要があります。そのため、デザインの段階で通常の単芯 MMF を使用するか、MPO/MTP コネクタがついたパラレルケーブルを使用するか明確にする必要があります。
逆にいえば、高速化へ移行の可能性がある場合は当初から MPO/MTP コネクタのタイプのケーブルやコードを利用することで、物理層の改修を最小限にすることができるようになります。

(4) 10GbE から 40GbE への移行手順

10GbE から 40GbE への移行手順の例を示します。

（ア）ⒶMPO－LC 変換パネルにより、当初は LC パッチコードで機器と接続します

1. 機器もしくはモジュールを 10GbE モジュールから 40GbE モジュールへ交換
2. Ⓐのパッチパネル内の MPO-LC 変換パネルをⒸの MPO アダプターパネルへ交換
3. Ⓑの LC-LC パッチコードをⒹの MPO-MPO パッチコードへ交換
4. ケーブルを引きなおす必要がないため、ラック単位での移行が行いやすい

（イ）Ⓐの部分を、最初からⒸMPO アダプターパネルを使用した場合

1. 機器もしくはモジュールを 10GbE モジュールから 40GbE モジュールへ交換
2. ⒺMPO-LC 変換コードを MPO-MPO パッチコードに交換

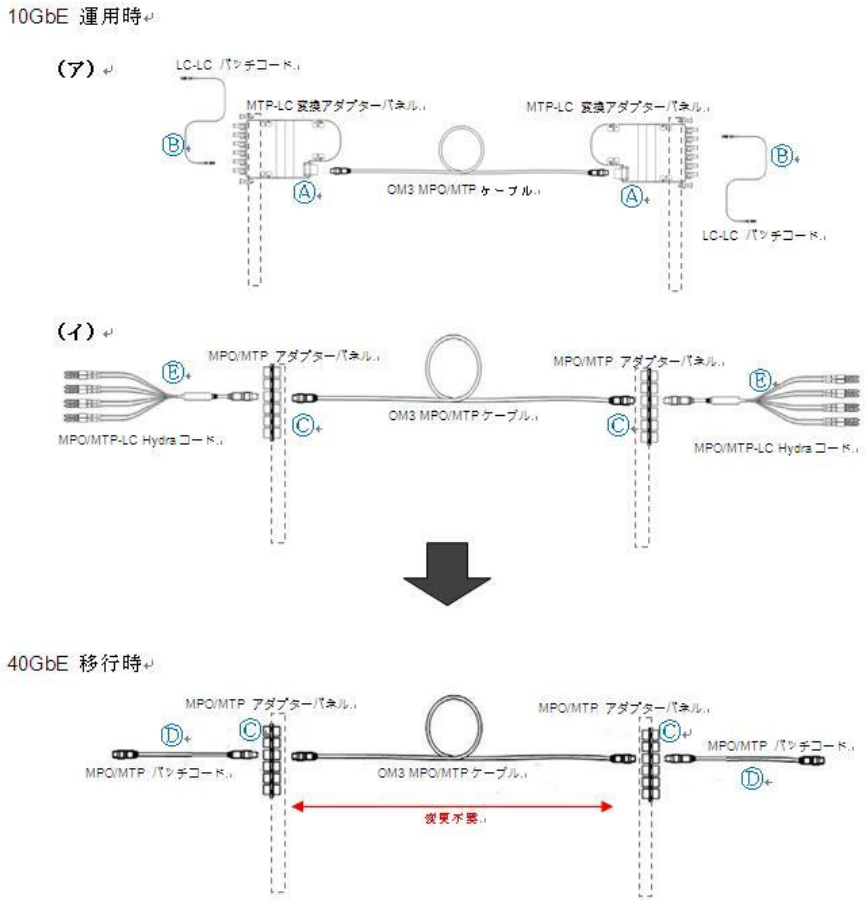


図 3-2p　10GbE から 40GbE への移行イメージ

３－２－７．物理ネットワークのトレンドと今後

2010 年から 2015 年におけるデータセンター全体の IP トラフィックは今後 5 年間に 4 倍に増加。2015 年には世界のデータセンターの IP トラフィックは 4.8 ゼッタバイトに到達する見込みと予測される中、データセンターにおけるトラフィックの多くはデータセンター内に留まるトラフィックであると示されています。（参照：図 3-2q）

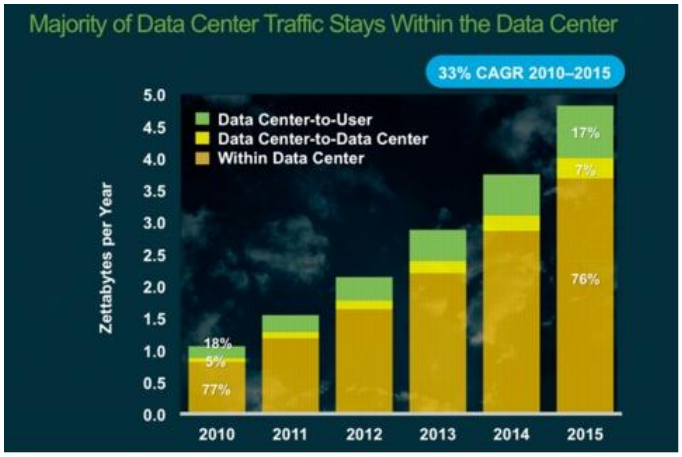


図 3-2q データセントートラフィックの宛先

幾つかの原因として、利用者数の増加はさることながら、利用するアプリケーション内でのトラフィックの扱い方の変化、具体的にはアプリケーションサーバとストレージ、データベースサーバの機能的な分離、分散システム、並列処理などの利用により、タスク処理が複数の小さなタスクに分割され、それらが複数のサーバに送信され処理、また、サーバ仮想化の導入に伴う仮想マシンイメージファイルのコピー、稼働中の仮想マシンの移動（引越し）をすることでデータセンター内部のトラフィックが増大していることが一因と言えます。

これらのトラフィック増加の要求に対応すべく、従来のデータセンターネットワークの多くは 10GbE を搭載したルータ、スイッチを用いてコアネットワークを構築していましたが、新たなインタフェースとして 100G、40G イーサネットが標準化されました。今後のコアネットワークはこれらにとって代わり、サーバなどを収容（接続）するアクセスネットワークは従来の GbE から 10GbE に変化し、サーバは新たな CPU の登場によりマザーボードにも変化が現れ、搭載される LAN インタフェース（LOM：LAN on Motherboad）は GbE から 10GbE に変化しようとしています。（参照：図 3-2r）

現在、アクセスネットワークで 10GbE を実現する為には SFP+に対応したスイッチを用いて、SFP+トランシーバと光ケーブルで接続。サーバ側は拡張カードを追加し対応するのが殆どですが、今後のサーバにおいては LOM の標準搭載される中、10GbE はコスト的な配慮から 10GBASE-T になると見込まれていることから、これらサーバを集約する主にアクセス層のスイッチは、SFP+対応の 10GbE スイッチから 10GBASE-T をサポートしたスイッチの採用と増加が見込まれています。

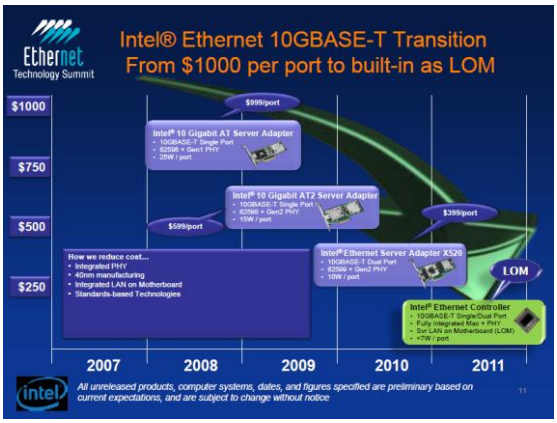


図 3-2ｒ Intel Ethernet 10GBASE-T Transition

これにより、既設ケーブルとして Cat6、6a、7 のメタルケーブルを利用している場合はその再利用は可能ですが、ケーブル種類の相違により伝送距離が異なること、隣り合ったケーブル

(Twisted Pair ケーブル)の間で伝わるエイリアンクロストークと呼ばれるノイズへの影響の考慮が必要になることから 10GBASE-T の導入の際には改めて敷設、施工、測定の全体的な見直しが必要になります。

伝送規格	Ethernet規格	帯域	ケーブル	距離
IEEE802.3an	10GBASE-T	10Gbps	Cat6A(RJ45)	100m
IEEE802.3ae	10GBASE-SR		MMF(SFP他)	300m
	10GBASE-LR		SMF(SFP他)	10km
	10GBASE-ER		MMF(SFP他)	40km
IEEE802.3ak	10GBASE-CX		4対2芯銅線 (CX4) 同軸	15m

表 3-2E　10GbE の規格

40G/100G のインタフェースについては、先に示した通り標準化が完了しましたが、更なる高速化として、光ケーブルを用いて 2015 年の標準化を目標に「1 Terabit Ethernet」「400G Ethernet」、2020 年頃を目標にした「100 Terabit Ethernet」。また、メタルケーブルを用いて 2014 年に「100G Ethernet」、また、2012 年 7 月に「Next Generation BASE-T」としてツイストペアケーブルで 40G、100G 対応の検討が開始されました。

	Twisted Pair	Multimode Fiber	Single-mode Fiber	Twinax
100Gb/s	?	100GBASE-SR10	100GBASE-LR/ER	100GBASE-CR10
40Gb/s	?	40GBASE-SR4	40GBASE-LR/ER	40GBASE-CR4
10Gb/s	10GBASE-T	10GBASE-SR	10GBASE-LR/ER	10GBASE-CX4/SFP+DAC
1Gb/s	1000BASE-T	10GBASE-SX	1000BASE-LX	1000BASE-CX

表 3-2F　Ethernet の規格

データセンターは利用者のニーズと共に建築構造物な含めた最新設備が求められる一方、
クラウドサービスのような仮想技術など新たな技術を用いたサービス、ネットワーク機器の特性の課題を整理した上で、物理ネットワークの要件を考慮し検討、導入をする必要があります。

出典

:図 3-2r http://www.cisco.com/web/JP/solution/isp/ipngn/literature/Cloud_Index_White_Paper.html

:図 3-2s http://www.ethernetsummit.com/English/Collaterals/Proceedings/2012/20120223_T1_2A_panel.pdf

３－３．論理ネットワーク

３－３－１．論理ネットワークに求められる要件

(1)仮想化を中心とした論理設計

サーバ仮想化技術をデータセンター内で活用していくにあたって、大きく 2 つの課題に直面し、その対策の検討が必要となります。

一つは、仮想マシンを動作させる物理サーバの台数の増大に伴い直面する課題で、もう一つは、多数の利用者を取り込んだマルチテナントの実現にあたって直面する課題です。

(2)物理サーバの増大に伴い直面する課題

物理サーバの増大に伴い、それらを収容するためのネットワーク機器が多くなることで構成が複雑となり、合わせて各仮想ホストとストレージで形成される SAN(Strage Area Network)も大きくなり物理・論理での構成が膨大なものとなります。また、従来の L2 設計での冗長設計においては、STP(Spanning Tree Protocol)が主流ですが、仕様上一部経路が使えなくなるため、ネットワーク全体の帯域を十分に使用できなくなり、また L2 ドメインが大きくなることで管理が複雑になります。これらの課題の対策としては、複数のネットワーク機器を論理的に一つにすることや、スパニングツリーに変わる L2 設計の採用、SAN と LAN の統合が考えられます。

(3)マルチテナントの実現にあたって直面する課題

マルチテナントの実現方式においては、複数のテナントでリソースを共有することになります。共有するリソースとしてはファイアウォールやサーバロードバランサといったネットワークで提供する機能や、VLAN ID や IP アドレスなども含まれ、限りあるリソースを有効に活用する施策が求められます。また、サービス提供の考え方によってはテナント毎に求められるネットワーク構成に柔軟に応えなければならないことやテナント間のセキュリティ確保が必要になります。物理的な構成変更ではなく、論理的にこれらの構成変更に対応することが必要となります。

本章においては、これらの課題解決の一助となるようなネットワークの仮想化技術の紹介をします。ネットワークの論理設計に関連して、性能を向上するための仮想ホスト上のソフトウェアスイッチの負荷をオフロードする技術や、近年話題となっている OpenFlow といった、従来のネットワーク設計の考え方からの大きな変革となる、SDN(Software-Defined Networking)についても紹介します。

３－３－２．物理ネットワークをシンプルにするための仮想化技術

サーバの増大や仮想化の普及に伴い、シンプル且つ L2 フラットなデータセンターネットワークが求められており、それらの要望に対して様々なソリューションが出てきています。本項では、それらのソリューションの中からスタック／マルチシャーシクラスタ、データセンターファブリックについて紹介します。

(1)スタック／マルチシャーシクラスタ

スタック／マルチシャーシクラスタとは、物理的には複数台のスイッチを、論理的には 1 台のスイッチのように動作させるソリューションです。

従来のネットワークでは、冗長性を考慮し複数の機器を接続した場合に起こる L2 ループへの対策として、一部のポートをブロック状態(未使用の状態)にしてしまう STP を利用することが一般的でした。STP を用いたネットワークは、正常時でも約半分のポートが使われていない状態となり、非常に非効率なネットワークと言えます。

これに対し、複数のスイッチを論理的に 1 台のスイッチとして動作させるスタック／マルチシャーシクラスタと呼ばれる技術を用いることにより、L2 ループを無くし、STP を利用する必要の無いネットワークを組むことが可能です。

また、論理的には 1 台のスイッチ同士を接続していることになりますので、冗長性、および帯域の確保にリンクアグリゲーション(IEEE 802.3ad)が利用でき、シンプルなネットワークを構成することが出来ます。リンクアグリゲーションは STP と違い、一方のポートをブロックするのではなく、両方のポートに通信を分散させ、ネットワークの帯域を有効に使うことが出来ます。

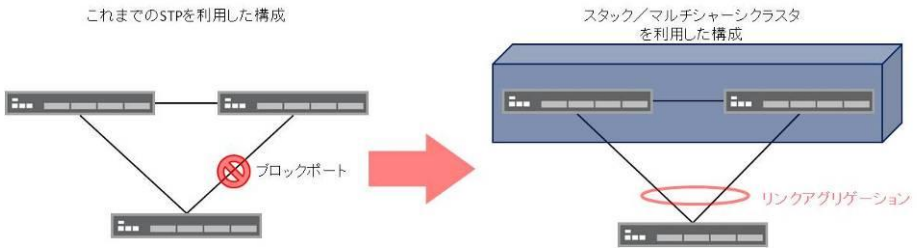


図 3-3a　スタック／マルチシャーシクラスタ構成

また、スタック／マルチシャーシクラスタと呼ばれる機能を実装している機器の多くは複数台で設定情報も共有している場合が多く、複数台の機器を一括で設定できるため、運用管理の負荷も軽減させることが出来ます。

(2)データセンターファブリック

データセンターファブリックとは、近年のデータセンター内トラフィック増加、ネットワーク構成の複雑化に対して、ネットワークをシンプルにすることを目的としたソリューションです。代表的なソリューションとして、TRILL(Transparent Interconnection of Lots of Links)、SPB(Shortest Path Bridging)、大型スイッチについて紹介します。

①TRILL

TRILL とは、STP を使わずに L2 マルチパスを実現可能なソリューションの一つです。冗長化と高速化を同時に実現可能で、IETF(Internet Engineering Task Force)で標準化されております。

従来の STP を用いた冗長化では、正常時でも約半分のポートが使われていない状態でしたが、TRILL では、複数の経路がある場合でも、一定のアルゴリズムで経路を選択して、自動的に L2 ループ対策と負荷分散を行います。

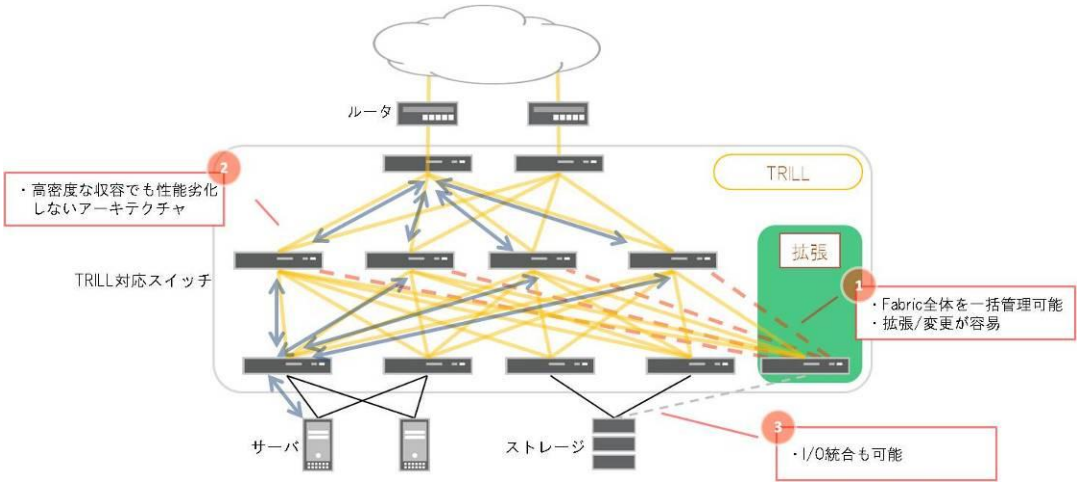


図 3-3b　TRILL を利用したネットワーク

TRILL 網内のトラフィック転送には、リンクステートプロトコルである IS-IS(Intermediate System to Intermediate System)や OSPF(Open Shortest Path First)等を応用して経路選択を行い、TRILL 用のヘッダを付与して転送を実施します。TRILL 網内では、エンドホストの MAC アドレスではなく TRILL ヘッダのみでパケットの転送が実施されるため、MAC アドレスの拡張性も備えています。また、新規に機器を追加する場合も、自動で情報のやり取りが行われ、既存の TRILL 網に組み込まれる等の特長もあります。

また、TRILL はストレージネットワークの統合(FCoE(Fibre Channel over Ethernet)/DCB(Data Center bridging)等)とも親和性が高く、ストレージネットワークも含めたシンプルなネットワークを実現することが出来ます。さらに、標準化技術のため、将来的には異なるベンダ間でも相互接続できるようになる可能性もあります。

②SPB(IEEE 802.1aq Shortest Path Bridging)

SPB とは、TRILL と同じく L2 マルチパスを実現可能なソリューションであり、IEEE(The Institute of Electrical and Electronics Engineers, Inc.)で標準化されています。SPB も、TRILL と同様に IS-IS を応用し経路制御を行います。また、バックボーン側で MAC アドレスの学習をさせないことも特長の一つです。

TRILL との違いとしては、SPB では、カプセル化に PBB(IEEE 802.1ah Provider Backbone Bridge)を応用しており、既存技術である PBB との親和性が高く、パス管理のための OAM(Operation Administration and Maintenance：保守・管理機能)にイーサネットの技術を使用出来ます。SPB も標準化技術のため、将来的には異なるベンダ間でも相互接続できるようになる可能性があります。

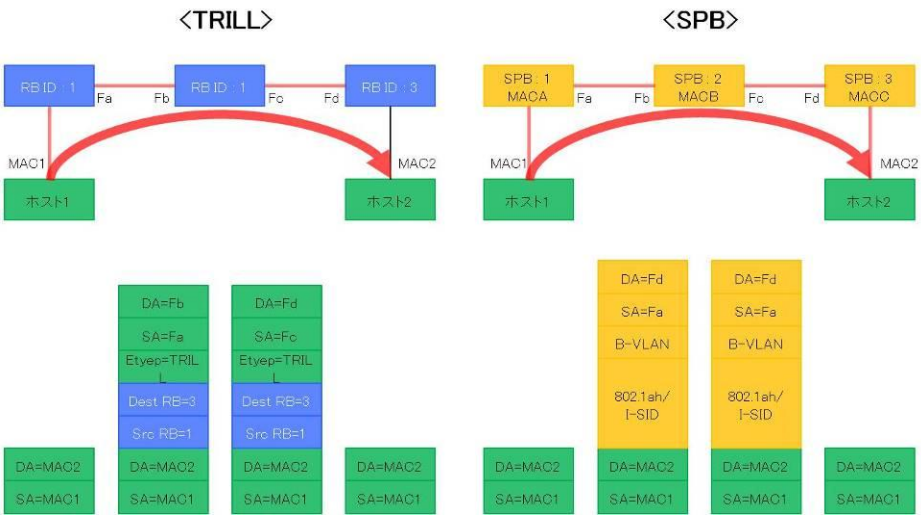


図 3-3c TRILL と SPB の比較

表 3-3a　フレームのオーバーヘッド

TRILL：20 バイト	TRILL ヘッダ	8 バイト
	Outer MAC ヘッダ	12 バイト
SPB(+PBB)：22 バイト	802.1ah タグ	18 バイト(Outer MAC 含む)
	B-VLAN タグ	4 バイト

③大型スイッチ

大型スイッチとは、ポート収容率や機器単体のパフォーマンスを向上させ、1 台のスイッチでより多くのポートを収容できるように設計されたスイッチです。

大型スイッチには、これまでのシャーシ型スイッチの収容度を更に大きくした EoR(End of Row)モデルと、シャーシ型スイッチの各モジュールを機能毎に分散配置することで拡張性を向上させた ToR(Top of Rack)モデルに分けられます。

―EoR モデルの大型スイッチ

EoR モデルの大型スイッチは、10G ポートの集約率を飛躍的に上げることで、ラックの列の端、もしくは中央に 1 台の大きなスイッチを配備し、そこから各サーバと直接接続するモデルになります。最近ではノンブロッキングで 10G 数百ポートを収容可能なスイッチもあります。

メリットとしては、複数のスイッチを 1 台のように見せるのではなく、そもそも 1 台のスイッチであるため、大規模なネットワークでも運用が容易な点があげられます。また、複数の機器を連携させるためのプロトコルも必要ありません。ただし、1 つの大きなスイッチから数十台(数百台)のサーバやスイッチが接続されるため、ラック間の配線が複雑になるというデメリットもあります。

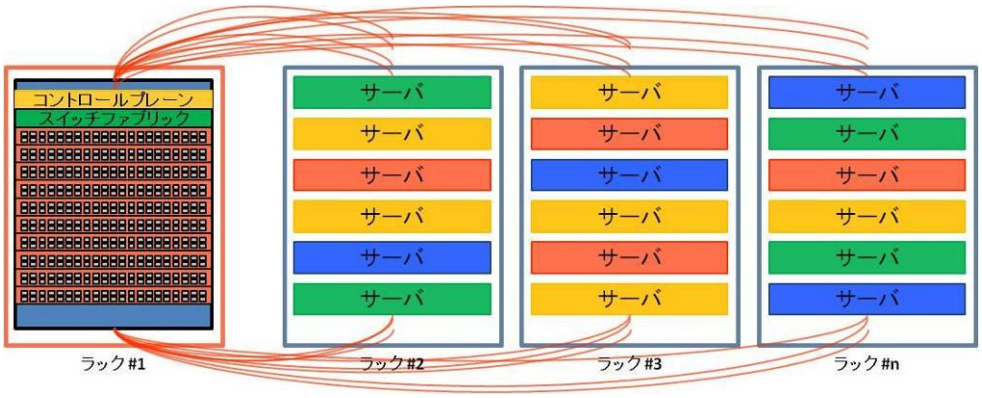


図 3-3d　EoR 配線イメージ

また、EoR モデルの大型スイッチは、万が一の障害時の影響範囲が大きくなってしまうため、CPU モジュールの冗長や無停止でソフトウェアのアップグレードを行う ISSU(In Service Software Upgrade)等、可用性を高める対策・機能が必要となります。

―ToR モデルの大型スイッチ

ToR モデルの大型スイッチは、1 台の大型スイッチを、ToR に設置するポート部分と、コントロールプレーンやスイッチファブリックを分離させて動作させるスイッチです。

ポート部分とスイッチファブリックが分離され、その間は広帯域のネットワークで接続されるため、ラック間を跨いだ柔軟な物理構成が可能になります。また、各サーバは ToR に設置されるポートに接続されるため、ラックを跨ぐ配線が少なくて済むメリットがあります。

各モジュールを管理するコントロールプレーン(CPU モジュール)も別コンポーネントとなっており、スイッチコンポーネント全体を一元的に管理可能です。

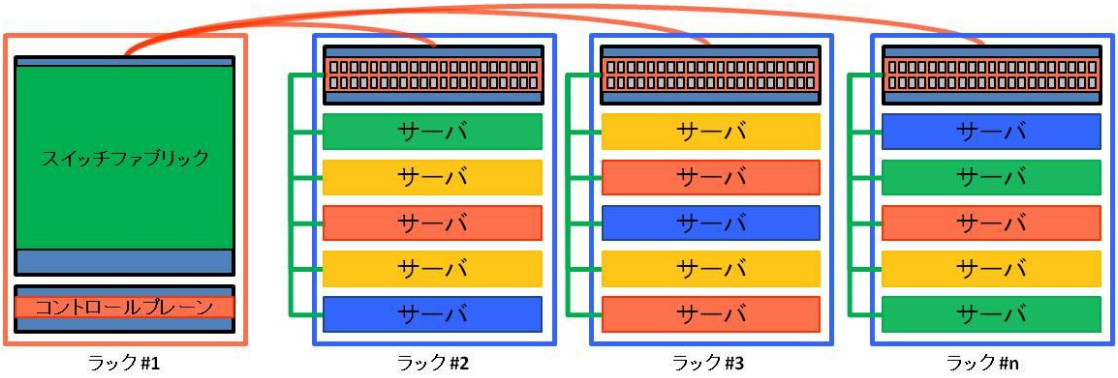


図 3-3e　ToR 配線イメージ

(3) ソリューション毎の比較

それぞれのソリューションについて、拡張性、コスト等を比較すると以下のようになります。

表 3-3a　物理ネットワークをシンプルにするソリューション

比較項目		スタック／マルチシャーシクラスタ	データセンターファブリック TRILL	SPB	大型スイッチ (EoR モデル)	大型スイッチ (ToR モデル)
スモールスタート		○	○	○	×	×
拡張性		×	△	△	△	○
運用性		○	△	△	○	○
FCoE/DCB との親和性		△	○	×	○	○
コスト	小規模	○	△	△	△	×
	中規模	—	○	○	○	△
	大規模	—	—	—	—	○
	備考	初期投資は低く抑えることが可能だが、中規模以上の環境には対応できない。FCoE/DCB は製品によっては対応可能。	初期投資はある程度低く抑えることが出来るが、大規模環境には対応できない。	初期投資はある程度低く抑えることが出来るが、大規模環境には対応できない。FCoE/DCB は、現時点では対応不可。	初期投資はある程度低く抑えることが出来るが、大規模環境には対応できない。	初期投資は高くなるが、大規模構成への拡張性、大規模構成時のコストメリットがある。

３－３－３．マルチテナントを実現するための仮想化技術

事業者のサービスでは、単一のネットワークに複数の利用者を収容する必要があるケースが多々あります。マルチテナント機能は、複数の利用者を効率良く、単一のネットワークに収容可能なソリューションです。

マルチテナントの実現方法としては、従来から使われている VLAN が最も有名で容易な方法ですが、VLAN では使用できる ID の最大数が約 4,000 という制限があり、それを超えるような場合には、PB(IEEE802.1ad Provider Bridge)等の VLAN を拡張する為のソリューションが必要となります。

(1) VLAN(Virtual LAN)

VLAN とは、1 台のスイッチを論理的に分割し、ブロードキャストドメインを分けたい場合に使用されます。VLAN は IEEE 802.1q として標準化されており、Ethernet フレームに VLAN タグと呼ばれるヘッダが付与することで、各ネットワークを VLAN ID という識別子で区別します。VLAN ID の最大数は約 4,000 となります。

VLAN が使われる前のネットワークでは、ネットワークを分割するためには、ルータ、L3 スイッチ等の L3 機器を使用し、個別にスイッチを設置する等の対処が必要でしたが、VLAN を使用することで、スイッチでネットワークを分離することが可能になります。現在では、各企業の中で、ごく一般的に使用されており、部門ごとのネットワークを分ける等の用途で用いられています。

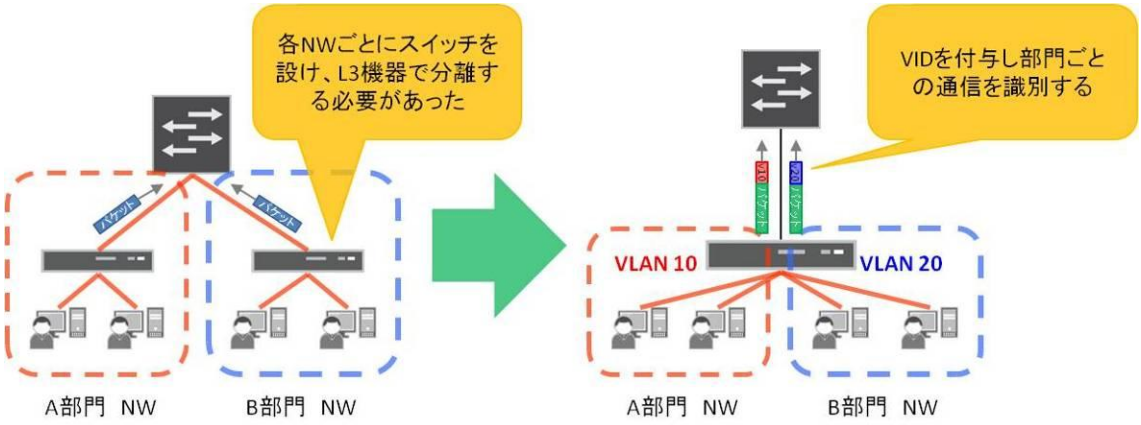


図 3-3f VLAN のイメージ

(2) PB(IEEE802.1ad Provider Bridge)

PB は Q-in-Q とも呼ばれる技術です。PB では、企業内で使用される VLAN タグ(C-TAG)に加え、企業を識別するための VLAN タグ(S-TAG)を付与します。

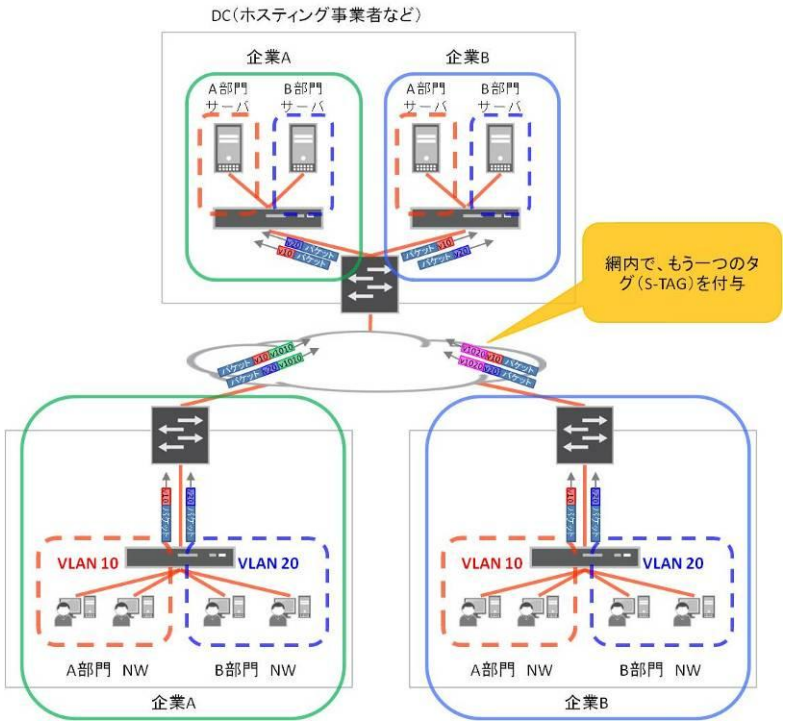


図 3-3g　PB のイメージ

マルチテナントを実施する上で、約 4,000 の VLAN ID で不足しているような場合や、収容する企業の中で既に VLAN が使用されているような場合、C-TAG を S-TAG によりカプセリングすることで企業を区別し、企業毎に約 4,000 の VLAN ID を自由に利用することが可能となります。

約 4,000 の C-TAG を、約 4,000 の S-TAG でカプセリング可能な為、理論上 4,000×4,000＝約 16,000,000 の VLAN が利用可能となります。

表 3-3b　L2 マルチテナント技術の比較

	VLAN	PB
テナント間の IP アドレス重複	○	○
テナント間の VLAN ID 重複	×	○
VLAN 数の拡張性	×	△
備考	一般的に使用されており、ほとんどの機器が対応している。ただし、データセンター事業者が求めるマルチテナント技術としては現実的ではない。	VLAN と比べると若干高価な機器が必要となる。また、ホストの MAC アドレスはそのまま転送されるため、ネットワーク全体の MAC アドレステーブルのサイズについて注意が必要。

(3) VR (Virtual Router)

VR は、物理的な 1 台のルータの中で、仮想的に複数のルータが動作しているように見せるソリューションになります。

前節までの VLAN や PB といった技術によって、複数の企業を効率的に収容し、通信をセキュアに分離することが可能になりますが、L2 ネットワーク間の通信が必要な場合は、ルータ、L3 スイッチ等の機器を企業毎に準備する必要があります。

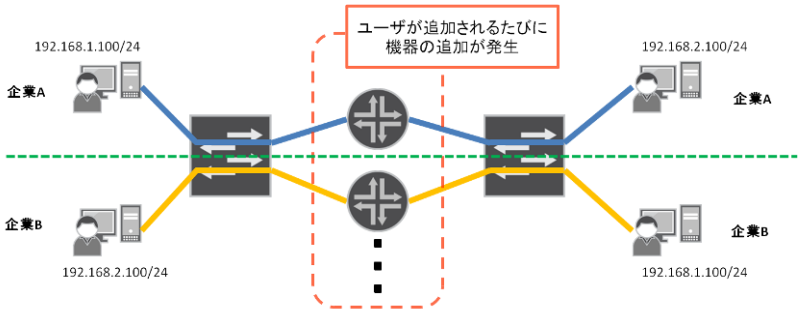


図 3-3h　従来の方法

例えば、図 3-3h のように企業毎にルータを設置した場合、機器の数も増え管理が非常に煩雑になりますが、図 3-3i のように VR を用いると、ルータの中に仮想的なルータを複数作成することで、一台のルータで複数の企業を収容することが可能となります。

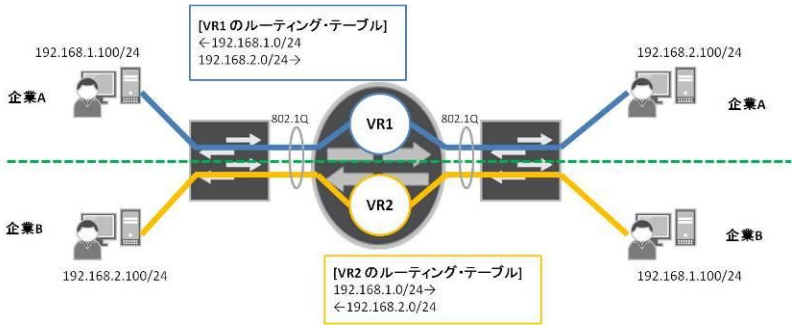


図 3-3i　VR イメージ

各 VR はそれぞれの個別のルーティングテーブルを保持している為、複数の利用者企業で IP アドレスが重複していても、問題無く収容が可能です。また、それぞれの VR で別々のルーティングプロトコルを動作させることも可能です。

３－３－４．サーバ仮想化環境で必要となるネットワーク仮想化技術

ハイパーバイザによるサーバの仮想化が進むにつれて、ネットワークにおいては 3 つの大きな課題が明らかになってきました。

1 つ目は、仮想スイッチによるパケットの転送負荷です。仮想スイッチはソフトウェア処理であるため CPU の処理能力が問題になります。

2 つ目は、ネットワークとサーバの管理境界があいまいになる点です。本来ネットワーク管理者が担当すべきスイッチが、仮想スイッチとしてサーバの中に存在する為、サーバ管理者とネットワーク管理者の責任範囲が曖昧になり、運用管理が難しくなってきています。

3 つ目は、仮想サーバの移動に対するネットワークの設定変更に関してです。仮想化されたサーバは、物理的な場所に捉われず、自由に移動できてしまうことから、その移動を想定したネットワークの設定、設定変更が必要となってきており、これらの対策が不十分であると、運用管理の負荷が増大したり、サーバ仮想化のメリットを十分に享受出来ない可能性もあります。

これらの課題を解決するために、EVB(IEEE802.1Qbg Edge Virtual Bridging)という技術が標準化されています。

EVB とは、サーバ仮想化環境におけるネットワークに必要な機能をまとめた技術標準で、VEB(Virtual Ethernet Bridge)と VEPA(Virtual Ethernet PorTAGgregator)の 2 つの機能や、VDP(VSI Discovery Configuration Protocol)等のプロトコルが定義されています。

(1)VEB

VEB とは、仮想サーバ間の通信を NIC(Network Interface Card)等を使って折り返す機能になります。

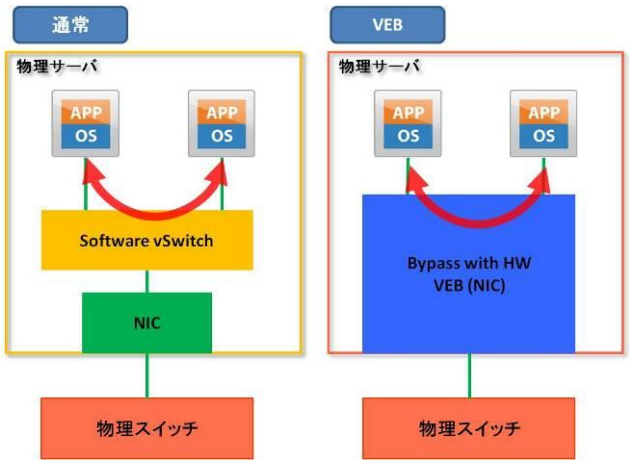


図 3-3j　VEB の通信イメージ

仮想スイッチ(vSwitch：Virtual Switch)で実施されていたパケット転送を、物理 NIC に処理させることで、CPU 負荷を抑え、高いパフォーマンスを実現可能になります。
ただし、現時点で製品化されている物では、アクセスリストやモニタリング等の機能を利用できない製品が多いため、これらの機能が必要な場合は注意が必要です。

(2) VEPA

VEPA とは、仮想サーバ間の通信を、外部の物理スイッチの機能を使って折り返す機能になります。

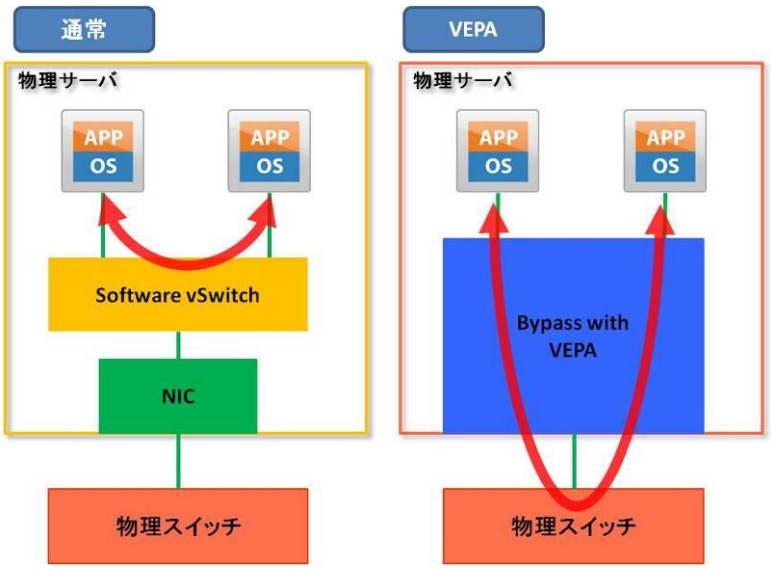


図 3-3k　VEPA の通信イメージ

VEPA では、すべての通信が外部の物理スイッチで転送されるため、サーバ、ネットワークの管理境界が明確になり、従来通りネットワーク管理者がネットワーク機能を運用・管理することが可能となります。また、アクセスリストやモニタリング、QoS(Quality of Service)等の機能も従来通り利用可能です。ただし、全ての通信が一度外部スイッチに転送されてい

る為、折り返し通信により外部ネットワーク接続用の帯域を多く消費してしまうというデメリットもあります

表 3-3c VEB vs VEPA

比較項目	標準仮想スイッチ	VEB	VEPA
パケット転送処理	物理サーバ内(CPU)	物理サーバ内(NIC)	物理スイッチ
パフォーマンス	△	○	○
外部ネットワーク帯域	○	○	△
機能性	モニタリングや QoS 等の機能が不足している機器が多い	モニタリングや QoS 等の機能が不足している機器が多い	物理スイッチの機能を使えるため比較的、高機能
ネットワーク管理	サーバ担当者	サーバ担当者	ネットワーク担当者

(3)VDP(VSI discovery and Configuration Protocol)

VDP とは、仮想サーバの移動に伴う物理スイッチの自動設定変更を支援する為のプロトコルです。

物理スイッチとハイパーバイザとの間でやり取りされ、物理スイッチのどのポートに仮想インタフェース(仮想サーバと仮想スイッチをつなぐインタフェース：VSI)が所属しているのかを把握します。この情報を用いることで、仮想サーバが異なる物理サーバ、異なるスイッチのポートの先に移動したことを検知し、物理スイッチの設定を自動的に変更することが可能となります。この機能により、仮想サーバのライブマイグレーションを想定したネットワークの設計、設定変更負荷が大幅に軽減されます。

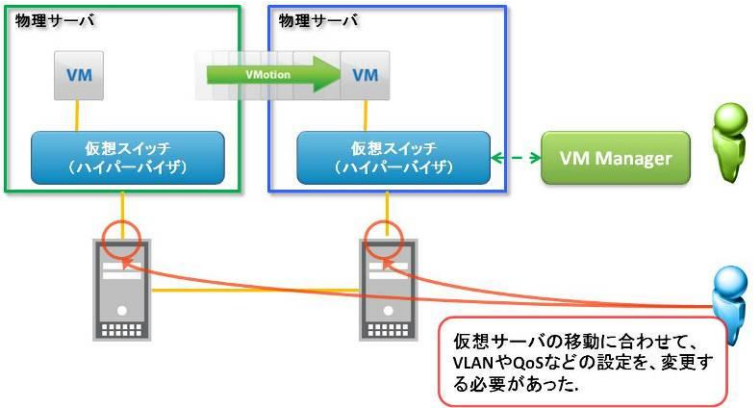


図 3-3l　従来の運用

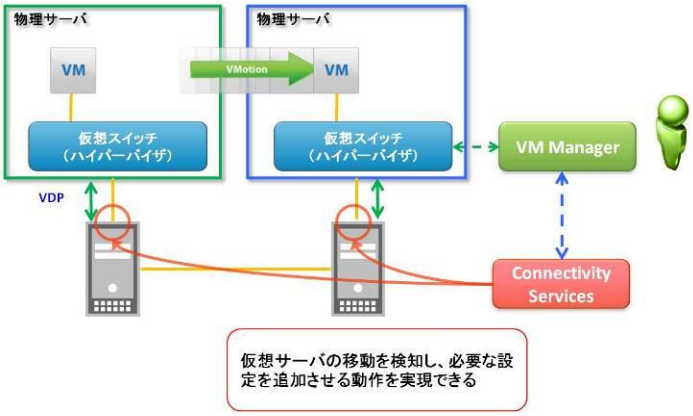


図 3-3m　VDP を利用した自動化イメージ

３－３－５．ストレージネットワーク

(1)仮想化・I/O とネットワーク統合

ストレージネットワークについて触れる前に、現在のストレージを含めたネットワークの傾向について、簡単にまとめてみますと、大きく２つの要素を考慮する必要があります。１つは仮想化とネットワークの関係、もう１つは I/O とネットワークの関係になります。昨今の技術革新に伴い、仮想化と I/O のそれぞれについて、幾つかの課題もあり、ネットワーク設計・構築・運用に大きな影響を与えるようになっています。

①仮想化とネットワークの関係

各種の企業バックボーンを支えるデータセンター内部では、一般的に複数の異なるネットワークが運用されています。代表的なイーサネットに加え、ストレージネットワークとしてイーサネットベースの iSCSI（IP-SAN） とファイバーチャネル SAN（FC-SAN)、広帯域低遅延通信として特別な用途で使用される InfiniBand といったネットワークが多くの環境では混在していることも珍しくありません。

仮想化の進展により生じた課題として、今までのシステムにはなかったネットワーク用途が増え、仮想化環境の管理やコントロール用途等に対して、1 つのサーバ／ホストから複数のネットワークへの接続が必要となっていることが挙げられます。それに加えてビジネスの拡大や加速に対応すべく、システム毎にもネットワークを増設する要求も増えています。よって、利用者の要求に対応してネットワークへの要求は増大し、ポート数や VLAN 数は増加の一途を辿っています。

これらの課題に対して、ネットワークを物理的に統合し、その中身を論理分割して効率化を図るという技術が台頭してきているのが現在の傾向です。

②I/O とネットワークの関係

サーバやホストに対しても同様に、新しい課題への対応が求められてきています。複数の用途のネットワークが増えることで、トラフィックは増加し、またより大きなデータサイズや膨大な量のデータを一気に扱うような要求も増えたため、従来の技術や設計では要求されるスループットに応えられないという課題が出てきました。これに対応すべく、トラフィックの増加やスループット向上への要求に対応するための新しい I/O 技術が台頭してきています。

従来のサーバ I/O はネットワークとストレージに関して完全に分けて考えられており、スイッチやケーブルをそれぞれに対して用意しなければなりませんでした。それ故に、サーバ I/O もネットワークの末端であるにも関わらず、ネットワークとストレージで別の投資をすることになり、一部の利用者等から疑問の声があがっていました。

昨今、技術の向上や市場ニーズの変化に伴い、サーバとストレージの間で閉じていたストレージトラフィックが、ネットワーク上に集約される事例が増えてきており、トラフィックバースト等による影響を回避するための適切なネットワーク設計を考慮することがますます重要になってきています。また各社からも、I/O やネットワークに関する最新の技術に対応した製品が次々と登場してきており、こうした動向からも、I/O やネットワーク周りに関連する技術動向や仕様について知ることは、今後のデータセンターネットワークの運

用を考えていく上で非常に重要ことになってきています。

最近の技術革新の流れを受け、全ての I/O を“ファブリック”という概念で統一することで、いわゆる従来の意味のネットワークとストレージは完全に別という考え方から解き放ち、同じネットワーク技術として考える素地ができてきています。

この考えに則って I/O を物理的に統合することで、スペース、リソース、運用負荷の削減を図り、効率的に利用することで、コスト効果を期待できることが、新しい技術の台頭を後押ししています。

(2) ファブリックの統合と 10 ギガビットイーサネットの普及

前述のファブリックという概念で統一することで、仮想化プラットフォームやストレージも含めた企業のシステム環境を複数の管理ドメイン間でシームレスに管理することができるようになります。ただしストレージトラフィックも統合されることで、トラフィックバースト等によるデータロス等を防ぐという課題を解決するために、トラフィックフローを今までよりもより最適化して提供できることが必要となってきます。

サーバにはイーサネット用に NIC（ネットワークインタフェースカード）とファイバーチャネル用に HBA（ホストバスアダプタ）が搭載され、ネットワークアーキテクチャの各レイヤにそれぞれスイッチを冗長化して導入してきましたが、最近ではサーバ側のインタフェースとしてそれらを統合するコンバージド・ネットワーク・アダプタ （CNA）も使用されるようになってきています。

コンバージドネットワークとは、ファブリックの統合（ユニファイドファブリック）を実現するために必要な技術で、10 ギガ以上のイーサネットをベースに考えられています。ユニファイドファブリックにより、データセンター内の I/O の基盤を統合することができ、シンプルなネットワークを構築することができるようになります。

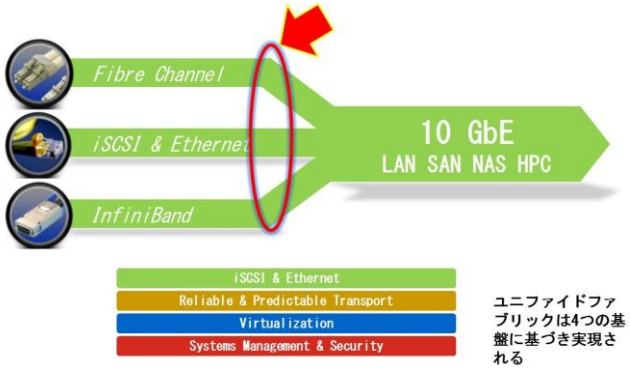


図 3-3n　ユニファイドファブリック

ユニファイドファブリックにより、サーバの各ネットワークカード枚数、スイッチポート数、ケーブル数削減を実現でき、各機器にかかるコストの削減を期待できます。また、機器数やケーブル数の削減は、ラック内部の通気性能の向上を促進し、より効率的な空調と空間利用の実現により、消費電力や設置面積等での長期的な TCO 削減効果も期待されます。

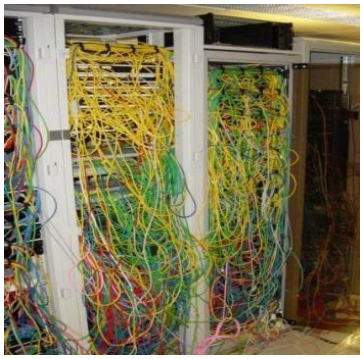



図 3-3o ケーブルの状態によってはハードウェア機器背面の熱溜りの問題を引きおこす。

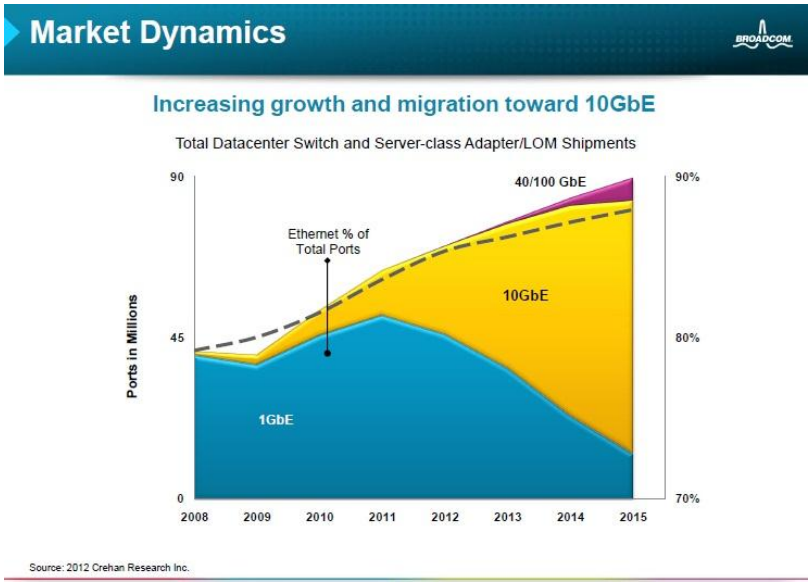
サーバハードウェアの観点からも、2012 年初頭のインテル社の新世代 CPU の登場に伴い、特にブレードサーバのオンボードイーサネット NIC では 10 ギガビットイーサネットを標準搭載するような動きが加速しています。背景としては、以下の 2 つが大きく影響しています。今後もこの動きは広まっていくと想定されます。

- CPU 性能が向上し、より多くのコアを搭載できる新しい世代の CPU の登場により、10 ギガビットイーサネットの帯域を生かしつつ、仮想サーバや仮想デスクトップを搭載したホストからのトラフィックをより柔軟に処理できるようになったこと。
- PCIe Gen3（Interconnect Bandwidth 8Gb/s）の登場により、サーバ等へ標準搭載されるようになってきているため、x8 レーンの場合には双方向で 64Gb/s の帯域を確保できること、また 10 ギガビットイーサネットなら 6 本まで、40 ギガビットイーサネットなら 1 本までをフルスピードで処理可能となったこと。

ファブリックが統合されることにより、同じスイッチやインタフェース上でストレージトラフィックを扱うことも考慮する必要があります。イーサネットをベースにしたネットワークにおいてストレージトラフィックを導入することは、設計次第ではストレージへの I/O 性能に影響を与えてしまうことになりかねません。影響を考慮すべきポイントは下記になります。

- サーバ側インタフェースがストレージトラフィックを通すのに十分な帯域幅を持っていること。
- ストレージ側インタフェースが帯域を制御できる機能を持っていること。
- ネットワークにおける帯域制御設計を実施できること。
- ストレージトラフィックをロスしない設定にできること。

またイーサネットの市場の状況としては、2011 年から 2012 年にかけて、10 ギガビットが急速に増えています。既に市場出荷の約 1/3 を占めるまでになってきており、今後は 10 ギガに置き換わっていくことが加速すると思われます。



出展 http://www.broadcom.com/docs/features/Broadcom_PowerDell_HP_PPT.pdf

図 3-3p インターネット市場予測

以上のように、今後のトラフィックバーストやデータ量増加に対応するためには 10 ギガビットイーサネットへの移行を検討する必要があります。ストレージのトラフィックも考慮すると、正しい設計の元に 10 ギガビットイーサネットを導入することは一般的になりつつあり、10 ギガビットイーサネット自体は、もはや普及した技術であるといっても過言ではありません。データセンター運用としては、10 ギガビットイーサネットを標準に据えた検討を早急にする必要があります。

⑶ストレージトラフィックに関連するネットワークプロトコル

ストレージトラフィックがネットワーク上に集約される要求が増えるにあたって、ストレージトラフィックに関する技術はどのようなものがあり、どういった技術がベースとなっているかを把握しておく必要があります。ストレージトラフィックを導通可能なネットワークプロトコルとして、主に下記 4 つがあげられます。

①ファイバーチャネル
②iSCSI
③FCoE
④InfiniBand

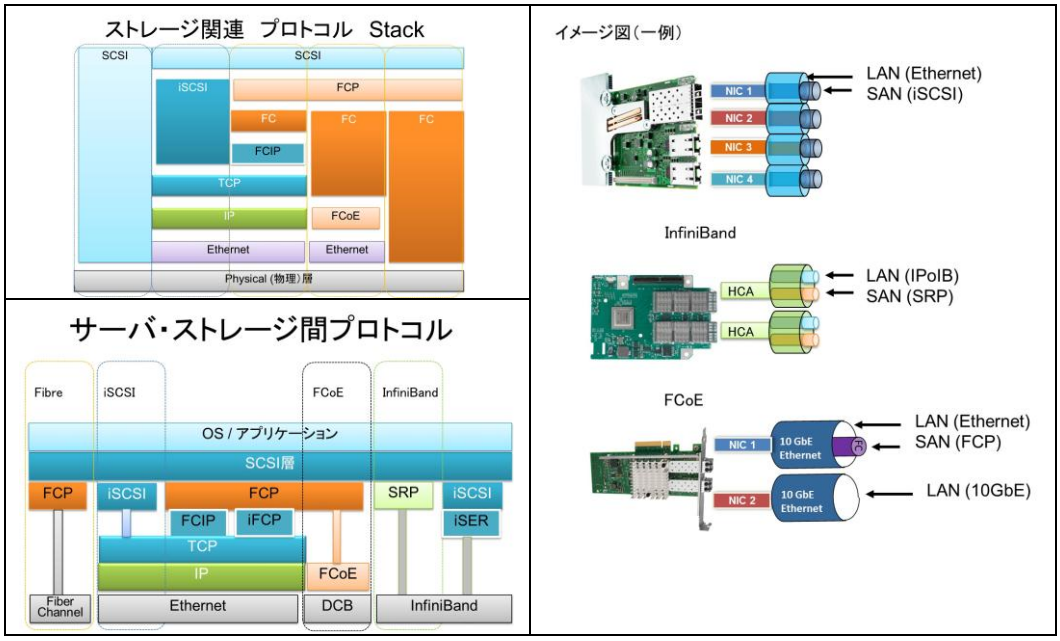


図 3-3q 技術トレンド

①ファイバーチャネル

INCITS(情報技術規格国際委員会）の T11 技術委員会により標準化された、主にストレージネットワーキング（SAN - Storage Area Networks)で使用されている、ギガビット速度のネットワーク技術になります。ファイバーチャネルプロトコル（FCP）は、ファイバーチャネルネットワーク上で SCSI コマンドを転送するためのトランスポートプロトコル（IP ネットワークで使用される TCP に相当）であり、ファイバーチャネルを使用することで、ネットワーク上で SCSI コマンドをやり取りすることができます。

・Fibre Channel Backbone（FC-BB）

この規格は、ファイバーチャネルをトランスポートとする際のマッピング等に関する定義を主に行うための規格になります。これにより、ファイバーチャネルを様々な伝送プロトコル上で通信させることができるようになります。最近の規格動向としては、下記が主なものとなります。

- FC-BB-5（標準化済）:

ファイバーチャネルを様々なネットワークトランスポーテーション上で伝送させる様式を決める規格。主に TCP/IP、イーサネット等でファイバーチャネルをマッピングするための決まりごとを決めています。FCoE や FCIP のスタック等はこの規格で決められています。

- FC-BB-6（標準化検討中）

ネットワークトランスポート上でのファイバーチャネルのエンドデバイス間でのやり取りやスイッチ側の応答に関して等を議論しています。最近は主に FCoE Initialization Protocol 等が議論されています。

②iSCSI（Internet Small Computer System Interface）

既存のイーサネット環境上に導入可能なストレージ通信用プロトコル。TCP/IP をベースとした SCSI コマンドのマッピングにより、デバイス間のブロック I/O をネットワーク上で実現

可能です。既存環境との親和性が高く、導入時の初期投資を抑えることができます。通常のイーサネットベースの基盤を利用することで、信頼性の低いネットワークでのパケットロスへの対応等を再送処理やエラー訂正等の機能により実施することで、ストレージ I/O としての信頼性を高めています。

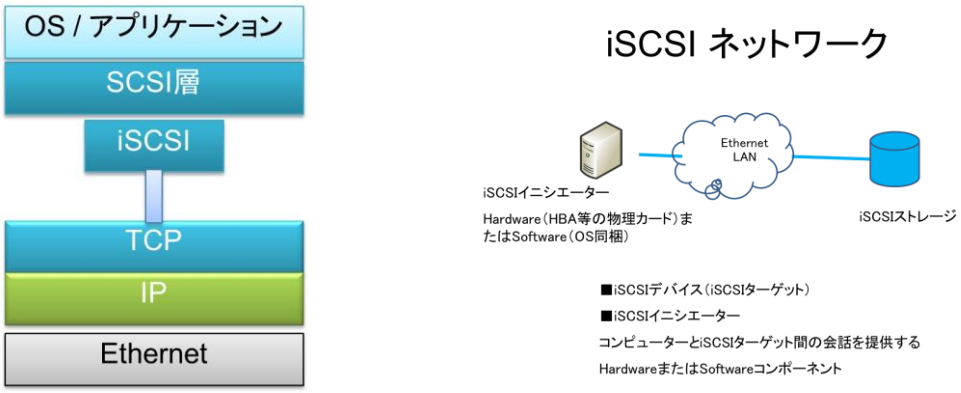


図 3-3r iSCSI

③Fibre Channel over Ethernet (FCoE)

ファイバーチャネルをイーサネット上にマッピングするプロトコルで、FC-BB-5 の 1 つの規格として定義されています。基本の通信はファイバーチャネルなので、既存ファイバーチャネル環境にあるストレージとの共存が可能になります。ただし、イーサネット上で動作させるため、ロスレスなイーサネット環境を用意して、データロス確率の非常に低いネットワークを構築する必要があります。よってロスレスイーサネットに対応したスイッチが必要となり、従来のイーサネットスイッチでは対応不可となりますので、構築時には注意が必要です。

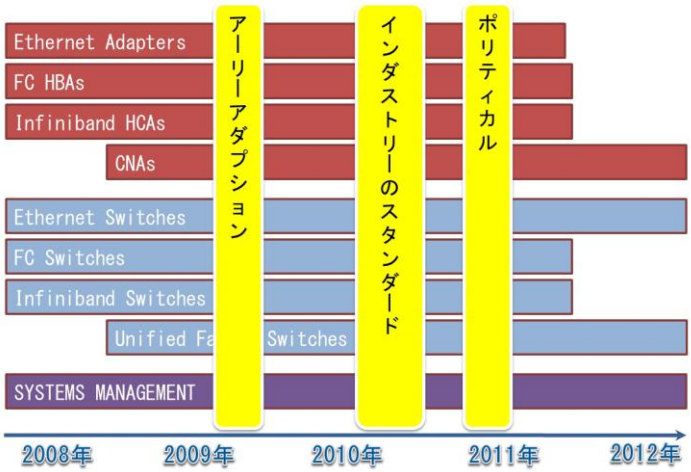


図 3-3s FCoE への進化の動向

FCoE では、10GbE ギガビットイーサネットのデータリンク層相当部分を DCB（Data Center Bridging）という技術で拡張し、パケットロスを防ぐ（ロスレス）事により信頼性を高め、イーサネット上でファイバーチャネルフレームを伝送させることができるようにカプセル化します。よってその実現にはイーサネット拡張が必須で、そのベースとなる DCB は、別章でも触れているように、既に標準化されています。

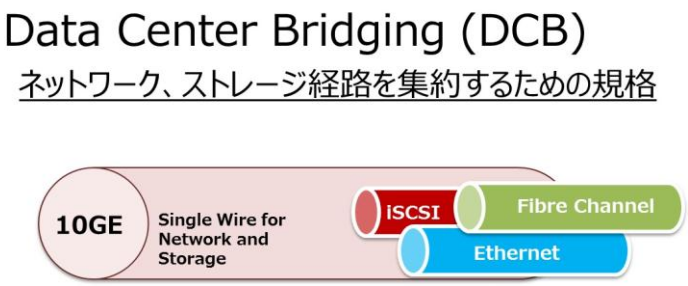


図 3-3t DCB

④InfiniBand

InfiniBand は、ハイパフォーマンス・コンピューティングとエンタープライズのデータセンターで使用されているスイッチファブリック間の通信リンクです。ストレージ I/O というよりも、通信を高速化することに主眼を置いた技術です。高スループット、低遅延、サービス、およびフェイルオーバーの品質、といった特徴をスケーラブルに生かせるよう設計されており、上位にイーサネットやファイバーチャネル等をのせられる高速サーバ間通信プロトコルです。複数の転送レートをサポートしており、PCI Express のように複数のチャネルを束ねることも可能です。

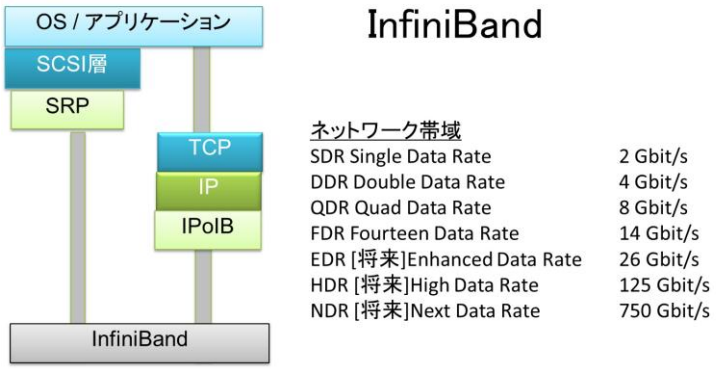


図 3-3u InfiniBand によるネットワーク統合

(3)イーサネットの更なる進化（40／100 ギガイーサネット）

イーサネットはさらに拡張を進められており、一部では既に 40 ギガまでの帯域幅を実現しております。さらにその先には 100 ギガへの拡張が予定されており、一部では試験的に活用されているところもあります。現時点でのこれらの広帯域イーサネットは、センター間通信等のスイッチ間での通信が主な用途となり、サーバやエンドデバイスからの通信としての実装はま

だ検討が進んでいないのが実状です。トラフィック急増へ対応するためのファブリックのバックボーン通信としての統合が主な用途となります。よって、データセンターネットワークのバックボーン構築の検討には重要なポイントの１つとなります。ストレージサービス等を展開し、バックアップや災害対策等も一緒にサービス提供しているような場合には、センター間の通信のベースとして検討の選択肢に加える必要があります。

(4)オープンなインタフェース仮想化

仮想化と広帯域イーサネットの普及に伴い、帯域を効率的に使用し、仮想化をベースとしたインフラを利用したサービス展開をするような場合等に対して、物理インタフェースを複数の論理インタフェースに分けて利用する技術が注目されています。それらの技術は業界標準という形で実現しつつあります。一般的な総称としては、NIC パーティショニング（NPAR）という表記がされ、文字通り NIC を分割して使用する技術となります。業界標準としては Single Route IO Virtualization（SRIOV）として、2007 年 10 月に PCI バス規格を管理している「PCI-SIG」（PCI Special Interest Group）により策定されています。従来の仮想化においては、仮想マシン毎の IO はハイパーバイザが調停して処理してきましたが、これらの技術を使用することで、その処理をハードウェア側の処理として実装できるようになるため、仮想環境におけるパフォーマンス向上も期待できる技術となります。ストレージも含めた仮想環境の複数ネットワーク制御によるセキュリティの向上や、仮想マシンのパフォーマンス改善によるサービス品質の向上等に貢献する技術となります。

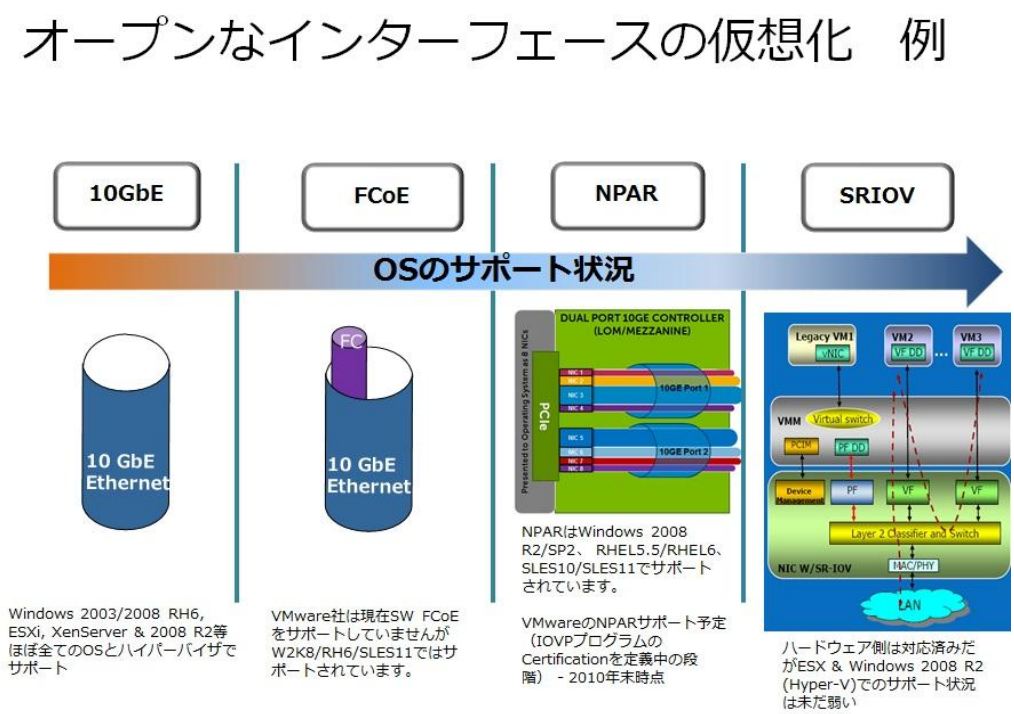


図 3-3v IO インタフェース仮想化

(5) 今後のシステム最適化を支援する技術動向

上述の技術以外にも、仮想化やクラウドでの I/O を最適化又は向上できる様々な技術が登場しています。下記にその一覧をまとめています。ハイパーバイザによるフレームのソーティング、スケジューリング等がパフォーマンス劣化の元となるため、これらを制御できる技術や、10 ギガビットイーサネットの恩恵を受けられるように、ハイパーバイザのバイパスを行うことのできる技術も登場してきています。これらも利用することで、仮想環境におけるストレージ I/O の劣化やトラフィックの厳格な区分けにより制御等の課題を解決できる可能性があります。

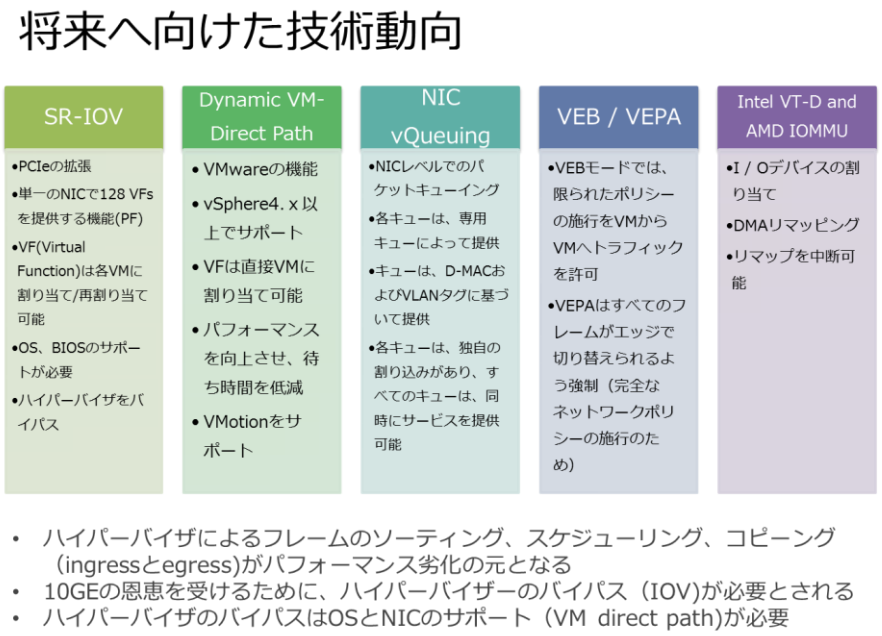


図 3-3w IO 最適化技術の一覧

３－３－６．今後注目される SDN とは？

(1)SDN(Software-Defined Networking)概要

これまでのネットワーク機器は、ハードウェアとソフトウェアが一体化されたモデルが一般的でした。同じメーカがハードウェア、ソフトウェアの両方を開発・提供し、独自の機能や付加価値をつけることで、メーカ毎に特徴のある製品が提供されておりました。しかし、それらの独自機能や付加価値は相互接続性が保証されていない物が多く、マルチベンダ環境、ベンダーロックイン環境、共にネットワークコストの削減の難しさの一因となっていました。

SDN は、これらの課題を解決する手段として、注目されているコンセプトです。SDN では、これまで個別のネットワーク機器で提供されていた様々なネットワーク機能を、ソフトウェアにより一元的に制御します。また、SDN によるネットワークの仮想化・自動化により、Network as aService 等の新たなサービスの実現や、サービスリードタイムの短縮などのサービスレベルの向上、ネットワークトータルコストの削減等が期待されています。

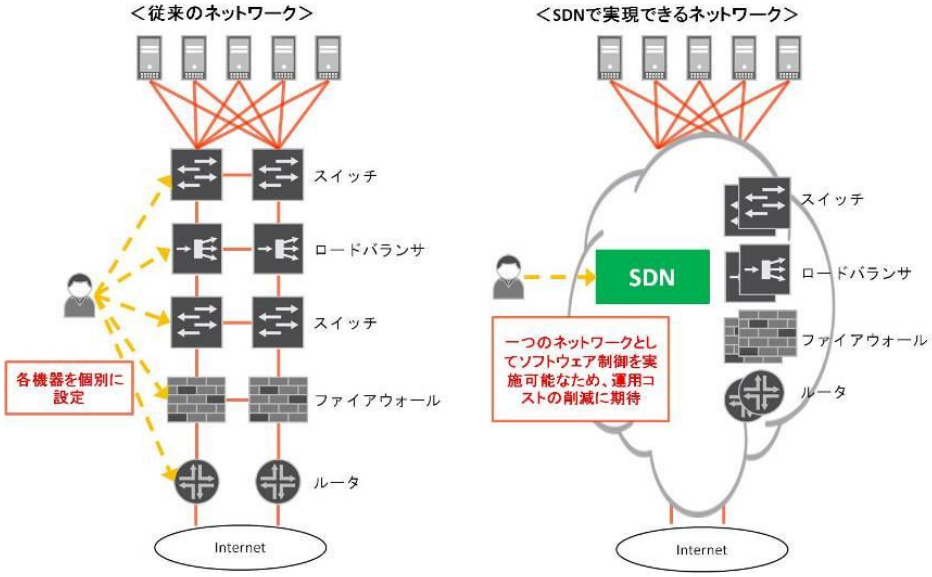


図 3-3x　SDN のコンセプト

(2)SDN アーキテクチャ概要

従来のネットワーク機器では、制御部分であるコントロールプレーンと、実際にパケットの処理を行うデータプレーンがそれぞれの機器に搭載されていました。これに対し、SDN では、コントロールプレーンとデータプレーンを分離し、コントロールプレーンを SDN コントローラーに統合することで複数機器の処理情報をまとめて一括制御します。

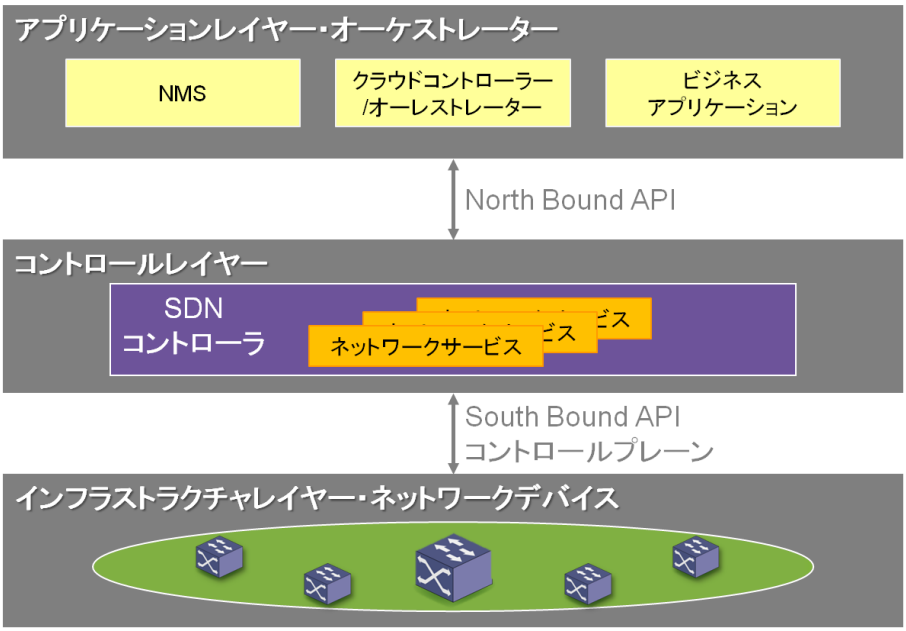


図 3-3y SDN のアーキテクチャ概要

また、SDN コントローラーの多くは外部からの制御を容易にする為の API(Application Programming Interface)を備えております。これによって、ソフトウェアによってネットワーク全体の構成を動的に制御することが容易になります。

(3)OpenFlow 概要

SDN において、コントローラーとネットワーク機器間で情報伝達を行う為の手法には幾つかの候補がありますが、代表的なプロトコルとして OpenFlow が知られています。

従来の L2 スイッチ、L3 スイッチでは、MAC アドレス、IP アドレスに基づきパケット転送を実施しておりましたが、OpenFlow ではフローと呼ばれるトラフィック単位毎にパケット転送を行います。フローは、MAC アドレス、IP アドレスの他に、物理ポート番号、MPLS (Multi Protocol Label Switching)ヘッダ、VLAN ID、TCP/UDP ポート番号等の情報を元に定義可能であり、より柔軟な経路制御、QoS の適用が可能となります。

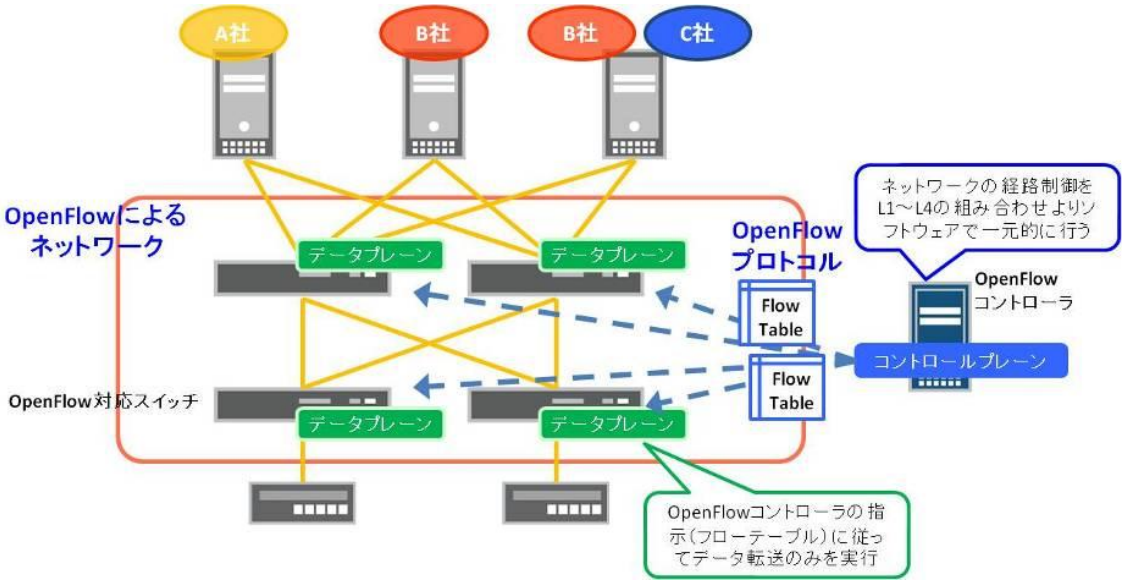


図 3-3z SDN(OpenFlow)のイメージ

OpenFlow ではスイッチはフローのみを参照して転送を行うため、複数のフローで IP アドレスや VLAN ID が重複している場合でも競合が発生することなく転送が可能となります。これにより VLAN に依存しないマルチテナントを実現することも可能です。

(4)SDN の標準化と今後の期待

SDN は、ONF(Open Networking Foundation)、OpenDaylight、ONRC(Open Network Research Center)、IETF(Internet Engineering Task Force)等で標準化、実装に当たっての検討が行われています。また、関連、補完し合う概念として NFV(Network Function Vertualization)との協調も注目されています。

利用可能なソリューションや適応範囲はまだ少なく、メーカ間の相互接続性にも課題がある状況の為、OpenFlow / SDN で出来ることは現時点ではまだ限定的と言えますが、標準化の推進、今後の機能拡張・適応範囲の拡大、様々なメーカからの製品リリースが期待されております。

特に、今後より高い拡張性や柔軟性が求められるデータセンターネットワークにおいては、SDN ベースのネットワークが普及することが予想されています。

３－４．運用管理

３－４－１．目的

昨今のインターネットサービスの利用拡大とクラウドサービスの勃興により、これらを支えるデータセンターの運用管理はより複雑になってきており、更に顧客の品質に対する要求レベルも高いものとなってきています。とりわけネットワークを中心としたシステム群の運用品質の向上はこれらすべてのサービスに直結しているため、極めて重要といえます。

本章は前述のネットワークを中心としたシステム運用についてベンチマークとなるべく、標準的な内容について記したものです。

３－４－２. Scope of Network Operation

運用業務を行う上で最初に重要な事は、その運用業務の範囲を定義づけることです。所謂責任分界点を明確にすることとなるが、これは定常時の運用や故障対応時に問題箇所を切り分ける上で最初に認知すべき重要な情報とも言えます。

その上で本章では「Scope」という観点で２つの整理を行います。一つはデータセンターシステム全体に置ける「ネットワーク」そのもののスコープであり、もう一つは同じくデータセンター全体に置けるネットワークに関わる「業務範囲」というスコープです。後述しますが、前者においては故障対応時の問題所在を明確にする為に有益であり、他方後者は故障対応等の業務的なボトルネックを明確にする為に有益な情報となり得ます。

(1) Scope of Network

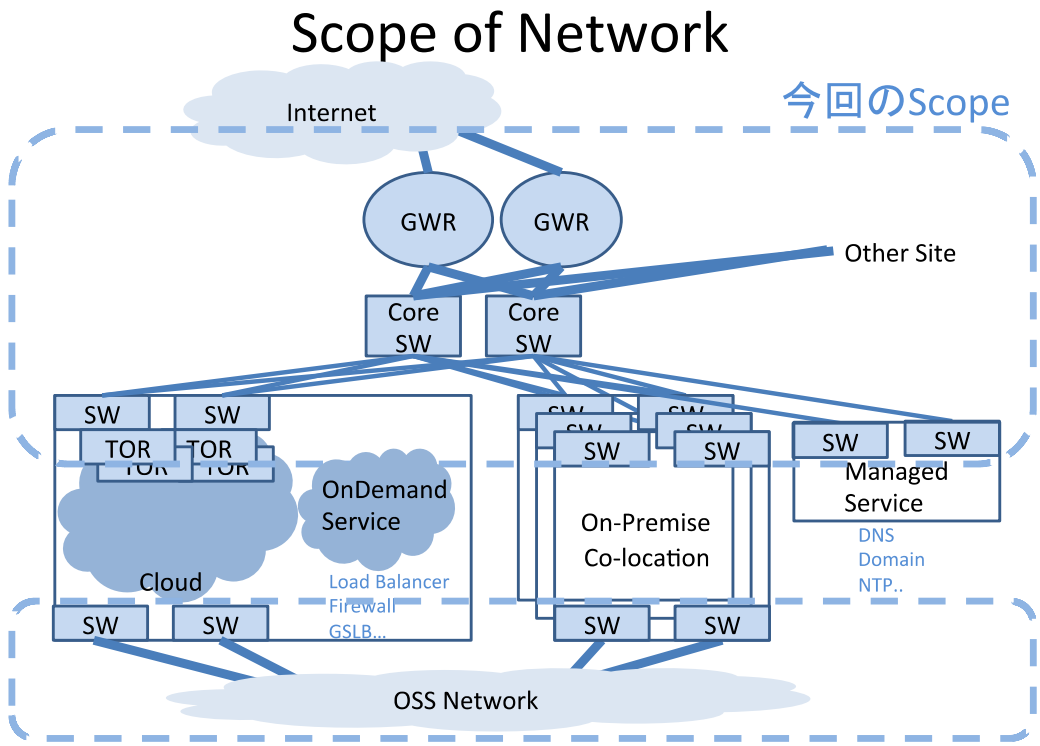


図 3-4a Scope of Network

（2）Scope of Work

ここではデータセンター内における運用業務に関わる組織を定義します。
大きく「フロント系管理業務」「サービス品質維持管理業務」「設計構築及び構成管理業務」の３つに分類します。それぞれ事業者内の部署イメージ、業務分署／内容、期待されるアウトプット、課題について詳説していきます。

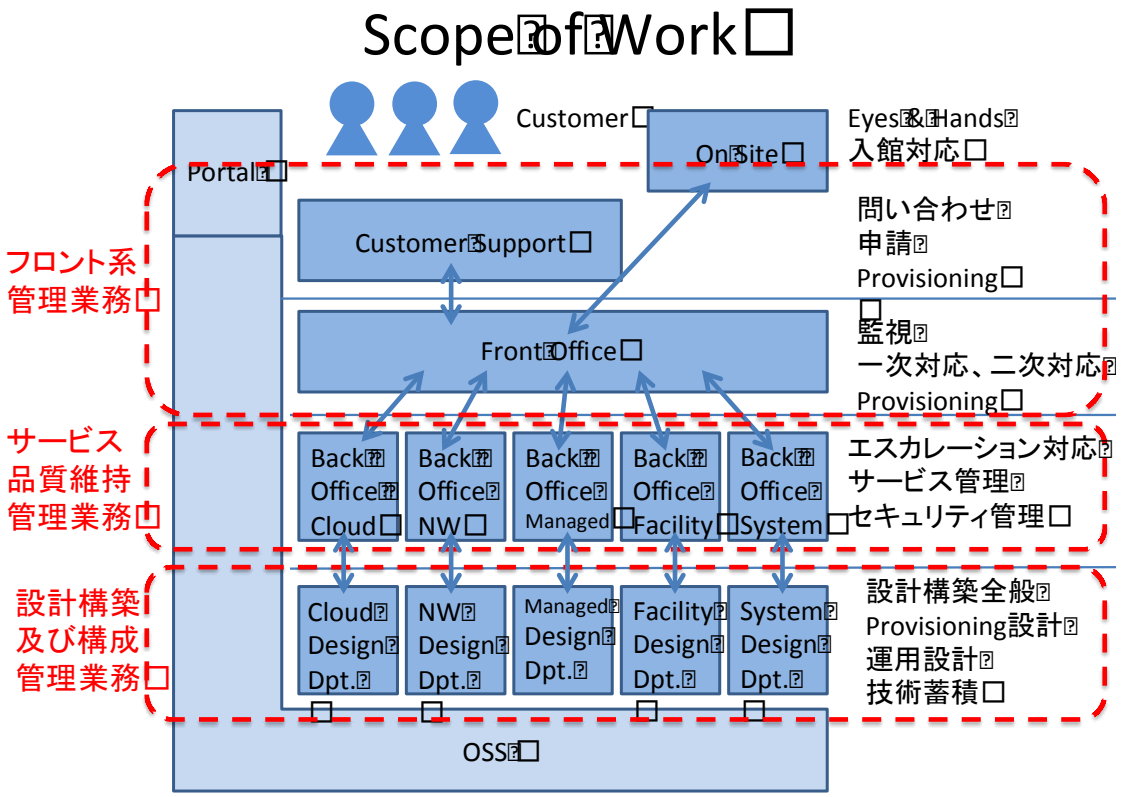


図 3-4b Scope of Work

①フロント系管理業務

・事業者内部署イメージ
全てにおいて最初のインプットを受ける部署であり、利用者からのインプットであればカスタマーサポートやテクニカルサポートとなります。また監視システム等からのインプットであれば監視オペレーター部門のような部署がそれに相当します。

・業務分掌／内容
カスタマーサポートやテクニカルサポート部門であれば、顧客からのテクニカルな相談、故障受付、顧客へのメンテナンス通知、顧客からのサービスオーダー受付などを行ないます。
監視オペレーター部門であれば、まずは監視システムからのアラーム対応。二次サポート

へのエスカレーション。マニュアルに定義されている範囲の異常部位切り分け、パラメータ変更、サービスプロビジョニング。定常時のパフォーマンスモニタリング、業務品質測定。品質改善への提案、各業務のマニュアル整備などを行ないます。

・期待されるパフォーマンス／有るべき姿
基本的には整備されたマニュアル上の業務を正確かつ迅速に行う事が求められます。顧客への対応も含まれる事から常に冷静沈着であり安定的な業務遂行が理想とされます。また細やかな問題点にも気付き、それらをチーム内での改善活動に活用し、バックオフィスチームへの改善提案などを積極的に行うことも重要です。

・課題
この業務においての課題は、アラームの見逃しや判断の誤りなどの人為的ミスの発生やスキルレベルのばらつき・個人のノウハウへの依存などがあげられます。また２４時間３６５日のシフト勤務である場合が多いので業務の平準化や安定性が重要です。

②サービス品質維持管理業務

・事業者内部署イメージ
定常組織としては各サービスの運用部門が該当します。フロント系管理業務部門で一次切り分けが困難なインシデントや、より高度な障害対応が求められる場合に技術的バックグラウンドをもった運用者によってこれらを解決に向かわせます。また設計構築部門と対峙する部署として設計構築部門がリリースしようとするサービスや構成変更などが顧客へのサービス品質を鑑みた上で受け入れ可能かどうかの判断や牽制を行うのも重要な役目となります。その他に定常組織以外では品質管理委員会などの横断的組織もこの範疇となります。

・業務分掌／内容
フロント系業務部署からのエスカレーションを受領し障害や問題の高度な切り分けと原因分析、復旧を行ないます。サービス品質の定義と定点観測の内容決定、これに基づく品質向上施策の策定。リスクの管理とセキュリティ対策、キャパシティの管理、パートナー・サプライアの管理など多岐にわたる業務を行ないます。併せてフロント業務部門で集約された顧客からの声を各部門へフィードバックを行う起点ともなります。

・期待されるパフォーマンス／あるべき姿
全てのステークホルダーとの間でサービスレベルやセキュリティ要件を高いレベルで策定することが求められます。ここでいうステークホルダーとは顧客、経営陣、設計部門、フロント系管理部門等です。それぞれの立場で相違がみられる意見を集約しつつサービス事業者として事業継続可能なポイントを抽出しなければなりません。
またこれを維持しより高いサービスレベルやオペレーションレベルを目指す為に日頃のオペレーションの見える化を行い、所謂 PDCA サイクルを廻し一定の評価と施策を検討しなければなりません。その中で顧客や顧客と対峙するフロント部門あるいは設計部門へのフィードバックを定期的に出す必要があります。

・課題

この業務においての課題は、常にコストと対峙しながらサービスレベルやセキュリティレベルを維持することにあります。具体的にはミスオペレーションの撲滅策や顧客影響を常に念頭においたメンテナンス計画、技術設計部門との調整などがあげられ、それらは全てにリスクマネジメントを念頭に置きながら遂行して行く必要性があります。

④ 設計構築及び構成管理業務

・事業者内部署イメージ

定常組織としては各サービスの設計構築部門がそれにあたります。顧客ニーズやマーケットトレンドを反映し企画部門等から新規サービスの提案、既存サービスの改変などに対して技術的にソリューションを導き、実サービスネットワークへ基本設計から実施設計、サービス検証、構築、サービスリリースまでを行う部門です。「運用品質の８割は設計品質に左右される」という言葉があるように、コストとの見合いをとりながらも運用品質を念頭においた設計は事業全般に影響を及ぼす重要な要素となります。またここで構成されたネットワークの構成情報が運用情報の全ての起点となることから運用上も重要な任務を果たす部門です。

・業務分掌／内容

基本設計時におけるトポロジーおよび設定ポリシーの定義、運用設計に関わるネットワーク品質設計。顧客回線からバックボーンにいたる全てのネットワーク構成の管理、変更時の更新、機器インベントリ情報の管理など定常運用に引き渡す以外の全てのコントロールを取り仕切ります。また新技術導入に関する情報収集や運用からのフィードバックによるナレッジ収集蓄積なども重要な業務です。

・期待されるパフォーマンス／あるべき姿

最新の技術トレンドとコストパフォーマンスを追求しながらも常に顧客志向、サービス品質指向の設計を心がけ、運用部門への負担を最小限に抑える事を目指すべきです。基本設計からリリースまで全てのプロセスでこれらが求められますが、最も重要なのは「サービス検証」プロセスです。ここでのアウトプットの精度の高さが事前の不具合を撲滅し、リリース後の安定品質に繋げることとなります。加えて運用上の起点となる構成情報管理が常に正確に反映される仕組みづくりを行う事も重要な任務となります。

・課題

この業務においての課題は、企画部門ならびに運用部門の要望とコストパフォーマンスの折り合いをつけた設計構築を行う事です。つまり顧客要望を満たしながらも限られたコストの中で安定した運用がなされる設計や、運用部門へ引き渡された後の業務遂行が安定的に行える環境を如何に構築するかです。

３－４－３．ITマネジメントシステム

(1)NGOSSとeTOM

NGOSS（new generation operations systems and software）は、通信事業者の業務にかかわるオペレーションを柔軟かつスリムにするためのフレームワークで、ビジネスプロセスの自動化を実現するOSS/BSSを構築するガイドラインとして、①ビジネスプロセス、②情報モデル、③システム統合方式、④アプリケーションコンポーネントに関するノウハウを集大成したものです。

NGOSSのフレームワークは、eTOM（enhanced telecom operation map）、SID（shared information/data model）、TAM（telecom applications map）、TNA（technology neutral architecture）という4種類のフレームワークで構成されます。

その中でもeTOMは業務プロセスのフレームワークで、NGOSSフレームワークでは最も頻繁に採用されており、所謂「サービスオーダー」「故障受付」「回線開通」等通信事業の業務プロセスをグローバルに通用する用語で統一し、通信事業者、ソフトベンダー、システムインテグレーターが共通に使える情報定義を提供しています。バラバラに構築された既存システム群を整理する際に必須となる情報体系の整理統合のガイドラインとして有用です。

(2)TQM

TQM（total quality management）は全社的品質管理手法のTQC（total quality control）を基盤とし、その考え方を業務や経営へと発展させた管理手法です。品質をトータル管理することが目的であり、ITサービスに限らず様々な業種における経営的なマクロ視点から顧客満足度向上および品質を向上するためのマネジメント手法を取っており、経営品質の向上を主眼としています。

(3)ITILv3 （Information Technology Infrastructure Library version3)

英国商務局（OGC：Office of Government Commerce）が、ITサービス管理・運用規則に関するベストプラクティスを調和的かつ包括的にまとめた一連のガイドブック集です。ITサービス管理を実行する上での業務プロセスと手法を体系的に標準化したもので、ITサービスに関する社内規則や手順などの設定･見直しを行う際のガイドラインとして活用されています。

また、ITILでは「3つのP」という概念があり、これはprocess（過程）、people（人）、products（成果物）の3つを指します。これらはプロセスだけが充実していても、担当者のスキルだけが素晴らしくとも、どんなに高価で便利なツールを使用しようとも、それぞれがバランス良く配置されなければ効果は得られないと警鐘しています。

さらに 最近はpartners（協力会社） を加え「4つのP」と表現しているものもあり、これは2007年6月に新たにリリースされたITILversion3で大きな要素として盛り込まれ、アウトソーシングが意識されたものになっています。

(4)ISMS

情報セキュリティマネジメントシステム(Information Security Management System) は、企業、組織が情報セキュリティを適切に管理するための仕組みであり、情報資産に関する脅威、リスクをマネジメントすること主眼としています。企業が情報・機密を守るために IT システムのセキュリティ対策だけでなく、全ての情報資産に対するセキュリティが対象となります。

それらのリスクアセスメントを行い、必要なセキュリティレベルを定義し、それぞれのリスク評価を実施する管理手法で、それらを定期的に評価することにより有効なリスクマネジメントを実施するものです。

上記以外にも様々な IT マネジメントシステムとしての手法やフレームワークは存在しますが、データセンター事業者のネットワーク運用においてはシステムにおける網羅性の広範さ観点から ITILv3 が最も適しており、経営的なリスクからサービス品質向上までを包括的に捉えることができると考え、本書においては ITILv3 について解説します。

ただし、それぞれの事業者に置いてそれぞれのサービス内容からどのフレームワークが最も適しているかは、それぞれの判断に委ねます。すでに、その事業者で取得しているマネジメント認証システムがあれば、これに基づいた OSS の構築が早道であると言っても過言ではありません。

また、それぞれのフレームワークには ISO 化されたものもあり、TQM であれば ISO9001、ISMS であれば ISO27001、ITILv3 であれば ISO20000(ITSMS)です。元来認証を取得することが目的ではなく業務分掌、品質向上活動、オペレーションフロー、各種手順書まで一連の流れのなかで IT フレームワークが紐づけられており、あくまでも要求事項を満たしながらコストパフォーマンスの高い運用マネジメントを目指すべきであり、これらを実現する為の OSS の設計や実装がなされることが非常に重要だと考えます。

３－４－４．ITIL v3 からの展開

前述のデータセンター事業者におけるネットワークや運営組織上の様々な問題点や課題を解決する為には標準的で且つ包括的なフレームワークが求められます。とりわけ冒頭にもあるように近年クラウドサービスをはじめ様々なサービスポートフォリオがダイナミックに変化するのに対して事業運営上はこれらを追随する必要があります。ITILv3 はこのような背景においてビジネス要求事項や顧客要求事項などのインプットから顧客へのサービス提供・SLA 改善、満足度向上等アウトプットにいたる中で、前述「4 つの P」等の要素に対して PDCA（Plan ・Do ・Check・Action）サイクルを通じ改善する IT マネジメントシステムと言えます。

以下に ITIL がターゲットとしている PDCA サイクルの概念を示します。

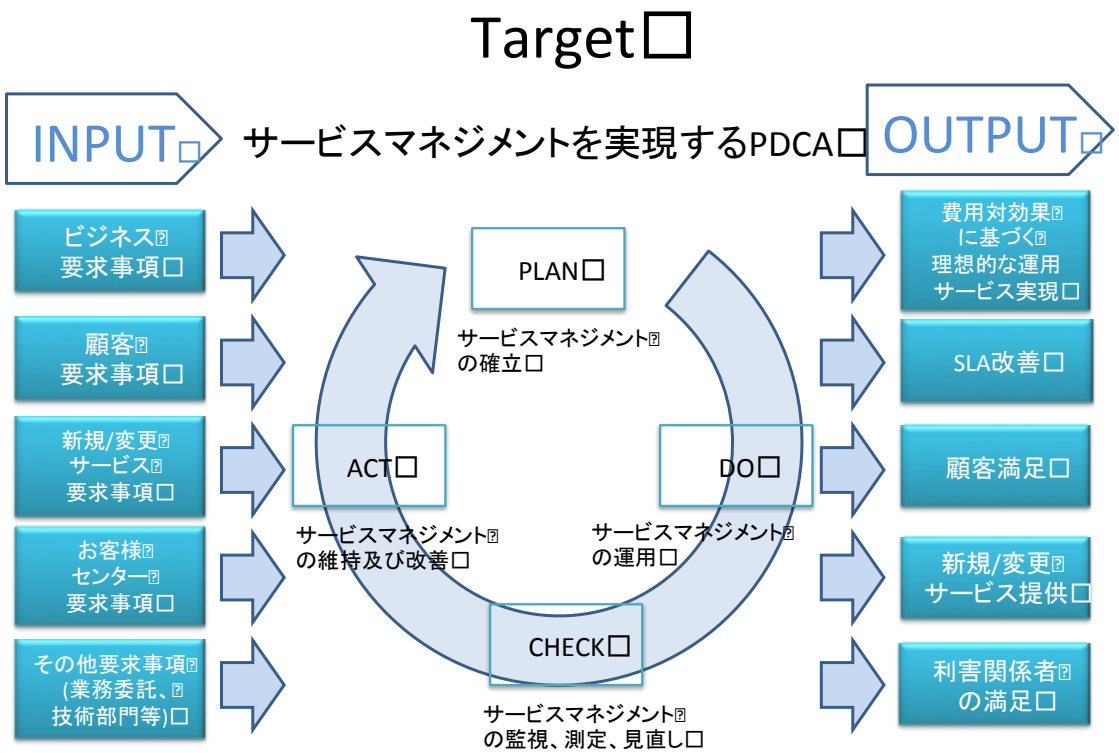


図 3-4c ITIL がターゲットとしている PDCA サイクル

詳しくは ITIL に関する書籍および出典を参照下さい。
推奨図書：毎日コミュニケーションズ発行
「ITIL の基礎 ITIL v3 ファンデーション試験　対応」
出典:特定非営利活動法人 IT サービスマネジメントフォーラムジャパン
：@IT 情報マネジメント「IT サービスをマネジメントする「ITIL」とは？」
http://www.atmarkit.co.jp/im/cop/special/costitil/01.html

３－４－５．Scorp of Work と ITIL v3 の紐付け

ITIL v3 ではサービス・ライフサイクルを示す５つの中核の書籍から構成されています。

- サービスストラテジ（戦略）
- サービスデザイン（設計）
- サービストランジション（移行）
- サービスオペレーション（運用）
- 継続的サービス改善（改善）

以下にそれぞれのプロセス名を示します。全てのプロセスは網羅的に活動すべきですが、今回は主にデータセンター運用で重要とされている赤枠のプロセスに注目して次項以降、内容に応じ解説します。

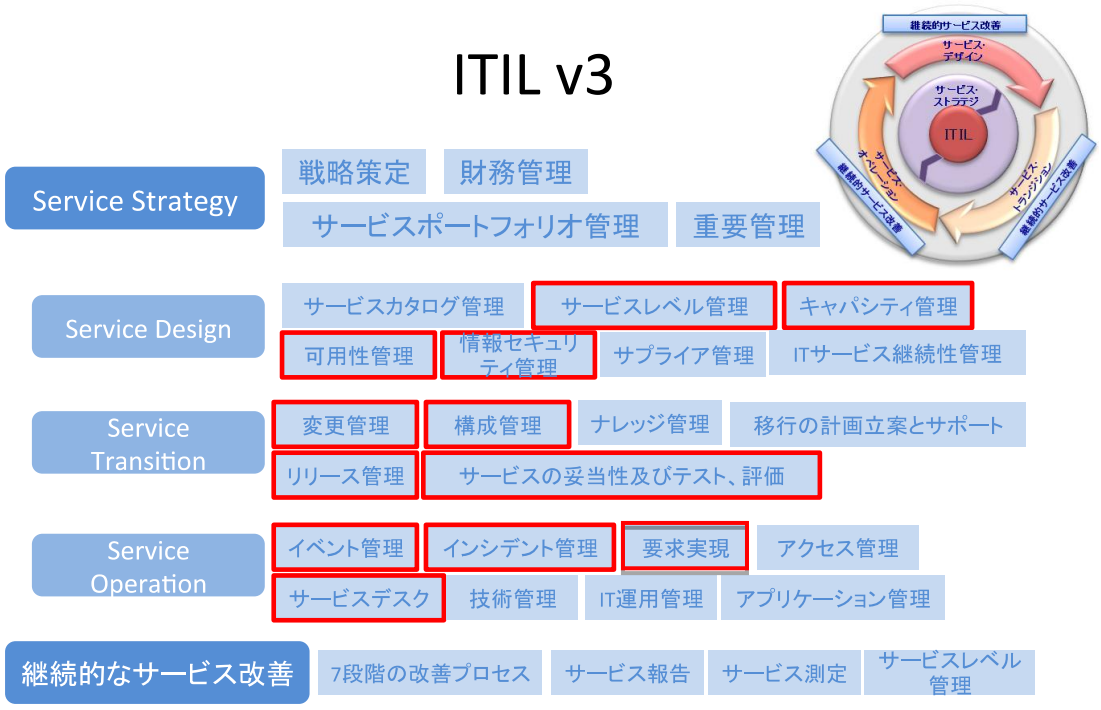


図 3-4d ITILv3

ここでは、３－４－２で述べた Scorp of Work での各管理業務と ITIL v3 のプロセスを結びつけて解説する。

(1) フロント系管理業務と主なプロセス

①サービスデスク（サービスオペレーション）
顧客のために単一窓口を提供し、インシデントやサービスの要求をコントロールします。

②イベント管理（サービスオペレーション）
インフラストラクチャの状態の変化を受け取り、積極的にチェックしながら、サービスの品質の関わる情報を抽出し、そのイベントの内容を担当者に通知することでサービスマネジメント活動のきっかけを提供します。

③インシデント管理（サービスオペレーション）
サービスの品質を損なう、あるいは損なう可能性がある「通常の運用」とは異なる事象=インシデントが解決されるように、カテゴリ化、優先順位付け、エスカレーション判断基準などの一連のプロセスを整備します。

④要求実現（サービスオペレーション）
インタラクション管理ともいい、サービス要求を合意された規則や手順に基づいて処理することで、顧客のサービス利用を支援するプロセスです。
例えば、データセンターへの入館申請やオプションサービスの変更申請に対する対応もこのプロセスに含まれます。

（２）サービス品質維持管理業務と主なプロセス

①サービスレベル管理（サービスデザイン）
顧客との間で明示的な SLA に合意し、それを達成するためにモニタリング、レポーティング、レビュー（チェック）、改善といった定常的なプロセス（PDCA サイクル）を回して、サービスレベルの維持あるいは継続的な品質向上を図るマネジメント活動のことです。

②キャパシティ管理（サービスデザイン）
キャパシティ管理には以下の２つのサブスロセスから構成されます。
サービスキャパシティ管理:サービスパフォーマンスやインフラの利用状況の監視、計測、記録、分析、報告、SLA の目標達成に責任をもつサブプロセスです。
コンポーネント・キャパシティ管理 : サービス品質に影響を与えるリソースの使用状況の監視、記録、分析、報告に責任を持つサブプロセスです。

③可用性管理（サービスデザイン）
一定の期間中にサービスやそのコンポーネントが、要求され合意している機能を供給する能力を可用性といい、この能力が不足する場合にしかるべき部署にエスカレーションし問題解決にあたります。
※　可用性＝実際のサービス供給時間/合意したサービス供給時間×100

④情報セキュリティ管理（サービスデザイン）

事業を営む上で重要とされる情報資産をあらゆる脅威から全社的な企業統治の枠組みの中で守り、情報やサービスを安全に利用できることを確実にする一連の活動です。なお情報セキュリティ管理はITサービスを行う上で情報資産が広範にわたることからここでの詳説は避けることしますが、事業者によってはISMSのフレームワークと織り交ぜながら活動する場合もあります。

（３）設計構築及び構成管理業務と主なプロセス

①構成管理（サービストランジション）

サービス資産の正確な最新情報を提供することで、有効で効率的なサービスマネジメント活動を支援するプロセスです。詳細は後述しますが、全てのプロセスに関係し連動するCMDBを中心とするプロセスで有る為、全体のフレームワークの中で最も重要な位置づけに有るといっても過言ではありません。

②リリース管理（サービストランジション）

顧客に価値を供給できるように、リリースを本番に展開し、サービス運用へ引き継いでサービスの効果的利用を定着させることです。

※ リリース＝承認された１つ以上の変更の実行によって、サービス運用に展開されるインフラストラクチャ、文章、プロセス等の集合を指します。

③変更管理（サービストランジション）

変更に起因する事業への悪影響を抑制し、事業のニーズに整合させる変更要求に対応することでサービスの価値の最大化を図ることです。また、運用上の秩序を守るため、全ての変更は記録され目的やリスクが評価され、テストによって妥当性が確認される必要があります。

⑤ サービスの妥当性及びテスト、評価（サービストランジション）

新規または変更されたITサービスの妥当性およびテストを責務とするプロセスです。サービスの妥当性およびテストでは、ITサービスが設計仕様に合致しており、事業体のニーズを満たすようにします。従来、変更管理とリリース管理の間で明確になっていなかったテストのプロセスを、サービス内容が目的に適ったものであるのかも含めて明確にする品質保証のための活動です。

出典参考：http://www.proseed.co.jp/word/000298.html

（４）目標設定と評価

前述の各管理プロセスが成功したかどうかを客観的に評価する必要があります。その為の指標がKPI(Key Performance Indicators)です。KPIを予め設定することで、そのプロセスが正常に稼働しているか、またその貢献度がわかりやすくなります。これらを視覚的に表現する

ものがダッシュボードです。
以下に特にデータセンターのネットワーク運用における KPI 項目を例として挙げます。

①フロント系管理業務（サービスオペレーション）の主な KPI
［インシデント管理］
・インシデントの解決時間
　　カテゴリ毎のサービスデスクが費やした合計時間
・エスカレートされたインシデントの割合(%)
　　測定期間中にオープンされたインシデント合計に対するエスカレーション率
［要求実現］
・1 次受けで解決出来た問い合わせの割合(%)
　　顧客より受けたインタラクション合計に対するフロントでの解決率
・平均インタラクションクローズ時間
　　インタラクション作成からクローズまでの平均経過時間

②サービス品質維持管理業務（サービスデザイン）の主な KPI
［可用性管理］
・レイテンシー
　・ネットワークレイテンシー(内部)
　自社ネットワーク内部のネットワーク遅延
　・ネットワークレイテンシー(外部)
　主な対外接続先とのネットワーク遅延
　・サービスレイテンシー(内部)
　自社ネットワーク内部の主なサービスプロトコルでのサービス遅延
　・サービスレイテンシー(外部)
　主な対外接続先との主なサービスプロトコルでのサービス遅延
・稼働率
　　MTTR(平均修理時間)と MTBF(平均故障間隔)から算出される稼働率
［キャパシティ管理］
　・ネットワークデバイスの使用率(%)
　ネットワークデバイスの合計数に対する使用率
　・ネットワークやその他サービス利用率(%)
　顧客によって契約された各リソース値と実際に利用されている値の割合
　・ネットワークキャパシティ率(%)
　顧客によって契約された各リソース合計値通りソース合計値の割合
　・ネットワークキャパシティの冗長率と拡張性
　ネットワークキャパシティの冗長率と拡張性

［サービスレベル管理］
・SLA を達成した割合(%)
　　測定期間中のプロセス活動の合計数に対する、SLA を満足したプロセス数
・SLA に対するダウンタイム割合(%)

測定期間中の SLA の合計稼働時間に対する停止回数

③設計構築及び構成管理業務（サービストランジション）の主な KPI

[構成管理]

・ハードウェア資産調達時間

ハードウェア資産を調達するのに必要な平均時間

・ハードウェア資産の平均保有年数

ハードウェア資産の平均使用年数

・ハードウェア資産の予備品率(%)

サービス利用されている資産に対する予備品の数

・ハードウェア資産の在庫品率(%)

測定期間中にサービス利用開始されている資産に対する在庫品の数

・使用中のソフトウェアライセンス割合(%)

ソフトウェアライセンス数と利用率

[変更管理]

・緊急変更の割合(%)

測定期間中の変更作業の合計数に対する緊急変更の数

・計画外変更、個別変更の割合(%)

測定期間中に予期しない変更や通常プロセス以外の変更の数

・ノードのパッチに要する平均時間

ノードのパッチにかかった平均時間

・顧客リソースの移設、収容変更に要する平均時間

顧客リソースの移設、収容変更に要する平均時間

[リリース管理]

・ノードの構成に要する平均時間

ノード構成作業にかかった平均時間

・ノードの増設に要する平均時間

ノードの増設に要する平均時間

・プロビジョニングに要する平均時間

プロビジョニングに要する平均時間

いずれも重要な指標ですが、これらの KPI を指標に定義しつつ、OSS と各管理プロセスとその運用が一体となり、それらのライフサイクルを回し続けることにより顧客へのサービス品質は維持されるとともに、顧客ニーズの変化に合わせたサービス品質の向上が可能となります。

現状、トラフィックの急激な需要増加、スマートフォンによるショートパケットやセッション数の増加、また管理ノード数の急激な増加と既存サービス機器の管理負荷、そして利用者ニーズの多様化による品質へのシビアな要求の増加などネットワーク運用に関する課題は一気に膨らみつつあります。今後更にネットワークが仮想化していった場合においても、この構成管理及び各プロセスが確実に行われていることが重要です。

３－４－６．運用を意識したネットワーク OSS について

OSS（Operation Support System）とは、サービス事業者がサービスを運用管理するための運用支援システムであり、事業者にとってまさに生命線であり、OSS の出来によりサービス運用品質および運用コストが大きく左右されるといっても過言ではありません。

これまで OSS は個々の業務単位に構築されるケースが多く見られましたが、サービスの多様化や求められる品質の変化、クラウドサービスの登場に伴い柔軟性を求められ、尚且つライフサイクル管理やサービス統合化、他のシステムとの相互接続性の担保など、サービス運営全体を網羅的にサポートすることが要求されています。

このような背景から、ITILv3 で定義されたフレームワークを確実にかつ効果的に機能するための業務支援システムとしての OSS のあるべき姿を改めて考えていきます。

(1)OSS のあるべき姿への最初の施策、構成管理の標準化

安定したサービス品質を提供するためにはプロセスやリソースの最適化・共通化が課題となりますが、これは全体を標準化することが近道であり肝要です。データセンター事業の運用管理において、すべてのプロセスは構成情報を参照しており、構成情報を標準化することが、データセンター事業での全てのプロセスの標準化のスタートラインとなります。よって本資料策定にあたり、OSS のあるべき姿に近づくための最初の施策として、「構成管理の標準化」を提言します。

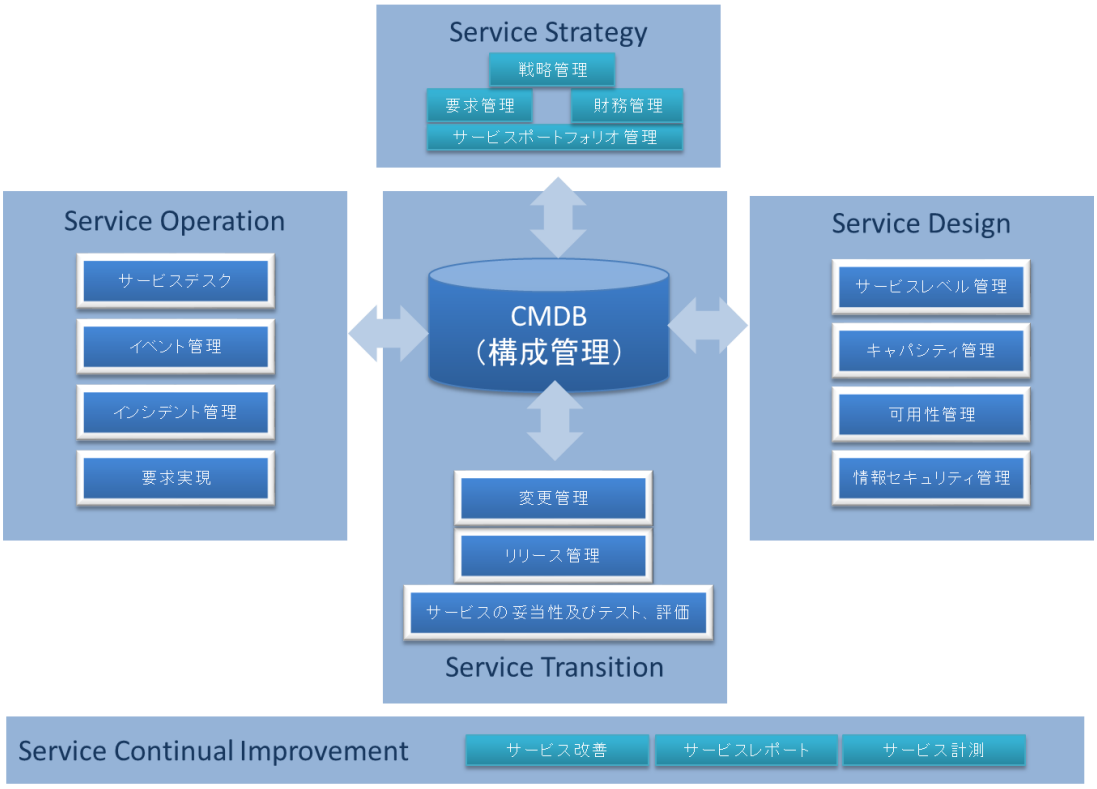


図 3-4e 構成管理情報の標準化

ここでいう標準化とは、それぞれのサービス事業者におけるポリシーを定義するものであり、現状のサービスにおける構成情報をそれぞれ共通項目で洗い出し、管理標準指標を作ることにより、すべてのサービスを網羅的に管理するためのものです。
これにより、新しい技術要素や顧客ニーズを吸収することができ、サービスの進化とともに構成要素も進化させることができます。

構成管理の標準化は以下のような効果が期待できます。

･コスト削減
- 作業効率の向上によるコスト削減が可能です。

･サービス品質向上
- 顧客からのサービス・構成変更要求への柔軟な対応や、迅速な障害切り分けや、サービス影響分析（インパクト分析）など、さまざまな業務における品質向上に貢献します。

･自動化の実現
- 自動化においては、イベント（シナリオ）やアラームをトリガーとして構成管理情報と連携して自動化を実現します。
  自動化の実現は、作業の効率化、オペレーションミス防止につながるとともにクラウドサービスにおいてはオーケストレーションの基本機能となります。

構成管理をすることにより対象の機器が明確になり、バランス、アンバランスの健在化が企業の品質にもコストにも大きな影響を与えることになります。

構成管理を行うに当たり以下の要素が基本となります。

①CMDB (Configuration Management Database)
構成管理データベースであり、各プロセスと密接に結合します。これは資産を管理するものではなく、あくまで各構成アイテム間がどのような相関関係にあるかや、バージョンやステータスなどの構成要件や管理責任者等を明確にします。

②CI (Configuration Item)
CMDB にて管理される各構成アイテムを指します。これらを適切に管理するためには事前にどの範囲でどの程度細かく登録するかを定義しておく必要があります。

③属性
CI を管理するに当たり、個々の CI を特定するものです。名前やバージョン、ステータスなどが含まれます。

これら CI と属性を個々ではなく構成要素としてリアルタイムに管理することにより、各管理プロセスのすべての土台とします。また同時にその効果の出来不出来を左右するものとなります。

(2) 可視化

これら KPI 指標の評価をする際には、全体像を網羅的に把握し、かつそれぞれのプロセスの状況を確認する必要があり、過去からのトレンド、現在の状況、そして今後の予測が見えることが望ましいと言えます。それをグラフィカルに確認するために一目見て傾向が掴めるダッシュボードが重要になります。

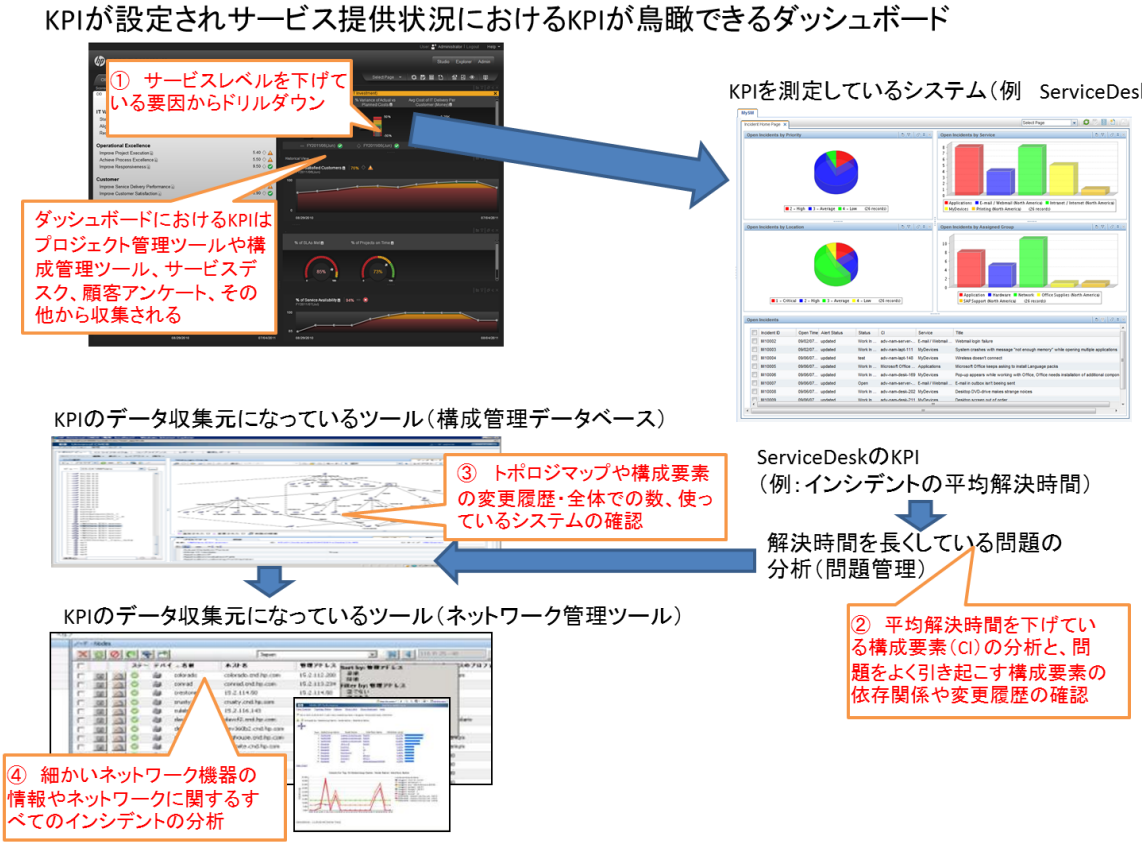


図 3-4f ダッシュボードのイメージ

３－４－７．まとめ

（標準化されたフレームワークとマネジメントシステム運用から人材育成に向けて）

ITILv3 などのフレームワークにおけるプロセスと OSS システムが正確に運用されていることが重要ですが、最も重要なのはそれらのプロセスが定期的に見直しされているか、顧客ニーズやマーケットの変化に追随しているか、新しいサービスを導入する際に各プロセスでの評価が確認されているかなどのマネジメントシステムそのものの運用です。

各プロセスの完成度が高い場合でも、これらを判断し運用するのは人です。これには、管理している人材の目的意識や部門間連携が非常に重要になります。管理することが目的ではなく、様々の情報を見える化し、それにより次のアクションとして何をすべきか判断するプロ

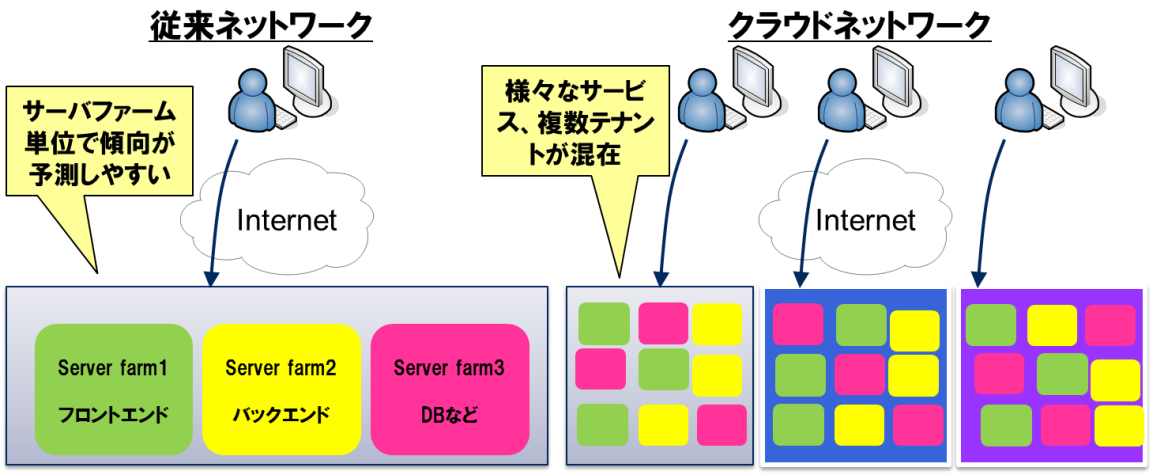
セスを見直すサイクルを繰り返すことにより、サービス運用者を育成しまた相互の信頼関係を築くことが、結果的にサービス運用の品質を向上させ、利用者の満足度、信頼を得ることにつながります。

３－５．トラフィックマネジメント

３－５－１．クラウドにおけるトラフィックマネジメントの考え方

従来のネットワークでは、特定用途で利用するサーバあるいはサーバファーム単位で配置しているケースが多いため、トラフィックの流量や傾向をある程度予測することができました。それに対してクラウドの環境では、仮想サーバ単位でトラフィックが発生し、また、動的に仮想サーバがネットワークを移動することにより、トラフィックの予測が難しい状況となってきていると言えます。

	従来ネットワーク	クラウドネットワーク
ノード（用途）	1物理サーバ サーバファーム単位	仮想サーバ 様々な用途が混在
配置	ほぼ固定	流動的
トラフィック傾向	予測しやすい シングルテナント	予測しにくい マルチテナント



以上より、クラウドでのトラフィックマネジメントを行う上で重要な点としては下記が挙げられます。

1. 仮想サーバ単位の（大よそな）想定トラフィックの把握
2. ボトルネックポイントにおけるトラフィック上昇の早めの検知（増速対応の判断）
3. 早めかつ適切な増速対応

以上について、以降の章にて詳しく述べていきます。

３－５－２．トラフィック増が想定されるボトルネックポイント

トラフィックマネジメントを行うためには、トラフィックが溢れてしまい、サービスに影響が出てしまうボトルネックポイントを把握することが重要となります。一般的なクラウドネットワークではトラフィック増に対して、下記のボトルネックポイントと対策が考えられます。

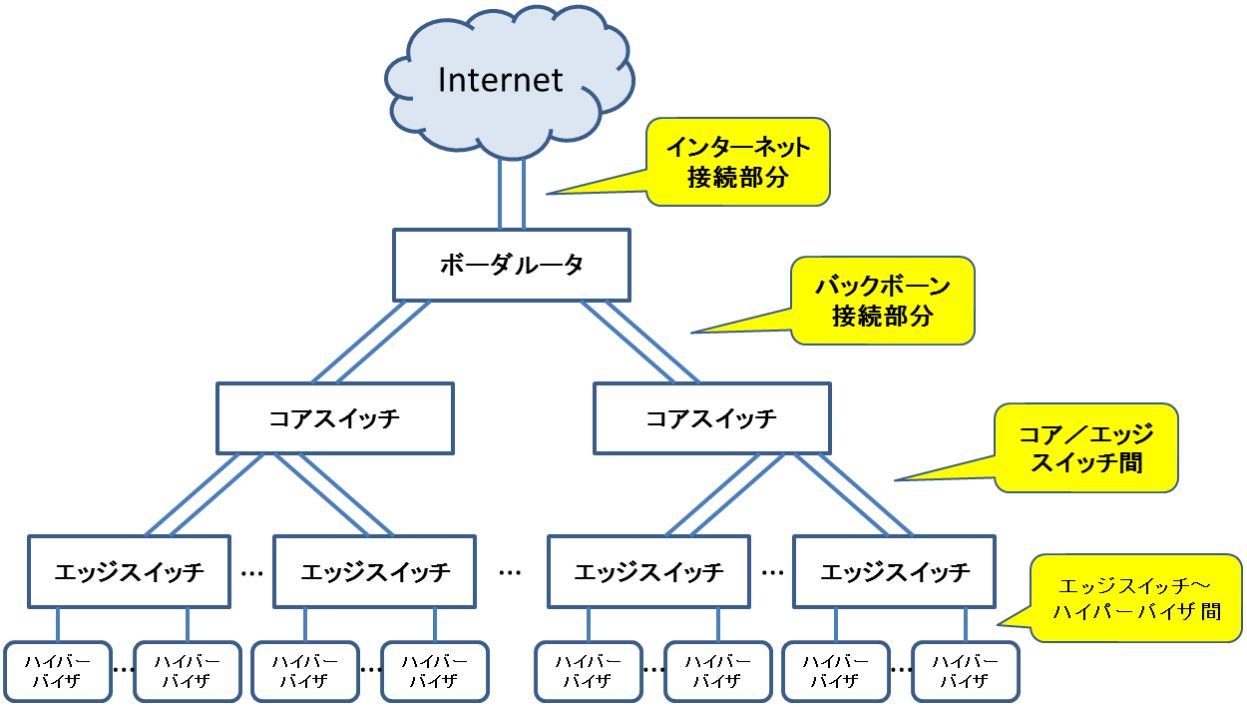


図 3-5a　主なボトルネックポイント

- インターネット接続部分
  - 余裕を持ったネットワーク設計
  - 経路調整（トランジット、ピアリング調整など）
- バックボーンとの接続部分
  - 閾値設定
  - 増速対応
- コアスイッチとエッジスイッチ間
  - 閾値設定
  - 増速対応
- エッジスイッチとハイパーバイザ間
  - 利用者自身によるトラフィックコントロール
  - クラウド提供者側でのトラフィックコントロール

クラウドネットワークにおける特徴としては、インターネットとの間のトラフィックよりもデータセンター内のトラフィックの比率が増える傾向にあります。理由としては、同一データセンター内あるいはクラウド内において CSP（Contents Service Provider）間でデ

ータ転送を行う場合や、マイグレーションやバックアップ目的によるトラフィックが増大する可能性といったことが挙げられます。従って、特にバックボーン接続部分やコア／エッジスイッチ間の接続を増速することが推奨されます。

３－５－３．トラフィック増に対する具体的な対応方法

トラフィック増への対応については、単純に決まった方法により解決できるものではなく、下記のような方法により、臨機応変にケースバイケースで対応する必要があると考えます。

(1) 力技

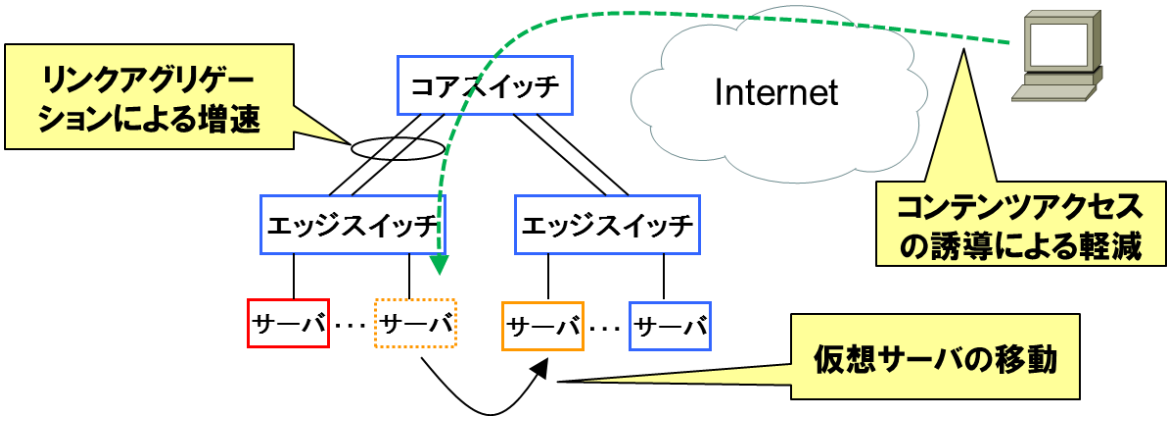
実際にトラフィックが帯域の限界まで近づき、トラフィックが溢れるといったケースが発生した場合、どうしても人手の運用による対応が必要となります。具体的には下記のような作業が挙げられます。

①物理的な増速

例えば、コアスイッチとエッジスイッチ間のポートを増やし、リンクアグリゲーションを行うことで帯域を増やします。

②トラフィックの誘導

トラフィックの元となるコンテンツの掲載を外したり、不要な通信を減らすことで、トラフィックを減らします。他には利用者と交渉し、仮想サーバの移動などの対策が考えられます。



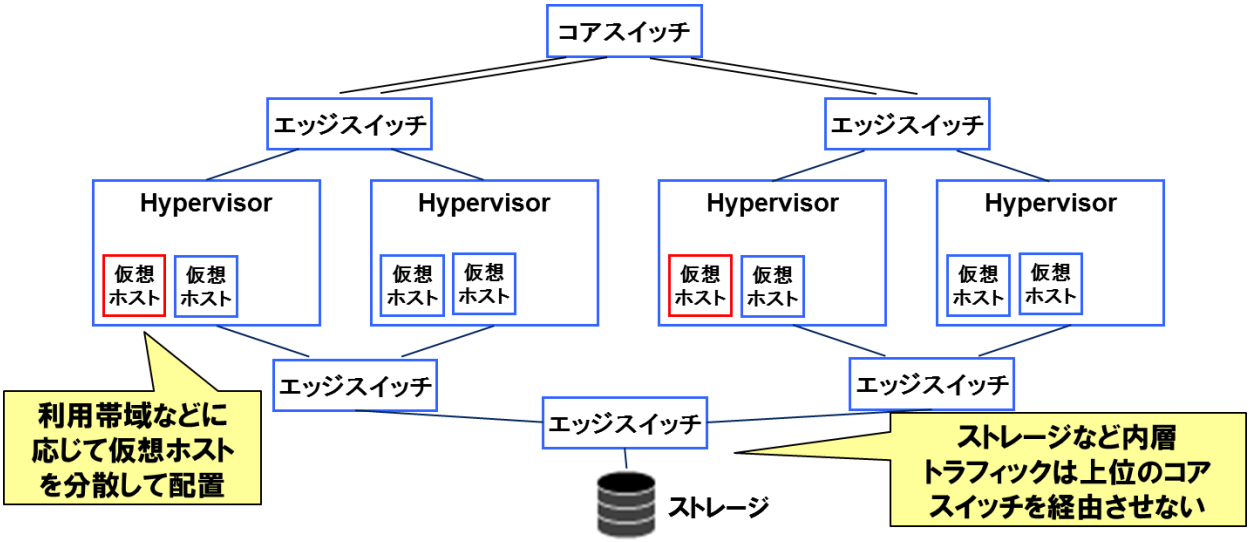
(2) キャパシティ管理

ここで取り上げるキャパシティ管理とは、必要な帯域を定常的に把握し、予め予測されるトラフィックを適切なネットワークに割り振ることです。そのためには下記のような対策が必要です。

- 利用帯域の事前申告による分散配置

各仮想サーバの利用帯域を予め把握することで、ハイパーバイザやコア/エッジスイッチ配下の配置を変え、トラフィックを分散する方法。

- 内層トラフィックに関する適切な配置
  内層トラフィックとはクラウド内のサーバあるいはストレージ間で通信が行われるトラフィックでインターネットなど外部へは流れないトラフィックのことです。そのようなトラフィックは可能な限り、低いレイヤー（エッジスイッチあるいはコアスイッチ配下）で行われるように仮想サーバを配置すべきです。なぜならば上位のレイヤーにそのトラフィックが流れれば流れる程、より多くのボトルネック部分を経由することになり、より多くの増速箇所を増やさなければいけなくなるため、非効率となります。典型的な例として、ストレージをマウントするケースには特にその点を考慮する必要があると言えます。



(3)増速ポリシー

キャパシティ管理を行っていても、サービスを継続するに従って、トラフィックが純増する場合があります。そのような場合に備え、日頃より MRTG などでトラフィックの監視を行い、閾値を設定し、帯域の 50%以上で原因追究、70%以上で増速対応など、ポリシーを事前に設定し、余裕を持ったポリシーにより増速対応を行うことも重要であると言えます。

(4)分散

キャパシティ管理に近いですが、同一サービスをトラフィック・BCP の観点により異なる拠点に配置し、GSLB で分散させる方法もよく使われる手法です。

(5)傾向性の把握

インターネット側に近いポートでは、トラフィックの傾向性が非常に顕著に出ます。静的なしきい値での管理も重要ですが、トラフィックの通常の傾向を把握し、そこから大きく変動があった場合には、正常にサービスが提供されていないといった、システム上で何らかの問題が発生しているケースも考えられます。トラフィックマネジメントは

キャパシティ管理だけでなく、障害の予兆やサイレント障害といった、トラブルを把握するといった活用方法もあります。

３－５－４．トラフィック増の想定シナリオ

トラフィック増となる原因は様々ですが、コンテンツプロバイダーの視点では下記のようなシナリオが想定されます。

・　新サービス・コンテンツのリリース

新しいサービスやコンテンツがリリースされると突発的な新しいトラフィックが生まれる可能性が高いです。主に初期構築時の設計（キャパシティ管理）でのトラフィックの見積もりが肝要となります。

・　キャンペーン（広告からのリード）

キャンペーンや広告などにより、利用者が誘導されるケースもよくあると言えます。

この場合は一時的なトラフィックの伸びが想定されるため、比較的空いているネットワークにおいて一時的な仮想サーバの増強を行うなどの対策が有効であると言えます。

・　震災（公共コンテンツなど）

震災発生時には予測しえないトラフィックが発生する可能性が高く。事前のキャパシティ管理では対応できない可能性が高いと言えます。このような場合は主に力技での対応と事前に震災を想定した BCP を考えることが必要です。また、サービスのプライオリティによっては震災時のサービス提供を諦める（ごめんなさいページを出す）という方法も１つの手段として考えられます。

３－５－５．その他の考慮点

⑴セッション数に関して

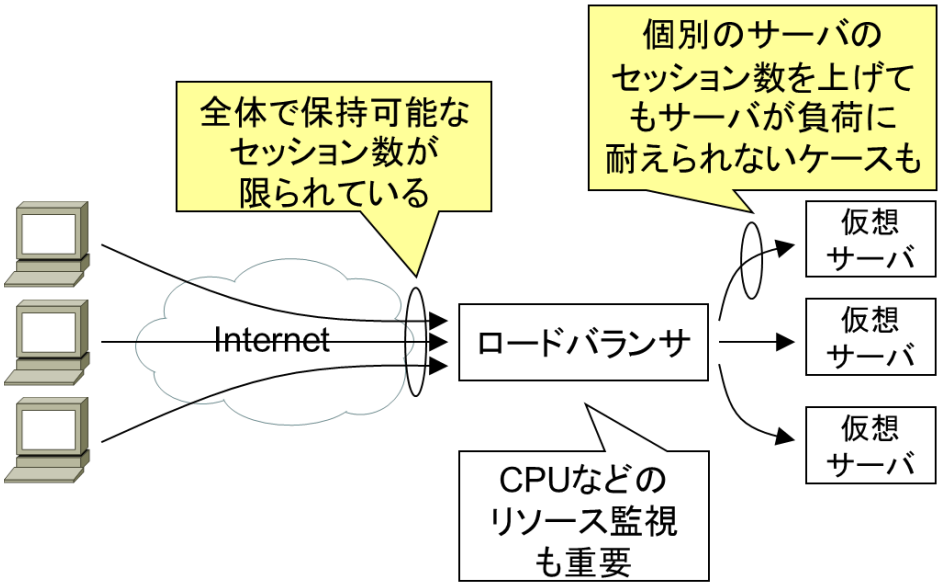
ネットワークにおいては、物理的な帯域の制限だけでなく、例えば、ファイアウォールやロードバランサにおいては、セッション数のリソースについても考慮する必要があります。

機器の設定等で IP 単位での最大コネクション数を調整することが可能となりますが、例えば、あるサービスにおいて、サービスの不具合により異常なセッション数を張りっぱなしの状態になった場合に他のサービスにおいて新たなセッションが張れなくなるといった場合が想定されるため、むやみに IP 単位での最大セッション数を上げることは推奨されません。

よって、初期構築時にも導入する機器の最大セッション数なども考慮の上、機器選定を行うことも重要だと言えます。

また、アプライアンスや使用するサービスによっては最大セッション数に到達する前に、CPU といった他のリソースの限界に到達するケースもあります。ファイアウォールやロードバランサでは、セッション数と CPU で相関関係が見受けられるケースがあります。 各リソースを把握し、セッション数の上昇で CPU がどのように上昇するか、CPU の使用率から

本アプライアンスやサービスでのセッション上限値が予想出来る事もあります。キャパシティ管理をおこなう上でも、各アプライアンスのトータル的なリソース管理が重要なポイントとなります。



(2)ハイパーバイザの物理ポートの制限について

ハイパーバイザによって利用できる物理ポート（NIC）数の制限がある場合があります。
【例】
・バージョンによって利用できる NIC 数が異なる
⇒ESXi4 と ESXi5 など
・速度の異なる NIC との混在により利用できるポート数が減る
⇒10G と 1G の組み合わせにより本来同じ速度で利用可能な最大ポート数よりも減ってしまうなど
・異なるベンダー同志の NIC の混在は推奨されない
など。
※参考：http://kb.vmware.com/kb/1020808

(3)エッジスイッチのトラフィック監視について

従来は物理ポート単位のトラフィックを MRTG などで監視していたが、今後のクラウド化促進により、VM 単位のトラフィック監視が必要となる可能性も考えられます。
ただし、エッジスイッチの Uplink の 10G 化に伴い、そこまで厳密な（VM 単位の）トラフィック監視が不要な場合もあります。（ハイパーバイザ側の利用帯域にもよる）
従って、VM 単位のトラフィック監視が必要となるのはケースバイケースと言えますが、今後のクラウドネットワークにおいては、エッジスイッチの 10G 化が望ましいと言えます。

４．分散データセンター（データセンター間ネットワーク）の技術動向

事業継続、災害対策、バックアップ等の目的や、データセンターの物理的な制約に囚われない拡張性の確保の為、異なるデータセンター間に跨るシステム確立の需要が高まってきています。このため、サーバ仮想化環境やストレージデータを、異なるデータセンター間にシームレスに拡張し、柔軟性の高い高付加価値なシステム・サービスの実現が求められており、これには、データセンター間ネットワークの機能、設計が非常に重要となります。
本章では、データセンターの外部接続回線の選択枝や一般的な課題・検討事項を整理し、需要の高まりを見せるデータセンター間のフラットL2ネットワークと、データレプリケーションの実現に当たって留意すべき点を、技術動向を中心に紹介します。

４－１．データセンターにおける外部接続回線

４－１－１．外部接続回線の種別

データセンターにおける外部接続回線としては次のパターンが考えられます。

表 4-1a

パターン	用途	接続先	回線種別
DC間接続　もしくは クラウド間接続	システム連携	DC および 特定ラック間	閉域網
外部サイト参照	システム連携	DC	インターネット
インターネット接続	システム参照	インターネット	インターネット

*)DC = Data Center

一般に閉域網は VPN (Virtual Private Network:仮想閉域網)と呼ばれます。事業者としてのデータセンター間やシステム間の接続は、それらの多くが高い品質を要求されるため、通信帯域や遅延、揺らぎなどの品質保証が必要となります。従い、厳密には品質を保証しかねるインターネットを利用した閉域はここでは望ましくないといえます。

４－１－２．外部接続において考慮すべき点

データセンターにおいて外部接続を実施する際には、下記観点での技術について考慮しておく必要があります。考慮漏れがあると、そもそも接続できない場合や、予定のサービスレベルに達しない、情報漏えいの発生、などが危惧されます。
外部接続を行うための回線種別には、ダークファイバー、閉域網（L3系、L2系）、インターネット、といった種類があり、それぞれには次のような特徴があります。

① ダークファイバー
通信キャリアよりダークファイバーその物を借り受けるサービスです。ダークファイバーをどのように用いるかは自由となります。ダークファイバーと WDM 等の伝送装置を組み合わせ

ることで、通常の回線サービスでは実現出来ないような広帯域・大容量通信を実現することが可能です。ただしダークファイバーの利用には、次の考慮が必要です。

- 入手困難性：そもそも利用データセンターにてダークファイバー（加入者光ファイバー）が敷設されていない場合があります。敷設されていない場合はキャリアとの交渉が必要です。長距離伝送の場合は中継光ファイバーを利用し、リピータをキャリアコロケーションラックに設置する必要があります。キャリア通信設備との接続のための事前調査申し込みは、電気通信事業者であることが前提となっています。また、物理工事を伴うため、ケーブル敷設経路や各種既存設備利用などの調整が必要となります。
- 運用上の課題：利用においては、事業者間確認事項として物理責任分解を定め障害時の対応方法をあらかじめ確認しておく必要があります。また、ダークファイバーはケーブル貸しであり、その品質や可用性は特に規定されず、保守に関する確認事項の範疇での対応となります。
- 利用料の特徴：敷設距離と利用芯線数に比例し、定額料金で提供されています。

② 閉域網

回線提供において、利用者の申込ごとに区別される、セキュリティグループに応じて提供される回線のことです。似て異なるものに、インターネット-VPN、L3 系閉域サービス（IP-VPN）、L2 系閉域サービス（広域イーササービス）、専用線などがあります。閉域網の場合には閉域番号が与えられ、その番号同士の回線であれば相互に通信が可能となる、という特徴があります。利用者独自の網を構成することができ、個別の要件（例えば、音声とデータの併用時の音声優先など）に応じた品質、特性、コストを選択することもできます。

- L2 系の特徴：IP ベースに制限されることなく外部と通信させることが可能です。CPE（Customer Premises Edge:加入者宅内装置）となる LAN/WAN の境界装置を設置する際、利用者の要件に応じた L3 以上の機能を、独自に構成できます。必要がなければ L2 のまま利用することもできます。L2 であるために Vlan(Customer Tag)を指定しますが、第２タグ(Carrier Tag)を付与(拡張タグ VLAN 利用)させることにより Vlan 重畳させ、複数閉域回線を１本の物理線に乗せることもできます。
- L3 系の特徴：多くの場合、IP ベースの通信に限定して提供されます。CPE 設置の際、キャリアの提供条件に応じた装置であれば利用可能です。また、特定の通信先をＩＰでフィルタしたり、マルチキャストを利用するオプションも存在します。
- 利用料の特徴：ダークファイバーやインターネットに比べ閉域網での回線利用は、キャリアにより品質保証されていますが、導入に当たってはコストとのトレードオフとなります。また、土日夜間などの高トラフィック時だけ帯域上限を拡大させることが可能な時間帯割引などを実験的に提供したり、クラウドサービスと回線をセットで販売しているキャリアもあります。

③ インターネット回線

世界規模に広がっているネットワークの集合体「The Internet」に接続するための回線で、この回線を用いて世界中の公開ネットワークへ接続することができます。

- インターネット回線の特徴：世界中の誰とでも通信可能ではありますが、逆に特定の通信だけを許すためには、ファイアウォールや認証システムによる通信制御、サイバーアタックから身を守る IPS(Intrusion Prevention System：侵入防止システ

ム)/IDS(Intrusion Detection System：侵入検知システム)などによる通信監視・制御が必要になる場合があります。また通信相手の構成、設定はアンコントローラブルであり、優先制御や特殊プロトコルなどのやり取りには注意が必要です。

- 提供構造：回線提供者特有の網構成にて提供されます。アクセス回線は個別の要件に応じたものを選べますが、キャリア内の網構成自体を指定することはできません。閉域であってもインターネットであっても、別途料金にて CPE となる装置をキャリア側から提供を受けることも可能です。
- 利用料の特徴：各々有用なオプションサービスも用意されていますので、必要に応じて、また用途、機能、性能、運用の各要件に応じて選択できます。例えば、料金オプションには、トラフィック上限まで定額制となるものや、バースト部分に対して従量課金となるものがあります。また、セキュリティオプションには、インターネット回線内部で IPS/IDS を実施することにより、最終足回り回線が細いことに起因する洪水攻撃を、上流の網内で食い止めることができるものもあります。

以下回線種別ごとに、考慮すべきポイントについて整理・記述します。

表 4-1b

回線種別	L1	L2	L3	L4 以上
ダークファイバー	(1)伝送損失 (2)波長			
閉域網		(3) 閉域番号指定 (4) STP 等	IP アドレス (5) QoS (6) マルチキャスト	
インターネット			アドレス変換 (7) BGP	
共通項目	(8)冗長性 拡張性	リンクパススルー フレームサイズ (9)オートネゴシエーション フレームサイズ	ルーティング	負荷分散 (10)通信セキュリティ維持

(1)伝送損失

ダークファイバーを利用する際には、ファイバー上で発生する伝送損失について考慮する必要があります。ネットワーク機器の光インタフェースには、光ファイバー上で許容される伝送損失に関する仕様が存在し、許容範囲を上回る伝送損失が発生すると正常に通信が出来ない状態となります。伝送損失は通常距離に応じて高くなり、計算方法の目安も存在しますが、ファイバーの特性や中継で用いるパッチの特性や数によっても異なる為、利用の検討に当たってはダークファイバーの提供元への確認が必須となります。

(2)波長

ダークファイバーの重要な仕様の一つとして、伝送可能な波長というものがあります。WDM(Wavelength Division Multiplexing：波長分割多重)等では、様々な波長を利用して大容量の伝送を実現する為、ダークファイバー側で利用可能な波長と、ネットワーク機器側で利用する波長の双方について確認が必要となります。

(3) 閉域番号指定

Vlan 重畳では、一つの物理回線に、複数の閉域を同時に収容させることができます。例えば、顧客 A と顧客 B を 1 本の物理回線で収容し、論理的には相互に接続させないようにすることができます。この技術によって顧客ごとに回線開通をせずに済むことが可能となります。技術的には拡張タグ VLAN を利用するために、それを利用可能な CPE の設置が必要となります。

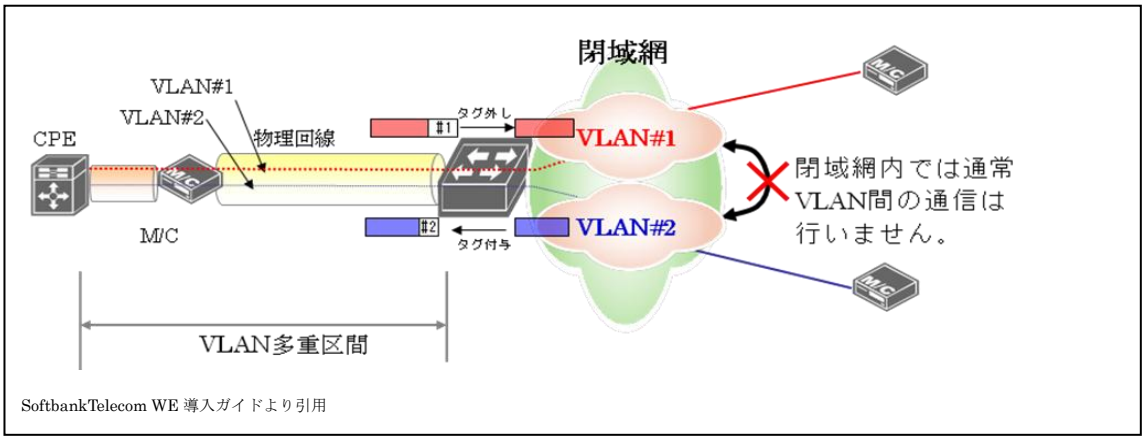


図 4-1a 閉域番号指定

(4) STP(Spanning Tree Protocol)など

L2 系閉域網を利用する場合、CPE となる装置は L3 系装置（L3SW やルータなど）の使用が推奨されています。L2 系閉域網では STP などのブリッジング系プロトコルは利用できないことが多く、CPE 間での冗長技術としては利用できない可能性があるためです。

経路負荷分散や経路冗長などは、L3 レイヤ以上の技術を用いて構築することが常套手段となっています。

(5) QoS (Quality of Service)

閉域網の場合に適応できる技術で、優先制御と帯域制御の２種類があります。予定帯域より多くの通信が発生した場合に通信が混雑しますが、これを輻輳と言い、通信遅延・揺らぎ・パケットロスが発生します。輻輳を避けるために QoS の設定により優先度を設けることができます。

例えば、文字データと音声データが同時に流れてこれが輻輳した場合、データは少し遅延があっても多少は許容できることが多いですが、音声は聞き取りにくくなります。

通常のキャリア回線では QoS を無視することが多いですが、QoS を理解して優先的に通信させるオプションがあります。

ただし、インターネットではいろいろなキャリアをまたぐため、ほとんどの場合こういった個別制御は行えません。

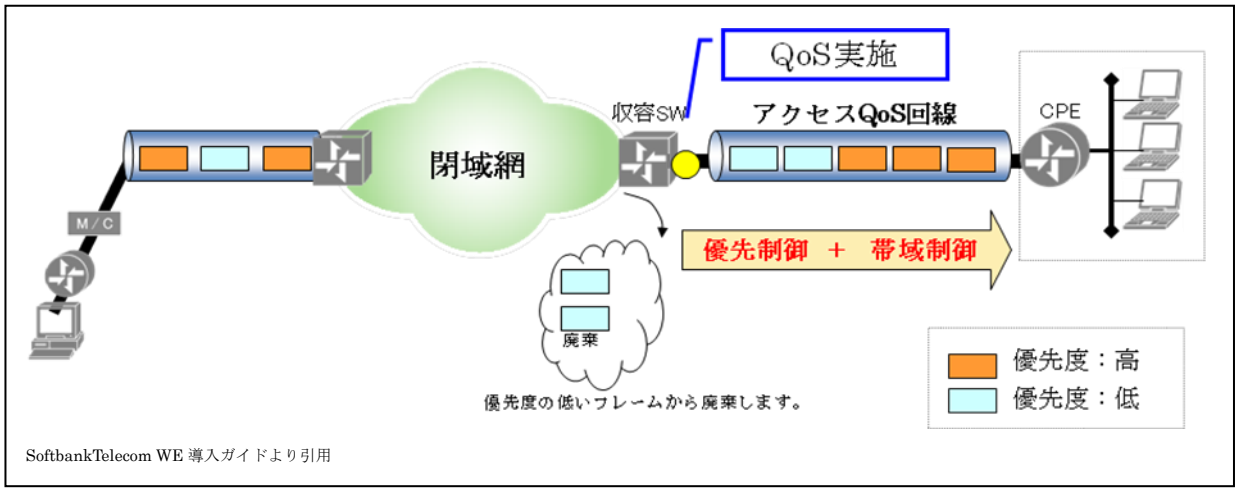


図 4-1b　Qos

(6) IPv4 における「マルチキャスト」の利用（Multicast）

マルチキャストは映像などの大量データを放送する際に、トラフィックを軽減できる技術ではありますが、主に閉域網内で利用できるものです。ただし、閉域網内でもマルチキャスト、ブロードキャストの最大トラフィック量に上限を設けている場合もあり、事前に確認する必要があります。

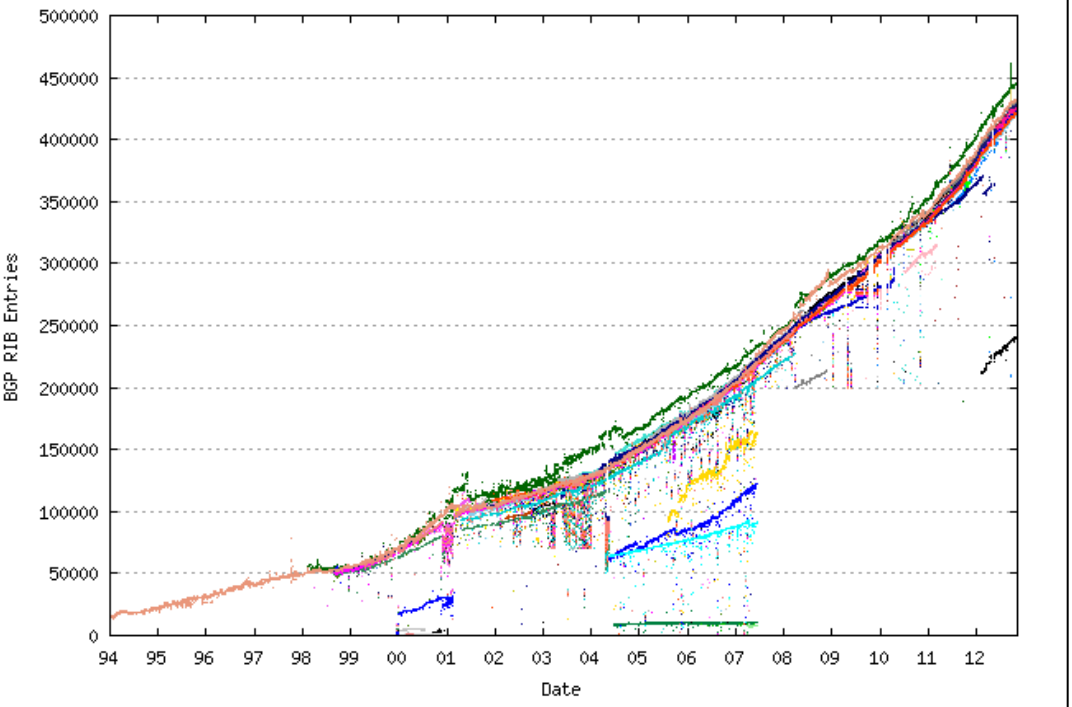
閉域網を利用した、データセンター間接続などでは、個別に利用できますが、経路上のすべての装置に対してマルチキャストについて考慮する必要があります。

インターネットにおいては、経由するプロバイダがマルチキャストをサポートしているかどうかによりますので、一般には使用できないと考えた方が賢明です。ただし、アプリケーションによってはマルチキャストトンネルを構成して提供しているものもあります。

(7) BGP(Border Gateway Protocol)ルーティング

一般に、DC においてインターネットを利用するのであれば、BGP AS(autonomous system：自律システム)番号を取得する必要はありません。ほとんどの場合はフルルートを受ける必要はなく、スタティックルートで十分な実装が可能です。注意点としては以下の事柄があります。

- 近年、IPv4 の IP アドレス枯渇により、ISP(Internet Service Provider：インターネット接続事業者)の事業を始めることで IP アドレスを取得できると誤解している人が多いようです。そのようなことはなく、単に AS の乱立による経路増加、プロバイダの負荷高騰につながっています。
- BGP を理解して構築、運用できるエンジニアが不足しています。きちんとした NW 基礎技術習得をキャリアパスの一つとし、技術者を育てていく必要があります。
- 実際にフルルートを受ける構成をとる場合、性能要件・運用要件をしっかり検討することが必要です。2012 年現在流通している IPv4 でのルート数は４５万程度と言われています。



BGP Full Route 数　http://bgp.potaroo.net/ より引用

図 4-1c BGP Full Route

BGP を用いて冗長化の検討を行う場合、マルチホーミング、マルチリンクを検討することになります。

冗長技術	特徴	
マルチリンク	同一 ISP への物理冗長回線	物理リンク断に対する冗長対策です
マルチホーミング	異なる ISP（異なる AS)への接続	対インターネットの冗長経路として使えますが、AS の経路が異なることを理解して使用する必要があります。

表 4-1c BGP を用いた冗長化手法と特徴

(8) 冗長化検討

サービス維持のためには、いろいろな個所での冗長について検討が必要です。ただし、冗長にはコストがかかり、本当に必要であるかは吟味しておくべきです。

冗長技術	考慮点
BGP による経路冗長	１つの ISP への接続において、異経路での接続を行い、経路上の障害を回避する
装置冗長	装置を二重化し、筐体障害を回避する
回線冗長	回線周りの物理障害に対する対策
キャリア冗長	回線冗長に加え、キャリア側装置（網）障害に対する対策
ISP 冗長	ISP 利用不可となってもサービス提供を継続する また、選択した ISP の AS によっては、途中経路の帯域が太い細いという差が出る場合がある。ISP がどの IX(Internet Exchange point:インターネット相互接続ポイント)とピアリングしているかも検討する必要がある。
電源冗長	電源障害、電力不足があってもサービス継続 を行う
製造業者冗長	特定製造業者のバグ等に左右されないよう、別業者装置で冗長を組む
ルーティング冗長	ルーティング経路を L3 レベルで冗長
L2 系冗長	古くは STP (Spanning Tree Protocol) 、最近ではクラスタやスタックといった STP フリーな構成を検討する。

表 4-1d 冗長技術と考慮点

(9) オートネゴシエーション

オートネゴシエーションを利用すると、接続する機器間でのモードを自動調整するのですが、時には自動調整がうまくいかないために、全二重のはずが半二重のモードとなり通信不良が発生する場合があります。いろいろな原因がありますが、指定されたモードで固定設定する、ネゴシエーション完了後に何のモードで動作しているかを確認したほうが無難です。

(10) 通信セキュリティ維持

通信におけるセキュリティ維持は、大きくはサービス維持、情報漏えい防止のために、アクセス管理、ログ取得などを行うことで実装されますが、目的、効果を考えて実装する必要があります。

・性能面

目的に応じた性能値の考慮が必要となります。

・機能面

アクセスログ取得、通信状態検査の必要性があるならば、FW マシンの導入が必要となりますが、必要ないならば、ルータ等のアクセス制御機能による実装も検討のうちです。

・運用面

IPS/IDS などの機能は、事象発生から対策実施までが短時間であることが多く、どのように運用すべきかを予め考えておく必要があります。

・拡張性

セキュリティ維持機能にはセッション維持が必要な場合があり、スケールアウトがし辛いものとなります。設計時点で拡張のさせ方を考慮しておくことが肝要です。

４－２．データセンター間 L2 ネットワーク

昨今、データセンター間においてフラットな L2 ネットワークを構築したいという要件が強くなっています。フラットな L2 ネットワークは幾つかの用途がありますが、現状最も多いのがデータセンター間でのサーバ仮想化対応が挙げられます。

サーバの仮想化は、データセンター内においてサーバの収容効率を上げるために広く用いられておりますが、サーバ集約以外のメリットとして仮想マシンのモビリティとスケーラビリティがあげられます。

サーバを仮想化することで、仮想サーバは物理サーバに固定させる必要が無くなる為、仮想マシンは物理サーバ間を自由に移動することが可能となり、ロケーションフリーなサーバ環境をもたらします。また運用管理者は、急なメンテナンス作業や、一時的なシステム高負荷に対応する必要がある場合でも、ライブマイグレーション等の機能を用いることで、システム全体を停止させることなく、最低限のダウンタイムで対策を行うことが可能です。

また、大量の仮想マシンを短時間で展開したり、削除したりといった構成変更も容易になる為、全体の処理能力を柔軟に拡張・縮小することも可能となります。

しかしながら、仮想サーバが自由に移動出来るということは、仮想サーバがどこにあっても同一のネットワーク機能、ポリシーを適用出来るようにする必要があるとも言えます。また、ライブマイグレーション等の仮想サーバの移動を行う為には、移動元のサーバと移動先のサーバは、同一の L2 ネットワーク上に存在する必要があります。

これまで、これらの機能は主にデータセンター内でのみ利用されてきましたが、データセンターを跨った拡張性の確保、事業継続、災害対策の観点からの需要の高まりにより、データセンター間でもサーバ仮想化の機能を利用したいという要求が高まっています。

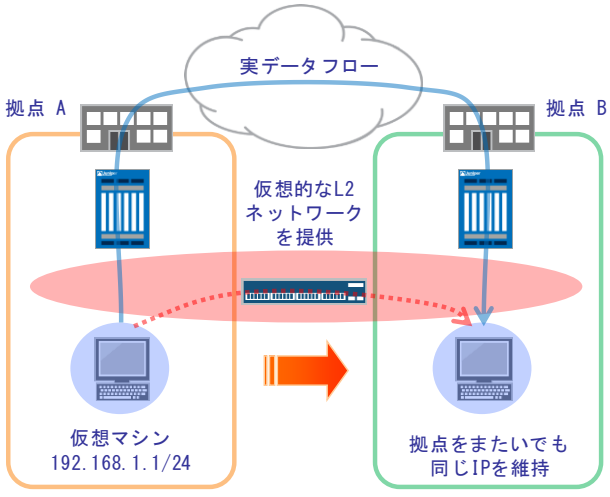


図 4-2a データセンター間に求められる L2 ネットワークイメージ

しかしながら、同一の L2 ネットワークである必要があるという要件は、データセンター内であればそれ程難しくありませんが、データセンター間で実現する為には様々な課題をクリアする必要があります。本項ではこれらの課題点と、それを解決するソリューションについて説明しま

す。

４－２－１．検討にあたり考慮すべき点

データセンター間でフラットなL2ネットワークを構築する為に考慮すべき点を、以下に挙げます。

(1)L2フラットなネットワークを構成する区間

フラットなL2ネットワークを構築する上で、まず考慮しなければならないのが、どの区間をL2ネットワーク化するかです。これは事業者のサービス区分、POI(Point of Interface)によって異なりますが、それぞれ利用可能なソリューションや設計が異なります。

・ネットワーク - ネットワーク間をL2化する場合

事業者がデータセンターとデータセンターをつなぐネットワーク、或いはラックよりも上位のネットワークのみを提供している場合に該当します。データセンター内のネットワークについては、利用企業、またはSIer(System Integrator)が独自に構築しており、その上位ネットワーク区間についてL2ネットワークを提供する場合となります。

・サーバサーバ間をL2化する場合

事業者がコンテンツサービス、クラウド等の基盤自体を保有している場合に該当します。データセンター内のネットワークからサーバまで、全てのネットワークを事業者側で構築・運用している場合となります。

(2)マルチテナント

代表的なマルチテナントの実現方法として VLAN が挙げられます。各利用者に対して一意のVLAN IDを割り与えることで利用者間のトラフィックを分離し、マルチテナント性を確保します。しかしながら、VLANはその仕様上約4,000のVLAN IDしか利用することが出来ません。

・必要なマルチテナント数が4,000より少ない場合

将来的な拡張を見越しても、収容テナント数が、4,000より少ない場合は、VLANのみでもある程度のマルチテナント性を確保可能となります。

・必要なマルチテナント数が4,000より多い場合

VLANのみのマルチテナントでは収容出来ない為、VLAN数を拡張させる等の他の方法を用いる必要があります。

(3)L2パスの冗長化

データセンター間でフラットなL2ネットワークを構築した場合、利用する手法や構成次第でL2ループが発生する可能性があります。

・Point to Point でデータセンター間のネットワークを冗長化しない場合

　データセンターの回線が単一障害点となりますが、L2 ループが発生しない為ループ対策は不要です。

・3 拠点以上の構成、Point to Point でデータセンター間ネットワークを冗長化する場合

　L2 ループが発生する可能性がある為、手法、設計について検討する必要があります。

(4)MAC テーブルの制限

　データセンター間に跨る大きな L2 ネットワークを構築した場合、ブロードキャストドメインについてもデータセンター間に広がる形となります。そのため 1 つのブロードキャストドメインが保持する MAC 数も大きくなり、複数のブロードキャストドメインを収容した場合大量の MAC を保持出来るネットワークが必要となります。

・全体の MAC 数が数万レベルの場合

　従来のスイッチで MAC アドレス数が大きめの製品を利用すれば、特別な考慮は必要ありません。

・全体の MAC 数が数十万レベルの場合

　従来のスイッチでも、十万程度の MAC 数を保持できる製品もありますが、それ以上の MAC を収容する必要がある場合には、収容可能な MAC アドレス数を拡張する為の手法を検討する必要があります。

(5)ブロードキャストコントロール

　データセンター間ネットワークでループ対策を実施している場合でも、利用者側ネットワークの障害、またはオペレーションミスにより、大量のブロードキャストやマルチキャストがデータセンター間ネットワークに流れ込んでしまう場合があります。その場合、他の利用者向けのサービスに影響を及ぼしてしまう可能性もある為、対策の検討が必要です。具体的な対応策としては、スイッチに実装されているブロードキャスト、マルチキャストコントロール機能があげられます。スイッチの実装によって動作や設定可能なパラメータは異なりますが、概ね以下のような動作が可能です。

・フレーム破棄

　一定の通信量を超えたブロードキャスト、マルチキャストフレームを破棄します。

・ポートのシャットダウン

　ブロードキャスト、マルチキャストフレームが一定の通信量を超えた場合、その物理ポートをシャットダウン(利用不可)状態にします。再度ブロードキャスト、マルチキャストが一定の通信量以下に戻った場合に、自動的にポートを復旧させる機能を持った製品もあります。

何れの機能についても、ブロードキャスト、マルチキャストのそれぞれで設定が可能な製品が一般的ですが、動画トラフィック等大量のマルチキャスト通信を行うアプリケーションもありますので、マルチキャストのリミット設定に関しては注意が必要です。

４－２－２．データセンター間 L2 ネットワークを実現する技術

前述の検討事項を踏まえ、データセンター間で L2 を実現するためのソリューションを紹介します。

(1)WDM(Wavelength Division Multiplexing) /TDM(Time Division Multiplexing)

主に長距離のデータ転送を行う際に使用されるソリューションであり、一般に伝送装置等と呼ばれています。

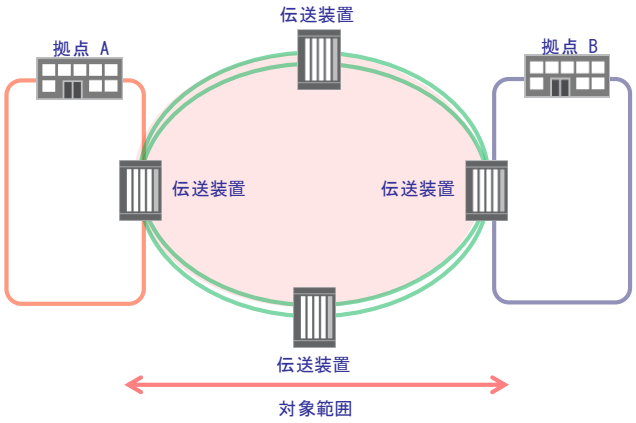


図 4-2b WDM/TDM の対象範囲

伝送装置では、Ethernet よりも下位のレイヤにてデータ伝送を行う為、一般的に VLAN や MAC アドレスの拡張性による制約を受けることが有りません。
データの伝送方式には、WDM や TDM 等があり、それぞれ以下の特長があります。

①WDM 方式

Wavelength Division Multiplexing（波長分割多重）と呼ばれ、複数の利用者データを、それぞれの独立した光波長に分け、1 つの光ファイバー上に多重化する方式です。
8 波長程度を中距離伝送可能な CWDM(Coarse Wavelength Division Multiplexing)方式と、10 波以上の多くの波長を長距離伝送することが可能な DWDM(Dense Wavelength Division Multiplexing)方式があります。

現状 1 波長当たり 100G の伝送が可能な製品もあり、数十の波長を多重することで 1 本の光ファイバー上に非常に大容量のデータを伝送することが可能です。ただし、経路の制御は基本的には波長単位となり、波長内のトラフィックを細かく制御することは出来ません。
DWDM はメトロネットワーク以上の大規模・大容量なコアネットワークに適しており、CWDM はメトロネットワークに適したソリューションとなります。

また、DWDM では製品や光ファイバーの特性によって利用可能な波長帯が異なる為、導入前には仕様の確認が必要となります。

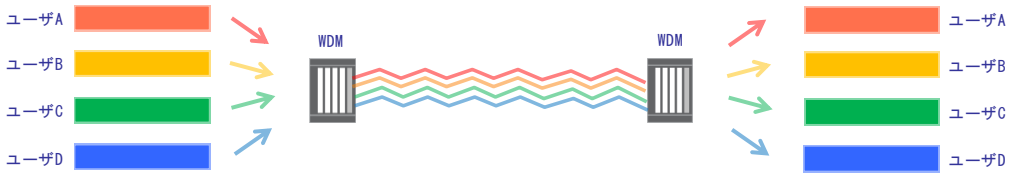


図 4-2c WDM のデータ伝送イメージ図

②TDM 方式

Time Division Multiplexing（時分割多重）と呼ばれ、複数の利用者データをタイムスロット毎に分け、1 つの光ファイバー上に多重化する方式です。

主な技術仕様としては、ANSI（American National Standards Institute）で標準化された SONET（Synchronous Optical Network）と、ITU-TS（International Telecommunication Union Telecommunication Standardization sector）で標準化された SDH（Synchronous Digital Hierarchy）がありますが、国内においては SDH の方が多く用いられています。

タイムスロット単位での経路制御が可能な為、WDM と比べると、光ファイバーあたりの伝送容量は小さくなりますが、タイムスロット単位でのトラフィック制御（経路制御、帯域制御）が可能となる為、よりメトロネットワークに適したソリューションとなります。

しかしながら、安価な CWDM 製品の登場や、Ethernet の大容量化、IP/Etherner パケット転送時のオーバーヘッドの課題等の理由より、TDM を用いたメトロネットワークの需要は徐々に減りつつあります。

TDM の実質的な後継技術としては、パケット転送の効率化が考慮された OTN（Optical Transport Network）や、伝送機能とパケット転送機能の双方のメリットを併せ持つ P-OTS（Packet Optical Transport System）といった技術が注目されています。

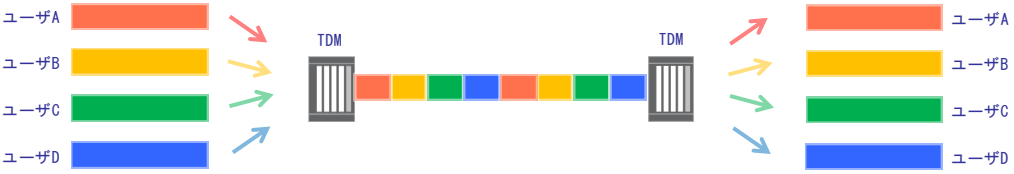


図 4-2d TDM のデータ伝送イメージ図

・伝送装置の物理トポロジー

TDM や WDM を使用したネットワークを構成する場合、物理トポロジーは以下の 3 種類があります。尚、TDM、WDM では、一般的にループプロテクションの機能が含まれている為、拠点間で物理的なループが発生しても L2 ループの対策は不要です。

―Point to Point

名前の通り機器間を Point to Point で接続します。

―Linner Add/Drop

Point to Point の構成を複数台直列につないだ形で接続します。

―Ring

名前の通り機器間を Ring 状に接続します。

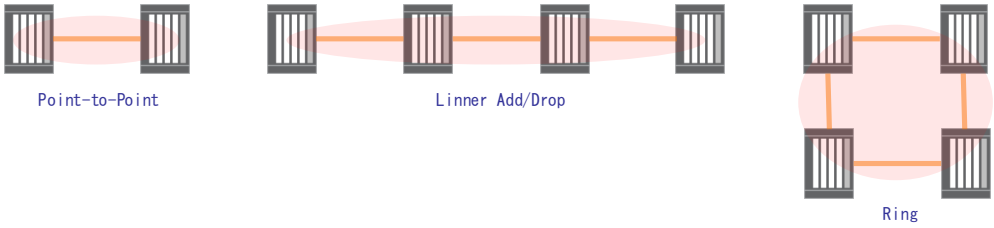


図 4-2e 伝送装置の物理トポロジー図

・伝送装置の障害時の動作

障害時の動作に関しては、大きく分けると 2 通りあります。

― 1+1 方式

Work/Protection 双方に同じデータを送信し、受信側でデータを選択します。

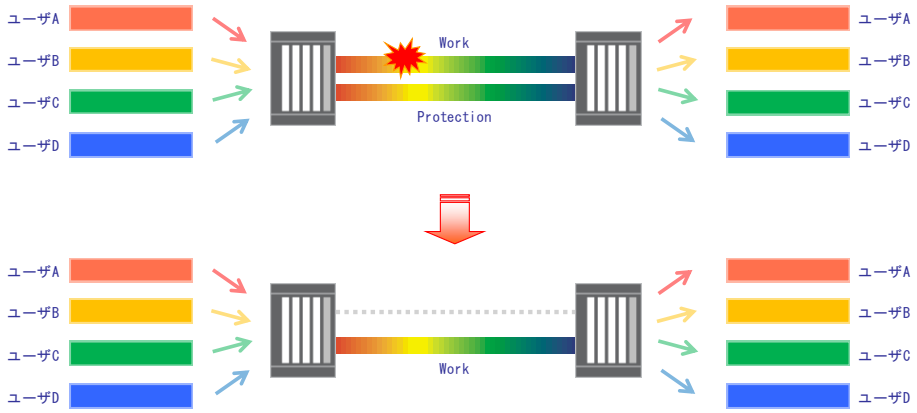


図 4-2f 1+1 の障害動作図

― 1:1(1:n) 方式

Work 側にのみデータを送信し、障害時に Protection 側へ送信/受信の双方を切り替えます。

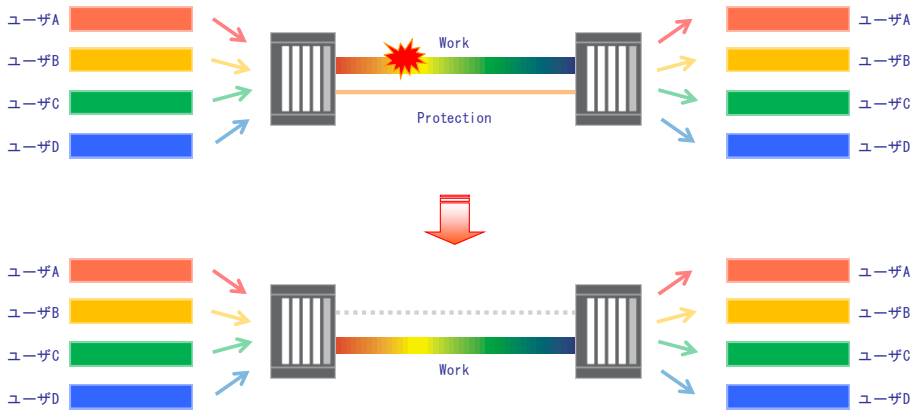


図 4-2g 1:1(1:n)の障害動作図

(2)PB (IEEE802.1ad Provider Bridge)

VLAN 数を約 4,000 以上に拡張させるソリューションとして、PB があります。PB は、利用者企業で利用する VLAN タグ (C-TAG)に加え、VLAN タグ(S-TAG)を付与することで、ネットワークとして区別可能な範囲を 4,000×4,000＝約 16,000,000 まで拡張可能となります。これにより、最大で約 16,000,000 のマルチテナント性を確保することが出来ます。

ただし、PB 自体には L2 ループ対策の機能は含まれていない為、ループ対策が必要な場合は、別途 RSTP(Rapid Spanning Tree Protocol)等との併用を検討する必要があります。

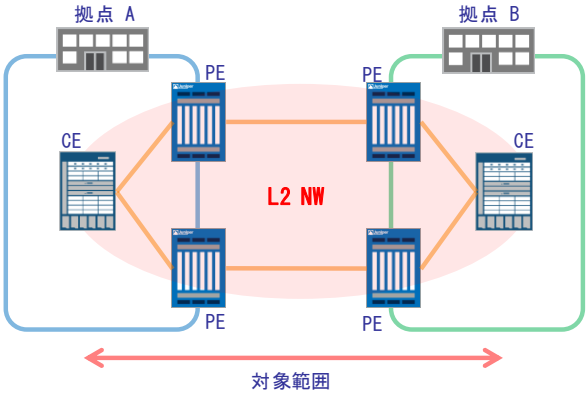


図 4-2h PB の対象範囲

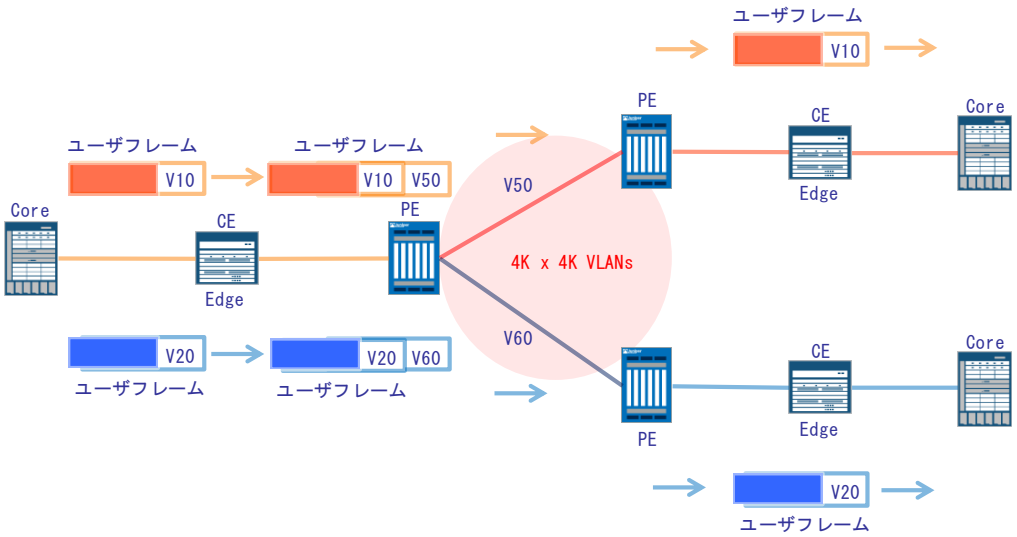


図 4-2i PB を使用した VLAN 拡張方法

(3)PBB(IEEE802.1ah Provider Backbone Bridge)

PB の VLAN 拡張に加え、MAC 収容数等更に拡張性を高めたソリューションが PBB です。PBB では、PB のフレームに I-TAG、B-TAG、B-MAC と呼ばれる追加ヘッダを付与してカプセル化を行います。PBB の場合、バックボーン内でのフレーム転送はこれらの識別子のみで行われ、PB フレーム内のタグや MAC については参照しない為、VLAN や MAC アドレス含めた拡張性を提供しています。

しかしながら、PBB に対応した機器は PB のみ対応した機器と比べて高価な物が多いです。また、PB 同様 PBB 自体には L2 ループ対策の機能は含まれていない為、ループ対策が必要な場合は、別途 RSTP 等との併用を検討する必要があります。

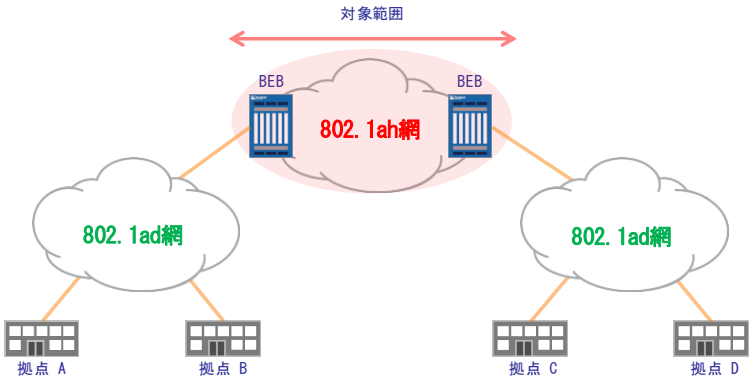


図 4-2j PBB の対象範囲

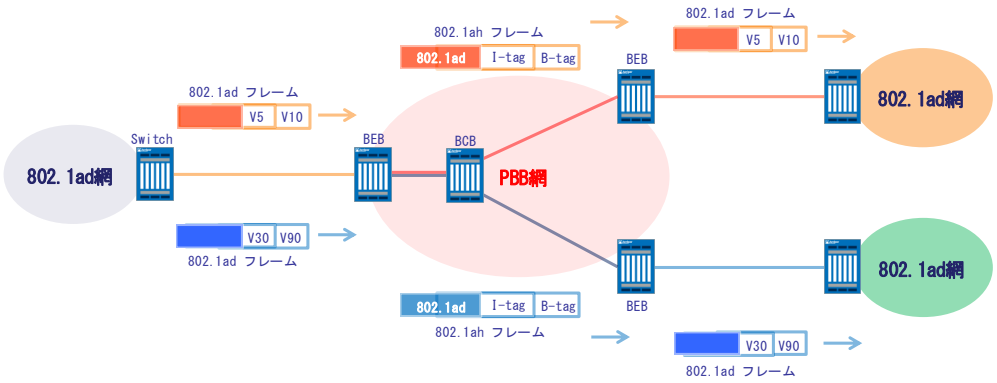


図 4-2k PBB のイメージ図

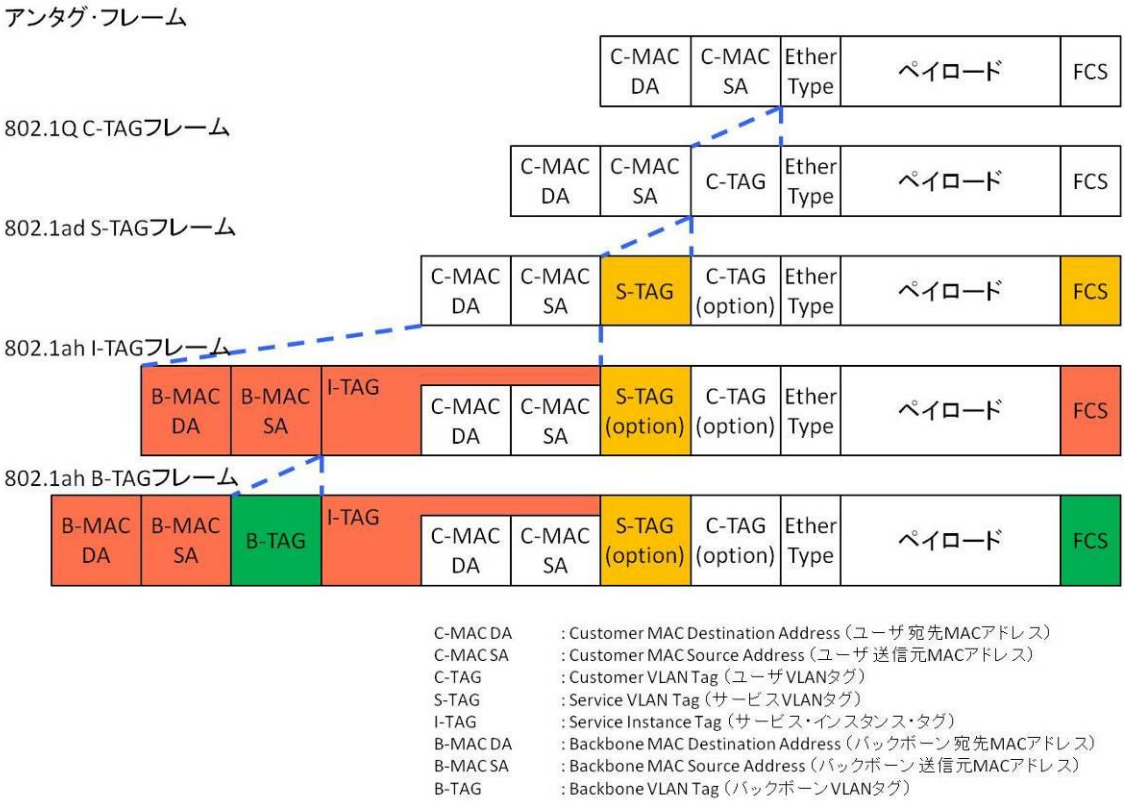


図 4-21 PB/PBB のフレームフォーマット比較

(4)VPLS(Virtual Private LAN Service)

広域のネットワークを構築する際によく用いられるソリューションとして、MPLS を拡張した VPLS があります。MPLS は、Multi Protocol Label Switching の略であり、MPLS では網内の通信にラベルと呼ばれるシンプルな識別子を用います。P ルータ(Provider ルータ:MPLS 網内のルータ)、PE ルータ(Provider ルータ:MPLS の境界線となるルータ)と呼ばれる MPLS 対応ルータ間でラベルをもとに通信を行うことで、VLAN/PB/PBB や IP と比較すると、より柔軟なトラフィック制御が可能となります。VPLS は、MPLS ネットワーク上に仮想的な L2 ネットワークを構築可能な技術であり、複数の拠点間で L2 ネットワークを構築することが可能となります。

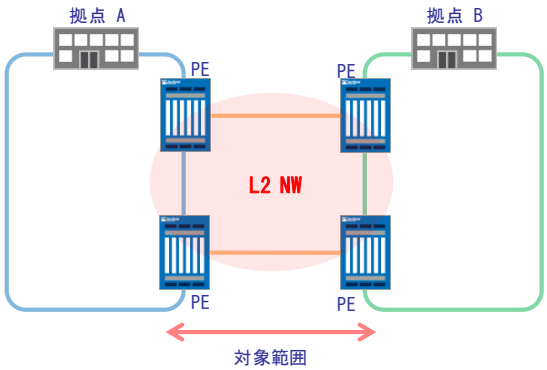


図 4-2m 広域 L2 ネットワークの対象範囲

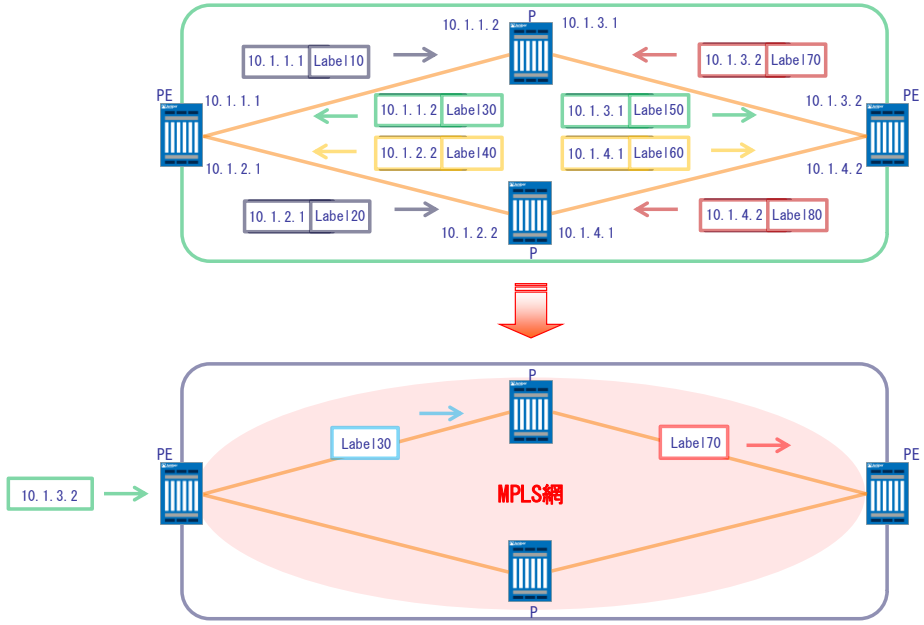


図 4-2n MPLS の動作イメージ

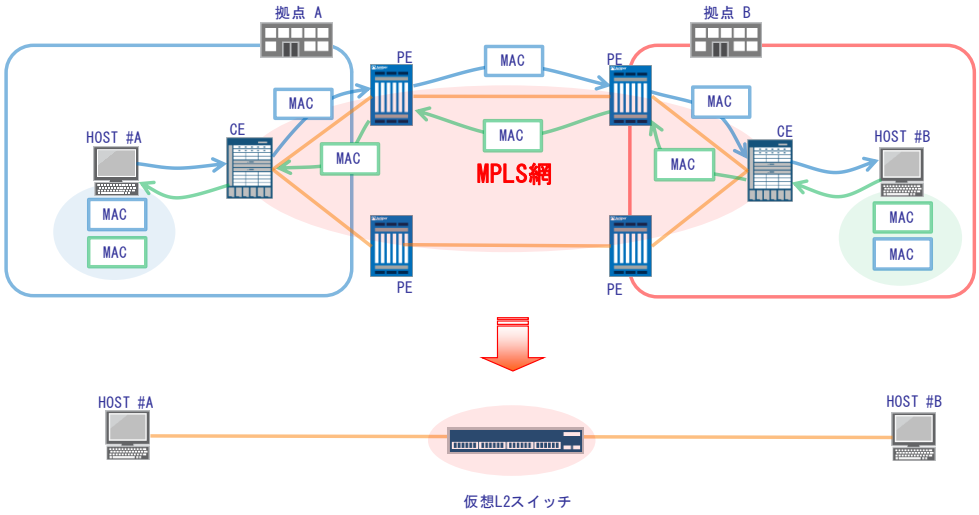


図 4-2o VPLS のイメージ図

VPLS を用いた場合、バックボーンの転送に VLAN 情報は不要な為、4,000×n の VLAN 拡張性を持たせることが可能です。しかしながら、MAC アドレステーブルは保持する為、MAC の収容数については必要数と機器の性能を確認しておく必要があります。

VPLS 自体は、ループ対策機能を含んでいない為、構成によって L2 ループが発生します。ただし、VPLS に対応した機器の多くは独自のループ対策機能を実装しています。代表的な実装例としては、PE をアクティブ-スタンバイ化して利用する方法があります。

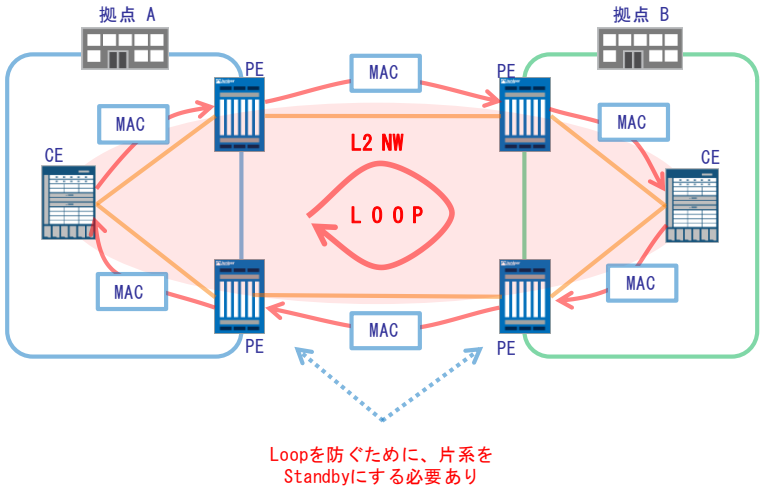


図 4-2p VPLS を使用した場合の L2 ループ対策

(5)Ethernet VPN(Ethernet Virtual Private Network)

Ethernet VPN は、VPLS の拡張技術として RFC(Request for Comments)で標準化中の技術です。VPLS の機能に加え、MAC アドレスの拡張対策が含まれております。
また、L2 ループ対策も含まれており、PE をアクティブ-アクティブで利用することも可能です。

上記以外にもオペレーションを容易にする工夫等が実装される予定となっており、データセンター間の L2 技術として期待されておりますが、標準化中の技術の為、現時点で Ethernet VPN を実装した製品はありません。

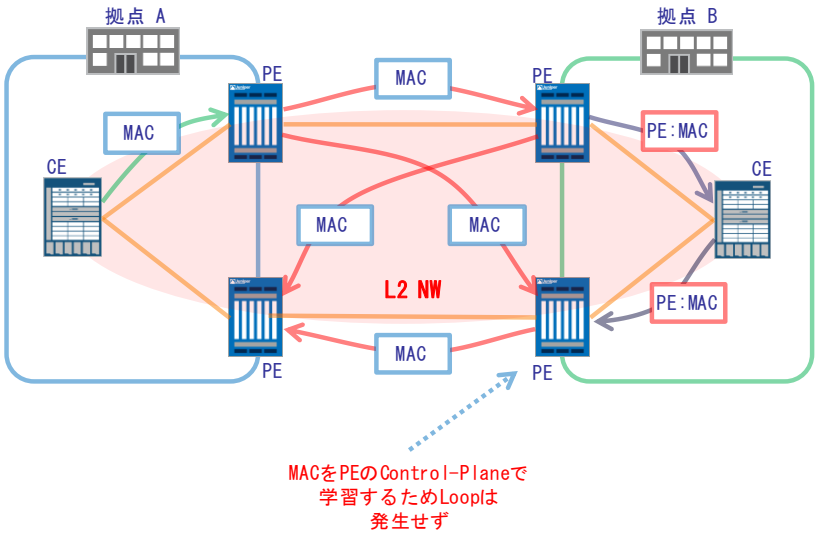


図 4-2q Ethernet VPN を使用した場合の L2 ループ対策

(6) OpenFlow / SDN(Software-Defined Networking)

VLAN に依存せずに、マルチテナントを実現するソリューションとして、SDN も期待を集めています。

利用企業やアプリケーション毎のトラフィック識別を行う方法として、OpenFlow 等を用いた SDN がありますが、OpenFlow / SDN は大きく分けて 2 通りの実装方法があります。

①ホップバイホップ（Hop by Hop）方式

End to End の全てのスイッチにおいて、OpenFlow を用いた転送を実施する方式です。

フレームが入ってきたスイッチは、外部のフローコントローラを参照し、フローテーブルに定義された振る舞いに従い処理を行います。この処理は、End to End の経路上の各スイッチが全て OpenFlow に対応している必要があり、ホップバイホップモデルと呼ばれます。フローテーブルの参照は、通常最初の一回のみ実施され、その後は定義されたフローテーブルに基づいて転送処理を行います。

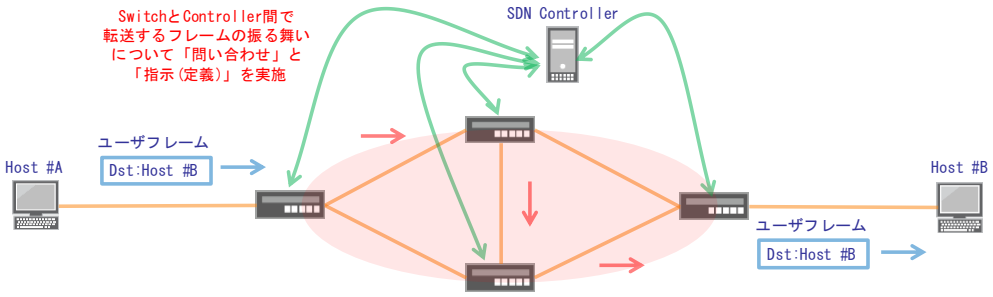


図 4-2r OpenFlow/SDN(ホップバイホップ)を使用した経路制御

フロー自体の識別方法は、物理ポート番号、VLAN、MAC、IP、TCP/UDP ポート番号、MPLS ラベル等、様々な情報を利用可能であり、それぞれのフローは独立制御可能な為、複数の識別子を用いて VLAN 数に依存しないマルチテナントを実現することが可能です。

②オーバーレイ（Overlay）方式

ホップバイホップモデルが全てのスイッチで OpenFlow を用いるのに対して、オーバーレイモデルでは、両端のスイッチのみで OpenFlow を用います。

両端のスイッチは、サーバ内の仮想スイッチ、または専用のゲートウェイスイッチを用います。これらのスイッチ間でトンネルを張る(オーバーレイする)ことで、間のネットワークについては従来のネットワークをそのまま利用可能であり、データセンター間のネットワークが L3 ネットワークであっても、L2 フラットなネットワークを構築可能です。

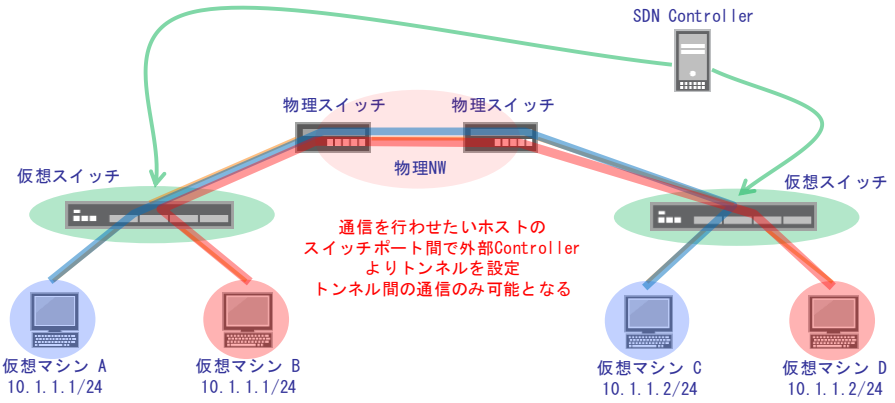


図 4-2s OpenFlow/SDN(オーバーレイ)を使用した経路制御

利用可能なトンネリングプロトコルは、従来の GRE(Generic Routing Encapsulation)、IPSec(Security Architecture for Internet Protocol)を含め様々な物がありますが、SDN との連携においては VXLAN(Virtual eXtensible Local Area Network)、NVGRE(Network Virtualization using Generic Routing Encapsulation)、STT(Stateless Transport Tunneling Protocol)等のプロトコルが注目されています。これらのトンネリングプロトコルは、大規模なマルチテナントを実現するための識別子を保有している為、単独で利用した場合でも VLAN 数に依存しないマルチテナント構成を実現可能です。

(7) ソリューション毎の比較

それぞれのソリューションについて、適用区間、VLAN、MAC の拡張性等を比較すると以下のようになります。

表 4-2a データセンター間で L2 ネットワークを実現可能なソリューション

項目		TDM/WDM	VLAN	PB	PBB	VPLS	Ethernet VPN	OpenFlow /SDN (Hop by Hop)	OpenFlow /SDN (Overlay)
主な適用区間	NW to NW 間	○	○	○	○	○	○	○	○
	サーバ to サーバ間	×	○	×	×	×	×	○	○
利用可能な外部接続回線	ダークファイバー	○	○	○	○	○	○	○	○
	専用線	×	○	○	○	○	○	×	○
	L2VPN	×	○	×	×	○	○	×	○
	L3VPN	×	×	×	×	○	○	×	○
L2 ループ対策		○	× ※1	× ※1	× ※1	× ※1	○	○	− ※2
4K VLAN の拡張		○	×	○	○	○	○	○	○
MAC の拡張		×	×	×	○	×	○	○	○

※1：L2 ループ対策については、別途方式の検討が必要です。

※2：L2 ループ対策については、物理ネットワークの構成に依存します。

※3：導入コスト、および運用コストについては、対象ネットワークのサービスモデルにより異なります。

４－３．広域レプリケーション

前項では、データセンター間におけるフラットL2ネットワークの実現方法について触れましたが、これらのネットワークを使って実際に事業継続、災害対策、バックアップ等のシステムを実現する為には、ストレージデータを如何に高速、且つ効率的にレプリケーション出来るかが次の課題となります。
本項では、ストレージデータのレプリケーション設計に当たって、ネットワークで考慮すべき点について説明します。

４－３－１．ネットワーク上におけるデータレプリケーション方式について

ネットワーク上にストレージトラフィックが集約されるという意味では、既にWAN経由の広域データレプリケーションは普遍的に行われています。既存ネットワーク上でデータレプリケーションを実現するためには、まずデータレプリケーションの方式としてどのようなものがあるかを把握しておく必要があります。下記にその方式についてまとめています。

データレプリケーション方式の比較

	レプリケーションタイプ		
	ストレージ型	ホスト型	ネットワーク型
異機種環境でのサポート	低 ・類似ストレージ間のみで機能する	高 ・ストレージに依存せず、ネットワーク接続およびダイレクト接続のストレージで機能する	高 ・ストレージやプラットフォームに依存しない
性能と拡張性	・ストレージに依存する ・ハイエンドストレージでは非常に良い	良い ・サーバに負荷かかる ・管理性の面で、拡張性に制限あり	非常に良い
コスト	・類似ストレージが必要 ・高い導入コスト ・箇所が増えるごとに高くなる	・ハードウェア不要 低い導入コスト ・サーバの台数が増えるごとに高くなる	・インテリジェントスイッチまたは、インライン型アプライアンスが必要 ・高い導入コスト ・拠点が増えるごとに高くなる
複雑性	中から高	低	中から高
モード	同期、非同期	非同期	同期、非同期
主要なレプリケーションタイプ	論理ユニット番号(LUN)またはボリュームブロックレベル	ファイルシステム	論理ユニット番号(LUN)またはボリュームブロックレベル

出展：　http://www.jdsf.gr.jp/backup/replication.html

従来の方式としては、ホスト型に分類されるバックアップソフトによる方式や、高機能ストレージの機能を使用するストレージ型のタイプが多く導入されてきました。ネットワーク型はアプライアンス等を利用することで、それらの処理をネットワーク上の別の場所に肩代わりさせる方式のために、ホストへの負荷は低くなりますが、ネットワーク帯域を圧迫したり、専用の機材が必要となったりするために、導入へのハードルが高いことがあまり普及していない原因となってい

ます。
今後更なる災害対策等の重要性が増すことは確実で、データをどのようにネットワークを利用して効率的に遠隔地へ複製するかが課題となってきます。

４－３－２．データレプリケーションと広域通信網

広域通信網を利用したデータレプリケーションは災害対策等には欠かせない技術となります。遠隔地とネットワークで結ぶことで、従来のテープ保管と運送のような方式よりも効率的に迅速にデータを遠隔地に送ることができるようになります。

広域レプリケーションにはWAN回線の品質が大きな影響を与えます。しかしながら、一般的にはセンター間の回線は共有化されており、全ての帯域をストレージのレプリケーションに使用できることは現実的に不可能ですので、帯域を絞って利用することになります。また回線遅延は、ただでさえ少ない帯域に対してデータを送るには致命的な影響を与えかねません。これらの影響を最小化するための技術が普及しています。これらは総称として「WAN 高速化技術」と呼ばれ、様々な製品やプロトコルが登場しています。WAN高速化には大きく分けて2つの方式があります。1つはTCPベース、もう1つはUDPベースです。ストレージ通信に使用されるものの多くはTCPベースで信頼性を高めたものが多く採用されています。

(1)TCPベースWAN高速化

TCP は輻輳によりパケット損失が発生した際には送信データ量を半分にして、そこから緩やかに通信量を回復させることにより、パケット損失が再発しないような動きを取ろうとします。回復途中にパケット損失が起こると、更にスループットが落とされて回復が更に遅れることになります。これにより、遠距離や高遅延環境では帯域を十分に使いきれない事象が発生することがあります。これらの事象を回避するために、ウィンドウサイズをコントロールして送出するデータ量を制御し帯域を抑制して輻輳を回避する技術や、HiSpeed TCP（HSTCP）やキャッシュ等を使用して通信を先読みして高速に返答する技術が開発されています。

(2)UDPベースWAN高速化

UDPは送信確認をしないプロトコルなので、パケット損失には基本的に対応しません。TCPのようなACKを確認して送信する仕組みもないため、高速化しづらいプロトコルです。これをTCPの高速化をベースにして、TCPでカプセル化して高速化の仕組みを利用する等の方式でUDP通信を高速化する技術が開発されてきています。

（３）ファイバーチャネルの広域通信高速化技術（FC over IP）

上記TCPベースでの高速化を利用して、ファイバーチャネル通信を遠隔地間で高速化する技術があります。IPベースの通信環境でTCPを利用してあらかじめ読み込む方式を利用し、回線の遅延を極小化して遠隔地間のファイバーチャネル通信を実現します。距離に依存しますが、主に非同期のファイバーチャネルストレージ間レプリケーションに利用される技術になります。

４－３－３．広域レプリケーションのために検討すべき項目

広域レプリケーションを実装するためには、ネットワーク構成やストレージ機能以外にも検討すべき項目があります。特に検討すべき項目には主に下記が挙げられます。これらの項目はネットワーク設計や品質にも大きく左右されるので、広域レプリケーションにとってネットワークやI/O技術を知ることは重要な要素となります。

(1)Recovery Time Objective（RTO）/ Recovery Point Objective（RPO）

バックアップや災害対策検討をする際に必須な項目になります。データ復旧にかかる時間（RTO）とデータ取得のポイントをいつに取るか（RPO）を設計することが重要です。ネットワーク品質や帯域によっては取得できる時間や転送できるデータ量に限りが出てくるので、ネットワーク構成が大きく影響します。これについては5章で詳細に説明します。

(2)同期／非同期

ストレージ間のデータの状態を決める場合、2つの方式があります。1つはデータを完全に同期させる方式（同期）、もう1つはデータを一定間隔で複製してリアルタイムでは複製しない方式（非同期）があります。同期は一般的には近距離（一般的には10km圏内程度）接続、非同期は長距離（一般的には数十から数百km程度）接続になります。同期については、ネットワークや回線の品質によっては実現ができない場合があるので注意が必要です。非同期の場合でも、ネットワークや回線の品質によってはデータレプリケーションが終えられない等のことも考えられますので、いずれの場合においても、ネットワーク構成は重要な要素となります。

(3)回線遅延

回線環境は広域レプリケーションには非常に大きな影響を与えます。遅延の増大により、データの到達時間が遅れ、それに引っ張られてデータを送出する側がデータを送り出す量が制限されてしまうために、スループットが極端に低下することも起こりえます。この遅延を最小化するために距離を縮めるか、遅延を発生させないようにあらかじめバッファするための領域を設計する等の配慮がネットワーク側にも必要になります。

(4)帯域の節約

広域レプリケーションのストレージトラフィックが利用できる回線帯域量は、送ることのできるデータ量や複製の完了時間に大きな影響を与えます。またストレージトラフィックを制御しなければ、センター間の通信網を圧迫する要因にもなります。回線帯域をいかに効率よく、しかもなるべく影響の少ないように利用させるかがポイントになります。それにはストレージ側だけでなく、ネットワーク側にも帯域を制御する技術（QoS等）やストレージトラフィックの上限を設定する技術（Rate Limiting等）を考慮する必要があります。

(5)転送データの圧縮技術

上述の帯域利用にも関係しますが、ストレージからのデータ転送量を減らすことで、帯域の圧迫や転送量増大による複製完了時間の遅延を極力なくすことができます。その 1 つとして、転送するデータの圧縮を行うことで、転送量を減らすことができるようになります。

一般的には転送パケット内のペイロードの圧縮を行うことで、ペイロードサイズ自体を減らし、更には減ったペイロード同士をひとまとめにして送り出すことで、転送パケット数自体を減らすという方法があります。またパケットサイズを大きくすることでパケットサイズを減らすという方法もあるので、ネットワーク側でジャンボフレーム等の技術への対応検討が必要な場合も出てきます。

(6) 重複排除による送出データ量の削減

こちらも上述の帯域利用にも関係しますが、そもそものストレージ内部のデータ量を減らすことで、送出されるデータ量を減らして帯域の圧迫や複製完了時間の遅延を極力なくすという方法もあります。ストレージ内のデータ量を減らす方法としては、重複排除という技術が一般的です。

5. ディザスタ･リカバリを実現するためのネットワーク

５－１．ディザスタ・リカバリを実現するに当たり

2011年の東日本大震災においては、長時間の停電や通信ケーブルの切断、通信局舎設備の津波による被害等により各ITサービスが広範囲かつ長時間にわたり多大な影響を受けました。

東日本大震災以降、ディザスタ･リカバリ対策として各社メインサイトから離れたデータセンターにサイトを構築するケースが増えており、その後も電力会社の計画停電の影響の懸念やその他の震災や津波の可能性などを想定した、より広域のディザスタ･リカバリ対策のニーズが大きくなっています。

まず、ディザスタ･リカバリを検討する際に基本となるのが、RPO とRTO、およびそれを実現するアーキテクチャとサイトの選定であり、最初にどこまでの障害や災害を想定し、その影響の範囲をどの程度に押さえることを目標として設計するかが重要となります。

･RPO (Recovery Point Objective)

復旧作業を行うに当たってどの時点の状態に戻すかの目標値。サービスが再稼働したときに、被災直前のデータに回復するのか、数日前のデータに戻ることを許容するのかで、バックアップの頻度や復旧後のオペレーションはかなり違ったものになります。

･RTO（Recovery Time Objective）

災害発生時点から何時間後もしくは何日後までにサービスを再稼働するのかを示す目標値。したがってサービスのダウンタイムとなります。ダウンタイムが長引けば事業の存亡にかかわる他、コミュニケーションサービスや情報サービスは、災害直後に最も重要なサービスになるため高い目標値が求められます。

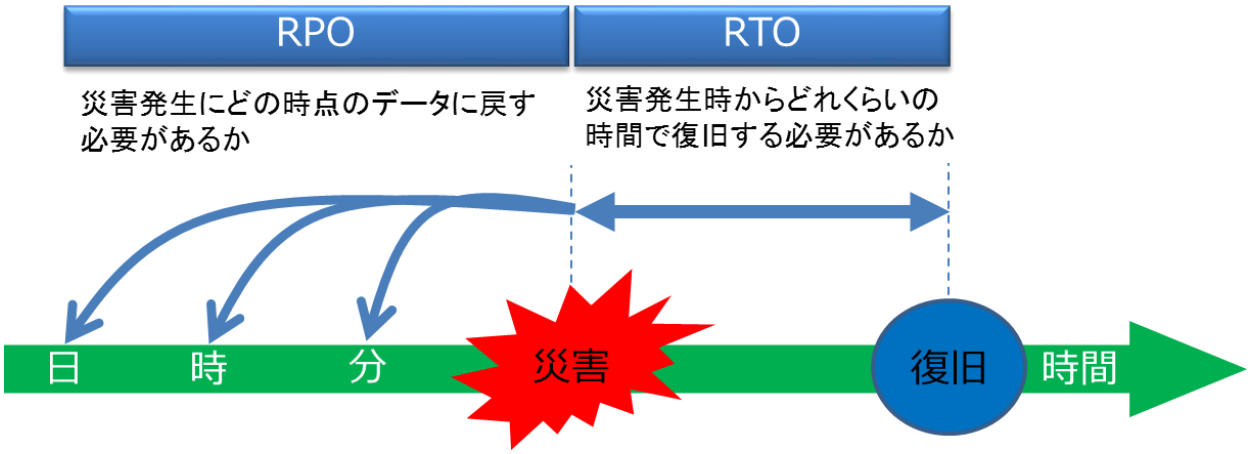


図 5-1a；RPO と RTO

次に上記目標値にしたがって求められるアーキテクチャとサイトの選定を検討します。

以下のようなデータの定期バックアップからレプリケーション(常時バックアップ)、または金融系サービスでは完全同期のクラスタリングが主流でしたが、最近ではGSLB(GlobalServer Load Balancing) やKVS(Key Value Store:分散ストレージ)といった技術要素の普及からそもそもサービス自体を各サイトで分散させ、ディザスタ・リカバリサイトもサービスを提供することにより、災害時においてもサービスを継続させるソリューションも増えてきています。

ただし、どのソリューションを採用するかはサービスの内容や目標設定により異なるため、求められる品質を十分に理解しサービスに最も適した設計することが重要です。

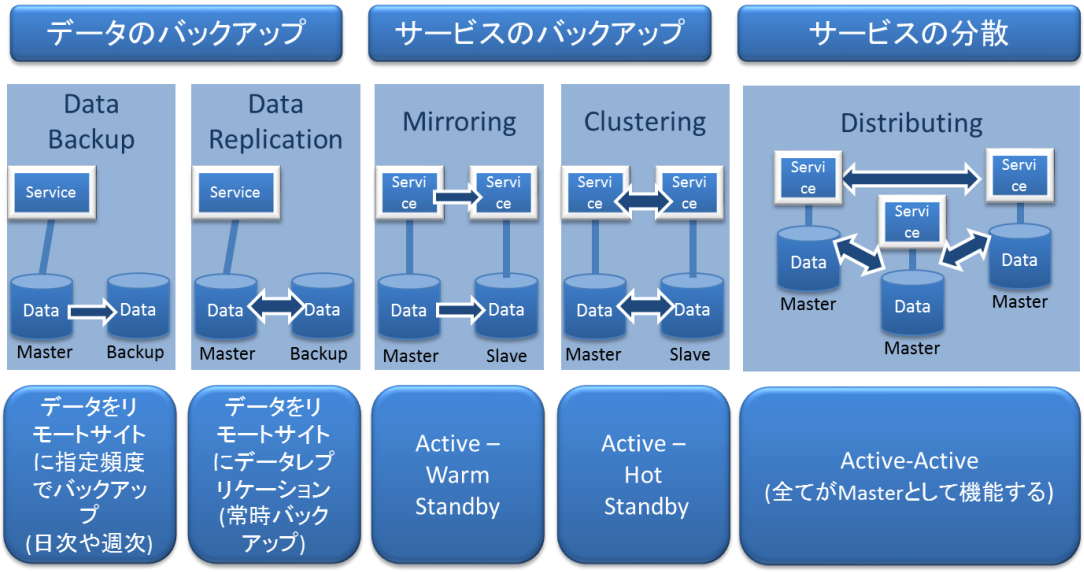


図 5-1b;提供サービスとバックアップの関連性

アーキテクチャを検討する際には、サイトのロケーションも重要になります。サイト間の距離に比例して耐障害性は向上することになりますが、通常距離に反比例してネットワークの遅延量は増加する為、システムが許容しうる遅延量、スループットを確認する必要があります。

	想定の障害、災害	DR サイト設定
近距離 DR	DC やシステムの単一障害など	同一エリア内での第二サイト。広域災害時には機能しない。
近郊 DR	15～30km 圏内の地域災害（台風、水害など）	60 ㎞以上離れた距離にて DR サイトを構築 電力ケーブル、通信ケーブルのルートにも注意が必要
広域 DR	関東地区、近畿地区などの都市単位の災害(地震や津波など)や通信設備、電力会社の障害など	ネットワークだけでなく、電力会社などのインフラ冗長性が必要。東日本と西日本にて分散させるなど。 もしくは国外の DC やクラウドサービスを利用する場合もある。

表 5-1a;.想定災害と DR サイト設定の考え方（例）

クラウド系サービスは本来サイトロケーションを公開しないものが過去多い傾向がありましたが、最近では各事業者によりリージョンやエリアといった定義のもとロケーションを含めて選択できるようになっているものが多くなっています。ロケーションを検討する際には、各公共機関のハザードマップ等も確認するとともに、電力会社や通信ケーブルルートといった物理的な構造などにも配慮することが必要となります。

また、バックアップ方式のディザスタ・リカバリを機能させるためには、バックアップをリストアさせるオペレーションが最も重要となります。システムデータのバックアップがあっても、いざ障害や災害が発生した時にオペレーションスタッフの体制が整えられなければ意味をなさない為、連絡網の整備や駆けつけ要員の確保、復旧オペレーションの訓練等を様々な想定の元、予め準備しておく必要があります。

したがって、以下のような各接続性を把握し、予め障害や災害が発生したケースを想定したシミュレーションを実施し、イメージしておくことが重要です。

５－２．ディザスタ・リカバリでのネットワーク設計

５－２－１．ネットワークの接続性

ディザスタ･リカバリサイトのネットワークを設計する際には、そのサービスへアクセスする利用者環境との接続性を予め想定しておくことが重要です。携帯向けサービスであればモバイルキャリアとの接続性、また海外からの接続性や運用スタッフやパートナーがアクセスするネットワークとの接続性などを考慮して設計しないと、いざ災害時に期待していた効果を得られない可能性があります。

したがって、以下のような各接続性を把握し、予め障害発生時や災害時を想定したシミュレーションをしイメージしておくことが必要です。

・国内の各サービスプロバイダとの接続性
　インターネット接続やプライベート回線を契約している事業者のバックボーン構成およびその他各事業者との接続地域とその接続までの構成

・海外との接続性
　インターネット接続やプライベート回線を契約している事業者もしくはその事業者が接続している国際キャリアの海底ケーブルルートや接続地域

・その他サービスとの接続性
　GSLBやDNS、その他システムが利用している各種サービス

例えばプライマリ DNS が停止し、セカンダリ DNS によりサービスを継続した場合、プライマリがある期間以内に復旧しない場合はセカンダリDNS が保持するゾーン情報が期限切れとなった時点でサービスが停止するといったことも起こりえます。

５－２－２．データレプリケーション用ネットワーク

データのレプリケーションやデータベース同期用ネットワーク接続に関しては、4―3章にて解説されている内容を参照ください。

５－２－３．接続性の切り替え手段

コールドスタンバイやウォームスタンバイではなく、ディザスタ･リカバリサイトのシステムを稼働させておくことによりRPOをできる限り小さくすることができます。具体的にはDNSラウンドロビンやGSLBなどが有効なソリューションとなります。

RPO を長めに設定している場合は、DR サイトのサービス提供準備を確実に行った上で、DNS やプログラム側を手動にて切替することができるが、システムの同期や半同期が確保されている場合には GSLB を利用することにより自動での切り替えや、負荷の軽いサイトへ分散するロードバランス的な設計が可能になります。

・DNS ラウンドロビン
　DNS を利用して 1 つのサービスを複数のサーバに分散するシンプルな仕組みであり、DNS の A レコードに複数の IP アドレスを登録するのみです。追加の投資等や複雑なオペレーションは必要ない

が、優先順位を設定することはできず、かつ均等に分散されるとは限りません。
　また、サーバやシステムに障害が発生してもDNSはそのサーバのIPアドレスを応答し続けるため、サービス品質としてはリトライやタイムアウトといった上位アプリケーションの仕様に大きく左右されます。

また、Windows Vista や Windows server 2008 においては IPv6 における RFC3484 の Destination IP address selection のルールを IPv4 に対しても適用しまったことにより、ラウンドロビンが機能しないといった事例も発生しております。この問題は、Windows 7 や Windows server 2008 R2 以降では改善され発生していないようですが、クライアント OS の仕様等により左右される例と言えます。

本事象の詳細は以下のリンクを参照ください。
参考: http://support.microsoft.com/kb/968920

・GSLB （Global Server Load Balancing）
　クライアントからのアクセスを物理的に離れた場所に設置したサービスサーバに振り分けて処理を分散する仕組みで、広域サーバ負荷分散とも言います。簡易的なGSLBとしては、ロードバランシング機能付きのDNSとして利用されており、DNSラウンドロビンよりも細かな制御が可能となります。ただしセッション同期・維持についての確認が必要です。
GSLB の利用方法は以下のような設計が考えられます。

1） Master – Backup の自動切り替え
　サイトヘルスチェック機能により Master サイトの障害発生時に自動的に Backup サイトへの切り替えを実施することにより、サービス継続性を維持します。

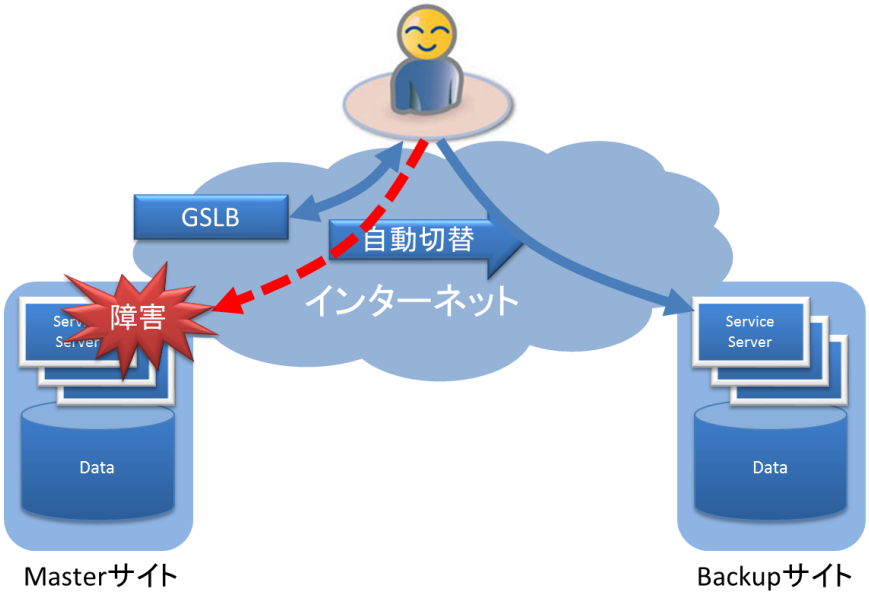


図 5-2a；Master-Backup 自動切替

2） Master – Master の負荷分散
　ハッシュ等により利用者からのアクセスを分散させるほか、サイトヘルスチェック機能によりシステ

ムの負荷を確認し、より負荷の軽いシステムへのアクセスへ誘導する、アクセス元のロケーションによってアクセス先を最も地理的に近いサイトへ誘導する、などで利用者レスポンスの向上を実現します。

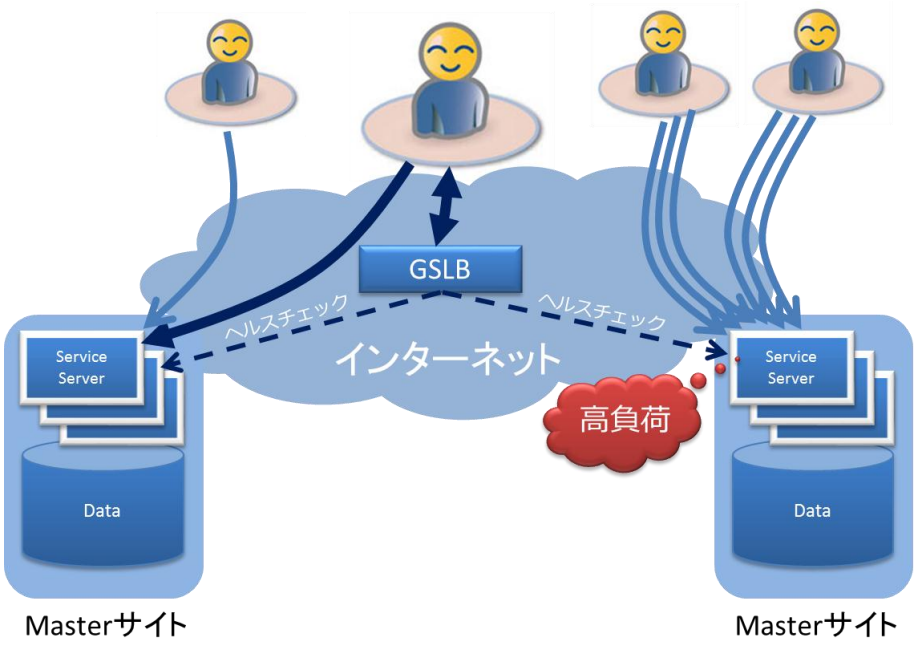


図 5-2b；Master-Master

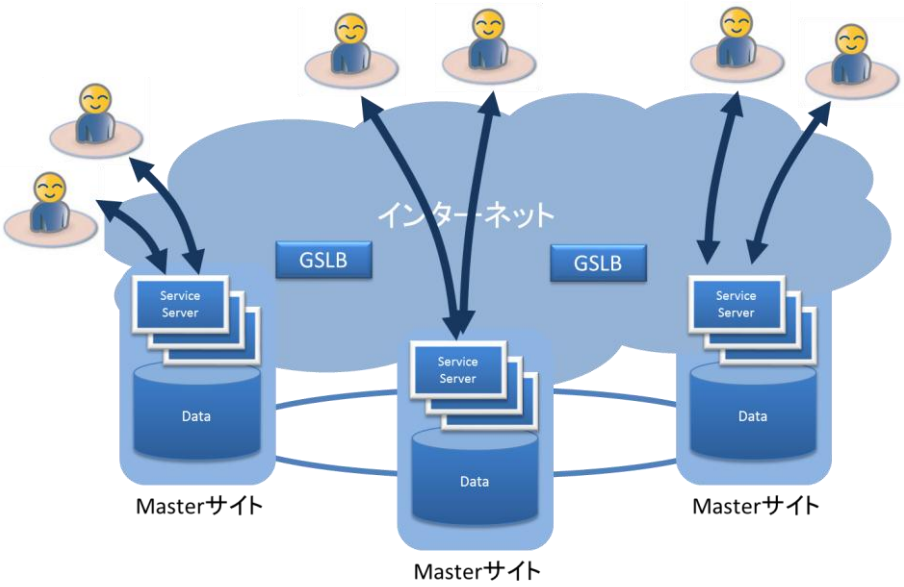


図 5-3c；Master 複数分散

また、クラウド系サービスとGSLBが連動することで、Masterサイトに障害が発生した際に、DRサイトが自動的にスケールアウトするように設計することも可能です。

このように、ネットワーク、アプリケーション、サービス、データベース等の可用性、拡張性を高め、各

リソースを適切に配置および分散することにより、災害時だけでなく通常運用時においても突発的なアクセス急増にも対応できるようになり、サービス品質と顧客満足度向上につなげることができます。

５－３．今後の災害対策に求められるネットワーク

３－3章で記載した SDN 等の導入やネットワークの仮想化、４－3章で記載したデータベース側のレプリケーションといった要素も非常に重要となりますが、それらを活用しながらサービスシステム側の分散を行い、ユーザアクセスを適切にコントロールすることが、災害対策と同時にサービスの拡張性やユーザへのサービス品質の向上を実現することになります。

また現在東京に集中している IT サービス全体で災害対策を考えることにより、日本の IT サービスを発展させ、そのニーズに対応できるネットワークを各事業者が協力し提供することで更により災害に強いネットワークを形成していくことになると考えます。

６．今後の技術動向

第 6 章ではデータセンターにおける今後の課題、技術動向として、昨今の話題でもある「IPv4 アドレス枯渇」「IPv6」「セキュリティ」をテーマに取り上げることにしました。

６－１．ＩＰｖ４アドレス枯渇

2011 年 2 月 3 日に IANA(Internet Assigned Number Authority)が管理するグローバル IPv4 アドレス(以下、IPv4 アドレス)在庫が枯渇し、同年 4 月 15 日にはアジア環太平洋地区の RIR(地域インターネットレジス通り)である APNIC においても在庫が枯渇しました。
これにより、顧客増加、新サービスの追加など含む事業拡大、そして、インターネットの拡大・発展に影響が出始めようとしています。

図 6a: IPv4 枯渇時計

日本データセンター協会では、以前から IPv4 アドレス枯渇に備え「IPv4 アドレス枯渇対応ワーキンググループ」を立ち上げ、その対策や IPv6 対応について検討を進め 2011 年 4 月 11 日に『データセンター利用者のための IPv4 アドレス枯渇対策と IPv6 対応の考え方』をご案内しています。IPv4 アドレス枯渇対応ワーキンググループはドキュメント完成後と同時に活動が終了したことから、ネットワーク WG 内で継続検討を行っておりますので、その一部について触れたいと思います。

IPv4 アドレス枯渇の対策として、次の 3 点があげられます。

1. 利用効率の向上と IPv4 アドレスの確保
2. プロトコルトランスレーション、NAT(Network Address Translation)などの導入
3. ネットワークとサービスの IPv6 対応

「2. プロトコルトランスレーション、NAT などの導入」、「3. ネットワークとサービスの IPv6 対応」については IPv4 アドレス枯渇対応ワーキンググループのドキュメントで触れられていることから、本節では「1. IPv4 アドレスの確保」に焦点をあてることにします。

IPv4 アドレスの確保の方法例として 2 つの手段があると考えられます。

・既存ネットワークから IPv4 アドレスを回収
- 既存ネットワークの整理、統合
- データセンター内バックボーンのプライベートアドレス化
- CGN(Carrier Grade NAT)を用いてプライベートアドレス化

・外部から IPv4 アドレスを取得
- レジストリからの割り当て
- IPv4 アドレス移転制度の活用
- 上位 ISP からの割り当て
- グループ企業間でのアドレス整理(事業譲渡など含む)

既存ネットワークからの回収については、アドレス利用率の低いネットワーク、サーバセグメントを改修し効率の良いネットワークに集約/変更、ネットワーク/サーバの構成変更に伴い機器を減らす、バックボーンの IPv4 アドレスをプライベートアドレスにリナンバリングをすることにより IPv4 アドレスの回収が可能となります。

外部からの IPv4 アドレス取得は、レジストリからの新規割り当てが困難な状況であることから、2011 年 8 月に JPNIC が開始した「IPv4 アドレス移転申請」の活用が注目されています。これは、休眠中の IPv4 アドレスなど含め、分配済の IPv4 アドレスの効率的な流動化を目的に JPNIC と IP アドレスの管理に関する契約を締結している組織間で、指定事業者、歴史的 PI アドレス・ホルダ、特殊用途 PI アドレス・ホルダ間での移転する制度です。この制度を利用することで外部からのアドレス取得が可能となります。2012 年 7 月 17 日現在、32 件(約/11～/12)のアドレスが移転されています。

アドレス移転はアドレス枯渇にとっては非常に有益なものですが、サービスの観点から見た場合、次の弊害と課題が考えられますので注意が必要です。
具体的には、IPv4 アドレス移転、グループ企業間でのアドレス整理、外資系企業の日本におけるアドレス割り当ての場合が該当すると考えられており、その背景となる技術として、「5-2-2.Master-Master の分散コントロール」で触れられている「Geo-Location」(IP Geolocation とも言われます)があります。これは、IP アドレスに位置情報や接続環境などの情報を付加したもので、ゲーム、金融、インターネットラジオなど多くのサービスで適用されており、利用する利用者がどこの地域、どこからアクセスしているかなどを調べ、それに応じて地域毎にサービスの提供可否などの内容に特徴を与えていることがあります。

例えば、以前は日本に割り当てられた IP アドレスを使用していた利用者(事業者含む)が、何不都合なくサービスの利用が出来ていたにも関わらず、何らかの理由で、北米地域で使用していた IP アドレスが IPv4 アドレス移転制度含む何等かの事情により日本に割り当てられ、それを利用者が使用したとします。利用者は IP アドレスの変更に気が付かないまま、以前のサービスを利用しようとしても「Geo-Location」のデータベースの変更はされず、また、それを利用しているサービス提供事業者の認識が無いまま利用者はサービスを享受できなくなる可能性もあります。

IPv4 アドレス枯渇の根本的な解決策は「IPv6 ネットワークの導入/移行」です。しかし、未だ多くのサービス、接続サービスは IPv4 ネットワークを利用していることから、IPv6 だけのサービス提供/展開ならびにビジネスは困難と考えられています。よって、当面の間は IPv4 によるサービス提供/展開/継続と IPv4 アドレスが必要になることから、データセンター事業者は IPv6 導入/移行と共に必要な IPv4 アドレスの確保、調達方法の検討が必要となります。

参照

・IPv4 アドレスの在庫枯渇に関して
　http://www.nic.ad.jp/ja/ip/ipv4pool/
・日本データセンター協会
　データセンター利用者のための IPv4 アドレス枯渇対策と IPv6 対応の考え方

http://www.jdcc.or.jp/news/article.php?nid=eccbc87e4b5ce2fe28308fd9f2a7baf3&sid=56

・JPNIC における IPv4 アドレス移転申請の受付開始

http://www.nic.ad.jp/ja/topics/2011/20110801-03.html

・IPv4 アドレス移転履歴

http://www.nic.ad.jp/ja/ip/ipv4transfer-log.html

出典

：図 6a　http://inetcore.com/project/ipv4ec/index.html

６－２．ＩＰｖ６

「6-1.IPv4 アドレス枯渇」の通り、新規 IPv4 アドレスの割り当てが限定的になっているにも関わらず、インターネットの拡大は進み、新たなサービス、新規利用者などへの対応を含め、データセンター事業者含む各事業者の対応は益々困難なものになっています。

これらの解決策として以前から検討されている IPv6 の導入/対応が必須であり、唯一の恒久的解決策は IPv6 インターネット接続を普及させ利用することにあります。しかし、IPv6 は IPv4 と異なるプロトコルであることから技術的には相互に通信をすることが出来ない為、IPv6 に対応させるために機器のデュアルスタック化(IPv4/IPv6 対応)などが必要となります。一部の機器だけの対応ではエンド-エンドの IPv6 による通信が出来ないため、通信に関係するデバイス含めた各種機器、そしてアプリケーションなど含めた全体的な対応が必要であり、それらを提供するインターネットサービスプロバイダ(ISP)、通信事業者、データセンター事業者、コンテンツサービスプロバイダ (CSP)などの対応が必要になります。

本節では、「6-1.IPv4 アドレス枯渇」で紹介した「データセンター利用者のための IPv4 アドレス枯渇対策と IPv6 対応の考え方」にデータセンター事業者の IPv6 ネットワーク、サービス対応する際の考え方、チェックリストなどが示されていることから、現在の状況、技術的課題を取上げます。

データセンター事業者のみならず多くのサービス提供者の視点としては、現在提供している IPv4 によるサービスと同様なプロセス、例えばサービス企画からネットワーク設計、サービス/ネットワーク運用、利用者設定/管理画面、課金など全てのプロセス、ワークフローの項目において IPv6 が関連しますので、現在 IPv4 で提供しているサービスと同等の検討と対応が必要となりますが、特にアドレス設計、運用管理･監視、ロギングなどの検討/計画/導入時については注意が必要です。IPv6 対応/導入の考え方、進め方は事業者、サービスにより若干の差異が出てくると思われますが、中長期的な観点で事業継続を前提にした場合、新たなサービス、または現在提供しているサービスは IPv6 でも提供可能な状態にする必要があります。

このような中、2011 年 6 月 8 日 0 時 UTC(日本時間で午前 9 時)から 24 時間の 1 日間、ISOC(Internet Society)を中心に Google、Yahoo、facebook、Cisco、Juniper、Microsoft などの米大手 ICT/サービス提供企業が一斉に自社のサービスを IPv6 対応にして各種影響を全世界的に探ってみる試みである「World IPv6 Day」が行われました。参加はそれぞれの事業者や個人が自主的に実施。主な参加対象者として Web サイト、Web サービスをメインに誰でも参加できる試みでした。この試みにより IPv6 による通信量が増えたことが確認できたと同時に、日本はもとより全世界的な IPv6 対応の準備状況、潜在的な IPv6 対応、各種技術的課題である「フォール

図 6b:World IPv6 launch Web サイト

バック問題」「AAAA フィルタ」など明らかとなり非常に有意義な成果となりました。

これらの成果/結果を受け、更なる IPv6 導入/展開を加速させるプログラムとして、2012 年 1 月 12 日に ISOC から 2012 年 6 月 6 日 0 時 UTC(日本時間で午前 9 時)から開始する「World IPv6 Launch」がアナウンスされ開始されました。「World IPv6 Day」は Web サイト、Web サービスを 1 日間だけ IPv6 化するある種の実験的な試みでしたが、「World IPv6 Launch」は次の 3 つの参加カテゴリにすることで IPv6 の導入/展開を全世界的に促しています。

・World IPv6 Launch の参加カテゴリ
- Web サイトを恒久的に IPv6 化
- ISP が新規利用者向けに IPv6 接続サービスを提供
- 一般家庭用ルータ(ホームルータ)の標準設定を IPv6 対応

これらの施策により IPv6 通信のトラフィックはさらなる増加傾向を示し(参照 図 6c)、日本国内においての対応も増加傾向を示しています。

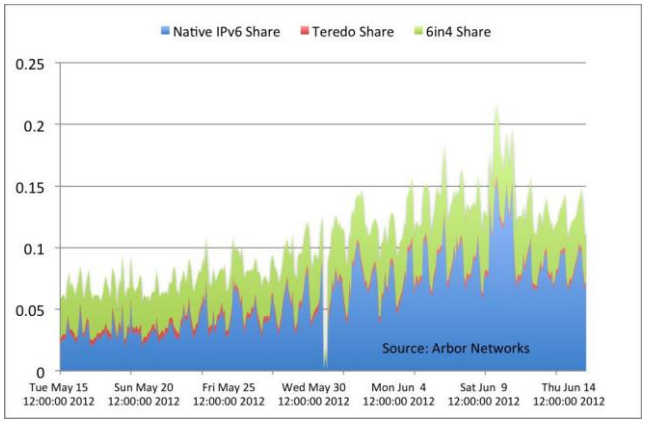


図 6c:World IPv6 Launch 前後 IPv6 トラフィック

しかし、日本国内においては NTT 東西が提供するフレッツ光ネクストのような IPv6 閉域網を用いた特殊な接続環境などにより「フォールバック」によるアクセス遅延(フォールバック問題)が発生することがあります。このことからアプリケーション、サーバ、ネットワークなどの各サービス含めたシステム全体が IPv6 に対応した環境であっても、アクセス遅延により提供するサービス品質に影響を及ぼすことを懸念し「World IPv6 Launch」への参加を見送る事業者が存在しています。

「フォールバック」とは(参照 図 6d)、送信端末の OS(オペレーション・システム)に Windows XP, Vista, Windows 7, MAC OS X など IPv6/IPv4 デュアルスタックに対応したものを使用した場合、IPv6 通信が優先されることが多くあります。この環境において、送信端末のアプリケーションが IPv6 通信を試みますが、何らかの理由で通信が成立しない場合、IPv4 通信で再送を試みます。これを「フォールバック」と言います。これは、使用する OS、Web ブラウザ、アプリケーションなどの組み合わせにより若干の違いはありますが、接続時に IPv6 から IPv4 への再送をすることでアクセス遅延が発生し、状況によっては通信不可能な場合があります。これを「フォールバック問題」と言います。NTT 東西では、この問題を緩和する対策をすることでアクセス遅延を大幅に短縮していますが、Web サイ

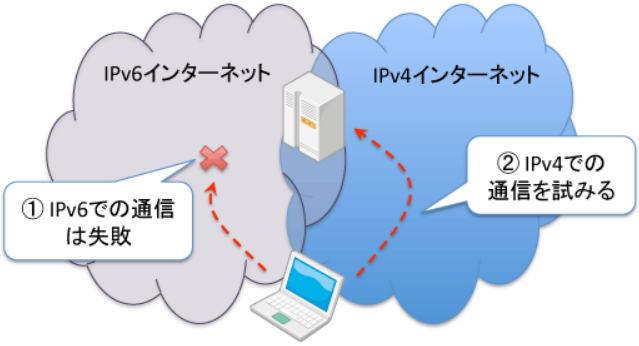


図 6d:フォールバックとは

ト上のコンテンツ、広告などの表示時間、リアルタイム性を重視するコンテンツ、アプリケーションなどを提供するサービス事業者にとってはいまだ課題と考えられています。
これらの暫定的な解決策として「AAAA フィルタ」があります。これは、IPv4 トランスポートで DNS のクエリがあった場合、IPv6 のアドレス（AAAA レコード）を ISP の DNS キャッシュサーバでフィルタし、利用者に対し IPv6 アドレスを通知しない仕組みのことです。利用者は IPv4 アドレスで接続ためフォールバックが起きませんが、その DNS を使うと IPv6 では接続できなくなります。

「フォールバック問題」の多くは NTT 東西と ISP 各社が回避策の検討と対応を進めていますが、それら以外の解決の試みとして、異なる事業者間の連携による共同実験である「DNS ホワイトリスト実験」があります。これは、IPv6 インターネット利用者が IPv6 ネットワーク上でより多くのコンテンツが利用できるようになることを目的に、通常は、ISP 側で「AAAA フィルタ」を行うことで「フォールバック問題」を回避しますが、本実験では、インターネット接続事業が IPv4 接続用の DNS サーバと IPv6 接続専用の DNS サーバを 2 つ用意。実験参加社は、IPv4 向けの DNS サーバに AAAA レコードを返さず、IPv6 専用 DNS サーバに対して AAAA レコードを返すようにしました。これにより「フォールバック問題」を解決しながら IPv6 での接続が可能となりました。

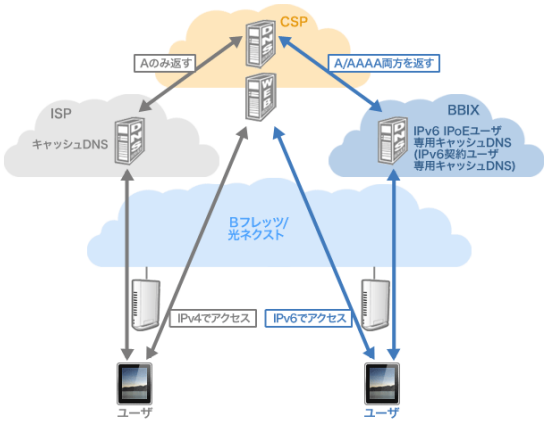


図 6e：DNS ホワイトリスト実験イメージ

今後、この実験を通じて業界全体に問題解決のひとつとして採用されることが考えられます。

参考として、
「AAAA フィルタ」を行うにあたっては、グーグル社は自社 Web サイトへのアクセスの統計データから IPv6 接続に問題があるネットワークを「AAAA レコードを応答しない可能性のあるリゾルバ」として独自にリストアップし公開しています。

Google no AAAA List
https://www.google.com/intl/en_ALL/ipv6/statistics/data/no_aaaa.txt

このリストは頻繁に更新しており、日々対象となるネットワーク（リゾルバ）の数は変化しています。2012 年 11 月 13 日の時点では、256 個のネットワークが登録され 70 個が日本のネットワークになっています。

「フォールバック問題」は、IPv6/IPv4 デュアルスタック環境に対応した端末であれば起こり得る課題の一つですが、日本が特に多くリストアップされている理由に先に示したアクセス回線があげられます。日本では、これらによる混乱の極小化の一環として日本インターネットサービスプロバイダー協会(JAIPA)が「World IPv6 launch についてのご案内」として「一般利用者にお

ける確認、対処方法」「対策を予定している ISP の一覧」などを積極的に紹介しています。

参照：

・BBIX 株式会社　IPv6 ネットワーク実験　フォールバック問題
http://www.bbix.net/ipv6trial/fb/report/1204.html

・日本ネットワークイネーブラー株式会社　フォールバックの問題について
http://www.jpne.co.jp/wp/fallback_at_closed_network/

・Geek なページ　NTT IPv6 閉域網フォールバック問題
http://www.geekpage.jp/blog/?id=2012/3/28/1

・JAIPA World IPv6 launch についてのご案内
http://www.jaipa.or.jp/ipv6launch/index.html

・Google IPv6 Statistics
http://www.google.com/ipv6/statistics.html

出典

：図 6b　http://www.worldipv6launch.org/

：図 6c　http://ddos.arbornetworks.com/2012/06/ipv6-launch-day-a-longer-view/

：図 6d　http://www.geekpage.jp/blog/?id=2012/3/28/1

：図 6e　http://www.bbix.net/news/2012/20120903_01.html

６－３．セキュリティ

データセンター(事業者)はクラウド、ソーシャル、モバイルなどの社会経済活動とその利用/依存度が増すことで情報通信基盤へと変化し、その依存度が高くなるに従い重要度が高まると同時に各種データの重要性も高くなってきています。これら社会基盤となったデータセンターに対する情報セキュリティの要求度合は日々変化していることからデータセンター事業者はこれら要求にみあうような情報セキュリティの確保と維持が望まれています。

データセンターにおける情報セキュリティに関しては ISO/IEC など各種規格が注目されていますが範囲が広いことから、ここでは次の 5 つとし、主に「サービスに対するセキュリティ」「ネットワーク機器、サーバシステムに対応したセキュリティ」についての課題と傾向を示すことにしました。

- ·運用/管理の信憑性
- ·データの保護
- ·サービスに対するセキュリティ
- ·ネットワーク、サーバに対するセキュリティ
- ·入館管理などの設備に関する物理的なセキュリティ

なお、日本データセンター協会では、データセンターに関するサービス品質の向上、ＩＴサービスの提供者及び利用者の誰もが信頼し安心して利用できる信頼性を確保することを目的に、データセンターのセキュリティについて、セキュリティワーキンググループにおいて検討を進めおり、この検討成果を「データセンターセキュリティガイドブック」として策定しています。
本書もあわせてご覧いただくようお勧めします。

http://www.jdcc.or.jp/news/article.php?nid=c81e728d9d4c2f636f067f89cc14862c&sid=96

６－３－１．ネットワーク、ネットワーク機器に対するセキュリティ

ネットワークのセキュリティ(ネットワーク·プロテクション)モデルは、従来からのサービスとインターネット側のクライアントとデータセンター内のサーバ通信を前提としたデータフローを元に計画、設計、構築、運用を行っています。しかし、新たなアプリケーション、仮想化技術などが登場し始めたことでデータフローも変化していることから、それらへの対応と同時に、新たな拡張を踏まえた自由度の高いものを検討する必要があります。図 6d は、データセンターのネットワーク構成並びにデータフローを示したのであり、赤い四角に囲まれた「コア」と「サービス」におけるセキュリティについて触れていきます。

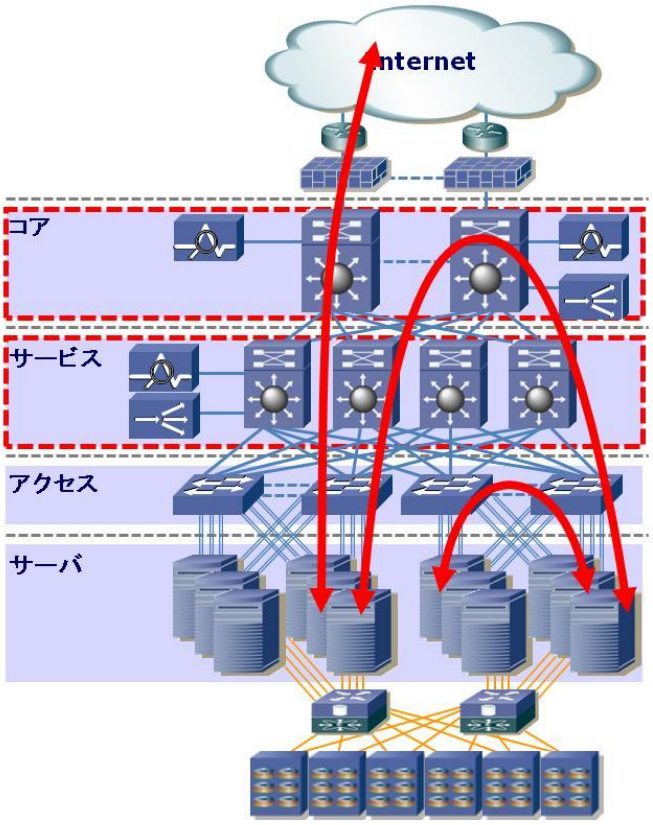


図 6d:ネットワークモデルとデータフロー

データセンターネットワークの機能として、「コア」は、主にファイアウォール、IPS/IDS を配置しイン/アウトトラフィックのフィルタリング、不正な侵入の兆候を検知し通報とこれらの侵入の防止を行い、「サービス」は利用者の個別のサーバ、サービス個別のサーバとそのアプリケーションなどの要件に応じたサービス/データの保護を目的に IDS/IPS を配置します。Web アプリケーションの場合は、アプリケーションファイアウォール(WAF)などを配置することで Cross-Site Scripting(XSS)、HTTP、SQL インジェクション、XML ベースなどの攻撃から保護します。

従来からのトラフィックに対する注意は、主にインターネット側からのトラフィック(インバンドトラフィック)からの盗聴、踏み台、Web 改ざん、DoS/DDoS 攻撃などのトラフィックに着目していましたが、仮想化技術、攻撃手法の多様化により、新たな課題として「ネットワーク/サーバ仮想化」「分散型アプリケーション」そして「仮想化を利用した DoS 攻撃手法」がもたらすセキュリティへの考慮が必要になるとともに、データセンター内部からインターネットへのトラフィック(アウトバンドトラフィック)とデータセンター内部のトラフィックにも注意が必要となっています。

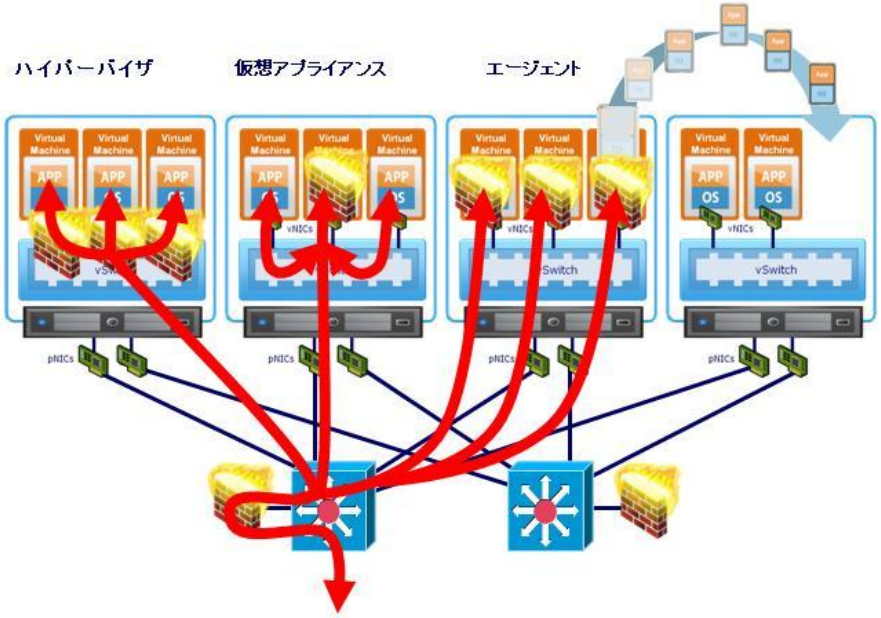


図 6e:仮想化セキュリティ

これは、データセンター内部の仮想マシンなどから他の仮想マシンへの攻撃、外部から仮想化サービス上の攻撃用プログラムを稼働させ、データセンター内部、インターネットに対してトラフィックを送信する可能性、または、知らずに攻撃プログラムに感染してしまうことが一因としてあげられます。ネットワーク/サーバ仮想化がもたらすセキュリティの予防と対策として仮想環境に対応したセキュリティ機能の配置が効果的です。仮想環境に対応したセキュリティ機能は大別すると次の 3 種類になり、それぞれ特徴がありますので注意が必要になります。

種類	主な機能
ハイパーバイザー型	ハイパーバイザーにセキュリティ機能を配置し、ハイパーバイザー上の仮想スイッチ、仮想マシンを含めたトラフィックに対するセキュリティ機能を提供。
仮想アプライアンス型	専用の仮想マシンにセキュリティ機能を持たせ、他の仮想マシンのセキュリティを保護。アプライアンスのFWを通過し、他の仮想マシンと通信を行う
エージェント型	個々の仮想マシンにセキュリティ機能を配置しセキュリティ機能を提供

表 6f:仮想環境の種類とセキュリティ機能

以前からのスパムやフィッシングなど迷惑メールなどで用いるシグネチャマッチング、ヒューリスティック手法などを併用し重みづけを行いホワイト/ブラックリストなどの作成を行い最適化していましたが、新たな脅威と攻撃に対するパターンマッチングなどが出来ない、追いつかないなどと言った事態が発生することが多くなってきました。
最近の傾向として、リアルタイムにプロビジョニングした結果から疑わしい脅威、攻撃を仮想環境内で再現、解析、特定し自動的にシグネチャを作成し迅速な対応を促す機器も登場しはじめようとしています。

６－３－２．DNS に関わるセキュリティ

DC 事業者の多くはレンタルサーバや DNS アウトソーシングなどのサービスで顧客のドメイン名（ゾーン）を収容するための「権威 DNS サーバ(DNS コンテンツサーバ)」と、顧客のサーバなどに名前検索サービスを提供するための「キャッシュ DNS サーバ」の提供を行っています。
DNS(Domain Name System)は、インターネットの重要な基盤技術の一つで、全世界のネームサーバが連携し、ドメイン名と IP アドレスの対応付けを行っていますが、これらが抱えるセキュリティのリスク/課題/問題など潜在的なものを含め幾つかあります。

･セキュリティに係るトピック
- DoS(Denial of Service)、DDoS(Distributed DoS)のサーバ攻撃への悪用
- DNS ポイズニングやドメイン名の引っ越しが妨げられるなどの危険性
- キャッシュ DNS サーバ利用者のアクセス先の漏洩
- 運用によってはドメインハイジャックの恐れ
- 不適切な登録、設定による脅威

･主なセキュリティ対策
次の対策により DNS サーバの安全性/安定性を高めることができます。

- 権威 DNS サーバとキャッシュ DNS サーバの分離
  : 権威 DNS サーバと、キャッシュ DNS サーバを同一のサーバで兼用している場合、DNS ポイズニングや、ドメイン名の引っ越しが妨げられるなどの危険性が低くなります。
  : DNS Amp 攻撃(DDoS 攻撃の一種)、DNS ポイズニングのリスクの軽減
- 定期的な脆弱性、仕様変更、実装上の不具合、など確認
  : 特定の脆弱性を利用した DoS(Denial of Service)攻撃、ハイジャック、DoS/DDoS(Distributed DoS)攻撃に悪用されることが少なくなります。
- 注意喚起などのアナウンスの確認
  : 各関係機関、コミュニティなどからの最新情報とソフトウェアップデート情報などの取得することで、最新情報が得られることで各種対策が可能となりリスクが低減します。

・更なるセキュリティ対策

多くの DNS には、DNS のセキュリティを向上させる為の拡張機能として、DNS 応答の偽造を防止する「DNSSEC」が実装されています。これは、応答を送信する DNS サーバが秘密鍵を使って応答に署名し、受信する側が公開鍵で検証することで、正しい DNS サーバからの回答を証明します。また、単に鍵と署名を受け取っただけではその内容の正当性を判断できないことから、DNSSEC　では DNS の階層構造に対応した形で著名で用いる鍵の正当性を証明し「信頼の連鎖」と呼ばれる仕組みにより担保しています。

これにより、DNS キャッシュポイズニングのような DNS 応答のなりすまし攻撃、また、この攻撃を飛躍的に高める方法であるカミンスキー型攻撃からの防止するために用いられています。

しかし、DNSSEC で用いる著名と鍵を長期間使用することによるセキュリティ・リスクが生じる可能性もあることから、セキュリティを高めるためにも、これらの定期的な更新が必要となります。また、定期的に更新することで、署名の有効期限切れによる DNSSEC 検証の失敗を防ぐことが出来ます。

参照：

・日本レジストリサービス
http://jprs.jp

・日本レジストリサービス DNSSEC とは
http://jprs.jp/dnssec/doc/dnssec.pdf

・DNSSEC ジャパン
http://dnssec.jp/

６－３－３．データセンターネットワークのセキュリティ対策で考慮すべき事項

(1)RTBH (Remote Triggered Black Hole filtering)

RTBH とは、Dos/DDos 攻撃を受けている際に攻撃トラフィックをネットワークの入り口で破棄する技術です。
昨今の Dos/DDos 攻撃は 10Gbps 以上といった大規模な攻撃も散見されており、網内および上位 ISP との間の回線が輻輳する懸念もあります。そのような攻撃に対しネットワークの入り口で攻撃トラフィックを破棄できる RTBH は回線輻輳を免れるための有効な手段となります。
RTBH の技術としては、BGP と Null ルーティングを利用します。攻撃対象となっている IP アドレスに RTBH 用の community を付与して網内に BGP で広報し、ネットワークの入り口のルータで Null ルーティングする手法です。なお、特定の機器ベンダに依存した技術ではないため、マルチベンダ環境での利用が可能です。
利用方法としては、自社ネットワークで RTBH を実装する場合と、上位 ISP の RTBH を利用する場合の 2 パターンが考えられます。

①自社 AS で RTBH を導入する

自社ネットワークの入り口のルータで攻撃トラフィックを破棄することができます。一方で大規模な攻撃に襲われた際に上位 ISP との回線が輻輳する恐れがあります。

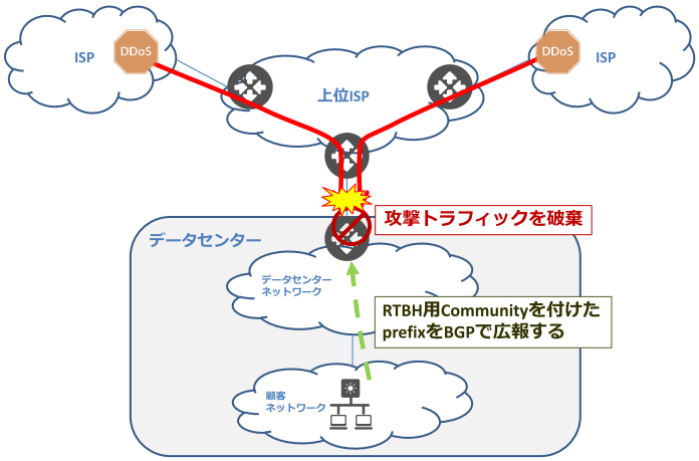


図 6g:自社 AS で RTBH を導入

②上位 ISP の RTBH を利用する

上位 ISP ネットワークの入り口で攻撃トラフィックを破棄してくれます。そのため、大規模な攻撃に襲われた際にも上位 ISP との間の回線が輻輳することを免れることができます。

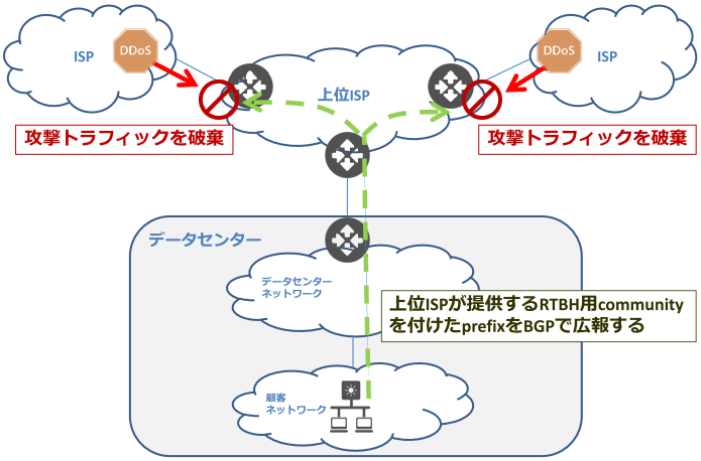


図 6h:上位 ISP の RTBH を利用

利用方法などは上位 ISP にお問い合わせ下さい。

(2)DNS Amp 攻撃への対策

①オープンリゾルバへの対策

不特定多数の IP アドレスからの DNS 要求に対して応答を返さないようにします。

②IP スプーフィングへの対策

送信元アドレスの詐称を防ぎます。

参照：

・日本ネットワークインフォメーションセンター

https://www.nic.ad.jp/ja/dns/openresolver/

７．用語集

エイリアンクロストーク：隣り合ったケーブル(Twisted Pair ケーブル)の間で伝わるノイズ。

CoreSW：Core Switch、このスイッチには主に２つの役目が有り、一つ目はそれぞれのサービスセグメントを集約する事であり、二つ目は GWR からのインターネットトラヒックを各サービスセグメントへ分ける事である。事業者によって複数 DC が有る場合は多拠点間通信を行う為に接続する場合もある。

CPE：Customer Premises Edge、加入者宅・施設に設置される通信機器のこと。「顧客構内設備」「カスタマー構内設備」などと訳されることもある。

GWR：Gateway Router、インターネットと接続する為のルータ(ルーティング機器)であり、AS 番号を取得している事業者であれば BGP-4＋プロトコルを利用して Transit 接続、あるいは合意した事業者と Peering 接続をしトラフィック交換を行うものである。

MMF:Multi Mode (optical) Fiber、マルチモード・光ファイバー、光が多くのモードに分散して伝送されるケーブル。シングルモード型と比較して、コア径が太く曲げに強い、光ファイバー同士の接続や光ファイバーと機器との接続が比較的容易であるという特長がある。

Managed Service:DNS や NTP Server などの付帯サービス群を指し、データセンターに置けるネットワークの接続性を支える上で重要なサービスとなる故、Layer3 以上のシステム群ではあるが高品質な運用が求められる。

MPLS:Multi-Protocol Label Switching、フレームやパケットの前方にラベルと呼ばれる識別子を付加して転送を行うことにより、通信の高速化や機能の付加を図る技術。

OSS :Operation Support System、サービス継続や品質管理といった観点から商用ネットワークと同等に重要なシステムとなる。

SMF: Single-Mode (optical) Fiber、シングルモード・光ファイバー、光が単一のモードで伝送されるケーブル。遠距離通信用のガラス製光ファイバーは

STP:Spanning Tree Protocol、複数の機器を接続した場合に起こる L2 ループへの対策として、一部のポートをブロック状態（未使用の状態）にしてしまうプロトコル。

TOR:Top of Rack、従来はサーバだけのラックとサーバからの通信を束ねる通信機器だけのラック構成が多くみられ、これを End of Row と呼んでいた。また、サーバからの通信を同じラック内に設置された SW で集約するものを Top of Rack という。とりわけ最近ではイーサネットファブリック技術等によりこの Top of Rack の SW と集約 SW を仮想的に接続し一体型オペレーションが可能な機器も登場している。

UTP:Unshield Twisted Pair、シールドが施されていないツイスト・ペア・ケーブル。

●改版履歴

版数	発行日	改訂履歴
第 1 版	2012 年 11 月 13 日	日本データセンター協会内で公開
第 2 版	2014 年 1 月 6 日	全体記載見直し 第 6 章に「データセンターネットワーク のセキュリティ対策で考慮すべき事項」を追補

日本データセンター協会　ネットワークワーキンググループ
データセンターネットワークリファレンスガイド執筆協力者

リーダ	西牧　哲也	（ヤフー株式会社）
サブリーダ	泓　宏優	（日本電気株式会社）
メンバ	梅田　聡	（株式会社 IDC フロンティア）
	太田　有彦	（株式会社野村総合研究所）
	大塚　健一郎	（住友電気工業株式会社）
	小原　篤人	（日商エレクトロニクス株式会社）
	川崎　貴裕	（デル株式会社）
	高木　恵一	（デル株式会社）
	剣持 良太	（パンドウィットコーポレーション）
	白井 謙良	（ソフトバンクテレコム株式会社）
	花山 寛	（ネットワンシステムズ株式会社）
	林　眞樹	（株式会社 IDC フロンティア）
	福田 克	（日商エレクトロニクス株式会社）
	福田　知夫	（日本電気株式会社）
	福智 道一	（BBIX 株式会社）
	干野　義明	（日本電気株式会社）
	松本　拓也	（ヤフー株式会社）
事務局	高橋　衛	（株式会社三菱総合研究所）

データセンターネットワークリファレンスガイド

2012 年 11 月 13 日発行（初版）
2014 年 1 月 6 日(第 2 版)

NPO 法人　日本データセンター協会
http://www.jdcc.or.jp/

お問い合わせ　info@jdcc.or.jp