シリーズ

シリーズ「電子政府を支える情報通信基盤技術」第９回

IDCのアーキテクチャと電子政府

㈱KDDI研究所所長　浅見　徹

はじめに

企業向け通信サービスの黎明期から存在するサービスに、ハウジングサービスがある。これは、企業の通信設備や情報システムの一部もしくは全部をキャリアの局舎に収容して運用を代行することに端を発している。データセンタ（Internet Data Center＝IDC）は、キャリアのビジネス顧客向けのハウジングサービスから起こったサービスであり、換言すればインターネットのサーバ収容の観点からハウジングサービスを再構成したものとも言うことができる。

IDCを実現する技術は、現状ではVRRP（Virtual Router Redundancy Protocol、RFC2338）等のごく一部の技術を除いてルータやサーバ等のベンダ依存性が強く、異なったベンダ技術を用いたデータセンタを全世界規模で相互接続するのは困難である。このため、同一のルータやサーバベンダを用いた個々のデータセンタ事業者が、地理的に分散したデータセンタを設け、センタ間の負荷分散・耐障害対策サービスを提供しているのが現実である。

ここでは、データセンタの機能をFoundry Networks社の技術をベースに概観する。

１　データセンタへの要求条件

その発生から、一般的にIDCに要求される条件には、以下が考えられる。

⑴　１日24時間、年365日運用が可能であること

⑵　フリーアクセスフロアを持つこと

⑶　数日間設備を運用できるバッテリーバックアップ（発電装置）を持つこと

⑷　個別空調設備を持つこと

⑸　煙探知機、自動消火設備、モーションセンサ、ビデオカメラ等のセキュリティ機能が充実していること

⑹　種々の冗長構成（発電機、インターネット接続用通信回線、等々）を持つこと

⑺　大都市に近接し、IXと併設して運用されることが多いことから判るように、インターネットへの高速回線が確保されていること

さらに、実際にデータセンタをサービスとして運用していくには、以下の要求条件も必要になる。

・ミッションクリティカルなアプリケーションを実行可能であること

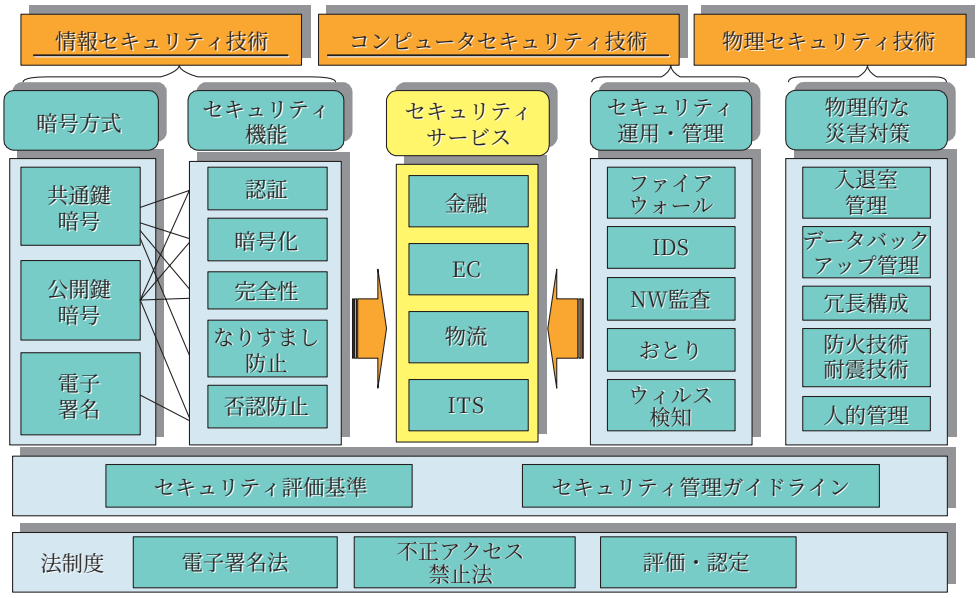
・セキュリティ対策がなされていること

・顧客の需要に応じて柔軟にトポロジーを変更できること

・機能に応じた価格設定ができること

ここで、セキュリティ面での考慮は、電子政府のための社会インフラとなりつつあるIDCの場合、非常に重要であり、物理セキュリティ、コンピュータセキュリティ、情報セキュリティの面か

図１　データセンタのセキュリティ



ら考えていかなければならない。図１にデータセンタのセキュリティの一般分類を示す。データセンタが考慮すべきセキュリティには、先ず、セキュリティ評価基準とセキュリティ管理ガイドラインに基づき、物理的災害対策を行う物理セキュリティがある。人的管理、入退室管理、防火・耐震、冗長構成、データバックアップなどがこの範疇である。また、セキュリティの運用・管理面で、ファイアーウォール、IDS（Intrusion　Detection System、侵入検知システム）から、ウィルス検知、おとりサーバの運用やネットワーク監査などのコンピュータセキュリティも、広義の意味でIDSのサービス内に含めることができる。

一方、情報セキュリティに関しては、基本的にデータセンタの顧客によるエンド・エンドの管理であり、通常はIDSのサービス外と考えることができる。

２　データセンタの一般的ネットワーク構造

現在の技術で一般的なデータセンターにおける設備構成を図示すると、図２に示す構造になる。センター内外の接続構成はかなり複雑になっており、このネットワークを簡易に運用する運用ツールの存在が不可欠である。

各レイヤの機能を以下に示す。

⑴　コアレイヤ（Core Layer）

・データセンタ内のIPネットワークをインターネットやIX（Internet Xchange point）に接続する

・要求条件：

・BGP4やOSPF等の標準経路制御プロトコルを安定に運用可能であること

・GbE（Gigabit　Ethernet）やPOS（Packet Over　SONET）等の高速インタフェースをWAN側に持っていること

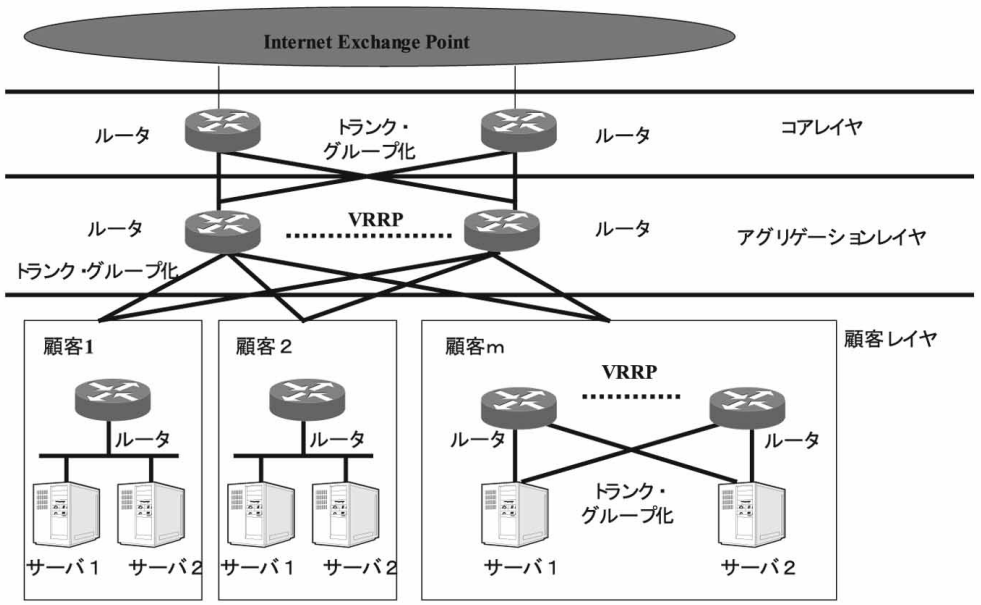
・高性能かつノンブロッキングなアーキテクチャを採用していること

・インターネットへの接続経路（回線）を複数持つこと

⑵　アグリゲーションレイヤ（Aggregation Layer）

・種々の顧客の機器を納めたケージを集約して

図２　データセンタの基本構造



収用できること。

・このレイヤの機能は、インターネットへの高速接続回線の有効利用と、タスクの負荷分散にある。前者では、例えば、１企業がT1（1.5Mbit/s）回線でインターネットやIXに繋がっているより、100企業がSTM-1（155 Mbit/s）の回線を共有しているほうが、統計多重効果があるので、１企業あたりのスループットは遥かに高速になる。また、回線費用は100倍にはならないので、１企業あたりが負担する回線費用はかえって安くなる利点がある。一方、タスクの負荷分散とは、ファイヤーウォール等セキュリティ関連処理の高速化等を含む各種ネットワーク・サービスの負荷分散を行うことを意味し、これにより、スケーラブルなソルーションを提供することができる。

・要求条件：

・多数のGbE経由で顧客を収用しトランク結合が可能であること

・ワイヤスピード（回線速度）でアクセス制御できること

・冗長構成による高い稼働率を保証できること

・ノンブロッキングアーキテクチャを採用していること

⑶　顧客レイヤ（Customer Layer）

・ホスティング・サービスやコロケーション・サービスを提供する機構があること

・要求条件：

・サーバのロードバランスのようなL4スイッチ機能があること

３　顧客収用形態

顧客収用形態は色々あり、以下では、具体例をベースに説明する。

⑴　コアとアグリゲーション部分を簡易化し、高速インターネットアクセス環境を安価に提供する形態

ここで、サービス形態はシングル接続とデュア

図３　高速インターネットアクセス環境自体を提供

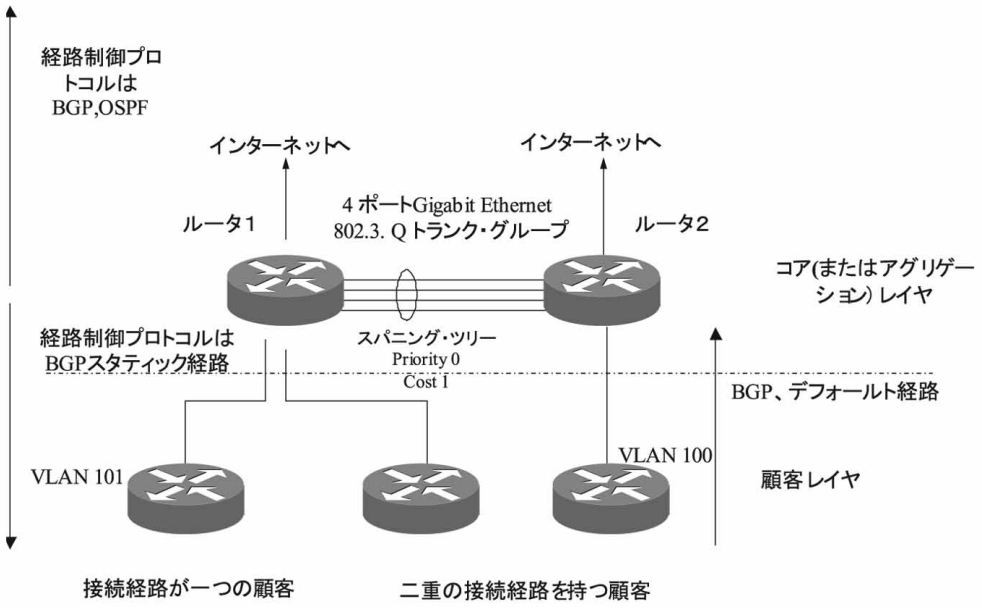
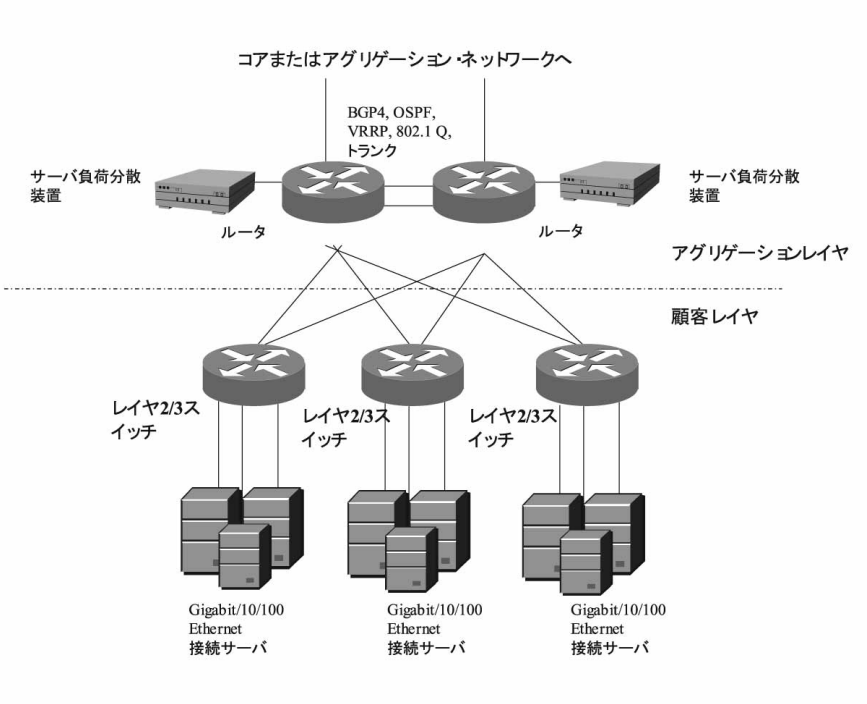


図４　フル冗長構成の顧客収用形態



ル接続があり、対障害特性から考えて当然デュアルが安定なサービス（付加価値）である。

図３では、インターネットに接続した２台のコアレイヤのルータをトランク結合し、どちらのインターネット接続回線が障害になっても、トランク経由で迂回させて接続が確保できるような冗長構成を採用している。顧客レイヤは、ルータ１台でコアレイヤと接続したシングル接続と２台の

ルータで接続したデュアル接続の二通りあり、前者は顧客レイヤのルータとコア・ルータ間の回線障害でサービス不良になるが、後者はどちらかの顧客レイヤのルータ接続回線が稼動していればサービスは維持できる利点がある。

⑵ フル冗長構成を採用した顧客の収容形態

顧客の規模により使用機器は異なるが、基本的トポロジーは図４と同形である。ここで、アグリゲーションレイヤは２台のルータと２台のサーバ負荷分散装置から構成されている。３台のレイヤ２/３スイッチは各々顧客レイヤのルータである。図３に対して、顧客ルータは２台のアグリゲーション・レイヤのルータどちらにも回線を持っていることから回線の冗長構成による稼働率の向上を図っている。２台のサーバ負荷分散装置は、ロードバランス等のアグリゲーション機能を担っているが、これも冗長構成によりサービス稼働率の向上を狙っている。

４ 機能別ネットワーク形態

4.1 サーバのロードバランス機能について

ロードバランスは、図５に示すサーバ負荷分散装置のように、スケーラビリティを持っている必要がある。ここでは、異なったMACアドレス（Ethernet等が使っているアドレス）を持つ５台のサーバが、インターネット側のクライアントからは202.255.44.1をIPアドレスに持つ１台のサーバに見えるように設計されている。また、５台のサーバは、それぞれHTTP、FTP、DNS、Email、Video中の２つの機能を持ち、負荷状態によりメールサーバにもFTPサーバにもなれるように設計されていて次の条件を満たしている。

⑴ サーバ群に対し１つのIPアドレスを付与することにより、サーバ間の付加分散を図れること

⑵ 提供するサービスとそれを実現するサーバの関係は独立（あるサービスを実行するサーバが特定のものに限定されてはならない）にできること

⑶ サービス（少なくともHTTP、DNS、SMTP、POP3、LDAPv3、NNTP、IMAP4、FTP、TelNetやRadius）の稼動状況をモニタできること。

⑷ 種々の機能のサーバをミックスし、かつ各サーバの能力を最大限に利用できること

⑸ 上記のロードバランスをするサーバ負荷分散

図５ サーバ間の付加分散

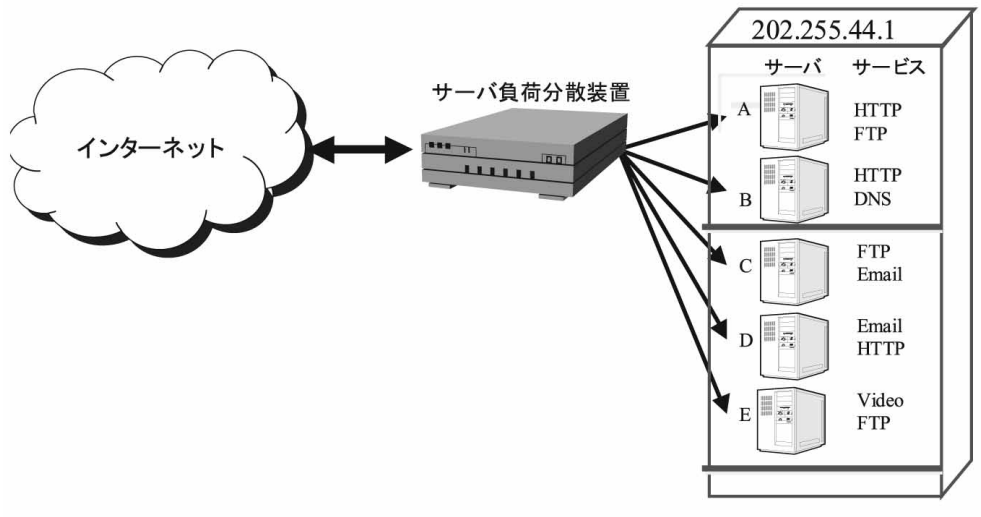


図６　フォールトトレラントなロードバランス装置

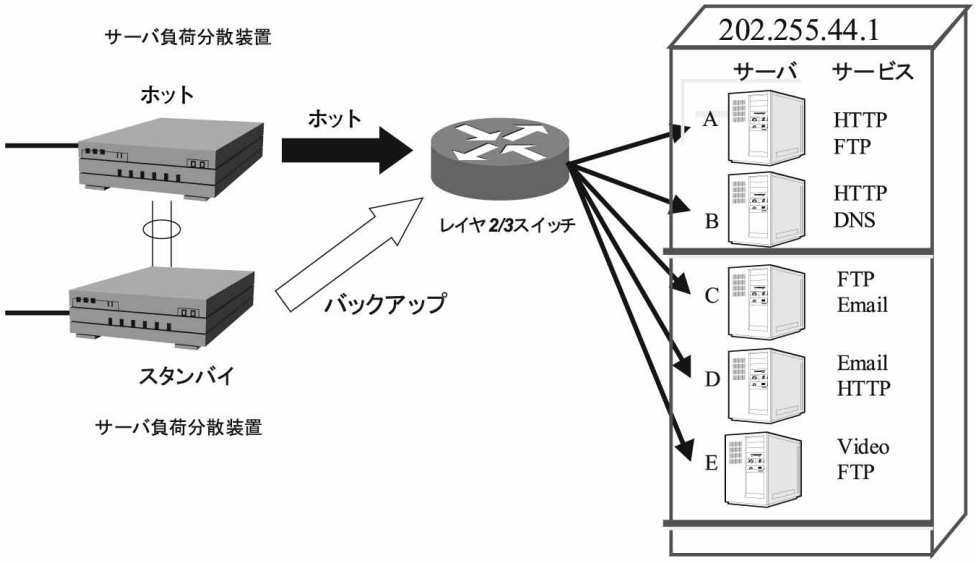
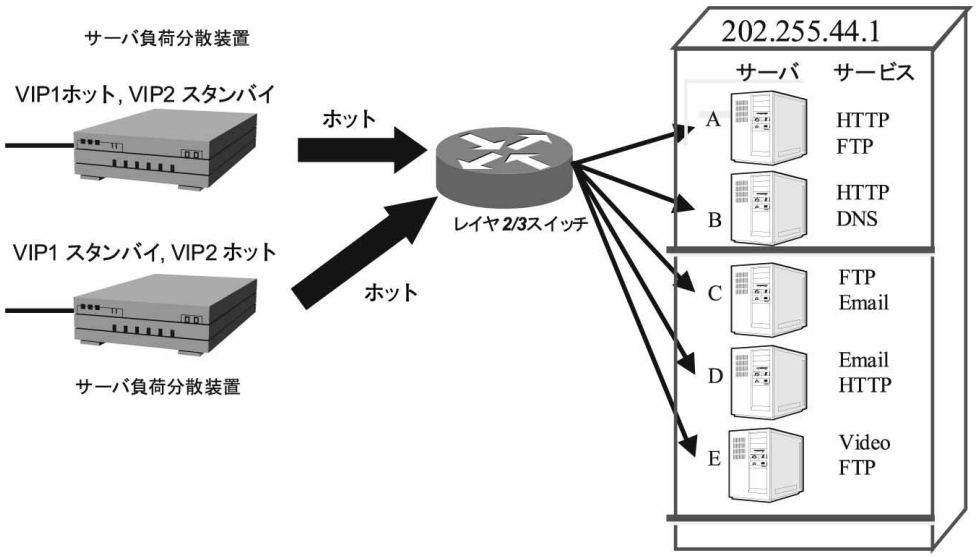


図７　ロードバランス処理が過負荷時の装置構成



装置自体も、フォールトトレラントでなければならず、図６に示すようなホット／スタンバイの冗長構成をとり、ホット／スタンバイ間で動作状況を相互モニタし、障害時に瞬時に切り替えられること。

⑹　上記のサーバ負荷分散装置は、ロードバランスの処理負荷が増加した場合には、図７に示すように、両方ともホット（アクティブ）になり、負荷を軽減できること

⑺　TCP Syn Attack Protection

データセンタに収容された各顧客サーバへは、サービス断を狙ってハッカーの攻撃がしかけられることを考慮する必要がある。これを防御するため、図８に示すように、以下の機能をもっている必要がある。

１）各サーバへのTCP Syn要求速度に上限を

図８　サーバのセキュリティ対策

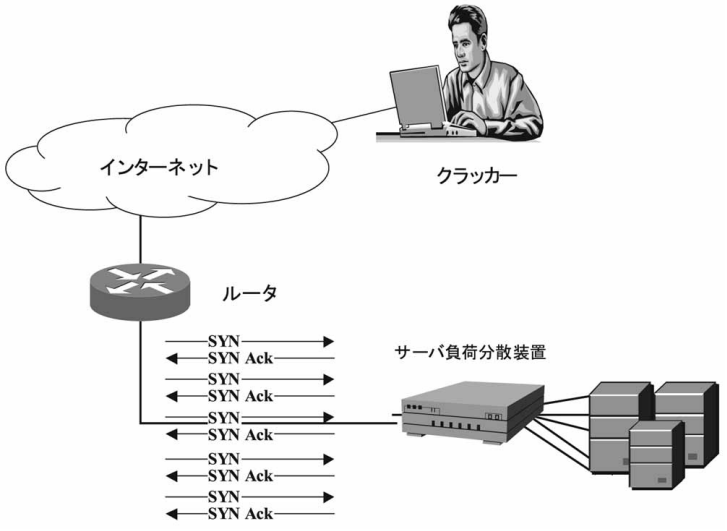
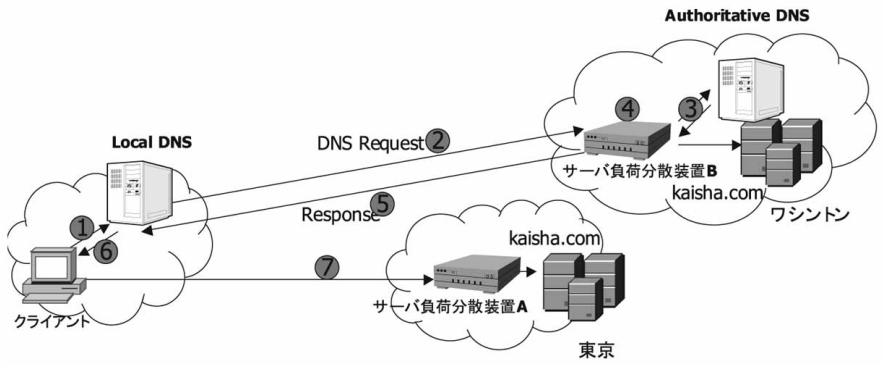


図９　地理的負荷分散



設けられること

2）最後のTCP不完了呼用に割り当てられたリソースを新規TCP呼用に割り当てること

3）サーバに割り当てられたリソースを開放するよう要求できること

4）悪質なソースIPアドレスからの接続は拒否できること

5）TCP Syn攻撃があったときにSNMPによる通知機能があること

⑻　サービス（ポート番号)、ソース（発信）IPアドレス、着信仮想IPアドレスの組み合わせによりアクセス制御ができること

⑼　地理的に離れたサーバ群をロードバランスできること（図９のように複数のデータセンタに同一ドメイン（ここではkaisha.com）のサーバが配置されているとき必要な機能）

1）地理的に離れたサーバ群をクライアントに対しては単一のサーバに見せ、最もネットワーク的に近いサーバを割り当てられること

2）サーバがクラッシュしたときはクライアントが最適の代替サーバにアクセスするようガイドできること（データセンタ自体が地震等の自然災害で機能しなくなったときに代替サーバを全世界に散らばったサーバ群から自動選択できなければならない）

⑽　クライアントに対しては単一のサーバに見せ、