平成２６年度 文部科学省

成長分野等における中核的専門人材養成の戦略的推進事業

実践クラウドセキュリティ

目次

1. クラウドコンピューティングとは
2. クラウドコンピューティングを支える技術
3. クラウドサービスにおける情報セキュリティ
4. クラウドサービスのセキュリティの要件
5. クラウドサービスのSLA、規約の解釈

1.「クラウドコンピューティング」とは

「クラウドコンピューティング」とは？

「クラウドコンピューティング」とは？

「クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものである。このクラウドモデルは5つの基本的な特徴と3つのサービスモデル、および4つの実装モデルによって構成される」

～NIST SP800-145「NISTによるクラウドコンピューティングの定義」

5つの基本的な特徴(1)

オンデマンドセルフサービス(On-demand self-service)	ユーザは、各サービスの提供者と直接やりとりすることなく、必要に応じ、自動的に、サーバーの稼働時間やネットワークストレージのようなコンピューティング能力を一方的に設定できる。
幅広いネットワークアクセス(Broad network access)	コンピューティング能力は、ネットワークを通じて利用可能で、標準的な仕組みで接続可能であり、そのことにより、様々なシンおよびシッククライアントプラットフォーム（例えばモバイルフォン、タブレット、ラップトップコンピュータ、ワークステーション）からの利用を可能とする。
リソースの共用(Resource pooling)	サービスの提供者のコンピューティングリソースは集積され、複数のユーザにマルチテナントモデルを利用して提供される。様々な物理的・仮想的リソースは、ユーザの需要に応じてダイナミックに割り当てられたり再割り当てされたりする。物理的な所在場所に制約されないという考え方で、ユーザは一般的に、提供されるリソースの正確な所在地を知ったりコントロールしたりできないが、場合によってはより抽象的なレベル（例：国、州、データセンタ）で特定可能である。リソースの例としては、ストレージ、処理能力、メモリ、およびネットワーク帯域が挙げられる。

5つの基本的な特徴(1)

スピーディな拡張性(Rapid elasticity)	コンピューティング能力は、伸縮自在に、場合によっては自動で割当ておよび提供が可能で、需要に応じて即座にスケールアウト／スケールインできる。ユーザにとっては、多くの場合、割当てのために利用可能な能力は無尽蔵で、いつでもどんな量でも調達可能のように見える。
サービスが計測可能であること (Measured Service)	クラウドシステムは、計測能力を利用して、サービスの種類（ストレージ、処理能力、帯域、実利用中のユーザアカウント数）に適した管理レベルでリソースの利用をコントロールし最適化する。リソースの利用状況はモニタされ、コントロールされ、報告される。それにより、サービスの利用結果がユーザにもサービス提供者にも明示できる。

サービスモデルの違い

サービスによって、提供される機能が異なる。
そこで、利用者側の責任やるべきことも異なる。

実行環境のセキュリティ確保はユーザーの責任

3つのサービスモデル(1)

インフラストラクチャ・アズ・ア・サービス（サービスの形で提供されるインフラストラクチャ） IaaS(Infrastructure as a Service)	利用者に提供される機能は、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースを配置することであり、そこで、ユーザはオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し走らせることができる。ユーザは基盤にあるインフラストラクチャを管理したりコントロールしたりすることはないが、オペレーティングシステム、ストレージ、実装されたアプリケーションに対するコントロール権を持ち、場合によっては特定のネットワークコンポーネント機器（例えばホストファイアウォール）についての限定的なコントロール権を持つ。

3つのサービスモデル(2)

プラットフォーム・アズ・ア・サービス（サービスの形で提供されるプラットフォーム）PaaS(Platform as a Service)	利用者に提供される機能は、クラウドのインフラストラクチャ上にユーザが開発したまたは購入したアプリケーションを実装することであり、そのアプリケーションはプロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを用いて生み出されたものである。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、管理したりコントロールしたりすることはない。一方ユーザは自分が実装したアプリケーションと、場合によってはそのアプリケーションをホストする環境の設定についてコントロール権を持つ。

3つのサービスモデル(3)

ソフトウェア・アズ・ア・サービス（サービスの形で提供されるソフトウェア） SaaS(Software as a Service)	利用者に提供される機能は、クラウドのインフラストラクチャ上で稼動しているプロバイダ由来のアプリケーションである。アプリケーションには、クライアントの様々な装置から、ウェブブラウザのようなシンクライアント型インターフェイス（例えばウェブメール）、またはプログラムインターフェイスのいずれかを通じてアクセスする。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、各アプリケーション機能ですら、管理したりコントロールしたりすることはない。ただし、ユーザに固有のアプリケーションの構成の設定はその例外となろう。

【補足】その他の「○○ as a Service」

AaaS – Architecture as a Service
BaaS – Backend as a Service
DaaS – Desktop as a Service
EaaS – Ethernet as a Service
HaaS – Hardware as a Service
LaaS – Lending as a Service
MaaS – Mashups as a Service
VaaS – Voice as a Service

XaaS – Everything as a Service

4つの実装モデル(1)

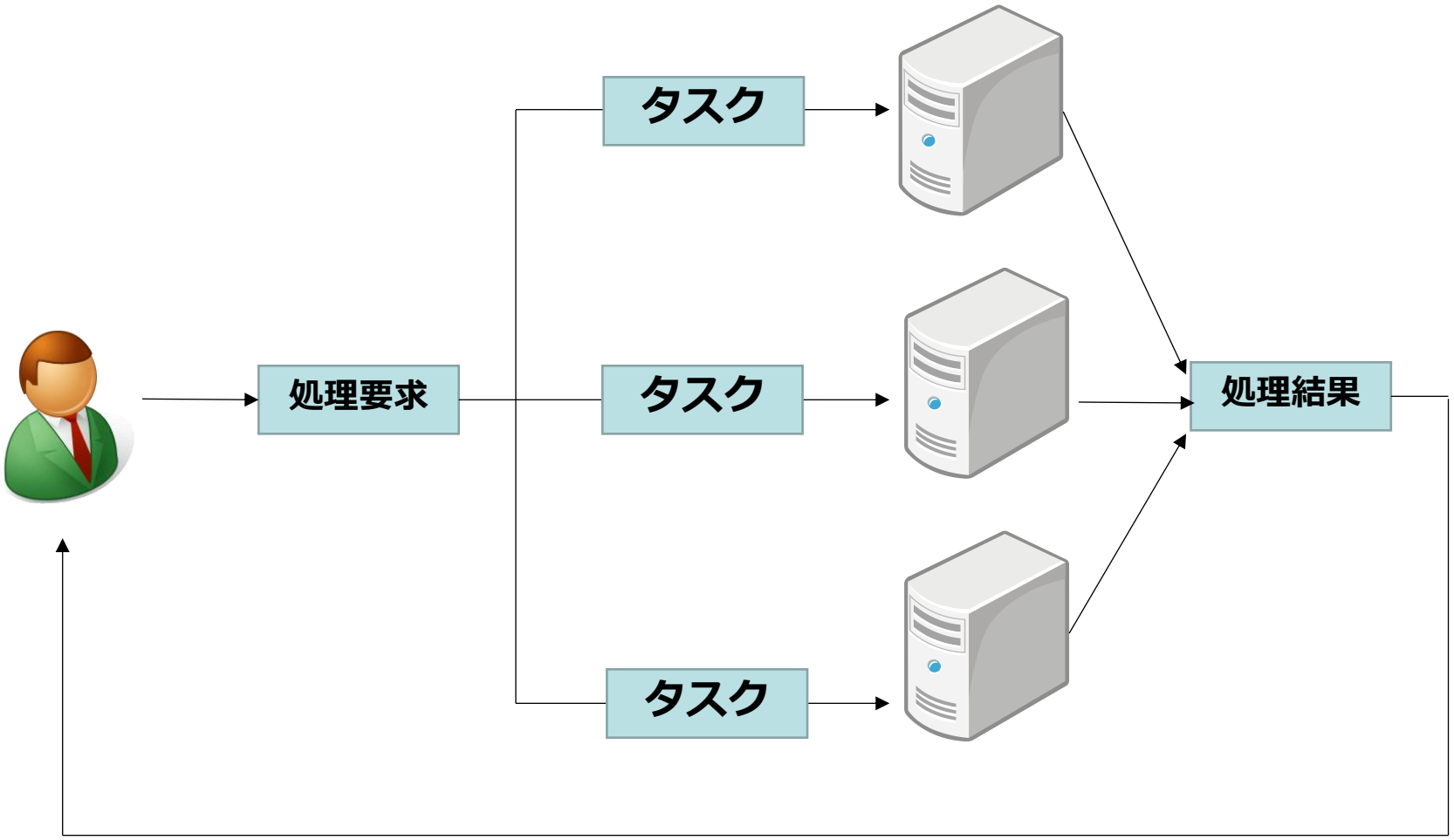
プライベートクラウド (Private cloud)	クラウドのインフラストラクチャは、複数の利用者（例：事業組織）から成る単一の組織の専用使用のために提供される。その所有、管理、および運用は、その組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。
コミュニティクラウド (Community cloud)	クラウドのインフラストラクチャは共通の関心事（例えば任務、セキュリティの必要、ポリシー、法令順守に関わる考慮事項）を持つ、複数の組織からなる成る特定の利用者の共同体の専用使用のために提供される。その所有、管理、および運用は、共同体内の１つまたは複数の組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。

4つの実装モデル(2)

パブリッククラウド(Public cloud)	クラウドのインフラストラクチャは広く一般の自由な利用に向けて提供される。その所有、管理、および運用は、企業組織、学術機関、または政府機関、もしくはそれらの組み合わせにより行われ、存在場所としてはそのクラウドプロバイダの施設内となる。
ハイブリッドクラウド (Hybrid cloud)	クラウドのインフラストラクチャは二つ以上の異なるクラウドインフラストラクチャ（プライベート、コミュニティまたはパブリック）の組み合わせである。各クラウドは独立の存在であるが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移動可能性を実現している（例えばクラウド間のロードバランスのためのクラウドバースト）。 ※ クラウドバースト：（訳注）burstとは爆発とかはじけるという意味であり、「クラウドバースト」はクラウド間をまたがる移動や連携を意味する概念として使われるケースが多い。定義の確定した用語ではないと考えられる。

2. クラウドコンピューティングを支える技術

分散処理

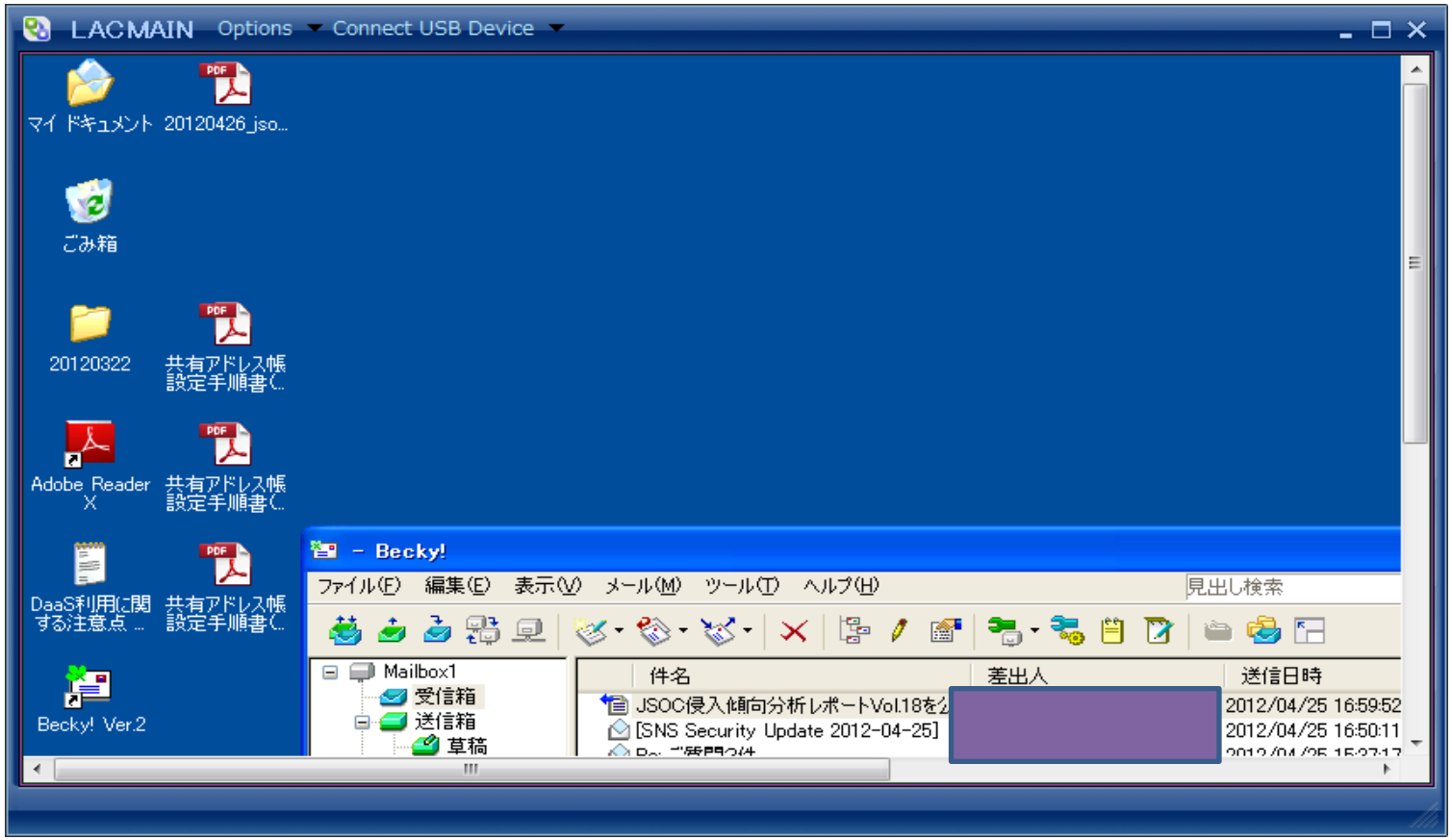


QoS

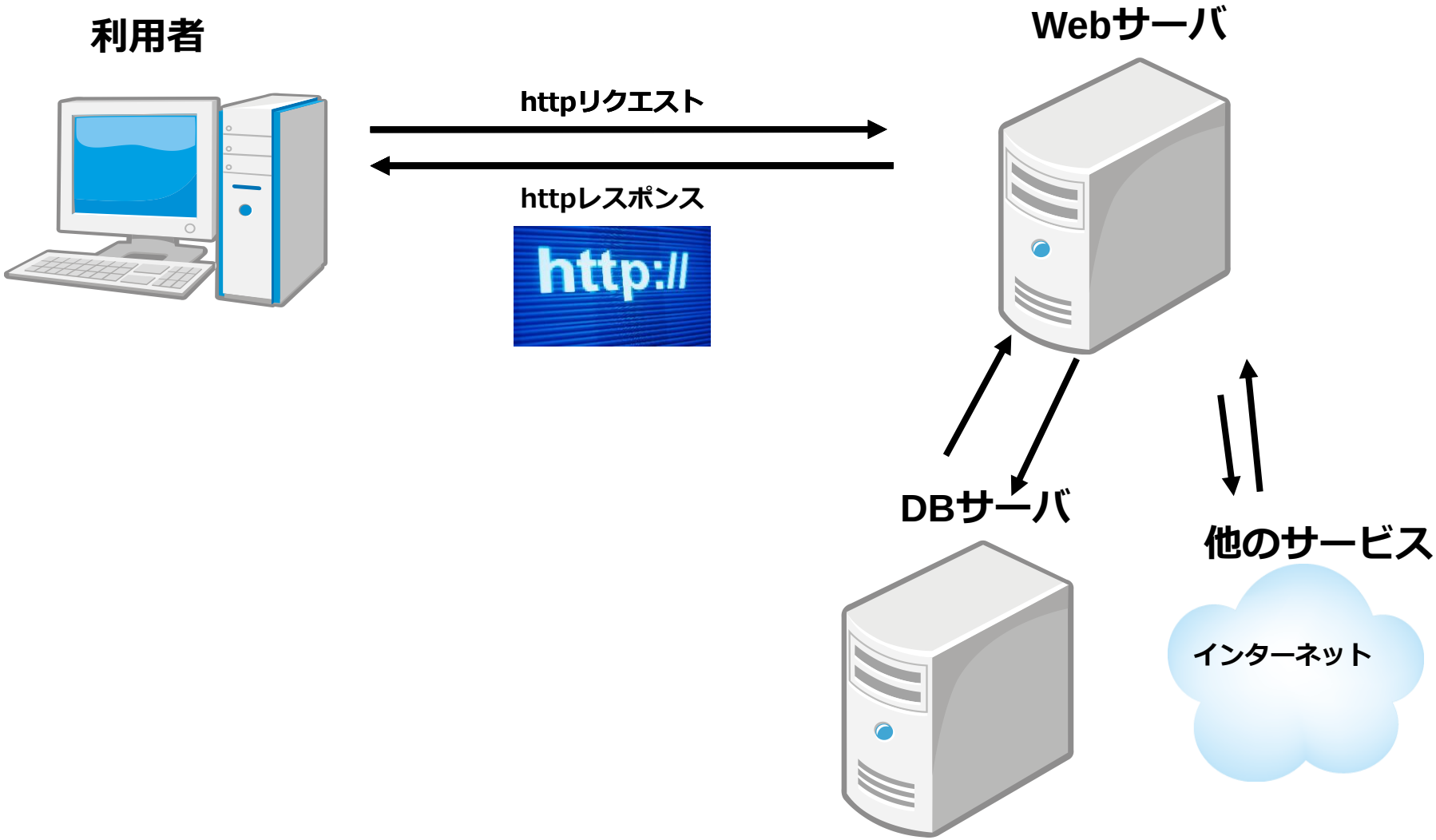
- 遅延が許容できないトラフィックや優先度の高いトラフィックを優先的に処理し、パケットの損失、サービスの低下などの影響を緩和する技術。

- 優先制御：パケットの優先度に従い、優先度の高いパケットを先に伝送する。
- 帯域制御：パケットの種類ごとに、帯域幅を制限管理する。

エミュレータ

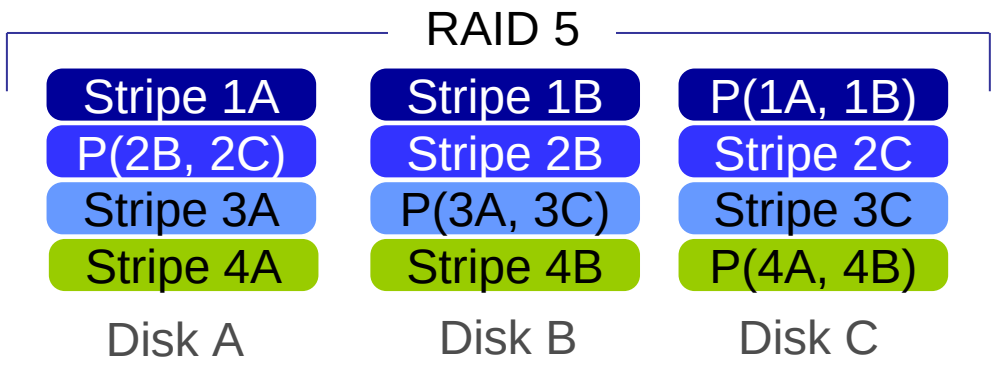

LACMAIN
Options
Connect USB Device
マイ ドキュメント
20120426_jso...
ごみ箱
20120322
共有アドレス帳設定手順書(...
Adobe Reader X
共有アドレス帳設定手順書(...
DaaS利用に関する注意点 ...
共有アドレス帳設定手順書(...
Becky! Ver.2
Becky!
ファイル(F) 編集(E) 表示(V) メール(M) ツール(T) ヘルプ(H)
見出し検索
Mailbox1
受信箱
送信箱
草稿
件名
差出人
送信日時
JSOC侵入傾向分析レポートVol.18を
2012/04/25 16:59:52
[SNS Security Update 2012-04-25]
2012/04/25 16:50:11

Webアプリケーション



RAID

RAID0	ストライピング。2台以上のディスクにデータを分散して格納
RAID1	ミラーリング。2台以上のディスクにデータを複写して格納。RAID0と比較すると冗長性があるが、使用するディスク容量は大きくなり、パフォーマンスは低くなる。
RAID5	パリティ情報を利用したブロック単位でのストライピング。RAID2/3/4ではできなかった並列処理を可能にしている。現在、もっとも一般的に利用されているRAIDの方式。
RAID6	2次元パリティ情報を利用したストライピング。RAID5では、ディスク2台同時のクラッシュがあった場合、データの再構成ができなかった。このRAID6では、パリティ情報を2台に分散して格納しているため、ディスク2台同時のクラッシュがあった場合でもデータの再構成が可能になっている。



モバイル通信

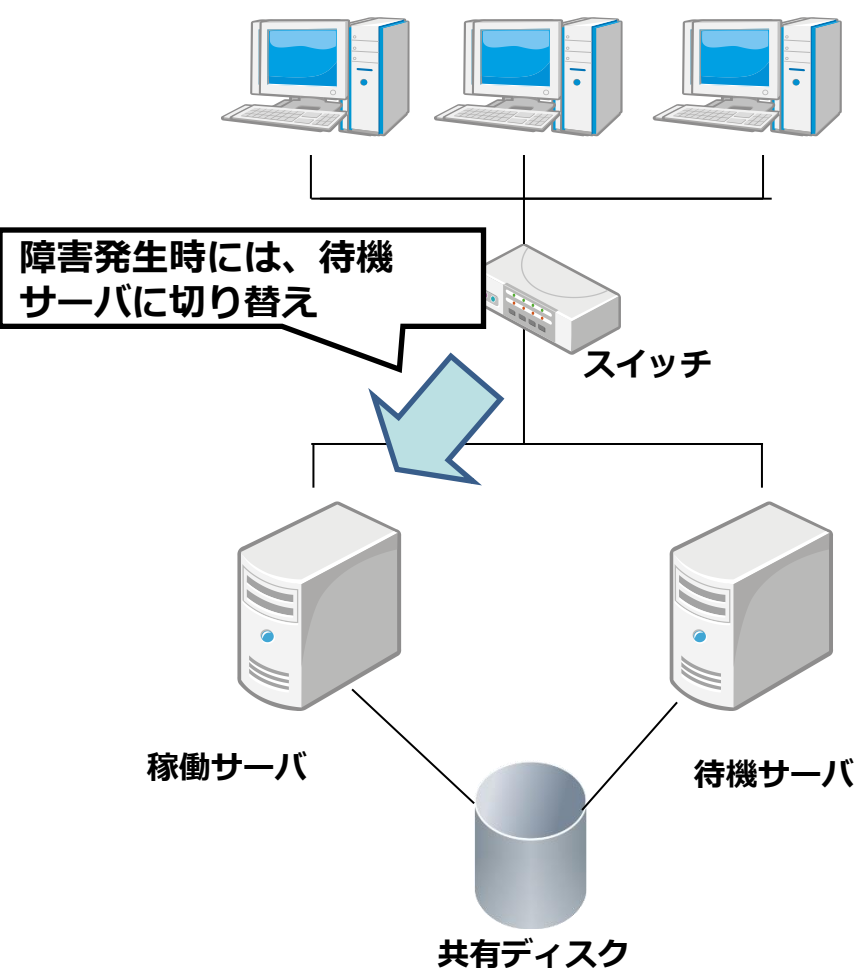
外出先など

クラウドサービス

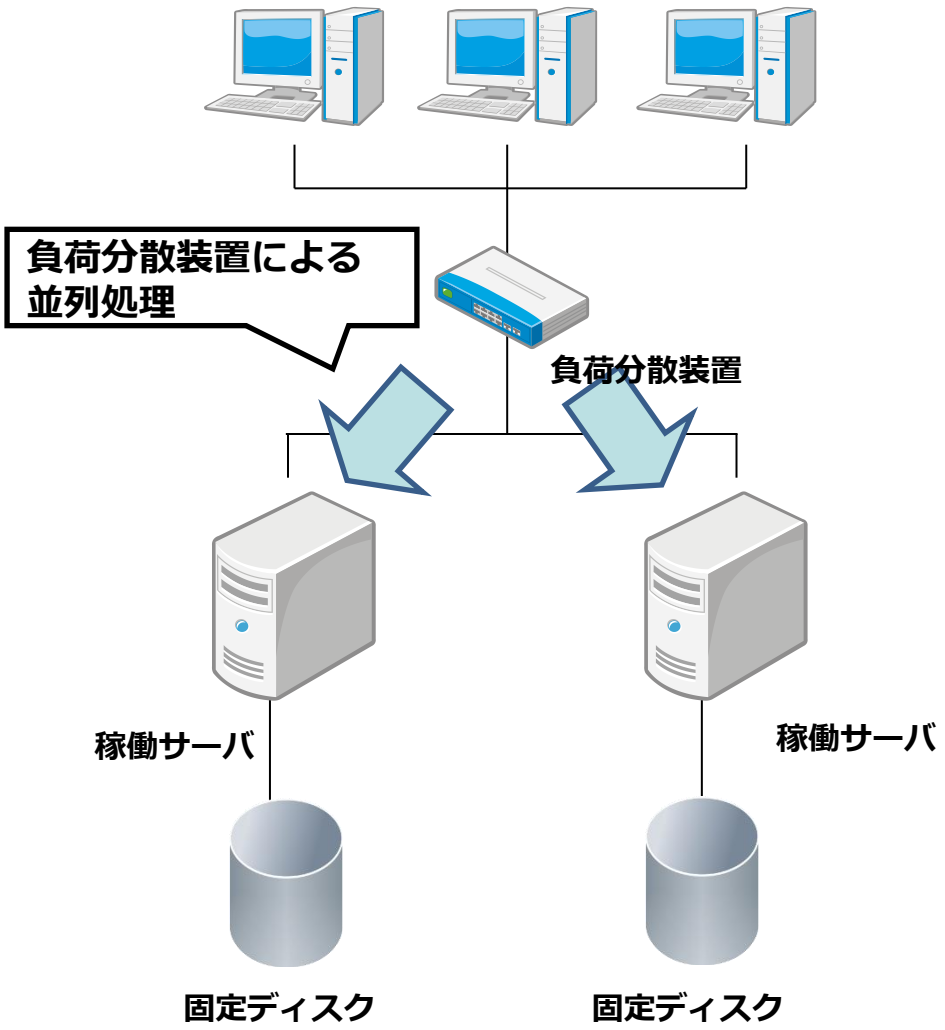
YouTube
USTREAM
Google
skype
YAHOO! JAPAN
EVERNOTE
Windows Live
twitter
Dropbox
facebook
LINE

クラスタリング

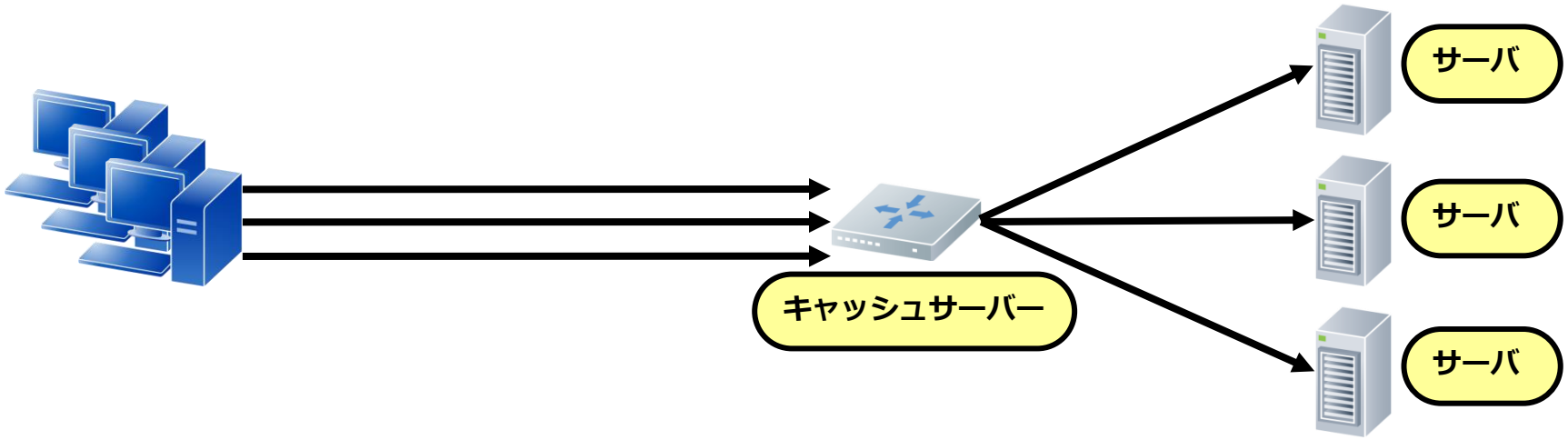
HAクラスタリング構成



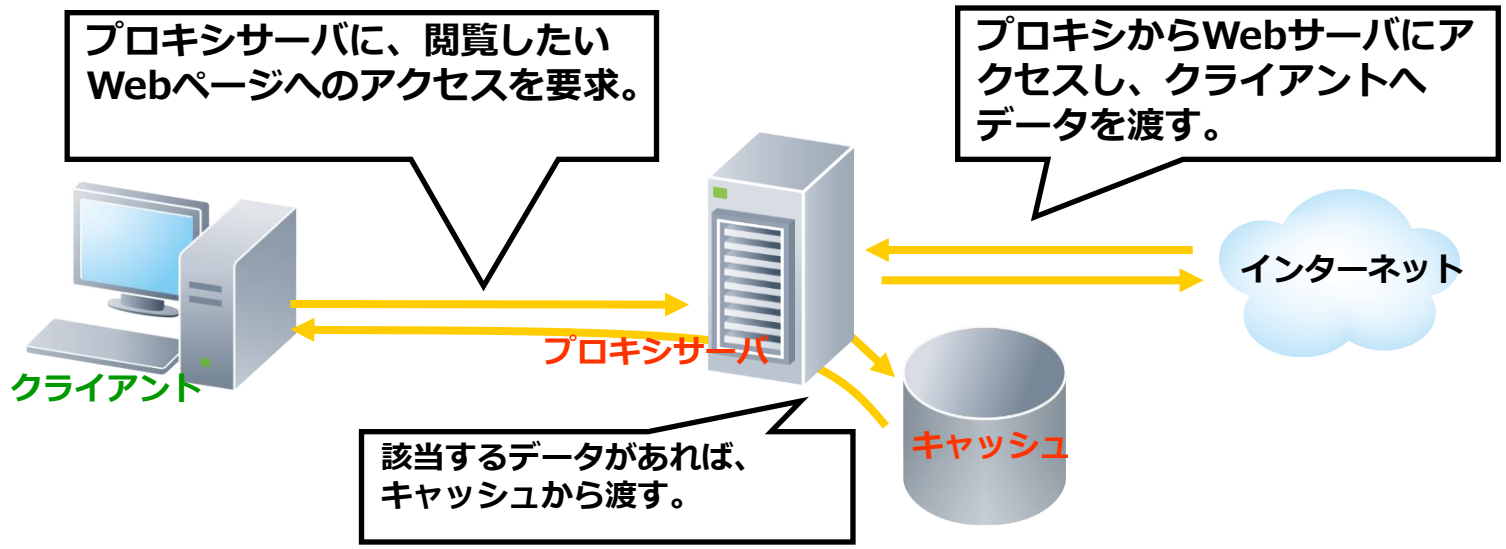
負荷分散クラスタリング構成



キャッシュサーバー



プロキシサーバー


プロキシサーバに、閲覧したい
Webページへのアクセスを要求。
プロキシからWebサーバにア
クセスし、クライアントへ
データを渡す。
インターネット
クライアント
プロキシサーバ
該当するデータがあれば、
キャッシュから渡す。
キャッシュ

仮想化技術

「仮想化」とは

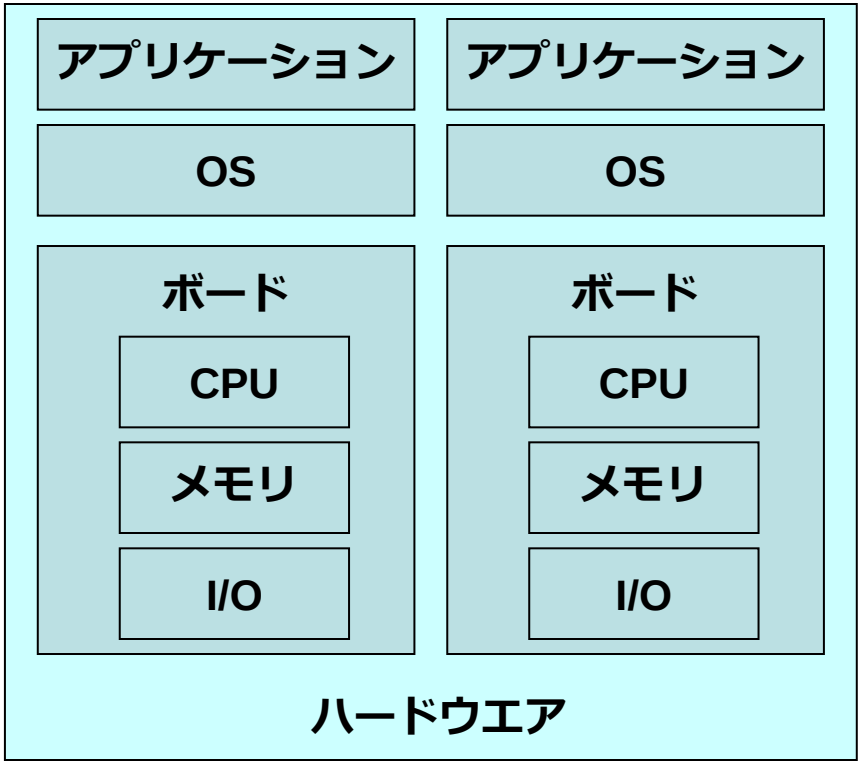
- 様々なリソースを抽象化する技術
- 物理的なコンピュータ上に、独立してOSやアプリケーションを稼動させる擬似的なコンピュータを構築する技術

仮想化のパターン

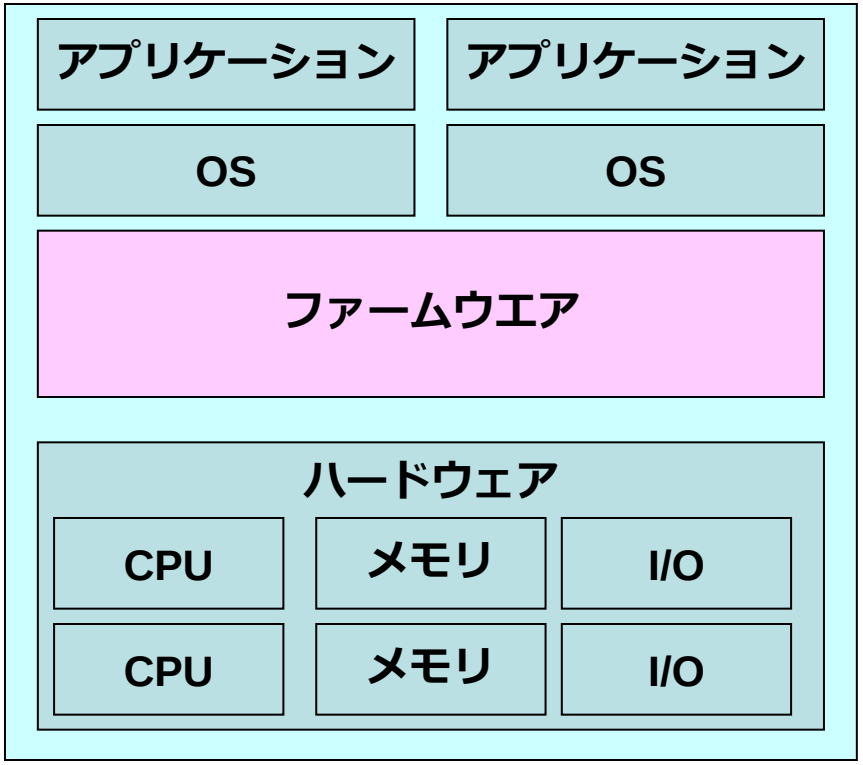
種類	特徴
資源の分割（パーテショニング）	1つの物理的資源を複数の論理的資源に分割して利用する。例としては、ハードディスクのパーテーション分割、サーバの仮想化、などがあります。
資源の統合（アグリゲーション）	複数の物理資源を1つの論理的資源として利用する。例としては、RAID、グリッドコンピューティング、などがあります。
資源の模倣（エミュレーション）	ある物理資源を別種の物理資源のように見せかける論理的資源として利用する。例としては、エミュレータ、Java Virtual Machine、などがあります。

サーバの仮想化（分割）

物理パーテショニング型

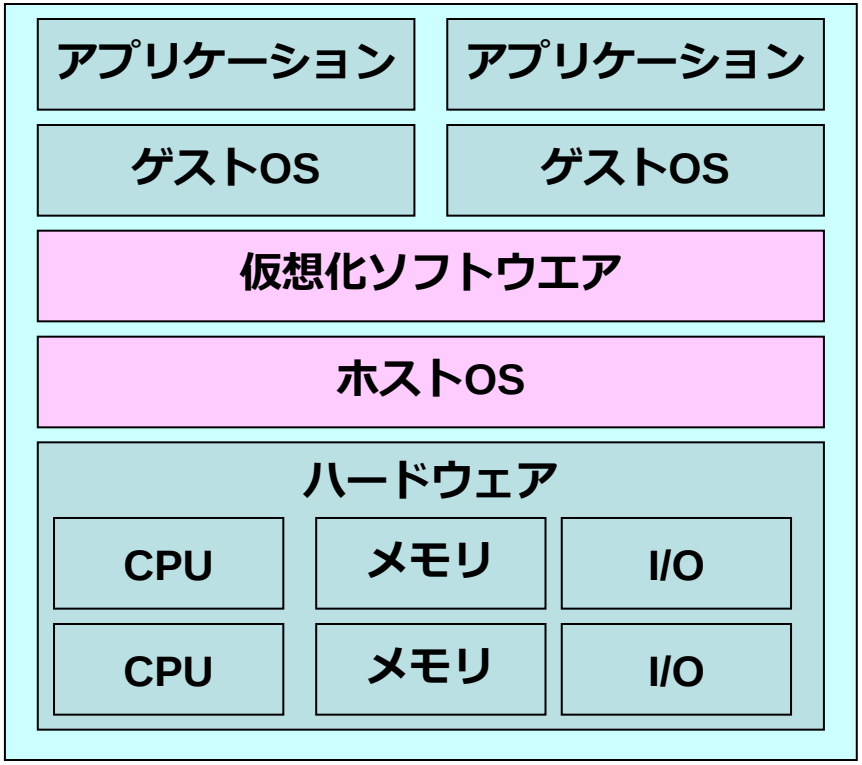


論理パーテショニング型

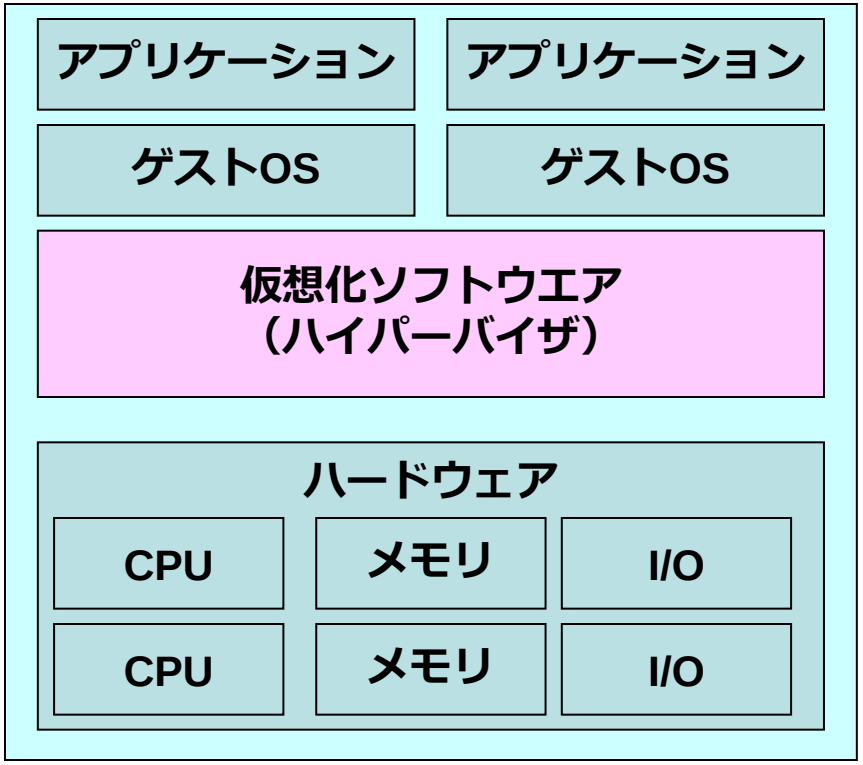


仮想マシン

ホストOS型



ハイパーバイザ型

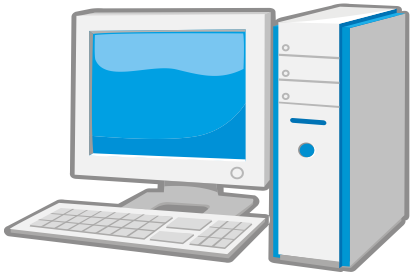


仮想マシン

- 仮想マシンの実体は単なるファイル群
- それゆえに、物理サーバーでは実現できなかった様々な運用が可能になる
  - サーバーのコピー、移動、スペックの変更など
- IaaSでサーバーを一台借りると、実際に行われているのはファイル(仮想サーバーの)のコピーと起動。人手は一切かかっていない

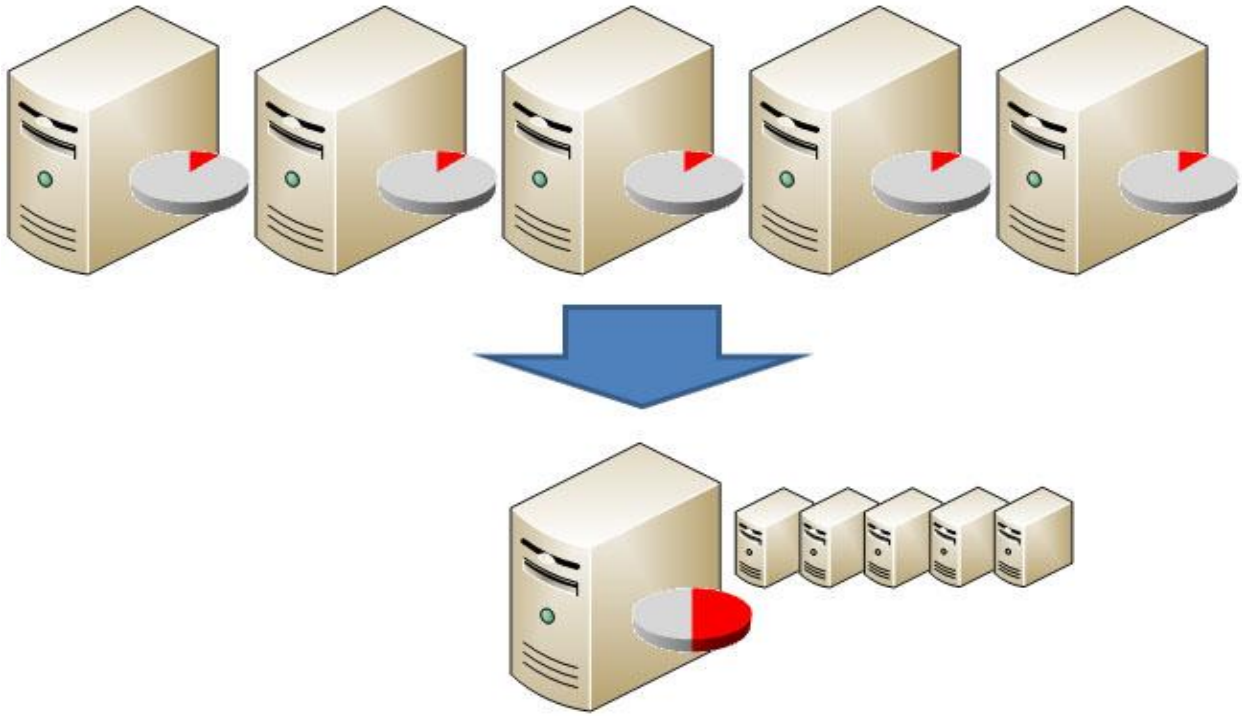
デスクトップの仮想化

利用者



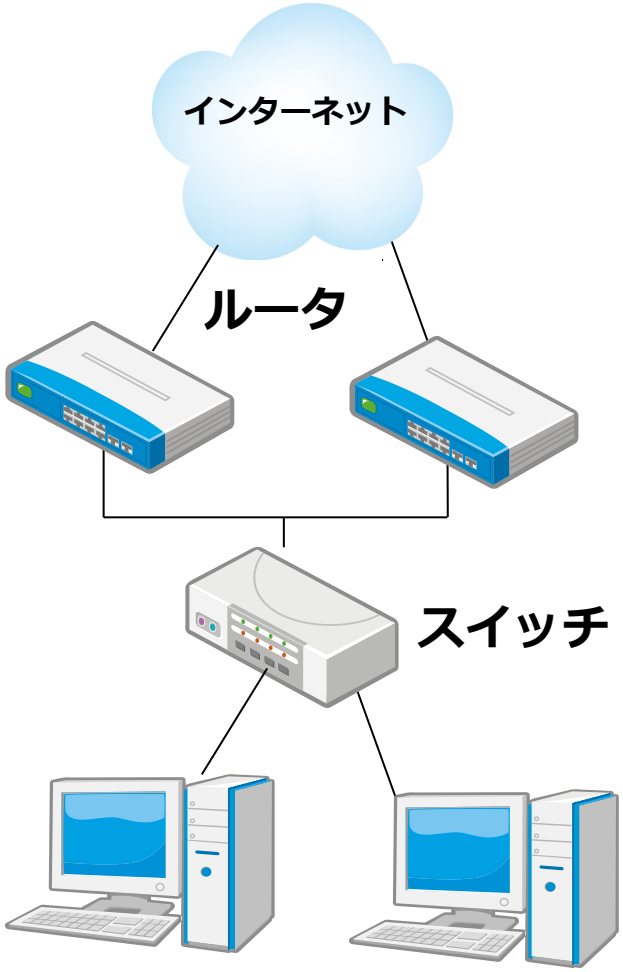
仮想マシン

ストレージの仮想化（統合）

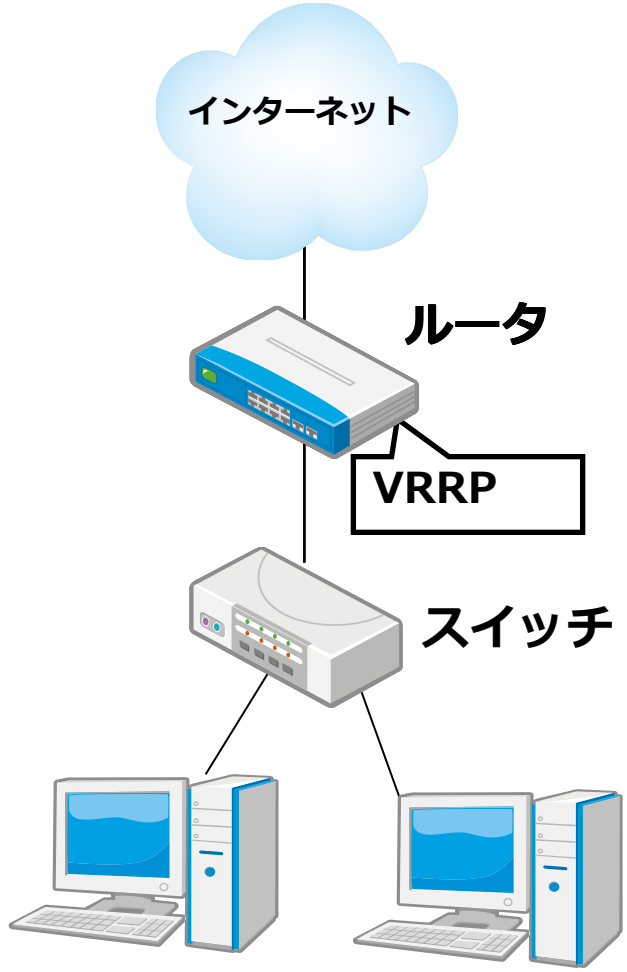


ルータの仮想化

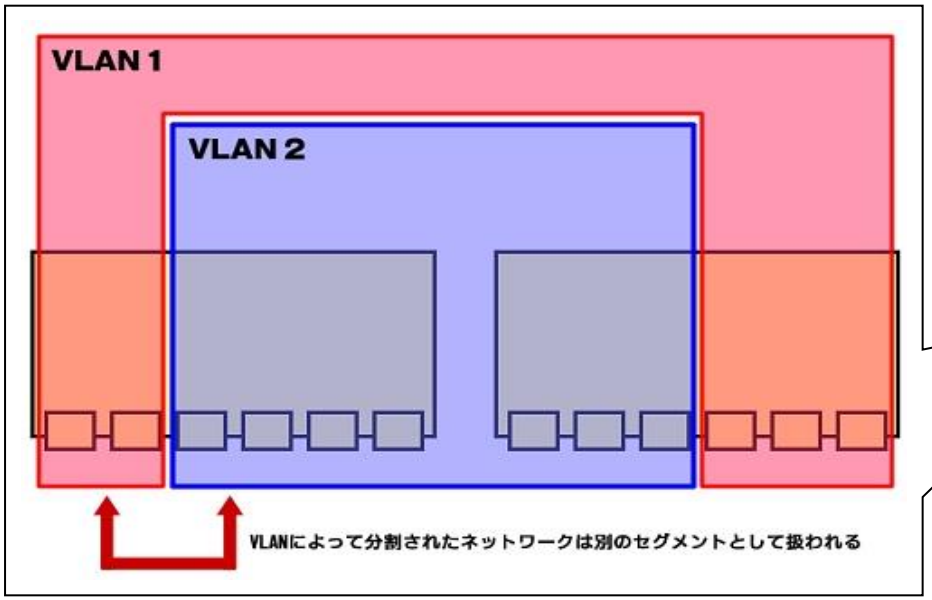
物理構成



論理構成

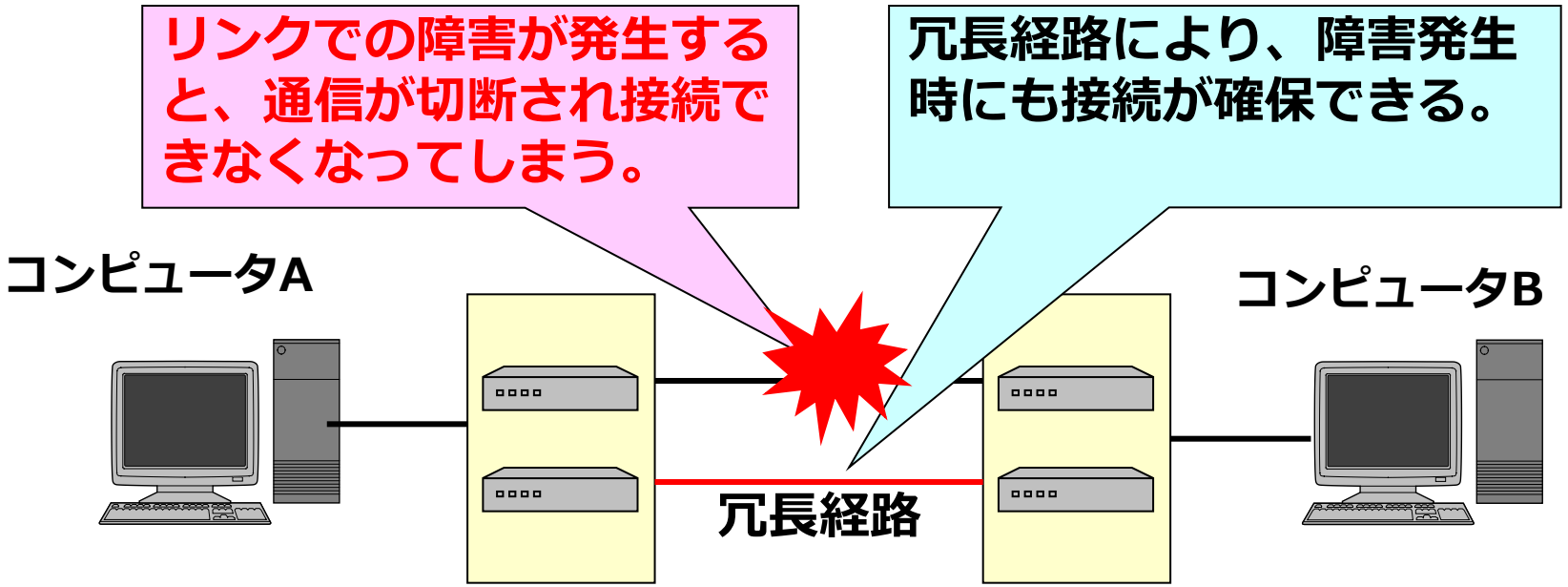


VLAN（L3スイッチ）

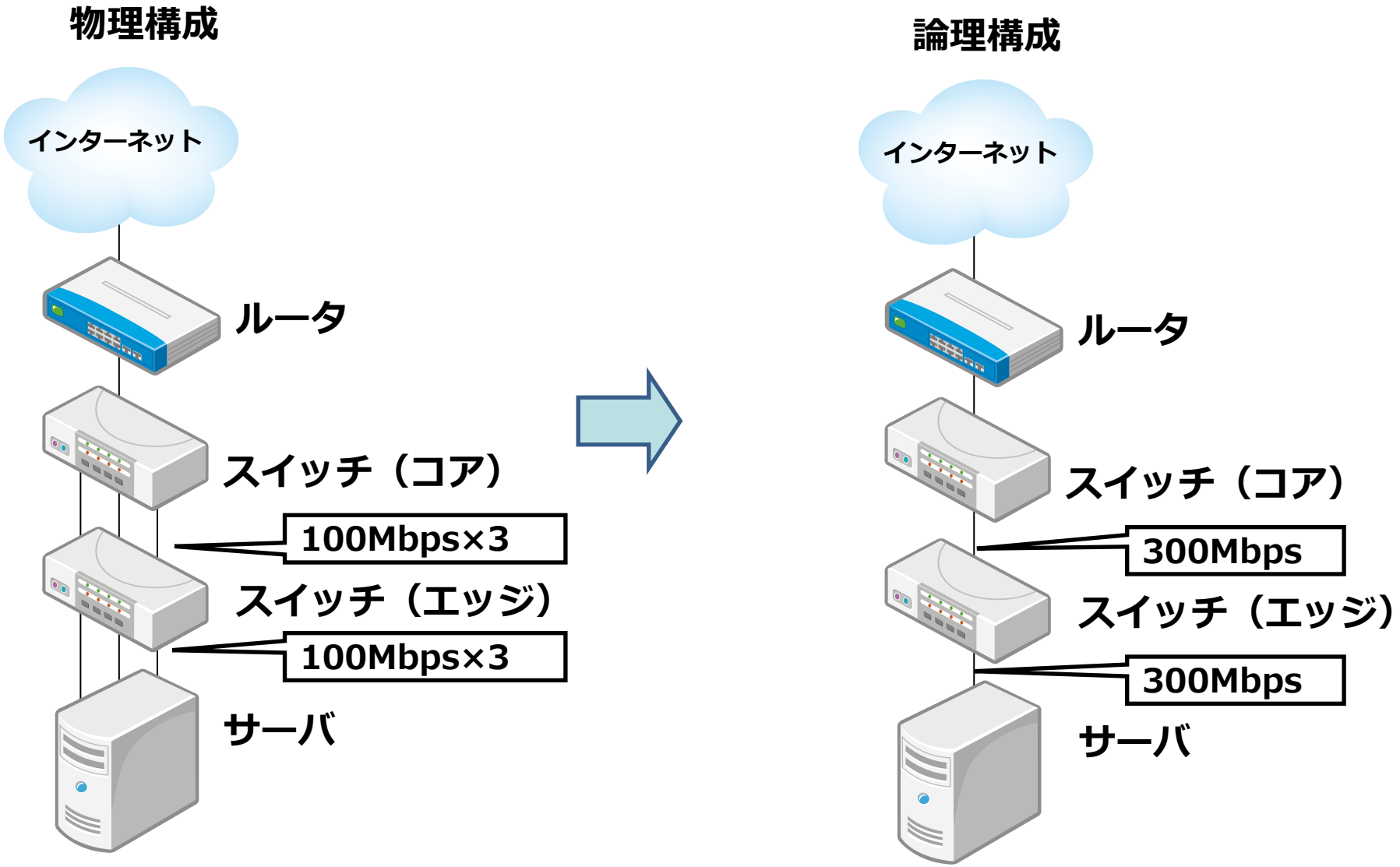

VLAN 1
VLAN 2
VLANによって分割されたネットワークは別のセグメントとして扱われる


L3スイッチ

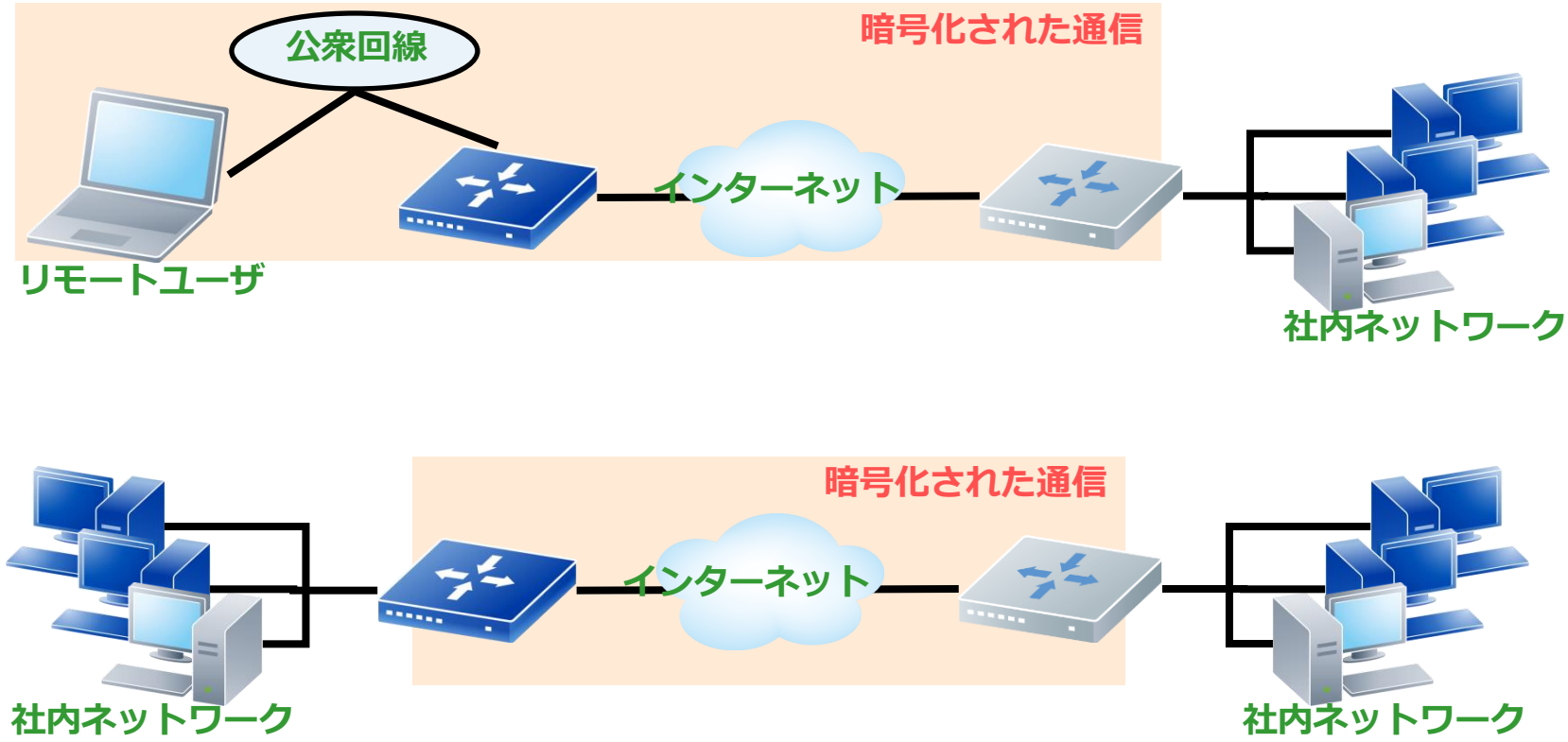
接続の冗長化


リンクでの障害が発生すると、通信が切断され接続できなくなってしまう。
冗長経路により、障害発生時にも接続が確保できる。
コンピュータA
コンピュータB
冗長経路

リンクアグリゲーション



VPN


暗号化された通信
公衆回線
インターネット
リモートユーザ
社内ネットワーク
暗号化された通信
インターネット
社内ネットワーク
社内ネットワーク

＜参考＞商用クラウドサービスの例

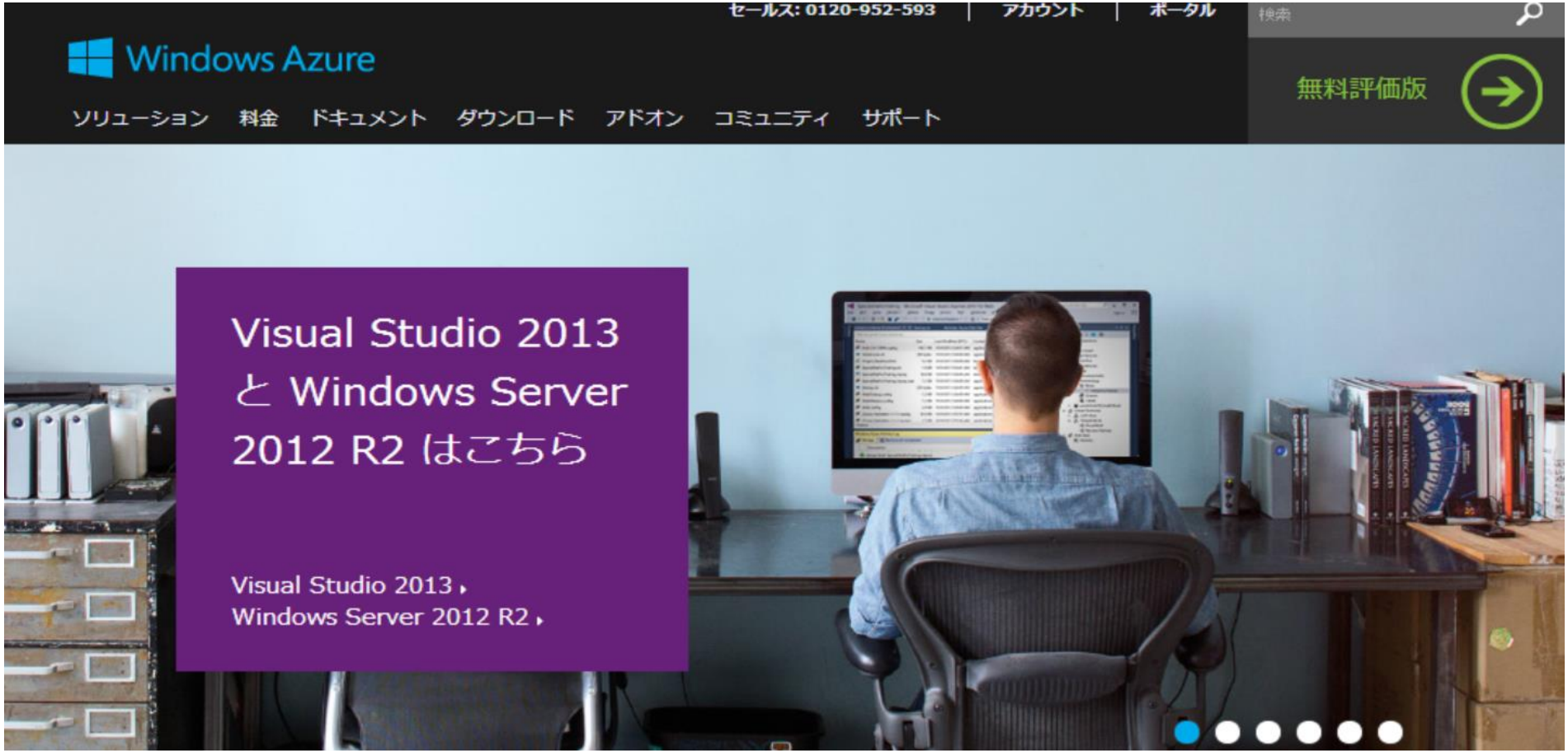
Google


Google Apps for Business
営業担当へお問合せ | ログイン
特長
サービス内容
成功事例
料金
資料ダウンロード
イベントとパートナー
ご利用の流れ
開始する
ワークスタイルの新しいかたち
どこからでも作業できるウェブベースの
メール、カレンダー、ドキュメント
開始する
31
500 万以上の企業が Google Apps を導入しています

Amazon


amazon web services
サインアップ
アカウント / コンソール
English
製品とソリューション
AWS Product Information
開発者
サポート
Amazon EC2 詳細
EC2 概要
EC2 よくある質問
EC2 価格
EC2 の SLA
EC2 インスタンスタイプ
EC2 インスタンス購入の方法
リザーブド インスタンス
スポットインスタンス
Windows インスタンス
Amazon EC2 の機能
Elastic Block Store
Amazon Elastic Compute Cloud（Amazon EC2）
Amazon Elastic Compute Cloud（Amazon EC2）とは、クラウド内で規模の変更が可能なコンピュータ処理能力を提供するウェブサービスです。開発者がより簡単にウェブスケールでのコンピュータ作業をできるように設計されています。
Amazon EC2 のシンプルなウェブサービスインターフェイスによって、手間をかけず、必要な機能を設定して利用することができます。お客様のコンピュートリソースに対して、高機能なコントロールが提供され、Amazon の実績あるインフラストラクチャ上で実行できます。Amazon EC2 は、わずか数分間で新規サーバーインスタンスを取得して起動することを可能にします。これにより、コンピューティング要件の変化に合わせて、素早く能力を拡張または縮小することができます。実際に使用した分だけ料金を払えばよいので、Amazon EC2 は、クラウドコンピューティングサーバーの経済性を変革しました。Amazon EC2 は、開発者にツールを提供して、障害に耐性のあるアプリケーションの構築と、一般的な障害シナリオからの脱却を可能にします。
AWS無料体験セミナー開催
AWS体験ハンズオン
～アカウント開設＋仮想サーバーAmazon EC2編～
AWS を
無料で使用開始
今すぐ無料アカウント作成
導入・資料請求のお問い合わせ »
AWS の無料利用枠には Linux および Windows の毎月 750 時間分のマイクロインスタンスが含まれます（1 年間）。無料利用枠内に抑えるには、EC2 マイクロインスタンスのみを使用してください。
AWS 無料利用枠の詳細 »
アカウント作成の流れはこちら »

Microsoft


セールス: 0120-952-593
アカウント
ポータル
検索
Windows Azure
無料評価版
ソリューション
料金
ドキュメント
ダウンロード
アドオン
コミュニティ
サポート
Visual Studio 2013
と Windows Server
2012 R2 はこちら
Visual Studio 2013
Windows Server 2012 R2

ニフティ


NIFTY Cloud
ニフティクラウド
クラウドサービスならニフティクラウド
各種お問い合わせ
パートナープログラム
@niftyトップ
導入相談窓口
(平日 9:00~17:45)
0120-22-1200
特長
仕様・機能
料金
事例
イベント/お知らせ
サポート
サイト内検索
検索
NIFTY Cloud
ニフティクラウド
始めるなら今!
ニフティクラウド初得2倍
ご好評につき延長!
通常の2倍
ニフティクラウド新規お申し込みで
6万円値引き!
キャンペーン期間:
12月25日(水)まで
詳細はこちら
1 2 3 4 5
ニフティクラウドは、ニフティが2010年1月から開始したIaaS型パブリッククラウドコンピューティングサービスです。
VMwareで仮想化されたサーバー資源を利用でき、短時間で利用/停止できるオンデマンド性や、時間単位の従量課金、国内データセンターによる高いパフォーマンスなどを特長としています。
※サービス提供開始以来、2,000件以上の導入実績(2013年1月末現在)
お申し込み、資料請求はこちら
お申し込み
資料ダウンロード

IIJ

IIJ GIO

サイトマップ　お問い合わせ　サイト内検索　検索　IIJ Internet Initiative Japan

トップ | IIJ GIOとは | サービス一覧 | 導入事例 | パートナープログラム

持たない
プライベートクラウド

IIJのクラウドサービス上にお客様専用のVMware仮想化環境を用意。
アセットレスにプライベートクラウドを実現します。

オンプレミス環境からの移行はもちろん、
既存VMware基盤とハイブリッドでの利用も可能です。

IIJ GIOコンポーネントサービス
仮想化プラットフォーム VWシリーズ

資料請求、見積依頼もお気軽に

お問い合わせ

電話でのお問い合わせ
03-5205-4466
（土日祝日除く 9:30～17:30）

Facebook
IIJ GIOファンページ

IIJ GIO
いいね！

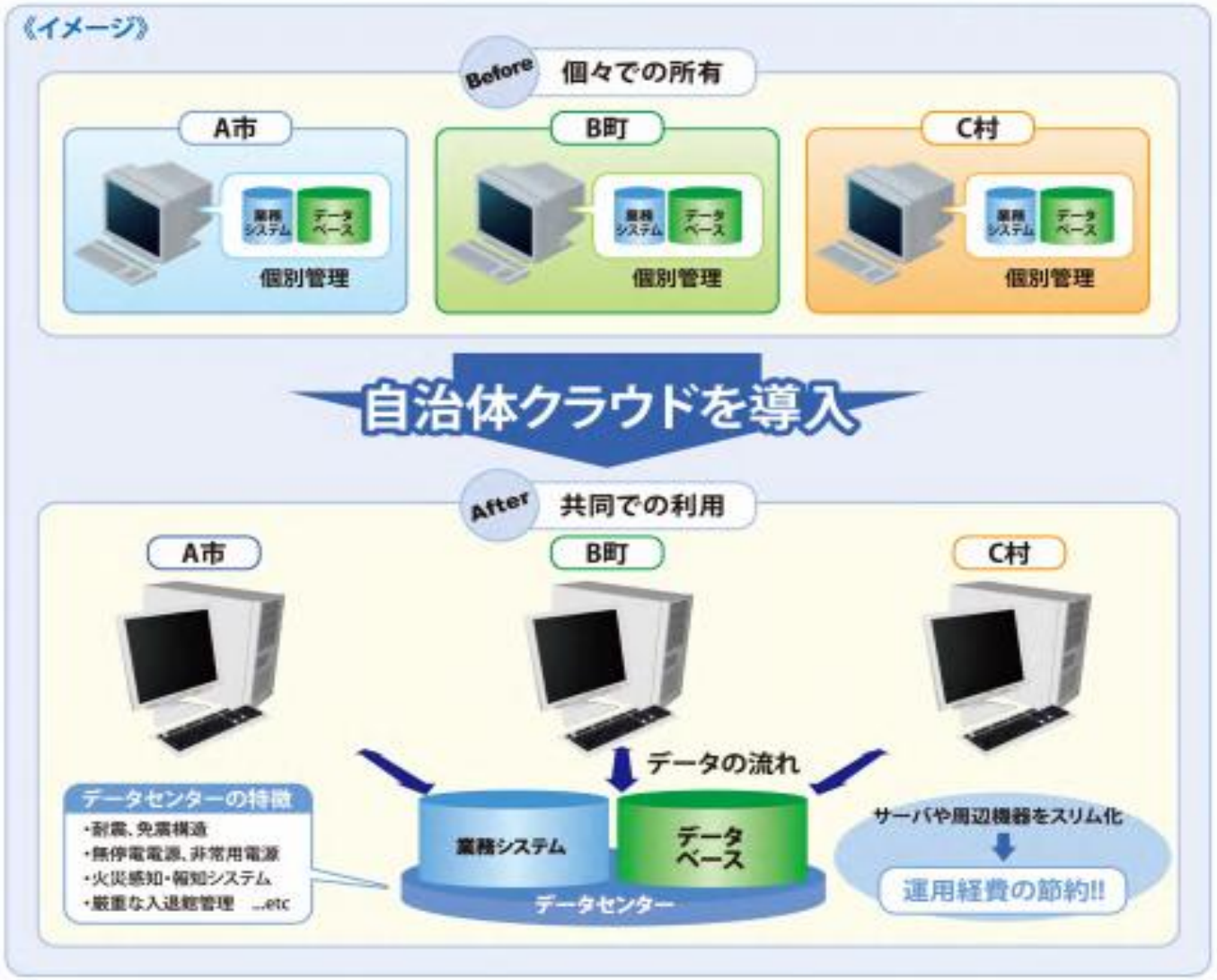
IIJ GIO サービスラインアップ

一覧を表示

IaaS
- IIJ GIOコンポーネントサービス

SaaS/PaaS
- IIJ GIOサイボウズガルーン SaaS

行政クラウド：自治体クラウド



マルチクラウド

- 複数のクラウドを連携させて横断的に利用するという考え方、または、そうした方式を導入したサービス
- 可用性向上やベンダーロックイン回避を期待できるが、それほど簡単ではない
  - 仮想マシンのイメージは最低でも数GB以上であるため、ネットワーク上を簡単に移動できない
  - 事業者が利用している仮想化基盤によって、対応する仮想マシンの形式が異なる

コンテナ技術

- マルチクラウドを容易に実現する技術として、「コンテナ」に近年注目が集まっている
- コンテナ＝ＯＳを含まない軽量なアプリ実行環境＋アプリケーション
  - Linuxが動作する環境であれば、ほぼ100%コンテナが動作する
  - 例えば、事業者AのLinux(仮想マシン)上でコンテナを作り、そのコンテナ内でミドルウェアやアプリケーションプログラムを作成すると、そのコンテナ(数100MB程度)を事業者BのLinuxにコピーすれば、全く同じアプリケーションを動作させられる

自動化

- 仮想化技術によって実現されているクラウドは、多くの機能をコマンドやプログラムによって実行できる
  - →すなわち、自動化できる
- 例えば、「夜間のみ仮想サーバーの台数を減らす」や、「ある事業者のクラウドサービスに障害が発生したら、担当者にメール通知の上、別の事業者で仮想サーバーを起動してサービスを継続する」などが全て自動化できる
- プログラムで自動化可能な範囲は事業者によって異なるので、コスト削減を目的にするなら選定のポイントになり得る

質疑応答（Q&A）

※ この講演における発言、及び資料の内容は、個人の見解であり、所属する企業や団体を代表するものではありません。