# クラウドコンピューティングの技術と利活用に向けての課題

2010年　5月　25日

NTT　情報流通基盤総合研究所
三宅　功

# 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. なぜクラウドなのか？

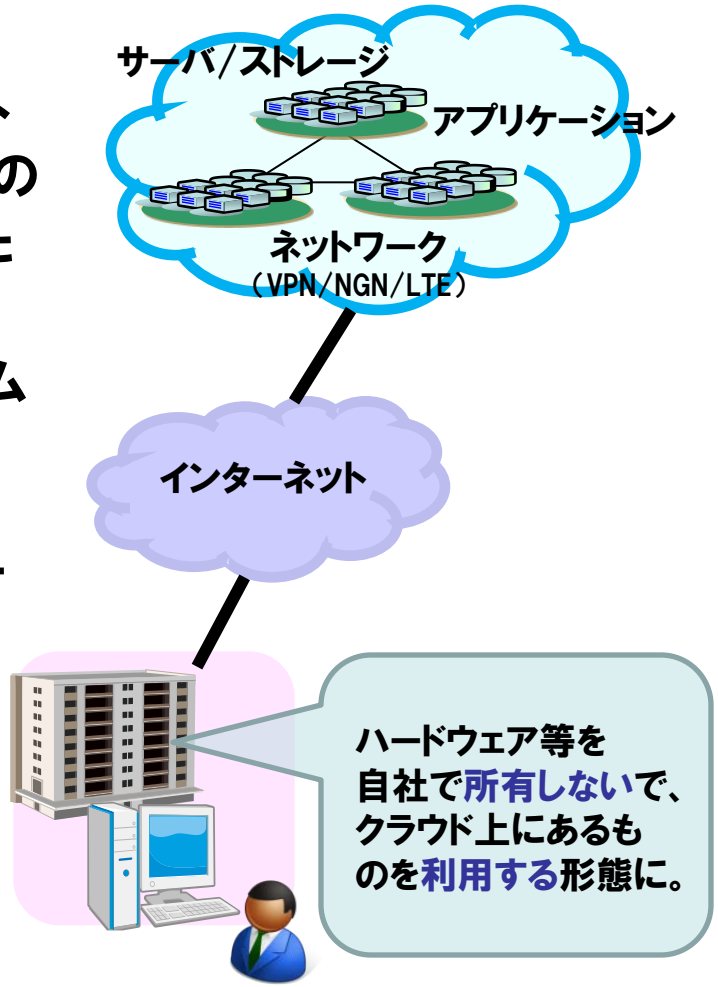
クラウドコンピューティングの技術と利活用に向けての課題

# 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」とは明確な定義のない抽象的な概念
## かなり広範囲で用いられ、最近の流行を全て包含

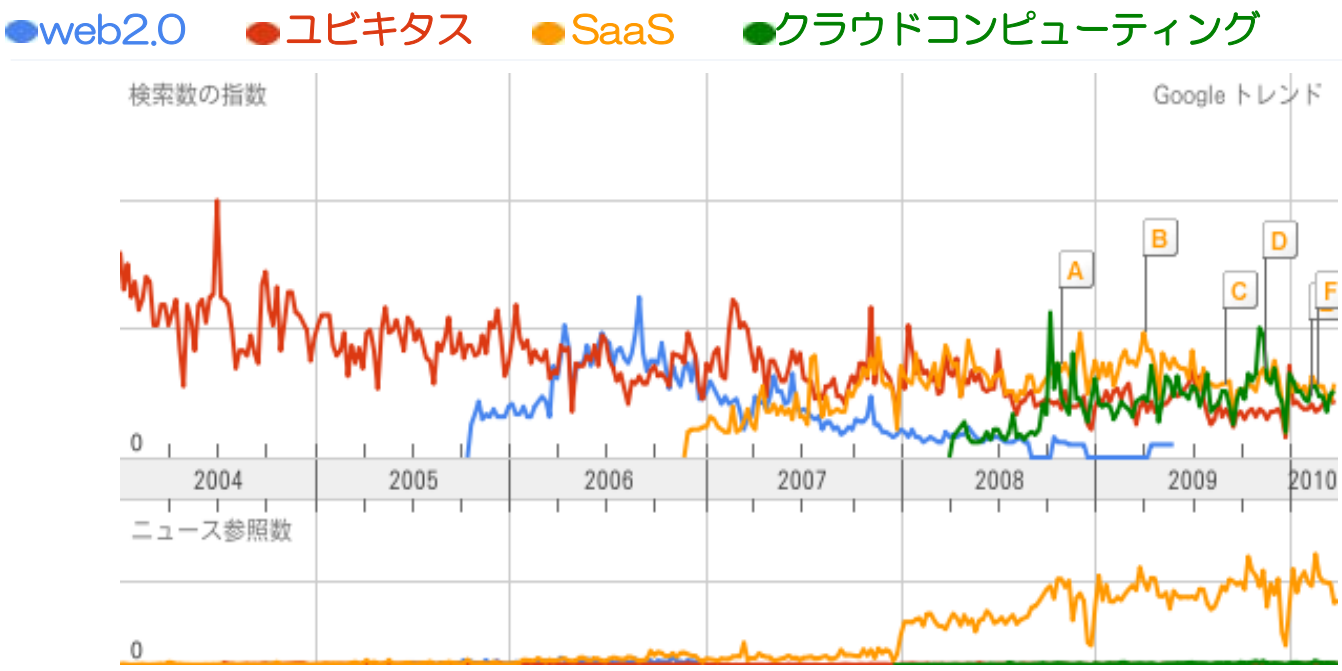
- 2006年8月、GoogleのCEOエリック・シュミット氏がSearch Engine Strategies Conferenceの講演で「クラウド・コンピューティング」と表現したことが始まり。
- 従来ユーザの手元にあったデータやICTシステムが、サーバー(＝クラウド)上へ移行。
- ブラウザ等があればPC、Mac、携帯電話、BlackBerry、新たに登場するデバイスなどのすべての端末からアクセス可能。



# クラウドの注目度合い

## 「クラウドコンピューティング」はIT業界で注目のキーワード

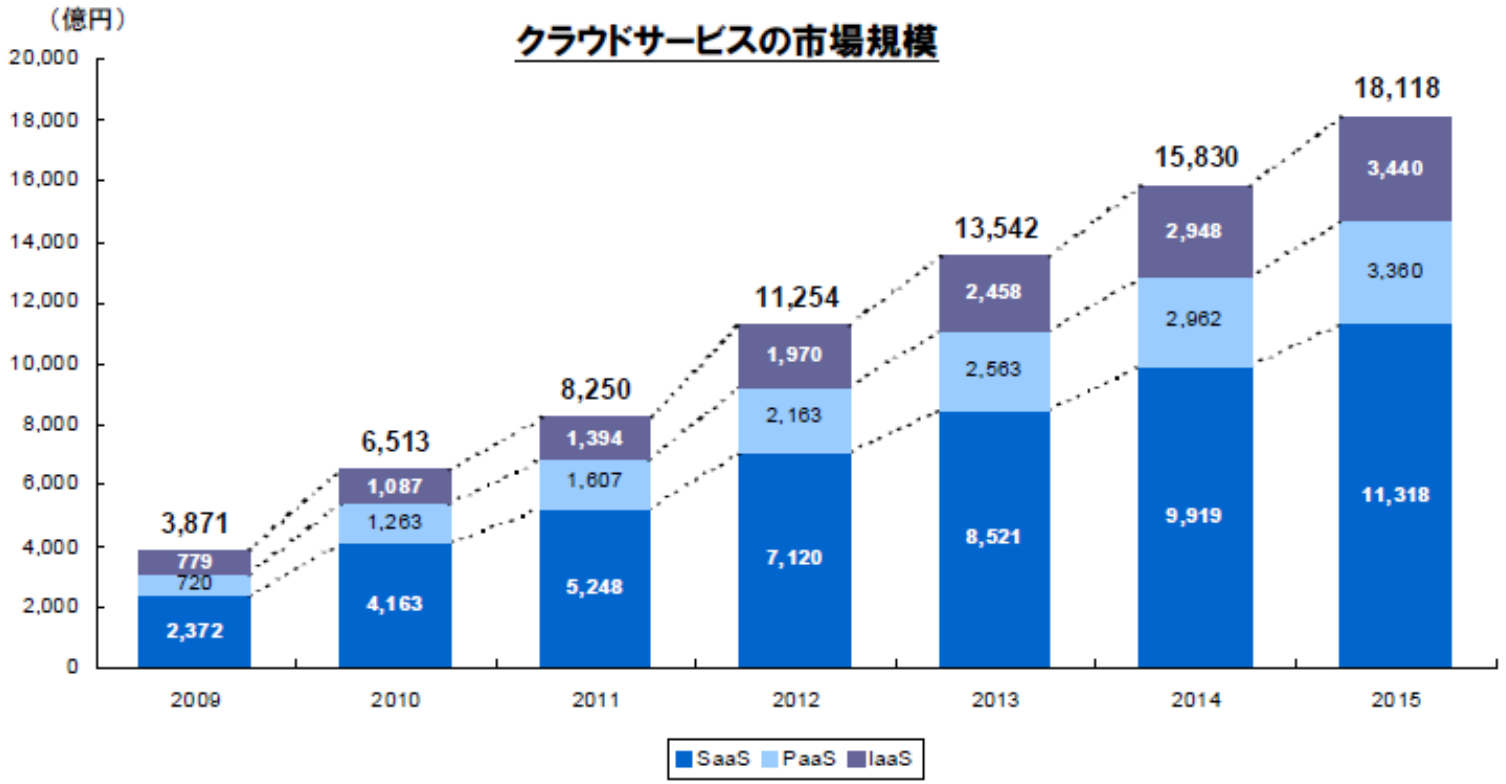
- SaaS：2006年後半に出現、その後注目。
- Web2.0：2005年後半に出現、2006年に大ブレーク。その後衰退。
- クラウドコンピューティング：2008年に出現、2008年中頃には、SaaSを超える注目も。




google トレンド　日本に限定してキーワードを入れて作成
http://www.google.co.jp/trends

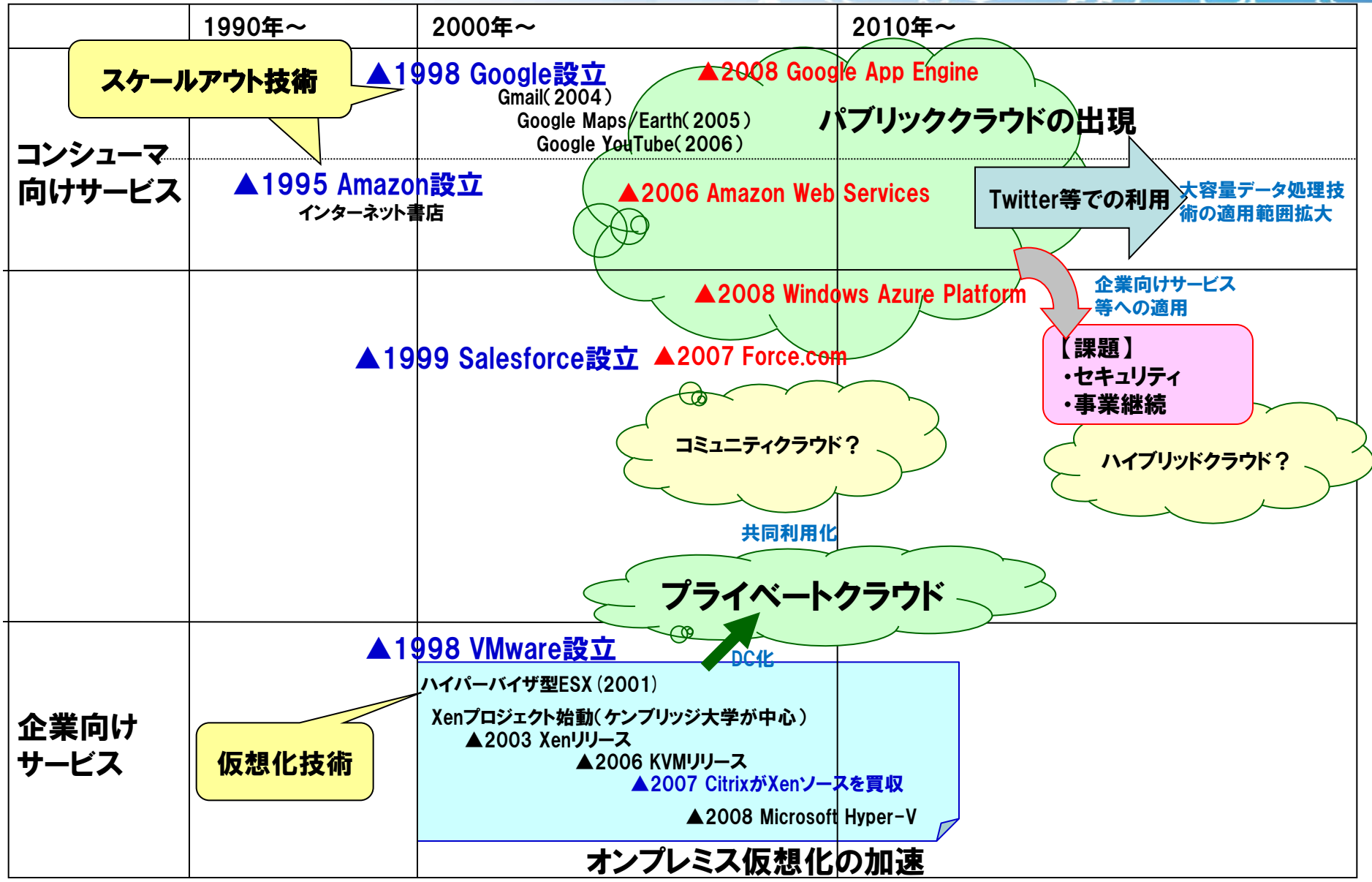
# クラウドの国内市場規模予測

## 2015年時点で約1.8兆円の市場規模
## 年率成長率は30%と極めて高い（SaaS市場が6割強）



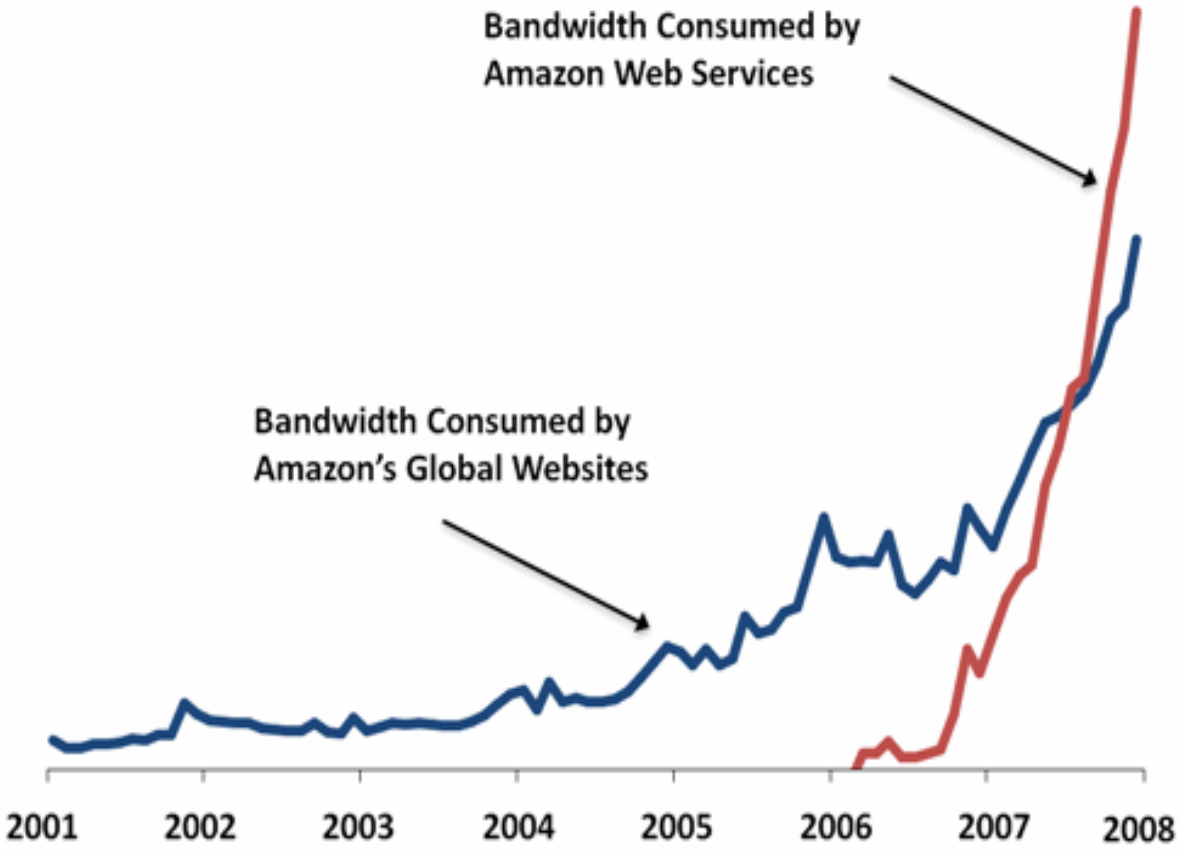

出典：総務省スマート・クラウド研究会報告書（2010年5月）

# クラウド関連の変遷


1990年～
2000年～
2010年～
コンシューマ向けサービス
企業向けサービス
スケールアウト技術
▲1998 Google設立
Gmail(2004)
Google Maps/Earth(2005)
Google YouTube(2006)
▲2008 Google App Engine
パブリッククラウドの出現
▲1995 Amazon設立
インターネット書店
▲2006 Amazon Web Services
Twitter等での利用
大容量データ処理技術の適用範囲拡大
▲2008 Windows Azure Platform
企業向けサービス等への適用
▲1999 Salesforce設立
▲2007 Force.com
【課題】
・セキュリティ
・事業継続
コミュニティクラウド？
ハイブリッドクラウド？
共同利用化
プライベートクラウド
DC化
▲1998 VMware設立
仮想化技術
ハイパーバイザ型ESX(2001)
Xenプロジェクト始動(ケンブリッジ大学が中心)
▲2003 Xenリリース
▲2006 KVMリリース
▲2007 CitrixがXenソースを買収
▲2008 Microsoft Hyper-V
オンプレミス仮想化の加速

# （参考）AmazonウェブサイトとAWSの帯域幅の比較

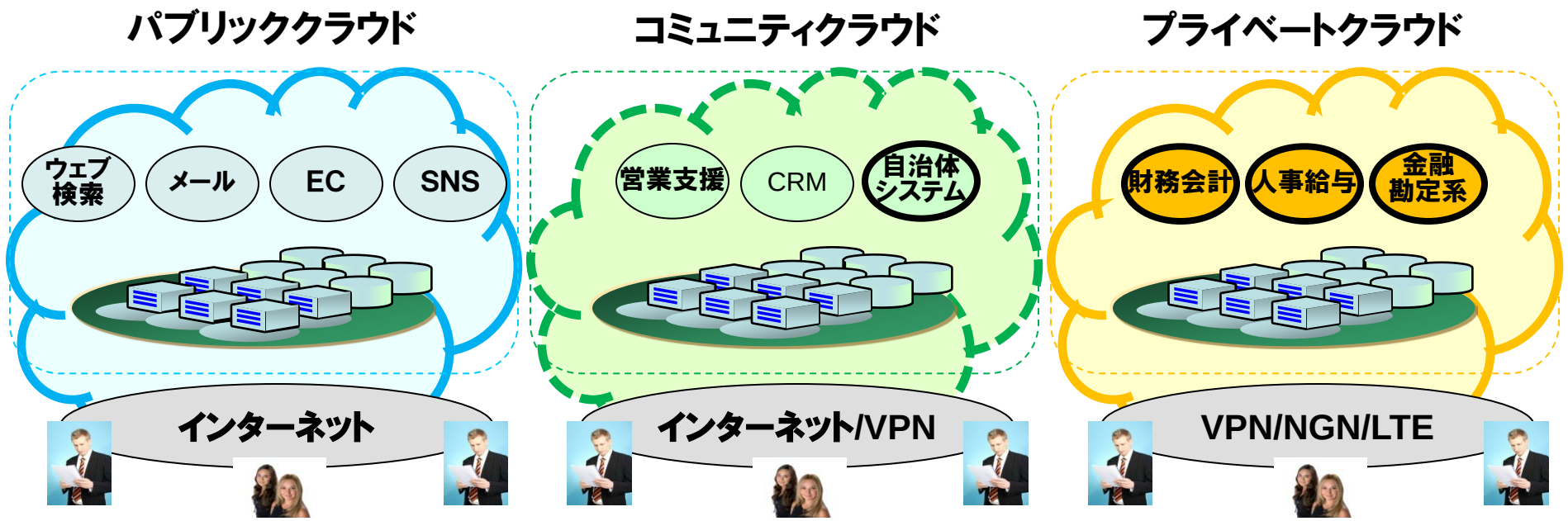
## 2007年半ば、Amazonのクラウドコンピューティングサービスで使用する帯域幅が、ウェブサイトのものを超えた




http://aws.typepad.com/aws/2008/05/lots-of-bits.html

# クラウドの種類

## 所有と利用の形態により、セキュリティに対する要件が異なる



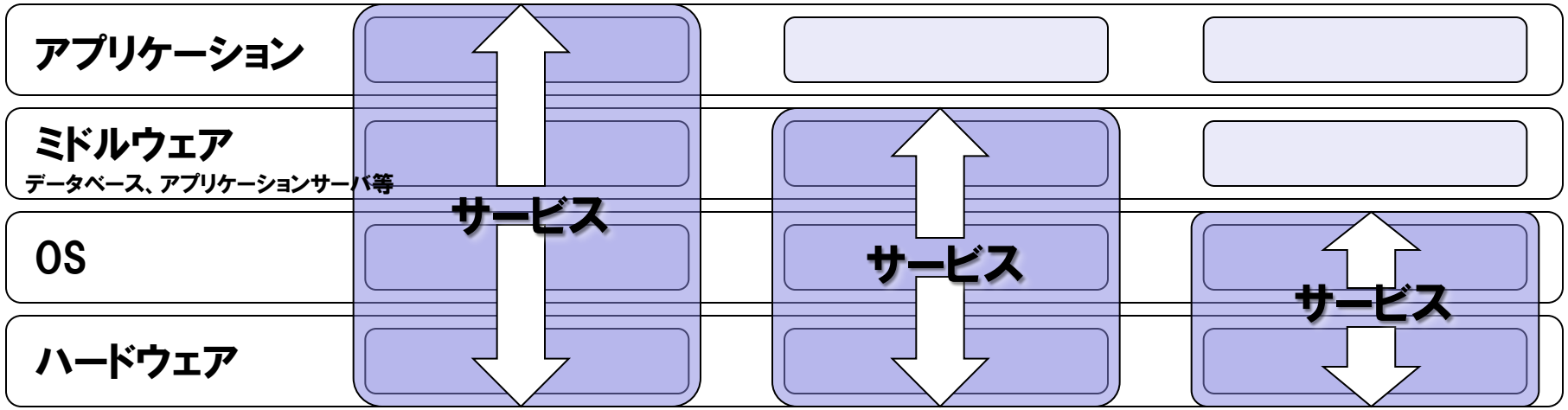

| コンシューマが利用 | 限定されたユーザが共同利用 | 企業ユーザが利用 |
|---|---|---|
| ウェブ検索、電子コマース、ソーシャルネットワークなどで利用 | 自治体クラウド<br>CRMアプリによる営業支援 | 情報共有や財務人事情報を取り扱う基幹系システムで利用 |
| インターネット上のどこにあるか<br>データ保存先を把握不可能 | コミュニティによって設備を分け<br>データ保存先をある程度特定可能 | 所有設備内のため<br>データ保存先を特定可能 |

注：ハイブリッドクラウドは、上記3つの組み合わせ。

# クラウドサービスの提供形態

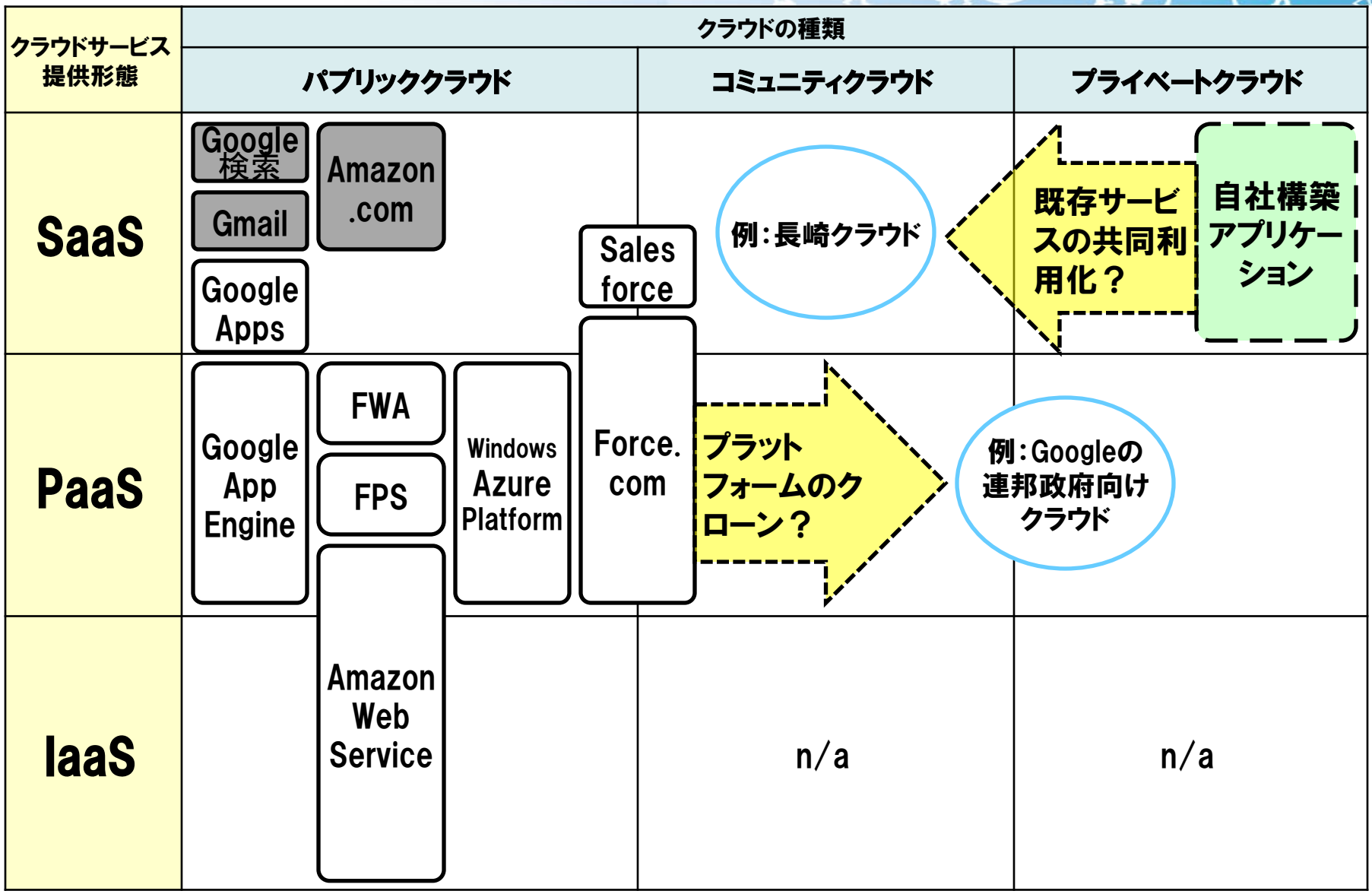
## SaaS、PaaS、及びIaaS/HaaSに大別される。

| 名前 | SaaS<br>Software as a Service | PaaS<br>Platform as a Service | IaaS/HaaS<br>Infrastructure as a Service<br>Hardware as a Service |
|---|---|---|---|
| 主なサービス例 | Saleforce<br>Google Apps（Gmail） | Force.com<br>Google App Engine | Amazon Web Services |
| ユーザ利用形態 | 提供される<br>アプリケーションを利用 | API/仕様に従い<br>アプリケーションを構築 | 既存の<br>アプリケーションを移行 |




注：HaaS/IaaSは境界が曖昧

# クラウドサービスのマッピング

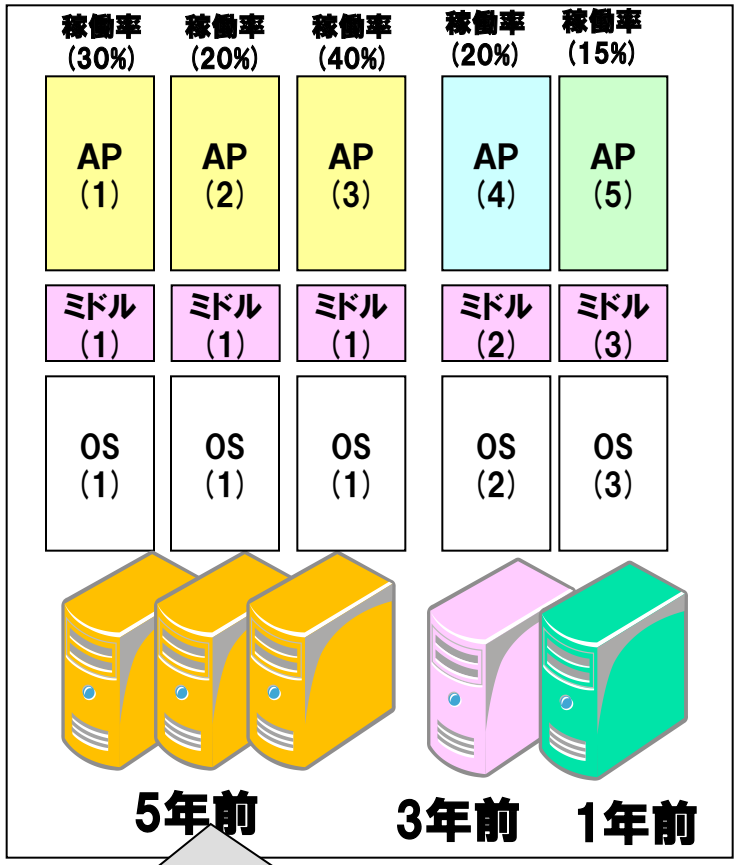



FWA（Fulfillment Web Service）：Amazon.comの受注処理業務サービス（在庫管理、梱包、配送の代行サービス）を利用するためのAPI
FPS（Flexible Payments Service）：Amazon.comのオンライン決済システムを他のサービスで利用するためのAPI

# 仮想化とは

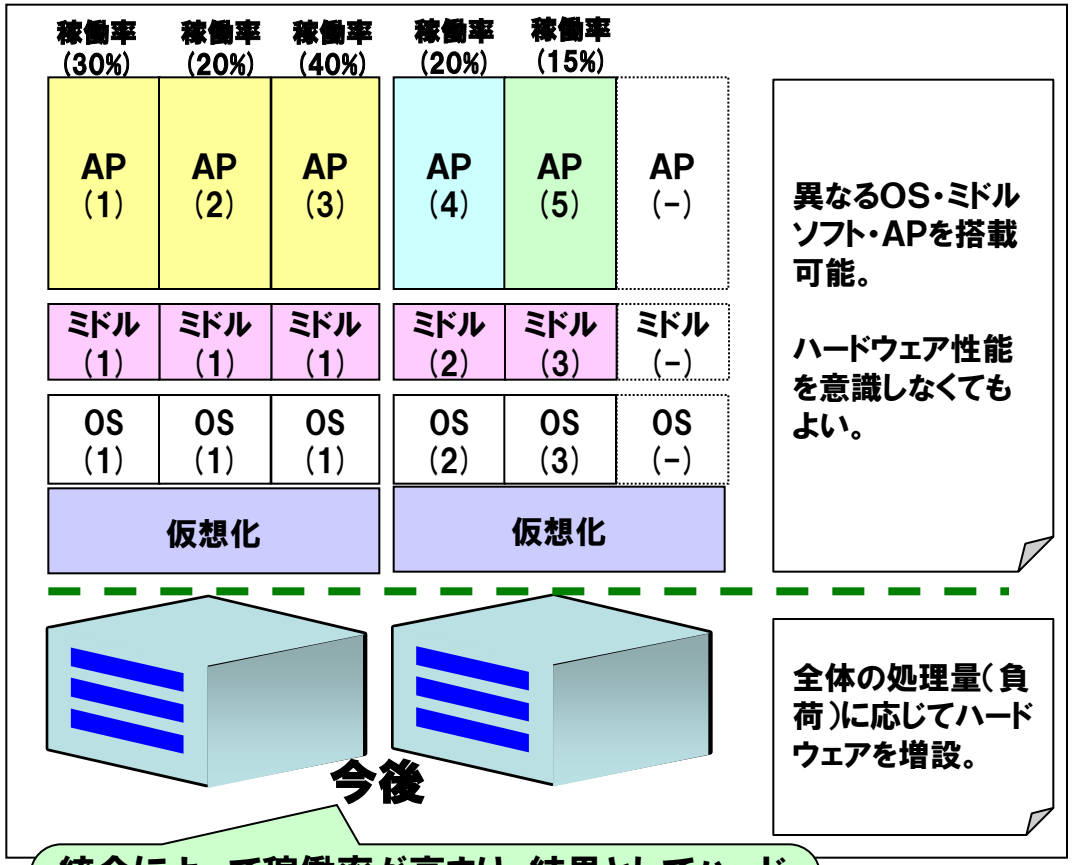
## 仮想化技術の進歩により、ハードウェアとソフトウェアが分離され、サーバ統合が可能に。

### これまでの社内システム（乱立）




ハードウェア更改時には、多くの場合、APを改造する必要あり

### ハードウェアとソフトウェアを分離→統合化




統合によって稼働率が高まり、結果としてハードウェアを削減。資産管理稼動も削減。

**環境負荷の低減に期待**

クラウドコンピューティングの技術と利活用に向けての課題

# 2. クラウドコンピューティングを支える技術

# クラウドを構成する技術体系

■分散処理・システム技術

- スケールアウト技術（LB, KVS, P2P etc.）
- 並列処理（GFS, MapReduce, BigTable）
- CAPバランス（データコピー、分散ロック　etc.）
- 分散システム設計・開発技法（開発環境、パフォーマンスモニタetc.）
- インターオペラビリティ

■仮想化技術

- 大規模な仮想化（プロビジョニング、ライブマイグレーション、VMI etc.）
- 相互運用性と既存システムからの移行技術

■セキュリティ・システム運用技術

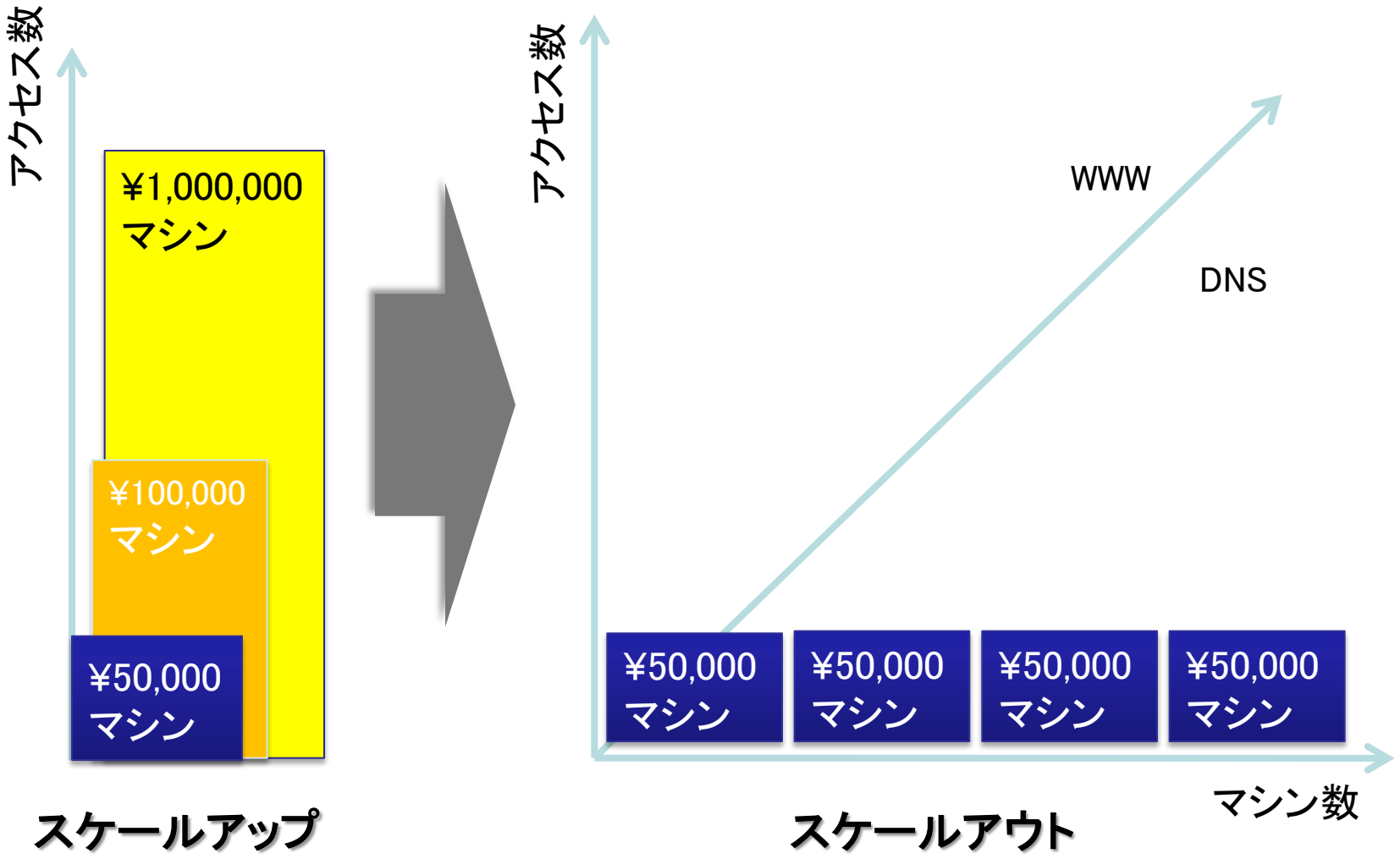
- システム隔離技術
- データ保全・ログ管理技術
- システムモニタリング・ジョブ管理技術
- ドメイン管理技術
- ユーザ・機器認証技術

■データセンタ構成技術

- サーバインターコネクション技術
- 消費電力管理技術

# スケールアップからスケールアウトへ

## 大容量データの分散処理技術により、スケールアップからスケールアウトへ



# CAP定理・ACID・BASE

## CAP定理：ウェブ上のサービスは「一貫性」と「可用性」と「分散耐性」の3つのうち、最大でも2つまでしか同時に満たすことはできない

2000年カリフォルニア大学バークレー校Eric Brewer教授が提案

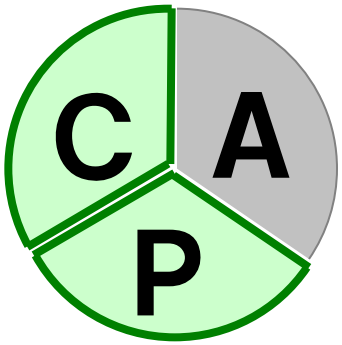
Consistency（一貫性）：クライアント（ユーザ）は、一連のデータ処理を同時に起きたものとして扱えること。（あるクライアント（ユーザ）がデータ更新した場合、それ以降にそのデータを利用するクライアント（ユーザ）は、全ての処理で更新後のデータを取得できることを保証する。）

Availability（可用性）：すべての処理は所定時間内に終了すること。（いつでも、街頭データをお読み書きができる。）

Partition-tolerance（分散耐性）：システムの構成要素（物理的あるいは仮想的サーバ）が壊れてもシステム全体が問題なく動作すること。

### ACID

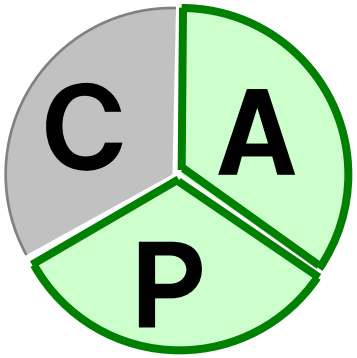
分散処理ではPは必須。Cを達成するためにAの条件を緩和




- **A**tomicity　不可分性、原子性
- **C**onsistency　一貫性、整合性
- **I**solation　独立性
- **D**urability　永続性

### BASE

分散処理ではPは必須。Aを達成するためにCの条件を緩和




- **B**asically **A**vailable　基本的に可用
- **S**oft state　厳密でない状態保持
- **E**ventually consistency　結果としての一貫性

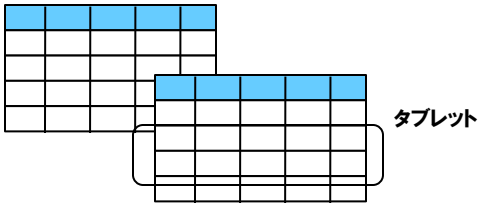
# 大規模データの分散処理技術(Googleの例)

## Googleは大規模データを処理する技術を保有する

### BigTable 分散テーブル

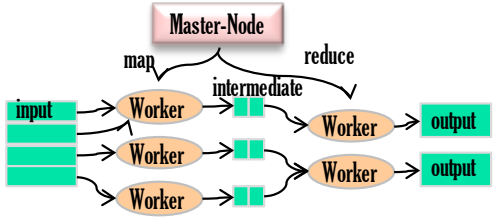
Key-Value Store

- 膨大な量のレコードを管理することを目的とした簡易DB
- 複数のレコードをタブレットと呼ばれる単位で束ねて管理



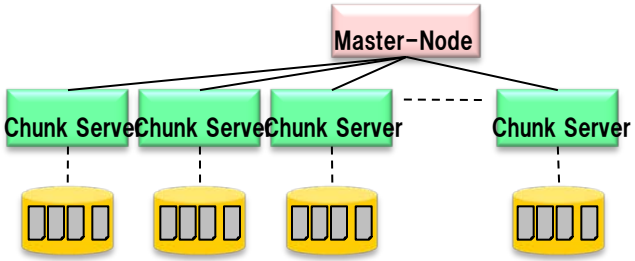

### MapReduce 並列並列分散処理フレームワーク

- 大量レコードに対する分散計算処理を行うことが目的
- 並列スケルトンモデルの一つであるMapReduceを複数台マシンで実装したモデル
- レコードを分割し、Mapと呼ばれる処理、並びにReduceと呼ばれる処理を適用。




### Google File System 分散ファイルシステム

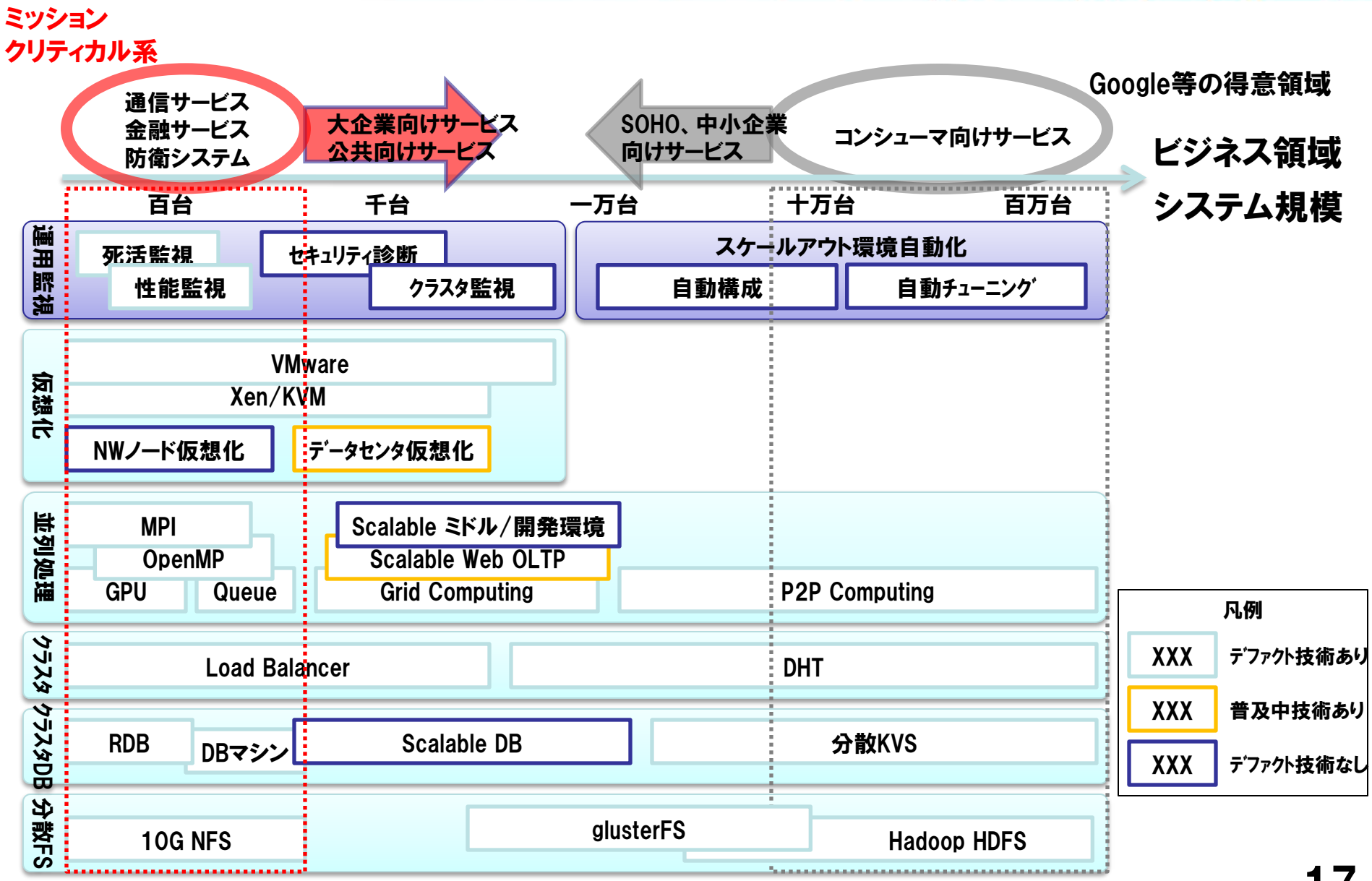
- マスタ・スレーブ型の分散ファイルシステム
- ファイルの位置等のメタ情報を管理するマスタと、実データを管理するスレーブから構成される。




### Chubby 分散ロック管理機構

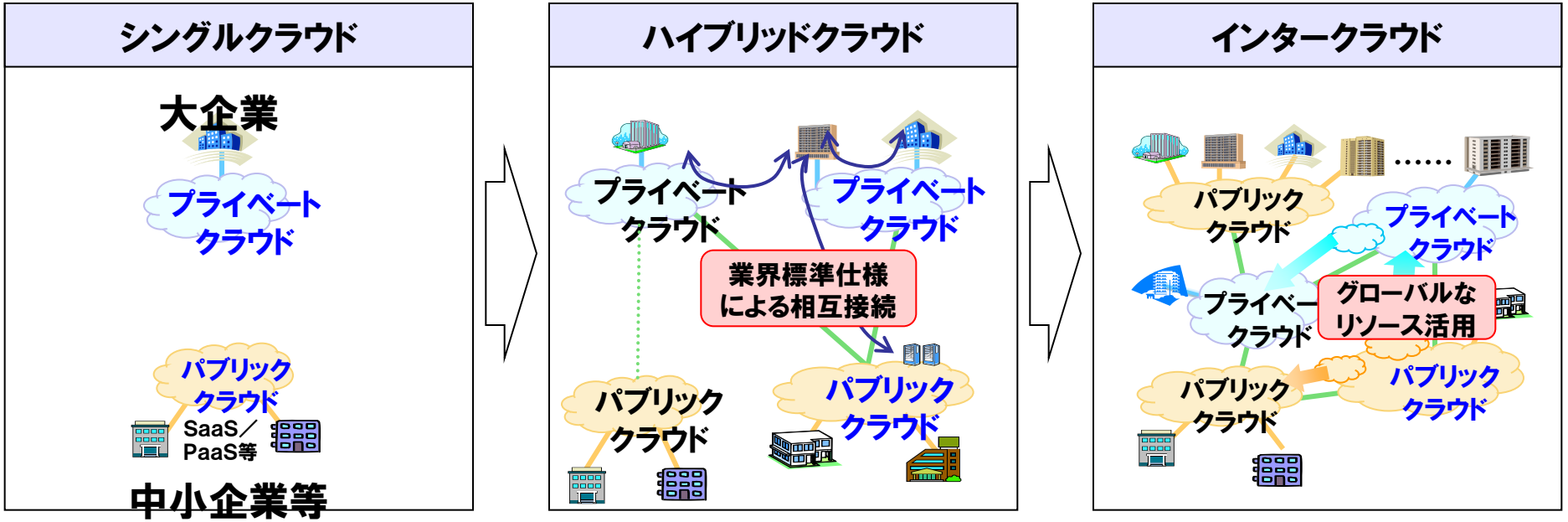
- 分散環境に置いてロックを実現するための機構
- マルチマスタ問題の解決
- 死活監視

# 大規模データ処理技術の適用領域



# クラウドサービスのインターオペラビリティ

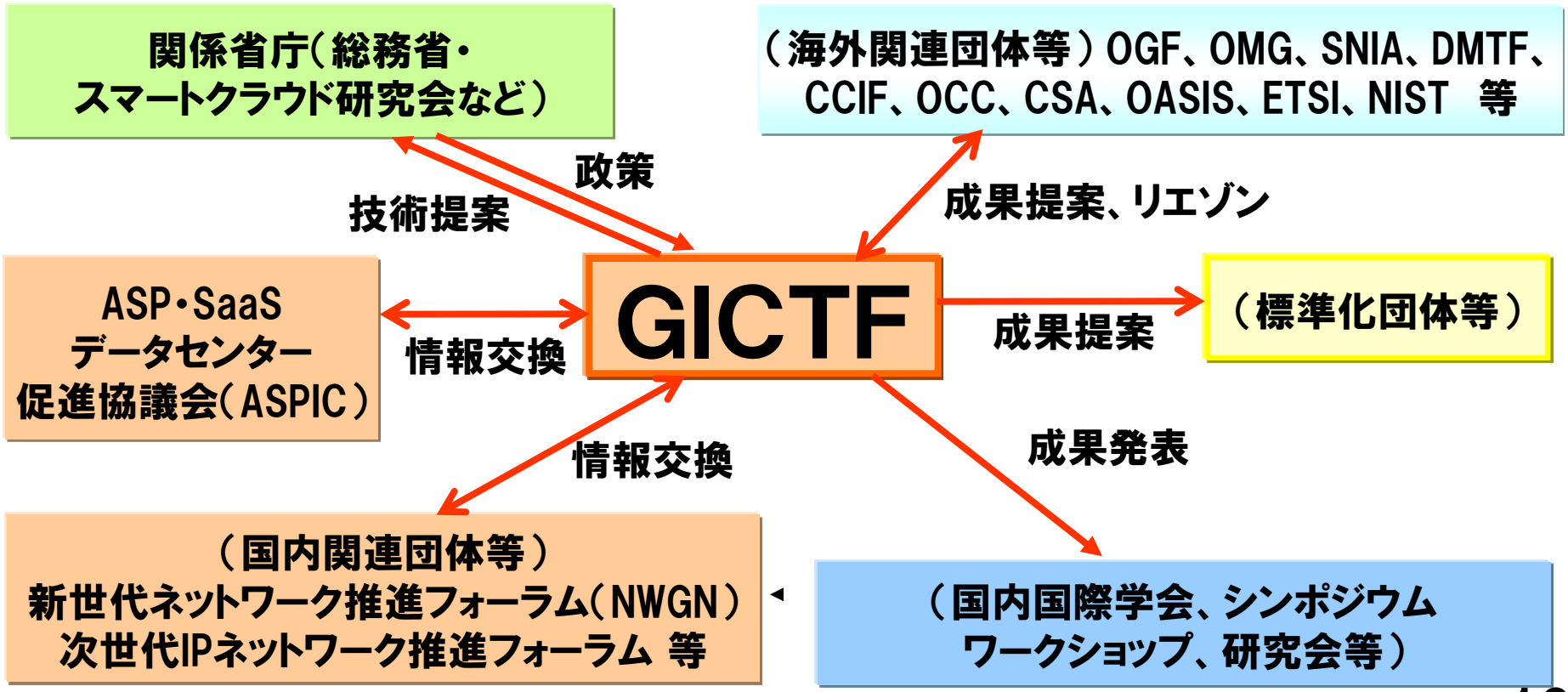
## 中長期的には、単一クラウドの時代から、プライベート・パブリック間が連携される時代を経て、クラウド相互接続の時代へ進化すると予想される



# グローバルクラウド基盤連携技術フォーラム（GICTF）

- クラウドシステム間連携インタフェースのオープン化を産官学で推進
- 国内外関係団体とのリエゾン、利用者への普及啓発
- 会員：47企業、3団体、有識者（大学教授等）、【総務省：オブザーバ】
  ＊NTT、KDDI、NEC、日立、富士通、IBM、Sun、Oracle、Cisco、IIJ、BIGLOBE、VMWare、NICT、NII等

（Global Inter-Cloud Technology Forum: GICTF） http://www.gictf.jp/



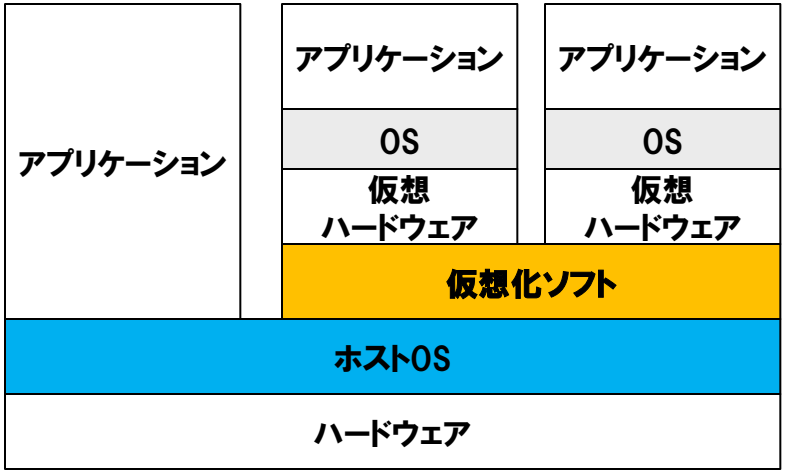
# 仮想化技術

- 仮想化はコンピュータやストレージなどの物理的なリソースを隠ぺいする技術

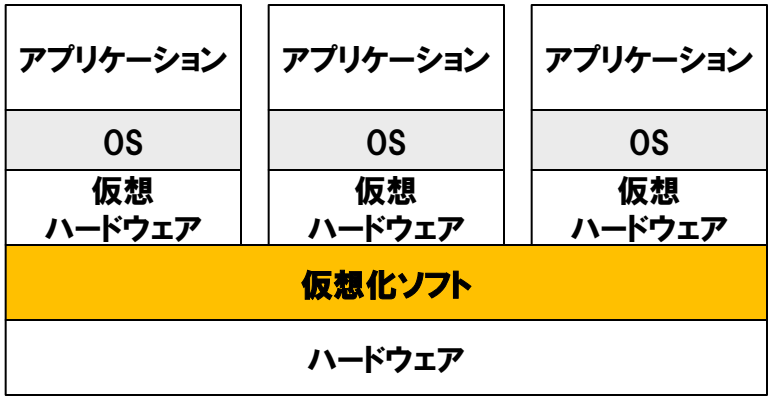
- 「**サーバー仮想化**」では、物理的に1台のコンピュータをあたかも複数台のように扱え、1台のコンピュータで別々のOSとアプリケーションを同時に稼働させられる。
- PCサーバー用の仮想化ソフトは「**ホストOS型**」と「**ハイパーバイザー型**」に大別される。

- 「**ストレージ仮想化**」では、複数のストレージを一つにまとめたり、物理的なリソースの容量にとらわれずに領域を分割したりできる。

- 「**ネットワーク仮想化**」では、VPNやVLANに加え、最近では1台のネットワーク機器を複数台のように扱う、または複数台の機器を1台のように扱う技術が普及しつつある。




ホストOS型




ハイパーバイザー型

# サーバー統合向け仮想化ソフトウェア

- 主な仮想化ソフトウェアとして、Hyper-V(Microsoft)、VMware ESXi／Infrastructure(VMware)、Xen(Citrix/オープンソース)、KVMの4種類を掲載。

## VMware ESXi/Infrastructure

- 1998年に設立されたVMware社の製品。
- VMware ESXiは、前身のVMware ESXから管理機能を提供するサービス・コンソール(Linuxベースのコンソール OS)が省かれ、無償版として提供された仮想化エンジン。
- VMware Infrastructureは、ESX／ESXiに各種機能を追加した有償製品として提供されているもの。

## Xenベースの製品

- Xenは、XenSource(Citrixに買収)が開発し、オープンソースとしても提供されている仮想化エンジン。
- 現在、Xenをベースに各種管理機能などを加えた仮想化ソフトウェアが複数のベンダーからリリースされている。Linuxディストリビューションと一体化している製品もある。

## KVM

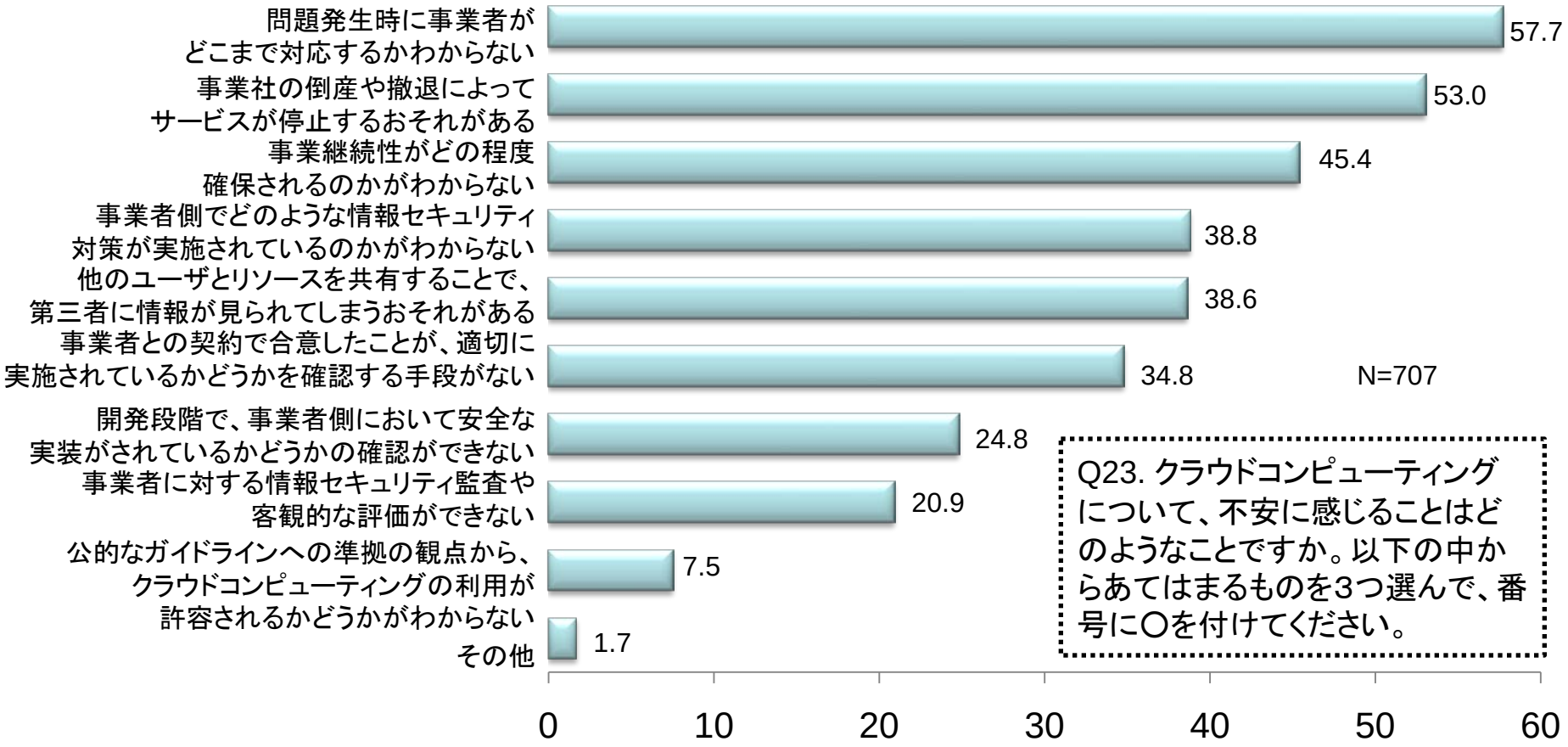
- QUMRANET社が開発して2006年にGPLで公開。カーネルベースの仮想化エンジン。
- 2007年2月にLinux2.6.20にマージされた。
- Linuxカーネルに仮想化ソフトウェアを組み込み処理速度を改善した。

## Microsoft Hyper-V

- マイクロソフト初のハイパーバイザー型の仮想化エンジン。
- Windows Server 2008に標準で組み込まれている。

# クラウドへの不安

## クラウドに対する漠然とした不安として事業継続性やセキュリティ対策がある




出典：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2009」より

# クラウドのセキュリティに対する課題

| | 制度面・ビジネス面およびクラウドの利活用 | 技術的側面 | |
|---|---|---|---|
| | | システム | データセンタの管理・運用 |
| 情報セキュリティ | データセンター施設のセキュリティ | アーキテクチャ自体に関わるセキュリティ | 運用の管理 |
| | クラウドーユーザ間通信のセキュリティ | データストレージのセキュリティ | |
| | 情報のライフサイクル管理 | | 情報のライフサイクル管理 |
| | 暗号と暗号鍵管理 | | |
| | 利用端末のセキュリティ | 暗号化ソリューション：通信、データ、操作 | |
| | ユーザ認証とアクセス管理の仕組み、モニタリング | | |
| 事業継続 | クラウド事業者の存続性 | ハードウェアの信頼性・冗長性 | |
| | クラウド事業者の経営とガバナンス | 災害復旧計画と災害対策 | |
| | クラウド事業者のＢＣＰ | システム及びサービスの可用性・信頼性 | |
| コンプライアンス | 法制度への対応 | 監査可能性と対応(ユーザ・第三者、行政・司法当局)<br>デジタル・フォレンジックス対応 | |
| | データの保管場所と立地国の法制度・プライバシー法制の影響 | | 社員の忠実義務・善管注意義務 |
| | SLA標準／ガイドライン | | |
| オペレーション | データおよびアプリケーションのポータビリティ／ロックイン | | サービスレベルの保障 |
| | 相互運用性と標準化(クラウドークラウド間、クラウドーユーザ環境間) | | |
| | | | ネットワークトラブル・データ転送のボトルネック |

出典：IPA　H22年3月4日　クラウド・コンピューティング社会の基盤に関する研究会報告書(案)P123をもとに作成

# 情報の保管場所や越境問題に対する課題

**法の適用と効力の範囲（属地主義）**
- **原則：適用すべき法は場所的な要素によって定め、その法の効力はその法が制定された領域（国・地域）内に限定する（属地主義）**
- **例外：刑法の国外犯への適用、外国所得税額控除、独占禁止法・証券取引法などの公法の域外適用**
- **国際私法上、国をまたがる法律関係・不法行為の際に適用すると決められた法を準拠法という**
- **日本の場合、準拠法の判断基準は「法の適用に関する通則法」**

## ■事例１　ＥＵにおける個人データの域外移動に関する規制によって、適切な保護レベルにない域外のサーバ、ストレージに個人データを移動できない。

【参考】 EU指令第25条（いわゆる第三国条項）
1. 加盟国は、処理されている、又は後に処理される予定の個人データの第三国への移動は、当該第三国が適切なレベルの保護を提供している場合に限られることを規定するものとする。但し、本指令に従って採択された国内規定に対する遵守を害しないことを条件とする。

## ■事例２　米国では捜査令状の通知なしにストレージが強制捜査を受ける

【参考】テロリズムの阻止と回避のために必要な適切な手段を提供することによりアメリカを統合し強化する2001年の法（米国愛国者法）
第213条令状執行通知を延期する権限
裁判所が、予め通知することが捜査に対して悪い影響を与えると認める場合には、捜査官は、裁判所命令又は令状の執行を直ちに通知することなく被疑者の財産等について捜査を行うことができる。捜査官が裁判所に対し、差押えの相当の必要性を示すことができない場合には、令状を財産又は電子的情報を入手するために利用することはできない。また、個人は、捜査が行われてから「合理的な期間内」に通知を受けなければならない。

# 法制度の限界

## ■事例１　日本の個人情報保護法に基づく主務官庁による規制は、国内の事業者に対しては適用され、国外の事業者に対しては適用されない。

【参考】 法の適用に関する通則法（当事者による準拠法の選択）

第七条　法律行為の成立及び効力は、当事者が当該法律行為の当時に選択した地の法による。（当事者による準拠法の選択がない場合）第八条　前条の規定による選択がないときは、法律行為の成立及び効力は、当該法律行為の当時において当該法律行為に最も密接な 関係がある地の法による。

【対応策の例】
米国GSA(連邦調達庁)は、IaaSの調達ガイドラインにおいて、ハワイ州等を除く米国大陸CONUS(Continental　United States)にリソース(ハードウェア)が所在することを要件としている。

## ■事例２　警察の捜査権は国外には及ばず、強制捜査による証拠保全はできない

【参考】 刑事訴訟法
第九十九条　裁判所は、必要があるときは、証拠物又は没収すべき物と思料するものを差し押えることができる。但し、特別の定のある場合は、この限りでない。
２　裁判所は、差し押えるべき物を指定し、所有者、所持者又は保管者にその物の提出を命ずることができる。
第百六条　公判廷外における差押又は捜索は、差押状又は捜索状を発してこれをしなければならない。
第百八条　差押状又は捜索状は、検察官の指揮によつて、検察事務官又は司法警察職員がこれを執行する。但し、裁判所が被告人の保護のため必要があると認めるときは、裁判長は、裁判所書記又は司法警察職員にその執行を命ずることができる。

## ■事例３　犯罪容疑者のデータと第三者である自己のデータが書き込まれたストレージが、一括して強制捜査を受け、押収されることがある

【参考】 米国ではデータセンタに対するFBIの捜査によって、50社以上の顧客がサービス停止に陥った事例がある。

# クラウドサービスの「SLA」の例

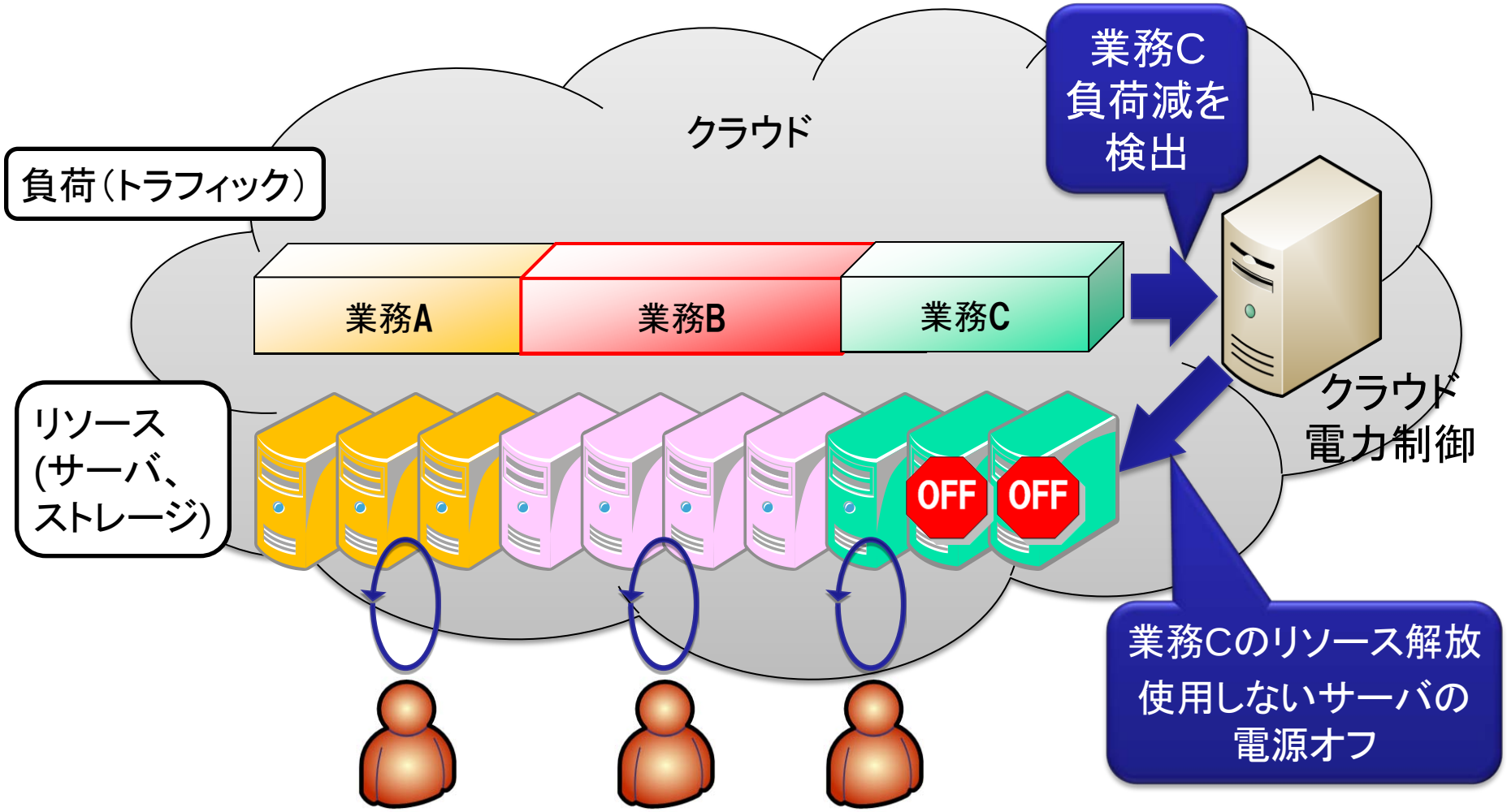
- 現時点では「稼働率」のみであるが、本来は可用性、パフォーマンス／応答時間、スループット、復旧可能性、災害復旧といった点もSLAで規定することができる。
- また、AT&Tのクラウドインフラサービスでは、アプリケーションの可用性までを含めたエンドツーエンドのSLAをうたっている。

| プロバイダー/サービス名 | SLA | ペナルティ等 |
|---|---|---|
| Google / Google Apps Premier Edition | 稼働率99.9%/月 | サービス期間終了後に3～15日間のサービスを無料で追加 |
| Amazon.com / Amazon S3 | 稼働率99.9%/月 | SLAを満たさなかった月の利用料金の10～25%を次回以降の支払いに充てることが可能 |
| Salesforce.com / Salesforce | 標準契約ではなし | 標準契約ではなし |
| NetSuite / NetSuite | 稼働率99.5%/月 | SLAを満たさなかった月の利用料金の10～25%を次回以降の支払いに充てることが可能 |
| ServePath / GoGrid | 100% Uptime SLA | 10,000% Guaranteedと表示しており、ダウンタイムの間の料金の100倍分に相当する利用時間を無料にする |
| Microsoft / Microsoft Online Services | 稼働率99.9%/月 | SLAを満たさなかった月の利用料金を最大全額返金する |
| AT&T / AT&T Synaptic Hosting | 稼働率99.9% | アプリケーションの可用性まで含めた「業界唯一のエンドツーエンドな単一のSLAに基づいた個別サポート」をうたっている |

# 仮想化運用管理機能による電力制御

通常はサーバの電源は入ったまま
⇒サーバが無負荷でも電力を消費

負荷に応じてサーバを制御（停止）
⇒消費電力を削減

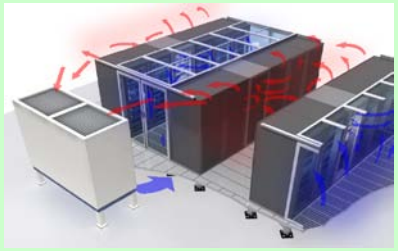


# 環境負荷の低減

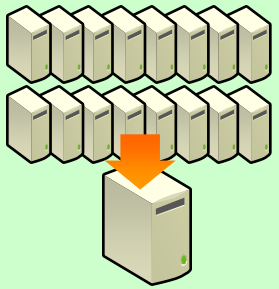
## Green of ICT と Green by ICT

### 太陽光発電システム

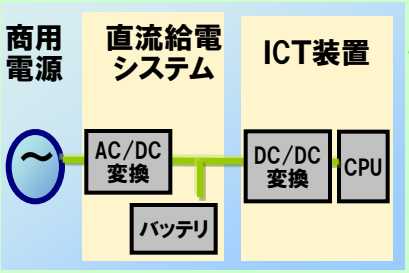
### 高効率空調設計　ICT機器と空調の連係制御



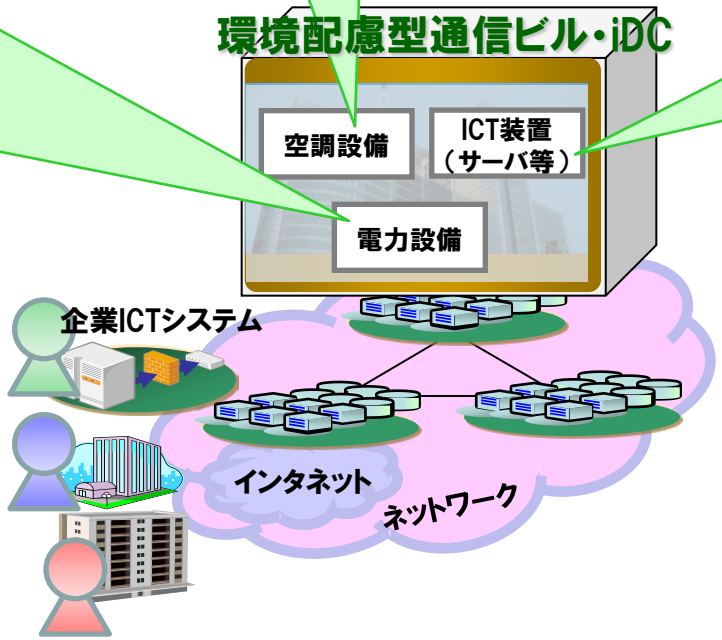

### 仮想化技術



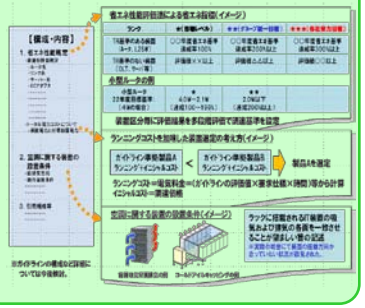
### 高電圧直流給電




### 環境配慮型通信ビル・iDC




### 環境性能ガイドライン



・「環境性能ガイドライン」の取組みは、「ICT分野におけるエコロジーガイドライン協議会」（事務局：電気通信事業者協会）と連携しています。

クラウドコンピューティングの技術と利活用に向けての課題

# 3．なぜクラウドなのか？

# NISTによるクラウドの定義

NIST: National Institute of Standards and Technology

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

  *http://csrc.nist.gov/groups/SNS/cloud-computing/*

  - On Demand and Self Services
  - Broad Network Access
  - Resource Pooling
  - Rapid Elasticity
  - Measured Services

# クラウドへの期待と課題

## 【期待】

- 情報共有の集中化によるメリット
  - アプリケーション・データの共有、共通化が図りやすい
  - 利用者相互にとってICT基盤の共通化が図りやすい； ICT習熟度、リテラシー
  - アプリケーションの開発が容易
- システム構築・運用の効率化、経済化
  - システム部品の共通化、調達スケールメリットによる経済化
  - 保守・運用の一元化による効率化
- セキュリテーの確保
  - 統一したセキュリティーポリシーが取りやすい
- 環境負荷低減
  - システムの集中化により

## 【課題】

- 新たなビジネスモデルへの脅威 → 独占化、寡占化
- 管理ドメインの曖昧化（所有と利用の関係再構築）
- 集中化によるリスクの拡大

# 米国政府の取り組み

## 米国では政府機関が中心になって クラウドを強力に推進

- オバマ政権は2009年12月にOpen Government Directiveを正式発表
  - 各連邦政府機関に対して、価値の高いデータを誰でも入手できるようにすることや、正式なオープンガバメント計画を迅速に策定し発表することを求めている

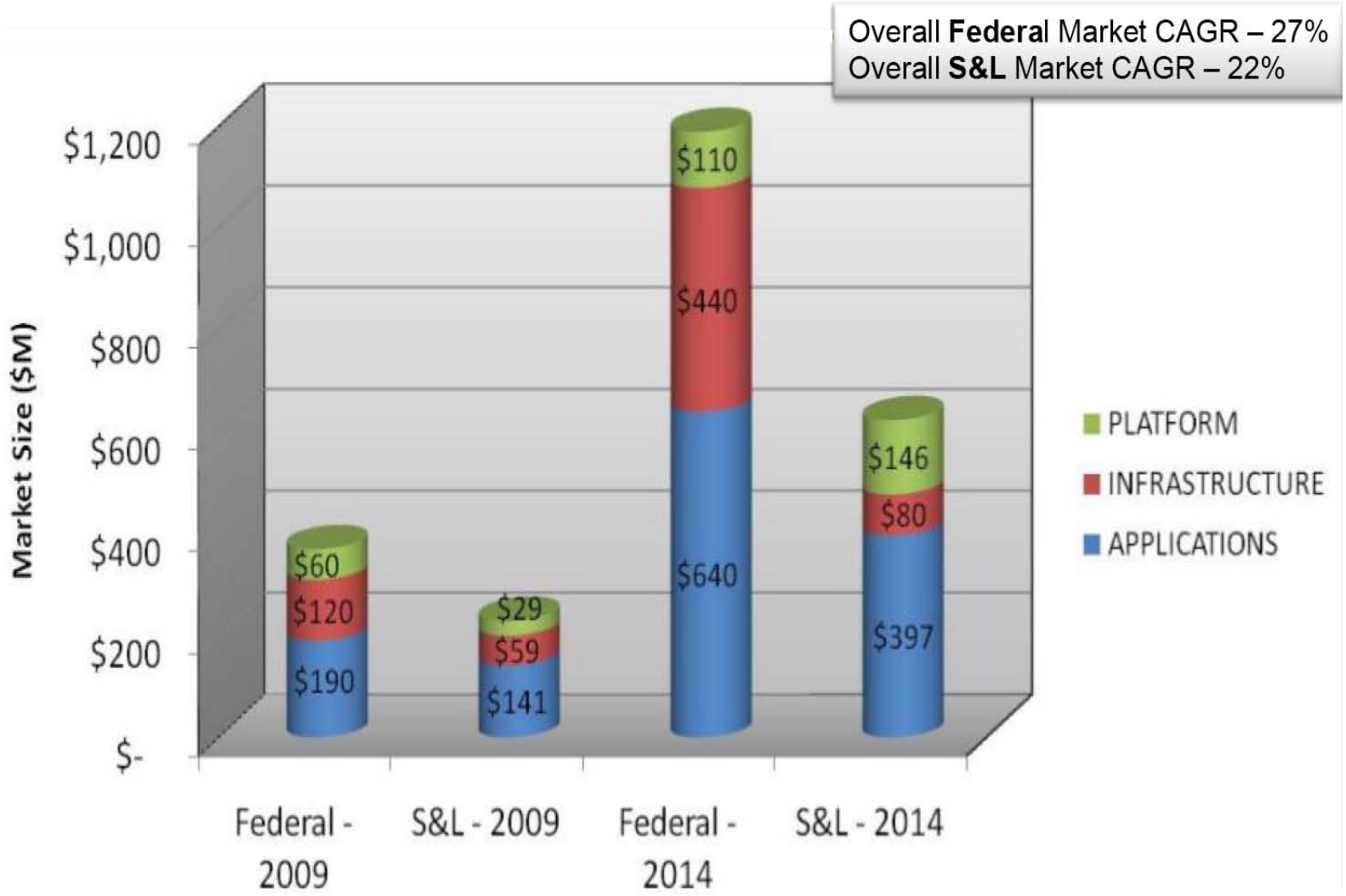
- 連邦政府最高情報責任者(CIO)Vivek Kundra氏が2009年3月に「Federal Cloud Computing Initiative」というプログラムを立ち上げ、同年9月に連邦クラウド戦略(Federal Cloud Strategy)を発表
  - クラウド採用の最大の目的はITインフラにかかるコストや環境に与える影響の抑止
  - 取組の一環として、米連邦政府一般調達局(GSA)が政府機関のクラウド・サービス利用を支援するサイトApps.govを構築

出典:IPA　H22年3月4日　クラウド・コンピューティング社会の基盤に関する研究会報告書(案)P123をもとに作成

# 米行政クラウド市場規模予測（INPUT社レポートから）

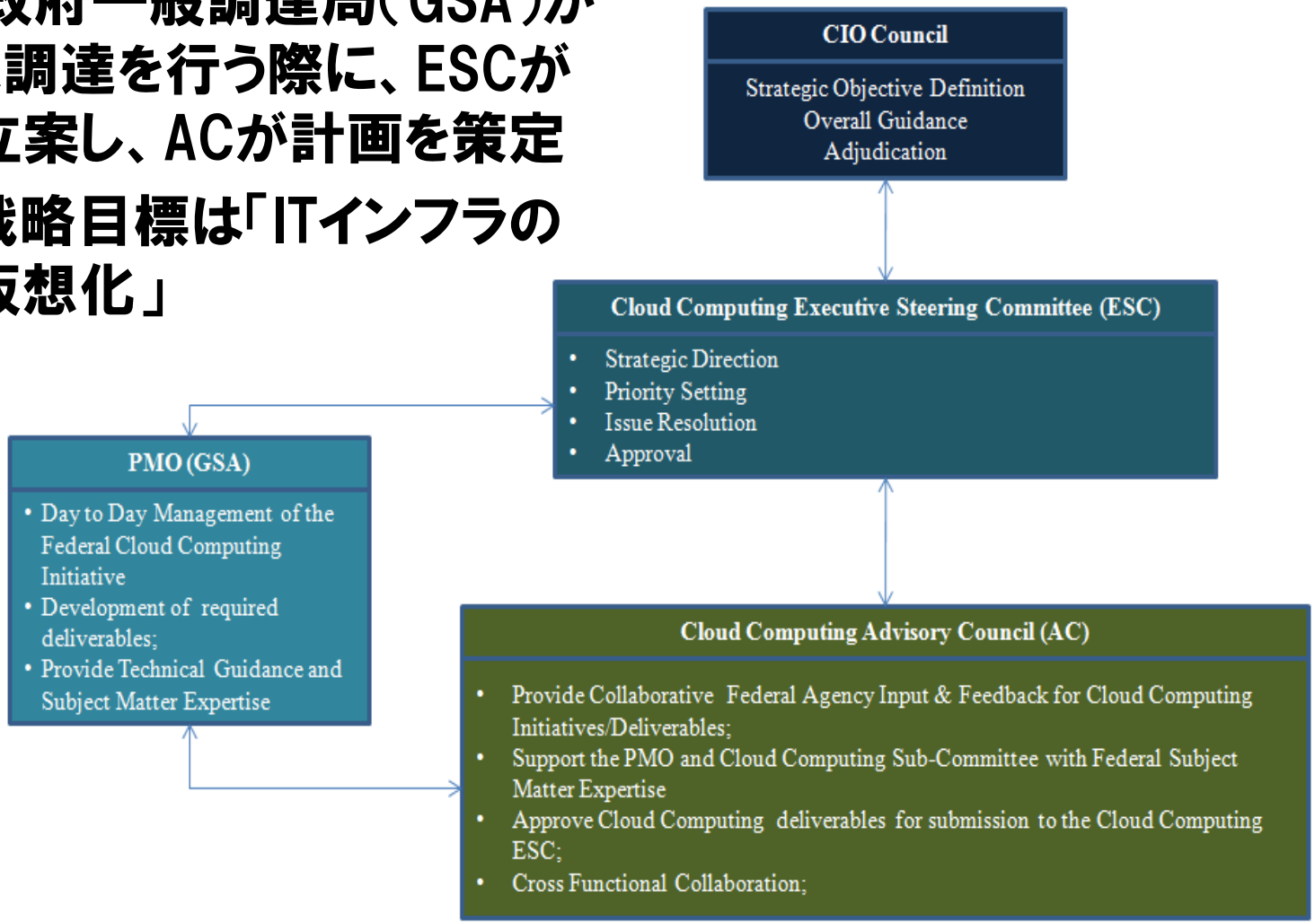
■Federal：＄310M（2009年）→＄1,190M（2014年） 約4倍

■State&Local：＄229M（2009年）→＄623M（2014年） 約2.5倍



# Federal Cloud Computing Initiativeの実施組織

- 米連邦政府一般調達局(GSA)がシステム調達を行う際に、ESCが戦略を立案し、ACが計画を策定
- 主たる戦略目標は「ITインフラの統合と仮想化」



# 米連邦政府クラウドのための重要な問題

1. セキュリティ
   - クラウドのデータ、アプリケーション、およびリソースは攻撃から守られているか?
2. データとアプリケーションのインターオペラビリティ
   - クラウドにあるデータ、アプリケーション、およびリソースは実行時にクラウド間を跨ってアクセスできるか?
3. データとアプリケーションのポータビリティ
   - データ、アプリケーション、およびリソースはデプロイメント時にクラウド間で移動できるか?
4. ガバナンスとマネジメント
   - データ、アプリケーション、およびリソースに対するポリシーをクラウドで守れるか?
5. 測定とモニタリング
   - クラウド内のアクティビティを追跡、分析そして処理できるか?
6. モバイルネットワーク
   - 様々なモバイルネットワークでクラウドリソースを活用できるか?

出典:http://federalcloudcomputing.wik.is/July_15,_2009