クラウドコンピューティングのセキュリティを考える

JNSA　NSF　パネルディスカッション

パネリスト（自己紹介）

- 株式会社IIJテクノロジー　加藤雅彦さん
- 株式会社ラック　加藤智巳さん
- グーグル株式会社　山本真人さん

モデレータ

- 二木真明 （ふたぎ　まさあき）
- 所属：住商情報システム株式会社

  戦略ビジネス事業部門新規事業開発室
  室長付　　CISSP, CISA

- 現在は、自社のクラウドビジネスを主導する立場の部署にいるが、その前の数年間、自社IT部門でセキュリティや情報システムの企画などに携わっていた。今回のパネルディスカッションはどちらかといえば、利用者目線で見たクラウドを念頭に問いかけをしてみたい。

はじめに

- クラウド(コンピューティング)を、一応定義しておきましょう。
- 米国NISTの定義の紹介
  - http://csrc.nist.gov/groups/SNS/cloud-computing/

JNSA的には、様々なビジネスがあり、なかなかクラウドという言葉の定義が難しいのですが、議論のためのベースラインとしてこれを仮置きします。

NISTの定義

Definition of Cloud Computing:
クラウドコンピューティングの定義

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. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

クラウドコンピューティングは、(任意の規模に)設定が可能な共有リソースプール(たとえば、ネットワーク、サーバ、ストレージ、アプリケーションやサービスなど)への便利でオン・デマンドなアクセスを提供するが、最小限の利用者や事業者の作業で、極めて短時間に計画、リリースができるものである。このクラウドモデルでは、5つの基本的な(クラウドの)特性、3つのサービスモデルそして4つの導入モデルについて提唱している。

NISTの定義（クラウドの特性）

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

オンデマンド・セルフサービス：利用者は、サーバタイムやネットワークストレージを必要に応じて自動的に、サービスプロバイダの人員の関与なしに、自ら設定できる。

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

広範囲なネットワークアクセス：サービスはネットワーク上で標準的な方法で利用可能であり、これにより異なるタイプのクライアント（シンクライアントを含む）から利用可能である。（携帯電話、ノートPC,PDAなど）

NISTの定義（クラウドの特性）

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

リソースプーリング：事業者のコンピュータリソースは複数の利用者のために、マルチテナントモデルを使用してプールされている。これらの物理的な、もしくは仮想的なリソースはユーザの要求に応じて、ダイナミックに割り当て、解除などが行われる。そのため、ロケーションからの独立性、つまり一般にユーザがその（ユーザが利用する）リソースの正確な所在を知ったり制御したりすることが難しいという意味合いを含んでいる。しかし、少し荒っぽいレベル（たとえば国、州、もしくはデータセンタのレベル）では特定できる場合もある。リソースの例として、ストレージ、CPUの処理能力、メモリ、ネットワークの帯域や仮想マシンなどがある。

NISTの定義（クラウドの特性）

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

リアルタイムな柔軟性：処理能力は柔軟かつ迅速に、いくつかのサービスでは自動的に調整され、（必要なリソースを）すばやく（必要に応じて）確保する、もしくは（必要な部分をのこして）解放ことができる。利用者にとっては、しばしば無制限の能力を要求でき、また必要な単位でいつでも必要な能力の調達が可能である。

NISTの定義（クラウドの特性）

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

サービス（利用状況）の計測：クラウドシステムは自動的にリソースを制御して最適化するが、これはサービスのタイプ（ストレージ、処理能力、帯域、利用しているユーザの人数など）に最適な粒度で（利用状況を）計測することで実現される。リソースの利用状況はモニターしたり制御したり、レポートすることが可能であり、これは事業者と利用者の双方にサービス利用についての透明性を提供することに寄与している。

NIST：サービスモデル（SaaS)

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

SaaS：事業者が提供するクラウド基盤上のアプリケーションを利用する形態のサービス。このアプリケーションは様々なクライアント機器からある種のシン・クライアント的なユーザインターフェイス（たとえばWebメールなどの場合は）Webブラウザ、を通じて、アクセスされる。利用者は、それらのアプリケーションが動作するネットワークやサーバなどのクラウド基盤について、特定のユーザ向けアプリケーション設定などを除いて管理する必要はない。

NIST:サービスモデル（PaaS)

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

PaaS:事業者が提供するプログラム言語やツールを使用して、ユーザが開発もしくは調達したアプリケーションをクラウド基盤上で動作させられるサービス。利用者は、導入したアプリケーションが動作するネットワークやサーバ、オペレーティングシステム、ストレージなどのクラウド基盤を管理する必要はないが、導入したアプリケーションについてはすべて制御ができ、その動作環境についても一部、制御できる場合がある。

NIST:サービスモデル（IaaS)

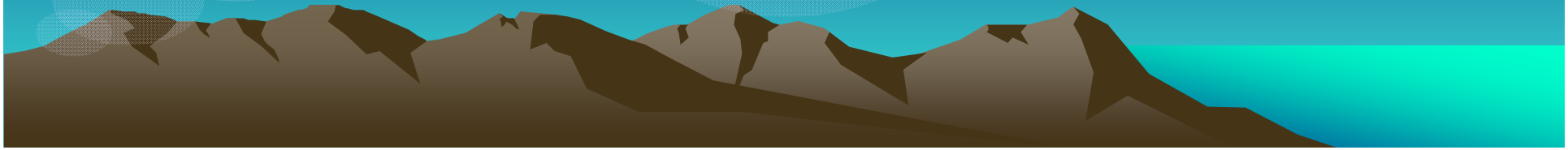
Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

IaaS:このサービスは、利用者に対して、処理能力やストレージ、ネットワークその他、基本的なコンピュータリソースなど、その上で利用者がオペレーティングシステムやアプリケーションを含む、任意のソフトウエアを導入できる環境を提供する。利用者は、それらが依存しているクラウド基盤を管理する必要はないが、オペレーティングシステムやストレージ、導入されたアプリケーションのすべてと、場合によっては、制限はあるものの、ネットワークコンポーネントのいくつかについて、制御が可能である。（例えば、ホストのファイアウォール設定など）

NIST:導入モデル（プライベート）

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

プライベートクラウド：クラウド基盤は、個々の組織について独立した形で運用される。これらは、その組織が独自に運用する場合もあれば、サードパーティによって運用される場合もあり、また、自組織のサイトに設置される場合もあれば、外部にアウトソースされる場合もある。



NIST:導入モデル（コニュニティ）

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

コミュニティクラウド：クラウド基盤は複数の組織によって共有され、共通の関心（同じミッション、セキュリティ要件、ポリシーやコンプライアンス要件など）をもつ、特定のコミュニティをサポートする。この基盤は、これらの組織が運用する場合もあれば、サードパーティが運用する場合もある。また、自組織のサイトに設置される場合もあれば、外部にアウトソースされる場合もある。

NIST:導入モデル（パブリック）

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

パブリッククラウド：クラウド基盤は、公共用に、もしくは、大きな業界レベルで利用できるように作られる。また、この基盤はクラウドサービス事業者によって所有され、（サービスとして）販売される。

NIST:導入モデル（ハイブリッド）

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

ハイブリッドクラウド：クラウド基盤は、2種類以上のクラウド形態（プライベート、コミュニティ、パブリックなど）の混成形式となる。各サービスはそれぞれ独立しているが、標準的な、または独自の技術でデータやアプリケーションのやりとりが出来るようになっている。（例、Cloud burstingによるクラウド間の負荷分散など）

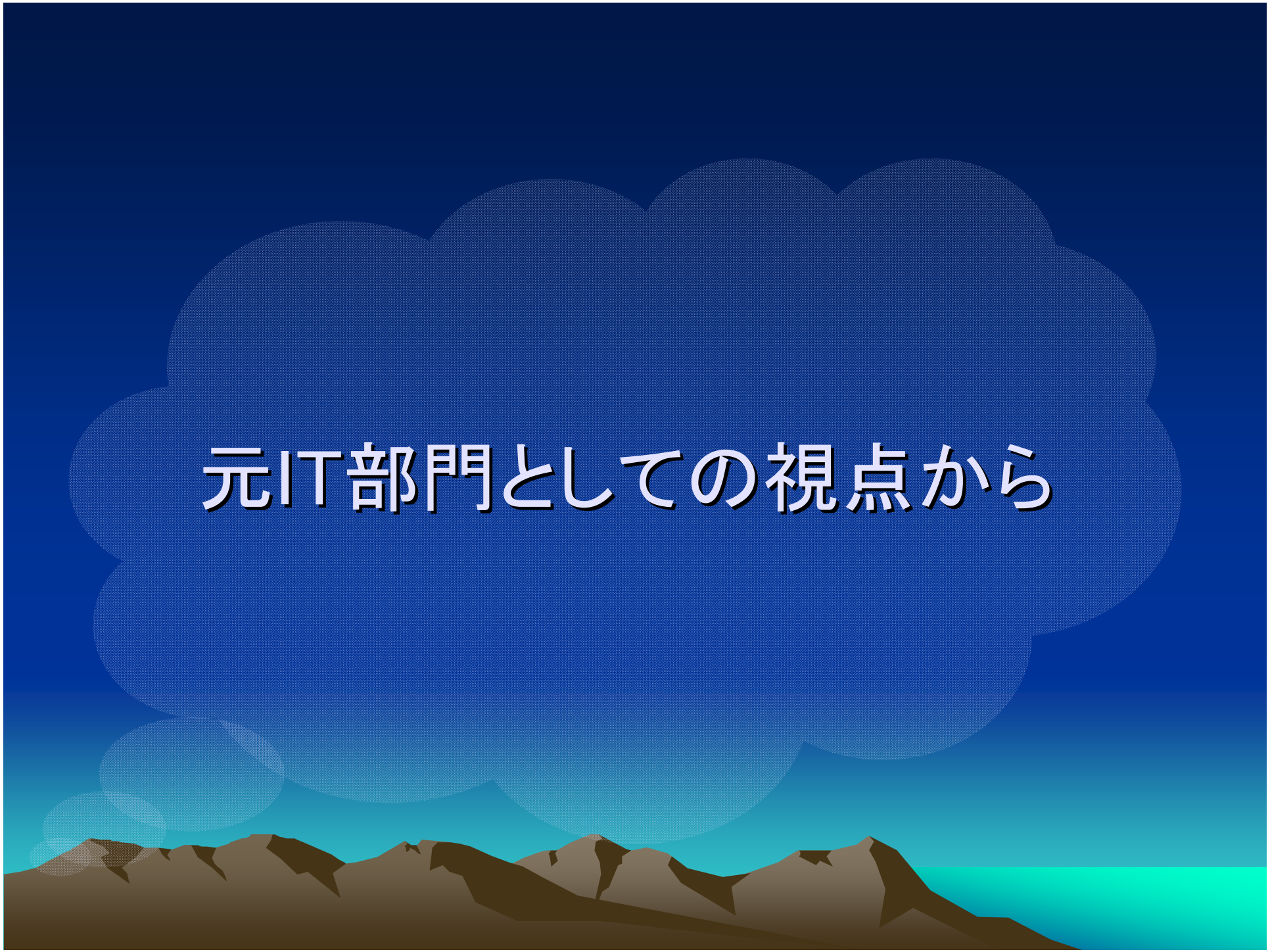
Note: Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

注：クラウドソフトウエアは、ステートレス（つまり、一連の機能が順序に依存せずに利用できること）かつ、個々の機能が相互依存なく独立に作られ、相互運用性が確保されるような形で、サービスオリエンテッド化されていることにより、クラウドというパラダイムにおける最大限の利点を享受できるものとなる。


クラウドのレイヤモデル
ビジネスエリア
ユーザニーズ
アプリケーション
サービス・サポート
ビジネス
開発・構築
ビジネス
データセンタ
ビジネス
使い勝手をもっとよくしたい、他のSaaSや既存システムと統合したい・・・
セキュリティをもっと向上させたい・・・・
高層雲
Software as a Service （SaaS）
・目的別のアプリケーション
中層雲
・Platform as a Service （PaaS）
・アプリケーション構築基盤
・仮想OS環境
・仮想データベース
低層雲
・Infrastructure as a Service（IaaS）
・大規模分散環境
・仮想化基盤
・セキュアなデータセンタ
コストを
かけずに
使いたい
コストを
かけずに
作りたい
運用コスト
保有リスク
を減らし
たい

クラウドの課題って何だろう

- 本当にコストが下がるの？
  - その代償は何？？
  - 見えないコストがあったりしない？
- クラウドのセキュリティってどうよ！？
  - 安かろう、悪かろう・・・・なの？（何が「悪」なんだろう？）
    - セキュリティ対策レベルの良し悪しよりも、保証（保障、補償）が欲しい？
    - でも、安くして・・・・ってどうよ？！！（お値段は安く、責任は重く？？）
    - ハイリスク・ロープライス　V.S　ローリスク・（ベリー）ハイプライス
      - どちらを選ぶ？
      - 利用者の責任、負うべきリスクは？
  - ブラックボックス化が不安？
    - セキュリティ認証だけじゃダメ？
  - 技術的に何か新しいもの（クラウド固有の脅威）があるのでは？
- 意外と重たい、リーガル問題


元IT部門としての視点から

IT部門は

なぜクラウド化を考えるのでしょう

ITコスト削減！！！

でも、お仕事はちゃんとしてね

IT部門とコストダウンの歴史

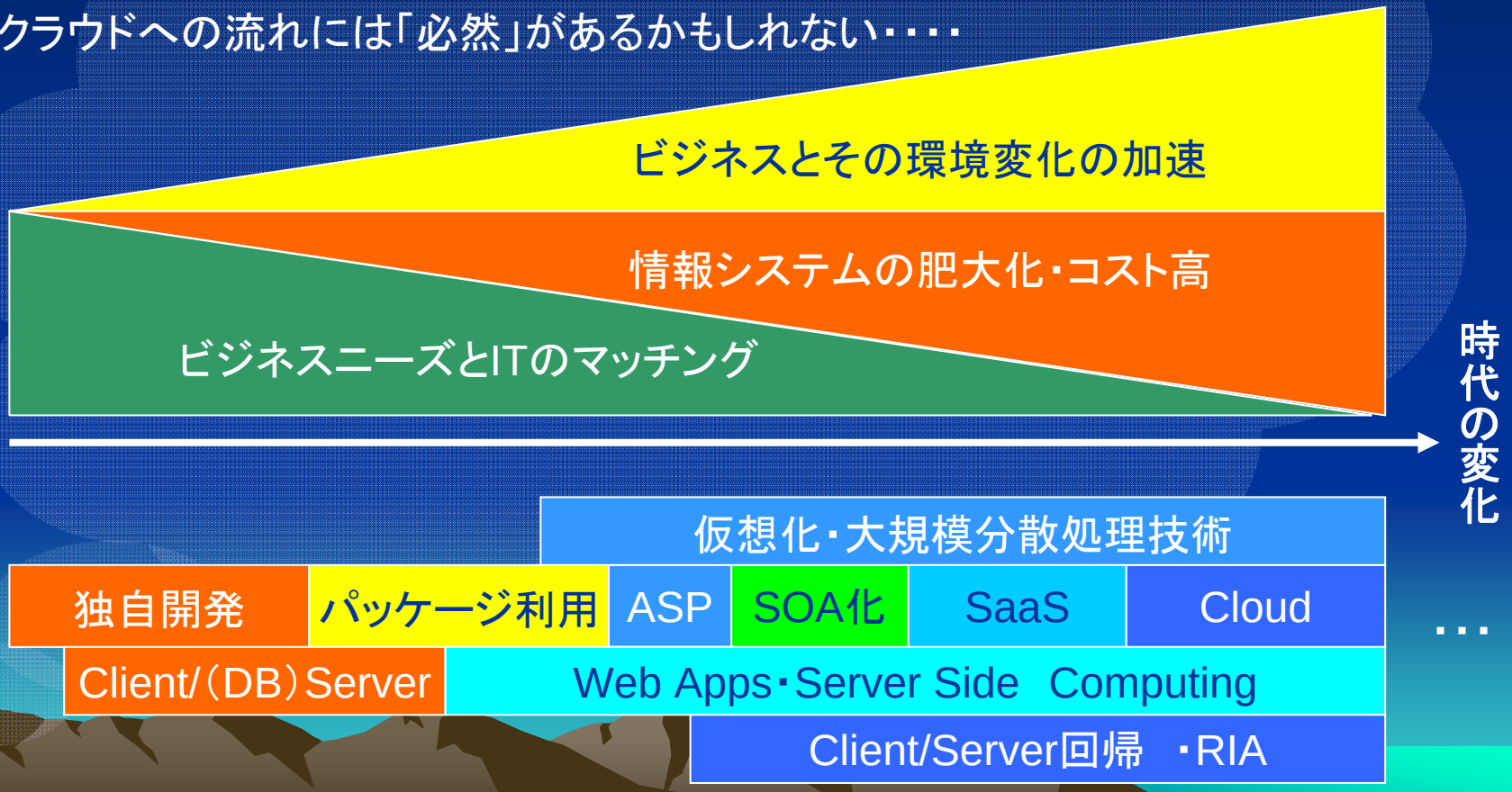
- （大昔）メインフレームからオープンシステムへの移行
  - 【メーカー縛りからの離脱、でも体質は簡単には・・・・】
- （かなり昔）自社開発からパッケージ利用へ
  - 【開発工数の削減・・・しかし、結果は？】
- （ちょっと昔）システムのオープンソース化
  - 【ライセンスフィーの削減・・でも保守コストと責任は？】
- （ちょっと昔）専用線からインターネットVPNへ・・・
  - 【回線コストの削減、でも品質は・・・？】
- （大昔～ちょっと昔）システム開発、運用のアウトソーシング
  - 【人材保有リスクの回避・人件費低減・責任●×△】
- （最近）エンタープライズアーキテクチャ、SOA
  - 【システム保守、更新コストの削減？　でも、現場からは疑問の声も・・・・】
- （そして・・・）SaaS,クラウド・・・・・・・

なんとなく仕事と一緒に責任も投げているような気もしないではないですが・・・・

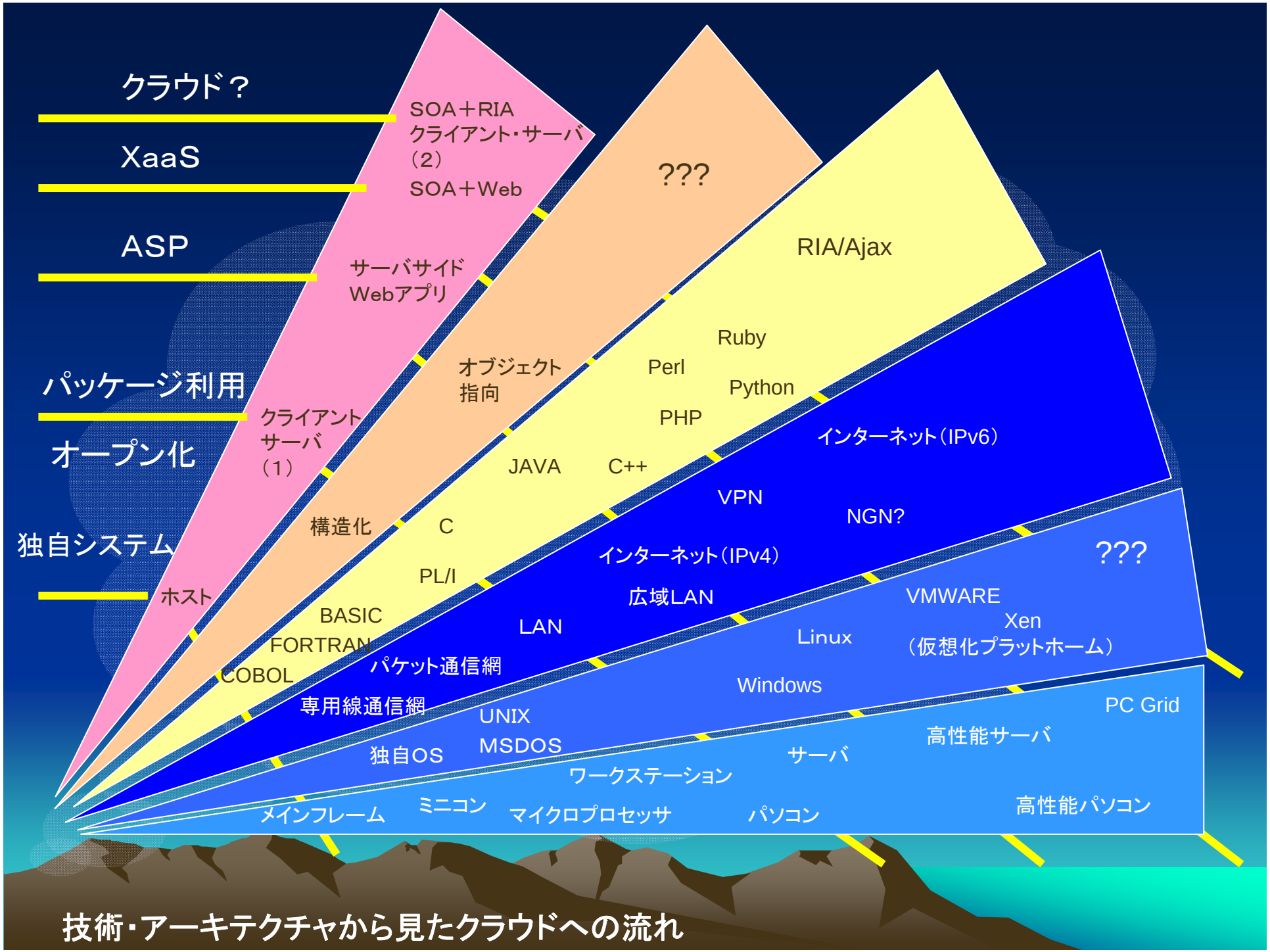
企業システムとクラウド

- IT利用の高度化とITコストの増大

クラウドへの流れには「必然」があるかもしれない・・・・



ITコストを減らし、ビジネスとのマッチングを高めるための技術


クラウド？
XaaS
ASP
パッケージ利用
オープン化
独自システム
SOA＋RIA
クライアント・サーバ
（2）
SOA＋Web
サーバサイド
Webアプリ
クライアント
サーバ
（1）
ホスト
???
オブジェクト
指向
構造化
C
PL/I
BASIC
FORTRAN
COBOL
RIA/Ajax
Ruby
Perl
Python
PHP
JAVA
C++
インターネット（IPv6）
VPN
NGN?
インターネット（IPv4）
広域LAN
LAN
パケット通信網
専用線通信網
???
VMWARE
Xen
（仮想化プラットホーム）
Linux
Windows
UNIX
MSDOS
独自OS
PC Grid
高性能サーバ
サーバ
ワークステーション
メインフレーム
ミニコン
マイクロプロセッサ
パソコン
高性能パソコン
技術・アーキテクチャから見たクラウドへの流れ

IT部門から見たアウトソース

- 本当に「コスト削減」なのだろうか
  - なんとなく、「リスクヘッジ」的な匂いも・・・（悪く言えば「責任」の外出し？）
  - でもそれをはっきり言うと、お値段がはります・・・と言われる。（ベンダの営業は決して「できません」と言わないところがミソ）
  - だから、とりあえずウヤムヤにして、「よろしく！」で済ませておくことにする。（「言外に意を汲んでね」的な・・・・「メインフレーム時代」の名残？？）
- 不景気やJSOX対応などで変わりつつある（変わってほしい）こと
  - ベンダも「無い袖」は振れなくなっている。（リソースの最小化を余儀なくされている）
  - 問題が発生した際の責任からユーザ側も逃げられなくなっている。（管理・監督責任の明確化：JSOXなどの影響）

（再）クラウドの課題って何だろう

- 本当にコストが下がるの？
  - その代償は何？？
  - 見えないコストがあったりしない？
- クラウドのセキュリティってどうよ！？
  - 安かろう、悪かろう・・・・なの？（何が「悪」なんだろう？）
    - セキュリティ対策レベルの良し悪しよりも、保証（保障、補償）が欲しい
    - でも、安くして・・・・ってどうよ？！！（お値段は安く、責任は重く？？）
    - ハイリスク・ロープライス　V.S　ローリスク・（ベリー）ハイプライス
      - どちらを選ぶ？
      - 利用者の責任、負うべきリスクは？
  - ブラックボックス化が不安？
    - セキュリティ認証だけじゃダメ？
  - 技術的に何か新しいもの（クラウド固有の脅威）があるのでは？
- 意外と重たい、リーガル問題

IT部門としての考え方

- 責任（リスク）とコストのバランスをきちんと考えて判断する
  - リスクアセスメントが大切。無視できるか、自前で対策した方が安くつくようなリスクなら、事業者には負わさず、価格（つまり事業者側の責任のお値段）を下げる。
- 最上流工程まで「まる投げ」しない
  - コンサルティングサービスを使うのはいいが、任せきるのではなく、あくまでEAのレベルまでは自分たちで、エンドユーザ・経営との合意のもとに決めたい。（下流作業に直接手をだすようなコンサルは、あまり信用したくない）
- 最小限のIT（セキュリティ）専門家（上流作業経験者）は、自社に確保しておく
  - アウトソース先やコンサルタントと技術的なコミュニケーションができないと意図が伝わらないことも多い。
  - 最新技術を意識したアーキテクチャを考えるには、それができる人材が必要。（そこそこの規模の会社なら、少なくとも2人は・・・・）
  - 事業者の範囲外の（どうやっても事業者には負えない）領域をきちんと判断して対応する必要がある。（たとえば、SaaSにおける、ユーザID,パスワード管理など）

ある意味、「理想論」であることは、承知しておりますが・・・・・・・

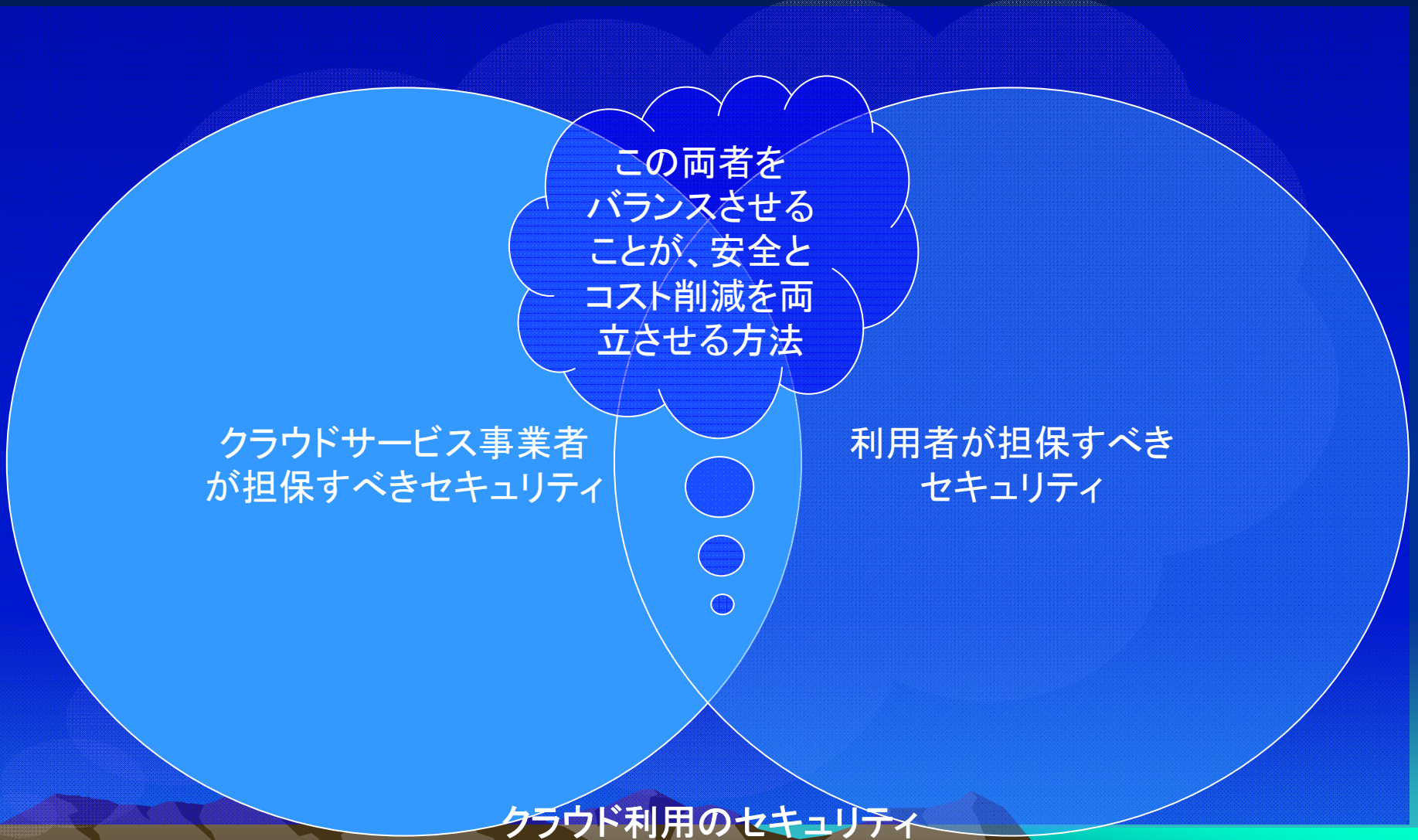
そう考えて見ると・・・・

- クラウドはIT部門にとっての変革のチャンス
  - 自社とアウトソース先との責任分担をきちんと考えるきっかけに
  - コスト削減とリスク転嫁をきちんと分離して考えるきっかけに
  - なにより、「自ら考えて行動する」きっかけに
- 是々非々で・・・・システムの「仕分け」を
  - クラウドも使えるところはどんどん使おう
  - 使えないところはきちんと判断して、他の方策を考えよう
  - 最終的に、すべて自社のアーキテクチャへの組み込みを前提に考えよう

セキュリティ屋としての立場で

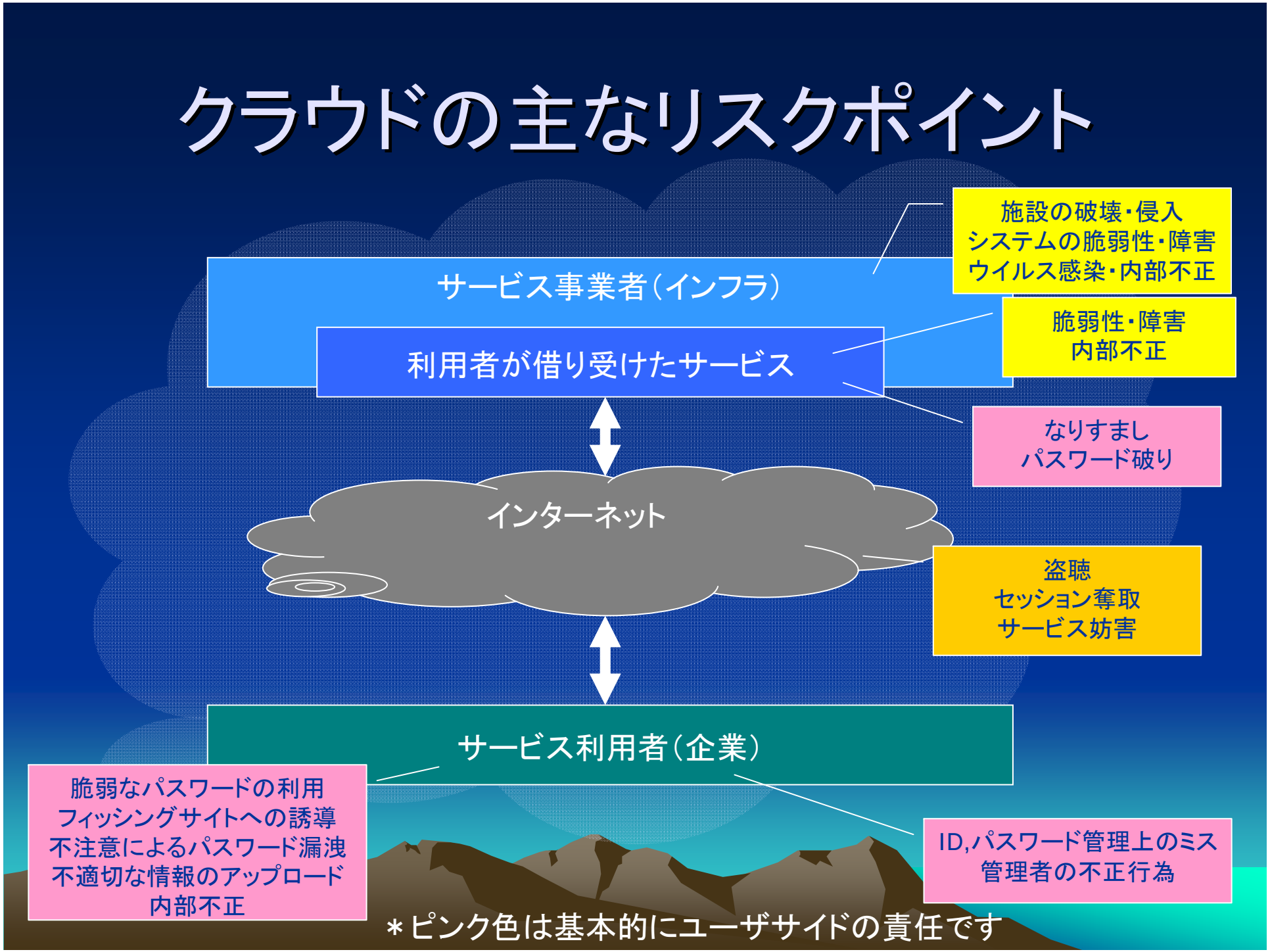

クラウド
「雲」に抱く一抹の不安
なんとなく・・・・・不安
機密データ置いても大丈夫？
ネットから使える・・って怖い
データはどこにあるの？
国外に出ちゃうのは困る・・・
どこまで管理を任せていいのだろう
どれだけ安全っても保証ないよね
セキュリティポリシーと矛盾するかも
使って大丈夫だろうか

「雲」の安全・安心をどう考えるか

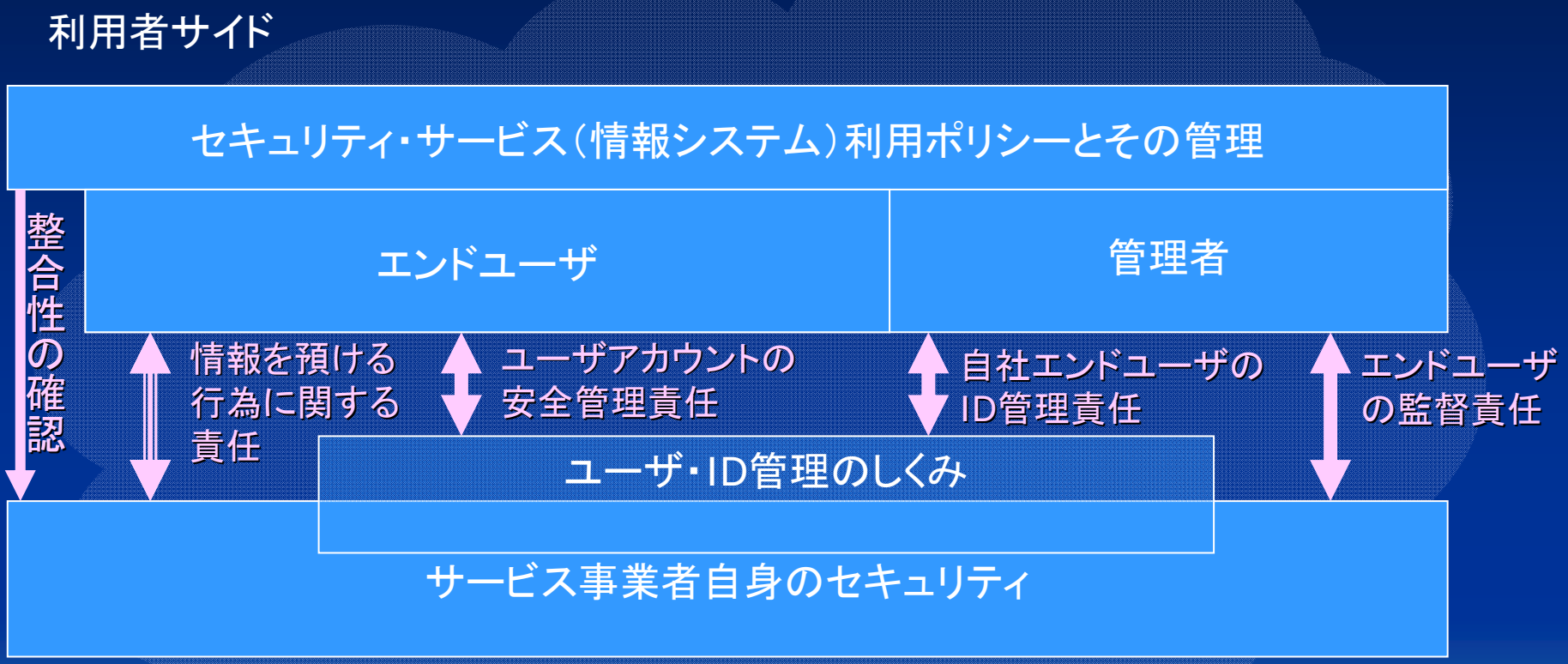


本来この話はすべてのアウトソーシングでしなければいけない話ですが・・・

クラウドの主なリスクポイント



利用者が負わなければいけない責任



これは、一般のアウトソーシングの場合と同じです。但し、クラウドの場合、一般には利用契約の柔軟性は低くなっており、自社ポリシーとの間で不整合が発生した場合、個別交渉するか、自社側で問題解決の方策を考える必要があります。

社会的な認知・制度面の問題

避けて通れない問題：リーガル

- クラウドは想定外・・・・かもしれない問題
  - レガシーな形態を想定した守秘義務、業務委託契約など
    - たとえば、情報の地理的な意味での所在を明示する必要が明記されてしまっている場合
    - 個々に契約を見直すか、情報をきちんと仕分けして管理するしかなさそう。
  - 法令、関連ガイドラインなどとの整合性問題
    - たとえば、輸出規制にかかるような情報をクロスボーダーなクラウド事業者に置くような場合
    - しかるべき筋にお伺いをたてるしかなさそう・・・・

【参考例】ハイテク情報の輸出

- 【規制の厳格化】
  - 海外駐在（在住）の自社社員（日本人）に渡す（参照させる）ことも輸出許可が必要に・・・・（日本人かつ日本在住者（出張者はOK）に限定する必要がある）
- 【クラウドを含む海外へのアウトソース】
  - アウトソース先のシステム管理・運用担当者が、その情報を参照する手段を持つ場合、輸出許可が必要。（経産省見解）
  - その手段がない場合で、かつ参照が許されないことが契約上明記されている場合は輸出許可は不要（安全保障貿易センターの見解）
  - 適切に情報が暗号化されていて、その鍵が日本在住者のみで管理されている場合（もちろん、海外在住者には見せない前提で）輸出許可は不要（安全保障貿易センターの見解）

個人的な「思い」と「願い」

- クラウドを「恐れる」のではなく「取り込む」こと
  - クラウドに至る流れには「必然」が多い。
  - 逆らっても流れは変わらない。
  - ならば、海外勢に勝てる「本当の」クラウドを作るにはどうすればいいか、それを考えることが日本のIT業界の国際競争力にもつながる。
- 安易に規制にたよらないでほしい（IT業界＋霞が関へ）
  - 「非関税障壁」を安易に作れば、日本のIT業界は一層ガラパゴス化する。それでは利用者（国民）が不幸になる。企業の国際競争力もそがれてしまう。（自動車や家電、建設業界だって世界で通用してるのに・・・・I（C）T業界は？？・・・・って言い過ぎですか？）
  - 利用者、事業者（業界）がWin/Winの関係を作るにはどうすればいいか、それを考えたい。
- 責任は等しく負うことが必要
  - 事業者、利用者のそれぞれが責任・リスクをきちんと分担して考えることが、互いにWin/Winな関係をつくる基礎となるはず

このスライドはパネルでは時間がなくて出せませんでしたが・・・・・