クラウドコンピューティングの
セキュリティとガバナンス

情報通信総合研究所　主席研究員
大阪大学工学部特任教授
ISACA国際本部　副会長
原田要之助

Disclaimer

- 本日の発表は、情報通信総合研究所の公式な見解ではありません。ISACA国際本部の副会長としての立場で、ISACAの公式見解を発表させていただきます。
- なお、ISACAはCSA及びENISAと提携関係にあり、両者の意見について代弁できます。また、ISACAとCSAは、NISTと意見交換しており、NISTの定義を基本にしています。
- 本日の発表では、日本国内でのクラウドについての用語や概念が明確でなく、事業者により、解釈が異なるところがあるので、ISACA、NIST、CSA、ENISAをベースに構成しています。
- まとめ及びエコシステムについては、原田の個人的な見解です。

目次

- クラウドとは
  - クラウドの定義（NIST）
  - クラウドの特徴
- クラウドのセキュリティとガバナンス
  - 各種のガイドラインの紹介
- エコシステムとクラウド

クラウドに対する不安

- 「問題発生時に事業者がどこまで対応するかがわからない」
- 「事業者の倒産や撤退によってサービスが停止するおそれがある」
- 「事業継続性がどこまで確保されるかがわからない」
- 「他のユーザーとリソースを共有することで、第三者に情報が見られてしまうおそれがある」
  - クラウドコンピューティングの本質的な問題点を懸念している企業も4割近い。

出所：クラウドコンピューティングについて不安に感じる点は何か?
資料:NRIセキュアテクノロジーズ

クラウドに対する期待

- 運用負荷の軽減とコスト削減に対する期待が大きい
  - 「運用負荷の軽減」(50.4%)
  - 「初期コストの低さ」(42.7%)
  - 「社内ITリソースの削減」(40.7%)
  - 「構築費用の削減」(34.8%)

- 機能面に期待する企業は、コスト削減や運用負荷軽減に期待する企業に比べて少ない。
  - 「常に最新のハードウェアやソフトウェアが利用できる」(22.7%)
  - 「可用性や情報セキュリティの向上」(19.3%)

出所：クラウドコンピューティングについて不安に感じる点は何か?
資料:NRIセキュアテクノロジーズ

NISTの定義

- Peter Mell, Tim Granceらが中心となって、定義を定期的に見直している
- 最新は、Version 15, 10-7-09
- NIST, Information Technology Laboratory
- http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

出所：NIST

NISTの定義によるクラウド

3つのサービスモデルから構成される

- Cloud Software as a Service (SaaS)
  - ネットワークを経由してアプリケーションを利用する
- Cloud Platform as a Service (PaaS)
  - 顧客が開発したアプリケーションをクラウドで提供する（そのためのプラットフォームを提供）
- Cloud Infrastructure as a Service (IaaS)
  - サーバ（処理能力）、ストレージ、ネットワークなどを借りるサービス
- 上記の複合型サービスとしてハイブリッド型（HaaS)がある
- さらに、ソフトウェアの開発を含むモデルとしてXaaSなどの新語もある

出所：NIST

SaaSからクラウドへ

- 1999年、セールスフォース・ドットコムがSalesforce CRMを提供、（SaaS）
- 2002年、Amazon Web Services(AWS)を提供
- 2006年8月、Googleが、「クラウド・コンピューティング」を提唱
- 2007年6月、ブランドダイアログが、グリッドコンピューティングを提供
- 2007年7月、セールスフォース・ドットコムがPaaSを提唱
- 2008年5月、GoogleがGoogle App Engine(GAE)を発表
- 2008年10月、マイクロソフトが Microsoft Windows Azureを発表
- 2009年2月、ブランドダイアログがグリッドコンピューティング技術を活用したSaaS型クラウド・グループウェア「GRIDY（グリッディ）」を発表。
- 2009年3月、サン・マイクロシステムズがOpen Cloud Platformを発表
- 2009年3月、Open Cloud Manifesto
- 2009年3月、CSAがガイドラインを発表

出所：WIKIPEDIA

NISTのクラウドに関する歴史認識

- “Comes from the early days of the Internet where we drew the network as a cloud… we didn’t care where the messages went… the cloud hid it from us” – Kevin Marks, Google
- 最初のクラウド：TCP/IP によるネットワーク
- 第2段階のクラウド：文書の共有(WWW の利用)
- 現在：サービス、アプリケーション、データ、これらを提供するプラットホーム
  - インターネットの専門家は
    昔から雲として表現していた

出所：NIST

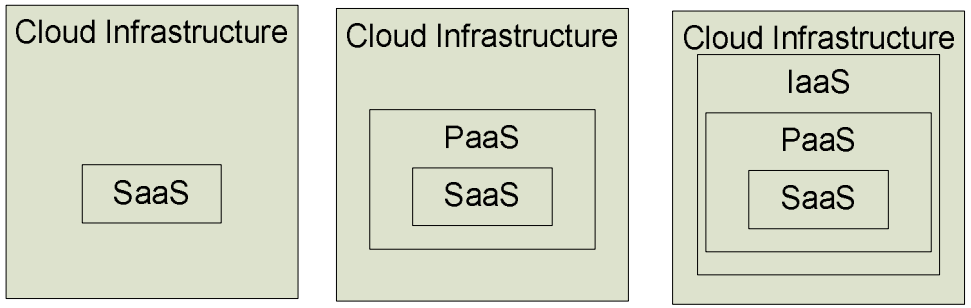
NISTの定義によるクラウドの特徴

クラウドは以下の特徴を持つ

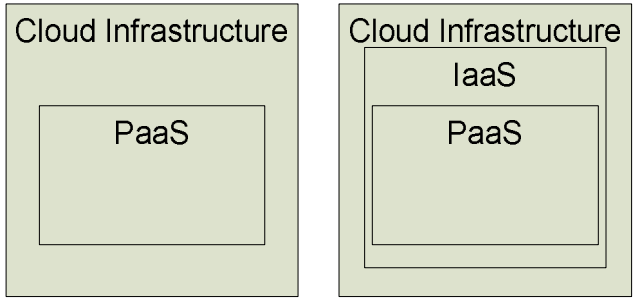
- オンデマンド（On-demand self-service）
- ブロードバンドネットワーク
- リソースの共有
  - 地理的な制約がない（地球上どこでも）
- 柔軟性
- サービス（性能）が測定可能

出所：NIST

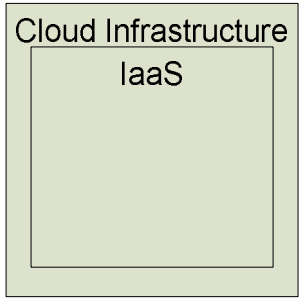
Service Model Architectures



Software as a Service (SaaS) Architectures



Platform as a Service (PaaS) Architectures



Infrastructure as a Service (IaaS) Architectures

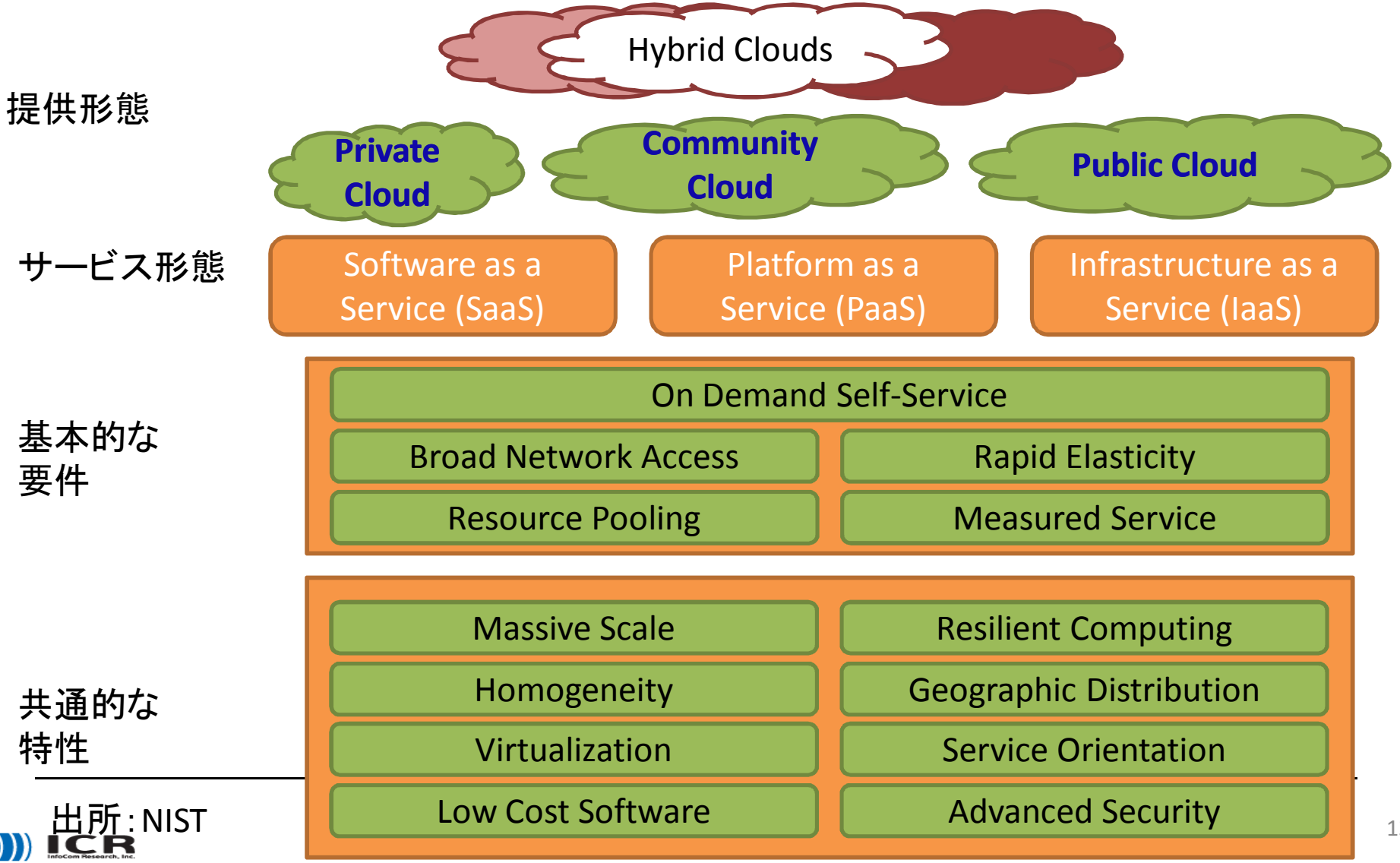
出所：NIST

NISTの定義によるクラウド提供形態

- Private cloud
  - 企業が個別に所有するなり専用にリースする
  - IP-VPNの進化形態
- Community cloud
  - コミュニティ向けのシェアードサービスのインフラを提供
  - YouTube、Mixiなど
- Public cloud
  - 一般大衆向けのインフラを提供
  - GoogleのG-mailなど
- Hybrid cloud
  - 上記の複合形態

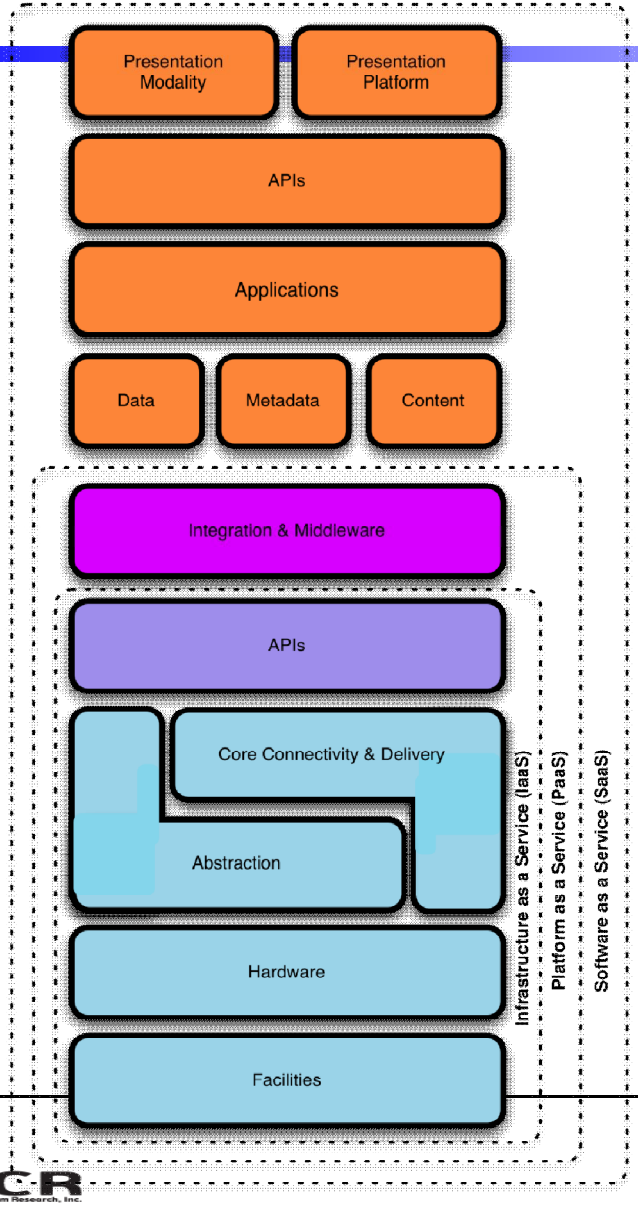
出所：NIST

The NIST Cloud Definition Framework



出所：NIST

CSAのクラウドのモデル



- CSA では、以下のように定義している
  - ーIaaS が基本
  - ーPaaSが IaaS にミドルウェアを追加
  - ーSaaS はPaaS 上で、アプリケーションを実現

出所：CSA

S-P-I モデル

You "RFP" security in

SaaS

Software as a Service

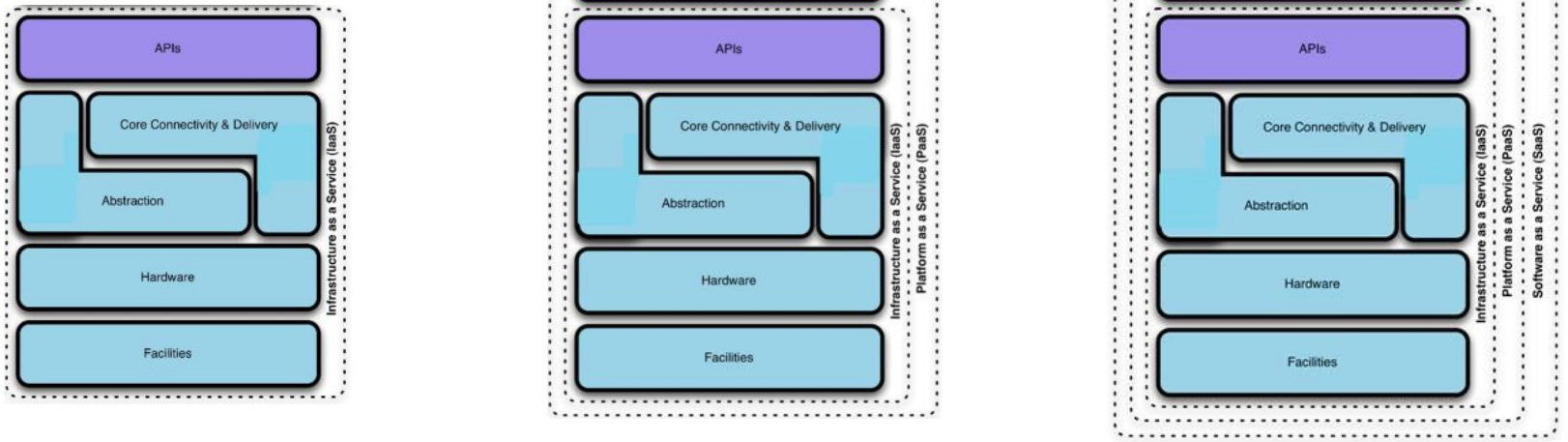
You build security in

PaaS

Platform as a Service

IaaS

Infrastructure as a Service



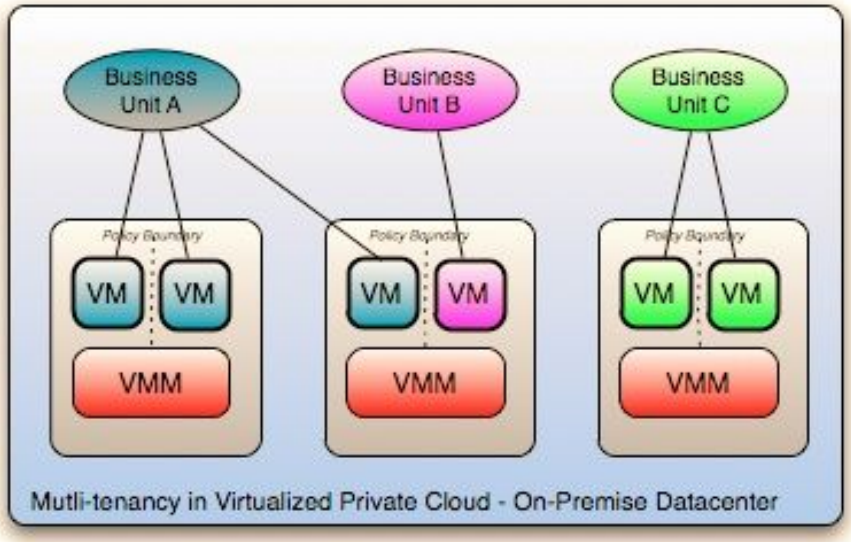
出所：CSA

クラウドの特徴

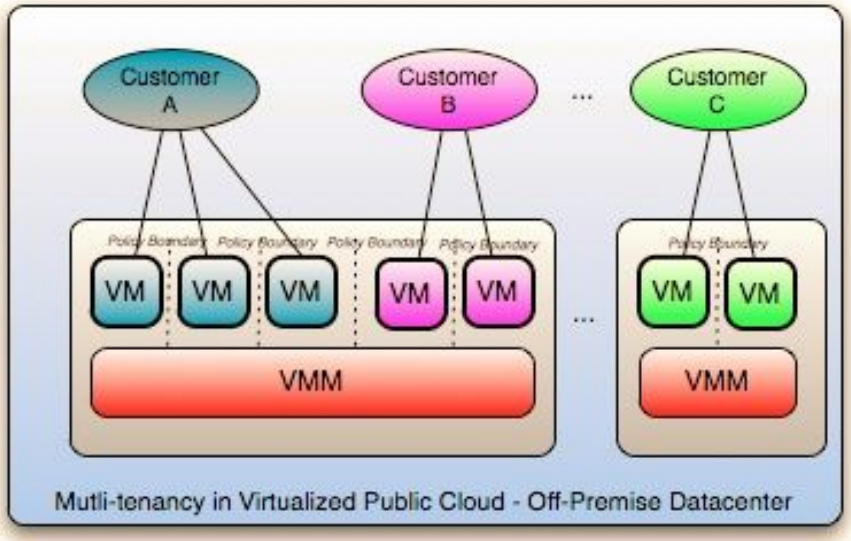
- クラウドの特徴には以下の物がある
  - スケールが自由：小規模から大規模まで提供可能
  - 仮想化：さまざまなアプリケーションを実装できる
  - 高信頼な処理：高価なサーバを共同利用
  - ソフトウェア使用料が不要
  - Muliti-tenancy：品質の違うサービスを同一のサーバで提供することができる
  - 地域的に分散：災害や需要のピークに対応
  - サービスの開始が早い：開発が不要
  - 高度なセキュリティの早期導入が可能

出所：NIST

Muliti-tenancyとは



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure



Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Muliti-tenancy：異なる企業にサービス提供する場合が基本であるが、同一の企業の異なる部門に対するサービス提供も含まれる。

出所：CSA

NISTが主張するクラウドの利点

- 内部管理の徹底が図れる
  - 企業の機密ではない情報の処理や保存をクラウドを利用することで、内部では重要な機密情報のみを管理することなり、情報漏えいのリスクを低減させる
- 監査の頻度の削減
  - クラウドを（共通的に）監査することで個別の監査を減らすことができる（SAS70-II）
- セキュリティ機能の自動化と管理の共通化
  - 情報セキュリティマネジメントを共通化（自動化）できる
- 冗長化と災害復旧
  - 個別の二重化やバックアップが不要
  - 災害復旧がやりやすい

出所：NIST

ISACAが主張するクラウドのメリット

- コストの封じ込め
  - 経営者にとってITのコストが膨張するのは感なできない。利用したITに合わせた使用料を払いたい。不要なIT機器を持ちたくない
- 即応
- 可用性
- スケーラビリティ
- 効率性
- 信頼性

出所：ISACA

NISTが主張するクラウドの課題（問題点）

- ベンダのセキュリティモデルに依存する
- 利用者はクラウドに問題があった場合に改善に無力
  - 監査での指摘事項への対応を義務にできない
- 利用者が関わる問題解決にはCSPの協力が不可避
  - ユーザの問題を解決する場合、CSPに依頼せざるを得ない
- 運用管理の報告ラインが直接ではない
  - 問題が発生しても（すぐに）知らされない
- CSPの課題の優先度付けについて口を出せない
- 物理的なコントロールが実施できない

出所：NIST

クラウドのセキュリティの論点（NIST)

- 重要なテーマ:
  - 信頼性, マルチ・テナンシー, 暗号の利用, コンプライアンス
- 視点
  - クラウドは、企業の複雑になった情報システムを単純な原点に立ち戻らせたものであり、共通的な機能とその組合せによって実現している。
- クラウドのセキュリティの課題
  - クラウドのサービスには、長所と解決すべき課題がある。

（NISTによるとセキュリティの課題は「扱いやすい」）

クラウドを支える要素技術

基本要素技術

- 仮想化技術
- グリッドコンピューティング（スマートグリッド）
- SOA
- 分散コンピューティング
- ブロードバンドネットワーク
- ブラウザ
- オープンソースソフトウェア

関連要素技術

- Web 2.0
- Web開発技術
- ファイアウォール

出所：NIST

SLA(Service Level Agreements)とは

- サービスレベルをクラウド提供者と利用者（企業）が相談して決め、契約に盛り込む
- 性能（保証）要件
  - 稼働時間、スループット（性能）、応答時間
- 運用要件
  - サービス（構成）変更への対応時間
  - 問題対応能力（問題解決までの時間）
- セキュリティ要件
  - 情報の管理（機密漏洩や不正アクセスの禁止）
- 違約条件

SaaSとは

- スケーラブル
  - 作業量の増加に柔軟に対応できる
  - 利用したサービスに応じたコスト負担
- 共同利用型（サービス）
  - アプリケーションが多数の顧客企業に提供できる
  - ホスティング（個々の顧客企業がそれぞれサーバをデータセンタに設置して利用する形態）とは異なる
- サービスのカスタマイズ
  - 顧客のアプリケーション（プログラム）を開発するのではなく、顧客が利用できるパラメータを変更してカスタマイズする

出所：NIST

クラウドとアウトソーシングの違い

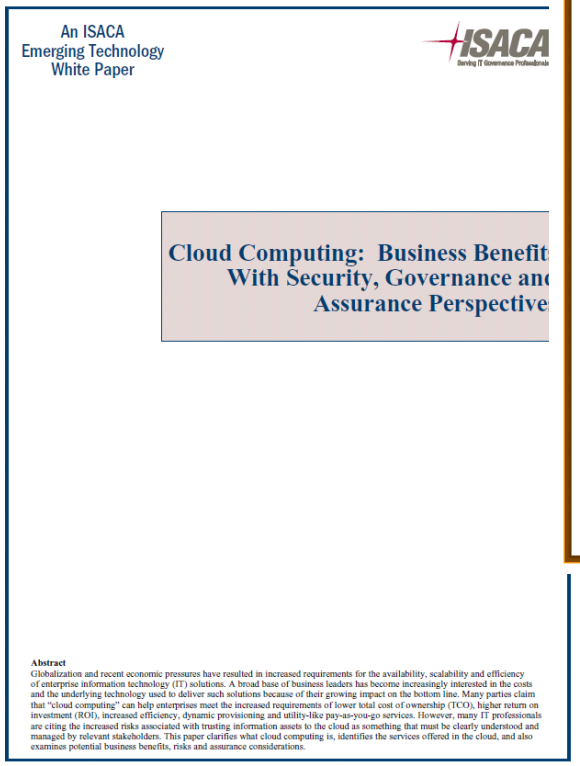
- IaaS & PaaS – NISTは違うとしているが、
  - データセンタのホスティングサービスでユーザ機器の運用管理を実施している場合、運用・保守のアウトソーシング
- SaaS –NISTはアウトソーシングと位置づけている
  - 理由として、複数の事業者に対してスケーラブルなサービスを提供している
  - 日本では、通信事業は約款でサービス提供されており、アウトソーシングにはならないケースもある

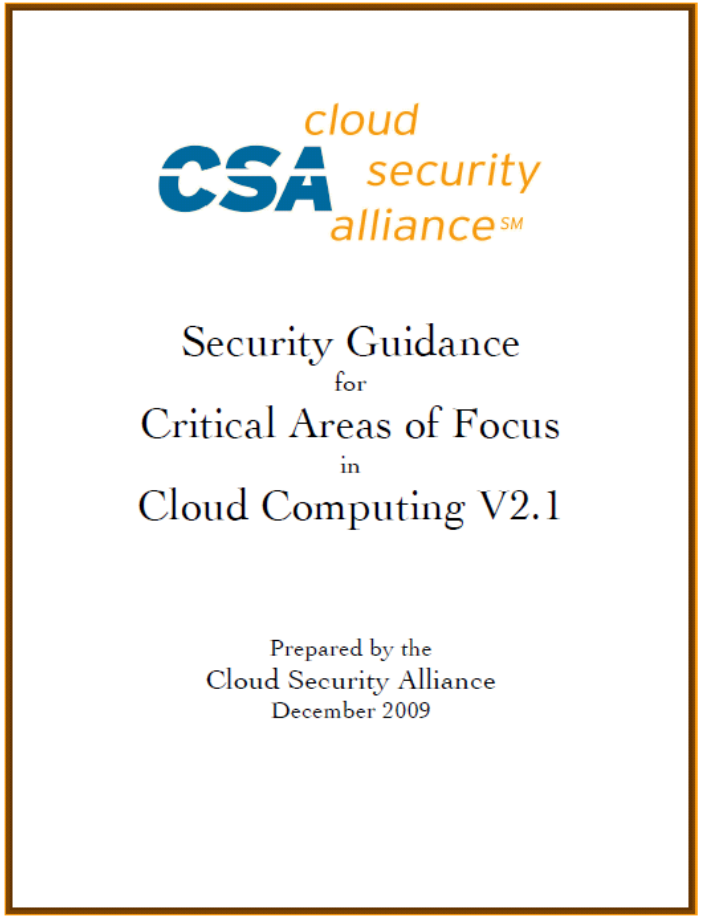
出所：NIST

クラウドに関する標準化、団体、主要機関

- CSA（Cloud Security Alliance ）
- ENISA（EU の調査研究機関）
- ISACA（IT audit and tools）
- OWASP（web-specific issues）
- Distributed Management Task Force (DMTF)
- 標準化
  - ISO
    - SC38
  - 通信分野
    - ITU
    - ETSI (The European Telecommunications Standards Institute)
  - National Institute of Standards and Technology (NIST)
  - Storage Networking Industry Association (SNIA)

クラウドのセキュリティに関するガイドライン





ICR
InfoCom Research, Inc.

CSAのガイドライン

- クラウドの構造
  - クラウド・コンピューティングの構造的フレームワーク
- クラウドのガバナンス
  - ガバナンス及びエンタープライズ・リスク・マネジメント
  - 法的課題及び電子的証拠開示手続
  - コンプライアンスと監査
  - 情報ライフサイクル・マネジメント
  - ポータビリティと相互運用性
- クラウドの運用
  - 伝統的なセキュリティ、ビジネス継続、及び災害復旧
  - データセンターの運用
  - インシデントレスポンス、被害の通知、及び被害からの救済
  - アプリケーションのセキュリティ
  - 暗号利用と鍵管理
  - アイデンティティとアクセス管理
  - 仮想化

出所：CSA

ENISAのリスク分析結果から

- インシデントの発生頻度とビジネスへの影響を考慮して、クラウドについて分析している
  - Low risk: 0-2
  - Medium Risk: 3-5
  - High Risk: 6-8

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

We have based the estimation of risk levels on ISO/IEC 27005:2008 (10).

出所：ENISA

ENISAによるクラウド関係のリスク1

組織的なリスク

	リスク評価結果
R1　ロックイン	
R2　ガバナンスの喪失	
R3　コンプライアンス対応	
R4　共同サービスの提供による企業価値の低下	
R5　クラウド・サービスのサービス停止及び障害	
R6　クラウド・プロバイダーの買収	
R7　サプライ・チェーンのトラブル	

出所：ENISA

ENISAによるクラウド関係のリスク2

技術的なリスク

R8　リソースの問題(不足又は過剰)
R9　独立性（サービスの共有から来るPublic Cloudの問題点）
R10　内部者の悪意、管理者の特権濫用
R11　管理者機能の悪用（Public Cloudの管理機能の弱点）
R12　データの妨害
R13　データ漏洩（データの転送時）
R14　データの不確実又は非効果的な消去
R15　DDoSへの対応
R16　EDOS(利用者のリソースの不正利用)への対応
R17　暗号鍵の紛失
R18　悪意あるスキャン
R19　サービス提供の欠陥
R20　顧客とクラウドでのセキュリティ対策の違いからくる問題

リスク評価結果

出所：ENISA

ENISAによるクラウド関係のリスク3

法的なリスク

		リスク評価結果
R21	法令による命令や証拠保全	
R22	裁判管轄の違いによるリスク	
R23	データ保護に係るリスク	
R24	ライセンスに係るリスク	

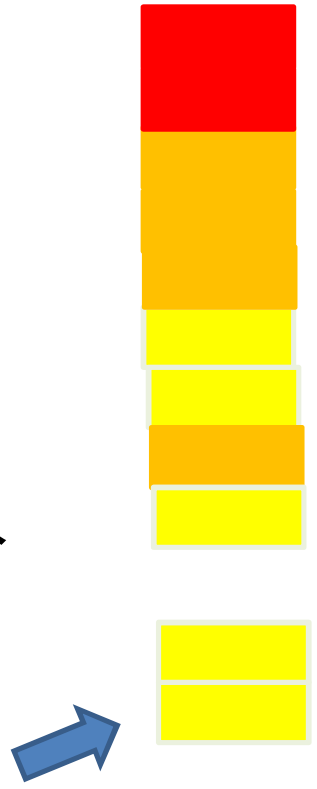
出所：ENISA

ENISAによるクラウド関係のリスク4

共通事項

R25	ネットワークのダウン
R26	ネットワーク管理(例、輻輳/誤接続/不適切利用)
R27	ネットワークトラフィックの経路変更
R28	権限奪取（root 権限を奪われる）
R29	ソーシャルエンジニアリング攻撃
R30	ログの滅失又は漏洩
R31	セキュリティ・ログの滅失又は漏洩
R32	バックアップの毀損、盗難
R33	構内への無権限アクセス(装置やその他の施設への物理的アクセスを含む）
R34	機器の盗難
R35	災害

リスク評価結果



日本との違いに注目

出所：ENISA

ENISAが提唱する責任分解について

	Customer	Provider
Lawfulness of content	Full liability	Intermediary liability with Liability exemptions under the terms of the E-commerce Directive (1) and its interpretation.[1]
Security incidents (including data leakage, use of account to launch an attack)	Responsibility for due diligence for what is under its control according to contractual conditions	Responsibility for due diligence for what is under its control
European Data Protection Law status	Data controller	Data processor (external)

出所：ENISA

ENISAの勧告から

- クラウドにおける信頼関係の樹立
  - クラウドの認証と標準化（CobiT、ITILなど）
  - クラウドのROI
  - 適切なセキュリティレベルを保証するための透明性のある手法
- 大規模なクラウドのデータ保護の必要性
  - データ（情報）のライフサイクル
  - 管理するデータ（情報）のCIA
  - （データ）のフォレンシクスと（不正などの）証拠収集機能
  - 多国籍クラウドが機能するような法制度
- 大規模な情報システムについてのエンジニアリングの確立

出所：ENISA

法的な問題（NIST）

- 規制、法律、契約（民事）など法的な観点が必要
  - 未整備な分野が多く、当面は、アウトソーシングや委託契約をベースに展開することになる
- 契約、約款（SaaSの場合など）
  - サービス提供に関する取り決め
  - 契約の変更や中止とそれに伴う条件
- CSPの情報開示
  - 情報セキュリティに対する取り組みや認証など
  - 利用企業による監査
- CSPによるデータの二次利用
  - CSPによる監視業務から副次的に得られるデータを含む（例　アクセス先のモニタリング）
  - 守秘義務（ユーザ企業に提供しているサービスでクラウドが作成する中間データ）

出所：NIST

法的な勧告（ENISA）

- データ保護
- データセキュリティ
- データ移送（転送）
- 施行法令の確認
- 機密保持と守秘義務
- 知的所有権の保護
- リスクの分担と責任の限定
- コントロールを変える場合の契約見直し

出所：ENISA

クラウドの監査（ISACA）

クラウドコンピューティングの監査への考慮
（Assurance Considerations for Cloud Computing）

- 統制性と説明責任
- 個人情報の保護
- コンプライアンス
- 国境を超えるデータの流れ
- 情報セキュリティに関する認証

出所：ISACA

クラウドの課題（監査の観点から）

Figure 1—Cloud Computing Service Models		
Service Model	**Definition**	**To Be Considered**
Infrastructure as a Service (IaaS)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.	Options to minimize the impact if the cloud provider has a service interruption
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider	• Availability • Confidentiality • Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite) • Data ownership • Concerns around e-discovery
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).	• Who owns the applications? • Where do the applications reside?

出所：ISACA

まとめ　クラウドをめぐる脅威

- 技術（Technology）
  - 技術進歩をどのようにサービスに織り込むか
  - 仮想化による見えない技術部分が多く、現場の技術者の対応が困難
  - 利用企業のミスユースによる問題
  - 管理技術の複雑化
- ビジネス
  - クラウドのサービス競争：新規事業者は新しい技術でサービス競争に挑んでくるため、常に新しい技術を見据えたサービス開発が必要）
  - 利用者のニーズ（エンドユーザに向けたサービスを考える必要がある）
- セキュリティ
  - 既存の脅威（Malware、Virus）への対応が必要
  - 新しい攻撃への対応

まとめ　監査の必要性

- 情報セキュリティ対策の有効性
  - 保証型監査が必要
- データの管理
  - 情報管理体制（個人情報保護法では委託先の監督義務）
  - データの分類とそれに応じた機密保護の要請（JIS Q 15001：2006（個人情報保護マネジメントシステム））
- コンプライアンス
  - データの移転が制限されている（EU）
  - 関連する法令に準拠している
- 認証や委託先評価（ISMS、SAS 70 IIの利用）
  - 分りやすい共通的な評価機能が必要

まとめ　コンプライアンス

- CSPのコンプライアンスに関する姿勢、取組み。
  - 例えば、個人情報保護法が厳しいので、法の適用を避けるために、法の適用の弱い他国でデータを保管したり処理したりしている場合、企業にはコスト低減を図ることができるものの、利用企業側にも法的リスクが生じる可能性がある
- CSPのSLAへの準拠
  - サービスの性能面の評価が難しい。客観的なパラメータで双方が合意することが必要

データの国境を越えた問題

- EUのデータ保護法では、個人情報などの保護すべきデータについては、国境（EU域外）を超える場合、転送先の保護レベルがEUと同等なレベルを要求
  - EUから十分な保護水準を確保していると認められた国・地域、スイス、カナダ、アルゼンチン、ガンジー島、マン島、ジャージー島
  - 米国：包括法がないため、特定の認証基準を設け、その認証を受けた企業ごとにセーフ・ハーバー協定をEU内企業と締結
  - 日本、オーストラリア
    - EUが十分な保護水準を確保していると認めていない
    - 日本への個人データの移転の都度「標準契約条項」への適用及び、EU当局への届け出でが必要
    - 航空会社の搭乗者リストなどは例外の扱い

まとめ　運用面の情報セキュリティ

- データ漏えい
  - 運用者の管理
- 性能
  - 利用企業のピーク特性の考慮
- ウイルスやマルウェアの影響
  - ITは共用しているリスクが存在する
- バックアップ
  - バックアップの方法と暗号の適用
- データのリテンション
  - フォレンジックとしてのデータの保全

事業継続

- 企業側は、クラウドサービスの停止を見込んだ事業継続計画を策定できるか。
- CSPの事故や災害によってサービスが停止する
- CSPが倒産してサービスを中止したり、事故でサービス中断が起きる
- ビジネスへの影響を低減できるか

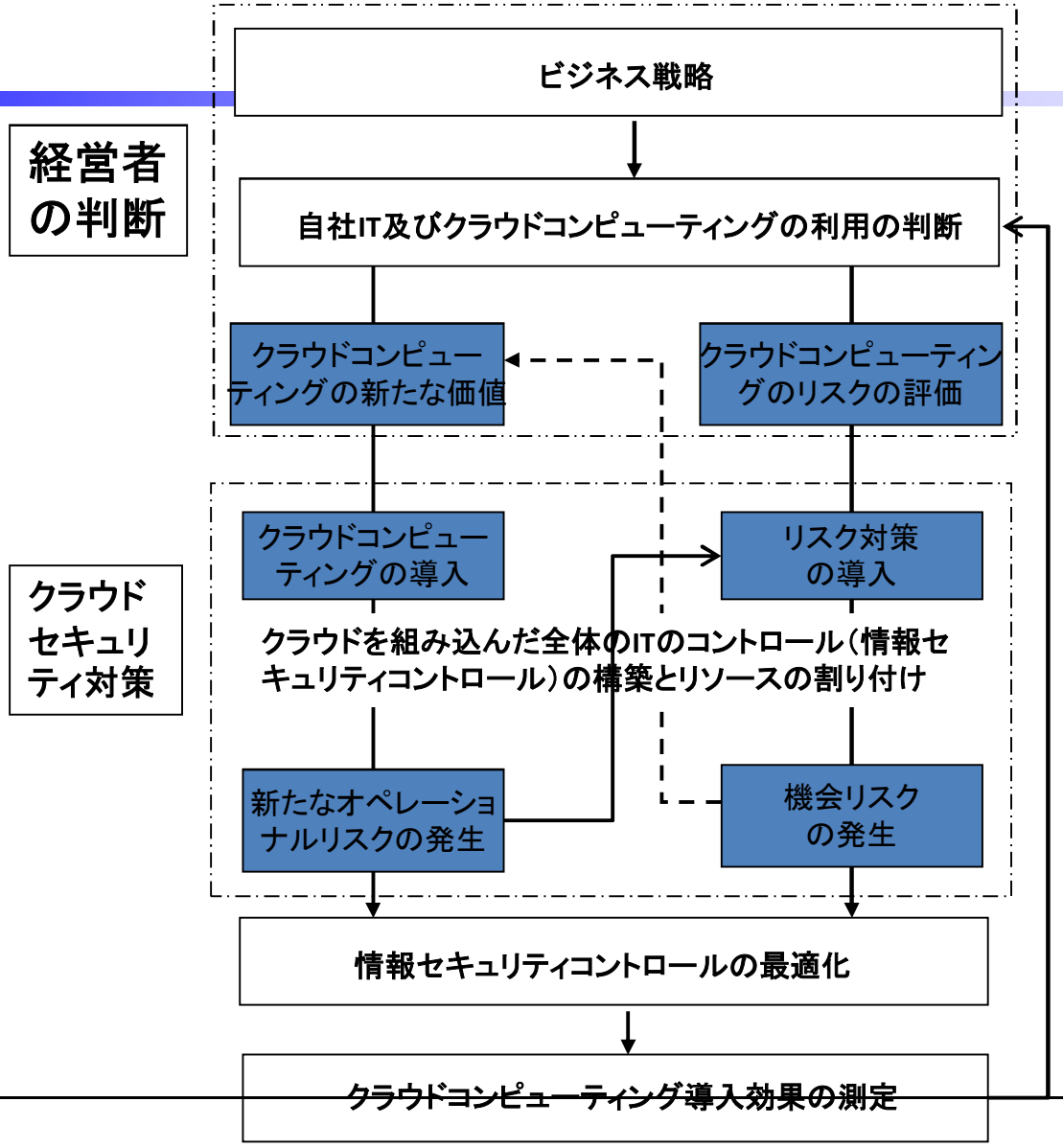
ガバナンスとリスクマネジメント

- クラウド利用によるコスト削減だけで十分なのか？
  - CSPをコスト削減だけと考えると、CSPはコスト削減の観点から国外に逃避する可能性がある→社会的なコストとして跳ね返ってくる
- クラウドの利用によるリスクは本当に提言になるのか？
  - CSPは、多数の事業者を対象にセキュリティ管理をシンプルするため、セキュリティリスクの移転にならない可能性もある
- CSPの透明性？
  - 利用する事業者や他のプロバイダへの依存が見えない
  - CSPの経営基盤の脆弱性
- CSPの説明責任？
  - CSPの能力不足（実力が伴わ合ない可能性がある）
- CSPの柔軟性？
  - クライアントの要求への対応（複数社からの要請ならば受け入れる）

ガバナンスの観点（利用企業）

- IT（情報処理）に係るコストの低減
  - 提供されるサービスの内容とコスト
  - 提供される情報セキュリティのレベル
- リスクの移転
  - 運用面の情報セキュリティ
  - コンプライアンス
  - 事業継続
- 自社のどの部分にクラウドを提供するか
  - アウトソーシング、運用の外部委託との違いの認識
  - 専門性なのか、コストなのか
  - CSPへのロックインの課題

CSPを利用する企業のガバナンスモデル



出所：ISACA

CSPを選定する場合に考慮すべき情報セキュリティ

- サービス利用のリスク
- （ブロードバンド）ネットワーク（速度）
- アクセス管理機能
- サービス管理機能
- データ管理のリスク
- 契約（SLAを含む）の考慮

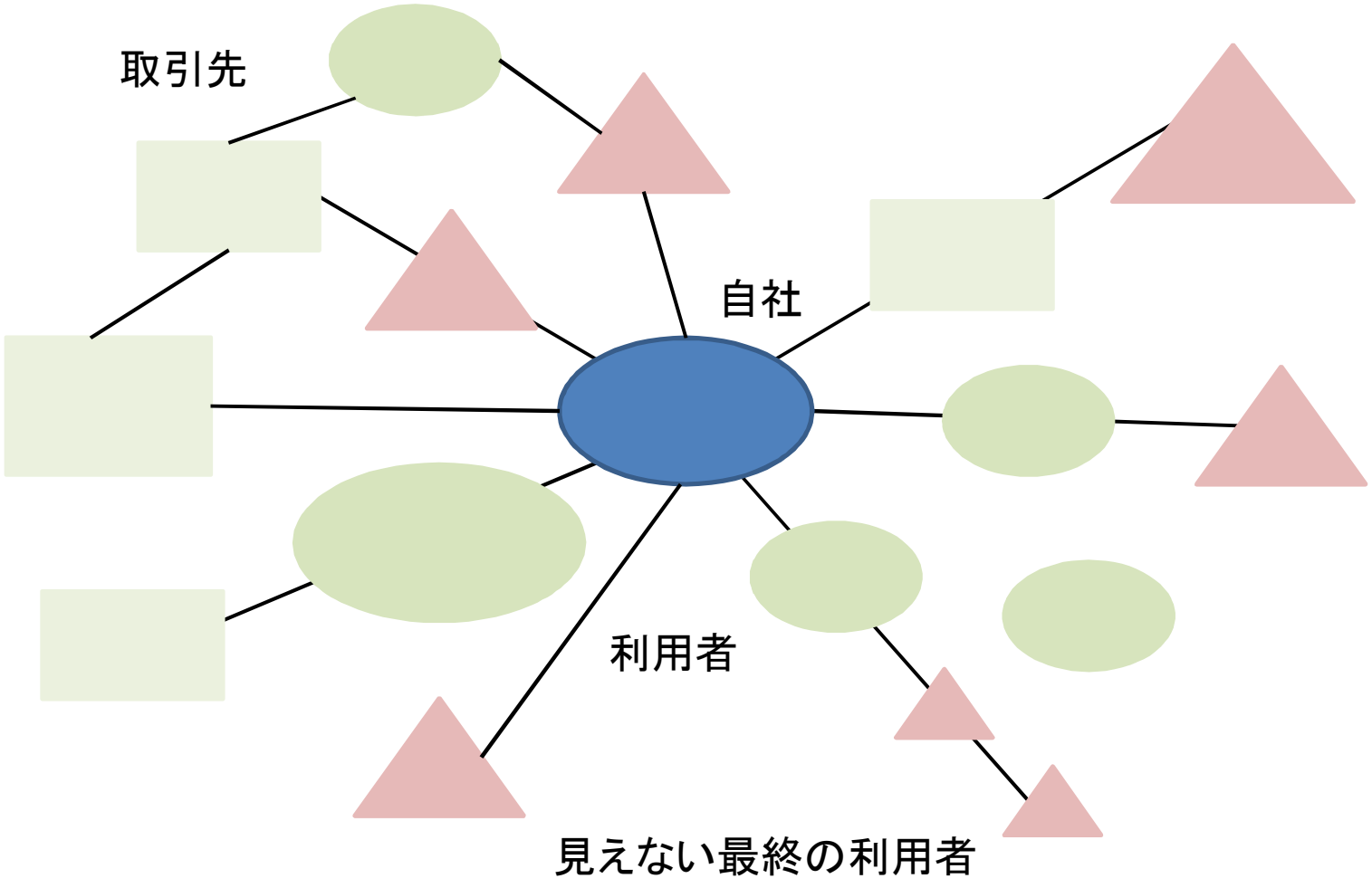
ガバナンスの観点（クラウド事業者）

- CSPの経営問題（経営破たん、M&A）
- CSPの技術戦略
  - ベンダのITにロックインされない
- CSPの情報セキュリティ体制
  - 認証の取得（ISMS、SAS-70、PCIDSSなど）
  - 事故情報などの公表（透明性）
- CSPの事業継続計画（災害、事故への対応）
  - コンプライアンスと契約やSLAの遵守
- カントリーリスク
  - Data Centers を設置した国の法律が変わる（例　スイスの銀行が顧客データを開示するようになった）

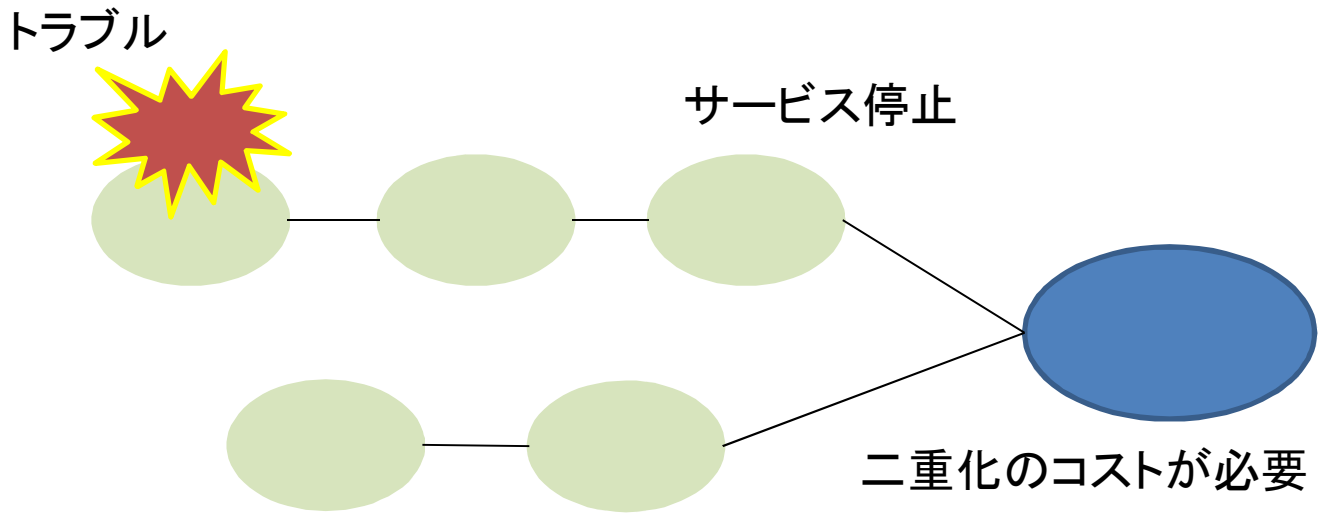
エコシステムとは

- 「エコシステム」とは、植物、動物又は微生物の群集とこれを取り巻く非生物的な環境とが相互に作用して一の機能的な単位を成す動的な複合体をいう」
- エコシステムアプローチでは、生態系の複雑で動的な本質に対応し、生態系の機能に関する完全な知識と理解の欠如に対応するために順応的管理が求められる。

自社を囲むステークホルダ



サプライチェーンの課題

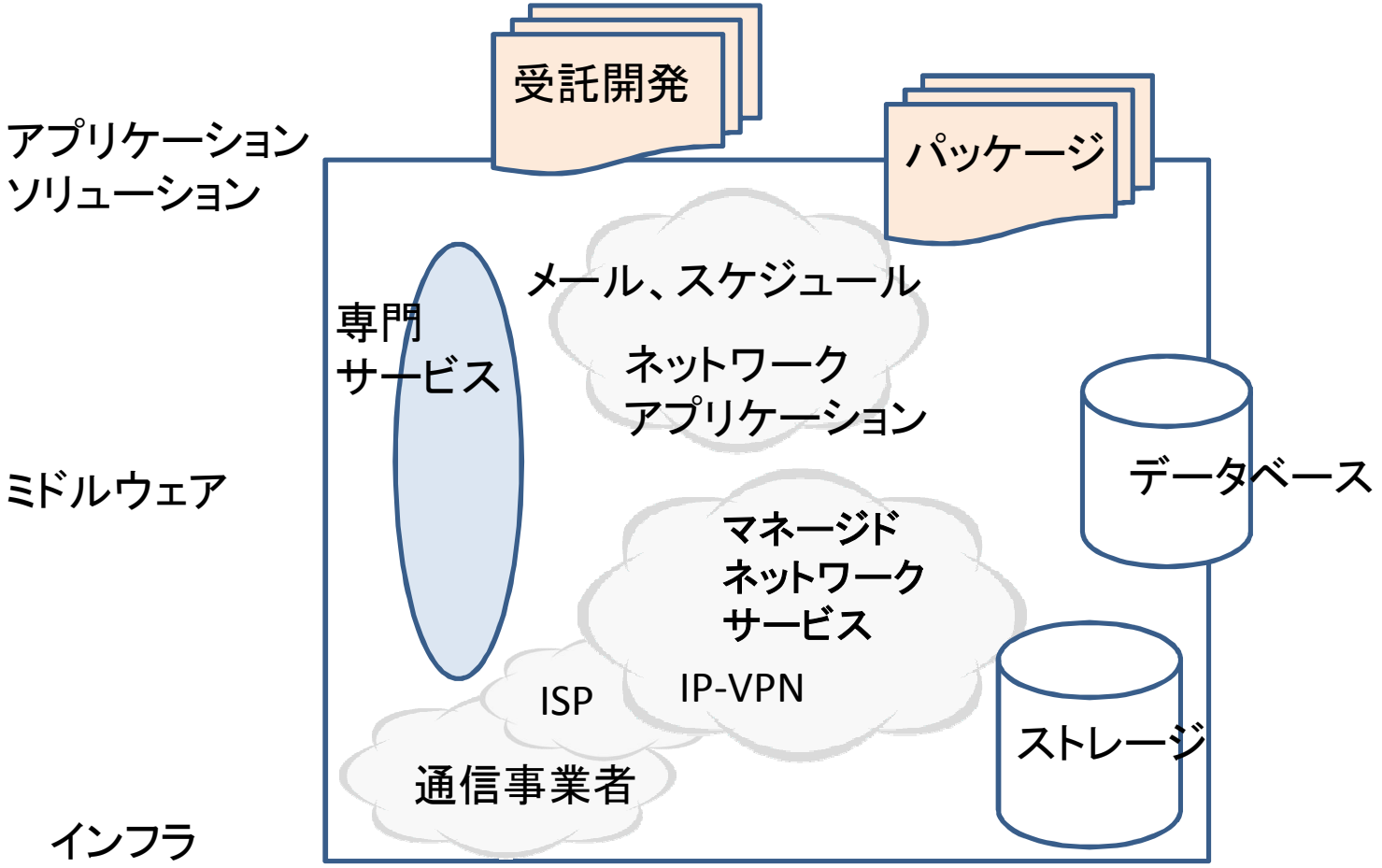


取引先のトラブルが自社に及ぼす影響を考える必要がある。

しかし、CSPの多くも他のCSPに依存

CSPの二重化を考えるのも必要であるが、本当にコスト的に優位なのか？

クラウドの世界はエコシステム



情報通信を含んだ形で変遷していくダイナミックなシステムを考える必要がある

エコシステムとして成長するためには

- 標準化が必要
  - オープンなインタフェース条件
  - 情報セキュリティ条件
  - 事業継続
- 契約の体系化（テンプレート）
  - SLAの体系化
- 業界としての自主規制
  - データの管理に対する規制
  - 紛争解決のための機関の設置
- 法令や規制
  - 国境を超える場合の国家・地域間での法律の整備
  - 犯罪の際のクラウドへの捜査権、データの開示
  - エコシステムが根付くまでの非対称規制（大規模事業者への規制）
- 政府のサポート
  - 税制優遇（研究開発費、情報セキュリティ対策）