OCDET/atoll project
Tutorial Publication
2013/04/06

事業継続性と運用弾力性に配慮したクラウド リファレンス アーキテクチャ チュートリアル

v1.0

事業継続性と運用弾力性に配慮したクラウド リファレンス アーキテクチャ チュートリアル v1.0

2013/04/06

OCDET/atoll project

著者 川田大輔

注意

この文書中で特定される商業的組織、装置、資料は、実験的な手順または概念を適切に説明するためのものです。したがって、OCDET/atoll project による推薦または保証を意味するものではなく、これら組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもありません。

1. はじめに

1.1 目的と範囲

各種オープンソースベースのクラウド基盤技術の評価と相互接続による連携、運用ノウハウ蓄積と周知を図るにあたって、連携、運用ノウハウの利用が適切な情報セキュリティを含むガバナンス体制のもとに行えるよう、事業継続性と運用弾力性の確保を主眼に置いたクラウド定義とリファレンスアーキテクチャを提供することを目的として公開した事業継続性と運用弾力性を考慮したクラウド リファレンス アーキテクチャ v1.0 についての解説を提供します。

1.2 対象読者

本文書は、事業継続性と運用弾力性を考慮したクラウド リファレンス アーキテクチャ v1.0 についての理解を深めたい方を読者として想定しています。

1.3 作成組織

1.2.1 OCDET

オープンクラウド実証実験タスクフォースは、オープンソース実装の評価は個別の実装単位での検証に留まり、各基盤間の連動性を実証する機会が乏しいという問題があり連携実験の実施が課題となっている今、オープンソースベースの各クラウド基盤技術の実証実験を通じて相互接続による連携、運用ノウハウを周知し、クラウド基盤の一般化と利活用の促進を図る事を目的としてします。また、構築運用ベストプラクティス等を業界全体で共有し、クラウド基盤の整備を行うと同時に質の高いクラウドサービス構築を支援し、IT 業界の活性化に貢献します。詳細については http://www.ocdet.org 参照。

1.2.2 atoll project

は、クラウドガバナンスという概念がスコープしている領域の全体像を明らかにすることでクラウドに関連する技術やサービスの提供者と利用者それぞれが自らの指針を決定する一助となることを目標とします。atoll project は OCDET 参加団体として基盤統合ワーキンググループにおいて本リファレンスアーキテクチャ策定を担当しました。詳細については http://atoll.jp 参照。

2. クラウドサービスに関連するリスクと対策

あらゆる選択には常にリスクが伴っていますが日常生活においてリスクをはっきりと意識する機会はまれです。これは通常の日常生活において受け入れられないリスクから解放され、「安全」が確保されているためです。また、日常を離れ慣れない土地へと旅行している際などは旅の高揚感もありますが未知の環境に身を置いているため、日常生活よりも「安全」に敏感になるのではないでしょうか。クラウドサービスへの取り組みが初めての方にとって、クラウドサービスは未知の安全が確保されているか不確かな、故にリスクが溢れているサービスであると感じられるかもしれません。本文書ではクラウド リファレンス アーキテクチャ v1.0 の解説を通して、クラウドサービスに関連するリスクとその対策を取り扱い、読者がクラウドサービスに適切に対処するためのガイドを提供することで、クラウドサービスの安全確保の方法確立の一助としたいと願っています。

2.1 リスク、危害、安全の定義

はじめに、リスクとは何かを整理しておきましょう。「ISO/IEC Guide51:1999（JIS Z 8051:2004）」はリスクを

リスク（Risk）：危害の発生確率およびその危害の程度の組み合わせ

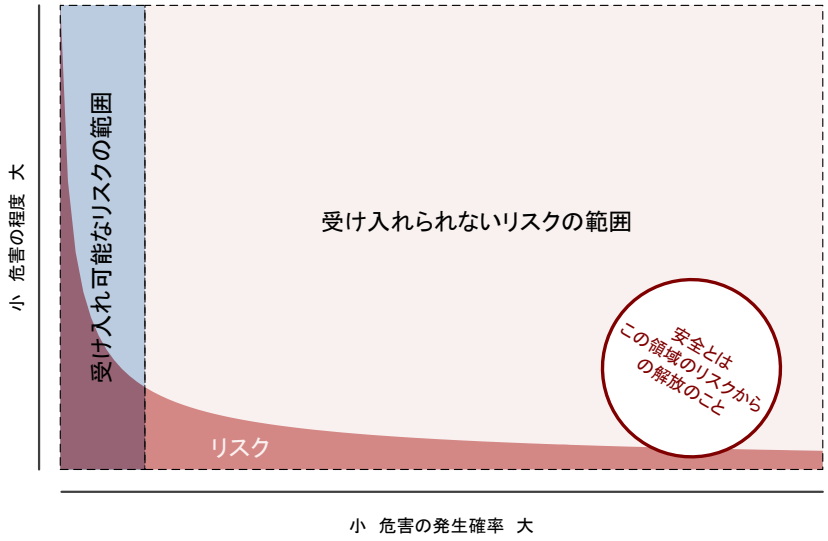
と定義し続いて、

危害（Harm）：人の受ける身体的傷害もしくは健康傷害、または財産もしくは環境の受ける害

であるとしています。このリスクと危害の定義を利用して、

安全（Safety）：受け入れ不可能なリスクから解放されていること

と定義しています。この定義は裏返して読むと「完全な安全は存在しない」ことを示しています。さて、それでは受け入れられないリスクとは何でしょうか？リスクとは危害の発生確率と危害の程度の組み合わせとして表せ、自然災害や株式市場の崩壊など複雑適応系として振る舞うシステムでは危害の程度と発生確率の組み合わせは冪乗則に従うことが知られています。



リスクモデル図

あまりにも発生率が稀で、その代り危害の程度が極端に大きなリスクに対して対策を施すと、事業期間内にリスクが顕在化せずにリスク対策費用が掛け倒れになってしまいます。たとえば、巨大隕石の衝突による事業継続性の喪失などの極端なリスクを考慮に入れて事業計画を策定している方はあまり多くないはずです。
クラウドサービスにおいても読者各々の事情に応じて受け入れられないリスクの範囲を確定し、自身の要件に適した利活用を計画しなければなりません。

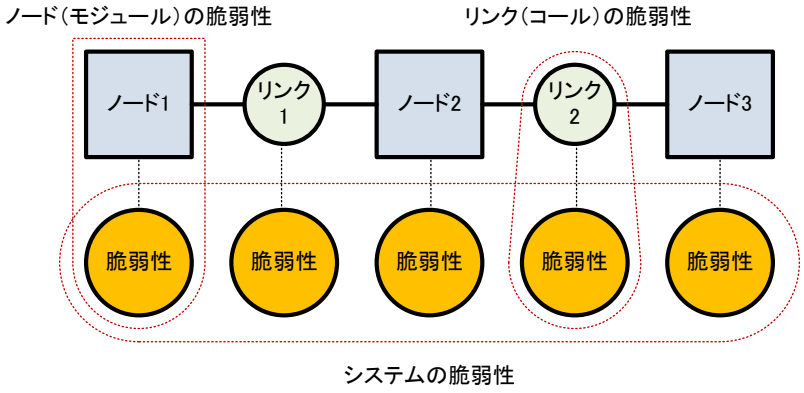
2.2 リスク評価

2.2.1 脅威と脆弱性、危害の定義

受け入れられないリスクの範囲を確定するためには、リスクが顕在化する構造を理解する必要があります。リスクが顕在化する原因は脅威であり、言い換えると、脅威によって脆弱性が顕在化することによって危害が現実のものとなる構造となっています。

脅威・脆弱性・危害関連図

脅威とは脆弱性を顕在化させる働きで、脆弱性とはセキュリティ機能の弱点、危害とは脆弱性によって侵害された結果であって実装の面から見ると障害のことです。この分野の標準としては情報セキュリティ評価基準 CC/CRM または CC/CRM を国際規格化した ISO/IEC15408 を参照するとよいでしょう。
脆弱性はセキュリティ対象を構成するあらゆる要素に潜在しますがその構造自体はシンプルです。セキュリティ対象が三つのノードと二つのリンクを持った構造の場合、ノード、リンクのそれぞれが固有の脆弱性を持っています。また、リンクされた構造全体または構造の一部は他の要素が持つ固有の脆弱性の影響を受けます。



脆弱性分類図

2.2.2 脆弱性の分類

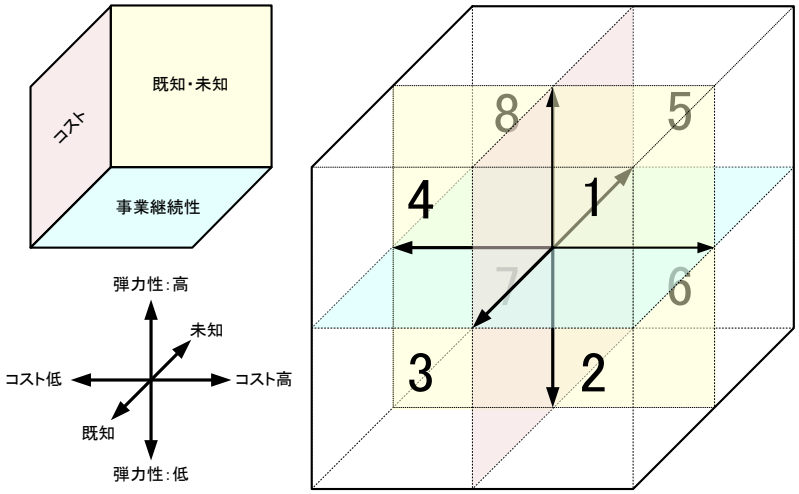
構造に含まれる機能と接続それぞれに脆弱性があります。現在知られている脆弱性は CWE によって体系化されています。また CWE のうち、代表的な脆弱性については IPA によって共通脆弱性タイプ一覧として日本語化されています。CWE が開発した Common Weakness Scoring System(共通脆弱性スコアリングシステム)を利用して算出された CWE/SANS Top 25 Most Dangerous Software Errors(CWE/SANS 最も危険なソフトウェアエラー トップ 25)を利用すると脆弱性の重要性判定が容易になります。

2.2.3 脅威の分類

脆弱性は脅威によって顕在化し危害をもたらしますので、脆弱性に続いて、脅威についても分類が必要です。脅威は WASC によって分類・体系化(タクソノミ化)されています。同じく WASC が提供している Web Hacking Incident Database(Web ハッキング インシデント データベース)を参照すれば発生頻度の高い攻撃を確認することができます。

2.2.4 リスク影響分類

受け入れられないリスクの範囲を確定するために、脆弱性分類を利用して、要件である事業継続性に対する影響の程度を分類します。既知のリスクと未知のリスク、対策コストの大小、弾力性・俊敏性（レジリエンス）の大小の 3 つの軸を利用して八象限に分類します。



クラウドリスク分類図

第一象限

高い俊敏性・弾力性を持ち、対策が高コストで既知のリスクの領域です。この領域には DoS 攻撃、EDoS 攻撃などの脅威や突発的な負荷集中、ゼロデイ攻撃などの脆弱性問題が含まれます。

第二象限

低い俊敏性・弾力性を持ち、対策が高コストで既知のリスクの領域です。この領域にはベンダーロックインや TBTF（Too Big To Fail:大きすぎてつぶせない）問題などの慢性的な問題が含まれます。

第三象限

低い俊敏性・弾力性を持ち、対策が低コストで既知のリスクの領域です。この領域にはウィルス対策、スパム対策、ID/Pw によるアクセス管理などのクラシックな問題が含まれます。

第四象限

高い俊敏性・弾力性を持ち、対策が低コストで既知のリスクの領域です。この領域には内部不正を含む人的ミス、機器故障よるシステム停止が含まれます。システム停止リスクが第四象限に含まれることに違和感が感じられるかもしれませんがオンプレミスの場合と異なりクラウドにおいては機器故障によるシステム停止は低コストリスクに分類できます。

第五象限

高い俊敏性・弾力性を持ち、対策が高コストで未知のリスクの領域です。第五から第八象限については未知であるゆえに具体的な例を挙げることはできませんが、突発性とコストが高いリスクと認識してください。ただし、冪乗則に従うならば発生確率の低いリスクでもあります。

第六象限

低い俊敏性・弾力性を持ち、対策が低コストで未知のリスクの領域です。第二象限に類した構造で現在知られていないリスクとなります。

第七象限

低い俊敏性・弾力性を持ち、対策が低コストで未知のリスクの領域です。第三象限に類した構造で現在知られていないリスクとなります。クラウド固有の利用方法が一般化するにしたがって顕在化すると予想できます。

第八象限

高い俊敏性・弾力性を持ち、対策が低コストで未知のリスクの領域です。後述するクラウドエコシステムが一般化するにしたがって顕在化すると予想できます。

これら八象限にリスクを割り付けして受け入れられないリスクを確定する必要があります。

2.3 クラウド定義

受け入れられないリスクを確定したらクラウドサービスがリスクをどのように取り扱っているかクラウドサービスのアーキテクチャやガバナンス体制を参照して求めるリスク対策がなされているかを確認します。その前に、まず、クラウドサービスとはどのようなものなのか定義をしておく必要があります。経済産業省クラウドサービス利用のための情報セキュリティマネジメントガイドラインでは、クラウドコンピューティングを

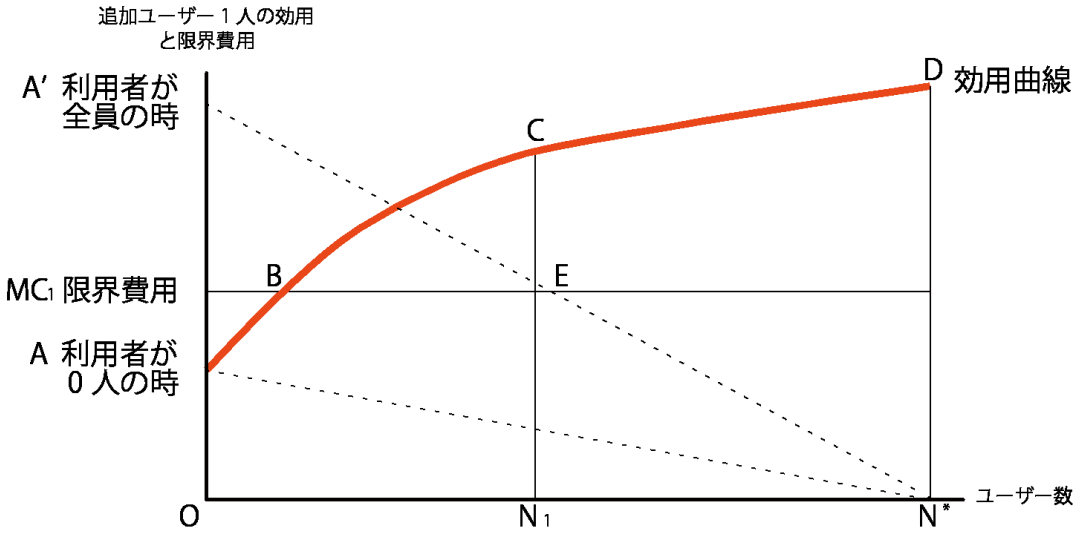
共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーション等）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とする情報処理形態。

と定義しています。ほかにも世界で広く参照されているクラウド定義には NIST や ENISA による定義があります。

そもそも、なぜ、コンピュータリソースを共有化し利用者の要求に応じて適宜・適切にネットワークを通じて配分・提供するサービスが求められたのでしょうか。それはネットワーク外部性について理解する必要があります。

2.3.1 クラウドの本質的特徴

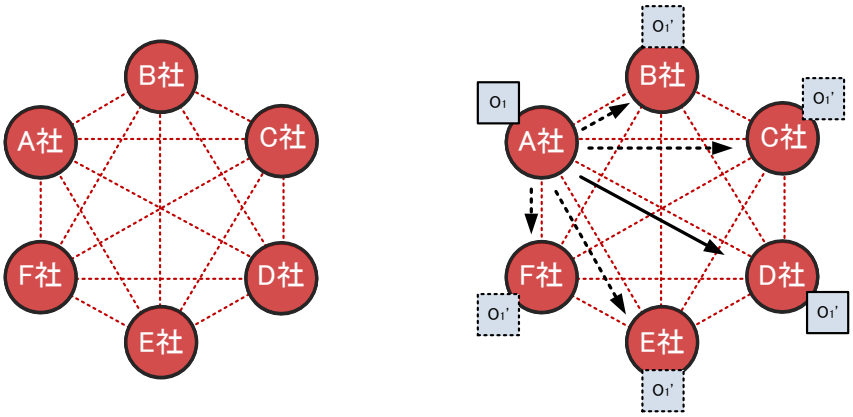
電話などの情報通信サービスの場合を考えてみましょう。ネットワークにつながっていない電話機が一台だけあっても電話機としての役には立ちません。これを効用がゼロの状態といいます。けれどもネットワークにつながった電話機の台数が増えるごとに二台の電話機が接続された状態の効用を出発点に収穫が逓増していきます。このようにそのサービスの利用者数の増加が利用者一人あたりの効用を増大させる場合をネットワーク外部性が働く、といいます。



ネットワーク外部性効用曲線図

クラウドサービス利用のための情報セキュリティマネジメントガイドライン定義がいう、コンピュータリソースの共有化によって、コンピューティングという行為それ自体にネットワーク外部性が働き、利用者が増えるにしたがって利用者一人あたりの効用が増大する効果が期待できるといえます。

さて、ネットワーク外部性が働くためには、電話の場合と同じようにネットワークにつながったコンピュータリソースの相互運用性と可搬性確保が確保されている必要があります。ISO/IEC 25010 は、相互運用性とは外部測定法に基づくとデータ形式に基づくデータ交換性であり、内部測定法に基づくとインターフェース一貫性であるとしています。クラウドサービスにおいては異なる運営主体が提供しているクラウドサービスが相互に一貫したインターフェースを利用してデータ交換性を確保している状態と言えます。次に、同じくISO/IEC 25010 は、可搬性について、異なる環境への移しやすさと定義し、移しやすさを表す順応性や同等物との置換性などの副特性を持つとしています。



相互運用性・可搬性モデル図

つまり、相互運用性を確保することでクラウドサービス間のデータ交換性を確保し、さらに可搬性を確保することでクラウドサービス相互の置き換えを可能にすることで高いネットワーク外部性が働く状態を実現し、効用を高めることが可能になります。

では、さまざまな運営主体が提供するクラウドサービスで相互運用性と可搬性を確保するためにはどうすればよいでしょうか。そのためには相互運用性と可搬性の確保を求められる事業者が合意または強制によって同一のデータ形式とインターフェース提供を行う必要があります。電気通信や電力などの場合は法令によって形式が厳しく定められています。発達途上にあるクラウドサービスについては標準化団体による標準化活動が中心となって進められています。

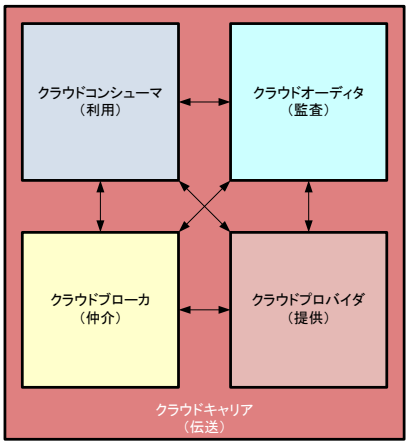
より高いネットワーク外部性を働かせるために国内にとどまらず広く世界で標準化を進め相互運用性と可搬性を高いレベルで確保することが重要です。

相互運用性と可搬性確保の初めはインターフェース標準の確立ですから、広く利用されているインターフェース標準である OSI 参照モデルにクラウドサービスの階層構造を引き当ててみましょう。第一階層、第三階層、第五階層で OSI 参照モデルとは異なるレイヤー界面構成となっています。インターフェースの問題として考えると、NISTSP800-145 が IaaS を含む全提供形態に要求しているオンデマンドセルフサービス機能を実装する場合、IssS は、オンデマンドセルフサービスを実現するダッシュボードや API をアプリケーション層にあたる SaaS として装備している必要があることになり、ダッシュボードや API を動作させるアプリケーションプラットフォームをサービス層にあたる PaaS として装備している必要があることになります。

クラウド階層モデル図

次にクラウドに関わるアクター類型について整理しておきましょう。文書内で直接言及はしていませんが、クラウド リファレンス アーキテクチャ v1.0 は、NIST SP500-292 の定義したアクターモデルを支持しています。NIST SP500-292 定義のアクター構造としてクラウドサービスの提供者と利用者を表すクラ

ウドプロバイダとクラウドコンシューマの定義は当然として、透明性を担保するクラウドオーディタ（監査者）の設定は数理組織論の立場から妥当性が支持されますし、さまざまな中間リスクの引き受け手としても機能する垂直的取引関係の担い手であるクラウドブローカ（仲介者）の設定も合理的です。これらアクター間の通信を担うクラウドキャリア（伝送者）についてはITU条約に基づく国際的な通信秩序がインターネットを含む通信基盤動作の前提となっている点から粒度設定として支持できます。



クラウドアクター図

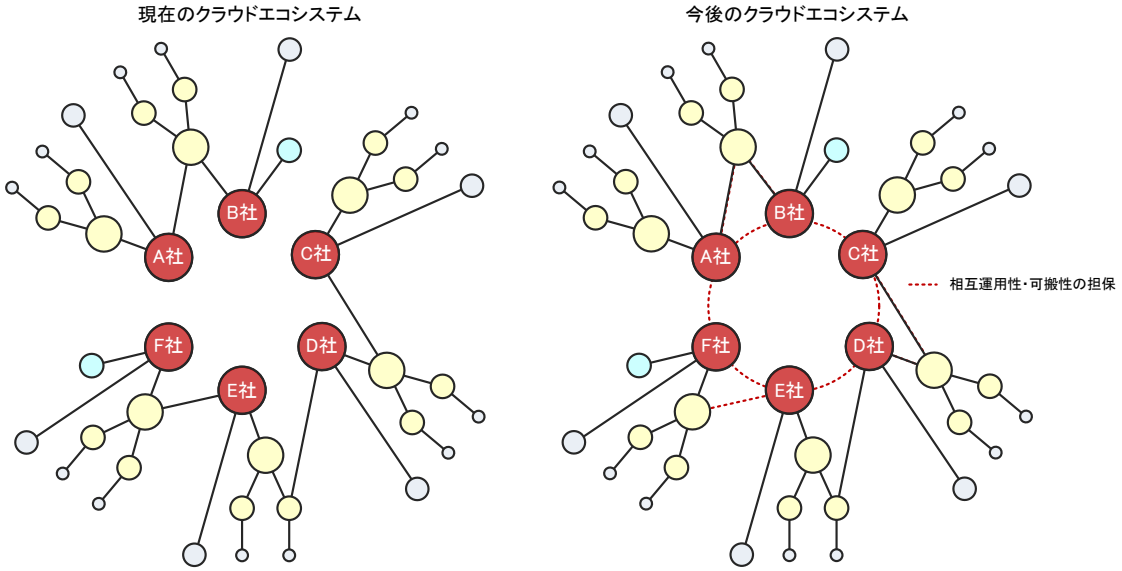
ここまでの検討を踏まえ、具体的にセキュリティについて検討するために必要なクラウド定義は、

> **共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーション等）について，利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供することを可能とし相互運用性と可搬性が担保されている情報処理形態。**

とすることができました。

2.3.2 クラウドエコシステム

相互運用性と可搬性を考慮し、クラウドコンシューマ（利用者）とクラウドプロバイダ（提供者）のほかにクラウドオーディタ（監査者）とクラウドブローカ（仲介者）をアクターとして備えたクラウドサービスは、単一事業者の提供するサービスではなく、さまざまな事業者が相互に接続したJames F. Mooreのいう（ビジネス）エコシステムと見ることができるようになります。

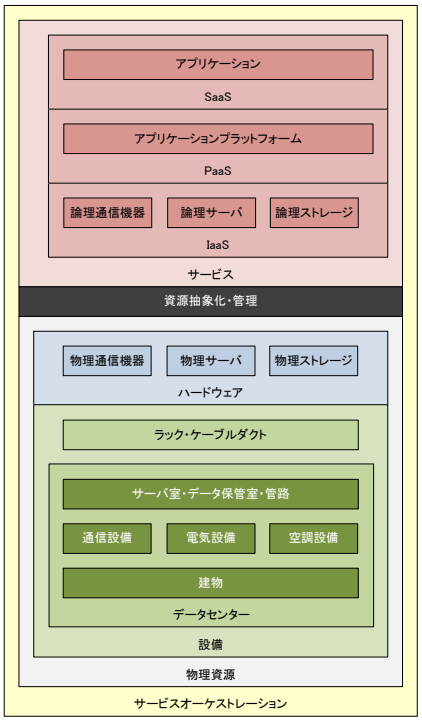


エコシステム成長モデル図

2.4 リファレンスモデル定義

受け入れられないリスクとクラウドサービスのアーキテクチャやガバナンス体制を突合せするために、先ほど拡張した相互運用性と可搬性を考慮したクラウド定義に対応したクラウドアーキテクチャを用意します。

OSI 参照モデルをもとにインターフェース問題として考えた場合、2.3.1 でも言及しましたが、TCI Reference Architecture v1.1 や NIST SP500-292 が想定しているような IaaS、PaaS、SaaS の入れ子構造は否定されます。また、TCP/IP 階層モデルに当てはめて考えた場合は IaaS、PaaS、SaaS といった層構造はサービス層として統合され、個別階層の区別は消失します。クラウド リファレンス アーキテクチャ v1.0 では抽象化粒度の違いを意識し IDC などの市場推計分類との整合性を考慮して OSI 参照モデル準拠の階層モデルを採用しました。OSI 参照モデルに基づくクラウド階層モデルでは、IaaS が装備しているセルフマネジメントダッシュボードなどは SaaS として識別されます。定義が要求する適宜・適切の程度が、たとえば高い俊敏性をもったリスクに即応性を以て対応したいとされる場合などは、即時、セルフサービスが必須要件となり、セルフマネジメントダッシュボードや API を装備したクラウドサービスを選択する必要があります。
クラウド リファレンス アーキテクチャ v1.0 では、NIST SP800-145 がクラウドの本質的特徴として定義した On-demand Self Service、Resource Pooling、Rapid elasticity、Measured Service の各性質の実現度について定量的な要求は定義しませんでした。各性質の適切な実現度はネットワーク外部性が働く市場環境のもとで、各アクターが相互作用することで決まる均衡点として表されると考えています。



クラウドリファレンスアーキテクチャ図

2.4.1 設備層

後述するハードウェア層と合せて物理資源層を構成します。データセンターとは、ハードウェア層に含まれる物理資源を収容する建物全体またはその一部で、サーバ室・データ保管室・管路と通信設備、電気設備、空調設備を備えたものをいいます。データセンターに加えてハードウェア層に含まれる物理資源を収容するラック・ケーブルダクト等を総称して設備といいます。詳細について、手順の観点からは TIA-942 記載の定義や構造を参考にするとよいでしょう。また、要件の観点からは JDCC データセンターファシリティスタンダードや UpTimeInstitute TIER が相互運用性と可搬性の検証手段として利用できます。

2.4.2 ハードウェア層

前述のハードウェア層と合せて物理資源層を構成します。計算資源（物理サーバ）、記憶資源（物理ストレージ）通信資源（物理通信機器）によって構成されます。設備層との界面はラックのマウントポジションと電源ケーブルのプラグ、通信ケーブルの端子となります。後述する資源抽象化・管理層によって抽象化されますので構築主体からみると構成選択の自由度が高い層ですがハードウェア層の構成が上位層の挙動特性に大きな影響を与えるため要件に応じた構成選択を慎重に行う必要があります。

2.4.3 資源抽象化・管理層

物理資源層を抽象化して後述するサービス層に提供する層となります。物理資源層の計算資源（サーバ）、記憶資源（ストレージ）、通信資源（通信機器）を管理し、仮想マシンなどの形態に抽象化して IaaS 層での利用を可能にします。サービス層に対する抽象化された物理資源の割り当て管理を含む構成

管理と変更管理の機能も提供します。仮想化等によって資源抽象化と管理を行うプログラムを資源抽象化・管理層としハードウェア層、サービス層との界面と認識されます。

2.4.4 サービス層

クラウドコンシューマが直接触れる IaaS、PaaS、SaaS で構成されます。抽象化粒度によって階層は識別され、物理資源が提供する計算資源（サーバ）、記憶資源（ストレージ）、通信資源（通信機器）を物理資源層と同一の粒度のまま、利用者の要求に応じて適宜・適切に配分する IaaS 層、IaaS 層を隠ぺいしてアプリケーションプラットフォームとして提供する PaaS 層、PaaS 層を隠ぺいしてアプリケーションを提供する SaaS 層に分類されます。

2.5 リファレンスモデルから導出されるリスクドメイン構成

COBIT 4.1、HIPAA / HITECH Act、ISO/IEC 27001-2005、NIST SP800-53 R3、FedRAMP Security Controls、PCI DSS v2.0、BITS Shared Assessments SIG v6.0、BITS Shared Assessments AUP v5.0、GAPP、Jericho Forum、NERC CIP、AICPA TS Map、AICPA Trust Service Criteria（掲載順は原資料まま）記載の各リスクドメインモデルの互換性を一覧化している CSA Cloud Control Matrix のリスクドメインモデルを元に、経済産業省クラウドサービス利用のための情報セキュリティマネジメントガイドラインが指摘する各種リスクを分類すると

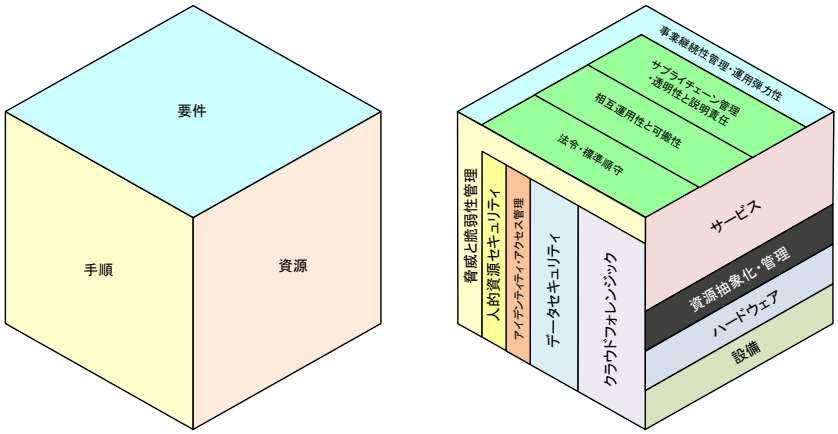
要件は

事業継続性管理・運用弾力性
サプライチェーン管理・透明性と説明責任
相互運用性と可搬性
法令と標準順守

にまとめられ、手順として

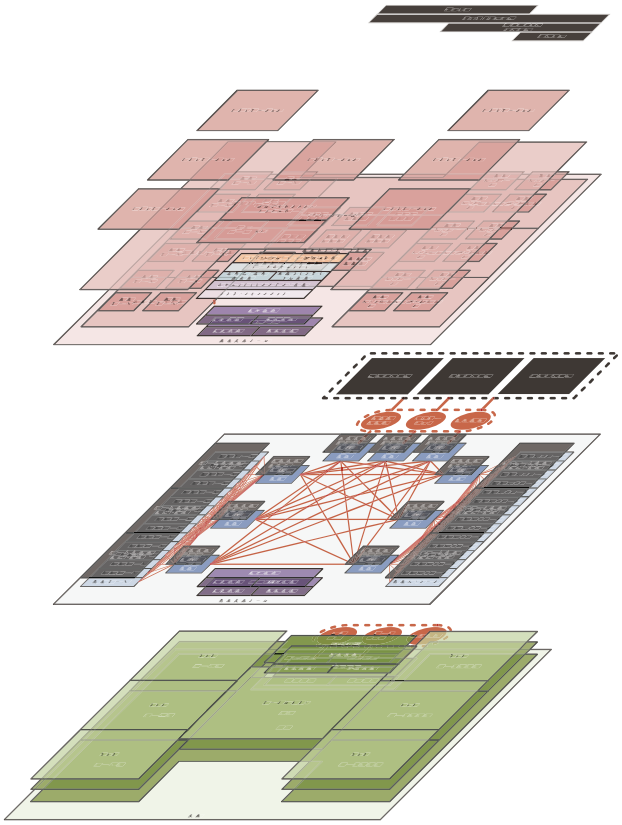
脅威と脆弱性管理
人的資源セキュリティ
アイデンティティとアクセス管理
データセキュリティと情報ライフサイクル管理
暗号化と暗号鍵管理
セキュリティインシデント管理・電子証跡とクラウドフォレンジック
変更制御と構成管理
アプリケーションとインターフェースセキュリティ
インフラストラクチャと仮想化セキュリティ
データセンターセキュリティ

にまとめることができます。これらの要素をコントロールエリアと呼びます。さらに個々のコントロールエリアは複数のコントロールポイントで構成されています。
この要件と手順を COBIT に倣い、ガバナンスキューブに割り付けると以下のようになります。クラウド資源を手順として実装したコントロールエリアで制御することによって要件となるコントロールエリアの目標が達成されます。



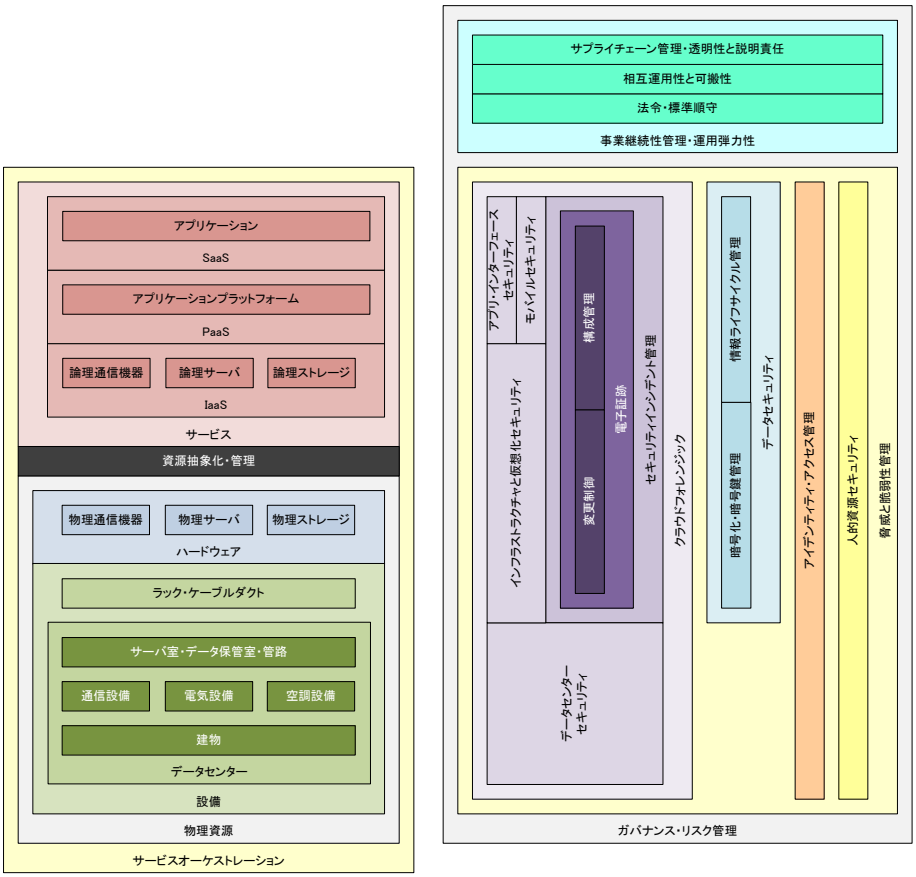
クラウドガバナンスキューブ図

さらに手順に含まれるコントロールエリアをリファレンスアーキテクチャ上に実装として組み込むと割り当て階層は以下の通りとなります。



クラウドレイヤーモデル図（部分）

レイヤーモデルに割り当てた手順と要件の関係をリファレンスモデルで表現すると以下の通りとなります。



クラウドガバナンスマップ図

データセンターセキュリティやインフラストラクチャと仮想化セキュリティ、アプリケーション・インターフェースセキュリティなどの構成要素個々のコントロールエリアがあり、変更制御、構成管理の結果を電子証跡によって記録しセキュリティインシデント管理を実現し、セキュリティインシデント管理と構成要素個々のコントロールと組み合わせてクラウドフォレンジックを実現します。暗号化・暗号鍵管理と情報ライフサイクル管理を利用してデータセキュリティを実現し、これら機能群にアイデンティティ・アクセス管理と人的資源セキュリティを加えて脅威と脆弱性管理を総合的に行うことでガバナンス・リスク管理を実現する構成となっています。

2.6 リスクドメイン解説

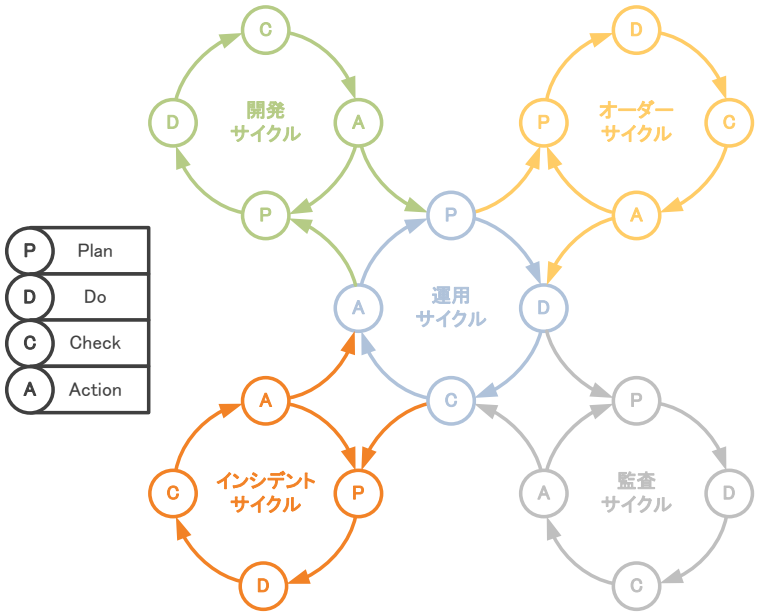
2.6.1 要件

2.6.1.1 事業継続性管理・運用弾力性

事業継続性管理とは、価値創造活動を維持するために、事業中断リスクを識別して危害の発生を抑止または回避する能力をいい、運用弾力性とは、抑止または回避できない危害への対応または復旧能力をいいます。利用者の要求に応じて適宜・適切に配分し，ネットワークを通じて提供されるクラウドサービスにおける事業継続性管理と運用弾力性の確保には運用中心の視点が欠かせません。クラウドサービスにおけるライフサイクルは以下の五つの要素で構成されています。

開発サイクル
オーダーサイクル
運用サイクル
監査サイクル
インシデントサイクル

各サイクルはそれぞれ固有の PDCA サイクルを持ち、固有 PDCA サイクルの 2 点で中心となる運用サイクルと接続しています。



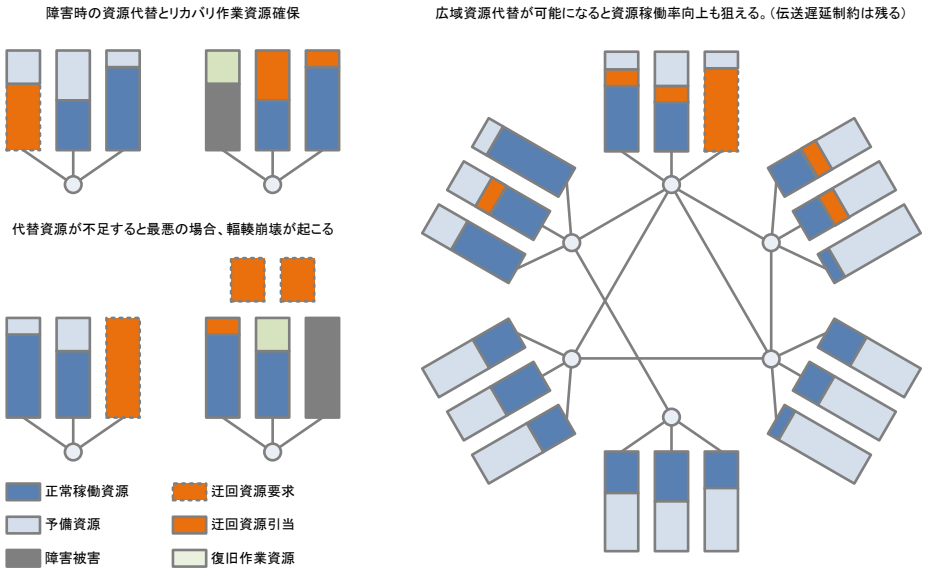
クラウドライフサイクル図

高度な事業継続性管理と運用弾力性を求める場合データセキュリティと情報ライフサイクル管理コントロール群とセキュリティインシデント管理・電子証跡とクラウドフォレンジックコントロール群がクラウドサービス全体で精密に実施されている必要があり、その制御のためにセルフマネジメントダッシュボードや API の利用が必要になるでしょう。

2.6.1.2 相互運用性と可搬性

相互運用性とは、特定のデータ形式に基づくデータ交換性であってインターフェース一貫性をいい、可搬性とは異なる環境への移しやすさをいいます。利用者がディザスタリカバリを含む高可用性の確保やベンダーロックインリスクの排除を求める場合、または特定のクラウドプロバイダでのサイジング上限によって事業成長が阻害されている場合、相互運用性と可搬性の確保が重要になります。

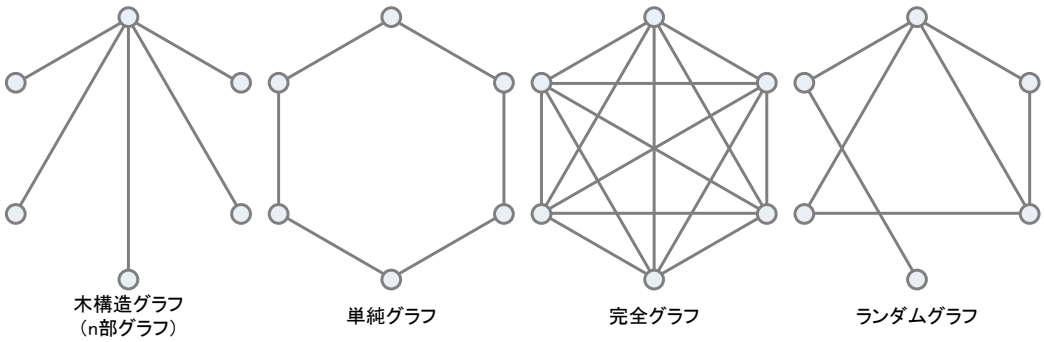
特に高可用性の確保を図る場合は何らかの理由で利用できなくなった資源の代替資源確保と復旧作業のための作業資源確保、復旧後の切り戻し作業を無停止で行うためのローリングアップデート能力も必要になるでしょう。



相互運用性・可搬性が確保されたクラウドエコシステムにおける運用弾力性モデル図

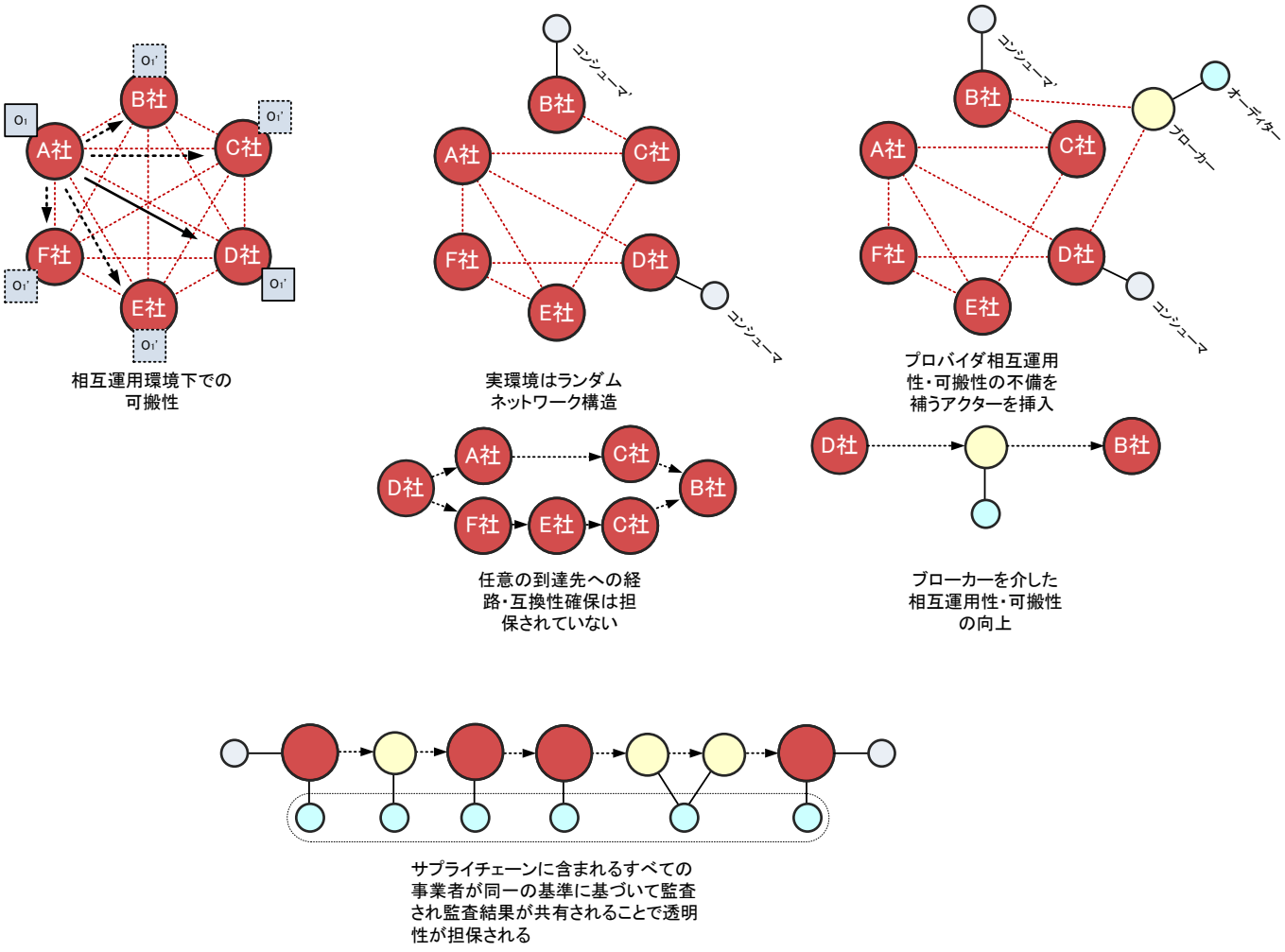
2.6.1.3 サプライチェーン管理・透明性と説明責任

資源、材料の調達に始まり、製品・サービスの出荷を経て輸送手段(陸上・海上を含む)を通じてエンドユーザーにまで及ぶプロセスをサプライチェーンといい、透明性と説明責任とは、サプライチェーンに含まれる個々のプロセス活動結果についての合理的な報告義務と報告内容の検証可能性の担保をいいます。モデルとしての相互運用性では事業者相互の接続がフルメッシュとなっていますが、実際に市場で提供されているサービスの相互運用性は提供主体個々の事業戦略や制約条件によってランダムネットワーク構造となります。



ネットワーク(グラフ)バリエーション図

ノードとリンクの関係で表現できる構造はグラフ理論を利用して表現します。インターネットはスケールフリー性とスモールワールド性、クラスター性を備えたランダムネットワークであることが知られています。このような構造を持つため、発側サービスから着側サービスまで複数のサービスを中継しないと到達できない場合も想定されます。このように中継事業者を介在した接続を行う場合、中継事業者すべてを含むサプライチェーンの信頼性が確保されないと中間者攻撃リスクが顕在化してしまいます。また、発サービスと着サービス間を受け入れ可能なリスクの範囲で接続する経路が存在しない場合、クラウドブローカなどの業態を介した接続を行うことも想定できます。これらサプライチェーン全体の管理と透明性確保を通して説明責任を果たすために標準に準拠した相互運用性と可搬性を確保した監査制度とサプライチェーンに対して中立な第三者としてのクラウドオーディタが必要になります。



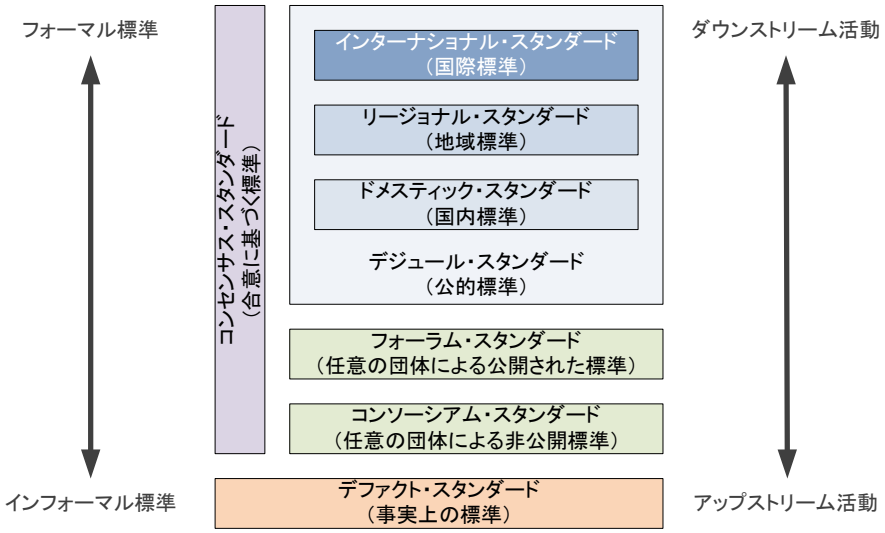
アクター連携およびサプライチェーンの透明性確保のための監査連携モデル図

2.6.1.4 法令と標準遵守

公平性や誠実性など普遍的倫理観に基づいて、組織の活動が社会及び環境に及ぼす影響に対して社会的責任を果たし、利害関係者へ配慮した対応を行い、各国の法令を尊重し順守し、国際的行動規範と人権を尊重することをいいます。クラウド リファレンス アーキテクチャ v1.0 は、クラウドサービス個々の約款に規定される準拠法やデータセンター立地やデータ由来によって強制適用される各国法の問題に対して技術的に中立ですので、本文書ではクラウド リファレンス アーキテクチャ v1.0 に基づくクラウドサービス実装が遵守すべき標準について記述します。

標準には国際標準、地域標準、国内標準を含む公的標準と任意の団体による公開された標準であるフォーラムスタンダード、任意の団体による非公開の標準であるコンソーシアムスタンダードと事実上の標準と訳されるデファクトスタンダードがあります。また、デファクトスタンダードを除く各標準は総称してコンセンサススタンダードと呼ばれます。

下図では上位にフォーマル、下位にインフォーマルな標準を配置して各標準の位置づけを図示しています。従来は 1865 年成立の万国電信連合を祖とする ITU 標準などのインターナショナルスタンダードなどのデジュールスタンダードは国の代表などが集まって課題発見と将来予見を行い標準化を進め市場を誘導するダウンストリーム活動が中心でしたが、昨今は PC やインターネットの関連規格の例など標準化活動メンバー個々の利益追求が原動力となり、デファクトスタンダードとしての地位を市場での競争によって獲得した規格がインターナショナルスタンダードに採用される例も増えています。このようなアップストリーム活動の結果インターナショナルスタンダードに採用されたクラウド関連の規格の例として OASIS が策定し ISO/IEC 29362 として国際標準化された WS-I や、Common Criteria が策定し ISO/IEC 15408 となった CC、TM Forum が策定し ITU-T M.3190 となった SID などが挙げられます。



ダウンストリーム活動：課題発見と将来予見に基づく標準誘導
アップストリーム活動：標準化活動参加メンバー個々の利益追求

スタンダード分類モデル図

クラウドサービスはリファレンスアーキテクチャやレイヤーモデルで示したようにサービスを構成する要素がさまざまな分野に及んでおり、ここに挙げたあらゆる標準が何らかの形で関与しています。ここでは以下に公開されている標準を例示しておきます。

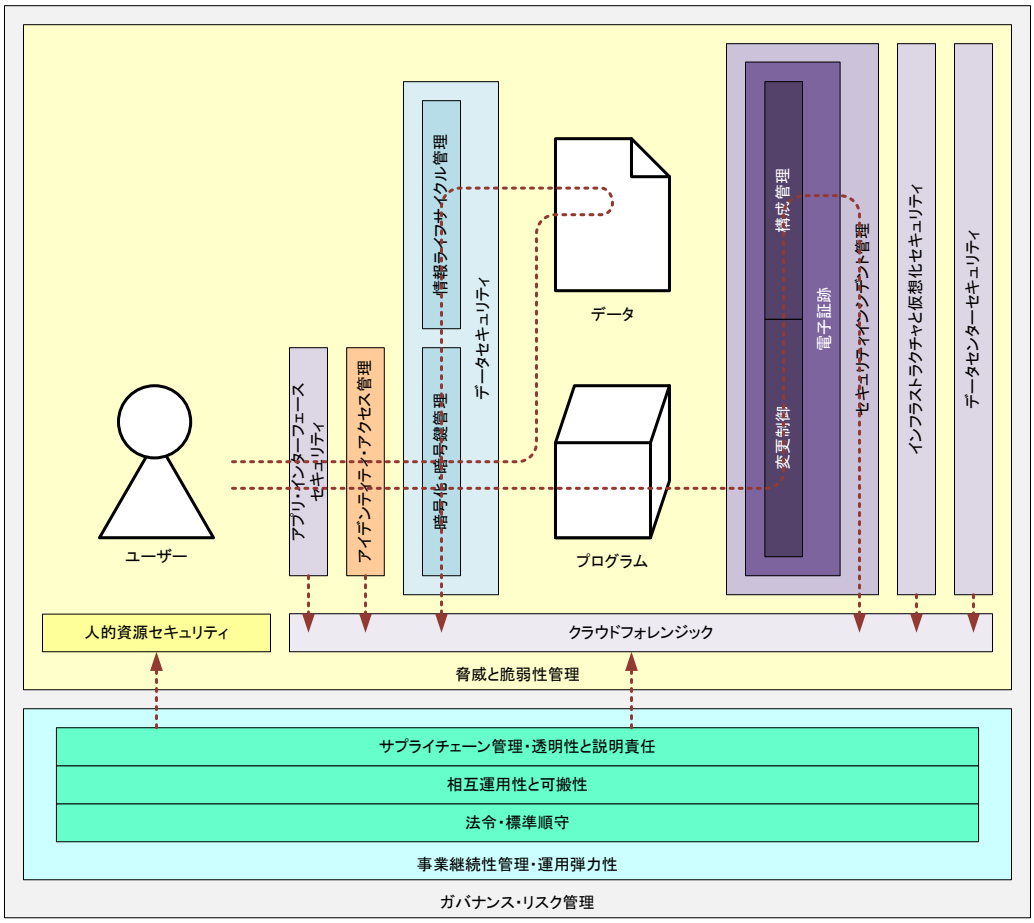
		団体	規格・組織	ポインタ
定義・原則	要件・手順関連定義	ISO/IEC	ISO/IEC Guide51:1999 Safety aspects -- Guidelines for their inclusion in standards	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=32893
		ISO/IEC	ISO/IEC 25000:2005 Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Guide to SQuaRE	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35683
		ISO	ISO 26000:2010 Guidance on social responsibility	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42546
	クラウド定義	NIST	NIST SP800-145 Definition of Cloud Computing	http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
	リファレンスアーキテクチャ	NIST	NIST SP500-292 Cloud Computing Reference Architecture	http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
		CSA	TCI Referene Architecture	https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf
		The Open Group	The Open Group Architecture Framework (TOGAF)	http://www.opengroup.org/togaf/
		The Open Group	Service-Oriented Cloud Computing Infrastructure (SOCCI) Framework	https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12510
		ISO/IEC JTC 1/SC 38	Distributed Application Platforms and Services (DAPS)	http://www.iso.org/iso/jtc1_sc38_home
		ITU	ITU-T SG13: Future networks including cloud computing, mobile and next-generation networks	http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/default.aspx
要件	ガバナンス	COSO	Committee of Sponsoring Organizations of the Treadway Commission (COSO)	http://www.coso.org/
		ISACA	COBIT5	http://www.isaca.org/COBIT/Pages/default.aspx
		UK Cabinet Office	e-Government Interoperability Framework	http://www.fiorano.com/docs/solutions_e-GIF-guidelines.pdf
		BSI	Governance Framework	http://www.bsigroup.com/en-GB/about-bsi/governance/
	相互運用性・可搬性	OASIS	Topology and Orchestration Specification for Cloud Applications (TOSCA)	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
		OASIS	Public Administration Cloud Requirements (PACR)	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pacr
		IPA	情報システムに係る相互運用性フレームワーク	http://www.ipa.go.jp/software/open/ossc/doc/inope_framework.pdf
		TM Forum	Information Framework (SID)	http://www.tmforum.org/InformationFramework/1684/Home.html
		ITU	ITU-T M.3190 Shared information and data model (SID)	http://www.itu.int/ITU-T/recommendations/rec.aspx?id=9541
	サプライチェーン管理	TM Forum	Business Process Framework (eTOM)	http://www.tmforum.org/BusinessProcessFramework/1647/home.html
		TM Forum	Application Framework (TAM)	http://www.tmforum.org/ApplicationFramework/2322/Home.html
	透明性・説明責任	IFAC	International Standard on Assurance Engagements (ISAE) No. 3402	http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf
		ISO/IEC	ISO/IEC 20000 (ITSMS) 情報技術－サービスマネジメント－(1,2,3,4,5)	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51986
手順	セキュリティ	CSA	Cloud Security Guideline v3.0	https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
		CSA	CSA Cloud Controls Matrix v3.0 PEER REVIEW	https://interact.cloudsecurityalliance.org/index.php/ccm/index
		PCI	Data Security Standards (PCIDSS)	https://www.pcisecuritystandards.org/security_standards/
		ENISA	Cloud Computing Security Risk Assessment	http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
		METI	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	http://www.meti.go.jp/press/2011/04/20110401001/20110401001-3.pdf
		ISO/IEC	ISO/IEC 27000 (ISMS) 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム	http://www.webstore.jsa.or.jp/webstore/ISO/FlowControl.jsp
		ISO/IEC	ISO/IEC 27017 Information technology Security techniques Security in cloud computing (DRAFT)	http://www.iso27001security.com/html/27017.html
		Common Criteria	CC/CEM バージョン3.1 リリース4	http://www.ipa.go.jp/security/jisec/cc/index.html
		ISO/IEC	ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security -- (1,2,3)	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50341
		CWE	Common weakness Enumeration	http://cwe.mitre.org/index.html
資源	サービス層	OWASP	The Open Web Application Security Project	https://www.owasp.org/index.php/Main_Page
		OASIS	Identity in the Cloud	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud
		OASIS	Symptoms Automation Framework (SAF)	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=saf
		OASIS	Cloud Authorization (CloudAuthZ)	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cloudauthz
		OGF/OCCI	Open Cloud Computing Interface - RESTful HTTP Rendering	http://www.ogf.org/documents/GFD.185.pdf
		OASIS	OASIS Web Services Security	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
		ISO/IEC	ISO/IEC 29361:2008 Web Services Interoperability - WS-I Basic Profile Version 1.1	http://www.iso.org/iso/catalogue_detail.htm?csnumber=45422
		ISO/IEC	ISO/IEC 29362:2008 Web Services Interoperability - WS-I Attachments Profile Version 1.0	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45423
		ISO/IEC	ISO/IEC 29363:2008 Web Services Interoperability - WS-I Simple SOAP Binding Profile Version 1.0	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45424
		TM Forum	Frameworx	http://www.tmforum.org/TMForumFrameworx/1911/Home.html
	資源抽象化・管理層	DMTF	Open Virtualization Format (OVF)	http://dmtf.org/standards/ovf
		DMTF	Cloud Infrastructure Management Interface (CIMI)	http://dmtf.org/sites/default/files/standards/documents/DSP2027_1.0.1.pdf
		SNIA	Cloud Data Management Interface (CDMI)	http://www.snia.org/tech_activities/standards/curr_standards/cdmi
		OGF/OCCI・SNIA	Cloud Storage for Cloud Computing	http://ogf.org/Resources/documents/CloudStorageForCloudComputing.pdf
		ONF	Open Flow	https://www.opennetworking.org/standards/intro-to-openflow
		OASIS	Cloud Application Management for Platforms (CAMP)	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=camp
		OGF/OCCI	Open Cloud Computing Interface - Core	http://ogf.org/documents/GFD.183.pdf
		OGF/OCCI	Open Cloud Computing Interface - Infrastructure	http://ogf.org/documents/GFD.184.pdf
	ハードウェア層	OCP	Open Compute Project	http://www.opencompute.org/
	設備層	TIA	ANSI/TIA 942-2005 Telecommunications Infrastructure Standard for Data Centers	http://global.ihs.com/tia_telecom_infrastructure.cfm?currency_code=USD&customer_id=21254A2A5C0A&oshid=21254A2A540A&shopping_cart_id=21254A2A530A&rid=TIA&country_code=US&lang_code=ENGL&input_doc_number=%20&input_doc_title=%20
		UTI	Uptime Institute Tier Certifications	http://uptimeinstitute.com/TierCertification/
		Open DataCenter Alliance	Master Usage Model: Commercial framework REV 1.0	http://www.opendatacenteralliance.org/docs/ODCA_Commercial_Framework_MasterUM_v1.0_Nov2012.pdf
		JDCC	データセンターファシリティスタンダード	http://www.jdcc.or.jp/news/article.php?nid=eccbc87e4b5ce2fe28308fd9f2a7baf3&sid=81

参考	規格間調整組織	NIST	Standards Acceleration to Jumpstart the Adoption of Cloud Computing	http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/SAJACC
		ITU	Joint Coordination Activity on Cloud Computing (JCA-Cloud)	http://www.itu.int/en/ITU-T/jca/Cloud/Pages/default.aspx
		ETSI	Cloud Standards Coordination	http://www.etsi.org/news-events/news/614-201212-cloudsp
	ユースケース・ワークフロー	The Open Group	Business Scenario Workshop Report	http://www.opengroup.org/cloud/whitepapers/bsw/index.htm
		ARTS	Cloud Computing for Retail	http://www.nrf-arts.org/content/whitepapers

クラウド関連標準一覧

2.6.2 手順

リファレンスアーキテクチャでの手順化されたコントロールエリアの挙動は下図のようになります。以下、各コントロールエリアについて解説します。



クラウドガバナンスコントロールエリア挙動モデル図

2.6.2.1 アプリケーションとインターフェースセキュリティ

最低限、アプリケーション毎に OWASP または同等のセキュリティフレームワークに準拠したサービス層でのユーザー資格およびパスワードコントロールの自動化された実装をします。アイデンティティとアクセス管理との連携を推奨します。

2.6.2.2 アイデンティティとアクセス管理

資源および手順として識別されるすべての要素に対して OWASP ESAPI を参照し、紛失、誤用、不正アクセス、開示、改ざんおよび破壊を含む脅威から資産やデータを保護するために自動化されたアクセス管理技術と物理的な保護手段を実装します。また、資産やデータ、アクセス権限の組み合わせによって構成されるロールと利用者の本人性確認手法を適切に実装します。

2.6.2.3 暗号化と暗号鍵管理

資源および手順として識別されるすべての要素について、紛失、誤用、不正アクセス、開示、改ざんおよび破壊を含む脅威からデータを保護するために暗号化技術と物理的な保護手段の実装が必要です。また、データとアクセス権限の組み合わせによって構成されるロールと利用者の本人性確認手法によって暗号鍵を適切に管理します。

2.6.2.4 データセキュリティと情報ライフサイクル管理

資源および手順として識別されるすべての要素について、規制、法令、契約やビジネス要件への適合性を確保するために、資産やデータにコントロール ID を付与する必要があります。コントロール ID は標準データモデルに従った分類ラベル、変更履歴、構成情報、制約条件等の情報を保持するための自動化された管理手段を備えます。

2.6.2.5 変更制御と構成管理

資源および手順として識別されるすべての要素について、資産やデータの初期構成はコントロールIDに付与された構成情報によって管理されます。資産やデータの変更は、事前に定められた手続きに従ったテスト結果が適正な承認権限のもとに承認されるまでテスト対象となった資産やデータの変更は、本番環境に適用することはできません。テスト結果が承認され変更された資産やデータの状態は変更履歴としてコントロール ID に追加されます。変更制御、構成管理ともにポリシーベース管理することを推奨します。

2.6.2.6 セキュリティインシデント管理・電子証跡とクラウドフォレンジック

資源および手順として識別されるすべての要素について、データセキュリティと情報ライフサイクル管理に格納された、変更制御と構成管理にかかる情報は電子証跡として管理します。電子証跡を利用して時系列にコントロール ID の状態を比較することによって、紛失、誤用、不正アクセス、開示、改ざんおよび破壊といった顕在化した脅威（セキュリティインシデント）の検出と原因究明などのクラウドフォレンジック手段を実装します。

2.6.2.7 インフラストラクチャと仮想化セキュリティ

変更制御と構成管理の対象となる資産のうち、サーバ、ストレージ、通信機器それぞれの資源抽象化・管理機能によって構築される論理サーバ資源、論理ストレージ資源、論理ネットワーク資源を利用者の要求に応じて適宜・適切に論理サーバ、論理ストレージ、論理通信機器、プラットフォーム、アプリケーションまたはこれらを組み合わせたサービスとして提供するオーケストレーションについて、事前に定められた制約条件に従って自動化された実行と管理の手段を実装します。

2.6.2.8 データセンターセキュリティ

物理資源として識別されるすべての要素を紛失、誤用、不正アクセス、開示、改ざんおよび破壊を含む脅威から保護するために、物理的セキュリティ境界（塀、壁、障壁、ガード、ゲート、電子監視、物理的な認証メカニズム、レセプションデスク、セキュリティパトロール）を実装します。物理的セキュリティ境界によって隔離された物理資源に対する物理的アクセスは適切な物理アクセス管理手段によって保護します。物理的セキュリティ境界は保護領域、検疫領域、公開領域の三層以上を設定することを推奨します。

2.6.2.9 人的資源セキュリティ

アイデンティティとアクセス管理またはデータセンターセキュリティで規定されるアクセス管理の対象となる資産またはデータへあらゆるアクセス権限の付与にあたっては法令と標準順守および規制、倫理、契約制約に基づき雇用候補、雇用者、請負業者や第三者も含めて事前に適切な水準の背景調査を行います。

2.6.2.10 脅威と脆弱性管理

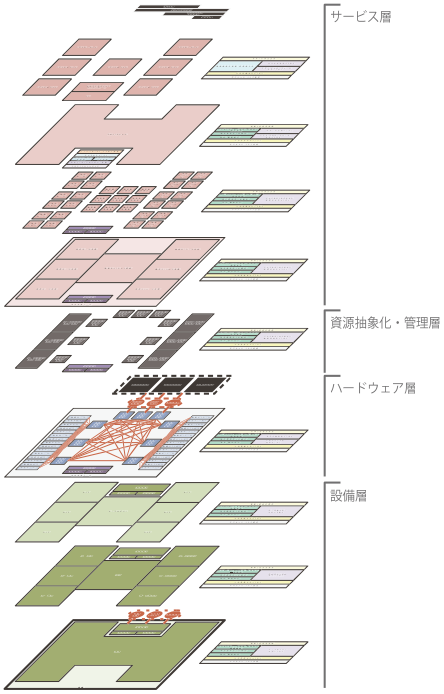
アプリケーションとインターフェースセキュリティ、アイデンティティとアクセス管理、暗号化と暗号鍵管理、データセキュリティと情報ライフサイクル管理、変更制御と構成管理、セキュリティインシデント管理・電子証跡とクラウドフォレンジック、インフラストラクチャと仮想化セキュリティ、データセンターセキュリティ、人的資源セキュリティの各コントロール領域について詳細なコントロールポリシー（情報セキュリティポリシー文書）を作成します。また、経営者は承認した情報セキュリティポリシー文書を従業員、請負業者、およびその他の関連する外部関係者に公開します。情報セキュリティポリシーは役員、従業員、請負業者、およびその他の関連する外部関係者を含むセキュリティプログラムによってサポートします。情報セキュリティポリシー文書ならびに情報セキュリティプログラムは継続的な有効性と正確性を確保するために最低限でも年に一回は再評価を実施します。再評価結果は公開を推奨します。

2.6.2.11 ガバナンス・リスク管理

事業継続性管理・運用弾力性、相互運用性と可搬性、サプライチェーン管理・透明性と説明責任、法令と標準順守および脅威と脆弱性管理の各コントロール領域について詳細なサービス仕様を作成します。また、経営者は承認したサービス仕様を公開します。サービス品質はサービス仕様に基づいて第三者に検証可能となっていることを推奨します。サービス品質は継続的な有効性と正確性を確保するために常時計測し公開することを推奨します。

2.6.3 資源

サービスオーケストレーションの対象となる設備層、ハードウェア層、資源抽象化・管理層、サービス層に含まれるすべての資産やデータを総称して資源といいます。手順として実装をもつコントロールエリアもその実装については資源と認識されます。

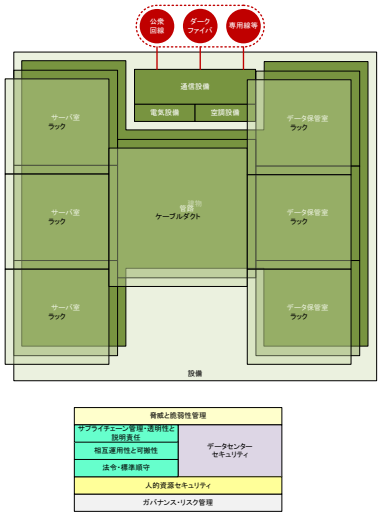


クラウドリファレンスアーキテクチャレイヤーモデル図

2.6.3.1 設備層と要件・手順の関係

手順および要件の観点から見て必須となる設備層でのセキュリティ対策は従来の情報セキュリティ施策の範囲を超えません。ただし構成面では、事業継続性管理・運用弾力性コントロールエリアの要件を高い水準で実現し、高可用性の実現を考慮した場合、変更制御と構成管理コントロールエリアを意識して本番環境とテスト環境が分離された、冗長構成を持った設備構成が必要となります。ローリングアップデート等による無停止運用を含む高可用性を実現する設備層を実現する際の冗長構成は n+1 構成となり最小限、設備を三重冗長させることになります。

法令・基準順守コントロールエリアの観点から見ると設備層の基底となる建物の立地選定にあたっては立地場所の適用法規と事業戦略の適合性検討が重要です。また、相互運用性と可搬性コントロールエリアの観点から見ても伝送遅延の大きさは光速度不変の法則に従い、利用者の所在地と立地場所の距離の隔たりが最大の決定要因となるためサービス品質に影響を与える重要な要素となります。

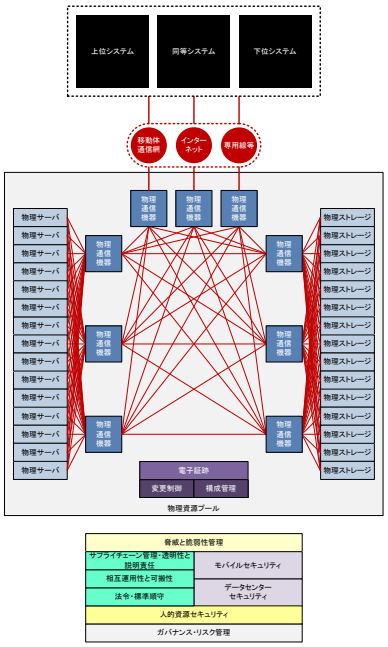


設備層（三層）

2.6.3.2 ハードウェア層と要件・手順の関係

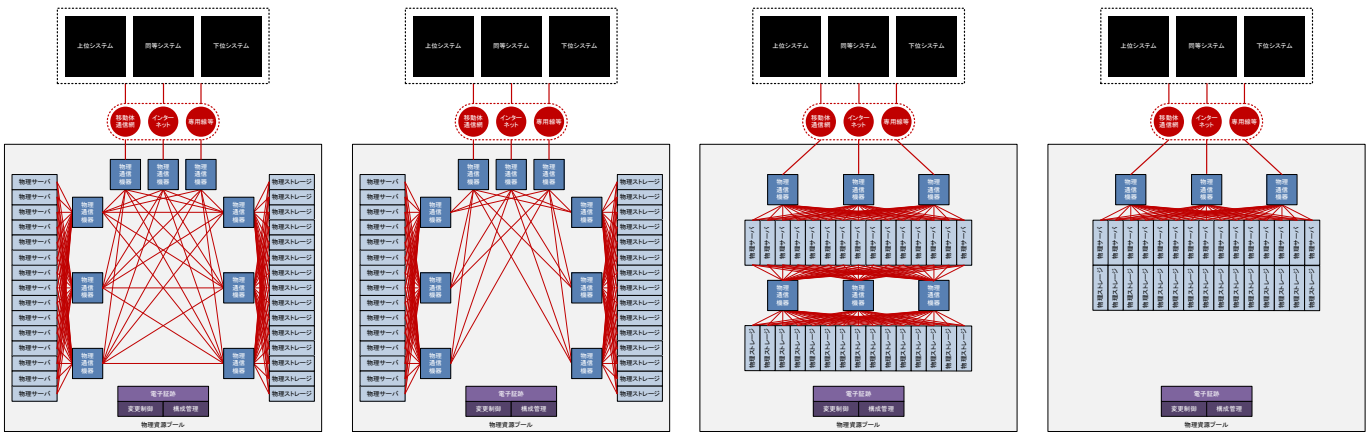
手順の観点から見ると必須となるハードウェア層でのセキュリティ対策は従来の情報セキュリティ施策の範囲を超えません。ただし構成面では、事業継続性管理・運用弾力性コントロールエリアの要件を高い水準で実現し、高可用性の実現を考慮した場合、変更制御と構成管理コントロールエリアを意識して本番環境とテスト環境が分離された、冗長構成を持ったハードウェア構成が必要となります。ローリングアップデート等による無停止運用を含む高可用性を実現するハードウェア層を実現する際の冗長構成は n+1 構成となり最小限、ハードウェアを三重冗長させることになります。

要件の観点から見ると市販製品を利用してハードウェア層を構成する場合のリスクは従来通りほぼ外部化できているといえます。オープンソースのハードウェアなどを利用してハードウェア層を構成する場合は、輸出規制法令や製品安全関係法令、技術基準適合認定、各種標準準拠などの担保が自己責任となり、市販製品利用と比較して、自由と責任負担のトレードオフおよび、開発コストおよびリスク負担と製品価格の間にトレードオフの関係が成り立ちます。



ハードウェア層

ハードウェア層を構成する物理サーバ、物理ストレージ、物理通信機器の接続構成は資源抽象化・管理層の実装構成とパフォーマンス特性に直接影響しサービス品質特性の決定に重要な影響を与えます。機器構成と接続構成は事業戦略の要求と要件および手順の制約を考慮して決定します。さらに機器構成と接続構成は資源抽象化・管理層の構成と合せてクラウドサービスのスケールアウト性能を決定する最大の要因でもあります。

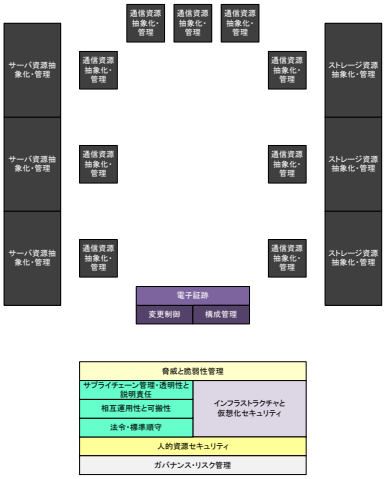


ハードウェア層接続バリエーション図

2.6.3.3 資源抽象化・管理層と要件・手順の関係

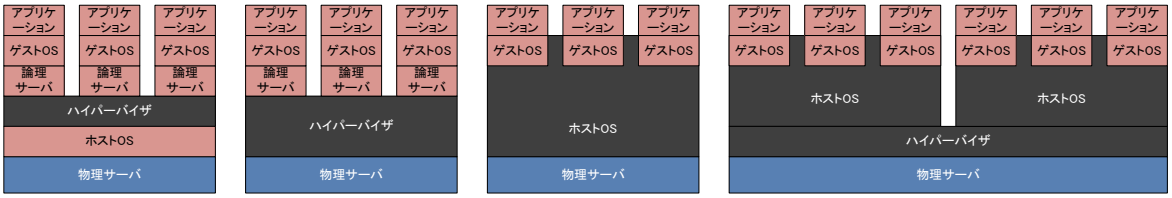
手順の観点から見ると必須となる資源抽象化・管理層でのセキュリティ対策は従来の情報セキュリティ施策の範囲を超えません。ただし構成面では、事業継続性管理・運用弾力性コントロールエリアの要件を高い水準で実現し、高可用性の実現を考慮した場合、変更制御と構成管理コントロールエリアを意識して本番環境とテスト環境が分離された、冗長構成を持った資源抽象化・管理構成が必要となります。ローリングアップデート等による無停止運用を含む高可用性を実現する資源抽象化・管理層を実現する際の冗長構成は n+1 構成となり最小限、実装モジュールを三重冗長させることになります。ハードウェア層の機器構成と一対一対応する資源抽象化モジュールは常時三重冗長している必要がありますが、抽象化資源量に余裕がありオートスケール能力をローリングアップデート能力による動的構成管理能力を持つ場合は、管理モジュールは二重化+最小規模のステージング環境の構成とすることができます。

要件の観点から見ると市販製品を利用して資源抽象化・管理層を構成する場合のリスクは従来通りほぼ外部化できているといえます。オープンソースソフトウェアなどを利用して資源抽象化・管理層を構成する場合は、輸出規制法令や知的財産権、各種標準準拠などの担保が自己責任となり、市販製品利用と比較して、自由と責任負担のトレードオフおよび、開発コストおよびリスクと製品価格のコスト振り替えの関係が成り立ちます。



資源抽象化・管理層

資源抽象化・管理層のうち、資源抽象化モジュールの実装はサービス層の実装構成とパフォーマンス特性に直接影響しサービス品質特性の決定に重要な影響を与えます。資源抽象化モジュール構成は事業戦略の要求と要件および手順の制約を考慮して決定します。さらに資源抽象化モジュールはハードウェア層の構成と合せてクラウドサービスのスケールアウト性能を決定する最大の要因でもあります。

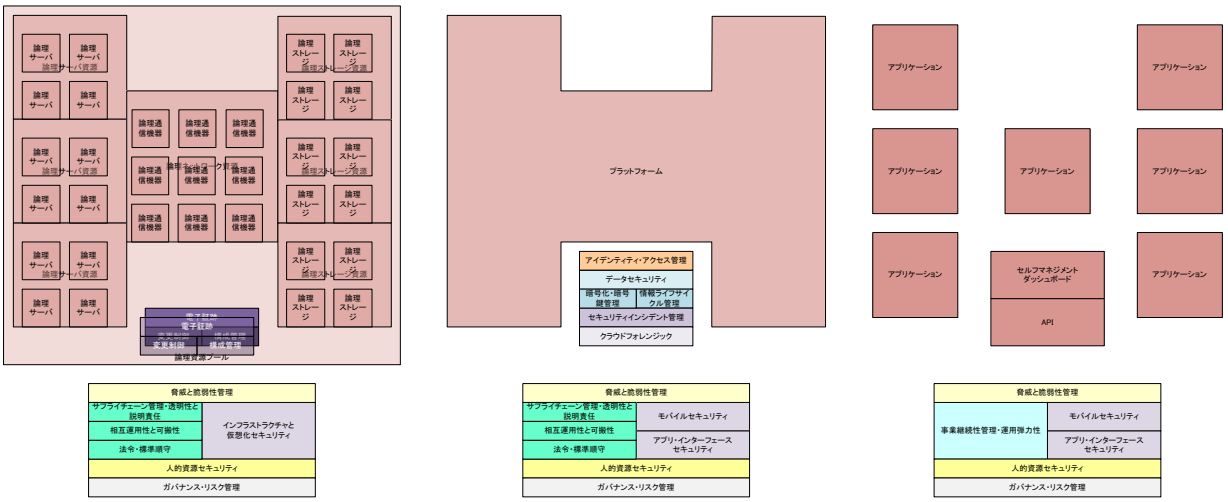


資源抽象化手法バリエーション図

2.6.3.4 サービス層と要件・手順の関係

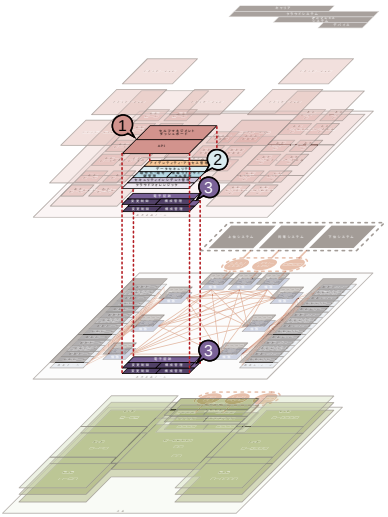
手順の観点から見ると必須となるサービス層でのセキュリティ対策は従来の情報セキュリティ施策の範囲を超えません。ただし構成面では、事業継続性管理・運用弾力性コントロールエリアの要件を高い水準で実現し、高可用性の実現を考慮した場合、変更制御と構成管理コントロールエリアを意識して本番環境とテスト環境が分離された、冗長構成を持ったサービス構成が必要となります。抽象化資源量に余裕がありオートスケール能力をローリングアップデート能力による動的構成管理能力が利用できる場合は、二重化+動的に生成されるステージング環境の構成と

することができます。ただし、二重化は物理資源層と資源抽象化・管理層が SPOF とならないよう系統毎に独立した物理資源層および資源抽象化・管理層を利用するべきです。同一の物理資源と資源抽象化・管理モジュール上に冗長サービスを構築した場合、同時処理能力の向上は得られますが可用性の向上はサービス層固有の脆弱性に起因する範囲に限定されます。
要件の観点から見ると市販製品を利用してサービス層を構成する場合またはクラウドプロバイダが提供するサービスを利用する場合のリスクは従来通りほぼ外部化できているといえます。オープンソースソフトウェアなどを利用してサービス層を構成する場合は、輸出規制法令や知的財産権、各種標準準拠などの担保が自己責任となり、市販製品利用と比較して、自由と責任負担のトレードオフおよび、開発コストおよびリスクと製品価格のコスト振り替えの関係が成り立ちます。



サービス層（IaaS、PaaS、SaaS）

資源抽象化・管理層と IaaS 層に実装をもつ電子証跡および変更制御と構成管理コントロールエリアは PaaS 層に実装を持つセキュリティインシデント管理、クラウドフォレンジックコントロールエリアが動作するための基盤となります。セキュリティインシデント管理、クラウドフォレンジックコントロールエリアはアイデンティティ・アクセス管理、データセキュリティ、暗号化・暗号鍵管理、情報ライフサイクル管理コントロールエリアによって保護され SaaS 層において API およびセルフマネジメントダッシュボードとして提供され、オンデマンドセルフサービスを実現することで、利用者の要求に応じて適宜・適切に配分することを可能にし、運用弾力性を実現します。



IaaS セルフマネジメントダッシュボードを例とした層を跨いで構成されるサービスモデル図

2.7 付録

2.7.1 参考文献

競争政策研究センター共同研究 ネットワーク外部性の経済分析
http://www.jftc.go.jp/cprc/reports/cr0103.pdf
RIETI 経済の強靭性に関する研究の展望
http://www.rieti.go.jp/jp/publications/pdp/12p008.pdf
経済産業省 システム／ソフトウェア製品の品質要求定義と品質評価のためのメトリクスに関する調査報告書
http://www.meti.go.jp/policy/it_policy/softseibi/metrics/20110324product_metrics2010.pdf
経済産業省 システム及びソフトウェア品質の見える化、確保及び向上のためのガイド
http://www.meti.go.jp/policy/it_policy/softseibi/metrics/product_metrics.pdf
ENISA Risk Management
http://www.enisa.europa.eu/activities/risk-management
ENISA Cloud Computing Security Risk Assessment（和訳）
http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf
IPA 共通脆弱性タイプ一覧
http://www.ipa.go.jp/security/vuln/CWE.html
Common Weakness Scoring System (CWSS™)
http://cwe.mitre.org/cwss/
2011 CWE/SANS Top 25 Most Dangerous Software Errors
http://cwe.mitre.org/top25/
WASC Threat Classification
http://projects.webappsec.org/w/page/13246978/Threat%20Classification
WASC Web Hacking Incident DataBase
http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database

2.7.2 図版出典

2.1 リスクモデル図

本文書初出

2.2 脅威・脆弱性・危害関連図

本文書初出

2.2 脆弱性分類図

本文書初出

2.2.4 クラウドリスク分類図

本文書初出

2.3.1 ネットワーク外部性効用曲線図

競争政策研究センター共同研究 ネットワーク外部性の経済分析掲載図を著者補足

2.3.1 相互運用性・可搬性モデル図

本文書初出

2.3.1 クラウド階層モデル図

本文書初出

2.3.1 クラウドアクター図

NIST SP500-292 掲載図を著者改変

http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 P4 Figure2 参照

2.3.2 エコシステム成長モデル図

IT Media TechTarget 利用者が IaaS の信頼度を計算するには？掲載図を改定
http://techtarget.itmedia.co.jp/tt/news/1210/12/news01.html

2.3.3 クラウドリファレンスアーキテクチャ図

OCDET/atoll project クラウドリファレンスアーキテクチャ v1.0 収録

2.5 クラウドガバナンスキューブ図

OCDET/atoll project クラウドリファレンスアーキテクチャ v1.0 収録

2.5 クラウドレイヤーモデル図（部分）

本文書初出

2.5 クラウドガバナンスマップ図

OCDET/atoll project クラウドリファレンスアーキテクチャ v1.0 収録

2..6 クラウドライフサイクル図

IT Media TechTarget クラウドの応答性能とサポート品質を客観的に比較するには掲載

http://techtarget.itmedia.co.jp/tt/news/1201/26/news01.html

2.6.1.2 相互運用性・可搬性が確保されたクラウドエコシステムにおける運用弾力性モデル図

IT Media TechTarget 利用者が IaaS の信頼度を計算するには？掲載

http://techtarget.itmedia.co.jp/tt/news/1210/12/news01.html

2.6.1.3 ネットワーク（グラフ）バリエーション図

IT Media TechTarget 着実に姿を現しつつあるクラウド化した IT 市場掲載

http://techtarget.itmedia.co.jp/tt/news/1206/19/news03.html

2.6.1.3 アクター連携およびサプライチェーンの透明性確保のための監査連携モデル図

本文書初出

2.6.1.4 スタンダード分類モデル図

IT Media TechTarget クラウドのベンダーロックインを回避するための処方せん掲載

http://techtarget.itmedia.co.jp/tt/news/1203/23/news07.html

2.6.1.4 クラウド関連標準一覧

本文書初出

2.6.2 クラウドガバナンスコントロールエリア挙動モデル図

本文書初出

2.6.3 クラウドリファレンスアーキテクチャレイヤーモデル図

OCDET/atoll project クラウドリファレンスアーキテクチャ v1.0 収録

クラウドリファレンスアーキテクチャレイヤーマップ v1.0 ポスターに再録

2.6.3.1 設備層（三層）

本文書初出

クラウドリファレンスアーキテクチャレイヤーチュートリアル 01 に再録

2.6.3.2 ハードウェア層

本文書初出

クラウドリファレンスアーキテクチャレイヤーチュートリアル 01 に再録

2.6.3.2 ハードウェア層接続バリエーション図

本文書初出

2.6.3.3 資源抽象化・管理層

本文書初出

クラウドリファレンスアーキテクチャレイヤーチュートリアル 01 に再録

2.6.3.3 資源抽象化手法バリエーション図

本文書初出

2.6.3.4 サービス層（IaaS、PaaS、SaaS）

本文書初出

クラウドリファレンスアーキテクチャレイヤーチュートリアル 01 に再録

2.6.3.4 IaaS セルフマネジメントダッシュボードを例とした層を跨いで構成されるサービスモデル図

本文書初出

クラウドリファレンスアーキテクチャレイヤーチュートリアル 02 に再録