OCDET/atoll project
Reference Publication
2013/04/05

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 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 v1.0

2013/04/05

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ます。世界的に広く受け入れられているNIST SP800-145に示されているクラウド定義とENISAや経済産業省などの定義の差分を整理し、NIST SP500-292 に示されているクラウドリファレンスアーキテクチャと TCI Reference Architecture に共通するレイヤー整理上の問題の解決を図ります。

1.2 対象読者

本文書は、NIST SP500-292 が定義しているクラウドプロバイダ、クラウドブローカ、クラウドオーディタ、クラウドキャリア、クラウドコンシューマとしてサービスを提供または利用している人々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. 定義

本文書では 2.1 に示される既存定義を準用します。独自の定義については 2.2 以降.に示します。

2.1 準拠定義

2.1.1 リスク、危害、安全 ISO/IEC Guide51:1999

2.1.2 脅威、脆弱性 ISO/IEC15408

2.1.3 脆弱性分類 Common Weakness Enumeration

2.1.4 脅威分類 Web Application Security Consortium

2.1.5 相互運用性、可搬性 ISO/IEC 25010

2.1.6 信頼性、保守性、可用性 ISO/IEC 2382-14

2.1.7 事業継続性、弾力性 ISO22301

2.1.8 サプライチェーン ISO28000

2.1.9 セキュリティフレームワーク The Open Web Application Security Project : OWASP

2.1.10 OSI 参照モデル ISO/IEC 7498-1

2.1.11 アクター分類 NIST SP500-292

2.1.12 エコシステム James F. Moore Predators and Prey: A New Ecology of Competition 1993 Harverd Business review

2.2 最小限のクラウド定義

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。

2.3 最小限のクラウド定義に基づくクラウドアーキテクチャ定義

2.3.1 設備層

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。

2.3.2 ハードウェア層

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。

2.3.3 資源抽象化・管理層

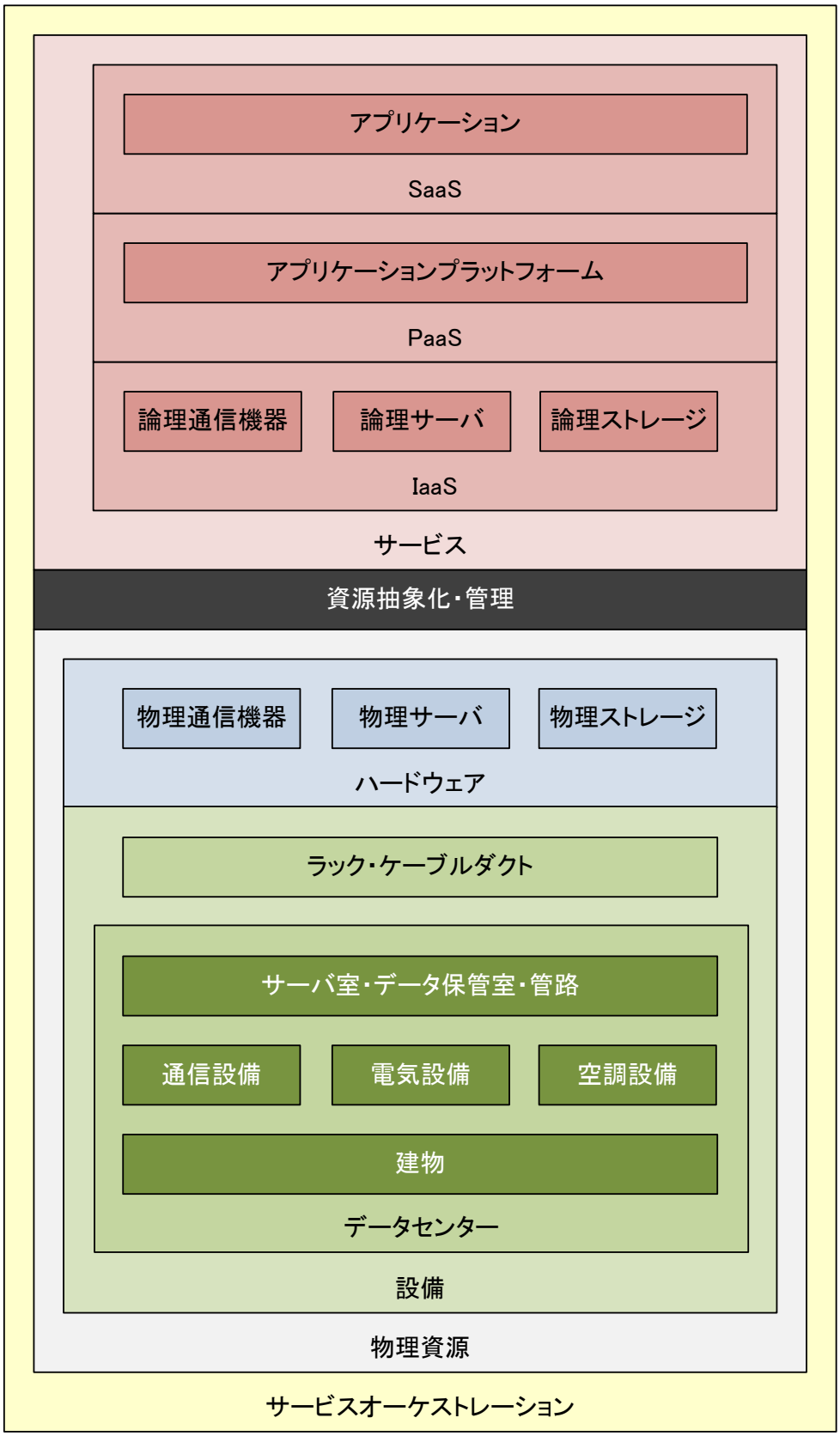
物理資源層を抽象化して後述するサービス層に提供する層となります。物理資源層の計算資源（サーバ）、記憶資源（ストレージ）、通信資源（通信機器）を管理し、仮想マシンなどの形態に抽象化して IaaS 層での利用を可能にします。サービス層に対する抽象化された物理資源の割り当て管理を含む構成管理と変更管理の機能も提供します。

2.3.4 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。

2.3.5 リファレンスクラウドアーキテクチャモデル図



2.4 ガバナンスドメイン定義

2.4.1 要件

クラウドがもたらす効果を実現するにあたって考慮されるべき条件を要件といいます。

2.4.1.1 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。

2.4.1.2 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。

2.4.1.3 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。

2.4.1.4 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。

2.4.2 手順

クラウドに求められる要件を満足させる処理過程を手順といいます。

2.4.2.1 脅威と脆弱性管理

各コントロール領域についての詳細なコントロールポリシーの作成と、経営者によって承認されたコントロールポリシーの公開とセキュリティプログラムによるコントロールポリシーに基づく実行をいい、コントロールポリシーとセキュリティプログラムの定期的再評価を含みます。

2.4.2.2 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。

2.4.2.3 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。

2.4.2.4 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。

2.4.2.5 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。

2.4.2.6 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。

2.4.2.7 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。

2.4.2.7 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。

2.4.2.8 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。

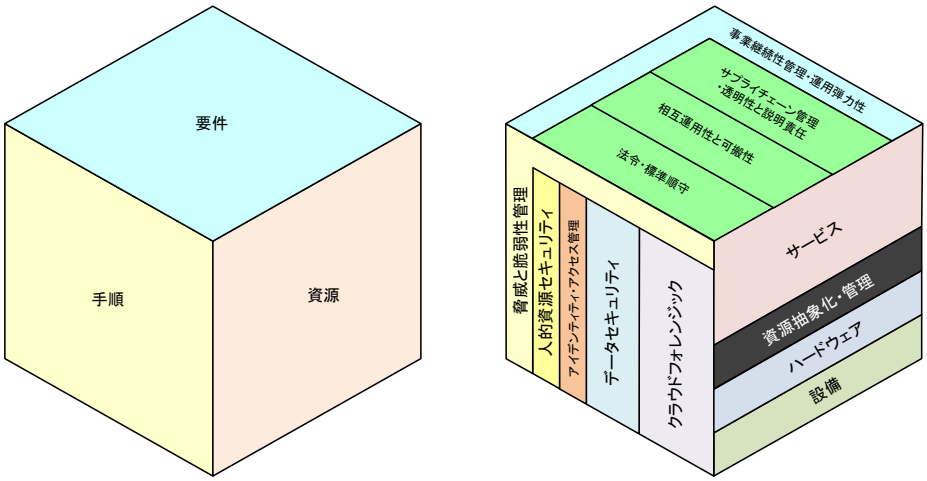
2.4.2.9 データセンターセキュリティ

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

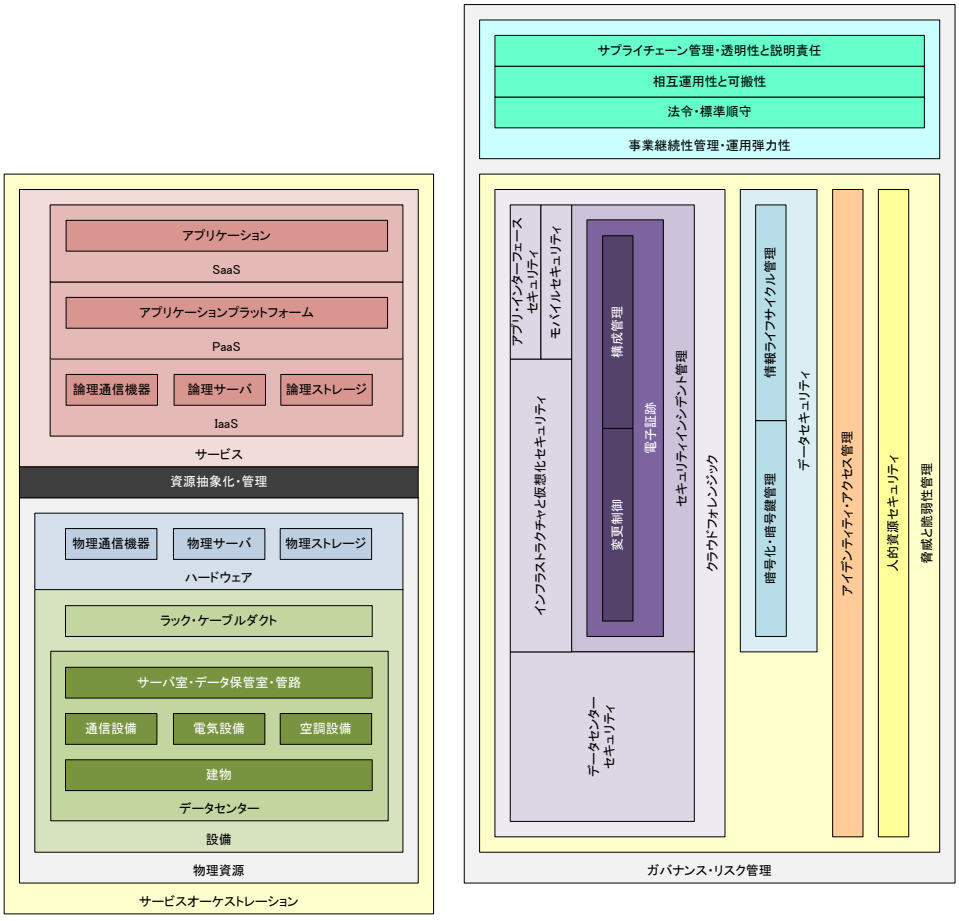
2.4.3 資源

手順の適用対象となるアーキテクチャおよび実装を資源と言います。本文書では 2.3 に示したリファレンスクラウドアーキテクチャを指します。

2.5 ガバナンスドメインのクラウドガバナンスキューブ表現



2.6 リファレンスモデルへのガバナンスドメインコントロールエリアマッピング



2.7 リファレンスモデルのレイヤーモデル表現とガバナンスドメインコントロールエリアマッピング