ORACLE

利用に当たっての注意点

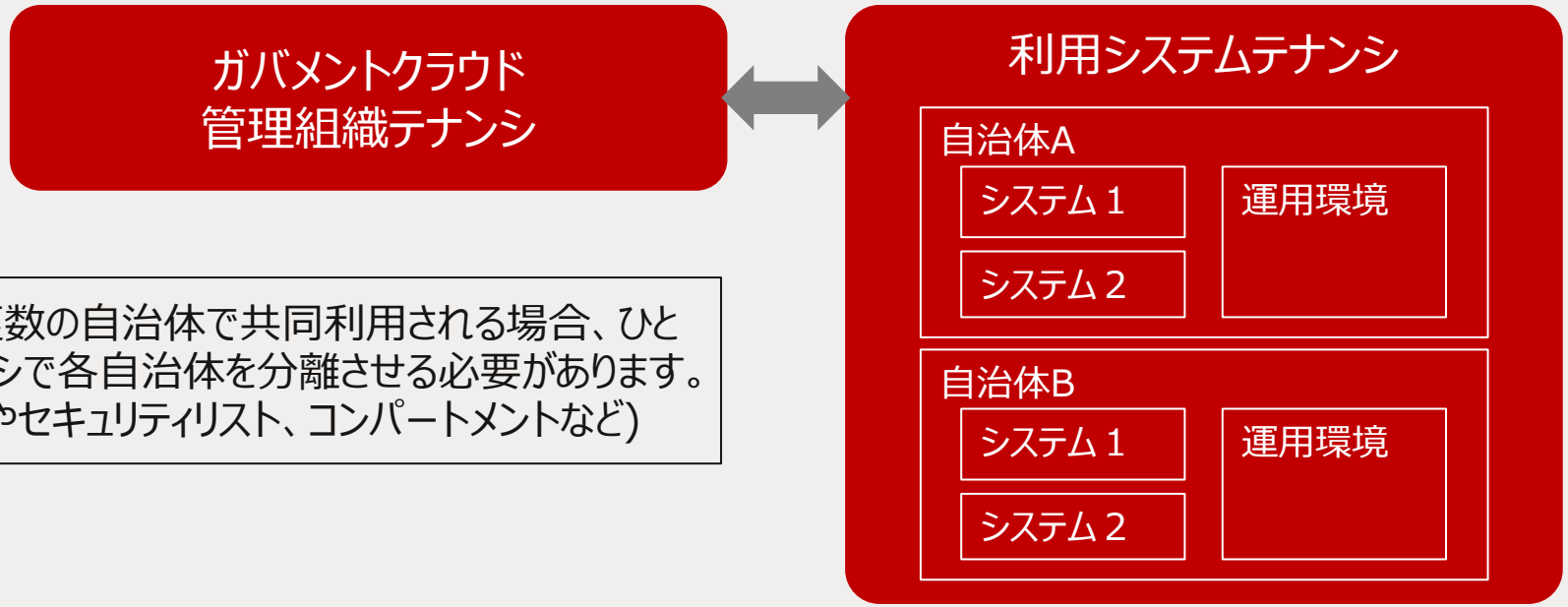
2025年2月吉日

日本オラクル株式会社
クラウド事業統括
公共・社会基盤営業統括　公共営業本部
デジタルガバメント推進部

安全なシステム

「移行に当たっての留意点」でも、ご説明したとおり、ガバメントクラウドでは全体管理のためのガバメントクラウド管理組織テナンシと、利用システム向けテナンシが存在します。利用申請に基づき払い出されるテナンシは、ガバメントクラウド管理組織の保有するテナンシより払い出され、各利用システムに付与されます。

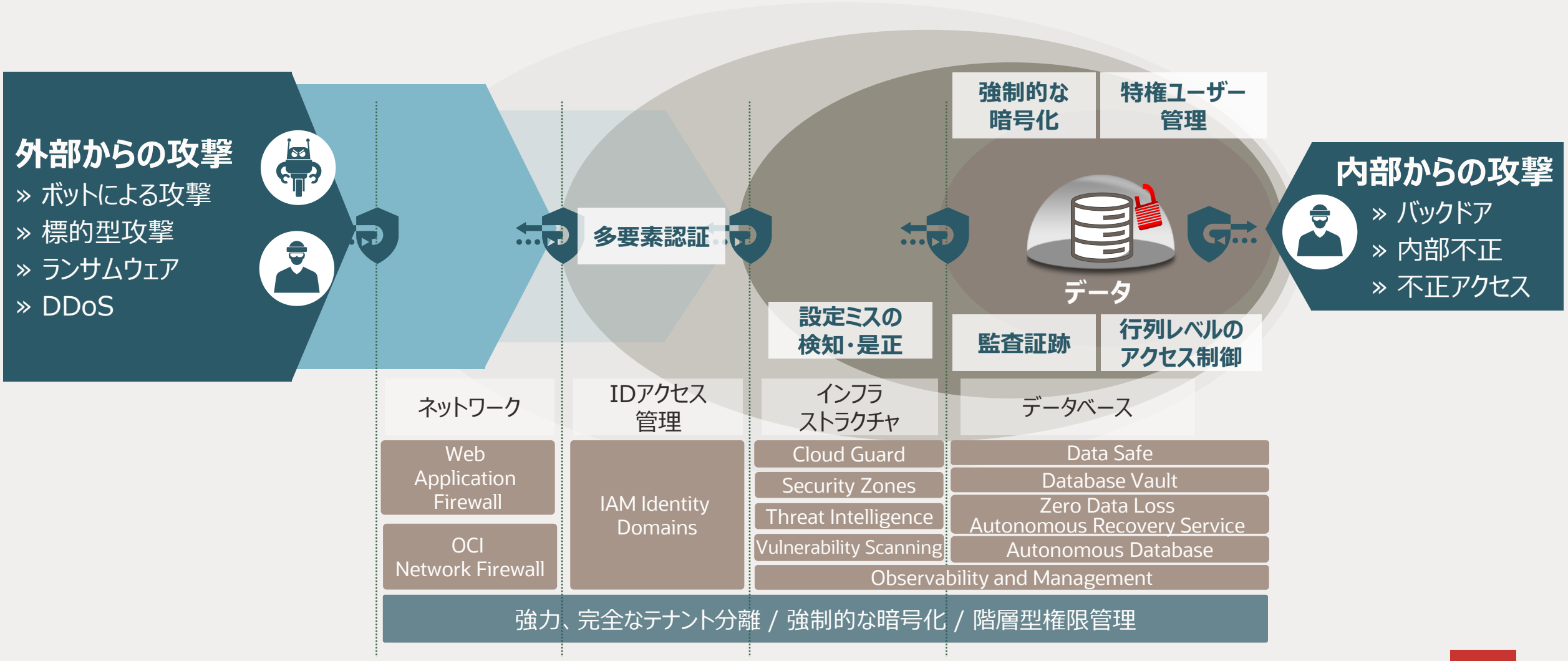
利用システムテナンシはOCIの全機能が利用可能な独立した環境ですが、必須適用テンプレートによりガバメントクラウドとして利用するための最低限の統制が強制されています。ただし、必須適用テンプレートで設定される統制はあくまで最低限であるため、利用システムはガバメントクラウドの利用ルールに従い安全なシステムを設計・構築・運用する必要があります。



例えば、複数の自治体で共同利用される場合、ひとつのテナンシで各自治体を分離させる必要があります。
(ルート表やセキュリティリスト、コンパートメントなど)

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

安全なシステム
多層防御によるデータ中心のセキュリティ



Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

安全なシステム

【ご参考】データベースを最大限保護するOracle Database Security

Oracle Maximum Security Architecture

ユーザーやセッション情報に基づいて
表のアクセスを列・行レベルで制限

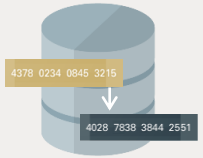
- Virtual Private Database
- Data Redaction
- Label Security
- SQL Firewall

DB管理者の無制限のアクセスを
強制的に禁止、厳格な職務分掌を実現

- Database Vault

アプリケーションへの影響がない
透過的な暗号化

- Transparent Data Encryption



機密データをマスキングし
セキュアなテストデータを作成

- Data Masking and Subsetting

アクセス制御

暗号化

監査

Oracle Database

認証強化

外部認証基盤による認証強化

- Centrally Managed Users
- トークン・ベース認証

データベースのアクセスログを
漏れなく詳細に記録

- Unified Audit

アクセスログの分析を自動化し
不正なアクセスの検知・アラート

- Audit Vault and Database Firewall

クラウド・サービス

- OCI Data Safe
- OCI Logging Analytics

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

安全なシステム

【ご参考】情報を安心、安全にご利用いただくためのOCIセキュリティ施策の提供

カテゴリ	機能	機能名	単価
セキュリティ・バイ・デザイン	強力、完全なテナント分離	Isolated Network Virtualization	標準機能
	強制的な暗号化	Encryption by Default	標準機能
	階層型権限管理	Compartment	標準機能
自動化されたセキュリティ管理	リスクのある設定を自動検知	Cloud Guard	無償
	ユーザーの振る舞い検知	Oracle Cloud Guard Threat Detector	無償
	SaaSユーザーの利用状況の監視	Oracle Cloud Guard Fusion Applications Detector	無償
	脅威インテリジェンスの集約・管理	Oracle Threat Intelligence Service	無償
	ポリシーの自動適用	Security Zones	無償
	脆弱性スキャン	Vulnerability Scanning	無償
	オンラインでのパッチ適用	Autonomous Database	無償 (*1)
	自動化されたログ分析	Logging Analytics	10GBまで無償
データ中心の多層防御	DBセキュリティ対策の自動化	Data Safe	無償～ (*2)
	特権ユーザー管理	Database Vault	DBCS HP ～ (*3)
	多要素認証、リスクベース認証	IAM Identity Domains	無償～ (*4)
	ボット対策とWAF	Web Application Firewall	無償～ (*5)
	次世代FW	Network Firewall	有償

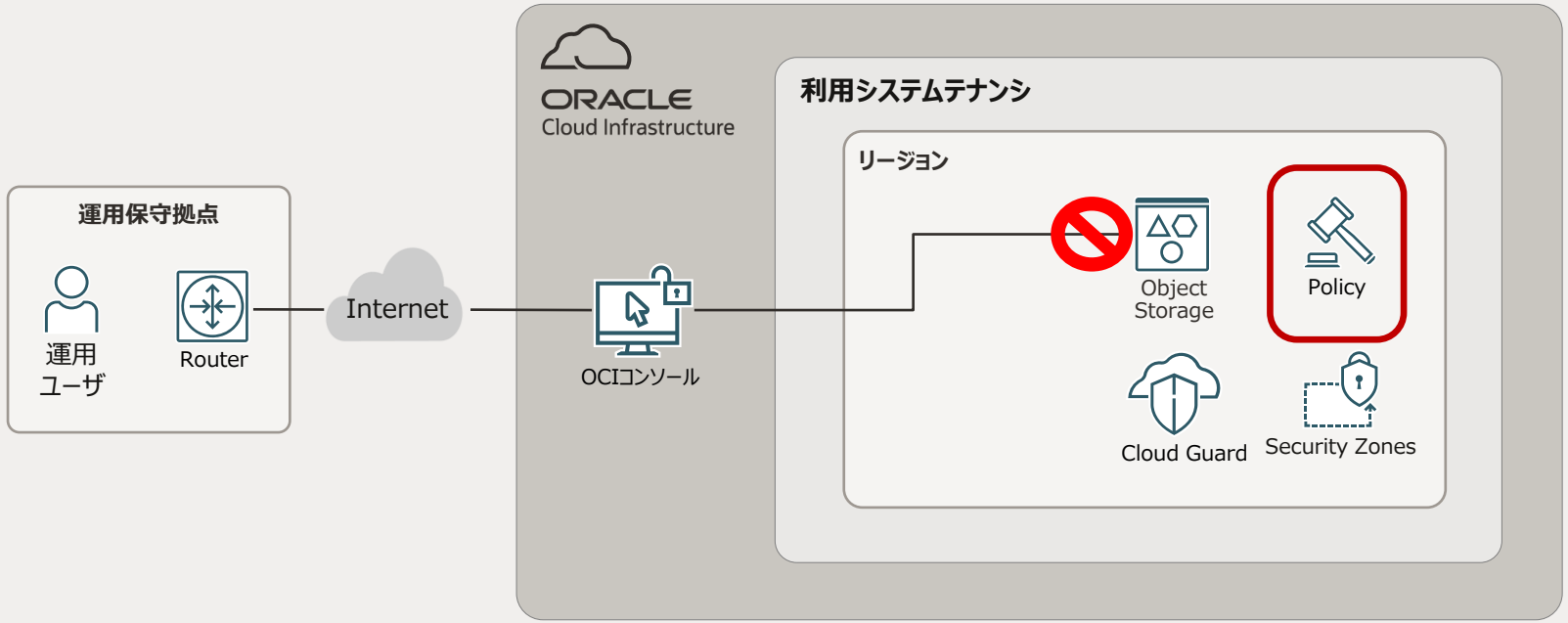
*1 Autonomous Database 利用時に無償で利用可能
*2 Oracle Cloud Databaseの利用でサービスを無償提供。監査記録の蓄積は100万レコード/ターゲット/月まで無償
*3 DBCS High Performance以上で利用可能
*4 無償で利用できるユーザー数や機能に制限あり
*5 1インスタンス、1000万インカミングリクエスト/月まで無償。価格単位：¥93 [1,000,000インカミングリクエスト/月]、¥775[インスタンス/月]

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

安全なシステム
インターネット経由でのObject Storage接続を抑止

オンプレミスや事業者とガバメントクラウドのネットワーク接続は、セキュリティが十分担保された上でインターネット経由での接続が基本となっています。しかし、自治体情報システムにおける三層分離の考え方に基づき、インターネットからのアクセスを抑止する必要があります。

デジタル庁様から払い出される利用システムテナンシには、予防的統制や発見的統制にてパブリック・アクセスが制限されていますが、APIキーやOCI管理コンソールを経由したインターネットアクセスも制限する必要があるため、ポリシーの設定で補完する必要があります。



Cloud Guard、Security Zones
(予防的統制、発見的統制)

オブジェクト・ストレージに対し、パブリック・アクセスを禁止する。

Policy

ネットワーク・ソースに登録した必要最小限のIPアドレスからのみオブジェクト・ストレージにアクセスできるようポリシーにて制御する。

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

安全なシステム
不要になったデータの破壊

OCIでは、廃棄したハードウェアにデータが残ることのないように、物理的な破壊と論理的なデータ消去のプロセスを使用しています。

ストレージ・メディアは、セキュリティの確保された容器で保管し、消磁と細断にて物理破壊されます。

ネットワーク接続で使用するストレージにおいては、AT Attachment (ATA)セキュリティ消去コマンドを使用してデータが消去されます。消去後はBIOSのフラッシュおよびドライバの更新により、ハードウェアを既知の良好な状態に戻すプロセスが開始され、ハードウェアに障害がないことを確認するテストが行われます。ワークフローが失敗するか、障害が検出された場合、そのホストにはさらなる調査が実施されます。

なお、データ消去の証明書を発行することはできませんが、下記のとおり、SOC2レポートにてご確認頂けます。

Oracle Cloud Infrastructureは、データが意図せず公開されることがないように、米国標準技術局(NIST)のSpecial Publication 800-88 Guidelines on Media Sanitization (媒体のサニタイズに関するガイドライン)に従っています。このガイドラインは、電子的サニタイズと物理的サニタイズの両方を網羅しています。

これらプロセスにおける監査結果については、Service & Organization Control 2(SOC2)レポートにて、ご確認頂けます。

ブロック・ストレージ・ボリュームを終了すると、暗号鍵が取消不可能な方法で削除され、データが完全にアクセス不可になります。

これらプロセスが正常に実行されたことは、お客様にもLoggingの監査ログにて確認頂くことが可能です。右にインスタンス(ブロック・ストレージ含む)を終了した際の監査ログ(抜粋)を記します。

※OCI内の通信とストレージは、強制的に暗号化されます。

<ブロックボリュームを含めたインスタンス削除で出力されるログの例>

"massage": "instance-name TerminateInstance succeeded”
com.oraclecloud.BlockVolumes.DeleteBootVolume.end
com.oraclecloud.BlockVolumes.DeleteBootVolume.begin
com.oraclecloud.ComputeApi.DeleteBootVolume.end
com.oraclecloud.ComputeApi.DeleteBootVolume.begin

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

Infrastructure as Code (IaC)の活用

Infrastructure as Codeはサーバーやネットワークなどのインフラ構成をプログラムのようなコードで記述し、そのコードを用いてインフラ構成の管理やプロビジョニングの自動化を行うことです。

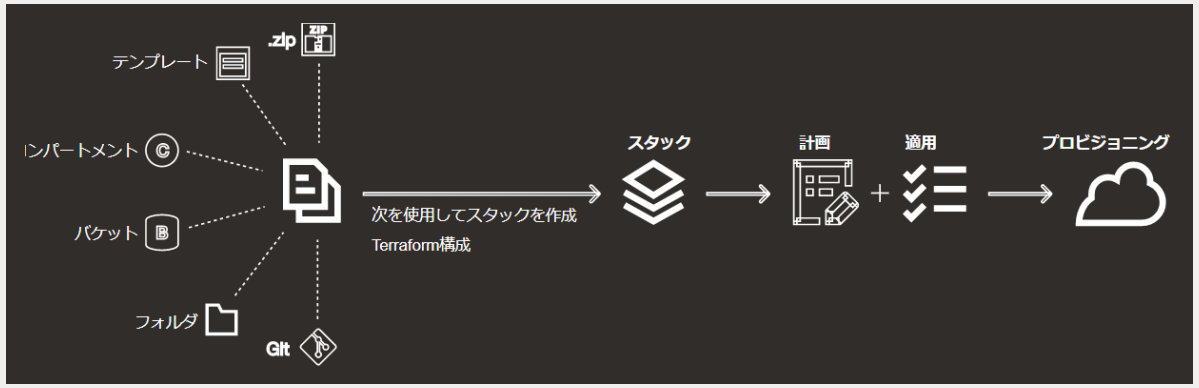
デジタル庁様より払い出された利用システムテナンシは、必須適用テンプレートをIaCを利用して予防的統制と発見的統制が適用されます。

同様に利用システムのインフラ構成も、管理やプロビジョニングをIaCにて自動化することで、作業の手間や時間を低減しつつ、属人化や煩雑さも減らすことが可能です。

OCIでは、業界標準のTerraformをベースにしたマネージのOCI Resource Managerを無償でご提供しています。

※業界標準のツールを使用することで、マルチクラウド環境においても同じコードを利用でき、学習コストの低減が可能

Resource Manager



Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

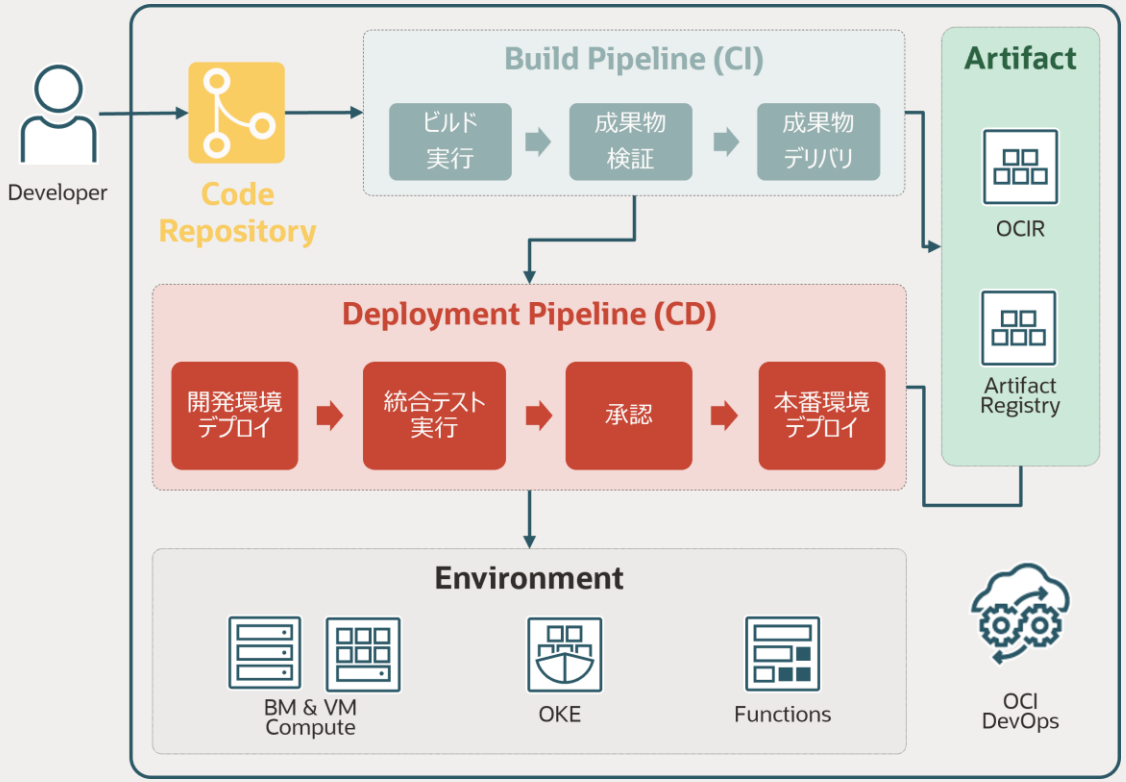
DevOpsの活用

アジャイル開発

素早い変化に対応するため、アプリケーション開発を効率化するアジャイル開発という手法があります。「計画、設計、実装、テスト」を機能単位に短いサイクルで繰り返す手法で、開発期間とサービスインまでの時間を短縮することが可能です。ウォータフォール開発と異なり、仕様変更に強く、常に進化する変化の多い事業や業務に適している言えます。

DevOps

短期間でのリリースを実現する手段として、開発と運用を一体化するDevOpsという考えがあります。開発(Development)と運用(Operations)が互いに協力することで、アプリケーションの品質を高め、より早く、安全にリリースし、業務や住民サービスを高めるため、「CI/CD」という手法や 、「コンテナ」、「コンテナ・オーケストレーション」といったテクノロジーの活用が期待されています。



OCI DevOps

注意：CI/CDパイプラインで利用するツールに特段の制限はないが、特定のベンダーのみが利用できるようなツールはベンダーロックインのリスクがあります。

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

業務継続の備え
データベースの可用性を向上させる方法

自治体業務の継続性を向上させるため、データベースの可用性を検討する必要があります。障害に備えローカルリージョン内にバックアップを取得したり、別リージョンに退避させることも大切なことです。

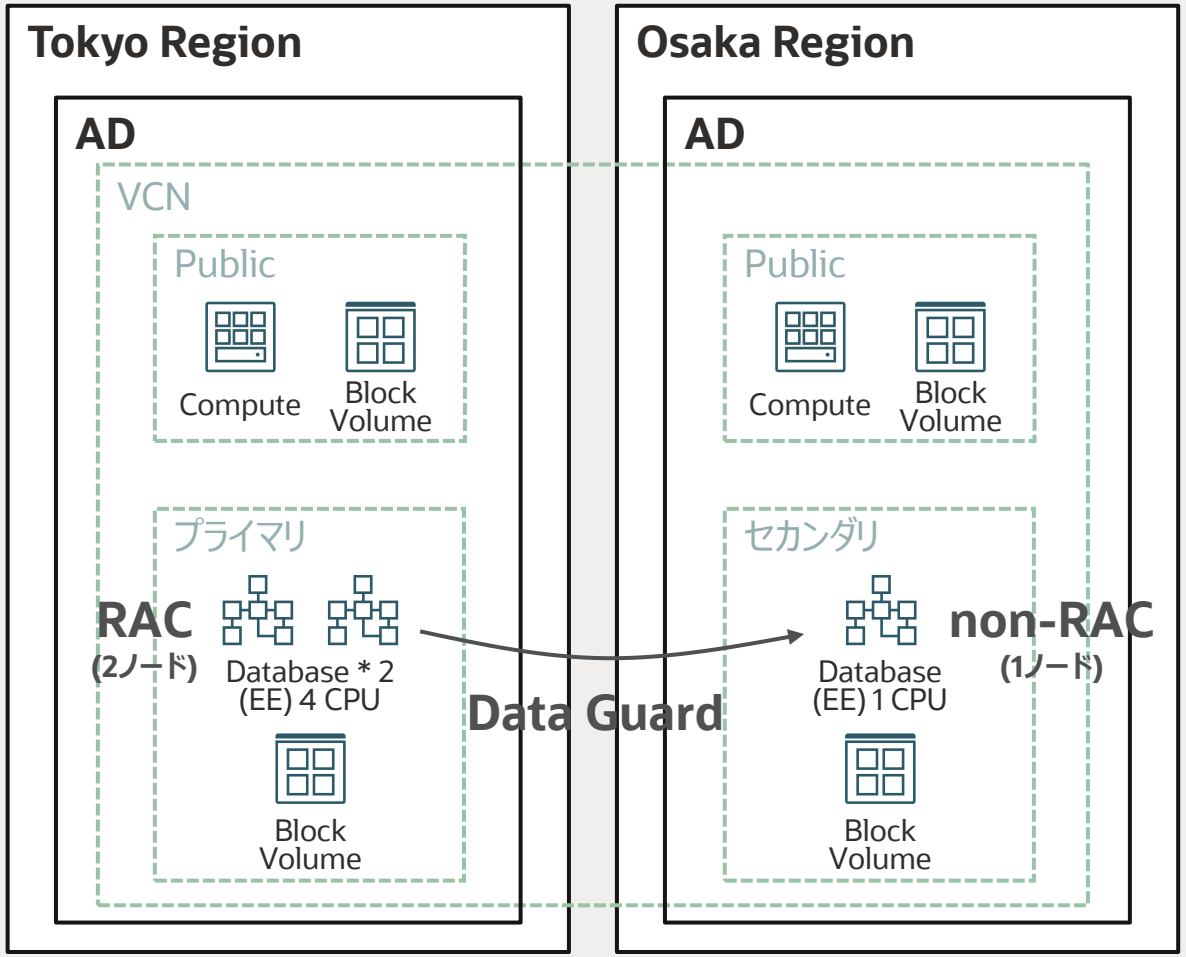
更にOracle Databaseでは、本番データベースの障害に備えたRACによるクラスタ機能やリージョン間でリアルタイムなレプリケーション機能もご用意しており、ご要件にあった可用性を検討頂けます。

Real Application Clusters (RAC)

- Active-Activeのクラスタ機能
- パブリッククラウドで唯一利用可能

Data Guard

- 災害/障害対策のためのレプリケーション機能
- 東京/大阪リージョン間で自動構成



Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

予実管理とコストの最適化

予実管理

ガバメントクラウドの利用にあたり、クラウド利用料の予算と実績の確認を行う必要があります。

予算設定は、日本円で月単位での設定を必須とし、任意で四半期単位、年単位等の設定を行います。

OCIは、円建ての価格設定となっていますので、予算設定が容易です。

また、タグまたはコンパートメント(ルート・コンパートメントを含む)を設定することで、必要な予算を分類して確認することも可能です。

コストの最適化

ガバメントクラウドが推奨する定常的なコスト管理運用フローは、クラウド利用料を月次で「可視化」「分析」「コストの最適化」の順に、コスト最適化基準の確認及び対策を行います。

OCIでは、支出トレンドのスポット・チェックおよびレポートの生成が可能なコスト分析(OCI Cost Analysis)を使用します。

また、予算の使用状況に、しきい値を設定し、アラートを発生させることが可能です。必要に応じてアラート情報を電子メールにて通知することができます。

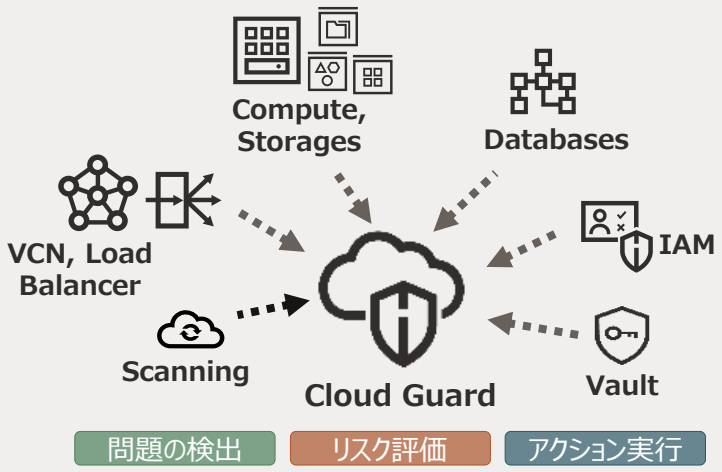
Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

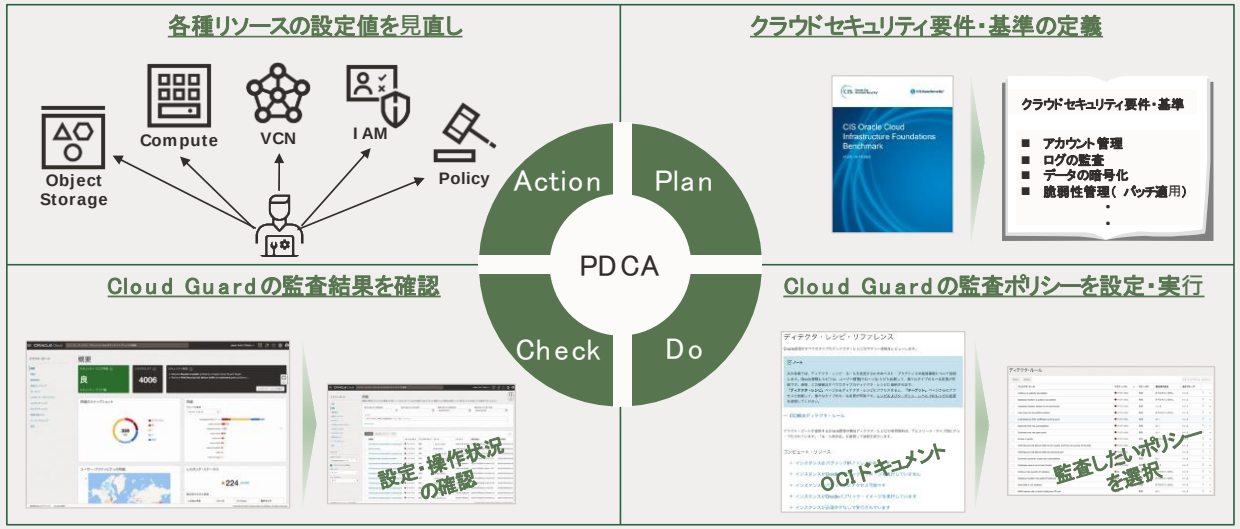
OCI Cloud Guard で発見された結果の調整　(発見的統制)

Cloud Guardは、OCIのリソース構成に関連するセキュリティ脆弱性がないか、およびオペレータとユーザーがリスクのあるアクティビティを行っていないかを調べ、ディテクタ・レシピにより問題が検出された際、OCIのリソース構成問題をユーザに報告します。

Cloud Guard の発見時アクションは、メールからの通知を受信し、Cloud Guardのダッシュボードを確認する必要がある場合と、日次/週次でCloud Guardのダッシュボードの確認を行う場合があります。

明らかに対応が不要と判断されたものについては、今後通知されないようディテクタ・ルールを修正することで、今後は問題として検出させないように設定することができます。





Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

データベース管理・監視

Database ManagementとEnterprise Manager(Diag/Tuning)の管理・監視サービス比較

Oracle Databaseの管理・監査には、オンプレミスで慣れ親しんで頂いたEnterprise ManagerをOCI上にセットアップ頂くことも可能ですが、マネージドサービスとしてご提供しているDatabase Managementをご使用頂くことも可能です。

EMのライセンス	EMの機能	O&M(DB Management)	タスク頻度
基本機能	DBの起動/停止	-	小
	可用性監視	○	
	パラメータ管理	○	中
	スキーマ管理	-	中
	記憶域管理	○(表領域管理)	中
	ユーザ/ロール/プロファイルの管理	○(監視)	中
	ジョブ	○(SQLジョブ:DML/DDL/PLSQL)	
	バックアップ/リカバリ	-	
	パッチ推奨	-	中
	複数DBの管理	○	

EMのライセンス	EMの機能	O&M(DB Management)	タスク頻度
Diagnostics Pack	AWR管理	○	中
	アクティブセッション履歴	○	高
	期間比較ADDM	○	高
	リアルタイムADDM	○	高
	稼働情報 (Exa,BaseDB,ExaDB-D)	○	高
	稼働状況のレポート	○(AWR,SQL,ASH)	
	ハング分析	○Blocking Session	
	メトリック作成	○*1	高
	通知（メールなど）	○(メール,SMSなど)*1	高

EMのライセンス	EMの機能	O&M(DB Management)	タスク頻度
Tuning Pack	SQLチューニングアドバイザ	○	高
	SQLチューニングセット	○	高
	自動SQLチューニング	○	高
	リアルタイムSQL監視	○	高

*Enterprise Managerの主要機能をもとに作成しております。
最新の情報は下記を参照ください。
Enterprise Manager13c(13.5)
https://docs.oracle.com/cd/F45244_01/oemli/enterprise-database-management.html#GUID-B7FDEFFE-DECB-4826-A3C8-7660B013C5DE

*1 OCI Monitoringまたはにて複数DBのメトリック問い合わせやアラートをセット
Stack Monitoringにてより詳細なメトリックを監視可能

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

Oracle Cloud Infrastructureの画面イメージ(1/2)
OCIコンソール

OCIにサインインすると、下記のようなOCIコンソールのHome画面が表示されます。

OCIコンソールでは、サービスを利用するためのメニュー・リンクが用意されています。

① サービスメニュー
② コンソール表示言語設定
③ リージョン選択・管理
④ OCIのステータス確認
⑤ サポート・サービス利用
⑥ お知らせ
⑦ Cloud Shell
⑧ 最新情報の紹介
⑨ リソースとサービスの検索
⑩ OCIコンソールの表示

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

Oracle Cloud Infrastructureの画面イメージ(2/2)
サブメニューへの遷移

左上のサービスメニューボタンをクリックすると各種OCIサービスを操作する画面へ遷移するメニューが表示されます。

①②③
右側の各種OCIサービスのリンクを押しますと、それぞれのサービス操作画面(サブメニュー)へ遷移します。

④
Home画面でお気に入りのサービスを固定してメニューをカスタマイズすると、すばやくアクセスしたり、最近の訪問から選択したりできます。

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

サービス制限 (Service Limits)

サービス制限の確認とサービス制限の引上げのリクエスト

一般的なクラウドでは、無制限にサービスを使用できるものではなく、初期状態でサービス制限が設けられており、サービス使用計画に合わせてサービス制限の解除が必要になります。

OCI でも同様にサービス制限が設定されており、その制限に達するとプロビジョニング時にエラーが表示されます。

(確認) 制限、割当ておよび使用状況

コンソールにて、ナビゲーション・メニューを開き、「ガバナンスと管理」-「テナント管理」-「制限、割当ておよび使用状況」を選択すると、画面上に現在の「サービス制限」「使用量」「使用可能」を表示されます。

(申請) サービス制限のリクエスト

コンソール右上の「ヘルプ」()-「制限の引上げのリクエスト」を選択し、「Support Chat」から「Limit Increase」を選択し、続けて応答メッセージの「Limit Increase」を選択することで、リクエスト画面が表示されるので、必要事項を入力し「サポート・リクエストの作成」をクリックして下さい。

サービス制限の引上げのリクエストは、早ければ数分で処理されますが、数日掛かることもありますので、サービス利用までの期間に余裕を持って実施頂きますようお願いします。

<ご参考> [Oracle Cloud Infrastructureドキュメント]-[サービス制限]

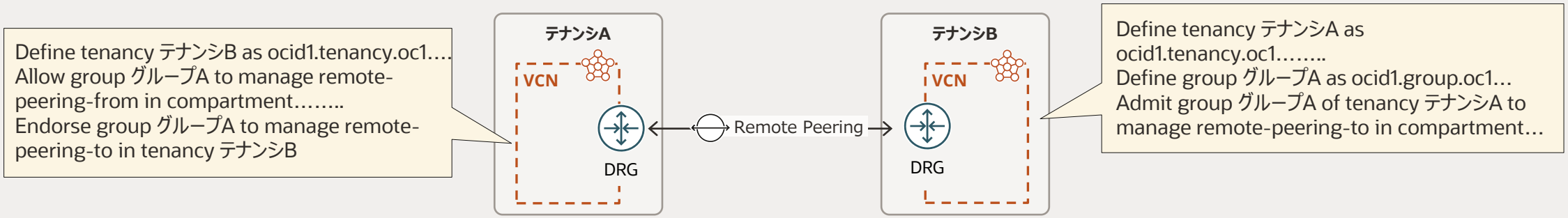
https://docs.oracle.com/ja-jp/iaas/Content/General/Concepts/servicelimits.htm

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

テナンシ間連携
クロステナンシ・ポリシーの設定

異なるテナンシのリソースにアクセスするためには、双方のテナンシで**クロステナンシ・ポリシー**を設定する必要があります。

例えば以下のように異なるテナンシのVCNをDRG経由でピアリング接続する際など、テナンシを跨いだリソースの利用時に必要になるのがクロステナンシ・ポリシーです。



クロステナンシ・ポリシーはルート・コンパートメントに対して適用するため、rootユーザー相当の権限が求められます。

一方で、現在ガバメントクラウド環境では各利用者に払い出されているAdminユーザーでは、ユーザー・コンパートメントまでの設定は可能ですが、ルート・コンパートメントに対しての操作は許可されていません。

そのため、クロステナンシ・ポリシーの設定が必要な場合には、別途デジタル庁様へご相談願います。

<ご参考> [Oracle Cloud Infrastructureドキュメント]-[クロステナンシ・ポリシー]

https://docs.oracle.com/ja-jp/iaas/database-tools/doc/cross-tenancy-policies.html

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

Oracle Cloud Infrastructure 主要情報一覧

https://blogs.oracle.com/oracle4engineer/post/oci-information

- OCIの主要技術情報一覧です。ご興味にあわせた情報を公開しております。

1 **OCI：サービス別資料一覧**

https://blogs.oracle.com/oracle4engineer/column_cloud_material

OCIの個別サービス毎の、概要資料、技術資料、チュートリアルへのリンク一覧です。

2 **OCI活用資料集**

https://oracle-japan.github.io/ocidocs/

OCIを使ってみたい! という方のための**技術ドキュメント集**。 OCIのサービス別技術資料をはじめ、PPTスライドを中心とした公開ドキュメントや、セミナーで使用した資料をアップロードしています。

3 **チュートリアル: OCI を使ってみよう**

https://oracle-japan.github.io/ocitutorials/

OCIを使ってみよう! という人のための**チュートリアル集**。各項ごとに画面ショットなどを交えながらステップ・バイ・ステップで、OCIの機能についてひととおり学習することができます。

4 **OCIサービスアップデート**

https://blogs.oracle.com/oracle4engineer/category/o4e-oci-service-update

毎月公開する**OCIのサービス・アップデート情報**をスライドで分かり易く説明。各サービスの詳細なアップデート情報は、各サービスのドキュメントや「OCI活用資料集」をご覧ください。

5 **Oracle LiveLabs**

https://apexapps.oracle.com/pls/apex/dbpm/r/livelabs/home

お客さまのクラウド環境ですぐに利用できる、**ハンズオン・ワークショップ**を多数掲載。画面キャプチャおよび実行コマンドを記載、実環境にて順を追って操作方法を学習することが可能です。ブラウザの翻訳機能でご利用ください。

6 **Oracleアーキテクチャ・センター**

https://docs.oracle.com/ja/solutions/

クラウド環境の検討や実装に役立つように設計された**リファレンス・アーキテクチャ**とソリューション・プレイブックのカタログを多数掲載。ダウンロード、カスタマイズ、およびデプロイできるコードまたはスクリプトも含む。解説ブログはこちら。

7 **OCIお客様活用事例**

https://blogs.oracle.com/oracle4engineer/post/oci-customer-reference

OCIを活用した**お客様の事例**のご紹介。データベースはもちろんのこと、アナリティックス、セキュリティ、システム管理、コンテンツ管理、ブロックチェーン、チャットボットなど様々なサービスのお客様事例をご紹介します。

8 **OCIセミナー情報**

https://blogs.oracle.com/oracle4engineer/post/oci-seminar

今後開催予定の**ウェビナー(含むハンズオントレーニング)**についてご案内します。

ほぼ毎週＋ハンズオンを様々なテーマで開催中！

9 **Oracle Code Night**

https://oracle-code-tokyo-dev.connpass.com/

オラクルのテクノロジーだけに限定しない、Developer（開発者）のDeveloper（開発者）によるDeveloper（開発者）のための**開発者向けコミュニティ Meetup セミナー。**

ほぼ毎週　様々なテーマで開催中！

10 **OCIドキュメント**

https://docs.cloud.oracle.com/ja-jp/iaas/Content/home.htm

各サービスの**公式マニュアル**です。

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

政府・地方公共団体向けOCI　ページ https://www.oracle.com/jp/cloud/government/

ガバメントクラウドに関わるお客様に向けて各種情報提供（タスクリスト・インタビュー記事等）

オラクル　地方公共団体  様々なドキュメント取得可能→

https://www.oracle.com/jp/cloud/government/

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

お問合せ窓口

見積り作成支援

OCI資格取得

資料提供

日本オラクル株式会社
クラウド事業統括　公共・社会基盤営業統括
デジタル・ガバメント推進部

oracle_governmentcloud_oci_jp_grp@oracle.com

OCI勉強会

その他

お気軽にお問い合わせください。

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.


ORACLE

Safe harbor statement

本資料はデジタル庁様の「ガバメントクラウド OCI 利用ガイド」(https://guide.gcas.cloud.go.jp/oci/)をベースに作成しています。

以上の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することを確約するものではないため、購買決定を行う際の判断材料になさならないで下さい。
オラクル製品に関して記載されている機能の開発、リリース、時期及び価格については、弊社の裁量により決定され、変更される可能性があります。

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.