ORACLE
Cloud Infrastructure

Oracle Cloud Infrastructure and the GDPR

欧州連合一般データ保護規則

ORACLEホワイトペーパー | 2018年4月

ORACLE

免責事項

下記事項は、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。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

目次

概要

欧州連合（EU）一般データ保護規則（GDPR）は、2018年5月25日に施行される新しい包括的なデータ保護法です。EU域内およびそれ以外の地域に拠点を置き、EU居住者の個人情報を収集および処理する組織に対して広く適用されます。

このホワイトペーパーでは、顧客がGDPRの要件を満たす上でOracle Cloud Infrastructureの機能がどのように役立つかを解説します。GDPRの要件について徹底的に論じたり、コンプライアンスに関する助言を行ったりするものではありません。顧客が自身で法的助言を求め、GDPRコンプライアンス・プログラムを策定および実施することを推奨します。

Oracle Cloud Infrastructureは、セキュリティに対する責任をOracle Cloud Infrastructureと顧客で共有するInfrastructure as a Service（IaaS）製品です。詳細は、『Oracle Cloud Infrastructure Security』ホワイトペーパーを参照してください。同様に、プライバシーに関するコンプライアンスもOracle Cloud Infrastructureと顧客で共有する責任です。このホワイトペーパーでは、こうした責任の共有について、GDPRとOracle Cloud Infrastructureに関連付けて解説します。

役割

GDPRでは、3種類の主な当事者が規定されています。

- **データ主体:** 管理者によって収集および処理されるパーソナルデータを所有する人
- **管理者:** データ処理の目的と手段を決定する事業体（エンティティ）
- **処理者:** 管理者の命令に従ってデータ処理のみを行う事業体（エンティティ）

次の図に、これらの役割の関係を示します。

データ主体 ↔ 管理者 ↔ 処理者

クラウド・サービス・ベンダーであるオラクルは、*処理者*.の役割を担います。Oracle Cloud Infrastructureの直接の顧客（Oracle Cloud Infrastructureの機能を使用してアプリケーションを構築する顧客）は通常、*管理者*の役割を担います。一方、こうした顧客には、Oracle Cloud Infrastructureで構築したアプリケーションのユーザーがいます。このユーザーは*データ主体*になります。前述の関係を手直しすると、次のようになります。

データ主体（ユーザー） ↔ 管理者（オラクルの顧客） ↔ 処理者（オラクル）

顧客データ

一般的に、Oracle Cloud Infrastructureは顧客とのやり取りの中で2種類のデータを扱います。

- **顧客のアカウント情報:** 顧客のOracle Cloud Infrastructureアカウントを運用するために必要な情報。この情報は主に、顧客への連絡と請求に使用されます。オラクルがアカウント管理の目的で顧客から収集する個人情報の使用は、オラクルのプライバシー・ポリシーに従います。顧客のアカウント情報を保有することになるため、Oracle Cloud Infrastructureはこの場合に限り、*管理者*の役割を担います。
- **カスタマ・サービス・データ:** 顧客がOracle Cloud Infrastructure内に保管することを選択したデータ。これには、データ主体ユーザーから収集されたパーソナルデータが含まれている可能性があります。オラクルは、このデータの内容について、あるいはこのデータの収集および使用に関する顧客の決定について関知しません。また、オラクルがデータ主体ユーザーと直接の関係を持たないことに注意してください。前に述べたように、顧客はこの状況における*管理者*であり、データを管理します。オラクルは、顧客の命令に従って行動する*処理者*です。

このホワイトペーパーの残りの部分では、カスタマ・サービス・データと、その中に含まれている可能性のある顧客のデータ主体ユーザーの個人情報に焦点を当てます。

原則

GDPR第5条で「パーソナルデータの処理に関する原則」が規定されています。この点に関連して、パーソナルデータには以下のことが求められます。

- 適法に、公正に、透明性のある手段で処理されること
- 限定的な目的のために収集および処理されること（目的制限）
- 目的のために必要な最小限の量であること（データの最小化）
- 正確であること
- 必要な期間に限って保管されること（保管制限）
- セキュアに処理されること（完全性と機密性）

以降の項では、これらの原則のいくつかについて、Oracle Cloud Infrastructureとその顧客がどのように責任を割り当てるか、または共有するかを概説します。

適法性、公正性、透明性

「パーソナルデータは、データ主体に関して適法に、公正に、透明性のある手段で処理されなければならない…」
第5条(1)(a)

適法な処理

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureは、データ主体ユーザーと直接の関係を持たず、顧客がデータ主体ユーザーから収集したデータについて関知しません。
- **顧客:** 顧客は、データ主体ユーザーから収集したパーソナルデータを処理するにあたり、（GDPRで規定されている）適法な根拠があるかどうかを確認しなければならない場合があります。

データ漏えい通知

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureにはインシデント対応のメカニズムおよびプロセスが用意されています。これらは、オラクルが実装したセキュリティ環境におけるデータ漏えいの可能性を検出できるよう設計されています。オラクルは、Data Processing Agreement for Oracle Cloud Servicesに記載された条件に従い、データ漏えいについて顧客に通知します。
- **顧客:** 顧客は、自身が管理するセキュリティ環境におけるデータ漏えいの検出について責任を負う場合があります。たとえば、Oracle Cloud Infrastructureでは、顧客のテナンシへのユーザー・ログインが不正に行われたかどうかを検出できません。顧客がOracle Cloud Infrastructure Auditサービスを使用して、Oracle Cloud Infrastructureに設定した環境を監視する必要があります。Oracle Cloud Infrastructureプラットフォームに実装した機能によっては、その他の監視ソフトウェアを実装できる場合もあります。また、顧客は管理者としてデータ漏えい通知規則に従うとともに、法規制が求める場合はデータ主体ユーザーまたは規制当局、あるいはその両方に通知しなければならないことがあります。

公正な処理

- **Oracle Cloud Infrastructure:** Oracle Services Privacy Policyで、オラクルが処理者としてデータを扱う際のアプローチ全般について、顧客に透明性を提供しています。
- **顧客:** 顧客がデータ主体ユーザーのパーソナルデータをどのように処理するか、またそのデータを処理する目的に関して、データ主体ユーザーに透明性を提供できるのは顧客自身のみです。オラクルは、顧客がOracle Cloud Infrastructureに保管および処理するデータについて、あるいはそれが特定のデータ主体に属するパーソナルデータかどうかについて関知しません。オラクルは、データ主体ユーザーと関係を持たないため、

顧客が管理者となるデータ処理の詳細について、データ主体ユーザーへの通知は行いません。顧客のみがその情報を提供できます。

場所の透明性

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureは顧客に対し、顧客のデータが処理および保管される場所についての透明性を確保しています。顧客は、Oracle Cloud Infrastructureアカウントを設定する際、最初にテナンシを配置するホーム・リージョンを選択します。顧客がデータをリージョン外に移動することを選択しないかぎり、顧客のデータはそのリージョン内にとどまります。Oracle Cloud Infrastructureは、テナンシ間またはリージョン間で機能する強力なサービスを提供します。Oracle Cloud Infrastructureでは（コンソールのユーザー・インタフェースとAPIドキュメントで）透明性が維持されており、顧客のアクションによってデータが別のリージョンやテナンシに移動する場合は必ず顧客に通知されます。
- **顧客:** オラクルは、顧客がOracle Cloud Infrastructureに保管するデータについて、あるいはそれが特定のデータ主体ユーザーに属する個人情報かどうかについて関知しません。データ主体ユーザーと直接の関係を持つこともありません。したがって、データ主体ユーザーのパーソナルデータが保管される地理的位置の詳細について、データ主体ユーザーに通知することが必要と顧客が判断した場合に、それができるのは顧客のみです。

監査

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure は 、Oracle Cloud Infrastructureのパブリック・アプリケーション・プログラミング・インタフェース（API）へのコールをログに記録する監査サービスを提供しています。この読取り専用のログは、ユーザー・データ・アクセスの透明性確保に役立ちます。
- **顧客:** 監査ログの記録は自動的に行われます。顧客は、監査ログの保存期間を設定できます。

目的制限

「パーソナルデータは指定された明確かつ適法な目的のために収集されなければならず、それらの目的と相いれない方法でさらに処理されてはならない…」第5条(1)(b)

技術的な観点から見ると、目的制限には以下を使用することで対応できます。

- コンパートメント
- 仮想クラウド・ネットワーク
- タグ付け

コンパートメント

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureでは、顧客が初期ルート・コンパートメント（またはテナンシ）の下にコンパートメントを作成できます。この種のプランニングを行うことにより、収集した個人情報の目的制限を徹底する上でのデータ管理目標を顧客が定め、それに沿った方法でクラウド・リソースを整理および分離することが可能になります。
- **顧客:** 顧客は、データ主体ユーザーの個人情報を収集および使用する目的を確認し評価する必要がある場合があります。

仮想クラウド・ネットワーク

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureの顧客が仮想クラウド・ネットワーク（VCN）を設定すると、アタッチされたコンピュート・インスタンス・リソースと通信できるようになります。このVCNには、VCN内での構成の単位となるサブネットが1つ以上含まれています。サブネットは、パブリック（デフォルト）またはプライベートに指定できます。プライベート・サブネットを使用する場合、アタッチされたコンピュート・インスタンスにパブリックIPアドレスが割り当てられることはありません。したがって、そのコンピュート・インスタンスにはインターネットからアクセスできなくなります。同じサブネット内のコンピュート・インスタンスはすべて同じルート・テーブルおよびセキュリティ・リストを使用します。このルート・テーブルおよびセキュリティ・リストは、類似したコンピュート・インスタンス・リソース間での一種の目的制限として機能します。
- **顧客:** 顧客はVCNアーキテクチャを慎重に計画する必要があります。VCNアーキテクチャにおける潜在的ネットワーク分離が次の構成のどちらによるにせよ、その分離が必要な目的制限に対応していなければなりません。
    - インターネットからアクセスできないプライベート・サブネット内のコンピュート・インスタンス
    - 共通のサブネット内で同じルート・テーブルおよびセキュリティ・リストを共有するコンピュート・インスタンス

タグ付け

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureでは、類似した目的を持つリソースにラベルを付ける柔軟なタグ付け操作が可能です。タグ付けを行うことで、ユーザーが同じタグ付けグループ内のリソースに対して特定の処理を実施できます。
- **顧客:** タグ付けは、顧客が類似の目的を持つリソースを集約するのに役立ちます。タグ付けを行うことで、同じタグの付いたリソースに対して一括操作を実行できます。顧客のテナンシにおけるタグ付けは、顧客の管理者が管理します。

正確性

「パーソナルデータは正確でなければならない…」第5条(1)(d)

データ・ストレージ

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureは、顧客が顧客データを正確に保管するために利用できるObject Storage、Block Volume、File Storageの各サービスを提供しています。
    - Object Storageサービスを利用すると、顧客は任意のコンテンツ・タイプの非構造化データを保管できます。Object Storageでは、チェックサムを使用してデータの完全性を能動的に監視し、破損データを自動的に検出して修復します。データの冗長性も能動的に監視し、保証します。冗長性の喪失が検出されると、追加のデータ・コピーを自動的に作成します。
    - Block Volumeサービスを利用すると、ブロック・ボリュームがコンピュート・インスタンスにアタッチされ接続されているときに、それを通常のハード・ドライブとして使用できます。データを失うことなくボリュームを切断して、別のコンピュート・インスタンスにアタッチすることも可能です。ボリュームは、データ損失から保護するために自動的にレプリケートされます。顧客が選択した場合はバックアップすることもできます。
    - File Storageサービスを利用すると、顧客は共有ファイルシステムの管理、ターゲットのマウント、ファイルシステムのスナップショットの作成が行えます。File Storageサービスでは、同期レプリケーションおよび高可用性フェイルオーバーを使用して、自己修復性に優れたデータ保護を実現しています。
- **顧客:** 顧客は、Oracle Cloud InfrastructureでObject Storage、Block Volume、File Storageの各サービスを使用して、データの正確なコピーを保持できます。これらのデータ・ストレージ・オプションは、顧客がビジネスの継続性、ディザスタ・リカバリ、長期アーカイブの目的で使用することも可能です。

可用性ドメインとレプリケーション

- **Oracle Cloud Infrastructure:** 顧客のテナンシは、顧客が選択したホーム・リージョンに作成されます。Oracle Cloud Infrastructureのリージョンは、物理的に分離されたフォルトトレラントな可用性ドメインで構成されます。この可用性ドメインは、レプリケートされたシステムの構築に顧客が使用できます。
- **顧客:** 顧客は、Oracle Cloud Infrastructureにおけるシステムを同じリージョン内の複数の可用性ドメインにまたがって構築することを選択できます。これを選択した場合、システムのレプリケーションが可能になるため、Oracle Cloud Infrastructureに保管されているデータの正確性をより効果的に維持することができます。

完全性と機密性

「パーソナルデータは当該パーソナルデータの適切なセキュリティを確保する方法で処理されなければならない。それには、不正または違法な処理に対する保護、および偶発的な損失、破壊または損傷に対する保護を含む…」第5条(1)(f)

カスタマ・サービス・データがホスティングされている顧客のクラウド環境のセキュリティは、次の方法を用いることで強化できます。

- 最小権限のアクセス制御およびポリシー
- 暗号化
- APIリクエスト認証
- 顧客の既存ネットワークに対するセキュア通信
- IDCSを介した多要素認証

最小権限

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureにおけるアクセス制御は、*最小権限*という概念に基づいています。新しいリソース（ブロック・ストレージ・ボリューム、コンピュート・インスタンスなど）は「デフォルトでセキュア」です。リソースが作成されると、顧客の管理者グループのユーザーのみにアクセス権が付与されます。その他の既存ユーザーのアクセス権は、顧客の管理者がポリシーを使用して明示的に付与する必要があります。顧客のテナンシに作成された新規ユーザーには、顧客の管理者がリソースへのアクセス権を明示的に付与する必要があります。この場合も、アクセス権の付与にはポリシーを使用しなければなりません。
- **顧客:** リソースへのアクセスは制限されており、デフォルトで最小権限に設定されます。顧客の管理者は、ポリシーを使用して明確に対処し、ユーザーへのアクセス権をオープンする必要があります。

暗号化

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureでは、次のサービスを通じて顧客のデータを暗号化します。
    - Block Volumeサービスの暗号化: Block Volumeストレージは保存時に暗号化され、バックアップもObject Storageで暗号化されます。
    - Object Storageサービスの暗号化: 各オブジェクトは専用の鍵で暗号化されます。暗号化はデフォルトで有効になっており、オフにすることはできません。
    - File Storageサービスの暗号化: データおよびメタデータは保存時に暗号化されます。暗号化をオフにすることはできません。

注意: この項で説明している暗号化は、基礎となるデータの性質にかかわらず行われます。Oracle Cloud Infrastructureでは、顧客のデータの性質（パーソナルデータなのか、機微なデータなのか、それ以外なのか）について関知しません。

- **顧客:** GDPR第32条(1)に、「セキュリティ・レベルをリスクに見合ったものにするために」取り得る技術的手段としてパーソナルデータの暗号化があげられています。顧客は、保管するデータのタイプにかかわらず、Block Volume、Object Storage、File Storageの各サービスによりデフォルトで暗号化を行うことができます。

APIリクエスト認証

- **Oracle Cloud Infrastructure:** 顧客によるOracle Cloud InfrastructureのパブリックAPIへのコールはすべて、セキュアな署名付きAPIリクエストを使用して行う必要があります。そうしないと、コールは失敗します。
- **顧客:** 顧客がOracle Cloud Infrastructure APIをセキュアにコールしたい場合、リクエスト署名手順に従ってOracle Cloud Infrastructure APIリクエストに署名する必要があります。

顧客の既存ネットワークに対するセキュア通信

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureでは、顧客は2種類の方法でOracle Cloud Infrastructure内の仮想クラウド・ネットワーク（VCN）から既存のオンプレミス・ネットワークにセキュアに通信できます。
  - IPSec VPN
  - FastConnect。この場合、トラフィックがインターネットを横断しないプライベート接続が提供されます。
- **顧客:** 顧客は、オンプレミス・ネットワークへの接続手順に従って、オンプレミス・ネットワークからOracle Cloud Infrastructure内のVCNへのセキュアなIPSec VPN接続またはFastConnect接続を設定することができます。

多要素認証

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructureの顧客は、Oracle Identity Cloud Service（IDCS）を通じて多要素認証（MFA）を使用できます。詳細は、「Oracle Identity Cloud Servicesによる多要素認証」を参照してください。
- **顧客:** 顧客がIDCS製品の追加を選択した場合、Oracle Identity Cloud Serviceとのフェデレーション手順に従って、Oracle Cloud Infrastructureインスタンスを IDCSとフェデレーションを行った後、MFAを有効にすることができます。

認証と第三者監査レポート

オラクルはOracle Cloud Infrastructureについて、ISO/IEC 27001 Stage 2とService Organization Control（SOC）1、2および3の監査を成功裏に完了しました。監査の対象となったのは、フランクフルト（ドイツ）、アリゾナ州フェニックス（米国）、バージニア州アッシュバーン（米国）の各データ・センター・リージョンにおけるCompute、Networking、Block Volume、Object Storage、Governance、Load Balancing、Databaseの各サービスです。

- EY/CertifyPointによって実施されたOracle Cloud InfrastructureのISO/IEC 27001:2013 Stage 2監査は、Oracle Cloud Infrastructureにおいて、情報セキュリティ規格ISO 27002:2013（情報技術 - セキュリティ技術 - 情報セキュリティ・マネジメントの実践のための規範）に従って情報セキュリティ・マネジメント・システム（ISMS）が設計および実装されていることを保証するものです。
- Ernst & Youngによって実施されたOracle Cloud InfrastructureのSOC 1 Type 2検査は、財務報告の内部統制に関する統制が効果的に設計され、機能していることを保証するものです。SOC 2 Type 2検査は、AICPA Trustサービスのセキュリティおよび可用性原則に関する統制が効果的に設計され、機能していることを保証するものです。SOC 3検査は、Oracle Cloud InfrastructureでIaaSサービスのセキュリティおよび可用性に関して効果的な統制が維持されていることを保証するものです。

Oracle Cloud Infrastructureのドキュメント

Oracle Cloud Infrastructureのサービスおよび機能の詳細は、Oracle Cloud Infrastructureのオンライン・ドキュメントを参照してください。

Oracle Cloud Infrastructureに関するその他のホワイトペーパーは、https://docs.us-phoenix-1.oraclecloud.com/Content/General/Reference/aqswhitepapers.htmにあります。

GDPRに関するその他のオラクル・ドキュメント

- セキュリティ
  - https://go.oracle.com/gdpr-compliance
  - https://www.oracle.com/uk/corporate/features/gdpr.html
- データベース
  - http://www.oracle.com/technetwork/database/security/wp-security-dbsec-gdpr- 3073228.pdf
- クラウド・アプリケーション
  - https://www.oracle.com/applications/gdpr/index.html

- Marketing Cloud
    - https://www.oracle.com/marketingcloud/about/events/gdpr.html

その他の参考資料

- オラクルにおけるプライバシー: https://www.oracle.com/legal/privacy/index.html
- Oracle Cloud Servicesの契約: http://www.oracle.com/us/corporate/contracts/cloud-services/index.html
- データ保護に関するEU公式ポータル: https://ec.europa.eu/info/law/law-topic/data-protection_en

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7000

オラクルをフォロー

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

Oracle Cloud Infrastructure and the GDPR
2018年4月
著者: Jim Feltis