ORACLE
Cloud Infrastructure

Oracle Cloud Infrastructureのプライバシおよびセキュリティ機能およびPIPEDA

カナダ個人情報保護および電子文書法

ORACLE WHITE PAPER | 2018年12月

ORACLE

免責事項

以下の事項は、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。マテリアルやコード、機能を提供することをコミットメント(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、認証、コンプライアンス状況の開発、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。

Oracle Cloud Infrastructureホワイトペーパーの最新版は
https://cloud.oracle.com/iaas/technical-resourcesでご覧いただけます。

目次

概要

カナダ個人情報保護および電子文書法(PIPEDA)とは、カナダのデータ・プライバシー法です。カナダに拠点を置き、個人の個人情報を収集し処理する、多くの組織に適用されます。

このホワイトペーパーでは、カナダのお客様がPIPEDAの原則を遵守する上でOracle Cloud Infrastructureの機能がどのように役立つかを説明します。PIPEDAの要件について徹底的に論じたり、遵守に関する助言を行ったりするものではありません。一般に、オラクルはお客様がOracle Cloud Infrastructureに保管するデータの内容や、お客様のデータの処理に関する特定の法的要件について関知しません。このホワイトペーパーは法的な助言をするものではありません。お客様がプライバシー・コンプライアンス・プログラムを策定、実施する場合や、法規制上の要件に関してOracle Cloud Infrastructureで提供される機能を評価する場合には、ご自身で弁護士に相談することをお薦めします。

Oracle Cloud Infrastructureは、データのセキュリティとデータのプライバシーに対する責任をOracle Cloud Infrastructureとお客様が共有するInfrastructure as a Service (IaaS)製品です(セキュリティの詳細は、『Oracle Cloud Infrastructure Security』ホワイトペーパーを参照してください)。

お客様のデータ

一般的に、Oracle Cloud Infrastructureはお客様とのやり取りの中で大きく分けて2種類のデータを扱います。

- **お客様に関するデータ**: これは、お客様のOracle Cloud Infrastructureアカウントの運用とサービスの料金請求に必要な情報です。オラクルがアカウント管理の目的でお客様から収集する個人情報の使用は、Oracle General Privacy Policyに従います。
- **お客様が保管するデータ**: これは、お客様がOracle Cloud Infrastructureに保管するファイル、ドキュメント、データベースなどのデータです。データには個人情報が含まれている可能性がありますが、オラクルは、このデータの内容、このデータの収集方法や使用方法、このデータがカナダその他の特定のデータ・プライバシー規制の対象になるかどうかについて関知しません。また、オラクルはエンド・ユーザー(お客様が個人情報を収集する可能性のある個人)と直接の関係を持たないことに注意してください。このデータはお客様が管理し、このデータの処理やこのデータを保管するリージョンについてもお客様が決定することになります。オラクルによるこのデータの扱いについては、Oracle Services Privacy PolicyとData Processing Agreementに記載されています。

このホワイトペーパーでは、お客様がOracle Cloud Infrastructureに保管するデータと、その中に含まれている可能性のある個人情報に焦点を当てます。

原則

PIPEDAは、組織が遵守しなければならない10の公正情報原則を定めています。

- 説明責任
- 目的の特定
- 同意
- 収集の制限
- 使用、開示および保持の制限
- 正確性
- セーフガード
- オープン性
- 個人のアクセス
- 遵守に関する異議

この後の項では、Oracle Cloud Infrastructureのお客様がOracle Cloud Infrastructureサービスを使用する際に、製品の機能をどのように利用すればこれらの原則を遵守できるかを概説します。このホワイトペーパーでは、これらの原則に対する責任をオラクルとお客様がどのように共有するかについても説明します。

説明責任

組織は、自身が管理する個人情報に対して責任を負う。これらの公正情報原則の遵守について説明責任を負う人を任命しなければならない。PIPEDA第1原則

- Oracle Services Privacy Policyに、グローバル・データ保護責任者が任命されているという説明があります。グローバル・データ保護責任者は、Oracle Cloud Infrastructureがお客様のデータの処理者としてオラクルの義務を果たしているかどうかといったプライバシーの問題について、現場からの問合せに対応します。
- オラクルのお客様はすべて、オラクルの義務に関するプライバシー上の懸念をいくつの方法で解消することができます。Oracle Cloud InfrastructureはOracle Services Privacy Policyを遵守しており、このポリシーの中で次の情報が提供されています。
    - プライバシー・コンプライアンスの問題についてオラクルのグローバル・データ保護責任者に連絡する方法の説明
    - データ・プライバシー問合せフォームへのリンク
    - プライバシーおよびセキュリティに関する苦情の解決プロセスの概要

- オラクルとお客様の間のData Processing Agreementに、オラクルのデータ保護プラクティスが記載されており、オラクルがその関連会社と第三者サブプロセッサにデータ保護プラクティスへの準拠を求めていることが示されています。

目的の特定

個人情報を収集する目的は、収集前または収集時に組織によって特定されなければならない。PIPEDA第2原則

- クラウド・プロバイダであるオラクルは一般に、お客様が個人からパーソナル・データを収集する目的について関知しません。

同意

個人情報の収集、使用または開示には、個人の認識と同意が必要である(不適切な場合を除く)。PIPEDA第3原則

- クラウド・プロバイダであるオラクルは、お客様がパーソナル・データを保管する可能性のあるエンド・ユーザーやその他の個人との関係を確立したり維持したりしません。そのため、お客様がパーソナル・データを取得することに関して、オラクルがエンド・ユーザーに通知することも、エンド・ユーザーから同意を得ることもありません。

収集の制限

個人情報の収集は、組織が特定した目的に必要なものに制限されなければならない。情報は、公正かつ合法的な手段で収集されなければならない。PIPEDA第4原則

- クラウド・プロバイダであるオラクルは一般に、お客様がエンド・ユーザーから収集してOracle Cloud Infrastructureで処理する個人情報について、またはそれが収集された目的について関知しません。

使用、開示および保持の制限

個人が同意している場合、または法によって義務付けられている場合を除き、個人情報はそれを収集した目的でのみ使用または開示できる。個人情報は、その目的を果たすために必要な期間のみ保持されなければならない。PIPEDA第5原則

- クラウド・プロバイダであるオラクルは一般に、お客様が個人からパーソナル・データを収集する目的について関知しません。ただし、Oracle Cloud Infrastructureには、お客様の目的限定に役立つ機能(タグ付け)やデータの保持および削除に役立つ機能(Object Lifecycle Management)があります。

タグ付け

オラクルは、柔軟なタグ付け操作をお客様に提供しています。タグ付けは、リソースに(複数のコンパートメントにまたがって)ラベルを付けて、同様の目的を持つリソースを集約し、そのリソース・グループに対して一括処理を実行するのに役立ちます。テナント管理者は、リソースのタグ付け戦略を策定して実施することにより、処理対象のデータを目的に即して収集することを徹底できます。

Object Lifecycle Management

オラクルは、データ・オブジェクトのアーカイブと削除を自動化するのに役立つObject Lifecycle Managementを提供しています。Object Lifecycle Managementを使用すると、同じバケット内のデータ・オブジェクトの存続期間の終了を、オブジェクトをアーカイブするのか削除するのかも含めて定義できます。

正確性

個人情報は、それを使用する目的を適切に果たすために可能なかぎり正確、完全かつ最新でなければならない。PIPEDA第6原則

- クラウド・プロバイダであるオラクルは一般に、お客様が個人情報を保管するかどうかや、その個人情報が個人に関して正確かどうかについて関知しません。ただし、Oracle Cloud Infrastructureは、データの正確なコピーを保管するのに役立つObject Storage、Block Volume、File Storageの各サービスを提供しています。これらのデータ・ストレージ・オプションは、ビジネス継続性、ディザスタ・リカバリ、アーカイブの目的でも使用できます。選択したデータ・ストレージ・サービスにかかわらず、データを保管するリージョンを必ず選択します。

データ・ストレージ

- Object Storageサービスを利用すると、多くのコンテンツ・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。お客様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、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。

セーフガード

個人情報は、情報の機微性に応じた適切なセキュリティによって保護されなければならない。PIPEDA第7原則

- Oracle Cloud Infrastructureは、ISO 27001監査を受け、SOC 1およびSOC 2の報告書を受領しています(「Oracle Cloud Compliance」を参照してください)。Oracle Cloud Infrastructureで提供されているセキュリティ関連機能の一部について、この後の項で説明します。

最小権限

最小権限方式では、パーソナル・データを保護するための1つの統制として、「need-to-know」の原則(知る必要がある人にだけ知らせるという原則)に基づいたアクセスが求められます。Oracle Cloud Infrastructureにおけるアクセス制御は、最小権限の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・ボリュームやコンピュート・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、当初は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。他のユーザーのアクセス権は、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。クラウド管理者は、このポリシーを使用して明示的なアクションを取り、「知る必要がある」ユーザーにまでアクセス権を拡大する必要があります。

暗号化

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、お客様のデータの性質（パーソナル・データなのか、機微データなのか、それ以外なのか）について関知しません。

データの保護に役立つ1つの方法として、暗号化を使用できます。データの暗号化は、保管され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提供されます。

- Block Volumeサービスの暗号化: Block Volumeストレージはデフォルトで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: 各オブジェクトが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います。
- File Storageサービスの暗号化: お客様のデータはデフォルトで保存時に暗号化されます。

コンパートメント

Oracle Cloud Infrastructureでは、お客様のテナントにコンパートメントを作成できます。コンパートメントにより、クラウド・リソース(たとえば、ブロック・ボリュームやコンピュート・インスタンス)とその中に含まれるデータを整理し、特定のグループのみがそれらにアクセスできるようにすることが可能です。管理者は、テナント内のコンパートメントをプランニングして作成できます。このプランニングでは、データ管理目標に即し、処理の対象となる個人情報の目的限定を徹底するのに役立つ方法で、クラウド・リソースを整理する必要があります。

仮想クラウド・ネットワーク

Oracle Cloud Infrastructureのお客様は、アタッチされたコンピュート・インスタンス・リソースとの通信を可能にする仮想クラウド・ネットワーク(VCN)を設定できます。このVCNには1つ以上のサブネットが含まれており、サブネットがVCN内の構成の単位となります。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として指定できます。プライベート・サブネットにアタッチされたコンピュート・インスタンスは、パブリックIPアドレスを持つことができません。したがって、こうしたコンピュート・インスタンスにはインターネットからアクセスできません。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・テーブルとセキュリティ・リストを使用します。このことが、同様のコンピュート・インスタンス・リソース間での一種の目的限定の役割を果たす場合があります。

VCNアーキテクチャは慎重にプランニング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、その分離が必要なセキュリティと目的限定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・テーブルとセキュリティ・リストを共有するコンピュート・インスタンス

お客様の既存ネットワークに対するセキュア通信

Oracle Cloud Infrastructureでは、2種類の方法でOracle Cloud Infrastructure内のVCNから既存のオンプレミス・ネットワークに通信できます。

- 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。

「オンプレミス・ネットワークへのアクセス」ドキュメントで概説されている手順に従って、オンプレミス・ネットワークからOracle Cloud Infrastructure内のVCNへのIPSec VPN接続またはFastConnect接続を設定できます。

Key Managementサービス

Oracle Cloud Infrastructure Key Managementは、お客様のデータの暗号化を、お客様が管理する鍵によって一元的に管理できるようにします。これを使用すると、マスター暗号化鍵とデータ暗号化鍵を作成する、鍵をローテーションして新しい暗号マテリアルを生成する、暗号操作で使用する鍵を有効化または無効化する、鍵をリソースに割り当てる、鍵を使用して暗号化と復号化を行い、データを保護するといったことが可能になります。

多要素認証

Oracle Cloud Infrastructureのお客様は、Oracle Identity Cloud Service (IDCS)を通じて多要素認証(MFA)を使用し、アカウントをさらに保護することができます(お客様のテナントはIDCSと自動的にフェデレートされるようになりました)。詳細は、「IAMフェデレーション」と「アイデンティティ・プロバイダおよびフェデレーション」を参照してください。

監査

Auditサービスは、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)に対するコールをログに記録します。ログに記録されたイベントのデータを使用すると、テナント内のアクティビティを監視できるようになり、データの保護に役立ちます。このロギングは自動的に行われます。お客様は監査ログの保存期間を設定できます。

データベース・セキュリティ

Oracle Cloud Infrastructure Databaseインスタンスを管理する際のセキュリティに関する具体的な推奨事項が「データベースの保護」ドキュメントに記載されています。この推奨事項には、次のツールの使用が含まれています。

- Transparent Data Encryption (TDE)とOracle Key Vault
- Database Security Assessment Tool (DBSAT)
- Audit Vault and Database Firewall (AVDF)

Oracle Databaseのセキュリティ・ガイド(「Oracle Databaseドキュメント」ポータルから入手可能)では、Oracle Cloud Infrastructureで実行することを選択したOracleデータベースのデータのアクセスとプライバシーを、次の機能を使用して強化する方法が説明されています。

- Virtual Private Database (VPD)を使用すると、セキュリティ・ポリシーまたはグループ・ポリシーを作成して、データベースへのアクセスを行および列のレベルで制御できます。これにより、複数のユーザーに対して単一スキーマへのアクセスを許可する一方で、それらのユーザーに無関係なデータへのアクセスを阻止することができます。
- Oracle Label Security (OLS)は、行のラベルをユーザーのラベルおよび権限と比較することで、行の内容へのアクセスを制御します。これにより、データ分類ラベルを定義して、機微データに対するアクセスの制御のような特定のビジネス要件やコンプライアンス要件を照合することが可能になります。

- Data Masking and Subsettingを使用すると、データのコピーまたはサブセット全体をOracleデータベースから抽出し、その中の機微データを検出、不明瞭化して、企業内外のパートナーと共有したり、非本番環境でのテストに使用したりすることができます。

クラウド・アクセス・セキュリティ・ブローカー

Oracle Cloud Infrastructure向けのOracle Cloud Access Security Broker (CASB)は、次の項目を監視し、検出されたセキュリティの問題について警告します。

- テナント内のリソースのセキュリティ
- 異常なユーザー行動
- その他のリスク

オープン性

組織は、個人情報の管理に関連したポリシーおよびプラクティスについての詳細な情報を公開し、容易に利用できるようにしなければならない。PIPEDA第8原則

- Oracle Services Privacy PolicyとData Processing Agreementで、オラクルがお客様のデータを扱う際のアプローチ全般について透明性を実現しています。ただし、クラウド・プロバイダであるオラクルは一般に、お客様がOracle Cloud Infrastructureに保管し処理するデータについて、またそれが特定のエンド・ユーザー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、エンド・ユーザーとは無関係であるため、お客様のデータ処理のいかなる詳細についてもエンド・ユーザーに通知しません。

個人のアクセス

要求に応じて、個人は自身の個人情報の存在、使用および開示について通知を受け、その情報へのアクセス権を与えられなければならない。個人は、必要に応じて情報の正確性および完全性について異議を唱え、情報を修正させることができるものとする。PIPEDA第9原則

- クラウド・プロバイダであるオラクルは一般に、どのような個人情報が個々のエンド・ユーザーから収集されてOracle Cloud Infrastructureで処理されるかについて関知しません。ただし、Data Processing Agreement に、Oracle Cloud Infrastructureサービスが必要なアクセスをお客様に提供しない場合にオラクルが行うことのできる支援について記載されています。

遵守に関する異議

個人は、組織における上記の原則の遵守について異議を唱えることができるものとする。個人からの異議には、組織におけるPIPEDAの遵守について説明責任を負う人(通常は最高プライバシー責任者)が対処すべきである。PIPEDA第10原則

- Oracle Cloud InfrastructureはOracle Services Privacy Policyを遵守しており、このポリシーの中で次の情報が提供されています。
  - プライバシー・コンプライアンスの問題についてオラクルのグローバル・データ保護責任者に連絡する方法の説明
  - データ・プライバシー問合せフォームへのリンク
  - プライバシーおよびセキュリティに関する苦情の解決プロセスの概要

認証と第三者監査レポート

オラクルはOracle Cloud Infrastructureについて、次の監査を成功裏に完了しました。

- ISO/IEC 27001:2013
- Service Organization Control: SOC 1およびSOC 2
- PCI-DSS
- HIPAA統制に関連した評価 詳細は「Oracle Cloud Compliance」を参照してください。

Oracle Cloud Infrastructureの参考資料

- Oracle Cloud Infrastructureのドキュメント
- 『Oracle Cloud Infrastructure and the European Union General Data Protection Regulation』ホワイトペーパー
- 『Oracle Cloud Infrastructure Security』ホワイトペーパー
- Oracle Cloud Infrastructureのその他のテクニカル・ホワイトペーパー

その他の参考資料

- オラクルによるプライバシーの取扱い
- Oracle Cloud Servicesの契約

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Oracle Cloud Infrastructureのプライバシおよびセキュリティ機能およびPIPEDA
2018年12月