

Global Customer Support Security Practices

発効日:2011年3月11日

概要

Oracle Global Customer Support (以下「GCS」といいます)は、オラクルのお客様(以下「お客様」といいます)のライセンス契約、お客様からのテクニカル・サポートの注文(以下「注文」といいます)及びOracle Software テクニカル・サポート・ポリシー及び/又はOracle Hardware及びSystems サポート・ポリシーの条件に基づいて、お客様に対し、プログラムとハードウェアの標準のテクニカル・サポートを実施する際、本書に明記されているSecurity Practiceに従います。Advanced Customer Servicesに関する条件はすべて、当該サービスの注文書に記載されるものとし、本書の適用範囲外となります。本書において「お客様のデータ」とは、お客様のコンピュータ・システムに保存され、サービスの実施中にリモート・アクセスされるあらゆるデータをいいます。オラクルは、オラクルの従業員及び業務委託先が、お客様の注文の条件及び本Global Customer Support Security Practicesに従いテクニカル・サポートを提供すること(提供の際に生じるお客様のデータへのアクセス及びその利用を含みます)について責任を負います。GCSのデータ管理のプラクティスやオラクルのテクニカル・サポート・ツールにより収集されるデータの管理方法について、より詳しい説明は、後述の「データ管理」セクションを参照してください。

本Global Customer Support Security Practicesは、オラクルの裁量により変更の可能性があります。ただし、オラクルによるポリシーの変更は、テクニカル・サポートについて既に支払われた期間中、本書に記載されているセキュリティのレベルについて実質的な低下を生じさせるものではありません。変更の詳細は[「変更履歴」](#)を参照してください。

情報セキュリティプログラム

オラクルの情報セキュリティ管理プログラムは、ISO/IEC 27001:2005に適合しており、オラクルは以下の内容に関する情報Security Practice及び手順を導入し、実行しています:情報セキュリティ・ポリシー;セキュリティの経営者責任(management responsibility);情報資産の所有権及び分類;物理的及び論理的なアクセス保護;ネットワーク;メディア及びO/Sのセキュリティ管理及び制御;監査及び監視;コンフィギュレーション管理及び変更管理;リスクの評価、軽減及び改善;ぜい弱性管理;インシデント報告及び管理;事業継続マネジメント;並びに遵守状況報告。

GCSのプラクティスは、オラクルのGlobal Information Security及びGlobal Product Security組織が策定したコーポレート・ポリシー、並びに、オラクルのGlobal Information Technology組織が定めた技術上のセキュリティ基準及び手順に適合しています。

GCSは、GCSのスタッフに対し、新入社員トレーニング・コース、特定のワークフロー及びビジネス事例に関するカスタム・トレーニング、及び「注目を集める話題(hot topics)」についての定期的なトレーニング及びコミュニケーションも提供しています。

GLOBAL CUSTOMER SUPPORTの業務

GCSは、グローバル規模の機能的能力(competencies)による技術問い合わせ(SR)管理、及びグローバル規模の業務割当、分類及び処理など、グローバル規模で業務を行っています。SRは、「follow-the-sun(太陽の動きに合わせた24時間体制)」モデルにより、重要性、時間帯及び発生した問題の性質に基づき、世界中のサポート・センターでGCSの技術者により処理されます。

Webによるカスタマ・サポート・サイト

オラクルは、お客様に対し、複数のカスタマ・サポートWebサイトを提供しています。各サイトは、それぞれ異なるオラクルのプログラム及びハードウェアの製品ラインをサポートするために機能しています。以下に記載されているものは、My Oracle Supportのサイトに適用されるSecurity Practiceです。各サポートWebサイトでサポートされているオラクルのプログラム及びハードウェアの詳細については、最新のオラクル・テクニカル・サポート・ポリシーをご覧ください。

My Oracle Supportのセキュリティ

My Oracle Supportは、オラクルのプログラム及びハードウェアについてGCSとのやり取り（SRアクセス、ナレッジ（Knowledge）検索／閲覧、サポート・コミュニティ及び技術フォーラムを含みます）を可能にする主要なWebサイト・サービスです。

My Oracle Supportでは、以下のセキュリティ制御が使用されています。

- My Oracle Supportは、Secure Socket Layer（SSL）暗号を使用したHTTPSエクストラネット用Webサイト・サービスです。
- お客様がMy Oracle Supportに登録する際は、お客様のサポート契約に紐づく固有のCustomer Support Identifier（CSI）が使用されます。
- 各CSIに対して、お客様はMy Oracle SupportのCustomer User Administrator（ユーザー管理者）を1名以上指定します。お客様のユーザー管理者は、ユーザーからの新規アカウント及び既存アカウントへのCSIの追加のリクエストを承認／拒否します。お客様は、適時にユーザーを追加及び削除することについて責任を負います。
- お客様のユーザー管理者は、お客様のユーザーがMy Oracle Supportでどの機能にアクセスできるかを制御することができます（例えば、特定のユーザーに対し、SR作成のアクセスを可能とする、又は不可能とするなど）。
- お客様のユーザー管理者は、自己のCSIに関連するユーザーを閲覧し、ユーザーのアクセス権限を削除することができます。
- My Oracle Support SRの添付書類（My Oracle Support SRの作成／更新プロセスの一部としてアップロードされるドキュメント）は、専用のGCSリポジトリに保存されます。お客様と当該リポジトリとのコミュニケーションは、Secure File Transfer Protocol（sftp）及び／又はHypertext Transfer Protocol over Secure Socket Layer（https）を使用して保護されます。
- GCSのリポジトリは、ファイアウォールで保護されたDemilitarized Zone（DMZ）ネットワークで展開されています。DMZは、プライベート・ネットワークのセキュリティを維持しながら、当該ネットワークへのインターネット・アクセス及び当該ネットワークからのインターネット・アクセスを許可するように設計されています。アプリケーション・サーバに直接インターネット接続をすることはできません。My Oracle Supportのサイトは、情報を暗号化し、発信元及び送信先の場所を隠すSSLアクセラレータ／リバース・プロキシを利用しているバーチャル・サーバに登録されたIPアドレスに解決します。SSL暗号化の終了時点で、リバース・プロキシは、アプリケーション・サーバにトラフィックを送ります。
- My Oracle Support SRの添付書類は、GCSリポジトリに転送され、SRがオープンになっている間、及びSRがクローズになってから7日間、保存されます。
- お客様が許可し、自己のプロファイルにSRに紐づく同一のCSIを有するユーザーのみが、My Oracle Supportでお客様のSRを閲覧することができます。
- オラクルに報告された技術上の問題は、Knowledge Managementの内容のベースとして利用されることがありますが、その場合においても、お客様及びお客様データ及びお客様に関連する記載は、Knowledge Managementの項目から削除されます。

テクニカル・サポートの実施で使用するテクノロジーのセキュリティ

GCSは、オラクルのプログラム及びハードウェアのサポートの双方で、SRの診断及び解決の一環として、多くの手法及びツールを使用します。当該手法及びツールに関連するセキュリティ基盤は、以下に記載されています。

Collaboration Tools

GCSは、オラクルに報告された問題を調査するため、プログラムに対してはOracle Web Conferencing (OWC)、ハードウェアに対してはOracle Shared Shell、という主に2つのcollaboration toolを使用します。両ツールは、共通した以下の特徴を有しています。

- お客様は全てのOWCセッションを管理し、それに積極的に参加することができます。お客様は、どのようなナビゲーションが行われるか、どのようなデータが表示されるか、及びどのようなコマンドが発行されるかなどについて、セッションを管理します。また、お客様は、理由の如何を問わず、いつでもセッションを停止することもできます。
- インターネット上で送信されるデータに対し、Secure Socket Layer (SSL) による暗号化が実施されま

す。

OWC及びShared Shellに関するその他の詳細は、以下になります：

- OWCは、お客様に対し積極的にSRの診断及び解決を支援するために、GCSが一对一のWeb会議を設定することを可能にします。
 - OWCは、追加のポートを開く必要なく、インターネット・プロキシ及びファイアウォールと連動するように設計されています。
 - お客様は、GCSの技術者がSR用のOWCセッション毎にパスワードを設定するよう要請することができます。
 - オラクルは、その後の診断及び解決のために、OWCセッションを記録する場合があります。お客様はGCSに対し、記録をやめるよういつでも自由に指示することができます。
- Shared Shellは、GCSがリモートでお客様のサポート対象のハードウェアの端末／コマンドのインターフェースを閲覧又はアクセスすることを可能にします。
 - お客様はセッション参加者のアクセスを制御することができます。お客様はセッションに参加者を招待し、参加者を承認／拒否することに責任を負います。お客様はいつでも参加者の接続を解除することができます。
 - 参加者に設定されるデフォルトのアクセス権は「view only」であり、参加者は端末／コマンドのウィンドウに表示される画面のみ閲覧することができます。お客様は参加者に対して「no execute」のアクセス権を選択し、参加者がコマンドをタイプすることは許可するが、コマンドの実行はお客様のみが可能な状態にすることもできます。あるいは、「full access」を選択し、参加者がコマンドをタイプして実行することを許可することもできます。
 - Shared Shellには、お客様とセッション参加者との間でファイルを転送する機能が含まれます。ファイル転送のリクエストは、お客様又は他のセッション参加者によって可能です。ファイル送信又は受信のリクエストを承認するのは、お客様のみ可能です。

- Shared Shellのイニシエータ・システムはオープンなインバウンドのコネクションを行ういかなるポートも必要としません；全てのインターネットのコミュニケーションは、イニシエータ・システムからのアウトバウンドのコネクションを通して開始されます。
- オラクルは、その後の診断及び解決のため、Shared Shellのセッションをログに残します。ログ・ファイルは、承認プロセスを通じてアクセスが制限されている、オラクルのシステムに保存されます。ログ・ファイルは、お客様が立ち上げたイニシエータ・システムにも保存されます。

プログラム及びハードウェアに対するツール

- GCSは、問題の解決を支援するため、データの収集を目的とする、多様なツールをお客様に提供します。これらのツールは、共通した以下の特徴を有しています。
 - ツールが起動しているシステム又はデバイスから本番データを入手、収集、伝送又は使用することはありません。
 - お客様の積極的な関与なくオラクルに直接データが伝送される際、多様な暗号化テクノロジーの1つを使用して伝送されます。

プログラム及びハードウェアのテクニカル・サポートに対して現在GCSが利用しているツールの一部について、以下に詳細が記載されています。その他のツールに関する追加情報は、My Oracle Supportにて提供されている場合があります。

プログラムに対するツール

Oracle Configuration Manager (OCM) はMy Oracle Supportからダウンロード可能であり、お客様の環境のコンフィギュレーション情報をアップロードするために使用されます。OCMは、コンフィギュレーション情報を収集し、その情報をオラクルのCustomer Configuration Repository (CCR) にロードします。自動的に収集されたコンフィギュレーション情報をオラクルに提供することは、任意であり、OCMライセンス契約の承諾を通じてお客様が同意した場合に限り行われます。

- お客様は、OCMのインストール及びコンフィギュレーションを管理します。お客様が、情報をオラクルに送信するようOCMを設定した場合、OCMは、定期的に、お客様が選択したコンフィギュレーションをオラクルのCCRにアップロードします。OCMは、オラクルへのアウトバウンド通信のみを起動し、インバウンド通信は受信しません。
- データベースの詳しいコンフィギュレーション情報を収集するために、お客様のオラクル・データベースは、特定のOCMが提供するPL/SQLプロシージャを用いて構成される必要があります。オラクル・データベースに対して実行できるスクリプトは、お客様がOCMをインストールした後にOCMにより提供されます。当該スクリプトは、オラクル・データベース内に「ORACLE_OCM」という名前のデータベース・アカウントを作成します。そのアカウントは、コンフィギュレーション情報を収集するPL/SQLプロシージャを保存し、収集を実行するデータベース管理システム (DBMS) ジョブを所有します。そのアカウントが設定されると、ログイン権限が必要なくなるか、求められなくなるので、そのアカウントは直ちにロックされ、パスワードは無効となります。
- お客様は、OCMの自動更新を可能にすることができます。OCMの自動更新には、認証及び暗号化が使用されます。ダウンロードされた更新版が適用される前に、デジタル署名が検証され、証明書（この証明書は、通信リンクを保護するために使用される証明書とは異なります）がオラクルに発行されたうえで更新版が署名されたことが確認されます。署名されたソフトウェアは、オラクルの企業ネットワークに接続されないシステム上にあります。
- オラクルにコンフィギュレーション情報を送信する際、OCMは、すべての通信に対して、公開鍵／秘密鍵の交換を利用したSecure Socket Layer (SSL) 及び業界標準のプロトコル (HTTPS) 並びに128ビット暗

号化（非対称暗号化としても知られています）を使用します。OCMは、オラクルが返送した証明書（オラクルが指定した公認認証機関が、オラクルに証明書を発行します）の問い合わせを行うことにより、オラクルを受信者として認証します。

- OCMアップロード・サーバは、ファイアウォールで保護されたDMZネットワークで運用されています。アプリケーション・サーバに直接インターネット接続をすることはできません。OCMのサイトは、情報を暗号化し、発信元及び送信先の場所を隠すSSLアクセラレータ/リバース・プロキシを利用して、バーチャル・サーバに登録されたIPアドレスへと解決します。SSL暗号化の終了時点で、リバース・プロキシはアプリケーション・サーバにトラフィックを送ります。そして、コンフィギュレーション情報が、オラクルの内部ネットワーク上のCCRデータベース層（CCR database tiers）に送信されます。
- オラクルは、セキュリティ関連の事象が特定された際に、それを阻止しそれに対応するため、ネットワーク侵入検知システム（nIDS）を活用して、OCMアップロード・サイトを継続的に監視しています。
- オラクルは、既知のぜい弱性を探知するため、四半期ごとに、OCMアップロード・サーバのぜい弱性スキャンを行っています。
- CCRで収集されたコンフィギュレーション情報は、オラクルのTier 4セキュリティレベルであるオーティン・データセンター内で守られ、オラクルのネットワーク・セキュリティ基盤及びセキュリティチームにより保護されます。
- お客様は、具体的なコンフィギュレーション情報及び削除要請の範囲を記載したSRに登録することにより、それらのコンフィギュレーション情報の削除を依頼することができます。

どのような情報がOCMにより収集されるか、それがどのように利用されるかなどの詳細については、My Oracle Supportで入手可能なOCMライセンス条件及びその他関連ドキュメントを参照してください。

Remote Diagnostic Agent (RDA) は、SRの診断及び解決に役立つ詳しい情報を提供します。コンフィギュレーション、パラメーター及びその他設定をシステムから検索するために、GCSでのSRの診断及び解決プロセスへの入力及びその状況としてのRDAスクリプトがGCSからお客様に提供されます。

- RDA情報は、お客様が保存します。ただし、お客様は、My Oracle SupportでのSRの登録及び更新プロセスを通じて、当該情報を添付情報としてアップロードするよう選択することができます。オラクルへのRDAのアップロードは、前述のとおり、専用のGCSリポジトリで保護されるものとします。

Database Diagnostic Data

オラクル・データベース（Release 11g以上）では、診断情報は、システムがその稼働中にエラーを検知した際に、データベースにより自動的に生成されます。診断データは、エラー、トレース、コンフィギュレーション及びデータベースの問題に関連するその他情報を提供するように設計されています。当該情報は、GCSが関与することなく、お客様が自己の問題を特定、診断及び解決するのに役立ちます。

- 診断データは、お客様が保存します。ただし、お客様は、My Oracle SupportでのSRの登録及び更新プロセスを通じて、診断データを添付情報としてアップロードするよう選択することができます。お客様は、OCMで保護されているネットワークを使って診断データをオラクルに転送することができます。オラクルへの診断データのアップロードは、前述のとおり、専用のGCSリポジトリで保護されるものとします。

ハードウェアに対するツール

システムに対するAuto Service Request

システムのためのAuto Service Request（以下「ASR」といいます）は、お客様のサポート対象のオラクルのハードウェアにおける障害を検出するために、障害イベントのテレメトリ（遠隔診断データ）によりハードウェアのテクニカル・サポートのプロセス自動化を支援し、診断及びサービス・リクエスト作成のた

め、オラクルにデータを転送します。お客様のシステムから入手し、オラクルに伝送・保存されたASRの情報は、診断及び解決のための製品障害情報と、テクニカル・サポートご利用の可否を確認するための顧客情報に限られます。それは、障害事象データ、登録データ、及びASR アセット・アクティベーション・データ（例えば、ホスト名、シリアル・ナンバー、及びサービス・リクエストのデータ）を含みます。

- お客様のシステムでASR managerを設定する上で、お客様は当該システムを登録し、プライベート暗号化キー／パブリック暗号化キーを交換します。オラクルのASRのコアのインフラストラクチャでメッセージ認証を提供するため、特定のASR managerのその後の全てのメッセージ（要求及び応答）を認証するには1024-bitのRSAキーが使用されます。
- お客様のASR ハードウェア・アセットを有効化している間、シリアル・ナンバーや製品情報を読み出すため、ASR managerは当該アセット上で稼動しているサービス・タグを見つけ出します。ASR managerは、ASRアセットからテレメトリ・メッセージを受信し、必要な場合は、アラームを有効化または停止するオペレーションを実行します。処理を行うためにテレメトリ・メッセージがオラクルのコアASRインフラストラクチャに送信される必要がある場合、当該メッセージはXMLデータ・ストラクチャーにコード化され、RSA with RC4（128 bit）SSL 暗号化を使用した HTTPS（port 443）にて送信されます。
- オラクルのコアASRインフラストラクチャは、ユーザー認証のためユーザー・アカウントの証明書、顧客システムの認証のためデジタル署名及び暗号化されたトラフィックを活用します。ASRによって保存される全てのデータは、複数層のセキュリティ・モデルにより隔離されています。このセキュリティは、複数層のAPIベースのアクセス及び権限管理を通して実施されています。コアASRインフラストラクチャに保存されているデータへの、直接的なアクセス及び外部からのアクセスはありません。

ストレージ（Service Delivery Platform）に対するAuto Service Request

ASR Service Delivery Platform（SDP）は、お客様のサイトに設置されている、オラクルが構成及び管理するサーバーで、お客様のサポート対象のオラクルのストレージ・デバイスに接続し監視します。SDPはオラクルのASRのコアのインフラストラクチャを利用するので、上述の「システムに対するASR」におけるインフラストラクチャ、ネットワーク、セキュリティ・プラクティスは、SDPと同じものです。オラクルはSDPに対して、以下の追加のセキュリティ対策も採用しています。

- お客様とオラクルの間の全てのSDPトラフィックは、オラクルが提供するVirtual Private Network（VPN）ルーター、又は、オラクルが提供するVPNルーターに接続可能なお客様のデバイスから起動されます。
- VPNを通してお客様のストレージ・デバイスにアクセスするオラクルのサービス・エンジニアは認証されており、指定されたSDPグループの権限の一部である様々な役割をアサインされています。全てのエンジニアの認証情報は、シークレットキーを使って暗号化されます。SDPは認証プロセスにHTTPプロトコルを利用します；しかしながら、HTTPはユーザーのパスワードを暗号化しないため、当該ユーザーのセッションは2048 bit RSA認証を使って暗号化されます。
- お客様のストレージ・デバイスに保存されている本番データは、オラクルのサービス・エンジニアには見えません。
- SDPサーバーの設置においては、運用前にお客様にネットワークの変更を求める場合がありますので、お客様の正式なレビュー及び承認を必要とします。暗号化タイプ及びVPNトンネルのハッシュ・アルゴリズムは、この正式レビュー中に確認及び同意されます。
- SDPセキュリティのメカニズムは、リモート管理ツールのためのCERT／Coordination Centerガイドラインに従っています。
- 追加の詳細はSDP Security White Paperにて参照することができます（ご要望により提供可能です）。

データ管理及び保護

GCSプラクティスは、オラクルの情報保護に関するポリシーに適合しており、当該ポリシーは、お客様のデータを、オラクルにおいて最も機密性の高い2種類の情報に分類しています。また、当該ポリシーは、お客様のデータの保存及び配布について制限を加えています。

GCSは、SRデータを、テクニカル・サポート関連の情報に関する個別の保存期間に関する規定に従い保持しています。GCSは、お客様のデータ及びメディアの安全な処分についてコーポレート・セキュリティ・ポリシーに従います。

データ管理

GCSは、お客様のデータの作成又は更新は致しません。オラクルがテクニカル・サポートの提供にあたり、お客様のデータにアクセスする場合には、GCSは、<http://www.oracle.com/jp/corporate/privacy2-150700-ja.html>及びそこからリンクに記載されているオラクルの個人情報保護基本方針/情報保護基本方針/プライバシー・ポリシーに従うものとします。

お客様のデータへのアクセスは、セントラル・プロビジョニング・リポジトリでセットアップされるアクセス権（承認プロセスの対象となります）により、職務／職責に基づきオラクルにより付与されます。

お客様は、自己のコンピュータ環境にあるお客様のデータについて継続して管理し、責任を負うものとします。お客様は、自らによるお客様のデータの収集に関するあらゆる事項（収集の範囲及び目的の決定及び管理を含みます）について責任を負います。お客様がオラクルに対し、サービス実施中に使用するために個人を識別可能な情報を提供した場合、お客様は、当該データの収集及び使用に関して必要となる通知を行い、及び／又は必要となる同意（オラクルがサービスを提供するために必要となるあらゆる同意を含みます）を得る責任を負います。オラクルは、現在及び将来にわたり、お客様のデータ主体からデータを収集したり、そのデータについてデータ主体と連絡を取ることはありません。

GCSのサービス及びシステムは、特定の類の機微なデータを保存又はプロセスするために要求される場合がある特別なセキュリティ管理を提供するようには構築されていません。本セキュリティ・プラクティスに明記されているよりも厳重な保護を必要とする、健康状態、ペイメント・カード、その他いかなる機微なデータを送付しないように注意してください。お客様のデータから機微なデータを削除する方法に関する情報は、My Oracle Supportの

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1227943.1>にて提供されています。

報告違反

- GCSは、お客様のデータが不正に利用されている疑いがあるインシデントに対し、速やかに評価し、それに対応します。Oracle Global Information Security (GIS) は、そのようなインシデントの報告を受け、行為の性質に応じて、インシデントに対処するエスカレーション・パス及び対応チームを明確にします。
- オラクルは、お客様のデータが不正に利用されていると判断した場合（オラクルの従業員による場合を含みます）、お客様に対し当該不正利用を画面により速やかに報告するものとします。
- オラクルの要員は、お客様のデータが不正に利用されている場合の対応にあたり、速やかな報告及びエスカレーション手続きなどの指示を受けます。

開示

オラクルがお客様に対しサービスを実施するために必要な場合を除き、お客様は、お客様のデータをオラクルに開示すべきではありません。オラクルは、お客様の注文又は指示に基づく場合、あるいは法律で定める場合を除き、お客様のデータ（テキスト及び画像を含みます）を開示しません。オラクルは、法律で認められている範囲内で、開示がなされる前に開示の要請をお客様に通知するよう真摯な努力をするものとします。

メディアの返却

お客様は、修復／交換のためハード・ディスク・ドライブ及びソリッド・ステート・ドライブ（合わせて以下「ドライブ」と言います）を返却する前に、ドライブに保存されている全ての情報及びデータを削除することに責任を負います。

返却された全てのドライブは、お客様の地域のオラクルの物流・修理ベンダーを通して処理されます。追加のセキュリティのための予防措置として、使用可能な全てのドライブに対して、当該ベンダーは、U.S. Department of Defense Sanitizing Standard 5220.22-Mに適合するソフトウェアによるデータ消去プロセスを実行するように求められています。当該消去プロセスは、オラクルがそのデバイスに対して新たな処理又は対処を進める前に実行されます。返却されたドライブが使用不能の場合、消去及び処理のために製造メーカーに返却されるか、又は、シリアル・ナンバーを登録し、まとめてドライブを粉砕する電子部品の廃棄ベンダーに送付されます。

お客様は、いかなる場合でも、返却するテープ・ドライブにテープを残すことはできません。テープが取り外しできないドライブの内部に詰まっている場合、取り外しを支援するため、お客様の地域の担当営業にご相談ください。

ネットワーク・セキュリティ

オラクルは、自己の企業ネットワーク上で、ファイアウォール及びルーター・ルール、アクセス制御リスト、並びにセグメンテーションを使用しています。オラクルのGlobal IT部門は、すべてのルーター及びファイアウォールのログを管理及び監視しています。ネットワーク・デバイスは、集中認証により保護されます。オラクルは、不審な活動がないかどうか企業ネットワークの利用状況を監査します。

遠隔地で作業を行う要員は、業界標準のVPN又は同等のテクノロジーを活用して、VPNにより暗号化されたネットワーク・トラフィックを使用します。

物理的セキュリティ

オラクルは、その環境にアクセスされる可能性があるオラクルの施設（以下「サービス場所」といいます）について、以下の物理的セキュリティ基準を維持しています。

- ・ サービス場所への物理的アクセスは、オラクルの従業員、業務委託先及び権限を与えられたビジターに限定されます。
- ・ オラクルの従業員、業務委託先及び権限を与えられたビジターには、IDカードが発行され、施設にいる間は、それを着けなければなりません。
- ・ ビジターは、ビジター名簿に署名し、施設にいるときは同伴され及び／又は監視され、及び／又はオラクルとの間で締結した機密保持契約の条件に拘束される必要があります。
- ・ Oracle Corporate Securityは、鍵／アクセス・カードの所持及びサービス場所へのアクセス権を監視します。オラクルを退職するスタッフは、鍵／カードを返却するものとし、鍵／カードは、退職時に無効となります。
- ・ サービス場所への業務時間外の入場は、Oracle Corporate Securityにより監視及び管理されます。

- Oracle Corporate Securityが、サービス場所での物理的セキュリティ・バリア又は入館管理に対するすべての修復及び変更を許可します。

ORACLE CORPORATE SECURITY PRACTICES

コンピュータ・ウィルス管理

オラクルは、自己の従業員に貸与された全てのコンピュータ上において、オラクルに及びオラクルから送信される電子メールすべてを悪質なコードがないかスキャンし、配信前に既知の悪質なコードに感染した電子メールの添付ファイルを削除する仕組みをオラクルのネットワーク内で維持しています。オラクルは、オラクルの従業員のコンピュータすべてに、ウィルス対策ソフトウェアを搭載するよう求めています。また、オラクルは、ウィルス定義が定期的に更新され、最新の定義が従業員に公開及び伝達されることを確実にする仕組みも維持しています。さらに、これらの仕組みにより、従業員は、自動的に新規の定義をダウンロードし、ウィルス対策ソフトウェアを更新することもできます。Oracle Global Information Securityは、従業員がウィルス対策ソフトウェアをインストールしているか、また、全てのデスクトップ及びラップトップのウィルス定義が更新されていることを確実にするために、随時遵守状況の調査を実施します。

要員

オラクルは、人的エラー、窃盗、詐欺及びオラクルの資産及び、システムの不正使用のリスクを軽減することを非常に重視しています。オラクルが行っている取り組みには、要員のスクリーニング、セキュリティ・ポリシーを要員に周知すること及びセキュリティ・ポリシーを履行するための従業員トレーニングなどが含まれます。例えば、従業員は、パスワードに関するポリシー、「クリア・デスク」ポリシー（机の上に情報漏えいにつながるものを放置しないという方針）及び機密データの取扱いに関するポリシーを明確に理解することを期待されています。

従業員トレーニング

オラクルの従業員は、オンライン・データのプライバシーに対する意識向上トレーニング・コースを修了する必要があります。このコースで、従業員は、データ・プライバシー及び個人データの定義、個人データに関するリスクの認識、データに対する従業員の責任の理解、並びに、プライバシー侵害の疑いがある場合の報告について指導を受けます。また、従業員は、企業倫理についてのトレーニングも修了する必要があります。

オラクルは、従業員がオンライン・データのプライバシーに対する意識向上トレーニング・コースを修了したかどうか判断するために、定期的に遵守状況の調査を実施します。従業員がそのコースを修了していないとオラクルが判断した場合、当該従業員は、即座に通知を受け、できる限り速やかにそのトレーニングを修了するよう指示を受けます。また、懲戒処分の対象となる場合もあります。

オラクルは、セキュリティに関する問題に対する意識を高め、それについて従業員に対し教育を行っています。オラクルは、セキュリティに関する四半期ごとのニュースレター、臨時の通知及びその他資料を作成し、従業員に配布しています。また、オラクルは、既存のトレーニング・コースを更新し、また、適宜新規のコースを開発することがあり、従業員は、それらのコースを修了するよう指示を受けます。

実施

セキュリティの見直し、評価及び監査は、オラクルの情報セキュリティ・ポリシー、手順及びプラクティスの遵守状況を確認するために、定期的に実施されます。情報セキュリティ・ポリシー、手順及びプラクティスを遵守していない従業員は、解雇を含む懲戒処分の対象となる場合があります。