Oracle Global Customer Support Security Practices

発効日：2020 年 3 月 5 日

本Oracle Global Customer Support Security Practices（以下「本セキュリティ・プラクティス」といいます）は、Oracle Corporate Security Practices を補完するものであり、Oracle Global Customer Support（以下「GCS」といいます）が、オラクルのお客様（以下「お客様」といいます）が締結されたオラクルの契約、お客様からのテクニカル・サポートの注文書（以下「注文書」といいます）、及び オラクルのテクニカル・サポート・ポリシー（https://www.oracle.com/corporate/contracts/support-services/policies.html）の条件に基づき、スタンダードなソフトウェアとハードウェアのテクニカル・サポートをお客様に提供する際に従う追加のセキュリティ・プラクティスを明記するものです。また本書で使用される「お客様のデータ」とは、お客様のコンピュータ・システムに格納され、かつ、当該サービスの実施のためにリモート・アクセスされるか又はオラクルに提供されるあらゆるデータを意味します。本セキュリティ・プラクティスにおいて別途定義されていない大文字で始まる用語は、適宜、当該オラクルの契約、お客様の注文書又はポリシーにおいて当該用語に付与された意味を有するものとします。なお Advanced Customer Services に関する条件は全て、当該サービスの注文書に明記されるものとし、本書の対象外となります。

本セキュリティ・プラクティスは、オラクルの裁量により変更される場合があります。ただし、テクニカル・サポート料金が既に支払われた期間中、オラクルによるポリシーの変更が本書に明記されているセキュリティのレベルを実質的に低下させることはありません。変更の詳細は、付属の*「変更履歴」*（PDF）をご参照ください。

1. セキュリティ・ポリシー

オラクルのCorporate Security Practicesは、オラクルの社内業務及びオラクルがお客様に提供するサービスに関するセキュリティ管理を扱っており、オラクルの全ての従業員に適用されます。このポリシーは、一般的に ISO27002 Code of Practice（実践規範）及び ISO27001 規格に適合しており、スタンダードなソフトウェアとハードウェアのテクニカル・サポート・サービスの実施に適用される全てのセキュリティ分野に適用されます。お客様には、お客様のリスクベースのアセスメント及びビジネス要件に従い、ポリシー、基準及び手順に関するお客様自身の包括的なシステムの導入実施を強くお勧めします。

2. GLOBAL CUSTOMER SUPPORT オペレーション

GCS とは、グローバル・コンピテンシー（グローバル対応（能）力）やグローバルレベルでの業務の役割分担・カテゴリ化・処理に基づくサービス・リクエスト（SR）管理による、グローバル・オペレーション（運用）のことです。サービス・リクエスト は、重要性や時間帯、また発生した問題の性質に基づき、「follow-the-sun（太陽の動きに合わせた24時間体制）」モデル（体制）で、世界中のサポート・センターで GCS のエンジニア（オラクルの従業員及び業務委託先を含みます）により処理されます。オラクルは、お客様の注文書の条件及び本セキュリティ・プラクティスに従いオラクルの従業員及び業務再委託先がテクニカル・サポート・サービスの提供（提供の結果として生じるいかなるお客様のデータへのアクセスやその利用を含みます）につき責任を負います。

3. Web ベースのカスタマ・サポート・サイト

オラクルでは、カスタマ・サポート Web サイトを数多く提供しています。各サイトは、それぞれ異なるオラクル・プログラムやオラクル・ハードウェアの製品ラインをサポートするために運営されています。以下には、My Oracle Support サイト（My Oracle Support Mobile サイトを含みます）に適用されるセキュリティ・プラクティスを記載しています。なお、各サポート Web サイトでどのオラクル・プログラムやオラクル・ハードウェアがサポートされているのかについてのさらに詳しい情報は、最新のオラクル・テクニカル・サポート・ポリシー（https://www.oracle.com/jp/support/policies.html）をご参照ください。

4. My Oracle Support

My Oracle Support は、オラクル・プログラム及びオラクル・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）を可能にするオラクルの主要な Web ベースのサービスです。

My Oracle Support では、以下のセキュリティ制御を現在実施しています。

- My Oracle Support は、Secure Socket Layer（SSL）暗号化を使用した 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 には、少なくとも 1名の My Oracle Support Customer User Administrator（以下「ユーザー管理者」といいます）をお客様が指定します。お客様のユーザー管理者は、カスタマー・ユーザーからの新規 My Oracle Support アカウントのリクエストや既存 My Oracle Support アカウントへの CSI の関連づけのリクエストを承認／拒否する責任を負います。お客様は、お客様の My Oracle Support ユーザーのプロビジョニングとプロビジョニング解除をお客様のアクセス・ポリシーに従い適時に行う責任も負います。
- お客様のユーザー管理者は、お客様のユーザーが My Oracle Support 上でどの機能にアクセスできるのかを制御することができます（例：特定のユーザーに対して、サービス・リクエスト への書き込みアクセス権限の有効化や無効化が可能）。
- お客様のユーザー管理者は、自らの CSI に関連するユーザーを閲覧することができ、またユーザーのアクセス権限を削除又は追加することができます。
- My Oracle Support SR 添付ファイル（My Oracle Support SR 作成／アップデート・プロセスの一環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通信は、Hypertext Transfer Protocol over Secure Socket Layer（https）を使用して確保されます。
- 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）ネットワークに配置されています。この 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・サーバー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、発信元や送信先のロケーションを隠すため、SSL アクセラレータ／リバース・プロキシを使用した環境で、バーチャル・サーバーに登録されたIPアドレスの解決を行います。SSL 暗号化（通信）の終端点で、リバース・プロキシはアプリケーション・サーバーにトラフィックを送ります。
- お客様が My Oracle Support とのやり取りを行う間、お客様やお客様のサービス・リクエストに対応している GCS エンジニアは、インタラクティブなオンライン・チャットをリクエストすることができます。お客様がチャットの招待を承諾する（承諾は必須でも前提でもありません）又はチャットを開始する場合、お客様がオラクルに提出した該当するSR 添付ファイルとともに、お客様と当該 GCS エンジニアとのチャット記録が保存されます。なお当該チャット記録は、当該サービス・リクエストがオープンの間は、チャット参加者がいつでも閲覧できるようになっています。また、GCS エンジニアがお客様とのチャット・セッションを要約する場合もあります。エンジニアが要約する場合、それらの要約は当該サービス・リクエスト・アクティビティの一部と

なり、お客様は、そのサービス・リクエストのそれ以外の部分と同様にそれらの要約をレビューすることができます。

- 自らのプロファイルに特定の CSI を追加することをユーザー管理者により承認された、お客様の正規ユーザーのみが、その CSI に関連するサービス・リクエストを My Oracle Support 上で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使用することができますが、カスタマに関するコンテキストのほか、お客様又はお客様のコンテンツに関連する参考情報は全て、Knowledge Management の項目から削除されます。
- My Oracle Support には、サービス・リクエストの作成をお客様に要求しないセルフサービス型ツール Guided Resolution があります。Guided Resolution ツールを使用して分析用にお客様がアップロードしたファイルは、アップロードされてから 7日後に削除されます。
- 登録前にお客様が保存するサービス・リクエストのドラフト版は、（そのサービス・リクエストが）登録されると30日後に削除され、また（そのサービス・リクエストが）未登録の場合は90日後に削除されます。
- My Oracle Support SR 添付ファイルが、そのサービス・リクエストに対処するために、必要に応じて保持され、そのサービス・リクエストのクローズから 7日後に削除されます。ただし、当該サービス・リクエストの考えられる根本的原因としてバグが確認されている場合には、当該 SR 添付ファイルは、Oracle Development のバグに関するデータベースに保存され、そのバグがオープン状態の間は保持されます。またこのバグが重複バグではない場合、このバグにコード修正が不要な場合、あるいはコード修正ではこのバグを解決できない場合は、当該 SR 添付ファイルは、そのバグがクローズされてから 7日後にバグに関するデータベースから削除されます。なお、バグの解決にコード修正を必要とする場合には、当該 SR 添付ファイルは、(i) 診断を支援したり、他の関連コードで確認された問題との一致を確認したりするために、そのバグがクローズされてから、又は(ii) オラクルのCritical Patch Update (CPU) プロセスの一環としての、セキュリティの脆弱性に関連するバグの修正の発表から、最長 6か月間保持され、その後削除されます。当該 SR 添付ファイルに含まれるデータの一部又は全てが製品のコード修正の確認を行う際のテスト・ケースとして使用される場合は、後継バージョンで当該バグが再び取り込まれることがないよう、当該製品がサポートされている間、回帰テストを実施する目的で、そのデータがオラクルのソース・コード・リポジトリに格納される場合があります。
- サービス・リクエストに関連する My Oracle Support SR データ及び記録は、記録が作成された日から10年間保存されます。

5. テクニカル・サポート提供に使用されるテクノロジー

GCS では、オラクル・ソフトウェア及びオラクル・ハードウェアのサポートの双方で、サービス・リクエストの診断及び解決の一環として、数多くの手法やツールを使用します。これらの手法及びツールに関連するセキュリティ・インフラストラクチャについては、後述に記載しています。

Collaboration Tools

GCS では、オラクルに報告された問題をレビューするため、次の 2つのコラボレーション・ツールを使用します：プログラムに対してはCisco Webex、ハードウェアに対してはOracle Shared Shell と Cisco Webex。これらのツールには、以下の共通する特徴があります。

- お客様は、全てのセッションを管理し、且つそれらに積極的に参加します。
- お客様は、どのようなナビゲーションが行われるのか、どのようなデータが表示されるのか、またどのようなコマンドが発行されるのかについて、セッションを管理します。
- 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。

追加詳細：

- **Cisco Webex Conferencing** を使用して、GCS は、サービス・リクエストの診断と解決についてお客様を積極的に支援するために、Web 会議を設定することができます。
  - オラクルは、以降に行われる診断や解決のために、当該セッションを記録し、その記録内容をSR 添付ファイルとして当該サービス・リクエストに添付する場合があります。お客様は、GCS に記録をやめるよう、いつでも自由に指示することができます。
  - インターネット上で送信されるデータに対して、Secure Socket Layer（SSL）による暗号化が行われます。
  - Cisco Webex Conferencing は、Transport Layer Security（TLS）プロトコル v1.2 を必要とします。

- **Shared Shell** を使用して、GCSは、お客様がサポート契約締結中のハードウェアの端末／コマンド・インタフェースを遠隔的に閲覧したり又はアクセスしたりすることができます。
  - お客様は会議参加者のアクセス制御を行うことができます。お客様はセッションに参加者を招待するほか、参加者の承認や拒否を行う責任を負います。またお客様は任意の参加者（のアクセス）をいつでも終了することができます。
  - 会議参加者に設定されるデフォルトのアクセス制御は「view only」であり、参加者は端末／コマンド・ライン・ウィンドウに表示される内容のみを閲覧することができます。お客様は、アクセス制限に「no execute」を選択することもでき、この場合、参加者はコマンドをタイプすることはできますが、その実行ができるのはお客様のみです。あるいは「full access」を選択することで、お客様は、参加者がコマンドをタイプして実行できるようにすることもできます。
  - 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通信は、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、デバッグ、診断、また問題の解決のため、最長90日まで Shared Shell セッション・ログを保持します。当該ログ・ファイルは、承認プロセスを経てプロビジョニングされるアクセス制限のあるオラクルのシステムに格納されます。なおこれらのファイルは、お客様が Shared Shell セッションを起動したイニシエータ・システム上でも、お客様は閲覧可能ですが、お客様がセッションに招待している参加者のシステム上では閲覧できません。

- Shared Shell では、Transport Layer Security プロトコル v1.2 を実施します。

プログラム及びハードウェアに対して使用されるツール

GCS では、問題の解決を支援する目的でデータを収集するように設計された各種ツールを提供します。これらのツールには、以下の共通する特徴があります。

- これらのツールは、ツールが実行されているシステム又はデバイスから本番データを入手したり、収集したり、伝送したり、使用したりするようには設計されていません。当該ツールは、システムのテレメトリ・データ（遠隔測定データ）（例：ハードウェア及びソフトウェアのコンポーネント、バージョン、適用されるパッチ）を特に対象としています。
- お客様の積極的な関与なくオラクルに直接当該システムのテレメトリ・データが送信される際、さまざまな暗号化テクノロジーの １つを使用して送信が行われます。

ソフトウェア及びハードウェアのテクニカル・サポートに対して GCS が使用する一部の主なツールについては、さらに詳しく、以下に記載しています。なお、サポート・ツールに関する追加情報のほか、以下に記載の各ツールにより収集されるメトリックに関する詳細は、My Oracle Support で閲覧可能です。

プログラムに対するツール　—

Oracle Configuration Manager（OCM）

Oracle Configuration Manager（OCM）は、My Oracle Support から入手可能であり、お使いの環境のコンフィギュレーション情報を収集し分析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。なお、ここで自動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、お客様が同意した場合に限り行われます。OCM のインストールとコンフィギュレーションは、お客様が管理します。情報をオラクルに送信するよう、お客様が OCM を構成した場合、OCM は、プッシュを実行して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 に定期的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開始し、インバウンド通信のリッスン（待機）は行いません。

- 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、OCM が提供する特定の 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お客様が実行できるスクリプトは、OCM が提供します。これらのスクリプトは、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。当該アカウントは、コンフィギュレーション情報を収集する PL／SQL プロシージャを格納し、その収集情報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。当該アカウントが設定されると、ログイン権限が不要となる又は要求されなくなるため、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 の自動アップデート機能を有効にすることができます。OCM の自動アップデートには、認証及び暗号化が使用されます。ダウンロード済みのアップデートが適用される前に、デジタル署名が検証され、オラクルに発行された証明書（この証明書は、通信リンクを確保するために使用される証明書とは異なります）でそのアップデートが署名済みであることが確認されます。なお、デジタル署名ソフトウェアは、オラクルの企業ネットワークに接続されてい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 では、全ての通信に対して、Secure Socket Layer（SSL）及び業界標準のプロトコル（HTTPS）、並びにパブリック・キー／プライベート・キーの交換を用いた 128-bit 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、オラクルから返された証明書（オラクルが指定した公認認証機関が、オラクルにこの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 ネットワークに配置されています。アプリケーション・サーバー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、発信元や送信先のロケーションを隠すため、SSL アクセラレータ／リバース・プロキシを使用した環境で、バーチャル・サーバーに登録された IP アドレスの解決を行います。SSL 暗号化（通信）の終端点で、リバース・プロキシはアプリケーション・サーバーにトラフィックを送ります。すると、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）にプッシュされ、そのコンフィギュレーション情報を含むファイルはその後削除されます。
- 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、既知のぜい弱性を検出するため、四半期ごとに、OCM アップロード・サーバーのぜい弱性スキャンを行います。
- 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 Austin Data Center 内に確保され、オラクルのネットワーク・セキュリティ・インフラストラクチャ及びセキュリティ制御により保護されます。
- お客様は、お客様のコンフィギュレーション情報の削除を、その具体的なコンフィギュレーション情報と削除依頼の範囲を示したサービス・リクエストをログ記録することで依頼することができます。
- Platinum Services に関しては、OCM は、後述の Oracle Advanced Support Gateway（以下「ゲートウェイ」といいます）上にインストールされます。通信は、そのゲートウェイからオラクルまで確立された、暗号化済みの VPN を経由して行われます。

どのような情報が OCM により収集されるのか、そしてそれがどのように利用され且つ保護されるのか、について、さらに詳しくは、My Oracle Support で閲覧可能な OCM ライセンス条件並びにその他関連ドキュメントをご参照ください。

Remote Diagnostic Agent（RDA）

Remote Diagnostic Agent（RDA）は、サービス・リクエストの診断と解決を支援するさらに詳しい情報を提供します。GCS での SR 診断・解決プロセスへのインプットとして、またそのプロセスのコンテキストとして、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、RDA スクリプトが GCS によりお客様に提供されます。

RDA 情報は、お客様側で格納されます。ただし、お客様は、My Oracle Support での SR ログ記録・アップデート・プロセスを通じて、RDA 情報を添付ファイルとしてアップロードするよう選択することができます。なお、オラクルへの RDA のアップロードはいずれも、安全な GCS リポジトリに格納されます。

RDA 情報（Hardware and Systems 用 Explorer ファイルを含みます）は、プロアクティブ（事前予防的）なテクニカル・サポート・サービスに有用なもので、つまり、これらのファイルは、リアクティブ（事後対応的）な SR 診断・解決プロセスとは別に、お客様により提供されるものです。RDA ファイルや Explorer ファイルのプロアクティブ（事前予防的）な活用は、潜在的リスクのある領域を特定したり、お客様が採用を考える可能性のあるオラクル推奨のプラクティスを特定したりするのに用いられます。なお、ライセンス及びサービスのコンプライアンスのため、またオラクルが製品やサービスの提供を向上させるため、お客様のオラクル製品のポートフォリオ管理をオラクルが支援するうえで、当該ツール・データがオラクルに使用される場合があります。

- プロアクティブ（事前予防的）なRDA の収集情報や Explorer ファイルは、反復的な障害解析を行うため、最長 6年まで保持されます。
- オラクルでは、My Oracle Support 上で、Proactive Hardware Services による Proactive Analysis Center への安全なアクセスをお客様に提供します。ここでは、プロアクティブ（事前予防的）な収集情報に基づく My Oracle Support 推奨事項をご参照いただけます。
- オラクルは、プロアクティブ（事前予防的）なサポート向けにアップロードされた最初と最後の 5つの Explorer ファイルを保持します。
- カスタマは、My Oracle Support 上で、Contact Us オプションを使用してサービス・リクエストを Support に登録することで、自らが所有するプロアクティブ（事前予防的）なファイルを消去してもらうようリクエストすることができます。

Database Diagnostic Data

オラクル・データベース（Release 11g 以上）の診断インシデント及びパッケージ情報は、システムの運用中にそのシステムがエラーを検知すると、当該データベースにより自動生成されます。診断データは、エラー、トレース、コンフィギュレーション、また当該データベースからの問題に関連する他の情報を提供するように設計されています。この情報は、GCS が関与することなく、お客様が自らの問題を特定し、診断し、解決するのに役立ちます。

- 診断データは、お客様側で格納されます。ただし、お客様は、My Oracle Support 上での SR ログ記録・アップデート・プロセスを通じて、診断データを添付ファイルとしてアップロードするよう選択することができます。またお客様は、OCM を使用してどの診断データもオラクルに転送することができます。なお、オラクルへの診断データのアップロードはいずれも、上述の通り、専用の GCS リポジトリで確保されます。

ハードウェアに対するツール　―

システムに対する Auto Service Request

システムに対する Auto Service Request（以下「ASR」といいます）は、お客様がサポート契約締結中のオラクル・ハードウェア上にある障害を検出するために、障害イベントのテレメトリを使用することで、そのハードウェアのテクニカル・サポート・プロセスの自動化を促進するほか、分析やサービス・リクエストの作成向けに、オラクルにその（テレメトリ）データを転送します。なお、お客様のシステムから入手された後、オラクルに転送され格納される 当該 ASR 情報は、診断と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カスタマ情報に限られま

す。これには、障害イベント・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（ホスト名、シリアル・ナンバー、サービス・リクエストのデータ等）が含まれます。

- お客様のシステム上で ASR manager の初期化を行うにあたり、お客様はそのシステムを登録し、プライベート暗号化キー／パブリック暗号化キーの交換を行います。オラクル側のコア ASR インフラストラクチャでメッセージ認証を行うため、特定の ASR manager の以降のメッセージ全て（リクエストと応答の両方）の署名には、1024-bit の RSA キーが使用されます。
- お客様の ASR ハードウェア・アセットを有効化する間、ASR manager は、それらアセットのシリアル・ナンバーや製品情報を検索するために、当該アセット上で実行中のあらゆるサービス・タグを見つけ出します。当該 ASR アセットから、ASR manager がテレメトリ・メッセージを受信し、必要な場合にはアラームを有効にする及び抑制する操作を行います。そのテレメトリ・メッセージが、処理のため、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、そのメッセージは、RSA with RC4 （128-bit）SSL 暗号化を使用して、XML データ・ストラクチャにコード化され HTTPS （port 443）を経由して送信されます。
- オラクルのコア ASR インフラストラクチャは、ユーザー認証にはユーザー・アカウントの証明書を、そしてカスタマ・システムの認証にはデジタル署名され且つ暗号化されたトラフィックを活用します。当該 ASR システムにより格納されるデータは全て、マルチ・テナンシーのセキュリティ・モデル構築により隔離され、またこのセキュリティは、多層構造の API ベースのアクセス制御及び権限制御により実施されます。コア ASR インフラストラクチャに格納されている当該データに、直接外部からアクセスすることはできません。

なお Oracle Platinum Services のお客様並びに Oracle Business Critical Service for Systems のお客様には、後の項目「Advanced Support Gateway Services」に詳述の通り、オラクルが Oracle Advanced Support Gateway（以下「ゲートウェイ」といいます）上に ASR のインストールを行います。ASR アラートは、当該ゲートウェイ接続を経由してオラクルにライトバック（書き戻し）されます。また Platinum Services では、http://www.oracle.com/us/support/library/platinum-fault-monitoring-1958297.pdf に詳述されている特定の OEM の障害イベントに対して、自動生成のサービス・リクエストを作成することが可能です。

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

ASR Service Delivery Platform（SDP）は、お客様がサポート契約締結中のオラクルのストレージ・デバイスに接続し（そのデバイスの）監視を行う、お客様のサイトにインストールされている、オラクルが構成と管理を行うサーバーです。当該 SDP はオラクル側でコア ASR インフラストラクチャを使用するので、上述の「システムに対する ASR」における ASR 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 においても同じです。またオラクルでは、 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：

- お客様とオラクルとの間の全ての SDP トラフィックは、オラクルが提供する Virtual Private Network （VPN）ルーター又はカスタマ VPN 対応デバイスから、オラクルの VPN ターミネーション・ルーターへと、開始されます。
- VPN を経由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、割り当てられた SDP グループの権限の一部である様々なロール（役割）を割り当てられます。エンジニ

アの認証情報はシークレット・キーを使用して暗号化されます。 SDP は認証目的に HTTP プロトコルを使用しますが、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 認証を使用して暗号化されます。

- お客様のストレージ・デバイスに格納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。
- 当該 SDP サーバーのインストールには、デプロイ前にお客様にネットワークの変更を求める場合があるため、お客様の正式なレビューと承認を必要とします。VPN トンネルの暗号化タイプやハッシュ・アルゴリズムは、この正式レビュー時にレビューされ同意されます。
- 当該 SDP のセキュリティ・メカニズムは、リモート管理ツールのための CERT／Coordination Center ガイドラインに従います。

6. Advanced Support Gateway Services

上述の項目「テクニカル・サポート提供に使用されるテクノロジーのセキュリティ」の手法やツールに加えて、GCS では、Platinum Services や Business Critical Service for Systems を含む、Advanced Support Gateway を使用して提供される全てのサービス向けに特別に設計された手法やツールも使用します。これらの手法及びツールに関連するセキュリティ・インフラストラクチャについては、後述に記載しています。Platinum Services についての情報は、
http://www.oracle.com/jp/support/library/platinum-services-policies-1664597-ja.pdf
で閲覧可能です。また Business Critical Service for Systems に関する情報は、
http://www.oracle.com/us/corporate/contracts/bus-critical-service-for-systems-1927926.pdf. で閲覧可能です。

Oracle Advanced Support Gateway

当該ゲートウェイは、My Oracle Support 上で利用可能な Oracle Advanced Support Gateway と物理的又は仮想的なハードウェア・プラットフォームから構成されるコンピューティング・プラットフォームで、オラクルの障害監視ツール（例：Auto Service Request、Oracle Configuration Manager、Oracle Enterprise Manager）をホストします。このゲートウェイは、障害イベントのテレメトリを収集してオラクルに転送し、お客様がお使いの環境に、オラクルがリモート・アクセスできるようにします。

- 当該ゲートウェイは、お客様側のロケーションにあるお客様の DMZ 内又は信頼性の高いネットワーク内にインストールされます。お客様は、このゲートウェイとの通信を可能にするために、お客様の信頼性の高いネットワークとファイウォールに適切な変更を行う必要があります。
- 当該ゲートウェイは、以下に記載の通り、Oracle Continuous Connection Network（以下「OCCN」といいます）という、オラクルのプライベートで暗号化された安全なネットワーク接続を使用してオラクルに接続します。全てのメッセージは、2048-bit RSA キーを使用して署名され暗号化されます。

Oracle Continuous Connection Network

OCCN は、当該ゲートウェイからオラクルに障害イベントのテレメトリを送信するために使用され、且つお使いの環境へのリモート・アクセスを容易にする、プライベートで暗号化された安全なオラクル・ネットワークです。

- OCCN は、オラクルのイントラネット（社内ネットワーク）から分離した専用のプライベート・ネットワークです。
- OCCN は、以下に記載の通り、GCS のワークステーションを Oracle Advanced Support Platform に接続し、またインターネット上で Oracle Advanced Support Platform を当該ゲートウェイと接続します。
- OCCN へのアクセスは、2ファクター認証（2因子認証）で管理され、権限を有する GCS の従業員のみアクセス可能です。
- オラクルでは、Oracle Advanced Support Platform と当該ゲートウェイとの間の接続のために 2つのオプションを用意しています。どちらも接続にインターネットを使用します。お客様はいずれかのオプションを選択することができます。
    - Internet Protocol Security（IPSec）に基づくネットワーク間 VPN が、お客様とオラクルとの間で確立されます。この接続は、IPSec のセキュリティ・フレームワークを使用して確保され暗号化されます。なお、この接続を終端するには、お客様は、オラクルが提供する VPN 又はお客様側の VPN のいずれかを選択することができます。
    - Logical-Tunnel を構築し確保する AES256-SHA1 の暗号化アルゴリズムを使用した Software SSL VPN。

Oracle Advanced Support Platform

Oracle Advanced Support Platform を使用して、お客様は、当該ゲートウェイを通じてサービスを受けるお客様のコンフィギュレーションに対するサービス・リクエストのステータスと同様に、ニア・リアルタイムのステータスや提供の有無を閲覧することができます。GCS では、当該ゲートウェイを通じてサービスを受けるお客様のコンフィギュレーションを遠隔的に監視するために Oracle Advanced Support Platform を使用します。

- Oracle Advanced Support Platform は隔離されたオラクルのネットワーク内でホストされます。
- Oracle Advanced Support Platform は一元管理され、選任された GCS の従業員にのみアクセスを許可する詳細な権限スキームを使用します。
- Oracle Advanced Support Platform は My Oracle Support に統合されており、上述の「Web ベースのカスタマ・サポート・サイト」に記載のセキュリティ機能を採用します。初期セットアップ時、オラクルは、Oracle Advanced Support Platform にお客様のアカウントがアクセスできるようにします。また、お客様の代わりにお客様のアカウントを管理する Oracle Services Coordinator が 1名指定されます。
- Oracle Advanced Support Platform は、権限の確認、ログ・エントリーの作成及び必要なパスワードの格納を行うことで、当該ゲートウェイへのアクセスを、お使いの環境内で制御します。

Oracle Analyst Access and Logging

全ての Advanced Support Gateway Services においては、お客様のシステムへのオラクルのリモート・アクセスは、OCCN と当該ゲートウェイを通じて管理されます。権限を有する GCS の従業員は、このゲートウェイにアクセスする前に、まず OCCN にアクセスする必要があります。リアルタイム・モニタリングを可能にするために、Enterprise Management のエージェントがカスタマ・ホスト上にインストールされます。当該エージェントは、個別のユーザー ID にインストールされ、またオラクル・プログラムを監視する権限を有している必要があります。

当該 OCCN ゲートウェイやお使いの環境へのオラクルのアクセスは、ユーザー名、タイムスタンプ及びホスト名でログ記録されます。これらのログは、暗号化されたデータベースに格納され、1年間保存されます。

7. データ管理及び保護

GCS プラクティスは、上記で参照されたオラクルの Corporate Security Practices 及び情報保護に関するポリシーに準拠しており、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レベルの高い 2クラスの情報に分類します。また当該ポリシーにより、お客様のデータの格納や配布について、制限が課されます。

データ管理

GCS は、お客様のデータの作成もアップデートも行いません。テクニカル・サポート・サービスの提供に伴い、お客様がオラクルに対してお客様の個人情報にアクセスできるようにした場合には、GCS は以下に従います。

- https://www.oracle.com/legal/privacy/services-privacy-policy.html で閲覧可能なオラクルの Services Privacy Policy
- https://www.oracle.com/dataprocessingagreement で閲覧可能なオラクル・サービスのデータ処理契約の適用されるバージョン

お客様は、お使いのコンピュータ環境に存在する自らのデータ（あらゆる個人情報を含みます）の管理維持を行い、またそのデータについて責任を負います。お客様は、お客様による自らのデータの収集に係る一切（収集の範囲や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。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することも、それらデータについてデータ主体と連絡を取ることもありません。

なお GCS のサービス及びシステムは、特定の機微なデータを格納したり、処理したりするのに必要となりうる特別なセキュリティ制御に対処するようには設計されていません。本セキュリティ・プラクティスに明記されるものよりも厳重な保護を必要とする、医療記録、ペイメント・カード、又はその他機微なデータを登録しないようご注意ください。お客様の登録内容から機微なデータを削除する方法についての情報は、My Oracle Support の https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1227943.1 で閲覧可能です。

以上の制限事項にかかわらず、お客様が、テクニカル・サポート・サービスを受ける一環として、該当欧州データ保護法（オラクル・サービスのデータ処理契約で定義されています）の適用対象である個人情報又は United States Health

Insurance Portability and Accountability Act（以下「HIPAA」といいます）（米国における医療保険の相互運用性と説明責任に関する法令）の適用対象である Protected Health Information（以下「PHI」といいます）（保護対象の医療情報）をオラクルに提出することを希望される場合、お客様は、以下を行わなければなりません。

- PHIの場合、お客様のテクニカル・サポート・サービスを具体的に参照し網羅する HIPAA 事業提携者契約（Business Associate Agreement：BAA）をオラクルと締結する。
- 該当欧州データ保護法の適用対象である個人情報や PHI を、My Oracle Support カスタマ・ポータル上において、サービス・リクエストの添付ファイルでのみ提出する。
- 当該サービス・リクエストの本文には、（オラクルがそのサービス・リクエストに対応するうえで必要となる連絡先情報以外）該当欧州データ保護法の適用対象である個人情報も PHI も含まないようにする。
- My Oracle Support で入力を促されたら、当該サービス・リクエストの添付ファイルに該当欧州データ保護法の適用対象である個人情報（My Oracle Support で EEA Personal Data として指定されている場合もあります）又は PHI が含まれる可能性があることを明示する。

8. メディアの返却

お客様は、修復／交換のためにハード・ディスク・ドライブや半導体ドライブ（以下、総称して「ドライブ」といいます）を返却する場合、事前に、それらのドライブにお客様が格納した全ての情報とデータを削除する責任を負います。

返却されたドライブは全て、お客様の地域にあるオラクルの物流・修理ベンダーにより処理されます。当該ベンダーは、使用可能な全てのドライブに対して、National Institute of Standards and Technology NIST SP800-88 の規格を満たすように設計された、ソフトウェアによるデータ消去プロセスを実行する必要があります。この消去プロセスは、オラクルが当該デバイスに何らかの追加の処理や取扱い作業を進めるにあたり、事前に行われます。返却されたドライブが使用不能の場合、そのドライブは、消去及び処理のために Original Equipment Manufacturer（OEM）に返却されるか、又はシリアル・ナンバーによりバッチ（一括処理）でログ記録され、消磁され、不活性化された後、ドライブを破壊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。テープがドライブの内部に詰まり取り外しができない場合は、その取り外しの支援をお客様のグローバル・フィールドの担当者にご相談ください。

9. Oracle Enterprise Tape Analysis and Data Recovery

Oracle Enterprise Tape Analysis and Data Recovery は、Oracle Premier Support for Systems に対する有効なサポート契約を有するお客様にご利用いただけます。Enterprise Tape についてデータ・リカバリーやデータ分析を必要とする問題がお客様に発生すると、オラクルのテープ・データ・リカバリー・ラボが以下のセキュリティ対策を実施します。

- お客様は、対象のテープ上のデータの機密性又はデータの完全性を脅かすことがないよう、安心且つ安全な方法で、オラクルのデータ・リカバリー・ラボにそのテープを送付する責任を負います。テープがドライブの内部に詰まり取り外しができない場合は、その取り外しの支援をお客様のグローバル・フィールドの担当者にご相談ください。取り外された後、お客様はオラクルに当該テープを送付することができます。
- オラクルが当該テープを受領すると、処理の準備ができるまで、そのテープは「In Process」のロックされたキャビネットに保管されます。データ・リカバリー・プロセスを開始するのに必要となる情報をお客様が提供済みであることを確認したうえで、データ・リカバリー・エンジニアは当該テープを書込み不可（ライトプロテクト）にし、カスタマ名、VOLSER（バーコードのテープ ID）及びケース番号が特定できるラベルを作成して貼付し、そしてソフトウェア制御のカスタム設計 RFID テープ・ロッカー・システムであるテープ・ログイン・システムにそれらの情報を入力します。当該テープは、分析／データ・リカバリー・プロセスを通して、データ・リカバリー・ラボ内のロックされたキャビネットに保管されます。メディアは、お客様により別の引き出しに保管されます。
- 当該ラボにアクセスできるのは、Oracle Tape Technology Service Center 組織と Tape Product Sustaining Engineering 組織の限られた人数のオラクルの従業員に限定されます。該当する従業員にはアクセス用バッジが個別に用意され、アクセスはログ記録され、アクセス権限は定期的にレビューされます。またデータ・リカバリー・ラボのツールやファームウェアは全て、そのデータ・リカバリー・ラボ内で処理されます。Tape Product Engineering が追加分析を行う必要がある場合は、（その組織の）テープ製品エンジニアが当該データ・リカバリー・ラボでその作業を行います。
- 分析／リカバリーの完了後、オラクルは、Oracle Key Manager Appliance を使用して対象のデータを暗号化します。オリジナル・テープとリカバリー・テープは、通常翌日配達便で出荷され、また国際貨物の場合は、オラクルから出荷されるにあたり、標準的な米国オラクルの輸出に係るコンプライアンス手続きに従う必要があります。当該荷物が出荷されると、追跡番号をはじめ、その他関連する追跡情報がサービス・リクエストの注記に記載されます。なおお客様は、当該ラボから直接当該テープを受け取る手配をすることもできますが、受け取った時点で、お客様が、（そのテープ上の）データの機密性及び完全性に対して、単独で責任を負います。