ORACLE

Oracle Databaseとインド準備銀行のセキュリティ・ガイドライン

Oracle DatabaseでRBI要件を満たすための実践的なアプローチ

2020年6月 | バージョン20.01
Copyright © 2020, Oracle and/or its affiliates

目的

このテクニカル・ホワイト・ペーパーでは、Oracle Databaseの保護の概要について説明します。機能、オプション、無償で提供される製品についても説明します。本書は、セキュリティ・リスクを低減し、お使いのOracle Databaseの規制遵守を向上するための選択肢を評価できるよう支援することを目的としています。

対象読者

本書は、Oracle Databaseのセキュリティ制御を設計、実装、保守、または操作する責任を担うユーザーを対象としています。

免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この機密文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本文書は、ライセンス契約の一部ではありません。また、オラクル、オラクルの子会社または関連会社との契約に組み込むことはできません。

本書の目的は、企業がOracle Database Securityテクノロジーを活用してインド準備銀行の特定要件に準拠できるようにする方法の理解を助けることです。Oracle Database Securityテクノロジーの中には企業の具体的な環境によっては、関連するものもあれば関連しない場合もあります。オラクルは、必ずユーザーの具体的な環境でセキュリティ・ソリューションを検証することで、確実に性能、可用性、整合性を維持することを推奨しています。

本書の情報は、いかなる法律、規制、規制ガイドラインの内容、解釈、適用に関する法的なアドバイスとして解釈したり、使用することはできません。顧客（将来の顧客を含む）は、自身で法的助言を求め、個人データの取り扱い（いかなるベンダーの製品やサービスの利用も含めて）に関して適用される可能性のあるあらゆる法律や規制を理解する必要があります。

エグゼクティブ・サマリー

RBIのガイダンスはその幅広さに圧倒されるかもしれませんが、データベース・セキュリティの観点から見ると、そのガイダンスは次のようないくつかのコアとなる原則に要約できます。

1. パッチ・レベルや構成などを含め、データベースについて理解します。どのデータベースに機密データが含まれているかを把握します。
2. 保存中および移動中の機密データを暗号化します。
3. 機密データへのアクセスを制御し、付与する特権は最小限にして、個人の職務遂行に必要なもののみにアクセスを制限します。
4. データへのアクセスを監視し、監査証跡を保護して、改ざんや破壊を防止します。

Oracle Databaseのセキュリティ機能を使用することは、RBIガイダンスに準拠する助けとなります。

Copyright © 2020, Oracle and/or its affiliates

目次

Copyright © 2020, Oracle and/or its affiliates

背景

インド準備銀行（RBI）は、インドの銀行と非銀行系金融会社を監督および管理しています。これには、国民のプライバシーを保護し、詐欺の機会を最小限に抑え、金融取引の公正性を向上させるデータ・セキュリティ慣行を奨励する務めが含まれます。RBIは2011年に、情報セキュリティ、電子バンキング、テクノロジー・リスク管理、サイバー詐欺を扱うワーキング・グループの報告書と推奨事項、およびそれに続く*Guidelines on Information security, Electronic banking, Technology risk management and cyber frauds*（参考資料1）を整えることによって、安全なバンキング・システムへの道を開きました。これにより金融サービス機関は、情報資産のライフサイクルにおけるすべての段階で、情報セキュリティを考慮した経営陣承認の情報セキュリティ・ポリシーを制定することが求められるようになりました。ワーキング・グループの推奨事項のガイドラインには、データへのアクセスの制御と監査に関する要件も含まれていました。これらのガイドラインにより、データを保護するためのRBI推奨事項の詳細レベルが向上しました。

2016年に、RBIは*Cyber Security Framework in Banks*をリリースしました（参考資料2）。2016年のガイドラインでは、銀行に対し、財務データの機密保護、整合性、可用性を維持するために適切な措置を講じることを義務付けており、緊急であることを強調しています。銀行によるガイドラインの遵守を支援するために、ベースライン管理のリストが付録1に含まれています。これらのガイドラインは、2011年の元のワーキング・グループのガイドラインを補強するものであり、それら2つの年のガイドラインを組み合わせることによって、財務データの保護に関する現在のRBIポリシーの基礎が形成されています。RBIガイダンスは、Urban Cooperative Banks (UCB) in 2018（参考資料3）にも拡張され、2011年と2016年のガイドラインにおける以前のガイダンスと非常によく似た管理フレームワークを持っています。UCBガイダンスは2019年に、UCBを異なる報告要件を持つ4つの異なるカテゴリに分類するRBI（参考資料4）によって更新されました。

RBIの包括的なガイダンスを理解するには、4つの文書すべてが重要ですが、もっとも具体的な技術ガイダンスは参考資料1および2にあります。

Oracle Databaseは、グローバルな金融サービス業界全体で、あらゆる大手金融機関によって使用されています。データベースが作成されたとき以来、セキュリティはデータベースのコア機能であり続けており、Oracle Databaseは時間の経過とともに、事実上あらゆるコンプライアンス目標を達成できる包括的な一連のセキュリティ機能を進化させてきました。RBIガイドラインも例外ではありません。ここでは、データベース関連のガイドラインの一部と、要件を満たすのに役立つ、対応するデータベース・セキュリティ機能を紹介します。

RBIガイドラインのDatabaseコントロールへのマッピング

Oracle Databaseには、何百もの機能、オプション、サポート製品があります。以下に示すのは、Oracle Databaseに関連するRBIガイドラインと、ガイドラインを満たすのに役立つ推奨データベース機能です。「出典」列には、関連する文書、付録、および段落番号が記載されています。参考資料へのリンクを含むキーは、このセクションの最後にあります。

本書は、RBIガイドラインと対応するデータベース機能の概要です。多くの場合、要件は複数の異なる参考資料に記載されています。参考資料として記載されているすべてのガイドラインは現在も有効であるため、それぞれの出典を記載しています。Oracle Databaseは金融機関で非常に幅広く使用されているため、オラクルでは、以下に概説されているアクティビティ監視要件についてもさらに詳細な情報を提供しています。それとともに、ガイドラインの要件を満たすための推奨されるコントロールの構成に関する具体的な推奨事項を示しています。その詳細な資料は、リクエストすることで入手できます。

「出典」列に記載されている4つの参考資料のキー:

1. Guidelines on Information security, Electronic banking, Technology risk management and cyber frauds
2. Cyber Security Framework in Banks
3. Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs)
4. Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach

注：記載されているページ番号は、実際の文書に示されているページ番号ではなく、*PDF*のページ番号に基づいています。

Copyright © 2020, Oracle and/or its affiliates

RBIガイドライン	出典	Oracle Databaseコントロール
すべてのユーザーによるIT資産へのアクセスのロギングと監視を監査します。	参考資料1、20ページ、項目（vi）（h）	Oracle Databaseには、システムへのすべてのユーザー・アクセスを監査する機能があります。 Oracle Audit Vault and Database Firewallは、分析、レポート作成、アラート生成のために、データベース監査情報を安全なリポジトリで一元管理します。
情報資産所有者によるユーザー・アクセスの定期的なレビューにより、適切なアクセスが維持されていることを確認します。	参考資料1、20ページ、項目（vi）（i）	Oracle Audit Vault and Database Firewallは、Oracle Databaseのユーザー・アカウントとエンタイトルメント情報を取得し、データ所有者が確認して証明できるレポートを生成します。
4つの目の原則を非常に重要な、または非常に機密性の高いIT資産に適用します。	参考資料1、20ページ、項目（vi）（j）	Oracle Database Vaultコマンド・ルールは、機密性の高いデータベース・コマンドに対して4つの目要件を適用するために使用できます。
特権ユーザーによるリモート・アクセスに対する強力な制御を策定します。	参考資料1、20ページ、項目（xiii）（b）	Oracle Database Vaultは、銀行ポリシーに従ってリモート・ネットワーク・アクセスからの接続機能を制限できます。 Oracle Databaseは、リモート・ネットワークからのアクセスを監査できます。 Oracle Audit Vault and Database Firewallは、データベース監査証跡でリモート・ネットワーク・アクセスが検出されたときにアラートを発行することができます。
昇格されたシステム・アクセス権限を持つ担当者は、システム制御とセキュリティ手順を回避するための内部知識とリソースを持っているため、すべてのシステム・アクティビティを記録して厳重に監督する必要があります。	参考資料1、20ページ、項目xiii	Oracle Databaseは、特権ユーザーのアクティビティを監査できます。Oracle Audit Vault and Database Firewallは、監査データを収集し、分析とレポート作成のために安全なリポジトリに保存します。
特権ユーザーが実行したシステム・アクティビティの監査ロギングを維持します。	参考資料1、21ページ、項目（xiii）（e）	Oracle Databaseは、特権ユーザーが実行するシステム・アクティビティを監査できます。 Oracle Audit Vault and Database Firewallは、特権ユーザーのアクティビティに関する情報を収集し、そのアクティビティに関するレポート作成、分析、アラート生成をサポートします。
アクティビティが取得されているシステム・ログに特権ユーザーがアクセスできないようにします。	参考資料1、21ページ、項目（xiii）（f）	Oracle Audit Vault and Database Firewallは、データベースとオペレーティング・システムから監査ログを抽出し、その情報をデータベース管理者やシステム管理者から分離できる安全なリポジトリに一元的に保存します。
ログの定期的な監査または管理レビューを実施します。	参考資料1、21ページ、項目（xiii）（g）	Oracle Audit Vaultを使用すると、監査データの定期的なレビューが可能になり、レビューアがレビューの完了を証明できるようになります。

Copyright © 2020, Oracle and/or its affiliates

RBIガイドライン	出典	Oracle Databaseコントロール
アプリケーションはデータベース内で無許可のエントリの更新を許可してはならない。	参考資料1、25ページ、項目15	Oracle Database Vaultは、侵害された特権ユーザーからのものを含め、データに対する無許可の更新をブロックできます。 Oracle Databaseは、無許可アクセスの実行の試みを、その試みがOracle Database Vaultによってブロックされている場合でも監査できます。 Oracle Audit Vault and Database Firewallは、分析、レポート作成、アラート生成のためにこの監査情報を収集して保存できます。
すべてのアプリケーション・システムには、この点での明確な責任の割当てを含む、システムのログ監視のポリシー/手順とともに、監査証跡が必要です。財務、顧客、管理、規制、法的側面など、重要/機密情報に影響を与えるすべてのアプリケーションは、トランザクションID、日付、時刻、発信者ID、承認者ID、指定されたユーザーIDにより実行されたアクションなどの詳細を含む精密な監査証跡/ロギング機能を提供する必要があります。クライアント・マシンのIPアドレス、端末のID、または場所のロギングなどのその他の詳細も考慮できます。	参考資料1、25ページ、項目5	Oracle Databaseは、包括的な監査機能を提供します。Oracle Audit Vault and Database Firewallは、レポート作成と分析のために、監査情報を安全なリポジトリで一元管理します。
アプリケーションは、とりわけ、失敗したログオン試行のロギングと、アプリケーションでの機密オプションへのアクセス（マスター・レコードの変更、アクセス権の付与、システム・ユーティリティの使用、システム構成の変更など）のロギングも提供する必要があります。	参考資料1、25ページ、項目6	Oracle Databaseは、失敗したログイン、アクセス権の付与、データベース構成の変更を監査します。
監査証跡は、内部/規制/法的要件に応じ、定義された期間に従って保存する必要があり、改ざんされていないことを保証する必要があります。	参考資料1、25ページ、項目7	Oracle Audit Vault and Database Firewallは、監査情報を、監査データを生成するソースとは別の耐改ざん性リポジトリに保存します。Audit Vault内の監査データの保持は、データベースごとに割り当てられた保持期間によって制御され、単一のAudit Vaultで複数の保持期間要件を満たすことができます。
開発、テスト、本番環境は適切に分離する必要があります。	参考資料1、25ページ、項目9 参考資料2、10ページ、項目6.5	Oracle Data Masking and SubsettingとOracle Data Safeは両方とも、データベースの非本番コピーから機密データを削除します。
アプリケーションへのアクセスは、最小限の特権付与という原則と、職責に応じての"知るべき必要"を満たすという原則に基づいて許可する必要があります。適切な職務の分離を実施する必要があります。	参考資料1、25ページ、項目10	Oracle Database Vaultは、特権ユーザー・アクセスを制御し、データベース管理を機密データへのアクセスから分離し、管理者と開発者によるデータベースの直接の更新を厳密に制御できるようにします。

Copyright © 2020, Oracle and/or its affiliates

RBIガイドライン	出典	Oracle Databaseコントロール
データベースへの直接のバックエンド更新は、間違いなく業務上の必要がある緊急時と、関連ポリシーに従う正当な認可が与えられた場合を除き、許可するべきではありません。	参考資料1、26ページ、項目16	Oracle Database Vaultは、データへのトラステッド・パス・アクセスを強制し、アプリケーション・サービス・アカウントの使用を制限して、データへの非定型アクセスに使用できないようにします。
データベース・プロンプトへのアクセスは、データベース管理者のみに制限する必要があります。	参考資料1、26ページ、項目17	Oracle Database Vaultは、データへのトラステッド・パス・アクセスを強制し、アプリケーション・サービス・アカウントの使用を制限して、データへの非定型アクセスに使用できないようにします。
アプリケーションは、非アクティブ状態が一定期間続いた場合にユーザーをログアウトするように構成する必要があります。アプリケーションは、不完全なトランザクションのロールオーバーを保証するか、そうでなければログアウトした場合のデータの整合性を保証する必要があります。	参考資料1、26ページ、項目26	Oracle Databaseパスワード・プロファイルは、非アクティブなセッションのタイムアウト期間を制御します。プロファイルはユーザー・レベルで割り当てられるため、単一のデータベースでさまざまなクラスのユーザーに対してさまざまな非アクティブ・タイムアウトをサポートできます。
銀行は、データベース、データウェアハウス、データ・アーカイブなど、電子形式で保存されているすべてのデータの整合性と一貫性を確保するための手順を定義して実装する必要があります。	参考資料1、29ページ、項目15）i	Oracle Databaseでは、DB_BLOCK_CHECKSUMパラメータを指定することで、データ・ブロック・チェックサムを適用し、破損したデータ・ブロックまたは悪意を持って変更されたデータ・ブロックを識別できます。 チェックサムは、すべてのブロックを対象とすることも、ブロックのサンプリングを対象とすることもできます。
非常に機密性の高いIT資産や非常に重要なIT資産では、イベントを記録し、リスクのレベルに比例したレベルで監視するためにロギングを有効にする必要があります。	参考資料1、32ページ、項目v	Oracle Databaseの監査では、さまざまなデータベース・オブジェクトとユーザーに対してさまざまなレベルの監査が可能であり、リスクに比例してロギングの量を調整できます。
システム管理者など、昇格されたアクセス権限を持つユーザーは、リスクが高くなっていることを考慮して、より高いレベルの監視を受ける必要があります。	参考資料1、32ページ、項目vi	Oracle Databaseの監査により、エンド・ユーザー・アクティビティの監査が可能になります。これには、アプリケーション・サービス・アカウントとユーザー開始のセッションを区別する機能が含まれます。
監視ログとプロセスの整合性は、適切なアクセス制御と職務の分離によって保護される必要があります。	参考資料1、32ページ、項目vii	Oracle Databaseの監査では、更新および削除操作から保護されたスキーマで監査レコードが保存され、厳密に定義された条件下でのみ監査証跡のパージが許可されます。 Oracle Audit Vault and Database Firewallは、データベース管理者によるアクセスから保護されている安全なリポジトリにデータベース監査証跡を移動することで、この保護を拡張します。

Copyright © 2020, Oracle and/or its affiliates

RBIガイドライン	出典	Oracle Databaseコントロール
銀行はすべてのシステム・アカウントを頻繁に確認し、ビジネス・プロセスやビジネス・オーナーに関連付けることができないアカウントを無効にする必要があります。システムから生成され、頻繁に確認されるレポートには、ロックアウトされたアカウント、無効化されたアカウント、パスワードが最大有効期間を超えているアカウント、パスワードが期限切れなしに設定されているアカウントのリストなどを含めることができます。	参考資料1、32ページ、項目viii	Oracle Audit Vault and Database Firewallは、データベース・アカウントとそのアカウントに割り当てられた権限についてレポートします。未使用/休眠アカウントやロックされたアカウントのレポートも含まれます。 Database Security Assessment ToolとOracle Data Safeはどちらも、パスワードが期限切れになっているアカウントと、期限切れが設定されていないパスワードを持つアカウントを識別します。
銀行はすべてのアカウントの使用状況を定期的に監視し、標準的な非アクティブ期間が経過するとユーザーを自動的にログオフする必要があります。	参考資料1、32ページ、項目x	Oracle Databaseパスワード・プロファイルは、非アクティブなセッションのタイムアウト期間を制御します。プロファイルはユーザー・レベルで割り当てられるため、単一のデータベースでさまざまなクラスのユーザーに対してさまざまな非アクティブ・タイムアウトをサポートできます。
銀行はアカウントの使用状況を監視して、一定期間（たとえば15日間）使用されていない休眠アカウントを特定し、ユーザーまたはユーザーの管理者に休眠状態について通知する必要があります。それより長い期間（たとえば30日）が経過すると、アカウントを無効にできます。	参考資料1、32ページ、項目xi	Oracle Audit Vault and Database Firewallは、休眠アカウントまたは非アクティブなアカウントを含むデータベース・アカウントに関するレポートを作成します。
定期的に、たとえば月次や四半期ベースで、銀行は管理者に対し、勤務している従業員および取引のある請負業者と、管理対象のスタッフのものである各アカウントを突き合わせて照合することを求める必要があります。セキュリティ/システム管理者は、勤務している従業員または取引のある請負業者に割り当てられているものではないアカウントを無効にする必要があります。	参考資料1、32ページ、項目xii	Oracle Audit Vault and Database Firewallは、割り当てられたシステム権限やオブジェクト権限など、データベース・アカウントに関するレポートを作成します。レポートは、データ所有者と管理者による管理された証明に利用できます。
銀行は、監査ロギングによって、非アクティブ化されたアカウントへのアクセスの試みを監視する必要があります。	参考資料1、32ページ、項目xiii	Oracle Databaseは、ロックされたアカウントでのログイン試行を監査できます。
銀行は、各ハードウェア・デバイスとそれにインストールされているソフトウェアの監査ログ設定を検証し、ログに各パケットやトランザクションの日付、タイムスタンプ、送信元アドレス、宛先アドレス、その他のさまざまな有用な要素が含まれていることを確認する必要があります。システムは、syslogエントリなどの標準化された形式でログを記録する必要があります。システムが標準化された形式でログを生成できない場合、銀行はログ正規化ツールを導入して、ログを標準化された形式に変換する必要があります。	参考資料1、32ページ、項目xiv	Oracle Databaseの監査レコードには、タイムスタンプ、送信元アドレス、データベースとOSのユーザー名、およびトランザクションの分析に役立つその他の情報が含まれます。
システム管理者と情報セキュリティ担当者は、特定のシステムからの一般的なイベントのプロファイルを考案することを検討する必要があります。そうすることにより、異常なアクティビティに焦点を当てて検出を調整し、誤検出を減らし、異常をさらに迅速に特定し、重要でないアラートでアナリストが圧倒されてしまうのを防ぐことができます。	参考資料1、32ページ、項目xv	Oracle Audit Vault and Database Firewallは、データベース・アクティビティについてネットワークベースの監視を実行します。Database Firewallプロファイルは、通常のアクティビティをホワイトリストに登録し、通常のアクティビティのパターンからの逸脱についてはブロック/記録/アラート生成するように調整されています。

Copyright © 2020, Oracle and/or its affiliates

RBIガイドライン	出典	Oracle Databaseコントロール
銀行は、規制や法的要件を含む銀行のビジネス要件を満たし、監査を進めやすいものとし、必要な場合にフォレンジックな証拠として機能し、紛争解決を支援するために、IT資産の監査証跡を確実に存在させる必要があります。これには、該当する場合には、財務上の影響がある取引、顧客アカウントの開設、変更、または閉鎖、機密マスター・データの変更、機密性の高いデータ/情報のアクセスまたはコピー、機密性の高いIT資産にアクセスするためのシステム・アクセス権や特権の付与、変更、または取消しなどのさまざまな分野が含まれる可能性があります。	参考資料1、36ページ、項目21）i	Oracle Databaseの監査には柔軟性と拡張性があり、規制および法的コンプライアンスに貢献し、フォレンジック調査をサポートします。
監査証跡は、証拠の保全を含め、取得された情報の整合性を保証するために保護する必要があります。 監査証跡の保持は、ビジネス、規制、法的要件に準拠する必要があります。	参考資料1、36ページ、項目21）ii	Oracle Audit Vault and Database Firewallは、暗号化と強力なアクセス制御を組み合わせて監査証跡を保護します。監査証跡の保持は、さまざまなビジネス要件に対応できるように、データベースごとに構成されます。
近年の事件により、すべての銀行でネットワーク・セキュリティを徹底的に見直す必要性が浮き彫りになってきました。さらに、ビジネスまたは運用上の要件を満たしやすくするために、指定された期間、ネットワーク/データベースへの接続が許可されるということがよくあります。 ただし、その接続が見落とされてしまい閉じられず、ネットワーク/データベースがサイバー攻撃に対して脆弱になるということがあります。ネットワークやデータベースへの無許可アクセスは許可しないことがもっとも重要であり、許可する場合は必ず、明確に定義された、常に従うプロセスに沿います。このようなネットワークやデータベースに対する責任は明確に説明されるべきであり、銀行の職員は常にその責任を負うべきです。	参考資料2、3ページ、項目9	Oracle Databaseは、セッション、データ・オブジェクト、コマンド・レベルで無許可アクセスをブロックするように調整できる、さまざまなアクセス制御メカニズムをサポートしています。
銀行の情報分類/機密基準に基づいてデータ/情報を分類します。	参考資料2、7ページ、項目1.2 参考資料3、1ページ、項目1.2	透過的機密データ保護（TSDP）：TSDBを使用すると、異なる表の列を任意の分類タイプにグループ化できます。特定のタイプであるすべての列は、暗号化と監査を必要とするポリシーによって管理される場合があります。
さまざまなベンダー/OEMによるパッチのリリース、CERT-Inや他の類似の機関によって発行される勧告を継続的に監視し、銀行のパッチ管理ポリシーに従ってセキュリティ・パッチを迅速に適用します。	参考資料2、8ページ、項目2.3	Oracle Critical Patch Update（CPU） - オラクルの顧客は登録して、対処されたリスクのCVSSスコアを含む、セキュリティ・パッチの通知を受け取ることができます。
システム、サーバー、ネットワーク・デバイス、エンドポイントにおける異常なアクティビティを検出して修復するメカニズムを導入します。	参考資料2、9ページ、項目4.7	Oracle Audit Vault and Database Firewallは通常のアクティビティをプロファイルし、異常なアクティビティにアラートを発行したり、それをブロックしたりすることができます。

Copyright © 2020, Oracle and/or its affiliates

RBIガイドライン	出典	Oracle Databaseコントロール
すべてのシステムの重要なデバイス（ファイアウォール、ネットワーク・スイッチ、セキュリティ・デバイスなど）の構成とパッチ・レベルを定期的に評価します。	参考資料2、9ページ、項目5.2	Oracle Database Security Assessment ToolとOracle Data Safeはどちらもデータベース構成を評価し、ベスト・プラクティスからの差異をレポートします。
保存中のデータ/情報を保護することで、銀行のネットワーク内外から銀行の資産/サービスへの安全なアクセスを提供します。	参考資料2、11ページ、項目8.1	透過的データ暗号化は、データベース内の保存データを暗号化します。
一元管理型の認証および認可システムを実装するか、アプリケーション、オペレーティング・システム、データベース、ネットワーク、セキュリティ・デバイス/システム、接続ポイント（ローカル/リモートなど）へのアクセスと管理を実装します。これにはリスク評価に応じた強力なパスワード・ポリシーおよび2要素/多要素認証の実施が含まれ、最小限の特権と職務の分離の原則に従います。	参考資料2、11ページ、項目8.4	エンタープライズ・ユーザー・セキュリティと集中管理ユーザーは、Oracle Databaseに一元的な認証と認可を提供します。 認証には、パスワード、Kerberos、PKI証明書、RADIUSを介した多要素を使用できます。 Oracle Databaseは、パスワードの複雑さ、最小長要件、有効期限などをサポートしています。 Oracle Database Vaultは、データベース管理者の機密データへのアクセスを制限するなど、職務の分離を実施します。
重要なシステムへの特権/スーパーユーザー/管理アクセスを許可、管理、記録、監視するための適切な（例：一元管理型の）システムと制御を実装します。	参考資料2、11ページ、項目8.5 参考資料3、3ページ、項目7.4	Oracle Audit Vault and Database Firewallは、データベースへの特権アクセス、スーパーユーザー・アクセス、および管理アクセスに関する一元管理型のロギングと監視を提供します。
無効なログオン数を最小限に抑え、休眠アカウントを非アクティブ化するための制御を実装します。	参考資料2、11ページ、項目8.6	Oracle Audit Vault and Database Firewallは、休眠ユーザー・アカウントおよび失敗したログイン試行に関するレポートを作成します。
ログオン・パターンの異常な変化を監視します。	参考資料2、11ページ、項目8.7	Oracle Audit Vault and Database Firewallは、異常なログイン・パターンを検出し、アラートを発行し、ブロックします。
包括的なデータ損失/漏えい防止戦略を策定し、機密性の高い（機密情報を含む）ビジネスおよび顧客のデータ/情報を保護します。	参考資料2、14ページ、項目15.1	Oracle Database Security Assessment Tool、Oracle Data Masking and Subsetting、およびOracle Data Safeはそれぞれ、機密データの検出機能を提供します。Oracle Audit Vault and Database Firewallは、機密データへのアクセスを検出します。
監査ログを体系的に管理および分析して、攻撃を検出、理解し、攻撃からの回復を図ります。	参考資料2、14ページ、項目16.1	Oracle Audit Vault and Database Firewallは、分析のために監査ログを収集し、安全に保管します。監査ログは安全なリポジトリに転送されるので、攻撃の発生時に起きた事柄を理解するために使用できます。

Copyright © 2020, Oracle and/or its affiliates

RBIガイドライン	出典	Oracle Databaseコントロール
各デバイス、システム・ソフトウェア、アプリケーション・ソフトウェアの適切なログ/監査証跡を取得するための設定を実装して定期的に検証し、日付、タイムスタンプ、送信元アドレス、宛先アドレスなど、ログを一意に識別するための最小限の情報がログに含まれていることを確認します。	参考資料2、14ページ、項目17.1 参考資料4、8ページ、項目6.3	Oracle Audit Vault and Database Firewallは、データベースやオペレーティング・システムのセキュリティ・ログを含む、各データベース・サーバーの監査ログを取得します。このシステムは拡張可能であり、カスタム・コレクタ・フレームワークを使用して、ほとんどのアプリケーションの監査証跡を取得することもできます。
すべての重要なシステムに対して脆弱性評価と侵入テストを定期的に実施します。	参考資料2、14ページ、項目18.1	Oracle Database Security Assessment ToolとOracle Data Safeはどちらも、システムの脆弱性の評価に使用できるセキュリティ評価機能を提供し、既知の脆弱性の早期検出と修復によって侵入テスト体制を強化します。
システム内のユーザー・アクションに関する監査ログを取得します。このような仕組みにより、必要な場合のフォレンジック監査は容易になるはずです。	参考資料4、6ページ、項目10.1	Audit Vault and Database Firewallは、監査ログを取得し、分析とレポート作成のために安全なリポジトリに保存します。
ログ設定の変更を監視するように、アラート・メカニズムを設定する必要があります。	参考資料4、6ページ、項目10.2	Audit Vault and Database Firewallでは、監査設定の変更に関するレポート作成とアラート生成が可能です。
保存中のデータ/情報の保護（デバイスでサポートされている場合は暗号化を使用するなど）および転送中のデータ/情報の保護（VPNやその他の標準的なセキュア・プロトコルなどのテクノロジーを使用するなど）により、UCBのネットワーク内外からUCBの資産/サービスへの安全なアクセスを提供します。	参考資料4、6ページ、項目6.1	Oracle Databaseは、転送中のデータを保護するために、Native Network Encryptionと業界標準のTransport Layer Security（TLS）1.2の両方を提供しています。Oracle Transparent Database Encryptionは、データベースのバックアップ、クローン、エクスポートなどの保存データを暗号化します。
監査ログを体系的に管理および分析して、攻撃を検出、対応、理解し、攻撃からの回復を図ります。	参考資料4、8ページ、項目6.2	Audit Vault and Database Firewallは、監査ログを管理および分析する機能を提供します。

まとめ

インド準備銀行のガイドラインは、金融機関のセキュリティのための包括的な枠組みを提供します。Oracle Databaseのセキュリティ機能は、これらのガイドラインの遵守において重要な役割を果たします。

参考資料

1. Guidelines on Information security, Electronic banking, Technology risk management and cyber frauds http://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf
2. Cyber Security Framework in Banks https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56 272EB.PDF
3. Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs) http://rbidocs.rbi.org.in/rdocs/content/pdfs/63NT19102018_A1.pdf
4. Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI129BB26DEA3F5C54198BF24774E1222E61A.PDF

Copyright © 2020, Oracle and/or its affiliates

CONNECT WITH US

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。
北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

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

Copyright © 2020, Oracle and/or its affiliates.All rights reserved.本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は、その内容に誤りがないことを保証するものではなく、また、口頭による明示的保証や法律による黙示的保証を含め、商品性ないし特定目的適合性に関する黙示的保証および条件などのいかなる保証および条件も提供するものではありません。オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはOracleおよびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

データベース・セキュリティと規制遵守
2020年6月
Database Security Product Management、Russ Lowenthal