クラウドデータベース(データベースサービス)におけるセキュリティベストプラクティス

	AWS				OCI				Azure				Google Cloud			
	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所	カテゴリ	機能・サービス名	設定方法・構成案	記載箇所
1	アクセス制御															
1-1	認証方式	IAM	Amazon RDS リソースを管理するユーザー (本人を含む) ごとに個別のユーザーを作成します。	Amazon RDS のセキュリティのベストプラクティス	認証方式	DBパスワード管理	ユーザーはパスワードを利用してデータベース認証されるため、パスワードはガイドラインに従った強固なパスワードを推奨。 ・12~30文字の英数字 ・少なくとも1つの数字、1つの大文字、1つの小文字 ・大文字と小文字を混在させ、特殊文字を使用する　など	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure Virtual Network	論理的にセグメント化し、ゼロトラストアプローチを採用	Azure Virtual Network	アクセス制御	VPC	データベースへのアクセスを制限し、自己ホスト型データベースでは許可されたホストのみに情報のやり取りを認め、不要なポートとエンドポイントをブロックする。	Google Cloud データベース セキュリティのベスト プラクティス
1-2	認証方式	IAM	Amazon RDS リソースの管理には、AWS ルート認証情報を使用しないでください。 それぞれの職務の実行に最低限必要になる一連のアクセス許可を各ユーザーに付与します。	Amazon RDS のセキュリティのベストプラクティス	アクセス制御	仮想クラウドネットワーク(VCN)	VCNのネットワーク・セキュリティ・グループまたはセキュリティ・リストを構成し、データベースに対して最小限のアクセスのみ許可することを推奨。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure Virtual Network	ネットワーク セキュリティ グループ (NSG) でルーティング制御とセキュリティゾーンを強化	ネットワーク セキュリティ グループ	認証方式	Cloud KMS	サービスアカウントの鍵を自動ローテーションし、Googleデータベースへの権限付与を簡略化する。	Google Cloud データベース セキュリティのベスト プラクティス
1-3	認証方式	IAM	Amazon RDS のシークレットが自動的にローテーションされるように、AWS Secrets Manager を設定します。 どのユーザーが Amazon RDS リソースの管理を許可されるかを決定するアクセス許可を割り当てます。	Amazon RDS のセキュリティのベストプラクティス	アクセス制御	仮想クラウドネットワーク(VCN)	セキュリティ・ルールをプライベート・サブネットとともに使用して、データベース・システムへのアクセスを制限可能。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure DDoS Protection Azure Bastion	DDoS 攻撃から保護するための強化された DDoS 軽減機能、 RDP/SSHアクセスを簡効化し、安全な接続を提供	Azure DDoS Protection Azure	認証方式	Cloud KMS	認証情報のローテーションを管理する。	Google Cloud データベース セキュリティのベスト プラクティス
1-4	認証方式	AWS Management Console	AWS CLI、RDS API マスターユーザーのパスワードを変更します。	Amazon RDS のセキュリティのベストプラクティス	アクセス制御	仮想クラウドネットワーク(VCN)	複数層デプロイメントでは、プライベート・サブネットおよびVCNセキュリティ・ルールを使用して、アプリケーション層からデータベース・システムへのアクセスを制限可能。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Azure ExpressRoute Azure VPN Gateway	専用WANリンクを活用し、インターネットへの露出を避けてパフォーマンスを最適化	Azure ExpressRoute Azure VPN Gateway	認証方式	IAM	ユーザー権限を管理する際に強力なツールとして使用し、個々のアプリケーションには必要な許可を与えたサービスアカウントを作成する。	Google Cloud データベース セキュリティのベスト プラクティス
1-5	アクセス制御	VPC	Virtual Private Cloud (VPC) 内で DB インスタンスを実行して、ネットワークアクセス制御を最大限に拡張します。	Amazon RDS のセキュリティのベストプラクティス	認証方式	Identity and Access Management (IAM)	OCIリソースへアクセス、操作する権限の管理を実施可能。 特にデータベースの削除権限(DATABASE_DELETEおよびDB_SYSTEM_DELETE)は、最小限のIAMユーザーおよびグループに付与することを推奨。	セキュリティのベスト・プラクティス データベースの保護	アクセス制御	Private Link (プライベート エンドポイント) Service Endpoints	Azureリソースへのアクセスを仮想ネットワーク内に制限	プライベート エンドポイント Service Endpoints				
1-6	アクセス制御	VPC	セキュリティグループを使用して、どの IP アドレスまたは Amazon EC2 インスタンスが DB インスタンスの上のデータベースに接続できるかを制御します。	Amazon RDS のセキュリティのベストプラクティス	管理者権限の分掌	Identity and Access Management (IAM)	DELETE権限はテナンシ管理者およびコンパートメント管理者にのみ付与。	セキュリティのベスト・プラクティス データベースの保護	認証方式	Microsoft Entra ID	一元的なID管理とパスワード認証の最小化	Microsoft Entra の多要素認証				
1-7	認証方式	AWS RDS	DB エンジンのセキュリティ機能を使用して、DB インスタンスのデータベースにログインできるユーザーを制御します。 これらの機能は、データベースがローカルネットワーク上にあるかのように動作します。	Amazon RDS のセキュリティのベストプラクティス					認証方式	Microsoft Entra ID	テナント全体やActive Directoryドメインに対して多要素認証を適用	Microsoft Entra の多要素認証				
1-8	認証方式	AWS Backup	バックアップに関して、職務とアクセス権を明確に分離して管理します。 バックアップはアカウントレベルで分離し、イベントの発生時に影響を受ける環境から分離した状態を維持できるようにします。	AWS Well-Architected フレームワーク					認証方式	Azure Key Vault	パスワードやシークレットを保護し、アクセス ポリシーで管理	Azure Key Vault				
1-9									認証方式	Azure RBAC	リソースごとの細分化されたアクセス許可と、データベースロールやSQL Managed Instanceのサーバーロール単位での制御	Azure RBAC				
1-10									認証方式	SQL 脆弱性評価 (VA)	脆弱性評価 (VA) を使用して、アクセス許可の適切性をチェック	SQL 脆弱性評価 (VA)				
2	暗号化															
2-1	データ暗号化・鍵管理	AWS RDS	データベースエンジンを実行している DB インスタンスと Transport Layer Security (TLS) の接続を使用します。	Amazon RDS でのセキュリティ	データ暗号化・鍵管理	TDE暗号化	OCIに作成されるすべてのデータベースは、透過的データ暗号化(TDE)を使用して暗号化される。 ただし、RMANを使用して、暗号化されていないデータベースをオンプレミスからOCIに移行する場合、暗号化を実施する必要があることに注意。	セキュリティのベスト・プラクティス データベースの保護	データ暗号化・鍵管理	Transparent Data Encryption (TDE)	Transparent Data Encryption (TDE) によるサーバーレベルの暗号化	Transparent Data Encryption (TDE)	データ暗号化・鍵管理	Cloud KMS	自動的な保存時暗号化に加え、アプリケーションレベルでも暗号化を実施する。	Google Cloud データベース セキュリティのベスト プラクティス
2-2	データ暗号化・鍵管理	AWS RDS	Amazon RDS 暗号化を使用して、DB インスタンスおよび保管時のスナップショットのセキュリティを確保します。	Amazon RDS でのセキュリティ	データ暗号化・鍵管理	TDE暗号化	TDEマスター・キーを定期的にローテーションすることを推奨。推奨のローテーション期間は90日以内です。	セキュリティのベスト・プラクティス データベースの保護	データ暗号化・鍵管理	Azure Key Vault	カスタム・データベースレベルでの暗号化	Azure Key Vault	データ暗号化・鍵管理	Cloud SQL	データベースに送られるあらゆる入力にはサニタイズなどの防衛手段を講じる。	Google Cloud データベース セキュリティのベスト プラクティス
2-3	データ暗号化・鍵管理	AWS RDS	Amazon RDS 暗号化は業界スタンダードのAES-256暗号化アルゴリズムを使用してDBインスタンスをホストしているサーバーでデータを暗号化します。	Amazon RDS でのセキュリティ	データ暗号化・鍵管理	Oracle Wallet	Oracle Walletを作成する場合、Oracle Walletのパスワードは強力なパスワード(8文字以上で少なくとも1つの大文字、1つの小文字、1つの数字および1つの特殊記号を含む)を設定することを推奨。	セキュリティのベスト・プラクティス データベースの保護	データ暗号化・鍵管理	Always Encrypted	Always Encryptedでデータへのアクセスを細かく制御し、DBAやクラウド管理者、悪意のあるアクターからのデータ保護	Always Encrypted				
2-4					データ暗号化・鍵管理	Oracle Key Vault(OKV)	Oracle Key Vault (OKV)は、Oracle TDEマスター・キーの管理に使用されるキー管理アプライアンス。OKVでは、TDEマスター・キーの格納、ローテーションおよびアクセスの監査を実施可能。	セキュリティのベスト・プラクティス データベースの保護								
3	構成、設定、運用管理															
3-1	ポリシーの策定と適用	AWS Security Hub	リソース設定とセキュリティ標準を評価し、お客様がさまざまなコンプライアンスフレームワークに準拠できるようサポートする。	AWS セキュリティ監査のガイドライン	ポリシーの策定と適用	Security zones	要件に応じた複数のポリシーまとめたレシピを作成し適用することで、複数のポリシーを一括で適用することが可能。 パブリックアクセス可能なリソース作成の禁止、暗号化の強制化など、セキュリティ要件を強制することで人為的なミスを防止。	セキュリティのベスト・プラクティス セキュリティ・ゾーンの保護	ポリシーの策定と適用	データの検出と分類	SQLデータの検出と分類 (SQL Data Discovery and Classification)	データの検出と分類	ポリシーの策定と適用	Security Command Center	ソフトウェアのアップデートポリシーを策定し、古くなったパッケージについてアラートを送る。	Google Cloud データベース セキュリティのベスト プラクティス
3-2					ポリシーの策定と適用	Oracle Database Security Assessment Tool	Oracleデータベースの自動的なセキュリティ構成チェックを提供。 ユーザー権限、データベース認可、ポリシー、データベース・リスナー構成、OSファイル権限、格納される機密データについてセキュリティ・チェックを実行。	セキュリティのベスト・プラクティス データベースの保護	ポリシーの策定と適用	Microsoft Defender for Cloud / Microsoft Defender for SQL SQL 脆弱性評価 (VA)	脆弱性評価を実施し、データベースの潜在的な脆弱性を検出・修復	SQL 脆弱性評価 (VA)				
4	監視、ログ、監査															
4-1	不正な通信の監視/通知	AWS Security Hub	セキュリティのベストプラクティスに関連する RDS の使用状況をモニタリングできます。	AWS セキュリティ監査のガイドライン	不正な通信の監視/通知	Audit Vault and Datab	データベース内のアクティビティやネットワークトラフィックを監視し、不正アクセスや異常な動作を検出、即座にアラートを生成。	セキュリティのベスト・プラクティス データベースの保護	不正な通信の監視/通知	Microsoft Defender for SQL SQL Advanced Threat Protection	SQLデータベースの保護と監視	Microsoft Defender for SQL SQL Advanced Threat Protection	不正な通信の監視/通知	Cloud Logging	ファイアウォールに対する変更のログを収集し、予期しない変更にはアラートが送信されるようにする。	Google Cloud データベース セキュリティのベスト プラクティス
4-2					定期監査の実施	Cloud Guard	セキュリティ脅威や誤構成を検出、ユーザーによる安全でないアクティビティの監視を実施。	セキュリティのベスト・プラクティス クラウド・ガードの保護	不正な通信の監視/通知	Always Encrypted (キーの管理) Azure Storage へのアクセスの承認	ストレージアカウントへのアクセス制限、職務分離をサポートし、DBAと監査者を分離	Always Encrypted (キーの管理) Azure Storage へのアクセスの承認	定期監査の実施	Cloud Logging	ログは、データベースとは離れた場所にホスティングされた書き換え不能なロギングサービスで集約する。	Google Cloud データベース セキュリティのベスト プラクティス
4-3					定期監査の実施	Data Safe	セキュリティ構成の評価、ユーザーのリスク評価、アクティビティの監査、機密データの発見、データ・マスキング等の機能があり、専門知識がなくともデータベースセキュリティ対策を講じることが可能。	セキュリティのベスト・プラクティス データベースの保護	定期監査の実施	SQL Database Auditing	Azure SQL Database および Azure Synapse Analytics の監査	Azure SQL Database および Azure Synapse Analytics の監査	不正な通信の監視/通知	Security Command Center	GCPのファイアウォールを変更すると、アラートの送信が自動的に行われる。	Google Cloud データベース セキュリティのベスト プラクティス
4-4					定期監査の実施	Cloud Guard	ユーザーによる安全でない振る舞いを監視し不正な操作を早期発見	セキュリティのベスト・プラクティス クラウド・ガードの保護	不正な通信の監視/通知	Microsoft Defender for SQL SQL Advanced Threat Protection	データベースの不審なアクティビティを監視し、SQLインジェクション攻撃や異常なデータベースアクセスを検知・通知	Microsoft Defender for SQL SQL Advanced Threat Protection	監査ログの保全	Cloud SQL	データベースはすべてのキーイベント、特にログイン試行や管理者機能のログを生成する。	Google Cloud データベース セキュリティのベスト プラクティス
4-5													監査ログの保全	IAM	ログの認証情報と読み出しアクセスは、データベースの認証情報から完全に切り離す。	Google Cloud データベース セキュリティのベスト プラクティス
5	システムの冗長化、バックアップ															
5-1	定期バックアップ	AWS Backup	AWS サービス間のデータのバックアップを自動化することを検討してください。	AWS Well-Architected フレームワーク	定期バックアップ	管理対象バックアップ	バックアップは管理対象バックアップ(Oracle Cloud Infrastructureコンソールまたは API を使用して作成されるバックアップ)を使用することを推奨。 管理対象バックアップは、Oracleによってオブジェクト・ストアのユーザーと資格証明が管理され、暗号化も自動的に実施される。 管理対象バックアップを使用しない場合は、オブジェクト・ストアのパスワードを定期的に変更することを推奨。	セキュリティのベスト・プラクティス データベースの保護	定期バックアップ	Azure Storage	ローカル冗長ストレージ（LRS）やゾーン冗長ストレージ（ZRS）による可用性を確保	Azure Storage				
5-2					定期バックアップ	自動バックアップ	Autonomous Recovery ServiceまたはObject Storageをバックアップ先として選択可能。Autonomous Recovery Serviceは、リアルタイムでデータベースを保護し、被害の直前まで完全な復旧が可能。Object Storageは、週次の完全バックアップと日次の増分バックアップを作成。どちらもバックアップの保持期間やスケジュールの管理機能を提供。	Oracle Cloud Infrastructure向けの適切に設計されたフレームワーク：データのバックアップ	定期バックアップ	自動バックアップ ポイントインタイム リストア	自動バックアップ機能とポイントインタイムリストアでデータ保護	自動バックアップ ポイントインタイム リストア				
5-3					定期バックアップ	Autonomous Recovery Service	Zero Data Loss Autonomous Recovery Service(ZRCV)では、データベースをリアルタイムで保護し、停止またはランサムウェア攻撃が発生したとき1秒未満までのリカバリが可能。 データベースの自動バックアップを有効にする際、保護されたデータベースバックアップを保持するためには、次のいずれかのオプションを指定 ・保護ポリシー保持期間に従ってバックアップを保持：データベース終了後、リカバリサービスは、割り当てられた保護ポリシーで定義された期間のバックアップを引き続き保持。 ・バックアップを72時間保持してから削除：リカバリサービスは、データベース終了後、72時間（3日）のバックアップを保持後、削除。	Autonomous Recovery Serviceの保護	定期バックアップ	高速データベース復旧 (ADR)	高速データベース復旧（ADR）で迅速かつ一貫性のある復旧、トランザクションのロールバック、ログの積極的切り捨て	高速データベース復旧				
5-4					可用性（データベース）	Oracle Data Guard/Oracle Active Data Guard	ビジネスの生命線となるミッションクリティカルなデータベースに対して、最適なデータ保護とデータ可用性のソリューションを提供	Oracle Cloud Infrastructure向けの適切に設計されたフレームワーク：データのレプリケート	定期バックアップ	Azure Geo-replication Azure Backup	データの冗長性と長期リテンションを提供	長期リテンション				
5-5					可用性（インフラ全体）	Full Stack Disaster Recovery	インフラストラクチャー、ミドルウェア、データベース、アプリケーションなど、アプリケーション・スタックのすべてのレイヤーに対して包括的なディザスタ・リカバリ機能を提供	Oracle Cloud Infrastructure向けの適切に設計されたフレームワーク：障害回復戦略の計画								
6	その他															
6-1					その他	Maximum Security Architecture	Oracle Maximum Security Architectureは、データベース内の機密データを保護するための堅牢なフレームワーク。データベースセキュリティに対する包括的なアプローチを提供し、評価、検出、及び防止の3つの重要な領域に分類。データベースの現在の状態を評価することで、組織は攻撃者が悪用する可能性のある脆弱性や弱点を特定。これには、データベースの構成、ユーザー・アクセス制御、データ保護対策の評価を含む。	Oracle Cloud Infrastructure向けの適切に設計されたフレームワーク：データベースの保護					その他	Cloud SQL	独自データベースをどうしてもデプロイしなければならない理由がなければ、マネージドサービスを使うことをお勧めする。	Google Cloud データベース セキュリティのベスト プラクティス
6-2													その他	Cloud SQL	Googleのマネージドデータベースサービスは大規模環境に耐えられるように設計され、Googleのセキュリティモデルの利点を備えている。	Google Cloud データベース セキュリティのベスト プラクティス
6-3													その他	Cloud SQL	PCI、SOX、HIPAA、GDPRなどの規則に準拠することを目指す企業にとって、共有責任モデルにより自社の要件が大幅に減る。	Google Cloud データベース セキュリティのベスト プラクティス
6-4													その他	Cloud SQL	規則が適用されない場合でも、PCI SAQ A（PCI DSS自己問診タイプA）に従うことをお勧めする。	Google Cloud データベース セキュリティのベスト プラクティス