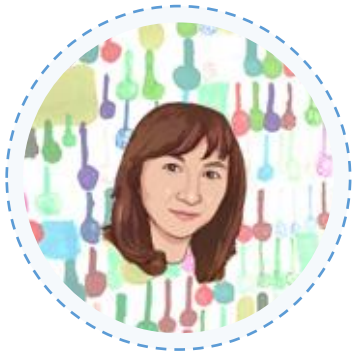
データを守る！
クラウドDBセキュリティ要件対応ガイド
AWS・OCI・Azure・Google Cloudの活用術

伊藤忠テクノソリューションズ株式会社 村山 佳子
サブスクライバ 安澤 弘子
日本電気株式会社 岩本 裕司
株式会社オープンストリーム（在籍当時） 北島 悠
日本オラクル株式会社 大澤 清吾
データベースセキュリティWG

自己紹介



サブスクライバ 安澤

CTC 村山

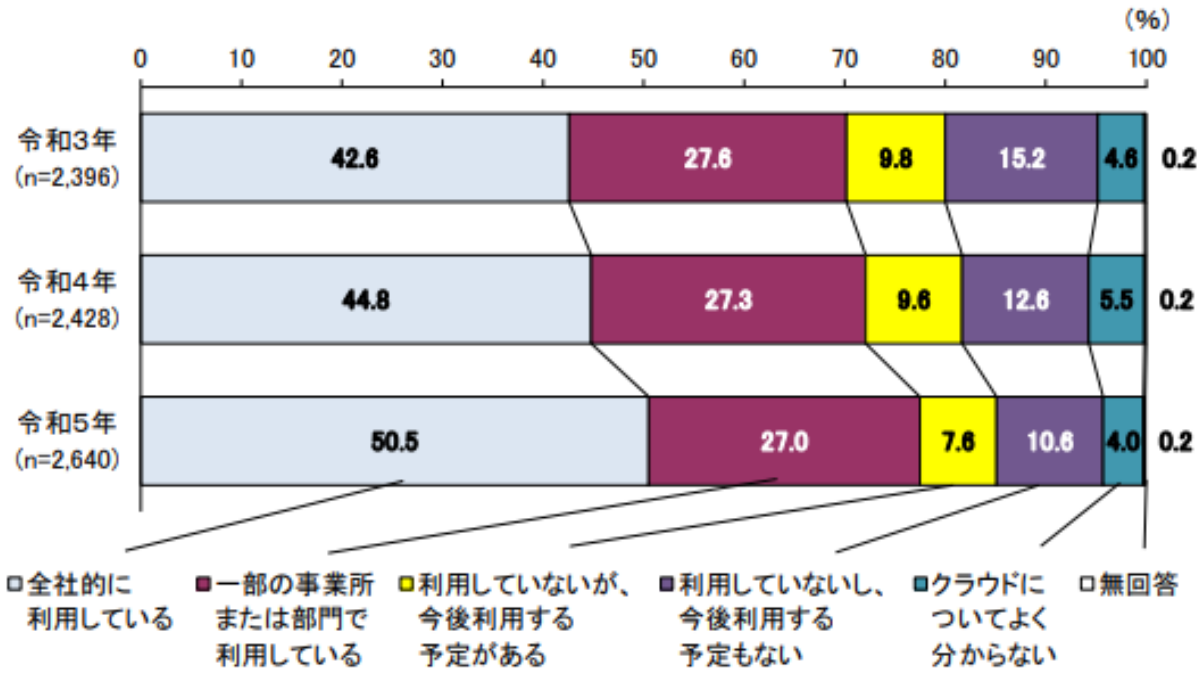
オープンストリーム（在籍当時） 北島

NEC 岩本

日本オラクル 大澤

チームの活動目的・背景

企業における**クラウドサービスの利用は年々増加**し、
クラウド環境におけるリスクを考慮したセキュリティ対策が必要



（出典）総務省「令和５年 通信利用動向調査報告書（企業編）図表 3-1 クラウドサービスの利用状況（時系列） 」
https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202300_002.pdf

- 各クラウドベンダーから
セキュリティのベストプラクティスや
必要なセキュリティ機能が提供されている

- 各クラウドサービスが提示している、データベースサービスにおけるベストプラクティスを、セキュリティ要求事項ごとに整理し、対応する機能やその特徴を比較・横断的に参照していただけるものを目指した

目次

1. クラウド環境におけるリスク

1-1. クラウドならではのセキュリティのリスクと責任分界点

1-2. クラウドでDBを使う際の考慮点

2. 各クラウドベンダー（AWS・OCI・Azure・Google Cloud）のセキュリティガイドラインの概要

2-1. 調査内容・結果サマリ

2-2. AWSのベストプラクティスの概要・特筆ポイント

2-3. OCIのベストプラクティスの概要・特筆ポイント

2-4. Azureのベストプラクティスの概要・特筆ポイント

2-5. Google Cloudのベストプラクティスの概要・特筆ポイント

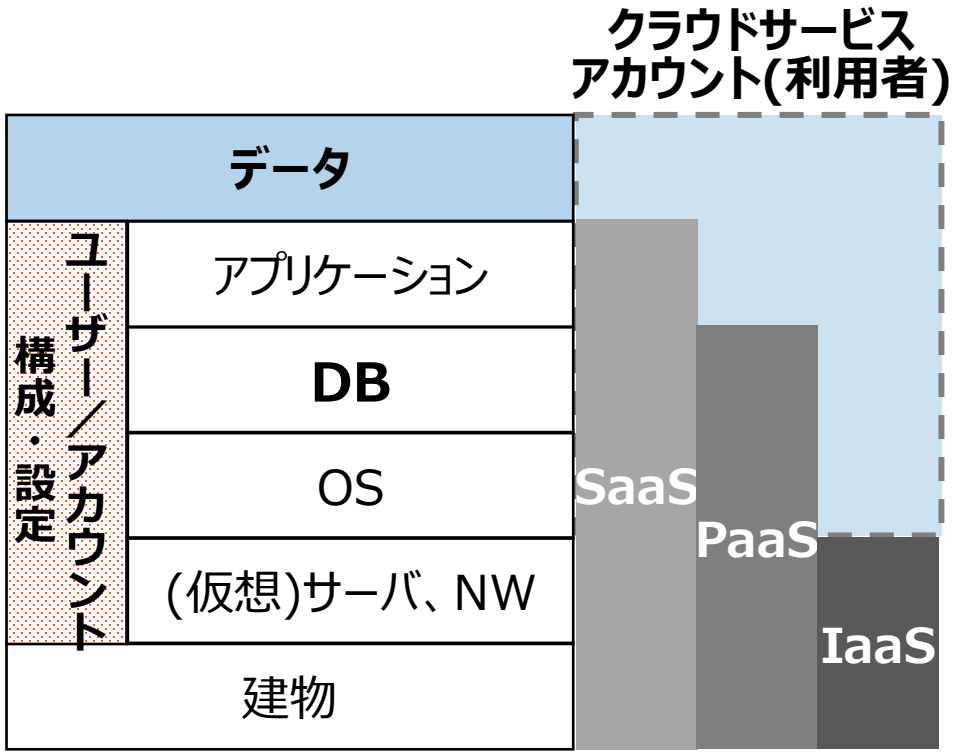
3. まとめ

1.クラウド環境におけるリスク

クラウドならではのセキュリティのリスク
クラウド環境のセキュリティで留意すべきこと

責任共有モデル（責任分界点）の理解

- クラウドスサービスでは、一般的に仮想サーバ・NWレイヤ以上がセキュリティの責任範囲であり、オンプレよりセキュリティ対策における責任範囲が少ない
- 「ユーザー/アカウント」および「構成・設定」はすべてのレイヤーにおいて利用者の責任である
  例えば、PaaS環境ではデータベースに特化したセキュリティ対策だけでなく、**クラウド全体でのユーザー管理やアクセス制御の設定、データベースへアクセスするネットワーク構成のセキュリティ対応にも留意**する必要がある



クラウドならではのセキュリティのリスク
クラウドならではの恐ろしさ(1/2)

1 機密性・完全性

アクセスコントロール設定でフルオープンになってしまうリスク

- 設定自体は簡単で容易に行えるが、オンプレだとインフラ/NW管理者が行うことをアプリ管理者やユーザーが行うことで、オペレーションミスが起きやすい
- その結果、意図せず誰でもアクセスできる状態になり、データがフルオープンになってしまう
- 最終的には、データが簡単に破壊されてしまうことも

2 可用性

ボタン一発で消去できるリスク

- 全データが環境ごとボタン一発で消去できてしまう

クラウドならではのセキュリティのリスク
クラウドならではの恐ろしさ(2/2)

3 体制・運用

- クラウドサービスの変化が速い
  - クラウドサービス自体の変化が迅速で、また環境構築や変更が簡単にできるため、セキュリティ対応が追い付かない
- 全体像が見えづらく管理が難しい
  - サービスやシステムごとに環境構築や変更が容易に行えるため、管理部門がセキュリティ対応の全体を把握しづらい

クラウドでデータベースを使う際の考慮点

クラウドでデータベースを使う時ならではのセキュリティリスクがある

従来の境界型防御を適用できない場合がある

ユーザー管理のネットワークではなく、
クラウド事業者管理のネットワーク上に
データベースが配置されるサービスもある

データベースでのセキュリティ設計・設定が必須

- クラウドデータベースサービスにおいても、情報漏えい・データ消失・サイバー攻撃・不正アクセス等のリスクが存在
- クラウドでは物理セキュリティ対策は不要だが、ネットワークセキュリティ、アクセス制御（権限・認証）、暗号化、監査、バックアップは対策必須

オペレーションミスが発生しやすい

オンプレミスではDBAが行うことを
アプリユーザーが担当することも多い

正しく設定できているかを監視

クラウドの構成チェック・監視機能を活用

PaaS・SaaSを活用

セキュリティ対策の範囲が狭くなるため、
データベースでの対策に絞ることが可能

2.各クラウドベンダーのセキュリティガイドラインの概要

調査内容・結果サマリ

【調査内容】 クラウドベンダー提示のベストプラクティスを、セキュリティ要件事項ごとに整理

- 対応する機能やその特徴を比較・参照できるよう、Excelファイルに一覧化
- 特徴的な点をピックアップ

#	セキュリティ要件	概要
1	アクセス制御	DBユーザー、認証・認可、権限管理に関するベストプラクティス
2	暗号化	データや接続経路の暗号化に関するベストプラクティス
3	構成・設定、運用管理	データベースの構成・設定やパッチ適用に関するベストプラクティス
4	監視、ログ、監査	データベースアクティビティの監視方法、ログ取得や監査方法に関するベストプラクティス
5	システムの冗長化、バックアップ	可用性確保のための冗長化やデータのバックアップに関するベストプラクティス
6	その他	上記1～5に分類できないベストプラクティス

【調査対象】

- AWS、OCI、Azure、Google Cloud
- クラウドのPaaSを前提とし、IaaSに構築するケースは対象外

【調査結果】 全ベンダーですべての分野でベストプラクティスが提供されている

- ただし粒度には違いがあり、実装方法の違いもあり

AWS：ベストプラクティスの概要・特筆ポイント

概要

AWS でワークロードを構築する際に役立つAWS Well-Architected というフレームワークがあり、その中でセキュリティに関する指針が示されています。また、Amazon RDS、Amazon Aurora などのデータベースサービス毎にセキュリティのベストプラクティスが公開されています。AWSのデータベースサービスは、IAMを用いたDBユーザー認証、キー管理サービスでのDB暗号化キーの管理など、AWSのセキュリティ関連サービスを活用してセキュリティを高めることができます。

特筆ポイント

1. AWS Security Hub

   セキュリティ業界標準およびベストプラクティスに照らした AWS 環境評価を実施し、 AWS のセキュリティ状態を包括的に把握することができます。セキュリティのベストプラクティスに照らし合わせたDBの使用状況をモニタリングできます。

2. AWS Secrets Managerを用いたシークレット管理

   データベース認証情報、アプリケーション認証情報などのシークレットのライフサイクル管理を提供します。データベースパスワードを含む認証情報をアプリケーション内にハードコードする代わりに Secrets Manager への API コールに置き換えてプログラムでシークレットを取得できます。認証情報はアプリケーションに保存されないため、シークレット更新時にアプリケーションやクライアントの変更は不要です。これにより、シークレットの有効期間を短期することが可能となり、セキュリティリスク減少に役立ちます。

OCI：ベストプラクティスの概要・特筆ポイント

概要

OCIは、「セキュリティ・バイ・デザイン」に基づき、ストレージとデータベースの全データが強制的に暗号化されたインフラ基盤を提供しています。また、「セキュリティ管理の自動化」に注力し、データベースセキュリティを統合的に管理するData Safeや、Zero Data Loss Autonomous Recovery Service によるランサムウェア対策も提供しています。さらに、Database Vaultによる職務分掌や、総合的なセキュリティフレームワークMaximum Security Architectureを提供します。

特筆ポイント

1. Data Safe

   専門知識がなくてもデータベースセキュリティ対策を実施できるサービスで、構成やユーザー情報からセキュリティリスクを評価し、監査ログの可視化、テスト用のマスキングデータ生成、SQLファイアウォールの管理が可能です。

2. Database Vault

   データベースの特権ユーザーのアクセス制御をおこなうことができる機能です。この機能を利用して特権ユーザーによるデータアクセスを制御することによって、データ漏洩・破壊を防ぐことができます。

3. 強制的なデータ暗号化

   OCIで作成されるすべてのデータベースと自動バックアップは強制的に暗号化されます。キー管理では、Oracle管理キーと顧客管理キーを選択でき、OCI Vaultを使用してキーのローテーション管理コストを低減できます。

4. ランサムウェア対策に有効な高度なバックアップ

   Zero Data Loss 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です。

Azure：ベストプラクティスの概要・特筆ポイント

概要

Azureでは、一般的なセキュリティ要件に対応するため、データ層を含む多層防御アプローチを推奨しています。このアプローチは、ネットワークセキュリティ、アクセス管理、脅威防止、情報保護と暗号化を組み合わせたものです。さらに、データベースセキュリティ向上のため、脆弱性評価、機密データの検出と分類、コンプライアンス対応を支援するセキュリティ管理機能を提供します。

特筆ポイント

1. きめ細かなアクセス制御

   Azure SQL Databaseでは、ユーザーやデータ項目ごとにアクセス権限を階層的に設定できる階層型アクセス制御を提供しています。これにより、特定の行や列単位でのアクセス制御が可能です。

   また、Azure Active Directory (AAD)との統合により、シングルサインオンや条件付きアクセスポリシー、多要素認証、IP制限といった高度なアクセス管理機能を実現します。

2. リスク分析や脅威検知の自動化

   Microsoft Defender for SQL （SQL脆弱性評価やAdvanced Threat Protection）を活用することで、データベース環境の脆弱性診断、機密データの分類、脅威の検知およびアラートの自動化が可能です。これにより、セキュアなデータベース運用を効果的かつ継続的に実現します。

Google Cloud：ベストプラクティスの概要・特筆ポイント

概要

Google Cloudのデータベースセキュリティベストプラクティスは、データベースを保護し、データの盗難や消失を防ぐための一連の推奨事項を提供します。これには、環境の設計からアクセス制御、データの保持と暗号化、災害復旧計画まで、さまざまなセキュリティ対策が含まれます。データベースのセキュリティは最初のレコードが格納される前から始まっています。

特筆ポイント

1. Cloud SQL Proxy

   Cloud SQL Proxyは、Google Cloud SQLのデータベースに接続する際のセキュリティを強化するツールです。これにより、データベース接続時にSSL/TLSによる暗号化が自動的に適用され、認証情報の管理も簡素化されます。アプリケーションから直接接続情報を取得せず、環境変数を使って接続するため、セキュリティが向上し、不正アクセスを防ぐことができます。また、IPホワイトリストなどを設定しなくても、接続元が認証されるため、データベースのセキュリティリスクを減らすことができます。

2. Security Command Center

   Security Command Center（SCC）は、Google Cloudのセキュリティ管理ツールで、クラウドリソースのセキュリティ状態を可視化・監視し、脆弱性や設定ミスを検出します。リスクを早期に発見し、コンプライアンスチェックやアラート通知、対応の自動化が可能です。

セキュリティベストプラクティスのサマリ

セキュリティ要求分類、DB内部不正対策ガイドライン/JPCERT ランサムウエア対策特設サイトの指針とのマッピング

分類	1. アクセス制御				2.暗号化	3.構成・設定、運用管理			4.監視、ログ、監査				5.システムの冗長化、バックアップ		その他	
DB内部不正対策ガイドライン/ JPCERT ランサムウエア対策特設サイト	アクセス制御	認証方式	管理者権限の分掌	N/A	データ暗号化・鍵管理	ポリシーの策定と適用	ソフトウェアを最新化	N/A	定期監査の実施	不正な通信の監視/通知	監査ログの保全	N/A	定期的なバックアップ	N/A	DB周辺機器の管理	N/A
AWS	IAM	IAM,AWS Management Console, AWS RDS	–	VPC	AWS RDS	–	–	AWS Security Hub	–	–	–	AWS Security Hub	AWS Backup	–	–	
OCI	IAM, VCN, Compartments	IAM, Oracle Identity Cloud Service	IAM, Database Vault	VCN, Security Zones	TDE, Oracle Key Vault, Data Safe	Data Safe, Database Security Assessment Tool,Security Zones	–	–	Data Safe, OCI logging	AVDF, OCI Flow Logs	Data Safe , AVDF, Oracle Logging	Cloud Guard	Automatic Backups, ZRCV	Oracle Data Guard, Full Stack Disaster Recovery	–	Maximum Security Architecture
Azure	Private Link Service Endpoints	Microsoft Entra ID, Azure Key Vault, Azure RBAC, Azure Security Center	–	Azure Virtual Network, Azure Firewall	Azure SQL Database, Azure Key Vault	SQL VA, Microsoft Defender for Cloud, Microsoft Defender for SQL	–	–	SQL Database Auditing	Advanced Threat Protection		Always Encrypted	Azure SQL Database, Azure Geo-replication Azure Backup	Azure Storage	–	–
Google Cloud	VPC	Cloud KMS,IAM	–	VPC	Cloud KMS, Cloud SQL	Security Command Center	Cloud Monitoring	–	Cloud Logging	Cloud Logging, Security Command Center	Cloud SQL, IAM	–	–	–	–	Cloud SQL

注意：機能としては存在しているが、ベストプラクティスに記載されていない場合もある

3.まとめ

まとめ

クラウドでデータベースを利用する時ならではのリスクがある

- 従来の境界型防御ではなく、データベースでのセキュリティ対策の重要性が高まっている
- 設定も簡単だけど、設定ミスが起きる可能性が高い

ベストプラクティスは各ベンダーから必要な情報は提供されている

- 各ベンダーごとに特徴があるので、それをおさえることも肝要
- クラウドならではのセキュリティ機能・ツールを活用を検討

クラウドで注意するべきは運用開始した後の対応

- クラウドサービスは刻々と変わっていくため、セキュリティ構成確認の重要性が増している
- 脅威検知や設定ミスのチェック機能の活用を検討する