セキュリティと運用

セキュリティの確保

データ保護

ELB・EBS・S3・RDS・KMS

権限管理

IAM・MFA

インフラ保護

VPC

検出制御

CloudWatch・CloudTrail・AWSGuaedDuty・AmazonInspector

データ保護：暗号化

多くのDBサービスはKMSと統合されている暗号化を容易にできる

CloudHSM（ハードウェア専用モジュール）

暗号化方式

S3

サーバサイド暗号化 ：SSE

クライアントサイド暗号化：KMS

RDS

セキュリティグループでアクセス制御

SSL/TLSで通信暗号化

リソースの暗号化

権限管理

AWS Directory Service

IAMと連携して使っていく

ユーザ認証を実現する

実現機能：  
 運用効率の向上

コンプライアンス向上

セキュリティ強化

Amazon Cognito

SNS認証を実現

SAML

インフラの保護

VPCを使って範囲を決めていく

アクセス制御：セキュリティグループ・NWACL

検出制御

CloudTrail ：AWSユーザの行動ログを取得

CloudWatch ：リソースやアプリケーションのメトリクスを収集・追跡

AWS GuardDuty ：脅威検出サービス

Amazon Inspector ：自動でセキュリティ評価を実施するサービス

AWS WAF ：WebAplicationFirewall

AWS Shield ：DDoS攻撃に対応

IAM Access Analyzer ：外部エンティティと共有されているリソースへの

不正アクセスを特定

AWS Security Hub ：セキュリティアラートを一元的に管理

　現在のセキュリティ状態を把握できる

コスト最適化

主要サービス

需要と供給の一致

AutoScaling

コスト効率の高いリソース

EC2インスタンスの購入方式

TrustedAdvisor（コスト最適化のアドバイスを受けられる）

支出の認識

CloudWatch

見積ツール

継続した最適化

AWS最新情報を追う

TrustedAdovisor

AWSの料金改定

頻繁に料金表を確認していく

<https://aws.amazon.com/jp/pricing/>

EC2の購入オプション

オンデマンドインスタンス

スポットインスタンス

リザーブドインスタンス

ハードウェア専有インスタンス

Dedicated　Host

Bare Metal

AWS Organizationsで一括請求するとボリュームディスカウント適用できる

リザーブドインスタンスを他のアカウントと共有

SavingPlan：一定の使用量の上限を守ることでコスト最適化する

72%節約可能

AWS公式ツールでの見積ツール

簡易見積ツール ：AWSサービスに対する月額料金

TCO計算ツール ：別サービスとの比較

PricingCalculator ：ニーズに沿った個別の細かい見積もりができる

コスト可視化

CloudWatchのBilling機能：

請求額に対するアラーム設定を行う

TrustedAdovisor

コスト最適化

セキュリティ

耐障害性

パフォーマンス向上　をアドバイスしてくれる

運用上の優秀性

コード化された運用実行

ビジネス目的に沿った運用手順

定期的かつ小規模で増加的な変更管理

予期せぬイベントへの対応テストの実施

モニタリングにより障害を予測する

運用上の失敗やイベントから学習する

運用手順を繰り返しアップデートする

準備

CloudFormation

Codeシリーズ

RunbookPlaybook（運用手順のドキュメント）

運用

SystemManager

ServiceCatalog

CloudTrail

AWS Artifact

AWS GuardDuty

など