AWS Black Belt Online Seminar

AWS Secrets Manager

サービスカットシリーズ

押川令（Ray Oshikawa）

Solutions Architect
2023/08

自己紹介

名前：押川令（おしかわ　れい）

所属：パブリックセクター技術統括本部

　　自治体担当　ソリューションアーキテクト

好きなAWSサービス：AWS Secrets Manager

本セミナーの対象者とゴール

本セミナーの対象者

- AWS 環境におけるデータベース認証情報や API キーなどのシークレット管理に関心をお持ちの方
- これから AWS Secrets Manager をご利用予定の方や、理解を深めたい方

本セミナーのゴール

- AWS Secrets Manager の機能と、どのようにセキュリティ要件を満たすように構築されているかを理解していただき、安心して AWS 上のシークレットを管理していただくことができるようになること

アジェンダ

1. シークレット管理の必要性
2. AWS Secrets Manager 概要
3. AWS Secrets Manager の機能詳細
4. AWS Secrets Manager の仕組みとセキュリティ
5. ベストプラクティス
6. 料金
7. まとめ

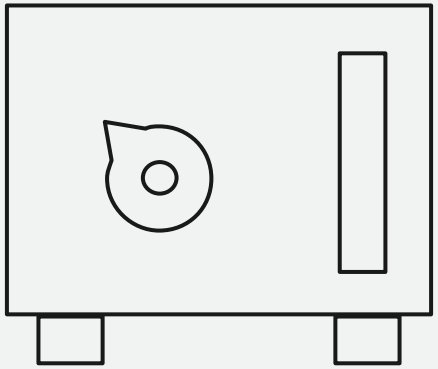
シークレット管理の必要性

ITシステムを支えるシークレット

システムの中にはさまざまなシークレット情報が存在

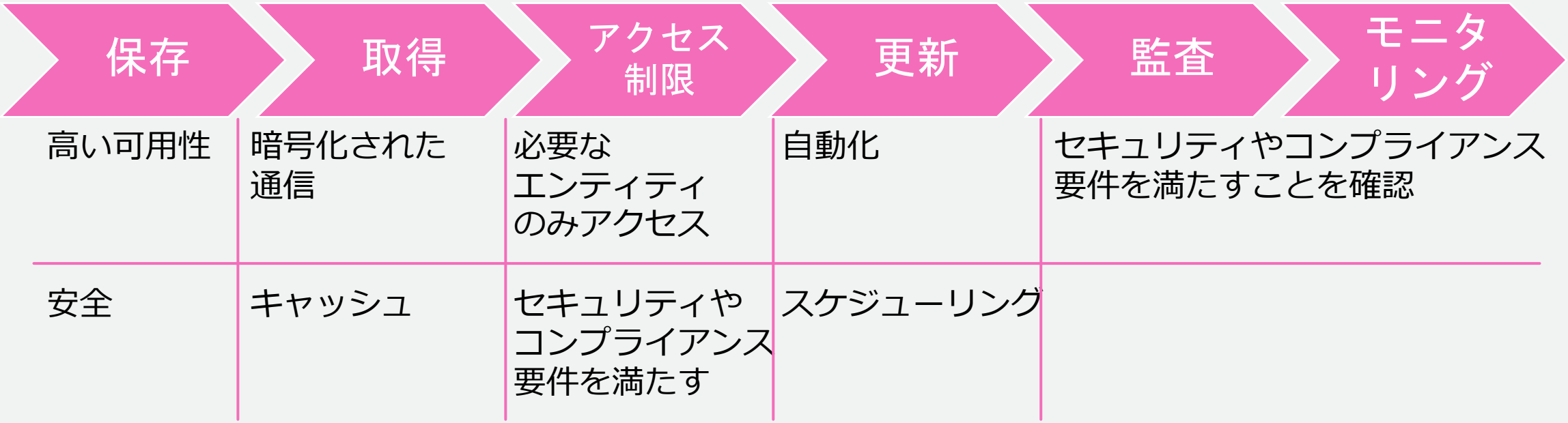
主なシークレット情報の例：

- データベース認証情報
- オンプレミスリソース認証情報
- SaaS アプリケーション認証情報
- サードパーティー API キー
- SSH の秘密鍵



シークレット管理とは

シークレット情報（パスワード、データベース認証情報、API キー等）
について、以下のライフサイクルを一元的に管理



適切なシークレット管理における課題の例

- 安全なストレージの用意
- 災害時にシークレットのデータが消えてしまう可能性
- プログラムから簡単に利用できるような整備
- シークレット情報へのアクセスの適切な制御
- 要件に合致したローテーションが煩雑
- 利用状況のモニタリングと監査の運用コスト

AWS Secrets Manager の機能

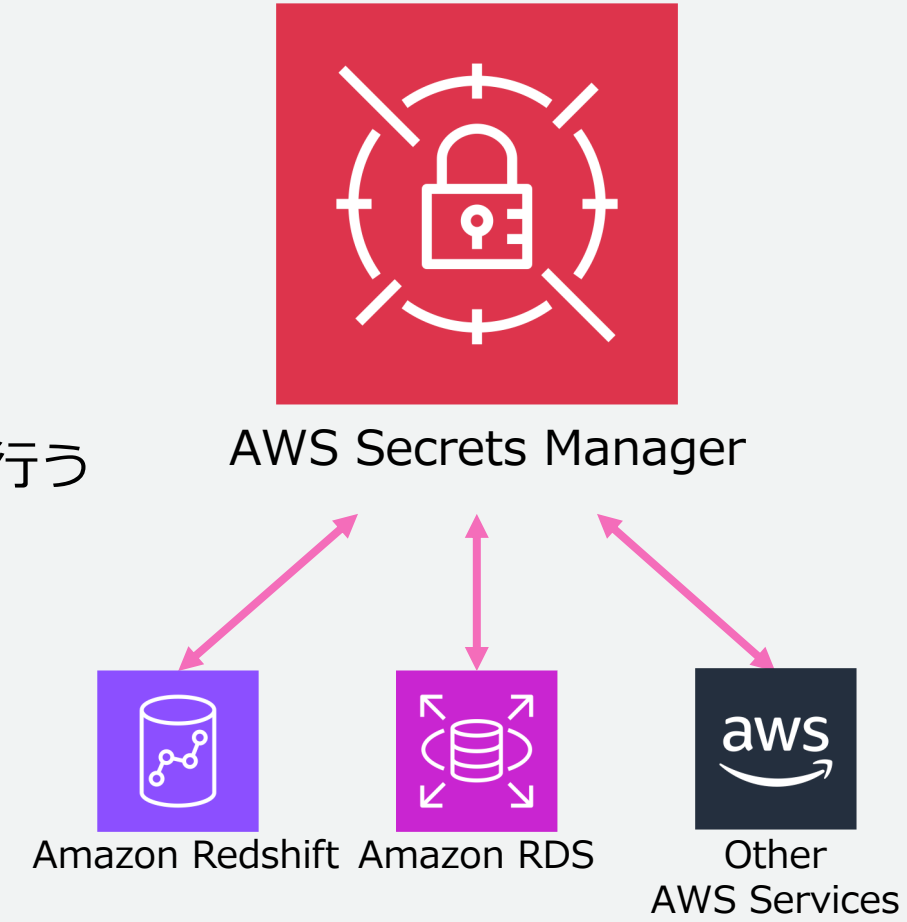
- 暗号化された安全なストレージに保管
- 別リージョンへの自動レプリケーション
- AWS SDK などのライブラリと統合されており、プログラムから簡単に利用可能
- AWS Identity and Access Management (IAM) を用いたシークレット情報へのアクセス制御
- 手動・自動ローテーションが可能、プログラムの書き換えは不要
- AWS CloudTrail などによる利用状況のモニタリングと監査

AWS Secrets Manager 概要

AWS Secrets Manager 概要

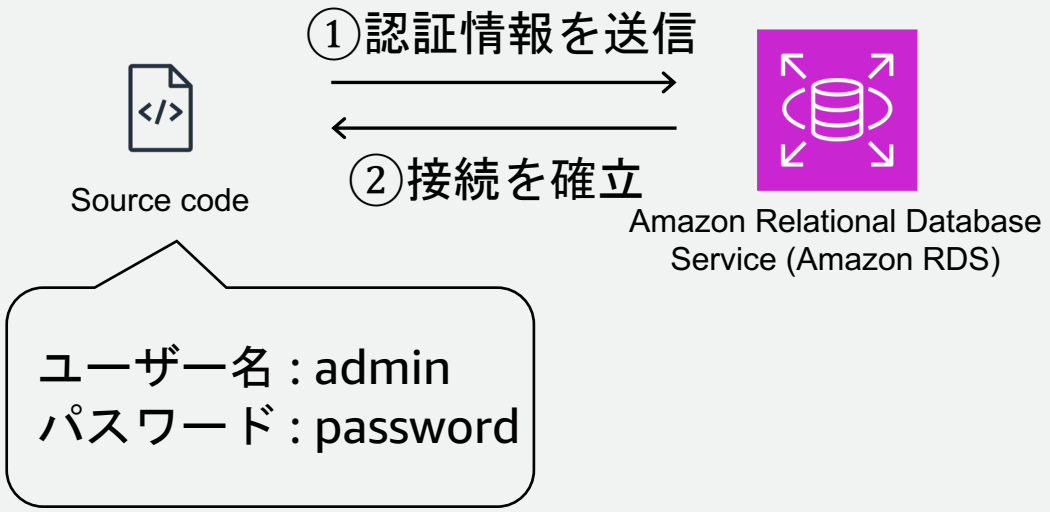
シークレットのライフサイクルを一元的に管理

保存、取得、更新、 アクセス制限、 監査、モニタリングを行う

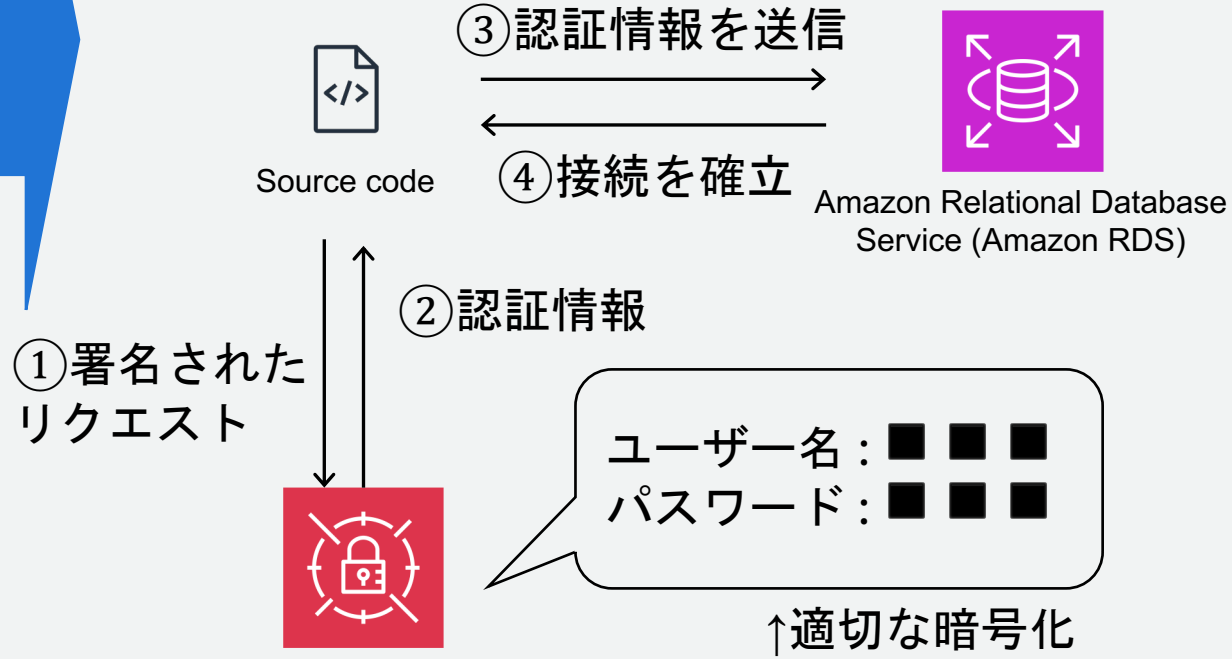


AWS Secrets Manager 利用方法

ソースコード上のハードコーディング
されたシークレット（危険）

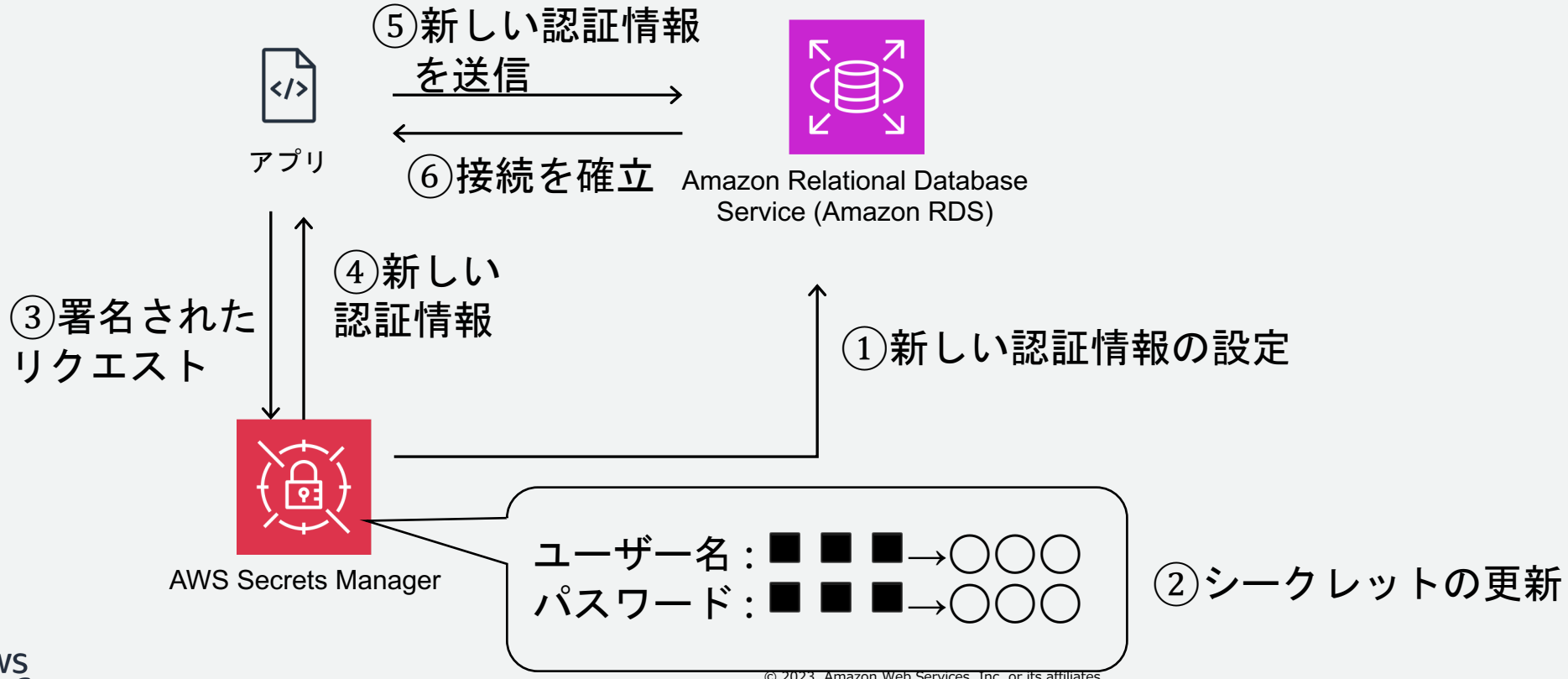


AWS Secrets Manager サービスへの
ランタイム呼び出しに置き換え



ローテーションとは

シークレットを定期的に更新する
目的：万が一シークレットが漏洩した際に、盗まれた情報が長期間悪用される
　　ことを防ぐため



AWS Secrets Manager の機能詳細

アクセス方法

AWS マネジメントコンソール

コマンドラインツール (AWS CLI)

AWS SDK：C++, Java, PHP, Python, Ruby,
.NET, Node.js, Go

HTTPS クエリ API：AWS Secrets Manager の
エンドポイントに接続
リクエストへの署名やレスポンスの
変換を実装する必要あり

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/asm_access.html

AWS Secrets Manager エンドポイント

プログラムからのアクセスの際に接続

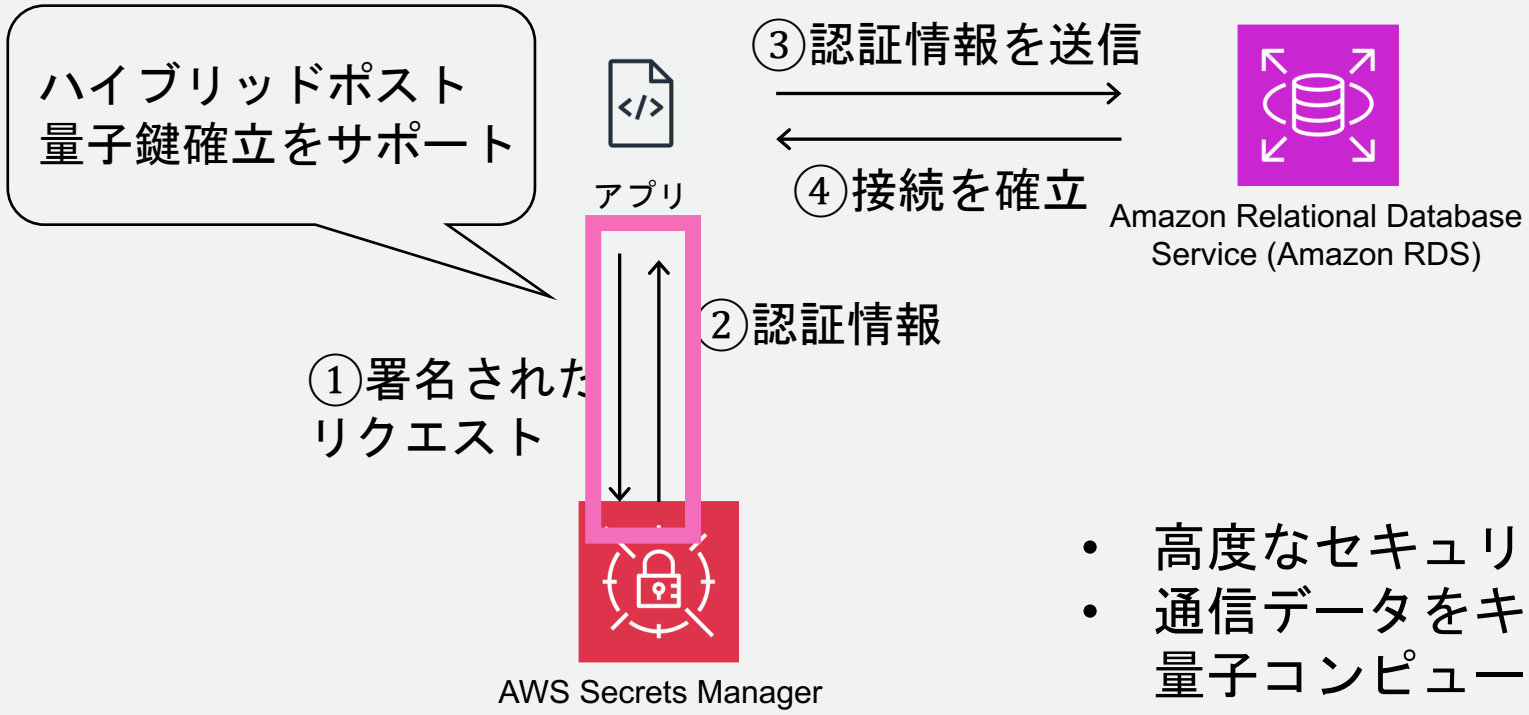
接続できるクライアントの条件

- TLS 1.2 以上をサポート
- Perfect Forward Secrecy（PFS） を使用した暗号スイートに対応
- リクエストに アクセスキー または AWS Security Token Service (AWS STS) で署名できること

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/endpoints.html

ハイブリットポスト量子 TLS もサポート（2022/08-）

AWS Secrets Manager API エンドポイントに接続するときに使用可能



- 高度なセキュリティを必要としている組織向け
- 通信データをキャプチャしておいて、将来に量子コンピュータで解読をする攻撃への対策

https://aws.amazon.com/jp/about-aws/whats-new/2022/08/aws-secrets-manager-connections-support-hybrid-post-quantum-tls-kyber/

保存・取得に関する機能

AWS Secrets Manager への保存と取得

マネジメントコンソール, AWS CLI, AWS SDK からシークレットを取得・保存

プログラム言語・サービス	シークレットの取得方法
Java	AWS Secrets Manager SQL 接続ドライバー キャッシュコンポーネント AWS SDK の直接呼び出し
Python, .NET, Go	キャッシュコンポーネント AWS SDK の直接呼び出し
JavaScript, PHP, Ruby	AWS SDK の直接呼び出し
Amazon ECS や AWS Lambda	統合機能により直接的にシークレットを参照

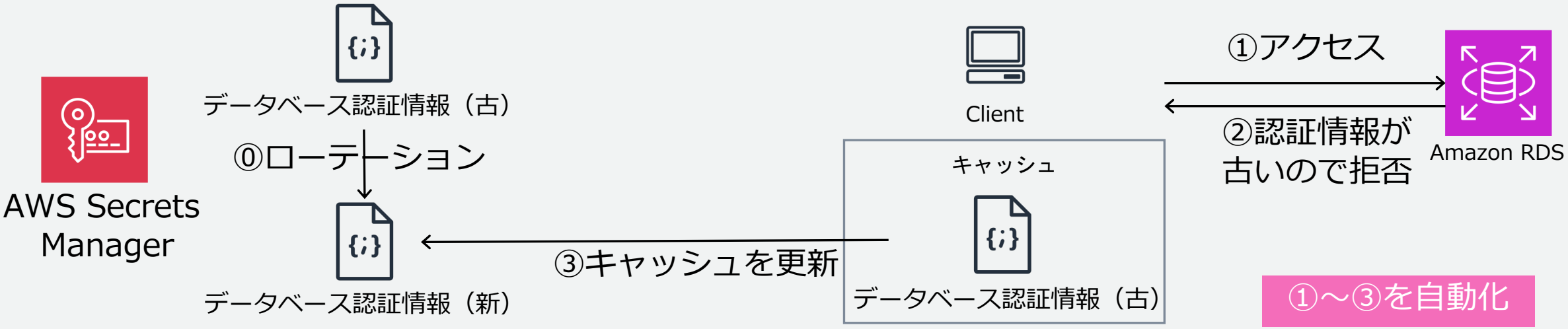
JDBC ドライバーを利用したシークレットの取得

シークレットの ID を指定すると、

シークレットの取得からデータベースの接続までを管理

キャッシュライブラリを使用して認証情報をキャッシュ

指定した時間ごと、およびローテーションされた時にキャッシュを更新



①～③を自動化

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/retrieving-secrets_jdbc.html

アクセス制限に関する機能

AWS Secrets Manager での保管時のアクセス制限

AWS Key Management Service (KMS) を介した暗号化

暗号化に使用する KMS キー	アクセス許可設定
AWS マネージドキー aws/secretsmanager	必要なアクセス許可が自動的に割り当て済
カスタマー KMS キー	AWS Secrets Manager から その KMS キーを利用できるようにアクセス許可を割り当てる

AWS Secrets Manager へのアクセス

リソースベースのポリシーをサポート→IP制限などが可能

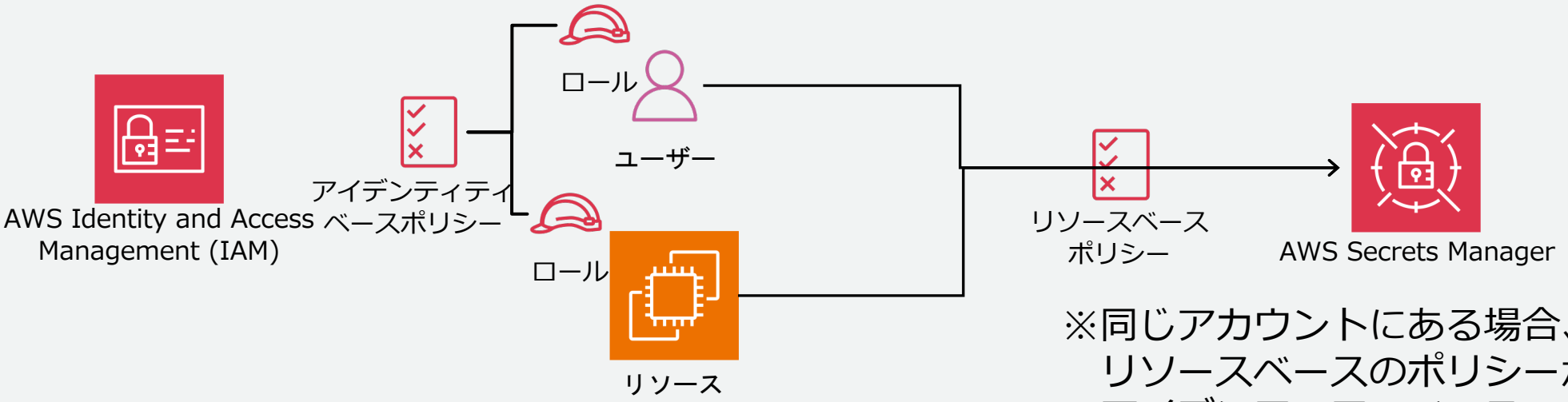
VPCエンドポイントに対応

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/auth-and-access.html

認証とアクセスコントロール

AWS Identity and Access Management（IAM）を使用して
アクセスを保護

リソースベースのポリシーも設定可能



※同じアカウントにある場合、
リソースベースのポリシーか
アイデンティティベースの
ポリシーのどちらかで許可されていれば
アクセスできます

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

シークレット管理に必要なアクセス権限設定

シークレットを管理するユーザーに必要なアクセス権限

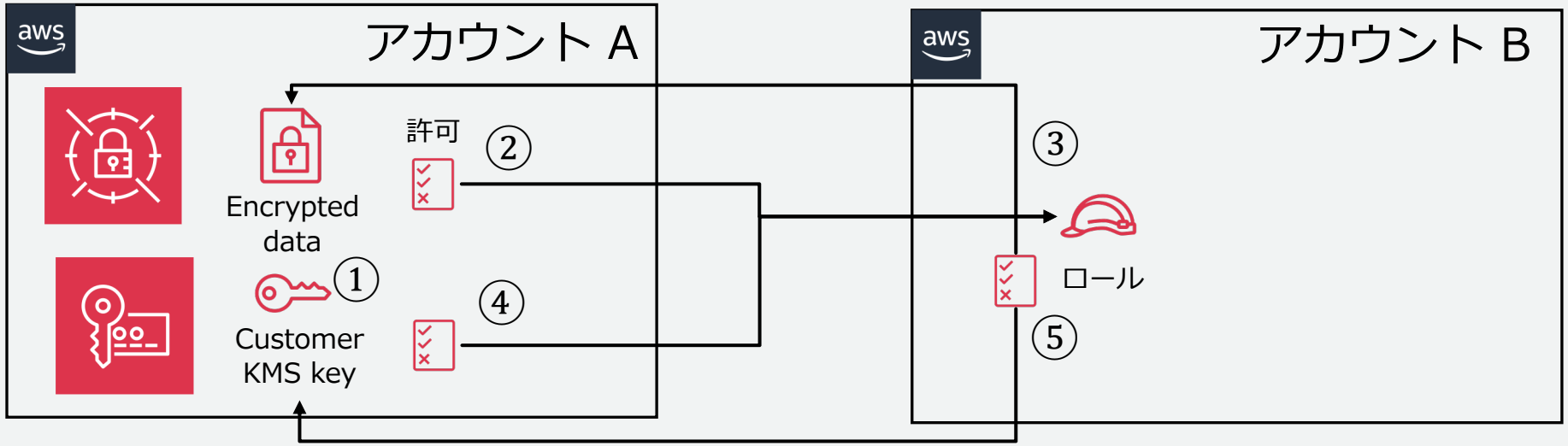
- SecretsManagerReadWrite
- （ローテーションを有効にする場合） IAMFullAccess
  - 留意点：エンドユーザーにはこの権限を付与しない

ローテーションに用いる Lambda 関数に必要なアクセス権限

- シークレットへのアクセス権限・データベースなどサービスへのアクセス権限
- 利用している KMS カスタマーキーへのアクセス権限
- 交代ユーザーローテーションの場合はスーパーユーザーの認証情報を保管しているシークレットへのアクセス権限

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/auth-and-access.html

クロスアカウントアクセス



①マネージドキー aws/secretsmanager の使用不可、 カスタマー KMS キーを作成
②シークレットのリソースベースポリシーでアカウント B のロールからのアクセスを許可
③アカウント B のロールに付与するアイデンティティベースポリシーでシークレットへのアクセスを許可
④暗号化に使用している KMS キーのリソースベースポリシーで アカウント B のロールからのアクセスを許可
⑤アカウント B のロールに付与するアイデンティティベースのポリシーで KMS キーへのアクセスを許可

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/auth-and-access_examples_cross.html

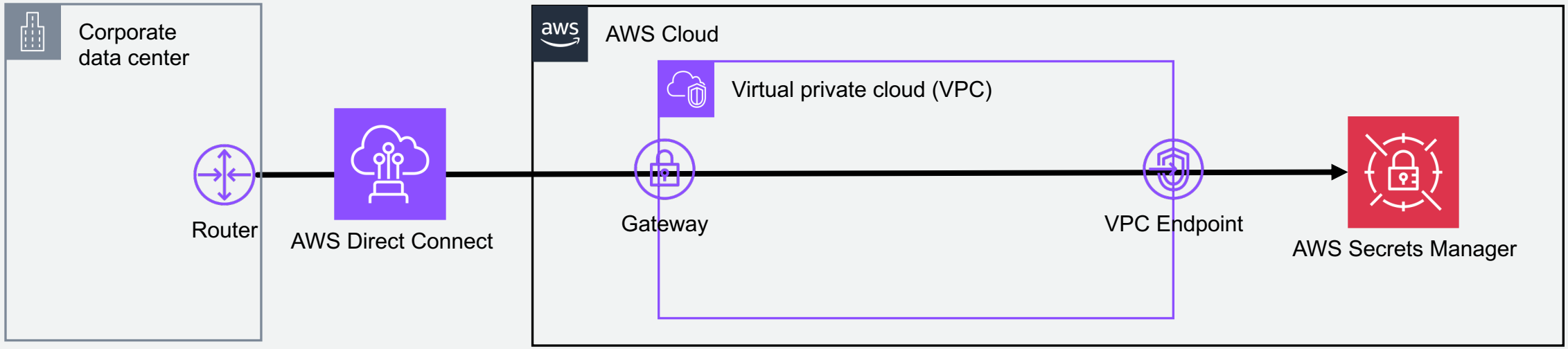
VPC エンドポイント

インターフェイス型のエンドポイントを作成可能

パブリックインターネットからアクセスできないプライベートネットワーク上で通信

インターネット上にトラフィックが出ない形でシークレットを管理

リソースポリシーに条件を含めることで、エンドポイント越しのアクセスのみに制限可能



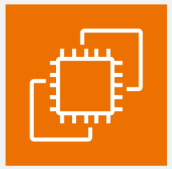
https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/vpc-endpoint-overview.html

更新に関する機能

AWS Secrets Manager によるローテーション

Amazon RDS, Amazon Aurora,
Amazon Redshift, Amazon DocumentDB の場合

その他の認証情報の場合



Amazon Elastic Compute Cloud (Amazon EC2)

⑤新しい認証情報を送信

⑥接続を確立

Amazon Relational Database Service (Amazon RDS)

AWS Lambda

③署名されたリクエスト

④新しい認証情報

AWS Secrets Manager

①新しい認証情報の設定

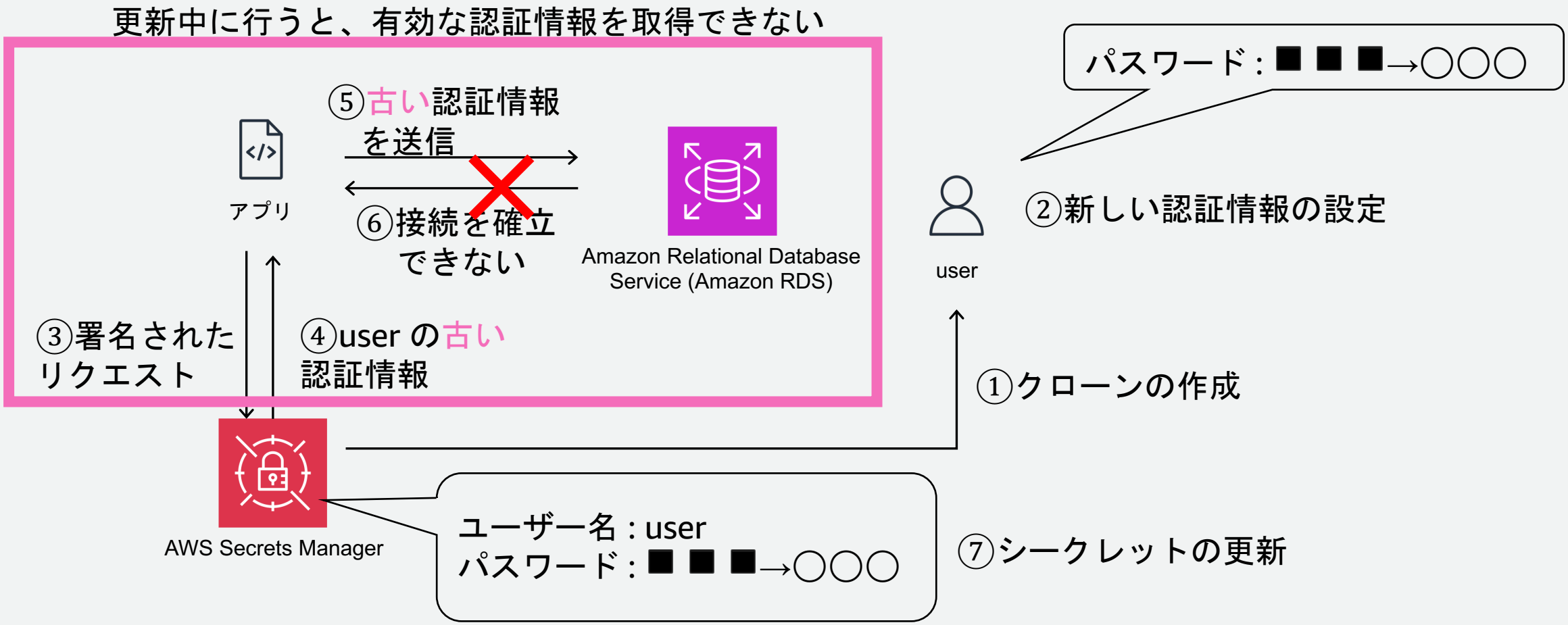
サービス内での認証情報を更新し
その内容を AWS Secrets Manager に
反映するような Lambda 関数

ユーザー名：■ ■ ■→○○○
パスワード：■ ■ ■→○○○

②シークレットの更新

シングルユーザー戦略

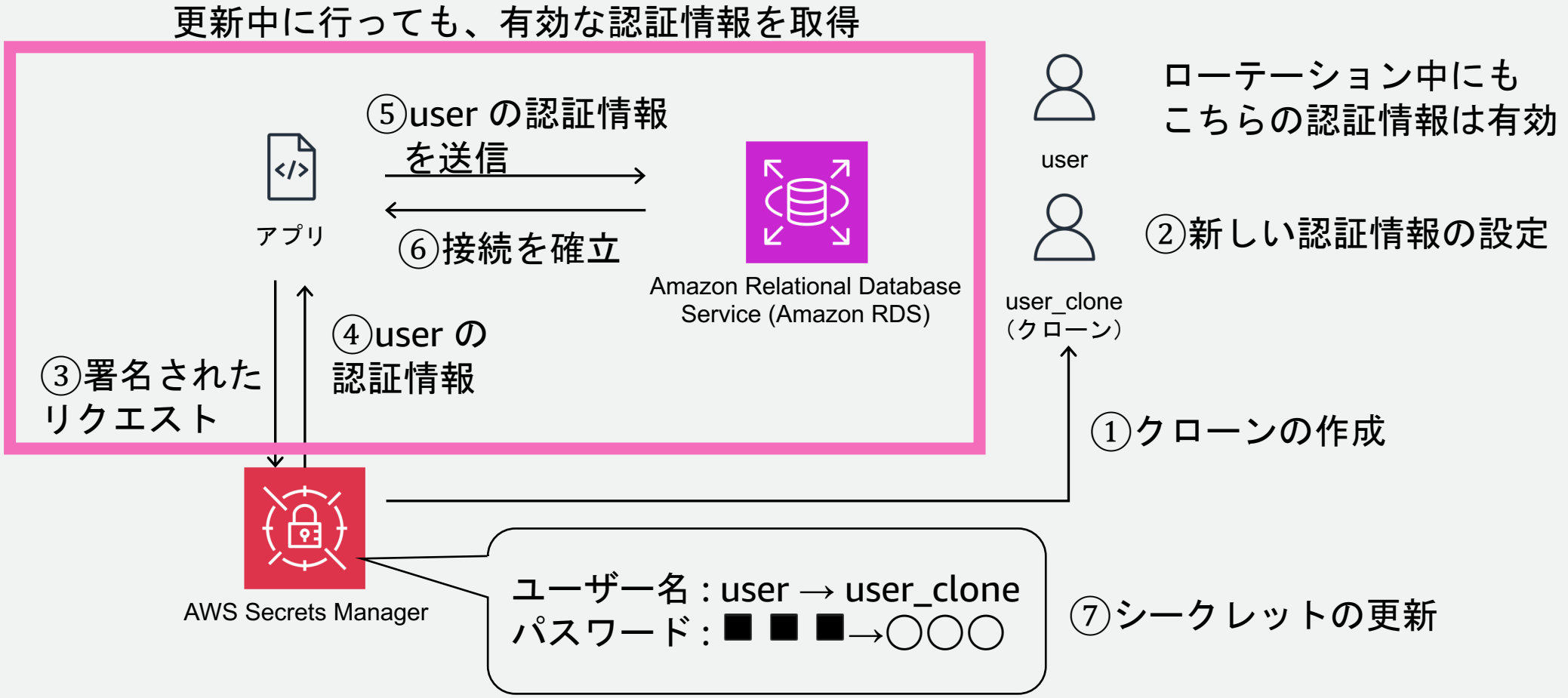
1 つのシークレット内で 1 人のユーザーの認証情報を更新



https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-db.html

交代ユーザー戦略

1 つのシークレット内で 2 人のユーザーの認証情報を交互に更新



https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-db.html

シークレットの自動ローテーションにおける戦略

	シングルユーザー戦略	交代ユーザー戦略
認証情報の更新	1 つのシークレット内で 1 人のユーザーの認証情報を更新	2 人のユーザーの認証情報を交互に更新
ローテーション中の認証情報の取得	データベースのパスワードが変更されてからシークレットの更新までにラグがある 既存のデータベース接続は切断されない	ローテーション中にシークレットを取得しても、引き続き有効な認証情報を取得
必要な権限	自身のパスワードを更新する権限が必要	クローン作成権限のある認証情報が必要 （別のシークレット内で用意）
使用パターン	アドホックユーザーまたは インタラクティブユーザーの認証情報	高可用性を必要とするアプリケーション

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-db.html

バージョン管理

シークレットの値を変更したりローテーションしたりすると
新しいバージョンを作成し、以下のラベルを張り替えることで管理

AWSPREVIOUS - ひとつ前のバージョン

AWSPENDING - ローテーション中のバージョン

AWSCURRENT - 現在利用しているバージョン

独自のラベルを含め、最大 20 のステージングラベルをアタッチ可能

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/getting-started.html#term_version

シークレットの削除

- シークレットの削除をスケジューリングすると、すぐにアクセス不能に
  - 最短で 7 日間の指定した復旧期間の間、復旧が可能
- レプリカがある場合はレプリカを先に削除
  - レプリカは即時削除される
- シークレットのバージョンは削除できず、ラベルを削除する
  - バージョンが 100 を超える場合は、 ラベルがついていないかつ24 時間以内に作成されていないものを削除
- Amazon CloudWatch で削除対象へのアクセスをモニタリング可能

監査・モニタリングに関する機能

シークレットの監査とモニタリング – 1/2

AWS CloudTrail：利用証跡の記録

AWS Secrets Manager の全ての API 呼び出しをイベントとして記録

Amazon EventBridge：メール送信などのアクションを実行

イベントからアクションを起こすことができる

Amazon CloudWatch：メトリクスの監視

アカウントのシークレット数を監視できる

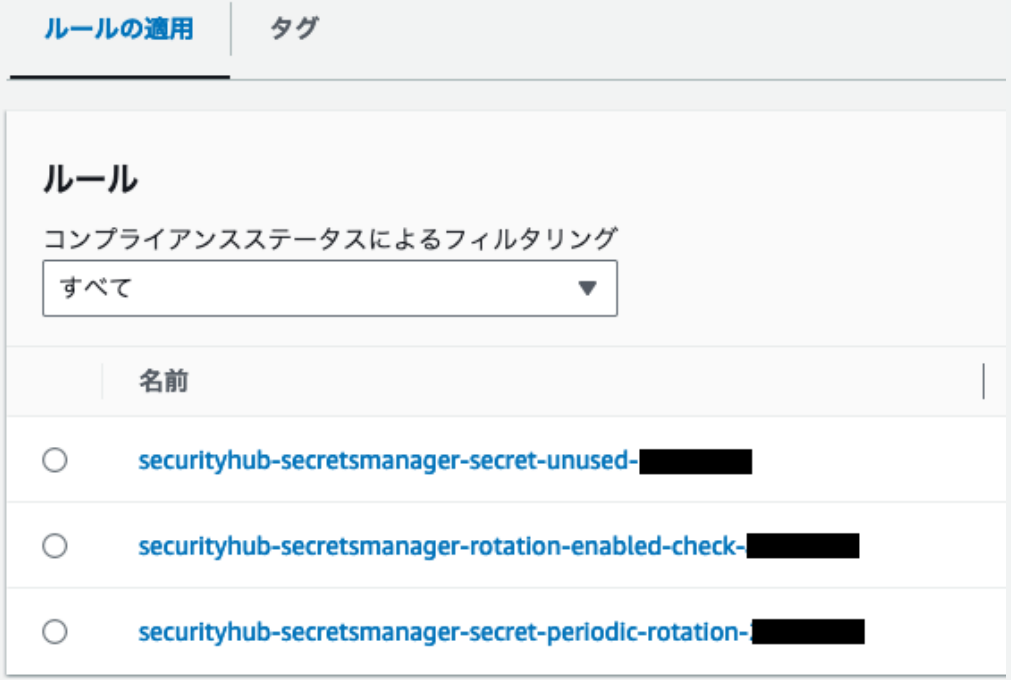
AWS CloudTrail のログファイルを受信し、状況に応じてアラームを作成

例）削除がスケジュールされたシークレットへのアクセスを検知

シークレットの監査とモニタリング – 2/2

AWS Config：意図しない設定の防止

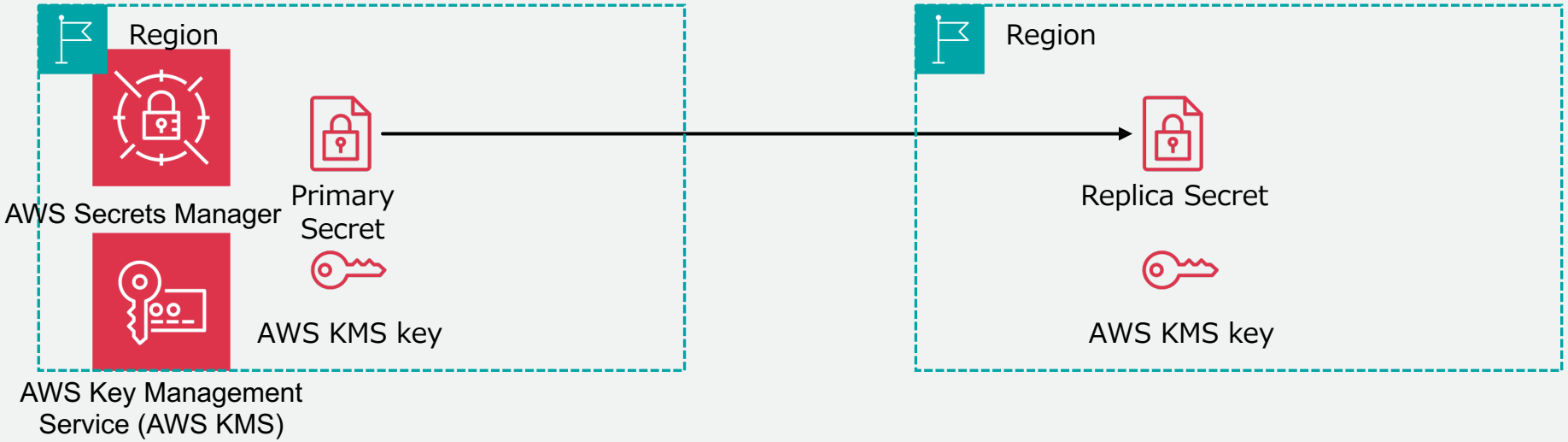
AWS Secrets Manager に関するルールを設定し、ルールに準拠していないシークレットを特定することができる



その他の機能

シークレットのレプリケーション

他のリージョンからアクセスできるようになる
レプリカ先の KMS キーで暗号化できる



プライマリをローテーションすると全てのレプリカに反映される
（プライマリシークレットと別に更新することはできない）

災害時などに、レプリカをスタンドアロンに昇格できる

他の AWS サービスとのマネージドな統合 – 1/3

Amazon Elastic Container Service (Amazon ECS)

- Amazon ECS
  - コンテナの定義で参照可能
  - コンテナ内で環境変数をクエリすることでシークレットの内容を取得

他の AWS サービスとのマネージドな統合 – 2/3


AWS Lambda

- AWS Lambda
  - “AWS Parameters and Secrets Lambda Extension” を利用して、SDK を使用せずにシークレットを取得してキャッシュ可能（関数にレイヤーを追加する必要あり）


AWS CloudFormation

- AWS CloudFormation
  - シークレットを取得して他のリソースで利用可能
  - AWS Secrets Manager によりシークレットを作成し、DB の認証情報に利用可能

```
Resources:
  RDSDBCluster:
    Type: 'AWS::RDS::DBCluster'
    Properties:
      MasterUserPassword: '{{resolve:secretsmanager:[secret-id]:SecretString:[key]}}'
```

他の AWS サービスとのマネージドな統合 -3/3

以下のサービスについても連携可能です。（2023年8月時点）

Alexa for Business
App Runner
AWS App2Container
AWS AppConfig
Amazon AppFlow
AWS AppSync
Amazon Athena
AWS CodeBuild
Amazon CodeGuru Reviewer
AWS DataSync
Amazon DataZone
AWS Direct Connect
AWS Directory Service
Amazon DocumentDB
AWS Elastic Beanstalk
Amazon Elastic Container Service
Amazon ElastiCache
AWS Elemental Live
AWS Elemental MediaConnect
AWS Elemental MediaConvert
AWS Elemental MediaPackage
AWS Elemental MediaTailor
Amazon EMR
Amazon EventBridge
Amazon FSx
AWS Glue DataBrew
AWS Glue Studio
AWS IoT SiteWise
Amazon Kendra
Amazon Kinesis Video Streams
AWS Launch Wizard
Amazon Lookout for Metrics
Amazon Managed Grafana
AWS Managed Services
Amazon Managed Streaming for Apache Kafka
Amazon Managed Workflows for Apache Airflow
AWS Migration Hub
AWS Panorama
AWS ParallelCluster
AWS OpsWorks for Chef Automate
Amazon QuickSight
Amazon RDS
Amazon Redshift
Amazon Redshift クエリエディタ v2
Amazon SageMaker
AWS SCT
AWS Toolkit for JetBrains
AWS Transfer Family
AWS Wickr

詳しくはこちら：https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/integrating.html

AWS Systems Manager パラメーターストアとの違い

ライフサイクル管理を備えたシークレット専用のストアが欲しい場合、
AWS Secrets Manager を使う

	AWS Secrets Manager	パラメータストア
KMS による暗号化	できる	できる
値を取得できるレート	10,000/秒	10,000/秒 （スループットを設定で上げた場合※）
ライフサイクル管理 （ローテーションなど）	サポート	自分で行う必要がある
料金	有料	無料

※リージョンによっては KMS のスループット制限に制限される場合があります

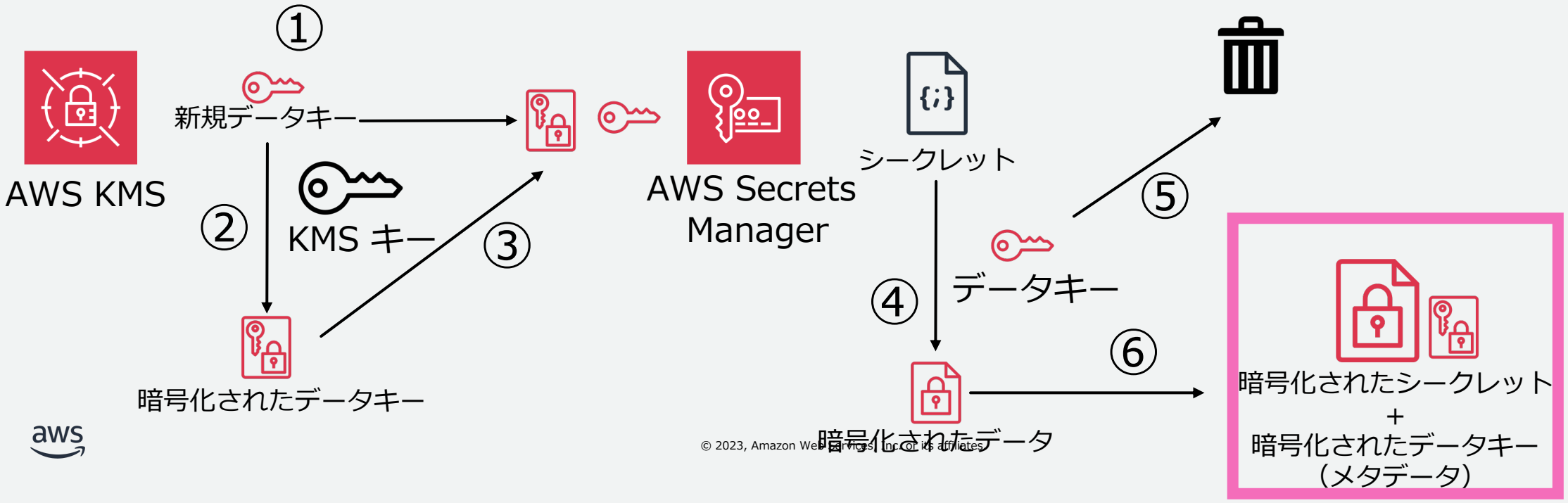
https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/reference_limits.html
https://docs.aws.amazon.com/ja_jp/general/latest/gr/ssm.html https://aws.amazon.com/jp/systems-manager/faq/

AWS Secrets Manager の仕組みとセキュリティ

AWS Secrets Manager での保存時のセキュリティ

AWS KMS を介した暗号化

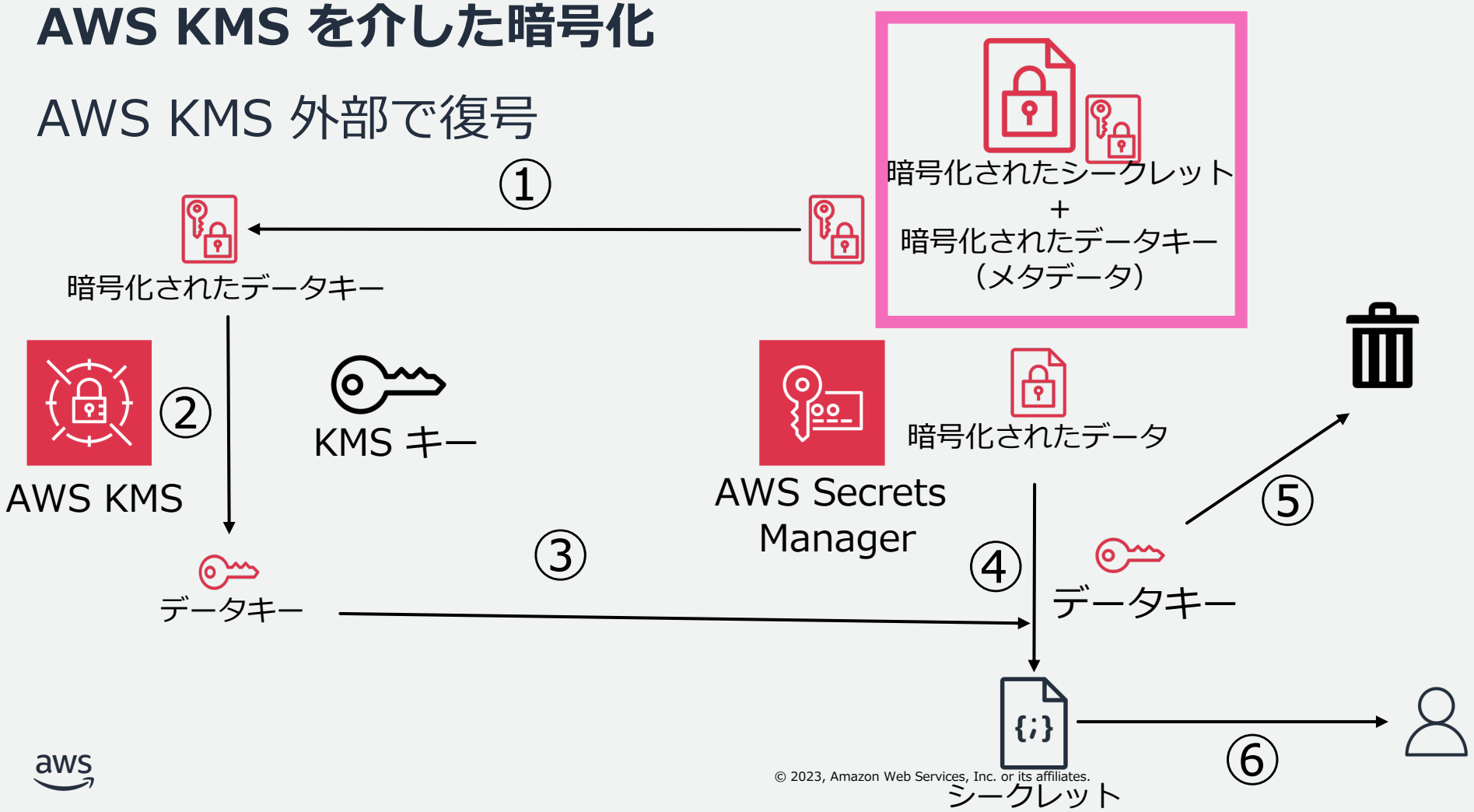
新しいバージョンを暗号化するごとに KMS キーから新しいデータキーを生成しエンベロープ暗号化



AWS Secrets Manager での取得時のセキュリティ

AWS KMS を介した暗号化

AWS KMS 外部で復号



暗号化コンテキスト

AWS KMS では、メタデータである暗号化コンテキストの一部または全部を渡さないと復号できないような設定にできる

AWS Secrets Manager から AWS KMS に渡す暗号化コンテキスト：

- SecretArn：シークレットの ARN （Amazon リソースネーム）
- SecretVersionId：バージョンID

ベストプラクティス

セキュリティのベストプラクティス

- 各アカウントのルートユーザーで多要素認証（MFA）を使用する
- SSL/TLS を用いて 保存・取得・ローテーションなどの際の通信を行う
  - TLS 1.3 をお勧め
- タグや名前フィールドは暗号化されないため、機密情報をタグや名前フィールドに入力しない
- Amazon CodeGuru Security によりハードコードされたシークレットを発見し、AWS Secrets Manager に追加

運用のベストプラクティス

- 複数のリージョンからアクセスするシークレットはレプリケーション
- AWS Config を利用して、構成の変更管理を行う
- AWS CloudTrail を利用して、すべての API コールを記録する
- Amazon EventBridge でを利用して、シークレットの削除や削除されるシークレットに対するアクセスに関して、アラートを発報する

暗号化 のベストプラクティス

- AWS Secrets Manager で利用する KMS キーへのアクセスは、AWS Secrets Manager からに限定する
  - KMS キーのキーポリシーに kms:ViaService を設定
- AWS KMS で 暗号化コンテキストペアのキーと値が一致していないと復号できない設定にする
  - IAM やキーポリシー、Grantを設定する

https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/secrets-manager.html

料金

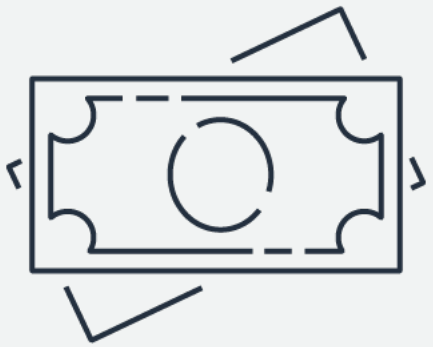
料金（東京リージョン）

- シークレットあたり月 0.40 USD
  - 保管期間が1ヶ月に満たない場合は 1 時間単位で料金計算
  - レプリカのシークレットにも独立に月 0.40 USD 課金
  - 削除対象としてマークされたシークレットに対しては料金は発生しない
- 10,000 API コールにつき 0.05 USD

- 最初のシークレットを保管してから 30 日間は無料使用期間

料金における注意事項

- 料金は保存するシークレットの数と、使用する API コールの数に基づき、最低料金等は設定されていない
- AWS Secrets Manager が作成した AWS マネージドキー aws/secretsmanager は、無料で作成・保管される（API リクエストには別途課金）
- ローテーション関数は、別途 Lambda レートで課金



まとめ

まとめ

AWS Secrets Manager は、シークレットのライフサイクルを一元的に管理するマネージドサービス

保存、取得、更新、 アクセス制限、 監査、モニタリングを行う

- AWS Key Management Service（AWS KMS) を利用した安全な暗号鍵の保存と取得
- 自動ローテーション機能
- AWS IAM を利用したアクセス制限
- さまざまな AWS サービスと統合された監査とモニタリング

参考資料

- AWS Secrets Manager サービスページ

https://aws.amazon.com/jp/secrets-manager/

- AWS Secrets Manager ユーザーガイド

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/userguide/intro.html

- AWS Secrets Manager API Reference

https://docs.aws.amazon.com/ja_jp/secretsmanager/latest/apireference/Welcome.html

- AWS Prescriptive Guidance

https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/secrets-manager.html

- AWS Secrets Manager 料金ページ

https://aws.amazon.com/jp/secrets-manager/pricing/

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (https://aws.amazon.com/) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- 技術的な内容に関しましては、有料の AWS サポート窓口へお問い合わせください
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください (マネジメントコンソールへのログインが必要です)

Thank you!