

重要データを保護するための アーキテクチャとアプローチ

河井 信彦

技術統括本部 ソリューションアーキテクト
Amazon ウェブ サービス ジャパン合同会社

自己紹介

名前：河井信彦

所属：アマゾン ウェブ サービス ジャパン合同会社
西日本担当ソリューションアーキテクト

経歴：前職はセキュリティベンダー

好きな AWS サービス：セキュリティ系サービス全般

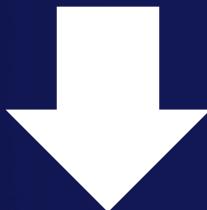


本セッションの対象者

- ・ データの安全性や重要情報の保護に携わるお客様
- ・ クラウド上の重要なデータを強固に保護したいお客様
- ・ セキュリティに関する設定や実装に携わるエンジニアの方

本セッションの目的

- データ保護の必要性を理解する
- AWS のデータ保護関連サービスの概要を理解する
- サンプルアプリケーションを通してデータ保護のアプローチを理解する



データ保護実装の第一歩を踏み出していただく

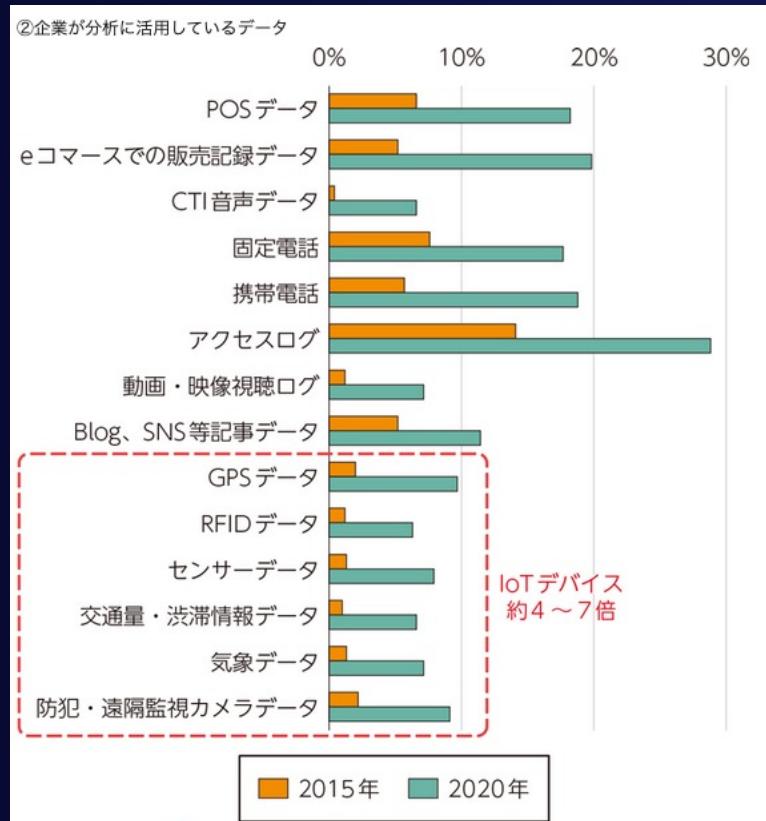
Agenda

1. なぜデータ保護が必要なのか？
2. AWS におけるデータ保護
3. データ分類
4. アクセス制御
5. データの暗号化
6. データ保護のアプローチ
7. まとめ

1. なぜデータ保護が必要なのか

企業が扱うデータ量は増加の一途をたどる

従来と比べ、販売記録や機器・センターなどが取得するログデータ、音声データなどの活用も進んでおり、データ分析による企業経営の高度化の流れがうかがえる



IT 環境における脅威

IPA 「情報セキュリティ10大脅威 2022」より抜粋

順位	組織における脅威	昨年順位
1 位	ランサムウェアによる被害	1 位
2 位	標的型攻撃による機密情報の窃取	2 位
3 位	サプライチェーンの弱点を悪用した攻撃	4 位
4 位	テレワーク等のニューノーマルな働き方を狙った攻撃	3 位
5 位	内部不正による情報漏えい	6 位
6 位	脆弱性対策情報の公開に伴う悪用増加	10 位
7 位	修正プログラムの公開前を狙う攻撃 (ゼロデイ攻撃)	New
8 位	ビジネスメール詐欺による金銭被害	5 位
9 位	予期せぬ IT 基盤の障害に伴う業務停止	7 位
10 位	不注意による情報漏えい等の被害	9 位

組織のデータに対する脅威

データ保護の必要性

- ・組織にとってデータが重要な資産になった
- ・企業や組織が持つデータに対する脅威が大きな影響を及ぼすようになった
- ・GDPR をはじめ各国で個人情報やプライバシー情報を保護する枠組みや法律の重要性が高くなっている

2. AWS におけるデータ保護

AWS のデータ保護への取り組み



プライバシーの管理

データプライバシーを自らコントロールできる



データ利用の管理

データがどのように利用されるかを自らコントロールできる



アクセスの管理

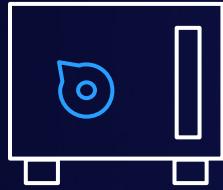
データが誰にアクセスされるかを自らコントロールできる



暗号化の管理

データがどのように暗号化されるかを自らコントロールできる

データ保護がビジネス成果の向上を促進



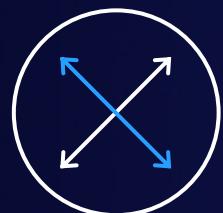
知的財産や企業秘密の保護



顧客情報を保護と信頼の獲得



自動化による時間の
節約とリスク軽減



ビジネスの成長に合わせた
可視性と制御の拡張



AWS サービスとの統合

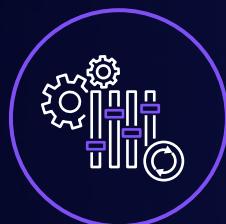


グローバルレベルのセキュリティと
コンプライアンスの管理

様々なシチュエーションのお客様を支援することができる AWS データ保護関連サービス



アクセスとポリシーの適用をきめ細かく制御



自動化と可視性の向上により、運用リスクを軽減



セキュリティ領域のコンサルティングパートナーとの連携

AWS のデータ保護関連サービス

データ分類



Amazon Macie

アクセス制御



AWS Identity and
Access Management
(IAM)

暗号化



AWS Secrets Manager



AWS Key Management
Service (AWS KMS)



AWS CloudHSM

AWS のデータ保護関連サービス

データ分類

アクセス制御

暗号化



AWS Secrets Manager



Amazon Macie



AWS Identity and
Access Management
(IAM)



AWS Key Management
Service (AWS KMS)



AWS CloudHSM

3. データ分類

Amazon Macie



Amazon Macie

機械学習とパターンマッチングを使用して
Amazon Simple Storage Service (Amazon S3) の
利用状況の可視化し、重要情報を検出する
マネージドサービス

- S3 バケットの利用状況とオブジェクトの可視化
- S3 バケット内の機密データや個人情報を含むデータの検出を効率的に実行
- 検出結果の参照と他サービスとの連携
- AWS マネジメントコンソールか単一の API コールを使用して、簡単に利用開始

Amazon Macie - 重要情報の検出例

The screenshot shows the Amazon Macie console interface. On the left, a search results table lists findings across various categories like Credentials, Financial, and Multiple. On the right, a detailed view of a specific finding is shown, highlighting personal information and its context.

検出結果

表示中: 8 / 10 1 1 8

Suppress findings

保存済みフィルタ / 自動アーカイブ 保存済みのフィルタがありません

現在 S3 バケット名: macie-sample-finding-bucket Save rule X
● 重要度: 高 Add filter

検出結果タイプ 影響を受けるリソース 更新日

重要度	検出結果	最終更新日	
High	[サンプル] Sensi...t/Credentials	macie-sample-fin...credentials.json	4 分 前
High	[サンプル] Sensi...ect/Financial	macie-sample-fin...et/financial.txt	4 分 前
High	[サンプル] Sensi...ject/Multiple	macie-sample-fin...spreadsheet.xlsx	4 分 前
High	[サンプル] Polic...redExternally	macie-sample-finding-bucket	4 分 前
High	[サンプル] Sensi...tomIdentifier	macie-sample-fin...employeeInfo.csv	4 分 前
High	[サンプル] Polic...3BucketPublic	macie-sample-finding-bucket	4 分 前
High	[サンプル] Polic...tedExternally	macie-sample-finding-bucket	4 分 前
High	[サンプル] Polic...cessDisabled	macie-sample-finding-bucket	4 分 前

概観

重要度	High
リージョン	ap-northeast-1
アカウント ID	[REDACTED]
資源	macie-sample-finding-bucket/sample_excel_spi
作成日	2022年3月3日, 22:07:35 (3 分 前)
更新日	2022年3月3日, 22:07:35 (3 分 前)

結果

ジョブ ID	5e8ff9bf55ba3508199d22e984129be6 [Q Q]
カスタムデータ識別子	
Employee Id identifier	1 [Q Q]
個人情報	
Name	1 [Q Q]
Phone number	1 [Q Q]
Usa social security number	1 [Q Q]
詳細	
ステータス	COMPLETE [Q Q]
分類されたサイズ	9 KB
MIME タイプ	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
詳細な結果の場所	s3://sample-macie-results-bucket/AWSLogs/71
財務情報	
Credit card number	1 [Q Q]
影響を受けるリソース (S3 バケット)	
バケット名	macie-sample-finding-bucket [Q Q]

オブジェクトに
含まれている
個人情報の一覧

オブジェクトの場所

クレジットカード番号が
検出された数

4. アクセス制御

AWS Identity and Access Management (IAM)

AWS リソースをセキュアに操作するために、
認証・認可の仕組みを提供するマネージドサービス



AWS Identity and Access
Management (IAM)

- アクセス権限をユーザー毎に付与
- JSON 形式のドキュメントで詳細に権限を制御
- 一時的な認証トークンを用いた権限の委任
- 他の ID プロバイダーとの連携
- IAM 自体の利用は無料

アイデンティティベースのポリシーと リソースベースのポリシー



アイデンティティベースのポリシーと リソースベースのポリシー

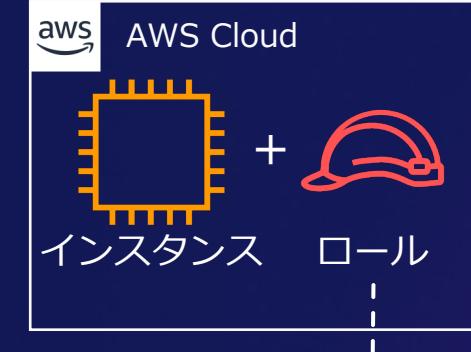


アイデンティティベースの
ポリシー

リソースベースのポリシー

アイデンティティベースのポリシーか
リソースベースのポリシーのどちらかで許可が必要

どちらかのポリシーで明示的に拒否された場合は拒否



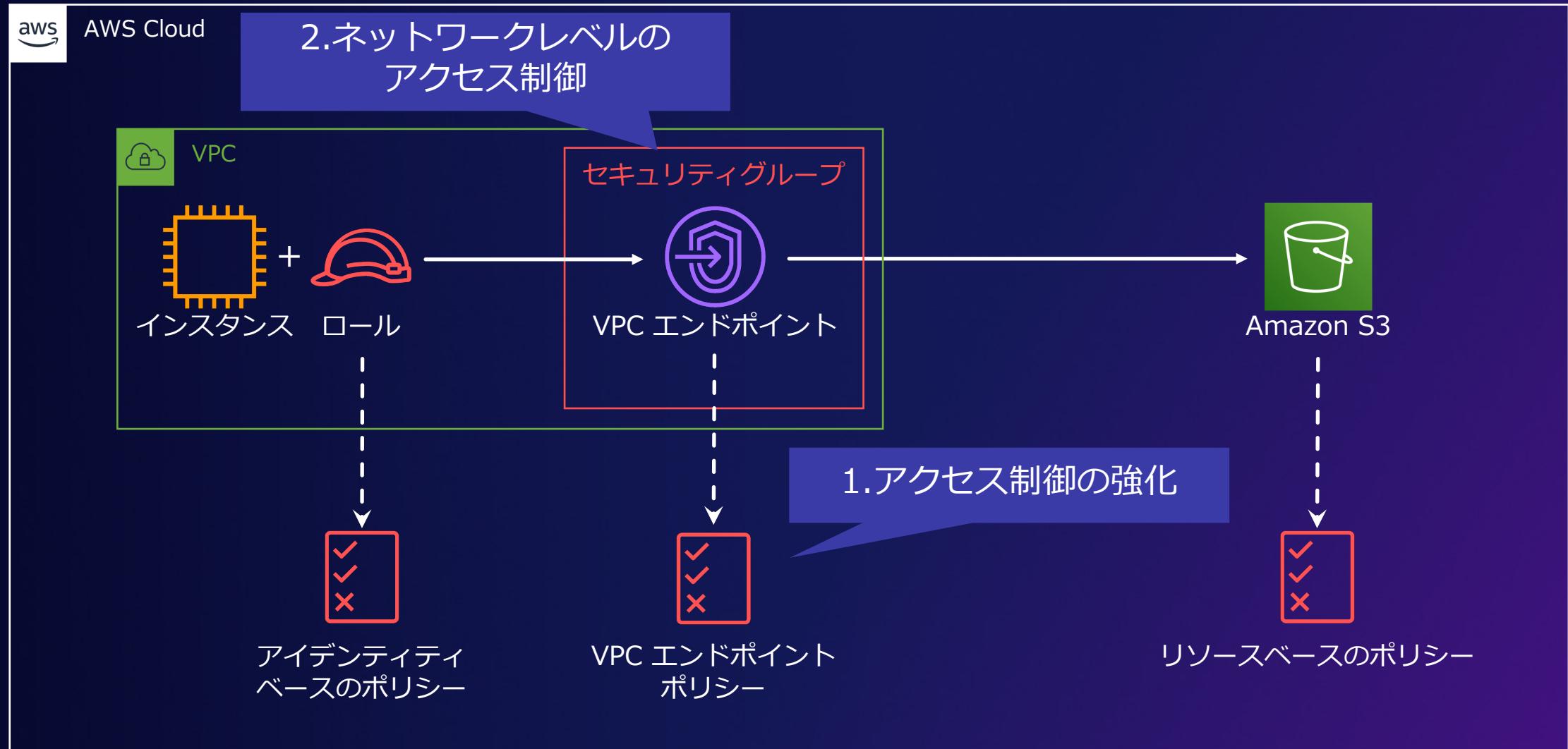
アイデンティティベースの
ポリシー

リソースベースのポリシー

アイデンティティベースのポリシーか
リソースベースのポリシーの両方で許可が必要

どちらかのポリシーで明示的に拒否された場合は拒否

VPC エンドポイントを使った制御



5. データの暗号化

AWS Key Management Service (AWS KMS)

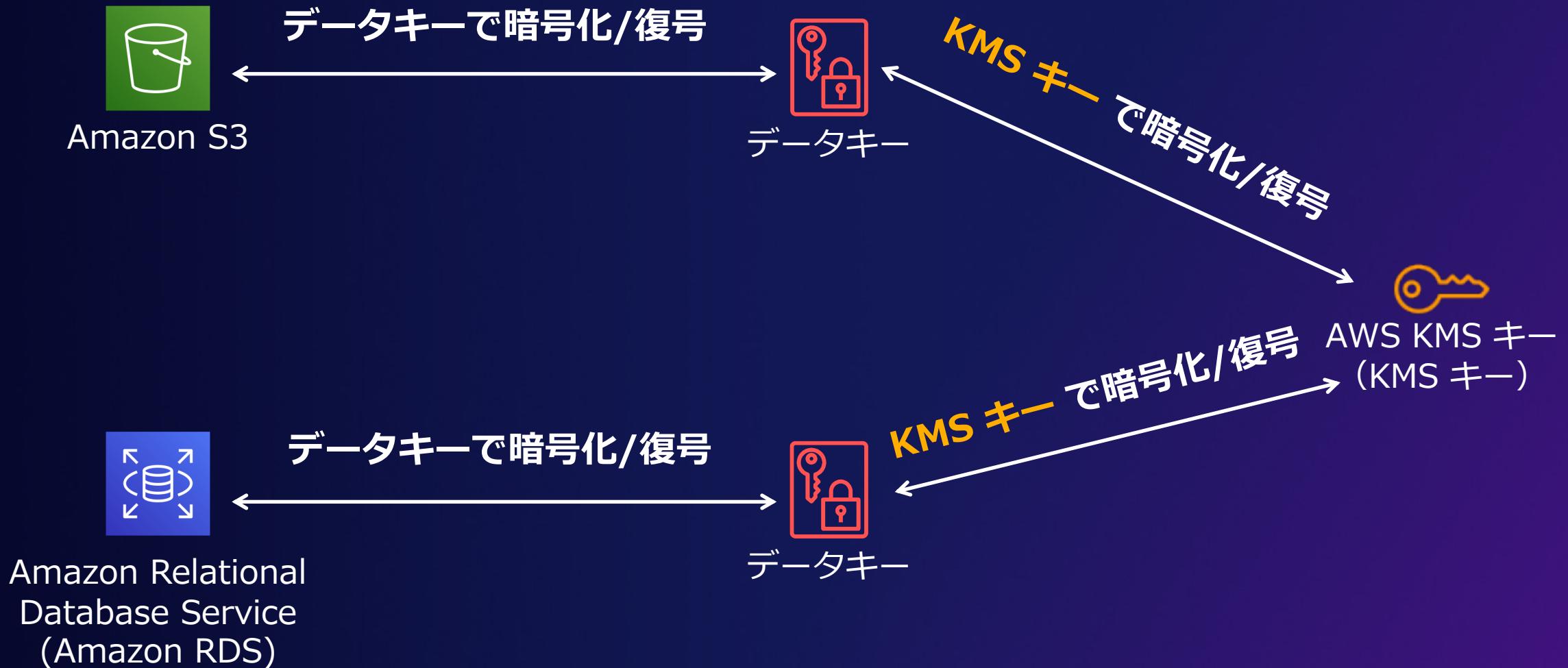


AWS Key Management
Service (AWS KMS)

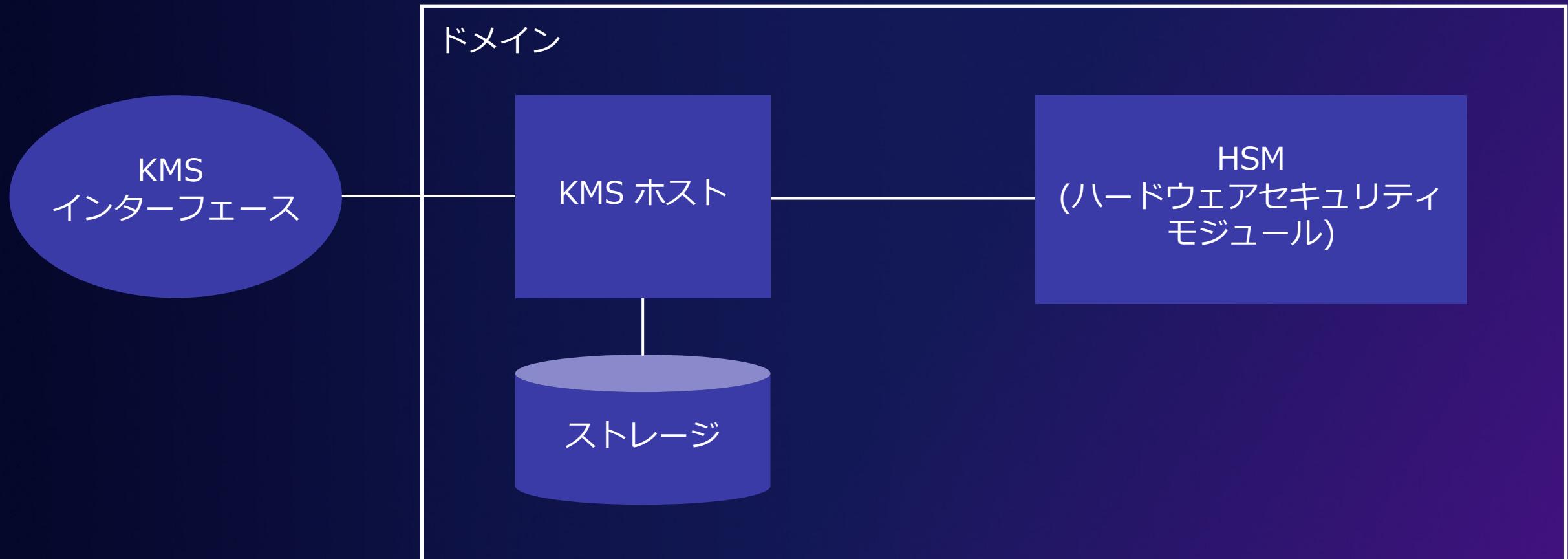
暗号鍵を効率的に作成、管理、運用するための
マネージドサービス

- 可用性、物理的セキュリティ、ハードウェアの管理を AWS が
担当するマネージドサービス
- 暗号鍵を使用するための安全なロケーションを提供
- FIPS 140-2 認証済み暗号化モジュールによって鍵を保護
- AWS でデータを保持するサービスとの連携

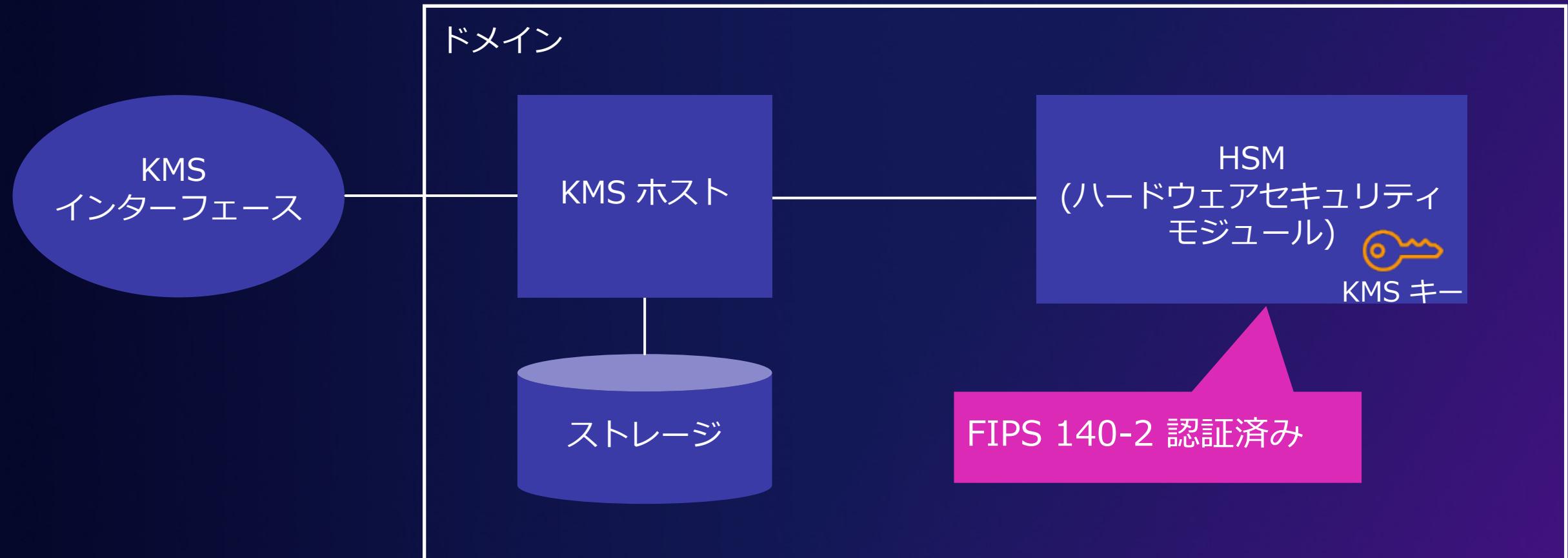
鍵の階層化



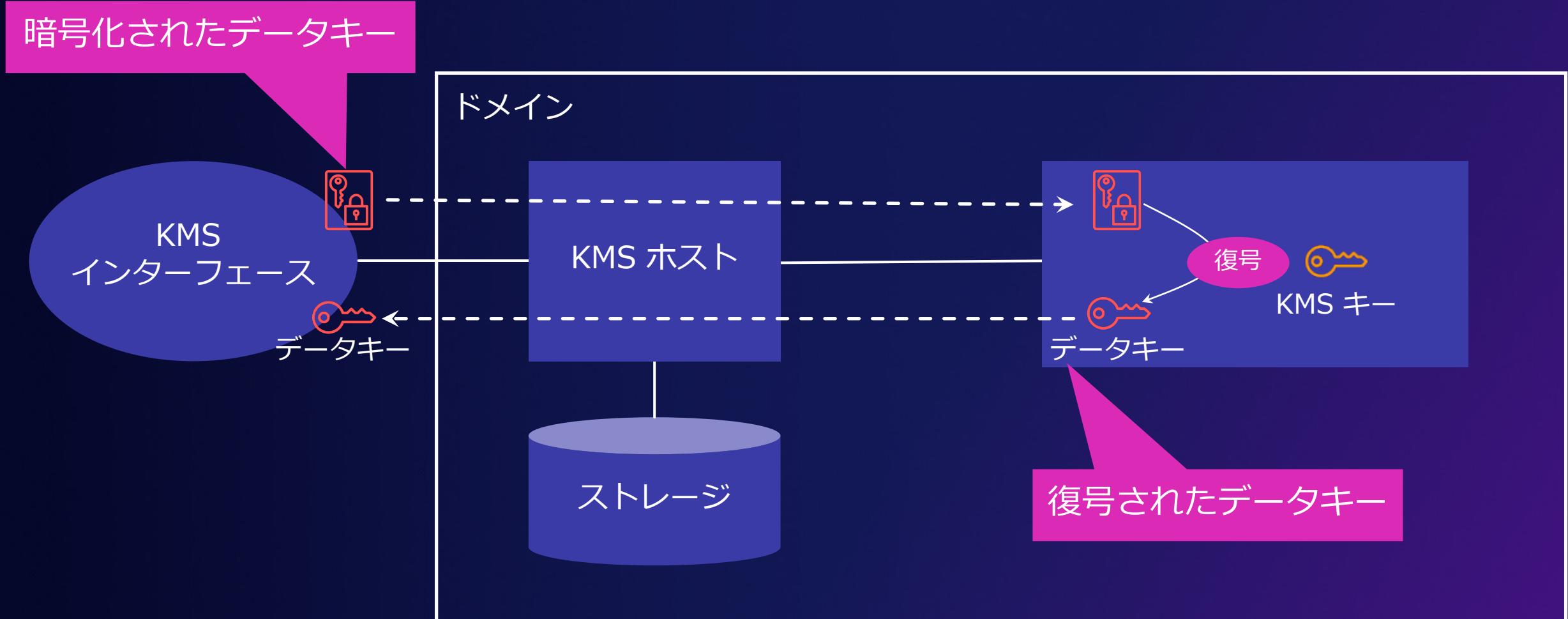
AWS KMS のアーキテクチャ



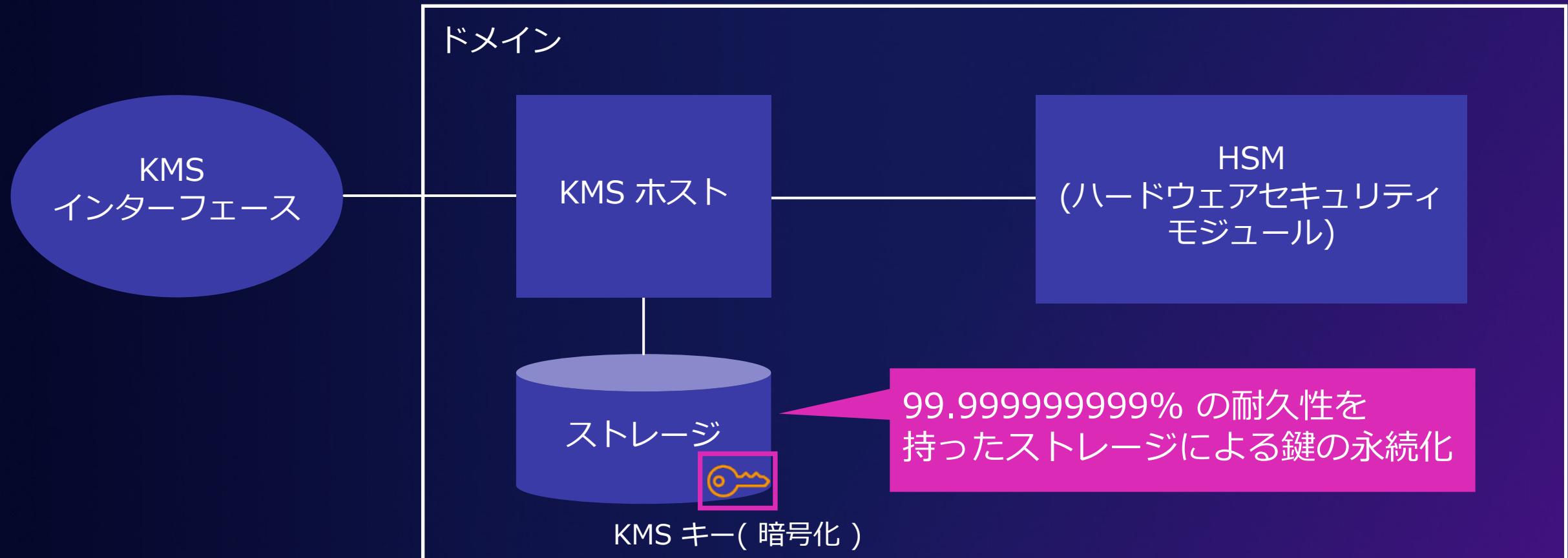
AWS KMS のアーキテクチャ



AWS KMS のアーキテクチャ



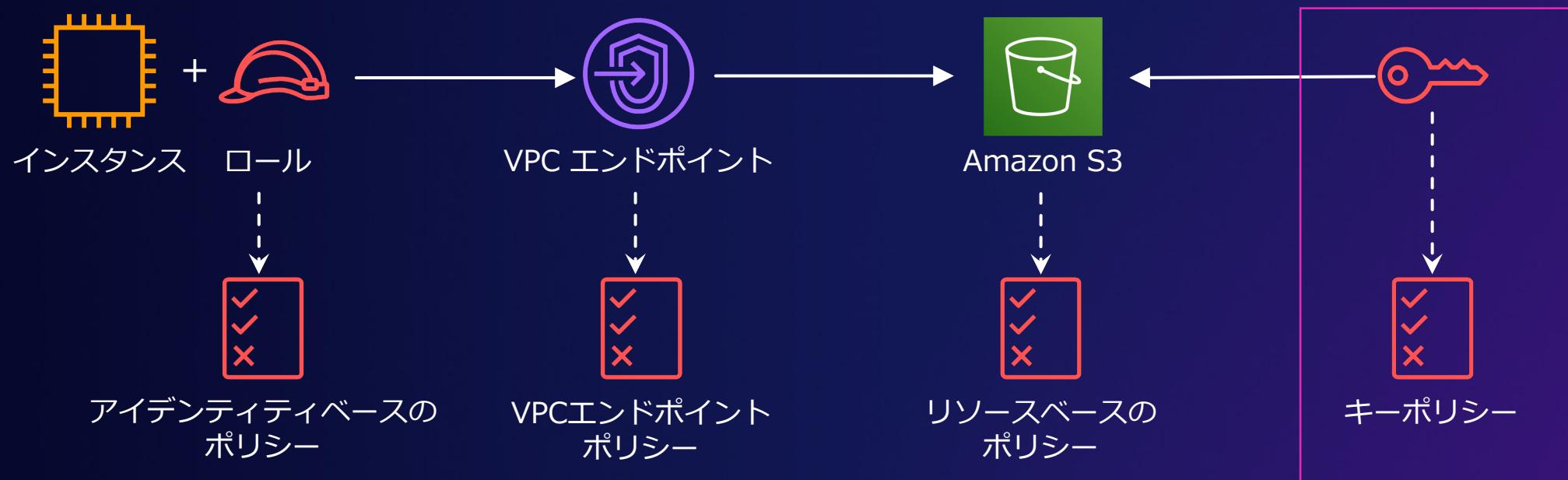
AWS KMS のアーキテクチャ



キー・ポリシー

AWS KMS キーはお客様が管理するキー
キー・ポリシーとは AWS KMS キーへのアクセスを制御するためのポリシー

- 全ての AWS KMS キーには1つのキー・ポリシーが必要
- 各 AWS KMS キーをホストするリージョンのみで有効
- AWS KMS キーの使用を許可するユーザとのその使用方法を JSON 形式で記述



ポリシーの設定例

キー ポリシー

```
{  
  "Version": "2012-10-17",  
  "Id": "key-consolepolicy-2",  
  "Statement": [  
    {  
      "Sid": "Enable IAM policies",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam:: 111122223333 :root"},  
      "Action": "kms:*",  
      "Resource": "*"  
    },  
  ]  
}
```

アイデンティティベースのポリシー

```
{  
  "Sid": "Allow use of the key",  
  "Effect": "Allow",  
  "Action": [  
    "kms:Encrypt",  
    "kms:Decrypt",  
    "kms:ReEncrypt*",  
    "kms:GenerateDataKey*",  
    "kms:DescribeKey"  
  ],  
  "Resource": [  
    "arn:aws:kms:us-west-2:111122223333:key/<Key-ID>",  
    "arn:aws:kms:us-west-2:111122223333:key/<Key-ID>"  
  ],  
}
```

6. データ保護のアプローチ

データ保護のアプローチ

AWS Well-Architected フレームワークのセキュリティ柱ではデータ保護対策として3つのアプローチを紹介しています

アプローチ 1：データ分類

- 重要度と機密性に基づいて組織データをカテゴリ別に分類して、各カテゴリに適した保護と保持方法でデータを管理する

アプローチ 2：保管中のデータの保護

- 暗号化と適切なアクセスコントロールを実装して保管中のデータを保護することで不正アクセスのリスクを軽減する

アプローチ 3：伝送中のデータの保護

- 転送中のデータに適切なレベルの保護を提供することにより、ワークフローのデータの機密性と整合性を守る



データ保護のアプローチ

AWS Well-Architected フレームワークのセキュリティ柱ではデータ保護対策として3つのアプローチを紹介しています

アプローチ 1：データ分類

- 重要度と機密性に基づいて組織データをカテゴリ別に分類して、各カテゴリに適した保護と保持方法でデータを管理する

アプローチ 2：保管中のデータの保護

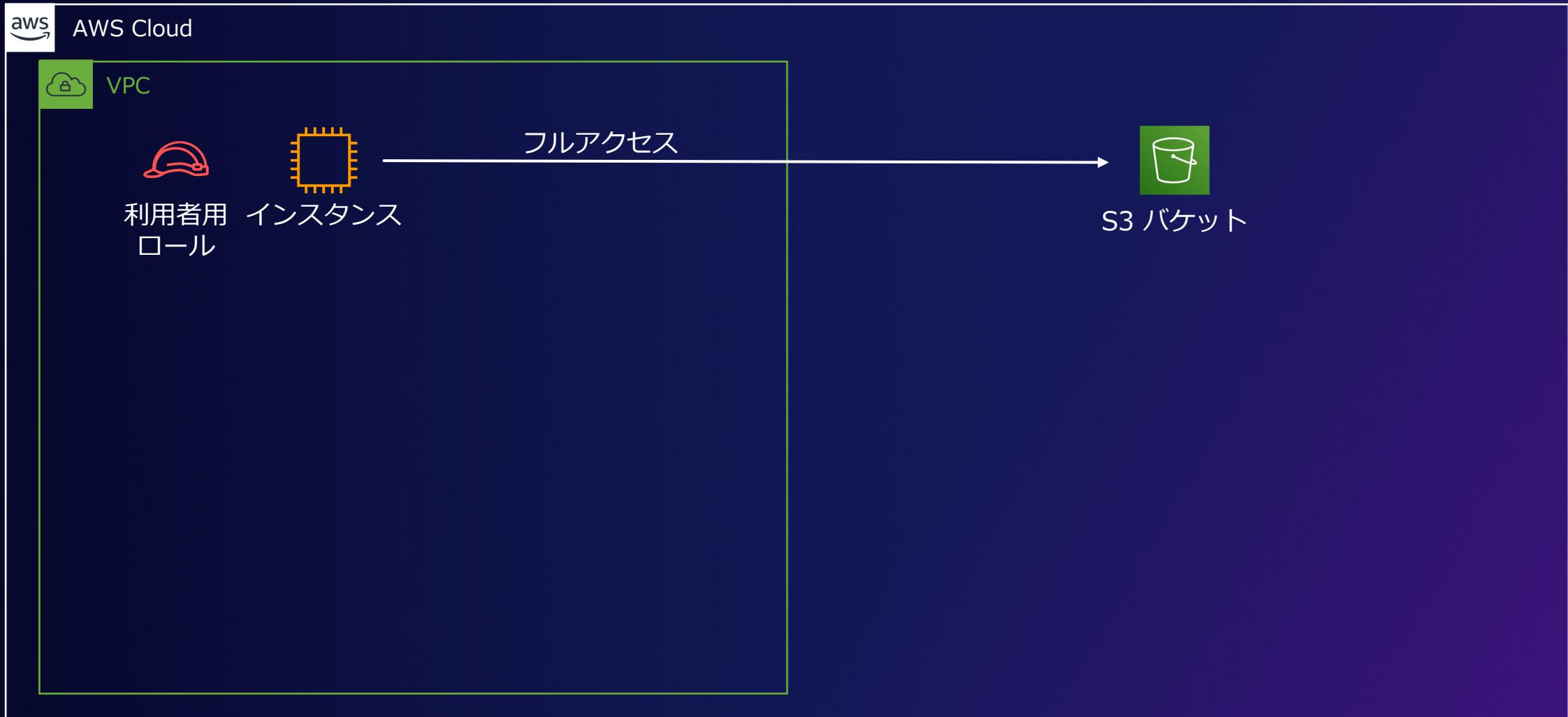
- 暗号化と適切なアクセスコントロールを実装して保管中のデータを保護することで不正アクセスのリスクを軽減する

アプローチ 3：伝送中のデータの保護

- 転送中のデータに適切なレベルの保護を提供することにより、ワークフローのデータの機密性と整合性を守る



初期構成



アプローチ 1：データ分類

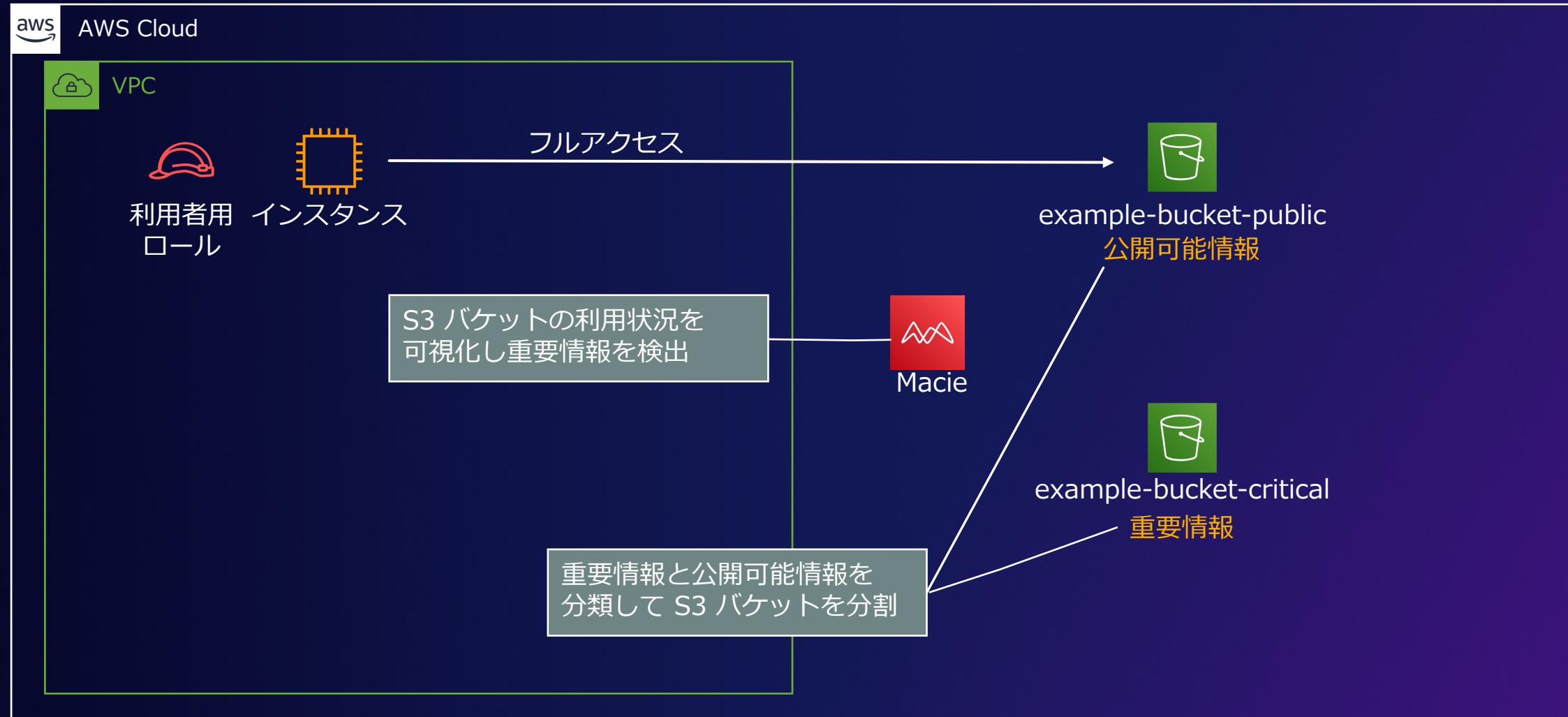
データ分類

アプローチ 1：データ分類

➤ 重要度と機密性に基づいて組織データをカテゴリ別に分類して、各カテゴリに適した保護と保持方法でデータを管理する

- S3 バケットの利用状況可視化
- 重要情報を別の S3 バケットに保存

S3 バケットの可視化と分割



アプローチ 2：保管中のデータの保護

保管中のデータの保護

アプローチ 2：保管中のデータの保護

➤ 暗号化と適切なアクセスコントロールを実装して保管中のデータを保護することで不正アクセスのリスクを軽減する

- 最小権限のメカニズムでアクセスコントロールを実施する
- 重要情報へのアクセス経路を限定する
- 重要情報を暗号化して鍵を安全に管理する
- 暗号鍵にアクセスできる人を制限する

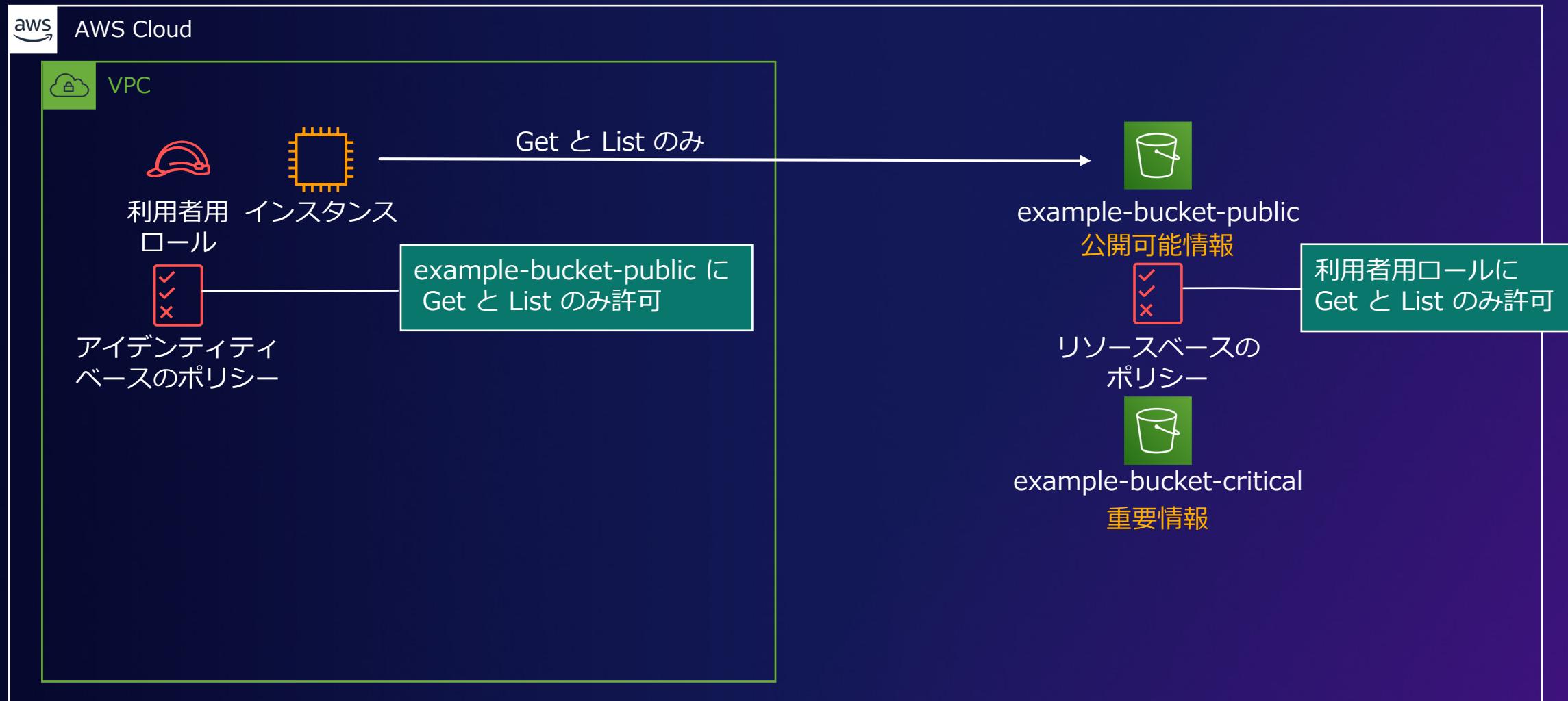
保管中のデータの保護

アプローチ 2：保管中のデータの保護

➤ 暗号化と適切なアクセスコントロールを実装して保管中のデータを保護することで不正アクセスのリスクを軽減する

- 最小権限のメカニズムでアクセスコントロールを実施する
- 重要情報へのアクセス経路を限定する
- 重要情報を暗号化して鍵を安全に管理する
- 暗号鍵にアクセスできる人を制限する

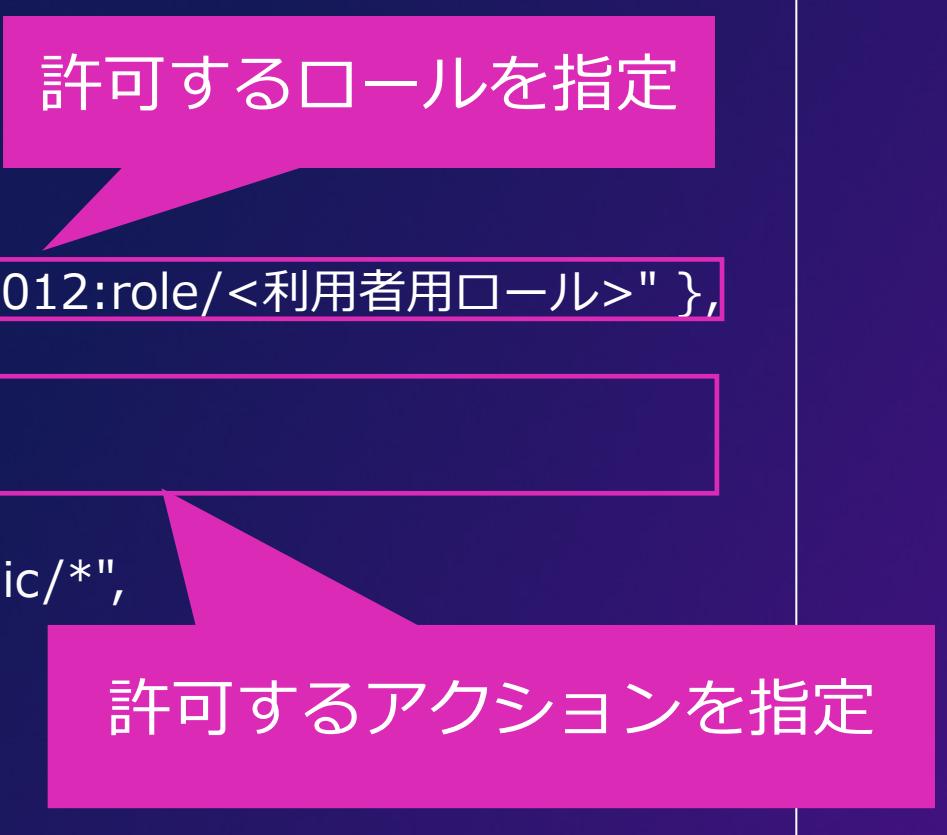
公開可能情報に対するポリシーの設定例



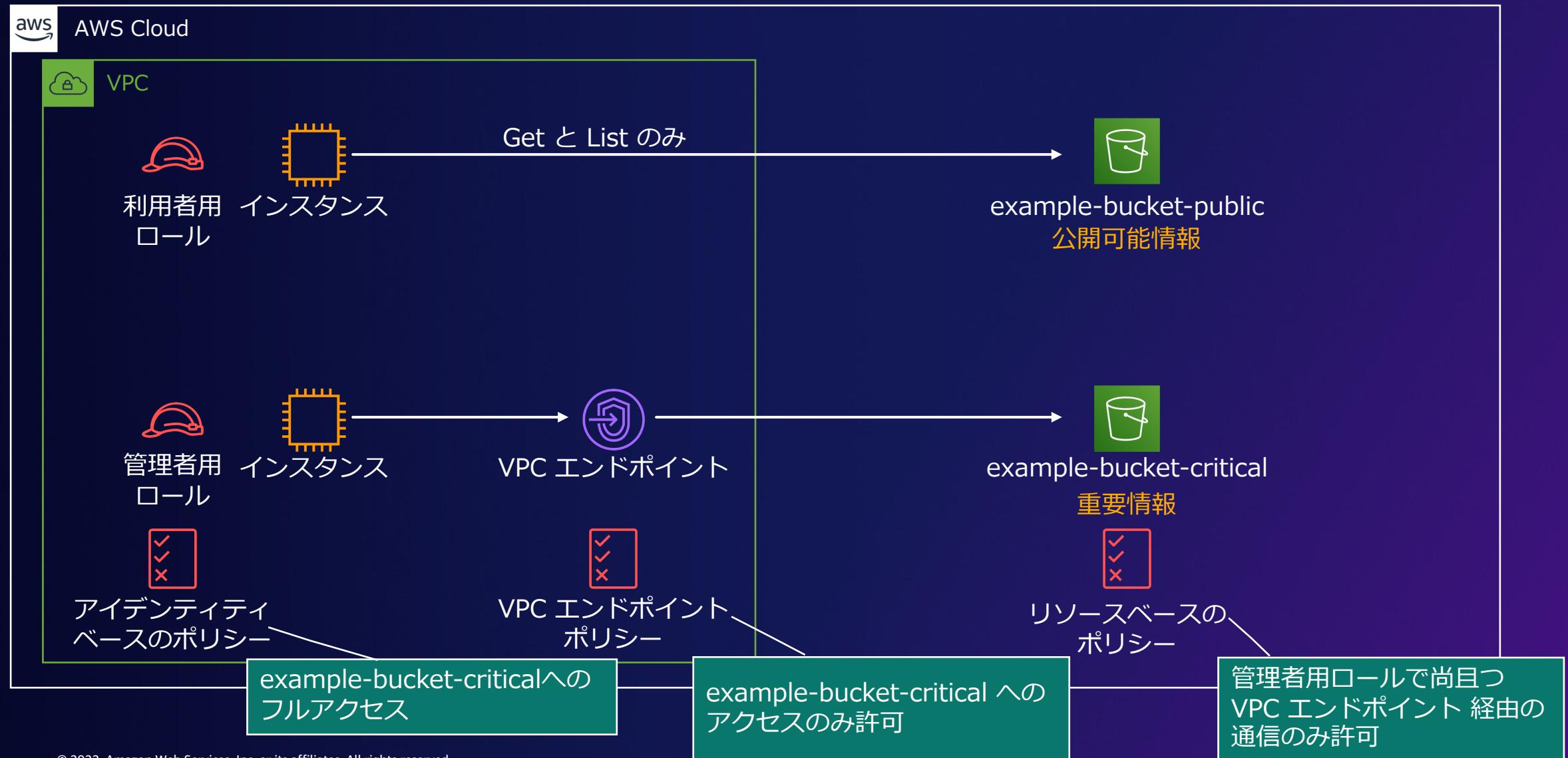
リソースベースのポリシーの設定例

example-bucket-public

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": { "AWS": "arn:aws:iam::123456789012:role/<利用者用ロール>" },  
            "Action": [  
                "s3>ListBucket",  
                "s3GetObject"  
            ],  
            "Resource": "arn:aws:s3:::example-bucket-public/*",  
        }  
    ]  
}
```



重要情報に対するポリシーの設定と経路制御



VPC エンドポイントポリシーの設定例

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "*",  
      "Resource": [  
        "arn:aws:s3:::example-bucket-critical/*",  
        "arn:aws:s3:::example-bucket-critical"  
      ]  
    }  
  ]  
}
```

アクセスを許可するバケットを指定

リソースベースのポリシーの設定例

example-bucket-critical

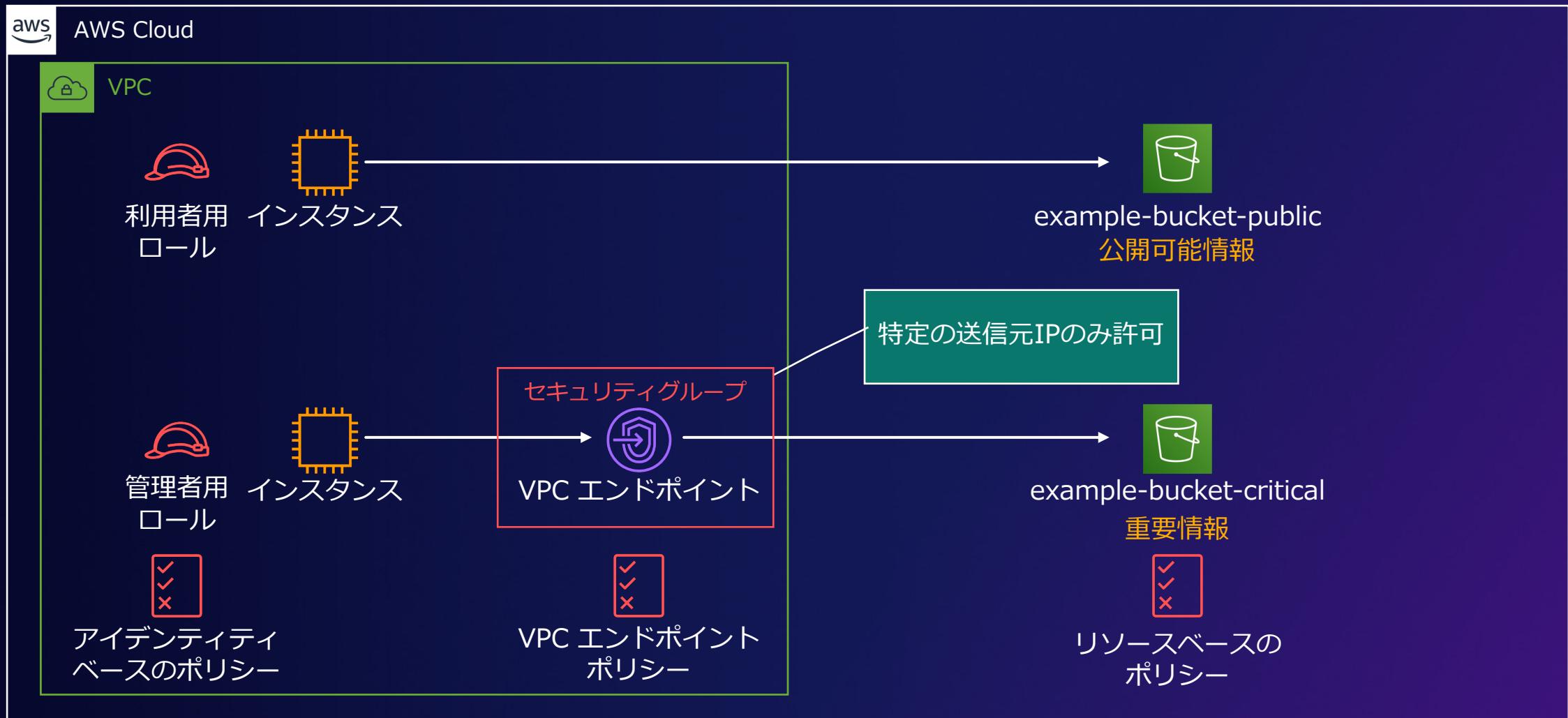
```
{  
  "Version": "2012-10-17",  
  "Id": "Policy1415115909152",  
  "Statement": [  
    {  
      "Sid": "Access-to-specific-VPCE-only",  
      "Principal": "*",  
      "Action": "s3:*",  
      "Effect": "Deny",  
      "Resource": ["arn:aws:s3:::example-bucket-critical",  
                  "arn:aws:s3:::example-bucket-critical/*"],  
      "Condition": {  
        "StringNotEquals": {  
          "aws:SourceVpce": "vpce-xxxxxx"  
        }  
      }  
    }  
  ]  
}
```

注意：

- この例は VPC エンドポイント経由のアクセスのみ許可する記述です
- このポリシーを設定した場合、マネジメントコンソール経由で example-bucket-critical にアクセスできなくなります

許可するVPC エンドポイントを指定

セキュリティグループの追加



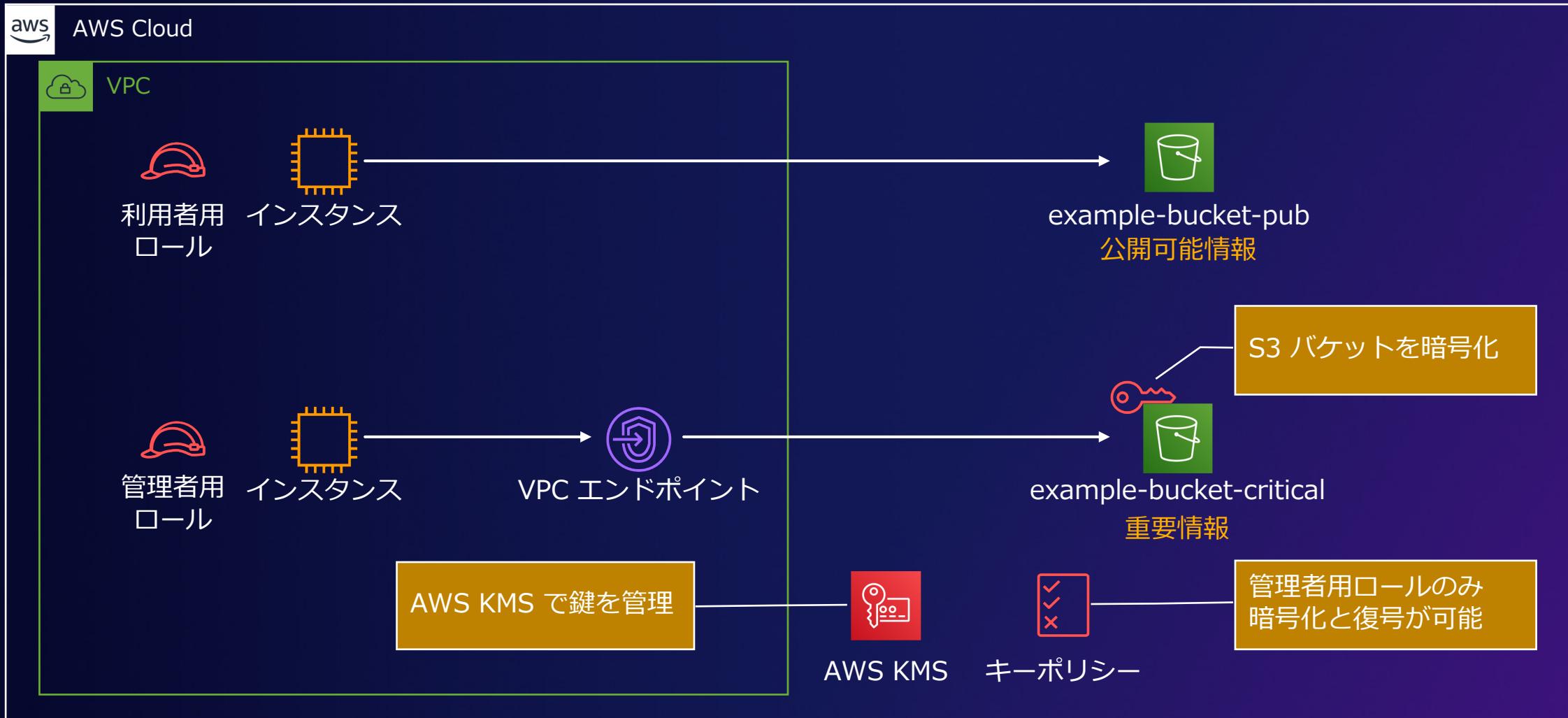
保管中のデータの保護

アプローチ 2：保管中のデータの保護

➤ 暗号化と適切なアクセスコントロールを実装して保管中のデータを保護することで不正アクセスのリスクを軽減する

- 最小権限のメカニズムでアクセスコントロールを実施する
- 重要情報へのアクセス経路を限定する
- 重要情報を暗号化して鍵を安全に管理する
- 暗号鍵にアクセスできる人を制限する

重要情報の暗号化と鍵管理



キー policy の設定例

```
{  
  "Sid": "Allow access for Key Administrators",  
  "Effect": "Allow",  
  "Principal": {"AWS": [  
    "arn:aws:iam::111122223333:role/<管理者用ロール>" ,  
  ]},  
  "Action": [  
    "kms:Encrypt",  
    "kms:Decrypt",  
    "kms:ReEncrypt*",  
    "kms:GenerateDataKey*",  
    "kms:DescribeKey"  
  ],  
  "Resource": "*"  
},
```

許可する暗号化と復号のアクションを指定

「この KMS キー」を対象に指定

データ保護のアプローチ - まとめ

アプローチ		実装例
アプローチ 1 データ分類	S3 バケットの利用状況を可視化	<ul style="list-style-type: none">Macie で S3 バケットの可視化と重要情報を検出
	重要情報を別の S3 バケットに保存	<ul style="list-style-type: none">重要情報と公開情報で S3 バケットを分割
アプローチ 2 保管中のデータの保護	最小権限のメカニズムでアクセスコントロールを実施	<ul style="list-style-type: none">example-bucket-public に アイデンティティベースのポリシーと リソースベースのポリシーを設定
	重要情報へのアクセス経路を限定	<ul style="list-style-type: none">example-bucket-critical に VPC エンドポイントを追加して VPC エンドポイントポリシーを設定
	重要情報を暗号化して鍵を安全に管理	<ul style="list-style-type: none">example-bucket-critical に アイデンティティベースのポリシーと リソースベースのポリシーを設定
	暗号鍵にアクセスできる人を制限	<ul style="list-style-type: none">VPC エンドポイントに セキュリティグループを設定AWS KMS で暗号鍵を管理キー policy を設定



7. まとめ

まとめ

- **データ保護の必要性を理解する**
 - ✓ 様々な分野でデータ活用が進み、企業が分析するデータ量が増加
 - ✓ データは重要な資産
 - ✓ 組織のデータに対する脅威 (ランサムウェア、標的型攻撃など)
- **AWS のデータ保護関連サービスの概要を理解する**
 - ✓ きめ細かいアクセス制御、自動化と可視性向上により運用リスクを低減
 - ✓ ビジネス促進への貢献
 - ✓ データ分類では Amazon Macie、アクセス制御では AWS IAM、暗号化については AWS KMSを紹介
- **サンプルアーキテクチャを通してデータ保護のアプローチを理解する**
 - ✓ AWS Well-Architected フレームワークに沿ったデータ保護のアプローチ
 - ✓ Amazon Macie、AWS IAM、AWS KMS の具体的な利用方法
 - ✓ 具体的なポリシーの設定例

参考資料

- AWS KMS の暗号化の詳細説明

https://docs.aws.amazon.com/ja_jp/kms/latest/cryptographic-details/intro.html

- Amazon EC2 でのデータ保護

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/data-protection.html

- Amazon RDS でのデータ保護

https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/DataDurability.html

- AWS Well-Architected フレームワーク セキュリティの柱 - データ保護

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/data-protection.html

- AWS Well-Architected フレームワーク セキュリティの柱 - データ保護 - 伝送中のデータの保護

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/protecting-data-in-transit.html

- AWS パートナーの検索

<https://partners.amazonaws.com/jp/search/partners>

Thank you!



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.