AWS 決定ガイド

AWS 暗号化サービスの選択

AWS 暗号化サービスの選択: AWS 決定ガイド

Table of Contents

AWS 暗号化サービスの選択

最初のステップを実行する

目的	どの AWS 暗号化サービスが組織に最適かを判断するのに役立ちます。
最終更新日	2025 年 1 月 31 日
対象サービス	• AWS Certificate Manager • AWS CloudHSM • AWS データベース暗号化 SDK • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
関連ガイド	AWS セキュリティ、アイデンティティ、ガバナンスサービスの選択

序章

暗号化はクラウドコンピューティングにおけるセキュリティの基礎であり、データの機密性、完全性、信頼性を確保するのに役立ちます。クラウド環境では、機密データがパブリックネットワークを経由し、共有インフラストラクチャに存在する可能性があるため、不正アクセスや改ざんから保護するために堅牢な暗号化対策が不可欠です。

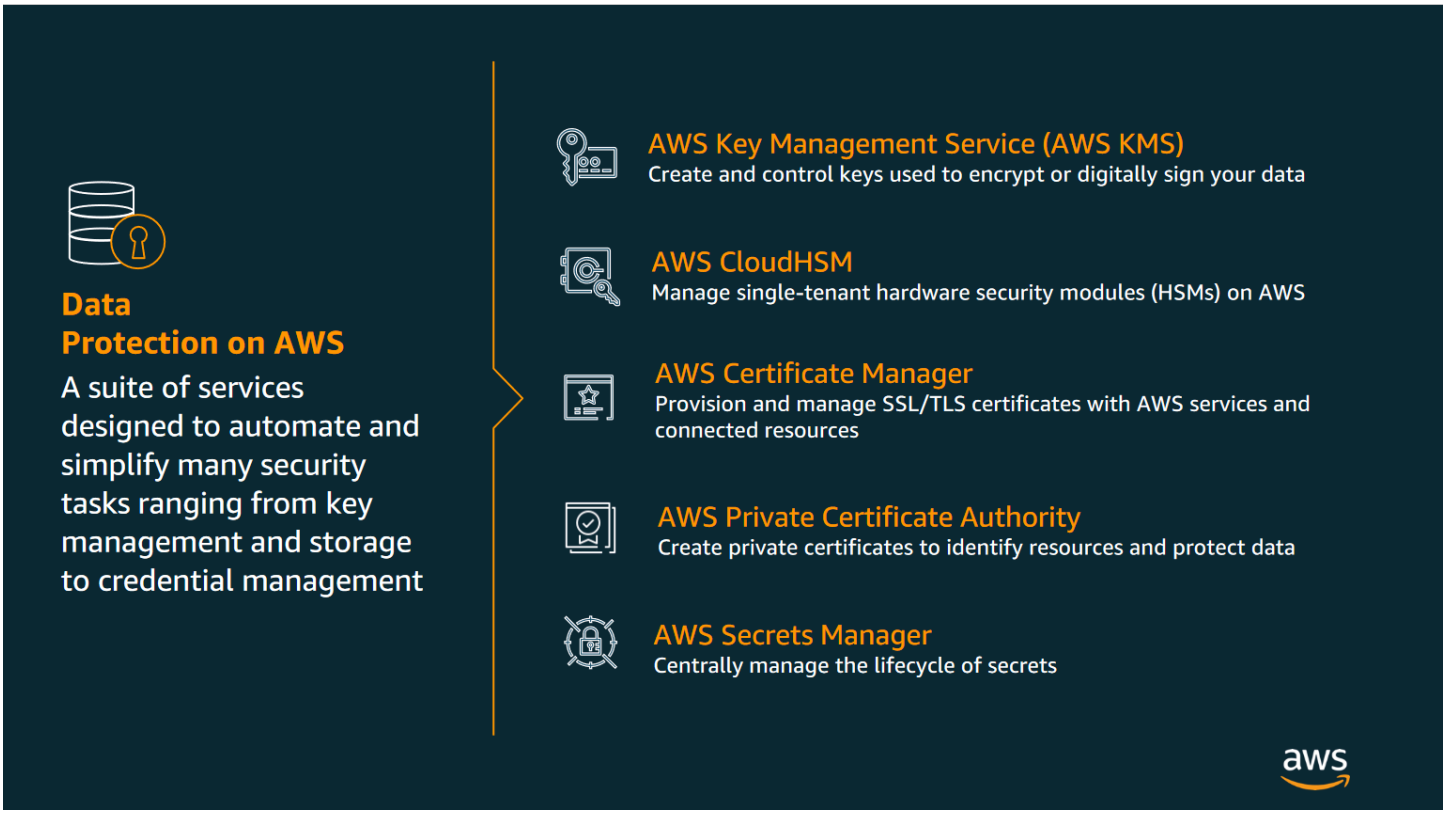
AWS は、データの保護、暗号化キーの管理、機密情報の保護のための包括的な暗号化サービスを提供します。これには、一元化されたキー管理用の AWS Key Management Service (KMS)、PKCS11 アプリケーションおよび専用ハードウェアセキュリティモジュール AWS CloudHSM 用の、クライアント側の暗号化 AWS Encryption SDK 用の が含まれます。 AWS Secrets Manager は、データベース認証情報、API キー、その他のシークレットなどの機密情報をライフサイクルを通じて安全に保存、管理、取得できるサービスです AWS Certificate Manager (ACM) は、 で使用するパブリックに信頼されたトランスポートレイヤーセキュリティ (TLS) 証明書のプロビジョニング、管理、デプロ

イのプロセスを簡素化します AWS のサービス。(PCA) AWS Private Certificate Authority を使用すると、内部リソースの x509 証明書を生成して配布できます。

このガイドは、ニーズと組織に最適な AWS 暗号化サービスとツールを選択するのに役立つように設計されています。

次の動画は、暗号化のベストプラクティスを紹介するプレゼンテーションの 2 分間のセグメントです。

を理解する



適切な AWS 暗号化サービスの選択は、次の表に示すように、特定のユースケース、データセキュリティ要件、コンプライアンス義務、運用上の好みによって異なります。

Key management

暗号化キーを安全に管理する必要がある場合は、 AWS Key Management Service (KMS) を検討してください。これにより、他の と統合された暗号化キーを作成、更新、管理できます AWS のサービス。KMS は FIPS 検証済みの HSMs を使用して、コンプライアンスの見直しに対応し、KMS によって公開される暗号化プリミティブの実装の正確性を保証します。一部のアプリケーションでは、従来の HSM でのみ使用できる特定の暗号化関数またはアプリケーションイン

ターフェイスが必要であり、クラウド内に専用のハードウェアセキュリティモジュール (HSMs) AWS CloudHSM が用意されているため、暗号化キーとオペレーションを完全に制御できます。

Data encryption

顧客の詳細や知的財産などの機密データを暗号化するために、 AWS KMS はストレージ、データベース、メッセージングサービス (S3、RDS、EBS など) と緊密に統合 AWS されています。クライアント側の暗号化が必要な場合、 AWS Encryption SDK はアプリケーション内のデータをクラウドに送信する前に簡単に暗号化できるオープンソースライブラリです。

Secure communications

(AWS Certificate Manager ACM) は、転送中のデータを保護するために、パブリックに信頼された TLS 証明書の管理を簡素化します。インターネット向けアプリケーションのアイデンティティをアサートし、証明書の更新を心配することなく、アプリケーション、ユーザー、クラウドサービス間の通信の暗号化を容易にするために使用します。内部アプリケーションでは、 AWS プライベート認証局 (PCA) を使用して、クライアントとサーバーの両方を含む内部リソースの x509 証明書を生成および配布できます。

Secrets and credentials management

データベース認証情報、API キー、証明書などのアプリケーションシークレットを安全に保存および取得するには、 を検討してください AWS Secrets Manager。自動シークレットローテーションときめ細かなアクセスコントロールを提供します。または、 AWS Systems Manager パラメータストアは、機密性の高い設定を管理するための低コストのオプションであり、 と統合できます AWS Secrets Manager。

Compliance and auditing

規制コンプライアンス作業では、暗号化標準を確実に満たす AWS CloudHSM ために、 AWS KMS と を検討してください。 AWS Artifact は、ISO 証明書や SOC レポートなどの AWSセキュリティおよびコンプライアンスレポートへのオンデマンドアクセスを提供するセルフサービスポータルであり、Business Associate Addendum (BAA) などの契約を確認および受け入れる機能も提供します。また、Config AWS や などのサービスを使用してコンプライアンス AWS Audit Manager をモニタリングし AWS Security Hub、独自の使用や利害関係者による使用に適したアーティファクトを生成することもできます。

AWS 暗号化サービスを選択するときは、次の要件を考慮してください。

要件	サービス
低労力、フルマネージド	AWS KMS or AWS Secrets Manager
KMS でサポートされていない特定のアプリケーションインターフェイスまたは暗号化アルゴリズムを要求する	AWS CloudHSM
アプリケーションのデータの暗号化/復号	AWS Encryption SDK
パブリック TLS 証明書管理の簡素化	AWS Certificate Manager
シークレットの管理	AWS Secrets Manager

要件をこれらのオプションに合わせることで、セキュリティと運用のニーズに合わせた暗号化ソリューションを実装できます。

考慮する

適切な AWS 暗号化サービスを選択するには、特定のセキュリティ、運用、コンプライアンスのニーズを理解する必要があります。 AWS は、キー管理からデータ暗号化、安全な通信まで、さまざまなユースケースに対応するように設計されたさまざまな暗号化サービスを提供します。情報に基づいた意思決定を行うには、ユースケース、統制と柔軟性のニーズ、コンプライアンス義務、コスト上の考慮事項、 との統合など、いくつかの重要な基準に基づいて要件を評価する必要があります AWS のサービス。これらの基準は、組織のセキュリティ目標と運用ワークフローに合わせて選択を行うのに役立ちます。

Use case

データ暗号化、キー管理、安全な通信、シークレット管理など、暗号化サービスに必要なものを検討してください。例えば、 AWS KMS は に統合される暗号化に最適ですが AWS のサービス、 は、厳格なコンプライアンスや特定のアプリケーションのニーズにより、特定の暗号化機能、アプリケーションインターフェイス、またはシングルテナント HSM を必要とする組織 AWS CloudHSM に適しています。目的を明確にすることで、要件に適したサービスを選択し、機能とコストの両方を最適化できます。

Control and flexibility

暗号化オペレーションに必要なコントロールのレベルを評価します。などのマネージドサービスは AWS KMS 、キーマテリアルを完全に制御しながら、マルチテナント HSM による最小限の管理オーバーヘッドで使いやすさを提供します。対照的に、 は、特定のアプリケーション、暗号化、またはコンプライアンスのニーズに合わせてシングルテナントモデル AWS CloudHSM を提供します。

Compliance requirements

規制された業界で運用している場合は、サービスが GDPR、PCI DSS、HIPAA などの標準に準拠 AWS KMS し AWS CloudHSM 、両方とも FIPS 140-2 Level 3 認定を受けていることを確認してください。非機能的な要件を満たすサービスを選択すると、信頼を維持し、潜在的な法的または金銭的な罰則を回避できます。

Cost considerations

予算をサービスの料金モデルと照らし合わせて評価します。 AWS KMS は一般的な暗号化ニーズに対して費用対効果が高く、専用ハードウェアによりコスト AWS CloudHSM が高くなります。コストへの影響を理解することで、セキュリティ支出を最適化できます。

Integration with AWS ecosystem

を頻繁に使用する場合は AWS のサービス、S3、RDS、Lambda とシームレスに統合する や AWS KMS ACM などの暗号化ソリューションを優先します。これにより、ワークフローがスムーズになり、開発作業が軽減されます。統合機能により、運用効率が大幅に向上します。

選択

適切な AWS 暗号化サービスを選択するには、特定のセキュリティ、運用、コンプライアンスのニーズを理解する必要があります。 AWS は、キー管理からデータ暗号化、安全な通信まで、さまざまなユースケースに対応するように設計されたさまざまな暗号化サービスを提供します。情報に基づいた意思決定を行うには、ユースケース、統制と柔軟性のニーズ、コンプライアンス義務、コスト上の考慮事項、 との統合など、いくつかの重要な基準に基づいて要件を評価する必要があります AWS のサービス。これらの基準は、組織のセキュリティ目標と運用ワークフローに合わせて選択を行うのに役立ちます。

ターゲットユースケース	いつ使用するか?	推奨サービス
キー管理	他の と統合された暗号化キーを安全に作成、ローテーショ	AWS KMS

ターゲットユースケース	いつ使用するか?	推奨サービス
	ン、管理するには AWS のサービス	
キー管理	特定のアプリケーション統合または暗号化プリミティブの場合	AWS CloudHSM
データの暗号化	クライアント側の暗号化を実装して、顧客の詳細や知的財産などの機密データを保護する。	AWS Encryption SDK AWS データベース暗号化 SDK
安全な通信	転送中のデータを保護し、SSL/TLS 証明書の管理を簡素化するため。	AWS Certificate Manager AWS Private CA
シークレットと認証情報の管理	データベース認証情報、API キー、証明書などのアプリケーションシークレットを安全に保存および取得するには。	AWS Secrets Manager AWS パラメータストア

使用アイテム

これで、各 AWS 暗号化サービスの動作と、どちらが適切かを明確に理解できたはずです。

を使用し、利用可能な AWS 各暗号化サービスの詳細について調べる方法を検討するために、各サービスの動作を調べるためのパスを用意しました。以下のセクションでは、詳細なドキュメント、実践的なチュートリアル、その他のリソースへのリンクを提供します。

AWS Certificate Manager

- の使用を開始する AWS Certificate Manager

  パブリック証明書とプライベート証明書の両方の使用を含め AWS Certificate Manager、 の使用を開始します。

ガイドを見る

- のベストプラクティス AWS Certificate Manager

  より効果的に を使用する AWS Certificate Manager のに役立つ推奨事項を確認します。

  ガイドを見る

- AWS Certificate Manager よくある質問

  ACM の機能、機能、使用状況に関する一般的な質問に対する詳細な回答については、 AWS Certificate Manager 「(ACM) のよくある質問」ページを参照してください。ACM が管理する証明書のタイプ、他の との統合 AWS のサービス、SSL/TLS 証明書のプロビジョニングと管理に関するガイダンスなどのトピックについて説明します。

  FAQsを確認する

AWS CloudHSM

- の使用を開始する AWS CloudHSM

  でクラスターを作成、初期化、アクティブ化する方法について説明します AWS CloudHSM。これらの手順を完了したら、ユーザーやクラスターを管理できるほか、付属のソフトウェアライブラリを使用して、暗号化オペレーションを実行できるようになります。

  ガイドを見る

- のベストプラクティス AWS CloudHSM

  クラスターを管理およびモニタリングするためのベストプラクティスについて説明します AWS CloudHSM 。

  ガイドを見る

- AWS CloudHSM 料金

  料金については、 AWS CloudHSM 料金ページを参照してください。 AWS CloudHSMの使用には初期費用はかかりません。では AWS CloudHSM、HSM を終了するまで、起動する HSM ごとに時間単位の料金を支払います。このガイドでは、各 AWS リージョンの時間料金について説明します。

  料金ページを見る

- AWS CloudHSM よくある質問

  AWS CloudHSM に関するよくある質問ページでは、機能 AWS CloudHSM、料金、プロビジョニング、セキュリティ、コンプライアンス、パフォーマンス、サードパーティーアプリケーションとの統合など、一般的な質問に対する詳細な回答を確認できます。

  FAQsを確認する

AWS Encryption SDK

- の使用を開始する AWS Encryption SDK

  AWS Encryption SDK で を使用する方法について説明します AWS KMS。

  ガイドを見る

- のベストプラクティス AWS Encryption SDK

  データの保護に を効果的に活用 AWS Encryption SDK するためのガイダンスについては、AWS Encryption SDK 「ベストプラクティス」ページを参照してください。これらのベストプラクティスに従うことで、暗号化されたデータの機密性と完全性を確保できます。

  ガイドを見る

- AWS Encryption SDK よくある質問

  機能 AWS Encryption SDK、サポートされているプログラミング言語、実装のベストプラクティスなど、 に関する一般的な質問に対する回答については、 AWS Encryption SDK よくある質問ページを参照してください。

  よくある質問を確認する

AWS Database Encryption SDK

- AWS Database Encryption SDK の使用を開始する

  で AWS Database Encryption SDK を使用する方法について説明します AWS KMS。

  ガイドを見る

- AWS Database Encryption SDK を設定する

プログラミング言語の選択やラッピングキーの選択など、 AWS Database Encryption SDK を設定する方法について説明します。

ガイドを見る

AWS KMS

- の使用を開始する AWS KMS

  対称暗号化キーと非対称暗号化キーを含む KMS キーを作成する方法について説明します。

  ガイドを見る
- のベストプラクティス AWS KMS

  の暗号化のベストプラクティスについて説明します AWS KMS。

  ガイドを見る
- AWS KMS 料金

  キーストレージ、API リクエスト AWS KMS、カスタムキーストアなどのオプション機能の料金など、 の使用に関連するコストについては、 AWS Key Management Service (KMS) 料金ページを参照してください。

  料金ページを見る
- AWS KMS よくある質問

  AWS Key Management Service (KMS) FAQ ページには、機能 AWS KMS、セキュリティ対策、請求プラクティス、キー管理オプション、他の との統合など、 に関する一般的な質問に対する詳細な回答が記載されています AWS のサービス。

  FAQsを確認する

AWS Private CA

- のベストプラクティス AWS Private CA

  を効果的に使用する AWS Private CA のに役立つ推奨事項を確認します。

  ガイドを見る

- の使用を開始する AWS Private CA

  ルート CA をプログラムで作成してアクティブ化する方法について説明します。

  ガイドを見る
- AWS Private CA 料金

  プライベート CAs運用とプライベート証明書の発行に関連するコストを確認します。

  料金表ページを確認する
- AWS Private CA よくある質問

  機能 AWS Private CA、料金、プロビジョニング、セキュリティ、コンプライアンス、パフォーマンス、他の との統合など、 に関する一般的な質問に対する詳細な回答を取得します AWS のサービス。

  FAQsを確認する

AWS Secrets Manager

- の使用を開始する AWS Secrets Manager

  AWS Secrets Manager シークレットを作成する方法について説明します。

  ガイドを見る
- のベストプラクティス AWS Secrets Manager

  を使用する際に考慮すべきベストプラクティスについて説明します AWS Secrets Manager。

  ガイドを見る
- AWS Secrets Manager 料金

  AWS Secrets Manager 料金表ページでは、データベース認証情報や API キーなどのシークレットを安全に保存、管理、取得するためのコストについて説明します。

  料金ページを見る
- AWS Secrets Manager よくある質問

  AWS Secrets Manager よくある質問ページでは、機能 AWS Secrets Manager、セキュリティ対策、料金、統合機能など、 に関する一般的な質問に対する詳細な回答を確認できます。

FAQsを確認する

Explore

- 調査とリソース

  暗号化に関する AWS ブログ、動画、ツールをご覧ください。

  リソースを確認する
- 動画

  YouTube の AWS デベロッパーチャンネルからこれらの動画を見て、暗号化戦略をさらに開発および改良してください。

  暗号化ビデオを詳しく見る

ドキュメント履歴

次の表に、この決定ガイドの重要な変更点を示します。このガイドの更新に関する通知については、RSS フィードをサブスクライブできます。

変更	説明	日付
初版発行	ガイドが最初に公開されました。	2025 年 1 月 31 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。