Amazon MWS
アプリケーションの保護

データ暗号化

amazonservices

お知らせ

Amazon の出品者および開発者は、この文書の情報について独自の評価を行う責任があります。この文書は、(a)情報提供のみを目的として、(b)現在の慣行を示しており、これらは予告なく変更されることがあります。また、(c)Amazon.com Services LLC(Amazon)およびその関連会社、サプライヤー、ライセンサーのコミットメントまたは保証を発生させるものではありません。Amazon マーケットプレイス Web サービス(Amazon MWS)の商品またはサービスは、明示または黙示を問わず、いかなる種類の保証、表明、条件もなく、「現状のまま」提供されます。Amazon MWS に関する Amazon の責任は、Amazon の MWS 契約(Amazon 出品パートナーAPI 開発者契約、Amazon 出品パートナーAPI ライセンス契約など)によって管理されており、このドキュメントは Amazon といかなる当事者間の契約の一部ではなく、それを修正するものでもありません。

目次

データ保護ポリシーの要件

転送中の暗号化: 開発者は、Amazonの情報を送受信する際は、すべて暗号化する必要があります（例：データをネットワークで転送する、ホスト間で送受信する）。暗号化にはHTTP over TLS（HTTPS）を使用します。購入者が使用するすべての外部エンドポイント、内部の通信チャネル（例：ストレージレイヤーのノード間のデータプロパゲーションチャネル、外部依存関係への接続）、運用ツールに、このセキュリティ管理を実装する必要があります。転送中に暗号化しない通信チャネルは、未使用であっても無効にする必要があります（たとえば、関連するデッドコードを削除する、依存関係を暗号化チャネルのみに設定する、暗号化チャネルを使用するようにアクセス認証情報を制限する）。信頼できないマルチテナントハードウェア（信頼できないプロキシなど）において、TLSなどのチャネル暗号化が中断するデータメッセージレベルで暗号化を実装する必要があります（AWS Encryption SDKを使用するなど）。

使用していないPIIの暗号化: 開発者は、業界のベストプラクティス標準（AES-128、AES-256、2048ビットのRSAキーサイズ以上など）を使用して、保存されているすべてのPIIを暗号化する必要があります。使用していないPIIの暗号化に使用するマテリアル（暗号化キーや復号キーなど）と暗号化機能（信頼性の高い仮想化プラットフォームモジュールを実装し、暗号化/復号APIを提供するデーモンなど）へのアクセスは、開発者のプロセスとサービスに限定する必要があります。開発者は、取り外し可能メディア（USBなど）や、セキュリティが確保されていないパブリッククラウドアプリケーション（Google Driveを使ってアクセスできるパブリックリンクなど）に、PIIを保存してはなりません。開発者は、PIIが記載された印刷文書を安全に廃棄する必要があります。

データ暗号化の基礎

組織がより迅速で大規模な運用を模索するにつれて、重要な情報の保護はますます重要になります。暗号化によってデータを保護すると、コンテンツは、コンテンツを復号化して読み取り可能な形式に戻す秘密キーなしでは読み取り不能になります。暗号化とは、暗号文として知られている別の形式にプレーンテキストをエンコードすることです。メッセージ（データ）を暗号化するには、キーが必要です。データ暗号化では、秘密キーとも呼ばれるキーを使用して、メッセージを暗号化（ロック）および復号化（ロック解除）します。正しいキーを持つユーザー/デバイスだけがメッセージを復号化し、その内容を読み取ることができます。暗号化は、Amazon の情報の安全性を維持するのに役立ちます。悪意のあるユーザーが暗号文を取得しても、復号化するキーを持たずにメッセージの内容を読み取ることはできません。さらに、これらの暗号化キーは、不正な使用、アクセス、開示、変更を防ぐために、ライフサイクル全体にわたって保護する必要があります。ハッシュ関数と暗号化には違いがあることに注意してください。ハッシュ関数は、大きなランダムサイズのデータを小さな固定サイズのデータに変換するために使用される暗号化アルゴリズムです。ハッシュにより、データの検証が可能になります。一方、暗号化は、メッセージを暗号化および復号化する 2 段階のプロセスです。暗号化は、不正なアクセスに対

してデータを理解不能にすることによって、データを保護します。データは、保存時または転送中に暗号化できます。フレームワークに NIST 800-53 を使用している開発者は、環境の保護に関する具体的なガイダンスについて、システムと通信の保護（SC）を参照してください。主な NIST コントロールの 1 つは、SC-13 暗号化保護です。SC-13 は特定のコントロールを識別し、開発者が Amazon MWS 暗号化要件を理解するのに役立つ追加の詳細を提供します。

開発者は、Amazon の情報とお客様の PII を保護するために、暗号化を使用する必要があります。以下のセクションでは、データ暗号化の重要なコンポーネントについて説明し、開発者が Amazon MWS データ保護ポリシー（DPP）暗号化要件に準拠できるようにするための推奨事項を示します。

データの分類

データの分類は、機密性のレベルに基づいて組織データを分類する方法を提供します。これには、使用可能なデータ型、データの格納場所、アクセスレベル、およびデータのセキュリティについての理解が含まれます。Amazonの情報は、次の2つのカテゴリーのデータに分類できます。 PIIと非PII。PIIデータは、Amazonのお客様を特定するために使用できる任意のデータです。非PIIデータは、商品の出品情報など、その他のAmazonのデータです。開発者は、適切なデータ分類システム、アクセスレベル、およびDPP要件を満たすデータの暗号化を慎重に管理することで、Amazonの情報を保護できます。Amazonのお客様を識別するために使用できるAmazonの情報は、暗号化され、保護された状態で保存される必要があり、情報へのアクセスには承認を義務付ける必要があります。Amazonでは、多層防御アプローチを採用し、Amazonのお客様のPIIへの人的アクセスを減らすことを推奨しています。開発者は、アプリケーションに強力な認証メカニズムを設定する必要があります。さらに、開発者は、アプリケーションへのすべての接続が信頼できるネットワークから発信され、必要なアクセス権を持っていることを確認する必要があります。

データの整合性

開発者は、システムにあるAmazonの情報がシステム内を移動しても、整合性が保たれるようにすることが重要です。暗号化ハッシュ関数は、データの整合性を確立する信頼性の高い方法です。ハッシュ関数は、任意のサイズの元のデータが固定サイズのハッシュ値にマッピングされる不可逆関数です。開発者がダウンロード経由でAmazonの情報を提供する場合、その整合性に関する主な脅威が2つあります。ネットワーク/ストレージの問題による偶発的なデータ変更、および攻撃者による改ざんです。開発者は、ハッシュ関数を使用してファイルの整合性を検証することにより、これらの脅威を軽減できます。たとえば、開発者は、ダウンロードできるようにする前にファイルの内容をハッシュすることができます。ファイルがアプリケーションにアップロードされると、開発者はアップロードされたファイルに対してハッシュ関数を実行し、ハッシュ出力を元のファイルのハッシュ出力と比較して、ファイルの整合性を検証できます。これにより、データ変更がネットワークまたはストレージの問題によって偶発的に発生したか、攻撃者が意図的に引き起こしたかにかかわらず、最善の保護が提供されます。開発者は、複数のハッシュ関数でハッシュを検証することで、データの整合性の信頼を高めることができます。

転送中の暗号化

データはあるシステムから別のシステムに送信されるため、権限のないユーザーや第三者による望ましくない干渉の影響を受けやすくなります。データ送信は開発者のプライベートネットワークまたはパブリックネットワークに限定できますが、悪意のある攻撃の影響は受けやすいままです。開発者は、転送中の暗号化を実装することにより、他のサービスとエンドユーザー間の通信を含め、転送中のAmazonの情報を保護する必要があります。これは、データの機密性と整合性を保護するのに役立ちます。

転送中の暗号化は、TLS 1.2 や HTTPS（HTTP over TLS）などのサポートされている暗号化プロトコルを使用して情報を保護します。このレベルの暗号化は、すべての外部エンドポイントと内部エンドポイントに適用する必要があります。チャネルを介して伝搬されるデータ、外部依存関係への接続、および運用ツールは、転送中の暗号化で保護する必要があります。Amazon の情報が送信される際には、不正な干渉が起きないように、使用される通信チャネルを暗号化する必要があります。ベストプラクティスは、すべてのトラフィックを暗号化して認証することです。NIST 800-53 では、転送中の暗号化がコントロール SC-8 伝送の機密性と整合性で概説されています。このコントロールを活用する開発者は、SC-8 コントロールの拡張の採用を検討する必要があります。これは、各拡張により、転送中のデータをさらに保護できるためです。

開発者は、転送中のデータを暗号化する際に、次の点を考慮する必要があります。

- 転送中の暗号化をサポートできない通信チャネルを無効にします。
- マルチテナントインフラストラクチャノードを介したトラフィックのルーティングは避けます。
- エンドツーエンドのTLSが許可されていない場合は、データメッセージレベルの暗号化を使用します。

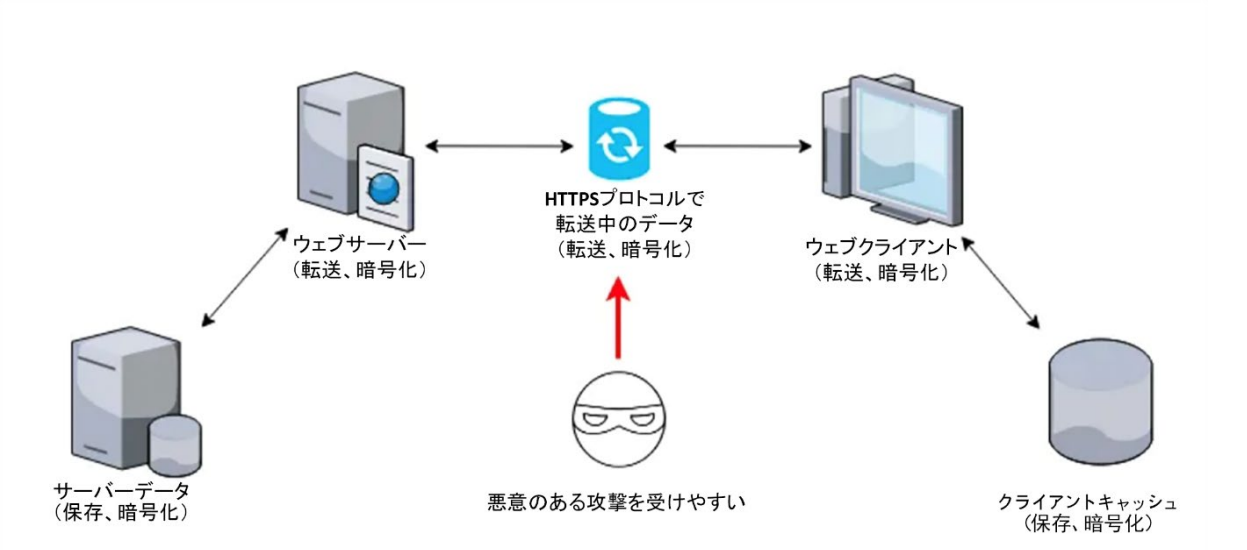

図1：使用中のHTTPSプロトコル

表1に、転送中のデータを暗号化するためのAmazon準拠のセキュリティプロトコルを示します。

転送タイプ	安全でないプロトコル（非準拠）	安全なプロトコル（準拠）
Webアクセス	HTTP	HTTPS（TLS 1.2以降）
メールサーバー	POP3、SMTP、IMAP	POP3S、IMAPS、SMTPS
ファイル転送	FTP、RCP	SFTP、SCP、HTTPS経由のWebDAV
リモートシェル	Telnet	SSH-2
リモートデスクトップ	VNC	r-admin、RDP

表1：転送中のデータを暗号化するための安全なプロトコルと安全でないプロトコル

保存時の暗号化

開発者がデータストアにAmazonの情報を保持する場合、情報は常に保護する必要があります。データストアとは、指定した期間にわたってデータを保存および保持できる任意の記憶媒体を指します。データベースソリューション、ブロックストレージ、オブジェクトストレージ、アーカイブデータブロックはすべて、保護する必要があるデータストアの例です。開発者は、暗号化を使用してデータストア内のデータを保護できます。これは、保存時の暗号化と呼ばれます。暗号化と適切なアクセス制御を実装することで、不正アクセスのリスクが軽減されます。NISTでは、保存時の暗号化についてSC-28保存情報の保護で説明しています。SC-28（1）は、保存中の情報を暗号化して保護することを目的とし、SC-28（2）はオフラインストレージを介して情報を保護することを目的としています。これらのコントロールは、Amazon MWS DPPで説明されているように、Amazonのお客様のPIIを処理する開発者にとって必要です。ベストプラクティスは、Amazon情報をストレージにアップロードする前に暗号化し、承認された暗号化アルゴリズムでストレージ自体を保護することです。これにより、ソースからストレージへの転送中、およびストレージでの保存期間中の2つのレベルでデータが保護されます。

ストレージに Amazon S3 を使用している開発者は、S3 のネイティブ暗号化機能を使用して、保存中のデータを保護できます。開発者は、S3 管理暗号化キーによるサーバー側の暗号化（SSE-S3）または AWS KMS 管理キーによるサーバー側の暗号化（SSE-KMS）を使用している場合を除き、暗号化されていないオブジェクトのアップロードを防止する Amazon S3 バケットポリシーを実装できます。Amazon S3 は、エンベロープ暗号化を使用して保存中のデータを保護します。各オブジェクトは、強力な多要素暗号化を採用した一意のキーで暗号化されます。追加の保護策として、AWS はマスターキーを使用してキーを暗号化します。Amazon S3 のサーバー側の暗号化では、AES-256 を使用してデータを暗号化します。図 2 では、暗号化ソリューションによって暗号化キーとデータが保護されています。

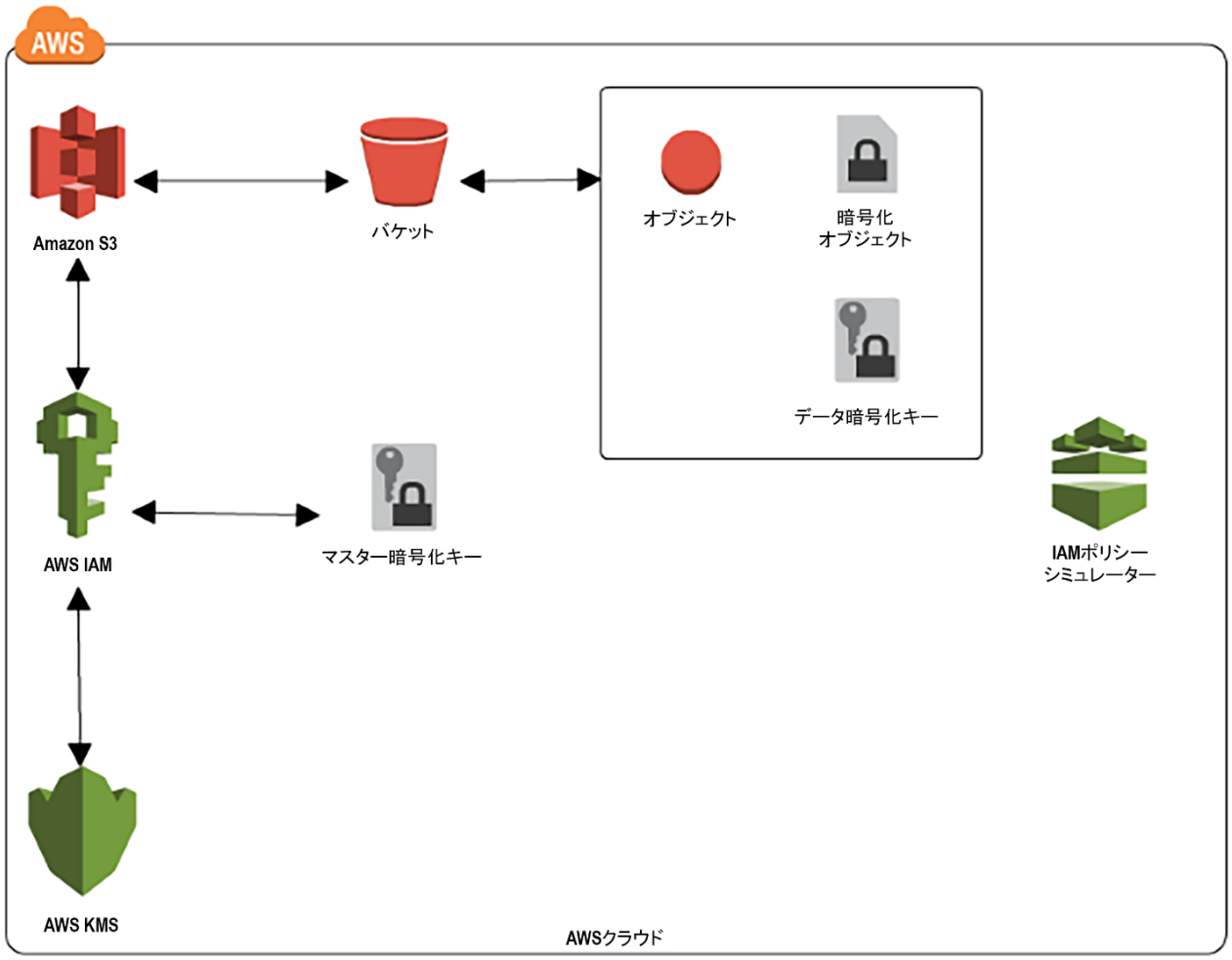

図 2: Amazon S3 での保存時の暗号化

詳細については、「暗号化されていないオブジェクトが Amazon S3 にアップロードされないようにする方法」を参照してください。

転送中および保存中のデータを保護するためのベストプラクティス

転送中か保存中かに関わらず、保護されていないデータによって、企業は攻撃を受けやすくなります。開発者は、すべてのデータが暗号化によって保護されていることを確認する必要があります。開発者は、転送中および保存中のデータを堅牢に保護するために、次のベストプラクティスに従う必要があります。

- 堅牢なネットワークセキュリティ制御を実装して、転送中のデータを保護できるようにします。たとえば、開発者は、ファイアウォールとネットワークアクセスコントロールリストを使用して、マルウェア攻撃や侵入からネットワークを保護できます。

- リスクのあるデータを特定し、転送中および保存中のデータに対して効果的なデータ保護を実装する、積極的なセキュリティ対策を実施します。セキュリティインシデントによってセキュリティ対策が実装されるのを待たないでください。
- ユーザーのプロンプトやブロックを有効にするポリシーや、転送中のPIIデータの暗号化を自動化するポリシーを使用するソリューションを選択します。PIIデータを含むファイルのEメールへの添付、クラウドストレージへの移動、他の場所への転送などが行われると、アプリケーションによって警告が表示されたり、アクションがブロックされたりします。
- すべてのAmazonの情報を体系的にカテゴリーに分け、分類するためのポリシーを作成します。
- データの格納場所に関係なく、データの保存中は適切なデータ保護対策を適用してください。
- 権限のないユーザーによるデータのアクセス、使用、転送が行われた場合にトリガーを生成します。
- Amazonの情報の保存に使用されるパブリック、プライベート、またはハイブリッドのクラウドプロバイダーを、そのデータのセキュリティ対策に基づいて慎重に評価します。

転送中および保存中のデータは、リスクプロファイルが多少異なりますが、固有のリスクは主にAmazonの情報の機密性と価値に大きく影響します。悪意のある攻撃者は、転送中または保存中の貴重なデータにアクセスしようとします。データとセキュリティプロトコルを分類してカテゴリーに分け、すべての段階でAmazonの情報を効果的に保護することが重要です。

暗号化の種類

一般的な暗号化の種類は次のとおりです。

- **対称暗号化。** これは、暗号化と復号化に同じキーを使用します。したがって、送信者と受信者の両方が同じキーを持っている必要があります。
- **非対称暗号化。**これには、送信者と受信者が異なるキー（公開キーと秘密キー）を使用する必要があります。公開キーは広く共有されますが、秘密キーはその所有者によってのみ保護され、使用されます。秘密キーはデータの暗号化に使用され、公開キーはデータの復号化に使用されます。
- **エンベロープ暗号化。**これは、暗号化キーを使用してデータを暗号化し、別のキーを使用して暗号化キーを暗号化する方法です。

一般に、対称キーアルゴリズムは高速で、非対称アルゴリズムよりも小さな暗号テキストを生成します。しかし、非対称アルゴリズムでは役割が本質的に区別され、キー管理が簡単です。エンベロープ暗号化では、開発者は対称アルゴリズムと非対称アルゴリズムの両方の長所を

組み合わせることができます。開発者がAmazonの情報を暗号化する場合、暗号化キーも保護する必要があります。エンベロープ暗号化は、開発者が暗号化キー自体を保護するのに役立ちます。

SSE-KMSを使用している開発者は、1つの暗号化キーを使用してデータを暗号化し、別のキーを使用して暗号化キーを暗号化することができます。1つのキーはプレーンテキストのままであるため、クライアントは暗号化キーを復号化し、復号化された暗号化キーを使用してデータを復号化できます。最上位レベルのプレーンテキストキーは、マスターキーと呼ばれます。

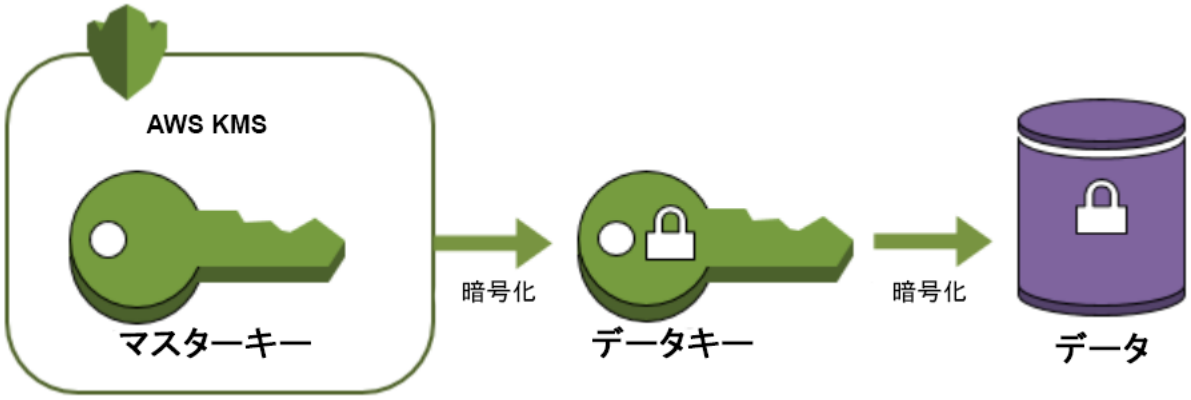

図3: AWS KMSマスターキーの保存と管理

詳細については、「AWS Key Management Service の概念」を参照してください。

キーサイズは、暗号化キーの強度を定義する際に重要です。Amazon DPP で必要とされているように、キーの長さは 128 ビット以上である必要があります。Amazon では、開発者が Amazon のお客様の PII には 128 ビットを超えるキーを使用することを推奨しています。追加のビットにより、暗号化キーに対するブルートフォース攻撃の複雑さが飛躍的に増加します。対称 256 ビットキーは、128 ビットキーの 2128 倍の計算能力を必要とします。開発者は、システムをさらに保護するために、暗号化キーをローテーションする必要があります。キーサイズが大きいほど解読しにくくなりますが、権限のないエンティティが公開されたキーを使用して Amazon の情報にアクセスできるため、公開されたキーはキーサイズに関係なく表示されます。キーローテーションに関する具体的なガイダンスは、NIST 800-53 個コントロール SC-12 暗号化キーの確立と管理にあります。SC-12 コントロールとその拡張により、開発者は、組織にとって許容可能な方法でキーを確立、保護、およびローテーションし、必要なときにキーを使用できるようにすることができます。

Amazon MWSの適正な暗号化基準

高度暗号化標準（AES）

高度暗号化標準（AES）は、ブロック暗号を使用する対称暗号化アルゴリズムです。ブロック暗号は、固定テキストブロックを同じ長さの暗号テキストブロックに暗号化します。AESは、128ビット、192ビット、または 256ビットの設定可能な対称キー長を持つ128ビットの固定長ブロック上で動作します。128ビットキーであっても、2128個の可能なキー値（ブルートフォース攻撃）をそれぞれチェックしてAESをクラッキングするタスクは非常に計算集約的であり、最速のスーパーコンピューターでも平均で100兆年以上かかります。開発者がAESキーを使用する場合、キーサイズは（Amazon DPPで要求される）AES128ビット以上である必要があります。Amazonでは、AES-256の使用を推奨しています。Amazonは、AES-GCM/CBC/XTSの使用も承認しています。

Rivest-Shamir-Adleman暗号化規格（RSA）

Rivest-Shamir-Adleman暗号化規格（RSA）は、公開キー暗号化を使用して安全でないネットワーク上でデータを共有する非対称アルゴリズムです。RSAは、2つの大きな素数の積である大きな整数を考慮して、キーサイズを確立します。通常は1024ビットまたは2048ビットのキーを使用します。キーのサイズが大きいほどセキュリティは高くなりますが、情報の暗号化と復号化に多くの計算能力を使用します。開発者は、暗号化標準としてRSAを選択する場合、そのキーが、Amazon DPPで要求される2048ビット以上であることを確認する必要があります。

その他の暗号化アルゴリズム

開発者が使用できる暗号化標準は他にもありますが、Amazon DPP ではAESまたはRSAを使用する必要があります。表2に、Amazonが承認した暗号化アルゴリズムを示します。以下の表に記載されていない他の業界標準の暗号化アルゴリズムを開発者が使用している場合、security@amazon.comに連絡して相談してください。

暗号化アルゴリズム	Amazonが承認したタイプ
AES	256ビット（推奨）
	128ビット以上のキー。
GCMモードでのAES	96ビット暗号論的乱数初期化ベクトル
	128ビットのタグ長。
CBCモードのAES	128ビット暗号論的乱数初期化ベクトル
	PKCS7パディング
XTSモードのAES	Linux：dm-crypt、LUKS Amazon EBS暗号化
RSA	2048ビット以上のキー。
	RSA-OAEP

表2：Amazon MWSで承認されている暗号化アルゴリズム

暗号化のベストプラクティス

Amazon の情報の暗号化に関するベストプラクティスを以下に示します。

- Amazonの情報を機密性レベルに分類し、重要なデータを暗号化します。Amazonのお客様のPIIは、常にAmazonが承認した暗号化メカニズムを使用して暗号化する必要があります。
- 転送中の重要なデータの暗号化を要求または自動化する自動ポリシーを確立します。
- AESや秘密キーなど、一般に公開され、査読されたアルゴリズムを使用して、暗号化および復号化します。
- クラウドインフラストラクチャを使用する開発者は、提供するセキュリティ対策と保有するセキュリティコンプライアンス認定に基づいて、クラウドベンダーを評価する必要があります。

その他のリソース

- MWSデータ保護ポリシー
- MWS利用規約
- AWSセキュリティのベストプラクティス
- 転送中のデータの保護
- 保存時のデータの保護

業界の参考資料

- NIST 800-53 Rev.5（ドラフト）：情報システムと組織のセキュリティ&プライバシーコントロール

文書の変更履歴

データ	内容
2020年1月	初版