Amazon MWS
アプリケーションの保護

データの保持と回復

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 セリングパートナー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、この文書は Amazon と第三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

開発者は、注文の処理または税金の計算/送金の目的に限り、必要な期間（注文出荷後30日以内）PIIを保持するものとします。税務上または同様の規制の目的で、開発者がPIIのアーカイブコピーを保持するよう法律で求められている場合、このアーカイブされたAmazonの情報は、物理的に安全な施設に「コールド」またはオフラインで（つまり、即時の使用または双方向の使用ができない）バックアップとして保存し、バックアップメディアのすべてのアーカイブデータは暗号化する必要があります。PIIが失われた場合（システムのクラッシュやランサムウェアが原因でデータが消去されたり、処理できなくなったりした場合）は、失われたPIIをすべて回復する必要があります。

データの保持と回復の基礎

購入者のIDの整合性を確保するため、Amazonのカスタマー PIIを非公開のまま維持することが重要です。この種類の情報の保護が必要な理由は、詐欺や迷惑なマーケティング、または個人のIDの窃盗に使用される恐れがあるということです。不要になった古いコンテンツを削除することで、訴訟やセキュリティ侵害のリスクが軽減されます。

開発者は、NIST-800-53管理策番号**SI-12**: **情報管理と保持**を活用できます。この管理策の目的は、この情報（PIIを含む）が、規制、契約、およびビジネス要件に従って確実に保持されるようにすることです。また開発者は、情報の保持期間を決定する際（システムの廃棄を超える場合を含む）に、適用可能なすべての要件を考慮する必要があります。開発者は、Amazon MWSに連絡することで、義務を果たすために必要な過去の情報を取得することができます。

開発者は、次の用語に精通している必要があります。

- **個人識別情報**（PII）とは、単独で、または他の関連データとともに使用された場合に個人を識別できる情報です。
- **データ保持**とは、法令遵守やビジネス上の理由からデータを保存するプロセスです。
- **データ保持期間**とは、組織が特定の種類のデータを保持する期間です。データタイプによって異なる保持期間を設定する必要があります。
- **アーカイブ**とは、すでに使用されていないデータを、保持のために別のストレージデバイスまたは場所（コールドストレージ内が好ましい）に移動するプロセスです。
- **コールドストレージ**とは、使用されておらず、使用頻度の低いデータの保存媒体です。
- **バックアップ**とは、元のデータに不備が発生した場合に備えて作成されたデータのコピーです。そのバックアップコピーにポリシーが適用されると、バックアップデータ保持と呼ばれます。
- **破壊**は、データを通常の民間による手段では復旧できないようにする、データの物理的または技術的な破壊として定義されています。

収集

Amazonのカスタマー PIIを収集する前に、組織はデータの収集に対するビジネスニーズを判断する必要があります。また、組織は、どのユーザーがこのデータにアクセスできるかを決定する必要もあります。
開発者のAmazonのカスタマー PIIに対する要件は、Amazon MWSのデータ保護ポリシーに準拠している必要があります。

開発者は、出品者の代理での注文処理や、税金の計算/送金の必要がある場合に限り、Amazonのカスタマー PIIを保持する必要があります。Amazonのカスタマー PIIは、注文の発送後30日を超えて開発者システムに保管することはできません。返品または保証の処理のために後からAmazonのカスタマー PIIが必要になった場合、開発者は、Amazon MWS APIを呼び出して必要なデータを取得する必要があります。開発者の責任として、Amazon MWSのデータ保持条項に準拠するため、システム全体でAmazonカスタマー PIIのライフサイクルポリシーに従う必要があります。

税務上または同様の規制の目的でAmazonカスタマー PIIのアーカイブコピーを保持するよう法律で求められている場合、このアーカイブされたAmazonの情報は、物理的に安全な施設に「コールド」またはオフラインでバックアップとして保存する必要があります。バックアップメディア上のすべてのアーカイブデータは暗号化する必要があります。従来、これには高価な専用ハードウェアが必要であり、データ保持量の増加に伴い、ストレージコストを急速に引き上げる要因となっていました。長期的なアーカイブにAmazon Glacierなどのクラウドストレージを使用することで、組織はコスト効率に優れた方法で、数年間から数十年間にわたってデータを保存できます。このアプローチにより、組織はストレージの管理と拡張に伴う管理上の負担を軽減できます。

開発者は、開発者システムに保持されているAmazonの情報が常に暗号化されていることを確認する必要があります。また開発者は、このデータにアクセスできるのは権限を持つユーザーのみであることを確認する必要があります。暗号化の詳細については、Amazon MWSの暗号化に関するホワイトペーパーを参照してください。

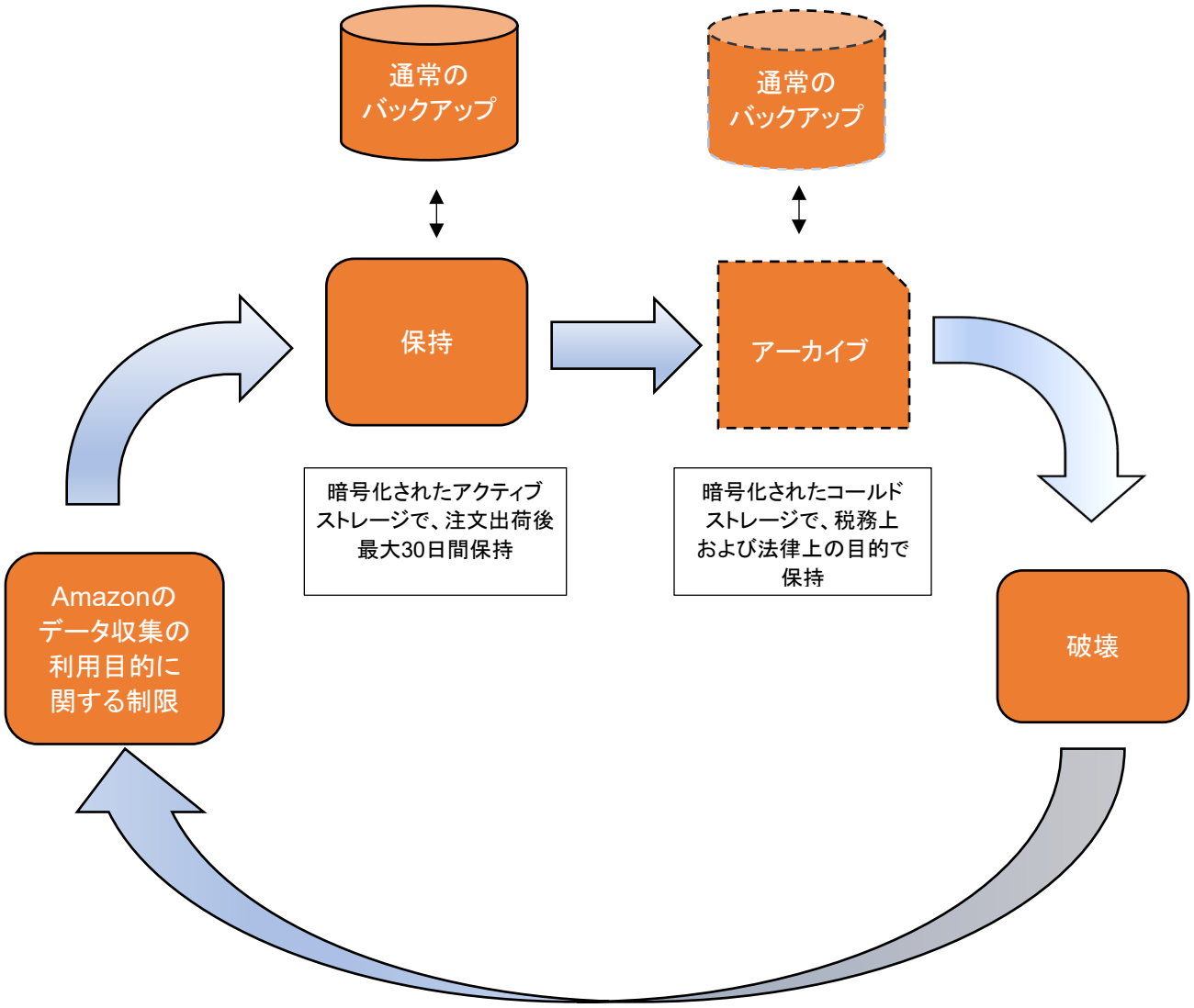

図1：Amazonのデータ処理

保持

開発者は、データ保持プランを作成または修正する際に、次のことを行う必要があります。

- **データ保持ポリシーを作成します。**このポリシーは、Amazon MWSのデータ保護ポリシーに準拠し、開発者の法的要件を満たしている必要があります。
- **データ保持タスクを自動化**します。これは、タスクを要件の変更に応じて簡単に変更できる方法で行う必要があります。ポリシーに基づいてデータを自動的にアーカイブできるクラウドベースのアーカイブの例として、Amazon Glacierがあります。Amazon Glacierの詳細については、「アーカイブ」セクションを参照してください。

- **データをアーカイブまたは削除する必要があるかどうかを検討**します。削除は永続的なものですが、アーカイブには運用コストが発生します。データタイプやユースケースごとに異なるライフサイクルを実装します。たとえば、フルフィルメントと税務のユースケースでは、法的要件とビジネス要件が異なります。
- 情報が不要になった場合、またはその他の保持義務の対象となった場合、**Amazonの情報を削除**します。
- データ保持の手順、および出品者のAmazonのカスタマーPIIへのアクセスや処理の際に従う必要のある基準について、**Amazonの出品者に通知**します。
- **Amazonの情報を常にバックアップし、保護します。**これは、Amazon MWSのポリシーに従って行う必要があります。これは、全般的なデータ保持とデータ管理において重要なことです。

アーカイブ

法令遵守または規制上の理由からAmazonの情報を保存する必要がある場合、開発者はその情報をアーカイブする必要があります。データの破損や消失からの回復を目的として実行中のデータのコピーを短期間保持するバックアップの作成とは異なり、アーカイブでは、保持ポリシーの期限が切れるまですべてのデータのコピーが維持されます。

優れたアーカイブシステムは、次の機能を備えています。

- 長期的な整合性のためのデータの耐久性。
- データのセキュリティ。
- 回復の容易さ。
- 低コスト。

フレームワークとしてNIST 800-53を使用している開発者は、管理策番号**MP-4**: **メディアストレージ**を参照することができます。この管理策はメディア保護（MP）ドメインに属しますが、Amazon MWSの開発者は、物理的に保護された施設にある「コールド」バックアップまたはオフラインのバックアップにアーカイブおよび保管する必要があります。MP-4では特に、メディアを物理的に制御して安全に保管し、適切に廃棄することによって、メディアを保護することが求められます。開発者は、SC-28（1）に記載されているように、暗号化保護を実装することで、この管理策をさらに強化できます。この管理策の要件を満たすには、パブリッククラウドでの「コールド」ストレージオプションの活用を検討してください。

Amazon Web Services（AWS）を使用したデータのアーカイブ

Amazon Simple Storage Service（S3）Glacierは、データのアーカイブと長期的なバックアップのための、安全性と耐久性に優れた低コストのソリューションです。さらにこのソリューションでは、保管時のデータのネイティブ暗号化、イレブンナインの耐久性、無制限の容量を提供します。Amazon S3 Glacierのお客様は、1か月あたり、1テラバイトごとにわずか1米ドルでデータを保存できます。また、アーカイブにアクセスする方法には3つのオプションがあり、取得に必要な時間は数分から数時間にわたります。

Amazon S3の標準～低頻度アクセスは、データの迅速な取得を必要とするユースケースに適しています。Amazon S3 Glacierは、データへのアクセス頻度が低く、データの取得に数時間が許容されるユースケースに適しています。

オブジェクトは、Amazon S3またはAmazon S3 Glacier APIのライフサイクルルールのいずれかによって、Amazon S3 Glacierに階層化されます。Amazon S3 Glacierのボールトロック機能を使用すると、ボールトロックポリシーを使用して、個々のAmazon Glacierボールトに対してコンプライアンスコントロールを簡単にデプロイおよび適用できます。開発者は、ボールトロックポリシーで「write once, read many」（WORM）などのコントロールを指定することで、ポリシーを将来編集されないようにロックできます。

以下は、AWS製品を使用してデータ保持と回復の要件を満たす方法を視覚的に示しています。

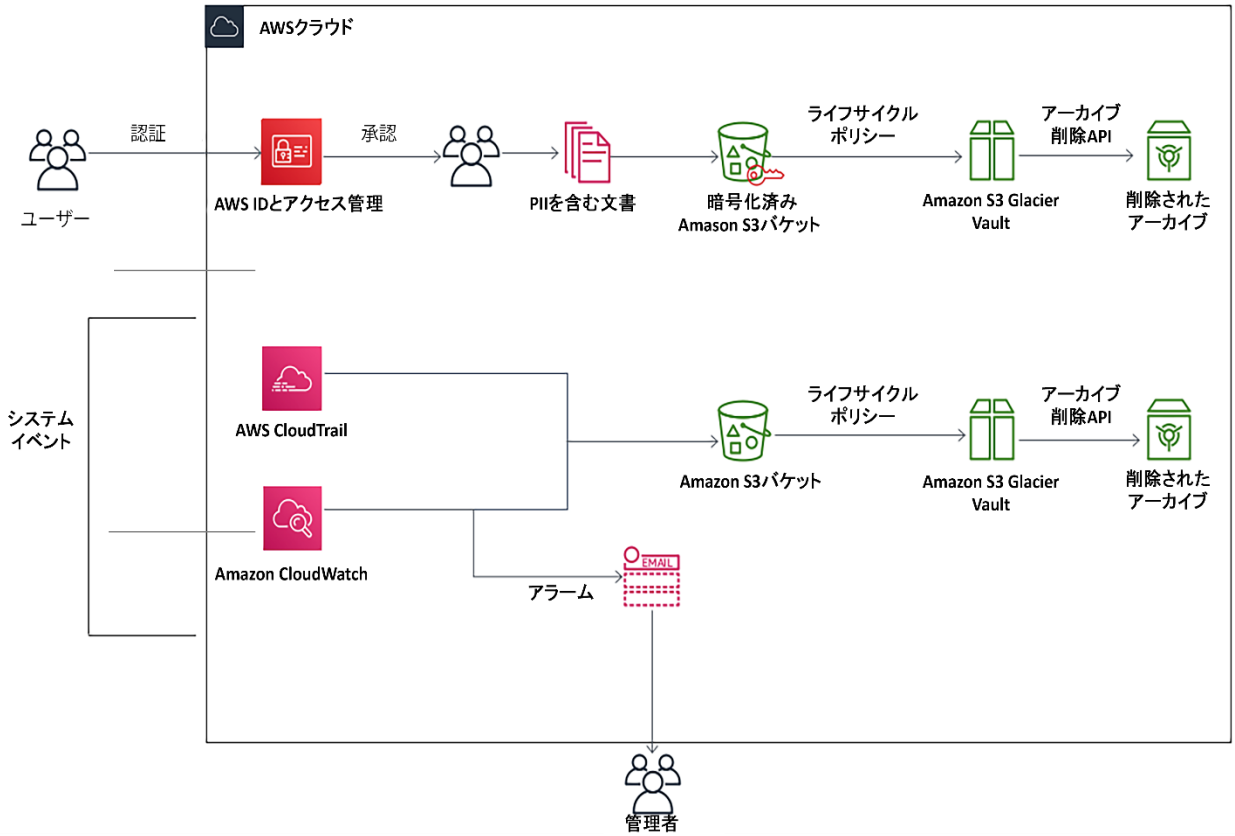

図2：AWSを使用したデータのアーカイブ

図2では、ユーザーがAWSクラウドで認証を行い、暗号化されたAmazon S3バケットにPIIを含む文書をアップロードします。そこから、ライフサイクルポリシーを使用して、Amazon S3バケットからAmazon S3 Glacierボールトにデータを自動的にシフトできます。情報が規制目的で必要とされなくなったら、Amazon S3 Glacierの「アーカイブの削除」APIが呼び出され、情報が削除されます。さらに、AWS CloudTrailとAWS CloudWatchが有効化され、環境内のアクションを記録し、イベントが発生した場合に管理者に電子メールで通知します。Amazon S3バケットに保存されたログも、ライフサイクルポリシーの対象となります。これにより、不要なストレージコストを削減できます。

詳細については、「Amazon Glacier」および「AWSでコンプライアンスアーカイブを設定する」を参照してください。

ハイブリッドシナリオ

このセクションは、大規模なハイブリッド環境を使用する開発者向けです。たとえば、開発者がAmazon EC2インスタンス、スタンドアロンサーバー、仮想マシン、データベースがバックアップされる環境を管理しているとします。この環境には1,000台のサーバーがあります。オペレーティングシステム、ファイルデータ、仮想マシンイメージ、およびデータベースがバックアップされます。バックアップ対象のデータベースは20種類あります（MySQL、Microsoft SQL Server、Oracleが混在しています）。バックアップソフトウェアには、オペレーティングシステム、仮想マシンイメージ、データボリューム、SQL Serverデータベース、Oracleデータベース（RMANを使用）をバックアップするエージェントがあります。MySQLなどのアプリケーションで、バックアップソフトウェアにエージェントがない場合、mysqldumpクライアントユーティリティを使用してディスクにデータベースダンプファイルを作成できます。その後、標準のバックアップエージェントでデータを保護できます。使用しているサードパーティのバックアップソフトウェアでは、この環境を保護するために、バックアップ、アーカイブ、および回復アクティビティを制御するグローバルカタログサーバーまたはマスターサーバー、あるいは複数のメディアサーバーを備えている場合があります。このサーバーは、ディスクベースのストレージ、リニアテープオープン（LTO）テープドライブ、およびAWSストレージサービスに接続できます。このバックアップソリューションをAWSストレージサービスで強化するには、開発者はAmazon S3またはAmazon Glacierを使用しているバックアップベンダーの使用を検討する必要があります。Amazonでは、ベンダーと連携して、統合とコネクターのオプションを把握することを提案しています。AWSを使用しているバックアップソフトウェアベンダーのリストについては、AWSパートナーディレクトリを参照してください。

既存のバックアップソフトウェアがバックアップまたはアーカイブのためのクラウドストレージをネイティブでサポートしていない場合は、ストレージゲートウェイデバイスを使用できます。このストレージゲートウェイは、バックアップソフトウェアとAmazon S3またはAmazon Glacierの間のブリッジとして機能します。サードパーティのゲートウェイソリューションは数多くあります。AWS Storage Gateway仮想アプライアンスは、iSCSIベースのボリュームや仮想テープライブラリ（VTL）などの一般的な技術を使用しているため、このギャップを埋めるために使用できます。この構成でアプライアンスをホストするには、サポートされているハイパーバイザー（VMwareまたはMicrosoftHyper-V）とローカルストレージが必要です。

破壊

データを正しく削除するには、開発者は、ライブデータストアだけでなく、そのデータのバックアップやその他のコピーからもデータを削除する必要があります。つまり開発者は、こうしたバックアップやコピーに対して適切な、ビジネスの目的と一致した保持メカニズムを設定する必要があります。**データの匿名化は、Amazonの情報の削除に対して適正な方法とはみなされません。**たとえば、AmazonのカスタマーPIIをハッシュしてデータストアで匿名化することは、Amazonの情報を削除するためのオプションとしては認められません。

Amazonのデータ破壊基準

このセクションでは、データが安全に削除されたとみなされるAmazonの最低基準を示します。

ケース1 – データを直接管理している場合
開発者がデータを直接管理している場合（たとえば、永続的な保存の際にクラウドサービスではなくインスタンスにデータを保存している場合）、データを安全に削除するには、次の3つのことを行う必要があります。

1. 業界標準に準拠して、データへのアクセスに使用できるAPIやその他の既存のメカニズムを使用して、お客様がデータを回復できないようにします。
2. 業界標準に準拠して、データの論理的関連付けを解除します（ポインタを削除したり、データへのinodeのリンクを解除したりするなど）。このアクションは通常、最初の条件と重複します。
3. 業界標準に準拠して、サービスによって再割り当てされる、削除されたデータを含むメディア領域をマークします。

ケース2 – クラウドサービスを使用している場合
データの管理にAmazon S3やAmazon DynamoDBなどのサービスを使用している場合、データを保存するサービスでサポートされている削除メカニズムを、そのサービスで呼び出す必要があります。これは、「削除」APIの使用、または「time to live」メカニズムの実装により行うことができます。サービスアカウントのAmazon S3オブジェクトのポインタの削除およびデータの孤立化は、適正な削除アクションとしてみなされません。

適正なAmazonのデータ破壊の方法

このセクションでは、Amazonのデータを破壊する適正な方法を示します。

Clear操作
Clear操作では、「キーボード攻撃」によりデバイス上のデータの読み取りができなくなります。これは、フォレンジックアプリケーションを使用したユーザーによる攻撃であり、ラボの技術ではありません。Clear操作には、デバイスの上書きパス、ファームウェア消去コマンド、またはNIST SP800-88r1で定義されているその他の方法が1つ以上必要になる場合があります。

Purge操作
Purge操作では、ラボの回復技術によりデバイス上のデータの読み取りができなくなります。Purge操作には、高度なファームウェア消去コマンド、自己暗号化ドライブでのキーのスクランブリング、またはNIST SP800-88r1で定義されているその他の方法が必要になる場合があります。

物理的な破壊
次のサブセクションで説明するように、物理的な破壊には、破砕、粉砕、細断、焼却、消磁などがあります。これにより、デバイス上のデータは回復不能になり、デバイス自体が使用不能になります。

- **消磁**

  消磁とは、磁気メディアの保磁力を上回る強度の磁場を適用することです。これは磁気メディアに対してのみ有効であり、メディアの保磁力はモデルやメーカーによって異なります。開発者は、製造元から直接情報を入手し、消磁器を特定のデバイスに対して適切に適用する必要があります。

- **破砕**

  破砕とは、デバイスに大きな圧縮力を加えて破壊することです。

- **粉砕**

  粉砕とは、デバイスを小さな粒子に砕くことです。

- **細断**

  細断とは、メディアを再収集できない小さな断片に切断することです。最大限の効果を得るには、切断された断片を、データのブロックを保存するのに必要な物理的な領域よりも小さくする必要があります。

- **焼却**

  焼却とは、デバイスに超高温の熱を加え、燃焼や溶融によってデバイスを破壊することです。磁気メディアにキュリー温度以上の熱を加えることも効果的です。

その他のリソース

- Amazon Glacier
- AWSでコンプライアンスアーカイブを設定する
- AWS APNパートナーを探す
- MWSのデータ保護ポリシー
- MWS利用規約

業界の参考資料

- NIST特別刊行物800-88 Rev 1
- 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

ドキュメントの変更履歴

改訂日	内容
2020年1月	初版