AWS における GDPR コンプライアンスに関する情報提供

2018 年 9 月

注意

本書は情報提供のみを目的としています。本書の発行時点における AWS の現行製品と慣行を表したものであり、それらは予告なく変更されることがあります。お客様は本書の情報、および AWS 製品またはサービスの利用について、独自の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本書のいかなる内容も、AWS、その関係者、サプライヤー、またはライセンサーからの保証、表明、契約的責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間の契約に属するものではなく、また、当該契約が本文書によって修正されることもありません。

目次

要約

このドキュメントは、「顧客が一般データ保護規則 (GDPR) に準拠するために、AWS はどのようなサポートを提供するのか」といった疑問に答えることを目的としています。 アマゾン ウェブ サービス (AWS) では、お客様の事業活動が適用対象となり得る GDPR 要件に準拠するための支援となるサービスおよびリソースを提供します。これには、AWS による CISPE 行動規範の遵守、粒度の高いデータアクセスコントロール、モニタリングとログ記録ツール、暗号化、キー管理、監査機能、IT セキュリティスタンダード、AWS のクラウドコンピューティングコンプライアンスコントロールカタログ (C5) 認証の達成が含まれます。

一般データ保護規則: 概要

GDPR はヨーロッパの新しいプライバシー法です。GDPR はEU 加盟各国すべてが準拠義務を負う同一のデータ保護法を適用することで、各国のデータ保護法を統一することを目的としています。
GDPR は、EU 内に所在地を持つすべての組織、および EU 市民の「個人データ」を処理し、EU 内での個人への商品やサービスの提供を行うすべての組織に適用されます。個人データは、特定のあるいは識別可能な自然人に関する情報を指します。

GDPR によって EU 内で活動する組織に適用される変化

GDPR のキーポイントの 1 つが、EU 加盟国間で個人データを安全に処理、使用、やり取りする方法を統一化することを目的としていることです。各組織は、技術的、組織的に適確な措置およびコンプライアンスポリシーを実施し、定期的に見直すことで、処理するデータのセキュリティおよび GDPR への準拠を継続的に証明することを義務付けられます。監督当局が科すことのできる罰金は、最大 2 千万ユーロか、世界市場全体の年間売上高の 4% 相当の額のどちらか高いほうになることがあります。

GDPR に対する AWS の準備

AWS コンプライアンス、データ保護、セキュリティ専門家は、世界中のお客様と協力を重ね、問い合わせにお応えし、GDPR 施行後のクラウド環境におけるワークロードの実行準備を支援してまいりました。また、エキスパートチームは、AWS が実行しているすべての事案について GDPR 要件を準拠しているかを見直しました。

AWS のサービスが GDPR に準拠していることをここに確認いたします。

第 32 条は、管理者と処理者が「適切な技術的、組織的措置の実施」において「実施措置の最新性と実装コスト、処理の種類、範囲、背景と目的、そして自然人の権利と自由に影響を及ぼす可能性があり重大なリスク」について考慮することを義務付けています。GDPR は、求められるセキュリティ措置について、以下に示すような提案を具体的に用意しています。

- 個人データの仮名化と暗号化。
- システムとサービスの処理における継続的な機密性、完全性と復元力を確実にする機能。
- 物理的あるいは技術的事由が発生したときに、適時に個人データの可用性とアクセスを復元する機能。

- 処理過程のセキュリティを確保するための技術的、組織的な措置の効率性を定期的にテスト、査定および評価するプロセス。

AWS データ処理契約 (DPA)

AWS では、GDPR に準拠したデータ処理補遺条項 (GDPR DPA) を規定しており、これがお客様の GDPR 規則の義務への準拠を可能にします。AWS サービス条件が包含する AWS GDPR DPA は、GDPR 準拠が求められる世界中のすべてのお客様に自動的に適用されます。

GDPR における AWS の役割

AWS は GDPR において、データ処理者とデータ管理者の両方として行動します。

- **データ処理者としての AWS ー** お客様と AWS パートナーネットワーク (APN) パートナー が AWS のサービスを使用して、コンテンツ内で個人データを処理する際は、AWS はデータ処理者として行動します。お客様と APN パートナーは、個人データ取扱いの目的で、セキュリティ設定の管理など AWS のサービスで使用可能な管理権限を行使します。そのような場合、お客様または APN パートナーは、データ管理者またはデータ処理者として行動する場合があります。また、AWS はデータ処理者またはデータ副処理者として行動します。AWS は、データ処理者として、AWS のコミットメントに含まれている GDPR に準拠したデータ処理補遺条項 (DPA) を用意しています。
- **データ管理者としての AWS ー** AWS が個人データを収集し、その個人データを処理する目的と方法を決定した場合、たとえばアカウント登録、管理、サービスへのアクセスの目的でアカウント情報を保存したり、カスタマーサポート活動の一環として支援のために AWS アカウントの連絡先情報を保存した場合、AWS はデータ管理者として行動します。

CISPE 行動規範

GDPR は行動規範の認証を規定して、管理者と処理者がコンプライアンスとベストプラクティスを証明することを支援します。公的認証が期待される規範の 1 つがクラウドインフラストラクチャサービスプロバイダー用の行動規範である CISPE (「規範」) です。この規範は、クラウドプロバイダーが GDPR に準拠した適切なデータ保護標準を採用しているという安心感をカスタマーに提供します。この規範には次の重要な利点があります。

- データ保護に関しては、誰が何に対して責任を負うかを明らかにしています。行動規範は、GDPR におけるプロバイダーとカスタマー双方の役割をクラウドインフラストラクチャサービスのコンテキストに絞って説明しています。
- 行動規範は、プロバイダーが準拠すべき原則を規定しています。行動規範は、カスタマーの準拠を支援する目的でプロバイダーが採用すべき明確な行動と責任に関する GDPR における重要な原則を構築しています。カスタマーは独自のコンプライアンスおよびデータ保護戦略に、これらの具体的な利点を活用できます。

- 行動規範は、コンプライアンスに関する意思決定のためにカスタマーが必要とするセキュリテイ情報を提供します。行動規範は、プロバイダーはセキュリティの責任において採用する手順を明示することを求めています。この手順の例としては、データ侵害、データ削除、サードパーティーによる準処理に関する通知、さらには法執行機関および国家機関の要件に関するものが含まれます。カスタマーはこの情報を使用して、提供される高レベルのセキュリティを完全に理解できます。

2017 年 2 月 13 日時点で AWS は、Amazon EC2、Amazon Simple Storage Service (Amazon S3)、Amazon Relational Database Service (Amazon RDS)、AWS Identity and Access Management (IAM)、AWS CloudTrail および Amazon Elastic Block Store (Amazon EBS) がこの規範を完全に履行していることを宣言します (https://cispe.cloud/publicregister を参照してください)。これにより、当社のお客様は、AWS 使用時にデータを安全、セキュアかつ準拠した環境で完全に制御しているという付加的な保証が得られます。当社の同規範への準拠は、ISO 27001、ISO 27018、ISO 9001、SOC 1、SOC 2、SOC 3、PCI DSS Level 1 など、AWS が履行済みの多数の国際認証および認定のリストに追加されるものとなります。

データアクセス制御

GDPR 第 25 条は、管理者が「適切な技術的および組織的措置を実施することで、原則として、特定の処理目的ごとに必要な個人データのみが処理されることを確保しなければならない」と定めています。 以下の AWS のアクセスコントロールメカニズムは、AWS リソースとカスタマーデータへのアクセスを認証されたシステム管理者、ユーザー、アプリケーションに限ることで、お客様のこの要件への準拠を支援する役割を果たします。

- **S3-バケット/SQS/SNS およびその他における AWS オブジェクトへの粒度の高いアクセス権限 –** 異なるリソースへの異なるアクセス権限を異なる人に付与できます。たとえば、一部のユーザーに、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Simple Storage Service (Amazon S3)、Amazon DynamoDB、Amazon Redshift やその他の AWS サービスへの完全なアクセスを許可できます。他のユーザーには、一部の S3 バケットへの読み取り専用アクセス、一部の EC2 インスタンスのみへの管理アクセス、または請求情報のみへのアクセスを許可できます。
- **Multi-Factor-Authentication (MFA) –** アカウントおよび個々のユーザーに 2 要素認証を追加することで、セキュリティを強化できます。MFA を使用すると、ユーザーはお客様のアカウントで使用しているパスワードまたはアクセスキーの入力だけでなく、特別に設定されたデバイスからのコードの入力も必要になります。
- **API リクエスト認証 –** IAM 機能を使用して、EC2 インスタンスで動作

するアプリケーションに、S3 バケット、RDS、DynamoDB データベースなど、その他の AWS リソースにアクセスするために必要な認証情報を安全に付与できます。

- **地域制限 –** 地域制限 (地理的ブロッキング) を使用すると、CloudFront ウェブディストリビューションを通じて配信しているコンテンツについて、特定地域のユーザーによるアクセスを回避できます。地域制限を使用するには、次の 2 つの方法があります。
  - CloudFront の地理制限機能を使用する。ディストリビューションに関連するすべてのファイルへのアクセスを制限し、国レベルでアクセスを制限する場合は、この方法を使用します。
  - サードパーティーの位置情報サービスを使用する。ディストリビューションに関連するファイルのサブセットへのアクセスを制限する場合や、国レベルより粒度の高いレベルでアクセスを制限する場合は、この方法を使用します。
- **STS を通じた一時的アクセストークン –** AWS Security Token Service (AWS STS) を使用すると、AWS リソースへのアクセスを制御できる一時的セキュリティ認証情報を持つ、信頼されたユーザーを作成および提供することができます。一時的セキュリティ認証情報の機能は、IAM ユーザーが使用できる長期的なアクセスキー認証情報とほとんど同じですが、次の相違点があります。
  - 一時的セキュリティ認証情報は、その名前が示すとおり、使用期限が短くなっています。有効期限は数分から数時間に設定できます。認証情報が失効すると、AWS はそれらを認識しなくなり、また、その認証情報によって作成された API リクエストによるあらゆるタイプのアクセスが許可されなくなります。
  - 一時的セキュリティ認証情報はユーザーとともに保存されることはなく、ユーザーのリクエストに応じて動的に生成され、提供されます。一時的セキュリティ認証情報が失効すると (または失効する前でも)、ユーザーは新しい認証情報をリクエストできます。ただし、リクエストするユーザーがまだその権限を持っている場合に限ります。

  これらの違いから、一時的認証情報を使用する利点は次のようになります。
  - アプリケーションに長期の AWS セキュリティ認証情報を配布したり埋め込んだりする必要はありません。
  - ユーザーに対して AWS の ID を定義する必要なく、AWS リソースへのユーザーアクセスを提供できます。一時的認証情報はロールおよび ID フェデレーションの基本となります。
  - 一時的セキュリティ認証情報の有効期限は限られているので、認証情報が不要になった際にローテーションしたり、明示的に取り消したりする必要がありません。一時的セキュリティ認証情報の有効期限が切

れると、再利用することはできません。認証情報が有効な期間を、最大限度まで指定できます。

モニタリングとロギング

GDPR は、「各管理者、および該当する場合には管理者の代表者は、その責任において処理活動の記録を維持する」ことを義務付けています。また、この条項には記録すべき情報の詳細が含まれています。言い換えれば、GDPR は PII データの処理をモニタリングすることを義務付けています。これに加え、タイムリーな違反通知義務により、インシデントはほぼリアルタイムで検知されることが必要です。お客様が以上の義務を履行できるように、AWS は複数のモニタリングおよびログ記録サービスを提供します。

- **AWS Config を使用したアセットマネジメントと設定** – AWS Config は、AWS アカウントの AWS リソースの設定の詳細な表示を提供します。これには、リソース間の関係と設定の履歴が含まれるため、時間の経過とともに設定と関係がどのように変わるかを確認できます。
  AWS リソースとは、たとえば Amazon Elastic Compute Cloud (EC2) インスタンス、Amazon Elastic Block Store (EBS) ボリューム、セキュリティグループ、Amazon Virtual Private Cloud (VPC) などの AWS で使用できるエンティティです。AWS Config でサポートされる AWS リソースの完全なリストについては、「サポートされている AWS リソースタイプ」を参照してください。
  AWS Config では、以下を実行できます。
  - AWS リソースの設定が最適な設定であるかどうかを評価する。
  - AWS アカウントに関連付けられているサポート対象リソースの現在の設定のスナップショットを取得する。
  - アカウント内にある 1 つ以上のリソースの設定を取得する。
  - 1 つ以上のリソースの設定履歴を取得する。
  - リソースが作成、変更、または削除されるたびに通知を受け取る。
  - リソース間の関係を表示する(特定のセキュリティグループを使用するすべてのリソースを確認する場合など)。
- **AWS CloudTrail を使用したコンプライアンスの監査とセキュリティ分析 –** AWS CloudTrail を使用すると、アカウントで行った AWS API 呼び出しの履歴を取得することで、クラウドへの AWS デプロイをモニタリングできます。これには、AWS マネジメントコンソール、AWS SDK、コマンドラインツール、および高レベルの AWS サービスを経由して行われた API 呼び出しが含まれます。CloudTrail に対応するサービスの AWS API を呼び出したユーザーやアカウント、呼び出し元であるソース IP アドレ

ス、呼び出しが発生した時間を特定できます。CloudTrail と API を使用しているアプリケーションとの統合、組織の証跡作成の自動化、証跡のステータスのチェック、および管理者が CloudTrail ロギングを有効または無効にする方法の制御を行うことができます。

- **TrustedAdvisor による設定の課題の洗い出し –** ログ記録は S3 バケットに保存されているデータに詳細なアクセスログの配信を提供します。アクセスログには、リクエストのタイプ、リクエストに指定されたリソース、リクエストが処理された日時など、リクエストの詳細が記録されます。ログの内容に関する詳細については、『Amazon Simple Storage Service 開発者ガイド』でサーバーアクセスログの形式を参照してください。
- サーバーアクセスログから、バケット所有者の制御下にないクライアントからのリクエストの特性について理解できるため、多くのアプリケーションにとって有用です。デフォルトでは、Amazon S3 はサービスアクセスログを収集しませんが、ログ記録を有効にすると Amazon S3 は 1 時間ごとにバケットにアクセスログを配信します。
- S3 オブジェクトへのアクセスの粒度の高いログ記録
- VPC-FlowLogs によるネットワーク内のフローに関する詳細情報
- AWS Config ルールによるルールベースの設定チェックとアクション
- CloudFront の WAF 関数によるアプリケーションへの HTTP アクセスのフィルタリングとモニタリング

AWS におけるデータの保護

GDPR は、組織が「(...) 個人データの仮名化と暗号化 (...) を含む適切な技術的および組織的措置を実施することで、リスクに対応するセキュリティレベルを確保する」ことを義務付けています。また、組織は個人データの不正な開示あるいはアクセスに対する安全策を講じる必要があります。最終的に個人データ違反が発生し、自然人の権利と自由に大きなリスクが生じる結果となる危険がある場合でも、管理者が「暗号化などの適切な技術的および組織的保護措置 (...)」を講じている場合には、管理者は違反の影響を受けるデータ対象者に通知する必要はなく、これによって管理コストおよび信用の棄損を回避できます。AWS は、AWS で保管され処理されるカスタマーデータの保護に役立つ複数の高度にスケーラブルで安全なデータ暗号化メカニズムを提供しています。

暗号化: AWS におけるデータを暗号化する

- **AES256 (EBS/S3/Glacier/RDS) による保管時のデータの暗号化 –** 保管時のデータの暗号化は、ディスクに保存された機密データが有効なキーを持たない、いかなるユーザーまたはアプリケーションからも読み取り不可であることを確保するための法規制準拠においてとても重要です。AWS は、暗号化プロセスをサポートする保管時のデータオプション

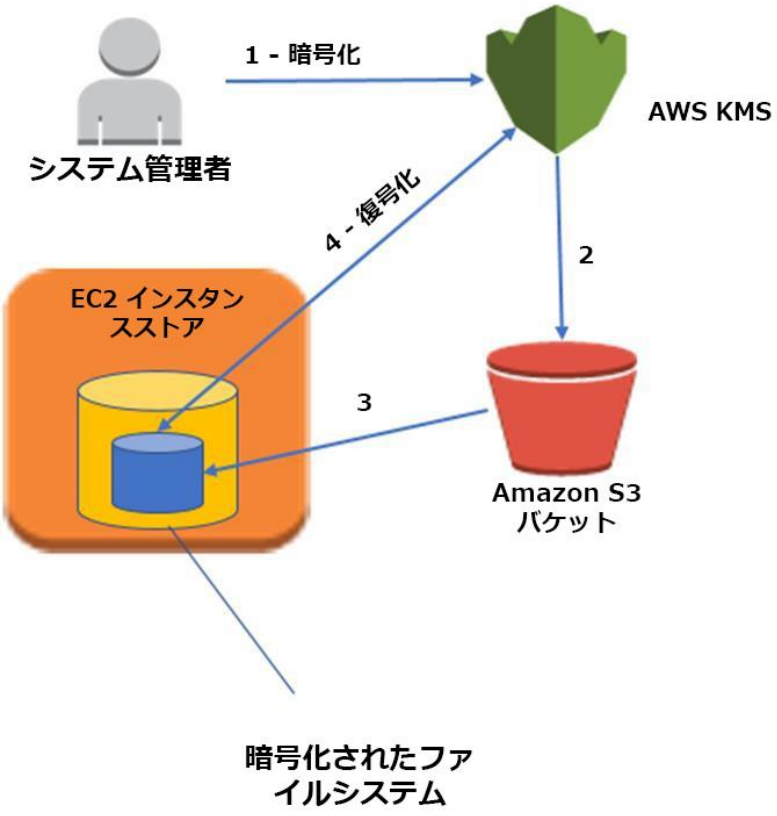
およびキー管理を提供しています。たとえば、AES-256 暗号化を使用して、Amazon EBS ボリュームを暗号化し、サーバー側の暗号化 (SSE) 用の Amazon S3 バケットの設定ができます。加えて、Amazon RDS は透過的なデータ暗号化 (TDE) をサポートしています。

インスタンスストレージは、Amazon EC2 インスタンス用のブロックレベルの一時ストレージを提供します。このストレージは、ホストコンピュータに物理的にアタッチされたディスク上にあります。インスタンスストレージは、バッファ、キャッシュやスクラッチデータなど、頻繁に変化する情報の一時ストレージに最適です。デフォルトでは、このディスクに保存されるファイルは暗号化されません。Linux EC2 インスタンスストアにあるデータの暗号化メソッドでは、Linux 組み込みライブラリが使用されています。このメソッドでは透過的にファイルを暗号化することで、機密データを保護します。その結果、データを処理するアプリケーションではディスクレベルの暗号化が認識されません。

- **ディスクとファイルシステムの暗号化 –** インスタンスストアでは 2 つのファイル暗号化メソッドを使用できます。まず 1 つ目はディスクの暗号化です。1 つ以上の暗号化キーを使用して、ディスク全体あるいはディスク内のブロックを暗号化します。ディスクの暗号化はファイルシステムレベル下で作動し、オペレーティングシステムに依存せず、ディレクトリおよび名前やサイズなどのファイル情報を隠します。たとえば、ファイルシステムの暗号化は、ディスクの暗号化を提供する Microsoft 拡張子である Windows NT オペレーティングシステムの新しいテクノロジーファイルシステム (NTFS) です。
  2 つ目のメソッドは、ファイルシステムレベルの暗号化です。ファイルとディレクトリは暗号化されますが、ディスク全体やパーティションは暗号化されません。ファイルシステムレベルの暗号化はファイルシステムの上位で作動し、オペレーティングシステム間で移動可能です。
- **Linux dm-crypt インフラストラクチャ –** Dm-crypt は、Linux カーネルレベルの暗号化メカニズムです。暗号化されたファイルシステムのマウントができます。ファイルシステムのマウントは、ファイルシステムがディレクトリにアタッチ (マウントポイント) し、オペレーティングシステムで利用可能にするプロセスを指します。マウント後、ファイルシステムのすべてのファイルは、追加の操作の必要なくアプリケーションで利用可能となりますが、これらのファイルはディスクに保存される際に暗号化されます。
  デバイスのマッパーとは、ブロックデバイスの仮想レイヤーを作成する一般的な方法を提供する Linux 2.6 および 3.x カーネルのインフラストラクチャのことです。デバイスマッパー暗号ターゲットは、カーネル暗号化 API を使用したブロックデバイスの透過的暗号化を提

供します。このポストのソリューションでは、dm-crypt を Logical Volume Manager (LVM) によって倫理ボリュームにマップされたバックアップディスクファイルシステムと合わせて使用します。LVM は、Linux カーネル用の倫理ボリューム管理を提供します。

- **アーキテクチャの概要 –** 以下の高レベルアーキテクチャダイアグラムは、EC2 インスタンスストアの暗号化を可能にするために提案されたソリューションを示しています。詳細な実装計画は、次のセクションで紹介します。



1. 管理者は、KMS を使用してシークレットパスワードを暗号化します。暗号化されたパスワードはファイルに保存されます。
2. 管理者は、暗号化されたパスワードがあるファイルを S3 バケットに置きます。
3. インスタンスブート時に、インスタンスは暗号化されたファイルを内部ディスクにコピーします。
4. 続いて、EC2 インスタンスは KMS を使用してファイルを復号化し、プレーンテキストのパスワードを取得します。このパスワードは、Linux 暗号化ファイルシステムを LUKS で設定するために使用します。暗号化されたファイルシステムに書き込まれたすべてのデータは、ディスク保存時に AES-256 暗号化アルゴリズムを使用して暗号化されます。

- **一元 (リージョンごと) 管理の Key-Management –** AWS Key Management Service (KMS) とは、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージドサービスで、キーのセキュリティを保護するために Hardware Security Modules (HSM) を使用します。AWS Key Management Service は、AWS の他のいくつかのサービスと統合されており、これらのサービスに保存したデータが保護されます。また AWS Key Management Service は AWS CloudTrail とも統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。
  - **一元化 Key Management –** AWS Key Management Service は、暗号化キーの一元化管理を提供します。AWS マネジメントコンソールから、または AWS SDK か CLI を使用して、キーを簡単に作成、インポート、ローテーションすること、さらに使用ポリシーを定義し、使用を監査することができます。ユーザーが自身でインポートしたか、KMS により作成されたかに関わらず、KMS のマスターキーは必要なときに取得できるように、暗号化された形式で高い耐久性を持つストレージに格納されます。1 年ごとに KMS が自動的にマスターキーを更新するように設定できます。この場合は、マスターキーで暗号化済みのデータを再度暗号化する必要はありません。KMS によって以前の暗号化データを復号化できるため、マスターキーの旧バージョンを追跡する必要はありません。新しいマスターキーを作成し、そのキーにアクセスできるユーザー、利用できるサービスをいつでも制限できます。また、独自のキー管理インフラストラクチャからキーをインポートして、KMS で使用できます。
  - **AWS サービス統合 –** AWS Key Management Service は、他のいくつかの AWS サービスとシームレスに統合されています。この統合により、AWS KMS マスターキーを使用して、これらのサービスに保存したデータを簡単に暗号化できます。自動的に作成され、統合されたサービス内でのみ使用可能なデフォルトのマスターキーを使用することも、KMS で作成した、または独自のキー管理インフラストラクチャからインポートしたカスタムのマスターキーを選択することもできます。
  - **機能監査 –** AWS アカウントに AWS CloudTrail を有効化している場合には、KMS に保存する各キー使用はログファイルに記録され、AWS CloudTrail を有効化した際に指定した Amazon S3 バケットに配信されます。記録される情報はユーザーの詳細、時間、日付、使用されたキーなどです。
  - **スケーラビリティ、耐久性、高可用性 –** AWS Key Management Service はマネージドサービスです。AWS KMS 暗号化キーの使用

量が増えても、キー管理インフラストラクチャを追加購入する必要はありません。AWS KMS は暗号化キーのニーズに合わせて自動でスケールします。
AWS KMS により作成されたマスターキーまたはインポートされたマスターキーは、サービスからエクスポートすることはできません。AWS KMS はキーの複数の暗号化バージョンを 99.999999999% の耐久性で設計されたシステムに保存しており、常にキーにアクセスして利用できます。KMS にキーをインポートする場合は、いつでも再インポートできるように、キーのコピーを安全に保持する必要があります。
AWS KMS は AWS リージョンの複数のアベイラビリティーゾーンにデプロイされており、暗号化キーに高可用性を提供しています。

- **安全性 –** AWS KMS は、誰もマスターキーにアクセスできないように設計されています。このサービスは、プレーンテキストのマスターキーを決してディスクに保存しない、メモリにマスターキーを残さない、キーを使用するホストにアクセスできるシステムを制限するなどの広範囲にわたってハードニングしたテクニックによるマスターキーの保護を目的として設計されたシステム上に構築されています。サービス内でソフトウェアをアップデートしようとするすべてのアクセスは複数の関係者によって管理され、このプロセスは Amazon 内の独立したグループによって監査およびレビューされます。
AWS KMS の機能に関する詳細については、AWS Key Management Service に関するホワイトペーパーをご覧ください。

- **VPN ゲートウェイによる AWS への IPsec トンネル –** Amazon VPC は、定義する仮想ネットワークで AWS リソースを起動できるアマゾン ウェブ サービス (AWS) クラウドの論理的に分離したセクションを確保します。独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。また、会社のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成できるので、AWS クラウドを貴社の既存のデータセンターの延長として活用できます。
Amazon VPC のネットワーク設定は容易にカスタマイズすることができます。たとえば、インターネットへのアクセスがあるウェブサーバーのパブリックサブネットを作成し、データベースやアプリケーションサーバーなどのバックエンドシステムをインターネットアクセスがないプライベートサブネットに配置できます。セキュリティグループやネットワークアクセスコントロールリストなどの複数のセキュリティレイヤーを活用し、各サブネットの Amazon EC2 インスタンスへのアクセスをコントロールすることができます。

- **CloudHSM によるクラウドの HSM 専用モジュール –** AWS CloudHSM サービスは、AWS クラウド内の専用ハードウェアセキュリティモジュール (HSM) アプライアンスを使用して、データセキュリティに対する企業コンプライアンス要件、契約上のコンプライアンス要件、および法令遵守の要件を満たすようサポートします。CloudHSM を使用して、暗号化キーや HSM によって実行される暗号化操作を管理します。
  AWS および AWS Marketplace のパートナーにより、AWS プラットフォーム内の重要なデータを保護するためのさまざまなソリューションが用意されています。しかし、暗号化キーの管理に関する厳格な契約上の要件や法律的な要件が課せられたアプリケーションとデータに対しては、さらなる保護が必要になることがあります。これまで、機密データ (またはそれを保護する暗号化キー) はオンプレミスのデータセンターに保管するという選択肢しかありませんでした。困ったことに、これではアプリケーションをクラウドに移行させることはできず、アプリケーションのパフォーマンスも非常に低いものでした。AWS CloudHSM サービスにより、安全なキー管理に対する米国政府標準規格に適合するように設計/検証された HSM 内で暗号化キーを保護することができるようになります。データ暗号化に使用される暗号化キーを安全に生成、保存、管理することで、ユーザーだけが暗号化キーにアクセスできるようになります。AWS CloudHSM により、アプリケーションのパフォーマンスを低下させることなく、厳密なキー管理要件に準拠することができます。
  AWS CloudHSM サービスは Amazon Virtual Private Cloud (VPC) とともに動作します。CloudHSM インスタンスは、ユーザーが指定した IP アドレスで VPC 内にプロビジョニングされます。これにより、Amazon Elastic Compute Cloud (EC2) インスタンスに対してシンプルなプライベートネットワーク接続が可能になります。CloudHSM インスタンスを EC2 インスタンスの近くに配置することで、ネットワークレイテンシーは低減され、アプリケーションのパフォーマンスが向上します。AWS は、他の AWS ユーザーとは分離した、CloudHSM インスタンスへの排他的な専用 (シングルテナント) アクセスを提供します。複数のリージョンとアベイラビリティーゾーン (AZ) で利用可能な AWS CloudHSM により、お客様のアプリケーションに安全で耐久性のあるキー保存を実現することができます。
  - **統合 –** CloudHSM は、Amazon Redshift、Amazon Relational Database Service (RDS) Oracle、「ルートオブトラスト」として行動する SafeNet Virtual KeySecure、Apache (SSL ターミネーション) や Microsoft SQL Server (透過的データ暗号化) などのサードパーティーのアプリケーションとともに使用できます。また、独自のアプリケーションを構築し、PKCS#11、Java JCA/JCE、Microsoft

CAPI および CNG などの使い慣れたスタンダード暗号化ライブラリを継続して使用する場合にも、CloudHSM を使用できます。

- **監査可能 –** リソースの変更追跡、またはセキュリティおよびコンプライアンス目的でアクティビティ監査が必要な場合、CloudTrail によりアカウントから行われた CloudHSM API 呼び出しのすべてを確認することができます。さらに、syslog を使用して HSM アプライアンスについての操作を検査したり、syslog ログメッセージを独自のコレクターに送信したりすることも可能です。

強力なコンプライアンスフレームワークとセキュリティスタンダード

GDPR に従い、適切な技術的および組織的措置には「処理するシステムおよびサービスの現存の機密性、完全性、可用性と回復性を確実にする機能」、そして信頼できる復元、テスト、全体的なリスクマネジメントプロセスを含める必要性が生じることがあります。AWS では、強力なコンプライアンスフレームワークと高度なセキュリティスタンダードをお客様に提供しています。

責任分担セキュリティモデル

AWS がデータのセキュリティをどのように確保するかを詳しく説明する前に、クラウドのセキュリティがオンプレミスデータセンターのセキュリティとは少し異なるということを説明する必要があります。コンピュータシステムとデータをクラウドに移行する場合、セキュリティについてはお客様とクラウドサービスプロバイダーが共同で責任を負います。この場合、クラウドをサポートする基盤インフラストラクチャのセキュリティ保護は AWS が担い、クラウドに置かれるリソースやクラウドに接続する手段についてはお客様が責任を負います。このセキュリティ責任分担モデルにより、多くの面でお客様の運用の負担が軽減されるだけでなく、追加の対策を行わなくても現状のセキュリティ体制を強化できる場合さえあります。

セキュリティに関する AWS の責任

アマゾン ウェブ サービスは、AWS クラウドで提供されるすべてのサービスを実行するグローバルインフラストラクチャの保護を担います。このインフラストラクチャは、AWS サービスを実行するハードウェア、ソフトウェア、ネットワーキング、および施設で構成されます。このインフラストラクチャの保護は AWS の最優先事項です。お客様は当社のデータセンターやオフィスを訪れてこの保護を直接確認することができない代わりに、サードパーティーの監査人による複数のレポートを受け取ることができます。監査人は、当社がコンピュータセキュリティに関するさまざまな基準や規制に準拠していることを証明しています (詳細な情報については、aws.amazon.com/compliance をご覧ください)。このグローバルインフラストラクチャの保護に加え、AWS はマネージドサービスとみなされる AWS 製品のセキュリティ設定についても責任を負います。このタイプのサービスには、Amazon DynamoDB、Amazon RDS、Amazon Redshift、Amazon Elastic MapReduce、Amazon WorkSpaces などがあります。これらのサービスには、クラウドベースリソースの拡張性と柔軟性だけでなく、マネージドサービスとしての利点もあります。これらのサービスについては、ゲストオペレーティングシステム (OS) やデータベースのパッチ適用、ファイアウォールの設定、災害対策などの基本的なセキュリティタスクを AWS が行いま

す。ほとんどの場合、これらのマネージドサービスでお客様が行う作業は、リソースの論理アクセスコントロールを設定してアカウントの認証情報を保護することだけです。一部のサービスでは、データベースユーザーアカウントの設定などの追加タスクが必要になる場合がありますが、全般的なセキュリティ設定作業はサービスに含まれています。

セキュリティに関するお客様の責任

AWS クラウドでは、通常なら数週間かかる仮想サーバー、ストレージ、データベース、およびデスクトップのプロビジョニングを数分で完了できます。また、必要に応じてクラウドベースの分析やワークフローツールを使用してデータを処理し、そのデータを独自のデータセンターやクラウドに保存することもできます。セキュリティに関してお客様の責任で行う設定作業の必要性は、どの AWS サービスを利用するかによって決まります。

Infrastructure as a Service (IaaS) の上級者向けカテゴリに属する AWS 製品 (Amazon EC2、Amazon VPC、Amazon S3 など) の場合、管理は完全にお客様の責任となり、必要なセキュリティ設定と管理タスクもすべてお客様自身で行う必要があります。たとえば、EC2 インスタンスの場合、ゲスト OS の管理 (アップデートやセキュリティパッチの適用を含む)、各インスタンスにインストールしたアプリケーションソフトウェアやユーティリティ、各インスタンスに AWS が提供するファイアウォール (セキュリティグループ) の設定は、お客様がその責任を負います。これは、サーバーの設置場所が異なるだけで、これまでに実行してきたセキュリティタスクと基本的には同じです。

Amazon Relational Database Service (RDS) や Amazon Redshift といった AWS マネージドサービスには特定のタスクの実行に必要なすべてのリソースが含まれており、それらに伴う設定作業も必要ありません。マネージドサービスでは、インスタンスの起動や管理、ゲスト OS やデータベースのパッチ適用、データベースのレプリケートなどに頭を悩ませる必要はありません。お客様に代わって AWS がこれらを行います。ただし、ユーザーに個々の認証情報を付与して役割分担を行えるように、Amazon Identity and Access Management (IAM) による AWS アカウント認証情報の保護と個々のユーザーアカウントの設定は、他のサービス同様お客様自身で行う必要があります。また、AWS では各アカウントに Multi-Factor Authentication (MFA) を使用し、AWS リソースへのアクセスに SSL/TLS の使用を義務付け、AWS CloudTrail で API/ユーザーアクティビティのログを記録するように設定することを推奨しています。追加で行える対策の詳細については、AWS セキュリティのベストプラクティスに関するホワイトペーパー、および AWS セキュリティリソースウェブページ の推奨する参照情報を参照してください。

AWS コンプライアンスプログラム

アマゾン ウェブ サービスのコンプライアンスにより、クラウドでセキュリティとデータ保護を維持するために AWS に導入されている堅牢な管理について、お客様にご理解いただけるようにしています。システムは AWS クラウドインフラストラクチャの最上部に構築されるため、コンプライアンス上の責任は共有されます。ガバナンスに重点を置き、監査に適したサービス機能を該当するコンプライアンス規格または監査規格と結び付けることで、AWS コンプライアンスの実現を支援するドキュメントは従来のプログラムに基づいて構築されており、お客様が AWS セキュリティ統制環境を確立し、運用するのに役立ちます。AWS がお客様に提供する IT インフラストラクチャは、セキュリティのベストプラクティス、および各種 ITセキュリティ基準に合わせて設計、管理されています。これには、次が含まれます。

- SOC 1/SSAE 16/ISAE 3402 (旧称 SAS 70)
- SOC 2
- SOC 3
- FISMA、DIACAP、FedRAMP
- DoD SRG
- PCI DSS レベル 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Tier 3

さらに、AWS プラットフォームが提供する柔軟性と制御により、お客様は以下のような業界特有の標準を満たすソリューションをデプロイすることができます。

- 犯罪司法情報サービス (CJIS)
- クラウドセキュリティアライアンス (CSA)
- 家族の教育上の権利およびプライバシーに関する法律 (FERPA)
- 医療保険の相互運用性と説明責任に関する法令 (HIPAA)
- アメリカ映画協会 (MPAA)

AWS は、ホワイトペーパー、レポート、認定、認証評価、およびその他のサードパーティーによる証明を通して、当社の IT 統制環境に関するさまざまな情報をお客様に提供しています。詳細については、リスクおよびコンプライアンスホワイトペーパーを参照してください。

クラウドコンピューティングコンプライアンスコントロールカタログ (C5 – ドイツ政府の認証スキーム)

クラウドコンピューティングコンプライアンスコントロールカタログ (C5) は、連邦情報セキュリティ庁 (BSI) によってドイツで導入されたドイツ政府の認証スキームです。これは、ドイツ政府の「クラウドプロバイダーへのセキュリティ勧告」のコンテキスト内での一般的なサイバー攻撃に対して、企業が運用上のセキュリティを実現するのに役立ちます。

C5 認証を使用することにより、AWS のお客様やコンプライアンスアドバイザーはワークロードをクラウドに移行する際、AWS で提供される IT セキュリティ保証サービスの範囲を把握できます。C5 では、クラウド特有のコントロールの追加とともに、IT 基本保護法 (IT-Grundschutz) と同等の規制上定義された IT セキュリティレベルが追加されます。

C5 では、データのロケーション、サービスのプロビジョニング、管轄の場所、既存の認定、情報公開義務、および全サービスの説明に関連した情報を提供する詳細なコントロールも追加されます。この情報を利用することで、お客様はクラウドコンピューティングサービスの使用に関する法規制 (データプライバシーなど)、お客様独自のポリシーや脅威環境の評価を行うことができます。

ドキュメントの改訂

日付	説明
2018 年 9 月	マイナーな更新。
2017 年 11 月	初版発行