日本におけるプライバシーに関する考慮事項に照らした AWS の利用

2018 年 5 月

(本書の最新版については、
を参照してください)

概要

本書は、個人情報を含むコンテンツの保存や処理に AWS を使うことを希望するお客様向けに、プライバシーに関する重要な考慮事項や個人情報の保護に関する法律 (**個人情報保護法**) の観点から役立つ情報を提供します。本書はお客様が以下の内容を理解するために役立ちます。

- AWS のサービスの運用方法 (お客様がセキュリティ対策やコンテンツの暗号化をどのように実施できるかなど)
- お客様がコンテンツの保存場所として選択できる地理的ロケーションと、それに関連する考慮事項
- AWS のサービスに保存されたコンテンツの管理とセキュリティ保護において、お客様と AWS がそれぞれ果たす役割

本書の対象範囲

このホワイトペーパーでは、個人情報を含むコンテンツの保存や処理に AWS を使うお客様が個人情報保護法の影響を考慮する際に一般的に問題となる事項を説明します。各お客様は、本書で取り上げる事項に加えて、業界特有の要件やお客様が事業を行う各地域の法律への準拠、または第三者に対する契約上の責任などについて個別の対応が必要になる場合があります。

本書は情報提供のみを目的としており、法的助言として作成されたものではないため、お客様が本書を法的助言として使用することはできません。要件はお客様ごとに異なるため、プライバシー要件やデータ保護要件への対応についても、お客様の責任において、お客様の事業に適用される法令および他の要件を踏まえたうえで適切な助言を得ることが強く推奨されます。

本書の "コンテンツ" とは、お客様またはエンドユーザーが AWS のサービスを使用して保存または処理するソフトウェア (仮想マシンイメージを含む)、データ、テキスト、音声、動画、画像などを意味します。例えば、Amazon Simple Storage Service を使用してお客様が保存したオブジェクト、Amazon Elastic Block Store ボリュームに保存されたファイル、Amazon DynamoDB データベーステーブルの内容などがお客様のコンテンツとなります。このようなコンテンツには、必ずではありませんが、お客様やお客様のエンドユーザーまたは第三者に関連する個人情報が含まれることがあります。お客様のコンテンツには、AWS カスタマーアグリーメント (または、AWS と合意された、AWS のサービス利用を規定するその他の契約) が適用されます。なお、AWS アカウントの作成または管理に関してお客様が AWS に提供するお客様の会社名、電話番号、電子メールアドレス、請求情報などの情報はお客様のコンテンツには該当しません。これらの情報は、アカウント情報と呼ばれ、AWS プライバシー通知[1] で管理されます。

[1] http://aws.amazon.com/jp/privacy/

お客様のコンテンツ: プライバシーおよびデータ保護に関する考慮事項

コンテンツを保存する場合、どのような組織の業務でも一般的に次のような事項を考慮する必要があります。

- コンテンツのセキュリティは確保されるか?
- コンテンツをどこに保存するか?
- コンテンツへのアクセス権を誰に付与するか?
- コンテンツに適用される法令にはどんなものがあるか? その遵守には何が必要か?

このような考慮事項は、新しいものでもクラウド特有のものでもありません。第三者がホストする従来型のサービスにも、社内でホストされ運用されるシステムにも該当します。いずれの場合も、第三者の機器または第三者の施設にコンテンツが保存される可能性や、そのコンテンツが第三者によって管理、アクセス、または使用される可能性があります。AWS のサービスを使用する場合、コンテンツの所有権と管理権は AWS のお客様側にあるため、以下のような点はお客様側で決定できます。

- どのコンテンツを AWS のサービスを使用して保存または処理するか
- どの AWS のサービスをコンテンツに使用するか
- どのリージョン (1 つまたは複数) にコンテンツを保存するか
- どの形式または構造をコンテンツに適用するか、どのセキュリティ対策を施行するか (マスキング、匿名化、暗号化の有無など)
- お客様の AWS アカウントにおけるコンテンツへのアクセス権を誰に付与するか、そのアクセス権をどのように付与、管理、解除するか

AWS 環境にあるコンテンツの所有権と管理権は AWS のお客様側にあるため、お客様も AWS "責任共有" モデルの一員としてコンテンツのセキュリティに責任を負います。この責任共有モデルは、AWS のサービスを使用して保存や処理を行うとお客様が決定したコンテンツについて、プライバシー要件およびデータ保護要件の観点からお客様と AWS それぞれの役割を理解する際の基礎となります。

クラウドセキュリティの管理に対する AWS 責任共有の考え方

お客様のコンテンツのセキュリティは確保されるか?

IT インフラストラクチャが AWS に移行されると、セキュリティの運用および管理にお客様と AWS の双方が重要な役割を担うことになるため、お客様と AWS は責任共有モデルに従って責任を分担します。AWS が運用、管理、統制する対象は、AWS のサービスを実行する基盤施設の物理的セキュリティに関するコンポーネントから、ホストオペレーティングシステムおよび仮想化レイヤーまでです。お客様の責任の対象は、ゲストオペレーティングシステム (ゲストオペレーティングシステムに適用する更新プログラムおよびセキュリティパッチを含む) と、関連するアプリケーションソフトウェアの管理、ならびに AWS から提供されるセキュリティグループファイアウォールおよびその他のセキュリティ関連機能の構成となります。お客様は一般に、第三者 (例えば、インターネットサービスプロバイダー) から提供されるサービスを経由して AWS 環境に接続します。AWS はこのような接続サービスを提供していないため、これはお客様が責任を負う領域に属します。お客様は、このような接続のセキュリティと、お客様のシステムに関連する第三者のセキュリティに関する責任を考慮する必要があります。責任共有モデルにおけるお客様と AWS のそれぞれの役割を図 1 に示します。

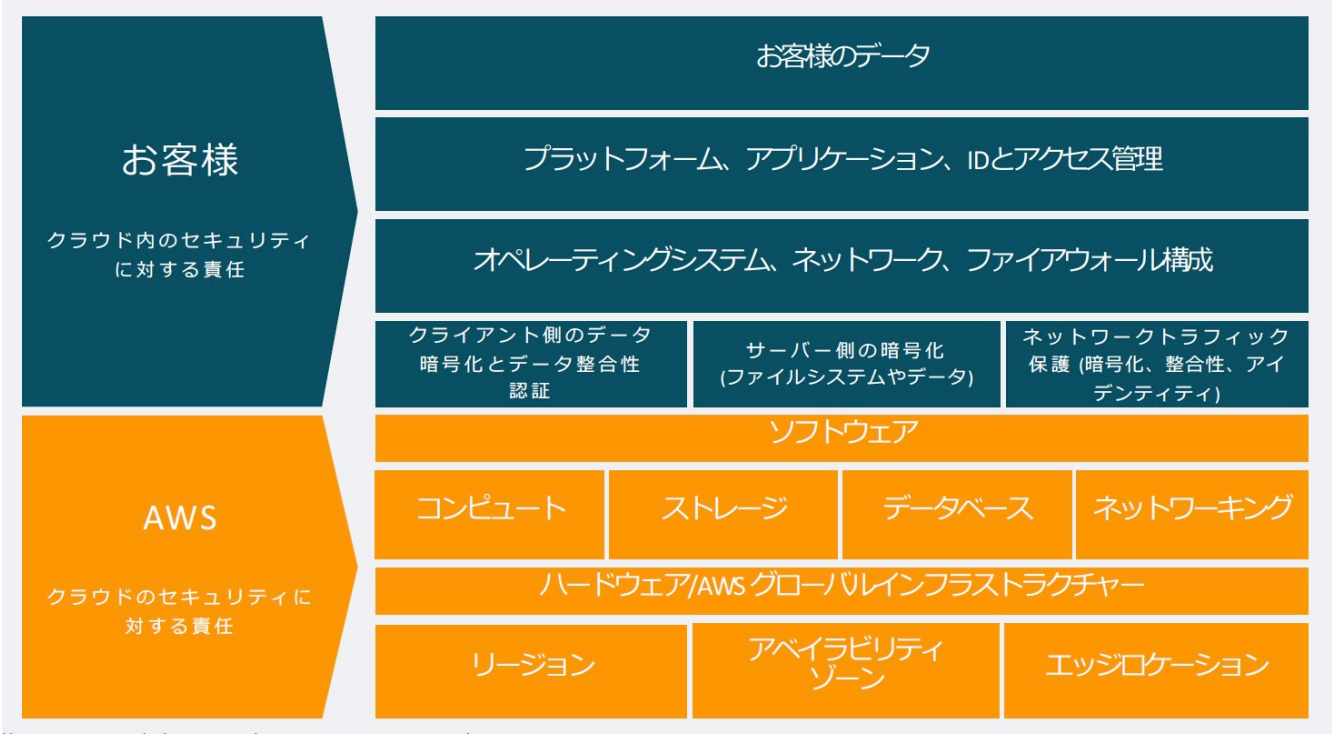


図 1 – 責任共有モデル

お客様のコンテンツのセキュリティに対する責任共有モデルの意味

クラウドソリューションのセキュリティを検討する場合、下記の 2 つを理解し、両者を区別することが重要です。

- クラウドサービスプロバイダー (AWS) が実装および運用するセキュリティ対策 – "クラウド**の**セキュリティ"
- AWS のサービスを使用するお客様のコンテンツとアプリケーションのセキュリティに関連して、お客様が実装および運用するセキュリティ対策 – "クラウド**内の**セキュリティ"

AWS がクラウド**の**セキュリティを管理する一方で、クラウド**内の**セキュリティはお客様の責任となります。お客様が所有するコンテンツ、アプリケーション、システム、ネットワークを保護するためにどのようなセキュリティを実装するかについての決定権はお客様側にあり、この点は社内データセンターと変わりません。

クラウドのセキュリティを理解

AWS は、基盤となるクラウド環境のセキュリティを管理する責任を負います。AWS のクラウドインフラストラクチャのアーキテクチャは、現存のクラウドコンピューティング環境の中で最高レベルの柔軟性と安全性を実現できるよう設計されています。また、設計では、お客様単位で完全に分離しながら、可用性が最適になるように考慮されています。AWS から提供するスケーラビリティと信頼性に優れたサービスによって、お客様はアプリケーションやコンテンツの展開を、迅速かつ安全に、また必要であれば世界規模で行うことができます。

AWS のサービスはあらゆるコンテンツに対応しています。保存するコンテンツの種類やその保存場所に関係なく、すべてのお客様に同じように高度なセキュリティが提供されます。AWS の安全性の高い世界規模のデータセンターでは、最先端技術を用いた電子監視と多要素アクセス制御システムが活用されています。訓練された警備員が 24 時間年中無休で常駐し、アクセス権の許可は最小権限を基準として厳格に管理されています。コアとなる AWS クラウドインフラストラクチャおよびサービスに組み込まれたすべてのセキュリティ対策の一覧については、「セキュリティプロセスの概要[2]」ホワイトペーパーをお読みください。

AWS は、お客様のセキュリティを守るため常に警戒を徹底し、不正アクセスに対して高度な技術的対策や物理的対策を実装しています。AWS 環境内で実施されているセキュリティ制御の有効性については、AWS 認定およびレポート (AWS System & Organization Control (SOC) 1、2[3]、3[4] レポート、ISO 27001[5]、27017[6]、27018[7]、9001[8] 認証および PCI DSS[9] コンプライアンスレポートを含む) で確認できます。AWS の ISO 27018 認証では、AWS がお客様のコンテンツのプライバシー保護に特化した制御システムを提供していることが示されています。これらのレポートおよび認証は、独立した第三者である監査人によって作成され、AWS のセキュリティ制御の設計および運用の効果を証明しています。

[2] https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf
[3] http://aws.amazon.com/jp/compliance/soc-faqs/
[4] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
[5] http://aws.amazon.com/compliance/iso-27001-faqs/
[6] http://aws.amazon.com/compliance/iso-27017-faqs/
[7] http://aws.amazon.com/compliance/iso-27018-faqs/
[8] https://aws.amazon.com/compliance/iso-9001-faqs/
[9] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

AWS のコンプライアンス認証およびレポートについては、https://aws.amazon.com/compliance/contact からご請求ください。AWS のコンプライアンス認証やレポートについての詳細と、ベストプラクティスや規格との整合についての詳細は、AWS コンプライアンス[10] のサイトをご覧ください。

クラウド内のセキュリティを理解

AWS のサービスを使用する場合、コンテンツの所有権と管理権は常にお客様が有します。AWS のサービスを使用して保存や処理するコンテンツを決定するのは、AWS ではなく、お客様です。AWS のサービスを使用して保存または処理するコンテンツの決定権はお客様にあるため、AWS を使用して保存および処理するコンテンツに必要なセキュリティの程度を判断できるのはお客様のみです。どのサービスを使用するか、コンテンツやサービスへのアクセス権を誰に付与するか (どのような認証情報を使うか) についても、お客様に完全な決定権があります。

お客様は、環境の構成方法や、コンテンツに施行するセキュリティ対策 (移動時や保管時の暗号化の有無など) を管理できます。さらに、追加のセキュリティ機能およびツールと、その活用方法も管理できます。お客様の構成設定は、お客様側で決定して管理する設定であるため、AWS 側から変更することはありません。お客様のコンプライアンスのニーズに合わせてセキュリティアーキテクチャを自由に設計できます。プロバイダーがアーキテクチャを決定する従来型のホスティングソリューションとの大きな違いはこの点です。AWS では、いつ、どのようにクラウドのセキュリティ対策を実装するかを、お客様のビジネスニーズに合わせてお客様が決定できます。例えば、お客様のコンテンツを保護するために可用性の高いアーキテクチャが必要な場合は、お客様側でシステム、バックアップ、ロケーション、ネットワークアップリンクなどを冗長化してアーキテクチャの回復性や可用性を高めることができます。また、お客様のコンテンツへのアクセスを制限する必要がある場合は、お客様が AWS を使ってシステム単位での制御やデータ単位での暗号化を実装してアクセス権管理を実施できます。

お客様側で安全な AWS 環境を設計、実装、運用できるように、AWS ではお客様が利用できるセキュリティツールや機能を数多く提供しています。もちろん、お客様独自のセキュリティツールとセキュリティ制御や、サードパーティー製の各種セキュリティソリューションを使用することも可能です。AWS のサービスはお客様側で構成できるので、ID 管理とアクセス管理のツール、セキュリティ防御、暗号化、ネットワークセキュリティなど、高度な機能を実現する多様なセキュリティ機能、ツール、制御を活用してコンテンツを保護することができます。例えば、お客様はコンテンツを保護するために以下のような対策を実施できます。

- アクセスキーの保護対策として、厳しいパスワードポリシーの設定、ユーザーへの適切な権限の割り当て、厳格な手順の徹底を行う。
- データ損失や不正アクセスのリスク低減対策として、適切なファイアウォールの導入とネットワークのセグメント化、コンテンツの暗号化、システムの適切なアーキテクチャ設計を行う。

こうした重要な要素は、AWS ではなくお客様が管理します。そのため、その選択についてはお客様が責任を負います。AWS のサービスを使用して保存または処理するコンテンツや、AWS インフラストラクチャに接続するコンテンツのセキュリティの責任はお客様側にあります。つまり、ゲストオペレーティングシステムや、コンピューティングインスタンス上のアプリケーション、さらに AWS ストレージ、データベースなどのサービスで保存または処理されるコンテンツのセキュリティはお客様の責任となります。

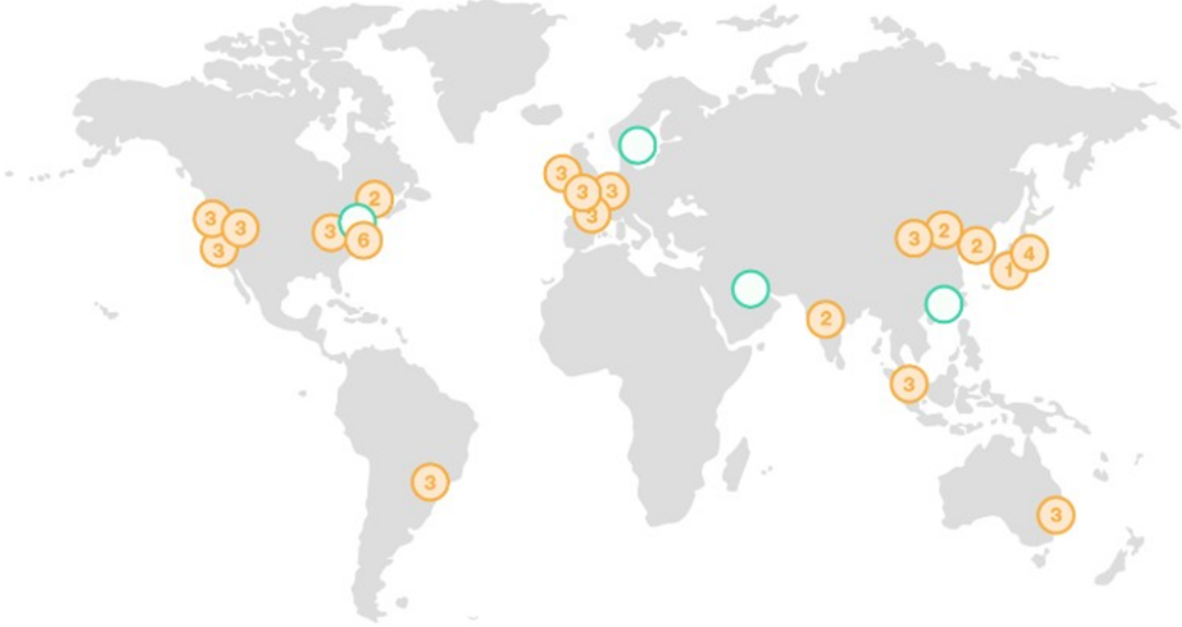
[10] http://aws.amazon.com/jp/compliance/

AWS は、お客様がコンテンツを効果的に管理できるよう、アクセス、暗号化、ログ記録などの高度な機能 (AWS Key Management Service および AWS CloudTrail を含む) を数多く提供しています。また、セキュリティ、ガバナンス、リスク、コンプライアンスに関するホワイトペーパー[11] や、チェックリストおよびベストプラクティスも数多く公開しています。これらの資料を参照して、AWS のセキュリティ制御をお客様の既存の統制フレームワークに統合したり、お客様組織の AWS のサービス利用に対するセキュリティ評価を設計して実行したりすることができます。セキュリティ評価は、個別の組織環境に応じて自由に設計して実行できます。クラウドインフラストラクチャのスキャンを行う権限を要求することもできます。ただし、スキャンの対象はお客様のコンピューティングインスタンスに限定され、AWS 適正利用規約[12] に違反しない範囲に限ります。

[11] https://aws.amazon.com/jp/compliance/#whitepapers
[12] http://aws.amazon.com/jp/aup/

AWS リージョン: コンテンツをどこに保存するか?

AWS のデータセンターは、世界のいくつかの場所にまとめて建設されています。各国内でのデータセンターのかたまりを "AWS リージョン" と呼びます。お客様は、アジアパシフィック (東京) リージョンおよびアジアパシフィック (大阪: ローカル) リージョンを含む、世界中の多くの AWS リージョンにアクセスできます[13]。お客様は、1 つのリージョンを使用するか、すべてのリージョンを使用するか、または任意の AWS リージョンを組み合わせて使用するかを選択できます。図 2 は、2018 年 5 月時点での AWS リージョンのロケーションを示しています。[14]



リージョンと、そのアベイラビリティーゾーン数

米国東部
バージニア北部 (6)、
オハイオ (3)

米国西部
北カリフォルニア (3)
オレゴン (3)

アジアパシフィック
ムンバイ (2)
ソウル (2)
シンガポール (3)
シドニー (3)
東京 (4)
大阪: ローカル (1)

カナダ
中部 (2)

中国
北京 (2)、
寧夏 (2)

欧州
フランクフルト (3)
アイルランド (3)
ロンドン (2)
パリ (3)

南米
サンパウロ (3)

AWS GovCloud (US-West) (3)

新しいリージョン (近日追加予定)

バーレーン

香港特別行政区、中国

スウェーデン

AWS GovCloud (US-East)

図 2 – AWS のグローバルリージョン

[13] AWS GovCloud (US) は独立した AWS リージョンとして設計されており、米国の政府機関やお客様が機密性の高いワークロードをクラウドに移行できるよう、該当する規制およびコンプライアンス要件に対応しています。AWS 中国 (北京) リージョンも独立した AWS リージョンです。AWS 中国 (北京) リージョンの利用を希望されるお客様は、中国 (北京) リージョン専用の認証情報で別途サインアップする必要があります。

[14] リアルタイムのロケーションマップについては、次のページをご覧ください。

https://aws.amazon.com/jp/about-aws/global-infrastructure/

コンテンツおよびサーバーを配置する AWS リージョン (1 つまたは複数) は AWS のお客様が選択します。このため、地理的ロケーションに関して特別な要件のあるお客様は、1 つまたは複数の特定のロケーションを選択してそこに環境を構築することができます。例えば、日本国内の AWS のお客様は、日本にコンテンツを保存したい場合、アジアパシフィック (東京) リージョンなどの AWS リージョンのみに AWS のサービスを展開するように選択することにより、コンテンツを常に日本国内に保存できます。お客様がこのように選択した場合、法律上必要なときを除き、お客様の同意なしに AWS がそのコンテンツを日本から移動することはありません。

コンテンツの保存および処理にどの AWS リージョンを利用するかについては、常にお客様に決定権があります。AWS は、お客様が選択した AWS リージョン (1 つまたは複数) においてのみ、また、お客様が選択したサービスを使用してのみ、お客様のコンテンツを保存および処理します。AWS は、法律上必要な場合を除き、お客様の同意なしにお客様のコンテンツを移動することはありません。

リージョン (1 つまたは複数) を選択する方法

AWS のサービスを使用する AWS リージョン (1 つまたは複数) を指定するには、AWS マネジメントコンソールを使用するか、AWS アプリケーションプログラミングインターフェイス (API) でリクエストを送信します。

図 3: AWS グローバルリージョンの選択は、AWS マネジメントコンソールを使用して AWS ストレージサービスにコンテンツをアップロードするときや、コンピューティングリソースをプロビジョニングするときに、お客様に表示される AWS リージョン選択メニューの例を示しています。

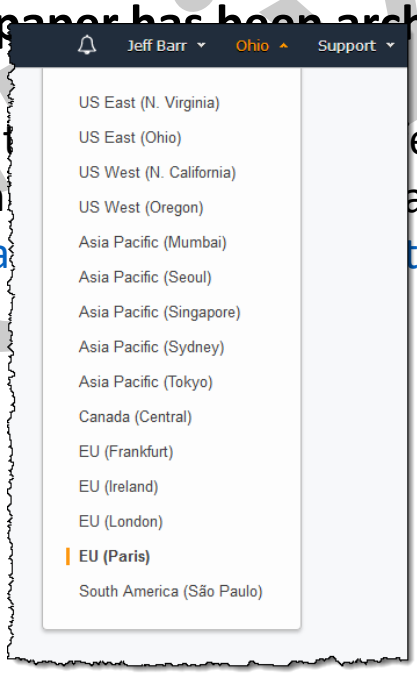


図 3 – AWS マネジメントコンソールでの AWS グローバルリージョンの選択

AWS Virtual Private Cloud (VPC) 機能を利用すると、コンピューティングリソースに AWS リージョンを使用するように指示することもできます。AWS VPC では、AWS クラウドの非公開で独立したセクションをお客様にプロビジョニングできます。このセクション使用すると、お客様が定義した仮想ネットワーク内に AWS リソースを起動できます。AWS VPC では、自社のデータセンターで運用されている従来型のネットワークに類似した仮想ネットワークトポロジーを定義できます。

お客様によって VPC に起動されるコンピューティングリソースなどのリソースは、お客様が指定した AWS リージョンに配置されます。例えば、VPC をアジアパシフィック (東京) リージョンに作成し、そこから自社のデータセンターへリンク (VPN[15] または Direct Connect[16] のいずれか経由) を設定すると、VPC に起動されるすべてのコンピューティングリソースの場所をアジアパシフィック (東京) リージョンにすることができます。この方法は、他の AWS リージョンにも活用できます。

国境を越えた個人データの移転

2016 年に、欧州委員会は新しい「一般データ保護規則 (General Data Protection Regulation, GDPR)」を承認し、採択しました。EU データ保護指令および関連するすべての現地法が GDPR に置き換えられました。AWS のすべてのサービスは GDPR に適合しています。AWS は、業務に適用される GDPR 要件にお客様が適合できるように、サービスとリソースをお客様に提供します。これらには、AWS の CISPE 行動規範の遵守、きめ細かなデータアクセス制御、監視およびロギングツール、暗号化、キー管理、監査機能、IT セキュリティ標準への準拠、AWS C5 証明が含まれます。詳細については、AWS 一般データ保護規則 (GDPR) センター[17] の Navigating GDPR Compliance on AWS のホワイトペーパー[18] を参照してください。

お客様は、AWS のサービスを利用する際、個人データを含むコンテンツの国境を越えた移転を選択できます。そのため、このような移転に適用される法的要件を考慮する必要があります。AWS は、個人データ (GDPR で定義される) を含むコンテンツを EU から欧州経済圏の域外の国 (シンガポールなど) に移転する AWS のお客様に対し、標準契約条項 2010/87/EU (いわゆる"モデル条項") が含まれるデータ処理補足条項を提供します。AWS の EU データ処理補足条項およびモデル条項により、AWS のお客様は、欧州において設立された企業であれ、欧州経済圏で営業するグローバル企業であれ、GDPR に完全に準拠しつつ、AWS を利用してグローバルな運用を継続できます。AWS データ処理補足条項は AWS サービス条件に組み込まれ、AWS でのお客様の個人データの処理に GDPR が適用される範囲で、自動的に適用されます。

[15] http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_VPN.html
[16] http://aws.amazon.com/directconnect/
[17] https://aws.amazon.com/jp/compliance/gdpr-center/
[18] https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf

コンテンツへのアクセス権を誰に付与するか?

コンテンツに対するお客様の管理権

AWS を利用するお客様は、AWS 環境内のコンテンツに対して管理権を保有したままであり、放棄していません。お客様は次のような事項を実施できます。

- コンテンツをどこに配置するかを決定する (例えば、AWS で使用するストレージの種類と、AWS リージョンで示す地理的ロケーション)
- コンテンツの形式、構造およびセキュリティを管理する (マスキング、匿名化または暗号化を行うかどうかなど)。AWS では、コンテンツの保管中および移動中に強力な暗号化を実装できるオプションを提供しています。また、AWS では、独自の暗号化キーを管理したり、お客様が選択した第三者の暗号化メカニズムを使用したりするオプションも提供しています。
- その他のアクセス制御を管理する (アイデンティティアクセス管理、権限およびセキュリティ認証情報など)

この AWS の機能により、お客様が AWS 上にあるコンテンツをライフサイクル全体にわたって管理できるようになります。お客様の個別のニーズに応じたコンテンツの管理 (コンテンツ分類、アクセス制御、保持および削除を含む) が可能になります。

お客様のコンテンツへの AWS のアクセス

ウェブサイトに記載されているように、AWS では、お客様が選択したコンピューティング、ストレージ、データベース、ネットワーキングまたはその他のサービスが利用可能になります。サービスを利用する際、お客様にはコンテンツを暗号化する多数の選択肢 (AWS 暗号化機能の利用 (AWS Key Management Service など) や独自の暗号化キーの管理、お客さまが選択した第三者の暗号化メカニズムの利用を含む) があります。AWS は、法律上必要な場合を除き、お客様の同意なしにお客様のコンテンツにアクセスしたり使用したりすることはありません。AWS では、マーケティングや広告などの他の目的のためにお客様のコンテンツを利用したり、そこから情報を抽出したりすることはありません。

政府機関のアクセス権

日本では、多くの国々と同様に、日本の法執行機関および政府セキュリティ機関が情報へのアクセスを求めることのできる法制度が定められています。外国の法執行機関も、現地の法執行機関および政府セキュリティ機関と連携して、日本で情報へのアクセスを求めることができます。ただし、関連する法律すべてにおいて、該当する政府機関によるアクセスを許可する前に満たさなければならない基準があります。例えば、アクセスを求める政府機関は、コンテンツへのアクセスの提供を求める正当な理由があることを当事者に示す必要があります。

クラウドサービスに保存されたコンテンツに対して、国内および国外の政府機関がアクセスできるかどうかについて、問い合わせを受けることがあります。多くの場合、そこにはデータの主権の問題についての誤解があります (政府機関がお客様のコンテンツにアクセスできるかどうかや、アクセスが発生する事情など)。一部のお客様にとっては、コンテンツが配置される法域内で適用される現地法は重要な考慮事項です。さらに、他の法域内の法律が適用される可能性も考慮する必要があります。お客様のビジネスと運営に関連する法律の適用状況について、お客様の責任において適切な助言を求めてください。

クラウドに保存されたコンテンツへのアクセス権を求める国内または国外の政府機関につ

いて、その権利に懸念や疑問が生じたときは、お客様に既に適用されている法律に基づき、該当する政府機関がそのコンテンツに対する要請を行う権限を有しているかどうかを理解することが重要です。例えば、X 国で事業を経営している企業は、コンテンツが Y 国に保存されていても、X 国の情報に対する法的要請に従う場合があります。ある法人のデータへのアクセス権を求める政府機関は通常、クラウドプロバイダーではなく、その法人に対して直接情報を要請します。

多くの国々には、データアクセス関連の法律で、域外適用されるものがあります。クラウドサービスの文脈でよく例に出される域外適用の米国法が、愛国者法です。他の先進国の法律と同様に、愛国者法では国際的なテロリズムやその他の海外情報の問題に関連する調査において、政府機関による情報の取得が可能になります。愛国者法に基づく文書の要請には、その要請が同法に準拠していることを示す裁判所の命令が必要です (例えば、要求が合法的な調査に関連しているか、など)。愛国者法は一般的に、企業が法人化されているか、および/または、世界的に経営されているかを問わず、また、情報がクラウド、オンサイトのデータセンター、物理的な記録のいずれに保存されているかを問わず、米国で事業を経営しているすべての企業に適用されます。米国で事業を経営している日本企業についても、事業経営内容によっては愛国者法に従う必要がある場合があります。

政府機関に対するアクセスの付与に関する AWS のポリシー

AWS は、お客様のセキュリティに気を配り、法的に有効かつ拘束力のある命令 (召喚状または裁判所の命令など) を遵守するために法律上必要な場合、またはその他適用法令上必要な場合を除き、米国またはその他の国の政府機関の要請に応じてデータを開示したり移動したりすることはありません。政府以外の機関または規制当局は通常、有効かつ拘束力のある命令を得るために[illegible]との刑事共助条約など) を利用する必要があります。さらに、AWS の実務では、法的に禁止される場合、または AWS のサービスの利用に関連して違法行為であることの明示的な示唆がない限り、お客様が開示からの保護を求めることができる場合、能な場合には、お客様のコンテンツを開示する前にお客様に通知します。詳細については、オンラインの Amazon 情報リクエストポータル[19] を参照してください。

[19] https://aws.amazon.com/jp/compliance/amazon-information-requests/

日本におけるプライバシーおよびデータ保護: 個人情報の保護に関する法律

データ保護を取り扱う日本の主要な法令は、個人情報の保護に関する法律 (個人情報保護法) とその関連法令です。また、現在に至るまで、各業界を所管するさまざまな政府省庁や最近設立されたデータ保護に関する政府機関である個人情報保護委員会[20] が複数のガイドラインを公表しています。

本書のこの部分では、2017 年 5 月 30 日に施行された改正後の個人情報保護法について説明します[2121]。

他の多くの国と異なり、個人情報保護法では、個人情報およびその情報の利用目的を管理するデータ管理者と、データ管理者の指示に従ってデータ管理者の代わりに情報を処理するデータ処理者が厳密には区別されていません。個人情報保護法は、個人情報を取り扱うすべての事業者 (個人および法人) に適用されます。また、個人情報保護法では個人情報と、個人情報保護法で個人データと定義される個人情報データベースを構成する個人情報を区別します。事業者に課される義務は、事業者が個人情報または個人データについて、取得、利用、または提供を行っているかどうかによって異なります。

AWS はサービスが、さまざまなビジネス目的に応じて多様な状況で利用されていると認識しています。そのため、AWS サービスを利用して保存または処理されたカスタマーコンテンツに含まれる個人情報のデータライフサイクルに、複数の当事者が関与する可能性があります。以下の表に含まれるガイダンスでは、簡略化のために、カスタマーコンテンツが AWS のサービス上に保存されるという前提で、お客様が以下の状況にあてはまるものと仮定しています。

- エンドユーザーから個人情報を取得し、その情報の取得目的を判別し、その個人情報を利用する
- 誰が個人情報にアクセス、アップデート、および利用できるかを管理する能力を持つ
- 通知および同意の要件を遵守するために、必要に応じて個人とやり取りなどを行って、個人情報に係る個人との関係を管理する

お客様が実際にこれらの責任を果たすために第三者と連携したり第三者に協力を求めたりする可能性がありますが、AWS ではなく、お客様が第三者との関係を管理します。

以下の表に 個人情報保護法のデータ保護原則をまとめました。この表では、個人情報保護法 の要件に関連する AWS サービスについても説明します。

[20] https://www.ppc.go.jp/

[21]個人情報保護法の法文については、以下のページからご覧いただけます。
https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

データ保護原則	データ保護義務の概要	考慮事項
取得、通知 および利用目的	事業者は、個人情報を取得するために偽りその他不正の手段を用いることが禁止されています。事業者は、要配慮個人情報を取得するときに、本人の同意を得る必要があります[22]。 事業者は、個人情報を取得するときは、このような個人情報の利用目的を本人に速やかに通知するか、これを公表しなければなりません。利用目的はできる限り詳細に特定しなければならず、また利用目的の変更は合理的である必要があります。事業者は、本人の同意をあらかじめ得ている場合や個人情報保護法またはその他の適用法令に基づく例外によって認められる場合を除き、利用目的の達成に必要な範囲を超えて個人情報を利用してはなりません。	**お客様**: お客様は個人情報を個人からいつ、どのように、どのような目的で取得するかを決定および管理します。AWS のサービスを利用して保存または処理するカスタマーコンテンツに、その個人情報を含めるかどうかを決定します。お客様はまた、そのデータの取得目的と、認められたソースからデータを取得して認められた目的のみのためにそのデータを利用することを、該当者に通知または公表することが必要になる場合があります。 お客様と AWS の関係において、個人情報が AWS に保存されている個人との関係を有しているのはお客様です。そのため、その個人と直接やり取りしたり、その個人情報の取得および取扱いについて適宜公表したりすることができます。個人情報の取得に関連する個人に対する通知や、お客様により取得される上記個人の同意の範囲を把握するのは、AWS ではなくお客様です。 **AWS:** お客様が AWS を利用して保存または処理するコンテンツに含まれた個人情報について、AWS が個人情報を取得することはありません。AWS はこれらの個人にコンタクトすることはありません。お客様の AWS の利用に関連する個人とやり取りする必要はなく、やり取りすることもできません。 AWS はお客様が選択した AWS のサービスをお客様に提供する目的でのみカスタマーコンテンツを利用します。それ以外の目的ではカスタマーコンテンツを利用しません。
個人データの精度	事業者は、個人データ (個人情報データベースを構成する個人情報) が常に正確かつ最新になるように努力する必要があります。	**お客様:** AWS を利用して個人データを保存することを選択しても、その個人データに対する品質の管理権およびアクセス権はお客様が保有しており、個人データの訂正もお客様が行えます。つまり、お客様は、個人データを正確で完全な、誤解が生じない最新の状態に保つために、必要なすべての措置を取る必要があります。

[22]要配慮個人情報とは、個人の人種、信条、社会的身分、病歴、犯罪の経歴、または個人が犯罪により害を被った事実その他個人に対する不当な差別、偏見その他の不利益が生じないように、その取り扱いに特に配慮を要するものが含まれる個人情報です。

データ保護原則	データ保護義務の概要	考慮事項
		AWS: AWS の SOC 1 Type 2 レポートには、データの移動、保存および処理を含むすべてのフェーズにわたってデータの整合性を合理的に確保できるコントロールが含まれています。
個人データのセキュリティ	事業者は、個人データの安全管理のために必要かつ適切な安全管理措置を行う必要があります。	**お客様:** お客様のコンテンツとクラウド**内の**セキュリティ (さらに、コンテンツに含まれる個人データ) の責任は、お客様が負います。 **AWS:** AWS は、基盤となるクラウド環境**の**セキュリティを管理する責任を負います。コアとなる AWS クラウドインフラストラクチャおよびサービスに組み込まれたすべてのセキュリティ対策の一覧については、「セキュリティプロセスの概要」[23] ホワイトペーパーをお読みください。AWS 環境内で実施されているセキュリティ制御の有効性については、AWS 認定およびレポート (AWS System & Organization Control (SOC) 1、2[24]、3[25] レポート、ISO 27001[26]、27017[27]、27018[28]認証および PCI DSS[29] コンプライアンスレポートを含む) で確認できます。
第三者への個人データの提供	事業者は一般に、一定の例外にあたる場合を除き、個人データを第三者に提供するには、本人から同意を得る必要があります。 個人情報保護委員会が 2017 年に公表した Q&A[30] では、事業者からクラウドサービスプロバイダーに対して個人データを提供しても、クラウドサービスプロバイダーがそのサーバーに保存された個人データを操作しない限り、個人データの提供とみなされないとされています。	**お客様:** 第三者への個人データの提供に関連して、関連する個人から同意を得る必要があるかを検討する必要があります。お客様と AWS の関係において、AWS に個人情報が保存されている当事者本人との関係を有しているのはお客様です。そのため、お客様が、上記事項について関連する個人と直接やり取りすることができます。 **AWS:** お客様が AWS を利用して保存または処理するコンテンツから AWS が個人データを取得することはありません。また、AWS にあるお客様のコンテンツに個人情報が保存されている当事者本人に対して AWS がコンタクトすることもありません。提供の同意を得るために AWS が該当する個人とやり取りする必要はなく、やり取りすることもできません。

[23] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
[24] http://aws.amazon.com/jp/compliance/soc-faqs/
[25] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
[26] https://aws.amazon.com/jp/compliance/iso-27001-faqs/
[27] https://aws.amazon.com/jp/compliance/iso-27017-faqs/
[28] https://aws.amazon.com/jp/compliance/iso-27018-faqs/
[29] https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/

データ保護原則	データ保護義務の概要	考慮事項
個人データの国際的な移転における制限	事業者は、移転先の国が、個人情報の保護について日本の制度と同等と見なされる法制度を備えている場合、または個人データの保護について適切な措置をとっている国外の第三者にデータを移転する場合に、個人データを外国に移転できます。それ以外の場合、事業者は、国際的なデータ移転を行うために本人の同意を得る必要があります。 この制限は、外国にある受領者に 個人データを移転する場合のみ適用されます。個人情報保護委員会が 2017 年に公表した Q&A[30] では、外国のクラウドサービス事業者が運営する日本のサーバーに個人データを保存することは、国際的なデータ移転にあたらないとされています。	**お客様:** お客様はコンテンツが配置される AWS リージョン (1 つまたは複数) を選択できます。AWS のサービスをアジアパシフィック (東京) リージョンのみにデプロイするようにも選択できます。 AWS のサービスは、コンテンツに使用する AWS リージョンがどこであっても、お客様がコンテンツを効果的に管理できるように構成されています。 お客様は、個人情報を保存または処理するロケーションをその個人に開示するかどうかを検討し、そのロケーションに関連して、必要に応じて該当する個人から同意を得る必要があります。お客様と AWS の関係において、個人情報が AWS に保存されている個人との関係を有しているのはお客様です。そのため、お客様が、上記事項について関連する個人と直接やり取りすることができます。 お客様が自身のコンテンツを複数のリージョンに保存するのも、リージョン間でコンテンツをコピーまたは移動するのも、お客様が自由に行えます。どこで保存および処理する場合でも、引き続き効果的にコンテンツを管理できます。 **AWS:** AWS は、お客様が選択した AWS リージョン (1 つまたは複数) においてのみ、また、お客様が選択したサービスを使用してのみ、お客様のコンテンツを保存および処理します。AWS は、法律上必要な場合を除き、お客様の同意なしにお客様のコンテンツを移動することはありません。 AWS は ISO 27001 の認証を受けており、コンテンツが保存される地理的リージョンに関係なく、すべてのお客様に堅牢なセキュリティ機能を提供します。
第三者への個人データの提供の記録と確認	事業者は、第三者への個人データの提供および受領に関連して、個人情報保護委員会によって指定された特定の情報を確認し、記録する必要があります。	**お客様:** お客様は個人データの追跡可能性を確保するために、第三者から受領した、または第三者に提供した個人データに関連して、個人情報保護委員会によって指定された特定の情報の確認および記録の責任を負います。

[30] https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf

データ保護原則	データ保護義務の概要	考慮事項
		AWS: AWS 側では、お客様がどの個人データ (存在する場合) をアップロードするか、またはお客様が個人データを第三者に提供するかどうかを把握していないため、個人データの提供に関する情報の確認も記録もできません。
保有個人データに関する開示	個人情報を取り扱う事業者は、苦情に対応するために、以下の情報を本人の知りうる状態に置く必要があります。(i) 個人情報を取り扱う事業者の名称、(ii) 保有個人データの利用目的、(iii) 事業者が保有する個人情報の本人による開示、訂正および利用停止に応じるための手続き、(iv) 事業者の連絡先情報。	**お客様:** 個人情報が AWS に保存されている個人に対してこれらの開示要件を満たす責任は、お客様が負います。 **AWS:** AWS は、個人情報を含む可能性のあるコンテンツがいつ AWS にアップロードされるのかを把握していません。AWS に保存されている個人情報を、その当事者本人から取得することもしません。このような状況であるため、AWS から該当する個人に情報を提供することはできません。
開示、訂正および消去	事業者は、本人から要求された場合に、保有個人データを本人に開示する必要があります。事業者は、本人から訂正を要求された場合、保有個人データの誤った情報を訂正する必要があります。事業者は、利用目的に違反している場合に、保有個人データの利用を停止するように要求される場合があります。	お客様: お客様が保有個人データを含むコンテンツについて、AWS を利用して保存することにした場合、お客様はそのコンテンツの管理権およびアクセス権を有しており、そのため保有個人データの訂正または利用停止を行うことができます。すなわち、お客様は、カスタマーコンテンツに含まれる個人データを正確で完全な、誤解が生じない最新の状態に保つために、必要なすべての措置を取る必要があります。 **AWS**: AWS はお客様がどのような種類のコンテンツを AWS に保存することにしたのかを把握しません。お客様は、お客様のコンテンツがどのように保存、利用および開示から保護されるのかについての管理権を保有します。AWS のサービスは、AWS ドキュメント[31] に記載されているように、お客様がコンテンツを削除できるようお客様に管理権を提供しています。

[31] http://aws.amazon.com/jp/documentation

プライバシーの侵害

AWS の利用中でもコンテンツの管理権はお客様にあるため、プライバシーが侵害されないように環境を監視し、監督機関および影響を受けた個人に対して適切な法令に基づき適宜通知する責任は、お客様が負うことになります。お客様のみがこの責任を管理できます。

AWS ではなくお客様がこの職責を担うことが適切である理由を説明するために、お客様の AWS アクセスキーを例にしてみます。

アクセスキーを管理し、誰が AWS アカウントへアクセスできるのかを決定するのはお客様です。AWS からアクセスキーは見えず、誰がアカウントへのログインを許可されているかも把握できません。AWS は、お客様によるアクセスキーの利用、誤用、配布または紛失について監視を行う責任を負っています。

個人情報の不正アクセスや不正開示時に個人に対して通知を行うことは、現時点では個人情報保護法の義務的な要件ではありません。ただし、一部の法域では、個人情報の不正アクセスや不正開示を個人または監督機関に通知することは義務とされています。個人または監督機関への通知が義務でない場合でも、この対応はリスクを回避するためのベストアプローチになります。個人に通知する適切なタイミングと通知のプロセスは、お客様が決定する事項です。

その他の考慮事項

このホワイトペーパーでは、個人情報保護法以外でお客様に関連する可能性がある日本の他のプライバシー法令 (都道府県条例および業界固有の要件を含む) については説明しません。個別のお客様に適用される法令は、お客様のビジネスの拠点、業界、保存するコンテンツの種類、コンテンツの発生元の場所または人、コンテンツが保存される場所などの要因に応じて変わります。

日本のプライバシー規制に関する義務に関心をお持ちのお客様は、まず、適用される要件を確認し、お客様の責任において適切な助言を求める必要があります。

まとめ

AWS にとって、セキュリティは常に最優先事項です。AWS は、190 か国を超える国々で、企業、教育機関、および政府機関などの数百万のアクティブなお客様にサービスを提供しています。金融機関や医療機関のお客様とも取引があり、信用の厚さから最も配慮を要する情報も託されています。

AWS のサービスは、保存場所、保存方法、アクセスできるユーザーなどのコンテンツをお客様が管理できるようにするだけでなく、ソリューションの構成およびデプロイも柔軟に実行できるように設計されています。そのため、AWS のお客様は、独自の安全なアプリケーションを構築して、AWS にコンテンツを安全に保存することができます。

その他のリソース

プライバシーおよびデータ保護要件への対応方法についての理解を深めるには、AWS のウェブサイトで公開されているリスク、コンプライアンスおよびセキュリティに関するホワイトペーパー、ベストプラクティス、チェックリストおよびガイダンスを確認することをお勧めします。これらの資料は、http://aws.amazon.com/compliance および http://aws.amazon.com/security でご確認いただけます。

本書の日付時点で、以下の国またはリージョンに対して、プライバシーおよびデータ保護の考慮事項についての特定のホワイトペーパーも入手できます。

欧州連合[32]
ドイツ[33]
オーストラリア[34]
香港[35]
シンガポール[36]
マレーシア[37]
ニュージーランド[38]
フィリピン[39]

詳細情報

AWS では、トレーニングも提供しており、AWS クラウドで利用可能な効率的で安全なアプリケーションを設計、開発、および運用する方法をお客様が理解して AWS のサービスおよびソリューションに習熟できるようにサポートしています。また AWS では無料の説明動画[40]、セルフペースラボ[41]、およびクラスルームトレーニング[42] を提供しています。AWS トレーニングの詳細については、http://aws.amazon.com/training/ をご覧ください。

AWS 認定では、AWS のテクノロジーを利用して安全で信頼性の高いクラウドベースアプリケーションを構築するためのベストプラクティスを達成できるスキルおよび知識を認定します。AWS 認定の詳細については、http://aws.amazon.com/jp/certification/ をご覧ください。

さらに詳しい情報については、https://aws.amazon.com/jp/contact-us/ ページから AWS にお問い合わせいただくか、お客様の地域の AWS アカウント担当者にお問い合わせください。

[32] https://d1.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf
[33] https://d1.awsstatic.com/whitepapers/compliance/German_Data_Protection_Whitepaper.pdf
[34] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf
[35] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Hong_Kong_Privacy_Considerations.pdf
[36] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf
[37] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf
[38] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf
[39] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Philippines_Privacy_Considerations.pdf
[40] https://www.aws.training/
[41] http://aws.amazon.com/jp/training/self-paced-labs/
[42] http://aws.amazon.com/jp/training/course-descriptions/

文書改訂

日付	説明
2017 年 12 月	初版
2018 年 5 月	第 2 版

This paper has been archived

For the latest technical content, refer to the AWS Whitepapers & Guides page:
https://aws.amazon.com/whitepapers