EU データ保護に関するホワイトペーパー

2016 年 11 月

(本書の最新版については http://aws.amazon.com/compliance/aws-whitepapers/、およびドイツ語版については http://aws.amazon.com/de/data-protection/ を参照してください。)

はじめに

本書では、AWS を使用して個人情報が含まれるコンテンツを保存するお客様に役立つ情報を提供します。特に、本書では、EU 指令 95/46/EC「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」(1995 年 10 月 24 日) に準拠して、AWS サービスを使用する方法について説明します。本書は、お客様が以下のことを理解することを目的としています。

- お客様が EU 法に準拠し、自身のセキュリティニーズに対処して、暗号化および他の手段でコンテンツを保護する方法を含む、AWS サービスの運用方法
- コンテンツを保存およびアクセスできる地理的な場所および他の関連するコンプライアンスの考慮事項に対する、お客様による完全な制御
- AWS サービスに保存されているコンテンツの管理およびセキュリティ保護で、お客様および AWS が果たすそれぞれの役割

このホワイトペーパーでは、AWS サービスを使用して個人データが含まれるコンテンツを保存する場合の EU 指令の影響について考慮する際に、AWS のお客様から寄せられる一般的な質問に焦点を置いて説明しています。業界特有の要件およびお客様がビジネスを行う他の管轄区域での法律に適合するためのお客様のニーズなど、お客様が対処する他の関連考慮事項についても説明しています。本書は情報の提供のみを目的としており、法律相談ではないため、法律相談に使用されるべきではありません。お客様によってそれぞれの要件が異なっているため、プライバシーやデータの保護環境の実装、および、それぞれのビジネスに関連する適用法令に関する一般的な事柄に関しては、お客様が各自で適切なアドバイスを受けることをお勧めします。

お客様のコンテンツに関する考慮事項

コンテンツの保存では、すべての組織で以下のような実際的な問題がよく発生します。

- コンテンツは保護されるか?
- コンテンツはどこに保存されるか?
- 誰がコンテンツへのアクセス権を持つか?
- コンテンツにどの法律および規制が適用されるか、およびそれらに準拠するには何が必要か?

これらの考慮事項は新しいものではなく、クラウド固有でもありません。これらは、社内でホストして運用するシステムや従来のサードパーティーでホストされるサービスにも該当します。AWS サービスを使用する場合、以下のように、お客様は、自身のコンテンツの統制を維持し、個々のコンテンツのセキュリティ要件を管理および制御する責任があります。

- どのコンテンツを AWS に保存するかの選択
- コンテンツを暗号化するかどうか - 保存時および伝送時
- コンテンツにどの AWS サービスを使用するか
- 世界中のどこでコンテンツを保存および処理するか
- コンテンツの形式と構造、およびコンテンツをマスクまたは匿名化するかどうか
- コンテンツへのアクセスを誰に許可するか、およびアクセス権限を付与、管理、取り消す方法

お客様のコンテンツのセキュリティは、AWS とお客様の両方が適切な対策を実施しているかどうかに依存しています。AWS は基盤となるクラウド環境でのセキュリティ統制を実施し、AWS のお客様は、自身のコンテンツおよびそのコンテンツのセキュリティに関して統制を実施します。AWS に保存される個人データに適用されるデータ保護要件に関しては、お客様と AWS のそれぞれの異なる役割を理解しておくことが不可欠です。

お客様のコンテンツのセキュリティ:

IT インフラストラクチャを AWS に移すことは、お客様と AWS の両方がそれぞれの責任領域でセキュリティのオペレーションと管理に関して重要な役割を持つことを意味します。AWS は、ホストオペレーティングシステムや仮想化レイヤー、AWS サービスが稼働している施設の物理的なセキュリティまでに至るコンポーネントの運用、管理、制御を行います。お客様には、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の更新やセキュリティパッチを含む)、その他の関連アプリケーションソフトウェア、および AWS で提供されるセキュリティグループファイアウォールや他のセキュリティ関連機能の設定を管理する責任があります。お客様は通常、サードパーティー (インターネットサービスプロバイダーなど) が提供するサービスを介して AWS 環境に接続します。AWS ではこれらの接続を提供しないため、その接続のセキュリティ、およびシステムに関連するサードパーティーのセキュリティ上の責任については、お客様が考慮する必要があります。これは、オンプレミスのデータセンターへの接続を提供するネットワークサービスプロバイダーの場合と同じです。

このモデルを次の図 1 に示します。

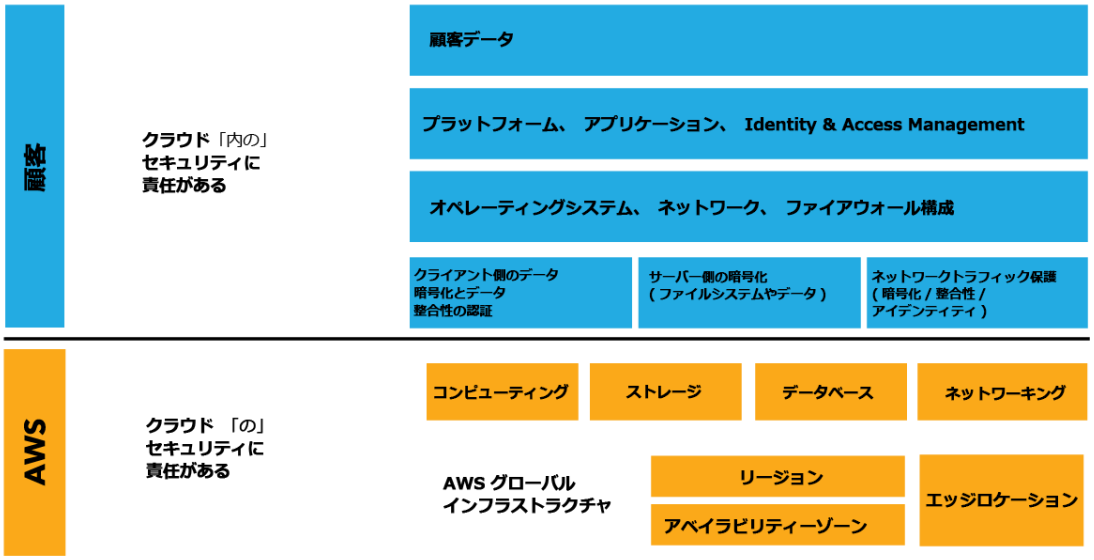

図 1 - セキュリティモデル

お客様のコンテンツのセキュリティにおいて、このモデルは何を意味しますか?

クラウドソリューションのセキュリティを評価する際に、お客様が以下の 2 つを理解して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) が実装して運用するセキュリティ対策 – ″クラウド**の**セキュリティ″ および
- お客様のコンテンツ、および AWS サービスを使用するためのアプリケーションに関連して、お客様が実装して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 はクラウド**の**セキュリティを管理しますが、クラウド**内の**セキュリティはお客様が責任を持ちます。これは、お客様のコンテンツ、プラットフォーム、アプリケーション、システム、およびネットワークの保護を実装するためにどのようなセキュリティ対策を選択するかはお客様が統制を保持しているためです。これは、オンサイトのデータセンターでのアプリケーションの場合と同じです。AWS ではさまざまなサービスの一環として、お客様がセキュリティ対策を選択でき、お客様はサードパーティーの各種セキュリティソリューションの使用を選択することもできます。AWS のお客様は、自身のコンプライアンスの要求に応えるためにセキュリティアーキテクチャを完全に自由に設計できます。これは、プロバイダーがアーキテクチャを決定していた従来のホスティングソリューションとの大きな違いです。AWS では、セキュリティ対策を実装するかどうかをお客様が決定できます。実装する場合は、クラウド内でどのセキュリティ対策を実装するかを決定でき、その対策がお客様のビジネスに適切であるかどうかを判断できます。たとえば、データを保護するために可用性を高めるアーキテクチャが必要であれば、お客様はシステム、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の冗長化を追加して、復元力がより高い高可用性アーキテクチャを構築できます。データへのアクセスを制限する必要がある場合は、AWS コントロールにより、システムレベルと暗号化を使用したデータレベルの両方でアクセス権限の管理概念をお客様が実装できます。このように、AWS では、データセキュリティに関する技術的および組織的な対策を形成する多くの要素をお客様が直接制御できます。

クラウドのセキュリティについて

AWS は基盤となるクラウド環境のセキュリティの管理に責任があります。AWS クラウドインフラストラクチャは、利用可能なクラウドコンピューティング環境の中で最も柔軟性があり最も安全であるように構築されていて、ユーザーの完全な分離を実現する一方で、可用性を最大限に高めるように設計されています。AWS は、お客様が必要に応じて大規模でグローバルなスケールでアプリケーションとコンテンツをすばやく安全にデプロイできる、非常にスケーラブルで信頼性が高いプラットフォームを提供しています。AWS サービスはコンテンツに依存しないため、保存されるコンテンツの種類やコンテンツが保存される地理的リージョンに関係なく、すべてのお客様に同じ高いレベルのセキュリティを提供します。AWS ではお客様が AWS サービスにどのようなデータを保存しているかを関知しないため、お客様のコンテンツの一部として保存されているデータでの個人データとその他の種類のデータを AWS では区別できません。

世界レベルで高いセキュリティを誇る AWS のデータセンターでは、最先端の電子監視システムおよび多要素アクセス制御システムが利用されています。データセンターでは、トレーニングを受けた警備員が 24 時間年中無休で配置されていて、アクセスは最小権限ベースで厳格に認証され、システム管理の目的に限定されています。中核となる AWS クラウドインフラストラクチャ、プラットフォーム、サービスに組み込まれているすべてのセキュリティ対策の包括的なリストについては、『セキュリティプロセスの概要』ホワイトペーパーをお読みください。

AWS では、基盤となるクラウド環境のセキュリティに気を配り、不正アクセスに対する洗練された技術的かつ組織的な対策を実装しています。AWS Service Organization Control (SOC) 1 および 2 のレポート、ISO 27001 認定基準、PCI-DSS 準拠レポートなどの AWS の認定およびレポートで、お客様は AWS 環境内で実施されているセキュリティ統制を検証できます。これらのレポートおよび認定は、独立したサードパーティーの監査人によって生成されていて、AWS のセキュリティ統制の設計と運用効率を保証しています。該当する AWS のコンプライアンス認定とレポートは、https://aws.amazon.com/compliance/contact でリクエストできます。AWS のコンプライアンス認定、レポート、およびベストプラクティスと標準への適合の詳細については、AWS コンプライアンスサイトを参照してください。

AWS では、お客様のデータ保護の義務に合わせるために役立つデータ処理追補の追加が提供されています。AWS では、お客様が個人データを EU から欧州経済地域外に移転するために必要な場合は、標準契約条項 2010/87/EU (「モデル条項」とも呼ばれる) をお客様のデータ処理追補に追加することもできます。

AWS のデータ処理追補は、モデル条項を含め、データ保護指令第 29 条作業部会と呼ばれる EU データ保護機関のグループによって 2015 年 3 月 6 日に承認されました。この承認により、モデル条項を必要とするすべてのお客様は、この指令に従って国際的なデータフローを可能にするために十分な契約上のコミットメントを提供する際に、AWS のデータ処理追補に依存できるようになりました。データ保護指令第 29 条作業部会による承認に関する詳細については、次のルクセンブルクデータ保護庁のウェブページを参照してください。
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

データ処理追補およびモデル条項に加えて、AWS の欧州リージョンから米国リージョンに個人データを転送するお客様は、AWS の EU-U.S.Privacy Shield Framework への参加による恩恵も受けることができます。Amazon.com, Inc.、および AWS を含むその一部の米国子会社は、2016 年 10 月 21 日に EU-U.S.Privacy Shield Framework の認定を受けています。EU-U.S.Privacy Shield Framework はお客様による AWS の使用方法または作業方法に影響しませんが、EU によって認可された、欧州から米国に個人データを転送するための追加のメカニズムを提供します。EU-US Privacy Shield Framework に基づく米国サービスプロバイダーの義務の詳細については、以下の欧州委員会のウェブサイトを参照してください。http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm また、EU-U.S.Privacy Shield Framework のウェブサイトは以下を参照してください。https://www.privacyshield.gov/welcome.

クラウド内のセキュリティについて

AWS サービスを発行する場合、お客様は自身のコンテンツを制御します。どのようなコンテンツを AWS に保存するか、環境をどのように設定してコンテンツを保護するか、保管時および伝送時にコンテンツを暗号化するかどうか、コンテンツに誰がアクセスしてどのような認証情報 (Multi-Factor Authentication を含む) が必要か、どのような追加のセキュリティ機能やツールを使用してそれらをどのように使用するかは、AWS ではなくお客様が決定します。

AWS のお客様は、各自でセキュリティを制御しているため、お客様の組織が AWS に配置するすべてに対するセキュリティの責任があり、(ゲストオペレーティングシステム、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、および AWS のストレージ/プラットフォーム/データベースのサービスで保存および処理されるコンテンツなど) AWS インフラストラクチャへの接続に対するセキュリティの責任があります。

お客様は、コンテンツを保護するためのさまざまなセキュリティ機能、ツール、およびコントロール (洗練されたアイデンティティ & アクセス管理ツール、可用性の設定、バックアップ機能、セキュリティ機能、暗号化、ネットワークセキュリティなど) を活用するように、AWS サービスを設定できます。お客様が安全な AWS 環境を設計、実装、および運用できるように、AWS ではお客様が使用できる幅広いセキュリティ機能を提供しています。お客様は独自またはサードパーティーのセキュリティツールやコントロールを使用することもできます。コンテンツの保護に役立つように講じる措置の例として、以下の項目の実装が挙げられます。

- ユーザーに適切なアクセス権を割り当て、堅牢な措置を講じてアクセスキーを保護する、強力なパスワードポリシー
- データ損失や不正アクセスのリスクを軽減するための、Virtual Private Cloud、コンテンツの暗号化、SSL の使用、適切なアーキテクチャのシステムなどを含む、適切なファイアウォールとネットワークセグメンテーション
- データの損失や使用不可を軽減するための、適切な冗長方式およびバックアップ方法

これらの要因はすべて、AWS ではなくお客様が制御します。AWS ではお客様が AWS に配置しているコンテンツを把握できないため、お客様の設定を変更することはありません。それらはお客様が決定および制御します。AWS クラウドにどのようなコンテンツを配置するかを決定するのはお客様であるため、そこに保存されるデータに適切なセキュリティのレベルを判断できるのはそのお客様だけです。

お客様が既存のコントロールフレームワークに AWS を統合でき、お客様の組織での AWS サービスの使用に対するセキュリティ評価を設計および実行できるように、AWS ではセキュリティ、ガバナンス、リスク、およびコンプライアンスに関連するいくつかのホワイトペーパー、チェックリスト、およびベストプラクティスを公開しています。お客様は独自の設定に従ってセキュリティ評価を自由に設計および実行でき、クラウドインフラストラクチャのスキャンを実施する許可をリクエストできます (このスキャンは、その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 の適正利用規約に違反しません)。

AWS リージョン

AWS のデータセンターは世界各地にクラスターの状態で構築されています。特定の国にあるそれぞれのデータセンタークラスターを「リージョン」と呼んでいます。お客様は、世界中に 14 ある AWS リージョンを利用でき、そのうちアイルランド (ダブリン) とドイツ (フランクフルト) の 2 つのリージョンは EU 内にあります。お客様は 1 つのリージョン、すべてのリージョン、またはリージョンの任意の組み合わせを使用することを選択できます。図 2 に AWS リージョンの場所を示します。

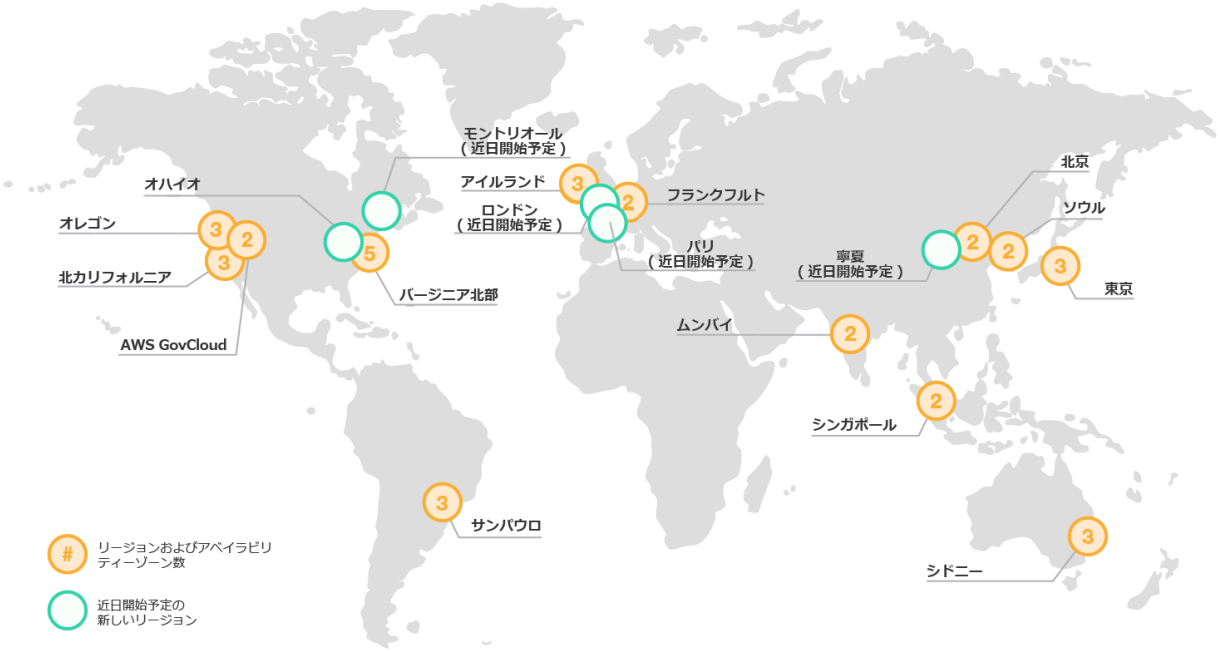

図 2 - AWS グローバルリージョン

AWS のお客様はコンテンツをホストする AWS リージョンを選択します。これにより、具体的な地理的要件を持っているお客様が、選択した場所で環境を構築できます。たとえば、欧州の AWS のお客様は EU (ドイツ) リージョンに専用で AWS サービスをデプロイすることを選択できます。お客様がそれを選択した場合、お客様が別の AWS リージョンを選択しない限り、そのお客様のコンテンツはドイツに保存されます。

お客様は複数のリージョンにコンテンツをレプリケートしてバックアップできますが、AWS はお客様が選択した 1 つ以上のリージョンの外部にコンテンツを移動することはありません。

リージョンを選択するにはどうすればいいですか?

お客様は、AWS マネジメントコンソールの使用時、または 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) を介したリクエストの送信時に、AWS サービスを使用する特定のリージョンを特定します。図 3 の AWS グローバルリージョンの選択では、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場合またはコンピューティングリソースをプロビジョニングする場合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

お客様は、Amazon Virtual Private Cloud (VPC) 機能を利用して、コンピューティングリソースに使用される AWS リージョンを指示することもできます。Amazon VPC により、お客様が定義した仮想ネットワーク内で AWS リソースを起動できる AWS クラウドのセクションをお客様がプロビジョニングできます。Amazon VPC では、お客様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を忠実に模した仮想ネットワークのトポロジーを定義できます。

お客様が VPC で起動したすべてのコンピューティングリソースおよび他のリソースは、お客様が指定したリージョンに配置されます。

お客様のコンテンツに対するお客様による制御とアクセス

コンテンツに対するお客様による制御

AWS を使用するお客様は、AWS 環境内の自身のコンテンツの制御を維持します。以下のことができます。

- コンテンツが配置される場所を決定する (たとえば、ストレージ環境の種類および地理的な保存場所)
- コンテンツの形式を決定する (たとえば、プレーンテキスト、マスク化、匿名化、または AWS で提供されている暗号化またはサードパーティーの暗号化メカニズムを使用した暗号化をお客様が選択できる)
- 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、セキュリティ認証情報など)
- SSL、Virtual Private Cloud、およびその他のネットワークセキュリティ対策を使用して不正アクセスを防止するかどうかを制御する

これにより、AWS のお客様は AWS でのコンテンツのライフサイクル全体を制御でき、コンテンツの分類、アクセス制御、保持、削除などの独自の特定のニーズに従ってコンテンツを管理できます。

お客様のコンテンツへのアクセス

AWS は、お客様が選択している AWS サービスを提供するために必要な場合を除いて、お客様のコンテンツにアクセスすることはありません。AWS は、その他の目的でお客様のコンテンツにアクセスすることはありません。

AWS はお客様が AWS にどのようなデータを保存しているかに関知せず、個人データとその他のコンテンツを区別できないため、AWS はお客様のすべてのコンテンツを同様に扱います。そのため、コンテンツに個人データが含まれているかどうかに関係なく、お客様のすべてのコンテンツは同様に AWS の堅牢なセキュリティ対策の恩恵を受けます。AWS は、AWS が提供するクラウドインフラストラクチャに最先端のセキュリティ対策を適用し、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、およびネットワーキングのサービスを使用できるようにします。お客様は、お客様独自の要件に基づいてそのインフラストラクチャ上でセキュリティを自由に構築できます。

政府機関によるアクセス権限

国内および外国の政府機関がクラウドサービスに保持されているコンテンツにアクセスする権限についてよく問い合わせを受けます。また、政府機関にお客様のコンテンツへのアクセス権限があるかどうか、およびどのような状況でそれが行われるかなどの、データ主権の問題についてお客様が懸念されることもよくあります。コンテンツが置かれている管轄区域に適用される現地の法律は、一部のお客様にとっては重視すべき事項です。ただし、お客様自身またはお客様の顧客がビジネスを行っている場所に応じて他の管轄区域の法律が適用される可能性があるかどうかを考慮する必要もあります。お客様は、ビジネスおよびオペレーションに関連する法律の適用を理解するために助言を求める必要があります。

国内または外国の政府がクラウドに保存されているコンテンツへのアクセス権を申請する権限についての懸念または質問がある場合は、お客様に既に適用されている法律の下で、関連する政府機関がコンテンツに対して要請を行う権限を持つ可能性があることを理解することが重要です。たとえば、X 国でビジネスを行っている会社は、コンテンツが Y 国に保存されている場合であっても、法的情報要請の対象になることがあります。通常、ある主体のデータへのアクセスを申請する政府機関は、クラウドプロバイダーではなく直接その主体に情報を要請します。

一般的に、欧州連合の加盟国には、公法の執行機関および国家安全保障機関が情報へのアクセスを申請できるようにする法令があります。外国の法律の執行機関が現地の法律の執行機関および国家安全保障機関と協力して、EU 内の情報へのアクセスを取得することもあります。実際に、ほとんどの国には、適切な法的情報要請 (犯罪行為に関する場合など) に応じて、他の国に情報を移転できる手続き (相互法的援助契約を含む) があります。ただし、関連する法律の執行機関によるアクセス要請が許可されるには、関連法律の下で満たす必要がある特定の条件があることを覚えておくことが重要です。たとえば、アクセスを申請する政府機関は、コンテンツへのアクセスの提供を当事者に要求するための正当な理由があることを提示する必要があり、裁判所の命令または令状の取得が必要になることがあります。

ほとんどの国には、域外適用を表明しているデータアクセス法令があります。クラウドサービスに関してよく言及され、域外適用される米国法の例として、米国愛国者法があります。愛国者法は、国際テロおよび他の外国諜報に関連する調査に関して政府が情報を取得できるようにしている他の多くの先進国の法律と同様です。愛国者法の下での文書の要請には、その要請が法律に準拠している (たとえば、その要請が適法な調査に関連している) ことを実証する裁判所命令が必要です。

AWS ポリシー

お客様のコンテンツに対する要請の発信元またはそのお客様が誰であるかに関係なく、AWS は常にお客様のコンテンツの保護に注意を払っています。召喚状や裁判所の命令などの、法的に有効で拘束力のある命令に従う必要がある場合を除き、AWS はお客様のコンテンツを開示することはありません。通常、米国以外の政府または規制団体は、有効で拘束力のある命令を取得するには、米国政府との相互法的援助契約など、認められた国際手順を使用する必要があります。それぞれの要請を慎重に吟味してその正確さを認証し、該当する法律に準拠していることを確認します。適用範囲が広過ぎる、要請者の権限を越えている、または該当する法律に完全には準拠していない要請には異議を申し立てます。お客様のコンテンツの開示を強要された場合は、法律で禁止されている場合を除いて、開示前にお客様に通知して開示の保護を申請する機会をお客様に提供します。

EU におけるデータ保護：指令

この指令[1] に含まれる義務について、以下で検討します。概略を言えば、この指令では、個人データが処理される場合に適用されるいくつかのデータ保護要件が提示されています。ここで言う "処理" には、個人データに対して実行されるすべてのオペレーションまたはオペレーションのセットが含まれます。この指令では、"個人データ" は、個人が特定または同定される可能性がある情報として定義されています (「データ主体」と呼ばれる)。さらに、この指令では、(a) "データ管理者" (個人データの処理の目的と手段を決定する当事者) と (b) "データ処理者" (管理者に代わって個人データを処理する当事者) が区別されます。

個人データがデータ保護義務に準拠して処理されるようにする必要があるのはデータ管理者です。たとえば、データ管理者は個人データが公正かつ適法に処理され、そのデータが不正または違法な処理から保護されるようにする必要があります。

AWS では、そのサービスがさまざまなビジネスオペレーションの一部として使用され、サプライチェーンに複数の当事者が関与している場合があることを認識しています。ただし、AWS サービスを使用して保存されているお客様のコンテンツに個人データが含まれている場合の一般的なガイドラインを以下に示します。

- お客様がデータを処理する目的を決定してデータの処理方法を選択した場合、その個人データに関してはお客様が管理者になります。
- 第三者 (管理者、サプライチェーンの別の第三者、または国内生産力のためだけに従事する個人) の代わりにお客様が AWS ネットワーク上の個人データを処理するだけの場合、その個人データに関してはお客様が処理者になります。

[1] この指令は、欧州連合の加盟国に直接設立された組織には適用されないことに留意する必要があります。その代わりに、欧州連合の加盟国は国内法令でこの指令を実施する必要があります。そのため、異なる加盟国での義務の正確な意味にはいくつかのバリエーションがあり、お客様はどの国内法が適用されるかについて助言を求める必要があります。

AWS は、お客様が (データを "処理" するかどうか、およびその方法を含めて) 完全に制御するセルフサービスインフラストラクチャのプロバイダーとして、AWS ネットワーク上でコンテンツをアップロードして処理するお客様に対し、インフラストラクチャサービスのみを提供します。この状況では、AWS はお客様がネットワークに何をアップロードしたかについては、そのコンテンツに個人データが含まれているかどうかも含めて全く把握または関知しません。AWS のお客様は AWS で暗号化を使用して、解読できないようにデータをレンダリングすることもできます。AWS は、サービスの提供に必要な場合 (または、法律や、法的に有効で拘束力のある命令に従う場合) を除いて、お客様のコンテンツを処理することはありません。

AWS には、AWS 従業員がお客様のコンテンツにアクセスするのを防止するために実施しているシステム、手続き、およびポリシーもあります。また、個人データを処理するお客様のために、AWS ではお客様がデータ保護義務に合わせるために役立つデータ処理追補を提供しています。AWS では、お客様が個人データを EU から欧州経済地域外に移転するために必要な場合は、モデル条項をお客様のデータ処理追補に追加することもできます。

AWS のデータ処理追補は、モデル条項を含め、データ保護指令第 29 条作業部会と呼ばれる EU データ保護機関のグループによって 2015 年 3 月 6 日に承認されました。この承認により、モデル条項を必要とするすべてのお客様は、この指令に従って国際的なデータフローを可能にするために十分な契約上のコミットメントを提供する際に、AWS のデータ処理追補に依存できるようになりました。データ保護指令第 29 条作業部会による承認に関する詳細については、次のルクセンブルクデータ保護庁のウェブページを参照してください。
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

データ管理者には、偶発的または違法な破壊、不慮の損失、改変、または不正な開示やアクセスから個人データを保護するために適切な技術的および組織的な対策を実施する責任があります。データ管理者に代わってデータ処理者によって処理が実行される場合、データ管理者には、実施される処理を規定する十分な技術的および組織的な対策を提供する処理者を選択する責任もあります。

この状況でお客様が通常考慮するデータ保護のいくつかの基本原則の概要を下記の表に示します。これらの原則に関連する AWS サービスの側面についても説明しています。この表の目的のために、AWS のお客様がデータ管理者になることを想定しています。ただし、前述のように、AWS のお客様がデータ処理者になる場合も多いことを認識しています。その場合でも、AWS のお客様には自身と管理者との関係で下記の表が役に立つことがあります。

データ保護の原則	**データ保護の義務の概要**	**考慮事項**
公正性	データ主体には、管理者のアイデンティティ、処理の目的、および公正な処理を保証するために必要なその他の情報について、正確で完全な情報を与える必要があります。	**お客様:** どのような情報を収集するか、およびその情報の使用目的を決定するお客様 (または、その顧客) です。多くの場合、お客様はすべてのデータ主体と直接的な関係があるため、データ主体と直接通信するのに最適なのはお客様です。さらに、お客様は以前にデータ主体に与えられたすべての通知の適用範囲を知っています。 **AWS:** AWS は、お客様が AWS に保存することを選択したコンテンツの種類およびその目的について一切制御できません。AWS は、このコンテンツについて (個人データが含まれているかどうかについても) 把握していません。AWS には、お客様が AWS に保存することを選択した個人データのデータ主体を特定したり、データ主体に連絡したりする手段がありません。そのため、関連するデータ主体に情報を提供することはできません。

法的根拠	管理者は、その処理に、指令で提示されている 1 つ以上の条件を満たす法的根拠を持つ必要があります。	**お客様:** 個人データを処理するかどうか、およびその目的を決定する際に、お客様は指令のいずれかの条件を満たしているかどうかを検討する必要があります。たとえば、データ主体の同意を得ていること、データ主体が当事者である契約の履行にその処理が必要であることなどがあります。 **AWS:** 前述のように、お客様が AWS に保存することを選択したコンテンツの種類について (個人データが含まれているかどうかについても) AWS は一切制御できません。AWS は、AWS サービスと組み合わせて構築するためにお客様がどのようなアーキテクチャを選定するか、およびそれがお客様の特定のニーズに適切かどうかを判断できません。AWS は、このデータが処理されるかどうか、およびその目的に関する意思決定に関与しません。したがって、AWS はその処理の法的根拠があるかどうかを確認できません。
目的の制限	個人データは、指定され明示された適法な目的のためにのみ収集でき、その目的に合わない方法で処理することはできません。	**お客様:** どのような個人データを収集するか、およびその使用目的を決定するお客様です。この決定を行う際に、指定され明示された適法な目的があることをお客様が確認する必要があります。お客様は、その他の目的のためにさらに処理を行うかどうかを決定し、それが当初の目的に合っているかどうかについて評価することができます。 **AWS:** AWS は、お客様がコンテンツを使用してそれを AWS クラウドに保存する目的について一切制御できません。お客様のコンテンツに個人データが含まれていても、AWS は、お客様が選択している AWS サービスをそのお客様に提供するためだけに、そのデータを処理します (ただし、法律や、法的に有効で拘束力のある命令に従う必要がある場合を除く)。

データ主体の権利	データ主体は自身の個人データにアクセスできる必要があり、この指令に従っていない方法で処理されている個人データを修正、抹消、またはブロックできる必要があります。	**お客様:** お客様は、AWS に保存されているコンテンツを統制しているため、コンテンツに含まれる自身の個人データにデータ主体がどのようにアクセスできるかを決定できます。同様に、お客様のデータ処理アクティビティの合法性に関するデータ主体からの要求や苦情に対応するのに最適なのはお客様です。 **AWS:** 前述のように、AWS は、お客様が AWS に保存することを選択したコンテンツの種類およびその目的について一切制御できません。AWS は、このコンテンツについては (個人データが含まれているかどうかについても) 把握していません。AWS は、お客様が AWS に保存することを選択した個人データのデータ主体を特定することも、データ主体に連絡することもできない (お客様自身に関する場合を除く) ため、関連するデータ主体に情報を提供することは一切できません。AWS には、特定の人物が AWS に保存しているデータに接続する機能はありません。その情報を制御できるのはお客様だけです。
正確性	データ管理者は、個人データが正確であり、必要であれば最新の状態に維持されるようにする必要があります。	**お客様:** お客様は、AWS に保存することを選択した個人データに関して制御します。したがって、その正確性を確認および維持する責任があります (必要であれば、更新および訂正できます)。さらに、お客様はクラウド "内の" セキュリティを管理し、その責任を負います。そのため、データの破損から保護するための適切な対策が実装されていることを確認できます。 **AWS:** AWS は、お客様が AWS に保存することを選択したコンテンツの種類について一切制御できず、このコンテンツを把握していません。AWS がお客様の代わりにデータを入力または変更することはありません。したがって、

		このデータの正確性を確認することや、データを更新することはできません。ただし、SOC 1 Type 2 レポートには、基盤となるクラウド環境のレベルでデータの整合性を保つために AWS が実行しているコントロールの詳細が記載されています。
データセキュリティ	データ管理者は、偶発的または違法な破壊、不慮の損失、改変、または不正な開示やアクセスから個人データを保護するために、適切な技術的および組織的な対策を実施する必要があります。	**お客様:** 設計または実装している特定のセキュリティアーキテクチャが、個人データを含む特定の種類のコンテンツに適切であるかどうかを判断できるのはお客様だけです。お客様は、クラウド**内の**セキュリティに責任があります。それには、コンテンツ (および、コンテンツに含まれるすべての個人データ) のセキュリティ、および AWS サービスを使用して適切なアーキテクチャを実装することも含まれます。特に、お客様には、(a) AWS サービスの設定、(b) そのサービスに関連した利用可能なコントロールの使用、(c) 個人データに適切なセキュリティコントロールとバックアップを維持するために必要な措置を講じること (たとえば、暗号化テクノロジーを使用して不正アクセスから個人データを保護する、定期的にアーカイブを作成する) を適切に実施する責任があります。 **AWS:** AWS は基盤となるクラウド環境**の**セキュリティの管理に責任があります。中核となる AWS クラウドインフラストラクチャ、プラットフォーム、サービスに組み込まれているすべてのセキュリティ対策の全リストについては、セキュリティプロセスの概要 [3] のホワイトペーパーをお読みください。 AWS では、AWS がサービスを提供している物理的なデータセンターのセキュリティも含めて、外部の監査人によってセキュリティ対策の有効性が確認されています。お客様の書面による要求と NDA への署名に応じて、AWS は監査

		人のレポートの要約をお客様に提供します。それにより、お客様は AWS のセキュリティ対策を適切に確認できます。AWS は、要請に応じてデータ保護機関にもこの要約を提供します。
データ保持	個人データは、その個人データが収集または処理される目的に必要な期間より長く (識別可能な形式で) 保持しないようにする必要があります。	**お客様:** AWS クラウドに保存されている個人データの使用目的を決定するのはお客様であるため、その個人データを保持する必要がある期間を決定するのもお客様です。お客様は、個人データが必要なくなったときにそれを削除または匿名化できます。 **AWS:** AWS は、保存されているデータに個人データが含まれているかどうか、およびクラウドに保存されている特定のデータをお客様が処理している目的を把握していません。したがって、目的を達成するためにそのデータを保持する必要がある期間について判断できません。 お客様がコンテンツを AWS サービスから削除すると、そのコンテンツは解読不能な形式でレンダリングされるかまたは無効化され、そのコンテンツを保存するために使用されていた AWS の基盤となるストレージ領域は、AWS の標準ポリシーおよび削除のタイムラインに従って、再利用または上書きされる前に完全に消去されます。AWS の処理手順には、AWS サービスを提供するために使用されていたストレージメディアを廃棄する前に実施される安全な廃棄プロセスも含まれています。そのプロセスの一環として、業界標準の方法に従って、ストレージメディアは消磁または消去され、物理的に破壊または無効にされます。

移転	個人データは、移転先の国または地域で個人データの処理に関してデータ主体の権限と自由に対する適切なレベルの保護が保証されている場合を除いて、欧州経済地域外の国または地域に移転することはできません。	**お客様:** お客様は、コンテンツとサーバーが配置される AWS リージョンを選択できます。お客様は、AWS のドイツまたはアイルランドの EU リージョンに専用で AWS サービスをデプロイすることを選択できます。 **AWS:** AWS は、法律や、法的に有効で拘束力のある命令に従う場合を除いて、お客様が選択したリージョン外にお客様のコンテンツを移転することはありません。AWS では、お客様のデータ保護の義務に合わせるために役立つデータ処理追補が提供されています。AWS では、お客様が個人データを EU から欧州経済地域外に移転するために必要な場合は、モデル条項をお客様のデータ処理追補に追加することもできます。AWS のデータ処理追補は、モデル条項を含め、データ保護指令第 29 条作業部会と呼ばれる EU データ保護機関のグループによって 2015 年 3 月 6 日に承認されました。この承認により、モデル条項を必要とするすべてのお客様は、この指令に従って国際的なデータフローを可能にするために十分な契約上のコミットメントを提供する際に、AWS のデータ処理追補に依存できるようになりました。データ保護指令第 29 条作業部会による承認に関する詳細については、次のルクセンブルクデータ保護庁のウェブページを参照してください。 http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html データ処理追補およびモデル条項に加えて、AWS の欧州リージョンから米国リージョンに個人データを転送するお客様は、AWS の EU-U.S.Privacy Shield Framework への参加による恩恵も受けることができます。EU-U.S.Privacy Shield Framework はお客様による AWS の使用方法または作業方法に影響しませんが、EU によって認

		可された、欧州から米国に個人データを転送するための追加のメカニズムを提供します。EU-US Privacy Shield Framework に基づく米国サービスプロバイダーの義務の詳細については、以下の欧州委員会のウェブサイトを参照してください。http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm また、EU-U.S.Privacy Shield Framework のウェブサイトは以下を参照してください。https://www.privacyshield.gov/welcome.

データ漏えい

お客様が AWS の使用時に個人データの管理と制御を維持する場合、お客様は自身の環境でプライバシー違反を監視し、該当する法律で義務付けられているように法律規制当局と影響のある個人に通知する責任があります。この責任を管理できるのはお客様だけです。

お客様は自身のアクセスキーを制御し、AWS アカウントへのアクセスを誰に許可するかを決定します。AWS ではアクセスキーを確認できず、アカウントへのログインが誰に許可されていて誰に許可されていないか分からないため、アクセスキーの使用、悪用、配布、消失を監視する責任はお客様にあります。

該当する法律で義務付けられているように、AWS ネットワークに関する AWS セキュリティ基準の違反を AWS が実際に確認した場合は、AWS はお客様に迅速に通知します。

請負業者

AWS では、サービスのプロビジョニングを支援するために多数のサードパーティーの請負業者を利用しています。ただし、それらの請負業者にはお客様のコンテンツへのアクセス権はありません。さらに、AWS では信頼できる請負業者のみを利用し、必要な基準が維持されるように監視する適切な契約上の保障措置を講じています。

お客様のサードパーティーサービスプロバイダー

本書で前述したように、AWS 環境はサードパーティー (インターネットサービスプロバイダーなど) によって直接提供される他のサービスにも接続しています。これらのサードパーティーは、セキュリティを含めて自身のシステムに関して責任があり、AWS はこれらのサードパーティーのアクティビティには責任を負いません。

その他の考慮事項

このホワイトペーパーでは、この指令以外のプライバシー関連の他の法律については説明していません。それらも、お客様に関係がある可能性があります (業界特有の要件など)。個々のお客様に適用されるプライバシーおよびデータ保護関連の法律および規制は、お客様がビジネスを行う場所、運営する業界、保存するコンテンツの種類、コンテンツの出所または作成者、コンテンツの保存場所などのいくつかの要因に依存します。

プライバシー規制の義務について懸念があるお客様は、まず適用される要件を特定および理解してから、適切な助言を求める必要があります。

最後に

AWS では、セキュリティは常に最優先事項です。AWS は、190 か国以上で、エンタープライズ、教育機関、政府機関を含めて数十万のビジネスにサービスを提供しています。AWS のお客様には金融サービスプロバイダーや医療サービスプロバイダーも含まれていて、個人の健康データや財務記録などの最も機密性が高い情報に関しても AWS は信頼を得ています。

AWS サービスは、保存場所、保存方法、アクセス権の許可などのコンテンツの制御だけでなく、お客様のソリューションの設定とデプロイの方法に関しても、お客様に柔軟性を提供するように設計されています。AWS のお客様は独自の安全なアプリケーションを構築し、コンテンツを AWS に安全に保存できます。

その他のリソース

プライバシー保護およびデータ保護の要件にどのように対処できるかについてお客様がさらに理解を深めるために、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のホワイトペーパー、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参照いただくことをお勧めします。この資料については、http:/aws.amazon.com/compliance および http://aws.amazon.com/security を参照してください。

AWS では、AWS クラウドで利用可能で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習得し、AWS のサービスとソリューションに熟達するのに役立つトレーニングも提供しています。無料の講習動画、セルフペースラボ、インストラクター主導のクラスが用意されています。AWS トレーニングの詳細については、http://aws.amazon.com/training/ を参照してください。

AWS 認定では、AWS テクノロジーを使用して安全で信頼できるクラウドベースの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に関する技術的なスキルと知識が認定されます。AWS 認定の詳細については、http://aws.amazon.com/certification/ を参照してください。

さらに詳細な情報が必要な場合は、https://aws.amazon.com/contact-us/ から AWS にお問い合わせいただくか、またはローカル AWS 顧客担当者までお問い合わせください。