Microsoft Azure

Microsoft Azure のプライバシーの概要

2014 年 2 月

目次

はじめに

マイクロソフトは、クラウド サービスの課題として企業がプライバシーの保護に懸念を抱いていることを認識しており、企業にクラウドのメリットを実感していただけるように、強力なプライバシー保護機能を Microsoft Azure サービスに実装して顧客データのプライバシー確保に努めると共に、お客様が、データがどこにあり、だれがアクセスできるのかを明確に認識できるように透明性の確保と維持に注力しています。

このドキュメントでは、クラウドのプライバシーに対するマイクロソフトのアプローチと具体的なポリシー、運用方法、および Microsoft Azure の顧客データのプライバシーを確保するために導入しているテクノロジについて説明します。

クラウドのプライバシーに対するマイクロソフトのアプローチ

マイクロソフトは堅牢なオンライン ソリューション実現の先駆者であり、20 年間にわたってお客様のプライバシーを保護しており、現在では、世界各地で膨大な数のお客様が利用する 200 以上のクラウド サービスおよびオンライン サービスを運営しています。弊社のエンタープライズ クラウド サービスである Office 365 や Microsoft Azure は数百万人規模のエンド ユーザーが利用しており、彼らが勤める企業のミッションクリティカルなデータはマイクロソフトがお預かりしています。

こうした経験をもとに、業界をリードするビジネス プラクティス、プライバシー ポリシー、コンプライアンス プログラム、セキュリティ対策を策定し、弊社のクラウド コンピューティング エコシステム全体に導入しています。企業が自社データの収集、利用、配布を管理できるようにすることを念頭に長年にわたって実証を重ねてきたマイクロソフトのプライバシー保護の取り組みは、お客様のプライバシー要件に応え、クラウド コンピューティングに対する信頼性を向上するための確固たる基盤となっています。

Microsoft Azure の顧客データ

Microsoft Azure ではお客様が自らのデータを所有します。マイクロソフトでは、顧客データは「本サービスの利用を通じてお客様がマイクロソフトに提供する、またはお客様のためにマイクロソフトに提供されるすべてのテキスト、音声、ソフトウェア、画像ファイルを含むすべてのデータ」と定義しています。これには、たとえば、保管または処理するためにアップロードするデータや、Microsoft Azure で実行するアプリケーションが含まれます。Microsoft Azure のデータの分類の詳細については、Microsoft Azure トラスト センターを参照してください。

お客様は、いつでも理由にかかわらず、また、通常マイクロソフトの支援を得ることなく、顧客データを取得できます。お客様がデータを削除したり、サービスの利用を終了したりすると、マイクロソフトは管理下にあるすべてのシステムから顧客データを消去します。シス

テムが寿命を迎えると、マイクロソフトの運営担当者が厳格なデータの取扱手順とハードウェアの廃棄手順に従って処理を行います。

顧客データの場所

データの保存場所を知ること、そしてその場所を管理することは、多くのお客様にとってコンプライアンスおよびガバナンスにおける重要な要素です。Microsoft Azure では顧客データを保管するマイクロソフト データセンターの所在地 ("geo" および "リージョン" と呼ばれる) をお客様が指定できます。利用可能な geo およびリージョンは下表のとおりです。

Geo	リージョン
アジア太平洋	アジア太平洋東部 (香港) アジア太平洋南東部 (シンガポール)
ヨーロッパ	北ヨーロッパ (アイルランド) 西ヨーロッパ (オランダ)
米国	米国中北部 (イリノイ州) 米国中南部 (テキサス州) 米国東部 (バージニア州) 米国西部 (カリフォルニア州)
日本	東日本 (埼玉県) 西日本 (大阪府)

最新の geo およびリージョンのリストについては、Microsoft Azure のトラスト センターを参照してください。データセンターのグローバル ネットワークについては、Microsoft Azure のリージョンのページを参照してください。

マイクロソフトはデータの冗長化確保などを目的に、顧客データを同一 geo 内で転送することがあります (例: 北ヨーロッパから西ヨーロッパへ転送)。たとえば、データセンターで大規模な災害が発生した場合のデータの高耐久性を確保するために、Microsoft Azure は同一 geo 内の 2 つのリージョン間で BLOB データおよびテーブル データをレプリケートします。

マイクロソフトは、顧客データをお客様が指定した geo の外部に転送することはありません (例: ヨーロッパから米国へ、米国からアジアへ)。ただし、カスタマー サポートの提供、サービスのトラブルシューティング、法的要件の遵守のために必要となる場合、または Microsoft Azure トラスト センターで説明する特定の機能およびサービスを使用して geo 外部に顧客データを転送できるようお客様がアカウントを設定している場合は除きます。

お客様またはお客様のエンド ユーザーがどの geo から顧客データにアクセス可能かをマイクロソフトが管理または制限することはありません。

データのアクセスおよび使用

マイクロソフトのスタッフによる顧客データへのアクセスは禁止されています。顧客データへのアクセスは、お客様による Microsoft Azure の利用を支援するために必要な場合に限られ、これには Microsoft Azure の運用に影響する問題の防止、検知、修正を目的としたトラブルシューティング、およびユーザーに対する新たな脅威や進化した脅威 (マルウェアやスパムなど) を検知および防止する機能の改良が含まれます。アクセスが許可されると、細心の注意をもってアクセスを制御し、アクセス履歴を記録します。多要素認証などの強力な認証により、承認を得たスタッフにアクセス権の付与を限定できます。不要になったアクセス権は直ちに無効となります。

Microsoft Azure では顧客データを広告付きサービスと共有することはありません。また、広告を目的とした顧客データのデータ マイニングを行うこともありません。

Microsoft Azure の顧客データへのアクセスおよび使用を規定する運用手順および統制手続は厳格に行われており、公認監査法人による検証を定期的に実施しています。

契約上の義務履行の努力

マイクロソフトは、顧客データの安全を確保しプライバシーを保護するという契約上の義務を果たすことに尽力しています。個人データに関する追加の統制手段をあらゆる地域および業種のお客様に提供することもその 1 つです。

EU データ保護指令

欧州の法律は、特定の条件下を除き、企業が個人データを EU から外部へ転送することを禁じています。こうしたデータの転送を可能にする方法の 1 つとして、米国と EU 間のセーフ ハーバー フレームワークおよびスイスと米国間のセーフ ハーバー フレームワークを遵守する企業からクラウド サービスを調達することができます。

欧州企業のデータのプライバシー保護に対する要求に応えるべく、マイクロソフトは米国商務省によるセーフ ハーバーの認定 (英語) を取得しています。このセーフ ハーバー認定の取得により、合法的に EU 内の個人データを EU 外部のマイクロソフトに転送して処理することが可能になります。これにより、お客様が指定したリージョンの外部にデータが転送されるケースに対応できます。また、マイクロソフトは企業顧客に対して次の契約上の義務を果たします。

- データ処理契約: マイクロソフトによる EU データ保護指令の遵守および ISO/IEC 27001:2005 適用範囲内の Microsoft Azure コア機能に対する関連セキュリティ要件の詳細が記載されています。
- EU モデル契約条項: ISO/IEC 27001:2005 適用範囲内の Microsoft Azure コア機能について、個人情報の転送に関する追加の契約上の保証事項が盛り込まれています。

HIPAA 事業提携者契約 (Business Associate Agreement: BAA)

Microsoft Azure は、医療保険の携行性と責任に関する法律 (Health Insurance Portability and Accountability Act: HIPAA)、および、経済的および臨床的健全性のための医療情報技術に関する法律 (Health Information Technology for Economic and Clinical Health Act: HITECH) も遵守しています。これらの米国法は、保護対象の医療情報 (Protected Health Information: PHI) と呼ばれる患者情報にアクセスする医療関連法人に適用されます。これらの法律が適用される医療関連法人が Microsoft Azure のようなクラウド サービスを使用する際、そのサービスを提供する側は多くの場合、HIPAA および HITECH 法が定めるセキュリティおよびプライバシーに関する特定の規定を遵守することを書面にて同意する必要があります。お客様が HIPAA および HITECH 法を遵守するのを支援するために、マイクロソフトは企業のお客様に事業提携者契約 (BAA) を契約の補遺として提供しています。

BAA の署名に先立ち、お客様には Microsoft Azure HIPAA 履行ガイダンス (英語) をお読みいただき、関連する Microsoft Azure の機能について理解していただく必要があります。このガイダンスでは HIPAA に準拠したアプリケーションを構築するためのベスト プラクティスをいくつか紹介しているほか、セキュリティ侵害への対処に関する Microsoft Azure の規定を詳細に説明しています。

下請業者

マイクロソフトは、カスタマー サポートなど一部のサービスの提供を他社に委託することがあります。マイクロソフトが顧客データを下請業者に開示するのは、下請業者に委託したサービスを下請業者が提供できるようにするという目的に限られます。下請業者はそれ以外の目的のために顧客データを使用してはならず、弊社のお客様の情報の秘密を保持することが要求されます。

マイクロソフトは、下請業者に対してマイクロソフトのサプライヤー セキュリティ & プライバシー アシュアランス プログラムへの加入、契約上のプライバシー保護要件の遵守、プライバシー保護に関する定期研修の受講を要求します。マイクロソフトが管理する施設または設備を使用して業務を行う下請業者は、マイクロソフトのプライバシー基準に従うことが契約により義務付けられます。その他のすべての下請業者については、マイクロソフトのプライバシー基準と同等のプライバシー基準に従うことが契約により義務付けられます。Microsoft Azure の顧客データを処理する権限を持つ下請業者の一覧はこちら (英語) からダウンロードできます。

法執行機関の要求

マイクロソフトは、お客様のデータは、保存場所が自社内かクラウド サービスかを問わず、お客様が管理すべきものと考えています。このため、お客様から指示された場合または法律により義務付けられている場合を除き、顧客データを第三者 (法執行機関、その他の政府機関または民事係争者を含む) に開示することはありません。第三者から顧客データの提供を要求された場合、マイクロソフトは直接お客様から顧客データを要求するよう第三者に要請します。その際、お客様の基本的な連絡先情報を第三者に提供する場合があります。マイク

ロソフトは、裁判所命令または令状の提示をもって法執行機関に対するコンテンツの開示を検討します。やむを得ず第三者に顧客データを開示する場合は、法律で禁止されている場合を除き、その旨を速やかにお客様に通知し、開示要求の内容をお客様にご連絡いたします。

また、マイクロソフトはこうした要求の範囲や件数を示した法執行機関要求レポート (英語) を発行します。顧客データの要求に対するマイクロソフトの対応の詳細については、マイクロソフトのゼネラル カウンセルが執筆したブログ記事「顧客データの提供を要求する政府機関への対応 (英語)」を参照してください。

ビルトインのデータ保護

マイクロソフトは、お客様が自らのデータとプライバシーを保護できるように Microsoft Azure プラットフォームを設計および実装しています。Microsoft Azure はお客様が次のことを実現するために役立つインフラストラクチャを提供します。

- データやアプリケーションへのアクセス管理
- 通信中のデータおよび保存されたデータの保護
- Microsoft Azure との安全な接続

ID およびアクセス

マイクロソフトは、Microsoft Azure やその他のマイクロソフト クラウド サービス全体で利用できる包括的な ID およびアクセス管理ソリューションを提供しています。Microsoft Azure については、お客様が自らのデータやアプリケーションへのアクセスを制御することを可能にする以下の機能が用意されています。

- **エンタープライズ クラウド ディレクトリ:** 企業はオンプレミスの ID を Microsoft Azure Active Directory に同期してシングル サインオンを実現し、クラウド アプリケーションへのユーザー アクセスを簡単にすることができます。
- **アクセス監視:** セキュリティ レポートを通じて一貫性のないアクセス パターンを監視し、潜在的な脅威を抑制します。
- **強力な認証:** Microsoft Azure の多要素認証では、パスワードとパスワード以外の認証手段を併用することで不正なアクセスを阻止します。
- **ロールベースのアクセス制御:** 承認スキームを実装すると、ユーザーに割り当てられたロール、ロールの承認、およびアクセス許可の承認に応じてリソースへのユーザーのアクセスを制御できます。

データの暗号化と分離

Microsoft Azure は暗号化、隔離、破壊という 3 つの手法によって顧客データを保護します。

- **通信中のデータ:** Microsoft Azure では、ユーザー デバイスとマイクロソフト データセンター間の通信やデータセンター内での通信に、業界標準の転送プロトコルである SSL や TLS などを使用します。また、IPsec を使用して Microsoft Azure 仮

想ネットワーク (VNET) による VPN 接続を確立することもあります。お客様は所有する仮想マシンとエンド ユーザー間のトラフィックを暗号化することができます。

- **保存されたデータ:** Microsoft Azure に保管されているデータがお客様の基準に沿って暗号化されているかどうかは、お客様の責任で確認していただくことになります。Microsoft Azure には幅広い種類の暗号化機能が用意されており、お客様は自分のニーズに最適なソリューションを選択できます。そうした選択肢として .NET 暗号化サービス、Windows Server 公開キー インフラストラクチャ (PKI) コンポーネント、Microsoft StorSimple クラウド統合ストレージ、Active Directory Rights Management Services (AD RMS) などが用意されており、データのインポート/エクスポートには BitLocker を使用できます。
- **データの分離:** Microsoft Azure はマルチテナント サービスです。つまり、複数のお客様のデプロイメントおよび仮想マシンが同一の物理ハードウェア上に保管されています。Microsoft Azure ストレージでは、論理的分離により顧客データを他の顧客のデータから隔離しています。これによりマルチテナント サービスのスケール面および経済面でのメリットが生まれると共に、他の顧客データへのアクセスを厳格に阻止します。
- **データの破壊:** お客様がデータを削除したり Microsoft Azure の利用を終了した場合、ストレージ リソースの再利用に先立ち厳格な基準に従ってリソースを上書きし、廃棄処分となったハードウェアを物理的に破壊します。

ネットワーク セキュリティ

Microsoft Azure ネットワーキングは、仮想マシンどうしのセキュアな接続や、オンプレミスのデータセンターと Microsoft Azure 仮想マシン間の接続に必要なインフラストラクチャを提供します。Microsoft Azure は、ファイアウォール、NAT、パーティション化されたローカル エリア ネットワークおよび外部と接続したインターフェイスからのバックエンド サーバーの物理的分離など、さまざまな技術を用いてマイクロソフト データセンターへの、そしてマイクロソフト データセンター内での不正なトラフィックを阻止します。

- **顧客データとネットワークの分離:** 顧客間の分離は、あらゆる共有型クラウド アーキテクチャに不可欠な条件です。Microsoft Azure では、サブスクリプション 1 つにつき複数のデプロイメント、デプロイメント 1 つにつき複数の仮想マシンを利用できます。また、デプロイメントおよび仮想ネットワークがそれぞれ分離されます。顧客が定義したエンドポイントを通過したものを除き、個別の仮想マシンがインターネット トラフィックを受信することはありません。
- **通信の暗号化:** ビルトインの暗号化テクノロジにより、お客様はデプロイメント内およびデプロイメント間の通信、Microsoft Azure リージョン間の通信、Microsoft Azure からオンプレミス データセンターへの通信を暗号化できます。これらのプロトコルによってネットワークの既定のセキュリティ レベルが向上し、ビジネス ニーズに応じて柔軟に Microsoft Azure を構成できるようになります。管理者はリモート デスクトップやリモート Windows PowerShell から仮想マシンにアクセスできます。また、Microsoft Azure 管理ポータルは常時暗号化されています。

- **Express Route の使用:** オプションの Express Route プライベート ファイバー リンクを使用して Microsoft Azure データセンターに接続することで、トラフィックがインターネットに流れるの防ぐことができます。

まとめと関連情報

マイクロソフトは Microsoft Azure の構築、デプロイ、管理において不可欠な要素であるプライバシー保護に長年にわたって取り組んでおり、プライバシー保護対策における透明性の維持、プライバシー保護に関して有効な選択肢をお客様に提供すること、保管するデータを責任を持って管理することに努めてきました。

顧客データのプライバシー保護を支援するために導入しているポリシー、運用プロセス、およびテクノロジをお客様に理解していただけるように、Microsoft Azure のプライバシー、セキュリティ、コンプライアンスの詳細をトラスト センターで公開し、監査報告書やコンプライアンス パッケージを開示しています。

また、クラウド サービス全体の顧客データを保護するためにマイクロソフトが行っている取り組みに関する全般的な情報については、Microsoft Cloud Privacy Web サイト (英語) およびホワイトペーパー「クラウド コンピューティング時代のプライバシー」を参照してください。

関連情報

- Microsoft Azure のプライバシーに関する声明
- Microsoft Trustworthy Computing Web サイトのプライバシー ページ (英語)
- 法執行機関要求レポート (英語)
- クラウド導入に向けたデータ分類 (英語)
- データ分類に関する CISO の見解 (英語)