Microsoft

クラウド内のデータとプライバシーの保護

目次

企業がクラウド コンピューティングのメリットを享受するには、最も貴重な資産の 1 つである顧客データをクラウド プロバイダーに安心して任せなければなりません。このホワイトペーパーでは、Windows Azure、Office 365、Dynamics CRM Online、Windows Intune を含むマイクロソフトのエンタープライズ サービスにおける、顧客データのプライバシーを保護するためのアプローチとプロセスの概要を説明します。クラウドのプライバシーに関する課題について取り上げた後、サービス構築時にサービスのプライバシー保護を確保し、データセンターでサービスを運用し、お客様がクラウドでデータ プライバシーを保護するために多くの情報に基づいて選択できるようにする方法について説明します。

クラウド内のデータとプライバシーの保護 - 概要

クラウド サービスの分類

- **Software as a Service (SaaS):** クラウド プロバイダーは Microsoft Dynamics CRM Online などの単一のアプリケーション、またはマイクロソフトの Office 365 などのアプリケーション スイートをホストします。Office 365 には、Exchange Online や SharePoint® Online などの複数の製品が含まれています。
- **Platform as a Service (PaaS):** ユーザーは独自のソフトウェア アプリケーションを作成して実行しますが、ソフトウェア開発ツールや、基盤となるインフラストラクチャおよびオペレーティング システムはクラウド プロバイダーに依存します。マイクロソフトの Windows Azure™ はこのようなクラウド プラットフォームの 1 つです。
- **Infrastructure as a Service (IaaS):** ユーザーはコンピューティング機能 (実際のハードウェアまたは仮想マシン) を借用して、自らのオペレーティング システムとソフトウェア アプリケーションを展開して実行します。Windows Azure はこのタイプのサービスも提供します。

政府、非営利団体、企業をはじめとする世界中のあらゆる組織にとって、クラウド コンピューティングは今日の IT 戦略の中核となっています。クラウド サービスを利用することで、あらゆる規模の組織が事実上無制限のデータ ストレージへアクセスできるようになり、独自のネットワークとコンピューター システムを購入、管理、更新する必要がなくなりました。マイクロソフトとその他のクラウド プロバイダーは、IT インフラストラクチャ、プラットフォーム、ソフトウェアを「サービスとして」提供しているため、お客様は必要に応じて規模を拡大 / 縮小することができ、使用したコンピューティング機能とストレージ分の代金を支払えば済むようになっています。

組織は、選択肢の広がりや、俊敏性と柔軟性の向上といったクラウド サービスのメリットを享受し、効率性を高めて IT コストを抑えることができます。しかしその一方で、クラウド サービスの導入がプライバシー、セキュリティ、コンプライアンスへの取り組みに与える影響についても把握しておく必要があります。マイクロソフトは、スケーラブルで信頼性が高く、管理性に優れたクラウド サービスを実現する一方で、クラウド サービス内のお客様のデータが保護され、透明性の高い状態で使用されるシステム作りについても取り組んできました。

お客様は、左記に示すような多数のクラウド サービスやクラウド インフラストラクチャの中から選んでご購入いただけます。最適なクラウド モデルは、お客様のニーズ、データ保護要件、必要となる処理タイプにより異なってきます。データ クラスが多岐にわたる組織の場合、「万能型」アプローチは適切とはいえません。特殊なデータ保護要件を持つ組織には、選んだデータをお客様がオンプレミスで保持できる、プライベート クラウドまたはハイブリッド クラウドのソリューションが適しています。マイクロソフトはあらゆるプライベート クラウドおよびハイブリッド クラウド ソリューションを取り揃えています。最近では『Microsoft Private Cloud: A comparative look at Functionality, Benefits, and Economics』(マイクロソフト プライベート クラウド : 機能、メリット、経済性の比較検証) というホワイトペーパーを公開しました。

言うまでもなくセキュリティは、優れたデータ保護を実現するうえで、あらゆるオンライン コンピューティング環境において欠かせない要素です (関連のホワイトペーパー『Information Security Management System for Microsoft Cloud Infrastructure』(マイクロソフトのクラウド インフラストラクチャにおける情報セキュリティ マネジメント システム) を参照してください)。消費者や企業が特定のクラウド コンピューティング製品の導入を検討する場合、情報のプライバシーが保護され、自らの顧客の期待に沿ってデータが使用されることを確信できることが大前提となります。

クラウド コンピューティングのインフラストラクチャ

- **パブリック クラウド:** お客様はクラウド サービスにアクセスし、複数の組織のデータを格納した何百もの仮想サーバーを備えた巨大なデータセンターにドキュメントを保存します。
- **プライベート クラウド:** 単一組織が専用のクラウド インフラストラクチャを使用します。
- **コミュニティ クラウド:** 共通の任務や関心、懸念材料を持つ組織のグループが、プライベート クラウドを共有します。たとえば、クラウド プロバイダーが政府機関専用のクラウドに、サービスのインスタンスを提供する場合などです。
- **ハイブリッド クラウド:** プライベート クラウドをパブリック クラウドに広げ、組織のデータセンターを拡張するもの、または、複数のタイプのクラウドをつなぎ、データとアプリケーションを制御しながら相互に利用するものを指します。

マイクロソフトは 20 年にわたり、お客様のプライバシーを保護する堅牢なオンライン ソリューションの構築におけるリーダー的役割を果たしてきました。今日、マイクロソフトは世界各地で何億人ものお客様が利用する、200 以上のクラウド サービスとオンライン サービスを運用しています。Office 365 や Windows Azure といった企業向けクラウド サービスは、ミッションクリティカルなデータをマイクロソフトに委任した企業で働く数百万人ものエンド ユーザーによって利用されています。

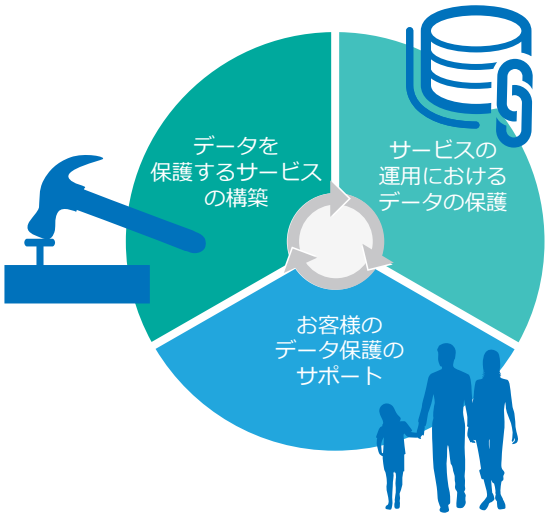
マイクロソフトはその経験に基づき、業界をリードするビジネス プラクティス、プライバシー ポリシー、コンプライアンス プログラム、セキュリティ対策を発展させ、これらをマイクロソフトのクラウド コンピューティングのエコシステム全体に適用することができます。マイクロソフトは、クラウド サービスが特有のセキュリティやプライバシーの問題を引き起こす可能性があることを認識しています。しかしながら、マイクロソフトの実績あるポリシーやプラクティスがお客様の懸念に対処する確固たる基盤となり、クラウド コンピューティングの信頼性をさらに高めることができると考えています。

クラウド サービスにおけるプライバシーおよびデータ保護に対するマイクロソフトのアプローチは、組織の情報の収集、使用、配布の制御をサポートする取り組みを基盤としています。この機能を提供し、優れた運用プラクティスを実装してデータ保護を実現することにより、マイクロソフトは認証、証明、契約の合意という形で、お客様に対してコンプライアンスについての責任を果たすことができます。マイクロソフトは欧州連合模範条項に署名した最初の企業の 1 つで、EU 諸国で事業を行うお客様のデータを保護する義務を文書化しています。Generally Accepted Privacy Practices (GAPP) や Fair Information Practice Principles (FIPP) といった基準の順守と同様に、欧州連合模範条項の順守は、お客様とパートナーの情報の管理に使用するマイクロソフト独自のプライバシー原則を作成する際の指針となりました。

マイクロソフトのプライバシー原則、データ処理に関する合意、企業のプライバシー ポリシーはすべて、マイクロソフトのすべてのお客様およびパートナーの情報の収集と使用の統制に役立っています。さらに、従業員が全社的にプライバシー コンプライアンスを順守するのに役立つ明確な枠組みを提供しています。

マイクロソフトは、オンライン アプリケーションが準拠しているプライバシー ポリシーと行動規範を定期的に見直し、消費者のニーズや期待に応えて変更する必要がある場合には、定期的に変更しています。

クラウド サービス全体にプライバシーおよびデータ保護対策を施すためのマイクロソフトの取り組みは、次の 3 つに分類されます。



第 1 に、マイクロソフトは顧客データを保護するために、クラウド サービスをゼロから構築しています。第 2 に、サービス実施中にデータセンターの顧客データを保護するために、標準ベースの技術とアプローチを使用しています。第 3 に、お客様が自らのデータを保護し、事業に該当するコンプライアンス要件を満たすのに最適な決定を行えるようにお客様をサポートします。

このホワイトペーパーの残りの部分では、これらの各アプローチについて詳しく説明していきます。

データを保護するサービスの構築

マイクロソフトは、システムとデータの整合性だけでなく、お客様のプライバシーを保護するサービスを構築するように、すべてのクラウド プロバイダーに働きかけています。マイクロソフトはエンタープライズ ソフトウェア ソリューション構築の経験を生かし、マイクロソフトのサービスに対するお客様の信頼を勝ち得るのに必要な、プライバシーとデータ保護の要件を把握します。

クラウド サービス構築時、お客様のデータを保護する際に鍵となる事項

- **積極的な取り組み:** 顧客データを保護し、利用を制限する。
- **「設計によるプライバシー」の原則に従う:** お客様のプライバシーを考慮したサービスをゼロから構築する。
- **機能の提供:** クラウド サービス内の情報をお客様が保護および管理するのに役立つ機能を提供する。

データ保護とデータ使用の制限に関する責任

マイクロソフトでは、企業がクラウド サービスでホストするデータはその企業に属するものであり、お客様のサービスを提供する以外の目的でクラウド プロバイダーが使用してはならないと考えています。この概念はエンタープライズ クラウド サービスの契約書に盛り込まれており、セキュリティ センターの Web サイトに説明が掲載されています。マイクロソフトでは、顧客データを「オンライン サービスの使用を通してお客様またはお客様の代理がマイクロソフトに提供する、すべてのテキスト、サウンド、ソフトウェア、またはイメージ ファイルを含むすべてのデータ」と定義しています。広告など、サービスの提供と関係のない目的で顧客データを使用することはありません。さらに、各サービスはデータの保存とバックアップのための一連の基準を設けており、お客様からの要求に応じてデータを安全に削除します。

設計によるプライバシー

新しい製品またはサービスを計画する際、マイクロソフトは開発の各段階で、プライバシーとデータ保護について検討しています。これは設計によるプライバシーに対するアプローチの一部です。設計によるプライバシーとは、製品の構築方法だけでなく、サービスの運用方法や内部のガバナンス プラクティスを構成する方法も同時に示したものです。この包括的なアプローチには、お客様のプライバシー保護の維持と強化をサポートするすべての人、プロセス、技術が含まれています。

プライバシーへの配慮は、マイクロソフトのセキュリティ開発ライフサイクル (SDL) 全体に組み込まれています。SDL は、開発者がより安全なソフトウェアを構築し、セキュリティとプライバシーのコンプライアンス要件を満たしながら、開発コストを削減するのに役立つソフトウェア開発プロセスです。マイクロソフトのすべてのクラウド サービスで SDL を採用することで、サービスとその機能の安全性を確保し、データ保護とプライバシー要件に対応しています。

SDL は 7 つのフェーズで構成されています。これらのフェーズには、開発者やプログラム マネージャーが基本的な概念について理解するためのトレーニング、プライバシーを保護する安全なソフトウェアの構築、セキュリティやプライバシーの問題が発生したときの対処方法が含まれています。

開発時に一貫したプライバシー プラクティスを実施するためのツールの 1 つに Microsoft Privacy Standards (MPS、マイクロソフト プライバシー標準) があります。このツールでは、標準となるプライバシー機能とプラクティスが定義されています。セキュリティはプライバシーに不可欠なので、このようにしてプライバシーとセキュリティのプロセスを補完的に連携させることにより、ソフトウェア コードの脆弱性を最低限に抑え、データ侵害を阻止するだけでなく、開発者は最初からマイクロソフトの製品とサービスにプライバシーへの配慮を組み込むことができます。Windows Azure、Office 365、Dynamics CRM Online、その他の企業を対象としたクラウド サービスはすべて、SDL と MPS に文書化されたプロセスを使用しています。ベスト プラクティスを IT 業界やプライバシー コミュニティで共有させようというマイクロソフトの取り組みの一貫として、マイクロソフトは『Privacy Guidelines for Developing Software Products and Services (ソフトウェア製品およびサービス開発のプライバシー ガイドライン)』の公式版を公開しました。

開発プロセスの一部としてプライバシー レビューが実施され、プライバシー要件が適切に対処されているかどうかが確認されます。マイクロソフトのクラウド サービスにおいて、これらのレビューで次のことが確認されます。

- データにアクセスできる人をお客様が制御し、法令上のプライバシー要件を満たすようにお客様がサービスを構成できる、プライバシー関連機能が存在するかどうかを確認する。
- プライバシー リスクを特定する。
- マイクロソフトのエンジニアリング　グループが実装できる、必須の仲介アクションを特定する。
- すべての要件が満たされているかどうかを最終レビューで確認する。

さらに、マイクロソフトの「信頼できるコンピューティング」イニシアチブの一環として、マイクロソフトでは、プライバシー保護に特化した 40 人以上のフルタイム スタッフを雇用しています。また、それ以外の 100 人以上の従業員の職責に、データ プライバシーの保護を盛り込んでいます。これらの従業員の一部はクラウド サービス製品グループに所属し、各サービスが企業のプライバシー要件を満たすようサポートしています。これらの従業員は、マイクロソフトの全従業員にプライバシーに関するガイダンス、教育、ガバナンスを提供する Trustworthy Computing (信頼できるコンピューティング) 部門のプライバシー グループと連携して作業を行います。

プライバシーを保護するためのサービス機能

お客様のプライバシーを保護するための投資とプロセスに加えて、マイクロソフトは高度なデータ保護およびセキュリティの機能をサービスに実装しています。たとえば、Office 365 と Dynamics CRM Online は両方とも、包括的な ID およびアクセス管理のクラウドソリューションである Windows Azure Active Directory を利用しています。お客様がこれらのサービスのいずれかでアカウントを作成すると、自動的に Active Directory クラウド アカウントが付与され、ユーザーのシームレスなシングル サインオン エクスペリエンスが実現します。オンプレミスのディレクトリを Windows Azure Active Directory に拡張することも可能で、企業の 1 組の資格情報を使ってクラウドベースのリソースに対して認証を行うことができます。

Windows Azure Active Directory アカウントを Office 365 または Dynamics CRM Online サブスクリプションへ自動的に含めることで、お客様はディレクトリ サービスから提供される数多くのセキュリティおよびプライバシー機能を利用できるようになっています。ソリューションには次のものがあります。

- **フェデレーション ID とアクセス管理:** お客様が複数のサービスを購入する場合。組織が Office 365、Dynamics CRM Online、Windows Intune などのその他のマイクロソフト サービスを購入する場合、同じ Active Directory アカウントを使用できます。また、組織は各サービスの ID を統一したり、既存のオンプレミスの Active Directory サービスを使用することによって、ハイブリッド クラウドに対するマイクロソフトのサポートを利用することもできます。これにより、オンプレミスとクラウド両方の企業リソースへのアクセスを管理するための単一の場所が管理者に提供されるので、複雑さが軽減されてエンドユーザー エクスペリエンスが改善されます。マイクロソフトのハイブリッド クラウドに対するサポートの詳細については、マイクロソフトのサイト「Server and Cloud Platform」の「ハイブリッド クラウド」のページを参照してください。
- **Rights Management サービス (RMS):** RMS を使用し、情報と共に保存されている一貫した使用ポリシーに基づいて情報を保護することにより、情報の保存場所にかかわらず、組織はデータ保護戦略を強化することができます。Office 365 には RMS 機能が組み込まれているため、電子メールや Word、Excel、PowerPoint によって作成されたドキュメントを RMS で保護することができ、機密情報の保護に役立ちます。情報を開いたり、変更、印刷、転送したりできるユーザーを指定することができます。組織は「機密情報-読み取り専用」などのカスタマイズされた使用ポリシー テンプレートを作成し、これを情報に直接適用することができます。

これらの Active Directory 機能に加えて、Office 365 の Exchange Online 電子メール サービスには優れたデータ損失防止 (DLP) サービスが含まれています。DLP は、組織が内容を詳しく分析して機密情報を識別、監視、保護するのに役立ちます。ビジネス上重要な電子メールには保護すべき機密データが含まれているため、企業のメッセージ システムにとって DLP はますます重要になっています。DLP は電子メールをスキャンして、金銭に関する情報、個人を特定できる情報 (PII)、知的財産データを探し、一致する内容を含む電子メールが見つかった場合には、データが外部へ送信されないようにブロックしたり、暗号化を要求するといった措置を講じます。

サービスの運用におけるデータの保護

優れた設計と実装に基づいたサービスであっても、安全でない環境で情報が展開されれば、顧客データやプライバシーを保護することはできません。お客様は、データが他のクラウド ユーザーに公開されないと考えています。また、データセンターで使用されているプロセスやそこで働く人々はすべて、データのプライバシー保護と安全の確保に貢献していると考えています。

これを実現するためには、計画と連携、そしてしっかりとトレーニングを受けたチームが必要です。このセクションでは、サービスの実施中に、顧客データのプライバシー保護に使用するプロセスと手順について説明します。また、お客様のプライバシーに関する企業の義務と責任に対処するために、サービスが準拠している重要なデータ プライバシーの基準を取り上げ、お客様が規制機関の IT プライバシーおよびセキュリティ要件を満たすためにサービスがどのように役立っているかを説明します。さらに、お客様が法律機関、政府機関、顧客に対してコンプライアンスを実証できるようにマイクロソフトが取り組んでいる、お客様への透明性の確保について説明します。

マイクロソフトのクラウド サービス セキュリティ センター

Dynamics CRM セキュリティ センター
http://www.microsoft.com/ja-jp/dynamics/crm-trust-center.aspx

Office 365 セキュリティ センター
http://office.microsoft.com/ja-jp/business/FX103030390.aspx

Windows Azure のトラスト センター
http://azure.microsoft.com/ja-jp/support/trust-center/

Windows Intune セキュリティ センター
http://www.microsoft.com/ja-jp/windowsintunetrust/

サービス実施中にプライバシーを保護する方法

マイクロソフトのクラウド サービスがサービス実施中にデータのプライバシーを保護するためによく使用する、一連の方法が存在します。

1 つ目の方法は、データ アクセスの制御です。データ アクセスの制御は、物理と論理の 2 つのカテゴリに分類されます。物理カテゴリにおいては、データセンター機能へのアクセスは、外側と内側の境界を作り、各レベルでセキュリティを強化することによって保護します。境界の囲い、警備員、サーバー ラックの施錠、多要素アクセス制御、統合警報システム、24 時間 365 日体制でのオペレーション センターからの広範囲にわたるビデオ監視などがあります。

顧客データへのアクセスは、業務のニーズに基づいて制限されます。アクセスの制限は、役割ベースのアクセス制御、2 要素による認証、実稼働データへの無期限アクセスの最小化、実稼働サービス環境で実施される作業のログ記録や監査などに基づいて行われます。

マイクロソフトはプライバシーおよびセキュリティ関連の脅威に対する定期的な実稼働環境の監視を行います。データセンター内の潜在的なプライバシーのリスクを報告する堅牢な内部プログラムを使用しています。プロセスが始動すると、プライバシー、科学捜査、法律、コミュニケーションの専門家とエンジニアが集まってチームとなり、プライバシーのインシデントを迅速に解決するための一連の適切なアクションを決定します。

データを同じクラウド サービスに保存しているお客様間のデータ プライバシーを確保するために、マイクロソフトはデータの分離テクニックを使用してクラウド テナントを論理的に分離し、お客様が自らのデータだけにアクセスできる環境を構築します。

データの地理的な場所は、規制の厳しい業界や、データ保護に関する法律がある国で業務を行うお客様にとって重要な要素です。一部のお客様が、EU や APEC 内など、特定の地理的な場所でデータを管理する必要があることを、マイクロソフトは理解しています。マイクロソフトの Global Foundation Services (GFS) チームは、クラウド規模のデータセンターの世界中のネットワークを管理し、各データセンターが厳しいセキュリティ要件を満たしていることを確認します。

マイクロソフトの各クラウド サービスには、顧客データの地理的な場所に関する独自のポリシーがあります。ポリシーは各サービスのセキュリティ センターで公開されており、お客様はサービスを申し込む前に、データが保管される地域を確認することができます。詳細については、関心をお持ちのサービスのセキュリティ センターを参照してください。

上の図は、マイクロソフトがエンタープライズ クラウド サービス向けのデータセンターを運用している地域を示したものです。Office 365 や Windows Azure を含む多くのサービスで、お客様はデータの保存場所を選択することができます。

マイクロソフトはサービスに関連するすべてのシステムを継続的に監視します。これは、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視することで、潜在的な脅威を特定するためです。この監視により、規格団体に要求されるプライバシーの有効性レポートのデータも提供されます。

データ プライバシー基準への準拠

Windows Azure、Office 365、Windows Intune、および Dynamics CRM Online は、国際的なデータ プライバシー基準に準拠するだけでなく、お客様もこのような基準に準拠できるようにサポートします。このような基準には、次のようなものがあります。

HIPAA および HITECH: Health Insurance Portability and Accountability Act (HIPAA、医療保険の相互運用性と説明責任に関する法律) および Health Information Technology for Economic and Clinical Health Act (HITECH、経済的及び臨床的健全性のための医療情報技術に関する法律) は、保護医療情報 (PHI) にアクセスする特定の医療機関に適用される米国の法律です。マイクロソフトは、お客様がこれらの法律に従うためのプラットフォームに加え、法律を順守する義務を文書化した Business Associate Agreement (BAA、業務提携契約) を提供します。Office 365、Windows Azure、Windows Intune、Dynamics CRM Online はすべて、サービスに関する契約の一部として BAA を提供します。詳細については、関心をお持ちのサービスのセキュリティ センターを参照してください。

EU 模範条項 :「Article 29 Working Party (第 29 条作業部会)」を通して活動する欧州連合の 28 のデータ保護機関は、マイクロソフトがクラウドの企業顧客に提供する契約上のプライバシー保護が、国家間でのデータ転送に適用される現行の EU 基準を満たしていると判断しています。マイクロソフトは、この種の承認を受けた最初の、唯一のクラウド プロバイダーです。実際、欧州のプライバシー規制当局は「マイクロソフトのエンタープライズ クラウドが、データの保存場所にかかわらず、欧州の厳しいプライバシー基準に準拠している」と評しました。この評価はマイクロソフトのエンタープライズ クラウド サービス (特 に Microsoft Azure、Office 365、Microsoft Dynamics CRM、Windows Intune) が対象となっています。模範条項の背景と、それらに対するマイクロソフトの対応については、「現状、クラウドのお客様が模範条項を無視できない理由」(英語情報) を参照してください。また、どのようにしてこれらの模範条項に従っているかを確認するには、関心をお持ちのマイクロソフト クラウド サービスのセキュリティ センターを参照してください。

ISO 27001: Office 365、Windows Azure、Windows Intune、Dynamics CRM Online を含むマイクロソフトのエンタープライズ サービスは ISO/IEC 27001 の認証を受けており、認証の証拠は監査機関から入手できます。各サービスの ISO 認証へのリンクは、それぞれのセキュリティ センターを参照してください。

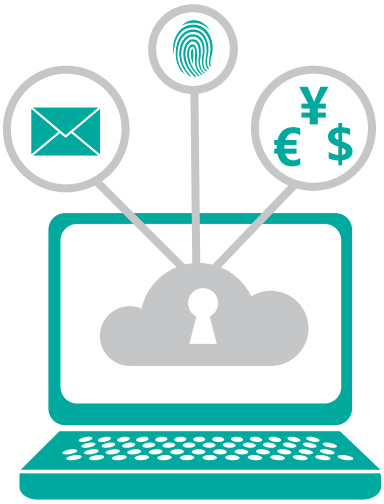
SOC1 および SOC2: Windows Azure、Office 365、Windows Intune、Dynamics CRM Online ではそれぞれ、SOC 1 Type 2 の要件に応じた AICPA の SSAE16 Service Organization Control (SOC) レポート フレームワークに従ってサービスを保護する管理機能が有効に運用されていることが証明されています。SOC1 Type 2 は、サービス プロバイダーによって実装されている管理機能の設計と運用上の有効性を証明します。さらに、Windows Azure およびマイクロソフトのデータセンターには、SOC 2 Type 2 監査に必要な管理機能が実装されていることが証明されました。この監査には、セキュリティ、可用性、機密性に関する管理機能に特化したサービスの調査が含まれています。このホワイトペーパーの執筆時点では、Office 365 と Dynamics CRM Online は SOC2 レポートの準備中でした。これらのレポートの詳細については、各サービスのセキュリティ センターを参照してください。

CSA STAR Registry: Windows Azure、Office 365、Dynamics CRM Online はそれぞれ、Cloud Security Alliance (CSA) STAR Registry プログラムに参加しています。これは、参加しているクラウド サービスの準拠姿勢をお客様が比較できるものです。このプログラムに参加するために、マイクロソフトは CSA Cloud Controls Matrix (CCM) に従って管理機能の動作をまとめました。CCM とは、クラウド ベンダーの指針となる基本的なセキュリティ原則の概要を示したもので、サービスを検討中のお客様がクラウド プロバイダーの全般的なセキュリティ リスクを評価するのに役立ちます。CCM に従って管理機能の動作を公開することにより、マイクロソフトがお客様のプライバシーとデータを保護していることを確信していただけます。マイクロソフトのサービスが CCM で定義されたセキュリティ、プライバシー、コンプライアンス、リスク管理の要件を満たしていることを詳しく説明したホワイトペーパーは、CSA の Security Trust and Assurance Registry (STAR) で公開されています。

透明性

法執行機関またはその他の政府機関からの顧客データの要求に関しては、マイクロソフトは顧客データを保護する義務を果たします。マイクロソフトがデータを提供するのは、特定のデータ セットに対して法に基づく要求があった場合だけです。Windows Azure や Office 365 といったエンタープライズ サービスについては、お客様の情報がオンプレミス、クラウド サービスのどちらに保存されている場合でも、お客様自身がその情報を管理するべきである、とマイクロソフトは考えています。そのため、お客様からの指示があった場合や、法律で義務付けられている場合を除き、顧客データをサードパーティ (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。サードパーティがマイクロソフトに対して顧客データを要求した場合は、お客様から直接要求するようにサードパーティに回答します。やむを得ず顧客データをサードパーティに開示するときは、法律で禁じられている場合を除き、すぐにお客様に通知し、要求のあったデータのコピーを提供します。また、マイクロソフトは要求の対象に関する情報を示す Law Enforcement Requests Report (法執行機関要求レポート) や、国家安全保障の要求に対するマイクロソフトの対応 (マイクロソフトの法律顧問からの情報) を公開しています。詳細については、TechNet サイトのブログ記事「Responding to government legal demands for customer data」(顧客データに対する政府機関からの法に基づく要求への対応) を参照してください。

さらに、ホワイトペーパー「クラウドの透明性に対するマイクロソフトのアプローチ」では、さまざまなリスクに対するマイクロソフトの対処方法、ガバナンス、CSA CCM を含む情報セキュリティの枠組みおよび標準の概要が提供されています。



お客様のデータ保護のサポート

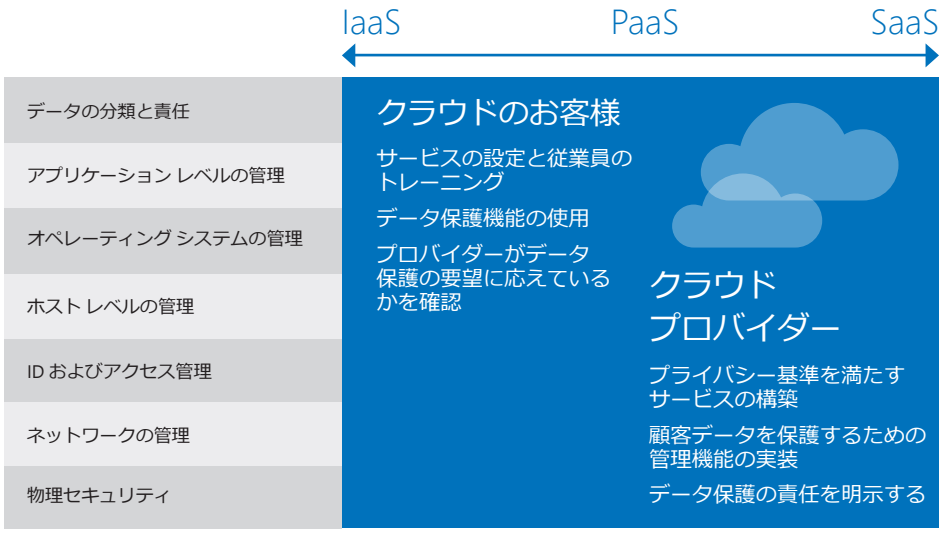
顧客データのプライバシー保護のためにマイクロソフトが集中的に取り組んでいる 3 つの領域の最後は、お客様や将来のお客様に十分な情報を提供し、お客様が情報に基づいた判断を下せるようにすることです。この情報には、マイクロソフトがどのようにして顧客データを保護するかだけでなく、プライバシーに関してマイクロソフトが負う責任や、データの安全性を確保するためにお客様が負う責任のレベルも含まれています。

データ保護の責任の範囲

マイクロソフトは顧客データのプライバシーの保護と維持に対する責任について真剣に取り組んでいます。お客様が保護された状態でマイクロソフトのサービスを実装、使用できるように、力強くサポートしていきます。データ保護とプライバシーは、プロバイダーおよびそのお客様の間で共有される責任です。プロバイダーはプラットフォームに対する責任を負います。また、顧客のセキュリティ、プライバシー、コンプライアンスに対するニーズを満たせるサービスを作成するという責任を果たす必要があります。

お客様はサービスがプロビジョニングされた後にそのサービスを設定して運用する責任を負います。この作業には、アクセス資格情報管理、規制と法令のコンプライアンス管理、サービスの設定可能な管理機能によるアプリケーションの保護、データ コンテンツの保護、自分のアカウントで使用する仮想マシンやその他のデータの保護が含まれます。

次の図は、クラウド プロバイダーの責任と顧客企業の責任を分類したものです。これらの責任の境界は必ずしも明確ではなく、お客様とその他の代理人によって署名された契約に基づいて決まります。マイクロソフトでは、このような役割と責任について、できるだけ透明性を高めたいと考えています。マイクロソフトは、契約上の義務を明確にし、本書のようなホワイトペーパーを発行して、クラウド サービスのセキュリティ センターにサービス固有の考慮事項を詳しく記載します。



プロバイダーは、該当するデータ保護およびプライバシーの規制と標準への準拠を容易にするサービスと機能を構築する責任を負います。ただし、業界や地域のコンプライアンス要件を維持しながらサービスが使用されるようにサービスを設定し、従業員をトレーニングするのはお客様の責任です。また、強力な運用管理を構築してクラウドの顧客データを保護するのはプロバイダーの責任ですが、意図しないデータ共有やデータアクセスを制限しながらこの管理を使用するのはお客様の責任です。最後に、認証を取得し、証明レポートを共有し、契約に署名することによってデータ保護の責任を明示するのは、プロバイダーの責任です。ただし、プロバイダーの監査レポート、証明、およびその他の証拠が組織のデータ保護に対する期待に応えるものかどうかを確認するのは、クラウドを使用するお客様の責任です。

マイクロソフトは、すべての顧客データがそのお客様の所有物であると断言します。

データ ポータビリティ

多くのマイクロソフトのサービスでは、お客様はマイクロソフトやパートナーのサポートを利用せずに、ご自分のデータのコピーをダウンロードすることができます。

たとえば、Office 365 では Exchange Online にインポート ウィザードとエクスポート ウィザードが提供されており、エンド ユーザーは電子メール、カレンダーの予定、連絡先、タスクをいつでもローカル コンピューターにダウンロードすることができます。さらに、このサービスは Windows PowerShell の「コマンドレッド」(マイクロソフトの PowerShell と互換性のあるサービスの管理に使用されるスクリプト可能コマンド) を提供しており、管理者は必要に応じてエンドユーザーのメタデータをダウンロードすることができます。最後に、お客様がマイクロソフトのエンタープライズ クラウド サービスの契約を終了する場合、マイクロソフトはアカウントの機能に制限を付けたうえで最低 90 日間データを保持するので、その間お客様はデータを取り出すことができます。その後、データは削除されます。これにより、お客様は業務のニーズに応じて、時間をかけてデータを他のサービスへ移行することができます。また、顧客データは指定された期間内に削除されるので、お客様のデータ プライバシーは維持されます。

その他のマイクロソフトのクラウド サービスにも、データ ポータビリティ、データ保有、データ削除に関する類似したポリシーが存在します。特定のサービスのポリシーの詳細については、該当するセキュリティ センターを参照してください。

パートナー ソリューション

マイクロソフトは幅広いパートナー ネットワークと連携して、製品とサービスを強化および拡張します。これはすべてのクラウド サービス製品が該当します。パートナーの資格を得るには、組織は特定の技術的能力を備えている必要があります。また、マイクロソフトのクラウド サービスの業務に携わる従業員が特定のマイクロソフトの認定試験に合格していることを文書で示さなければなりません。このような組織は、マイクロソフトのサービスの新しい機能を作成したり、既存の機能を拡張したりすることができます。

お客様にガイダンスと透明性を提供することにより、お客様はデータ プライバシーの処理方法について、情報に基づいた判断を下すことができます。

各サービスには、独自のパートナー プログラムと認定の要件があります。詳細については、関心をお持ちのサービスのホーム ページを参照してください。

データ保護とプライバシーのため、マイクロソフトには ID およびアクセスに関連した業務を受け持つパートナーが存在します。このパートナーは、お客様がクラウド ソリューションの情報にアクセスし、その情報を保護するのに役立つソリューションを提供します。また、パートナーはシングル サインオン (SSO)、フェデレーション ID、認証、データ保護のための機能も提供します。

お客様を力強くサポートするためのリソース

データ保護やプライバシーに関してお客様が情報に基づいた判断を下すためのもう 1 つの措置として、マイクロソフトは自らのポリシーとコミュニケーションの透明性をできる限り高めようとしています。これを実現するため、マイクロソフトはサービスに次の機能を求めています。

- **セキュリティ センターまたはプライバシーに関する声明をオンラインで提供する。** Office 365、Dynamics CRM Online、Windows Intune、および Windows Azure にはそれぞれ専用のセキュリティ センターが存在します。その他のマイクロソフトのクラウド サービスについては、専用のプライバシーに関する声明がオンラインで公開されています。

- **お客様のデータ プライバシーに影響を与えるサービスの機能を文書化する。** マイクロソフトのエンタープライズ クラウド サービスでは、データ プライバシーに影響を与える可能性のある機能について記載したドキュメントを提供します。たとえば、Office 365 には、管理者のための高度なプライバシー オプションについて説明した、小規模企業のお客様向けの情報ページがあります。中規模企業やエンタープライズ規模の企業、教育機関や政府機関の管理者向けの同様のページもあります。

- **Law Enforcement Requests Report (法執行機関要求レポート) へのアクセスをお客様に提供する。** 世界中の法執行機関によるマイクロソフトへの要求をまとめたレポートを、誰でも確認することができます。このレポートには、マイクロソフトが受けた要求の数に関するデータ、マイクロソフトのエンタープライズ クラウド サービスと特に関連性の高い要求の数、マイクロソフトが許諾した要求と拒否した要求の数の詳細が掲載されています。さらに昨年、マイクロソフトは米国の司法長官に対し、国家安全保障に基づく顧客情報の要求に対するマイクロソフトの対応を、さらに詳しく公開することを認めるように要請しました。詳細については、TechNet サイトのブログ記事「Respondingtogovernmentlegaldemandsforcustomerdata」(顧客データに対する政府機関からの法に基づく要求への対応) を参照してください。Law Enforcement Requests Report (法執行機関要求レポート) では、これらを頻繁に要求する国、マイクロソフトが拒否した数、要求されたデータを提供した数を確認することができます。

- **サービス固有のプライバシーに関するホワイトペーパーと、Cloud Security Alliance (CSA) STAR のドキュメントを投稿する。** マイクロソフトは、データ保護に関するマイクロソフトの幅広いアプローチと、各サービスのプライバシーに関する考慮事項への対応をまとめたプライバシーのホワイトペーパーを投稿することを、各サービスに求めています。多くのサービスのセキュリティ センターには、サービスがどのように CSA STAR の要件に準拠しているかを文書化した、CSA によって管理されているドキュメントへのリンクが提供されています。

プライバシーに関する考慮事項を踏まえてクラウド サービスを最初から構築し、クラウド サービス内にコンプライアンス メカニズムを用意することにより、お客様のデータ保護を優先するというマイクロソフトの責任を果たしています。

結論

クラウド コンピューティングは、組織や個人の選択肢の幅を広げ、柔軟性を高めて、コストを削減します。しかし、このようなメリットを実現するには、クラウドのお客様はデータのプライバシーとセキュリティに関する確かな保証をクラウド プロバイダーから得る必要があります。世界の規制当局と立法者は、プロバイダーとお客様の両方がデータ プライバシーの要件を定義するのに役立つ標準と指標を提供することで、クラウド コンピューティングの可能性を引き出す手助けをしています。

セキュリティと顧客データのプライバシーは、20 年以上前にマイクロソフトがクラウド サービスの提供を開始してから取り組んでいる、最も重要な課題です。それ以来、マイクロソフトは経験に基づいて、企業のプライバシー ポリシー、製品とサービスの開発ガイドライン、およびビジネス プラクティスを構築してきました。現在では、これらすべてを新しいクラウド サービスに適用しています。

マイクロソフトは、オンライン サービスのプライバシーおよびセキュリティに関する最も高い基準の維持に力を注ぎます。そして、お客様と協力してデータ プライバシーと保護プラクティスを向上させ、マイクロソフトのコンピューティング サービスに対するお客様の信頼を基に前進したいと考えています。

関連資料

ホワイトペーパーとブログ記事

- マイクロソフト クラウド インフラストラクチャの情報セキュリティ管理システム
  http://www.microsoft.com/ja-jp/download/details.aspx?id=11708
- ソフトウェア製品およびサービスの開発におけるプライバシー ガイドライン
  http://www.microsoft.com/ja-jp/download/details.aspx?id=16048
- クラウドの透明性に対するマイクロソフトのアプローチ
  http://www.microsoft.com/ja-jp/download/details.aspx?id=30157
- Windows Intune のプライバシー プラクティス (英語情報)
  http://download.microsoft.com/download/C/C/8/CC8065C4-829F-4635-B731-1D39287444C0/Windows_Intune_Privacy_and_Data_Protection_Overview.pdf
- 顧客データに対する法に基づく政府機関からの要求への対応 (英語情報)
  http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/16/responding-to-government-legal-demands-for-customer-data.aspx

Web サイト

- Microsoft Trustworthy Computing (信頼できるコンピューティング) (英語情報)
  http://www.microsoft.com/en-us/twc/default.aspx
- クラウド セキュリティ アライアンスの Security Trust and Assurance Registry (STAR) (英語情報)
  https://cloudsecurityalliance.org/star/

マイクロソフトのクラウド サービス セキュリティ センター

- Microsoft Dynamics CRM セキュリティ センター
  http://www.microsoft.com/ja-jp/dynamics/crm-trust-center.aspx
- Office 365 セキュリティ センター
  http://office.microsoft.com/ja-jp/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx
- Microsoft Azure セキュリティ センター
  http://azure.microsoft.com/ja-jp/support/trust-center/
- Windows Intune セキュリティ センター
  http://www.microsoft.com/ja-jp/windowsintunetrust/

次の世代の信頼できるコンピューティング