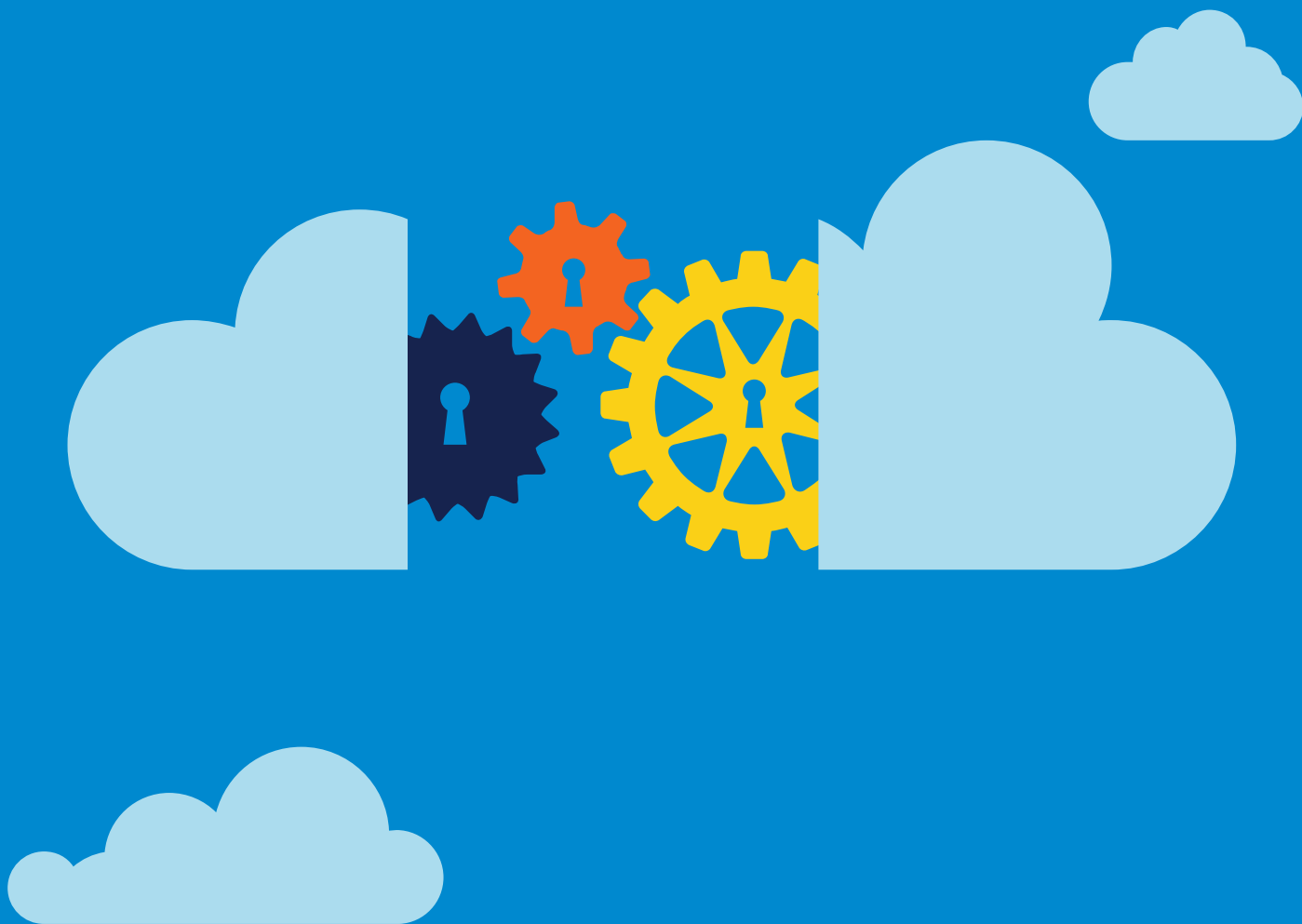


信頼できるクラウド: Microsoft Azure の セキュリティ、プライバシー、 コンプライアンス

2015年4月





目次

概要	4
お客様はクラウド プロバイダーに何を求めているか	5
Microsoft Azure: 信頼に応える設計	6
セキュリティ: 顧客データ保護の取り組み	7
セキュリティの設計と運用	7
インフラストラクチャの保護	9
ネットワークの保護	10
データの保護	11
ID とアクセスの管理	12
プライバシー: データの所有権と管理権はお客様に	12
お客様自身がデータを管理	14
透明性	15
コンプライアンス: Azure は国際標準に準拠	16
関連情報	19



概要

クラウド コンピューティングの登場に伴い、今日の IT 部門は、ビジネス戦略の推進においてますます重要な役割を果たすようになってきました。コスト削減が最優先課題であることに変わりはありませんが、スケーラビリティとビジネス アジリティもまた、IT 意思決定者の注目を集めています。その結果、クラウド ソリューションへの支出は 2013 年から 2018 年にかけて 30% の成長が予想され、エンタープライズ IT 全体では 5% の成長が見込まれています。その動きに足並みを揃えているのがクラウド サービスです¹。アナリストは、今後 4、5 年の間にクラウド ベース ソリューションの市場規模は 10 倍に拡大する、と予想しています。



出典

- 1 Forbes、「Roundup of Cloud Computing Forecasts and Market Estimates, 2015」(2015 年 1 月 24 日)
<http://aka.ms/forbes-cloud-2015> (英語)
- 2 Intel/McAfee、「Net Losses: Estimating the Global Cost of Cybercrime」(2014 年 6 月)、
<http://aka.ms/mcafee-cybercrime-report> (英語)
- 3 英国ビジネス・イノベーション・職業技能省、「2014 Information Security Breaches Survey」、
http://aka.ms/uk-gov_breach-survey (英語)
- 4 PWC、「Global State of Information Security Survey: 2015」、<http://aka.ms/pwc-cybercrime> (英語)
- 5 Gemalto、「2014 Breach Level Index Report」
- 6 McKinsey & Company、世界経済フォーラム レポート (2014 年 1 月)

依然として多くの CIO が、クラウド ファーストの戦略を全面的に推進することに躊躇しています。その理由の 1 つは、プライバシーとセキュリティに関連するさまざまな問題への不安です。2014 年を通じて大規模なデータ漏えい事件がニュースを賑わせ、現在も報道され続けています。IT 部門の責任者はいたるところで重大な課題に直面し、「データを保護し、企業全体のプライバシーとコンプライアンスを確保しながら、スケーラブルなクラウド ソリューションを構築してビジネス アジリティを改善することは可能なのだろうか?」と頭を悩ませています。

この課題への明確な解決策が見つからなければ、セキュリティ上の懸念がイノベーションの足手まといとなり、ビジネスの拡大を妨げるおそれがあります。IT とビジネスの責任者には、イノベーションとセキュリティ間のギャップの架け橋となる信頼できるパートナーが必要です。最適なテクノロジーとプロセスを採用すれば、きわめて複雑な要件を抱える企業でも、安心してクラウドに移行することができます。

「戦略的な購入担当者の
71% が、クラウド
サービス導入の
決め手となった
重要な要素として、
スケーラビリティ、
コスト、ビジネス
アジリティを
挙げています。」

Gigaom Research

お客様はクラウド プロバイダーに何を求めているか

ビジネスにはそれぞれ異なるニーズがあり、クラウド ソリューションから得られるメリットもビジネスごとに異なります。しかし、あらゆる業種のお客様が一様に、クラウドへの移行に関して同じ懸念を抱えています。お客様はクラウドに移行したとしても、引き続きデータを自ら管理し、安全性と機密性を保持し、透明性とコンプライアンスを維持したいと望んでいるのです。

データの保護: 侵入による被害の規模と範囲はますます拡大しています。2014 年には、サイバー犯罪により 1,500 件を超えるデータ漏えいが発生し、10 億件を超えるデータレコードが危険にさらされました⁷。McKinsey & Company による 2014 年の世界経済フォーラム レポート⁸ によると、サイバー攻撃のリスクが「テクノロジーとビジネスのイノベーションを著しく遅らせ、その影響は総額 3 兆ドル規模になる」と推定しています。あらゆるセキュリティ攻撃を前にしては、標的となった組織の安全性は最も脆弱なリンクと同程度でしかありません。セキュリティ保護されていないコンポーネントがあれば、システム全体が危険にさらされます。クラウドによってデータのセキュリティと管理コントロールが強化されることを理解してはいても、IT 責任者は、クラウドへ移行することで、既存の自社ソリューションに比べてハッカー攻撃に対して脆弱になるのではないかと懸念しています。

データの機密性の維持: クラウド サービスには、プライバシーの保護という特有の課題があります。クラウドに関心を寄せる企業は、インフラストラクチャ コストの節約と柔軟性の向上を望む一方で、データの保管場所やデータへのアクセス、データの使われ方を制御できなくなることをおそれています。2013 年の米国政府による大規模な情報収集問題の発覚以降プライバシーに対する懸念は強まり、クラウドに注がれる視線はいっそう厳しくなっています。

企業によるコントロール: 革新的なソリューションをデプロイするためにクラウドを利用するとしても、企業はデータに対するコントロールを失うことに強い懸念を抱えています。近年、法的手段と超法規的手段を用いた政府機関による個人情報へのアクセスが明るみに出たことで、CIO の一部はクラウドへのデータの保管に警戒心を強めています。こうしたことから、多くの企業はクラウドでのデータの保管場所を自ら選択し、自社のデータにアクセスできるスタッフを自ら管理することを求めています。

透明性の促進: ビジネスの意思決定者にとってセキュリティ、プライバシー、コントロールが重要なのはもちろんですが、データの保管、アクセス、保護の方法について独自に検証することも重要です。企業は、見えないものはコントロールできないことを知っています。お客様に対してこの種の可視性を提供するには、クラウド プロバイダーは、セキュリティ、プライバシー、コンプライアンスに対する取り組みと対策に関する透明性を保障し、お客様自身の意思決定に必要な情報を明らかにする必要があります。

⁷ Gemalto, 「2014 Breach Level Index Report」

⁸ McKinsey & Company, 世界経済フォーラム レポート (2014 年 1 月)



コンプライアンスの維持: 企業や政府機関がクラウド テクノロジーの利用を拡大するにつれ、標準や規制の複雑さと範囲も変化し続けています。企業は、自社のコンプライアンス標準が今後も満たされること、そして時と共に変化する各種規制に合わせて自社のコンプライアンスもまた進化するということを知っておく必要があります。

Microsoft Azure: 信頼に応える設計

Microsoft Azure は、企業と政府機関の幅広いお客様に対応したクラウド サービスを提供しています。その中核を成すのは、仮想環境やアプリケーション、関連する構成をお客様が構築、管理するための 4 つの主要機能です。

Microsoft Azure

今日の企業向けの統合プラットフォーム



グローバルに展開された
物理インフラストラクチャ
サーバー/ネットワーク/データセンター

- 10 兆を超えるオブジェクトを格納
- 1 秒あたり平均 12.7 万件の要求を処理
- ピーク時には 1 秒あたり 88 万件の要求を処理



マイクロソフトは独自のエクスペリエンスと規模で、これらのサービスを世界の多くの主要企業と政府機関に提供しています。現在マイクロソフトのクラウド インフラストラクチャでは、企業向けおよびコンシューマー向けサービスを通じて、140 か国の 10 億以上のお客様をサポートし、10 の言語、24 種類の通貨に対応しています。この規模と実績を活かし、マイクロソフトはセキュリティ機能を強化したソフトウェアの開発、運用管理、脅威への対策を行い、お客様単独では達成しえない高水準のセキュリティ、プライバシー、コンプライアンスを備えたサービスを提供しています。

マイクロソフトは、ベスト プラクティスを政府や企業と共有し、デジタル犯罪対策部門、サイバー犯罪対策センター、マルウェア プロテクション センターなどの開設を通じて、幅広いセキュリティ対策に取り組んでいます。

セキュリティ: 顧客データ保護の取り組み

Azure は、コスト削減、複雑さの解消、クラウド内のセキュリティやコンプライアンス上のリスク低減に効果を発揮します。マイクロソフトが出資し ComScore⁹ が実施した調査によれば、導入前の多くの企業がクラウドへの移行に懸念を抱いているものの、クラウドを導入した企業の大多数はセキュリティ面で多くのメリットがあったと報告しています。このようにセキュリティ面でのメリットが報告された背景として、一部の企業ではマイクロソフトの使用するテクノロジーや運用プロセスをレプリケートして、自社のクラウド サービスの保護や幅広い種類の国際標準の遵守に活用できていることが挙げられます。Azure を使用することで、企業は、規制に準拠したオンライン サービスを世界中で運用しているマイクロソフトの比類ない規模や経験からメリットを得ることができます。マイクロソフトの専門知識をお客様自身の知識として活用することができるのです。

導入前の懸念

60%

導入の障壁として、データセキュリティに対する懸念を挙げている企業

45%

クラウド導入によってデータを制御できなくなることを懸念している企業

得られたメリット

94%

これまでの自社運用にはなかったセキュリティ上のメリットを実感している企業

62%

クラウドへの移行によってプライバシー保護が強化されたと感じている企業

マイクロソフトのクラウド サービス

200 以上のクラウド サービス



100 万を超えるサーバー



150 億ドルを超えるインフラストラクチャへの投資



10 億の顧客



2,000 万の企業



世界 140 各国



セキュリティの設計と運用

安全なクラウド ソリューションの実現は、総合的な計画策定、革新的な設計、そして、効率的な運用手段があってこそです。マイクロソフトは、コードの開発からインシデント対応までのあらゆる段階でセキュリティを重視しています。

セキュリティを基盤とした設計: Azure の開発は、マイクロソフトのセキュリティ開発ライフサイクル (SDL) に準拠しています。SDL は、開発者がよりセキュリティの強化されたソフトウェアを開発し、セキュリティのコンプライアンス要件へ対応できるように支援するソフトウェア開発プロセスです。このプロセスは 10 年前からマイクロソフトの開発手法の中核的要素となっており、業界およびお客様に無償で公開されています。SDL では、計画、設計、開発、デプロイメントというフェーズを通じて、セキュリティ要件をシステムおよびソフトウェアに組み込みます。

⁹ <http://aka.ms/twc-cloud-trust-study> (英語)

運用上のセキュリティの強化: Azure は、運用とサポートに関する厳格なセキュリティ対策基準を遵守しています。不正な開発行為や管理行為を阻止するために、以下のメカニズムを含む、予防的、防衛的、かつ即応性の高いコントロールを複合的に配置しています。

- 機密データを扱う処理を実行する際にスマートカード ベースの 2 要素認証を要求するなど、機密データに対する堅固なアクセス制御
- 不正行為の自発的な検出を強化するコントロールの組み合わせ
- 複数レベルの監視、ログ記録、レポート作成

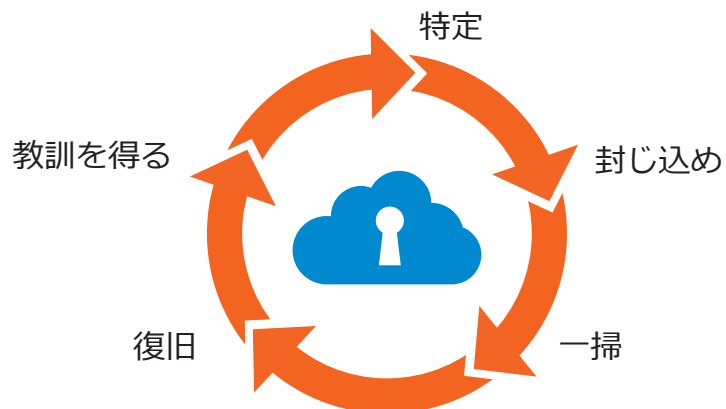
さらに、特定の運用担当者に関する経歴確認を実施し、確認基準に応じて、アプリケーション、システム、ネットワーク インフラストラクチャへのアクセスを制限しています。

侵害を想定した対策: クラウド サービスの安全性をより強化するためにマイクロソフトが採用している重要な運用上のベスト プラクティスの 1 つが、「侵害想定」戦略と呼ばれるものです。ソフトウェア セキュリティの専門家で作成される「レッド チーム」がネットワーク、プラットフォーム、アプリケーションの各レイヤーを実際に攻撃し、セキュリティ侵害に対する Azure の検知、防御、復旧能力を検証しています。サービスのセキュリティ機能を頻繁にチェックすることで、マイクロソフトは新たな脅威に対して先手を打つことができます。

インシデント管理と対応: マイクロソフトは、攻撃や悪意のある活動の影響抑制を任務とする、24 時間 365 日体制のグローバルなインシデント対応サービスを提供しています。インシデント対応チームは、確立されたインシデントの管理、連絡、復旧の手順に従って行動し、社内スタッフも外部パートナーも一様に見つけやすく予測可能なインターフェイスを使用します。セキュリティインシデントが発生した場合、セキュリティ チームは以下の 5 つのステップに従って対応します。

「当校には 24 時間
365 日体制で
セキュリティ上の
脅威に対応するため
の人的リソースは
ありませんが、
マイクロソフトには
あります。」

Bo Wandschneider 氏
CIO 兼副学長
クイーン大学 (カナダ)






- **特定:** セキュリティ上の問題を示唆するインシデントが発生した場合、深刻度が割り当てられ、マイクロソフト内で適宜エスカレーションされます。
- **封じ込め:** エスカレーション チームの最優先事項として、インシデントを確実に封じ込め、データの安全を確保します。
- **一掃:** 事態の収拾後、エスカレーション チームはそのセキュリティ インシデントに起因するすべての損害の一掃に取り組み、セキュリティ インシデントの根本原因を特定します。
- **復旧:** ソフトウェアまたは構成の更新をシステムに適用し、サービスを復旧して全面的に稼働させます。
- **教訓を得る:** 各セキュリティ インシデントは分析され、今後の再発を防ぐために適切な対策が講じられます。

インフラストラクチャの保護

Azure のインフラストラクチャには、ハードウェア、ソフトウェア、ネットワーク、管理と運用の担当スタッフ、およびそれらすべてを収容する物理データセンターが含まれます。Azure は、インフラストラクチャ全体のセキュリティ リスクに対応します。

物理セキュリティ: Azure は地理的に分散されたマイクロソフトの施設で運用され、施設のスペースや設備は他の Microsoft Online Services と共有されています。各施設は 24 時間 365 日体制で運用できるように設計されており、停電や物理的な侵入、ネットワーク障害から運用を保護するためにさまざまな手段が講じられています。これらのデータセンターは、物理的なセキュリティと可用性の維持を定めた ISO 27001 などの業界標準に準拠し、マイクロソフトの運用担当者が管理、監視しています。

監視、ログ記録: Azure 環境内のデバイスによって生成される大量の情報は、監視、相関関係の特定、分析を行う中央システムによって管理されます。サービス管理チームが継続的に状況を把握し、アラートに適宜対応します。追加の監視、ログ記録、レポート機能によって情報が可視化され、お客様に提供されます。

境界 	建物 	コンピューター ルーム 
<ul style="list-style-type: none">• 24 時間常駐の警備員• 施設のセットバック規定• 柵• フェンス	<ul style="list-style-type: none">• 警報機• セキュリティ オペレーションセンター• 耐震補強ブレース• 監視カメラ	<ul style="list-style-type: none">• 2 要素アクセス制御: 生体認証、カード リーダー• カメラ• 数日分のバックアップ電力

更新プログラム管理: セキュリティ更新プログラムの管理により、既知の脆弱性からシステムを保護します。Azure では、マイクロソフト ソフトウェアのセキュリティ更新プログラムの配布とインストールの管理に統合デプロイメント システムを使用します。マイクロソフトおよびサードパーティのスキャン ツールを併用し、Azure 環境内の OS、Web アプリケーション、データベースをスキャンします。

ウイルス対策、マルウェア対策: Azure のソフトウェア コンポーネントをデプロイする際は、事前にウイルス スキャンで確認することを必須としています。「感染なし、正常に完了」というウイルス スキャン結果が得られなければ、コードは運用環境には移行されません。さらに、Azure VM にはネイティブのマルウェア対策機能を提供しています。マイクロソフトは、お客様にすべての仮想マシン (VM) に対してマルウェア対策およびウイルス対策を実施されることをお勧めします。お客様は Cloud Services および Virtual Machines 用の Microsoft Antimalware またはその他のウイルス対策ソリューションを VM にインストールできます。また、VM を定期的に再イメージ化して、侵入が検知されなかった脅威を一掃することができます。

侵入テスト: マイクロソフトは、Azure のセキュリティ対策やプロセスを改善するために、侵入テストを定期的に実施しています。セキュリティ評価もまた、お客様のアプリケーション開発とデプロイメントの重要な要素です。このため、マイクロソフトはお客様向けのポリシーを定め、お客様自らが、Azure にホストしている自社アプリケーションに対して承認を得た侵入テストを実施できるようにしています。

DDoS 対策: Azure は、Azure プラットフォーム サービスへの分散型サービス拒否 (DDoS) 攻撃に対する防御システムを備えています。このシステムでは、標準的な検出技術および回避技術を使用しています。Azure の DDoS 防御システムは、プラットフォームの外部と内部どちらからの攻撃にも耐えうる設計です。

ネットワークの保護

Azure のネットワークは、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 Azure の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。Azure の共有インフラストラクチャでは何億台ものアクティブな VM をホストしているため、ネットワークトラフィックのセキュリティと機密性を保護することはきわめて重要です。

従来のデータセンター モデルでは、ネットワーク設備への物理的なアクセスを含め、ネットワークシステムの管理は企業の IT 部門が担当します。クラウド サービス モデルでは、ネットワークの保護と管理の責任は、クラウド プロバイダーとお客様の双方が負担します。お客様は物理的にアクセスすることはできませんが、ゲスト オペレーティング システム (OS) ファイアウォール、Virtual Network Gateway 構成、仮想プライベート ネットワークなどのツールを通じて、論理的にクラウド環境内にアクセスできます。

ネットワークの分離: 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や VM は同一の物理ハードウェア上に保管されています。Azure では、論理的分離によりお客様のデータを他のお客様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と経済面でのメリットが生まれると共に、他のお客様のデータへのアクセスが厳格に阻止されます。

仮想ネットワーク: お客様は、仮想ネットワークのサブスクリプション 1 つに複数のデプロイメントを割り当て、これらのデプロイメント間をプライベート IP アドレスで通信させることができます。仮想ネットワークは他の仮想ネットワークから分離されています。

VPN、ExpressRoute: Site-to-Site VPN または Point-to-Site VPN を使用して、お客様のサイトとリモートワーカーから Azure Virtual Network への接続が可能です。パフォーマンスをさらに向上させる場合は、オプションの ExpressRoute プライベート ファイバー リンクを使用して 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出するのを防ぐことができます。

通信の暗号化: ビルトインの暗号化テクノロジーにより、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、Azure リージョン間の通信、Azure からオンプレミス データセンターへの通信を暗号化することができます。

「クラウドの導入に踏み切れない理由がセキュリティ上の懸念であったとしたら、ためらうことはもうありません。」

FORRESTER

データの保護

Azure では暗号化、隔離、破壊という 3 つの手法によって、データの暗号化とキー管理を行い、アプリケーション、プラットフォーム、システム、ストレージの顧客データを保護します。

データの分離: 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や仮想マシンは同一の物理ハードウェア上に保管されています。

保存されたデータの保護: 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。Azure Key Vault では、クラウドのアプリケーションやサービスがデータを暗号化する際に使用されるキーの管理を合理化し、簡単かつコスト効率よくキーを保持できるよう支援します。

通信中のデータの保護: お客様は、使用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。Azure では、2 つの仮想ネットワーク間を移動するデータなど、通信中のデータを保護します。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は、業界標準の転送プロトコルである TLS などを使用しています。

暗号化: お客様は、機密性とデータの整合性を保護するためのベスト プラクティスに沿って、ストレージ内のデータと通信中のデータを暗号化することができます。Azure では、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を使用しています。お客様の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可能です。

データの冗長化: お客様は、コンプライアンスまたはレイテンシへの懸念を理由に国内でのデータ保管を選択することも、セキュリティや災害復旧目的で国外でのデータ保管を選択することも可能です。データの冗長化のために、選択した地域内でデータがレプリケートされる場合があります。

データの破壊: お客様がデータを削除するか 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、マイクロソフトは厳格な基準に従ってストレージ リソースを上書きします。Azure Storage、Azure VM、Azure Active Directory などのクラウド サービスに関する契約の一環として、マイクロソフトはデータを所定の手続きに従って削除することを契約上お約束しています。

「セキュリティの観点からいうと、ほとんどの銀行のデータセンターよりも Azure の環境の方が明らかに安全ですね。」

John Schlesinger 氏

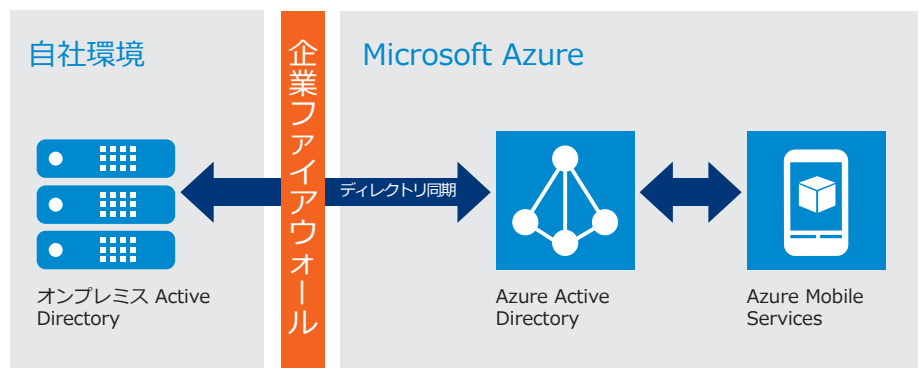
Temenos 社 (スイス)、チーフ エンタープライズ アーキテクト

ID とアクセスの管理

マイクロソフトには、マイクロソフトの従業員による Azure へのアクセスを制限する厳格な規制があります。Azure では、環境、データ、アプリケーションへのアクセスをお客様自身で管理できます。

エンタープライズ クラウド ディレクトリ: Azure Active Directory はクラウドの包括的な ID およびアクセス管理ソリューションであり、コア ディレクトリ サービス、高度な ID ガバナンス、セキュリティ、アプリケーション アクセス管理が統合されています。Azure Active Directory を使用することで、開発者はポリシーベースの ID 管理をアプリケーションに容易に組み込むことができます。Azure Active Directory Premium には、企業の ID やアクセスに関するより高度な要件に対応可能な機能が用意されています。Azure Active Directory により、オンプレミス、クラウド、モバイルのソリューション間での単一 ID 管理が可能になります。

Active Directory



2 要素認証: Microsoft Azure は、Multi-Factor Authentication (MFA) 機能を提供しています。これにより、オンプレミスとクラウド両方のアプリケーションへの簡素なサインイン プロセスを望むユーザーの需要を満たしながら、データとアプリケーションへのアクセスのセキュリティを強化して、規制を遵守することができます。通話やテキスト メッセージ、モバイル アプリの通知といった、ユーザーが選べる簡易的な各種照合オプションを通じて強力な認証が実現されます。

アクセス監視とログ記録: アクセス パターンの監視や潜在的な脅威の特定と抑制のために、セキュリティ レポートが使用されます。システムへのアクセスといったマイクロソフトによる管理操作はログに記録されるため、不正な変更や意図しない変更があった場合に監査証跡として使用できます。その他の脅威については、Azure のその他のアクセス監視機能を有効にするか、サードパーティの監視ツールを使用して検出することができます。また、お客様はマイクロソフトに対して、自社環境へのユーザー アクセスに関するレポートを要求できます。

プライバシー: データの所有権と管理権はお客様に

お客様が利用したいと考えるのは、信頼のおけるクラウド プロバイダーだけです。お客様にとっては、自社の情報のプライバシーが保護され、適切な方法でデータが使用されているという確信を持つことが重要になります。

マイクロソフトでは、プライバシーを保護するための製品やサービスの開発方法と運用方法を定めたプログラムであるプライバシー バイ デザイン (Privacy by Design) に従って、Azure にプライバシー保護を組み込んでいます。プライバシー バイ デザインの原則をサポートする基準とプロセスには、Microsoft Online Services のプライバシーに関する声明 (重要なプライバシー要件と実施基準を詳述したもの) と、マイクロソフトのセキュリティ開発ライフサイクル (プライバシー要件への対処を取り入れたプロセス) が含まれます。

「論点はもはや、『どのようにクラウドに移行するか』ではなく、『クラウドに移行した後、投資とリスクエクスポージャーが最適化されたことをどのように把握するのか』に移っています。」



マイクロソフトでは、顧客データを保護するために、EU モデル条項（個人情報の取扱いに関する規約）の提示や国際標準への準拠をはじめとする契約上の義務履行の努力を払うことで、さらなる保護を施しています。

Azure に保管された顧客データは、サービスの提供目的（サービスの提供に適合する目的を含む）にのみ使用されます。Azure では、広告宣伝または広告宣伝に準ずる営利目的で顧客データを使用することはありません。

契約上の義務履行の努力: マイクロソフトは大手クラウド サービス プロバイダーとして唯一、対象の Azure サービスに強固なプライバシー保護を組み入れていることを保証する契約上の義務を果たしています。マイクロソフトがサポートする契約上の義務履行への取り組みは、以下のとおりです。

- EU モデル条項: EU データ保護法は、EU 内の顧客の個人データの欧州経済領域 (EEA) 外への移転について定めるものです。マイクロソフトはお客様に、該当するサービスの個人データの移送に関する契約上の保証事項を盛り込んだ EU 標準契約条項を提示します。ヨーロッパのプライバシー規制当局は、Azure のエンタープライズ クラウドのお客様に対して履行するプライバシー保護契約が、国際的なデータ移送に関する現在の EU 標準を満たしていると認定しています。マイクロソフトは、クラウド プロバイダーとして初めてこの認定を受けました。
- 米国と EU 間の Safe Harbor フレームワーク、および米国とスイス間の Safe Harbor フレームワーク: マイクロソフトは、EEA およびスイスからのデータの収集、使用、保持に関して米国商務省が設定したこれらのフレームワークに従います。
- ISO/IEC 27018: クラウドのプライバシー保護について定めた初の国際的な実施基準であり、マイクロソフトはこれに準拠した最初の大手クラウド プロバイダーです。ISO/IEC 27018 は、クラウドに保存される個人データのプライバシーを保護する統一された国際的な取り組みを確立するために開発されました。第三者機関の British Standards Institution (BSI) が行った審査によって、Microsoft Azure はこのガイドラインの実施基準を満たしていることが認められました。ISO 27018 では、お客様の明示的な同意を得ずに、顧客データを広告およびマーケティングの目的に使用することを禁止しています。

マイクロソフトのスタッフによるアクセスの禁止: 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 Azure の利用を支援するために必要な場合に限り、これには、Azure の運用に影響する問題の防止、検出、修復を目的としたトラブルシューティングと、ユーザーに対する新たな脅威や進化する脅威（マルウェア、スパムなど）の検出と防止にかかわる機能の改善が含まれます。アクセスが許可された場合、アクセスは制御され、アクセス履歴が記録されます。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。

合法的な情報開示要求の通知: マイクロソフトは、お客様のデータは、その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ます。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、マイクロソフトが Azure の顧客データを法執行機関に開示することはありません。政府が Azure の顧客データに対する合法的な開示要求をマイクロソフトに対して行った場合でも、マイクロソフトは原則に基づいて開示するデータを制限し、透明性のある行動に徹します。

- マイクロソフトは、第三者に対して顧客データへの直接的または制限のないアクセスを提供しません。マイクロソフトは、妥当な合法的な要請があった場合にのみ、特定のデータを開示します。
- 国家の安全保障目的も含め、政府が顧客データの開示を求める場合、その要請は適用できる法的手続きに従って行われなければなりません。政府はコンテンツに対する令状または裁判所命令、あるいはアカウント情報の召喚令状を交付する必要があります。マイクロソフトがやむを得ず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します。

- マイクロソフトは、特定のアカウントまたは ID からの要求にのみ対応します。マイクロソフトの顧客データに対する全面的なアクセスまたは無差別アクセスは存在しません。すべての要求は、マイクロソフトの法務部門によって明確に検討されます。同部門が要求の正当性を確認し、正当ではない要求については却下し、徹底して要求に指定されたデータのみを提供します。

この透明性への契約上の履行義務の一環として、マイクロソフトは法執行機関から受けた顧客データ開示要請の範囲と件数を詳述する「Law Enforcement Requests Report (法執行機関要求レポート)」を定期的に公開しています。

データ使用ポリシーの透明性と簡素化の促進

マイクロソフトは、データのプライバシーとセキュリティを保護するプロセスについて、運用とポリシーを含め、お客様に継続的に情報を提供します。さらに、第三者によるサービスの監査の要約も提供します。これは、お客様自身によるコンプライアンスの徹底に役立ちます。

「ユーザーが破損や紛失に備えてノート PC のバックアップをとるように、エストニアはロシアからの攻撃を想定して、国家のバックアップに取り組んでいます。」

The Economist
エストニアの Azure クラウドによるバックアップに関するレポート

お客様自身がデータを管理

クラウドへの移行によって、多くの組織がメリットを得られることは明らかです。一方で、データを管理できなくなるのではないかという不安が、企業意思決定者をためらわせています。データはどこに保存されるのか、データの帰属先はどこになるのか、だれがデータにアクセスするのか、プロバイダーを乗り換える場合はどうなるのかというような疑問を持っているのです。疑問は当然です。マイクロソフト自身、データをお客様の管理下に置くことを契約上の義務としたときに同じことを考えました。このような契約上の義務は、他の大手クラウド サービス プロバイダーには類を見ません。

データの所有者はお客様自身: この信念は、マイクロソフトの取り組みの基盤を成すものです。Azure を利用する際、お客様はデータの排他的な所有権を保持します。マイクロソフトは、多様なデータを保護するための措置を講じます。

マイクロソフトでは、顧客データとは「オンライン サービスの利用を通じて、お客様またはお客様の代理人によって当社に提供されるすべてのテキスト、音声、ビデオ、画像ファイル、およびソフトウェアを含むすべてのデータ」と定義しています。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、Azure で実行するアプリケーションなどです。

お客様はいつでも、理由にかかわらず、またマイクロソフトの支援を得ることなく、自社のデータにアクセスできます。マイクロソフトは、広告を目的としてお客様のデータまたはその派生情報を利用することはしません。お客様のデータは、サービスの提供目的 (サービスの提供に適合する目的を含む) にのみ使用されます。

-
- **顧客データ**とは、Azure の利用を通じてお客様またはお客様の代理人によってマイクロソフトに提供されるすべてのテキスト、音声、ビデオ、画像ファイル、およびソフトウェアを含むすべてのデータです。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、Azure で実行するアプリケーションなどです。
 - **管理者データ**は、Azure のサインアップ、購入、または管理の際に提供された氏名、電話番号、メール アドレスといった管理者 (アカウント担当者、サブスクリプション管理者など) に関する情報です。
 - **メタデータ**には、構成情報や技術的な設定と情報が含まれます。たとえば、Azure Virtual Machines のディスクの構成設定や、SQL Database のデータベース設計などです。メタデータには、顧客データの発生元の情報は含まれません。
 - **アクセス制御データ**は、Azure 内の他の種類のデータまたは機能へのアクセスを管理するために使用されるデータです。これには、パスワード、セキュリティ証明書、認証に関連するその他のデータなどが含まれます。
-

「当社のブランドの
存続は、IT システム
の継続性にかかって
います。今は Azure
で実行しているので
以前よりもずっと
安定しています。」

Andrew Goodin 氏
Zespri International 社
(ニュージーランド)
情報システム担当グローバル
マネージャー

データの保存場所の管理: お客様がマイクロソフトを信頼し、データを託されたとしても、データの管理権はお客様のものです。多くのお客様にとってデータの保存場所を把握すること、そしてその場所を管理することは、データのプライバシー、コンプライアンス、ガバナンスにおける重要な要素です。Microsoft Azure は、世界規模で拡大を続けるデータセンターのネットワークを提供しています。Azure の大半のサービスでは、顧客データを保管する特定の地域をお客様が指定できます。データの冗長化のために指定した地域内でデータがレプリケートされることがありますが、地域外に転送されることはありません。

暗号化キーの管理: 暗号化データを管理するために、お客様は独自の暗号化キーを生成して管理し、暗号化キーの使用権限をだれが持つのかを決定することができます。また、そのような暗号化キーのマイクロソフト側のコピーを無効にすることもできます。ただし、コピーを無効にすることによって、問題やセキュリティ上の脅威のトラブルシューティングや修復を行うマイクロソフトの権限が制限される場合があります。

ロールベースのアクセス制御: マイクロソフトでは、ロールの割り当て、ロールの認証、アクセス許可の認証に基づいて、お客様がシステムへのアクセスを許可されたユーザーのみに制限できるようにする手法を採用しています。ロールに基づく承認をサポートするツールはさまざまなマイクロソフトのクラウド サービスで提供されており、あらかじめ定義されたユーザー グループのアクセス制御を簡単に行うことができます。

データの破壊の管理: お客様がデータを削除するか、マイクロソフトのクラウド サービスの利用を終了した場合、マイクロソフトはストレージ リソースの再利用に先立ち、厳格な基準に従ってストレージ 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。これは、データの削除とストレージ ハードウェアの破壊に関して所定の手続きに従うことを契約上の義務としてお約束しています。

透明性

データを管理する権限を効果的に行使するためには、データへのアクセス権と可視性が必要です。データの保管場所を知る必要もあります。また、明文化され、すぐに使用できるポリシーと手続きを通じて、クラウド プロバイダーが顧客データのセキュリティを確保する方法、アクセスを許可するユーザー、アクセスを許可する条件などについても把握しておく必要があります。

データの保管場所と使用方法: Microsoft Azure では、世界規模で拡大を続けるデータセンターのネットワークのどこに顧客データが保管されるかをお客様自身が把握できます。災害発生に備えて複数の場所にバックアップを保管する必要性と、データを特定の地域に置かないという必要性を両立させることができます。マイクロソフトでは、全データセンターについて明確なデータ マップと地理的境界情報を提供します。

データの保護方法: お客様は、セキュリティ ポリシーと手続きに関する最新の情報にアクセスできます。マイクロソフトは、セキュリティ開発ライフサイクルを公開し、これに準拠することで、透明性を促進しています。

顧客データへのアクセス要請者の公開: マイクロソフトは、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る場合を除き、Azure の顧客データを政府期間または法執行機関に開示することはありません。Azure の顧客データに対する合法的な開示要求に応えながら、原則への準拠、公開範囲の限定、透明性の確保に取り組んでいます。マイクロソフトでは、法執行機関から受けた顧客データ開示要請の範囲と件数を詳述する「Law Enforcement Requests Report (法執行機関要求レポート)」を定期的に公開しています。

セキュリティ侵害の通知: 顧客データが侵害された場合、マイクロソフトはお客様にその旨を通知します。Azure では、「特定」から「教訓を得る」までの全工程でのインシデント対応を規定する包括的で透明性のあるポリシーを定めています。

監査による基準の認定: British Standards Institute (BSI) などの第三者が実施する厳格な監査により、国際標準が要求する厳格なセキュリティ規制を Azure が遵守しているかどうかを検証します。マイクロソフトが透明性確保のために実施している取り組みの一環として、お客様は第三者機関による監査結果を要求して、Azure が多くのセキュリティ対策を実装していることを確認できます。

お客様向けのガイド: マイクロソフトは、セキュリティ レスポンス センターの進捗状況レポートやセキュリティ インテリジェンス レポートを発行してお客様に脅威の状況を知らせると共に、お客様の資産を保護するためのリスク管理を規定したガイドを提供します。

透明性センター: マイクロソフトでは、透明性センターを運営しています。このセンターを通じて、政府機関のお客様はソースコードをレビューし、その整合性について再確認して、抜け道がないことを確認できるようにしています。

「2020 年までに、クラウドは『パブリック』とも『プライベート』とも呼ばず、IT をプロビジョニングするための単なるビジネス手段に過ぎなくなっていることでしょう。」



コンプライアンス: Azure は国際標準に準拠

マイクロソフトは、堅牢かつ革新的なコンプライアンス プロセスの開発に重点的に投資しています。マイクロソフトのオンライン サービス向けコンプライアンス フレームワークには、複数の規制基準に対応した統制活動が整備されています。これにより、マイクロソフトは共通の統制手法によってサービスを設計、構築することが可能になり、現在そして今後のさまざまな規制に円滑に対応できるようになります。

また、マイクロソフトのコンプライアンス プロセスにより、お客様は複数のサービス全体でコンプライアンスを容易に達成し、変化するニーズに効率的に対応することが可能になります。セキュリティを強化したテクノロジーと効果的なコンプライアンス プロセスの双方を合わせることで、マイクロソフトは第三者機関によるさまざまな認定を維持、取得することが可能になり、お客様はコンプライアンス体制が整備されていることを自社の顧客、監査人、規制当局に実証できるようになります。透明性に対する取り組みの一環として、マイクロソフトは第三者機関による検証結果をお客様と共有します。

認定と認証: Azure は、ISO 27001、FedRAMP、SOC 1 および SOC 2 など、国際的なコンプライアンス標準と、地域および業界に固有のコンプライアンス標準を幅広く満たしています。これらの標準に含まれている厳格なセキュリティ統制に Azure が準拠していることは、第三者の厳しい監査によって認められ、Azure サービスが世界トップレベルの業界標準、認定、認証、承認と連携し、これらを満たすことが証明されています。

独立機関により審査された包括的なコンプライアンス: Azure は、お客様のビジネス目標達成と、業界標準および規制への対処を支援するコンプライアンス戦略を念頭に設計されています。このセキュリティ コンプライアンス フレームワークには、認定および認証の獲得を目的とした、テスト/監査フェーズ、セキュリティ分析、リスク管理のベスト プラクティス、セキュリティベンチマーク分析が含まれます。Microsoft Azure は、すべての対象サービスに次の証明書を提供します。

CDSA: Content Delivery and Security Association (CDSA) は、デジタル メディアを統制する著作権侵害対策に準拠した Content Protection and Security (CPS) 標準を規定しています。Azure はコンテンツの開発と配布の安全なワークフローを実現し、CDSA の監査に合格しました。

CJIS: 米国州政府または地方行政機関が FBI の犯罪司法情報サービス部 (CJIS) のデータベースにアクセスするには、CJIS のセキュリティ ポリシーに従うことを求められます。Azure は、CJIS のセキュリティ ポリシーへの準拠を契約により履行する唯一の大手クラウド プロバイダーです。マイクロソフトでは、法執行機関と公安組織が満たさなければならない要件と同じ要件を厳守することを確約しています。

CSA CCM: Cloud Security Alliance (CSA) は会員運営型の非営利団体であり、クラウド内のセキュリティ確保に向けたベスト プラクティスを広め推奨することを使命としています。CSA の Cloud Controls Matrix (CCM) バージョン 1.2 には、その中で定義されているセキュリティ、プライバシー、コンプライアンス、リスク管理の諸要件への対応状況に関して詳細な情報が記載されています。これは、CSA の Security Trust and Assurance Registry (STAR) で公開されています。

EU モデル条項: マイクロソフトは、EU 外部への個人データの移送に関する契約上の保証事項を盛り込んだ EU 標準契約条項をお客様に提示します。マイクロソフトは、EU の第 29 条作業部会から、Azure のエンタープライズ クラウドのお客様に提供するプライバシー保護契約が国際的なデータ移行に関する現在の EU 標準を満たしていることを認める共同書簡を付与されました。この認定を受けた企業はマイクロソフトが初めてです。これにより Azure のお客様は、マイクロソフトのサービスを利用してヨーロッパとその他の地域の間でクラウド上のデータを自由に移動させられるようになりました。

FDA 21 CFR Part 11: 米国食品医薬品局 (FDA) 連邦規則集 (CFR) 21 条第 11 章は、米国内で製造または消費される食品および医薬品を販売する企業の電子記録の安全性に関する要件を定めたものです。独立した第三者である SSAE および ISO の監査法人により作成される Azure のコンプライアンス レポートは、マイクロソフトで確立された手続きと技術による対策を明らかにしています。このレポートは、21 CFR Part 11 の要件を満たすために使用できます。マイクロソフトは、これらのレポート内の関連した対策がどのように FDA 21 CFR Part 11 規制の遵守に影響を及ぼすかについて提示することができます。

FedRAMP: Azure は、連邦政府によるリスクおよび認証管理プログラム (FedRAMP) の合同認定委員会 (JAB) から、FIPS 199 分類に基づくインパクト レベルで「Moderate」に達していると評価され、P-ATO (Provisional Authority to Operate) を取得しています。FedRAMP は、米国連邦機関で使用されるクラウド サービスに対するセキュリティ評価、認定、モニタリングの標準的アプローチを策定する米国政府のプログラムです。このプログラムを通じて、納税者および個々の企業は、個別の評価を実施する時間とコストを節約できます。

FERPA: 家庭教育の権利とプライバシーに関する法 (FERPA) は、学生の教育記録のプライバシーを保護する米国連邦法です。マイクロソフトは、FERPA によって課される使用と開示に関する制限に同意するものとします。

FIPS 140-2: Azure は、暗号化を実装する製品およびシステムに対する最小限のセキュリティ要件を規定する米国連邦政府標準規格である Federal Information Processing Standard (FIPS) 140-2 に準拠しています。

HIPAA: 医療保険の携行性と責任に関する法律 (HIPAA) は、保護対象の医療情報 (PHI: Protected Health Information) と呼ばれる患者情報へのアクセスを制限する米国連邦法です。Azure はお客様に、HIPAA 法および HITECH 法の特定のセキュリティ条項およびプライバシー条項の遵守を規定する HIPAA 事業提携者契約 (BAA) を提供しています。お客様の個々のコンプライアンスへの取り組みを支援するために、マイクロソフトはお客様に BAA を Azure の契約の補遺として提供します。

IRAP: Azure は、オーストラリア政府の Information Security Registered Assessors Program (IRAP) の査定を受けました。これは、マイクロソフトが適切で効果的なセキュリティ対策を行っていることを公共機関のお客様に保証するものです。

ISO/IEC 27018: マイクロソフトは、クラウド サービス プロバイダーによる個人情報の取り扱いについて定めた ISO/IEC 27018 実施基準に準拠した最初のクラウド プロバイダーです。

ISO/IEC 27001/27002:2013: Azure は、情報セキュリティ管理システムに必要なセキュリティ対策を定義したこの標準に準拠しています。

MLPS: 情報セキュリティ等級保護管理弁法 (MLPS) は、中国公安部によって公布された中国政府の標準に基づいています。21Vianet によって運営される Azure はこの標準に準拠し、クラウド システムの管理面および技術面双方におけるセキュリティに対する保証を提供しています。

MTCS: Azure は、シンガポールの情報技術標準委員会によって開発された、データ セキュリティ、機密性、ビジネスへの影響、運用上の透明性などについて定めたクラウド セキュリティ標準である Multi-Tier Cloud Security Standard for Singapore (MTCS SS) のレベル 1 認定を取得しました。

PCI DSS: Azure は、ほとんどのクレジットカード支払いを受け付ける組織、およびカード会員情報を保管、処理、伝送する組織のためのグローバル認定基準である Payment Card Industry Data Security Standard (PCI DSS) バージョン 3.0 へのレベル 1 準拠を達成しています。

SOC 1、SOC 2: Azure は、Service Organization Control (SOC) レポート フレームワーク SOC 1 Type 2 および SOC 2 Type 2 の監査を実施しており、この両レポートは、米国および国際的な監査要件を広範に満たすために、お客様にご利用いただけます。

SOC 1 Type 2 監査レポートは、Azure の各種統制の設計と運用の有効性を証明します。SOC 2 Type 2 監査レポートには、Azure のセキュリティ、可用性、機密性に関連する統制環境のさらなる検証が含まれます。Azure は毎年監査を受け、セキュリティ統制が維持されていることを保証しています。

TCS CCCPPF: 21Vianet によって運用される Azure は、China Cloud Computing Promotion and Policy Forum (CCCPF) によって策定された Trusted Cloud Service 証明書に合格した中国で最初のクラウド プロバイダーです。

英国 G-Cloud: 英国政府の G-Cloud は、英国内の政府公共機関が使用するクラウド サービスに向けたクラウド コンピューティングに関する証明書です。Azure は、UK Government Pan Government Accreditor から公式認定を受けています。

関連情報

Microsoft Azure トラスト センター

<http://azure.microsoft.com/ja-jp/support/trust-center/>

Cloud Security Alliance Cloud Controls Matrix (英語)

<https://cloudsecurityalliance.org/research/ccm/>

信頼できるクラウド コンピューティング

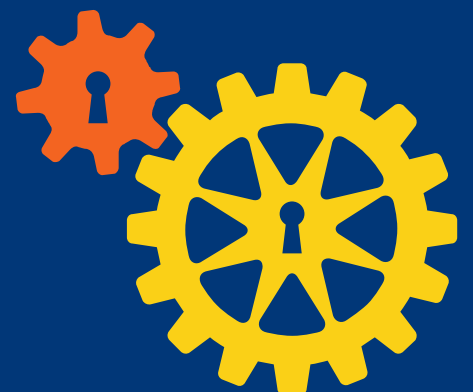
<http://www.microsoft.com/trustedcloud>

Microsoft オンライン サービスのプライバシーに関する声明

<https://www.microsoft.com/privacystatement/ja-jp/OnlineServices/Default.aspx>

プライバシーに関するマイクロソフトの実施基準 (英語)

<http://aka.ms/privacy-practices>





注: このドキュメントで紹介されている推奨事項には、データ量、ネットワーク使用量、コンピューティング リソース消費の増大や、ライセンス コストまたはサブスクリプション コストの追加を伴うものがあります。

© 2015 Microsoft Corporation. All rights reserved. 本ドキュメントは“現状のまま”で提供されます。本ドキュメント (URL などのインターネット Web サイトにある参照先を含む) に記載されている情報や見解は、将来予告なしに変更することがあります。このドキュメントの使用に起因するリスクは、利用者が負うものとします。ここで記載された例は、説明のみを目的とした架空のもので、実在する事物とは一切関係ありません。本ドキュメントは、あらゆるマイクロソフト製品に対する何らかの知的財産権をお客様に付与するものではありません。このドキュメントは、内部的な参照目的でのみ複製および使用することができます。