

# Microsoft Azure の データ保護

## 要約

マイクロソフトは、あらゆるお客様のデータを常に現状のまま保持しています。Microsoft Azure では、多層型のセキュリティ テクノロジとガバナンス テクノロジ、さまざまな運用手順、コンプライアンス ポリシーを通して、保存するデータの機密性と整合性をきめ細かく維持しています。このホワイト ペーパーでは、暗号化のメカニズム、シークレットの管理、アクセス制御など、こうした機密性と整合性を実現する Microsoft Azure のさまざまな機能について説明します。各セクションでは、構造化データ、非構造化データ、転送中データ、保存中データなど、種類と状態にかかわらずエンタープライズ環境の重要データを保護する Microsoft Azure プラットフォームの各種機能の利用方法について詳しく説明します。

## 対象者

Microsoft Azure のデータ保護を中心に説明するこのドキュメントは、情報資産管理を専門とする、または総合的なクラウド IT 管理業務の一貫として情報資産管理に関わっている、情報テクノロジー (IT) プロフェッショナルや IT 導入担当者を対象としています。既に Microsoft Azure に関する知識をお持ちで、暗号化やアクセス制御など、Microsoft Azure プラットフォームと関連サービスのデータ セキュリティに関するツールとテクノロジーについてさらに詳しく知りたい方には、このドキュメントが最適でしょう。セクション 2.1、2.2、および 2.3 は Azure の概要の簡単な説明となるため、現在の Azure サービスに関する知識に応じて省略できます。

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。

公開日: 2014 年 8 月

(c) 2014 Microsoft Corporation. All rights reserved.このドキュメントは "現状のまま" で提供されます。このドキュメントに記載されている情報や見解 (URL 等のインターネット Web サイトに関する情報を含む) は、将来予告なしに変更される場合があります。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す。実在する事物とは一切関係ありません。

このドキュメントは、マイクロソフト製品の知的所有権に関する法的な権利をお客様に許諾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。

# 目次

<b>1</b>	<b>概要</b>	<b>5</b>
<b>2</b>	<b>Microsoft Azure のデータ ストレージ</b>	<b>7</b>
2.1	MICROSOFT AZURE STORAGE	8
2.1.1	データ構造	9
2.1.2	データ転送	9
2.2	MICROSOFT AZURE SQL DATABASE	10
2.2.1	Azure SQL Database の構造	10
2.3	MICROSOFT AZURE ACTIVE DIRECTORY	11
2.3.1	Azure Active Directory のアーキテクチャ	11
2.4	データにアクセスできるユーザー	12
2.4.1	シングル サインオン (SSO)	13
2.4.2	2 要素認証 (2FA)	13
2.4.3	アクセス制御: サブスクリプション	13
2.4.4	アクセス制御: ストレージ	14
2.4.5	アクセス制御: Azure Tables と SQL Database	14
<b>3</b>	<b>データ セキュリティについて</b>	<b>16</b>
3.1	リスクとリスク管理	16
3.1.1	データ リスクを理解する	16
3.2	データに対する脅威	17
3.2.1	データへの攻撃の分類	18
3.3	MICROSOFT AZURE における既定の保護対策	19
3.3.1	Azure AD におけるデータ セキュリティ	21
3.4	プラットフォームの暗号化	22
3.4.1	転送中の暗号化	23
3.4.1.1	VM 間	23
3.4.1.2	お客様とクラウド間	23
3.5	データの削除	24
3.5.1	サブスクリプション	24
3.5.2	Microsoft Azure Storage	25
3.5.3	Microsoft Azure Virtual Machines	25
3.5.4	Azure SQL Database	25
3.6	使用中データに対するコンピューティングのセキュリティ	26
3.7	物理的なデータ セキュリティ	26
<b>4</b>	<b>お客様が構成可能な保護対策</b>	<b>28</b>
4.1	ボリューム レベルの暗号化	29
4.1.1	BitLocker ドライブ暗号化	29
4.1.2	ドライブ暗号化 - パートナー	30

4.1.3	キーの管理とセキュリティ .....	31
4.1.4	サブスクリプションとサービス証明書 .....	31
4.2	AZURE VIRTUAL MACHINES で実行される SQL SERVER の暗号化.....	32
4.2.1	クラウドにおける実装 .....	32
4.3	AZURE の RIGHTS MANAGEMENT サービス.....	34
4.3.1	RMS の基礎: RMS コンポーネントが連携するしくみ.....	34
4.3.2	RMS サーバーの選択肢 .....	36
4.3.3	開発者向け RMS SDK .....	36
4.3.4	RMS 対応のアプリケーション .....	37
4.3.5	組織における RMS .....	37
4.3.6	RMS によるキー管理.....	37
4.3.7	キー配布の追跡 .....	38
<b>5</b>	<b>冗長化とバックアップによるデータ保護 .....</b>	<b>39</b>
5.1	AZURE STORAGE .....	39
5.2	AZURE BACKUP.....	39
5.3	STORSIMPLE クラウド統合ストレージ (CIS) .....	40
<b>6</b>	<b>プライバシーと説明責任 .....</b>	<b>41</b>
<b>7</b>	<b>まとめ .....</b>	<b>42</b>
<b>8</b>	<b>参考資料および関連資料 .....</b>	<b>44</b>
8.1	参考情報 .....	44

## 1 概要

Microsoft Azure では、複数のツールを使用して、セキュリティとコンプライアンスに関する企業のニーズに合わせてデータを保護できます。クラウドのデータ保護で最も重要なことの 1 つは、データが取り得る状態と、それらの状態に応じた制御方法を検討することです。具体的には以下の状態があります。

- **保管中:** 磁気ディスクまたは光ディスクの物理メディア上に静的に配置される、すべての情報ストレージ オブジェクトやコンテナがこの状態に該当します。情報の種類は関係ありません。
- **転送中:** ネットワークやサービス バス (オンプレミスからクラウドの移動と、クラウドからオンプレミスの移動。ExpressRoute などのハイブリッド接続を含む) を経由して、または入出力プロセスに伴ってコンポーネント、場所、プログラム間を移動するデータは、転送中と見なされます。これは、必ずしもクラウド サービス外のコンポーネントとの通信プロセスだけを指すわけではありません。たとえば 2 つの仮想ネットワーク間などの内部的なデータ移動も転送中と見なされます。
- **使用中 (処理中):** 仮想メモリ上のテーブルやメッセージ キュー内のトランザクションなど、動的に使用されているデータを指します。CPU キャッシュ内の暗号化キーも使用中と見なされます。プロセス中にホストまたはゲストが実行した操作に応じて情報が使用される場合 (ディスクへ送信されるページ ファイルではなく、アクティブなメモリ内で実行されるリアルタイムのデータベース クエリなど)、そのセキュリティ状態は、暗号化の有無やオペレーターのセキュリティ コンテキストに応じて変わります。

さらに、保管中のデータは基本的に以下の 2 つに分類されます。

1. **稼働中データ:** Azure SQL Database などのストレージの形式で保管されるデータです。稼働環境の運用では、そのストレージへのアクセスの要求はコンピューティングが処理します。この場合、こうしたストレージ内のデータ保護を目的に、保管中データの暗号化が適用されます (データが使用される場合はコンピューティング領域が処理します)。
2. **稼働中でないデータ:** データが仮想ハード ディスク (VHD) などのストレージ形式で保管されているが、その VHD が稼働環境で運用されていない場合、データは稼働中と見なされません。これに該当するのは、アップグレード対象の VHD が読み込みまたはマウントされていない場合などです。この場合も保管中データの暗号化は適用されますが、コンピューティング領域は関係しません。

データ保護では、暗号化対策に伴うコンピューティングのサイクル、アプリケーション パフォーマンス、リソース レイテンシ、管理作業で発生する負担、コンテンツの分類とフィルタリング、権限管理など、さまざまな面からコストを比較検討する必要があります。たとえばデータ損失回避のための冗長化を実現するには、追加のストレージ容量、リージョン固有のプレゼンス、地理冗長などが必要になりますが、どれを採用しても追加でコストがかかります。

ここからのセクションでは、暗号化、アクセス制御、その他の方法を通して、どうすれば、またどこに配置すれば情報を最も効果的に保護できるかについて触れていきます。要件の多くは、データ ガバナンスおよびコンプライアンスの取り組みにおける企業独自のニーズに基づいて決まります。また、

HIPAA や FedRAMP などの業界規制や政府規制、ISO 27001 などの国際標準に基づき、プロセスやポリシーの策定によって実施される対策もあります。こうした義務を果たすための有効なしくみを確立する責任は、Microsoft Azure とそのお客様が等しく分け合うものです。具体的には、サービス、アプリケーション、データの基盤となる各種規制や標準に準拠したプラットフォームをマイクロソフトが提供し、情報資産の信頼性と整合性を確保するクラウド環境の設計と構成は Azure のお客様が担当します。

## 2 Microsoft Azure のデータ ストレージ

まず、データ ストレージ (一時ストレージやアクティブなプロセスのメモリ以外のコンテナに保持されているデータ) の保護について見ていきましょう。Microsoft Azure では主に 3 種類の領域でデータを保持できます (図 1 を参照)。以下に示すように、各テクノロジーには、特定の種類のデータ処理に対応したセキュリティ モデルがあります。

- Azure Storage – 構造化データおよび非構造化データに対応した永続型のクラウド ストレージ
- SQL Database – 完全に管理されたリレーショナル データベース サービス
- Azure Active Directory – ID 管理とアクセス管理

一時ディスク領域の概念は Virtual Machines (IaaS: Infrastructure as a Service) と Cloud Services (PaaS: Platform as a Service) の両方に取り入れられています。Cloud Services の場合はロール インスタンス全体が非永続的なものとして扱われます。Azure Storage に明示的に書き込まれていないすべてのデータは常に失われる可能性があります。

Virtual Machines (VM) の一時ディスクはノード上の物理ディスクであり、スクラッチ領域 (OS のページ ファイルなど) として使用できます。ディスク上のデータは永続的ではなく、修正プログラムの適用中に VM が別の物理マシンに移動した場合や、Azure がホスト ノードに問題を検出した場合などによって、いつでも失われる可能性があります。

Virtual Machines にも Cloud Services にも同様の概念が採用されていますが、Virtual Machines が Cloud Services と異なるのは、プライマリ ディスクが永続的であるという点です。これは、オペレーティング システムなど、お客様がデプロイするすべての項目のホストとしてプライマリ ディスクが使用されるためです。IaaS をご利用のお客様には、一時ドライブも提供されます。一時ドライブはローカル ホストにあるため、一般的に高速なパフォーマンスが得られます。通常 D: ドライブ (Windows) または /dev/sdb1 (Linux) として表示されます。

仮想ハード ドライブ (VHD) は、ディスクとディスク イメージ (テンプレート) 用のコンテナを指します。VM が使用する VHD は Azure BLOB ストレージからマウントされます。Cloud Services のロール インスタンス (アプリケーションのコードとロール構成が実行される仮想マシン) は、ロール インスタンスが実行されるローカル ホスト上の VHD のみを使用します。この VHD は、ロールのプロビジョニングが解除されるたびに削除されます。新たに開始されたロールは、ベース イメージの最新コピーを取得します (つまり Cloud Services のロールは永続的ではありません)。

注意が必要なその他のさまざまなサービスやコンテナを以下に示します。これらも機密情報を格納する可能性があります。

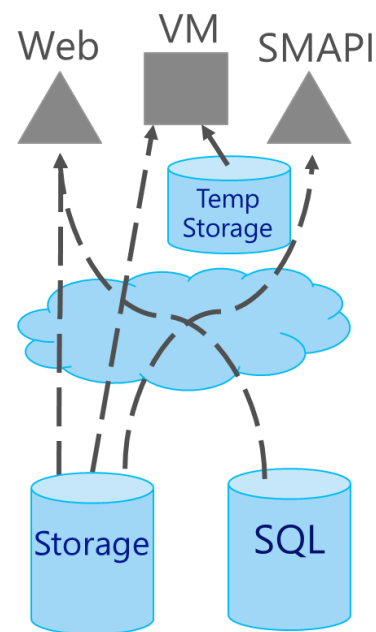


図 1: Azure のデータ ストレージ

- キー リポジトリ (クラウド内、オンプレミス、パートナーと共有、キー管理サービス (KMS) 内)
- ログとレポート (Azure Storage、SQL Database、Azure Active Directory などのコア サービス)
- カスタムのクラウド アプリケーションおよびサービス (HDInsight や BizTalk Services などのサービス)
- お客様が採用したサードパーティのクラウド サービスやデータ処理プロバイダー (EDI パートナーなど)
- ビジネス パートナーや顧客のクラウド環境 (または、オンプレミスのプライベート クラウド)。セキュリティ ログを保管、分析するサードパーティのセキュリティ情報/イベント管理 (SIEM) システムなどがあります。
- お客様がオフロードまたはエクスポートするデータ (仮想ハード ドライブ、データベース、バックアップなど)

## 2.1 Microsoft Azure Storage

Azure Storage は、VM、VHD、構成、お客様のデータを実行するためのリポジトリです。「ログベースのファイル システム」を基盤とするため、Azure Storage (の BLOB、Table、Queue) にいつ何を書き込んでも、書き込まれた項目によってディスク上の既存の値が上書きされることはありません。書き込まれるオブジェクトの種類にかかわらず、すべての書き込みは循環キューに書き込まれた後、物理ディスクにフラッシュされます。新しいデータが配置されるまでトランザクションが完了しないため、データの破損に対する保護をさらに高めることができます。Azure Storage に転送されるすべてのデータは、複数のチャンクに分割され、複数の物理ディスク (および、地理レプリケーションを有効にしている場合は複数の地域) 間でコピーされます。

- **Azure Table ストレージ:** 緩やかに構造化されたデータの格納に使用される (パーティション分割と負荷分散を自動実行する) 分散ソリューションです。一般的なリレーショナル データベースのようなデータ エンジンには搭載されていないため、永続データをシンプルに格納できますが、高度なクエリ、複雑なインデックス処理、直接操作が必要な場合には Microsoft Azure SQL Database (または VM で実行される SQL Server) が適しています。
- **Azure BLOB (バイナリ ラージ オブジェクト) ストレージ:** ドキュメント、メディア ファイル、アプリケーション インストーラー、ドライブ (例: VHD) など、あらゆる種類のテキスト ファイルとバイナリ ファイルを格納できます。BLOB ストレージは Table ストレージのような構造化データやクエリ機能には対応できないため、サイズの大きな非構造化データの格納に最も適しています。
- **Azure Queues ストレージ:** 信頼性に優れた、先入れ先出し (FIFO) によるメッセージ機能を提供します。Cloud Services のコンポーネント間の通信やワークフローの処理に使用されるのが一般的です。複雑なパイプラインの場合には、Queue に似た機能を提供する、構成可能で柔軟性にも優れた Azure Service Bus を使用できます。

Azure Storage と SQL Database の永続データには複製と冗長保存によって高い可用性が実現されますが、Azure Virtual Machines に保存される一時データは、ハードウェア、システム、アプリケーションの障害発生によって失われる可能性があります。



Azure Storage のすべてのノードは Azure コンピューティングのマシンから独立しています。これらのノードは異なるハードウェアにデプロイされ、それらのハードウェアがそれぞれ独自の管理モデルとセキュリティ モデルを適用します。たとえば、アクセス制御ポリシーは Azure Storage が実行し、すべてのストレージ要求には認証が必要です。認証には Bearer トークン モデルが使用され、正しいトークン (キー) を所有しているすべてのユーザーとシステムにデータへのアクセス権が付与されます。無制限のアクセス権を付与する場合は、ストレージ キーに高い特権を許可する必要があります。例外は、BLOB の構成によって匿名認証をサポートできる点です。

Azure Storage ではその他に、Shared Access Signature (SAS) という種類のトークンをサポートしています。これを URL に追加することによって、BLOB、Table、Queue に対する限定的な代理人アクセスを許可できるようになります。アクセスは、ストレージの種類に応じて、操作 (読み取り、書き込み、追加、エンキュー、デキューなど) や時間帯を限定することができます。

### 2.1.1 データ構造

Microsoft Azure Storage は、すべての BLOB をコンテナに整理することで、オブジェクトのグループにセキュリティ ポリシーを割り当てられるようにしています。すべての Azure サブスクリプションでストレージ アカウントを複数設定できます。1 つのストレージ アカウントが保持できるコンテナの数は無制限で、1 つのコンテナが保持できる BLOB の数も、ストレージ アカウントの容量の上限に達しない限りは無制限です。Azure Storage は以下の 2 種類の BLOB を提供します。

- **ブロック BLOB** – ドキュメント、メディア ファイル、バックアップなど、クラウド オブジェクトのストリーミングと格納に最適化されています。
- **ページ BLOB** – Virtual Machines の VHD や Cloud Services のドライブとしての利用と、ランダム書き込みのサポートに最適化されています。

### 2.1.2 データ転送

データの量や利用可能な帯域幅などの考慮事項によって、オンプレミスのデータセンターから Azure Storage へのデータ移動にインターネット接続を使用することが必ずしも最適でない場合があります。Azure Import/Export サービスを活用すれば、BLOB ストレージの大容量データをハードウェアベースのオプションによって配置/取得できます。このサービスでは、BitLocker で暗号化されたハード ディスク ドライブをお客様が Azure データセンターに直接発送していただければ、クラウド オペレーターがお客様のストレージ アカウントにコンテンツをアップロードします。オペレーターが Azure のデータをドライブにダウンロードしてお客様に返送することも可能です。このプロセスでは暗号化されたディスクだけを受け付けます (ジョブ設定時にサービスによって生成された BitLocker キーが使用されます)。BitLocker キーを別途 Azure に提供することによって、アウトオブバンドのキー共有が実現されます。

## 2.2 Microsoft Azure SQL Database

構造化データまたはトランザクション データを扱うには、SQL Server インスタンス全体を Azure VM にデプロイする (IaaS)、または Azure SQL Database を使用する (PaaS) といういずれかのオプションを選択できます。Azure VM の SQL Server は、独自のオンプレミス データセンターで仮想化して実行される SQL Server と同等で、ドメインに参加させれば、企業の 1 つの信頼境界の下にオンプレミスとクラウド両方の環境に対応できるハイブリッド アプリケーションを簡単に開発できます。

Azure SQL Database は SQL Server と多くの部分で共通していますが、以下のような設計方針の違いから、VM の SQL Server とはいくつかの点で機能が異なります。

- VM で実行される SQL Server は、既存のアプリケーションとの高い互換性を保つことと、ハイブリッド アプリケーションでの利用に最適化されています。SQL Server のパッケージ製品の全機能が提供されており、管理者は専用の SQL Server インスタンスとクラウド ベースの VM をすべて管理できます。
- SQL Database は、スケールアウト データ層をクラウド内に迅速かつ容易に構築することに最適化されています。Virtual Machines やデータベース ソフトウェアのプロビジョニングとメンテナンスが不要になるため、お客様の管理コストは継続的に削減されます。

必要な拡張性や可用性がどの程度得られるかというデータベース運用上の特性とは別に、VM の SQL Server と SQL Database には構成と管理のレベルという点でもいくつかの違いがあります。お客様が VM をデプロイした場合は、構成とセキュリティに関するすべての責任はお客様にあります (SQL Server と Azure SQL Database の TDE に関するセクションを参照)。一方 Azure SQL Database では、プラットフォームの構成やアップグレード、修正プログラムの適用といった作業はマイクロソフトが担当します。

インターネットの両側で機能が運用されるハイブリッド アプリケーション (さまざまなコンポーネントをオンプレミスと Azure で同時に実行し、機密データをお客様のローカルに保存しながら、クラウドへのレプリケーションも実行できる多層アプリケーション) を実現することで、トランスポート、プロトコル、認証/承認の各層に実装された保護対策を活用できるようになります。

### 2.2.1 Azure SQL Database の構造

Azure SQL Database は PaaS によるリレーショナル データベース サービスです。お客様は標準のインターフェイスを使用してデータベースにアクセスでき、基盤となるシステムは Azure プラットフォームとマイクロソフトが管理します。各物理マシンには数百以上のユーザー データベースを配置できます。お客様のデータベースは独自の論理サーバー インスタンスに配置され、これらのインスタンスは独立した複数のコンテナによって実装されています。こうすることで、お客様の環境とデータの高い独立性を維持しながらマシンの容量を最適化し、経済性にも最適化されたソリューションを実現しています。

## 2.3 Microsoft Azure Active Directory

Azure Active Directory (AD) は、機能の面では、マルチテナントのクラウド サービスとアプリケーションのニーズを満たす設計が追加された、Windows Server Active Directory のクラウド版拡張と言えます。ID リポジトリであり、組織のユーザー、グループ、オブジェクトに対して認証、承認、アクセス制御を実行するエンジンでもある点は、Windows Server Active Directory Domain Services (AD DS) と変わりません。Azure AD ではクラウド サービスという利点を活かして高い拡張性と可用性を実現しており、300 万以上のアクティブ ユーザーと 80 万以上のアクティブ テナントを同時にサポートします。

### 2.3.1 Azure Active Directory のアーキテクチャ

Azure AD の内部構造は AD DS と非常によく似ています。いずれも、スキーマが定義するオブジェクトとルールによる高度な階層型リレーショナル データ ストアです。テナントはコンテナに割り当てられ、コンテナは複製されたディレクトリ ストア パーティションに格納され、各パーティションは特定のリージョンに割り当てられています (図 2 を参照)。データの損失を防ぐため、書き込みは独立したデータセンターのレプリカにローカルでコミットされた後に、呼び出し側に返されます。リージョン間のレプリケーションは、各リージョンのコンプライアンス要件に基づいて制御されます。

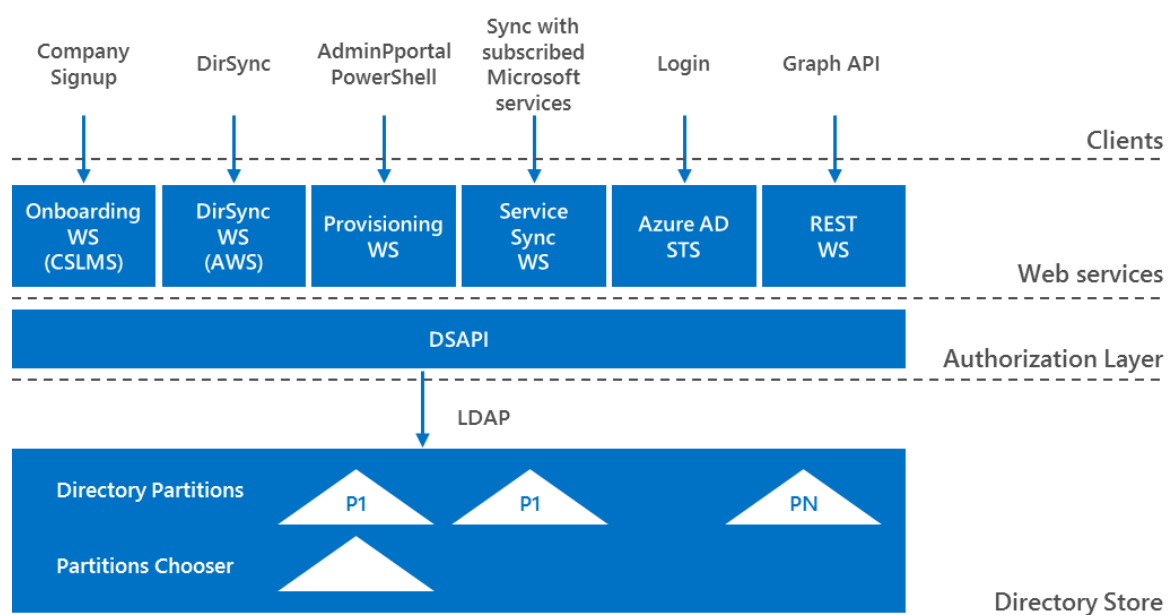


図 2: Azure Active Directory のアーキテクチャの概要

それぞれの組織 (Azure AD テナント) はセキュリティ境界によって論理的に分離されているため、隣接するテナントへのアクセスや侵入は意図的にも偶発的にも不可能です。Azure AD は、独立したネットワーク セグメントに隔離された「ベア メタル」サーバー上で実行されています。そこでは、

ホストレベルのパケット フィルタリングと Windows Firewall によって、許可されない接続やトラフィックがブロックされています。

## 2.4 データにアクセスできるユーザー

Microsoft Azure Storage のすべての種類には、必須のデータ アクセス手順に加えてデータ アクセスとデータ制御に関する独自のモデルがあり、これらを活用することでデータの利用方法や格納方法を制御できます。制御に使用できるメカニズムについては以下で詳しく説明します。

各 Microsoft Azure サブスクリプションでは 1 つ以上のストレージ アカウントを作成できます。各ストレージ アカウントにはプライマリ キー (ストレージ アカウント キー (SAK)) とセカンダリ秘密キー (Shared Access Signature (SAS)) が割り当てられます。そのストレージ アカウントのすべてのデータへのアクセスは、これらのキーによって制御されます。サブスクリプション所有者は、その権限に基づいてアクセス キーの取得や変更をユーザーに許可できます。また、1 つのサブスクリプションでは、複数の管理者がストレージ アカウントを (その他のリソースと共に) 作成および破棄できます。これにより、あるストレージを (ストレージ キーを保持する) 複数のアプリケーションに関連付け、それらのアプリケーションに関連データをフル コントロールで利用できるようにするという一般的なシナリオが成立します。ストレージ アカウントには、適切な資格情報に基づいて Azure サービスやオンプレミスのアプリケーションからアクセスできます。さまざまな要求元に提供される一般的なアクセス パターンを表 1 に示します。

利用者	サブスクリプション	認証の種類
開発者とオペレーター	Microsoft Azure ポータル/SMAPI	フェデレーション ID/管理対象 ID (Microsoft Azure ポータル) 自己署名証明書 (SMAPI) Azure AD と、お客様がサポートする 2 要素認証 (例: Azure Multi-Factor Authentication (MFA))
ロール インスタンス	ストレージ	SAK
外部アプリケーション	ストレージ	SAK
Azure SQL Database	ストレージ	ユーザー名/パスワード、接続文字列

表 1: Azure のお客様のデータとアプリケーションが利用できる認証の種類

### 2.4.1 シングル サインオン (SSO)

管理者は、オンプレミスの AD またはその他のディレクトリ ストアと、Azure AD をフェデレーションすることができます。マイクロソフトは組織のオンプレミス ディレクトリ情報と SSO の同期を推奨しています。これによって、オンプレミス ディレクトリから削除されたユーザーは常に Azure AD から削除されるようになり、適切なアクセス制御を維持できます。また、可用性に優れたセキュリティ トークン サービス (STS) (Active Directory フェデレーション サービス 2.0 (AD FS) など) をオンプレミスにデプロイする必要があります。この STS が、すべてのユーザー ログインの認証フローに組み込まれます。フェデレーションが構成されると、フェデレーション先のドメインに基づく ID を所有するすべての Azure AD ユーザーが、既存の企業ログオン情報を使用して Azure AD サービスの認証を受けられるようになります。フェデレーションによって、すべての Azure アプリケーションにトークンベースの安全な認証と SSO が実現されます。

### 2.4.2 2 要素認証 (2FA)

マイクロソフトは、第 2 の認証要素に電話を使用する多要素認証を Azure の管理に提供しています。また、オンプレミスの STS 統合を活用した、サードパーティの認証ソリューションとの統合もサポートしています。

### 2.4.3 アクセス制御: サブスクリプション

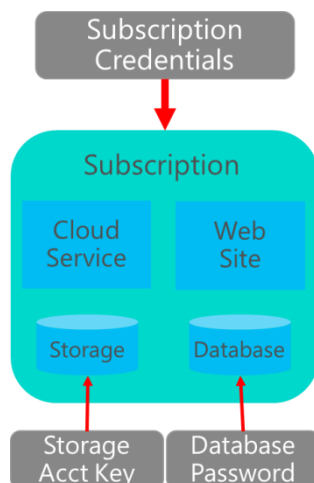
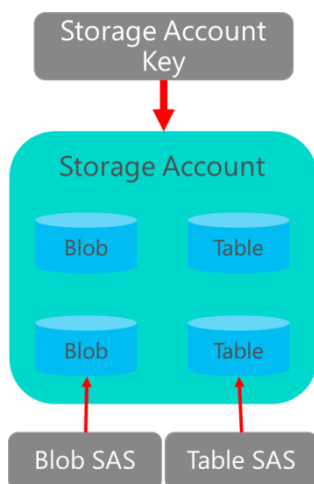


図 3: サブスクリプションへのアクセス

Azure のデータは、種類と場所にかかわらずすべて 1 つのサブスクリプションに関連付けられます (図 3 を参照)。お客様は複数のサブスクリプションを所有でき、それぞれのサブスクリプションに複数のデプロイメント/テナントを設定できます。ただし、サブスクリプションに格納されているすべてのデータに対する完全な権利は、サブスクリプションの作成と管理に使用されているアカウントが保持します。

Azure ポータルへの認証は、Microsoft アカウント (以前の LiveID) または Azure AD 認証 (Azure AD で作成された ID またはオンプレミス ディレクトリとフェデレーションされた ID を使用) によって実行されます。

既定では、VM へのアクセスには、対象の VM のローカルに保存されている資格情報が使用されます (通常はユーザー名とパスワードですが、Linux の場合は SSH 経由の相互証明書認証による認証オプションが許可されます)。VM をオンプレミスの Active Directory ドメインに参加させるなど、別の認証スキームをテナントで選択することもできます。



#### 2.4.4 アクセス制御: ストレージ

Azure Storage のデータ (テーブルを含む) へのアクセスを制御するには、SAS トークンを使用して限定的なアクセス権を付与します。SAS は、SAK で署名されたクエリ テンプレート (URL) によって作成されます。署名された URL を別の (委任された) プロセスに渡し、この別プロセスでクエリの詳細を指定することで、Storage サービスへの要求を行うことができます。SAS によって、ストレージ アカウントの秘密キーを公開することなく、時間に基づくアクセス権をクライアントに付与することができます。主な流れを図 4 に示します。

図 4: ストレージ アカウントへのアクセス

#### 2.4.5 アクセス制御: Azure Tables と SQL Database

Azure Tables は Storage Access Signature を使用した URL ベースのアクセスをサポートします。一方 SQL Database では、ユーザー名とパスワードを含む接続文字列によってデータベースとの接続を確立する必要があります。また、従来の SQL Server データベースで使用されているアクセス制御モデルと同じモデルも引き続き有効です (SQL Server VM の場合、VM がドメインに参加していれば Kerberos トークンを使用した認証も可能です)。

また、セキュリティ資格情報 (ハッシュベース メッセージ認証コード (HMAC) や、SQL のユーザー名とパスワードなど) を、後述する暗号化などの適切な手段によって必ず保護する必要があります。SQL Database および Azure Tables へのアクセスについて表 2 にまとめました。

比較条件	Azure Table ストレージ	SQL Database
認証	<b>Shared Access Signature、ストレージ アカウント キー</b> ユーザー認証に 512 ビットの HMAC キーを使用	<b>SQL 認証</b> ユーザー認証に標準の SQL 認証を使用
ロールベースのアクセス	<b>可能</b> 読み取り、読み取り/書き込み、追加	<b>可能</b> 標準の SQL データベース ロールとアプリケーション ロールに基づく

表 2: Azure SQL Database と Table ストレージでサポートされているアクセスと認証のメカニズム

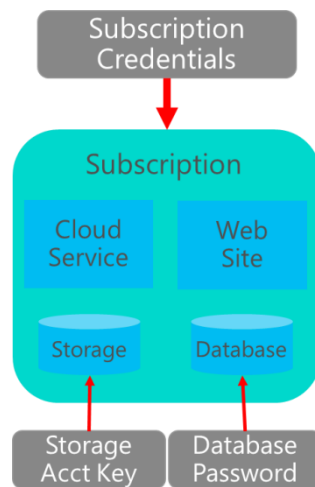


図 5: Azure SQL Database へのアクセス

Azure SQL Database インスタンスに採用されているアクセス セキュリティ モデルは SQL Server のモデルと非常によく似ています (図 5 を参照)。サブスクリプションのアクセス権に従って、完全なアクセス権があればユーザー名とアカウントを作成でき、管理者アクセス権がある場合は、データへのアクセス権 (読み取り、書き込み、読み取り/書き込み) がきめ細かく設定されたその他のユーザー名とパスワードを作成できます。管理者は、サブスクリプション内の SQL Database を作成および破棄することも可能です。

Azure SQL Database は Tabular Data Stream (TDS) プロトコルをサポートしています。これは、従来のデータベースに使用されているデータ アクセス テクノロジ (ADO.Net、Entity Framework など) と同じテクノロジを使用してデータをクエリすることを意味します。インターネットに接している入力ポートには注意が必要です。これは、ポート 1433 をインターネットに開放することがセ

キュリティ上の懸念となるためです。SQL Database インスタンスへのすべてのアクセスは、権限を持つコンピューターを指定するまで Azure SQL Database ファイアウォールによってブロックされます。このファイアウォールは、各要求の送信元の IP アドレスに基づいてアクセス権を付与します。



### 3 データ セキュリティについて

IT プロフェッショナルは、データ セキュリティと暗号化を同等のものとして扱いがちな傾向にあります。暗号化はもちろん大切ですが、暗号化はデータ セキュリティの一要素でしかありません。損失、破損、誤使用の対策をより幅広い視点で考え、ビジネス プロセスの改善によるデータの整合性維持を促進するためには、「いかにデータ セキュリティを実施するか」ではなく「いかにデータの安全性を高めるか」と考えた方がよいのかもしれません。

#### 3.1 リスクとリスク管理

データは、場所や使用方法に関係なく常にリスクにさらされていると考える必要があります。データセンターの物理サーバー ラックにデータを静的に配置せず、公開されたインターネット エンドポイントを使用して共有ストレージにデータを配置するクラウドであればなおさらです。ただし、こうしたリスクのレベルは、ワークロードの種類とデータ保護対策の内容によって変化します。また、リスクの影響はデータの価値によって変わります。

このため、データ自体、データの機密性とリスクのレベル、データが悪用された場合の被害を分類し、組織全体の情報セキュリティ管理ポリシーに基づいてデータをカテゴリに分けることが重要になります。また、データ フローの要件とプロセスを分析して文書化し、リスクと（保護の）強化が必要なポイントを見極めることも必要になります。こうした作業は、各種標準に準拠するための取り組みでも非常に重要な要素です。内部整合性を維持するために Azure が提供しているサポートの内容については、[Microsoft Azure トラスト センターの「コンプライアンス」セクション](#)を参照してください。

##### 3.1.1 データ リスクを理解する

利用するクラウド サービス モデル（パブリック、プライベート、ハイブリッド）に応じてセキュリティの考慮事項は変わりますが、コンピューティング モデル（IaaS、PaaS、SaaS）に応じた考慮事項もあります。Azure Cloud Services では、実行する VM の機能がロールによって定義されます（WIF、WCF、Azure AD によって Azure アプリケーションに実装されるロールベースのアクセス制御と混同しないようにご注意ください）。つまり、これらに含まれるアプリケーションとデータのセキュリティ特性もロールによって定義されます。これらのロールの基本的なアーキテクチャを図 6 に示します。

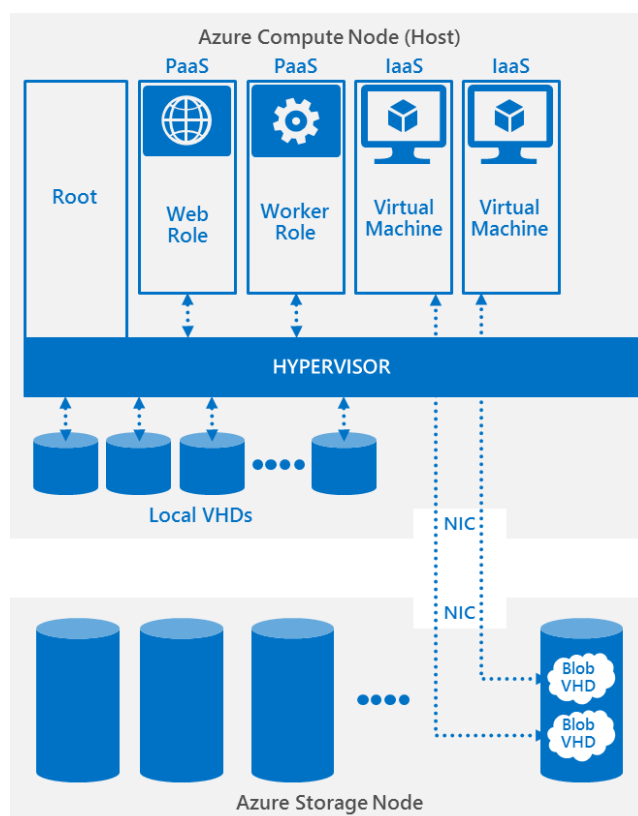




図 6: Azure におけるコンピューティングの種類と、それらに伴って定義されるセキュリティ要件

Cloud Services ロール (PaaS) はアプリケーション ファイルと 1 つの構成によって成り立っています。このロールには以下の 2 種類があります。

- **Web ロール:** 専用のインターネット インフォメーション サービス (IIS) Web サーバーを提供します。この Web サーバーを使用してフロントエンド Web アプリケーションをホストします。
- **Worker ロール:** Worker ロール内にホストされるアプリケーションは、ユーザーの操作や入力とは関係なく、非同期タスク、長時間かかるタスク、常駐タスクを実行できます (IIS は存在していますが無効化されています)。

Virtual Machines (IaaS) は、VHD として Azure にアップロード (または Azure で管理) される Windows イメージまたは Linux イメージであり、サーバー インスタンスに対するより包括的な制御を提供します。ここから導き出されるのは、Azure インフラストラクチャのセキュリティ実現の鍵となる「専門化」という概念です。上述の Web ロールと Worker ロールの説明でもわかるとおり、Azure 内のインフラストラクチャ システムが実行する一連の責務は非常に限定的です。1 つのシステムに割り当てるタスク セットは開発時に定義でき、Virtual Machines または Cloud Services ロールのインスタンスは、この具体的なタスクに基づいて構築されます。

### 3.2 データに対する脅威

Azure のワークロードとアプリケーションはさまざまな形式でデータを利用します。情報に関する情報 (メタデータ) が使用されることもあり、こうした情報に機密の内容が含まれている場合もあります。また、アプリケーションと第三者との通信方法に関する情報から、自社の運用に関する内容が外部に知られてしまう可能性もあります。こうしたデータの構造について表 3 にまとめました。

サービス	データの種類	データ要素
Cloud Services、Storage、ネットワーク	お客様のデータ	お客様のパッケージ (CSPKG ファイル)
	アプリケーションの構成および設計データ	お客様のサービス構成 (CSCFG ファイル) お客様の完全修飾ドメイン名 (FQDN)
	お客様のデータ	お客様の保管中データ
	アクセス制御データ	サブスクリプション管理者とユーザー アカウントのパスワード お客様の証明書 お客様アカウントのストレージ キー Shared Access Signature

Virtual Machines	お客様のデータ	カスタム VM イメージ
	アプリケーションの構成および設計データ	エンドポイント構成
	アクセス制御データ	管理者とユーザー アカウントのパスワード
Virtual Network	メタデータ	VPN ゲートウェイの IP アドレス/範囲
	アクセス制御データ	事前共有キー

表 3: Azure のワークロードが使用するデータの例

クラウド データに対する脅威の多くは、オンプレミス データセンターの場合の脅威と変わりません。オンプレミスにおける以下のような脅威は、仮想環境に移行しても再現されます。

- 損失 (“データ漏えい”) – 不注意、災害、データ盗難などによる
- 改変 (“整合性の侵害”) – 改ざんやデータ破損などによる
- 不正使用 – 不注意または故意による情報開示 (傍受を含む)
- 否認 – 十分な監査ログがない状態でのイベントの発生

### 3.2.1 データへの攻撃の分類

攻撃を実行する手段はオンラインにもオフラインにもあります (表 4 を参照)。オンライン攻撃とは、攻撃者がネットワークに接続して、ネットワーク上で実行中または利用可能な状態にあるリソースを攻撃すること、またはこうした攻撃のために攻撃者が接続を試みることです。オフライン攻撃とは、攻撃者がリソースを物理的に所有して自由に操ることができるときに発生します。

攻撃の種類	特徴
オンライン	<ul style="list-style-type: none"> <li>• VM が実行状態にあるときに発生する可能性がある</li> <li>• 多くの場合、システム管理者の認証情報と承認情報が漏えいしたときに発生する</li> <li>• 通常は論理的攻撃が実行される (URI と盗難により入手したシークレットで BLOB ストレージにアクセスし VHD を盗むなど)</li> </ul>
オフライン	<ul style="list-style-type: none"> <li>• 承認されていない個人による、攻撃対象の場所にあるファイルの削除や物理コンテナの破壊など</li> <li>• 物理的に実行されるという特性がある (ノート PC の盗難、データセンターの物理ハード ドライブの取り外し、バックアップ メディアの盗難など)</li> <li>• 攻撃者が VHD を改変しマルウェアを仕込むなど</li> </ul>

表 4: 2 つの主な攻撃の特徴

### 3.3 Microsoft Azure における既定の保護対策

Microsoft Azure では、お客様の制御が及ばないプラットフォーム層におけるセキュリティ問題を低減するために、既定の情報セキュリティ対策を数多く整備しています。セキュリティ プロセスの自動化、包括的な情報セキュリティ/プライバシー ポリシーの実施、Microsoft Services の管理者に対するセキュリティ/プライバシー関連のトレーニングなど、物理的な方法と論理的な方法の両面からセキュリティ制御を実施しています。

以下に、お客様の作業を必要としない、Azure プラットフォームがネイティブで提供する保護対策を紹介します。Azure では、インフラストラクチャとデータ (メタデータ、ログなどを含む) への脅威からプラットフォームを保護するためにさまざまな対策を講じています。

機能	説明
開発	Microsoft Azure の開発基盤となるテクノロジーは多くの部分が Windows Server と共通しています。Microsoft Azure 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) と Operational Security Assurance (OSA) が定める要件と手順に従って開発、テスト、デプロイされています。また、クラウドのセキュリティとプライバシーに関する考慮事項もこれらの標準に従って対処されています。SDL と OSA の手法では、設計段階に脅威モデルを適用する、開発ベストプラクティスに準拠する、コードにセキュリティ標準を組み込む、さまざまな必須のツールを用いてデプロイメントの前とサービス運用中にテストと検証を実施するなど、Azure サービスの開発プロセスと運用におけるセキュリティ脅威への対策を包括的に提供しています。
プラットフォームの暗号化	後述の「 <a href="#">プラットフォームの暗号化</a> 」セクションを参照してください。
ネットワークのセキュリティと分離	<p>Azure では、<a href="#">ネットワークを分散し仮想化することによって</a>、それぞれのお客様のプライベート ネットワークのトラフィックと、その他のお客様によるトラフィックを分離しています。お客様は、1 件のサブスクリプションに複数の分離されたプライベート ネットワークを設定し、それぞれのネットワークでファイアウォール、負荷分散、ネットワーク アドレス変換を実行できます。</p> <ul style="list-style-type: none"><li>• <b>デプロイメント ネットワーク:</b> それぞれのデプロイメントはネットワーク レベルで相互に分離されています。あるデプロイメントの中に存在する複数の VM は、プライベート IP アドレスを使用して相互に通信できます。</li><li>• <b>仮想ネットワーク:</b> それぞれの Virtual Network は相互に分離されています。同じ Virtual Network に (同じサブスクリプションに含まれる) 複数のデプロイメントを配置でき、各デプロイメントはプライベート IP アドレスを使用して相互に通信できます。</li></ul> <p>既定では、プライベート ネットワークの Virtual Machines はデプロイメント外</p>

	<p>部からのトラフィックを受信しません。管理者は、入力エンドポイントを定義することによって、分離されたデプロイメントのネットワーク外からのトラフィックを受信する仮想マシン上のポートを指定できます。これによって、インターネットや Azure に存在する別のデプロイメントや利用者からのトラフィックを受信できるようになります。</p>
<b>シークレットとシークレットの格納</b>	<p>SSL 証明書、秘密キー、RDP パスワード、SAK などのお客様のシークレットは、SMAPI または Azure ポータル経由でアップロードできます (いずれの場合も TLS/SSL で保護されたチャネルが使用されます)。Azure にアップロードされたお客様のシークレットは暗号化された形式で保存されます。</p>
<b>ログのセキュリティ</b>	<p>Azure では、セキュリティ関連イベントに対する信頼性の高い認証済みのログ記録を実行します。改ざん対策が組み込まれたこのログ記録から監査証跡を生成することもできます。ログには、Azure インフラストラクチャの VM や Azure AD におけるセキュリティ イベント ログなどのシステム情報も記録されます。</p>
<b>侵入テスト</b>	<p>マイクロソフトでは「レッド チーム」と呼ばれる手法を用いて Microsoft Azure インフラストラクチャへの侵入テストを定期的に行っています。これは、実際に運用されているインフラストラクチャに対して、悪意のある攻撃者と同じ技術とメカニズムでシステムをテストする作業です。このテストの目的は、稼働環境の (現実に発生し得る) 脆弱性、構成エラー、セキュリティの欠落を一定のプロセスを通して特定することと、セキュリティの検出、分析、応答に関するプロセスとテクノロジーをテストすることです。</p>
<b>セキュリティ強化されたワークステーション</b>	<p>Azure Operations チームでは、セキュリティ強化された管理者用ワークステーションを使用して Microsoft Azure インフラストラクチャのコンポーネントとお客様の環境に接続し、これらを管理しています (サポート インシデント対応時)。これらのマシンでは署名済みのコードと最低限の数のアプリケーションが実行され、運用環境も論理的に分離されています。さらに、指定された Microsoft 資格情報の使用と 2 要素認証の実施が義務付けられ、アクセスは監視、記録され、ログは厳重に保管されます。スパイ型フィッシングを始めとするさまざまな攻撃の標的にされやすい Outlook や Office などのアプリケーションは、セキュリティ強化されたワークステーション内の VM に隔離されて実行されます。</p>
<b>個人</b>	<p>Microsoft Azure のスタッフには、マイクロソフトとの雇用契約に基づくセキュリティとプライバシーに関するトレーニングを毎年受講することが義務付けられています。トレーニングでは、安全な運用、データの安全な取り扱い手順、各種の行動規範などの分野について学習します。</p>
<b>監査</b>	<p>マイクロソフトは厳格な手順に従って Azure を運用、管理、監視しています。さらに、正式な資格を有する第三者機関によって、ISO、SOC、FISMA、FedRAMP などの枠組みに基づく包括的な監査が実施されており、データ保護要</p>

---

件を満たしていることが証明された場合は認定証が発行されています。

---

**一時的なアクセス** お客様の情報に対する保護強化のため、マイクロソフトの担当者がお客様のデータ (VM、ファイル、キー、データベース、AD テナント、ログなど) への永続的なアクセス権を保持することは、ポリシーによって禁止されています。ただし、お客様が明示的にアクセス権を付与した場合を除きます。緊急の問題解決が必要な場合は、Microsoft Azure の管理者またはサポート担当者に、お客様のデータに対する一時的なアクセス権が与えられます。問題が解決した場合や依頼があった場合、このアクセス権はすぐに無効化されます。

**メディアの廃棄** お客様のデータが Azure のデータセンター施設外に持ち出されないようにするための物理的な管理を実施しています。たとえば、これまでお客様のストレージに使用されていたディスク ドライブを (ハードウェア障害などで) 取り外す場合などは、交換/修理のためにメーカーに発送する前に、ディスクのデータが確実に消去されます。ディスクの欠陥によってデータを完全に消去できない場合は、[NIST 800-88 \(英語\)](#) のガイドラインに従ってディスクが廃棄されます。ドライブの利用を計画的に停止する場合も同じ手順が実行されます。

**データの削除** 十分なデータのライフサイクルを確保しているにもかかわらず、必要以上に機密性の保持を求められる場合があります。Azure Storage のサブシステムでは、削除操作が呼び出されると、お客様のデータは使用できなくなります。削除を含むすべてのストレージ操作は、即座に同じ状態になるよう設計されています。削除操作が成功すると、関連するデータ項目へのすべての参照が削除され、Azure Storage API からアクセスすることはできなくなります。初期化されていないデータを Azure Storage インターフェイスから読み取ることはできないため、同じお客様や別のお客様によって上書きされる前に、削除済みのデータが読み取られることはありません。削除済みデータのコピーはすべてガベージ コレクションの対象となります。物理的なビット要素は、関連するストレージ ブロックが他のデータの保存のために再利用されると上書きされます。これは、標準的なコンピューターのハード ドライブで通常行われている処理です。

**データセンターのセキュリティ** Azure データセンターでは、[物理的な手段によるデータ漏えい防止](#)を目的に、サーバーのケージやラックの施錠、スマートカード リーダー、警備員による年中無休 (24 時間 365 日) の監視など、ISO に準拠したさまざまな安全対策を実施しています。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。

---

### 3.3.1 Azure AD におけるデータ セキュリティ

Azure AD に保存されている重要な ID 情報は、以下の手段によって保護されます。

- **転送中データ:** お客様に公開されるすべての Web サービスは SSL/TLS によって保護されます。ディレクトリ ストアに送信される、またはディレクトリ ストア内で転送される (データセンター内およびデータセンター間の) すべての LDAP およびパーティション/レプリケーション トラフィックは署名されます。
- **保管中データ:** 保管中の場合、ディレクトリに保存されているシークレット (対称キー、秘密の非対称キー、パスワード) は、Distributed Key Manager (DKM) (英語) を使用して暗号化されます。

Microsoft Azure AD は、別のテナントの ID が発行したすべての操作を既定で禁止しています。別のテナントの ID には、必要に応じて、テナントの管理者によってディレクトリへのアクセス権を明示的に付与できます。

テナント コンテナという概念は、ポータルから永続ストレージに至るすべての層のあらゆるディレクトリ サービスに深く浸透しています。境界を確立することで、特定のテナントを対象としたクエリが別のテナントのディレクトリ データを返すようなことがなくなります。すべてのフロントエンド (Azure AD Sync、PowerShell、Graph) は、データの格納と取得に内部ディレクトリ サービス API (DSAPI) を使用します。この API が認証層を呼び出すことによって、要求されたデータがデータを要求したユーザーに対して許可されます。認証層では以下の 3 段階の確認が実行されます。

1. Microsoft Azure AD に対するユーザー アクセスの有効性
2. このテナントのデータに対するユーザー アクセスの有効性
3. 要求された種類のデータ アクセスについて、このテナントにおけるユーザーのロールを認証できるかどうか

Azure AD のデータに対するアクセスには、セキュリティ トークン サービス (STS) によるユーザー認証が必要です。認証された後は、認証トークンと複製されたパーティションからユーザー プリンシパル名 (UPN) が読み取られ、ユーザーのドメインに対応するコンテナが判断されます。認証システムでは、ユーザーの存在、有効化の状態、ロールに関する情報に基づいて、対象のテナントへのアクセス要求について、当該セッションの当該ユーザーを認証できるかどうか判断されます。認証済みの操作 (ユーザーの作成、パスワードのリセットなど) を実行すると監査証跡が作成されます。この監査証跡は、テナントの管理者によるコンプライアンスの管理や調査に使用されます。

### 3.4 プラットフォームの暗号化

Microsoft Azure のデータ保護機能では、組み込みのサービス、コンポーネント、構成によって内部のデータとトラフィックに暗号化を適用することができます。これらは、お客様情報に対するセキュリティを強化し、業界規制に基づくデータのガバナンスとコンプライアンスを支援するために欠かせない機能です。

Azure プラットフォームではこうしたメカニズムの多くが既定で有効化されていますが、いくつかはお客様の管理者による構成が必要です (IPsec VPN など)。また、サービス構成ファイルの使用やア

アプリケーション コンポーネントからの直接呼び出しによって、VM の起動時に選択的に起動できるものもあります。

Azure では、対称キーと非対称キーの両方を使用した暗号化を実装し、データの暗号化と機密性保持を実現しています。

- ソフトウェアベースの AES-256 による対称暗号化/暗号化解除
- 2048 ビット以上の非対称キー
- SHA-256 以上のセキュア ハッシュ

### 3.4.1 転送中の暗号化

Microsoft Azure では仮想ネットワークを使用して、テナントのトラフィックをテナント間で相互に分離しています。ここでは、ホストレベルおよびゲストレベルのファイアウォール、IP パケットフィルタリング、ポートのブロック、HTTPS エンドポイントなどの手段が使用されていますが、インフラストラクチャ間や、インフラストラクチャとお客様 (オンプレミス) 間など、Azure 内部の通信の大部分も暗号化されています。

Azure データセンター内の通信では、マイクロソフトのネットワーク管理によって、別の VM の IP アドレスが偽装または傍受されることはありません。Azure Storage や SQL Database へのアクセス、または Cloud Services への接続には TLS/SSL が使用されます。この場合、TLS/SSL 証明書の取得とテナント インフラストラクチャへの証明書のデプロイはお客様の管理者が実施する必要があります。

#### 3.4.1.1 VM 間

同じデプロイメント内の Virtual Machines 間や、1 つのデプロイメント内のテナント間の Microsoft Azure Virtual Network を経由したデータ トラフィックは、HTTPS、SSL/TLS などの暗号化通信プロトコルによって保護できます。

お客様の Cloud Services 環境から送信されるデータはインターネット接続の利用を考慮する必要があるため、HTTPS や VPN などによって適切に保護することが推奨されます。

#### 3.4.1.2 お客様とクラウド間

お客様のクラウド環境を出入りするデータの移動は、Azure で提供されるさまざまなオプションによって保護されます。こうした移動は、運用管理、データの移動、キーのプロビジョニングなどが含まれます。お客様は必要に応じて TLS/SSL を構成することで Virtual Network に多層防御を実現できます。Azure ポータルや System Management API (SMAPI) へのアクセスでは TLS/SSL が必須です。



データ量が少ない場合、テナント環境に対する IPsec VPN などの暗号化接続を使用して Azure Virtual Network に直接接続できます。大きいデータ セットは、新機能 ExpressRoute などの分離された高速チャネルを利用して移動できます。ExpressRoute を利用している場合、TLS/SSL またはその他のプロトコルを使用してアプリケーション レベルでデータを暗号化し、セキュリティを強化できます。

また、Azure ポータルからの Azure Storage の対話では、すべてのトランザクションが HTTPS 経由で発生します。Azure Storage と Azure SQL Database との対話では Storage REST API over HTTPS も使用することができます。Azure SQL Database にデータを入力する際は、コピーされる前に情報を暗号化できます。データが使用され、Azure SQL Database コンピューティング ノードのメモリに配置されるとデータの暗号化が解除されますが、それまではデータの暗号化された状態が続くことに注意してください。

## 3.5 データの削除

サブスクリプション全体、ストレージ、Virtual Machines、データベースなど、破壊するデータ オブジェクトの種類によってデータの破壊手法は異なります。Microsoft Azure のようなマルチテナント環境では、データが他の利用者のデータに「漏えい」しないように、また削除したデータに他の利用者 (多くの場合、データを過去に所有していた利用者も含む) がアクセスできないようにするために十分な注意を払っています。

### 3.5.1 サブスクリプション

サブスクリプションがキャンセルまたは終了された場合、マイクロソフトはデータ抽出のための期間としてお客様のデータを 90 日間保持します。お客様のデータは、この保持期間の終了から 90 日以内にすべて削除されます。つまり、キャンセルまたは終了から 180 日以内にすべてのデータが削除されます。

既存のサブスクリプションのストレージ アカウントを削除した場合 (またはサブスクリプションの削除の期限に達した場合) も、誤って削除した場合に復元できるよう、実際にはそれからさらに 2 週間にわたって保持されます。ストレージ アカウントが最終的に削除されると、あるいは BLOB や Table のデータがストレージ アカウントの削除とは別に削除されると、データは完全に利用できなくなります。

**メモ:** ストレージ データをもっと早く復元不可能にしたい場合は、ストレージ アカウントやサブスクリプションを削除する前にテーブルや BLOB を個別に削除します。



### 3.5.2 Microsoft Azure Storage

Azure Storage ではディスクへの書き込みはすべてシーケンシャルに実行されます。これによってディスクの「シーク」回数を最小化できますが、書き込みのたびにオブジェクトへのポインターを更新する必要があります (新しいバージョンのポインターもシーケンシャルに書き込まれます)。ただし、このシステムでは、ディスクに機密情報が記録されている場合、他のデータを上書きすることでその情報を消去できるという確証はありません。元のデータがディスクに残ったまま、新しい値がシーケンシャルに書き込まれます。ポインターが更新されるので、削除した値を見つける手段がなくなるということです。

ディスクが満杯になると、古いデータの削除によって解放されたディスク領域に新しいログが書き込まれます。ディスク セクターからログ ファイルを直接割り当てる代わりに、New Technology File System (NTFS) が稼働するファイル システムにログ ファイルが作成されます。Azure Storage ノードで実行されているバックグラウンドのスレッドは一番古いログ ファイルをチェックし、一番古いログ ファイルから参照されているブロックを最新のログ ファイルにコピー (およびすべてのポインターを更新) して領域を解放します。そして最も古いログ ファイルを削除します。ディスクには 2 種類の空き領域があります。1 つは NTFS が空き領域だと認識しており、このプールから新しいログ ファイルを割り当てる領域であり、もう 1 つはポインターが存在しないため Azure Storage が空き領域だと認識しているログ ファイル内の領域です。

### 3.5.3 Microsoft Azure Virtual Machines

Virtual Machines は Microsoft Azure Storage に BLOB として保存されているので、上記で説明した削除時のルールが当てはまります。ただし、仮想化では、データが再び書き込まれるまでディスクの特定箇所を別の利用者 (または同じ利用者) が読み出せないようになっており、データ漏えいのおそれは少なくなります。新しい仮想ディスクが VM 用に作成されると、VM ではゼロ埋めされているように見えますが、データ バッファの明示的なゼロ埋めは、仮想ディスクに書き込みをする前に読み取りを行った場合に発生します。仮想マシンのインスタンスの再初期化は、新しいハードウェアに移動した場合と同じ結果になります。

### 3.5.4 Azure SQL Database

Azure SQL Database では、削除されたデータには削除のマークが設定されます。データベース全体の削除は、データベースのコンテンツ全体を削除したのと同じです。SQL Database の実装は、SQL Database API の使用を除き、ストレージへのアクセスを一切禁止することでユーザー データの漏えいを防いでいます。この API を使用してデータの読み取り、書き込み、削除を行うことが可能ですが、自分が以前に書き込んだものではないデータを読み取ることはできません。

### 3.6 使用中データに対するコンピューティングのセキュリティ

Azure の基本的な設計手法に、従来の「多層防御」の概念をさらに拡大した「侵害を想定した対応」によってデータを保護するという方法論があります。つまり、マイクロソフトでは、何らかのシステムや手順には障害が発生するものであるという前提でシステムと手順を設計しています。Azure は、共有インフラストラクチャ上のマルチテナント サービスとして完全に基礎から構築されています。その目的は、各層における設計と実装 (英語) の最適なバランスを実現しながら、お客様向けのサービスや内部の管理サービスを問わず、お客様の情報をスタックのあらゆる層で保護することです。

この方針をさらに強化するのが、Azure で広く取り入れられている「コンパートメント化」という概念です。たとえば、Azure データセンターのすべてのホスト ノード (お客様の VM のホストに使用されるマシン) は拠点として機能しています。お客様とホスト間の分離境界は Azure Hyper-V によって維持されています。トラブルシューティングのためにシステムにログインするオペレーターは、特定のホストの資格情報だけを取得します。それ以外のホストの資格情報は入手せず、入手した資格情報も短期間で有効期限が切れます。

Azure プラットフォームでは、シークレットの管理が設計の最も基本的な要素として位置付けられています。インフラストラクチャによって構築されたロールは、必要なジョブの実行に必要なシークレットだけが付与され、プロビジョニングされます。お客様は、この機能を応用して、Azure を使用して秘密キーを管理できます (お客様のキーは暗号化された形式で保存、転送され、Azure のシークレットストアで保持されます)。シークレットは Azure インフラストラクチャの機能によってマシンにプッシュされ、キーは Azure 内で定期的に移動します。

### 3.7 物理的なデータ セキュリティ

「データを物理的に盗むことができるか」というのは、ホスティング サービスを利用しているお客様に共通した疑問です。確実な答えを出すことは難しいですが、ひとつ言えるのは、このような大胆な行動にはさまざまな難問があるということです。

- **データセンターへの侵入:** マイクロソフトでは、年中無休 (24 時間 365 日) のビデオ監視、訓練を積んだ警備員、施錠されたサーバー ラック (コンピューティング、ストレージ、ネットワーク用ハードウェアを格納)、スマートカード、生体認証など、数々のセキュリティ/コンプライアンス監査に認められた厳格な運用体制とプロセスを備え、許可のない立ち入りを防止しています。許可された訪問者もすべて記録に残されます。
- **ディスク ドライブの持ち出し:** 侵入者は、データが置かれているデータセンター、建物、フロア、部屋、サーバー ラックを特定しないと、狙った企業のデータに到達できません。さらに Azure Storage のデータはストライピングによって細かく分割されてディスクに書き込まれています。つまりお客様のデータの多くは複数のディスクにまたがって保存されているため (データベースなどの大規模なファイルは複数のドライブにまたがっている場合もあります)、侵入者は、取り外すべきディスク格納装置とドライブを特定しなければなりません。

ディスクを適当に取り出したとしても、メディアを読み出すには Azure Storage の秘密キーが必要です。

- **リムーバブル USB メディアへのデータ コピー:** ディスクの盗難と同様に、リムーバブル メディアを使うとしても、目的のデータを格納するストレージ デバイスを特定する必要があります。また、Azure ノードは物理的に保護されているだけでなく、ヘッドレス運用、ハードウェア パスワード、各種のセキュリティ強化技術でコードのローカル実行を防止しています。さらに、サーバー クラスタは光学メディアをサポートしておらず、物理ポートはアクセスがブロックされています。メディアを接続しようとするセキュリティ 警告が生成されます。
- **ネットワーク スニффイング** (無線、有線、リモート タップによる物理的な接続): Azure 内部のルーターはインターネット接続されたエンドポイントには接続していません。また、厳格に制限されたモードで実行することで、未認証の接続をすべてブロックしています。Azure で稼働しているネットワーク システムやインフラストラクチャにはワイヤレス アクセスできないため、モバイル デバイスが悪用される脅威は事実上存在しません。また、Azure は、マイクロソフトの Global Foundation Services (GFS) グループによって ISO 27001 準拠のデータセンターで運用され、セキュリティ管理を通じて物理ネットワーク アクセス ポートがロックダウンされています。

物理セキュリティの詳細については、[Microsoft GFS の Web サイト \(英語\)](#) を参照してください。

## 4 お客様が構成可能な保護対策

このセクションでは、Azure のデータ保護における重要な概念のうち、お客様自身が制御できるものについて説明します。

- 暗号化対策 (暗号化と暗号化解除を、データの保存処理、アプリケーション内、ネットワーク上で使用)
- キー管理 (プロビジョニング、ライフサイクル管理、セキュリティ/保護)
- 認証、承認、アクセス制御 (前述)

これらの機能を組み合わせることによって、標準や規制に準拠した基盤を構築し、お客様の重要なデータの整合性、プライバシー、セキュリティを常に制御することができます。これによって、攻撃行為に自動で対策を実施する防御策を確立し、効果のある対策を確保できます。

使用するデータ保護メカニズム (図 7 を参照) は、対象となるワークロードやデータ コンテナにとって適切でなければなりません。特に以下の点に注意してください。

- データ セキュリティは、暗号化/暗号化解除、キー管理 (キー ライフサイクル)、キーの保護によって構成されるが、暗号化ソリューションがこれらの 3 つすべてに対応しているか。
- 暗号化ソリューションは、オンラインとオフラインの攻撃を防御できるか。
- 最も適したデータ/コンテナ層に暗号化が施されているか。
- 発生するワークロードの種類に関係なく暗号化が適用されるか。
- 暗号化されたデータを、許可された担当者が必要に応じて復元できるか。

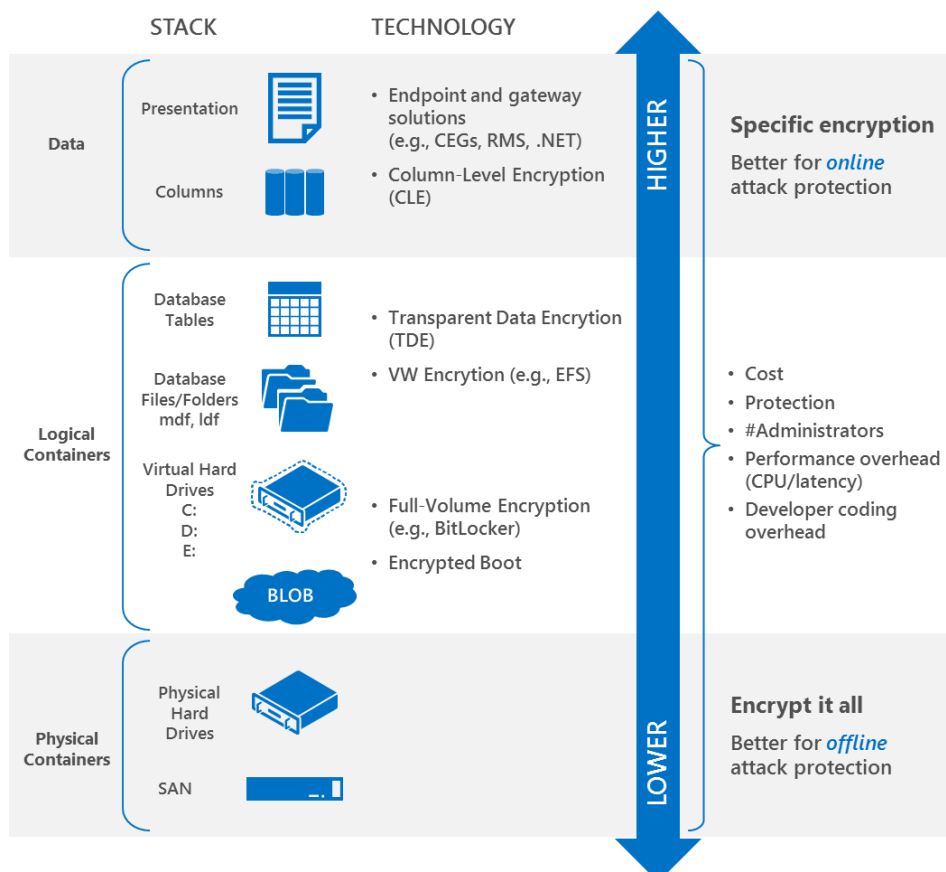


図 7: 一般的なデータ暗号化メカニズム

## 4.1 ボリューム レベルの暗号化

一般的には、暗号化対策は、暗号化/暗号化解除、キー管理 (キー ライフサイクルなど)、キー セキュリティで構成されます。お客様は、Windows オペレーティング システムが提供する暗号化ルーチン (.NET CAPI、CNG) によってデータを暗号化してから Azure に保存できます。同じメカニズムは Azure VM 内でも使用することが可能です。

暗号化/暗号化解除が必要な領域 (クラウド、オンプレミス、アプリケーション内、クライアントなど) は、維持すべき制御のレベル、許容可能な (パフォーマンス面、管理面などの) コスト、維持すべき機密性、リスク発生の可能性に応じて変化します。表 5 に一般的なオプションをまとめました。

層	暗号化サポート	キー管理	詳細	
透過的なデータ	アプリケーション	.NET Cryptography API	お客様が管理	<a href="#">.NET の暗号化に関するドキュメント</a>
		RMS SDK によるデータ暗号化	お客様が管理 (オンプレミスの AD RMS サービスまたは Azure RMS を使用)	<a href="#">RMS SDK に関するドキュメント (英語)</a>
	プラットフォーム	Azure IAAS VM で実行される SQL Server の <a href="#">SQL TDE/CLE</a>	お客様が管理	<a href="#">SQL TDE/CLE に関するドキュメント</a>
		プライマリ、バックアップ、アーカイブを <a href="#">StorSimple</a> が提供	お客様が管理	<a href="#">詳細情報</a>
	システム	EFS、BitLocker によるデータ ボリュームとブート ボリュームのサポート	お客様が管理	<a href="#">BitLocker コマンドライン ツール (機械翻訳)</a>
	その他	ドライブのデータのインポート/エクスポートを BitLocker が保護	お客様が管理	<a href="#">インポート/エクスポート手順に関するブログ (英語)</a>

表 5: Microsoft Azure の主なサービスとコンテナで利用できる暗号化対策メカニズム

### 4.1.1 BitLocker ドライブ暗号化

Azure Virtual Machines は通常ストレージ ディスク (VHD) に関連付けられ、VHD は Azure Storage に格納されています。Azure Storage では、データを細かく分割し、分割されたまとまりをストライピングによって複数の物理ディスクに配置することで、ディスクの障害に対する保護対策

を実現しています。ドライブ暗号化のような追加の保護を実施することで、(VHD で使用される) SAK の悪用などの脅威を抑制することができます。ディスクを暗号化すれば、不正なユーザーがキーを入手して Azure Storage から VHD を取得しようとしても、VHD が暗号化されているためディスクを読み取ることはできません。

Windows では、データ ボリュームとブート ボリュームに対応した BitLocker がアプリケーションに対して透過的に実行されるため、ディスクに対して完全に透過的な暗号化が可能です。BitLocker ドライブ暗号化 (BDE) は、

「manage-bde」などのコマンド ライン ツールを使用して Azure VM および VHD にも同様に実行できます。

BitLocker では、パスワードや証明書などのさまざまなプロテクターを通じてボリュームを暗号化します (図 8 を参照)。

また、Azure PowerShell で「manage-bde」を使用して暗号化コマンドをリモートで実行したり、スタートアップ スクリプトで暗号化を制御したりすることも可能です。BitLocker の自動ロック解除機能では、対話型のセッションを省略してボリュームのロックを自動的に解除できます。

キーは、ハードウェア セキュリティ モジュール (HSM) など、オンプレミスのキー管理サービスによって保護できます。Azure VM では BitLocker を使用してブート ボリュームも暗号化できます。詳細については、BitLocker コマンドライン ツール「manage-bde」に関する[こちらの MSDN 記事 \(機械翻訳\)](#) などの BitLocker 関連ドキュメントを参照してください。

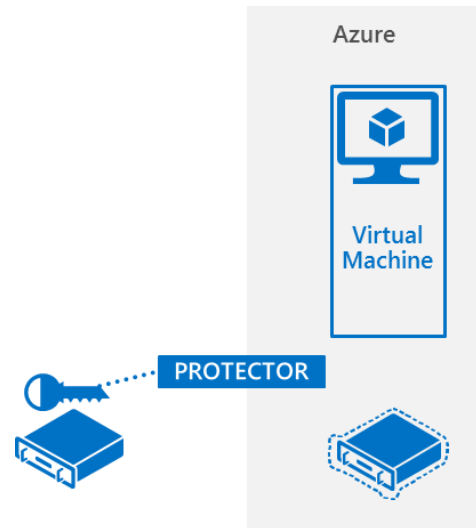


図 8: BitLocker ドライブ暗号化

#### 4.1.2 ドライブ暗号化 – パートナー

ボリューム レベルの暗号化や暗号化関連のポリシー管理には、Trend Micro を始めとするパートナーのソリューションを利用できます。これらのパートナー ソリューションはサードパーティの HSM と統合することができます。また、Windows と Linux 両方の VM に対応したソリューションです。暗号化は OS やアプリケーションに対して透過的に実行されるため、アプリケーションの変更は必要ありません。

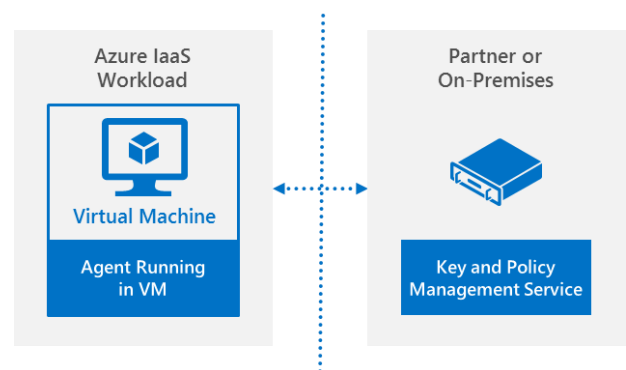


図 9: サードパーティ製 HSM の使用

ソリューションの実装方法はさまざまですが、一般的には、エージェントが OS スタックのディスクドライバとファイル システム ドライバの間に常駐してデータを暗号化します。暗号化はインスタンスの停止後も有効です (図 9 を参照)。

キーの管理には、HSM やその他のキー管理サービスなどクラウド外のシステムも利用できます。

#### 4.1.3 キーの管理とセキュリティ

キーそのものが適切に保護されていないければ、暗号化や認証を実施してもセキュリティは強化されません。安全性と信頼性を高水準で維持し、管理負担を削減するには適切なキー管理が必要です。このため、キーのライフサイクル管理は重要な IT セキュリティ タスクとして認識されています。

暗号化キー管理はお客様が実装する必要があります。お客様は、お客様固有のソリューションに最適な、安全なアーキテクチャを構築することでデータ暗号化を完全に制御できます。

#### 4.1.4 サブスクリプションとサービス証明書

Azure プラットフォームでは、Windows セキュリティ モデルに組み込まれたわかりやすいキー管理手法を基盤に、証明書によるデータ保護機能を提供しています (Virtual Machines と Cloud Services の両方で .NET、CAPI、CNG などの Windows の暗号化手法を利用できます)。

お客様のアプリケーションやサービスの保護に使用される代表的な証明書がサービス証明書です。これは、エンドポイント通信のセキュリティ保護に使用される一般的な SSL 証明書です (お客様がアップロードします)。サービス証明書は、公開キー暗号化標準 (PKCS) によるデータ暗号化や、ストレージ アクセス キーのようなシークレット構成情報の暗号化など、その他の目的にも利用することができます。

Azure のサブスクリプションには論理証明書ストアが関連付けられています。サービス固有の証明書をここから自動でデプロイしたり、お客様が独自の証明書をここにアップロードすることができます。証明書ストアはホストされているすべてのサービスから独立しているため、現在証明書がサービスに使用されているかどうかに関係なく証明書を格納できます。これらの証明書および Azure にアップロードされる証明書は暗号化された形式で保存されます。

また Azure では、管理者用のパスを使用して証明書と秘密キーをアップロードできます。ただし秘密キーを取得することはできません。証明書、秘密キー、RDP パスワード、SAK などのお客様のシークレットは、SMAPI と Representational State Transfer (REST) ベースのプロトコル、または Azure ポータルと SSL を介して転送されます。証明書と秘密キーは Azure のファブリック コントローラーに暗号化された形式で保存されます。お客様の証明書とお客様の VM の間に参照を作成することで、エクスポート不可能な形式で証明書を自動でインストールできます。

証明書はサービスと切り離して管理できるだけでなく、複数の異なるユーザーによって管理できます。たとえば、IT マネージャーが以前 Azure のシークレット ストアにアップロードした証明書を参照するサービス パッケージを、別の開発者がアップロードできます。同じ IT マネージャーがこれらの証明書を引き続き管理し、更新できますが、その際サービスを停止したり新しいサービス パッケージをインストールする必要はありません。



## 4.2 Azure Virtual Machines で実行される SQL Server の暗号化

オンプレミスの SQL Server 2008 以降のインストールでは、SQL Server の透過的なデータ暗号化 (TDE) を使用してストレージを暗号化できます。SQL Server 構成によって設定され、アプリケーションの変更を必要としない TDE によって、ストレージ デバイスの物理的な盗難や、ファイル システムにアクセスされデータベース ファイルが公開されるような論理的侵害への保護対策が実現されます。SQL Server の TDE の詳細については[こちらの記事](#)をご覧ください。

SQL Server の列レベルの暗号化 (CLE) では、よりきめ細かい暗号化が可能です。データの暗号化はそのデータが使用されるまで解除されません (TDE の場合は、ストレージのデータベース全体が暗号化され、アクセスされるとデータベースの各ページが完全に暗号化解除されます)。つまり、ページがメモリに読み込まれている状態でも、SQL Server の処理が実行されるまで機密データは暗号化されています。CLE の場合、テーブルに書き込まれたデータを暗号化および暗号化解除するには、呼び出し元のアプリケーションの変更が必要です。また、暗号化された列のクエリ最適化に影響が及ぶため、暗号化によるパフォーマンス低下についても注意が必要です。このため CLE は、暗号化対象のデータ量が少ない場合や、独自の設計要件が存在する場合に使用されるのが一般的です。SQL Server CLE の詳細については[こちらの記事 \(英語\)](#)をご覧ください。

また、データの暗号化に使用されるキーを安全に保護しない限り、暗号化の効果を得ることはできません。SQL Server の既定のシナリオでは、データベースの暗号化解除に必要なすべてのキーはマスター データベースに保持されます。マスター データベースがユーザー データベースと同じストレージ デバイス上にあると、このストレージ デバイス 1 台が公開されることによってデータ流出の可能性が発生します。この場合、SQL Server が提供する拡張キー管理 (EKM) プロバイダー アーキテクチャを利用することで、キーの安全性確保と格納をサーバー外部のキー管理サービス (KMS) にリダイレクトできます。

ハードウェア セキュリティ モジュール (HSM) とは、暗号化キーの安全性確保を目的に設計されたハードウェア デバイスです。キー管理用の HSM と SQL Server 向けの EKM プロバイダーは、さまざまな商用ベンダーから入手できます。

### 4.2.1 クラウドにおける実装

アプリケーションをクラウドに移行した場合も、SQL Server を実行している VM で同じ TDE/CLE の機能を活用して、オンプレミス デプロイメントと同じようにデータベースを暗号化できます。これによって、クラウド ストレージに保存されている保管中データと潜在的な攻撃者との間にセキュリティ バリアが構築されます。攻撃者がデータベース サーバーの基盤となる VHD へのアクセスを試みても、あるいはストレージ デバイスへの物理的なアクセスが成功した場合も、データが暗号化されているためそれ以上侵入することはできません。

データベースのマスター キーから派生した証明書を使用せず、HSM 暗号化プロバイダーを指定した場合、SQL Server は HSM の非対称キーを使用してデータベース暗号化キー (DEK) を暗号化します (図 10 を参照)。



お客様がハイブリッド ネットワークを利用している (サイト間 VPN または Azure ExpressRoute で Azure Virtual Network (VNET) と オンプレミス ネットワークが 接続されている) 場合、キー管理タスクをオンプレミスの HSM またはキー管理サービス (KMS) にリダイレクトすることで、クラウド外のインフラストラクチャでキーを適切に管理できます。この場合にも、HSM ベンダーが SQL Server 向けに提供している拡張キー管理 (EKM) プロバイダーを利用できます。

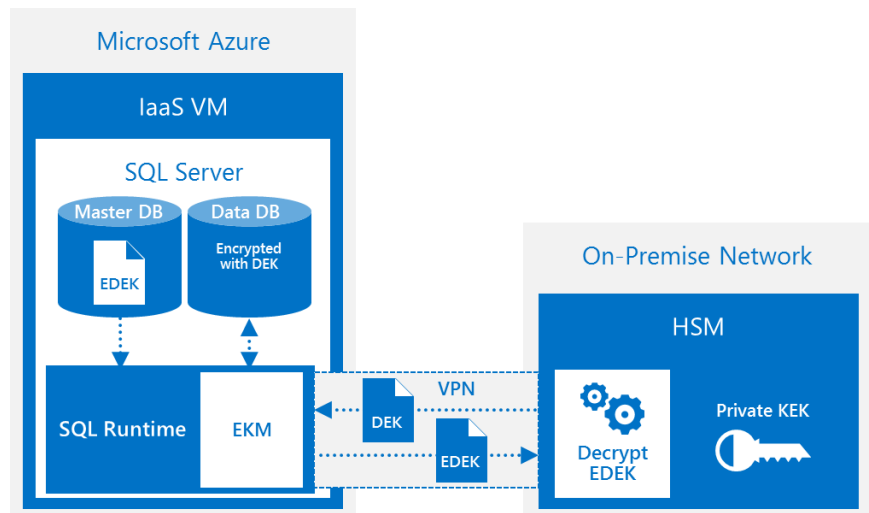


図 10: SQL Server の暗号化におけるキーの流れ

開始された SQL Server インスタンスが、このような方法で暗号化されたデータベースをマウントする場合、暗号化されたデータ暗号化キー (EDEK) の暗号化解除を EKM、HSM の順で要求します。返された DEK はメモリに格納され、以降のデータベースの暗号化解除に使用されます。

この方法によって、マスター データベース ファイルとユーザー データベース ファイルの両方に不正にアクセスされたとしても、HSM に対する直接のアクセス権を持つ人物以外には、データベースの暗号化は解除されません。

マイクロソフトは、Azure VM で SQL Server 2008 および 2012 Enterprise インスタンスを実行し、このシナリオをテストしました。使用された VM は、ExpressRoute を利用してマイクロソフトのオンプレミス ネットワークに参加している Virtual Network に配置され、企業ドメインに参加していました。SQL Server インスタンスは、Thales の EKM モジュールを利用して、マイクロソフトのコーポレート ネットワークにある Thales の HSM にキー管理をリダイレクトしました。ネットワーク アクセス可能な自社の HSM を同様のシナリオでテストしているかどうかは、お客様が HSM ベンダーに直接問い合わせる必要があります。

SQL Server CLE とオンプレミスの HSM によるキー管理を使用する場合、パフォーマンスに対する考慮事項が増えます。これは、SQL Server TDE よりもキー要求が発生することが原因です (SQL 列の暗号化または暗号化解除のたびに発生します)。要求が発生するたびに、オンプレミスの HSM からキーをリモートで取得する必要があります。お客様はこのことを念頭に設計してください。Azure VM からの HSM アクセスをセキュリティ保護する最適な方法については、HSM ベンダーに問い合わせる必要があります。

## 4.3 Azure の Rights Management サービス

Microsoft Rights Management サービス (RMS) は、開発者向け SDK、追加設定不要のインフォメーション ワーカー向けアプリケーション、IT 管理者向けの管理ツールを含む、包括的なツールキットです。RMS を利用することで、企業では以下が可能になります。

- データの暗号化と暗号化解除
- 暗号化キーの管理、配布、追跡
- キーの受信者と、暗号化されたデータに許可される操作の制御

データの多くは複数のアプリケーション、コンピューター、デバイス、ユーザー、組織で共有され、送信者から受信者へのデータ フローの多くには複数のホップがあります。RMS モデルでは、暗号化とアクセス ポリシーは常にデータと共に移動します (RMS クライアント SDK は Windows、iOS、Android、および OS X 向けに提供されています)。

### 4.3.1 RMS の基礎: RMS コンポーネントが連携するしくみ

すべての RMS フローには、1 台の RMS サーバーと 1 つ以上の (RMS SDK を使用する) RMS 対応アプリケーションがあります。図 11 に示したフローでは、青色のユーザー (発行者) が緑色のユーザー (利用者または受信者) とデータを共有しています。「ユーザー」には、ID を持つすべての個人やサービスが該当します。

最初に発行者が RMS サーバーを設定します。設定では、サーバー ライセンサー証明書 (SLC) キーと呼ばれる一意の RSA キー ペアを、RMS サーバーが組織ごとに生成します (または発行者がインポートします)。

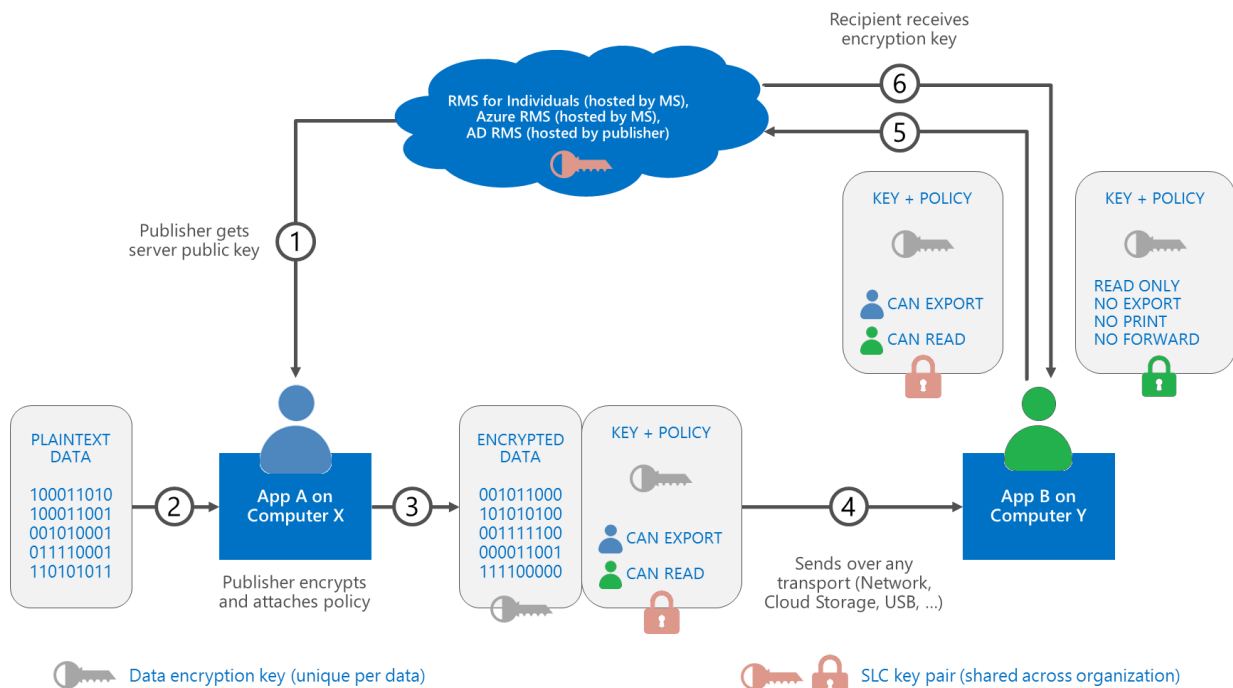


図 11: RMS におけるキーとデータの流れ

次に、発行者が RMS 対応アプリケーション (図のアプリケーション A) を使用します。

- アプリケーション A が、RMS SDK (図には表示されていません) を使用して新しいデータ暗号化キー (灰色) を生成し、生成されたキーでデータを暗号化します (手順 2 および 3)。
- アプリケーション A が使用ポリシー (暗号化解除可能なユーザー、データに許可される操作) を指定します。
- RMS SDK が RMS サーバーから SLC 公開キーを取得します (手順 1)。このキーを使用して、データ暗号化キーと使用ポリシーを暗号化します。この組み合わせは発行ライセンスと呼ばれます。

次に、暗号化されたデータと発行ライセンスを、対象の受信者/利用者に発行者が送信します (手順 4)。データは暗号化されて移動するため、転送方法や「ホップ」の回数は自由です。

最後に受信者がアプリケーション B を使用してデータの暗号化を解除します。

- アプリケーション B が RMS SDK を使用して RMS サーバーの場所を探して認証を受け、暗号化された発行ライセンスを提示します (手順 5)。
- 発行ライセンスによって受信者によるデータの暗号化解除が許可されると、データ暗号化キーとユーザー (緑色) 固有の権限が RMS サーバーによって返されます (手順 6)。
- アプリケーション B が RMS SDK を使用してデータの暗号化を解除します。使用ポリシーは、このアプリケーションと RMS SDK によって保持されます (この手順はユーザーが信頼済みであることが前提です)。

注目されるのは、RMS サーバーはキー交換のブローカーとしてのみ機能するため、データに関知しないという点です。発行者から利用者へのデータとキーは異なる経路で移動するため、データとキーを組み合わせられるのは発行者と利用者以外にいません。

RMS の動作の詳細については、<http://blogs.technet.com/b/rms/archive/2012/04/16/licenses-and-certificates-and-how-ad-rms-protects-and-consumes-documents.aspx> (英語) を参照してください。

#### 4.3.2 RMS サーバーの選択肢

マイクロソフトは RMS サーバーの実装方法として以下の 3 つを提供しています。

- Microsoft Rights Management for Individuals と呼ばれる無料のホスティング サービス。初めて実装するユーザーに適した最も簡単なオプションです。<https://portal.aadrm.com> でサインアップできます。
- 組織向けの管理機能が追加されたプレミアム ホスティング サービス。Microsoft Rights Management サービスまたは Azure RMS と呼ばれます。前提条件、購入方法、試用方法については <http://technet.microsoft.com/ja-jp/library/dn655136.aspx> を参照してください。
- Active Directory Rights Management サービスと呼ばれるオンプレミスの実装方法。<http://technet.microsoft.com/ja-jp/windowsserver/dd448611.aspx> を参照してください。

#### 4.3.3 開発者向け RMS SDK

開発者は RMS SDK を使用して、アプリケーション内でデータの暗号化と暗号化解除を実行できます。RMS SDK を使用すると、メモリのバイト単位で、またはファイル全体を一度に暗号化または暗号化解除できます。

RMS SDK によるファイル全体の暗号化では、一般的なファイルの種類 (PDF、Microsoft Office 形式、JPG、TXT) には事前定義済みの形式が使用され、その他の種類には汎用コンテナ形式 (PFILE) が使用されます。これによって、これらのファイルを既存の RMS アプリケーションで開けるようになります。

バイト単位で暗号化する場合は、暗号化されたデータの格納場所、格納する形式、発行ライセンスの格納場所を指定する必要があります。また、データを利用 (暗号化解除) するアプリケーションが、この構成を認識できることが必要です。

Azure アプリケーション開発者に適した 2 つのコード サンプルが用意されています。1 つは Cloud Services で RMS を使用してデータを暗号化した後に Azure Storage に格納するものです。もう 1 つは、Web アプリケーションがユーザーに配布するデータを RMS で暗号化するというものです。これらのサンプルは <http://go.microsoft.com/fwlink/?LinkId=398638> (英語) で公開されています。

このソリューションを正常に稼働させるには、アプリケーションを使用する全員が RMS サーバーを利用する必要があります。

RMS SDK の詳細な使用方法については、[http://msdn.microsoft.com/en-us/library/hh552972\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/hh552972(v=vs.85).aspx) (英語) を参照してください。

#### 4.3.4 RMS 対応のアプリケーション

アプリケーションを新しく開発しなくても、処理の実行には既存のアプリケーションを利用できます。以下のアプリケーションは RMS に対応しています。

- メール: Outlook (Windows)、NitroDesk Touchdown (各種デバイス)。Exchange Server 環境では Outlook Web Access も利用可能 (Exchange 管理者が IRM を有効にしている場合)
- Office ドキュメント: Word、PowerPoint、および Excel
- PDF: FoxIt PDF Reader および NitroPDF Reader
- その他:<https://portal.aadrm.com/Home/Download> で公開されている RMS アプリケーションを利用可能

#### 4.3.5 組織における RMS

組織で利用する RMS サーバーをデプロイする場合や、RMS サーバー構成をカスタマイズする場合は、Azure RMS またはオンプレミスの AD RMS が推奨されます。これらのバージョンでは、無料で入手できる RMS for Individuals よりも充実した機能が IT 管理者に提供されます。以下のような機能を利用できます。

- 組織における SLC キーの管理方法をカスタマイズする
- データ暗号化キーの受信者を監視する
- 特定のデータ利用ポリシーの適用を、テンプレートを使用して従業員に要求する
- RMS で保護されたデータを Exchange Server と SharePoint Server で発行および利用できるようにする

詳細については、<http://technet.microsoft.com/en-us/dn175751> (英語) を参照してください。

#### 4.3.6 RMS によるキー管理

RMS では、SLC キーの保護オプションやデータ暗号化キーの配布オプションを提供しています。AD RMS では、互換性のある HSM を使用して SLC キーを管理できます。

Azure RMS は BYOK (Bring Your Own Key) にも対応しています。BYOK モードでは、オンプレミスの HSM からマイクロソフトの HSM に SLC キーをアップロードします。キーは HSM で常時保護され、使用ログも参照できます。これらを組み合わせることによって、キーの適切な利用に対す

る信頼性を高めることができます。こうした機能の詳細については、  
<http://technet.microsoft.com/ja-jp/library/dn440580.aspx> を参照してください。

RMS の認証情報は Active Directory または Azure Active Directory に関連付けられます。関連付けられた AD または Azure AD からユーザー (またはアプリケーション プリンシパル) が削除されると、そのユーザー (またはアプリケーション) は、以前はキー受信が許可されていても、その RMS サーバーからデータ暗号化キーを受信できなくなります。

#### 4.3.7 キー配布の追跡

AD RMS と Azure RMS によるログはほぼリアルタイムで入手できるため、データの特定部分のデータ暗号化キーへのアクセスを取得したユーザーを、管理者が常に監視できます。

詳細については、AD RMS の場合は [http://technet.microsoft.com/en-us/library/dd772686\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd772686(v=WS.10).aspx) (英語) を、Azure RMS の場合は <http://blogs.technet.com/b/rms/archive/2014/01/07/enabling-and-using-logging-in-azure-rms.aspx> (英語) を参照してください。

## 5 冗長化とバックアップによるデータ保護

Azure は、データ可用性を維持するためのメカニズムを数多く提供しています。Azure Storage ではデータが複数のドライブに複製されます。Virtual Machines で実行される SQL Server などのアプリケーションでは可用性セットを作成できます。また、負荷分散とフェールオーバーにはオートスケール機能や Traffic Manager を利用できます (このホワイト ペーパーでは説明しませんが、これによって DoS 攻撃からインフラストラクチャを保護できます)。

### 5.1 Azure Storage

Microsoft Azure Storage サービスは、お客様の BLOB、Table、Queue の各データの地理レプリケーションを実行します。データは同じリージョン内の数百キロ離れた 2 拠点間で複製されます (例: 米国北部と南部、北ヨーロッパと西ヨーロッパ、東アジアと東南アジア)。データの地理レプリケーションによって、データセンターの大規模な災害や一時的なハードウェア障害に対する耐久性が実現されます。ユーザーのストレージ アカウントにはデータ レプリケーションのオプションが 3 種類提供されます。

- **ローカル冗長ストレージ (LRS):** 同じデータセンター内でデータが 3 回複製されます。BLOB、Queue、Table にデータを書き込むと、書き込み操作が 3 つのレプリカすべてに対して同時に実行されます。LRS によって一般的なハードウェア障害からデータを保護できます。
- **地理冗長ストレージ (GRS):** データが同じリージョン内で 3 回複製されると共に、プライマリ拠点から数百キロ離れた場所にあるセカンダリ拠点への複製が非同期で実行されます。GRS では、各リージョンに 3 つずつ、合計 6 個のデータ コピー (レプリカ) が保持されます。大規模な障害や災害が発生しプライマリ拠点のデータを復元できない場合、セカンダリ拠点へのフェールオーバーをマイクロソフトが実行します。ローカル冗長ストレージよりも GRS のほうがお勧めです。
- **読み取りアクセス地理冗長ストレージ (RA-GRS):** 上記の地理冗長ストレージの機能がすべて提供されることに加えて、プライマリ拠点が利用できなくなった場合に、セカンダリ拠点のデータに読み取り専用でアクセスできます。耐久性と最大の可用性が必要な場合は、読み取りアクセス地理冗長ストレージを推奨します。

### 5.2 Azure Backup

Azure Backup は System Center 2012 Data Protection Manager (DPM) のディスクベースの保護機能と連携します。オンライン保護を有効にすると、ディスク ベースのレプリカがオンラインの場所にバックアップされます。オンプレミス データセンターのサーバー (またはクラウド サービス) のバックアップは暗号化されて送信され、AES-256 で暗号化されて Azure に格納されます (図



12 を参照)。Windows ファイル システムと DPM によるバックアップも、同様に自動で暗号化されます。オプションで Windows Server ファイル分類インフラストラクチャ (FCI) (英語) を使用すると、Azure RMS などの権限管理における機密ファイルを特定することによって、さらに保護を追加できます。

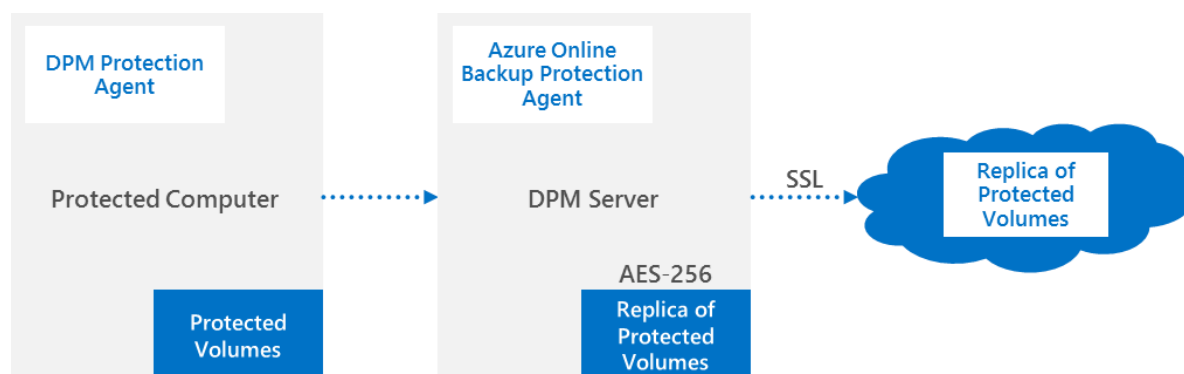


図 12: Azure における暗号化されたバックアップ データの流れ

### 5.3 StorSimple クラウド統合ストレージ (CiS)

StorSimple のデータ保護プロセスは 2 つの部分で構成され、ローカル スナップショットとクラウド スナップショットの両方が提供されます。ローカルとクラウドのスナップショットは、データのバックアップおよび復元のために使用されます。このバックアップ方法では、クラウド統合ストレージ モデル内の場所に関係なく、バックアップ データの可用性が維持され必要な回復ポイントが関連付けられます。これによってデータのセキュリティと管理に関する IT 部門の懸念を解消することができます。

データは複数のレベルで保護されます。各ファイルは複数のブロックに分割され、各ブロックで重複除去が実行されるため、変更されたブロックだけが格納されます。各データ ブロックはクラウドに送信されて AES 256 ビットで暗号化され、圧縮された後に格納されます (秘密キーはクラウドではなくクライアント側に保存されます)。

セキュリティを維持するために、CiS システムがクラウドで送信および格納するすべての Microsoft ボリューム シャドウ コピー サービス (VSS) データに暗号化が適用されます。これらのデータには必ず、データの整合性を保証する手段として、SHA-256 ハッシュが適用されます。



## 6 プライバシーと説明責任

マイクロソフトは、個人情報のセキュリティを保護することを確約します。マイクロソフトのオンライン サービス提供チームは、セキュリティに関するさまざまなテクノロジーと手順を駆使して、不正なアクセス、利用、または開示から顧客情報を保護しています。また、マイクロソフトのソフトウェア開発チームは、マイクロソフトのセキュリティ開発ライフサイクル (SDL) と Operational Security Assurance (OSA) が定める PD3+C の原則を社内のあらゆる開発と運用の作業に適用しています。

- **プライバシー バイ デザイン** – マイクロソフトでは、プライバシー バイ デザインの原則をアプリケーションの開発、リリース、メンテナンスの各段階にさまざまな形で組み込むことにより、お客様から収集したデータが特定の目的以外に使用されないことを保証すると共に、十分な情報に基づいて判断できるようにするための適切な情報をお客様に提供しています。収集するデータが分類され、高い機密性があると判断された場合は、転送中、保管中、またはその両方のデータを暗号化するなど、追加のセキュリティ対策を実施します。
- **プライバシー バイ デフォルト** – マイクロソフトの製品とサービスでは、常にお客様の許可を得てから機密データを収集または転送します。許可が得られた後も、アクセス制御リスト (ACL) などの手段と ID 認証メカニズムを組み合わせることで機密データを保護します。
- **プライバシー イン デプロイメント** – マイクロソフトでは、組織のお客様にプライバシー保護のメカニズムを公開することによって、こうしたお客様によるユーザー向けのプライバシー/セキュリティ ポリシー策定をサポートしています。
- **コミュニケーション** – マイクロソフトでは、プライバシー ポリシー、ホワイト ペーパー、その他のプライバシー関連ドキュメントの公開を通して、お客様であるかどうかにかかわらず、ユーザーとの幅広い関係構築に取り組んでいます。

## 7 まとめ

情報のセキュリティとプライバシーを維持するには、オンプレミス データセンターと Azure 環境の両方にまたがる長期的な視点に立ったプロセスが必要です。実装を検討していただく必要がある主な機能を以下の表にまとめました。

シナリオ	軽減される脅威	暗号化テクノロジー	詳細情報
Virtual Machines (IaaS) を実行し、機密データを保存する VHD が Azure Storage に格納され、コンピューティング インスタンス (Windows ワークロード) に接続されている	<ul style="list-style-type: none"> <li>• ディスクの損失</li> <li>• VHD の格納先のストレージ アカウント キーの損失</li> </ul>	<ul style="list-style-type: none"> <li>• BitLocker ドライブ暗号化</li> <li>• ISV パートナーによるボリュームレベルの暗号化</li> </ul>	<a href="http://technet.microsoft.com/ja-jp/library/cc732774.aspx">http://technet.microsoft.com/ja-jp/library/cc732774.aspx</a>
Virtual Machines を実行し、機密データを保存する VHD が Azure Storage に格納され、コンピューティング インスタンス (Linux ワークロード) に接続されている		<ul style="list-style-type: none"> <li>• ISV パートナーによるボリュームレベルの暗号化</li> </ul>	<a href="http://azure.microsoft.com/ja-jp/gallery/store/#all">http://azure.microsoft.com/ja-jp/gallery/store/#all</a>
Virtual Machines と SQL Server データベースを実行する		<ul style="list-style-type: none"> <li>• SQL の透過的なデータ暗号化</li> <li>• SQL の列レベルの暗号化</li> </ul>	<a href="http://technet.microsoft.com/ja-jp/library/bb934049.aspx">http://technet.microsoft.com/ja-jp/library/bb934049.aspx</a> <a href="http://technet.microsoft.com/en-us/library/cc278098(v=SQL.100).aspx#_Toc1893846882">http://technet.microsoft.com/en-us/library/cc278098(v=SQL.100).aspx#_Toc1893846882</a> (英語)
Virtual Machines または Cloud Services を実行し、データを Azure Storage に格納し、Storage Client Library/REST API を使用する	<ul style="list-style-type: none"> <li>• ディスクの損失</li> </ul>	<ul style="list-style-type: none"> <li>• .NET crypto API やその他の言語によるアプリケーション レベルの暗号化</li> </ul>	<a href="http://msdn.microsoft.com/en-us/library/dn720893(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/dn720893(v=vs.85).aspx</a> (英語)

ワークロードをオンプレミスで実行し、データを Azure Storage に格納し、Storage Client Library/REST API を使用する	<ul style="list-style-type: none"> <li>• ディスクの損失</li> <li>• クラウド サービス プロバイダーの管理者</li> </ul>	<ul style="list-style-type: none"> <li>• .NET crypto API やその他の言語によるアプリケーションレベルの暗号化</li> </ul>	<a href="http://blogs.msdn.com/b/windowsazurestorage/archive/2012/11/06/windows-azure-storage-client-library-2-0-tables-deep-dive.aspx">http://blogs.msdn.com/b/windowsazurestorage/archive/2012/11/06/windows-azure-storage-client-library-2-0-tables-deep-dive.aspx</a> (英語)
ワークロードを拡張するため、オンプレミスストレージのバックアップ/アーカイブ/追加用として Azure を使用する	<ul style="list-style-type: none"> <li>• クラウドに対するインターネット上の攻撃</li> </ul>	<ul style="list-style-type: none"> <li>• Azure Backup</li> <li>• StorSimple</li> </ul>	<a href="http://blogs.msdn.com/b/windowsazure/archive/2011/04/22/storing-encrypted-data-in-windows-azure.aspx">http://blogs.msdn.com/b/windowsazure/archive/2011/04/22/storing-encrypted-data-in-windows-azure.aspx</a> (英語)

## 8 参考資料および関連資料

ここでは、マイクロソフトが提供する Microsoft Azure 関連のサービスの一般的な情報、および本ドキュメントで言及した特定の項目に関する情報を入手するためのリソースを記載しています。

- Microsoft Azure ホーム – Microsoft Azure 関連のサービスの一般的な情報と各種リンク
  - <http://azure.microsoft.com/>
- Microsoft Azure ドキュメント センター – 開発者向けのガイダンスと情報
  - <http://msdn.microsoft.com/ja-jp/windowsazure/default.aspx>
- Microsoft Azure トラスト センター
  - <http://azure.microsoft.com/ja-jp/support/trust-center/>
- Microsoft セキュリティ レスポンス センター (Microsoft Azure を始めとするマイクロソフト製品のセキュリティ脆弱性について報告できます)
  - <http://www.microsoft.com/ja-jp/security/msrc/default.aspx>
  - または、[secure@microsoft.com](mailto:secure@microsoft.com)

### 8.1 参考情報

- Azure のセキュリティ概要に関するトレーニング モジュール (英語)
  - <http://www.microsoftvirtualacademy.com/tracks/windows-azure-security-overview>
- Azure のセキュリティ レビュー (英語)
  - <http://blogs.msdn.com/b/buckwoody/archive/2011/08/02/windows-azure-security-review.aspx>
- Crypto Primer: 公開/秘密キー、署名、証明書を理解する (英語)
  - <http://blogs.msdn.com/b/plankytronixx/archive/2010/10/23/crypto-primer-understanding-encryption-public-private-key-signatures-and-certificates.aspx>
- Field Note: Microsoft Azure アプリケーションで証明書ベースの暗号化を使用する (英語)
  - <http://blogs.msdn.com/b/windowsazure/archive/2011/09/07/field-note-using-certificate-based-encryption-in-windows-azure-applications.aspx>
- Azure のセキュリティに関するガイダンス
  - <http://azure.microsoft.com/ja-jp/documentation/articles/best-practices-security/>
- Microsoft Azure のセキュリティに関するベスト プラクティス – パート 7: ヒント、ツール、コーディングに関するベスト プラクティス (英語)
  - <http://blogs.msdn.com/b/usisvde/archive/2012/03/15/windows-azure-security-best-practices-part-7-tips-tools-coding-best-practices.aspx>
- すべてのデータを既定で暗号化する必要性について (英語)
  - <http://blogs.msdn.com/b/buckwoody/archive/2011/08/09/should-all-data-be-encrypted-by-default.aspx>
- Crypto Primer: SSL のしくみ (英語)

- <http://blogs.msdn.com/b/plankytronixx/archive/2010/10/28/crypto-primer-how-does-ssl-work.aspx>
- Microsoft Azure のデータ セキュリティ (データ クレンジングおよびデータの漏えい)
  - <http://blogs.msdn.com/b/windowsazurej/archive/2014/05/15/blog-microsoft-azure-data-security-data-cleansing-and-leakage.aspx>
- Microsoft Azure における暗号化サービスとデータ セキュリティ
  - <http://msdn.microsoft.com/ja-jp/magazine/ee291586.aspx>
- Microsoft Rights Management サービス (RMS) (英語)
  - <http://www.microsoft.com/rms>
- 可用性が高く、セキュリティで保護されたクラウド ソリューションの展開 (英語)
  - <http://Aka.ms/avail>
- Azure のセキュリティに関する 10 の事実 (英語)
  - <http://technet.microsoft.com/en-us/cloud/gg663906.aspx>
- Microsoft Azure セキュリティの基礎 (英語)
  - <http://technet.microsoft.com/en-us/gg621084.aspx>
- Microsoft Azure SQL Database と SQL Server のパフォーマンスとスケーラビリティの比較
  - <http://msdn.microsoft.com/ja-jp/library/azure/jj879332.aspx>
- Azure Table ストレージと Microsoft Azure SQL Database の比較
  - <http://msdn.microsoft.com/ja-jp/library/azure/jj553018.aspx>
- データ シリーズ: Microsoft Azure のドライブ、ディスク、イメージについて
  - <http://blogs.msdn.com/b/windowsazurej/archive/2012/07/10/data-series-exploring-windows-azure-drives-disks-and-images.aspx>
- Azure ストレージ アカウントへのアクセスの認証
  - <http://msdn.microsoft.com/ja-jp/library/hh225339.aspx>
- 方法: WIF および ACS を使用して要求対応の ASP.NET アプリケーションで役割ベースのアクセス管理 (RBAC) を実装する
  - <http://msdn.microsoft.com/ja-jp/library/gg185914.aspx>
- Azure Virtual Machines の一時ドライブを理解する (英語)
  - <http://blogs.msdn.com/b/wats/archive/2013/12/07/understanding-the-temporary-drive-on-windows-azure-virtual-machines.aspx>
- RMS ブート キャンプ (英語)
  - <http://curah.microsoft.com/56313/boot-camp-for-windows-azure-rights-management-rms>