認証取得済みクラウドサービスの
評価に関する調査

2017 年 1 月 31 日

株式会社三菱総合研究所

本書について

本書は、日本マイクロソフト株式会社からの委託により、株式会社三菱総合研究所が、日本マイクロソフト株式会社が提供するクラウドサービス「Microsoft Azure」を評価した結果をレポートするものです。Microsoft Azure は、JASA – クラウドセキュリティ推進協議会によるクラウド情報セキュリティ監査制度「CS ゴールドマーク」を日本で最初に取得したクラウドサービスです。また、米国公認会計士協会（AICPA）が定めた内部統制基準である「SOC2」の認証も取得しており、クラウドサービスにおける情報セキュリティ対策がグローバルレベルで第三者から認証されています。

しかし、CS ゴールドマーク及び SOC2 の認証で要求される管理事項は、情報セキュリティに関連するリスク分析に基づいた管理施策であり、その内容は多岐にわたる上、理解するには技術的な知識・背景が要求される場合も少なくないことから、その有用性が十分に評価・認識されないケースがあるのも事実です。

そこで、CS ゴールドマーク及び SOC2 の管理策のうち、特徴的な観点を抽出し、Microsoft Azure における取り組みや、それにより軽減されるリスク・脅威について、本レポートにて解説しました。理解の促進のため、第三者認証を取得しているクラウドサービスである Microsoft Azure を、一般的なデータセンター（DC）にサーバを設置し利用する方式（一般的にはホスティングやハウジングと呼ばれる手法です）と、利用者の事業所内に設置するオンプレミス（設置型）方式の 2 つのパターンを、セキュリティの観点から比較するというアプローチで記述しています。

CS ゴールドマーク、SOC（Service Organization Control）とは

CS マークとは、特定非営利活動法人　日本セキュリティ監査協会(JASA)の下部組織である、クラウドセキュリティ推進協議会(JCISPA)が実施しているクラウド情報セキュリティ監査制度で発行する認証マークです。CS マークには、クラウド事業者の自主監査の結果として発行される「CS シルバーマーク」と、自主監査の結果を外部の監査人により評価した結果として発行される「CS ゴールドマーク」があります。監査は、JCISPA が定める「クラウド情報セキュリティ管理基準」に基づいて行われます。CS ゴールドマークを取得したクラウドサービスは、一定水準の情報セキュリティ対策が実施されていることを、第三者によって認められていることになります。

SOC とは、米国公認会計士協会(AICPA)が定めたクラウドサービス事業者の内部統制に関する保証報告書のことで、「SOC 報告書」（Reporting on Controls at a Service Organization)とも呼ばれます。SOC には、クラウドサービス事業者の財務諸表等の監査を目的とした「SOC1」、セキュリティ・可用性・機密保持等の内部統制の監査を目的とした「SOC2」、SOC2 の内容を不特定の利用者に公開することを目的とした「SOC3」があります。SOC2 を取得したクラウドサービスは、一定水準の内部統制が行われていることを、第三者によって認められていることになります。

- Column -

パブリッククラウド環境にて提供するアプリケーションやサービスが CS ゴールドマークを取得する場合、対象となるアプリケーション・サービスが CS ゴールドマークの要件を満たすことに加え、それらを稼動させるインフラ環境も同様に CS ゴールドマークの要件を満たすことが求められます。既に CS ゴールドマークを取得しているマイクロソフト社の Microsoft Azure をインフラ環境として活用することにより、サービスの提供事業者はアプリケーション・サービスの部分に特化して、CS ゴールドマークの要件を満たすことに注力できるようになります。

比較検討のモデル

前述のとおり、本書では認証取得済みクラウドサービス（Microsoft Azure）を、一般的なデータセンターに設置する方式及び利用者の事業所内に設置するオンプレミス方式と比較し、その論点を整理しています。

本書では、それぞれの比較対象について、以下の表に示すとおり、モデルを定義しています。

表　比較検討のモデルの定義

モデル	定義	想定利用者
オンプレミス	サーバハードウェアを利用者が独自に調達・構築し、自社内のサーバルームに設置した上で、ハードウェア・ OS ・アプリケーションのメンテナンスを自社で実施する形式	国内の 中小企業
一般的な データセンター	サーバハードウェアを利用者が独自に調達・構築し、データセンター（DC）に設置した上で、ハードウェア・ OS ・アプリケーションのメンテナンスを自社で実施する形式	国内の 大企業
認証取得済み クラウドサービス	Microsoft Azure の仮想マシン（IaaS）を利用して仮想マシンをサービスとして調達し、OS ・アプリケーションのメンテナンスを自社で実施する形式。特に、CS Mark Gold や SOC2 の認証を取得し、適切な運用管理を行っている。	国内の 企業全般

いずれの方式であっても、IT システムを構築し運用することは可能ですが、モデルによってシステムの運用責任の範囲と主体が異なります。

たとえば、オンプレミスの場合はサーバやネットワークなどの機器を設置するスペースやサーバラック、電気・空調などのファシリティ、外部と通信するインターネット回線などを独自で構築した上で、サーバやネットワーク機器の設置から故障時の障害対応や、サーバ上のソフトウェアの保守まで、利用者が責任を持って運用しなければなりません。この運用には物理的・技術的なセキュリティ対策の導入、及び維持管理も含まれます。

一方で認証取得済みクラウドサービスの場合、利用者はサーバやネットワーク機器を購入することなくサービスとして利用することができるため、そのサービスの提供に必要な運用業務は全てクラウドサービスの事業者が責任を持ちます。利用者は OS・アプリケーションの部分にのみ責任を持てばよいことになります。

それぞれのモデルにおいて、利用者が自社で運用しなければならない領域と、サービスとして提供される領域について以下の図のとおり整理しています。

図　比較検討のモデルとサービス利用範囲

セキュリティ評価のポイント

本書では、認証済みクラウドサービスと、オンプレミス及び一般的なデータセンターをセキュリティの観点から比較する上で、6 つの観点を選定しています。これらの観点は、IT システム及びそこで管理されるデータを安全に管理し、安定的に利用できる環境を整えるという意味において、どれも欠かせないものです。

① システムを停止させないインフラ環境
② 運用者の特権管理
③ 入退室の管理
④ セキュリティインシデント監視
⑤ 脆弱性管理と対策
⑥ 暗号鍵の管理

セキュリティは、「機密性（Confidentiality）」「完全性（Integrity）」「可用性（Availability）」の 3 つの要素から構成されます。機密性とは「許可された者だけが情報にアクセスできるようにすること」、完全性とは「保有する情報が正確であり、完全である状態を保持すること」、可用性とは「許可された者が必要なときにいつでも情報にアクセスできるようにすること」を指しています。

一般的にセキュリティについて、正当な権限を有さない外部の人間が不正に情報を取得することを防止するもの、と解釈されることが多いですが、この解釈には機密性の要素しか含まれていません。情報システムにおけるセキュリティを考える上で、完全性及び可用性に関する観点を欠かすことはできません。上記の 6 つの要素は、この機密性・完全性・可用性を担保するうえで重要なポイントとなっています。

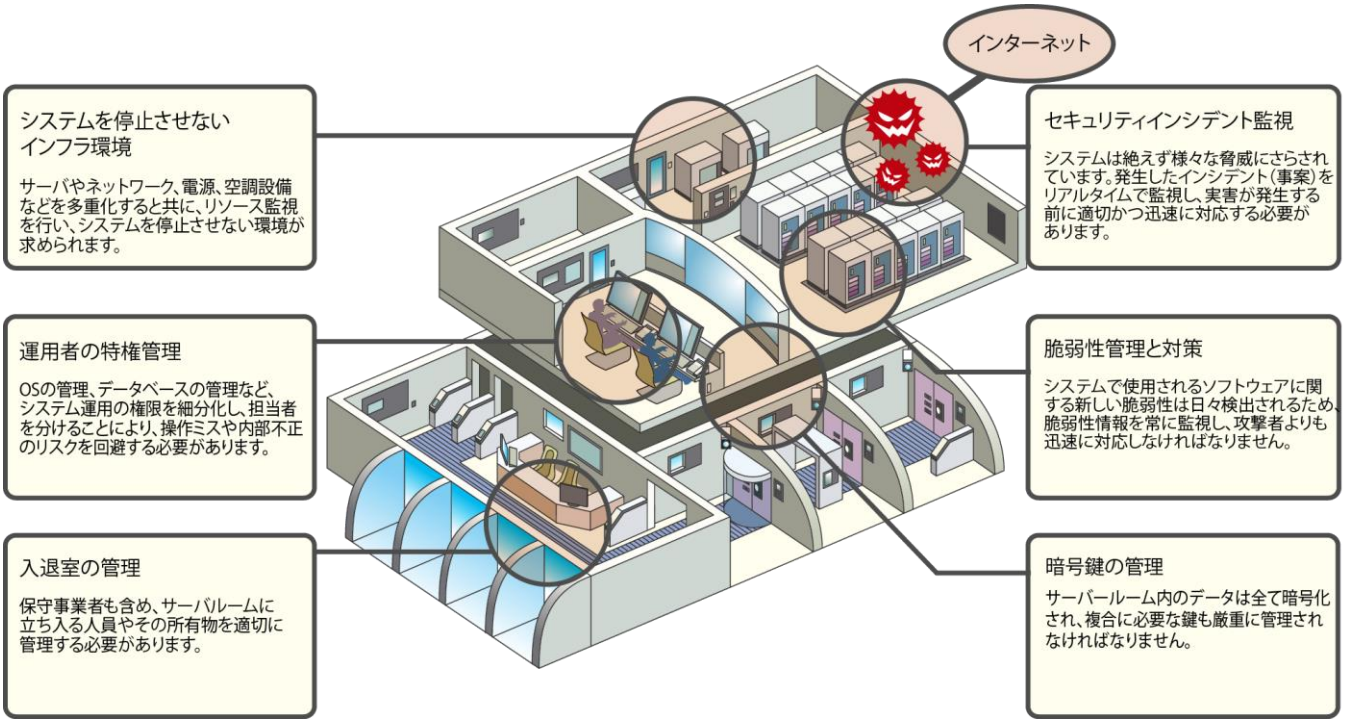

図　セキュリティ評価の 6 つのポイント

認証取得済みクラウドサービスにおけるセキュリティの優位性

機密性・完全性・可用性の観点で高い評価を得る認証済みクラウドサービス
オンプレミスで同様の対策を行う場合、膨大なコストと時間が必要となる

前ページに記載した評価観点に基づき、認証済みクラウドサービス、一般的なデータセンター、オンプレミスの各モデルを比較した結果のサマリーを以下の図に示します。

前述のとおり、いずれのモデルであっても IT システムの構築、運用は可能ですが、セキュリティの観点では大きな違いあることが分かります。認証取得済みクラウドサービスでは、非常に高いセキュリティレベルの環境が既に構築されており、その環境を多くのユーザーが利用することから、その利用にかかるコストを大きく削減することが可能です。

しかし、それと同等のセキュリティレベルをオンプレミスで実現しようとすると、技術面・運用面の全てのセキュリティ対策を自社で構築し、運用しなければならないため、膨大な初期費用及びランニング費用が発生します。

一般的なデータセンターの場合、インフラの整備や入退室の管理などの物理的セキュリティ対策や、監視のサービスなどは整っていると考えられますが、その実現レベルはデータセンターのサービス提供事業者によって異なるため、提供されるサービスのレベル・品質を、利用者の責任において確認して利用することが求められます。

また、サービス提供事業者内におけるオペレーションの運用状況については、利用者に情報が開示されないことも多く、その実態がブラックボックスになりがちです。

さらに、データセンターの事業者が提供しないサービスについては利用者自らが実施しなければならないことから、提供されるサービスの範囲を正確に把握し、カバーする領域に漏れや重複がないようにシステム全体をデザインする必要があります。

表　セキュリティ評価のポイント毎の評価結果のサマリー

セキュリティ評価のポイント	認証取得済みクラウドサービス	一般的なデータセンター	オンプレミス
①システムを停止させないインフラ環境	◎ 空調・電気設備等が充実 拠点の被災に備えデータを多重化	○ 空調・電気設備等が充実 データの多重化にはコストがかかる	△ ファシリティ設備は自前での準備が必要 データ多重化には膨大なコストがかかる
②運用者の特権管理	◎ 運用権限の細分化、担当者の分離など特権管理の制度が整っている	△ 運用管理フローは事業者に依存し、 担当者分離まで行うケースは少ない	△ 運用フローの設計、人員の確保と 教育等に膨大な時間とコストがかかる
③入退室の管理	◎ 多様な入退室制御機能に加え 外部事業者も対象にした管理フロー	○ 入退室制御機能は充実するが、 運用管理フローは事業者に依存する	△ 入退室制御システムの導入、運用 管理フローの制定にはコストが発生
④セキュリティインシデント監視	◎ インシデントを常時監視するSOCや 対応するCSIRTなどの組織が整う	○ 管理レベルは事業者によってまちまち 追加サービスとしてコストになる場合も	△ 独自のリアルタイム監視体制の構築は コスト、体制の両面で現実味が薄い
⑤脆弱性管理と対策	◎ 脆弱性情報の定期的な収集や システム脆弱性検査を定期的に実施	△ 脆弱性情報の検知から適用まで すべて利用者の責務となる	△ 脆弱性情報の検知から適用まで すべて利用者の責務となる
⑥暗号鍵の管理	◎ 独自に定義されたプロセスに基づき 暗号化の秘密鍵を厳重に保管	△ 事業者が特別なサービスを提供して いない限りは利用者の責務となる	△ 厳重な保管や利用ルールの徹底など 環境の整備にコストと時間が必要

① システムを停止させないインフラ環境

ネットワーク、電源、空調など、システムの安定運用に欠かせないインフラ環境の重要性
機器故障や広域災害の際にもシステムの停止やデータの損失を極小化する仕組みが求められる

重要なサービスを提供する IT システムでは、システムが常時安定的に利用できる状態を維持し、データの欠損などを防止する必要があります。また、利用者のニーズによっては、大地震等の広域災害の際であってもシステムを停止させず、業務を継続する必要性が生ずる場合もあります。そのため、電力の安定供給、空調の管理、通信回線の維持等、サーバやネットワーク機器が安定して稼動するために必要なインフラ環境の整備や、各種機器の多重化など、機器故障や広域災害の際であってもシステムを停止させない仕組みが求められます。

Microsoft Azure では、堅牢なデータセンターにてサーバ及びネットワーク機器が稼動しており、システムを停止させない安定したインフラ環境が整えられています。また、地理的に離れた二つの拠点のデータセンターを利用することにより、拠点の間でデータやシステムを複製することにより、万が一広域災害によりデータセンターが被災した場合であっても、顧客が利用するシステムやデータの損失を最小化することも可能です。

一方、一般的なデータセンターの場合、空調管理や電源管理などの設備は充実していることがほとんどですが、データセンターに設置するサーバやネットワーク機器は利用者自ら多重化しなければならず、機器の購入と、構築及び保守運用にコストが発生します。さらに設置型の場合、安定した電力供給や空調維持のための環境を独自に整える必要があります。システムが必要とする電力や空調システムを供給するために、電気工事が必要となるケースもあり、システム環境の整備とその維持に多額のコストが発生することが想定されます。

対策の要点

電力の安定供給、空調の管理、通信環境の維持など、サーバやネットワーク機器が安定して稼動するために必要な**インフラ環境の整備や、各種機器を多重化**することにより、**機器の故障時でもシステムを停止させない仕組み**が求められます。

認証取得済みクラウドサービスにおける対策

- ✓ Microsoft Azure サービスを提供するデータセンターでは、温度管理システム、冷暖房・換気・空調システム、火災検知および抑制システム・電力管理システム等による、各種機器の安定稼動を支える環境が整っています。
- ✓ ネットワーク機器、データ蓄積領域（ストレージ）は多重化され、機器に障害が発生した場合であっても、システムの停止やデータの欠損のリスクを限りなく抑制する仕組みが整っています。

一般的なDCにおける対策

- ✓ 空調や電力管理等は対策されているケースが一般的ですが、システムの多重化は利用者の責務となり、ハードウェア購入・構築・運用にかかる費用は高額になる傾向があります。

オンプレミスにおける対策

- ✓ システムが安定的に稼動する環境の確保及び維持管理から、システムの多重化による可用性の確保まで、全てが利用者の責務となり、導入・運用に膨大なコストが発生します。

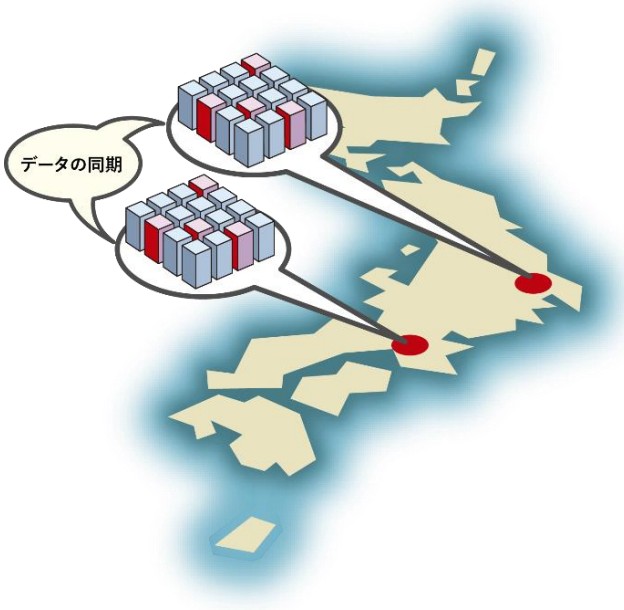

図　クラウドサービスにおけるデータ同期

② 運用者の特権管理

システム運用に必要な特権を厳格に管理
操作可能な範囲や期間を限定し、運用のブラックボックス化を防ぐ仕組みづくりが重要

IT システムには必ずシステム管理者が存在し、ハードウェア及びソフトウェアの日常的なメンテナンスや、障害発生時の復旧作業などを行います。これらの業務を行うためには、一般の利用者には許可されていない特別な権利（特権）が必要です。この特権を持つことにより、システム管理者は IT システムに対して様々な操作を行うことができるようになります。裏を返すと、システム管理者がこの特権を悪用してデータの盗み見や持ち出し、改ざんなどの不正行為を行うことも可能となってしまうため、誰が、何に対して、いつ、何ができるのかといった状態を、厳格に管理する必要があります。

しかし、この特権を厳密に管理することの業務的な負荷は小さくなく、ひとたびシステム管理者が特権を入手するとそのまま継続的に使用できてしまうケースが少なくありません。またその利用状況が記録され、定期的に監査されることも多くはないのが実情です。内部不正を迅速に検知し、対応するための体制やルールを整備し、継続的に運用することは難しく、緩やかな運用が許容されているケースが多く見られます。

一方、Microsoft Azure ではこの特権は極めて厳密に管理されています。平常時にエンジニアは特権を有しておらず、障害対応や利用者からの要求対応のために特権が必要となった場合は、管理者の承認を得た上で特権を得ることができます。この特権もシステム全体に対する権限ではなく、作業に必要な操作のみが実施できる権限だけが切り出されて付与されます。さらにその権限は、使用可能な時間も限定されている、極めて揮発性の高いものとなっています。このような仕組みを整えることにより、IT システムの運用が俗人化・ブラックボックス化することを防ぎ、利用者が安心して IT システムを使用できる環境を維持しています。

対策の要点

クラウド事業者の**従業員や委託事業者等による内部犯行**や、組織の**意図しない作業**が無管理状態で実施されることにより、システムの機密性や完全性が損なわれる恐れがあるため、システムにおける**特権の利用状況や、操作内容の適切な管理**が求められます。

認証取得済みクラウドサービスにおける対策

- ✓ Microsoft Azure では、主要な変更の実装を制御するための開発およびリリース管理プロセスが確立されており、重要な機能については職務が分離されています。
- ✓ Microsoft Azure への管理者アクセスは Customer Lockbox という仕組みでコントロールされており、作業の実行に必要となる最少の特権が、作業に必要な期間に限定して有効化されます。

一般的なDCにおける対策

- ✓ 事業者が特別なサービスを提供している場合を除き、システムの変更管理責任は利用者側にあります。管理者アカウントの管理や担当者の職務分離は、利用者が適切に管理する必要があります。

オンプレミスにおける対策

- ✓ システムの変更管理責任は全て利用者にあります。管理者の特権利用による内部犯行を防止するための運用ルールや監視・記録の仕組みを整え、適切に運用されていることを管理する必要があります。

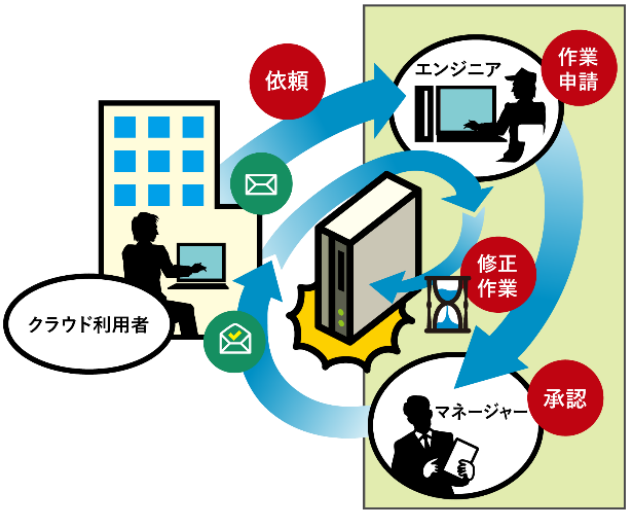

図　クラウドサービスにおける特権管理

③ 入退室の管理

高セキュリティエリアに対する厳重な入退室の管理が重要
いつ、だれが、何に対して物理的なアクセスが可能な状態にあったかを追跡できるような仕組み

重要な IT システムやデータが格納されているサーバルームなど、高いセキュリティを確保すべき区画では、その区画への立ち入りは厳重に制限し、管理しなければなりません。高セキュリティ区画に対する物理的な対策が不十分な場合、外部からの侵入が行われ、IT システムの停止や故障、情報の漏えいなどのセキュリティリスクが増大します。そこで、適切な権限をもった人員のみが入場できるように管理し、かつ入退室の記録を残しておくことにより、いつ、だれが、何に対して物理的にアクセス可能な状態にあったかを追跡できることが重要となります。

Microsoft Azure のデータセンターにおいて、重要なシステムが設置されている区画に立ち入る際は、電子カード（IC カード）、キーロック、生体認証など様々な方法によって、正当な権限を持っている人員であるかどうかの認証が厳密に行われます。また、正当な権限を持っている人員とそうでない人員とが同時に入場する「共連れ」を防止するメカニズムも整えられており、一人ひとりを正しく特定して、区画への立ち入りを制限し、記録しています。この入退室管理の仕組みは社員のみならず、ハードウェアの障害対応のために来訪した外部の契約業者や、その他の訪問者に対しても適用される運用フローが整備されています。

一般的なデータセンターでも、サーバルーム等のセキュリティエリアに対する入退室管理システムなど、物理的な対策が講じられていることは珍しくありませんが、認証方式の複雑さやその運用レベルはサービス提供事業者によって異なるため、利用者はその内容を把握し、リスクを判断する必要があります。さらに、設置型の場合は上述の入退室管理の仕組みを独自に構築し、運用ルールを定め、運用体制を整えたうえで厳格に適用することが必要であるため、導入及び運用には多額のコストが発生します。

対策の要点

セキュリティを確保すべき区画に対する、従業員やベンダ等の**人員の入場、退場、及びそれに伴う物品の持込みを厳格に制限**し、**適切な権限を持った人員のみが入場するように管理**し、システムの可用性や機密性を損ねるリスクを軽減するとともに、いつ、だれが、何に対して**物理的にアクセス可能な状態にあったかを追跡できる状態**にしておくことが求められます。

認証取得済みクラウドサービスにおける対策

- ✓ Microsoft Azure を運用するデータセンターの、重要なシステムが設置されている部屋は、電子カードアクセスコントロール、キーロック、共連れ防止、生体認証デバイスなどの様々な機能によって入室が制限されています。
- ✓ また、物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順が導入されています。

一般的なDCにおける対策

- ✓ 物理的なアクセスの制限や、入退室の管理システムが導入されているケースが一般的ですが、運用事業者によって、管理レベルには差があります。

オンプレミスにおける対策

- ✓ 物理的なアクセス制限、入退室管理などの導入や、運用フローの整備及び徹底には多くのコストが必要で、徹底が行き届かないケースが見受けられます。

■データセンターに導入されている物理的セキュリティメカニズム

異なる要素による認証を多重的に組み合わせることによりセキュリティを確保している。

電子カードアクセスコントロール	有効なIDカードを所有している人のみ入室を許可する（所有による認証）
キーによるロック	正しいキーを知っている人のみ入室を許可する（知識による認証）
生体認証	虹彩や静脈、指紋等その人しか持ち得ない特徴に合致する人のみ入室を許可する（本人の特長による認証）
共連れ防止	認証された人とともに、認証されていない人が入室することを防止する

図　クラウドサービスにおける物理的セキュリティ

④ セキュリティインシデント監視

増加、複雑化するサイバー攻撃に対抗できる体制の構築と維持
セキュリティインシデントをリアルタイムに監視し、迅速に対応できる体制が重要

IT システムの停止やデータの窃取を狙うサイバー攻撃は、増加かつ複雑化の一途を辿っています。世界中でサイバー攻撃が行われており、多数の被害が発生しています。

マイクロソフト社は世界で最も多くのサイバー攻撃を受けやすい企業のひとつと言われています。しかしながら、マイクロソフトはそれらのサイバー攻撃に対して適切に対応し、利用者のシステムの停止やデータの棄損といった損害を発生させることはありません。ネットワークに接続している以上、サイバー攻撃を受けないようにすることは不可能であり、攻撃を受けることを前提に、いかに迅速にその痕跡や傾向を検出し、適切な対応を講ずることができるかがセキュリティを担保するうえでの鍵となります。

マイクロソフトでは、膨大な数のサーバやネットワーク機器など Microsoft Azure を構成する機器をリアルタイムで監視し、セキュリティを侵害するインシデント（事故・事案）につながる可能性のある形跡を早期に発見する体制が整っています。SOC（Security Operation Center）と呼ばれる監視チームが IT システムの監視を行い、インシデントを検出した場合、CSIRT（Computer Security Incident Response Team）と呼ばれるチームがインシデントの対応を行います。経営層や内部組織、また外部の関連団体等とのコミュニケーションもこの CSIRT が中心となって実施され、組織全体としてセキュリティインシデントの対応に責任を持つ仕組みが整備されています。

SOC や CSIRT といった体制を構築し、効果的なインシデント対応ができるように成熟させるまでには、膨大な時間とコストがかかります。近年 CSIRT は多くの企業で立ち上がっているものの、事実上の効果は組織によって大きなばらつきがあることも事実です。重要な情報資産を確実に保護できる体制を構築できている企業は残念ながら多くはありません。

対策の要点

インターネットに接続されている全てのシステムは常にあらゆる脅威にさらされています。日々発生するセキュリティインシデント（事案）をリアルタイムで監視し、インシデントの影響範囲や重要度、緊急度に応じて適切な対応を行い、被害を極小化する体制・仕組みが必要となります。

認証取得済みクラウドサービスにおける対策

- ✓ Microsoft Azure では、専門のグループにより、システム上の悪意のある動作を識別するために、多数の主要なセキュリティパラメーターが監視されています。
- ✓ セキュリティインシデント対応チーム（CSIRT）を組織し、全社CSIRTとの相互連携が行われています。また、サイバー犯罪対応ユニットにより最新の状況の監視と対応が行われ、関係者と情報の共有が進められています。

一般的なDCにおける対策

- ✓ データセンター事業者によって、サービスとして提供されている場合とそうでない場合があります。また、有償のオプションサービスとして別途コストが発生するケースも存在します。

オンプレミスにおける対策

- ✓ 24時間365日でのインシデント監視体制を整える必要があり、自前で構築する場合は、システムの導入や運用フローの構築、人員の維持や教育に膨大なコストが発生します。

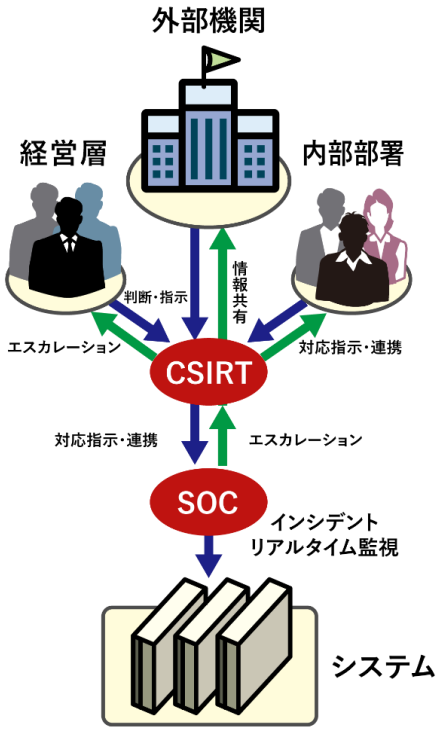

図 クラウドサービスにおけるインシデント対応体制

⑤ 脆弱性管理と対策

IT システムに対するセキュリティ侵害を可能にする脆弱性をいかにコントロールするか 日々新たに検出される脆弱性をスピーディかつ適切に評価し、対応するプロセスと体制が求められる

脆弱性とは、IT システムにて使用されているソフトウェアにおける、セキュリティを侵害する可能性のある不具合です。脆弱性には、外部からの不正な侵入やプログラムの実行によりデータを窃取するもの、システムの正常な動作を妨げるものなどいくつかの種類があり、サイバー攻撃を行う攻撃者にとって格好の的となっています。

システムの安全性を侵害する脆弱性が検出され、かつその脆弱性が自社の IT システムに関連する場合、攻撃者がその脆弱性を悪用するよりも前に適切な対応を行わなければなりません。脆弱性は日々新しいものが検出されているため、リアルタイムで監視し、迅速にリスク分析や対応を実施することが求められます。

Microsoft Azure では、使用している様々なソフトウェアに対して、脆弱性の有無を確認するスキャンが定期的に行われています。また、新たな脆弱性が発見された場合に備え、Microsoft Azure に対する影響範囲の調査、その脆弱性の危険度の評価、リスク軽減のためのアクションなど、脆弱性をハンドリングするプロセスが予め定められており、専門のチームにより運用されています。

IT システムを利用者が独自に構築して運用する場合、これらの脆弱性ハンドリングのプロセスを独自に定め、常時運用することが求められます。監視体制やシステム管理台帳の整備、リスク判断方法の決定や対応手順の策定など、整備しなければならない要素は多数に上ります。また情報資産を狙うサイバー攻撃の手法は日々高度化しており、適切な脆弱性ハンドリングを行うためには、高いスキル及び経験を有する技術者を育成して維持していくことが求められ、おのずと高いコストが発生します。

対策の要点

システムで利用するソフトウェアでは、**新たな脆弱性が日々検出**されています。
これらの脆弱性に対する適切かつ迅速な対応を怠ると、攻撃者に悪用され、システムの停止や、情報の改ざん、漏えいなどのインシデントが発生するリスクが高まるため、**脆弱性をリアルタイムで監視し、適切な管理と対策を迅速に行うことが重要**です。

認証取得済みクラウドサービスにおける対策

- ✓ Microsoft Azure では、マイクロソフト セキュリティ レスポンス センターから通知された脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを主導するとともに、セキュリティインシデント、脆弱性、異常動作について報告し処理する手順が整備されています。
- ✓ Microsoft Azure では、システムをスキャンして脆弱性の有無を定期的にチェックしており、不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフが対処できるような仕組みが整っています。

一般的なDC　及び　オンプレミスにおける対策

- ✓ 仮想基盤において、新たに検出された脆弱性の監視、自社システムにおける対応の要否、リスク規模の評価、対応方法の検討と評価、実施体制の確保など、脆弱性ハンドリングは全て利用者の責務となります。

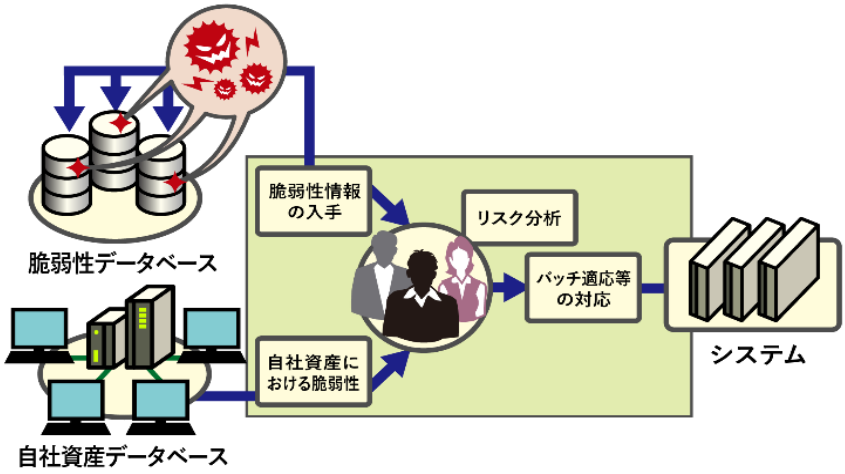

図　クラウドサービスにおける脆弱性対策

⑥ 暗号鍵の管理

サーバ上のデータや通信データは、適切なアルゴリズムによる暗号化で保護
暗号を解く復号鍵は厳格に管理し、高いセキュリティを担保するする運用が求められる

IT システム上のデータや、通信されるデータを保護するための重要な技術として、暗号化があります。暗号を解く鍵（復号するための鍵＝復号鍵）を持っていない第三者は暗号化されたデータの中身を確認できないため、安心してデータの通信や保管を行うことができる技術です。

このように、暗号化を行えば情報のセキュリティを高めることが可能ですが、注意しなければならない事項が二つあります。ひとつは暗号化の方式（アルゴリズム）です。暗号化する方法そのものが脆弱だと、復号鍵を持っていない場合であっても、暗号が解けてしまう場合があります。コンピュータの計算能力は年々向上しており、古い技術を元に実装された暗号化アルゴリズムは、安全性が損なわれている恐れがあります。

もうひとつの注意事項は復号鍵の取り扱いです。いくら十分な強度を備えたアルゴリズムで暗号化されていたとしても、復号鍵が流出してしまえば、暗号化されていないのと同じ状態となるため、復号鍵は厳密な管理が要求されます。

Microsoft Azure はインターネット経由で利用するクラウドサービスですが、利用者とデータセンターの間の通信は、十分な強度を持ったアルゴリズムによって暗号化されており、悪意のある攻撃者による傍受や改ざん、窃取を防止します。また、復号鍵は通常のサーバシステムよりもさらに厳重な保管が行われています。さらに、復号鍵を使用するためには複数の管理者による同時の操作を必要とするなど、内部的な不正行為に対する対策も講じられています。

設置型のシステムやデータセンターに保管しているシステムに対して、これらの仕組みを自社で整え、厳格に運用することは困難なケースも少なくありません。

対策の要点

クラウド環境に保存されている各種の重要な情報は、**強度が保たれているアルゴリズムに基づき暗号化**し、万が一外部に漏えいした場合でも、内容の改ざんや悪用から保護することが必要です。
また、**暗号化や復号に利用するための暗号鍵も、厳重に管理**されることが求められます。

認証取得済みクラウドサービスにおける対策

- ✓ マイクロソフトには、データセンター内のデータおよび伝送中のデータの暗号化をサポートする、効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムが存在しています。
- ✓ Microsoft Azure に保存されているデータの暗号化において、現時点で十分な強度が確認されているアルゴリズムを用いた暗号化機能が選択可能です。

一般的なDC　及び　オンプレミスにおける対策

- ✓ 暗号化のためのアルゴリズムの選択、暗号化・復号に使用する鍵の管理は全て利用者の責務となります。
- ✓ 鍵管理を外部の事業者に委託する場合、事業者による管理体制、管理方針、管理レベルなどを確認する必要があります。

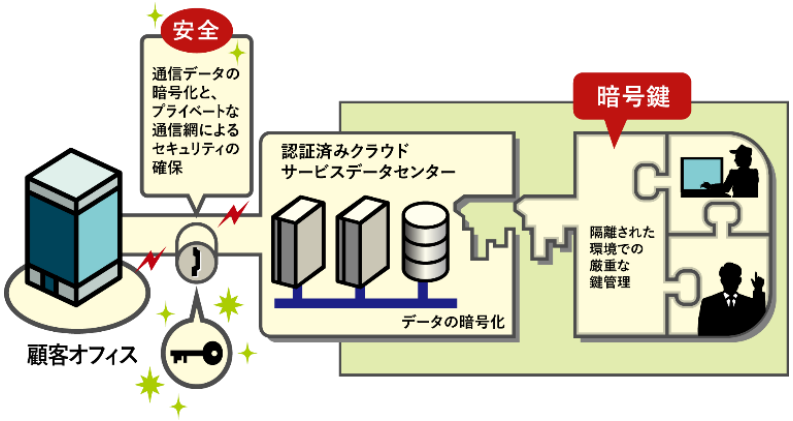

図　クラウドサービスにおける暗号鍵管理

【参考】各項目において対応する情報セキュリティ管理基準

特定非営利活動法人日本セキュリティ監査協会「クラウド情報セキュリティ管理基準 2013 年度改正版 Ver1.1」（平成 26 年 9 月）より抜粋

① システムを停止させないインフラ環境	➢ 5.2.1 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、又は保護する ➢ 5.2.2 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する ➢ 5.2.3 データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受又は損傷から保護する ➢ 6.3.1 要求されたシステム（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）性能を満たすことを確実にするために、資源の利用を監視・調整し、将来必要とする容量・能力を予測する ➢ C.1.1 情報処理設備（クラウドサービスの提供にかかわるもの、クラウドサービスを提供するもの及びクラウドサービスとして提供されるものを含む。）は、一部の機能の喪失がクラウドサービスを停止させないために冗長化する。また、冗長化の状況について、クラウド利用者に示す ➢ C.2.1 情報処理設備（クラウドサービスの提供にかかわるもの、クラウドサービスを提供するもの及びクラウドサービスとして提供されるものを含む。）は、一部の機能の喪失がクラウドサービスを全面的に停止させないために分散化する
② 運用者の特権管理	➢ 6.1.1 操作手順（クラウドサービスの提供にかかわるシステムのもの、クラウドサービスを提供するシステムのもの及びクラウドサービスとして提供されるシステムのものを含む。）は、文書化し、維持する。また、その手順は、必要とするすべての利用者（クラウド利用者を含む。）に対して利用可能にする ➢ 6.1.2 情報処理設備及びシステム（クラウドサービスの提供にかかわるもの、クラウドサービスを提供するもの及びクラウドサービスとして提供されるものを含む。）の変更は、管理し、クラウド利用者に影響を及ぼす変更は、事前にクラウド利用者に示す ➢ 6.1.3 組織の職務及び責任範囲は、組織及びクラウド利用者の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分割する。また、クラウド利用者の責任範囲は、クラウド利用者の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために分割すべきものを、クラウド利用者に示す
③ 入退室の管理	➢ 5.1.1 情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いる ➢ 5.1.2 セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する ➢ 5.1.3 オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する ➢ 5.1.5 セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し、適用する。また、提供するクラウドサービスにおいてクラウド利用者の利用環境を拡大させる機能を提供する場合には、クラウド利用者にその機能を示す ➢ 5.1.6 一般の人が立ち寄る場所（例えば、荷物などの受渡場所）及び敷地内の認可されていない者が立ち入ることもある場所は、管理する。また、可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す
④ セキュリティインシデント監視	➢ 8.2.3 業務用ソフトウェア（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）の真正性を確実にするための要求事項及びメッセージの完全性を保護するための要求事項を特定し、また、適切な管理策を特定し、実施する ➢ 8.3.1 情報（クラウドサービス上の情報を含む。）を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。また、提供するクラウドサービスの暗号利用に関して、クラウド利用者に示す ➢ 8.3.2 組織における暗号技術の利用を支持するために、かぎ管理を実施する。また、提供するクラウドサービスのかぎ管理に関する情報提供の方針を定め、クラウド利用者に示す
⑤ 脆弱性管理と対策	➢ 6.10.1 利用者（クラウドサービスの利用者を含む。）の活動、例外処理及びセキュリティ事象を記録した監査ログを取得し、将来の調査及びアクセス制御の監視を補うために、合意された期間、保持する。また、クラウドサービスの利用者の活動、例外処理及びセキュリティ事象を記録した監査ログを取得する機能をクラウド利用者に示し、提供する ➢ 6.10.2 情報処理設備（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）の使用状況を監視する手順を確立し、監視活動の結果を定めに従ってレビューする。また、クラウドサービスの使用状況を監視する機能を、クラウド利用者に提供する ➢ 6.10.3 ログ機能及びログ情報（クラウドサービスの提供にかかわるもの及びクラウドサービスに含まれ提供されるものを含む。）は、改ざん及び認可されていないアクセスから保護する ➢ 6.10.6 組織又はセキュリティ領域内のすべての情報処理システム（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）内のクロックは、合意された正確な時刻源と同期させる。また、クラウドサービスとして提供される情報システムの同期の仕組みをクラウド利用者に示す
⑥ 暗号鍵の管理	➢ 8.6.1 利用中の情報システムの技術的ぜい弱性（クラウドサービスの提供にかかわるもの、クラウドサービスを提供するもの、及びクラウドサービスとして提供されるものを含む。）に関する情報は、時機を失せずに獲得し、必要に応じてクラウド利用者に通知する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる