

金融機関向け『Microsoft Azure』対応 セキュリティリファレンス（FISC第9版改訂）

概要説明資料

2020年1月31日

セキュリティリファレンスの概要（１）

■金融機関向けクラウドサービス対応セキュリティリファレンスとは？

近年、クラウドサービスは急速に普及しつつあり、大企業、中堅企業、中小企業の様々なビジネスシーンにおいて活用されています。ただし、金融業界においては、金融庁の監督指針や検査マニュアル、公益財団法人金融情報システムセンター（FISC）の「金融機関等コンピュータシステムの安全対策基準」（以下、「FISC安全対策基準」という。）等の基準があり、それらを満たさなければ業界内でクラウドを採用することは難しいとされています。

そこで、金融業界におけるクラウドサービスの利活用促進を目的として、FISC安全対策基準の各項目に対して、対象とするクラウドサービスの対応状況を確認・整理した結果を、ここでは「金融機関向けクラウドサービス対応セキュリティリファレンス」と呼んでいます。

※「FISC安全対策基準」は金融情報システムセンター（FISC）の刊行物です。

FISC安全対策基準の項番の記載についてはFISCからの承諾を得ております。

■金融機関向け『Microsoft Azure』対応セキュリティリファレンスとは？

今回公開する金融機関向け『Microsoft Azure』対応セキュリティリファレンス（FISC第9版改訂）（以下、「Azure対応セキュリティリファレンス」という。）は、Microsoft社のクラウドサービスである『Microsoft Azure』に関して、仮想マシン（IaaS）を利用し、金融機関が独自のアプリケーションを稼働させることを想定して、FISC安全対策基準（第9版改訂）の各項目に対する対応状況を調査したものです。

調査は、株式会社三菱総合研究所、日本ビジネスシステムズ株式会社、トレンドマイクロ株式会社、株式会社電通国際情報サービス、SCSK株式会社、株式会社FIXERおよび日本電気株式会社が実施し、FISC安全対策基準の各項目（統制基準26項目、実務基準144項目、設備基準137項目、監査基準1項目）のそれぞれについて確認・整理しました。

セキュリティリファレンスの概要（2）

■Azure対応セキュリティリファレンスの使い方

Azure対応セキュリティリファレンスは、金融機関等（利用者）が自らMicrosoft Azureを使用したり、SI事業者（システムインテグレータ）等がMicrosoft Azureを利活用して金融機関にサービスを提供する場合に、FISC安全対策基準にどのように適合しうるかをセルフチェックするためのツールとして利用することを想定しています。

Azure対応セキュリティリファレンスでは、FISC安全対策基準の各基準（項番を記載）に対して、「FISC安全対策基準（第9版改訂）に対するMicrosoftの見解」、「Microsoft Azureにおける対応」（「FISC安全対策基準への適合性」、「本調査で確認した内容」、「確認した公開文書」、「第三者認証等から確認した内容」、「Microsoftへのインタビューで確認した内容」）、「SI事業者・利用者で必要な対応」を示しています。

利用者やSI事業者が「SI事業者・利用者で必要な対応」に示した対応を自らが実施することと、「Microsoft Azureにおける対応」に示した状況の両方の結果により、FISC安全対策基準に適合できると考えています。

※本セキュリティリファレンスは、セキュリティリファレンス（FISC第9版）に、第9版改訂に伴う追記事項を加える様式で構成しています。

■Azure対応セキュリティリファレンスの利用許諾について

Azure対応セキュリティリファレンスは、「金融機関向け『Microsoft Azure』対応セキュリティリファレンス（FISC第9版改訂）利用許諾契約書」（以下、「利用許諾契約書」）を読み、その内容に同意した方のみに利用を許諾しています。詳細な利用条件等については、Azure対応セキュリティリファレンスと同時に公開される利用許諾契約書をご覧ください。

Azure対応セキュリティリファレンスの読み方

Azure対応セキュリティリファレンスには、FISC安全対策基準の各項目に対して、以下の表に示した項目が記載されています。

| Azure対応セキュリティリファレンスの項目 | | 項目の説明 |
|----------------------------|--------------------------|---|
| FISC安全対策基準の項目 | | 「金融機関等コンピュータシステムの安全対策基準」に示された「項番」を記載した。 |
| FISC安全対策基準に対するMicrosoftの見解 | | FISC安全対策基準の基準小項目ごとのMicrosoft社の見解を記載した。 |
| Microsoft Azure における対応 | FISC安全対策基準への適合性 | 「本調査で確認した内容」ならびに「SI事業者・利用者で必要な対応」からFISC安全対策基準への適合性を次の分類で整理した。 「適合可能」：Azureの状況に加えて、SI事業者・利用者が必要な対応を行うことで適合可能。 「対象外」：Azureにおける対応の対象外であり、必要に応じてSI事業者・利用者が対応。 |
| | 本調査で確認した内容 | 本調査で確認したAzureの対応状況。 確認にあたっては、公開文書の確認、第三者認証等からの確認に加えて、Microsoft社に対するインタビューの内容を用いた。 |
| | 確認した公開文書 | 確認に使用した公開文書への参照を記載した。 文献番号に対応する公開文書の情報は「参照文書リスト」に示した。 |
| | 第三者認証等から確認した内容 *1 | Azureが取得済みの第三者認証の認証状況から対応状況を確認した内容を記載した。 参照した第三者認証等の情報は「参照文書リスト」に示した。 |
| | Microsoftへのインタビューで確認した内容 | Microsoft社に対するインタビューにより確認した内容を記載した。 |
| SI事業者・利用者で必要な対応 | | FISC安全対策基準に適合するために、SI事業者・利用者での対応が必要な項目について、その対策例を示した。 |

*1：第三者認証等の文書はMicrosoftのサービストラストポータル(<http://aka.ms/stp>)から入手可能。

参照公開文書リスト（１）

| 番号 | 公開文書名 / URL |
|----|---|
| 01 | Microsoft Azure Responses to Cloud Security Alliance Consensus Assessments Initiative Questionnaire v3.0.1 https://gallery.technet.microsoft.com/Azure-Responses-to-CSA-46034a11 |
| 02 | Azure セキュリティの概要 https://docs.microsoft.com/ja-jp/azure/security/azure-security |
| 03 | Azure の暗号化の概要 https://docs.microsoft.com/ja-jp/azure/security/security-azure-encryption-overview |
| 04 | Microsoft クラウド サービスとネットワーク セキュリティ https://docs.microsoft.com/ja-jp/azure/best-practices-network-security |
| 05 | Azure Active Directory ポータルの監査アクティビティ レポート https://docs.microsoft.com/ja-jp/azure/active-directory/active-directory-reporting-activity-audit-logs |
| 06 | Microsoft Azure Security Response in the Cloud https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678 |
| 07 | Azure Active Directory のパスワードポリシーと制限 https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/concept-sspr-policy |
| 08 | Azure のデータセキュリティと暗号化のベストプラクティス https://docs.microsoft.com/ja-jp/azure/security/azure-security-data-encryption-best-practices |
| 09 | Security Development Lifecycle https://www.microsoft.com/en-us/sdl |
| 10 | Azure Security Center とは https://docs.microsoft.com/ja-jp/azure/security-center/security-center-intro |

参照公開文書リスト（２）

| 番号 | 公開文書名 / URL |
|----|---|
| 11 | 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 https://info.microsoft.com/JA-Azure-CNTNT-FY15-06Jun-MS-Azure-security-privacy-compliance.html |
| 12 | Azure リージョン https://azure.microsoft.com/ja-jp/global-infrastructure/regions/ |
| 13 | マイクロソフトは高速で信頼性の高いグローバルネットワークをどのように構築しているのか https://blogs.technet.microsoft.com/mssvrpmj/2017/05/01/how-microsoft-builds-its-fast-and-reliable-global-network/ |
| 14 | FISC安全対策基準 第9版 適合説明書 統制基準/監査基準編 (Compliance Companion for Japan FISC Guidelines v9 - Japanese) https://servicetrust.microsoft.com/ViewPage/TrustDocuments |
| 15 | オンライン サービス条件 (OST) https://www.microsoft.com/ja-jp/licensing/product-licensing/ |
| 16 | マイクロソフトのデータ管理 https://www.microsoft.com/ja-jp/trustcenter/privacy/where-your-data-is-located |
| 17 | Azure Multi-Factor Authentication とは https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/multi-factor-authentication |
| 18 | Site Recovery について https://docs.microsoft.com/ja-jp/azure/site-recovery/site-recovery-overview |
| 19 | 欠番 |
| 20 | 欠番 |

参照第三者認証レポートリスト

Azureの第三者認証に関する監査レポートはサービストラストポータル(<http://aka.ms/stp>)から入手可能※です。

※要サインイン

| 番号 | 第三者認証レポート名 |
|----|---|
| 01 | ISO 27001:2013 ISO Reports / Azure - ISO 27001 and 27018 Assessment Report - 11.2.2017 |
| 02 | SOC2レポート SOC Reports / Azure & Azure Government SOC 2 Type 2 Report (2017-04-01 to 2018-03-31) |
| 03 | FedRAMP System Security Plan FedRAMP Reports / Azure - FedRAMP Moderate System Security Plan v3.02 |