FIXER

cloud.config for Financial Services

ホワイトペーパー

ver1.1

2018 年 12 月 14 日

株式会社 FIXER

内容

1. はじめに

1.1. cloud.config とは

cloud.config(クラウドコンフィグ）は、株式会社 FIXER（以下 FIXER と記載）が提供するクラウドのフルマネージドサービスです。マイクロソフト社が提供するクラウドプラットフォーム「Microsoft Azure（マイクロソフトアジュール、以下 Azure と記載)」の導入設計、運用・保守をサポートし、アプリケーションから OS＋ミドルウェア以下のレイヤーを 24 時間 365 日サービスの運用要件に合わせた監視・保守を行います。

株式会社 FIXER コーポレートサイト
https://fixer.co.jp

cloud.config 公式サイト
https://cloud-config.jp

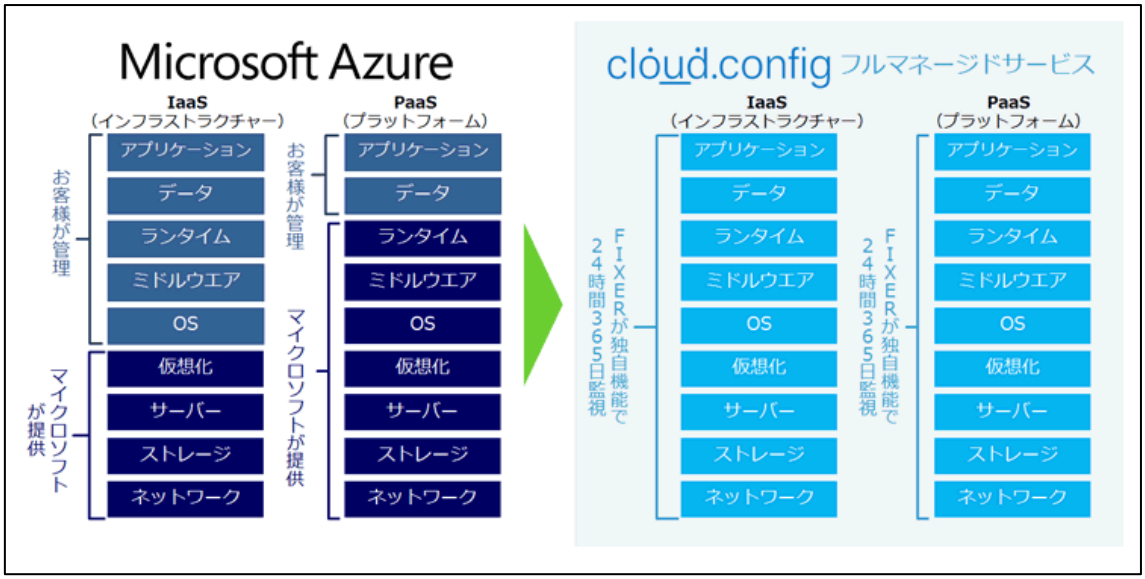

図 1　cloud.config のサービススタック

cloud.config の詳細については、別紙「cloud.config ホワイトペーパー」を参照してください。

1.2. cloud.config for Financial Services とは

cloud.config for Financial Services は、金融情報システムセンター（以下 FISC と記載）が発行する「金融機関等コンピュータシステムの安全対策基準（第 9 版)」(以下安全対策基準と記載）に対応した cloud.config サービスです。

cloud.config for Financial Services の利用により、金融機関のお客様は、安全対策基準が要求する高度なセキュリティや信頼性に迅速・安価に対応することができます。

なお、FISC および安全対策基準については第 3 章で説明します。

1.3.　本ホワイトペーパーについて

本ホワイトペーパーは、cloud.config for Financial Services について、サービス開発の背景、サービス内容およびサービス導入のメリットを読者にご理解いただくために提供するものです。

対象読者：
クラウドをご利用中の金融機関関係者の方
クラウドの導入をご検討中の金融機関関係者の方

2. 金融機関のクラウド活用

2.1. 金融システムのクラウド化

近年、金融機関が相次いでシステムをクラウドに移行しています。

当初はクラウド化の対象は情報系システムが中心でしたが、今後は勘定系システムを含めた業務系システムもクラウド化する流れになると考えられます。勘定系を含めたシステムのフルクラウド化により、ユーザーとのコミュニケーションに必要なデータをワンストップで扱うことができ、FinTech をはじめとしたビジネスの変革に迅速に対応することができるようになります。

2018 年 5 月には、金融機関のデジタルトランスフォーメーションの推進に寄与する「金融クラウド」の検討を目的として、「金融デジタルイノベーションコンソーシアム」が設立されました。

金融デジタルイノベーションコンソーシアム（FDIC）
https://fdic.connpass.com/

今後は、金融システムも「クラウドファースト」で検討されていくと考えられます。

2.2. クラウドのセキュリティ

かつては、クラウド自体のセキュリティに対して懸念が示されていました。しかし、昨今の大手クラウドベンダーはセキュリティに大変注力しており、非常に高いレベルのセキュリティを実現しています。

Azure も、各種セキュリティ関連認証を取得する等、クラウドサービスとしてトップレベルのセキュリティを実現しており、金融機関からもセキュリティの観点で高い評価を得ています。

Azure のセキュリティ
https://azure.microsoft.com/ja-jp/overview/security/

一方で、クラウドを利用したシステムのセキュリティは、プラットフォームとしてのクラウドだけでは実現できません。アプリケーション等、クラウド上に構築されるコンポーネントを含めて全体としてセキュリティを確保する必要があります。

クラウドベンダーとクラウドユーザーは、セキュリティに関する責任を分担します。すなわ

ち、クラウドベンダーは、自社が提供するプラットフォームと、そのプラットフォームを配置する設備のセキュリティに責任を持ち、クラウドユーザーは、プラットフォームの上に構築したコンポーネントのセキュリティに責任を持ちます。

Azure におけるセキュリティも、この責任分担の考え方に則ります。

> Azure セキュリティの管理と監視の概要
> https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview

2.3. 金融システムのセキュリティ

経済活動の生命線とも言える金融システムには、高い安全性・安定性が求められます。

インターネットバンキングの登場により、ユーザーの利便性は飛躍的に向上しました。金融機関にとって、新たなテクノロジーの導入は、ビジネスの可能性を切り拓く鍵になります。

一方で、金融システムは、金銭目的のサイバー攻撃者から狙われ、その安全性・安定性が脅かされています。警視庁の統計によると、平成 28 年上半期におけるインターネットバンキングの不正送金事案は、発生件数が 857 件、被害額は約 8 億 9,800 万円にのぼりました。

> 平成 28 年上半期におけるインターネットバンキングに係る不正送金事犯の発生状況等について
> http://www.npa.go.jp/cyber/pdf/H280908_banking.pdf

サイバー攻撃は増々高度化・複雑化しており、金融機関は、テクノロジーの導入と併せて、セキュリティを導入していくことが必須になります。

3. FISC 安全対策基準

3.1. 金融情報システムセンター（FISC）とは

金融情報システムセンター（FISC）は、金融情報システムに関連する諸問題の国内外における現状、課題、将来への発展性とそのための方策等についての調査研究を行うために、昭和 59 年 11 月に財団法人として設立されました。金融機関、保険会社、証券会社、コンピューターメーカー、情報処理会社等が参画しています。

金融情報システムセンター（FISC）
https://www.fisc.or.jp/

3.2. FISC 安全対策基準とは

FISC 安全対策基準は、正式名称を「金融機関等コンピュータシステムの安全対策基準・解説書」といい、金融情報システムの安全性確保のために FISC が発刊する自主基準です。

昭和 60 年 12 月に初版が発刊されて以降､時代の潮流に合わせて改訂が重ねられています。直近では、クラウドサービスの利用やサイバー攻撃対応を踏まえた第 8 版追補改訂が平成 27 年 6 月に発刊されました。その後、リスクベースアプローチを導入した第 9 版が平成 30 年 3 月に発刊され、この第 9 版が現在の最新版となっています。

高度なセキュリティや信頼性が必要とされる金融システムは、安全対策基準への対応は必須であると言えます。

※ 本書では、以降断りがないかぎり、本書発行時点における最新版である安全対策基準の第 9 版を対象とします。

4. cloud.config for Financial Services

4.1. 責任分担モデル

「2.2 クラウドのセキュリティ」に記載したとおり、クラウドを利用したシステムのセキュリティは、クラウドベンダーとクラウドユーザーで責任を分担して確保します。cloud.configにおいては、マイクロソフト（Azure）、FIXER（cloud.config）、お客様の 3 者で責任を分担することになります。

cloud.config の FISC 安全対策基準への対応においても、この考え方を採用しています。すなわち、3 者の責任分担は下図のようになります。

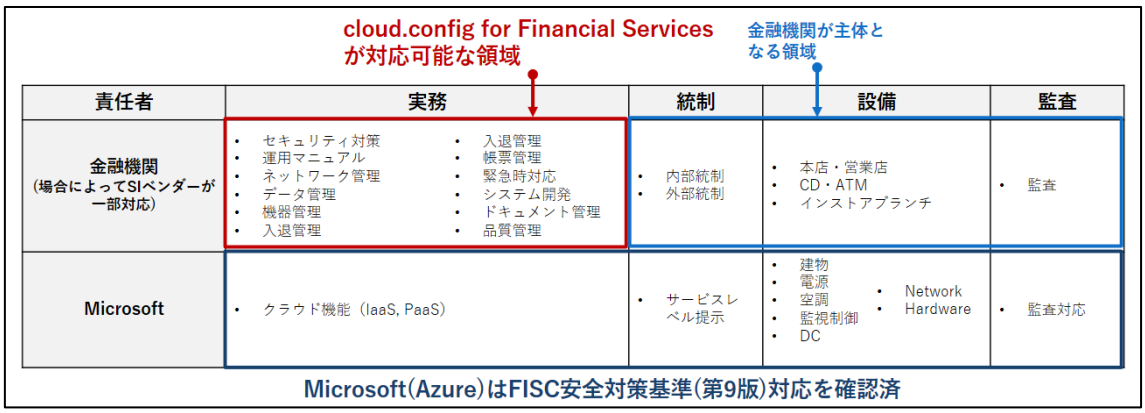

図 2 cloud.config for Financial Services の責任分担モデル

Azure に関するセキュリティはマイクロソフトが責任を負いますが、お客様と FIXER の間での責任分担は、業務要件によって異なります。

例えば、お客様自身がアプリケーションを開発・運用し、cloud.config がミドルウェア以下の構築・運用をカバーする場合、アプリケーションやデータのセキュリティは、原則としてお客様の責任となります。一方、アプリケーション開発を FIXER にご依頼いただく場合は、アプリケーション・データを含めて FIXER がセキュリティを担います。

また、安全対策基準は、例えば店舗の安全対策のような物理セキュリティも対象としています。このような cloud.config のサービス対象外となる部分については、お客様がセキュリティを担うことになります。

4.2. Azure の FISC 安全対策基準への対応

マイクロソフトは、Azure の安全対策基準 第 9 版への対応を確認したことを、2018 年 5 月

に公表しました。

4.3.　cloud.config の FISC 安全対策基準への対応

4.3.1.　対応方針

cloud.config は、「1.1 cloud.config とは」に記載したとおり、アプリケーションレイヤーまでをカバーするフルスタックのサービスです。

一方、cloud.config for Financial Services では、原則としてアプリケーションレイヤーは金融機関またはシステムインテグレーター／アプリベンダーの担当領域としています。これにより、金融機関またはシステムインテグレーター／アプリベンダーが独自の強みを発揮した金融ビジネスを展開しつつ、安全対策基準に対応した cloud.config for Financial Services をプラットフォームとして活用することができます。

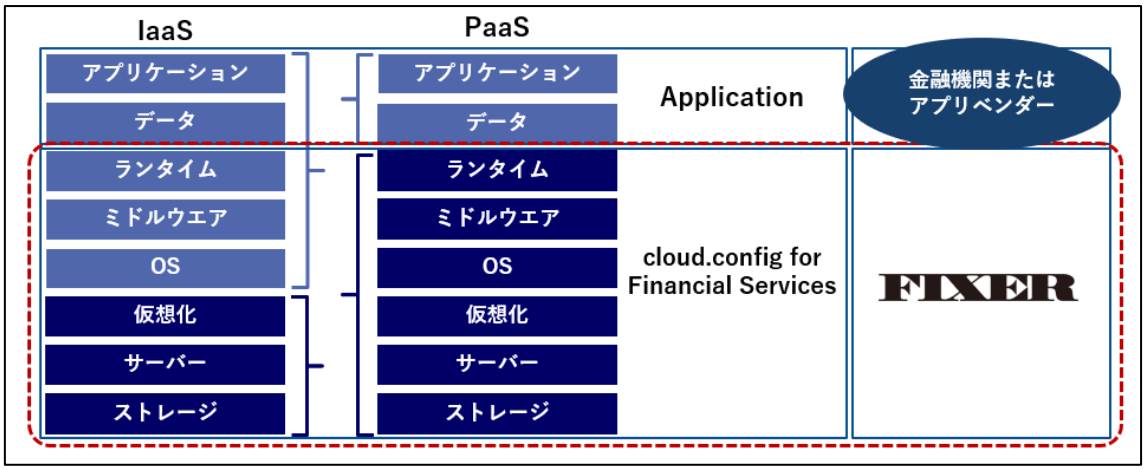

図 3　プラットフォームとしての cloud.config for Financial Services

cloud.config for Financial Services では、様々な技術／運用により、金融機関の安全対策基準対応をサポートします。

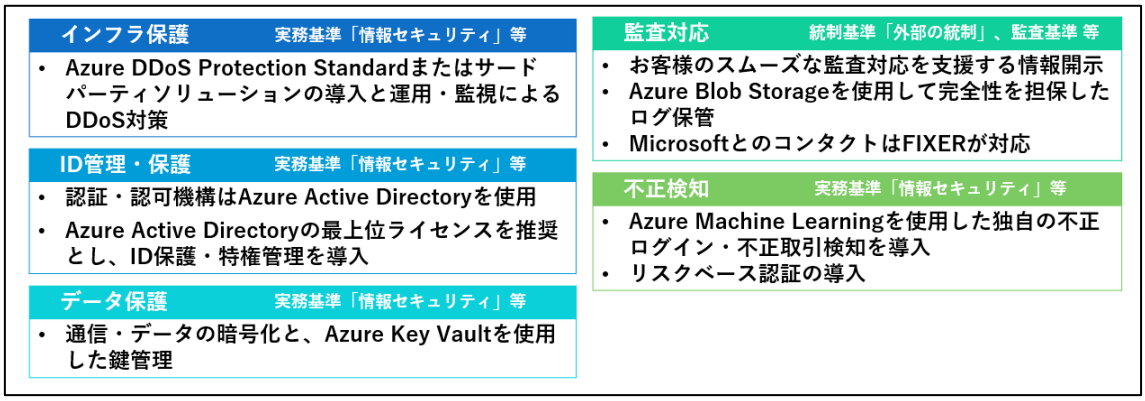

図 4　cloud.config for Financial Services の特長

次節以降で、cloud.config for Financial Services の主要な安全対策基準対応を記載します。

4.3.2.　セキュリティ対策

cloud.config for Financial Services は、Azure の機能を活用した包括的なセキュリティ対策を提供します。

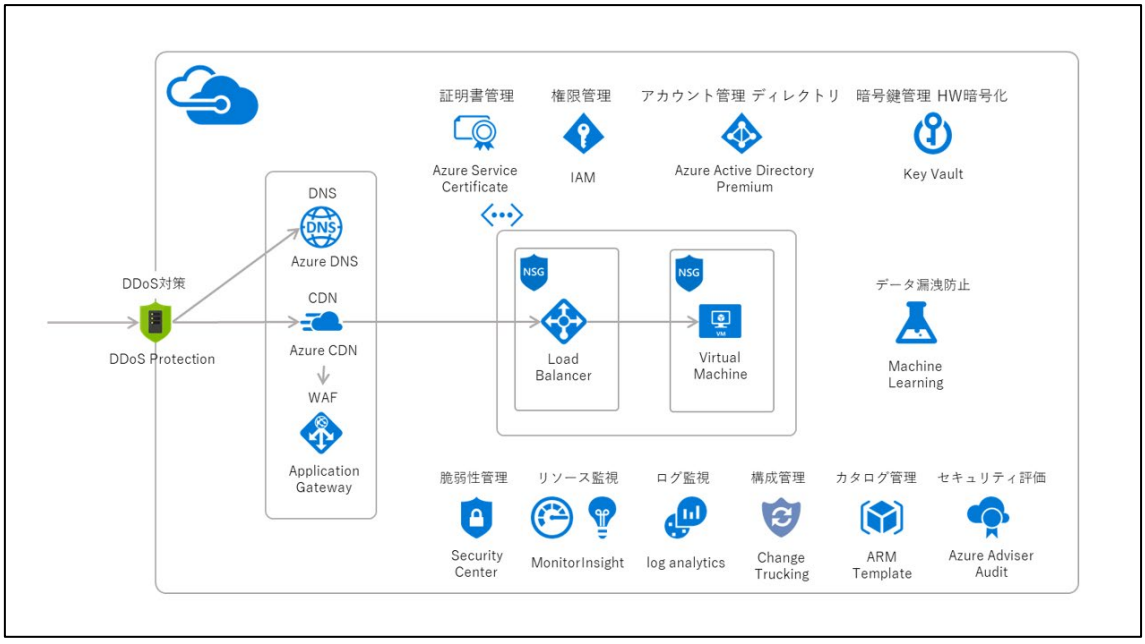

図 5　cloud.config for Financial Services の Azure ネイティブなセキュリティ対策

Azure は、マイクロソフトのセキュリティ対策技術が凝縮された多数のセキュリティ機能を提供します。これらの対策は、サイバー攻撃の高度化に合わせて日々進化を続けます。

オンプレミスにおけるセキュリティは、新たなサイバー攻撃手法が登場するたびに対応策

をアドオンで導入する必要があり、そのたびに予算確保やシステム構成変更などが発生します。攻撃者が常に先手を打ってくる状況の中で、ユーザーは後手回りのセキュリティ対策を行わざるを得ません。

Azure のセキュリティ機能は常に進化しており、また cloud.config for Financial Services ではその進化する Azure のセキュリティ機能を最適化して構成するため、お客様のセキュリティ対策における労力を大幅に低減します。

また、cloud.config for Financial Services では、安全対策基準のリスクベースアプローチに適したセキュリティ対策のテンプレートを用意しています。これにより、お客様は一層迅速なセキュリティ対策の導入が可能となります。

4.3.3. 不正検知

「2.3 金融システムのセキュリティ」に記載したとおり、金融機関における不正対策は喫緊の課題です。前節に記載したとおり、cloud.config for Financial Services では、Azure の機能を最大限に活用したセキュリティ対策を実施します。

更に、機械学習を活用した独自開発のリスク検出エンジンにより、不正なログインや異常な取引を検知して、不正防止を行います。

4.3.4. 監査対応

金融機関は、安全対策基準の監査基準に基づいた監査を実施します。金融機関が cloud.config for Financial Services を利用する場合、外部委託関係は以下のようになります。

金融機関（金融サービス）
　↓
FIXER（cloud.config for Financial Services）
　↓
マイクロソフト（Azure）

金融機関は、委託先または再委託先である FIXER およびマイクロソフトの監査を実施する必要があります。

cloud.config for Financial Services では、FIXER は金融機関による監査への対応体制を整備し、第三者機関認証等の証跡を提出します。また、Azure を使用したシステムを利用する場合、通常であれば金融機関がマイクロソフトに対して監査を実施する必要がありますが、cloud.config for Financial Services では、FIXER がマイクロソフトとのコンタクトを代行し、

金融機関の監査業務の負担を低減します。

4.4. cloud.config for Financial Services のエコシステム

cloud.config for Financial Services は、金融機関やシステムインテグレーター／アプリベンダーにとって、安全対策基準に対応したビジネスプラットフォームとして活用することができます。

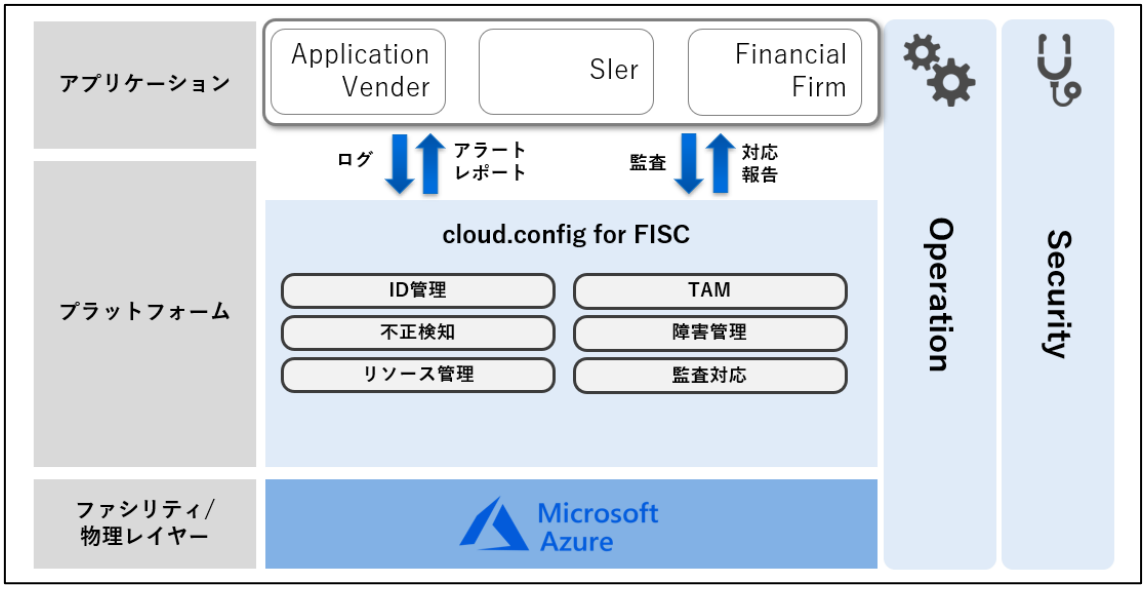

図 6　cloud.config for Financial Services エコシステム

安全対策基準の各基準項目に対応した機能・運用をプラットフォームとして提供するため、金融機関やシステムインテグレーター／アプリベンダーをはじめとした金融ビジネスの各プレイヤーは、安全対策基準への対応レベルを維持しながら、自身のビジネス領域に注力できることになります。

安全対策基準対応への負担が低減することにより、金融機関は迅速に第 9 版に対応することができます。また運用コストが低減することにより、FinTech をはじめとしたイノベーションに経営資源を投入することが可能となります。更に、進化するクラウドの機能を最大限に活用することにより、cloud.config for Financial Services をビジネスの競争力につなげることができます。

5. cloud.config for Financial Services の安全対策基準への対応

5.1. 概要

本章では、cloud.config for Financial Services の安全対策基準への対応内容を記載します。

次節以降において、FISC 安全対策基準の中項目単位で、cloud.config for Financial Services の対応方針と、お客様の対応要否の概要を記載します。

なお、各基準項目の内容につきましては、FISC 安全対策基準の原文をご参照ください。

5.2. 統制基準

5.2.1. 内部の統制

内部の統制は、お客様において各基準項目への対応が必要です。

以下においては、cloud.config for Financial Services に係る FIXER としての各基準項目への対応を記載します。

表 1 内部の統制 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	統 1～3	FIXER は、システムリスク管理ポリシーおよびスタンダードを定め、それに則ったシステムの安全対策を実施します。 cloud.config for Financial Services に係るシステム化計画は、経営計画との整合性を取って策定し、経営レベルでの承認を行います。
(2)	統 4～12	cloud.config for Financial Services では、お客様のシステムの稼働状況やセキュリティアラートを 24 時間 365 日監視し、対応が必要と判断される場合には迅速に対応を行います。 cloud.config for Financial Services の運用は、組織体制、業務分掌、業務規則を定め、それに基づいて行います。
(3)	統 13	cloud.config for Financial Services は、FIXER のセキュリティ関連規程に基づいて運用されます。運用担当者の規定遵守状況は定期的に確認します。
(4)	統 14～19	cloud.config for Financial Services の運用組織においては、セキュリティ教育および障害時に備えた教育・訓練を行います。また、運用要員の人事管理・健康管理を行います。

5.2.2. 外部の統制

外部の統制は、cloud.config for Financial Services のご利用を含めて、お客様において各基準項目への対応が必要です。

以下においては、cloud.config for Financial Services に係る FIXER としての各基準項目への対応を記載します。

表 2 外部の統制 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	統 20～23	お客様による cloud.config for Financial Services のご利用が、お客様にとって外部委託となります。 FIXER は、お客様が cloud.config for Financial Services を選定される際に必要な評価事項に対する情報を提供します。
(2)	統 24	cloud.config for Financial Services では、お客様の統制要件に合致する Azure のリージョンを提案します。 また、FIXER は、自己監査または専門知識を有する第三者監査人による監査を実施し、その結果をお客様に提供します。
(3)	統 25	cloud.config for Financial Services で共同センターを構築または利用する場合、お客様と FIXER は、緊急事態対応等についてお客様との役割分担を決定します。
(4)	統 26	本基準項目は、cloud.config for Financial Services の対象外です。

5.3. 実務基準

実務基準は、業務要件によりお客様と FIXER の責任分担が決定します。アプリケーションをお客様が開発・運用される場合は、お客様において各基準項目への対応が必要です。

本節においては、cloud.config for Financial Services の基本機能に関する各基準項目への対応を記載し、アプリケーションをお客様が開発・運用される場合のお客様の対応については記載を省略します。

5.3.1. 情報セキュリティ

表 3 情報セキュリティ 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 1～7	cloud.config for Financial Services では、お客様のデータを保護するために、Azure Active Directory によるアカウント管理や Network Security Group(NSG)を使用したアクセス制御、データの暗号化等を行います。 キャッシュカードや機器類等の物理的な対策は、お客様において本基準項目に対応する必要があります。
(2)	実 8～13	cloud.config for Financial Services では、Azure Active Directory によりアカウント管理を行い、不正使用を防止します。アクセス履歴はログを取得し、不正使用を迅速に検知します。
(3)	実 14～15	cloud.config for Financial Services では、Network Security Group(NSG)を使用したアクセス制御等、お客様の業務要件に合わせた不正アクセス防止措置を行います。また、不正アクセスを検知して防止する技術的手段を講じます。
(4)	実 16～18	cloud.config for Financial Services では、Azure Active Directory によりアカウント管理を行い、不正使用を防止します。アクセス履歴はログを取得し、不正使用を迅速に検知します。 機器類等の物理的な対策は、お客様において本基準項目に対応する必要があります。
(5)	実 19	cloud.config for Financial Services では、アクセス履歴のログを取得します。不正を検知した場合、取得したログを元に発生元、発生原因、影響範囲を特定します。 対応は、お客様と FIXER で分担して実施します。
(6)	実 20～22	cloud.config for Financial Services では、Azure に最適化した開発・運用方法を確立し、システムのライフサイクル全体において不正プログラム対策を実施します。 Azure 上に構築する仮想マシンには、ウイルス対策ソフトを導入します。

5.3.2. システム運用共通

表 4 システム運用共通 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 23～24	cloud.config for Financial Services の運用は、多くが自動化されています。自動化されていない部分については、運用マニュアルを作成し、それに則って運用します。

中項目	基準番号	cloud.config for Financial Services 対応
		また、障害時・災害時マニュアルおよび事業継続計画を策定し、定期的に見直しを行います。障害時・災害時等の対応は、お客様と FIXER で分担して実施します。
(2)	実 25～27	cloud.config for Financial Services では、Azure Active Directory によりアカウント管理を行い、アカウントに紐づけられた権限管理を行います。 パスワード管理およびアクセス権限管理については、お客様においても本基準項目への対応が必要です。
(3)	実 28～30	cloud.config for Financial Services では、Azure Active Directory によりアカウント管理を行い、データ授受・管理については、アカウントに紐づけられた権限管理を行います。暗号鍵は、Azure Key Vault 等を使用して安全に管理します。 データの取り扱い等の運用については、お客様においても本基準項目への対応が必要です。
(4)	実 31	cloud.config for Financial Services は、お客様の業務をフルスタックでサポートします。運用担当者は、定期的および必要に応じてオペレーションの教育・訓練を受けます。 システムの利用については、お客様においても本基準項目への対応が必要です。
(5)	実 32	cloud.config for Financial Services では、Azure Active Directory によるアクセス管理やウイルス対策ソフト等によりコンピューターウイルス等の不正プログラムを防御します。また、自動化されたセキュリティ監視により不正プログラムを検知し、問題が発生した場合は、原因と影響範囲を特定し、復旧を行います。 対応と復旧においては、お客様と FIXER との連携が必要となります。
(6)	実 33～34	Azure にアクセスするまでのネットワーク経路に関する契約については、お客様が回線事業者との間で協議する必要があります。

5.3.3. 運行管理

表 5 運行管理 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 35～38	cloud.config for Financial Services では、オペレーションの体制と権限を明確化し、確立した手順により実行します。また、オペレーションの記録を取得し、検証を行います。多くのオペレーションは自動化されます。 システムの利用については、お客様においても本基準項目への対応が必要です。
(2)	実 39	cloud.config for Financial Services では、Azure Backup 等を使用してデータのバックアップを取得し、管理を行います。 バックアップ要件の決定および見直しは、お客様と FIXER との連携が必要となります。
(3)	実 40～41	cloud.config for Financial Services のプログラムファイル管理は、開発から運用までがシームレスに連携します。プログラムリポジトリへのアクセス権限は厳密に管理されます。
(4)	実 42～43	cloud.config for Financial Services では、ネットワーク設定情報をコードとして管理します。 ネットワーク設定情報のバックアップは、Azure の機能により実現されます。
(5)	実 44～45	cloud.config for Financial Services では、運用の多くがコードにより自動化されています。 運用コードのバックアップは、Azure の機能により実現されます。
(6)	実 46	cloud.config for Financial Services では、運用するお客様のシステムの稼働状況やセキュリティアラートを 24 時間 365 日監視し、対応が必要と判断される場合には迅速に対応を行います。

5.3.4. 各種設備管理

表 6 各種設備管理 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 47	cloud.config for Financial Services では、お客様のシステムのリソース状況を随時モニタリングします。アラートが発生した場合は、スケーリング等の対応を行います。
(2)	実 48～52	cloud.config for Financial Services では、Azure のハードウェアおよび設備は、マイクロソフトの管理に依存します。 ソフトウェアの構成およびバージョンは、常に最新の状態が把

中項目	基準番号	cloud.config for Financial Services 対応
		握できるよう管理されます。 お客様が独自のハードウェアを保有し Azure と連携するシステムを構築する場合は、お客様独自のハードウェア部分については、お客様において本基準項目に対応する必要があります。
(3)	実 53～55	cloud.config for Financial Services では、Azure のハードウェアおよび設備は、マイクロソフトの管理に依存します。 お客様のシステムのリソース状況は随時モニタリングし、アラートが発生した場合は、スケーリング等の対応を行います。 お客様が独自の設備を保有し Azure と連携するシステムを構築する場合は、お客様独自の設備部分についてはお客様において本基準項目に対応する必要があります。
(4)	実 56～59	cloud.config for Financial Services では、Azure 関連施設の入退館(室)管理はマイクロソフトの管理に依存します。 FIXER は、cloud.config for Financial Services の運用エリアをセキュリティ区画とし、認証およびアクセス管理を行います。 お客様が独自の施設を保有する場合は、お客様独自の施設部分についてはお客様において本基準項目に対応する必要があります。
(5)	実 60	cloud.config for Financial Services では、Azure のハードウェアおよび設備は、マイクロソフトの管理に依存します。 お客様のシステムのリソース状況は随時モニタリングし、アラートが発生した場合は、スケーリング等の対応を行います。 お客様が独自の設備を保有し Azure と連携するシステムを構築する場合は、お客様独自の設備部分についてはお客様において本基準項目に対応する必要があります。

5.3.5. システムの利用

表 7 システムの利用 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 61～64	本基準項目は、cloud.config for Financial Services の対象外です。 アプリケーションの開発を FIXER が担当する場合は、本基準項目に対応する要件を提案します。
(2)	実 65～66	本基準項目は、cloud.config for Financial Services の対象外で

中項目	基準番号	cloud.config for Financial Services 対応
		す。 アプリケーションの開発を FIXER が担当する場合は、本基準項目に対応する要件を提案します。
(3)	実 67～68	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(4)	実 69	本基準項目は、cloud.config for Financial Services の対象外です。 アプリケーションの開発を FIXER が担当する場合は、本項目に対応する要件を提案します。

5.3.6. 緊急時の対応

表 8 緊急時の対応 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 70～72	cloud.config for Financial Services では、Azure の機能を利用してシステムの耐障害性を担保します。また、災害時対応計画を策定し、定期的に見直しを行います。 災害時対応計画の策定については、お客様においても本基準項目への対応が必要です。障害時・災害時の対応においては、お客様と FIXER との連携が必要となります。
(2)	実 73	cloud.config for Financial Services では、Azure の特性を考慮した事業継続計画を策定し、定期的に訓練を行います。 コンティンジェンシープランの策定については、お客様においても本基準項目への対応が必要です。
(3)	実 74	cloud.config for Financial Services では、Azure の複数リージョンを使用してシステムの可用性を確保します。Azure Site Recovery 等を使用したサイト復旧を行います。

5.3.7. システム開発・変更

表 9 システム開発・変更 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 75～77	cloud.config for Financial Services では、開発・テスト・デプロイがシームレスに連携されており、プロセスの多くが自動化されています。

中項目	基準番号	cloud.config for Financial Services 対応
		お客様の既存環境からの移行を FIXER が担当する場合は、本基準項目に対応する要件を提案します。
(2)	実 78～79	cloud.config for Financial Services では、アプリケーションの開発・保守を FIXER が担当する場合は、お客様との取り決めに基づき本基準項目に対応する方法でドキュメント管理を行います。 お客様が取り扱うドキュメントは、お客様において本基準項目に対応する必要があります。
(3)	実 80～81	本基準項目は、cloud.config for Financial Services の対象外です。
(4)	実 82～83	cloud.config for Financial Services では、システムの廃棄は Azure 上で完結します。廃棄手順に基づいて作業を行い、情報漏洩対策を講じます。 お客様が独自のシステムを保有し Azure と連携する場合は、お客様独自のシステム部分については、お客様において本基準項目に対応する必要があります。

5.3.8. システムの信頼性向上対策

表 10 システムの信頼性向上対策

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 84～88	cloud.config for Financial Services では、ハードウェアの予備は Azure に依存します。 お客様が独自の機器類等を保有する場合は、お客様において本基準項目に対応する必要があります。
(2)	実 89～98	cloud.config for Financial Services では、システムの構成要素は一元管理され、変更は全て承認を受けます。適用された変更は自動的にテストが行われ、本番環境へのデプロイの検証が行われます。
(3)	実 99～101	cloud.config for Financial Services では、開発から本番環境へのデプロイまでのプロセスの多くが自動化され、適切な検証が行われます。また、本番環境のリソース状況について監視を行います。
(4)	実 102～106	cloud.config for Financial Services では、お客様のシステムの稼働状況やセキュリティアラートを 24 時間 365 日監視し、対応

中項目	基準番号	cloud.config for Financial Services 対応
		が必要と判断される場合には迅速に対応を行います。 アプリケーションをお客様が開発・運用される場合は、お客様において本基準項目のうち業務要件に依存する部分への対応が必要です。

5.3.9. 個別業務・サービス

表 11 個別業務・サービス 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	実 107～111	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(2)	実 112～117	cloud.config for Financial Services では、システムの脆弱性管理を行い、適時に対応を行います。また、不正アクセスのモニタリングを行います。 利用者への対応事項は、お客様のサービスに関する内容であり、お客様において本基準項目への対応が必要です。
(3)	実 118	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(4)	実 119～124	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(5)	実 125	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(6)	実 126～131	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(7)	実 132～135	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(8)	実 136～137	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。
(9)	実 138～139	cloud.config for Financial Services では、サービスで送受信する電子メールについて、電子メール運用方針に則った運用を行います。 サービス提供にあたり、お客様にてメールの送受信が発生する場合は、お客様においても本基準項目への対応が必要です。
(10)	実 140～141	本基準項目は、cloud.config for Financial Services の対象外であり、お客様において本基準項目への対応が必要です。

5.4. 設備基準

cloud.config for Financial Services では、全ての機能において Azure を使用しています。Azure は、FISC 安全対策基準のうち設備基準の各項目に対応しているため、cloud.config for Financial Services およびお客様は、システムおよび関連設備について、本基準項目への対応は不要です。

なお、お客様が保有するオンプレミス環境と Azure の連携によりシステムを構築する場合は、Azure 以外の部分についてはお客様において設備基準への対応が必要です。また、CD・ATM 等の設備についても、お客様において設備基準への対応が必要です。

5.5. 監査基準

5.5.1. システム監査

表 12 システム監査 基準対応表

中項目	基準番号	cloud.config for Financial Services 対応
(1)	監 1	FIXER は、自己監査または専門知識を有する第三者監査人による監査を実施し、その結果をお客様に提供します。

6. まとめ

長らく安定性が最重視されてきた金融システムは、これからは変革し続けるビジネス環境に適応し、ユーザーに革新的な体験を提供し続けなければなりません。金融クラウドは、その前提条件です。

一方で、金融機関は、高度化・複雑化するサイバー攻撃から顧客資産と自社の事業を守るために、金融システムについて高度なセキュリティや信頼性を確保しなければなりません。FISC 安全対策基準は、最も包括的かつ実践的な基準のひとつです。

cloud.config for Financial Services は、Azure を活用したフルスタックサービスにおいて高度なセキュリティ対策を実現し、金融機関のデジタルトランスフォーメーションを全面的にサポートします。cloud.config for Financial Services は、FinTech 時代において金融機関が迅速かつ柔軟にビジネスを変革させていくためのベストソリューションです。