COMPANY Core
セキュリティスタンダード

公益財団法人 金融情報システムセンター
「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（第12版）」対応

Version 4.00

2025/04/11

株式会社Works Human Intelligence

目次

1. 改訂履歴

Version	改版内容	更新日
1.00	新規作成	2020/08/31
1.01	「2.5 補足事項」の修正	2021/02/03
1.10	第9版令和2年3月版対応	2021/03/12
1.20	第9版令和3年12月版対応	2022/06/10
2.00	第10版	2023/07/27
3.00	第11版	2024/06/28
4.00	第12版	2025/04/11

2. COMPANY Coreセキュリティスタンダード概要

ここではCOMPANY Coreセキュリティスタンダードの目的、対象範囲、策定手順を解説します。

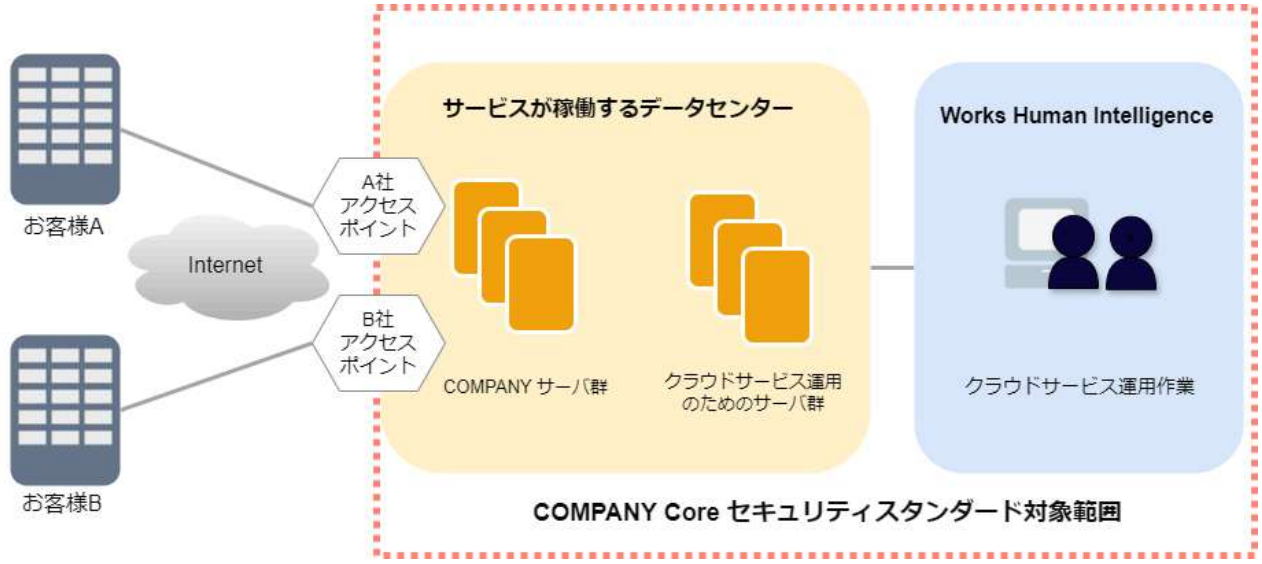
○2.1. 目的

- お客様に製品の安全性について確認して頂くための情報を提供します。
- COMPANY Coreクラウドサービス（以下、クラウドサービス）における安全対策の骨子を定めます。

○2.2. 対象範囲

- クラウドサービス
  アプリケーションのバージョンアップや PTF の適用を行う他、サービスが動作するサーバおよびサービスの提供に必要なミドルウェアの運用を行うサービスです。

○2.3. 対象範囲イメージ



クラウドサービスでは、クラウド事業者が提供するデータセンター (以下、クラウドサービスが稼働するデータセンター) 上にコンピュータシステムを構築します。お客様はサービスを利用するために、インターネット経由でお客様用のアクセスポイントに接続します。

クラウドサービスにおける運用作業は、弊社がリモート操作により実施します。COMPANY Coreセキュリティスタンダードでは、クラウドサービスが稼働するデータセンターおよび弊社でのクラウドサービス運用作業を対象範囲とします。

○2.4. 策定方針

- 「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」の考え方に基づきます。
- 弊社のセキュリティポリシーに則ります。
- ISO27001に基づいた情報セキュリティ管理を活用し、改善を図ります。
- 弊社が必要と定めた社会的要求およびお客様の要望を必要に応じ
  COMPANY Core セキュリティスタンダードに反映します。

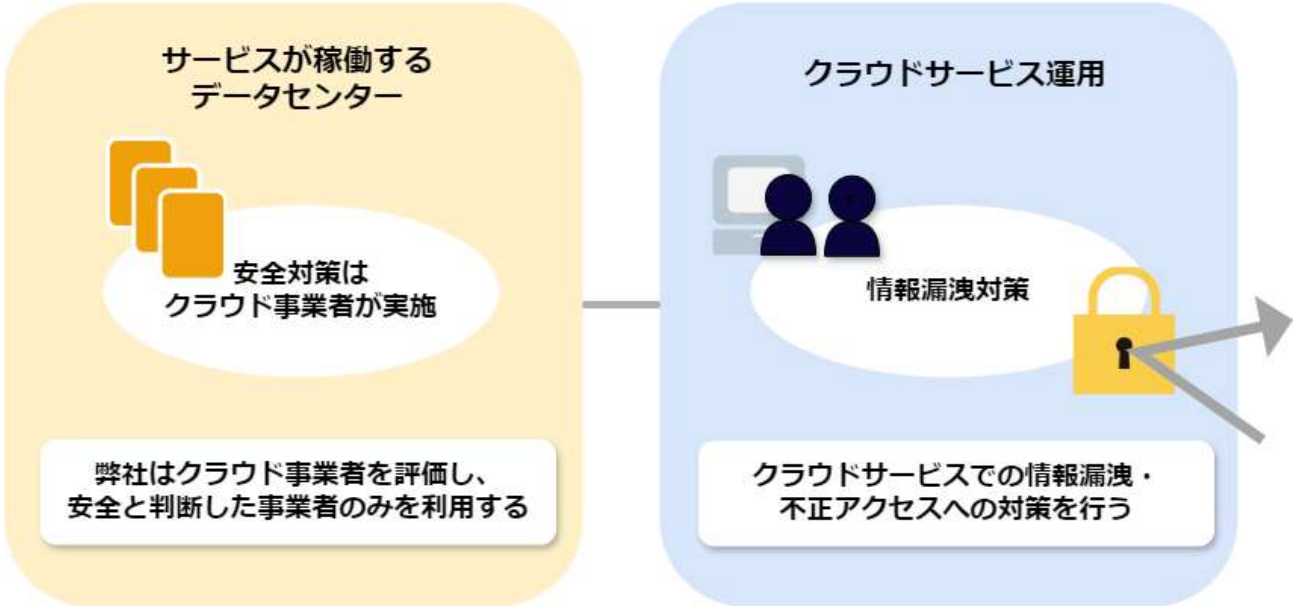
3. 安全対策の概要

ここではサービスの安全対策の概要を解説します。

○3.1. 設備および運用について

クラウドサービスが稼働するデータセンターの設備管理は、クラウド事業者に安全対策の責任があります。弊社ではクラウド事業者が行う安全対策を確認し、安全であると判断されたクラウド事業者のみを利用しています。

またクラウドサービスでは、弊社オペレーターがお客様の利用する環境を保守・運用しています。弊社では、不正な操作によるお客様情報の破壊や漏洩を防ぐため、責任者から承認を受けた担当者のみにオペレーション権限が付与され、作業終了後には権限が剥奪されるよう制御しています。



4. 金融機関等コンピュータシステムの安全対策基準・解説書への弊社およびクラウド事業者の対応

ここでは「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」に対してクラウドサービスを提供する弊社および、サービスが稼働するデータセンターを管理するクラウド事業者がどのように対応するのかを解説します。

○4.1. なぜクラウド事業者の対応状況も確認するのか

「2.2. 対象範囲」の通り、コンピュータシステムはクラウド事業者が管理するデータセンター上で稼働しています。このため、本書式のみでなくクラウド事業者の対応状況も併せて確認する必要があります。クラウド事業者の最新の対応状況は各事業者が公表している資料等をご確認ください。

○4.2. 対応状況表の見方

金融機関等コンピュータシステムの安全対策基準・解説書からの引用	対応状況
項番	
項目を一意に識別する識別記号	本項目に対して、クラウドサービスおよび弊社はどのような対応を行うか

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
統1	ISO27001を基準としたセキュリティに関する責任の分担、ポリシーおよび手順が確立されています。 同基準は運用業務の実態に合っているか定期的に見直しがされています。
統2	全社的に中長期的視点に立った計画の策定を実施しています。
統3	提供サービスの開発計画は、中長期のシステム化計画と整合性が取れており、技術調査を実施して、開発責任者の承認を得て、計画を作成しています。
統4	ISO27001を基準とした Works Human Intelligence のセキュリティポリシーで情報セキュリティの確保を目的として「情報セキュリティ委員会」を設置すると共に、情報セキュリティの責任者として情報セキュリティ管理責任者を選任するように定めています。
統5	クラウド事業者が提供する機能およびセキュリティ情報を追跡し、随時見直しを実施しています。 PSIRTの体制構築および運用も実施しており、セキュリティインシデントへの対策を整えています。 また、全役職員（派遣社員を含む）のセキュリティレベルの向上を図るために、情報セキュリティの維持に向けて必要な教育を継続的に実施しています。
統6	ISO27001の取り組みの一環で、管理する情報資産を情報資産管理台帳に定め、その資産に対してリスクの評価と対応策の策定を行っています。また、システム管理は Operation Manual に従い、整備しています。また、権限は互いに牽制ができるように付与されています。
統7	ISO27001の取り組みの一環で、管理する情報資産を情報資産管理台帳に定め、その資産に対してリスクの評価と対応策の策定を行っています。また、システム管理は Operation Manual に従い、整備しています。また、権限は互いに牽制ができるように付与されています。
統8	ISO27001の取り組みの一環で、「情報システム管理規程」および管理体制を整備しています。また、権限は互いに牽制ができるように付与されています。
統9	事業や、職務別（営業・開発・運用・コンサルタント）に組織が整備されており、それに合致するように権限が付与されています。また、権限は互いに牽制ができるように付与されています。
統10	災害時に、「事業継続管理規程」に基づき、対策本部を立ち上げる体制が整備されています。 また、クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
統11	弊社として防犯組織を明確に規定はしていませんが、各種防犯対策は実施しております。 また、クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、防犯対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
統12	情報セキュリティの確保を目的に、情報セキュリティ委員会を設置しています。その委員会にて、各種規定を整備しています。
統13	情報セキュリティが遵守されていることを点検するために、定期的に内部監査を実施しています。この監査による改善に加え、情報システムの変更や新たな脅威などの環境変化に対応した見直しを行い、継続的な改善を実施しています。 また、全役職員(派遣社員を含む)のセキュリティレベルの向上を図るために、周知徹底し、情報セキュリティの維持に向けて必要な教育を継続的に実施しています。
統14	全役職員(派遣社員を含む)に対して、入社入場時に加え、定期的なセキュリティ教育を（年1回以上）実施しています。業務内容により、追加の教育も実施しております。
統15	当社製品の開発、運用および利用に携わる要員(外部委託要員を含む)に対して、担当する業務内容等に応じた社内教育を実施しております。
統16	ISO27001に準拠し、障害時・災害時に備えた教育・訓練を実施しております。 また、クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
統17	非常時に備えて防災訓練を実施しております。 また、クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、防災・防犯対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
統18	人員毎のスキル評価を実施し、要員の配置、交替、権限分離等の人事管理を適時行っております。
統19	社内規程に従い定期的な健康診断および産業医による面談等を実施しております。
統20	プライバシーマークおよびISO27001 の管理策に基づき外部委託先の選定手続きを明確にしています。 外部委託先はホワイトペーパーおよび第三者機関による認証・レポート、提供している機能などで状況を確認、評価しています。 サービスをご利用中のお客様は、SOC1報告書にて弊社の統制状況をご確認いただけます。
統21	プライバシーマークおよびISO 27001の管理策に基づき契約を締結しています。
統22	外部委託先には弊社と同等の安全対策を行うことを要求した委託契約を結んでいます。その中には同等の教育および監査が含まれます。 また、クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
統23	外部委託先に委託した業務については、弊社内で評価・検証を行っております。
統24	お客様は弊社の統制について SOC1 報告書や本セキュリティスタンダードによってご確認頂き、安全対策を講じることが可能です。 お客様と弊社間の責任分界点は、クラウドサービス説明書に明示されています。 弊社では、お客様からのご依頼に基づき、接続元の制限やネットワーク設定等を行っています。依頼内容の妥当性については、お客様側でのご確認をお願いしています。
統25	緊急事態発生時に弊社が行う対応計画については、クラウドサービス説明書に定められています。 お客様はこれをご確認頂き、安全対策を講じることが可能です。
統26	クラウドサービスでは、金融サービスの提供は行っていません。 また、金融機関相互ネットワークへの接続もしていません。
統27	同上

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実1	クラウドサービスでは、暗証番号・パスワードは非表示・非印字としています。 また、既に利用していない運用者からは権限を剥奪し、利用を停止した運用者からの漏洩に対策しています。
実2	クラウドサービスでは、公衆通信網を通じて自動着信端末に金融情報を出力する機能は提供していません。
実3	蓄積データへの暗号化を実施しています。暗号化に際しては、電子政府推奨暗号リストに準拠したアルゴリズムを利用しています。
実4	クラウドサービスでは、異なるネットワーク間の通信はすべて適切な方式で暗号化されます。 暗号鍵は、クラウド事業者の提供する機能で管理しています。
実5	OSの備えるアクセス制限の方法を使用し、不正アクセス等からのデータ保護を行っています。
実6	クラウドサービスではデータ入力は行いませんが、アプリケーション、または、データベースの機能を用いて、不良データが入力されないようにしています。
実7	外部との通信は HTTPS 通信を利用しています。
実8	クラウドサービスでは、運用ツールの利用にあたり本人確認および接続元の確認を行っています。 またサービスが稼働するサーバへは、許可された接続元からの通信のみ許可するように設定しています。
実9	クラウドサービスでは、定期的に運用ツールのユーザ棚卸を実施しています。 またパスワードは、推測されにくい文字列を設定するようOperation Manual に定めており、漏洩による被害が大きいと考えられるツールについては、二段階認証等を用いて防御しています。 サービスが稼働するサーバへは、許可された接続元からの通信のみ許可するように設定しています。 なお、クラウド事業者から提供される管理者アカウントは、弊社にて厳格に管理しており、お客様へは公開しておりません。
実10	運用のためのツールはシステムやデータへのアクセス履歴が取得・保管され、定期的にチェックされています。 サービスにはアクセス履歴の管理機能が用意されています。 サーバ内に保管されるログは、定期的にバックアップが取得されます。その他のログについては、冗長性を確保した状況で保管されています。 なお、お客様がサービスを利用する際のログイン記録については、アプリケーションの機能としての提供となります。
実11	クラウドサービスでは、金融サービスの提供は行っていません。
実12	同上
実13	クラウドサービスでは、セキュリティを確保したプロセスに沿って、暗号鍵の管理に必要な要件を文書化し、運用しています。暗号アルゴリズムや鍵の長さについては、CRYPTREC推奨の暗号リストに掲載されている設定値を使用しています。 弊社ではクラウド事業者の提供する機能を利用して、これらの暗号鍵を厳格に管理・統制しており、改変や紛失から保護しています。 なお、COMPANY Coreクラウドサービスでは、暗号鍵の所有権は弊社が保持しております。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実14	クラウドサービスでは、クラウド事業者が提供する仮想プライベートネットワーク機能とファイアウォール機能を活用し、サーバー外部からの不正侵入を防止する策を講じています。 また情報セキュリティの遵守状況を確認するために定期的な内部監査を実施しており、監査結果に基づいた改善や情報システムの継続的な見直しも行っています。
実15	お客様が、クラウド事業者の管理インターフェースへアクセスすることは禁止しています。 また、クラウド事業者が提供する機能によって外部からアクセス可能な経路や機器はネットワークレベルで制限されています。
実16	クラウドサービスが稼働しているサーバにはセキュリティ対策ソフトウェアを導入し、ウイルス対策、侵入検知、侵入防御を行っています。 また、弊社の運用作業ではアクセス権限を制限し、ログイン失敗時の記録の取得を行っています。 なお、お客様によるアプリケーションのログイン記録は、アプリケーションの機能としての提供となります。
実17	クラウドサービスでは、金融サービスの提供は行っていません。
実18	同上
実19	不正アクセスを検知した場合には、サーバの停止、ネットワークの切り離し、ファイアウォール機能による通信の制御等を行い対処します。
実20	クラウドサービスでは、厳格なアクセス制御や通信の暗号化など不正侵入に対する重層的な防御策をとっております。もし不正プログラムの感染が検知された場合には、感染拡大を防ぐための対応措置を取ります。 バックアップについては、クラウド事業者により適切に保管されており、不正プログラムの発見時からシステム復旧までの対策も講じております。 なお、セキュリティ上の理由から操作手順の詳細については公開しておりません。
実21	同上
実22	同上
実23	弊社では、構築や運用などの各種手順に関するOperation Manual を整備しており、システムの変更が発生した場合など、必要に応じて手順を見直しています。 セキュリティ上の理由から、操作手順の詳細については公開していません。 また、COMPANYなどのアプリケーション操作に関するマニュアルは、弊社のサポートサイト上に公開しています。
実24	各種災害や大規模障害に対しては「事業継続管理規程」を制定しており、ISO27001の規定に基づいて、定期的に弊社の検証環境にて事業継続性の確認および手順の見直しを行っています。 また通常時障害対応についても、復旧作業の基本フローを確立し、Operation Manual として整備しています。
実25	クラウドサービスではアクセス管理のための台帳を作成し、アクセス可能な要員および職務に基づいたアクセス権のレベルを設定しており、定期的な見直しも行っています。 またサーバへのアクセス権は、作業ごとに作業報告書を提出し、責任者の承認を得た後に付与されるため、常にアクセス権限を持つオペレーターは存在しません。 なお、お客様による運用ツールや管理インターフェースへの操作は許可されていません。
実26	同上

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実27	同上
実28	お客様のデータを取り扱う際には、個人情報保護に関する社内規程や手引書に基づき、適切な対策を行います。 ただし、クラウドサービスではデータファイルの送受信は行っておらず、データファイルの修正や管理作業も行いません。 また、外部からアクセス可能な経路や機器については、クラウド事業者が提供する機能によってネットワークレベルで制限されています。
実29	同上
実30	COMPANY Coreクラウドサービスでは、セキュリティを確保したプロセスに沿って、暗号鍵の管理に必要な要件を文書化し、運用しています。暗号アルゴリズムや鍵の長さについては、CRYPTREC推奨の暗号リストに掲載されている設定値を使用しています。 弊社ではクラウド事業者の提供する機能を利用して、これらの暗号鍵を厳格に管理・統制しており、改変や紛失から保護しています。 なおセキュリティ上の理由により、詳細はお客様へ公開しておりません。
実31	オペレーションの習熟のため、手順書の作成および担当業務に応じた教育を実施しております。 なお、お客様による運用ツールや管理インターフェースへの操作は許可されていません。
実32	クラウドサービスが稼働しているサーバは、コンピュータウイルス等の不正プログラムに対する検知・防護策を講じています。 またバックアップについては、クラウド事業者により適切に保管されており、不正プログラムの発見時からシステム復旧までの対策も講じております。
実33	お客様とクラウド事業者間の接続の設備および回線は、クラウド事業者から提供されるものを除き、お客様で調達、構築および維持する契約となっております。
実34	相手先確認や接続条件(パスワード等)の登録・変更管理をISO27001に準じたOperation Manualで管理しています。 OS、ミドルウェアについても、定期的に脆弱性等を確認し、必要に応じて対応(パッチを適用する等)を実施しています。 また、外部からアクセス可能な経路や機器については、クラウド事業者が提供する機能によってネットワークレベルで制限されています。
実35	クラウドサービスでは、正当な権限がなければコンピュータシステムを使用できないようにオペレータの資格確認が行われています。
実36	クラウドサービスでは、コンピュータシステムのオペレーション実施依頼・権限付与依頼・権限付与の手続きは明文化されています。
実37	オペレーション実行体制はオペレーションの実行前に定められ、記録されています。定められた体制に従い、オペレーションを所定のオペレータが記録し、作業承認者が確認します。
実38	同上
実39	クラウドサービス説明書によって、サービスのバックアップおよび、データ破損時のリカバリについて定義しています。 バックアップ取得時には、データファイルだけでなく、利用するクラウド環境の設定情報も取得しています。
実40	バージョン管理システムを用いてプログラムファイルが管理されています。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実41	プログラムのバックアップを確保しています。このバックアップについては管理方法が定められています。
実42	クラウド事業者提供のコンソールから関連設定を変更する際には、変更手続きを経た上で実施しています。ネットワーク設定変更は、権限を持つ担当者のみが実施しています。
実43	サービスを提供するネットワーク設定の為のスクリプトがサービスのプログラムの一部として出荷ファイルに含まれ管理されています。 この出荷ファイルはバックアップが確保・管理されています。
実44	Operation Manual はバージョン管理システムで管理されていて、アカウントを付与されたものしか参照、編集できないものになっています。また、編集の際にはログが残るようになっています。
実45	復旧に必要なドキュメントは世代管理とバックアップが行われています。
実46	クラウドサービスでは、稼働状況やセキュリティ状況を常時監視し、異常を検知して通報します。また、必要に応じてリソースの調整やインシデント対応などを行います。 なお、クラウドサービスはSaaS形式での提供となり、しきい値等は非開示となります。 ※お客様が外部連携のために使用するサーバなどについては、クラウドサービスの責任範囲外です。
実47	同上
実48	クラウドサービスで利用するデータセンターの管理はクラウド事業者に依存しますが、定期的にハードウェアの管理や保守点検が実施されていることをクラウド事業者のFISC安全対策基準対応リファレンス等にて確認しています。 また、クラウドサービスのソフトウェアおよび、ソフトウェアの構成はバージョン管理システムで管理されており、周辺機器に関しても適切に管理を実施しております。 なお、クラウドサービスはSaaS形式での提供となり、システム構成の詳細は非開示となります。
実49	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、盗難や不正利用への対策が建物、敷地内にとられており、特にカスタマーデータを保持するエリアでは厳重な管理が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 また、クラウドサービスではアクセス管理のための台帳を作成し、サービスの資産にアクセスが可能な要員及びそれぞれの職務に基づいたアクセス権のレベルを設定しています。
実50	同上
実51	クラウドサービスで利用するデータセンターの管理はクラウド事業者に依存しますが、専門知識を有する担当者によって定期的に予防保守が実施され、設備の安定運用に努めていることをクラウド事業者のFISC安全対策基準対応リファレンス等にて確認しています。 また、クラウドサービスが稼働している論理リソースはモニタリングされ、異常事態が発生した場合は関係者に告知されます。
実52	同上
実53	同上
実54	同上
実55	同上

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実56	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、盗難や不正利用への対策が建物、敷地内にとられており、特にカスタマーデータを保持するエリアでは厳重な管理が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 また、システムへのアクセス権限についても、作業ごとに申請を提出し責任者の承認を得た後にのみ付与される仕組みとなっており、適切に管理しています。作業後には権限が剥奪されるため、常時アクセス権限を取得する者はいません。
実57	同上
実58	同上
実59	同上
実60	クラウドサービスで利用するデータセンターの管理はクラウド事業者に依存しますが、定期的にハードウェアの管理や保守点検が実施されていることをクラウド事業者のFISC安全対策基準対応リファレンス等にて確認しています。 クラウドサービスでは、稼働状況やセキュリティ状況を常時監視し、異常を検知して通報します。また、必要に応じてリソースの調整やインシデント対応などを行います。
実61	クラウドサービスでは、金融サービスの提供は行っていません。
実62	同上
実63	同上
実64	同上
実65	クラウドサービスでは、Operation Manual にてデータの入力手順を定めています。
実66	作業担当者は、作業報告を提出し責任者の承認を得た後に権限を付与されます。また、作業後に権限は剥奪されます。 作業内容はあらかじめ定められたものである他、作業報告書として記録されます。 自動実行ツールで行う作業の際にも、実行スケジュールは責任者の承認がなければ設定されません。また、作業内容はあらかじめ定められたものである他、作業ログが出力されます。
実67	クラウドサービスの運用作業では、未使用重要帳票の利用や管理、帳票の出力は行いません。
実68	同上
実69	クラウドサービスでは金融取引等において取得された金融機関等の顧客データについては、取り扱っておりません。 そのため顧客データの適正利用に関する管理は実施していません。
実70	障害時・災害時には、関係者へ連絡する方法が確立されています。 障害発生時のサポート内容については、クラウドサービス説明書に記載しています。
実71	クラウドサービスはSaaS形式での提供となり、システムの障害復旧作業は弊社で行います。 多くの障害は自動復旧システムにより復旧されますが、復旧できない場合の対応手順も規定しています。 また、ISO27001の規定に基づいて、定期的に弊社の検証環境で事業継続性を確認しています。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実72	検知した障害ごとに対応方法が確立されており、発生した障害の原因・対応方法を記録、管理しています。 クラウドサービスの利用に重大な影響を及ぼす状況が発生した場合には、サポート用WEBサイトで通知します。
実73	サービスの BCP に従い、策定しています。この BCP は定期的にテストされており、合わせて方法が適切であるかの見直しがされています。
実74	弊社では、複数の拠点を持つクラウド事業者を採用しており、お客様環境のあるデータセンターが利用不能になった場合には、別のデータセンターにサービスを復旧させます。 クラウドサービスはSaaSでのサービス提供となり、システム構成の詳細は非開示となりますが、サービスのRPO/RTOについては、クラウドサービス説明書に記載しています。
実75	クラウドサービスでは、各種手順を記載した Operation Manual を整備し、管理しています。
実76	クラウドサービスでは、本番環境とは論理的に分離されたテスト環境が構築されるため、お客様にてテスト環境で検証を行った後に、本番環境への適用を行うことが可能です。 なお、テスト環境は、機能確認のための最小構成にて準備されます。
実77	クラウドサービスには本番へ移行するためのスクリプトおよび手順書が含まれており、移行手順は明確になっています。また、これらはテストされた末に出荷され、その過程で整合性も確認されています。
実78	Operation Manual はドキュメントの範囲、体系、様式、記述方法が定められ明文化されています。
実79	Operation Manual はバージョン管理システムで管理しているため、改ざんはできません。
実80	お客様に向けて導入されるパッケージは社内で定められた基準に従い、評価部門によって評価されたのちに合格した物のみ出荷されます。アプリケーションの設定・運用方針はサービス利用者個々に設定変更が可能であり、有効性・信頼性・生産性に関する評価については、お客様にて行っていただく必要があります。
実81	クラウドサービスでは、トラブル対応および機能拡張の流れについてOperation Manual に定義しています。
実82	システムの廃棄については、クラウドサービス説明書に記載しています。 また弊社での廃棄手順についても、操作手順書を整備しています。
実83	データの破棄はクラウド事業者に依存していますが、デバイスの設置、修理、および破棄 の方法について厳格な基準が設けられていることを、クラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
実84	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
実85	同上
実86	同上
実87	同上
実88	同上

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実89	クラウドサービスの保守・運用・管理のためのツール群は全て評価を受け、必要な機能が取り込まれていることが確認されてから開発されています。 アプリケーションも同様に計画段階で評価を受け、機能が十分であることを確認したうえで開発が開始されます。
実90	同上
実91	クラウドサービスの保守・運用・管理のためのツール群及びアプリケーションは評価されたプログラム仕様書に基づいて開発されます。プログラム作成作業は標準化・自動化されており、これによって、ソフトウェアの品質は確保されます。
実92	クラウドサービスの保守・運用・管理のためのツール群、およびアプリケーションは定められたテストプロセスに従って評価されます。
実93	同上
実94	アプリケーションの機能およびお客様の既存システムとの整合性の確認はお客様が行う必要があります。
実95	クラウドサービスの運用における定型的作業は全て Operation Manual に従い、評価されたツールによって行われます。
実96	クラウドサービスの保守・運用・管理のためのツール群及びアプリケーションは定められたテストプロセスに従って評価され、合格したものだけがお客様に提供されます。
実97	クラウドサービスでは、アプリケーションが管理するファイルへアクセスはしません。
実98	同上
実99	クラウドサービスでは、監視やシステム起動などの一部の定型作業にオペレーションツールを導入し、システムの自動化・簡略化を図っています。 また、これらのツールは事前に設定値のチェックが行われ、運用試験に合格したもののみが採用されます。 データセンターのオペレーション等のセキュリティについては、クラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
実100	同上
実101	クラウドサービスでは、稼働状況やセキュリティ状況を常時監視し、異常を検知して通報します。 また、必要に応じてリソースの調整やインシデント対応などを行います。 なお、SaaSでのサービス提供となる為、詳細な設定値等は公開していません。
実102	障害の早期発見・回復のために、クラウドサービスではコンピュータシステムの運用状況(稼働状態、停止状態、エラー状態)を監視する機能を設けています。
実103	クラウドサービスでは、障害箇所に応じて復旧する機能を設けています。 また、クラウドサービスの利用に重大な影響を及ぼす状況が発生した場合には、サポート用WEBサイトで通知します。
実103-1	クラウドサービスを構成する重要なサーバは冗長化されており、障害により一部の処理が中断されてもシステム全体を停止することなく、運転が継続されます。 また、ISO27001の規定に基づいて、定期的に弊社の検証環境で事業継続性を確認しています。 なおクラウドサービスでは、金融サービスの提供および金融機関のオンラインシステムへの接続は行っていません。
実104	同上

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
実105	クラウドサービスでは、金融サービスの提供および周辺機器、キャッシュカード等の管理は行っていません。
実106	クラウドサービスでは、障害箇所に応じて復旧する機能を設けています。
実107	クラウドサービスでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。
実108	同上
実109	同上
実110	同上
実111	同上
実112	同上
実113	同上
実114	同上
実115	同上
実116	同上
実117	同上
実118	同上
実119	同上
実120	同上
実121	同上
実122	同上
実123	同上
実124	同上
実125	同上
実126	同上

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用 基準番号	対応状況
~~実127~~	（欠番）
~~実128~~	（欠番）
~~実129~~	（欠番）
~~実130~~	（欠番）
~~実131~~	（欠番）
実132	クラウドサービスでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。
実133	同上
実134	同上
実135	同上
実136	同上
実137	同上
実138	同上
実139	クラウドサービスでは、システム監視や定期的なセキュリティ教育の実施など、不正使用防止策を講じています。
実140	クラウドサービスでは、生体認証の利用および管理は行っていません。
実141	同上
実142	クラウドサービスでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。
実143	同上
実144	同上
実145	テレワークで使用するハードウェア及びソフトウェアについては、管理方針を策定し、テレワーク勤務者に周知しております。
実146	クラウドサービスにアクセスするためのアカウントには、多要素認証など不正なアクセスを防止するための対策を講じています。 不要になったアカウント及びアクセス権の削除を行うための仕組みは整備しておりますが、現在のところ、弊社ではテレワークを終了する予定はございません。
実147	テレワークにおける情報漏洩を防止するため、重要なデータの管理方針を定めております。 また通信の暗号化を含めた対策も講じております。
実148	テレワークにおける物理的な手段による情報漏洩やWeb会議での情報漏洩を防止するため、全役職員(派遣社員を含む)への注意喚起および対策を実施しております。

○4.3. 安全対策対応表

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 からの引用 基準番号	対応状況
設1	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 またデータセンターの場所は公表されておらず、外部からはそれとはわからないようになっています。
設2	同上
設3	同上
設4	同上
設5	同上
設6	同上
設7	同上
設8	同上
設9	同上
設10	同上
設11	同上
設12	同上
設13	同上
設14	同上
設15	同上
設16	同上
設17	同上
設18	同上
設19	同上
設20	同上

○4.3. 安全対策対応表

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 からの引用 基準番号	対応状況
設21	同上
設22	同上
設23	同上
設24	同上
設25	同上
設26	同上
設27	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられており、特にカスタマーデータを保持するエリアでは厳重な管理が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設28	同上
設29	同上
設30	同上
設31	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、自動火災検知および消火装置や、漏水検知デバイス等、各種災害、障害に対する対策が建物内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設32	同上
設33	同上
設34	同上
設35	同上
設36	同上
設37	同上
設38	同上
設39	同上

○4.3. 安全対策対応表

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 からの引用 基準番号	対応状況
設40	同上
設41	同上
設42	同上
設43	同上
設44	同上
設45	同上
設46	同上
設47	同上
設48	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、地震を含む各種災害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設49	同上
設50	同上
設51	同上
設52	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、自動火災検知および消火装置や、漏水検知デバイス等、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 また、データセンターの場所は公表されておらず、外部からはそれとは分からないようになっています。
設53	同上
設54	同上
設55	同上
設56	同上
設57	同上
設58	同上

○4.3. 安全対策対応表

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 からの引用 基準番号	対応状況
設59	同上
設60	
設61	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、地震を含む各種災害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設62	同上
設63	同上
設64	同上
設65	同上
設66	同上
設67	同上
設68	同上
設69	同上
設70	同上
設71	同上
設72	クラウドサービスで利用するデータセンターの管理はクラウド事業者に依存しますが、温度と湿度をモニタリングし制御することで、サーバの過熱を防止し、サービス停止を抑制することをクラウド事業者のFISC安全対策基準対応リファレンス等にて確認しています。
設73	同上
設74	同上
設75	同上
設76	同上
設77	同上
設78	同上

○4.3. 安全対策対応表

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 からの引用 基準番号	対応状況
設79	同上
設80	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、システムおよび設備の監視を行い、早急に対応する体制を整えていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設81	同上
設82	クラウドサービスで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、ネットワークケーブルの適切な保護が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 またデータセンターの場所は公表されておらず、外部からはそれとはわからないようになっています。
設83	同上
設83-1	同上
設備基準84～137 は「本部・営業店等」「流通・小売店舗との提携チャネル」の基準であり、対象外	

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書からの引用	対応状況
基準番号	
監1	ISO27001、27017、27701およびJISQ15001に基づき、システム等の運用監査体制を整備しております。 サービスをご利用中のお客様は、SOC1報告書にて弊社の統制状況をご確認いただけます。