

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)
統制基準					
1 内部の統制／内部の統制を行うために必要となる規程・体制の整備等に関する基準項目。					
(1) 方針・計画 システムの安全対策を適切に実施するために必要となる基本方針の整備及び必要な経営資源を考慮した中長期システム計画の策定に関する基準項目。	統 1	システムの安全対策に係る重要事項を定めた規程を整備すること。	必須	ISO27001規格に準拠している。「情報セキュリティ基本方針」を定め、それに基づき「ISMSマニュアル」など文書類を整備している。	適合
	統 2	中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること。	必須	システム開発計画は事業計画との整合性をとり、計画を策定している。	適合
	統 3	システム開発計画は中長期システム計画との整合性を確認するとともに、承認を得ること。	必須	システム開発計画は事業計画との整合性をとり、承認手続きが定められている。	適合
(2) 組織体制 システムの安全対策を適切に実施するために必要な組織体制の整備（責任者の選任、管理体制の整備、各種規則の整備等）に関する基準項目	統 4	セキュリティ管理体制を整備すること。	必須	「ISMSマニュアル」に定めている。	適合
	統 5	サイバー攻撃対応態勢を整備すること。	必須	定期的にリスク評価を実施している。また、「事業継続マネジメントマニュアル」を整備し、対応フローを整備している。	適合
	統 6	システム管理体制を整備すること。	必須	システムに関する管理体制を整備し、手順を文書化している。	適合
	統 7	データ管理体制を整備すること。	必須	データ管理に関する手順を文書化している。また、定期的にリスク評価を実施し、リスクに応じて対策を講じることを定めている。	適合
	統 8	ネットワーク管理体制を整備すること。	必須	ネットワークに関する管理体制を整備し、手順を文書化している。	適合
	統 9	業務組織を整備すること。	必須	基準の対策を講じている。	適合
	統 10	防災組織を整備すること。	必須	「事業継続に関する基本方針」を定め、それに基づき「事業継続マニュアル」を整備している。その中で、組織、責任者を明確にしている。	適合
	統 11	防犯組織を整備すること。	必須	防犯組織、責任者を明確にしている。（業務管理部）	適合
	統 12	各種業務の規則を整備すること。	必須	「業務分掌規程」、「ISMSマニュアル」、「事業継続マニュアル」、「業務手順書」を整備している。	適合
	(3) 管理状況の評価 セキュリティ関連の規程に定められた事項について、その遵守状況の確認及び評価に関する基準項目。	統 13	セキュリティ遵守状況を確認すること。	必須	ISMS活動の中で、情報セキュリティの遵守状況を定期的に確認している。全役員および全従業員の力量を定期的に確認している。
(4) 人材（要員・教育） システムの開発・運用等に携わる要員の人事管理及び健康管理並びに要員に対し実施するセキュリティ教育及び訓練に関する基準項目。	統 14	セキュリティ教育を行うこと。	必須	定期的に全役員および全従業員に対して教育を実施している。	適合
	統 15	要員に対するスキルアップ教育を行うこと。	必須	基準の対策を講じている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については適合性に「対象外」と記載しています)	
		統 16	障害時・災害時に備えた教育・訓練を行うこと。	必須	基準の対策を講じている。	適合
		統 17	防災・防犯訓練を行うこと。	必須	事業継続訓練、ビルの防災訓練を定期的実施している。	適合
		統 18	要員の人事管理を行うこと。	必須	基準の対策を講じている。	適合
		統 19	要員の健康管理を行うこと。	必須	従業員は健康診断を年1回受診している。	適合
2 外部の統制／外部の統制を行うために実施すべき外部委託管理等に関する基準項目。						
(1) 外部委託管理 外部委託管理を適切に行うために必要な、利用検討時、契約時、運用時における対策、管理体制の整備に関する基準項目。	統 20	外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。	必須	基準の対策を講じている。	適合	
	統 21	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。	必須	基準の対策を講じている。	適合	
	統 22	外部委託先の要員にルールを遵守させ、その遵守状況を確認すること。	必須	外部委託の契約の際には、セキュリティ状況を確認したうえで契約をしている。また、定期的に状況確認を実施している。	適合	
	統 23	外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。	必須	基準の対策を講じている。	適合	
	(2) クラウドサービスの利用 クラウドサービス固有のリスクを踏まえ、金融機関等が実施すべき対策及び考慮すべき事項に関する基準項目。	統 24	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。	必須	基準の対策を講じている。	適合
	(3) 共同センター 勘定系システムで共同センターを利用する場合における、緊急事態の発生に備えた安全対策に関する基準項目。	統 25	共同センターにおける緊急事態の発生に備えて安全対策を講ずること。	必須	共同センターの利用はない。対象外	対象外
	(4) 金融機関相互のシステム・ネットワークのサービス 金融機関相互のシステム・ネットワークのサービスを利用する場合において実施すべき対策及び考慮すべき事項に関する基準項目。	統 26	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。	必須	金融機関の業務は行っていない。対象外	対象外

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)
実務基準					
1 情報セキュリティ 顧客データ漏えい防止、改ざんの防止、システムの不正使用の防止等、情報セキュリティに関する基準項目。					
(1) データ保護 データの漏えい、破壊、改ざんの防止及び暗号鍵の適切な 管理等、データ保護に関する基準項目。	実 1	他人に暗証番号・パスワード等を知られないための対策を講 ずること。	必須	パスワード入力是非表示（オートコンプリート機能は無効） としている。	適合
	実 2	相手端末確認機能を設けること。	必須	公衆通信網を利用した自動着信は行っていない。対象外	対象外
	実 3	蓄積データの漏洩防止策を講ずること。	必須	不正アクセス、改ざん防止などのセキュリティ対策はしている が、蓄積データの暗号化は未対応	適合
	実 4	伝送データの漏洩防止策を講ずること。	必須	S H A - 2 による通信の暗号化している。	適合
	実 5	ファイルに対するアクセス制御機能を設けること。	必須	不正アクセスはIPS（不正侵入防御システム）により検知 している	適合
	実 6	不良データ検出機能を充実すること。	必須	不正アクセスはIPS（不正侵入防御システム）により検知 している	適合
	実 7	伝送データの改ざん検知策を講ずること。	必須	基準の対策を講じている。	適合
(2) 不正使用防止 不正取引、データやソフトウェアの改ざん等の防止、アクセス 権限の確認、利用範囲の制限等、システムの不正使用防 止に関する基準項目。	実 8	本人確認機能を設けること。	必須	本番環境へのアクセスは特定端末に制限し、IDは許可され た者のみに付与している。	適合
	実 9	ID の不正使用防止機能を設けること。	必須	本番環境へのアクセスは特定端末に制限し、IDは許可され た者のみに付与している。	適合
	実 10	アクセス履歴を管理すること。	必須	本番環境へのアクセスは特定端末に制限し、IDは許可され た者のみに付与している。アクセスログを取得し、定期的に 確認している。	適合
	実 11	取引制限機能を設けること。	必須	金融機関取引は行っていない。対象外	対象外
	実 12	事故時の取引禁止機能を設けること。	必須	カード、通帳、印鑑等は利用していない。対象外	対象外
	実 13	電子化された暗号鍵を蓄積する機器、媒体またはそこに含 まれるソフトウェアには、暗号鍵の保護機能を設けること。	必須	取得した鍵はセキュリティ管理されたサーバーに保管してい る。	適合
(3) 外部ネット ワークからの不正アクセス防止 ネットワークを介した外部からの不正アクセスの防止等、外 部からのアクセスにおいて実施すべき対策に関する基準項 目。	実 14	外部ネットワークからの不正侵入防止機能を設けること。	必須	インターネット接続環境にファイアウォールを設置している。	適合
	実 15	外部ネットワークからアクセス可能な接続機器は必要最小 限にすること。	必須	外部からアクセス可能な通信経路、通信関連機器等は最 小限としている。	適合
(4) 不正検知策 不正アクセスを早期に発見するための監視機能や異例取	実 16	不正アクセスの監視機能を設けること。	必須	不正侵入検知ツールにより監視している。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については適合性に「対象外」と記載しています)	
	引・不正取引の監視・検知等に関する基準項目。	実 17	異常な取引状況を把握するための機能を設けること。	必須	金融業務は行っていない。対象外	対象外
		実 18	異例取引の監視機能を設けること。	必須	金融業務は行っていない。対象外	対象外
	(5) 不正発生時の対応策 不正アクセス、不正使用を検知した際、被害の範囲を調査・特定し、被害の拡大を防止するとともに、システムの復旧を行うために実施すべき対策に関する基準項目。	実 19	不正アクセスの発生に備えて対応策、復旧策を講じておくこと。	必須	不正アクセスを検知した場合の対応策、復旧手順を定めたものは特になし。 データの改ざんが行われた場合、バックアップからの復旧が可能。	適合
	(6) 不正プログラム対策 システムの安全性確保を目的に、不正プログラム等のシステムへの侵入または組込みを防止するための対策に関する基準項目。	実 20	コンピュータウイルス等の不正プログラムへの防御対策を講ずること。	必須	不正侵入検知ツールにより監視している。	適合
		実 21	コンピュータウイルス等の不正プログラムの検知対策を講ずること。	必須	不正侵入検知ツールにより監視している。	適合
		実 22	コンピュータウイルス等の不正プログラムによる被害時対策を講ずること。	必須	「事業継続基本方針」を定めており、「事業継続マネジメントマニュアル」、対応フローを整備し、定期的に見直しを実施している。	適合
2 システム運用共通/システムの運用部門（主に委託先）及び利用部門（金融機関等）が実施すべき基準項目。						
(1) マニュアルの整備 システムを正確かつ安全に運用するための通常時及び障害・災害時における各種運用手順等のマニュアルの整備に関する基準項目。	実 23	通常時マニュアルを整備すること。	必須	基準の対策を講じている。	適合	
	実 24	障害時・災害時マニュアルを整備すること	必須	「事業継続に関する基本方針」を定め、それに基づき「事業継続マニュアル」を整備している。 障害や災害時の対応、復旧手順を文書化している。	適合	
(2) アクセス権限の管理 システムを構成する機器、データ等の各種資源に対する破壊及び不正使用を防止するためのアクセス権限の設定等に関する基準項目。	実 25	各種資源、システムへのアクセス権限を明確にすること。	必須	基準の対策を講じている。	適合	
	実 26	パスワードが他人に知られないための措置を講じておくこと。	必須	基準の対策を講じている。	適合	
	実 27	各種資源、システムへのアクセス権限の付与、見直し手続きを明確にすること。	必須	アクセス制御方針に基づき、権限の付与、見直し手続きの文書化をしている。	適合	
(3) データ管理 データファイルの不正使用、改ざん、紛失等を防止するために実施すべきデータファイルの授受・保管における管理手順及び暗号鍵の管理手順等に関する基準項目。	実 28	データファイルの授受・管理方法を明確にすること。	必須	データファイルの取扱いについて、手順を定めている。	適合	
	実 29	データファイルの修正管理方法を明確にすること。	必須	データファイルの取扱いについて、手順を定めている。	適合	
	実 30	暗号鍵の利用において運用管理方法を明確にすること。	必須	基準の対策を講じている。（I P S E C）	適合	
(4) オペレーション習熟 システムや端末の誤操作による事故を防止するために実施すべき、コンピュータセンター等におけるシステムのオペレーション及び営業店等における端末操作に関する教育・訓練に関する基準項目。	実 31	オペレーション習熟のための教育及び訓練を行うこと。	必須	基準の対策を講じている。	適合	

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
	(5) コンピュータウイルス対策 コンピュータウイルス等の不正プログラムによる情報漏えい、プログラムの改ざん、破壊等を防止するために実施すべき、不正プログラムの侵入防止策及び、侵入した場合の検知策に関する基準項目。	実 32	コンピュータウイルス対策を講ずること。	必須	基準の対策を講じている。	適合
	(6) 外部接続管理 不正アクセス、データ漏えい等の防止を目的とした、接続先の正当性の確認及び外部接続管理等に関する基準項目。	実 33	接続契約内容を明確にすること。	必須	基準の対策を講じている。	適合
		実 34	外部接続における運用管理方法を明確にすること。	必須	基準の対策を講じている。	適合
3 運行管理 日々のシステム運行にあたり、システムの運用部門（主に委託先）が実施すべき基準項目。						
	(1) オペレーション管理 システムの運用を安全・円滑に行うために必要となるオペレーション管理（作業依頼、承認、実行記録、結果確認等）に関する基準項目。	実 35	オペレータの資格確認を行うこと。	必須	アクセス制御方針に基づき、権限の付与、見直し手続きの文書化をしている。	適合
		実 36	オペレーションの依頼・承認手続きを明確にすること。	必須	アクセス制御方針に基づき、権限の付与、見直し手続きの文書化をしている。	適合
		実 37	オペレーション実行体制を明確にすること	必須	アクセス制御方針に基づき、権限の付与、見直し手続きの文書化をしている。	適合
		実 38	オペレーションの記録、確認を行うこと。	必須	操作ログを記録し、定期的な確認を行っている。	適合
	(2) データファイル管理 障害・災害、サイバー攻撃等による破壊・改ざんに備えて実施すべき、データファイルのバックアップ等に関する基準項目。	実 39	データファイルのバックアップを確保すること。	必須	データベースのバックアップを定期的に取得している。管理方法を手順書として文書化し、明確にしている。	適合
	(3) プログラム ファイル管理 プログラムファイルの適切な管理及び障害・災害等の発生に備えたプログラムのバックアップ等に関する基準項目。	実 40	プログラムファイルの管理方法を明確にすること。	必須	基準の対策を講じている。	適合
		実 41	プログラムファイルのバックアップを確保すること。	必須	データベースのバックアップを定期的に取得している。管理方法を手順書として文書化し、明確にしている。	適合
	(4) ネットワーク設定情報管理 ネットワーク設定情報の不正な改ざんを防止するために実施すべき、ネットワーク設定情報の管理障害・災害等の発生に備えたバックアップの確保に関する基準項目。	実 42	ネットワークの設定情報の管理を行うこと	必須	基準の対策を講じている。	適合
		実 43	ネットワークの設定情報のバックアップを確保すること。	必須	基準の対策を講じている。	適合
	(5) 運用時ドキュメント管理 不正使用、紛失等を防止するために実施すべき、ドキュメン	実 44	運用時のドキュメントの保管管理方法を明確にすること。	必須	文書管理規程により管理している。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については適合性に「対象外」と記載しています)	
	トの管理、障害・災害等の発生に備えたバックアップの確保に関する基準項目。	実 45	災害時の復旧対応に必要なドキュメントのバックアップを確保すること。	必須	基準の対策を講じている。	適合
	(6) 運行監視 異常状態の早期発見のために実施すべき、システムの運行監視に関する基準項目。	実 46	システムの運行状況の監視体制を整備すること。	必須	計画的に保守点検を実施している。また、ソフトウェアによるリアルタイム監視を行っている。	適合
4 各種設備管理 コンピュータ機器やコンピュータ関連設備の管理を行うために、システムの運用部門（主に委託先）が実施すべき基準項目。						
	(1) 資源管理 システムの障害、処理能力の低下を回避するために実施すべき、各種資源の容量・能力等の把握に関する基準項目。	実 47	各種資源の能力及び使用状況の確認を行うこと。	必須	基準の対策を講じている。	適合
	(2) 機器の管理 ハードウェア・ソフトウェア等の障害及び不正使用・破壊・盗難等の防止など、システムの信頼性向上のために実施すべき、コンピュータ本体及び周辺機器の障害発生等の抑制に関する基準項目。	実 48	ハードウェア及びソフトウェアの管理を行うこと。	必須	システムの導入、変更、廃棄について、手順を定め、文書化している。	適合
		実 49	機器の管理方法を明確にすること。	必須	基準の対策を講じている。	適合
		実 50	ネットワーク関連機器の保護措置を講ずること。	必須	基準の対策を講じている。	適合
		実 51	機器の保守方法を明確にすること。	必須	計画的に保守点検を実施している。また、ソフトウェアによるリアルタイム監視を行っている。	適合
		実 52	機器の予防保守を実施すること。	必須	計画的にメンテナンスを行っている。	適合
	(3) コンピュータ関連設備の 保守管理 コンピュータシステムを円滑に運用するために実施すべき、電源、空調、給排水、防災、防犯、監視回線関連等の設備の管理及び各種設備の容量・性能及び使用状況の把握に関する基準項目。	実 53	コンピュータ関連設備の管理方法を明確にすること。	必須	基準の対策を講じている。	適合
		実 54	コンピュータ関連設備の保守方法を明確にすること。	必須	基準の対策を講じている。	適合
		実 55	コンピュータ関連設備の能力及び使用状況の確認を行うこと。	必須	要求されたシステム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・調整している。	適合
	(4) 入退館（室）管理 不法侵入、危険物持込み、不法持出し等を防止するために実施すべき、コンピュータセンターやコンピュータ室等の重要な室における入退室管理及び入室者の作業管理に関する基準項目。	実 56	入館（室）の資格付与及び鍵の管理を行うこと。	必須	基準の対策を講じている。	適合
		実 57	入退館管理を行うこと。	必須	基準の対策を講じている。	適合
		実 58	入退室管理を行うこと。	必須	基準の対策を講じている。	適合
		実 59	入室後の作業を管理すること。	必須	基準の対策を講じている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については適合性に「対象外」と記載しています)	
	(5) 監視 異常状態の早期発見のために実施すべき、システムの稼働に必要な各種設備の稼働状況の監視等に関する基準項目。	実 60	各種設備の監視体制を整備すること。	必須	要求されたシステム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・調整している。	適合
5 システムの利用/システムの適切な利用及び顧客データを保護するために利用部門(金融機関等)が実施すべき基準項目。						
	(1) 取引の管理 端末機操作による不正、不当取引を防止するために実施すべき、取引の操作内容の記録・検証及び顧客からの届出の受付体制の整備に関する基準項目。	実 61	各取引の操作権限を明確にすること。	必須	基準の対策を講じている。	適合
		実 62	オペレータカードの管理を行うこと。	必須	オペレータカードは使用していない。対象外	対象外
		実 63	取引の端末機操作の内容を記録・検証すること。	必須	銀行業務は実施していない。対象外	対象外
		実 64	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。	必須	銀行業務は実施していない。対象外	対象外
	(2) 入出力管理 データの完全性を確保するために必要となるデータの入力管理ルール作成、出力情報の不正使用の防止及び顧客データを保護するために必要となる出力情報の管理ルールの作成に関する基準項目。	実 65	データの入力管理を行うこと。	必須	基準の対策を講じている。	適合
		実 66	出力情報の作成、取扱いについて、不正防止及び機密保護対策を講ずること。	必須	重要帳票の出力情報はない。対象外	対象外
	(3) 帳票管理 帳票の不正使用及び漏えいを防止するために実施すべき、帳票の管理及び廃棄手続きに関する基準項目。	実 67	未使用重要帳票の管理方法を明確にすること。	必須	未使用重要帳票はない。対象外	対象外
		実 68	重要な印字済帳票の取扱方法を明確にすること。	必須	重要な印字済帳票の取扱いはない。対象外	対象外
	(4) 顧客データ保護 顧客データを保護するために実施すべき、管理手順の策定及び管理体制の整備等に関する基準項目。	実 69	顧客データの保護策を講ずること。	必須	顧客受領データの取扱いについて、手順に定めている。	適合
	6 緊急時の対応/システムの管理部門、運用部門及び利用部門において、緊急事態の発生に備え実施すべき基準項目。					
	(1) 障害時・災害時対応策 システムの障害や災害時に顧客、本部・営業店等への影響を最小限にとどめ、かつ、早期復旧を図るために実施すべき、障害・災害時対応策に関する基準項目。	実 70	障害時・災害時の関係者への連絡手順を明確にすること。	必須	「情報セキュリティポリシー」、「事業継続方針」に従い、障害時、災害時の連絡手順を文書化している。	適合
		実 71	障害時・災害時復旧手順を明確にすること	必須	「情報セキュリティポリシー」、「事業継続方針」に従い、障害時、災害時の連絡手順を文書化している。	適合
		実 72	障害の原因を調査・分析すること。	必須	「情報セキュリティポリシー」、「事業継続方針」に従い、障害時、災害時の連絡手順を文書化している。	適合
	(2) コンティンジェンシープランの策定 障害・災害が発生した際に必要となる、コンティンジェンシープランの策定に関する基準項目。	実 73	コンティンジェンシープランを策定すること。	必須	事業継続マネジメントシステムを構築しており、災害発生時の対応計画を策定している。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
	(3) バックアップサイト コンピュータセンターが災害等により機能しなくなった場合に備えた、バックアップサイトの設置に関する基準項目。	実 74	バックアップサイトを保有すること。	必須	複数拠点の運用により対応している。	適合
7 システム開発・変更/システム開発部門が、システムの安全性を確保するために実施すべき基準項目。						
	(1) システム開発・変更管理 システム開発・変更における内容の正当性と本番システムの安全性を確保するために実施すべき、システム開発・変更手順及びテスト環境の整備に関する基準項目。	実 75	システムの開発・変更手順を明確にすること。	必須	基準の対策を講じている。	適合
		実 76	テスト環境を整備すること。	必須	基準の対策を講じている。	適合
		実 77	本番への移行手順を明確にすること。	必須	本番への移行手順を定め、文書化している。	適合
	(2) 開発・変更時ドキュメント管理 システム開発・変更作業を円滑に行うとともに、改ざん、不正使用を防止するために実施すべき、システム開発・変更に係わるドキュメントの管理に関する基準項目。	実 78	開発・変更時のドキュメントの作成手順を明確にすること。	必須	システムドキュメントの作成について、手順を定め文書化している。	適合
		実 79	開発・変更時のドキュメントの保管管理方法を明確にすること。	必須	システムドキュメントの保管について、改ざん、不正使用防止を適正に行っている。	適合
	(3) パッケージの導入 パッケージを導入する場合に実施すべき、パッケージの信頼性・生産性・既存システムとの親和性等の評価及びパッケージの運用・管理体制の整備に関する基準項目。	実 80	パッケージの評価体制を整備すること。	必須	システム導入時の手順を定め、文書化している。	適合
		実 81	パッケージの運用・管理体制を明確にすること。	必須	システム導入時に開発・変更について、手順を定め、文書化している。	適合
	(4) システムの廃棄 システムの廃棄時における情報漏えいの防止及び不正防止等のために実施すべき、廃棄計画の作成及び廃棄手順に関する基準項目。	実 82	システムの廃棄計画を策定するとともに、廃棄手順を明確にすること。	必須	システムの廃棄について、手順を定め、文書化している。	適合
		実 83	システム廃棄時の情報漏洩防止対策を講ずること。	必須	システムの廃棄について、手順を定め、文書化している。	適合
8 システムの信頼性向上対策/システムの安定運用及び品質向上など、システムの信頼性向上のために実施すべき基準項目。						
	(1) ハードウェアの予備 コンピュータシステムの信頼性を向上させるために実施すべき、ハードウェア構成の冗長化等に関する基準項目。	実 84	本体装置の予備を設けること。	必須	障害時の対応として、複数拠点に設備を設置している。	適合
		実 85	周辺装置の予備を設けること。	必須	障害時の対応として、複数拠点に設備を設置している。	適合
		実 86	通信系装置の予備を設けること。	必須	障害時の対応として、複数拠点に設備を設置している。	適合
		実 87	回線の予備を設けること。	必須	障害時の対応として、複数拠点に設備を設置している。	適合
		実 88	端末系装置の予備を設けること。	必須	障害時の対応として、複数拠点に設備を設置している。	適合
	(2) ソフトウェア等の品質向上対策 システムの信頼性向上のために実施すべき、設計工程や製造工程、本番適用段階におけるソフトウェアの品質向上に	実 89	必要となるセキュリティ機能を取り込むこと。	必須	システム計画段階において必要となるセキュリティ機能を考慮している。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については適合性に「対象外」と記載しています)	
	関する対策及びパッケージ等の利用にあたり検討すべき事項に関する基準項目。	実 90	設計段階におけるソフトウェアの品質を確保すること。	必須	開発業務の手順化、システム開発における各フェーズでのレビューを実施している。	適合
		実 91	プログラム作成段階における品質を確保すること。	必須	開発業務の手順化、システム開発における各フェーズでのレビューを実施している。	適合
		実 92	テスト段階におけるソフトウェアの品質を確保すること。	必須	開発業務の手順化、システム開発における各フェーズでのレビューを実施している。	適合
		実 93	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。	必須	サービス提供先へ事前に要件を伝え、環境等の準備を依頼している。	適合
		実 94	パッケージ導入にあたり、ソフトウェアの品質を確保すること。	必須	新規システム導入時は、業務手順に則り、選定レビューや試験を実施している。	適合
		実 95	定型的な変更作業時の正確性を確保すること。	必須	基準の対策を講じている。	適合
		実 96	機能の変更、追加作業時の品質を確保すること。	必須	基準の対策を講じている。	適合
		実 97	ファイルに対する排他制御機能を設けること。	必須	本番環境へのアクセスは特定端末に制限している。	適合
		実 98	ファイル突合機能を設けること。	必須	基準の対策を講じている。	適合
	(3) 運用時の信頼性向上対策 システムの運用時における信頼性向上を図るために実施する、オペレーションの自動化・簡略化及びシステムの処理結果の妥当性・正当性のチェック機能等の充実に関する基準項目。	実 99	オペレーションの自動化、簡略化を図ること。	必須	基準の対策を講じている。	適合
		実 100	オペレーションのチェック機能を充実すること。	必須	基準の対策を講じている。	適合
		実 101	負荷状態の監視制御機能を充実すること。	必須	負荷状態を監視し、必要に応じ対応している。	適合
	(4) 障害の早期発見・回復機能 障害が発生した際に、障害状況を検知・把握し、その影響を最小限に抑え、速やかに回復するための機能及び管理方法に関する基準項目。	実 102	システム運用状況の監視機能を設けること	必須	日次でシステム稼働状況を監視している。	適合
		実 103	障害の検出及び障害箇所の切り分け機能を設けること。	必須	日次でシステム稼働状況を監視している。	適合
		実 104	障害時の縮退・再構成機能を設けること。	必須	複数拠点の運用により対応している。	適合
		実 105	障害時の取引制限機能を設けること。	必須	金融機関取引は行っていない。対象外	対象外
実 106		障害時のリカバリ機能を設けること。	必須	複数拠点の運用により対応している。	適合	
9 個別業務・サービス/個別業務・サービスにおいて実施すべき基準項目。						
	(1) カード取引サービス カード取引サービスに係る事故・犯罪を防止し、安心・安全	実 107	カードの管理方法を明確にすること。	必須	カードを利用していない。対象外	対象外

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
	なサービスを提供するために実施すべき、カード管理及びカード取引の監視に関する基準項目	実 108	カード取引等に関する犯罪について注意喚起を行うこと。	必須	カードを利用していない。対象外	対象外
		実 109	CD・ATM 等の機械式預貯金取引における正当な権限者の取引を確保すること。	必須	銀行業務は実施していない。対象外	対象外
		実 110	指定された口座のカード取引監視方法を明確にすること。	必須	カードを利用していない。対象外	対象外
		実 111	カードの偽造防止対策のための技術的措置を講ずること。	必須	カードは利用していない。対象外	対象外
(2) インターネット・モバイルサービス 利用者との取引の安全性を確保するために実施すべき、インターネット・モバイルサービスにおける脅威への対策及びサービス利用における顧客への注意喚起等の対策に関する基準項目。	実 112	インターネット・モバイルサービスの不正使用を防止すること。	必須	金融取引サービスはおこなっていない。対象外	対象外	
	実 113	インターネット・モバイルサービスの使用状況を利用者が確認できるようにすること	必須	金融取引サービスはおこなっていない。対象外	対象外	
	実 114	インターネット・モバイルサービスの安全対策に関する情報開示をすること。	必須	金融取引サービスはおこなっていない。対象外	対象外	
	実 115	インターネット・モバイルサービスの顧客対応方法を明確にすること。	必須	金融取引サービスはおこなっていない。対象外	対象外	
	実 116	インターネット・モバイルサービスの運用管理方法を明確にすること。	必須	金融取引サービスはおこなっていない。対象外	対象外	
	実 117	インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと。	必須	銀行業務は実施していない。対象外	対象外	
(3) 渉外端末の管理 顧客データ保護及びシステム機器保護の観点から実施すべき、渉外端末等の可搬型端末の管理（端末の破損、紛失、盗難等に備えた対策等）に関する基準項目。	実 118	渉外端末の運用管理方法を明確にすること	必須	金融取引サービスはおこなっていない。対象外	対象外	
(4) CD・ATM等及び無人店舗の管理 CD・ATM 等及び無人店舗における犯罪の未然防止、システム機器等の保護に必要となる各種対策及び障害・災害や犯罪発生時の対応方法を定めたマニュアル等の整備に関する基準項目。	実 119	CD・ATM 等及び無人店舗の運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること。	必須	CD・ATMおよび無人店舗はない。対象外	対象外	
	実 120	無人店舗の監視体制を明確にすること。	必須	無人店舗はない。対象外	対象外	
	実 121	無人店舗の防犯体制を明確にすること。	必須	無人店舗はない。対象外	対象外	
	実 122	無人店舗の障害時・災害時の対応方法を明確にすること。	必須	無人店舗はない。対象外	対象外	
	実 123	無人店舗の関係マニュアルの整備を行うこと。	必須	無人店舗はない。対象外	対象外	

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
		実 124	CD・ATM 等の遠隔制御機能を設けること	必須	無人店舗はない。対象外	対象外
	(5) インストアブランチ インストアブランチにおける安全性を確保するために実施すべき、出店先地域やストアの選定基準等に関する基準項目。	実 125	インストアブランチの出店先の選定基準を明確にすること。	必須	インストアブランチはない。対象外	対象外
	(6) コンビニ ATM コンビニ ATM の利用者及びメンテナンス要員等の安全確保に関する基準項目。	実 126	コンビニ ATM の出店先の選定基準を明確にすること。	必須	コンビニ ATM はない。対象外	対象外
		実 127	コンビニ ATM の現金装填等メンテナンス時の防犯対策を講じること。	必須	コンビニ ATM はない。対象外	対象外
		実 128	コンビニ ATM の障害時・災害時対応手順を明確にすること。	必須	コンビニ ATM はない。対象外	対象外
		実 129	コンビニ ATM のネットワーク関連機器、伝送データの安全対策を講ずること。	必須	コンビニ ATM はない。対象外	対象外
		実 130	コンビニ ATM の所轄の警察及び警備会社等関係者との連絡体制を確立すること。	必須	コンビニ ATM はない。対象外	対象外
		実 131	コンビニ ATM の顧客に対して犯罪に関する注意喚起を行うこと。	対象外	コンビニ ATM はない。対象外	対象外
		(7) デビットカード・サービス デビットカード・サービスの安全性を確保するために実施すべき、サービスの提供形態に応じた情報処理センターや加盟店等との総合的な対策及び顧客がデビットカードを利用する際の安全性を確保するための顧客保護に関する基準項目。	実 132	デビットカード・サービスにおける安全対策を講ずること。	必須	デビットカードは利用していない。対象外
	実 133		デビットカードの口座番号、暗証番号等の安全性を確保すること。	必須	デビットカードは利用していない。対象外	対象外
	実 134		デビットカード利用時の顧客保護の措置を講ずること。	必須	デビットカードは利用していない。対象外	対象外
	実 135		デビットカード利用上の留意事項を顧客に注意喚起すること。	必須	デビットカードは利用していない。対象外	対象外
	(8) 前払式支払手段 プリペイドカード等の前払式支払手段を利用する際の安全性を確保するために実施すべき、不正検知等の対策及び不正利用に関する利用者への注意喚起等に関する基準項目。	実 136	前払式支払手段における機器及び媒体の盗難、破損等に伴い、利用者が被る可能性がある損失及び責任を明示すること。	必須	カードは利用していない。対象外	対象外
		実 137	前払式支払手段における電子的価値の保護機能、または不正検知の仕組みを設けること。	必須	カードは利用していない。対象外	対象外
	(9) 電子メール・イントラネットの利用 電子メールを利用したサービスを行う場合において必要とな	実 138	電子メールの運用方針を明確にすること。	必須	基準の対策を講じている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
	る運用方針の策定及び電子メールの送受信やホームページの閲覧等によるデータ漏えい等の発生を防止するために必要な対策に関する基準項目。	実 139	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。	必須	業務目的以外の電子メールの送受信やホームページの閲覧は禁止している。	適合
	(10) 生体認証 生体認証を用いる場合に必要となる、生体認証情報の入手・保管における安全管理及び生体認証の導入・運用において必要な対策に関する基準項目。	実 140	生体認証における生体認証情報の安全管理措置を講ずること。	必須	生体認証は用いていない。対象外	対象外
		実 141	生体認証の特性を考慮し、必要な安全対策を検討すること。	必須	生体認証は利用していない。対象外	対象外
	(11) QRコード決済 ・QRコード決済（読取り支払方式）に関する基準	実 142	QRコード決済の安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センター、加盟店等とともに安全対策を講ずること。	必須	QRコード決済は利用していない。対象外	対象外
		実 143	QRコード決済利用時の顧客保護の措置を講ずること。	必須	QRコード決済は利用していない。対象外	対象外
		実 144	QRコード決済利用上の留意事項を顧客に注意喚起すること。	必須	QRコード決済は利用していない。対象外	対象外

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
設備基準						
1 コンピュータセンター／コンピュータセンターの建物・付帯施設及び設備に関する基準項目。						
(1) 建物（環境） コンピュータセンターの建物において、障害・災害が発生した場合に被害を最小限にとどめ迅速に復旧させるために必要となる立地環境の調査、建物周囲の状況ごとに講ずるべき対策等に関する基準項目。	設 1	各種災害、障害が発生しやすい地域を避けること。	望ましい	弊社ではコンピュータセンターとして商用のデータセンターを利用している。災害等の影響の少ない立地にあるデータセンターを選定している。	適合	
	(2) 建物（周囲）	設 2	立地環境の変化に伴う災害及び障害の発生の可能性を調査し防止対策を講ずること。	望ましい	利用している、利用しようとしているデータセンターに対して定期的リスク評価を実施し、リスクに応じて対策を講ずることを定めている。リスク評価には、環境、災害を含めている。	適合
		設 3	敷地には通路を確保すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 4	隣接物との間隔を十分に取ること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 5	塀または柵及び侵入防止装置を設けること。	望ましい	利用しているデータセンターの外周に塀、柵はなく建物境界で入退館管理をおこなっている。	不適合
		設 6	看板等を外部に出さないこと。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 7	建物には避雷設備を設置すること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 8	建物はコンピュータシステム関連業務専用、または建物内においてコンピュータシステム関連業務専用の独立区画とすること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 9	敷地内の通信回線・電力線は、切断・延焼の防止措置を講ずること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
	(3) 建物（構造）	設 10	耐火建築物であること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 11	構造の安全性を有すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 12	外壁、屋根等は十分な防水性能を有すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 13	外壁等に強度を持たせること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
	(4) 建物（開口部）	設 14	窓には防火措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 15	防犯措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
		設 16	常時利用する出入口は1カ所とし、出入管理設備、防犯設備を設置すること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 17	非常口を設けること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 18	防水措置を講ずること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 19	出入口の扉は、十分な強度を持たせるとともに、錠を付けること。	必須	利用しているデータセンターは基準を満たしている。	適合
(5) 建物（内装等）	設 20	不燃材料及び防災性能を有するものを使用すること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 21	地震による内装等の落下・損壊の防止措置を講ずること。	望ましい	利用しているデータセンターは基準を満たしている。	適合	
(6) コンピュータ室・データ保管室（位置） コンピュータ室・データ保管室に収容されているネットワーク機器及びデータ記録媒体等の安全性を確保するために実施すべき自然災害または不正行為等に対する対策に関する基準項目。	設 22	災害を受けるおそれの少ない位置に設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 23	外部から容易に入れない位置に設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 24	室名等の表示は付さないこと。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 25	必要空間を確保すること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 26	専用の独立した室とすること。	必須	利用しているデータセンターは基準を満たしている。	適合	
(7) コンピュータ室・データ保管室（開口部）	設 27	常時利用する出入口は1カ所とし、前室を設けること。	望ましい	利用しているデータセンターは基準を満たしている。	適合	
	設 28	出入口の扉は、十分な強度を持たせるとともに、錠を付けること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 29	窓に防火、防水、破損防止措置を講じ、外部から室内の機器等が見えない措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 30	非常口、避難器具、誘導灯等を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合	
(8) コンピュータ室・データ保管室（構造・内装等）	設 31	独立した防火区画とすること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 32	漏水防止対策を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 33	静電気の防止措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合	
	設 34	内装等には不燃材料及び防災性能を有するものを使用すること。	必須	利用しているデータセンターは基準を満たしている。	適合	

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
(9) コンピュータ室・データ保管室 (設備)		設 35	地震による内装等の落下・損壊の防止措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 36	フリーアクセス床は地震時に損壊しない構造とすること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 37	自動火災報知設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 38	非常時の連絡装置を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 39	消火設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 40	ケーブルの難燃化、延焼防止措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 41	排煙設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 42	非常用照明設備、携帯用照明器具を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 43	水使用設備を設置しないこと。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 44	地震感知器を設置すること。	望ましい	利用しているデータセンターに基準を満たしていないものがある。	不適合
		設 45	出入口には出入管理設備、防犯設備を設置すること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 46	温湿度自動記録装置または温湿度警報装置を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 47	ネズミの害を防止する措置を講ずること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		(10) コンピュータ室・データ保管室 (コンピュータ機器、什器・備品)		設 48	什器・備品は不燃性とすること。	必須
設 49	静電気防止措置を講ずること。			必須	利用しているデータセンターは基準を満たしている。	適合
設 50	耐震措置を講ずること。			必須	利用しているデータセンターは基準を満たしている。	適合
設 51	運搬車等に固定装置を取り付けること。			必須	利用しているデータセンターは基準を満たしている。	適合
(11) 電源室・空調機械室 電源室及び空調機械室における障害等の早期発見と被害を最小限にとどめるための対策に関する基準項目。		設 52	災害を受けるおそれの少ない場所に設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 53	保守点検に必要な空間を確保すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 54	専用の独立した室とすること。	望ましい	利用しているデータセンターは基準を満たしている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
		設 55	無窓とし、錠を付けた扉を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 56	耐火構造とすること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 57	自動火災報知設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 58	ガス系消火設備を設置すること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 59	空調設備の漏水防止措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 60	ケーブル、ダクトからの延焼防止措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
	(12) 電源設備 停電、異常電圧、異常周波数、電源の瞬断過電流、漏電及び電源設備自体の障害によりシステムの運用に影響を及ぼさないための異常検知や災害等に対する対策に関する基準項目。	設 61	電源設備の容量には余裕を持たせること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 62	電源は複数回線で引き込むこと。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 63	良質な電力を供給する設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 64	自家発電設備、蓄電池設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 65	電源設備には避雷設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 66	電源設備には耐震措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 67	分電盤からコンピュータ機器への電源の引込みは専用とすること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 68	負荷変動の激しい機器との共用を避けること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 69	コンピュータシステムのアースは適切に施工すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 70	過電流、漏電により各機器に障害を及ぼさないよう措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 71	防災、防犯設備用の予備電源を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
	(13) 空調設備 空調設備を安定的に運用するための対策及び空調設備が建物外に設置されることを想定した外部からの侵入防止等の対策に関する基準項目。	設 72	空調設備の能力には余裕を持たせること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 73	空調設備は安定的に空気調和できる措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 74	空調設備はコンピュータ室専用とすること。	必須	利用しているデータセンターは基準を満たしている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
		設 75	空調設備の予備を設置すること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
		設 76	空調設備には自動制御装置、異常警報装置を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 77	空調設備には侵入、破壊防止対策を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 78	空調設備には耐震措置を講ずること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 79	空調設備の断熱材料、給排気口は不燃材料とすること。	必須	利用しているデータセンターは基準を満たしている。	適合
	(14) 監視制御設備 監視制御設備において必要となる、電源設備、空調設備、 防災設備、防犯設備等の監視機能及び異常等の速やかな 発見・通報等を可能とするための対策に関する基準項目	設 80	監視制御設備を設置すること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 81	中央管理室を設置すること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
	(15) 回線関連設備 回線関連設備において必要となる、通信回線の保護策及び システムへの不正アクセス等を防止するための対策に関する 基準項目	設 82	回線関連設備には錠をつけること。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 83	回線関連設備の設置場所の表示は付さないこと。	必須	利用しているデータセンターは基準を満たしている。	適合
		設 83-1	回線は、専用の配線スペースに設けること。	望ましい	利用しているデータセンターは基準を満たしている。	適合
2 本部・営業店等／本部・営業店等の建物・付帯施設及び設備に関する基準項目。						
	(1) 建物（周囲） 本部・営業店等において実施すべき、設備面の対策及び自動 機器等の無人運用を行う場合（店舗外現金自動設備 を含む）における、周辺環境を考慮した防犯・防災対策に 関する基準項目。	設 84	敷地内の通信回線・電力線の切断・延焼の防止措置を講 ずること。	望ましい	基準の対策を講じている。	適合
	(2) 建物（構造）	設 85	耐火建築物であること。	望ましい	基準を満たしている。	適合
		設 86	構造の安全性を有すること。	必須	基準を満たしている。	適合
		設 87	外壁、屋根等は十分な防水性能を有すること。	必須	基準を満たしている。	適合
		設 88	外壁等の強度を確保すること。	望ましい	本部・営業店は3階以上にあり、公道等の外部から外壁を 破壊し、侵入されるリスクはない。	適合
	(3) 建物（開口部）	設 89	窓には防火措置を講ずること。	必須	基準を満たしている。	適合
		設 90	窓・扉には防犯措置を講ずること。	必須	基準の対策を講じている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
		設 91	出入口の扉は十分な強度を持たせるとともに、錠を付けること。	必須	基準の対策を講じている。	適合
		設 92	通用口には、入室者の識別設備を設置すること。	必須	基準の対策を講じている。	適合
		設 93	出入口には防水措置を講ずること。	望ましい	基準の対策を講じている。	適合
	(4) 建物（内装等）	設 94	天井及び壁は、遮熱、吸音機能を持たせること。	望ましい	基準の対策を講じている。	適合
		設 95	地震による内装等の落下・損壊の防止措置を講ずること。	必須	基準の対策を講じている。	適合
		設 96	床表面は、塵埃や静電気が発生しにくい材質のものとする こと。	望ましい	基準の対策を講じている。	適合
		設 97	端末機器への回線等は、切断のおそれのない措置を講ず ること。	必須	基準の対策を講じている。	適合
		設 98	端末機器に接続している回線、電源ケーブル等への漏水防 止対策を講ずること。	望ましい	基準の対策を講じている。	適合
	(5) 建物（設備）	設 99	自動火災報知設備及び消火器を設置すること。	必須	基準の対策を講じている。	適合
		設 100	設備等の耐震措置を講ずること。	望ましい	基準の対策を講じている。	適合
		設 101	耐火金庫を設置すること。	必須	基準の対策を講じている。	適合
		設 102	避雷設備を設置すること。	望ましい	基準の対策を講じている。	適合
		設 103	防犯措置を講ずること。	必須	基準の対策を講じている。	適合
	(6) 建物（回線関連設備）	設 104	回線関連設備の設置場所の表示は付さないこと。	必須	基準の対策を講じている。	適合
		設 105	回線関連設備には錠を付けること。	必須	基準の対策を講じている。	適合
		設 106	回線関連設備から各端末機器までの配線を二重化する こと。	望ましい	基準の対策を講じている。	適合
	(7) 建物（電源設備）	設 107	電源ケーブルは、端末機器等に支障を来さないよう布設す ること。	必須	基準の対策を講じている。	適合
		設 108	防災、防犯設備用の予備電源を設置すること。	必須	基準の対策を講じている。	適合

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
		設 109	自家発電設備等を設置すること。	望ましい	基準の対策を講じている。(蓄電池内蔵の無停電電源装置)	適合
	(8) 建物 (空調設備)	設 110	空調設備を設置すること。	必須	基準の対策を講じている。	適合
	(9) 建物 (自動機器室)	設 111	通話装置を設置すること。	必須	ATM等の自動機器室はない。対象外	対象外
		設 112	非常通報装置を設置すること。	必須	ATM等の自動機器室はない。対象外	対象外
		設 113	防犯措置を講ずること。	必須	ATM等の自動機器室はない。対象外	対象外
		設 114	照明設備及び非常用照明設備を設置すること。	必須	ATM等の自動機器室はない。対象外	対象外
		設 115	扉は、一部を素通しにすること。	必須	ATM等の自動機器室はない。対象外	対象外
		設 116	自動機器の現金の装填と保守のための必要な空間を確保すること。	望ましい	ATM等の自動機器室はない。対象外	対象外
		設 117	自動運行設備を設置すること。	望ましい	ATM等の自動機器室はない。対象外	対象外
		(10) 建物 (端末機器)	設 118	端末機器には耐震措置を講ずること。	望ましい	重量のある装置に転倒防止措置を講じている。
	設 119		機器のアースを確実に取ること。	必須	基準の対策を講じている。	適合
	設 120		漏水及び塵埃等に対する保護措置をとること。	望ましい	基準の対策を講じている。	適合
	(11) サーバ-設置場所 (位置) 本部・営業店等に設置されるシステムにおいて、サーバ-等の盗難・破壊等を想定した、サーバ-設置等において考慮すべき事項に関する基準項目。	設 121	災害を受けるおそれの少ない位置とすること。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外
		設 122	外部から容易に入れない位置とすること。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外
		設 123	室名等の表示は付さないこと。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外
		設 124	専用の区画とすること。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外
	(12) サーバ-設置場所 (構造・内装等)	設 125	防火区画に設置すること。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外
		設 126	漏水防止対策を講ずること。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外
		設 127	フリーアクセス床は地震に備えて耐震措置を講ずること。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外
	(13) サーバ-設置場所 (設備)	設 128	消防設備を有すること。	望ましい	本部・営業店にはサーバ-は設置していない。対象外	対象外

基準大項目	基準中項目	基準番号	基準小項目	必須or 望ましい	当社の対応状況及び適合性判断 (当社は金融機関ではないため、対応する必要がないと判断した基準については 適合性に「対象外」と記載しています)	
		設 129	地震感知器を設置すること。	望ましい	本部・営業店にはサーバーは設置していない。対象外	対象外
		設 130	サーバーを設置した室の出入口には出入管理設備、防犯設備を設置すること。	望ましい	本部・営業店にはサーバーは設置していない。対象外	対象外
		設 131	温湿度自動記録装置または温湿度警報装置を設置すること。	望ましい	本部・営業店にはサーバーは設置していない。対象外	対象外
		設 132	空調設備を設置すること。	望ましい	本部・営業店にはサーバーは設置していない。対象外	対象外
		設 133	ネズミの害を防止する措置を講ずること。	望ましい	本部・営業店にはサーバーは設置していない。対象外	対象外
		設 134	電源コンセントの抜け防止対策を講ずること。	必須	本部・営業店にはサーバーは設置していない。対象外	対象外
	(14) インストアブランチ インストアブランチにおいて、ストアの既設設備の利用または、ストア等との営業時間が異なる場合があることを想定した、設備の防犯対策、破壊侵入等の防御に関する基準項目。	設 135	他の区画からの侵入防止措置を講ずること。	必須	インストアブランチはない。対象外	対象外
	設 136	使用するストアの設備状況に応じて、適切な補強策を講ずること。	必須	インストアブランチはない。対象外	対象外	
3 流通・小売店舗との提携チャネル／流通・小売店舗等と提携してサービスを提供する場合の建物・付帯施設及び設備に関する基準項目。						
	(1) コンビニ ATM コンビニ ATM の特性として、不特定多数の人が行き来する場所に機器が単体で設置されることが多い点を踏まえた、強化すべき防犯対策に関する基準項目。	設 137	防犯措置を講ずること。	必須	ATMはない。対象外	対象外
監査基準						
1 システム監査／システムの監査体制の整備に関する基準項目。						
	(1) システム監査 システムの有効性、効率性、信頼性、遵守性、安全性を確保するために必要となる、システム監査体制の整備に関する基準項目。	監1	システム監査体制を整備すること。	必須	定期的に内部監査および外部監査により状況を確認している。	適合