FISC安全対策基準 第9版改訂版 対外公開ドキュメント『1/3』

基準大項目	基準中項目	項番	基準小項目	ウイングアーク1stの回答
1 内部の統制	(1) 方針・計画	統1	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。	ウイングアーク1stでは、ISO27001に基づき、関連する文書類、ルールを整備しています。 また、独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		統2	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。	
		統3	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。	
	(2) 組織体制	統4	統4 セキュリティ管理体制を整備すること。	ウイングアーク1stでは、ISO27001に基づき、関連する文書類、ルールを整備しています。 また、独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		統5	統5 サイバー攻撃対応態勢を整備すること。	
		統6	統6 システム管理体制を整備すること。	
		統7	統7 データ管理体制を整備すること。	
		統8	統8 ネットワーク管理体制を整備すること。	
		統9	統9 業務組織を整備すること。	
		統10	統10 防災組織を整備すること。	
		統11	統11 防犯組織を整備すること。	
		統12	統12 各種業務の規則を整備すること。	
	(3) 管理状況の評価	統13	統13 セキュリティ遵守状況を確認すること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(4) 人材(要員・教育)	統14	統14 セキュリティ教育を行うこと。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		統15	統15 要員に対するスキルアップ教育を行うこと。	
		統16	統16 障害時・災害時に備えた教育・訓練を行うこと。	
		統17	統17 防災・防犯訓練を行うこと。	
		統18	統18 要員の人事管理を行うこと。	
		統19	統19 要員の健康管理を行うこと。	
2 外部の統制	(1) 外部委託管理	統20	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		統21	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。	
		統22	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。	
		統23	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。	
	(2) クラウドサービスの利用	統24	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
1 情報セキュリティ	(1) データ保護	実3	実3 蓄積データの漏洩防止策を講ずること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実5	実5 ファイルに対するアクセス制御機能を設けること。	
		実6	実6 不良データ検出機能を充実すること。	
	(2) 不正使用防止	実8	実8 本人確認機能を設けること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実9	実9 IDの不正使用防止機能を設けること。	
		実10	実10 アクセス履歴を管理すること。	
		実13	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。	
	(3) 外部ネットワークからの不正アクセス防止	実14	実14 外部ネットワークからの不正侵入防止策を講ずること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(5) 不正発生時の対応策	実19	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(6) 不正プログラム対策	実20	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実21	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。	
		実22	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。	
2 システム運用共通	(1) マニュアルの整備	実23	実23 通常時マニュアルを整備すること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実24	実24 障害時・災害時マニュアルを整備すること。	
	(2) アクセス権限の管理	実25	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実26	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。	
		実27	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。	
	(3) データ管理	実28	実28 データファイルの授受・管理方法を明確にすること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実29	実29 データファイルの修正管理方法を明確にすること。	
	(4) オペレーション習熟	実31	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(5) コンピュータウイルス対策	実32	実32 コンピュータウイルス対策を講ずること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(6) 外部接続管理	実34	実34 外部接続における運用管理方法を明確にすること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
3 運行管理	(1) オペレーション管理	実35	実35 オペレータの資格確認を行うこと。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実36	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。	
		実37	実37 オペレーション実行体制を明確にすること。	
		実38	実38 オペレーションの記録、確認を行うこと。	
	(2) データファイル管理	実39	実39 データファイルのバックアップを確保すること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(3) プログラムファイル管理	実40	実40 プログラムファイルの管理方法を明確にすること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実41	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。	
	(4) ネットワーク設定情報管理	実42	実42 ネットワークの設定情報の管理を行うこと。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実43	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。	
	(5) 運用時ドキュメント管理	実44	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実45	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。	
	(6) 運行監視	実46	実46 システムの運行状況の監視体制を整備すること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
4 各種設備管理	(1) 資源管理	実47	実47 各種資源の能力及び使用状況の確認を行うこと。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(2) 機器の管理	実48	実48 ハードウェア及びソフトウェアの管理を行うこと。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実49	実49 機器の管理方法を明確にすること。	
		実50	実50 ネットワーク関連機器の保護措置を講ずること。	
		実51	実51 機器の保守方法を明確にすること。	
		実52	実52 機器の予防保守を実施すること。	
	(4) 入退館(室)管理	実56	実56 入館(室)の資格付与及び鍵の管理を行うこと。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実57	実57 入退館管理を行うこと。	
		実58	実58 入退室管理を行うこと。	
		実59	実59 入室後の作業を管理すること。	
5 システムの利用	(4) 顧客データ保護	実69	実69 顧客データの保護策を講ずること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
6 緊急時の対応	(1) 障害時・災害時対応策	実70	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実71	実71 障害時・災害時復旧手順を明確にすること。	
		実72	実72 障害の原因を調査・分析すること。	

FISC安全対策基準 第9版改訂版 対外公開ドキュメント『2/3』

基準大項目	基準中項目	項番	基準小項目	ウイングアーク1stの回答
6 緊急時の対応	(2) コンティンジェンシープランの策定	実73	実73 コンティンジェンシープランを策定すること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
	(3) バックアップサイト	実74	実74 バックアップサイトを保有すること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
7 システム開発・変更	(1) システム開発・変更管理	実75	実75 システムの開発・変更手順を明確にすること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実76	実76 テスト環境を整備すること。	
		実77	実77 本番への移行手順を明確にすること。	
	(2) 開発・変更時ドキュメント管理	実78	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実79	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。	
	(3) パッケージの導入	実80	実80 パッケージの評価体制を整備すること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実81	実81 パッケージの運用・管理体制を明確にすること。	
	(4) システムの廃棄	実82	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。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実83	実83 システム廃棄時の情報漏洩防止対策を講ずること。	
8 システムの信頼性向上対策	(1) ハードウェアの予備	実84	実84 本体装置の予備を設けること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実85	実85 周辺装置の予備を設けること。	
		実86	実86 通信系装置の予備を設けること。	
		実87	実87 回線の予備を設けること。	
		実88	実88 端末系装置の予備を設けること。	
	(2) ソフトウェア等の品質向上対策	実89	実89 必要となるセキュリティ機能を取り込むこと。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実90	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。	
		実91	実91 プログラム作成段階における品質を確保すること。	
		実92	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。	
		実93	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。	
		実94	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。	
		実95	実95 定型的な変更作業時の正確性を確保すること。	
		実96	実96 機能の変更、追加作業時の品質を確保すること。	
		実97	実97 ファイルに対する排他制御機能を設けること。	
		実98	実98 ファイル突合機能を設けること。	
	(3) 運用時の信頼性向上対策	実99	実99 オペレーションの自動化、簡略化を図ること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実101	実101 負荷状態の監視制御機能を充実すること。	
	(4) 障害の早期発見・回復機能	実102	実102 システム運用状況の監視機能を設けること。	独立した監査機関によりFISCの当該項目が検証され、要件を満たしていることが確認されています。
		実103	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。	
		実104	実104 障害時の縮退・再構成機能を設けること。	
		実106	実106 障害時のリカバリ機能を設けること。	
1 コンピュータセンター	(1) 建物(環境)	設1	設1 各種災害、障害が発生しやすい地域を避けること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
	(2) 建物(周囲)	設2	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。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設3	設3 敷地には通路を確保すること。	
		設4	設4 隣接物との間隔を十分に取ること。	
		設5	設5 塀または柵及び侵入防止装置を設けること。	
		設6	設6 看板等を外部に出さないこと。	
		設7	設7 建物には避雷設備を設置すること。	
		設8	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。	
		設9	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。	
	(3) 建物(構造)	設10	設10 耐火建築物であること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設11	設11 構造の安全性を有すること。	
		設12	設12 外壁、屋根等は十分な防水性能を有すること。	
		設13	設13 外壁等に強度を持たせること。	
	(4) 建物(開口部)	設14	設14 窓には防火措置を講ずること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設15	設15 防犯措置を講ずること。	
		設16	設16 常時利用する出入口は1カ所とし、入退館管理設備、防犯設備を設置すること。	
		設17	設17 非常口を設けること。	
		設18	設18 防水措置を講ずること。	
		設19	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。	
	(5) 建物(内装等)	設20	設20 不燃材料及び防炎性能を有するものを使用すること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設21	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。	
	(6) コンピュータ室・データ保管室(位置)	設22	設22 災害を受けるおそれの少ない位置に設置すること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設23	設23 外部から容易に入れない位置に設置すること。	
		設24	設24 室名等の表示は付さないこと。	
		設25	設25 必要空間を確保すること。	
		設26	設26 専用の独立した室とすること。	
	(7) コンピュータ室・データ保管室(開口部)	設27	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。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設28	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。	
		設29	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。	
		設30	設30 非常口、避難器具、誘導灯等を設置すること。	

FISC安全対策基準 第9版改訂版 対外公開ドキュメント『3/3』

基準大項目	基準中項目	項番	基準小項目	ウイングアーク1stの回答
1 コンピュータセンター	(8) コンピュータ室・データ保管室(構造・内装等)	設31	設31 独立した防火区画とすること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設32	設32 漏水防止対策を講ずること。	
		設33	設33 静電気の防止措置を講ずること。	
		設34	設34 内装等には不燃材料及び防炎性能を有するものを使用すること。	
		設35	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。	
		設36	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。	
	(9) コンピュータ室・データ保管室(設備)	設37	設37 自動火災報知設備を設置すること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設38	設38 非常時の連絡装置を設置すること。	
		設39	設39 消火設備を設置すること。	
		設40	設40 ケーブルの難燃化、延焼防止措置を講ずること。	
		設41	設41 排煙設備を設置すること。	
		設42	設42 非常用照明設備、携帯用照明器具を設置すること。	
		設43	設43 水使用設備を設置しないこと。	
		設44	設44 地震感知器を設置すること。	
		設45	設45 出入口には出入管理設備、防犯設備を設置すること。	
		設46	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。	
		設47	設47 ネズミの害を防止する措置を講ずること。	
	(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	設48 什器・備品は不燃性とすること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設49	設49 静電気防止措置を講ずること。	
		設50	設50 耐震措置を講ずること。	
		設51	設51 運搬車等に固定装置を取り付けること。	
	(11) 電源室・空調機械室	設52	設52 災害を受けるおそれの少ない場所に設置すること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設53	設53 保守点検に必要な空間を確保すること。	
		設54	設54 専用の独立した室とすること。	
		設55	設55 無窓とし、錠を付けた扉を設置すること。	
		設56	設56 耐火構造とすること。	
		設57	設57 自動火災報知設備を設置すること。	
		設58	設58 ガス系消火設備を設置すること。	
		設59	設59 空調設備の漏水防止措置を講ずること。	
		設60	設60 ケーブル、ダクトからの延焼防止措置を講ずること。	
	(12) 電源設備	設61	設61 電源設備の容量には余裕を持たせること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設62	設62 電源は複数回線で引き込むこと。	
		設63	設63 良質な電力を供給する設備を設置すること。	
		設64	設64 自家発電設備、蓄電池設備を設置すること。	
		設65	設65 電源設備には避雷設備を設置すること。	
		設66	設66 電源設備には耐震措置を講ずること。	
		設67	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。	
		設68	設68 負荷変動の激しい機器との共用を避けること。	
		設69	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。	
		設70	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。	
		設71	設71 防災、防犯設備用の予備電源を設置すること。	
	(13) 空調設備	設72	設72 空調設備の能力には余裕を持たせること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設73	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。	
		設74	設74 空調設備はコンピュータ室専用とすること。	
		設75	設75 空調設備の予備を設置すること。	
		設76	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。	
		設77	設77 空調設備には侵入、破壊防止対策を講ずること。	
		設78	設78 空調設備には耐震措置を講ずること。	
		設79	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。	
	(14) 監視制御設備	設80	設80 監視制御設備を設置すること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設81	設81 中央管理室を設置すること。	
	(15) 回線関連設備	設82	設82 回線関連設備には錠をつけること。	ウイングアーク1stのMotionBoard, SPA Cloud, SVF CloudではAWS上でサービスを構築しており、本件についてはAWS発行の「金融機関等コンピュータシステムの安全対策基準 第8版 Amazon Web Servicesの回答 2012年6月」にて対応しています。 https://d1.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
		設83	設83 回線関連設備の設置場所の表示は付さないこと。	
		設83-1	設83-1 回線は、専用の配線スペースに設けること。	
1 システム監査	(1) システム監査	監1	監1 システム監査体制を整備すること。	ウイングアーク1stではISO27001の認証を取得しており、所定の監査を定期的に実施しています。 外部による監査とともに、内部監査も実施できる体制を整備しています。