金融機関等コンピュータシステムの安全対策基準 第８版追補改訂

IBM Bluemix における対応状況　－　２０１５年１０月２１日

大項目	中項目	項番	小項目	Bluemix の対策実施状況
建物	環境	設 1	各種災害､障害が発生しやすい地域を避けること。	地震、放射能汚染、高潮、洪水等の危険の少ない地域を選定するとともに、支持基盤までの打杭を行っている。
	周囲	設 2	立地環境の変化に伴う災害および障害の発生の可能性を調査し､防止対策を講ずること。	周辺環境の変化に関する情報入手を定期的に行うとともに、看板の不掲出、通路や隣接物との間隔の十分な確保、避雷設備や地中配線等の対策を行っている。
		設 3	敷地には通路を確保すること。	
		設 4	隣接物との間隔を十分に取ること。	
		設 5	塀または柵および侵入防止装置を設けること。	
		設 6	看板等を外部に出さないこと。	
		設 7	建物には避雷設備を設置すること。	
		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	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。	
	構造	設 10	耐火建築物であること。	建築基準法上の耐火建築物であり、十分な強度や防水性能を確保している。
		設 11	構造の安全性を有すること。	
		設 12	外壁､屋根等は十分な防水性能を有すること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		設 13	外壁等に強度を持たせること。	
	開口部	設 14	窓には防火措置を講ずること。	センサ等を利用した監視を行うとともに、浸水対策、出入口の十分な強度の確保、非常口の設置を行なっている。
		設 15	防犯措置を講ずること。	
		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。	
		設 17	非常口を設けること。	
		設 18	防水措置を講ずること。	
		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。	
	内装等	設 20	不燃材料および防炎性能を有するものを使用すること。	防火性能を有する内装を使用し、落下防止対策を行っている。
		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。	
コンピュータ室・データ保管室	位置	設 22	災害を受けるおそれの少ない位置に設置すること。	コンピュータ室は独立した防火区画であり、災害や侵入の可能性の低い位置に設置している。保守や避難のため必要な空間を確保している。
		設 23	外部から容易に入れない位置に設置すること。	
		設 24	室名等の表示は付さないこと。	
		設 25	必要空間を確保すること。	
		設 26	専用の独立した室とすること。	
	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。	常時利用する出入口は 1 カ所とし、施錠または ID カードによる入退管理を行っている。扉や窓は十分な安全性を確保するとと

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		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。	もに、非常口、誘導灯を設置している。
		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	非常口、避難器具、誘導灯等を設置すること。	
	構造・内装等	設 31	独立した防火区画とすること。	天井板、ラック、照明は落下防止対策を行い、床は支柱耐震措置、帯電防止措置、防水措置を行っている。内装には防炎性能を有するものを使用している。
		設 32	漏水防止対策を講ずること。	
		設 33	静電気の防止措置を講ずること。	
		設 34	内装等には不燃材料および防炎性能を有するものを使用すること。	
		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	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。	
	設備	設 37	自動火災報知設備を設置すること。	所定の安全対策設備を備え、火災、地震、漏水、侵入、ネズミ害等に備えている。
		設 38	非常時の連絡装置を設置すること。	
		設 39	消火設備を設置すること。	
		設 40	ケーブルの難燃化、延焼防止措置を講ずること。	
		設 41	排煙設備を設置すること。	
		設 42	非常用照明設備、携帯用照明器具を設置すること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		設 43	水使用設備を設置しないこと。	
		設 44	地震感知器を設置すること。	
		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	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	ネズミの害を防止する措置を講ずること。	
コンピュータ室・データ保管室（続き）	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。	コンピュータ機器、什器、備品に対する防火、耐震、静電気防止対策を行っている。
		設 49	静電気防止措置を講ずること。	
		設 50	耐震措置を講ずること。	
		設 51	運搬車等に固定装置を取り付けること。	
電源室・空調機会室	—	設 52	災害を受けるおそれの少ない場所に設置すること。	災害を考慮して設置階等の位置を選定するとともに、所定の防災設備を設置している。
電源室・空調機会室	— —	設 53	保守点検に必要な空間を確保すること。	災害を考慮して設置階等の位置を選定するとともに、所定の防災設備を設置している。
		設 54	専用の独立した室とすること。	
		設 55	無窓とし、錠を付けた扉を設置すること。	
		設 56	耐火構造とすること。	
		設 57	自動火災報知設備を設置すること。	
		設 58	ガス系消火設備を設置すること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		設 59	空調設備の漏水防止措置を講ずること。	
		設 60	ケーブル、ダクトからの延焼防止措置を講ずること。	
電源設備	— —	設 61	電源設備の容量には余裕を持たせること。	所定の電源設備を設置するとともに、負荷変動や漏電を考慮した配置を行っている。
		設 62	電源は複数回線で引き込むこと。	
		設 63	良質な電力を供給する設備を設置すること。	
		設 64	自家発電設備、蓄電池設備を設置すること。	
		設 65	電源設備には避雷設備を設置すること。	
		設 66	電源設備には耐震措置を講ずること。	
		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	負荷変動の激しい機器との共用を避けること。	
		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	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。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		設 71	防災、防犯設備用の予備電源を設置すること。	
空調設備	— —	設 72	空調設備の能力には余裕を持たせること。	十分な能力と安定した空気調和を確保し、自動制御や警報装置を設置するとともに、侵入、破壊、防火対策を行っている。 監視制御設備を設置し、中央管理室が監視を行っている。
		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	空調設備はコンピュータ室専用とすること。	
		設 75	空調設備の予備を設置すること。	
		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	空調設備には侵入、破壊防止対策を講ずること。	
		設 78	空調設備には耐震措置を講ずること。	
		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。	
監視制御設備	— —	設 80	監視制御設備を設置すること。	監視制御設備を設置し、中央管理室が監視を行っている。 施錠や専用配線スペースの確保等により安全回線関連設備の安全を確保している。
		設 81	中央管理室を設置すること。	
回線関連設備	—	設 82	回線関連設備には錠をつけること。	施錠や専用配線スペースの確保等により安全回線関連設備の安全を確保している。
		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	回線は、専用の配線スペースに設けること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
管理体制の確立	セキュリティ管理と責任の明確化	運 1	セキュリティ管理方法を具体的に定めた文書を整備すること。	セキュリティポリシーを制定するとともに、社内の管理体制や責任分担を明確化したうえ、管理手順の整備を行っている。
		運 2	セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。	
		運 3	セキュリティ管理体制を整備すること。	
		運 4	システム管理体制を整備すること。	
		運 5	データ管理体制を整備すること。	
		運 6	ネットワーク管理体制を整備すること。	
	組織の整備	運 7	防災組織を整備すること。	防災、防犯および業務運営の組織体制を整備するとともに、役割分担、規則および手順等を明確化することにより、サービス運営の安全を確保している。
		運 8	防犯組織を整備すること。	
		運 9	業務組織を整備すること。	
	各種規定の整備	運 10	各種規定を整備すること。	セキュリティポリシーの下位規定を定め、遵守状況を定期的に確認している。
	セキュリティ遵守状況の確認	運 10-1	セキュリティ遵守状況を確認すること。	
入退管理	入退館（室）管理	運 11	資格付与および鍵の管理を行うこと。	入退館室の権限付与ルールや手順を明確化するとともに、定期的に権限の見直しを行っている。
		運 12	入退館管理を行うこと。	
		運 13	入退室管理を行うこと。	
運用管理	マニュアルの整備	運 14	通常時マニュアルを整備すること。	通常運用時および障害時、災害時の運用手順を定めるとともに、自動化機能を活用して運用の安全を確保している。
		運 15	障害時･災害時マニュアルを整備する	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
			こと。	
	アクセス権限の管理	運 16	各種資源、システムへのアクセス権限を明確にすること。	システムへのアクセス権限付与ルールや手順を明確化するとともに、定期的に権限の見直しを行うとともに、パスワードの秘匿性確保の措置を講じている。
		運 17	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。	
		運 18	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化すること。	
	オペレーション管理	運 19	オペレータの資格確認を行うこと。	オペレーションの実施体制、手順、ルールを明確化することにより、安全な運用を確保している。
		運 20	オペレーションの依頼・承認手続きを明確にすること。	
		運 21	オペレーション実行体制を明確にすること。	
		運 22	オペレーションの記録、確認を行うこと。	
		運 23	クライアントサーバー・システムにおける作業の管理を行うこと。	
	入力管理	運 24	データの入力管理を行うこと。	データ入力は利用企業により管理される。
	データファイル管理	運 25	授受・管理方法を定めること。	データファイルは利用企業により管理される。
		運 26	修正管理方法を明確にすること。	
		運 27	バックアップを確保すること。	
	プログラムファイル管理	運 28	管理方法を明確にすること。	プログラムファイルは利用企業により管理される。
		運 29	バックアップを確保すること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
	コンピュータウィルス対策	運 30	コンピュータウイルス対策を講ずること。	ウィルス対策ソフトを導入するとともに、インフラ、プラットフォームおよび結合サービスに係る脆弱性評価を定期的に実施している。
運用管理（続き）	ネットワーク設定情報管理	運 31	設定情報の管理を行うこと。	ネットワーク設定情報の管理手続きを定めるとともにバックアップ取得や遠隔保管を行っている。
		運 32	設定情報のバックアップを確保すること。	
	ドキュメント管理	運 33	保管管理方法を明確にすること。	アプリケーションのドキュメントは利用企業により管理される。IBM 所管部分のドキュメントは所定の手続きにより管理され、バックアップの所得や遠隔保管を実施している。
		運 34	バックアップを確保すること。	
	帳票管理	運 35	未使用重要帳票の管理方法を明確にすること。	帳票管理は利用企業により実施される。
		運 36	重要な印字済帳票の取扱方法を明確にすること。	
	出力管理	運 37	出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること。	システムの処理結果の出力は利用企業により管理される。
	取引の管理	運 38	各取引の操作権限を明確にすること。	取引管理は利用企業により実施される。
		運 39	オペレータカードの管理を行うこと。	
		運 40	取引の操作内容を記録・検証すること。	
		運 41	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。	
		運 42	機器および媒体の盗難、破損等に伴	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
			い、利用者が被る可能性がある損失および責任を明示すること。	
	暗号鍵の管理	運 43	暗号鍵の利用において運用管理方法を明確にすること。	社内の管理体制を明確化している。
	厳正な本人確認の実施	運 44	本人確認を行うこと。	金融取引における本人確認は利用企業により管理される。
		運 44-1	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。	
	CD･ATM 等および無人店舗の管理	運 45	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。	CD、ATM および無人化店舗に関する事項は利用企業により管理される。
		運 46	監視体制を明確にすること。	
		運 47	防犯体制を明確にすること。	
		運 48	障害時・災害時の対応方法を明確にすること。	
		運 49	関係マニュアルの整備を行うこと。	
運用管理（続き） システム開発・変更	渉外端末の管理	運 50	運用管理方法を明確にすること。	海外端末に関する事項は利用企業によって管理される。
	カード管理 顧客データ保護	運 51	カードの管理方法を明確にすること。	キャッシュカード、クレジットカード等に関する事項は利用企業により管理される。
		運 51-1	顧客に対して犯罪に関する注意喚起を行うこと。	
		運 52	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。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
	顧客データ保護	運 53	顧客データの保護策を講ずること。	預金者等の顧客データは利用企業により管理される。
		運 53-1	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。	
	資源管理	運 54	能力及び使用状況の確認を行うこと。	プラットフォーム、インフラ、結合サービスの負荷状況を監視するとともに、利用企業への開示を行っている。
	外部接続管理	運 55	接続契約内容を明確にすること。	外部接続の安全管理のため、VPN 接続あるいは専用線接続と、ファイアウォール機能の利用が可能である。
		運 56	外部接続における運用管理方法を明確にすること。	
	機器の管理	運 57	管理方法を明確にすること。	各機器へのアクセスは所定の権限を付与された者に限定している。機器の故障等に備え部品交換等の保守を迅速に行える態勢を整備している。
		運 58	ネットワーク関連機器の保護措置を講ずること。	
		運 59	保守方法を明確にすること。	
	運行管理	運 60	監視体制を整備すること。	24 時間体制により利用企業の緊急連絡を受付可能とし、障害等の記録を作成している。
	コンピュータ室　データ保管室の管理	運 61	入室後の作業を管理すること。	作業実施は所定の承認を受け実施し、記録を残すほか、監視カメラによる牽制を図っている。
	障害時・災害時対応策	運 62	関係者への連絡手順を明確にすること。	24 時間体制により利用企業の緊急連絡を受付可能とし、障害等の記録を作成している。
		運 63	障害時･災害時復旧手順を明確にすること。	
		運 64	障害の原因を調査・分析すること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
	コンティンジェンシープランの策定	運 65	コンティンジェンシープランを策定すること	利用企業の要望に応じてオフサイトバックアップシステムを設置することが可能である。
システム開発・変更	ハードウェア、ソフトウェア管理	運 66	ハードウェア､ソフトウェアの管理を行うこと。	プラットフォーム、インフラおよび結合サービス所管組織が連携して構成情報を管理している。
	システム開発・変更管理	運 67	開発・変更手順を明確にすること。	アプリケーション開発は利用企業により管理される。
		運 68	テスト環境を整備すること。	
		運 69	本番への移行手順を明確にすること。	
	ドキュメント管理	運 70	作成手順を定めること。	アプリケーション開発に係るドキュメントは利用企業により管理される。
		運 71	保管管理方法を明確にすること。	
	パッケージの導入	運 72	評価体制を整備すること。	Bluemix でオープンソースソフトウェアを利用する場合は、レビューやリスク評価により安全性を確認している。
		運 73	運用・管理体制を明確にすること。	
	システムの廃棄	運 74	廃棄計画、手順を策定すること。	リソース見通しに基づく廃棄計画を策定している。利用企業より解約の申し出を受けた場合は、米国連邦政府認定を受けたソフトウェアによりデータ消去を行っている。
		運 75	情報漏洩防止対策を講ずること。	
各種設備管理	保守管理	運 76	管理方法を明確にすること。	設備の管理体制、管理基準および手順を明確化するとともに、定期的な点検と結果レビューを実施している。
		運 77	保守方法を明確にすること。	
	資源管理	運 78	能力および使用状況の確認を行うこと。	設備の管理体制、管理基準および手順を明確化するとともに、定期的な点検と結果レビューを実施している。 各設備に応じた管理基準を定め、余裕度を設けて監視している。
	監視	運 79	監視体制を整備すること。	各設備を自動監視し、異常検知時は警報に基づき対処している。

大項目	中項目	項番	小項目	Bluemix の対策実施状況
教育・訓練	教育・訓練	運 80	セキュリティ教育を行うこと。	IBM グローバルのセキュリティポリシーに従ったセキュリティ教育、インフラ構築およびシステム運用に関する研修、障災害時の復旧オペレーション、データセンタの防犯防災等の教育訓練を定期的に実施している。
		運 81	要員に対するスキルアップ教育を行うこと。	
		運 82	オペレーション習熟のための教育および訓練を行うこと。	
		運 83	障害時・災害時に備えた教育・訓練を行うこと。	
		運 84	防災・防犯訓練を行うこと。	
要員管理	要員管理	運 85	要員の人事管理を適切に行うこと。	担当の職務記述に基づくパフォーマンス評価を行うとともに、健康診断受診を義務付けている。
		運 86	要員の健康管理を行うこと。	
外部委託管理 システム監査	外部委託計画	運 87	システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲を明確にすること。	日本国内のデータセンタを賃借するにあたり、全世界のデータセンタと同様の機密保護および安全運行に関する委託契約を締結している。
		運 87-1	外部委託先の選定手続きを明確にすること。	
		運 88	安全対策に関する項目を盛り込んだ委託契約を締結すること。	
	外部委託業務管理	運 89	外部委託先の要員にルールを遵守させ、その遵守状況を管理、検証すること。	インフラサービスの運営に直接影響する外部委託は行っていない。
		運 90	外部委託における業務組織の整備と業務の管理、検証を行うこと。	
		運	金融機関相互のシステム・ネットワー	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		90-1	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。	
システム監査	システム監査	運 91	システム監査体制を整備すること。	ISO27001、SOC、FFIEC、HIPAA、FISMA 等の外部監査を受けている。
インストアブランチ		運 92	出店先の選定基準を明確にすること。	インストアブランチに関する事項は利用企業により管理される。
コンビニ ATM		運 93	出店先の選定基準を明確にすること。	コンビニ ATM に関する事項は利用企業により管理される。
		運 94	現金装填等メンテナンス時の防犯対策を講じること。	
		運 95	障害時･災害時対応手順を明確にすること。	
		運 96	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。	
		運 97	所轄の警察および警備会社等関係者との連絡体制を確立すること。	
		運 98	顧客に対して犯罪に関する注意喚起を行うこと。	
デビットカード	サービスの安全性確保	運 99	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。	デビットカードに関する事項は利用企業により管理される。
		運 100	口座番号､暗証番号等の安全性を確保すること。	
	顧客保護	運 101	デビットカード利用時の顧客保護の措置を講ずること。	
	顧客への	運 102	デビットカード利用上の留意事項を	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
	注意喚起		顧客に注意喚起すること。	
オープンネットワークを利用した金融サービス	インターネット、モバイル	運 103	不正使用を防止すること。	インターネットバンキングに関する事項は利用企業により管理されるが、次のようなセキュリティ機能の利用が可能である。 ・不正侵入検知、予防 ・ファイアウォール ・通信の暗号化
		運 104	不正使用を早期発見すること。	
		運 105	安全対策に関する情報開示をすること。	
		運 105-1	顧客対応方法を明確にすること。	
		運 106	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。	
	電子メール	運 107	電子メールの運用方針を明確にすること。	IBM グローバルの基準により電子メールを管理している。
クラウドサービスの利用	—	運 108	クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること。	クラウド事業者の選定は利用企業の判断により行われるが、IBM は選定作業の資するため、サービスやリスク管理に係る情報を公開している。
		運 109	クラウド事業者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。	
		運 110	クラウドサービス利用にあたって、データ漏洩防止策を講ずること。	
		運 111	クラウド契約終了時のデータ漏洩防止策を講ずること。	
		運 112	クラウド事業者に対する立入監査・モ	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
			ニタリング態勢を整備すること。	
サイバー攻撃対応態勢の整備		運 113	サイバー攻撃対応態勢を整備すること。	各種のセキュリティ対策を実施するとともに、PSIRT*チームを組成し、サイバー攻撃や製品の脆弱性に伴う問題に対し、グローバルな全社態勢で連携、対応を行うこととしている。* Product Security Incident Response Team
ハードウェアの信頼性向上対策	ハードウェアの障害予防策	技 1	予防保守を実施すること。	各データセンタには担当者を 24 時間体制で常駐させ、故障時の部品交換等を迅速に行える態勢を整備している。
	ハードウェアの予備	技 2	本体装置の予備を設けること。	ディスクや電源系統等の共通インフラを冗長化するとともに、利用企業の要望に応じて個社環境を冗長構成とすることが可能である。
		技 3	周辺装置の予備を設けること。	
		技 4	通信系装置の予備を設けること。	
		技 5	回線の予備を設けること。	
		技 6	端末系装置の予備を設けること。	
ソフトウェアの信頼性向上対策	開発時の品質向上対策	技 7	システム開発計画は中長期計画との整合性を確認するとともに､承認を得ること。	アプリケーション開発は利用企業により管理されるが、DevOps サービスにより各種の開発支援機能を提供している。
		技 8	必要となるセキュリティ機能を取り込むこと。	
		技 9	設計段階でのソフトウェアの品質を確保すること。	
		技 10	プログラム作成段階での品質を確保すること。	
		技 11	テスト段階でのソフトウェアの品質	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
			を確保すること。	
		技 12	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。	
		技 13	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。	
	メンテナンス時の品質向上対策	技 14	定型的変更作業時の正確性を確保すること。	インフラの変更作業の手順化、ルール化による誤操作防止を図っている。
		技 15	機能の変更、追加作業時の品質を確保すること。	
運用時の信頼性向上対策	運用時の信頼性向上対策	技 16	オペレーションの自動化、簡略化を図ること。	運用の手順化、自動化を進め誤操作防止を図るとともに、インフラの負荷状況を監視している。
		技 17	オペレーションのチェック機能を充実すること。	
		技 18	負荷状態の監視制御機能を充実すること。	
		技 19	CD・ATM 等の遠隔制御機能を設けること。	
障害の早期発見・早期回復	障害の早期発見	技 20	システム運用状況の監視機能を設けること。	各種ツールを利用した監視を行うとともに、構成情報に基づく切り分け実施態勢を整備している。
		技 21	障害の検出および障害箇所の切り分け機能を設けること。	
	障害の早期回復	技 22	障害時の縮退・再構成機能を設けること。	縮退・再構成、取引制限およびジャーナルやチェックポイントを利用したリカバリ機能は利用企業により管理される。
		技 23	取引制限機能を設けること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		技 24	リカバリ機能を設けること。	
災害時対策	バックアップサイト	技 25	バックアップサイトを保有すること。	利用企業の要望により、オフサイトバックアップシステムを設置することが可能である。
データ保護	漏洩防止	技 26	暗証番号･パスワード等は他人に知られないための対策を講ずること。	データベースの暗号化は利用企業がニーズに応じて実施する。 通信の暗号化機能の利用が可能である。
		技 27	相手端末確認機能を設けること。	
		技 28	蓄積データの漏洩防止策を講ずること。	
		技 29	伝送データの漏洩防止策を講ずること。	
	破壊・改ざん防止	技 30	ファイルに対する排他制御機能を設けること。	ファイルに関する各種制御は利用企業によって管理される。
		技 31	ファイルに対するアクセス制御機能を設けること。	
		技 32	不良データ検出機能を充実すること。	
	検知策	技 33	伝送データの改ざん検知策を講ずること。	データ改ざんや不整合の検知は利用企業により管理される。
		技 34	ファイル突合機能を設けること。	
不正使用防止	予防策（アクセス権限確認）	技 35	本人確認機能を設けること。	アクセス権限を管理し、ログの記録を行っている。
		技 35-1	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。	
		技 36	ID の不正使用防止機能を設けること。	

大項目	中項目	項番	小項目	Bluemix の対策実施状況
		技 37	アクセス履歴を管理すること。	
	予防策（利用範囲の制限）	技 38	取引制限機能を設けること。	取引の制限、禁止機能は利用企業により管理される。
		技 39	事故時の取引禁止機能を設けること。	
	予防策（不正・偽造防止対策）	技 40	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。	カード、電子的価値および利用企業の暗号鍵の保護は利用企業により実施される。Bluemix で管理する暗号鍵は管理責任を明確化している。
		技 41	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。	
		技 42	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。	
		技 42-1	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。	
	外部ネットワークからのアクセス制限	技 43	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。	ファイアウォールやログ管理システムにより不正侵入を防止するとともに、モニタリングを行っている。
		技 44	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。	
	検知策	技 45	不正アクセスの監視機能を設けること。	トラフィック状況の監視を行い、不正が疑われる場合は遮断を含めた対応を行う。
		技 46	異常な取引状況を把握するための機能を設けること。	
		技 47	異例取引の監視機能を設けること。	
	対応策	技 48	不正アクセスの発生に備えて対応策、	不正が疑われる場合の遮断等の対応および、構成情報からの復

大項目	中項目	項番	小項目	Bluemix の対策実施状況
			復旧策を講じておくこと。	旧を手順化している。
不正プログラム防止	防御策	技 49	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	ウィルス対策ソフトを導入するとともに、復旧手順を整備している。
	検知策	技 50	コンピュータウイルス等不正プログラムの検知対策を講ずること。	
	復旧策	技 51	コンピュータウイルス等不正プログラムによる被害時対策を講ずること。	