参考資料　3-2

セキュリティに関する主な事項一覧

注１　この資料は、（財）金融情報システムセンター発行「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7版」（以下、『金融機関システムの安全対策基準・解説書』）掲載の安全対策基準一覧表に、「適用にあたっての考え方」欄を追加したものを、事務局において編集し、地方自治体のコンピュータシステムの安全対策基準として見た場合の地方自治体における適用区分欄、各ガイドラインの記載箇所欄を併記したものである。

注２　『金融機関システムの安全対策基準・解説書』は、金融機関等を対象とした安全対策基準であるため、本資料の利用にあたっては、項目ごとに地方自治体のコンピュータシステムの安全対策基準として用いることが妥当であるかを十分に検討する必要がある。

注３　『金融機関システムの安全対策基準・解説書』の適用区分欄における記号の意味は以下のとおりである。
◎：当該基準を取り入れることが必要であることを示す。したがって「適用にあたっての考え方」の欄を、「…すること」と記述する。
〇：金融機関等の業務の実態に照らし、必要に応じて取り入れる基準であることを示す。したがって「適用にあたっての考え方」の欄を、「…望ましい」と記述する。
地方自治体における適用区分欄においても上記を準用する。

設備基準

[Ⅰ．コンピューターセンター]

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分 コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	自治体における適用区分 クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
（Ⅰ）建物												
	1. 環境	設　1	災害発生地域の回避	コンピュータセンターへの災害の影響を少なくするため、各種災害および障害が発生しやすい地域の立地を避けることが望ましい。	○				○			
	2. 周囲	設　2	環境変化に対する措置	コンピュータセンターへの災害の影響を少なくするため、コンピュータセンターの自然環境、地域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が望ましい。	○				○			
		設　3	消火・避難用通路の確保	敷地には火災時の安全かつ適切な消火活動、避難を容易にするため、建築基準法に定められた幅員の通路を確保すること。	◎				◎			
		設　4	隣接物との間隔確保	延焼の防止および消火活動を容易にするため、隣接する建物との間隔を十分取ることが望ましい。	○				○			
		設　5	塀または柵および侵入防止装置の設置	敷地内への不法侵入、建物等の破壊行為を防止するため、隣地境界において入退管理を行う場合は塀または柵を設けることが望ましく、必要に応じて侵入防止装置を設けることが望ましい。	○				○			
		設　6	看板の非設置	外部からの侵入、破壊行為等の人為的災害を未然に防止するため、コンピュータセンター等の所在を示した表示板、看板等は外部に出さないことが望ましい。	○				○			
		設　7	避雷設備の設置	落雷による障害、事故を防止するため、周囲に高い建物がない場合または落雷多発地域においては、建物には避雷設備を設置することが望ましい。	○				○			
		設　8	専用の建物または独立区画	安全管理の徹底のため、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が望ましい。	○				○			
		設　9	通信回線・電力線の切断・延焼防止装置	コンピュータシステムのサービス中断を防止するため、敷地内の通信回線・電力線は、工事や外部からの侵入等による切断・延焼の防止措置を講ずることが望ましい。	○				○			
	3. 構造	設　10	耐火建築物	防火対策のため、コンピュータセンターの建物は、建築基準法に規定する耐火建築物とすること。	◎				◎			
		設　11	構造の安全性	コンピュータシステムに障害を及ぼさないため、建築基準法に規定する構造の安全性を有すること。	◎				◎			
		設　12	外壁、屋根の防水性能	コンピュータシステムに障害を及ぼさないため、外壁、屋根等は漏水の防止措置を講ずること。	◎				◎			
		設　13	外壁の強度の確保	コンピュータ関連設備を破壊行為等から防御するため、公道等外部に面する外壁等は、強度を持たせることが望ましい。	○				○			
	4. 開口部	設　14	窓の防火措置	延焼を防止するため、延焼のおそれのある窓には防火措置を講ずること。	◎				◎			
		設　15	窓の防犯措置	コンピュータセンター建物内への不法な侵入等を防止するため、外部からの容易に接近、侵入できる1階等の窓には、防犯措置を講ずること。	◎				◎			
		設　16	出入口1ヵ所、出入管理設備・防犯設備の設置	入退館管理を確実に行うことによる不法侵入の防止、不審物品の搬出入防止のため、常時利用する出入り口は1ヵ所とし、出入管理設備、防犯設備を設置することが望ましい。	○				○			
		設　17	非常口の設置	災害時の安全な避難と非常時持ち出しの円滑化のため、適切な位置に非常口を設けること。	◎				◎			
		設　18	防水措置	浸水および漏水によるコンピュータ機器等への障害を防止するため、出入口、窓、機器の搬出入口等の開口部は、防水措置を講ずることが望ましい。	○				○			
		設　19	出入口扉の強度の確保、錠の取付け	防犯・防災のため、出入口には十分な強度を有する扉を設置し、鍵を付けること。	◎				◎			
	5. 内装等	設　20	不燃材料、防炎性能	要員およびコンピュータシステムを守るため、内装等には、建築基準法に規定する不燃材料および消防法に規定する防炎性能を有するものを使用すること。	◎				◎			
		設　21	落下・損壊防止措置	要員およびコンピュータシステムに被害を及ぼさないようにするため、地震による内装等の落下・損壊の防止措置を講ずることが望ましい。	○				○			

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分 コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	自治体における適用区分 クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
（Ⅱ）コンピューター室・データ保管室												
	1. 位置	設　22	災害の少ない位置	コンピュータシステムへの影響を防止するため、地震、火災、浸水等の災害を受けるおそれの少ない位置に設置すること。	◎				◎			
		設　23	容易に入れない位置	侵入、破壊、機密漏洩等を防止するため、出入口付近およびエレベータまたは階段で直接は入れる位置を避けて設置すること。	◎				◎			
		設　24	室名等の非表示	侵入、破壊、機密漏洩等を防止するため、コンピュータ室・データ保管室の室名等の表示は付さないこと。	◎				◎			
		設　25	必要空間の確保	保守、避難のため、必要空間を確保すること。	◎				◎			
		設　26	室の専用化	安全管理の徹底のため、専用の独立した室とすること。	◎				◎			
	2. 開口部	設　27	出入口1ヵ所、前室の設置	入退室管理を確実に行うため、常時利用する出入口は1ヵ所とすることが望ましい。また、安全性を保ち、外部からの熱、湿気、塵埃の侵入を防止するため、常時利用する出入口には、前室を設けることが望ましい。	○				○			
		設　28	出入口扉の強度の確保、錠の取付け	防犯・防災のため、出入口には十分な強度を有する扉を設置し、鍵を付けること。	◎				◎			
		設　29	窓の防火・防水・破損防止措置・外部から見えない措置	防犯・防災のため、窓を設ける場合は防火・防水措置および窓ガラスの破損防止措置を講じ、さらに外部から室内の機器等が見えない措置を講じること。	◎				◎			
		設　30	非常口、非難器具、誘導灯の設置	災害時の避難と非常持ち出しの円滑化のため、コンピュータ室には適切な位置に非常口および避難器具を設置すること。また、非常口への誘導灯および誘導標識を設置すること。	◎				◎			
	3. 構造・内装等	設　31	独立した防火区画	建物内他区画からの火災の延焼防止のため、コンピュータ室・データ保管室は、建築基準法に規定する独立した防火区画とすること。	◎				◎			
		設　32	漏水防止対策	建物、設備等の損傷およびコンピュータ機器等に対する障害を未然に防止するため、天井、壁、床面からの漏水防止対策を講ずること。	◎				◎			
		設　33	静電気防止措置	コンピュータシステムへの悪影響を防止するため、コンピュータ室の床表面材料は、静電気の発生、帯電等による影響を防止する措置を講ずること。	◎				◎			
		設　34	不燃材料、防炎性能	要員およびコンピュータシステムを火災による被害から守るため、内装等には、建築基準法に規定する不燃材料および消防法に規定する防炎性能を有するものを使用すること。	◎				◎			
		設　35	落下・損壊防止措置	要員およびコンピュータシステムへ被害を及ぼさないようにするため、間仕切壁、天井、照明器具等、地震の際に落下・損壊の危険のあるものは、落下・損壊防止措置を講ずること。	◎				◎			
		設　36	フリーアクセス床の耐震措置	地震時に損壊することのないよう、フリーアクセス床は耐震措置を講ずること。	◎				◎			
	4. 設備	設　37	自動火災報知設備の設置	火災が発生した場合、早期に発見、通報して、初期消火や避難等ができるように、適切な自動火災報知設備を設置すること。	◎				◎			
		設　38	非常時の連絡装置の設置	火災等の異常事態の発生を知らせ、初期消火、避難等について適切な指示を与えるため、非常時の連絡装置を設置すること。	◎				◎			
		設　39	消火設備の設置	火災時に備えて、適切な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	ケーブルの燃焼・延焼を防止するため、ケーブルの難燃化措置を講ずることが望ましい。また、壁面等のケーブル貫通部分は延焼防止措置を講ずること。	◎				◎			
		設　41	排煙設備の設置	火災時に備えて、必要な排煙設備を設置すること。	◎				◎			
		設　42	非常用照明設備、携帯用照明器具の設置	火災時の異常事態発生時に室内要員が安全に避難できるように、コンピュータ室には、非常用照明設備および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	適用にあたっての考え方	適用区分				自治体における適用区分			
					コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
		設　43	水使用設備の非設置	漏水によるコンピュータシステムへの影響を防止するため、コンピュータ室・データ保管室に水使用設備を設置しないこと。	◎				◎			
		設　44	地震感知器の設置	コンピュータシステムの運転継続を判断し、データ破壊や電気火災等の二次災害発生を防止するため、コンピュータ室には地震感知器を設置することが望ましい。	○				○			
		設　45	出入口の出入管理設備、防犯設備の設置	不法侵入を防ぐため、コンピュータ室・データ保管室の出入口には入退室者を識別、記録する出入管理設備を設置すること。さらに、防犯設備を設置することが望ましい。	○				○			
		設　46	温湿度自動記録装置または温湿度警報装置の設置	コンピュータシステムの予防保全、障害時の原因分析のため、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	ネズミ害の防止措置	ネズミによってケーブルが害を受けることを防止するため、適切な措置を講じることが望ましい。	○				○			
	5. コンピューター機器、什器、備品	設　48	不燃性	引火と火災拡大を防止するため、什器・備品はスチール製品等の不燃性とすること。	◎				◎			
		設　49	静電気防止措置	コンピュータシステムへの悪影響を防止するため、コンピュータ機器、什器・備品は、静電気防止措置を講ずること。	◎				◎			
		設　50	耐震措置	地震の際に要員やコンピュータ機器に影響を与えないよう、コンピュータ機器および什器等の耐震措置を講ずること。	◎				◎			
		設　51	運搬車の固定装置の取付け	地震の際に要員やコンピュータ機器に損傷を与えないよう、磁気テープ、磁気ディスク等の運搬車等は、制動または固定する装置を取り付けること。	◎				◎			
（Ⅲ）電源室・空調室												
		設　52	災害の少ない位置	コンピュータシステムへの影響を防止するため、地震、火災、浸水等の災害を受けるおそれの少ない場所に設置すること。	◎				◎			
		設　53	保守点検用空間の確保	機器、装置等の保守点検および災害時の避難のため、必要な広さ、高さの空間を確保すること。	◎				◎			
		設　54	室の独立・専用化	保守管理および障害の拡大防止のため、他の室とは独立した専用の室とすることが望ましい。	○				○			
		設　55	無窓、扉への錠の取付け	外部からの侵入防止、防火、防水のため、無窓とすることが望ましく、錠を付けた扉を設置すること。	◎				◎			
		設　56	耐火構造	火災による延焼防止のため、耐火構造とすること。	◎				◎			
		設　57	自動火災報知設備の設置	早期に火災を発見するため、自動火災報知設備を設置すること。	◎				◎			
		設　58	ガス系消火設備の設置	火災時に備えて、全域放出型のガス系消火設備を設置することが望ましい。	○				○			
		設　59	空調設備の漏水防止措置	漏水による障害を回避するため、冷却水の水漏れ、結露等による漏水の防止措置を講ずること。	◎				◎			
		設　60	ケーブル、ダクトの延焼防止措置	延焼を防止するため、ケーブル、ダクトからの延焼防止措置を講ずること。	◎				◎			

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分 コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	自治体における適用区分 クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
(Ⅳ)電源設備												
		設　61	容量の余裕	コンピュータシステムに必要な電力を安定的に供給するため、電源設備の容量には余裕を持たせること。	◎				◎			
		設　62	複数回線による引込み	受電設備の障害時に備え、電源は複数回線で引き込むことが望ましい。	○				○			
		設　63	良質な電力の供給	コンピュータシステムを安定稼働させるため、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、蓄電池設備の設置	停電時でもコンピュータシステムを継続して稼働させるため、自家発電設備および蓄電池設備を設置すること。	◎				◎			
		設　65	避雷設備の設置	落雷による被害を防止するため、電源設備には避雷設備を設置すること。	◎				◎			
		設　66	耐震設置	地震による移動、損傷等を防止するため、電源設備には耐震措置を講ずること。	◎				◎			
		設　67	分電盤からの電源引込みの専用化	コンピュータシステムへの影響を最小限にするため、コンピュータ機器への電源の引込みは専用分電盤から専用回路にて配線すること。	◎				◎			
		設　68	負荷変動の激しい機器との共用回避	コンピュータシステムに安定して電力を供給するため、コンピュータシステムを負荷変動の激しい機器との電源系統は分けること。	◎				◎			
		設　69	アースの専用化	電源設備や電気機器等からの影響を防止するため、コンピュータシステムのアースは専用とすること。	◎				◎			
		設　70	過電流、漏電の影響回避	各機器に障害を及ぼさないように、過電流や漏電への措置を講ずること。	◎				◎			
		設　71	防災・防犯設備用予備電源の設置	停電した場合でも防災、防犯設備が作動するように、予備電源を設置すること。	◎				◎			

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分 コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	自治体における適用区分 クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
（Ⅴ）空調設備												
		設　72	能力の余裕	コンピュータ室の温湿度を適切に調整するため、空調設備の能力には余裕を持たせること。	◎				◎			
		設　73	安全性の確保	コンピュータシステムの継続した運用を確保するため、空調設備には安定的に空気調和ができる措置を講ずること。	◎				◎			
		設　74	コンピューター室専用化	コンピュータ室の温湿度制御を的確に行うため、空調設備は他の室との共用を避けコンピュータ室専用とすること。	◎				◎			
		設　75	予備の設置	障害の発生に備えて、主要な空調設備機器については予備を設置することが望ましい。	○				○			
		設　76	自動制御装置、異常警報装置の設置	空調設備を安定的に稼働させるため、各種の自動制御装置のほか、機器の異常を迅速に検知する異常警報装置を設置すること。	◎				◎			
		設　77	侵入・破壊防止対策	コンピュータシステムの運用に支障を来さないようにするため、空調設備には侵入、破壊に対する防止対策を講ずること。	◎				◎			
		設　78	耐震設置	地震による移動、損傷等を防止するため、空調設備には耐震措置を講ずること。	◎				◎			
		設　79	断熱材料、吸排気口の不燃材料	火災時の空調設備の損傷を防止するため、空調設備のダクト等の断熱材料および吸排気口は不燃材料とすること。	◎				◎			
（Ⅵ）監視制御設備												
		設　80	監視制御設備の設置	障害発生等を早期に発見するため、電源設備、空調設備、防災設備、防犯設備等の監視制御設備を設置すること。	◎				◎			
		設　81	中央管理室の設置	電源設備、空調設備、防災設備、防犯設備等の運営管理を円滑にし、かつ有効活用を図るため、これらの設備を集中管理する中央管理室を設置することが望ましい。	○				○			
（Ⅶ）回線関連設備												
		設　82	錠の取付け	不正アクセス、破壊等の不法行為を防止するため、コンピュータ室外に設置される回線関連設備の機器収容架等には錠を付けること。	◎				◎			
		設　83	設置場所の非表示	部外者に回線関連設備の設置場所を知らせないため、設置場所の表示は付さないこと。	◎				◎			
		設　83-1	配線スペースの専用化	回線を障害および犯罪から防護し、また、他の電源ケーブル等からのノイズの混入を防止するため、専用の配線スペースに設けることが望ましい。	◎				◎			

設備基準

[Ⅱ. 本部・営業店等]

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分				自治体における適用区分			
					コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
（Ⅰ）建物												
	1. 周囲	設　84	通信回線・電力線の切断・延焼防止措置	コンピュータシステムのサービス中断を防止するため、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が望ましい。		○				○		
	2. 構造	設　85	耐火建築物	防火対策のため、建物は建築基準法に規定する耐火建築物であることが望ましい。		○				○		
		設　86	構造の安全性	構造の安全性を確保するため、建物は建築基準法の規定に従うこと。		◎				◎		
		設　87	外壁、屋根の防水性能	漏水を防止するため、十分な防水性能を有するように講ずること。		◎				◎		
		設　88	外壁の強度の確保	破壊侵入等を防御するため、公道等外部に面する外壁は強度を持たせることが望ましい。		○				○		
	3. 開口部	設　89	窓の防火措置	延焼を防止するため、延焼のおそれのある窓には防火措置を講ずること。		◎				◎		
		設　90	窓・扉の防犯措置	不法な侵入等を防止するため、外部から容易に接近、侵入できる窓・扉には、防犯措置を講ずること。		◎				◎		
		設　91	出入口扉の防火構造、鍵の取付け	防犯・防災のため、出入口には十分な強度を有する扉を設置し、錠を付けること。		◎				◎		
		設　92	通用口の入室者識別設備の設置	不法侵入を防止するため、営業時間外に利用する通用口には、インターホン等室内から相手確認ができる識別装置を設置すること。		◎				◎		
		設　93	出入口の防水措置	雨水等の浸水を防止するため、出入口には防水措置を講ずることが望ましい。		○				○		
	4. 内装等	設　94	天井および壁の遮熱、吸音機能	端末機器等を正常に機能させるため、天井および壁は遮熱機能および吸音機能を持たせることが望ましい。		○				○		
		設　95	落下・損壊防止措置	人身および端末機器等へ被害を及ぼさないようにするため、天井、壁、照明器具等、地震の際に落下・損壊の危険のあるものは、落下・損壊防止措置を講ずること。		◎				◎		
		設　96	床表面の塵埃、静電気防止措置	端末機器への悪影響を防止するため、床表面は塵埃や静電気が発生しにくい材質のものが望ましい。		○				○		
		設　97	回線の切断防止措置	通行時に切断することのないよう、端末機器への回線、電源ケーブル等は適切な位置に布設すること。		◎				◎		
		設　98	回線の漏水防止対策	事故による漏水等でシステムが停止しないよう、端末機器に接続している回線、電線ケーブル等は漏水防止対策を講ずることが望ましい。		○				○		
	5. 設備	設　99	自動火災報知設備、消火器の設置	火災が発生した場合、早期に発見、通報して、初期消火や避難ができるように、煙感知器等を用いた自動火災報知設備および消火器を設置すること。		◎				◎		
		設　100	耐震措置	端末機器等に影響を与えないよう、什器、備品等は耐震措置を講ずることが望ましい。		○				○		

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分				自治体における適用区分			
					コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
		設　101	耐火金庫の設置	火災等の災害に起因するシステム障害の影響を最小限にするため、耐火金庫、耐火キャビネット等のデータ保管庫を設置し、復旧に必要な媒体、資料等のデータを保管すること。		◎				◎		
		設　102	避雷設備の設置	落雷によるコンピュータシステムの障害、室内にいる人の感電死傷、火災等の事故を防止するため、周囲に高い建物がない場合は避雷設備を設置することが望ましい。		○				○		
		設　103	防犯措置	犯罪の未然防止と発生時の対応のため、防犯カメラ、非常通報装置等の防犯措置を講ずること。		◎				◎		
	6. 回線関連設備	設　104	設置場所の非表示	部外者に回線関連設備の設置場所を知らせないため、回線関連設備の設置場所の表示は付さないこと。		◎				◎		
		設　105	鍵の取付け	不正アクセス、破壊等の不法行為を防止するため、関係者以外に触れやすい場合には錠を付けること。		◎				◎		
		設　106	端末機器までの配線の二重化	回線障害時に迅速に対応するため、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が望ましい。		○				○		
	7. 電源設備	設　107	電源ケーブルの布設	端末機器等に支障を来さないようにするため、電源ケーブルは分電盤から直接布設するか、他の機器の影響を受けないよう布設すること。		◎				◎		
		設　108	防災・防犯設備用予備電源の設置	停電に備えて、防災、防犯設備および非常用照明設備が作動するように予備電源を設置すること。		◎				◎		
		設　109	自家発電設備の設置	停電に備えて、自家発電設備等を設置することが望ましい。		○				○		
	8. 空調設備	設　110	空調設備の設置	端末機器等の異常動作を防止するため、端末機器台数に応じた空調設備を設置すること。		◎				◎		
	9. 自動機器室	設　111	通話装置の設置	自動機器室の機器の障害に対し、迅速に対応するため、電話、インターホン等の通話装置により、障害時に営業室等との通話ができること。		◎				◎		
		設　112	非常通報装置の設置	自動機器室で発生した非常事態に対し、迅速に対応するため、非常時に営業室等への通報ができる非常通報装置を設置すること。		◎				◎		
		設　113	防犯設置	自動機器室の安全を確保するため、設置形態と周辺の環境に応じて、自動機器室の防犯設備と自動機器本体の防犯措置等とを適切に組み合わせた防犯対策を講ずること。		◎				◎		
		設　114	照明設備および非常用照明設備の設置	自動機器室における各種犯罪を未然に防止するため、室内の状況が外部から確認できるように、十分な照度の照明設備を設置すること。		◎				◎		
		設　115	扉の一部素通し	各種犯罪を未然に防止するため、扉は外部から内部が見えるように、一部を素通しにすること。		◎				◎		
		設　116	現金装填、保守用空間確保	現金の安全な装填と保守のために、必要な空間を自動機器後面に確保することが望ましい。		○				○		
		設　117	自動運行設備の設置	無人運用を適切に行うため、必要な自動運行設備を設置することが望ましい。		○				○		
	10. 端末機器	設　118	耐震措置	端末機器の移転、転倒による故障や破損を防止するとともに要員を保護するために、移動や転倒を防止する措置を講ずることが望ましい。		○				○		
		設　119	機器のアース	機器の保護のために、アースの必要な機器は必ずアースを分電盤から取ること。		◎				◎		
		設　120	漏水、塵埃への機器の保護措置	水滴や塵埃等から機器を防護するために、防水カバー等の必要な措置を取ることが望ましい。		○				○		

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分 コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	自治体における適用区分 クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク
（Ⅱ）サーバ設置場所												
	1. 位置	設　121	災害の少ない位置	コンピュータシステムへの影響を防止するため、地震、火災。浸水等の災害を受けるおそれの少ない位置とすることが望ましい。		○				○		
		設　122	容易に入れない位置	侵入、破壊、機密漏洩等を防止するため、出入口付近およびエレベータまたは階段で直接入れる位置を避けて設置することが望ましい。		○				○		
		設　123	室名等の非表示	侵入、破壊、機密漏洩等を防止するため、室名等の表示は付さないことが望ましい。		○				○		
		設　124	区画の専用化	安全管理の徹底のため、専用の区画とすることが望ましい。		○				○		
	2. 構造・内装等	設　125	防火区画	建物内他区画の火災による延焼防止のため、建築基準法に規定する防火区画内に位置することが望ましい。		○				○		
		設　126	漏水防止対策	漏水によるサーバー等の被害を未然に防止するため、天井、壁、床面からの漏水防止対策を講ずることが望ましい。		○				○		
		設　127	フリーアクセス床の耐震措置	フリーアクセス床は地震時に損壊することのないよう耐震措置を講ずることが望ましい。		○				○		
	3. 設備	設　128	消防設備の設置	火災によるサーバー等の被害を防止するため、必要な消防設備を設置することが望ましい。		○				○		
		設　129	地震感知器の設置	運転継続の判断のため、サーバー設置場所に地震感知器を設置することが望ましい。		○				○		
		設　130	出入口の出入管理設備、防犯設備の設置	不法侵入を防止するため、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が望ましい。		○				○		
		設　131	温湿度自動記録装置または温湿度警報装置の設置	コンピュータシステムの予防保全、障害時の原因分析のため、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が望ましい。		○				○		
		設　132	空調設備の設置	適切な温湿度条件を確保するため、専用空調を設置することが望ましい。		○				○		
		設　133	ネズミ害の防止設置	ネズミによってケーブルが害を受けることを防止するため、適切な措置を講ずることが望ましい。		○				○		
		設　134	電源コンセントの抜け防止対策	電源プラグが簡単にはずれることのないようにするため、電源コンセントの抜け防止対策を講ずること。		◎				◎		
（Ⅲ）インストアブランチ												
		設　135	他の区画からの侵入防止措置	破壊侵入等を防御するため、インストアブランチの区画はストアの他の区画から独立した防犯区画とすること。		◎						
		設　136	ストアの設備補強策	破壊侵入等を防御するため、ストアの既設施設が金融機関等が求める基準と相違する場合には、設備の補強や運用面での対策を実施すること。		◎						

［Ⅲ．流通・小売店舗等との提携チャネル］

（Ⅰ）コンビニATM												
		設　137	防犯設置	コンビニATMの安全を確保するため、設置形態と周辺の環境に応じて、防犯設備とATM本体の防犯措置等とを適切に組み合わせた防犯対策を講ずること。			◎					

運用基準

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
(I)管理体制の確立																	
	1. 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定めた手順書等の整備	セキュリティ管理を適切に行うため、セキュリティ管理の具体的手順、責任等を明確にした文書を整備すること。	◎						◎	◎			3.2.		3.2.1
		運 2	セキュリティ管理方法を定めた手順書等の評価と改定	セキュリティ管理の方法を最適なものとするため、作成された文章については、実態にあっているかを定期的に評価し、必要に応じて改訂すること。	◎						◎	◎					
		運 3	セキュリティ管理体制の整備	セキュリティ管理を適切に行うため、セキュリティ管理の責任者等を定め、その職務範囲と権限および責任について定めること	◎						◎	◎					
		運 4	システム管理体制の整備	システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、管理体制を整備すること。	◎						◎	◎					
		運 5	データ管理体制の整備	データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備すること。	◎						◎	◎					
		運 6	ネットワーク管理体制の整備	コンピュータネットワークの適切かつ効率的な運用と不正アクセス等の防止のため、ネットワークの管理手順を定め、関係者に周知徹底させることにより、管理体制を整備すること。	◎						◎	◎					
	2. 組織の整備	運 7	防災組織の整備	災害の予防および被害軽減のため、防災組織を整備し、責任者を明確にすること。		◎	◎				◎	◎			3.2.	Ⅱ	
		運 8	防犯組織の整備	犯罪を防止するため、防犯組織を整備し、責任者を明確にすること。		◎	◎				◎	◎					
		運 9	業務組織の整備	コンピュータシステムに係わる業務を円滑かつ適正に運営するとともに、不正を防止するため、業務範囲および責任と権限を明確にし、相互牽制体制を整備すること。		◎	◎				◎	◎					
	3. 各種規定の整備	運 10	各種規定の整備	コンピュータシステムを円滑かつ適正に運用、管理するため、防災、防犯、業務の各組織における責任と権限を明確にした規定を整備すること。	◎						◎	◎			－		
	4. 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の確認	セキュリティ関連文書に定められた事項の遵守状況を確認し、全役職員（外部要員を含む）のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ること。	◎						◎	◎	◎		3.7.2.		5.4 5.5 5.6 5.7 5.8 5.9
(Ⅱ)入退管理																	
	1. 入退館(室)管理	運 11	資格付与および鍵の管理	コンピュータセンターへの入館者、およびコンピュータ室、データ保管室等重要な室への入室者を特定するため、資格付与と鍵の管理を行うこと。		◎	◎				◎	◎			3.4.2.	Ⅲ4.4.1	5.9.5
		運 12	入退館管理	不法侵入、危険物持ち込み、不法持出し等を防止するため、入退館者の資格確認により、コンピュータセンターの入退館管理を行うこと。		◎					◎						
		運 13	入退室管理	不法侵入、危険物持ち込み、不法持出し等を防止するため、コンピュータ室およびデータ保管等重要な室については、資格確認により入退室管理を行うこと。		◎	◎				◎	◎					

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
(Ⅲ)運用管理																	
	1. マニュアルの整備	運 14	通常時マニュアルの整備	コンピュータシステムを正確かつ安全に運用するとともに、本部・営業店等設置の端末機器の誤操作を予防し、事務処理を円滑に行うため、通常時における各種手順（含む操作手順）を定めたマニュアルを整備すること。	◎						◎	◎			－	Ⅱ.2.1.3 Ⅱ.6.1.1	－
		運 15	障害時・災害時マニュアルの整備	障害・災害によるコンピュータシステムへの影響の極小化と早期復旧ならびに本部・営業店等における業務継続のため、障害時・災害時における代替措置、復旧手順および対応方法等について定めたマニュアルを整備すること。	◎						◎	◎					
	2. 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の明確化	無資格者によるアクセスを防止するため、コンピュータシステムとシステムの運用上および業務上重要なファイルは、アクセス権限所有者を特定すること。	◎						◎	◎	◎		3.6.2.	Ⅲ.3.1.2 Ⅲ.3.1.3	5.5.16 5.5.7
		運 17	パスワードが他人に知られないための措置	パスワード等の漏洩防止のため、他人に知られないための注意喚起等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取得・見直し手続きの明確化	各種資源、システムへのアクセスを管理するため、アクセス権限を与えるにあたってその手続きを明確に定めることが必要である。さらに、アクセス権限を適切に保つため、見直しの手続きを明確化することが必要である。	◎						◎	◎	◎				
	3. オペレーション管理	運 19	オペレータの資格確認	コンピュータシステムの不正使用を防止するため、オペレータの資格確認を行うこと。		◎					◎				－	－	－
		運 20	依頼・承認手続の明確化	コンピュータシステムの不正使用を防止するため、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	実行体制の明確化	コンピュータシステムの誤動作および不正使用を防止するため、オペレーション実行体制を明確にすること。		◎					◎						
		運 22	オペレータの記録・確認	オペレーションの正当性を検証するため、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	クライアントサーバーシステムにおける不正使用等を防止するため、依頼、承認等の手続きを明確にし、実行、記録、結果確認等を適切に管理することが望ましい。		○	○				○	○					
	4. 入力管理	運 24	データの入力管理	データの正確な処理と不正防止のため、入力手順を定めること。		◎	◎				◎	◎	◎		－	－	－
	5. データファイル管理	運 25	授受、管理方法の明確化	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、データファイルの授受、保管は定められた方法によって行うこと。	◎						◎				－	Ⅲ.2.3.1	5.5.16
		運 26	修正管理方法の明確化	不正使用・改ざんを防止するため、データファイルに不整合が生じた場合のデータファイルの修正および管理は定められた方法で行うこと。	◎						◎						
		運 27	バックアップの確保	重要なデータファイルの破損、障害等への対応のため、バックアップを取得し、管理方法を明確にすること。	◎						◎	◎					
	6. プログラムファイル管理	運 28	管理方法の明確化	プログラムの改ざん、破壊等を防止するため、プログラムファイルの管理は、定められた方法によって行うこと。	◎						◎				3.6.3.	Ⅲ.2.3.1	5.6
		運 29	バックアップの確保	プログラムの破損・障害等への対応のため、バックアップを取得し、管理方法を明確にすること。	◎						◎						
	7. コンピュータウイルス対策	運 30	コンピュータウイルス対策	コンピュータウイルス等の侵入および感染に備えて、防御、検知、復旧の手順を明確にしておくこと。	◎						◎	◎	◎		3.6.4.	Ⅲ.2.2.1	5.5
	8. ネットワーク設定情報管理	運 31	設定情報の管理	ネットワーク機器の設定情報が不正に変更されないように管理を行うこと。	◎						◎	◎			3.6.1.	Ⅲ.2.3.1	－
		運 32	設定情報のバックアップの確保	ネットワーク設定情報の不正な変更、障害等への対応のため、バックアップを取得し、管理方法を明確にすること。	◎						◎	◎					
	9. ドキュメント管理	運 33	保管管理方法の明確化	不正使用、改ざん、紛失等を防止するため、ドキュメントは定められた方法によって管理すること。	◎						◎	◎	◎		3.3.	Ⅲ.5.3	3.2.1
		運 34	バックアップの確保	災害時の復旧対応のため、復旧に必要なドキュメントはバックアップを取得し、管理方法を明確にすること。	◎						◎	◎					

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
	10. 帳票管理	運　35	未使用重要帳票の管理方法の明確化	不正使用を防止するため、未使用重要帳票の在庫管理および廃棄は定められた方法によって行うこと。	◎										－	－	－
		運　36	重要な印字済帳票の取扱方法の明確化	不正使用を防止するため、重要な印字済帳票の受渡しおよび廃棄は定められた方法によって行うこと。	◎												
	11. 出力管理	運　37	出力情報の作成、取扱いについての不正防止および機密保護対策	出力情報の改ざん、盗難、漏洩等を防止するため、作成、取扱い等にあたっては、不正防止および機密保護対策を講ずること。	◎						◎	◎	◎		－	－	－
	12. 取引の管理	運　38	取引の操作権限の明確化	端末機操作による不正、不当取引を防止するため、取引内容ごとに端末機操作者等が操作できる権限の範囲を明確にすること。		◎	◎								－	－	－
		運　39	オペレータカードの管理	端末機操作による不正取引を防止するため、オペレータカードは管理者を定め管理すること		◎	◎										
		運　40	取引の操作内容の記録・検証	端末機操作による不正取引を防止するため、取引明細表、端末機操作記録等により、取引内容が検証できる体制を整備すること。		◎	◎										
		運　41	届出の受付体制の整備および事故口座の管理	事故による不正使用を防止するため、口座とリンクして顧客資産の移動を可能とする機器および媒体の盗難等の届けを受け付けられる体制を整備すること。また、事故届のあった口座の管理は定められた方法により行うこと。	◎												
		運　42	機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任の明示	利用者に責任と注意を喚起するため、電子的価値を蓄積する媒体および通信等に使用する機器の盗難、破損等に伴い、利用者が被る可能性がある損失および利用者側の責任についてもわかり易く明示すること。	◎												
	13. 暗号鍵の管理	運　43	暗号鍵の管理方法の明確化	不正行為を防止するため、暗号鍵の利用において、暗号鍵の生成、配布、使用および保管等に係わる手続きを定めておくこと。また、その管理書類等は役席者が厳重に管理すること。	◎						◎				－	－	－
	14. 厳正な本人確認の実施	運　44	本人確認の実施	インターネットバンキング等の非対面取引において、口座開設等を行う場合は適切な方法により本人確認を行うこと。			◎								－	－	－
		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の確保	不正払戻し防止のための措置を講ずることにより機械式預貯金払戻し等が正当な権限を有する者に対して適切に行われることを確保すること。	◎												
	15. CD・ATM等および無人化店舗の管理	運　45	運用管理方法の明確化	CD・ATMおよび無人化店舗の安全性を確保し、円滑に稼働させるため、運用管理方法を明確に定めること。			◎	◎							－	－	－
		運　46	監視体制の明確化	無人化店舗における異常状態を発見するため、監視体制を明確にすること。			◎										
		運　47	防犯体制の明確化	無人化店舗における犯罪を防止するため、防犯方法および犯罪発生時の対応方法を明確にすること。			◎										
		運　48	障害時・災害時対応方法の明確化	無人化店舗の円滑な運営のため、障害児・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	無人化店舗の円滑な運営、安全確保のため、各種対応を想定した関係マニュアルを整備しておくこと。			◎										
	16. 渉外端末の管理	運　50	運用管理方法の明確化	渉外端末の不正使用を防止するため、運用管理方法を明確にすること。			◎								－	－	－
	17. カード管理	運　51	管理方法の明確化	安全性の確保および処理の円滑化のため、カードの発行、保管、交付、回収および廃棄は定められた方法によって行うこと。		◎	◎	◎							－	－	－
		運　51-1	顧客に対して犯罪に対する注意喚起	顧客並びに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。			◎	◎									
		運　52	指定口座のカード取引監視方法の明確化	不正使用を防止するため、指定された口座のカード取引を監視できる方法を明確にすること。		◎	◎	◎									
	18. 顧客データ保護	運　53	顧客データの保護策	顧客データを保護し、適正に利用するため、管理・取扱い方法を定めること。	◎						◎	◎	◎		3.3.	Ⅱ.4.2	3.2.3
		運　53-1	生体認証における生体認証情報の安全管理	顧客を認証する手段として、生体認証を用いる場合に、生体認証情報を安全に管理するための手順を定めること。	◎						◎	○	○				

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
	19. 資源管理	運 54	能力および使用状況の確認	コンピュータシステムの障害および処理能力の低下を回避するため、各種資源の能力および使用状況の確認を行い、適切な措置を講ずること。	◎						◎				－	Ⅲ2.1	5.7.1 5.7.2
	20. 外部接続管理	運 55	接続契約内容の明確化	外部との接続を安全かつ正確に行うため、回線接続によるデータ授受に係わる契約締結にあたっては、接続の方法、データフォーマット、データ内容等を明確にすること。	◎						◎				3.6.1.	Ⅲ.3.1	3.2.1
		運 56	運用管理方法の明確化	データ漏洩、不正アクセス等を防止するため、外部接続時には運用管理方法を明確にし、相手先確認、接続条件（パスワード等）の登録・変更管理などを適切に行うこと。	◎						◎						
	21. 機器の管理	運 57	管理方法の明確化	コンピュータシステムを構成する各機器の不正使用、破壊、盗難等を防止するため、定められた方法によって管理すること。		◎	◎				◎	○	○		3.4.1.	－	5.7.1
		運 58	ネットワーク関連機器の保護措置	不正使用、破壊、盗難等を防止するため、重要なデータを扱うシステムを構成するネットワーク機器等は、適切な保護措置が講じられていることが望ましい。		○	○	○			◎	○	○				
		運 59	保守方法の明確化	コンピュータシステムを構成する各機器の障害を防止するため、保守点検を実施し、点検内容および結果を把握すること。		◎	◎				◎	○	○				
	22. 運行監視	運 60	監視体制の整備	異常状態早期発見のため、監視対象、監視内容および監視方法を定めること。	◎						◎	○			3.7.1.	Ⅲ1.1	－
	23. コンピュータ室・データ保管室の管理	運 61	入室後の作業管理	不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室およびデータ保管室等重要な室における入室者の作業を管理すること。		◎	◎				◎				3.4.2.	－	5.9.5
	24. 障害時・災害時対応策	運 62	関係者連絡手順の明確化	障害時・災害時に関係者へ迅速かつ確実に連絡を行うため、連絡手順を定めておくこと。	◎						◎	◎	◎		3.7.3.	Ⅱ.6.1	5.5 5.6
		運 63	対応手順の明確化	障害または災害等によりコンピュータシステムが正常に稼働しなくなった場合の復旧手段を明確にすること。なお、当該手順については、コンティンジェンシープランとの整合性のとれた内容にすること。	◎						◎	◎	◎				
		運 64	障害原因の調査・分析	すばやく復旧するため、障害の原因を調査する手法を講じておくこと。また、障害の発生原因を記録し、傾向分析等を通じて再発防止に役立てること。	◎						◎						
	25. 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の策定	不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧をはかるために、あらかじめコンティンジェンシープラン（緊急時対応計画）を策定しておくこと。	◎						◎	◎	○				
(Ⅳ)システム開発・変更																	
	1. ハードウェア、ソウトウェア管理	運 66	ハードウェア、ソフトウェアの管理	システムの導入、変更、廃棄を確実に行うため、ハードウェア、ソフトウェアの構成管理、版数管理などを行うこと。	◎						◎				－	－	－
	2. システム開発・変更管理	運 67	開発・変更手順の明確化	システム開発・変更における内容の正当性を確保するため、開発・変更手順を明確にすること。	◎						◎						
		運 68	テスト環境の整備	本番システムの安全性を確保するため、本番環境へ影響を与えないようなテスト環境を整備すること。	◎						◎						
		運 69	本番への移行手順の明確化	本番システムの安全性を確保するため、本番への移行に際しては、各システムの特性を考慮し、移行手順を明確にするとともに、関連する各部門の手順の整合性を確認すること。	◎						◎						
	3. ドキュメント管理	運 70	作成手順の明確化	システムドキュメントを適切に作成するため、作成対象とするものを決め、それらについての作成手順を定めること。	◎						◎						
		運 71	保管管理方法の明確化	円滑な利用および改ざん、不正使用等の防止のため、システムドキュメントの保管管理を適正に行うこと。	◎						◎						
	4. パッケージの購入	運 72	評価体制の整備	パッケージを導入する場合のシステム開発・変更を円滑に行うため、パッケージの有効性、信頼性、生産性等を評価する体制を整備すること。	◎						◎						
		運 73	運用・管理体制の明確化	パッケージを導入する場合のシステム開発・変更を円滑に行うため、パッケージの有効性、信頼性、生産性等を評価する体制を整備すること。	◎						◎						
	5. システムの廃棄	運 74	廃棄計画、手順の策定	システムの廃棄を円滑、確実かつ安全に実施するため、運用およびユーザー責任者の承認を得て不正防止、機密保護対策を含めた計画、手順を策定すること。	◎						◎				3.4.1.	Ⅲ.5.3.2	5.5.23
		運 75	情報漏洩防止対策	機密保護や不正防止等のため、システムの廃棄にあたっては機器等から情報漏洩が生じないように防止策を講ずること。	◎						◎						

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
(Ⅴ)各種設備管理																	
	1. 保守管理	運 76	管理方法の明確化	コンピュータシステムを円滑に運用するため、設備の管理責任者および管理方法を明確にし、定められた方法によって管理すること。また、障害時・災害時の対応方法を明確にすること。		◎	◎				◎	◎	◎		3.4.1.	Ⅲ.2.1 Ⅲ.3.1 Ⅲ.3.2	－
		運 77	保守方法の明確化	コンピュータシステムを円滑に運用するため、保守点検を実施し、点検内容および結果を把握すること。		◎	◎				◎	◎	◎				
	2. 資源管理	運 78	能力および使用状況の確認	異常状態早期発見のため、各種設備の容量および性能の限界を把握し、使用状況の確認を行うこと。		◎	◎				◎	◎	○		－	－	5.7.1 5.7.2
	3. 監視	運 79	監視体制の整備	異常状態早期発見のため、監視対象、監視内容および監視方法を定めること。		◎	◎				◎	○	○		3.7.1.	Ⅲ.1.1	5.7.2 5.7.3
(Ⅵ)教育・訓練																	
	1. 教育・訓練	運 80	セキュリティ教育	セキュリティ意識の向上を図るため、全役職員（外部要員を含む）に対するセキュリティポリシーの周知徹底と、具体的なセキュリティ対策実施に関するセキュリティ教育を、担当する業務内容等を勘案のうえで行うこと。	◎						◎	◎	◎		3.5.2.	Ⅱ.5.2.1	5.5
		運 81	要員の教育	システムとその開発対象となる適用業務に関する知識および技能の向上を図るための教育を、担当する業務内容等を勘案のうえで行うこと。	◎						◎	◎	○				
		運 82	オペレーション習熟の教育・訓練	コンピュータシステムに係わる通常時運用の円滑化および営業店事務処理に係わる端末機器の操作習熟のため、オペレーション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	障害時・災害時に備えるため、コンピュータシステムの運用に係わるオペレーション等の教育・訓練を行うこと。	◎						◎	◎	◎				
		運 84	防災・防犯訓練	非常時に備えて、防災・防犯訓練を行うこと。	◎						◎	◎	◎				
(Ⅶ)要員管理																	
	1. 教育・訓練	運 85	人事管理	システムの円滑な運用のため、要員の配置、交代等人事管理を適切に行うこと。	◎						◎	○	○		－	－	－
		運 86	健康管理	作業環境の整備や定期的に健康診断を実施するなど要員の健康管理を適切に行うこと。	◎						◎	○	○				
(Ⅷ)外部委託管理																	
	1. 外部委託計画	運 87	事前での目的や範囲の明確化	システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲等を明確にすることが必要である。	◎						◎	◎	◎		－	－	－
		運 87-1	選定手続きの明確化	外部委託先の選定に際しては手続きを明確にし、委託業者を客観的に評価すること。委託業者の決定にあたっては、責任者の承認を得ること。	◎						◎	◎	◎				
		運 88	作業契約の締結	安全性確保のため、機密保護、安全運行等に関する項目を盛込んだ委託契約を締結すること。	◎						◎	◎	◎				
	2. 外部委託業務管理	運 89	外部委託先の要員の各種ルールの遵守	外部委託先の要員のセキュリティ管理を適切に行うため、外部委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、教育、監査を行うこと。	◎						◎	◎	◎		－	－	3.2.3
		運 90	外部委託先の業務組織の整備と作業の管理、検証	外部に委託した業務内容を確認するため、業務組織の整備を行うとともに、委託契約に基づき管理・検証を行うこと。	◎						◎	◎	◎				
(Ⅸ)システム監査																	
	1. システム監査	運 91	システム監査体制の整備	コンピュータシステムおよびその管理について、有効性、効率性、信頼性、遵守性、および安全性の面から把握、評価するため、システム監査体制を整備すること。	◎						◎	◎	◎		3.8.1.	Ⅱ.3.1.2	3.2.2

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
(X)インストアブランチ																	
		運 92	出店先の選定基準の明確化	インストアブランチの安全性を確保するため、出店先地域やストアの選定基準を明確にすること。			◎								－	－	－
(XI)コンビニATM																	
		運 93	出店先の選定基準の明確化	コンビニATMおよび利用者の安全性を確保するため、出店先地域やコンビニエンスストアの選定基準を明確にすること。				◎							－	－	－
		運 94	現金装填等メンテナンス時の防犯対策	コンビニATMのメンテナンス時の安全性を確保するため、防犯体制および防犯方法を明確にすること。				◎									
		運 95	障害時・災害時対応手順の明確化	コンビニATMの障害時・災害時に迅速な対応を行うため、その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	伝送データの安全性、信頼性を確保し、また不正使用、破壊、改ざん等を防止するため、ネットワーク関連機器の適切な保護措置および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の確立	犯罪発生時に関係者へ迅速に連絡を行うため、所轄の警察および警備会社等関係者との連絡体制の確立および訓練を行うこと。				◎									
		運 98	顧客に対して犯罪に関する注意喚起	顧客ならびに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。				○									
(XII)デビットカード																	
	1. 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	デビットカード・サービス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、情報処理センターや加盟店等と共に安全対策を講ずること。				◎							－	－	－
		運 100	口座番号、暗証番号等の安全性の確保	口座番号、暗証番号等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、情報処理センターや加盟店等と共に安全対策を講ずること。安全対策を講ずること。				◎									
	2. 顧客保護	運 101	デビットカード利用時の顧客保護の措置	デビットカード・サービス利用時の安全性を確保するため、適切な顧客保護の措置を講ずること。				◎									
	3. 顧客への注意喚起	運 102	デビットカード利用時の留意事項の顧客への注意喚起	顧客に注意を喚起するため、デビットカード利用上の留意事項を顧客に明示すること。				◎									
(XIII)オープンネットワークを利用した金融サービス																	
	1. インターネット、モバイル	運 103	不正使用の防止	オープンネットワークを利用した金融サービスの安全性を確保するため、接続相手先が本人であることを確認する予防策やアクセス制限、検知策等の不正使用防止機能を設けること。					◎		○	○		○	－	－	－
		運 104	不正使用の早期発見	利用者を不正使用から守るため、利用者自身が使用状態を確認する機能を設けること。					◎		○	○					
		運 105	安全対策に関する情報開示	利用者が適切に取引機関や金融サービスの選択を行うため、安全対策に関する情報を開示することが望ましい。					○		○	○					
		運 105-1	顧客対応方法の明確化	インターネット、モバイル等を用いた金融サービスにおいて、注意喚起や受付対応等の顧客対応方法を明確にすること。					◎		○	○					
		運 106	運用管理方法の明確化	インターネット、モバイル等を用いた金融サービスにおいて、利用者を保護し、安全性を確保し、円滑に稼働させるため、運用管理方法を明確化すること。					◎		○	○					
	2. 電子メール	運 107	電子メールの運用方針の明確化	電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針を明確にすること。					◎		○	○					

技術基準

[Ⅰ．システム信頼性向上策]

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
(Ⅰ)ハードウェアの信頼性向上対策																	
	1. ハードウェアの障害予防策	技 1	予防保守の実施	ハードウェアの障害を予防するため、装置の特性や重要度に応じ、予防保守を定期的にまたは随時実施すること。		◎	◎				◎	◎	○		－	－	5.7.3
	2. ハードウェアの予備	技 2	本体装置の予備	本体装置の障害時に迅速に対応するため、重要な本体装置には予備を設けること。		◎	◎				◎	◎	○				
		技 3	周辺装置の予備	周辺装置の障害時に迅速な対応を行うため、重要な周辺装置は予備または代替機能を設けること。		◎	◎				◎	◎	○				
		技 4	通信系装置の予備	通信系装置の障害時の迅速な対応のために、重要な通信系装置は予備を設けること。		◎	◎				◎	◎	○				
		技 5	回線の予備	回線障害時の迅速な対応のために、重要な回線は予備を設けることが望ましい。		○	○				○	○	○	◎			
		技 6	端末系装置の予備	端末系装置の障害時の迅速な対応のため、端末系装置は予備または代替機能を設けること。		◎	◎				◎	◎	○				
(Ⅱ)ソウトウェアの信頼性向上対策																	
	1. 開発時の品質向上対策	技 7	システム開発計画における中長期計画との整合性の確認	コンピュータシステム全体の信頼性向上のため、システム開発計画は、中長期のシステム化計画と整合性が取れており、かつ内外の技術調査を実施していること、また開発責任者（システムを企画、開発する部門の長）の承認を得ていること。	◎					◎	◎				－	－	－
		技 8	セキュリティ機能の確保	セキュリティ対策を確実に実施するため、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が取り込まれていることを明確にすること。	◎					◎	◎						
		技 9	設計段階での品質確保	設計段階でのソフトウェアの信頼性向上のため、開発の前提となる要件を明確にするとともに、信頼度設計の考慮や設計作業の標準化等を行い、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確保	プログラミング作成段階での、ソフトウェアの信頼性向上のため、プログラム仕様書に基づいたプログラミングを行うとともにプログラム作成作業に標準化・自動化等を行い、ソフトウェアの品質を確保すること。	◎					◎	◎						
		技 11	テスト段階での品質の確保	テスト段階でのソフトウェアの信頼性向上のために、テスト計画の策定、テスト環境・体制の整備、テストサポート機能の活用、テスト実施段階での各種管理等を行い、ソフトウェアの品質を確保すること。	◎					◎	◎						
		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の確保	配布時のソフトウェアの信頼性を確保するため、配布先の稼働環境との整合性確認やウイルスチェックを行うこと。	◎					◎							
		技 13	パッケージ導入時の品質確保	パッケージソフトウェアの品質を確保するために、機能および自社システムとの整合性を十分確認すること。	◎					◎	◎						
	2. 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確保	営業店新設、機器増設等の定型的変更作業時における正確性を確保するため、変更作業の合理化等の必要な対策を講ずること。	◎					◎	◎				－	－	－
		技 15	機能の変更・追加作業時の品質確保	機能の変更、追加作業時におけるソフトウェアの品質を確保するため、開発時の品質向上対策を準用すること。	◎					◎	◎						

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
(Ⅲ)運用時の信頼性向上対策																	
	1. 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	オペレーションの信頼性を向上させるため、オペレーションの自動化、簡略化を図ることが望ましい。	○					○	◎				－	－	－
		技 17	オペレーションチェック機能の充実	オペレーションミスを防止するため、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の充実	コンピュータシステムの安定稼働のために、各種資源の能力や容量の限界を超えないように負荷状態を監視し、必要に応じて制御する機能を充実すること。	◎					◎	◎				－	Ⅲ.2.1	5.7.1 5.7.2
		技 19	CD・ATM等遠隔制御機能	無人化店舗におけるCD・ATM等の安定運用のために、運用状況を集中監視し、必要に応じて遠隔制御を行う機能を設けること。		◎	◎	◎			◎	◎	◎		－	－	－
(Ⅳ)障害の早期発見・早期回復																	
	1. 障害の早期発見	技 20	システム運用状況の監視機能	障害の早期発見・回復のために、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ること。	◎						◎	○		○	3.7.1.	Ⅲ．1．1	5.7.2 5.7.3
		技 21	障害の検出および障害箇所の切り分け機能	迅速な障害回復に役立てるため、コンピュータシステムに発生する各種障害を的確に検出し、障害箇所を切り分ける機能を設けること。	◎						◎						
	2. 障害の早期回復	技 22	障害時の縮退・再構成機能	障害時に、一部の処理を中断しても、システム全体を停止させることなく運転を続行させるため、機能を縮小し、システムを再構成する機能を設けること。	◎						◎	◎	○		－	－	5.7.4
		技 23	取引制限機能	ファイル障害やプログラムミス等による影響を極小化するため、ファイル単位、科目単位等による取引制限機能を設けること。	◎					／	／	／	／	／			
		技 24	リカバリ機能	障害が発生した場合は、速やかにシステムを回復させ業務を支障なく続行させるために必要なリカバリ機能を設けること。	◎						◎	◎	○				
(Ⅴ)災害時対策																	
	1. バックアップサイト	技 25	バックアップサイトの保有	コンピュータセンター等が災害等により機能しなくなった場合に備えて、業務の優先度を考慮してバックアップサイトを保有することが望ましい、。		○					○				－	－	－

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
[Ⅱ. 安全性侵害対策]																	
(Ⅰ)データ保護																	
	1. 漏洩防止	技 26	暗証番号等の漏洩防止	暗証番号・パスワード等の漏洩防止のため、非表示、非印字等の必要な対策を講ずること。	◎						◎	◎	◎		3.4.4.	Ⅲ.3.1.3	3.2.3 5.5.18 5.5.22 5.5.4
		技 27	相手端末確認機能	公衆電話網を通じて自動着信端末に出力する場合には、誤接続を防止するため、確認可能なものについては相手端末を確認する機能を設けることが望ましい。	○						○	○	○				
		技 28	蓄積データの漏洩防止策	フェイルのコピーや盗聴等による漏洩を防止するため重要なデータについては暗号化の対策を講ずることが望ましい。	○						○	○	○				
		技 29	伝送データの漏洩防止策	データ伝送時の盗聴等による漏洩を防止するため、重要なデータについては暗号化の対策を講ずることが望ましい。	○						○	○	○	◎			
	2. 破壊・改ざん防止	技 30	排他制御機能	ファイル内容の矛盾発生防止のため、ファイルに対する排他制御機能を設けること。	◎						◎				3.6.2	Ⅲ.3.2.1	
		技 31	アクセス制御機能	不正アクセス等からデータを保護するため、プログラムとファイル間のアクセス権限チェック機能等を設けること。	◎						◎	◎	◎				
		技 32	不良データ検出機能	システムへの不良データの混入を防止するため、不良データの検出・除外機能を充実すること。	◎						◎						
	3. 検知策	技 33	伝送データの改ざん検知策	重要なデータの伝送においては、改ざん検知のため対策を講じておくことが望ましい。	○						○				3.6.5.	Ⅲ.3.2.2	
		技 34	ファイル突合機能	故意または過失により起きたファイル間の不整合を早期に発見するため、元帳、精査表、ジャーナル等のファイル間の突合機能を設けること。	◎						◎						

大項目	中項目	項番	小項目	適用にあたっての考え方	適用区分					自治体における適用区分					各ガイドラインの記載箇所		
					建屋、チャネルに依存せず適用	コンピュータセンター	本部・営業店等	流通・小売店舗等との提携チャネル	ダイレクトチャネル	建屋、チャネルに依存せず適用	クラウドセンター	自治体（本庁等）	自治体（支所・出張所・施設等）	ネットワーク	地方公共団体における情報セキュリティポリシーに関するガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	公共ITアウトソーシングに関するガイドライン
(Ⅱ)不正使用防止																	
	1-1. 予防策(アクセス権限確認)	技 35	本人確認機能	不正使用防止のため、業務内容や接続方法に応じ、接続相手先が本人もしくは正当な端末であることを確認すること。	◎						◎	◎	◎	○	3.6.2.	Ⅲ.3.1.3	5.5.7
		技 35-1	生体認証機能	生体認証の導入と運用にあたっては、技術の最新動向等に留意し、その特性を十分考慮し、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	不正アクセス防止のため、システムやデータ等へのアクセスに用いるIDの不正使用防止機能を設けること。	◎						◎	◎	◎				
		技 37	アクセス履歴の管理	アクセス状況を管理するため、システムやデータへのアクセス履歴を取得し、監査証跡として必要期間保管するとともに定期的にチェックすること。	◎						◎	◎	◎				
	1-2. 予防策(利用範囲の制限)	技 38	取引制限機能	不正アクセスを防止するため、端末等取引に使用する機器・媒体の種類、設置場所、用途等により、取引内容の制限機能を設けること。	◎										－	－	－
		技 39	事故時の取引禁止機能	カード、通帳、印鑑等の盗難・紛失等の事故に対処するため、その口座に対する当該媒体による取引を禁止する機能を設けること。また、渉外端末の盗難・紛失等の事故に対処するため、端末ごとの取引禁止機能を設けること。	◎												
	1-3. 予防策(不正・偽造防止対策)	技 40	カードの偽造防止対策	不正使用防止のため、カードの偽造防止のための技術的措置を講ずることが望ましい。		○	○	○			○	○	○		－	－	－
		技 41	電子的価値の保護機能、不正検知の仕組み	電子的価値のコピー、二重使用等の不正行為に対処するため、データの保護機能を具備するか、あるいはその発生を検知できる仕組みを構築しておくことが望ましい。	○						○	○	○				
		技 42	暗号鍵の保護機能	暗号鍵が他人に知られることによる不正行為を防止するため、暗号鍵の保護機能を機器、媒体または、ソフトウェアに具備すること。	◎						◎	◎	◎				
		技 42-1	電子メール、ホームページ閲覧等の不正使用防止機能	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等に対処するため、不正使用防止対策を講ずることが望ましい。	○						○	○	○				
	2. 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	不正侵入を防止するため、重要なデータやプログラムを扱うシステムについては、外部ネットワーク(オープンネットワーク、リモートアクセス等)との接続部分に適切な不正侵入防止策を講ずること	◎						◎	◎	◎	◎	3.6.4.	Ⅲ.3.1 Ⅲ.3.2	5.5.2
		技 44	接続機器の必要最小限化	不正アクセスによるコンピュータシステムへの侵入を防ぐため、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、不必要な機器は接続しないこと。	◎						◎	◎	◎	◎			
	3. 検知策	技 45	不正アクセスの監視機能	不正アクセスを早期に発見するため、アクセスの失敗や不正アクセスを監視する機能を設けること。	◎						◎	◎	◎	◎	3.6.5.	Ⅲ.3.1.5	5.5.3
		技 46	不正な取引の検知機能	不正取引による被害発生の防止等のため、異常な取引状況を早期に把握するための機能を検討し実施すること。	○												
		技 47	異例取引の監視機能	不正アクセスを早期に発見するため、異例取引の監視機能を設けること。	◎												
	4. 対応策	技 48	不正アクセス発生への対応策、復旧策	不正アクセスを検知した場合に備えて、不正アクセスの拡大防止のための対応策、復旧手順を明確にしておくことがの望ましい。不正アクセスを検知した場合、その被害の有無にかかわらず、不正アクセスの拡大防止策、復旧策を講ずること。また、不正アクセスの原因を分析後、再発防止策を講ずること。	◎						◎	◎	◎				
(Ⅲ)不正プログラム防止																	
	1. 防御策	技 49	不正プログラム防御対策	開発、保守、運用時におけるコンピュータウィルス等不正プログラムによる被害を防ぐため、防御対策を講ずること。	◎						◎	◎	◎	◎	3.6.4	Ⅲ.2.2.1 Ⅲ.3.2.1	5.5.6
	2. 検知策	技 50	不正プログラム検知対策	システムの信頼性を確保・維持するため、コンピュータウィルス等の不正プログラムの侵入や組込みの有無を検証する検知対策を講ずること。	◎						◎	◎	◎	◎			
	3. 復旧策	技 51	不正プログラムによる被害時対策	コンピュータウィルス等の不正プログラムによる被害を最小限にするため、発見時からシステム復旧までの対策を講ずること。	◎						◎	◎	◎				