4 各種設備管理
(1) 資源管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　47	各種資源の能力及び使用状況の確認を行うこと。

コンピュータシステムの障害及び処理能力の低下を回避するため、各種資源の能力及び使用状況の確認を行い、適切な措置を講ずること。

1. コンピュータシステムを構成する各種資源の性能及び容量には限界があり、それに起因するコンピュータシステムの障害及び処理能力の低下を回避するため、能力及び使用状況の確認を行うことが必要である。
   また、使用状況の確認結果を継続的に分析し、システムの性能強化、機能強化、組合せの再検討等を行うことが必要である。

   各種資源としては、以下の例がある。
   (1) ハードウェア資源
      ①本体装置
      ②周辺装置
      ③通信系装置
   (2) ソフトウェア資源
      ①各種プログラム
      ②各種ファイル
      ③入出力バッファ、キュー等の緩衝エリア
   (3) ネットワーク資源

2. 資源管理を実施するにあたっては、以下の手順を明確にすることが必要である。
   なお、新たなサービスの提供及び環境変化が想定される場合には、その内容に応じて、業務部署と連携して事務量の変動を加味することが必要である。
   (1) 計画
      管理対象資源の設定、使用状況の確認方法と確認頻度等の資源管理計画の策定
   (2) 実施
      統計プログラム、モニタリング等による各種資源の利用率、使用容量等のデータ収集、分析、評価の実施
   (3) 検証・報告
      資源容量等の設定内容の妥当性検証、資源不足等によりシステム運行に支障が見込まれる場合の対応策の検討及びまとめ

会員意見募集版

能力及び使用状況の確認としては、以下の例がある。

(1) レスポンス時間及びバッチ処理時間が、許容範囲であることを確認する。
レスポンス時間とは、オンラインシステムで取引 1 件を処理する時間を指し、バッチ処理時間とは、バッチシステムにおけるジョブのスタートからエンドまでの所要時間を指している。
なお、オンライン処理においては単位時間当たりの処理件数、バッチ処理においてはオンライン処理に影響を与えないことを確認する。

(2) 各種資源の能力限界を把握し、定期的に使用状況の確認を行う。
各種資源の使用状況を確認し、能力限界との比較を行うことにより、あらかじめ対応策を考えておく。
また、システム処理における上限（同時アクセス数、1 日における最大値等）を設定している場合には、その設定内容の定期的な確認と事務量等の管理を行う
なお、Web システムにおいて、想定事務量を超えた際には、アクセスの制限（流量制限）等を行う。

(3) 各ファイルの使用可能容量を把握し、定期的に使用状況の確認を行う。

(4) 新規システムの追加、ネットワークの拡大、接続形態の変更などを行った際には、ネットワークの能力と使用状況を確認し、レスポンス時間等の処理能力が許容範囲内であることの確認を行う。

（参考）
勘定系オンライン運行中は、使用する資源やオンラインシステムとの競合等について確認がなされ、オンラインに影響を与えないことが確認されているプログラム以外の走行を禁止すること。

会員意見募集版

4 各種設備管理
(2) 機器の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　48	ハードウェア及びソフトウェアの管理を行うこと。

システムの導入、変更及び廃棄を確実に行うため、ハードウェア及びソフトウェアの構成管理、並びに版数管理などを行うこと。

1. システム開発、導入時においては、下記項目について、考慮し把握することが望ましい。
   (1) 製品入手可能期間（販売終了予定日等）
   (2) サポート期間（サポート終了予定日、サポート期間延長の可否）
   特にサポート期間については、製品、バージョンにより異なるので、注意が必要である。

2. ハードウェア及びソフトウェアを適切に管理するため、台帳等を作成することが必要である。
   なお、本部・営業店等に設置されているハードウェア及びソフトウェアを主管部署が一括管理する場合には、主管部署で作成した台帳を配布し、本部・営業店等においても識別管理できるようにすることが望ましい。
   また、主管部署においては、当該システムのシステム構成図、ネットワーク接続図等を整備し、システム構成変更などに的確に対応できるようにすることが必要である。

   管理する項目としては、以下の例がある。
   (1) ハードウェア
   ①ハードウェア名称
   ②製造会社名と型式名（型式番号）
   ③識別用シリアル番号
   ④費用
   ⑤導入日
   ⑥資産管理番号もしくはリース契約番号
   ⑦当初の配備先
   ⑧現在の配備先
   ⑨使用責任を持つユーザー名
   ⑩保守契約先
   (2) ソフトウェア
   ＜自社開発ソフトウェア＞
   ①プログラム名
   ②当初開発年月日
   ③最終更新年月日
   ④利用部署名もしくはユーザー名

会員意見募集版

＜購入ソフトウェア＞
①製品名
②製造会社名及び契約代理店名
③買取り、あるいはライセンス契約の区別
④費用
⑤導入日
⑥資産管理番号
⑦バージョン番号
⑧シリアル番号
⑨利用ユーザー名
⑩サーバーソフトウェアとして導入された場合のライセンス数
⑪保守契約先

3. システム運用時においてもサポート確保、バージョンアップ、脆弱性対策等を可能とするために、サポート期間（サポート終了予定日、サポート期間延長の可否等）について考慮し把握することが望ましい。

4. コンピュータセンター、システム主管部署などにおいては、オペレーティングシステムなどの基本ソフトウェアについてベンダー等から修正情報を収集し、適切なバージョンのものを導入することが必要である。

5. オペレーティングシステムなどの基本ソフトウェア及びソフトウェア製品（ミドルウェアを含む）については、ベンダー等から修正情報を収集し、対応を検討することが必要である。
対応としては、脆弱性に対応する適切な修正プログラムの適用することが考えられるが、修正プログラムを適用しない場合には運用による回避策、代替策等が考えられる。
また、発見された脆弱性の業務への影響度に応じて、業務の継続可否等を検討することが望ましい。

6. パソコン等を別の用途に再利用するときには、コンピュータウイルス及び不正プログラムが混入されていないかチェックすることが必要である。
コンピュータウイルスについては、以下の基準項目を参照のこと。
(1) コンピュータウイルス等不正プログラムへの防御対策 【実 20】
(2) コンピュータウイルス等不正プログラムの検知対策 【実 21】

7. ハードウェアの損害やソフトウェアのバグ、不正プログラムによるシステムの障害により生じた損害賠償責任、逸失利益、業務継続に要した費用等について保険の適用を検討することが望ましい。

会員意見募集版

4 各種設備管理
(2) 機器の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　49	機器の管理方法を明確にすること。

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。

1. コンピュータシステムを構成する各機器については、管理責任者を明確にするとともに、以下の点を考慮して管理することが必要である。
   (1) 関係者以外容易に接近できない。
   (2) 入力機器（端末機など）、出力機器（プリンターなど）及び重要なサーバー等は、許可された人のみ操作ができる。

   なお、システムの構成、使用形態、使用状況、設置台数等を把握することが望ましい。

   具体的な実施方法としては、以下の例がある。
   (1) 関係者以外の接近防止
      ①コンピュータ室や重要なサーバーの設置場所への入室資格付与【実 56】
      ②施錠による管理【実 56】
   (2) 機器の操作資格の付与
      ①操作者の資格確認【実 35】
      ②ID の付与や鍵の貸与などによるアクセス権限の付与【実 25、実 27】
      ③端末の権限制限機能の設定【実 11】
   (3) 持出しが容易な機器類の盗難防止
      ①ワイヤー等により設置機器の固定
      ②鍵付ラックへの収納
   (4) 記録媒体の使用制限【実 3】
      ①持出し、持込み許可
      ②使用許可

2. 機器を修理等で外部に持ち出す時、情報漏洩等がなされないように、修理時等の管理方法についても定めておくことが必要である。

3. 機器の不正使用、破壊、盗難等により生じた損害、業務上の逸失利益、業務の継続に要した費用等について保険の適用を検討することが望ましい。

会員意見募集版

（参考）
スマートデバイスに関わる考慮点については【実 118】を参照のこと。

会員意見募集版

4 各種設備管理
(2) 機器の管理

適用区分					基準分類
共	セ	本	提	ダ	付加
	◎	◎	◎		

実　50	ネットワーク関連機器の保護措置を講ずること。

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については、適切な保護措置を講ずること。

1. 重要なデータを扱うシステムの場合、MDF、IDF、ルータ、ファイアウォール等のネットワーク機器に関しても不正使用、破壊、盗難等された場合の影響が大きい。このため、ネットワーク機器も、必要に応じてサーバー設置場所に準ずる機器管理を行うことが望ましい。

(1) サーバーの機器管理については【実 49】参照のこと。
(2) ネットワーク機器の設定情報管理については【実 42、実 43】参照のこと。

会員意見募集版

4 各種設備管理
(2) 機器の管理

適用区分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　51	機器の保守方法を明確にすること。

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、点検内容及び結果を把握すること。

1. コンピュータシステムの保守には、定期保守と随時保守があり、保守の計画は対象機器ごとの使用状況及び緊急度とメーカーの体制を勘案し作成することが必要である。
   その場合、以下のような点について取り決めておくことが必要である。【実 52】
   また、保守点検実施後、その内容と結果について把握することが必要である。
   (1) 点検対象
   (2) 点検周期
   (3) 点検内容

2. 保守点検の際は、機器の盗難、破壊、情報の持出し等がなされないように、機器の重要性に応じて、当該機器を管理する部署の者が立ち会うことが必要である。

3. 連絡等に備えてメーカーの保守体制、責任者・担当者の氏名、電話番号、保守担当範囲等を十分に把握することが必要である。なお、メーカーには、保守専門会社を含んでいる。

   保守要員の確保の方法としては、以下の例がある。
   (1) 必要時に電話等の連絡による招集
   (2) メーカー保守要員の常駐

4. 保守点検については、以下の点について管理運用することが必要である。
   (1) 保守内容の報告制度
   (2) 保守連絡会議
   (3) 保守についての統計分析
   (4) 保守計画の策定
   (5) 前回の保守点検以降のエラーログ解析結果

5. 保守点検のスケジュールについては、以下のような点を考慮することが必要である。
   (1) 設備関連工事と保守点検スケジュールを調整すること。
   (2) CD･ATM 等の休日稼働、夜間稼働等を考慮し、保守点検スケジュールを調整すること。

会員意見募集版

4 各種設備管理
(2) 機器の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実　52	機器の予防保守を実施すること。

ハードウェアの障害を予防するため、装置の特性及び重要度に応じ、予防保守を定期的にまたは随時実施すること。

1. コンピュータシステムの信頼性を向上させるためには、まずシステムの構成要素であるハードウェアの信頼性向上が重要であり、ハードウェアの障害の発生を極少化させるため、装置の特性及び重要度に応じ、予防保守を実施することが必要である。

   予防保守の具体的な内容としては、以下の例がある。【実 51】

   (1) 定期保守

   定期保守とは、装置の特性及び重要度に応じ、あらかじめ定められた点検項目及び周期に従って、障害を未然に防止するために行うもので以下の形態がある。

   ①全体保守

   システム全体を停止して、総合的に行う予防保守である。

   ②個別保守

   システム運転時も含め、運用に影響を与えない範囲で、装置個別に行う予防保守である。なお、オペレータが始業前に行うクリーニング等も重要な項目である。

   (2) 随時保守

   随時保守とは、装置個別の使用状況、障害発生状況やエラーログ情報の収集・分析から今後の障害発生の可能性を察知し、障害を未然に防止するために随時行うものである。

2. 24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた適切な予防保守を行うことが必要である。

会員意見募集版

4 各種設備管理
(3) コンピュータ関連設備の保守管理

適用区分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

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。

コンピュータシステムを円滑に運用するため、設備の管理責任者及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。

1. コンピュータシステムの円滑な運用を確保するため、コンピュータシステム（含む端末機器等）に係わる電源、空調、給排水、防災、防犯、監視及び回線関連の設備は、各設備の管理責任者を明確にするとともに、定められた方法によって管理することが必要である。
   また、障害時・災害時のコンピュータシステムへの影響を最小限にとどめるために、対応方法を明確にすることが必要である。

2. 端末機器、CD・ATM 等の自動機器等を円滑に運用するために、電源設備、各種センサー、カメラ等防災・防犯設備等の管理方法を明確にすることが必要である。
   また、災害の発生に備えて、消火設備、監視設備等が正常に稼働するよう適切な管理を行うことが必要である。
   さらに、電源容量等各設備の能力を把握し、OA 機器、パソコン等の増設に備える必要がある。

   管理方法としては、以下の例がある。
   (1) 各設備の操作手順書を備える。
   各設備の誤操作を防止するとともに、障害・災害発生時の対応を適切かつ迅速に行うため、各設備の操作手順書を備える。
   (2) 障害時の切替手順を定める。
   (3) 障害時における保守要員の緊急招集体制を定める。
   (4) 非常時における関係者への連絡方法及び連絡内容を明確にする。
   コンピュータシステムへ影響を及ぼす障害・災害発生時の対応を迅速に行うため、コンピュータシステムの管理責任者等への連絡方法及び連絡内容を明確にする。
   (5) 非常時の稼働に必要な燃料等を把握する。
   障害・災害発生時にもコンピュータシステムを円滑に運用するため、各設備で使用する重油、水等の管理を適切に行う。
   (6) 定期的な設備の機能点検・確認の計画を立て実施する。
   例えば、バックアップサイトへの切替えや復旧等の大掛かりな障害テスト、毎月の自家発電テスト、空調バックアップテスト及び絶縁テスト等を行うことが必要と考えられる。

会員意見募集版

(7) 設備関連機器の保守・運用を外部業者に委託する場合は、特に管理責任を明確にし、安全指導を徹底する。
(8) 夜間、休日サービス等無人化運転で使用される設備を明確にし、管理を行う。
(9) 設備の操作盤等の鍵は、鍵の管理責任者が管理する。
(10) 携帯電話等から放射される電波により、コンピュータ関連機器が誤動作するおそれがあるため、コンピュータ室及び重要なサーバー設置場所における携帯電話等の機器の使用については、メーカーと協議のうえ、当該機器の使用を制限する等の対策を講ずる。
(11) 障害原因を把握し、対策を講ずるとともに、障害記録を整理保存し、障害発生原因を時系列的に分析することにより、問題点の改善を図る。

会員意見募集版

4 各種設備管理
(3) コンピュータ関連設備の保守管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

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。

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、点検内容及び結果を把握すること。

1. コンピュータシステム（含む端末機器等）に係わる電源、空調、給排水、防災、防犯、監視及び回線関連等の設備の保守点検にあたっては、コンピュータシステムの運転スケジュールとの調整を図り、点検対象、点検周期、点検内容等を明確にして行うことが必要である。
   なお、保守点検にあたっては、事前の作業計画及び事後の作業結果について各々書面にて報告を求め、検収後記録として保管することが必要である。

2. 防災設備の保守については規則を設け、定期的に点検を実施することが必要である。防災設備については【設 80】を参照のこと。

3. 設備を長時間停止した場合の再稼働にあたっては、保守点検を実施することが必要である。

4. 代替機等の常時稼働しない設備は、正常稼働することを定期的に確認することが必要である。

5. 設備保守にあたっては、設備管理責任者とシステム運用管理者の連絡を密にし、システム運用に影響を与えないようにすることが必要である。

6. 電源設備、空調設備のようなコンピュータシステムに直接影響を与える可能性のある設備の保守作業は、オンライン時間帯を避けて行うことが望ましい。

7. システム稼働中に一部機器を保守する場合には、稼働中のシステムに影響を与えないための手順を徹底するとともに、当該機器の責任者立会いのもとに作業を行うことが必要である。

8. 電源及び監視装置の接続系統を正確に把握するとともに、変更増設工事後も接続系統を整備することが必要である。

参照法令	消防法第 8 条、第 17 条の 3 の 3、消防法施行規則第 31 条の 4

会員意見募集版

4 各種設備管理
(3) コンピュータ関連設備の保守管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

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。

コンピュータシステムの異常状態を早期に発見するため、各種設備の容量及び性能の限界を把握し、使用状況の確認を行うこと。

1. コンピュータシステムの安定稼働を維持し、各種設備の異常状態を早期に発見するため、管理者は各設備の容量及び性能を把握するとともに、以下のような点に留意することが必要である。

(1) コンピュータシステムを構成する各機器の増設
現在の各種設備の限界容量を超えないか、各種設備の容量も増設する必要がないかを検討する。

(2) コンピュータ室内のレイアウト変更
レイアウト変更後も通路、保守スペースの確保、床加重等の安全性を確認する。

ここでいう設備とは、以下のようなものを指している。

(1) 受電設備（契約容量に留意すること）
(2) 定電圧定周波装置（CVCF）
(3) 蓄電池設備
(4) 自家発電設備
(5) 水冷装置
(6) 空調設備
(7) 給・排水設備
(8) 消火設備
(9) 監視設備
(10) 回線関連設備（障害時対応の DDX 等）
(11) 非常用通信設備（無線、衛星通信等）

会員意見募集版

4 各種設備管理
(4) 入退館（室）管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　56	入館（室）の資格付与、及び鍵の管理を行うこと。

コンピュータセンターへの入館者、及びコンピュータ室、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。

1. コンピュータセンターへの入館者を特定するため、写真入り入館許可証を発行する等、資格の付与を行うことが必要である。
   また、コンピュータセンターへの入館が許可された者であっても、コンピュータ室、データ保管室、中央管理室（中央監視室、防災センター等）、電源室、空調機械室、及び重要なサーバー設置場所への入室者を特定するため、所属、立入場所等を判別できる識別章を発行することが必要である。
   さらに、本部・営業店等における重要なサーバーの設置場所への出入についても、入室者への資格付与及び鍵の管理を行うことが必要である。
   なお、プログラム開発場所についても十分な管理を行うことが望ましい。

   重要なサーバーの設置場所については、以下の基準項目を参照のこと。
   (1) 重要なサーバー設置場所　位置　【設 121～124】
   (2) 重要なサーバー設置場所　構造・内装　【設 125～127】

   資格付与の方法としては、以下の例がある。
   (1) 常駐者（コンピュータセンター業務に従事する役職員・他社の勤務者、コンピュータセンター業務に係わりの深い他部門の役職員等。以下同じ）に対しては、写真入り入館許可証の発行（機械により入退管理を行う場合は、資格の登録・入退出カードの発行、及び識別コードの付与等）及び所属、立入場所等を判別できる識別章の発行を行う。なお、所属、立入場所等が明示された写真入り入館許可証は識別章を兼ねることができる。
      ①資格付与されたことが確認できるものであれば、ここでいう写真入り入館許可証に該当すると考えられる。
      ②ここでいう識別章とは、名札、バッジ、腕章等を指している。所属、立入場所が容易に判別できる方法としては、例えば、これら識別章の色分けが考えられる。
      ③ここでいう機械とは、あらかじめ設定された入退資格を識別し、扉の開閉（施錠、解錠）を行う出入管理設備を指している。【設 16】
   (2) 資格喪失時には、写真入り入館許可証、及び識別章を回収する。

   鍵管理の方法としては、以下の例がある。

会員意見募集版

(1) 出入口の鍵は定められた場所に保管し、管理は特定者が行う。
なお、鍵の複製を要する場合は、所定の方法により行う。

(2) 鍵の受渡者の氏名、及び受渡時の時刻を記録する。
記録の目的は鍵の授受の明確化により責任の所在を明らかにするとともに、管理の徹底を図ることにある。なお、貸出用の入退出カード等についても、この項目を適用し、管理の徹底を図る。

(3) 入退出カードの発行管理、識別コード等の管理は特定者が行う。
①入退出カードの発行管理は特定者が定められた方法によって行うとともに、有資格者が資格を喪失した場合は、入退出カードを速やかに回収する。
②入退出カードの紛失には十分注意して保管管理する。
③入退管理用識別コードの登録・変更・抹消は特定者が定められた方法によって行う。なお、入退管理用識別コードの登録・変更にあたっては、容易に推測できないコードを選択する。
④入退出カード等の紛失、毀損、不携帯等の場合の手続きを明確にする。
⑤入退管理用テンキーは、定期的に清掃またはテンキー保護カバーを交換するなど、外見的にパスワードが推測できない措置を講ずる。
⑥カード、識別コード、パスワード以外による資格確認については【設 16】を参照のこと。

2. 資格付与にあたっては、コンピュータ室、データ保管室、中央管理室（中央監視室、防災センター等）、電源室、空調機械室、及び重要なサーバー設置場所への入室者を特定することが必要である。
入室者を特定する例としては、表１のようなものが考えられる。
なお、ここに示した者以外に入室を許可する場合は、その際の資格付与方法についても明確にすることが必要である。

表１　入室者の特定例

室	入室資格者
コンピュータ室 データ保管室 電源室 空調機械室 中央管理室 重要なサーバー設置場所	オペレータ、コンピュータシステムの管理者 ライブラリ管理者、データの保管管理者、プログラムの保管管理者 電源設備の管理者 空調設備の管理者 電源設備、空調設備、及び防災・防犯設備の管理者 サーバーの管理者

会員意見募集版

＜会員意見募集版＞

4 各種設備管理
(4) 入退館（室）管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎				

実　57	入退館管理を行うこと。

不法侵入、危険物持込み、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。

1. 不法侵入、危険物持込み、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が必要である。
   共同ビルを利用しているコンピュータセンターでは、入退館管理を行うことができない場合が考えられる。そのような場合は、入退室において、入退館管理と同等の管理を行うことが必要である。

   入退館管理の具体的な内容としては、以下の例がある。
   (1) 常駐者に対しては、写真入り入館許可証（機械により入退管理を行う場合は、カード、識別コード等）により入退館の資格を確認する。また、館内にあっては、識別章を常時着用させる。
   (2) 訪問者（常駐者以外の役職員、写真入り入館許可証未発行の他社の勤務者を含む。以下同じ）に対しては、身元及び用件を確認のうえ、入退館を許可する。また、訪問者用の識別章を貸与し、館内にあっては常時着用させ、退館時に回収する。
   (3) 訪問者については、来訪者名簿に氏名、勤務先、電話番号、用件、訪問先、入館時刻、退館時刻、貸与識別章番号等を記録する。
   (4) 訪問者に対しては、面会場所を特定し、被面会者が訪問者を確認のうえ、案内する。
   (5) 必要に応じ入退館者の所持品検査を行う。
   (6) 搬出入物品は、納品書・受渡し書、許可証等で確認を行う。
   (7) 警備員を配置する。

2. 入退資格が付与されている者であっても、夜間、休日の入退館については、入退館者名の入館受付への事前通知、入退館記録の事後チェックなど、手続きを明確にすることが必要である。

会員意見募集版

4 各種設備管理
(4) 入退館（室）管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　58	入退室管理を行うこと。

不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室及びデータ保管室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。

1. コンピュータ室及びデータ保管室、中央管理室（中央監視室、防災センター等）並びに重要なサーバー設置場所は、コンピュータ処理の中枢を占める機器、データファイル、プログラムファイル等が設置・保管されているため、入館を許可されたものであっても、入室に際しては再度、資格確認を行うことが必要である。

   入退室管理の内容としては、以下の例がある。

   (1) 入退室者の資格確認は識別章等により行う。

   コンピュータ室及びデータ保管室、中央管理室並びに重要なサーバー設置場所への入退室は、以下のような方法で行うことが考えられる。

   ①機械により入退室管理を行っている場合は、入退室カードに付与されている資格の確認または識別コードの確認等により、自動的に入室許可を与える。

   ②入室受付窓口で、受付係等が識別章を確認のうえ、入室許可を与える。

   ③管理者が、入室の際に資格確認を行い、入室許可を与える。

   (2) 入退室者の氏名、入退室時刻、危険物や可搬記憶媒体等の持込み物、及び持出し物の記録をする。

   記録の目的は、在室時間を明確にし、障害及び不正使用等が発生した場合の原因究明を容易にするためであり、当該記録については一定期間保管する。

   なお、機械により自動的に記録することも考えられる。

   (3) コンピュータ室への用紙等可燃物の持込みは、必要最小限にする。

   (4) 保守または工事の目的以外、危険物または燃焼器具をコンピュータ室及びデータ保管室、中央管理室へ持ち込まない。

   (5) コンピュータ室への可搬記憶媒体の持込み及び持出しは、必要最小限とし、管理者が許可を与える。なお、管理者が持込み及び持出しを行う場合は、別の管理者が許可を与える等、相互牽制が働くような仕組みを考慮する。

   (6) 訪問者による作業については、必要に応じて管理者または管理者の指示を受けた者の監視下に置く。

2. 本部・営業店等における重要なサーバー設置場所については、上記に準じて入退室管理を行うことが望ましい。

会員意見募集版

3. 入退室を許可された者の搬出入物品であっても、不審な場合は内容を確認することが必要である。

会員意見募集版

4 各種設備管理
(4) 入退館（室）管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　59	入室後の作業を管理すること。

不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室及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。

1. コンピュータ室及びデータ保管室、中央管理室（中央監視室、防災センター等）並びに重要なサーバー設置場所への入室を認めた場合には、入室後の作業を管理することが必要である。

   入室後の作業管理の内容としては、以下の例がある。
   (1) 重要な室へ入室して行われる作業には監督者を配置する。
   (2) 許可された区画以外に立ち入らないよう制限する。
   (3) 未使用区画は施錠し、定期的に確認する。
   (4) カメラ、ビデオ、パソコン、記憶媒体等の記録用機器を許可なく使用させない。

2. 本部・営業店等における重要なサーバー設置場所等については、上記に準じて入室者の作業の管理を行うことが望ましい。

会員意見募集版

4 各種設備管理
(5) 監視

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　60	各種設備の監視体制を整備すること。

各種設備の異常状態を早期に発見するため、監視対象、監視内容及び監視方法を定めること。

1. 各種設備の異常状態を早期に発見し、コンピュータシステムへの影響を軽減させるため、以下の監視対象、監視内容及び監視方法等の監視体制を整備することが必要である。
   (1) コンピュータセンターにおける監視体制
      ①監視対象、内容
         a.コンピュータシステムの正常稼働のための監視
            対象：電源、空調、給・排水設備
         b.防災、防犯のための監視
            対象：火災警報装置、センサー警報装置、入退館チェックシステム及び遠隔監視モニター装置等
      ②監視方法
         異常状態を発見する方法としては、以下の例がある。
         a.操作盤、バルブ等に正常値または正常位置を明示し、巡回監視の際に確認する。
         b.警告灯または警告ブザーにより、異常状態を中央管理室に通報する。
         c.中央管理室（中央監視室・防災センター）等において、電源、空調、給排水、防犯設備等の集中監視を行う。
   (2) 本部・営業店等における監視体制
      本部・営業店等に設置された重要なサーバーについては、運用状況に合った最適な監視方法をベンダー等と相談し、コンピュータセンターに準じた監視体制を整備することが望ましい。

2. 異常状態を発見した場合の対応方法を設備ごとに明確にすることが必要である。

   対応方法を決定する要素としては、以下の例がある。
   (1) 各種設備の容量及び停止可能時間 【設 61】
   (2) 代替機の有無

会員意見募集版

5 システムの利用
(1) 取引の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　61	各取引の操作権限を明確にすること。

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。

1. 不正、不当取引を防止するため、取引の重要度等により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が必要である。
   また、営業店以外の場所で１人で端末機操作が行える渉外端末等については、権限の範囲を明確にすることが必要である。

2. 異例取引を行う場合には、オペレーションに先立ち、当該取引権限保持者の承認を得ることが必要である。

会員意見募集版

5 システムの利用
(1) 取引の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実　62	オペレータカードの管理を行うこと。

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。

1. 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必要がある。

ここでいうオペレータカードとは、端末機の操作にあたり操作権限者であることを確認するためのものを指し、オペレータキー、ID 等を含むものとする。

オペレータカードの管理方法としては、以下の例がある。

(1) オペレータカードの管理者を明確にするとともに端末機操作者にオペレータカードを貸与する場合は貸与簿等により管理する。
(2) 異例取引を実行できる役席カード（監査カード）は役席者が管理し、使用記録を残す。
(3) 有資格者が使用資格を失った場合、その者に貸与したオペレータカードは速やかに回収する。

ID 等の管理方法としては、以下の例がある。

(1) ID 等の登録、変更、抹消に際しての依頼手続きを明確にする。
(2) ID 等の登録、変更、抹消の処理にあたる責任者を明確にするとともに管理簿等により管理する。
(3) 有資格者が使用資格を失った場合、その者に付与されていた ID 等は速やかに抹消する。

会員意見募集版

5 システムの利用
(1) 取引の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実　63	取引の端末機操作の内容を記録・検証すること。

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。

1. 取引内容等が記録された端末機のジャーナル、コンピュータセンターから還元される取引明細表等を使用した検証方法を定めておくことが必要である。

検証方法としては、以下の例がある。

(1) 端末機操作者等を記録する。

端末機操作記録等に記録する内容として、取引内容のほか以下の項目が考えられる。

①端末機操作者

②端末番号

③処理通番

④処理時刻

ここでいう端末機操作記録等とは、営業店における伝票、端末機のジャーナル、コンピュータセンター及び営業店におけるジャーナルファイルなどを指している。

なお、端末機から入力された取引の正当性を検証するため、取引通番の管理を行うことが考えられる。

(2) 異例取引は取引記録を当該取引権限保持者が検証する。

検証の方法としては、以下の例がある。【実 18】

①還元帳票による方法

②オンライン照会による方法

③モニター専用（指定）端末による方法

(3) 端末機操作記録等の保存期間を定め保存する。

会員意見募集版

5 システムの利用
(1) 取引の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

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及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。

1. 金融機関等においては、顧客からの届出を速やかに受け付ける体制を整備し、事故による不正使用を防止することが必要である。
   なお、顧客の不安を防ぐためには、届出の受付は有人対応とすることが望ましい。

   「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」（以下、預金者保護法）により、預金者は真正カード等が盗取されたと認めた後、速やかに、当該金融機関に対し盗取された旨の通知を行うことが求められている。

   ここでいう事故とは、金融機関等が顧客に提供した機器、IC カード、磁気ストライプ付カード、通帳、印鑑、証書、証券等の盗難、紛失等を指している。

（参考 1）
預金者保護法
第五条（盗難カード等を用いて行われた不正な機械式預貯金払戻し等の額に相当する金額の補てん等）
預貯金者は、自らの預貯金等契約に係る真正カード等が盗取されたと認める場合において、次の各号のいずれにも該当するときは、当該預貯金等契約を締結している金融機関に対し、当該盗取に係る盗難カード等を用いて行われた機械式預貯金払戻しの額に相当する金額の補てんを求めることができる。
一　当該真正カード等が盗取されたと認めた後、速やかに、当該金融機関に対し盗取された旨の通知を行ったこと。
二　当該金融機関の求めに応じ、遅滞なく、当該盗取が行われるに至った事情その他の当該盗取に関する状況について十分な説明を行ったこと。
三　当該金融機関に対し、捜査機関に対して当該盗取に係る届出を提出していることを申し出たことその他当該盗取が行われたことが推測される事実として内閣府令で定めるものを示したこと。

会員意見募集版

2. 事故届を受け付けた場合は、受付時刻等を記録するとともに、直ちに登録管理することが必要である。なお、盗難等の電話連絡を受けた場合、書面による届出を受領するまでの間、適切な措置を講ずることのできる体制を整備することも必要である。【実 12】

3. 夜間、休日においても CD・ATM 等のサービス提供時間帯においては、例えば管理センター等において顧客からの届出を受け付け、即時に支払停止等の処置を行う必要がある。
また、CD・ATM 等のサービス提供時間帯外に顧客からの届出を受け付けた場合は、CD・ATM 等の稼働開始前までに支払停止等の処置が必要である。
なお、個別金融機関が受け付けしない時間帯の受付窓口を、共同で運営する方式もある。

（参考 2）
預金者保護法第五条第一項において、預金者が被害額の補償を受けるための条件として、『当該真正カード等が盗取されたと認めた後、速やかに、当該金融機関に対し盗取された旨の通知を行ったこと。』が定められており、金融機関においては、預金者から速やかに通知を受けるための体制を整備することが、立法過程や、金融庁「偽造キャッシュカード問題に関するスタディグループ」の議論等において求められている。

「偽造キャッシュカード問題に関するスタディグループ最終報告書」
http://www.fsa.go.jp/

4. 事故登録等の解除にあたっては、規則、事務手続き上でも問題のないことを確認する等、特に注意を払うことが必要である。

5. 事故届の受付窓口が、事務センター、コンピュータセンター、及び外部委託先である場合も同様の措置を講ずることが必要である。

6. 顧客に対し、事故届の受付窓口（連絡先電話番号等）を周知する必要がある。

周知方法としては、以下の例がある。
(1) 配布パンフレット、ホームページ、店頭ポスター等に掲載
(2) カード、通帳等に掲載

7. 事故届の受付窓口を電話会社の電話番号案内サービスに登録する際には、オペレータが検索しやすいように適切な名称で連絡先を登録することが必要である。

参照法令	偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律（平成 17 年法律第 94 号）

会員意見募集版

5 システムの利用
⑵ 入出力管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
	◎	◎			

実 65	データの入力管理を行うこと。

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。

1. 情報システムに入力するデータを正確に処理するとともに完全性を確保し、機密を保護し、不正を防止するために、データの入力手続き、承認等の手順を定め、遵守することが必要である。

入力管理ルールの制定項目としては、以下の例がある。

(1) 入力管理の責任者の設置、職務の明示
(2) 入力データ作成の手続き
　①原始データの作成要領
　②入力指示
(3) 入力データの授受
　①手続き
　②担当者
　③授受の記録
　　a.授受者
　　b.日付
　　c.データ件数
　　d.授受データの形状とラベル内容
(4) 重要データ、機密データの取扱者の限定、確認のタイミング
(5) 入力承認（入力データの承認者）
(6) 承認時期（入力前、入力後）
(7) データのチェック
　①データ内容の確認
　②データ原票と入力データの照合
(8) 入力の取消し、修正、追加
(9) 入力記録の取得、管理、保存

会員意見募集版

5 システムの利用
(2) 入出力管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

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及び機密保護対策を講ずること。

1. 重要な出力情報の作成、授受、保管、管理及び廃棄については、改ざん、盗難、漏洩等の不正防止対策及び機密保護対策を講ずることが必要である。

ここでいう出力情報とは、帳票、電子媒体等の形態には係わらず、コンピュータシステムの処理結果として作成された情報を指している。

対策のポイントとしては、以下の例がある。

(1) 出力情報の作成手順は、不正を防止する内容である。
(2) 不正な複写、複製等を防止する対策を講ずる。
(3) 出力情報の機密度に応じて取扱者を限定する。

対策の内容としては、以下の例がある。

(1) 出力情報の作成手順と取扱い
　①端末、パソコン等への情報出力
　　a.操作者のアクセス資格の確認並びに使用機器に適用業務の設定を行う。
　　b.長時間の継続表示は行わない。
　　c.社外に設置した機器への情報出力は、取扱いルールを契約や取引規定等によって明確にする。
　②コンピュータセンター処理における情報出力
　　a.オペレーション指示書等により、出力処理を行う。
　　b.複数のオペレータによるオペレーション作業を行う。
　　c.オペレーション日報等に作業結果を記録する。
　　d.出力情報を確実に依頼者に引き渡す。
　　e.処理途中における機密の漏洩、紛失を防止するために、プリンターなどの使用する機器及び取扱者を限定する。
(2) 不正防止対策
　①端末、パソコン等への表示
　　a.権限のない者による操作、画面の覗き込み、ハードコピー取得を防止する。
　　b.長時間の継続表示は行わない。

会員意見募集版

②出力情報のプリント

a.プリント処理者を限定する。

b.情報出力の量、範囲を限定する。

規定以上の部数、量が出力された場合に発見できるようにする。

(3) 複写、複製の取扱い

①重要なデータの複写、複製は記録を残す。

(4) 出力の記録

①情報出力に関する記録を残す。

②ネットワーク等を介する端末、パソコンへのデータ出力の記録を取得する。

③出力記録を作成する。

項目としては、以下の例がある。

a.処理業務

b.処理日時

c.処理結果（正常、異常）

d.処理担当者

e.処理依頼者

f.出力量

(5) 出力情報のチェック

①誤った処理が行われていないことを確認する。

確認項目としては、以下の例がある。

a.レコード ID

b.パスワードによる資格確認

c.データ件数

d.レコード項目の合計（トータルチェック）

(6) 保管と廃棄

①責任者を定める。

②保管場所、及び管理方法を定める。

③廃棄方法を定める。【実 68】

（参考）

平成 17 年 4 月に「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（e-文書法）が施行され、それまでの法令で書面による保存を義務づけられていた文書が原則として電子データによる保存を容認されることとなった。

具体的に電子データによる保存が認められる対象の文書と保存方法は、保存を要求しているそれぞれの法令の主務省令で指定されるので、文書ごとに確認が必要である。

保存方法を要求する例としては、電子署名【実 8】やタイムスタンプ（注）を必要とする文書や、紙文書を電子化する際のイメージスキャナの解像度を指定している文書があげられる。

なお、電子署名が必要な場合においては、署名の有効期限に留意する必要がある。

（注）タイムスタンプ：電子データが特定時刻より前に存在したことの証明と、その内容が当該時刻以降に変更・改ざんされていないことを証明するための技術。

会員意見募集版

5 システムの利用
(3) 帳票管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　67	未使用重要帳票の管理方法を明確にすること。

不正使用を防止するため、未使用重要帳票の在庫管理、及び廃棄は定められた方法によって行うこと。

1. 不正使用を防止するため、未使用重要帳票の在庫管理、及び廃棄は定められた方法によって行うことが必要である。

   ここでいう重要帳票とは、例えば社長印、頭取印等代表者印、社印等の押印された領収証、支払通知書、証券等金銭を受領できる帳票、及び契約に係わる帳票、通帳・証書（預金通帳等）を指している。

2. 在庫管理、及び廃棄にあたっては、使用枚数、廃棄枚数等を管理することが必要である。

   管理方法の具体的な内容としては、以下の例がある。
   (1) 重要帳票は防火区画内の施錠可能なキャビネット等で保管、格納する。防火区画がない場合は、耐火金庫、耐火キャビネット等で保管、格納する。
   (2) 入出庫は責任者立会いのもとに行い、受渡簿等を使用し授受の記録を明確にする。
   (3) 処理後は次により残存枚数を確認する。
   残存枚数＝印刷前在庫枚数－印刷枚数－印刷失敗枚数－プリンター紙送り廃棄枚数
   (4) 在庫は帳票・用紙在庫管理簿により記録・管理するとともに適宜在庫確認を行う。

3. 印刷ミス、印刷不鮮明、帳票改訂等による廃棄にあたっては、責任者が立ち会う等により裁断、焼却、溶解等が実施されたことを確認することが必要である。

会員意見募集版

5 システムの利用
(3) 帳票管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　68	重要な印字済帳票の取扱方法を明確にすること。

不正使用を防止するため、重要な印字済帳票の受渡し、及び廃棄は定められた方法によって行うこと。

1. 重要な印字済帳票の不正使用を防止するため、授受、廃棄は定められた方法によって特定者が行い、管理責任者等がその状況を確認できることが必要である。
   また、授受の過程で一時保管が必要な場合は、厳重に保管することが必要である。

   ここでいう重要な印字済帳票とは、【実 67】にいう帳票に所定の事項が印字されたもの、顧客データ、取引情報等重要なデータが印字されたコンピュータセンターから配布された帳票、端末から出力された帳票、電子媒体等の形態には係わらず、コンピュータの処理結果として作成された電子帳票を指している。

2. 重要な印字済帳票の授受は、授受伝票、授受管理簿、発送管理表、印刷枚数一覧表等により確認することが必要である。

3. 重要な印字済帳票を保管する場合、定められた場所に保管することが必要である。また、障害時・災害時に使用する帳票は、防火区画内の施錠可能なキャビネット等で保管することが望ましい。防火区画がない場合は、耐火金庫、耐火キャビネット等で保管することが必要である。

4. 使用済みもしくは回収された重要な印字済帳票の廃棄にあたっては、責任者が立ち会う等により、裁断、焼却、溶解等が実施されたことを確認することが必要である。

会員意見募集版

5 システムの利用
(4) 顧客データ保護

適用区分					基準分離
共	セ	本	提	ダ	基礎
◎					

実 69	顧客データの保護策を講ずること。

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。

1. 金融機関等は顧客に関する厳密な守秘義務に基づき、顧客データの取扱いに関しては、管理責任者、管理方法及び取扱い方法を定め適正に管理することが必要である。また、顧客データについては【統 12、統 14、統 20、統 21、実 68】を参照のこと。

   ここでいう顧客データとは、金融機関等が取引等において収集、蓄積し、業務上利用する顧客に関するすべての情報を指している。

2. 不正アクセス等で顧客データが漏洩して顧客が被害を受けることを想定し、損害賠償責任等についての保険の適用を検討することが望ましい。

3. 機微（センシティブ）情報を取り扱う場合は、以下の点を考慮する必要がある。
   (1) 各管理段階において、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」の 1−2 及び（別添 1）に掲げる措置を実施することが必要である。なお、各管理段階とは、「取得・入力」「利用・加工」「保管・保存」「移送・送信」「消去・廃棄」のことをいう。
   (2) 機微（センシティブ）情報の「取得・入力」「利用・加工」「移送・送信」は、「金融分野における個人情報保護に関するガイドライン」第 5 条第 1 項各号に定められる場合に限定することが必要である。
   (3) 各管理段階において取扱者、アクセス権限の設定は必要最小限に限定するとともに、「利用・加工」「保管・保存」「移送・送信」の各段階においてはそれを担保するアクセス制御を実施することが必要である。
   (4) 「取得・入力」及び「利用・加工」の段階にあたっては、本人同意が必要である場合には、機微（センシティブ）情報の利用目的及び利用範囲について本人に明示し、同意を得ることが必要である。
   (5) 機微（センシティブ）情報に該当する生体認証情報を取り扱う場合は上記(2)(3)(4)に加えて、【実 140】を実施することが必要である。

   ここでいう機微（センシティブ）情報とは、「個人情報の保護に関する法律第２条第３項に定める要配慮個人情報並びに労働組合への加盟、門地、本籍地、保健医療及び性生活（これ

会員意見募集版 配布禁止

らのうち要配慮個人情報に該当するものを除く。）に関する情報（本人、国の機関、地方公共団体、個人情報の保護に関する法律第 76 条第１項各号若しくは個人情報の保護に関する法律施行規則第６条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。）」を指している。（個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」第 5 条）

4. 匿名加工情報（匿名加工情報データベース等を構成するものに限る。）を作成するときは、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」の３－２に定める「匿名加工情報の適正な加工（法 36 条第１項関係）」に従い、当該個人情報を加工することが必要である。

参照法令	・個人情報の保護に関する法律 ・個人情報の保護に関する法律についてのガイドライン ・金融分野における個人情報保護に関するガイドライン ・金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針

会員意見募集版

6 緊急時の対応
(1) 障害時・災害時対応策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

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、連絡手順を定めること。

1. 障害時・災害時に連絡を行い、招集する関係者には以下のような対象者をあらかじめ整理しておき、定期的に見直すことが必要である。
   また、各関係者は必ず正副 2 名以上を決め、連絡のつかないことが無いようにするとともに、関係部署及び店内に定められた連絡手順を周知徹底させることが必要である。
   特に重大な障害、災害については、想定される最大リスク等を含め、経営層への報告を適宜行う必要がある。
   (1) コンピュータセンターにおける関係者
      ①コンピュータセンター運営担当者及び管理者
      ②システム担当者及び管理者
      ③コンピュータメーカー及び UPS 等の設備関連業者の担当者
      ④本部・営業店等への連絡責任者
      ⑤外部共同システム（全銀センター、統合 ATM システム、共同 CMS 等）への連絡責任者
      ⑥広報責任者
   (2) 本部・営業店等における関係者
      ①本部・営業店等の責任者
      ②コンピュータセンターへの連絡責任者
      ③メーカー等の保守部門担当者
      ④警備会社
   (3) 重要なシステムを委託している外部委託先

2. 複数の連絡手段を考慮した連絡網を定めることが必要である。

   連絡手段としては、以下の例がある
   (1) 電話（携帯電話、衛星電話を含む）
   (2) ファクシミリ
   (3) 別系統オンラインシステムの一斉通報機能
   (4) 無線
   (5) 電子メール、インターネット等の利用
   (6) 災害用伝言サービス

会員意見募集版

3. CD･ATM 等への障害を考慮して、無人監視による時間帯（夜間、土曜日、日曜日、祝祭日等）の連絡網、連絡方法を別途作成するとともに、定期的な見直しを行うことが必要である。

4. 顧客へ正しい情報提供を行うため、広報窓口をあらかじめ一本化して取り決めておくことが必要である。提供する情報の例として、障害の内容・発生原因、復旧見込等が考えられる。また、広報窓口に対する各種情報の提供責任者もあらかじめ決めておくことが必要である。

5. 顧客受付窓口は、広報窓口と連携して、整合性がとれた情報を顧客に提供する必要がある。また、顧客受付窓口として、必要に応じてコールセンター等を開設することも有効である。

（参考）

災害時優先電話

正しくは「災害時優先通信」といい、災害の復旧等や公共の秩序を維持するため、法令に基づき、防災関係等各種機関等に対し、固定電話及び携帯電話の各電気通信事業者が提供しているサービスである。災害等で電話が混み合うと、発信規制や接続規制といった通信制限により、通常の電話は被災地からの発信や被災地への接続は制限されるが、優先電話はこうした制限を受けずに発信や接続を行うことが可能となっている。ただし、「優先」するものであって必ずつながることを保証しているものではない。

会員意見募集版

6 緊急時の対応
(1) 障害時・災害時対応策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 71	障害時・災害時復旧手順を明確にすること。

障害時・災害時におけるコンピュータシステムの早期復旧のため、復旧手順を明確にするとともに、コンティンジェンシープランとの整合性を図ること。

1. 障害時・災害時におけるコンピュータシステムの早期復旧のため、復旧手順を明確にするとともに、コンティンジェンシープランとの整合性を図ることが必要である。

   ここでいう復旧手順とは、障害または災害等により正常に稼働しなくなったコンピュータシステムを復旧させるための手続きを明確にしたものを指している。

   コンピュータシステムの復旧手順を作成する障害としては、以下の例がある。
   (1) コンピュータ装置の故障
   (2) 端末機器等の故障
   (3) 関連設備（電源、空調、給排水設備等）の故障
   (4) 通信回線の障害
   (5) ソフトウェアの障害

   障害時・災害時の復旧手順において考慮する事項としては、以下の例がある。
   (1) 業務開始時の手順（システム立上げ時等）
   (2) 影響を局所化する縮退等
   (3) バックアップシステム（バックアップサイト設置分を含む）への切替え（強制切替え、システム運用時の諸制約等を踏まえた切替え判断及び運用手順、共同センターにおける切替え判断等を含む）
   (4) バックアップシステム（バックアップサイト設置分を含む）への切替えによる社内のシステムへの影響確認（周辺システム、EUC システム等）
   (5) ファイルの不整合や取引データの欠落の有無の確認手順
   (6) 対応要員の確保と当該要員への必要な権限委任
   (7) 本部・営業店等への業務影響範囲、復旧見込み等の連絡手順
   (8) 社外のシステムへの影響確認（全銀センター、統合 ATM システム、共同 CMS 等の関連会社等）
   (9) 稼働に必要な ID・パスワードの取得方法の明確化　【実 27】
   (10) バックアップシステム（バックアップサイト設置分を含む）からの切戻しが必要な場合の対応方針、手順

会員意見募集版

2. 業務及びシステム運用を外部に委託している場合に、外部委託先が契約どおりに委託業務を遂行できない場合の対応策についても、事前に考慮しておくことが望ましい。

3. 障害時・災害時に使用するバックアップシステム（バックアップサイト設置分を含む）が正常に稼働することを定期的に確認することが必要である。
なお、冗長構成によって信頼性を確保しているシステムにおいては、冗長構成の機器が正常に稼働していることを定期的に確認することが必要である。

障害時・災害時復旧については【実 104～106】を参照のこと。

会員意見募集版

6 緊急時の対応
(1) 障害時・災害時対応策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 72	障害の原因を調査・分析すること。

障害から速やかに復旧するため、障害の原因を調査する手法を講じておくとともに、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。

1. 障害から速やかに復旧するためにも障害の原因を調査する手法を講じておくことが必要である。具体例については【実 102、実 103】を参照のこと。

2. コンピュータメーカーによる障害事前検知、障害発生後の早期原因把握のため、メーカー社内からシステムの診断が可能な遠隔診断システムの導入も原因調査の手段として考えられる。

3. 障害の再発を防止するため、発生した障害に係わる各種データを収集・分析し、障害発生原因を調査のうえ、根本原因を究明し、当該障害についての対策を講ずることが必要である。根本原因を究明する際は、システム的要因だけではなく、人的要因等からも究明する必要がある。なお、人的要因には操作者の過誤、要員の繁忙による集中力の低下、要員不足等が挙げられる。

4. 障害の未然防止の観点から、可能な範囲で社内及び社外（同業他社、他業態）の障害等の情報を収集・分析し、必要に応じて対策を講ずることが望ましい。

5. 障害の再発防止及び未然防止に向けた施策については、障害件数の上限目標値等の障害管理の指標を用いて、その施策の実効性を客観的に評価することが望ましい。また、障害管理の指標は、システムの重要度及び障害の影響範囲に応じて、システム別・発生原因別等に定めることが有効である。

6. 障害の傾向分析などを継続的に行い、類似障害を事前防止できるよう態勢を整え運用することが望ましい。なお、障害の分析結果を定期的に経営層へ報告することも考慮して態勢を整備することが望ましい。

7. EUC システムについても、取り扱う業務の重要度及び障害発生時の影響度に応じて、障害情報の収集・分析・障害対応・報告を行うための管理体制を整備することが必要である。

会員意見募集版

6 運用管理
(2) コンティンジェンシープランの策定

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　73	コンティンジェンシープランを策定すること。

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、早期復旧を図るため、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）を策定すること。

1. 不慮の災害や事故、あるいは障害時に、あらかじめ想定される複数のケースに応じてコンティンジェンシープランを策定しておくことが必要である。
   なお、集中豪雨、降雪等による交通遮断、あるいは感染症のパンデミック発生などから生じる職員不在等の不測の事態についても、要員確保の観点から考慮することが必要である。
   また、障害等が発生した時期、曜日、時間帯やシステム環境の違いにより対応する範囲や方法が異なる場合には、これらの対応を考慮する必要がある。
   特に、広範囲に重大な影響を及ぼすような資金決済システム等の障害については、時限性や社内関連システム及び社外への影響等にも留意する必要がある。

   ここでいうコンティンジェンシープランとは、金融機関等のコンピュータシステムが、不慮の災害や事故･犯罪､障害等により重大な損害を被り業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務の復旧を行うためにあらかじめ策定された緊急時対応計画のことを指している。

   想定される緊急事態としては、以下の例がある。
   (1) コンピュータセンター、本部・営業店等の全面被災、一部被災
   (2) コンピュータ装置の破壊、損傷
   (3) 端末機器等の破損、損傷
   (4) 関連設備（電源、空調、給排水設備等）の破壊、損傷
   (5) 回線の切断、通信設備の損傷
   (6) 公共インフラの障害（停電、断水、交通遮断等）
   (7) ソフトウェアの障害
   (8) サイバー攻撃

   コンティンジェンシープランの策定に際して考慮する内容としては、以下の例がある。
   (1) 緊急事態を想定し、自社の業務や各種施設に対してどのような影響が起こるかを評価する。
   (2) 緊急時における業務の継続の優先順位を評価する。

会員意見募集版

(3) 被災拠点及び対策本部における緊急時対応組織の体制（コンティンジェンシープラン発動権限も含む）や要員等を明確にし、手順書として文書化する。
(4) 緊急事態発生時における、顧客・職員の安全確保、資産の保全、被災状況の把握等の措置を明確にし、手順書として文書化する。
(5) 業務、顧客サービスの中断あるいは、中断による損失を極小化するために、業務の通常的な継続が困難な緊急事態のもとで、重要と判断される業務の暫定的継続を図るために必要な措置を明確にし、手順書として文書化する。
(6) 早期に事態を収拾して、平常業務への復旧を図るために必要な措置を明確にし、手順書として文書化する。
(7) 緊急時における要員の移動、機器等の物資の搬送手段及びルートを決めておく。
(8) プランの維持管理体制の確立を行い、定期的な訓練の実施とその結果に基づくプランの見直し等の維持管理を明確にする。
(9) 業務が外部委託されている場合は、外部委託先のみならず再委託先の役割等も定め、文書化する。（クラウドサービス及び共同センターも含む）

設備及び技術面の復旧策、並びに災害時・障害時等に備えた運用訓練については、以下の基準項目を参照のこと。また、コンティンジェンシープランを変更する際も、必要に応じて以下の基準項目を参照のこと。

(1) 環境 【設 1】
(2) 周囲 【設 2～設 4、設 7～設 9】
(3) 構造 【設 10～設 13、設 31～設 36】
(4) 開口部 【設 14、設 17～設 19、設 28～設 30】
(5) 内装等 【設 20、設 21】
(6) 位置 【設 22、設 25、設 26】
(7) 設備 【設 37～設 44】
(8) コンピュータ機器、什器、備品 【設 48、設 50、設 51】
(9) 電源室、空調機械室 【設 52、設 54～設 60】
(10) 電源設備 【設 62～設 71】
(11) 空調設備 【設 74～設 79】
(12) 監視制御設備 【設 80、設 81】
(13) 回線関連設備 【設 82、設 83、設 83-1】
(14) ハードウェアの予備 【実 84～88】
(15) 障害の早期回復 【実 104～106】
(16) バックアップサイト 【実 74】
(17) 教育、訓練 【統 14～17】

なお、コンティンジェンシープランの策定に関する詳細内容については、当センター発刊の『金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書』を参照のこと。

2. コンティンジェンシープランが策定された後においても、適宜見直しをすることが必要であ

会員意見募集版

る。見直しを行う際は、事務手続き等の変更点にも考慮することが必要である。

見直しが必要となる契機としては、以下の例がある。

(1) 重要な業務についてその内容に変更が生じた場合
(2) 従来、コンティンジェンシープランでは考慮していなかった業務についてその重要度が高まった場合
(3) 上記業務遂行の前提となる組織や拠点施設、インフラ、システム構成等の条件に変更が生じた場合
(4) 政府の取組みやガイドライン等が変更された場合

3. 組織図や緊急連絡網等については、最新の情報を維持するとともに、組織内に周知することが必要である。

4. コンティンジェンシープランの策定及び重要なプラン内容の見直しを行うにあたっては、経営層の承認を得ることが必要である。

5. コンティンジェンシープランは、対策本部、各拠点、バックアップサイトにおいて、必要な部分が常時保管され、全役職員が必要な部分を閲覧できる状態を保つことが必要である。

6. 障害時・災害時等におけるシステムの復旧やバックアップサイトへの切替えを行う際は、セキュリティ管理のレベルが低下するおそれがある。当該事象が発生した場合のセキュリティについても通常時と同等のレベルを維持することが必要である。

7. 障害・災害によって生じる可能性のある損害賠償責任、逸失利益、業務継続に要する費用等に備えて、保険の適用を検討することが望ましい。

会員意見募集版

6 緊急時の対応
(3) バックアップサイト

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎				

実　74	バックアップサイトを保有すること。

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るため、業務の優先度を考慮したバックアップサイトを保有すること。

1. 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、リスク分散の意味で、別の地域に業務の優先度を考慮したバックアップサイトを保有することが望ましい。
特に、資金決済等を行う重要なシステムについては、原則としてバックアップサイトを保有することが必要である。
ただし、バックアップサイトを保有しない場合は、障害による社会への影響を十分に検討のうえ、他に代替する方法による業務継続態勢を整備し、経営層が承認する必要がある。

   バックアップサイトの運営形態としては、以下のものがある。
   (1) 自営センター
   自社専用の代替施設として利用する。
   (2) 共同利用センター
   複数企業が共同で代替センターを設立し、必要時に利用する。
   (3) 相互利用センター
   別地域にある同一企業（グループ）内の事業部門と相互に被災時等にバックアップし合う。代替施設提供部門は、被災時等には緊急度の低い業務は一時運用を止めて対応する。
   他企業（協力企業）間でバックアップし合う場合もある。
   (4) 代行処理センター
   第三者にバックアップを委託し、必要時に利用する。

2. バックアップサイトを外部に委託している場合、複数の委託元で同時に緊急事態が発生するケースを想定して、バックアップを受ける優先順位、最低保証の範囲などのサービスを確認し、事務量の変化に対応して定期的に見直すことが必要である。

3. バックアップサイトの保有にあたっては、以下の事項を考慮し、総合的に判断することが望ましい。
   (1) コンピュータセンターと同一のリスク要因（火災、地震、停電等）を共有しないこと。
   (2) 被災時の要員、データ、物資等の移動・移送時間を含む復旧時間を確認すること。

（参考）
バックアップサイトの立地条件については、コンピュータセンターの立地条件と同様に考える必要があるため【設 1】を参照のこと。

会員意見募集版

7 システム開発・変更
(1) システム開発・変更管理

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 75	システムの開発・変更手順を明確にすること。

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。

1. システムの信頼性を向上させるとともに、内容の正当性を確保するため、システム開発・変更の各段階における確認、検証等は定められた手順によって行うことが必要である。

   ここでいう開発・変更手順とは、以下のようなものを指している。
   (1) 新規システムの開発または既存システムの変更における要件検討、企画の承認手順
   (2) 設計、プログラム作成、テスト等各段階における検証・承認手順
   (3) 開発・変更作業完了時における検証・承認手順
   (4) 障害時、災害時対応手順等への反映の検証・承認手順 【実 24、実 73】

2. システム開発工程を適切に管理するため、プロジェクトごとに責任者を明確にし、効率的な開発手法を確立して、プロジェクト管理を実施することが必要である。
   また、適切なプロジェクト管理の実施には、プロジェクトの支援環境を整備することも有効である。

   ここでいうプロジェクト管理とは、システム開発・変更作業を与えられた時間と資源（人、物、金等）の範囲内で合理的に進め、確実かつ効率的に目的を達成するために、定められた方法にしたがってプロジェクトの状況を十分に把握し、適切な対応をとることを指している。

3. システムの信頼性向上を図るうえで、ソフトウェアの信頼性向上対策を講ずることが必要である。ソフトウェアの品質確保については【統 3、実 89～96】を参照のこと。

会員意見募集版

（参考 1）

開発の各段階における管理ポイントとして、以下のような例がある。

1. システム要件検討、企画
   (1) 社内の組織横断的な審議機関を設置し、案件の開発可否を審議しているか。
   (2) 情報システムの投資効果とそのリスクが開発案件の検証・承認ルールの中で評価され、必要に応じ、経営層に報告されているか。 なお、この投資効果の計測にあたって考慮する要素としては、以下の例がある。
      ・システム開発コスト
      ・開発により得ることができる収益の向上、事務量の削減効果などの「定量効果」
      ・その他、定量的に計測することのできない「定性効果」
   (3) ユーザー要件の確認は十分か。また、依頼文書は受付簿等で管理されているか。
2. システム設計
   (1) 各段階で作成した設計書等のドキュメント類は標準化ルールにそった内容となっているか。
   (2) 設計内容等のチェック・レビューは行われているか。
3. プログラム作成
   (1) プログラム作成作業等を外部に委託するにあたっては、詳細作業指示、ドキュメント授受・内容の検証等、受渡票等により、ドキュメント類の受渡しの事実が明らかになっているか。
   (2) プログラム仕様の検証、承認は定められた手続きに従い、適切に行われているか。また、仕様変更は必ず権限者の承認を受けて行われているか。
4. テスト
   (1) テスト方法や確認の手順が確立しており、かつ遵守されているか。
   (2) バグ管理表等により、未解決バグ、問題点・懸案事項等の把握、管理、対策が行われているか。
   (3) 必要に応じ、ユーザー部門によるテストデータの作成や出力結果の確認等が行われているか。
   (4) ピーク処理時の性能評価、及び許容最大件数を考慮した負荷評価が行われているか。
5. システム運用
   (1) 運用部門（運用担当者）への引継ぎ資料、説明、初期運用時のフォローは十分か。
   (2) システムの維持管理体制、維持管理用ドキュメント等は適切に整備されているか。
   (3) システムのリスクの評価を継続的に行い、その維持・改善のための投資が計画的に行われているか。
6. 開発の段階全般
   (1) システム開発・変更スケジュールが明確にされ、進捗管理が行われているか。また、遅延した場合の問題解決が行われているか。
   (2) 特に重要なシステムの開発プロジェクトにおいては、業務部門や顧客対応部門等の状況を把握するための社内の組織横断的な検証体制が整備されているか。また、その整備や状況チェックには経営層が関与しているか。

会員意見募集版

（参考 2）

システム開発を効率化するためにはプロジェクトマネジメントが重要であり、その基礎プロセスを明確にして、プロジェクトの計画・遂行管理を成功に導くための知識体系を整備することが有効である。この知識体系の一例として、プロジェクトマネジメントの知識体系 PMBOK（Project Management Body of Knowledge）がある。

（参考 3）

プロジェクトの支援環境整備の一例として、プロジェクトを横断的に支援する組織 PMO（Project Management Office）の設置がある。

会員意見募集版

7 システム開発・変更
(1) システム開発・変更管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　76	テスト環境を整備すること。

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。

1. システムの開発・変更作業に係わるテストにおいては、本番環境へ影響を与えずに十分なテストが実施できることが必要である。また、本番環境とテスト環境の差異についても把握することが必要である。
   なお、本番機と開発機は分離することが望ましい。

   テスト環境整備の対策事項としては、以下の例がある。
   (1) 本番環境へ影響を与えないテスト環境の設定
   ①テスト用ファイルと本番用ファイルを分離する。
   テストを行う際は、本番用ファイルを参照、更新及び破壊しないように、本番用ファイルと分離したテスト用ファイルを用意する。
   ②テスト用端末からの本番ファイルへのアクセス防止策を講ずる。
   不正アクセス防止については【実 25～27】を参照のこと。
   また、テスト用端末ではログオン手順、ID 体系、メニュー画面を変更するなどの対策を行い、本番端末との混同を避ける。
   ③本番機器を使用したテストを行う場合は、本番システム稼働中のテスト等を回避する。
   本番システム稼働中のテスト等の実施は極力回避し、やむを得ず実施する場合は、テストによる影響度を明らかにし、それに対するテスト制限を設ける。
   ④本番機器を使用したテストを行う場合は、テスト後の戻し、切替え手順を明確にする。
   本番機器を使用したテストを行う場合、機器を本番システムの環境に戻す手順を明らかにし、本番システムに影響が出ないことを確認する。
   ⑤営業店側における事務処理上の留意点について連絡、徹底する。
   営業店を含むテストを実施する場合には、現行システムとの関連で混乱が発生しないよう、以下のような点の取扱いについて連絡し、周知徹底する。
   a.端末ハードウェア・ソフトウェアの入替え
   b.使用帳票等の分離、管理
   c.事務手続き・マニュアル類の分離、管理
   ⑥開発用 ID と本番用 ID を明確に区別する。
   本番移行後に開発用 ID がセキュリティホールとならないように開発用 ID と本番用 ID を明確に区別し、本番移行時には不要な開発用 ID を抹消する。

会員意見募集版

(2) 本番稼働へ向けて十分なテストが実施できる環境の設定

①開発・テスト用資源等を確保する。

開発・テスト用のコンピュータ等の資源は十分に確保する。その際、使用する媒体やテスト用ファイル等がコンピュータウイルスに感染していないかをチェックする。

②外部システム（全銀センター、共同 CMS センター等）との接続テストの予約を行う。

外部システムとの接続テストを実施する場合には、事前にテスト日程、テスト範囲・分担、テスト内容等を十分に検討し、調整する。

③本番を想定したテストを実施する。

テストの種類については【実 92】を参照のこと。

(3) オープンネットワークを使用したテストを行う際の留意点

オープンネットワークと接続する必要のあるテストを行う場合は、不正侵入防止機能を設ける。【実 14】

2. 本番データをもとにテストデータを作成する場合、個人を識別できる情報を削除またはスクランブル化することが必要である。

やむをえず本番データを使用する場合には、以下のような漏洩防止策を講ずることが必要である。

(1) データ管理者への本番データコピー借用依頼、承認

(2) アクセスできる要員の必要最小限化

(3) 使用後（借用期日到来時）のデータ管理部門への返却、及び開発・テスト環境からの削除

(4) テスト結果の出力リスト等の保管、廃棄　等

会員意見募集版

7 システム開発・変更
(1) システム開発・変更管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　77	本番への移行手順を明確にすること。

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。

1. 本番への移行は、移行時における障害を防止することが重要であり、本番システムへの切替えを安全・確実に行うためのシステムの特性に応じた移行手順を明確にすることが必要である。
   また、円滑に本番運用に移行するため、運用部門（運用担当者）への引継ぎ、説明及びユーザーへの説明を十分に行い、準備状況を確認することが必要である。

   本番への移行手順で考慮するものとしては、以下の例がある。

   (1) 移行方法の明確化
   移行作業手順及びカットオーバー可否の判断基準等を明確にする。判断基準については、数値化等による客観的な指標を用いることも有効である。
   また、以下のような事項も考慮する。
   ①移行に支障が生じた場合の対処として、旧システムを継続稼働させるために必要な対応等（制度対応等のシステム変更、保守、契約期限の延長等）を実施する。
   ②待機系システムがある場合、現用系システムと同様に移行作業手順等を明確にする、また現用系システムと待機系システムの設定値の整合性確認をする。
   ③外部接続がある場合、カットオーバー判断のため外部接続先の要件等の十分な調査・調整を実施する。

   (2) 運用部門及びユーザーへの説明や準備状況の確認
   円滑に本番運用に移行するため、運用部門に対し、システムの運用に必要なドキュメント類を引き継ぐとともに十分に説明を行う。また、ユーザーに対しては移行のタイミングや変更点及び制約事項等を十分に説明するとともに、事務処理や顧客周知等の準備状況を確認する。

   (3) 移行リハーサルの実施
   システムの移行にあたっては、必要に応じて事前に移行のリハーサルを行い、安全・確実に移行できることを確認するとともに、移行処理時間の測定や正当性確認のためのチェックポイントなどを明確にする。
   なお、具体的には以下のようなものが考えられる。
   ①ファイル移行確認テスト
   ②移行手順確認テスト

会員意見募集版

③回線接続確認テスト

④オペレーション確認テスト

⑤残高照合等確認テスト

(4) 移行判定

カットオーバー可否の判断基準に照らして準備状況を確認し、移行判定を行う。また、特に重要なシステムにおいては、社内横断的に関連する部門（業務部門、顧客対応部門等）の準備状況等を確認し、リスク管理部門等の評価も踏まえたうえで経営層が判定する。

(5) 移行作業の実施

移行のための組織・体制を整備し、移行手順書に従いデータファイル（環境設定ファイル等を含む）及びプログラム等の移行作業を実施する。移行作業については、(3)移行リハーサルの実施等において、正確性（移行順序やタイミング等）を確認する。また、必要に応じて新旧の比較により変更箇所を確認することも有効である。

なお、異常時に備えて、作業中止・復旧作業に移るための判断ポイントを設定し、速やかに復旧作業ができるように関連する各部門の手順の整合性を確認のうえ、準備する。

(6) 最終確認

移行実施後は、ユーザーと協力のうえ、残高照合等のデータの整合性を確認するテストを行い、既存システムを含めた本番稼働に支障がないことを確認する。

また、開発用に使用したコマンド、JCL、ツール、開発用 ID 等については、本番移行に伴い不要なものを削除することが重要であり、本番環境に持ち込む場合には、オペレータの誤操作等で起動されることがないよう措置を講じる。

2. コンピュータセンターの移転に際しては、1 の対策に加え、データの運搬に関して発生するリスクを考慮して、十分な対策を講じる必要がある。

対策としては、以下の例がある。

(1) 運搬中の事故、紛失、破損、盗難等への対策

①電磁波、塵埃などに留意した安全な経路の確保、天候・道路周辺事情の把握、警備

②データの保存時の暗号化

③運搬経路の多重化

(2) バックアップデータの保存もれ、保存時のエラー、紛失への対策

①バックアップの多重化

会員意見募集版

7 システム開発・変更
(2) 開発・変更時ドキュメント管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

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。

1. 一貫した適切なドキュメントを作成するため、作成対象とするドキュメントの範囲、体系、様式、記述内容等について明文化した手順を定め、遵守することが必要である。
   また、ドキュメントは、その品質を確認し、共有できるシステム資産とするために、作成部門及び利用部門の責任者の承認を得ることが必要である。
   なお、定められた手順は開発方法の変更、運用形態などに応じて適時見直す必要がある。

2. ドキュメントの作成手順については、ドキュメントの作成者、利用者及び管理者等の関係者に周知徹底させることが必要である。

3. ドキュメントの作成手順の遵守状況を、ドキュメントの作成、利用及び管理の各責任者が確認していることが必要である。

   ドキュメントの作成手順における制定項目としては、以下の例がある。

   (1) 作成範囲
   　作成するドキュメントの種類
   (2) 作成方法
   　ドキュメント作成の手段及び方法
   (3) 分類方法
   　開発用、保守用、運用用など、ドキュメントの分類
   (4) 記述要領
   　標準様式、記述項目、記入要領、事例集
   (5) 変更手順
   　システムの変更に伴うドキュメントの変更方法、更新履歴の管理方法
   (6) 作成部門
   　ドキュメントの作成担当部門
   (7) 保守部門
   　ドキュメントの保守担当部門
   (8) 利用部門
   　ドキュメントの利用部門

会員意見募集版

(9) 承認手続き

ドキュメントのレビューから承認に至るまでの手続き

会員意見募集版

7 システム開発・変更
(2) 開発・変更時ドキュメント管理

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　71	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。

円滑な利用及び改ざん、不正使用等の防止のため、ドキュメントの保管管理を適正に行うこと。

1. ドキュメントの保管管理は、その利用を円滑にし、かつ不正使用防止及び機密保護のために、定められた手順に従って適正に行うことが必要である。なお、ドキュメントの形態には、印刷物のみならず電子媒体上の文書ファイル等も含んでいる。

2. コンピュータシステムの内容と整合したドキュメントを維持するためには、一元管理することが望ましい。

   ドキュメントの管理方法としては、以下の例がある。
   (1) ドキュメントの管理は管理簿にて行い、管理記録を整備する。
   (2) ドキュメントごとの保管期間を明確にする。
   (3) 管理責任者を明確にする。
   (4) 重要なドキュメントは定められた保管場所（施錠可能な保管室やキャビネット等）に保管する。
   (5) 重要なドキュメントは閲覧者を特定するとともに、コピーの制限を設けるなどの措置を講ずる。

会員意見募集版

7 システム開発・変更
(3) パッケージの導入

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　80	パッケージの評価体制を整備すること。

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。

1. パッケージ導入に際しては、システム開発部門、運用部門及び利用部門（本部・営業店等）による総合的評価が必要である。

   パッケージ導入に際しての評価項目としては、以下の例がある。

   (1) パッケージ自体の評価項目

   ①業務機能の充足性
   ②性能（レスポンス、処理時間等）
   ③運用の容易性
   ④ドキュメントの整備状況
   ⑤拡張性
   ⑥柔軟性
   ⑦セキュリティ機能
   ⑧パッケージ供給元の保守・支援体制（脆弱性への対応体制を含む）
   ⑨使用実績、導入実績
   ⑩カスタマイズの可否と範囲

   (2) 既存システム等との整合性に関する評価項目

   ①OS や DBMS、ミドルウェア等との親和性
   a.既存プラットフォームで実現できる性能
   b.バージョン相違などによる不整合
   ②入出力仕様
   a.データ入力方法や出力形式等（帳票、伝票、ファイル仕様）
   ③コード体系
   a.漢字コード、フォント、外字の取扱い

2. 必要なカスタマイズ及び将来の案件対応のために、パッケージのソースコード開示の可否を確認することが必要である。

会員意見募集版

7 システム開発・変更
(3) パッケージの導入

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　81	パッケージの運用・管理体制を明確にすること。

パッケージの導入後のトラブル対応、機能拡張等を円滑に行うため、パッケージの運用・管理体制を明確にすること。

1. パッケージの運用・管理体制を明確にすることが必要である。

パッケージの運用管理項目としては、以下の例がある。

(1) トラブル発生時の影響を最小にするため、パッケージ供給元の連絡窓口と保守体制及び確認事項（トラブル現象の把握方法、応急措置方法等）の明確化

(2) 不正使用やトラブルの発生を抑制するための、ライセンス管理、バージョン管理体制の明確化

(3) システムの運用を円滑に行うためのメンテナンス体制とパッケージ供給元の支援体制（脆弱性への対応体制を含む）の明確化

(4) パッケージに関する教育、問合わせ等の体制の明確化

(5) パッケージの主要な設定内容等（各種設定値、有効期限等）管理の明確化

会員意見募集版

7 システム開発・変更
(4) システムの廃棄

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

システムの廃棄を円滑、確実かつ安全に実施するため、運用及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。

1. システムの廃棄計画を策定するとともに、廃棄手順を明確にし、運用及び利用部門の責任者の承認を得て廃棄することが必要である。

2. システムを廃棄するにあたっては、あらかじめ、ユーザー、システム資産の管理部署及び廃棄作業にあたる部署などの関係先に確実に連絡することが必要である。
   また、廃棄作業に着手する前に、当該システムの運用が完全に終結していることを確認する必要がある。

   廃棄計画の内容としては、以下の例がある。
   (1) 廃棄の目的
   (2) 廃棄の対象範囲
   (3) 廃棄する時期
   (4) 廃棄する方法
   (5) 計上資産の処分方法

会員意見募集版

7 システム開発・変更
(4) システムの廃棄

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　83	システム廃棄時の情報漏洩防止対策を講ずること。

機密保護、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。

1. コンピュータシステムを廃棄するにあたっては、当該コンピュータシステムの重要度を考慮し、機密保護、プライバシー保護及び不正防止のための対策を講ずることが必要である。

2. 廃棄が確実に行われるように、廃棄方法（データ消去を含む）及び廃棄時期を明確にし、廃棄作業完了後には廃棄記録について責任者の承認を得ることが必要である。

   データ消去の方法としては、以下の例がある。
   (1) 物理的消去（消磁や破壊）
   (2) 論理的消去
      ① データ管理領域とデータ保存領域におけるリンク情報の不可逆的な切断
      ② 全データの保存領域の上書き（意図的で無意味なデータもしくは他のユーザーのデータによる上書き）
      ③ 保管データが暗号化されている場合における暗号鍵の廃棄

3. ハードウェアを廃棄する場合には、内部の重要なデータを読み出し不可能とすることが必要である。

   ハードウェアの廃棄方法としては、以下の例がある。
   なお、リース契約期限切れに伴うリース会社への機器の返却等においても必要に応じて以下の例を参照すること。
   (1) パソコン等のハードディスクのデータを消去するツールを使用したデータの完全消去
   (2) IC カード等の破壊
   (3) 記録媒体の消磁もしくは破壊
   (4) ATM 等に内蔵している暗号化・復号装置等の破壊

   ソフトウェアの廃棄方法としては、以下の例がある。
   (1) システムからのアンインストール
   (2) 記録媒体の消磁もしくは破壊
   (3) ドキュメントの廃棄

会員意見募集版

なお、ライセンス契約上、廃棄時の定めがある場合はそれに従う。

ドキュメントの廃棄方法としては、以下の例がある。

(1) 焼却、裁断

(2) 記録媒体の消磁もしくは破壊

4. 第三者に廃棄を委託する場合においては、上記に準じて行うことが必要である。また、秘密保持契約を締結することが望ましい。

会員意見募集版

8 システムの信頼性向上対策
(1) ハードウェアの予備

適用区分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実 84	本体装置の予備を設けること。

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。

1. コンピュータシステムの中核となる重要な本体装置は、予備を設ける必要がある。
また、物理的な予備装置を設けることのほか、並列処理装置及び同一筐体内の複数の中央処理装置による継続運転の仕組みにより同等の効果を持たせることも可能である。

ここでいう本体装置とは、中央処理装置、主記憶装置、チャネル装置の総称であり、クライアントサーバー・システムの場合は、システムの中核となるサーバーを指している。

2. システムの目的及び重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。
特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。
なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認する必要がある。

本体装置の予備の持ち方としては、以下の例がある。

(1) デュプレックスシステム

待機系の本体装置を備えておき、現用系に障害が発生した場合、待機系に切り替えて業務を続行できるシステムである。待機系の本体装置は、待機中ほかの業務で使用しても構わないが、現用系と同程度の能力を持っていることが有効である（図 1）。
なお、待機の形態によって以下の方式がある。

①ホットスタンバイ方式

事前にプログラムロード等の事前処理を一部行っておき、現用系に障害が発生したときに、直ちに業務を続行できるように待機する方式である。

②コールドスタンバイ方式

事前の処理は特に行っていないが、現用系に障害が発生したときに、切り替えて業務を続行できるように待機する方式である。

会員意見募集版

＜会員意見募集版＞

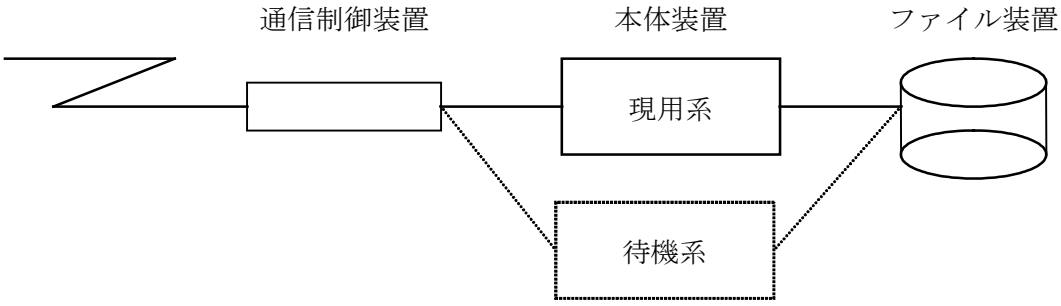


図 1　デュプレックスシステムの例

(2) デュアルシステム

2 つの系の本体装置を常時並列で運転して、互いに監視し合い、一方の系に障害が発生した場合は残りの系だけで運転を継続するシステムである。

(3) フォールトトレラントシステム

誤りもしくは障害となり得る状態にかかわらず、外部から見る限り、一定の性能を維持する能力を備えたシステムである。一般にはシステムの中の本体系装置、磁気ディスク装置等の主要なハードウェアを多重化することによってシステムが停止しない設計となっているフォールトトレラントシステム・コンピュータをメインフレームやサーバーに用いて構成したシステムである。

(4) マルチプロセッサシステム

性能と信頼性の向上を目的として、複数の中央処理装置（プロセッサ）を結合したシステム。

信頼性を向上させるため、ある中央処理装置に障害が発生しても、その中央処理装置を切り離して継続運転を行うことが可能な仕組みを持つ。

なお、切り離して運用する場合でも、ある程度の能力が確保できるように、中央処理装置の能力には余裕があることが有効である（図 2）。

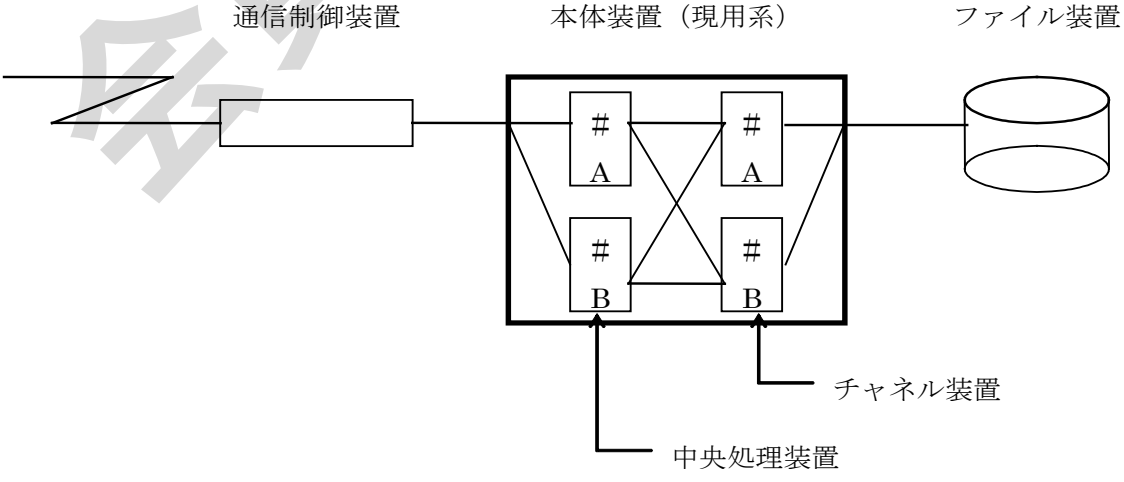
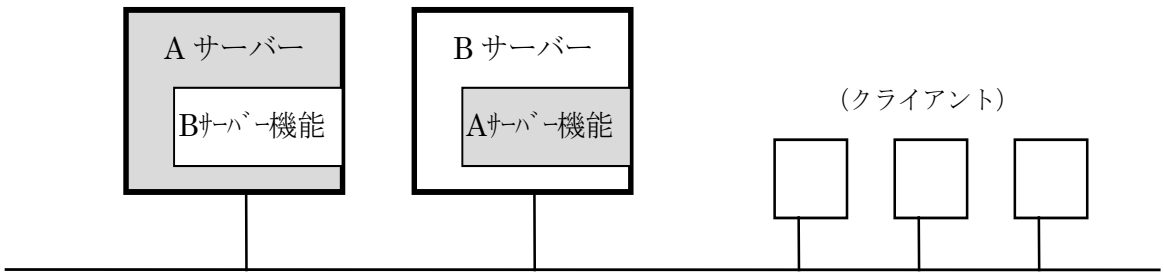


図 2　マルチプロセッサシステムの例

会員意見募集版

(5) フェールオーバー機能

クライアントサーバー・システムにおいて、１つのサーバーが停止したときに別のサーバーが処理を代行する機能（図 3）。



（いずれかのサーバーの障害時に一方が機能を代替する）

図 3　フェールオーバー機能の例

(6) 待機系セグメント構成（レプリカ構成）

クライアントサーバー・システム等において、重要なサーバーを含む LAN 構成そのものを二重化し、一方を待機系として持つ構成（図 4）。

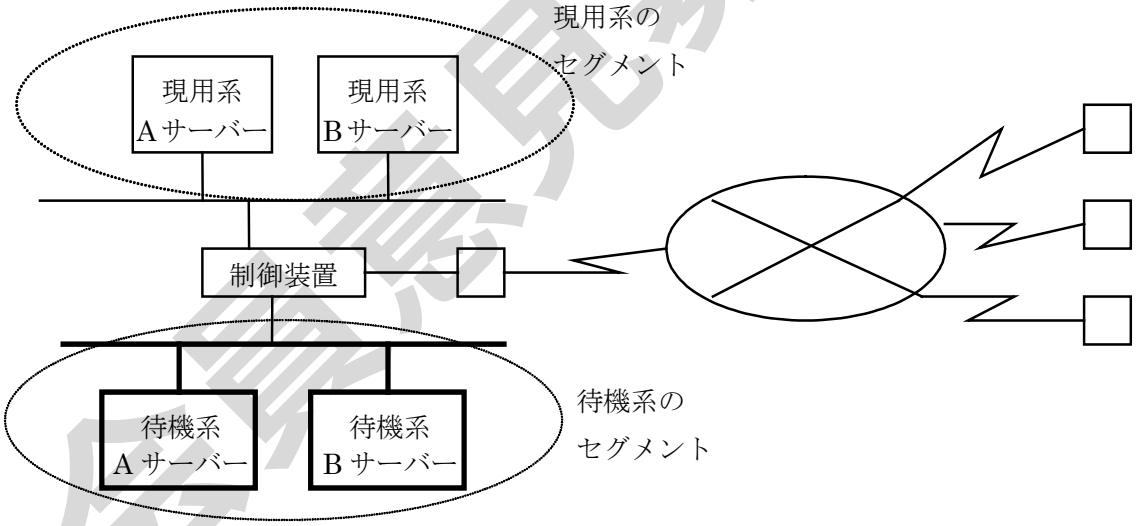


図 4　待機系セグメント構成の例

会員意見募集版

8 システムの信頼性向上対策
(1) ハードウェアの予備

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実　85	周辺装置の予備を設けること。

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。

1. 重要な周辺装置は予備または代替機能を設けることが必要である。

ここでいう周辺装置とは、ファイル装置（磁気ディスク装置、半導体ディスク装置、光磁気ディスク装置、磁気テープ装置等）、コンソールディスプレイ等を指している。
（サーバーの場合は、筐体内部のディスク装置も周辺装置に該当するものとする。）

重要な周辺装置の予備または代替機能を設ける方法としては、以下の例がある。

(1) 複数台の周辺装置ごとに予備を設ける。
なお、ファイル装置においては、通常はバッチ業務等で使用していて、障害発生時にオンライン用に切り替え、ファイルのリカバリ等を行い業務を続行させる方法もある。また、装置としての予備ばかりでなく、空き容量を持つことにより予備とする方法もある。

(2) 複数台設置により予備機装置と同様の効果を持たせる。

(3) 異種装置により代替させる。
ジャーナル情報を半導体ディスク装置に記録している場合、障害時に磁気ディスク装置に代行記録するような事例がある。

(4) ネットワーク上の他のサーバーのファイル装置に代替させる。
ネットワーク上の他のサーバーのファイル装置を自身のファイル装置の予備とする方法もある。

(5) 冗長構成を持ったディスクアレイを、ファイル構成装置として利用する。
（注）ディスクアレイとは、データを分解し、複数のディスクドライブに対して並列にリード＋ライトすることで、大容量、高性能、データの保護、無停止運転を可能にした磁気ディスク装置。RAID（Redundant Arrays of Inexpensive Disks）とも呼ばれる。
冗長性を持つディスクアレイの種類としては、以下の例がある。
①RAID1（ミラーリング方式）
②RAID5（パリティ付ストライピング方式）
③RAID6（ダブルパリティ付ストライピング方式）

2. 重要なファイル装置については、代替パスを設け、アクセスパスの障害時に一群のファイル

会員意見募集版

装置が使用不能となる事態の発生を回避する手段を講じることが考えられる。

アクセスパスの構成方法としては、以下の例がある（図 1）。

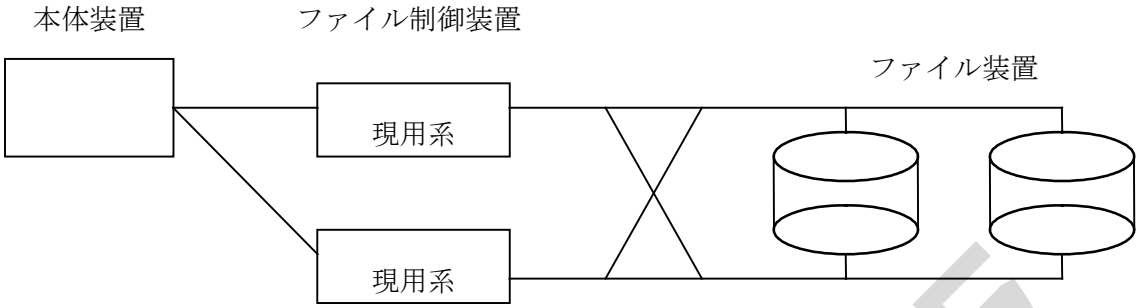


図 1　アクセスパス構成例

3. さらに高い信頼性が必要となるファイルは二重化を考慮することが望ましい。

二重化の対象となる重要なファイルとしては、以下の例がある。

(1) 主要業務ファイル
(2) ジャーナルファイル
(3) その他システム系制御ファイル

4. システムの目的及び重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。
特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。
なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認する必要がある。

会員意見募集版

8 システムの信頼性向上対策
(1) ハードウェアの予備

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実　86	通信系装置の予備を設けること。

通信系装置の障害時の迅速な対応のため、重要な通信系装置は予備を設けること。

1. 重要な通信系装置は予備を設けることが必要である。

予備が必要な通信系装置としては、以下の例がある。

(1) 通信制御装置

①通信制御部の予備構成例（図 1）

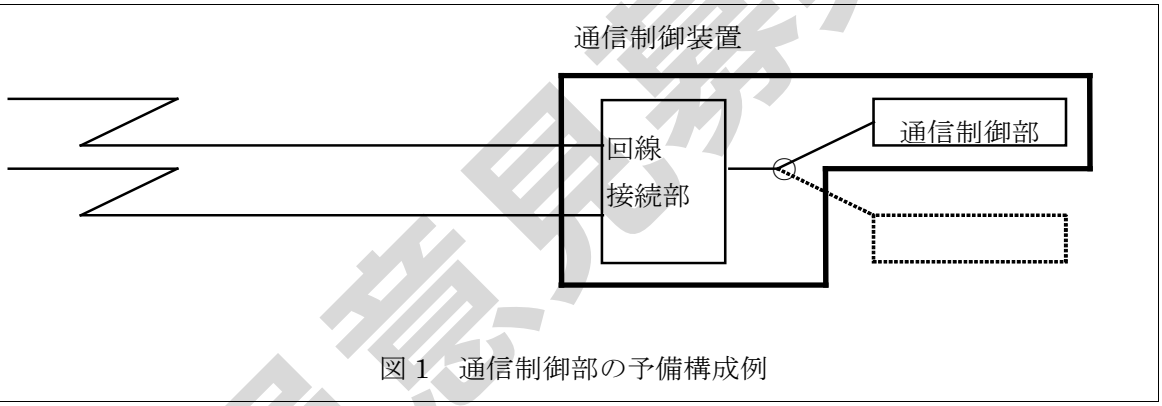


図 1　通信制御部の予備構成例

②通信制御部・回線接続部の予備構成例（図 2）

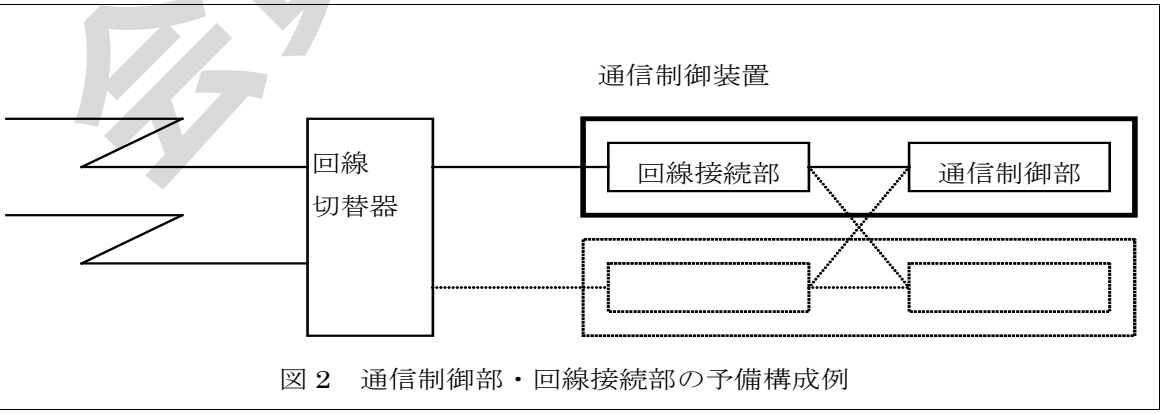


図 2　通信制御部・回線接続部の予備構成例

なお、複数台の通信制御装置ごとに予備を設置することも考えられる。また、回線切替器の設置等、それぞれの実情に応じた切替方法を検討する。

会員意見募集版

(2) 回線終端装置等

回線終端装置等についても、重要なものについては予備を設ける等、あらかじめ障害時に速やかな対応がとれるようにしておく。なお、ここでいう回線終端装置等には時分割多重装置（TDM）、デジタル回線終端装置（DSU）等も含むものとする。

(3) ルータ等

ルータ及び HUB についても障害時の速やかな対応のために、重要なものについては予備を設ける。

なお、フィルタリング情報等のネットワーク設定情報を持つものについては、装置の予備だけでなく、設定情報のバックアップやリカバリの手順を含めて信頼性の向上対策を講ずる。【実 42、実 43】

(4) 交換装置等

交換装置等についても障害時の速やかな対応のために、重要なものについては予備を設ける。なお、ここでいう交換装置等には、非同期転送モード（ATM）装置等も含むものとする。

（ATM：Asynchronous Transfer Mode）

2. 回線終端装置、ルータ等の予備の持ち方として、自社で保有することのほかにベンダーとの保守契約において必要時に代替機の提供を依頼できるようにすることも有効である。

3. システムの目的及び重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。

特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。

なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認する必要がある。

会員意見募集版

＜会員意見募集版＞

8 システムの信頼性向上対策
(1) ハードウェアの予備

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実　87	回線の予備を設けること。

回線障害時の迅速な対応のため、重要な回線は予備を設けること。

1. 重要な回線は予備を設けることが望ましい。

2. 地点間（構外）の重要な回線は複数化するか、またはバックアップ回線を確保することが望ましい。なお、回線を複数化する際は、物理的別ルート化（別の収容交換設備等（旧電話局）を経由するもの）を図ることが望ましい。また、回線のルート、回線容量等は、通信事業者に該当の回線の利用目的等を明示し、適切な設計・構築を図ることが望ましい。

   予備の内容としては、以下の例がある。

   ①専用回線の複数化の例

   a. 端末系装置を 2 つのグループに分け、それぞれ別々の回線に接続する方法

   b. 回線の一方を予備とし、必要に応じて切り替える方法

   ②電話回線（xDSL を含む）、 ISDN 回線、回線交換回線、パケット交換回線、ATM 回線、衛星通信回線、光ファイバー通信網等を利用したバックアップ回線の確保（図 1）。

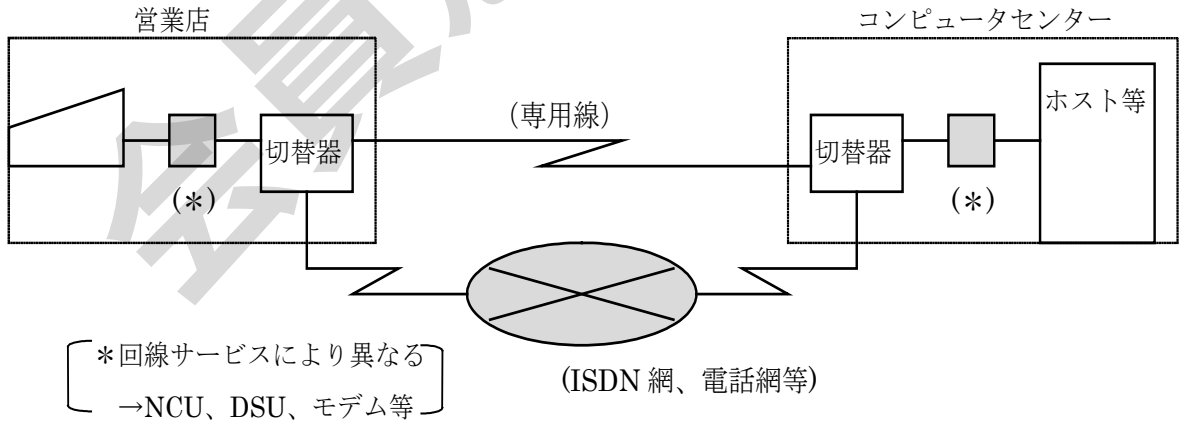


図 1　バックアップ回線の例

回線の別ルート化とは、回線ルートに障害が発生した場合に、全回線が同時に使用できなくなる事態を防ぐため、複数の回線により別々に接続し、並行して危険分散を図るための方法である。

なお、単一の通信事業者を利用し、中継局を分ける（物理的に別ルートにする）方法と、複数の通信事業者を利用する方法がある（図 2、図 3）。

①単一の通信事業者の利用

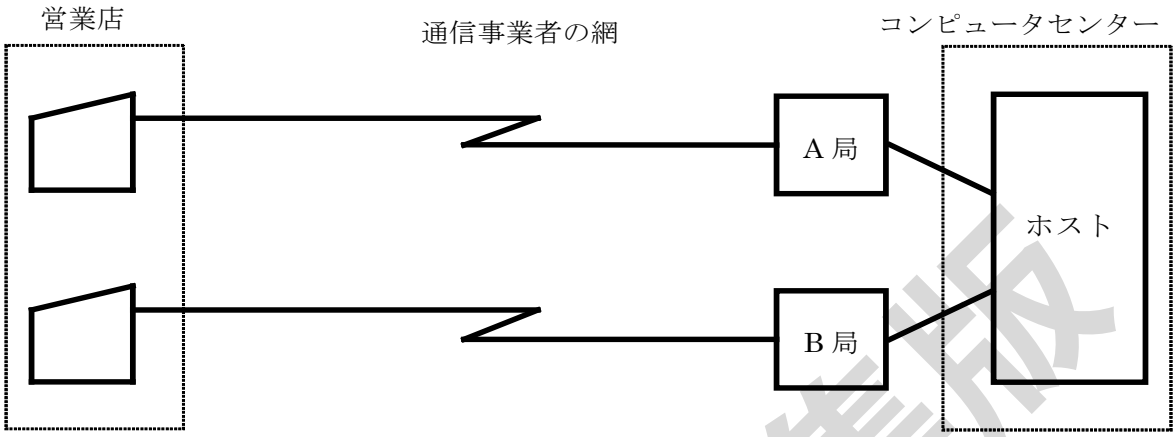


図 2　単一の通信事業者の利用例

②複数の通信事業者の利用

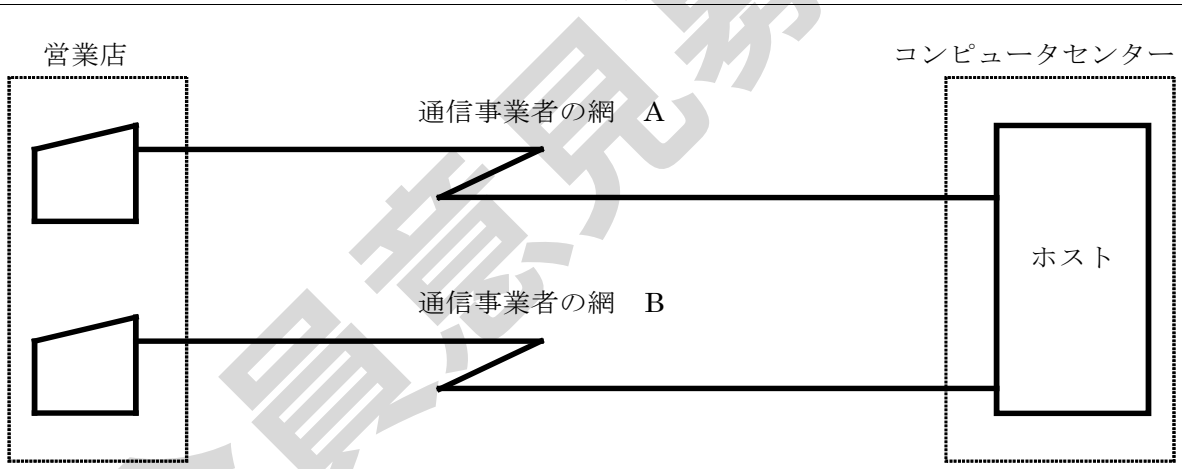


図 3　複数の通信事業者の利用例

代表的なデータ伝送経路の構成には、スター型構成（コンピュータセンター等の主要拠点と営業店等の拠点を 1 対 1 で接続する構成）、ツリー型構成（コンピュータセンター等の主要拠点より事務センター、基幹営業店等の中継結節点を経由し、複数の営業店等の拠点を接続する構成）等がある。構成によって、障害時の影響範囲、通信量及びコスト等について留意し、選択にあたっては、各種構成の特徴を踏まえ、業務への影響等を勘案する（図 4、図 5）。

会員意見募集版

①スター型の構成

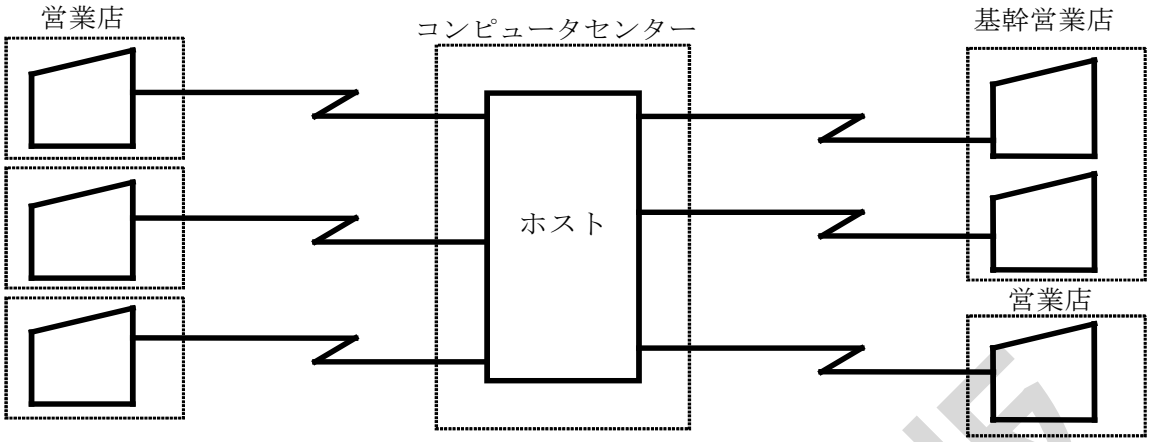


図 4　スター型の構成の例

②ツリー型の構成

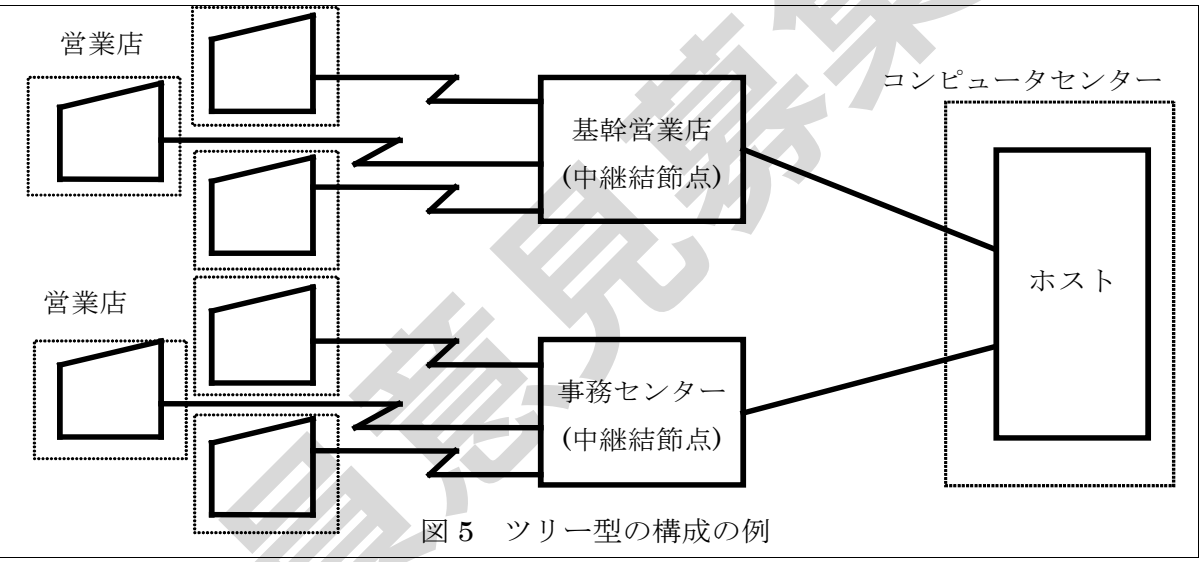


図 5　ツリー型の構成の例

3. 構内回線について、コンピュータセンター内の構内配線及び重要な部門 LAN は予備を設けることが望ましい。
コンピュータセンターにおいては、回線関連設備から重要な各機器までの配線は二重化することが望ましい。特に、建物外の回線を二重化した場合、コンピュータセンター内において、MDF から通信制御装置等の重要な各機器までの配線を二重化することが望ましい。

構内 LAN の予備としては、以下の例がある（図 6）。

会員意見募集版

＜会員意見募集版＞

①基幹 LAN の多重化（図 6）

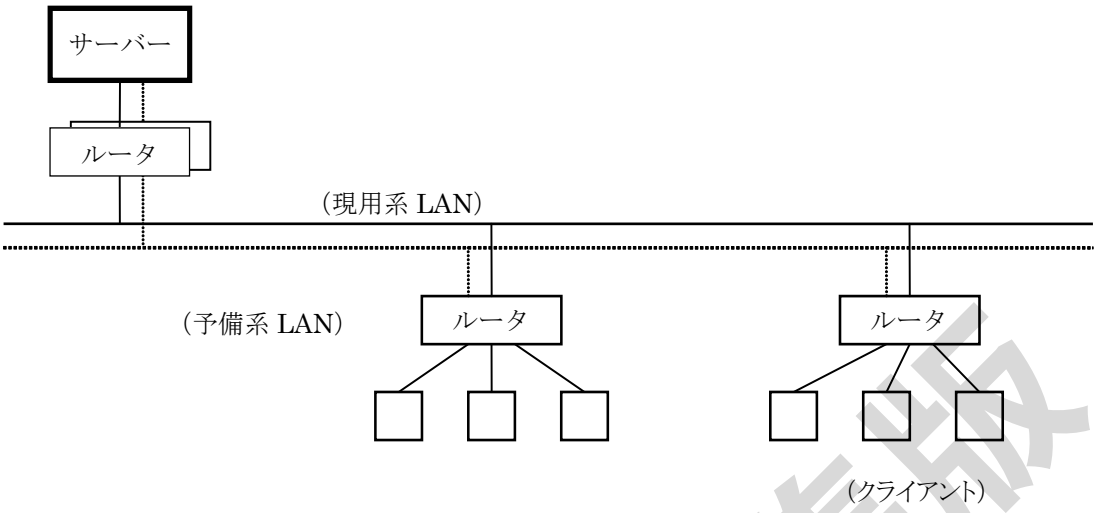


図 6　構内 LAN の多重化の例

4. システムの目的及び重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。
特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。
なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認する必要がある。

会員意見募集版

＜会員意見募集版＞

8 システムの信頼性向上対策
(1) ハードウェアの予備

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎			

実　88	端末系装置の予備を設けること。

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。

1. 端末系装置は予備または代替機能を設けることが必要である。

   端末制御装置（TC 等）、端末装置、クライアント機の予備または代替機能の持ち方としては、以下の例がある。

   (1) 規模などにより、地域ごと、主要営業店ごと、またはコンピュータセンターに予備を保有する。
   (2) 複数台設置することにより、予備と同様の効果を持たせる。
   (3) 端末制御装置に障害が発生したときに、配下の端末を他店等の端末制御装置に接続して使用する。
   なお、制御装置内にローカルファイルを有する場合、このファイルの障害に対する復旧対策及び予備の保有について考慮する。
   (4) ベンダーとの保守契約により代替機の提供を受ける。
   (5) 端末装置の障害の場合、異なる種類の端末装置や他の業務で使用している端末装置で代替する。
   ①CD・ATM 等、イメージ OCR 等の専用端末装置の障害時に汎用端末装置で代替する。
   ②汎用端末装置の障害時に渉外端末装置で部分的に代替する。
   ③業務系端末装置と情報系端末装置で相互に部分的に代替する。
   (6) 他店またはコンピュータセンター等の端末で代行入出力する機能を設ける。

2. システムの目的及び重要性に応じ、必要な予備（能力の余裕）を確保できるようにシステムを構築することが望ましい。
   特に、24 時間稼働システム等の長時間連続稼働システムにおいては、当該システムの機能及び制約に応じた予備（能力の余裕）を設けることが望ましい。
   なお、コンピュータシステムは本体装置のほか、周辺装置・通信系装置・回線・端末系装置等から構成されるため、障害が発生した場合に、それらの予備を含めたシステム全体が有効に機能することを確認する必要がある。

会員意見募集版

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 89	必要となるセキュリティ機能を取り込むこと。

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。

1. 開発するシステムが具備すべきセキュリティ機能、及びそれらを実現するために必要となる技術については、システム計画段階から考慮することが必要である。

2. セキュリティ対策は、全体のシステム開発計画と整合性がとられ、処理する業務、データの重要性及びリスクに応じて決定されることが必要である。

（参考）OECD 理事会勧告のセキュリティガイドライン（1992 年）における
情報システムセキュリティの目的

「情報システムセキュリティの目的は、情報システムに依存するものの利益を可用性（Availability）、機密性（Confidentiality）、完全性（Integrity）の欠如に起因する危害から保護することである」

・可用性（Availability） ……ハードウェア、ソフトウェア、情報をいつでも利用できるように保持すること
・機密性（Confidentiality） …アクセスを許されていない者からハードウェア、ソフトウェア、情報を守ること
・完全性（Integrity）……改ざん等されないようにハードウェア、ソフトウェア、情報を完全な形態で保持すること

会員意見募集版

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

設計段階における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、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。

1. 設計段階において、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、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が必要である。

ソフトウェアの品質を確保するためには、まず設計段階から品質を高めることが重要であり、そのために考慮すべき点としては、以下の例がある。

(1) システム開発の前提となる要件の明確化

①セキュリティ要件の明確化

セキュリティ要件の明確化については、以下の点に留意する。

a.セキュリティポリシーとの整合性を確認する。

b.ユーザー要件としてのセキュリティ機能を満足する。

c.システムの開発においては、既に開発・導入済のシステムについて発見されたセキュリティ上の弱点を解決すること。また、開発時点で広く知られているセキュリティ上の弱点を解決する。【実 91】

d.監査証跡（処理内容の履歴を跡付けできるジャーナル等の記録）の作成機能の要件を明確にする。

②ユーザー要件の明確化

開発対象システムのユーザー要件となるものに入出力要件、主要機能要件（業務処理内容）、ハードウェア要件等がある。これらのユーザー要件について漏れのないようにするため、要件定義書及びシステム設計書のユーザーインタフェース仕様等についてユーザー側責任者の承認を得る手続きを明確にし、遵守する。

ここでいうユーザー側の責任者とは、そのシステムの利用に関して責任を負う人であり、部門の長、プロジェクトリーダー等を指している。

③開発目標の設定

ユーザー要件に基づく安全性の確保及びソフトウェアの品質確保に関して、信頼性、機能、性能、操作性、拡張性、保守性等の目標を設定する。

(2) 設計作業の標準化

設計作業の標準化の対象としては、以下の例がある。

会員意見募集版

①設計工程

設計の各工程ごとに行うべき作業、内容、範囲、完了条件

②ドキュメント

設計内容を記述するドキュメントの内容、作成手順

③レビュー

レビューの手順、実施基準

(3) 信頼度設計の考慮

エラー発生時のことを考慮して設計することも重要であり、以下の例がある。

①エラー局所化ルーチンの設計

ソフトウェアにエラーが発生しても、その影響が広がらないように影響範囲を局所化する。

②異常ケースの洗出しと対処策の設計（回避または代行）

異常ケースの洗出しを行い、その対処策を体系的に行う。

(4) レビューの実施

レビューとは、システムの完成度を高めるために、開発の各フェーズごとに検討会を開き設計書の検証を他人の目で行うことである。また、レビューを実施する際には、テストのしやすさ、読みやすさ、保守の容易性等さまざまな観点から検証する。

(5) 品質向上のための設計技法及びツールの活用

設計技法及びツールは技術の進歩にあわせて常に新しいものが提案されており、それらの検討とあわせて、組織体制の整備、標準化の推進、教育の実施等を行う。

会員意見募集版

（参考 1）

システムの信頼性を高め、開発の効率化を推進する例として、以下のものがある。

1. ソフトウェア開発形態、ソフトウェア開発手法

(1) ソフトウェア開発形態

①ウォーターフォールモデル

ソフトウェアのライフサイクルをいくつかのフェーズ（要求分析フェーズ、設計フェーズ等）に分け、各々のフェーズを滝とみなして、全体を上流から下流に至る滝の連なりと見なして開発していく形態。

②スパイラルモデル

目的とするソフトウェアを開発する前に、その一部を試作の形態で早期に動作させて評価し、その結果を本番ソフトウェアの開発にフィードバックする、プロトタイプ開発→評価→フィードバックという流れをステップごとに繰り返して開発を進めていく形態。

③アジャイルモデル

速い環境変化に対応し、よりニーズに合致したサービスをスピーディに提供していくことを目的として 1 週間～1 か月サイクルで、ビジネス価値が高い順に要件を整理→開発→レビューを繰り返し行い継続的に価値が高いシステムを開発する形態。

(2) ソフトウェア開発手法

①プロセス中心設計

プロセスを中心にとらえ、データをそれに付随するものとする考え方に基づく設計法。

②データ中心設計

データを中心にとらえ、プロセスをそれに付随するものとする考え方に基づく設計法。

③オブジェクト指向設計

プロセスとデータを一体化して独立したオブジェクトとしてとらえ（一体化することをカプセル化という）、オブジェクト間のインタフェースはメッセージ送受信のみで行う手法。

2. CASE（Computer Aided Software Engineering）ツールを利用したソフトウェア設計作業の効率化

(1) 設計情報の統合管理

データ項目の属性（長さ、タイプ等）、内容等を一元管理するための辞書及びツール等を利用し設計情報を統合管理する。

(2) 仕様記述言語の利用による後工程への活用

コンピュータ処理が可能なように作られた、仕様を記述する言語を利用して、後工程の作業へ活用する。

(3) 設計情報を再利用するための機能辞書システム

よく使う機能をパターン化し辞書に登録しておいて、それを再利用する。

会員意見募集版

3. 「共通フレーム 2013 ～経営者、業務部門とともに取組む「使える」システムの実現～」等を参照し、開発要員の間で作業内容を共有することがソフトウェアの開発の効率化に有効である。

4. 発注者視点による設計書等ドキュメントの記述やレビューに関する考慮点については、独立行政法人情報処理推進機構（IPA）ソフトウェア・エンジニアリング・センターに詳しい情報があるので参照のこと。
・独立行政法人情報処理推進機構（IPA）ソフトウェア・エンジニアリング・センター
http://sec.ipa.go.jp/reports/20080710.html

（参考 2）
スマートデバイスのアプリケーション設計に関する留意点
利用者情報の取扱いにおいては、総務省より公開されている「スマートフォン プライバシー イニシアティブ」の「第５章　スマートフォンにおける利用者情報の取扱いの在り方　1 スマートフォン利用者情報取扱指針」に参考となる情報が記載されているので参照されたい。
・「スマートフォン　プライバシー　イニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－」の公表
（平成 24 年８月）
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
総務省 利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会

提出意見募集版

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　91	プログラム作成段階における品質を確保すること。

プログラム作成段階における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の標準化・自動化等を行い、ソフトウェアの品質を確保すること。

1. プログラム作成段階において、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の標準化・自動化等を行い、ソフトウェアの品質を確保することが必要である。

プログラム作成作業の標準化・自動化としては、以下の例がある。

(1) 標準化

①適切な言語の選択

全体的な効率性を考慮し、目的にあった言語を選択する。

②プログラム検証のルール化（インスペクション）

作成されたプログラムがプログラム仕様書に基づいたものであるかを、他人が検証するものである。中核的なプログラム、及び新人等の技術及び標準化について経験の浅いプログラマーが作成したプログラムを対象に検証をルール化することはエラーの早期発見に有効である。

また、検証結果に基づくフォローアップを実施することも、その後のエラー削減に有効である。

③部品化、パターン化の有効活用

よく使う典型的なプログラムをパターンプログラムとして、使用頻度の高いコーディング部分を部品プログラムとして登録しておき、それを活用する方法である。

④その他

a.コーディング規約の作成

プログラマー間の個人差を解消し、他人に見やすくするようにするとともに、プログラムの誤りを少なくするために行うものである。

b.構造化プログラミングの利用

3 つの基本制御構造（命令を連続して実行する単純構造、命令のいずれかを実行する分岐構造、命令を繰り返し実行するループ構造）及びその組合せを使用してプログラムを作成する方法で、プログラムの誤りを発生しにくくするものである。

(2) プログラム作成の自動化

①プログラム自動作成ツールの活用

会員意見募集

以下のようなプログラム自動作成ツール等の活用も有効である。

a.仕様記述言語の利用による半完成プログラムの作成ツール

b.会話形式による画面定義作成ツール

c.設計仕様とコーディングの整合性をチェックするツール

②ドキュメント作成ツールの活用

以下のようなドキュメント作成ツール等の活用も有効である。

a.プログラム詳細処理説明書（フローチャート等）の作成ツール

b.日本語仕様書作成ツール

2. プログラム作成段階においてもコンピュータウイルス等の不正プログラムの侵入を防ぐことが必要である。特に、ネットワーク環境における開発において開発者同士がファイルを共有するケース、市販パッケージソフトを使用する場合等は、コンピュータウイルスの侵入機会が多いと考えられるため、抗ウイルスソフトによる監視が必要である。【実 20、実 21】

3. Web システムについては、Web アプリケーションの脆弱性対策を考慮してシステムを構築することが望ましい。

現在知られている Web アプリケーションで考慮すべき脆弱性としては、以下の例がある。

(1) SQL インジェクションの脆弱性
(2) OS コマンド・インジェクションの脆弱性
(3) ディレクトリ・トラバーサルの脆弱性
(4) セッション管理機構の脆弱性
(5) クロスサイト・スクリプティングの脆弱性
(6) CSRF（クロスサイト・リクエスト・フォージェリ）の脆弱性
(7) HTTP ヘッダ・インジェクションの脆弱性
(8) アクセス制御と認可制御の脆弱性

脆弱性対策としては、以下の例がある。

(1) 入力データを元に処理（SQL、スクリプト、シェル等）をアプリケーションで生成し実行する場合は、意図しない処理が実行されないような、各脆弱性に対応した適切な実装を行う。追加的対策として、入力項目及び入力パラメータについて、値の属性、データ長、制御文字の有無等の確認を行い不正なデータを排除する。
(2) ユーザーを特定する情報は推測困難なものとし、暗号化を施して送受信するなど漏洩しない方法で受け渡しする。また、なりすましの予防としてユーザーを特定する情報の発行をログイン成功後にするなどの実装を行う。
(3) データベース、システムファイル等の重要な資源に対し、適切なユーザー認証機能及び認可制御を設けて必要最小限の権限・アクセスのみを許可するような実装を行う。

会員意見募集版

（参考 1）

Web システムの脆弱性対策の参考文献として、以下のものがある。

(1)「安全なウェブサイトの作り方 改訂第 7 版」
　独立行政法人情報処理推進機構（IPA）セキュリティセンター

(2)「安全な Web サイト利用の鉄則」
　独立行政法人産業技術総合研究所情報セキュリティ研究センター

(3)「フィッシング対策ガイドライン」
　フィッシング対策協議会

（参考 2）

スマートデバイスのアプリケーション開発に関する留意点

スマートデバイスのアプリケーション開発においては、セキュリティを確保するコーディングのガイドとして、日本スマートフォンセキュリティ協会（JSSEC）より「Android アプリのセキュア設計・セキュアコーディングガイド」が公開されている。このガイドには Android に依存しない一般的な基礎知識の情報も記載されているので参照のこと。

・「Android アプリのセキュア設計・セキュアコーディングガイド」
　http://www.jssec.org/activities/index.html
　　一般社団法人 日本スマートフォンセキュリティ協会

会員意見募集版

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

テスト段階における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。

1. ソフトウェアに内在する欠陥を事前に発見・除去するとともに、ソフトウェアの正確性を十分に検証することが必要である。

2. ソフトウェアの品質を確保するために、以下のような事項に留意することが必要である。

(1) テスト計画書の作成

システムに求められる要件が多様化するにつれ、開発すべきシステム自体が複雑になり、信頼性の評価などソフトウェアの品質を検証するためのテストも複雑になってきている。
こうした状況において重要となるのは、テスト段階を円滑に行うための計画書である。
テスト計画書で明確にする主要項目は以下のとおりである。

①実施方針

テストの分類と目的、完了基準、テスト・スケジュール等

②実施体制

実施体制と役割分担、要員選出等（詳細下記）

③実施方法

テストツール及びその使用方法、検証方法、作業の依頼方法等

④実施資源

テスト環境、リソース見積等

⑤実施管理

プログラム管理（ライブラリ管理、資源管理等）、トラブル管理、ドキュメント管理、進捗管理、品質管理、外部委託管理等

(2) テスト体制の整備

テスト項目の量が膨大なシステムの場合には、テストの効率性、ソフトウェアの品質確保等を考慮し、テスト実施の専任体制を整備し分業化を図ることが必要である。
テスト結果の検収は、内容を十分理解できる要員によって実施する必要がある。
また、要員の選出にあたっては、利用部門、運用部門などの参画も有効な場合が考えられる。

(3) テスト工程の分類

テスト工程の分類としては、以下の例がある。

会員意見募集版

①単体テスト

モジュール単位等のある特定のプログラム範囲の機能を検証するテスト

②結合テスト（統合テスト）

モジュールを結合した（プログラム単位、サブシステム単位など）機能を検証するテスト

③システムテスト（総合テスト、総合運転テスト）

設計段階で計画したシステムの要件が計画のとおり機能することをシステム全体で検証するテスト

なお、ソフトウェアの品質を検証するため、システムテスト用ツール、過負荷テスト用ツール、異常テスト用ツール等によるシステムテストに加えて、本番に近い状態においてシステムテストを行うことも有効である。

a.性能テスト（ピーク処理時の性能評価を含む）

b.例外処理テスト

c.リカバリ・テスト

d.システムの利用者も参加したリハーサル

e.限界値テスト（許容最大件数を考慮した評価を含む）

f.連続運転テスト（閏日等の実際の日付構成や連続運用に即したテストを含む）

g.接続テスト（全銀システム、統合 ATM システム、共同 CMS 等の他システムとの回線接続、記録媒体授受を含む）

h.機密保護等のセキュリティ機能テスト

i.脆弱性テスト（Web アプリケーション、外部ネットワークとの接続部分の機器等）

(4) 各種テストツールの活用

テストを効率的に行うためのテストツールとしては、以下の例がある。

①単体テスト、結合テスト（統合テスト）工程におけるテストツール事例

a.ドライバー等（下位モジュールテスト実行ツール）

コンパイルの最小単位を実行するためのテスト用ツール

b.スタブ・シミュレーター等（未完成モジュール代理実行ツール）

プログラムをテスト実行するときに、未完成下位モジュールをシミュレートするテストツール

c.デバッガー

プログラム等のテスト実行において、デバッグを支援するテストツール

d.カバレージ等（テスト範囲管理ツール）

プログラムの全ルートのうち、どの程度のルートをテストしたか、その割合を測定するためのツールであり、テストの十分性評価の指標を与えるのに有効であるとともに、テストの進捗管理にも使えるツール

e.テストデータ・ジェネレータ

豊富なテストデータを作成するために、ひな型テストケースを基に詳細なケースに分かれたテストデータを自動的に作り出すツール

②システムテスト（総合テスト、総合運転テスト）工程におけるテストツール

a.システムテスト用ツール

システムを総合的に動作させてテストするためのテスト環境、テストデータの発生

会員意見募集版

機能、テスト結果のロギング機能等を備えたツール

b.過負荷テスト用ツール

過負荷状態を作り出す機能等を備えたツール

c.異常テスト用ツール

異常状態を作り出す機能等を備えたツール

d.脆弱性テスト用ツール

アプリケーションの脆弱性やネットワークの設定不備等のシステムの潜在的な脆弱性を発見するために、擬似攻撃（不正リクエストや不正パケットを送信して実際の攻撃手法のシミュレートを行う）の機能等を備えたツール

(5) テスト実施段階における各種管理

テスト実施段階における各種管理としては、以下の例がある。また、テスト終了後は、テスト結果報告書を作成し、開発責任者へ報告する。

①プログラム管理

プログラム等の作成、変更、削除が容易に行えるように、プログラムを管理するためのものである。この中には、以下の管理も含む。

a.ライブラリ管理

テスト段階では、テスト、バグ（欠陥）発見、プログラム修正（欠陥除去）という作業を繰り返し行うが、それらの作業を効率的に行うため、単体テスト、結合テスト（統合テスト）、システムテスト（総合テスト、総合運転テスト）等の工程ごと、または業務ごとにライブラリを分ける等の保有手段を提供し、その管理を行うものである。

b.データ・ディクショナリー管理

プログラム等で参照するデータ及びプログラムの相互関係等を一元的に管理することにより、テスト段階の変更を漏れなく行うためのものである。

c.変更管理

新規要件の追加、要件の変更等に対し、ドキュメント、プログラム等の変更管理を明確にするとともにそれを管理し、関係者に周知されるようにするためのものである。

②トラブル管理

トラブルの原因を解明し、そのトラブルの迅速かつ確実な解決を行うとともに、トラブルの発生状況及び発生傾向を把握・管理し、同一・類似トラブルの再発を未然に防ぐためのものである。【実 72】

③ドキュメント管理

テスト仕様書（テストケース一覧表、テスト項目等）、テストデータ、テスト結果報告書、カバレージ報告書等のテストドキュメントを各テスト工程ごとに整備し、その管理を行うものである。

④進捗管理

テストで発生する問題の早期発見と対策の早期実現を図り、テスト計画に基づき遅滞なくテストが実施されていることを管理するものである。

⑤品質管理

テストで得られた結果が、品質管理基準値を満たしているかを検証、管理するもので

会員意見募集版

ある。なお、テスト環境（テストツールやテスト用媒体）からのコンピュータウイルス等の不正プログラムの侵入を防止することもテスト段階における品質管理である。

会員意見募集版

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

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及びウイルスチェックを行うこと。

1. 業務用アプリケーション等のプログラムを配布する際は、プログラムを開発し検証した環境と、稼働する機器の環境の違いを考慮し、整合性を確認することが必要である。

   考慮すべき環境の違いとしては、以下の例がある。
   (1) ハードウェア環境（マイクロプロセッサ、メモリ容量等）の相違
   (2) OS、ミドルソフト等の相違、それらのバージョンの相違

2. 環境の違い等の要因により、配布したプログラムが正常に稼働しないケースを想定し、リカバリ手順を含めた更新手順を取り決めておくことが望ましい。

3. プログラム開発時及びテスト時にコンピュータウイルス等の不正プログラムが混入するケースを想定し、プログラムの配布前にウイルスチェックを行うことが必要である。
   コンピュータウイルス等の不正プログラムの防止については【実 20、実 21】を参照のこと。

会員意見募集版 配布資料

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

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。

パッケージの品質を確保するため、機能及び自社システムとの整合性を確認すること。

1. パッケージの導入にあたっては、機能及び自社システムとの整合性を確認することが必要である。

パッケージ導入時の品質確保の対策としては、以下の例がある。

(1) パッケージ導入の前提となる要件の明確化

①ユーザー要件の明確化

購入するパッケージのユーザー（利用者）の要件となるものに入出力要件、主要機能要件（業務処理内容）、ハードウェア要件などがある。

②目標の設定

ユーザー要件に基づいて、安全性確保やソフトウェアの品質確保に関して、信頼性、機能、性能、操作性、拡張性、保守性等の目標を設定するものである。

(2) 機能について記載された仕様書、設計書、テスト確認書等のドキュメントの確保

安全性確保やソフトウェアの品質確保及びメンテナンスのため必要となるものである。

(3) 自社によるテスト

機能、性能、操作性等を確認するためのテストについては【実 92】を参照のこと。

(参考 1)

契約により、販売者と購入者の責任を明確にすべき例として、以下のようなものがある。

・パッケージのソフトウェアを使用する装置等の使用条件
・ソフトウェアについてのバグ（欠陥）その他の瑕疵を発見した場合の責任所在
・障害発生時の支援体制
・メンテナンスの範囲、期限等（脆弱性の修正パッチの提供を含む）

会員意見募集版

（参考 2）

パッケージ購入にあたり、留意すべき事項として、以下のようなものがある。

特にクライアントサーバー・システムの場合、インストールする機器ごとに OS のバージョンやハード要件等の環境が相違することもあるため十分に留意すること。

1. オペレーティングシステムのバージョンレベルの確認
   パッケージのソフトウェアが動作可能なオペレーティングシステムであることを確認するものである。
2. アプリケーションパッケージ間の連係時のバージョンレベルの確認
   すでに導入しているアプリケーションパッケージとの連係や、同時に購入する複数のパッケージ間の連係について、バージョンレベルの確認を行うものである。
3. 最大利用記憶容量等の必要資源の確認
   自社システムの記憶容量等がパッケージのソフトウェアを稼働させるのに十分であることを確認するものである。
4. コード体系の確認
   自社システムとパッケージのソフトウェアにおけるコード体系の整合性を確認するものである。
5. 機密保護への対応
   機密保護等のセキュリティ機能がパッケージに組み込まれていること。また、必要に応じてカスタマイズが可能であること。
6. コンピュータウイルスのチェック
   購入パッケージそのものにコンピュータウイルスが潜むケースもあるため、導入時のウイルスチェックが必要である。

会員意見募集版

＜会員意見募集版＞

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 95	定型的な変更作業時の正確性を確保すること。

定型的な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。

1. 定型的な変更作業時は、作業の合理化等の必要な対策を講ずることが必要である。

定型的な変更作業の例として、営業店新設、機器の増設に伴うプログラムの定義変更等があるが、それらの変更作業時における正確性を確保するための対策としては、以下の例がある。

(1) 変更作業の合理化

①定義の一元化

テーブル化またはデータベース化することなどにより、営業店、機器等の定義を一元化し、1項目の変更のための修正が複数箇所とならないようにする。

②変更手順の簡略化

変更作業の信頼性向上のため、各種テーブルまたはデータベースに関する変更、追加、削除の手順の簡略化を進める。

(2) 変更内容と作業手順のドキュメント化

定型的変更に伴い変更やテストを要するプログラム等のすべてが、最新の状態で把握でき、かつ変更箇所や変更方法が記述してあるドキュメントを作成する。

これを使用して変更作業に抜け落ちがないかを確認し、正確性の確保を図る。

(3) テスト及び検証手順の確立

変更結果の整合性及び妥当性をチェックするためのツールの作成（変更部分のテスト、副作用テスト、チェックリスト等）、手順のマニュアル化等により、変更作業の正確性を確保する。

会員意見募集版

＜会員意見募集版＞

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　96	機能の変更、追加作業時の品質を確保すること。

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。

1. 機能の変更、追加作業時は、開発時の品質向上対策を準用することが必要である。

2. 機能の変更、追加作業時においては、他への影響をチェックし、極小化することが望ましい。

対策としては、以下の例がある。

(1) 変更、追加箇所の確認

①ドキュメント生成支援ツールの活用

プログラムのドキュメント生成支援ツールを有効活用し、変更箇所をドキュメントで検証・確認する。

②プログラムの新旧比較ツールの活用

変更、追加作業前後のプログラムを比較し、目的のとおりに作業されていること、及び不要な箇所が変更されていないことを確認し、新たなバグの発生、不正ロジックの組込みを防止する。

(2) 影響度の検証

①テスト環境、テストデータ等の整備

変更前のテストデータを用い、変更箇所以外の部分について、テスト結果が変更前と一致することを確認するため、テスト環境、テストデータ等を整備して活用する。

②影響度確認支援ツールの活用

プログラムとプログラム、プログラムとファイル、プログラムとデータ等、それぞれの間のクロスリファレンスを作成し、機能の変更、追加がどのプログラムやファイル等に影響を与えるか確認する。

(3) 機能の変更、追加作業時の障害対策

①バックアップ

機能の変更、追加時の品質確保に努める一方で、機能の変更、追加による障害対策として、変更前のシステムをバックアップとして準備する。

②障害時回復手順の作成

障害発生に備えて、その回復のための手順の確立、テスト、訓練等を行う。

ソフトウェアの品質確保については【実 90～92】を参照のこと。

意見募集版

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適用区分					基準分類
共	セ	本	提	ダ	付加
◎					

実 97	ファイルに対する排他制御機能を設けること。

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。

1. 同一ファイルに複数のプログラムから同時更新がある場合は、データ内容に矛盾を起こし、結果的にファイル破壊となる。これを防止するため、ファイルに対する排他制御機能を設けることが必要である。

2. 同一システム内の複数のプログラムでファイルを共用する場合は、同一ファイルに対する同時アクセスが起こり得る。このため、一方がアクセス中はその処理が終了し、ファイルを解放するまで要求中のプログラムを待たせる排他制御機能を設けることが必要である。

   排他制御のレベルとしては、以下の例がある。
   (1) ファイルレベル
   (2) ブロックレベル
   (3) レコードレベル

3. 複数システム間でファイルを共用する場合、複数システムで共用されるファイルは、各システムから排他制御をかける対策が必要である。

   排他制御をかける対策としては、以下の例がある。
   (1) システム間における排他制御情報の伝達、確認
   (2) ファイル制御装置の排他制御機能の活用

4. ファイルに対する排他制御機能組込みにより、デッドロックが発生することがある。このためデッドロックによる待ち状態を回避する対策が必要である。

   デッドロック回避の対策としては、以下の例がある。
   (1) デッドロックの検知と解除
   　デッドロックの発生を検知し、デッドロックが発生したトランザクションの一方をいったん無効とし、デッドロック状態を解除したうえで当該トランザクションを再処理する。

会員意見募集版

8 システムの信頼性向上対策
(2) ソフトウェアの品質向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　98	ファイル突合機能を設けること。

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。

1. ファイル間の内容不整合、論理エラー等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内容を突合、検証する機能を設けることが必要である。

   不整合の原因としては、以下の例がある。
   (1) データの改ざんによる不整合
   (2) プログラムのミスによる不整合
   (3) システム障害時、仕掛かり中取引のリカバリ不備による不整合

   ファイル突合機能としては、以下の例がある
   (1) トータルチェック
   トータルチェックは、元帳ファイルと精査表を合計数値により突合するものである。
   さらに、元帳ファイルと取引ジャーナルとの突合を行うことは、整合性の精度を高めることに役立つ。

2. 分散処理においてファイルを分散している場合には、ファイル間の整合性に留意することが必要である。

会員意見募集版

8 システムの信頼性向上対策
(3) 運用時の信頼性向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　99	オペレーションの自動化、簡略化を図ること。

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。

1. 汎用機、サーバーのオペレーションについては、自動化、簡略化を図ることが望ましい。

オペレーションの自動化、簡略化としては、以下の例がある。

(1) コンピュータセンターにおけるオペレーション

①自動化

システムの起動や業務の開始を自動的に行う機能、ジョブの起動やジョブと記憶装置の対応を自動化する機能等、各種自動運転機能を活用する、またはそれぞれの実情に応じた機能を開発することなどによりセンターオペレーションの自動化を図るものである。

また、運用スケジュールの規模に応じてシステムの電源投入を自動的に行う機器、テープハンドリングを自動的に行う機器を活用することもオペレーションの信頼性、安全性、情報の機密保護を向上させるうえで有効である。

スケジュール化されたジョブグループのジョブシーケンスに従ったジョブの自動起動やタイマーによるジョブの時間起動のほかに自動化としては、以下の例がある。

a.電源投入からシステムの立上げ、オンラインジョブの起動、端末の開局等、業務が開始できるまでの一連処理の自動化

b.平常日、繁忙日、月末日、土曜日等パターンごとにスケジュール化された一斉同報通知の送出や端末モード変更の自動化

c.取引ジャーナル等のファイルのバッチジョブへの引継ぎの自動化

d.取引ジャーナル等のファイルの他システム（系）への引継ぎの自動化

e.端末の閉局からオンラインジョブの停止までの一連の処理の自動化

f.システム停止の自動化

g.テープハンドリングの自動化

なお、自動運用の注意事項として処理の順序や運転状況、条件の変更が生じた際にも、システム全体の運用に支障がないように、自動化を変更できる機能を充実することが重要であり、変更内容としては、以下の例がある。

a.一斉同報通知や端末モード変更を行う時刻の変更

b.システム（系）の変更（現用系から待機系への変更、またはその逆）

会員意見募集版

c.自動運用からマニュアル運用への変更

d. ジョブネットワークへのジョブの追加、変更

e.ボリュームの追加、変更

f.実行 JCL（ジョブ制御言語）の変更

②簡略化

コマンド体系の一元化、出力メッセージの日本語化を図るなどして、オペレータインタフェースを平易化する。さらに、運用をケースによりパターン化し、一連のコマンド列を一括実行できるように準備することなどにより、オペレーションを単純化、簡略化する。

オペレーションの単純化、簡略化としては、以下の例がある。

a.コマンド入力の極少化

b.テープハンドリングの極少化

c.異常終了後再開オペレーションのパターン化

③自動化、簡略化の留意点

センターオペレーションの自動化の推進は、オペレーションの信頼性向上のために有効であるが、過度の自動化は、機械運行の安全性を阻害する可能性もある。そのような場合には、単にオペレータへの通報にとどめる等、オペレータによる判断の余地を残しておく。

オペレータの応答を必要とするメッセージやオペレータに注意を喚起する必要があるメッセージ等は、高輝度出力、赤字出力やブザーを鳴らす（オペレータの応答で解除）方法等で重要メッセージの見落としを防ぐように工夫する。さらに、大量メッセージによるシステム停止等を防ぐため、冗長なメッセージを抑止する等の仕組みを合わせて構築する。

(2) 本部・営業店等におけるオペレーション

本部・営業店等における重要なサーバーのオペレーションは、コンピュータセンターにおけるオペレーションに倣って自動化、簡略化を図る。さらに、本部・営業店等でコンピュータ運用に必要な知識や技能を持つ専門のオペレータを配置することが困難な場合には、自動化等の運用をリモート操作で行う機能を設ける。

①自動化

本部・営業店等のサーバーオペレーションの自動化としては、以下の例がある。

a.電源の投入やシステムの立上げ、業務アプリケーションの起動

b.バックアップの取得やデータベース更新手順

c.障害発生時の縮退運転の手順やシャットダウン手順

②簡略化

簡略化としては、以下の例がある。

a.オペレーション用のインタフェースを平易化（ユーザーフレンドリなインタフェースの採用）

b.一連のコマンドを一括実行しコマンド入力を極少化

c.異常終了時の再開オペレーションの単純化

2. データ入力作業（端末オペレーション）については、自動化、簡略化を図ることが望ましい。

データ入力作業のオペレーションの自動化、簡略化としては、以下の例がある。

(1) 自動化

磁気ストライプ読取装置、現金処理機、OCR 等の活用により、手入力操作の一部またはすべてを削減する。

(2) 簡略化

オペレーションガイダンス機能の活用等により、入力判断の平易化やコード入力による簡略化を行う。

会員意見募集版

8 システムの信頼性向上対策
(3) 運用時の信頼性向上対策

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 100	オペレーションのチェック機能を充実すること。

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。

1. コンピュータセンターにおける汎用機、サーバーのオペレーションミスの防止、早期発見のために、チェック機能を充実することが必要である。

   コンピュータセンターにおいてオペレータの作業をチェックする機能としては、以下の例がある。

   (1) コマンド入力の再確認機能

   センターオペレーションについて、誤操作により重大なシステム障害を起こす可能性のあるコマンドの再確認機能を設ける。

   (2) 妥当性チェック機能

   処理の順序性や運転状況、条件（時間帯、曜日等）により、入力されたコマンドが妥当なものであるかどうかをチェックする機能を組み込む。

   (3) テープ使用時のラベルチェック機能

   使用する磁気テープの妥当性をチェックするため、ジョブとボリュームラベルの対応チェック機能を有効に活用する。

2. 本部・営業店等で重要なサーバーのオペレーションを行う場合には、コンピュータセンターに準ずるチェック機能を備えることが必要である。

3. コンピュータシステムの端末操作者が入力したデータについて、チェック機能を設けることが必要である。

   データ入力作業におけるチェック機能としては、以下の例がある。

   (1) 入力のチェック機能

   入力するデータ項目ごとのチェック（桁数オーバーの検出、省略不可の検出等）や項目間の関連性チェック、または口座番号などのチェックディジットの検出等により、チェック機能を充実する。

   (2) 各種合計突合機能

   個々の入力データのチェックだけでなく、端末の取り扱った件数・金額等の合計を突合する機能（精査カウンター等）を設ける。【実 6】

全銀協 会員意見募集版

（参考）本部・営業店等におけるオペレーションチェックについて

オペレーションのチェックは、第一義的には処理目的の正当性や操作者の権限を確認することが重要である。本部･営業店等において、この点の確認を確実に行うためには、以下のような機能を持つこと、及び手順を定めることが望ましい。

1. 処理目的や根拠を責任者がチェックし、作業そのものの妥当性を確認する手順
2. 作業手順や実施タイミングの正当性を確認する手順
3. 処理結果を責任者がチェックするためのレポート出力機能や、作業履歴を取得し、保存する機能

会員意見募集版

＜会員意見募集版＞

8 システムの信頼性向上対策
(3) 運用時の信頼性向上対策

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　101	負荷状態の監視制御機能を充実すること。

コンピュータシステムの安定稼働のため、各種資源の能力及び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。

1. 各種資源の能力及び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が必要である。

   負荷状態の監視制御機能としては、以下の例がある。

   (1) 監視機能

   ①負荷状態表示機能

   中央処理装置、チャネル装置、ファイル装置、通信制御装置、回線等の負荷状態が把握できるような表示機能である。

   ②使用状況照会機能

   主記憶装置、ファイル装置等の資源の使用状況（バッファ、ファイル容量等）を把握するため、照会機能を設けておく方法である。

   さらに、使用率が限界値に近づいた場合、警告を発する機能を設けておく方法もある。

   また、各種資源の使用状況について、平均値、最大値等の統計データが得られるようにしておき、それを定期的にチェックし、対策を事前に講じておくことも考えられる。

   (2) トラフィック制御機能

   メッセージの待ち行列やシステムコントロール上重要なカウンター類等の使用状況が限界に近づいた場合、コンピュータシステムへの入力を抑える制御機能を設けておき、コンピュータシステムを安定的に稼働させるものである。

   また、トラフィック制御はジョブの優先度・多重度を変更することによって行うこともある。

2. 本部・営業店等に分散配置された機器等については、リモートによる集中監視・制御が有効である。なお、分散環境における負荷状態の監視機能としては、SNMP 等の監視用プロトコルを使用することによって、分散したシステムのノード装置の管理情報データベース（MIB）の定期的な収集、しきい値を超えたノードのアラーム自動送出、ノード装置のリモート制御が可能になる。

   （SNMP：Simple Network Management Protocol）

   （MIB：Management Information Base）

会員意見募集版

（参考）
過負荷発生のトラフィック制御のミスにより、重大な故障に発展したケースがあるので参考までに事例を以下に取りまとめた。
過負荷トラブルはオンラインシステムを構成する各種資源が、さまざまな要因で不足することに起因して発生する。

1. 資源不足の具体例としては、以下のようなものがある。
   (1) CPU 能力の不足（マルチプロセッサの片側 CPU 故障時等）
   (2) ファイル装置またはチャネル装置の使用率オーバー（パス系故障による片パス運用時の考慮洩れ等）
   (3) 主記憶装置容量不足（業務追加に伴うメモリ不足等）
   (4) 回線容量不足（部分的回線故障に起因等）
   (5) タスク数不足（トラフィック増加に伴う使用率増大等）
   (6) 一部の主記憶上のカウンター類への負荷集中（異常なトラフィックによる使用率増大等）
2. 主な障害の現象としては、タイムオーバーを繰り返す場合と、バッファ負荷となり過負荷通知はするが、負荷制御機能が働かずシステム異常になる場合とがある。
   前者のケースは、レスポンスタイムの悪化により、システム異常にみえるが、システムとしては、正常な動作をしているので、入力電文を減少させれば回復する場合が多い。
   後者のケースは、以下のような要因によるものであり、回復措置としてシステムの初期化を要する場合が多い。
   (1) バッファ過負荷発生の限界値の指定ミス（タイムオーバー等の同一エラーの繰返し、負荷通知用のバッファ不足等）
   (2) 負荷制御処理タスク（または入力キュー）の優先順位の設定ミス
   (3) スタック容量の不足（OS のテーブルチューニングにより設定）

会員意見募集版

8 システムの信頼性向上対策
(4) 障害の早期発見・回復機能

適用区分					基準分類
共	セ	本	提	ダ	基礎
◎					

実 102	システム運用状況の監視機能を設けること。

障害の早期発見・回復のため、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。

1. コンピュータシステムの運用状況については、システムの重要性に応じた適切な監視を行う必要がある。特に、個人データを取り扱うシステムにおいては、この措置は必要である。
また、待機中の機器についても、本番環境に接続されている等により監視可能な場合には、本番機と同様の扱いとすることが必要である。

   監視機能の具体的な内容としては、以下の例がある。
   (1) ソフトウェアによる監視
   一定時間ごとに装置へのアクセスを行い状態把握を行う。
   (2) コンソールからのステータスディスプレイ機能による表示
   オペレータからの照会コマンドにより各機器の状態を表示する。
   (3) 遠隔監視盤等によるリモート監視
   システムの運転状況、エラーメッセージ等を表示するディスプレイ装置により、コンピュータ室から離れた室で監視を行う。
   (4) サービスプロセッサによる監視
   保守診断専用の独立したプロセッサであり、リアルタイムにシステムの運転状況を把握する。

   システムの規模が大きくなるにつれ、集中監視が重要になるが、集中監視の内容としては、以下の例がある。
   (1) コンピュータシステムの監視については中央処理装置、チャネル装置、各種ファイル装置等の運転状況を集中監視する方法がある。
   (2) ネットワークの監視については、回線、マルチメディア変換装置、時分割多重装置、モデム、TA、ルータ、HUB、端末等の運用状況を集中監視する方法がある。

2. システムの重要度により、本部・営業店等に設置されたサーバーの監視も必要である。本部・営業店等において必要な技能を持った担当者を置くことが困難な場合には、リモートによる集中監視のみならず以下のようなリモート制御の機能を持つことが望ましい。
   (1) サーバーのパワーコントロール（リモート電源 ON／OFF）
   (2) DBMS 等のミドルソフトウェア及び業務アプリケーションの起動・終了

会員意見募集版 無断転載禁止

(3) システム環境の最適化
(4) データアクセスの分散化及びトランザクションのプライオリティ制御

（参考）本部・営業店等に設置されたサーバー・システムにおける考慮点

本部・営業店等に設置されたサーバー・システムの安全性・信頼性に関しては、以下の点を考慮する必要がある。

(1) コンピュータセンター以外の場所に設置された機器等については、熱、振動、水、煙、埃、電圧変化などの脅威に晒される機会が増加する。
(2) LAN 等のネットワークの大規模化、複雑化が進展し、障害発生時の原因究明を困難にしている。

このようなことから、危険な兆候や業務処理に支障の起こる可能性のある状態（例えば、磁気ディスクの I/O エラーの増加や局所的なトラフィックの集中）を早期に発見し、しかるべき対処を行うことも必要である。そのため、システムの運用状況を監視することが重要であり、監視・制御専用のネットワークサーバー等を用いた集中監視・制御が有効である。

会員意見募集版

8 システムの信頼性向上対策
(4) 障害の早期発見・回復機能

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

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。

1. 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が必要である。

   障害を検出し、障害箇所の切り分けを行うための機能としては、以下の例がある。

   (1) 異常検出機能

   迅速な障害回復に役立てるための異常を検出する機能。

   ①中央処理装置、主記憶装置、ファイル装置、回線、端末装置等の障害検出機能

   ②ソフトウェア障害検出機能

   (2) ロギング機能

   迅速な障害箇所切り分けに役立てるための機能。

   ①エラー発生時の状態に関する詳細情報のロギング機能

   ②コンソールメッセージのロギング機能

   ③障害発生までの稼働状況がトレースできる情報をロギングする機能

   （例：I/O トレース、モジュールトレース等）

   (3) テスト機能

   迅速な障害箇所切り分けに役立てるための以下の機能。

   ①折返しテスト機能

   ②診断テスト機能

会員意見募集版

8 システムの信頼性向上対策
(4) 障害の早期発見・回復機能

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　104	障害時の縮退・再構成機能を設けること。

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。

1. 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が必要である。
なお、縮退・再構成時のオペレーションについてもパターン化し、極力オペレータの介入を少なくすることも有効である。

縮退・再構成機能としては、以下の例がある。
(1) 障害が発生した部分に関する取引を閉塞する機能
(2) 障害が発生した部分の切離しを行う機能
　オンラインシステムに影響を与えないで修理できるようにすると、さらに有効である。
(3) 正常な構成要素で運転が続行できるように構成しなおす機能
　障害復旧後、再組込みができるようにすると、さらに有効である。

対象となる構成要素として、ハードウェア、ソフトウェアの両面があるが、ハードウェアとしては、以下の例がある。
(1) マルチプロセッサシステム等における中央処理装置
(2) 主記憶装置
(3) チャネル装置
(4) ファイル装置
(5) 通信制御装置
(6) 回線、端末系装置

会員意見募集版

8 システムの信頼性向上対策
(4) 障害の早期発見・回復機能

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

実　105	障害時の取引制限機能を設けること。

ファイル障害、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。

1. 障害の影響を極小化するため、障害の状況に応じ一部取引を稼働中のシステムから切り離すなどの措置がとれるような取引制限機能を設けることが必要である。

   取引制限の単位としては、以下の例がある。
   (1) 業務
   (2) 科目
   (3) 提供サービス・商品
   (4) 稼働プログラムの制御単位
   (5) 営業店等の営業地域
   (6) 端末装置
   (7) 取引相手、取引口座

会員意見募集版

＜会員意見募集版＞

8 システムの信頼性向上対策
(4) 障害の早期発見・回復機能

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

実　106	障害時のリカバリ機能を設けること。

障害が発生した場合に、速やかにシステムを回復させ業務への支障を最小限にして続行させるため、必要なリカバリ機能を設けること。

1. 障害時の回復時間を短縮し業務への影響を少なくするため、リカバリのための機能が必要である。

   リカバリ機能としては、以下の例がある。

   (1) リカバリ用ジャーナル機能
   各種リカバリに役立たせるため、データ処理の過程を記録する。

   (2) チェックポイント機能
   迅速なリカバリを行うため、主記憶装置に展開している重要カウンター及び端末テーブル等を一定時間ごとまたは一定取引量ごとに外部記憶装置に記録する。

   (3) 部分リカバリ機能
   プログラムやタスク等が異常終了した場合、他のプログラムやタスクには影響を与えず（システムダウンさせず）、ジャーナル情報を基に回復させる。

   (4) ダウンリカバリ機能
   システムダウンに至った場合、ジャーナル情報を基に回復させる。
   そのためには、取引の成立基準を定めるとともに、再開始時に最終成立取引が把握できるようにすることも重要である。

   (5) ファイルリカバリ機能
   ファイルに障害が発生した場合、バックアップファイルやジャーナルに基づき、ファイルを回復させる。
   なお、迅速なファイルリカバリのため、装置の特性に応じて、例えばユニット単位、シリンダー単位等により回復範囲の極小化を図る方法もある。

2. 複数サーバーで構成される分散処理システム等、複数のコンピュータで構成されるシステムの場合は、各コンピュータ間のシステム的な整合性を維持して復旧できるリカバリ手順を決定する必要がある。

3. 24 時間オンライン運転を行う場合は、リカバリに必要なデータをオンライン運転中にオンラインサービスに支障を与えることなく取得できる機能もしくは仕組みを考慮する必要がある。

会員意見募集版

該当する機能としては、以下の例がある。

(1) ファイルの復旧においては通常、元帳ファイル等のバックアップファイルを起点としてジャーナル情報により回復させる。そのためには、元帳のバックアップファイルが有効となる。

これら元帳のバックアップをオンライン運転中にも取得できるように元帳ファイルのスワップを行う機能等を考慮する。

(2) プログラム修復においては、プログラム内容に起因する障害が発生した場合、システムを停止させることなく、該当プログラムの修正を行う。

なお、分散処理システムのプログラムを修復させる方法としては、オフラインによるメンテナンスやオンラインによるリモートメンテナンス機能等がある。

会員意見募集版

9 個別業務・サービス
(1) カード取引サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎	◎		

実　107	カードの管理方法を明確にすること。

安全性の確保及び処理の円滑化のため、カードの発行、保管、交付、回収及び廃棄は定められた方法によって行うこと。

1. 不正行為を防止するとともに、不正行為に対する牽制効果を目的として、カードの発行（再発行も含む）、保管、交付、回収及び廃棄は定められた方法によって行うことが必要である。

2. カード発行業務に携わる責任者及び担当者を特定することが必要である。

3. カード発行依頼書に暗証番号が記入されている場合は、役席者が厳重に当該依頼書を管理することが必要である。

4. カードの発行は、定められた方法によって行うことが必要である。カード発行時に暗証番号の登録が必要な場合は、暗証番号の漏洩防止に万全の措置を講ずることが必要である。

   発行依頼書に基づき作成する場合の確認事項としては、以下の例がある。
   (1) 発行カードの正当性（エンコード、エンボス内容）の確認
   (2) 発行カード枚数とカード発行依頼枚数の一致確認

   漏洩防止措置としては、以下の例がある。
   (1) 登録時等にやむを得ず暗証番号の印字が必要となるような場合は、登録票に印字し管理を厳重に行う。
   (2) 金融機関職員が暗証番号登録に介在しない方式とする。具体的な方法としては、以下の例がある。
   ①顧客が暗証番号を直接キーパッドから入力する方法
   ②顧客が暗証番号を設定するのではなく、金融機関が初期暗証番号を割り当て顧客に暗証番号を変更させる方式

5. カードの保管管理は、定められた方法によって行う必要がある。

   カードの保管管理内容としては、以下の例がある。
   (1) カード（未使用、送付待ち、郵送返却、廃棄待ち）は金庫または施錠可能なキャビネットに厳重に保管する。

会員意見募集版

(2) 未使用カードの授受は、授受簿等に記録し、その事実を明確にする。
(3) カード発行後は下記方法により未使用カードの在庫を確認する。
在庫枚数＝作成前在庫枚数－作成枚数－作成失敗枚数

6. 顧客へのカードの送付は、原則として書留等受領の記録が残る郵便物により行い、発送管理簿等に記録を残しておくことが必要である。なお、やむを得ず営業店外で作成したカードを営業店で顧客に対し交付する際は、カード作成部署から社内書留等重要物件送付方法によりカードの送付を受け、十分な本人確認を行い、授受の明確化（受領書等の徴求）を行った後に交付することが必要である。
また、金融機関等から顧客に送付し、窓口で本人確認後に使用可能とすること、及び店頭交付の際の複数職員によるダブルチェックも有効である。

7. 書留等で郵送したカードが返送されてきた場合、役席者が保管管理簿等を用いて厳重に管理するなど、定められた方法で管理することが必要である。
なお、返却理由が「居所不明」のものは、原則として廃棄処分することが必要である。

8. 作成ミス、デザイン変更等により使用できなくなったカード及び長期未交付または口座解約等で回収したカードは、責任者立会いのもとで裁断、焼却等により廃棄する等、廃棄手続きを明確にすることが必要である。

9. 顧客本人が暗証番号を安全かつ容易に変更できる方法を顧客に明示することが必要である。

暗証番号の変更の方法としては、以下の例がある。
(1) 本部・営業店等の届出用紙等により、顧客の本人確認のうえ、暗証番号の変更を申請する方法
(2) 本部・営業店等の CD・ATM 等により、顧客本人が暗証番号を直接入力する方法

10. 顧客からカードの発行依頼があった場合、他人にわかり難い暗証番号を選定するように勧めることが必要である。その際、生年月日等の推測されやすいものを暗証番号として認めない仕組みがあることが望ましい。また、併せて暗証番号の重要性及び適切な管理方法について説明するか、カード送付時に同様の内容を明示した文書を添付することが必要である。【実108】

11. 磁気ストライプ上には、暗証番号並びに暗証番号が推測されるおそれのある情報は書き込まないことが必要である。
また、ゼロ暗証化されていない（非ゼロ暗証化）磁気キャッシュカードが残っている場合は、新規カードへの切替、ゼロ暗証化の手続きを顧客に促す等の適切な処置を講ずることが必要である。

12. テスト用カードの作成及び使用にあたっては、その目的を明確にするとともに、カードの作成時や使用開始から終了まで管理する体制を整備することが必要である。

全銀協 意見募集版

なお、管理体制の整備にあたっては、管理者も含め相互牽制が働くようにすることが望ましい。

(参考)
多機能カード発行においては、カードの盗難、破損等に伴い利用者が被る可能性がある損失等について、機能別にサービス提供者を特定するなど、責任の所在を明確にすることが重要である。【実 136】

会員意見募集版

9 個別業務・サービス
(1) カード取引サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎	◎		

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。

顧客並びに取引の安全性を確保するため、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。

1. 顧客を狙ったカード取引等に関する犯罪に対しては、サービスを提供する側の設備、運用だけでは限界があるため、顧客に対して犯罪に対する注意喚起を行うことが必要である。

   カード取引等に関する犯罪としては、以下の例がある。
   (1) CD・ATM 利用後店舗内外における襲撃
   (2) 盗難カードや偽造カードによる預金の不正引出し

   顧客に対する注意喚起の方法としては、以下の例がある。
   (1) 口座開設時に説明及びパンフレット等への明記
   (2) 配布パンフレット、ホームページ、店頭ポスター、CD・ATM 画面等へ注意事項等の情報掲載
   (3) DM 送付時に犯罪対処に関する情報を提供

2. カード及び暗証番号の適切な管理方法について顧客に注意喚起することが必要である。また、最新の犯罪事例をもとに必要な対策を周知することが必要である。

   注意喚起すべき事項としては、以下の例がある。
   (1) カードを安易に第三者に渡さないこと
   (2) カード上に暗証番号を記入しないこと
   (3) 他人に暗証番号を知らせないこと
   (4) 推測されやすい暗証番号を使用しないこと
   (5) キャッシュカードの暗証番号を他のパスワードと共用しないこと（貴重品ロッカー等のパスワードに使用しない等）
   (6) 不特定多数の者が使用するパソコンでは金融機関との取引を行わないこと（スパイウェアにより暗証番号・パスワード等が盗まれる危険性がある）
   (7) 警察官や金融機関の職員が、暗証番号等を直接顧客に照会することは無いこと（警察官や金融機関の職員を詐称し、暗証番号等を聞きだす犯罪行為があること）
   (8) 暗証番号は定期的に変更することが望ましいこと
   (9) ATM 利用明細書の取扱いに注意すること

会員意見募集版

3. CD・ATM 等の取引時の安全のため必要な事項を顧客に注意喚起することが必要である。

注意喚起すべき事項としては、以下の例がある。
(1) 不審者の有無等、周囲の安全に気を配ること
(2) 暗証番号等の覗き見に注意すること
(3) CD・ATM 等の周辺に見慣れないカード読取機等があった場合には気を付けること

4. 不正使用の早期発見のため、定期的（できれば毎月）に残高照会、通帳記帳等により取引内容を確認するように顧客に推奨することが望ましい。

5. 推測されやすい暗証番号を使用している顧客に対しては変更するように、個別具体的に対応することが望ましい。

具体的な対応方法としては、以下の例がある。
(1) 窓口対応
(2) 電話対応
(3) ダイレクトメール　等
なお、ダイレクトメール等を用いる場合には、当該顧客が推測されやすい番号を使用しているという情報が漏洩するリスクを考慮する。対策の例としては、通知内容に口座番号を記載しないことがあげられる。

推測されやすい暗証番号としては、以下の例がある。
(1) 生年月日
(2) 自宅の電話番号
(3) 職場の電話番号
(4) 自宅の住所
(5) 自家用自動車のナンバー　等

（参考）
国会における審議によると、盗難カード等による被害の場合、暗証番号を生年月日等の推測されやすいものとしていただけで、直ちに預金者の過失を問うことはできないとしている。そのためには、まず、金融機関から預金者に対し、生年月日等の推測されやすい暗証番号から別の番号に変更するように、複数回にわたる働きかけが行われることが前提となるとしている。加えて、この働きかけは、推測されやすい暗証番号を使用している預金者に対して、電話やダイレクトメール等により個別的、具体的に行う必要があり、ポスター等による預金者一般に向けた広報では、ここに言う働きかけには該当しないとしている。

参照法令	偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律（平成 17 年法律第 94 号）

会員意見募集版

9 個別業務・サービス
(1) カード取引サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

不正払戻し防止のため、CD・ATM 等の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。

1. 不正払戻し防止のため、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が必要である。

対策としては、以下の例がある。

(1) 認証技術の開発としては、
ICカード、生体認証技術の導入【実8】

(2) 情報漏洩の防止としては、
自動機器室等における覗き見防止設備の設置、ICカードの導入、CD・ATM等の伝送データの暗号化【実4】【実8】【設113】【設137】

(3) 異常な取引状況の早期の把握のための措置
異常取引検知技術の導入【実17】

(4) その他不正払戻し防止の措置
カードの偽造防止対策や携帯電話による取引ロック機能の導入【実11】【実111】

(参考)
預金者保護法
第九条第一項(偽造カード等又は盗難カード等を用いて行われる不正な機械式預貯金払戻し等の防止のための措置等)
金融機関は、偽造カード等又は盗難カード等を用いて行われる不正な機械式預貯金払戻し等の発生を防止するため、できるだけ速やかに、機械式預貯金払戻し等に係る認証の技術の開発並びに情報の漏えいの防止及び異常な取引状況の早期の把握のための情報システムの整備その他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ができるようにするとともに、預貯金者に対するこれらの措置についての情報の提供並びに啓発及び知識の普及、容易に推測される暗証番号が使用されないような適切な措置の実施その他の必要な措置を講じなければならない。

参照法令	偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律（平成17年法律第94号）

会員意見募集版

＜会員意見募集版＞

9 個別業務・サービス
(1) カード取引サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎	◎		

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。

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。

1. 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が必要である。また、休眠口座についても監視対象とすることが望ましい。

   ここでいう指定された口座のカード取引とは、犯罪に絡んで犯人の所在を把握するために捜査当局から依頼のあった口座のカード取引を指している。

2. 監視方法としては、当該口座に対しカード取引があった場合、取引のあった端末もしくは端末の設置場所を特定する情報等をコンソール上に表示するのが一般的である。
   なお、実際に取引のあった場合の連絡手続きを定めることも必要である。

   (1) 監視方法については【実 46】参照のこと。
   (2) 監視機能については【実 18】参照のこと。

会員意見募集版

9 個別業務・サービス
(1) カード取引サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎	◎		

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。

不正使用防止のため、カードの偽造防止の技術的措置を講ずること。

1. カード犯罪を防止し、カードを利用したサービスを安全に提供するため、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。

   カードの偽造防止対策としては、以下の例がある。
   (1) IC カード化
   (2) 磁気ストライプへの偽造を判別するコードの記録
   　当該コードは、容易に推察されない仕組みとする。
   　利用者の利便性を考慮して IC と磁気ストライプを併用したカードを導入する場合、IC 単独のカードに比べ安全性が低いことに十分留意する。例えば、IC を使用した場合と磁気ストライプを使用した場合とで、利用できる取引の種類、金額を区別することが考えられる。
   (3) カードへ有効期限を設定し、期限経過時に更新
   (4) 顔写真、ホログラム等の券面への印刷

2. キャッシュカードの IC カード化にあたっては、「全銀協 IC キャッシュカード標準仕様」に要求される要件を満たすこと（セキュリティ、互換性など）が必要である。また、IC カードの運用面及び技術面について、セキュリティ対策上注意し、定期的に見直すことにより時々の技術水準を反映することが必要である。

   IC カードの運用面及び技術面について、セキュリティ対策上注意すべき事項としては、以下の例がある。
   (1) IC カードの有効期限（電子証明書の有効期限）
   (2) 電子証明書の認証機関の信頼性（運用規則等）
   (3) 使用される暗号の強度
   (4) 耐タンパー性

会員意見募集版

9 個別業務・サービス
(2) インターネット・モバイルサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

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。

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、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。

1. 不正使用防止策として、厳正な本人確認を実施することが必要である。特に資金移動及び注文等の取引に関しては、より厳正な本人確認を実施することが必要である。

2. 不正使用防止策は、必要に応じて複数の対策を組み合わせることが望ましい。

不正使用防止策としては、以下の例がある。

(1) 予防策

①パスワード 【実 8】
②パスワードの入力失敗回数の制限及び監視 【実 9】
③ログイン時の本人認証に加え、資金移動、注文等の取引確定時、ID・パスワード、住所、登録メールアドレス等重要な登録事項の変更時等における更なる本人認証の実施
④指紋などバイオメトリクス 【実 8】
⑤同時ログオンの禁止
⑥前回の最終ログオフ日時の明示 【実 9】
⑦無アクセス時間による自動ログオフ 【実 9、実 10】
⑧コールバックによる端末、本人確認 【実 8】
⑨クライアント証明書の導入 【実 8】
⑩通常使用している端末以外からのログイン時、通常とは異なる取引が行われた時等、取引のリスクに応じた更なる本人確認 【実 8】
⑪暗号化 【実 8】
⑫電子署名 【実 8】
⑬Web アプリケーションの脆弱性対策 【実 14】
⑭フィッシング対策 【実 20】(参考 2)
⑮利用者機器（パソコンなど）のシステム環境チェック機能
⑯取引内容をモニタリングし、疑わしい取引及び異常を検知した場合は取引を一時的に中断する仕組み
⑰ハードウェアトークン等を利用したトランザクション認証

(2) 外部ネットワークからのアクセス制限

会員意見募集版

①プロバイダー（ドメイン）限定 【実 14】
②プロバイダーとの専用線接続 【実 14】
③登録済み IP アドレスのみ接続を許可 【実 8】

(3) 検知策
①不正侵入検知時、ログオン失敗を検知した場合のアラーム鳴動 【実 16】
②前回の最終ログオフ日時の明示 【実 16】
③暗号技術を活用した認証、並びに暗号技術を活用した改ざん検知 【実 7】
④送金等の取引及び重要事項の変更があった際の顧客への通知 【実 17】
⑤同一 IP アドレスからの複数アカウントによるログインの検知
⑥複数 IP アドレスからの同一アカウントによるログインの検知

なお、既に発見され、公表されている不正行為（侵入及び組込みの手口）の事例は、防御対策、検知対策に対する有益な情報となることが多い。したがって、これらについて記載されている文献、ガイド等を参考にすることも有効である。

3. 脆弱性が発見または報告された場合の手順を決めることが必要である。

4. 不正を検知した場合の手順を決めることが必要である。

（参考 1）
サイバー攻撃の脅威とその対策
(1) サイバー攻撃とは、重要インフラの基幹をなす重要な情報システムに対して、情報通信ネットワークや情報システムを利用した電子的な攻撃のことを言う。サイバー攻撃により国民生活や社会経済活動に重大な影響を及ぼす可能性があることが懸念される。
(2) 外国においては、金融機関等の情報システムが被害を受けた事例や、個人がいわゆるハッカーとして、重要インフラ等の情報システムに対する侵入、サービス不能攻撃（DoS 攻撃）、コンピュータウイルスの流布等によって重大な被害を起こした事例もある。
(3) 政府では、内閣官房を中心として、官民の緊密な連携の下、「情報セキュリティ対策に係る行動計画」等の実施に努めている。
(4) 個別金融機関等においては、サイバー攻撃による被害の可能性を極力少なくするために、外部ネットワークからのアクセス廻りの強化を行う等、ネットワークセキュリティ対策を強化することが望まれる。

（参考 2）
重要インフラ防護のための政府のサイバーテロ対策
・重要インフラの情報セキュリティ対策に係る行動計画
http://www.nisc.go.jp/

会員意見募集版

（参考 3）
不正アクセス対策、Web アプリケーションの脆弱性、セキュアプログラミング等については、独立行政法人情報処理推進機構（IPA）セキュリティセンターに詳しい情報があるので参照されたい。
・独立行政法人情報処理推進機構（IPA）セキュリティセンター
http://www.ipa.go.jp/security/index.html

（参考 4）
フィッシング対策の参考文献として、以下のものがある。
・「フィッシング対策ガイドライン」フィッシング対策協議会

（参考 5）
スマートデバイスを用いたインターネットバンキングサービス提供時の考慮点
(1) スマートデバイスは携帯性に優れている反面、紛失・盗難のリスクが高く、Web サイトにおける不正使用対策の充実が求められる。この対策として、【実 8】を参照されたい。
(2) スマートデバイスは、画面サイズの制約により接続した URL が一部しか表示できないため、不正な URL に気づかずフィッシングサイトにアクセスするリスクがある。 このようなフィッシング詐欺への対策については、（参考 4）にある「フィッシング対策ガイドライン」を参照されたい。

会員意見募集版

9 個別業務・サービス
(2) インターネット・モバイルサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

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。

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。

1. ユーザーID 等が不正使用されていないか、利用者自身で確認可能にすることが必要である。特に資金移動及び注文等の取引に関しては、不正使用の早期発見のため、処理結果が確認できる機能を提供することが必要である。
なお、不正に使用されていないかの確認を利用者自身が行うことを注意喚起することが望ましい。

不正使用の早期発見対策としては、以下の例がある。
(1) ログイン日時とログオフ日時の履歴表示 【実 16】
(2) 資金移動、注文処理結果等の取引結果表示
(3) 資金移動、注文処理結果等を郵送または登録アドレスへの電子メールによる通知
(4) ID・パスワード、登録メールアドレス等の重要な登録事項の変更処理結果等を郵送または登録アドレスへ電子メールで通知、住所変更の場合は登録アドレスへ電子メールで通知
(5) なりすましによるメールアドレスの変更を検知するため、登録アドレスの変更の際は、新旧登録アドレスに変更通知を出す。通知する内容としては、変更受付日時、変更に心当たりがない場合の連絡先がある。

2. 顧客への通知に電子メール等を用いる際は、顧客データが漏洩しないよう文面等に注意することが必要である。例えば、取引があったことだけを記載し、取引内容は記載しない文面とすることなどが考えられる。

会員意見募集版

9 個別業務・サービス
(2) インターネット・モバイルサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

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。

利用者が適切に取引機関及び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。

1. 利用者が適切に取引機関及び金融サービスの選択を行えるように、金融機関等はセキュリティポリシー等を開示することが望ましい。

   開示内容としては、以下の例がある。
   (1) 情報漏洩防止のために暗号化していること。
   (2) なりすまし防止のために認証（パスワード、電子認証）を行っていること。
   (3) 顧客に関する厳密な守秘義務に基づき、顧客データを保護していること。

   開示方法としては、以下の例がある。
   (1) DM への記載
   (2) 店頭や自動機器コーナーのポスターへの記載
   (3) 金融機関等ホームページへの記載
   (4) 新聞広告等
   (5) 電子メール

2. 開示にあたっては図、イラスト等を使用し、利用者に理解しやすいように工夫することが望ましい。

3. 利用者からの問合せ及び苦情に対応することが望ましい。
   問合せ及び苦情対応先、並びにその開示手段としては、以下の例がある。
   (1) 相談窓口の設置
   (2) パンフレット、ホームページ等に連絡先を明記

   利用者への安全対策に関する情報開示を実施するにあたっては、当センター発刊の「安全対策に関する情報開示研究会報告書」等を参照のこと。

会員意見募集版

9 個別業務・サービス
(2) インターネット・モバイルサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

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。

利用者との取引を安全に実施するため、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、受付対応等の顧客対応方法を明確にすること。

1. 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、受付対応等の顧客対応方法を明確にすることが必要である。

サービスの利用に関して顧客に周知すべき事項としては、以下の例がある。

(1) サービス内容・規約
(2) 操作方法
(3) 顧客対応窓口
(4) 金融機関等が実施している安全対策の概要等
(5) 顧客の利用環境（利用可能な機種やブラウザ等）
顧客の利用環境を周知する場合には、以下の内容を Web サイトに掲載、またはインターネット利用取引の開始案内で利用者に通知する。
①OS（必須パッチが含まれる場合はその内容を含む）
②ブラウザとその設定
③必要となるプラグイン
④専用ソフトがある場合はそのバージョン 等

口座が不正に利用されることを防止するため顧客に注意喚起すべき事項としては、以下の例がある。

(1) ID やパスワード、乱数表、トークンといった本人確認用の情報や媒体を他人に渡さないこと
(2) 推測されやすいパスワードを使用しないこと
(3) パスワードを他のパスワードと共用しないこと
(4) 不特定多数の者が使用するパソコンでは金融機関等との取引を行わないこと（スパイウェアによりパスワード等が盗まれる危険性がある）
(5) 警察官や金融機関等の職員がパスワードを直接顧客に照会することはないこと（警察官や金融機関等の職員を詐称し、パスワードを聞きだす犯罪行為があること）
(6) パスワードは定期的に変更することが望ましいこと
(7) パスワードをメモ等に残した場合のリスクを認識すること（紙に書いた場合やパソコンやスマートデバイスにファイルで保管した場合には盗難のリスクがある）
(8) 使用するパソコンやスマートデバイス等への市販または金融機関等が配布する抗ウイルスソフトやセキュリティパッチ等の適用と、その最新化を行うこと

会員意見募集版

(9) 基本ソフト（OS）やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新すること
(10) 金融機関等の正当なサイトであることの確認手段（不用意に ID・パスワード等の本人確認用情報を入力すると、フィッシング等の詐欺を目的とした偽サイトに入力している場合がある）
(11) 金融機関等からの正当な電子メールであることの確認手段
(12) （金融機関等が利用者向けアプリケーションを提供している場合）アプリケーションが正式なものであることの確認手段【実 20】
(13) 不審な CD-ROM 等の受領時は、金融機関等の公式ホームページ等で確認すること
(14) 使用するパソコンを廃棄する際には、ツールの使用等によりハードディスク内のデータを完全に消去すること
(15) 金融機関等が乱数表の全内容の入力を求めることはないこと
(16) ワンタイムパスワードの利用を推奨すること
(17) 可能であれば、インターネットバンキングへのログイン等に使用するパソコンの利用目的を限定し、使用していないときには電源を切ること【実 15】。また、法人であれば取引の申請者と承認者とで異なるパソコンを利用することも有効であること。
(18) 取引明細や取引通知メール等から、身に覚えのない取引がないか確認すること
(19) 電子証明書は、金融機関等が指定した正規の手順以外では利用しないこと
(20) （顧客ごとに振込等の限度額の設定が可能な場合）限度額については取引上の必要性に応じてできるだけ低く設定すること【実 11】

顧客への周知の方法としては、以下の例がある。
(1) 口座開設時における説明及びパンフレット等への明記
(2) 電話による通知
(3) ホームページへの掲載
(4) 電子メールによる通知

2. 顧客への注意喚起をホームページに掲載する際は、改ざん防止策を実施することが必要である。また、電子メールによる通知時にはそれ自体が情報の漏洩につながらないように、文面には注意するとともに、なりすまし防止、改ざん防止策を実施することが必要である。

3. 不正使用の早期発見のため、定期的に残高及び取引履歴を確認するよう顧客に推奨することが望ましい。

4. 顧客からの問合せ、相談及び届出に対応する窓口を整備することが必要である。また、届出を受け付けた場合は定められた方法により対応することが必要である。
顧客からの届出を速やかに受け付ける体制の整備が必要な時間帯としては、インターネットバンキングにおけるサービスの場合、例えば振込が可能な時間帯及びその前の一定の時間帯とすること等が考えられる。

顧客からの問合せ、届出としては、以下の例がある。
(1) サービス内容や規約に関する照会
(2) 操作方法の照会

会員意見募集版

(3) 取引に用いる携帯電話や IC カード等の紛失による利用停止等の届出
(4) 口座残高や取引履歴に疑義が生じた場合の利用停止等の届出
(5) フィッシングメールや偽サイト（フィッシングサイト）に関する通報
(6) 不正取引の届出
(7) インターネットバンキング利用中に、利用マニュアル等に記載されているものとは異なる画面が表示された場合の照会

5. 被害の拡大防止のため、犯罪が発生した際の対応方針を定めておくことが必要である。

犯罪が発生した際の対応方針の具体的な内容としては、以下の例がある。
(1) 被害に遭った口座のインターネット取引を停止する。
(2) スパイウェアやフィッシングなどにより不正取引が発生した場合には、ホームページ上の公表に加え、個別メールによる周知を行う。
また、犯罪手口についても可能な限り公表する。
なお、公表・周知の時間帯としては、個人顧客は夕刻以降にアクセスすることが多いなど、顧客の利用傾向も踏まえ、多くの顧客が利用開始する時間帯までに可能な限り公表・周知を行う。
(3) フィッシングにより不正取引が発生した場合には、当該フィッシングサイトの閉鎖等の対応を行う。なお、閉鎖に際しては専門機関との連携やフィッシングサイト閉鎖サービス事業者の利用も有効である。
(4) 原因究明・捜査協力のため、被害に遭った顧客が特定できる場合には、当該顧客に対して使用したパソコン等の現状を保全し、警察に連絡するよう要請する。

（参考 1）
コンピュータウイルス等の不正プログラム対策やフィッシング対策等、利用者に周知すべき事項に関する情報を公開している公的な Web サイトを以下に示す。

独立行政法人情報処理推進機構（IPA）セキュリティセンター
http://www.ipa.go.jp/security/index.html

警察庁サイバー犯罪対策
http://www.npa.go.jp/cyber/

警察庁セキュリティポータルサイト@police
http://www.cyberpolice.go.jp/

フィッシング対策協議会
https://www.antiphishing.jp/

（参考 2）
フィッシングサイト閉鎖の協力を行う専門機関
一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
http://www.jpcert.or.jp/form/

会員意見募集版 金融庁

9 個別業務・サービス
(2) インターネット・モバイルサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

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。

インターネット・モバイルサービスにおいて、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にすること。

1. インターネット・モバイルサービスにおいては、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にすることが必要である。

不正な取引を防止する対策としては、以下の例がある。

(1) 伝送データの漏洩防止策 【実 4】
(2) 本人確認機能 【実 8】
　①認証機関が発行する電子的な証明書等による認証（【実 8】参考 1 項番 6）
　②取引の重要度に応じた、ログインパスワードとは異なるパスワード設定
　③パスワードの入力失敗回数の制限と監視
　④パスワード再発行時の本人確認の厳格化（リマインダー機能において回答が推測できる質問を提供しない　等）
(3) アクセス履歴の管理 【実 10】
(4) 取引制限機能 【実 11】
　①顧客より資金移動先や限度額の登録を受け、取引を制限する
(5) 事故時の取引禁止機能 【実 12】
(6) 暗号鍵の保護機能 【実 13】
(7) 不正侵入防止機能 【実 14】
(8) 不正アクセス監視機能 【実 16】
(9) 異常な取引状況の把握機能 【実 17】
　①取引履歴や取引結果を利用者自身が確認可能とする
(10) 異例取引監視機能 【実 18】
(11) 不正アクセス時の復旧策 【実 19】
(12) DNS サーバーの登録状況の管理
　①TLD（Top Level Domain）レジストリへの登録情報が正しいこと
　②ドメイン名の設定情報が正しいこと

顧客の誤操作や誤認を防止する対策としては、以下の例がある。

(1) リンク等による利用者の誤認・混同防止策
(2) 取引確定前に確認のための画面を表示する等の操作支援機能

会員意見募集版

サービスの信頼性を向上させる対策としては、以下の例がある。

(1) 予想される取引量に対するインターネットサービス・プロバイダーとの間の十分な回線容量の確保や予備の設置 【実 47】【実 87】

(2) 予想される取引量に対し十分な性能を持つサーバーの導入や予備サーバーの設置【実 84～86】

(3) システムの負荷状態の監視、制御やトラフィック制御機能の設定 【実 101】

2. 障害時・災害時対応手順を明確にすることが必要である。【実 71】

参照法令	金融商品の販売等に関する法律、消費者契約法

会員意見募集版

9 個別業務・サービス
(2) インターネット・モバイルサービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎		◎	

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。

不正取引防止のため、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適切な方法により本人確認を行うこと。

1. 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不正取引防止のために、以下の手順等により本人を確認することが必要である。
   (1) 公的証明書の原本またはコピーの送付を受ける。
   (2) 顧客の住居に取引関連書類（キャッシュカード等）を書留郵便等で返送する。

2. 利用者からの暗証番号等の照会において、対面・非対面にかかわらず、十分な本人確認ができない場合には、直ちに回答するのではなく、別途、登録されている顧客情報をもとに、金融機関等から電話連絡や書留郵便等の手段で本人であることを確認したうえで、回答する必要がある。

   不正取引を防止する策については【実 112】を参照のこと。

参照法令	犯罪による収益の移転防止に関する法律 （旧 金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律）

会員意見募集版

9 個別業務・サービス
(3) 渉外端末の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎			

実　118	渉外端末の運用管理方法を明確にすること。

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。

1. 渉外端末の運用管理方法を明確にすることが必要である。

   ここでいう渉外端末とは、ハンディ端末、スマートデバイス、携帯型パソコン等の可搬型端末を指している。

2. 渉外端末には各々識別 ID を付与し、その取扱者を明確にする必要がある。

3. 渉外端末は可搬型の端末であるため、定められた場所に保管し、その保管方法を明確にする必要がある。　【実 49】

4. 盗難、紛失等を早期に発見するため、渉外端末の管理者を明確にし、定期的に台数の確認をする必要がある。また、盗難、紛失等の届出・受付体制を整備する必要がある。　【統 4】

5. 渉外端末が使用不可能になった場合に備え、取引の記録またはデータファイルのバックアップを取得する必要がある。

   バックアップの方法としては、以下の例がある。
   (1) ジャーナル（明細票等）の保管
   (2) 記録媒体によるバックアップの取得

6. 渉外端末の盗難、紛失等が発生した場合に備え、データ保護のための対策を講じておく必要がある。

   データ保護のための対策としては、以下の例がある。
   (1) 起動時に識別コード、パスワード等の入力、または特殊操作による起動等により不正アクセスを防止する。
   (2) 端末内または着脱可能な記録媒体にあるデータファイルは、その重要度に応じて暗号化またはデータファイルへのパスワード設定など、適切な漏洩防止策を講ずる。【実 3】
   (3) データファイルを端末に保存する際は、その重要度に応じた保管・管理方法を明確にする。【実 28】

7. データ漏洩、不正アクセス、コンピュータウイルスの侵入等を防止するため、社内ネットワ

会員意見募集版

ークへの接続及びリモートアクセスの利用は、定められた方法によって行うことが必要である。

(1) 外部接続の運用管理については【実 34】を参照のこと。

(2) ウイルス対策については【実 32】を参照のこと。

8. 使用しない機能は停止、もしくは使用を制限するとともに、使用しないソフトウェアを搭載しない等、セキュリティを考慮した設定とする必要がある。
端末機器操作の権限管理については【実 61】を参照のこと。

9. 渉外端末の廃棄方法を明確にする必要がある。 【実 48】

（参考）

1. スマートデバイスの業務利用に関わる考慮点

スマートデバイスは、業務利用で必要となるセキュリティ機能を実装することが困難な場合がある。また、パソコンと異なる「機器の特性」、「アプリケーションの特性」、「ネットワークの特性」を理解して以下の点を考慮することが求められる。

(1) 端末へのデータ保存

導入しているアプリケーションのデータ保存の仕組みを理解し、情報漏洩の原因とならないよう考慮する。例えば、利用者がインターネット上のサービス等を利用する場合、端末データがサービス等に同期されることで、外部環境にもデータが保存され、情報が漏洩するリスクがある。

(2) MDM（Mobile Device Management）の導入

スマートデバイスを制御する仕組みとして、MDM があり、デバイスの利用制限、アプリケーションのインストール制限、端末の状態監視等の管理を行うことができる。このような MDM を導入する場合には、サービス機能が異なるため、提供される機能を調査し、自社の要件を満たす最適な製品を選択する。

(3) 紛失・盗難対策

紛失や盗難時に MDM 等の機能を利用した遠隔操作によるデータ消去の対策はあるが、通信圏外や SIM カードが抜き取られた場合には、遠隔操作でデータ消去はできないことを考慮した運用が求められる。

(4) 機種または OS の選択

スマートデバイスは機種や OS の種類が様々にあり、システムやセキュリティに関わる仕様も一様ではないため、会社（もしくは組織）のセキュリティポリシーに基づき、最適な機種・OS を選択することが求められる。例えば、パソコンと異なり脆弱性に対するセキュリティパッチの適用の遅れも発生しており、セキュリティパッチの適用等が十分な機種を選択することが考えられる。

(5) 通信機能の利用

スマートデバイスは通信機能を備えており、企業内無線 LAN、携帯電話回線網、または公衆無線 LAN 等の複数の経路で社内ネットワークへアクセス可能であり、不正認証（なりすまし）、盗聴、情報漏洩といったセキュリティ上の脅威に対して、経路別に様々な対処（無線 LAN 使用時に利用可能なアクセスポイントを制限する等）の考慮が求められる。（【実 4】【実 8】【実 14】参照）

会員意見募集版

(6) 抗ウイルスソフト

抗ウイルスソフトは、コンピュータウイルス等不正プログラムの防御対策として一定程度有効であるが、アプリケーションの一種として動作をしており、管理者権限を持たないため、システム領域における対策は困難であり、パソコン用の抗ウイルスソフトと同等の効果は期待できないことを理解した運用が求められる。

2. スマートデバイス特有のセキュリティに関わる留意点

自社のセキュリティポリシーに基づいて、利用する業務や保持するデータの重要性に応じて、会社（もしくは組織）として必要なセキュリティ対策を講じることが求められる。

(1) テザリング

スマートデバイスの一部には、スマートデバイスを無線ネットワークのルータとして利用し、パソコン等をインターネットに接続させるテザリングという機能を有する機器がある。社内ネットワークへの接続を承認されたスマートデバイスのテザリング機能を有効とした場合、未承認のパソコン等が社内ネットワークに接続されるリスクがある。

(2) 管理者権限の不正取得（特権解除）

通常、スマートデバイスの利用者は管理者権限を有しないが、OS の脆弱性を突くなどの方法で、管理者権限を不正に取得することを特権解除という。これが行われた機器は、コンピュータウイルスの侵入、端末 ID やユーザーID 等の認証子が盗難・改ざんされる等のリスクが増大する。

(3) アプリケーションの Web サイトからの導入

スマートデバイスへのアプリケーション等の導入は、パソコンと異なり Web サイトから行われることが多い。Web サイトからアプリケーションを導入する場合、アプリケーションの安全性が審査されていないケースがあるため、コンピュータウイルスに感染するリスクがある。【実 20】（参考 1）「コンピュータウイルス対策の例」を参照し、対応することが求められる。

(4) 組込み機能に対する制御

スマートデバイスには、カメラ、GPS 等の組込みの機能がある。これら機能の使用により、利用者の意図しない操作・動作による情報漏洩のリスクがある。

3. スマートデバイスのセキュリティ対策や利用者に周知すべき情報を公開しているガイドラインを以下に示す。

・「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン【第二版】」（2014 年 4 月）

http://www.jssec.org/activities/index.html

一般社団法人 日本スマートフォンセキュリティ協会

なお、スマートデバイスの業務利用の１つの形態として、個人所有の端末機器を業務に利用する「BYOD（Bring Your Own Device）」がある。ただし、BYOD が原因で情報漏洩が生じる可能性もあるので、個人所有の端末を業務で利用する場合は、十分な検討が求められる。

会員意見募集版

9 個別業務・サービス
(4) CD・ATM 等及び無人店舗の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎	◎		

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。

CD・ATM 等及び無人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。

1. CD・ATM 等は設置場所、所有者、運用方法、稼働時間等によりさまざまな運用形態が考えられるため、それぞれの運用形態に合わせた運用管理方法を定めることが必要である。

   具体的項目としては、以下の例がある。
   (1) 現金の装填手順
   (2) CD・ATM 等の操作記録の保存（保存期間を定めておく）
   (3) 故障時の対応方法
   (4) 防犯監視体制
   　防犯監視体制については【設 113】【設 137】【実 121】を参照のこと。

2. 店舗外 CD・ATM 等については、母店等における運用管理方法を定めることが必要である。

3. 無人店舗では、運用管理方法を定めるとともに、関係者に周知徹底することが必要である。

   考慮する事項としては、以下の例がある。
   (1) 現金切れを極力少なくするために、適正量の現金を装填する。
   (2) ジャーナル等、CD・ATM 等で必要とする用紙等についても十分に装填する。
   (3) 現金切れ、機械故障等に備え、無人店舗における機械設置は複数台とする。
   (4) 現金切れ、機械故障等に備え、近隣無人店舗の地図をコーナーに掲示する。

4. 犯罪に対しては、防犯カメラ及び防犯ビデオが抑止策となるとともに、犯罪解決には有効な手段であるため、その運用、管理方法を明確にし実施することが必要である。【設 103】
   なお、ビデオとジャーナルの時刻の不一致度合いを極力少なくするため、定期的に時刻合わせを実施するとともに、テープ・ディスク等の記録媒体の交換及びレンズの清掃を実施することが望ましい。
   また、犯罪解決及び同様の被害防止の観点から、犯罪手口の特定化のために防犯カメラ、防犯ビデオ及び CD･ATM ジャーナル等の提供など、積極的な捜査協力が必要である。加えて、捜査依頼に対して迅速かつ適切に協力する観点から、あらかじめ捜査協力に関する手順等を定め、従業者に教育・周知しておくことが必要である。

会員意見募集版

（参考）
捜査協力時の個人データ提供についての根拠は
・令状による捜査に協力する場合：個人情報の保護に関する法律　第 16 条第 3 項第 1 号、第 23 条第 1 号
・任意捜査に協力する場合：個人情報の保護に関する法律　第 16 条第 3 項第 4 号、第 23 条第 4 号を参照のこと（個人情報の目的外利用の制限の除外事項として、規定あり）

防犯カメラ、防犯ビデオ及び CD･ATM ジャーナルの運用、管理に関して明確にする項目としては、以下の例がある。
(1) CD･ATM ジャーナル及びテープ・ディスク等の保存期間及び保存場所
(2) 責任者
(3) 運用方法

防犯カメラ及び防犯ビデオに関する運用実施策としては、以下の例がある。
(1) 金融機関等による運用及び管理
(2) 警備会社等の外部委託を利用した運用及び管理
また、コンビニ ATM の防犯カメラ及び防犯ビデオは、コンビニエンスストアで運用及び管理を行う場合もある。

5. ハードディスク等を使用して防犯ビデオを集中管理する場合は、捜査協力を想定してダビングの容易性についても考慮することが必要である。

6. 防犯ビデオは一定期間の保存を考慮することが望ましい。例えば警察庁の「金融機関の防犯基準」においては「少なくとも、3 月を下回るような短期間の保存は避けること」の記述がある。

7. ATM 利用明細書から、口座番号を他人に知られないための対策を講ずる必要がある。

具体的な対策としては、以下の例がある。
(1) ATM 利用明細書の口座番号等の一部あるいはすべてを非表示とする。
(2) 照会等の一部取引において ATM 利用明細書を出力しない。
(3) ATM 利用明細書を持ち帰るように注意喚起する。
(4) ゴミ箱を設置する場合は、鍵やシュレッダー付のものを選択する。
(5) コンビニ ATM に設置したゴミ箱に捨てられた ATM 利用明細書の扱いについては、関係者間で取り決める。

会員意見募集版

＜会員意見募集版＞

9 個別業務・サービス
(4) CD・ATM 等及び無人店舗の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎			

実　120	無人店舗の監視体制を明確にすること。

無人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。

1. 無人店舗における異常状態を発見するため、管理センター等で監視することが望ましい。

   管理センター等における対応内容としては、以下の例がある。
   (1) CD・ATM 等の障害、破壊等のオンライン監視
   (2) 直通電話による顧客の操作誘導
   (3) 警備会社への必要な対応依頼（障害時顧客対応、犯罪発生時対応等）
   (4) 犯罪発生時の警察への通報
   (5) 障害・災害発生時における母店等関係者への連絡

2. 管理センター等を設置できない場合、並びに管理センターにおける監視では不十分と考えられる場合には、代替策として警備会社による定期的巡回等の方法が考えられる。
   巡回にあたっては、巡回時間を特定されないよう配慮することが必要である。また、設置場所等の環境に応じて、巡回・点検頻度を上げることが望ましい。

3. 最低限の措置として顧客が連絡を取れる先を店舗内に表示するとともに、顧客からの連絡を受ける責任者を定めておき、連絡が必ず取れるようにすることが必要である。

会員意見募集版

9 個別業務・サービス
(4) CD・ATM 等及び無人店舗の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎			

実　121	無人店舗の防犯体制を明確にすること。

無人店舗における犯罪を防止するため、防犯方法及び犯罪発生時の対応方法を明確にすること。

1. 無人店舗では、CD・ATM 等の破壊による現金盗難、隠しカメラ設置による暗証番号盗撮等の犯罪が行われる可能性が高くなるため、周辺地域の犯罪発生状況を把握することに努め、事前に防犯方法及び発生時の対応方法を明確に定めておくことが必要である。

   防犯方法としては、以下の例がある。
   (1) 契約された警備会社による巡回
   (2) 警察にあらかじめ依頼することによる警察官の巡回
   (3) 防犯カメラによる監視 【設 103】
   なお、巡回時に CD・ATM 機、その周囲及び出入口付近に隠しカメラ、カード情報の不正な読取装置等の不審な装置がないか確認する。また、ゴミ箱が荒らされていないか確認することも対策として有効である。

   犯罪発生時の対応としては、以下の例がある。
   (1) 警報装置による警報鳴動（自動鳴動、遠隔監視による鳴動指示等が考えられる）
   (2) 警備会社、警察等への管理センター等からの連絡
   (3) 警備員等の迅速な駆けつけ
   (4) 防犯ビデオへの犯人像の記録 【設 103】

2. 現金装填を行う場合には必ず複数名により行うことが必要である。
   また、職員が行う場合には警備会社等に立会いを依頼することも有効である。
   現金装填は直接現金が人目に触れない方式とし、短時間でできるようにすることが必要である。
   CD・ATM 等は後面装填型が望ましいが、前面装填型 CD・ATM 等の現金装填については、装填者の背後が無防備になるため、特に配慮が必要である。

会員意見募集版

9 個別業務・サービス
(4) CD・ATM 等及び無人店舗の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎			

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。

無人店舗の円滑な運営のため、障害時・災害時の対応方法を明確にすること。

1. 無人店舗における障害時の対応方法を明確にすることが必要である。

   具体的に検討、整理する項目としては、以下の例がある。
   (1) 利用客への状況連絡方法、説明方法
   (2) 利用客へのカード等の返却方法
   　　自動返却、職員、警備会社等による個別手作業返却が考えられる。
   (3) 特定店に障害が限定されている場合における他店への誘導
   (4) 自社ホストに係わる障害でない場合に最寄の CD・ATM 等への誘導
   (5) 回復後のサービス時間延長への対応
   (6) 関係者（営業店、本部、コンピュータセンター、警備会社等）の招集方法及び役割

2. 災害時における対応方法についても、障害時の対応方法を参考にして検討、整理することが必要である。

会員意見募集版

9 個別業務・サービス
(4) CD・ATM 等及び無人店舗の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎			

実　123	無人店舗の関係マニュアルの整備を行うこと。

無人店舗の円滑な運営、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すること。

1. 無人店舗における各種対応を想定した関係マニュアルを整備することが必要である。

   関係マニュアルとしては、以下の例がある。
   (1) 管理センター等における監視対応マニュアル
   (2) 防犯マニュアル
   (3) 障害時対応マニュアル
   (4) 災害時対応マニュアル
   (5) 母店における店舗外 CD・ATM 等管理マニュアル
   (6) 警備会社、警察等との連絡方法マニュアル
   (7) 現金、ジャーナル等の装填マニュアル

2. マニュアルは本部、コンピュータセンター、管理センター、営業店、警備会社等にそれぞれ必要なものを作成し、最新版を常備することが必要である。

会員意見募集版

9 個別業務・サービス
(4) CD・ATM 等及び無人店舗の管理

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
	◎	◎	◎		

実　124	CD・ATM 等の遠隔制御機能を設けること。

無人店舗における CD・ATM 等の安定運用のため、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。

1. 無人店舗における CD・ATM 等の安定運用のため、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が必要である。

2. 無人店舗の CD・ATM 等の運用状況を集中監視する場合、設備基準に加え、技術面にも考慮した安全対策を行う必要がある。【設 111～設 117】

   技術面に考慮した安全対策としては、以下の例がある。
   (1) 異常状態（現金切れ、ジャム、機器異常、回線断等）の検知機能を設ける。
   (2) 現金、ジャーナル等のニアエンドを検知して、適切な処置を行う。
   (3) 装置等の稼働状況を検知（エラー等の集計）し、適切な予防保守を行う。

会員意見募集版

9 個別業務・サービス
(5) インストアブランチ

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
		◎			

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。

インストアブランチの安全性を確保するため、出店先地域及びストアの選定基準を明確にすること。

1. インストアブランチは、開放的なレイアウト及び少人数の運営等、従来の本部・営業店等の運営と異なる点がある。インストアブランチの安全性を確保するため、出店先地域及びストアの選定基準を明確にすることが必要である。

   明確にする選定基準としては、以下の例がある。
   (1) ストアの経営体質、警備方針
   (2) 出店先地域における過去の犯罪発生履歴等

2. インストアブランチの出店にあたっては、出店先の設備状況についても考慮する必要がある。出店先の設備状況の考慮点については【設 136】を参照のこと。

3. インストアブランチでは、出店先の設備状況及びインストアブランチの要員体制に応じた安全対策が必要である。

   インストアブランチの安全対策としては、以下の例がある。
   (1) 防犯カメラ及び防犯ビデオ 【設 103】【設 113】
   (2) 警察、警備会社のステッカー
   (3) 警察官の立ち寄り
   (4) 警備員の巡回
   (5) 非常押ボタンの設置、非常押ボタンの携帯 【設 113】

会員意見募集版

9 個別業務・サービス
(6) コンビニ ATM

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

実　126	コンビニ ATM の出店先の選定基準を明確にすること。

コンビニ ATM 及び利用者の安全性を確保するため、出店先地域及びコンビニエンスストアの選定基準を明確にすること。

1. コンビニ ATM 及び利用者の安全性を確保するため、出店先地域及びコンビニエンスストアの選定基準を明確にすることが必要である。

   明確にする選定基準としては、以下の例がある。
   (1) コンビニエンスストアの経営体質、警備方針
   (2) 出店先地域における過去の犯罪発生履歴等

2. コンビニ ATM の出店にあたっては、出店先の設備状況についても考慮する必要がある。

3. コンビニ ATM では、出店先の設備状況及びコンビニエンスストアの店員に対する安全対策が必要である。

   コンビニ ATM 及び利用者の安全対策としては、以下の例がある。
   (1) 防犯カメラ及び防犯ビデオ 【設 103】【設 137】
   (2) 警察、警備会社のステッカー
   (3) 警察官の立ち寄り
   (4) 警備員の巡回
   (5) 駐車場の照明
   (6) 非常押ボタンの設置、非常押ボタンの携帯 【設 137】

会員意見募集版

＜会員意見募集版＞

9 個別業務・サービス
(6) コンビニ ATM

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

コンビニ ATM のメンテナンス時の安全性を確保するため、防犯体制及び防犯方法を明確にすること。

1. コンビニ ATM は開放的な場所に設置されるため、現金装填等メンテナンス時の防犯体制及び防犯方法を明確にすることが必要である。

   現金装填等メンテナンス時の防犯対策としては、以下の例がある。
   (1) 犯罪が発生しやすい深夜等の装填は行わない。
   (2) 現金装填は直接現金が人目に触れない方式とし、短時間で実施できるようにする。
   (3) 現金装填は警備会社等防犯の専門家に委託する。
   (4) 本体扉の内側に非常通報装置等を設置する。

2. コンビニ ATM の鍵をコンビニエンスストアに置くことは店員が犯罪に巻きこまれる可能性が高くなる。このため、コンビニエンスストアではコンビニ ATM の鍵を管理せず、警備会社または金融機関等の専門家が管理することが望ましい。

3. カード情報の不正な読取装置等の設置を防ぐなどの防犯上の観点から、巡回時等にコンビニ ATM 等の周囲に不審な装置がないか確認することが必要である。また、最新の犯罪状況等を踏まえ、カード情報の不正な読取装置などに関する情報を巡回者に適宜教育・周知することが必要である。

会員意見募集版

9 個別業務・サービス
(6) コンビニ ATM

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

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。

1. コンビニ ATM の障害時・災害時の対応手順を明確にすることが必要である。

   コンビニ ATM の障害時の対応項目としては、以下の例がある。
   (1) 顧客への状況連絡方法、説明方法
   (2) 顧客へのカード等の返却方法
   　自動返却、警備会社等による個別手作業返却が考えられる。
   (3) 特定店に障害が限定されている場合における他店への誘導
   (4) 自社ホストに係わる障害でない場合に最寄の CD･ATM への誘導
   (5) 回復後のサービス時間延長への対応
   (6) 関係者（営業店、本部、コンピュータセンター、警備会社等）の招集方法及び役割
   (7) コンビニ ATM の電源設備等の障害対策状況の確認とその対策
   (8) コンビニ ATM の回線設備等の状況の確認とその対策

2. 災害時における対応方法についても、障害時の対応手順を参考にして検討、整理することが必要である。

会員意見募集版

9 個別業務・サービス
(6) コンビニ ATM

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

伝送データの安全性及び信頼性を確保し、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及び伝送データの安全対策を講ずること。

1. コンビニ ATM のネットワーク関連機器は、適切な保護措置を講ずることが必要である。【実 50】

2. 伝送データの安全対策を講ずることが必要である。回線は、コンビニエンスストア等の回線とは別の回線であることが望ましい。

   伝送データの安全対策としては、以下の例がある。
   (1) 伝送データの重要性に応じた適切な漏洩防止策 【実 4】
   (2) 伝送データの不正な破壊、改ざん等を早期に発見するための適切な検知策 【実 7】

会員意見募集版

9 個別業務・サービス
(6) コンビニ ATM

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

犯罪発生時に関係者へ迅速に連絡を行うため、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の確立及び訓練を行うこと。

1. 犯罪発生時にコンビニ ATM の所轄の警察及び警備会社等への迅速に連絡できる体制の確立及び訓練を行うことが必要である。

   迅速で簡素化された連絡体制の確立及び訓練としては、以下の例がある。
   (1) 店舗警備と連動した一括した管理
   (2) 非常押ボタンが押下されたときの運用の明確化及び訓練
   (3) 運用マニュアルの常備
   (4) 店員に対する教育及び訓練

   迅速な連絡を行うための装置としては、以下の例がある。
   (1) 非常押ボタン
   (2) リモート監視装置

2. 出店時及び日頃から所轄の警察等に認識してもらうとともに連絡を取ることが望ましい。

3. 犯罪抑止策として、出入口等に警察、警備会社等のステッカーを貼ることが望ましい。
   例えば、警官立ち寄り所、警備会社等のステッカー等がある。

会員意見募集版

9 個別業務・サービス
(6) コンビニ ATM

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

コンビニ ATM における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。

1. コンビニ ATM においては、犯罪に関する注意喚起を行うことが必要である。

   内容については【実 108】を参照のこと。

会員意見募集版

9 個別業務・サービス
(7) デビットカード・サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

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、加盟店等と共に安全対策を講ずること。

1. 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、加盟店等と共に総合的な安全対策を講ずることが必要である。

サービスの提供形態に応じて検討する安全対策としては、以下の例がある。

(1) 顧客データの適切な保護 【実 69】
　口座番号等のカード情報が記載された印刷物の適切な管理
(2) 顧客への注意喚起 【実 135】
(3) 口座番号、暗証番号等の安全性の確保 【実 133】
(4) デビットカードの不正使用の防止策
　①加盟店の店員によるカード券面の確認による不正なカードの検知 【実 111】
　②カードの不正使用取引の検知 【実 17】
(5) デビットカードをデビットカード端末で読み取る際の安全対策上の配慮
　①加盟店の店員による顧客の目の届く範囲内でのカードの読取り
　②顧客本人によるカードの読取り
(6) 犯罪抑止並びに犯罪者を特定しやすくする措置
　①適切な利用限度額の設定等 【実 134】
　②加盟店への防犯カメラ等の設置 【設 103】
　③デビットカード端末が正当な加盟店に設置されていること
(7) セキュリティ管理と責任の明確化 【統 4～統 8】
(8) セキュリティ教育の実施 【統 14】

会員意見募集版

9 個別業務・サービス
(7) デビットカード・サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

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、加盟店等と共に安全対策を講ずること。

1. 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、加盟店等と共に総合的な安全対策を講ずることが必要である。

口座番号等の安全性の確保としては、以下の例がある。

(1) デビットカード端末からの盗難防止策
　①端末の耐タンパー性による保護
　②カード情報の暗号化による保護
(2) 伝送データからの漏洩防止策 【実 4】
(3) 利用明細書等からの口座情報等の漏洩防止策
　①利用明細書への口座番号等のカード情報を一部あるいはすべて非印字
　②端末への口座番号等のカード情報を一部あるいはすべて非表示
(4) デビットカードの偽造防止策 【実 111】

暗証番号の安全性の確保としては、以下の例がある。

(1) デビットカード端末からの盗難防止策
　①端末の耐タンパー性による保護
　②カード情報の暗号化による保護
(2) 伝送データからの漏洩防止策 【実 4】
(3) 蓄積データからの漏洩防止策 【実 3】
(4) 暗証番号の盗み見防止策
　①暗証番号入力用のキーパッドへのかざしの設置
　②暗証番号を入力する場所のパーティション等の設置
　③加盟店に防犯カメラ等を設置する場合は、暗証番号を入力する際の顧客の手元が映らないような配置の工夫
(5) 他人に推測されにくい暗証番号の使用 【実 26】
(6) 顧客本人による暗証番号の変更 【実 107、実 134】
(7) 顧客への注意喚起 【実 26、実 108】

会員意見募集版

＜会員意見募集版＞

9 個別業務・サービス
(7) デビットカード・サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

デビットカード利用時の安全性を確保するため、顧客保護の措置を講ずること。

1. 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に、顧客保護の措置を講ずることが必要である。

   デビットカード利用における顧客保護の措置としては、以下の例がある。

   (1) 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。【実 135】

   (2) 1 日当たりの利用限度額等を設ける。

   ①利用限度額を一律に設定する。

   ②利用限度額を顧客本人が選択、変更可能とする。

   (3) デビットカードとして利用する要否を顧客本人が選択、変更可能とする。

   (4) デビットカードの紛失、盗難、偽造等により発生した顧客の損失を補償するための適切な対策を講ずる。

   (5) CD･ATM 等により顧客本人が暗証番号を変更可能とする。【実 107】

会員意見募集版

9 個別業務・サービス
(7) デビットカード・サービス

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
			◎		

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。

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。

1. 顧客に対して、デビットカードのサービス内容及び取扱い上の留意事項をわかり易く明示することが必要である。

   デビットカードのサービス内容及び留意事項の顧客への周知方法としては、以下の例がある。
   (1) 取引規定への記載
   (2) カードの裏面等への記載
   (3) デビットカードや CD・ATM 等の利用明細書への記載
   (4) DM への記載
   (5) 店頭や自動機器コーナーのポスターへの記載
   (6) 金融機関等のホームページへの記載
   (7) 新聞広告等

   周知する留意事項としては、以下の例がある。
   (1) デビットカードとして利用できるカードの種類と特徴
   (2) デビットカードのサービス利用可能時間帯
   (3) 暗証番号を他人に知られないようにすること 【実 26】
   (4) 本人が暗証番号をデビットカード端末に入力すること
   (5) 利用明細書を持ち帰るようにすること
   (6) 通帳記帳時等の日付、利用金額、残高の確認
   (7) デビットカード利用口座の限定等
   (8) 暗証番号の変更方法 【実 107、実 134】
   (9) 利用限度額等の利用条件並びに変更届けの有無及び届出方法
   (10) デビットカードの利用停止届けの有無及び届出方法
   (11) 紛失、盗難、破損時の届出方法
   (12) 紛失、盗難、偽造等により発生した損害に対する責任や補償

会員意見募集版

9 個別業務・サービス
(8) 前払式支払手段

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

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、及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、及び利用者側の責任についてもわかり易く明示すること。

1. 電子的価値を蓄積する媒体等の紛失、盗難、破損に関し、利用者が被る可能性のある損失及び責任を利用者に対して明示することが必要である。

   明示する場所としては、以下の例がある。
   (1) 契約時の取引規定
   (2) 電子的価値を蓄積する媒体の裏面

   明示する項目としては、以下の例がある。
   (1) 電子的価値の保証について
   (2) 紛失、盗難、破損時の届出について
   (3) 盗難にあった媒体・機器により発生した損害に対する責任について

会員意見募集版

9 個別業務・サービス
(8) 前払式支払手段

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

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設けること。

1. 電子的価値を蓄積する機器、媒体あるいはそれに含まれるソフトウェアには、価値を保護する機能を設けることが望ましい。

2. 上記の機能がない場合には、改ざん、不正コピーによる二重使用等の不正行為を検出できる仕組みを設けることが望ましい。

3. セキュリティ確保のためには、複数の手段を組み合わせて総合的に対応する必要がある。
なお、セキュリティ技術は最新の技術の動向に留意し、その安定性、互換性、実装の容易さなどを適切に評価したうえで採用することが必要である。

セキュリティ確保のための手段としては、以下の例がある。
(1) IC カード型電子マネーにおける耐タンパー性を向上させる保護機能
(2) IC カード等には有効期限を設定するなどの偽造抑止対策
(3) シリアルナンバー方式による不正検知
(4) 証拠センター方式による不正検知

（注）・耐タンパー性　　：ソフトウェアやハードウェアの内部構造や記憶しているデータなどの解析の困難な状態。
・シリアルナンバー方式：電子的価値の使用単位ごとに固有の識別番号を付与し、同一番号のものが二重に使用されないようにチェックする方式。
・証拠センター方式　　：付与された電子的価値の総額に対して、実際の使用額と残額とを突合して不正使用をチェックする方式。証拠センターにおいて使用額と残額とが突合されるため、事後的なチェックとなる。

会員意見募集版

9 個別業務・サービス
(9) 電子メール・イントラネットの利用

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
				◎	

実　138	電子メールの運用方針を明確にすること。

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。

1. 電子メールを利用し、利用者に対して取引通知、情報提供及び問合せ等のサービスを行う場合には、電子メールの危険性を考慮する必要がある。

   考慮する電子メールの危険性としては、以下の例がある。
   (1) 盗聴及びなりすましの可能性
   (2) 情報漏洩に利用される可能性
   (3) 送信先を間違い、誤った宛先に送信する可能性
   (4) コンピュータウイルスに感染する可能性
   (5) コンピュータウイルスに感染した添付ファイルを送信する可能性
   (6) 遅延及び紛失する可能性
   (7) 同一ネットワークを利用する他業務システムのレスポンスに影響を与える可能性
   (8) システム障害による業務中断の可能性

2. 電子メールの危険性を考慮し、電子メールの運用方針を明確にする必要がある。

   明確にする電子メールの運用方針としては、以下の例がある。
   (1) 不正アクセス防止のための方策 【実 8】【実 26】
   (2) 機密漏洩防止のための方策
   (3) コンピュータウイルスチェック 【実 20～22】
   (4) 添付ファイルの取扱い
   (5) 送受信容量の制限
   (6) なりすまし防止の方策
   フィッシング等によるなりすましを防止する方策としては、以下の例がある。
   ①電子署名を使用する。
   ②メール本文中には URL を記述しない。
   ③メールの形式は、HTML をできるだけ使用しない。

3. 取引通知、情報提供、問合せ等で電子メールを利用する場合は、その運用方針を明確にすることが必要である。

会員意見募集版

明確にする運用方針としては、以下の例がある。

(1) 取引データの保護策
(2) 取引等に必要な情報の保管
(3) メッセージ受領確認の方策
(4) 障害発生時における業務継続策
(5) 施設面における保護対策

なお、取引データ等の保護のため、電子メールには取引時の情報を記載せず、金融機関のホームページからの照会を案内するような文言とすることも考えられる。
また、登録アドレスへの電子メールの通知を確実なものとするため、登録アドレスの変更の際は、新旧登録アドレスに変更通知を出すことも有効である。通知する内容としては、変更受付日時、変更に心当たりがない場合の連絡先等がある。

4. 運用方針の管理を行う体制を明確にする必要がある。

会員意見募集版

9 個別業務・サービス
(10) 電子メール・イントラネットの利用

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

業務目的以外の電子メールの送受信、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。

1. 業務目的以外の電子メールの送受信、ホームページの閲覧等に対処するため、セキュリティポリシーと整合性がある不正使用防止対策を講ずることが望ましい。なお、個人データを扱う場合には、この措置は必要である。

   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としては、以下の例がある。

   (1) 電子メールの送受信
   　①業務に関係しない私的な情報の交換・連絡
   　②業務上適切な範囲を逸脱した電子メールの利用（不適切なメーリングリストやメールマガジンの利用等）
   　③公序良俗に反する情報の送信
   (2) ホームページの閲覧
   　①業務に関係しないホームページの閲覧
   　②ホームページへの業務上適切な範囲を逸脱したコメントの掲載（掲示板等への公序良俗に反するコメント掲載等）

   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の不正使用防止対策としては、以下の例がある。

   (1) 電子メールの送受信やホームページの閲覧が可能な利用者を適切な範囲に限定する。【実 25】
   (2) メールフィルタリング等を導入し、電子メールの内容を判断し、不適切な情報の送受信を防止する。また、不適切な電子メールを送受信した利用者に対して適切な措置を行う。
   (3) 社外に送信された電子メールを自動的に送信者の管理者等に転送する。
   (4) コンテンツフィルタリング等を導入し、ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防止する。また、不適切なホームページを閲覧した利用者に対して警告等の措置を行う。

2. 運用面においても、全役職員（外部要員を含む）に対するセキュリティ教育を行い、責任、義務、懲罰等について周知徹底を図ることが必要である。【統 14】

会員意見募集版

（参考）

メールフィルタリング：電子メールの内容を判断し、不適切な情報の送受信を防ぐ目的で利用されるソフトウェアであり、利用者が受信したくないメールアドレスを設定しスパムメールの着信を拒否できる機能も含めることがある。

コンテンツフィルタリング：ホームページのコンテンツの内容を判断し、不適切な情報の閲覧を防ぐ目的で利用されるソフトウェアであり、不適切なホームページを閲覧した利用者のアクセスログを取得する機能も含めることがある。

会員意見募集版

9 個別業務・サービス
(10) 生体認証

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

顧客データを保護し、適正に利用するため、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。

1. 生体認証情報を取り扱う各段階（取得、入力、利用、保存、消去）について、安全に管理するための手順を定めることが必要である。
   また、各段階において、取扱者は必要最小限に限定することが必要である。【実 69】

   ここでいう生体認証と生体認証情報とは、以下を指している。
   生体認証・・・
   　生体認証情報を、本人の同意に基づき用いて、本人確認手段として実施する機械による自動認証。
   生体認証情報・・・
   　機械による自動認証に用いられる身体的特徴の情報のうち、非公知の情報を、コンピュータ等で扱えるデータに変換したもの。
   　（ここで身体的特徴の情報は、「金融分野における個人情報保護に関するガイドライン」第 5 条の機微（センシティブ）情報に該当するもの。）
   　（注１）①生体認証情報の例としては、静脈・虹彩等がある。
   　②一方、公知な情報としては、一般的な顔写真等があげられる。（ただし、医療用に撮影された顔写真等は除く）
   　③行動的特徴（キーストローク、筆順、筆速、筆圧、声紋等）は、非公知であるとしても、身体的特徴の情報ではないため、本基準でいう生体認証情報には含まない。
   　（注２）一般的に、「個人の身体的特徴及び行動的特徴を識別情報とした本人確認技術」及び「身体的特徴及び行動的特徴の情報そのもの」を「バイオメトリクス」と呼ぶことがある。本項目においては、この概念から対象を上記のとおり絞って、「生体認証」及び「生体認証情報」という用語を用いる。

会員意見募集版

(1) 取得

①顧客の同意

事前に金融機関等は、顧客に対し、生体認証情報の利用目的、利用範囲、生体認証のシステム利用手順等について説明し、顧客より同意を得ることが必要である。

本人の同意に基づかない、もしくは、本人確認の目的以外で、生体認証情報を取得することは、「金融分野における個人情報保護に関するガイドライン」第 5 条に反する。

②厳正な本人確認の実施

生体認証に使用する生体認証情報を取得する場合は、「犯罪による収益の移転防止に関する法律」（旧「金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律」）に定める手段に準拠し、なりすましによる登録を防止し、本人であることを厳格に確認することが必要である。

（例：口座開設時の手続きの一環として、公的証明書（パスポート、運転免許証等）により、対面で確かに本人であることを確認したうえで、生体認証情報を取得すること等があげられる）

③本人確認に必要な最小限の生体認証情報のみの取得

生体認証情報の取得にあたっては、本人確認に必要な最小限の生体認証情報のみに限定することが必要である。具体的には、raw（生）データそのものを登録して使用することなく、特徴点を抽出して用いることが求められる。

(2) 入力

①テンプレートの登録

a.テンプレートの登録時には、新たに生成したテンプレートが、被登録者本人の認証に適合することを、利用開始に先立ち、確認することが必要である。

b.金融機関等がテンプレートをコンピュータ上に登録する場合は、テンプレートの作成場所から保存場所への、安全な移送・伝送手順を明確にすることが必要である。（例、暗号の使用など）

c.顧客が保持する記録媒体（以下、トークンという）にテンプレートを登録する場合は、トークンへテンプレートを安全に格納する手順、及び顧客への安全な発行手順を明確にすることが必要である。

d.伝送データの漏洩防止については【実 4】を参照のこと。

e.蓄積データの漏洩防止については【実 3】を参照のこと。

f.データ保護、破壊・改ざん防止については【実 5】を参照のこと。

g.外部ネットワークからのアクセス制限については【実 14】を参照のこと。

（注）テンプレート・・・認証時に参照するために、事前に登録する生体認証情報のこと。

②顧客への通知

取引開始に先立ち、テンプレートの登録が完了した旨、顧客への通知を行うことが望ましい。

（例：その場で本人に通知する。または、登録が完了した時点で、電子メール、はがきを出状する。）

③サンプル・データの消去

テンプレートを作成するために、顧客から取得したサンプル・データについては、その消去の条件と方法を明確にし、安全な管理のもとに速やかに消去することが必要である。

会員意見募集版

（注）サンプル・データ ・・・認証の都度（日常取引、登録時等）、センサー等の機器を介して取得する生体認証情報のこと。

(3) 利用

①暗号化

a.生体認証情報の不正利用等を防止するため、生体認証情報を移送、伝送する場合は暗号化することが必要である。

ここで対象となる生体認証情報としては、以下の例がある。

(a)テンプレート

(b)サンプル・データ

(c)ログに含まれる生体認証情報

b.また、テンプレートの改ざん検知策を講ずることが望ましい。

（例：メッセージ認証コードの使用など）

改ざん検知策については【実 7】を参照のこと。

②暗号鍵の管理

利用する暗号鍵の管理方法を明確にし、運用することが必要である。

暗号鍵の管理については【実 30】を参照のこと。

③サンプル・データの消去

日常取引において、顧客から取得したサンプル・データについては、その消去の条件と方法を明確にし、安全な管理のもとに速やかに消去することが必要である。

(4) 保存

①テンプレートの保存

a.金融機関等が、テンプレートを保存する場合、安全に保存するための手順を定めることが必要である。

b.金融機関等が、テンプレートをサーバー等の検索可能なデータベースに保存する場合は、「氏名等の個人情報」と「生体認証情報」を分別管理することが望ましい。ここでいう「氏名等」とは、氏名、顧客番号のように顧客を容易に特定できる情報を指している。

（例：具体的には、データベースを分ける。サーバーを分ける。バックアップ先の媒体を分ける。）

(a)伝送データの漏洩防止については【実 4】を参照のこと。

(b)蓄積データの漏洩防止については【実 3】を参照のこと。

(c)データ保護、破壊・改ざん防止については【実 5】を参照のこと。

(d)外部ネットワークからのアクセス制限については【実 14】を参照のこと。

②暗号化

登録された生体認証情報の不正利用等を防止するため、生体認証情報を移送、伝送、保管する場合は暗号化することが必要である。

ここで対象となる生体認証情報としては、以下の例がある。

a.テンプレート

b.ログに含まれる生体認証情報

③暗号鍵の管理

利用する暗号鍵の管理方法を明確にし、運用することが必要である。

a.暗号鍵の管理については【実 30】を参照のこと。

会員意見募集版

(5) 消去

生体認証情報、及びそれを記録した記憶媒体等を、本人確認に用いる必要性がなくなった場合、及び本人から消去の申し入れがあった場合には、速やかにこれらを消去するための手順を明確にし、安全な管理のもとに、実施することが必要である。

(6) トークンの取扱管理

①顧客が保持するトークンにテンプレートを保存する場合

a.トークンを顧客に安全に発行するための、手順を明確にすることが必要である。

b.また、発行後のトークンの使用停止、使用停止解除、再発行、消去を、安全に実施するための手順、及びトークンの紛失、盗難、汚損時等の取扱手順を明確にすることが必要である。

c.トークンを本人確認に用いる必要性がなくなった場合、及び本人から消去の申し入れがあった場合には、速やかにこれを消去するための手順を明確にし、安全な管理のもとに、実施することが必要である。

（例：顧客との授受及び登録手続きを窓口で対面で確実に行う。受領確認を行い、そのログを記録する。顧客がトークンを保有する際は、生体認証情報の漏洩防止対策がなされている。）

②不正アクセス技術の向上等に対応し、必要かつ適切な安全管理措置を実施する観点から、トークンの使用期限を考慮することが望ましい。

カードの管理方法の明確化については【実 107】も参照のこと。

テンプレートの再発行については【実 141】を参照のこと。

参照法令	・個人情報の保護に関する法律 ・個人情報の保護に関する法律についてのガイドライン ・金融分野における個人情報保護に関するガイドライン ・金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針

（参考）

「生体認証情報」を取り扱ううえで、安全対策基準に「重要」データ、「機密」データ等として記述がある下記の基準を参考にされたい。

【統 1、統 7、統 12、統 14、統 20～23、実 3～5、実 7、実 14、実 21、実 25、実 28、実 37、実 39、実 41、実 44、実 49、実 50、実 53、実 56、実 58 ～60、実 65、実 66、実 68、実 79、実 82、実 83、実 89、実 92、実 94、実 99、実 100、実 138、設 23、設 24、設 26、設 31、設 93、設 101、設 106、設 122、設 123】

会員意見募集版

9 個別業務・サービス
(10) 生体認証

適　用　区　分					基準分類
共	セ	本	提	ダ	付加
◎					

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。

生体認証の導入と運用にあたっては、不正使用防止のため、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。

1. 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が必要である。

生体認証の導入と運用にあたり、考慮すべき特性としては、以下のものがある。

(1) 認証精度

認証精度設定等の適切性の確認を行うことが必要である。（認証のしきい値を厳しく設定すると、一般に本人拒否率が高くなり、利用者はフラストレーションを引き起こすため、実務においては、これをゆるく設定しがちになる。しかし、しきい値をゆるく設定すると、他人受入率の上昇につながり、他人によるなりすまし等の可能性を高める。この観点から、両者のトレードオフを、（生体認証の結果が適用される）アプリケーションの特性を考慮し、調整することが重要となる。）

また、テンプレートを生成・発行する際は、テンプレートが十分なデータ・ポイントを有し、設定した精度を充足するように考慮することが必要である。

なお、顧客に対して認証精度を提示している時は、実装されている認証精度が提示値を充足することが必要である。

(2) 代替措置手続き

生体認証が機能しない場合（例、正当なアクセス権限を有する顧客から「認証時に拒否される旨」申告された場合等）に備えて、代替措置手続き及び手段を明確にすることが必要である。

なお、具体的策定にあたっては、代替措置手続き及び手段がセキュリティ・ホールとならないようにすることが必要である。

(3) 否認防止

「顧客による否認」防止の機能を用いる場合には、以下の点を考慮することが望ましい。

① 生体認証の結果を記録し、事後に検証する手段、手順、あるいは運用上の措置。

措置としては、以下の例がある。

a.IC カード発行時に、その IC カードが本人の認証に適合したことを、顧客本人に確

会員意見募集版

認してもらいその記録を残す
b.防犯カメラによる日常の監視　等。【設 103】

②認証判定に使用された、サンプル・データとテンプレートの照合結果を記録する。
（注）「顧客による否認」として想定している状況とは、悪意を持った顧客や勘違いをしている顧客が、その本人の口座から、生体認証にて預金の払戻しをした後、その行為を否認して被害を訴え補償を求める場合等である。

(4) 不正認証（なりすまし）等の防止
①生体認証情報の登録時、及び日常取引における認証時に、センサー等の機器を介して取得する、「真正な顧客」のサンプル・データに関して、本人ではない者による不正入手、偽造、不正使用等を防ぐ手段及び運用上の措置を講ずることが必要である。

リスクと対応策としては、以下の例がある。
(a) 偽 ATM（偽センサー機器等）の設置による、生体認証情報のだまし取り。また、センサー部分の残存情報からの指紋等のコピー。対応策としては、防犯カメラによる監視、職員による巡回点検、利用者への注意喚起等。【設 103】
(b) 人工的に合成してつくった偽造生体を使った不正認証（なりすまし）。対応策としては、生体検知装置による確認、職員による対面確認等。
(c) ホスト照合の場合には、センサーで取得した生体認証情報をホストへ送信する際にスパイウェア、フィッシングなどにより詐取され、悪用される可能性がある。対応策としては、ホストへの送信時に、暗号化や生体認証情報の読み取り日時等の情報を付加するなど、照合時にチェック可能とすることにより詐取された情報の再利用を防ぐなどが考えられる。

② テンプレートの不正利用を防ぐ手段、運用上の措置を講ずることが必要である。

リスクと対応策としては、以下の例がある。
a.悪意を持った内部者や、ネットワークを経由等した外部者が、「真正な顧客」のテンプレートを、不正に入手・使用して、それをサンプル・データ等に不正流用し、認証をパスする。対応策として、そもそもテンプレートは、サンプル・データに流用できない設計とする。ほかに、テンプレートとサンプル・データの類似度が極端に高い場合は、認証をパスさせない。（センサー機器等へかざす生体の位置・角度やぶれ等により、100%の一致は、認証方式によっては不自然な場合がある。）

(5) テンプレート保護技術
テンプレートのデータ保護について、「取り消し可能なバイオメトリクス認証」（Cancellable biometrics）など技術動向を考慮することが望ましい。

会員意見募集版

（参考）
取り消し可能なバイオメトリクス認証とは、何らかの原因でテンプレートが流出した場合等に、以前のテンプレートを無効として新規のテンプレートを再発行できる方式である。
取り消し可能なバイオメトリクス認証では、サンプル・データと変換パラメータを入力として、不可逆関数を用いて変換し、テンプレートを作成する。不可逆関数を用いて変換した場合、元のサンプル・データを復元することは不可能である。
加えて、変換パラメータは必要に応じ変更可能なので、万一テンプレートの信頼性が失われた場合には、変換パラメータを変更することによりテンプレートの再発行が可能となる。

会員意見募集版

＜会員意見募集版＞

Ⅶ. 設　備　基　準

会員意見募集版

1 コンピュータセンター
(1) 建物(環境)

適 用 区 分			
セ	本	提	ダ
○			

設 1	各種災害、障害が発生しやすい地域を避けること。

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、各種災害及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。

1. 各種災害及び障害とは、火災、落雷、津波、高潮、出水、地震、電界・磁界障害、空気汚染、重塩害、振動、土壌汚染、放射能汚染等をいう。

2. コンピュータセンターを建設する場合、各種災害及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。すでにコンピュータセンターの建物が各種災害及び障害の発生しやすい地域に立地している場合、または立地せざるを得ない場合は、各種災害及び障害に対する適切な対応策を講ずることが必要である。
なお、関係省庁、各地の自治体等が公表している災害等に関する資料等も利用すること。

（参考）

参考資料の例としては、以下のようなものがある。

・全国の地震の基礎データを取りまとめたもので全国を概観した地震動予測報告
全国地震動予測地図（地震調査研究推進本部地震調査委員会・平成 22 年 5 月更新）

・中央防災会議の専門調査会が特定地域における防災対策のシナリオを取りまとめた各専門調査会報告等
例　首都直下地震対策専門調査会報告（中央防災会議首都直下地震対策専門調査会・平成 17 年 7 月）
首都直下地震対策大綱（中央防災会議・平成 22 年 1 月修正）

・各地の自治体が独自の調査により取りまとめた各地域の地震被害想定調査報告等
例　首都直下地震による東京の被害想定報告書（東京都防災会議・平成 24 年 4 月）
地震に関する地域危険度測定調査報告（東京都都市整備局・平成 20 年 2 月）

・地震以外の調査報告等
例　大規模水害対策に関する専門調査会報告（中央防災会議大規模水害対策に関する専門調査会・平成 22 年 4 月）

・各種災害に対応したハザードマップが一覧できるサイト
例　ハザードマップポータルサイト（国土交通省）　http://disapotal.gsi.go.jp/

会員意見募集版

3. 火災

火災の発生しやすい地域とは、以下のような地域をいう。

(1) 木造建物の密集地域

(2) 多量の可燃物を取り扱う施設のある地域

(3) 火災時に爆発性のある危険物のある地域

4. 落雷

金融機関等のコンピュータシステムに障害を及ぼす自然災害のうち、最も発生件数の多いのが落雷によるものである。

立地場所の検討にあたっては、一般に公表されている年間雷雨日数の資料を参考にすることが望ましい。

5. 津波

(1) 津波は地震等による海底変動により、周期の長い波が発生して海岸に伝播し、海岸部の浅瀬でさらに大きな波となって押し寄せる。

(2) 津波の起こりやすいのは、沖合大地震の多い太平洋側で、かつ波の高くなるリアス式海岸の三陸沿岸、熊野灘沿岸、紀伊沿岸等である。

6. 高潮

高潮は台風や強い低気圧により、海水面が異常に高くなり、強風とともに海水が陸に浸水してくる現象で、Ｖ字形やＵ字形に開いた湾に起こりやすい。

7. 出水

出水の危険性のある地域とは、以下のような地域をいう。

(1) 都市化の進んだ丘陵地・台地内の谷底低地

(2) 地盤沈下地域、ゼロメートル地帯、干拓地

(3) 河川の合流点付近、屈曲した凹岸部、堤防に接して池のある地域

8. 地震

地震による被害のおそれのある地域とは、以下のような地域をいう。

(1) 過去に大地震があって、最近大地震が起きていない地域

(2) 地震により過去に断層運動を起こしたことのある地域

(3) 地殻活動が活発な地域

会員意見募集版

（参考）
地震調査研究推進本部が公表する全国地震動予測地図のデータが、独立行政法人防災科学技術研究所が運営する「地震ハザードステーション（J-SHIS）」から公表されている。
「地震ハザードステーション（J-SHIS）」では、震源断層、約 250m メッシュの確率論的地震動予測地図、主要断層帯で発生する地震に対する詳細な強震動予測に基づく震源断層を特定した地震動予測地図（想定地震地図）、地盤情報に関する地図（表層地盤増幅率や深部地盤モデルを含む）等が閲覧できる。
地震ハザードステーション（J-SHIS）　http://www.j-shis.bosai.go.jp/

なお、地震等による被害を大きくする要因のひとつに液状化現象がある。
液状化現象については、地震動による上昇水圧等により砂や水が噴出することがあり、特に飽和状態に近い水を含む砂層では砂粒子が水中に浮遊した現象を引き起こし、いわゆる液状地盤となり建物の沈下が発生しやすい状態をいう（表 1）。

表 1　液状化の可能性と地形

液状化の可能性	地形からみた判定	液状化履歴からみた判定
（A）可能性が高い	・埋立地、水面上の盛土地 ・現、旧河道 ・発達が微弱な自然堤防 ・砂丘と低地の境 ・砂丘間低地	液状化履歴地点
（B）場合によって可能性あり	上記以外の低地	液状化履歴がない地点
（C）可能性が低い	・台地　　・丘陵 ・山地	

9.　電界・磁界障害
電界・磁界障害のおそれのある地域とは、電波塔やマイクロ回線の近辺等、電界・磁界が強く、コンピュータへの影響のある地域をいう。

10.　空気汚染
空気汚染による被害のおそれのある地域とは、以下のような地域をいう。
(1) 各種の工場等から発生する有毒ガスや硫黄分を含んだ汚染空気の多い地域
(2) 火山地帯、塵埃の多い鉱山近辺、土砂貯蔵施設の近辺

11.　重塩害
重塩害地域とは、海岸に近い地域をいう。
塩害としては、送電線、通信回線の碍子（がいし）に風雨で塩水、塵埃が付着し、導電性を帯びて短絡（ショート）する被害等がある。

会員意見募集版

12. 振動

振動による障害のおそれのある地域とは、鉄道線路、幹線道路等に近い地域をいう。

13. 土壌汚染

土壌汚染のおそれのある地域とは、土壌中に重金属、農薬等の有害物質が溶け込んでおり、人の健康や生活に大きな影響を及ぼすと考えられる地域をいう。

14. 放射能汚染

放射能汚染による被害のおそれのある地域とは、原子力発電所や原子力関連施設の事故等により放射線や放射性物質が飛散し、人の健康や生活に大きな影響を及ぼすと考えられる地域をいう。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(2) 建物(周囲)

適　用　区　分			
セ	本	提	ダ
○			

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。

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、地域環境等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。

1. 産業、都市、住宅、交通等のコンピュータセンターの立地する周辺の環境は少しずつ変貌しており、これに伴い災害および障害の発生する原因、場所、影響範囲等も少しずつ変化し、多様化している。
   このため、コンピュータセンターの立地する周囲の自然環境、地域環境等の各項目を任意に設定し、環境の変化に伴う災害および障害の発生の可能性について定期的に調査を行い、災害および障害の発生を未然に防止する適切な対応策を事前に講ずることが望ましい。

2. 環境の変化に伴う災害の発生の可能性は、立地条件によって異なるが、以下のような例がある。
   (1) 都市化の進展による雨水の流出率、流出速度の変化による浸水、河川災害
   (2) 切土、盛土等による地すべり、崖崩れ、土砂の流出等土砂災害
   (3) 地下水系の変化による基礎地盤の構造変化
   (4) 近隣における危険物施設、構造物の建設
   (5) 近隣に送電用鉄塔、電波塔等が立つことによる電界・磁界障害
   (6) 有毒ガス等を出す工場の建設、火山活動の活発化等による空気汚染
   (7) 鉄道線路、地下鉄、高速道路等の建設による振動障害

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(2) 建物(周囲)

適　用　区　分			
セ	本	提	ダ
◎			

設　3	敷地には通路を確保すること。

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。

1. 消火活動、避難のための通路については、建築基準法に規定されたものとすることが必要である。

2. 通路は二方向に避難できるようにすることが望ましく、夜間でも安全に避難できるよう標識、照明を備えることが必要である。また、非常口や避難通路の整理整頓を常に心掛け、消火活動および避難の妨げとなる物品を置かないように留意することが必要である。

参照法令	建築基準法第 35 条、建築基準法施行令第 128 条

会員意見募集版

1 コンピュータセンター
(2) 建物(周囲)

適 用 区 分			
セ	本	提	ダ
○			

設　4	隣接物との間隔を十分に取ること。

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。

1. 建築基準法では、延焼のおそれのある部分とは、図 1 のように隣地境界線、道路中心線または同一敷地内の 2 以上の建築物相互間の外壁間の中心線から、1 階にあっては 3m 以下、2 階以上にあっては 5m 以下の距離にある部分としている。
   このため、隣接する建物との十分な間隔とは、10m 以上をいう。

2. 防火上十分な間隔を確保することが困難な場合は、図 2 のように防火塀や防火植樹帯を設けることが望ましい。
   防火植樹帯とは、火熱力の減少と熱風遮断の効果のあるサンゴジュ、マテバシイ、ユズリハ等の常緑広葉樹を帯状に植えたものをいう。

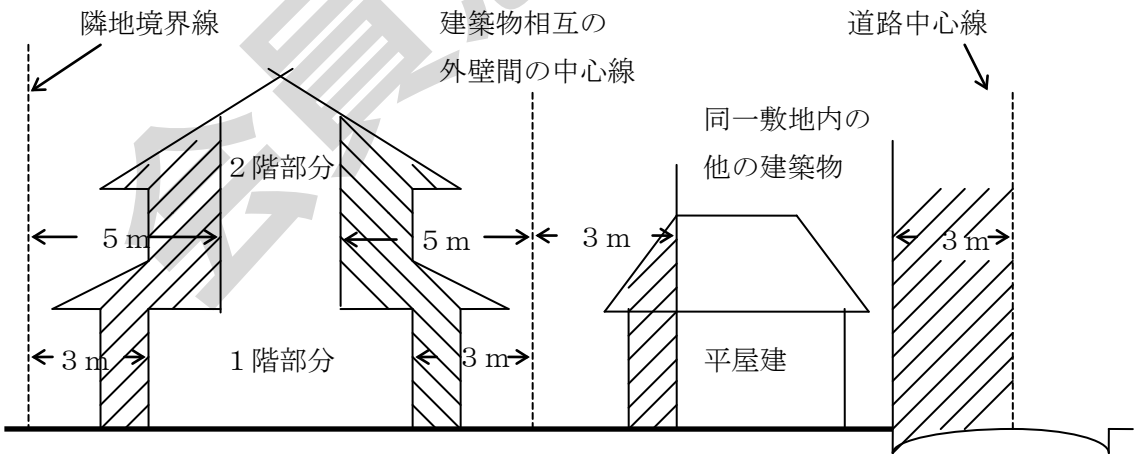
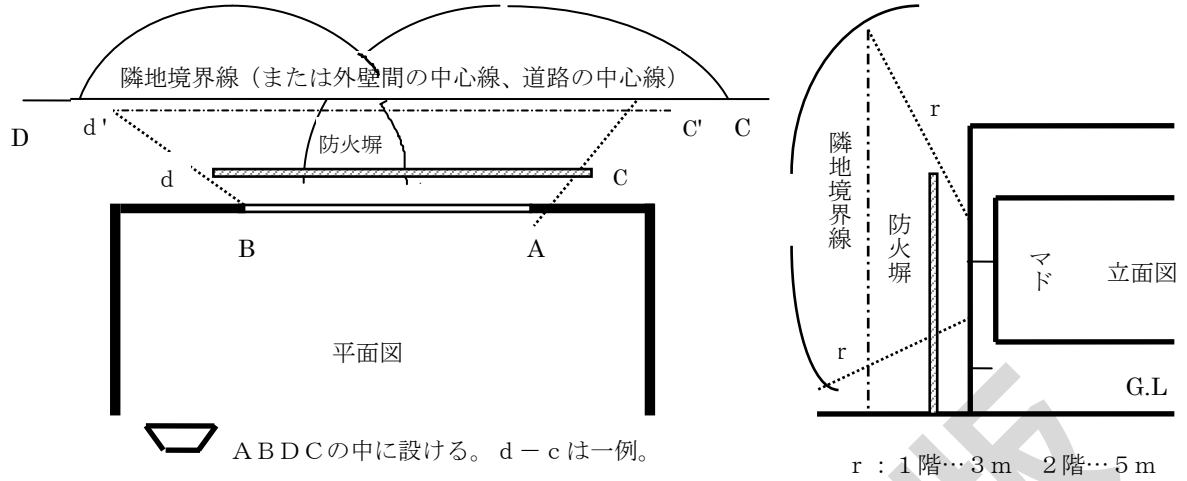


図 1　延焼のおそれのある部分の例

会員意見募集版



ＡＢＤＣの中に設ける。ｄ－ｃは一例。
ｄ′－ｃ′でも可。Ｄ－Ｃでもよい。

ｒ：１階…３ｍ　２階…５ｍ

図２　防火塀の設置例

参照法令	建築基準法第 2 条第 6 号、建築基準法施行令第 109 条

会員意見募集版

1 コンピュータセンター
(2) 建物(周囲)

適 用 区 分			
セ	本	提	ダ
○			

設 5	塀または柵および侵入防止装置を設けること。

敷地内への不法侵入、建物等の破壊行為を防止するため、敷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。

1. 敷地境界で行う入退管理は、敷地内の建物で行う入退管理を補完する措置である。

2. 塀または柵

塀または柵の設置にあたっては、周囲の環境との調和に留意し、部外者の侵入を防止できる 2m 程度の高さで、破壊に対して堅固な構造とすることが必要である。ただし、周囲の状況により人が立ち入るおそれがない場所についてはこの限りではない。

3. 侵入防止装置

侵入を防止する措置としては、警備員によるものと侵入防止装置によるものがある。
侵入防止装置には、以下のような例がある。

(1) 赤外線検知装置

片側に赤外線投光器を設置し、一方に受光器を設置して侵入者が赤外線ビームを遮断することにより作動する。警戒範囲が線となるため、光線を 2 本放射するとより効果的である。装置により最大検出距離が数百メートルになるものもあるが、設置にあたっては、立木や造形物等のない見通しのきく場所に限定される（図 1）。

(2) トラップセンサー

塀や金網フェンス等に取り付けて、乗り越え、切断、突破等を感知する（図 2）。

4. 照明設備

照明設備を設置する場合は、以下のような点に留意することが必要である。

(1) 建物の周囲の敷地、地上より 2 階までの壁面、非常階段等侵入が予想される場所については、夜間において照明装置により十分な照度を確保する（図 3）。

(2) 照明設備自体も投石等により壊されることのないようにする。

会員意見募集版

＜会員意見募集版＞

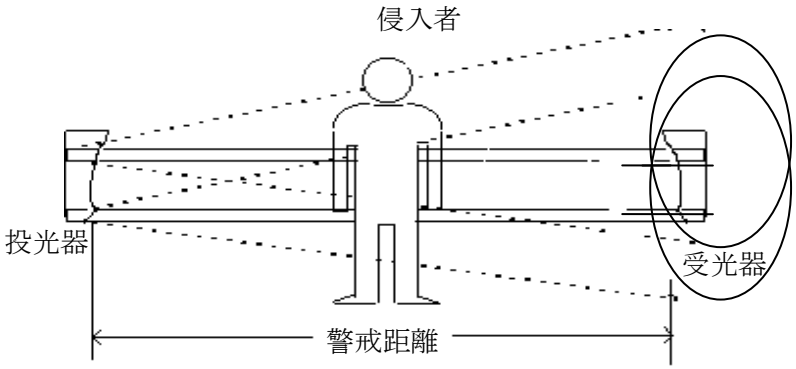


図１　赤外線検知装置の例

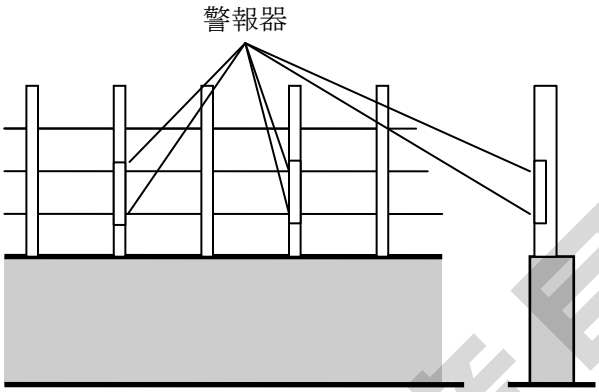


図２　トラップセンサーの例

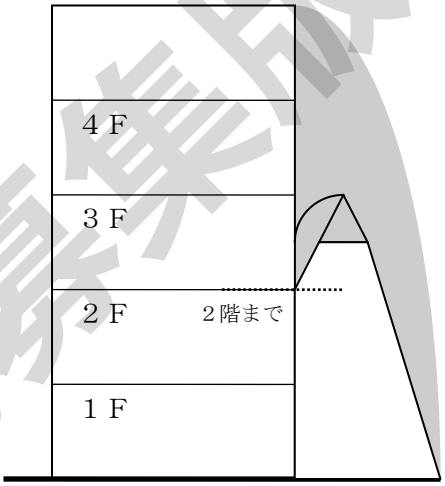


図３　照明設備の例

会員意見募集版

1 コンピュータセンター
(2) 建物(周囲)

適　用　区　分			
セ	本	提	ダ
○			

設　6	看板等を外部に出さないこと。

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。

1. コンピュータセンター等の所在を示した表示板、看板等とは、例えば○○コンピュータセンター、××銀行事務センター等と表示したものをいう。

2. 共同ビル等においても、コンピュータおよび同関連設備が設置されている場所等に、容易に判明できる表示、標識等を出さないことが望ましい。【設 24】参照

会員意見募集版

1 コンピュータセンター
(2) 建物(周囲)

適　用　区　分			
セ	本	提	ダ
○			

設　7	建物には避雷設備を設置すること。

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。

1. 避雷設備を設置し、雷撃電流を安全に大地に放流（アース）することにより、落雷によるコンピュータシステムの障害のほか、内部にいる人の感電死傷、建物の損傷、火災等の事故を防止することが必要である。

2. 建築基準法では、建物の高さが 20m を超える場合、ならびに危険物の規制に関する政令では取り扱う危険物の数量が指定の 10 倍以上である場合、避雷設備の設置が義務づけられている。上記以外の場合であっても、以下のような落雷の可能性の高い場合には、避雷設備を設置することが望ましい。
   (1) 雷の多い地方
   (2) 過去に落雷があったか、または付近に落雷のあった場合
   (3) 平地に単独で建っている場合、山または丘の頂上にある場合

3. 避雷設備は国土交通大臣が指定する日本工業規格に定める構造とすること。

参照法令	建築基準法第 33 条、建築基準法施行令第 129 条の 14、15、危険物の規制に関する政令第 9 条、JIS A4201（2003）

会員意見募集版

1 コンピュータセンター
(2) 建物(周囲)

適 用 区 分			
セ	本	提	ダ
○			

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。

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。

1. 建物を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目的は、以下のとおりである。
   (1) コンピュータセンターは本部・営業店等の勤務状態と異なることがあるため、運用上も安全管理が徹底できる。
   (2) 入退館（室）管理が徹底できる。
   (3) 各種設備の保全や安全のための運用管理が徹底できる。
   (4) 立地環境の変化に伴う速やかな対応策が講じやすい。

2. コンピュータセンターが共同ビル等にある場合においては、安全管理を徹底するため、設備面、運用面においてコンピュータシステム関連業務専用の建物に準じた配慮をすることが必要である。

会員意見募集版 配布資料

1 コンピュータセンター
(2) 建物(周囲)

適　用　区　分			
セ	本	提	ダ
○			

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。

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。

1. コンピュータセンター敷地内に布設された通信回線・電力線は、ガス、水道等の埋設工事、外部からの侵入等による切断・延焼の防止措置を講じ、コンピュータシステムの安全性を確保することが必要である。

2. 一般にコンピュータセンター建物への通信回線・電力線の引込み方法は、地中ケーブルによって行われる場合が多い。コンピュータセンター敷地内における管路は通常金融機関等の施設となっているが、引込みケーブルは電話会社および電力会社が布設するため、施工にあたっては事前に図面等により協議を行ったうえで切断、延焼の防止措置を講ずることが望ましい。

3. 敷地内の通信回線・電力線の施工方法としては、以下のような例がある。
   (1) 引込柱以降の構内通信回線・電力線は、地中方式とする。
   (2) 地中電線は、難燃ケーブルを使用するか、ケーブルを不燃材で覆う。
   (3) 地中電線路を管路引入れ式または暗きょ式により施設する場合は、堅牢で重量物の圧力に耐え、かつ水が侵入し難い管または暗きょを使用する。
   (4) 地中電線路を直接埋設方式により施設する場合は、重量物の圧力を受けるおそれがある場所においては地表から 1.2m 以上、その他の場所においては、60cm 以上の深さに埋設する。
   (5) 高圧または特別電圧の地中電線線路を管またはトラフに収めて施設する場合は、概ね 2m の間隔での物件の名称、管理者名、電圧を表示する。
   (6) 地中電線路は、地中通信回線路に対して漏洩電流または誘導作用により通信上の障害を及ぼさないよう地中通信回路から十分離して施設する。
   (7) 地中電線が、地中通信回線等と接近し、または交差する場所において相互の離隔距離が低圧または高圧の地中電線にあっては 30cm 以下、特別高圧地中電線にあっては 60cm 以下のときは、間に堅牢な耐火性の隔壁を設ける場合を除き、地中電線を堅牢な不燃性または自消性のある管に収め、当該管が地中通信回線等と直接接触しないように施設する。
   (8) 経路の選定にあたっては、将来の増築、舗装等で支障を受けないように考慮する。

会員意見募集版

参照法令	電気事業法　電気設備の技術基準の第 120 条、第 124 条、第 125 条

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(3) 建物(構造)

適 用 区 分			
セ	本	提	ダ
◎			

設 10	耐火建築物であること。

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。

1. 今後建築される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にすることが必要である。建物を耐火建築物にすることにより、防犯対策、入退館管理および空気調和の実施面でも効果が得られる。

2. 都市計画法においては、市街地における火災の危険を防止するため、防火地域、準防火地域を定めることになっている。
   防火地域内においては階数が 3 以上であり、または延べ面積が 100 ㎡を超える建築物は耐火建築物としなければならない。

3. 耐火建築物
   (1) 耐火建築物とは、壁、柱、屋根等の主要構造部を耐火構造とした建築物で、外壁の開口部で延焼のおそれのある部分に法令で定める構造の防火戸、その他の防火設備を有するものをいう。
   (2) 耐火構造とは、鉄筋コンクリート造、れんが造等の構造で、法令で定める耐火性能を有するものをいう。
   (3) 耐火構造の性能は、通常の火災時の耐火時間を基準として、建築基準法で表 1 のように定められている。

参照法令	建築基準法第 2 条第 7 号、第 9 号の 2、第 61 条 建築基準法施行令第 107 条、第 108 条の 3、第 109 条の 2 都市計画法第 8 条

会員意見募集版

＜会員意見募集版＞

表１　建物部位別必要耐火性能

建築物の部分／建築物の階	壁		柱	床	はり	屋根	階段
	間仕切壁（耐力壁に限る）	外壁（耐力壁に限る）					
最上階および最上階から数えた階数が 2 以上 4 以内の階	1 時間	1 時間	1 時間	1 時間	1 時間	30 分	30 分
最上階から数えた階数が 5 以上 14 以内の階	2 時間	2 時間	2 時間	2 時間	2 時間		
最上階から数えた階数が 15 以上の階	2 時間	2 時間	3 時間	2 時間	3 時間		

会員意見募集版

1 コンピュータセンター
(3) 建物(構造)

適 用 区 分			
セ	本	提	ダ
◎			

設 11	構造の安全性を有すること。

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。

1. 建物の自重、積載荷重、積雪、風圧および地震等の震動ならびに衝撃に対する構造の安全性を講ずることにより、コンピュータシステムに障害を及ぼさないようにすることが必要である。

2. 現行の建築基準法は、施行または適用の際に現存する建築物について、現行建築基準法に適合しない部分を有する場合においては、その部分に対しては当該規定は適用しないとしている。
   しかしながら、旧建築基準法で設計されたコンピュータセンターの建物については、耐震の安全性を公的機関等に診断、判定を依頼し、構造の安全性に問題がある場合は、耐震補強をするなど、現行建築基準法に準じた構造の安全性を確保することが望ましい。

3. 建築基準法で定める積載荷重は 2900 ニュートン／㎡（約 300kg／㎡）以上であるが、設置する機器の実態に応じて必要な強度を有する必要がある。

参照法令	建築基準法第 3 条第 2 項、第 20 条 建築基準法施行令第 85 条

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(3) 建物(構造)

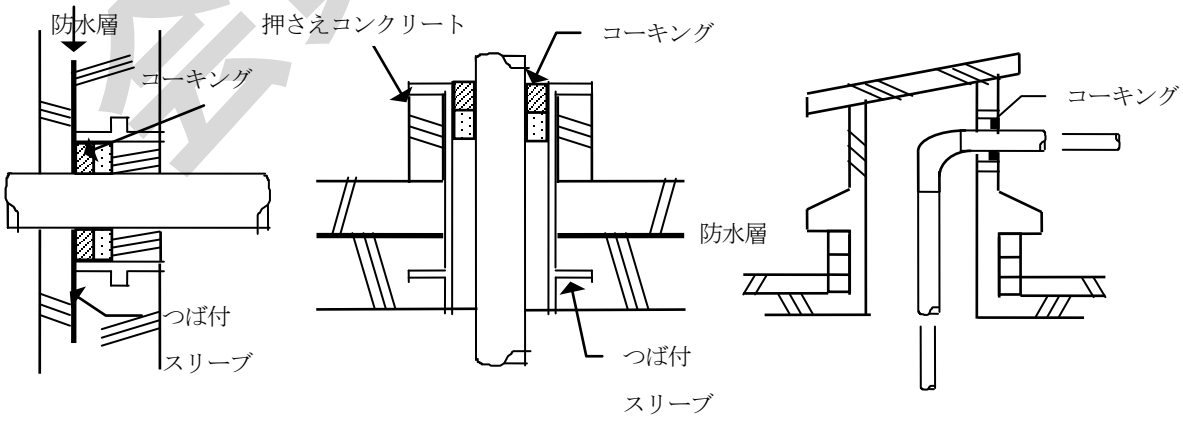
適 用 区 分			
セ	本	提	ダ
◎			

設 12	外壁、屋根等は十分な防水性能を有すること。

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。

1. 外壁、屋根等の長年の使用による防水、排水性能の低下、または排水能力を超えた豪雨や排水口にゴミが詰まった場合等の漏水によって、コンピュータシステムに障害を及ぼさないよう、漏水の防止措置を講ずることが必要である。

2. 漏水に対する防止措置を行うにあたっての留意点としては、以下のような例がある。
   (1) 屋根、外壁
   屋上、屋根、擁壁、コンクリート目地部分の損傷や防水層の劣化・破れ、コンクリート亀裂の進行
   (2) 屋上工作物等
   屋上の手摺、吊輪、高架水槽・冷却塔設備や広告塔等による屋上の防水層の損傷
   (3) 屋根、外壁の貫通部
   屋上、外壁の防水層を貫通する給排気口、ダクト、配管、配線等の防水性の保持（図 1）また、給湯、蒸気配管の熱の影響、およびダクト等の風の影響による防水層の剥離、破断



例 1　防水壁の場合　　例 2　防水床の場合　　例 3　屋上を貫通する場合

図 1　防水層貫通の配管の例

＜会員意見募集版＞

1 コンピュータセンター
(3) 建物(構造)

適　用　区　分			
セ	本	提	ダ
○			

設　13	外壁等に強度を持たせること。

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。

1. 破壊行為等から防御できる外壁の例としては、鉄筋コンクリート造、カーテンウォールのうち防犯強度を有するもの等がある。カーテンウォールとは、建物の荷重支持の機能を持たない薄い壁で、材質としては金属パネル、鉄筋コンクリート材等多様であり、一般にはパネル化されて工場で生産される。カーテンウォールに防犯機能を持たせる場合は、十分な強度を有するものを選択することが必要である。
   また、ガラスには、防火、防犯用のガラス等がある。

会員意見募集版

1 コンピュータセンター
(4) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
◎			

設 14	窓には防火措置を講ずること。

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。

1. 延焼のおそれのある窓とは、窓と隣接境界線、道路中心線または同一敷地内の 2 以上の建築物相互の外壁間の中心線との距離が、1 階にあっては 3m 以下、2 階以上にあっては 5m 以下の場合をいう。

2. 耐火建築物および準耐火建築物にあっては、外壁の開口部で延焼のおそれのある部分に防火戸、その他の防火設備を設置すること。
なお、開口部から 1 階にあっては 3m 以下、2 階以上にあっては 5m 以下に隣地境界線、道路中心線等が入る場合、開口部をさえぎる耐火、準耐火または防火構造の外壁、そで壁、塀その他これに類するものは防火設備とみなされる。

3. 防火設備の構造方法には防火設備、特定防火設備の 2 種類の技術基準があり、それぞれ以下のように規定されている。
(1) 防火設備
①鉄製で鉄板の厚さが 0.8mm 以上 1.5mm 未満のもの
②鉄骨コンクリート製または鉄筋コンクリート製で厚さが 3.5cm 未満のもの
③土蔵造で厚さが 15cm 未満のもの
④鉄および網入ガラスで造られたもの
⑤国土交通大臣が、同等の防火性能を有すると認めたもの
(2) 特定防火設備
①骨組を鉄製とし、両面に厚さ 0.5mm 以上の鉄板を張ったもの
②鉄製で鉄板の厚さが 1.5mm 以上のもの
③鉄骨コンクリート製または鉄筋コンクリート製で厚さが 3.5cm 以上のもの
④土蔵造で厚さが 15cm 以上のもの
⑤国土交通大臣が、同等以上の防火性能を有すると認めたもの

4. 特定防火設備と同等の防火性能を有する設備としてドレンチャー設備がある。
ドレンチャー設備とは、外壁、窓等の開口部に設置して、隣接建物からの延焼を防止するために、水幕を張って火災や輻射熱を遮断する設備をいう。

会員意見募集版

参照法令	建築基準法第 2 条第 6 号、第 9 号の 2、第 9 号の 3 建築基準法施行令第 109 条、建設省告示第 1360 号、1369 号

会員意見募集版

1 コンピュータセンター
(4) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
◎			

設 15	防犯措置を講ずること。

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。

1. 窓の防犯措置としては、以下のような例がある。
   (1) 防犯用のガラス
   (2) 開閉可能な鉄格子またはシャッター
   (3) 窓の開閉を磁気の動作により感知するマグネットスイッチ（図 1）
   (4) ガラスの破壊時に生じる特定高周波などを感知する感知器（図 1）

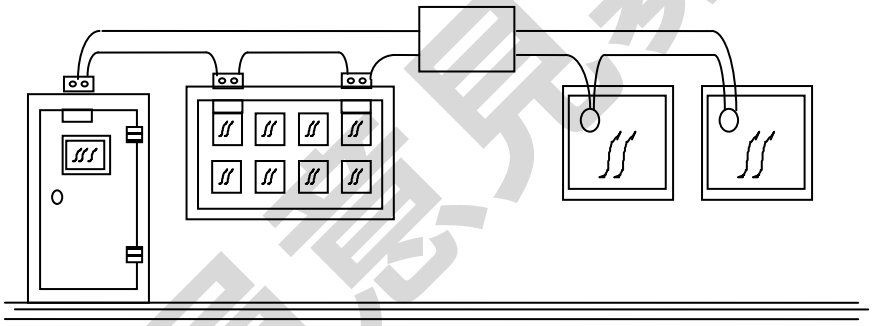


図 1　マグネットスイッチ（左）、はめごろし、窓用の感知器（右）の例

2. 建物の周囲に広告看板、建物、歩道橋、高速道路等があり、2 階以上の階に接近が容易であれば、それぞれの窓にも防犯措置を講ずることが望ましい。

（参考）
「ガラスの防犯性能に関する板ガラス協会基準」で以下のように明記されている。
単体ガラスのフロートガラス、網入りガラス、強化ガラスについては、ドライバーなどでガラスを破壊し、侵入する「こじ破り」に対する防犯性能は期待できない。なお、簡単に破壊できないガラスとして防犯ガラス（ポリカーボネートを単板ガラスで圧着したもので、性能ランク P2A（「打ち破り」を想定した性能基準）以上かつ P2K（「こじ破り」を想定した性能基準）以上の基準を満たすもの）がある。

会員意見募集版

1 コンピュータセンター
(4) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
○			

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。

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、常時利用する出入口は１カ所とし、出入管理設備、防犯設備を設置することが望ましい。

1. 常時利用する出入口に設置する出入管理設備として、以下のような例がある（図 1）。
   (1) 受付
   警備員により入退館者を識別し、あらかじめ入館を許可された者以外は所定の手続きにより入館を記録する。
   (2) 開閉装置
   開閉装置によりあらかじめ設定された入退館資格を識別、記録し、扉の開閉を行う。共連れ防止機能を持つ開閉装置にはフラッパーゲート、サークルゲート等がある。
   入退館資格の識別手段には以下のような例がある。
   ①磁気カード出入管理装置･･･････磁気カードをカードリーダーに挿入してチェックする（図 2）。
   ②カードセンサー装置･･･････････カードをセンサーに近づけてチェックする。
   ③IC カード･光カード出入管理装置･･･IC カード、光カードをカードリーダーに挿入してチェックする。
   ④パスワード入力装置･･･････････パスワードを入力することによりチェックする。
   ⑤掌形・掌紋識別装置･･･････････掌形、掌紋を光学的に読み取りチェックする。
   ⑥指紋照合装置･･･････････････････指紋を光学的に読み取りチェックする。
   ⑦網膜パターン識別装置･･･････････網膜パターンを光学的に読み取りチェックする。
   ⑧リアルタイムサイン識別装置････サインを書く際の筆圧、時間、筆跡を読み取りチェックする。
   ⑨声紋認識装置･･･････････････････声紋を読み取りチェックする。

2. 常時利用する出入口に設置する防犯設備として、以下のような例がある（図 1）。
   (1) インターホン･･･････ドアを開けずに館内と会話し、入館者をチェックする。
   (2) 防犯カメラ･･･････････カメラにより出入口、前室の状況を撮影、監視する。【設 103】
   (3) 防犯ビデオ･･･････････防犯カメラにより撮影した出入口、前室の状況を、ビデオ装置で記録する。【設 103】
   (4) 防犯警報装置･･･････特定場所の接近、通過、開閉等をチェックし、異常の場合に警報する。【設 113】
   (5) 金属探知機･･･････････金属を検知し、電子機器等の所持を警報する。

会員意見募集版

3. 常時利用する出入口が 2 カ所以上の場合は、それぞれの出入口において確実に入退館管理を行うか、常時利用する出入口は 1 カ所として、他の出入口は施錠することが必要である。
共同ビル等で建物の出入口を 1 カ所に限定できない場合は、建物内の階、コンピュータ室の出入口等で同様の措置を講ずることが必要である。

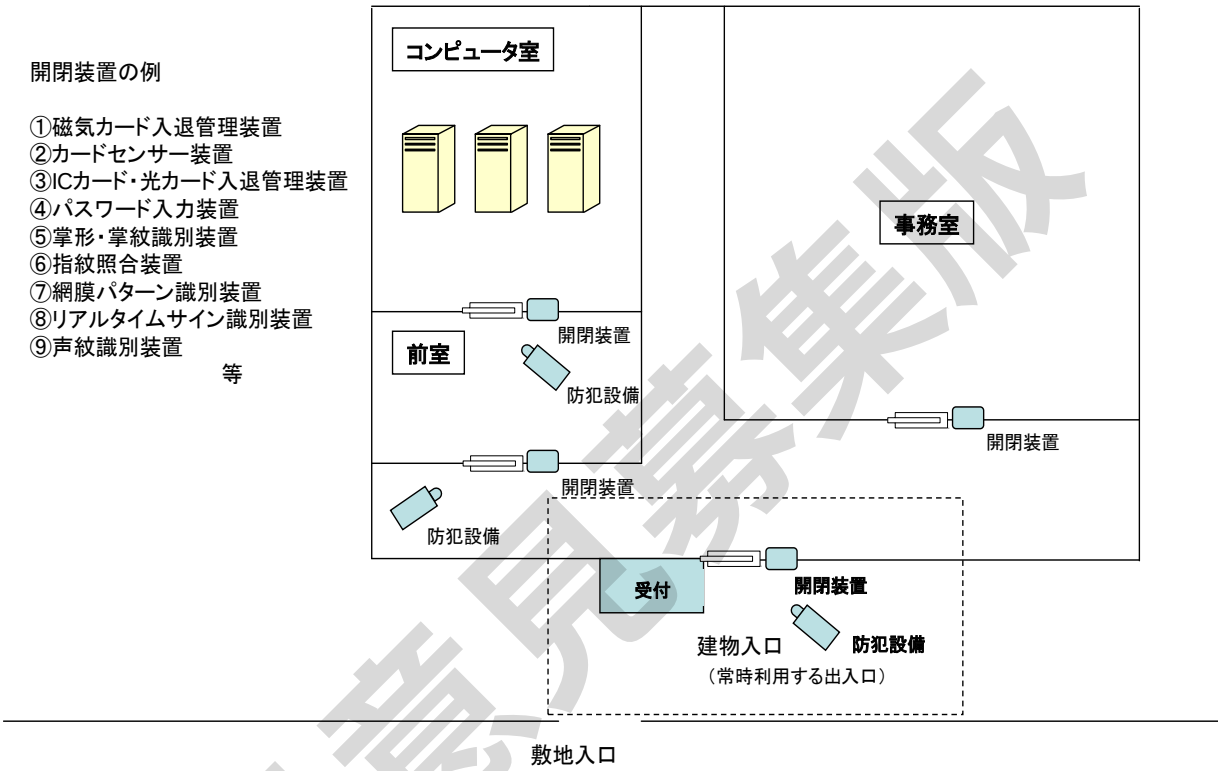


図 1　出入管理設備　開閉装置配置の例

会員意見募集版

＜会員意見募集版＞

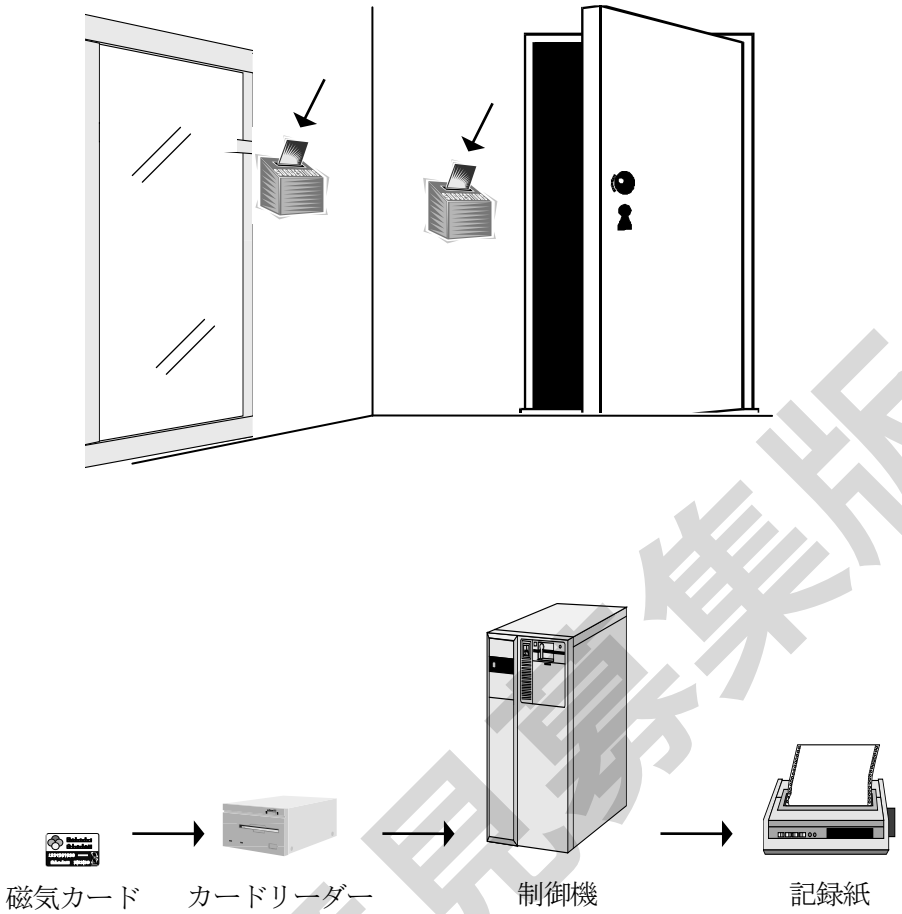


図２　磁気カード出入管理装置の例

会員意見募集版

1 コンピュータセンター
(4) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
◎			

設 17	非常口を設けること。

災害時の安全な避難と非常時持出しの円滑化のため、適切な位置に非常口を設けること。

1. 非常口は、火災等の災害の際に、コンピュータセンターから避難するための非常出口をいい、非常口および非常口へ至る避難通路は、図１のように建物のどの場所からも二方向に避難できる位置に設けることが必要である。

2. 非常口は、屋内から鍵を用いることなく開くことができる構造となっていること。

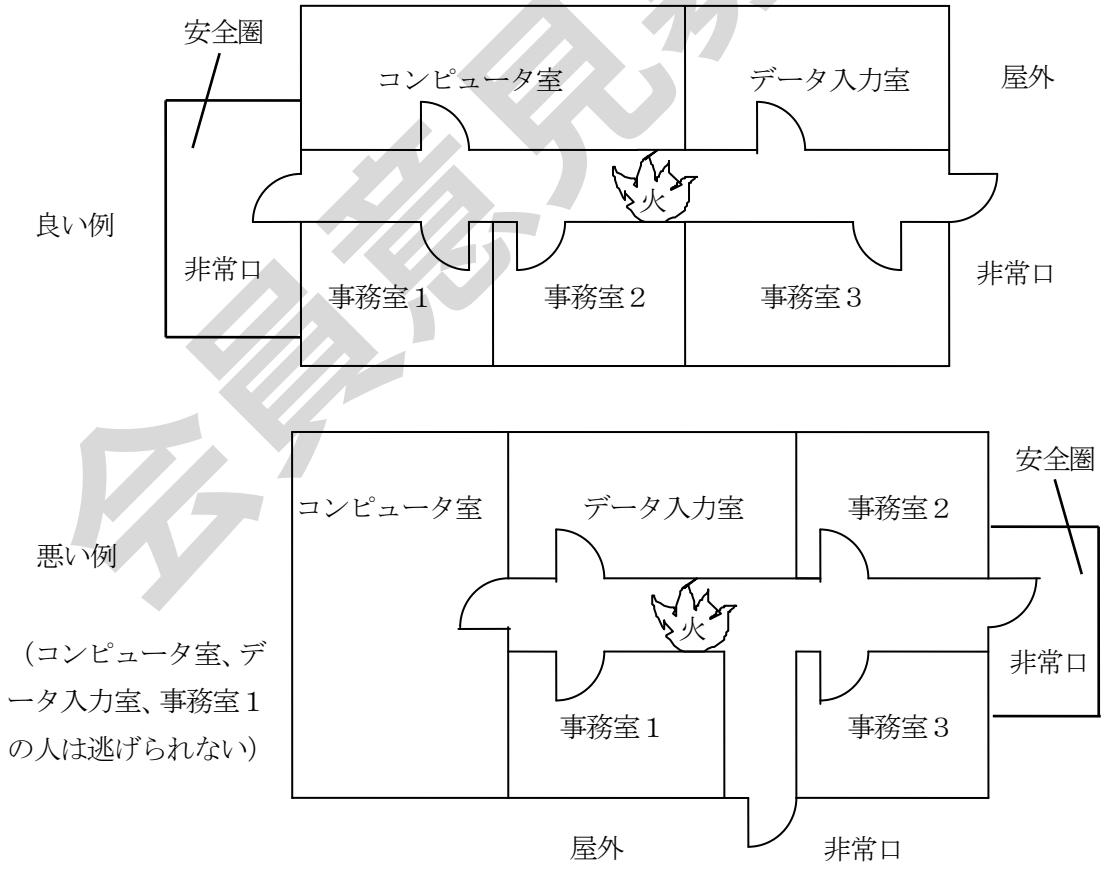


図１　非常口および非常口へ至る避難通路の例

参照法令	建築基準法第 35 条、建築基準法施行令第 117 条第 1 項、第 125 条の 2

会員意見募集版

1 コンピュータセンター
(4) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
○			

設 18	防水措置を講ずること。

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。

1. 開口部の防水措置として、以下のような例がある。
   (1) 出入口扉、シャッター、回転ドア等の補強
   (2) 排水溝や防水堤、防水板、防水扉等の設置
   (3) 防水用砂袋の設置

2. 水害対策として、建物出入口は地面から高くし、道路へは階段およびスロープを設けることが望ましい。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(4) 建物(開口部)

適　用　区　分			
セ	本	提	ダ
◎			

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。

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。

1. 出入口の扉は十分な強度を有する特定防火設備を使用し、不法侵入、危険物の投込み、延焼等を防止することが必要である。

2. 出入口の扉には錠を付け、非常時または業務終了時に出入口が閉鎖できる構造となっていることが必要である。

3. 出入口の扉の錠は、緊急避難時において屋内から鍵を用いることなく解錠が可能な機器を有することが必要である。また、自動ドアにする場合は、停電でも屋内から開閉できる機能を有することが必要である。

4. 特定防火設備については、【設 14】参照のこと。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(5) 建物(内装等)

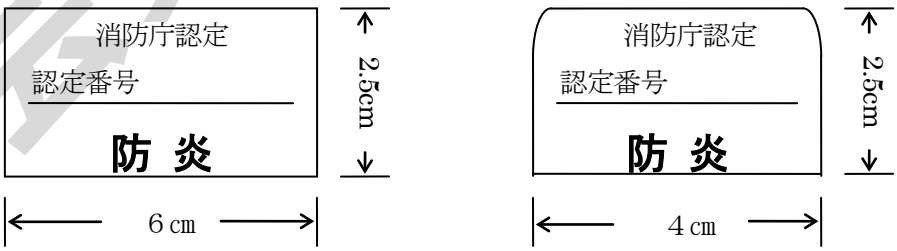
適 用 区 分			
セ	本	提	ダ
◎			

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。

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。

1. 不燃材料は、通常の火災時の加熱に対して燃焼せず、防火上有害な変形、溶融、亀裂、その他の損傷を生じないものであって、かつ、防火上有害な煙またはガスが発生しないものをいう。
   建築基準法では、不燃材料はコンクリート、れんが、瓦、鉄鋼、アルミニウム、ガラス、モルタル、しっくい、その他これらに類する建築材料とされている。
   不燃材料として国土交通大臣が認定した内装材の例としては、石膏ボードにロックウール板を組み合わせたものなどがある。
   なお、石綿については、厚生労働省の定める石綿障害予防規則により、石綿を使用している建築物等における管理、解体等の業務に係る措置等が定められているので、石綿を使用している建築物の管理ならびに解体については建築業者に確認するなど、注意が必要である。

2. 消防法に規定する防炎性能を有するカーテン、じゅうたん等には、図 1 のように防炎表示が付いている。防炎処理済であっても、燃焼しないというものではなく、発炎しても大きな火力にならないというものであるから、コンピュータ室ではなるべく金属ブラインド等、不燃性のものを用いることが必要である。



カーテン等　　じゅうたん等

図１　防炎表示

3. 合板、繊維板、壁紙等の内装材は、日本工業規格等の防火性能の表示マークが付されているものを用いることが必要である。

参照法令	建築基準法第 2 条第 9 号、建築基準法施行令第 108 条の 2、第 109 条の 2 消防法第 8 条の 3、平成 16 年国土交通省告示第 1178 号、石綿障害予防規則

会員意見募集版

1 コンピュータセンター
(5) 建物(内装等)

適　用　区　分			
セ	本	提	ダ
○			

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。

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。

1. 鉄骨造の場合は、建物構造体の耐火性保持のため、柱、はり等は不燃材料により耐火被覆することが必要である。なお、耐火被覆を行うに際しては、地震による落下および損壊の防止措置を講ずることが望ましい。

2. 地震等により配管損傷による漏水が発生した際、漏水範囲を局所化するような対策を講ずることが望ましい。

3. 【設 35】参照

（参考）
建築非構造部材の耐震資料については、「官庁施設の総合耐震計画基準及び同解説」（社団法人公共建築協会）がある。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(6) コンピュータ室・データ保管室(位置)

適　用　区　分			
セ	本	提	ダ
◎			

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。

1. 建物内において、コンピュータ室・データ保管室は、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により、コンピュータシステムへの影響を防止することが必要である。災害を受けるおそれのある位置にやむを得ず設置する場合は、各種災害による被害の防止対策を講ずることが必要である。
   また、コンピュータ室・データ保管室は、電磁界の影響を受けるおそれの少ない位置に設置することが必要である。やむを得ない場合には、電磁シールド等の措置を講ずることが必要である。

2. 建物内において災害を受けるおそれの少ない位置として、以下のような例がある。
   (1) 地震
      ①剛構造の建物においては地震の震動が少ない下層階
      ②重量設備が直上階の直上部にない場所
      ③火気を扱う食堂、喫茶等が隣室または上下階にない場所
   (2) 火災
      ①爆発による火災の危険性の高いボイラー室、燃料保管室等が隣室または上下階にない場所
      ②大量の可燃物を貯蔵する文書保管庫、物品倉庫等が隣室にない場所
   (3) 浸水
      ①浸水の危険性のない２階以上
      ②水使用設備が隣室または直上階にない場所
      ③屋上から漏水の危険性のない最上階以外の階
   (4) ガス滞留等
      ①可燃性または腐食性のガス、蒸気、粉塵、塩分等が侵入または滞留のおそれの少ない場所

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(6) コンピュータ室・データ保管室(位置)

適 用 区 分			
セ	本	提	ダ
◎			

設 23	外部から容易に入れない位置に設置すること。

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。

1. コンピュータ室・データ保管室を設ける場合、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、外部から容易に入れない位置に設置することが必要である。

2. やむを得ず、コンピュータ室・データ保管室を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に設ける場合の措置としては、以下のような例がある。
   (1) 室に直接入れないように、例えば図１のように出入口に前室を設ける。前室に入るドアとコンピュータ室・データ保管室に入るドアは同時に開かないように連携させる。
   (2) 室の出入口等に出入管理設備等を設置する。
   (3) 室を十分な強度を有する壁等で遮蔽する。

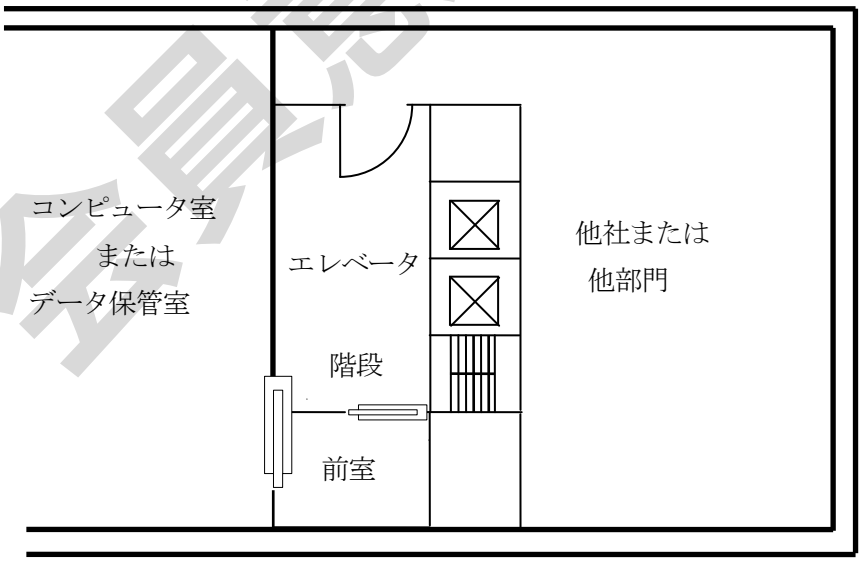


図１　コンピュータ室またはデータ保管室の位置の例

会員意見募集版

1 コンピュータセンター
(6) コンピュータ室・データ保管室(位置)

適 用 区 分			
セ	本	提	ダ
◎			

設 24	室名等の表示は付さないこと。

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。

1. コンピュータセンターの建物内においては、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の表示、案内板の設置は行わないこと。

2. コンピュータ室・データ保管室の位置が消防担当者に明示できるよう、コンピュータセンター内の見取図を、建物の入口、中央管理室等で部外者の目に触れないように保管しておくことが必要である。

会員意見募集版

1 コンピュータセンター
(6) コンピュータ室・データ保管室(位置)

適　用　区　分			
セ	本	提	ダ
◎			

設　25	必要空間を確保すること。

保守、避難のため、必要空間を確保すること。

1. コンピュータ室の各種機器の配置にあたっては、各機器の操作、保守に必要な空間をあらかじめ確保することが必要である。また、各機器の搬出入口および経路を確保することも必要である。
   また、非常時に出入口または非常口等安全な場所へ、短い距離で避難できる空間を確保することが必要である。

2. 保守に必要な空間は、コンピュータおよび周辺機器等の扉の開閉が機器を移動しなくてもできる広さを目安とすることが必要である。

3. コンピュータ室にはシステムの運営上、帳票等消耗品や什器、備品等が必要となるが、整理整頓に心掛け、保守、避難に必要な空間に積み上げたり、通路を狭隘化しないようにすること。

会員意見募集版

1 コンピュータセンター
(6) コンピュータ室・データ保管室(位置)

適 用 区 分			
セ	本	提	ダ
◎			

設 26	専用の独立した室とすること。

安全管理の徹底のため、専用の独立した室とすること。

1. コンピュータ室・データ保管室を専用の独立した室とする目的は以下のとおりである。
   (1) 防火対策、耐震対策等を講じやすくする。
   (2) 入退室管理により侵入、破壊等の不法行為を防止する。
   (3) 機密の漏洩を防止する。
   (4) 温湿度調整を確実にする。

2. コンピュータ室の一隅をデータ保管場所にしたり、事務室やプログラマ室、消耗品保管庫等と共用したりすることは、入退室管理の徹底を欠くなど、運用管理上問題があり、機密の漏洩、不正行為等が生じやすいため、避けることが必要である。

(参考)
共同利用型システムの場合においては、複数委託元の機器、データを共通のコンピュータ室・データ保管室に保管することも考えられる。
(1) 設備面における入退管理は、【設 16、設 27】を参照
(2) 運用面における入退管理、アクセス権管理は、【実 25、実 28、実 57、実 58、実 69】を参照
(3) 技術面の暗号化は、【実 3】を参照

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(7) コンピュータ室・データ保管室(開口部)

適 用 区 分			
セ	本	提	ダ
○			

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。

入退室管理を確実に行うため、常時利用する出入口は 1 カ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。

1. コンピュータ室・データ保管室の常時利用する出入口は、できるだけ 1 カ所とすることが望ましい。出入口が 2 カ所以上の場合は、確実に 1 カ所と同等の入退室管理を行うことが望ましい。
   また、前室においては、入室者のチェックを確実に行うとともに、外部からの熱、湿気、塵埃の侵入を防止することが望ましい。

2. コンピュータ室の前室の例　【設 16】参照

3. 【設 16】【設 23】【設 103】参照

会員意見募集版

1 コンピュータセンター
(7) コンピュータ室・データ保管室(開口部)

適 用 区 分			
セ	本	提	ダ
◎			

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。

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。

1. コンピュータ室・データ保管室の出入口の扉は、不法侵入、危険物の投込み、延焼の防止等のため、特定防火設備以上の十分な強度を有するものを使用し、錠を付けることが必要である。

2. 扉の錠は、非常時において室内から鍵を用いることなく解錠が可能な機能を有することが必要である。また、出入口を自動ドアにする場合、停電でも開閉できる機能を有することが必要である。

3. 特定防火設備については、【設 14】参照のこと。

会員意見募集版

1 コンピュータセンター
(7) コンピュータ室・データ保管室(開口部)

適　用　区　分			
セ	本	提	ダ
◎			

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。

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ずること。

1. コンピュータ室・データ保管室に窓を設ける場合は、窓に防火、防水、防犯措置および窓ガラスの破損防止措置を講じ、さらに建物外部から室内のコンピュータ機器、データ保管設備等が見えないようにカーテン、ブラインド等で遮蔽できるようにすることが必要である。
   また、コンピュータ室を室外から見学できるようにガラス張りにする場合は、安全管理上の措置を講ずることが必要である。

2. 窓ガラスの破損防止の措置としては、以下のような例がある。
   (1) 窓ガラスに網入りガラス、強化ガラスや防犯ガラス等を使用する。
   (2) 普通ガラスにガラス飛散防止フィルム等を貼付する。

3. 外部から容易に接近できる 1 階等の位置にコンピュータ室・データ保管室を設置するような場合には、外部に面する壁をできるだけ無窓にすることが望ましい。
   無窓にすることにより、以下のような災害等を防止することができる。
   (1) 火災による延焼
   (2) 外部からの侵入、破壊
   (3) 雨水等による漏水
   (4) 直射日光による機器障害

4. 建築基準法、消防法では、避難上または消火活動上有効な開口部を有しない階を無窓階としているが、無窓階には消火器、スプリンクラー設備、自動火災報知設備、避難器具、排煙設備等の設置について、避難上および消火上支障がないようにしなければならないとされている。

（参考）
【設 15】参照

| 参照法令 | 建築基準法第 35 条、消防法施行令第 10 条第 1 項第 5 号、第 10 条第 2 項第 1 号
消防法施行規則第 5 条の 2、第 11 条 |
|---|---|

会員意見募集版

1 コンピュータセンター
(7) コンピュータ室・データ保管室(開口部)

適 用 区 分			
セ	本	提	ダ
◎			

設 30	非常口、避難器具、誘導灯等を設置すること。

災害時の避難と非常持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。

1. 非常口

(1) 非常口は室内の避難通路上に設置し、2 カ所以上設けること。また、コンピュータ室が広い場合は、いくつかの区画に分割して区画ごとに避難通路を設定し、非常口への誘導灯および誘導標識を設置すること。

(2) 非常口は部外者の侵入を防止するため、外から開けられない構造とし、施錠する場合は室内から鍵を用いることなく解錠できること。また、非常口の近くの見やすい場所に、その解錠方法を表示すること。

2. 避難器具

(1) 避難器具は、火災が発生した場合、階段等の避難施設を利用できないときに用いるものである。

消防法では階数に応じて避難器具の種類を表 1 のように定めている。

なお、無窓の室等、避難器具を設けても意味のない場合は、特に設ける必要はない。

表 1　階数による避難器具

	地　階	3　階	4 階、5 階	6 階～10 階
避難はしご	○	○	○	○
避難用タラップ	○	○	－	－
すべり台	－	○	○	○
緩降機	－	○	○	○
避難橋	－	○	○	○
救助袋	－	○	○	○

＊「地階」とは「床が地盤面下にある階で、床面から地盤面までの高さがその階の天井の高さの三分の一以上のものをいう」。

(2) 避難器具の設置については以下の点に注意することが必要である。

①避難器具は、避難に際して容易に接近できる場所にある開口部に常時取り付けておく。

会員意見募集版

②避難器具を設置する開口部は、相互に同一垂直線上に位置しないようにする。
③避難器具の設置場所には、避難器具の使用法を記した標識を設ける。

3. 誘導灯

(1) 誘導灯には、図 1 のように避難口である旨を緑色の灯火で示し、その避難口の上部に設ける避難口誘導灯と、図 2 のように白地に緑色の矢印で避難の方向を示した通路誘導灯がある。

(2) 誘導灯および誘導標識の構造および性能については、誘導灯および誘導標識の基準（平成 13 年消防庁告示第 39 号）に定められている。

図 1　避難口誘導灯

図 2　通路誘導灯

4. 誘導標識

誘導標識は避難口であること、または避難の方向を明示した灯火のない標識であり、多数の者の目に触れやすい場所に設けること。

なお、誘導灯を設置した場合は、誘導灯の有効範囲の部分について誘導標識を設置しないことができるとされている。

参照法令	建築基準法施行令第 125 条の 2、消防法施行令第 25 条、第 26 条、 消防法施行規則第 27 条、第 28 条の 3、平成 13 年消防庁告示第 39 号

会員意見募集版

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）

適 用 区 分			
セ	本	提	ダ
◎			

設 31	独立した防火区画とすること。

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。

1. 建物の構造上、防火区画のデータ保管室を設置できない場合は、火災から一定時間安全に磁気媒体のデータを守る耐火金庫、耐火キャビネット等のデータ保管庫を使用することが必要である。

2. データ保管室以外に分散して保管される各種データについても、重要なデータについては磁気媒体等のデータを守る耐火金庫、耐火キャビネット等のデータ保管庫に保管することが必要である。

参照法令	建築基準法施行令第 112 条

会員意見募集版

＜会員意見募集版＞

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）

適 用 区 分			
セ	本	提	ダ
◎			

設 32	漏水防止対策を講ずること。

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。

1. コンピュータ室・データ保管室の隣室に水を使用する室、設備がある場合の漏水防止対策としては、以下のような例がある。
   (1) 室の床を高くし、段差を設ける。
   (2) 漏水の予想される位置および配水管周辺等に漏水検知器、受皿等を設置する。
   (3) 漏水の流入を防止する防水堤を設置する。
   (4) 漏水を排出する水勾配、排水溝、桶等を設置する。
   (5) 配水管が貫通する部分の直前または設置可能な位置に止水弁を設置する。
   (6) 配水管に地震の振動を吸収する伸縮継手を使用する。

2. 直上階に水を使用する室、設備がある場合の漏水防止対策としては、以下のような例がある。
   (1) 直上階の床板にアスファルト防水工事を施工する。
   (2) 直上階に長尺塩化ビニール等を布設する。

3. 直上階に防水施工ができない場合の措置としては、以下のような例がある。
   (1) 防水カバーを備え付ける。
   (2) 天井面に受皿を設置する。
   (3) 天井面等に漏水検知器を設置する。

会員意見募集版

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）

適 用 区 分			
セ	本	提	ダ
◎			

設 33	静電気の防止措置を講ずること。

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。

1. 静電気の発生、帯電を防止する措置としては、以下のような例がある。
   (1) コンピュータ室の湿度が 30%以下になると、静電気の発生による障害が生じやすくなるので、コンピュータの許容する空調条件（通常 40～60%程度）を満たすように管理する。
   (2) コンピュータ室の床材には静電気を除去する帯電防止フリーアクセスフロア、アースシート等を使用する。
   (3) 導電剤を添加した塩化ビニールタイル、高圧ラミネート、帯電防止カーペット等を使用する。
   (4) 床表面に静電気防止ワックス等、静電気防止剤を塗布する。ただし、静電気防止剤は歩行頻度等により、その有効期間が変わるので注意が必要である。

会員意見募集版

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）

適 用 区 分			
セ	本	提	ダ
◎			

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。

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。

1. 天井、壁等の内装材料やカーテン類を不燃化または難燃化することにより、煙の発生、火災の拡大から室内要員およびコンピュータシステムを守ることができる。

2. 壁、天井等の内装については、建築基準法に規定する不燃材料を使用することが必要である。また、カーテン、じゅうたん等は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が必要である。

3. フリーアクセス床の主要部分（床板、支柱、固定フレーム等）は、不燃材料を使用することが必要である。

4. 不燃材料、防炎性能については、【設 20】参照のこと。

会員意見募集版

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）

適 用 区 分			
セ	本	提	ダ
◎			

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。

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。

1. 室の内部空間に取り付けられた可動間仕切壁は、フリーアクセス床板と天井仕切面下部とで固定されていることが多く、地震時に損壊しやすい。
   間仕切壁の損壊防止対策としては、以下のような例がある。
   (1) 上部を天井面でなく、上階の床板下面に固定し、下部はフリーアクセス床の下の建物床に固定する。
   (2) 柱、壁間に固定した補強材に接続する。
   (3) ガラスを用いる場合は、破損、飛散を防止するため、網入りガラス等を使用するか、ガラス飛散防止フィルム等を貼付する。

2. 天井はつり金具と骨組で上階床からつり下げられていることが多いので、地震時に落下することのないよう、天井ボード等をビス等で固定することが必要である。

3. 照明器具の落下防止措置としては、以下のような例がある。
   (1) 照明器具は上階床または天井骨組に固定する。
   (2) 吊り下げ型照明器具は、金物、鎖等で振れ止めをするか、直付け型とする。
   (3) カバー付照明器具は、カバーの落下防止をする。
   (4) 照明器具の管球落下防止、飛散防止フィルム貼付等による落下時の飛散防止に留意する。

（参考）
【設 21】参照

意見募集版 会員

＜会員意見募集版＞

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)

適 用 区 分			
セ	本	提	ダ
◎			

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。

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。

1. フリーアクセス床は、コンピュータ機器に必要な配線類の布設や空気調和のため、建物床の上に支柱を設けて設置されるが、床板はパネル式で取外しが容易なため、地震時に損壊するおそれがある。このため、本対策により地震時に床板のずれまたは落下、支柱の転倒等のないような耐震補強、もしくは免震床の設置を行うことが必要である。

2. フリーアクセス床の具体的な耐震補強としては、以下のような例がある。

(1) 支柱

支柱は一般に垂直荷重に対しては十分な強度を持っている。

支柱を水平の力に対しても十分な強度を持たせるためには、以下のような措置がある。

①支柱の太さやペデスタルの大きさを大きくした強固な独立支柱を採用するか支柱相互をアングルやストリンガー等で連結する（図 1、図 2）。

②支柱が建物床に接する台をボルト等で固定する。

③支柱を建物床に接着剤で固定する接着工法を採用する。

(2) 床パネル

床パネルは隣接する床板相互が支え合っているため、一部の床板の落下等により、床全体の構造の崩壊につながるおそれがある。

パネルの固定には以下のような措置があるが、この措置はすべてのパネルに行う必要はなく、機器の直下周辺や通路部分を重点的に固定してもよい。

①固定用金具にねじ止めで固定する（図 3）。

②固定クリップを利用する。

③固定用つめの付いたパネルを利用する。

(3) パネルカット部

床下空調の吹出口としてパネルを外した部分には、周囲のパネルが移動しないようにスチール製グリル等をはめ込む（図 4）。

また、ケーブル配線用のカット部分は、補強枠（図 5）、補助支柱、ストッパ（図 6）の取付けを行う。

なお、パネルカットは最小限の大きさにすること。

3. 建物床、壁との間にスプリング等の緩衝器を置くことにより、地震の震動を吸収する、免震構造のフリーアクセス床(免震床)の設置にあたっては以下のような点を考慮し、十分に検討

会員意見募集版

＜会員意見募集版＞

する必要がある。

(1) コンピュータ機器および関連設備（分電盤、端子盤等）の設置位置に制約を受けることがある。

(2) 床下ケーブル布設時のレイアウト、床下スペースに制約を受けることがある。

(3) コンピュータ機器設置の有効床面積が減少する。

(4) ケーブルが固定床との接点で摩耗する可能性がある。

(5) 既存建物に免震床を設置する場合には、採用する免震床システムと既存建物との共振を避けるよう検討する必要がある。

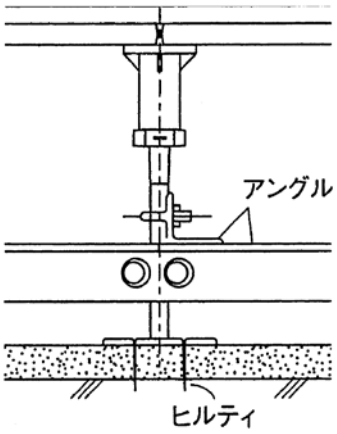


図１　アングルによる根がらみ補強例

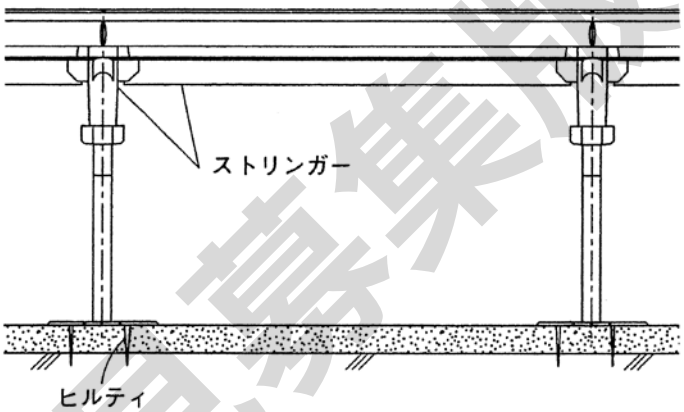


図２　ストリンガーによる補強例

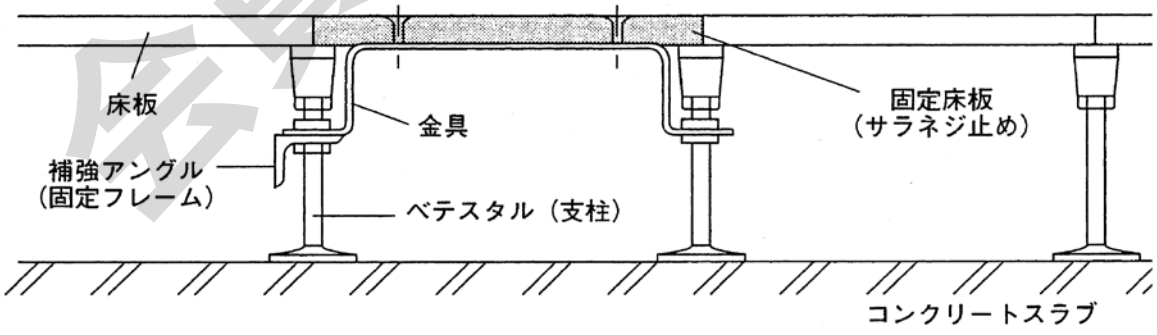


図３　床パネルの固定例

会員意見募集版

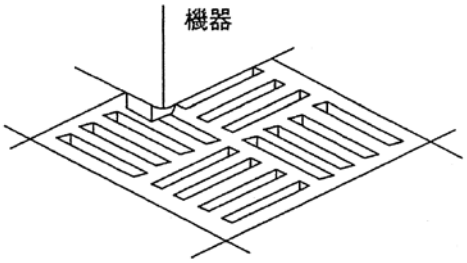


図 4　スチール製グリルの例

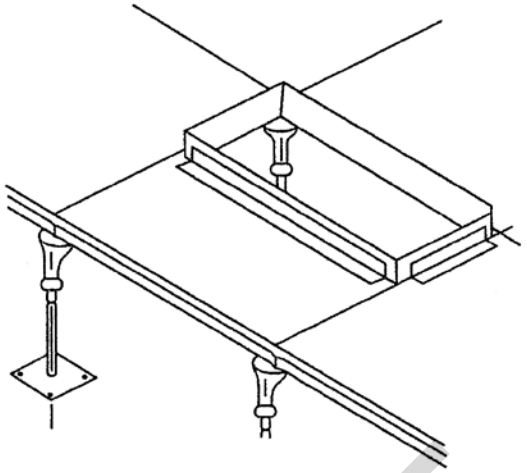


図 5　開口部の補強枠の取り付け

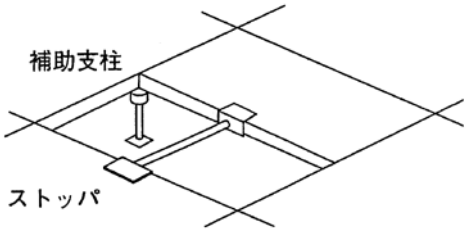


図 6　補助支柱とストッパの例

（参考）亜鉛の導電性ヒゲ状結晶について

電気亜鉛メッキを施したフリーアクセスフロアの床板や支柱から、亜鉛の導電性ヒゲ状結晶（Whisker：以下ウイスカと呼ぶ）が発生し、コンピュータ機器に悪影響を及ぼすケースが（社）電子情報技術産業協会（以下 JEITA と呼ぶ）から報告されている。この現象は、導電性のある亜鉛ウイスカが何らかの原因で剥離し、床下から浮遊しコンピュータ内部に入り込み、プリント基板や端子部分で電気的短絡が発生することにより生じる問題である。事例として、コンピュータ室内の電気メッキを施した床パネル、ストリンガー、支柱、耐震用平鋼等に発生し、これが飛散し悪影響を与えた例がある。

なお、ウイスカの発生は亜鉛だけではなく、錫、カドミウム等もウイスカを発生させることが知られている。また、分電盤のブレーカにウイスカが発生し電気的な障害が発生したことが報告されている。

ウイスカに対する対策としては、以下のような例がある。

(1) ウイスカの発生しない部材の使用

(2) 発生したウイスカの飛散防止

対策に関する詳細は、フリーアクセスフロアメーカー等と相談のうえで検討する必要がある。

社団法人　電子情報技術産業協会（JEITA）のホームページ

http://www.jeita.or.jp/japanese/index.htm

フリーアクセスフロア工業会（JAFA）のホームページ

http://www.free-access-floor.jp/index.htm

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
◎			

設　37	自動火災報知設備を設置すること。

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。

1. コンピュータ室・データ保管室には、高温や煙による損傷を受けやすい機器や磁気媒体が設置されているが、通常はオペレータ等の少数の関係者しかいないことが多い。したがって、火災を早期に発見し対処するため、自動火災報知設備を設置する必要がある。

2. 自動火災報知設備は、火災感知器とその感知状況を通報する受信機とに大別される。
   感知器はさまざまな原理・構造のものがあるが、大別すると熱感知器、煙感知器および炎感知器に分類され、一般に煙感知器が早期に火災を感知するため、広く利用されるようになっている。
   これについては、設備メーカーとも協議のうえ最適な機能のものを選択し、さらには必要に応じて組み合わせて使用することが必要である。
   なお、自動火災報知設備には、商用電源が停電した場合に備えて予備電源を備え付けなければならない。

3. 感知器の取付場所、取付個数等は、感知器の種類により決めることが必要である。火災発生の可能性が高い通信・電力ケーブル類が多量にあるフリーアクセス床の下等にも、設置することが望ましい。

会員意見募集版

（参考）

コンピュータ室では機器冷却のための大量の空調気流が常時室内を循環しているため、火災時に発生する煙は空調気流によって希釈されながら室内全体に拡散され、火災の早期発見が困難な場合が予想される。このような状況でも室内環境の変化を敏感に察知し、火災の予兆を検知できるシステムを設置することが望ましい。

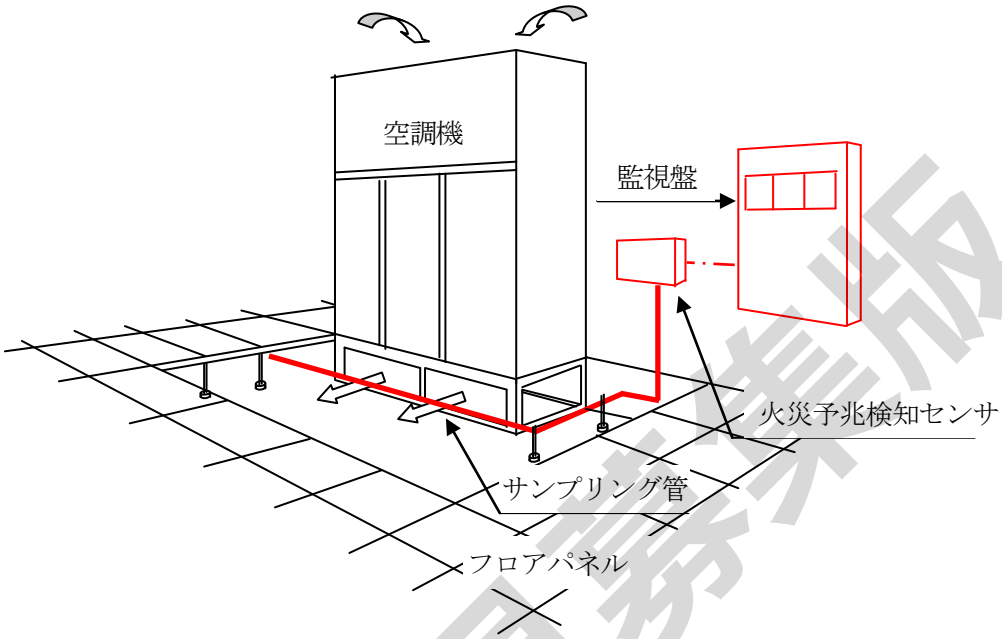


図１　火災予兆検知システム設置例

参照法令	消防法施行令第 21 条、消防法施行規則第 23 条、第 24 条

意見募集版 仮訳

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
◎			

設　38	非常時の連絡装置を設置すること。

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。

1. 非常時の連絡装置としては、非常ベル、警報サイレン、非常放送設備、非常電話等の設備があり、コンピュータ室・データ保管室の状況に合わせて、いずれか、または組み合わせて設置することが必要である。

2. 非常電話の設置により、火災発生時等の非常時に中央管理室（中央監視室、防災センター等）担当部署等への迅速な通報が可能となる。非常電話は防災専用とし、非常時用である旨の表示を行い、非常時の連絡先電話番号を明示しておくなどの措置を講ずることが必要である。また、非常電話はコンピュータシステムの障害発生時の連絡用ホットライン電話とは別回線とすることが望ましい。

3. 非常通報、非常放送等を行う拠点は、迅速な通報や避難誘導等ができるように、常時建物を管理する者が勤務する場所または中央管理室等、建物の防災上の中心となるところに設置することが必要である。

参照法令	消防法施行令第 24 条、消防法施行規則第 25 条の 2

意見募集版 消防庁

＜会員意見募集版＞

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適 用 区 分			
セ	本	提	ダ
◎			

設 39	消火設備を設置すること。

火災時に備えて、適切な消火設備を設置すること。

1. 実際に火災が発生した場合には、消火が速やかに行われるとともに、火災を免れた部分に設置されたコンピュータシステム機器や保管中のデータが損傷を受けずに、消火後速やかに再利用できることが望ましい。そのため、設備業者およびコンピュータメーカーと協議のうえ、適切な消火設備を設置する必要がある。

2. 一般に、コンピュータ室・データ保管室の消火設備としては、消火による機器の損傷の少ないガス系消火設備が適している。その他の消火設備として、スプリンクラー設備も効果的である。
   また、局所的な火災を消火するために、二酸化炭素消火器等のガス系消火器を設置することが必要である。なお、二酸化炭素又はハロゲン化物（ブロモトリフルオロメタンを除く）を放射する消火器の設置には地階・無窓階に関する法令上の制限もあるので注意すること。
   【設 29】【設 99】参照

3. ガス系消火設備
   (1) コンピュータ室のガス系消火設備としては、全域放出型が望ましい。
   全域放出型とは、不燃材料で区画された室全体に消火剤を噴射ヘッドから放射する消火設備であり、図 1 のように、噴射ヘッド、起動装置、音響警報装置、配管、電源、自動火災報知設備の感知器等から構成されている。
   (2) ガス系の消火設備に用いられる消火剤はハロゲン化物消火設備において、ハロン 2402、ハロン 1211、ハロン 1301、HFC-227ea、HFC-23、また不活性ガス消火設備において、窒素、IG-541、IG-55、二酸化炭素が定められている（平成 13 年消防予第 102 号）。
   ハロン 1301 は消火剤として優れた性能をもつが、地球環境保護の立場から現在は生産されておらず、回収されたものを必要不可欠な分野で使用している。
   ガス系消火設備の新設、更改の際は設備メーカー等と十分協議のうえ、対応することが必要である。
   (3) ガス系消火設備を設置する場合は、以下の事項に留意することが必要である。
   ①消火剤の人体への影響を考慮し、使用場所、使用方法を決定する。
   ②消火剤が放出されて危険であることを知らせる放出表示灯を室の出入口等に設ける。
   ③消火後は人に影響を及ぼさずに換気できるよう、換気設備の操作は外部から行えるようにする。

会員意見募集版

④消火剤放出前に消火効果を減ずるおそれのあるダクトを閉鎖できる自動開閉装置を設ける。

⑤HFC-227ea、HFC-23、窒素、IG-55、IG-541 を使用する全域放出型の消火設備を設置した防護区画には、当該防護区画の圧力上昇を防止するための措置（避圧口の設置）を講ずること。

4. スプリンクラー設備

(1) スプリンクラー設備を設置する場合には、プリアクション方式（予作動式）を採用することが望ましい。

プリアクション方式とは、誤作動（ヘッドの不慮の破損等）による水の噴出を防ぐ方式である。図 2 のように、閉鎖型のスプリンクラーヘッド、火災報知器と連動したプリアクションバルブ、メイン立管等で構成されており、通常時はプリアクションバルブとヘッドの間の配管には水が入っていないので、ヘッドが誤作動しても放出されず、また、火災報知器が誤作動してバルブが開いた場合もヘッドが閉鎖型であるので放水されない。

(2) スプリンクラー設備を設置する場合は、以下の事項に留意することが必要である。

①水の被害が拡がらないようにフリーアクセス床下に排水溝等を設ける。

②放出された水の排水と室の乾燥対策を講ずる。

③水に濡れた機器の復旧には時間がかかるので、万一の場合でも主要システムの運転が短時間で可能になるように、本番機と予備機を離して設置する等機器レイアウトに十分配慮する。

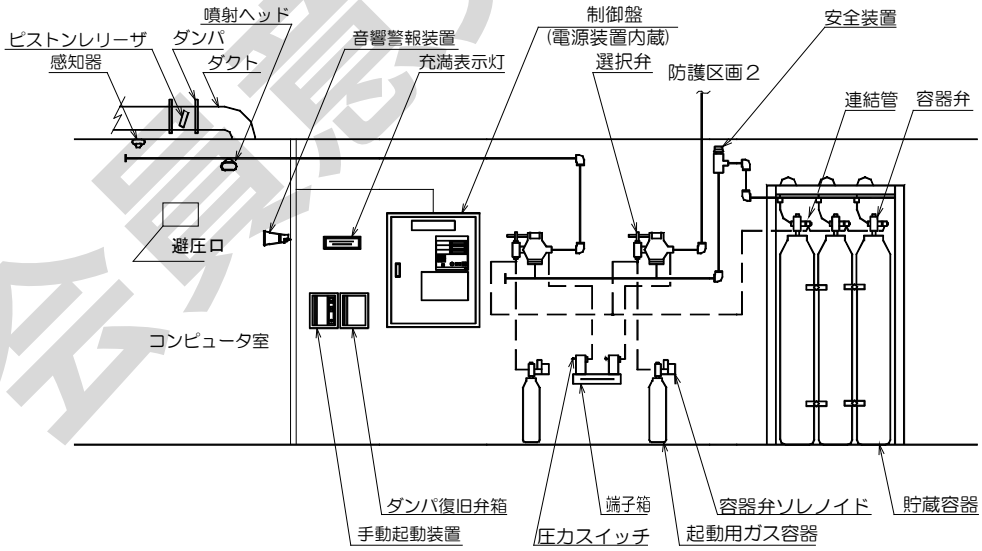


図１　ガス系消火設備の例

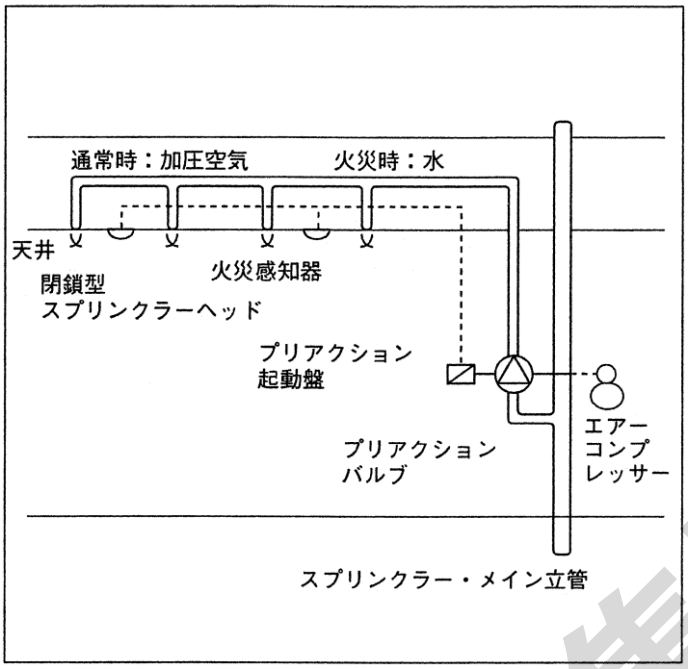


図２　プリアクション方式のスプリンクラー設備の例

（参考 1）ハロゲン化物消火設備の使用について

平成 4 年 11 月に開催された第 4 回モントリオール議定書締約国会議では、特定ハロンの生産を平成 6 年以降全廃し、既存のハロンの回収、再生、リサイクルが決議された。わが国においては本決議に従い、既に生産が廃止されたが、使用そのものは禁止されておらず、既存ハロンのリサイクルによる有効活用策としてハロンバンク推進協議会が設置されている。（平成 3.8.16 消防予第 161 号、消防危第 88 号「ハロゲン化物消火設備・機器の使用抑制等について」）

また、平成 13 年 5 月に使用抑制の見直しが行われ、クリティカルユース（必要不可欠な分野での使用）の考え方が明確に示された。

（平成 13.5.16 消防予第 155 号、消防危第 61 号「ハロン使用抑制等の見直し」）

（参考 2）二酸化炭素消火設備の人体への影響について

二酸化炭素自体には毒性はないが、濃度が約 2%以上になると中毒症状が発生し、人体に対する危険性が発生する。特に、消火用に用いられる濃度は約 35%であり、即時に意識喪失し、その後短時間で生命の危険があることに留意する必要がある。

また、隣接区画に漏洩した事故例もあるため、防護区画だけでなく隣接区画に対しても、人体に対する危険性、避難方法、出入口管理、注意喚起、作業内容の周知等が必要である。

「二酸化炭素消火設備の安全対策について」（消防予第 193 号、消防危第 117 号、平成 8 年 9 月 20 日）

会員意見募集版

参照法令	消防法施行令第 16 条、第 17 条、消防法施行規則第 9 条、第 19 条、第 20 条、平成 13 年消防予第 102 号

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
◎			

設　40	ケーブルの難燃化、延焼防止措置を講ずること。

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、防火壁、床等のケーブル貫通部分は延焼防止措置を講ずること。

1. ケーブルは過電流、周辺の火災等から絶縁体に着火する危険性があり、万一発火した場合、燃焼力が強く、腐食性の燃焼ガスが発生する危険がある。また、ケーブルから発生する煙と有毒ガスによって、火災の熱による直接的被害を受けない範囲にまで二次的災害が及ぶ可能性がある。
   このため、ケーブルの難燃化措置を講ずることが望ましく、防火壁、床等ケーブル貫通部分の延焼防止措置を講ずることが必要である。

2. ケーブルの火災対策としては、難燃ケーブルの使用、延焼防止剤の塗布、ケーブルを鋼板等で囲う等の方法がある。難燃ケーブルとは、不燃性または自消性の被覆を有するケーブルである。延焼防止剤にはケーブルの着火および延焼を防止する塗料と、ケーブルの防火壁貫通部の充填に用いる防火パテ等があり、公的機関で認められた材料を使用することが必要である。

3. ケーブルが耐火構造もしくは防火構造の床または壁面を貫通する場合、火災による煙の進入と延焼を防止するため、図１のようにケーブル貫通部分のすき間にモルタル、ロックウール、防火パテ等の不燃材料を充填するなど、適切な延焼防止措置を講ずること。
   また、ケーブルが防火壁等を貫通する場合、貫通する部分および貫通する部分からそれぞれ両側に１m 以内の部分は不燃材料で造ること。

会員意見募集版

＜会員意見募集版＞

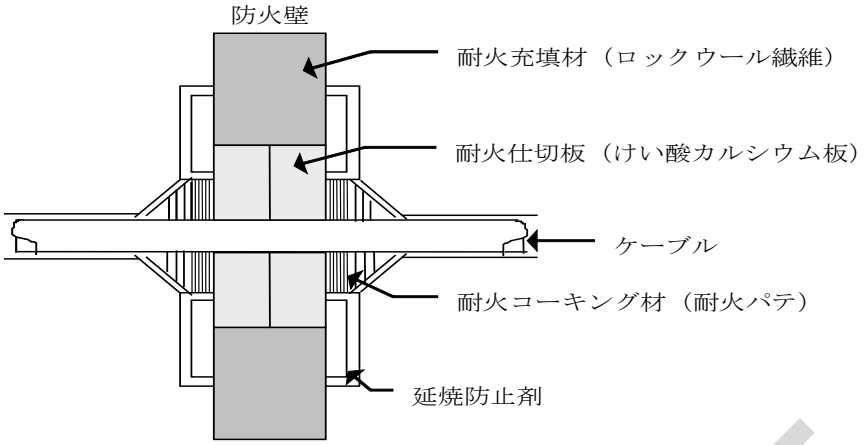


図１　ケーブルが防火壁または床を貫通する場合の延焼防止措置の例

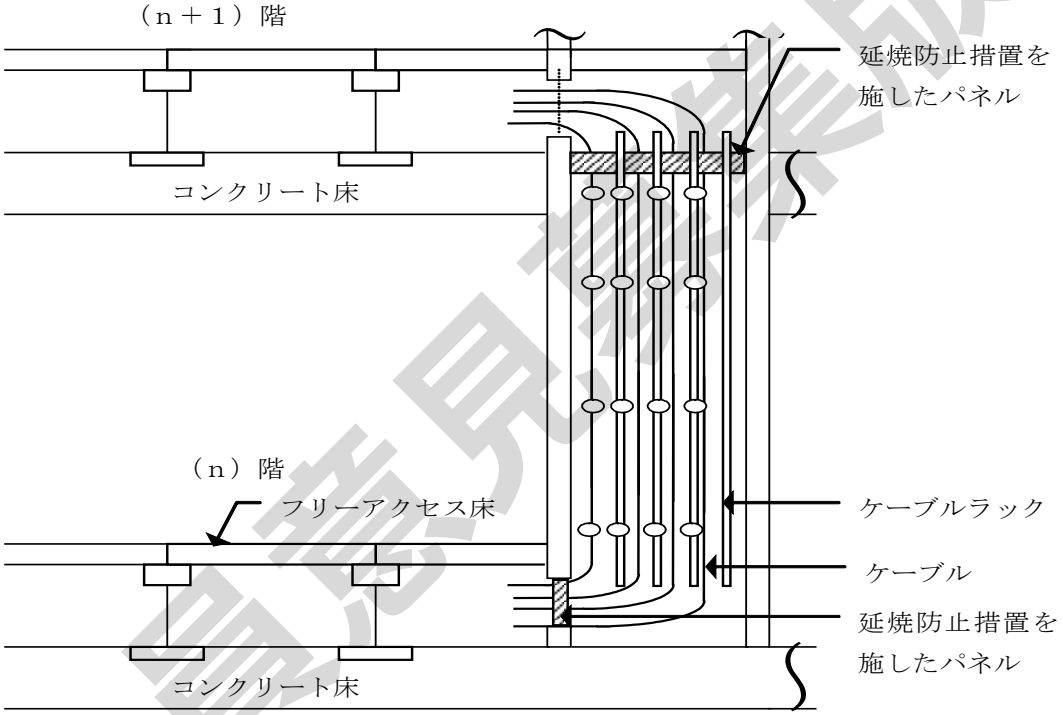


図２　階渡りケーブルダクトの火災対策例

参照法令	建築基準法施行令第 112 条第 15 項

会員意見募集版

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
◎			

設　41	排煙設備を設置すること。

火災時に備えて、必要な排煙設備を設置すること。

1. 火災発生時には、煙を屋外に排出することにより、避難通路等他の部分への漏煙を極力抑えて、安全な避難および消火活動を容易にさせるとともに、コンピュータ機器、データ等の煙による汚損を防止することが必要である。

2. 排煙設備については、排煙口の位置、大きさ、排煙機の性能や自動開放装置等について建築基準法の規定に従い、必要な能力を確保すること。

参照法令	建築基準法施行令第 126 条の 2、3、消防法施行令第 28 条

会員意見募集版

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
◎			

設　42	非常用照明設備、携帯用照明器具を設置すること。

火災等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。

1. 非常用照明設備に必要な構造および性能としては、以下のようなものがある。
   (1) 照明は直接照明とし、床面において 1 ルクス以上の照度を有する。
   (2) 照明器具のうち主要な部分は不燃材料で造るか、または覆う。
   (3) 予備電源を設ける。

2. 非常用照明設備の予備電源は、照明器具の中に電源を持つ電池内蔵型と、1 カ所にまとめて大きな電池を置く電源別置型の 2 種類がある。電池内蔵型は小規模の建築物に使われ、電源別置型は大規模建築物に使われることが多い。

3. 携帯用照明器具とは、携帯可能な懐中電灯等の照明器具をいう。

参照法令	建築基準法施行令第 126 条の 4、5

会員意見募集版

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
◎			

設　43	水使用設備を設置しないこと。

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。

1. 漏水を防止するため、流し台、給湯設備等の水使用設備を設置しない。さらに、壁、天井、直上階の床等からの漏水を防止するため、防水措置を講ずるとともに、漏水に対して迅速に検知できるよう、配水管の周辺には漏水検知器を設置する必要がある。

2. コンピュータ室に、水冷式のコンピュータや空調設備等、水使用設備を設置しなければならない場合、水使用設備の周囲に漏水検知器、受皿、防水堤、排水溝、配水管の設置等、漏水を防止するための措置を講ずることが必要である。

3. 【設 32】参照

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
○			

設　44	地震感知器を設置すること。

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。

1. 地震感知器は震度に応じた防災行動の判断基準ともなり、地震後の震度に応じた各種点検にも利用できる。このため、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。
   なお、運転継続、停止等の具体的判断基準については、メーカー等と、よく協議して決めておくことが必要である。

2. 地震感知器は、設定された規模以上の地震に対して音、ランプによる警報を発し、震度の大きさを表示する。
   警報および震度表示によりコンピュータシステムを手動で停止する場合、前述の判断基準を参考にして責任者が指示し、定められた手順の操作を行う。

3. 地震感知器に連動して自動運転制御をする場合の留意事項としては、以下のような例がある。
   (1) 地震感知器に連動してコンピュータシステム、電源・空調設備の自動運転制御やデータ保護を行う場合は、ハードウェアやソフトウェア等コンピュータシステム全体の連携体制を確保する。
   (2) 地震感知器は、コンピュータ室内またはその近くに設置する。
   (3) 地震感知器は誤動作せず、コンピュータシステム全体の信頼性に見合ったものとする。
   (4) 自動運転制御システム自体が地震に強いものとする。
   (5) 停止させたコンピュータ、空調設備等を復帰させるための動作が簡単なものとする。

会員意見募集版

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
○			

設　45	出入口には出入管理設備、防犯設備を設置すること。

不法侵入を防止するため、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。

1. 出入管理設備としては、以下のような例がある。
   (1) 受付設備
   (2) 開閉装置【設 16】参照

2. 防犯設備　【設 16】参照

3. 出入口の入退室管理を警備員により行う場合においても、防犯設備を併用することにより、管理を徹底することが可能である。

会員意見募集版

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
◎			

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。

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。

1. 温湿度自動記録装置は、コンピュータ室・データ保管室の温湿度を自動的に検出して記録する装置である。
   温湿度警報装置は、定められた温湿度の限界を超えた場合、注意を促し、迅速な対応を図るため警報を発する装置である。
   温湿度自動制御装置と連動した温湿度自動記録装置は、コンピュータ室・データ保管室を規定の温湿度に保つことができ、障害時の原因分析にも役立てることができる。

2. 温湿度を測定する位置は、コンピュータ機器の排気および空調設備からの吹出空気が直接当たる場所、出入口付近等、温湿度の変化の大きな場所を避けて設置することが必要である。

会員意見募集版

1 コンピュータセンター
(9) コンピュータ室・データ保管室(設備)

適　用　区　分			
セ	本	提	ダ
○			

設　47	ネズミの害を防止する措置を講ずること。

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。

1. ネズミの侵入、営巣による回線・電源ケーブルの漏電、接続不良、腐食、断線等によって発生するコンピュータシステムの障害を防止するため、ネズミの害を防止する措置を講ずることが望ましい。

2. ネズミの害を防止する措置としては、以下のような例がある。
   (1) 配管、配線等による壁のすきまを閉鎖する。
   (2) 下水道、排水口、通気口等を金網張りする。
   (3) 忌避剤をケーブル、壁面に塗布する。
   (4) 忌避剤混入ケーブルを使用する。

3. ビル内に厨房、飲食店等、ネズミの生息に適した場所がある場合は、ネズミの被害も多くなりやすいので、食料品の完全格納、残飯等の完全処理等について設備面の配慮が必要である。

会員意見募集

1 コンピュータセンター
(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）

適 用 区 分			
セ	本	提	ダ
◎			

設 48	什器・備品は不燃性とすること。

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。

1. コンピュータ室・データ保管室で使用する什器・備品は、火災時に有害な煙やガス等が発生しないスチール、アルミ等の不燃性の材料でできたものを使用し、可燃性のいす等の持込みは極力少なくすることが必要である。

2. コンピュータ室・データ保管室で使用する消耗品や書類についても、防火上収納方法を考慮することが必要である。

(参考)

サーバー収納ラック・ネットワーク機器収納ラック設置時の注意事項として、ラック内の熱溜まり防止や機器の接地確保などに関しての事例が以下のガイドラインに紹介されている。

「情報システムの設備ガイド」（社）電子情報技術産業協会

会員意見募集版

1 コンピュータセンター
(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)

適 用 区 分			
セ	本	提	ダ
◎			

設 49	静電気防止措置を講ずること。

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。

1. 静電気の発生、帯電を防止する措置としては、以下のような例がある。
   (1) コンピュータ室の湿度が 30%以下になると、静電気の発生による障害が生じやすくなるので、コンピュータの許容する空調条件（通常 40～60%程度）を満たすように管理する。
   (2) コンピュータ室で作業に従事する要員からの静電気を抑制するために、導電性繊維を用いた帯電防止服、導電性ゴムを用いた帯電防止靴などを使用する。
   (3) コンピュータ室には、必要なアースが取れるようにアースの取り口を設ける。
   (4) 可動式什器（磁気テープ等の運搬車等）はスチール製等で静電気が発生しない材質のものを使用する。

会員意見募集版

1 コンピュータセンター
(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)

適 用 区 分			
セ	本	提	ダ
◎			

設 50	耐震措置を講ずること。

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。

1. コンピュータ機器の移動、転倒を防止するための措置としては、以下のような例がある。
   (1) 建物構造体に固定する。
      ①耐震脚で固定する。
      ②移動防止金具、ゴム等で固定する（図 1、図 2）。
      ③転倒防止金具で固定する（図 3）。
   (2) 免震構造で支持する。
      ①免震建築物に収容する。
      ②制振建築物に収容する。
      ③免震床に機器を設置する。
      ④機器ごとに免震構造で支持する。
   (3) 机等に載せる機器は落下防止金具、バンド等で固定する（図 4、図 5）。
   (4) ラック内に設置したモデム等の機器についても落下防止金具、バンド等で固定する。

2. 地震時の移動、転倒によりシステムに影響を与えるような什器・備品、データ保管設備の移動、転倒防止措置としては、以下のような例がある。
   (1) 据置式の什器・備品、データ保管設備等
      ①固定金具で床、壁、天井に固定する（図 6・例 1）。
      ②間隔のある備品は、上部をスチールパイプ等の連結金具で連結する（図 6・例 2）。
      ③背中合せの備品は、上部および下部を連結する。
      ④机の上の備品は机に固定するか、落下防止枠を机に取り付ける（図 6・例 3）。
      ⑤備品の扉や引出しはロック付きとする。
      ⑥扉のない開放棚型のデータ保管設備は、磁気媒体の飛び出し防止ストッパを取り付ける（図 7）。
   (2) 可動式の什器・備品、データ保管設備等
      ①移動式ラックはレールからの脱輪を防止する（図 8）。
      ②台車・いす等は車輪にストッパ、ブレーキ等を取り付ける。

3. コンピュータ機器の移動、転倒を防止する耐震施工方法は、機器の重量、形状、設置場所等により異なる。また、メーカーによっても推奨する施工方法が異なるため、メーカー、建築

会員意見募集版

業者と協議のうえ実施することが必要である。

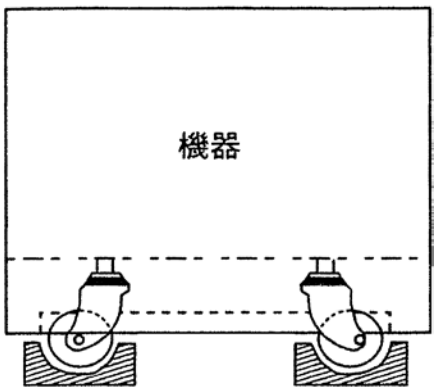


図１　キャスタホルダの例

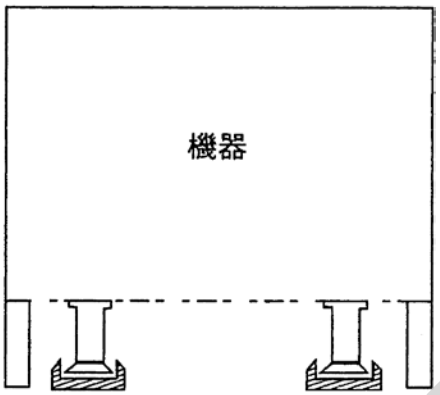


図２　ゴム足の例

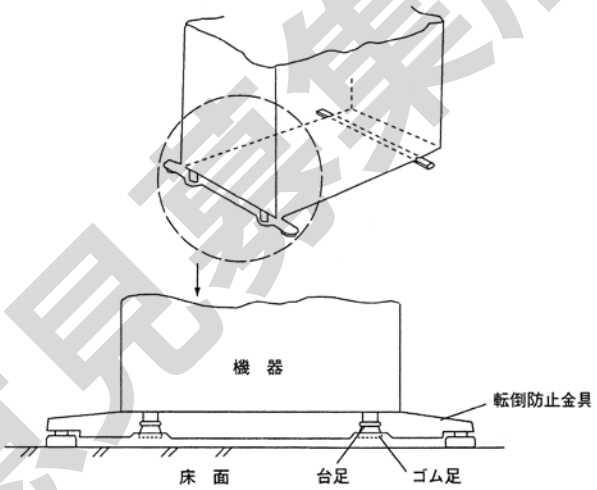


図３　転倒防止金具の取付例

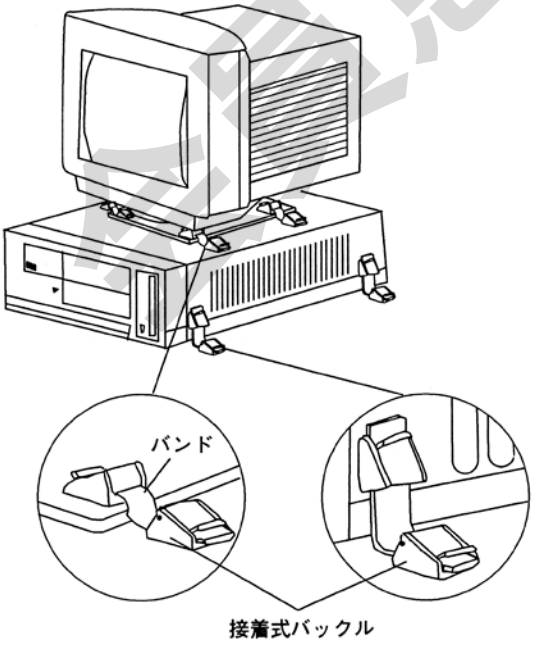


図４　耐震バンドで固定する例

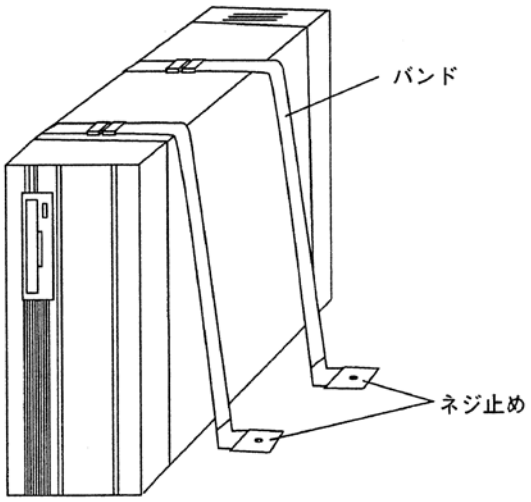


図５　耐震バンド設置例

会員意見募集版

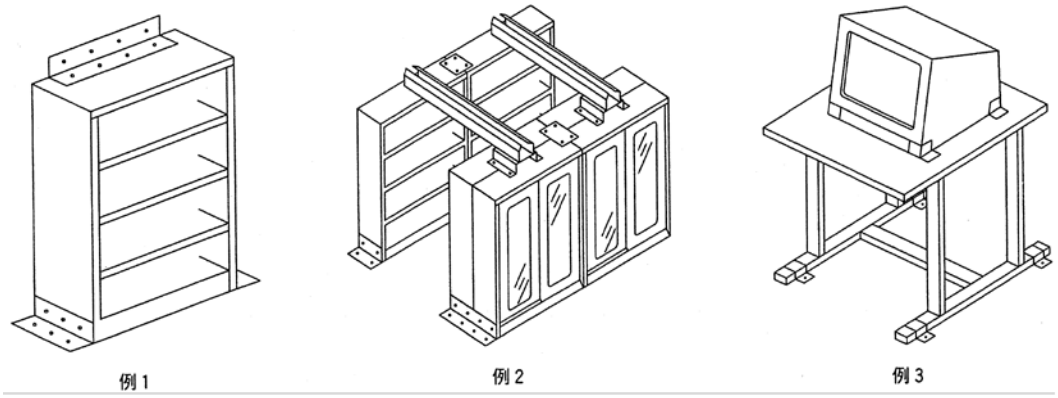


図 6　備品などの固定の例

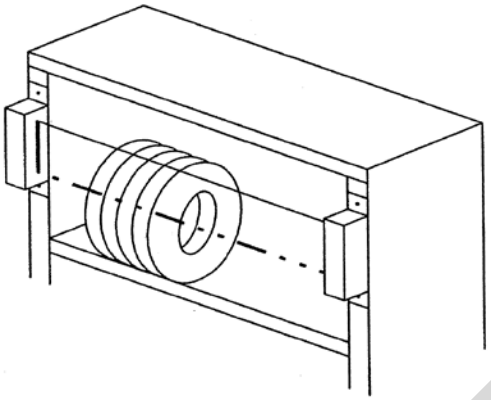


図 7　飛び出し防止ストッパの例

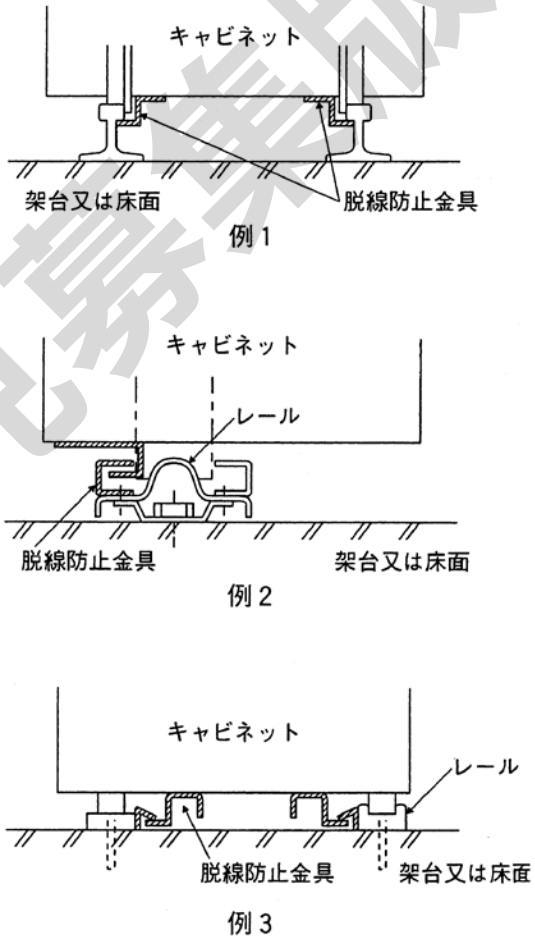


図 8　移動保管庫の固定の例

会員意見募集版

1 コンピュータセンター
(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)

適 用 区 分			
セ	本	提	ダ
◎			

設 51	運搬車等に固定装置を取り付けること。

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。

1. 運搬車等を制動または固定するための装置としては、以下のような例がある。
   (1) 車輪にキャスタストッパ、ブレーキ等を取り付ける（図 1、図 2）。
   (2) ロープ、鎖等により固定する（図 3）。

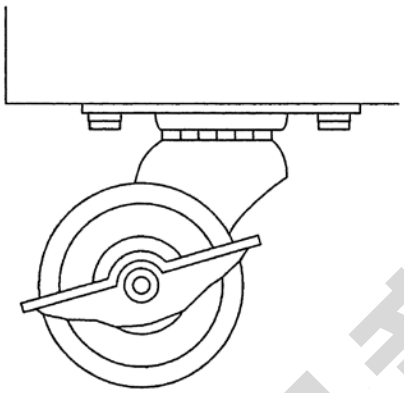


図 1　キャスタストッパの例

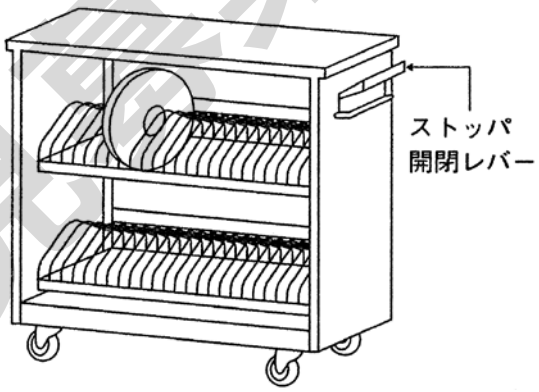


図 2　レバーを離すと車輪にストッパがかかる運搬車の例

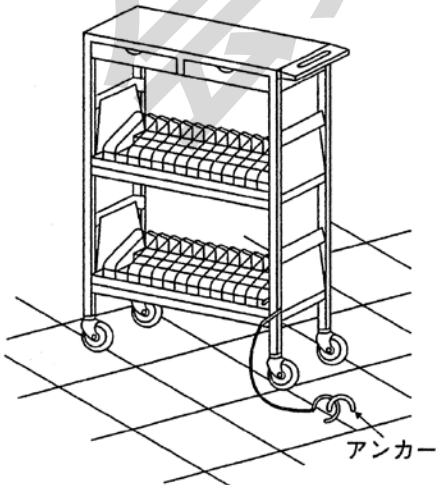


図 3　ロープ等で固定する例

意見募集版

1 コンピュータセンター
(11) 電源室・空調機械室

適 用 区 分			
セ	本	提	ダ
◎			

設 52	災害を受けるおそれの少ない場所に設置すること。

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。

1. 建物内において各種災害を受けるおそれの少ない電源室・空調機械室の場所としては、以下のような例がある。なお、災害を受けるおそれのある場所に電源室・空調機械室をやむを得ず設置する場合は、各種災害による被害防止に必要な対策を講ずることが必要である。
   (1) 地震による震動の少ない場所
   (2) 火災の被害を受けるおそれの少ない場所
   (3) 浸水または水が浸透するおそれの少ない場所
   (4) 危険物貯蔵所、危険物取扱所等の危険物から損傷を受けるおそれの少ない場所
   (5) 可燃性または腐食性の蒸気、ガスもしくは粉塵等の発生するおそれの少ない場所
   (6) 温度が高温、低温になりすぎない場所

会員意見募集版

1 コンピュータセンター
(11) 電源室・空調機械室

適　用　区　分			
セ	本	提	ダ
◎			

設　53	保守点検に必要な空間を確保すること。

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。

1. 電源室・空調機械室の機器の配置については、関係法規に定める距離を有することが必要である。

（参考）

東京都火災予防条例では変電設備の保有距離を表１のように規定している。

表１　変電設備の保有距離

保有距離を確保する部分		保　有　距　離
配電盤	操作を行う面	①1.0m以上 ②1.2m以上：操作を行う面が互いに面する場合
	点検を行う面	0.6m以上
	換気口を有する面	0.2m以上
変圧器、コンデンサ、その他のこれらに類する機器	点検を行う面	①0.6m以上 ②1.0m以上：点検を行う面が互いに面する場合
	その他の面	0.1m以上

（注）東京都火災予防条例施行規則第４条による。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(11) 電源室・空調機械室

適 用 区 分			
セ	本	提	ダ
○			

設 54	専用の独立した室とすること。

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。

1. 保守、管理を容易にするとともに、電源室・空調機械室から発生する障害の拡大を防止するために、電源室・空調機械室は独立した専用の室にすることが望ましい。

2. 専用の独立した室とは、電源室・空調機械室が、コンピュータ室、データ保管室、事務室等と併用されていない室をいう。
なお、室内設置型の電源設備、空調設備を独立した専用の電源室・空調機械室だけでなく、コンピュータ室に設置する場合は、防火、防水等の措置を講ずることが必要である。

3. 通常、電源室・空調機械室は無人のため、錠を取り付けるなど、保守運用者以外の者が入室できないような措置を講ずることが必要である。

4. 電源室・空調機械室については、侵入、破壊等を防止するため、案内板の設置は行わないこと。また、電源室・空調機械室の位置が消防担当者に明示できるよう、電源室・空調機械室の見取図を、建物の入口、中央管理室等で部外者の目に触れないように保管しておくことが必要である。

会員意見募集版

1 コンピュータセンター
(11) 電源室・空調機械室

適 用 区 分			
セ	本	提	ダ
◎			

設 55	無窓とし、錠を付けた扉を設置すること。

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。

1. 通常、電源室・空調機械室は無人で、定時巡回による保守点検が一般的である。このため、電源室・空調機械室はできるだけ無窓とし、錠を付けた扉を設置することにより、外部からの侵入、火災、浸水等を防止することが必要である。

2. 扉は錠を付けた特定防火設備を使用し、十分な強度を持たせることが必要である。特定防火設備については、【設 14】参照のこと。

3. 電源室・空調機械室の出入口は 1 カ所とし、2 カ所以上の場合は、1 カ所と同等の管理を行うことが必要である。

4. 電源室・空調機械室に窓、換気口がある場合は、防災、防犯措置を講ずる必要がある。

5. 【設 29】参照

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(11) 電源室・空調機械室

適 用 区 分			
セ	本	提	ダ
◎			

設 56	耐火構造とすること。

火災による延焼防止のため、耐火構造とすること。

1. 電源室・空調機械室は、建築基準法に規定する耐火構造とすることが必要である。

2. 電気配線等が電源室・空調機械室の耐火構造の壁面等を貫通する場合は、延焼防止措置を講ずることが必要である。

3. 【設 31】参照

参照法令	建築基準法施行令第 112 条

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(11) 電源室・空調機械室

適 用 区 分			
セ	本	提	ダ
◎			

設 57	自動火災報知設備を設置すること。

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。

1. 通常、電源室・空調機械室は無人のため、火災が発生した場合、早期に出火を発見し、中央管理室等に通報して迅速な初期消火ができるよう、自動火災報知設備を設置することが必要である。

2. 感知器としては、熱感知器、炎感知器および煙感知器があるが、電源室・空調機械室の火災報知器としては煙感知器が適している。

3. 【設 37】参照

会員意見募集版

1 コンピュータセンター
(11) 電源室・空調機械室

適　用　区　分			
セ	本	提	ダ
○			

設　58	ガス系消火設備を設置すること。

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。

1. 通常、電源室・空調機械室は無人のため、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。なお、消防法施行令第 13 条で 200 ㎡以上の電源室は、所定の消火設備設置が義務づけられている。

2. 消火器を使用して対応する場合は、火災時に迅速に使用できるよう、出入口付近等扱いやすい場所に配置しておくことが必要である。

3. 【設 39】参照

参照法令	消防法施行令第 13 条

会員意見募集版

1 コンピュータセンター
(11) 電源室・空調機械室

適 用 区 分			
セ	本	提	ダ
◎			

設 59	空調設備の漏水防止措置を講ずること。

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。

1. 空調機械室においては、空調設備の周辺または直下に受皿、防水堤、排水口等を設置することにより、空調設備からの冷却水の水漏れ、結露、ゴミのつまり等による漏水の防止措置を講ずること。

2. 外壁に設置された外気取入口、排気口についても雨水が浸水しない防水構造とすることが必要である。

会員意見募集版

1 コンピュータセンター
(11) 電源室・空調機械室

適　用　区　分			
セ	本	提	ダ
◎			

設　60	ケーブル、ダクトからの延焼防止措置を講ずること。

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。

1. ケーブル、ダクトからの延焼を防止するため、壁面のケーブル、ダクト貫通部分およびこれと近接する部分には延焼防止措置を講ずることが必要である。

2. 【設 40】参照

会員意見募集版

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

設 61	電源設備の容量には余裕を持たせること。

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。

1. ここでいう電源設備の容量とは、変圧器の定格容量、発電機の定格出力、UPS の定格容量および配線の許容電流等をいう。

2. 電源設備が容量の余裕を持つための留意事項としては、以下のような例がある。
   (1) 電源設備の容量は、建物の規模、コンピュータ室の規模、各室に設置された機器の使用量、各室の使用目的や使用条件等を検討し、余裕を見込んで設置する。
   (2) コンピュータシステムの各機器は、変圧器や電動機が実装されているため、電源投入時に突入電流が流れ電源条件を逸脱することのないようにする。
   (3) 電源ケーブルは、瞬時的な電圧変動および配線の長さによる電圧降下等、コンピュータシステム等の各機器に支障を来さないように選定、布設する。
   (4) 保守が容易で信頼性の高いものとする。
   (5) 将来の負荷増に備える必要がある場合は、配線の増設スペースを確保するか、電源室内に増設または上位の容量に取替え可能なスペースを見込んでおく。

3. 電源設備に悪影響を及ぼさないように、コンピュータシステム用の三相電源に単相機器を接続する場合には、設備不平衡率が 30%未満とする。
   (1) 設備不平衡率は、各線間に接続される単相負荷総設備容量（VA）の最大と最小の差と、総負荷設備容量（VA）の平均値の比（%）をいい、次式で表される。

$$\text{設備不平衡率}=\frac{\text{各線間に接続される単相負荷総設備容量の最大最小の差}}{\text{総負荷設備容量の 1/3}}\times 100$$

   (2) 設備不平衡率の算出に当たっては、電源設備からコンピュータシステムまでの範囲を対象とする。したがって、コンピュータシステムの各機器は、内部の回路が単相であるか三相であるかにかかわらず、全体として総負荷設備容量を算出すればよい。

会員意見募集版

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
○			

設　62	電源は複数回線で引き込むこと。

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。

1. 受変電設備に障害が発生した場合においても、コンピュータシステムへの安定的な電力の供給を確保するため、電力会社からの受電は複数の回線で引き込むことが望ましい。

2. 複数回線の受電方法としては、以下のような例がある。
   (1) 本線、予備線 2 回線受電（図 1）
   (2) ループ受電（図 2）
   (3) スポットネットワーク受電（図 3）

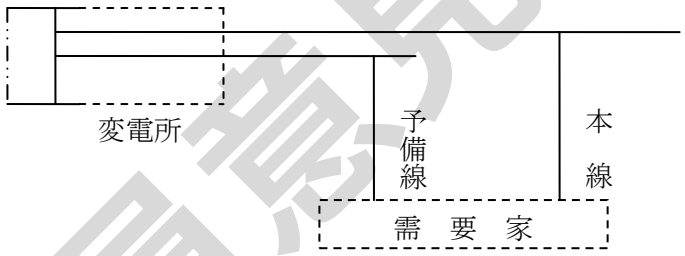


図 1　本線、予備線、2 回線受電の例

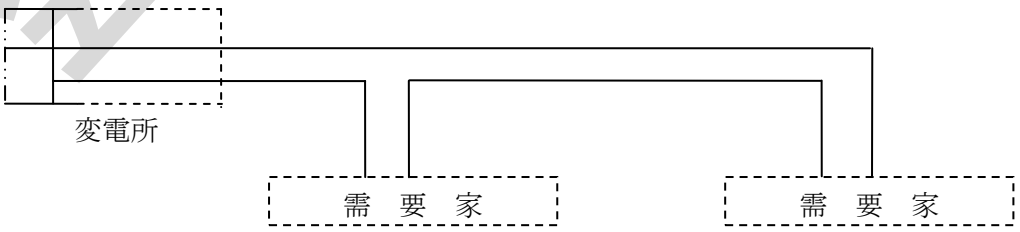


図 2　ループ受電の例

会員意見募集版

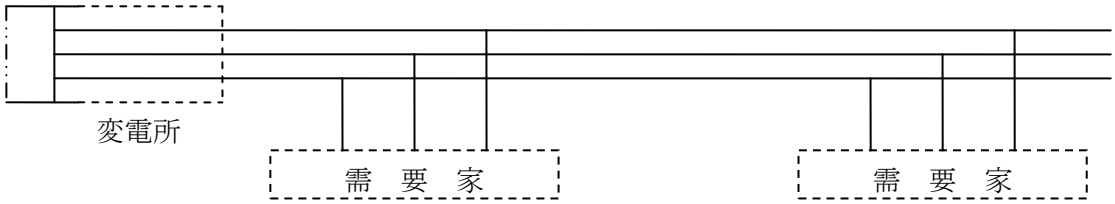


図３　スポットネットワーク受電の例

（参考）
　地域によっては、変電所が障害となった時に他の変電所から送電されるよう、自動的に送電ルートが変更される場合もある。事前に電力会社に確認しておくとよい。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(12) 電源設備

適　用　区　分			
セ	本	提	ダ
◎			

設　63	良質な電力を供給する設備を設置すること。

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。

1. コンピュータシステムを常時安定的に稼働させるため、品質の良い電力を供給することができるように UPS（Uninterruptible Power Supply: 無停電電源装置）を設置することが必要である。
   UPS は、商用電源が短時間停電しても蓄電池から電力を供給し、運転を継続させる機能とともに、CVCF（Constant Voltage Constant Frequency Power Supply: 定電圧定周波装置）の機能を併せ持ち、瞬断、停電等の電源の入力変動や出力負荷の変化に関係なく、コンピュータシステムへ供給する電圧および周波数を一定に保つことができる。

2. UPS は商用電源が長時間停電しても運転を継続できるよう、自家発電設備から電力の供給を受けられるようになっていることが望ましい。この場合には、UPS に接続する蓄電池・充電器等は自家発電設備が起動、出力安定する間、電力を供給できる容量を有することが必要である。過電流を含む UPS 障害時対策としてバイパス無瞬断切替方式をとることが望ましい。
   無停電の電源システムとしては、以下のような例がある。
   (1) 完全独立型並列冗長運転無瞬断バックアップ方式（図 1）
   (2) 待機冗長無瞬断切替方式（図 2）

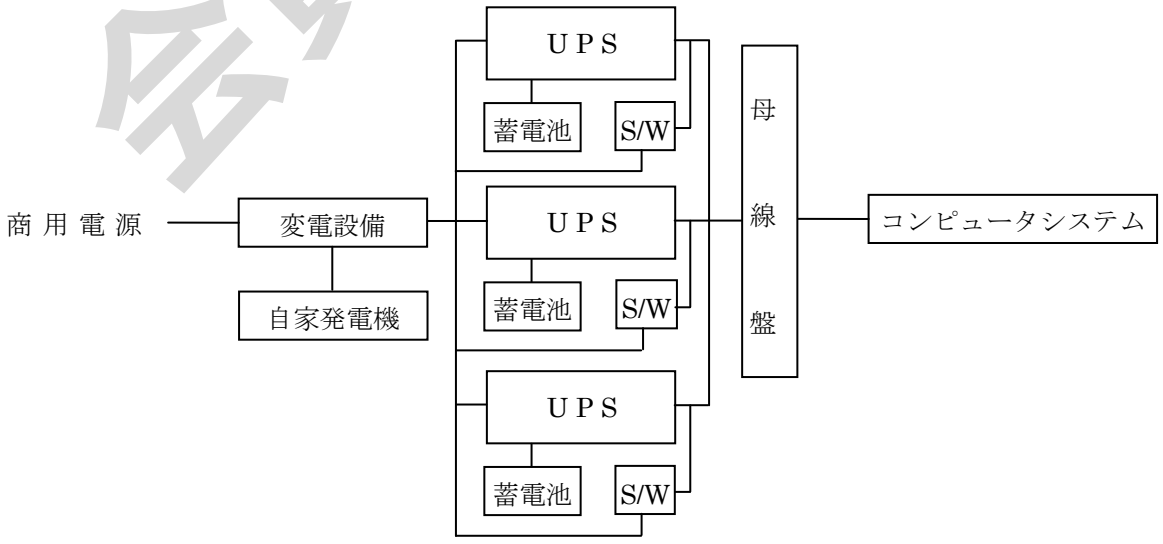


図 1　完全独立型並列冗長運転無瞬断バックアップ方式

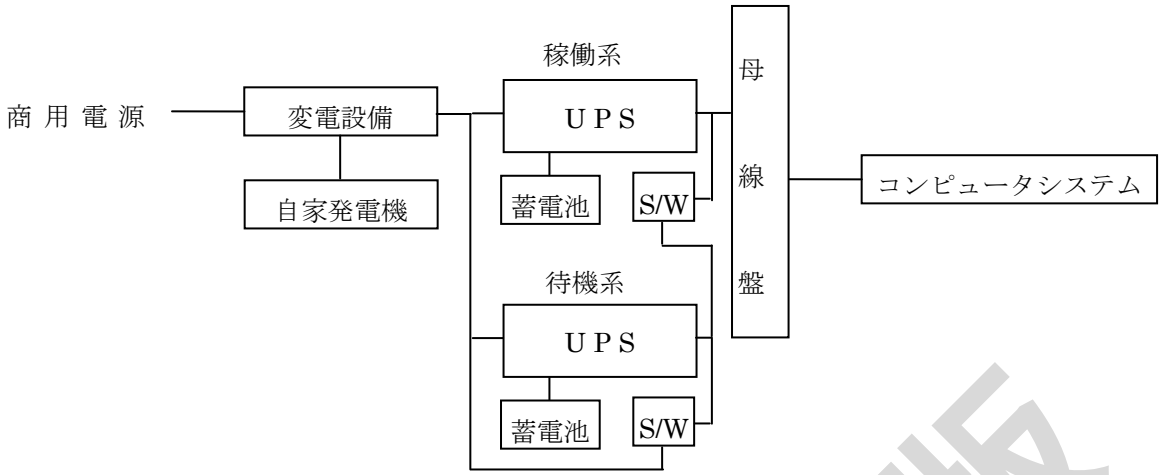


図２　待機冗長無瞬断切替方式

会員意見募集版

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

設　64	自家発電設備、蓄電池設備を設置すること。

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、自家発電設備及び蓄電池設備を設置すること。

1. 自家発電設備は、電力会社から供給されている商用電源が停電した場合、ディーゼル機関またはガスタービン等の原動機により発電機を駆動させ、自動的に電圧確立及び投入が行われて送電する電源設備である。
   自家発電設備の構造、性能等については、商用電源が停電した場合に自動的に電圧確立及び投入が行われるまでの所要時間は 40 秒以内とされるなど、自家発電設備の基準（昭和 48 年消防庁告示第 1 号）において定められている。

2. 蓄電池設備は、蓄電池と充電器を組み合わせ、商用電源が停電したとき自動的に蓄電池設備側に切り替えて送電し、復旧したときは自動的に商用電源側に切り替える電源設備である。
   蓄電池設備の構造、性能等については、蓄電池設備の基準（昭和 48 年消防庁告示第 2 号）において定められている。

3. 自家発電設備からの電力の電圧及び周波数を一定に保つためには、UPS（CVCF）が必要である。
   UPS、CVCF については【設 63】参照のこと。

4. コンピュータシステムの運用に必要となる照明及び空調については、自家発電設備から電源の供給を受けられるようになっていることが望ましい。自家発電設備への電源切替には多少の時間を要するため、コンピュータシステムの状況によってはこの間の温度上昇が問題になる場合がある。温度上昇を抑止するためには、自家発電設備からの給電開始順序を空調優先にする、または UPS 等を利用するなどの対策が考えられる。

5. 非常時に自家発電設備等が稼働した際に利用できる施設、設備、コンピュータシステム等を確認しておくこと。また、それらが必要とする電力量を各機器の追加や更改時等に確認しておくこと。

6. 非常時に自家発電設備や蓄電池設備が正しく機能するよう、定期的に点検すること。
   (1) 自家発電設備
   - 燃料容量（備蓄による運転可能時間）
   - 冷却水（不足時の運転可能時間）

会員意見募集版

・動作確認

(2) 蓄電池設備

・蓄電池容量

・蓄電池更改時期

7. 自家発電設備の稼働時に必要となる燃料等の確保について以下の内容を考慮しておくこと。

(1) 燃料

・燃料の補給体制（燃料供給会社との優先供給契約締結の内容等）

・燃料の補給が不可能となった場合の対策（電力使用の抑制、企業間の相互協力等）

(2) 冷却水

・ライフラインの途絶等による水不足時の補給対策（給水車等による補給等）

参照法令	消防法施行規則第 12 条第 4 号、昭和 48 年消防庁告示第 1 号、第 2 号 危政令第 11 条、第 12 条、第 13 条、第 19 条

会員意見募集版

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

設　65	電源設備には避雷設備を設置すること。

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。

1. 落雷により電源の架線に大きな誘導電圧が発生した場合、電源設備の絶縁破壊等によるコンピュータシステムの障害を防止するため、電源設備の電源引込口にできるだけ接近した場所に避雷設備を設置することが必要である。

2. 避雷設備としては、高圧電路には避雷器、低圧電路には避雷器、電源保護用保安器および異常電圧吸収装置等がある。

（参考 1）内部雷による被害

当該建築物に落雷した時に流れる雷電流、あるいは当該建築物以外に落雷し、雷により誘起された異常電圧・異常電流（雷サージ）が当該建築物と接続されている電源ケーブル等から進入することにより発生する害を内部雷（誘導雷）による被害という。その被害形態としては、以下が挙げられる。

・配電系統の瞬時電圧低下によるシステムダウン
・コンピュータ電源装置破壊
・監視装置、警報装置の破壊　等

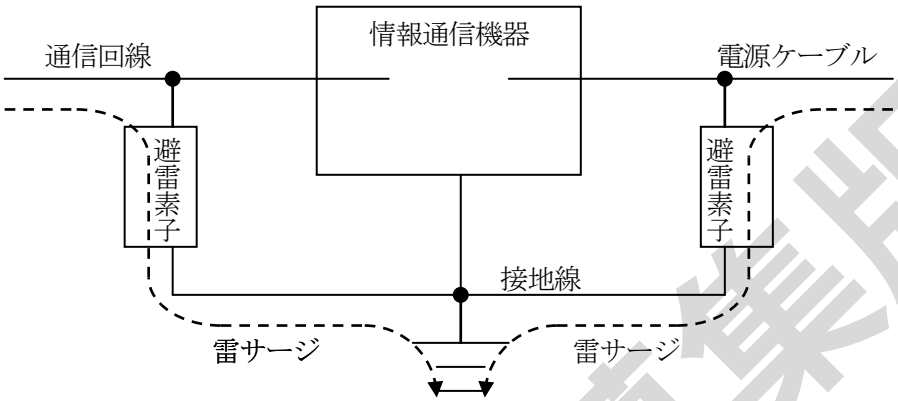
ここで、雷電流および雷サージは、電源ケーブル、通信回線等から機器に進入するので、落雷多発地域において機器障害が多発する場合は、それぞれのラインに対して対策を実施することが有効と考えられる。

会員意見募集版

（参考 2）内部雷対策の例

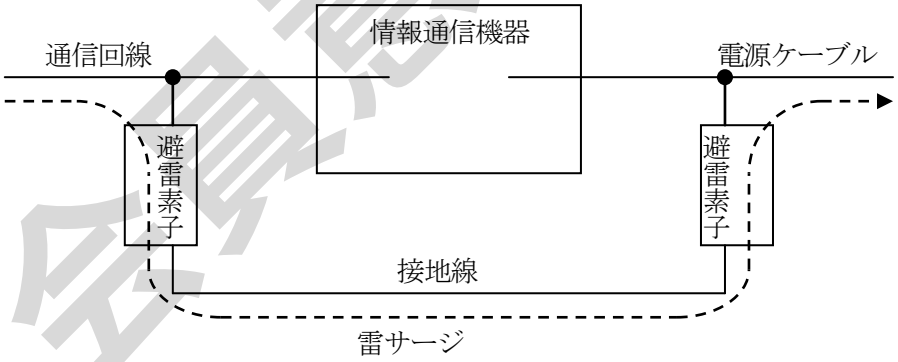
(1) 等電位化

等電位化とは、機器、通信回線、電源ケーブルの電位をすべて同一にすることである。1つの接地にすべての接地を接続する共通接地が用いられる。通信回線や電源ケーブルは直接接地できないために、避雷素子（アレスタやバリスタなど）を介して接地する。これにより、すべての電位が接地点で同電位となり、雷サージが進入しても機器全体が同電位となるため、機器内部に雷サージが流入することがなく機器を保護できる。



(2) バイパス

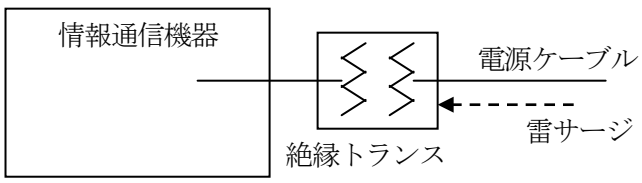
この方法は、接地をとらない機器でよく利用される方法である。通信回線と電源ケーブルのそれぞれに避雷素子を組み込み、その接地側を接続し通信回線と電源ケーブルをバイパスする回路を構成する。雷サージが一方のインタフェースから進入した場合、避雷素子を経由しバイパス回路を流れ、別のインタフェースに流れる経路をとるため、機器の内部回路が保護できる。



注）通信回線から雷サージが進入した場合

(3) 絶縁

絶縁は、雷サージを進入させない方法である。電源ケーブルに絶縁トランスを挿入し、雷サージを通過させない構成にする。



（参照）日本工業規格　JIS A4201(2003)、JIS C 0367-1、JIS C 5381-1、JIS C 5381-21

会員意見募集版

会員意見募集版

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

設　66	電源設備には耐震措置を講ずること。

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。

1. 地震時の震動により電源設備各機器の移動や損傷、配線の短絡、切断等によってコンピュータシステムに障害が発生するのを防止するために、耐震措置を講ずることが必要である。

2. 電源設備の耐震措置として、以下のような例がある。
   (1) 取付部を補強する。
   (2) 配管、配線は天井、壁等に固定またはつり下げる。
   (3) 機器等の接続部に可とう電線管（フレキシブルパイプ）を使用し、室内ケーブルに余裕を持たせる。
   (4) 重量の大きな機器は建物床等の構造体に、図１のような耐震ストッパを取り付け、移動、転倒を防止する。
   (5) 軽量の機器は、床、壁または柱等に固定する。

3. 蓄電池設備については、設置台を補強し、床、壁に固定するなど、転倒、損壊を防止する対策を講ずることが必要である。

4. 地震時に電源設備各機器の機能が停止することがないよう、機器の設置条件、稼働条件等を加味し耐震設計されたものを使用することが望ましい。

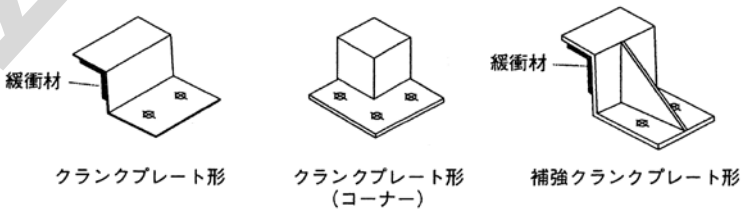


図１　移動・転倒防止形耐震ストッパの例

会員意見募集版 無断複製禁止

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

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。

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。

1. コンピュータシステム以外の機器の電源ケーブルに短絡、漏電、切断等の事故が発生した場合でも、コンピュータ機器や通信関連機器への影響を最小限にするため、コンピュータ機器および通信関連機器の分電盤は専用とするとともに、分電盤からの電源の引込みは他の配線、配管類とは独立してコンピュータ機器ならびに通信関連機器ごとに専用回路とすることが必要である。
   なお、コンピュータ機器１台ごとではなく、入出力装置の種類ごとに専用回路で配線してもよい。

2. 電源室から分電盤への幹線は専用にて配線すること。防火上または誘導障害等の影響を防止するためには金属管工事、金属ダクト工事、可とう電線管（フレキシブルパイプ）工事等を行うことが必要である。
   なお、電源室から分電盤への幹線は事故や点検時の影響を最小限にするため複数にすることが望ましい。

3. 分電盤やコンピュータ機器との配線に生じる磁界が、コンピュータ室の各機器の配線に影響を与えないよう、電磁遮蔽の措置を講ずることが必要である。

4. コンピュータ機器の分電盤は専用とし、部外者が触れないよう、コンピュータ室内に設置して分電盤の露出した通電部分を施錠できる鉄板等で覆うなどの措置を講ずることが必要である。

5. コンピュータ室内で、蛍光灯スタンド、小型掃除機等の電気機器を使用する場合は、コンピュータ機器に雑音（ノイズ）の影響を及ぼさないよう、電気用品安全法に規定する雑音防止器を内蔵したものを使用し、保守作業等のためのコンセントも含めてコンピュータ室への配線とは別の回路を使用することが必要である。

会員意見募集版

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

設　68	負荷変動の激しい機器との共用を避けること。

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と負荷変動の激しい機器との電源系統は分けること。

1. コンピュータシステムと負荷変動の激しい機器とが同一の電源系統を共用している場合にはコンピュータシステムに安定した電力供給が行われないおそれがあるため、負荷変動の激しい機器とコンピュータシステムを同一の変圧器に接続して共用することは避けることが必要である。

2. ここでいう負荷変動の激しい機器とは、エレベータや空調設備等、電源の起動、停止の頻度が高く、消費電力の大きな機器をいう。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

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。

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適切に施工すること。

1. 電源設備や他の電気機器等から発生するノイズ等の悪影響を防止するため、図 1 のようにコンピュータシステムのアースは専用のアース線を独立に接地極より分電盤まで用意する等適切に施工することが必要である。
   なお、コンピュータメーカーによってアースの方式が異なるためメーカーと相談することが必要である。

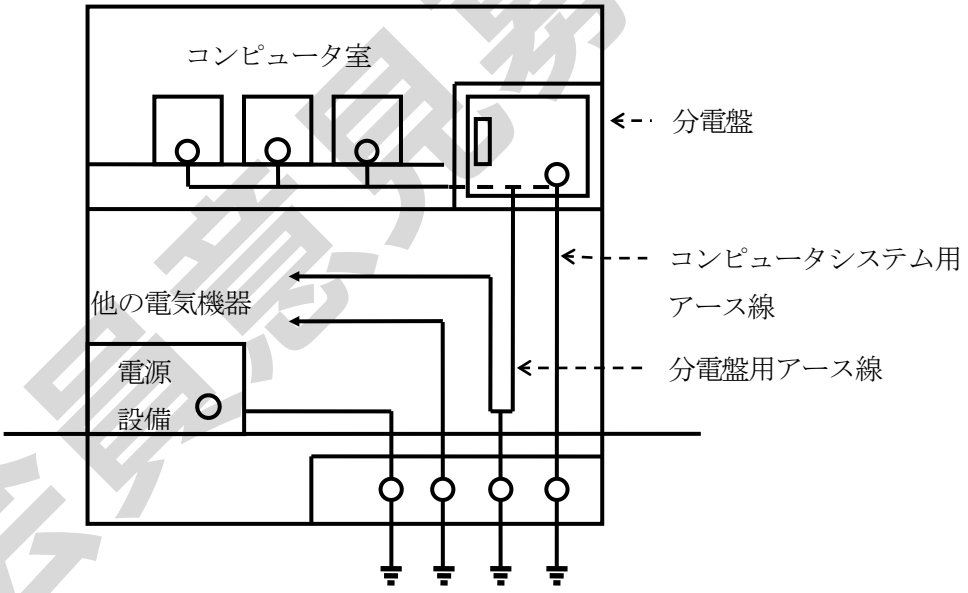


図 1　コンピュータシステムのアースの例

(参考)
日本工業規格（JIS C 0364　建築電気設備）では、接地端子を専用としない「共用接地方式」を採用している。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(12) 電源設備

適　用　区　分			
セ	本	提	ダ
◎			

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。

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。

1. コンピュータシステムの回路が漏電したとき、感電、火災の発生を防止するため、漏電警報器を分電盤の回路に設けることが必要である。なお、コンピュータメーカーによって設置方法が異なるため、設置にあたってはメーカーと相談することが必要である。

2. 空調設備用の回路についても、漏電したとき、感電、火災の発生を防止するため、漏電警報器を設けることが必要である。

3. 過電流による配線及び電気機器の過熱、焼損を防止するため、過電流遮断機を設置することが必要である。

4. コンピュータシステムの低域濾波器（ラインフィルタ）に許容値以上の透過電流が流れる場合は、絶縁変圧器を設置して非接地系にて配電する方法があるが、メーカーに相談して適切な措置を講ずることが必要である。

（参考）
　低域濾波器は、外来の電気的雑音によって機器が誤動作することを防止するため、機器の電源側に装着される。低域濾波器は雑音除去の立場からは容量の大きい方が望ましいが、容量が大きいと透過電流が大きくなり、感電の危険および真の漏電検出の妨げとなる。

協議会 意見募集版

1 コンピュータセンター
(12) 電源設備

適 用 区 分			
セ	本	提	ダ
◎			

設 71	防災、防犯設備用の予備電源を設置すること。

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。

1. 地震、火災等により商用電源の供給が停止した場合においても、要員の安全な避難とコンピュータシステムへの影響を最小限にするため、防災、防犯設備を正常に作動させる予備電源の設置が必要である。
   ここでいう予備電源とは、防災、防犯設備に給電している商用電源が停電等により断たれた時、所定の時間、防災、防犯設備の機能を確保するための電源で、自家発電設備や蓄電池設備等をいう。

2. 建築基準法、消防法では、防災設備ごとに予備電源の種類を表 1、表 2 のように規定している。

3. 防災、防犯設備の電線については、火災時に溶断しないように、耐火、耐熱電線を使用するか、または耐熱保護することも重要である。

参照法令	建築基準法施行令第 126 条の 3、5、7 等、消防法

会員意見募集版

＜会員意見募集版＞

表１　建築基準法による防災設備と適応防災電源

防災設備＼防災電源		自家発電設備	蓄電池設備	自家発電設備と蓄電池設備との併用	容量（以上）
排煙設備	特別避難階段の付室	○	○	－	30 分間
	特殊建築物等				
	地下街の各構えの接する地下道				
	非常用エレベータの乗降ロビー				
非常用の照明位置	避難階段、特別避難階段	＊１ ○	○	＊２ ○	30 分間
	特殊建築物等				
	地下街の各構えの接する地下道				
	非常用エレベータの乗降ロビー				
非常用の進入口（赤色灯）		○	○	－	30 分間
非常用の排水設備	地下街の各構えの接する地下道	○	○	－	30 分間
非常用エレベータ		○	－	－	60 分間
防火戸		○	○	－	30 分間
ダンパー		○	○	－	30 分間

備考　本表の記号は、以下のとおり。

○　：適応できるものを示す。

－　：適応できないものまたはほとんど用いられないものを示す。

（注）＊１：10 秒以内に始動するものに限る。

＊２：10 分間容量の蓄電池設備と 40 秒以内に始動する自家発電設備に限る。

会員意見募集版

表２　消防法による防災設備と適応防災電源

防災設備＼防災電源	非常電源専用受電設備	自家発電設備	蓄電池設　備	自家発電設備と蓄電池設備との併用	容　量（以 上）
屋内消火栓設備	△	○	○	－	30 分間
スプリンクラー設備	△	○	○	－	30 分間
水噴霧消火設備	△	○	○	－	30 分間
泡消火設備	△	○	○	－	30 分間
不活性ガス消火設備	－	○	○	－	60 分間
ハロゲン化物消火設備	－	○	○	－	60 分間
粉末消火設備	－	○	○	－	60 分間
自動火災報知設備	△	－	○	－	10 分間
ガス洩れ火災警報設備	－	－	○	○＊	10 分間
非常警報設備	△	－	○	－	10 分間
誘導灯	－	－	○	－	20 分間
排煙設備	△	○	○	－	30 分間
非常コンセント設備	△	○	○	－	30 分間
無線通信補助設備	△	－	○	－	30 分間

備考１　本表の記号は、以下のとおり。

○　：適応できるものを示す。

△　：特定防火対象物以外の防火対象物または特定防火対象物で延べ面積 1,000 ㎡未満のものにのみ適応できるものを示す。

－　：適応できないものを示す。

備考２　本表は、消防法施行令及び同施行規則によったもので、地方条例によって若干相違する場合があるので注意を要する。

（注）＊　１分間以上の容量の蓄電池設備と 40 秒以内に始動する自家発電設備に限る。

（参考）

予備電源を利用する機器として考慮すべきものに、緊急時の連絡手段である電話等の通信設備（PBX 等の構内交換機や IP 電話等のネットワーク機器等）がある。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(13) 空調設備

適 用 区 分			
セ	本	提	ダ
◎			

設 72	空調設備の能力には余裕を持たせること。

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。

1. コンピュータシステムの障害を防止するためには、空調設備に能力の余裕を持たせ、コンピュータ室に設置された機器類に対し温湿度を適切な状態に保つことが必要である。
   空調設備がコンピュータ室の温湿度を適切に調整できるように能力の余裕を持たせるため、以下のような点に留意することが必要である。
   (1) 耐久性、保守管理の容易性等を考慮して設置する。
   (2) 建物の構造、コンピュータ室の規模、各室に設置された機器の発熱量や各室の使用目的および使用条件等を検討して、最大負荷熱量で空調能力を決定する。一般的に、コンピュータ室、事務室、電源室、空調機械室等にあっては、個々に空調条件を設定する。
   (3) 空調設備の熱分配機能は、間取りの変更等、空調条件の変化に対し、あらかじめ柔軟性を持たせる。
   (4) コンピュータ室の将来の負荷増加に対応できるよう、空調設備の増設スペースを確保することが望ましい。

会員意見募集版

1 コンピュータセンター
(13) 空調設備

適 用 区 分			
セ	本	提	ダ
◎			

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。

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。

1. 空調設備には汚染された外気、塵埃等の侵入を防止するため、外気取入口および外気と再循環空気とが混合する箇所にフィルタによる除塵や集塵器の設置等、適切な措置を行うことが必要である。

2. 空調設備に利用する補給水は水質の良いものを使用し、定期的な水質検査により、水質が悪い場合は必要に応じて水処理装置を設けることが必要である。

3. 寒冷地または冬季において冷却塔の循環水が凍結するのを防止するため、水温を検知して設定温度で作動する電気ヒーターを取り付けた場合、作動時に水量の減少により過熱しない措置を講ずることが必要である。

4. 空調設備の外気取入口、排気口、煙突先端、冷却塔等は、給気と排気とが互いに短絡して機能が低下しないように風向き等を考慮し、相互の位置を決めることが必要である。

5. 冬季に空調設備を使用する場合は、次のような点に留意することが必要である。
   (1) 水冷式空調設備は、冷却水温を調整するため、冷却水温度制御装置を設置する。
   (2) 空冷式空調設備は、外気の低下により機能が低下しないよう、風量制御装置および圧力調整装置を設置する。

6. 空調設備のドレントラップは管部をU字形等に曲げて水封したもので、悪臭や汚染空気の侵入を防止し、空調設備と外部との圧力差を利用して外部に排水するが、安定的に空気調和するためにはドレントラップの内面が平滑で汚物が付着しにくいこと、内部の点検、掃除がしやすく、構造が簡単であることなどが必要である。

7. 空調設備の運転は振動が伴うため、各種機器、ダクト、配管類は設置場所により振動を防止できる構造にすることが必要である。

8. 床下吹出しによりコンピュータ機器の空調を行う場合、各種ケーブル等の積み重なりにより適切な空調が阻害されることがあるので注意することが必要である。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(13) 空調設備

適　用　区　分			
セ	本	提	ダ
◎			

設　74	空調設備はコンピュータ室専用とすること。

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。

1. コンピュータ室の空調設備については、コンピュータ機器に適切な一定範囲の温度、湿度を維持する機能が求められる。このため、熱源製造部分以外の空調設備は事務室等他の室との共用を避け、コンピュータ室専用の空調設備とすることが必要である。
   また、空調設備をコンピュータ専用とすることによって、保守管理が容易となる。

2. 空調設備をコンピュータ室専用とすることにより、コンピュータ室の空調設備の障害時に、他の室の空調設備をコンピュータ室用に切り替えて使用することも可能である。

3. やむを得ず空調設備を他の室と共用する場合は、以下のような点に配慮することが必要である。
   (1) 共用している空調設備の障害がコンピュータ機器への適切な温湿度の供給に影響を及ぼさないように、予備機を設置すること。【設 75】参照
   (2) 共用する室とダクトがつながっている場合、コンピュータ室への延焼を防止するための措置、または共用する室にコンピュータ室と同一レベルの防火対策を講ずること。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(13) 空調設備

適　用　区　分			
セ	本	提	ダ
○			

設　75	空調設備の予備を設置すること。

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。

1. 空調設備は、各機器が一貫した関連性を持っているので、各機器の障害がコンピュータシステム全体の機能に影響を及ぼすことがある。
   このため、空調設備の主要な機器については複数台の設置により運転を行い、一部機器に障害が発生してもコンピュータシステムへの適切な空調が行えることが望ましい。複数台設置することにより、【設 72】の空調設備の能力の余裕を持たせることも可能である。

2. 空調設備の主要な機器としては、以下のような例がある。
   (1) 熱源装置……冷凍機、冷却塔、ボイラー
   (2) 空気調和機……空調機、加湿器、パッケージユニット
   (3) 搬送装置……ポンプ、送風機

会員意見募集版

1 コンピュータセンター
(13) 空調設備

適　用　区　分			
セ	本	提	ダ
◎			

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。

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。

1. 空調設備の自動制御装置は、温湿度の変動に的確に反応するため、室内温湿度や空調機器の運転状態等の監視、空調機器の最適制御等の遠隔操作を集中的に行うものである。

2. 空調設備の冷却水の温度、圧力および冷媒圧力等を自動制御し、稼働状態を確認するため、ポンプ、熱源装置および熱交換装置の吸込側、吐出側には圧力計、温度計を設置することが必要である。

3. 空調設備のタンク類、加湿器、排水受皿等は、異常増水、渇水による火災の防止やコンピュータ室への漏水を防止するため、異常警報装置を設置することが必要である。

4. 自動制御装置の故障時には、自動から手動に切り替えて、空調設備を停止することなく、継続して運転できる措置を講ずることが必要である。

会員意見募集版

1 コンピュータセンター
(13) 空調設備

適 用 区 分			
セ	本	提	ダ
◎			

設 77	空調設備には侵入、破壊防止対策を講ずること。

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。

1. ビルの屋上、敷地内等、建物の外部に設置された空調設備については、部外者の侵入、破壊の防止対策を講ずることにより、コンピュータシステムに影響を及ぼさないようにすること。

2. 部外者の侵入、破壊に対する防止対策として、以下のような例がある。
   (1) 空調設備への通路扉等に施錠し、特定者以外が出入りできないようにする。
   (2) 空調設備の周囲に金網等の囲いを設け、囲いの出入口に施錠する。
   (3) 空調設備の蓋、点検出入口等に施錠する。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(13) 空調設備

適 用 区 分			
セ	本	提	ダ
◎			

設 78	空調設備には耐震措置を講ずること。

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。

1. コンピュータシステムへの影響を最小限にするためには、空調設備には耐震措置を講じ、地震時の損壊を防止することが必要である。
   また、地震時に空調設備各機器の機能が停止することがないよう、機器は設置条件、稼働条件等を加味し、耐震設計されたものを使用することが望ましい。

2. 空調設備の耐震措置としては、以下のような例がある。
   (1) 地震時に空調設備が移動および転倒しないように、床、壁、天井等に堅固に取り付ける。
   (2) コンピュータ室のフリーアクセス床上にパッケージ型の空調設備を設置する場合は、フリーアクセス床の耐震補強をするか、建物床、壁に固定する（図 1）。
   (3) 屋上に設置する空調設備は、地震等に対して安全なように、可とう管継手、耐震支持材等を使用する（図 2、3）。
   (4) 空調設備の振動を吸収するため防振措置を施している場合、地震時に平常運転時の振幅以上の変位が起こらないようにストッパを取り付ける（図 4、5）。

3. 配管、ダクトの耐震措置としては、以下のような例がある。
   (1) 地震による震動、建物の変位等により損傷を生ずることがないように、変位を吸収する継手等を使用する。
   (2) 壁、床、天井に沿った配管、ダクトは、適切な間隔でふれ止めの耐震支持を行う（図 6）。

参照法令	建築基準法施行令第 39 条

会員意見募集版

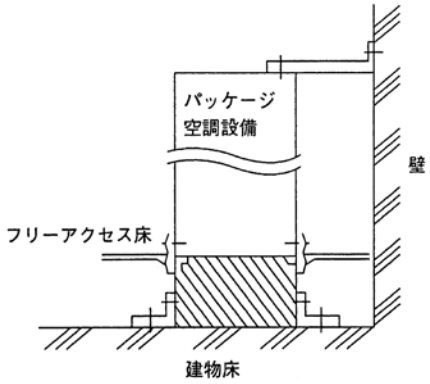


図１　空調設備の固定の例

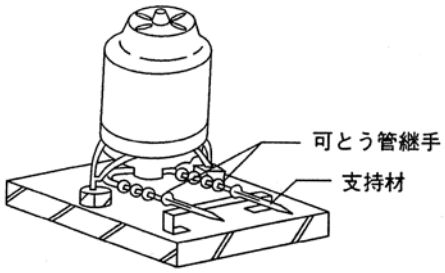


図２　冷却塔まわり配管接続の例

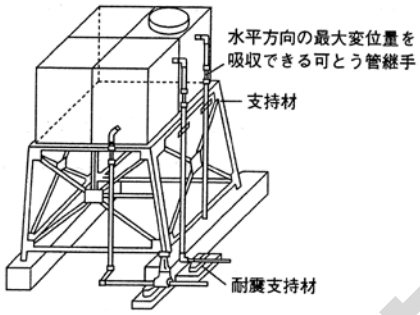


図３　高架台の例

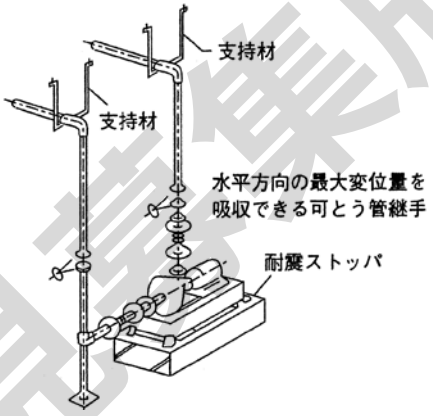


図４　防振されている機器への配管接続の例

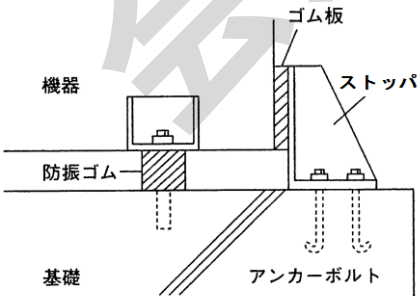


図５　ストッパ取付けの例

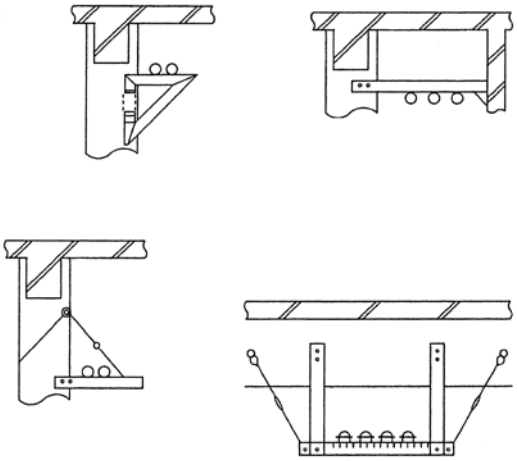


図６　配管の耐震支持の例

会員意見募集版

1 コンピュータセンター
(13) 空調設備

適 用 区 分			
セ	本	提	ダ
◎			

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。

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給排気口は不燃材料とすること。

1. 火災時における断熱材料および給排気口からの煙の発生と火災による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は、燃焼せず、防火上有害な変形、溶融、亀裂等の損傷が生じない不燃材料を用いることが必要である。

2. 空調設備のダクトが防火区画を貫通する場合は、貫通する部分またはこれに近接する部分に防火ダンパーを設置すること。またダクトの吹出口および吸込口は、不燃材料とすることが必要である。

3. 空調設備の配管、継手、弁類および伸縮継手は、熱による変形から起こる圧力変動や火災による機器の損傷防止を図るため、耐火性に優れ、十分な強度を有する金属性の材質のものを使用することが必要である。

4. 空調設備がパッケージ型の場合でも、特にファン、フィルタ等の構成部分は不燃材料または難燃処理したものを用いることが必要である。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(14) 監視制御設備

適　用　区　分			
セ	本	提	ダ
◎			

設　80	監視制御設備を設置すること。

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。

1. コンピュータセンターの複雑化した各種設備について管理運営の円滑化を図り、障害発生等を早期に発見するためには、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が必要である。
   なお、これらの設備を１カ所で操作できるように、集中監視制御設備を設置することが望ましい。

2. 監視制御の対象となる設備としては、以下のようなものがある。
   (1) 電源設備：受変電設備、自家発電設備、UPS（蓄電池＋CVCF）等
   (2) 空調設備：熱源設備、空調機 等
   (3) 防災設備：自動火災報知設備、ガス漏れ火災警報設備、漏電火災警報器、地震感知器、非常通報装置、非常放送設備、消火設備、排煙設備、換気設備、漏水検知器 等
   (4) 防犯設備：出入監視設備、防犯センター 等
   (5) その他　：エレベータ運行設備 等

会員意見募集版

1 コンピュータセンター
(14) 監視制御設備

適 用 区 分			
セ	本	提	ダ
○			

設　81	中央管理室を設置すること。

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。

1. 中央管理室（中央監視室、防災センター等）は、コンピュータセンターの平常時および災害等の非常時の中枢であり、室自体の防災対策や入退室管理等の防犯対策を講ずる必要がある。

2. コンピュータセンターの構造や中央管理室の運用形態により、電源設備、空調設備等を管理する中央監視室と防災設備、防犯設備等を管理する防災センターのように複数の室に機能を分散する場合がある。各室の特性に合わせ、設置場所や防災、防犯対策を講ずることが望ましい。

3. 建築基準法では、高さ 31m を超える建築物等には、避難階またはその直上階もしくは直下階に中央管理室の設置が義務づけられている。建築基準法、消防法では、中央管理室で集中管理する必要のある設備として、以下のようなものがある。
   (1) 機械換気設備
   (2) 中央管理方式の空調設備
   (3) 排煙設備
   (4) 消防機関へ通報する火災報知設備
   (5) スプリンクラー設備の自動警報装置
   (6) 自動火災報知設備の受信機
   (7) ガス漏れ火災警報設備の受信機
   (8) 漏電火災警報器の音響装置
   (9) 非常警報設備である放送設備の増幅器および操作部

   集中管理の対象となる設備については【設 80】参照のこと。

4. 自治体の火災予防条例（例: 東京都火災予防条例）で設置場所、構造、機能が規定されていることがあり注意が必要である。

会員意見募集版

参照法令	建築基準法施行令第 20 条の 2 第 2 号、第 126 条の 3 第 11 号、消防法施行令第 23 条第 2 項、消防法施行規則第 14 条第 1 項第 4 号ニ、第 24 条第 2 号ニ、第 24 条の 2 の 3 第 1 項第 3 号へ、第 24 条の 3 第 3 項第 3 号イ、第 25 条の 2 第 2 項第 3 号ル

会員意見募集版

1 コンピュータセンター
(15) 回線関連設備

適　用　区　分			
セ	本	提	ダ
◎			

設　82	回線関連設備には錠をつけること。

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。

1. 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た MDF、IDF、回線終端装置等回線関連設備の機器収容架等が関係者以外に触れられるおそれのある場合、収容架等に錠を付けること。

2. コンピュータ室内に設置された回線終端装置等回線関連設備の機器収容架等については、コンピュータ室の前室で入退室管理を行うことにより、錠と同じ機能を持たせることができる。

会員意見募集版

1 コンピュータセンター
(15) 回線関連設備

適　用　区　分			
セ	本	提	ダ
◎			

設　83	回線関連設備の設置場所の表示は付さないこと。

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。

1. 部外者による破壊等を防止し、コンピュータネットワークの安全性を確保するため、回線関連設備については、看板、表示板等設置場所の表示は付さないことが必要である。

会員意見募集版

＜会員意見募集版＞

1 コンピュータセンター
(15) 回線関連設備

適 用 区 分			
セ	本	提	ダ
○			

設 83-1	回線は、専用の配線スペースに設けること。

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。

1. 回線の配線専用スペースとしては、以下のような例がある。
   (1) LAN 等の回線を、専用の金属管、金属ダクト、配線ピット等に布設する。
   (2) 統合配線システムを導入する。
   統合配線システムとは、従来別々に配置されていた「情報線」と「電話線」を、1 種類のケーブル（ツイストケーブル）に統合して配線する方法のことである。
   オフィス内のケーブルすべてをパッチパネルと呼ばれる「情報線・電話線分岐盤」で 一元管理する点が特徴。レイアウト変更時は、手近にある OA コンセントに電話や OA 機器を接続し、その後パッチパネルで系統を切り替えることにより対応可能である。

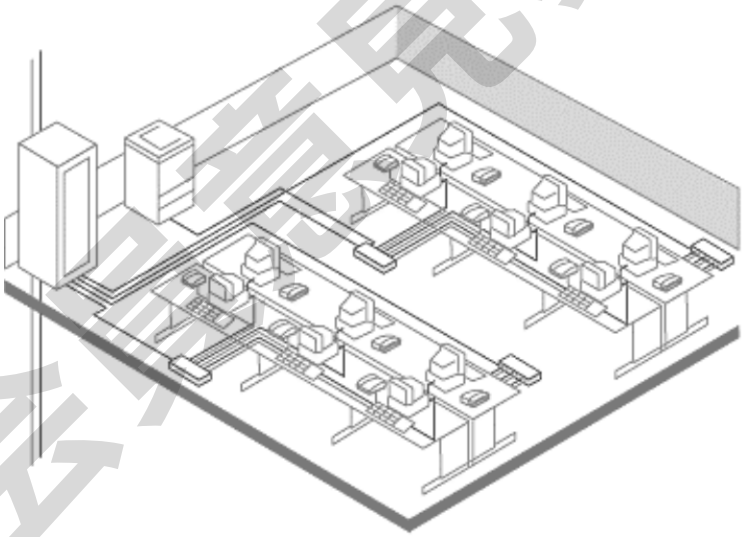


図 1　統合配線システムによる配線の例

＜会員意見募集版＞

2 本部・営業店等
(1) 建物(周囲)

適 用 区 分			
セ	本	提	ダ
	○		

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。

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。

1. 本部・営業店等の敷地内に布設された通信回線・電力線は、ガス・水道等の埋設工事、架空線工事、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。

2. 通信回線・電力線の施工にあたっては引込み工事を行う電話会社または電力会社と事前に協議を行ったうえで切断、延焼の防止措置を講ずることが望ましい。

3. 【設 9】参照

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(2) 建物(構造)

適 用 区 分			
セ	本	提	ダ
	○		

設　85	耐火建築物であること。

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。

1. 建築基準法では、耐火建築物および耐火建築物と木造建築物の中間に準耐火建築物を規定している。
   本部・営業店等の建築構造としては、耐火性能および安全性の観点から耐火建築物が望ましい。【設 10】参照。

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(2) 建物(構造)

適 用 区 分			
セ	本	提	ダ
	◎		

設　86	構造の安全性を有すること。

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。

1. ここでいう構造の安全性とは、建物の自重、積載荷重、積雪、風圧ならびに地震等の震動および衝撃に対して、現行の建築基準法に規定する構造の安全性を有することをいう。

2. 現行の建築基準法は、施行または適用の際に現存する建築物について、現行建築基準法に適合しない部分を有する場合、これを適用しないとしている。
しかしながら、旧建築基準法で建築された本部・営業店等に構造の安全性の問題がある場合は、現行の建築基準法に準じた構造の安全性を有するように配慮することが望ましい。

3. 『建築物の耐震改修の促進に関する法律』に従い、特定建築物に該当する場合は耐震診断を行い、必要に応じて耐震改修を行うことが必要である。

4. 【設 11】参照

会員意見募集版

2 本部・営業店等
(2) 建物(構造)

適　用　区　分			
セ	本	提	ダ
	◎		

設　87	外壁、屋根等は十分な防水性能を有すること。

漏水を防止するため、十分な防水性能を有するように措置を講ずること。

1. 外壁、屋根等の長年の使用による防水、排水性能の低下、または排水能力を超えた豪雨や、排水口にゴミが詰まった場合等の漏水によって、端末機器等コンピュータシステムに障害を及ぼさないよう、漏水の防止措置を講ずることが必要である。

2. 【設 12】参照

会員意見募集版

2 本部・営業店等
(2) 建物(構造)

適 用 区 分			
セ	本	提	ダ
	○		

設　88	外壁等の強度を確保すること。

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。

1. 公道等外部に面する外壁、窓、自動化コーナー等に強度を持たせることにより、建物内部のコンピュータ関連設備を破壊行為、および犯罪等から防御することが望ましい。

2. 破壊行為等から防御できる外壁の例としては、鉄筋コンクリート造、カーテンウォールのうち防犯強度を有するもの等がある。カーテンウォールとは、建物の荷重支持の機能を持たせない薄い壁で、材質としては金属パネル、鉄筋コンクリート材等多様であり、一般にはパネル化されて工場で生産される。カーテンウォールに防犯機能を持たせる場合は、十分な強度を有するものを選択することが必要である。
   また、ガラスには、防火、防犯用のガラス等がある。

会員意見募集版

2 本部・営業店等
(3) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
	◎		

設　89	窓には防火措置を講ずること。

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。

1. ここでいう延焼のおそれのある窓とは、窓と隣地境界線、道路中心線または同一敷地内の 2 つ以上の建築物相互の外壁間の中心線との距離が、1 階にあっては 3m 以下、2 階以上にあっては 5m 以下の場合をいう。

2. 耐火建築物および準耐火建築物にあっては、外壁の窓等開口部で延焼のおそれのある部分に防火設備または特定防火設備の基準を満たす構造の設備を有していなければならない。
防火設備の例としては、窓枠を不燃材料のスチールサッシまたはアルミサッシとし、網入りガラスを入れたものがある。

3. 【設 14】参照

会員意見募集版

2 本部・営業店等
(3) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
	◎		

設　90	窓・扉には防犯措置を講ずること。

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。

1. 外部から容易に接近、侵入できる 1 階等の窓や扉に防犯措置を講ずることにより、本部・営業店等の建物内への不法な侵入等を防止することが必要である。

2. 窓や扉の防犯措置としては、以下のような例がある。
   (1) 防犯用のガラス
   (2) 開閉可能な鉄格子またはシャッター
   (3) 窓や扉の開閉を磁気の動作により感知するマグネットスイッチ
   (4) ガラスの破壊時に生ずる特定高周波等を感知する振動感知器
   (5) 扉の内・外側に設置する赤外線リレー警報装置
   (6) 防犯カメラ、防犯ビデオ 【設 103】

3. 【設 15】参照

会員意見募集版

2 本部・営業店等
(3) 建物(開口部)

適　用　区　分			
セ	本	提	ダ
	◎		

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。

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。

1. 出入口の扉を火災等の非常時または営業時間外に閉鎖し、施錠できる防火構造とすることによって、延焼、不法侵入、危険物の投込み等を防止し、端末機器等コンピュータシステムへの影響を防止することが必要である。

2. 出入口の扉は、十分な強度を有する特定防火設備が望ましい。

3. 扉の錠は複数設置することが望ましい。

4. 【設 19】参照

会員意見募集版

2 本部・営業店等
(3) 建物(開口部)

適　用　区　分			
セ	本	提	ダ
	◎		

設　92	通用口には、入室者の識別設備を設置すること。

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。

1. 部外者の侵入による営業室内の端末機器の破壊等を防止するため、営業時間外に利用する通用口にはインターホン、防犯カメラ、ビデオ装置等の入室者の識別設備を設置することが必要である。【設 103】

2. 通用口の入室者の管理方法の例としては、図 1 のように、通用口に設置されたインターホンとの通話を室内のインターホン親機で行い、防犯カメラ等で入室者を確認したうえ、扉の錠を室内から解錠する等の措置がある。

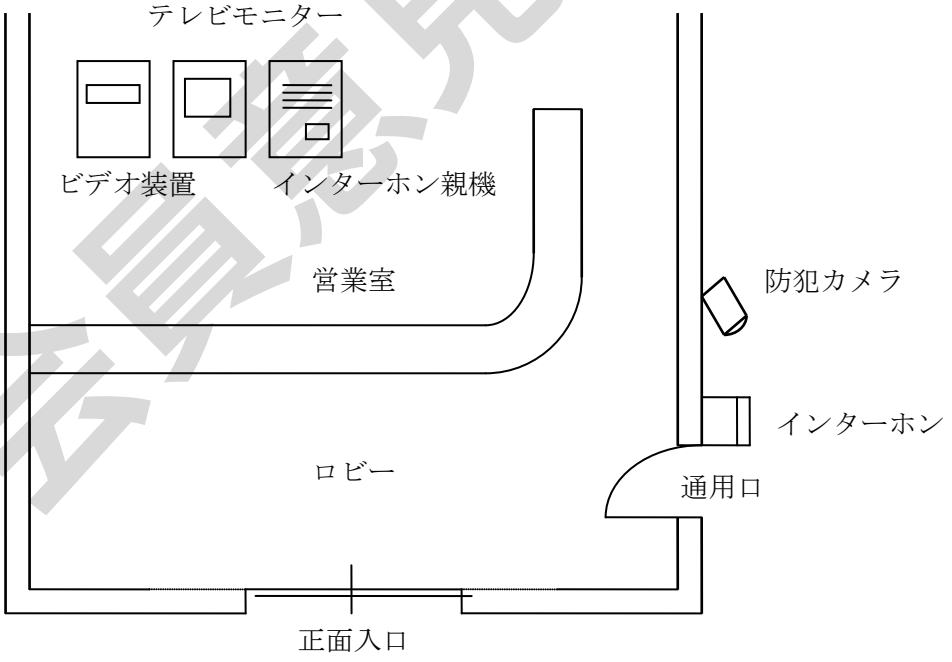


図 1　通用口の入室者識別設備、防犯設備の例

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(3) 建物(開口部)

適 用 区 分			
セ	本	提	ダ
	○		

設　93	出入口には防水措置を講ずること。

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。

1. 営業室の出入口に雨水等の浸水のないよう防水措置を講ずることにより、端末機器等へ被害を及ぼさないようにすることが望ましい。

2. 強風を伴う降雨等による営業室の出入口の防水措置としては、以下のような例がある。
   (1) 出入口扉、シャッター、回転ドア等の補強
   (2) 排水溝、防水堤、防水板、防水扉等の設置
   (3) 防水用砂袋の設置

3. 出水の危険性のある地域においては、上記の防水措置のほかに、営業室内への浸水を想定して、端末機器はじめ各種設備、重要書類等の浸水防止対策を講ずることが望ましい。

会員意見募集版

2 本部・営業店等
(4) 建物(内装等)

適 用 区 分			
セ	本	提	ダ
	○		

設　94	天井および壁は、遮熱、吸音機能を持たせること。

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。

1. 天井および壁は、安定した空気調和のための遮熱機能を有するとともに、端末機器等の騒音を吸収するための吸音機能を持たせることが望ましい。

2. 遮熱機能とは、室内の冷暖房の損失を防ぎ、端末機器等に必要な条件を保つ機能をいう。
遮熱材料の例としては、ポリスチレンフォーム保温板、ロックウール保温板、グラスウール保温板等がある。

3. 吸音機能とは、端末機器等から発生する騒音を吸収する機能をいう。
吸音材料の例としては、グラスウール吸音板、ロックウール吸音板、吸音テックス等がある。

会員意見募集版

2 本部・営業店等
(4) 建物(内装等)

適　用　区　分			
セ	本	提	ダ
	◎		

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。

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。

1. 天井、間仕切壁、照明器具、衝立等が、地震の際に落下・損壊しないような措置を講ずることが必要である。

2. 時計、防犯カメラ、掲示板、装飾品等を設置する場合は、人の動線付近または端末機器の上部空間を避けるか、取付強度を十分にして落下を防止することが必要である。

3. 【設 35】参照

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(4) 建物(内装等)

適 用 区 分			
セ	本	提	ダ
	○		

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。

端末機器等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。

1. 床表面は、塵埃や静電気が発生しにくい塩化ビニールタイル、高圧ラミネート、カーペット等の材質にすることが望ましい。

2. 静電気の発生を防止するためには、導電剤を添加した塩化ビニールタイル、高圧ラミネート、帯電防止カーペット等を使用することが必要である。
   また、床表面に静電気防止ワックス等、静電気防止剤を塗布する場合は、歩行頻度によりその有効期間が変わるので注意が必要である。

3. サーバー機器の設置にあたっては、【設 33】に準ずる静電気防止措置を講ずることが望ましい。

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(4) 建物(内装等)

適　用　区　分			
セ	本	提	ダ
	◎		

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。

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。

1. 端末機器への回線、電源ケーブル等は、損傷をうけたり、切断されることがなく、保守が容易なように床下の配線用の溝（ピット）、低床式のフリーアクセス床等を通すことが望ましい。
   なお、フラットケーブルを使用する場合は、カーペットの下に通すことも考えられる。

2. 構造上、床上に露出する場合は、職員や移動式キャビネット等の通行時に損傷をうけたり、切断されることのない位置を選んで布設するか、プロテクターを用いるなど、回線等を保護する措置を講ずることが必要である。
   プロテクターとは、図 1 のように回線または電源ケーブルを床または壁に固定し、保護するための金属製または合成樹脂製の角型または半丸の管をいう。

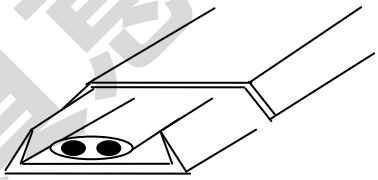


図１　プロテクターの例

会員意見募集版

2 本部・営業店等
(4) 建物(内装等)

適 用 区 分			
セ	本	提	ダ
	○		

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。

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、電源ケーブル等は漏水防止対策を講ずることが望ましい。

1. 漏水防止対策を講ずることにより、端末機器への回線、電源ケーブル等に対する障害を未然に防止することが必要である。

2. 漏水防止措置については、以下のような例がある。
   (1) 空調機、給湯室等からの漏水が端末機器設置場所に流れこまないように、設備面を考慮する。
   (2) 床下の配線用の溝(ピット)を使用している場合は、浸水したときの排水方式を考慮する。

会員意見募集版

2 本部・営業店等
(5) 建物(設備)

適 用 区 分			
セ	本	提	ダ
	◎		

設 99	自動火災報知設備および消火器を設置すること。

火災が発生した場合、早期に発見、通報して、避難ができるよう、煙感知器等を用いた自動火災報知設備を設置し、初期消火を行うための消火器を設置すること。

1. 火災が発生した場合、早期に発見、通報して、避難ができるよう、煙感知器等を用いた自動火災報知設備を設置することが必要である。自動火災報知設備については、【設 37】参照。

2. 火災時に備えて、適切な消火器を設置する必要がある。消火器には、以下に示すように火災の標識が表示されており、適応する消火器を設置することが必要である。
   (1) A火災（一般火災）に適応するもの：白の円に「普通火災用」の黒文字
   (2) B火災（油火災）に適応するもの　：黄色の円に「油火災用」の黒文字
   (3) C火災（電気火災）に適応するもの：青色の円に「電気火災用」の白文字

地色：白色　文字：黒色　　地色：黄色　文字：黒色　　地色：青色　文字：白色

3. 電子機器が存在する場所に設置する消火器としては、放射時に電子機器に対する影響が少ない消火器が望ましい。なお、電子機器が存在する場所に設置する消火器には以下の例がある。

   (1) 純水ベース消火器
   純水を主成分とする消火液を霧状にして放射するもので、他の水系消火器とは異なり電子機器に放射しても短絡等の危険性は少ないため、電子機器が存在する場所に適している。なお、電子機器の発錆等を防止するため、放射後は消火液の拭き取り、乾燥を行う。

   (2) 二酸化炭素消火器
   ガス系消火器であり、周囲を汚損することはないが、窒息消火のため消火範囲が限定的である。また、密閉された狭い室内での使用は窒息作用に注意する他、以下のような禁止設置場所が法令で定められている。
   ①地下街、準地下街
   ②換気について有効な開口部の面積が床面積の１／３０以下で、かつ、床面積２０㎡以下の地階、無窓階又は居室の部分

会員意見募集版

(3) 粉末消火器

一般に最もよく利用されている消火器であるが、粉末消火器の薬剤は粒子径の小さい（１８０μm 以下）微粉末であり、放射すると広範囲に飛散し、電子機器に入り込むと故障、誤動作の原因となる他、飛散した粉末粒子の完全な除去が困難となる場合がある。

4. 二酸化炭素消火器は、消防法に適合する消火能力を有していないため、消防法における消火器設置義務のある場所に二酸化炭素消火器を設置する場は、A火災（一般火災）に適応する消火器を重複設置する必要がある。

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(5) 建物(設備)

適　用　区　分			
セ	本	提	ダ
	○		

設　100	設備等の耐震措置を講ずること。

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。

1. 地震により端末機器周辺の什器、備品等が落下、移動および転倒し、端末機器の機能に障害が生じないよう耐震措置を講ずることが望ましい。
   また、地震によりオンラインシステムに障害を与えるおそれのある回線設備等については、振動、移動および転倒を防止する措置を講ずることが望ましい。

2. 什器、備品等の耐震措置としては、以下のような例がある。
   (1) L 型金具、アンカーボルト等で床、柱、壁等に固定
   (2) 転倒のおそれのない備品類は、L 型金具等で移動を防止
   (3) 車輪付の椅子、台車等
      ①鎖、ロープ等で連結する。
      ②ストッパ、ブレーキ等を取り付ける。
   (4) 机上の機器、備品等の落下防止枠の設置や机への固定
      ①移動防止枠に納める。
      ②耐震バンドで固定する。
      ③粘着テープ等で固定する。

(参考)
「情報システムの設備ガイド」(社)電子情報技術産業協会

3. 【設 50】参照

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(5) 建物(設備)

適　用　区　分			
セ	本	提	ダ
	◎		

設　101	耐火金庫を設置すること。

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。

1. 耐火金庫を利用する際は次のような点に留意する必要がある。
   (1) 耐火金庫等の性能により耐火時間が異なるため、保管内容、消火設備等の状況により選択することが必要である。
   (2) 耐火金庫等に保管する磁気媒体、資料等は、修復、再現の難しい重要なものを優先することが必要である。
   (3) 磁気媒体は熱、湿気に敏感なため、専用の磁気媒体用耐火金庫等で保管することが望ましい。

2. なお、室全体が耐火構造の耐火金庫室となっている場合は、本項の限りではない。

会員意見募集版

2 本部・営業店等
(5) 建物(設備)

適　用　区　分			
セ	本	提	ダ
	○		

設　102	避雷設備を設置すること。

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。

1. 建築基準法では、建物の高さが 20m を超える場合に避雷設備の設置を規定しているが、20m 以下の建物であっても周囲の状況や、本部・営業店等に設置されているコンピュータシステムの重要性によって、避雷設備を設置することが望ましい。

2. 落雷多発地域においては、電力線等を通じての落雷に備えて、電源設備等に避雷措置を講ずることが望ましい。

3. 【設 7、設 65】参照

会員意見募集版

2 本部・営業店等
(5) 建物(設備)

適 用 区 分			
セ	本	提	ダ
	◎		

設　103	防犯措置を講ずること。

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。

1. 防犯ビデオ、防犯カメラ、防犯センサー、非常押ボタン等の防犯設備を設置することにより、犯罪の未然防止と、発生した場合の記録に役立てる必要がある。
   なお、非常押ボタンには携帯可能なものもある。

2. 非常時に、防犯機関等への通報ができる非常通報装置を設置すること。

3. 犯罪の未然防止を考慮したレイアウトとすること。
   未然防止対策としては、以下のような例がある。
   (1) 監視性を高めるため、死角を作らない。
   (2) 多額の現金を取り扱う場所（金庫、出納等）は、来客用ロビーから現金の取扱いが見えないよう工夫する。

（参考）「金融機関等防犯カメラシステムの設計基準・解説」（平成 26 年 11 月）
公益社団法人 日本防犯設備協会　http://www.ssaj.or.jp/guidebook/kinyu_system.html
(1) デジタル方式で、設置目的に合った記録フレームレートでの記録ができること。
(2) 出入口、ロビー、窓口、ATM、営業室等では、低照度環境を除いてカラー撮影ができること。
(3) 撮影目的と画角に従った十分な解像度を確保するために、メガピクセル防犯カメラやプログレッシブ防犯カメラを有効活用すること。
(4) 必要に応じ、逆光が起きる場所はダイナミックレンジ拡大機能を持つこと。
(5) ロビー、窓口、ATM、営業室等では少なくとも 3 ヶ月以上の画像を記録できること。
(6) 記録画像は年月日時分と関連付けて記録できること。
(7) 記録画像を装置外部に出力する機能を持ち、必要に応じて設置場所以外からも映像監視できること。
(8) アラーム記録を実施する場合には、非常通報装置との連動ができること。
(9) 防犯カメラシステムに記録された画像の保全につとめること。
(10) 防犯カメラシステムの定期点検・保守計画を定め、十分な画質を維持すること。

会員意見募集版

2 本部・営業店等
(6) 建物(回線関連設備)

適　用　区　分			
セ	本	提	ダ
	◎		

設　104	回線関連設備の設置場所の表示は付さないこと。

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。

1. MDF、IDF、回線終端装置等回線関連設備については、不正アクセス、破壊等の不法行為を防止し、コンピュータシステムの安全性を確保するため、設置場所の表示は付さないこと。

会員意見募集版

2 本部・営業店等
(6) 建物(回線関連設備)

適　用　区　分			
セ	本	提	ダ
	◎		

設　105	回線関連設備には錠を付けること。

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。

1. 回線関連設備が関係者以外に触れられるおそれのある場合は、誤ってまたは故意に触れないよう回線の安全性確保のため、錠を付けることが必要である。

2. 回線関連設備に錠を付けることが難しい場合は、回線関連設備を遮蔽したり、関係者以外が触れるおそれの少ない場所に移転させる等の対策を講ずることが必要である。

会員意見募集版

2 本部・営業店等
(6) 建物(回線関連設備)

適　用　区　分			
セ	本	提	ダ
	○		

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。

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。

1. 重要な回線は予備を設けることが望ましい。【実 87】参照

2. 本部・営業店等において、回線関連設備から各端末機器までの重要な配線は、断線等が発生した際に、迅速に切り分け・回復できるように事前に予備回線を布設しておくなど、二重化することが望ましい。

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(7) 建物(電源設備)

適 用 区 分			
セ	本	提	ダ
	◎		

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。

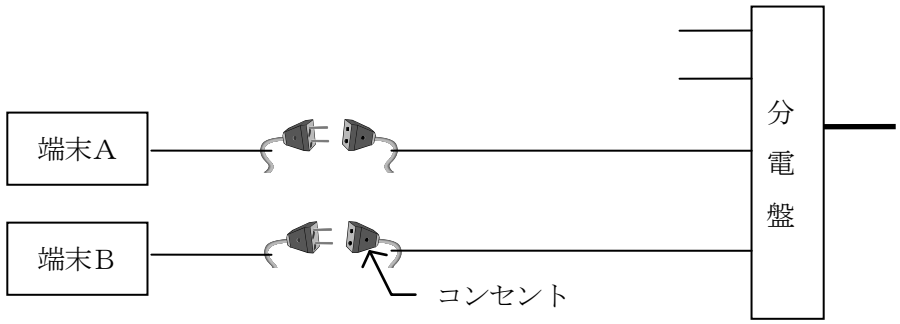
端末機器等に支障を来さないようにするため、電源ケーブルは分電盤から直接布設するか、他の機器の影響を受けないように布設すること。

1. 電源ケーブルの引き方としては、以下のような点に配慮することが必要である。
   (1) 電源ケーブルの配線は、保守点検の容易な経路を選ぶ。
   (2) 電源ケーブルの配線方法は、過負荷および短絡に対して端末機器等を安全に保護する。
   (3) 電源ケーブルは、通信回線にノイズの影響を与えないようにするか、または近接かつ並行しないように布設する。

2. 他の機器の影響により、端末機器等に支障を来さない電源ケーブルの布設方法としては、以下のような例がある。
   (1) 分電盤より端末機器まで電源ケーブルを直接引く（図 1・例 1）。
   (2) 配線容量は、接続される端末機器に応じた十分な余裕を持たせる（図 1・例 2）。
   ①a の配線容量は、接続される端末機器 A と B の容量を考慮する。
   ②分電盤のヒューズは端末機器 A と B の容量を考慮する。

会員意見募集版

＜例１＞



＜例２＞

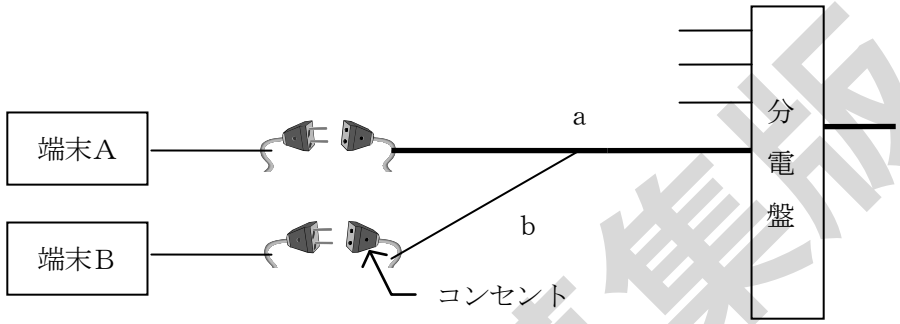


図１　電源ケーブルの布設の例

会員意見募集版

2 本部・営業店等
(7) 建物(電源設備)

適 用 区 分			
セ	本	提	ダ
	◎		

設 108	防災、防犯設備用の予備電源を設置すること。

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。

1. 地震、火災等の発生により停電した場合でも要員の安全な避難とコンピュータシステムへの影響を最小限にするために、防災、防犯設備が予備電源で正常に作動することが必要である。

2. 無人運用を行う自動機器室の場合でも、自動機器室の安全性を確保するため、設置されている非常用照明等は予備電源で正常に作動させる必要がある。

3. 【設 71】参照

会員意見募集版

2 本部・営業店等
(7) 建物(電源設備)

適　用　区　分			
セ	本	提	ダ
	○		

設　109	自家発電設備等を設置すること。

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。

1. 長時間の停電により、オンラインシステムが停止するのを防止するため、太陽光発電等の代替エネルギーシステムの活用を含め自家発電設備等を設置することが望ましい。

2. 自家発電設備等は、本部・営業店等の規模、建物の所有形態等によっては設置が難しい場合もあるため、一部に設置する方法、移動電源車を用意する方法、小型の発電装置を設置する方法等もある。

3. 停電によるデータ破壊を避けるため、サーバー等に UPS（無停電電源装置）を設置することが望ましい。

4. 非常時に自家発電設備等が稼働した際に利用できる施設、設備、端末等を確認しておくことが望ましい。また、それらが必要とする電力量を各機器の追加や更改時に確認しておくことが望ましい。

5. 非常時に自家発電設備等が正しく機能するように【設 64】を参照し、定期的に点検することが望ましい。

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(8) 建物(空調設備)

適　用　区　分			
セ	本	提	ダ
	◎		

設　110	空調設備を設置すること。

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。

1. 端末機器等の設置環境または端末機器等の機種により空調設備が必要な場合は、端末機器台数に応じた空調設備を設置することが必要である。

2. 本部・営業店等の温湿度が端末機器の運用許容限度を超えると、端末機器等に異常動作が起こる可能性があるため、空調設備の設置により温湿度が端末機器の運用許容限度を超えないようにすることが必要である。

3. 日中最高温度と夜間最低温度の差が大きな地域の本部・営業店等においては、急激な温度変化等による端末機器の結露のため、端末機器に障害が生ずる可能性があり、空調条件に十分留意することが必要である。

4. 営業店において自動機器室は、一般に営業室から独立した空間になっているが、自動機器から発生する熱等により室内が高温となりやすいので、自動機器室の空調設備について配慮することが必要である。

会員意見募集版

2 本部・営業店等
(9) 建物(自動機器室)

適　用　区　分			
セ	本	提	ダ
	◎		

設　111	通話装置を設置すること。

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。

1. 営業店において自動機器室の機器に故障があった場合等、顧客が営業室内、管理センター等の係員に迅速に通知、連絡できるよう電話、インターホン等の通話装置を自動機器に近く、顧客の目につきやすい場所に設置することが必要である。
   ここでいう管理センター等とは、遠隔で自動機器室等を集中監視するセンター、外部委託した業者の監視センター等をいう。

2. 無人運用時には、管理センター等との通話ができることが必要である。

3. 自動機器室には、自動機器の障害時の通知連絡方法等を表示した案内板等を、自動機器の近くの目につきやすい場所に設置することが必要である。

4. 【設 117】参照

会員意見募集版

2 本部・営業店等
(9) 建物(自動機器室)

適　用　区　分			
セ	本	提	ダ
	◎		

設　112	非常通報装置を設置すること。

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。

1. 営業店において自動機器室で発生した非常事態を営業室、管理センター等へ通報する非常通報装置は、自動機器に近く、顧客の目につきやすい場所に設置し、非常通報装置である旨の表示をすることが必要である。また、営業室には、非常通報の作動を確認できる設備を設置することが必要である。

2. 機械室（保守・現金装填室）においても同様に非常通報装置を設置することが望ましい。なお、保守要員の目につきやすい場所に設置し、非常通報装置である旨の表示をすることが必要である。

3. 無人運用時には、管理センター等への通報ができる非常通報装置を設置することが必要である。

4. 自動機器室には、非常時の通知連絡方法等を表示した案内板等を、自動機器の近くの目につきやすい場所に設置することが必要である。

5. 【設 117】参照

会員意見募集版

2 本部・営業店等
(9) 建物(自動機器室)

適　用　区　分			
セ	本	提	ダ
	◎		

設　113	防犯措置を講ずること。

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。

1. 自動機器室は一般に営業室から離れた場所に設置される場合が多いので、適切な防犯措置を講ずる必要がある。防犯措置としては、防犯カメラ、ビデオ装置等自動機器室に対する防犯設備、および筐体強化用品等自動機器本体に対する防犯措置等を適切に組み合わせ、総合的に行う必要がある。
   また、これら防犯措置により、端末機器の破壊、カードの不正使用、カード情報の不正な読取装置の設置、隠しカメラの設置、強盗等の犯罪の未然防止と、発生した場合の記録に役立てる必要がある。
   なお、CD・ATM 周辺のレイアウト（販売促進用リーフレットを入れる小箱の設置等）においては、隠しカメラ等が設置されないように配慮することが必要である。

2. 自動機器室の防犯設備としては、以下のような例がある。
   (1) 防犯カメラおよび防犯ビデオ 【設 103】
   ①図１のように、防犯カメラにより、出入口、自動機器室の状況を撮影、監視する。
   ②防犯カメラにより撮影した出入口、自動機器室、および機械室の状況を、ビデオ装置で記録する。
   ③静止画像電送装置を設置し、閉店時の残留者確認等を管理センター等で行う。
   なお、カラー画像の静止画像電送装置は細部まで監視でき、認識性を高めることができる。
   ④監視および録画ができ、少なくとも利用者の上半身の撮影を可能とする。また、カード情報の不正な読取装置や隠しカメラ等の設置の防止と発生時の記録に役立つよう、アングルや解像度等に十分配慮すること、並びに暗証番号を入力する利用者の手元が撮影されない配慮が必要である。
   ⑤異常発報時には自動的に高解像モードに切り替わるものが望ましい。デジタル方式の採用等解像度に配慮する。
   ⑥小型のカメラは、その設置場所を判明されにくく、防犯対策にも有効である。

   (2) 防犯センサー
   ①閉店後の自動機器室、および機械室への侵入検知用として、赤外線センサー、焦電式赤外線センサー、ガラス破壊センサー、扉開閉センサー、シャッターセンサー、焼切り

会員意見募集版

センサー等がある。

②自動機器破壊検知用として、衝撃センサー、焼切りセンサー、扉こじ開けセンサー等がある。

③閉店後の防犯センサー感応時には、防犯カメラ等を作動させる。

(3) 集音マイク

集音マイクにより、現場の状況が把握できる。

(4) 非常押ボタン

緊急時に警備会社、金融機関等の管理センター等に直接異常を知らせる装置を設置すること。集音機能または画像伝送機能を有するものが望ましい。設置する位置は、利用中の犯罪を考慮し、通報しやすい位置や高さとすること。

(5) 非常ベル

ボタンを押すと警鳴し、周囲に異常を知らせるとともに犯人を威嚇する装置を設置すること。

(6) 複数錠の設置

機械室扉の錠は複数設け、不法な侵入を防止する。

(7) 窓や扉の防犯設備

①防犯用のガラス

②開閉可能な鉄格子またはシャッター

(8) 出入管理装置

夜間の入退室がある場合、キャッシュカード等の挿入がなければ入室できないような出入管理装置を設置することにより自動機器室内における各種犯罪を防止することができる。なお、出入管理装置に似せたカード情報の不正な読取装置の設置を防止するため、防犯カメラや巡回等の防犯措置等を適切に組み合わせて実施することが必要である。

(9) 覗き見防止装置

自動機器室内に設置された CD・ATM 利用時に後方や周りから暗証番号等の覗き見を防止する設備とすることが必要である。覗き見防止対策としては、以下のようなものがある。

①間仕切り

②入力操作を隠す設備（手元覆いカバーの装着等）

③後方確認用ミラーの装着

④画面の視野角制限（覗き見防止フィルム等）

⑤利用者待機位置の明示

(10) 盗撮カメラ等の不正設置を検知する装置 【実 1】

3. 自動機器本体等の防犯措置としては以下のような例がある。

(1) 本体の強度

筐体の強度としては、「ATM 等の技術的防犯対策について」に定めるレベル 2 以上が望ましい。また、レベル 1 の場合は、筐体強化用品の取付け等の措置を講ずることが望ましい。

(2) 本体の固定

①床・壁等へ本体をボルト等で固定する。なお、固定にあたっては、金属板を床・壁等に埋め込み補強することが望ましい。

②温度の異常、本体の傾き、振動等を感知して発報し、警備会社、金融機関等の管理センター等に知らせるセンサーを設置し、非常ベルと連動させる。また、センサーは、盗難時の破壊に対して影響を受け難い箇所に設置することが望ましい。

(3) 配線および回線

①外部から見えないようにする。

②外部から見える場合には、切断されないような補強等を行う。

③万一切断された場合には異常発報を行う。

4. 店舗外ブース

店舗外ブースは、屋外独立型、店舗隣接型、屋内独立（ロビー）型、カプセル型等の形態で設置される。

(1) 店舗外ブースで特に考慮すべき防犯措置として、以下のような例がある。

①ブースの固定・強化

②錠前の追加

③ドア錠前部の補強

④ドアと壁の間を目板で補強

⑤ヒンジ部を合決（あいじゃくり）で補強

(2) 筐体の強度としては、「ATM 等の技術的防犯対策について」に定めるレベル 3 を確保することが望ましい。

(3) 店舗外ブースは、重機等が侵入困難な場所に設置することが望ましい。

(4) CD・ATM 等には GPS 装置等追跡可能な手段を有することが望ましい。

5. 偽造硬貨等に対しても適切な対策を講じることが望ましい。例えば、取り消し時に投入した現金自体が戻ってくる等がある。

6. 【設 15】参照

会員意見募集版

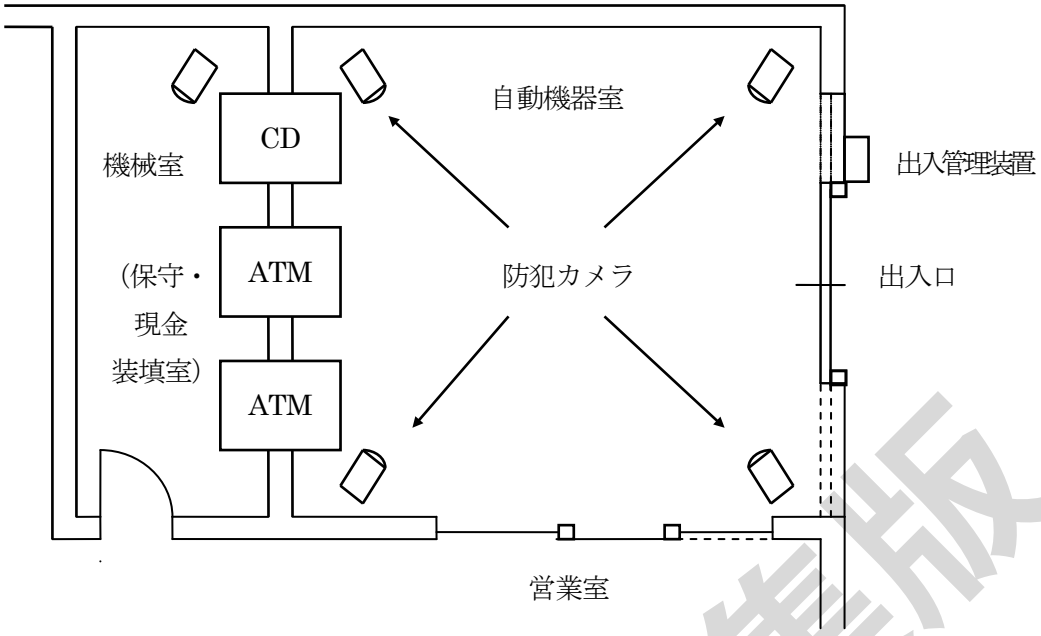


図１　自動機器室の防犯設備の例

（参考）ATM 等の技術的防犯対策について（平成 12 年 12 月）
　日本自動販売機工業会　金融システム委員会
レベル１：レベル２に満たないもの
レベル２：手工具等による破壊に対して 15 分間以上耐える構造
レベル３：手工具等による破壊に対して 25 分間以上耐える構造

会員意見募集版

2 本部・営業店等
(9) 建物(自動機器室)

適　用　区　分			
セ	本	提	ダ
	◎		

設　114	照明設備および非常用照明設備を設置すること。

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。

1. 自動機器室は無人で運用されることも多く、各種犯罪を未然に防止するために、十分な照度の照明設備を設置することが必要である。

2. 無人運用を行う自動機器室では、停電時等にも安全を確保するための非常用照明設備を設置することが望ましい。

3. 店舗外ブースにおいては、犯罪を未然に防止するため、周囲の状況に応じ、夜間照明を設置することが望ましい。

会員意見募集版

2 本部・営業店等
(9) 建物(自動機器室)

適　用　区　分			
セ	本	提	ダ
	◎		

設　115	扉は、一部を素通しにすること。

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。

1. 自動機器室の出入口の扉は中央部分を除いて上下部分を素通しにするなど、外部から自動機器室内の内部が見えるようにすることが必要である。

2. 扉の一部を素通しすることにより、CD・ATM 等の自動機器に直射日光による障害が発生しないよう配慮することが必要である。

会員意見募集版

2 本部・営業店等
(9) 建物(自動機器室)

適　用　区　分			
セ	本	提	ダ
	○		

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。

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。

1. 自動機器の現金の装填、保守のためには、自動機器の後面に機械室を確保することが望ましい。
   機械室については、【設 113】の図 1 を参照のこと。

2. 機械室の入退室に対する安全対策を講ずることが必要である。機械室の入退室に対する安全対策としては、以下のようなものがある。
   (1) 覗き穴
   (2) 防犯カメラおよび防犯ビデオ 【設 103】
   (3) 防犯センサー
   (4) 鍵やパスワードによるドアの安全対策の設置
   (5) 非常押ボタン

3. 機械室が確保できない場合には、間仕切りをするなど、部外者が入れない措置を講ずることが必要である。

4. 自動機器の現金の装填、保守のために必要な空間は機種によって異なるため、自動機器製造メーカーと協議のうえ決定することが必要である。

会員意見募集版

2 本部・営業店等
(9) 建物(自動機器室)

適 用 区 分			
セ	本	提	ダ
	○		

設 117	自動運行設備を設置すること。

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。

1. 自動運行設備

ここでいう自動運行設備とは、あらかじめ設定されたプログラムにより、スケジュールに従い自動機器室内の各装置の自動発停を制御する等の機能を提供するものであり、これらを実現する設備として以下のようなものがある。

区分	設備・機器名	機　能　等
自動運行管理	自動運行装置本体	年間スケジューラー部、シーケンスコントロール部、音声発生部、表示部、手動操作部、電源部、端子部、I/O部から構成され、プログラム機能により、自動機器室内部設備の自動発停を行う。
電源設備関連	電磁制御部付分電盤	自動運行装置からの命令により、各設備の電源の ON／OFF を行う負荷制御および負荷状態の確認信号を受けとる機能を持つもの。
通信設備関連	送信機	自動運行情報､その他の情報を管理センター等に伝送し､また管理センター等側からの制御データを受信する。
	自動ダイヤル通話装置	営業時間帯は営業室内へ、無人運用時は管理センター等へ通話できるように、自動運行装置で切替え。
	静止画像電送装置	自動化機器のモニター。
防犯関連設備	防犯カメラ・防犯ビデオ	自動機器室内の映像記録の取得。
	防犯センサー	赤外線センサー、マットセンサー、シャッターセンサー、扉開閉センサー等。 自動機器室への侵入検知、音声ガイダンスや防犯ビデオ記録のトリガーとなる。
	電気錠	自動機器室出入口扉の自動施解錠を行う。 施解錠のモニターができ、内部から自由に出られる仕組みである。 既設扉には電気ストライクでも可。
	シャッター安全装置	自動運用のシャッター下降時の安全システム。
	スピーカー	各種音声ガイダンスを行う。
サービス設備等	空調設備	必要な空気調和を行う。
	照明設備	必要な室内照明を行う。
	自動機器等	自動機器本体、TC、回線終端装置等。

会員意見募集版

2. 遠隔監視設備

無人運用を行う場合には、運用状況を監視するため、管理センター等に遠隔監視設備を設置する必要がある。

会員意見募集版

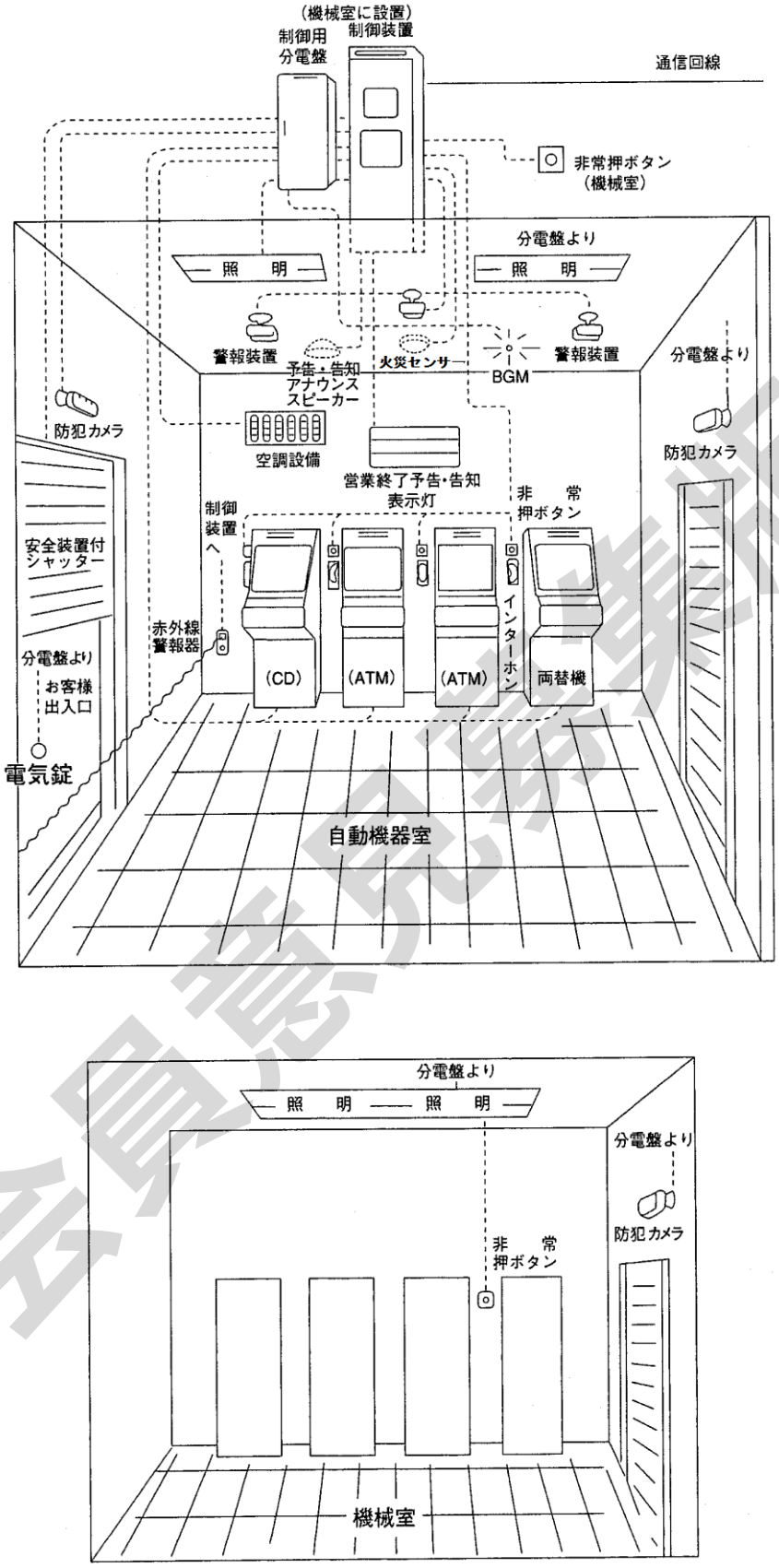


図１　自動運行設備の設置例

会員意見募集版

2 本部・営業店等
(10) 建物(端末機器)

適　用　区　分			
セ	本	提	ダ
	○		

設　118	端末機器には耐震措置を講ずること。

端末機器の移動、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。

1. 端末機の移動、転倒を防止するための措置として、以下のような例がある。
   (1) 床上に設置する機器の例
   ①キャスタホルダー、ゴム足、転倒防止枠を取り付ける（図 1、図 2、図 3）。
   ②建物の床に固定する（図 4）。
   ③機器相互を連結し、固定する。

（床上に設置する機器の固定）

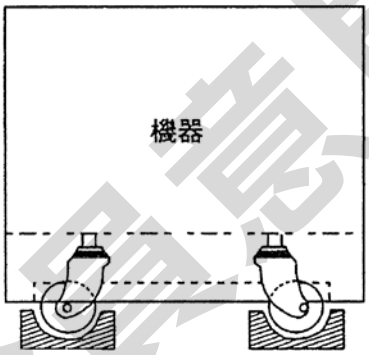


図 1　キャスタホルダの例

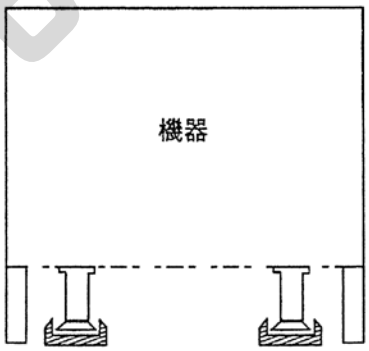


図 2　ゴム足の例

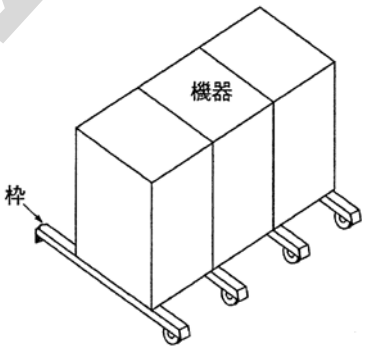


図 3　転倒防止枠の例

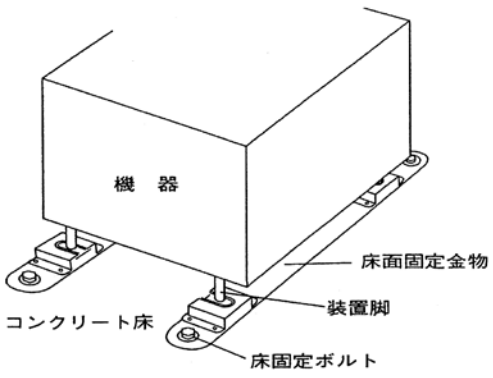


図 4　床への固定の例

会員意見募集版

(2) 卓上に設置する機器の例

①固定金具により機器をデスクに固定する（図 5）。

②ゴム足により機器をデスクに固定する。

③デスクに機器の移動を防止するストッパを取り付ける（図 6、図 7）。

（卓上に設置する機器の固定）

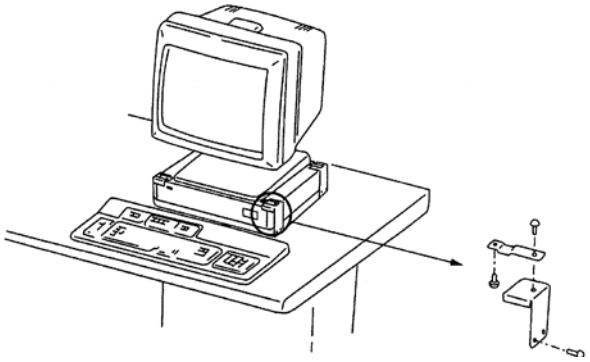


図 5　固定金具の例

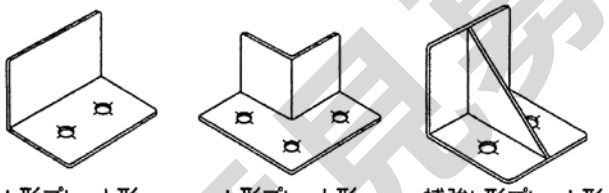


図 6　移動防止型耐震ストッパの例

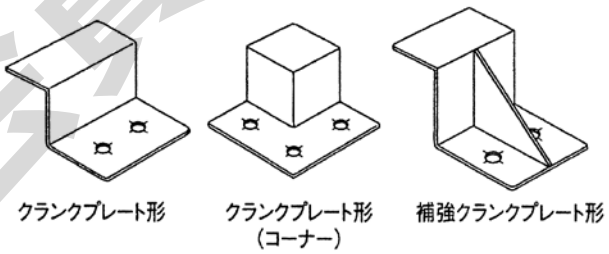


図 7　移動・転倒防止型耐震ストッパの例

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(10) 建物(端末機器)

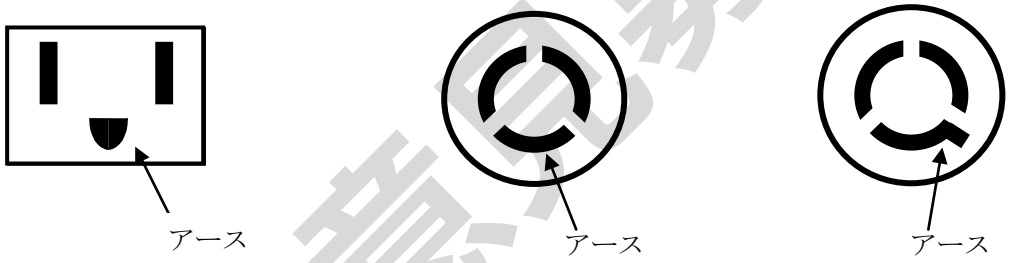
適 用 区 分			
セ	本	提	ダ
	◎		

設　119	機器のアースを確実に取ること。

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。

1. アースを取ることが設置要領書で要求されている端末機器等は、確実にアースを取ることが必要である。アースが取られていない場合、エアコン等のリレーが入った際に IC 素子等が破損されたり、保存データが破壊されることがある。

2. アースの取り方としては、アース付のコンセントや延長タップの使用が望ましい。新規に電源ケーブルを布設する際は、アース付とすること。アース付コンセントの例を図 1 に示す。



(1) 平行アース付型　(2) 引掛 15A 型　(3) 引掛 20A 型

図 1　アース付コンセントの例

会員意見募集版

2 本部・営業店等
(10) 建物(端末機器)

適　用　区　分			
セ	本	提	ダ
	○		

設　120	漏水および塵埃等に対する保護措置をとること。

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とることが望ましい。

1. 漏水、塵埃、煙等により、端末機器に障害が発生しないよう、端末機器の運転停止時等の防水・防塵カバーの使用や必要な空調設備等を備えることが望ましい。

(参考)
端末機器を漏水や煙等の害から保護するためには、機器の周辺での喫煙や飲食を禁止する等、使用時のルール等の措置もあわせて実施することが望ましい。

会員意見募集版

2 本部・営業店等
(11) サーバー設置場所(位置)

適　用　区　分			
セ	本	提	ダ
	○		

設　121	災害を受けるおそれの少ない位置とすること。

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。

1. 建物内において、サーバー設置場所は地震、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により、コンピュータシステムへの影響を防止することが望ましい。
   災害を受けるおそれのある位置にやむを得ず設置する場合には、各種災害の防止に必要な対策を講ずることが必要である。

2. 建物内において災害を受けるおそれの少ない位置は、【設 22】を参照のこと。

(参考)
サーバー収納ラック・ネットワーク機器収納ラック設置時の注意事項として、ラック内の熱溜まり防止や機器の接地確保などに関しての事例が以下のガイドラインに紹介されている。
「情報システムの設備ガイド」（社）電子情報技術産業協会

会員意見募集版

2 本部・営業店等
(11) サーバー設置場所(位置)

適　用　区　分			
セ	本	提	ダ
	○		

設　122	外部から容易に入れない位置とすること。

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。

1. サーバー設置場所を設ける場合、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、外部から容易に入れない位置に設置することが望ましい。

2. やむを得ず、サーバー設置場所を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に設ける場合の措置は、【設 23】を参照のこと。

会員意見募集版

2 本部・営業店等
(11) サーバー設置場所(位置)

適　用　区　分			
セ	本	提	ダ
	○		

設　123	室名等の表示は付さないこと。

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。

1. 本部・営業店等の建物内においては、侵入、破壊、機密漏洩等を防止するため、サーバー設置場所の表示、案内板の設置は行わないことが望ましい。

2. サーバー設置場所の位置が消防担当者に明示できるよう、建物内の見取図を部外者の目に触れないところに保管しておくことが必要である。

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(11) サーバー設置場所(位置)

適　用　区　分			
セ	本	提	ダ
	○		

設　124	専用の区画とすること。

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。

1. サーバー設置場所を専用の区画とする目的は【設 26】を参照のこと。

2. サーバー設置場所を専用の区画とした場合は、以下の措置を講ずることが望ましい。
   (1) 監視制御設備を設ける。監視制御設備については【設 80】【設 81】を参照のこと。
   (2) 運用に必要な空間を確保する。空間の確保については【設 25】を参照のこと。
   (3) コンピュータシステムへの影響を最小限にするため、分電盤を専用とする。分電盤の専用化については【設 67】を参照のこと。

3. やむを得ずサーバー設置場所を他の場所と共用する場合には、以下のような例がある。
   (1) パーティション等で区画を分ける。
   (2) 出入口への鍵の取付け。
   (3) サーバー自体への鍵の取付け。

会員意見募集版

2 本部・営業店等
(12) サーバー設置場所(構造・内装等)

適　用　区　分			
セ	本	提	ダ
	○		

設　125	防火区画に設置すること。

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。

1. サーバー設置場所は、建物内他区画等からの火災の影響を最小限にするため、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。

参照法令	建築基準法施行令第 112 条

会員意見募集版

2 本部・営業店等
(12) サーバー設置場所(構造・内装等)

適 用 区 分			
セ	本	提	ダ
	○		

設 126	漏水防止対策を講ずること。

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。

1. サーバー設置場所は、漏水防止対策を講じた場所に位置することが望ましい。漏水防止対策については【設 32】を参照のこと。

2. サーバーに接続している回線、電源ケーブル等の漏水防止対策については、【設 98】参照のこと。

会員意見募集版

2 本部・営業店等
(12) サーバー設置場所(構造・内装等)

適　用　区　分			
セ	本	流	ダ
	○		

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。

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。

1. サーバー設置場所にフリーアクセス床を使用する場合は、【設 36】に準ずる耐震措置を講ずることが望ましい。

会員意見募集版

＜会員意見募集版＞

2 本部・営業店等
(13) サーバー設置場所(設備)

適　用　区　分			
セ	本	提	ダ
	○		

設　128	消防設備を有すること。

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。

1. サーバー設置場所には、火災による損傷を受けやすい機器が集中しているうえ、通常は無人であり、防火に対して特に留意する必要がある。さらに、消火器の選択等にあたってはコンピュータ機器の汚損や安全性の観点からの配慮が必要である。

2. サーバー設置場所に設置する消防設備の例として、以下のようなものがある。
   具体的な対策の実施おいては、サーバーや機器の重要性に応じて、これらの設備を組み合わせた適切なものとすることが必要である。
   (1) 自動火災報知設備
   【設 37、設 99】参照
   (2) 非常時の連絡装置
   【設 38】参照
   (3) 消火設備
   【設 39、設 99】参照
   (4) ケーブル等の難燃化、延焼防止措置
   【設 40】参照
   (5) その他（携帯用照明器具の設置、排煙設備の設置等）
   【設 41、設 42】参照

会員意見募集版

2 本部・営業店等
(13) サーバー設置場所(設備)

適 用 区 分			
セ	本	提	ダ
	○		

設　129	地震感知器を設置すること。

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。

1. 地震によるデータ破壊や電気火災の二次災害防止および地震発生時の運転継続の判断のため、サーバーの設置場所に地震感知器を設置しておくことが望ましい。
   地震感知器はサーバーの重要度、設置台数、設置状況に応じて配置しておくことが必要である。

2. 地震感知器に関する留意事項については、【設 44】を参照のこと。

会員意見募集版

2 本部・営業店等
(13) サーバー設置場所(設備)

適　用　区　分			
セ	本	提	ダ
	○		

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。

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。

1. 出入管理設備、防犯設備については【設 45】参照。

会員意見募集版

2 本部・営業店等
(13) サーバー設置場所(設備)

適 用 区 分			
セ	本	提	ダ
	○		

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。

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。

1. 温湿度自動記録装置または温湿度警報装置を設置する場合、温湿度を測定する位置は、コンピュータ機器の排気および空調設備からの吹出空気が直接当たる場所、出入口付近等、温湿度の変化の大きな場所を避けて設置することが必要である。
   また、設置する場合、温湿度自動記録装置または温湿度警報装置は、サーバーの重要度、設置台数、設置状況に応じて配置しておくことが必要である。

2. 【設 46】参照

会員意見募集版

2 本部・営業店等
(13) サーバー設置場所(設備)

適　用　区　分			
セ	本	提	ダ
	○		

設　132	空調設備を設置すること。

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。

1. 使用するサーバーの動作条件にあった温湿度条件を確保するために専用の空調が必要な場合は、専用空調を設置し、空調の能力、安定性の確保ならびに空調の電源の安定性を確保することが必要である。

2. 空調設備の設置にあたっては【設 72～設 79】参照。

会員意見募集版

2 本部・営業店等
(13) サーバー設置場所(設備)

適　用　区　分			
セ	本	提	ダ
	○		

設　133	ネズミの害を防止する措置を講ずること。

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。

1. ネズミの侵入、営巣による回線・電源ケーブルの漏電、接続不良、腐食、断線等によって発生するコンピュータシステムの障害を防止するため、回線・電源ケーブルに対するネズミの害を防止する措置を講ずることが望ましい。

2. ビル内に厨房、飲食店等、ネズミの生息に適した場所がある場合は、ネズミの被害も多くなりやすいので、食料品の完全格納、厨芥や残飯等の完全処理等について設備面の配慮が必要である。

3. ネズミの害を防止する措置の例としては【設 47】参照。

会員意見募集版

2 本部・営業店等
(13) サーバー設置場所(設備)

適　用　区　分			
セ	本	提	ダ
	◎		

設　134	電源コンセントの抜け防止対策を講ずること。

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。

1. サーバーおよび周辺機器の電力を電源コンセントから給電している場合は、不注意によるひっかけ等により電源プラグがコンセントから簡単に抜けることのないように抜け防止の対策を講じておくことが必要である。

2. 抜け防止対策を施したコンセントの例としては、以下のようなものがある。
   ・抜け止めコンセント
   ・引掛形コンセント

会員意見募集版

2 本部・営業店等
(14) インストアブランチ

適 用 区 分			
セ	本	提	ダ
	◎		

設　135	他の区画からの侵入防止措置を講ずること。

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。

1. 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が必要である。ストア内の他の区画からの侵入を防ぐ対策としては、以下のようなものがある。
   (1) シャッターによる遮断
   (2) 防犯センサーによる感知 【設 113】
   (3) 防犯カメラおよび防犯ビデオによる監視 【設 103】【設 113】

2. インストアブランチにおいては、ストアおよびストア内の他のテナントと営業日および営業時間が異なる場合がある。ストアの他区画の営業時間にインストアブランチの営業を行わない場合には、中が見えるワイヤー入りのシャッターの採用等によりストア全体のイメージに配慮した防犯措置が望ましい。

3. インストアブランチでの現金･帳票等の保管方法については、不特定多数の出入りがあるストア内での営業であることを考慮する必要がある。

4. CD･ATM 等を設置する場合は、防犯カメラによる監視が可能な場所やカウンターから見える場所に設置する等、防犯対策を強化すること。

会員意見募集版

2 本部・営業店等
(14) インストアブランチ

適 用 区 分			
セ	本	提	ダ
	◎		

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。

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。

1. ストアの既設施設が金融機関等の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が必要である。

2. 出店先のストアの設備状況による設備面での対策としては、以下のようなものがある。
   (1) 側壁等が天井まで達していない場合、現金、帳票等を取り扱う事務室等の格子天井の設置。
   (2) 側壁等の強度が不足する場合の補強。

3. 使用するストアの状況により検討すべき運用面での対策としては、以下のようなものがある。
   (1) 防犯センサーを増設し、側壁等による物理的な侵入防止策を補完すること。【設 113】
   (2) 防犯カメラ、防犯ビデオによる監視を行うこと。【設 103】【設 113】

会員意見募集版

3 流通・小売店舗との提携チャネル
(1) コンビニ ATM

適　用　区　分			
セ	本	提	ダ
		◎	

設　137	防犯措置を講ずること。

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。

1. 従来の本部・営業店等における自動機器室に設置された CD・ATM に比べてより防犯対策を強化する必要がある。
   CD・ATM 等は、防犯カメラによる監視が可能な場所やカウンターから見える場所に設置する等の対策を実施すること。

2. 隠しカメラ等の設置による犯罪を防止するため、CD・ATM 周辺のレイアウト（販売促進用リーフレットを入れる小箱の設置等）においては、隠しカメラ等が設置されないように配慮することが必要である。

3. コンビニ ATM 利用時に後方や周りから暗証番号等の覗き見を防止する設備とすることが必要である。
   特に、コンビニ ATM 周辺は金融機関の自動機器室と比較して、より顧客相互が近接するなど、覗き見されるリスクが高いことを考慮し、十分な覗き見対策を実施することが必要である。

4. コンビニ ATM 利用時に後方や周りから暗証番号等の覗き見を防止する対策としては、以下のようなものがある。
   (1) 間仕切り
   (2) 入力操作を隠す設備（手元覆いカバーの装着等）
   (3) 後方確認用ミラーの装着
   (4) 画面の視野角制限（覗き見防止フィルム等）
   (5) コンビニ ATM 自体を、雑誌販売コーナー等の長居ができる場所の近くに設置しない。

5. コンビニ ATM の防犯設備としては、以下のようなものがある。
   (1) 防犯カメラおよび防犯ビデオ 【設 103】
   ①監視および録画ができ、少なくとも利用者の上半身の撮影を可能とする。また、カード情報の不正な読取装置や隠しカメラ等の設置の防止と発生時の記録に役立つようアングルや解像度等に十分配慮すること、並びに暗証番号を入力する利用者の手元が撮影されない配慮が必要である。
   ②異常発報時には自動的に高解像モードに切り替わるものが望ましい。デジタル方式の採

全銀協 意見募集版

用等解像度に配慮する。

③小型のカメラは、その設置場所を判明されにくく、防犯対策にも有効である。

(2) 非常押ボタン

緊急時に警備会社、金融機関等の管理センター等に直接異常を知らせる装置を設置すること。集音機能または画像伝送機能を有するものが望ましい。設置する位置は、利用中の犯罪を考慮し、通報しやすい位置や高さとすること。

利用中の犯罪としては、以下のようなものがある。

・後ろから羽交い締めにされる。

・横から現金を奪われる。

・催涙スプレー、各種凶器等。

(3) 非常ベル

ボタンを押すと警鳴し、周囲に異常を知らせるとともに犯人を威嚇する装置を設置すること。

(4) 防犯センサー

コンビニ ATM 破壊検知用として、衝撃センサー、焼切りセンサー、扉こじ開けセンサー等がある。

(5) 集音マイク

集音マイクにより、現場の状況が把握できる。

6. コンビニ ATM 本体等の防犯措置としては、以下のようなものがある。

(1) 本体の強度

・筐体の強度としては、「ATM 等の技術的防犯対策について」に定めるレベル 3 を確保する。

・筐体強化用品などの取付けによる補強等を行う。

(2) 本体の固定

・床・壁等への本体をボルト等で固定する。

・温度の異常、本体の傾き、振動等を感知して発報し、警備会社、金融機関等の管理センター等に知らせるセンサーを設置し、非常ベルと連動させる。

・保護筐体への収納等によりコンビニ ATM 本体を容易に移動できないようにする。

(3) 配線および回線

・外部から見えないようにする。

・外部から見える場合には、切断されないような補強等を行う。

・万一切断された場合には、異常発報を行う。

(4) 重機等が侵入困難となるよう、車止め等の対策を実施することが望ましい。

(5) CD・ATM 等には GPS 装置等追跡可能な手段を有することが望ましい。

7. 偽造硬貨等に対しても適切な対策を講じることが望ましい。例えば、取り消し時に投入した現金自体が戻ってくる等がある。

会員意見募集版

（参考）ATM 等の技術的防犯対策について（平成 12 年 12 月）
　日本自動販売機工業会　金融システム委員会
レベル 1：レベル 2 に満たないもの
レベル 2：手工具等による破壊に対して 15 分間以上耐える構造
レベル 3：手工具等による破壊に対して 25 分間以上耐える構造

会員意見募集版

＜会員意見募集版＞

Ⅷ. 監　　査　　基　　準

会員意見募集版

1 システム監査
(1) システム監査

適　用　区　分					基準分類
共	セ	本	提	ダ	基礎
◎					

監　1	システム監査体制を整備すること。

コンピュータシステム及びその管理について、有効性、効率性、信頼性、遵守性、及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。

1. コンピュータシステムの運用、システム開発・変更等においては、コンピュータシステムの有効性、効率性、信頼性、遵守性、及び安全性を確保するため、コンピュータ部門から独立した監査人がシステムの総合的な評価・検証を行い、経営層に監査結果を報告する必要がある。
   なお、被監査部門としては、コンピュータシステムに関して、その開発及び運用を担当する部門（外部委託先を含む）が該当するが、本部各部門や営業店などの利用部門、EUC（エンドユーザーコンピューティング）実施部門等においてもシステム監査またはそれに準じた監査を受けることが望ましい。特に、個人データを取り扱う情報システムの利用及び個人データへのアクセスの監視状況については、システム監査またはそれに準じた監査を受けることが必要である。
   システム監査を実施するにあたっては、当センター発刊の『金融機関等のシステム監査指針』等を参照のこと。

2. 監査人として、コンピュータシステムに精通し、監査スキルを保有する人材を確保する必要がある。

3. システム監査の実施手段の 1 つとして、内部者による監査に加え、外部の専門機関を活用することが望ましい。特に機微（センシティブ）情報を取り扱う場合は、外部の専門機関を活用することが望ましい。なお、機微（センシティブ）情報に該当する生体認証情報を取り扱う場合は、より客観性が求められることから、外部の専門機関を活用することが必要である。

4. システム監査における指摘事項については、システム監査部門と被監査部門の間で、事実確認、及び十分な意見交換を行い、問題があると認められた点について改善のための措置を講ずることが必要である。また、改善策の実施状況について、定期的にフォローアップすることが望ましい。

5. 金融機関等が外部委託を行う場合には、委託する業務の遂行状況及び、外部委託先の要員によるルールの遵守状況等について、評価・検証することが必要である。
   また、提出された情報のみで委託業務の適切性の評価・検証が十分にできない場合は、外部

会員意見募集版

委託先のオフィスまたはデータセンターへの監査・モニタリング等により実地で確認することが必要である。なお、特定システムが再委託される場合には、再委託先に対しても金融機関等の責任において監査を行う必要がある。

外部委託先の監査の方法としては、以下の例がある。

(1) 金融機関等がみずから外部委託先の監査を行う。また、複数の金融機関等が同一の共同センター等を利用する場合は、金融機関等が共同で監査を行うことも考えられる。なお、金融機関等による監査等が実効的でない場合には、第三者監査等（注１）により代替することも考えられる。なお、監査を行う際に、外部委託先から提供されたデータ抽出のツールを利用したデータ検証を行うことも考えられる。

（注１）金融機関等が監査法人を利用した監査を行う場合、監査の対象期間において外部委託先の会計監査に従事していない監査法人とし、また、選定した監査法人が外部委託先の SOC2、IT7 号の保証業務に従事している場合には、外部委託先の保証業務に直接従事していない監査責任者を選定するなどにより、外部委託先との利益相反に疑義が生じないような外観とすることが考えられる。なお、第三者監査人の適格性の担保のため、監査人(監査法人)が日本公認会計士協会等の指導や指針等に基づいて、適切な品質管理体制の整備、運用を実施することも考えられる。また、外部委託先のリスク特性を踏まえた検証、金融機関等の検証ニーズに則った検証を行う。

(2) 外部委託先の内部監査部門の監査結果報告について確認を行う。なお、共同センター等、委託元となる金融機関等が複数の場合は、監査結果を複数の金融機関等に報告することも考えられる。

(3) 第三者保証による報告書（注２）または第三者認証に関する情報（注３）について確認を行う。

（注２）SOC1、SOC2、監査・保証実務委員会実務指針第 86 号、IT 委員会実務指針 7 号等に基づく第三者保証による報告書。

（注３）情報セキュリティ体制やプライバシー保護体制の基準等に係る認証。代表的なものとして、ISMS(ISO27001、ISO27017)や PCI DSS level1、プライバシーマーク等に関する情報。

(4) 外部委託先が作成したセキュリティ及びコンプライアンスに係るホワイトペーパーについて確認を行う。

非会員意見募集版

【会員意見募集用】
平成 29 年 11 月 28 日
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』改訂原案に関するよくあるご質問（FAQ）

Ⅰ 全般

（Ⅰ－1）各金融機関が、安全対策基準の改訂内容に基づき対策を適用するには相応の時間を要することが予想される。新しい安全対策基準はいつから適用する必要があるのか。

（答）

今回の改訂は、従来の改訂と異なり、安全対策基準の適用の考え方から抜本的に変更を行うことから、安全対策基準を使用する金融機関等においては、社内規程の見直しや、場合によっては組織体制等の見直しが発生するなど、その影響が大きいことが予想されます。そのため、現在安定的に運営されている金融情報システムについては、従来どおりの取扱いを継続することとし、所要の行内体制や規程等の整備を行ったうえで、システムの更改時や新システムの導入時に、変更後の安全対策基準を適用するなど、順次移行を図ることとしています。

（Ⅰ－2）改訂内容の新旧対照表は公開されるのか。

（答）

今回の改訂は、「金融機関における外部委託に関する有識者検討会」及び、「金融機関における FinTech に関する有識者検討会」の報告内容・提言を受け、安全対策基準にリスクベースアプローチや IT ガバナンスの発揮の考え方を取り入れるとともに、外部への統制を拡充させるなど、安全対策基準の構成・適用方法等の抜本的な見直しを行いました。また、すべての基準について記述様式の統一化の観点から広範に文書の構成変更や修正等を行ったことから、これまでのように新旧対照表により改訂箇所を示す方法は、却って読みづらく、理解されにくいと判断しました。

改訂原案のⅠ概説、Ⅱフレームワーク、Ⅲ本書の利用にあたっては、今回の改訂において、新設あるいは大幅改訂されたものですので、【資料２】「改訂原案（全編）」をご確認ください。また、基準の改訂箇所は、【資料３】「改訂原案（改訂履歴版）」で確認願います。

（Ⅰ－3）リスクベースアプローチの手順について、より詳細な内容をFISCから示してもらいたい。

（答）

リスクベースアプローチとは、リスク特性の分析結果を安全対策の優先順位など金融機関等が安全対策を決定するための合理的な意思決定に活用するとともに、金融機関等の経営資源が有限である点を踏まえ、リスクゼロを追求することは必ずしも合理的ではないという認識に基づき、安全対策に対する資源配分を経営資源全体の中で調整する考え方であり、リスクベースアプローチの考え方を導入する際には、「金融機関等がみずから」その安全対策の達成目標とその対策を決定することが前提となります。

したがって、安全対策基準では、リスクベースアプローチに関する大枠のプロセスは示していますが、より詳細な一律の手順等を示すことは、適切ではないと考えています。

なお、ご参考としまして、「金融機関におけるクラウド利用に関する有識者検討会」報告書で

は、リスクベースアプローチの適用例が掲載されています。また、リスク評価の手法につては、当センター発行の『金融機関等のシステムリスク管理入門』で解説されています。

当センターでは、今後も、リスクベースアプローチの実例などを各種レポート等で紹介していくことを考えております。

（Ⅰ－4）今回の改訂によって、安全対策基準の適用対象となるコンピュータシステムが変更になるのか。

（答）

改訂前の安全対策基準の適用対象は、「基幹業務のオンラインコンピュータ・システム」であり、それ以外の情報システムは、安全対策基準を「適宜取り入れる」あるいは「そのシステムの重要性によって個別に判断する」とされており、これまでも各金融機関においてリスク特性等を判断し、必要に応じて安全対策基準を適用する形となっていました。

今回の改訂において本基準の適用対象として定義された「金融情報システム」は、「顧客に商品・サービスを提供するために利用する情報システム」です。従って、「基幹業務のオンラインコンピュータ・システム」に加えて、それ以外のシステムのうち顧客に商品・サービスを提供するために利用されるものが明確に適用対象に含まれることとなりました。「金融情報システム」以外のシステムについては、これまでと同様に適用対象外となりますが、技術基盤やリスク特性等に類似性がある場合、本基準を適宜取り入れることとされています。

Ⅱ 特定システム

（Ⅱ－1）「外部性」とは、具体的に何を指すのか。

（答）

例えば、個別金融機関等におけるシステム障害等によって、個別金融機関等のみならず、他の金融機関やその顧客に影響を与える可能性のある性質をいいます。なお、「外部性」には、自社の顧客への影響は含まれません。

（Ⅱ－2）「外部性」に「重大な」を付けることの意味は。

（答）

金融機関等の情報システムにおいて、外部性を有するシステムは多岐にわたりますが、その中でも例えば、為替や預金を取り扱うシステムは、深刻なシステム障害が発生した場合、他の金融機関やその顧客に対して広く影響を及ぼし、社会全体に経済的損失を与える可能性があります。こうした情報システムを「重大な外部性」を有するシステムといいます。リスクベースアプローチを採用する場合であっても、「重大な外部性」を有するシステムは、システム障害に伴う影響を正確に把握し、障害を防止するためのコストを事前に算定・内部化して、安全対策の立案に的確に反映することは困難です。従って、「高い安全対策」を適用することが必要となります。

（Ⅱ－3）FISCにて「重大な外部性」にあたる具体例を示せないのか。

（答）

Ⅱフレームワーク p 12 の脚注 12 には、「重大な外部性」を有すると思われる代表的なシステムや、業態によって「重大な外部性」を有する可能性のあるシステムを例示しています。各金融機関の情報システムのリスク特性が異なる中、これ以上の具体例の列挙は難しく、また無理に列挙すると誤解を生む可能性もあるため、こうした記述にとどめています。

（Ⅱ－4）機微情報を保有するシステムで示される「機微」にあたる情報を具体的に示してほしい。

（答）

金融庁の「金融分野のおける個人情報保護に関するガイドライン」で定めるセンシティブ情報が参考となります。もっとも、各金融機関等において独自に機微情報に位置付けられる情報もあると考えられます。本人の許諾なく、その情報が流出した場合、経済的損失に留まらず、プライバシー等、個人の人権等の侵害といった広範かつ甚大な損失を被る可能性がある情報を、みずから判断していただくことになります。

Ⅲ 基礎基準・付加基準

（Ⅲ－1）基礎基準の中にある「必要である」は、すべての金融情報システムにおいて「必須対策」となるのか。基準によっては必ずしもそうとはならないケースがあるのではないか。

（答）

システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要となります。例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要です。その旨、「Ⅱフレームワーク１．総論(2) 基準の分類及び(4) 安全対策決定のプロセス」に記載しています。

（Ⅲ－2）これまで「基準項目の解説」の例示部分の記載において、語尾が「必要である」となっていた箇所が、記述の統一によって「必要である」の記載が削除されているが、これに伴い基準が緩和されたと考えて良いのか。

（答）

これまでも安全対策基準において、「基準項目の解説」で示された「～のようなものがある」等の対策は、具体的な例示と定義されており、今回の改訂によってその位置付けに変更はありません（基準が緩和されたわけではありません）。

これまで、例示は選択的に適用する対策という位置づけが必ずしも明確ではありませんでしたが、今回の改訂において、例示はリスクベースアプローチによって選択的に適用する対策として位置付けることを明確化しました。

なお「～のようなものがある」等の記載は、今回の改訂によって「以下の例がある」に記述を統一しています。

（Ⅲ－3）基礎基準の解説部分に「～重要度を考慮し」といった表現が複数あるが、その表現はリスクベースアプローチを表すもので、基礎基準にそぐわないのではないか。

（答）

基礎基準、付加基準の「必須対策」には、「個人データを扱うシステムにおいては～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれています。その点に留意する必要があることを、「Ⅱフレームワーク１.総論(2) 基準の分類及び(4) 安全対策決定のプロセス」に記載しています。

（Ⅲ－4）基礎基準の選定根拠として、完全性や可用性の観点も重要ではないか。

（答）

基礎基準の選定根拠については、「Ⅱ フレームワーク１． 総論(2)基準の分類」に記載しております。統制・監査に関する基準、顧客データ漏えい防止に関する基準、コンティンジェンシープラン策定に関する基準については、リスクベースアプローチを採用する場合であっても、適用必須の基準と位置付けられます。完全性や可用性に関する基準については、金融情報システムのリスク特性が多岐にわたるため、すべての基準を基礎基準とすることは適当ではないとの検討結果になりました。そこで、「システムの不正使用防止に関する基準」及び「システムの運行管理に最低限必要な基準」を基礎基準に加えることにしました。完全性や可用性に関連する重要な基準は、それらに織り込まれる形となっています。

（Ⅲ－5）設備基準について、「基礎基準」及び「付加基準」を区分し、リスクベースアプローチの考え方を適用する必要があるのではないか。

（答）

設備基準については、収納するコンピュータシステムに求められる基準を一意に定めることが難しいことから、基礎基準及び付加基準を区分していません。また、設備基準は、もともと、センターや本部・営業店、提携先等といった対象拠点等に応じて、適用すべき対策と適用が望ましい対策に整理されており、リスクベースアプローチの考え方を必要としないと判断しました。

Ⅳ 外部委託管理

（Ⅳ－1）APIを接続する際に適用される対策が「API接続チェックリスト」と安全対策基準のダブルスタンダードになるのではないか。

（答）

「ＡＰＩ接続チェックリスト」は、ＡＰＩを接続する際、主に金融機関等が、ＡＰＩ接続先事業者に対し確認を求めるものとなります。一方、安全対策基準における基礎基準は、金融機関等みずからが保有・運用する金融情報システムにおいて最低限実施すべき対策となります。「ＡＰＩ接続チェックリスト」は、改訂後の安全対策基準（基礎基準）を踏まえながら、チェックリストの試行結果等も勘案して、今後完成バージョンを策定する予定であり、その検討の中で、ダブ

ルスタンダードにならない配慮を行っていくものと考えております。

（Ⅳ－2）安全対策基準が対象とするクラウドサービスは定義されているのか。

（答）

米国の NIST（National Institute of Standards and Technology ： 国立標準技術研究所）におけるクラウドの定義を採用しています。

＜参考＞【NIST におけるクラウドの定義】

最小限の管理負荷やプロバイダー交渉だけで、迅速に提供され稼働する構成変更自在のコンピュータ資源（ネットワーク、サーバー、記憶装置、サービス等）の共有プールに対する、ネットワークを通じた便利で随時のアクセスを可能とするモデル。