参考

金融機関等コンピュータシステムの安全対策基準における関連項目の要旨

設備基準

【設 16】 入退館管理を確実に行うことによる不法侵入防止、不審物の搬出入防止のため、コンピュータセンターについて、常時利用する出入り口は一箇所とし、出入管理設備、防犯設備を設置するよう規定している。出入管理設備としては、警備員による識別や機械による識別方法を例示している。

【設２６】コンピュータ室やデータ保管庫については、機密漏洩防止の観点からも専用の独立した室とすることとしている。また、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することは、入退室管理の徹底を欠くなど、運用管理上の問題があり、機密漏洩や不正行為が生じやすいため、避けることが必要としている。

【設１２２】本部や営業店のサーバー設置場所については、侵入、破壊、機密漏洩を防止するため、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としている。

運用基準

【運１１・１２・１３】コンピュータセンターやコンピュータ室等重要な室へ出入する人・物を管理するため、資格付与および鍵の管理、入退館管理、入退室管理を行うよう規定し、具体的な管理方法についても例示している。

【運１８】機密情報等の各種資源やシステムへのアクセスを管理するため、アクセス権を与える場合の手続きを明確に定め、それを適切に保つための見直し手続きを明確にするよう規定している。また、アクセスに用いるＩＤはグループでの共用を避けるよう推奨し、その他管理上の留意事項を記述している。

【運５６】外部接続時の運用管理方法を明確にすることにより、データ漏洩や不正アクセス等を防止するため、相手先の確認や、接続条件の登録･変更等を適切に行うよう規定している。また、接続先確認や外部接続の利用管理上の留意事項について例示している。

【運１０３】インターネット等の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の確認機能やアクセス制限機能、不正防止機能を設けるよう規定している。また、これらの具体的な実現方法について例示している。

技術基準

【技３１】不正アクセス等からデータを保護するため、プログラムとファイル間のアクセス権限チェック機能を設けることとし、その実現方法を例示している。

【技３７】不正使用を防止する観点から、アクセス状況を管理するため、システムやデータへのアクセス履歴を取得し、監査証跡として必要期間保管するとともに定期的にチェックするよう規定している。また、具体的な履歴の取得項目やタイミングについて例示している。