第４　インターフェイスシステムの環境及び設備
１　建物及び重要機能室
⑴　建物等への侵入の防止等
ア　インターフェイスシステムを設置する建物及び重要機能室（以下「建物等」という。）の壁、窓、ドア等が容易に破壊されないよう必要な措置を講ずること。
イ　建物等への侵入を検知するための措置を講ずること。
ウ　電力及び電気通信回線の切断等を防止するための措置を講ずること。
エ　重要機能室の外に設置された関連設備に対する不当な接触の防止について、必要な措置を講ずること。
⑵　重要機能室の配置及び構造
ア　重要機能室の配置及び構造については、セキュリティ対策及び保守が容易に行えるよう配慮すること。
イ　重要機能室については、外部に対してその表示を行わない等、できるだけ所在を明らかにしないようにすること。
ウ　重要機能室に、緊急事態発生の際の連絡設備を設ける等、連絡体制を整備すること。
エ　電子計算機室及び可搬記憶媒体等保管室は、他の部屋と区分された、施錠可能な専用の部屋とすること。施錠可能な専用の部屋を確保できない場合は、電子計算機及び電気通信関係装置を厳重に固定し、可搬記憶媒体及びドキュメントを専用保管庫により施錠保管すること。
オ　電子計算機室及び可搬記憶媒体等保管室の常時利用する出入口を限定すること等により、侵入の防止を容易に行えるよう配慮すること。
２　障害の防止等
⑴　電気的及び機械的障害の防止等
インターフェイスシステムの構成機器又は関連設備の電気的及び機械的障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
⑵　水又は蒸気による障害の防止等
水又は蒸気によるインターフェイスシステムの構成機器又は関連設備の障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
⑶　火災による破損の防止等
建物等からの出火の防止のため、必要な措置を講ずること。また、建物等の火災によるインターフェイスシステムの構成機器又は関連設備の損傷を防止し、それらの損傷の発生を検知し、及びこれらの損傷が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
⑷　地震による破損の防止等
地震による建物等又はインターフェイスシステムの構成機器若しくは関連設備の損傷を防止し、これらの損傷を検知し、及びこれらの損傷が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
⑸　急激な温湿度変化等に対する措置
空気調和設備について、その容量に配慮するとともに、急激な温湿度変化等に対する措置を講ずること。
⑹　転倒、移動等に対する措置
インターフェイスシステムの構成機器及び関連設備について、転倒、移動等に対する措置を講ずること。
⑺　その他の障害の防止等
動物等によるインターフェイスシステムの構成機器及び関連設備の障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を行うため、必要な措置を講ずること。
３　電気通信回線の設備
電気通信回線からのデータの盗取を防止するため、インターフェイスシステムとコアシステム又は他のインターフェイスシステムとを結ぶ電気通信回線について、総務大臣が別に定める高度なセキュリティを確保した行政専用の電気通信回線を使用すること。ただし、同一の電子計算機室にある等情報の盗取の防止について必要な措置が講じられていると認められる場合については、この限りでない。
第５　インターフェイスシステムの管理
１　入退室管理
⑴　入退室及び鍵の管理
ア　重要機能室への入室者を限定すること。
イ　重要機能室の出入口の鍵を所定の場所に保管し、その管理は定められた者が行うこと。
ウ　重要機能室への入室者が入室する権限を有することを確認する方法をあらかじめ定めるとともに、重要機能室に入室しようとする者に重要機能室の出入口の鍵を貸与する際に、その者が入室する権限を有することを確認すること。
エ　重要機能室への入退室については、入退室管理台帳により適切に管理すること。
⑵　搬出入物品の確認
重要機能室へ物品を搬出入する際、重要機能室に入室する権限を有する職員に当該物品の内容を確認させること。
⑶　重要機能室の管理
インターフェイスシステムの構成機器及び関連設備等の盗難、損壊等を防止するため、重要機能室に入室する権限を有する者が不在となる時の重要機能室の施錠等、必要な措置を講ずること。
２　インターフェイスシステムの通信制御等
⑴　アクセス権限の限定
インターフェイスシステムの運用保守を実施する職員等必要な者に対してのみ、電子計算機、データ、ドキュメント、ファイル、可搬記憶媒体等に関し、必要なアクセス権限を付与すること。
⑵　ファイアウォールによる通信制御
電気通信回線に接続する電子計算機若しくは電気通信関係装置における不正行為又は電子計算機若しくは電気通信関係装置への不正アクセス行為に対して情報提供ネットワークシステムを保護するため、インターフェイスシステムとコアシステム又は他のインターフェイスシステムとの間にファイアウォールを設置し、通信制御を行うこと。ただし、同一の電子計算機室にある等、通信制御を行う必要がないと認められる場合については、この限りでない。
⑶　通信相手の認証
インターフェイスシステムとコアシステム又は他のインターフェイスシステムとの間の通信について、通信相手の認証を行うこと。ただし、同一の電子計算機室にある等、通信相手の認証を行う必要がないと認められる場合については、この限りでない。
⑷　通信の暗号化
インターフェイスシステムとコアシステム又は他のインターフェイスシステムとの間の通信について、暗号化を実施すること。ただし、同一の電子計算機室にある等、通信の暗号化を行う必要がないと認められる場合については、この限りでない。