物理的管理規程

1.0版

物理的管理規程

物理的管理規程

１　趣旨

本規程は、敷地・建物・室（サーバルーム等（以下、「サーバルーム」という））・機器・設備等を保護し、それらの損傷や利用の妨害、許可されていないアクセスを防止し、格納する情報の安全性を確保することを目的とする。

２　対象者

敷地・建物・室（サーバルーム等）の設置と利用、機器・設備等の利用に関わるすべての従業員。

３　対象システム

敷地内のすべての情報システム及びすべての機器。

４　遵守事項

４．１　物理的セキュリティ

４．１．１　セキュリティ区画の設定

（A.11.1、A.11.1.2、A.11.1.3、A.11.1.4）

対象物が必要なセキュリティ条件が異なる場合は、セキュリティ区画を明確化し、以下を遵守しなければならない。

（１）重要度の高い機器・設備を設置する場所にはその重要度に応じたセキュリティ区画が設定されなければならない。

（２）セキュリティ区画はその範囲を明確にしていなければならない。

（３）セキュリティ区画の管理については管理責任者を置かなければならない。

（４）セキュリティ区画には施錠設備を設けなければならない。

（５）セキュリティ区画は区画およびそこに設置する機器・設備等に関するセキュリティ上の各種のリスクを評価した上で必要な対策を実施しなければならない。リスクの要素には以下のものがある。

・盗難、破壊、地震、火災、水害等の水の事故、ほこり、振動、化学作用、電源事故、電磁波、静電気、小動物等の侵入等

４．１．２　セキュリティ区画の運用

（A.11.1.3）

セキュリティ区画の運用では、以下を遵守しなければならない。

（１）セキュリティ区画は従業員不在時には施錠しなければならない。

（２）セキュリティ区画への入場は、管理責任者の許可を受けて登録した特定のメン

バに制限しなければならない。

（３）セキュリティ区画への未登録者の入場については必ず入退場を記録し、登録メンバが同伴しなければならない。

（４）セキュリティ区画に入場する外部からの来訪者には区画内での注意事項を事前に説明しておかなければならない。

（５）セキュリティ区画に入場可能な登録メンバは定期的に見直さなければならない。

（６）セキュリティ区画に入場するものは身分証明となるカードあるいはバッジ等を常に明示しておかなければならない。また従業員は身分証明の明示がない入場者の相互確認を行わなければならない。

４．１．３　機器・設備の保護

(A.11.2.1)

機器、設備を保護するため、以下を遵守しなければならない。

（１）機器・設備の設置位置については、不正な操作が実施しにくく、不用意な操作ミス（間違いや見落とし）が起こりにくいように配慮しなければならない。

（２）重要度の高い機器・設備は他のものと分離して設置しなければならない。

（３）機器を設置する場合、落下や損傷の防止措置をとらなければならない。

（４）機器周辺では飲食・喫煙等を行ってはならない。

４．１．４　電源・空調の保護

(A.11.2.1、A.11.2.2、A.12.1.3)

電源、空調を保護するため、以下を遵守しなければならない。

（１）電源・空調室およびその設備には耐震、耐火、耐水などの防災対策を実施しなければならない。

（２）電源は、安定化装置の導入、負荷変動機器との配電隔離等によって電源容量と品質を確保しなければならない。

（３）電源は過電流・漏電等による機器への障害に対する保護措置をとらなければならない。

（４）電源には避雷設備を設置しなければならない。

（５）重要度の高い機器・設備に対する電源には、無停電装置、バックアップ電源等を設置しなければならない。

（６）空調設備は機器・設備を適切に運転するために十分な温度・湿度の調整能力を確保しなければならない。

（７）重要度の高い機器・設備に対する空調設備については予備装置を確保しなければならない。

４．１．５　ケーブルの保護

(A.11.2.3)

ケーブルを保護するため、以下を遵守しなければならない。

（１）ケーブルは、損傷（小動物対策を含む）や回線の盗聴を避けるため、保護用の電線管・カバーの使用や、敷設経路に対する配慮などの対策を行わなければならない。

（２）干渉防止のため、電源ケーブルと通信ケーブルは分離しなければならない。

（３）重要度の高いケーブルについては代替経路を準備しなければならない。

（４）ケーブルおよび端子については、未認可の機器・設備の接続や設置に対する監視または定期的チェックを行わなければならない。

４．２　サーバルームのセキュリティ

４．２．１　サーバルームの定義

サーバルームを以下と定義する。

（１）サーバルームは「重要度の高い情報資産が格納されているサーバがまとめて設置される部屋」とする。重要度の高い情報資産については別途定める。

（２）電子化されたデータとして保存する重要度の高い情報資産は、『システム利用規程』および『システム管理規程』に基づいて管理される場合を除き、サーバルームに設置するサーバでのみ保存されなければならない。

４．２．２　サーバルームの物理的セキュリティ

(A.11.1.3、A.11.1.4)

サーバルームを保護するため、以下を遵守しなければならない。

（１）サーバルームは独立した部屋として設置し、一般オフィスとの共用や他社オフィスとの隣接は避けなければならない。

（２）サーバルームは、危険物保管場所、火気施設、水道設備等、災害のリスクの大きい場所からは遠ざけて設置しなければならない。

（３）サーバルームの外観は目立ちにくいものとし、室名表示等も最小限にとどめなければならない。

（４）サーバルームの出入り口は原則 1 ヶ所に限定し、施錠設備を設けなければならない。

（５）サーバルームに窓を設けることは極力避け、設ける場合は網付きガラス・強化ガラス等を用いなければならない。

（６）サーバルームには設置する機器・設備の重要度に応じて、防犯カメラ、侵入報知機等の防犯設備の設置を検討しなければならない。

（７）サーバルームには必要に応じて、非常電話、非常ベル等の非常用連絡設備の設

置を検討しなければならない。

（８）サーバルームにはコピー・FAX 等、情報の複写や送信のための設備を設置してはならない。

４．２．３　サーバルームの運用

(A.11.1.2、A.11.1.5)

サーバルームの運用では、以下を遵守しなければならない。

（１）サーバルームは従業員不在時には施錠しなければならない。

（２）サーバルームおよびその鍵の管理については管理責任者を置かなければならない。

（３）サーバルームへの入室は、受付または認証装置（入館カード、パスワード入力、生体認証）等によって特定の登録メンバに制限されなければならない。

（４）サーバルームへの未登録者の入室および作業実施については管理責任者の許可と登録メンバの同伴がなければならない。

（５）サーバルームに入室可能な登録メンバは定期的に見直さなければならない。

（６）サーバルームに入室不要となった登録メンバは速やかに登録を解除し、入室のための認証を無効にしなければならない。

（７）サーバルームへの入退室は記録しなければならない。

（８）サーバルーム内で長時間作業を行う場合は一人では実施せず、必ず同伴者を伴わなければならない。

（９）サーバルーム内で管理責任者の許可なく撮影・録音を行ってはならない。

（１０）サーバルームには作業に必要のないもの（許可されていないパソコン、カメラ、携帯電話、スマートデバイス等）を持ち込みし置いてはならない。もし置いてあった場合は速やかに撤去しなければならない。

（１１）サーバルーム内の環境（機器・設備の有無、配置、利用状況等）は定期的に点検しなければならない。

４．３　職場環境におけるセキュリティ

４．３．１　書類・媒体等の取扱いと保管（クリアデスクポリシー）

(A.11.2.9)

書類、媒体等を取扱い、保管においては、以下を遵守しなければならない。

（１）従業員は使用していない書類や媒体をキャビネット等へ収納し、机上等に放置してはならない。

（２）従業員は重要度の高い書類や媒体を施錠保管し、特に必要な場合は耐火金庫・耐熱金庫に保管しなければならない。

４．３．２　画面に表示する情報の管理（クリアスクリーンポリシー）

(A.11.2.9)

離席時におけるパソコンについて、以下を遵守しなければならない。

（１）従業員は不正な操作や盗み見を防止するため、離席時にはログオフするか、画面・キーボードロック等の保護機能を使用しなければならない。

４．３．３　事務・通信機器の取扱い

(A.11.2.9、 A.12.1.1)

ホワイトボードやコピー機、FAX、プリンタなどの取扱いについて、以下を遵守しなければならない。

（１）従業員はホワイトボード等への書き込み内容を使用後に必ず消去し、放置してはならない。

（２）従業員はコピー機、FAX、プリンタ等の入出力書類を放置してはならない。特に重要度の高い書類は印刷および送受信の間、従業員が常に機器に（FAX の場合は送受信の両側とも）立ち会うようにしなくてはならない。

（３）従業員は FAX 送信時には必ず宛先を確認し、誤送信を防止しなければならない。

４．３．４　搬入物の受渡し

(A.11.1.6)

物の搬入にあたっては、以下を遵守しなければならない。

（１）搬入物の受渡しについては受渡し場所を設置し、サーバルームおよびセキュリティ区画とは分離しなければならない。

（２）受渡し場所への従業員以外のスタッフによるアクセスは、必ず従業員の監視付きで行い、アクセスを記録しなければならない。

（３）搬入物の受入れを行う従業員は受入れの際に危険物持込や情報漏洩等のリスクがないかどうか点検しなければならない。

（４）搬入物が登録の必要な情報資産である場合、搬入物の受入れを行う従業員は受入れ後速やかに登録作業を行わなければならない。

（５）郵便物の受入れ場所には盗み見や抜き取りを防止する対策を行わなければならない。

４．３．５　盗み聞きによる情報漏えい防止

(A.7.2.2)

盗み聞きに対応するため、以下を遵守しなければならない。

（１）従業員は電話や立ち話、オープンな会議スペースでの発言について、盗み聞きを防止するよう配慮しなければならない。

５　運用確認事項

物理的管理において、以下が行われていることを確認しなければならない。

（1）本規程に基づき、記録・運用が管理されている事を定期的に確認すること。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。