

物理的及び環境的セキュリティ規程	
文書番号	
制定日	
改定日	
総ページ数	9ページ（表紙含む）

【機密分類】社外秘

物理的及び環境的セキュリティ規程

株式会社

文書番号		文書名	物理的及び環境的セキュリティ規程	ページ	2/9
章番号		内容			

制定 / 改定履歴

版数	制定または改定主旨	承認	査問	作成	制定 / 改定日
1	制定				

配付

配付先の定義

配付用ではない。

配付先リスト

配付用ではない。

文書番号		文書名	物理的及び環境的セキュリティ規程	ページ	3/9
章番号		内容			

目次

1	目的	4
2	責任	4
3	要求事項	4
4	承認	4
5	セキュリティを保つべき領域	5
5.1	物理的セキュリティ境界	5
5.2	物理的入退室管理	5
5.3	オフィス、部屋及び施設のセキュリティ	7
5.4	外部及び環境の脅威からの保護	8
5.4	セキュリティが保たれた領域での作業	8
5.5	一般の人の立ち寄り場所及び受け渡し場所	9
6	装置のセキュリティ	エラー! ブックマークが定義されていません。
6.1	装置の設置及び保護	エラー! ブックマークが定義されていません。
6.2	支援ユーティリティ (電源)	エラー! ブックマークが定義されていません。
6.3	ケーブル配線のセキュリティ	エラー! ブックマークが定義されていません。
6.4	装置の保守	エラー! ブックマークが定義されていません。
6.5	構外にある装置のセキュリティ	エラー! ブックマークが定義されていません。
6.6	装置の安全な処分又は再使用	エラー! ブックマークが定義されていません。
6.7	装置の移動	エラー! ブックマークが定義されていません。

文書番号		文書名	物理的及び環境的セキュリティ規程	ページ	4/9
章番号		内容			

1 目的

本書は、ISO27001:2005 附属書 A「詳細管理策」の「7.物理的及び環境的セキュリティ」要求事項に対応する、内部規定である。

2 責任

情報セキュリティ管理責任者

3 要求事項

本書は次の管理目的を達成する為に規定する。

1. 業務施設及び業務情報に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。
2. 資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため。

4 承認

社長

文 書 番 号		文 書 名	物理的及び環境的セキュリティ規程	ペ ー ジ	5/9
章 番 号		内 容			

5 セキュリティを保つべき領域

【管理目的】

目的：組織の施設及び情報に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

5 . 1 物理的セキュリティ境界

【要求事項】

情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いること。

【ポリシー】

- (1) 第3者アクセスからの保護：当社のオフィス、コンピュータ施設及びその他重要な情報資産がある場所は、ガードマン、受け付け担当等のスタッフによって、守られなければならない。
- (2) 物理的セキュリティ計画：当社の全てのコンピュータ施設は、物理的セキュリティ計画が立案され、毎年設備担当管理者によってレビューされなければならない。
- (3) コンピュータ施設の場所：サーバや通信設備は、ビルの1階で水や火を扱う場所から離れ、外壁から離れた窓の無い内壁に囲まれた場所に設置する。
- (4) コンピュータ施設の防火：コンピュータ施設を囲う防火壁は、難燃性で最低1時間の火災に耐えるものである。又そこに付くドアや換気ダクトは火災の際、自動遮蔽式でなければならぬ。
- (5) コンピュータ施設のドアの強さ：コンピュータ施設に付けるドアは、無理に押し入ることができない、十分な強度がなければならない。
- (6) コンピュータ施設のドアの開閉：コンピュータ施設のドアは、開けたら直ちに自動的に閉じるものでなければならない。又開いたままの時に作動するアラームが確実に動作するか定期的に検査しなければならない。
- (7) コンピュータ施設の第2ドア：コンピュータ施設の入口のドアには第2ドアを、入退室管理システムとともに設置する。

5 . 2 物理的入退室管理

【要求事項】

文 書 番 号		文 書 名	物理的及び環境的セキュリティ規程	ペ ー ジ	6/9
章 番 号		内 容			

セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護すること。

【ポリシー】

- (1) 重要情報に対するアクセス制御：重要情報を含む全てのオフィス、コンピュータ室、作業場所は、物理的なアクセス制御を施さなければならない。
- (2) オフィスの施錠：オフィスを無人にする場合は、必ず施錠すること。
- (3) IDバッジ：全ての従業員は、安全が保たれた施設内では、IDバッジを衣服の上に着用しなければならない。IDバッジは写真と情報が明瞭に見えなければならない。
- (4) 仮IDバッジ：従業員がIDバッジを忘れた場合、1日限りのIDバッジを適用しなければならない。IDの発行には免許証等写真付きの証明手段によって行われる。
- (5) バッジによるアクセス制御：従業員はアクセス制御された入口で、各自のバッジのアクセス権限が確認されなければ、入る事が許可されない。
- (6) 同時アクセスの禁止：従業員はセキュリティで制限されたエリアに入る入口等を通過する際、同時に見知らぬ他人が通過することが無い様に注意しなければならない。
- (7) データセンターの2重扉：データセンターの人が通行する入口は、インターロック式の2重扉を備え、不審者のすり抜けを防ぐ。
- (8) 物理的不正アクセスの試みの禁止：従業員は組織の認可されていない施設の、物理的不正アクセスを試みてはならない。
- (9) 持ち物検査：組織の施設を出る全ての人は、守衛によりバッグ類の中を調べられなければならない。
- (10) アクセス制御記録の維持：施設等のセキュリティ部門は、直近の物理的アクセス記録を最低3か月間は保持しなければならない。
- (11) 退職社員のアクセス権限の失効：社員が退職してオフィスを去る時、その社員が使用していた物理的アクセス権限を全て失効させるか、変更しなければならない。
- (12) 退職社員の重要施設へのアクセス権限の無効：退職社員の重要施設へのアクセス権限は直ちに無効にしなければならない。
- (13) 管理職の物理的アクセス権限監査：管理職の物理的アクセス権限は常に更新され、アクセス権限を持つ他の委任された管理職によって、定期的レビューされなければならない。
- (14) IDバッジ付与状況報告：各部門に於けるIDバッジ付与状況を部門長に対して毎月報告し、レビューを受けなければならない。

文 書 番 号		文 書 名	物理的及び環境的セキュリティ規程	ペ ー ジ	7/9
章 番 号		内 容			

- (1 5) 外来者の認証: 組織のセキュリティ制限領域に入ろうとする外来者は、写真付きの証明を提示し、入場記録にサインしなければならない。
- (1 6) 来訪者への同伴: オフィスを含め組織の施設への外来者は、認可された社員が必ず同伴しなければならない。これには顧客、元社員、社員の家族、保守契社員、宅配業者、警察官等制限が無い。
- (1 7) 時間外の来訪者に対する同伴: 通常業務時間外の組織の施設、オフィスへの来訪者に対しては、認可された部門のマネージャが同伴しなければならない。
- (1 8) 第三者の監視: 認可された契約社員やコンサルタント等、社員で無い者が重要な情報資産のある場所にいる時は、常に監視しなければならない。
- (1 9) IDバッジを付けていない場合: 正しいIDバッジを付けていない人物を発見したら、直ちにその旨を質問し、受付へ同行させなければならない。
- (2 0) 同伴者のいない外来者: 従業員は組織のセキュリティ領域内を同伴者無しでいる外来者を見たら、直ちに質問し受付や守衛所へ同行させなければならない。
- (2 1) データセンターやコンピュータルームへの来訪者: 機器のメンテナンス等以外、明らかにそこに用事がないと思われる外来者を、データセンターやコンピュータルームへ入室させてはならない。
- (2 2) コンピュータ及び通信システムへの物理的アクセス: サーバや通信システムが収められたビル等は、物理的セキュリティ規定に従い、外部からの不正アクセス対策を講じなければならない。
- (2 3) 重要情報を取り扱う場所: 重要情報を取り扱う場合、不正アクセスや情報に損傷を与えない物理的に保護された場所で行わなければならない。
- (2 4) コンピュータルームへのアクセス: プログラマーやコンピュータユーザ等以外、業務上不要な者はコンピュータルームへの立ち入りを禁止する。
- (2 5) コンピュータルームスタッフのアクセス: コンピュータルームの運用管理者は、4半期毎に、コンピュータルームにアクセスするスタッフのリストをレビュー、更新しなければならない。
- (2 6) メディア保管場所へのアクセス: 重要な磁気メディア、書類の保管場所は、一般従業員のアクセスを制限する。
- (2 7) コンピュータ施設の見学: 一般へ、主要なコンピュータや通信施設の

5 . 3 オフィス、部屋及び施設のセキュリティ

【要求事項】

オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する

文 書 番 号		文 書 名	物理的及び環境的セキュリティ規程	ペ ー ジ	8/9
章 番 号		内 容			

こと。

【ポリシー】

- (1) 不正な監視装置盗聴装置等の搜索：通信システム部門マネージャは、重要施設内に不正な盗聴装置や録音装置等が無いが、定期的に搜索をする。
- (2) サーバや通信機器の保護：サーバや主要な通信機器は鍵の架かる部屋に保護する。
- (3) コンピュータルームのドアが開放されている時：コンピュータルームのドアが開放状態にある時は、施設保安部門の要員によって、監視しなければならない。
- (4) 機密情報保管エリア内の機器：組織の機密情報保管エリア内には、プリンター、コピー、FAXを設置してはならない。
- (5) コンピュータ及び通信システムセンターの掲示：コンピュータ及び通信システムセンターの建物、部屋を示す掲示をしてはならない。

5 . 4 外部及び環境の脅威からの保護

【要求事項】

火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害による被害からの物理的な保護を設計し、適用すること。

【ポリシー】

- (1) 重要な情報資産が格納された部屋には火災に対する監視及び 소화設備を備える事。
- (2) 情報のバックアップは、別な建物に保管する等、災害の影響を受けない事。
- (3) 情報な情報資産が格納された施設、部屋はそれと判る表示をしない事。

5 . 4 セキュリティが保たれた領域での作業

【要求事項】

セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し、適用すること。

【ポリシー】

- (1) コンピュータセンターの人員配置：組織の主要なコンピュータセンターは、1年365日、1日24時間、技術スタッフを常駐させなければな

文 書 番 号		文 書 名	物理的及び環境的セキュリティ規程	ペ ー ジ	9/9
章 番 号		内 容			

らない。

- (2) 携帯電話の使用：マシン室内での携帯電話の使用は禁止する。
- (3) 制限エリア内での作業：重要な情報がある制限エリア内では一人きりで作業をしてはならない。
- (4) 制限エリア内での作業時間：認可された従業員の、重要情報が存在する制限エリア内での作業は、認可された時間内に限られる。
- (5) 廃棄処分となった情報機器の格納：廃棄処分となった情報機器の格納場所は施錠し、できればリモートで監視できる様にする。
- (6) 通信機器エリア：主要な通信機器（電話交換機、ルータ、ハブ、通信関連サーバ等）が収まる部屋は常に施錠される。もし外来者入室する場合は認可された技術スタッフが同伴し行動を監視する。
- (7) 録音又はビデオ機器：組織の制限エリア内でカメラ、録音機、ビデオの使用を禁止する。

5 . 5 一般の人の立ち寄り場所及び受け渡し場所

【要求事項】

一般の人が立ち寄る場所（例えば、荷物などの受渡し場所）及び、敷地内の、許可されていない者が立ち入ることもある場所を管理し、また、可能なならば、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離すこと。

【ポリシー】

- (1) コンピュータルームへの配送：コンピュータルームは、そこへの物品の受け渡しの為の安全な受け渡しエリアを設けなければならない。