# IT-Professor

物理セキュリティ対策基準

2018年7月

IT-Professor IT 部

## 更新履歴

	更新日	更新箇所	更新内容
1	2021/10	初版	

## 1. 趣旨·目的

この実施基準は、IT-Professor(以下、IT-P と称す)グループ情報セキュリティポリシー第 5章(第 14、15 条)の規定に基づき、情報資産の設置・保管に対する物理的な安全対策について、必要な基準を定めたものである。

## 2. 定義

本基準で用いる主な用語の定義は、以下のとおりとする。

1) データセンター

情報システムを安全に収容するための、情報システム安全対策基準(経済産業省)に準拠した専用施設。

## 3. 対象

- 1) 対象となる情報資産
  - ・情報システム(ハードウェア、ソフトウェア、ネットワーク)
  - ・電子化情報を保存した外部媒体

## 4. 役割

次のとおり役割を定義する。

- 1) 部門長
  - 自部門の情報資産の設置・保管に対する物理的な安全管理策を講じる責任を負う。
- 2) 従業員等

本基準および自部門の物理的な安全管理策に基づき、情報資産を取り扱う。

## 5. 遵守事項

情報の漏洩または改ざん等の不正行為や情報システムの破壊、盗難等から物理的に保護するため、本基準で定めた事項を遵守しなければならない。

#### 1) 入退管理策

- i 情報資産の設置・保管場所の物理的な安全を確保するため、許可のない者の入退館を制限しなければならない。
- ii 特に、重要な情報または情報システムの設置・保管場所については施錠等による物理的な設備対策を講じ、申請により許可された者のみが出入りされるよう管理すること。
  - ・入退館者の氏名、所属、連絡先、入退館の目的、日付・時間など記録すること。
  - ・社員カードや入退館許可証など身分を証明できるものを着用すること。

#### 2) 情報システムの設置場所

- i 企業活動への影響が大きい情報システムは、原則として情報システム安全対策基準に準拠したデータセンター(あるいはデータセンター相当の施設)に設置すること。
  - ii 前項以外のシステムの設置にあたっては、次の事項を考慮することが望ましい。
  - ・ 火災や地震等の災害、電源等設備の障害、不法侵入者による破壊行為等の危険から物理的に保護するため、防災・防犯設備及び無停電電源設備や空調設備などが備えられていること。
  - ・情報システムを設置する建物・場所への入退館は許可された者のみに制限されるととも に、受付の設置、カード等の制御による物理的な入退管理を実施すること。
  - ・情報システムの設置場所で外部の作業者が作業を行う場合には、必ず従業員の立会いの下で行い、その内容を記録すること。

#### 3) 機器・媒体に関する対策

- i PC は、盗難や不正操作を防止し、また誤操作が起こりにくいように配慮のうえ設置すること。 またノート PC 等可搬性の高い機器を安全に保管するため、施錠可能な場所・保管庫を備えること。
- ii 外部媒体は、盗難や紛失の防止に配慮のうえ、保管・管理すること。また必要に応じて、 施錠可能な保管庫を設置すること。
- iii 重要度の高い機器、および外部媒体は他のものと分離して設置、保管できるよう保管場所や保管方法を考慮しなければならない。

#### 4) 移動・持ち出し時の対策

- i 重要な情報が保管された機器・外部媒体は、事前に上長の許可を得たうえで、持ち出すこととし、盗難や紛失対策として台帳等管理簿にて適切に管理すること。
  - ・利用者の氏名、所属、連絡先、利用目的、持ち出しの日付・時間などを記録すること。
  - ・台帳等管理簿を定期的に点検し、機器・媒体等の紛失がないか確認すること。
  - ii 機器の修理は、重要な情報が保護されていることを確認したうえで依頼しなければならない。
    - ・修理に出す前に、情報を退避すること。
    - ・ 故障の内容により、情報が退避できない場合は、機密保持(守秘義務)契約を締結した

うえで依頼すること。

iii ノート PC・媒体等を外部に持ち出して使用する際には、常に携行するなど慎重に取り扱い、盗難や紛失に十分注意しなければならない。

### 5) 廃棄に関する対策

i 機器・媒体を廃棄する場合には、保存されていた情報を再生不可能な状態に消去または破壊し廃棄すること。但し、リース・レンタル品は情報を消去し、初期化等決められた手続きに従うこと。

- ・ 消去ツールなどを利用し、データおよびソフトウェアを再使用できないよう完全に消去する こと。
  - ・書込み制限によりツール等で消去できない場合、物理的に破壊・破砕すること。
- ・外部委託する場合は、信頼できる専門業者を選定し、機密保持(守秘義務)契約を締結したうえで依頼すること。

## 6. 例外事項

法令または別途定められた規程等により特別の定めがある場合には、責任体制に基づき適切に判断し処理しなければならない。

## 7. 公開の範囲

本基準は、「社外秘」とし、IT-P グループの従業員等を対象に公開する

#### 8. 改廃

本基準は、定期的に見直しを行うこととし、IT 部にて適宜改定を行うこととする。

また、改定が必要と判断された場合は、速やかに変更を行い、責任体制(情報セキュリティ管理体制)を通じ、その内容をすべての従業員等に周知することとする。

## 改附則

本基準は、2021年10月1日より適用とする。