公益財団法人大阪市中小企業勤労者福祉サービスセンター
情報セキュリティ基本方針

令和６年５月８日

（目的）
第１条　この要項は、公益財団法人大阪市中小企業勤労者福祉サービスセンター（以下「センター」という。）が保有する情報資産の機密の保持及び正確性、完全性の維持を確保するため、情報資産の取り扱いと情報セキュリティ対策の基本的な考え方及び方策を定め、センターにおける情報資産の管理を徹底することを目的とする。

（定義）
第２条　この要項において「ネットワーク」とは、コンピュータ等を相互に接続するための通信網、その構成機器(ハードウエア及びソフトウエア）をいう。
２　この要項において「情報処理システム」とは、コンピュータ、端末装置、通信回線等により、電子情報を処理するシステムをいう。
３　この要項において「情報資産」とは、以下のものをいう。
（１）ネットワーク、情報処理システム及びこれらに関する設備、電磁的記録媒体（以下「情報システム等」という。）
（２）情報システム等で取り扱う電磁的な情報
（３）情報システム等の仕様書及びネットワーク図等のシステム関連文書
４　この要項において「情報セキュリティ」とは、情報資産の機密性、完全性及び可用性を維持することをいう。
（１）機密性とは、情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。
（２）完全性とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。
（３）可用性とは、情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（職員等の遵守義務）
第３条　すべての職員（非常勤職員及び臨時職員を含む。以下、「職員等」という。）に対して基本方針の趣旨を理解・認識し、遵守させるため必要な措置を講じる。また外部委託業者に対しても、契約を通じて、または別途取決めを行うことにより基本方針を遵守させるための必要な措置を講じる。

（情報セキュリティ管理体制）
第４条　センターの保有する情報資産について、事務局長が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

（情報資産の分類）
第５条　情報資産については、その重要度に応じて分類を行う。

（情報資産への脅威）
第６条　情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。
（１）部外者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難、故意の障害発生行為によるサービスの停止等
（２）職員等及び外部委託業者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等
（３）地震、落雷、火災等の災害並びに事故、故障等によるサービスの停止
２　上記の脅威を十分認識した上で、情報資産の分類の後、各々の情報資産に対する脅威の洗出しを行なうものとする。

（情報セキュリティ対策）
第７条　前条の洗出しにより明確になった脅威から情報資産を保護するために、以下のセキュリティ対策を講ずるものとする。
（１）物理的セキュリティ対策
　情報処理システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。
（２）人的セキュリティ対策
　情報セキュリティに関する権限や責任を定め、職員等に基本方針及び情報セキュリティに関する法令等の内容を周知徹底する等、十分な教育および啓発が行われるよう必要な対策を講ずる。
（３）技術的セキュリティ対策
　情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。
（４）運用におけるセキュリティ対策
　情報セキュリティに関する法令等及び基本方針の遵守状況の確認等の運用面の対策を講ずる。また、緊急事態が発生した場合に迅速な対応を可能とするための危機管理対策を講ずる。

（情報セキュリティ自己点検の実施）
第８条　情報セキュリティ基本方針の遵守状況を検証するため、定期的及び必要に応じて情報セキュリティ自己点検を実施する。

（情報セキュリティ基本方針の見直し）
第９条　情報セキュリティ自己点検の結果、情報セキュリティ基本方針の見直しが必要となった場合及び情報セキュリティに関する状況の変化への対応が必要となった場合には、情報セキュリティ基本方針を見直す。

（附則）
この基本方針は、令和６年５月８日から施行する。