

地方独立行政法人大牟田市立病院情報セキュリティ基本方針

1 目的

この基本方針は、地方独立行政法人大牟田市立病院（以下「法人」という。）の有する情報資産の機密性、完全性及び可用性を維持するための適正な管理運用を組織的かつ計画的に実施するため、法人における情報セキュリティの考え方及び対策に関し必要な事項を定めることを目的とする。

2 定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準（以下「対策基準」という）をいう。

(2) 情報セキュリティ

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。

(3) ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器をいう。

(4) 情報システム

コンピュータ、ソフトウェア、ネットワーク等で構成され、情報処理を行う仕組みをいう。

(5) 記録媒体

ハードディスク、フロッピーディスク、USBメモリ、CD-ROM、磁気テープその他これらに類する媒体をいう。

(6) 機密性

情報にアクセスすることを認められた者のみが、情報にアクセスできる状態を確保することをいう。

(7) 完全性

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。

(8) 可用性

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。

3 対象とする脅威

情報資産に対する脅威として、次の各号を想定し、情報セキュリティ対策を講じる。

(1) 部外者の侵入、不正アクセス、ウィルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、プログラム上

- の欠陥、操作ミス、故障等の非意図的要因による情報資産の漏えい、破壊、消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

4 対象範囲

(1) 対象部署の範囲

この基本方針が対象とする部署は、地方独立行政法人大牟田市立病院業務分掌規程（平成22年規程第3号）第2条に掲げる局、部及び室とする。

(2) 対象者の範囲

この基本方針が対象とする者は、法人の職員（地方独立行政法人大牟田市立病院職員就業規則（平成22年規程第4号）第1条に規定する職員）（以下「職員等」という。）とする。

(3) 対象情報資産の範囲

この基本方針が対象とする情報資産は、次の各号に定めるところによる。

ア ネットワーク、情報システム及び記録媒体

イ ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ 情報システムの仕様書及びネットワーク図等のシステム関連文書

5 職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たり情報セキュリティに関する法令、情報セキュリティポリシー（以下「ポリシー」という）及び情報セキュリティ実施手順（以下「実施手順」という）を遵守しなければならない。

6 情報セキュリティ対策

上記3の脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講じる。

(1) 組織体制

法人の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の管理

法人の有する情報資産に対して適切な情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ、情報システム室、ネットワーク、職員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

- (5) 技術的セキュリティ
コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
- (6) 運用
情報システムの監視、ポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、ポリシーの運用面の対策を講じるものとする。
- (7) 緊急時セキュリティ
情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応マニュアルの策定等、危機管理対策を講じる。

7 情報セキュリティ対策基準の策定

上記6に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める対策基準を策定する。

なお、対策基準は、公にすることにより法人の運営に重大な支障を及ぼすおそれがあることから非公開とする。

8 実施手順の策定

対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた実施手順を策定するものとする。

なお、実施手順は、公にすることにより法人の運営に重大な支障を及ぼすおそれがあることから非公開とする。

9 自己点検及び情報セキュリティ監査の実施

ポリシーの遵守状況を検証するため、定期的又は必要に応じて自己点検及び情報セキュリティ監査を実施する。

10 ポリシー及び実施手順の見直し

自己点検及び情報セキュリティ監査の結果、ポリシー及び実施手順の見直しが必要と評価された場合又は情報セキュリティに関する状況の変化に対応するため新たに対策が必要と判断された場合には、ポリシー及び実施手順を見直さなければならない。

付 則

この基本方針は、平成30年10月1日から施行する。