# 情報セキュリティ確保のための基本方針

## １．目的

本方針は、地方独立行政法人栃木県立がんセンター（以下「当センター」という。）が保有し、又は利用する全ての情報資産について、その機密性・完全性・可用性を確保し、サイバー攻撃、情報漏えい、システム障害その他のリスクから適切に保護することにより、法人業務の安定的かつ継続的な遂行並びに社会的信頼の維持を図ることを目的とする。

## ２．基本的な考え方

当センターは、情報システムが業務運営の基盤であることを踏まえ、情報セキュリティ対策を経営上の重要課題の一つとして位置付ける。

国、県及び各関係機関が示す情報セキュリティに関する指針等を踏まえ、組織的・人的・技術的及び運用的な対策を総合的かつ継続的に実施する。

## ３．用語の定義

本方針において使用する主な用語の定義は、次のとおりとする。

(1) 情報資産

情報システム、ネットワーク、サーバ、端末、クラウドサービス、電磁的記録媒体及びこれらにより取り扱われる全ての情報。

(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。

(3) 情報セキュリティポリシー

基本方針及び情報セキュリティ対策基準をいう。

(4) 機密性

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。

(5) 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。

(6) 可用性

情報にアクセスすることを認められた者が、必要な時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。

(7) インターネット接続系

インターネットの送受信、ホームページの管理及び公開を行うシステム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(8) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

(9) 情報セキュリティインシデント

情報資産の安全性を損なう、又はそのおそれのある事象をいう。このうち、業務の遂行に支障が生じた又は情報セキュリティが保てなくなったものを情報セキュリティ侵害という。

## ４．想定される脅威

当センターは、次に掲げる脅威を想定し、必要な対策を講じるものとする。

(1) 不正アクセス、マルウェア、ランサムウェア等のサイバー攻撃

(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、設計・開発の不備、プログラム上の欠陥、操作、設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器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) 職員等による誤操作、管理不備又は内部不正等

(4) 地震、落雷、火災等の災害、設備故障等によるシステム障害

(5) 外部委託先又はクラウドサービス等に起因するリスク

(6) 電力供給の途絶、通信の途絶等のインフラの障害からの波及等

## ５．適用範囲

本方針は、当センターが管理又は利用する全ての情報資産及びこれを取り扱う役職員、非常勤職員、派遣職員並びに業務委託事業者等に適用する。

## ６．職員等の遵守義務

５の範囲にあるすべての職員（以下「職員等」という。）は、本方針及びこれに基づき定める情報セキュリティ対策基準並びに実施手順を遵守し、情報セキュリティの確保に努めなければならない。

## ７．情報セキュリティ対策

上記４の想定される脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

サイバーセキュリティに関する責任の所在を明確にするとともに、全体を統括する体制及び実務を推進する体制を整備する。また、業務を委託する事業者を含めた適切な管理体制を確立する。

(2) 人的対策

職員等に対し、情報セキュリティに関する教育・啓発及び訓練を継続的に実施する。

(3) 物理的対策

サーバ室等の重要施設への入退室管理及び機器の盗難・破損防止対策を実施する。

(4) 技術的対策

アクセス制御、認証管理、暗号化、不正プログラム対策、脆弱性管理及びログ管理等

を適切に実施する。

また、クラウドサービス等を利用する場合にあっては、契約内容及び設定内容を十分に確認し、情報資産の安全性の確保を図る。

(5) 運用的対策

情報資産の重要度に応じた管理区分を設定し、平常時における適切な管理及び監視を行う。

## ８．インシデント対応

サイバーセキュリティに関するインシデントが発生した場合又はそのおそれがある場合には、別途定めるＢＣＰ（事業継続計画）との整合性を確保しつつ迅速かつ適切な対応を行い、被害の拡大防止及び早期収束を図るとともに、重要業務である医療サービスの継続性の確保又は早期復旧に向けた対応を適切に実施すること。

また、必要に応じて国、県や各関係機関及び所管部局と連携する。

## ９．監査及び点検

当センターは、本方針及び関連規程の遵守状況について、定期的に自己点検又は監査を実施し、その結果を踏まえ、必要な改善を行う。

## 10. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシー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に対応するため新たに対策が必要になった場合には、社会情勢、技術動向、脅威の変化等を踏まえ、システム委員会の下で見直すものとする。

## 11. 対策基準及び実施手順

本方針を具体化するため、対策基準として「総合情報システム運用管理規程」等を定め、実施手順として具体的なマニュアルを別に定める。また、大規模災害等に備えた「ＢＣＰ（事業継続計画）」を別途策定し、本方針との整合性を維持する。なお、当該対策基準及び実施手順については、公にすることにより当センターの業務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。

附　則

この基本方針は、令和８年４月１日から実施する。