亀岡市立病院
情報セキュリティポリシー

亀岡市立病院

令和8年４月

－ 目 次 －

（1）　職員
（2）　教育・訓練
（3）　外部委託に関する管理
（4）　パスワード等の管理
（5）　接続時間の制限

4　物理的セキュリティ
（1）　入退室の管理
（2）　職員の情報処理システムの機器管理
（3）　機器等の搬入・搬出
（4）　電源
（5）　配線

5　技術的セキュリティ
（1）　ネットワーク及び情報処理システムの管理
（2）　情報処理システムのアクセス制限
（3）　情報処理システムの開発・導入・保守
（4）　コンピュータウイルス対策
（5）　不正アクセス対策
（6）　セキュリティ情報の収集

6　運用
（1）　ネットワーク及び情報処理システムの監視
（2）　情報セキュリティポリシーの遵守状況の確認
（3）　セキュリティ障害時の対応

7　法令遵守

8　違反に対する措置

9　評価・見直し等
（1）　点検
（2）　情報セキュリティポリシーの更新

亀岡市立病院情報セキュリティポリシー

序章　亀岡市立病院情報セキュリティポリシーの構成

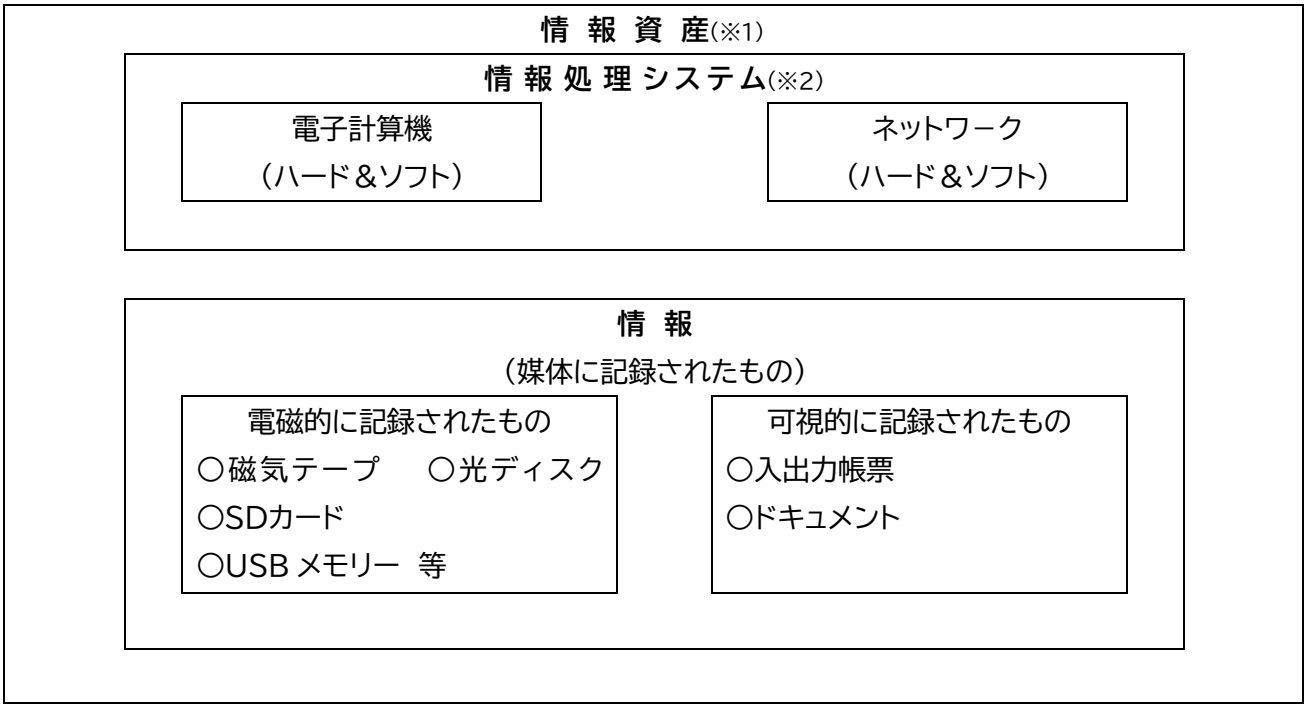
亀岡市立病院情報セキュリティポリシーとは、亀岡市立病院が所掌する情報資産(※1)に関する情報セキュリティ対策について、総合的、体系的かつ具体的にとりまとめたものである。

亀岡市立病院情報セキュリティポリシーは、亀岡市立病院が所掌する情報資産に関する業務に携わる全職員、非常勤、臨時職員（以下「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、亀岡市立病院情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の 2 階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報資産及び情報システム(※2)の具体的な運用管理として「亀岡市立病院情報システム運用管理規程」を策定することとする。

亀岡市立病院情報セキュリティポリシーの構成

文書名		内容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報資産に共通の情報セキュリティ対策の基準
亀岡市立病院情報システム運用管理規程		情報資産及び情報システムの具体的な運用管理の詳細



第1章　情報セキュリティ基本方針

1 目的

亀岡市立病院（以下、「本院」という。）が取り扱う情報資産には、患者の個人情報のみならず病院運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報資産を人的脅威や災害、事故等さまざまな脅威から防御することは、患者の財産、プライバシー等を守るためにも、また、継続的かつ安全、安定的な診療運営のためにも必要不可欠である。ひいては、このことが本院に対する患者からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、地域（他院、診療所等）での患者情報の共有化の実現が期待されており、本院がこれらに積極的な対応をするためには、本院が管理している全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件となる。

このため、本院の情報資産の機密性、完全性及び可用性(注)が維持するための対策を整備するため、亀岡市立病院情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

このうち、情報セキュリティ基本方針については、本院の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）/国際電気標準会議（IEC） 27000 情報技術-セキュリティ技術-情報セキュリティ管理システムに関する国際規格群（日本工業規格 JIS Q 27000）が定める用語

機密性（confidentiality）:情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること。

完全性（integrity）: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。

可用性（availability）:情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。

2 定義

（1）電子計算機等

・ハードウエア及びソフトウェアで構成するコンピュータ及び周辺機器並びに記録媒体をいう。

（2）ネットワーク

・電子計算機等を相互に接続するための通信網及びその機器（ハードウエア及ソフトウエア）で一体的に情報処理を行う仕組みをいう。

（3）情報処理システム

・電子計算機及びネットワークで構成され、処理を行う仕組みをいう。

・情報処理システムは、電子カルテシステム及びその他の部門システムをいう。

（4）情報資産

・情報処理システム及び情報処理システムの開発と運用に係る全ての情報並びに情報処理システムで取り扱う全ての情報をいう。なお、情報資産には紙等の有体物に出力された情報も含むものとする。

（5）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 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本院の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

4 情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は、本院の情報資産に関する業務に携わる全ての職員（非常勤職員及び臨時職員並びに外部委託事業者を含む。）とする。

5 職員等の義務

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つとともに、情報資産の利用にあたっては情報セキュリティポリシーを遵守するものとする。

6 情報セキュリティ管理体制

本院の情報資産について、適切に情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

7 情報資産の分類

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

8 情報資産への脅威

情報セキュリティポリシーを講ずる上で、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

特に、認識すべき脅威は以下のとおりである。

（1）権限外者による故意の不正アクセス又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、機器及び記録媒体の盗難、改造又は改変等。
（2）職員及び外部委託者による意図しない操作、故意の不正アクセス又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、機器及び記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏えい等。
（3）地震、落雷、火災等の災害や事故、故障等によるサービス及び業務の停止。

9 情報セキュリティ対策

本院の情報資産を上記 8 の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

（1）人的セキュリティ対策

情報資産に接する職員の情報セキュリティに関する権限や責任等を定めるとともに、すべての職員に情報セキュリティポリシーの内容を周知徹底させる。

（2）物理的セキュリティ対策

電子カルテサーバー室等について不正な立入り等から保護するため、入退室や危機管理上の物理的な対策を講ずる。（入室鍵をコードキーもしくは入室鍵を経営企画室で保管し入室記録を残す。）

（3）技術的セキュリティ対策

情報資産を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、コンピュータウイルス対策等を実施する。

（4）運用におけるセキュリティ対策

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、ネットワークの監視等の運用面における必要な措置を講ずる。また、障害が発生した際の迅速な対応を可能とするため、障害時の対応を講ずる。

10 情報セキュリティ対策基準の策定

本院の情報資産について、上記 9 の情報セキュリティ対策を講ずるに当っては、職員が遵守すべき事項、判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策基準を策定するものとする。

11 情報セキュリティ実施手順の策定

情報セキュリティ対策を確実に実施していくためには、情報資産及び情報システムの具体的な運用管理規程を定めておく必要があることから、「亀岡市立病院情報システム運用管理規程」（別冊）を策定することとする。

12 評価・見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準等の見直しを実施す

るものとする。

第2章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、本院の情報資産に関する情報セキュリティ対策の基準である。

1　管理体制

情報セキュリティの管理については、以下の体制とする。

（1）最高情報統括責任者（CIO）

・亀岡市立病院における全てのネットワーク、情報処理システム、情報資産及び情報セキュリティに関する最終決定権及び責任を有する最高情報統括責任者（CIO）を置き、病院長をもってこれに充てる。

（2）ネットワーク統括管理者兼医療情報システム安全管理責任者

・亀岡市立病院における全てのネットワーク及び情報処理システムを統括するためネットワーク統括管理者兼医療情報システム安全管理責任者を置き、副院長をもってこれに充てる。

・ネットワーク統括管理者兼医療情報システム安全管理責任者は、最高情報統括責任者を補佐しなければならない。

・ネットワーク統括責任者兼医療情報システム安全管理責任者は、次に掲げる事務を統括して管理しなければならない。

・電子計算機（電子カルテ）、電子カルテサーバー室等の管理の適正化に関すること。

・データ及びドキュメントの保護及び管理に関すること。

・端末機等の適正な管理及び効率的な運用に関すること。

・情報システムを適正に管理及び運用するための連絡体制の構築に関すること。

・情報セキュリティに関する職員に対する教育、訓練、助言及び指示に関すること。

（3）ネットワーク管理者

・ネットワーク及び情報処理システムの適切な管理運営を行うためネットワーク管理者を置き、経営企画室長をもって充てる。

・ネットワーク管理者は、ネットワーク統括管理者を補佐しなければならない。

・ネットワーク管理者は、所管するネットワーク及び情報処理システムにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

・ネットワーク管理者は、ネットワーク及び情報処理システムの適正かつ効率的な運用を図るため、ネットワーク接続基準を定めるものとする。

・ネットワーク管理者は、所管するネットワーク及び情報処理システムに係る情報セキュリティ実施手順の作成、維持及び管理を行うとともに、定められている事項について職員に実施及び遵守させなければならない。

（4）システム管理者

・情報処理システムの適切な管理運営を行うため、システム管理者を置き、経営企画室長をもって充てる。
・システム管理者は、担当する情報処理システム設定の変更、運用、更新等を行う権限及び責任を有する。
・システム管理者は、担当する情報処理システムにおける情報セキュリティに関する権限及び責任を有する。
・システム管理者は、担当する情報処理システムに係る情報セキュリティ実施手順の作成、維持及び管理を行うとともに、定められている事項について職員に実施及び遵守させなければならない。

(5)運用責任者

・情報処理システムの適切な管理運営を行うため、運用責任者を置き、情報処理システムに係る業務を担当する室・課・科・所等の長を充てる。
・運用責任者は、担当する情報処理システム設定の変更、運用、更新等を行う権限及び責任を有する。
・運用責任者は、担当する情報処理システムにおける情報セキュリティに関する責任を有する。
・運用責任者は、担当する情報処理システムに係る維持及び管理(マスタ修正など)を行うとともに、定められている事項について職員に実施及び遵守させなければならない。

(6)セキュリティ統括責任者

・亀岡市立病院における全ての情報資産のセキュリティ対策を総合的に実施するため、セキュリティ統括責任者を置き、診療部長、診療技術部長、看護部長、管理部長、経営企画室長、患者支援センター長、訪問看護ステーション所長をもって充てる。
・セキュリティ統括責任者は、所掌に属する部・室・課・科・所等における情報セキュリティに関する統括的な権限及び責任を有する。

(7)電子カルテシステム運営管理委員会

・電子カルテシステムを中心とした情報システムの安定運用を図るとともに、「サイバーセキュリティインシデントの予防、早期検知、対応および復旧を迅速に実施するため、本院の CSIRT(Computer Security Incident Response Team)としての機能を担う組織として電子カルテシステム運営管理委員会(以下「委員会」という。)を設置する。
・委員会は、電子カルテシステムの運営管理及び情報セキュリティ対策に関する重要な事項を審議する。
・委員会の委員は、次の者をもって充てる。

委員長 兼 最高情報統括責任者(CIO:病院長)
副委員長 兼 ネットワーク統括管理者兼医療情報システム安全管理責任者(副院長)
セキュリティ統括責任者(管理部長)
セキュリティ統括責任者(診療部長)
セキュリティ統括責任者(診療技術部長)
セキュリティ統括責任者(看護部長)
セキュリティ統括責任者兼ネットワーク及びシステム管理者(経営企画室長)

・委員会の庶務は、経営企画室が行う。

2 情報の分類と管理

（1）情報の分類

対象となる全ての情報は、次の重要性分類に従って分類する。

ア 重要性分類Ⅰ

・個人情報の保護に関する法律に規定する個人情報

・法令又は条例（以下「法令等」という。）の定めにより守秘義務を課せられている情報（上記個人情報を除く。）

・法人その他の団体に関する情報で漏えいすることにより当該団体の利害を害するおそれのあるもの

・漏えいした場合、行政に対する信頼を著しく害するおそれのある情報

・滅失し、又はき損した場合、その復元が著しく困難となり、病院診療の円滑な執行を妨げるおそれのある情報

・ネットワーク及び情報処理システムに係るパスワード及び設定情報

イ 重要性分類Ⅱ

・脅威にさらされた場合に実害を受ける危険性は低いが、病院診療の執行において重要性は高いと評価される情報（公開されると病院の円滑な診療に著しく障害を生ずるおそれのある情報等）

ウ 重要性分類Ⅲ

・上記ア、イ以外の情報

（2）情報の管理方法

ア 情報の管理及び取扱

・情報の重要性分類に従い、パスワード等によるアクセス制限及び暗号等による通信内容の秘匿を行わなければならない。

・重要性分類Ⅰの情報の不用意な複製や、送付、送信は行ってはならない。

・職員は、業務上必要な場合には、セキュリティ統括責任者に許可を得たうえで情報の複製、送付及び送信を行わなければならない。

イ 記録媒体の管理

・重要性分類Ⅰ及びⅡの情報を記録した取り外し可能な記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない。また、保管状況等を記録しなければならない。

・重要性分類Ⅰ及びⅡの情報を記録した記録媒体を外部に持出しする場合は、職員又は守秘義務を明記した契約等を締結した外部業者に行わせるとともに、記録媒体の物理的な保護措置を講じなければならない。

ウ 記録媒体の処分

・記録媒体が摩耗等により不要となった場合は、当該記録媒体に記録されている重要性分類Ⅰ及びⅡの情報をいかなる方法によっても復元できないよう消去等を行ったうえで廃棄しなければならない。

・重要性分類Ⅰ及びⅡの情報を記録した記録媒体の廃棄は、セキュリティ統括責任者の許可を得た上

で行わなければならない。また、廃棄を行った日時、担当者及び処理内容を記録しなければならない。

3 人的セキュリティ

(1)職員

・職員は、ネットワーク管理者及びシステム管理者の指示等に従い、情報処理システムの開発、設定の変更、運用、更新等の作業を行わなければならない。

・職員は、情報セキュリティポリシー及び亀岡市立病院情報システム運用管理規程に定められている事項を遵守しなければならない。

・職員は、情報セキュリティ実施手順について不明な点、遵守することが困難な点がある場合には、速やかに運用責任者及びセキュリティ統括責任者に相談し、指示を仰がなければならない。

・職員は、セキュリティ統括責任者の許可を得ずに、情報処理システムの機器、記録媒体等を担当部署外に持ち出してはならない。

・職員は、異動等により業務を離れる場合には、知り得た情報を他に漏らしてはならない。

(2)教育・訓練

・最高情報統括責任者は、職員に対し情報セキュリティポリシーについて啓発に努めるとともに、職員を対象とした情報セキュリティポリシーに関する研修を設けるよう努める。

・ネットワーク統括管理者兼医療情報システム安全管理責任者は、上記の研修等について最高情報統括責任者を補佐するように努める。

・ネットワーク管理者は、ネットワークを管理運営していく上で、必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けるよう努める。

・システム管理者は、情報処理システムを管理運営していく上で、必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けるよう努める。

・運用責任者及びセキュリティ統括責任者は、情報セキュリティ対策を実施する上で必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けるよう努める。

・ネットワーク管理者及びシステム管理者は、ネットワーク及び情報処理システムの運用に支障を来たさない範囲において、緊急時対応を想定した訓練等を職員に行わせるよう努める。

・ネットワーク又は情報処理システムの開発・保守及び運用に携わる職員は、担当者として必要な技術力を習得及び維持するための研修を受けるよう努める。

・職員は、情報セキュリティポリシーに関する研修を受講し、情報セキュリティポリシー及び「亀岡市立病院情報システム運用管理規程」を理解し、情報セキュリティ上の問題が生じないように努める。

(3)外部委託に関する管理

・情報処理システムの開発、保守、運用管理、委託検査等を外部事業者に委託する場合は、情報セキュリティポリシーのうち外部委託事業者が守るべき内容の遵守及びその守秘義務を明記した契約を締結し、その遵守を管理しなければならない。

(4)パスワード等の管理

・職員は、自己の保有するパスワードについて、不用意に漏らしたりメモを作ったりしないようにするなど、パスワードの秘密保持に努めなければならない。

(5)接続時間の制限

・職員は、情報処理システムへの接続について、必要最小限の接続時間で行うように努めるものとする。

(6)インターネットの利用制限

・職員は、インターネットを利用する場合、次に掲げる行為をしてはならない。

① 公的良俗に反する行為
② 事実に反する情報を提供する行為
③ 営利を目的とした行為
④ 他人を詐称する行為
⑤ 他人の財産又はプライバシーを侵害する行為
⑥ 他人の著作権、その他の権利を侵害する行為
⑦ 他人を誹謗中傷する行為
⑧ ネットワークの正常な運用に支障を及ぼす行為
⑨ システムの不正利用又はそれを助ける行為
⑩ 権限なくプログラムやデータ等の改変又は破壊をする行為
⑪ 政治活動又は宗教活動を目的とする行為
⑫ インターネットの円滑な運用を妨げる行為
⑬ インターネット上の各種有料サイトを利用する行為
⑭ 法令等に違反する行為又は違反のおそれがある行為
⑮ その他社会慣行に反する行為

4 物理的セキュリティ

(1)入退室の管理

・セキュリティ統括責任者は、重要性分類Ⅰ及びⅡの情報の記録されている媒体保管場所及びそれを取り扱う情報機器の設置場所への入退室の管理について必要な措置を講じなければならない。

(2)職員の情報処理システムの機器管理

・職員は担当部署に職員が不在となる場合には、情報漏洩を防ぐ措置を講じなければならない。

(3)機器等の搬入・搬出

・電子カルテサーバー室等へ機器を搬入、搬出する場合は、あらかじめ当該機器等の既存情報処理システムに対する安全性について、職員による確認を行わなければならない。

・機器等の搬入・搬出には、職員が立ち会う等の必要な措置を講じなければならない。

(4)電源

・停電、電圧異常等によりデータ等が破壊され、業務処理に支障を来たすおそれのある情報処理システム等の機器の電源は、当該機器を適切に停止するまでの間、必要な電力を供給する容量の予備電源を備え付ける等の措置を講じなければならない。(無停電装置等の設置)

(5)配線

・配線は、傍受、損傷等を受けることがないよう可能な限り必要な措置を施さなければならない。

・主要な個所の配線は、損傷等についての定期的な点検を行わなければならない。

5 技術的セキュリティ

(1)ネットワーク及び情報処理システムの管理

ア ネットワーク及び情報処理システムの管理記録と作成と管理

・ネットワーク管理者及びシステム管理者は、所管するネットワーク及び情報処理システムにおいて行ったシステムの変更作業を記録し(情報システム様式2)、適切に管理しなければならない。

イ ネットワーク及び情報処理システムの仕様書の管理

・ネットワーク管理者及びシステム管理者は、所管するネットワーク及び情報処理システムの仕様書を最新の状態にしなければならない。また、仕様書変更等の処理を行った場合は、その記録を保管しなければならない。

・ネットワーク管理者及びシステム管理者は、仕様書を業務上必要とする者のみが閲覧できる場所に保管しなければならない。

ウ アクセス記録の取得

・ネットワーク管理者は、可能な範囲でアクセス記録を分析しなければならない。

エ 障害記録の作成

・ネットワーク管理者及びシステム管理者は、可能な範囲で障害記録を作成し、一定期間保存しなければならない。

オ バックアップの取得

・ネットワーク管理者及びシステム管理者は、情報の重要度に応じて定期的にバックアップを取り、施錠等のできる安全な場所へ保管しなければならない。

カ ソフトウェアの導入に関する注意

・職員は、新たにソフトウェアを導入する場合は、最高情報統括責任者又はネットワーク統括管理者兼医療情報システム安全管理責任者の許可(情報システム様式2)を得なければならない。

・職員は、正規のライセンスのないソフトウェアを導入してはならない。

・職員は、業務上不必要なソフトウェア、出所不明なソフトウェア等で安全性が確認されていないソフトウェアを導入してはならない。

・職員は、導入されているソフトウェアを適切に運用管理しなければならない。

キ 電子メール(以下「メール」という。)の送受信等

・職員は、メールの送受信に当たっては、ネットワーク管理者が指定したメールソフトウェアを用いなければならない。(電子カルテシステム内メール配信機能、グループウエア内ローカルメール機能のみを利用可能としその他は認めない。)

・職員は、メールの自動転送機能を用いて、業務上不必要な者へ職場のメールを転送してはならない。

・職員は、不必要となった送受信済みメールを削除しなければならない。

ク 暗号化

・学会や関連病院、医院等へ個人情報の含まれる情報を院外へ持ち出す場合、暗号化などの処理を行い、個人情報の漏洩を防がなければならない。

ケ 職員以外の者が利用できる情報システム

・システム管理者は、職員以外の者が利用できる情報処理システムについては、情報処理セキュリティ

対策について特に強固な対策をとらなければならない。

コ　情報処理システムの入出力データ

・システム管理者は、情報処理システムに入力されるデータの適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

・システム管理者は、情報処理システムから出力されるデータの処理が正しく行われていることを確認しなければならない。

サ　業務目的以外の使用の禁止

・職員は、業務目的以外での情報処理システムへのアクセス、メールの使用及びインターネット接続を行ってはならない。

(2)情報処理システムアクセス制御

ア　利用者登録

・ネットワーク管理者及びシステム管理者は、情報処理システムの利用者の登録、変更、抹消等について、情報処理システム毎に定められた方法に従って行わなければならない。

・利用者登録、変更等は、ネットワーク管理者及びシステム管理者に対する申請（情報システム様式1）により行わなければならない。

イ　ネットワークへのアクセス制御

・ネットワーク管理者は、不必要なネットワークサービスにアクセスできないよう必要な措置を講じなければならない。

ウ　外部ネットワークとの接続

・外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成及び情報セキュリティレベルを詳細に検討し、本院の情報資産に影響が生じないことを明確に確認した上で、ネットワーク管理者の許可に基づき接続しなければならない。

・ネットワーク管理者は、外部ネットワークとの接続を行うことで内部ネットワークの安全が脅かされることの無いようにセキュリティ対策に努めなければならない。

・接続した外部ネットワークの情報セキュリティに問題が認められた場合には、ネットワーク管理者は速やかに当該外部ネットワークを物理的に遮断しなければならない。

・内部ネットワークの情報セキュリティに問題が認められた場合には、ネットワーク管理者は速やかに当該ネットワークを、外部ネットワークから遮断しなければならない。

エ　パスワードの管理

・ネットワーク管理者は、情報処理システムで使用する ID 及びパスワードを厳重に管理しなければならない。

・ネットワーク管理者は、ネットワーク及びネットワーク上で利用する各種サービスの ID、パスワードを厳重に管理しなければならない。

(3)情報処理システムの開発・導入・保守

ア　ネットワーク及び情報処理システムの開発・導入

・ネットワーク管理者及びシステム管理者は、ネットワーク及び情報処理システムを新規に開発、導入する場合及び大規模な変更等を行う場合は、情報セキュリティ上の問題が無いかどうか確認しなければならない。

・ネットワーク管理者及びシステム管理者は、ネットワーク及び情報処理システムを新規に開発・導入する場合及び大規模な変更等を行う場合は、ネットワーク構成図、情報処理システム仕様書等を整備しなければならない。
・システム管理者は、開発したソフトウェアを情報処理システムに取り入れる場合は、既に稼働している情報処理システムに接続する前に十分な試験を行わなければならない。

イ　ネットワーク及び情報処理システムの変更管理

・ネットワーク管理者及びシステム管理者は、重要なネットワーク及び情報処理システムを追加、変更、廃棄した場合は、その際の設定、構成等の履歴を記録、保存し(「システム(登録・変更)申請願書(情報システム様式2)」)、必要な場合には復旧できるようにしなければならない。

ウ　ソフトウェアの保守及び更新

・ネットワーク管理者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切な保守が行われるようにし、その不具合については、速やかに修正等の対応を行わなければならない。
・職員は、ネットワーク管理者の指示に従いソフトウェアの修正パッチ等の適用を行わなければならない。

エ　機器の修理及び廃棄

・記録媒体の含まれる機器を、外部の業者に修理させる場合又は賃借期間終了等により廃棄する場合は、可能な範囲でバックアップを取り、記録媒体内のすべての情報を消去又は他者が復元出来ない策を講じなければならない。
・故障等で外部の業者に修理させる際、情報を消去することが難しい場合は、修理を委託する業者と守秘義務を明記した契約を締結しなければならない。

オ　機器構成の変更

・職員は、情報処理システムの機器について改造又は機器の増設、交換を行ってはならない。
・職員は、情報処理システムの機器について業務を遂行するため機器の増設、交換を行う必要がある場合には、ネットワーク統括責任者の許可を得なければならない。
・職員は、モデム等の機器を増設して、他のネットワークへ接続を行う場合及び他のネットワークからアクセスを可能とする仕組みを構築する場合には、ネットワーク管理者及びシステム管理者の許可を得なければならない。ネットワーク管理者及びシステム管理者は、許可に当ってネットワーク及び情報処理システムにセキュリティ上の問題を生じさせてはならない。

(4)コンピュータウイルス対策

ア　ネットワーク管理者及びシステム管理者は、次の事項を実施しなければならない。

・情報処理システムのサーバ及び必要な機器にウイルス対策ソフトウェアを導入すること。
・ウイルスチェック用のパターンファイルは常に最新のものに保つこと。
・定期的に新種のウイルスに関する情報収集や情報処理システム内部の感染状況等について情報収集すること。
・コンピュータウイルス情報について、職員に対する注意喚起を行うこと。
・コンピュータウイルスについて、職員に対して必要な啓発活動を行うこと。

イ　職員は、次の事項を遵守しなければならない。(申請による許可制とする)

・外部からのデータ又はソフトウェアを取り入れる場合または外部に持ち出す場合には、必ずウイルス

チェックを行うこと。

・ウイルスチェックの実行を途中で止めないこと。

・ネットワーク管理者が提供するコンピュータウイルス情報を常に確認すること。

・ウイルスチェック用のパターンファイルは、常に最新のものに保つこと。

(5)不正アクセス対策

・ネットワーク管理者及びシステム管理者は、セキュリティポリシー等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録、保存しなければならない。

・ネットワーク管理者及びシステム管理者は、ネットワーク及び情報処理システムに不正な進入や利用があった場合に探知できるよう、適切な対策に努めなければならない。

・システム管理者は、情報処理システムに攻撃を受けていることが明らかな場合には、システムの停止を含め必要な措置を講じなければならない。

・職員により本院ネットワーク、外部ネットワーク及び情報処理システムに対して不正なアクセスがあった場合、ネットワーク管理者及びシステム管理者は、当該職員が所属する運用責任者に通知し、適切な処置を求めなければならない。

・職員は、外部ネットワークにより不正なアクセスがあった場合には、ネットワーク管理者及びシステム管理者に報告し、適切な措置を講じなければならない。

(6)セキュリティ情報の収集

・ネットワーク統括責任者兼医療情報システム安全管理責任者は、情報セキュリティに関する情報を収集し、セキュリティ対策上必要な措置を講じなければならない。

・最高情報統括責任者は、情報セキュリティに関する情報について定期的に取りまとめ、関係部署に通知しなければならない。

6 運用

(1)ネットワーク及び情報処理システムの監視

・ネットワーク管理者及びシステム管理者は、ネットワーク及び情報処理システムの運用にあたっては、常にネットワーク及び情報処理システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

(2)情報セキュリティポリシーの遵守状況の確認

・セキュリティ統括責任者及び運用責任者は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じないかについて確認を行わなければならない。

(3)セキュリティ障害時の対応

・セキュリティ障害が発生した場合には、ネットワーク管理者及びシステム管理者は、速やかに対応するとともに、再発防止の措置を講じなければならない。

ア 障害拡大の防止措置

・ネットワーク管理者及びシステム管理者は、故意の不正アクセス又は不正操作によりネットワーク及び情報処理システムに障害を及ぼすことが明らかな場合には、ネットワーク及び情報処理システムの停止を含む必要な措置を講じなければならない。

・ネットワーク管理者及びシステム管理者は、ネットワーク及び情報処理システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。

イ　障害の調査

・ネットワーク管理者及びシステム管理者は、セキュリティ障害が発生した場合、次の項目について調査をしなければならない。

① 障害の内容

② 障害が発生した原因

③ 確認した被害、影響範囲

・調査した内容は速やかにネットワーク統括責任者兼医療情報システム安全管理責任者へ報告しなければならない。ただし、障害の程度が軽微なものについては、報告を要しないものとする。

ウ　障害への対応

・ネットワーク統括管理者兼医療情報システム安全管理責任者は、速やかにセキュリティ障害を復旧し、その措置について最高情報統括責任者に報告しなければならない。

・障害が外部に重大な影響を及ぼすおそれがある場合には、速やかに最高情報統括責任者に報告のうえ必要な指示を仰がなければならない。

エ　再発防止の措置

・ネットワーク統括管理者医療情報システム安全管理責任者は、必要な再発防止の措置を講じるとともに、その結果を最高情報統括責任者に報告しなければならない。

・セキュリティ統括責任者及び運用責任者はセキュリティ障害の原因が、人的セキュリティによる場合は、職員に対して再発を防止するため必要な措置を講じなければならない。

7　法令等遵守

職員は、使用する情報資産について、次の法令等を遵守し、マナーと倫理をもって情報システムを利用しなければならない。

・不正アクセス行為の禁止等に関する法律（平成 11 年　法律第 128 号）

・著作権法（昭和 45 年　法律第 48 号）

・亀岡市個人情報保護条例（平成 12 年　亀岡市条例第 37 号）

・個人情報の保護に関する法律（平成 15 年　法律第 57 号）

・医療従事者の守秘義務

医師、歯科医師、薬剤師：刑法第 134 条の 1 項

保健師、助産師、看護師、准看護師：保健師助産師看護法第 42 条の 2

診療放射線技師：診療放射線技師法第 29 条

臨床検査技師：臨床検査技師に関する法律第 19 条

理学療法士、作業療法士：理学療法士及び作業療法士法第 16 条

視能訓練士：視能訓練士法第 19 条

臨床工学士：臨床工学技士法第 40 条

救急救命士：救急救命士法第 47 条

言語聴覚士:言語聴覚士法第 44 条
精神保健福祉士:精神保健福祉士法第 40 条
歯科衛生士:歯科衛生士法第 13 条の 6
歯科技工士:歯科技工士法第 20 条の 2

8 違反に対する措置

・最高情報統括者は、情報セキュリティポリシーに違反した職員及び当該職員の所属する課・科等の長に対し、情報セキュリティを確保するために必要な措置を講ずるものとする。
・最高情報統括責任者は、必要と認めるときは、違反した職員の氏名、所属名及び違反した内容を病院事業管理者に報告するものとする。
・情報セキュリティポリシーに違反した職員については、その重大性、発生した事案の状況等に応じて、亀岡市個人情報保護条例に則り処分等の対象とするとともに、その結果について責任を負わなければならない。

9 評価・見直し等

(1)点検

セキュリティ統括責任者及び運用責任者は、当該部署の情報セキュリティが確保されていることを確認するため、自主点検を行い、必要に応じて改善措置を講じなければならない。

(2)情報セキュリティポリシーの更新

最高情報統括責任者は、評価及び見直しが必要となる事象が発生した場合には、委員会に諮り必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。

≪本規定で示される責任者一覧≫

最高情報統括責任者(CIO)・・・・・・病院長
ネットワーク統括責任者兼医療情報システム安全管理責任者・・・・・・副院長
ネットワーク管理者・・・・・・経営企画室長
システム管理者・・・・・・経営企画室長
運用責任者・・・・・・各課、科等の長
セキュリティ統括責任者・・・・・・診療部長、診療技術部長、看護部長、管理部長、経営企画室長、患者支援センター長、訪問看護ステーション所長

附 則

平成 25 年 4 月 1 日:初版
平成 25 年 7 月 1 日:改正
平成 29 年 4 月 1 日:改正
令和 5 年 4 月 1 日:改正
令和 8 年 4 月 1 日:改正