１．セキュリティ方針書

１　方針

山口大学医学部附属病院情報システム（ 以下「情報システム」という。）が取扱う情報は不当な暴露、不当な改ざん、不当な処理妨害がなされないように管理および保護されなければならない。

情報システムで処理、保管されているいかなるデータもこの情報システムに関係のない者には公表しないことを原則とする。

２　目的

本セキュリティ方針書は、上記１の方針に基づき、情報の管理や保護のための技術的な対策及びシステムの利用者や管理者への教育の実施等を定めた「セキュリティ方針」を定めることを目的とする。

３　修正

医療情報部運営委員会は､本セキュリティ方針に定められた事項について修正の必要が生じた場合には、速やかに見直しを行う。

４　適用範囲

本セキュリティ方針は、情報システムを構成する全ての部分（コンピュータシステムに関連する装置、システムの運用に携わる人、システムの利用者等をいう。以下同じ。）に適用する。

特に、個人情報（ 診療情報等を含む。）を扱う全ての部分に対しては、運用時の必須要件として本セキュリティ方針を適用する。

５　配布

本セキュリティ方針書は、情報システムに関係する全ての者に配布する。

６　医療情報部運営委員会

１）　セキュリティ方針を実施するため、その実施方法について、その評価や問題点などを検討し、情報セキュリティの保護、管理を行うとともに、病院内で実施されるセキュリティ対策に矛盾が生じないよう調整を行う。

２）　業務内容

⑴　病院のデータ保護に関するセキュリティ方針の適切な運用とそれに関する責任の検討

⑵　病院の情報財産に対する脅威の監視と予防対策の検討

⑶　セキュリティ対策を実践するための総括管理責任者への提言

３）　業務の実際は、委員会の責任のもとに医療情報部が行う。

７　リスク管理

リスク管理は、セキュリティ対策と保護対象となる情報の価値とのバランスを維持するために、下記の点に留意して方針が決定される。

１）　情報システムのセキュリティ上の想定脅威（発生が懸念される不正暴露、改ざん、処理妨害等）

２）　想定脅威に対して、その発生が及ぼす損失とそのセキュリティ対策費用及び利便性を考慮した有効な対策とその速やかな実施

８　プライバシー情報

独立行政法人の保有するプライバシー情報は「 独立行政法人等の保有する個人情報の保護に関する法律 」（２００５年４月施行）によって法的に保護が義務づけられている。個人情報という他人の財産を管理し、しかも、一度暴露等の事故が発生すると、取り戻すことができないという情報固有の特性を考え、委託民間企業も含めた情報システムに関与するすべての利用者は、その保護に最優先で取り組まなければならない。

9　セキュリティ管理

総括管理責任者は、情報システムのセキュリティ確保のために各部門から業務管理責任者を指名する。

10　責任の分散

セキュリティ管理の責任を分散し、特定の個人に権限と責任が集中して、矛盾を引き起こさないように配慮する。

11　違反者に対する処置

本セキュリティ方針を含む組織、機関の定めた情報セキュリティに違反した者には、職員にあっては「国立大学法人山口大学職員の懲戒等に関する規則」に基づき、学生にあっては「国立大学法人山口大学学則」に基づき、罰則を科されるものとする。

12　診療にかかわる情報のアクセス

1）　診療にかかわる情報にアクセスできる者は、医師及び関連する医療スタッフとする。

2）　診療上必要であると医師が判断した情報を当該患者に開示する場合は、担当医師の責任において行うこととする。ただし、診療情報開示の要請に基づくカルテの開示を行う場合は、別に定める「診療情報開示規則」によるものとする。

3）　臨床教育、症例研究、カンファレンス等の目的で診療にかかわる情報にアクセスする場合は、教育を担当する医師及び医療スタッフの責任において行うこととする。

4）　教育、研究、病院運営、その他の各種業務を遂行する目的で二次利用可能な形式に変換した診療にかかわる情報（二次診療情報）は、集学系情報システムから集学系に設置された部門情報システムに伝送して利用する。

⑴　二次診療情報は診療にかかわる情報を連結可能匿名化した情報とする。

⑵　二次診療情報を利用する場合、集学系情報システムにアクセスして部門情報システムに取得する。

⑶　二次診療情報の利用は業務管理責任者の責任において行うこととする。

13　情報システムへのアクセス

1）　通常の診療業務時の情報システムへのアクセスは、外来・入院を問わず、診察を希望する旨の根拠となる情報が患者又は患者の代理人の意志により表明され、かつ、患者の受診手続きが済まされていなければならない。

2）　緊急時の情報システムへのアクセス

⑴　患者氏名が不祥の場合は、新たに診察券（患者ＩＤ）を作成する。

⑵　この診察券は、新規のＩＤで作成されるため、患者の重複登録にならないよう作成にあたっては、万全の配慮をしなければならない。

⑶　患者名が確認できた場合で、従来ＩＤが存在していたときは、そのＩＤと新規ＩＤの融合方法を関係部門と調整しなければならない。

14　物理的なセキュリティ管理

自然災害や装置の故障、盗難、破壊等から情報システムを保護するために以下の対策を実施する。

1）　コンピュータ装置本体、ネットワーク管理装置等、情報システムの処理に重大な影響を与える装置は盗難や破壊、関係者外の利用から保護するための物理的な対策を実施する。

2）　全装置の一覧表を維持管理し、不正な持ち出し等が発生しないようにする。

3）　システム診断用のハードおよびソフトの使用は利用目的を限定し、その使用を管理する。

4）　回線は、全ての部分で物理的に保護されることとし、定期的に検査する。

5）　電源設備の故障による停電等の場合は、停電電源供給装置（ＵＰＳ）等の別系統電源供給によって電力の供給に努める。

6）　重大な故障又は災害時の業務継続計画（「ダウン(システム障害時)対応マニュアル」）は、別途定める。

15　情報セキュリティ管理

1）　利用者の識別と認証

⑴　情報システムのアクセスの範囲は業務要件に基づいて管理される。利用者のアクセス権限は業務管理責任者の申請に基づき総括管理責任者が決定する。

⑵　利用者は、利用者ＩＤによって識別し、本人の確認はパスワードによって行う。

2）　ファイル管理

⑴　ファイル（データベースを含む。）やプログラムを管理しているシステム（以下「管理システム」という。）あるいは、業務上特別な条件下で必要なツール、さらに、後利用データベースにおいて患者のプライバシーに影響を与えるデータなどは、特別に権限を付与された利用者のみ利用できる。

⑵　システム運用関連及びファイル管理関連のプログラムやデータの変更は、特別な権限を付与された者のみが事前に変更手続きを行った後に、行うことができる。

⑶　管理システムは、運用中は常時、システム管理者が管理できる状態にしておく。

3）　ネットワークセキュリティ管理

⑴　ネットワークの利用及びネットワークの構成の登録・変更は、業務管理責任者からの申請に基づきシステム管理者が決定する。

⑵　内部ネットワーク（業務で使用するサーバ、無線ＬＡＮ及び端末が接続されたネットワーク）から部門情報システム等を介して外部と通信する場合（リモートメンテナンスなど）には、院外のリモートメンテナンス端末の管理方法も把握して許可を与えなければならない。

⑶　院内の外部ネットワークは、内部ネットワークと接続しないものとする。

⑷　特に許可された者以外は、院外回線を通じて内部ネットワークを利用できない。

⑸　部門情報システムのサブシステムの保守管理のために直接院外の回線を結びつけてダイアルアップなどのネットワークを構築する場合は、必ずその機能に関する仕様書を医療情報部に提出し、定期的にその安全性の維持について報告しなければならない。

⑹　プライバシーに関係する重要なデータをネットワーク上で使用する場合は、ネットワーク環境がセキュリティの確保上完全ではないことを考慮した上で使用しなければならない。

⑺　二次診療情報を利用するために集学系情報システムに接続する部門情報システムを設置する場合、業務管理責任者からの申請に基づきシステム管理者が許可を与えるものとする。

4）　分散管理

⑴　部門サーバ間のセキュリティレベルを統一する。

⑵　部門サーバ間で一貫したセキュリティ属性の解釈が行えるように管理する。

5）　電子メール管理

プライバシーに関係するような重要データを、電子メールで送信する場合は、その送信方法について考慮されなければならない。

6）　監査

⑴　監査責任者は、情報セキュリティの管理のため、監査情報を収集し、それらを監査し、その結果を総括管理責任者に報告する。

⑵　監査責任者は、常に第三者的立場を堅持して公正にシステムの不正、改ざんあるいは混同の存在について指摘しなければならない。

⑶　監査情報には、利用者（利用者ＩＤ）、利用場所、日時、アクセスした資源名、利用事象のタイプ、アクセスの可否結果を記録する。

⑷　監査情報が収められているファイルは、保護されなければならない。

⑸　監査責任者は、監査情報を少なくとも年２回、チェックする。

⑹　違反に関する監査記録は、少なくとも６０日間は保存しておく。

⑺　監査ツールの使用は、特別な権限を付与された医療情報部の構成員に限る。

7）　データ保全とコンピュータウィルス

⑴　利用者が持ち込むデータや、システム運用に直接関連するプログラム等重要なプログラムを扱う場合には、利用前にウィルスチェックを実施する。

⑵　ウィルスワクチンプログラムは、サーバでの一括管理とする。

⑶　利用者は、使用中にウィルス感染の疑いが生じた場合は、医療情報部に連絡する。

⑷ 医療情報部は、障害の状況を分析しウィルスが確認された場合は、その旨を全利用者に通知して注意を喚起し、同時にシステム管理者に報告しなければならない。
⑸ 部門情報システムで使用する記録媒体の管理は、業務管理責任者が管理する。

8） 法的に使用される電子保存された情報の管理

⑴ 法的に使用される電子保存された情報は、その真正性を確保するように講じられていること。
⑵ 法的に使用される電子保存された情報の真正性は、操作を行う者の利用者ＩＤとパスワードで認識させて、操作を行う者が入力した確定情報は、確定入力を動機付けできる画面で構成し、その修正は原本を保存しながら修正データが見読できるように設計されていること。
⑶ 法的に使用される電子保存された情報は、法的に求められる期間中保存でき、機器等の新調によるデータの互換性は保持できること。
⑷ 法的に使用される電子保存された情報を、保存及び出力する機器は、法的に求められる期間内は、常に稼動できる状態にしておくこと。
⑸ 法的に使用される電子保存された情報の所在を明確にし、法的保存期間の情報の開示を求められた場合、速やかに開示できるようにすること。
⑹ 紙面での保存が法的に必要な情報は、その法的根拠が保たれる状態で保存すること。

16 運用管理

1） 運用管理

システムは、以下の条件に従って適切に管理されなければならない。

① システムが災害にあった場合の対処方法と復旧方法について手順を明確にし、必要に応じて医療情報部で見直しを実施すること。
② システムのバックアップを定期的に実施するとともに、バックアップ媒体は、安全な場所に保管されること。
③ 機密性の高いバックアップデータは、厳重に保管されること。
④ 可搬媒体（テープ、ディスク、カセット、及びプリントしたレポート等）に関する管理手順を明確にし、利用者に遵守させること。
⑤ システム資源の容量を定期的に確認し、容量不足が予想される場合には速やかに対処すること。

2） システム管理

⑴ 利用者の本人確認は、システムの利用を開始する時点で実施する。
⑵ 不正なシステム利用は、許可しない旨の通知を行う。

3） システムの運用を適切に管理するために、「管理者マニュアル」及び「利用者マニュアル」を定める。

4） 各部門別において、システム運用実施細則を定める。

17 スタッフセキュリティ

1） 外部委託管理

⑴ 情報システムを利用することのできる職員を雇用する委託企業は、職員に十分な利用者教育を行わなければならない。
⑵ 情報システムの利用者は、守秘義務と同時に、情報システムの構造を熟知して、院外からのアクセスに注意を払わなければならない。
⑶ 委託契約の締結に際しては、契約上に職員の情報セキュリティに関する項目を盛り込まなければならない。

2） 教育・訓練

⑴ 情報システムの利用者は、情報システムの利用を許可される前にセキュリティ方針及びセキュリティ対策、運用の教育を受けなければならない。
⑵ セキュリティに理解の乏しい利用者に対し、業務管理責任者はセキュリティ方針及びセキュリティ対策の研修を受けさせなければならない。
⑶ 教育内容には、以下の項目を盛り込まなければならない。

① 情報システムの利用者に対する教育

ア セキュリティ侵害や情報の漏洩が何によって起きるかを含めた、プライバシー、機密性、完全

性、可用性、情報公開及び情報セキュリティの概念
イ　プライバシー、機密性及びセキュリティに影響を与える情報技術
ウ　利用者のセキュリティ管理における個人の責任及び立場による責任範囲の違い
エ　診療情報の重要性と、その利用者および使用用途
オ　利用者情報の重要性
カ　情報セキュリティに対する想定脅威の種類
キ　データ保護の方式
ク　セキュリティ違反の重大さと罰則
ケ　セキュリティに対する定期的な評価と改良

② 管理者に対する教育

初めて管理者になった者に対する教育は、利用者に対する教育に加えて以下の項目を履修しなければならない。

ア　情報セキュリティ教育のプログラムを確立するための管理責任
イ　情報セキュリティ方針とその実践を実現、監視、評価するための戦略
ウ　全ての利用者に対する情報の取扱い方法・内容
エ　情報セキュリティに影響を与える新技術や、セキュリティ計画に影響を与える規制・規則について熟知する責任
オ　不適切な情報の漏洩によって発生する法律上の要件や罰則
カ　セキュリティ侵害時の一貫した対応と訓練

⑷ 情報システムを利用するすべてのスタッフは、教育・訓練を受けなければならない。

このセキュリティ方針書による運用は平成１７年４月１日より実施する。