県立医療大学情報セキュリティ実施手順

第１章 総則

（趣旨）

第１条 この要項は，茨城県情報セキュリティ基本方針を定める規程（平成 21 年 6 月 15 日茨城県訓令第２７号，以下「規程」という。）第７条の規定に基づき，茨城県立医療大学（以下「本学」という。）の情報システム（大学情報サブシステム，学務事務システム，医療情報システム及びＰＡＣＳ系システムを含む。以下「システム」という。）並びに学内において使用するコンピュータ及び情報機器（これに搭載されているソフトウェア等を含む。以下「端末」という。）並びにこれらシステムや端末内のすべての情報の情報セキュリティ実施手順を定めるものである。

（用語の定義）

第２条 この要項において，次の各号に掲げる用語の定義は，それぞれ当該各号に定めるところによる。

（１）情報資産 規程第 2 条第 1 項に規定する情報システム及び情報をいう。

（２）利用者 システムの利用を認められた者をいう。

（３）管理者権限ユーザ システムの設定変更等を行える権限を与えられた者をいう。

（４）パスワード 利用者及び本学の情報保護のため，利用者自身で管理する文字列をいう。

（５）情報セキュリティ管理者 茨城県情報セキュリティ対策基準（以下「対策基準」という。）第９条に規定する職員をいう。

（６）情報システム管理者 対策基準第１１条に規定する職員をいう。

（７）情報セキュリティ管理事務局 対策基準第８条に規定する機関をいう。

（８）情報セキュリティ担当者 対策基準第１０条に規定する職員をいう。

（９）情報システム担当者 対策基準第１２条に規定する職員をいう。

（10）最重要（Ⅰ）情報 対策基準第１６条の規定により最重要（Ⅰ）に分類される情報。

（11）重要（Ⅱ）情報 対策基準第１６条の規定により重要（Ⅱ）に分類される情報。

（情報セキュリティ対策の原則）

第 3 条 学長は情報資産のうち教育研究情報に関する情報セキュリティ対策を，付属病院長は情報資産のうち医療情報に関する情報セキュリティ対策を，事務局長はその他の情報資産に関する情報セキュリティ対策を所管するものとする。

（学内委員会等との関係）

第４条 情報セキュリティ管理者及び情報システム管理者は，情報セキュリティ対策を実施するにあたり学内委員会等の意見を参考にすることができる。

（情報セキュリティ管理者（副），情報システム管理者（副））

第５条 事務局長を情報セキュリティ管理者（副）および情報システム管理者（副）とする。

（情報セキュリティ担当者，情報システム担当者）
第６条 総務課長を情報セキュリティ担当者及び情報システム担当者とする。

（システムの対象範囲）
第７条 システムの対象範囲は，規程第２条第１項に定める県行政全般の情報資産のうち，情報システム管理者が所掌する別表第１に掲げる全てのサブシステムについての情報資産とする。

（アクセス権限）
第８条 利用者のシステムへのアクセス権限の設定は，別表第１に掲げるサブシステムの管理者が別に定めるシステム利用要項の規定に従い行うものとする。

第２章 物理的セキュリティ

（セキュリティ区域）
第９条 情報セキュリティ管理者が，対策基準第１６条第１項第１号で定めるセキュリティ区域を指定するにあたっては，「管理区域チェックリスト」（様式第１号）に従い審査を行った上で，セキュリティ区域を指定するものとする。
２ 情報システム管理者は，職員にセキュリティ区域に新たな機器を増設させる時は，既存情報システムに対する安全性について，次の各号に掲げる事項を確認しなければならない。
（１）発熱量等を調査し，部屋の温度等の上昇による問題が発生しないこと。
（２）電源容量を調査し，接続したことによる容量オーバーで既存情報システムがダウンしないこと。
（３）搬入の際には，既存情報システムの機器に接触して破損しないよう，物理的な保護を施すこと。
（４）搬入時に，危険物や不要なものを持ち込ませないよう，事前に確認を行うこと。
（５）搬入業者が不正な行為を行わないよう，職員が立会いを行うこと。

第３章 技術的セキュリティ

（情報システム仕様書の管理）
第１０条 情報システム担当者は，次の各号に掲げる事項が遵守され情報システム仕様書が適切に管理されるよう，必要な措置を講ずるものとする。
（１）情報システム仕様書及びネットワーク構成図（以下「仕様書等」という。）がその記録媒体の種類にかかわらず，施錠可能な場所に保管され，その鍵が適切に管理されること。
（２）業務上必要と認めた者に対してのみ仕様書等の閲覧が許可されること。
（３）仕様書等の一覧表及び閲覧承認者一覧表が作成され，随時更新されること。
（４）３か月に１回以上仕様書等の保管状況が点検されること。

（管理簿の作成）

第１１条 情報システム担当者は，次の各号に掲げる台帳が整備され，第１号及び第２号の台帳が重要(Ⅱ)情報として，第３号の台帳が最重要(Ⅰ)情報として管理されるよう，必要な措置を講ずるものとする。

（１） ハードウェア管理簿（様式第２号ア）・ハードウェア管理簿（ＵＳＢメモリ用）（様式第２号イ）

（２）ソフトウェア管理簿（様式第３号）

（３）管理者用パスワード管理簿（様式第４号）

（ユーザＩＤ登録）

第１２条 情報システム担当者は，ユーザ登録等が次の各号に掲げる手順等に従い適切に処理されるよう，必要な措置を講ずるものとする。

（１）処理票を作成し，利用者のユーザＩＤ登録，変更及び抹消を行うこと。

（２）処理票には，処理の種別，氏名，職名及び所属等が記載されること。

（３）ユーザＩＤ管理簿が作成され，重要(Ⅱ)情報として管理されること。

（４）ユーザＩＤ管理簿に，承認日，利用者の氏名，連絡先，利用可能なサブシステム名，ユーザＩＤ，使用目的及び有効期限等ユーザ管理を適切に行うための事項が記載されること。

（管理者権限）

第１３条 情報システム担当者は，次の各号に掲げる事項を遵守して管理者権限ユーザの管理が適切に行われるよう，必要な措置を講ずるものとする。

（１）管理者権限ユーザＩＤ管理簿が重要(Ⅱ)情報として管理されること。

（２）管理者権限ユーザＩＤ管理簿に， 承認日，管理者権限ユーザの氏名，連絡先，管理者として利用可能なサブシステム名，ユーザＩＤ，使用目的及び有効期限等管理者権限ユーザ管理を適切に行うための事項が記載されること。

（３）管理者権限ユーザの管理者権限の必要性が随時確認され，管理者権限が不要と判断した場合に，ただちに管理者としての登録を抹消されること。

（経路制御）

第１４条 ネットワークの経路制御の設定，閲覧及び変更は，情報システム担当者が行うものとする。

２ 茨城県の所管するネットワーク以外のネットワーク（インターネットを含む。）との通信は，全てファイアウォールを経由する設定としなければならない。

３ 情報システム担当者は，次の各号に掲げる事項を参考に，ネットワーク機器に適切なパスワードを設定しなければならない。

（１）デフォルトパスワードを使用しないこと。

（２）パスワードなしを許可しないこと。

（３）パスワードは８文字程度とし，半角英文字及び数字を組み合わせたものとすること。

（学外からのアクセス）

第１５条 情報システム担当者は，学外に公開しているサーバとそのサーバで許可しているサービスについての学外向けサービス一覧表を作成し，随時更新しなければならない。

２ 学外向けサービス一覧表には，次の各号に掲げる事項を記載するものとする。

（１）サーバ名
（２）サービス内容
（３）サービス目的
（４）サービス期間
（５）サービス時間
（６）利用者
（７）責任者
（８）使用プロトコル
（９）その他セキュリティ対策に関する特記事項

（ログイン手順）

第１６条 情報システム担当者は，利用者のログイン手順に関して，次の各号に掲げる設定が可能であればその設定が行われるよう，必要な措置を講ずるものとする。

（１）ログイン手順中に，ユーザ登録されていない者が不正にログインを行うための助けとなるメッセージ（ユーザＩＤが存在しない。パスワードが間違っている。等）を表示させない。
（２）許容されるログイン試行失敗回数を３回に制限する。
（３）ログインに失敗した試みをログに記録する。
（４）ログイン失敗から次のログインが可能になるまで１０秒以上の時間をおく。

（パスワードの管理方法）

第１７条 情報システム担当者は，次の各号に掲げる事項に留意したパスワードの管理が行われるよう，必要な措置を講ずるものとする。

（１）利用者にパスワードを発行する場合，推測され難いランダムなパスワードを発行すること。
（２）強制的にパスワードの変更を行わせることができるサブシステムについては，必要に応じて，パスワードの変更を強制的に行わせる設定とすること。
（３）必要に応じて，パスワード解析ツールを使用してパスワードの脆弱性の調査を行い，脆弱性のあるパスワードを使用している利用者にパスワードを変更させること。

（その他のアクセス制御）

第１８条 利用者が利用できる基本的なプロトコルは，mail(SMTP，POP3)，WWW(HTTP，HTTPS)，FTP とする。

２ 職員は，業務に必要なプロトコルの利用を希望する場合には，情報システム管理者に利用申請をしなければならない。
３ 職員は，利用申請をしたプロトコルを業務で使用する必要がなくなった時は，ただちに情報システム管理者に利用廃止申請をしなければならない。
４ 情報システム管理者は，業務に必要でないプロトコルがルータ及びファイアウォールを越えないように設定し，必要に応じて，随時その設定を更新しなければならない。

（アクセス記録の取得等）
第１９条 情報システム担当者は，ログファイルの参照及び更新に関して，ファイル及びディレクトリのアクセス権限を適切に設定しなければならない。
２ 情報システム担当者は，許可された処理だけが実行されていることを確認するため，別表第２に掲げるサーバのログを１日１回以上解析するよう努める。
３ 情報システム担当者がログを解析した結果において，次の各号に掲げる事象が確認された場合，当該事象の状況を情報セキュリティ管理者に報告しなければならない。
（１）連続したアクセスの失敗
（２）連続した認証の失敗
（３）大量のデータの送受信
（４）権限外の処理の試み
（５）データ処理票に基づかないユーザアカウントに関する変更（追加，削除，グループ変更等）
（６）データ処理票に基づかないアクセス権の変更

（システム管理における作業と記録）
第２０条 情報システム担当者は，作業計画書を作成した上でシステム管理作業を実施されるよう，必要な措置を講ずるものとする。
２ 作業計画書には，次の各号に掲げる事項を記載するものとする。
（１）作業開始予定日時及び終了予定日時
（２）作業者
（３）目的
（４）作業内容
（５）作業対象サブシステム名
（６）重要性分類
（７）サービス停止周知の必要性
（８）他のサブシステム等への影響検討結果

（利用者への周知）
第２１条 情報システム担当者は，利用者に対して余裕をもってサービス停止の周知がなされるよう，必要な措置を講ずるものとする。
２ 利用者には，次の各号に掲げる事項を周知するものとする。

（１）作業対象サブシステム名
（２）影響を受けるサービス名
（３）影響の範囲（サービス停止，処理遅延等）
（４）作業開始予定時間及び終了予定時間
（５）作業内容

（障害記録）

第２２条 情報システム担当者は，障害管理簿が作成され随時更新されるよう，必要な措置を講ずるものとする。

２ 障害管理簿には，次の各号に掲げる事項を記載するものとする。
（１）障害発生の日時
（２）復旧の日時
（３）障害が発生したサブシステム名
（４）障害の種別
（５）障害内容及び状況
（６）影響の範囲
（７）発生原因
（８）対策した内容
（９）再発の可能性

（障害の再発防止）

第２３条 情報システム担当者は，３か月に１回以上障害記録が確認され障害の再発防止が図られるよう，適切な措置を講ずるものとする。

２ 特に次の各号に掲げる障害記録については，再度確認作業が行われるようにするものとする。
（１）復旧が完了していないもの
（２）発生原因が不明のままのもの
（３）再発可能性が高いもの
（４）障害発生による影響範囲が広いもの

（情報システムの監視）

第２４条 情報システム担当者は，ネットワーク管理システム等により，常時サーバ及びネットワーク機器の稼動状況を監視するものとする。

２ 監視は，次の各号に掲げる事項について行うものとする。
（１）機器の起動及び停止の状況
（２）入出力トラフィック量
（３）ＣＰＵ使用率
（４）メモリ使用率

（バックアップ）

第２５条 情報システム担当者は，次の各号のいずれかに該当する場合，各バックアップ対象についてバックアップ計画書に基づきその前後にフルバックアップが取られるよう，必要な措置を講ずるものとする。

（１）サーバの初期セットアップ（又はＯＳの再インストール）を行うとき

（２）サーバ等に重要な新しいソフトウェアの導入を行うとき

（３）サーバ等のＯＳ等のバージョンアップ（又はパッチ適用）を行うとき

２ バックアップ計画書には，次の各号に掲げる事項を記載するものとする。

（１）バックアップ方式

（２）バックアップ周期

（３）バックアップ対象データ

（４）バックアップ装置及び記憶媒体

（５）保管場所

（６）保管期間

（７）リストア作業手順

（８）作業責任者

３ バックアップを定期的に行うサーバ等は，別表第３に掲げるサーバ等とする。

（情報及びソフトウェアの交換）

第２６条 情報システム管理者は，組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）について，必要に応じてその合意内容に関する正式な契約を締結するものとする。

２ 前項の契約には，次の各号に掲げる事項を記載するものとする。

（１）通知確認手順（発送者から受領者への発送したことの連絡。受領者から発送者への受領の有無の連絡。）

（２）配送者の身分を確認する方法

（３）データが紛失した場合の責任及び補償

３ 情報システム管理者は，物理的な配送（郵便又は宅配便等による送付）を行う場合，次の各号に掲げる項目を考慮しなければならない。

（１）信頼できると判断する輸送機関又は宅配業者のみを用いること。

（２）配送途中の物理的損傷から内容物を保護するのに十分な梱包とし，製造者の仕様を満たすこと。

（３）慎重に取り扱うべき情報については，施錠されたコンテナを使用するか，開封した証拠が残るような開封防止包装を使用すること。

４ 情報システム管理者は，他機関と電子媒体を交換する場合，ウイルスチェックの実施を徹底するものとする。

（セキュリティ情報の収集及び提供）

第２７条 情報システム担当者は，ソフトウェア管理簿及びハードウェア管理簿を参考にして，所掌する全てのハードウェア及びソフトウェアのセキュリティ情報が定期的に

収集されるよう，必要な措置を講ずるものとする。
2 情報システム担当者は，メーリングリストなどの受動的に情報を収集できる手段を用いるほか，Ｗｅｂページ等の更新情報を能動的に１日１回以上確認することにより，セキュリティ情報が収集されるよう，必要な措置を講ずるものとする。
3 情報システム担当者は，収集したセキュリティ情報を重要性，影響範囲などから次の各号のとおり分類するものとする。
（1）危険度 高
即座に対応が必要なもの。サーバの管理権限剥奪などにより，業務停止等の影響を与える可能性があるもの。
（2）危険度 中
定期メンテナンス時などに対応する必要があるもの。業務停止などのおそれはない。
（3）危険度 低
特に対処しなくともよいもの。特殊な環境や設定においてのみ発生し，学内のシステムへの影響はない。
4 情報システム担当者は，危険度 中以上のセキュリティ情報を関係者に周知するとともに, パッチ適用, ウイルス定義ファイルの更新等の必要な作業を行わなければならない。

（コンピュータウイルス対策）
第２８条 情報システム担当者は，次の各号に掲げる機能を有するウイルス対策ソフトが使用されるよう，必要な措置を講ずるものとする。
（1）定義ファイルが１日１回以上自動更新される機能
（2）常時スキャン機能
2 情報システム担当者は，セキュリティ関連の代表的なサイト及びウイルス対策ソフトベンダ等のサイトから，コンピュータウイルスに関する情報を常に収集しなければならない。
3 情報システム管理者は，ウイルスに感染した場合の連絡方法を作成しなければならない。
4 利用者は，ウイルスに感染したことを発見した場合，前項で規定する連絡方法に従い報告しなければならない。
5 情報システム担当者は，次の各号に掲げるウイルス対策の実施が利用者に徹底されるよう，必要な措置を講ずるものとする。
（1）端末に導入されたウイルス対策ソフトを常駐設定にすること。
（2）１週間に１回以上，ファイル全体に対するウイルススキャンを実施すること。
（3）ウイルスが検出された場合，ウイルス対策ソフトにより駆除すること。
（4）ウイルスの駆除結果を情報システム担当者に報告すること。

(不正アクセス対策)
第２９条 情報システム担当者は，次の各号に掲げる不正アクセス対策が実施されるよう，必要な措置を講ずるものとする。

（１）使用されていないポートへの接続を可能な状態にしておかないこと。
（２）セキュリティホールの発見に努め，メーカ等からのパッチがあり次第速やかにパッチを適用すること。
（３）不正アクセスによるＷｅｂページの書換を確実に防止するため，担当職員によるものか否かにかかわりなく，データの書換を検出し，情報システム担当者へ通知する設定を施すこと。
（４）重要なシステムの設定に係るファイル等について，１日１回以上当該ファイルの改ざんの有無を検査すること。
２ 利用者による不正アクセスがあった場合，情報システム管理者は，情報セキュリティ管理事務局に次の各号に掲げる事項を報告しなければならない。
（１）不正アクセスの対象となったサブシステム
（２）不正アクセスの日時
（３）不正アクセスの方法
（４）不正アクセスが行われたことによる影響
（５）その他参考となる事項

（アクセス記録の閲覧）
第３０条 情報システム担当者は，不正アクセス等重大なセキュリティ違反を行った利用者がいるおそれがある場合，当該利用者のアクセス記録等の調査を行うものとする。
２ 情報システム担当者が利用者のプライバシーに関する情報を調査する場合，セキュリティ管理者に次の各号に掲げる事項を記載した書面を提示し，当該調査実施についての承認を得なければならない。
（１）調査の必要性
（２）調査対象となる利用者の所属及び氏名
（３）調査の方法
（４）調査立会人の所属及び氏名
３ 情報システム担当者は，前項の規定により実施する調査の経過等をプライバシー情報調査記録簿に記録し，最重要(Ⅰ)情報として管理しなければならない。

第４章 委託先管理

（契約締結前の情報公開）
第３１条 情報システム管理者は，入札の実施等において，県の保有する情報を公開する場合，当該情報を公開する前に，情報を公開する相手と機密保持に関する協定書（様式第５号）が結ばれるよう，必要な措置を講ずるものとする。

（委託契約の締結）
第３２条 委託契約を締結するときは，契約書雛形（様式第６号）の各条項を参考にして契約書を作成するものとする。

（委託先管理）

第３３条 情報システム担当者は，外部委託の管理に関して，次の各号に掲げる説明等が実施されるよう，必要な措置を講ずるものとする。

（１）外部委託先事業者用遵守事項説明シート（様式第７号）に従い，遵守すべき事項を委託先に説明すること。

（２）前項の説明実施後，委託先法人の代表者及び従事者に情報セキュリティポリシー遵守に関する同意書（様式第８号）へ署名及び押印（法人の代表者については記名及び押印でもよい。）してもらうこと。

（３）貸与する情報資産等（ＰＣ，名札等）がある場合，情報資産授受簿（様式第９号）により適切に管理すること。

（４）使用を認めるサブシステムは業務に必要な最低限のものとし，適切に管理すること。

（５）利用者登録を行った者については，第１０条第３項で規定するユーザＩＤ管理簿等により適切に管理すること。

（６）契約書の記載事項を遵守させ，適切に管理すること。

（貸与物品の回収等）

第３４条 情報システム担当者は，委託契約の終了にあたり，次の各号に掲げる貸与物品の回収等が行われるよう，必要な措置を講ずるものとする。

（１）貸与した情報資産等（ＰＣ，名札等）を回収し，前条第３号に規定する情報資産授受簿に情報システム担当者及び受託者が署名すること。

（２）前条第５項によりユーザ登録を承認したユーザを，ユーザＩＤ管理簿により削除すること。

第５章 事案処理

（事案の報告）

第３５条 事案の報告は，事案報告書（様式第１０号）により，情報セキュリティ担当者に行うものとする。

２ 情報セキュリティ担当者が不在のときは，情報セキュリティ管理者（副）に報告し，情報セキュリティ管理者（副）も不在のときは，情報セキュリティ管理者に報告するものとする。

（事案対応体制）

第３６条 情報システム管理者は，情報セキュリティに関する事案を発見した場合には，必要に応じて速やかに情報セキュリティ管理事務局へ事案の報告を行うとともに，次の各号に掲げる事項を実施するものとする。

（１）原因の調査及び対策の実施。

（２）事案解決後の再発予防先の検討。

（３）庁内における情報共有のため事案報告書の写しを情報セキュリティ管理事務局へ送付すること。

第６章 システム利用要項

（システム利用要項）

第３７条 次の各号に掲げるサブシステムの管理者は，このセキュリティ実施手順を実施するために必要なシステム利用要項を情報システム管理者の承認を得て定めるものとする。

（１）大学情報サブシステム

（２）学務事務システム

（３）医療情報システム

（４）ＰＡＣＳ系システム

第７章 学内において使用される端末や情報資産の管理

（端末の適切な管理）

第３８条 本学において端末を使用する者は，前条までの規定を参考にして端末を自ら適切に管理しなければならない。

２ 前項の規定により端末を適切に管理できる見込みのない者は，公費で端末を購入してはならない。

（電子メール等の送信を除く情報資産の持ち出し）

第３９条 本学の教職員は，本学の情報資産を執務室外に持ち出す場合は，情報資産持出申請書(様式第１１号)により情報セキュリティ管理者の許可を得るとともに，持ち出した情報資産を適切に管理しなければならない。

２ 本学の教職員は，外部で県の情報資産を用いて情報処理業務を行う場合は，情報セキュリティ管理者の許可を得るとともに，適切な安全管理措置を実施しなければならない。

３ 本学の教職員は，前２項に係る情報資産が不要になった場合は，適切に処分しなければならない。

４ 情報セキュリティ管理者は，本学の教職員が情報資産を持ち出す場合，情報資産持出記録台帳（様式第１２号）を作成し，保管しなければならない。

（電子メール等を用いた情報資産の送信）

第４０条 電子メールやその添付文書等により，次の各号のいずれかに該当する情報資産を送信しようとする本学の教職員は，必要に応じ暗号化，電子署名付与又はパスワード設定を行わなければならない。

（１） 不開示に相当する機密性を有する情報資産

（２） 不開示に相当する機密性は要しないが，直ちに一般に開示することを前提としていない情報資産

（３）改ざん，誤びゅう又は破損により，個人の権利が侵害される，又は本学の教育研究並びに事務運営に支障（軽微なものを除く。）を及ぼすおそれがある情報資産

（私物の機器等の持ち込み禁止）

第４１条 本学の教職員は，私物のパソコン等の機器を執務室に持ち込んではならない。

第８章 専決

（専決）

第４２条 事務局長は，本実施手順により情報セキュリティ管理者及び情報システム管理者が行うものと規定される事項を専決するものとする。

付 則

１ この要項は，平成１６年５月１７日から施行する。

２ この要項において規定されている各種台帳及び機器の設定等については，平成１６年９月３０日までに，各サブシステムの管理者が整備するものとする。

３ 通信における電子署名及び暗号化については，暗号化通信のための条件が整備された段階で，この要領に規定するものとする。

付 則

この要項は，平成２３年７月１２日から施行する。

ただし，第４０条の規定にかかわらず，教育研究用情報機器の整備が整うまでの間，教育研究活動に著しい支障が生じるおそれがあり，外部のパソコン等をやむを得ず使用しようとする場合は，原則として情報システム運用管理責任者に協議を行うものとする。

付 則

この要項は，平成２６年４月１日から施行する。

別表第1（第7条） 情報システム管理者が所掌する全てのサブシステム

システム名称	サブシステム名称	サブシステム管理者	個別システム名称	個別システム管理者
大学情報システム	大学情報サブシステム	総務課長	HP公開システム	総務課長
			学内HP公開システム	
			グループウェアシステム	
			メール中継システム	
			ファイルサーバシステム	
			ターミナルサーバシステム	
			予算物品管理システム	
			統計計算システム	
			給与計算システム	
			図書館システム	
			就職情報システム	教務課長
			健康管理システム	
			インターネット対応CD-ROMシステム	総務課長
			CD-ROMチェンジャーシステム	
			学生用パソコンシステム	
			院生用パソコンシステム	
			教員用パソコンシステム	
			講義用パソコンシステム	
			事務用パソコンシステム	
			カード作成システム	
			ユーザー括登録システム	
			電子掲示板システム	
			クライアントパソコン用ウイルス対策システム	
			クライアントパソコン管理システム	
			LANシステム	
	学務事務システム	教務課長		
	PACS系システム	画像LAN管理責任者＊		
	教員が備品として購入したコンピュータ	教員個人　＊		
医療情報システム		病院管理課長	病院情報システム	病院管理課長
			OAシステム	総務課長
			LANシステム	

＊情報システム部会長が管理指導する。

別表第２（第１９条第２項）　ログの解析を行うサーバ等

システム名称	サーバ等名称
大学情報サブシステム	ＨＰ公開システム
	FW
付属病院情報システム	FW

別表第３（第２５条第４項）　バックアップを行うサーバ等

システム名称	サーバ等名称	サーバ等の種類	バックアップ実施の時期	台数
大学情報サブシステム	ＨＰ公開システム	WWWサーバ	１か月に１度	1
		DNSサーバ	設定内容を変更した時（プライマリのみ）	1
	学内ＨＰ公開システム	イントラネットサーバ	毎日（平日の夜）	1
	グループウェアシステム	メールサーバ	毎日（平日の夜）	1
	ファイルサーバシステム	NetWareサーバ（４台）	毎日（平日の夜）	4
	予算物品管理システム	予算管理サーバ	毎日（平日の夜）※NetWareｻｰﾊﾞの１台を利用	（1）
	統計計算システム	統計計算サーバ	随時	1
	給与計算システム	給与データベースサーバ	１か月に１度	1
	図書館システム	図書館データベースサーバ	毎日（平日の夜）	1
	就職情報システム	就職情報システムサーバ	毎日（平日の夜）	1
	ｸﾗｲｱﾝﾄﾊﾟｿｺﾝ用ｳｲﾙｽ対策ｼｽﾃ	ｳｲﾙｽ対策用ｻｰﾊﾞ	随時	1
	ｸﾗｲｱﾝﾄﾊﾟｿｺﾝ管理ｼｽﾃﾑ	修正ソフト配付用サーバ	随時	1
付属病院情報システム	医療情報システム		毎日（平日の夜）	
	ＯＡシステム		毎日（平日の夜）	

様式第1号（第9条第1項）

管理区域チェックリスト

注）○・・・必須、 △・・・代替策があれば可

		チェック項目	セキュリティ区域	業務区域		チェック欄	備考
物理環境	1	警備員が配置されている。	△	△			
	2	身分証等による入館チェックを実施している。	○	△	注1		
	3	ICカードによる入室チェックを実施している。	△	△			
	4	その他（暗証番号、バイオメトリクス等）による入室チェックを実施している。	△	△			
	5	入室の際警備員等による荷物チェックを行っている。	△				
	6	必要な物以外の荷物をロッカーに預けるようになっている。	△				
	7	夜間・土日・休日は入口が制限されている。	○	○			
	8	搬入・搬出及び外部業者の入退館は定められた出入口に限定している。	○	○			
	9	土日・休日の入退館の記録を取っている。	○	○			
	10	第3者(県民・企業等)の入退館の記録を取っている。	○				
フロア	11	二重床になっている。	△				
火災	12	消火器が設置されている。	○	○			
	13	消火用のスプリンクラーが設置されている。		△			
	14	防火壁が採用されている。	△				
	15	ハロゲン等の特別な消火設備が設置されている。	△				
水害	16	防水設備又は排水設備を設置している。	○	○			
	17	セキュリティ区域は2F以上に設置されている。	△				
	18	セキュリティ区域には特別な耐水装置を設置している。	△				
空調	19	通常の空調設備を設置している。	○	○			
	20	セキュリティ区域にはメーカが推奨するレベルの空調設備を設置している。	△				
粉塵	21	定期的な清掃が行われている。	○	○			
	22	セキュリティ区域では飲食、喫煙を禁止している。	○				
耐震	23	震度5以上の耐震構造となっている。	○				
	24	震度6以上の耐震構造となっている。	△				
	25	重要なシステムは耐震用ラックに収容されている。	△				
電源	26	UPSを設置している。	○				
ケーブル	27	重要なケーブルは二重床に設置されている。	○				
	28	LANと電源ケーブルは区別されて設置されている。	○				

注1：業務区域の要件として、1～4に△印がついているが、
このうちの一つが必ず備わってるということを、必須要件とする。

ハードウェア管理簿

（ハードウェア管理簿　記入例）

様式2

担当部署：
情報システム管理者：
情報システム担当者：
連絡先：
E-Mail：
最終更新日：

機器名	利用目的	OS※1	HDD容量※1	CPU※1	メモリ※1	製造番号（S／N）	周辺機器	設置場所	ホスト名	利用者※2	機器管理者※3	保守業者	保守業者連絡先	障害履歴No※4	購入年月日	破棄確認年月日	リースについて	持出記録※5	備考
Compaq ProLiant ML330	検証サーバ	Windows2000Serv	100GB	PentiumIII1.4G	512MB	****-***	FDD、CD-RW、外付DAT	本庁○F	ex_1	ー	山田太郎	-	-		2003/xx/xx		なし		
cisco2501	検証	ー	ー	ー	ー	****-*****-**	ー	本庁○F	ex_2	ー	山田太郎	日立	029-301-xxxx	sample-001	2003/xx/xx		なし		
IBM　Thinkpad	クライアント	Windows98	10GB	PentiumIII1G	128MB	*****-**	FDD	本庁○F	ex_c01	山田太郎	ー	-	-		2003/xx/xx		なし		

貸与PC以外のハードウェアについて記入（外部委託先事業者の持込PC、各部PC、各部プリンタ、サーバ、NW機器（ルータ、SW、HUB）等）
※1：NW機器、プリンタについては不要。PCについても必要に応じて記入する
※2：利用者、職員IDは、クライアント端末のみ記入する
※3：サーバ、NW機器等の場合に当該機器を管理している者（情報システム担当者等）を記入。クライアント端末の場合は不要
※4：障害履歴Noは、障害履歴と連動されていること
※5：持出記録は、別に記録簿を作成しリンクさせても良い

ハードウェア管理簿（USBメモリ用）

様式2（イ） その2

（第11条第1号）

管理番号	所属	利用者名	メーカー、製品名、特徴（色等）	容量	通常の保管場所	購入年月日	廃棄確認年月日	備考

USBメモリについて記入

※1:『管理番号』は、「看護学科は、N0001から」、「理学療法学科は、P0001から」、「作業療法学科は、O0001から」、「放射線技術科学科は、R0001から」、「医科学センターは、M0001から」、「人間科学センターは、H0001から」　連番を付与する。

※2:『メーカー、製品名、特徴（色等）』は、USBメモリが特定できるような内容を記入する。

様式第3号（第11条第2号）　　ソフトウェア管理簿

担当部署：	茨城県立医療大学
ｻﾌﾞｼｽﾃﾑ名：	
情報システム管理者：	
情報システム担当者：	
連絡先：	
E-Mail：	
最終更新日：	

ソフト名	ソフト種別（ソフトウェアの機能等）	ライセンス数	ライセンス残数	バージョン	利用目的	ソース・マニュアル保管場所	購入年月日	破棄確認年	備考

※1：企画部情報政策課でライセンスを管理しているソフトについては記載不要。
※2：各部、各担当、プロジェクト等でライセンスを購入した場合はライセンス数とライセンス残数を記載。

様式第４号（第11条第３号）

管理者用パスワード管理簿

サブシステム名	ソフト名等	管理者権限ﾕｰｻﾞID	パスワード	備考

様式第５号（第３１条）

機密保持に関する協定書

　茨城県立医療大学（以下「甲」という。）と〇〇株式会社（以下「乙」という。）とは，甲乙間で相互に開示される機密情報の取扱いに関して，次のとおり協定書を締結する。

（目的）

第１条　本協定書は，甲乙間で「〇〇業務に関わる受託者公募」に関する事前検討（以下，「事前検討」という。）を行うにあたり，甲乙間で相互に開示される機密情報の秘密保持に関する取扱いを定めることを目的とする。

（機密情報）

第２条　機密情報とは，事前検討に関して，甲又は乙が相手方から開示を受ける機密性を有する一切の営業上又は技術上の情報で，次の各号に掲げるものである。

（１）書面又は電子媒体で開示される情報で，当該書面又は電子媒体に「機密」又はそれに類似した表示を明示して相手方に開示されるもの。

（２）口頭で開示される情報で，開示者が開示時点で機密である旨を明確に示し，開示後 14 日以内に開示者が「機密」又はそれに類似した表示を示した文書によりその内容を詳記して，受領者に交付し，その文書の内容・範囲について書面により受領者の確認を得るもの。

（機密保持等）

第３条　甲および乙は，次の各号に掲げる事項を遵守しなければならない。

（１）相手方の事前の書面による承諾なく，機密情報を第三者に対して開示又は漏洩しないこと。

（２）相手方の事前の書面による承諾なく，本協定の条項及び条件並びに本協定に基づく相手方との情報の授受及び打合せの存在を第三者に対して開示又は漏洩しないこと。

（３）相手方の事前の書面による承諾なく，本協定に基づく権利義務の全部又は一部を第三者に譲渡し又は承継しないこと。

（４）本協定における機密情報に該当するか否かにかかわらず，相手方から受領したいかなる情報も，法令等により許される場合を除き，いかなる国へも輸出しないこと，また非居住者に提供しないこと。

（５）善良なる管理者の注意をもって機密情報を管理し，本条に定める機密保持義務を果たすこと。

（適用除外）

第４条　次の各号に掲げる情報については，機密情報に含まれないものとする。

（１）受領者が開示者又は正当な権利を有する第三者から守秘義務を負うことなく正当に入手した情報。

（２）受領者が既に保有していた情報。
（３）受領者への開示後に受領者の責めに帰すべからざる事由により公知の事実となった情報。
（４）受領者が開示者の情報によらず独自に開発した情報。
２　受領者は，本協定に基づく機密保持義務を告知した上で，機密情報を知る必要がある自己の役員及び職員（以下「職員等」という。）のみに当該機密情報を開示することができる。
３　受領者は，事前検討のため必要な範囲で機密情報を複製することができる。この場合，当該機密情報に付された著作権表示その他の表示を当該複製物に付さなければならない。

（目的外使用の禁止）
第５条　甲および乙は，相手方の事前の書面による承諾なく，機密情報を事前検討以外の目的に一切使用してはならない。

（情報の帰属）
第６条　本協定書に基づき開示される情報に関する商標，特許，著作権その他の知的財産権に基づく権利について受領者は，情報の開示を受けたことにより，黙示的であると否とを問わず，当該権利について開示者から何らの権利を許諾されるものではない。

（保証）
第７条　甲および乙は，正当に開示する権利を有する機密情報を相手方に開示するものとする。ただし，甲および乙は，機密情報およびその利用に関して，第三者の知的財産侵害の有無を含め，機密情報につき，いかなる保証責任も負わないものとする。

（損害賠償）
第８条　甲および乙は，本協定の条項に違反し相手方に損害を与えた場合は，相手方に生じた直接かつ通常の損害に対して，賠償の責を負うものとする。

（協定の効力）
第９条　本協定書のいかなる規定も，相手方に何らかの機密情報の開示義務を課すものではない。
２　甲および乙は，本協定書に基づく甲又は乙の相手方への機密情報の開示により，甲乙間で何らかの取引を行うことを約束するものではない。

※必要に応じて入れること

（協定書の有効期間）
第１０条 本協定書の有効期間は，本協定書の締結日より〇年とする。但し，必要ある場合は甲乙協議の上これを延長することができる。
２　本協定書の有効期間に関わらず，第４条および第５条の規定は，本協定書終了後も２年間有効に存続するものとする。

（情報の返還等）
第１０条 甲および乙は，本協定書の有効期間が終了した場合，又は有効期間中に相手方から機密情報の返還請求が為された場合は，当該機密情報の使用を直ちに中止し，受領した機密情報を速やかに相手方に返還し，又は相手方の指示に従って廃棄等を行うものとする。受領した機密情報の複製物についても同様とする。

（合意管轄）
第１１条 甲および乙は，本協定もしくはその条項に関連して発生する紛争については，水戸地方裁判所を第一審の専属的合意管轄裁判所としてこれを解決するものとする。

（協議事項）
第１２条　本協定に定めのない事項に関して解釈に疑義が生じた場合については，甲乙双方において協議のうえ，円満にこれの解決を図るものとする。

上記のとおり契約して本協定書２通を作成し，甲乙記名捺印のうえ，各１通を保管する。

平成　　年　　月　　日

茨城県稲敷郡阿見町阿見 4669 番地 2
（甲）
茨城県立医療大学
学長　　○○　○○

○○○○
（乙）
○○○○
○○　○○

様式第６号（第３２条）契約書雛形

○○○業務委託契約書

茨城県立医療大学（以下「甲」という。）と○○○（以下「乙」という。）とは，○○○について，次のとおり委託契約を締結する。

（委託業務）

第１条　甲は，次の業務（以下「委託業務」という。）の実施を乙に委託し，乙は，これを受託するものとする。

（１）委託業務名　○○○業務

（２）委託業務の内容　別添○○○業務委託仕様書（以下「仕様書」という。）のとおり

（３）実施期間　この契約の締結の日から平成○○年○○月○○日まで

（委託業務の実施）

第２条　乙は，委託業務を仕様書に従って実施しなければならない。仕様書が変更された場合も同様とする。

（委託費）

第３条　甲は，委託業務に要する費用（以下「委託費」という。）として金○○円（うち取引に係る消費税及び地方消費税の額○○円）を乙に支払うものとする。

（委託費の支払）

第４条　甲は，委託費を，第10条の規定による適合の通知をした後に，乙の請求により支払うものとする。

２　甲は，前項の請求を受けた日から起算して３０日以内に，委託費を支払うものとする。

（契約保証金）

第５条　契約保証金は免除する。

（権利義務等の譲渡等の制限）

第６条　乙は，この契約によって生ずる権利又は義務を第三者に譲渡し，又は承継させてはならない。ただし，書面により甲の承認を受けた場合又は，信用保証協会及び中小企業信用保険法施行令（昭和２５年政令第３５０号）第１条の２に規定する金融機関に対して売掛債権を譲渡する場合にあっては，この限りでない。

２　前項ただし書きにより，乙が売掛債権を譲渡した場合，甲の乙に対する弁済は，甲が茨城県財務会計オンラインシステムによる支出命令等決裁入力をした時に提供されたものとする。

（再委託の制限）

第７条　乙は，委託業務達成のため，委託業務の一部を第三者に委託し，又は請け負わせることを必要とするときは，あらかじめ甲の書面による承諾を得なければならない。

（秘密の保持）

第８条　乙は，委託業務の実施に際して知り得た秘密を第三者に漏らしてはならない。

２　乙は，前条の規定により甲が承諾した再委託の相手方に，前項の規定を遵守させなければならない。

（実績報告）
第９条　乙は，委託業務が終了したときは，遅滞なく，委託業務の成果を記載した実績報告書を甲に提出しなければならない。
（適合の審査及び通知）
第10条　甲は，前条の規定により，乙から実績報告書の提出を受けたときは，遅滞なく，当該事業がこの契約の内容に適合するものであるかどうかを審査し，適合すると認めたときは，その旨を乙に対して通知するものとする。
（委託業務の中止等）
第11条　乙は，災害その他やむを得ない事由により委託業務の遂行が困難となったときは，その事由及び経過を記載した書面を甲に提出し，その指示を受けなければならない。
２　甲は，前項の書面が提出されたときは，乙と協議のうえ，この契約を解除し，又は変更するものとする。
３　第４条，第９条及び前条の規定は，前項の規定によりこの契約を解除した場合に準用するものとする。
（委託業務の変更）
第12条　乙は，前条第１項に規定する場合を除き，仕様書に記載された委託業務の内容を変更しようとするときは，その旨を書面により甲に申し出て，甲の書面による承認を受けなければならない。
（契約の解除等）
第13条　甲は，乙がこの契約に違反した場合は，この契約を解除し，又は変更し，既に支払った金額の全部又は一部の返還を請求することができる。
（業務内容の変更等）
第14条　甲は，必要があると認めるときは，委託業務の内容を変更し，又は委託業務の処理を一時中止することができる。この場合において，委託費，実施期間その他この契約の内容を変更する必要があるときは，甲乙協議して書面により定めるものとする。
２　前項の場合において，乙が損害を受けたときは，甲は，その損害を賠償しなければならないものとし，その賠償額は甲乙協議して定めるものとする。
（損害のために必要を生じた経費の負担）
第15条　乙は，委託業務の処理に当たって，甲又は第三者に損害を与えたときは，その損害を賠償しなければならない。ただし，その損害のうち，甲の責めに帰すべき事由により生じたものについては，甲が負担するものとする。
（実施期間の延長等）
第16条　乙は，その責めに帰することができない事由により実施期間内に委託業務を完了することができないことが明らかになったときは，甲に対し，遅滞なく，その理由を示して実施期間の延長を求めることができる。
２　甲は，乙の責めに帰すべき事由により履行期間内に委託業務を完了することができないときは，乙から損害金を徴収して実施期間を延長することができる。
３　前項の損害金の額は，延長日数に応じ，委託料に年3．6パーセントの割合を乗じて得た額（その額に100円未満の端数があるとき又は金額が100円未満であるときは，その端数額又はその金額を切り捨てた額）とする。

（契約の解除）

第17条　甲は，乙が次の各号のいずれかに該当するときは，この契約を解除することができる。

（１）その責めに帰すべき事由により実施期間又は実施期間経過後相当の期間内に委託業務を完了する見込みがないと明らかに認められるとき。

（２）正当な理由なく，委託業務に着手すべき時期を過ぎても委託業務に着手しないとき。

（３）第７条及び第８条の規定に違反したとき。

（４）前各号に掲げる場合のほか，この契約に違反したことによりこの契約の目的を達成することができないと認められるとき。

（委託業務の報告等）

第18条　甲は，必要があると認めるときは，乙から委託業務の実施状況，委託費の使途その他必要事項について報告を求め，又は実地に調査できるものとする。

２　乙は，前項の規定により甲から報告を求められたときは，速やかに甲に報告するものとする。

（著作権）

第19条　乙が委託業務により取得した著作権は，甲が継承するものとする。

（帳簿等）

第20条　乙は，委託業務に係る経費について，帳簿を備え，収入支出の額を記載し，その出納を明らかにしておくとともに，これをその完結の日から５年間保存するものとする。

（疑義の処理）

第21条　この契約に定めのない事項及びこの契約に関して疑義が生じたときは，甲の指示により処理するものとする。

この契約を証するため，本書２通を作成し，甲乙記名押印のうえ，各１通を保有する。

平成　年　月　日

茨城県稲敷郡阿見町阿見４６６９番地２

甲

茨城県立医療大学学長　○○　○○　印

○○○○

乙

○○○○　　○○　○○　　印

様式第７号（第３３条第１号）

外部委託先事業者用遵守事項説明シート

説　明　日　：

【茨城県庁側】

所　属		情報システム管理者	
		説明実施者	

【外部委託先事業者側】

会社名		セキュリティ責任者	
契約期間	～	委託先社員(対象者）名	

遵守内容	
パソコン設定・使用	
☐	ＰＣで使用するソフトウェアは情報システム管理者に許可されたソフトウェアのみ使用する
☐	庁内ＮＷ、庁内システム等への初期パスワードは利用開始後速やかに変更する
☐	各種システムのパスワードは推測できないフレーズとし、使いまわし（同じパスワードの再利用）はしない。また、ＰＣに電子メール等のパスワードを記憶させてはならない。
☐	私用メールや業務外ホームページ閲覧の禁止
☐	帰宅の際、ノートＰＣについては施錠可能な書庫・袖机等に保管する、ワイヤケーブルで施錠するなど各部で定められたルールに従う
☐	作成中または作成済みの重要なファイルは、担当やプロジェクトのルールに従って保存し、出来るだけクライアントＰＣには保存しない
（ウイルス対策）	
☐	庁外からのダウンロードファイル、出所不明なメディアのソフトウェアの利用やリムーバルディスク（ＦＤ、ＣＤ－Ｒ等）からのファイルを使う場合、必ずウイルスチェックを実施する
☐	庁内ＬＡＮに接続する場合、ウイルス対策ソフトを常時起動し、最新のパターンファイルに更新されるよう設定する
☐	ウイルスに感染した場合、感染したＰＣ等をネットワークから切り離し、速やかに情報システム管理者に報告する
クリアデスク・クリアスクリーン	
☐	各部で定めた重要な書類は、長時間の離席や帰宅の際に机上、足回り、キャビネット上などに放置せず、書庫やキャビネットに施錠保管する等各部で定められたルールに従う
☐	ＰＣにはスクリーンセーバにパスワード設定を行うとともに、離席の際はＰＣにファイルを開いたままにしない
☐	重要な情報をプリントアウト、コピー、ＦＡＸ受信する際は、出力後放置せずすぐに回収する
☐	重要な情報を廃棄する場合は、シュレッダー等各部で定められたルールに従う
入退室関連	
☐	庁舎等・管理区域への入退館（入退室）に必要な身分証等は紛失しないように厳重に取扱う
☐	セキュリティ区域・業務区域では、顔写真入りの身分証(指定部門のみ)等は名札を周囲に見えるように提示する
☐	深夜、休日等に業務を行なう場合は、情報システム管理者に許可を得る
機密保持	
☐	貸与ＰＣ、持込ＰＣを問わず、契約期間中の庁外持出は禁止する　（業務上やむを得ず持ち出す場合は、情報システム管理者の承諾を得る）
☐	業務上知り得た情報についての会話に注意する　（飲食店、通勤途中、委託会社内は勿論、庁内でも食堂等の共用区域では話題にしない）
☐	契約期間終了後において、契約期間中にインストールしたソフトウェアや作成したファイルがＰＣ、媒体に保存されている場合は、情報システム管理者の指示に従い、速やかに破棄を行なう
☐	契約終了時には、貸与物品を速やかに返却する　（顔写真入り身分証(指定部門のみ)、貸与ＰＣ、電話機等）

様式第８号（第３３条第２号）

情報セキュリティポリシー遵守に関する同意書

茨城県立医療大学学長　　殿

平成　　年　月　　日

住所
　契約会社

代　表　者　　印
従　事　者　　印

私こと上記の従事者は，平成　年　月　日から貴学の施設に立入るにあたり，下記事項を守ることを同意します。

記

１．貴学の指導に従い規律を維持し，業務を誠実に遂行し専念すること。
２．貴学の定める規律，規程，指示等を遵守すること。
３．貴学より業務遂行上貸与されているシステムにおいて，私用メールの利用及び業務外ホームページの閲覧を一切しないこと。
４．貴学から貸与されているパソコン及び個人持込パソコンについては業務従事期間中は庁外に持ち出さないこと。なお，やむを得ず持ち出す場合は貴学の承諾を得ること。
また，業務期間終了後は，貴学から貸与されているバソコン及び個人持込パソコンに保存されている業務上知り得た全てのデータを消去したうえで，貴学から貸与されているパソコンについては，貴学に返却すること。
５．貴学において業務上知り得た知識，資料及び情報（有形･無形を問わない）を機密事項とし，貴学の承諾なしに，貴学職員，社外者及びその他第三者に書面・口頭などいかなる方法によっても開示しないこと。
６．機密事項は貴学から指示された業務の遂行のためにのみ使用し，自己のため，その他第三者のためなどその他の目的には使用しないこと。
７．機密事項に関する書類その他の記録（電磁的媒体に記録されたものを含む）は，使用目的が終了した場合または貴学からの請求がある場合は，直ちに返却するかまたは貴学の指示に従い破棄することとし，庁外に持ち出さないこと。
８．機密事項について，本業務に従事する期間はもとより本業務に従事しなくなった後も守秘義務を遵守すること。
９．本同意書の各条項のいずれかに違反し，故意又は重大な過失によって貴学に損害を与えた場合（ただし，貴学の指揮命令に起因して発生した損害については除く）には，私は，貴学から就業終了についての通告を受けても異議を唱えないこと，また，貴学に対し賠償の責任を負うこと。

様式第9号（第33条第3号）

情報資産授受簿

契約件名	
契約期間	

会社名	
セキュリティ責任者	

茨城県立医療大学 情報システム管理者名	

管理番号	情報資産名(PC端末等含む)	貸与数	貸与（サイン）			返却（サイン）			備考
			貸与月日	貸与者	委託者	返却月日	受領者	委託者	

様式第１０号（第３５条第１項）

事案報告書

報告元

- **報告者：** ＿＿＿＿＿＿＿＿＿＿
- **部局名：** ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- **連絡先：** Tel.　　E-mail：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

１．事案の内容

- **対象（情報システム名等）：** ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
- **発生日時：**　　年　月　日（　）　　時　　分頃
- **事案の種別：**　ウィルス感染／不正侵入／情報漏洩／NW・システム障害
- **事案の発生状況：** ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

２.原因

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

３.対策

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

４.再発防止策

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

５.対応履歴

年　月　日／報告者名：	／概要：
年　月　日／報告者名：	／概要：
年　月　日／報告者名：	／概要：
年　月　日／報告者名：	／概要：

６.その他（障害履歴、変更履歴等）

様式第１１号（第３９条）

情報資産持出申請書

申請日　　年　　月　　日

県立医療大学情報セキュリティ管理者　殿

持出媒体	□１.PC　□２．外部記録装置　□３．USBメモリー　□４．その他（　　）			
	製品名等：			
	備品番号・管理番号等：　　数量：			
持出日時	年　月　日　時　分　・　未　定			
返却（予定）日時	年　月　日　時　分　・　未　定			
申請者（管理責任者）	所　属		フリガナ	
	職　名		氏　名	
	ﾕｰｻﾞｰID		電話(内線)	
用　途				
持出内容	情報の内容： 持出場所（作業場所）： 接続先（該当ある場合記入）：			
セキュリティ対応	○不開示情報　有　・　無　（不開示情報を含む場合は，持出作業はできません）			
	○盗難・紛失への対応(本体)：有　・　無　（パスワードの設定・暗号化・その他）			
	○盗難・紛失への対応(ﾌｧｲﾙ)：有　・　無　（パスワードの設定・暗号化・その他）			
備　考	※長期持出該当（３ケ月以上４ケ月間未満）：　無　・　有　（　　ケ月			
※返却日時	（事務局記入欄）			

注：情報の内容・持出場所・接続先は，具体的に記載してください。
　：必ず，所属学科長又は教授の承認を得て提出願います。
　：長期持出に該当する場合は，承認シールを貼り付けの上，
　　貼り付け状態の写真添付し情報係へ送付してください。

情報セキュリティ管理者（事務局長）	情報セキュリティ担当者（総務課長）	受　付（総務課情報係）	

情報システム運用管理責任者（情報システム部会長）	学科長・センター長

＊ メールアドレス：
　　ｊｏｕｈｏｕ@ｉｐｕ．ａｃ．ｊｐ

様式第12号(第39条)

情報資産持出記録台帳

茨城県立医療大学

No.

	備品番号・管理番号等	持出記録媒体等	持出日及び時刻	利用者（職氏名）	管理者許可印	情報の内容（ファイル名）	持出場所（作業場所）	用途（持ち出した情報資産を用いて処理する業務の内容）	持出先（記録媒体を接続する端末等）	返却日及び時刻	管理者確認印
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

＜茨城県情報セキュリティ対策基準を定める要項＞
（情報資産の持ち出しの記録）
第19条　情報セキュリティ管理者は，所管する所属の職員が情報資産を持ち出す場合，記録を作成し，保管しなければならない。
（情報資産の持ち出し）
第24条　職員は，県の情報資産を執務室外に持ち出す場合は，情報セキュリティ管理者の許可を得るとともに，持ち出した情報資産を適切に管理しなければならない。
2　職員は，外部で県の情報資産を用いて情報処理業務を行う場合は，情報セキュリティ管理者の許可を得るとともに，適切な安全管理措置を実施しなければならない。
3　職員は，前2項に係る情報資産が不要になった場合は，適切に処分しなければならない。