別表第一の一

対象システム、機器の場所および扱う情報及び安全管理上の重要度（高・低）は、下表のとおり。

※安全管理上の重要度「高」：患者及び職員の個人情報（ＩＤ番号を含む）を含む。

※安全管理上の重要度「低」：上記を含まない。

対象システム	機器の場所	扱う情報	安全管理上の重要度
電子カルテ・オーダリング・看護システム	サーバ室・各部門	患者の診療記録、看護記録等	**高**
資源管理サーバ	サーバ室	電子カルテシステムの設定に関わる情報（患者ＩＤを含む）	**高**
ネットワーク監視システム	サーバ室	医療情報システム用ネットワークの稼動情報（患者ＩＤを含まない）	**低**
遠隔監視システム	サーバ室	各医療情報システムサーバの稼動情報（患者ＩＤを含まない）	**低**
統合ＤＷＨ・参照カルテシステム	サーバ室・各部門	患者の診療記録、看護記録等	**高**
眼科ファイリングシステム	サーバ室・各部門	眼科に関わる患者の診療記録、看護記録等	**高**
看護勤務表・コメディカル勤務表システム	サーバ室・各部門	看護師及びコメディカルの勤怠記録情報（職員情報を含む）	**高**
看護職員人事情報システム	サーバ室・各部門	看護師の人事に関わる情報（職員情報を含む）	**高**
ＰＤＡシステム	サーバ室・各部門	患者の注射実施、バイタル、食事量、看護実施等に関わる情報	**高**
院内表示システム	サーバ室・各部門	外来診察順の表示に関わる情報（患者ＩＤを含む）	**高**
医事会計システム	サーバ室・各部門	患者の診療会計に関わる情報	**高**
医事ＤＷＨ	サーバ室・各部門	患者の診療会計に関わる情報	**高**
調定（債権管理）システム	サーバ室・各部門	患者の診療会計に関わる情報	**高**
レセプト総括システム	サーバ室・各部門	患者のレセプトに関わる情報	**高**
ＰＯＳレジスタシステム	サーバ室・各部門	患者の診療会計に関わる情報	**高**
レセプトチェックシステム	サーバ室・各部門	患者のレセプトに関わる情報	**高**
再来受付機システム・窓口受付システム	サーバ室・各部門	患者の診療受付に関わる情報	**高**
診察券発行機システム	各部門	患者の診察券に関わる情報	**高**
自動精算機システム	各部門	患者の診療会計に関わる情報	**高**
会計番号表示システム	各部門	会計の待ち順表示に関わる情報（患者ＩＤを含む）	**高**

面会案内システム	各部門	患者の入院病棟に関わる情報	**高**
調剤支援システム	サーバ室・各部門	患者の処方に関わる情報	**高**
治験管理システム	サーバ室・各部門	患者の治験に関わる情報	**高**
服薬指導システム	サーバ室・各部門	患者の服薬指導に関わる情報	**高**
麻薬管理システム	サーバ室・各部門	患者の麻薬に関わる情報	**高**
薬番号表示システム	各部門	薬の待ち順表示に関わる情報（患者ＩＤを含まない）	**低**
放射線受付システム	サーバ室・各部門	患者の放射線撮影に関わる情報	**高**
放射線画像管理システム	各部門	患者の放射線撮影に関わる情報	**高**
内視鏡受付システム	サーバ室・各部門	患者の内視鏡検査に関わる情報	**高**
内視鏡部門システム	サーバ室・各部門	患者の内視鏡検査に関わる情報	**高**
検体・細菌検査システム	サーバ室・各部門	患者の検体検査・細菌検査に関わる情報	**高**
病理検査システム	サーバ室・各部門	患者の病理検査に関わる情報	**高**
輸血システム	サーバ室・各部門	患者の輸血に関わる情報	**高**
生理検査受付システム	サーバ室・各部門	患者の生理検査に関わる情報（心電図、超音波、脳波に関わる情報を含む）	**高**
心電図システム	サーバ室・各部門	患者の心電図に関わる情報	**高**
超音波システム	サーバ室・各部門	患者の超音波に関わる情報	**高**
脳神経（脳波）システム	サーバ室・各部門	患者の脳波に関わる情報	**高**
手術管理システム	サーバ室・各部門	患者の手術に関わる情報	**高**
麻酔記録作成システム	サーバ室・各部門	患者の麻酔記録に関わる情報	**高**
術中患者生体情報システム	サーバ室・各部門	術中患者の生体情報	**高**
病棟患者生体情報システム	サーバ室・各部門	病棟患者の生体情報	**高**
ＮＩＣＵ生体情報システム	サーバ室・各部門	ＮＩＣＵにおける患者の生体情報	**高**
ＩＣＵシステム	サーバ室・各部門	ＩＣＵにおける患者の生体情報	**高**
透析システム	サーバ室・各部門	患者の透析に関わる情報	**高**
リハビリ管理システム	サーバ室・各部門	患者のリハビリテーションに関わる情報	**高**
診療情報管理・サマリシステム	サーバ室・各部門	患者のサマリに関わる情報	**高**

がん登録システム	サーバ室・各部門	患者のがん登録に関わる情報	**高**
がん登録連携システム	サーバ室	患者のがん登録に関わる情報	**高**
地域連携システム	サーバ室・各部門	患者の地域連携に関わる情報	**高**
医療相談システム	サーバ室・各部門	患者の医療相談に関わる情報	**高**
健診システム	サーバ室・各部門	患者・職員の健診に関わる情報	**高**
栄養管理・食事指導システム	サーバ室・各部門	患者の栄養管理・食事指導に関わる情報	**高**
物品・薬剤管理システム	サーバ室・各部門	物品管理、薬剤管理に関わる情報（患者ＩＤを含まない）	**低**
経営支援システム	サーバ室・各部門	経営に関わる情報（患者ＩＤを含まない）	**低**
グループウェア	サーバ室・各部門	職員間で共有が必要な情報（職員情報を含む）	**高**
ID-LINK	サーバ室・各部門	病院間のカルテ情報共有に関わる情報	**高**
診断書管理システム	サーバ室・各部門	各種診断書に関わる情報	**高**
血糖測定システム	サーバ室・各部門	患者の血糖に関わる情報	**高**
抗がん剤管理システム	各部門	患者の抗がん剤に関わる情報	**高**
入退室管理システム	各部門	サーバ室への入退室情報（職員情報を含む）	**高**
感染管理システム	サーバ室・各部門	患者の感染管理に関わる情報	**高**
計数調剤支援システム	サーバ室・各部門	患者の処方・注射に関わる情報	**高**

別表第一の二

別表第一の一で重要度「高」としたものに関わるリスク分析（リスクとリスク対策）は、下表のとおり。

※リスク分析は、別表第一の一に掲げたシステムごとに行う必要性が薄いため、医療情報システム全体を対象として一括して行う。

※「リスク」の内容は「厚生労働省　医療情報システムの安全管理に関するガイドライン　第５．２版」の「６．２．３リスク分析」に準ずる。

リスク	リスク対策
①　医療情報システムに格納されている電子データ	
（ａ）権限のない者による不正アクセス、改ざん、毀損、滅失、漏えい	・各システムは、ログオン時にユーザーＩＤ及びパスワードで認証することとし、利用者にはユーザーＩＤ及びパスワードを適正に管理するように周知する。 ・電子カルテにはパスワードの最低文字数、有効期間及び認証の有効回数を設定し、パスワードの規定回数を間違えた場合に強制ログオフを行う。 ・サーバ室では静脈認証による入室管理を行う。
（ｂ）権限のある者による不当な目的でのアクセス、改ざん、毀損、滅失、漏えい	・電子カルテには職種ごとにアクセス範囲の設定をし、アクセスログの収集を行う。
（ｃ）コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称を持つ不正なソフトウェア（以下「不正ソフトウェア」という。）や標的型メール等を用いたサーバ攻撃等による不正アクセス、改ざん、毀損、滅失、漏えい	・各システムにはウイルス対策ソフトを導入し、ウイルス定義ファイルを定期的に更新する。また、許可のないソフトウェアのインストールを制限する。
②入力の際に用いたメモ、原稿、検査データ等	
（ａ）メモ、原稿、検査データ等の覗き見	・個人情報を他人の目に触れる場所に放置しないことを周知する。
（ｂ）メモ、原稿、検査データ等の持ち出し	・個人情報の持ち出しの運用に関わる基準を定め、周知する。
（ｃ）メモ、原稿、検査データ等のコピー	・不必要に個人情報のコピーをしないことを周知する。
（ｄ）メモ、原稿、検査データ等の不適切な廃棄	・個人情報を機密文書として分別して適正に廃棄する。
③個人情報等のデータを格納したノートパソコン等の情報端末	
（ａ）情報端末の持ち出し	・個人情報の入った情報端末の持ち出しは禁止する。 ・持ち出す情報端末には、起動パスワードの設定、ウイルス対策ソフトのインストール、許可されていないアプリケーションのインストール制限を行う。

（ｂ）ネットワーク接続による不正ソフトウェアによるアクセス、改ざん、毀損、滅失、漏えい	・各システムを外部ネットワーク（インターネット）とは接続しない。ただし、各サーバの遠隔監視及びリモートメンテナンスは、セキュリティを確保した回線に接続して行う。 ・無線ＬＡＮにはセキュリティ対策（８０２．１ｘを用いた認証）を行う。
（ｃ）情報端末に格納されたデータの漏えい	・各システムでは許可されていないソフトウェアのインストールを禁止する。
（ｄ）情報端末の盗難、紛失	・情報端末が設置された部屋が無人になる際は、施錠を行う。 ・個人情報を含む機器には盗難防止ワイヤーを設置する。 ・監視カメラの設置や、職員及び業者の名札着用を義務化し、不審者の進入を監視する。
（ｅ）情報端末の不適切な破棄	・個人情報の入った情報端末は適切にデータ消去を行ってから廃棄する。
④データを格納した可搬媒体等	
（ａ）可搬媒体の持ち出し	・個人情報の入った可搬媒体の持ち出しは原則禁止とする。ただし、バックアップ媒体の外部保存等については、安全管理事項を契約に明記した上で行う。
（ｂ）可搬媒体のコピー	・不必要に個人情報のコピーをしないことを周知する。
（ｃ）可搬媒体の不適切な廃棄	・個人情報の入っていた可搬媒体は適切にデータ消去を行ってから廃棄するように周知する。
（ｄ）可搬媒体の盗難及び、紛失	・個人情報の入った可搬媒体を適正に管理するように周知する。
（ｅ）可搬媒体接続による不正ソフトウェア感染	・ＵＳＢメモリ等接続させないよう接続ポートに制限を行う。
⑤参照表示した端末画面等	
（ａ）端末画面の覗き見	・電子カルテには一定期間操作しない場合にスクリーンセーバや自動ログオフをするように設定する。また各外来受付のディスプレイに覗き見防止フィルタを設置する。
⑥データを印刷した紙やフィルム等	
（ａ）紙やフィルム等の覗き見	・個人情報を他の患者の目に触れる場所に放置しないことを周知する。
（ｂ）紙やフィルム等の持ち出し	・個人情報の持ち出しの運用に関わる基準を定め、周知する。
（ｃ）紙やフィルム等のコピー	・不必要に個人情報のコピーをしないことを周知する。
（ｄ）紙やフィルム等の不適切な廃棄	・個人情報を機密文書として分別して適正に廃棄する。
⑦医療情報システム	
（ａ）サイバー攻撃によるＩＴ障害	

・不正侵入、不正操作	・システムを外部ネットワークと接続する必要がある場合は、外部の機関とセキュリティ面を中心にリスク分析を行い、対策を講じ責任の所在をはっきりさせた上で、電子情報システム整備検討委員会の承認および院長の決裁をもって行う。
・改ざん・毀損	
・不正ソフトウェアによる攻撃	
・サービス不能（DoS：Denial of Service）攻撃　等	
（ｂ）非意図的要因によるＩＴ障害	
・システムの仕様やソフトウェア上の欠陥（バグ）	・各システムにバグが判明した場合は、速やかに修正する。
・操作ミス	・システム運用マニュアルを整備し、正しい運用を周知する。
・故障外部サ―ビスの利用に伴うシステムポリシー等の意図しない変更等	・サーバ機器は、定期的に保守を行い未然に故障を防ぐ。また、情報のバックアップを行う。 ・端末等の故障については、速やかに修理が可能な体制を整える。また運用が滞らないように予備機を確保する。
（ｃ）災害によるＩＴ障害	
・地震、水害、落雷、火災等の災害による電力供給の途絶	・病院全体としては自家発電装置を設置し、各サーバには無停電電源装置を設置する。
・地震、水害、落雷、火災等の災害による通信の途絶	・各システムを外部ネットワーク（インターネット）と接続しない。
・地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等	・各サーバの設置場所には、耐震化を施し、無水消火装置、漏電防止装置を設ける。
・地震、水害、落雷、火災等の災害による重要インフラ事業者等におけるＩＴの機能不全	・非常時の運用について、別に定める。
（d）許可されていない医療情報システムの利用	
・許可されていない機器、ソフトウェア、サービスの業務利用	・電子カルテには許可されていない機器の接続、ソフトウェアのインストールを制限する、
・管理されている機器、ソフトウェア、サービスの目的外利用	・操作ログを収集し、いつ、どこで、誰が利用したのかを事後に確認できるようにする。