東京医科大学茨城医療センター
病院情報システムの安全管理に関する運用管理規程

第１章　総則

（目的）

第１条　この規程は、東京医科大学茨城医療センター（以下「茨城医療センター」という。）において、法令にて保存義務が規定されている診療録及び診療諸記録（以下「保存義務のある情報」という。）の電子媒体による保存のために使用される情報システムの機器、ソフトウェア及び運用について、その取り扱い及び管理に関する事項を定め、保存義務のある情報の適正保存及び、適正利用に資することを目的とする。

（対象）

第２条　この規程の対象は，次の各号に掲げるところによるものとする。

(1)対象者は，病院情報システムを扱う全ての利用者である。

(2)対象システムは、電子カルテシステム、オーダーリングシステム、医事システム、画像情報システム、検査システム、薬剤システム、その他電子カルテシステムと連動するシステムとする。

(3)対象情報は，全ての診療に関する情報である。

第２章　管理体制

（管理者，責任者の任命）

第３条　茨城医療センターに情報システム管理者（以下「システム管理者」という。）を置き，病院長をもってこれに充てる。

２　病院長は必要な場合，システム管理者を別に指名することができる。

３　情報システムを円滑に運用するため，情報システムに関する運用を担当する責任者（以下「運用責任者」という。）を置き，病院長が指名した情報システム室長をもってこれに充てる。

４　各部門の情報システムを円滑に運用するため，各部門に情報システム責任者（以下「部門責任者」という。）を置き，各部門の長をもってこれに充てる。

５　情報システムに関する取り扱い及び管理に関し必要な事項を審議するため，幹部会議のもとに茨城医療センター情報システム委員会（以下「情報委員会」という。）を置く。

６　情報委員会の運営については，別途定める規定による。

７　その他，この規程に関し必要な事項がある場合については，情報委員会の審議を経て，幹部会議がこれを定める。

（監査体制，監査責任者）

第４条　情報システムを円滑に運用するため，情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置く。

２　監査責任者は，幹部会議が委嘱する。

３　運用責任者は，監査責任者に毎年1回，情報システムの監査を実施させ，監査結果の報告を受け，問題点の指摘等がある場合には，直ちに必要な措置を講じなければならない。

４　監査の内容については，総合情報部会の審議を経て，幹部会議でこれを定める。

５　運用責任者は必要な場合，臨時の監査を監査責任者に命じなければならない。

（事故対策）

第５条　部門責任者は，緊急時及び災害時の連絡，復旧体制並びに回復手順を定め，非常時においても参照できるような媒体に保存し保管すること。

（教育・訓練など周知体制）

第６条　運用責任者は，情報システムの取扱いについてマニュアルを整備し，情報システムを利用しようとする者（以下「利用者」という。）に周知の上，常に利用可能な状態におくこと。

２　運用責任者は，情報システムの利用者に対し，定期的に情報システムの取扱い及びプライバシー保護に関する研修を行うこと。

第３章　管理者及び責任者，利用者の責務

（システム管理者及び運用責任者，部門責任者の責務）

第７条　情報システムを円滑に運営し，システム全体の管理状況を把握しなければならない。

２　不正利用者の報告を受けた場合，適切な処置を行わなければならない。

３　システムに用いる機器及びソフトウェアを導入するに当たって，システムの機能を確認し，これらの機能が「法令に保存義務が規程されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」に示される各項目に適合するよう留意すること。

４　第１９条に定める情報システムの機能要件に挙げられている機能が支障なく運用される環境を整備すること。

５　診療情報及び診療諸記録の安全性を確保し，常に利用可能な状態に置いておくこと。

６　利用者の登録を管理し，そのアクセス権限を管理し，不正な利用を防止すること。

７　操作マニュアルを整備し，利用者の教育を行うこと。

８　常時ウイルス等の不正ソフトウェアの混入を防ぐ適切な措置をとること。また，その対策の有効性・安全性の確認と維持を行うこと。

９　定期的にネットワークの利用履歴やネットワーク負荷等を検査し，通信環境の効率的な運用を維持するとともに，不正に利用された形跡がないかを確認すること。

（情報システム利用の申請及び承認等）

第８条　情報システムの利用者は，次の各号に掲げる方法により，利用の承認を得なければならない。

⑴利用者が所属する部門責任者（契約等により茨城医療センターの諸業務に当たっている者は，当該業務を所管する部門責任者）の同意を得て，所定の様式により運用責任者に利用申請を行うものとする。

⑵前号の申請があったときは，運用責任者は，利用目的及び資格等を審査し，適当と認めるときは，承認するものとする。

⑶前号の承認をしたときは，運用責任者は，認証番号及びパスワードを交付するものとする。

（利用者の責務）

第９条　利用者は，次の各号に掲げる責務を負う。

⑴情報システムの情報の参照や入力（以下「アクセス」という。）に際して，認証番号やパスワード等によって，システムに自身を認識させる。

⑵自身の認証番号やパスワードを管理し，これを他者に利用させない。

(3)正当な認証番号及びパスワード等の管理を行わないために生じた事故や障害に対しては，その利用者が責任を負う。
(4)情報システムへの情報入力に際して，確定操作（入力情報が正しい事を確認する操作）を行い，入力情報に対する責任を明示する。
(5)与えられたアクセス権限を越えた操作を行わない。
(6)患者等のプライバシーを侵害してはならない。
(7)法令上の守秘義務の有無に関わらず，アクセスにより知り得た情報を目的外に利用したり，漏らしてはならない。異動，退職等により職務を離れた場合においても同様である。
(8)離席する際は，窃視防止策を実施する（ログアウト等）。
(9)情報システムに蓄積された病院情報の維持に努めるとともに，運用責任者の許可なく情報システム環境を改変してはならない。
(10)他施設等からの新たな情報を情報システムに受け入れる場合は，運用責任者の指定する方式によるものとする。
(11)病院情報を個人媒体又は情報システム以外の情報システムにダウンロードする場合は，運用責任者の指定する方式によるものとする。
(12)システムの異常や不正アクセスを発見した場合，速やかに部門責任者に連絡し，その指示に従う。
(13)ウイルスに感染又はその恐れを発見した場合は，ネットワークから端末を切り離すとともに，部門責任者へ連絡し指示を仰ぎその指示に従う。

（利用者の変更等）
第１０条　利用者は，利用申請の内容に変更が生じたときは，その内容を速やかに運用責任者に届け出なければならない。

第４章一般管理における運用管理事項

（電子保存する情報の範囲）
第１１条　情報システムにて扱う情報の範囲
一 診療記録（カルテ）
二 オーダー情報・履歴
三 検体検査結果・病理検査結果
四 放射線画像

（情報保管場所への入退者の記録，管理について）
第１２条　個人情報が保管されている機器の設置場所および記録媒体の保存場所（以下，「サーバ室等」という。）への入退者は，名簿に記録を残すこと。
２　運用責任者の承認なしにサーバ室等に立ち入ってはならない。
３　運用責任者は，サーバ室等の出入り口は常時施錠管理し，所在表示の制限等の措置を講ずること。
４　運用責任者は，入退出の記録の内容について定期的にチェックを行い，問題があればシステム管理者に報告する。

（外部記憶装置・デジタルカメラ運用管理）
第１３条　システム管理者は、外部記憶装置の安全な運用、デジタルカメラ画像を電子カルテシステムに取込む場合、リスク分析を行い、安全に運用されるように別途規定を定める。

（情報システムへのアクセス制限，記録，点検等のアクセス管理）

第１４条　部門責任者は，利用者の職務や情報の機密度に応じたデータアクセスの範囲を定め，必要に応じてハードウェア，ソフトウェアの設定を行うものとする。

２　利用者が入力した情報について，確定操作を行った情報の記録及び更新日時を記録すること。

３　利用者が情報にアクセスした記録を保存し，これを追跡調査できるようにすること。

４　主治医は病院長の了承のもと、運用責任者に患者別アクセス制限の申請が行えること。

５　アクセスログは、特定の担当者以外アクセスできない仕組みとすること。

（他の情報システムの接続条件）

第１５条　情報システムに接続しようとする他の情報システムは，情報システムと同等以上の安全性を有するものとする。

２　情報システムネットワークを利用できる他の情報システムを制限・管理し，許可されていない情報機器の接続を制御する。

（情報システムの記録媒体の管理）

第１６条　情報システムの記録媒体は空調，入室管理が完備された安全な部屋で管理すること。

２　記録媒体の劣化を考慮し，情報の定期的なバックアップ作業を行うこと。

３　保管，バックアップの作業にあたる者は，手順に従い，その作業を記録し，部門責任者の承認を受けること。

（端末機等の管理）

第１７条　情報システムの端末機等は，主に一次利用（診療業務や病院管理を目的とする利用）のため，診察室，病棟，カンファレンスルーム，ミーティングルーム，その他運用責任者が適当と認めた場所に設置すること。利用者が診療事務処理，調査研究，教育等を目的とした個人部屋（個室）への設置は認めない。

２　前条の場所に設置された端末機等の情報保護と盗難等の事故防止のため，各部署に責任者（以下，「部署責任者」という。）を置き，適切な管理を行わなければならない。

３　部署責任者は，次の各号の職にある者，又は各部門の長をもって充てる。

(1)各外来診療室・・・・・・・・・診療科長

(2)各病棟・・・・・・・・・・・・病棟医長

(3)ミーティングルーム(医局) ・・・診療科長

(4)カンファレンスルーム・・・・・病棟医長

(5)各中央部門・・・・・・・・・・部門長

(6)各事務部門・・・・・・・・・・課長，室長等

（個人情報を含む記録媒体の廃棄）

第１８条　個人情報を記した記録媒体の廃棄に当たっては，安全かつ確実に行われる事を，運用責任者が作業前後に確認し，結果を記録に残すこと。

２　端末機等やサーバといった茨城医療センター内での廃棄が難しく，廃棄を外部業者に委託する場合，契約書を締結し，確実に廃棄された事を証明すること。

３　ＣＤ，フロッピーディスク等のメディアの場合，メディアシュレッダー等を用いて物理的に破壊

すること。

（リスクに対する予防，発生時の対応）

第１９条　運用責任者は，業務上において情報漏洩，システム停止などのリスクが予想されるものに対し，運用規程の見直しを行うこと。また，事故発生に対しては，速やかに運用責任者に報告することを周知すること。

（利用の承認の取消し等）

第２０条　利用者がこの規程に違反し情報システムの運用に重大な支障を生じさせたとき，又はその恐れがあるときは，運用責任者は，その者の利用を停止又は利用の承認を取消すことができるものとする。

（システム機能要件）

第２１条　情報システムは，次の機能を備えるものとする。

イ　情報にアクセスしようとする者の識別と認証機能

ロ　情報の機密度に応じた利用者のアクセス権の設定と，不正アクセスを排除する機能

ハ　利用者が入力した情報について，操作確定が行えることができる機能

ニ　利用者が確定操作を行った情報を正確に保存する機能

ホ　利用者が確定操作を行った情報の記録及びその更新日時並びに実施者を，これらの情報に関連付けて保存する機能

ヘ　管理上または診療上の必要がある場合，記録されている情報を速やかに出力する機能

ト　複数の機器や媒体に記録されている情報の所在を一元管理できる機能

チ　情報の利用範囲，更新履歴，機密度等に応じた管理区分を設定できる機能

リ　利用者が情報にアクセスした記録を保存し，これを追跡捜査できる機能

ヌ　記録された情報の複製（バックアップ）を作成する機能

（損害賠償）

第２２条　利用者は，故意又は重大な過失により情報システムを損傷したときは，その損害に相当する費用を賠償しなければならない。

（守秘義務の違反に対する賠償責任）

第２３条　利用者が，不当に情報を入手し，又は漏洩した場合は，当該事件において損害を受けた当事者に対してその損害に相当する賠償の責任を負うものとする。

（情報の二次利用）

第２４条　二次利用（診療業務や病院管理を目的としない利用）においては，個人のプライバシーが侵害されないようにしなければならない。

２　次に該当するとき以外は，収集した情報の目的以外の利用又は外部への提出をしてはならない。

イ　法令の規程に基づくとき。

ロ　個人の生命の保護のため，緊急かつやむを得ないと認められたとき。

ハ　個人の利益のため，他の医療機関等へ診療情報を提出する必要があるときで，患者本人や代理人が同意・承諾したとき。

ニ　その他，患者本人や代理人が同意・承諾したとき。
ホ　東京医科大学茨城医療センター個人情報保護規程（以下「センター個人情報保護規程」という。）の条件を充たしたとき。
ヘ　関連のある日本の法律や都・市の条例等を遵守しなければならないとき。

第５章業務委託の安全管理措置

（委託契約における安全管理に関する条項）
第２５条　業務を茨城医療センター外の所属者に委託する場合，守秘事項を含む業務委託契約を結ぶこととする。
２　契約の署名者は病院長とする。
３　各担当者は，委託作業内容が個人情報保護の観点から適正にかつ安全に行われていることを確認すること（委託先が，許可無く個人情報を含むデータを組織外に持ち出すことは禁止する）。

（システム改造及び保守に関するデータ参照）
第２６条　運用責任者は，開発・保守業者における作業に関し，その作業者，作業内容につき報告を求め，それらが適切であることを確認すること。
２　必要と認めた場合には，適時監査を行うこと。

（再委託の場合の安全管理措置事項）
第２７条　業務委託の契約書には、再委託での安全管理に関する事項を含む。

（情報の外部保管における運用管理）
第２８条　別に「病院情報の外部保管における運用管理規程」を運用開始する場合は定める。

第６章 情報の持ち出しについて

（持ち出し可能となる情報）
第２９条 システム管理者は、情報の持ち出しに関しリスク分析を行い、持ち出し可能となる情報を定め、それ以外の情報の持ち出しを禁止する。
２　持ち出し可能となる情報は、東京医科大学の各病院における医療情報の管理に関する規程第７条外部への持出し」に定める安全対策を遵守すること。

（持ち出した情報の運用管理）
第３０条　情報を持ち出す場合は、所属、氏名、連絡先、持ち出す情報の内容、格納する媒体、持ち出す目的を、別途定める書式でシステム管理者に届け出て、承認を得る。
２ システム管理者は、届け出のあった内容について保管する。その内容を定期的に確認する。

（持ち出した情報への安全管理措置）
第３１条　持ち出す情報について記憶媒体、ファイルに起動時のパスワードを設定すること。そのパスワードは推測されやすいものは避け、定期的に変更する。
（盗難、紛失時の対応策）
第３２条　持ち出した情報の格納された媒体の盗難、紛失時には、直ちにシステム管理者に届け出る。

第７章　外部機関とのネットワーク接続について（リモートメンテナンス）

（技術・運用面での安全管理措置）

第３３条　システム管理者は、外部機関とネットワーク接続する場合のリスク分析を行い、安全に運用されるように、技術面、運用面での対策を講じること。

２　技術的対策が適切に実施されているか定期的に確認すること。

３　定期的にアクセスログの提供を受け、作業日時、作業内容、作業者を確認すること。

（情報処理業者・外部機関との責任分界点について）

第３４条　外部機関とのネットワーク接続を行う場合、通信業者、運用委託業者との間で、責任分界点や責任の所在を契約書等で明確にすること。

２　上記契約状態が適切に維持管理されているか、定期的に確認すること。

（外部接続の関わる運用管理について）

第３５条　外部から接続を許容する回線については別途定める「東京医科大学の各病院における医療情報の管理に関する規程」に従ったものに限定すること。その機器が許可された際の状態を保持しているか定期的に確認すること。

第８章 災害等の非常時の対策

（事業継続計画（BCP）における情報システムの運用）

第３６条　災害、サイバー攻撃等により一部医療行為の停止等、医療サービスの提供体制に支障が発生する非常時の場合、別途定める事業継続計画（BCP）に従って運用を行う。

２　どのような状態を非常時と見なすかについては、BCP の定める基準、手順に従って運用責任者が判断する。

（報告先と内容一覧）

第３７条　災害、サイバー攻撃等により一部医療行為の停止等、医療サービス提供体制に支障が発生した場合、BCP に定める連絡先に連絡する。

第９章 教育と訓練

（マニュアルの整備）

第３８条 システム管理者は、情報システムの取り扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態にする。

（プライバシー保護、セキュリティー意識向上に関する研修）

第３９条 システム管理者は、利用者に対し、情報システムの取り扱い及びプライバシー保護に関する研修を行う。

（利用者に対する人的安全管理措置）

第４０条 情報システムの利用者は、在職中のみならず、退職後においても情報システムを利用した上で知った個人情報に関する守秘義務を負うものとする。

第１０章　監査

（監査体制と監査責任者の任命）

第４１条　情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置く。

２ 監査責任者の責務は別に定める。

３ 監査責任者は学校法人東京医科大学総合情報部部長（以下「総合情報部長」という。）をもってこれに充てる。

４　システム管理者は、監査責任者に毎年１回の、情報システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じる。

５　監査の内容については、法人情報システム委員会の審議を経て、総合情報部長がこれを定める。

６　システム管理者は必要な場合、臨時の監査を監査責任者に命じ、監査を実施させる。

第１１章　構内無線LAN

（無線ＬＡＮに関する事項）

第４２条　無線LANの利用は「東京医科大学の各病院における医療情報の管理に関する規程第６条（８）無線LANの利用」に定める技術的安全対策を遵守すること。

２　無線LANアクセスポイントの設定状態を適宜確認し，無線機器による電波干渉を防止すること。

３　通信を傍受されないよう，親機と子機（パソコン・携帯端末等）との通信を暗号化すること。

４　利用者以外に無線ＬＡＮの利用を特定されないよう，ユーザID，パスワード，電子証明書などを利用したクライアント認証によるアクセス制御を行うこと。

第１２章　電子保存３原則の確保

（電磁的記録に関する事項）

第４３条　電子媒体に保存の際の要件として，次項の３条件を充たすこと。

１　真正性の確保

イ　正当な人が記録し確認された情報に関し，第三者から見て作成の責任と所在が明確であり，かつ故意又は過失による虚偽入力，書換え，消去及び混同が防止されていること。

ロ　確定操作された情報は，別途で定める保存期間内は，履歴を残さないで改変や削除ができないこと。

２　見読性の確保

イ　情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。

ロ　電子保存に用いる機器及びソフトウェアを導入するに当たって，保存義務のある情報として電子保存された情報毎に見読用機器を常に利用可能な状態に置いておくこと。

ハ　応答時間の大幅な遅延が無いようにシステムの維持に努めること。

３　保存性の確保

イ　記録された情報が，法令などで定められた期間にわたって，真正性を保ち，見読可能にできる状態で保存されていること。

ロ　電子保存システムで使用されるソフトウェアを使用の前に審査し，情報の安全性に支障がないことを確認すること。

ハ　記憶媒体は，記録された情報が保護されるよう，別の媒体にも補助的に記録すること。

ニ　品質の劣化が予想される記録電子媒体は，障害を防ぐため，情報の保管期間，記録媒体の種別により，定めた期間内に複製を作成すること。

ホ　保存するデータを読み取れることの確認を定期的に実施すること。

へ　情報機器やソフトウェアの変更に当たっては，データ移行のための業務計画を作成すること。

ト　証跡記録の信頼性を確保するために、病院情報システムの時刻を、タイムサーバを用いて標準時刻に同期すること。

第１３章　その他

（雑則）

第４４条　この規程に定めるもののほか，情報システムに関し必要な事項は，情報委員会の議を経て，幹部会議が別に定めるものとする。

附則

この規程は，平成２４年８月２７日から施行する。

附則

この規程は、平成２７年７月２日から施行する。

附則

この規程は、平成２８年１１月２８日から施行する。

東京医科大学茨城医療センター外部記憶装置・デジタルカメラ運用管理細則

（目的）

第１条

本細則は、東京医科大学 茨城医療センター 病院情報システムの安全管理に関する運用管理規定（以下「運用管理規定」という。）に基づき、使用する外部記憶装置の安全な運用確保、デジタルカメラの識別・管理及び撮影した静止画の電子保存システムへの適正な保存について安全な運用の確保を目的とする。

（外部記憶装置の定義）

第２条

運用管理規定第 13 条で定める安全な運用に基づき、病院情報システムに外部記憶装置を接続する機器は必要最小限とする。この細則における外部記憶装置用語の定義は各号に定めるとおりとする。

(1) USB フラッシュメモリ、CD、フロッピー、外付けハードディスク、DVD ドライブなど、可搬型記憶装置、記憶媒体、及び外部接続型の記憶媒体読書き装置全般。ただし、カードリーダ等の専用機器、マウス、キーボードなどの記憶機能を持たない機器はこれに該当しない。

(2) 外部記憶装置の利用者は、電子カルテ端末と接続して使用する外部記憶装置一台毎に、別に定める「病院情報システム 機器接続 申請書（記憶媒体装置）」を作成し、情報をシステム管理者に提出し承認を得ること。

(3) パスワードロック機能付き等の外部記憶装置を使用すること。

(4) 外部記憶装置の盗難、紛失による情報漏えい、外部記憶装置を介したコンピュータウイルスの感染拡大が生じないように適正に使用すること。

(5) システム管理者から許可されていない端末と外部記憶装置を接続しないこと。システム管理者により許可された目的以外で端末と外部記憶装置を接続しないこと。

（デジタルカメラの識別と認証）

第３条

運用管理規定第 13 条で定める安全な運用に基づき、病院情報システムに接続可能なデジタルカメラは以下の各号の条件を満たすこととする。

(1) 申請可能なデジタルカメラは静止画・動画の撮影を主目的として製造された光学機器を指し、これらを付属機能として有する携帯電話等は含まない。

(2) 個体製造番号などを用いたデジタルカメラ一台毎の認証が可能なこと。

(3) デジタルカメラの利用者は、電子カルテ端末と接続して使用するデジタルカメラ一台毎に、別に定める「病院情報システム（HIS）デジタルカメラ接続申請書」を作成し、「デジタルカメラ　使用条件の承諾」に記載された接続申請手続きに沿って、機器の識別と認証に関する情報をシステム管理者に提出し承認を得ること。
(4) 申請するデジタルカメラ毎に病院職員からなる管理者をおくこと。
(5) システム管理者は、直ちに「病院情報システム（HIS）デジタルカメラ接続申請書」の内容と該当するデジタルカメラが安全に病院情報ネットワークと接続できるか確認すること。

（デジタルカメラの運用）
第４条
デジタルカメラの接続申請者は以下の各号に定める使用条件に沿って運用を行うことを承諾すること。
(1) 撮影画像（静止画）を電子保存システムに取り込むに当たり、「デジタルカメラ　使用条件の承諾」定められた手順にて運用すること。
(2) 「デジタルカメラ　使用条件の承諾」に記載されている、セキュリティ対策、ウイルス感染時の対応、保管する画像の形式や１回あたりの保管枚数を遵守すること。
(3) デジタルカメラの設定日時は、始業時に日時設定が正しいか確認し、間違っている時は修正すること。

（不正プログラムへの対応）
第５条
電子カルテ端末とデジタルカメラとの接続における不正プログラムへの対策として、デジタルカメラ内に入れる記録カード（SD カードなど）の事前準備を以下の各号に定める。
また、記録カードは他の用途には使用しないこと。
(1) ウイルスチェックを実施すること。
(2) 初期化(フォーマット処理)を実施すること。

（記録の確定）
第６条
デジタルカメラの撮影画像の電子保存システムへの保管手順は、以下の各号に定める。
(1) 電子カルテ端末にて患者選択を行い、指定された画像取り込み画面を開くこと。
(2) デジタルカメラと電子カルテ端末を USB 接続して、必要な静止画を選択して取込むこと。

2　画像形式、解像度と電子カルテシステムへの1回当たりの保管枚数については以下の各号に定める。

(1) 画像形式はJPEG形式の静止画像とすること。

(2) 解像度は1枚当たり2MB(2304×1728ピクセル前後：300万画素相当)とすること。

(3) 電子保存システムへの1回当たりの保管枚数は電子カルテの記事記載に対応する1連の撮影につき5枚以下とすること。

(不正プログラム検知時の対応)

第7条

不正プログラム検知時の対応及び報告については以下の各号に定める。

(1) 直ちに電子カルテ端末との接続を切断すること。

(2) 該当するデジタルカメラのウイルスチェックを実施すること。

(3) 上記(1)、(2)の手順を実施後、情報システム室へ対応状況を報告すること。

(接続要件の変更)

第8条

接続申請書に記載されたデジタルカメラの要件変更が生じた場合は、速やかに要件変更に沿った接続申請書の再提出を行うこと。

(接続有効期間)

第9条

機器廃棄漏れを防ぐため、有効期間は申請日より 4 年間とする。但し継続使用は再申請にて対応することとする。

(申請者の責務)

第１０条

申請者は、「デジタルカメラ　使用条件の承諾」に記載される項目についてデジタルカメラ利用者へ周知徹底を行うこととする。

附則

本細則の改定については情報システム委員会の承認を要する。

本細則は平成29年1月20日より施行する。

以上