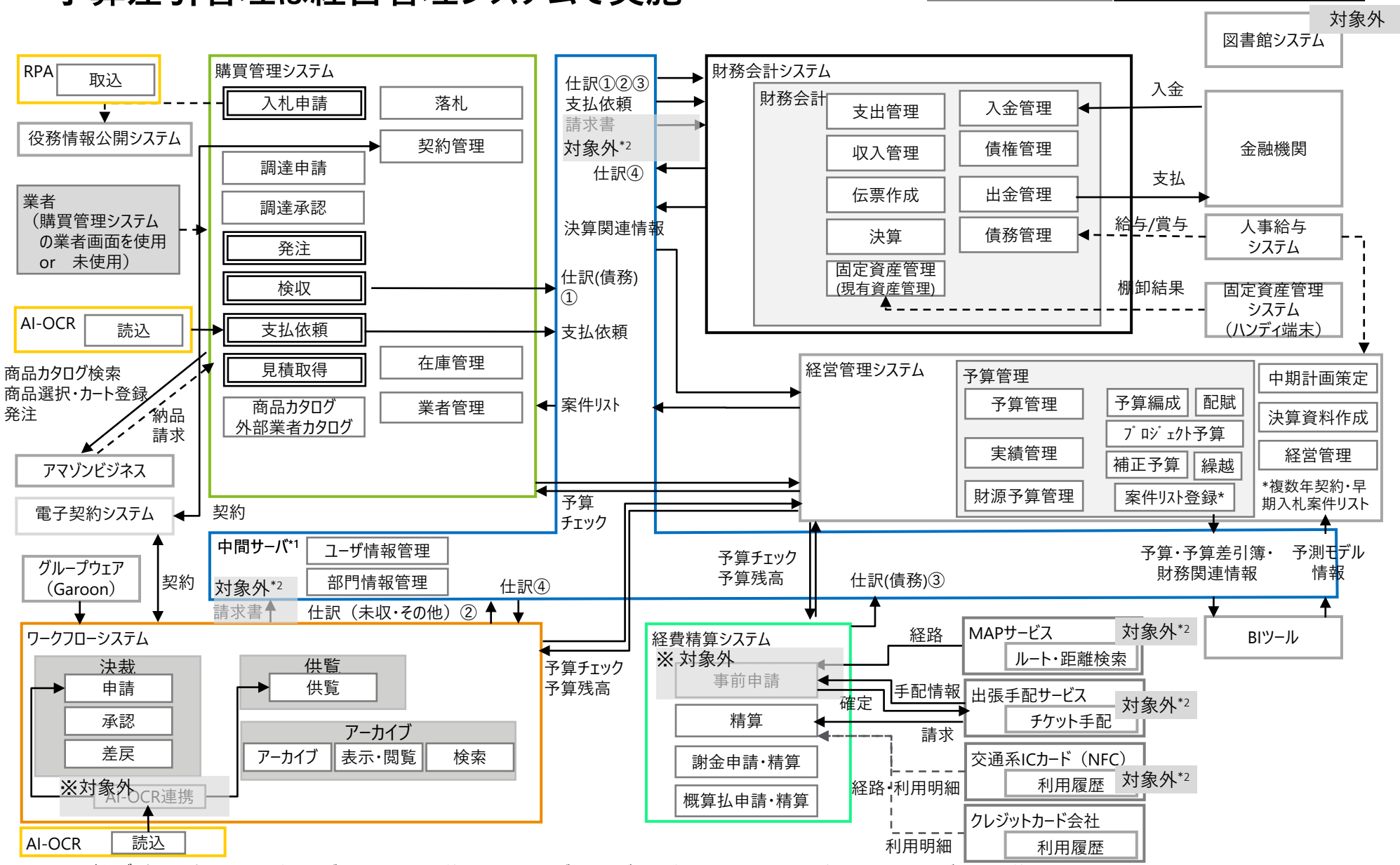
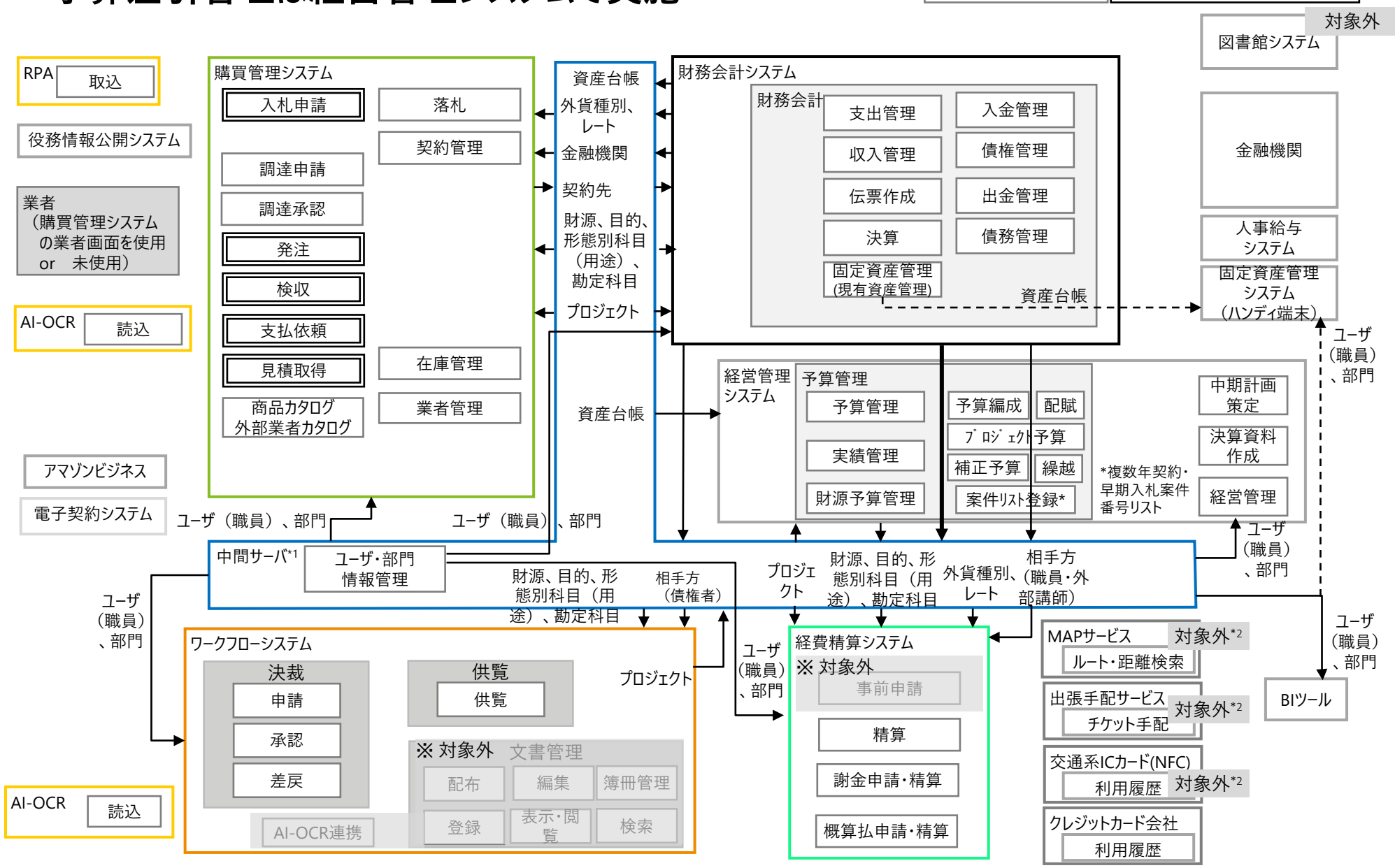
別紙１ システム全体図（トランザクションデータ）
＜予算差引管理は経営管理システムで実施＞



0

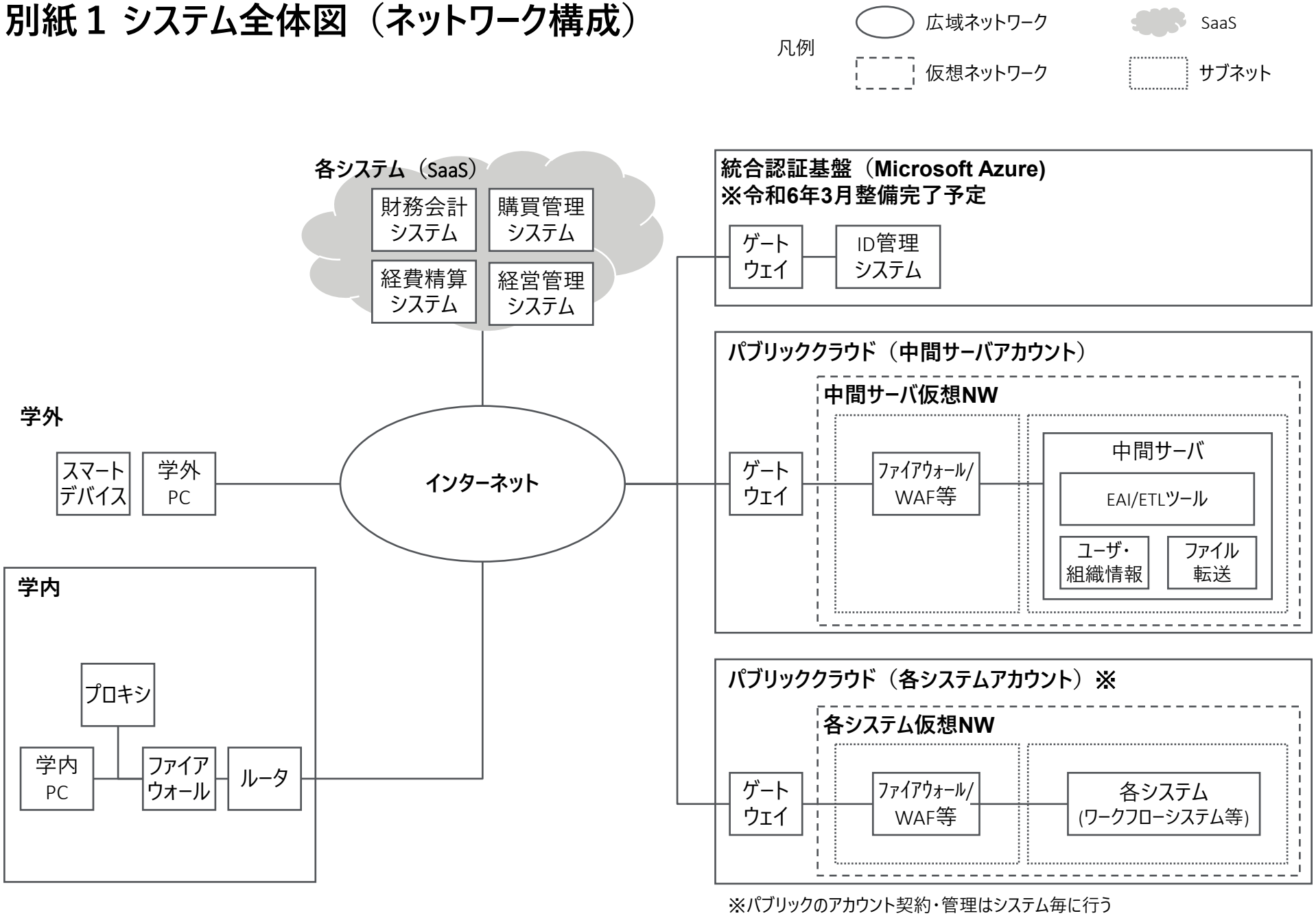
読込データ　*1）中間サーバはユーザ情報/部門情報管理の他、トランザクションデータの各システム間連携の仲介/制御を行う。ただし、経営管理システムへはセキュリティ確保のために通信を経由するのみで変換作業等は行わない。　*2）現時点では対象外だが、将来的に連携する可能性あり。

別紙１ システム全体図（マスタデータ）
＜予算差引管理は経営管理システムで実施＞



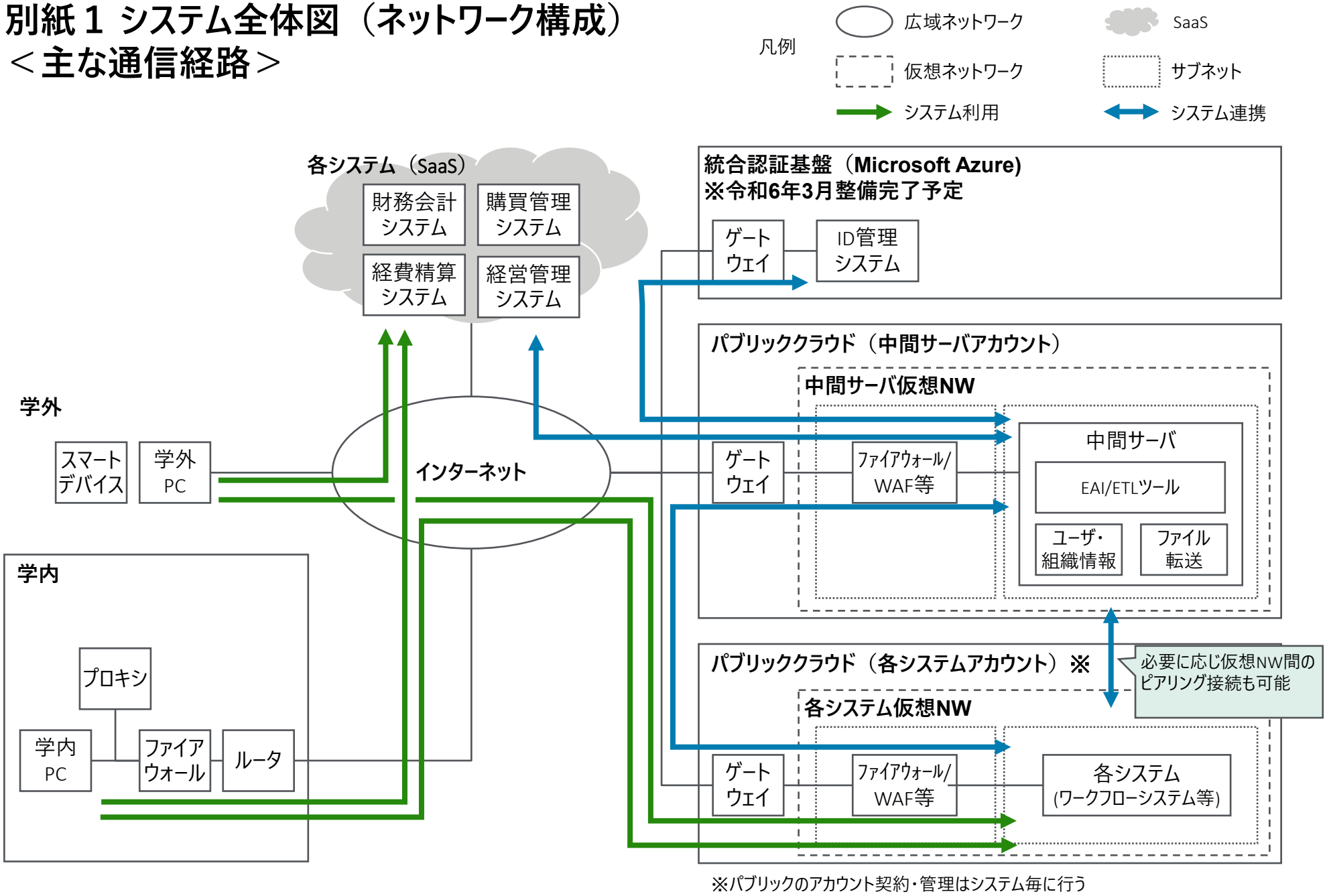
*1）中間サーバはユーザ情報/部門情報管理の他、各システム間連携の仲介/制御を行う　*2）現時点では対象外だが、将来的に連携する可能性あり

別紙１ システム全体図（ネットワーク構成）



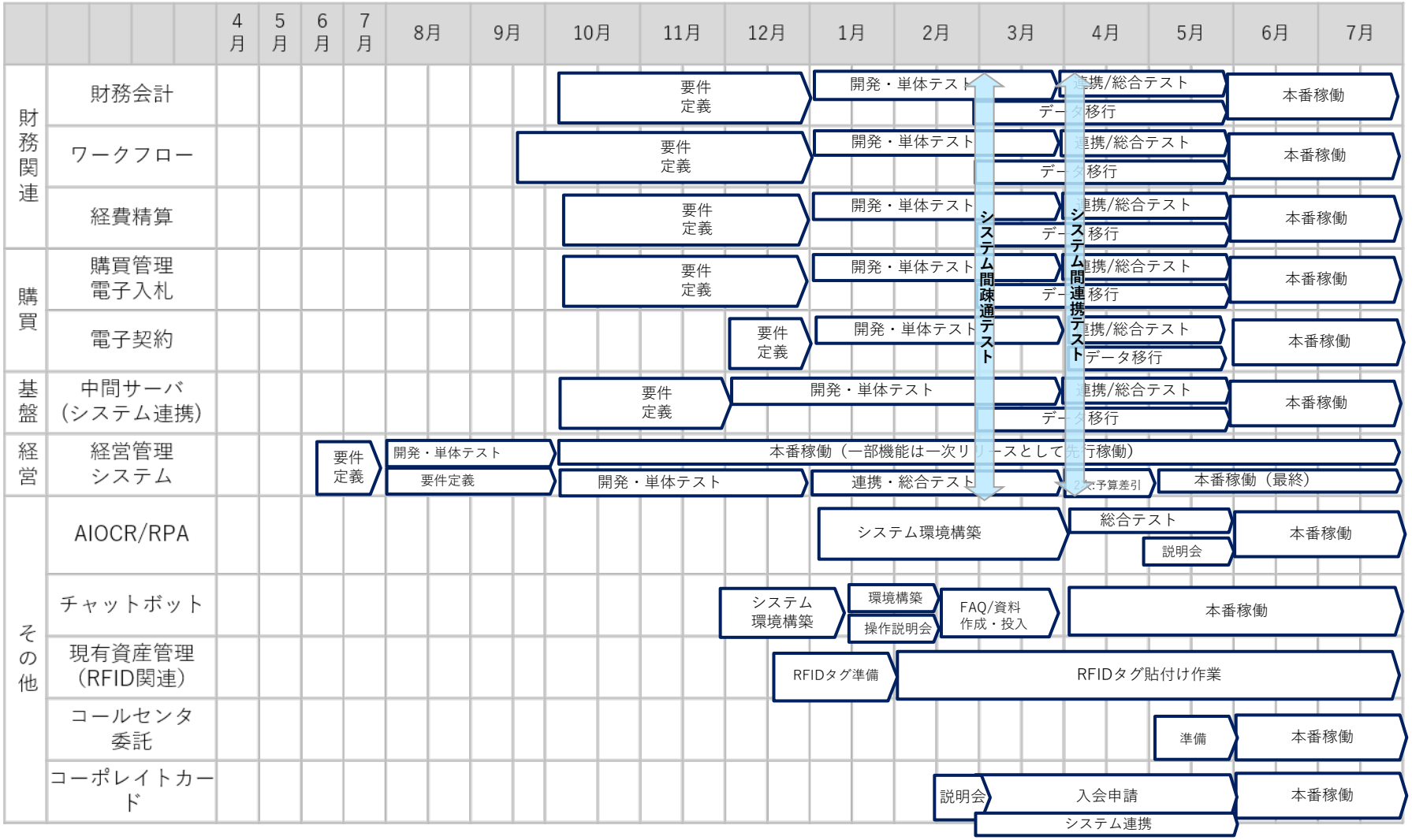
※パブリックのアカウント契約・管理はシステム毎に行う

別紙１ システム全体図（ネットワーク構成）
＜主な通信経路＞



※パブリックのアカウント契約・管理はシステム毎に行う

別紙２ プロジェクトマスタスケジュール



公立大学法人和歌山県立医科大学個人情報保護安全管理措置要綱

制　　定　平成 28 年 4 月 1 日
最終改正　平成 30 年 3 月 15 日

第 1 章　総則

第１　趣旨

この要綱は、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）、和歌山県個人情報保護条例（平成 14 年和歌山県条例第 66 号。以下「条例」という。）及び和歌山県個人情報の安全管理に関する基本的な考え方に基づき、公立大学法人和歌山県立医科大学（以下「法人」という。）の事務を執行するうえで個人情報の適正な取扱いの確保を図ることを目的として必要な事項を定めるものである。

第２　個人情報の管理体制

１　事務局総務課長の責務

事務局総務課長は、個人情報の保護に関する事務が円滑に行われるよう当該事務を総括し、必要な指導等を行うとともに、個人情報の管理の改善に努めるものとする。

２　個人情報保護責任者の設置

(1) 個人情報の保護に関する事務を円滑に実施するため、事務局各課室（危機対策室及び地域医療支援センターを含む。以下同じ。）に個人情報保護責任者を置く。

(2) 個人情報保護責任者は、次の事務を行うものとする。

ア　個人情報の適正な取扱いについての指導、監督及び教育研修に関すること。

イ　個人情報を取り扱う事務の目的や性質、利用形態等を踏まえ、その取扱手続を明確にすること。

ウ　個人情報を複数の所属で取り扱う場合の各所属の任務分担及び責任の明確化を行うこと。

エ　個人情報の漏えい、滅失又は毀損等事案の発生、又はそれらの兆候を把握した場合の対応に関すること。

オ　開示請求者、訂正請求者、利用停止請求者及び実施機関非識別加工情報の提案者並びに個人情報の取扱いに関する苦情相談者に対する対応についての指導に関すること。

カ　事務局総務課長及び関係各課室との連絡及び調整に関すること。

キ　その他個人情報の保護に関する事務の処理の改善に関し必要なこと。

(3) 個人情報保護責任者は、公立大学法人和歌山県立医科大学文書処理規程（平成 19 年 3 月 19 日和医大規程第 13 号。以下「文書処理規程」という。）第５条第２項の規定により定められた文書管理責任者をもって充てる。

3　事務局各課室で行う事務

事務局各課室においては、次の事務を行うものとする。

(1) 個人情報ファイル簿の作成等に関すること。

(2) 個人情報取扱事務における保有個人情報の適切な管理のために必要な措置を講ずること。

(3) 保有個人情報の特定等に必要な情報の提供

(4) 保有個人情報開示請求書（以下「開示請求書」という。）、保有個人情報訂正請求書（以下「訂正請求書」という。）及び保有個人情報利用停止請求書（以下「利用停止請求書」という。）の収受等に関すること。

(5) 当該請求に係る保有個人情報の開示決定等、訂正決定等及び利用停止決定等（以下「開示・訂正・利用停止決定等」という。）に関すること。

(6) 当該決定に係る開示、訂正及び利用停止の実施に関すること。

(7) 保有個人情報の開示申込書の受理に関すること。

(8) 保有個人情報が記録された文書の写しの作成に係る費用徴収に関すること。

(9) 口頭による開示請求に関すること。

(10) 実施機関非識別加工情報をその用に供して行う事業に関する提案書及び作成された実施機関非識別加工情報をその用に供して行う事業に関する提案書の収受等に関すること。

(11) 実施機関非識別加工情報の提案に係る審査等に関すること。

(12) 実施機関非識別加工情報の利用に関する契約の締結の申込書の受付等に関すること。

(13) 実施機関非識別加工情報の利用に関する契約に関すること。

(14) 実施機関非識別加工情報の利用に関する手数料の徴収等に関すること。

(15) 実施機関非識別加工情報の作成及び提供に関すること。

(16) 当該各課室に係る個人情報の取扱いに関する苦情の申出の受付及び処理に関すること。

(17) 当該各課室が所管する事業者の個人情報の取扱いについての苦情相談の受付及び処理のあっせん等に関すること。

4　個人情報窓口の設置

個人情報の保護に関する相談及び案内、保有個人情報に対する開示請求、訂正請求及び利用停止請求の受付、実施機関非識別加工情報をその用に供して行う事業に関する提案書及び作成された実施機関非識別加工情報をその用に供して行う事業に関する提案書の受付その他個人情報の保護に関する事務を行うため、個人情報窓口を事務局総務課に設置する。

5　個人情報窓口で行う事務

個人情報窓口においては、次の事務を行うものとする。

(1) 相談・案内に関すること。

(2) 個人情報ファイル簿の備付け及び公表に関すること。
(3) 法人が保有する全ての個人情報に対する開示請求書、訂正請求書及び利用停止請求書の受付等に関すること。
(4) 開示・訂正・利用停止決定等又は不作為に対する審査請求書の受付等に関すること。
(5) 開示・訂正・利用停止決定等又は不作為に対する審査請求に係る審議会への諮問及び裁決に関すること。
(6) 実施機関非識別加工情報をその用に供して行う事業に関する提案書及び作成された実施機関非識別加工情報をその用に供して行う事業に関する提案書の受付等に関すること。
(7) 条例第６条第２項第６号、第３項第５号、第４項第２号、第 12 条第７号、第 14 条第２項第３号、第 45 条の 10 第２項又は第 45 条の 15 第２項において審議会に意見を聴くこととされている場合の審議会への諮問に関すること。
(8) 法人における個人情報の取扱いに関する苦情の申出の受付等に関すること。

第２章　個人情報に関する安全管理措置等

第１　個人情報の取扱い

個人情報（実施機関非識別加工情報及び削除情報に該当するものを除く。この章において同じ。）の取扱いは、次の１から６に掲げる事項に留意して行うものとする。

１　関係法令等の遵守

(1) 個人情報が記録された文書の取扱いについては、文書処理規程を遵守すること。

また、個人情報を含む情報資産（和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針第１章第２節第４項に規定する情報資産をいう。）は、和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ対策要綱（以下「情報セキュリティ対策要綱」という。）を遵守すること。

(2) 特定個人情報の取扱い

ア　特定個人情報の取扱いは、番号法及び特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体編）（平成 26 年特定個人情報保護委員会告示第 6 号）等を遵守すること。

イ　特定個人情報保護評価に関する規則（平成 26 年特定個人情報保護委員会規則第 1 号）に基づく特定個人情報保護評価を実施した事務においては、その評価書に記載した内容を確実に実行すること。

ウ　個人番号関係事務実施者（番号法第２条第 13 項に規定する個人番号関係事務実施者をいう。）は、当該関係事務に係る個人番号利用事務実施者（番号法第２条第 12 項に規定する個人番号利用事務実施者をいう。）の指示に従うこと。

２　収集方法

(1) 個人情報は、個人情報取扱事務の目的を達成するために必要な範囲内で、適法かつ適正な方法により収集すること。

(2) 個人情報は、原則として、本人に対し個人情報取扱事務の目的を明示し、本人から直接収集すること。ただし、条例第６条第２項又は第３項の各号に該当する場合はこの限りではない。

(3) 特定個人情報の取扱い

ア　特定個人情報は、番号法第 20 条に基づき、同法第 19 条各号のいずれかに該当する場合を除き収集してはならない。

イ　個人番号は、個人番号利用事務等を処理するために必要があるときに収集すること。

ウ　個人番号を収集するときは、次に掲げる本人確認の措置を講じること。

(ｱ)　本人から個人番号を収集する場合

個人番号カード、通知カード、個人番号等が記載された住民票の写し等により番号確認を行うとともに、個人番号カード、運転免許証、旅券、在留カード又は特別永住者証明書等により身元確認を行うこと。

(ｲ)　本人の代理人から個人番号を収集する場合

当該代理人が法定代理人であるときは戸籍謄本等、任意代理人であるときは委任状等により代理権の確認を行い、当該代理人の個人番号カード、運転免許証、旅券、在留カード又は特別永住者証明書等により身元確認を行うとともに、本人の個人番号カードの写し、通知カードの写し、個人番号等が記載された住民票の写し等により番号確認を行うこと。

(ｳ)　(ｱ)及び(ｲ)における確認に際して、確認書類の写しを取得する場合は、保管や廃棄等に当たって安全管理の措置を適切に講ずる必要があることを前提に収集すること。

３　利用・提供方法

(1) 利用について

ア　個人情報（特定個人情報を除く。）は、個人情報取扱事務の目的以外の目的のために利用しないこと。ただし、条例第 12 条各号に該当する場合はこの限りではない。

イ　個人情報は、業務上必要とする者以外の目に触れないよう、個人情報を取り扱う事務を実施する区域を明確にし、座席配置の工夫、端末装置等の設置場所及びディスプレイの向きに注意する等の物理的な措置を講ずること。

ウ　個人情報の利用に当たって、離席時等には、机上の整理による個人情報の保護やスクリーンセーバーの作動、ログオフ又はシャットダウンによるパソコン画面上にある個人情報の保護等の適切な措置を講ずること。

エ　個人情報を印刷する際には、印刷機へ印刷要求した後、印刷に立ち会い、出力された印刷物は直ちに回収し、印刷機上に放置しないこと。

オ　個人情報が記録された文書は、学外に持ち出してはならない。ただし、特に必要がある場合は、あらかじめ当該文書を所管する事務局各課室の長（以下「課室長」という。）の承認を受けた上で、封かん、目隠しシールの貼付、施錠できる搬送容器の使用等の措置を講じ、持ち出した文書は常時携帯するなど管理下におき、放置しないこと。

カ　個人情報をＵＳＢメモリ等の記憶媒体に記録してはならない。ただし、特に必要がある場合は、情報セキュリティ管理者（情報セキュリティ対策要綱第５条に規定する情報セキュリティ管理者をいう。）の承認を得て、所属が配備した記憶媒体を使用し、個人が所有する記憶媒体を使用してはならない。

キ　個人情報が記録された記憶媒体は、原則として携行しないこと。ただし、特に必要があり携行する場合は、事前に情報セキュリティ管理者の許可を受け、携行した当該記憶媒体は常時携帯するなど管理下におき、放置しないこと。

ク　特定個人情報の取扱い

特定個人情報を取り扱う事務の目的以外の目的のために特定個人情報を利用しないこと。本人の同意を得ていても、特定個人情報を取り扱う事務の目的以外の目的のために利用してはならない。ただし、条例第 12 条の２第２項にある人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意があり、又は本人の同意を得ることが困難であるときはこの限りではない。

(2) 提供について

ア　個人情報（特定個人情報を除く。）は、個人情報取扱事務の目的以外の目的のために外部に提供しないこと。ただし、条例第 12 条各号に該当する場合はこの限りではない。

イ　特定個人情報の取扱い

特定個人情報は、条例第 12 条の 2 第 3 項に基づき、番号法第 19 条各号のいずれかに該当する場合を除き提供してはならない。

(3) 利用及び提供について

個人情報を学内に配布する等の利用する場合、及び、学外へ提供する場合は、封かんの上、配布先等に持参する等により直接手渡すこと。また、電磁的記録である個人情報については、電子的な伝送等により配布等しないこと。ただし、特に必要がある場合は、次に掲げる配布等の方法によること。

ア　郵送等により個人情報を配布等するときは、宛先に間違いがないか確認し、発信課室の名称を明記した上で、二重封かん等により外部から内容物を確認できないような体裁により郵送等を行うこと。

イ　ファクシミリの送信により個人情報を配布等するときは、業務上必要となる者以外の者に見られないよう、受信者が直ちにファクシミリ等受信文書を回収できる状態にあることを確認の上、送信すること。

ウ　電磁的記録である個人情報の配布等を電子的な伝送等により行うときは、情報

管理者（情報セキュリティ対策要綱第６条に規定する情報管理者をいう。）の許可を受け、原則として、当該電磁的記録を暗号化した上で伝送すること。

４　保管方法

(1) 個人情報は、保管する場所を定めること。

(2) 個人情報の保管場所は、業務上必要とする者以外の目に触れないよう取り扱うことができる場所とし、必要があると認めるときは、耐火金庫への保管、施錠等を行うこと。

(3) 個人情報を取り扱う執務室等を使用しないときは施錠すること。

(4) パソコンのハードディスクに個人情報を記憶し、保存するときは、盗難防止のための施錠等による物理的保護管理措置がなされ、かつ、起動パスワード等のセキュリティ設定がなされたパソコンを用いること。

５　廃棄方法

(1) 保存期間が経過した個人情報は確実かつ速やかに廃棄し、又は消去すること。

(2) 個人情報が文書、図画、写真及びフィルムであるときは、焼却、シュレッダーによる裁断等、判読不可能な状態にすること。

(3) 電磁的記録である個人情報は、消去ツールの使用その他の方法により完全に廃棄又は消去すること。

(4) 特定個人情報の取扱い

ア　特定個人情報が記載された書類等は、焼却又は溶解等の個人番号を復元できない手段により廃棄すること。

イ　特定個人情報が記録された機器及び記憶媒体等は、消去ツールの使用又は物理的な破壊等の個人番号を復元できない手段により廃棄又は消去すること。

ウ　特定個人情報を廃棄又は消去した場合には、廃棄又は消去した記録を保存し、記録の内容に個人番号自体は含めないこと。

エ　特定個人情報を廃棄又は消去する作業を委託する場合には、委託先が確実に廃棄又は消去したことについて、証明書等により確認すること。

６　取扱状況等の明確化

(1) 個人情報ファイル簿の作成等

ア　個人情報ファイル簿の作成及び公表

条例第 15 条に規定する個人情報ファイル簿の作成及び公表については、遺漏なきよう取り扱うこと。

イ　個人情報ファイルの明確化

個人情報ファイル簿は、県民等が事務局各課室における個人情報ファイルを確認できるものであるため、事務局各課室は、個人情報ファイルについて、その名称、目的、個人情報ファイルの対象者の範囲、記録項目、収集方法等を明確に記載すること。

(2) 文書管理簿の作成等

個人情報が記録された文書は、文書処理規程に基づき文書管理簿を作成すること。また、当該個人情報が特定個人情報である場合は、文書管理簿の備考欄にその旨を明示すること。

(3) 取扱状況の記録

個人情報の秘匿性等その内容に応じて、当該個人情報の利用及び提供等については、決裁等を得るものとし、当該決裁等は、文書処理規程に基づき保存すること。

なお、決裁等により難い場合は、台帳等を整備し、当該個人情報の利用及び保管等の取扱いの状況について記録すること。

(4) 個人情報取扱事務の事務担当者の明確化

個人情報取扱事務については、事務局各課室において事務分担を明確にすること。

(5) 情報システム等における取扱い

ア　情報提供等の記録

特定個人情報を情報提供ネットワークシステム（番号法第２条第 14 項に規定する情報提供ネットワークシステムをいう。）を利用して提供する場合は、番号法第 23 条第１項及び第２項（これらの規定を番号法第 26 条において準用する場合を含む。）に基づき情報提供等の記録を記録及び保存すること。

イ　バックアップ及びログの保存

情報システムにおいて特定個人情報を取り扱う場合は、定期的にバックアップを実施するとともに、ログ及び情報セキュリティの確保に必要な記録を取得し、一定期間適切に保存すること。

第２　個人情報を取り扱う事務の委託

個人情報を取り扱う事務の全部又は一部を委託する場合は、和歌山県個人情報取扱事務委託基準に基づき対応し、委託先（再委託先を含む。）に対して、法人が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な対応を行うこと。

第３　個人情報の漏えい事案等の発生時における対応

１　報告体制

個人情報の漏えい、滅失又は毀損の事案の発生又は兆候を把握した者、及び番号法に関する規定に違反している事実又は兆候を把握した者は、速やかに個人情報保護責任者に報告すること。

２　対応の手順

当該報告を受けた個人情報保護責任者は、次に掲げる対応を迅速に行うこと。

(1) 二次被害の防止のための必要な措置を速やかに講じること。

(2) 漏えい事案等の状況を確認し、課室長及び事務局総務課長へ報告するとともに、事案の内容に応じ、課室長の指示に基づき、事務局長へ報告すること。

(3) 漏えい事案等に係る原因を究明すること。

(4) 再発防止策等について検討すること。

(5) 漏えいした個人情報に係る本人への連絡及び説明等を行うこと。

(6) 事案の内容に応じ、報道機関に対する記者発表又は資料提供等により公表すること。

(7) 個人情報の漏えい事案等の発生時は、関係機関と連帯した対応を行うこと。

(8) 特定個人情報の漏えい等の番号法違反の事案又は番号法違反のおそれがある事案を把握した場合は、課室長、事務局総務課長及び文書法制専門員と協議の上、文書法制専門員が番号法第29条の4に基づいて行う個人情報保護委員会への報告に協力するとともに必要な対応を行うこと。

3 特定個人情報保護評価の再実施等

特定個人情報保護評価に関する規則に基づく特定個人情報保護評価を実施している事務について、発見された特定個人情報の漏えい等事案が、故意による又は当該特定個人情報の本人の数が 100 人を超えるもの（配送事故等のうち当該評価実施機関の責めに帰さない事由によるものを除く。）に該当する場合において、当該特定個人情報保護評価のしきい値判断の結果が変更されるときは、特定個人情報保護評価の再実施を行うこと。

また、特定個人情報保護評価のうち、重点項目評価又は全項目評価を実施している事務にあっては、評価書における個人情報に関する重大事故に該当する内容等を見直すこと。

第4 教育研修

1 教育研修の実施

事務局総務課長は、個人情報保護責任者及び個人情報を取り扱う担当者に対し、個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他の必要な教育研修を行うこと。

2 教育研修への参加の機会の付与

個人情報保護責任者は、個人情報を取り扱う担当者に対し、個人情報の適切な管理のために、事務局総務課長等が実施する教育研修への参加の機会を付与する等の必要な措置を講じること。

第5 点検等の実施

1 点検

個人情報保護責任者は、当該所属における個人情報の記憶媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を事務局総務課長へ報告すること。

2 特定個人情報の監査

課室長（必要に応じ、それらに相当する者）は、特定個人情報の適切な管理を検証するため、本要綱に定める措置の状況を含む特定個人情報の管理の状況について、定期に及び必要に応じ随時に監査を行い、その結果を事務局総務課長へ報告すること。

3 事務局総務課長の指示等

事務局総務課長は、必要に応じて、課室長及び個人情報保護責任者に対し、点検又

は監査を実施するよう指示をすること、又は、個人情報の取扱いについて是正の指示等をすることができる。

4　評価・見直し

事務局総務課長は、点検及び監査の結果を踏まえ、実効性の観点から評価し、必要があると認めるときは、本要綱の見直し等の措置を行うこと。

第３章　実施機関非識別加工情報に関する安全確保の措置等

第１　実施機関非識別加工情報等の取扱い

1　実施機関非識別加工情報等の取扱い

実施機関非識別加工情報等の取扱いについては、この第１に定めるもののほか、第２章第１の個人情報の取扱いの例による。

2　関係法令等の遵守

(1) 文書処理規程の遵守

実施機関非識別加工情報の取扱いについては、文書処理規程を遵守すること。

(2) 情報セキュリティ対策要綱の遵守

実施機関非識別加工情報が情報資産に該当する場合は、情報セキュリティ対策要綱を遵守すること。

(3) 条例の趣旨に則り、関連する法令及び規程等の定め並びに個人情報保護責任者の指示に従い、実施機関非識別加工情報等を取り扱うこと。

3　利用及び提供等について

(1) 利用及び提供の制限

法令に基づく場合を除き、利用目的以外の目的のために実施機関非識別加工情報及び削除情報を自ら利用し、又は提供してはならない。

(2) 第三者の閲覧防止

端末機器の使用に当たっては、実施機関非識別加工情報等が当該職員以外の第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講じなければならない。

(3) 複製の制限

業務上の目的で実施機関非識別加工情報等を取り扱う場合であっても、次に掲げる行為については、当該実施機関非識別加工情報等の秘匿性等その内容に応じて、当該行為をできる限り行わないこととし、当該行為を行う必要があると認められる場合は、個人情報保護責任者の指示に従うこと。

ア　実施機関非識別加工情報等の複製

イ　実施機関非識別加工情報等の送信

ウ　実施機関非識別加工情報等が記録されている媒体の外部への送付又は持出し

エ　その他実施機関非識別加工情報等の適切な管理に支障を及ぼすおそれのある行

為

(4) 誤りの訂正等

実施機関非識別加工情報等の内容に誤り等を発見した場合には、個人情報保護責任者の指示に従い、訂正等を行うこと。

(5) 媒体の保存

個人情報保護責任者の指示に従い、実施機関非識別加工情報等が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、当該媒体の耐火金庫への保管、施錠等を行うこと。

4　廃棄

(1) 不要情報の廃棄

実施機関非識別加工情報等について、一時的に加工等の処理を行うため複製を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去すること。

(2) 廃棄方法

実施機関非識別加工情報等又は実施機関非識別加工情報等が記録されている媒体（端末機器及びサーバに内蔵されているものを含む。）が不要となった場合には、個人情報保護責任者の指示に従い、当該実施機関非識別加工情報等の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行うこと。

5　取扱状況等の明確化

(1) 個人情報ファイル簿の作成等

ア　個人情報ファイル簿の作成及び公表

条例第15条に規定する個人情報ファイル簿にある実施機関非識別加工情報に係る項目について、その作成及び公表については、遺漏なきよう取り扱うこと。

イ　個人情報ファイルの明確化

個人情報ファイル簿は、県民等が事務局各課室における実施機関非識別加工情報の提案を行う基礎資料であるとともに実施機関非識別加工情報の取扱状況を示すものであるため、事務局各課室は、個人情報ファイル簿を明確に記載すること。

(2) 文書管理簿の作成等

実施機関非識別加工情報等は、その保管状況等を明らかにするため、文書処理規程に基づき文書管理簿を作成すること。

(3) 取扱状況の記録

実施機関非識別加工情報等の秘匿性等その内容に応じて、当該実施機関非識別加工情報等の利用及び提供等については、決裁を得るものとし、当該決裁は、文書処理規程に基づき保存すること。

なお、決裁により難い場合は、台帳等を整備し、当該実施機関非識別加工情報等の利用及び保管等の取扱いの状況について記録すること。

(4) 情報システム等における取扱い

情報システムにおいて実施機関非識別加工情報等を取り扱う場合は、定期的にバックアップを実施するとともに、ログ及び情報セキュリティの確保に必要な記録を取得し、一定期間適切に保存すること。

(5) 個人情報保護責任者の確認

個人情報保護責任者は、実施機関非識別加工情報等の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認すること。

6　契約相手方における実施機関非識別加工情報等の取扱い

(1) 確認対応

実施機関非識別加工情報の利用に関する契約を締結した者（以下「契約相手方」という。）から、当該契約相手方が講じた実施機関非識別加工情報の適切な管理に支障を及ぼすおそれがある旨の報告を受けた場合、個人情報保護責任者は、直ちに事務局総務課長に報告するとともに、当該契約相手方がその是正のために講じた措置を確認すること。

(2) 総務省への報告

個人情報保護責任者は、契約相手方が条例第 45 条の 14 各号に該当すると認められ契約を解除した場合には、直ちに事務局総務課長に報告すること。

なお、当該報告を受けた事務局総務課長は、直ちに和歌山県総務部総務課長に報告し、当該事実、契約相手方の氏名又は名称及び住所又は居所並びに法人にあっては、その代表者の氏名について総務省に報告すること。

第２　実施機関非識別加工情報を取り扱う事務の委託

１　委託

実施機関非識別加工情報の委託については、この第２に定めるもののほか、第２章第２の個人情報を取り扱う事務の委託の例による。

２　委託業者の選定及び契約

実施機関非識別加工情報の作成に係る業務又は実施機関非識別加工情報等の取扱いに係る業務を外部に委託する場合には、実施機関非識別加工情報等の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じること。

また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理及び実施体制、実施機関非識別加工情報等の管理の状況についての検査に関する事項等の必要な事項について書面で確認すること。

(1) 実施機関非識別加工情報等に関する秘密保持、目的外利用の禁止等の義務

(2) 再委託の制限又は事前承認等再委託に係る条件に関する事項

(3) 実施機関非識別加工情報等の複製等の制限に関する事項

(4) 実施機関非識別加工情報等の漏えい等の事案の発生時における対応に関する事項

(5) 委託終了時における実施機関非識別加工情報等の消去及び媒体の返却に関する事項

(6) 違反した場合における契約解除、損害賠償責任その他必要な事項

3　検査

実施機関非識別加工情報等の取扱いに係る業務を外部に委託する場合には、委託する実施機関非識別加工情報等の秘匿性等その内容に応じて、委託先における実施機関非識別加工情報等の管理の状況について、年１回以上の定期的検査等により確認を行うものとする。

4　再委託

委託先において、実施機関非識別加工情報の作成に係る業務又は実施機関非識別加工情報等の取扱いに係る業務が再委託される場合には、委託先に２の委託業者の選定及び契約の措置を講じさせるとともに、再委託される業務に係る実施機関非識別加工情報等の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが３の検査の措置を実施するものとする。

第３　教育研修

1　教育研修の実施

事務局総務課長は、個人情報保護責任者及び実施機関非識別加工情報等の取扱いに従事する職員に対し、実施機関非識別加工情報等の取扱いについて理解を深め、実施機関非識別加工情報等の適切な管理に関する意識の高揚を図るための啓発その他の必要な教育研修を行うこと。

2　教育研修への参加の機会の付与

個人情報保護責任者は、実施機関非識別加工情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、実施機関非識別加工情報等の適切な管理のために、事務局総務課長等が実施する教育研修への参加の機会を付与する等の必要な措置を講じること。

第４　漏えい事案への対応

1　報告体制

実施機関非識別加工情報等の漏えい等の事案の発生又は兆候を把握した場合等、安全確保の上で問題となる事案の発生又は発生のおそれを把握した場合に、その事案の発生等を把握した者は、直ちに当該実施機関非識別加工情報等を管理する個人情報保護責任者に報告すること。

2　対応の手順

当該報告を受けた個人情報保護責任者は、次に掲げる対応を迅速に行うこと。

(1) 二次被害の防止のための必要な措置を速やかに講じること。

(2) 漏えい事案等の状況を確認し、課室長及び事務局総務課長へ報告するとともに、事案の内容に応じ、課室長の指示に基づき、事務局長へ報告すること。

(3) 漏えい事案等に係る原因を究明すること。

(4) 再発防止策等について検討すること。

(5) 漏えいした個人情報に係る本人への連絡及び説明等を行うこと。

(6) 事案の内容に応じ、報道機関に対する記者発表又は資料提供等により公表すること。

第５　点検等の実施

１　点検

個人情報保護責任者は、当該所属における実施機関非識別加工情報等の記憶媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を事務局総務課長へ報告すること。

２　監査

課室長（必要に応じ、それらに相当する者）は、実施機関非識別加工情報等の適切な管理を検証するため、本章に定める措置の状況を含む実施機関非識別加工情報等の管理の状況について、定期に及び必要に応じ随時に監査を行い、その結果を事務局総務課長へ報告すること。

３　事務局総務課長の指示等

事務局総務課長は、必要に応じて、課室長及び個人情報保護責任者に対し、点検又は監査を実施するよう指示をすること、個人情報の取扱いについて是正の指示等をすることができる。

４　評価・見直し

事務局総務課長は、点検及び監査の結果を踏まえ、実効性の観点から評価し、必要があると認めるときは、見直し等の措置を講ずるものとする。

附　則

この要綱は、平成 28 年４月１日から施行する。

附　則

この要綱は、和歌山県個人情報保護条例及び和歌山県情報公開条例の一部を改正する条例（平成 29 年和歌山県条例第 54 号）の施行の日から施行する。

和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ管理要綱

制　　定　平成30年３月28日
最終改正　令和３年３月29日

第１章　　総則

（目的）
第１条　この要綱は、和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針（以下「基本方針」という。）に基づき、和歌山県立医科大学の情報の秘密を守ること（以下「機密性」という。）、情報を改ざんされないこと（以「完全性」という。）、利用が停止されないこと（以下「可用性」という。）を維持し、当該情報資産の適正な運用による大学の信頼性の確保を図るため、職員等が遵守すべき必要な事項を定めるものとする。
（用語の定義）
第２条　本要綱で、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
⑴　大学　和歌山県立医科大学をいう。
⑵　学内規程等　和歌山県立医科大学が制定した規程、要綱、要領、基準、要項及び行細則をいう。
⑶　情報管理委員会　和歌山県立医科大学情報管理委員会をいう。
⑷　所属長　医学部の講座、先端医学研究所の研究部、保健看護学部、薬学部、助産学専攻科、センター、図書館、共同利用施設、附属病院の診療科・中央部門、紀北分院の診療科・中央部門、危機対策室及び事務局課室の長をいう。
⑸　ネットワーク　大学で使用される情報通信機器及び通信回線をいう。医療情報システムネットワーク、医学情報ネットワーク（学内ＬＡＮ）など。
⑹　情報システム　大学で使用されるネットワーク、ハードウェア、ソフトウェア及び記憶媒体で構成された情報を処理する仕組みをいう。
⑺　データ　情報をコンピュータが扱える形態にしたもの。
⑻　記録媒体　データを記録した磁気ディスク、磁気テープその他の媒体をいう。
⑼　サーバ　他のコンピュータからの要求を受けて処理を実行するコンピュータをいう。
⑽　端末機等　サーバ及び通信機器等を除く電子計算機（付属する入出力・記憶装置を含む。）をいう。単独で事務に使用する電子計算機、サーバの機能提供を受ける電子計算機、サーバ等からデータを取り入れ持ち運んで利用する携帯端末機、ハードディスク装置を搭載した複写機など記憶装置とソフトウェアを搭載する事務機器などをさす。
⑾　ユーザ　情報資産を操作する権限を許可された大学の職員（非常勤、準職員、臨時職員等を含む。）及び学外受託者（大学の業務に従事する派遣会社社員、協力会社社員及び業務受託会社社員をいう。）をいう。
⑿　システム管理者　情報システムを管理、運用する各所属の所属長をいう。学内ＬＡＮ接続のパソコン及び単体でのパソコンを保有している部署の各所属長を含む。
⒀　コンピュータ入出力情報　フロッピーディスク、ＭＯ、ＵＳＢメモリ、メモリカード、CD・DVD、紙等に記録された、コンピュータ上で入出力される情報資産をいう。
⒁　コンピュータ内情報　ハードディスク、メモリ等に記録されたコンピュータの内部で使用している情報資産をいう。
⒂　職員間電子メール　職員の使用するＩＤ（ユーザ及び情報通信機器の識別に使用する記号をいう。）から職員の使用するＩＤへの電子メールをいう。
⒃　外部向け電子メール　職員の使用するＩＤから職員の使用するＩＤ以外のアドレスへの電子メールをいう。
⒄　学内配布　学内での情報資産を有する記憶媒体、文書等の配布をいう。
⒅　学外配布　郵便、宅配便等を利用した学外への情報資産を有する記憶媒体、文書等の配布をいう。
⒆　インターネット　世界中のコンピュータを１つのネットワークで結んだネットワーク方式をいう。
⒇　Ｗｅｂ　正確には「World Wide Web」で、インターネット等で使用されているハイパーテキスト（それぞれの情報を関連付け、すぐに参照できる機能をもつ文字列のことをいう。）で表したドキュメントシステムで、文字や画像、動画、音楽などを簡単に利用することができる。
(21)　プログラム　コンピュータの動作を規定し、記述したものをいう。
（情報資産）
第３条　本要綱の適用対象となる情報資産は、次の各号に掲げるものとする。
⑴　大学で使用されるネットワーク及び情報システムの開発にかかわる全ての文書、図画、写真、フィルム及び電磁的記録

⑵　大学で使用されるネットワーク及び情報システムで取り扱う全ての電磁的記録
⑶　大学で使用されるネットワーク及び情報システムの運用にかかわる文書及び図画。ただし、和歌山県立医科大学文書処理規程第２条に規定する文書を除く。

（情報セキュリティ責任者、総括責任者及び情報管理委員会）

第４条　大学における情報セキュリティ（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。以下同じ。）について、責任と権限をもって情報の取扱方法等を指示する者として、和歌山県立医科大学に情報セキュリティ責任者を置く。

２　情報セキュリティ責任者は、次の各号に定める者をもって充てる。

⑴　学生部長、医学部長、保健看護学部長、薬学部長、附属病院長、紀北分院長、産官学連携推進本部長、地域・国際貢献推進本部長及び事務局長

⑵　教育研究開発センター長、入試・教育センター長、図書館長、共同利用施設長、助産学専攻科長、みらい医療推進センター長、健康管理センター長、ワークライフバランスセンター長、看護キャリア開発センター長及び危機対策室長

３　情報セキュリティ責任者を総括し、大学における情報セキュリティに関する最高責任者として、情報セキュリティ総括責任者を置く。学長がその任に当たる。

４　大学の情報セキュリティに関する重要な事項の調査・検討・審議は、情報管理委員会で行う。情報管理委員長は情報管理委員会で情報セキュリティに関する重要な方針等を審議した場合は、情報セキュリティ総括責任者に報告する。

（情報セキュリティ管理者及び職員）

第５条　情報セキュリティ責任者の指示の下、各所属において情報セキュリティ活動の指導及び監督を行う者として、情報セキュリティ管理者を置く。ただし、前条第2項第2号に定める情報セキュリティ責任者は、情報セキュリティ管理者の業務を併せて行うものとする。

２　情報セキュリティ管理者は、所属長をもって充てる。

３　職員は、この要綱の目的及び情報セキュリティの重要性について認識し、情報資産を適切に取り扱わなければならない。

４　職員は、情報資産の取扱いに当たっては、次に掲げる法令等を遵守しなければならない。

⑴　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）
⑵　著作権法（昭和45年法律第48号）
⑶　個人情報の保護に関する法律（平成15年法律第57号）
⑷　和歌山県個人情報保護条例（平成14年和歌山県条例第66号）
⑸　学内規程等

（情報管理者）

第６条　主管する業務において情報を収集し、若しくは作成し、又は県民等から情報を預託された所属の所属長を情報管理者とする。

（情報セキュリティ確保のための方策）

第７条　情報セキュリティ管理者は、当該所属において情報資産を分類し、適切な情報セキュリティの水準を維持するために、当該分類に応じ次に掲げる方策を定めなければならない。

⑴　情報システムを設置した場所への不正な立ち入り又は情報資産の持ち出し若くは破壊等の物理的な侵害から情報資産を保護するための物理的なセキュリティ確保のために必要な方策
⑵　情報資産を取り扱う職員に対する指導等の人的セキュリティ確保のために必要な方策
⑶　情報資産に対する不正アクセスの防止、コンピュータウィルス対策等の技術的なセキュリティ確保のために必要な方策

（情報区分）

第８条　情報資産は、機密性、完全性及び可用性の度合いに応じた効果的な情報セキュリティを確保するため、次のとおり区分する。

⑴　機密性区分
ア　区分３　情報管理者が必要であると認めた者のみが取り扱う情報を含む情報資産。例えば、個人情報などをいう。
イ　区分２　大学の職員及び情報管理者が必要であると認めた者（職員を除く。）のみが取り扱う情報を含む情報資産。（アに規定する情報資産を除く。）例えば、学内向けの情報などをいう。
ウ　区分１　ア及びイに該当しない情報資産。例えば、ホームページで既に学外に公開している情報などをいう。

⑵　完全性区分
ア　区分３　改ざんされることにより、県民等の生命、身体、財産及びプライバシーに重大な影響がある情報を含む情報資産。例えば、患者基本情報、診療情報などに当たる情報資産をいう。
イ　区分２　改ざんされることにより、大学事務の執行等に影響がある情報を含む情報資産（アに規定する情報資産を除く。）
ウ　区分１　ア及びイに該当しない情報資産

(3) 可用性区分
ア 区分３　業務処理の停止時間が30分以下であっても、重大な影響を及ぼす情報システムで取り扱われる情報を含む情報資産
イ 区分２　業務処理の停止時間が24時間以下であっても、重大な影響を及ぼす情報システムで取り扱われる情報を含む情報資産（アに規定する情報資産を除く。）
ウ 区分１　ア及びイに該当しない情報資産

（セキュリティレベル）

第９条　前条の区分に基づき、職員が情報資産を取り扱う上での判断を容易にするため、次のとおり情報資産のセキュリティレベルを分類する。
(1) セキュリティレベル３　機密性区分及び完全性区分のうち、いずれか１つでも区分３と評価されるもの
(2) セキュリティレベル２　セキュリティレベル３と評価されるもの以外で、機密性区分及び完全性区分のうち、いずれか１つでも区分２と評価されるもの
(3) セキュリティレベル１　前２号に該当しないもの

（セキュリティレベル３の一般保護管理要件）

第10条　セキュリティレベル３の情報資産の一般保護管理要件を次のとおり定める。
(1) 収集　情報管理者は、情報資産を収集するときは、関係する法令等を遵守すること。
(2) 保管
ア 職員は、情報セキュリティ管理者の指導に従い、情報資産を業務上必要とする者以外の目に触れないように取り扱い、及び保管すること。
イ 職員は、情報資産が保管されているエリアにおいては、エリアを使用しないときは、施錠すること。
ウ 職員は、情報資産が保管されているエリアにおいては、エリアに立ち入る者を把握し、職員以外の者が保守、点検又は清掃の作業で立ち入るときは、立ち会うこと。
エ 情報セキュリティ管理者は、年１回及び必要に応じ情報資産の調査及び点検を行うこと。
オ 情報セキュリティ管理者は、情報資産が持ち運びできる記憶媒体（ハードディスクを除く。）に暗号化されていない状態で記憶されているときは、当該情報資産の保管責任者を定め、施錠された保管庫等に保管すること。
カ 職員は、情報システム用の持ち運びできる記憶媒体で、第24条第1号の入退室管理エリアに保管されている情報資産を他のエリアへ移動させるときは、情報セキュリティ管理者及びシステム管理者の承認を得ること。
キ 職員は、パーソナルコンピュータ（以下「パソコン」という。）のハードディスクに情報資産を記憶し、保存するときは、パソコンの盗難防止のために施錠等による物理的保護管理下に置くとともに、始動パスワード等のセキュリティ設定を行うこと。
(3) 使用
ア 職員は、事前に情報管理者の定めた利用目的に限って情報資産を使用すること。また、利用にあたっては情報管理者の許可を受けること。
イ 職員は、学術研究のため情報資産を利用する場合、個人情報の取扱いには十分注意し、学会や研究会での報告や統計資料作成にあたっては、氏名、住所、生年月日等の個人を特定できるような情報を消去し、顔写真についてはマスキングにより匿名化すること。なお、匿名化が困難な場合は、当該個人情報の利用に対して本人の同意を得ること。
(4) 配布
ア 職員は、情報資産を配布するときは、業務上知る必要のある者に限定して配布すること。
イ アに規定する配布をするときは、受取人になっている者以外の者による受信又は開封ができないようにすること。
ウ 職員は、情報資産を学内配布するときは、情報資産が同封されていることが判断可能な体裁とし、又は専用の封筒を用いること。
エ 職員は、情報資産を学外配布するときは、二重封かん等により外部から内容物を確認できないような体裁とし、収受の確認が可能な配送で行うこと。
オ 職員は、情報資産を学外配布の方法で職員に配布するときは、内側封筒に受取人名と「セキュリティレベル３」を表示し、外封筒にはセキュリティレベルを表示しないこと。
カ 職員は、情報資産に係るコンピュータ内情報を電子メールで送付しないこと。
キ 職員は、情報資産をやむを得ずファクシミリ等（配信印刷）により配布するときは、業務上必要となる者以外の者に見られないよう、受信者が直ちにファクシミリ等受信文書を回収できる状態にあることを確認の上、送信すること。
(5) 複写　職員は、情報資産を複写するときは、情報管理者に事前の許可を受けること。
(6) 携行

ア　職員は、情報資産を保管エリア外に原則として携行しないこと。ただし、やむを得ず携行する必要がある場合で、情報セキュリティ管理者に事前の許可を受けたときは、この限りではない。
イ　職員は、情報資産をやむを得ず携行するときは、常時携帯するものとし、当該情報資産を放置しないこと。また、携行時は鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じること。この場合において、盗難又は紛失にあったときは、速やかに所属の情報セキュリティ管理者及び情報管理者に報告すること。

(7)　廃棄

ア　情報資産の廃棄は情報管理者又は情報管理者に指示された職員が行うこととし、当該情報資産が文書、図画、写真及びフィルムである場合は、シュレッダ等により判読不能な状態にすること。
イ　廃棄すべき情報資産が電磁的記録であるときは、データの完全削除を行うプログラムの使用その他の方法により当該情報資産を消去し、復元できない状態にすること。

（セキュリティレベル２の一般保護管理要件）

第11条　セキュリティレベル２の情報の一般保護管理要件を次のとおり定める。

(1)　収集　情報管理者は情報資産を収集するときは、関係する法令等を遵守すること。

(2)　保管

ア　職員は、情報セキュリティ管理者の指導に従い、情報資産を業務上必要とする者以外の目に触れないように取り扱い、及び保管すること。
イ　職員は、情報資産が保管されているエリアにおいては、エリアを使用しないときは、施錠をすること。
ウ　職員は、情報資産が保管されているエリアにおいては、エリアに立ち入る者を把握し、職員以外の者が立ち入るときは、留意すること。

(3)　使用　職員は、特に制限なく情報資産を使用することができる。

(4)　配布

ア　職員は、情報資産を職員以外の者へ配布するときは、名あて人について情報管理者の承認を受けること。
イ　職員は、情報資産を学内配布するときは、情報資産が同封されていることが判断可能な体裁とすること。
ウ　職員は、情報資産を学外配布するときは、収受の確認が可能な配送で行うこと。
エ　職員は、情報資産に係るコンピュータ内情報を電子メールを使用して配布するときは、ファイルをパスワードにより保護し、又は暗号化すること。その場合、解錠又は復号のためのパスワードは、電話、ファクシミリ等で伝達するか又は事前に申し合わせておくこととし、決して電子メールによる伝送は行わないこと。

(5)　複写　職員は、情報資産を特に制限なく複写することができる。

(6)　携行

ア　職員は、情報資産を学外に原則として携行しないこと。ただし、やむを得ず携行する必要がある場合で、情報セキュリティ管理者に事前の許可を受けたときは、この限りではない。
イ　職員は、情報資産をやむを得ず携行するときは、常時携帯するものとし、当該情報資産を放置しないこと。また、携行時は鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じること。この場合において、盗難又は紛失にあったときは、速やかに所属の情報セキュリティ管理者及び情報管理者に報告すること。

(7)　廃棄

ア　情報資産の廃棄は情報管理者又は情報管理者に指示された職員が行うこととし、当該情報資産が文書、図画、写真及びフィルムである場合は、シュレッダ等により判読不能な状態にすること。
イ　廃棄すべき情報資産が電磁的記録であるときは、可能な限りデータの完全削除を行うプログラムの使用その他の方法により当該情報資産を消去し、復元できない状態にすること。

（セキュリティレベル１の一般保護管理要件）

第12条　セキュリティレベル１の情報資産は、セキュリティ面の管理を必要としないものとする。

２　職員は、特に制限なく情報資産を外部の者へも提供できるものとする。

（セキュリティレベルの表示）

第13条　セキュリティレベル３の情報資産には、必要に応じそのセキュリティレベルを表示するものとし、表示の方法は、次の各号の定めるところにより行うものとする

(1)　見やすく目立つように表示すること。
(2)　コンピュータ入出力情報で紙に印刷されたものその他判読が可能なものは、各頁に表示すること。
(3)　コンピュータ内情報はファイル名に表示すること。
(4)　複数の情報資産を有する記憶媒体及び媒体ケース又はトランクには、含まれる情

報資産の最高のセキュリティレベルを表示すること。

第２章　　人的措置

（情報管理者の役割と責任）
第14条　情報管理者の役割と責任は、次に定めるとおりとする。
⑴　情報管理者は、情報資産のセキュリティレベルを決定し、及び特別保護管理要件（一般保護管理要件に加えて守るべき特別な要件をいう。以下同じ。）を定め、当該情報資産を使用する所属の情報セキュリティ管理者及びシステム管理者に通知する責任を有するものとする。
⑵　情報管理者は、情報資産の管理状況等を検証し、並びに必要に応じて情報資産のセキュリティレベル及び特別保護管理要件の見直しを行うものとする。
⑶　情報管理者は、セキュリティレベル３の情報資産について、当該情報資産を使用しようとする所属の所属長の申請に基づき、当該情報資産の使用者を決定し、当該申請を行った所属の所属長に許可の通知を行い、及び許可履歴を記録するものとする。
⑷　情報管理者は、情報資産の損失、不正使用又は一般保護管理要件及び特別保護管理要件（以下「保護管理要件」という。）が遵守されていない旨の報告を受けたときは、速やかに情報セキュリティ責任者、情報管理委員会事務局及び危機対策室に報告するものとする。
（情報資産管理）
第15条　情報管理者は、情報資産の管理をするために、情報資産台帳を作成し、適正な整備を行い、常に最新の内容を保たなければならない。
（セキュリティレベルの変更等）
第16条　情報管理者は、必要に応じて、情報資産のセキュリティレベルを変更することができる。
２　情報管理者は、情報資産のセキュリティレベルを変更するときは、情報資産台帳に記載している変更前のセキュリティレベルを取り消し、変更後のセキュリティレベルを記入するものとする。この場合において、変更日付及び変更者氏名を記入するものとする。
３　情報管理者は、情報資産のセキュリティレベルを変更したときは、当該情報資産を使用することができる職員の所属の情報セキュリティ管理者及び情報管理者にセキュリティレベルの変更及び管理方法の変更を通知するものとする。
４　前項の場合において、情報管理者は、セキュリティレベルをレベル３にアップしたときは、必要に応じて、使用を許可した職員以外の者に使用させないため、関係所属の情報セキュリティ管理者及び情報管理者に指示し、当該情報資産を回収し、又は廃棄させなければならない。
（情報セキュリティ管理者の役割と責任）
第17条　情報セキュリティ管理者の役割と責任は、次に定めるとおりとする。
⑴　情報セキュリティ管理者は、管轄する所属で利用又は保管をする情報資産を、保護管理要件に基づき管理するものとする。（情報機器管理のマニュアルにより管理する。）
⑵　情報セキュリティ管理者は、管轄する所属の職員及び学外受託者に本要綱及び必要な保護管理要件を理解させ、遵守状況を管理するものとする。
⑶　情報セキュリティ管理者は、管轄する所属の情報資産を保護するための最適な物理的及び手続的保護管理手段を確保し、提供するものとする。
⑷　情報セキュリティ管理者は、管轄する所属の職員及び学外受託者を教育し、セキュリティ意識を高めるよう努めるものとする。
⑸　情報セキュリティ管理者は、管轄する所属の情報資産の損失、不正使用又は保護管理要件が遵守されていないことを発見したときは、速やかに関連する情報管理者、情報セキュリティ責任者、情報管理委員会事務局及び危機対策室に報告するものとする。
（職員の役割と責任）
第18条　職員の役割と責任は、次に定めるとおりとする。
⑴　職員は、情報資産の保護管理要件を遵守するものとする。
⑵　職員は、情報システムを使用するときは、当該情報システムのシステム管理者から当該情報システムの使用についての許可を受けるものとする。
⑶　職員は、端末機等を管理するシステム管理者の許可を受けずに情報システムで使用する端末機等を他の業務に使用しないものとする。
⑷　職員は、情報資産の保護管理のため、情報セキュリティ管理者から提供されている物理的保護管理手段を有効に使用するものとする。
⑸　職員は、情報資産の損失、不正使用又は保護管理要件が遵守されていないことを発見したときは、速やかに情報セキュリティ管理者に報告するものとする。
⑹　職員は、本要綱及び情報セキュリティ管理者の指示を遵守し、情報資産が不正な手段で取得され、又は不正に使用されることを防止する責任を有するものとする。

⑺　職員は、退職し、異動し、又は業務を変更若しくは終了したときは、業務において使用する必要のなくなった全ての情報資産の使用を取りやめ、保有する当該情報資産については所属していた所属の情報セキュリティ管理者に返却しなければならない。
⑻　職員は、ネットワーク及び情報システムの利用が自己責任の原則に基づいて行われることを十分理解しなければならない。
（システム管理者の役割と責任）
第19条　システム管理者の役割と責任は、次に定めるとおりとする。
⑴　システム管理者は、情報管理者の指示に従い、情報システムに対するユーザの使用を許可するものとする。
⑵　システム管理者は、情報資産の損失又は不正使用を発見したときは、速やかに関連する情報管理者、情報管理委員会事務局及び危機対策室に報告するものとする。
⑶　システム管理者は、情報資産の損失又は不正使用が発生したときは、速やかに対処し、必要な改善策をとるものとする。
（学外受託者への情報資産の使用許可）
第20条　情報管理者は、セキュリティレベル３の情報資産を、学外受託者に原則使用させないものとする。ただし、特殊な事情によりやむを得ないと判断したときは、リスク分析及びリスク管理を行った上で許可するものとする。
２　情報管理者は、セキュリティレベル３の情報資産について、前項ただし書きの許可をしたときは、情報セキュリティ責任者に報告しなければならない。
（契約）
第21条　大学が第三者と情報資産を扱う業務に係る契約を締結するときは、次の各号の掲げる内容を契約書に定めるものとする。
⑴　情報資産の取扱い
⑵　情報セキュリティ上の責任
⑶　損害賠償
２　セキュリティレベル３の情報資産に関わる契約は、前条第２項の情報セキュリティ責任者への報告後に締結しなければならない。
（情報セキュリティ教育及び訓練）
第22条　情報セキュリティ管理者は、管轄する所属の職員及び学外受託者が大学での業務に初めて従事するときは、事前に本要綱について教育し、研修させるものとする。
２　情報セキュリティ管理者は、業務の慣れによる情報セキュリティ意識の低下を防ぐことを目的として、情報セキュリティ責任者の指示に従い、管轄する所属の職員及び学外受託者を教育し、研修させるものとする。
３　情報セキュリティ管理者は、緊急時の対応を想定した訓練をユーザに行わせるものとする。
（事件及び事故の報告）
第23条　プログラムの変更、破壊等を行う不正なプログラム（「ウィルス」という。以下同じ。）の侵入、情報漏洩、情報システムの停止等情報セキュリティに関する事件又は事故（以下「事故」という。）が発生したときの報告は、情報セキュリティ管理者、情報セキュリティ責任者、情報管理者、情報管理委員会事務局及び危機対策室に行うものとする。
２　前項の事故がセキュリティレベル３の情報資産に発生した場合及び大学外に害を与えると予想される場合、情報管理委員会事務局は速やかに情報セキュリティ統括責任者及び同委員会に報告を行い、情報管理委員会事務局及び危機対策室は当該事故について公表を行うものとする。
３　情報セキュリティ管理者は、事故の内容に応じて迅速に情報セキュリティ責任者及び情報管理委員会に事故時のログ（情報システム上の業務記録をいう。以下同じ。）等を添えて報告書を提出するものとする。
４　情報セキュリティ管理者は、システム管理者等と協力し、事故原因の調査を行うものとする。
５　情報セキュリティ管理者は、事故原因の調査終了後、必要に応じて保護管理要件に基づき業務の見直しを行うものとする。

第３章　物理的措置

（エリアのセキュリティ）
第24条　情報資産を適切に管理するため、エリアのセキュリティを、次のとおり分類する。
⑴　入退室管理エリア　システム管理者及び情報セキュリティ管理者が許可した者のみが立ち入ることができ、入退室者を特定できるエリア
⑵　オフィスエリア　情報セキュリティ管理者若しくは情報セキュリティ管理者の指定した職員が許可をした者又は職員のみが立ち入ることができるエリア
⑶　内部エリア　前２号に該当しないエリア
（入退室管理エリアの要件）

第25条　入退室管理エリアへの入室を希望する者は、システム管理者若しくは情報セキュリティ管理者に、入室の許可を受けなければならない。
２　前項の規定により、入退室管理エリアの入室を許可された者（以下「入室者」という。）は、当該入退室管理エリアへ入室するときは、入退室管理簿に氏名、所属、入室日付、時刻及び作業内容等を記録しなければならない。
３　入室者は、当該入退室管理エリアから退室するときは、入退室管理簿に退室時刻を記録しなければならない。
４　システム管理者及び情報セキュリティ管理者は、入退室管理エリアについて、次の各号に掲げる措置をとるものとする。
⑴　サーバ等の設置場所である旨の表示をエリア外に出さないこと。
⑵　エリア外から情報機器を認識できないようにすること。
⑶　常時利用する出入口を限定すること。
⑷　出入口のドアは常時施錠すること。
（情報機器の設置と管理）
第26条　システム管理者は、情報機器を設置するときは、関係する所属長と協議し、エリアのセキュリティと各情報機器の特性を考慮に入れ、設置場所を決定するものとする。
２　システム管理者は、情報機器を管理するために情報機器台帳を作成するものとする。
３　前項に規定する情報機器台帳に記入する項目は、次の各号のとおりとする。
⑴　情報機器名
⑵　設置場所
⑶　シリアル番号又は識別番号
⑷　セキュリティレベル３の情報資産の使用の有無
（端末装置等）
第27条　情報セキュリティ管理者及び職員は、セキュリティレベル３の情報資産を端末機等で取り扱うときは、業務上知る必要のある者以外に、当該情報資産の内容を読まれないように、端末機等の設置場所及びディスプレイの向きに注意しなければならない。
（印刷機の使用）
第28条　職員は、セキュリティレベル３の情報資産を印刷するときは、システム管理者が特定した印刷機を使用しなければならない。
（サーバの設置）
第29条　システム管理者は、サーバを設置するときは、火災、水害、埃、振動、温度、湿度、静電気等の影響をできる限り排除した場所に設置し、容易に取り外せないよう適切に固定する等の必要な措置をとるものとする。
２　システム管理者は、セキュリティレベル３の情報資産を扱うサーバを設置するときは、入退室管理エリアに設置するように努めなければならない。入退室管理エリアに設置できない相当の理由がある場合は、施錠した保管庫内に設置する等の方策を講じなければならない。
（サーバの電源）
第30条　システム管理者は、通常の電源から一時的に十分な電力の提供を受けられなくなった場合においても、サーバを適切に停止することが可能な電力を提供することができる予備電源を、必要に応じて備え付けるものとする。
２　システム管理者は、可用性区分３の情報資産を扱うサーバについて、ＵＰＳ（無停電電源装置をいう。）による連続運転の確保等を必要に応じて施すものとする。
（通信回線）
第31条　システム管理者は、学内の通信回線が損傷等を受けることがないように必要な措置をとるものとする。
２　システム管理者は、前項の規定により行った措置が有効であること及び通信回線が損傷等を受けていないことについて定期的に点検をしなければならない。
（情報機器の管理施設外設置）
第32条　システム管理者は、情報機器を大学の管理する施設以外の施設に設置するときは、当該施設の情報セキュリティ対策（情報セキュリティがなされていることをいう。以下同じ。）の実施状況の審査及び確認を十分に行い、情報セキュリティ責任者に報告しなければならない。
２　前項の規定により、情報機器を大学の管理する施設以外の施設に設置したときは、システム管理者は、情報セキュリティの確保が有効に実施されていることについて定期的に確認をしなければならない。
（情報通信機器の設置）
第33条　システム管理者は、情報通信機器（端末機等からルータまでを接続するネットワークを構成する情報通信機器は除く。この条において以下同じ。）は原則として入退室管理エリアに設置するものとする。
２　前項の規定にかかわらず、建物の事情等により情報通信機器を入退室管理エリアに設置できないときは、当該情報通信機器の施錠可能な保管庫内への設置、施錠可能なカバーの装着等情報通信機器を入退室管理エリア内で管理されている状態に近い状

態にする措置を行うものとする。
（情報資産の確認）
第34条　システム管理者は、当該システムのネットワーク上にどのような情報資産が存在するかを確認し、その記録を施錠された保管庫又は入退室管理エリアに保管するものとする。
（情報機器の移動及び廃棄）
第35条　システム管理者は、情報機器を移管し、廃棄し、又は使用することを休止するときは、情報機器台帳に記入を行うものとする。
２　システム管理者は、情報機器を移管するときは、移管先を情報機器台帳に記入しなければならない。
３　システム管理者は、セキュリティレベル３の情報資産を使用していた記憶媒体が組み込まれている情報機器を学内で移管するときは、消去ツールの使用その他の方法により、記憶媒体（メモリ等一時的に記憶する媒体を除く。）にある情報資産を完全に消去するものとする。
４　システム管理者は、記憶媒体が組み込まれている情報機器を学外へ移管するとき又は廃棄するときは、記憶媒体にある情報資産を前項と同様の方法で完全に消去するものとする。
５　システム管理者は、記憶媒体と一体化している情報機器の修理又は廃棄を、修理又は廃棄を行う業者に委託するときは、記憶媒体にある情報資産を消去するものとする。
６　前項の規定による消去が難しいときは、修理又は廃棄を行う業者に対しコンピュータ内情報の秘密を守ることを契約に定めた上で委託しなければならない。
（クリアデスク）
第36条　職員は、クリアデスク（机の上及び周辺の整理をいう。以下同じ。）を定期的に行い、周囲にある情報資産の適切な管理を行わなければならない。
２　情報セキュリティ管理者は、管轄する所属のクリアデスクの実施についての具体的な計画を作成し、定期的に職員のクリアデスクの実施状況を点検するように努めるものとする。
３　情報セキュリティ管理者は、前項に規定する点検をしたときは、点検内容の記録を残すものとする。
（クリアスクリーン）
第37条　職員は、セキュリティレベル３の情報資産を取り扱う端末機等及びパソコンの使用時に席を離れるときは、スクリーンセーバ（一定時間入力がないと画面の表示を消し、　焼き付きが起こらないように模様が画面上を動くようにするソフトウェアをいう。）等を使用して、当該端末機等及びパソコンの画面並びに情報を保護しなければならない。
２　職員は、前項に規定する保護をするときは、必要に応じて画面の保護を解除するためのパスワードを設定し、他の者が使用できないようにしなければならない。
（クリアプリンタ）
第38条　職員は、セキュリティレベル３の情報資産を印刷するときは、印刷機へ印刷を要求した後印刷に立ち合い、及び出力された印刷物を直ちに回収し、印刷機上に放置してはならない。
２　印刷機の設置されている入退室管理エリアを最後に退出する職員は、当該印刷機上を確認し、放置してある印刷物を発見したときは、適切に対応するものとする。

第４章　技術的措置

（ＩＤ）
第39条　職員は、ＩＤを他の者に使用させてはならない。
２　システム管理者は、特定のＩＤを使用して情報システムに不正なアクセスを行った事実を発見したときは、ただちに当該ＩＤを使用不能にすることができる。
３　システム管理者は、異動等で不要になったＩＤについて、速やかに停止又は登録抹消をしなければならない。
（ユーザ認証）
第40条　システム管理者は、情報システム（不特定多数の者に公開している情報システムを除く。以下この条及び第４２条において同じ。）のユーザを特定するために、適切なユーザ認証（情報システムに接続しようとする者が情報システムの使用を許可された本人であることを確認することをいう。）の方法を用いなければならない。
２　職員は、ユーザ認証の方法としてパスワードを用いる情報システムを使用するときは、パスワードを他の者に教えてはならない。
３　職員は、ユーザ認証の方法としてパスワードを用いる情報システムを使用するときは、パスワードを他の者に知られないように努めなければならない。
４　システム管理者及び職員は、ユーザ認証の方法としてパスワードを用いるときは、パスワードが記載された情報資産をセキュリティレベル３として管理するものとする。
（特権ユーザ管理）

第41条　システム管理者は、情報システム管理のために、特別な権限を与えられている特権ユーザのパスワードを、必要に応じ適切な時期に変更するものとする。
（接続の制御）
第42条　システム管理者は、情報システムに接続する者を、第19条に規定する許可したユーザに限定し、かつ、許可を受けた行為に限り使用できるように管理しなければならない。
（ネットワークの経路制御）
第43条　ネットワークの管理を行うシステム管理者は、ネットワークへの不正な接続を防止するために、ネットワークの経路制御を適正に設定し、及び管理するものとする。
（ネットワークの領域分割）
第44条　ネットワークの管理を行うシステム管理者は、ネットワークの領域を分割し、ネットワークの利用者及びネットワークを使用する情報システムのグループごとに使用する領域を設定しなければならない。
（ウィルス対策ソフトウェア）
第45条　システム管理者は、ウィルスが情報機器に密かに侵入することを予防及び監視するために、ウィルスを検索し、駆除するソフトウェア（「ウィルス対策ソフト」という。　以下同じ。）を必要に応じ導入し、及び常時稼動させるものとする。
２　システム管理者は、ウィルス対策ソフトで使用するウィルス定義ファイルについては、最新のものを使用するものとする。
３　システム管理者は、第1項の規定により導入したウィルス対策ソフトについては、プログラム全体及びエンジン（プログラムの中心となる部分をいう。）の改訂状況に注意することとし、必要に応じ更新するものとする。
（情報システムの最新化）
第46条　システム管理者は、使用しているソフトウェアの最新のパッチ（修正プログラムのことをいう。）の情報に注意し、最新パッチが必要であると判断したときは、速やかにパッチによるプログラムの修正を行い、管理している情報システムの最新化に努めるものとする。
（その他の不正なプログラム）
第47条　システム管理者は、ウィルス以外の不正なプログラムの情報についても定期的に確認し、ユーザに対して注意喚起を行い、オペレーティングシステムにプログラムの実行を制限する設定を行う等の措置を行うものとする。
（外部接続）
第48条　システム管理者は、大学が管理する情報システムと大学以外の者が管理する情報システムとの接続（以下「外部接続」という。）を原則として行ってはいけない。業務遂行のため、やむを得ず外部接続をする必要がある場合は、当該外部接続をする相手の情報セキュリティの確保状況の審査及び確認を十分に行い、その結果を添えて接続の許可申請書を情報セキュリティ責任者を経由して情報管理委員会に提出し、特別に許可を受けなければならない。
２　システム管理者は、外部接続をしたときは、当該外部接続をした相手の情報セキュリティ確保のための措置が有効に実施されていることについて定期的に確認をしなければならない。
３　システム管理者は、外部接続の内、インターネット接続（インターネットとの接続をいう。以下同じ。）及び電話回線接続（電話回線を通じた接続をいう。以下同じ。）をしたときは、ユーザが当該外部接続を使用するに当たっての使用要件を定めるものとする。
（インターネット接続）
第49条　システム管理者は、インターネット接続が可能なサーバ（情報資産を有するものに限る。）について、リスク評価を行わなければならない。
２　システム管理者は、インターネット接続する情報システムでセキュリティレベル３の情報資産を使用するときは、当該情報資産を暗号化して保護する措置をとるように努めるものとする。
（外部接続の遵守事項）
第50条　システム管理者は外部接続をする場合は、前２条に定めるもののほか、次の各号の要件を遵守しなければならない。
⑴　システム管理者は、必要に応じ外部接続をする相手との間で機密保持及び損害賠償を含んだ契約を締結すること。
⑵　システム管理者は、外部接続の管理状況を情報管理委員会事務局に書面により報告すること。
⑶　システム管理者は、外部接続する情報システムについて、必要最小限のものとすること。
（医学情報ネットワークとの接続）
第51条　職員は、医学情報ネットワークとの接続に関し、関係規程等の留意事項を遵守し、適切な運用管理を行うものとする。
（学術情報ネットワークシステムとの接続）
第52条　職員は、学術情報ネットワークシステム（以下「ＳＩＮＥＴ」という。）との

接続に関し、ＳＩＮＥＴ側の留意事項を遵守し、適切な運用管理を行うものとする。

（国、県及び他の地方公共団体との接続）

第53条　前２条に定めるもののほか、国、県又は他の地方公共団体が管理するネットワーク又は情報システムと接続する場合は、別途定めるネットワークセキュリティに関わる基準等を遵守しなければならない。

第５章　情報システムの開発・運用上のセキュリティ確保

（公開する調達仕様書）

第54条　システム管理者は、情報システムの調達をするときは、一般に公開する調達仕様書が、当該情報システムの情報セキュリティ確保の上で支障にならないことを確認するものとする。

（情報機器又はソフトウェア購入時のセキュリティ確認）

第55条　システム管理者は、情報機器又はソフトウェアを購入するときは、当該製品が情報セキュリティ確保の上で支障にならないことを確認するものとする。

（情報システムの動作試験等）

第56条　情報システムの動作試験を行うときは、試験用に作成された情報資産を用いなければならない。

２　運用試験をするときも、できる限り試験用に作成された情報資産を用いなければならない。

（変更管理）

第57条　システム管理者は、情報システムを追加し、及び変更するときは、追加及び変更後の当該情報システムの設定、構成等の履歴を記録し、保存するものとする。

（業者管理）

第58条　システム管理者又は情報システムの開発を行う所属の所属長は、情報システムの開発、運用及び保守を職員以外のものに委託するときは、次に掲げる事項についてあらかじめ調査及び検討をし、委託先の信頼性を確認するものとする。

⑴　委託先の経営内容及び技術水準等の状況に関すること。

⑵　委託先の要員管理体制及び情報セキュリティ確保の状況に関すること。

２　システム管理者は、情報システムの開発、運用及び保守について委託するときは、委託契約書又は仕様書に、次に掲げる事項を明記するものとする。

⑴　秘密保持義務に関すること。

⑵　権利義務譲渡に関すること。

⑶　再委託の禁止又は制限に関すること。

⑷　善良なる管理者の注意義務に関すること。

⑸　情報資産の目的外使用及び第三者への提供の禁止に関すること。

⑹　情報資産の複写又は複製に関すること。

⑺　事故発生時における報告義務に関すること。

⑻　著作権の譲渡に関すること。

⑼　和歌山県個人情報保護条例（平成14年和歌山県条例第66号）に基づく個人情報の保護に関すること。

⑽　納品物がウィルスに感染していないことの確認に関すること。

⑾　情報システムの運用に関する文書の作成に関すること。

⑿　作業員の資格に関すること。

３　システム管理者は、委託先から要員の派遣を受けるときは、必要に応じ、委託先の責任者から秘密保持及び情報資産の適正な取扱いに関する誓約書を提出させるものとする。

４　システム管理者は、委託先が再委託契約を行うときは、再委託先の経営状況等、契約履行が可能であることを確認させなければならない。

（作業者の確認）

第59条　システム管理者は、前条第１項の委託先が大学の管理する施設内で作業をするときは、作業員に身分証明書の提示を求め、作業の資格を有する者であることを確認するものとする。

２　システム管理者は、前条第１項の委託先が大学の管理する施設以外の施設で作業をするときは、必要に応じ立ち入り検査等を行い、作業の資格を有する者が作業をしていることを確認するものとする。

（情報システム開発・保守環境管理）

第60条　システム管理者は、情報システムの開発・保守環境（情報システムの開発又は保守を行う場所、設備等のことをいう。）について、運用システムと分離し、開発・保守環境で使用する情報資産を厳重に保護するものとする。

（操作マニュアル）

第61条　システム管理者は、明確で文書化された情報システムの操作マニュアルを作成し、保管するものとする。

２　システム管理者は、前項の操作マニュアルを必要に応じて見直すものとする。

（運用変更の管理）

第62条　システム管理者は、情報処理施設及び情報システムの変更について、記録の作成及び管理を行うものとする。
２　職員は、原則として情報システムで使用する情報機器の増設及び変更を行ってはならない。ただし、システム管理者が必要と認め、情報機器の増設及び変更を許可した場合については、この限りではない。
（職務及び責任領域の分離）
第63条　システム管理者は、情報システムの管理に携わる職員の職務の領域を明確にし、職員に相互監視を行わせ、職員の活動を監視し、及び監査するものとする。
（容量、能力の計画）
第64条　システム管理者は、情報システムの処理能力及び記憶容量の現状を把握し、将来必要とされる処理能力及び記憶容量を予測し、十分な処理能力及び記憶容量の利用を可能にする措置をとるものとする。
（情報システムの導入）
第65条　システム管理者は、新しい情報システムを導入するとき又は情報システムに性能を向上させるための変更を行ったときは、当該情報システム上にプログラムの誤りがないことを試験により確認しなければならない。
２　システム管理者は、新しい情報システムを導入するとき又は情報システムに性能を向上させるための変更を行ったときは、運用する上で関係する他の情報システムとの整合性を確認するものとする。
３　システム管理者は、第１項の試験により情報セキュリティに重大な影響を及ぼすプログラムの誤りが発見されたときは、当該プログラムの誤りを速やかに修正しなければならない。
（情報資産のバックアップ）
第66条　システム管理者は、セキュリティレベル３の情報資産の中でも特に重要な情報資産について、バックアップ（通常使用している記憶媒体にある情報資産が使用できなくなった場合に備えて、情報資産を通常使用している記憶媒体とは別のものに保存することをいう。以下同じ。）を定期的に実施するものとする。
（ログの保存）
第67条　システム管理者は、セキュリティレベル３の情報資産の中でも特に重要な情報資産を扱う情報システムについて、ログ及び情報セキュリティの確保に必要な記録を取得し、関係所属長と協議の上、一定の期間適切に保存するものとする。
（運用・障害記録）
第68条　システム管理者は、情報システムの整備作業を記録し、一定の期間保存するものとする。
２　システム管理者は、情報システムに障害が発生したときは、当該障害の内容を記録し、重大な障害については、情報セキュリティ責任者及び情報管理委員会事務局に報告しなければならない。
（時計の同期）
第69条　システム管理者は、正確なログを取るため、情報システム内の情報機器の時計を定期的に同期化（２つ以上の時計を同一の時刻にあわせることをいう。）しなければならない。
（情報資産の外部提供の制限）
第70条　システム管理者は、情報資産を外部に提供してはならない。ただし、和歌山県情報公開条例（平成13年和歌山県条例第２号）に基づく開示請求によるときのほか、当該情報資産を提供することが法令等に違反しない場合で、次の各号のいずれかに該当し、情報管理者の許可を受けたときはこの限りではない。
⑴　提供することにより個人又は法人その他の団体の権利利益を侵害するおそれがないと認められるとき。
⑵　国の行政機関又は他の地方公共団体に提供するときで、当該機関の業務遂行のため、特に必要があると認められるとき。
⑶　公共の利益のために必要であると認められるとき。
⑷　専ら統計業務を目的とするもので、特定の個人が識別できない状態で使用されるとき。
２　前項ただし書きの規定により、情報資産を外部に提供するときは、次の各号に掲げる事項を明記した契約あるいは文書を取り交わすものとする。ただし、前項第２号に該当する場合はこの限りではない。
⑴　情報資産の内容及び範囲に関すること。
⑵　情報資産の使用目的に関すること。
⑶　情報資産の提供期間に関すること。
⑷　情報資産の秘密保持に関すること。
⑸　情報資産の目的外の使用及び第三者への提供の禁止に関すること。
⑹　情報資産の複写及び複製の禁止に関すること。
⑺　情報資産の返還又は廃棄に関すること。
⑻　事故発生時における報告義務に関すること。
⑼　損害賠償請求に関すること。

（公開情報）
第71条　情報管理者は、Ｗｅｂ等により、情報資産をインターネット経由で外部に公開するときは、　情報セキュリティ管理者に公開の許可を受けなければならない。
２　システム管理者は、公開した情報資産の改ざんを防止する等、正しい情報資産を維持するための措置をとるものとする。
（業務目的以外の使用禁止）
第72条　職員は、私用でＷｅｂを閲覧し、又は電子メールを使用する等、情報システムを業務目的以外に使用してはならない。
（ダウンロードの制限等）
第73条　職員は、安全の確認できないインターネット上のプログラム及びソフトウェアをダウンロードしてはならない。
２　職員は、出所不明のプログラム及び実行後に情報システムを破壊する等の恐れがあると考えられるプログラムを実行してはならない。
（ソフトウェア導入の許可）
第74条　職員は、ソフトウェアを情報システムに導入するときは、システム管理者の許可を受けなければならない。
（事前検査）
第75条　職員は、記憶媒体で受け取ったファイル又はネットワーク経由で受け取ったファイルを開くときは、事前にウィルス検査を行わなければならない。
（感染の通報）
第76条　職員は、情報システムを構成する情報機器がウィルスに感染したときは、速やかにシステム管理者に報告しなければならない。
（システム管理者の指示）
第77条　職員は、情報システムの使用に当たり、システム管理者の指示を遵守しなければならない。
２　システム管理者は、ウィルス対策等で職員の電子メールの内容、Ｗｅｂの閲覧状況等を職員に調査させるときは、調査させる職員を限定しなければならない。
（セキュリティ情報の収集）
第78条　情報セキュリティ管理者は、情報管理委員会からの通知等により情報セキュリティに関する情報を収集し、セキュリティ確保のために必要な措置をとるものとする。

第６章　緊急時の対応

（緊急時の対応）
第79条　職員は、情報セキュリティ事故の発生等緊急時に対応する場合は、情報セキュリティ管理者の指示に従わなければならない。
（緊急時対応への協力）
第80条　情報管理者は、情報セキュリティ管理者から緊急時に対応するための分析に関して協力の依頼があったときは、協力しなければならない。
（情報セキュリティ事故対策）
第81条　情報セキュリティ管理者は、情報セキュリティ事故が発生した場合に備え、大学の事業及び事務の継続が困難となることのないよう、緊急対応手順、緊急連絡体制、応急措置等を定めた情報セキュリティ事故対応計画を作成しなければならない。

第７章　その他

（所属内の点検）
第82条　情報セキュリティ管理者は、情報セキュリティ責任者の指示により、定期的に、所属内において情報資産が適正に保護され、及び管理されていることを点検するものとする。
（職員以外の準用）
第83条　この要綱は、大学が保有する情報資産を使用する職員以外の者にも準用する。

附　則
１　この要綱は平成30年４月１日から適用する。
２　和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ対策要綱（平成１８年６月６日制定）は、廃止する。

附　則
この要綱は、令和３年４月１日から適用する。

和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針

制　　定　平成30年３月28日
最終改正　令和３年３月29日

序　文

和歌山県立医科大学は、医学、保健看護学及び薬学に関する学術知識について教育、研究するとともに、附属病院においては、質の高い安全な医療の提供、病院運営の効率化のために「総合医療情報システム」を活用して、高度医療を提供している。本学の研究・教育・診療・運営業務については、近年情報通信技術に対する依存度が高まる一方、本学が取り扱う情報には、附属病院の患者の個人情報のみならず大学運営上重要な情報が含まれており、漏洩、損壊等の事故があった場合に極めて重大な結果を招く可能性がある。

また、不正アクセス、マルウェアなどの外部からの脅威も高度化しており、さらに内部職員又は業務受託事業者等による機密情報又は個人情報の漏洩・悪用の可能性も皆無とはいえず、ネットワーク及び情報システムに関する情報セキュリティ管理の重要性がますます高まっているところである。

そこで、本学は、県民等が安心・信頼して本学の提供するサービスを利用することができるようにするとともに、本学における継続的かつ安定的な大学運営業務の実施を確保するために、情報セキュリティ管理に関する総合的、体系的かつ具体的な対策を和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）として定める。

情報セキュリティポリシーとは、情報資産の機密性（秘密を守る）、完全性（改ざんされない）、可用性（サービスが停まらない）という３つの情報セキュリティの要素を一定以上に保ち、維持するためのルールである。情報セキュリティポリシーは、本学の情報資産をさまざまな脅威から守るための基本的な考え方（基本方針）と基本方針を実現するために、組織的、技術的、物理的、人的に何をやらなければならないかという基準（管理要綱）から構成される。

本学構成員は、このルールを理解し、遵守するとともに、情報セキュリティ管理は本学構成員ひとりひとりの責任であることを自覚しなければならない。

第１章　和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針の目的

第１節　基本方針の目的

和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針（以下「基本方針」という。）は、情報セキュリティポリシーを構成し、和歌山県立医科大学（以下「大学」という。）の職員（非常勤職員、準職員及び臨時職員を含む。）及び学外受託者（大学の業務に従事する派遣会社社員、協力会社社員及び業務受託会社社員）など、情報資産を扱う者全員が従うべき、情報セキュリティを確保するための基本的な考え方であり、情報セキュリティポリシーの適用範囲や取扱い、人と組織の役割と責任、情報セキュリティ対策の基本的な方向性等を定めるものである。

第２節　適用範囲

第１項　組織

情報セキュリティポリシーの適用範囲は、大学の全ての部署とする。

第２項　ネットワーク

大学で使用されるコンピュータを接続する情報通信機器及び通信回線とする。

第３項　情報システム

大学で使用されるネットワーク、ハードウェア、ソフトウェア及び記憶媒体で構成された情報を処理する仕組みとする。

第４項　情報資産

情報セキュリティポリシーが適用される情報資産は以下のものとする。

⑴　大学で使用されるネットワーク及び情報システムの開発に関わる文書、図画、写真、フィルム並びに電磁的記録

⑵　大学で使用されるネットワーク及び情報システムで取り扱う電磁的記録

⑶　大学で使用されるネットワーク及び情報システムの運用に関わる文書及び図画で、和歌山県立医科大学文書処理規程第２条に規定するものを除く。

第２章　基本的な考え方

第１節　情報資産に対する脅威

情報資産に対する脅威の発生度合や発生した場合の影響を考慮し、特に備えるべき脅威を次のとおりとする。

⑴　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏洩・破壊・消去等

⑵　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏洩・破壊・改ざん・消去、重要情報の詐取、内部不正等

⑶　地震、落雷、火災等の災害によるサービス及び業務の停止等

⑷　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

⑸　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

第２節　情報資産の保護

前節の脅威から情報資産を保護するため、以下の方策を講ずるものとする。

⑴　物理的方策

サーバ及びその設置エリア、通信回線等並びに職員の使用するパソコン等の管理について物理的に必要な方策を講じる。

⑵　人的方策

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的に必要な方策を講じる。

⑶　技術的方策

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的に必要な方策を講じる。

⑷　運用上の方策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面で必要な方策を講じるものとする。

第３章　情報セキュリティポリシーの取扱い

第１節　基本方針

基本方針は、大学のネットワーク及び情報システム内の情報を安全に管理するために、全ての使用者が守るべき方針とする。

第２節　管理要綱

基本方針に基づいて情報セキュリティを確保するに当たり、遵守すべき行為、判断などの基準を統一的に定めるために、必要となる基本要件を明記した管理要綱を策定する。

要綱は、大学の情報資産を取り扱う全ての職員及び学外受託者に対し、周知徹底する。

第３節　点検

情報セキュリティ管理者等は、情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうか、定期的に点検を行う。

第４節　情報セキュリティポリシーの改正

情報セキュリティを取り巻く状況の変化に迅速に対応するため、情報セキュリティ点検の結果なども踏まえ、情報セキュリティポリシーは定期的に見直し、必要に応じて改正する。

第４章　人と組織

第１節　職掌上の役割と責任

第１項　学長の役割と責任

学長は、セキュリティに関する指針を明らかにし、職員及び学外受託者に対してセキュリティ意識を浸透させ、必要な指示をする役割と責任を持つ。

第２項　所属長の役割と責任

所属長は、セキュリティ確保の責任を負い、所属部署の職員及び業務関係者が、情報セキュリティポリシーを理解し遵守することを徹底し、かつ管理する。

また、所属長は、所属部署の職員が退職、転出又は業務変更する場合、利用する必要のなくなった全ての情報資産を回収する責任を持つ。また、学外受託者が契約終了した場合も同様である。

第３項　職員の役割と責任

職員は、法令、情報セキュリティポリシー及び所属長の指示等を遵守し、情報が不正な手段で取得されること又は不正に使用されることを防止する責任がある。

職員は、退職、転出又は業務変更する場合に利用する必要のなくなった全ての情報資産を大学に返却しなければならない。

職員は、自己責任の原則に基づいてネットワーク及び情報システムの利用を行うことを十分理解しなければならない。

第４項　職員以外の者（学外受託者等）の役割と責任

学外受託者は、業務委託契約等に反しない範囲で、前項の役割と責任を負う。

第２節　セキュリティの管理体制及び組織

大学の保有する情報資産について、統一的な情報セキュリティを確保するため、全学的な管理体制を以下のとおりとする。

第１項　管理体制

⑴　情報セキュリティ総括責任者

大学におけるセキュリティ責任者を総括し、セキュリティを含む情報管理全般に関する最高責任者であり、全ての責任及び権限を有する。学長がその任に当たる。

⑵　情報セキュリティ責任者

ア　各部署における情報セキュリティに関する責任と権限を有し、情報セキュリティ管理者に指示する。次の者がその任に当たる。

学生部長、医学部長、保健看護学部長、薬学部長、附属病院長、紀北分院長、産官学連携推進本部長、地域・国際貢献推進本部長及び事務局長

イ　各部署における情報セキュリティに関する責任と権限を有し、所属の職員に対し情報セキュリティ活動の指導及び監督を行う。次の者がその任に当たる。

教育研究開発センター長、入試・教育センター長、図書館長、共同利用施設長、助産学専攻科長、みらい医療推進センター長、健康管理センター長、ワークライフバランスセンター長、看護キャリア開発センター長及び危機対策室長

⑶　情報セキュリティ管理者

情報セキュリティ責任者の指示の下、各所属の職員に対し情報セキュリティ活動の指導及び監督を行う。各所属長がその任に当たる。

第２項　組織

⑴　情報管理委員会

ア　大学のネットワーク及び情報システムに係る情報セキュリティに関する重要な事項を調査、検討、審議し決定する。

イ　情報管理委員会は、和歌山県立医科大学情報管理委員会規程（以下、「情報管理委員会規程」という。）で定める者で構成する。

ウ　情報管理委員長は、情報セキュリティに関する重要な方針等を審議した場合、情報セキュリティ総括責任者に報告する。

⑵　情報管理委員会事務局

情報管理委員会事務局は、情報管理委員会規程に定める。

第３項　情報管理者

主管する業務において、情報収集、作成又は県民等から情報を預託された部署の所属長を情報管理者とする。

情報管理者は、自ら所有する情報資産の保護管理要件を定め、情報の使用者を決定する。

第３節　セキュリティに関する教育等

情報セキュリティ管理者等は、情報セキュリティポリシーの職員等への浸透と情報セキュリティ意識向上のため、情報セキュリティに関する教育・啓発を実施する。

第４節　第三者による情報資産使用に関する方針

大学の情報資産を、当該情報を大学に預託した本人以外の第三者に使用させる場合は、事前に当該情報の情報管理者の承認を必要とする。

情報資産のうち、特に個人情報の取扱いについては、個人情報保護法、和歌山県個人情報保護条例及び関係法令の規定を遵守すること。

第５章　情報資産の分類

第１節　セキュリティレベルの設定

情報セキュリティ管理者は、情報資産の重要度に応じて、機密性、完全性及び可用性を維持するために、セキュリティレベルを設定する。

セキュリティレベルごとに情報資産の保護管理要件を明確にし、想定されるリスク及びその対策を明確にする。

第２節　情報資産の分類

情報管理者は、自らが所管する情報資産を重要度に応じてセキュリティレベルに分類する。必要な場合は、追加の保護管理要件を設定することができる。

第６章　情報セキュリティの確保

情報セキュリティを確保するため、セキュリティレベルに応じて、情報の機密性、完全性及び可用性を維持するものとし、物理、技術及び運用の面から以下の方策を行う。

第１節　物理的方策

第１項　情報資産

セキュリティレベルに応じ、情報資産の保管等に関し必要な方策を講じなければならない。

第２項　情報システム

情報システム内で取り扱う情報資産のセキュリティレベルに応じ、情報システムを構成する機器の設置環境、物理的アクセス等に関し必要な方策を講じなければならない。

第３項　ネットワーク

ネットワーク内を通過する情報資産のセキュリティレベルに応じ、ネットワークを構成する機器の設置環境等に関し必要な方策を講じなければならない。

第２節　技術的方策

第１項　情報資産

セキュリティレベルに応じ、情報資産の保護のため、情報漏洩の防止等について必要な方策を講じなければならない。

第２項　情報システム

情報システム内で取り扱う情報資産のセキュリティレベルに応じ、利用者の識別方法、アクセス制御方法等に関し必要な方策を講じなければならない。また、システム開発及び保守に関するセキュリティ要件を明確にしなければならない。

第３項　ネットワーク

ネットワーク内を通過する情報資産のセキュリティレベルに応じ、ネットワークの経路制御等に関し必要な方策を講じなければならない。

第３節　運用上の方策

第１項　情報資産

情報資産のセキュリティレベルに応じ、データの取扱い、保管、使用、バックアップ等運用上の管理に関し必要な方策を講じなければならない。

第２項　情報システム

⑴　情報システム内で取り扱う情報資産のセキュリティレベルに応じて、操作手順書等を作成し、適切に管理運用しなければならない。

⑵　情報機器の設置、廃棄及び構成の変更について、管理手順を定め適切な管理を行わなければならない。

⑶　情報システムのセキュリティレベルに応じて、不正アクセスや障害検知等のための監視を行わなければならない。

⑷　情報セキュリティ管理者は、所管する情報システムのセキュリティを確保するための情報を収集し、必要な方策を講じなければならない。

第３項　ネットワーク

⑴　ネットワーク内を通過する情報資産のセキュリティレベルに応じて運用手順書等を作成し、適切に管理運用しなければならない。

⑵　ネットワーク機器の設置、廃棄及び構成の変更について、管理手順を定め適切な管理を行わなければならない。

⑶　ネットワーク内を通過する情報資産のセキュリティレベルに応じて、不正アクセスや障害検知等の監視を行わなければならない。

第７章　緊急時の対応

情報セキュリティ管理者は、主要業務毎にセキュリティレベルに基づいた緊急対応手順・緊急連絡体制・応急措置・バックアップ手順・業務再開手順等を含む情報セキュリティ事故対策マニュアルを作成する。

附　則

１　この基本方針は、平成30年４月１日から適用する。

２　和歌山県立医科大学ネットワーク及び情報システムに関わる情報セキュリティ基本方針（平成18年６月６日制定）は、廃止する。

附　則

この基本方針は、令和３年４月１日から適用する。