**用語集**

|  | 用　語 | 説　明 | 定義文書 |
| --- | --- | --- | --- |
| A | A大学全学認証基盤 | A大学における教育研究、福利厚生のためのサービスを提供する際に必要となる、利用者認証と主体認証情報の提供を行う情報システムをいう。 | C2601 |
|  | A大学認証局 | A大学電子認証局ポリシー及び運用規則に定める認証局をいう。 | C2601 |
| B | BCP（Business Continuity Plan: 事業継続計画) | 組織において特定する事業の継続に支障を来すと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適切に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。狭義には、このうちの事態発生後の事業の維持を主とした計画をいう。 | C2502 |
| C | CRYPTREC | Cryptography Research and Evaluation Committeesの略称であって、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。 | C2502 |
|  | CSIRT | 本学において発生するインシデントに対処するために設置された体制をいう。Computer Security Incident Response Teamの略。 | C2501 |
| D | DNSサーバ | 名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させる電子計算機をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の二種類に分けることができる。 | C2502 |
| I | ICカード | C2101-02情報システム運用・管理規程第二条三十八に定める主体認証情報格納装置のうち、主体認証情報をICに格納するものをいう。 | C2601 |
|  | IPv6移行機構 | 物理的にひとつのネットワークにおいて、IPv4技術を利用する通信とIPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、電子計算機や通信回線装置が２つの通信プロトコルを併用するデュアルスタック機構や、相互接続性のない２つのIPv6ネットワークを既設のIPv4 ネットワークを使って通信可能とするIPv6-IPv4トンネル機構等がある。 | C2502 |
|  | ISP | Internet Service Providerの略称であり、インターネットへの接続サービスを提供する事業者のことをいう。 | － |
| M | MACアドレス | 機器等が備える有線LAN や無線LAN のネットワークインタフェースに割り当てられる固有の認識番号である。識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割り当てる番号の組み合わせによって表される。 | C2502 |
| P | PIN | 電子証明書を格納したICカードを使った主体認証時に使われる主体認証情報をいう。Personal Identification Numberの略。 | C2601 |
| S | S/MIME | 公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。 | C2502 |
|  | SNS | Social Network Serviceの略称であり、会員による社会的コミュニケーションを目的とした情報交換や情報共有のためのサービスをいう。 | － |
| U | UPKI電子証明書発行サービス | 大学共同利用機関法人情報・システム研究機構国立情報学研究所（NII）の事業として実施されている、高等教育機関等を対象とした電子証明書発行サービスをいう。 | C2501 |
|  | URI | http://wwww.example.com/のようなウェブサイトをアクセスするためのキーとなる情報。URL（Universal Resource Locator）と呼ぶことも普通におこなわれている。 Universal Resource Identifierの略。 | － |
|  | URL | http://wwww.example.com/のようなウェブサイトをアクセスするためのキーとなる情報。URI（Universal Resource Identifier）と呼ぶこともある。 Universal Resource Locatorの略。 | － |
| V | VPN | 暗号技術等を利用し、インターネットなどの公衆回線を私設通信回線として広域化するための技術をいう。Virtual Private Networkの略。 | C2502 |
| あ | アイデンティティ情報 | 利用者に関する全学アカウントおよび属性情報を総称する情報をいう。 | C2601 |
|  | アクセス制御 | 情報へのアクセスを許可する者を制限することをいう。 | C2502 |
|  | アプリケーション | オペレーティングシステム上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。 | C2502 |
|  | アルゴリズム | ある特定の目的を達成するための演算手順をいう。 | C2502 |
|  | 暗号化 | 第三者に容易に解読されないよう、定められた演算を施しデータを変換することをいう。 | C2502 |
|  | 暗号モジュール | 暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。 | C2502 |
| い | 委託先 | 外部委託により本学の情報処理業務の一部又は全部を実施する者をいう。 | C2501 |
|  | インシデント | 情報セキュリティに関し、意図的または偶発的に生じる、本学規程または法律に反する事故あるいは事件をいう。 | C1001 |
|  | 物理的インシデント、セキュリティインシデントまたはコンテンツインシデントを言う。 | C3102 |
| う | ウェブクライアント | ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。 | C2502 |
|  | ウェブサーバ | HTTP サーバアプリケーション、当該サーバアプリケーションで動作するウェブアプリケーション及びデータベース並びに負荷分散装置等のようにウェブサーバと一体として動作するハードウェアをいう。 | － |
|  | 受渡業者 | 事務従事者との物品の受渡しを目的とした者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。 | C2502 |
| か | 外部委託 | 本学の情報処理業務の一部又は全部について、契約をもって学外の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。 | C2501 |
|  | 学外 | 本学が管理する組織又は施設の外をいう。 | － |
|  | 学外クレーム | 学内の利用者等による情報発信行為（本学の業務としてなされたものを除く）の問題を指摘しての連絡・通報及び学外(学内の者が、弁護士等の代理人を立てる場合も含む)からの発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び証拠、証言の収集や犯罪捜査等にかかわる協力要請や強制的命令を言う。 | C3102 |
|  | 学外通信回線 | 一つの本学が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、当該高等教育機関の管理下にないサーバ装置又は端末が論理的に接続されていないものをいう。学内通信回線には、専用線やVPN等物理的な回線を本学が管理していないものも含まれる。 | C2501 |
|  | 学外窓口 | インシデントについて学外から連絡・通報を受け、学外への連絡・通報、対外クレームをするための窓口を言う。 | C3102 |
|  | 学生等 | 本学通則に定める学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。 | C1001 |
|  | 学内 | 本学が管理する組織又は施設の内をいう。 | － |
|  | 学内通信回線 | 物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本学管理又は他組織管理）及び通信回線装置を問わず、本学が管理する電子計算機を接続し、当該電子計算機間の通信に利用する論理的な通信回線をいう。 | C2501 |
|  | 可用性 | 情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。 | C2502 |
|  | 可用性１情報 | 可用性２情報以外の情報（書面を除く。）をいう。 | C2103 |
|  | 可用性２情報 | 本学で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者等の権利が侵害され又は本学の活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。 | C2103 |
|  | 完全性 | 情報が破壊、改ざん又は消去されていない特性をいう。 | C2502 |
|  | 完全性１情報 | 完全性２情報以外の情報（書面を除く。）をいう。 | C2103 |
|  | 完全性２情報 | 本学で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者等の権利が侵害され又は本学の活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。 | C2103 |
| き | 機器等 | 情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。 | C2501 |
|  | 機密性 | 情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。 | C2502 |
|  | 機密性１情報 | 情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報をいう。 | C2103 |
|  | 機密性３情報 | 本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報をいう。 | C2103 |
|  | 機密性２情報 | 本学で取り扱う情報のうち、独立行政法人の保有する情報の公開に関する法律（平成13年12月5日法律第140号）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報をいう。 | C2103 |
|  | 教職員等 | 本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局総括責任者が認めた者をいう。 | C1001 |
|  | 業務継続計画 | 本学において策定されているBCP（Business Continuity Plan: 事業継続計画）をいう。 | C2502 |
|  | 共用識別コード | 複数の主体が共用することを想定した識別コードをいう。原則として、１つの識別コードは１つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。 | C2502 |
|  | 記録媒体 | 情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R等の外部電磁的記録媒体がある。 | C2501 |
|  | 緊急連絡網 | 運用・管理規程に基づき整備された［インシデント/障害等]に備え、特に重要と認めた情報システムについて、その部局技術責任者及び部局技術担当者の緊急連絡先、連絡手段、連絡内容を含む連絡網を言う。 | C3102 |
| け | 権限管理 | 主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。 | C2502 |
| こ | コンテンツインシデント | ネットワークを利用した情報発信内容（以下「コンテンツ」という）が著作権侵害等の他人の権利侵害や児童ポルノ画像の公開等の違法行為または公序良俗違反である行為(及びその旨主張する被害者等からの請求）による事故を言い、下記原因を含む。  －電子掲示板、ブログやウェブページ等での名誉・信用毀損にあたる情報の発信  －他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信  －通信の秘密を侵害する行為  －他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信  －秘密であるデータやプログラムの不正公開等守秘義務に違反する情報の発信  －児童ポルノやわいせつ画像の公開  －ネットワークを利用したねずみ講  －差別、侮辱、ハラスメントにあたる情報の発信  －営業ないし商業を目的とした本学情報システムの利用行為 | C3102 |
| さ | サーバ装置 | 通信回線等を経由して接続してきた電子計算機に対して、自らが保持しているサービスを提供する電子計算機をいう。 | C2501 |
|  | サービス | サーバ装置上で動作しているアプリケーションにより、接続してきた電子計算機に対して提供される単独又は複数の機能で構成される機能群をいう。 | － |
|  | サービス不能攻撃 | セキュリティホールを悪用しサーバ装置若しくは通信回線装置のソフトウェアを動作不能にさせること、又はサーバ装置、通信回線装置若しくは通信回線の容量を上回る大量のアクセスを意図的に行い通常の利用者のサービス利用を妨害する攻撃をいう。 | C2502 |
|  | 最小限の特権機能 | 管理者権限を実行できる範囲を必要最小限に制限する機能をいう。 | C2502 |
| し | 識別 | 情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。 | C2502 |
|  | 識別コード | 主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザIDが挙げられる。 | C2502 |
|  | 事業継続計画 | →BCP参照 | － |
|  | 実施規程 | ポリシーに基づいて策定される規程及び、基準、計画をいう。 | C1001 |
|  | 実施手順 | 事務情報セキュリティ対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。 | C2501 |
|  | 事務従事者 | 本学の事務に従事している本学のの指揮命令に服している者であって、本学の管理対象である情報及び情報システムを取り扱う者をいう。事務従事者には、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。 | C2501 |
|  | 事務情報 | 事務情報とは情報のうち次のものをいう。 (1) 「法人文書の管理に関する規程」の対象となる法人文書 (2)　(1)以外の法人文書で、部局長が指定した文書 | C1001 |
|  | 事務情報システム | 事務情報を扱う情報システムをいう。 | C1001 |
|  | 主体 | 情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。 | C2502 |
|  | 主体認証 | 識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。 | C2502 |
|  | 主体認証情報 | 主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。 | C2502 |
|  | 主体認証情報格納装置 | 主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、ＩＣカード等がある。 | C2502 |
|  | 情報 | 情報には次のものを含む。 (1)　情報システム内部に記録された情報 (2)　情報システム外部の電磁的記録媒体に記録された情報 (3)　情報システムに関係がある書面に記載された情報 | C1001 |
|  | 情報資産 | 情報システム並びに情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。 | C1001 |
|  | 情報システム | 情報処理及び情報ネットワークに係わるシステムで、次のものをいい、本学情報ネットワークに接続する機器を含む。 (1) 本学により、所有又は管理されているもの (2) 本学との契約あるいは他の協定に従って提供されるもの | C1001 |
|  | 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。 | C1001 |
|  | 情報セキュリティインシデント | JIS Q 27001:2006における情報セキュリティインシデントをいう。 | C2501 |
|  | 情報セキュリティ関係規程 | 事務情報セキュリティ対策基準及び実施手順を総称したものをいう。 | C2501 |
|  | 情報の移送 | 学外に、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体及び書面を運搬することをいう。 | － |
|  | 情報の抹消 | 電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。 | C2502 |
| せ | セキュリティパッチ | 発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。 | C2502 |
|  | セキュリティホール | オペレーティングシステム又はアプリケーション等に存在し、それら自身や処理する情報のセキュリティが侵害される原因となる可能性のある問題をいう。 | － |
|  | 全学アカウント | A大学全学認証基盤で主体認証を行う情報システムにおいて、主体に付与された正当な権限をいう。全学アカウントの付与は、識別コードと主体認証情報の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。 | C2201 |
|  | 全学情報システム | 全学の情報基盤として供される本学情報システムのうち、全学認証基盤を利用可能なものをいう。 | C1000 |
| そ | ソフトウェア | サーバ装置、端末、通信回線装置を動作させる手順及び命令を、電子計算機が理解できる形式で記述したものをいう。オペレーティングシステムやオペレーティングシステム上で動作するアプリケーションを含む広義の意味である。 | C2502 |
|  | 属性情報 | 全学アカウントに付随して管理・提供される利用者に関する情報をいう。 | C2601 |
| た | 対外クレーム | 対内的インシデントに対し、学外の発信者に対して連絡・通報し、または発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び当局に犯罪捜査の告訴・告発をすることを言う。 | C3102 |
|  | 対外的インシデント | インシデントのうち、利用者等による行為であって、外部ネットワークにおけるあるいは外部のシステムに対して行われた行為による事故、事件を言う。 | C3102 |
|  | 代替措置 | 例外措置の適用に伴い発生するリスクを低減するためにポリシー・実施規程・手順が定める内容とは異なる代替のセキュリティ対策をいう。 | C3101 |
|  | 耐タンパ性 | 暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。 | C2502 |
|  | 対内的インシデント | インシデントのうち、外部のネットワークから内部に向かって行われた行為による事故、事件を言う。 | C3102 |
|  | 端末 | 情報システムの構成要素である機器のうち、事務従事者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。 | C2501 |
| つ | 通信回線 | 複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。 | C2501 |
|  | 通信回線装置 | 通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。 | C2501 |
| て | 手順 | 実施規程に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。 | C1001 |
|  | 電子計算機 | コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。 | － |
|  | 電子署名 | 情報の正当性を保証するための電子的な署名情報をいう。 | C2502 |
|  | 電子証明書 | A大学認証局から発行された証明書でログイン時の主体認証等に利用するため証明書をいう。 | C2601 |
|  | 電磁的記録 | 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。 | C1001 |
|  | 電子メールクライアント | 電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。 | C2502 |
|  | 電子メールサーバ | 電子メールの利用者に対する電子メールの送受信のサービス及び電子メールの配送を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。 | C2502 |
| と | 特定用途機器 | テレビ会議システム、IP電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。 | C2501 |
|  | ドメインネームシステム（DNS） | クライアント等からの問合わせを受けて、ドメイン名やホスト名とIPアドレスとの対応関係について回答を行うデータベースシステムである。 | C2502 |
|  | ドメイン名 | 国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.sample.ac.jpというウェブサイトの場合は、sample.ac.jpの部分がこれに該当する。 | C2502 |
|  | 取扱制限 | 情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。 | C2103 |
| な | 名前解決 | ドメイン名やホスト名と IP アドレスを変換することをいう。 | C2502 |
| に | 認証接続 | 認証と認可を目的として、全学情報システム、もしくは部局情報システムがA大学全学認証基盤のアイデンティティ情報を利用することをいう。 | C2601 |
|  | 認証接続システム | A大学全学認証基盤に認証接続された全学情報システムもしくは部局情報システムをいう。 | C2601 |
|  | 認証接続責任者 | 認証接続システムの認証接続に係る責任を有する本学の職員をいう。 | C2601 |
| ひ | 非常事態 | 本学情報システムの運用に関するインシデントのうち特に緊急性を要するものをいう。 | C2102 |
| ふ | フィッシング（phishing） | 悪意ある第三者等が、実在する機関等からのお知らせであるかのように偽装した電子メールを送りつけ、受け取った者にその電子メールに記載されたURL をクリックさせ、あらかじめ用意された偽のウェブサイトに誘導し、ID、パスワード、その他重要な情報を記入させて、情報を窃取するという行為である。 | C2102 |
|  | 不正プログラム | コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。 | C2501 |
|  | 不正プログラム定義ファイル | 不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。 | C2502 |
|  | 物理的インシデント | 地震等の天災、火災、事故、盗難等によるネットワークを構成する機器や回線の物理的損壊や滅失及びその他の物理的原因による情報システムやネットワークの機能不全や障害等、情報セキュリティの確保が困難な事由の発生およびそのおそれを言う。 | C3102 |
|  | 踏み台 | 悪意ある第三者によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。 | C2502 |
| ほ | ポリシー | 本学が定める「C1000 情報システム運用基本方針」及び「C1001 情報システム運用基本規程」をいう。 | C1001 |
|  | 本学支給以外の端末 | 本学が支給する端末の端末をいう。いわゆる私物のPCのほか、本学への出向者に対して出向元組織が提供する端末も含むものとする。 | － |
| む | 無線LAN | IEEE802.11a、802.11b、802.11g、802.11n等の規格により、無線通信で情報を送受信する通信回線をいう。 | C2502 |
| め | 明示等 | 情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。 | C1001 |
| も | モバイル端末 | 端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。 | C2501 |
| や | 約款による外部サービス | 民間事業者等の学外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。 | C2501 |
| よ | 要安定情報 | 可用性２情報をいう。 | C2103 |
|  | 要管理対策区域 | 本学が管理する施設等（外部の組織から借用している施設等を含む。）本学の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。 | C2501 |
|  | 要機密情報 | 機密性２情報及び機密性３情報をいう。 | C2103 |
|  | 要保護情報 | 要機密情報、要保全情報及び要安定情報をいう。 | C2103 |
|  | 要保全情報 | 完全性２情報をいう。 | C2103 |
| り | リスク | 目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。 | C2502 |
|  | 利用者 | 教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。 | C1001 |
|  | 利用者等 | 利用者及び臨時利用者のほか、本学情報システムを取り扱う者をいう。 | C2201 |
|  | 臨時利用者 | 教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。 | C1001 |
| る | ルートヒントファイル | 最初に名前解決を問合わせるDNS コンテンツサーバ（以下「ルートDNS」という。）の情報をいう。ルートヒントファイルには、ルートDNS のサーバ名とIP アドレスの組が記載されており、ルートDNS のIP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルはInterNIC （Internet NetworkInformation Center）のサイトから入手可能である。 | C2502 |
| れ | 例外措置 | 教職員等がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、大学事務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。 | C3101 |
| ろ | ログイン | 何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。 | － |