**用語集**

|  | 用　語 | 説　明 | 定義文書 |
| --- | --- | --- | --- |
| 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。 | D2101 |
|  | CSIRT | 本学において発生するインシデントに対処するため、本学に設置された体制をいう。Computer Security Incident Response Teamの略。 | D1001 |
|  | CYMAT | サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援チーム）の略。 | D2101 |
| 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サーバ装置をいう。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2種類に分けることができる。 | D2101 |
| I | 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、サーバ装置及び端末並びに通信回線装置が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。 | D2101 |
| 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。 | D2101 |
| 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。 | D2101 |
| 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 |
| V | VPN | 暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。Virtual Private Networkの略。 | D2101 |
| W | Web会議サービス | 専用のアプリケーションやウェブブラウザを利用し、映像または音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。 | D2101 |
| あ | アクセス制御 | 情報又は情報システムへのアクセスを許可する主体を制限することをいう。 | CD101 |
|  | アプリケーション | OS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。 | D2101 |
|  | アプリケーション・コンテンツ | アプリケーションプログラム、ウェブコンテンツ等の総称をいう。 | D2101 |
|  | 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。 | D2101 |
|  | 暗号化 | 第三者が容易に復元することができないよう、定められた演算を施しデータを変換することをいう。 | D2101 |
|  | 暗号化消去 | 情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。 | D2101 |
|  | 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。 | D2101 |
| 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。 | D2101 |
|  | 受渡業者 | 教職員等との物品の受渡しを行う者をいう。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。 | D2101 |
|  | 運用監視暗号リスト | CRYPTRECが発行する「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」において、危殆化等により推奨すべきではないが、互換性維持のために継続利用を容認するものをいう。 | D2101 |
| か | 外部サービス | 学外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において本学の情報が取り扱われる場合に限る。 | D1001 |
|  | 外部サービス管理者 | 外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。 | D1001 |
|  | 外部サービス提供者 | 外部サービスを提供する事業者をいう。外部サービスを利用して本学に向けて独自のサービスを提供する事業者は含まれない。 | D1001 |
|  | 外部サービス利用者 | 外部サービスを利用する本学の利用者等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。 | D1001 |
|  | 学外通信回線 | 通信回線のうち、学内通信回線以外のものをいう。 | D2101 |
|  | 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。 | D1001 |
|  | 学内通信回線 | 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、本学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。 | D2101 |
|  | 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。 | D2101 |
|  | 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。 | D2102 |
|  | 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。 | D2102 |
|  | 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。 | D2101 |
|  | 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。 | D2102 |
|  | 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。 | D2102 |
| 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。 | D1001 |
|  | 基盤となる情報システム | 学外の機関等と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。 | D2101 |
|  | 基本規程 | 本学が定める「D1001 情報セキュリティ対策基本規程」をいう。 | D2101 |
|  | 基本方針 | 本学が定める「D1000 情報セキュリティ対策基本方針」をいう。 | D2101 |
|  | 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。 | D2101 |
|  | 機密性１情報 | 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。以下、「独立行政法人等情報公開法」という。）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。 | D2102 |
|  | 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。 | D2102 |
|  | 機密性２情報 | 本学で取り扱う情報のうち、独立行政法人等情報公開法第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む情報であって、「機密性３情報」以外の情報をいう。 | D2102 |
|  | 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。教職員等には、個々の勤務条件にもよるが、派遣労働者、一時的に受け入れる研修生等も含まれている。 | D1001 |
|  | 業務委託 | 本学の業務の一部又は全部について、契約をもって外部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。ただし、当該業務において本学の情報を取り扱わせる場合に限る。 | D1001 |
|  | 業務継続計画 | 本学において策定される、発災時に非常時優先業務を実施するための計画をいう。広義には、平常時からの取組等や復旧に関する計画も含まれる。 | D2101 |
|  | 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、一つの識別コードは一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。 | D2101 |
|  | 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。 | D1001 |
| く | 国の行政機関 | 法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。 | D2101 |
|  | クラウドサービス | 事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、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いう。 | D2101 |
| 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。 | D2101 |
| さ | サーバ装置 | 情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（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。 | D1101 |
|  | サービス不能攻撃 | 悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又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や、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを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。 | D2101 |
|  | 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。 | D2101 |
| 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。 | D2101 |
|  | 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。 | D2101 |
|  | 実施手順 | 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。 | D1101 |
|  | 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。 | D2101 |
|  | 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。 | D2101 |
|  | 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。 | D2101 |
|  | 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。 | D2101 |
|  | 情報 | 「高等教育機関の情報セキュリティ対策のためのサンプル規程集」において適用対象とする情報は、以下とする。  (1)　教職員等が職務上使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）  (2)　その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報  (3)　(1)及び(2)のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報 | D1001 |
|  | 情報システム | ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む）をいう。 | D1001 |
|  | 情報セキュリティインシデント | JIS Q 27001:2019における情報セキュリティインシデントをいう。 | D1001 |
|  | 情報セキュリティ関係規程 | 対策基準及び実施手順を総称したものをいう。 | D1001 |
|  | 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、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、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。 | D2101 |
| す | 推奨候補暗号リスト | CRYPTREC暗号リストにおいて、安全性及び実装性能は確認されているが、利用実績や普及見込みが十分ではないものをいう。 | D2101 |
| 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。 | D2101 |
| そ | ソーシャルメディアサービス | インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していくものをいう。 | D2101 |
|  | 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、当該サーバ装置等が理解できる形式で記述したものをいう。OSやOS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。 | D2101 |
| た | 対策基準 | 本学における情報及び情報システムの情報セキュリティを確保するための対策の基準として定める「D2101 情報セキュリティ対策基準」をいう。 | D1001 |
|  | 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。 | D2101 |
|  | 端末 | 情報システムの構成要素である機器のうち、利用者等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。特に断りを入れた例としては、本学が調達又は開発するもの以外を指す「本学支給以外の端末」がある。また、本学が調達又は開発した端末と本学支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。 | D1001 |
| 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。 | D1001 |
|  | 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。 | D1001 |
| て | 手順等 | 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などをいう。 | － |
|  | テレワーク | 情報通信技術（ ICT ＝ Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のことをいう。テレワークの形態は、業務を行う場所に応じて、自宅で業務を行う在宅勤務、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。 | D2101 |
|  | 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。 | D2101 |
|  | 電子政府推奨暗号リスト | CRYPTREC暗号リストにおいて、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストをいう。 | D2101 |
|  | 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。 | D2101 |
|  | 電子メールサーバ | 電子メールの送受信、振り分け、配送等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。 | D2101 |
| 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、入退管理システム、施設管理システム、環境モニタリング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。 | D2101 |
|  | 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システムである。 | D2101 |
|  | 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。 | D2101 |
|  | 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、読後廃棄その他の情報の適正な取扱いを利用者等に確実に行わせるための手段をいう。 | D2101 |
| 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。 | D2101 |
| ふ | 複合機 | プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。 | D2101 |
|  | 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。 | D2101 |
|  | 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。 | D2101 |
|  | 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。 | D2101 |
| ほ | ポリシー | 本学が定める「D1000 情報セキュリティ対策基本方針」及び「D1001 情報セキュリティ対策基本規程」をいう。 | D1001 |
| む | 無線LAN | IEEE802.11a、802.11b、802.11g、802.11n, 802.11ac, 802.11ad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。 | D2101 |
| 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。 | D2101 |
| も | モバイル端末 | 端末のうち、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。 | D1001 |
| よ | 要安定情報 | 可用性２情報をいう。 | D2101 |
|  | 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。 | D2101 |
|  | 要機密情報 | 機密性２情報及び機密性３情報をいう。 | D2101 |
|  | 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。 | D2101 |
|  | 要保全情報 | 完全性２情報をいう。 | D2101 |
| 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。 | D2101 |
|  | 利用者 | 教職員等及び学生等で、本学の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。 | D1001 |
|  | 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。 | D2101 |
|  | 臨時利用者 | 教職員等及び学生等以外の者で、本学の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。 | D1001 |
| れ | 例外措置 | 利用者等がポリシー並びにそれに基づく規程等を遵守することが困難な状況で、教育研究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。 | D2101 |