（ガイドライン別紙）電子データの機密性の具体例と取り扱うシステムで満たすべきセキュリティ

このガイドラインの対象は本学の教育・研究、大学業務に関わる電子データであり、各所属員個人に属するデータは対象としない

機密性	概要	具体例	取り扱うシステムで満たすべきセキュリティ対策
機密性Ⅰ	公開されても支障がなく、かつ以下の条件に該当するもの ・改ざんが行われても重大な被害がない ・所有権が移転しても支障がない	・打ち合わせやスケジュール調整等の情報（個人が特定されるような情報を含まない物） ・その他個人が特定されるような情報が含まれない、雑多な情報	ウィルス・マルウェアの感染に注意する。
機密性Ⅱ	公開を前提としたもの	・広報用Webページでの公開している情報 ・広報用のSNS等に掲載する公開している情報 ・公開を前提とした教育・研究に関する情報（教員業績DB、シラバス、オープンコースウェア、公開用の研究データ・研究成果） ・公開を前提としたライブ配信データ ※データ内の画像・動画・資料等については権利処理（著作権・肖像権）がすべて明確に完了していることが前提となる ・構成員以外の者も利用できるシステムのマニュアル	【クラウドサービスを用いる場合】 ①第三者評価・認定制度の認証（ISO/IEC 27017、SOC2等）を取得している業者のサービスを選定する。 ②データの所有権について第三者に移転しないサービスであることを確認する。
機密性Ⅲ	公開を前提としていないもの	・研究室の卒業生の進路情報 ・受託研究等、学外の組織が関わるものの中でも機密性が低い情報 ・研究に関する情報のうち、万が一漏えいしたとしても影響が軽微なもの ・ファイルにエクスポートされたメールデータでのうち機密性Ⅳ、Ⅴの内容を含まないもの ・本学、ならびに五島育英会の規程 ・授業や学内のイベントを収録した動画データ ・将来的に公開することを前提とした情報の原稿（作成途中のWebページの原案やシラバスの原稿等） ・学生に提示する教材 ・学生から提出されるレポート ・その他教育・研究の為に用いる情報で、機密性Ⅳ、Ⅴの内容を含まないもの ・学外機関からの依頼を受けて作成した情報で、機密性Ⅳ、Ⅴの内容を含まないもの ・構成員のみが利用できるシステムのマニュアル	機密性Ⅱの対策に加え ①パスワード等、1要素以上のアクセス制限を行う。 ②通信経路の暗号化（SSL、SSH等）に対応したシステムを選定する。
機密性Ⅳ	特定の職制，グループ又は部局等以外に対して機密を保持すべきもの	・住所、氏名、生年月日、メールアドレス、電話番号など一般的な個人情報が集積されたもの 例） 本学学生教職員の個人情報、学外者（本学で実施した催し物の参加者等）の個人情報、入学予定者の情報 ・学生指導の過程を記載したデータ ・受託研究等、学外の組織が関わるものの中でも機密性が高い研究に関する情報 例） 国の機関が関わる受託研究のデータや、漏洩することで共同研究者に損害を与える可能性のある研究データ ・入試情報・財務情報等、本学の経営の根幹に関わる情報 例） 入試に関わる非公開情報、 本学の戦略に関わる非公開情報	機密性Ⅲの対策に加え ①パスワードによる認証に加え、何らかの追加のアクセス制限（2要素認証、2重認証、ネットワーク的な制限等）を施す。 ②アクセスの為に必要な情報（ID・パスワード・システムのURL等）について、特定の職制・グループ以外が知り得ないよう厳密に管理したうえで、アカウントと実在する人物の対応が明確になるよう運用する。 【クラウドサービスを用いる場合】 ①個人向けではなく法人向けとしてリリースされており、かつ、十分な利用実績が公開されているサービスを選定する。 ②準拠法・管轄裁判所が国内となっているサービスを選定する。
機密性Ⅴ	特定の関係者以外に対し厳重に機密を保持すべきもの	・成績原簿に関する情報 例） 学生の成績データ ・人事評価等、機密性の高い人事情報 例） 人事評価 ・医療に関する情報 ・決済に関わる情報 例） クレジットカード番号（ならびにセキュリティコードなど付随する情報）、銀行口座番号等 ・個人に割り当てられた公的なIDに関する情報 例） マイナンバー、パスポート番号、ビザ番号、社会保険番号など	機密性Ⅳの対策に加え ①電子証明書等、ID・パスワード以外の要素を加えた認証を用いる。 【クラウドサービスを用いる場合】 ①別表：ネットワーク的な制限とサービスの分離度に関する点数評価　にて6点以上の評価を獲得しているサービスを選定する。

別表：ネットワーク的な制限とサービスの分離度に関する点数評価（以下に挙げられている要件で該当するもの（複数選択可）の加点を合計して評価を算出する）

カテゴリ	要件	加点
ネットワーク的な制限	サービスで本来使用するポートでのみ接続可能である。	1
	学内ネットワークからのみ利用できるよう制限されているが、それ以上の制限はされていない。	2
	アクセス可能なIPアドレス範囲が、学内ネットワークより細かい必要最低限の範囲に限定されている。	4
	ダイアルアップ等専用の接続サービスを用いないと接続できない	6
サービスの分離度	同一のサービスを第三者と共用する利用形態ではなく、ミドルウェアのプロセスレベルで分離されているサービスである	3
	仮想OSレベルで占有するタイプのサービスである	4

当資料は広島大学クラウドサービス利用ガイドラインならびに広島大学クラウドサービス利用ガイドラインチェックリスト（©広島大学 情報セキュリティ推進機構）を一部参考に作成している

http://www.media.hiroshima-u.ac.jp/news/cloudguide