（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	具体的な内容	対策
機密性1	公開・改ざんされても大きな影響がないもの	・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	［サービスを利用することそのものによって発生するリスクの軽減］ ・ウィルス・マルウェアの感染に注意する。 ［提供する情報の制限］ ・第三者に閲覧されうることを前提に、掲載・提供する情報の内容を考慮する。
機密性2	公開を前提とするが改ざんされると影響が大きいもの	・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	［改ざん防止/システムへの攻撃等による改ざんの防止］ ・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。 ［改ざん防止/第三者による想定されていない改ざんの防止］ ・情報の内容の更新にあたって、パスワード等1要素以上のアクセス制限を設けているサービスを利用する。 ・通信経路の暗号化やなりすまし対策の観点からSSLやSSH等の技術を利用したシステムを選定する。 ［データの所有権喪失の防止］ ・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3	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重要3、4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We b 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4、5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4、5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2の対策に加え以下の対策がおこなわれているサービスを選定する ［閲覧制限/第三者による想定されていない閲覧の防止］ 情報の閲覧にあたって、パスワードによるアクセス制限を設けているサービスを利用する。
機密性4	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3の対策に加え以下の対策を行う事 ［さらなる閲覧・更新の制限］ ・供託した情報の閲覧・更新にあたり、IDパスワードのみで認証する方式と比較して安全性が高いアクセス制限（2要素認証、2重認証、ネットワーク的な制限、電子支証明書による認証等）が可能であること。 ［システムの信頼性の確保］ ・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。 ［係争対策］ ・準拠法・管轄裁判所が国内となっている、 あるいは大元のサービス運用業者が国外であっても国内の代理店等により係争の際の対応が明記されており、係争となっても支障がないことが確認できる。 ［情報の適正な取り扱い］ 供託した情報の破損・漏洩等を防ぐ観点から、以下のような仕様を満たすシステムを選定すること。 ・供託しているデータの破損・喪失等が発生した場合テナント/ユーザーごとに情報の復元が可能な設計となっている。 ・利用サービスの移行等が発生した場合、データの取り出し等の移設作業が容易な設計となっている。 ・サービス終了時の供託データの取り扱い（消去）について明記されている。 ［システムの適切な運用］ ・脆弱性に対する攻撃への対策やサービスの安定的な稼働の観点から、サービスを構成するOS・ミドルウェア等が適切にアップデートされている。 ［適正なアカウント管理］ ・閲覧・更新で用いるアカウントについて、実在する人物と対応が明確になるよう運用する。 ・アカウント管理責任者は不要となったユーザーの削除や組織変更の内容がシステムに迅速に反映されるよう管理する。
機密性5	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	この機密性の情報をクラウドサービスに供託する場合、 機密性4の対策に加え、以下のようなさらなる対策が施されているかを確認し、サービスを選定すること ［利用状況の監視］ ・データの閲覧・更新に関する記録がとられている。 ［さらなる閲覧・更新の制限］ 以下のような形でアクセス制限が施されているシステムを選定する事（以下に記載の内容は例示であり、サービスの利用に支障が出ない範囲で可能な限り細かい制限が可能であることが要件となる）。 ・必要最低限のポート以外利用できないよう制限されている ・アクセス可能なIPアドレス範囲が、部署や建屋といった必要最低限の範囲に限定されている。 ・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。 ［システムへの攻撃等による、想定しない情報漏洩に対する対策］ 以下のような漏洩対策が施されているシステムを選定する事。 ・ユーザーデータの保存領域等がOS/ミドルウェア上でテナントごとに分離されており、 同一サービスの他テナントにて侵入が発生しても影響を受けない構造となっている。 ・同一のサービスを他テナント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。 ・仮想OSレベルで占有するタイプのサービスである。 ※なお、供託する情報そのものにパスワードをかける等、追加の対策を施すことで、機密性5に該当する情報も、機密性4の基準を満たすサービスに供託できることとする