業務上の情報セキュリティ確保ガイドライン

１．　目的

業務上の情報セキュリティ確保ガイドラインは、電子化された個人情報および機密データの漏えいを未然に防ぐこと、ならびに対象者の不注意またはサイバー攻撃等の事案により情報漏洩が発生した場合に備えて被害を最小限にとどめることを目的とし、情報機器やデータファイルの取り扱いに際して教員が守るべき具体的な最低限の行動規範を定める。

２．　対象範囲

２−１　対象者

本ガイドラインが定める行動規範は大阪工業大学 専任・特任・客員・非常勤の各教員に適用する。

２−２　対象とする範囲

(1) 学園規定により個人情報と定められた情報を電子化したデータファイル
（例：名簿、成績表、個人調書、活動記録、履歴書、推薦書、答案、レポート等）
(2) 試験問題（素案の段階や過去の試験問題を除く）のうち電子化されたデータファイル
(3) 大学運営や大学の意思決定にかかる文書を電子化したデータファイル
(4) 上記(1)～(3)を以下「対象データファイル」と呼び、対象データファイルに規定するデータファイルの保管または共有の方法

ただし、日本技術者教育認定機構(JABEE)の受審に要するデータなど、本ガイドライン以外に特別な取り扱いルールが別途定められている対象データファイルの取り扱いは当該ルールによる。また個人情報にかかるデータファイルで、関係者全員の同意があればその取り扱いについて本ガイドラインの対象外としてよい（例：卒研の卒業生名簿)。

３．　データファイルのライフサイクル管理

(1) 本ガイドラインの対象データファイルは、データの収集目的が達成された時点で速やかに廃棄すること。例として授業の成績関連データであれば成績確定時、ゼミ生調査書等であれば当該学生の卒業時、が収集目的の達成時点となる。
(2) 教育効果の分析など特定の利用目的が現に存在し、上記期間を超えてデータ保管を要する場合でも教員の管理下ではおおむね１年以上超過しないこと。それ以上の長期の保管を要する場合はデータを匿名化すること。

４．　対象データファイルの保管場所

本ガイドラインの対象データファイルは次の場所・サービスのいずれかで保管すること。

(1) 教員居室のデスクトップ PC や居室設置のファイルサーバー（設置場所の状況によりセキュリティワイヤーの使用も検討すること）
(2) USB メモリーを含むリムーバブルメディア、ノート PC など可搬性が高い媒体や機器に保存する場合は、教員不在時は施錠ロッカーで保管すること
(3) 学内ファイルサーバーの個人領域（Z ドライブ）
(4) 大学の業務アカウントに紐づく OneDrive / Google ドライブの各サービス（ただし当面はデータの暗号化を併用することとし、なるべく短期間の保存にとどめることが望ましい）。**個人契約に基づくクラウドストレージはサービス提供者・サービス内容・保管期間によらず、対象データファイルの保管場所として使用してはならない。**

５．　対象データファイルの持ち運び

本ガイドラインの対象となるデータファイルを大学キャンパスから持ち出す（校地間移動を含む）場合、USB メモリーを含むリムーバブルメディアによる持ち出し、ノート PC やタブレットデバイスの内蔵ストレージによる持ち出しのいずれも禁止とする（暗号化してあっても不可）。代替手段として次の２つの方法を提供する。

(1) 学内ファイルサーバーの個人領域（Z ドライブ）に置き学外から VPN 接続して参照、または本学の VDI サービスを用いて参照する。
(2) 大学の業務アカウントに紐づく OneDrive / Google ドライブの各サービスにデータを保管して、学外の PC から参照する。ただし当面はデータの暗号化を併用することとし、オンラインサーバー上にデータが保管されている期間を短くすることが望まれる。大学の業務アカウントに紐づかない（個人契約に基づく）クラウドストレージサービスの利用は禁止する。

６．　モバイルデバイスの利用

スマートフォンやタブレットデバイスによる業務上のデータ参照では、これらのデバイスが特に紛失や盗難に遭う危険性が高いことを勘案し、次の５項目を満たしたものでなければならない。

(1) 利用者の占有デバイスであること
(2) 他のサービスと共通ではない強固なログインパスワードや PIN で保護していること
(3) デバイスが個人契約の AppleID や Google アカウントに紐づく場合は、当該アカウントの二要素認証を有効化してあること
(4) 遠隔消去機能がある場合はテスト済みであることを強く推奨（少なくとも位置確認機能はテスト済みであること）
(5) メーカーによる端末保護機能を無効化していないこと（jailbreak や root 化と呼ばれる行為の禁止）

７．　電子メールの利用と対象データファイルの共有

工大では、非常勤講師を除き、業務アカウントに紐づく電子メールを交付している。工大の業務アカウントに紐づく電子メールの利用では、次の行動規範を遵守すること。

(1) メール受信時、常にフィッシング詐欺の可能性を念頭に添付ファイル閲覧や URL クリックの可否を判断する。送信時は添付ファイルによるデータ共有を安易に行わず、共有ファイルサーバーの活用など代替方法の検討を強く推奨する。
(2) 本ガイドラインの対象データファイルの電子メールによる送信は原則不可とする。やむをえない場合は必ず暗号化し、送受信後すぐに削除してゴミ箱からも削除。
(3) 【非常勤講師には適用外】業務用メールアドレスは大学教員としての業務にのみ用いるものとし、業務用メールアカウントと私用メールアカウント間の着信メール一括転送はいずれの方向にも禁止とする。また業務にかかる連絡は必ず業務用メールアドレス宛に送信するものとし、業務アカウントに紐づかないメールアドレスは大学教員としての連絡用に用いない。

８．　その他

他大学等が公開している報告書によると、情報漏洩の事案は情報セキュリティ確保に対する意識に欠ける従業員の行動や不作為が発端となっているケースが多い。本ガイドラインの対象者は常にガイドラインの趣旨を尊重し、本学の社会からの信頼を損なうことのないよう、細心の注意を払って対象データファイルの取り扱いを心がけていただきたい。

本ガイドラインは情報漏洩の脅威を許容できるレベルに低減・維持するため、すべての教員が意識すべき行動規範のごく一部を列挙したに過ぎず、言及のない行動について一律に許諾されていると解釈しないでいただきたい。特に通信事業者などの学外機関が提供する便利なサービスを使うことによって、意図せず組織全体の脅威レベルを著しく引き上げてしまう可能性がある。

情報セキュリティ委員会と情報センターは継続的に本ガイドラインを見直し、教員の不注意や外部からのサイバー攻撃による情報漏洩を防ぐ施策の立案を続けている。教員各位においても学外機関が提供する情報サービス等の利用に際して組織に与える脅威レベルについて慎重に判断いただき、判断が難しいケースは情報センターにご相談いただくようお願いしたい。

2019 年 6 月 1 日
大阪工業大学
　情報セキュリティ委員会
　情報センター