４．規程の変更に関する事項

（１）事業組織運営規程の一部変更

研究委員会第４条第２項（２）について、２０１６年度(平成２８年度)から事業活動を休止している情報教育高大接続分科会を廃止し、新たに２０１９年度事業計画で決定したデータサイエンス教育分科会を追加変更することについて、２０１９年(平成３１年)４月２７日の第６９回理事会において、以下の通り決定した。

事業組織運営規程

第１条から第４条（略）

第２章　事業組織

（研究委員会）

第４条　この法人の研究・促進機関として研究委員会を置く。

２　研究・促進機関として、次に定める委員会を設置する。但し、必要に応じて専門の分科会，小委員会を置く。

（１）　情報通信技術による教育改善を研究・促進する「学系別 FD/ICT 活用研究委員会」、「分野別サイバー・キャンパス・コンソーシアム運営委員会」。

（２）　情報教育の改善充実を研究・促進する「情報教育研究委員会」、「情報リテラシー・情報倫理分科会」、「情報専門教育分科会」、「分野別情報教育分科会」、「データサイエンス教育分科会」。

第５条から第２６条（略）

附　則

１　この規程は、公益社団法人の設立登記の日から施行する。

２から６（略）

７　変更後の規程は、平成３１年４月２７日から施行する。

（２）情報セキュリティに関する規程

「２０１９年(平成３１年)３月２５日内閣府の立入り検査において、個人情報保護規程などの情報セキュリティ対策の規定化について質問があり、２０１６年(平成２８年)に事務局内規で申し合せを設けて仕事を進めてきたが、理事会に諮っていないことから改めて規定化の手続きを行うことの要請があった。そこで、申し合わせの上位規程として「情報セキュリティに関する規程」を策定し、細部の取り扱いは「情報セキュリティに関する事務局内申し合わせ」として制定することについて、２０１９年(平成３１年)４月２７日の第６９回理事会において、以下の通り決定した。

公益社団法人私立大学情報教育協会
情報セキュリティに関する規程

第６９回理事会制定

（目的）

第１条　この規程は、公益社団法人私立大学情報教育協会（以下「この法人」という。）の情報セキュリティの維持及び向上のために必要な事項を定めるものとし、法令に定めるものの他はこの規程によるものとする。

（定義）

第２条　本規程における用語の定義は、次の各号に定めるとおりとする。

（１）「情報」とは、本協会が保有する一切の情報（本協会固有の情報、正当な手段に基づき入手した第三者からの情報を含む。）をいう。
（２）「情報資産」とは、全ての紙面、電子媒体の情報をいう。
（３）「情報システム」とは、情報を取り扱うハードウェア、ソフトウェア、プログラムをいう。
（４）「対象情報」とは、情報セキュリティの確保及び維持が必要と判断した重要な情報をいう。
（５）「不測事態」とは情報セキュリティの確保及び維持に重大な影響を与える災害、障害、セキュリティ侵害等の事態をいう。
（６）「事務局職員、事務局関係者」とは、本協会の事務局職員並びにこれに準ずる者（アルバイト、業務委託者、業務委託会社）をいう。

（適用範囲）
第３条　本規程は、事務局職員及び事務局関係者に適用する。

（情報セキュリティ管理体制）
第４条　本協会は、情報の機密性、安全性、可用性を維持するために、情報セキュリティに係る管理者を事務局内に置く。情報セキュリティの管理者は事務局長とする。
２　情報セキュリティの管理者は、本協会における情報セキュリティの維持及び向上に必要な基準や申し合わせ等を制定し、これらの周知徹底、運用及び見直し、改善を図るとともに、施策等の評価、見直し改善を行う。
３　事務局職員は、情報セキュリティの管理者の指示に従い、事務局内における情報セキュリティに係る業務について、情報セキュリティの維持及び向上に必要な措置をとるとともに見直し改善を行う。

（教育）
第５条　情報セキュリティの管理者は、事務局職員及び事務局関係者に対し、情報セキュリティ意識の向上を図り、情報セキュリティ管理体制、本規程及び情報セキュリティに関する事務局内申し合わせ、関係法令を理解させるために必要な教育を実施する。
（対象情報資産の管理）
第６条　事務局職員は、情報セキュリティに関する事務局内申し合わせ及び関係法令を遵守し、対象情報資産を適切に管理しなければならない。

（情報システムの情報セキュリティ）
第７条　情報セキュリティの管理者は、本協会の保有する情報システムの維持のための施策（コンピュータウィルスからの保護、記録情報のバックアップ、情報システムの運用の記録、ネットワークの管理、電子メールのセキュリティ、アクセス制御、不正アクセス対策など。）を講じるものとする。

（不測事態の報告）
第８条　事務局職員は、不測事態の発生又は発生の兆候を知った場合、直ちにこれを事務局長に報告するものとする。
２　情報セキュリティの管理者は、前項の報告を受けた場合、速やかに当該不測事態の原因究明を行うとともに、不測事態の発生を本協会の会長及び理事会に報告・相談し、必要な対策を講ずるものとする。

（規程等の遵守）
第９条　事務局職員は、情報セキュリティの重要性を認識の上、本規程及び情報セキュリティに関する事務局内申し合わせ、関係法令を遵守しなければならない。

（規程等の見直し・改善）

第１０条　情報セキュリティの管理者は、本規程及び情報セキュリティに関する事務局内申し合わせ及び関係法令の実効性を確保するために、必要に応じて理事会の審議を経て見直し、改善を図るものとする。

（規程の改廃）
第１１条 この規程の改廃は、理事会において決定する。

附 則
この規程は、平成３１年４月２７日から実施する。

公益社団法人私立大学情報教育協会
情報セキュリティに関する事務局内申し合わせ

平成 28 年 4 月 1 日作成
第 69 回理事会制定

Ⅰ． マイナンバー等の特定個人情報の取り扱い

１．関係法令・ガイドライン等の遵守

個人番号及び特定個人情報の取り扱いに関し、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「特定個人情報の適正な取扱いに関するガイドライン」、並びに「個人情報の保護に関する法律」及び各省庁のガイドラインを遵守します。

２．利用目的

提供を受けた職員、配偶者及び親族のマイナンバー等の特定個人情報は、事務局長が鍵のかかる事務机内に保管し、以下の目的以外に利用しません。

【税務に関する利用】
・源泉徴収票作成事務
・扶養控除等（異動）申告書、保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険に関する利用】
・健康保険・厚生年金保険届出、申請・請求事務
・雇用保険・労災保険届出、申請・請求、証明書作成事務

３．安全管理措置に関する事項

マイナンバー等の特定個人情報の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために万全を期し、法令、規制、規範及を遵守します。

４．委託の取り扱い

マイナンバー等の特定個人情報の取り扱いを第三者に委託することは禁止します。

５．継続的改善

マイナンバー等の特定個人情報等の取り扱いを継続的に改善するよう努めます。

６．マイナンバー等の特定個人情報等の開示

本人又はその代理人から、マイナンバー等の特定個人情報に係る保有個人データの開示の求めがあったときは、次の各号の場合を除き、遅滞なく回答します。
・本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
・業務の適正な実施に著しい支障を及ぼすおそれがある場合
・法令に違反することとなる場合

７．特定個人情報等の開示に関する問合せは事務局長が対応します。

Ⅱ．事業で扱う個人情報の取り扱い

１．関係法令・ガイドライン等の遵守

事業で扱う個人情報については、「個人情報の保護に関する法律」（個人情報保

護法）及び各省庁のガイドラインを遵守します。

２．利用目的

提供を受けて事業で扱う個人情報は、本協会のサーバーに適切に保管し、事業の目的以外には利用しません。

３．安全管理措置に関する事項

事業で扱う個人情報の漏えい、滅失又は毀損の防止と適切な管理のために万全を期し、法令、規制、規範及を遵守します。

４．委託の取り扱い

提供を受けて事業で扱う個人情報の全部又は一部を当社以外の者に委託するときは、委託先において、本協会が果たすべき安全管理措置と同等の措置が講じられるか否かについてあらかじめ確認した上で委託契約を行い、機密保持契約において個人情報等の安全管理について委託先が講ずべき措置を明らかにし、委託先における個人情報の取扱状況を把握するものとします。

また、委託先が事業で扱う個人情報の全部又は一部を再委託する場合には、本協会の許諾を得るものとし、再委託が行われた場合、委託先が再委託先に対して必要かつ適切な監督を行っているかについて監督するものとします。

５．継続的改善

事業で扱う個人情報の取り扱いを継続的に改善するよう努めます。

６．特定個人情報等の開示

提供を受けた事業で扱う個人情報について、本人又はその代理人から、個人情報等に係る開示の求めがあったときは、次の各号の場合を除き、遅滞なく回答します。

・本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
・業務の適正な実施に著しい支障を及ぼすおそれがある場合
・法令に違反することとなる場合

７．事業で扱う個人情報の開示に関する問合せは事務局長が対応します。

Ⅲ．情報セキュリティのための組織的取組

１．情報セキュリティ対策の最新情報の入手と共有

情報セキュリティ対策活動を推進するため、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し事務局内で共有する。

・独立行政法人情報処理推進機構（略称：IPA）
・一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）
・個人情報保護委員会

２．人的対策

（１）採用時の雇用条件

職員、派遣社員、パート・アルバイトを雇用する際は秘密保持を厳守できることを条件とします。

（２）職員の責務

① 職員は本協会が、個人情報及び組織運用上管理する情報及びその複製物の一切を許可されていない組織、人に提供してはならない。

② 職員は、本協会の情報セキュリティ方針及び関連規程を遵守する。違反時には就業規則に従い懲戒処分の対象とする。

（３）雇用終了時の対策

職員は、在職中に交付された業務に関連する資料、個人情報、事業内容その他の資料又はそれらの複製物の一切を退職時に返還し、在職中に知り得た業務上の情報もしくは業務遂行上知り得た情報を外部に提供してはならない。

（４）情報資産の事務局外持ち出し

情報資産を事務局外に持ち出す場合には、事前に事務局長の許可を得るものとし、ノートパソコンで持ち出す場合、USB メモリ、HDD 等の電子媒体に保存して持ち出す場合は、パスワード等で持ち出すデータの暗号化を行う。

（５）媒体の廃棄

個人情報等の情報資産を廃棄する場合は以下の処分を行う。

・ 書類、フィルムは溶解又は焼却

・ USB メモリ、HDD、CD、DVD は破壊又は細断

・ パソコン本体は OS を削除し専門業者に廃棄依頼

３．データのセキュリティ保全とバックアップ

（１）データのセキュリティ

データのセキュリティ保全のため、本協会のファイルサーバー、メールサーバー、Web サーバー、

NAS サーバ、ホームページの運用等の業務は、株式会社リブラスに置き、機密保持契約を締結した上で業務委託します。なお、委託先において、情報等の安全管理について委託先が講ずべき措置を明らかにし、機密保持契約により委託先における特定個人情報の取扱状況を把握するものとします。

（２）バックアップ対策

本協会の業務の継続性を図るため、株式会社リブラスに保管してあるデータは沖縄拠点に機械的はバックアップで保管し、月１回バックアップデータを定期的に取得します。

（３）クラウドサービスを利用したバックアップ

機密保持の観点からクラウドサービスを利用した外部サーバーへのバックアップは行いません。

４．事務局内の注意事項

以下の点に注意した業務を行うものとします。

・複合機、プリンタに原稿、印刷物を放置しない。

・FAX 送信時には誤送信防止のため宛先を複数回確認する。

・ホワイトボードは利用後に消去する。

５．ソフトウェアの利用

・業務に利用するパソコンには、正規の標準ソフトウェアを導入する。

・職員は、業務に不要なシステムやインストールされているソフトウェアを利用しない。

・ファイル共有ソフト、不審なソフト、正規ライセンス以外のソフトウェアは使用しない。

６．ウイルス対策ソフトウェアの利用

・職員は、正規のウイルス対策ソフトを利用し、ウイルス検知を実施する。

・電子媒体を用いてファイルの受け渡しを行う場合は、ファイルにウイルス検知を実施する。

・導入したウイルス対策ソフトウェアを随時更新する。

７．インターネットの利用

職員は、インターネットを利用する際には以下を遵守する。

（１）ウェブ閲覧

職員は、ウイルス等の悪意のあるソフトウェアに感染するおそれがあると認められる有害ウェブサイトを閲覧しない。

（２）業務でウェブ閲覧を行う場合は以下に注意する。

・公序良俗に反するサイトへのアクセスを禁止する。

・不審なサイトへのアクセス及び業務用メールアドレス登録を禁止する。

（３）オンラインサービス

インターネットで提供されているオンラインサービスは使用しない。但し、りそな銀行のインターネットバンキング・電子決済のみ、銀行が提供する専用アプリケーションソフトを用いて事務局長が利用する。

（４）業務で電子メールを利用する際には以下を実施する。

① 誤送信防止

電子メールソフトの即時送信機能は利用しない（停止する）。

② メールアドレス漏えい防止

・極秘の情報資産を送信する場合は、ファイルを暗号化して送信する。

・クラウド型メールは利用しない。

（５）ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため、以下の内容に複数合致する場合は十分に注意し、添付ファイルを開く、又はリンクを参照するなどしない。

① 怪しいメールに十分に注意する。

・知らない人からのメールで、メール本文の URL や添付ファイルを開かざるを得ない内容。
・新聞社や出版社からの取材申込や講演依頼。
・製品やサービスに関する問い合わせ、クレーム。
・心当たりのないメールだが、興味をそそられる内容。
・これまで届いたことがない公的機関からのお知らせ。
・情報セキュリティに関する注意喚起や災害情報。
・心当たりのない、決裁や配送通知 (英文の場合が多い)。
・航空券の予約確認、荷物の配達通知。
・ID やパスワードなどの入力を要求するメール。
・メールボックスの容量オーバーの警告や銀行からの登録情報確認。

② 怪しい差出人のメールアドレスに十分に注意する。

・フリーメールアドレスから送信されている。
・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる。
・不自然な日本語メール、日本語では使用されない漢字（繁体字、簡体字）が使われている。
・表示 URL と実際のリンク先の URL が異なる。
・署名の内容が誤っている、組織名や電話番号が実在しない。
・電話番号が FAX 番号として記載されている。

③ 添付ファイル

・実行形式ファイル(exe/scr/cpl など)が添付されている。
・ショートカットファイル(lnk など)が添付されている。
・アイコンが偽装されている。
・実行形式ファイルなのに文書ファイルやフォルダーのアイコンとなっている。
・ファイル拡張子が偽装されている。

（３）業務を執行する理事の職務規程

２０１９年３月の第２４回臨時総会において、２０１９年度事業計画書の中で事業組織の名称を「私情協 教育イノベーション大会」に変更したことから、「業務を執行する理事の職務規程」９号の「教育改革 ICT 戦略大会の運営・実施」も「私情協 教育イノベーション大会の運営・実施」に改めることになり、２０１９年(令和元年)第７１回理事会において変更遡及を行うとともに、規程の施行日も平成３１年４月１日からとした。