資料２

個人情報の持ち出し等に係る安全管理措置について（周知）

令和３年４月●日
個人情報保護委員会事務局

当委員会に報告された個人データの漏えい等事案のうち、私立大学における漏えい等事案の約 30%が個人情報の持ち出しを原因としており、これは、全業種における個人情報の持ち出しを原因とした漏えい等事案の平均（約４％）を大きく超えています。

報告等の中では、業務において個人情報を持ち出さなければならない一方、持ち出し時の規定が定められていなかったり、教員及び職員（非常勤等も含む）への周知や運用の徹底ができていなかったケースが多数ありましたところ、改めて学生等の個人情報を外部へ持ち出す際は、十分な対策を講じていただきますようお願いいたします。

対策の一例として、当委員会が公表している「個人情報の保護に関する法律についてのガイドライン（通則編）」（※１）の中から特に有効と思われる対策を抜粋し、各大学で実際に行われている参考事例とともに周知させていただきます。
同ガイドラインでは、今回抜粋した対策のほかにも、個人情報取扱事業者が具体的に講じなければならない安全管理措置及び同措置を実践するための手法が例示してありますので、ご参考としていただき、この機会に安全管理措置の見直しを行ってください。
（※１）個人情報の保護に関する法律についてのガイドライン（通則編）
https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf

最後に、個人情報保護委員会では、昨今、利用が増加しているテレワークやクラウドサービス利用時の注意喚起や研修用教材なども、当委員会ウェブサイト（※２）に掲載しておりますので、ご参考にしてください。
（※２）個人情報の研修資料・ヒヤリハットコーナー
https://www.ppc.go.jp/personalinfo/hiyarihatto/#warning

※講じなければならない措置及び手法の例示は、個人情報の保護に関する法律についてのガイドライン（通則編）からの引用です。

1. 組織的安全管理措置

講じなければならない措置	手法の例示	参考事例
<u>個人データの取扱に係る規律に従った運用</u> ➢ あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。 ➢ なお、整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、利用状況等を記録することも重要である。	個人データの取扱いに係る規律に従った運用を確保するため、例えば次のような項目に関して、システムログその他の個人データの取扱いに係る記録の整備や業務日誌の作成等を通じて、個人データの取扱いの検証を可能とすることが考えられる。 ➢ 個人情報データベース等の利用・出力状況 ➢ 個人データが記載又は記録された書類・媒体等の持ち運び等の状況 ➢ 個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。） ➢ 個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）	➢ 学生の個人データを分類し、種類別に、保管方法、持ち出し可否及び廃棄方法等を規定している。 ➢ 教職員（非常勤等も含む）が個人データを学外へ持ち出す際、責任者の事前承認を必要とし、責任者は従業者が持ち出した個人情報を記録して管理している。 ➢ 物理的な持ち出しに加え、クラウドサービスに個人データを保存する場合を持ち出しと定義し、保存できる個人データの範囲を限定している。
<u>取扱状況の把握及び安全管理措置の見直し</u> ➢ 個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。	➢ 個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。 ➢ 外部の主体による監査活動と合わせて、監査を実施する。	➢ 教職員（非常勤等も含む）に対するアンケート調査により、個人データの管理実態と管理規定に齟齬が生じていないかどうかを点検している。

2.　人的安全管理措置

講じなければならない措置	手法の例示	参考事例
従業者の教育 ➢ 従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。	➢ 個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。 ➢ 個人データについての秘密保持に関する事項を就業規則等に盛り込む。	➢ 非常勤等を含めた全教職員に対し、２年に１回、個人データの取扱いに関する研修を行っている。 ➢ e-learning による情報セキュリティ研修を毎年度実施している

3.　物理的安全管理措置

講じなければならない措置	手法の例示	参考事例
個人データを取り扱う区域の管理 ➢ 個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（以下「管理区域」という。）及びその他の個人データを取り扱う事務を実施する区域（以下「取扱区域」という。）について、それぞれ適切な管理を行わなければならない。	（管理区域の管理手法の例） ➢ 入退室管理及び持ち込む機器等の制限等。なお、入退室管理の方法としては、IC カード、ナンバーキー等による入退室管理システムの設置等が考えられる。 （取扱区域の管理手法の例） ➢ 間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止	➢ 個人データを保存・保管・利用する場所を「情報セキュリティ区画」と定め、当該区画の入退管理又は施錠等の運用方法も規定している。 ➢ 大学が規定した安全性等を満たすネットワーク環境を「情報セキュリティ区画」と定め、同区域内で大学が提供するシステムを利用する場合に限り、ネットワーク上での個人データの取扱いを許容している。
電子媒体等を持ち運ぶ場合の漏えい等の防止 ➢ 個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。	➢ 持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 ➢ 封緘、目隠しシールの貼付けを行う。 ➢ 施錠できる搬送容器を利用する。	➢ USB 等に個人情報を記録する場合はデータの暗号化やパスワードを設定し、目的達成後、速やかにデータを削除している。 ➢ 個人データを記録した端末、記憶媒体等を持ち出すことがないよう、仮想デスクトップを導入している。

4.　技術的安全管理措置

講じなければならない措置	手法の例示	参考事例
<u>アクセス制御</u> ➢ 担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない。	➢ 個人情報データベース等を取り扱うことのできる情報システムを限定する。 ➢ 情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ➢ ユーザーID に付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。	➢ 個人データを私物の電子媒体へコピー・送信することのできない学習支援システムを導入し、利用者毎に ID 等を割り振ってアクセス可能な個人情報の範囲を制御している。 ➢ SSO（シングルサインオン）方式を採用し、ログイン ID ごとに閲覧権限・範囲を設定している。
<u>アクセス者の識別と認証</u> ➢ 個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。	（情報システムを使用する従業者の識別・認証手法の例） ➢ ユーザーID、パスワード、磁気・IC カード等	➢ 教職員（非常勤等も含む）が利用する学内のシステムは多要素認証を必須とし、情報漏えいリスクへの対策として、アカウントへの本人以外からの不正アクセスを監視している。