個人情報の適正管理（平成26年度システム監査結果）　　対象受検機関：教育庁　教育振興室高等学校課

事務事業の概要	検出事項	監査の結果
＜平成26年度システム監査について＞ ・　システム監査とは、監査対象の情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動をいう。 ・　本年度のシステム監査は、平成26年度上半期の監査結果（教育委員会事務局「個人情報の流出」事案）を踏まえ、府立高校教職員が利用している「統合ＩＣＴネットワーク」及び「外部ファイル共有サービス」を対象として実施した。 ・　具体的手順としては、教育委員会事務局に対してヒアリングを行い、事務局管理下における個人情報保護に係る技術的な安全管理措置の実施状況について検証を行った。 １　平成26年度上半期監査結果（教育委員会事務局「個人情報の流出」事案）では、府立高校において、ＵＳＢメモリの紛失による個人情報の流出事案が多数発生したことを背景に、各学校において教職員が意見交換を行う研修を行うなど、現場レベルの個人情報保護意識を醸成するための効果的な取組を求めている。 　また、同事案では、「新システムの導入等によって、平成26年９月以降、ＵＳＢメモリへの個人情報の記録が禁止となるため、ＵＳＢメモリの紛失による個人情報流出事案への対応は一定行われることになるが、各種媒体による個人情報漏えいリスクは依然として残る」と示されている。 ２　平成26年度から、「教育委員会情報セキュリティポリシー実施手順」（以下「実施手順」という。）が運用されるとともに、上述の新システムとして「統合ＩＣＴネットワーク」が導入されている。「統合ＩＣＴネットワーク」とは、府立高校の校務（成績処理や出欠管理等）の効率化を目的としたネットワークで、大阪府の教職員約14,000人を対象としており（実際の利用件数は平成27年２月末時点で約4,000件／利用者数は約700人）、学校内に配備された端末機（パソコン等）により利用される。 ３　「統合ＩＣＴネットワーク」環境では、ＵＳＢメモリへの情報の記録が禁止されたため、ＵＳＢメモリを介さずにファイルの送受信ができる環境として、「外部ファイル共有サービス」が用意されている。 ４　「外部ファイル共有サービス」におけるファイルの送受信プロセスは以下のとおりである。 (1)　教職員は「外部ファイル共有サービス」にログオンし（個人に割り当てらえたＩＤとパスワードの入力が必要）、提供される格納場所に対象ファイルを保存する。 (2)　ファイルを渡したい相手（教職員以外の外部の者を含む。）に対し、メールを用いて格納場所を通知し、別途、ファイルを取得するためのパスワードを通知する。 (3)　通知を受け取った相手はメールに記載された格納場所へアクセスした上で、ファイル取得のためのパスワードを入力しファイルをダウンロードする。	１　「外部ファイル共有サービス」について、利用手順書では個人情報を含むファイルの送受信を禁止しているものの、監査で確認したところ、外部業者開催イベントの参加者名簿に係る情報が取り扱われていた。 　実務的にはＵＳＢの代替機能として個人情報が取り扱われている状況にある。 ２　「外部ファイル共有サービス」に関して、以下の事実が検出された。 ・　「外部ファイル共有サービス」において個人情報の送受信自体を制限する機能は組み込まれていない。 ・　監査で確認したところ、実施手順第７条第４項で定められているアクセス記録の定期的な検証は行われていない。 ３　「外部ファイル共有サービス」以外（電子メール）に係る個人情報の取扱いに関して、以下の事実が検出された。 ・　実施手順によれば、電子メールを使って個人情報を含むファイルを送受信する場合は、パスワード等によるアクセス制限をかけることになっているが、メール作成時に自動的にパスワードを設定する機能は組み込まれていない。 ・　監査で確認したところ、実施手順第７条第４項で定められているアクセス記録の定期的な検証は行われていない。	**【改善を求めるもの（意見）】** 　ＵＳＢメモリの紛失による個人情報流出事案への対応は一定行われているが、代替機能として利用されている「外部ファイル共有サービス」でも依然として個人情報が取り扱われている状況にあり、漏えいリスクは残ったままである。 　このようなリスクに鑑み、実施手順に従って、「外部ファイル共有サービス」、電子メール等のネットワーク、サーバ及びシステムのアクセス記録を定期的に検証し、個人情報に係る諸規程から逸脱している事例がある場合は、当該ユーザに対して警告する等の改善策を検討されたい。

５　外部ファイル共有サービス利用手順書（以下「利用手順書」という。）では、利用による個人情報の漏えいを防ぐため、個人情報を含むファイルの送受信は禁止とされており、さらに実施手順第７条第４項では必要な検証作業を行うことを求めている。

（参考）外部ファイル共有サービス利用手順書
１.４　禁止事項
１）個人情報を含むファイルの送受信
個人情報保護の観点より、個人情報を含むファイルの送受信は禁止です。

（参考）教育委員会情報セキュリティポリシー実施手順（平成26年４月１日改正）
第２章　管理者
第７条
４　ネットワーク管理者、サーバ管理者及びシステム管理者は、その管理下にあるネットワーク、サーバ及びシステムの稼働状況並びにアクセス記録を定期的に検証しなければならない。

６　「外部ファイル共有サービス」について、セキュリティに配慮して適切に利用されたとしても、電子メールで個人情報が転送される等のリスクは存在する。そこで、以下のとおり電子メールの場合でも実施手順第19条において、情報の重要度に応じた対応が求められている。また、「外部ファイル共有サービス」と同様の検証も求められている（実施手順第７条第４項）。

（参考）教育委員会情報セキュリティポリシー実施手順（平成26年４月１日改正）
第４章　情報の分類及び管理
第18条　重要度Ⅰ：情報が脅威にさらされた場合に実害を受ける危険性が高い情報
システム設定や個人情報等の秘匿情報
重要度Ⅱ：情報が脅威にさらされた場合に実害を受ける危険性は低いが重要性が高く、
公開することを予定していない情報

第19条　重要度Ⅰの情報については、パスワード等によるアクセス制限をかけること。重要度Ⅱ以上の情報の不用意な複製、送付及び送信は行ってはならない。

７　なお、「外部ファイル共有サービス」や電子メール以外を利用した個人情報の送受信については、外部オンラインストレージ（※）に対してはアクセス制限がかけられ、また、標準外のソフトウェアについてはインストール権限が教職員に付与されていない等、一定のリスク低減が図られている。

※　外部オンラインストレージ：インターネット上でファイル保管用のディスクスペースを貸し出すサービスのこと。

措 置 の 内 容
利用手順書の改訂（平成27年５月）と統合ＩＣＴネットワーク管理及び運用ガイドラインの改正（平成29年９月）を行い、外部ファイル共有サービス及び電子メールに係るアクセス記録を毎月検証することについて、教職員へ周知し、その検証手順を定めた（平成29年10月）。平成29年10月から、実施手順に従って、外部ファイル共有サービス及び電子メールに係るアクセス記録を毎月検証し、個人情報と想定される添付ファイルが含まれている場合は、個人情報に係る諸規程から逸脱していないか、当該ユーザに内容を確認の上、必要に応じた指導を行っている。