教総第５３９号
平成２０年3月6日

教育委員会本庁各課長
各教育事務所長　　様
各教育機関の長

教　育　長

情報セキュリティチェックシートによる自己点検違反事項の是正について（通知）

平成１９年１２月に実施した「情報セキュリティチェックシート」による自己点検（平成１９年１１月２９日付け情企第４２１号）について、岐阜県情報セキュリティポリシー（岐阜県情報セキュリティ基本方針、岐阜県情報セキュリティ対策基準）に対する違反の状況を集計したところ、教育委員会においては、違反件数が非常に多く見受けられました。これらの違反は、個人情報など重要な情報の漏えいを引き起こし、県民の信頼を失墜させるだけではなく、発生した損害の賠償責任や懲戒処分にも繋がる可能性があります。また、ウィルス感染などは、手元のパソコン、ＭＯ、ＨＤのデータが破壊され利用できなくなるだけではなく、県庁内のネットワーク全体のダウンに繋がりかねません。この場合の情報資産の損害の大きさは計り知れず、復旧するためには、莫大な事務量と費用が必要となります。

ついては、再度、自己点検結果を確認いただき、違反のあった所属においては下記により違反を是正されますようお願いします。また、所属職員に対し、再度、情報セキュリティポリシーの遵守について徹底していただき、適正に実行されますよう重ねてお願いします。

記

１自己点検結果の概要
・各所属において公物の記録媒体の管理が不十分である。
・私物の記録媒体（主にＵＳＢメモリ）の持ち込みが行われている。
　情報セキュリティポリシーで、私物のパソコン及び私物の記録媒体は持ち込みが禁止されています。緊急時などやむを得ない場合に持ち込む場合には必ず所属長の許可が必要です。
・個人情報などの重要情報を保存した記録媒体の管理が不十分である。
・記録媒体の処分時にデータを消去するなど、適正な処理が行われていない。

２是正方法
①１２月の自己点検時に提出した「情報セキュリティチェックシート」を確認
②違反者に対し事情を聴取
③「チェック項目の留意点」（別紙）を確認し、違反行為について是正

担当：教育総務課管理調整担当　小森　内線３５１４

別　紙

チェック項目の留意点

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象となりますので、以下の点に留意してください。

○ 情報資産の管理

（No.1）重要性分類Ⅱ以上の重要な情報は他と区別して管理されていますか？

情報資産を保護するには、重要性分類に応じて情報資産を分類し、分類に応じた管理を定める必要があります。情報資産の管理が不十分な場合、情報の漏えい、紛失等の情報セキュリティ事故が生じる怖れがあります。

（No.2）重要な情報を机上に置いたり、画面に表示したりしたまま席を外さないようにしていますか？

離席時に、記録媒体の使用後の保管や端末のロックを行い、第三者に使用されることがないようにする必要があります。管理が十分でない場合、記録媒体等の放置から生じる盗難や紛失、盗み見から生じる情報漏えいが発生することがあります。

（No.3）職場ではパソコン、記録媒体（FD、MO、CD、USB ﾒﾓﾘ等）などの盗難防止のための措置を講じていますか？

パソコンは、24時間の有人警備体制がない現地機関・学校等の場合、セキュリティワイヤーロックや施錠可能な場所への保管などの措置を講じる必要があります。

記録媒体は、来客者等に対し分かりにくい場所に保管したり、執務室内を無人にする際には施錠するなど、執務室内で盗難防止のための措置を講じる必要があります。

（No.4）職場で共有フォルダを設定している場合には、担当内など限られた者のみがアクセス可能な設定になっていますか？

アクセス管理が徹底されていない場合、情報の不正利用、情報漏えい、損傷、改ざん等の被害が生じる恐れがあります。共有フォルダの設定は、担当内限定、課内限定など、情報資産に応じて適切なアクセス管理をする必要があります。

（No.5）情報資産の持ち出しは禁止です。やむを得ず重要な情報を持ち出す場合には、所属長の許可を得ていますか？

パソコン、記録媒体の持ち出し限らず、私用のメールアドレスへの送信による情報の

持ち出しについても禁止しています。持ち出し先のパソコン等にセキュリティ対策が取られていない場合、情報漏えいが発生する恐れがあります。

○ パソコンの管理

（No.6）パソコンの持ち出しは禁止です。やむを得ず庁舎外に持ち出す場合には、所属長の許可を得ていますか？また、承認簿に必要事項を記録していますか？

情報の漏えいは、パソコンの持ち出しによる盗難や紛失が多いため、パソコンの持ち出しを禁止しています。やむを得ずパソコンを持ち出す場合には、「パソコン・端末等の持出/私物パソコンの持込・使用に関する申請・承認簿」（別紙4－2）により所属長の許可を得る必要があります。許可を受けたパソコンを持ち出す際には、目的以外の情報を保存しない、車上に放置しないなど、情報漏えいが発生しないように注意する必要があります。

（No.7）パソコン使用について、業務目的外の使用はしない、無許可ソフトウェアのインストールはしないなどの注意事項を遵守していますか？

パソコンの業務以外の使用、無許可ソフトウェアのインストールなどにより、コンピュータウイルス等の感染、情報漏えい等の被害や導入済みのソフトウェアに不具合が発生する恐れがあります。

○ 記録媒体の管理

（No.8）記録媒体の持ち出しは禁止です。やむを得ず持ち出す場合には、所属長の許可を得ていますか？また、承認簿に必要事項を記録していますか？

記録媒体の利用は所属で管理しているものを庁内で使用する場合に限定されています。やむを得ず記録媒体を持ち出す場合には、「パソコン・端末等の持出/私物パソコンの持込・使用に関する申請・承認簿」（別紙4－2）により所属長の許可を得る必要があります。

（No.9）重要性分類Ⅱ以上の重要な情報を記録した記録媒体は施錠可能な場所に保管していますか？

情報資産を保護するには、まず情報資産を分類し、分類に応じた管理方法を定める必要があります。個人情報や機密情報を記録した記録媒体は特に盗難や紛失が生じないように管理する必要があります。

（No.10）重要な情報については、バックアップを作成するなど、障害時や災害時に復旧が可能な状態にしていますか？

パソコン等の障害が発生した場合、公務の運営に支障が生じないようにするため、迅

速な復旧を行う必要があります。

○　私物パソコンの取扱

（No.11）私物パソコンの持ち込みは禁止です。やむを得ず私物パソコンを業務に使用する場合や私物パソコンを庁舎内に持ち込む場合には、所属長の許可を得ていますか？また、承認簿に必要事項を記録していますか？

庁内では、職員1人1台パソコンの体制となっているため、私物パソコンを持ち込む必要のない職場環境になっています。しかし、やむを得ず私物パソコンを業務に使用する場合や私物パソコンを庁舎内に持ち込む場合には、「パソコン・端末等の持出/私物パソコンの持込・使用に関する申請・承認簿」（別紙4－2）により所属長の許可を得る必要があります。

（No.12）許可された私物パソコンであっても、重要性分類Ⅰの情報処理は禁止です。こうした情報処理を行なっていませんか？

私物パソコンからの個人情報の漏えい事故の発生を防止するため、重要性分類Ⅰの情報処理をしないことを徹底してください。

（No.13）使用を許可された私物パソコンには、ウィルス対策を行っていますか？また、ファイル交換ソフトのインストールは厳禁です。遵守していますか？

私物パソコンの場合はコンピュータウイルス等の感染、情報漏えい等の対策を施していない可能性があります。許可を受けている前、パソコンのセキュリティ対策の状態を確認する必要があります。

○　私物記録媒体の取扱

（No.14）私物記録媒体の使用は禁止です。やむを得ず使用する場合には、所属長の許可を得ていますか？また、ウィルスに感染していないことを確認し、暗号化などのセキュリティ対策を講じていますか？

私物記録媒体を所属長の許可なく使用した場合、所属で情報の管理ができなくなるため、情報の持ち出しや情報漏えいの危険性が生じます。また、所属長の許可を受けて使用する場合であっても、私物記録媒体はセキュリティ対策が不十分なパソコン等で使用した可能性があるので、使用する前に必ずウィルスチェックをする必要があります。また、移動時には紛失や盗難に注意を払うとともに、紛失した場合に情報漏えいが起きないように暗号化などのセキュリティ対策が必要です。暗号化等のセキュリティ対策を行っていても、重要性分類Ⅰの情報を記録することは禁止しています。

○　記録媒体の処分

（No.15）記録媒体が不要となった場合には、重要性分類Ⅲ以上の情報について、すべての情報を消去し、情報を復元できないように処理していますか？

記録媒体が不要になっても、情報を消去せずに執務室の机等に保管している場合、無意識のうちに情報が漏えいすることがあります。保存されている情報が不明な記録媒体がある場合には、情報を確認の上不要と判断した場合、破砕等を行った上で廃棄してください。

（No.16）重要性分類Ⅱ以上の重要な情報資産の廃棄を行う場合には、所属長の許可を得ていますか？また、記録簿に必要事項を記録していますか？

情報資産の廃棄が確実に行われない場合、情報の漏えい、紛失等の被害が生じる恐れがあります。重要性分類Ⅱ以上の重要な情報資産の廃棄を行う場合には「情報資産の廃棄記録簿」（別紙4－1）により所属長の許可を得る必要があります。

○ インターネット使用

（No.17）インターネットの使用について、業務目的外の使用はしないなどの注意事項を遵守していますか？

地方公務員法第35条で、職務に専念する義務が定められています。業務に関係のない飲食店のサイトや株式サイトなど閲覧して業務を怠り、公務の運営に支障をきたしてはなりません。

○ 電子メール使用

（No.18）電子メールの使用について、業務目的外の使用はしない、送信元の不明なメールは速やかに削除するなどの注意事項を遵守していますか？

業務に関係のないメールを頻繁に行い、公務の運営に支障をきたしてはなりません。また、送信元の不明なメールは、ウィルス感染したファイルが添付されている可能性があるので、メールを開かずに速やかに削除してください。

（No.19）電子メールを送信する場合には、送信先に誤りがないか再確認していますか？

電子メール送信時に、送信先を再確認することにより誤送信を防止することができます。重要な電子メールを誤送信した場合には、情報セキュリティ責任者に報告する必要があります。

（No.20）複数人に電子メールを送信する場合には、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしていますか？（BCC による送信）

電子メールアドレスは、アドレスのつづりで個人が特定できる場合、個人情報に該当

する可能性があります。複数人に対して「TO」や「CC」で送信をすると、個人情報の漏えいに該当する場合があります。必要な場合以外は、「BCC」を利用してメールを送信する必要があります。

○ ID・パスワード管理

（No.21）ＩＤ・パスワードの設定や利用について、メモを作らない、他人と共有しないなどの注意事項を遵守していますか？

ID・パスワードが他人に知られた場合、情報システム等を不正に利用される恐れがあります。やむを得ずメモを作成する場合は、安全・確実に保管しなければなりません。また、情報セキュリティ責任者が認めた場合を除いて、職員等間でパスワードを共有してはなりません。

○ セキュリティ事故報告

（No.22）情報セキュリティに関する事故を発見した場合や発生する恐れがある場合には、所属長に報告していますか？

情報セキュリティ事故後に対応を行う目的は、情報セキュリティ事故による直接的、間接的被害を最小限に抑えることにあります。そのため、事故発生時には所属長へ報告し、事故対応のための体制を迅速に整える必要があります。

情報セキュリティ事故が発生した場合や事故が発生する恐れがある場合には、所属長に報告をする必要があります。報告方法については、「岐阜県情報セキュリティ事故対応マニュアル」を確認してください。