教総第３０９号
教研第４２２号
平成１９年１０月３日

各県立学校長様

教育総務課長
教育研修課長

情報セキュリティポリシーの改正に伴う私物パソコンの使用制限について（通知）

このことについて、岐阜県情報セキュリティポリシー（以下、「ポリシー」という。）が改正され、１０月９日付けで運用が開始される予定です。
本改正における大きなポイントは、「情報資産の持ち出し制限、私物パソコンの使用制限を強化」することです。

・情報資産の持ち出し制限、私物パソコンの使用制限を強化
　重要性分類Ⅰの情報資産（個人情報及びセキュリティの侵害が、住民の生命、財産等へ重大な影響を及ぼす情報資産）については私物パソコンによる情報処理を行ってはならない。

これにより、原則、私物パソコンによる個人情報の処理はできなくなりますが、「情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合」には、情報セキュリティ責任者（所属長）が、統括情報セキュリティ責任者（総合企画部長）の許可を得て、例外措置を取ることができます。
ついては、公的パソコンの絶対数が不足し、やむを得ず私物パソコンを使用しており、ただちに遵守できうる環境ではない県立学校においては、教育委員会において校内ＬＡＮアクセス用パソコンの更新・新規配備計画により整備が完了するまでの当分の間、個人情報を含む情報資産の私物パソコンによる情報処理に限り、例外措置の許可に関して、下記申請手続きによることとされましたので、申請していただきますようお願いします。
なお、ポリシーの改正の趣旨をご理解いただき、貴校教職員に対して、ポリシーを遵守することについて周知徹底していただきますようお願いします。

記

１改正概要
別添「岐阜県情報セキュリティポリシーの改正について」のとおり

２申請手続き
（１）毎年度当初に当該年度分の許可を得る。平成１９年度は、改正日から平成２０年３月３１日までの申請とする。
（２）各学校長は、３の申請様式を教育委員会（教育研修課）に提出する。教育委員会（教育総務課及び教育研修課）は、一括して統括情報セキュリティ責任者（総合企画部長）に申請する。

３申請様式
別紙様式のとおり

４提出先
教育研修課ＲＥＮＴＡＩ所属メール

５提出期限
平成１９年１０月９日（火）

担当	連絡先
教育総務課　管理調整担当　渡辺・小森	058-272-1111内線3514
教育研修課　情報化推進担当　藤田・櫛部	058-271-3457

別紙様式

○○第　　号
平成１９年１０月９日

統括情報セキュリティ責任者様

情報セキュリティ責任者　　○○○○学校長

岐阜県情報セキュリティポリシーに関する例外措置許可申請について

このことについて、下記のとおり許可くださいますようお願いします。

記

1　許可申請内容

重要性分類Ⅰの情報資産について、私物パソコンにより情報処理を行うことの許可

なお、私物パソコンの取扱いにあたっては、以下の事項を遵守します。
①私物パソコン及び私物の記録媒体に個人情報を含むデータは保存しない。
②私物パソコンの持ち込み及び業務での使用については、台帳により管理を行う。
③私物パソコンの持ち込み時には、コンピュータウイルスに感染していないこと及びファイル交換ソフトがインストールされていないことを確認する。

2　申請期間　　平成19年10月9日　～　平成20年3月31日

3　必要な理由

学校における情報処理業務の大半は、生徒等の個人情報を含むものである。また、同一生徒の情報を複数の教員が扱うという処理も行っている。本校では、独自のシステムにより情報処理を行っているが、現状では、その処理に必要な県備品のパソコンが不足しているため、教員の私物パソコンの使用を認めなければ業務に著しく支障を来たすこととなるため、許可を申請するものである。（各学校に応じた理由を記載）

4　例外措置の適用を受ける職員及び業務の範囲

	職　名	氏　名	職員番号	業務分類		
1	教諭	△△　□□	11111	3　教務	4　進路指導	
2	教諭			1　学級担任		
3	教諭			2　教科担任	5　生徒指導	6　特別活動
4	養護教諭			7　保健厚生		
5	講師			2　教科担任		
6	非常勤講師			2　教科担任		
7	事務職員			8　図書		
8	等					
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						

業務分類表

○学校で取り扱う個人情報

A　生徒管理	B　評価処理	C　出欠処理	D　各種証明書
1 生徒名簿	1 成績処理	1 出欠状況	1 奨学金申請書
2 保護者名簿	2 成績伝票	2 出欠理由	2 成績証明書
3 個人票	3 成績一覧表	3 学級日誌等	3 在学証明書
4 健康ﾃﾞｰﾀ	4 欠点者一覧表	4 特別指導記録	4 その他
5 運動能力ﾃﾞｰﾀ	5 成績会議資料	5 その他	
6 各種調査ﾃﾞｰﾀ	6 通知票		
7 緊急連絡網	7 調査書･推薦書		
8 指導記録	8 特別指導資料		
9 指導要録	9 授業記録		
10 卒業者名簿	10 その他		
11 その他			

○業務分類

1　学級担任	すべての項目（A1～D4）
2　教科担任	A1、A3、B1～B10、C1～C5
3　教務	すべての項目（A1～D4）
4　進路指導	A1～A3、A6、A8～A11、B7～B10
5　生徒指導	A1～A4、A6～A8、A10～A11、B7～B10、C1～C5
6　特別活動	A1～A8、A10～A11、C1～C2、C5
7　保健厚生	A1～A8、A11、C1～C5
8　図書	A1、A3
9　渉外	A1～A3、A6、A10～A11
10　その他(　　)	

※複数回答可

岐阜県情報セキュリティポリシーの改正について

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

情報セキュリティポリシー改正の必要性

○　現行の情報セキュリティポリシーは、総務省が平成１３年に策定した「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づき、平成１４年度に制定された。そのガイドラインが、5年ぶりに全面改定されたことから、その経緯と内容をふまえて現行の情報セキュリティポリシーを再検討する必要があった。

＜新ガイドラインの背景＞
・個人情報の漏えい等の情報セキュリティ侵害事案の状況
・情報セキュリティに関する新たな対策技術の動向
・政府の「第1次情報セキュリティ基本計画」に基づく改定　　等
＜ガイドライン改正のポイント＞
・最近の技術的動向をふまえたこと
・表現を簡素でわかりやすく変更
・高度な対策を推奨事項として盛り込んでいること

○　ＵＳＢメモリやWinnyといった新たな技術に対する情報セキュリティ対策は、その緊急性から通知により対応してきたが、これらの対策も情報セキュリティポリシーにおいて規定する必要があった。

○　平成１８年度に実施した外部監査において、情報セキュリティポリシーへの指摘事項に関する修正を行う必要があったこと。

＜主な指摘事項＞
・現在、情報セキュリティポリシーは公開して、対策を行っていることをアピールすることが一般的であるので、積極的に公開すべき。
・情報の複製に関する規定がない。

改正の主なポイント　基本方針・対策基準　共通１

○ *情報セキュリティポリシーの公開について*

＜現行＞
岐阜県情報セキュリティ基本方針に関する規定　＝　「訓令乙」文書となっており公表されていない。
岐阜県情報セキュリティ対策基準要綱　＝　「基本方針に関する規定」第７条３項で非公開となっている。

＜改正＞
岐阜県情報セキュリティ基本方針　＝　公開文書とする。(県ポータルなどで公開)
岐阜県情報セキュリティ対策基準　＝　公開文書とする。

＜ガイドライン＞
・「基本方針」を地方公共団体が積極的に情報セキュリティ対策に取り組み、情報セキュリティの確保を図ることを住民に示すものであると定義し、公開されることを前提としている。
・「対策基準」においても、旧ガイドラインでは「対策基準」と「運用手順」を非公開としていたが、新ガイドラインでは具体的かつ詳細な手順が記載されている「運用手順」のみを非公開としている。
＜外部監査指摘事項＞
・情報セキュリティポリシーを公開すべきである。
＜他県の状況＞
・基本方針を公開している都道府県　７１％
・対策基準を公開している都道府県　２８％　(非公開としている都道府県は旧ガイドラインに準拠しているため)

＜改正の考え方＞
・基本方針については、積極的に公開し岐阜県が情報セキュリティ対策に取り組んでいることを宣言する。
・対策基準についても、各条文を精査した結果、公開により岐阜県の行政の運営に支障を及ぼす恐れがないことから公開とする。
但し対策実施手順については各情報システムの詳細が記載されているため非公開のままとする。
(改正案　第１０条)

改正の主なポイント 基本方針・対策基準 共通2－1

○ 適用範囲の明確化

＜現行＞

（基本方針）

第4条 県の機関（公安委員会（警察本部を含む。）を除く。以下同じ。）における情報セ

キュリティ対策は、全てこの規程に定める情報セキュリティポリシーを遵守する必要が

あるものとする。

2 知事部局以外の県の機関においては、この規程に準じて必要な規程等の整備を行

うものとする。

（対策基準）

1 組織・体制

(2) 情報セキュリティ委員会

情報セキュリティ委員会の構成が、公安委員会を除くすべての機関である。

＜改正＞

（基本方針）

第2条

1 機関

基本方針が適用される機関の範囲は、知事部局、議会事務局、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、内水面漁場管理委員会とする。

2 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

(1) ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

(2) ネットワーク及び情報システムで取り扱う情報

(3) 情報システムの仕様書及びネットワーク図等のシステム関連文書

（対策基準）

1 対象範囲

(1) 機関

岐阜県情報セキュリティ対策基準（以下「対策基準」という。）が適用される機関の範囲は、知事部局、議会事務局、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、内水面漁場管理委員会とする。

(2) 情報資産の範囲

対策基準が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

改正の主なポイント 基本方針・対策基準 共通2－2

＜新ガイドライン＞
（1） 行政機関の範囲
本対策基準が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。
（2） 情報資産の範囲
本対策基準が対象とする情報資産は、次のとおりとする。
①ネットワーク、情報システム、これらに関する設備、電磁的記録媒体
②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
③情報システムの仕様書及びネットワーク図等のシステム関連文書

＜改正の考え方＞
・情報セキュリティ対策への取り組む機関と対策を講じる情報資産の範囲を明示する必要がある。

※ガイドラインの （これらを印刷した文書を含む） を採用しないことについて
①情報セキュリティポリシーは、公文書の中でも特に電子システムに含まれる情報資産に対する脅威へのセキュリティ対策について実施を確実に行われることを目的としていること。
②現場において、システムからの印刷物と県民や国などからの文書を一緒に保管する場合などが実務上頻繁にあるためこれらの取扱について混乱などを避けるため。

改正の主なポイント　対策基準１

○　管理区域（情報システム室）の入退室管理等についての規定を追加

改　　正	現　　行
4　物理的セキュリティ対策 （1）管理区域（情報システム室等）の管理 ②管理区域の入退室管理等 ア　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。 イ　職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。 ウ　情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じ、立ち入り区域を制限し、管理区域への入退室を許可された職員等を付き添わせるよう措置をとらなければならない。 ③機器等の搬入出 ア　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した事業者に確認を行わせなければならない。 イ　情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち会わなければならない。	「情報セキュリティ対策実施手順」で規定

＜ガイドラインの趣旨＞
・情報システム室（ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行う部屋）は、重要な情報資産が大量に保管されており、特に厳格に管理する必要がある。情報システム室が適切に管理されていない場合には、情報の盗難等による重大な被害が発生するおそれがあり、そうした危険を回避するための入退室管理を行う必要がある。

＜改正の考え方＞
・本県においては、情報企画課の他に原課が管理している情報システム室が複数あり、昨年度の外部監査及び内部監査における入退室管理が十分でないとの指摘を踏まえ「対策基準」において規定する。

改正の主なポイント　対策基準２－１

○ 情報資産の持ち出し制限、私物パソコンの使用制限を強化

改　　正	現　　行
5　人的セキュリティ対策 (1) 職員等の遵守事項 ③パソコン等の端末等の持ち出し及び持ち込みの制限 ア　職員等は、パソコン等の端末、記録媒体及びその他の情報資産を庁舎外に持ち出しはならない。やむを得ない理由により、これらを持ち出す場合には情報セキュリティ責任者の許可を得なければならない。 イ　職員等は、私物のパソコン及び記録媒体を庁舎内に持ち込んではならない。やむを得ない理由により、これらを持ち込む場合には情報セキュリティ責任者の許可を得なければならない。 ウ　情報セキュリティ責任者は、端末等の持ち出し及び持ち込みについて、記録を作成、保管しなければならない。 ④私物パソコン等を使用した業務の制限 ア　職員等は、情報セキュリティ責任者の許可を得ず以下の行為を行ってはならない。 (ア) 私物パソコンを用いて業務を行うこと。 (イ) 私物の外部記憶装置に業務情報を記録すること。 (ウ) 業務上のメール又は情報を私用のメールアドレスへ送信すること。 イ　職員等は、情報セキュリティ責任者の許可を得て、私物パソコン等を使用して業務を行う場合は、当該パソコンにウイルス対策等必要な情報セキュリティ対策を講じなければならない。 ウ　職員等はイの規定に関わらず、重要性分類Ⅰの情報資産については、私物パソコンによる情報処理を行ってはならない。	4　人的セキュリティ対策 (1) 職員等の義務 ア職員等 (イ) 情報の保護 ② 職員等は、情報セキュリティ責任者の許可を得ず、パソコン等を執務室外に持ち出してはならない。 ・通知文書「個人情報の持ち出し等による漏えい等の防止について」(H18.3.8　情シ第339号) により対応 ・情報セキュリティチェックシートにより対応

改正の主なポイント　対策基準２－２

○ *情報資産の持ち出し制限、私物パソコンの使用制限を強化*

＜ガイドラインの趣旨＞
・私物のパソコン、記録媒体を持ち込むことは原則禁止し、無許可での行政情報等を記録、持ち出す行為を防止する必要がある。
・私物パソコンの使用を許可する場合にも、管理者は、私物パソコンにコンピュータウィルスチェックやWinny等ファイル共有ソフトウエアの導入がされていないかを確認させる必要がある。
・特に個人情報を含む機密性の高い情報資産については、私物パソコンでの作業を禁止する必要がある。

＜改正の考え方＞
・県においても私物パソコンの紛失、盗難事故が発生していることを踏まえ、私物のパソコン及び記録媒体の持ち込みの制限についてガイドラインに準拠し規定を追加する。
・端末等の持ち出し、持ち込みについて情報セキュリティ責任者（所属長）の許可を得て行っていることを確実にするため、その記録を作成、保管する規定を追加する。
・個人情報等を含む情報資産については、機密性を確保する観点から私物パソコンでの処理を禁止する。

改正の主なポイント　対策基準３

○ 無線LAN及びネットワークの盗聴対策を追加

改　　正	現　　行
5　技術的セキュリティ対策 (1) コンピュータ及びネットワークの管理 ⑪無線LAN及びネットワークの盗聴対策 情報システム管理者は、無線LANを使用する場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。	規定なし ・実際の対応：無線LANの暗号化通信は既にを行っている。H19年度事業において、より高度な暗号化方法を採用し通信対策を強化している。

＜ガイドラインの趣旨＞
・特に無線LANを利用する際には、管理が不十分な場合、不正利用によるシステムへの攻撃、情報漏えい、改ざん等の被害が生じるおそれがあるので、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。

＜改正の考え方＞
・県のRENTAlにおいては、9割以上が無線LANを利用している状況を踏まえ、暗号化措置等による情報セキュリティを確保する必要があることから、ガイドラインに準拠して規定する。

改正の主なポイント　対策基準４

○ 電子メールの利用に関するセキュリティ対策を強化

改　　正	現　　行
6　技術的セキュリティ対策 (1) コンピュータ及びネットワークの管理 ⑬電子メールの利用制限 ア　職員等は、自動転送機能を用いて、電子メールを転送してはならない。 イ　職員等は、業務上必要のない送信先に電子メールを送信してはならない。 ウ　職員等は、複数人に電子メールを送信する場合、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なければならない。 エ　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ責任者に報告しなければならない。情報セキュリティ責任者は当該情報に個人情報等重要情報が含まれる場合は、速やかに情報セキュリティ対策管理部会に報告しなければならない。 オ　職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。	・通知文書「電子メールの送信誤りによる個人情報漏えい等の防止の徹底について」（H19.5.17　情企第127号）により対応 ・情報セキュリティチェックシートにより対応

＜ガイドラインの趣旨＞
・不正な情報の持ち出しを禁止する観点から、電子メールの自動転送を禁止する。
・プロバイダーが提供するサービスである、フリーメールやオンラインストレージサービスに対しては、外部への不正な情報の持ち出し等に利用される場合があることから、禁止する必要がある。

＜改正の考え方＞
・電子メールを利用した業務が一般化しているため、電子メールの利用制限について「対策基準」で明確に規定する。
・県においてファイルの添付誤り、送信方法の誤り等による情報漏えい事案が発生している状況を踏まえ、電子メールの利用制限についてガイドラインに準拠して規定する（ア、イ、ウ及びオ）。
・電子メールの誤送信による事故は、すばやい対応が必要となることから、事故報告について規定する。

改正の主なポイント　対策基準５

○ *例外措置に関する規定を追加*

改　　正	現　　行
7　運用 （5）例外措置 ①例外措置の許可 情報セキュリティ責任者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、統括情報セキュリティ責任者の許可を得て、例外措置を取ることができる。 ②緊急時の例外措置 情報セキュリティ責任者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに統括情報セキュリティ責任者に報告しなければならない。	・各事案に対し情報セキュリティ統括責任者等との協議により対応している

＜ガイドラインの趣旨＞
・情報セキュリティポリシーをそのまま適用した場合に、行政事務の適正な遂行を著しく妨げるなどにより、これに代わる方法によることやポリシーに定められた事項を実施しないことを認めざるを得ない場合についての例外措置の規定を設ける。

＜改正の考え方＞
・情報セキュリティポリシーの適用について、事務上著しく不都合が生じる場合の対応について例外措置規定を設ける。