令和６年度第３回龍ケ崎市情報セキュリティ委員会

日時：令和７年２月１０日（月）
情報化推進委員会終了後
場所：庁議室

１　令和６年度下半期情報セキュリティ内部監査の結果について

２　私物スマートフォンの業務での使用について
（龍ケ崎市コンピュータ等運用管理規程の一部改正）

３　龍ケ崎市保有個人情報安全管理措置規程について

４　その他

令和６年度（下半期）情報セキュリティ内部監査実施報告書

１　監査概要

（１）監査目的

情報セキュリティ内部監査は、龍ケ崎市情報セキュリティ内部監査実施規程（以下「監査規程」という。）第１１条の規定に基づき、情報セキュリティを維持・管理する仕組みが組織において適切に整備・運用されているかを点検し、評価するものです。

人的セキュリティ、物理的セキュリティ、情報セキュリティ研修受講状況、情報資産の管理、特定個人情報の取扱い、住民情報基幹系システムにおける電子データの保管等に関し、龍ケ崎市情報セキュリティ規則及び龍ケ崎市情報セキュリティ対策に関する規程等に基づき、適切に実施されているかを点検・評価し、課題については、システムの運用状況などを考慮しながら、個別に原因を究明した後に改善内容等を被監査部門に提示及び当該措置の実施により、情報資産、情報システム等の適切な運用を図ることを目的としております。

（２）監査対象課等及び対象システム

監査対象課等

健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局

対象システム

住民情報基幹系システム、イントラネット系システム、各課等が管理及び所有しているシステム

（３）監査実施日

令和６年１２月２６日（木）、２７日（金）

（４）監査実施体制

監査実施責任者：デジタル都市推進課長（監査規程第３条第２項）

監査担当部門：デジタル都市推進課（監査規程第３条第１項）

（５）監査の基準となる根拠

・龍ケ崎市情報セキュリティ規則・龍ケ崎市コンピュータ等運用管理規程
・龍ケ崎市情報セキュリティ対策に関する規程・龍ケ崎市電子文書取扱規程
・龍ケ崎市個人情報の保護に関する法律施行条例
・龍ケ崎市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に基づく個人番号の利用及び特定個人情報の提供に関する条例

・地方公共団体における情報セキュリティに関する監査ガイドライン（総務省）
・特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）

２　監査結果

（総評）

本市の情報セキュリティ対策に関しては、龍ケ崎市情報セキュリティ規則及び龍ケ崎市情報セキュリティ対策に関する規程からなる龍ケ崎市情報セキュリティポリシーを基に、デジタル都市推進課が事務局となって定期的な研修を行い、また、e-Learningの受講によりセキュリティ対策に関しての意識高揚を図っている。

今回の内部監査においては、対象課等から提出のあった各種チェックシート等の確認に加えて、対象課等職員に対するヒアリングを行い、情報セキュリティ対策が適切に行われているか確認した。また、特定個人情報を取り扱っている課においては、「特定個人情報の適正な取扱いに係るチェックリスト」により、特定個人情報の取扱い状況等も確認したところであり、より適正な取扱いに資するものであると考えられる。特定個人情報の適正な取扱いについて引き続きガイドライン等に基づき適正な取扱いに努めたい。

監査の結果としては、デスクトップへのファイルの貼付け等がいまだ見受けられる課があり、それについては情報セキュリティ事故につながる可能性が高く、直ちに是正を指示した。またファイルサーバの整理について、整理方法が各課ごとに異なっており、不要なファイル等も消去されておらず、その結果ファイルサーバの全体的な容量の圧迫を招いている状況であった。今後は、ファイリングの考え方に従い、文書保存年限が満了し廃棄する文書等は、併せてファイルサーバのデータについても消去を促していきたい。そのほか、業務に関係のないサイト等の閲覧が確認された課等もあったが、すぐに是正等を行わせ指摘事項とは至らなかった。それら事項については、今後も継続して指導を行っていくが、龍ケ崎市情報セキュリティポリシー等に則り、課内全職員で取り組む必要がある。

３　課別監査結果

別紙「令和６年度（下半期）情報セキュリティ内部監査結果一覧」のとおり

○人的セキュリティ

監査項目	適正に実施している課等	改善が必要な課等	改善内容等
１　情報資産等の業務以外の目的での使用禁止(職員等による業務以外の目的での	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	

情報資産の持ち出し、又は情報システムへのアクセス禁止）			
２　私物パソコン等の持込制限（職員等による私物のパソコン及び記録媒体の庁舎内への持込は行われていない。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
３(1)　パソコンの取扱い（離席時には、パソコンの第三者使用を防止するための適切な措置が講じられている。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
３(2)　パソコンの取扱い（デスクトップに文書等を保存していない。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	一部デスクトップに文書等を保存している課も見受けられたが、改善あり。
４　ＩＤ･パスワードの取扱い（職員等のパスワードは当該本人以外に知られないように取扱われている。また、定期的にパスワードを変更している。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
５　イントラネットにおけるメール送信（「ｔｏ」、「ｃｃ」、「ｂｃｃ」を正しく使い分けている。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
６(1)　公務用ＵＳＢメモリの取扱い（公務	健康増進課、介護保険課、下水道課、文化・生涯学習	なし	

用ＵＳＢメモリの中にデータを保存していない。）	課、学校給食センター、監査委員事務局		
６(2)　公務用ＵＳＢメモリの取扱い(公務用ＵＳＢメモリは使用するとき以外は適正に保管されている	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
７　セキュリティ研修への参加(職員等が積極的にセキュリティ研修に参加している。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	

○物的セキュリティ

監査項目	適正に実施している課等	改善が必要な課等	改善内容等
１　機器の取付け(サーバ､ＨＵＢ等を取付ける際､埃､振動等の影響を可能な限り排除した場所に設置し､容易に取外せないように固定するなどの対策が講じられているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
２　通信ケーブル等の保護(通信ケーブルや電源ケーブルの損傷を防止するための対策が講じられているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
３　机上のパソコンの取扱い(退庁時におけるノートパソコンは施錠できる保管庫で管理を行ってい	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	

る。）			
４　サーバの機器の定期保守（サーバの機器の定期保守が実施されているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	一部保守体制等が明確になってない課も見受けられたが、改善あり。
５　サーバ障害対策の手順（サーバに障害が発生した場合の対策手順が定められ、文書化されている。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	一部障害対策手順が明確になってない課も見受けられたが、改善あり。

○特定個人情報の適正な取扱い

監査項目	適正に実施している課等	改善が必要な課等	改善内容等
１　特定個人情報の取得について（業務手順が定められているか。裏面を見ない等の対応が周知徹底されているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
２　特定個人情報の利用について（職員を限定しているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
３　特定個人情報の保存について（文書管理規定により正しい保存年限を設定しているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
４　特定個人情報の削除・廃棄について（機密文書として適切に削除・廃棄している	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食セ	なし	

か。）	ンター、監査委員事務局		
５　特定個人情報の取扱い体制について（届出を行い、取扱者や範囲を定めているか。持ち運ぶ際の措置を講じているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
６　特定個人情報の運用について（指定範囲の外に持ち出していないか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
７　情報漏えい事案に対する体制（龍ケ崎市情報セキュリティ事故等手順書により対応できるか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	
８　特定個人情報事務取扱担当の監督、教育（所属長による取扱い確認が行われているか。）	健康増進課、介護保険課、下水道課、文化・生涯学習課、学校給食センター、監査委員事務局	なし	

令和６年度（下半期）情報セキュリティ内部監査結果一覧

Ⅰ　人的セキュリティに関して

監査内容	健康	介護	下水	文化	給食	監査
1　情報資産等の業務以外の目的での使用禁止	○	○	○	△	○	○
2　パソコンの取扱い（1）離席時におけるパソコンの第三者使用を防止措置	○	○	○	○	○	○
2　パソコンの取扱い（2）デスクトップ上でのデータの保存禁止	△	△	△	△	○	△
3　ＩＤ・パスワードの取扱い（他人に教えない、ログイン時に記憶させない、失念しない）	○	○	○	○	○	○
4　イントラネットにおけるメール送信（「ｔｏ」、「ｃｃ」、「ｂｃｃ」の使い分け）	○	○	○	○	○	○
5　公務用USBメモリの取扱い（1）データの保存禁止	○	○	○	○	○	○
5　公務用USBメモリの取扱い（2）適正な保管（施錠管理）	○	○	○	○	○	○
6　セキュリティ研修への参加（職員の情報セキュリティ研修への参加）	○	○	○	○	○	○

Ⅱ　物的セキュリティに関して

監査内容	健康	介護	下水	文化	給食	監査
1　ノートパソコン等の取扱い（1）水濡れによる故障の予防	○	○	○	○	○	○
1　ノートパソコン等の取扱い（2）衝撃、圧迫等による故障の予防	○	○	○	○	○	○
1　ノートパソコン等の取扱い（3）管理方法（施錠管理）	○	○	○	○	○	○
2　サーバ機器等の取り扱い（1）定期的な点検の実施	○	○	○	○	○	－
2　サーバ機器等の取り扱い（2）障害発生時の対応手順を定め、文書化	○	○	△	○	○	－
3　周辺機器の取り扱い	○	○	○	○	○	○
4　情報資産の管理について	○	△	○	○	○	○

○：適正　　△：監査指導により改善　　×：改善を要する　　－：該当なし

Ⅲ　特定個人情報の適切な取扱いに関して

監査内容	健康	介護	下水	文化	給食	監査
1　特定個人情報の取得について（取得手順が定められているか。裏面を見ない等の対応が周知徹底されているか。）	○	○	－	－	－	－
2　特定個人情報の利用について（利用職員が限定されているか。）	○	○	－	－	－	－
3　特定個人情報の保存・削除・廃棄について（文書管理規定により正しい保存年限を設定しているか。また、機密文書として適切に削除・廃棄しているか。）	○	○	－	－	－	－
4　特定個人情報の取扱い体制について（届出を行い、取扱者や範囲を定めているか。持ち運ぶ際の措置を講じているか。）	○	△	－	－	－	－
5　特定個人情報の運用について（指定範囲の外に持ち出していないか。）	○	○	－	－	－	－
6　情報漏えい事案に対する体制（龍ケ崎市情報セキュリティ事故等手順書により対応できるか。）	○	○	○	○	○	○
7　特定個人情報事務取扱担当の監督、教育（所属長による取扱い確認が行われているか。職員に対して研修等により教育を行っているか。）	○	○	○	○	○	○
備考（特定個人情報の取扱い）	検診	介護保険	関係事務	関係事務	関係事務	関係事務

Ⅳ　住民情報基幹系ファイルサーバ内の電子データ等の適正な取扱いに関して

監査内容	健康	介護	下水	文化	給食	監査
1　基幹系ファイルサーバ内のデータは、原則、文書管理に準じて分類している。	○	△	○	○	○	－
2　職員の個人名等のフォルダにデータを保管していない。	○	○	△	○	△	－
3　使用しなくなったデータは適宜消去している。	△	△	○	△	○	－
4　マイナンバーなど重要な電子データが含まれるファイルには、パスワードをかけて保存している。	○	△	○	○	○	－
5　基幹系システム（総合福祉システム、健康管理システム含む）の端末のデスクトップに電子データを貼り付けしていない。	○	△	○	○	○	－
6　原則、基幹系システムのデータ以外は、基幹系ファイルサーバに保管しない。	○	○	○	○	○	－

○：適正　　△：監査指導により改善　　×：改善を要する　　－：該当なし

様式第３号（第12条、第15条関係）

情報セキュリティ内部監査結果報告書

令和7年2月10日

1	監査目的	各課等において、情報セキュリティを維持・管理する仕組みが適切に運用されているかを点検し、情報セキュリティ事故等の未然防止に資するとともに市が管理する情報資産の保護に努める。
2	監査範囲	（１）イントラネット系システム （２）住民情報基幹系システム （３）その他各課等で使用しているシステム
3	被監査部門	健康増進課
4	監査方法	（１）監査項目（提出書類）の確認 （２）遠隔操作によるシステム等の管理状況の確認 ア．ログ（端末の操作記録）の確認等 イ．デスクトップ上のデータ確認 （３）職員へのヒアリング
5	監査実施日程	令和６年１２月２６日（木）
6	監査項目	（１）人的セキュリティに関する管理状況 （２）物理的セキュリティに関する管理状況 （３）情報セキュリティ研修受講記録状況 （４）情報資産管理状況 （５）特定個人情報の適正な取扱い状況等 （６）基幹系システムにおけるデータの管理状況　など
7	適用基準	（１）龍ケ崎市情報セキュリティ規則 （２）龍ケ崎市情報セキュリティ対策に関する規程 （３）龍ケ崎市コンピュータ等運用管理規程 （４）龍ケ崎市電子文書取扱規程 （５）　龍ケ崎市個人情報の保護に関する法律施行条例　など

〇人的セキュリティに関して
　概ね適正に運用が行われている。一部職員において、デスクトップへのデータ等の貼り付けが見られたが、改善が図られているため、今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

〇物的セキュリティに関して
　課にて調達している端末等について、情報資産管理簿にて適切に管理するとともに、万一の障害に備え連絡体制等を明確にすること。
指摘事項：なし

〇特定個人情報の適切な取扱いに関して
　概ね適正に取り扱われている。特定個人情報については、個人情報よりもさらに厳格な取り扱いが求められているとともに、事件・事故の際には罰則規定も設けられている。引き続き適正に管理・運用すること。
指摘事項：なし

〇住民情報基幹系ファイルサーバ内の電子データ等の適正な取扱いに関して
　データの整理について指導・改善を行った。引き続き適正な取扱いに努めること。
指摘事項：なし

様式第３号（第12条、第15条関係）

情報セキュリティ内部監査結果報告書

令和7年2月10日

1	監査目的	各課等において、情報セキュリティを維持・管理する仕組みが適切に運用されているかを点検し、情報セキュリティ事故等の未然防止に資するとともに市が管理する情報資産の保護に努める。
2	監査範囲	（１）イントラネット系システム （２）住民情報基幹系システム （３）その他各課等で使用しているシステム
3	被監査部門	介護保険課
4	監査方法	（１）監査項目（提出書類）の確認 （２）遠隔操作によるシステム等の管理状況の確認 ア．ログ（端末の操作記録）の確認等 イ．デスクトップ上のデータ確認 （３）職員へのヒアリング
5	監査実施日程	令和６年１２月２６日（木）
6	監査項目	（１）人的セキュリティに関する管理状況 （２）物理的セキュリティに関する管理状況 （３）情報セキュリティ研修受講記録状況 （４）情報資産管理状況 （５）特定個人情報の適正な取扱い状況等 （６）基幹系システムにおけるデータの管理状況　など
7	適用基準	（１）龍ケ崎市情報セキュリティ規則 （２）龍ケ崎市情報セキュリティ対策に関する規程 （３）龍ケ崎市コンピュータ等運用管理規程 （４）龍ケ崎市電子文書取扱規程 （５）　龍ケ崎市個人情報の保護に関する法律施行条例　など

○人的セキュリティに関して
　概ね適正に運用が行われている。一部職員において、デスクトップへのデータ等の貼り付けが見られたが、改善が図られているため、今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

○物的セキュリティに関して
　資産管理台帳について、現在の状況を精査し更新すること。
指摘事項：なし

○特定個人情報の適切な取扱いに関して
　概ね適正に取り扱われている。特定個人情報取扱者に変更が生じた際は、随時「特定個人情報取扱者登録届」を提出すること。特定個人情報については、個人情報よりもさらに厳格な取り扱いが求められているとともに、事件・事故の際には罰則規定も設けられている。引き続き適正に管理・運用すること。
指摘事項：なし

○住民情報基幹系ファイルサーバ内の電子データ等の適正な取扱いに関して
　データの整理について指導・改善を行った。引き続き適正な取扱いに努めること。
指摘事項：なし

様式第３号（第12条、第15条関係）

情報セキュリティ内部監査結果報告書

令和7年2月10日

1	監査目的	各課等において、情報セキュリティを維持・管理する仕組みが適切に運用されているかを点検し、情報セキュリティ事故等の未然防止に資するとともに市が管理する情報資産の保護に努める。
2	監査範囲	（１）イントラネット系システム （２）住民情報基幹系システム （３）その他各課等で使用しているシステム
3	被監査部門	下水道課
4	監査方法	（１）監査項目（提出書類）の確認 （２）遠隔操作によるシステム等の管理状況の確認 ア．ログ（端末の操作記録）の確認等 イ．デスクトップ上のデータ確認 （３）職員へのヒアリング
5	監査実施日程	令和６年１２月２６日（木）
6	監査項目	（１）人的セキュリティに関する管理状況 （２）物理的セキュリティに関する管理状況 （３）情報セキュリティ研修受講記録状況 （４）情報資産管理状況 （５）特定個人情報の適正な取扱い状況等 （６）基幹系システムにおけるデータの管理状況　など
7	適用基準	（１）龍ケ崎市情報セキュリティ規則 （２）龍ケ崎市情報セキュリティ対策に関する規程 （３）龍ケ崎市コンピュータ等運用管理規程 （４）龍ケ崎市電子文書取扱規程 （５）　龍ケ崎市個人情報の保護に関する法律施行条例　など

〇人的セキュリティに関して
　概ね適正に運用が行われている。今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

〇物的セキュリティに関して
　概ね適正に運用が行われている。今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

〇住民情報基幹系ファイルサーバ内の電子データ等の適正な取扱いに関して
　概ね適正に運用が行われている。今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

様式第３号（第12条、第15条関係）

情報セキュリティ内部監査結果報告書

令和7年2月10日

1	監査目的	各課等において、情報セキュリティを維持・管理する仕組みが適切に運用されているかを点検し、情報セキュリティ事故等の未然防止に資するとともに市が管理する情報資産の保護に努める。
2	監査範囲	（１）イントラネット系システム （２）住民情報基幹系システム （３）その他各課等で使用しているシステム
3	被監査部門	文化・生涯学習課
4	監査方法	（１）監査項目（書類）の確認 （２）遠隔操作によるシステム等の管理状況の確認 ア．ログ（端末の操作記録）の確認等 イ．デスクトップ上のデータ確認 （３）職員へのヒアリング
5	監査実施日程	令和６年１２月２７日（金）
6	監査項目	（１）人的セキュリティに関する管理状況 （２）物理的セキュリティに関する管理状況 （３）情報セキュリティ研修受講記録状況 （４）情報資産管理状況 （５）特定個人情報の適正な取扱い状況等 （６）基幹系システムにおけるデータの管理状況　など
7	適用基準	（１）龍ケ崎市情報セキュリティ規則 （２）龍ケ崎市情報セキュリティ対策に関する規程 （３）龍ケ崎市コンピュータ等運用管理規程 （４）龍ケ崎市電子文書取扱規程 （５）　龍ケ崎市個人情報の保護に関する法律施行条例　など

〇人的セキュリティに関して
　概ね適正に運用が行われている。一部において、業務に関係の無いサイトの閲覧も見受けられたため、指導・改善を行うこと。
指摘事項：なし

〇物的セキュリティに関して
　概ね適正に取り扱われている。独自調達システムについて、障害発生時の一時切り分けとしての手順書等を整え、障害の早急な復旧を図れる体制とすること。
指摘事項：なし

〇住民情報基幹系ファイルサーバ内の電子データ等の適正な取扱いに関して
　不必要なファイルを整理し、今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

様式第３号（第12条、第15条関係）

情報セキュリティ内部監査結果報告書

令和7年2月10日

1	監査目的	各課等において、情報セキュリティを維持・管理する仕組みが適切に運用されているかを点検し、情報セキュリティ事故等の未然防止に資するとともに市が管理する情報資産の保護に努める。
2	監査範囲	（１）イントラネット系システム （２）住民情報基幹系システム （３）その他各課等で使用しているシステム
3	被監査部門	学校給食センター
4	監査方法	（１）監査項目（書類）の確認 （２）遠隔操作によるシステム等の管理状況の確認 ア．ログ（端末の操作記録）の確認等 イ．デスクトップ上のデータ確認 （３）職員へのヒアリング
5	監査実施日程	令和６年１２月２６日（木）
6	監査項目	（１）人的セキュリティに関する管理状況 （２）物理的セキュリティに関する管理状況 （３）情報セキュリティ研修受講記録状況 （４）情報資産管理状況 （５）特定個人情報の適正な取扱い状況等 （６）基幹系システムにおけるデータの管理状況　など
7	適用基準	（１）龍ケ崎市情報セキュリティ規則 （２）龍ケ崎市情報セキュリティ対策に関する規程 （３）龍ケ崎市コンピュータ等運用管理規程 （４）龍ケ崎市電子文書取扱規程 （５）　龍ケ崎市個人情報の保護に関する法律施行条例　など

○人的セキュリティに関して
　概ね適正に運用が行われている。今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

○物的セキュリティに関して
　概ね適正に取り扱われている。今後独自調達システムが新たにオンプレミスとして稼働するため、保守体制を整え、ICT-BCP訓練に参加するなど万一の障害に備えること。
指摘事項：なし

○住民情報基幹系ファイルサーバ内の電子データ等の適正な取扱いに関して
　概ね適正に運用が行われている。今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

様式第３号（第12条、第15条関係）

情報セキュリティ内部監査結果報告書

令和7年2月10日

1	監査目的	各課等において、情報セキュリティを維持・管理する仕組みが適切に運用されているかを点検し、情報セキュリティ事故等の未然防止に資するとともに市が管理する情報資産の保護に努める。
2	監査範囲	（１）イントラネット系システム （２）その他各課等で使用しているシステム
3	被監査部門	監査委員事務局
4	監査方法	（１）監査項目（書類）の確認 （２）遠隔操作によるシステム等の管理状況の確認 ア．ログ（端末の操作記録）の確認等 イ．デスクトップ上のデータ確認 （３）職員へのヒアリング
5	監査実施日程	令和６年１２月２６日（木）
6	監査項目	（１）人的セキュリティに関する管理状況 （２）物理的セキュリティに関する管理状況 （３）情報セキュリティ研修受講記録状況 （４）情報資産管理状況 （５）特定個人情報の適正な取扱い状況等 （６）基幹系システムにおけるデータの管理状況　など
7	適用基準	（１）龍ケ崎市情報セキュリティ規則 （２）龍ケ崎市情報セキュリティ対策に関する規程 （３）龍ケ崎市コンピュータ等運用管理規程 （４）龍ケ崎市電子文書取扱規程 （５）　龍ケ崎市個人情報の保護に関する法律施行条例　など

〇人的セキュリティに関して
　概ね適正に運用が行われている。今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

〇物的セキュリティに関して
　概ね適正に運用が行われている。今後も継続して適正な管理・運用を行うこと。
指摘事項：なし

私物スマートフォンの業務での使用について

1　概要

現在、全庁的な公用携帯電話が無い状態であり、外出時などにおける業務連絡については私物のスマートフォンを使用しているのが実情である。そこで、前回の令和６年度第２回情報セキュリティ委員会にて、龍ケ崎市コンピュータ等運用管理規程を改正し、業務における私物スマートフォンの使用を認める方向で調整を行う旨を報告。

その後調整を進め、今回龍ケ崎市コンピュータ等運用管理規程を改正し、私物のスマートフォンについて業務での使用を認めることとした。

2　龍ケ崎市コンピュータ等運用管理規程改正案

別添のとおり

3　その他

後日全庁へ周知予定

龍ケ崎市コンピュータ等運用管理規程の一部を改正する訓令（一部抜粋）

龍ケ崎市コンピュータ等運用管理規程（平成２０年龍ケ崎市訓令第５号）の一部を次のように改正する。

次の表の改正前の欄に掲げる規定を同表の改正後の欄に掲げる規定に下線で示すように改正する。

改正後	改正前
（私用コンピュータ等及びソフトウェアの持込禁止） 第12条　職員は、私物としてのコンピュータ等及びソフトウェアを持ち込んではならない。ただし、通話機能を利用する目的のスマートフォン及びタブレットについては、この限りでない。 ２　職員は、前項ただし書の規定により持ち込んだスマートフォン及びタブレットは、原則として、勤務時間中に私用で使用してはならない。	（私用コンピュータ等及びソフトウェアの持込禁止） 第12条　職員は、私物としてのコンピュータ等及びソフトウェアを持ち込んではならない。ただし、通話機能を利用する目的のスマートフォン及びタブレットについては、この限りでない。 ２　前項ただし書の規定により持ち込んだスマートフォン及びタブレットは、原則として、勤務時間中は使用してはならない。

令和７年2月10日情報セキュリティ委員会

個人情報安全管理措置規程の策定について

総合政策部デジタル都市推進課
データ管理活用グループ

1　策定の趣旨

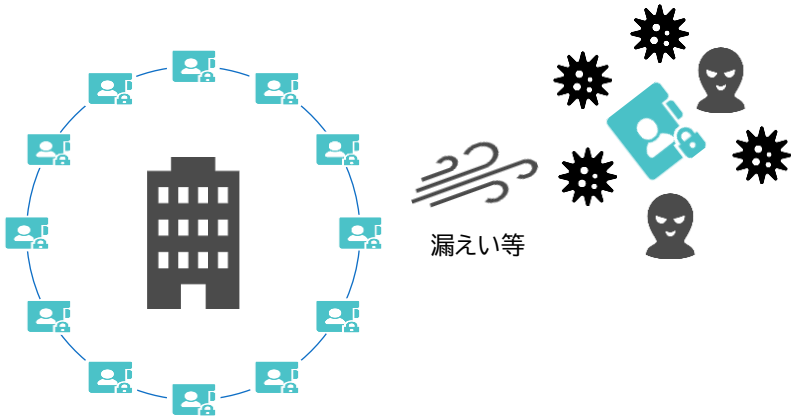
1　個人情報の保護に関する法律第66条第1項の規定

行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

行政機関等は、確実な安全管理措置を講じることが求められている。

⇒ 大量の保有個人情報を取扱う

⇒ 漏えい等が生じた場合の本人の権利利益が侵害される危険が大きい



安全管理措置

（1）安全管理のために必要かつ適切な措置

組織的安全管理措置	• 組織体制の整備 • 取扱規定等の運用 • 事案発生時の体制整備 • 見直し、改善の取組み　など
人的安全管理措置	• 取扱い担当者の監督 • 取扱い担当者への教育
物理的安全管理措置	• 個人情報を取扱う区域の管理 • 機器等の盗難等の防止 • 持ち出しによる漏えい等の防止　など
技術的安全管理措置	• アクセス制御 • アクセス者の認識・認証等 • 不正アクセス防止 • 情報漏えいの防止　など

（2）サイバーセキュリティ対策との連携

（3）委託先の監督

2　安全管理措置規程の位置づけ

【情報資産全般】

- 情報セキュリティ規則
- 情報セキュリティ対策に関する規程

最高情報セキュリティ責任者
CISO
～副市長～
規程第3条

情報セキュリティ委員会
～部等の長～
規程第4条

情報セキュリティ緊急対策会議
規程第6条

情報セキュリティ事案対応チーム
規程第6条の2

情報セキュリティ管理者
～課等の長～
規程第7条

【保有個人情報】

- 個人情報保護に関する法律施行条例
- 龍ケ崎市長が管理する個人情報の保護に関する規則

個人情報保護統括管理者
～総合政策部長～
規則第3条第1項第1号

監査責任者
～デジタル都市推進課長～
規則第3条第1項第1号

個人情報保護管理者
～課等の長～
規則第3条第1項第2号

個人情報保護担当者
～総括補佐～
規則第3条第2項

3　規程内容の構成

「行政機関等の保有する個人情報の適切な管理のための措置に関する指針」をもとに策定。

指針の規定項目	規定項目の詳細
項目	
管理体制	総括保護責任者 保護管理者 保護担当者 保有個人情報の適切な管理のための委員会
教育研修	教育研修の実施
職員の責務	職員等の責務
保有個人情報の取扱い	アクセス制限 複製等の制限 誤りの訂正等 媒体の管理等 誤送付等の防止 廃棄等 保有個人情報の取扱状況の記録 外的環境の把握
情報システムにおける安全等の確保	アクセス制御 アクセス記録 アクセス状況の監視 管理者権限の設定 外部からの不正アクセスの防止 不正プログラムによる漏えい等の防止 情報システムにおける保有個人情報の処理 暗号化 記録機能を有する機器・媒体の接続制限 端末の限定 端末の盗難防止等 第三者の閲覧防止 入力情報の照合等 バックアップ 情報システム設計書等の管理
情報システム室等の安全管理	入退管理 情報システム等の管理
保有個人情報の提供	提供する際の措置
個人情報の取扱いの委託	業務等の委託
サイバーセキュリティの確保	サイバーセキュリティに関する対策の基準等
安全管理上の問題への対応	事案の報告及び再発防止措置 法に基づく報告及び通知 公表等
監査及び点検の実施	監査 点検 評価及び見直し

4　規程内容の概要

構　成		別紙1ページ	該当条項	主な規定の概要
第1章	総則	1	第1条・第2条	総則的事項
第2章	管理体制	1-3	第3条ー第7条	• 総括責任者ー総合政策部長 • 保護管理者ー各課等の長 • 保護担当者ー総括課長補佐 • 監査責任者ーデジタル都市推進課長 • 会議体ー情報セキュリティ委員会（審議・報告）（スライド3位置づけを参照）
第3章	教育研修	3	第8条	個人情報の取扱いや情報セキュリティに関する研修を行う。 • 必要な研修を行うー対面及びeラーニングの双方を想定。毎年実施。
第4章	職員等の責務	3-4	第9条	個人情報を取扱う職員として、保護管理者等の指示に従い個人情報を取扱わなければいけない旨を規定。
第5章	保有個人情報の取扱い	4-6	第10条ー第17条	• 基本的には情報資産全般に係る情報セキュリティと同等の規定。 ➢ 個人情報へのアクセス権限や業務上取扱う個人情報の複製は必要最小限。 ➢ 保有個人情報の取扱い状況の記録 ➢ 個人情報の誤送付、誤掲載の防止、廃棄等の際の必要な措置 ➢ 外的環境の把握（従前の取扱規程等には規定なし） →従来のオンプレミス型のサーバー管理から事業者がクラウドサービスとして提供するパブリッククラウドに移行する事例も増加傾向。外国にある事業者かつ外国に設置するサービスを利用する場合など、ケースによっては、諸外国の個人情報関連法令が適用される場合があるため、状況や制度に関して正しく把握し、そのうえで安全管理措置を講じるものとしている。
第6章	情報システムにおける安全等の確保	6-9	第18条ー第32条	• 基本的には情報資産全般に係る情報セキュリティと同等の規定。主語を「各課等で個別に開発・調達した情報システム又は機器」を取扱う部署の保護管理者と定義。 ➢ 保有個人情報へのアクセス制限、記録、監視 ➢ 外部からの不正アクセスや不正プログラムによる漏えい等の防止 ➢ ファイルの暗号化や記録媒体の接続制限、機器の制限、第三者の閲覧防止　など
第7章	電算室等の安全管理	9-10	第33条・第34条	• セキュリティーポリシーを準用。（龍ケ崎市セキュリティ対策に関する規定第18条）
第8章	保有個人情報の提供及び業務の委託等	10-12	第35条・第36条	• 保有個人情報の提供や業務委託においてどのような措置を講ずるかを規定。 • 具体的には第36条の1～8号の明記などを記載。 • 契約書等に記載すべき禁止事項や遵守事項、検査事項について。
第9章	サイバーセキュリティの確保及び安全管理上の問題への対応	12-14	第36条ー第39条	• 保護管理者が遵守すべき法令等。 • 事案発生時の報告や被害拡大防止、再発防止の措置。（龍ケ崎市情報セキュリティ事故等対応手順書に基づき対応） • 個人情報保護委員会への報告や事案の公表について。 • 個人情報保護委員会への報告しなければならない事案に関しては、個人情報保護委員会規則に定められいる。
第10章	監査及び点検の実施	14	第40条ー第43条	• 保有個人情報の管理状況の監査。 • 監査、点検等の評価。

5　添付資料

別紙1　龍ケ崎市保有個人情報安全管理措置規程（案）

国の示す指針に基づき規定内容を検討。
龍ケ崎市で保有する情報資産の中で、個人情報の安全管理のために必要な措置を定める。
また、安全管理措置規程の位置づけから、龍ケ崎市セキュリティポリシーとの整合を図り策定。

龍ケ崎市保有個人情報安全管理措置規程（案）

第１章　総則（第１条・第２条）
第２章　管理体制（第３条―第７条）
第３章　教育研修（第８条）
第４章　職員等の責務（第９条）
第５章　保有個人情報の取扱い（第10条―第17条）
第６章　情報システムにおける安全等の確保（第18条―第32条）
第７章　電算室等の安全管理（第33条）
第８章　保有個人情報の提供及び業務の委託等（第34条・第35条）
第９章　サイバーセキュリティの確保及び安全管理上の問題への対応（第36条―第39条）
第１０章　監査及び点検の実施（第40条―第43条）
付則

第１章　総則

（趣旨）

第１条　この規程は、本市の保有する個人情報（以下「保有個人情報」という。）に関し、個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）第６６条第１項に規定する保有個人情報の安全管理のために必要な措置について定めることを目的とする。

（定義）

第２条　この規程における用語は、法において使用する用語の例による。

第２章　管理体制

（総括管理者）

第３条　保有個人情報の管理に関する事務を統括するため、龍ケ崎市長が管理する個人情報の保護に関する規則（令和５年規則第２３号。以下「規則」という。」）第３条第１項第１号に定める個人情報保護統括管理者（以下「統括管理者」という。）を置く。

２　統括管理者は、総合政策部長をもって充てる。
３　統括管理者は、本市における保有個人情報の管理に関する事務を総括する。
（保護管理者）
第４条　龍ケ崎市行政組織規則（平成１５年龍ケ崎市規則第３号。以下「組織規則」という。）第２条第１項に規定する課、龍ケ崎市会計管理者の補助組織設置規則（昭和６３年龍ケ崎市規則第１１号）第２条第１項に規定する会計課並びに組織規則別表第２に規定する八原保育所、西部出張所、東部出張所及び市民窓口ステーション（以下「各課等」という。）における保有個人情報の適切な管理を確保するため、規則第３条第１項第２号に定める個人情報保護管理者（以下「保護管理者」という。）を置く。
２　保護管理者には、各課等の長をもって充てる。
３　保護管理者は、各課等における保有個人情報の管理に関する事務を総括する。
４　保護管理者は、保有個人情報を情報システムで取り扱う場合は、当該情報システムの管理者と連携し、前項の事務に当たる。
（保護担当者）
第５条　各課等に規則第３条第２項に定める個人情報保護担当者（以下「保護担当者」という。）を置く。
２　保護担当者は、組織規則第４条第３号第１項に規定する総括整理することを命じられた課長補佐をもって充てる。
３　保護担当者は、保護管理者を補佐し、各課等における保有個人情報の管理に関する事務を行う。
（監査責任者）
第６条　保有個人情報の管理の状況について監査するため、規則第３条第３項第１号に定める監査責任者を置く。
２　監査責任者は、総合政策部デジタル都市推進課長をもって充てる。
（保有個人情報の適切な管理のための会議）
第７条　統括管理者は、保有個人情報の管理に係る重要事項の決定、連絡、調整等を行うため必要があると認めるときは規則第

３条第３項第２号に規定する会議において、審議又は報告をする。

２　統括管理者は、必要に応じて前項の会議に情報セキュリティ等について専門的な知識及び経験を有する者の参加を要請することができる。

第３章　教育研修

（職員等への教育研修の実施）

第８条　統括管理者は、保有個人情報の取扱いに従事する職員（地方公務員法（昭和２５年法律第２６１号）第２２条の２第１項に規定する会計年度任用職員を含む。以下「職員等」という。）に対し、保有個人情報の取扱いについて理解を深め、保有個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。

２　統括管理者は、保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に対し、保有個人情報の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

３　統括管理者は、保護管理者及び保護担当者に対し、各課等における保有個人情報の適切な管理のための教育研修を定期的に行う。

４　保護管理者は、職員等に対し、保有個人情報の適切な管理のため、統括管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずるものとする。

第４章　職員等の責務

（職員等の責務）

第９条　職員等は、法の趣旨にのっとり、関連する法令及び規程等の定め並びに統括管理者、保護管理者及び保護担当者（以下「統括管理者等」という。）の指示に従い、保有個人情報を取り扱わなければならない。

第５章　保有個人情報の取扱い

（アクセス制限）

第１０条　保護管理者は、保有個人情報の秘匿性等その内容（個

人識別の容易性（匿名化の程度等）、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを考慮する。以下同じ。）に応じて、当該保有個人情報にアクセス（紙に記録されている保有個人情報を取扱う行為を含む。以下同じ。）する権限を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限るものとする。

２　前項のアクセス権限を有しない職員等は、保有個人情報にアクセスしてはならない。

３　職員等は、第１項に規定するアクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスしてはならず、アクセスは必要最小限としなければならない。

（複製等の制限）

第１１条　保護管理者は、職員等が業務上の目的で保有個人情報を取り扱う場合であっても、次に掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、職員等は、保護管理者の指示に従うものとする。

（１）　保有個人情報の複製

（２）　保有個人情報の送信

（３）　保有個人情報が記録されている媒体の外部への送付又は持出し

（４）　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

（誤りの訂正等）

第１２条　職員等は、保有個人情報の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正、追加又は削除を行う。

（媒体の管理等）

第１３条　職員等は、保護管理者の指示に従い、保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、当該媒体の金庫への保管、保管場所の施錠等の保有個人情報の漏えい等を防止するための措置を

講ずるものとする。

２　職員等は、保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、保護管理者の指示に従い、原則として、パスワード、ＩＣカード、生体情報等（以下「パスワード等」という。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずるものとする。

（誤送付等の防止）

第１４条　職員等は、保有個人情報を含む電磁的記録又は媒体の誤送付、誤交付、誤送信又は市公式ホームページ等のウェブサイト及びSNS（ソーシャルネットワーキングサービス）等への誤掲載を防止するため、個別の事務又は事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員等による確認やチェックリストの活用等必要な措置を講ずるものとする。

（廃棄等）

第１５条　職員等は、保有個人情報又は保有個人情報が記録されている媒体（端末機器及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行うものとする。

２　保有個人情報の消去又は保有個人情報が記録されている媒体の廃棄を委託する場合（委託先が再委託する場合以降同じ。）には、必要に応じて職員等が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取るなど、委託先において消去及び廃棄が確実に行われていることを確認するものとする。

（保有個人情報の取扱状況の記録）

第１６条　保護管理者は、当該保有個人情報の保管等の取扱いの状況を把握するため、法第７５条第１項及び規則第４条第１項から第３項までに定める個人情報ファイル簿を整備して記録するものとする。

（外的環境の把握）

第１７条　保有個人情報が、外国において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

２　前項に規定する措置は、民間事業者が提供するクラウドサービスを利用する場合においてはクラウドサービス提供事業者が外国に所在する場合及び個人データが保存されるサーバが外国に所在する場合にも同様とする。

第６章　情報システムにおける安全の確保等

（アクセス制御）

第１８条　情報システム（龍ケ崎市情報セキュリティ規則（平成15年龍ケ崎市規則第24号）第２条第３号に規定する情報システムをいう。）及び情報システム機器（龍ケ崎市情報セキュリティ対策に関する規程（平成27年龍ケ崎市訓令第14号）第２条第６号に規定する情報システム機器をいう。以下「セキュリティ規程」という。）等（各課等で個別に開発又は調達したもの。）を取り扱う部署の保護管理者（以下「システム保護管理者」という。）は、保有個人情報（情報システムで取り扱うものに限る。以下第３５条を除き、この章及び次章において同じ。）の秘匿性等その内容に応じて、認証機能を設定し、当該保有個人情報へのアクセスを制御するために必要な措置を講ずるものとする。

２　システム保護管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備するとともに、パスワード等の読取防止を行うために必要な措置を講ずるものとする。

（アクセス記録）

第１９条　システム保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期的に分析するために必要な措置を講ずるものとする。

２　システム保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずるものとする。

（アクセス状況の監視）

第２０条　システム保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、アクセス記録又は操作記録等の定期的な点検又は分析する等、必要な措置を講ずるものとする。

（管理者権限の設定）

第２１条　システム保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずる。

（外部からの不正アクセスの防止）

第２２条　システム保護管理者は、アクセス権限を有しない者が外部から保有個人情報を取り扱う情報システムの内部へ侵入を行う行為（以下「不正アクセス」という。）を防止するため、ファイアウォール等の外部の通信回線（以下「ネットワーク」という。）からの不正アクセスを制御する仕組みの設定による経路制御等の必要な措置を講ずるものとする。

（不正プログラムによる漏えい等の防止 ）

第２３条　システム保護管理者は、情報システムに害悪な動作をさせるデータ（以下「不正プログラム」という。）による保有個人情報の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずるものとする。

（情報システムにおける保有個人情報の処理）

第２４条　職員等は、保有個人情報について、一時的に加工等の処理を行うため複製を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去するものとする。

２　前項の場合において、保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、利用状況等を確認するものとする。

（暗号化等）

第２５条　システム保護管理者は、保有個人情報の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずるものとする。

２　職員等は、前項の措置を踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化又はパスワードの付与を行うものとする。

（記録機能を有する外部電磁的記録媒体の接続制限）

第２６条　システム保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい等の防止のため、スマートフォン、USB メモリ等の記録機能を有する外部の電磁的記録媒体の情報システム端末への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずるものとする。

（端末機器の限定）

第２７条　システム保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の処理を行う端末機器を限定するために必要な措置を講ずるものとする。

（端末機器の盗難防止等 ）

第２８条　システム保護管理者は、端末機器の盗難又は紛失の防止のため、端末機器の固定、保管庫又は執務室の施錠等の必要な措置を講ずるものとする。

２　職員等は、システム保護管理者が必要と認めるときを除き、端末機器を外部へ持ち出し、又は外部から持ち込んではならない。

（第三者の閲覧防止）

第２９条　職員等は、端末機器の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフ（情報システムの利用を終了すること

をいう。）を行うことを徹底する等の必要な措置を講ずるものとする。

（入力情報の照合等）

第３０条　職員等は、情報システムで取り扱う保有個人情報の重要度に応じて、当該情報システムに入力する元となる申請書等と当該情報システムに入力する内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行うものとする。

（バックアップ）

第３１条　システム保護管理者は、保有個人情報の秘匿性等その内容に応じて、他の電磁的記録媒体にバックアップを作成し、分散保管するために必要な措置を講ずるものとする。

（情報システム設計書等の管理）

第３２条　システム保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について関係課以外に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずるものとする。

第７章　電算室等の安全管理

（入退管理）

第３３条　保有個人情報を取り扱う基幹的なサーバ等の機器を設置する電算室等の安全管理は、セキュリティ規程第１８条を準用する。

第８章　保有個人情報の提供及び業務の委託等

（保有個人情報の提供）

第３４条　保護管理者は、法第６９条第２項第３号及び第４号の規定により、行政機関等以外の者に保有個人情報を提供する場合には、法第７０条の規定に基づき、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面（電磁的記録を含む。）を取り交わすものとする。

２　保護管理者は、法第６９条第２項第３号及び第４号の規定に

より、行政機関等以外のものに保有個人情報を提供する場合には、法第７０条の規定により、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。

３　保護管理者は、法第６９条第２項第３号の規定により、他の行政機関等に保有個人情報を提供する場合において、必要があると認めるときは、法第７０条の規定により、前２項に規定する措置を講ずるものとする。

（業務の委託等）

第３５条　個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しないものを選定することがないよう、必要な措置を講ずるものとする。この場合において、契約書等に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認するものとする。

（１）　個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務

（２）　再委託（再委託先が委託先の子会社（会社法（平成１７年法律第８６号）第２条第３号に規定する子会社をいう。）である場合も含む。以下本項及び第４項において同じ。）の制限又は事前承認等再委託に係る条件に関する事項。

（３）　個人情報の複製等の制限に関する事項

（４）　個人情報の安全管理措置に関する事項

（５）　個人情報の漏えい等の事案の発生時における対応に関する事項

（６）　委託終了時における個人情報の消去及び媒体の返却に関する事項

（７）　法令等及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項

（８）　契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項

２　保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。

３　保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、委託先における責任者及び業務従事者の作業の管理体制及び実施体制や個人情報の管理の状況について、実地検査又は書面による報告により確認することができる。

４　委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に第１項に規定する措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項に規定する措置を講ずるものとする。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

５　保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記するものとする。

６　保有個人情報を提供し、又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずるものとする。

第９章　サイバーセキュリティの確保及び安全管理上の問題への対応

（サイバーセキュリティに関する対策の基準等）

第３６条　保護管理者は、個人情報を取り扱い、又は情報システムを構築し、若しくは利用するにあたっては、職務の遂行にお

いて使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、取り扱う保有個人情報の性質等に照らして適正なサイバーセキュリティの水準を確保（情報の機密性、完全性及び可用性を確保することをいう。）するものとする。

（１）地方公務員法（昭和２５年法律第２６１号）

（２）著作権法（昭和４５年法律第４号）

（３）不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）

（４）個人情報の保護に関する法律（平成１５年法律第５７号）

（５）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（平成２５年法律第２７号）

（６）サイバーセキュリティ基本法（平成２６年法律第１０４号）

（事案の報告及び再発防止措置）

第３７条　保有個人情報の漏えい等安全管理の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員等は、直ちに「龍ケ崎市情報セキュリティ事故等対応手順書」に基づき対応を行うものとする。

（法に基づく報告及び通知）

第３８条　個人情報の漏えい等が生じた場合であって法第６８条第１項の規定による個人情報保護委員会への報告及び同条第２項の規定による本人への通知を要する場合には、前条で定める事項と並行して、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力する。

（公表等）

第３９条　保護管理者は、法第６８条第１項の規定による報告及び同条第２項の規定による本人への通知を要しない場合であっても、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応等の措置を講ずるものとする。

２　公表を行う漏えい等が発生したとき、個人情報保護に関連す

る法令、関係例規等に対する違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があつたとき等、市民の不安を招きかねない事案が発生し、公表を行う場合には、当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会事務局に情報提供を行うものとする。

第１０章　監査及び点検の実施

（監査）

第４０条　監査責任者は、保有個人情報の適切な管理を検証するため、第２章から前章までに規定する措置の状況を含む各課等における保有個人情報の管理の状況について、定期及び必要に応じ随時に監査を行い、その結果を統括管理者に報告するものとする。

（点検）

第４１条　保護管理者は、各課等における保有個人情報の記録媒体、処理経路、保管方法等について、定期及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を統括管理者に報告するものとする。

（評価及び見直し）

第４２条　統括管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

（委任）

第４３条　この規程に定めるもののほか、必要な事項は、市長が別に定める。