○朝来市情報セキュリティ基本規程

平成30年３月30日

訓令第８号

朝来市情報セキュリティ基本規程（平成17年朝来市訓令第11号）の全部を改正する。

（目的）

第１条　この訓令は、市が保有する情報資産の機密性、完全性及び可用性を維持するため、市が実施する情報セキュリティを維持するための対策（以下「情報セキュリティ対策」という。）について基本的な方針を定めることを目的とする。

（定義）

第２条　この訓令において、次に掲げる用語の意義は、当該各号に定めるところによる。

(1) 情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

(2) 機密性　情報資産にアクセスを認可された者だけが情報資産にアクセスできることを確実にすることをいう。

(3) 完全性　情報資産及び処理方法が、正確であること及び完全であることを保護することをいう。

(4) 可用性　情報資産にアクセスを認可された利用者が、必要なときに、情報資産及び関連する資産にアクセスできることを確実にすることをいう。

(5) ネットワーク　通信を行うために用いられる機器及び回線をいう。

(6) 電磁的記録媒体　磁気的方式、電子的方式その他人の知覚によっては認識できない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものに係る記録媒体をいう。

(7) 情報システム　ハードウェア、ソフトウェア、ネットワーク、電磁的記録媒体等で構成されるものであって、これら全体で業務処理を行うもの（これらの仕組みを開発、運用及び保守するために作成された資料等を含む。）をいう。

(8) 情報資産　情報システム（教育委員会において児童生徒が教育のために用いるものを除く。）及び情報システムで取り扱う情報（印刷した文書を含む。）をいう。

(9) 職員等　一般職の職員、特別職の職員、国又は他の地方公共団体から派遣されている職員及び市の情報システムの開発、運用、保守等の業務委託契約を市と締結した者をいう。

(10) 情報セキュリティに関する事案　不正アクセス、コンピュータウイルスの感染等、情報セキュリティに関する事故及び事件をいう。

(11) 情報セキュリティポリシー　市が保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであって、この訓令及び朝来市情報セキュリティ対策基準（以下「対策基準」という。）をいう。

（適用範囲）

第３条　この訓令は、市の全ての情報資産及び職員等に適用する。

（情報資産への脅威）

第４条　市が認識するべき情報資産に対する脅威は、次に掲げるとおりとする。

(1) 物理的及び論理的侵入、窃盗、妨害、破壊、盗聴、なりすまし、改ざん、紛失、著作権の侵害、業務目的外使用、操作ミス、設計ミス、実装ミス、規定外の端末接続によるデータ漏えい、情報セキュリティポリシー違反等

(2) コンピュータウイルス等の悪意のあるプログラム

(3) 地震、雷、火災、風害、水害、感染症の集団発生等の災害

(4) 停電、回線断、故障、異常動作、容量超過等

（職員等の責務）

第５条　職員等は、この訓令、対策基準及び朝来市情報セキュリティ実施手順（以下「実施手順」という。）等を理解し、遵守することにより、情報資産を適切に保護しなければならない。

２　職員等は、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、次に掲げる法令のほか関係法令等を遵守し、これに従わなければならない。

(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48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) 朝来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に関する条例（平成27年朝来市条例第35号）

（情報セキュリティ対策）

第６条　市は、第４条各号に掲げる脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講じるものとする。

(1) 情報セキュリティ対策を推進する全庁的な組織体制の確立

(2) 機密性、完全性及び可用性に応じた情報資産の分類と管理

(3) 情報システム設置場所等への不正な立入り、サーバ等、通信回線等及び情報機器等の損傷、盗難及び破壊を防止するための物理的セキュリティ対策

(4) 情報セキュリティ確保のための職員等の役割、責任及び遵守事項の明確化並びに教育等の人的セキュリティ対策

(5) コンピュータ等管理、アクセス制御、不正プログラム対策、不正アクセス対策、データ改ざん対策等の技術的セキュリティ対策

(6) 情報システムの監視、情報セキュリティポリシーの遵守状況確認等の運用管理及び緊急時対応計画の策定等情報セキュリティに関する運用対策

（電磁的記録媒体の取扱い及び管理）

第７条　市は、情報システムに用いる電磁的記録媒体について、廃棄等を含めた適切な取扱い及び管理のための必要な対策を講ずるものとする。

（情報セキュリティに関する事案への対応）

第８条　市は、情報セキュリティに関する事案の発生に備え、あらかじめ事案発生時の対応を定め、当該事案発生時の際はその影響を最小限にとどめるための対応を迅速かつ円滑に実施するとともに、再発防止のための必要な対策を講じなければならない。

（対策基準の制定）

第９条　市は、この訓令に基づき、情報セキュリティ対策を実施するために必要となる対策基準を定めるものとする。

（実施手順の制定）

第10条　市は、対策基準に基づく情報セキュリティ対策を実施するため、情報システム又は業務ごとに情報セキュリティ対策の具体的な手順等を明記した実施手順を定めるものとする。

（違反に対する措置）

第11条　職員等は、この訓令、対策基準及び実施手順に違反した場合は、直ちに任命権者に報告しなければならない。

２　当該違反した職員等（次項に規定するものを除く。）については、地方公務員法に基づく懲戒処分その他必要な措置を行うことができるものとする。

３　職員等のうち市の情報システムの開発、運用、保守等の業務委託契約を市と契約した者が違反したときは、当該違反の重大性、発生した事案の状況等に応じ、損害賠償請求等必要な措置を行うことができるものとする。

（点検、評価及び見直し）

第12条　市は、新たな脅威及び情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティ監査の実施等により、定期的にこの訓令、対策基準及び実施手順の点検及び評価を行い、その見直しを実施する。

（委任）

第13条　この訓令に定めるもののほか、情報セキュリティ対策に関し必要な事項は、別に定める。

附　則

この訓令は、平成30年４月１日から施行する。

附　則（令和５年訓令第４号）

この告示は、令和５年４月１日から施行する。