郡山市情報セキュリティ要綱

（趣旨）

第１条　この要綱は、本市が所管する情報資産の機密性、完全性及び可用性を確保するため、様々な脅威を抑止し、予防し、及び検知し、並びに情報資産の機密性、完全性及び可用性を回復することについて、組織的、かつ、計画的に情報セキュリティ対策を実施するために基本的な考え方その他必要な事項を定めるものとする。

（適用範囲）

第２条　この要綱は、本市が所管する情報資産の生成、運用、管理及び利用に携わる者（以下「職員等」という。）に適用する。

（定義）

第３条　この要綱において、次の各号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確保し、維持すること。

(2) 情報資産　次に掲げるものをいう。

ア　ネットワーク、情報システム、これらに関する設備及び電磁的記録媒体

イ　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。）

ウ　情報システムの仕様書、ネットワーク図等のシステム関連文書

(3) 情報資産の機密性　情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできることを確保すること。

(4) 情報資産の完全性　情報資産及びその処理方法が正確であること並びに情報資産が破壊、改ざん又は消去されていない状態を確保すること。

(5) 情報資産の可用性　情報資産にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保すること。

(6) 情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(7) ネットワーク　コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

(8) 電磁的記録媒体　磁気ディスク、磁気テープ、フロッピーディスク、磁気カード、光ディスク、フラッシュメモリ、外付けハードディスクその他の磁性体又は光磁性体により電磁的記録を記録できる媒体をいう。

(9) 情報セキュリティポリシー　この要綱及び第10条に規定する対策基準をいう。

(10) 外部組織　郡山市個人情報の保護に関する法律施行条例（令和４年郡山市条例第31号）第２条に規定する市の機関等以外の法人その他の団体をいう。

（職員等の責務）

第４条　職員等は、情報セキュリティの重要性について共通の認識を持つとともに、情報セキュリティに関係する法令及び情報セキュリティポリシーその他の規程を遵守しなければならない。

（組織体制）

第５条　市長は、統一的な情報セキュリティ対策を実施するため、情報セキュリティを主導する組織を設置して、情報セキュリティ確保のための体制を整備するとともに、それぞれの役割及び責任を定めなければならない。

（情報資産の管理）

第６条　情報資産は、その機密性、完全性及び可用性を踏まえ、その重要性に応じ、適切に管理しなければならない。

（対象とする脅威）

第６条の２　市長は、情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん又は消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計若しくは開発の不備、プログラム上の欠陥、操作若しくは設定ミス、メンテナンス不備、内部又は外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい、破壊、消去等

(3) 地震、落雷、火災等の災害によるサービス又は業務の停止等

(4) 大規模かつ広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（情報セキュリティ対策）

第７条　市長は、前条各号に掲げる脅威から情報資産を保護するために、次に掲げる対策を講ずるものとする。

(1) 物理的セキュリティ対策　情報システムの基幹機器の設置及び当該機器等の管理、運用を行う部屋への不正な立ち入り、情報資産への損傷及び妨害から情報資産を保護するための物理的な対策

(2) 人的セキュリティ対策　情報セキュリティに関する事項を定め、職員等にその内容を周知徹底することその他職員等に十分な教育及び啓発を行うための対策

(3) 技術的セキュリティ対策　コンピュータ等の管理、ネットワークの管理、アクセス制御、不正プログラム対策、不正アクセス対策等の情報資産を適切に保護するための技術面の対策

(4) 運用におけるセキュリティ対策　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の確認、外部委託を行う際のセキュリティ確保等の情報セキュリティポリシーの運用面の対策

２　前項各号に掲げるもののほか、市長は、情報資産に対するセキュリティ侵害の発生等緊急事態が発生した場合に、迅速かつ適切な対応を可能とするための危機管理対策を整備しなければならない。

（業務継続）

第８条　市長は、重大な障害又は災害が発生した場合に、業務の中断に対処するとともに、その影響から重要な業務手続を保護する対策を整備しなければならない。

（外部組織との結合）

第９条　外部組織の情報システムとの通信回線等による結合については、次条に規定する統一的な基準において、結合に際しての許可及び協定並びに外部組織の責めにより生じた損害の賠償、情報資産に対する脅威のおそれが生じた場合の対応その他の措置を定めなければならない。

（対策基準の策定）

第10条　市長は、情報セキュリティを実施するに当たって遵守すべき事項及び判断等の統一的な基準（以下「対策基準」という。）を定めるものとする。

（実施手順の策定）

第11条　情報システムを所管する課等は、当該情報システムの情報セキュリティを具体的に実施するために、情報システムごとに情報セキュリティの実施のための手順（以下「実施手順」という。）を定めなければならない。

２　実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

（情報セキュリティ監査の実施）

第12条　市長は、情報セキュリティポリシー及び実施手順が遵守されていることを検証するため、定期的に監査（次条において「情報セキュリティ監査」という。）を実施しなければならない。

（評価及び見直しの実施）

第13条　市長は、情報セキュリティ監査の結果等により、情報セキュリティの評価を行う。

２　情報セキュリティポリシー及び実施手順は、随時見直しを図るものとする。

（違反に対する措置）

第14条　法令又は情報セキュリティポリシーその他の規程に違反した職員（会計年度任用職員を含む。）については、当該違反の状況等及びその重大性に応じて、地方公務員法（昭和25年法律第 261 号）第29条及び郡山市職員の懲戒の手続及び効果に関する条例（昭和40年郡山市条例第17号）による懲戒処分の対象とする。

２　本市の業務を委託された者が、法令又は情報セキュリティポリシーその他の規程に違反した場合の措置は、当該業務の委託契約において定めるものとする。

附　則

この要綱は、平成15年４月１日から施行する。

附　則

この要綱は、平成18年３月１日から施行する。

附　則

この要綱は、平成27年10月１日から施行する。

附　則

この要綱は、令和５年４月１日から施行する。