曽於市情報セキュリティに関する規則を改正し、地方自治法第244条の６第１項の地方公共団体におけるサイバーセキュリティを確保するための方針に位置付け、ここに公表する。

令和８年４月１日

曽於市長　竹田　正博
曽於市議会議長　重久　昌樹
曽於市教育委員会　教育長　中村　涼一
曽於市農業委員会会長　山口　裕之
曽於市選挙管理委員会委員長　澤　律雄
曽於市監査委員事務局代表監査委員 野村 行雄
曽於市固定資産評価審査委員会委員長　吉川　俊一

○曽於市情報セキュリティに関する規則

（趣旨）

第１条　この規則は、本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、本市が実施する情報セキュリティ対策に関し基本的な事項を定めるものとする。

（定義）

第２条　この規則において、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。

⑴ 実施機関　市長（公営企業管理者の権限を行う市長を含む。）、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会をいう。

⑵ 情報システム　コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

⑶ 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。

⑷ 情報資産

ア　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

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及びネットワーク図等のシステム関連文書

⑸ 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。

⑹ 情報セキュリティポリシー　本規則及び情報セキュリティ対策基準をいう。

⑺ 機密性　情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

⑻ 完全性　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

⑼ 可用性　情報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をいう。

⑽ マイナンバー利用事務系　個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

⑾ LGWAN接続系　総合行政ネットワーク（以下「LGWAN」という。）に接続された情報システム及びその情報システムで取り扱うデータ（マイナンバー利用事務系を除く。）をいう。

⑿ インターネット接続系　インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

⒀ 通信経路の分割　LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

⒁ 無害化通信　インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

⒂ 個人情報　個人情報の保護に関する法律（平成15年法律第57号）第２条第１項に規定する個人情報をいう。

⒃ 重要情報　市の行政運営上必要な情報で、その機密性、完全性、可用性が損なわれた場合、市に著しい損害を与える恐れがあるものをいう。

⒄ 職員等　市の実施機関に所属する常勤の職員、嘱託及び地方公務員法（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並びに特別職をいう。

（適用範囲）

第３条　この規則は、職員等及び実施機関の保有する情報資産について適用するものとする。

（職員等の責務）

第４条　職員等は、関係法令及び情報セキュリティポリシーを遵守し、情報システムの管理運営を適正に行わなければならない。

２　職員等は、その職務上知り得た個人情報及び重要情報並びに情報セキュリティ対策上の機密情報の秘密を漏らしてはならない。その職を退いた後も同様とする。

（対象とする脅威）

第５条　情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

⑴ 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃その他意図的な要因による情報資産の漏えい、破壊、改ざん及び消去、重要情報の詐取、内部不正等

⑵ 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、プログラム上の

欠陥、操作ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、故障その他非意図的要因による情報資産の漏えい、破壊及び消去等

⑶ 地震、落雷、火災その他災害によるサービス及び業務の停止等

⑷ 大規模・広範囲にわたる疾病による要員不足によるシステム運用の機能不全等

⑸ 電力の供給の途絶、水道の供給の途絶、通信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６条　前条各号に規定する脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

⑴ 本市の情報資産について、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

⑵ 本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づく情報セキュリティ対策

⑶ マイナンバー利用事務系について、他の領域との通信を遮断した上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入

⑷ LGWAN接続系について、LGWANと接続する業務用システムとインターネット接続系の情報システムとの通信経路の分割を行い、両システム間で通信する場合は、無害化通信を実施

⑸ サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理についての物理的な対策

⑹ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策

⑺ 技術的セキュリティに関し、コンピュータ等の管理、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技術的な対策

⑻ 情報の処理又は情報システムの運用管理を外部に委託契約する際に必要な対策及び措置

⑼ 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、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策

⑽ 情報システムに緊急事態が発生した際の迅速な対応を可能とするための緊急時対応計画の策定

⑾ 外部サービス（クラウドサービス）の利用に係る規定の整備

⑿ ソーシャルメディアサービスの利用に係る規定の整備

（情報セキュリティ対策基準及び実施手順の策定）

第７条　前条に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定する。

２　前項の対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。なお、対策基準及び実施手順は、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及び自己点検の実施）

第８条　情報セキュリティポリシーの運用状況を把握し、適正な運用のために必要な改善を施すため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

（管理運営方法等の評価及び見直し）

第９条　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため、新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

（委任）

第10条　この規則に定めるもののほか、この規則の施行に関し必要な事項は、市長が別に定める。