○筑西市情報セキュリティ規則

平成18年３月28日市規則第33号

改正

平成28年３月31日規則第23号

令和６年１月26日市規則第２号

筑西市情報セキュリティ規則

（目的）

第１条　この規則は、本市が取り扱う住民の個人情報及び行政運営上重要な情報資産を破壊、改ざん、消去、持出し等の脅威から保護し、住民の財産、個人のプライバシーを守り、安全かつ安定的な行政サービスを提供することを目的とする。

（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。

（１）　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。

（２）　ネットワーク　コンピュータを相互に接続するための通信回線網（通信回線網に接続する通信機器を含む。）をいう。

（３）　電磁的記録媒体　電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られた情報を記録するためのものをいう。

（４）　情報システム　情報処理を行う仕組みであって、コンピュータ（ハードウェア及びソフトウェアを含む。）、ネットワーク、電磁的記録媒体等により構成されるものをいう。

（５）　情報資産　情報システム及び情報システムで取り扱う全ての情報をいう。

（６）　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。

（７）　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。

（８）　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。

（９）　情報セキュリティ対策　情報資産の機密性、完全性及び可用性を維持するために必要な措置をいう。

(10)　情報セキュリティ対策基準　情報セキュリティ対策に係る具体的な順守事項、判断基準等を定めたもの（以下「対策基準」という。）をいう。

(11)　情報セキュリティポリシー　この規則及びこの規則に基づく対策基準をいう。

(12)　実施機関　市長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会及び固定資産評価審査委員会並びに議会をいう。

(13)　受託事業者　市長から情報資産の取扱いを委託された者をいう。

(14)　不正アクセス　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）第２条第４項に規定する不正アクセス行為をいう。

(15)　コンピュータウイルス　情報システムの正常な動作を妨害する目的で作成されたプログラムをいう。

(16)　マイナンバー利用事務系　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）第２条第５項に規定する個人番号を利用する事務又は戸籍事務等に係る情報システム又は当該システムで取り扱うデータをいう。

(17)　ＬGWAN接続系　ＬGWAN（地方公共団体の組織内ネットワークを相互に接続し、情報の高度利用を行うためのネットワークをいう。）に接続された情報システム及び当該システムで取り扱うデータ（前号のマイナンバー利用事務系に該当するものを除く。）をいう。

(18)　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当該システムで取り扱うデータをいう。

（適用範囲）

第３条　情報セキュリティポリシーは、実施機関が保有する情報資産並びに情報資産を取り扱う職員（臨時職員及び非常勤職員を含む。以下「職員等」という。）及び受託事業者に適用する。

（職員等及び受託事業者の責務）

第４条　職員等及び受託事業者は、情報セキュリティポリシーを順守し、情報資産を適切に取り扱わなければならない。

（情報セキュリティ管理体制）

第５条　市長は、情報セキュリティ対策を推進するため、その権限及び責任を明確にした管理体制を確立するものとする。

（情報資産の分類）

第６条　市長は、情報資産をその内容により分類し、その重要度に応じた情報セキュリティ対策を講じなければならない。

（情報資産への脅威）

第７条　情報セキュリティ対策の実施において特に認識すべき情報資産への脅威は、次に掲げる行

為等とする。

（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、消去、重要情報の詐取、内部不正等

（２） 情報資産の無断持出し、無許可ソフトウェアの使用等の規定違反、設計及び開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、内部又は外部の監査機能の不備、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

（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

（５） 電力供給、通信、水道供給の途絶等のインフラの障害からの波及

（情報セキュリティ対策）

第８条 市長は、前条の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なければならない。

（１） 職員等に対する効果的な教育、訓練の実施その他の人的セキュリティ対策

（２） 情報資産を有する区画への不正な立入りによる破壊、持出し等の行為から情報資産を保護するための入退室管理、地震、落雷、火災その他の災害による事故又は情報システムの故障から情報資産を保護するために必要な施設管理その他の物理的セキュリティ対策

（３） 外部からの不正アクセス、コンピュータウイルス等から情報資産を保護するためのネットワーク管理、アクセス制御その他の必要な技術的セキュリティ対策

（４） マイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系の区分に応じた対策

（５） 外部委託及び外部サービスの利用における対策

（６） 情報セキュリティポリシー順守状況の確認その他の運用における対策

（対策基準の策定）

第９条 対策基準は、市長が別に定める。

（実施手順の作成）

第10条 対策基準に基づき、情報セキュリティ対策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。）は、市長が別に定める。

２ 実施手順は、これを公開しない。

（監査等）

第11条　市長は、情報セキュリティポリシーが順守されていることを検証するため、定期的又は必要に応じて情報セキュリティ監査又は自己点検を実施する。

（評価及び見直し）

第12条　市長は、情報セキュリティポリシーに規定する事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取巻く状況の変化に対応するため、必要に応じて情報セキュリティポリシーの見直しを実施するものとする。

（補則）

第13条　この規則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、市長が別に定める。

附　則

この規則は、公布の日から施行する。

附　則（平成28年市規則第23号）

この規則は、平成28年４月１日から施行する。

附　則（令和６年１月26日市規則第２号）

この規則は、公布の日から施行する。