○多治見市情報セキュリティ基本規程

平成15年７月31日訓令甲第15号

第１章　総則

（目的）

第１条　この規程は、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ついて基本的な事項を定めることを目的とする。

（情報セキュリティポリシー）

第２条　本市の情報セキュリティ対策は、情報セキュリティポリシーに基づき実施する。

２　この規程を、本市の情報セキュリティ対策の基本方針とする。

３　この規程に基づき、本市の情報セキュリティ対策の基準として、別表に掲げる規程（この規程を除く。）を定めるものとする。

４　情報セキュリティポリシーに基づく情報セキュリティ対策を実施するため、各情報資産に係る情報セキュリティ対策実施手順等を別に定める。

（用語の定義）

第３条　情報セキュリティポリシーにおいて、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）　情報セキュリティポリシー　別表に掲げる各種規程をいう。

（２）　情報セキュリティ　機密性、完全性及び可用性を維持することをいう。

（３）　職員　地方公務員法（昭和25年法律第261号）第３条第２項に規定する一般職に属する本市の職員並びに同条第３項第３号及び第３号の２に掲げる特別職に属する本市の職員をいう。

（４）　外部要員　本市の情報資産を取り扱うことを認められた者であって､次に掲げるものをいう。

ア　人材派遣契約により本市に派遣された者

イ　委託契約又は請負契約に基づき、本市の情報資産を取り扱う者

ウ　その他本市の情報資産の取扱いを許可された者

（５）　推進会議　多治見市情報化推進会議設置規程（平成15年訓令甲第12号）第１条に規定する多治見市情報化推進会議をいう。

（６）　最高情報統括責任者　多治見市最高情報統括責任者等設置規程（平成15年訓令甲第16号。以下「最高情報統括責任者等設置規程」という。）第３条に規定する最高情報統括責任者をいう。

（７）　情報セキュリティ責任者　最高情報統括責任者等設置規程第４条に規定する情報セキュリティ責任者をいう。

（８）　情報化推進チーフ　最高情報統括責任者等設置規程第５条に規定する情報化推進チーフをいう。

（９）　情報資産　次に掲げるものをいう。また、本市以外の企業、団体又は個人から取得、借用又は預かり受けている情報資産を含む。

ア　情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　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関連文書

(10)　情報システム　情報機器、ソフトウェア、ネットワーク構成機器及び記憶媒体で構成されるものであって、これら全体で処理を行うものをいう。

(11)　ハードウェア　サーバ、端末その他のコンピュータをいう。

(12)　ソフトウェア　ハードウェア上で稼動するオペレーティングシステム、ミドルウェア、アプリケーション等をいう。

(13)　情報機器　次に掲げるものをいう。

ア　ハードウェア

イ　ＵＳＢメモリーその他の外部記憶媒体

ウ　スキャナ、プリンター、複写機その他の周辺機器

エ　携帯情報端末、携帯電話その他これらに類する物

(14)　ネットワーク構成機器　ネットワークケーブル及びルータ、ハブ等をいう。

(15)　脅威　次に掲げるものを想定し、情報セキュリティ対策を講ずるものをいう。

ア　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や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、重要情報の搾取、内部不正等

イ　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・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・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

ウ　地震、落雷、火災等の災害によるサービス及び業務の停止等

エ　大規模・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

オ　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

(16)　安全性　機密性、完全性及び可用性の総称をいう。

(17)　機密性　情報にアクセスすることを許可された者のみが情報の閲覧、利用等ができることをいう。

(18)　完全性　情報及びその処理方法が、正確及び完全であることをいう。

(19)　可用性　許可された者が、必要なときに常に情報資産を使用できることをいう。

(20)　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。

(21)　特定個人情報　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９項に規定する特定個人情報をいう。

(22)　マイナンバー利用事務系（個人番号利用事務系）　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。

(23)　LGWAN 接続系　LGWAN 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（マイナンバー利用事務系を除く。）。

(24)　インターネット接続系　インターネットメール、ホームページ管理システム等に関わる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。

（適用範囲）

第４条　情報セキュリティポリシーの適用範囲は、次の各号に定めるところによる。

（１）　情報資産の範囲　市が管理するすべての情報資産、建物及び関連設備とする。

（２）　対象者の範囲　前号に定める情報資産に接する職員及び外部要員とする。

第２章　基本原則

（安全性と利便性を両立した情報セキュリティ対策）

第５条　情報セキュリティ対策の実施に当たっては、安全性の確保と併せ、職員及び外部要員の利便性についても確保するものとする。

２　重要な情報資産については、利便性の確保よりも安全性の確保を優先しなければならない。

（体系的な情報セキュリティ対策）

第６条　情報セキュリティ対策の実施に当たっては、次に揚げる対策に応じ、事前の防止、発生時の検知及び復旧のために必要な措置を講じなければならない。

（１）　物理的セキュリティ　サーバ、情報システム室、通信回線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

（２）　人的セキュリティ　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

（３）　技術的セキュリティ　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対策

（継続的な情報セキュリティ対策）

第７条　情報セキュリティ対策は、定期的又は随時に評価し、継続的に実施する。

（効率的な情報セキュリティ対策）

第８条　情報セキュリティ対策の実施に当たっては、費用対効果を勘案するものとする。

第３章　体制

（体制）

第９条　本市における情報セキュリティ対策を運営するための全庁的な体制は、推進会議を中心に組織する。

第４章　情報セキュリティ対策の基本方針

（職員の責務）
第10条　職員は、情報セキュリティポリシーに基づき、かつ、これを遵守し、情報セキュリティ対策を行わなければならない。
（情報の安全管理）
第11条　情報については、次に掲げる措置を講ずるものとする。
（１）　機密性の区分を定め、その区分に応じて機密性を確保する。
（２）　情報の内容、影響等を勘案して、完全性を確保する。
（３）　情報を利用する者の要求に照らし、必要な可用性のレベルを確保する。
２　個人情報については、前項に加えて個人情報から特定される情報主体の利益を保護するための措置を講ずるものとする。
（情報機器の適正な管理）
第12条　情報機器については、その導入、設置、運用管理等において適正な管理を行う。
（建物設備の適正な管理）
第13条　情報資産を保管又は設置する建物及び関連設備については、適正な管理を行う。
（教育及び訓練）
第14条　職員に対する情報セキュリティに関する教育及び訓練は、定期的に行う。
（外部要員の監督）
第15条　外部要員が、本市の情報資産、建物及び関連設備を取り扱う場合においては、情報セキュリティポリシーに遵守する旨の契約を締結するとともに、外部要員に対して適切な監督を行う。
（業務委託と外部サービスの利用）
第15条の２　業務委託を行う場合には、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。
２　外部サービス（クラウドサービス）を利用する場合には、利用に係る基準を整備し対策を講じる。
（情報システムの適正な管理）
第16条　情報システムについては、その設計、構築、運用管理等において適正な管理を行う。
（情報システム全体の強靭性の向上）
第16条の２　情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。
（１）　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、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等により、住民情報の流出を防ぐ。
（２）　LGWAN 接続系においては、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を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。
（３）　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
（情報資産へのアクセス管理）
第17条　情報資産は、許可された者のみが取り扱えるよう、情報及び取り扱う者の区分に応じて、アクセス管理の措置を講ずる。
（ソフトウェアの適正な管理）
第18条　ソフトウェアについては、その設計、開発、運用管理等において適正な管理を行う。
（コンピュータウイルス対策）
第19条　コンピュータウイルス感染の被害者とならないため、及び本市以外の企業、団体及び個人に対して加害者とならないため適切な措置を講ずるものとする。
（情報セキュリティ事故への対応）
第20条　情報セキュリティ事故の発生又はその疑いが生じた場合の連絡手続等を明確にし、情報セキュリティ事故が発生したときは、業務継続のための復旧措置を講ずるとともに、再発防止措置を講ずるものとする。

（著作権の保護）
第21条　本市以外のものが作成した著作物を利用する場合には、その著作物に随伴する著作権に配慮した取扱いを行う。
２　一般に流通しているソフトウェアを導入する場合には、前項に加えて使用許諾条件を遵守し、その使用状況を適正に管理する。
（監査及び点検）
第22条　情報セキュリティ対策の状況等について、外部事業者による外部監査、デジタル推進課による内部監査又は各課等による自主点検を適宜実施する。
（評価及び見直し）
第22条の２　市長は、前条に規定する事項を実施した結果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、情報セキュリティポリシーの見直しが必要と判断した場合、それらの評価及び見直しを実施する。

第５章　その他

（法令遵守）
第23条　職員及び外部要員は、業務の遂行において使用する情報資産の取扱いに当たっては、著作権法（昭和45年法律第48号）、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）、個人情報の保護に関する法律のほか、関連する法令等を遵守しなければならない。
（秘匿義務）
第24条　職員及び外部要員は、業務上知り得た情報を他人に漏えいしてはならない。
（懲戒）
第25条　職員が、情報セキュリティポリシーに定める事項の遵守を怠った結果、本市に重大な損害をもたらした場合は、地方公務員法による懲戒の対象とする。
（例外措置）
第26条　情報資産の取扱いについて、情報セキュリティポリシーに照らして判断できないとき、又はその遵守が困難なときは、推進会議が対応を検討し、指示するものとする。
別表（第２条、第３条関係）

	区分	規定事項	文書の名称	文書の内容
情報セキュリティポリシー	情報セキュリティ基本方針	基本規程	情報セキュリティ基本規程	本市の情報セキュリティ対策の目的、方針、原則等を規定したもの（本規程）
	情報セキュリティ対策基準	体制	最高情報統括責任者等設置規程	本市における情報セキュリティ対策を実施するための全庁的な体制を規定したもの
		職員の責務	情報資産取扱倫理規程	本市の情報資産の取扱いに関して、すべての職員が遵守すべき倫理事項を規定したもの
		情報資産の分類と管理	電子化情報取扱規程	電子化情報の取扱いに関して、作成から保管、利用、消去までの全ライフサイクルでの管理の実施要領を規定したもの
		物理的セキュリティ	情報機器等物理的セキュリティ規程	本市に導入及び設置される情報機器及びネットワーク構成機器の物理的なセキュリティ対策の実施要領を規定したもの
			情報セキュリティに関する建物設備の管理規程	建物又は設備におけるセキュリティ対策の実施要領を規定したもの
		人的セキュリティ	情報セキュリティ教育及び訓練実施規程	情報セキュリティに関する教育及び訓練の実施要領を規定したもの
			外部要員監督規程	外部要員に対するセキュリティ上の監督の実施要領を規定したもの

		技術的セキュリティ	情報システムセキュリティ規程	庁内外の情報システムを構築する際の設計から設置、運用管理、保守までのセキュリティ上実施すべき管理の実施要領を規定したもの
			アクセス管理規程	本市の情報資産へのアクセス管理及び利用者管理の実施要領を規定したもの
			ソフトウェアセキュリティ規程	ソフトウェアについて設計、開発、運用管理、保守までのセキュリティ上実施すべき管理の実施要領を規定したもの
			コンピュータウイルス対策規程	コンピュータウイルス検査の実施要領を規定したもの
		運用	情報セキュリティ緊急時行動規程	情報セキュリティに関する緊急事態発生時における行動指針を規定したもの
		法令遵守	ソフトウェアライセンス管理規程	本市において導入し、利用するソフトウェアのライセンス管理の実施要領を規定したもの
		評価・見直し	情報セキュリティ自主点検規程	情報セキュリティポリシーの継続的遵守状況等に関する自主点検の実施要領を規定したもの