福生市サイバーセキュリティ基本方針

（目的）

第１条　福生市（以下「市」という。）は、地方自治法（昭和 22 年法律第 67 号）に基づき、市民の個人情報をはじめとする重要な情報を多数保有するとともに、市民生活及び地域社会経済活動の維持向上に必要不可欠な行政サービスを提供しており、市が保有する情報資産は、市の行政運営の基盤であり、その適切な保護及び管理は、市に課せられた責務であることから、本方針は、同法第 244 条の６に基づき、市が講ずべきサイバーセキュリティ対策に関する基本的事項を定め、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し、サイバー攻撃等の様々な脅威から情報資産を守ることにより、市の行政運営の安定的・継続的な遂行を実現することを目的とする。

２　全ての職員等は、サイバーセキュリティの重要性を認識し、市におけるサイバーセキュリティ対策の推進に積極的に取り組むものとする。

３　本方針は、サイバーセキュリティ基本法（平成 26 年法律第 104 号）及び地方公共団体における情報セキュリティポリシーに関するガイドライン（令和７年３月版総務省）を参考として策定する。

４　市が保有する個人情報の漏えい、滅失又は毀損の防止その他の安全管理措置については、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 66 条に基づき、本方針及び福生市情報セキュリティ対策基準（平成 27 年訓令第 10 号。以下「対策基準」という。）に基づいて実施されるものとする。

（定義）

第２条　この方針において、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）　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網及び構成機器で構成され、情報処理を行う仕組みをいう。

（２）　情報システム　コンピュータ及びネットワークにより業務処理を行う仕組みをいう。

（３）　情報資産　次のいずれかに該当するものをいう。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（出力した文書も含む。）

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

（４）　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。

（５）　サイバーセキュリティ　デジタル環境における情報の機密性、完全性、可用性を維持するための包括的な取組をいう。

（６）　機密性　情報にアクセスすることを認められた者のみが、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）　職員等　市の情報資産に接する全ての職員（受託事業者、指定管理者並びにその従業員、派遣及び再委託先従事者を含む。）をいう。

(10)　受託事業者　市から情報資産の取扱いを委託された者又は市から情報資産の取扱いを請け負う者をいう。

(11)　マイナンバー利用事務（個人番号利用事務）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。以下「マイナンバー法」という。）第９条第２項に規定する個人番号利用事務又は戸籍事務等に関わる情報システムをいう。

(12)　ＬGWAN接続（内部事務）系　総合行政ネットワーク（ＬGWAN）に接続された情報システム（マイナンバー利用事務系を除く。）をいう。

(13)　インターネット接続系　ＬGWAN接続系の情報システムで使用する電子メール以外の電子メール、Ｗｅｂサイト管理システム、内部事務を取り扱う情報システム等のインターネットに接続された情報システムをいう。

(14)　情報セキュリティインシデント　予期しない単独又は一連の情報セキュリティ事象であって、業務の遂行を危うくし、情報セキュリティを脅かす可能性の高いものをいう。

(15)　ＣＩＳＯ　最高情報セキュリティ責任者の事であり、副市長をいう。

(16)　ＣＳＩＲＴ　情報セキュリティインシデントに対処するための体制のことであり、企画財政部情報政策課をいう。

(17)　個人情報漏えい等　個人情報保護法第 68 条第 1 項に規定する個人情

報の漏えい、滅失、毀損その他の保有個人情報の安全の確保に係る事態であって、個人の権利利益を害するおそれが大きいものをいう。

（対象とする脅威）

第３条　次に掲げる市の情報資産に対する脅威を想定し、サイバーセキュリティ対策を実施する。この場合において、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

（１）　不正アクセス、ウイルス攻撃、ランサムウェア攻撃、サービス不能攻撃等のサイバー攻撃並びに侵入等の意図的要因による市の情報資産の漏えい、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

（３）　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

（４）　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

（５）　電力供給の途絶、通信の途絶等のインフラ障害からの波及等

（適用範囲）

第４条　この方針が適用される範囲は、次の各号のいずれかに該当する者（マイナンバー利用事務系、ＬＧＷＡＮ接続系又はインターネット接続系利用する者に限る。）とする。

（１）　福生市組織規則（昭和 53 年規則第１号）第２条に規定する部及び課

（２）　福生市教育委員会事務局処務規則（昭和 53 年教育委員会規則第１号）第２条に規定する部及び課

（３）　公民館

（４）　図書館

（５）　市立小中学校

（６）　議会、選挙管理委員会、農業委員会、固定資産評価審査委員会又は監査委員（事務局を含む。）

２　この方針が対象とする情報資産は、次のとおりとする。

（１）　情報システム及びネットワーク

（２）　個人情報のほか、情報システム等で取り扱うデータ

（３）　情報システム等に関するシステム設計書、ネットワーク図等のシステム関連文書

（職員等の遵守義務）

第５条　職員等は、市が保有する情報資産に対する脅威への対応の重要性について共通の認識を持ち、業務の遂行に当たって、本方針及び対策基準、実施手順等を遵守しなければならない。

（サイバーセキュリティ対策）

第６条　市は、第３条に規定する脅威から情報資産を保護するため、次のサイバーセキュリティ対策を講じる。

（１）　組織体制の確立　市の情報資産についてサイバーセキュリティ対策を推進する全庁的な組織体制を確立し、ＣＩＳＯ及び統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者等の役割・責任を明確化する。この場合において、情報セキュリティインシデント発生時に迅速かつ適切に対応するため、ＣＳＩＲＴを整備し、及び緊急時対応体制を確保し、インシデント発生時は、情報セキュリティ管理者を起点として統括情報セキュリティ責任者及びＣＩＳＯへ速やかに報告・連携する体制を維持する。

（２）　情報資産の分類と管理　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、当該分類に基づき、適切なセキュリティ対策を講じる。

（３）　情報システム全体の強じん性の向上　市は、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三層に分離した情報システム環境を構築し、各層の特性に応じた情報セキュリティ対策を講じることにより、情報システム全体の強じん性（業務継続能力及び迅速な復旧能力をいう。）を向上させる。

（４）　物理的セキュリティ対策　サーバ、電算室、通信回線及び職員のパソコン等の管理について、不正な立入り及び盗難、損傷、破壊、自然災害等から情報資産を保護するため、必要な物理的対策を講じる。

（５）　人的セキュリティ対策　情報セキュリティに関する権限や責任を定め、職員等に対する十分な教育及び啓発が講じられるように必要な対策を講じ

る。

（６）　技術的セキュリティ対策　コンピュータ等の管理、アクセス制御、ネットワーク管理、コンピュータウイルス対策その他の必要な技術的対策を講じる。

（７）　運用面での対策　情報システムの監視及び情報セキュリティポリシー等の遵守状況の確認のほか、次号の業務委託及びクラウドサービスを利用する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での対策を講じるものとする。この場合において、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応体制を整備する。

（８）　業務委託及びクラウドサービス利用に係る対策　市は、業務委託及びクラウドサービス等の外部サービス利用に当たり、委託事業者及び指定管理者（以下「委託事業者等」という。）の選定時に情報セキュリティ要件を明示し、個人情報の目的外利用禁止、秘密保持義務、情報の返却・廃棄等の事項を契約に明記するものとする。この場合において、委託期間中は委託事業者等における情報セキュリティ対策の履行状況を定期的に確認し、改善指導を行うとともに、情報セキュリティインシデント発生時は直ちに報告を求め適切に対処し、クラウドサービス等の外部サービスを利用する場合は、サービス提供者のセキュリティ水準、個人情報保護体制、情報の保存地域、廃棄方法等を事前に確認し、取り扱う情報の分類に応じて利用承認を得た上で、委託終了時には、提供した情報を確実に返却・廃棄させ、その処理内容を記録・保管するものとする。

（９）　個人情報保護対策　市が保有する個人情報については、個人情報保護法第 66 条に基づき、安全管理措置を講じ、情報セキュリティインシデントにより個人情報漏えい等が発生した場合は、個人情報保護委員会への報告を行うとともに、原則として本人に対する通知を行う。

（リスクに対する計画の策定）

第７条　情報セキュリティに係る内部環境及び外部環境の変化を踏まえ、市が保有する情報資産の情報セキュリティ上のリスクに対し、「福生市情報セキュリティポリシーに基づく緊急時対応計画」を策定し、毎年福生市情報セキュリティ委員会に報告する。

（自己点検及びセキュリティ監査の実施）

第８条　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて、自己点検及びセキュリティに関する監査を実施する。この場合において、セキュリティに関する監査は、被監査組織から独立し、監査及び情報セキュリティに関する専門知識を有する者が実施する。

（情報セキュリティポリシーの見直し）

第９条　自己点検及びセキュリティに関する監査の結果、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又は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となった場合には、情報セキュリティポリシーの見直しを実施し、福生市情報セキュリティ委員会にて審議する。この場合において、原則として毎年度、見直しが必要であるか否かを福生市情報セキュリティ委員会にて審議するものとする。

（対策基準・実施手順の策定）

第 10 条　第６条から前条までに規定する対策等を実施するため、具体的な遵守事項及び判断基準等を定める「福生市情報セキュリティ対策基準」及び情報システムごとに情報セキュリティ対策の具体的な手順等を定めた「情報セキュリティ実施手順」を策定する。この場合において、当該実施手順については、関連する情報システム等の情報セキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の運営に重大な支障を及ぼすおそれがあることから、第４条第１項に規定する行政機関の適用範囲以外に対しては非公開とする。

附　則

この方針は、令和８年４月１日から施行する。