善通寺市サイバーセキュリティを確保するための方針

（善通寺市情報セキュリティポリシー　第７版）

情報セキュリティ基本方針

令和８年３月

善通寺市

＜目次＞

善通寺市長、善通寺市教育委員会、善通寺市議会、善通寺市選挙管理委員会、善通寺市監査委員、善通寺市農業委員会、善通寺市固定資産評価審査委員会、善通寺市公平委員会は、善通寺市情報セキュリティ基本方針を共同で定める。

また、当該基本方針については、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

１．目的

本基本方針は、善通寺市（以下「本市」という）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。

２．定義

（１） ネットワーク

電子計算機等を相互に接続し、情報を伝送するための通信回線網その他の仕組みをいう。

（２） 情報システム

電子計算機により継続的に情報を処理する仕組み（ネットワーク上のものを含む。）をいう。

（３） 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。

（４） 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５） 機密性

情報が、不必要な若しくは権限なき閲覧、第三者への不当な開示又は盗聴等により漏えいされないことをいう。

（６） 完全性

情報が、意図しない変更、改ざん、又は損壊されないことにより、正確性を保つことをいう。

（７） 可用性

情報の利用を認められた者が、必要な時にその情報を適切に利用できる状態であることをいう。

３．対象とする脅威

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、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、水道供給の途絶等のインフラの障害からの波及等

４．適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、市長部局、教育委員会、議会、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、公平委員会、消防本部とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、（１）に示す行政機関が所掌する資産のうち、次の通りとする。

① 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電磁的記録媒体

② 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。）

③ 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

（３）職員等の範囲

本基本方針が適用される職員及び職員に準ずる者（以下、「職員等」という）は、次の通りとする。

① （１）に示す行政機関に所属し、（２）に示す情報資産を取り扱う職員、再任用職員、会計年度任用職員及び派遣職員

② ①に準じて（２）に示す情報資産を取り扱う特別職（市長、副市長、教育長、議員及び各行政委員会等の委員等）及び教職員

５．職員等の遵守義務

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ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

６．情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１） 組織体制

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を確立する。

（２） 情報資産の分類と管理

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、当該分類に基づき情報セキュリティ対策を実施する。

（３） 物理的情報保護対策

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、物理的な対策を講じる。

（４） 人的情報保護対策

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を講じる。

（５） 技術的情報保護対策

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

を講じる。

（6） 運用

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を講じるものとする。また、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、緊急時対応計画を策定する。

（7） 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、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。

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

７．情報セキュリティ監査及び自己点検の実施

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情報セキュリティ監査及び自己点検を実施する。

８．情報セキュリティポリシーの見直し

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

９．情報セキュリティ対策基準の策定

上記６、７及び８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を策定する。

ただし、市長部局が整備するネットワークと論理的または物理的に分離されているネットワークについては、当該ネットワークを所管する行政機関が個別に対策基準を必要に応じて策定するものとする。

１０．情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、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を策定するものとする。

なお、情報セキュリティ実施手順は、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。