臼杵市サイバーセキュリティ基本方針

1. 目的

本基本方針は、臼杵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、サイバー攻撃等の脅威に対する対策の基本的な事項を定め、もって臼杵市の行政運営の安全かつ円滑な実施を確保することを目的とします。また、本基本方針は、サイバーセキュリティ基本法及び地方自治法の趣旨に則り、本市におけるサイバーセキュリティの確保に関する施策を総合的かつ効果的に推進するための基本方針として位置づけます。

2. 定義

(1) 対象とする脅威

本市は、情報資産に対する脅威として、以下の脅威を想定し、サイバーセキュリティ対策を実施します。

① 不正アクセス、ウイルス攻撃、サービス不能攻撃(DDoS 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、システム障害等の非意図的要因による事故

③ 災害やインフラ障害によるサービス及び業務の停止

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

(2) 情報システムの分類

本市が保有する情報システムは、その取扱う情報の重要性等に応じ、「マイナンバー利用事務系」、「LGWAN 接続系」、「インターネット接続系」に分離・分割または適切なアクセス制御により管理します。

3. 適用範囲

本基本方針が適用される行政機関は、市長部局、議会事務局、監査事務局、選挙管理委員会事務局、農業委員会事務局、教育委員会事務局、消防本部及び地方公営企業とし、これらが取り扱うネットワーク、情報システム及びデータ等の全ての情報資産を対象とします。

4. 実施体制

臼杵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ため、全庁的な組織体制を以下の通り確立します。また、サイバーセキュリティ対策を確実に実施するために必要な予算及び人材を確保し、専門的な知識を有する職員の育成に努めます。

(1) 最高情報セキュリティ責任者(CISO)

副市長を充て、臼杵市における全てのネットワーク、情報システム等の情報資産の管理及び

情報セキュリティ対策に関する最終決定権限及び責任を有します。
（2） 統括情報セキュリティ責任者
デジタル政策監を充て、CISO を補佐し、全庁的な情報セキュリティ対策の権限及び責任を有します。
（3） 情報システム管理者
DX 戦略課長を充て、全庁的な情報システムの開発・運用・見直し等に関する権限及び責任を有します。
（4） CSIRT（Computer Security Incident Response Team）
サイバー攻撃等のインシデントに対処するための緊急時対応体制を整備します。事務局は DX 戦略課とし、インシデント発生時には CISO の指示の下、迅速な対応を行います。
（5） 情報セキュリティ委員会
全庁的な対策の審議・決定を行います。

5. 情報セキュリティ対策
脅威から情報資産を保護するため、以下の対策を講じます。
（1） 情報資産の分類と管理
保有する情報資産を機密性（3A・3B・3C・2・1）、完全性、可用性に応じて分類し、その重要度に応じた適切な管理措置を講じます。
（2） 情報システム全体の強靭性の向上（サイバーレジリエンス）
業務の効率性・利便性の観点を踏まえつつ、以下の対策を講じます。
① マイナンバー利用事務系における他の領域との通信遮断、端末からの情報持ち出し不可設定、多要素認証の導入。
② LGWAN 接続系とインターネット接続系の通信経路の分割および無害化通信の実施。
③ インターネット接続系における不正通信の監視機能強化および自治体情報セキュリティクラウドの導入等による高度なセキュリティ対策の実施。
（3） 物理的・技術的・人的セキュリティ
① 物理的対策: サーバ室等の入退室管理、機器の盗難防止、通信回線及び通信回線装置の管理等。
② 技術的対策: アクセス制御、不正プログラム対策、不正アクセス対策、システム開発・保守時のセキュリティ確保等。
③ 人的対策: 全職員等に対する定期的な教育・研修及び訓練の実施、パスワード管理の徹底等。
（4） 業務委託と外部サービス（クラウドサービス）の利用
① 業務委託（サプライチェーンリスク対策）: 委託事業者を選定する際、情報セキュリティ要件を明記した契約を締結し、必要な対策が確保されていることを確認します。
② クラウドサービスの利用: 利用にかかる規定を整備し、ISMAP（政府情報システムのた

めのセキュリティ評価制度）等を参考に、安全性が確保されたサービスを選定・利用します。ソーシャルメディアサービスの利用においても運用手順を定めます。

6．法令遵守

職員等は、サイバーセキュリティ基本法、地方公務員法、個人情報の保護に関する法律、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等の関係法令及び本市の規定を遵守します。違反した場合には、懲戒処分等の対象となります。

7．インシデント対応と事業継続

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します。また、災害等に備えた業務継続計画（BCP）との整合性を確保し、総務省、内閣サイバーセキュリティセンター（NISC）、警察、情報処理推進機構（IPA）、地方公共団体情報システム機構（J-LIS）、大分県及び他の地方公共団体との連携・情報共有を強化します。

8．評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的に情報セキュリティ監査及び自己点検を実施します。監査の実施にあたっては、被監査部門からの独立性を確保し、客観的な評価を行います。必要に応じて外部監査を活用します。また、情報セキュリティに関する状況の変化に対応するため、適宜ポリシーの見直しを行い、継続的な改善を図ります。