

御坊市サイバーセキュリティを確保するための方針

令和8年3月1日制定

- 1 目的
- 2 定義
 - (1) ネットワーク
 - (2) 情報システム
 - (3) 情報資産
 - (4) 管理区域
 - (5) 情報セキュリティ
 - (6) 情報セキュリティポリシー
 - (7) 機密性
 - (8) 完全性
 - (9) 可用性
 - (10) マイナンバー利用事務系（個人番号利用事務系）
 - (11) LGWAN 接続系
 - (12) インターネット接続系
 - (13) 通信経路の分離
 - (14) 無害化通信
- 3 対象とする脅威
- 4 適用範囲
 - (1) 市の機関の範囲
 - (2) 情報資産の範囲
- 5 職員等の遵守義務
- 6 情報セキュリティ対策
 - (1) 組織体制
 - (2) 情報資産の分類と管理
 - (3) 情報システム全体の強靱性の向上
 - (4) 物理的セキュリティ
 - (5) 人的セキュリティ
 - (6) 技術的セキュリティ
 - (7) 運用
 - (8) 業務委託と外部サービスの利用
 - (9) 評価・見直し
- 7 情報セキュリティ監査及び自己点検の実施

- 8 情報セキュリティポリシーの見直し
- 9 情報セキュリティ対策基準の策定
- 10 情報セキュリティ実施手順の策定

御坊市サイバーセキュリティを確保するための方針

1 目的

御坊市サイバーセキュリティを確保するための方針（以下「方針」という。）は、御坊市（以下「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、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とともに、市のサイバーセキュリティを確保するための方針として定めることを目的とする。

2 定義

(1) ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

コンピュータ等、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報資産

情報及び情報を取り扱うための仕組みをいう。

(4) 管理区域

ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋や電磁的記録媒体の保管庫をいう。

(5) 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。

(6) 情報セキュリティポリシー

御坊市情報セキュリティ基本方針及び御坊市情報セキュリティ対策基準をいう。

(7) 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。

(8) 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。

(9) 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。

(10) 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、地方税及び防災に関する事務）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。

(11) 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。）。

(12) 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。

(13) 通信経路の分離

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(14) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

3 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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の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) 市の機関の範囲

方針が適用される市の機関は、市長、教育委員会（小・中学校を除く。）、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、地方公営企業、消防本部及び議会とする。

(2) 情報資産の範囲

方針が対象とする情報資産は、次のとおりとする。

- ア ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体
- イ ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- 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

5 職員等の遵守義務

職員（再任用職員を含む。）、会計年度任用職員、派遣職員及び特に市長が認める者（以下「職員等」という。）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、次の情報セキュリティ対策を講じる。

(1) 組織体制

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

市の保有する情報資産を機密性、完全性及び可用性を踏まえて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点から踏まえ情報システム全体

に対し、次の対策を講じる。

ア 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。

イ 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離する。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。

ウ 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、県及び市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。

(4) 物理的セキュリティ

サーバ、管理区域、通信回線、パソコン等の管理について、物理的な対策を講じる。

(5) 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、教育及び啓発を行う等の人的な対策を講じる。

(6) 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を講じる。

(7) 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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(8) 業務委託と外部サービスの利用

業務委託を行う場合には、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た上で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する。

外部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に責任者を定める。

(9) 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し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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、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、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、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。

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、情報システム又は業務において具体的な対策の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。