西置賜行政組合
情報セキュリティ基本方針

令和８年４月

西置賜行政組合

1. 目的

本基本方針は、西置賜行政組合（以下「組合」という。）が保有し又は業務上取り扱う情報資産について、機密性・完全性・可用性を維持し、組合運営の継続性を確保するため、組合が実施すべき情報セキュリティ対策の基本的事項を定めることを目的とする。

2. 定義

本基本方針における用語は、次のとおり定義する。

用語	定義
ネットワーク	コンピュータ等を相互に接続する通信網及びその構成機器（ハードウェア・ソフトウェア）をいう。
情報資産	組合の事務及び事業に係る情報並びにそれを取り扱うための資産（文書・図面・写真・音声・映像・データベース等の情報）及びこれを処理・保存・伝送するための機器、媒体、ソフトウェア、設定情報等をいう。
情報システム	コンピュータ、ネットワーク、運用手順、及び電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。
重要業務システム	停止又は機能低下が、組合の運営に重大な影響を与える情報システムをいう。
情報セキュリティ	情報資産の機密性・完全性・可用性を維持することをいう。
職員等	組合の職員、委託先従事者、指定管理者その他組合の業務に従事する者で組合の情報資産を取り扱う者をいう。
個人情報等	個人情報の保護に関する法律その他の法令により保護される個人に関する情報をいう。
不正プログラム	コンピュータウイルス等、情報資産に不正な動作をさせるプログラムをいう。
不正アクセス	権限のない者が情報システムにアクセスし、又は権限を逸脱して操作することをいう。
クラウドサービス	インターネット等を介して提供される計算資源、アプリケーション又は保管領域等のサービスをいう。
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（対応組織）をいう。
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。

3. 対象とする脅威

組合は、情報資産に対する脅威として、次に掲げる脅威を想定し、対策を推進する。

1. 不正アクセス、なりすまし、権限の不正利用、サービス不能攻撃（DDoS）等のサイバー攻撃による情報の漏えい、改ざん、消去、破壊又は重要情報の詐取
2. 標的型攻撃メール、不正サイトの閲覧等を起点とするマルウェア（ランサムウェアを含む。）感染による情報の漏えい、暗号化又は業務停止
3. 内部不正、誤操作、設定不備、保守・メンテナンス不備、脆弱性の放置、誤送信等による情報の漏えい、消失又は改ざん
4. 媒体又は端末の紛失・盗難、庁舎への不正侵入、機器故障、停電、通信障害、災害等による情報資産の損壊又は情報システムの停止・性能低下
5. 委託先又はクラウド等の外部サービスに起因する事故、障害、設定不備等による情報漏えい又は業務への支障
6. 重要業務システムの停止又は遅延に伴う組合運営への重大な支障

4. 適用範囲

本基本方針は、組合が保有又は業務上取り扱う全ての情報資産に適用する。適用範囲は、次のとおりとする。

1. 組合の全ての組織及び情報資産を取り扱う全ての職員等
2. 組合が保有又は管理する全ての情報資産
3. 組合が管理する施設に設置された情報機器、ネットワーク及び関連設備
4. 組合が利用する全ての情報システム及びネットワーク
5. 職員等が業務に用いる端末及び記録媒体等（パソコン、スマートフォン、タブレット、車載端末、携帯端末、デジタル無線端末、外部記憶媒体その他これらに類するものを含む。）
6. 外部委託又はクラウドサービスにより取り扱う情報資産及び情報システム

ただし、法令・条例・規則等に特段の定めがある場合は、それらを優先する。

5. 職員等の遵守義務

職員等は、法令等及び組合の規程に従い、本基本方針並びに情報セキュリティ対策基準を遵守しなければならない。

1. 業務上知り得た情報の目的外利用、無断提供、持ち出し等を行わないこと。
2. 利用権限の範囲内でのみ情報資産にアクセスし、ID・パスワード等の認証情報を適切に管理すること。

3. 不審なメール、端末の異常、情報の誤送信・紛失等、インシデントの兆候を認知した場合は、速やかに所定の連絡先へ報告すること。
4. 組合が指定する研修・訓練を受講し、対策の理解と実践に努めること。

6. 情報セキュリティ対策

組合は、次に掲げる観点から情報セキュリティ対策を講じる。具体的な遵守事項及び判断基準は情報セキュリティ対策基準に定める。

（1）組織体制

1. 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し、役割と責任を明確化する。
2. インシデントに対処するための体制（CSIRT）を整備し、連絡体制と初動対応の方針を定める。

（2）情報資産の分類と管理

1. 情報資産を機密性・完全性・可用性に応じて分類し、分類に基づく取扱制限を行う。
2. 情報資産の台帳整備、取扱責任者の明確化、複製・伝送時の同等管理を行う。

（3）情報システム全体の強靭性の向上

1. 業務上必要な区分によりネットワークやシステムを分離し、相互の影響を最小化する。
2. インターネットとの通信は必要最小限とし、安全な通信（例：無害化・分離等）の実現に努める。

（4）物理的・人的・技術的対策

1. 庁舎・サーバ室等の入退室管理、設備管理、端末・媒体の持出し管理を実施する。
2. 研修・啓発、権限管理、点検等により、人的リスク及び内部不正リスクを低減する。
3. アクセス制御、暗号化、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実施する。

（5）運用・監視・インシデント対応

1. 情報システムの監視、ログの取得・保全、脆弱性情報の収集等を行い、平時から備える。
2. インシデント発生時に迅速かつ適切に対応するため、緊急時対応計画を整備する。
3. 必要に応じて関係機関等への報告、住民・関係者への通知、公表対応を行う。

（6）業務委託と外部サービス（クラウドサービス）の利用

1. 委託事業者の選定、情報セキュリティ要件を明記した契約締結、委託先対策の確認と監督を行う。
2. 外部サービス利用にあたっては、取り扱う情報の重要度に応じた評価・承認及び利用ルールを整備する。

3. ソーシャルメディアを利用する場合は、発信できる情報範囲、責任者、運用手順を定める。

（7）評価・見直し

1. 定期的又は必要に応じて監査及び自己点検を実施し、改善措置を講じる。
2. 社会情勢、脅威、技術、運用状況の変化を踏まえ、情報セキュリティポリシーを適宜見直す。

7. 情報セキュリティ監査及び自己点検

組合は、情報セキュリティポリシーの遵守状況及び対策の有効性を検証するため、情報セキュリティ監査及び自己点検を実施する。監査・点検の方法、頻度、結果の取り扱い及び是正措置は別に定める。

8. 情報セキュリティポリシーの見直し

監査・点検の結果、又は情報セキュリティを取り巻く状況の変化により見直しが必要となった場合には、脅威の発生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

本基本方針を具体化し、遵守事項及び判断基準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。実施手順は、原則として非公開とする。

附則

本基本方針は、令和 8 年 4 月 1 日から施行する。