西置賜行政組合

情報セキュリティ対策基準

令和８年４月

西置賜行政組合

本基準は、西置賜行政組合（以下「組合」という。）における情報資産の適正な管理と、組合業務の継続を確保するため、情報セキュリティ対策に必要な具体的対策及び遵守事項を定めるものである。

本基準に定めのない詳細手順は、別途「情報セキュリティ実施手順」等により定める。

1 組織体制

組合は、情報セキュリティ対策を推進するため、次の体制を整備する。職務の割当は、組織規則等に応じて管理者が定める。

1-1 最高情報セキュリティ責任者

最高情報セキュリティ責任者（事務局長）は、組合における情報セキュリティ対策を総括し、その最終責任を負うものとし、次に掲げる事項を所掌する。

1. 情報セキュリティに関する方針、基準及び計画の承認
2. 情報セキュリティ対策の企画、推進及び各部門間の調整
3. 情報資産の分類、管理台帳、アクセス権限その他情報資産管理に関する統制
4. 教育・訓練、監査、点検及び見直しの統括
5. 委託先管理及びクラウドサービス利用管理の統括
6. 重要なリスク及び対策状況の把握並びに是正指示
7. 重大インシデント発生時における意思決定（業務継続、外部通報、住民対応等）

1-2 情報セキュリティ責任者

情報セキュリティ責任者（各管理職）は、担当部門における情報資産及び情報システムの管理責任を負い、次を行う。

1. 担当部門の情報資産の管理及び取扱いの徹底
2. 担当部門の利用者への指導、点検、是正
3. 担当部門で発生した事故・障害の報告と初動対応

1-3 情報システム管理者

情報システム管理者（事務局長、荘長、及び総務課長）は、情報システムの運用管理責任を負い、次を行う。

1. アカウント管理、アクセス制御、設定管理、ログ管理
2. 脆弱性対応、パッチ適用、マルウェア対策の実施
3. バックアップ、復旧、冗長化、障害対応の実施
4. 委託先作業の管理及び受入確認

1-4 情報システム担当者

情報システム担当者（事務局補佐、副荘長及び総務課補佐）は、情報システム管理者を補佐し、日常の運用、端末管理、利用者支援等を行う。

1-5 職員等

職員等は、情報セキュリティ対策の主体として、次を行う。

1. 本基準及び手順の理解と遵守
2. 情報資産の適正な取扱い（持出・送信・廃棄等の手続遵守）
3. 不審なメール、端末異常、情報漏えい等の兆候を把握した場合の速やかな報告
4. 庁内外の活動時を含む、端末・書類等の紛失防止

2 情報資産の管理

2-1 情報資産の分類

情報資産は、その重要性に応じて次の区分に分類し、区分に応じた管理を行う。

区分	概要
I（極秘）	漏えい、改ざん又は消失により、住民の生命・身体の保護、重要住民サービスの継続又は重大な権利利益に深刻な影響を及ぼす情報
II（秘）	漏えい、改ざん又は消失により、組合の業務又は住民等の権利利益に相当の影響を及ぼす情報
III（内部）	漏えい等により影響は限定的だが、組織内での管理が必要な情報
IV（公開）	公開しても支障がない情報

2-2 情報資産管理簿

情報資産は、情報資産管理簿により一元管理し、次の事項を記録する。

1. 情報資産の名称、情報セキュリティ責任者、保管場所、媒体、分類区分

2. 取扱いに関する制限（閲覧・持出・複製・送信・保管期間等）
3. 情報システムの場合は、構成、委託先、保守契約、バックアップ方針、復旧目標等

2-3 情報資産の取扱い

情報資産の作成、利用、保管、送信、持出、廃棄は、分類区分に応じて次のとおり実施する。

1. 情報資産を取り扱う際は必要に応じて、暗号化、アクセス制御、持出制限を行い、必要最小限の者のみが取り扱う。
2. 電子媒体の送信は、原則として組織が指定する手段（暗号化メール、ファイル転送サービス等）に限定する。
3. 外部記憶媒体の利用は必要最小限とし、使用時はウイルスチェック及び持出記録を行う。
4. 紙媒体は施錠保管とし、廃棄時はシュレッダー又は溶解処理等により復元不能とする。
5. 業務上取得した画像・動画等は、業務用媒体に速やかに移送し、個人端末内に保持しない。

2-4 情報資産の持出し

情報資産を庁舎外へ持ち出す場合は、事前に情報セキュリティ責任者の承認を得て、次を実施する。

1. 持出目的、期間、持出者、持出物を記録する。
2. 庁外活動中も常に携行又は施錠保管する。

2-5 情報資産の廃棄・返却

情報資産の廃棄又は委託先等からの返却に当たっては、漏えい又は復元の防止を徹底し、廃棄・返却の記録を残す。

3 物理的対策

3-1 情報システムの設置・管理

情報システムを設置する区域（情報システム室、サーバ室、事務室等）は、次を実施する。

1. 重要業務システムの設置場所は、耐火、耐水、温湿度管理、電源（UPS 等）等を考慮する。
2. 端末・機器は盗難防止措置（ワイヤーロック、施錠保管等）を講じる。
3. 来庁者等が機器や情報資産に容易に接触できない配置とする。

3-2 管理区域の管理

管理区域（情報システム室、サーバ室、書庫等）への入退室は、必要最小限の者に限定し、次を実施する。

1. 入退室の記録（入退室管理簿又はログ）を取得し、一定期間保管する。
2. 来訪者には入館手続を実施し、必要に応じて同行又は監視する。
3. 鍵、入退室カード等は適切に管理し、紛失時は速やかに無効化する。

3-3 庁外活動等における物理的対策

庁外活動等で使用する端末・媒体（車載端末、携帯端末等を含む。）については、次を実施する。

1. 車両内への固定、施錠、持出時の携行等により盗難・紛失を防止する。
2. 業務上取得した写真・映像、通報・届出情報等の表示が第三者に閲覧されないよう配慮する。
3. 持出端末は画面ロック、暗号化、遠隔消去等を可能な範囲で設定する。

4 人的対策

4-1 雇用・配置に関する対策

職員等の採用・配置・離任に当たっては、次を実施する。

1. 守秘義務及び情報セキュリティ遵守に関する誓約を取得する。
2. 業務上必要な権限のみを付与し、異動・退職時は速やかに権限を変更又は削除する。
3. 委託先従事者についても同等の秘密保持及び教育を求める。

4-2 研修・訓練

組合は、情報セキュリティ意識の向上及び初動対応力の確保のため、次を実施する。

1. 全職員向けに年 1 回以上の情報セキュリティ研修を実施する（e ラーニングを含む）。
2. 新規採用者、異動者、委託先従事者に対し、着任時教育を実施する。
3. 重要業務担当者に対し、インシデント対応（ランサムウェア、システム停止等）を想定した訓練を実施する。
4. 不審メール訓練、机上訓練、復旧訓練等を計画的に実施する。

4-3 懲戒等

本基準に違反した場合は、条例規則等に基づき必要な措置を行う。

5 技術的対策

情報システム管理者及び情報システム担当者は、次の技術的対策を実施しなければならない。

5-1 アカウント管理

1. ID は利用者ごとに一意に付与し、共用 ID の使用は原則禁止する（やむを得ない場合は情報セキュリティ責任者が理由と範囲を明確化する）。
2. パスワードは推測困難なものとし、他システムとの使い回しを禁止する。
3. 多要素認証（MFA）が利用可能な場合は、特権 ID、外部接続、クラウド利用に適用する。
4. 管理者権限の付与は最小限とし、付与・変更・削除を記録する。

5-2 アクセス制御

1. 職務分掌に基づく権限管理（ロールベース）を実施し、必要最小限のアクセス権とする。
2. I・II の情報資産が格納されたフォルダ、データベース等は、アクセス権を明確化し定期的に棚卸する。
3. 離席時は画面ロックを徹底し、一定時間無操作時に自動ロックする設定とする。

5-3 アクセス記録等の取得・保管

1. 重要業務システム及びサーバ等について、認証、アクセス、重要操作、エラー等のログを取得する。
2. ログは改ざん防止に配慮して保管し、保管期間を定める（重要業務システムは長期保管を検討する）。
3. 不正アクセスの兆候（認証失敗の多発等）を検知した場合は、速やかに原因確認と封じ込めを実施する。

5-4 ネットワーク対策

1. ネットワークは用途に応じて分離し、不要な通信を遮断する（業務系とインターネット系の分離等）。
2. 外部接続はファイアウォール等により制御し、必要なサービス・ポートのみ許可する。
3. 無線 LAN は強固な暗号化及び認証を用い、ゲスト用と業務用を分離する。

4. 遠隔保守・リモートアクセスは、事前承認、VPN、MFA、アクセスログ取得等の条件を満たす場合に限定する。

5-5 端末対策

1. OS 及びソフトウェアはサポート期間内のものを利用し、セキュリティ更新を適用する。
2. ウイルス対策ソフト等によりマルウェア対策を行い、定義ファイルを最新化する。
3. 外部記憶媒体の自動実行を禁止し、許可された媒体のみ使用する。
4. 端末の暗号化（BitLocker 等）を可能な範囲で実施し、紛失時の漏えいを低減する。

5-6 電子メールのセキュリティ管理

1. メールゲートウェイ又は端末側で、ウイルス検査及びスパム対策を行う。
2. 標的型攻撃メールを想定し、添付ファイル及び URL の安全性確認を徹底する。
3. メール送信時の誤送信防止（宛先確認、外部宛て警告、送信保留等）の仕組みを導入又は運用で補完する。
4. なりすまし対策（SPF/DKIM/DMARC 等）は管理範囲で可能な対策を講じる。

5-7 電子メールの利用制限

1. 業務で個人のメールアドレス又はフリーメールを使用してはならない。
2. 情報資産をメールで送信する場合は、必要に応じて暗号化、パスワード別送、又は組織が指定する安全な送受信手段を用いる。
3. チェーンメール、機密情報の不用意な一斉送信等、情報漏えいの恐れがある行為を禁止する。
4. メールの自動転送を外部宛てに設定してはならない（業務上やむを得ない場合は最高情報セキュリティ責任者の承認を要する）。

5-8 外部ネットワークとの接続

1. 外部ネットワーク（インターネット等）との接続点は管理し、機器・設定を最新の状態に保つ。
2. 外部から内部ネットワークへの直接接続を原則禁止し、必要な場合は VPN 等により認証・暗号化を行う。
3. 外部公開が必要なサーバ等は、内部ネットワークから分離された領域（DMZ 等）に配置する。

5-9 文書サーバ等の設定

1. 文書サーバ、ファイル共有、クラウドストレージ等のアクセス権は、分類区分と職務に応じて設定する。
2. 共有フォルダの新設・権限変更は申請・承認制とし、定期的に棚卸を行う。

5-10 インターネットの利用制限

1. 業務上不要なサイトへのアクセスを制限し、有害サイト、違法サイト、情報漏えいリスクの高いサイトへのアクセスを遮断する。
2. ソフトウェアやファイルのダウンロードは必要最小限とし、信頼できる提供元からのみ実施する。
3. オンラインストレージ、ファイル共有サービス等は、組織が許可したもの以外を業務利用してはならない。

5-11 可用性対策（重要業務継続）

1. 重要業務システム等の停止時に備え、代替手段（手書き台帳、代替連絡手段、手動処理手順等）を整備する。
2. バックアップ、冗長化、予備機、復旧手順及び復旧目標（RTO/RPO）を定める。
3. 停電時の電源確保（UPS、自家発電等）及び通信回線の冗長性を検討する。
4. 災害時その他の非常時における情報共有システム等に係るアカウント、手順、連絡体制を平時から整備する。

6 外部委託及びクラウドサービスの利用

6-1 外部委託の管理

1. 委託範囲、取扱う情報資産の分類、責任分界、作業手順、再委託の可否を明確化する。
2. 委託先に対し、秘密保持、目的外利用の禁止、事故報告、監査協力等を契約で担保する。
3. 委託先の作業は事前承認とし、作業記録・ログを確保する。
4. 委託終了時は、情報資産の返却・消去を確認し記録する。

6-2 クラウドサービスの利用

1. 利用目的、取扱う情報資産の分類、保管場所（国内外）、暗号化、認証方式等を事前に確認する。

2. 重要情報を取り扱う場合は、MFA、アクセス制御、ログ取得、バックアップ等の要件を満たすサービスに限定する。
3. サービス終了や障害時の代替手段、データ移行・消去手順を確認する。

7 運用（情報システムの運用・開発・保守）

組合は、情報システムの安定運用及び継続的改善のため、次を実施する。

7-1 バックアップ

1．重要データ及び重要業務システムは、定期的にバックアップを取得し、保管場所を分散する。
2．バックアップデータは改ざん及びランサムウェア被害を考慮し、オフライン又は分離環境で保管することを検討する。
3．定期的に復旧テストを実施し、復旧可能性及び所要時間を確認する。

7-2 変更管理

1．システム設定、ネットワーク構成、アカウント権限等の変更は、申請・承認・記録により管理し、影響評価を行う。
2．緊急変更は事後に承認・記録を行い、恒久対策を検討する。

7-3 障害・インシデント記録

1．障害、事故、インシデント及びその復旧対応について、発生日時、影響範囲、原因、対応内容、再発防止策を記録する。
2．重要業務システムに影響する事象は、最高情報セキュリティ責任者へ速やかに報告する。

7-4 脆弱性管理

1．脆弱性情報を収集し、重要度に応じてパッチ適用、回避策適用等を実施する。
2．サポート切れ製品の利用を避け、やむを得ない場合は代替策（ネットワーク分離、アクセス制限等）を講じる。

7-5 システム開発・保守に関する管理

1．開発・保守を行う者の利用者 ID 及び権限は、作業終了後速やかに抹消する。
2．守秘義務、再委託管理、持込機器の管理等を徹底する。
3．開発環境、テスト環境、運用環境を分離し、移行手順を明確化する。
4．新規導入又は改修時は十分な試験を実施し、運用に影響が最小となるよう配慮する。

5．開発・保守に関連する資料、設計書、運用手順、ソースコード等は適切に整備・保管する。
6．入力データの妥当性チェック等を組み込み、誤入力・改ざんの影響を低減する。

7-6 監視及び点検

1．重要業務システム、ネットワーク、端末について、稼働監視、ログ点検等を行い、異常の早期検知に努める。
2．外部公開資産や委託先作業についても、必要に応じて監視・点検を実施する。

7-7 情報セキュリティインシデント対応

1．インシデント発生時は、別途定める手順に従い、封じ込め、原因究明、復旧、再発防止及び必要な外部通報を行う。
2．重要業務システムに影響する場合は、組合業務の継続を最優先とし、代替手段へ速やかに切り替える。
3．個人情報等の漏えいが疑われる場合は、法令等に基づき対応する。

8 手順等

本基準を実施するため、次に掲げる手順書等を整備し、必要に応じて改定する。

1．情報資産管理簿の運用手順
2．外部記憶媒体の運用手順
3．情報セキュリティインシデント対応手順（通報・連絡体制、初動対応、対外対応を含む）
4．重要業務に係る業務継続手順（代替手段、復旧手順等）

9 例外措置

業務上やむを得ず本基準の例外措置を講ずる必要がある場合は、情報システム管理者の承認を得た上で、代替措置を講じ、記録する。

10 法令等の遵守

職員等は、個人情報の保護に関する法律、地方公務員法、著作権法、不正アクセス行為の禁止等に関する法律その他関係法令を遵守しなければならない。

11 違反時の措置

職員等が本基準に違反した場合は、条例規則等に基づき必要な措置を行うとともに、必要に応じて関係機関への通報、被害者への通知等を実施する。

12 評価及び見直し

組合は、情報セキュリティ対策の有効性を評価し、少なくとも年 1 回又は重大な環境変化・事故発生時に本基準及び関連手順を見直す。