# 西海岸衛生処理組合
# 情報セキュリティポリシー

令和７年８月２０日策定

令和７年９月１日施行

<目次>

# 序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、西海岸衛生処理組合が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、西海岸衛生処理組合が所掌する情報資産に関する業務に携わる全職員、非常勤、臨時職員（以下、「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

① 情報セキュリティ基本方針
② 情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。(下表参照)。

情報セキュリティポリシーの構成

| 文　書　名 | | 内　　容 |
|---|---|---|
| 情報セキュリティポリシー | 情報セキュリティ基本方針 | 情報セキュリティ対策に関する統一的かつ基本的な方針。 |
| | 情報セキュリティ対策基準 | 情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。 |

# 第１章　情報セキュリティ基本方針

## １　目的

本基本方針は、当組合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、当組合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

コンピュータ等を相互に接続するための通信網、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、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。

（６）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。

（７）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。

## 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、外部委託管理の不備、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）組織の範囲

本基本方針が適用される組織は、内部部局、議会、監査委員とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム及びこれらに関する設備、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

## 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

当組合の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２）情報資産の分類と管理

当組合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）物理的セキュリティ

サーバ等、情報システム室等、通信回線等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、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。

（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等のため、運用面における必要な対策を講じるものとする。また、緊急事態が発生した場合に迅速に対応するため、危機管理対策を講ずる。

## 7　情報セキュリティ対策の実施状況の検証

情報セキュリティポリシーの遵守状況を検証するため、情報セキュリティ対策の実施状況について、定期的又は必要に応じて検証を行う。

## 8　情報セキュリティポリシーの見直し

情報セキュリティ対策の実施状況の検証結果または情報セキュリティに関する状況の変化に対応するため、必要に応じて情報セキュリティポリシーの見直しを行う。

# 第２章　西海岸衛生処理組合における情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、当組合における情報資産に関する情報セキュリティ対策の基準を定めたものである。

## １　組織体制

（１）情報セキュリティ責任者

①　事務局長を情報セキュリティ責任者とする。

②　情報セキュリティ責任者は、情報セキュリティ対策に関する統括的な権限及び責任を有する。

（２）情報セキュリティ管理者

①　事務局次長を情報セキュリティ管理者とする。

②　情報セキュリティ管理者は、所管する部局の情報セキュリティ対策に関する権限及び責任を有する。

③　情報セキュリティ管理者は、所管する部局の情報システムの開発、設定変更、運用、見直し等を行う権限及び責任を有する。

④　情報セキュリティ管理者は、所管する部局において、情報資産に対する侵害が発生した場合または侵害の恐れがある場合には、情報システム管理者に連絡するとともに、情報セキュリティ責任者に報告しなければならない。

（３）情報システム管理者

①　所長を情報システム管理者とする。

②　情報システム管理者は、情報システムのセキュリティに関する権限及び責任を有する。

③　情報システム管理者は、情報システムの開発、設定変更、運用、見直し等を行う権限及び責任を有する。

（４）情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

（５）情報セキュリティ委員会

当組合の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

## ２　情報資産の分類と管理

（１）情報資産の分類

当組合における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

| 分類 | 分類基準 | 取扱制限 |
|---|---|---|
| 機密性３ | 情報資産のうち、秘密文書に相当する機密性を要する情報資産 | ・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して）<br>・必要以上の複製及び配付禁止<br>・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止<br>・情報の送信、情報資産の運搬･提供時における暗号化･パスワード設定や鍵付きケースへの格納<br>・復元不可能な処理を施しての廃棄<br>・信頼のできるネットワーク回線の選択<br>・外部で情報処理を行う際の安全管理措置の規定<br>・電磁的記録媒体の施錠可能な場所への保管 |
| 機密性２ | 情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産 | |
| 機密性１ | 機密性２又は機密性３の情報資産以外の情報資産 | |

完全性による情報資産の分類

| 分類 | 分類基準 | 取扱制限 |
|---|---|---|
| 完全性２ | 情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産 | ・バックアップ、電子署名付与<br>・外部で情報処理を行う際の安全管理措置の規定<br>・電磁的記録媒体の施錠可能な場所への保管 |
| 完全性１ | 完全性２情報資産以外の情報資産 | |

可用性による情報資産の分類

| 分類 | 分類基準 | 取扱制限 |
|---|---|---|
| 可用性２ | 情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産 | ・バックアップ、指定する時間以内の復旧<br>・電磁的記録媒体の施錠可能な場所への保管 |
| 可用性１ | 可用性２の情報資産以外の情報資産 | |

（２）情報資産の管理

①　管理責任

ア　情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

イ　情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

②　情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③　情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

イ　情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④　情報資産の入手

ア　情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

イ　情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤　情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

イ　情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

ウ　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥　情報資産の保管

ア　情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

イ　情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

ウ　情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦　情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ、暗号化又はパスワード設定を行わなければならない。

⑧　情報資産の運搬

ア　車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

イ　機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨　情報資産の提供・公表

ア　機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

イ　機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

ウ　情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保し

なければならない。

⑩　情報資産の廃棄

ア　機密性２以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

イ　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

ウ　情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

## ３　物理的セキュリティ

### （１）サーバ等の管理

①　機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

②　機器の電源

ア　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

③　通信ケーブル等の配線

ア　統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

イ　統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

エ　統括情報セキュリティ責任者、情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加

できないように必要な措置を講じなければならない。

④　機器の定期保守及び修理

ア　情報システム管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

イ　情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

⑤　機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（２）管理区域（情報システム室等）の管理

①　管理区域の構造等

ア　管理区域とは、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（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ　情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

ウ　情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

②　管理区域の入退室管理等

ア　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿等による入退室管理を行わなければならない。

イ　外部からの訪問者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ　情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　情報システム管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

③　機器等の搬入出

ア　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響に

ついて、あらかじめ職員又は委託した業者に確認を行わせなければならない。

イ　情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

（3）通信回線及び通信回線装置の管理

① 情報システム管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

② 情報システム管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③ 情報システム管理者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

④ 情報システム管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑤ 情報システム管理者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

（4）職員等の利用する端末や電磁的記録媒体等の管理

① 情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

② 情報システム管理者は、情報システムへのログインにパスワードの入力を必要とするように設定しなければならない。

## 4　人的セキュリティ

（1）職員等の遵守事項

① 職員等の遵守事項

ア　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

イ　業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

ウ　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

・　職員等は、当町のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

・　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

エ　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

・　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

・　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

オ　持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

カ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

キ　机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

ク　退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

②　情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

③　外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

（2）研修・訓練

①　情報セキュリティに関する研修・訓練

情報システム管理者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

②　研修計画の策定及び実施

ア　情報システム管理者は、職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

イ　研修計画において、職員等は毎年度最低1回は情報セキュリティ研修を受講できるようにしなければならない。

③　研修・訓練への参加

職員等は、定められた研修・訓練に参加しなければならない。

（3）ID 及びパスワード等の管理

①　ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

ア　自己が利用している ID は、他人に利用させてはならない。

イ　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

②　パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ　パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

エ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

オ　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

カ　サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

キ　職員等間でパスワードを共有してはならない（ただし共有 ID に対するパスワードは除く）。

## 5　技術的セキュリティ

（1）コンピュータ及びネットワークの管理

①　バックアップの実施

情報システム管理者は、サーバ等に記録された情報について、定期的にバックアップを実施しなければならない。

②　他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、情報セキュリティ責任者の許可を得なければならない。

③　システム管理記録及び作業の確認

情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

④　情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

⑤　障害記録

情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

⑥　情報ネットワークの接続制御、経路制御等

ア　情報システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

イ　情報システム管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

⑦　外部の者が利用できるシステムの分離等

情報システム管理者は、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑧　外部ネットワークとの接続制限等

ア　情報セキュリティ管理者は、所管する情報ネットワークを外部ネットワークと接続しようとする場合には、情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

イ　情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、情報セキュリティ責任者及び情報システム管理者に報告するとともに、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑨　複合機のセキュリティ管理

ア　情報セキュリティ管理者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　情報セキュリティ管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

⑩　無線 LAN 及びネットワークの盗聴対策

ア　情報セキュリティ管理者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

イ　情報セキュリティ管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

⑪　電子メールのセキュリティ管理

ア　情報セキュリティ管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

イ　情報セキュリティ管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

⑫　電子メールの利用制限

ア　職員等は、自動転送機能を用いて電子メールを転送してはならない。

イ　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

ウ　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

エ　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

⑬　無許可ソフトウェアの導入等の禁止

ア　職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

イ　職員等は、業務上の必要がある場合は、情報セキュリティ管理者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。

ウ　職員等は、不正にコピーしたソフトウェアを利用してはならない。

⑭　機器構成の変更の制限

ア　職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

イ　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報セキュリティ管理者及び情報システム管理者の許可を得なければならない。

⑮　無許可でのネットワーク接続の禁止

職員等は、情報セキュリティ管理者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

⑯　業務以外の目的でのウェブ閲覧の禁止

ア　職員等は、業務以外の目的でウェブを閲覧してはならない。

イ　情報システム管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ責任者及び情報セキュリティ管理者に通知し適正な措置を求めなければならない。

（2）アクセス制御

①　アクセス制御

情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

②　利用者 ID の取扱い

ア　情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

イ　情報システム管理者は、利用されていない ID が放置されないよう点検しなければならない。

③　パスワードに関する情報の管理

情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。

（3）情報システム開発、導入、保守等

①　情報システムの調達

ア　情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ　情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

②　情報システムにおける入出力データの正確性の確保

ア　情報システム管理者は、情報システムに入力されるデータについて、範囲及び妥

当性のチェック機能並びに不正文字列入力の除去機能を組み込むように情報システムを設計しなければならない。

イ　情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合は、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ　情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

③　情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（４）不正プログラム対策

①　情報システム管理者の措置事項

ア　外部ネットワークから受信又は送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入又は外部への拡散を防止しなければならない。

イ　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じて、職員等に対して注意喚起しなければならない。

ウ　サーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

エ　不正プログラム対策のソフトウェア及びそのパターンファイルは、常に最新の状態に保たなければならない。

オ　インターネットに接続していないシステムにおいて、記録媒体を使う場合は、コンピュータウイルス等の感染を防止するため、組合が管理している媒体以外のものを職員等に利用させてはならない。

②　職員等の遵守事項

ア　パソコン等の端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合は、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

ウ　差出人が不明なメール又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

エ　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

オ　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

カ　コンピュータウイルス等の不正プログラムに感染した場合は、ＬＡＮケーブルの

取り外し及び機器の電源遮断を行わなければならない。

（5）不正アクセス対策

① 情報システム管理者の措置事項

ア 使用されていないポートを閉鎖しなければならない。

イ 不要なサービスについて、機能を削除又は停止しなければならない。

ウ 不正アクセスによるウェブページの改ざんを防止するため、データの書換えを検出するよう設定しなければならない。

② 攻撃の対処

情報システム管理者は、サーバ等に攻撃を受けることが明確になった場合は、システムの停止その他必要な措置を講じなければならない。

③ 記録の保存

情報システム管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止等法違反等の犯罪の可能性がある場合は、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

④ 内部からの攻撃

情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末を利用した組合サーバ等に対する攻撃及び外部サイトに対する攻撃を監視しなければならない。

⑤ 職員等による不正アクセス

情報システム管理者は、職員等による不正アクセスを発見した場合は、情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

（6）セキュリティ情報の収集

① セキュリティホールに関する情報の収集、共有等

情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じて、関係者間で共有しなければならない。この場合において、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

② 不正プログラム等のセキュリティ情報の収及び周知

情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じて、職員等に周知しなければならない。

## 6 運用

（1）情報システムの監視

① 情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

② 情報システム管理者は、重要なアクセスログ等を取得するため、サーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③ 情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

（2）情報セキュリティポリシーの遵守状況の確認

① 遵守状況の確認及び対処

ア 情報システム管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題があると認めた場合は、速やかに、情報セキュリティ責任者に報告し、発生した問題について、適切に対処しなければならない。

イ 情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合は、適切かつ速やかに対処しなければならない。

② 職員等の報告義務

職員等は、情報セキュリティポリシーに対する違反行為を発見した場合は、直ちに、情報システム管理者に報告しなければならない。

（3）侵害時の対応

情報セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合は、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施しなければならない。

（4）例外措置

① 例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合は、情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

② 緊急時の例外措置

情報セキュリティ管理者は、事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、当該例外措置を実施後、速やかに、情報セキュリティ責任者に報告しなければならない。

③ 例外措置の申請書の管理

情報セキュリティ責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

（５）法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次に掲げる法令その他の関係法令を遵守しなければならない。

① 地方公務員法(昭和 25 年法律第 261 号)
② 著作権法（昭和 45 年法律第 48 号）
③ 不正アクセス行為の禁止等に関する法律
④ 個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑤ サイバーセキュリティ基本法（平成28 年法律第31 号）
⑥ 西海岸衛生処理組合個人情報の保護に関する法律施行条例(令和 5 年条例第 1 号)

（６）懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

## 7 評価・見直し

（１）監査

① 実施方法

情報セキュリティ委員会は、情報システム担当者をして情報ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的又は必要に応じて、監査を行わせなければならない。

② 監査実施計画の立案及び実施への協力

ア 情報システム担当者は、監査を行うに当たっては、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

③ 外部委託事業者に対する監査

情報システム担当者は、外部委託事業者に委託している場合は、外部委託事業者から下請として受託している事業者も含めて情報セキュリティポリシーの遵守について、監査を定期的又は必要に応じて行わなければならない。

④ 報告

情報システム担当者は、監査結果を取りまとめ、情報セキュリティ委員会に報告しなければならない。

⑤ 保管

情報システム担当者は、監査の実施によって、収集した監査証拠又は監査報告書の作成のための監査調書を適切に保管しなければならない。

⑥ 監査結果への対応

情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する情報セキュリ

ティ管理者に対し、当該事項への対処を指示しなければならない。

⑦　情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し時に活用しなければならない。

（2）自己点検

①　実施方法

ア　情報システム管理者は、情報ネットワーク及び情報システムについて、必要に応じて、自己点検を実施しなければならない。

イ　情報セキュリティ管理者は、情報システム管理者の行う点検について、協力しなければならない。

②　報告

情報システム管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

③　自己点検結果の活用

ア　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　情報セキュリティ委員会は、点検結果を情報セキュリティポリシーの見直し時に活用しなければならない。

（3）情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティポリシーについて、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合は、その見直しを行うものとする。