大阪広域環境施設組合情報セキュリティ対策基準

制　定　平成 30 年３月 30 日
改　正　令和５年３月 31 日

1　目的

この大阪広域環境施設組合情報セキュリティ対策基準（以下「対策基準」という。）は、大阪広域環境施設組合情報セキュリティ管理規程（平成 27 年達３号。以下「管理規程」という。）第７条及び関連規定に基づき、本組合における情報資産の取扱いについて遵守すべき事項及び情報セキュリティ対策の実施に関する統一的な基準を定めることにより、本組合が保有する情報資産をさまざまな脅威から守り、機密性、完全性及び可用性（注）を維持することによって、本組合の円滑な運営を確保することを目的とする。

（注）：国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)
機密性(confidentiality)　：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完全性(integrity)　：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性(availability)　：許可された利用者が必要なときに情報アクセスできることを確実にすること。

2　用語

この対策基準において使用する用語は、管理規程において使用する用語の例によるほか、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 職員　大阪広域環境施設組合職員基本条例第２条に規定する職員をいう。
(2) 端末機　パソコンやモバイル端末等の機器をいう。
(3) サーバ　主としてデータやファイルの保存、配信及びバッチ処理に特化した共用の機器をいう。
(4) セキュリティインシデント　情報セキュリティに関する問題として捉えられる事象（障害、事件、事故、欠陥、攻撃、侵害等）をいう。
(5) 庁内情報ネットワーク　本組合において、共通の基盤となる通信ネットワークをいう。
(6) アクセス権限　情報システム及び通信ネットワーク（以下「情報システム等」という。）の利用者が、データ及びプログラムを利用できる権限をいう。

3　適用範囲

この対策基準の適用範囲は、本組合の保有する全ての情報資産とする。

4　想定する脅威

この対策基準が想定する脅威は次のとおりとする。

(1) 不正アクセス、ウイルス及び標的型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、火災等の災害等
(4) 電力供給の途絶、通信の途絶等のインフラの障害からの波及等

5　情報セキュリティ対策

情報セキュリティ対策の項目を次のとおり定める。

(1) 情報資産の分類

情報資産を機密性、完全性及び可用性を踏まえ分類すること。

(2) 物理的セキュリティ

サーバ、通信回線及び職員の端末機等の管理について、物理的な対策を講じること。

(3) 人的セキュリティ

職員が遵守すべき事項を定め、並びに教育及び啓発を行うこと。

(4) 技術的セキュリティ

端末機等の管理、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な対策を講じること。

(5) 運用

情報システム等の監視、情報セキュリティポリシー（以下「ポリシー」という。）の遵守状況の確認、外部委託を行う際のセキュリティ確保等、ポリシーの運用面の対策を講じること。

6　ＩＴ管理者の責務

ＩＴ管理者は、管理規程に定めるもののほか、統括情報セキュリティ責任者の命を受けて、次の責務を担う。

ア　情報セキュリティ対策の総括

イ　課情報セキュリティ責任者が実施するセキュリティインシデントを回復するための措置又はセキュリティインシデント発生のおそれがある場合の予防措置に関する助言又は調整

ウ　緊急時等の円滑な情報共有を図るための緊急連絡網の整備、運用

7　課情報セキュリティ責任者の責務

課情報セキュリティ責任者は、管理規程に定めるもののほか、統括情報セキュリティ責任者の命を受け、次の責務を担う。

ア　所管課における情報セキュリティ対策の総括

イ　ポリシーに基づく情報セキュリティ実施手順（以下「実施手順」という。）の作成

ウ　所管課における情報資産に関する台帳等の整備、運用

エ　所管課における情報システム等に対するアクセス権限の管理

8　情報資産の管理

(1) 情報資産の管理責任

①　情報資産の管理責任は、当該情報資産を所管する課の課情報セキュリティ責任者が有する。

②　情報資産を業務上利用する職員は、ポリシーに則って利用する責任を有する。

(2) データの管理

①　情報資産におけるデータは、各々のデータの機密性、完全性、可用性を踏まえ、以下の重要性分類に従って分類し、重要性分類に従ったアクセス権限を設定する。

重要性分類

Ⅰ　個人情報及び業務上必要とする最小限の者のみが扱うデータ

Ⅱ　公開することを予定していないデータ及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼすデータ

Ⅲ　外部に公開するデータのうち、セキュリティ侵害が行政事務の執行等に影響を及ぼすデータ

Ⅳ　上記以外のデータ

②　作成途上のデータであっても漏えい、滅失、き損、改ざん等を防止するため、作成済みのデータに準じて取り扱う。また、作成途上で不要になった場合は速やかに消去する。

③　所管課以外のものが作成したデータを入手した場合(データを複製したときを含む。)も自ら作成したものと同様に取り扱う。

(3)　情報資産の管理

①　情報資産の管理

ア　情報資産は、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び大阪広域環境施設組合個人情報の保護に関する法律の施行等に関する条例（令和５年条例第３号。以下「個人情報保護法等」という。）その他の関連する法令等及び規程に基づき、データの漏えい、滅失、き損、改ざん、消去、盗難等の防止を図る。

イ　複数種のファイル、データを格納する記録媒体、ドキュメント等の情報資産は、当該情報資産に含まれるデータのうち最も上位の重要性分類に従い取り扱う。

ウ　外部に公開するデータについては完全性を確保する。

エ　重要性分類Ⅰに属するデータは、課情報セキュリティ責任者の許可なく複製あるいは出力（記憶媒体への格納を含む。以下同じ。）し、庁外へ持ち出し（電子メール等に添付する場合を含む。以下同じ。）をすることはできない。

オ　重要性分類Ⅱ以上のデータを庁外へ持ち出すときは、課情報セキュリティ責任者の許可を得たうえで、暗号化又はパスワード設定を行う。

カ　重要性分類Ⅲ以下に属するデータを庁外へ持ち出す場合は、必要に応じ暗号化又はパスワード設定を行う。

キ　電子メールによりデータを送付するときは送信先のメールアドレスを十分に確認し、必要に応じ送信先に対し受領確認を行う。

ク　庁内におけるデータの取扱いについても、庁外へ持ち出す場合に準じて行う。

②　記録媒体等の管理

ア　データが格納された記録媒体等の授受に関しては、次の事項を記録する台帳等を整備する。また、記録媒体等を搬送するときは、データの漏えい、滅失、き損、改ざん等を防止するため、専用トランクを使用する。

(ｱ)　ファイルの名称

(ｲ)　搬入者及び受領者の氏名並びにその所属等の名称

(ｳ)　媒体の種別

(ｴ)　媒体の識別番号

(ｵ)　授受年月

(ｶ)　その他課情報セキュリティ責任者が必要と認める事項

イ　データが格納された記録媒体等の保管に関しては、データの重要性が容易に識別できるよう次の事項を記録する台帳等を整備する。

(ｱ)　ファイルの名称

(ｲ)　業務主管課名

(ｳ)　媒体の種別

(ｴ)　媒体の識別番号

(ｵ)　作成年月日

(ｶ) 保管期限
(ｷ) 消去年月日
(ｸ) 格納場所
(ｹ) その他課情報セキュリティ責任者が必要と認める事項

ウ　データが格納された記録媒体は、常用後廃棄するまでの間は書込禁止のプロテクトを設定して適切に保管する。

エ　磁気ディスクその他の記録媒体に不要なデータが放置されないよう、不要となったデータは速やかに消去する。

オ　情報資産を廃棄するときは、課情報セキュリティ責任者の許可を得て、データを復元できないよう確実な方法で消去したうえで廃棄するとともに、行った処理について、日時、担当者、処理内容等を記録する。

9　物理的セキュリティ

(1) サーバ

①　装置の設置等

ア　サーバは、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除できる環境に設置し、当該場所については施錠等により入退室管理を行う。

イ　停止することで本組合の業務運営に大きな影響を及ぼすおそれがあるサーバについては、原則として管理及び運用を行うため専用の部屋に設置する。

ウ　サーバは、転倒又は盗難を防止するため、固定する等の方法で管理する。

②　サーバの冗長化

サーバは原則として冗長化を図り、運用が停止しないよう予防する。

③　無停電電源設備等

サーバには停電等による電源喪失に備え、当該機器を適切に停止するまでの間に十分な電力を供給できる容量の予備電源を備え付け、また、落雷等による異常電流から保護するための保護回路を備える。

④　庁外への設置

課情報セキュリティ責任者は、所管する情報システム等に属するサーバを庁外に設置する場合は、随時セキュリティ対策状況について点検し、統括情報セキュリティ責任者へ報告する。

(2) 端末機等

職員が使用する端末機等については、ワイヤーによる固定や執務室等の施錠等により管理する。

(3) 接続機器等

①　ハブやルータ及び配線については、当該接続機器等が設置されている課の課情報セキュリティ責任者以外の者が容易に操作できないような場所に格納又は設置する。また、落雷等による異常電流及び停電等の電気的障害に対する保護回路を設置する。

②　情報システム等の接続に使用する回線については、伝送途上で情報の破壊、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が実装されているものを調達する。

特に、重要性分類Ⅱ以上の情報資産を取り扱う情報システムを接続する回線については、冗長構成等、継続的な運用が可能な回線を調達する。

③　通信ネットワークを構築するにあたり、有線による通信ネットワークの整備が適さない合理的な理由がある場合には、統括情報セキュリティ責任者の許可を得て無線回線による整備を行う。

10　人的セキュリティ

(1) ポリシー等の遵守

職員は、ポリシー及び実施手順に定められている事項を遵守しなければならない。

(2) 教育、研修

① 統括情報セキュリティ責任者は、情報セキュリティ対策の重要性に鑑み、情報セキュリティを確保するための基本方針を策定する。

② 課情報セキュリティ責任者は、統括情報セキュリティ責任者の策定した基本方針に則り、ＩＴ管理者と連携のうえ、情報セキュリティに係る研修を実施することにより、職員にポリシー及び実施手順の周知徹底を図るとともに、研修その他の機会を利用して、情報セキュリティの確保に必要な知識、技術について、教育、指導を行う。

(3) 端末機の目的外使用禁止

職員は、設定されているアクセス権限の範囲内で業務上必要な情報を処理するものとし、業務目的以外での情報システムへのアクセス及びインターネットへのアクセス、メールの使用等通信ネットワークの利用を行ってはならない。また、職員は、Web で利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。ただし、課情報セキュリティ責任者が業務上必要と判断した場合を除く。

(4) 情報漏えい等の防止

① 職員は、課情報セキュリティ責任者の許可なく端末機又は記録媒体等を執務室以外に持ち出し、庁外で情報処理業務を行ってはならない。ただし、同一庁舎内において常時携行するなど自己の管理下に置き、持ち出し先の会議室等において施錠等の盗難防止措置を確実に行える場合はこの限りではない。なお、携行中は端末機のロック、ログオフ、又はシャットダウンを行わなければならない。

② 職員は、業務用として貸与されたもの以外の端末機及び記録媒体等を業務に利用してはならない。ただし、災害対応等業務上必要な場合として課情報セキュリティ責任者の許可を得た場合はこの限りではない。

③ 職員は、モバイル端末を庁外で使用する際には遠隔消去機能等の紛失、盗難防止策が有効であることを確認したうえで使用しなければならない。

④ 職員は、異動又は退職する場合は、利用していた端末機等を返却しなければならない。

⑤ 職員は、使用する端末機や記録媒体について、権限を有しない者の使用や閲覧を防止するため、離席時には端末機をロックするなど容易に使用、閲覧されないよう管理しなければならない。

⑥ 課情報セキュリティ責任者は、端末機及び記録媒体の持ち出しについて、記録を作成し、保管しなければならない。

⑦ 職員は、端末機のソフトウェアに関するセキュリティ機能の設定を変更してはならない。

(5) 無許可ソフトウェアの導入等の禁止

① 職員は、課情報セキュリティ責任者の許可なく端末機へのソフトウェアのインストール及びアンインストール、若しくは設定変更をしてはならない。

② 職員は、著作権法や使用許諾契約等に違反するソフトウェアの使用又は複製等を行ってはならない。

(6) セキュリティインシデントに対する対応

① 職員は、セキュリティインシデントを発見した場合又は外部から通報を受けた場合は、速やかに課情報セキュリティ責任者に報告しなければならない。

② 課情報セキュリティ責任者は、セキュリティインシデントを発見又は報告通報を受けた場合、速やかにＩＴ管理者と連携し、その助言に基づき必要な措置を講じなければならない。

③ 職員は、課情報セキュリティ責任者の指示に従い、セキュリティインシデントに対し適切に対処しなければならない。

(7) ＩＤの取扱い

職員は、自己の管理するＩＤを他者に利用させてはならない。

また、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。

(8) パスワードの管理

① 課情報セキュリティ責任者は、所管する情報システム等を初めて利用する職員にパスワードを発行する場合は仮のパスワードを発行し、職員は、情報システム等にログイン後直ちに仮のパスワードを変更しなければならない。

② 職員は、自己の保有するパスワードに関して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すること。

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ないこと。

ウ パスワードは英数字記号の混在した 8 文字以上の十分な長さとし、想像しにくい文字列とすること。

エ 異なる情報システムや通信ネットワークとの間で、また職員間でパスワードを共有しないこと。ただし、組織メールへのアクセス用等、共用することを前提とする場合を除く。

オ 端末機等のパスワードの記憶機能を利用しないこと。

カ パスワードが流出した可能性がある場合は速やかに課情報セキュリティ責任者に報告し、パスワードを変更すること。

(9) IC カード等の取扱い

① 職員は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。

ア 自己が認証に用いる IC カード等を、職員間で共有しないこと。

イ 共用 IC カード等は、共用 IC カード等の利用者として登録された者以外に利用させないこと。

ウ 業務上必要のないときは、IC カード等をカードリーダ若しくはカードスロットから抜いておくこと。

エ IC カード等を紛失した場合には速やかに課情報セキュリティ責任者に報告し、その指示に従うこと。

② 課情報セキュリティ責任者は、所管する情報システム等に係る IC カード等の紛失等の通報があったときは、速やかに当該 IC カード等によるアクセス等を停止しなければならない。

③ 課情報セキュリティ責任者は、所管する情報システム等に係る IC カード等を更新する場合は、更新前のカードを回収し、物理的に破砕するなど認証情報等を復元不可能な状態にしたうえで廃棄しなければならない。

11 技術的セキュリティ

(1) アクセス制御

① アクセス権限の設定

課情報セキュリティ責任者は、所管するシステム等へアクセス可能な利用者及びその利用範囲等のアクセス権限を設定する。

② アクセス権限の管理

ア 課情報セキュリティ責任者は、所管する情報システム等へのアクセス権限を、ユーザＩＤ及びユーザＩＤごとに一意のパスワードにより管理する。

イ 課情報セキュリティ責任者は、情報システム等で正しくないログイン操作が繰り返しなされた場合等、不正アクセスが疑われる事象に対しては、アクセスを制限する。

ウ 課情報セキュリティ責任者は、所管する情報システム等のユーザＩＤ及びパスワードの付与や削除等の手続きについて定め、職員に周知する。

エ 課情報セキュリティ責任者は、利用されていないＩＤを放置しないよう点検する。

また、管理者権限等の特権を付与されたＩＤの発行は必要最小限にし、当該ＩＤ及びパスワードを厳重に管理する。

③　通信ネットワーク管理

ア　課情報セキュリティ責任者は、所管する通信ネットワークに接続するサーバ及び端末機等には個々の機器を特定する識別記号を設定・配付し、未登録機器による不正な接続を防止する。

イ　課情報セキュリティ責任者は、所管する通信ネットワーク設定情報については、不正に変更されないよう厳重に管理し、障害時等に備え、定期的に設定情報のバックアップを作成する。また、通信ネットワーク構成等に関する情報は、特別な事情がある場合を除き開示してはならない。

ウ　課情報セキュリティ責任者は、所管する通信ネットワーク上の通信利用状況並びに稼働実績及び資源の利用状況を、障害検知機能等を利用し常時監視する。

エ　課情報セキュリティ責任者は、所管する通信ネットワーク利用に大きな支障を生じさせかねない大容量のファイルの通信を制限する等とともに、フィルタリング及びルーティングについては、ファイアウォールやルータ等により通信制御を行う。

(2)　不正アクセス対策

①　課情報セキュリティ責任者は、所管する情報システム等において各種ログを取得し、業務目的以外の不適切な利用を検知した場合、アクセス制限等により接続を遮断する。

②　課情報セキュリティ責任者は、所管する情報システム等を外部の通信ネットワークと接続しようとするときは、ＩＴ管理者と協議のうえ、接続を行う外部通信ネットワークの構成、セキュリティレベル並びに接続することによって生じるリスク等を詳細に検討し、十分な情報セキュリティ対策が実装されていることを確認しなければならない。

③　課情報セキュリティ責任者は、所管する情報システム等を外部通信ネットワークに接続するときは、統括情報セキュリティ責任者の承認を受けなければならない。

④　課情報セキュリティ責任者は、データ提供のために本組合以外のものと電子計算機の結合を行うときは、外部からの不正なアクセスを防御するため、ファイアウォール、侵入検知装置の設置、ポートの管理、アクセス状況の監視、不要なサービスの停止等を行う。

⑤　外部通信ネットワークを利用し、本組合以外のものと通信（電子メールの利用又はWebサイトによる情報提供等を行う場合を除く。）するときは、原則として重要性分類Ⅱ以上のデータは取り扱ってはならない。業務上、重要性分類Ⅱ以上のデータの取扱いが特に必要なときは、情報の漏えい、改ざん等を防止するため、あらかじめ個人情報保護法等その他の関連する法令等に基づき対処するとともに、通信先との相互認証、データの暗号化、セキュリティの高い通信回線を利用する等の対策を実施する。また、その際、使用する暗号鍵については厳重に管理する。

Webサイトを利用した情報提供等においても、原則として個人情報を取り扱ってはならない。なお、グループウェアについても上記の取扱いに準じる。

⑥　課情報セキュリティ責任者は、接続した外部通信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恐れがある場合には、ＩＴ管理者と協議のうえ、速やかに当該外部通信ネットワークとの接続を物理的に遮断しなければならない。

⑦　課情報セキュリティ責任者は、所管する情報システム等への不正アクセスによる攻撃を発見したときは速やかに接続を遮断し、影響範囲及び侵入経路等の調査並びに攻撃の記録を保存する。

また、個人情報の漏えい等重大なセキュリティインシデントが発生した場合には、警察及び関係機関と緊密に連携し、被害の拡大を防止する。

⑧　課情報セキュリティ責任者は、攻撃の予告等により攻撃を受けることが明確になった場合は、所管する情報システム等の停止を含む防衛策を実施する一方、関係機関と連絡を密にして情報の収集に努める。

また、職員による不正アクセスに対しても同様の措置を実施する。

(3) コンピュータウイルス対策

① 課情報セキュリティ責任者は、外部の通信ネットワークから受信したファイルについてはウイルスチェックを行い、所管する情報システム等への感染を防止するとともに、外部の通信ネットワークへ送信するファイルについてもウイルスチェックを行い、ウイルスの拡散を防止する。

② 課情報セキュリティ責任者は、サーバ及び端末機にはウイルスチェック用のソフトウェアを常駐させ、ウイルスチェック用のソフトウェアによるフルチェックを定期的に実施する。

③ 課情報セキュリティ責任者は、不正プログラム対策ソフトウェアのパターンファイルを常に最新版に更新するとともに、業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したものを利用しない。

④ 職員は、外部からデータ又はソフトウェアを取り入れる場合には必ずウイルスチェックを行い、添付ファイルのあるメールを送受信するときは、添付ファイルにウイルスが感染していないかどうか確認するとともに、差出人が不明又は不自然に添付されたファイルは開かず速やかに削除し、許可された記録媒体以外は使用しない。

⑤ 職員は、ウイルスの感染を発見したときは、端末機等を即時に情報システム等から物理的に取り外し、課情報セキュリティ責任者に報告する。

⑥ 課情報セキュリティ責任者は、職員からウイルス感染の報告を受けたときは、影響範囲及び感染経路等を調査するとともに、速やかにウイルス駆除等の対策を実施する。

12 運用

(1) 情報システムの開発、導入、保守

① 情報システムの開発

ア 課情報セキュリティ責任者は、所管する事務を処理するために情報システムを開発しようとするときは、ＩＴ管理者と協議のうえ、リスク分析を行うとともに、事故、障害等による被害の発生を防止する､若しくは最小限に抑えるため次の事項に留意する。

(ｱ) 情報システムの運転状況を監視する機能を備えるとともに障害検知機能を備えること。

(ｲ) 障害箇所を特定するため、ロギング情報（処理及び操作の記録情報）が取得できること。

(ｳ) 必要に応じて故障箇所を閉塞し縮退運転ができること。

(ｴ) 必要に応じてサーバ、ディスク装置等主要機器の代替機器を備え、障害時に代替機器への切替が容易に行えること。

(ｵ) 本番の運用環境と開発、保守環境とは別に分けること。

(ｶ) 本番のデータ及びプログラムとテスト用のデータ及びプログラムは別に管理すること。

(ｷ) データ及び情報システムのバックアップが容易に行えること。

(ｸ) データ入力時のエラーチェックを行えること。

(ｹ) 情報システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除すること。

(ｺ) 情報システム開発の責任者及び作業者のアクセス権限を設定すること。

イ 課情報セキュリティ責任者は、情報システムの維持管理に必要な各種ドキュメントを整備し、保管場所を定め厳重に保管する。

② 情報システムの導入

課情報セキュリティ責任者は、情報システムを導入する前に、十分なテストを行い、不具合の発見及び解消に努める。

また、通信ネットワークを利用した情報システムを導入しようとするとき、あるいは庁内情報ネットワーク上に情報システムを構築しようとするときは、ＩＴ管理者と協議のうえ接続テストを行う。

③　外部委託における措置

課情報セキュリティ責任者は、情報システム等の開発又は運用、保守業務の全部又は一部を事業者に委託しようとする場合又は事業者の再委託を許可する場合は、事業者において情報セキュリティ対策が確実に実施されるよう、次の点に留意する。

ア　調整・管理機能、スケジュール等業務全体の遂行を左右する重要な要件や機能を本組合のコントロール下におくこと。

イ　情報システム等のブラックボックス化を防止するため定期的に報告会議等を開催すること。

ウ　情報システム等の開発、運用等において複数の事業者が関わる場合は、その分担範囲・責任範囲を明確にするとともに、それらの連携を確保すること。

エ　情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定すること。

オ　クラウドサービスを利用する場合は、データの重要性分類に応じたセキュリティレベルが確保されているサービスを利用すること。

カ　委託処理においては、次の事項を委託契約書若しくは協定書に明記し、事業者にその内容を遵守させること。

(ｱ)　ポリシー及び実施手順の遵守
(ｲ)　事業者の責任者、委託内容、作業者、作業場所
(ｳ)　提供されるサービスレベルの保証
(ｴ)　事業者にアクセスを許可する情報の種類と範囲、アクセス方法
(ｵ)　事業者の従業員に対する教育の実施
(ｶ)　提供された情報の目的外利用及び受託者以外の者への提供の禁止
(ｷ)　業務上知り得た情報の守秘義務
(ｸ)　再委託に関する制限事項の遵守
(ｹ)　委託業務終了時の情報資産の返還、廃棄等
(ｺ)　委託業務の定期報告及び緊急時報告義務
(ｻ)　本組合による監査、検査
(ｼ)　本組合によるセキュリティインシデント発生時の公表
(ｽ)　ポリシーが遵守されなかった場合の規定(損害賠償等)

キ　委託先となる事業者について委託内容に応じた情報セキュリティ対策が確保されていることを定期的に確認し、その内容を統括情報セキュリティ責任者に報告すること。

ク　重要な情報を処理する場合等には、本組合職員が処理に立ち会うこと。

ケ　契約で定められた資格を有する者が作業に従事していることを確認し、作業を行う者のユーザＩＤ、パスワード等について、作業終了後、不要となった時点で速やかに抹消されていることを確認すること。

④　情報システム等の保守

ア　課情報セキュリティ責任者は、所管する情報システム等の保守を行うときは、運用上の不具合を確認是正するとともに、情報システム等の運用に影響を及ぼさないよう実施する。

イ　課情報セキュリティ責任者は、所管する情報システム等の追加、変更、廃止等をしたときは、その履歴を記録するとともに、ドキュメントを変更整備する。

ウ　課情報セキュリティ責任者は、機器の保守点検を定期的に実施するとともに、その記録を保存する。

エ　課情報セキュリティ責任者は、記録媒体の含まれる機器について、修理を委託する場合は、当該機器に記録されている内容が消去された状態で行わせる。ただし、情報を消去することが難しいときは、守秘義務の厳守を契約に定めなければならない。

オ　課情報セキュリティ責任者は、記録媒体の含まれる機器を廃棄、リース返却等をする場合は、当該機器に記録されている全ての情報を消去し、復元不可能な状態にする。

(2) 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及び修正

ＩＴ管理者及び課情報セキュリティ責任者は、情報セキュリティに関する最新の情報を収集し、課情報セキュリティ責任者は、所管する情報システム等のサーバ及び端末機のソフトウェアに最新のプログラム修正を適用する。

② セキュリティ侵害の対策

ＩＴ管理者及び課情報セキュリティ責任者は、情報セキュリティに関する最新の情報を収集し、関係者間で共有する。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、速やかにセキュリティ侵害を未然に防止するための対策を検討、実施する。

③ ウイルス対策の周知・徹底

ＩＴ管理者及び課情報セキュリティ責任者は、常時ウイルスに関する情報を収集するとともに、ウイルス対策について職員に啓発を行う。

(3) 情報システム等の運用管理

① 運用管理手法、運用計画

課情報セキュリティ責任者は、所管する情報システム等の運用を開始する際は、運用管理手法及び体制等について定めるとともに、運用計画を策定し、年間・月間・週間等における運用スケジュール及び情報システム等の運用時間及び運用形態等運用管理に必要な事項を職員に周知する。

② 機器操作

ア　課情報セキュリティ責任者は、所管する情報システム等のサーバ及び端末機等について操作マニュアル等を作成し、機器の操作研修を実施する。また、情報システム等の追加、変更、廃止等をしたときは、その履歴を記録するとともに、操作マニュアル等を常に最新の状態に保つ。

イ　課情報セキュリティ責任者は、所管する情報システム等のオペレーション作業に関し次の事項について定め、適切な運用管理を行う。

(ｱ) スケジュール

(ｲ) 出力及び廃棄帳票の取扱い

(ｳ) 磁気テープ等記録媒体の取扱い

(ｴ) 専用室がある場合はその入退室方法

(ｵ) オペレーション作業の範囲、内容

(ｶ) 障害時の対応

(ｷ) その他必要な事項

③ データ等のバックアップ

課情報セキュリティ責任者は、万一の事故や障害等の発生に備え、バックアップコピーを取得するデータの範囲、取得の方法及びサイクルを定め、定期的にデータやプログラムのバックアップを取得する。

なお、プログラムを変更する場合はその都度プログラムのバックアップコピーを取得し、データのバックアップとは別に、バックアップ間の差分ファイルとしてデータベースの更新記録情報を取得する。

(4) 情報システム等の監視及び予防措置

① 課情報セキュリティ責任者は、常に所管する情報システム等の稼働監視を行い、特に、外部と接続する情報システム等については、ファイアウォール、侵入監視装置等を用い、不正なアクセスによる攻撃を受けていないかどうか監視、分析を行う。

② 課情報セキュリティ責任者は、常時監視により得られた結果については、消去や改ざんを防止したうえ、定期的に保管する。

③ 課情報セキュリティ責任者は、重要なログ等を取得するサーバについては、正確な時刻設定及びサーバ間の時刻同期ができるよう構成する。

④ 課情報セキュリティ責任者は、所管する情報システム等に障害又は侵害が発生し、当該情報システム等が利用できない場合に備え、代替処理方法を定めておくとともに、被害が生じるおそれがある事案を発見した場合、速やかに予防措置を実施する。また、直ちに統括情報セキュリティ責任者に報告する。

⑤ 統括情報セキュリティ責任者は、情報システム等に被害が生じるおそれがある事案について、課情報セキュリティ責任者から報告を受けたときは、ＩＴ管理者を通じ当該事案を他の課情報セキュリティ責任者に周知する。

(5) 情報システム等の障害時、侵害時の対応

① 障害時の対応

ア 課情報セキュリティ責任者は、所管する情報システム等に係る障害時の対応マニュアルを作成し、職員に周知する。

イ 職員は、障害を発見したときは、直ちに、課情報セキュリティ責任者に連絡し、課情報セキュリティ責任者は、直ちに障害状況及び影響範囲を調査するとともに、障害状況等を統括情報セキュリティ責任者に報告する。

ウ 統括情報セキュリティ責任者は、障害状況等の報告を受けたときは、その障害状況等をＩＴ管理者に連絡し、ＩＴ管理者はこれを障害に関係する課の課情報セキュリティ責任者に連絡する。

エ 課情報セキュリティ責任者は、ＩＴ管理者と連携し、所管するシステムの回復に向け適切な措置を講じる。

オ 課情報セキュリティ責任者は、障害の原因及び情報システム等を回復するために実施した処理内容を統括情報セキュリティ責任者に報告するとともに、障害記録を作成する。

② 侵害時の対応

ア 課情報セキュリティ責任者は、所管する情報システム等において、不正行為等による情報の漏えい、滅失、改ざん等の侵害事案が発生した場合、連絡、証拠保全、被害拡大の防止、復旧等を迅速に実施するとともに、ＩＴ管理者と協議のうえ再発防止策を実施する。また、統括情報セキュリティ責任者は、対応が円滑に実施されるよう、課情報セキュリティ責任者を監督、指導する。

イ 職員は、侵害事案の発生を発見したときは直ちに課情報セキュリティ責任者に報告し、課情報セキュリティ責任者は統括情報セキュリティ責任者に報告するとともに、ＩＴ管理者に連絡する。

ウ 課情報セキュリティ責任者は、侵害事案が法令等に違反するものと見込まれる場合、統括情報セキュリティ責任者と協議し、警察等関係機関に通報する。

エ 統括情報セキュリティ責任者は、侵害事案がサイバー攻撃等による緊急時の場合においては、ＩＴ管理者を通じ全職員間での情報共有を図り、情報セキュリティ対策が迅速に実施されるよう、監督、指導する。

オ 侵害を発見した者又は侵害の報告を受けた者は、当該侵害事案を報告すべき者が不在その他の事情により報告ができない場合で急を要するときは、報告すべき者の上席者に報告する。

カ 課情報セキュリティ責任者は、侵害事案に関し、その内容、原因、確認された被害及び影響範囲について調査し、記録を作成する。

キ　課情報セキュリティ責任者は、情報システム等の運用に著しい支障をきたす攻撃が継続し、コンピュータウイルス等不正プログラムによる情報資産への深刻な被害が発生している影響で、情報資産保護のために所管する情報システム等の停止がやむを得ないと判断したときは、ＩＴ管理者と協議のうえ情報システム等を停止する。ただし、情報資産を保護するため急を要する場合には、協議前に情報システム等を停止することができる。

ク　課情報セキュリティ責任者は、侵害事案に係る情報システム等のアクセス記録等事案に係る証拠保全を確実に行うとともに、再発防止の暫定措置が完了した後、情報システム等の復旧を行う。

ケ　ＩＴ管理者は、上記の対処に当たり、課情報セキュリティ責任者と連携し、作業の実施に関し助言と調整を行う。

③　再発防止

課情報セキュリティ責任者は、障害及び侵害事案に係る原因及びリスク等を分析し、ＩＴ管理者と協議のうえ再発防止に向け改善対策を検討、実施し、その内容を統括情報セキュリティ責任者に報告する。また、再発防止に向け、職員に対し対応方法について周知する。

(6) 例外措置

①　課情報セキュリティ責任者は、ポリシー等を遵守することが困難な状況で、行政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ときは、統括情報セキュリティ責任者の許可を受けて例外措置を取ることができる。

②　課情報セキュリティ責任者は、行政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、統括情報セキュリティ責任者の許可を得る前に例外措置を取ることができる。ただし、事後直ちに統括情報セキュリティ責任者に報告しなければならない。

13　遵守状況の確認

(1) 課情報セキュリティ責任者は、ポリシー及び実施手順の遵守状況について定期的に確認し、統括情報セキュリティ責任者に報告する。

(2) 課情報セキュリティ責任者は、不正アクセス、不正プログラム等の調査のために、職員が使用している端末機及び記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(3) 課情報セキュリティ責任者は、職員の行動がポリシーに違反していると確認した場合は、速やかに改善するよう指導する。

指導によっても改善されない場合、課情報セキュリティ責任者は、当該職員が情報システム等を使用する権利を停止あるいは剥奪する。

14　点検・評価及び見直し

(1) 課情報セキュリティ責任者は、所管する情報システム等に関し、情報セキュリティ対策の実施状況全般について、定期的に点検を行い、情報セキュリティ対策の改善に努めなければならない。また、点検結果において、対策基準を改定する要を認めたときは、統括情報セキュリティ責任者に報告する。

(2) 職員は、自己に与えられた権限の範囲内で改善に努めなければならない。

(3) 統括情報セキュリティ責任者は、管理規程に定める情報セキュリティ検査の指摘事項が、被検査部門以外にも同様に影響すると認められるときは、被検査部門以外の課情報セキュリティ責任者に対しても同様の改善を求めなければならない。

(4) 統括情報セキュリティ責任者は、情報セキュリティをめぐる情勢の変化及び情報セキュリティ検査の結果を踏まえ、適宜対策基準の実効性を評価し、その見直し、改善に努めなければならない。

(5) 統括情報セキュリティ責任者は、対策基準を改定したときは、速やかに課情報セキュリティ責任者に周知しなければならない。

(6) 課情報セキュリティ責任者は、対策基準が改定されたときは、速やかに職員に周知しなければならない。

附　則

この対策基準は、平成 31 年 3 月 1 日より施行する。

附　則

この対策基準は、令和元年 10 月 1 日より施行する。

附　則

この対策基準は、令和５年４月１日より施行する。