大阪広域環境施設組合情報セキュリティ対策基準

1　目的

この対策基準は、大阪広域環境施設組合情報セキュリティ基本方針（令和８年達第２号。以下「基本方針」という。）第８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。

2　用語

この対策基準において使用する用語は、基本方針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。

⑴　職員　大阪広域環境施設組合職員基本条例（平成27年条例第16号）第２条に規定する職員をいう。

⑵　端末機　職員が業務上使用するパソコンやタブレット等の機器をいう。

⑶　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。

⑷　標的型攻撃　明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

⑸　電磁的記録媒体　本組合が業務上の必要のため調達したＵＳＢメモリ、光学メディア、外付けハードディスク等の電磁的方式で作られた記録に係る記録媒体をいう。

⑹　アクセス権限　情報システムを利用する職員が、データ及びプログラムを利用できる権限をいう。

３　体制及び役割

基本方針第６条及び第７条に基づき、情報セキュリティ対策を円滑に推進するための体制及び役割を次のとおり定める。

⑴　統括情報セキュリティ責任者

統括情報セキュリティ責任者は、以下の必要な措置を行う。

ア　課情報セキュリティ責任者、ＩＴ管理者に対する情報セキュリティに関する指導及び助言

イ　本組合の情報資産に対するセキュリティインシデントが発生した場合又はセキュリティインシデントのおそれがある場合の必要かつ十分な措置

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

エ　緊急時の回復のための対策

オ　情報セキュリティ関係規程に係る課題及び問題点を含む運用状況の適時把握

カ　職員に対する情報セキュリティポリシー（以下「ポリシー」という。）の遵守に関する指導、助言及び研修その他本組合における情報セキュリティの確保のために必要な措置

⑵　課情報セキュリティ責任者

課情報セキュリティ責任者は、基本方針第７条第３項の規定に基づき、以下の必要な措置を行う。

ア　職員に対するポリシーの遵守に関する指導、助言又は研修その他情報セキュリティの確保のために必要な措置

イ　所管する情報システムに係る情報セキュリティ実施手順（以下「実施手順」という。）の作成及び維持管理

ウ　所管する情報システムの運用開始時における、ハードウェア及びソフトウェアの運用管理の方法等の決定

エ　所管する情報システムの運用において、入力資料の作成から、電子計

算機処理、帳票の出力等に至る業務全体の実施状況の把握及び管理

オ　所管する情報システムの利用者が、アクセス権限及び実施手順等に基づき、安全性に十分配慮した適切な利用を行うための端末機の運用管理

⑶　ＩＴ管理者

ＩＴ管理者は、基本方針第６条第３項に定める責務のほか、本組合における情報資産の管理、障害に関する連絡調整を行う。

4　情報資産の分類と管理

課情報セキュリティ責任者は、以下の情報セキュリティ対策を行わなければならない。

⑴　データの分類

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職員のみが扱うデータ

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

⑵　情報資産に関する責任及び重要性の効力

ア　管理責任

課情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。

イ　利用者の責任

情報資産を業務上利用する職員は、適切に利用する責任を有する。

ウ　重要性の効力

課情報セキュリティ責任者は、データ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⑴の分類に基づき管理しなければならない。

⑶　クラウドサービスの環境に保存される情報資産

課情報セキュリティ責任者は、クラウドサービスの環境に保存される情報資産についても⑴の分類に基づき管理しなければならない。

⑷　データの作成

ア　職員は、業務上必要のないデータを作成してはならない。

イ　データは、データの作成時に⑴の分類に基づき、当該データの重要性分類を定めなければならない。

ウ　データは、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わなければならない。また、作成途上で不要になった場合は速やかに消去しなければならない。

⑸　データの入手

ア　他の課が作成したデータは、入手元の重要性分類に基づいた取扱いをしなければならない。

イ　外部の者が作成したデータは、⑴の分類に基づき、当該データの重要性分類を定めなければならない。

ウ　入手したデータの重要性分類が不明な場合、課情報セキュリティ責任者に判断を仰がなければならない。

⑹　データの管理

ア　課情報セキュリティ責任者は、データの取扱いに当たっては、漏えい、滅失、き損、改ざん、不正な利用及び不正な提供等を防止するなど、適切に管理しなければならない。

イ　データの管理の方法その他必要な事項は、統括情報セキュリティ責任

者が定める。

⑺　情報資産の利用

ア　情報資産は、業務以外の目的に利用してはならない。

イ　情報資産は、電磁的記録媒体、ドキュメント等に記録されたデータの重要性分類に応じ、適正な取扱いをしなければならない。

ウ　電磁的記録媒体に重要性分類が異なるデータが複数記録されている場合、最高度の重要性分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑻　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）、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。）並びに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ために必要な措置を講じなければならない。

イ　外部に公開するデータについては完全性を確保しなければならない。

ウ　特定個人情報を取り扱う場合は、インターネットから切り離された環境で取り扱わなければならない。

⑼　データの送信

ア　本組合以外の外部に、電子メール等により重要性分類Ⅱ以上のデータを送信する場合は、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。

イ　重要性分類Ⅱ以上のデータをメールにより取り扱う必要がある場合は、課情報セキュリティ責任者の承認を得るとともに、送信先のメールアドレス及びメール受取の確認を行う等、厳格に取り扱わなければならない。なお、組合内においてメールを利用するときであっても、上記の取扱いに準じ、適切に運用を行わなければならない。

⑽　電磁的記録媒体等の管理

ア　課情報セキュリティ責任者は、データを記録した電磁的記録媒体を長期保管する場合は、必要に応じて書込禁止の措置を講じなければならない。

イ　課情報セキュリティ責任者は、データの重要性が容易に識別できるよう、ファイルが格納された電磁的記録媒体等の保管について台帳整備し、所定の場所において適切に管理しなければならない。また、ファイルのバックアップを定期的に取得するよう努め、所定の場所において適切に管理しなければならない。

⑾　データの運搬

ア　重要性分類Ⅱ以上のデータが格納された電磁的記録媒体等を庁外へ持ち出す場合は、必要に応じ鍵付きのケース等に格納し、データには暗号化又はパスワード設定を行う等、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　課情報セキュリティ責任者は、データが格納された電磁的記録媒体等の授受に関しては、台帳等を整備しなければならない。また、電磁的記録媒体等を搬送するときは、常時携行するなど自己の管理下に置き、あるいは専用トランクを使用する等データの漏えい、滅失、き損、改ざん等を防止するために適切な措置を講じなければならない。

⑿　情報資産の廃棄等

ア　情報資産を廃棄する場合は、データ消去その他の適切な措置を講じなければならない。特に、保護データについては、情報を復元できないよう確実に消去しなければならない。

イ　情報資産を廃棄する場合は、行った処理について、日時、担当者、処理内容等その他必要な事項を記録しなければならない。

ウ　ファイルが格納された電磁的記録媒体等の廃棄を行う場合は、課情報セキュリティ責任者の許可を得なければならない。

エ　クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

5　物理的セキュリティ

⑴　端末機

ア　課情報セキュリティ責任者は、情報資産を保管する執務室等においては、職員が不在時の盗難防止のため、職員が使用する端末機について、ワイヤーによる固定や執務室等の施錠等の物理的措置を講じなければならない。

イ　課情報セキュリティ責任者は、電磁的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、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。

ウ　課情報セキュリティ責任者は、磁気ディスクその他電磁的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を速やかに消去するなど、適正に運用しなければならない。

⑵　接続機器等

ア　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が設置状況を把握できるような場所に設置しなければならない。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しなければならない。

イ　通信ネットワークシステムにて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しなければならない。

ウ　情報システムを構築するにあたり、有線による情報システムの整備が適さない合理的な理由がある場合には、解読が困難な暗号化及び認証技術を用いることで、無線回線による整備を行うことができる。

6　人的セキュリティ

⑴　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。

⑵　教育及び研修

ア　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教育及び研修方針を策定する。

イ　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。

⑶　標的型攻撃対応訓練

統括情報セキュリティ責任者は、標的型攻撃への対応を想定した訓練を実施しなければならない。訓練計画は、情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

⑷　研修、訓練への参加

職員は、定められた研修、訓練に参加しなければならない。

⑸　業務目的以外の利用禁止

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。

⑹　情報漏えい等の防止

ア　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電磁的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。

イ　職員は、業務用として貸与されたもの以外の端末機及び電磁的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ない。

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

エ　職員は、使用する端末機や電磁的記録媒体について、本来の用途や目的ではない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。

オ　課情報セキュリティ責任者は、端末機及び電磁的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。

カ　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。

キ　職員は、クラウドサービスの利用にあたってもポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

ク　職員は、自動転送機能を用いて、外部へ電子メールを転送してはならない。ただし業務遂行上やむを得ない場合は課情報セキュリティ責任者の許可を得て行うことができる。

ケ　職員は、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。

コ　職員は、複数人に電子メールを送信する場合、必要があるときを除き、他の送信先の電子メールアドレスが判明しないようにしなければならない。

サ　職員は、重要な電子メールを誤送信した場合、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。

シ　職員は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

⑺　ソフトウェアライセンスの管理

ア　課情報セキュリティ責任者は、その所管する情報システムにおいて使用するソフトウェアのライセンス（当該ソフトウェアに係る使用許諾契約により認められた当該ソフトウェアを使用する権利をいう。以下「ソフトウェアライセンス」という。）を適切に管理しなければならない。

イ　課情報セキュリティ責任者は、ソフトウェアライセンスの管理状況を適宜調査し、その内容を定期的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。

ウ　統括情報セキュリティ責任者は、前項の規定による報告を受けた場合において、必要があると認めるときは、必要な措置が適切に講じられるよう指導及び監督を行なわなければならない。

エ　ソフトウェアライセンスの管理の方法その他必要な事項は、統括情報セキュリティ責任者が定める。

⑻　無許可ソフトウェアの導入等の禁止

ア　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。

イ　職員は、著作権法（昭和45年法律第48号）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。

⑼　セキュリティインシデントに対する対応

ア　課情報セキュリティ責任者は、その所管に係る情報資産に漏えい、滅失、き損、改ざん等の事故が発生したとき又は次項の規定に基づくＩＴ管理者からの報告があったときは、直ちに、必要な措置を講ずるとともに、当該事故の内容及び講じた措置を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。

イ　ＩＴ管理者は、本組合が所有する情報資産に漏えい、滅失、き損、改ざん等の事故が発生したことを検知したときは、直ちに、その状況を調査するとともに、当該情報資産を所管する課情報セキュリティ責任者に報告しなければならない。

ウ　統括情報セキュリティ責任者は、アの規定による報告を受けたときは、再発防止のために必要な措置が適切に講じられるよう指導及び監督を行わなければならない。

エ　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。

オ　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した場合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。

カ　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。

⑽　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を利用する場合も、共用ＩＤの利用者以外に利用させてはならない。

⑾　パスワードの管理

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。

イ　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間及び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。

⑿　Ｗｅｂ会議サービスの利用時の対策

ア　統括情報セキュリティ責任者は、Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。

イ　職員は、統括情報セキュリティ責任者の定める利用手順に従い、Ｗｅｂ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

ウ　職員は、Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

⒀　ソーシャルメディアサービスの利用

ア　統括情報セキュリティ責任者は、本組合が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

イ　本組合のアカウントによる情報発信が、実際に本組合のものであることを明らかにするために、本組合の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

ウ　パスワードや認証のためのコード等の認証情報を適正に管理するなどの方法で、不正アクセス対策を実施すること。

エ　重要性分類Ⅱ以上のデータはソーシャルメディアサービスで発信してはならない。ただし、人の身体生命に危険が及ぶ可能性が高い場合など、緊急性を要する場合を除く。

オ　統括情報セキュリティ責任者は、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なければならない。

カ　統括情報セキュリティ責任者は、アカウント乗っ取りを確認した場合は、被害を最小限にするための措置を講じなければならない。

キ　可用性が求められる情報の提供にソーシャルメディアサービスを用いる場合は、本組合の自己管理Ｗｅｂサイトに当該情報を掲載して参照可能としなければならない。

ク　Ｗｅｂサイトを利用した情報提供等においては、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。

7　技術的セキュリティ

⑴　アクセス制御

ア　アクセス権限の設定

課情報セキュリティ責任者は、所管する情報システム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明確にし、設定しなければならない。

イ　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しなければならない。

（イ）　課情報セキュリティ責任者は、所管する情報システムのユーザ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、職員に周知しなければならない。

（ウ）　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とともに、業務上必要がなくなった場合は、利用者登録を抹消しなければならない。

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しなければならない。

⑵　不正アクセス対策

ア　課情報セキュリティ責任者は、所管する情報システム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しなければならない。

イ　課情報セキュリティ責任者は、所管する情報システムへの不正アクセスによる攻撃を発見した場合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結果並びに攻撃の記録を保存しなければならない。

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ときは、警察及び関係機関と緊密に連携し、被害の拡大を防止しなければならない。

ウ　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なければならない。

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。

エ　統括情報セキュリティ責任者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。

⑶　コンピュータウイルス対策

ア　課情報セキュリティ責任者は、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しなければならない。

イ　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てはならない。

ウ　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、許可された電磁的記録媒体以外は使用してはならない。

エ　職員は、端末機において、不正プログラム対策ソフトウェアの設定を変更してはならない。

オ　職員は、ウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、端末機を即時に情報システム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しなければならない。

カ　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場合は、影響範囲及び感染経路等を調査するとともに、速やかに統括情報セキュリティ責任者に報告し、ウイルス感染拡大の防止に努めなければならない。

8　運用

⑴　情報システムの適正運用

ア　実施手順の作成

課情報セキュリティ責任者は、ポリシーに基づき、当該システムにおける情報セキュリティ対策の実施に関し必要となる事項を定めた実施手順を作成し、統括情報セキュリティ責任者の承認を得なければならない。

イ　情報システムの導入

課情報セキュリティ責任者は、情報システムの導入、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。

また、通信ネットワークシステム上に情報システムを構築しようとする場合は、ＩＴ管理者と協議のうえ接続テストを行わなければならない。

ウ　外部委託における措置

課情報セキュリティ責任者は、電子計算機処理業務や情報システムの整備又は運用、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、次の点に留意しなければならない。

（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）　情報システムの整備、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。

① ポリシー及び実施手順の遵守

② 事業者の責任者、委託内容、作業者、作業場所

③ 提供されるサービスレベルの保証

④ 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

⑤ 事業者の従業員に対する教育の実施

⑥ 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

⑦ 業務上知り得た情報の守秘義務

⑧ 再委託に関する制限事項の遵守

⑨ 委託業務終了時の情報資産の返還、廃棄等

⑩ 委託業務の定期報告及び緊急時報告義務

⑪ 本組合による監査、検査

⑫ 本組合によるセキュリティインシデント発生時の公表

⑬ ポリシーが遵守されなかった場合の規定（損害賠償等）

エ 情報システムにおける機器操作の適正化

（ア） 情報資産については、職員　以外が操作してはならない。ただし、メンテナンス等で職員以外が操作する場合は、この限りでない。

（イ） 課情報セキュリティ責任者は、電磁的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なければならない。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。

（ウ） 課情報セキュリティ責任者は、電磁的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しなければならない。

⑵ セキュリティ情報の収集

ア 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。

イ 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。

⑶ 情報システムの運用管理

ア 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、情報システム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しなければならない。

イ 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の端末機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しなければならない。また、情報システムの追加、変更、廃止等をしたときは、操作マニュアル等を常に最新の状態に保たなければならない。

（イ） 課情報セキュリティ責任者は、所管する情報システム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わなければならない。

① スケジュール

② 出力及び廃棄帳票の取扱い

③　電磁的記録媒体の取扱い

④　専用室がある場合はその入退室方法

⑤　オペレーション作業の範囲、内容

⑥　障害時の対応

⑦　その他必要な事項

ウ　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、定期的バックアップを取得しなければならない。

⑷　情報システムの障害時、侵害時の対応

ア　障害時の対応

（ア）　職員は、障害を発見した場合は、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しなければならない。

（イ）　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場合は、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しなければならない。

イ　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しなければならない。

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、指導しなければならない。

（イ）　職員は、侵害事案の発生を発見した場合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管理者に連絡しなければならない。

（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、指導しなければならない。

（オ） 侵害を発見した職員は、課情報セキュリティ責任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、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。

（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、記録を作成しなければならない。

（キ） 課情報セキュリティ責任者は、情報システム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の停止がやむを得ないと判断した場合は、ＩＴ管理者と協議のうえ情報システムを停止しなければならない。ただし、情報資産を保護するため急を要するときは、協議前に情報システム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。

ウ　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しなければならない。

⑸　例外措置

ア　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場合は、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。

イ　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。

9　情報セキュリティ検査の実施

⑴　統括情報セキュリティ責任者は、本組合においてポリシーが遵守され、情報セキュリティ対策が適切かつ確実に実施されているかどうかを検証するため、定期的に検査を実施しなければならない。

⑵　統括情報セキュリティ責任者は、前項に規定する検査のほか、必要と認めるときは随時に検査を行うことができる。

⑶　統括情報セキュリティ責任者は、前２項に規定する検査（以下「情報セキュリティ検査」という。）の結果に基づき、必要があると認めるとき

は、講ずべき改善措置の内容を定めなければならない。

⑷　課情報セキュリティ責任者は、前項の規定により統括情報セキュリティ責任者が定める改善措置を適切かつ確実に実施しなければならない。

⑸　情報セキュリティ検査の実施方法その他必要な事項は、統括情報セキュリティ責任者が定める。

10　遵守状況の確認

⑴　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しなければならない。

⑵　ＩＴ管理者は、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電磁的記録媒体等のログ、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。

⑶　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しなければならない。指導によっても改善されないときは、課情報セキュリティ責任者は、当該職員が情報システムを使用する権利を停止あるいは剥奪しなければならない。

⑷　ポリシーに違反した職員及びその監督責任者は、その重大性、発生した事象の状況等に応じて、地方公務員法（昭和25年法律第261号）及び大阪広域環境施設組合職員基本条例に基づき懲戒処分の対象となる場合がある。

11　点検・評価及び見直し

⑴　課情報セキュリティ責任者は、所管する情報システムに関し、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必要を認めた場合は、統括情報セキュリティ責任者に報告する。

⑵　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。

⑶　統括情報セキュリティ責任者は、基本方針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場合は、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。

⑷　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。

⑸　統括情報セキュリティ責任者は、対策基準を改定した場合は、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。

⑹　課情報セキュリティ責任者は、対策基準が改定された場合は、速やかに職員に周知しなければならない。

附　則

1　この対策基準は、令和８年４月１日から施行する。

2　大阪広域環境施設組合情報セキュリティ対策基準（平成31年３月１日施行）は、廃止する。