広島市情報セキュリティポリシーの要点

1　情報資産セキュリティ

(1)　本市の情報資産は、重要性により、次のとおり分類する。(P10-1)

ア　重要性分類Ⅰ

広島市情報公開条例（平成１３年広島市条例第６号）第7条各号に掲げる情報資産

イ　重要性分類Ⅱ

広島市情報公開条例第7条各号に掲げる情報資産に該当しないもの（重要性分類Ⅲに該当するものを除く。）

ウ　重要性分類Ⅲ

ホームページ、出版物等に掲載している情報資産

(2)　管理責任者は、職員が情報資産を作成又は入手した場合は、上記分類により情報資産を分類し、次の区分に従い、それぞれに定める事項を記載した管理台帳を作成すること。重要性分類を変更した場合、変更後の重要性分類に従った管理台帳を作成すること。(P11-2-(1)-イ)

ア　重要性分類Ⅰ

(ｱ)　管理責任者

(ｲ)　保管場所

(ｳ)　電磁的記録媒体

(ｴ)　利用範囲

(ｵ)　庁外への送付、持出及び貸与の記録

イ　重要性分類Ⅱ

(ｱ)　管理責任者

(ｲ)　保管場所

(ｳ)　電磁的記録媒体

(ｴ)　利用範囲

(3)　情報資産を保管する者は、情報資産の分類に応じ、次のとおり取り扱うこと。(P12-ウ-(ｳ))

ア　重要性分類Ⅰ

(ｱ)　電磁的記録媒体に情報資産を格納する際は、暗号化又は利用者の権限に応じたアクセス制御を行うこと。

(ｲ)　可搬記録媒体は、鍵の掛かる保管庫等に保管し、その利用を管理すること。

(ｳ)　情報資産が印刷された文書は、鍵の掛かる保管庫等に保管し、その利用を管理すること。

イ　重要性分類Ⅱ

(ｱ)　可搬記録媒体は、鍵の掛かる保管庫等に保管すること。

ウ　重要性分類Ⅲ

(ｱ)　原本が格納された可搬記録媒体は、鍵の掛かる保管庫等に保管すること。

(4)　情報資産を利用する者は、情報資産の分類に応じ、次のとおり取り扱うこと。(P12-オ-(ｲ)-a)

ア　重要性分類Ⅰ

(ｱ)　庁内に情報資産を送付し、持出し、貸与、又は提供する際は、情報資産の管理責任者の許可を得ること。

(イ) 庁外に情報資産を送付し、持出し、貸与、又は提供しないこと。ただし、職務上必要がある場合において、情報資産の管理責任者の許可を得たときは、この限りでない。

(5) 情報資産の廃棄やリース返却等を行う者は、情報資産の管理責任者の許可を得ること。(P13-カ-(ウ))

(6) 情報資産の管理責任者は、情報が印刷された文書を廃棄する場合、廃棄するまでの間、第三者に閲覧されることのない場所に保管するとともに、廃棄に際しては適切な方法を講ずること。(P13-カ-(エ))

2 物理的セキュリティ

(1) 管理責任者は、職員及び外部要員（委託事業者の従業員であって、契約に基づいて本市の施設で業務に従事する者をいう。以下同じ。）に対し名前札を着用させる等、施設内にいる職員、外部要員及び訪問者を容易に区別できるようにすること。(P16-1-(1)-ウ)

(2) 管理責任者は、複写機、ファクシミリ及びプリンタを、情報漏えいの危険性を考慮して職員の目の届く場所に設置すること。(P16-1-(2)-エ)

(3) 管理責任者は、パソコン等の端末や電磁的記録媒体、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、又は情報システム利用管理者の許可なく情報を閲覧されることがないように、適切な措置を講じること。(P16-1-(2)-カ)

(4) 管理責任者は、パソコン、モバイル端末等の情報システム機器について、盗難防止のため、次のいずれかの対策を実施すること。(P19-3-(2)-ア)

ア 鍵の掛かる保管庫等への保管

イ 机上への固定

ウ 情報システム機器を設置している執務室の施錠管理

(5) 管理責任者は、サーバ、ルータ、ファイアウォール等の重要な情報システム機器については、広島市情報システムの導入等に関するガイドラインに定める基準を満たした外部のデータセンターに設置する、又はクラウドサービスを利用すること。やむを得ず庁内にこれらを設置する場合は、管理区域等の入室が制限された場所に設置し、又は施錠できるラック内に設置すること。(P19-3-(2)-イ)

(6) 管理責任者は、庁外で使用するパソコン等の情報システム機器のうち、重要性分類Ⅰの情報資産を取り扱うものについては、次のいずれかの対策を実施すること。(P19-3-(2)-エ)

ア ＢＩＯＳパスワード等による起動の制限

イ 情報資産の暗号化

(7) 管理責任者は、廃棄予定の情報システム機器を一時的に保管する場合も、施錠管理された場所で保管すること。(P20-ク)

(8) 情報システム業務管理者は、外部要員が庁内に持ち込む情報システム機器について、不正プログラム対策等の必要な情報セキュリティ対策の実施の有無について確認すること。(P20-(3)-ア)

(9) 情報システム業務管理者は、許可を与えた場合を除き、外部要員の情報システム機器を庁内のネットワークに接続させないこと。(P20-(3)-イ)

3　人的セキュリティ

(1)　職員は、個人所有の情報システム機器を原則職務で使用しないこと。また、可搬記録媒体は、公用の物を用い、個人所有の物を一切使用しないこと。(P21-1-(1)-イ-(エ))

(2)　職員は、情報システム業務管理者の許可なく、情報システム機器をネットワークに接続しないこと。(P21-1-(1)-イ-(カ))

(3)　職員は、情報システムの利用中に離席する際は、次のいずれかの対策を実施すること。(P21-1-(1)-イ-(キ))

ア　情報システムのログオフ

イ　パスワードつきのスクリーンセーバーの利用による画面の非表示

(4)　職員は、インターネットの利用に当たり、次の行為をしないこと。(P22-ウ-(ア))

ア　職務に関係のないホームページの閲覧

イ　職務に関係のないメールマガジンの購読

ウ　外部機関の情報システムへの不正アクセス

エ　ソフトウェア等のダウンロードによる著作権侵害

(5)　職員は、不正プログラム感染防止のため、不審なメールは開かずに情報システム業務管理者に報告し、その指示に従うこと。(P22-ウ-(エ))

(6)　職員は、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わからないようにすること。(P22-ウ-(カ))

(7)　職員は、個人のユーザＩＤを他人に利用させないこと。(P22-エ-(ア))

(8)　職員は、パスワードを紙等に記載しないこと。(P23-(ウ))

(9)　職員は、パスワードを他人に漏らさないこと。(P23-(エ))

(10)　職員は、パスワードが漏えいした場合又は漏えいした可能性がある場合、直ちにパスワードを変更し、情報システム業務管理者に報告すること。(P23-(オ))

(11)　職員は、パスワードの自動保存機能の使用及び情報システム機器のファンクションキーへの割り当てをしないこと。(P23-(カ))

(12)　情報システム利用管理者は、非常勤職員及び臨時職員等を雇用する際に、情報セキュリティポリシーのうち、遵守すべき内容を理解させなければならない。(P23-(2)-イ)

(13)　情報システム業務管理者は、情報システムの利用者に対し、定期的に又は情報システムの変更時等に、情報システムに関する情報セキュリティ研修を実施すること。(P24-ケ)

4　技術的セキュリティ

(1)　管理責任者は、インターネット又は外部ネットワーク（本市以外の組織等（委託事業者を含む。）が管理するインターネット以外のネットワークのことをいう。以下同じ。）と接続するサーバについて、次の対策を実施すること。(P25-1-(6))

ア　構築時における脆弱性を確認するセキュリティ診断

イ　リアルタイムの不正アクセス監視

ウ　不正プログラム侵入監視

エ　情報システムの可用性条件に応じたサーバの冗長化

オ　脆弱性を確認する定期的なセキュリティ診断

カ　不正アクセスを検知した際に、サーバ内のファイルが改ざんされていないことの確認

(2) 情報システム業務管理者は、個人情報等を取り扱う機密性の高い情報システムについて、他のネットワークと完全に切り離した独立ネットワーク又はそれに近い構成にすること。他のネットワークと接続する場合、ファイアウォール等によるアクセス制御を行うこと。(P26-2-(1)-ク)

(3) 情報システム業務管理者は、外部ネットワークと接続する場合、その正当性、接続方法及び情報セキュリティ対策が適当であることを確認すること。また、必要に応じて利用者認証機能の強化等の対策を実施すること。(P27-イ)

(4) 情報システム業務管理者は、外部ネットワークとの接続口にファイアウォール等を設置し、庁内ネットワークを保護すること。(P27-キ)

(5) 情報システム業務管理者又は情報システム機器の管理責任者は、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最新の状態に保つこと。(P32-5-(1)-エ)

(6) 情報システム業務管理者又は情報システム機器の管理責任者は、情報システム機器の電磁的記録媒体全体の不正プログラムの検査を定期的に実施すること。(P32-5-(1)-オ)

(7) 管理責任者は、ソフトウェアの管理台帳を作成し、定期的にその内容を確認すること。管理台帳には、ソフトウェアのバージョンも記載し、内容に変更があった場合、随時台帳を更新すること。(P34-6-(1)-イ)

(8) 管理責任者は、利用者に対して、情報システム機器に無許可でソフトウェアをインストールさせないこと。(P34-6-(1)-ウ)

5　調達・運用におけるセキュリティ

(1) 情報システム業務管理者又は情報システム利用管理者は、情報システムの開発、導入、改修、保守、運用、機器及びソフトウェアの調達に係る検査・検収に当たっては、複数の者により確実に行わせること。(P36-1-(2)-ア)

(2) 情報システム業務管理者は、不正アクセスの兆候を発見するため、各種ログ（アクセスログ、システム稼働ログ、障害時のシステム出力ログなど）及び障害対応記録を取得し、１年以上保存すること。(P37-2-(4)-ア)

(3) 情報システム業務管理者は、管理対象物（プログラムソース、設計書、障害報告書等）を明確にすること。(P39-3-(5)-ア)

(4) 情報システム業務管理者は、管理対象物に関わる文書又は電磁的記録媒体を庁外に送付し、又は貸与する場合、送付又は貸与先が受領したことを確認できる対策を実施すること。(P39-3-(5)-ウ)

(5) 情報システム業務管理者は、情報システムの機能及び運用手順を記載した運用マニュアルを作成すること。(P40-(8)-ア)

(6) 情報システム業務管理者は、情報システムの概要、操作手順及び利用規約を記載した利用マニュアルを作成すること。(P40-(8)-イ)

(7) 情報システム業務管理者は、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施すること。(P41-4-(3)-ウ)

(8) 情報システム業務管理者又は情報システム機器の管理責任者は、定期的に保守を実施すること。(P41-4-(4)-ア)

(9) 情報システム業務管理者は、管理権限を有する者及びその権限内容について、１年ごとに妥当性を

見直すこと。(P42-(5)-キ)

⑽　情報システム利用管理者は、情報システムの利用者情報の登録、変更及び削除について、情報システム業務管理者に申請すること。(P44-5-(1)-イ)

⑾　情報システム業務管理者は、委託等により情報システムを職員以外の者に利用させる場合、利用範囲を明確にし、情報システムの利用権限を設定すること。また、委託事業者から情報資産の取扱い等についての覚書、誓約書等を提出させること。(P44-5-(1)-ウ)

⑿　情報システム業務管理者は、利用者の登録状況を定期的に確認し、人事異動や退職によって不要になったユーザＩＤを速やかに削除すること。(P44-5-(1)-ケ)

⒀　情報システム業務管理者は、パスワードについて、ユーザＩＤと同一文字列にすること及び同一文字の繰返しを禁止し、文字の種類、最低文字数等の制限を満たしたものとすること。また、利用者に定期的に変更させること。(P44-5-(2)-オ)

⒁　情報システム業務管理者は、所管する情報システムについて、情報セキュリティ事故、システム上の欠陥及び誤作動を想定した対応手順を明確にすること。対応手順には次の事項を含めること。(P46-6-(1)-ア)

ア　庁内外の関連する機関への連絡

イ　届出機関への報告

ウ　ログ、証拠物件の収集及び保管

エ　発生原因の調査

オ　対策手段の検討

6　業務委託と外部サービスの利用

⑴　業務委託主管課長は、委託事業者及び委託事業者の従業員に対して、情報セキュリティポリシー及び情報セキュリティ実施手順に定めている事項を遵守させること。また、委託事業者の再委託を認める場合、再委託先に対しても、同等の情報セキュリティ対策を実施させること。(P49-1-(1)-イ)

7　留意点

以上の内容は、情報セキュリティについて、指定管理者が広島市と同様の安全管理措置を講じるに当たり、広島市情報セキュリティポリシーから代表的な注意点を抜粋したものです。その他、講ずべき措置の詳細については、広島市情報セキュリティポリシーを参照してください。

なお、広島市情報セキュリティポリシーにおける管理体制に係る記載は、本市組織体制を前提としたものになっていますので、指定管理者において、広島市情報セキュリティポリシーに準じた取扱いを行うに当たっては、指定管理者の組織体制に合わせて適宜読み替えてください。

また、広島市情報セキュリティポリシーは、情報システムで個人情報を取り扱う前提で記載していますが、指定管理者によっては、例えば、１台のパソコンでエクセルファイルにより個人情報を管理している場合等があると考えられます。こうした場合は、当該パソコンやエクセルファイル等を情報システムに読み替える等、指定管理者における個人情報の取扱い状況に応じて適宜読み替えてください。