大阪狭山市情報セキュリティポリシー

平成28年1月1日

大阪狭山市

（令和 6 年 4 月1日　改訂版）

序　大阪狭山市情報セキュリティポリシーの構成

大阪狭山市において取り扱う情報には、市民の個人情報や行政運営上重要な情報など、外部への漏えい等が発生した場合に極めて重大な影響を及ぼす情報が多数含まれており、これらの情報資産を適切に保護し、責任を持って管理するためには、情報セキュリティマネジメント（情報資産を適切に保護するための組織としての継続的かつ計画的な取り組みをいう。以下同じ。）が必要不可欠である。

また、個人情報の適正な取扱いという観点からは、個人情報の保護に関する法律（平成１５年法律第５７号）や大阪狭山市保有個人情報等の安全管理に関する規程（令和５年大阪狭山市規程第４号）において各種保護措置が定められているが、特定個人情報については、行政手続における特定の個人を識別する番号の利用等に関する法律（平成２５年法律第２７号）において利用範囲を限定するなど、より厳格な保護措置が定められていることから、管理体制を整備し、職員等に遵守させるための措置を講じ、適正に取り扱う必要がある。

このため、大阪狭山市は、情報セキュリティマネジメントの実現に関する体系的かつ具体的な対策等を大阪狭山市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）として定めることとする。

情報セキュリティポリシーは、本市における情報セキュリティに関する基本的な考え方を述べた「情報セキュリティ及び特定個人情報等の安全管理に関する基本方針」と、この基本方針に基づき、情報セキュリティを確保するために遵守すべき行為等の基準を示した「情報セキュリティ対策基準」及び「特定個人情報等の安全管理に関する基準」からなるものとする。

なお、情報セキュリティポリシーに基づき、情報セキュリティ対策の具体的な手順を定めた「情報セキュリティ実施手順」を個別の情報システム又は業務ごとに、また、特定個人情報等の安全管理に関して具体的な手順を定めた取扱規程等を個別の事務ごとに作成するものとする。

大阪狭山市情報セキュリティ及び特定個人情報等の安全管理に関する基本方針

平成２８年１月１日制定
平成２８年４月１日改正
令和３年４月１日改正
令和６年４月１日改正

（趣旨）

第１条　この基本方針は、本市が所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、本市が行う情報セキュリティの確保に関する対策の統一的かつ基本的な事項を定めるとともに、行政手続における特定の個人を識別する番号の利用等に関する法律（平成２５年法律第２７号。以下「番号法」という。）により個人番号及び特定個人情報（以下「特定個人情報等」という。）を取り扱う全ての事務において適正に特定個人情報等を取り扱うための基本的な事項を特に示すものとする。

（定義）

第２条　この基本方針において、使用する用語は、番号法において使用する用語の例によるほか、次に掲げる用語の意義は、当該各号に定めるところによる。

⑴　部等　大阪狭山市事務分掌条例（昭和５３年大阪狭山市条例第２３号）第１条に定める室及び部、出納室、選挙管理委員会事務局、監査委員事務局、固定資産評価審査委員会事務局、農業委員会事務局、議会事務局並びに大阪狭山市教育委員会事務局組織規則（平成９年大阪狭山市教育委員会規則第１号）第２条第１項に規定する部をいう。

⑵　職員等　市長、副市長及び教育長並びに部等の職員（非常勤職員、臨時職員を含む。）をいう。

⑶　情報　職員等が職務上作成し、又は取得したもののうち電磁的に記録された情報（電磁的に記録された情報を紙等の有体物に出力した情報を含む。）をいう。

⑷　情報システム　ハードウェア、ソフトウェア、ネットワーク、記録媒体等で構成されるものであって、これら全体で業務処理を行うもの並びにこれらの仕組みを開発、運用及び保守するために作成された資料等をいう。

⑸　ネットワーク　通信を行うために用いられる機器及び回線をいう。

⑹　情報資産　情報及び情報システムをいう。

⑺　機密性　許可された者だけが情報資産にアクセスできることを確実にすること

をいう。

⑻　完全性　情報資産が正確及び完全であることを常に維持することをいう。

⑼　可用性　許可された者が確実に情報資産を利用できることをいう。

⑽　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。

⑾　外部委託事業者　情報資産に関連する開発、導入、保守等により委託したすべての事業者等をいう。

（対象範囲）

第３条　この基本方針は、本市の情報資産（教育機関で専ら教育用に使用する情報資産を除く。以下同じ。）及び特定個人情報等並びにこれらに接する職員等を対象とする。

（情報資産への脅威）

第４条　本市の情報資産に対して想定される脅威は、次に掲げるとおりとする。

⑴　部外者による情報資産の破壊又は盗難、不正アクセス又は不正操作による情報資産の持出し、盗難、改ざん、消去等

⑵　職員等及び外部委託事業者による意図しない操作、故意の不正アクセス又は不正操作による情報資産の持出し、盗難、改ざん、消去等及び規定外の操作、接続による情報の漏えい等

⑶　コンピュータウイルス、ワーム等の悪意のあるプログラム

⑷　地震、落雷、火災等の自然災害、事故、故障等

（情報セキュリティ対策基準等の策定）

第５条　この基本方針に基づき、情報セキュリティ対策を具体的に実施するに当たっての遵守すべき事項及び統一的な判断等の基準として情報セキュリティ対策基準（以下「対策基準」という。）を策定するとともに、特定個人情報等に関する適正な取扱いのため遵守すべき事項及び整備すべき事項等を定めるものとして特定個人情報等の安全管理に関する基準を策定するものとする。

（情報セキュリティ実施手順等の策定）

第６条　この基本方針及び対策基準等（対策基準及び特定個人情報等の安全管理に関する基準をいう。以下同じ。）に基づき、個々の情報システムについて具体的な情報セキュリティ対策を講じるため、情報セキュリティ実施手順（以下「実施手順」と

いう。）を、特定個人情報等の適正な取扱いを図るため、特定個人情報等を取り扱う事務ごとに特定個人情報等に関する取扱規程等を策定するものとする。

（法令等の遵守）

第７条　職員等は、業務の遂行について、情報セキュリティ及び特定個人情報等の適正な取扱いに関する法令等を遵守しなければならない。

（職員等の責務）

第８条　職員等は、情報セキュリティ及び特定個人情報等の適正な取扱いの重要性を認識し、業務の遂行に当たっては、この基本方針及び対策基準等を遵守しなければならない。

（組織体制の整備）

第９条　本市の情報資産について、情報セキュリティ対策を推進するための組織及び体制を確立するとともに、特定個人情報等について、適正な取扱いを図るための組織及び体制を整備するものとする。

（情報資産の分類と管理）

第１０条　本市の情報資産は、その重要度に応じた分類を行い、適切に管理するものとする。

（人的セキュリティ対策）

第１１条　情報資産又は特定個人情報等に接する職員等の情報セキュリティ及び特定個人情報等の取扱いに関する役割及び責任並びに遵守すべき事項を定めるとともに、すべての職員等に情報セキュリティ対策の内容及び特定個人情報等の適正な取扱いを周知徹底するための教育及び啓発が行われるよう必要な人的対策を講じるものとする。

（物理的セキュリティ対策）

第１２条　情報システムの設置場所又は特定個人情報等を取り扱う事務を実施する区域への不正な立入り、情報資産又は特定個人情報等の盗難及び毀損からこれらを適切に保護するため、入退室管理等の物理的な対策を講じるものとする。

（技術的セキュリティ対策）

第１３条　本市の情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の必要な対策を講じるものとする。

（コンピュータウイルス対策）

第１４条　本市の情報資産をコンピュータウイルス等の悪意のあるプログラムから適切に保護するとともに、コンピュータウイルス等の感染が認められたときは、感染の拡大を防止するために必要な対策を講じるものとする。

（記録媒体の取扱い及び管理）

第１５条　本市の情報システムにおける記録媒体については、適正な管理を行うために必要な措置を講じるものとする。

（情報システムの開発、導入及び保守）

第１６条　本市の業務に使用する情報システムの開発、導入及び保守については、情報資産を適切に保護するために必要な措置を講じるものとする。

（外部委託）

第１７条　本市の情報システムの開発、導入、保守等を外部に委託する場合は、情報セキュリティに関する必要な措置を講じるものとする。

２　本市の特定個人情報等を取り扱う事務の全部又は一部を委託する場合は、委託先（再委託先を含む。）において、番号法に基づき本市が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行う。

（特定個人情報等の適正な収集・保管・利用・廃棄、目的外利用の禁止）

第１８条　特定個人情報等は、番号法に定められた事務のうち、あらかじめ本人に通知した利用目的の達成に必要な範囲内で適正に収集し、保管し、利用し、及び提供するとともに、不要となった特定個人情報等は速やかに廃棄するものとする。

２　特定個人情報等について、目的外利用を防止するための措置を講じるものとする。

（情報セキュリティ侵害時等の対応）

第１９条　情報セキュリティの侵害に関する事案が発生した場合又は特定個人情報等に関する漏えい、滅失又は毀損等の事案が発生した場合（当該事案の兆候を把握した場合も含む。）の対応をあらかじめ定め、当該事案が発生したときは、定められた対応を適切かつ迅速に実施するとともに、当該事案の再発を防止するために必要な措置を講じるものとする。

（評価及び見直し）

第２０条　情報セキュリティ対策及び特定個人情報等の取扱いに関する実施状況、結果等について、定期的に評価するとともに、新たな脅威その他情報資産及び特定個人情報等を取り巻く状況の変化を踏まえ、適宜この基本方針、対策基準等及び実施

手順等の見直しを実施するものとする。