ORDEN における情報セキュリティ対策方針

1. 本方針の目的

大阪府がその目的を果たしつつ、府民のみなさまはもとより、様々な関係者や社会の信頼に応えるためには、ORDEN（ODPO（Open Data Platform in Osaka）*[1]/ my door OSAKA*[2]等）が取り扱うデータ（パーソナルデータを含む）を、事故・災害・犯罪などの様々な脅威から守り、漏えい、滅失又は毀損を防ぐことその他のデータの安全を確保することはもとより、ORDEN を支える情報システムの安全性及び信頼性の確保を行うことが必要であり、それが大阪府に課せられる責務となります。そこで、本方針は、大阪府が実施する「ORDEN における情報セキュリティ対策方針」に関する基本的な事項を定めます。

2. 情報セキュリティ管理体制

大阪府は、ORDEN で取扱うデータの保護および適切な管理を行うため、「プライバシーガバナンス統括責任者」「個人情報保護管理責任者」「個人情報保護管理補助者」「個人情報・プライバシー取扱事務担当者」「個人情報・プライバシー窓口担当者」を配置し、運用いたします。

3. 方針・ルールの周知

大阪府は、情報資産の保護および適切な管理を行うための明確な方針・ルールを府内及び関連組織に周知徹底します。

4. 定義

（1） 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います。

（2） 機密性

情報に関して正当な権限を持つ者だけが当該情報にアクセスできる状態をいいます。

（3） 完全性

情報が破壊、改ざん又は称呼されていない状態をいいます。

（4） 可用性

情報に関して正当な権限を持つ者が、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いいます。

5. 対象とする脅威

大阪府は、情報資産に対する脅威として、以下のものを想定して情報セキュリティ対策を実施するほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応します。

（1）不正アクセス、マルウェアによる攻撃、サービス不能攻撃といったいわゆるサイバー攻撃及び部外者の大阪府への侵入など、第三者の意図的な行為又は大阪府の職員等による不正行為に起因する大阪府の情報資産の漏えい、破壊、改ざん、消去又は、重要情報の窃取・詐取

（2）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、メンテナンスの不備、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又は、機器故障等の過失による情報資産の漏えい、破壊、改ざん又は消去等

（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、通信の途絶等のインフラの障害からの波及等

6. 情報セキュリティ対策

大阪府は、上記5の脅威から情報資産及び情報システムを保護するため、以下の対策を講じることとします。

（1） 組織課題としての取組

大阪府にて運営体制を整備し、組織的かつ継続的に情報セキュリティ対策を講じることとします。

（2） 体制整備

情報セキュリティの確保のために組織としての体制整備を行います。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応体制も整備します。

（3） 情報資産の分類及び管理・廃棄

大阪府が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、分類に基づく対策を講じるなど、情報資産に対するリスク評価及びリスクへの対応を実施することとします。また、不要なデータの削除及び機器、電子媒体等の廃棄にあたっては、復元不可能な手段で実施することとします。

（4） 物理的セキュリティ対策

データを取り扱う区域及びサーバの管理、機器及び記録媒体等の盗難等の防止、通信回線等及び業務用端末等の管理について、物理的な対策を講じることとします。

（5）　人的セキュリティ対策

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い、必要とされる知識・技術を習得させる等の人的な対策を講じることとします。

（6）　技術セキュリティ対策

アクセス制御、外部からの不正アクセス等の防止、不正プログラム対策、情報システムの使用に伴う漏えい等の防止等の技術的対策を講じます。

（7）　運用面での対策

情報システムの監視及び情報セキュリティ確保のための規程類の遵守状況の確認など、運用面での対策を講じることとします。

（8）　データの流通における対策

大阪府が様々な主体から提供を受けたデータを第三者に利用させることによりデータ流通を図る場合には、大阪府が定める規約等、セキュリティ対策上遵守が必要となる事項を条件として提示します。

（9）　外部委託に係る対策

大阪府の事業の全部又は一部を第三者に委託する場合には、大阪府が定めるセキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、委託事業者等の選定要件として提示します。さらに、契約や合意の締結時等に、委託先において大阪府が実施するセキュリティ対策と同等のセキュリティ対策が確保されていることを契約事項等に明記することとします。なお、約款による外部サービスを利用する場合には、当該利用に関連する規程類等を整備することとします。

（10）　データの保管場所

ORDEN で取扱うデータについては、日本国内において保管しています。大阪府は、関係するポリシーや規程類に基づき、データが安全に取り扱われるようにするための措置を講じます。

7. 情報管理プロセス

大阪府は、利用者のプライバシーを尊重し、利用者から提供される個人データの取り扱いについて、透明性と責任をもって行動します。

（1）取得

利用者が大阪府のサービスを利用する際に、必要最小限のパーソナルデータを収集します。これには、サービス提供のために必要な情報（例：氏名、メールアドレス）などが対象となります。

（2）保存・管理

利用者のデータは、大阪府／個人情報保護制度に関する法律・条例や総務省セキュリティガイドライン要件を満たす商用クラウドに保存し、適正に取り扱うと認めた事業者

に業務委託を行い、安全な環境下で保管され、サービス提供に必要な期間、または法律で定められた期間内に限り保管します。

（3）利用

収集したデータは、サービスの提供、改善、および利用者とのコミュニケーションの目的でのみ使用します。

（4）パーソナルデータ

パーソナルデータにおいては、利用者の同意した範囲内とし、原則二次流通は禁止します。不正使用を防ぐための適切な措置を講じます。

（5）非パーソナルデータ

非パーソナルデータにおいては、原則事業者間での合意に基づく利用とし、データの真正性・漏洩等による損害補償等は当事者間で解決するものとします。

（6）廃棄

大阪府がサービスの利用を終了するか、利用者がデータの削除をリクエストした場合、大阪府が遵守する適用法規に従い、速やかに利用者のデータを削除します。

（7）継承

利用者の同意なく第三者とパーソナルデータを継承・共有することはありません。ただし、法的義務の履行または利用者の同意に基づく場合はこの限りではありません。

8. 法令及び契約上の要求事項の遵守

大阪府は、情報管理プロセスの取扱いを含む関連する法令、ガイドライン、規制、規範、契約上の義務を遵守します。

9. 最新の考え方等の反映

大阪府は、情報セキュリティ対策が日進月歩であり考え方も変化することに鑑み、最新のセキュリティ対策に関する情報を収集し、必要に応じて有用なソリューションを活用するとともに、最新の考え方等を本方針に反映するよう努めます。

10. 自己点検及び情報セキュリティに関する監査の実施

大阪府は、本方針及び情報セキュリティ確保のための規程類の遵守状況を検証するため、定期的に規程類に基づくオペレーション実施の可否を判断し、必要に応じて、自己点検及び情報セキュリティに関する監査を実施します。

11. 本方針の改定

大阪府は、自己点検及び情報セキュリティに関する監査の結果、本方針及び情報セキュリティ確保のための規程類の見直しが必要となった場合、又は、情報セキュリティに関する状況の変化に対応するために新たな対策が必要となった場合には、本方針を見直すこととします。

この場合、変更後の本方針の施行時期及び内容を大阪府のウェブサイト上での表示その他の適切な方法により周知し、又は本サービスの利用者に通知いたします。

附則

令和 6（2024）年 3 月 26 日制定

令和 6（2024）年 8 月 29 日改定