官民連携データプラットフォーム　情報セキュリティ基本方針（素案）

1　本基本方針の目的

官民連携データプラットフォーム運営組織（仮）（以下「当組織」といいます。）がその目的を果たしつつ、都民の皆様はもとより、様々な関係者や社会の信頼に応えるためには、データプラットフォームが取り扱うデータを重要な情報資産として、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、データプラットフォーム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、それが当組織に課せられる責務となります。

そこで、本基本方針は、当組織における情報セキュリティの確保を目的として、当組織が実施する情報セキュリティ対策に関する基本的な事項を定めます。

2　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。

3　対象とする脅威

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当組織への侵入など、第三者の意図的な行為又は当組織の職員等による不正行為に起因する当組織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

4　情報セキュリティ対策

当組織は、上記3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

当組織は、経営層が主体となって、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

当組織は、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、情報セキュリティ確保のための規程等を定めるものとします。

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、緊急時対応体制を整備します。

（3）情報資産の分類及び管理・廃棄

当組織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）技術的セキュリティ対策

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

当組織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、当組織が定める規約等、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

当組織の事業の全部又は一部を第三者に委託する場合には、当組織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、委託先において当組織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。

5　法令及び契約上の要求事項の遵守

当組織は、情報の取扱いに関連する法令、ガイドライン、規制、規範、契約上の義務を遵守します。

6　最新の考え方等の反映

情報セキュリティ対策は日進月歩であり考え方も変化します。そこで、当組織は、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。

7　自己点検及び情報セキュリティに関する監査の実施

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。

8　情報セキュリティポリシーの見直し

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、本方針及び情報セキュリティ確保のための規程類を見直すこととします。