別記　データ保護及び管理に関する特記仕様書

第１ 目的

本契約において取り扱う各種データについて、適正なデータ保護・管理方策及び情報システムのセキュリティ方策ついて明確にすることを目的とする。

第２ 適用範囲

本契約を履行するに当たり、出版、報道等により公にされている情報を除き、九都県市首脳会議廃棄物問題検討委員会（以下「発注者」という。）が交付若しくは使用を許可し、又は契約の相手方（以下「受注者」という。）が作成若しくは出力したものであって用紙に出力されたものを含む全ての情報（以下「電子データ等」という。）を対象とする。

第３ 対象とする脅威

本書において対象とする脅威は、次に掲げる情報セキュリティが侵害された又はそのおそれがある場合とする。

（１）不正プログラムへの感染（受注者におけるものを含む。）

（２）サービス不能攻撃によるシステムの停止（受注者におけるものを含む。）

（３）情報システムへの不正アクセス（受注者におけるものを含む。）

（４）書面又は外部記録媒体の盗難又は紛失（受注者におけるものを含む。）

（５）機密情報の漏えい・改ざん（受注者におけるものを含む。）

（６）異常処理等、予期せぬ長時間のシステム停止（受注者におけるものを含む。）

（７）発注者が受注者に提供した又は受注者にアクセスを認めた発注者の電子データ等の目的外利用又は漏えい

（８）アクセスを許可していない発注者の電子データ等への受注者によるアクセス

（９）意図しない不正な変更等（受注者におけるものを含む。）

第４ 本契約を履行する者が遵守すべき事項

受注者は、本契約の履行に関して、以下の項目を遵守すること。

４．１ 業務開始前の遵守事項

受注者は、以下の（1）から（6）までの各項目に定める事項及び契約内容を一部再委託する場合は（7）に定める事項を取りまとめた「データ管理計画書」を作成し、業務開始前までに発注者の承認を得ること。

なお、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）による個人番号及び特定個人情報（以下「特定個人情報等」という。）を取扱う業務の場合は、他の電子データ等と明確に区分して管理することとし、特定個人情報の適正な取扱いに関するガイドラインに基づく安全管理措置について、「データ管理計画書」の各事項へ、追加で記載すること。

（1）データ取扱者等の指定

受注者は、電子データ等を取り扱う者（以下「データ取扱者」という。）及び、データ取扱者を統括する者（以下「データ取扱責任者」という。）を指定し、その所属、役職及び氏名等を記入した「データ取扱者等名簿」を作成すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等を明確に管理するため、特定個人情報等を取り扱う者（以下「特定個人情報ファイル取扱者」という。）及び特定個人情報ファイル取扱者を統括する者（以下「特定個人情報ファイル取扱責任者」という。）についても併せて指定し、「データ取扱者等名簿」に記載すること。

なお、データ取扱者、データ取扱責任者、特定個人情報ファイル取扱者及び特定個人情報ファイル取扱責任者（以下「データ取扱者等」という。）は、守秘義務等のデータの取扱いに関する社内教育、又はこれに準ずる講習等を受講した者とし、その受講実績も併せて「データ取扱者等名簿」に記入すること。

（2）データ取扱者等への教育・周知計画

受注者は、データ取扱者等を対象とした、本契約での電子データ等の取扱いや漏えい防止等の教育及び周知に関する「データ取扱者等への教育・周知計画」を作成すること。

（３）電子データ等の取扱いにおける情報セキュリティ確保の措置計画

受注者は、本契約に係る電子データ等の取扱いに関し、電子データ等の保存、運搬、複製及び破棄並びに電子データ等の保管場所を変更する場合において実施する措置を記載した「データ取扱計画」を作成すること。「データ取扱計画」には、以下に示す措置を含めること。

（ア）本契約の作業に係る電子データ等を取り扱うサーバ、パソコン、モバイル端末について、アクセス制御及び脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。

（イ）機密性２以上の電子データ等の取扱いは、発注者又は受注者のいずれかの管理下にない情報システム等（データ取扱者等の個人所有物であるパソコン及びモバイル端末を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（ウ）電子データ等名称、データ取扱者名、授受方法、使用目的、使用場所、保管場所、保管方法、返却方法、授受日時、返却日時、特定個人情報等の有無等を記録する「データ管理簿」を整備すること。

（エ）機密性２以上の電子データ等の保存に、発注者又は受注者のいずれかの管理下にない情報システム等又は電磁的記録媒体（データ取扱者等が私的に契約しているサービス及びデータ取扱者等の個人所有物である電磁的記録媒体を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（オ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者の作業に立ち会うなど適切な管理を行うこと。

（カ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者が作業を終了し作業場所を離れる際は、データの持ち出しの有無を厳重に検査すること。

（キ）機密性２以上の電子データ等を電子メールにて送信する場合には、暗号化を行うこと。

（４）外部設置における情報セキュリティ確保の措置計画

受注者は、発注者が指定する場所以外に情報システム機器を設置（外部設置）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、部外者

の侵入等の意図的な情報漏えい等を防止する措置を記載した「外部設置における情報セキュリティ措置計画」を作成すること。「外部設置における情報セキュリティ措置計画」には以下に示す措置を含めること。

（ア）情報システムにアクセス（一般向けに提供されているウェブページへのアクセスを除く。）する作業は、受注者の管理下にあり、部外者の立入りが制限された場所において行うこと。

（イ）電子データ等を取り扱うパソコン、モバイル端末等について、盗難、紛失、表示画面ののぞき見等による漏えいを防ぐための措置を講ずること。また、それらの措置を講じていないパソコン、モバイル端末等を用いた作業を制限すること。

（ウ）入退室記録、作業記録等を蓄積し、不正の検知、原因特定に有効な管理機能を備えること。

（５）外部接続における情報セキュリティ確保の措置計画

受注者は、発注者が指定するネットワーク以外のネットワークへ接続（以下「外部接続」という。）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、外部のネットワークからの侵入や改ざんを防御する措置を記載した「外部接続におけるセキュリティ措置計画」を作成すること。「外部接続におけるセキュリティ措置計画」には、以下に示す措置を含めること。

（ア）外部接続箇所にファイアウォールを設置し、不要な通信の遮断を行うこと。

（イ）外部接続箇所に侵入検知システムを設置し、ネットワークへの不正侵入の遮断を行うこと。

（ウ）外部接続箇所で不正な通信を検出した場合、発注者へ通報を行うこと。

（６）情報セキュリティが侵害された又はそのおそれがある場合における対処手順

受注者は、本契約に係る業務の遂行において情報セキュリティが侵害された又はそのおそれがある場合に備え、事前に連絡体制を整備し、発生した場合の対処手順を記載した「情報セキュリティ侵害時対処手順」を作成すること。「情報セキュリティ侵害時対処手順」には、以下に示す対処を含めること。

（ア）作業中に、情報セキュリティが侵害された又はそのおそれがあると判断した場合には、直ちに、発注者に、口頭にてその旨第一報を入れること。発注者への第一報は、

情報セキュリティインシデントの発生を認知してから１時間以内に行うこと。

（イ）当該第一報が行われた後、発生した日時、場所、発生した事由、関係するデータ取扱者等を明らかにし、平日の午前９時から午後５時の間は１時間以内に、それ以外の時間帯は３時間以内に発注者に報告すること。また、当該報告の内容を記載した書面を遅延なく発注者に提出すること。

（ウ）発注者の指示に基づき、対応措置を実施すること。

（エ）発注者が指定する期日までに、発生した事態の具体的内容、原因、実施した対応措置を内容とする報告書を作成の上、発注者に提出すること。

（オ）再発を防止するための措置内容を策定し、発注者の承認を得た後、速やかにその措置を実施すること。

（７）再委託における情報セキュリティの確保の措置計画

受注者は、本契約内容について一部再委託（更に順次行われる再委託を含む。）する場合、受注者が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対策を再委託先において確保させる必要があり、再委託先における情報セキュリティの十分な確保を受注者が担保するとともに、再委託先の情報セキュリティ対策の実施状況を確認するため、「再委託における情報セキュリティ措置計画」を作成すること。なお、特定個人情報等を取扱う業務を再委託したときは、発注者が行う再委託先の管理状況等の確認について、受注者は必要な協力を行うこと。

４．２ 業務実施中における遵守事項

（１）「データ管理計画書」に基づく情報セキュリティ確保

「データ管理計画書」に記載した、データ取扱者等への教育・周知、電子データ等の取扱い及び作業場所等の情報セキュリティ確保のための措置を実施すること。

（２）データ管理簿への記録

受注者は、データ取扱者等が電子データ等を取り扱う場合、「データ管理簿」に記録し、データ取扱責任者に確認させること。また、特定個人情報等を扱う業務の場合、特定個人情報ファイル取扱責任者に併せて確認させること。

（３）「データ管理計画書」の変更

（ア）受注者は、本契約に基づく請負作業中に、次の事項について作業開始前に提出した「データ管理計画書」の内容と異なる措置を実施する場合は、事前に「データ管理計画書」の変更について発注者に提出し、承認を得ること。また、承認された変更の内容を記録し保存すること。

・データ取扱者等の異動を行う場合

・データ取扱者等に対する教育・周知の計画を変更する場合

・電子データ等の取扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置を変更する場合

・再委託先及び再委託先の情報セキュリティ対策を変更する場合

（イ）一時的に「データ管理計画書」とは異なる措置を実施する場合は、原則として事前にその旨を発注者へ提出し、承認を得ること。ただし、情報セキュリティが侵害された又はそのおそれがある場合など緊急を要する場合等の場合、受注者は、実施内容について事後速やかに発注者へ報告すること。

（４）業務の報告・監査等

（ア）受注者は、発注者へ業務実施中の「データ管理計画書」の遵守状況について定期的に報告すること。

（イ）受注者は、発注者が「データ管理計画書」に係る管理状況について監査を要請した時は、定期・不定期にかかわらず、これを受け入れること。

（ウ）受注者は、「データ管理計画書」の評価、見直しを行うとともに、必要な改善策等について、発注者へ提案すること。

（５）情報セキュリティ対策の履行が不十分であった場合の対応

受注者の本契約に係る作業における情報セキュリティ対策の履行が不十分であると発注者が判断した場合、受注者は発注者と協議の上、必要な是正措置を講ずること。また、是正措置の内容を「データ管理計画書」に反映させること。

４．３ 業務完了時の遵守事項

（１）データ返却等処理

受注者は、本契約に基づく業務が完了したときは、「データ管理簿」に記録されている全てのデータについて、返却、消去、廃棄等の措置を行うものとし、処理の方法、日時、場所、立会者、作業責任者等の事項を記した、「データ返却等計画書」を事前に発注者へ提出し、承認を得た上で処理を実施すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等であることを「データ返却等計画書」に明示すること。

（２）作業後の報告

受注者は、「データ返却等計画書」に基づく処理が終了したときは、その結果を記載した「データ管理簿」を発注者へ提出すること。

（３）情報セキュリティ侵害の被害に関する記録類の引渡し

受注者は、本契約の業務遂行中に情報セキュリティが侵害された又はそのおそれがある事象が発生した場合、４．１（６）に基づいて取得し保存している記録類を発注者に引き渡すこと。

４．４ 記憶装置の修理及び廃棄等におけるデータ消去

受注者は、契約により発注者が利用する情報システム機器の修理及び廃棄、リース返却（以下、「廃棄等」という。）の場合、記憶装置から、全ての電子データ等を消去の上、復元不可能な状態にする措置（以下、「抹消措置」という。）を実施すること。

（１）抹消措置計画の作成

受注者は、「データ管理計画書」へ作業予定日時、作業予定場所、実施予定者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者などを記載した「抹消措置作業計画」を追加するとともに、必要に応じてその他の措置内容を変更したうえ、抹消措置実施日（賃貸借契約の場合は賃貸借期間満了日）の３０日前までに発注者に提出し、承認を得ること。

また、賃貸借契約の場合は賃貸借期間満了日から３０日以内に抹消措置実施日を設

定すること。

（２）抹消措置実施方法

ア マイナンバー利用事務系の領域において住民情報を保存する記憶媒体の抹消措置の方法

（ア）当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること。なお、対象となる機器について、リース契約による場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行うこと。

（イ）職員が抹消措置の完了まで立ち会いによる確認を行う。ただし、庁舎外で抹消措置を行う場合は、庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の証拠写真が添付された完了証明書により確認できること。

イ 機密性２以上に該当する情報を保存する記憶媒体（上記アに該当するものを除く。）の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うこと。

（イ）庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認できること。

ウ 機密性１に該当する情報を保存する記憶媒体の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態に消去すること。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

エ ＩｏＴ機器を含む特殊用途機器の抹消措置の方法

（ア）デジタル複合機などのＩｏＴ機器を含む特殊用途機器に保存された電子データ等の漏えいの対策について、国際標準に基づくセキュリティ要件と同等以上のセキュリティ要件とその要件に適合した第三者認証（「ＩＴ製品の調達におけるセキュリティ

要件リスト」適合製品など）を取得している機能を有する場合は、当該機能によるデータ消去をもって抹消措置とすることができる。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

（３）抹消措置の報告

受注者は、抹消措置実施日から３０日以内に、作業日時、実施者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者及び全ての記憶装置について抹消措置前後の写真を添付した「抹消措置完了報告書」を発注者へ提出し、承認を得ること。

第５ 情報システムの情報セキュリティ要件

受注者は、本契約により情報システムを導入する場合は、対象となる以下の項目を遵守すること。

５．１ 侵害対策

（１）通信回線対策

（ア）通信経路の分離

不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。

（イ）不正通信の遮断

通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

（ウ）通信のなりすまし防止

情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。

（エ）サービス不能化の防止

サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。

（２）不正プログラム対策

（ア）不正プログラムの感染防止

不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。

（イ）不正プログラム対策の管理

システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該

機能の動作状況及び更新状況を一元管理する機能を備えること。

（３）脆弱性対策

（ア）構築時の脆弱性対策

情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

（イ）運用時の脆弱性対策

運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。

５．２ 不正監視・追跡

（１）ログ管理

（ア）ログの蓄積・管理

情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、発注者が指定する期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。

（イ）ログの保護

ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。

（ウ）時刻の正確性確保

情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。

（２）不正監視

（ア）侵入検知

不正行為に迅速に対処するため、情報システムで送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。

（イ）サービス不能化の検知

サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。

５．３ アクセス・利用制限

（１）主体認証

情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体の認証を行う機能として、ＩＤ／パスワードの方式を採用し、主体認証情報の推測や盗難等のリスクの軽減を行う機能として、パスワードの複雑性及び指定回数以上の認証失敗時のアクセス拒否などの条件を満たすこと。

（２）アカウント管理

（ア）ライフサイクル管理

主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。

（イ）アクセス権管理

情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。

（ウ）管理者権限の保護

特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。

５．４ 機密性・完全性の確保

（１）通信経路上の盗聴防止

通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信内容を暗号化する機能を備えること。

（２）保存情報の機密性確保

情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存できないようにすることに加えて、保存された情報を暗号化する機能を備えること。

（３）保存情報の完全性確保

情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。

５．５ 情報窃取・侵入対策

（１）情報の物理的保護

情報の漏えいを防止するため、記憶装置のパスワードロック、暗号化等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。

（２）侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。

５．６ 障害対策（事業継続対応）

（１）システムの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハード

ウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。

（２）システムの可用性確保

サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として１日を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。

５．７ サプライチェーン・リスク対策

（１）受注者（再委託先含む）において不正プログラム等が組み込まれることへの対策

情報システムの構築において、発注者が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。

（２）調達する機器等に不正プログラム等が組み込まれることへの対策

機器等の製造工程において、発注者が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

５．８ 利用者保護

（１）情報セキュリティ水準低下の防止

情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。

（２）プライバシー保護

情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。