

情報資産の取扱いに関する特記事項

（基本的事項）

第1条 受注者は、大和市情報セキュリティポリシー及び地方公共団体における情報セキュリティポリシーに関するガイドラインに基づき、本情報資産の取扱いに関する特記事項（以下「特記事項」という。）を遵守し、情報資産の取扱いを適正に行わなければならない。

（責任体制の整備）

第2条 受注者は、情報資産の安全管理について、内部における責任体制を構築し、その体制を維持しなければならない。

（作業責任者等の届出）

第3条 受注者は、情報資産の取扱いに係る作業責任者及び作業従事者を定め、文書により発注者に報告しなければならない。

2 受注者は、情報資産の取扱いに係る作業責任者及び作業従事者を変更する場合の手続きを定めなければならない。

3 受注者は、作業責任者を変更する場合は、事前に文書により発注者に報告し、その承認を得なければならない。

4 受注者は、作業従事者を変更する場合は、事前に文書により発注者に報告しなければならない。

5 作業責任者は、特記事項に定める事項を適切に実施するよう作業従事者を監督しなければならない。

6 作業従事者は、作業責任者の指示に従い、特記事項に定める事項を遵守しなければならない。

（作業場所の特定）

第4条 受注者は、情報資産を取り扱う場所（以下「作業場所」という。）を定め、業務の着手前に文書により発注者に報告しなければならない。

2 受注者は、作業場所を変更する場合は、事前に文書により発注者に報告し、その承認を得なければならない。

3 受注者は、発注者の事務所内に作業場所を設置する場合は、作業責任者及び作業従事者に対して、受注者が発行する身分証明書を常時携帯させ、事業者名が分かるようにしなければならない。

（教育の実施）

第5条 受注者は、情報資産の保護、情報セキュリティに対する意識の向上、仕様書（本特記事項を含む）における作業従事者が遵守すべき事項その他本契約における業務の適切な履行に必要な教育及び研修を、作業従事者全員に対して実施しなければならない。

2 受注者は、前項の教育及び研修を実施するに当たり、実施計画を策定し、実施体制を確立しなければならない。

（守秘義務）

第6条 受注者は、本契約における業務の履行により直接又は間接に知り得た情報資産を

第三者に漏らしてはならない。契約期間満了後又は契約解除後も同様とする。

- 2 受注者は、本契約における業務に関わる作業責任者及び作業従事者に対して、秘密保持に関する誓約書を提出させなければならない。

(再委託)

第7条 受注者は、本契約のうち情報資産を取り扱う業務を再委託してはならない。

- 2 受注者は、本契約のうち情報資産を取り扱う業務の一部をやむを得ず再委託する必要がある場合は、次に掲げる事項を明確にした上で、業務の着手前に、文書により再委託する旨を発注者に申し出て、その承認を得なければならない。

(1) 再委託先の名称及び所在地

(2) 再委託する理由

(3) 再委託する業務内容

(4) 再委託先において取り扱う情報資産

(5) 再委託先における情報資産管理の安全性及び信頼性を確保する対策

(6) 再委託先に対する管理及び監督の方法

- 3 前項に規定する場合においては、受注者は、再委託先に本契約に基づく一切の義務を遵守させるとともに、発注者に対して、再委託先の全ての行為及びその結果について責任を負うものとする。

- 4 受注者は、再委託先との契約において、再委託先に対する管理及び監督の方法及び方法について具体的に規定しなければならない。

- 5 受注者は、本契約における業務を再委託した場合は、再委託先に対して、その履行状況を管理し、及び監督するとともに、発注者の求めに応じて、管理及び監督の状況を適宜報告しなければならない。

(派遣労働者等の利用時の措置)

第8条 受注者は、本契約における業務を派遣労働者、契約社員その他の正社員以外の労働者に行わせる場合は、正社員以外の労働者に本契約に基づく一切の義務を遵守させなければならない。

- 2 受注者は、発注者に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

(情報資産の管理)

第9条 受注者は、本契約における業務において利用する情報資産を保持している間は、次の各号及び別表1「機密性による情報資産の分類」に定めるところにより、その管理を行わなければならない。

(1) 情報資産は、施錠が可能な保管庫又は施錠若しくは入退室管理の可能な保管室で厳重に保管すること。

(2) 発注者が指定した場所へ持ち出す場合を除き、情報資産を定められた場所から持ち出さないこと。

(3) 情報資産を持ち出す場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。

(4) 事前に発注者の承認を受けて、業務を行う場所で、かつ業務に必要最小限の範囲で行

う場合を除き、情報資産を複製又は複写しないこと。

- (5) 情報資産を移送する場合、移送時の体制を明確にすること。
- (6) 情報資産を電子データで保管する場合、当該データが記録された媒体及びそのバックアップの保管状況並びに記録されたデータの正確性について、定期的に点検すること。
- (7) 情報資産を管理するための台帳を整備し、情報資産の利用者、保管場所その他の情報資産の取扱いの状況を当該台帳に記録すること。
- (8) 情報資産の紛失、漏洩、改ざん、破損その他の事故（以下「情報資産の漏洩等の事故」という。）を防ぎ、真正性、見読性及び保存性の維持に責任を負うこと。
- (9) 作業場所に、私用パソコン、私用外部記録媒体その他の私用物及び使用が許可されていない情報機器等を持ち込んで、情報資産を扱う作業を行わせないこと。
- (10) 情報資産を利用する作業を行うパソコン等に、情報資産の漏洩につながると考えられる業務に関係のないアプリケーションをインストールしないこと。
- (11) 情報資産をクラウドサービスや電子メール等のインターネットに接続するサービスで取り扱う場合には、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。

- 2 前項の規定に関わらず、機密性3の情報資産及び機密性2以上の個人情報に当たる情報資産は、クラウドサービス、電子メール等のインターネットに接続するサービスで取り扱ってはならない。ただし、ガバメントクラウド若しくはLGWAN-ASPサービスで取り扱う場合又は発注者が特に認める場合は、この限りでない。

（提供された情報資産の目的外利用及び第三者への提供の禁止）

- 第10条 受注者は、本契約における業務において利用する情報資産について、本契約における業務以外の目的で利用してはならず、かつ、発注者に無断で第三者へ提供してはならない。

（受渡し）

- 第11条 受注者は、発注者受注者間の情報資産の受渡しに関しては、発注者が指定した手段、日時及び場所で行った上で、発注者に情報資産の預り証を提出しなければならない。

（情報資産の返還、消去又は廃棄）

- 第12条 受注者は、本契約における業務の終了時に、本契約における業務において利用する情報資産について、発注者の指定した方法により、返還、消去又は廃棄（以下「処理」という。）を実施しなければならない。ただし、発注者が不要と認めるときは、この限りでない。

- 2 受注者は、前項の規定により本契約における業務において利用する情報資産を処理する場合は、事前に次に掲げる事項を文書により発注者に報告し、その承諾を得なければならない。

- (1) 情報資産の項目
- (2) 記録媒体
- (3) 数量
- (4) 処理予定日

(5) 処理方法

(6) 処理担当者

3 受注者は、情報資産の消去又は廃棄に際し発注者から立会いを求められた場合は、これに応じなければならない。

4 受注者は、本契約における業務において利用する情報資産を廃棄する場合は、別表2「情報の機密性に応じた機器の廃棄等の方法」に定めるところにより、当該情報資産を復元不可能な状態にしなければならない。

5 受注者は、情報資産の処理を行ったときは、次に掲げる事項を記録した証明書を作成し、発注者に提出しなければならない。

(1) 情報資産の項目

(2) 記録媒体

(3) 数量

(4) 処理実施日

(5) 処理方法

(6) 処理担当者

(定期報告及び緊急時報告)

第13条 受注者は、発注者から、情報資産の取扱いの状況について報告を求められた場合は、直ちにこれに応じなければならない。

2 受注者は、情報資産の取扱いの状況に関する定期報告及び緊急時報告の手順を定めなければならない。

(監査及び検査)

第14条 発注者は、本契約における業務に係る情報資産の取扱いについて、本契約の規定に基づき必要な措置が講じられているかどうか検証し、及び確認するため、受注者及び再委託先に対して、監査又は検査を行うことができる。

2 前項の場合において、発注者は、受注者に対して必要な情報を求め、又は本契約における業務の処理に関して必要な指示をすることができる。

(事故時の対応)

第15条 受注者は、本契約における業務に関し情報資産の漏洩等の事故が発生した場合は、その事故の発生に係る帰責の有無に関わらず、直ちに発注者に対して、当該事故に関わる情報資産の内容、件数、事故の発生場所、発生状況等を文書により報告し、発注者の指示に従わなければならない。

2 受注者は、情報資産の漏洩等の事故が発生した場合に備え、発注者その他関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置等を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

3 発注者は、本契約における業務に関し情報資産の漏洩等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

(契約解除)

第16条 発注者は、受注者が本特記事項に定める義務を履行しない場合は、本特記事項に関連する契約における業務の全部又は一部を解除することができる。

2 受注者は、前項の規定による契約の解除により損害を受けた場合においても、発注者に対して、その損害の賠償を請求することはできないものとする。

(損害賠償)

第17条 受注者の故意又は過失を問わず、受注者が本特記事項の内容に違反し、又は怠ったことにより、発注者に対する損害を発生させた場合は、受注者は、発注者に対して、その損害を賠償しなければならない。

(サービスレベルの保証)

第18条 受注者は、発注者が必要と認める場合、提供するサービスのサービスレベルの保証について発注者と受注者が協議の上、別途協定を締結しなければならない。

(定めのない事項等)

第19条 本特記事項に定めのない事項又は本特記事項に関して疑義が生じた時は、発注者と受注者が協議して決定する。

別表 1 「機密性による情報資産の分類」

分類	分類基準	取扱制限
機密性 3	行政事務で取り扱う情報資産のうち、マイナンバー利用事務系のネットワーク（基幹系ネットワーク）で取り扱う情報資産又はそれに準じる機密性を要する情報資産	・ 支給以外の端末での作業の原則禁止 ・ 必要以上の複製及び配付禁止 ・ 保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止
機密性 2	行政事務で取り扱う情報資産のうち、L G W A N 接続系のネットワーク（情報系ネットワーク）で取り扱う公表することを前提としていない次の情報を含む情報資産（機密性 3 の情報資産を除く） ・ 市民の生命に危険が及ぶ情報 ・ 市民の財産及びプライバシーを侵害する情報 ・ 企業、国及び他の自治体に影響が及ぶ情報 ・ 市内部の事務に影響が及ぶ情報	・ 個人情報の保存時における暗号化・パスワード設定・アクセス制限 ・ 情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・ 復元不可能な処理を施しての廃棄 ・ 信頼のできるネットワーク回線を選択 ・ 外部で情報処理を行う際の安全管理措置の規定 ・ 電磁的記録媒体の施錠可能な場所への保管
機密性 1	機密性 2 又は機密性 3 の情報資産以外の情報資産	—

別表2「情報の機密性に応じた機器の廃棄等の方法」

分類	廃棄等の手順
機密性3に該当する情報を記録する記録媒体 ※機密性3：行政事務で取り扱う情報資産のうち、マイナンバー利用事務系のネットワーク（基幹系ネットワーク）で取り扱う情報資産又はそれに準じる機密性を要する情報資産	(1) データ消去 職員立会又は庁内において、次のいずれかの方法で情報の復元が困難な状態までデータを消去する。 ①物理的な方法による破壊 ②磁気的な方法による破壊 ③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去 ④ブロック消去 ⑤暗号化消去 (2) 物理破壊 (1)の処理完了後、分解・粉碎・溶解・焼却・細断などによって物理的に破壊する（委託事業者による庁外での処理も可能）。 (3) 完了証明書 (1)、(2)の処理完了後、それぞれの処理の完了証明書を受領する。 完了証明書は、処理日時、処理担当者及び処理内容（証拠写真、対象機器のシリアル番号、処理方法など）の記載が必要。
機密性2に該当する情報を保存する記憶媒体 ※機密性2：行政事務で取り扱う情報資産のうち、LGWAN接続系のネットワーク（情報系ネットワーク）で取り扱う公表することを前提としていない次の情報を含む情報資産（機密性3の情報資産を除く） ・市民の生命に危険が及ぶ情報 ・市民の財産及びプライバシーを侵害する情報 ・企業、国及び他の自治体に影響が及ぶ情報 ・市内部の事務に影響が及ぶ情報	(1) データ消去 職員立会又は庁内において、次のいずれかの方法で情報の復元が困難な状態までデータを消去する。 ①物理的な方法による破壊 ②磁気的な方法による破壊 ③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去 ④ブロック消去 ⑤暗号化消去 (2) 完了証明書 (1)の処理完了後、処理の完了証明書を受領する。 完了証明書は、処理日時、処理担当者及び処理

	内容（証拠写真、対象機器のシリアル番号、処理方法など）の記載が必要。
機密性 1 に該当する情報を保存する記憶媒体 ※機密性 1：機密性 2 又は機密性 3 の情報資産以外の情報資産	(1) データ消去 次のいずれかの方法で情報の復元が困難な状態までデータを消去する（委託事業者による庁外での処理も可能）。 ①物理的な方法による破壊 ②磁気的な方法による破壊 ③OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去 ④ブロック消去 ⑤暗号化消去 ⑥OS 等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去 (2) 完了証明書 (1) の処理完了後、処理の完了証明書を受領する。 完了証明書は、処理日時、処理担当者及び処理内容（証拠写真、対象機器のシリアル番号、処理方法など）の記載が必要。