別記

情報セキュリティに関する特記事項

（総則）

第１　この特記事項は、受注者が業務を行うに当たって、機密情報取扱特記事項第１章第１に規定する「機密情報」が含まれた電磁的記録を取り扱う場合の特則を定めるものであり、受注者は、機密情報取扱特記事項と合わせて本特記事項を遵守しなければならない。

（基本的事項）

第２　受注者は、業務を行うに当たっては、別紙「受託者向け情報セキュリティ遵守事項」に基づき、情報を適正に取り扱わなければならない。

（安全管理措置）

第３　受注者は、機密情報を含む電磁的記録（以下「機密データ」という。）の取扱いに当たっては、機密データの漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等の防止のために、必要かつ適正な管理（以下「安全管理措置」という。）を行うものとする。

（作成、複製又は加工）

第４　受注者が、機密データを作成、複製又は加工（以下「作成等」という。）しようとする場合には、本件業務の履行のために必要な範囲において行うものとし、作成等の途上で生成される情報についても、第３と同等の安全管理措置を講じなければならない。また、作成等の途上で不要となった情報については、随時消去するものとする。

（機密データの保存等に係る届出）

第５　受注者はあらかじめ、業務の遂行において取り扱う機密データの保存先等の情報（オンラインストレージ等のクラウドサービスを使用している場合に当たっては、利用契約先の情報等を含む。）を別記様式により発注者に届け出るとともに、内容に変更が生じた場合には、速やかに再度の届出を行うものとする。

（機密データの持出等の禁止）

第６　受注者は、あらかじめ発注者の承認を得た場合を除き、機密データの社外への持出及び第５により届出を行っていないオンラインストレージ等のクラウドサービス上に保存する行為を行ってはならない。

（目的外利用・提供の禁止）

第７　受注者は、機密データの業務遂行の目的以外の目的による利用及び第三者（会社法（平成17年法律第86号）第２条第３号の２に規定する子会社等及び同条第４号の２に規定する親会社等を含む。）への提供を行ってはならない。

（生成ＡＩの利用）

第８　受注者は、本契約に基づく業務遂行のため、生成ＡＩ（文章、画像、プログラム等を生成できるＡＩモデルをいう。以下同じ。）又は生成ＡＩを利用したサービス（以下「生成ＡＩ等」という。）において機密データを取り扱う場合には、次の事項を遵守しなければならない。

１　受注者は、本業務に関して入力した内容が生成ＡＩ等の学習に利用されない生成ＡＩ等を使用すること。

２　生成ＡＩ等を利用して作成した納品成果物については、生成ＡＩ等を利用している旨を発注者に明示して納品すること。

３　利用する生成ＡＩ等に関する情報をあらかじめ別記様式により発注者に届け出るとともに、内容に変更が生じた場合には、速やかに再度の届出を行うこと。

（教育の実施）

第９　受注者は、機密データを取り扱う従事者に対し、別紙「受託者向け情報セキュリティ遵守事項」を理解し、実践するために必要な情報セキュリティに係る教育及び訓練を実施するものとする。

（再委託等に当たっての留意事項）

第10　受注者は、発注者の書面による承諾を得て業務の全部又は一部を第三者に委託（二以上の段階にわたる委託をする場合及び受注者の子会社（会社法第２条第３号に規定する子会社をいう。）に委託をする場合を含む。以下「再委託等」という。）する場合には、再委託等の相手方にこの特記事項及び別紙「受託者向け情報セキュリティ遵守事項」を遵守させなければならない。

（再委託等に係る連帯責任）

第 11　受注者は、再委託等の相手方の行為について、再委託等の相手方と連帯してその責任を負うものとする。

（機密データの返還等）

第 12　受注者は、本契約による業務を遂行するために利用又は作成した機密データについて、業務完了後直ちに、返還又は消去を行うものとする。ただし、発注者が別に指示したときは当該方法によるものとする。

（再委託等の相手方からの回収等）

第 13　受注者が発注者の承認を得て再委託等の相手方に機密データを提供した場合において、受注者は、業務終了後直ちに再委託等の相手方から機密データを回収し、又は再委託等の相手方に消去させるものとする。ただし、発注者が別に指示したときは当該方法によるものとする。

（報告等）

第 14　報告等については、次のとおりとする。

1　発注者は、必要があると認めるときは、受注者又は再委託等の相手方に対して、この特記事項の遵守状況その他のセキュリティ対策の状況について、定期的又は随時に報告を求めることができる。

2　受注者は、この特記事項に違反する行為が発生した場合、又は発生するおそれがあると認められる場合（再委託等の相手方により発生し、又は発生するおそれがある場合を含む。）は、直ちに発注者にその旨を報告し、その指示に従わなければならない。

3　受注者は、この特記事項への違反の有無にかかわらず、本契約に係る業務で取り扱う情報資産に対して、情報セキュリティインシデントが発生した場合、又は発生するおそれがあると認められる場合は、直ちに発注者にその旨を報告し、その指示に従わなければならない。

（立ち入り検査）

第 15　発注者は、この特記事項の遵守状況の確認のため、受注者又は再委託等の相手方に対して立ち入り検査（発注者による検査が困難な場合にあっては、第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査、検査又は国際的なセキュリティの第三者認証(ISO/IEC27001 等)の取得等の確認）を行うことができる。

（情報セキュリティインシデント発生時の公表）

第 16　発注者は、本契約に係る業務に関して、情報セキュリティインシデントが発生した場合（再委託等の相手方により発生した場合を含む。）は、必要に応じて、当該情報セキュリティインシデントを公表することができるものとする。

（情報セキュリティの確保）

第 17　発注者は、本契約に係る受注者の業務の遂行に当たって、前項までに定めるもののほか、必要に応じて、情報セキュリティを確保する上で必要な対策を実施するよう指示することができ、受注者はこれに従わなければならない。

（損害賠償）

第 18　受注者が本特記事項に違反したことにより発注者又は第三者に損害を及ぼした場合には、発注者が必要と認める措置を直ちに講ずるとともに、発注者又は第三者に対して生じた損害を賠償するものとする。

（存続期間）

第 19　本特記事項の効力は本件業務に係る契約期間の満了まで有効とする。ただし、第 12（機密データの返還等)、第 13（再委託等の相手方からの回収等)、第 14（報告等。ただし、第 1 項の規定を除く。）及び第 18（損害賠償）の規定については、契約期間の満了後も有効に存続するものとする。

（協議事項）

第 20　本特記事項に定めのない事項に関しては、別途発注者と誠実に協議の上、円満な解決を図るものとする。

別紙

受託者向け情報セキュリティ遵守事項

1　趣旨

この受託者向け情報セキュリティ遵守事項は、情報セキュリティに関する特記事項（以下「特記事項」という。）に基づき、受注者が業務を行う際の細則及び具体的な手順を定めたものであり、受注者は特記事項と合わせて遵守する義務を負う。

2　機密データの管理・保管及び持出

(1)　管理・保管

受注者は、本契約に係る業務の遂行に当たって入手した資料、データ、記録媒体等について、常に適正な管理を行うとともに、特に個人情報等の重要な情報について、暗号化、パスワードの設定、個人情報の匿名化、アクセス制限等、厳重に管理し、使用しない場合には、施錠ができる書庫等に保管しなければならない。

(2)　持出

受注者は、特記事項第６（機密データの持出等の禁止）に基づき、あらかじめ発注者の承認を得て機密データを社外へ持ち出す場合には、機密データを出力又は保存した機器又は媒体について盗難及び紛失が発生しないよう十分な対策を講じるとともに、機密データの暗号化又は電子ファイルを開くためのパスワードを設定するなど第三者への漏えい等を防ぐための安全管理措置を講じること。

3　クラウドサービスの利用

(1)　事前の届出

受注者は、オンラインストレージ等のクラウドサービス（以下「クラウドサービス」という。）を利用して機密データを取り扱う場合には、特記事項第５（機密データの保存等に係る届出）に基づき事前に届出を行ったクラウドサービスを利用するものとする。また、利用するクラウドサービスを変更しようとする場合には、あらかじめ再度の届出を行うものとする。

(2)　提供事業者によるアクセス等

受注者がクラウドサービスにおいて機密データを取り扱う場合には、当該クラウドサービスの提供事業者による機密データのアクセス若しくは利用等が可能な契約又は利用規約とされているクラウドサービスを使用してはならない。ただし、発注者から承諾がある場合にはこの限りではない。

(3)　機密データの消去等

受注者は、業務中にクラウドサービスにおいて取り扱う機密データについて、不要となった時点で随時に機密データの消去を行うとともに、業務完了後はデータの消去又は暗号鍵を削除する等の対応により、保存した機密データが復元困難となる措置を講じること。

4　情報機器等の管理

(1)　情報機器

受注者は、機密データを取り扱う機器（ノートPC及びタブレット等の端末、サーバ等）をネットワークに接続して使用する場合には、セキュリティ対策ソフトの導入等により外部からの侵入及び漏えい等を防止するための必要な対策を講じるとともに、OS及びソフトウェアを最新の状態に更新するなど、セキュリティの脆弱性に関する対策を講じなければならない。

(2)　ネットワーク接続

機密データを取り扱う機器又は情報システムを外部のネットワークと接続して利用する場合には、取り扱う機密情報の重要性に応じて、適正なセキュリティ対策を講じること。

5　パスワード管理

機密情報の保管・管理、電子ファイルの閲覧制限、情報システムの管理その他のセキュリティ対策のため、パスワードによる管理を行う場合は、次に掲げる事項を遵守すること。

(1)　従事者個人に割り当てられたパスワードは当該従事者以外の者に漏れることがないよう適切に管理すること。
(2)　パスワードが流出したおそれがある場合には、受注者におけるセキュリティ管理者に速やかに報告するとともに、パスワードを変更する対応を行うこと。

6　情報の送受信

受注者が、発注者又は発注者が送付先として指定した者を送り先として機密データを含む情報を送受信する場合には、次に掲げる事項を遵守すること。

(1)　電子メール

ア　宛先、メール本文、添付ファイルの中身について、送信前に確認すること。

イ　発注者が送付先として指定したメールアドレスが複数ある場合の送信については、送付先のメールアドレスをBCCに入れる又は個別送付が可能なソフトウェアを利用するなど、送付先のメールアドレスの漏えいを防ぐための適切な対策を講じること。

(2)　ファイル交換・転送サービス

ファイル交換・転送サービスによる送受信を行う場合は、発注者が指定したサービスとすること。

(3)　オンラインストレージ

オンラインストレージを利用して送受信を行う場合には、発注者が指定したオンラインストレージを利用すること。

7　従事者の教育

特記事項第９（教育の実施）に基づき、受注者は次の事項を遵守すること。

(1)　従事者の教育状況の管理

受注者において、本業務の従事者が適切な教育及び訓練を受けた者であるか確認すること。また、業務の履行期間中であっても、教育状況が不十分と思われる事案が生じた場合は、追加の教育及び訓練を実施すること。

(2)　教育状況の報告

受注者は、本契約の期間中に発注者が従事者の教育状況の確認を求めた場合には、教育及び訓練の内容、実施日時並びに受講状況等を報告すること。

(3)　再委託先等の従事者

再委託先等の従事者の教育状況について発注者が確認を求めた場合には、(2)の報告に代えて、受注者が再委託先等の教育状況を確認した方法及び内容について報告すること。

8　機密情報の漏えい・紛失の防止策の徹底

受注者は、機密情報の漏えい・紛失を防止するため、次の事項に留意するとともに、機密情報を取り扱う従事者に対し適切な指示及び監督を行うこと。

(1)　ノートPC等のモバイル端末の社外利用

ノートPC等のモバイル端末を社外で使用する場合には次の事項を遵守すること。

ア　ノートPC等のモバイル端末を第三者が使用することがないよう、利用認証等の適切なセキュリティ対策を行うこと。

イ　ノートPC等のモバイル端末に直接機密データを保存する場合には、データ暗号化等による紛失・盗難時の対策をとること。

ウ　飲食店、公共施設、休憩所など、本件業務と関わりのない不特定多数の者が利用する場所において、ノートPC等のモバイル端末を利用しての業務を行わないこと。

エ　公衆Wi-Fi等の不特定多数の者が利用可能なネットワークに接続しないこと。

オ　ノートPC等のモバイル端末の紛失及び盗難に十分注意するとともに、短時間であっても部外者が立ち入る恐れのある共用スペースや車内に放置しないこと。

カ　盗難及び紛失の防止のため、酒席へのノートPC等のモバイル端末の持込みを行わないこと。

(2)　書類の取扱いについて

機密データを印刷した書類については、次のとおり取り扱うこと。

ア　機密データを書類として出力する場合には、情報の流出防止のため、必要最低限の範囲に限るものとし、不要となった時点でシュレッダー等による廃棄を行うこと。

イ　飲食店、公共施設、休憩所など、本件業務と関わりのない不特定多数の者が利用する場所において、当該書類を用いた業務を行わないこと。

ウ　発注者の承諾がある場合を除き、第三者への閲覧、複写又は提供を行わないこと。

エ　盗難及び紛失の防止のため、酒席へ当該書類の持込みを行わないこと。

(3)　その他の禁止事項

ア　不特定多数の者が立ち入る場所で携帯電話等の通話手段を利用する場合には、機密情報が含まれる内容を話してはならない。

イ　部外者が聞き取る可能性がある場所（公共交通機関、エレベータ、食堂、飲食店、家庭内など）で本件業務に係る内容を話してはならない。

ウ　発注者の承諾がある場合を除き、ソーシャルメディアにおいて本業務に係る内容及び本業務を推察できる内容の発信を行なってはならない。

9　セキュリティ事案発生時の連絡・対応

受注者は、本業務に関し情報セキュリティインシデントが発生した場合の連絡・管理体制をあらかじめ定めるとともに、情報セキュリティインシデントの発生又は発生したおそれがある場合には次の対応を行わなければならない。

(1)　一報

受注者は、発注者が指定した連絡窓口に、最初に事案を認識した時点から 60 分以内に一報の連絡をすること。

(2)　続報

一報後、発注者が求める事項について、速やかに続報の連絡を行うこと。

(3)　受注者による公表

情報セキュリティインシデント事案の発生について受注者が公表する場合には、事前に発注者に対して公表を行う旨の連絡をするものとする。ただし、損害の発生が生じる可能性があり急を要するなど、やむを得ない事情がある場合はこの限りではない。