別紙3

情報セキュリティ対策チェックシート

	チェック内容	はい	いいえ	該当無
1. 契約時の「情報セキュリティ要件」等の遵守状況				
	貴社は、契約時の「情報セキュリティに関する要件」や「個人情報取扱特記仕様書」などの諸規定を、本業務に従事する技術者等（再委託先を含む。以下、「従事者」という。）に遵守させるよう教育し、教育・指導の記録を管理していますか？※特定個人情報取扱業務については、発注者の指示に従い、個人情報保護研修の実施状況、従事者の署名入りの研修記録を提出してください。	□	□	□
2. 組織的安全管理				
2-1	情報セキュリティ対策に関わる責任者と担当者の役割や権限が明確になっていますか？具体的には、個人情報保護責任者、個人情報保護担当者は任命されていますか？	□	□	□
2-2	重要な情報またはそれを管理する物品等について、入手、利用、保管、交換、提供、作成、消去、破棄における取扱手順を定めていますか？	□	□	□
2-3	情報資産の業務目的以外の使用及び第三者への提供の禁止を、従事者に対して遵守させていますか？	□	□	□
2-4	契約期間中及び契約終了後においても、業務で知り得た秘密を他に漏らしてはならないことを、従事者に対して遵守させていますか？	□	□	□
2-5	個人情報管理台帳等により、管理すべき重要な情報資産を把握し、区分していますか？また、その更新を行っていますか？	□	□	□
2-6	再委託を行う場合、発注者の事前の承認を得ていますか？また、再委託先の個人情報保護管理体制を確認し、機密保持契約を締結するとともに、本チェックシートによる点検をしていますか？	□	□	□
2-7	内部点検を定期的に実施していますか？また、点検に基づく改善を行っていますか？	□	□	□
2-8	情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づくISMS認証又はそれと同等の認証を取得し、適切に更新していますか？（受注者及び再委託先の事業者）（※特定個人情報取扱業務については、受注者及び再委託先の事業者についても認証証明書の写しを提出してください）	□	□	□
3. 人的安全管理				
3-1	委託業務に関わる従業員（契約社員、パート、アルバイトを含む）から機密保持に関する誓約書など取得していますか？	□	□	□
3-2	派遣社員を使用している場合、派遣会社と機密保持契約を結び、自社の個人情報保護の仕組み・手順を理解させ、誓約書を取得していますか？	□	□	□
3-3	アクセス権限を付与する従業員は必要最小限に限定し、かつアクセス権限の範囲も必要最小限に限定していますか？	□	□	□
4. 物理的安全管理				
4-1	私物のパソコン及び不正な記録媒体の接続を禁止していますか？	□	□	□
4-2	パソコン等の端末、記録媒体、情報資産及びソフトウエア等を外部に持ち出す場合、情報セキュリティ対策に関わる責任者等の許可を得ていますか？	□	□	□
4-3	重要な情報を含む書類、記憶媒体、モバイルPC等の保管場所やそれらを扱う場所について、施錠管理や入退管理を行っていますか？	□	□	□
4-4	重要な情報を含む書類、記憶媒体、モバイルPC等について、整理整頓を行うとともに、取り扱う場所への監視カメラ設置などの盗難防止対策や確実な廃棄を行っていますか？	□	□	□
4-5	市や外部の組織と情報をやり取りする際に、情報の取扱いに関する注意事項について合意し、管理簿等で保管期限（5年）を定めた上で、記録をとって実施していますか？	□	□	□
5. 技術的安全管理				
（1）情報システム及び通信ネットワークの管理				
5-1	情報システム（本業務システムだけでなく、貴社が管理するシステム、パソコン等も含む。）のセキュリティ対策に関する運用ルールを策定していますか？	□	□	□
5-2	ウイルス対策ソフトは常時最新のパターンファイルに更新していますか？	□	□	□
5-3	導入している情報システムに対して、最新のパッチを適用する等の脆弱性対策を行っていますか？	□	□	□
5-4	通信ネットワークを流れる重要なデータ、電子メールに添付する機密情報などに対して、暗号化等の保護策を実施していますか？	□	□	□
5-5	情報システムを扱う機器からUSBメモリ等へデータを外部に持ち出す場合、データ持出し制限、承認者による持出し許可、持出し記録の管理を行っていますか？	□	□	□
5-6	モバイルPCやUSBメモリ等の記憶媒体でデータを外部に持ち出す場合、盗難、紛失等に備えて、適切なパスワード設定や暗号化等の対策を実施していますか？	□	□	□
5-7	インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISPサービス等）や不正な通信、不正操作の有無を確認するため、ログ（通信記録）の取得や管理、監視を行っていますか？	□	□	□
5-8	無線LAN のセキュリティ対策（強力な暗号化方式（WPA2またはWPA3）と認証方式（AES方式））を行っていますか？	□	□	□
5-9	メール誤送信を防ぐ対策（メール送信前確認や強制BCC化）及び運用ルールを設けていますか？	□	□	□
（2）アクセス制御				
5-10	情報システム（本業務システムだけでなく、貴社が管理するシステム、パソコン等も含む）へのアクセスを制限するために、利用者IDの管理を行っていますか？	□	□	□
5-11	情報システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ対策（推測可能なパスワード、初期パスワードの設定禁止、認証の総当たり攻撃対策、機器内のセキュリティパラメータの保護）を行っていますか？	□	□	□
5-12	重要な情報に対するアクセス権限の設定を行っていますか？ また、アクセス記録は保管期限（5年）を定め取得し、保管していますか。	□	□	□
5-13	改ざんや漏えい防止のため、リスクが大きい振る舞いを検知する仕組みや、各種ログの点検を定期的に行う体制が整備されていますか？不要なポートを閉じ、外部からアクセスできる通信経路を必要最小限に絞っていますか？	□	□	□
6. 事故対応				
6-1	情報セキュリティに関する事件や事故等（情報漏洩、ウィルス感染等）の緊急時対応の手続き、報告書の様式、連絡体制は整備できていますか？また、事故の再発防止への取組はされていますか？	□	□	□
6-2	情報システムに障害が発生した場合、業務を再開するため緊急時対応計画、緊急時連絡網の整備を策定し、訓練をしていますか？	□	□	□

※「いいえ」に該当する項目については、業務着手までに対策を実施してください。対策については、発注者と協議の上実施してください。
※「該当無」に該当する項目については、特に対策は必要ありません。