別紙３

発注者施設外作業拠点設置に係る特記事項

（発注者施設外作業拠点）

第１条　発注者施設外作業拠点（以下「作業拠点」という。）とは、システム構築及び運用保守の実施を目的に、発注者施設外から発注者が利用するシステムの稼働環境に接続し、システム等で保有する発注者情報にアクセス可能な状態で作業を行う受注候補者施設をいう。

　発注者施設外拠点を設置する場合、本特記事項の記載事項を遵守しなければならない。

（責任体制の構築）

第２条　受注候補者は、作業責任者及び作業従事者を定め、書面により発注者に報告すること。

２　受注候補者は、作業責任者及び作業従事者を変更する場合、事前に書面により発注者に申請し、その承認を得ること。

３　作業責任者は、個人情報の取り扱いが適切に実施されるよう作業従事者を監督すること。

４　作業従事者は、作業責任者の指示に従い、適切に個人情報を取り扱うこと。

（作業拠点の限定）

第３条　作業拠点とする受注候補者施設は、発注者に届出を行った上で許可を得た施設でなければならない。

２　作業拠点の施設設備費用は受注候補者が負担すること。

３　受注候補者は、作業拠点内でシステム環境に接続して作業を行う区域（以下「作業区域」という。）を指定し、業務の着手前に書面によりに発注者に報告すること。

４　受注候補者は、作業区域を変更する場合は、事前に書面により発注者に申請し、その承認を得ること。

５　受注候補者は、作業区域について第２条第１項に基づき届出のあった作業責任者及び作業従事者以外立ち入ることができない措置を講じなければならない。

６　受注候補者は、作業区域の入退室を記録し定期的に発注者に状況を報告すること。

（通信回線）

第４条　作業拠点から発注者システム環境に接続するために利用する通信回線は、専用線や閉域ネットワーク等を用いることとし、暗号化等の十分な情報セキュリティ対策が講じられていること。

（保守作業端末）

第５条　作業拠点から発注者システム環境に接続する端末は、事前に発注者に届出を行った上で許可を得た端末でなければならない。

２　作業端末のログインアカウントは１人につき１アカウントを作成し、共有アカウントの利用は禁止とする。

３　作業端末のログインアカウントは、第２条第１項に基づき届出のあった作業責任者及び作業従事者以外の者が作成してはならない。

４　端末のログイン認証は、生体認証等の二つ以上を併用する認証を用いた多要素認証を導入しなければならない。

５　作業端末OSはサポート対象のバージョンを利用すること。

６　ウィルス対策ソフトウェアをインストールしウィルス定義は最新の状態を保つこと。

７　作業端末は施錠可能なロッカー等で保管し、使用時のみ作業責任者の許可を得た上で取り出すこと。また、使用終了後は速やかにロッカー等に戻し施錠すること。

８　机上等に常設する端末にはセキュリティワイヤー設置等による盗難防止措置を行うこと。

９　保守作業端末を作業区域から持ち出す場合、発注者に事前に許可を得た上で復元不可能な方法で記憶装置のデータ消去を行い、発注者に消去証明書を提出すること。

10　端末操作ログを取得し不正利用の有無を管理し定期的に発注者に報告すること。

（情報持出の制限）

第６条　受注候補者は、作業端末のいかなる情報も印刷してはならない。

２　受注候補者は、作業端末のいかなる画面も撮影してはならない。

３　受注候補者は、作業端末のいかなる情報もデバイスに複製してはならない。

　また、作業端末の情報をデバイスへ複製できない設定を行わなければならない。

４　受注候補者は、作業端末に情報の複製以外の用途でデバイスを接続する場合は、デバイスの種類、型番及び用途を発注者に事前に届出し許可を得なければならない。また、許可されたデバイス以外接続できない設定を行わなけ

ればならない。
５　受注候補者は、業務履行上デバイスへの複製が必要な場合は、発注者が実施し提供するものとする。

（緊急時報告）
第７条　受注候補者は、作業拠点で情報漏えい等の情報インシデントが発生したことを知覚した場合、ただちに発注者に報告しなければならない。
２　受注候補者は、情報インシデント報告の手順を定めなければならない。