別紙

ＲＦＱサプライチェーン・リスク対策関連要件

本依頼において提案する機器等（ネットワーク，情報システム，ネットワーク又は情報システムに関する施設及び設備，電磁的記録媒体等の情報資産をいう。以下同じ。）が以下の（１）及び（２）を満たしていることを担保すること。

（１）基本的なセキュリティ対策として，下記のア～エを全て満たしていること。

ア　必要なセキュリティ機能を含んでいること。

イ　設置時や保守時のサポート体制が確立されていること。

ウ　利用マニュアル・ガイダンスが適切に整備されていること。

エ　脆弱性検査等のテストの実施が確認できること。

（２）サプライチェーン・リスク対策として，下記のア又はイを満たしていること。

ア　情報資産の分類に応じて，「セキュリティ要件適合評価及びラベリング制度（ＪＣ－ＳＴＡＲ，経済産業省）」，「政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ，ＩＳＭＡＰ－ＬＩＵ，国家サイバー統括室・デジタル庁・総務省・経済産業省）」又は「デジタルマーケットプレイス（ＤＭＰ，デジタル庁）」（以下「政府の評価・登録制度」という。）に登録等がなされていることが確認できること。

イ　政府の評価・登録制度に登録等がなされていない機器等（政府の評価・登録制度の対象とならない製品分野に属する機器等を含む。）に関しては，次のとおり適切なサプライチェーン・リスク対策が講じられていることが確認できること。

（ア）機器等の開発等のライフサイクルにおいて，不正な変更が加えられない管理がなされていることが確認できること。具体的には以下のａ～ｄを全て満たしていること。

ａ　製造工程（開発工程を含む。以下同じ。）において，機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者（再委託先事業者等を含む。以下同じ。）による信頼できる品質保証体制が確立されていること。

ｂ　製造工程における不正な変更の有無について，機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者において，定期的又は随時に確認を行うこと。

ｃ　製造環境（開発環境を含む。）において，定められた要員以外がアクセスできないよう，機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者が，アクセス可能な要員を物理的（監視カメラ等の入退室管理等）かつ論理的（データシステム等へのアクセス制御）に適切に制限していること。

ｄ　調達した機器等に不正な変更やそのおそれがあることを発見した場合には，機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者並びに当該機器等の設置，保守等の役務を提供する事業者及びその委託先事業者に対して，必要に応じて追

跡調査や立入検査を行う等，本市と受注者が連携して原因を調査・排除できる体制を整備していること。

（イ）機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者並びに当該機器等の設置，保守等の役務を提供する事業者及びその委託先事業者について，当該事業者等の本社等（当該事業者等の総株主等の議決権の過半数を直接又は間接に保有する者の本社等を含む。）の立地する場所の法的環境や外部主体の指示等により，当該機器等に係る開発・供給又は役務の提供等の適切性が影響を受け，これにより悪意ある機能や不正な変更が機器等に組み込まれる又は当該機器等が取り扱う情報が窃取・破壊される等のリスクに係る懸念が払拭できない機器等を調達しないこと又は役務の提供を受けないこと。

（ウ）ISO/IEC 15408 等，国際標準に基づく第三者認証の取得又は第三者による監査結果により，セキュリティ機能の適切な実装，開発環境の管理体制の検査，脆弱性テスト等について客観的に評価できること。

（エ）ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とする場合には，SBOM（Software Bill of Materials：ソフトウェア部品表）の作成，提供等を行っていること。