■「EDRを利用したSOCサービスの設計、構築、導入及び運用保守業務」仕様書に関する問い合わせへの回答

令和5年(2023年)8月8日

仕様書に対して、問い合わせがあった内容について以下のとおり回答します。

札幌市デジタル戦略推進局情報システム部

項番	質問	回答
1	以下要件定義書に記載の要件に対する弊社提案内容が要件を満たしているか回答をお願いいたします。 ＜要件記載箇所＞ 別紙１　要件定義書（14）運用（ウ）ログ管理 ・監視対象の端末で収集されたログやアラート対象となるログは 1 年間保持可能であること。なお、ログの保存期間により、追加費用が発生しないことに留意すること。 ・受託者は、保存対象ログの取り出しについて、本市担当者から依頼・指示を受けた場合は、速やかに対応すること。 ＜弊社提案内容＞ ログの保管期間について EDRクライアント（EDRセンサー）から収集されたログをクラウド上ストレージに1年間保存します。費用は初期費用に含めてご提案します。 保管期間:1年間 ※保持できるログは1年分のみとなります。 例：2023年11月1日から2024年11月30日までの１年分保存（2024年12月1日以降、以前1年分ログはローテーションされます。） 保存対象ログの取出しについて クラウド上ストレージに保管しているログについて、お客様のご依頼に基づいて一定期間のログを専用UI(WEB)から閲覧し、CSVでダウンロードできるようにいたします。 ご依頼日より5営業日を目途にお客様にデータ閲覧環境を提供いたします。 ※取出し対象のログは監査において必要となる端末および期間のログでありログ全件ではない認識です。	左記で御提案いただいているログの取得方法で、仕様を満たしております。