■「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) 7月19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	「別紙１ 要件定義書」「３ 非機能要件」について、弊社ご提案のSOCサービスの運用は以下の通りとなります。受託後の認識の齟齬を無くすため、仕様を満たすかについて確認させて頂ければと思います。 (14) 運用 ウ 運用業務対象 （ア）「運用支援業務を行う時間は原則として開庁日8:45～17:15とすること。」 （ウ）「重大なインシデント等の緊急対応が必要な場合は、運用業務時間に限らず保守業務として対応すること。」 (15)保守 エ 保守業務 （ア）② 「判定されたインシデントレベルに応じて、SOC サービスから本市運用管理者へメール、電話による通知が可能なこと。」 この「重大なインシデント等の緊急対応が必要な場合」において、弊社ご提案のSOCサービスの運用では、開庁日の17:15以降および閉庁日にて重大インシデントが発生した場合、貴庁職員様（管理者様含む）へ自動通知、アナリストによる解析後、重大インシデントと確定した場合にはメール通知に加えお電話にて通報連絡を行います。メール通知の内容としては、インシデントに関連したサマリー、推奨対策、及びIRの推奨などでございます。お電話では貴庁職員様（管理者様含む）のフォローアップを行い、その情報をもとにして対応方法のご判断を行って頂くことを想定しております。 なお、お電話での通知に関しましては、メールでのご報告内容の補足的位置づけとさせて頂いております。インシデント発生時には正確な情報、証跡管理が重要と考えておりますので、原則はメールでのやり取りとさせて頂いております。	左記で御提案いただいているSOCサービスの運用で、仕様を満たしております。