■「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25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	・弊社ご提案予定の SOC サービスにつきまして、認識の齟齬をなくすため、「SOC サービス要求機能一覧」に記載の機能を満たすかどうか確認させていただきたく存じます。 弊社ご提案予定のSOCサービスのインシデントレベルは、以下の4段階に定めております。 ・ほぼ悪意ある攻撃と推定 ・悪意ある攻撃の可能性も否定できない ・悪意ある攻撃の可能性は低い ・攻撃とはいえないが留意すべき事象 攻撃が成功した可能性が高いインシデントに対して、早期対応が必要でないケースは考えにくいことから、 SOCサービス要求機能一覧No5のインシデントレベル4と3はほぼ同義と認識しております。 そのためご提案予定のSOC サービスにおいては、「ほぼ悪意ある攻撃と推定」を札幌市様の仕様におけるインシデントレベル4と3を包括するレベルと考えてよろしいでしょうか。	仕様書 別紙２「SOCサービス要求機能一覧」No.5のインシデントレベルの趣旨は以下となります。 Lv4：攻撃が成功し、横展開含め早期対応が必要 Lv3：危険性の高い攻撃を受けていることを検知 インシデントレベル4と3は包括せずに、「SOCサービス要求機能一覧」No.4、5で示す4段階以上のインシデントレベルを設定いただきますようお願いいたします。