「電力広域的運営推進機関　セキュリティログ監視サービス」に関する質問等

電力広域的運営推進機関

No.	仕様書等該当箇所 （ページ、項目等）	質　問	回　答
1	(別紙)要求仕様書 P1 1.(1)調達物品に係る用語定義 (別紙)要求仕様書P7 3. (1)表 3.1 役務に係る業務要件-業務手順	要求仕様書を見ると、「(2) 調達対象」にはSIEMの記載がないが、 「(1) 調達物品に係る用語定義」の図や「表 3.1 役務に係る業務要件-業務手順」には SIEMの記載があった。 SIEMを用いた解析は必須要件となるか。 例えばNDR製品を用いることでも、要求仕様書に記載の機能要件および業務要件を満たすことができる上に、 より深く分析し、組織を俯瞰して問題を確認することが可能となると考えているが、 要件を満たす別の製品を用いた監視の提案をすることも可能となるか。	SIEMを用いた解析は必須です。 SIEMについては、監視側にて対応して下さい。
2	(別紙)要求仕様書 P1 1.(1)調達物品に係る用語定義	SOC監視用セキュリティデバイスからのSOC内のSIEMへのSyslog転送に関して、 要求では、Internet VPNを経由するようにとのことだが、 Internet VPNデバイスの代わりに、SOC監視用セキュリティデバイスからログ受信と転送を行うログ転送装置を設置することは可能でしょうか？ ログ受信装置とSOC間の通信は、VPNとはなりませんが、ログ転送装置により暗号化された状態で行われる。 ※上記が可能な場合でも、Internet VPNデバイスは、SOC監視用セキュリティデバイスの保守用と使用させて頂く。	ログ転送装置の設置は可能です。 ログ転送装置とSOC間の通信は、以下の要件でお願いします。 ・機器間の認証接続があること（SSLclient認証のイメージ） ・通信は暗号化されること
3	仕様書 P3 2. (1)⑤設置・工事	「ラックの設置、電源工事、SOC 監視用セキュリティデバイス、インターネット回線の設置・工事を行うこと。」とのことだが、ラックの設置と電源工事は、作業の範囲外である認識だが、問題ないか？	問題ありません。 ラックの設置、電源工事は、範囲外です。
4	(別紙)要求仕様書 P5 2.(2)①表 2.2 設備に係る非機能要件-規模 「監視対象」	弊社SOCで監視するにあたり、syslogサーバが1台必要となる。 機関様内に下記要件を満たすサーバがあれば、本件のsyslogサーバとして利用させていただくことは可能か。 メモリ：最小64MB OS：Red Hat Enterprise Linux8 (64-bit) 　　Red Hat Enterprise Linux9 (64-bit) ディスク容量：30MB(ソフトウェアインストール用) ※別途ログ保管用ディスク容量が必要になる。	利用不可です。
5	(別紙)要求仕様書 P5 2.(2)①表 2.2 設備に係る非機能要件-規模 「監視対象」	メインサイトの10ポート及びバックアップサイトの5ポートについては全て銅線での接続になるか。 光ケーブルを接続する場合は、指定の光ケーブルがあれば提示してほしい。 指定のケーブルが無い場合、伝送帯域及びミラーリングするスイッチからSOC監視用セキュリティデバイスを設置するラックマウント場所までの距離を示してほしい。	全て銅線（UTP）での接続になります。

「電力広域的運営推進機関　セキュリティログ監視サービス」に関する質問等

電力広域的運営推進機関

No.	仕様書等該当箇所 （ページ、項目等）	質　問	回　答
6	(別紙)要求仕様書 P5 2.(2)①表 2.2 設備に係る非機能要件-規模 「監視対象」	メインサイトにSOC監視用セキュリティデバイスを2台設置する場合、アクティブ側とスタンバイ側のHA構成にする構成かと考えている。 その場合、要件としては1台で10ポート(2台で20ポート)見る形になるか。 それとも、アクティブ側で5ポート、スタンバイ側で5ポートの接続を想定されているか。	HA構成はアクティブパッシブ構成でお願いします。 アクティブ側で8ポート、スタンバイ側で８ポートの接続を想定しております。
7	(別紙)要求仕様書 P5 2.(2)①表 2.2 設備に係る非機能要件-規模 「通信量」	メインサイト及びバックアップサイトでミラーリングする通信の、これまでの最大通信量をbps単位で示してほしい。	7.8gbps以上を満たす機器でお願い致します。
8	(別紙)要求仕様書 P6 2.(2)②表 2.3 設備に係る非機能要件-信頼性 「耐障害性」	耐障害性について、障害発生時に迅速に調査/機器交換できる保守契約で満たすことが可能か。	HA構成はアクティブパッシブ構成は必須です。 機器単体での、障害発生時に迅速に調査/機器交換できる保守契約で満たすことで問題ありません。
9	(別紙)要求仕様書 P6 2.(2)③表 2.4 設備に係る非機能要件-情報セキュリティ 「ファームウェア」	「最新の OS 及びファームウェアを利用し、既知の脆弱性のない状態 で納品すること」 上記について、弊社SOCではサービス提供上問題ないか検証後、対応OS及びファームウェアとさせていただいている。 上記最新OS及びファームウェアについて、弊社対応の最新OS及びファームウェアのご提供でも要件満たすことが可能か。	可能です。 但し、その後のソフトウェア/ファームウェアのアップデートは、保守サービスの範囲内で実施して下さい。
10	(別紙)要求仕様書 P7 3.(1)①表 3.1 役務に係る業務要件-業務手順 「設計」	カスタムシグネチャの作成について、下記を検知可能なカスタムシグネチャを要件確認で詳細お伺いしたうえで作成する形になるか。 - HTTP：POST, PUT、User-Agent、Connect メソッド、特定拡張子 - Mail：特定拡張子 - DNS：txt レコード 作成が必要な場合、カスタムシグネチャの詳細要件を教示いただくことが可能か。現在弊社が保有しているカスタムシグネチャで要件を満たすことができるか確認したい。	設計工程の中で、要件確認を行っていきます。
11	(別紙)要求仕様書 P7 3.(1)①表 3.1 役務に係る業務要件-業務手順 「設計」	「システム運用における業務フロー、手順（判断基準を含む）、バックアップサイトへの切替手順、体制、連絡先を設計し、受託者のサービス仕様を運用設計書に取りまとめること。」 上記は調達範囲外の既存環境に対するフローや手順の設計という理解でよいか。	既存の業務システムは範囲外です。
12	(別紙)要求仕様書 P7 3.(1)①表 3.1 役務に係る業務要件-業務手順 「設計」	「システムの障害時に影響を受ける業務や業務復旧までの時間及び対応フローについて運用設計書に取りまとめること」 上記システムとは本件の調達対象であるSOC監視用セキュリティデバイスやVPN機器を指しているか。 ※SOC監視用セキュリティデバイスの障害発生時に、SOCサービスとして受ける影響を記載する形か。	その通りです。

「電力広域的運営推進機関　セキュリティログ監視サービス」に関する質問等

電力広域的運営推進機関

<table>
<tr><th>No.</th><th>仕様書等該当箇所
（ページ、項目等）</th><th>質　問</th><th>回　答</th></tr>
<tr><td>13</td><td>(別紙)要求仕様書 P8
3.(1)①表 3.1 役務に係る業務要件-業務手順
「試験」</td><td>「運用開始にあたり、本機関は情報セキュリティに関する検査を実施する。」

上記は調達範囲機器に対してセキュリティ診断を実施されるという理解でよいか。
その場合、セキュリティ診断の指摘事項修正含め本調達の範囲内という形になるか。</td><td>範囲内です。</td></tr>
<tr><td>14</td><td>(別紙)要求仕様書 P8
3.(1)①表 3.1 役務に係る業務要件-業務手順
「SIEMルールのチューニング」</td><td>「本機関が要求する SIEM ルール」とは、設計項目に記載のあるカスタムシグネチャを指しているか。

また、弊社ではアナリストによる分析及び簡易脆弱性診断により誤検知と判断した場合はお客様への緊急連絡の対象外としている。
そのため誤遮断発生時にみシグネチャの無効化もしくはホワイトリストを利用した誤遮断解除の対象としているが、誤遮断対応のみでも要件を満たすことが可能か。</td><td>運用設計で確認し決定していきます。</td></tr>
<tr><td>15</td><td>(別紙)要求仕様書 P10
3.(1)④表 3.4 役務に係る業務要件-業務管理
「コミュニケーション管理」</td><td>プロジェクト会議は定例会を指しているかと考えておりますが、頻度について機関側で指定があるか。</td><td>プロジェクト立ち上げ時は、週1回程度を想定しています。
それ以降については、検討や進捗状況により異なります。</td></tr>
<tr><td>16</td><td>(別紙)要求仕様書 P10
4.(1)①表 4.1 保守に係る業務要件-実施内容
「設定変更」</td><td>「本システムのデバイス及び提供機能に係る設定変更を実施すること。なお、設定変更は本機関の依頼から起算し、5 営業日以内に実施すること。」

上記について、弊社にて設定変更可能な項目は下表「FWにおける設定変更可能項目」のとおりだが、機関にて想定している設定変更項目と相違があるか。

FWにおける設定変更可能項目
<table><tr><th>項目</th><th>設定内容</th></tr><tr><td>Policy</td><td>Security(ACL)、NAT、QoS、Decryption、Captive Portal、Application Override</td></tr><tr><td>Object</td><td>Addresses/Address Groups、Applications/Application Groups、Services/Service Groups、Security Profiles/Security Profile Groups、Custom Objects(URL Category)、</td></tr><tr><td>Network</td><td>Virtual Routers(Static Routes)、QoS、Interfaces(Captive Portal)、Interface Management Profile、QoS Profile</td></tr><tr><td>Device</td><td>Certificate Management(Certificates)、User Identification(Group Mapping Settings)、Authentication Profile、LDAP Server Profile</td></tr></table></td><td>FWに限らず、設定変更可能なセキュリティディバイスも対象です。</td></tr>
<tr><td>17</td><td>(別紙)要求仕様書 P10
4.(1)①表 4.1 保守に係る業務要件-実施内容
「設定変更」</td><td>「ただし、緊急性の高い設定変更については、1 営業日以内に実施すること」

上記緊急性の高い設定変更について、具体的にどういった設定の変更を想定しているか。
弊社SOCでは監視する中でお客様環境に影響ありと判断したインシデントについては、送信元IPアドレスを指定して遮断する設定変更をするが、こちらの作業にて要件を満たすことが可能か。</td><td>設計工程で確認し決定していきます。</td></tr>
</table>

「電力広域的運営推進機関　セキュリティログ監視サービス」に関する質問等

電力広域的運営推進機関

<table>
<tr><th>No.</th><th>仕様書等該当箇所
（ページ、項目等）</th><th>質　問</th><th>回　答</th></tr>
<tr><td>18</td><td>(別紙)要求仕様書 P11
4.(1)①表 4.1 保守に係る業務要件-実施内容
「保守情報通知」</td><td>「当社にて使用中のソフトウェア/ファームウェアに脆弱性が発見された際、電話又はメールにて通知を行うこと。緊急性の高いものは即時情報を提供すること」

上記ソフトウェア/ハードウェアの脆弱性につきまして、弊社SOC利用に影響する脆弱性のみアナウンスを実施しているが、要件を満たすことが可能か。</td><td>可能です。</td></tr>
<tr><td>19</td><td>(別紙)要求仕様書 P11
4.(1)①表 4.1 保守に係る業務要件-実施内容
「月次報告」</td><td>「稼働状況及び本機関からの各種依頼への対応状況を月次で報告すること。」

上記月次報告はレポート形式での提示で問題ないか。</td><td>問題ありません。</td></tr>
<tr><td>20</td><td>(別紙)要求仕様書 P13
5.(1)①表 5.1 サービスに係る機能要件
「ログの取得及び保管機能」
「ログの監視機能」</td><td>ログをリアルタイムで収集/分析する要件につきまして、弊社SOCでは5分に1回syslogサーバから転送している。
5分に1回の転送後にリアルタイム分析をしている場合、要件を満たすことが可能か。</td><td>可能な限り短い時間でお願いします。</td></tr>
<tr><td>21</td><td>(別紙)要求仕様書 P14
5.(2)①表 5.2 サービスに係る業務要件-業務内容
「インシデントの分析」</td><td>「事前の運用設計に基づき、発生したインシデントのトリアージを行うこと（トリアージの基準は運用設計で定めること）」

上記トリアージの基準について、弊社SOCではお客様環境への影響度をベースに下表「弊社SOCにおける重要度」の通り定めている。
上記重要度について、機関側の考えているトリアージ基準と差分があるか。
弊社SOCにおける重要度
<table><tr><th>重要度</th><th>内容</th><th>連絡</th></tr><tr><td>Emergency</td><td>緊急事態と判断したインシデント
攻撃により以下の事象が顕著である場合が該当します。
・お客様Webページが改ざんされている
・お客様システムより情報漏えいが発生している
・マルウェア感染通信が確認でき、感染が拡大している　等</td><td rowspan="2">実害が発生している、
また発生しうる
緊急インシデントとして
電話/メールにてご連絡</td></tr><tr><td>Critical</td><td>攻撃が成功した可能性が高いと判断したインシデント
アナリストによる分析の結果、以下に該当する通信が該当します。
・マルウェアに感染後の通信が確認できている
・脆弱性をついた攻撃の成功を確認できている
・攻撃成否が不明だが影響を受ける可能性が著しく高いもの　等</td></tr><tr><td>Warning</td><td>経過観察が必要と判断したインシデント
アナリストによる分析の結果、以下に該当する通信が該当します。
・攻撃の成否を調査した結果、影響を受ける可能性が無いもの
・検知時点では影響を受ける可能性が低く、経過観察が必要なもの　等</td><td rowspan="2">直接実害がない
インシデントとして
Webポータルに
掲載する形でご連絡</td></tr><tr><td>Informational</td><td>攻撃ではないと判断したインシデント
・ポートスキャンなどの監査通信など、それ自体が実害を伴わない通信
・セキュリティ診断や検査通信　等</td></tr></table></td><td>設計工程で確認し決定していきます。</td></tr>
<tr><td>22</td><td>(別紙)要求仕様書 P14
5.(2)①表 5.2 サービスに係る業務要件-業務内容
「インシデントの分析」</td><td>「調査は、ログ保管期間である 1 年間に遡って調査すること」

上記について、緊急インシデント発生時に過去1年分のログで同様の事象がないか確認する要件になるか。</td><td>その通りです。</td></tr>
</table>

「電力広域的運営推進機関　セキュリティログ監視サービス」に関する質問等

電力広域的運営推進機関

No.	仕様書等該当箇所 （ページ、項目等）	質　問	回　答
23	㈱別紙㈱要求仕様書 P15 5.⑵①表 5.2 サービスに係る業務要件-業務内容 「定期報告」	「月次レポートの内容ついて、本機関からの問い合わせがあった場合は、会議を開催の上その内容について説明すること」 上記について、必要に応じて実施という形かと考えている。 こちらについて、１回あたりの費用を算出し、3ヵ月に1会実施する想定で提案してよいか。	年4回程度を想定して、当サービス費用に折り込んで下さい。