

「セキュリティログ監視等業務委託」に関する質問等

No.	質問日	仕様書等該当箇所 (ページ、項目等)	質問	回答
1	2017/8/30	仕様書 P4	設置場所のメインサイト及びバックアップサイトの場所（住所）をご教授ください。住所指定が難しい場合、都道府県レベル（可能であれば市区町村）までのご指定をお願いします（構築作業及びネットワーク回線のコストに影響するため）	仕様書 表1-1 用語の定義に記載のとおり、メインサイトが東京都江東区、バックアップサイトが大阪府北区となります。
2	2017/8/30	要求仕様書 P8 3. 役務に関する要件 (1) 業務要件	「①業務実施手順」の「設計」フェーズに記載されておりますカスタムシグネチャの作成についてどのくらいの量（シグネチャ数）を想定しているのでしょうか。	要求仕様書のP8 表3.1に記載のとおりですが、HTTPでPOST, PUT, User-Agent, Connectメソッド、特定拡張子、Mailで特定拡張子、DNSでtxtレコードの7つであり、User-AgentはInternet Explorer以外の全て、Connectメソッドは、80及び443ポート以外の全て、特定拡張子はHTML, DOC(X), XLS(X)等の業務で通常利用される以外の拡張子の全てが対象に含まれると想定しています。特殊な要件はないため、一般的に想定される量をご提案ください。
3	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	「①業務実施手順」の「設計」フェーズに記載されております「情報セキュリティの観点に基づく試験」とは具体的にどのような試験を指しているのでしょうか。	本仕様書に示す業務の実施に当たっては、仕様書P7の6.(2)遵守する法令等に記載する事項を参照してください。政府情報システムの整備及び管理に関する標準ガイドライン実務手引書では、機密保護テスト、ペネトレーションテスト、脆弱性テスト等の情報セキュリティの観点に基づく試験が挙げられており、これらを参考に要件確認で定義されたセキュリティ要求を検証する適切かつ十分な試験項目が試験設計に含まれるようにしてください。
4	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	「①業務実施手順」の「設置・工事」フェーズに記載されております設置工事について、下記2点についてご教授下さい。 1. データセンター内に敷設する各ケーブル長についてご教授下さい。 2. 既存システムとの責任分界点を判断する部材も含むで宜しいでしょうか？	1. ラック、既設デバイス、分電盤はいずれも同一フロアにあり、床下配線により今回新たに設置するラックまでの配線は、100m以下を想定してください。 2. 既存システムとSOC監視用セキュリティデバイス間にスイッチ等のネットワーク機器を設ける場合は当該ネットワーク機器、SOC監視用セキュリティデバイスに10ポートの監視機能を設ける場合は当該SOC監視用セキュリティデバイスが責任分界点になりますので、責任分界点を判断するためだけに別途部材を設ける必要はありません。
5	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	「①業務実施手順」の「試験」フェーズに記載されております運用開始にあたり、実施する「情報セキュリティに関する検査」について、「設計」フェーズで記載されている「情報セキュリティの観点に基づく試験」とは別にお客様による試験という認識でよろしいでしょうか。その場合、お客様にて試験を実施し、導入者は検査で検出された是正箇所の対応をする認識でよろしいでしょうか。	試験は試験設計に基づき、事業者と本機関で実施しますが、受入テストは本機関が主体となって実施し、合否判定を行うことを想定しています。なお、情報セキュリティの観点に基づく試験として運用開始に先立ち外部監査人によるペネトレーションテストを実施することを予定しています。

「セキュリティログ監視等業務委託」に関する質問等

No.	質問日	仕様書等該当箇所 (ページ、項目等)	質問	回答
6	2017/8/30	要求仕様書 P12 3. 保守に関する要件 (1) 業務要件	「①業務実施内容」の「設定変更」項目に記載されております「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」とは、どのようなシチュエーションでの設定変更を想定されているでしょうか。またその頻度についてご提示いただけますでしょうか。 その後に「本機関の依頼から」という記載があるため、お客様ご指示があつて行う作業と想定しております。	現時点では具体的な変更内容や頻度の想定はありませんが、誤検知及び過剰検知の排除並びに新たな脅威を検出するために、保守および運用業務において、本機関から設定変更をご依頼することを想定しています。
7	2017/8/30	要求仕様書 P2 1. 調達要件 (3) 調達対象となる数量の考え方	「本機関のバックアップサイトは、ホットスタンバイ構成であり、メインサイトが稼働している場合には、業務通信トラフィックが発生しない仕様である。」という記載があります。 ここでいうホットスタンバイ構成とは、どちらのサイトが稼働中であっても、両サイトのSOC監視用セキュリティデバイスならびにインターネット回線は常時稼働しており、監視センターからの保守及びサービスの提供が可能な状態と解釈してよろしいでしょうか。	ご認識のとおりです。
8	2017/8/30	要求仕様書 P13 4. 保守に関する要件 (1) 業務要件 要求仕様書 P17 5. サービスに関する要件 (1) 業務要件	4.(1) ②業務提供時間 保守の業務提供時間について、「設定変更」「シグネチャ更新」「バックアップ」「保守受付(回答)」「保守情報通知」は、平日9:00-18:00とあります。 5.(1) ②業務提供時間 サービスの業務提供時間について、「QA対応業務(回答)」「ログの提供」「定期報告」「改善提案」は、平日9:00-18:00とあります。 これは一義的に作業時間を限定するものではなく、システムへの影響や所要時間等を考慮しお客様と調整したうえで、場合により時間外(夜間・休日帯)の業務作業も可能と解釈してよろしいでしょうか。	ご認識のとおりです。
9	2017/8/30	要求仕様書 P1 1. 調達要件 (2) 調達対象	1.(2) 調達対象 1)設備 調達対象に「ラック及びラックマウントキット 2式」という記載があります。 調達するラックは、機器を収容可能なラックを受託者が選定するという理解でよろしいでしょうか。もし準拠すべき規定(寸法・重量・塗装色等)があれば指定をお願いします。	寸法・重量・塗装色等の指定はありませんので、機器を収容可能なラックを受託者にて選定ください。
10	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	3.(1) ①業務実施手順 - 設置・工事 「ラック、ラックマウントキットの敷設、電源工事及びインターネット回線の設置工事を行うこと」という記載があります。 ここでいう電源工事とは、電源ケーブルの敷設および分電盤への結線までを指し、電源引込み・分電盤の改造・壁面の穴あけ工事等は含まないという理解でよろしいでしょうか。	ご認識のとおりです。

「セキュリティログ監視等業務委託」に関する質問等

No.	質問日	仕様書等該当箇所 (ページ、項目等)	質問	回答
11	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	3.(1) ①業務実施手順－設置・工事 「ラック、ラックマウントキットの敷設、電源工事及びインターネット回線の設置工事を行うこと」「接続に必要となるネットワークケーブル等は、本業務の受託者にて用意すること」という記載があります。 「ラック」「既設デバイス」「分電盤」を結線する際の、配線ルートの概算距離をご教示ください。	ラック、既設デバイス、分電盤はいずれも同一フロアにあり、床下配線により今回新たに設置するラックまでの配線は、100m以下を想定してください。
12	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	3.(1) ①業務実施手順－設置・工事 「ラック、ラックマウントキットの敷設、電源工事及びインターネット回線の設置工事を行うこと」という記載があります。 ラック設置場所のフリーアクセス床の有無と、固定（耐震）方法に関する指定について教示ください。	ラック設置場所はフリーアクセス床になっています。メインサイトについては、受託者側でスラブにアンカーボルトで固定する工事を手配ください。バックアップサイトについては、架台の設置までをデータセンター側で実施します。
13	2017/8/30	要求仕様書 P4 2. 設備に関する要件 (1) 機能要件	Sandbox機能 「受信データを、検査用領域で実行(既知のマルウェアリストとの照合含む)し、マルウェアであるかの検査ができること」という記載があります。 運用環境に即したOSイメージを採用する事でSandbox精度向上に繋がる為、検査用領域で利用するOSイメージはお客様環境に合わせて構築すべきかをご教示下さい。	実現方法については指定はありませんが、要件を満たす最適なソリューションを検討のうえご提案ください。
14	2017/8/30	仕様書 P9 9. 再委託に関する事項 (1) 再委託の制限及び再委託を認める場合の条件	者に再委託することは不可。また、本業務の契約金額占める再委託金額は、原則2分の1未満とする。 上記再委託の対象となる調達対象は、要求仕様書1 ページ (2) 調達対象に記載の「2」役務」部分との理解で良いでしょうか？ 100%出資の子会社を利用する場合も、「再委託」に該当するとの理解で良いでしょうか？	再委託の対象となる調達対象は、要求仕様書P1 表1.1 調達対象のうち、「2) 役務」及び「4) サービス」となります。 また、100%出資の子会社を利用する場合も「再委託」に該当します。
15	2017/8/30	要求仕様書 P1 1. 調達要件 (2) 調達対象	サーバラックのサイズ指定はありませんので、小型のラックでも要件は満たすとの理解で良いでしょうか？ また データセンターに設置する際に、電源工事が必要なことは理解していますが、アンカーボルト等による耐震工事は不要との理解で良いでしょうか？	サーバラックのサイズ等の指定はありませんので、要件を満たすラックを提案事業者で検討のうえご提案ください。 メインサイトについては、架台の設置に当たってはスラブに対してアンカーボルトで固定することとさせていただきます。バックアップサイトはデータセンター側で架台の設置までを実施します。

「セキュリティログ監視等業務委託」に関する質問等

No.	質問日	仕様書等該当箇所 (ページ、項目等)	質問	回答
16	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	①表3.1 役務に係る業務要件 -業務手順 フェーズ“設置・工事” ラックの据付に際して耐震固定として、スタビライザーを用いた据付でよろしいでしょうか。(スラブに対してのアンカーボルト留めは想定しておりません)	スタビライザーを用いた据付ではなく、スラブに対してアンカーボルト固定することを想定しています。
17	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	①表3.1 役務に係る業務要件 -業務手順 フェーズ“設置・工事” 電源の配線工事について、同一フロア内のPD盤、電力盤を利用する想定でよろしいでしょうか。	ご認識のとおりです。
18	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	①表3.1 役務に係る業務要件 -業務手順 フェーズ“設置・工事” LAN配線工事について、ミラーのスイッチは同一フロア内にあり、床下配線により今回新たに設置するラックまで配線する(100m以下) 認識でよろしいでしょうか。	ご認識のとおりです。
19	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	①表3.1 役務に係る業務要件 -業務手順 フェーズ“設置・工事” 回線の開通に際して、データセンターのMDF～IDF～ラック設置場所の間の屋内配線については自営配線でしょうか。もしくはラック設置場所まで受注者側で手配する必要がありますでしょうか。	メインサイトについては、同一フロア内のIDF～ラック設置場所までの間の屋内配線を受注者側で手配してください。データセンターのMDF～IDFまでは、データセンターの屋内配線を借用することになるため、別途、屋内配線利用料(月額1万円程度)を見積に含めてください。 バックアップサイトについては、MDF～IDF～ラック設置場所の間の全てを受注者側で手配してください。
20	2017/8/30	要求仕様書 P9 3. 役務に関する要件 (1) 業務要件	今回納入する機材についてアースが必要となります。そのため、電源の配線工事と同様にアース線の配線工事も必要となるため、アースの端子盤をご提示願えますでしょうか。	メインサイトについては、同一フロア内のアースの端子盤からサーバ設置場所までの配線工事を受注者側で手配してください。 バックアップサイトについては、データセンター側でラック設置場所まで配線を行うため、配線工事の手配は不要です。