第２号議案

セキュリティログ監視システムの導入について
（案）

１．システム導入の計画及びプロジェクト計画の制定

「外部からの悪意ある攻撃を受けないようにするため適切なサイバーセキュリティ対策を講じる（業務規程第７条第４項)」ため、インターネット接続のセキュリティログを常時監視（２４時間３６５日）するセキュリティログ監視システムを新規に導入する。情報セキュリティ対策規程第７条が求める本システムの導入計画は、プロジェクト計画と一体のものとして、別紙１のとおり制定する。

２．重要システムの指定及びシステム管理者の選任

セキュリティログ監視システムは、ネットワーク設備の導入が必要であり、構築・運用・保守を含んだ予定価格が１億円以上となるため、情報セキュリティ対策規程第７条第２項に基づき本システムを重要システムに指定する。

また、情報セキュリティ対策規程第８条のシステム管理者として、総務部情報システムグループマネージャーを選任する。

３．セキュリティログ監視システムの導入、運用及び保守を委託により行うこととし、以下のとおり、委託先選定のための入札を実施する。

（１）調達方式

一般競争入札（総合評価方式）

（２）入札スケジュール

平成 29 年 8 月 10 日（木）	公告
平成 29 年 8 月 24 日（木）14 時開始	入札説明会
平成 29 年 8 月 30 日（水）17 時迄	入札に関する問い合わせ締切
平成 29 年 9 月　1 日（金）迄	問い合わせに対する回答を公表
平成 29 年 9 月 15 日（金）15 時必着	入札書・提案書等提出締切
平成 29 年 9 月 20 日（水）	技術審査プレゼンテーションの実施
平成 29 年 9 月 29 日（金）迄	落札者の決定

（３）入札説明書（仕様書を含む。）

入札説明書は、別紙入札説明書一式のとおり。なお、公告時にウェブサイト上で開示する。

（４）落札者の決定

総合評価結果に基づく落札者の決定及び落札者との契約の締結については、別途、理事会に付議する。

以　上

【添付資料】

別紙１：セキュリティログ監視システム開発のプロジェクト計画書

別紙２：入札説明書一式（内訳：入札説明書、入札書、仕様書、応札資料作成要領、評価項目一覧、評価手順書）

別紙２

セキュリティログ監視等業務委託

入　札　説　明　書

電力広域的運営推進機関

内　　訳

入　札　説　明　書
入　札　書
仕　様　書
応札資料作成要領
評　価　手　順　書
評　価　項　目　一　覧

入 札 説 明 書

電力広域的運営推進機関

電力広域的運営推進機関の「セキュリティログ監視等業務委託」に係る入札公告（平成２９年８月１０日付け公示）に基づく入札については、下記に定めるところによる。

記

１．競争入札を実施する事項

（１）件 名　　セキュリティログ監視等業務委託
（２）委 託 内 容　別紙仕様書のとおり。
（３）調 達 方 式　一般競争入札（総合評価落札方式）
（４）履 行 期 限　別紙仕様書のとおり。
（５）納 入 場 所　別紙仕様書のとおり。
（６）入 札 方 法　入札金額は、「セキュリティログ監視等業務委託」に関する総価で行う。
なお、本件については入札の際に提案書を提出し、技術審査を受けなければならない。落札決定に当たっては、入札書に記載された金額に当該金額の８パーセントに相当する額を加算した金額（当該金額に１円未満の端数が生じたときは、その端数金額を切捨てるものとする。）をもって落札価格とするので、入札者は消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積った契約金額の１０８分の１００に相当する金額を入札書に記載すること。

２．競争参加資格

（１）平成２８・２９・３０年度の競争参加資格（全省庁統一資格）において、「役務の提供等」で等級「Ｃ」以上の格付けをされている者であること。
（２）各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止を受けていない者であること。
（３）入札説明会に参加した者であること。
（４）予算決算及び会計令(昭和２２年勅令第１６５号)第７０条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
（５）予算決算及び会計令第７１条の規定に該当しない者であること。
（６）会社更生法（平成１４年法律第１５４号）に基づく更生手続開始の申立て又は民事再生法（平成１１年法律第２２５号）に基づく再生手続開始の申立てがなされている者でないこと（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く）。
（７）自己、自社若しくはその役員等（注１）が、暴力団員による不当な行為の防止等に関する法律第２条に定める暴力団、暴力団員又はその他反社会的勢力（注２）でない者であること。

（注１）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している者。
（注２）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から５年を経過しない者等、その他これに準じる者。

（８）破壊活動防止法に定めるところの破壊的団体およびその構成員でない者であること。
（９）入札者又は入札者の協力会社（社名を提出のこと）が経済産業省公表の「平成 28 年度 情報セキュリティ監査企業台帳（2017.5.10 版）」において以下に定める項目に該当すること。
(ア)「地域名」に「関東」を登録していること。

(イ)「IT 関連業務」に「セキュリティ監査」を登録していること。
(ウ)「セキュリティ関連業務」に「セキュリティシステム設計／構築」、「リスク評価／脆弱性評価サービス」及び「システム監査、コンサルティング」を登録していること。
(エ)「セキュリティ監査対象の分野・業種」に「公務（官公庁・自治体 等）」を登録していること。
(オ)「監査従事者が持つ取得済監査関連資格」に「公認情報システム監査人（CISA）」、「公認情報セキュリティ監査人」または「情報セキュリティスペシャリスト」を登録していること。
(カ)「取得している監査関連の認証」に「ISMS 適合性評価制度」または「プライバシーマーク(JIS Q 15001)」を登録していること。
（10）政府機関の情報セキュリティ対策のための統一基準群について理解し、電力事業者又は行政機関に対するセキュリティログ等監視業務の導入及び運用実績があること。

３．入札者の義務

この一般競争入札に参加を希望する者は、電力広域的運営推進機関が交付する仕様書に基づいて提案書を作成し、これを入札書に添付して入札書の提出期限内に提出しなければならない。

また、落札者決定までの間において電力広域的運営推進機関の職員から当該書類に関して説明を求められた場合は、これに応じなければならない。なお、入札者の作成した提案書は電力広域的運営推進機関において審査するものとし、採用し得ると判断した提案書を添付した入札書のみを落札決定の対象とする。

４．入札書・提案書・入札資格確認書類の提出期限、提出書類及び提出先

提出期限： 平成２９年９月１５日（金）１５時必着で必要書類を郵送または持参すること。

提出書類：・全省庁統一資格　資格審査結果通知書（写）
・入札書・・・別途封入すること
・提案書
・契約書（案）・・・環境構築、保守及びサービス含む
・適合証明書

提 出 先：〒１３５－００６１　東京都江東区豊洲６－２－１５
電力広域的運営推進機関　総務部経理グループ
セキュリティログ監視等業務委託　入札係

５．技術審査のプレゼンテーションの日時及び場所

平成２９年９月２０日（水）
時間、場所については、入札者に別途連絡の上調整

６．競争参加者は、提出した入札書の変更及び取消しをすることができない。

７．入札の無効

次の各号の一に該当する入札は、無効とする。
①「２．競争参加資格」に示した競争参加資格のない者による入札
②記名押印（外国人又は外国法人にあっては、本人又は代表者の署名をもってかえることができる。）を欠く入札
③金額を訂正した入札
④誤字、脱字等により意思表示が不明瞭である入札
⑤明らかに連合によると認められる入札
⑥提案書が電力広域的運営推進機関の審査の結果採用されなかった入札

⑦入札書提出期限までに到着しない入札
⑧その他入札に関する条件に違反した入札

８．落札者の決定方法

電力広域的運営推進機関が設定する予定価格の制限の範囲内で、電力広域的運営推進機関が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、電力広域的運営推進機関が定める総合評価の方法をもって落札者を定めるものとする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者とすることがある。

なお、開札をした場合において、各人の入札のうち予定価格の制限に達した価格の入札が無い場合は、各人に連絡の上、後日、再度入札を行う。

また、落札となるべき同総合評価点の入札をした者が２者以上あるときは、各人に連絡の上、当該入札をしたものにくじを引かせて落札者を決定する。

９．入札保証金及び契約保証金　免除

１０．契約書作成の要否 要

１１.契約書の記載内容

（１）契約書は仕様書に定める環境構築、保守及びサービスの内容全てを含むこととする。なお、環境構築、保守及びサービスにてそれぞれ別の契約書することも可能とする。

１２．支払の条件

（１）契約代金は、契約書記載の条件により、精算払請求書の受領日から３０日以内に支払うものとする。

１３．入札書等に使用する言語及び通貨

（１）入札書、提案書、契約書（案）、技術審査のプレゼンテーション等に使用する言語は日本語とし、通貨は日本国通貨に限る。

１４．落札決定の取消し

（１）落札決定後であっても、この入札に関して連合その他の事由により正当な入札ではないことが判明した時は、電力広域的運営推進機関は落札決定を取消すことができる。

１５．その他

（１）競争参加者は、提出した証明書等について説明を求められた場合は、自己の責任において速やかに書面をもって説明しなければならない。

（２）本入札結果については、落札者との契約締結後、原則として、契約相手方、契約締結日及び契約金額等の契約概要を公表する。

（３）この入札に関して不明な点は、平成２９年８月３０日（水）１７時までに下記問い合わせ先へ、電子メールで問い合わせることができる。問い合わせへの回答は、平成２９年９月１日（金）までに電力広域的運営推進機関ウェブサイトの本入札公告上に開示する。

【問い合わせ先】
電力広域的運営推進機関　総務部経理グループ（契約担当）
メールアドレス：keiyaku@occto.or.jp
【ウェブサイト】http://www.occto.or.jp/oshirase/chotatu/index.html

（様　式）

平成　　年　　月　　日

電力広域的運営推進機関　御中

住　　所

商号又は名称

代 表 者 氏 名　　印

入　札　書

入札金額　　￥

内訳　　別添支出計画書のとおり。

入札事項　　セキュリティログ監視等業務委託

貴機関「入札説明書」の内容を承知の上入札いたします。

（別　添）

支出計画書

【参考例】

区分	内訳	金額（円）	積算内訳
１．環境構築費用	・SOC 監視用セキュリティデバイス ・Internet VPN デバイス ・インターネット回線 ・ラック関連 ・その他工事費等 ・プロジェクト管理費	000,000,000	・SOC 監視用セキュリティデバイス 〇〇〇・・・z,zzz,zzz ・Internet VPN デバイス 〇〇〇・・・z,zzz,zzz ・インターネット回線 〇〇〇・・・z,zzz,zzz ・ラック・・・z,zzz,zzz ・ラックマウントキット・・・z,zzz,zzz ・電源工事・・・z,zzz,zzz （注１：調達対象機器の一覧を記載すること） ・プロジェクト管理費・・・z,zzz,zzz
２．保守に係る費用(年額)	・基本費用 ・プロジェクト管理費	000,000,000	・機器保守費用 〇〇〇・・・z,zzz,zzz ・プロジェクト管理費・・・z,zzz,zzz
３．サービスに係る費用(年額)	・ログ監視基本費用 ・オプション費用 ・プロジェクト管理費	000,000,000	・ログ監視基本費用 〇〇〇・・・z,zzz,zzz ・ログ長期保存オプション 〇〇〇・・・z,zzz,zzz ・プロジェクト管理費・・・z,zzz,zzz
４．保守及びサービスに係る費用計(年額)			２．保守に係る費用＋３．サービスに係る費用
５．保守及びサービスに係る費用計(5 年分)			４．保守及びサービスに係る費用計(年額)×5 年
６．合計			１．環境構築費用＋５．保守及びサービスに係る費用計(5 年分) （注２：入札金額と一致）

（様　式）

質問状

社名			
住所			
TEL		FAX	
質問者			
質問に関連する文書名及び頁			
質問内容			

電力広域的運営推進機関

セキュリティログ監視等業務委託

仕様書

電力広域的運営推進機関

電力広域的運営推進機関

目次

1.調達案件の概要に関する事項

(1) 調達件名

セキュリティログ監視等業務委託

(2) 調達の背景

電力広域的運営推進機関（以下「本機関」という。）においては、政府機関全体としてのサイバーセキュリティ強化の取り組み方針等を踏まえ、昨年度までに本機関が所有するシステムについて外部監査やペネトレーションテスト等を実施する等のサイバーセキュリティ対策を実施してきている。

今般、さらなるセキュリティ対策として、ファイアウォール等の通信機器や情報システムのセキュリティログからの異常検出及びアラート通知を行う技術的対策の導入及びセキュリティログの 24 時間監視、相関分析等の監視を行う Security Operation Center（以下「SOC 業務」という。）を導入することとした。

(3) 目的及び期待する効果

本調達は、本機関内のセキュリティログを 24 時間監視し、相関分析等を行い、以下の効果を実現する。

・対応時間の短縮・・・収集した過去のセキュリティログを調査することで、被害状況の特定までに必要となる人的な作業量を削減し、対応完了までの時間を短縮する。

・被害の低減・・・内部に侵入したマルウェアが外部の C&C サーバと通信を繰り返している段階で、異常を検知して対応することで、重大な情報漏えいの拡大を阻止する。

(4) 用語の定義

本仕様書で使用する用語の定義を以下に示す。

表 1-1 用語の定義

用語	定義
OA システム	本機関のインターネット接続を唯一保有し、役職員にメール、ファイル共有等の OA 環境を提供するシステム メインサイトとバックアップサイトの 2 拠点に設置している
既設スイッチ	OA システム内に既に設置されているスイッチ
C&C サーバ	悪意のあるソフトウェアに感染したコンピュータ群に指令を送るサーバ
SOC	本機関向けにセキュリティログの 24 時間監視、相関分析等の監視を行う組織又はサービス
SOC 監視用セキュリティデバイス	既設スイッチのミラーポートより受信したパケットをもとに、セキュリティ検査を行い、ログを記録し、SOC に送信する機器
Internet VPN デバイス	SOC と暗号化された通信経路を構築するために、サイト間 VPN を提供する機器
メインサイト	OA システムが通常に稼働する東京江東区のデータセンター

バックアップサイト	OA システムが災害等の大規模障害時にメインサイトから引き継いで稼働する大阪北区にあるデータセンター
運用細則	SOC 業務の運用にあたり、情報を適正に管理し、恒常的に情報セキュリティ対策を維持することを目的に、今後、本機関が定めるシステム運用の基本的ルール

(5) 業務・情報システムの概要

本調達における業務・情報システムは OA システムを対象に以下のとおり想定している。

① 既存システムである OA システム内に SOC 監視用セキュリティデバイスが検査するネットワークポイントを設定する。・・・導入時における OA システムに対する必要な設定変更等は本機関にて実施

② SOC 監視用セキュリティデバイスを設置し、OA システムの通信パケットに対して当該デバイスにてセキュリティ検査を実施する。

③ SOC 監視用セキュリティデバイスは各セキュリティ検査で取得したログを SOC にリアルタイムで転送する。

④ SOC は SOC 監視用セキュリティデバイスからのログを取得・保管し、リアルタイムで分析する。

⑤ SOC にてインシデントを検知した場合は本機関に通知し対応を協議する。

詳細については、別紙「セキュリティログ監視等業務委託要求仕様書」を確認のこと。

(6) 契約期間・作業スケジュール

① 環境構築については、契約締結日から平成 30 年 1 月末まで

② 保守については、機器導入時から平成 35 年 1 月末まで

③ サービスについては、平成 30 年 2 月から平成 35 年 1 月末まで（5 年運用）

2. 調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

(1) 調達案件及びこれと関連する調達案件の調達単位

関連する調達案件は以下のとおり

表 2-1 関連調達案件

項番	調達案件名	調達の方式	実施時期
1	セキュリティログ監視等業務の要件定義に係る業務委託	一般競争入札 （最低価格落札方式）	平成 29 年 7 月
2	セキュリティログ監視システム導入に伴う OA システムの改修	随意契約	平成 29 年 10 月

(2) 調達案件間の入札制限

公平性の観点から上記 2.(1)の項番 1 の受託者は入札制限の対象とする。

3. 作業の実施内容に関する事項

(1) 作業の内容

作業の実施内容は以下を想定している。

なお、詳細は別紙 「セキュリティログ監視等業務委託要求仕様書」を参照のこと。

Ａ．環境構築

① プロジェクト計画／管理

本作業の実施にあたり、目的、実施体制、役割、作業内容と作業方法、作業スケジュール、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること

② 要件確認

本機関における要件について、受託者との認識のずれや齟齬がないことを確認すること

③ 設計

確認した要件に基づき、基本設計、運用設計、試験設計、移行設計を行うこと。

④ 構築

設計に基づき、システムをセットアップすること。

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。

⑥ 試験

試験設計に基づき、システムの試験を実施すること。また、SOC と連携し、ログファイルの授受や SOC 業務のシナリオ試験を実施すること。

⑦ SIEM ルールのチューニング

試験設計に基づき、システムの試験を実施すること。また、SOC と連携し、ログファイルの授受や SOC 業務のシナリオ試験を実施すること。

Ｂ．保守

① プロジェクト計画／管理

本作業の実施にあたり、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること

② 保守

運用細則及び環境構築作業にて作成した運用設計書に基づき、作業計画書を策定のうえ、導入した機器に関する稼働監視やシグネチャ更新等を実施すること。

Ｃ．サービス

① プロジェクト計画／管理

本作業の実施にあたり、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること

② サービス

運用細則及び環境構築作業にて作成した運用設計書に基づき、インシデントの監視、検知、通知等の業務を実施すること。

(2) 成果物の範囲、納品期日等

A．環境構築

本調達における想定している調達機器（設備）は以下のとおりであり、受託者は作業の詳細スケジュールと併せて、納品予定日をプロジェクト計画書等に記載すること。

また、追加の調達機器（設備）などがあれば提案書に記載すること。

なお、設置場所については、メインサイト及びバックアップサイトの本機関が指定する場所とする。

表 3-1 調達機器（設備）

調達機器（設備）	数量
SOC 監視用セキュリティデバイス	2 式
Internet VPN デバイス	2 台
インターネット回線	2 本（5 年分）
UTP ケーブル、スイッチ	適量
ラック及びラックマウントキット	2 式

B．保守

本調達における想定している保守は以下のとおりである。

また、追加の保守などがあれば提案書に記載すること。

表 3-2 保守内容

保守内容	数量
SOC 監視用セキュリティデバイス	2 式*5 年分
Internet VPN デバイス	2 台*5 年分

C．サービス

本調達におけるサービスは以下のとおりである。

表 3-3 サービス内容

サービス	数量
SOC	5 年分

D．本調達に係る付帯業務

① 成果物・提出物

付帯業務において想定している成果物は以下のとおりであり、受託者は作業の詳細スケジュールと併せて、納品予定日をプロジェクト計画書等に記載すること。

また、追加の成果物があれば提案書に記載すること。

表 3-1 作業の内容と成果物

作業の内容	作業の内容	成果物
A．環境構築	プロジェクト計画／管理	プロジェクト計画書
		進捗管理表
		課題管理表
		リスク管理表
		会議議事録
	設計	基本設計書
		運用設計書
		試験設計書
		移行設計書
	試験	試験結果報告書
B．保守	プロジェクト計画／管理	プロジェクト計画書
	保守	作業計画書
		月次報告書
C．サービス	プロジェクト計画／管理	プロジェクト計画書
	サービス	運用マニュアル
		インシデント報告書
		月次報告書

② 納品方法

項番	分類	要件
1	言語	・成果物は、全て日本語で作成すること。ただし、日本国においても、英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。
2	準拠すべき規格	・用字・用語・記述符号の表記については、「公用文作成の要領（昭和 27 年４月４日内閣閣甲第 16 号内閣官房長官依命通知）」に準拠すること。 ・情報処理に関する用語の表記については、原則、日本工業規格（ＪＩＳ）の規定に準拠すること。

3	納品形態	・成果物は電磁的記録媒体（ＣＤ-Ｒ等）により作成し、本機関から特別に示す場合を除き、原則電磁的記録媒体は 2 部を納品すること。なお、保守及びサービスの成果物については、メールでの納品も可能とする。 ・紙媒体による納品について、用紙のサイズは、原則として日本工業規格Ａ列４番とするが、必要に応じて日本工業規格Ａ列３番を使用すること。また、バージョンアップ時等に差し替えが可能なようにバインダ方式とすること。 ・電磁的記録媒体による納品について、MicrosoftWord2013 、同 Excel2013 又は同 PowerPoint2013 で読み込み可能な形式、及びＰＤＦ 形式で作成し、納品すること。なお。これらは原則として文字列検索機能を活用して文字列が検索可能な状態のものを納品すること。ただし、本機関が他の形式による提出を求める場合は、協議の上、これに応じること。なお、受託者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。
4	セキュリティ対策	・成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。 ・電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行う等して、成果物に不正プログラムが混入することのないよう、適切に対処すること。
5	留意事項	・納品後、本機関において改変が可能となるよう、図表等の元データも併せて納品すること。 ・成果物の作成にあたって、特別なツールを使用する場合は、本機関の承認を得ること。

③ 納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、本機関が納品場所を別途指示する場合はこの限りではない。

〒135-0061

東京都江東区豊洲 6-2-15

電力広域的運営推進機関　総務部情報システムグループ

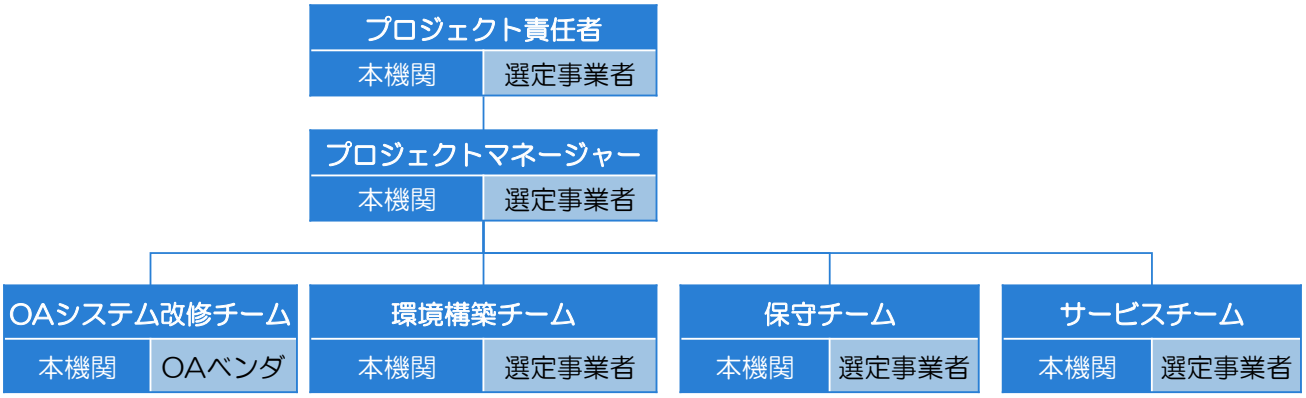
4. 満たすべき要件に関する事項

本調達の実施に当たっては、別紙「セキュリティログ監視等業務委託要求仕様書」の各要件を満たすこと。

5. 作業の実施体制・方法に関する事項

(1) 作業実施体制

本プロジェクト実施に当たり、以下の体制図及びその従事する人数について記載すること



(2) 作業場所

別紙「セキュリティログ監視等業務委託要求仕様書」に従うものとする。

(3) 作業の管理に関する要領

別紙「セキュリティログ監視等業務委託要求仕様書」に従うものとする。

6. 作業の実施に関する事項

(1) 機密保持、資料の取扱い

本機関から受託者に提供する秘密情報及び秘密情報を記録した資料等は、本契約期間中の如何を問わず、第三者に開示、漏えい又は他の目的に使用しないこと。ただし第三者に開示の必要性がある場合は、開示方針や漏えいの防止策を明示し本機関の承認を得ること。

(2) 遵守する法令等

① 本仕様書に示す業務の実施に当たっては、次の文書に記載された事項を遵守すること。

ア　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

イ　政府機関の情報セキュリティ対策のための統一基準

ウ　本機関の情報管理セキュリティ関連規程

② 受託者は、現行情報システムの設計書等を参照する必要がある場合は、作業方法等について本機関の指示に従い、秘密保持契約を締結する等した上で、作業すること。

③ 受託者は、受託業務の実施において、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、個人情報の保護に関する法律等の関連する法令等を遵守すること。

7. 成果物の取扱いに関する事項

(1) 検収

① 本仕様書に則って成果物を提出すること。

② 検査の結果、成果物の全部又は一部に不合格品を生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、指定した日時までに修正が反映された全ての成果物を納入すること。

③ 本仕様書以外にも、必要に応じて成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。

8. 入札参加資格に関する事項

(1) 入札参加要件

① 平成２８・２９・３０年度の競争参加資格（全省庁統一資格）において、「役務の提供等」で等級「C」以上の格付けをされている者であること。

② 各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止を受けていない者であること。

③ 入札説明会に参加した者であること。

④ 予算決算及び会計令(昭和２２年勅令第１６５号)第７０条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

⑤ 予算決算及び会計令第７１条の規定に該当しない者であること。

⑥ 会社更生法（平成１４年法律第１５４号）に基づく更生手続開始の申立て又は民事再生法（平成１１年法律第２２５号）に基づく再生手続開始の申立てがなされている者でないこと（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く）。

⑦ 自己、自社若しくはその役員等（注１）が、暴力団員による不当な行為の防止等に関する法律第２条に定める暴力団、暴力団員又はその他反社会的勢力（注２）でない者であること。

（注１）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している
（注２）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から５年を経過しない者等、その他これに準じる者。

⑧ 破壊活動防止法に定めるところの破壊的団体及びその構成員でない者であること。

⑨ 入札者又は入札者の協力会社（社名を提出のこと）が経済産業省公表の「平成 28 年度 情報セキュリティ監査企業台帳（2017.5.10 版）」において以下に定める項目に該当すること。

ア 「地域名」に「関東」を登録していること。

イ 「IT 関連業務」に「セキュリティ監査」を登録していること。

ウ　「セキュリティ関連業務」に「セキュリティシステム設計／構築サービス」、「リスク評価／脆弱性評価サービス」及び「システム監査、コンサルティング」を登録していること。

エ　「セキュリティ監査対象の分野・業種」に「公務（官公庁・自治体 等)」を登録していること。

オ　「監査従事者が持つ取得済監査関連資格」に「公認情報システム監査人（CISA)」，「公認情報セキュリティ監査人」又は「情報セキュリティスペシャリスト」を登録していること。

カ　「取得している監査関連の認証」に「ISMS 適合性評価制度」又は「プライバシーマーク(JIS Q 15001)」を登録していること。

⑩ 政府機関の情報セキュリティ対策のための統一基準群について理解し、電力事業者又は行政機関に対するセキュリティログ等監視業務の導入及び運用実績があること。

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

① 受託者は本仕様書に示す業務の全部又は総合的な企画及び判断並びに業務遂行管理部分を第三者に再委託することは不可とする。また、本業務の契約金額に占める再委託契約金額は、原則2分の1未満とする。

② 本仕様書「2.(2)調達案件間の入札制限」に該当する事業者は本項における再委託先となることはできない。

③ 受託者は、知的財産権、情報セキュリティ（機密保持及び遵守事項)、ガバナンス等に関して本仕様書が定める受託者の債務を、再委託先事業者も負うような必要な処置を実施すること。

④ 再委託者、再委託者が業務を委託する第三者（以下「再々委託者」という。）及び再々委託者が業務を第三者へ委託する場合の責任は受託者が負うこと。

⑤ 以下に示すものについても本仕様書「6 作業の実施に当たっての遵守事項」に示した事項を遵守させること。

ア　再委託者

イ　再々委託者

ウ　再々委託者が業務を委託する第三者

(2) 承認手続

① 本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性、契約予定金額について本機関に提出し、承認を受けること。

② 再委託の相手方からさらに第三者に委託が行われる場合には、当該第三者の商号又は名称及び住所並びに委託を行う業務の範囲について本機関に提出すること。

10. その他特記事項

(1) 前提条件及び制約条件

・本仕様書は、受託者に業務遂行を求める最低限の基準を示したものである。したがって、本仕様書

に記載していない事項であっても、本調達に必要と認められる事項は、本機関と追加負担を含め協議の上、これを行うこと。

・本件受託後に本仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって、本機関に申し入れを行うこと。

・受託者は、業務の遂行に当たり、本機関の作業負荷等を十分考慮すること。

・受託者のプロジェクトマネージャーは、業務の円滑な運営を図るため、本機関との連絡を密にして業務を遂行すること。

・本機関から貸し出された資料又は支給を受けた物品等については、善良なる管理者の注意をもって保管及び管理するものとし、紛失又は破損の場合直ちに本機関に報告し、本機関の指示に従って措置を講ずること。

・受託者は、常に作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、労働基準法、労働安全衛生法等を遵守して安全の徹底を図り、作業を行うこと。

・受託者が行う提案や報告及び相談等は全て書面を持って実施し、内容については、本機関の承認を得ること。

・本仕様書に記載したスケジュールは現時点での想定である。スケジュール変更があった場合の対応については、本機関と協議の上、決定すること。

11. 附属文書

別紙「セキュリティログ監視等業務委託要求仕様書」

以上

セキュリティログ監視等業務委託

要求仕様書

電力広域的運営推進機関

電力広域的運営推進機関

目次

1.調達要件

(1) 調達物品に係る用語定義

本調達に係る主要なコンポーネントを次のとおり定義する。

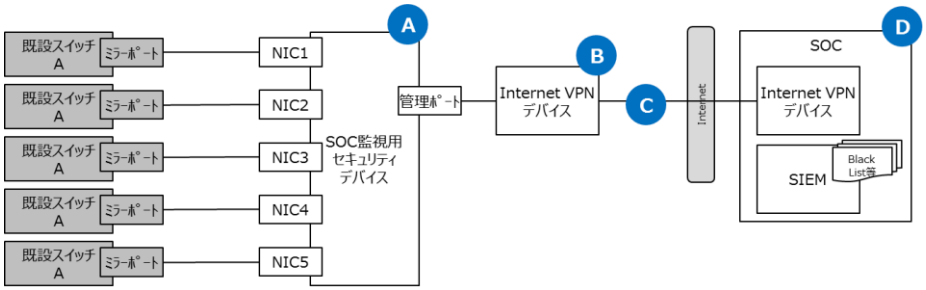


図 1.1 調達物品の定義

#	機器名	用途
A	SOC 監視用 セキュリティデバイス	既設スイッチのミラーポートより受信したパケットをもとに、セキュリティ検査を行い、ログの記録及びログを SOC に送信する役割を担う
B	Internet VPN デバイス	SOC と暗号化された通信経路を構築するために、サイト間 VPN を提供する役割を担う
C	インターネット回線	SOC との通信経路を提供する役割を担う
D	SOC	本機関向けにセキュリティログ監視業務を提供する組織又はサービスをいう

(2) 調達対象

(1)の用語定義に基づき、調達対象を次に記載する。なお、本機関における既設の設備に係る設計作業や設定変更作業は、調達の範囲外とする。

表 1.1 調達対象

カテゴリ	調達対象		数量
1) 設備	A	SOC 監視用セキュリティデバイス	2 台（※）
	B	Internet VPN デバイス	2 台
	C	インターネット回線	2 本*5 年分
	-	UTP ケーブル、スイッチ	適量
	-	ラック及びラックマウントキット	2 式
2) 役務	A, B, C, D	要件確認	1 式
	A, B, C, D	設計	1 式
	A, B, C, D	構築	1 式
	A, B, C	設置・工事	1 式
	A, B, C, D	試験	1 式
	D	チューニング	1 式
3) 保守	A	SOC 監視用セキュリティデバイス	2 台*5 年分

	B	Internet VPN デバイス	2 台*5 年分
4) サービス	D	SOC	5 年分

（※）単一製品でなく、優れる製品の組み合わせでも可

(3) 調達対象となる数量の考え方

本機関では、同一構成となるメインサイトとバックアップサイトを保有している。
本調達に係る設備は、メインサイトとバックアップサイトに配備するため、前述 表 1.1 の「1)設備、3)保守」の数量はバックアップサイトを含む数量となっている。

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。
このため、SOC 等のサービス費の見積もりにあたっては、監視対象となるアクティブな環境は、いずれか一方の環境（アクティブ-スタンバイ構成）であることに十分留意すること。

(4) サービス継続性の考え方

本機関における事業及びシステムは、前述(3)のとおりメインサイトとバックアップサイトを構築するなどサービス継続性をより重要視している。
今回調達する SOC サービスについても、可能な限り地震、災害などの発生時にも SOC サービスが継続できるよう関連設備や業務実施拠点などの DR 対応を希望している。
上記背景を理解のうえ、SOC サービスの継続性について入札者の対策状況を提案書に記述いただきたい。

(5) SOC 監視用セキュリティデバイスのポート数の考え方

SOC 監視用セキュリティデバイスは、既設スイッチの 5 か所のミラーポートから通信を受信する必要がある。
本機関におけるメインサイトの既存システムは、スイッチを含め冗長化構成としていることから、既設スイッチのミラーポートはアクティブ系スイッチ 5 ポート、スタンバイ系スイッチ 5 ポートの計 10 ポートとなる。バックアップサイトの既存システムは、シングル構成としていることからミラーポートはアクティブ系スイッチ 5 ポートとなる。
入札者においては、上記を理解のうえ、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か、既設スイッチと 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配置して通信を束ねるかなど、最適なソリューションを検討のうえ提案いただきたい。

2. 設備に関する要件

(1) 機能要件

本書で調達する設備に関する機能要件は次のとおりとする。

表 2.1 設備に係る機能要件

項目	内容
SOC 監視用セキュリティデバイスに関する要件	
TAP モード機能	・ スイッチ(ミラーポート)に接続のうえ、当該スイッチから SOC 監視用セキュリティデバイスに届く通信パケットに対して、「FW」「IDS」「URL フィルタ」「AntiVirus」「Sandbox」のセキュリティ検査を実施すること
FW 機能	・ 送信元/宛先 IP アドレス、プロトコル（ポート番号）に基づく通信ポリシーを設定できること ・ ポリシーにマッチした通信に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、データサイズ、セッション時間」を含むこと ※本機能はポリシーに基づくログ収集機能であり、通信制御を求めているものではない。
IDS 機能	・ シグネチャ（攻撃パターンのプロファイル）とのパターンマッチングによる攻撃の検知ができること ・ シグネチャにマッチした通信に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、シグネチャ名」を含むこと ・ パターンマッチングにより攻撃と判断した場合には、当該通信の PCAP データを取得すること
URL フィルタ機能	・ URL カテゴリ（Web サイトの種別リスト）とのパターンマッチングによる通信先となる Web サイトの分類ができること ・ 「クライアントから Proxy サーバ間の通信」、「Proxy サーバから Internet 間の通信」に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、URL、プロトコル、カテゴリ名」を含むこと ※本機能はパターンマッチングによるログ収集であり、特定の URL へのアクセス制御を求めているものではない。
AntiVirus 機能	・ パターンファイル（ウィルス、マルウェアのプロファイル）とのパターンマッチングによる不審ファイルの検査ができること ・ パターンファイルにマッチしたデータに対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、ウィルス名」を含むこと

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を含む）し、マルウェアであるかの検査ができること ・ マルウェアと判断した通信に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、マルウェア名」を含むこと
ログ管理機能	・ 各種セキュリティ機能で取得したログを Syslog プロトコルで、SOC にリアルタイムで転送すること ・ デバイスが記録したログは可能な限りデバイス内の記憶領域に保存し、本機関の要求に応じてログを提出できること
Internet VPN デバイスに関する要件	
FW 機能	・ 送信元/宛先 IP アドレス、プロトコル（ポート番号）に基づく通信ポリシーを設定できること
VPN 機能	・ 本機関と SOC との Site to Site の Internet VPN が構築できること。なお、VPN の機能及び動作仕様は、対向機器となる SOC デバイスと互換性のあるものとする
NAT 機能	・ SOC 監視用セキュリティデバイスからインターネットへの通信をグローバル IP アドレスに NAT すること ・ SOC 監視用セキュリティデバイスから SOC 設備への通信を SOC が指定するプライベート IP アドレスに NAT すること
インターネット回線に関する要件	
通信機能	・ SOC 監視用セキュリティデバイスから SOC、及び SOC 監視用セキュリティデバイスからインターネットに接続できること
グローバルアドレス	・ 固定のグローバル IP アドレスを少なくとも１つは利用できること
各デバイス共通の要件	
管理機能	・ 管理者によるオペレーションは、HTTPS や SSH など暗号化されたプロトコルが利用できること ・ 管理者のログインに対して、ID、パスワードによる認証、及び送信元 IP アドレスによる制御を行うこと
証跡管理	・ 管理者の設定変更履歴をログとして記録させること。ログには、少なくとも「時間、アカウント名/操作元 IP アドレス、操作内容」を含むこと ・ デバイスが記録したログは可能な限りデバイス内の記憶領域に保存し、本機関の要求に応じてログを提出できること
時刻同期	・ タイムゾーンは Asia/Tokyo（UTC+09:00）とし、本機関が指定する NTP サーバと同期できること
バックアップ機能	・ 機器の機能停止を伴わずにバックアップが取得できること

監視機能	・ SNMP 等のスタンダードプロトコルを用いた稼働監視・パフォーマンス監視に対応していること ・ ハードウェア等の障害が発生した場合に、SNMP Trap やエラーメールなどの通知機能を有すること
電圧	・ 100V 対応機器であること

(2) **非機能要件**

① 規模及び性能

本書で調達する設備に関する規模及び性能について記載する。本機関の通信量を考慮し、十分な性能が発揮できる機種及び回線を選定すること。

表 2.2 設備に係る非機能要件-規模

項目	内容
SOC 監視用セキュリティデバイスに関する要件	
監視対象となるシステムの規模	・ SOC 監視用セキュリティデバイスの検査対象となる本機関のメインサイトは、以下の規模とする 利用者数）150 名 端末数） 300 台
監視対象	・ デバイスが検査する（TAP する）ネットワークポイントは 5 か所とする（既存スイッチのアクティブ系 5 ポート、スタンバイ系 5 ポート）
通信量	・ デバイスが検査するポイントのそれぞれの通信量は下記のとおりとする ポイント 1）インターネット-FW 間 帯域 100Mbps：平均 11Mbps：ピーク 97Mbps ポイント 2）FW-DMZ 間 帯域 1Gbps：平均 22Mbps：ピーク 195Mbps ポイント 3）FW-内部ネットワーク間 帯域 1Gbps：平均 11Mbps：ピーク 97Mbps ポイント 4）内部 FW-内部サーバセグメント間 A 帯域 1Gbps：平均 22Mbps：ピーク 195Mbps ポイント 5）内部 FW-内部サーバセグメント間 B 帯域 1Gbps：平均 22Mbps：ピーク 195Mbps ※平均：過去 1 年間における 1 日平均の最大値 ※ピーク：過去 1 年間における 1 日の最大値
同時セッション	・ デバイスが検査するポイントのそれぞれのセッション数は不明であるため、通信量をもとに受託者にて推測のうえ提案すること

Internet VPN デバイスに関する要件	
通信量	・ SOC 監視用セキュリティデバイスが SOC に送信するログ量を主たる通信量として考えること。なお、当該デバイスが出力するログ量（EPS）は、現時点で不明なため、受託者の実績をもとに推測のうえ提案すること
VPN トンネル数	・ VPN トンネル数は、SOC 間と接続で必要となるスペックとすること
インターネット回線に関する要件	
通信量	・ SOC 監視用セキュリティデバイスが SOC に送信するログ量を含む本機関と SOC 間の通信量を推測のうえ提案すること ・ SOC 監視用セキュリティデバイスがシグネチャダウンロードなどインターネットにアクセスする通信量を踏まえ提案すること

② 信頼性・拡張性

本書で調達する設備に求める信頼性及び拡張性について記載する。

表 2.3 設備に係る非機能要件-信頼性

項目	内容
各デバイス共通の要件	
稼働時間	・ 24 時間 365 日の運用を前提とし、定期的な再起動やバージョンアップ以外の保守時の停止を要さないこと
耐障害性	・ シングル構成とするが、耐障害性の高い機器を選定すること
信頼性	・ 調達対象の設備に障害が発生しても、本機関の業務に影響を与えない製品を選定すること
バックアップ	・ 設定ファイルは、設定変更後の状態をリカバリポイントとすること。ただし、デバイス内に記録するログ等のデータは、リカバリ対象から除く
拡張性	・ 監視対象となる通信量が 1.5 倍となった場合でも、設備増強を必要としない製品を選定すること

③ 情報セキュリティ

本書で調達する設備に求めるセキュリティについて記載する。本書の要件に鑑み、追加で考慮すべきセキュリティ施策がある場合は、本機関に提案すること。

表 2.4 設備に係る非機能要件-情報セキュリティ

項目	内容
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

管理者アクセス	・ 本機関が指定する担当者に対して、管理者用画面を提供すること ・ 複数回の認証エラーは、アカウントロックアウト機能を有することが望ましい
管理者 ID	・ 管理者 ID は、本機関及び受託者で異なる ID を発行し、必要最低限の権限のみ与えること ・ 本機関の管理者 ID は共有ではなく、個人単位で発行すること
第三者認証	・ SOC 監視用セキュリティデバイスについて、「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「国際標準 に基づくセキュリティ要件」に準拠した第三者認証を取得していること

3. 役務に関する要件

(1) 業務要件

① 業務実施手順

本書で調達する役務について、要件を記載する。

表 3.1 役務に係る業務要件-業務手順

フェーズ	作業内容
要件確認	・ 本機関における要件（本書の要件）について、受託者との認識のずれや齟齬がないことを作業着手前に確認すること ・ 受託者が SOC 業務開始までの作業を進めるにあたり、前提となる要件を本機関にヒアリングし、当該内容を要件確認書として取りまとめること ・ 要件確認の内容を本機関と合意のうえ、設計作業に着手すること
設計	基本設計 ・ 要件確認に基づき、SOC 業務に必要なシステム及びシステムで利用する全ての機能について設計し、基本設計書として取りまとめること ・ 要件確認に基づき、SOC 監視用セキュリティデバイスの機能設計を行うこと。なお、設計には次のカスタムシグネチャの作成を含める - 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 ・ SOC 監視を実施することを十分に考慮のうえ、ネットワーク環境や機器のログ・アカウントなどの設計を行うこと 運用設計 ・ SOC 業務及び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。また、SOC 業務に係る通知メールやレポート等の内容についても、設計フェーズで本機関と合意すること ・ 運用設計書には、本機関と SOC との役割や責任及び情報連携方法などを含めること ・ 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 ・ システムの設定変更に関する依頼フォームを提示し、本機関と合意すること

	試験設計 ・ 単体試験、結合試験、障害試験、情報セキュリティの観点に基づく試験などの試験項目を計画し、その合否判定基準を設計すること。 ・ 運用設計にもとづき、SOC 業務及びシステム障害を想定したシナリオテストを行うこと 移行設計 ・ 本機関の既存システムに影響をあたえないように、設置作業及び工事計画を立て移行設計書として取りまとめること。また、既存システムとの接続に際し、リスクや留意事項があれば、本機関に提示すること ・ 本機関の既存システムに設定変更を必要とする場合は、その内容や順序についても可能な限り支援すること
構築	・ 設計に基づき、システムの設定値を設計し、セットアップすること ・ 各デバイスは、既知の脆弱性がないソフトウェアで構築すること ・ システムのバックアップファイルを取得すること
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 ・ デバイスをラックに搭載し、各デバイス間をネットワークケーブルで結線すること。なお、本機関の既設デバイスとの接続にあたっては、本機関の既存システムの停止は不可（停止が必要である場合は 2 重化を切替ながら実施）であることを前提に、平日深夜又は休日の作業を想定すること ・ 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 ・ データセンタでの工事にあたり必要な申請は本機関にて実施するが、申請内容の作成は受託者が実施すること
試験	・ 試験設計に基づき、システムの試験を実施すること ・ デバイス単体で、各機能が適切に動作していることを確認すること ・ 本調達に係るシステム及び各機能を結合し、設計通りに動作していることを確認すること ・ SOC と連携し、ログファイルの授受や SOC 業務のシナリオ試験を実施すること ・ バックアップ及びリストアの試験を実施し、設計通りに障害からの復旧ができることを確認すること ・ 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。

SIEM ルールのチューニング	・ 本機関が要求する SIEM ルールにおいて、誤検知、過剰検知が発生する場合は、必要に応じてルール条件の見直しやホワイトリストなどで誤検知排除に向けたチューニングを実施すること

② 業務実施期間

本書で調達する役務について、本機関が想定している実施期間を記載する。

表 3.2 役務に係る業務要件-業務実施期間

フェーズ	作業内容
要件確認	・ 契約締結日～2017 年 10 月中旬
設計	・ 2017 年 10 月中旬～2017 年 11 月中旬
構築	・ 2017 年 11 月中旬～2017 年 12 月中旬
設置・工事	・ 2017 年 12 月中旬
試験	・ 2017 年 12 月中旬
SIEM ルールのチューニング	・ 2017 年 12 月中旬～2018 年 1 月末

③ 業務実施場所

本調達に係る作業は、本機関が承認した作業場所でのみ実施を許可する。

表 3.3 役務に係る業務要件-業務実施場所

項目	内容
作業場所	・ 本役務の一部は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関の許可を得ること ・ 本役務に関する打合せ、レビュ、報告会議等については、本機関が提供する会議室で実施すること ・ 本役務における設置工事、試験については、本機関が指定するシステム設置場所で実施すること

④ 業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

表 3.4 役務に係る業務要件-業務管理

項目	内容
進捗管理	・ 進捗管理については、プロジェクト計画書に基づき各タスクの状況把握及びスケジュール管理を行うこと

リスク管理	・ 各作業工程における目標の達成に対するリスクの抽出、リスクの影響を最小限にする対応策の実施等のリスク管理を行うこと
文書管理	・ 各作業工程において作成する設計書等の文書について、改ざん、漏えい、盗用及び目的外の利用を未然に防止するよう文書管理を行うこと
課題管理	・ プロジェクト遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと
品質管理	・ 品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと
人的資源管理	・ 本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと ・ 主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること
コミュニケーション管理	・ 各作業工程における各種作業に関する打ち合わせ、成果物等のレビュ、進捗確認、課題共有等を行うためのプロジェクト会議を開催すること
構成・変更管理	・ 構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること

4. 保守に関する要件

(1) 業務要件

① 業務実施内容

本書で調達する保守及び運用業務について、要件を記載する。

表 4.1 保守に係る業務要件-実施内容

項目	内容
稼働監視	・ 本システムのデバイス及び提供機能を監視し、障害発生を検知した場合は、速やかに本機関にメールと電話で報告を行うこと。 ・ 稼働状況が確認できるための監視ポータル（監視結果レポート画面）を用意すること。 ・ トラフィック量やリソース情報を監視し、品質の低下が危惧される場合は通知すること
障害対応	・ システム障害を検知した場合は、速やかに切り分けを実施の上、事象及びその原因特定、及び復旧作業を行うこと。なお、障害対応においては、本機関と密に情報連携を行うこととする（情報連携の方法等は運用設計で定義すること） ・ 必要に応じて、ハードウェアを交換し、最新のバックアップファイルからリストアを行うこと
設定変更	・ 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。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 ・ 保守業務における設定変更作業では、本機関のメインサイトに影響を与えないように作業を実施すること。
シグネチャ更新	・ 本システムのデバイスに係るシグネチャやパターンファイルを更新し、最新の脅威が検知できる環境を維持させること
バックアップ	・ 設定変更及びバージョンアップ時には、設定ファイルのバックアップを取得すること ・ バックアップ保存期間は、3 世代又は 1 年のうち、保存期間の長いものを適用すること
バージョンアップ	・ 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とすること。ただし、ソフトウェア/ファームウェアのアップデートは、重大な脆弱性が発見された場合、又は SOC 業務の提供に影響を与える場合に限る。 ・ 保守業務におけるバージョンアップ作業では、本機関のメインサイトに影響を与えないように作業を実施すること

保守受付	・ 本機関からの各種依頼に対して、電話、メールによる受付窓口を準備し、依頼事項に対する支援を実施すること ・ 本システムの動作仕様や技術的な質問に対して、電話及びメールにて回答を行うこと ・ 専任の担当者を設置し、本機関の環境を踏まえた回答やサポートを行うことが望ましい。なお、専任担当者は、本機関の専属である必要はなく、本機関の環境を理解した応対ができればよい
保守情報通知	・ ソフトウェア/ファームウェアのリリースや、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 ・ メーカーサポート終了（EOL）が発表された場合、速やかに本機関へ通知すること ・ インターネット回線に保守作業による断時間が発生する場合、その内容を速やかに本機関に通知すること
月次報告	・ 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。また、各デバイスの脆弱性やソフトウェア不具合情報を提供し、バージョンアップの要否について報告すること
その他	・ 本機関では情報システムのセキュリティ検査及びシステム監査を毎年実施していることから、受託者は本機関からの求めに応じ、問合せへの対応や必要な資料を提供すること ・ 対応言語は日本語とすること

② 業務提供時間

受託者は保守契約の期間において、次の時間帯で保守業務を提供すること。

表 4.2 保守に係る業務要件-提供時間

項目	内容
稼働監視	・ 24 時間 365 日
障害対応	・ 24 時間 365 日
設定変更	・ 平日 9:00-18:00
シグネチャ更新	・ 平日 9:00-18:00
バックアップ	・ 平日 9:00-18:00
バージョンアップ	・ 平日 夜間、又は、休日（都度、本機関と調整すること）
保守受付	・ 受付：24 時間 365 日 ・ 回答：平日 9:00-18:00
保守情報通知	・ 平日 9:00-18:00

月次報告	・　平日 9:00-18:00（毎月 10 営業日以内に報告すること）

③　作業場所

本調達に係る保守作業は、原則として受託者の事業所とするが、予め本機関にその業務場所について開示すること。

表 4.3 保守に係る業務要件-業務場所

項目	内容
作業場所	・　保守業務は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関に案内すること ・　保守業務に関する打合せ、報告会議等については、本機関が提供する会議室で実施すること

④　業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

表 4.4 保守に係る業務要件-業務管理

項目	内容
情報セキュリティ管理	・　各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと、並びに発生した場合に被害を最小限に抑えること
課題管理	・　業務遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと
品質管理	・　品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと
人的資源管理	・　本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと ・　主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること
構成・変更管理	・　構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること

5.サービスに関する要件

(1) 機能要件

① 機能

SOC 側の運用設備に求める要件を次に記載する。

表 5.1 サービスに係る機能要件

項目	内容
ログの取得及び保管機能	・ SOC 監視用セキュリティデバイスから送信されるログをリアルタイムで収集すること ・ 収集・保管するログ情報は、漏えいや改ざん等の被害を防止し、1年間保管すること。なお、少なくとも 3 ヶ月分についてはオンラインでの保存が望ましい
ログの監視機能	・ SOC 監視用セキュリティデバイスから送信されるログをリアルタイムで分析すること ・ 本機関が指定する以下の分析要件を SIEM に実装すること。具体的なルール要件は、契約後に本機関が受託者に提示する
単純条件型①	・ SOC 監視用セキュリティデバイス（Sandbox、IDS 機能など）が異常と判断したセキュリティログが出力された場合に、アラートとすること ※IDS は、カスタムシグネチャを含めること
単純条件型②	・ 特定の条件に合致するセキュリティログが出力された場合に、アラートとすること ・ 例）プライベートアドレスからグローバルアドレス宛ての通信 ・ 例）URL フィルタで脅威サイトとカテゴリ分類された通信
相関分析型①	・ セキュリティログに記録された IP や URL を、SOC が保有する脅威 DB（ブラックリスト）と照合し、DB の内容に一致した場合、アラートとすること
相関分析型②	・ セキュリティログに記録された IP や国情報を、本機関が指定するブラックリストと照合し、DB の内容に一致した場合、アラートとすること
閾値型	・ ログの特定カラムを計算し、一定の閾値に達する場合、アラートとすること ・ 例）1 日分の送信データ Byte 数を積算し、閾値を超えた場合 ・ 例）指定した時間帯以外で、指定するログが出力された場合
VPN 接続機能	・ 本機関に設置する Internet VPN デバイスとの Site to Site の Internet VPN が構築できること

運用管理端末	・ 本機関のシステムを操作するオペレーション端末は、脆弱性のないセキュアな端末で実施すること。なお、パッチ管理、アンチウィルス、ID 管理、ログ管理のセキュリティ対策は必須とする

(2) 業務要件

① 業務内容

本書で調達する SOC 業務について、要件を記載する。

表 5.2 サービスに係る業務要件-業務内容

項目	内容
ログの取得保管	・ SOC 監視用セキュリティデバイスから送信されるログをリアルタイムで収集すること ・ 収集・保管するログ情報は、漏えいや改ざん等の被害を防止し、1 年間保管すること。なお、少なくとも 3 ヶ月分についてはオンラインでの保存が望ましい
インシデントの検知（ログの監視）	・ 収集したログを相関分析することにより、脅威や不正の発生を検知すること ・ 入札者が保有するナレッジや独自のブラックリストとの突合などで検知能力を高めること
インシデントの分析	・ 検知したアラートについて誤検知、過剰検知等を調査し実害の有無を判断すること ・ 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） ・ 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
インシデントの通知	・ インシデント発生を認めた場合、発生事象、その影響及びトリアージ結果と共に、隔離等の対処方法を通知・案内すること ・ インシデントの通知は、そのアラートが発生してから 4 時間以内を目標とすること。なお、詳細なレポートを待たずして初報が可能な場合は、可能な限り早期に行うこと
QA 対応業務	・ 本機関からの各種依頼に対して、電話、メールによる受付窓口を準備し、依頼事項に対する支援を実施すること ・ 本サービスの仕様や技術的な質問に対して、電話及びメールにて回答を行うこと ・ 専任の担当者を設置し、本機関の環境を踏まえた回答やサポートを行うことが望ましい。なお、専任担当者は、本機関の専属である必要はなく、本機関の環境を理解した応対ができればよい

インシデントの対応支援	・ 本機関からのインシデントの対応策等の問い合わせに対して、推奨手順等の回答を行うこと
定期報告	・ 月次レポートを発行し、定例会を開催の上、その内容について説明すること ・ レポート内容には、イベント発生状況だけでなく、世の中の脅威や脆弱性の情報を含めること ・ 月次レポートの内容は、上位層への報告を考慮し、全体要約と個別課題を分類して報告すること
改善提案	・ あらたなサイバー攻撃や脆弱性に対する監視方法や対処方法について、プロアクティブな提案を行うこと
その他	・ 本機関では情報システムのセキュリティ検査及びシステム監査を毎年実施していることから、受託者は本機関からの求めに応じ、問合せへの対応や必要な資料を提供すること ・ 本機関とのサービス契約終了時（途中解約等も含む）には、インシデント履歴やログデータ、レポート等の全ての情報を削除すること ・ 言語は日本語とすること

② 業務提供時間

受託者は SOC 契約の期間において、次の時間帯で保守業務を提供すること。

表 5.3 サービスに係る業務要件-提供時間

項目	内容
ログの取得保管	・ 24 時間 365 日
インシデントの検知（ログの監視）	・ 24 時間 365 日
インシデントの分析	・ 24 時間 365 日
インシデントの通知	・ 24 時間 365 日
QA 対応業務	・ 受付：24 時間 365 日 ・ 回答：平日 9:00-18:00
ログの提供	・ 平日 9:00-18:00
インシデントの対応支援	・ 24 時間 365 日
定期報告	・ 平日 9:00-18:00（毎月 10 営業日以内に報告すること）
改善提案	・ 平日 9:00-18:00

③ 作業場所

本調達に係る保守作業は、原則として受託者の事業所とするが、予め本機関にその業務場

所について開示すること。

表 5.4 サービスに係る業務要件-作業場所

項目	内容
作業場所	・ 保守業務は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関に案内こと ・ 保守業務に関する打合せ、報告会議等については、本機関が提供する会議室で実施すること

④ 業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

表 5.5 サービスに係る業務要件-作業場所

項目	内容
情報セキュリティ管理	・ 各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと、並びに発生した場合に被害を最小限に抑えること
課題管理	・ 業務遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと
品質管理	・ 品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと
人的資源管理	・ 本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと ・ 主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること
構成・変更管理	・ 構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること

以上

セキュリティログ監視等業務委託

応札資料作成要領

平成２９年8月１０日

電力広域的運営推進機関

目　　次

本書は、セキュリティログ監視等業務委託に係る応札資料(評価項目一覧及び提案書)の作成要領を取りまとめたものである。

第１章　電力広域的運営推進機関が応札者に提示する資料及び応札者が提出すべき資料

電力広域的運営推進機関は応札者に以下の表１に示す資料を提示する。応札者は、それを受け、以下の表２に示す資料を作成し、電力広域的運営推進機関へ提出する。

［表１ 電力広域的運営推進機関が応札者に提示する資料］

資料名称	資料内容
① 仕様書	セキュリティログ監視等業務の仕様を記述
② 応札資料作成要領	応札者が評価項目一覧及び提案書の作成する上での留意点等を記述
③ 評価項目一覧	提案書に記載すべき提案要求事項一覧、必須項目及び任意項目の区分、得点配分等を記述
④ 評価手順書	電力広域的運営推進機関が応札者の提案を評価する場合に用いる評価方式、総合評価点の算出方法及び評価基準等を記述

［表２ 応札者が電力広域的運営推進機関に提示する資料］

資料名称	資料内容
① 評価項目一覧の提案書頁番号欄に必要事項を記入したもの	仕様書に記述された要件一覧を達成するか否かに関し、提案書頁番号欄に、該当する提案書の頁番号を記入したもの。
② 提案書	仕様書に記述された要求仕様をどのように実現するかを説明したもの。
③ 契約書（案）	提案書に記述された内容を実現するにあたっての契約書類の案
④ 適合証明書	入札資格を満たしていることを証する書面

第 2 章　評価項目一覧に係る内容の作成要領

2.1　評価項目一覧の構成

評価項目一覧の構成及び概要説明を以下に記す。

［表 3 評価項目一覧の構成の説明］

評価項目一覧における項番	事項	概要説明
1～2	提案要求事項	提案を要求する事項。これら事項については、応札者が提出した提案書について、各提案要求項目の必須項目及び任意項目の区分け、得点配分の定義に従いその内容を評価する。
3	添付資料	応札者が作成した提案の詳細を説明するための資料。これら自体は、直接評価されて点数が付与されることはない。

2.2　提案要求事項

評価項目一覧中の提案要求事項における各項目の説明を以下に示す。応札者は、別添「評価項目一覧」の提案要求事項」における「提案書頁番号」欄に必要事項を記載すること。提案要求事項の各項目の説明に関しては、表 4 を参照すること。

［表 4 提案要求事項上の各項目の説明］

項目名	項目説明・記入要領	記入者
大項目～細項目	仕様書の分類	電力広域的運営推進機関
提案要求事項	応札者に提案を要求する内容	電力広域的運営推進機関
評価区分	必ず提案すべき項目（必須）又は必ずしも提案する必要は無い項目（任意）の区分を設定している。各項目について、記述があった場合、その内容に応じて配点を行う。	電力広域的運営推進機関
得点配分	各項目に対する最大加点	電力広域的運営推進機関
提案書頁番号	作成した提案書における該当頁番号を記載する。該当する提案書の頁が存在しない場合には空欄とする。評価者は各提案要求事項について、本欄に記載された頁のみを対象として採点を行う。	応札者

2.3　添付資料

評価項目一覧中の補足添付資料における各項目の説明を以下に示す。

［表 5 添付資料上の各項目の説明］

項目名	項目説明・記入要領	記入者
大項目～小項目	提案書の目次（提案要求事項の分類）。	電力広域的運営推進機関
資料内容	応札者に提案を要求する内容	電力広域的運営推進機関
提案の要否	必ず提案すべき項目（必須）又は必ずしも提案する必要は無い項目（任意）の区分を設定している。提案要求事項とは異なり、採点の対象とはしない。	電力広域的運営推進機関
提案書頁番号	作成した提案書における該当頁番号を記載する。該当する提案書の頁が存在しない場合には空欄とする。	応札者

第 3 章　提案書に係る内容の作成要領及び説明

3.1　提案書の構成及び記載事項

提案書は、評価項目一覧の提案要求事項及び添付資料の提案書の目次に従い、提案要求内容を十分に咀嚼した上で記述すること。

3.2　提案書様式

① 提案書は第 4 章（別紙 1）「提案書雛形」を参考にして記述する。
② 提案書及び評価項目一覧は A4 判カラーにて、全 10 部印刷し、特別に大きな図面等が必要な場合には、原則として A3 判にて提案書の中に折り込む。
③ 提出物は、上記の紙資料とともに、電子媒体でも提出する。その際のファイル形式は、原則として、MS-Word、MS-PowerPoint、MS-Excel 又は PDF 形式とする（これに拠りがたい場合は、電力広域的運営推進機関まで申し出ること。）

3.3　応札者による提案書の説明（プレゼンテーション）

① 応札者は、電力広域的運営推進機関に対し自らの提案内容の説明を行う。
② 当該説明に当たっては、電力広域的運営推進機関内会議室にてプレゼンテーションを行うこととし、その際には、原則としてプロジェクト・マネージャーに該当する者が実施する。
③ 当該プレゼンテーションの日時等については、入札締切（提案書提出期限）後に電力広域的運営推進機関と応札者とで別途調整する。また、プレゼンテーションの時間は、現時点では 1 社あたり 45 分程度（発表 30 分、質疑応答 15 分程度）を想定している。
④ プレゼンテーションにあたっては、与えられた時間を踏まえ、必要に応じて提案書とは別に要約版資料を用意するなど、効率的な実施のために工夫する。

3.4　留意事項

① 提案書を評価する者が特段の専門的な知識や商品に関する一切の知識を有しなくても評価が可能な提案書を作成する。なお、必要に応じて、用語解説などを添付する。

② 提案に当たって、特定の製品を採用する場合は、当該製品を採用する理由を提案書中に記載するとともに、記載内容を証明及び補足するもの（製品紹介、パンフレット、比較表等）を添付する。

③ 応札者は提案の際、提案内容についてより具体的・客観的な詳細説明を行うための資料を、添付資料として提案書に含めることができる(その際、提案書本文と添付資料の対応が取れるようにする)。

④ 電力広域的運営推進機関から連絡が取れるよう、提案書には連絡先（電話番号、FAX番号、及びメールアドレス）を明記する。

⑤ 提出物を作成するに際しての質問等を行う必要がある場合には、別紙２の質問状に必要事項を記載の上、平成２９年８月３０日（水）１７時までに下記問い合わせ先へ、電子メールで問い合わせる。

【問い合わせ先】

電力広域的運営推進機関　総務部経理グループ（契約担当）

メールアドレス：keiyaku@occto.or.jp

⑥ 上記の提案書構成、様式及び留意事項に従った提案書ではないと電力広域的運営推進機関が判断した場合は、提案書の評価を行わないことがある。また、補足資料の提出や補足説明等を求める場合がある。

第 4 章 別紙

4.1 （別紙 1） 提案書雛形

4.2 （別紙 2） 適合証明書

4.3 （別紙 3） 質問状

社名			
住所			
TEL		FAX	
質問者			
質問に関連する文書名及び頁			
質問内容			

（スライドタイトル）

4.1（別紙1）提案書雛形

記述内容	・

評価項目一覧（提案要求事項一覧及び添付資料）の提案要求事項と整合させる

- ○○○について

評価項目一覧を参照して提案書を作成する。

ア. 提案要求事項欄で求められている内容について具体的に記述する。

イ. 評価基準欄に記載の基礎点及び加点のポイントに対応した提案を記述する。特に、評価区分欄が「必須」となっている事項については必ず記述すること。

ウ. 電力広域的運営推進機関から連絡が取れるよう、 提案書には連絡先（担当者名、電話番号、 FAX番号、及びメールアドレス）を明記する。

■ **連絡先**

- 担当者名　XX　XX
- 電話（FAX）　XX-1XXXX
- メールアドレス　XXX@XXXXXX

電力広域的運営推進機関

御社名

セキュリティログ監視等業務委託

適合証明書

㊞

区分	入札説明書記載箇所	機能	適合※1	補足※2
入札資格	2（1）	平成２８・２９・３０年度の競争参加資格（全省庁統一資格）の「役務の提供等」において、Ｃ等級以上に格付けされており、関東・甲信越地域の資格を有する者であること。		
	2（2）	各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止を受けていない者であること。		
	2（3）	入札説明会に参加した者であること。		
	2（4）	予算決算及び会計令(昭和22年勅令第165号)第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。		
	2（5）	予算決算及び会計令第71条の規定に該当しない者であること。		
	2（6）	会社更生法（平成14年法律第154号）に基づく更生手続開始の申立て又は民事再生法（平成11年法律第225号）に基づく再生手続開始の申立てがなされている者でないこと（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く。）。		
	2（7）	自己、自社若しくはその役員等（注1）が、暴力団員による不当な行為の防止等に関する法律第2条に定める暴力団、暴力団員又はその他反社会的勢力（注2）でない者であること。 （注１）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している者。 （注２）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から5年を経過しない者等、その他これに準じる者。		
	2（8）	破壊活動防止法に定めるところの破壊的団体およびその構成員でない者であること。		
	2（9）	入札者又は入札者の協力会社（社名を提出のこと）が経済産業省公表の「平成28年度情報セキュリティ監査企業台帳」において以下に定める項目に該当すること。 (ア)「地域名」に「関東」を登録していること。 (イ)「IT関連業務」に「セキュリティ監査」を登録していること。 (ウ)「セキュリティ関連業務」に「リスク評価／脆弱性評価サービス」を登録していること。 (エ)「セキュリティ監査対象の分野・業種」に「公務（官公庁・自治体 等）」を登録していること。 (オ)「監査従事者が持つ取得済監査関連資格」に「公認情報システム監査人（CISA）」、「公認情報セキュリティ監査人」または「情報セキュリティスペシャリスト 」を登録していること。 (カ)「取得している監査関連の認証」に「ISMS適合性評価制度」または「プライバシーマーク(JIS Q 15001)」を登録していること。		
	2（10）	政府機関の情報セキュリティ対策のための統一基準群について理解し、電力事業者又は行政機関に対するセキュリティログ等監視業務の導入及び運用実績があること。		

※1　適合については，“○（要件を満たしている）”，“△（条件付きで要件を満たしている，代替手段で要件を満たす）”，“×（要件を満たしていない）”で記述をお願いします。また，“△”を記入した場合は，補足欄に説明をご記入ください。

※2　補足すべき事項がある場合は，その内容を補足欄に記入してください。また，各機能の適合を証する添付資料を同封し、提出をお願いします。

電力広域的運営推進機関

電力広域的運営推進機関
セキュリティログ監視等業務委託

評価手順書（加算方式）

平成２９年8月１０日

電力広域的運営推進機関

本書は、電力広域的運営推進機関セキュリティログ監視等業務に係る評価手順を取りまとめたものである。落札方式、評価の手続き及び提案の配点基準を以下に記す。

第 1 章　落札方式及び得点配分

1.1　落札方式

次の要件をともに満たしている者のうち、「1.2　総合評価点の計算」によって得られた数値の最も高い者を落札者とする。

① 入札価格が予定価格の範囲内であること。
② 別添「評価項目一覧」に記載される要件のうち必須とされた項目を、全て満たしていること。

1.2　総合評価点の計算

総合評価点　＝　技術点　＋　価格点

技術点＝基礎点 ＋ 加点
価格点＝価格点の配分(※) ×　(1 － 入札価格 ÷ 予定価格)
※なお、技術点の配分と価格点の配分は、３：１とする。

1.3　得点配分

技術点に関し、必須及び任意項目の配分を 300 点、価格点の配分を 100 点とする。

技術点	300 点
価格点	100 点

第 2 章　評価の手続き

2.1　一次評価

まず、以下の基準により一次判定を行う。

・別添「評価項目一覧」の「提案要求事項（項番 1～2）」の、評価項目が必須の「提案書頁番号」に提案書の頁番号が記入されている。

一次評価で合格した提案書について、「2.2　二次評価」を行う。

2.2　二次評価

「2.1　一次評価」にて合格した提案書に対し、「3　評価項目の加点方法」にて記す評価基準に基づき採点を行う。この際、別添「評価項目一覧」に記載される「提案要求事項（項番 1～2）」のうち必須とされた項目について基礎点の得点が 0 となった場合、その応札者を不合格とする。複数の評価者が評価を行うため、各評価者の評価結果（点数）を合計し、それを平均して技術点を算出する。

2.3　総合評価点の算出

以下を合計し、総合評価点を算出する。

①　「2.2　　二次評価」により与えられる技術点

②　入札価格から、「1.2　総合評価点の計算」に記した式より算出した価格点

③　技術点及び価格点に小数点第２位以下の端数を生じた場合は切り捨てとする。

第 3 章　評価項目の加点方法

3.1　評価項目得点構成

評価項目の得点は基礎点と加点の二種類に分かれており、その合計にて提案要求事項毎の得点が決定される。（評価項目毎の基礎点、加点の得点配分は「評価項目一覧」の「提案要求事項一覧」の「得点配分」欄を参照）

3.2　基礎点評価

基礎点は、提案要求事項の評価区分が必須である事項にのみ設定されている。評価の際には提案要求事項の要件を充足している場合には配分された点数が与えられ、充足していない場合は 0 点となる。提案者は、提案書にて基礎点の対象となる要件を全て充足することを示さなければならない。一つでも要件が充足できないとみなされた場合は、その応札者は不合格となる。

3.3　加点評価

加点は、全ての提案要求事項について設定されており、各提案要求事項の加点を評価する際の観点に沿って評価を行う。

電力広域的運営推進機関

Title: 評価項目一覧 - 提案要求事項一覧 -

仕様書の項目				提案要求事項	評価区分	得点配分			評価基準		提案書頁番号
大項目	中項目	小項目	細項目			合計	基礎点	加点	基礎点	加点	
1 調達案件の概要						27	2	25			
	1.1 調達の背景・目的及び期待する効果			・本調達の背景・目的を理解したうえで、目的が電力広域的運営推進機関（以下「本機関」という。）の目的に合致しているか。	必須	1	1	0	・本調達の背景を理解したうえで、提案書の目的が電力広域的運営推進機関（以下「本機関」という。）の目的に合致しているか。		
	1.2 作業スケジュール			・詳細なスケジュールが記載されているか。	任意	5	0	5		・詳細なスケジュールが記載されているか。	
	1.3 調達対象となる数量の考え方			・監視対象となるアクティブな環境は、メインサイト及びバックアップサイトのいずれか一方の環境であることを前提に見積もっているか。	任意	5	0	5		・監視対象となるアクティブな環境は、メインサイト及びバックアップサイトのいずれか一方の環境であることを前提に見積もっているか。	
	1.4 サービス継続性			・地震・災害時のSOCサービスの継続性について、対策状況が記載されているか。	任意	5	0	5		・地震・災害時のSOCサービスの継続性について、対策状況が記載されているか。	
	1.5 成果物の範囲、納品期日等			・成果物が記載されているか。	必須	1	1	0	・成果物が記載されているか。		
	1.6 入札参加要件			・電力事業者又は行政機関に対するセキュリティログ等監視業務の導入及び運用実績の記載があるか。	任意	10	0	10		・電力事業者又は行政機関に対するセキュリティログ等監視業務の導入及び運用実績の記載があるか。	
2 満たすべき要件に関する事項						273	73	200			
	2.1 環境構築に関する要件					72	17	55			
		2.1.1 機能要件				14	4	10			
			2.1.1.1 SOC監視用セキュリティデバイス	・SOC監視用セキュリティデバイスの記載があるか。 ・機能について比較検討した内容が記載されているか。	必須	11	1	10	・SOC監視用セキュリティデバイスの記載があるか。	・機能について比較検討した内容が記載されているか。	
			2.1.1.2 Internet VPNデバイス	・Internet VPNデバイスの記載があるか。	必須	1	1	0	・Internet VPNデバイスの記載があるか。		
			2.1.1.3 インターネット回線	・インターネット回線の記載があるか。	必須	1	1	0	・インターネット回線の記載があるか。		
			2.1.1.4 各デバイス共通	・各デバイス共通で求めている機能の記載があるか。	必須	1	1	0	・各デバイス共通で求めている機能の記載があるか。		
		2.1.2 非機能要件				20	5	15			
			2.1.2.1 SOC監視用セキュリティデバイス	・想定したログ量と性能を満たすSOC監視用セキュリティデバイスについて記載があるか。 ・性能について比較検討した内容が記載されているか。	必須	11	1	10	・想定したログ量と性能を満たすSOC監視用セキュリティデバイスについて記載があるか。	・性能について比較検討した内容が記載されているか。	
			2.1.2.2 Internet VPNデバイス	・想定したログ量と性能を満たすInternet VPNデバイスの記載があるか。	必須	1	1	0	・想定したログ量と性能を満たすInternet VPNデバイスの記載があるか。		
			2.1.2.3 インターネット回線	・想定した通信量と性能を満たす回線の記載があるか。	必須	1	1	0	・想定した通信量と性能を満たす回線の記載があるか。		
			2.1.2.4 信頼性・拡張性	・信頼性・拡張性について記載されているか。	必須	1	1	0	・信頼性・拡張性について記載があるか。		
			2.1.2.5 情報セキュリティ	・情報セキュリティについて記載されているか。 ・複数回の認証エラーは、アカウントロックアウト機能を有することが記載されているか。 ・追加で考慮すべきセキュリティ施策の記載があるか。	必須	6	1	5	・情報セキュリティについて記載があるか。	・複数回の認証エラーは、アカウントロックアウト機能を有することが記載されているか。 ・追加で考慮すべきセキュリティ施策の記載があるか。	
		2.1.3 業務管理要件（役務要件）				38	8	30			
			2.1.3.1 進捗管理	・進捗管理について記載されているか。 ・進捗管理の手順、フォーム、進捗の示し方について記載されているか。	必須	6	1	5	・進捗管理について記載があるか。	・進捗管理の手順、フォーム、進捗の示し方について記載があるか。	
			2.1.3.2 リスク管理	・リスク管理について記載がされているか。 ・リスク管理の手順、フォーム、報告方法について記載されているか。	必須	6	1	5	・リスク管理について記載があるか。	・リスク管理の手順、フォーム、報告方法、について記載があるか。	
			2.1.3.3 文書管理	・文書管理について記載されているか。 ・成果物の保管方法や持ち出しルールについて記載されているか。	必須	6	1	5	・文書管理について記載されているか。	・成果物の持ち出しルールや保管方法について記載されているか。	

Title: 評価項目一覧 - 提案要求事項一覧 -

仕様書の項目				提案要求事項	評価区分	得点配分			評価基準		提案書頁番号
大項目	中項目	小項目	細項目			合計	基礎点	加点	基礎点	加点	
			2.1.3.4 課題管理	・課題管理について記載されているか。 ・課題管理の手順、フォームについて記載されているか。	必須	6	1	5	・課題管理について記載されているか。	・課題管理の手順、フォームについて記載されているか。	
			2.1.3.5 品質管理	・品質管理について記載されているか。 ・品質管理の手順、フォームについて記載されているか。	必須	6	1	5	・品質管理について記載されているか。	・品質管理の手順、フォームについて記載されているか。	
			2.1.3.6 人的資源管理	・体制図が記載されているか。 ・プロジェクトに従事する要員の資格が記載されているか。	必須	6	1	5	・体制図が記載されているか。	・プロジェクトに従事する要員の資格が記載されているか。	
			2.1.3.7 コミュニケーション管理	・コミュニケーション管理について記載されているか。	必須	1	1	0	・コミュニケーション管理について記載されているか。		
			2.1.3.8 構成・変更管理	・構成・変更管理について記載されているか。	必須	1	1	0	・構成・変更管理について記載されているか。		
	2.2 保守に関する要件					14	14	0			
		2.2.1 業務要件				9	9	0			
			2.2.1.1 稼働監視	・稼働監視について記載されているか。	必須	1	1	0	・稼働監視について記載されているか。		
			2.2.1.2 障害対応	・障害対応について記載されているか。	必須	1	1	0	・障害が発生した際に対応することが可能か。		
			2.2.1.3 設定変更	・設定変更について記載されているか。	必須	1	1	0	・設定変更について記載されているか。		
			2.2.1.4 シグネチャ更新	・シグネチャ更新について記載されているか。	必須	1	1	0	・シグネチャ更新について記載されているか。		
			2.2.1.5 バックアップ	・バックアップについて記載されているか。	必須	1	1	0	・バックアップについて記載されているか。		
			2.2.1.6 バージョンアップ	・バージョンアップについて記載されているか。	必須	1	1	0	・バージョンアップについて記載されているか。		
			2.2.1.7 保守受付	・保守受付について記載されているか。	必須	1	1	0	・保守受付について記載されているか。		
			2.2.1.8 保守情報通知	・保守情報通知について記載されているか。	必須	1	1	0	・保守情報通知について記載されているか。		
			2.2.1.9 月次報告	・月次報告について記載されているか。	必須	1	1	0	・月次報告について記載されているか。		
		2.2.2 業務管理要件				5	5	0			
			2.2.2.1 情報セキュリティ管理	・情報セキュリティについて記載されているか。	必須	1	1	0	・情報セキュリティについて記載されているか。		
			2.2.2.2 課題管理	・課題管理について記載されているか。	必須	1	1	0	・課題管理について記載されているか。		
			2.2.2.3 品質管理	・品質管理について記載されているか。	必須	1	1	0	・品質管理について記載されているか。		
			2.2.2.4 人的資源管理	・人的資源管理について記載されているか。	必須	1	1	0	・人的資源管理について記載されているか。		
			2.2.2.5 構成・変更管理	・構成・変更管理について記載されているか。	必須	1	1	0	・構成・変更管理について記載されているか。		
	2.3 サービスに関する要件					187	42	145			
		2.3.1 業務要件				182	37	145			
			2.3.1.1 ログの取得保管	・ログの取得保管について記載されているか。 ・ログ情報の漏えいや改ざん等の対策が具体的に記載されているか。 ・ログ保管期間について具体的に記載されているか。	必須	15	5	10	・ログの取得保管について記載されているか。	・ログ情報の漏えいや改ざん等の対策が具体的に記載されているか。 ・ログ保管期間について具体的に記載されているか。	
			2.3.1.2 インシデントの検知（ログの監視）	・インシデントの検知（ログの監視）について記載されているか。 ・相関分析の方法について記載されているか。 ・検知能力の高さについて、保持している脅威DBの内容や実績を踏まえ記載されているか。 ・検知能力を維持・向上させるための具体的な方法が記載されているか。 ・誤検知、過剰検知を防ぐ手順が記載されているか。	必須	45	5	40	・インシデントの検知（ログの監視）について記載されているか。	・相関分析の方法について記載されているか。 ・検知能力の高さについて、保持している脅威DBの内容や実績を踏まえ記載されているか。 ・検知能力を維持・向上させるための具体的な方法が記載されているか。 ・誤検知、過剰検知を防ぐ手順が記載されているか。	

Title: 評価項目一覧 - 提案要求事項一覧 -

仕様書の項目				提案要求事項	評価区分	得点配分			評価基準		提案書頁番号
大項目	中項目	小項目	細項目			合計	基礎点	加点	基礎点	加点	
			2.3.1.3 インシデントの分析	・インシデントの分析について記載されているか。 ・誤検知、過剰検知を防ぐ手順が記載されているか。 ・検知したアラートの分析についてシナリオ、分析手法等具体的に記載されているか。 ・トリアージの区分について具体的に記載されているか。 ・分析を向上させる手順が具体的に記載されているか。	必須	45	5	40	・インシデントの分析について記載されているか。	・誤検知、過剰検知を防ぐ手順が記載されているか。 ・検知したアラートの分析についてシナリオ、分析手法等具体的に記載されているか。 ・トリアージの区分について具体的に記載されているか。 ・分析を向上させる手順が具体的に記載されているか。	
			2.3.1.4 インシデントの通知	・インシデントの通知について記載されているか。 ・インシデントの通知手順について記載されているか。 ・インシデントの通知内容について記載されているか。	必須	25	5	20	・インシデントの通知について記載されているか。	・インシデントの通知手順について記載されているか。 ・インシデントの通知内容について記載されているか。	
			2.3.1.5 QA対応業務	・QA対応業務について記載されているか。 ・QA対応できる要員が具体的に記載されているか	必須	15	5	10	・QA対応業務について記載されているか。	・QA対応できる要員が具体的に記載されているか	
			2.3.1.6 インシデントの対応支援	・インシデントの対応支援について記載されているか。 ・インシデントの対応支援の要員が具体的に記載されているか。 ・インシデントの対応支援の範囲についてオンサイト支援が可能か。	必須	20	5	15	・インシデントの対応支援について記載されているか。	・インシデントの対応支援の要員が具体的に記載されているか。 ・インシデントの対応支援の範囲についてオンサイト支援が可能か。	
			2.3.1.7 定期報告	・定期報告について記載されているか。	必須	1	1	0	・定期報告について記載されているか。		
			2.3.1.8 改善提案	・改善提案について記載されているか。 ・改善提案の回数について具体的に記載されているか。	必須	15	5	10	・改善提案について記載されているか。	・改善提案の回数について具体的に記載されているか。	
			2.3.1.9 その他	・サービス契約終了時の取扱いについて記載されているか。	必須	1	1	0	・サービス契約終了時の取扱いについて仕様書記載の要件を満たしているか。		
		2.3.2 業務管理要件				5	5	0			
			2.3.2.1 情報セキュリティ管理	・情報セキュリティについて記載されているか。	必須	1	1	0	・情報セキュリティについて記載されているか。		
			2.3.2.2 課題管理	・課題管理について記載されているか。	必須	1	1	0	・課題管理について記載されているか。		
			2.3.2.3 品質管理	・品質管理について記載されているか。	必須	1	1	0	・品質管理について記載されているか。		
			2.3.2.4 人的資源管理	・人的資源管理について記載されているか。	必須	1	1	0	・人的資源管理について記載されているか。		
			2.3.2.5 構成・変更管理	・構成・変更管理について記載されているか。	必須	1	1	0	・構成・変更管理について記載されているか。		
						300	75	225			

Title: 評価項目一覧 - 添付資料 -

仕様書の項目			資料内容	提案の要否	提案書頁番号
大項目	中項目	小項目			
3 添付資料					
	入札参加要件		・電力事業者又は行政機関における、事業の実績	任意	
			・サービスに従事する要員の資格、実績	任意	