広域機関統一
セキュリティ対策基準策定支援業務委託

入札仕様書

電力広域的運営推進機関

2025 年 6 月

1. 件名

広域機関統一セキュリティ対策基準策定支援業務委託

2. 適用範囲

本仕様書は、電力広域的運営推進機関（以下、「本機関」という）が発注する「広域機関統一セキュリティ対策基準策定支援業務委託」に適用する。本仕様書は、本機関が上記業務を委託するにあたり、受託者が実施すべき事項について定めるものである。

3. 目的

米国国立標準技術研究所（NIST）が策定したサイバーセキュリティ対策のフレームワークである NIST CSF Ver1.1 は多くの企業・組織がサイバーセキュリティ対策を向上させるための指針として広く活用されており、電力広域的運営推進機関（以下、「本機関」という。）においても NIST CSF Ver1.1 を活用してサイバーセキュリティ対策状況の現状の評価を実施した。

評価結果を踏まえて、本委託では、各システムにて復旧計画やインシデント対応計画等を策定するための前提条件として、サイバーセキュリティに関して組織全体で統一された基準や根拠を定めた文書を作成することを目的とし、専門的な知見と経験を有するセキュリティ会社の支援を受けることで、効率的かつ効果的に実施する。

4. 委託期間

契約締結日 ～ ２０２６年1月２８日（水）

5. 委託範囲

サイバーセキュリティに関して各システムの復旧計画やインシデント対応計画等を策定するにあたり、組織全体としての統一した考え方の基準や指針を取りまとめた文書の作成を本委託の範囲とし、各システムが個別に作成する文書は本委託の対象外とする。

6. 委託内容

NIST-CSF にて定義される 5 つの機能に関して、本機関における評価結果を踏まえて、組織全体としての統一した策定基準を定めた文書を作成すること。作成する文書は以下の案を基本とし、NIST-CSF の内容、本機関の組織体制やシステム環境、現行の規定内容等を踏まえて、本機関と協議のうえ、網羅する内容を精査するものとする。なお、本委託にて作成した文書は、今後、各システムにて個別に作成するインシデント対応計画書や手順書等の指針となるものである。

＜文書案＞

① リスク管理基準

組織におけるリスクを識別、評価、対応、監視するための基本的な方針等を定めた文書

・リスク管理の基本方針

・リスクの分類

・リスク評価方針
・リスク対応方針
・モニタリング（セキュリティに関する法律・規制等への対応）と見直し
・役割と責任

② リスク管理手順書作成指針

具体的なリスクの識別から対応までの手順を示した実務的なマニュアルの作成指針

・リスク識別の方法
・リスク評価の方法
・リスク対応策
・リスクの記録、管理方法
・モニタリング、レビュー方法
・報告、エスカレーション方法
・定期的な見直し、更新

③ インシデント対応計画書作成指針

セキュリティインシデント発生時に対応するための計画をまとめた文書

・インシデントの定義と分類
・対応体制
・対応フロー
・連絡体制、通報先
・関係機関への報告、連携
・訓練、教育、演習計画
・インシデント後の対応

④ インシデント対応手順書作成指針

実際のインシデント発生時に実施する対応手順を示したマニュアルの作成指針

・インシデントの初動対応手順
・通報、記録の手順
・被害範囲の特定方法
・一時対応（隔離、封じ込め）手順
・原因調査と復旧対応
・終息判断と報告手順
・事後レビューと再発防止策の検討方法

⑤ IT－BCP

災害やセキュリティインシデント等発生時に、業務や重要な IT サービスやインフラを継続または早期に復旧させるための戦略と手順を定めた文書

・文書適用対象となる危機的事象の定義
・重要業務、システムの定義
・災害等発生時の復旧時間目標
・情報システムの復旧優先度や考え方

・緊急時の対応体制
・対応方針
・対応マニュアル
・危機発生時の社内連絡体制
・緊急時の社外連絡
・有事のための平時の準備

⑥ 監視実施手順書作成指針

システムやネットワークの稼働状況を監視し、異常を早期に検知して対処するための具体的な手順を示したマニュアルの作成指針

・対象システム、範囲
・監視項目と閾値設定
・使用する監視ツール
・アラート発生時の対応フロー
・定期点検と報告方法
・ログ管理手順
・定期的な見直し

⑦ 委託先管理基準

外部委託先の監督、評価などの基準を定めた文書

・委託先の管理、評価方法
・リスク管理、セキュリティ対策
・委託先変更、終了時の対応

7. 納品物

次の納入物を電子データで提出すること。

項番	納入物名	提出期限	備考
1	実施計画書	着手時	
2	実施完了報告書	完了時	
3	作成文書	完了時	6項に定める委託成果物

8. 検収・支払い

I. 検収

納品物の確認終了をもって検収とする。(ただし、検収後であっても、納品物について実施内容との不一致が発見された場合は、当該不一致が広域機関の責に帰すべき場合を除き，貴社にて無償で納品物の修補を行うこと。)

II. 支払い

検収完了後、月末締翌月末までに銀行振込にて、支払うものとする。

9. 情報の取り扱い

I. 本業務における機密情報とは当機関が開示するすべての情報とする。
II. 当機関から開示された機密情報は本業務の目的にのみ使用するものとし、その他の目的には使用しないものとする。
III. 当機関から開示された機密情報を本業務のために知る必要のある自己の役員、従業員以外に開示、閲覧等させないものとする。
IV. 当機関から開示された機密情報を第三者に開示または漏えいしないものとする。
V. 本業務の実施に当たって第三者に機密情報を開示、閲覧等させる場合には、当機関の事前承諾を得た上で、当該第三者に開示するものとする。
VI. 上記(V)により、機密情報を開示する第三者に対し本業務に関する契約と同様の内容を負わせるものとする。
VII. 本業務の完了後は機密情報を破棄すること。
VIII. 本業務の実施に当たって機密情報を知る必要のある自己の役員、従業員に本業務委託に関する契約の内容を遵守させるものとする。
IX. 上記(V)で定める第三者が本業務委託の契約のいずれかの事項に違反した場合、または漏えい等の事故により当機関に損害を与えた場合、当機関が被った損害の賠償をするものとする。

10. サプライチェーン・リスク対策

本委託業務の契約に先立ち、事前に貴社の資本関係・役員の他社の役職との兼任に関する情報(※1)、セキュリティ管理体制、委託業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報(※3)を本機関に書面をもって提出すること。ただし委託業務従事者に関する情報は個人単位（名指し）である必要はない。

※1：役員の他社役職との兼任情報については、必ずしも全役員ではなく、当機関の委託業務情報を閲覧する権限のある役員に限定して提供を求めることも可とする。
※2：委託業務の実施場所については、単に住所だけでなく、情報セキュリティが確保される場所であることが分かる情報（施錠区画であるかどうかなど）があることが望ましい。
※3：委託業務従事者に関する情報は、個人単位（名指し）ではなく、何名あるいは何%の形式で受領することを推奨する。
国籍についての例：　例１：全員日本人　例２：日本人５名、中国人１名、アメリカ人１名

11. 特記事項

I. 本仕様書に記載されている事項について不明な点は、契約締結までに当機関へ確認を行うこと。
II. 本仕様書に記載のない事項及び疑義については、当機関と協議のうえ決定することとする。
III. 再委託は原則として禁止とするが、業務遂行上で再委託が必要となる場合は、『資料１　再委託承認申請書』に必要事項を記載の上、事前に当機関へ提出すること。

12. 添付資料

・資料１_再委託承認申請書

資料１_再委託承認申請書

再委託承認申請書

年　　月　　日

電力広域的運営推進機関
情報管理責任者　　殿

（受託者）住　　所
会 社 名
代表者名　　印

年　　月　　日付で締結した契約「　　」に関して、受託した業務の一部を下記のとおり再委託したく承認願います。

上記契約に係る遵守事項を再委託先にも徹底するとともに、再委託先の貴機関に対する一切の行為について最終責任は当社が負うこととといたします。また、貴機関による再委託先に対する直接の実地監査の実施要請があった場合には、業務委託契約書の（再委託）及び（報告、監査・監督）の条項の規定に基づき再委託先もその義務を負うことを確約し、協力することを誓約いたします。なお、申請内容に異動・変更が生じた場合は、速やかに再申請いたします。

再委託先（　　次委託先） 住所　　： 会社名　： 代表者名：
再委託する業務内容・範囲（別紙によることも可）
再委託する理由・必要性（別紙によることも可）
再委託期間 年　　月　　日　から　　年　　月　　日　まで
再委託に関する契約書の有無（有の場合写しを添付、無の場合その理由） □　有　（　　） □　無　（　　）