外部委託業者の募集

References: IO/24/CFT/70001110/LLU

“IT Security Global Support"

（IT セキュリティのグローバルサポート）

IO 締め切り 2024 年 6 月 17 日(月)

〇前文

この技術仕様書は、サービスおよび供給のための一般管理仕様書（GM3S）- [Ref 1]と組み合わせて読まれるべきであり、技術要件の完全な一部を構成します。

疑義が発生した場合、技術仕様書の内容が Ref [1]の内容を優先します。

〇目的

これらの技術仕様書は、枠組み契約の業務範囲を定義します。IO/IT（ITER機構情報技術）は、インフラストラクチャのITセキュリティを評価し、強化し、管理するためのコンサルティングおよび専門知識サービスを提供する契約者を求めています。

枠組み契約が完了すると、IO ITは、各ロットについて以下のプロセスを通じてタスクオーダーを設定します：

IO:サービスタスクのリクエスト

契約者:サービス、プロフィールおよび価格提案

IO:タスクオーダー提出

契約者:サービスの提供。

ロット

現在の技術仕様書は、2つのロットに分かれています：

ロット1: 拡張セキュリティワークフォース

このロットでは、熟練したプロフェッショナルサービスの提供業者を求めています。これらのサービスは、サイバーセキュリティオペレーションセンター（SOC）の運用のためのレベル2の専門知識を提供する上で重要な役割を果たします。さらに、契約期間中にサイバーセキュリティの改善プロジェクトを内部でリードします。ロット1の契約者は、フルタイムでの参加を提供し、連続性を確保し、サイバーセキュリティ能力の積極的な向上に貢献することが期待されています。

ロット2: 高度なサイバーセキュリティ専門知識

ロット2は、特定のプロジェクトにアドホックな形で貢献できる高度なサイバーセキュリティサービス向けに設計されています。この専門知識は、重要なイニシアチブに従事するプロジェクトチームの一部となり、必要に応じて専門的な洞察力とサポートを提供します。特定のプロジェクトの業務範囲内で結果を提供した実績のあるサービスを求めています。

〇作業範囲

1. IOの技術環境

- サーバ環境：
  - Windows Server
  - HyperVクラスタ
  - Linux
  - Kubernetes、Docker
- ビジネスアプリケーション：
  - SAP
  - .NET VB、C#
  - SmartPlant、PLM
  - Catia/Enovia
- 科学計算：
  - HPC Linux（RedHat Satellite、2500コア、200ユーザー、25TBのデータ）
- ネットワーキング：
  - Ciscoネットワーキング
  - Cisco Wifi
- ITセキュリティ：
  - F5 BigIP
  - Checkpoint FW
  - PaloAlto FW
  - Fortinet FW
  - SIEM：Elastic Search Cluster、Logstash、Kibana、TheHive、Cortex
  - MS Defender
  - Sysmon
  - セキュリティVA：Nessus
- クラウドサービス：
  - Azure / Entra ID
  - Microsoftセキュリティ、Azureセキュリティセンター、Microsoft Defender
- アクセス制御および物理的セキュリティシステム。
- デジタル計測および制御：
  - SCADAシステム：
  - EPICS
  - SIMATIC WinCC Open Architecture、WinCC
  - RHEV + RHSストレージ
  - プラントシステムスローコントローラ：Siemen Step7 PLC

○　プラントシステム高速コントローラ：産業用グレードPC、IOシャーシ（NI PXIe、NI cRIO、xTCA）。

フィールドデバイスコントローラとそのフィールドバスプロトコル、例えばModbus、Profibus…
(以下詳細は英文技術仕様書を参照ください)

〇契約スケジュール

本枠組み契約は、3 年間の確定期間に加えて 2 回の任意の 1 年を含む 5 年間で設定されます。タスクオーダーは、IO IT によって特定されたニーズに応じて設立されます。各活動の成果物についての詳細は英文技術仕様書を参照ください。

〇経験

IO IT が要求する各サービスについて、契約者は、タスクを遂行するための提案されたチームメンバーの詳細な履歴書を提供します。IO IT は、要求されたタスクに対するチームのスキルセットの適切さを評価します。

提供されるサービスは、要求されるサービスに関連する IO/IT 環境要素の適切な知識を持つチームメンバーによって実行される必要があります。適切な IT セキュリティの専門知識は、適切な経験と認定資格（CISSP、OSCP、CEH、GPEN、CASP、GIAC GSEC など）によって示される必要があります。

契約者は、プロジェクトマネージャー（契約者のプロジェクトマネージャー）を指名し、そのプロジェクトマネージャーがチームを率い、管理、監督するものとします。IO は、契約者のチームメンバーを監督しません。

（詳細は英文技術仕様書を参照ください）

【※　詳しくは添付の英語版技術仕様書「Site-wide central supervision of ITER fire protection systems」をご参照ください。】

ITER 公式ウェブ　http://www.iter.org/org/team/adm/proc/overview からもアクセスが可能です。

「核融合エネルギー研究開発部門」の HP：　http://www.fusion.qst.go.jp/ITER/index.html では ITER 機構からの各募集（IO 職員募集、IO 外部委託、IO エキスパート募集）を逐次更新しています。ぜひご確認ください。