意見招請に関する公示

次のとおり調達物品の仕様書案の作成が完了したので、仕様書案に対する意見を招請します。

令和８年９月15日

国立研究開発法人情報通信研究機構

契約担当理事　中山　裕司

◎調達機関番号　816　◎所在地番号　13

〇第１号

１　調達内容

(1)　品目分類番号　14

(2)　購入等件名及び数量　2026-2027年度サイバーセキュリティ統合システム基盤の構築　一式

２　意見の提出方法

(1)　意見の提出期限　令和８年10月15日17時00分まで必着のこと。

(2)　提出先　〒184－8795　東京都小金井市貫井北町４－２－１　情報通信研究機構サイバーセキュリティ研究所サイバーセキュリティネクサス CYNEX研究開発運用室　石川　大樹　電話　042－327－5238 E-mail ishikawa@nict.go.jp

３　仕様書案の交付

(1)　交付期間　令和８年９月15日から令和８年10月15日まで。

(2)　交付場所　情報通信研究機構ホームページの調達情報よりダウンロードして入手すること。

４　Summary

(1)　Classification of the products to be procured: 14

(2)　Nature and quantity of the products to be purchased: Hub for Integrated Knowledge, Operations, Monitoring, Analytics, Research, and Upskilling System, 1 set

(3)　Time limit for the submission of comments : 17:00 15 October 2026

(4)　Contact point for the notice: Hiroki Ishikawa, CYNEX Research, Development and Operations Laboratory, Cybersecurity Nexus, Cybersecurity Research Institute, National Institute of Information and Communications Technology, 4－2－1 Nukuikitamachi Koganei-shi Tokyo 184－8795 Japan ＴＥＬ 042－327－5238 E-mail ishikawa@nict.go.jp

仕　様　書

応札・応募を希望する場合、必ず機密保持誓約書を提出後に非公開仕様書を入手すること。

仕様書（非公開版）の交付を希望される方は、秘密保持誓約書を公告文書記載の担当部局へ

提出すること。

1　件名

2026-2027 年度サイバーセキュリティ統合システム基盤の構築

Hub for Integrated Knowledge, Operations, Monitoring, Analytics, Research, and Upskilling System

2　目的（用途）

本調達案件は、国立研究開発法人情報通信研究機構（以下「当機構」という。）において、サイバー攻撃対策の研究開発を推進するため、実際の業務環境に近いリアルな仮想環境上で、最新のサイバー攻撃を疑似的に再現できる大規模かつ高精度な次世代サイバー防御演習環境を構築し、その対処方法の研究及び実証等を行うと共にサイバーセキュリティ人材育成事業及び情報連携を行う。本調達は統合基盤を整備するものである。

3　共通事項

本仕様書に疑義が生じた場合、又は本仕様書に記載のない事項の詳細を決定する場合は、当機構担当者と速やかに協議し解決を図ること。協議に際しては、受注者において打ち合わせ議事録を作成すること。作成した議事録は、当機構の承認を得て発行すること。発行した打ち合わせ議事録に含まれる決定事項は、本仕様書に優先する。

なお、仕様書等の変更を要する事態が生じた場合には、協議をするので応じること。

4　納入期限

最終納品：2027 年 9 月 30 日

ただし、調達物品の数量及び構成内訳 項番：8.1.2～8.1.9、8.1.14～8.1.16 は契約の日の翌日から起算して 90 日以内納入すること。

受注者は可能な限り順次早期に納入をすること。

5　納入場所

5.1　納入・設置場所

〒923-1211
石川県能美市旭台２丁目１２番
国立研究開発法人情報通信研究機構　北陸連携研究センター
隣接地コンテナ型データセンター内 ラック設備あり

5.2　書類等提出場所
〒184-8795
東京都小金井市貫井北町４－２－１
国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所サイバーセキュリティネクサスCYNEX研究開発運用室

6 調達物品の数量及び構成内訳

仕様書（非公開版）を参照のこと。

7 全体構成

仕様書（非公開版）を参照のこと。

8 調達物品の要件

仕様書（非公開版）を参照のこと。

9 提出書類等
（1） 書類等一覧

	名称	数量	納品形式	提出期限	備考
①	納品書	１式	データ又は紙形式	納入期限まで	
②	説明書・マニュアル等	１式	データ又は紙形式	納入期限まで	
③	保証書	１部	データ又は紙形式	納入期限まで	本件調達物品に付帯する保証内容、保証期間を明示したもの。
④	製品にかかるサポート実	１式	データ又	納入期限ま	

	名称	数量	納品形式	提出期限	備考
	施体制及び担当部署の連絡先を明示した資料		は紙形式	で	
上記①～④は、受注者が通常、発行している方式でよい。					
⑤	性能検査書	1部	データ又は紙形式	納入期限まで	
⑥	議事録	1部	データ又は紙形式	打合せ後、速やかに。	打合せ議事録を発行した場合（3.共通事項参照）
⑦	設置報告書	1部	データ又は紙形式	納入期限まで	関係する機器の設置状況、配線状況がわかるように写真、図面等で報告書を作成すること。 納入品の固定方法に関する資料
⑧	説明会等実施報告書	1部	データ又は紙形式	納入期限まで	
⑨	検査計画書	1部	データ又は紙形式	納品検査実施1週間前まで	
⑩	検査報告書	1部	データ又は紙形式	納入期限まで	
⑪	設備等納入時確認チェックリスト	1　部（別紙様式）	データ又は紙形式	納入期限まで	仕様書最終頁の様式を使用してください。
⑫	納入機器及びその部品構成等（CPU、メモリ等の製品名等）やソフトウェアの構成（SBOM: Software Bill of Material））のリスト	1式	データ又は紙形式	納入期限まで	
⑬	預かり証兼データ破棄届	1部	データ形式		クラウドサービスからの破棄も含む

（2）提 出 先

東京都小金井市貫井北町４－２－１
国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所サイバーセキュリティネクサス
CYNEX 研究開発運用室

10 納入・設置条件

10.1 納入・設置時間

原則、土日休日及び年末年始（12 月 25 日から 1 月 5 日）を除く、平日 9 時から 17 時の間に行うこと。やむを得ない場合日時は別途調整する。

10.2 納入・設置場所の条件

［7.1 共通事項］に記載の通り。ほか入館や搬送にかかる入館者申請、車両申請等は別途指示する。

10.3 納入・設置作業に関する条件

10.3.1 納入時の作業日程と体制を納入予定日の 1 カ月以上前までに提示すること。

10.3.2 設置・調整等作業のスケジュールについては入念に事前打合せを行い、そのスケジュールに従い完了すること。

10.3.3 装置の設置・組み立て・電気配線・配管を行い、内部機構動作、装置機構の調整・確認を行うこと。

10.3.4 納入時には、装置・実験室に塵や埃等が付着・飛散しないように注意し必要な処置・養生を施すこと。

10.3.5 装置の導入・動作に関して必要となる電気配線（2 次側）、排気ダクト・循環冷却水・圧空配管等のユーティリティー、付帯設備については全て準備・繋ぎ込みを行うこと。

10.3.6 納品物の設置に当たっては、建築設備耐震設計・施工指針[国土交通省国土技術政策総合研究所及び独立行政法人建築研究所監修]等の各種基準例を参照し、適切に固定すること。

10.3.7 機器の移設・更新時に対応できるように、各ケーブル類にタグをつけること。名称のつけ方は当機構担当者と調整すること。

10.3.8 物品の搬入・据付等に関しては当機構の業務に支障をきたさないように配慮し、協議の上、実施すること。

10.4 環境への配慮

10.4.1 調達物品が「国等による環境物品等の調達の推進等に関する法律」（グ

リーン購入法）で規定する特定調達品目に該当する場合には、可能な限り適合品を納入するように努めること。

10.4.2　製品の包装又は梱包は、可能な限り簡易であって、再生利用の容易さ及び廃棄時の負荷低減に配慮するように努めること。

10.4.3　納入時においては、環境負荷の低減を実現した自動車を用いるように努めること。

10.4.4　梱包材などは持ち帰り、法令に従い処分すること。

10.5　注意事項

10.5.1　運送・搬入・据付実施中に、建築物、工作物等に損傷を与えた場合は、速やかに当機構担当者に申し出るとともに受注者の責任においてこれを原形に復すること。

10.6　教育体制等

10.6.1　機器の搬入・設置後、納入期限までに当機構担当者に対して機器の操作についての説明会を１回行うこと。日時は別途調整する。なお、説明会を実施した際には、説明会等実施報告書（様式適宜）を提出すること。

11　支給品の有無

無

12　貸与品の有無

無

13　検査について

納入場所において、当機構担当者により装置の員数確認及び動作確認を行う。

検査に際しては、予め検査計画書を作成し、当機構担当者の承認を得ること。その検査計画書に基づき当機構担当者による検査を実施する。その後、検査結果の報告書を作成し、当機構担当者の承認を得ること。

14　契約の目的物の種類又は品質に関する担保責任　（契約不適合責任）

当機構が本件調達物品について、納入検査合格後、所有権移転の日から起算して１か年以内に、契約の内容(目的物の種類、品質又は数量）に適合しないことを発見したときは、受注者にその内容を通知するものとし、受注者は当該物品の修補、代替物の引渡し又は不足分の引渡しによる履行の追完等、担保の責を負うこと。

15　関連文書及び関連仕様書

15.1 無

16 情報セキュリティについて

16.1 適切な情報セキュリティ管理の実施

受注者は、適切な情報セキュリティ管理を実施していること。適切な情報セキュリティ管理を実施しているとは、組織としての情報セキュリティ方針及び情報セキュリティ管理体制が制定され、リスク対応計画立案、管理策の実施、教育、内部監査を含む情報セキュリティ管理が、文書化された手順に従って実施されていることを言う。ISO/IEC 27001 又は JIS Q 27001 に準拠した管理は、適切な情報セキュリティ管理の例である

16.2 業務実施体制

受注者は、本業務を履行する体制について、予め以下の事項について提出し、当機構の了承を得ること。

16.3 業務実施体制

① 責任者　（専門性・実績・国籍等に関する情報を含むこと）
② 担当者　（専門性・実績・国籍等に関する情報を含むこと）
③ 連絡体制・窓口
④ 業務実施場所（国内・国外を問わず当機構外で業務する場合）
⑤ プロジェクト期間中の各担当者のエフォート率

16.4 構築すべき体制に関する留意点

受注者は、下記に留意して、体制を構築すること。なおこれらに変更があった場合は速やかに当機構に報告し、その了承を得ること。

① 本業務を履行するにあたり必要な経験、資格、業績等を有する者を確保して体制を構築すること。その際、必要な経験、資格、業績等を有する者は、背景となる適切な経歴、知見、語学、文化的背景を有することを書面で証明すること。
② 本業務を履行するにあたり受注者の従業員若しくはその他の者による意図しない変更や業務に関して知り得た情報の窃取や他言等が行われないことを保証する管理体制を構築すること。
③ プロジェクト管理者は IPA 情報処理技術者プロジェクトマネージャ合格もしくは PMP 資格を有すること。もしくは PMP 資格と同等以上の資格を有していることを書面で証明すること。なお経験年数等は PMP 資格以上の実力および専門性を有するとは判断できないためこれを認めない。
④ ネットワーク担当者は IPA 情報処理技術者ネットワークスペシャリスト合格

もしくはネットワークスペシャリスト資格と同等以上の資格（CCIE R&S 等）を有していることを書面で証明すること。なお経験年数等はネットワークスペシャリスト以上の実力および専門性を有するとは判断できないためこれを認めない。

⑤ 生成 AI エージェント等を利用する場合は提案審査時に詳細を提示すること。当機構の許可を得ず生成 AI/LLM を使用することは許可しない。当機構の審査と承認を受けた範囲において生成 AI を利用することは許可する。

16.5 情報セキュリティ対策の実施

受注者は、業務に関して知り得た情報の紛失、滅失、改ざん、き損、漏えい、その他の情報セキュリティ事故を防止するために必要な情報セキュリティ対策を講じなければならない。

16.6 情報セキュリティ対策の実施

情報セキュリティ事故発生時における報告

受注者は、契約の履行中、履行後を問わず情報セキュリティ事故、又はそのおそれのあることを知ったときは、必要な措置を講じるとともに、速やかに当機構に報告し、当機構の指示に従うものとする。

16.7 情報セキュリティ対策の実施

情報セキュリティ対策の実施状況の報告・点検

16.7.1 情報セキュリティ対策の実施

当機構は業務や情報の取扱いが適切に行われていることを確認するため、受注者に対して定期的な報告や自己点検、情報の適正な取扱いのための情報セキュリティ対策（ログの取得・監視等以下参照）を求めることができるものとする。

・情報セキュリティインシデント等への対処能力の確立・維持
・情報へアクセスする主体の識別とアクセスの制御
・ログの取得・監視
・情報を取り扱う機器等の物理的保護
・情報を取り扱う要員への周知と統制
・セキュリティ脅威に対処するための資産管理・リスク評価
・委託先が取り扱う情報及び当該情報を取り扱うシステムの完全性の保護
・セキュリティ対策の検証・評価・見直し

16.7.2　　情報セキュリティ対策の実施

特に重要な業務（情報の格付けに伴い重要と格付けされた業務、（例）個人情報を含むもの）を委託している場合、監査、サービス品質の保証を求めることができるものとする。また、個人情報を含む重大な情報セキュリティ事故が発生した場合、機構は受注者と協議の上、立入調査を求めることができるものとする。報告・点検の結果、改善が必要な点が見つかった場合、受注者は改善計画を立て当機構に提出するものとする。

16.7.3　　委託の制限

ア　受注者は当機構が書面で承諾した場合を除き、本件業務の全体又は一部を第三者に委託してはならない。受注者は第三者に委託するときは、責任を持って情報セキュリティの適切な管理を行う能力を有する者を選定するものとする。

イ　選定した委託先に対しては、情報セキュリティに関し受注者が履行すべき義務と同等の義務を負わせるものとし、受注者及び受注者の委託先との間で締結する契約書にその旨を明記するものとする。

ウ　受注者は委託先の情報セキュリティ管理全般、業務実施体制、情報セキュリティに関する点検・調査の受け入れ可否等の状況について、あらかじめ当機構に書面で提出するものとする。受注者の委託先が再委託を行うとき以降も同様とする。

エ　本案件で委託をおこなう場合は、応札提案・審査時に委託先・委託金額・委託内容について委細明示し提示すること。

16.7.4　　情報の目的外利用及び提供の禁止

受注者は業務に関して知り得た当機構所定の書式・方法により明示した保護すべき情報（契約を履行する一環として受注者が収集、整理、作成等した情報であって、当機構が保護を要さないと確認したものを除く。）その他の非公知の情報を本仕様書の業務履行にのみ利用し、他の目的に使用しないこと。当機構の承諾なしに第三者に提供してはならず、受注者は受注者の従業員その他受注者の委託先及びその再委託先に対し、受注者と同様の秘密保持義務、情報保全義務を負担させるものとする。

16.7.5　　要機密情報の取扱い

受注者は、当機構の要機密情報を取り扱う場合、契約書の秘密保持の事項に従うこと。

16.7.6　　情報の複写又は複製の禁止

受注者は、本業務のために当機構から提供された情報や資料等を当機構の承諾なしに複写又は複製してはならない。

16.7.7　　情報の受取り

当機構が一時的に電子ファイル等を受注者に預ける場合は、預かり証に受注者（作業員等を含む）の押印あるいは署名を求める場合があるので応じること。

16.7.8　　情報のやり取り

ア　当機構と通信回線を経由して電子ファイル等のやりとりを行う場合は、万一の事故に備えてパスワード付与や暗号化などの措置をとること。

イ　また最新のパターンファイルが適用されたウイルス検出ソフトで検査し、問題がないことを確認してから送付すること。

16.7.9　　資料・情報の保管

ア　受注者は、業務のために当機構から提供を受け、又は受注者自らが作成した情報が記録された資料を、適切に施錠管理された場所に保管すること。

イ　電子ファイルの場合は適切なアクセス制御が行われたフォルダーに保管すること。また当機構が特に指定した場合は暗号化などの対応をとること。

16.7.10　　情報セキュリティ対策の実施

資料の返却・情報の消去等

ア　受注者は、業務のために当機構から提供を受け、又は受注者自らが作成した情報が記録された資料は、業務完了後直ちに当機構に返還し、又は引き渡すものとする。ただし、当機構が別に指示したときは当該方法によるものとする。

イ　受注者は、情報を記録した資料を当機構に返還した後、なお当該情報が複写や電磁記録等として残されていることのないよう、遅滞なく復元又は判読が不可能な方法により当該情報を消去又は廃棄しなければならない。なおその際「預かり証兼データ破棄届」を当機構に提出すること。

17　クラウドサービス又は外部サービスの利用について

17.1 クラウドサービスの利用

受注者は、業務においてクラウドサービスを利用する場合には、事前に申し出ること。

17.2 クラウドサービスの選定

ア　クラウドサービスは、原則として ISMAP 又は ISMAP-LIU（以下、ISMAP 等）のクラウドサービスリストに登録されているクラウドサービスを利用すること。

イ　やむを得ずISMAP等のクラウドサービスリストに登録されていないその他のクラウドサービスを利用する場合には、ISMAP等と同等以上のセキュリティ対策を実施しているサービスを利用すること。

ウ　情報の格付けに係わらず、利用するクラウドサービスのサービス提供事業者は、ISO/IEC 27001（JIS Q 27001）等の情報セキュリティに関する第三者認証を取得している、或いは同等以上の情報セキュリティ管理を行っていること。

エ　情報の保存先は、情報の格付けに応じて日本国内のデータセンターを利用すること。

17.3 クラウドサービスの運用

ア　画一的な約款や規約等への同意のみで利用可能となる（無償の）クラウドサービスにより、要機密情報の取扱いはできない。

イ　クラウドサービスにおいて要機密情報を取り扱う場合、通信の暗号化（TLS1.2以上）を行うこと。エンドツーエンドの暗号化が可能な場合、これを用いること。

ウ　クラウドサービスに保存した情報は、管理すること。不要となった情報は速やかに削除する又はアクセス権を削除する等の対応を実施すること。

エ　情報の格付けによっては、クラウドサービスが利用できない状況になった際の代替手段を用意すること。

オ　クラウドサービスの利用者は、ID、パスワードにより管理し、多要素認証を用いること。

カ　システムログの保存

情報の格付けに応じて、アクセス制限を実施し、情報利用のログを取得・管理すること。

キ　本業務を第三者に委託する場合、委託先がクラウドサービスを利用する際にも、受注者と同様ここに示す事項を適用すること。

ク　クラウドサービスで取扱う情報は、当機構担当者の示す機構の定める格付けとそれに応じた取扱いを行うこと。

17.4 クラウドサービス利用の終了

クラウドサービスの利用終了の際、受注者は、利用のためのアカウントや、システムログ、クラウドサービス上に保存した情報を完全に抹消し、預かり証兼データ破棄届を当機構に提出すること。

18 提案書の取扱いについて

本件について、総合評価落札方式又は企画競争(公募型プロポーザル方式)により実施される場合は、仕様書並びに製作仕様書等で提案した内容に基づき履行すること。

設備等納入時確認チェックリスト

受注者確認欄	項目	要求者確認欄
□	1.　納入期限内の納品となっているか。	□
□	2.　員数検査 納入品について、仕様書及び業者提案書に記載された構成及び数量を満たしているか。	□
□	3.　外観検査 納入品について、傷、汚れ、凹み、歪みといった不良が無いか。	□
□	4.　設置状況 納入品に係る電源等への接続状況は要件を満たしているか。 納入品について、基準に基づき固定措置がされているか。	□
□	5.　機能検査 納入品について、仕様書及び業者提案書に記載されている、機能及び性能等の要件を満たしているか。	□
□	6.　提出書類 仕様書に規定した提出書類はすべて揃っているか。 提出書類に求めている記載内容は漏れなく記載されているか。	□
完了 □ 非該当 □	7.　法令遵守関係 1. 納入物について、電波法（昭和 25 年法律第 131 号）、建築基準法（昭和 25 年法律第 201 号）、その他の関係法令等に基づき、関係機関等に対する協議、必要な認可、許可、届出等の手続又は届出等に必要となる情報の提供が完了しているか。 （該当法令及び書類名称を以下に記載。記載しきれない場合は別紙	□
報告済 □ 非該当 □	2. 納入物について、構成品（部品）も含めて 10kHz 以上の周波数を使用する高周波利用設備に該当していないか。該当する場合は高周波の周波数と高周波発生部の最大出力（ピーク値）を文書で報告させているか。ただし、型式指定及び型式確認が明らかに確認できた場合を除く。	□

受注者側担当者　　確認年月日	財務部手続欄
会社名	資産管理 台帳反映
担当者名	
機構側要求者（監督員）　　確認年月日	
国立研究開発法人情報通信研究機構	
部署名	
要求者名	

※該当項目なき場合は、当該項目を二線にて抹消する（項目 7 を除く）。
※原本は機構側要求者（監督員）において保管し、写し 1 部を検査調書へ添付する。

秘密保持誓約書

国立研究開発法人情報通信研究機構
契約担当　殿

私（以下「乙」という。）は、国立研究開発法人情報通信研究機構（以下「甲」という。）の「2026-2027 年度サイバーセキュリティ統合システム基盤の構築」の調達（以下「本調達」という。）への参加に関し、甲が乙に対して開示する情報について、以下の事項を遵守することを誓います。

記

1　本調達に関連して、甲から開示された情報（仕様書：2026-2027 年度サイバーセキュリティ統合システム基盤の構築に掲げる資料を通じて知り得た情報を含むが、これに限らない。以下同じ。）は、本調達にかかる提案書等の作成業務に従事する乙の役員及び従業員以外のいかなる者にも開示若しくは漏洩し、又はかかる提案書等の作成以外のいかなる目的のためにも使用しない。

2　本調達に関連して甲から開示された情報を複写又は複製しない。また、乙が当該情報に基づいて発明、考案、意匠、著作物又はその他の創作等をなしたときは、直ちに甲に通知し、その扱いについて甲の指示を受ける。

3　本調達の結果が判明したとき又はそれ以前に甲の指示があるときは、その時点で、本調達に関連して甲から開示された全ての秘密情報を、甲の指示に従って返却又は破棄（情報の消去を含む。）のうえ、速やかに「データ返却・破棄届（別紙）」を提出する。

4　前各項に定める義務に違反し、甲に損害を与えた場合は、これを賠償する。

年　　月　　日

乙（住所）
（商号又は名称）
（部署名）
（役職氏名）

（連絡先）

別紙

データ返却・破棄届

国立研究開発法人情報通信研究機構
契約担当　殿

私（以下「乙」という。）は、国立研究開発法人情報通信研究機構（以下「甲」という。）の調達への参加に関し、下記のとおり、甲が乙に対して開示した全ての秘密情報を返却又は破棄したことを報告します。

記

１．案件名　2026-2027 年度サイバーセキュリティ統合システム基盤の構築

２．秘密情報の受領日　　年　　月　　日

３．返却／破棄の別（いずれかに〇を付ける）　　返却　／　破棄

４．返却／破棄の実施日　　年　　月　　日

年　　月　　日

乙（住所）
（商号又は名称）
（部署名）
（役職氏名）
（連絡先）