

仕様書

1 件名

所内ネットワーク再構築業務委託

2 履行期間

契約日から令和7年3月31日

3 調達要件仕様書

別添、「所内ネットワーク再構築業務委託仕様書」のとおり

4 対象拠点

（地独）神奈川県立産業技術総合研究所 海老名本部、溝の口支所、殿町支所

5 協議

本仕様書に記載されている事項及び本仕様書に記載のない事項について疑義が生じた場合は、発注者との協議のうえ、その決定に従うものとする

所内ネットワーク再構築業務委託仕様書

本仕様書は、地方独立行政法人神奈川県立産業技術総合研究所(以下、「KISTEC」又は「発注者」という。)が、調達する所内ネットワーク再構築業務委託に関して、設計・機器導入・設定等の受注者が行う作業など、必要な要件を示すものである。なお、本仕様書に明記していない事項についても、ネットワークの機能上又は情報セキュリティ対策上で当然備えるべき事項については、仕様に含まれるものとする。

1 目的

KISTECでは令和4年度から海老名本部ネットワーク網の刷新工事の実施し、モバイルPCの導入を進め、所内DXの推進やデジタル化を進める企業へのデジタル技術を活用したサービスの提供に向けたネットワーク環境の整備を順次進めているが、Web会議やクラウド利用が進むなかインターネット接続環境の改善や無線LAN導入など、利用者の利便性向上が求められる一方、所内ネットワークの情報セキュリティ対策向上への取り組みも急務である。

本業務は、上記の背景を踏まえ、所内ネットワークの再構築の取り組みを進め、職員の利便性向上と情報セキュリティ対策の更なる向上を図ることを目的とする。

2 履行期間

契約日から令和7年3月31日

※項目7で指定した成果物については3月14日までに一次提出を行い、発注者の確認後、修正事項を反映して履行期間内に提出すること

3 業務全般に関すること

- (1) 本案件に関する作業において、打合せ、現地調査・作業等で作業員がKISTECに出入りする場合は、必ず事前に作業員の所属する組織名、組織の住所及び組織の代表電話番号に加えて、各作業員の所属部署、役職、氏名、連絡先（直通電話番号、電子メールアドレス等）を通知又は申請し、発注者の承認を得ること。
- (2) 本案件においてKISTEC内での作業について、受注者は発注者と協議・調整の上、発注者の指示により行い、仕様書に示された導入機器のほか、受注者側の対応と明記されたもの以外の作業用資源（機器類等）、作業場所、その他必要となる環境や費用については、受注者の負担で用意すること。
- (3) 受注者が故意又は過失により、作業用資源等の一部又は全部を、滅失又は毀損した場合は、受注者の負担で速やかに原状に復すること。
- (4) 本案件の設計、構築、機器設定、展開、テスト等、すべての納入品の搬入はすべて受注者が責任をもって実施し、対象範囲の稼働確認を行うこと。なお、これらに要する費用はすべて本調達に含まれる。

4 導入機器

別紙1「導入機器一覧」のとおり（受注者負担で用意すること）

5 対象拠点・機器

本案件で対象とする拠点は、海老名本部、溝の口支所、殿町支所とする。

本案件で対象とする機器は、次のとおりと、各種作業を実施する。

対象機器(新規)：別紙1「導入機器一覧」のとおり（受注者負担で用意すること）

対象機器(既存)：別紙2「既存機器情報」のとおり

6 設計・導入に係る要件

(1) プロジェクト計画書等の作成

本業務の実施に先立ち、本業務に係る作業内容、作業体制、スケジュール表、成果物等を定めたプロジェクト計画書を作成し、発注者の承認を受けること。

(2) 設計

基本設計及び詳細設計を行い、発注者の承認を受けること。

(3) 環境構築・テスト

テスト工程における実施内容、テストの実施体制、スケジュール、テスト環境、テストデータの利用方針等を定めたテストにおける実施計画書を作成し、発注者の承認を受けること。また、テスト工程の実施結果について、実施結果報告書を作成し、発注者の承認を受けること。

7 作業内容

(1) ローカルブレイクアウト環境の導入

SaaS利用が増加することで将来的にインターネット環境が輻輳する可能性があることから最適な構成への見直しを行う

ア 次の用途で利用するローカルブレイクアウト用環境を構築する。

- ・ 現行所内ネットワーク接続パソコンからの特定SaaS接続用途として利用する。
- ・ その他インターネット接続は、従来どおり既存閉域網（WVS）経由のサービスを利用する。
- ・ 本部・支所間の所内通信は、既存閉域網（WVS）を利用する

イ 現行所外ネットワーク接続パソコンからのインターネット接続用途として利用する。

- ・ 所内システムへのアクセスは不可となるよう通信制限を設けるものとする。
- ・ 無線LAN、有線LANを各々別ネットワークセグメントとして作成する。

ウ ゲスト端末からのインターネット接続用途として利用する。

- ・ 所内アクセスは不可となるよう通信制限を設けるものとする。
- ・ 無線LAN、有線LANを各々別ネットワークセグメントとして作成する。

エ デバイス数

海老名本部：300台規模

溝の口支所：100台規模

殿町支所：10台規模

オ 構成

- ・ 所内端末からの経路①：特定SaaS通信：ローカルブレイクアウト
- ・ 所内端末からの経路②：その他のインターネット通信：既存閉域網(WVS)から接続

- ・ 所内端末からの経路③：所内間通信：既存閉域網(WVS)

※ローカルブレイクアウトのインターネット接続については、現行WVSからのインターネット接続と同等のUTM機能での導入とする

カ 可用性

- ・ 回線及び機器はシングル構成とする。
- ・ 全拠点対象とし機器のみコールドスタンバイとする。

キ 回線要件

- ・ 10G又は1Gベストエフォート回線
- ・ 固定IPサービスを利用

(2) 無線LAN導入

利用の拡大によるLTEの通信量制限や有線機器管理の煩雑さが課題となっているため、無線LAN導入により利便性を向上させる

- ・ 無線LANは次の構成の用途で利用するものとし、必要な認証設定や証明書発行は既存認証サーバを利用して実装するものとする。詳細については、別途調整する。
- ・ 所内インターネット用無線LANでクライアント証明書を利用する場合には、所内無線LANへの接続が不可となるよう証明書等で制限を設けるものとする。
- ・ 証明書は個別発行(ユーザ毎に発行する)することを前提とし、発行手順を作成する。

ア 評価用AP台数

- ・ 海老名：8台、溝の口：2台、殿町：1台
- ・ LAN配線及びAP設置作業は、別途、発注者側で対応する

イ ロケーション

別途協議とする

ウ 構成

将来的に庁舎全体を無線LANの導入範囲とするが、今回は、評価のための設置とし、範囲は一部エリアのみとする

無線LANはクラウドコントローラで管理する構成であること

既存の有線LAN環境に追加可能であること

- ・ 無線①(所内)：所内、インターネットアクセスを許可する。認証はEAP-TLS認証
- ・ 無線②(所内からインターネット)：インターネットアクセスのみ許可し、所内アクセスは不可とする。認証は802.1x想定
- ・ 無線③(ゲスト)：eduroamを利用したゲスト環境の提供。

エ その他

- ・ 認証サーバは既存認証サーバを利用すること
- ・ 端末側の設定は、発注者側作業するが、適宜支援を行うこと。

(3) 所内LANセキュリティの向上

不正な機器が接続できる構成となっていることから、証明書認証もしくはMACアドレス認証を導入し、セキュリティ強化を図ること

現行パソコンで、固定IPで運用しているものについては、セキュリティ強化のため、原則、DHCPで取得できる構成に変更すること

本案件では次のとおり認証LANを作成し、テスト環境で想定どおりの動作となることを確認する。エンドユーザ環境への本番導入は、利用者の利用状況を確認して個別に移行時期の調整が必要であることから、本番導入をするための手順作成は本案件範囲とし納品すること。

ア 構成

認証LAN環境は、新規ネットワークセグメントを用意し既存環境に追加する。認証サーバは既存認証サーバを利用する。なお、詳細は、調整の上実施する

- ・ 認証LAN①【所内有線LAN】

EAP-TLS認証、DHCP取得、信制限なし(LB0については一部制御予定※既存踏襲)

- ・ 認証LAN②【所内無線LAN】

EAP-TLS認証、DHCP取得、通信制限なし(ローカルブレイクアウトについては一部制御予定)

- ・ 認証LAN③【所内有線LANインターネット接続専用】

MACアドレス認証、DHCP取得又は固定IP、インターネット接続のみに制限

- ・ 認証LAN④【所内無線LANインターネット接続専用】

802.1x認証(PEAP又はEAP-TLS)、DHCP取得、インターネット接続のみに制限

- ・ 認証LAN⑤【有線LAN】

認証なし、DHCP取得又は固定IP、通信制限なし。将来的に所内リソースへの接続制限を実装する(既設セグメント)

- ・ 認証LAN⑥【有線LAN】

MACアドレス認証、DHCP取得、インターネット接続のみに制限

- ・ 認証LAN⑦【無線LAN】

eduroam、DHCP取得、インターネット接続のみに制限

(4) セグメント分割

現行ネットワークは、適切なセグメント分割となっていないため、障害発生の際に切り分けを含め対応が困難であり、性能上の問題で全体への影響も大きくなるため、適正なセグメンテーションのLAN環境を維持できるようにする。

- ・ 拠点セグメントの方針と拠点への新セグメントの導入を範囲とする。

エンドユーザ環境への本番導入は、利用者の利用の状況を確認して個別に移行時期の調整が必要であることから、本案件では、拠点L3機器へのセグメント作成とDHCPサーバへのセグメント追加及びテスト環境での動作確認を行う。

(5) その他

次の項目は発注者側で実施するが、適宜、必要な支援を行うこと

- ・ 閉域網(WVS)への変更申請関連
- ・ ローカルブレイクアウト用のインターネット回線手配
- ・ クライアント端末の変更
- ・ eduroamサービスへの申請及び問い合わせ

8 本業務における成果物は次のとおりとし、発注者が指定した期日までに提出すること。

- (1) プロジェクト計画書
- (2) 基本設計書
- (3) 詳細設計書
- (4) コンフィグ／パラメータシート
 - ・ 現行機器パラメータシート(現行ドキュメント改版想定)
 - ・ 新規機器パラメータシート
 - ・ コンフィグ
- (5) テスト計画書兼結果報告書
 - ・ 現地試験仕様書兼成績表
 - ・ 作業当日スケジュール及び手順書
- (6) 各種操作手順書
 - ・ 現行機器運用手順書(現行ドキュメント改版想定)
 - ・ 新規機器運用手順書
 - ・ NW構成図(現行ドキュメント改版想定)
 - ・ 認証LAN本番導入手順
 - ・ eduroamの本番化手順
 - ・ 各種マニュアル
 - クラウドネットワーク管理システム ダッシュボード管理方法
 - UTM 簡易設定方法 (MX)
 - ルーティング設定方法 (MX)
 - VLAN 追加、ACL 設定方法 (MS)
 - SSID 追加、認証設定方法 (MR) 等

9 成果物の作成及び提出

- (1) 受注者は、紙及び記録媒体により成果物をそれぞれ2部（正・副）提出すること。
- (2) 成果物を納入するための記録媒体は、受注者において準備すること。
- (3) 紙のサイズは、日本産業規格A4判を原則とする。図表については、必要に応じてA3判を使用することも可とする。
- (4) 電子ファイルの形式は、MicrosoftのWord、Excel及びPowerPoint並びにPDF形式とする。ただし、PDF形式とした場合は、元の電子ファイルも併せて提出すること。
- (5) 記録媒体の形式は、CD-R又はDVD-Rとすることし、記録媒体に保存する形式は電子ファイルの形式と同じとすること。

10 守秘義務について

別添の「特記事項」を参照すること。

11 協議

本仕様書に疑義又は定めのない事項が生じた場合には、発注者と別途協議の上、決定すること。ただし、業務遂行に当たり、当然必要と認められる軽微なものについては、受注者の負担でこれを行うものとする。

導入機器一覧

No	項目	型番	製品名	数量	単位	備考
1	Merakiルーター	MX95-HW	Meraki MX95 Router/Security Appliance	4	台	海老名本部、溝の口支所
2		LIC-MX95-SDW-5Y	Meraki MX95 Secure SD-WAN Plus License and Support 5YR	2	式	
3		MA-PWR-CORD-JP	Meraki AC Power Cord for MX and MS (JP Plug)	4	本	
4		MX68-HW	Meraki MX68 Router/Security Appliance	2	台	殿町支所
5		LIC-MX68-SDW-5Y	Meraki MX68 Secure SD-WAN Plus License and Support 5YR	1	式	
6		MA-PWR-CORD-JP	Meraki AC Power Cord for MX and MS (JP Plug)	2	本	
7	Merakiレイヤ3スイッチ	C9300-24T-M又は C9200CX-12P-2X2G-E	Meraki C9300 24-port data only又は Catalyst 9000 Compact Switch 12-Port PoE	2	台	溝の口支所
8		LIC-C9300-24E-5Y又は C9200CX-DNAE12-5Y	Meraki C9300 24-port Enterprise License 5 year又は C9200CX Cisco DNA Essentials, 5Y Term Li	2	式	
9		MA-PWR-CORD-JP	Meraki AC Power Cord for MX and MS (JP Plug)	2	本	
10	Meraki WiFi6Eアクセスポイント	MR57-HW	Meraki MR57 Wi-Fi 6E Indoor AP (屋内モデル)	11	台	海老名8台、溝の口 2台、殿町1台
11		LIC-ENT-5YR	Meraki MR Enterprise License 5 Years	11	式	
12	無線AP用Powerインジェクタ	MA-INJ-6	Meraki mGig 802.3bt PoE Injector (PowerCord Not Included)	11	台	
13		MA-PWR-CORD-JP	Meraki AC Power Cord for MX and MS (JP Plug)	11	本	
	合計					

※ 電源やラックマウントキット等、設置のための必要な部材は用意すること
クラウド管理型ネットワークのダッシュボード機能で一括管理又は監視が可能なネットワーク機器及びライセンスとすること
機器本体については、5年間の保守付とする（平日9時～17時受付、4時間着対応、オンサイト保守）
日本語の取扱説明書等を添付すること
設置据付後は、梱包材等不要品は引き取り処分を行うこと。

既存機器情報

拠点	用途	詳細	数量
海老名本部	認証サーバ兼DHCPサーバ	RADIUS GUARD S V7 500ライセンスセット(ライセンス数 : 500)	2
		RADIUS GUARD S V7 DHCPオプション	2
		外部LDAP/AD参照オプション	2
		RADIUS GUARD S V7 アドバンスド関係オプション	2
	コアL3スイッチ	AT-x550-18XTQ	1
	集約スイッチ・フロアスイッチ	AT-x550-18XTQ	6
	エッジスイッチ①	AT-x530L-52GPX	12
	エッジスイッチ②	AT-SH230-10GT うち、本案件内で変更する対象は、30台程度を予定	225
	WANルータ	Si-R G110B	1
溝の口支所	フロアスイッチ	C1200-16T-2G	10
殿町支所	フロアスイッチ	C1200-8T-2G	6