仕　様　書

1. **件　名**　ネットワーク等基盤の構築委託

2. **数　量**　1 式

3. **履行期間**　契約日から 2025 年 3 月 31 日まで

4. **履行場所**　東京都立産業技術研究センター本部　東京都江東区青海 2-4-10
東京都江東区青海 2-5-10 テレコムセンター東棟
多摩テクノプラザ　東京都昭島市東町 3-6-1
墨田支所　東京都墨田区横網 1-6-1 KFC ビル 12 階
城南支所　東京都大田区南蒲田 1-20-20
食品技術センター　東京都千代田区神田佐久間町 1-9

5. **支払方法**
本契約の履行を確認の上、受注者からの請求に基づき 60 日以内に支払うものとする。

6. **用語の定義**

本仕様書で用いる用語の定義を表 1 に示す。

表 1　用語の定義

用語	定義
都産技研	地方独立行政法人東京都立産業技術研究センターの略称
受注者	本業務委託の実施に関し、都産技研と委託契約を締結した個人もしくは会社その他の法人
契約図書	本業務委託の契約書(以下「契約書」という。) および本件における納品物等の成果資料
都産技研職員	契約図書に定められた範囲内で、受注者に対する要請、承認、協議、本業務委託履行状況の確認等の職務を行う職員
役職員	都産技研に所属している職員
管理者	デジタル化推進室に所属する職員
現行ネットワーク	現在のネットワークシステムを構成する機器およびソフトウェア・セキュリティなどのサービスの総称
新ネットワーク	新たに構築するネットワークシステムを構成する機器およびソフトウェア・セキュリティなどのサービスの総称
認証システム	情報端末の事務系ネットワークへの接続制御をするシステム
拠点	本部、テレコムセンター、多摩テクノプラザ、墨田支所、城南支所、食品技術センター、バンコク支所を指す
WAN 回線	拠点間を接続する通信回線
LAN	拠点内のネットワーク
事務系ネットワーク	通常業務に使用するネットワーク
装置	都産技研に設置されている試験・分析機器など
端末	役職員が利用するノートパソコンまたは、デスクトップパソコン
機器利用事業	役職員以外の不特定多数のものが試験機器を利用する事業。機器利用事業で利用する装置は、機器利用事業専用でなく、研究などにも利用される。
SASE	Secure Access Service Edge の略称 ネットワークセキュリティと WAN の機能を統合したアーキテクチャ

Saas	Software as a Service の略称 ソフトウェアサービス	
SDN	Software Defined Networking の略称 ソフトウェアを用いたネットワークを制御する技術	

7. 委託の概要

7.1. 委託の趣旨

都産技研は、東京都内に本部(テレコムセンターを含む)、城東支所、墨田支所、城南支所、食品技術センター、多摩テクノプラザ、海外にバンコク支所(タイ王国)を設置しており、都内中小企業への技術的な支援を行うことにより都内中小企業の振興を図り、都民生活の向上に寄与することを目的として、設置された公設試験研究機関である。

都産技研が 2018 年度に導入した現行のネットワークを構成する機器およびソフトウェア等が保守終了および老朽化によって更新の時期を迎えている。都産技研は、自らが研究開発するだけでなく、支援事業として企業から試料等をお預かりして試験を行う依頼試験事業、機器の空き時間を利用してお客様に試料等を持ち込んで機器を使用していただく機器利用事業を行っている。試験研究に用いられる機器は事業間で共用されることもある。また機器の中には、必ずしも安全でないものを取り扱う関係上、場所を定めておかなければならないものも存在する。新型コロナウイルス感染症の流行により、自宅勤務・リモートワークといった働き方も拡がっているが、適切な労務管理、各事業における適切なセキュリティ対策も怠ることはできない。ネットワーク上に存在する、ネットワークに接続されている都産技研の資産を適切に管理することが求められている。また、電話の IP 化、PHS からスマートフォンへの移行も行われている。

今後のデジタルトランスフォーメーションの推進のため、セキュリティ対策が十分できており運用性が高い新ネットワークを求めており、現行ネットワークの機能を維持・有効活用したリプレースを前提としつつ、表 2 のような課題の解決を図りたい。

表 2　解決したい課題の一例

No	項目	課題	対応策例
1	職員が利用する端末のネットワーク接続プロセスの改善	接続までのプロセスが煩雑	プロセスの自動化 不正端末の見える化
2	ネットワークのセキュリティ設定管理の改善	プロキシやファイアウォールなど別々の製品を利用しているため、都度設定が必要	管理を一元化できるサービスの導入 SASE の導入など
3	ネットワーク機器の管理	管理の工数が複雑。ネットワーク機器のインシデント発生時に対応までに時間がかかる。	ネットワーク機器を一元管理できるサービスの導入 トラブルシューティングの可視化・自動化サービスの導入など
4	通信量増加への対応	Web 会議等の利用が増え通信量が増加	通信の最適化 トラフィックの制御など
5	本部・支所の無線 LAN 利用エリアの改善	本部・支所内で、無線 LAN を利用できる箇所が少ない。	無線 LAN アクセスポイントの増設
6	機器利用のネットワークのセキュリティ対策	都産技研の機器利用事業用のセキュリティ対策が不十分	端末にセキュリティポリシーが設定できるようにするか、ネットワークを論理的に切り分けなど
7	情報セキュリティ対策の見直しと強化	各種システムのクラウド移行や DX 推進に伴い、セキュリティ対策の見直しが必要	SASE などを導入して、クラウド利用時の制限を導入

7.2.　委託の範囲

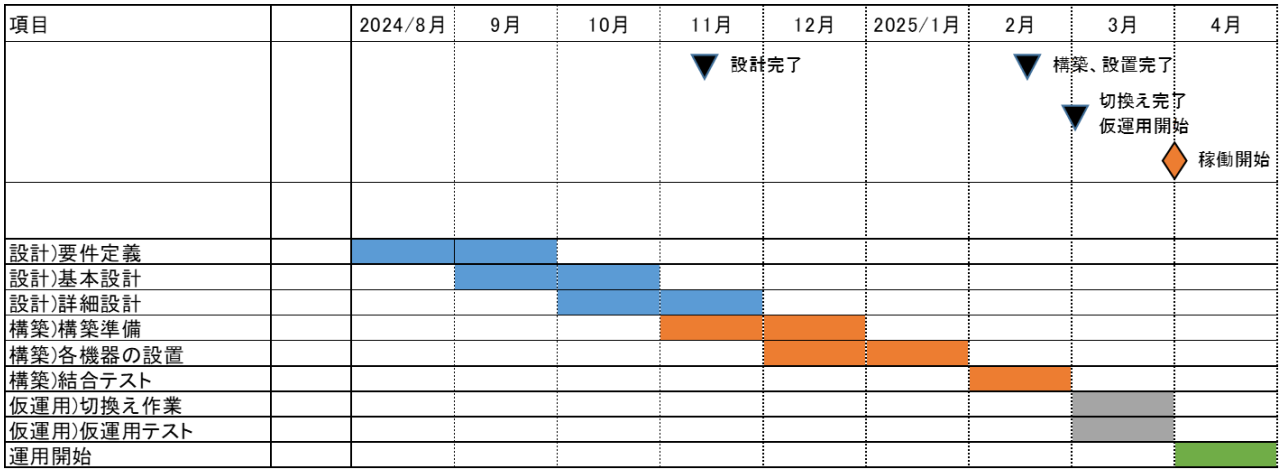
本委託は，新ネットワークを構成するハードウェアおよびソフトウェア、セキュリティ対策の導入までの管理業務、設計，構築(設定、試験、設置、移行)、導入したシステム・機器・ソフトウェアの保守の提供までを委託の範囲とする。

1. 管理業務は、作業実施計画書の作成，進捗管理、品質管理、課題管理等を実施し、包括的に管理すること。
2. 設計業務は、現行システムで稼働しているネットワーク設定および通信要件をすべて継続できる設計とし、本委託で追加されるサービスなどの要件を確認したうえで、適切なネットワークサービスや機器を選定し、設計すること。
3. 構築業務は、現行環境への影響を可能な限り抑制する計画を立案、設計に従い機器やソフトウェアを準備、設定・試験・設置して、現行環境から移行をすること。
4. 保守は、本委託で構築したシステム・機器、ソフトウェアなどを安定稼働するためのマニュアル(運用者や管理者向け)を整備し、2025 年 4 月 1 日から 2026 年 3 月 31 日の期間のハードウェアおよびソフトウェア不具合は、契約不適合責任の範囲で対応すること。

7.3.　委託のスケジュール

1. スケジュールは表 3 を考慮し、2025 年 4 月 1 日から新ネットワークの運用が開始できるようにすること。
2. 作業期間は本業務の受注者が提案可能とするが、詳細は都産技研と協議の上で確定すること。また、作業期間を策定する際には、都産技研による作業やレビューに必要な期間等も考慮した現実的な期間を策定する間を早める場合は、都産技研と協議すること。

表 3　運用開始までのスケジュール案



7.4.　構築の対象となる拠点

対象となる拠点は以下表 4 の通りとする。

表 4　設置などを行う拠点

	拠点名	住所(東京都内)
1	本部 (テレコムセンター含む)	江東区青海 2-4-10 青海 2-5-10 東棟 1 から 3 階
2	多摩テクノプラザ	昭島市東町 3-6-1
3	墨田支所	墨田区横網 1-6-1 KFC ビル 12 階
4	城南支所	大田区南蒲田 1-20-20
5	食品技術センター	千代田区神田佐久間町 1-9

城東支所については、現在大規模改修中のため、改修の目途が立ち次第、別契約として依頼する。

8. **納入成果物**

1　成果物の名称と提出期限の目安案を表 5 から表 8 に示す。委託途中段階で修正および見直しが必要な場合は、都産技研と協議し、再提出すること。受注者は、下表の書類を電子媒体（CD-R 又は DVD-R）で 2 部(正・複)提出すること。電子媒体は、都産技研のクライアント PC にて読み取り可能な Microsoft Word ファイル、Microsoft Excel ファイル、PDF ファイルで提出すること。

2　プロジェクト管理に関する納入成果物

表 5　プロジェクト管理に関する納入成果物の名称と提出期限の目安

名称	内容	期限(目安)
作業計画に関する文書	各成果物と関連付けた作業スケジュール、作業内容、作業担当者、レビュー実施計画、チェックポイント、開始条件/終了条件等プロジェクトの作業工程(WBS)、設計・構築段階計画を定義する成果物。	締結後 1 か月以内
情報セキュリティに関する文書	各作業工程において、内外の要因に伴う情報セキュリティ上の問題に対する対策案を計画する成果物。	締結後 1 か月以内
品質管理に関する文書	各作業工程において、本調達仕様書にて記述する各種要件を満たしていることを保証する品質確保・維持に関する成果物。	締結後 1 か月以内
人的資源管理に関する文書	各作業工程における作業体制に関する成果物および参画要員の保有スキル等に関する成果物	締結後 1 か月以内
課題管理に関する文書	遂行上、様々な局面で発生する課題について、課題の認識、対応案の検討、解決および報告のプロセスを定めた成果物。	都産技研と別途協議
情報伝達管理に関する文書	関連情報の作成、共有および蓄積等に関する基準（会議体開催方法、議事録管理方法等）を定める成果物	締結後 1 か月以内
用語定義集	使用する用語について定義した成果物	締結後 1 か月以内
議事録	各種打合せ時の議事録	都産技研と別途協議

3　設計・構築に関する成果物

表 6　設計・構築に関する成果物の名称と提出期限の目安

名称	内容	期限(目安)
構築計画書	ネットワークを構築するに当たり、構築全体を俯瞰し、作業工程、作業手順等を定める成果物。	締結後 1 か月以内
設計・構築実施計画書	ネットワークの設計・構築段階における体制、スケジュール、標準的な管理要領等について定める成果物	締結後 1 か月以内
要件定義書	都産技研の要件を調査して、要件をまとめた成果物	締結後 2 か月以内
基本設計書	都産技研の要求事項を整理し、利用サービスや製品を確定させた上で物理的なネットワーク構成、機器構成等を定めた成果物	締結後 3 か月以内
詳細設計書	基本設計書に基づき、各サービスおよび各機器へ設定するパラメータの設定根拠および設定ルール	締結後 4 か月以

	等を示す成果物	内
機器設置図	ネットワークが設置する機器等の設置箇所を示す成果物	締結後 5 か月以内
設計書	ネットワークにおける各サービスおよび各機器への設定パラメータの値を示す成果物	締結後 4 か月以内
テスト計画書	テストの実施スケジュール、実施内容、進捗の予定等、テストの計画を示す成果物	締結後 6 か月以内
研修計画書(役職員が利用する端末で作業がある場合)	役職員に対する研修内容、実施計画等を定める成果物	仮運用開始前まで

4　移行・導入に関する成果物

表 7　移行・導入に関する成果物の名称と提出期限の目安

名称	内容	期限(目安)
移行実施計画書	移行スケジュール（移行準備から正常稼動確認までにわたる日程計画、イベント、役割分担、チェックリスト等)、移行検査基準、新ネットワーク切替え判定基準、リスク発生時の対応期限、本稼動可否の協議およびそのタイミング等、システムを安全かつ円滑に移行するために必要な移行方針を定義した成果物。移行実施計画書は、全体計画書、拠点毎計画書を分けて作成し、関係する都産技研の承認を得た上で、移行・導入作業を実施すること。 各関係者間での調整や認識合わせを構築事業者が主体的に行うために活用すること	締結後 4 か月以内
移行手順書	移行・導入から運用開始にいたる手順を記述した成果物。移行・導入工程に入る前までに標準となる移行手順書を作成し、都産技研の承認を得ること。 標準となる移行手順書に個別システムおよび利用拠点毎に異なる事象を追加、変更した移行手順書を作成すること	締結後 4 か月以内
移行結果報告書	事前準備作業結果、移行処理実施結果、移行検証結果 等、移行作業の結果を報告する成果物	移行完了
テスト実施要領	テスト計画書に基づいて、テストの開始条件/終了条件、テスト管理方法、テスト環境、テスト運営方法等、テストの実施要領を示す成果物	締結後 4 か月以内
テスト結果報告書	テストの実績、障害対応、実施結果、残課題、品質指標、次工程開始の見通し等、テストの結果を報告する成果物	都産技研と別途協議締結後 5 か月以内

5　保守成果物

表 8　保守に関する成果物の名称と提出期限の目安案

名称	内容	期限(目安)
運用計画書	ネットワークの運用体制および各種手順等を定めた成果物	仮運用開始前まで
運用マニュアル	機器利用および障害発生時等におけるネットワークの運用に係る担当者の作業手順等を定めた成果物。	仮運用開始前まで
構成管理書	機器および関連システムの設定等に関する成果物。	運用開始前まで
サービス提供要領	継続的・安定的なサービスを利用者に提供するための実施手順を定めた成果物	運用開始前まで
研修用テキスト	運用者・管理者向けの操作マニュアル、研修用テキスト等	運用開始前まで
運用に係る情報セキュリティ実施手順	ネットワークを運用する上で遵守すべき情報セキュリティ実施手順を定めた成果物	運用開始前まで

6　その他の成果物

必要と判断された納入成果物を都産技研と協議の上別途提出すること。

16. 現行ネットワークの構成

16.1. 現行ネットワークシステムの概要

1．本委託で更新を検討する現行ネットワークシステムを構成する機器の台数は、添付資料別紙１「現状機器一覧」を参照すること。ネットワーク構成は、添付資料別紙２「ネットワーク構成図」を参照すること。

2．そのほか現行ネットワークについて資料が必要な場合は、入札期間中に都産技研本部にて職員立会いのもと情報(ルーティング情報、基本設計、仮想ネットワーク設定情報、物理・論理構成図など)を開示する。なおコピー等の複写およびデータでの受渡しは不可とする。

3．本部と支所、テレコムセンターは商用回線を利用してインターネット VPN 接続をしている(詳細は 9.4 を参照)。また、都産技研とは別テナントの Azure、AZCloud と SINET クラウド接続をしており、Azure と VPN 接続もしている。

4．バンコク支所は、VPN ルータを介して本部の LAN として接続している。

5．インターネットへの接続は本部の SINET 回線を経由して行っている。支所、テレコムセンターに L3 スイッチがあり、アクセスリストによるセグメント間制御を行っている。本部については SDN が存在し、ファイアウォールが L3 スイッチ相当のテナント間通信の制御を行っている。

6．2024 年 4 月から仮想化基盤(メモリ 256GiB、HDD/SSD:1.92TiB×2、HDD:6TiB×2 を 3 ノード分)を運用(CPU は 20%程度、メモリは 60%程度利用)している。本委託にてこの仮想化基盤を利用してもよいが利用せずに置き換えてもよい。利用する場合は、サービス提供期間を本委託で構築する機器と合わせことができるかを受注者にて確認して提供すること。※仮想化基盤を利用する場合は、都産技研が契約している Windows server2022 datacenter を利用することも可能である。

7．2024 年 4 月から新規に導入したファイアウォール(1 日の最大スループットは、1.1 Gbps 程度)を運用している。本委託にて上記の導入したファイアウォールを利用してもよいが利用せずに置き換えてもよい。利用する場合は、サービス提供期間を本委託で構築する機器と合わせことができるかを受注者にて確認して提供すること。

8．2024 年 4 月から新しく ActiveDirectory 用のサーバ(CPU:Xeon E2336、メモリ:16GiB、OS:Windows server2022 Standard)を本部と多摩テクノプラザに設置している。本委託にてこのサーバを利用しても良いが利用せずに置き換えてもよい。利用する場合は、サービス提供期間を本委託で構築する機器と合わせことができるかを受注者にて確認して提供すること。

９． 都産技研では、Microsoft365E5(defender、Intune、EntraID など)を契約している。本委託にてこれらの機能を利用する場合は、どの機能を利用するかなど都産技研と協議すること。

１０． 事業継続計画対策として ActiveDirectory を本部(物理サーバと仮想サーバ上)と多摩テクノプラザ(物理サーバ上)に合計 3 つ設置している。認証システムも本部および多摩テクノプラザに 1 台ずつ設置している。

１１． 職員が利用する情報端末は、認証システムにて MAC アドレスの登録および認証、または証明書の発行をしている。証明書は現在 560 枚程度を発行している。

１２． RADIUS サーバの 1 日あたりの認証数は、1, 000 から 1, 500 程度となる。なおこの認証数には有線接続と無線接続を切り替えての認証数も含む

１３． 情報端末の有線接続プロセスは、下記の流れとなる。

(ア) 役職員が購入した PC 等の情報端末の MAC アドレスを管理者に連絡

(イ) 管理者が RADIUS サーバに MAC アドレスと VLANID(一部のサーバのみ接続可能)を登録して、役職員に作業依頼(ドメインへの参加など)

(ウ) 役職員が作業完了後、管理者が,作業が完了しているかを確認。確認後 RADIUS サーバ上で VLANID を変更してネットワークに接続可能となる

１４． 情報端末の無線接続プロセスは、下記の流れとなる。

(ア) 9.1 の 13 の(ウ)までの作業を行う。

(イ) 管理者が RADIUS サーバに端末名を登録して、証明書を発行する。

(ウ) 情報端末をインターネットに接続させて作業を行う(証明書のインストールなど)

(エ) SSID の設定(証明書の設定)を行い、無線 LAN に接続可能となる。

１５． VLANID は 1,000 番、2,000 番、4,000 番台などで用途に分けて運用している。

１６． 本部は、一部の部屋以外のすべての部屋にエッジスイッチを配置しており、エッジスイッチまでは各階の EPS にパッチパネルを配置して光ケーブルを配線している。各支所は、サーバラックからエッジスイッチまで UTP ケーブル（CAT5、CAT5e、CAT６）で配線している。

１７． DHCP サーバは本部物理サーバ上に構築しており、NTP は本部内の物理サーバと仮想サーバ上にそれぞれ構築している

１８． 既存検疫サーバはアプライアンス製品で、仮想基盤（VMWare）上に構築している。稼働している VMware の仮想基盤は保守が延長できないため。運用を終了する。

16.2. 更新の対象

今回更新対象とする現行ネットワークを構成する機器は表 9 となる

表 9　現行ネットワークを構成する機器とサービス

現行ネットワークを構成する機器およびサービス類	ネットワークインフラを構成し、ネットワークサービスを提供するシステム 以下の機材とサービスを含む。 ・産技研外のクラウドへの接続、ネットワーク接続(SINET を利用) ・支所間接続(VPN ルータ) ・SDN コントローラ ・SDN スイッチ ・サーバスイッチ ・インターネットスイッチ ・L3 スイッチ ・L2 スイッチ ・認証スイッチ ・ファイアウォール ・無線 LAN 装置(コントローラ、アクセスポイント) ・ネットワーク配線(現行の配線を流用しつつスペックが足りない部分は新規に配線すること) ・仮想化基盤サーバ(※現行の仮想化基盤利用可能)

	・DHCP サービス(新規で立てても良い) ・DNS サービス（新規で立てても良い） ・NTP サービス(新規で立てても良い) ・メール中継サービス ・ログ管理サービス(本委託の調達機器が対象) ・ネットワーク監視サービス(本委託の調達機器が対象)

16.3. **利用人数と端末台数**

利用者人数は、職員数 560 名、端末台数 3,000 台以上、端末の OS は、Windows・Mac・Linux・Android・iOS・Chromebook 等を利用している。端末台数にはプリンタなどの端末も含み、同一端末での有線接続と無線接続は別の端末として数える。

16.4. **支所間接続回線**

現在、各拠点は別紙２より VPN ルータを通して本部を経由してインターネットに接続している。各拠点の VPN ルータ間は、UCOM の「光ビジネスアクセス　IP1」、又はソニーネットワークコミュニケーションズの「NURO　アクセス　スタンダード」、バックアップ回線として NTT 東日本の「光ネクスト VPN ワイド」を利用している。各拠点の速度は表 10 の通りである。

表 10　各拠点間の通信速度

拠点名	回線速度（1 Mbps は 1 000 000 bps とする）
多摩テクノプラザ	1 000 Mbps 以上
城南支所	100 Mbps 以上
墨田支所	100 Mbps 以上
テレコムセンター	100 Mbps 以上
食品技術センター	100 Mbps 以上

16.5. セグメント通信

VLAN セグメント間の通信制御は別紙 3「アクセスポリシー」を参照すること。それぞれに VLAN が割り振られており、〇が付いているところは通信ができるようにルーティングをしている。

10　新ネットワークに求める要求

10.1 新ネットワークに求める基本要件

1. 表 2 で示した課題のすべてについて解決を図るようなネットワークおよびセキュリティ対策が施されていること。
2. 最新の技術動向を踏まえたネットワークとセキュリティであること。
3. 現行ネットワークで稼働中のシステム(Azure 上に構築された技術支援事業管理システム・AZCloud 上に構築された総務システム・Azure 上に構築された財務会計システム)がすべて問題なく稼働・接続できること。各システムは、SINET クラウド接続で接続している。
4. バンコク支所の接続についても設定変更等行わずに接続することができること。
5. すべての拠点から共通して LAN に接続可能であること。
6. 各拠点から直接インターネットに接続できるとよい。(非必須)
7. 各拠点間の WAN 回線は、都産技研が利用している回線(9.4 を参照)を用いてもよい。(非必須)
8. 都産技研が利用している WAN 回線を用いない場合は、別途回線を用意すること。
9. 各種取得するログは、最低でも 30 日間は残すこと。また、ログは改ざんできないこと。
10. 各種取得するログは、一か所(一つの画面)で確認できるとよい。(非必須)
11. 現行業務に支障をきたすことのないネットワーク機器の選定・設計を行うこと。

12. ネットワークやシステムの応答時間がユーザにとってストレスのない範囲であること。また、通信データ量増加等により性能が低下しないように負荷分散を行うこと。
13. 構築後、負荷試験でレイヤー3 の往復経路遅延時間を確認すること。(遅延時間は、50ms 以下を目安とする)
14. プロトコルは、HTTP, FTP, SMTP, DNS、SIP など一般的なプロトコルが利用できること。
15. IPv4 プロトコル設計とすること。
16. 機器については IPv6 にも対応すること。
17. VLAN の割り当て や IP アドレスの払い出し、接続機器を管理できる機能を導入すること。
18. 役職員が利用する情報端末は、全面的に IEEE 802.1x 認証に移行(証明書が払い出しでき、いつでも利用できる状態)できるようにすること。
19. 無線 LAN アクセスポイントの設置は、天井や壁への固定を原則とすること。高天井に設置するのが難しい部分や温度・湿度などを管理している部屋への設置は、都産技研と協議して設置を検討すること。
20. 無線 LAN アクセスポイントは、別紙４の色がついている場所に必ず電波が届くように電波強度が周波数 2.4GHz または 5GHz で、－65dBm より電波強度が強いように配置すること。(別紙 4 の図面からヒートマップなどのシミュレーションをつけること)
21. 詳細な設置位置や台数は、受注後に現地調査やサーベイを行い必ず確認すること。設置後もサーベイをし、電波強度を確認し条件を満たしていない部分は改善すること。
22. スマートフォンで IP 電話（ZoomPhone など）が拠点内のどこでも利用できるように無線 LAN の電波範囲やアクセスポイントのローミングアシストなどで音声が途切れないことを考慮すること。
23. 現行ネットワークの接続構成および設定情報等は必要に応じて、新ネットワークへ引継ぐこと。
24. 移行および更新作業は、業務に影響が少なく最小限のネットワーク停止で実施できる移行方法であること。
25. DHCP、DNS、NTP は、都産技研で用意しているサーバを利用してもよい。(非必須)
26. DHCP、DNS、NTP は、都産技研で用意しているサーバを利用しない場合は、新規に構築すること。
27. SFP は、既設のものを再利用しても良い。ただし、接続確認などは受注者側で行うこと。また、故障時などは、継続利用サービスの範囲内で交換・修理などに対応すること。
28. 第三者のセキュリティ認証をうけた信頼性のある製品を導入すること。
29. 新ネットワークに独自技術がある場合は、根拠を示すこと。

10.2 **利便性･運用性**

1. 一般的に入手できるハードウェアとソフトウェアで構成し、管理者の使用や運用において特別な知識やスキルを必要とせず、GUI および CLI で操作できること。
2. 2030 年 3 月 31 日までは、運用が可能な構成であること。
3. 規格がある機器等については、標準化された規格を採用すること。
4. 本部・支所間でネットワーク設定更新時の方法に差異がないこと。
5. 機器等のファームウェアおよびソフトウェアは、安定している最新のバージョンを導入すること。
6. ネットワーク構成や無線 LAN 環境の現状を確認できること。
7. 端末の基本的な情報（ユーザ名、端末名、デバイスタイプ、MAC アドレス、IP アドレス 等）のログを取得して、確認できること。
8. 端末の基本的な情報で、無線 LAN の接続モード（IEEE 規格）や AP への接続履歴、ネットワークへの接続経路、接続位置が確認できるとよい。（非必須）
9. 導入後、機器等の設定や各種ソフトウェアの設定変更や機能拡張（バージョンアップなど）を行う場合に追加費用を生じさせることなく変更ができること。
10. 障害発生時に、復旧のための原因特定が可能なログ採取を考慮すること。
11. 全拠点の LAN を構成する機器や機器の各種設定を統合管理する機能(稼働状況や利用状況の可視化など)があること。
12. ネットワーク設定、新規ネットワーク作成が GUI 等を用いて容易に行えるとよい。(非必須)
13. 設定は、API・プログラム言語を用いて自動化でき効率化できるとよい。(非必須)

10.3 **拡張性・柔軟性**

1. ネットワークを構成する機器等は、ユーザ数やデータ増加などの変化に対応できるような構成として、十分な拡張性や柔軟性を有すること。今後の目安として、ユーザ数 600 人前後、端末台数は 4000 台前後(※ユーザや端末台数は、年度ごとに増えていくため、増加分のライセンスなどは別契約として、調達する)を想定している。
2. 今後予想される追加変更要件(組織改編・事業拡張、ユーザ数や端末台数増など)に柔軟に対応できるだけの十分な性能を有した構成とすること。
3. 有線ポート不足で機器を追加する際に、システム停止や長時間のリビルトを必要とせずに拡張ができる構成とすること。
4. VLAN 間のルーティング、フィルタ設定が容易にできること。
5. トラフィック量は、現在 2Gbps で運用しているが、最大で 10Gbps に拡張が可能なこと。
6. 費用の上限を設定して高負荷時に、自動拡張でき安定した性能を提供できるとよい。(非必須)
7. 拠点が追加された場合、既存のネットワーク環境や性能への影響がすくないとよい。(非必須)
8. 拠点が追加された場合、簡易にネットワーク設定などができるとよい。(非必須)

10.4 **信頼性・可用性**

1. 機器等は、停電などの場合を除き平日 9 時から 17 時の営業時間内の可用性が 99.5%など安定した連続運用ができること。
2. 機器等の故障時に対応するため、予備機を用意すること。
3. システム全体に影響を与える主要な部分は、機器等を冗長化してシステムが停止しない構成とすること。
4. ネットワーク機器故障時の冗長系への切替えは、ホットスタンバイまたはウォームスタンバイとして数分以内での切換えを基本とすること。(目安は 10 分以内)
5. 本部では、サーバ室より機器収容箱への光配線で冗長化されている部分はこれを活用してもよい。(非必須)
6. 主要な機器は、電源を冗長化して、電圧低下対策として無停電電源装置を導入すること。
7. 導入する機器で時刻設定が可能なものは NTP を用いた同期設定をすること。
8. 事業継続計画発動時、多摩テクノプラザで事業を継続するため、多摩テクノプラザ単独でも有線 ・無線での接続およびインターネットアクセスが利用できること。また、認証サーバを用いた認証機能が有効であること。
9. WAN 回線で障害が発生し、稼働できなかった場合の業務継続性を確保するための措置(サブ回線など)を講じること。

10.5 **セキュリティ**

1. セキュリティに関する設定がソリューション上の GUI で設定できること。
2. セキュリティインシデントが発生した場合に、原因を特定するために関連機器（端末や各スイッチなど）のログを集約し、各機器のログを横断的に検索・分析可能な仕組みを導入すること。
3. 拠点外(自宅や出張先などの場所)からのリモートアクセスを検知できること。
4. ユーザ毎に適切なアクセス制御ができること
5. ユーザ管理や個人情報などの重要なデータへアクセスした際のアクセスログを取得し、管理者が確認できるとよい。(非必須)
6. 各サーバへの不正侵入を検知・阻止できる仕組みを導入すること。
7. 機器等の監視ができるようにし、障害や異常時に管理者に警告を発する仕組みを考慮すること。現状、ZABBIX を使用しているが、本製品の継続利用か新規製品の選択は問わない。なお監視対象は、本委託で構築した機器のみとする。
8. MAC アドレスによらない端末の特定・管理が可能であること。
9. MAC アドレス偽装を検知する機能があるとよい。(非必須)
10. 管理外の端末が接続された場合、ネットワークへの通信ができないこと。

11. ネットワークに接続するサーバや端末等の全機器について、接続許可や認証情報が登録・管理できる機能を導入すること。
12. 不正接続が発見された際、不正接続機器の固有情報(IP アドレス、端末名、MAC アドレスなど)が特定可能であり、ネットワーク接続を停止させ、メールなどで管理者にアラートを発する機能があること。
13. サービス拒否攻撃(DoS 攻撃)があった場合に、アクセスを遮断しメールなどで管理者にアラートを発する機能があること。
14. 情報改ざんがあった場合に、メールなどで管理者にアラートを発する機能があること。
15. 主要な機器は、鍵付きのラックやボックスなどに搭載し管理者以外が操作できないようにすること。
16. プロファイル(ポリシー)を満たさない端末の検知が可能なこと。
17. プロファイル(ポリシー)を満たさない端末の検知後に自動で端末のネットワーク接続を停止させることが可能であるとよい。ポリシーは Windows の場合、 OS バージョン、更新プログラムの適用などを想定している。(非必須)
18. 上記は、Mac OS、Linux（Ubuntu） に関しても同様の動作が可能であるとよい。(非必須)
19. セキュリティ用のエージェントを導入する場合、業務への影響および端末への影響を明確にすること。
20. 都産技研の事業ごとにセキュリティに配慮し、VLAN などで論理的に LAN を分離できること。
21. 機器利用事業で用いられる端末は役職員も利用する。外部利用者など不特定多数も利用するため、端末のセキュリティを考慮すること。
22. プロキシやファイアウォールの設定の一元管理、クラウドサービスの利用状況の可視化、端末の状態確認をしてアクセスを制御できる SASE 製品を導入すること。

10.6 新ネットワークを構成する機器に関わる共通要求

1. 各機器は、現行の機器(別紙 1)と同等以上かそれ以上の性能を満たす機器であること。
2. 機器類は、学術情報ネットワーク(SINET)に 10 Gbps 以上で接続されることを前提とし、性能を活かせること。
3. 安定した運用が可能であり、機器や LAN の稼働情報(各機器の異常や LAN の接続状況など)を確認できること。
4. 利用人数と端末台数を考慮したうえで、十分な処理性能を有すること。
5. EIA 規格に準拠した 19 インチラックにマウントが可能なこと。
6. 冗長構成を組む機器は、テストを実施し想定通りの動作を保証すること。
7. ループ検知機能を設定し、設置時に動作確認をすること。

10.7 サーバスイッチとインターネットスイッチ

サーバスイッチは、内部のサーバ類をまとめ管理するスイッチ
インターネットスイッチは、外部ネットワークとの接続をするスイッチ(別紙２を参照)
これらを用いる場合は、下記要件を満たすこと。

1. スイッチング容量、最大パケット転送能力は搭載されたポートすべてでワイヤーレートの通信速度が出せて、新ネットワークの性能を損なわない性能であること。
2. ショートパケットでのワイヤーレートの通信速度が出せること。
3. 16 000 個以上の MAC アドレスを自動学習可能であること。
4. メインメモリ 2 GiB 以上、フラッシュメモリ 512 MiB 以上であること。
5. 2 台以上のスイッチをスタックして仮想的に 1 台のスイッチとして運用できる機能があること。また、スタック帯域は最大 40Gbps 以上であること。
6. 物理ポートごとにブロードキャスト/マルチキャストトラフィックを抑制する機能があること。
7. 2 000 個以上の VLAN を登録可能であり、また同時使用が可能なこと。
8. ポートベース又は、IEEE 802.1Q ベースまたは 802.1v プロトコルベースの VLAN をサポートしていること。
9. 同一 VLAN 内でのポート間の通信を不可にする機能があること。

10. IPv4 および IPv6 のルーティングをハードウェアで実行すること。
11. 2 048 個以上の IPv4 ルーティングテーブルを扱えること。
12. DHCP リレー機能を有すること。
13. MAC アドレスベースでの認証機能を有すること。また、MAC アドレスベースで認証した殆ど通信しない端末で、端末自身がログオフするか切断するまで認証状態を維持する機能を有すること。
14. 上記 10.6 の 12 はスタック構成でも対応できるとよい。(非必須)
15. 実現方法は問わないがパケットキャプチャ機能があるとよい。(非必須)
16. 設定を自動的にチェックポイントとして保存し、設定のロールバックができるとよい。(非必須)
17. 電源は冗長構成とすること。
18. スイッチ単体でサポートする機能はライセンス等の追加を必要とすることなく利用可能なこと
19. Web GUI を有すること。

10.8 コアスイッチ

コアスイッチは、データ転送や中継に用いるスイッチ(別紙 2 の QX-S5524GP-4X1C)
コアスイッチを用いる場合は、下記要件を満たすこと。

1. スイッチング容量、最大パケット転送能力は搭載されたポートすべてでワイヤーレートの通信速度が出せて、新ネットワークの性能を損なわない性能であること。
2. ショートパケットでのワイヤーレートの通信速度が出せること。
3. 制御端末を接続するポート（コンソールポート）を有していること。USB 2.0 または RJ-45 以外の方法で制御端末と接続する場合は、これらのいずれかへ端子変換するアダプタを付属すること。
4. 32 000 個以上の MAC アドレスを自動学習可能であること。
5. メインメモリ 2 GiB 以上、フラッシュメモリ 512 MiB 以上を有していること。
6. 2 台以上のスイッチをスタックし、仮想的に 1 台の論理スイッチとして運用可能にする機能を有すること。また、スタック帯域は最大 40Gbps 以上であること。
7. 物理ポートごとにブロードキャスト/マルチキャストトラフィックを抑制する機能を有すること。
8. 4 000 個以上の VLAN を登録可能であり、また同時使用が可能なこと。
9. VLAN の IP アドレスの設定が可能なインターフェースを 2 048 以上有すること。
10. 同一 VLAN 内でのポート間の通信を不可にする機能を有すること。
11. DHCP リレー機能を有すること。
12. ポリシーベースルーティング機能を有すること。
13. IEEE 802.1x 認証機能を有すること。
14. MAC アドレスベースでの認証機能を有すること。
15. MAC アドレスベースで認証した殆ど通信しない端末で、端末自身ログオフするか切断するまで認証状態を維持する機能を有すること。
16. 設定を自動的にチェックポイントとして保存し、設定のロールバックができるとよい。(非必須)
17. 電源は冗長化すること。
18. スイッチ単体でサポートする機能はライセンス等の追加を必要とすることなく利用可能なこと
19. Web GUI を有すること。

10.9 L3 スイッチ

L3 スイッチは、ネットワーク層機能を持ったスイッチ（別紙 2 の FG600D と QX-S5224GP-4X）
L3 スイッチを用いる場合は、下記要件を満たすこと。

1. スイッチング容量、最大パケット転送能力は搭載されたポートすべてでワイヤーレートの通信速度が出せて、新ネットワークの性能を損なわない性能であること。

2. ショートパケットでのワイヤーレートの通信速度が出せること。
3. コンソールポートを有していること。USB 2.0 または RJ-45 以外の方法で制御端末と接続する場合は、これらのいずれかへ端子変換するアダプタを付属すること。
4. 32 000 個以上の MAC アドレスを自動学習可能であること。
5. メインメモリ 2 GiB 以上、フラッシュメモリ 512 MiB 以上を有していること。
6. 2 台以上のスイッチをスタックし、仮想的に 1 台の論理スイッチとして運用可能にする機能を有すること。また、スタック帯域は最大 40 Gbps 以上であること。
7. 本部および多摩テクノプラザは 2 台以上設置し、他支所は、1 台以上設置すること。
8. 物理ポートごとにブロードキャスト/マルチキャストトラフィックを抑制する機能を有すること。
9. 4 000 個以上の VLAN を登録可能であり、また同時使用が可能なこと。
10. ポートベース又は、IEEE 802.1Q または 802.1v プロトコルベースの VLAN をサポートしていること。
11. VLAN の IP アドレスの設定が可能なインターフェースは 2,048 以上を有すること。
12. 同一 VLAN 内でのポート間の通信を不可にする機能を有すること。
13. IPv4 および IPv6 ルーティングをハードウェアで実行すること。
14. サポート可能なルーティングテーブル数は IPv4 が 6 000 以上、IPv6 は 3097 以上であること。
15. IPv4、IPv6 ルーティング･プロトコルとして、RIPv2、OSPF をサポートすること。
16. IPv4、IPv6 ルーティング･プロトコルとして、MP-BGP をサポーとしているとよい。(非必須)
17. IPv4, IPv6 の冗長化プロトコルとして VRRP, VRRPv3 をサポートすること。
18. IEEE 802.1x 認証機能を有すること
19. MAC アドレスベースでの認証機能を有すること
20. MAC アドレスベースで認証した殆ど通信しない端末で、端末自身がログオフするか切断するまで認証状態を維持する機能を有すること。
21. 設定を自動的にチェックポイントとして保存し、設定のロールバックができるとよい。(非必須)
22. 電源は冗長化すること。
23. 機器のサイズは 1U 以内であること。
24. スイッチ単体でサポートする機能はライセンス等の追加を必要とすることなく利用可能なこと。
25. Web GUI を有すること。

10.10　エッジスイッチ・PoE スイッチ

エッジスイッチは、末端で役職員の端末を接続するためのスイッチ
PoE スイッチは、無線アクセスポイントなどに給電をするためのスイッチ
エッジスイッチおよび PoE スイッチを用いる場合は、下記要件を満たすこと。

1. スイッチング容量、最大パケット転送能力は搭載されたポートすべてでワイヤーレートの通信速度が出せて、新ネットワークの性能を損なわない性能であること。
2. ショートパケットでのワイヤーレートの通信速度が出せること。
3. 8 000 個以上の MAC アドレスを自動学習可能であること。
4. メインメモリ 512 MiB 以上、フラッシュメモリ 128 MiB 以上を有していること。
5. 物理ポートごとにブロードキャスト/マルチキャストトラフィックを抑制する機能を有すること。
6. 送信または受信しかできないリンク状態を検出し、該当ポートを自動的にダウンさせる機能があるとよい。(非必須)
7. IEEE 802.3at または、802.3af または、802.3bt に基づく電力供給が可能なこと.
8. 4 000 個以上の VLAN を登録可能なこと。
9. ポートベース、IEEE 802.1Q ベースの VLAN をサポートしていること。
10. IP アドレスの設定が可能なインターフェースは 16 以上を有すること。
11. 同一 VLAN 内でのポート間の通信を不可にする機能を有すること。
12. IEEE 802.1x 認証機能を有すること。

13. MAC アドレスベースでの認証機能を有すること
14. MAC アドレスベースで認証した殆ど通信しない端末で、端末自身がログオフするか切断するまで認証状態を維持する機能を有すること。
15. 設定を自動的にチェックポイントとして保存し、設定のロールバックができるとよい。(非必須)
16. 機器のサイズは 1U 以内であること。
17. スイッチ単体でサポートする機能はライセンス等の追加を必要とすることなく利用可能なこと。
18. Web GUI を有すること。

10.11 無線アクセスポイント(AP)

無線アクセスポイントは、役職員の端末を無線 LAN で接続するための機器

1. 無線の規格として IEEE 802.11a/b/g/n/ac/ax に対応をしていること。
2. 2.4 GHz, 5 GHz, 6 GHz のうち、2 つの周波数帯を同時利用できる機能を有すること。
3. アンテナ内蔵タイプのアクセスポイントであること。
4. 電源アダプタでの電源受電が可能であるとよい。(非必須)
5. IEEE 802.3at または、802.3af または、802.3bt に基づく PoE 電源受電に対応をしていること。
6. 設定・管理用のコンソールポートを有すること。USB 2.0 または RJ-45 以外の方法で制御端末と接続する場合は、これらのいずれかへ端子変換するアダプタを付属すること
7. 状態確認用の LED を有し、点滅 /色で動作状態が判別可能なこと。天井設置の場合は、床面から LED が視認できること
8. AP ごとの利用率が容易に取得できること。
9. AP ごとに接続ユーザ、接続時刻のログが取得でき、レポートが表示できること。ログは個々の AP に接続しなくても取得できること。
10. Web、ssh による AP 管理が可能であること。また、AP の集中管理が可能であること。
11. 本部 4 階執務室に設置する機器は、ローミングアシスト機能、802.11i/k/v/r の規格に対応しているとよい。(非必須)

10.12 統合管理ソリューション

1. 日本語の GUI に対応しており、GUI でも各種操作ができること。
2. 機器(ネットワークを構成するハードウェア)やネットワークを管理できるソリューションであること。ソリューションはクラウドまたは物理環境、仮想環境のいずれかで動作すること。
3. 1 000 台以上のネットワークを構成する機器の管理ができること。役職員の端末は含まない。
4. ソリューションがクラウドで動作する場合、稼働率が 99.9%以上であること。また、クラウドが完全に停止しても、CLI などから各スイッチの機器設定やモニタリングができること。
5. ソリューションが物理環境の場合、管理機器へのアクセスは、コンソールアクセスに対応していること。
6. ソリューションで管理している機器の再起動ができること。
7. ソリューションで管理している機器の設定が可能なこと。
8. ユーザごとまたはグループごとにアクセス権限（参照のみ可、参照更新とも可）を個別に設定ができること。
9. アクセスログの取得と分析を実施し、監査証跡として 30 日以上保管できること。
10. 複数の拠点を一元的に管理する機能を有すること。
11. 管理している機器の設定を変更した際に、自動で変更が反映される機能を有すること。
12. 設定変更は、管理している機器に対して一括でできるとよい。(非必須)
13. 拠点を跨った複数の管理している機器をグループ登録して設定変更ができるとよい。(非必須)
14. ネットワーク機器をインターネットとの通信可能なネットワークへ接続するだけで管理や設定が可能となるゼロタッチプロビジョニングに対応可能であるとよい。(非必須)
15. PoE の電源供給機能の有効・無効の機能があるとよい。(非必須)
16. 管理しているスイッチの物理インターフェースの有効・無効の機能を有すること。
17. 管理しているスイッチのポート状態としてアップおよびダウンしているポートを表示できること。

18. 管理しているスイッチのポート状態はフロントパネル表示および一覧表示も対応可能なこと。
19. 管理しているスイッチのポート毎に動作状況、MAC アドレス、VLAN 情報などを表示可能であるとよい。(非必須)
20. 管理しているスイッチのポートにおける給電状況を一覧表示できるとよい。(非必須)
21. 管理しているスイッチのポート毎に PoE 給電情報を表示ができるとよい。また、PoE 消費電力についてはグラフ表示に対応しているとなおよい。(非必須)
22. 設定されている VLAN の情報を一覧で表示可能なこと。各 VLAN に対しては VLAN 名、VLANID を確認できること。
23. 拠点毎の管理機器のステータス、高メモリ使用のデバイス数、高 CPU 使用のデバイス数、高チャネル使用率、トラフィック利用状況、高ノイズの AP 数を一覧で確認するとよい。(非必須)
24. 端末が利用しているアプリケーションの利用率を一覧で確認することができ、拠点毎と拠点を跨った特定グループ毎に確認することができるとよい。(非必須)
25. 管理している機器の設置場所をサイトとして定義し、マップを使って管理できること。
26. 管理機器の相互接続状況を把握するためのトポロジー表示に対応していること。
27. 無線 LAN のヒートマップの表示、接続端末、不正 AP の位置情報も表示する機能があるとよい。(非必須)
28. 無線アクセスポイントのコントローラ障害時、有線スイッチの障害時（ハードウェアエラー）に、管理者にメールでアラート通知可能な機能を有すること
29. 接続端末数や端末タイプをレポート出力できること。
30. 管理機器のインベントリレポートを出力できること。
31. 上位の利用アプリケーション、上位の使用率端末、使用データの統計情報をレポート出力できるとよい。(非必須)
32. SSID 毎に何台の端末が接続しているかなども出力できるとよい。(非必須)
33. 使用率上位のスイッチとその使用率、有線アップリンク使用率ピーク時のトラフィック量の統計情報を取得できレポート出力できるとよい。(非必須)
34. 管理している機器からの任意の宛先への Ping による疎通確認する機能を有すること。
35. 管理している機器からの任意の宛先への Traceroute する機能を有すること。管理機器が統合管理ソリューションと通信できない状態でも、管理機器のコンソールに端末を接続してアクセスし、設定・状態の表示コマンドや debug をすることができるとよい。(非必須)
36. AI 等で接続や認証の障害を検知して、管理者にメールなどで通知出来る機能があるとよい。(非必須)

10.13 認証サーバ (RADIUS サーバ)

1. 日本語管理 Web UI に対応していること。
2. クラスタリング機能を有し、複数台で冗長構成が組めること。
3. 認証機能として、Web 認証、MAC アドレス認証、IEEE 802.1x 認証用 RADIUS 機能を有すること。
4. 柔軟な多要素認証を実現するため、認可情報として内部のデータベースを参照することで、スイッチや無線 LAN コントローラなどの機器側で MAC 認証の設定をせずとも MAC 認証を実現することができること。
5. マルチベンダーネットワークに対応しており、100 以上の RADIUS Vendor Dictionary がインストールされていること。
6. 端末情報をプロファイルする機能を有していること
7. 認証時に端末の OS タイプなどのプロファイル情報を元にポリシー付与する機能があるとよい。(非必須)
8. RADIUS CoA に対応し、認証済み端末のポリシーを変更することができるとよい。(非必須
9. Active Directory や EntraID などのユーザ情報を参照し、認証機能を提供できるとよい。(非必須)
10. Active Directory のドメインに参加する機能があること。
11. 複数の外部認証サービスと連携する機能があるとよい。(非必須)
12. RADIUS に対応していない有線デバイスにおいても、SNMP を使ってポリシーの適用が可能である

とよい。(非必須)
13. ユーザの属性や接続端末の情報等に基づき、予め決められた認証許可ルール(ロール)に従ってネットワーク接続を許可するロールベースのネットワーク認証制御機能(アクセス制御)があるとよい。(非必須)
14. ID やパスワード、MFA 認証などの機能を有すること。
15. 無線端末の IEEE 802.1x 構成プロファイルを自動プロビジョニングする機能を有すること。
16. Windows および Mac 端末でアプリケーションの導入や証明書の配布などを行えるプロビジョニング機能を有すること。
17. iOS, Android, chromebook, Ubuntu などの端末で上記のプロビジョニング機能があるとよい。(非必須)
18. 証明書の最大数は、3000 以上であること。
19. 証明書の無効化や失効等の管理を GUI 上で管理可能なこと。
20. 証明書の有効期限に対して管理者にメールなどで通知ができること。
21. 証明書発行時に検疫クライアントエージェントを同時に配布可能であるとよい。(非必須)
22. 登録済みの管理ユーザからの申請で証明書発行ができること。
23. 認証対象端末の検疫機能を有すること。認証対象端末の OS は、Windows, Mac OS, Linux(Ubuntu)をサポートしていること。
24. 上記の検疫機能は、iOS, Android をサポートしているとよい。(非必須)
25. 検疫項目としてセキュリティエージェントインストール有無およびバージョン管理ができること。
26. 以下検疫項目をサポートしているとよい。(非必須)
    (ア)指定するサービスの起動有無
    (イ)指定するプロセスの稼働有無
    (ウ)指定するレジストリキーの有無
    (エ)ピアツーピアアプリケーションのインストール有無
    (オ)Patch Management の有無
    (カ)指定する Windows 修正プログラムのインストール有無
    (キ)外部 USB デバイスの使用有無
    (ク)ネットワーク接続の状態
    (ケ)ディスク暗号化アプリケーションのインストール有無
    (コ)許可されていないアプリケーションのインストール有無
    (サ)端末に保存されたファイルの存在有無
    (シ)Firewall アプリケーションソフトのインストール有無およびバージョン管理
27. 検疫項目単位でのアクセス制御が可能であること。
28. エージェントは常駐型または非常駐型をサポートしていること。
29. エージェントレスの検疫機能をサポートしているとよい。(非必須)
30. 検疫状態が変化した場合に、Radius CoA で端末のポリシーを変更することができるとよい。(非必須)
31. 検査結果を外部のセキュリティ製品に渡せるとよい。(非必須)

10.14 SASE(セキュリティプラットホーム)

1. 包括的な WAN 機能とネットワークセキュリティ機能を組み合わせたプラットフォームを提供すること。
2. 外部 SaaS などで IP によるアクセス制限に対応できるために、契約者占有のグローバル IP が最低でも１つは割り当てられること。
3. 各サービスのソフトウェアバージョンアップやホットフィックスの適用は、サービス事業者により速やかに実施されること。クライアント側のアップデートはユーザ側で実施する。
4. 各機能の設定を管理 GUI で実施できること。
5. 各種セキュリティ機能の定義やパターンのアップデートは通信の停止を伴わず自動で実施されること。

6. ID 管理システムやオンプレミスの Active Directory または Entra ID と連携することで、各システム等へのアクセスについて、ID、場所および端末による認証を行い、適切なアクセス制御管理（IAM）が可能であること。
7. IPv4 および IPv6 通信に上位層のプロトコルに関係なく対応できること。
8. 拠点間の通信について上位層のプロトコルに関係なくも対応できるとよい。(非必須)
9. インバウンドおよびアウトバウンド通信について、TCP/UDP ポート通信にセキュリティポリシーを適用でき、通信可否(許可/遮断)などの制御が可能であるとよい。(非必須)
10. 攻撃を検知した場合、正規のトラフィックに影響を及ぼすことなく攻撃パケットやセッションを遮断できること。
11. 攻撃を検知した場合アラートを生成し、管理者に対してメール通知 syslog にログの転送が可能であること。
12. 攻撃後の侵入者と被害者間のトラフィックを記録可能であること。
13. 発生した脅威や通信を視覚的に表示し、GUI 上の簡易な操作で情報をフィルタして抽出できる機能を有すること。
14. IP アドレスごとに詳細なポリシーが定義できること。
15. Microsoft365 など SaaS 側で頻繁に変更される IP アドレスを動的に外部から取り込みホワイトリスト制御やポリシーベースルーティングができること。
16. 使用されているアプリケーションプロトコルを識別し、通信制御する機能を有すること。
17. 既知のコンピュータウイルス、ワーム、トロイの木馬等を含むファイルの検査を行い、検知および遮断できること。
18. HTTP、HTTPS, FTP、SMTP、POP3、IMAP4 に対応すること。　IP 電話(Zoom プロトコルを調べて追記)
19. パターンファイルのアップデートは、通信の停止を伴わず自動で実施されること。
20. ファイル転送の検査の対象となるファイルサイズは 1GB 以上に対応できること。
21. ファイル転送の検査の対象となるファイルサイズは、無制限であるとよい。(非必須)
22. ウイルス検出時の動作として、対応プロトコル（HTTP、HTTPS など）ごとに、ログに記録した上で許可・遮断のいずれかを管理画面により任意に設定可能であること。
23. インターネット上の C&C サーバとの通信など、スパイウェアによる通信の検査を行い、検知および遮断できること。
24. スパイウェア検出時の動作として、検出レベル（重大度）に応じて、許可、ログに記録した上で許可、遮断のいずれかを管理画面により任意に設定可能であること。
25. ソフトウェアや OS のセキュリティホールを利用して実行される不正アクセスやウイルス感染などの攻撃を検知および遮断できること。
26. 脆弱性防御の動作として、検出レベル（重大度）に応じて、許可、ログに記録した上で許可、遮断のいずれかを管理画面により任意に設定可能であること。
27. 特定の Web サイトへのアクセスを制限できること。
28. Web サイトへのアクセス制限は、既定の URL カテゴリおよびユーザ定義 URL カテゴリの両方で対応できること。
29. 既定の URL カテゴリは、60 種類以上に分類でき、自動的にアップロードを行うことで、最新の URL 情報に基づくフィルタリング機能を提供すること。ユーザ定義 URL カテゴリは、150 個以上作成可能であること。
30. URL カテゴリ単位で任意に許可、遮断の制御ができること。
31. Web サイトへのアクセスをブロックした場合、クライアントに任意の画面および文章を表示できること。
32. ホワイトリスト登録することで、任意の Web サイトへの通信のみを許可できること。
33. Web サイトのコンテンツ内容を機械学習などによって検査し、有害サイトへのアクセスをリアルタイムに遮断することが可能であるとよい。(非必須)
34. 規定で対応できる Saas アプリケーションの種類が 6000 以上であるとよい(非必須)
35. Google や Microsoft365 等の SaaS アプリケーションに対して、指定した組織アカウント以外の使用を制限できること。
36. オンラインストレージへのファイルのアップロードやダウンロードの可否を制御できること。

37. オンラインストレージへのファイルのアップロードやダウンロードを許可した場合、その動作がログに記録されること。
38. 制御対象のアプリケーション、ファイル種別、通信方向、許可遮断設定を任意に設定できること。
39. LAN 内の通信についても、マルウェアや標的型攻撃の解析ができること。
40. 実行可能ファイルやスクリプトファイルを検査し、有害ファイルをリアルタイムに遮断することが可能であること。
41. 検出された新しいマルウェアに対するシグネチャは、自動的に更新ができるとよい。(非必須)
42. 脅威が確認された場合に、感染の疑いのある実行ファイルなどの通信を自動で遮断か隔離する機能を有するとよい。端末についても通信を遮断か隔離する機能があるとよい。(非必須)
43. HTTPS 通信（暗号化通信）を復号することで、アプリケーション制御機能、アンチウイルス機能、アンチスパイウェア機能、脆弱性防御機能、Web フィルタリング機能、ファイルブロッキング機能、サンドボックス分析機能の対応を可能とすること。
44. クライアント PC への証明書インストール作業および更新管理は、本委託に含めること。
45. 各拠点は、インターネット回線を利用した接続が可能であり、通信経路は暗号化されること
46. 通信暗号化方式は、共通鍵方式か証明書方式から選択可能であるとよい。(非必須)
47. 将来的にトラフィックが増加した際に対応できるよう、帯域の増強に柔軟に対応できること。増強時に費用が発生する場合、都産技研と協議すること。
48. 端末のエージェントは接続ネットワークを自動識別し、外部ネットワークに接続された場合は自動的に最寄りの接続ポイントへ接続する機能を有すること。
49. インターネットへの通信だけでなく、リモートユーザの通信、拠点および拠点間通信においてもセキュリティポリシーが適用できること。
50. 次のログを収集保存し、確認できること。
    (ア)トラフィックログ
    (イ)脅威ログ（アンチウイルスアンチスパイウェア脆弱性防御）
    (ウ)Web フィルタリングログ
    (エ)サンドボックス分析ログ
51. ログの確認出力等について、単一の管理 GUI で実施できること。
52. 各機能で検知されたイベントログの保管場所について、オンプレミス環境に用意する必要がないこと。ログは SIEM（SecurityInformationandEventManagement）などとの連携のために、必要に応じて外部へ転送できること。
53. 指定の Syslog サーバに次の脅威ログを転送できること。
    (ア)アンチウイルス
    (イ)アンチスパイウェア
    (ウ)脆弱性防御
    (エ)サンドボックス分析
    (オ)Web フィルタリング

11. 管理業務に関わる要求

管理業務は、作業の実施体制を構築して、作業実施計画書の作成，進捗管理、品質管理、課題管理等を実施し、包括的な管理を行うこと。

11.1. 作業の実施体制

新システムの構築期間中は、全体を統括する統括責任者(プロジェクトマネージャおよび実施責任者（プロジェクトリーダ)、作業要員を配置すること。

11.1.1.構築期間中の実施責任者（プロジェクトリーダ、マネージャ）は、以下の条件を満たすこと。

1. 本業務の遂行上で問題が発生した場合には、速やかに都産技研に報告し、解決できる者であること。
2. 情報処理業務（システムの構築、運用・保守等）の経験年数を 10 年以上有すること。

3. ネットワーク構築案件において、5 名以上からなるプロジェクトの実施責任者（プロジェクトマネージャ）としての実績を有すること。
4. 中央省庁、独立行政法人、地方公共団体等の公共機関におけるシステム構築に関するプロジェクト管理実績を有すること。
5. 情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうちプロジェクトマネージャ試験の合格者、技術士（情報工学部門又は総合技術監理部門（情報工学を選択科目とする者））又は PMI が認定する PMP（Project Management Professional）のいずれかの資格を有しているとよい。(非必須)

11.1.2. 構築期間中の作業体制は、以下の条件を満たすこと。なお、複数名で以下の条件を満たすことでもよい。

1. 情報処理業務（システムの構築、運用・保守等）の経験年数を５年以上ある人員を充てること。
2. ネットワーク構築に関して中央省庁、独立行政法人、地方公共団体等の公共機関におけるシステム構築に関するプロジェクト実績がある人員を充てること。
3. 情報処理安全確保支援士、情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうち情報セキュリティスペシャリスト試験またはネットワークスペシャリスト試験の合格者、CISSP（Certified Information SystemsSecurity Professional）の資格を持っている人員を有しているとよい。(非必須)

11.2. 作業場所

本業務の作業場所および作業に当たり必要となる設備、備品及びおよび品等については、受注者において用意すること。ただし、定期的な会議場所については、都産技研が用意する。また、撤去した装置などの一時置き場も都産技研で用意する。

11.3. 管理に関する要領

1. 本業務の受注者は、本業務の実施に先立ち、コミュニケーション管理、進捗管理、品質管理、リスク管理、課題管理、変更管理、セキュリティ管理等の管理要領を定めたプロジェクト管理要領を作成し、当該要領に基づき、本業務に係るプロジェクト管理を適切に行うこと。
2. 本業務に係るプロジェクト管理は、体系化されたプロジェクト管理基準を定め行うこと。PMBOK（Project Management Body of Knowledge）等を踏まえていると良い。
3. 本業務の目的、受注する業務の範囲についての理解を明示すること。
4. 明示した目的および業務範囲は、プロジェクトの進行に従い変更を要する可能性が生じた場合は、都産技研と協議を行い、両者で合意した対応を取ること。

11.4. 進捗管理

1. 定量的かつ客観的な進捗管理を行うこと。
2. 設計・開発実施計画書作成時点においては、全工程の作業が把握可能なレベルまで掘り下げて、概略の WBS（Work Breakdown Structure）を作成し、別添として明示すること。
3. 各工程開始前までに、当該局面の各作業項目（WBS 項目）を 5 人日程度（最長でも 10 人日程度）の単位まで詳細化すること。詳細化に際しては、WBS の管理のし易さや都産技研への説明のし易さ等を鑑み、作業の粒度、プロジェクトの進捗段階、作業分野に合わせて適宜必要部分を別資料として詳細化する等、工夫すること。
4. WBS 上の各タスクについて、開始基準、完了基準および進捗を定量的に測定する方法を定義すること。
5. WBS 上の各タスクについて、作業実施体制に示すリーダーと担当者を明記すること。また、同一担当者が別のタスクで過度にスケジュールの重複が発生しないよう、作業工数として妥当かつ適切に管理された WBS とすること。
6. WBS の各タスクと成果物との関係を明確にするため、各タスクと各種成果物との紐付けを WBS に明示すること。

7. 進捗状況は、原則月に 1 回以上は都産技研に報告すること。進捗報告の際は、WBS とともに、進捗状況の概略を整理した進捗報告書を提示すること。また、WBS による報告時は、WBS 上で先行タスクおよび後続タスクを明確にした上で、クリティカルパスが明確になるように報告し、リスク管理の対象として管理すること。
8. 各工程の完了報告時において、受注者内で報告書等の確認を行い、次工程へ進むことに関して、都産技研に承認を求めること。
9. スケジュール変更が必要となった場合は、変更内容、変更理由、変更に伴う影響を報告し、都産技研に承認を得ること。

11.5. 会議体

1. 表 11 に示す会議体を主催すること。また、設計・開発実施計画書にて会議体の名称、目的、開催日時又は開催頻度、参加者および開催場所等の詳細を都産技研に提案し、両者で合意した会議体を運営すること。
2. 会議のアジェンダは、原則として1営業日前までに関係者に示すこと。
3. 資料の確認に時間を要するものについては、会議開催日前に資料を事前送付し、事前に資料を確認する時間を確保すること。
4. 都産技研や関係者が主催する会議体について、必要に応じて会議体に出席し、必要な資料作成、情報提供等の支援を行うこと。
5. 表 11 に示す会議体とは別に、都産技研と協議・検討が必要な事項がある場合は、適宜都産技研に会議を提案し、調整を図ること。
6. 通常の会議の実施場所は、原則として都産技研本部とする。

表 11　　会議体一覧

No.	会議体	概要	主催者	開催頻度
1	キックオフ会議	本業務受注者が、都産技研に、本業務に係る設計・開発実施計画書の内容を報告する。	本業務の受注者	開始時
2	定例進捗会議	本業務の受注者が、都産技研に設計・開発の進捗状況、課題管理、リスク管理、品質管理等のプロジェクト管理全般の対応状況を報告する。	本業務の受注者	原則隔週
3	検討会議	本業務の受注者が、都産技研に設計内容や各種計画書、仕様等の内容の確認を行う。	本業務の受注者	必要に応じて随時
4	各工程の完了報告会議	本業務の受注者が、都産技研に各工程の実施結果を報告し、各工程の完了基準を満たしていることの確認を行う。ただし、仕様の確定については、当会議とは別途実施することを想定している。	本業務の受注者	各工程の完了時

11.6. 議事録

1. 本業務の各種会議の決定事項および残課題や質疑応答等を記した議事録を作成すること。
2. 議事録は、原則として会議開催後 5 営業日以内に関係者に提出し、都産技研の承認を受けること。

11.7. コミュニケーション管理

1. 都産技研との連絡窓口を定め、連絡先を明記すること。

2. 工程別に複数の連絡窓口担当者を設置する場合も同様に明記すること。ただし、コミュニケーション経路の複雑化とミスコミュニケーションを防ぐため、連絡窓口担当者は必要最低限に抑えること。
3. 本業務受注後、本業務に係る関係者とコミュニケーションを取る必要がある場合は、その旨を都産技研に申し出た上で、連絡方法、連絡窓口等について協議すること。
4. 本業務において、都産技研を含めずに関係者と会議を実施する場合は、その議題等について事前に都産技研に通知し、参加の有無を確認すること。
5. 本業務の契約期間中において、本業務における成果物（中間成果物を含む）、会議資料等を相互に共有するための情報管理ツールを提供すること。なお、当該ツールは、インターネット経由での利用を想定しているが、不正アクセスや脆弱性対策等のセキュリティ対策がなされ、都産技研の情報セキュリティポリシーを遵守するものであること。また、都産技研の利用者数に関わらず、当該ツールの必要なライセンス等は本業務に含めること。
6. コミュニケーション管理を円滑に進める方法を設計・開発実施計画書にて提案し、都産技研の承認を受けること。

11.8. 品質管理

1. 各工程の特性に応じた品質管理指標、品質目標を設定し、定量的かつ客観的な品質管理を行うこと。また、各工程完了時には、設定した品質管理指標、品質目標との差異を分析するとともに、品質評価結果を報告すること。
2. 全ての成果物に対して、目的の品質が確保できているかを確認するため、受注者内部で複数回レビューを実施する等の措置を取ること。
3. 設計書等の成果物について、スケジュールに対応し、都産技研内でのレビュー期間(1 週間以上)を設けること。
4. 都産技研が指摘した内容について、レビュー記録管理表で記録し、対応状況および対応結果も含めて適切に管理すること。
5. レビューの評価尺度は本業務の受注者の社内規定がある場合はその規定を都産技研に開示した上で使用すること。
6. 上記以外に都産技研が、本業務の適正な実施のため必要があると判断する場合は、都産技研の要請に応じて成果物の品質について報告すること。また、都産技研が、成果物の品質について問題があると判断する場合は、是正要求に応じること。

11.9. 変更管理

1. 本業務の実施計画に対して、重要なマイルストーン、工数の増減、要件の変更に伴う著しい変更が生じた際の変更管理を行うこと。
2. 変更管理は、変更対象、影響範囲に応じて分類し、変更の状況について定期的に都産技研に報告すること。
3. 著しい変更は、変更管理表により起票し、変更の状況、実施有無、変更内容等について証跡を残すこと。
4. 設計・開発実施計画書において、変更管理の実施手順および様式を定めること。

11.10. 課題管理

1. 本業務で発生した課題事項を一覧化し、課題管理を行うこと。また、各課題は原因となったWBS と関連付けて管理すること。
2. 各課題は、課題区分、影響範囲、対応優先度に応じて分類し、各課題の対応状況について定期的に都産技研に報告すること。
3. 課題対応状況の報告は、対応の推移がわかるように行うこと。
4. 設計・開発実施計画書において、課題管理の実施手順および様式を定めること。

11.11.　リスク管理

1. 本業務の実施計画の阻害要因となり得る事項をリスクとして識別し、各リスクが顕在化した場合の影響を評価し、各リスクが顕在化しないようにすること。顕在化した場合には、影響を最小限に留めることができるよう対応策を整理し、追跡管理すること。
2. リスクとして識別した事項を一覧化し、リスクレベル、リスク区分、影響範囲に応じて分類し、各リスクの対応状況について、リスク要因と推定される WBS と対応付けて定期的に都産技研に報告すること。
3. 特に作業スケジュールに対して遅延が発生するリスクは、あらかじめ影響と対応策を検討し、工程ごとに評価内容を見直し、都産技研に報告すること。
4. リスクが顕在化した場合は課題管理対象とし、当該リスクのリスク管理を完了させること。
5. リスク対応状況の報告は、対応の推移がわかるように行うこと。
6. 設計・開発実施計画書において、リスク管理の実施手順および様式を定めること。

11.12.　Q&A 管理

1. 本業務に係る関係者間で発生した質問に対する回答管理を行うこと。
2. Q&A は、起票者、Q&A 先、対象区分、対応優先度、影響範囲に応じて分類し、Q&A の対応状況について定期的に都産技研に報告すること。
3. 設計・開発実施計画書において、Q&A 管理の実施手順、様式を定めること。

11.13.　文書管理

1. 受注者が文書標準を作成し、当該標準に従って成果物を作成すること。
2. 文書管理の対象は、各種計画書、仕様書、設計書、報告書、議事録、管理表など各工程およびプロジェクト管理において作成する成果物とすること。
3. 設計・開発実施計画書にバージョン管理方法を定めること。

12. 設計業務に関わる要求

設計業務は、現行システムで稼働しているネットワーク設定および通信要件、都産技研の要件を確認したうえで、適切なネットワークサービスや機器を選定し、設計すること。

12.1. 設計業務に求める基本要件

都産技研ネットワークの安定した稼働および業務の継続に影響を与えることがないよう、安全で確実な構築・導入計画を策定すること。円滑かつ迅速に導入され、かつ運用されるよう設計すること。

12.2. 設計・構築計画書等の作成

1. 業務に係る作業内容、作業体制、スケジュール（WBS を含む）、成果物等を定めた設計・構築計画書を作成し、都産技研の承認を受けること。
2. 本業務の契約期間中に、設計・構築計画書の修正又は見直しが必要となる場合は、速やかに都産技研に修正案を提示し、承認を受けること。なお、少なくとも後述する要件定義（補完工程）が完了し、基本設計工程を開始する前に、設計・構築計画書の内容を具体化、詳細化し、修正した内容について都産技研の承認を受けること。

12.3. 要件定義

1. 本書および別紙等から現行ネットワーク及びおよび業務を理解するよう努め、都産技研と現状の課題や背景等を確認した上で、要件の見直し及び詳細および含めた新ネットワークの要件定義を行うこと。
2. 本書および別紙等で都産技研から示した要件以外に、本業務の受注者が提案時に追加提案した要件、ソフトウェアやクラウドサービスなど標準で提供される機能やサービス等がある場合は、その採否を都産技研と協議の上、決定すること。
3. 要件定義書を作成し、都産技研の承認をうけること。

12.4. 設計

1. 都産技研が承認した要件定義書を満たすための基本設計および詳細設計を行い、成果物について都産技研の承認を受けること。なお基本設計で必要と考えている事項は以下を想定しているが、必要に応じて都産技研と協議すること。
   (ア) IP アドレス設計
   (イ) ルーティング設計
   (ウ) 物理構成設計
   (エ) 論理構成設計
   (オ) 情報セキュリティ設計
   (カ) 暗号化設計
   (キ) 帯域予約設計
2. 詳細設計は、基本設計をもとに各種機器等の設定内容の方針や理由を記述すること。詳細設計で必要と考えている事項は以下を想定しているが、必要に応じて都産技研と協議すること。
   (ア)ネットワーク機器の物理・論理設計(VLAN 構成等)
   (イ)セキュリティ機器の物理・論理構成(暗号化、認証等)
   (ウ)運用システム機器の物理・論理構成(ネットワーク管理システム等)
3. 現行ネットワークから新ネットワークへの移行の方法、対象範囲、環境、ツール等を記載した移行計画・設計書を作成し、都産技研の承認を受けること。
4. テスト工程における実施内容、開始条件・終了条件、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全体テスト計画書を作成し、都産技研の承認を受けること。
5. 新ネットワーク移行後に計画的に発生する運用・継続利用サービスの作業内容、その想定される時期等を取りまとめた運用設計および継続利用サービス設計を行い、監視対象や閾値等の設計等を取りまとめた設計書を作成し、都産技研の承認を受けること。
6. 定常的な作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた運用・保守手順書を作成し、都産技研の承認を受けること。
7. 教育・訓練におけるスケジュール、実施方法、実施体制等を定めた教育・訓練実施計画書を作成し、都産技研の承認を受けること

13. 構築業務に関わる要求

構築業務は、現行環境への影響を可能な限り抑制する計画を立案すること。また、設計に従い機器やソフトウェアを準備し、設定・試験・設置して、現行環境から移行をすること

13.1. 構築業務にかかわる基本要件

1. 設計工程の各種設計書、計画書等に基づき構築・テスト・移行を行うこと。
2. 2025 年 2 月末までに移行テストが完了し、2025 年 4 月 1 日までには新ネットワークによる運用が開始されること。
3. 基幹機器の設置個所は、本部はサーバ室、支所はラック内を予定している。必要な場合は、都産技研と協議すること。
4. 全体テスト計画書に基づき、各テスト工程の実施計画書、仕様書を作成し、都産技研の承認を受けること。
5. 各テスト工程の実施計画書に基づき、各テストの実施状況を都産技研に報告すること。
6. 各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、都産技研の承認を受けること。
7. 無線 LAN の構築は、受注後に現地調査などを行い、都産技研と協議して決めること。
8. 搬入および工事を行う場合は、その一週間前までに詳細な施行および作業内容、範囲、作業者名、スケジュールおよび使用車両を都産技研に連絡すること。
9. 現行ネットワークの運用に支障がないようにすること。

13.2. 作業に関する要件

1. 本委託において、光ケーブル、LAN ケーブル、情報コンセント、収納ボックス、電源コンセントなどは既設の設備を極力流用することとし、不足するもの、仕様・性能を満たさず変更が必要なものは増設を行うこと。費用は受注者が一定額を見込んで本委託に含めること。
2. 各種作業は、東京都電気設備工事標準仕様書に基づくこと。
3. 新たにケーブル敷設などが必要な場合は、本調達に含めること。
4. 都産技研ネットワークのサービス停止が避けられない場合は、一般利用者への影響を最小限に抑えるため、平日 9:00 から 18:00 以外、土日および休日を作業実施日として検討し、都産技研の承諾を得ること。
5. 導入時に機器等の追加が必要な場合は、受注者の負担において準備し、作業終了後に撤去すること。
6. 施工において、受注者の責に帰する事由による造営物および道路の損傷、土地踏み荒らし等、都産技研及びおよび関係者に与えた損害に対する費用等は、全て受注者の負担すること。
7. 都産技研の指示する場所に搬入・設置を行い、梱（こん）包箱・残ケーブル等当該機器の利用に不要なものは撤去すること。なお、運用開始日以前に当該機器の設置場所の変更が生じた場合は、都産技研の指示に従って移設等すること。除去および移設の費用は受託者の負担とする。
8. 建物の工事を行う場合は、作業前に法令に準拠して調査を行うこと。

13.3. 受入テスト支援

1. 受入テスト実施計画書案を作成し、都産技研の承認を受けること。
2. 都産技研が行う受入テストの具体的な手順および結果を記入するための受入テスト案を作成し、都産技研の承認を受けること。
3. 都産技研が行う受入テスト計画に基づき、必要な環境整備（テストデータの準備を含む）や運用等の支援を行うこと。

13.4. 移行

1. 移行計画・設計書にもとづいて、移行作業を行うこと。
2. 現行ネットワーク機器の構成変更等を伴う移行となる場合は、設計時に現行ネットワーク機器の設定情報等を調査し、変更内容について都産技研へ提示すること
3. 現行ネットワークサービス提供の停止を最小限にとどめ、効率的かつ確実な移行方式であること。
4. 移行に際して役職員への作業が発生する場合は、役職員の行う作業についてまとめてマニュアルを作成すること。
5. 移行に際して現行の機器からデータを取る場合は、都産技研職員の立会いのもと作業をすること。
6. 本番移行前に移行リハーサルを複数回行い、リハーサルの結果について、都産技研の確認を受けること。
7. 本番移行を行い、移行実施結果を整理した移行結果報告書を作成し、都産技研の承認を受けること。

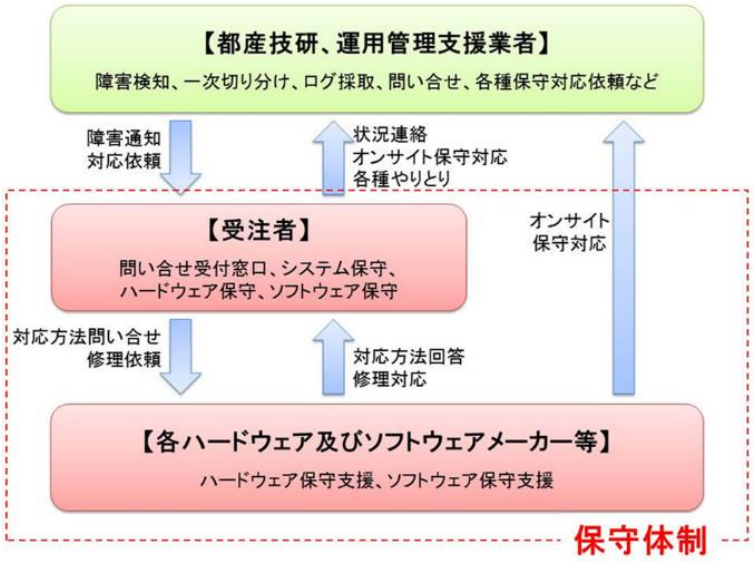
14. 保守に関わる要求

保守に関する業務は、本委託で構築したネットワーク、システム・機器・ソフトウェアなどを安定稼働するために確実なサービス提供体制の構築およびマニュアルを整備すること。サービス提供体制は遅延なく対応ができる体制を構築すること。設計・開発の設計書、作業経緯、残存課題等を文書化し、別途調達する運用支援業務の受注者に対して確実な引継ぎをすること。

14.1. 保守の基本要件

1. 受注者は、下図に示す条件を満たすサービス提供体制を用意すること。なお、サービス提供と

は、システム不具合対応、ハードウェア不具合対応、ソフトウェア不具合対応の総称を示す。



サービス提供体制図

2. 本委託内で納品されたすべてのハードウェアおよびソフトウェア・システムを対象とすること。
3. 本委託で構築したシステムおよびハードウェアおよびソフトウェアの保守期間は、2025 年 4 月 1 日から 2030 年 3 月 31 日までを想定しているため、期間内にサポートが終了しないこと。2025 年 4 月 1 日から 2026 年 3 月 31 日の期間は、契約不適合責任(メーカ保証)で 14.2 から 14.4 に対応すること。
4. 2026 年 4 月 1 日から 2030 年 3 月 31 日の保守は、別契約として単年度ごとに契約を結ぶ。
5. 各種ライセンスは、上記と同じ契約内で単年度ごとに契約を結ぶ。
6. 2026 年 4 月 1 日から 2030 年 3 月 31 日までの 1 年間ごとの保守費を参考に提出すること。保守費を算出する際は、現在の為替相場で算出してかまわない。
7. 2026 年 4 月 1 日からの保守は、統括責任者およびリーダーをそれぞれ 1 名選任すること。
8. 2026 年 4 月 1 日からの保守は、責任体制を明確にするため、作業統括責任者、リーダー、および各担当者名を明記したサービス提供体制図を提出すること。なお、体制を変更する必要が生じた場合には、変更内容を記載した書面をもって報告し、都産技研の承諾を得ること。
9. 機器などの障害発生時は、都産技研と綿密な調整・連携をして受注者の責任と負担で作業を行うこと。

以下は 14.1 の 10 から 18 は、2026 年 4 月 1 日以降の保守についての対応とする。

10. 都産技研でも管理するが、受注者側でも必要となる情報を適切に管理し、常に最新状態を維持しつつ、構成情報の履歴管理（変更箇所、変更日時等）を行うこと。
11. ハードウェアベンダ、ソフトウェアベンダからの計画保守要求やモジュールアップデート要求に対し、重要度を十分加味し、必要最低限のものに限定したうえで、対象となる機器全てについて情報を提供すること。モジュールアップデートは、都産技研で実施する。
12. 対応に係る調査の結果、構成情報を変更しようとする時は、必ず都産技研の承諾を得ることとし、都産技研の許可無く構成情報の変更を行わないこと。
13. 対応を行った際に、構成情報に変更があった場合、変更した構成情報の詳細が分かる資料を作成し、変更があった日から 1 週間以内に電子データとドキュメントを都産技研に提出すること。
14. 期間内において、前項で作成した資料を適切に管理し、都産技研から再提出を求められた場合、速やかに対応すること。
15. サービス拠点を東京 23 区内に有し、対応可能な人員体制が十分に確保されていること。また、都産技研より問い合せがあった際は、翌日までに対応が開始できること。なお対応に時間が要する案件は都産技研と相談して、日程を調整して対応すること。
16. 対応期間は概ね 1 か月程度とし、進捗がない場合は、理由を調査し、理由書を都産技研に提出すること。

17. インシデントの管理をして、完了まで対応を継続すること。
18. 対応は日本語で実施すること。

14.2. **システム対応**

1. 受注者は、ハードウェアおよびソフトウェアの各製造元が単独で解決できない事象発生を想定し、システム全体を理解しており、各製造元と協力して実施すること。
2. 発生した障害の解析・原因究明をし、再発防止策を施すこと。

14.3. **ハードウェア対応**

1. ハードウェア障害時は、受注者の負担により、当該機器または構成部品等の調達・交換・修理等を迅速に行い、正常稼働を保証すること。

14.4. **ソフトウェア対応**

1. 受注者は、ソフトウェアに関する問い合せ、セキュリティ情報等の提供、障害発生時における解決支援に対応すること。

15. **機密保持**

1. 受注者は、履行期間中はもとより履行期間終了後にあっても、本業務委託を履行するうえで知り得た都産技研に係る情報を原則第三者に開示または漏えいしてはならない。
2. 本業務委託の従事者に、知り得た秘密を他人に漏らさないことを誓約した書類を作成させ、都産技研へ提出すること。
3. 本業務委託の実施に必要な関係資料を本業務委託以外に使用しないこと。また、無断で第三者に提供しないこと。
4. 関係資料を無断で持ち出し・複写・複製をしないこと。
5. 本業務委託の実施または管理に関して関係資料に事故が発生した場合は、直ちに報告すること。
6. 本業務委託の従事者に対し、本業務委託に関して知り得た個人情報の内容をみだりに他人に知らせ、または不当な目的に利用してはならないこと、個人情報の違法な利用および提供に対して罰則が適用されること、その他個人情報の保護に関して必要な事項を周知させ、個人情報の保護が徹底されるように指導すること。

16. **情報セキュリティの確保**

1. 受注者は、都産技研が保有する情報セキュリティポリシー等（以下、「ポリシー等」という。）を遵守しなければならない。また、都産技研の保有するポリシー等については、「機密保持」に基づき、その内容を秘密にする措置をとらなければならない。受注者は、セキュリティを確保するために以下の措置を講ずることとし、発生する費用は本件に含まれるものとする。
2. 本件に係る業務の実施のために都産技研から提供する情報、およびその他当該業務の実施において知り得た情報については、情報のライフサイクルの観点から管理方法を定め、その秘密を保持し、また当該業務の目的以外に利用しないこと。
3. 受注者は、都産技研からの求めがあった場合に、受注者の資本関係・役員等の情報、受注作業の実施場所に関する情報、受注業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績および国籍に関する情報を提供すること。
4. 本件に係る業務の遂行において、情報セキュリティ対策の履行状況を本件に係る業務の開始時および変更がある度に報告するとともに情報セキュリティが侵害されまたはその恐れがある場合には、直ちに都産技研に報告すること。これに該当する場合には、以下の事象を含む。
5. 受注者に提供または受注者によるアクセスを認める都産技研の情報の外部への漏えいおよび目的外利用等。
6. 受注者による都産技研のその他の情報へのアクセス。また、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、都産技研の求めに応じて成果物と共に都産技研に引き

渡すこと。
7. 受注者の講ずる情報セキュリティ対策が都産技研の所有するポリシー等の基準を満たしていない場合には、受注者は、都産技研と協議のうえで追加的なセキュリティ対策を講ずること。
8. 本件に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、都産技研が情報セキュリティ監査の実施を必要と判断した場合は、都産技研がその実施内容（監査内容、対象範囲、実施等）を定めて、情報セキュリティ監査を行うことを妨げないこと。（都産技研が選定した事業者による監査を含む）
9. 受注者は受注者が受けた外部監査結果についても都産技研へ報告すること。
10. 情報セキュリティ監査の実施については、これらに記載した内容を上回る措置を講ずることを妨げるものではない。

17. **再委託**

1. 受注者は受注業務の全部を第三者に再委託することはできない。受注業務の一部を再委託する場合は、事前に再委託する業務、再委託先等を都産技研に報告し、承認を受けること。
2. 受注者は機密保持等に関して、本仕様書が定める受注者の責務を再委託先業者にも負うよう必要な措置を実施し、都産技研に報告し、承認を受けること。
3. 受注者は、受注業務の全部を一括して第三者に再委託してはならない。
4. 受注者は、受注業務における総合的な企画および判断並びに業務遂行管理部分を再委託してはならない。
5. 受注者は、本件に関する調達参加制限に該当する事業者に再委託してはならない。
6. 受注者は、受注業務の再委託を希望する場合は、あらかじめ都産技研の指示に従い、再委託の相手方の商号又は名称および住所並びに再委託を行う業務の範囲、再委託の必要性を記載した申請書を都産技研に提出し承認を得なければならない。承認した内容に変更が発生する場合も同様とする。
7. 受注者は、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および住所並びに委託を行う業務の範囲を記載した「履行体制図」を都産技研に届け出なければならない。届け出た内容に変更が発生する場合も同様とする。
8. 受注者は、再委託の相手方の履行体制および履行状況を適宜、把握し、都産技研職員からこの報告を求められた時は応じなければならない。
9. 受注者が都産技研の承認を得て第三者に業務委託しても、最終的な責任は受注者が負わなければならない。
10. 本件において、再委託とは、本来、受注者自ら行うべき業務の一部を効率性、合理性等の観点から例外的に外部発注するものであり、契約目的を達成するために遂行する一連の業務に付帯して印刷、通訳、翻訳等を外部の専門業者に発注することは再委託に該当しない

18. **その他**

1. 本契約の受注者は、ISO9001:2008 又は ISO9001:2015 の認証を受けているか、または、組織としての能力成熟度について CMMI レベル 3 以上と評価されていること。なお、取得している事業所、部門は問わない。
2. 本契約の受注者は、JIS Q 27001（ISO/IEC27001）認証を取得しており、情報セキュリティ管理を的確に行う体制が整備されていること。
3. ネットワーク構築やセキュリティ設計委託等について、営業年数が 3 年以上あること。
4. 直近の過去 3 ヵ年の平均売上高実績が 1 億円以上であること。
5. 過去 5 年以内に官公庁、独立行政法人、地方公共団体等の公共機関のネットワーク構築受託実績が 3 件以上あること。または、同等以上と認められる実績があること。
6. 本契約を履行する受注者は、契約書、本仕様書等に定める事項のほか、都産技研の定める別紙「電子情報処理委託にかかる標準特記仕様書」に従って契約を履行しなければならない。また、都産技研の保有する個人情報の取扱については、別紙「個人情報に関する特記事項」を遵守すること。
7. 本契約の実施にあたり故意又は過失により都や第三者に損害を与えた場合、その損害が都産技研の責任に帰する場合を除き、賠償等の責任は受注者が負うこととする。

8. 地方独立行政法人東京都立産業技術研究センター（以下、「都産技研」という。）で作業する場合は、受注者の負担と責任により、作業場所までの経路および作業場所周辺に必要な養生を行うこと。作業に伴い施設に損害を発生させた場合、受注者の責において原状回復を行うこと。
9. 本仕様書に定めのない事項および不明な点は担当職員との協議によること。
10. その他本仕様書に定めなき点、または疑義が生じた場合は、都産技研の担当職員と協議の上決定すること。
11. 委託業務の実施に当たり発生した特許権、著作権、実用新案権、意匠権、商標権、その他一切の無体財産等の成果物は、すべて都産技研に帰属し、契約期間後も必要な場合は、都産技研が自由に使用できるものとする。納品物となる画像データや版下データ等一切はすべて都産技研に帰属する。委託業務の実施にあたっては、著作権、成果物の保護に十分配慮すること。

ディーゼル車規制に適合する自動車による配送等

本契約の履行に当たって自動車を使用し、又は利用する場合は、次の事項を遵守すること。

（１） 都民の健康と安全を確保する環境に関する条例（平成 12 年東京都条例第 215 号）第 37 条のディーゼル車規制に適合する自動車であること。

（２） 自動車から排出される窒素酸化物および粒子状物質の特定地域における総量の削減等に関する特別措置法（平成 4 年法律第 70 号）の対策地域内で登録可能な自動車であること。

なお、当該自動車の自動車検査証（車検証）、粒子状物質減少装置証明書等の提示又は写の提出を求められた場合には、速やかに提示し、又は提出すること。

注意事項

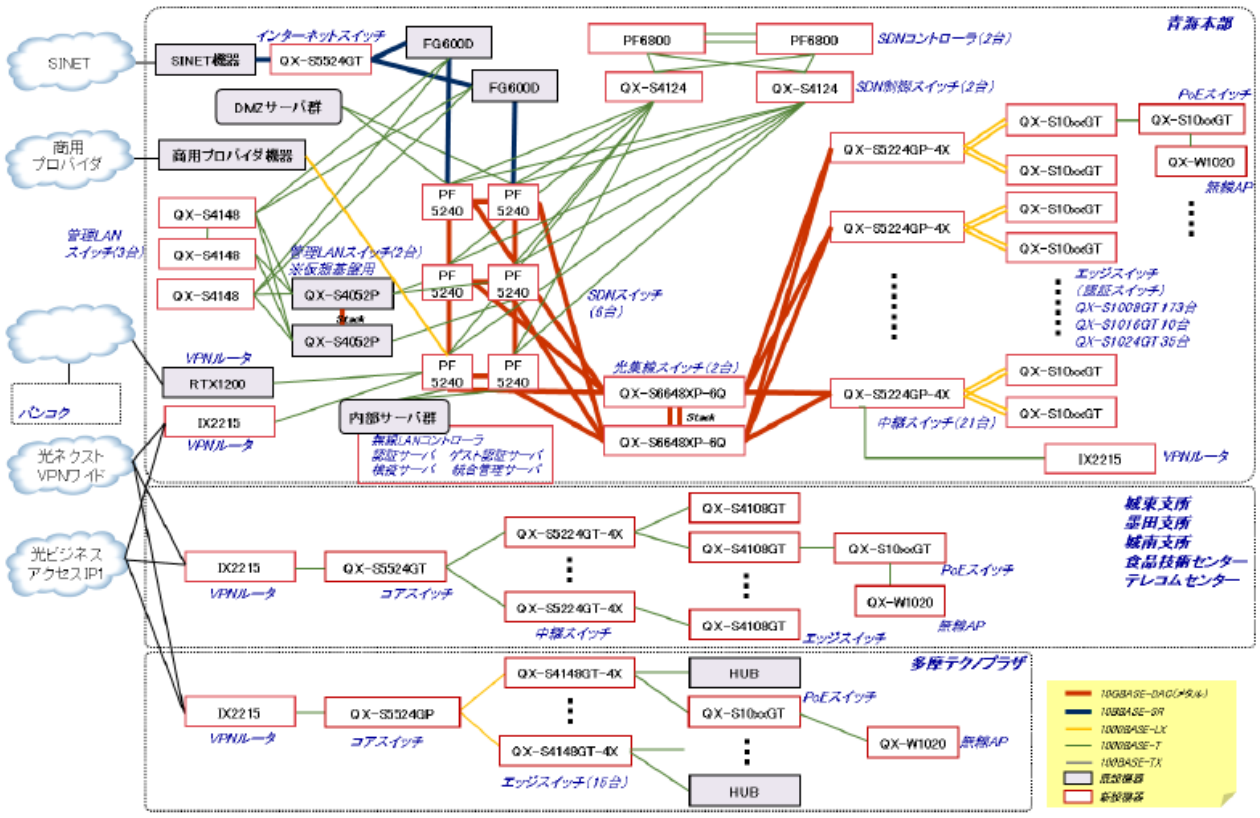
都産技研は、東京都により設置された試験研究機関であり、東京都内の中小企業に対する技術支援により、東京の産業振興を図り、都民生活の向上に貢献することを役割としています。　このため、購入した機器について、技術支援の一環として、中小企業等へ有償又は無償にて直接機器を利用させる機器利用事業等に使用する場合があります。

問い合わせ先　　地方独立行政法人東京都立産業技術研究センター　財務会計課経理係
所在地　〒１３５－００６４　東京都江東区青海２－４－１０
電　話　０３－５５３０－２７９０／ＦＡＸ　０３－５５３０－２７６７

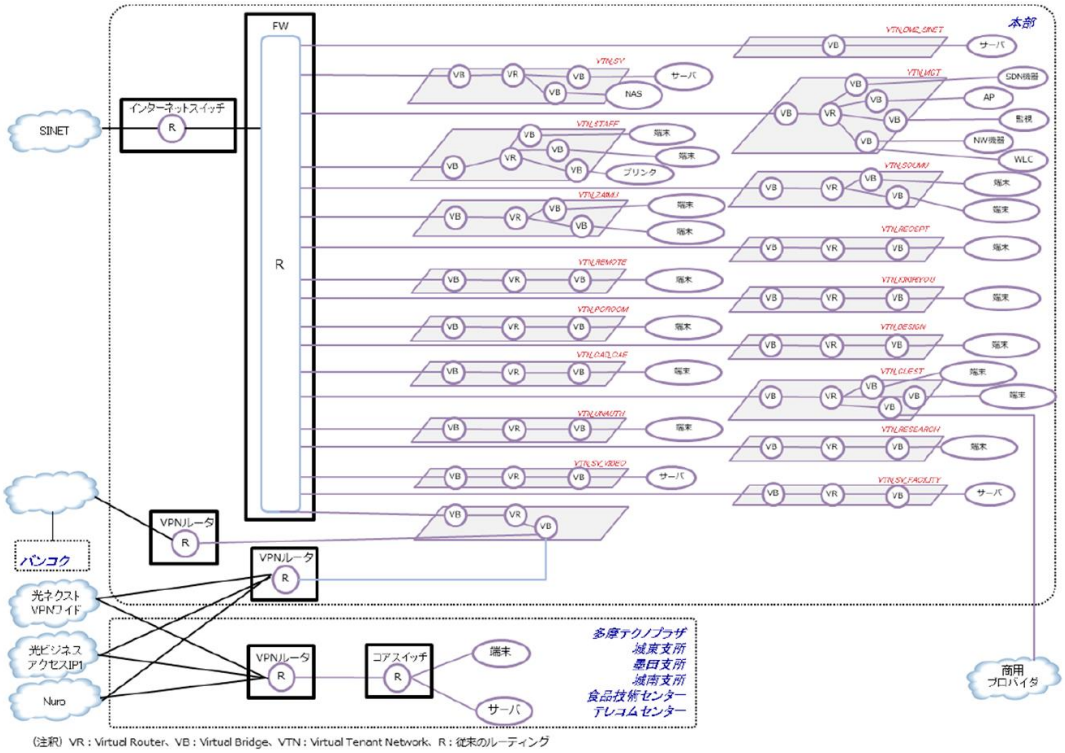
別紙 1 機器一覧

機種名	型番	本部	多摩テクノプラザ	墨田支所	城南支所	テレコムセンター	食品技術センター	合計
SDNコントローラ	UNIVERGE PF6800	2	—	—	—	—	—	2
SDNスイッチ	PF5240F-48T4 XW-A-N-S	6	—	—	—	—	—	6
SDN制御スイッチ	QX-S4124GT-4G	2	—	—	—	—	—	2
光集線スイッチ	QX-S6648XP-6Q	2	—	—	—	—	—	2
中継スイッチ①	QX-S5224GP-4X	21	—	—	—	—	—	21
中継スイッチ②	QX-S5224GT-4X	—	—	2	2	—	—	4
エッジスイッチ①	QX-S1008GT-2G	175	—	—	—	—	—	175
エッジスイッチ②	QX-S1016GT-4G	12	—	—	—	—	—	12
エッジスイッチ③	QX-S1024GT-4G	37	—	—	—	—	—	37
エッジスイッチ⑤	QX-S4108GT-2G	—	—	8	8	5	—	21
エッジスイッチ⑥	QX-S4124GT-4G	—	—	1	—	—	—	1
エッジスイッチ⑦	QX-S4116GT-4G	—	—	—	—	—	1	1
エッジスイッチ⑧	QX-S4148GT-2G	—	—	—	—	—	—	0
VPNルータ	UNIVERGE IX2215	2	—	1	1	1	1	6
インターネットスイッチ	QX-S5524GT-4X1C	1	—	1	1	—	—	3
コアスイッチ①	QX-S5524GP-4X1C	—	1	—	—	—	—	1
コアスイッチ②	QX-5628GT-4X2Q	—	—	—	—	1	1	2
管理LANスイッチ	QX-S4148GT-4G	3	15	—	—	—	—	18
管理LANコントローラ（WL	QX-W2230AC	2	—	—	—	—	—	2
無線アクセスポイント	QX-W1020	50	7	5	4	10	7	83
PoEスイッチ①	QX-S1008GT-2G-PW	12	1	—	2	3	—	18
PoEスイッチ②	QX-S1016GT-4G-PW	8	1	1	1	—	1	12
PoEスイッチ③	QX-S1024GT-4G-PW	4	—	—	—	—	—	4
認証サーバ	NetAttest EPS	1	1	—	—	—	—	2
証明書配布サーバ	NetAttest EPS-ap	2	—	—	—	—	—	2
ゲスト用認証サーバ	SecurePOPCHAT III	1	—	—	—	—	—	1
検疫サーバ	CounterAct（仮想）	1	—	—	—	—	—	1
統合管理サーバ	QX-MCソフトウェア（仮想）	1	—	—	—	—	—	1
UPS	無32停電電源装置（1500VA）	5	1	1	1	1	1	10

別紙２「ネットワーク構成図」と「論理図」



「ネットワーク構成図」



(注釈) VR：Virtual Router、VB：Virtual Bridge、VTN：Virtual Tenant Network、R：従来のルーティング

論理図

別紙３「アクセスポリシー」

		アクセス元																			
	セグメント	インターネット(SINET)	インターネット(商用)	DMZ	職員向けサーバー	共用・管理用サーバー	外部利用者向けサーバー	ネットワーク機器管理	監視	財務管理	総務管理	一般事務	研究	プリンタ	NAS	リモート接続	相談・会計・受付	機器利用	デザインセンター(本部)	CAD/CAE	未承認
アクセス先	インターネット(SINET)		×	○	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×
	インターネット(商用)	×		×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×
	DMZ	○	×		○	○	○	×	○	○	○	○	○	×	×	○	○	○	○	○	×
	職員向けサーバー	×	×	×		○	×	×	○	○	○	○	○	○	×	○	○	×	×	×	×
	共用・管理用サーバー	×	×	×	○			○	○	○	○	○	○	×	×	○	○	×	×	×	×
	外部利用者向けサーバー	×	×	×	×	×		×	○	×	×	×	○	×	×	○	×	○	○	○	×
	ネットワーク機器管理	×	×	×	○	○	×		○	×	×	×	×	×	×	×	×	×	×	×	×
	監視	×	×	×	○	○	×	○		×	×	×	×	×	×	×	×	×	×	×	×
	財務管理	×	×	×	○	○	×	○	○		×	×	×	○	○	○	○	×	×	×	×
	総務管理	×	×	×	○	○	×	○	○	×		×	×	○	○	○	○	×	×	×	×
	一般事務	×	×	×	○	○	×	○	○	×	×		×	○	○	○	○	×	×	×	×
	研究	×	×	×	○	○	×	○	○	×	×	×		○	○	○	○	×	×	×	×
	プリンタ	×	×	×	○	○	×	○	○	○	○	○	○		×	×	○	○	○	○	×
	NAS	×	×	×	○	○	×	○	○	○	○	○	○	×		×	○	×	×	×	×
	リモート接続	×	×	×	○	○	×	○	○	○	○	○	○	○	×		×	×	×	×	×
	相談・会計・受付	×	×	×	○	○	×	○	○	○	○	○	○	○	×	○		×	×	×	×
	機器利用	×	×	×	×	○	○	○	○	×	×	×	×	○	×	×	×		×	×	×
	デザインセンター(本部)	×	×	×	×	○	○	○	○	×	×	×	×	○	×	×	×	×		×	×
	CAD/CAE	×	×	×	×	○	×	○	○	×	×	×	×	○	×	×	×	×	×		×
	未承認	×	×	×	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×	×	

それぞれに VLANID が割り振られており、○が通信可能、×が通信不可となる。

別紙 4　無線 LAN 接続エリア

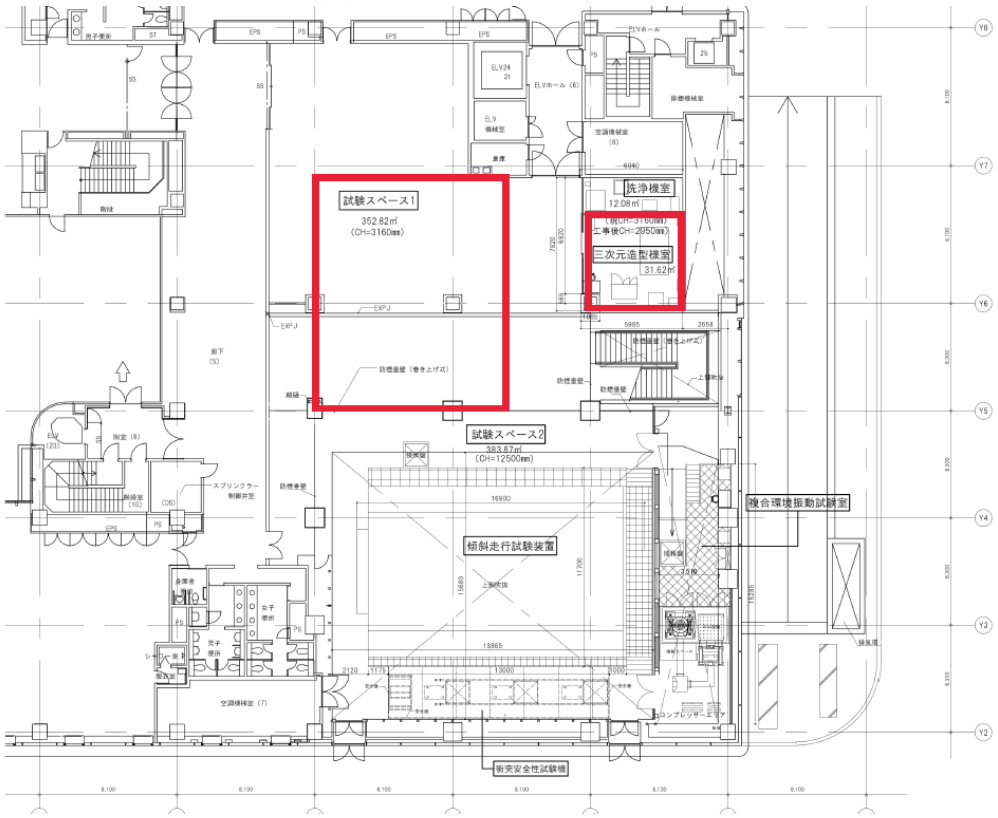
本部 1 階

本部２階

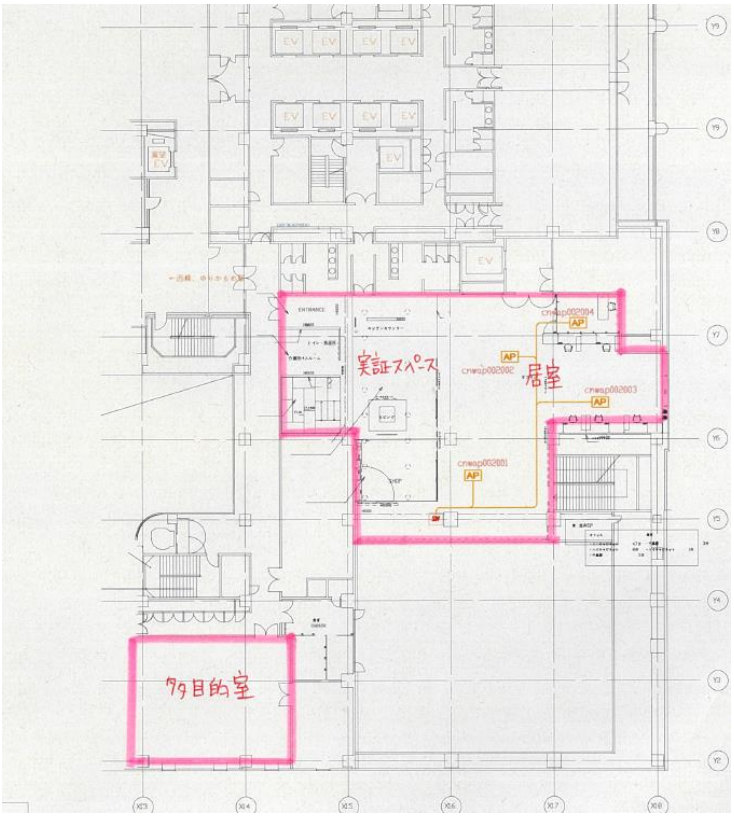
本部 3 階

本部 4 階

本部 5 階

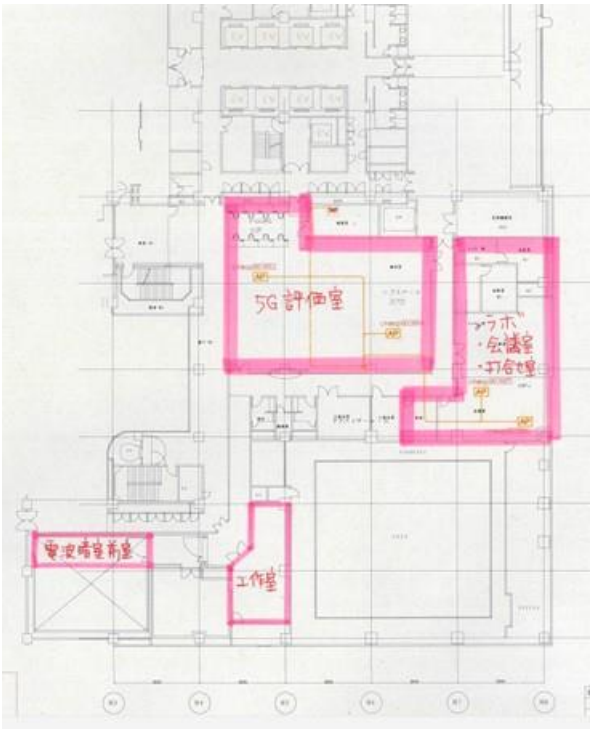


テレコムセンター1 階



テレコムセンター2 階

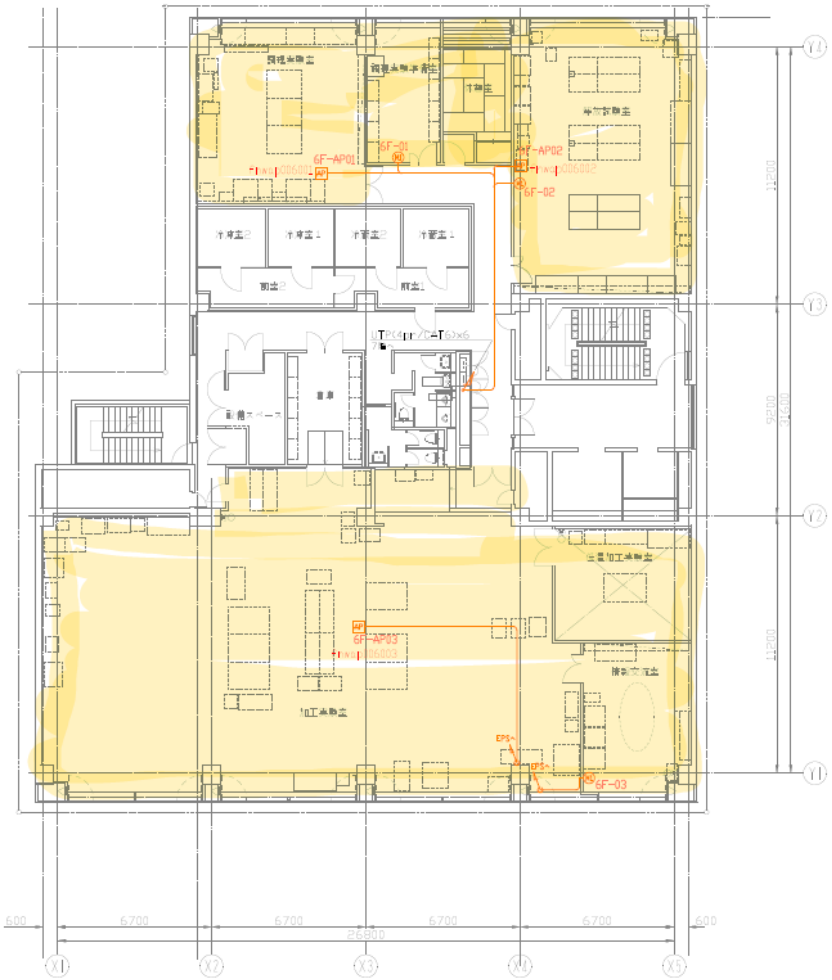
テレコムセンター3 階



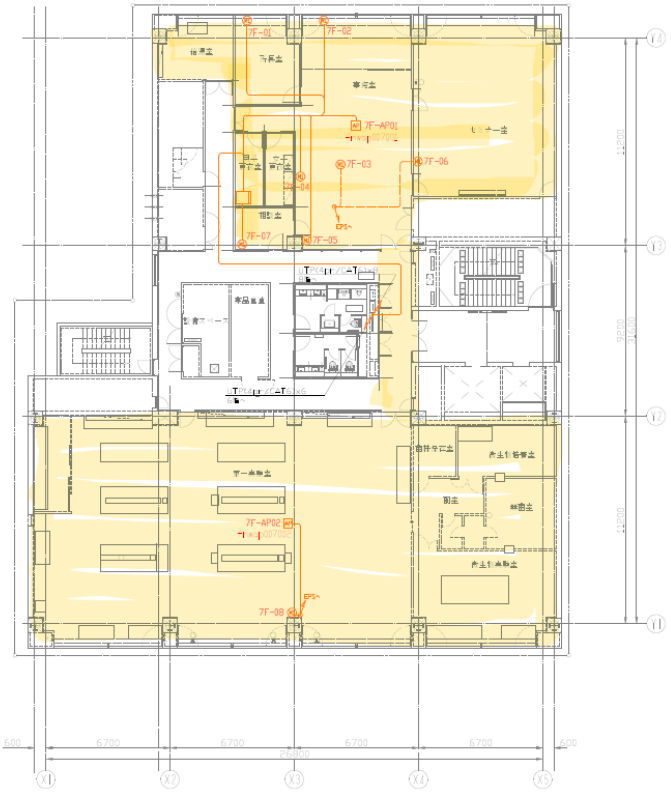
テレコムセンター3 階


生活空間計測スタジオ
染色加工試験室
クリーニング試験室
品質評価試験室
高度観察システム室
生活科学試験室
被服科学試験室
恒温恒湿室
官能検査室
デザイン制作室
生活環境試験室
システム管理室
日射フィールド試験室
snesw012006
snesw012010
snesw012011
工作室
実験参加者控室
耐光性試験室
セミナー室
墨田分室・事務室
会議室
応接室
用品保管庫
EV
用品倉庫
執務室
縫製試験室
SN ×2 snesw012008, 9

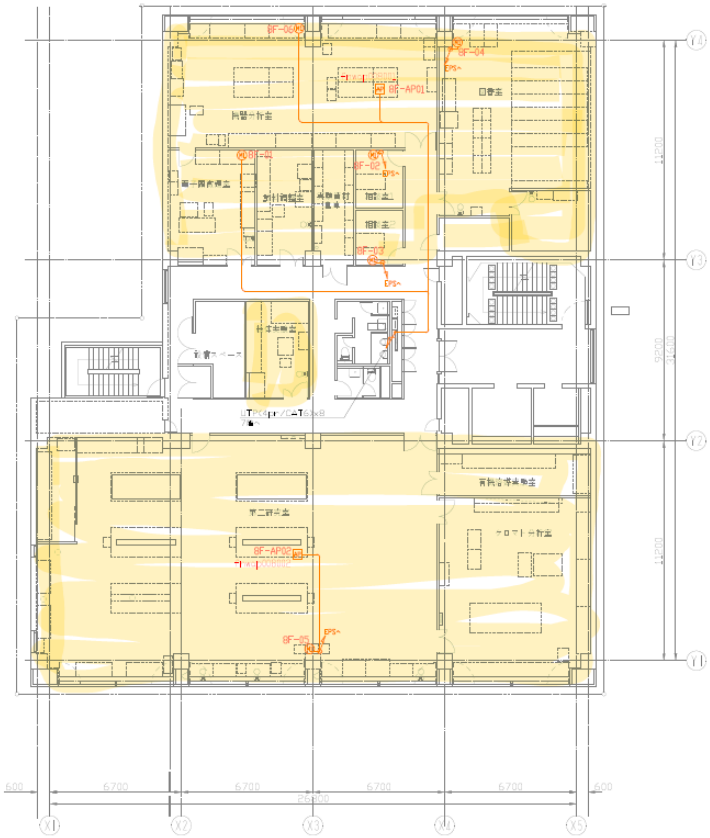
墨田支所


6F-AP01
6F-AP02
6F-AP03
6F-01
6F-02
6F-03
EPS
X1
X2
X3
X4
X5
Y1
Y2
Y3
Y4
600
6700
6700
6700
6700
600
26800

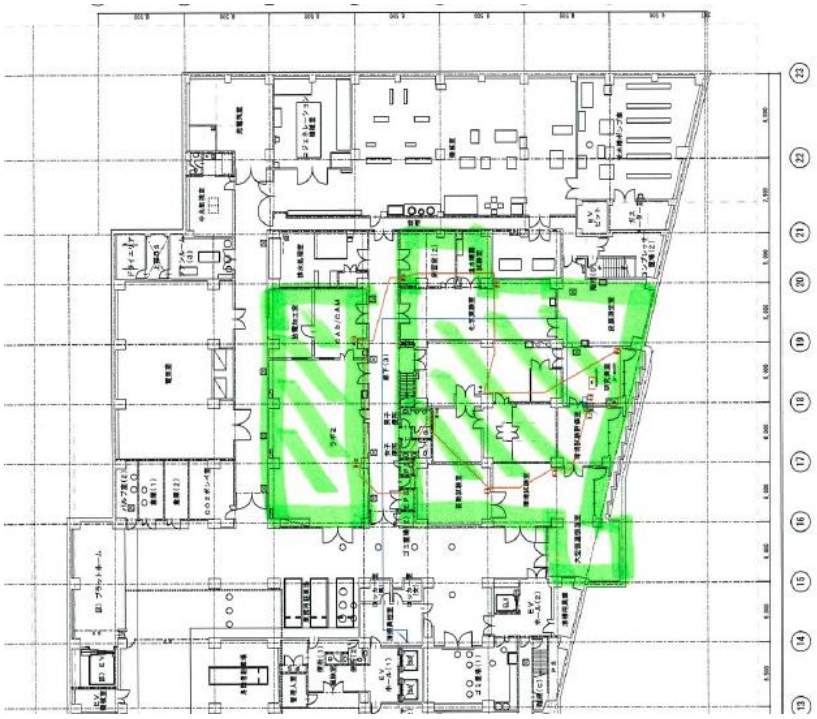
食品技術センター6 階



食品技術センター7 階



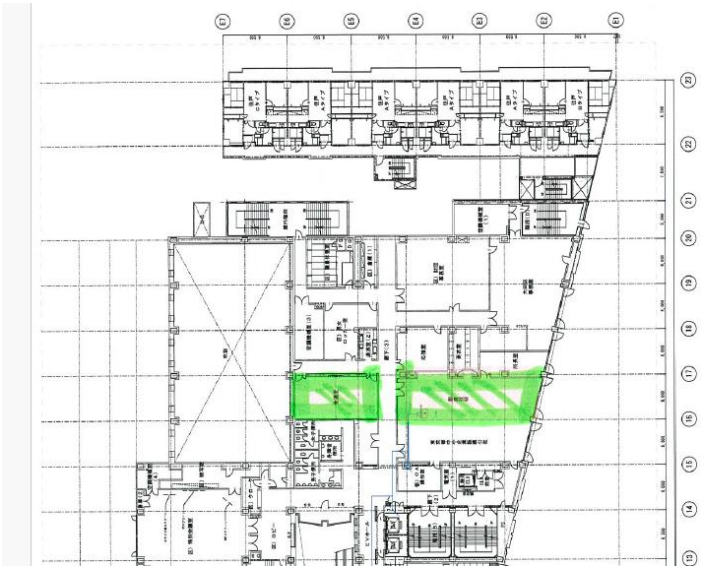
食品技術センター8 階



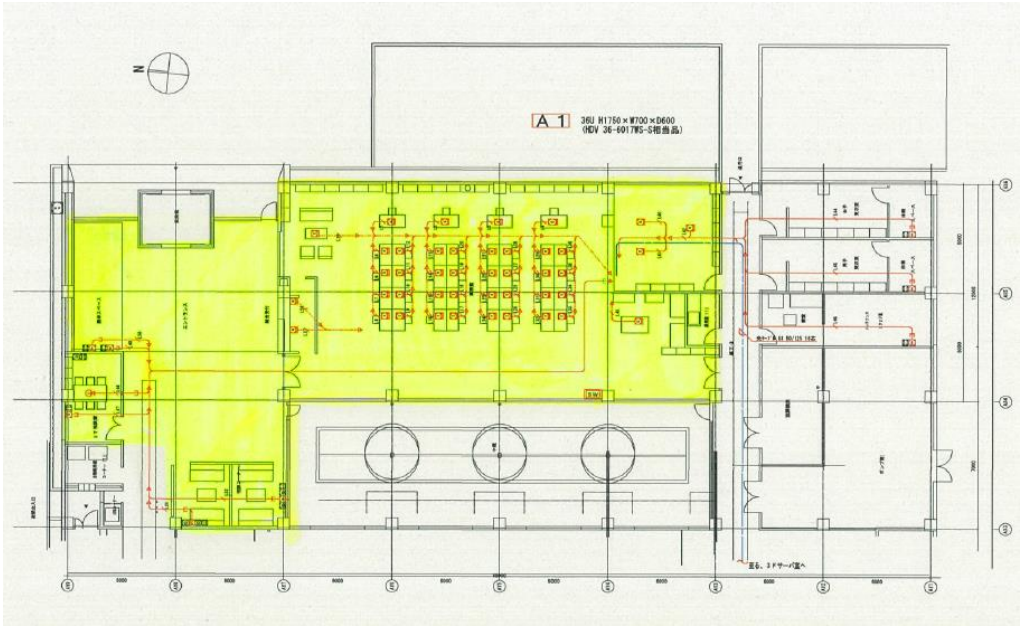
城南支所　地下１階

城南支所　１階

城南支所　2 階

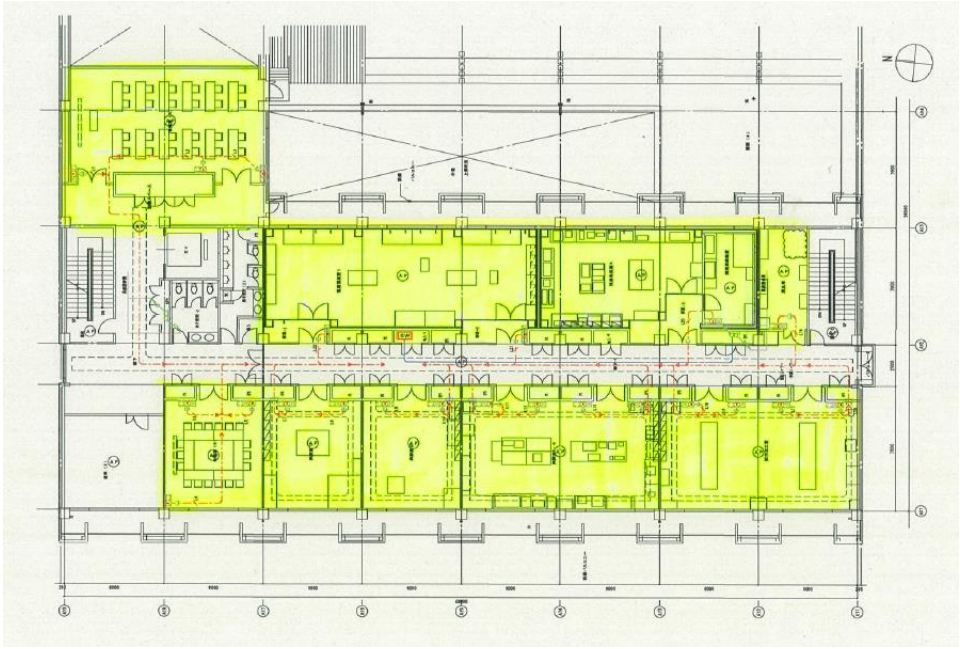


城南支所　3 階

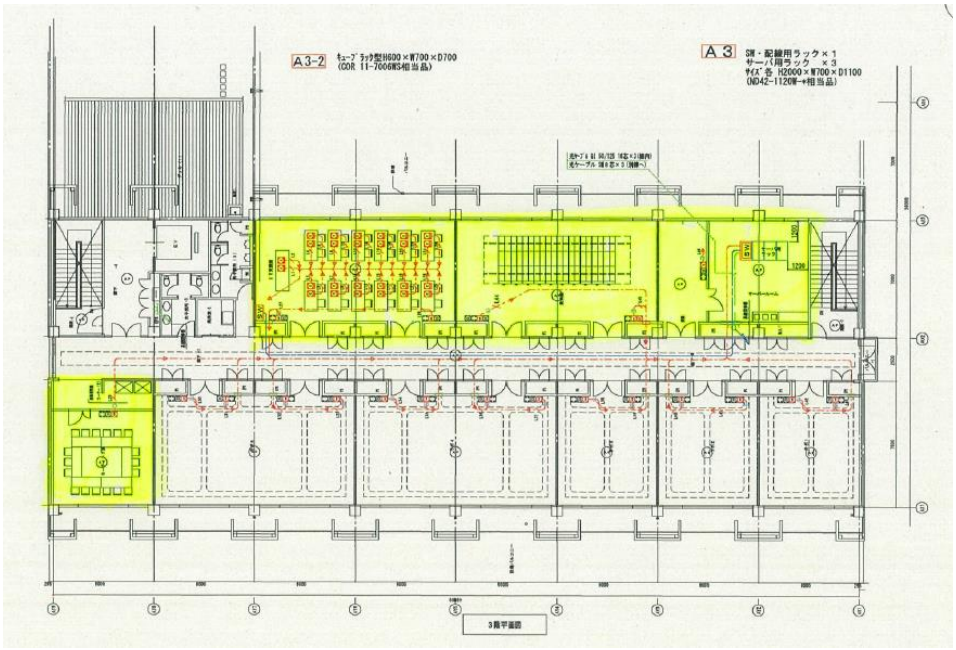


多摩テクノプラザ　1階東

多摩テクノプラザ　1階西

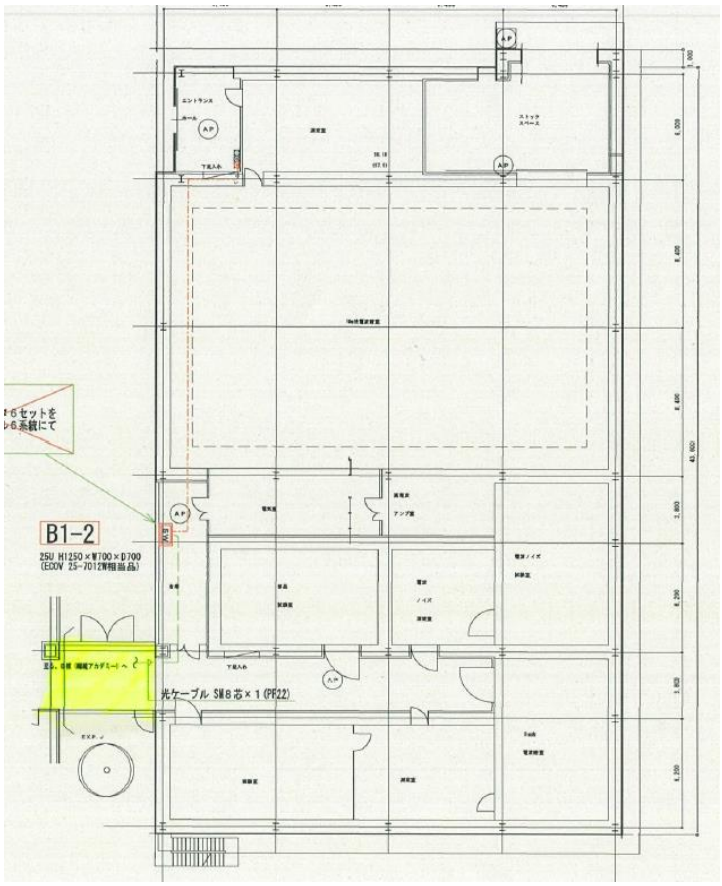


多摩テクノプラザ　２階



多摩テクノプラザ　３階

多摩テクノプラザ　B 棟



多摩テクノプラザ　電波暗室棟