# 神戸市立西神戸医療センターネットワーク基盤更新業務

神戸市民病院機構

## 1　総則

### 1.1　作業項目

①　神戸市立西神戸医療センター（以下　「西神戸医療センター」という）におけるネットワーク（インターネット系）基盤の更新業務

### 1.2　目的

神戸市民病院機構（以下 「機構」という）の法人本部、中央市民病院、西市民病院、神戸アイセンター病院については共通のネットワーク基盤で運用している。西神戸医療センターにおけるネットワーク基盤を更新・整備をすることで、機構全体の情報セキュリティ向上および利用者の利便性向上を目指す。

また、有線LANについては情報コンセント、及びアクセスポイントの追加をおこなう。

### 1.3　作業場所

神戸市立西神戸医療センター

神戸市西区糀台5丁目7番地1

### 1.4　工期

**契約締結後　～　令和7年3月31日**

### 1.5　作業スケジュール

導入に伴う詳細なスケジュールは受託者が作成したうえで機構に提示し了承を得ること。

## 2　作業概要

### 2.1　西神戸医療センターにおけるネットワーク基盤の整備

本作業は、西神戸医療センターの既設ネットワーク基盤を更新・整備するもので、以下の項目を実施すること。(別紙1　機器プロット・配線図 参照)

①　職員用有線LAN環境および無線LAN環境にかかる機器の更新（認証装置含む）

②　患者用無線LAN環境にかかる機器の更新（認証装置含む）

③　機器更新後の電波環境の調査および機器の調整

④　不正接続を防止する装置、及び患者用の無線利用を時間制限できる装置の更新

⑤ 無線LANコントローラ機器の更新

⑥ ネットワーク機器監視サーバの更新（西神戸監視機器用）

⑦ 遠隔監視用のネットワーク環境にかかる機器更新（西神戸監視機器用）

⑧ サーバセグメントにあるファイル共有サーバは更新しない。更新される機器と新たに接続を行うこと

⑨ サーバ室に設置するサーバがある場合はサーバラック用コンソールモニタを用意すること、但し今回導入するシステムがすべてアプライアンス型であり、サーバが存在しない場合はその限りではない。

⑩ スタッフページ（財務会計システム含む）およびメール送受信は既存の閉域網を使って中央市民病院側と通信させる等、既設ネットワークの設定を引き継ぐこと。

⑪ 購入による導入機器の取扱説明および運用に必要なドキュメント整備

⑫ 更新機器導入時において既設端末の設定変更等が必要な場合は病院と相談し対応すること。なお現在の端末数（WindowsOS端末）は（持込端末（持込セグメント）：500台弱、医療事務端末（医療・事務セグメント）：300台弱稼働している。）なお、IPADについては医療・事務セグメントで200台程度稼働しており、JAMFにて管理している。（持込セグメントのIPADについてはJAMFへの登録はしていない）

⑬ 導入後の運用サポート

⑭ 保守関連

⑮ 当調達で導入する機器類について、CPU室内およびEPS等で電源工事が必要な場合は二次側電源の工事をおこなうこと。

⑯ 職員用情報コンセントの追加工事（13箇所）

⑰ 5F手術部門の手術室内のアクセスポイント追加工事（8箇所）を行うこと。またアクセスポイントも追加で見込むこと。（別紙1参照）

⑱ 無線アクセスポイントの設置台数は、現状設置の場所は必ず踏襲すること、別紙1に示す無線LAN利用想定範囲において問題なく無線LANが利用できるよう必要に応じて追加すること。

# 3 作業実施内容に関する事項

## 3.1 施工上の基本事項

(1) 施工にあたっては、本仕様書に従い施工すること。

(2) 施工にあたって労働基準法、労働安全衛生法およびその他関連する諸法令に示された条項を遵守し、安全および衛生管理について十分な管理監督を行い施工すること。

## 3.2 作業の実施体制

(1) 作業実施体制

1）本業務に係るリーダとして、プロジェクトマネージャを設置すること。

2）プロジェクトマネージャもしくはその代理の者は、本調達に関わる機構との会議に全て参加できる体制を取ること。

⑵ 作業場所

1）本業務の作業場所（サーバー設置場所等を含む）は、西神戸医療センターまたは機構の承認した場所で作業すること。

2）西神戸医療センターまたは機構内での作業においては、立ち入り申請など必要な所定の手続を実施し承認を得ること。

3）機構職員は、必要に応じて現地確認を実施できることとする。

⑶ 作業の管理

1）受託者は、機構が承認したプロジェクト実施計画書に基づき、本業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、構成管理、変更管理、情報セキュリティ対策を行うこと。

### 3.3　作業実施にあたっての遵守事項

⑴ 基本事項

受託者は、次に掲げる事項を遵守すること。

1）本業務の遂行にあたり、業務の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。

2）本業務に従事する要員は、機構と日本語により円滑なコミュニケーションを行う能力と意思を有していること。

3）本業務の履行場所を他の目的のために使用しないこと。

4）本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。

5）要員の資質、規律保持、風紀および衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。

6）受託者は、本業務の履行に際し、機構からの質問、検査および資料の提示等の指示に応じること。また、修正および改善要求があった場合には、別途協議の場を設けて対応すること。

7）次回の本業務調達に向けた現状調査、機構が依頼する技術的支援に対する回答、助言を行うこと。

8）本業務においては、業務終了後の運用等を、受託者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

⑵ 機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおりとする。

1）受託者は、受注業務の実施の過程で機構が開示した情報（公知の情報を除く。以下同じ。）、他の受託者が提示した情報および受託者が作成した情報を、本受注業務

の目的以外に使用または第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。

2）受託者は、本受注業務を実施するにあたり、機構から入手した資料等については管理簿等により適切に管理し、かつ、以下の事項に従うこと。

・　複製しないこと。

・　用務に必要がなくなり次第、速やかに機構に返却または消去すること。

・　受注業務完了後、上記 1)に記載される情報を削除または返却し、受託者において該当情報を保持しないことを誓約する旨の書類を機構に提出すること。

3）応札希望者についても上記 1)および 2)に準ずること。

4）「地方独立行政法人神戸市民病院機構 情報セキュリティポリシー（基本方針・対策基準、個別基準）」を遵守すること。

5）「秘密保持等に関する誓約書」を別途提出し、これを遵守すること。

6）機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

(3) 遵守する法令等

本業務を実施するにあたっての遵守事項は、以下のとおりとする。

1）受託者は、最新の「政府機関のサイバーセキュリティ対策のための統一基準」、「府省庁対策基準策定のためのガイドライン」、「医療情報システムの安全管理に関するガイドライン」および前項（2）の 4）を遵守すること。

2）機構へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること。

3）民法、刑法、著作権法、不正アクセス禁止法、個人情報保護法等の関連法規を遵守することはもとより、下記の規程を遵守すること。

・　地方独立行政法人神戸市民病院機構 個人情報保護法等の施行等に関する規程

・　情報セキュリティ遵守特記事項

（契約時）

別紙 4「情報セキュリティ遵守特記事項」を付加

③契約後納品検査時(年 1 回。但し年間に複数回納品検査を行う場合は、年度内の初回検査時)

別紙 5「情報セキュリティ対策の実施状況報告書」を提出させて実施状況を確認

・　神戸市個人情報保護法の施行等に関する条例（令和 4 年 12 月条例第 17 号）

4）受託者は、本業務において取り扱う情報の漏洩、改ざん、滅失等が発生することを防止する観点から、情報の適正な保護・管理対策を実施するとともに、これらの実施状況について、機構が定期または不定期の検査を行う場合においてこれに応じること。万一、情報の漏洩、改ざん、滅失等が発生した場合に実施すべき事項および手順等を明確にするとともに、事前に機構に提出すること。また、そのような事態が発生した場合は、機構に報告するとともに、当該手順等に基づき可及的速やかに対応すること。

### 3.4　役務

(1) 計画

1. 受託者は、プロジェクト実施を円滑に行うための計画書を作成し、機構の承認を得ること

(2) 報告

1. 受託者は、プロジェクト計画書に基づき定期的に進捗状況を書面にて報告すること。報告内容には以下の内容を含めること。
   (ア)計画書と実績との差異
   (イ)課題等の対応状況
2. 機構が求めた場合は、機構施設内にて会議を実施し報告を行うこと。会議を実施した場合は、受託者が会議における議事録を開催後 3 営業日以内に作成し、機構の承認を受けること。
3. 受託者は、本調達の各工程における設計内容や成果物等に関する協議を随時行い、機構と受託者間での認識齟齬がないように努めること。
4. 受託者は、西神戸医療センターまたは機構の既存システムに対する変更および既存システムに影響のある作業を行う場合は、原則として作業を行う 14 日以上前に当該作業内容と影響内容・範囲を提示すること。当該作業が終了した後は速やかに作業結果を報告すること。

(3) 設計

1. 受託者は、本業務で実施する配線工事の設計、納入する物品および関連する既存基盤を安定して動作させるための設計を行い、機構の承認を得ること。

(4) 導入

1. 受託者は、機構に対して本業務で納入する物品の導入作業を行うこと。
2. 関連する既存基盤について必要な設定変更作業については、機構から既存ベンダーに対して随意契約を行う。
3. 既存機器の設定変更および新規に調達する機器の設定が、その調達範囲をまたぐ場合は相互に協力し作業を進めること。
   （別紙２　接続構成イメージ図参照）
4. 設計・構築時に必要なサポートを直接導入ベンダーによりサポートが受けれること。

(5) テスト

1. 受託者は、本業務に係るテストについて、テスト体制、テスト環境、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、機構の承認を得ること。
2. 導入機器の正常性試験、冗長構成での障害試験は、導入ベンダーにて実施すること。
3. 受託者は、テスト計画書に基づき作業工程毎に動作テストを行うこと。

4. 受託者は、動作テストの実施状況および結果を機構に報告すること。
5. 受託者は、テストの結果不都合が生じた場合、速やかに対策を講じること。
6. 中央市民病院内の既存機器も含めた動作確認試験は、既存機器保守ベンダーと協力して実施すること。また、正常確認が取れない場合には、既存機器保守ベンダーと原因究明を行い修正設定後の動作確認まで実施すること。また、調査や修正設定等に費用がかかる場合は病院と協議すること。

(6) 検収支援

1. 受託者は、機構が配線工事および納入物の検収を実施するにあたり、必要な情報の提供等の協力を行うこと。

(7) 施工にあたって労働基準法、労働安全衛生法およびその他関連する諸法令に示された条項を遵守し、安全および衛生管理について十分な管理監督を行い施工すること。

### 3.5 施工方法

(1) 作業日および作業時間は、別途打合せの上決定する。

(2) 作業に関する材料および工具類等は全て受注者が準備すること。

(3) ケーブルの色は別途指示する物を準備すること。(インターネットは黄色)

(4) 新設 LAN ケーブルについては、下記例を参考に行先表示をケーブルの両端に貼付すること。既設ネットワークで使用している記載条件を引き継ぐ事

(例)

| |
|---|
| From 機器名　ﾎﾟｰﾄ番号 |
| To 機器名　ﾎﾟｰﾄ番号 |

### 3.6 既設機器のネットワークへの接続および既存機器からの設定引き継ぎについて

(1) 既存の職員用不正接続防止機器の設定内容を新たに導入する不正接続防止機器に引き継ぐこと。

(2) 既存のインターネット系ファイアウォールの設定内容を新たに導入するファイアウォールに引き継ぐこと。

(3) 作業完了後は、運用開始時に立会い作業を実施し、正常に動作することを確認し機構の了承を得ること。

### 3.7 作業時の配慮

(1) 診療業務およびその他の病院業務に支障がでないよう、可能な限り配慮すること。特に患者等の安全確保に留意すること。

(2) 工事の実施にあたって、態度・服装に配慮すること。また作業時間については、必要に応じ事前に了承を得るなど、トラブル防止に努めること。

(3) 工事場所での作業完了後、後始末を確実に行い苦情および事故防止に努めること。

### 3.8　臨機の措置

(1) 災害または公害が発生した場合は、速やかに適切な措置をとり、直ちにその経緯を機構に報告すること。

### 3.9　人身事故の防止

(1) 安全設備および安全器具

工事施工に必要な安全装飾および安全器具は、事前に点検整備し、適正に使用すること。

(2) 転落防止

高所作業においては、適切な足場および手摺の設置等必要な措置を講じ、事故防止に努めること。

### 3.10　設備事故の防止

(1) 工事現場周辺の構造物を損傷し、または、現用通信回線に故障を発生させないように適切な予防措置を講じ、設備事故の防止に努めること。

(2) 電気、ガス、上下水道等作業現場周辺の他所管施設に接近して工事を行う場合は、必要により施設管理者の立会を求め、適切な防護措置を講じるとともに、常に保安点検を行い事故防止に努めること。

## 4　成果物の取扱いに関する事項

### 4.1　知的財産権の帰属

(1) 本件に係り作成・変更・更新されるドキュメント類およびプログラムの著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、受託者が本件のシステム導入の従前より権利を保有していた等の明確な理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外、機構が所有する現有資産を移行等して発生した権利を含めて、機構に帰属するものとする。

(2) 本件に係り発生した権利については、受託者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。

(3) 本件に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受託者は原著作物の著作権者としての権利を行使しないものとする。

(4) 本件に係り作成・変更・修正されるドキュメント類およびプログラム等に第三者が権利を有する著作物が含まれる場合、受託者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前に機構に報告し、承認を得ること。

(5) 本件に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら機構の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。この場合、機構は係る紛争の事実を知ったときは、受託者に通知し、必要な範囲

で訴訟上の防衛を受託者にゆだねる等の協力措置を講ずる。なお、受託者の著作または一般に公開されている著作について引用する場合は、出典を明示するとともに、受託者の責任において著作者等の承認を得るものとし、機構に提出する際は、その旨併せて報告するものとする。

### 4.2　瑕疵担保責任

(1) 本業務の最終検収後 1 年以内の期間において、委託業務の納入成果物に関して本システムの安定稼動等に関わる瑕疵の疑いが生じた場合であって、機構が必要と認めた場合は、受託者は速やかに瑕疵の疑いに関して調査し回答すること。調査の結果、納入成果物に関して瑕疵等が認められた場合には、受託者の責任および負担において速やかに修正を行うこと。なお、修正を実施する場合においては、修正方法等について、事前に機構の承認を得てから着手するとともに、修正結果等について機構の承認を受けること。

(2) 受託者は、瑕疵担保責任を果たす上で必要な情報を整理し、その一覧を機構に提出すること。瑕疵担保責任の期間が終了するまで、それらの情報が漏洩しないように厳重に管理をすること。

### 4.3　検収

(1) 納入成果物についてはテスト計画書を作成し、作業項目毎に確認テストを機構の立会いのもとで実施し、合否判定を受けること。最終的な納入成果物については「4.4（1）表１成果物」に記載の全てが揃っていることおよび合否判定後の改訂事項等が反映されていることを機構が確認し、これらが確認され次第、検収終了とする。

(2) 受託者は、瑕疵担保責任を果たす上で必要な情報を整理し、その一覧を機構に提出すること。瑕疵担保責任の期間が終了するまで、それらの情報が漏洩しないように厳重に管理をすること。また、以下についても遵守すること。

- 検査の結果、納入成果物の全部または一部に不合格品を生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、機構の承認を得て指定した日時までに修正が反映された全ての納入成果物を納入すること。
- 「納入成果物」に規定されたもの以外にも、必要に応じて成果物の提出を求めた場合は、機構と協議の上で作成すること。
- 機構の品質管理担当者が検査を行った結果、不適切と判断した場合は、品質管理担当者の指示に従い対応を行うこと。

### 4.4　納入すべき成果物

(1) 成果物の種類、期日

作業工程別の納入成果物を下記に示す。また、納入成果物の構成、詳細については、

受注後、機構と協議し取り決めること

表 1 成果物

| 項番 | 工程 | 納入成果物 | 納入期日 |
|---|---|---|---|
| 1 | 計画 | ・プロジェクト実施計画書 | 契約締結日から 2 週間以内 |
| 2 | 設計 | ・環境設計書<br>・環境定義書<br>・納入製品一覧（機器一覧、ソフトウェア一覧表、付属品・予備品表、機器・性能・動作説明書、付属マニュアル・取扱説明書、システム構成図、機器配置図等） | 導入工程着手まで |
| 3 | 導入 | ・導入・移行手順書<br>・導入・移行作業結果報告書 | 導入・移行作業着手まで<br>テスト工程着手まで |
| 4 | テスト | ・テスト計画書<br>・テスト結果報告書 | テスト作業着手まで<br>各テスト作業実施後 1 週間以内 |
| 5 | 検収 | ・構築資料（基本設計、詳細設計、設定シート、試験成績表等） | 検収時 |
| 6 | 運用・保守 | ・運用手順書<br>・操作、設定手順書<br>・保守マニュアル<br>・製品マニュアル<br>・利用者向け資料（端末設定手順書、操作マニュアル等） | 検収時 |
| 7 | その他 | ・打ち合わせ資料<br>・課題管理表<br>・議事録<br>・機密情報受理管理簿<br>・瑕疵担保責任対応に係る保有情報の一覧 | 必要に応じて随時 |

(2) 納入成果物に記載すべき内容

納入成果物に記載すべき内容を以下に記す。ただし、導入作業や運用を行うにあたり、追記若しくは他に作成すべきものがあれば、機構と協議の上で作成すること。

① プロジェクト実施計画書

- プロジェクトスコープ
- 体制表
- 受託者と機構の作業分担表
- スケジュール
- プロジェクト管理要領(文書管理要領、セキュリティ管理要領、品質管理要領、変更管理要領)
- WBS（作業分解図）

② 環境設計書

- 設計方針
- システム構成図(物理・論理)
- ネットワークおよびIP アドレス一覧

・　システムアカウントおよびアクセス方法、用途の一覧
・　運用設計
・　配線系統図、配線図
・　ラック搭載図(各ラックに搭載された機器等の配置図)

③　環境定義書
・　導入製品のパラメータ一覧
・　正常稼動するために必要なサービスの一覧
・　既存機器のパラメータ一覧

④　納入製品一覧
・　導入物品の一覧(シリアル、ライセンス、バージョン情報が分かるようにすること)

⑤　導入・移行手順書
・　導入および移行作業における具体的な手順(既存システムへの影響がある作業は特に影響範囲を明示すること)

⑥　導入・移行作業結果報告書
・　導入および移行作業後の結果と課題

⑦　テスト計画書
・　テストの実施方針
・　単体テスト、複合テスト、移行作業における正常および異常テストの内容

⑧　テスト結果報告書
・　テスト計画書に従い実施したテスト結果
・　テストデータ
・　テスト証跡

⑨　運用手順書
・　環境設計書に記した運用設計に基づいた導入製品の操作手順※1

⑩　保守手順書
・　導入製品のハードウェアおよびソフトウェアライフサイクル(導入時に判明しているもの)
・　保守体制図(連絡先および受付部署を明記すること)

⑪　製品マニュアル
・　導入製品の全マニュアル

⑫　打ち合わせ資料
・　打ち合わせに必要な資料を随時作成すること

⑬　課題管理表
・　各工程で発生する課題の一覧
・　課題発生日、起票者、回答者、解決期限、対応履歴を記載すること

⑭　議事録
・　各会議での議論概要

・　日時および場所
・　出席者

⑮　機密情報受理管理簿
・　機構から受領した機密情報の開示範囲および日時
・　機構が破棄を指示した機密情報の破棄日時
・　機構が返却を指示した機密情報の返却日時

⑯　瑕疵担保責任対応に係る保有情報の一覧
・　瑕疵担保責任対応に必要となる資料(導入作業時に言及のなかった資料がある場合に提出)

⑰　データ消去証明書
・　本調達の運用終了後に導入製品のデータ消去が確実に行われたとわかるもの

※1　起動・停止、バックアップ、リストア、障害監視、正常動作を確認する上で必要となる主要なログ監視、性能監視、主要な設定変更が分かるようなものとし、他の内容は機構と協議の上で作成すること

(3) 納入成果物の提出等

納入成果物を期日までに提出の上、機構の承認を得ること。納入成果物は以下の要件を満たすこと。

①　PDF 形式およびMicrosoft Officeで扱える形式とすること。ただし、機構が別に形式を定めて提出を求めた場合はこの限りではない。

②　各納入成果物は日本語により作成すること。製品マニュアルについては日本語または英語によるものとする。

③　納品成果物は西神戸医療センターに納入すること。

④　本業務を実施する上で必要となる一切の機器納入物等は受託者の責任で手配するとともに、費用を負担すること。

⑤　各工程の納入成果物も含め、本調達に係る全ての資料を納入すること。

⑥　ただし、調達機器の管理画面（ダッシュボード等）で参照できる情報について、機構が提出不要と認めた場合、これらの限りではない。

## 5　再委託に関する事項

(1) 受託者は、受注業務を自己の責任において完全に履行しなければならない。

(2) 書面による事前の承諾なくして、委託業務を第三者へ委託してはならない。

(3) 受注業務の全部または大部分についての一括した再委託の承諾をすることはできない。

(4) 書面による承諾なくして、この契約上の地位またはこの契約によって生ずる権利若しくは義務を第三者に譲渡してはならない。

(5) 再委託先が、更に再委託を行う場合も同様とする。

(6) 再委託における情報セキュリティ要件については以下のとおり。

- 受託者は、再委託先における情報セキュリティ対策の実施内容を管理し、機構に報告すること。
- 受託者は、業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、機構に報告すること。
- 受託者は、再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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して、機構から求めがあった場合には情報提供を行うこと。
- 受託者は、再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、機構に報告すること。
- 受託者は、再委託先における情報セキュリティ対策、およびその他の契約の履行状況の確認方法を整備し、機構へ報告すること。
- 受託者は、再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、機構へ報告すること。
- 受託者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。
- 受託者は、再委託先が自ら実施した外部監査についても機構へ報告すること。
- 受託者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、または抹消されたことを確認すること。

## 6　その他

(1) 受託者は、導入機器の引渡し以前に発生した障害について、機構と協議の上、決定した期間内に障害の復旧を完了すること。

(2) 導入段階での障害発生時には直接導入ベンダーによるサポートが受けることのできる体制とすること。

(3) 本仕様書に記載の無い事項については、その都度、指示を受けること。

(4) 撤去機器については廃棄すること。なお、廃棄されるサーバ等の機器については、データ消去等セキュリティ上の処理を施した上で廃棄すること。また消去した旨を書面等で証明すること。

(5) 受託者は、既設機器に対して保守ベンダーが存在する場合は、既存保守ベンダーと協力して作業を実施することとする。

(6) UPS はシステム毎に設置するのではなく、大規模容量の UPS を利用することにより、省電力、省スペース、コスト低減に努めること。また停電時に安全かつ自動的にシステム停止できる仕組みを導入すること。

(7) サーバ等の導入によりサーバ室の電源工事が必要となった場合は、受託者で対応すること。

(8) サーバ等の導入によりラックが必要となった場合は、受託者で対応すること。

(9) 入札に先立ち、希望により現地見学を実施した上で、仕様書に関する不明点等は質疑回答期間にて受け付けるものとする。

(10) 基本要件として応札業者においては 400 床以上の病院においてインターネット系ネットワーク※の導入実績を 3 件以上有すること。(※インターネット系ネットワークとは、400 床以上の病院で病棟および外来において、患者用フリーWi-Fi の利用ができるネットワークの構築や職員用の Wi-Fi・有線ネットワークが利用できるネットワーク構築業務の実績があることを言う）また、今回導入するネットワーク機器についてコアスイッチ、サーバスイッチ、PoE スイッチ、無線アクセスポイントについても同様に 400 床以上の病院においてインターネット系での実績があるメーカーを選定基準とする。また応札業者は ISO9001 を取得していること。

# 7　西神戸医療センターにおけるネットワーク基盤の整備

## 7.1　作業概要

① 西神戸医療センターにネットワーク基盤を更新・整備する。ネットワーク基盤は職員用および患者用とし、同じアクセスポイントを異なる SSID を付与することで論理的に分割する。また各 SSID は異なる VLAN を任意に割り当てできること。

② 職員用および患者用は西神戸医療センターに専用ゲートウエイ(Firewall・UTM 等)を個別に設け、これを経由してインターネットにアクセスする。

③ 各 VLAN ごとにアクセス制限を個別に設定可能であること。

④ 西神戸医療センター病院総合情報システムネットワークのアクセスポイントから発する電波の周波数が 5GHz 帯を使用しているため、アクセスポイントから発する電波の周波数は原則 2.4GHz 帯を用い、病院総合情報システムネットワークおよび既存の医療機器等と干渉しない設計とする。なお、受託者側の責任において別の周波数に変更したい場合は、既存の病院総合情報システムネットワークおよび医療機器等と干渉しない根拠となる資料を提示した上で、機構と相談すること。

⑤ 受託者の責任において、設置後のサーベイを実施し、電波測定を実施するとともに、既存システムネットワークに影響が出ないことを示すこと。

⑥ フロアスイッチは各階 EPS 室内に設置し、アクセスポイントは景観への配慮等の観点から天井または壁面に設置すること。通信用ケーブルは、コアスイッチからフロアスイッチ間を光回線とし、フロアスイッチ以下の機器へは Cate5e 以上のケーブルを用いること。仕様に満たない配線類はすべて新規で配線すること。

⑦ 既設のネットワーク配線は流用可能とする。

⑧ 中央市民病院の管理者が、各ネットワーク機器の状態が監視・設定変更ができるようにすること。

⑨ 既存のネットワーク環境から新ネットワーク環境への切替は速やかに実施して停止時間を最小化すること。

⑩ コアスイッチ、サーバスイッチ、フロアスイッチ、PoE スイッチ、無線アクセスポイント、無線コントローラ、ネットワーク監視装置は、保守性の観点より可能な限りメーカーを統一すること。

⑪ サービス提供型（クラウド利用）の場合、個人情報等が含まれる場合においては機構へ報告を行い、必要に応じて機構の定める別紙（外部サービス要件）の要件を満たすこと。

⑫ 有線 LAN については IP サブネット VLAN やダイナミック VLAN 等の機能を用いて異なるセグメントで設定された端末が利用できること（利用出来る端末は認証装置で許可されたものとする）各セグメント（持込・医療・事務）で設定された端末が会議室等で有線 LAN 接続で使用する際に問題なく利用できることとする。

⑬ 既設のプロキシサーバは廃止する。

## 7.2 ネットワーク機器仕様

(1) PoE SW（給電対応レイヤー 2 スイッチ）

以下の機能を満たすこと。

1. 装置単体で 10/100/1000BASE-T のインターフェースを 48 ポート以上有すること。
2. 装置単体で SFP スロットを 4 つ以上有すること。
3. IEEE 802.3z 1000BASE-LX/SX、IEEE 802.3ab 1000BASE-T、IEEE 802.3ah 1000BASE-BX10 に準拠した SFP を搭載可能なこと。
4. 装置単体でスイッチングファブリックは 336Gbps 以上であること。
5. 装置単体で MAC アドレス登録数は 16,384 以上であること。
6. 装置単体で IEEE 802.1Q に準拠した 4,094 以上の VLAN を設定可能なこと。
7. VLAN の種類として、ポートベース VLAN、IEEE 802.1Q タグベース VLAN、IP サブネットベース VLAN、プロトコルベース VLAN、マルチプル VLAN、Voice VLAN の各 VLAN に対応可能なこと。
8. IEEE 802.1AX-2008 に準拠した Link Aggregation (static and dynamic) 機能を有すること。
9. ポートミラーリング、リモートミラーリング機能を有すること。
10. DHCP クライアント機能を有すること。
11. IEEE 802.3af 準拠の PoE、および IEEE 802.3at 準拠の PoE+機能を持ったポートを 48 ポート以上搭載していること。
12. 1 ポートあたり 30W 以上、装置全体で 740W 以上の PoE 給電が可能であること。
13. 時刻同期を行うために NTP クライアント機能を有すること。
14. SNMP エージェント機能を有し、SNMPv1/v2c/v3 による管理が可能なこと。
15. Syslog サーバへログを転送できること。
16. 決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。
17. 装置内にファームウェアを複数保存可能なこと。

18. 19 インチラックに収容可能であること。
19. 動作時温度 0～45℃に対応していること。
20. 装置固有のベンダー定義 MIB が存在する場合にはその MIB 仕様を公開すること。

その他

1. 職員用セグメントは別途当調達で導入する認証装置にて MAC アドレス認証、及び 802.1x 認証が可能なこと。また、患者用セグメントは別途当調達で導入する認証システムで認証を行うこと。
2. 西神戸医療センターで使用する各ネットワークの設定を実施すること。また、西神戸医療センターで使用する VLAN を全ての導入機器に登録しておくこと。
3. 当調達で導入するネットワーク監視装置に登録し、死活確認をはじめトラフィックなど情報を収集するように設定すること。

(2) 無線アクセスポイント

機器の要件は以下を満たすこと。

1. 有線 LAN ポートを 2 ポート以上搭載し、本装置の配下にパソコンをカスケード接続可能であること。
2. 装置単体で 100/1000/2.5G/5GBASE-T のポートを 2 ポート以上搭載していること。
3. また、そのうち 1 ポート以上は IEEE 802.3at（Power over Ethernet +）に対応していること。
4. アンテナ形式が内蔵であること。
5. 最大接続台数が 1 ラジオにつき 500 台以上であること。
6. IEEE 802.1AX-2008 に準拠した Link Aggregation (static and dynamic) 機能を有すること。
7. Wi-Fi 規格及び IEEE 802.11a/802.11b/802.11g/802.11n/802.11ac/802.11ax に準拠していること。
8. IEEE 802.11k（Radio Resource Measurement of Wireless LANs)、IEEE 802.11r（Fast Basic Service Set Transition)、IEEE 802.11v（Basic Service Set Transition Management Frames）に準拠した Fast Roaming に対応していること。
9. 2.4GHz/5GHz 帯の同時使用に対応していること。
10. 複数アクセスポイント間のブリッジ接続を行う WDS(Wireless Distribution System)機能を有すること。
11. エアタイムフェアネスに対応していること。
12. IEEE 802.11ac Wave2 以降に対応した送信ビームフォーミングに対応していること。
13. SSID をブロードキャストするか否か（SSID 隠蔽）を設定する機能を有すること。
14. 無線端末間通信禁止機能を有すること。
15. 隣接アクセスポイントの検出機能を有すること。
16. 周囲の電波状況を考慮し、無線端末に対して混雑していない帯域への接続を促すバン

ドステアリング機能を有すること。

17. 上りと下りの OFDMA に対応し、複数の無線クライアントへの同時送信や複数の無線クライアントからの同時受信が可能なこと。
18. アクセスポイント 1 台で仮想的なアクセスポイントを、2.4GHz 帯・5GH z 帯ごとに最大で 15 個動作させる機能を有すること。また仮想的なアクセスポイントごとに SSID とセキュリティの設定を行うことや異なる VLAN を関連付けることができること。
19. スマートフォンやタブレットから容易に無線接続出来るための、無線設定情報を含む QR コードを生成可能であること
20. SSID ごとに利用する RADIUS サーバを自由に指定できること。
21. IEEE 802.1X 認証に対応し、EAP-TLS / EAP-TTLS / MSCHAPv2 / PEAPv0 /EAP-MSCHAPv2 / PEAPv1 / EAP-GTC / EAP-FAST 方式が使用可能なこと。
22. 認証方式としてオープンシステム認証、共有キー認証、WPA パーソナル、WPA エンタープライズが利用可能であること。
23. キャプティブポータルによる Web 認証を有すること。
24. 認証時に、ユーザー（無線クライアント）が所属する VLAN を動的に割当てる機能を有すること。
25. 暗号化機能として WPA/WPA2(TKIP/CCMP)、WPA3(CCMP/GCMP)が利用可能であること。
26. MAC アドレスフィルタリングが 2,048 以上設定可能なこと。また、CSV からのインポートやダッシュボードからのインポートが可能なこと。
27. IEEE 802.1Q に準拠した VLAN が設定可能なこと。
28. 無線の利用状態を収集して、常に最適な電波出力とチャンネルを分析しアクセスポイントへ適用する機能を持つ自律型無線 LAN コントローラにて管理ができること。
29. 自律型無線 LAN コントローラ離脱時でも無線サービスの提供を継続できること。
30. 時刻同期を行うために NTP クライアント機能を有すること。
31. SNMP エージェント機能を有し、SNMPv1/v2c/v3 による管理が可能なこと。
32. Syslog サーバへログを転送できること。
33. 日本語 Web GUI （HTTP/HTTPS） に対応していること。
34. 設定により LED を常時消灯させる機能を有すること。
35. PoE スイッチと AC アダプターの両方を同時に接続することにより、電源の冗長化が可能なこと。
36. 最大消費電力が 30W 以下であること。
37. 天井・壁にレイアウト可能な専用のブラケットに対応していること。
38. 環境温度 0~40℃に対応していること。
39. 日本語マニュアルをインターネット上に公開していること。
40. 装置固有のベンダー定義 MIB が存在する場合にはその MIB 仕様を公開すること。

その他

1. 職員用セグメントは別途当調達で導入する認証装置にて MAC アドレス認証、及び

802.1x 認証が可能なこと。また、患者用セグメントは別途当調達で導入する認証システムで認証を行うこと。

2. 天井または壁に取り付けるために必要な取付板やビス（アンカー）も含めること。また、取付作業も実施すること。
3. 無線 LAN コントローラと連携し、無線アクセスポイントの状態が把握できること。それに必要な設定を実施すること。
4. コントローラ内蔵型の無線アクセスポイントも可とする。
5. 取り付け位置は既設 AP と同じ位置に設置すること（切替に際して並行して設置する必要が有る場合は病院側と協議することは可とする）

(3) コアスイッチ（L3 スイッチ）

以下の機能を満たすこと。

1. 装置単体で 1000/2.5G/5G/10GBASE-T のインターフェースを 8 ポート有すること。
2. 装置単体で SFP/SFP+スロットを 8 つ以上有すること。
3. 装置単体で QSFP+スロットを 2 つ以上有すること。
4. IEEE 802.3z 1000BASE-LX/SX、IEEE 802.3ab 1000BASE-T に準拠した SFP を搭載可能なこと。
5. IEEE 802.3ae 10GBASE-ER/LR/SR 、 IEEE 802.3an 10GBASE-T に準拠した SFP+(Small Form-factor Pluggable+)を搭載可能なこと。
6. IEEE 802.3bz 2.5GBASE-T/5GBASE-T に準拠した SFP+(Small Form-factor Pluggable+)を搭載可能なこと。
7. IEEE 802.3ba 40GBASE-CR4/SR4/LR4/ER4 に準拠した QSFP+を搭載可能なこと。
8. 装置単体でスイッチングファブリックは 488Gbps 以上であること。
9. 装置単体で MAC アドレス登録数は 16,384 以上であること。
10. 装置単体で IEEE 802.1Q に準拠した 4,094 以上の VLAN を設定可能なこと。
11. VLAN の種類として、ポートベース VLAN、IEEE 802.1Q タグベース VLAN、IP サブネットベース VLAN、プロトコルベース VLAN、マルチプル VLAN、Voice VLAN の各 VLAN に対応可能なこと。
12. IEEE 802.1AX-2008 に準拠した Link Aggregation (static and dynamic) 機能を有すること。
13. ポートミラーリング、リモートミラーリング機能を有すること。
14. ソフトウェアを変更することなく、スタティックルーティング、RIPv1/v2、RIPng、OSPFv2、OSPFv3、PIM-SSMv4、PIM-SMv4、PIM-DMv4、PIM-SSMv6、PIM-SMv6 機能を有すること。(但しライセンス適用は可とする)
15. DHCP サーバ機能を有すること。
16. DHCP リレー機能を有すること。
17. スタックケーブルで機器間(最大 4 台)を接続することにより、仮想的に 1 台の装置と

して扱うことができる、スタック機能(以下、スタック)を有すること。

18. スタック接続されている装置間では、コンフィグ、FDB、ARP テーブル、IP ルーティングテーブル等の各種情報を同期することが可能なこと。
19. スタック接続した際は装置間の帯域を 160Gbps（双方向）以上有すること。
20. スタックケーブルやスタックポートに障害が発生し、スタックが分断されマスターが複数存在する構成となった場合に、一方のスイッチのスイッチポートを無効化する機能を有すること。
21. 特殊フレームの送受信によりループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせるなど設定した動作を自動実行可能なこと。
22. ループを検知したポート LED の点滅と全てのポート LED の点滅を繰り返すことで、ループ検知を視覚的に知らせる機能を有すること。
23. Telnet（クライアント/サーバ）機能および Secure Shell（クライアント/サーバ）機能を有すること。
24. 時刻同期を行うために NTP(クライアント/サーバ)機能を有すること。また他の NTP サーバに同期していない場合であっても、装置単体で権威のある NTP サーバとして動作することが可能なこと。
25. SNMP エージェント機能を有し、SNMPv1/v2c/v3 による管理が可能なこと。
26. Syslog サーバへログを転送できること。
27. 外部メディア（USB メモリ）へログを転送できること
28. 決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。
29. USB メモリにファームウェアやコンフィグファイルを直接アップロード/ダウンロード可能なこと。
30. 短時間でリンクダウン/アップを繰り返すポートフラッピング現象を検出し、当該ポートの自動シャットダウンが可能なこと。
31. 複数の設定ファイルを異なる名前で保存可能なこと。また、それらを必要に応じて切り替えて使用することが可能なこと。
32. 設定ファイルを直接編集するエディター機能を有すること。
33. 最大消費電力が 440W 以下であること。
34. 動作時温度 0～50℃に対応していること。
35. 装置前面に USB ポートおよびコンソールポートを各 1 つ以上有すること。
36. 日本語取扱説明書および日本語コマンドリファレンスをインターネット上に公開していること。
37. 装置固有のベンダー定義 MIB が存在する場合にはその MIB 仕様を公開すること。

その他

1. 職員用セグメントは別途当調達で導入する認証装置にて MAC アドレス認証、及び 802.1x 認証が可能なこと。また、患者用セグメントは当調達で導入する認証システムで認証を行うこと。

2. 西神戸医療センターで使用する各ネットワークの設定を実施すること。また、西神戸医療センターで使用する VLAN を全ての機器に登録しておくこと。
3. 当調達で導入するネットワーク監視装置に登録し、死活確認をはじめトラフィックなど情報を収集するように設定すること。

(4) サーバスイッチおよびフロアスイッチ（L２スイッチ）

以下の機能を満たすこと。

1. 装置単体で 10/100/1000BASE-T のインターフェースを 48 ポート以上有すること。
2. 装置単体で SFP スロットを 4 つ以上有すること。
3. IEEE 802.3z 1000BASE-LX/SX、IEEE 802.3ab 1000BASE-T、IEEE 802.3ah 1000BASE-BX10 に準拠した SFP を搭載可能なこと。
4. 装置単体でスイッチングファブリックは 336Gbps 以上であること。
5. 装置単体で MAC アドレス登録数は 16,384 以上であること。
6. 装置単体で IEEE 802.1Q に準拠した 4094 以上の VLAN を設定可能なこと。
7. VLAN の種類として、ポートベース VLAN、IEEE 802.1Q タグベース VLAN、IP サブネットベース VLAN、プロトコルベース VLAN、マルチプル VLAN、Voice VLAN の各 VLAN に対応可能なこと。
8. IEEE 802.1AX-2008 に準拠した Link Aggregation (static and dynamic) 機能を有すること。
9. ポートミラーリング、リモートミラーリング機能を有すること。
10. DHCP クライアント機能を有すること。
11. 時刻同期を行うために NTP クライアント機能を有すること。
12. SNMP エージェント機能を有し、SNMPv1/v2c/v3 による管理が可能なこと。
13. Syslog サーバへログを転送できること。
14. 決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。
15. TDR (Time-Domain Reflectometry) 方式のカッパーケーブル診断機能を有すること。
16. 最大消費電力が 54W 以下であること。
17. 19 インチラックに収容可能であること。
18. 動作時温度 0～45℃に対応していること。
19. 日本語取扱説明書および日本語コマンドリファレンスをインターネット上に公開していること。
20. 装置固有のベンダー定義 MIB が存在する場合にはその MIB 仕様を公開すること。

その他

1. 職員用セグメントは別途当調達で導入する認証装置にて MAC アドレス認証、及び 802.1x 認証が可能なこと。また、患者用セグメントは別途当調達で導入する認証システムで認証を行うこと。
2. 西神戸医療センターで使用する各ネットワークの設定を実施すること。また、西神戸医

療センターで使用する VLAN を全ての導入機器に登録しておくこと。

3. 当調達で導入するネットワーク監視装置に登録し、死活確認をはじめトラフィックなど情報を収集するように設定すること。

(5) 認証装置

職員用認証装置

1. 不正デバイス検知・ブロックシステムを設置し、西神戸医療センターで使用する VLAN 数に応じた設定が可能な機器を導入すること。
2. 特定の MAC アドレスの端末のみアクセスさせる機能を有すること。
3. 機器はアプライアンスまたはサーバとし、ラックマウント型とする。
4. 管理端末台数は 2000 台以上認証できること。
5. DHCP の機能または DHCP サーバと連携し、登録した MAC アドレスに対して自動で固定の IP アドレスを払い出す仕組みを有すること。
6. 管理外の不正デバイスが検知された際には管理者の通知が可能であること。また、管理外の不正デバイスをネットワークからの排除が可能なこと
7. 接続を許可する端末を一覧で表示可能なこと。また、端末情報を CSV 形式でダウンロード、アップロードが可能なこと
8. 冗長構成とし、故障発生時にも継続して動作可能なこと。
9. Web 認証画面は日本語に対応していること

患者用認証装置

1. 認証方式として、Web を利用したベーシック認証、管理者が提供する ID 認証、RADIUS 認証、メールアドレス認証、OpenID(SNS 連携)認証の認証方式等に対応すること。
2. 機器はアプライアンスまたはサーバとし、ラックマウント型とすること。
3. 持ち込み PC がネットワーク設定を変更することなく、患者サービス用ネットワークを利用することができる機能を提供すること
4. DHCP の機能または DHCP サーバと連携し、自動で IP アドレスを払い出す仕組みとすること。
5. 認証数は 1000 以上とすること。
6. 機器はラックマウント型とし、搭載可能なこと。
7. 接続時間や接続時間帯、接続期間設定が複数設定出来ること。
8. Web 認証画面は日本語に対応していること

その他

1. 当調達で導入するネットワーク監視装置に登録し、疎通確認をはじめトラフィックなど情報を収集するように設定すること。
2. 職員用認証装置は MAC アドレス認証、及び 802.1x 認証が可能なこと。

3. 職員用認証装置ではユーザごとに割り当てられたネットワーク以外には接続できない仕組みを導入すること。

(6) ルーター・ファイヤーウォール

職員用は以下の機能を満たすこと。

1. ハードウェアおよびソフトウェアが一体で提供されるアプライアンス製品であること
2. GbE RJ45 インターフェースを 18 ポート以上有すること。
3. GbE SFP インターフェースを 8 ポート以上有すること。
4. 10 GbE SFP+インターフェースを 4 ポート以上有すること。
5. シリアルコンソール用のインターフェースを 1 ポート有すること。
6. USB インターフェースを 1 ポート有すること。
7. ラックマウントに搭載可能でサイズは 1U 以内であること。
8. 重量は 4.5 kg 以下であること。
9. 最大消費電力は 120W 以下であること。
10. ファイアウォールスループットは UDP パケット 1518/512 バイトにおいて 27Gbps 以上、64 バイトにおいて 11Gbps 以上であること。
11. ファイアウォール同時セッション(TCP)は 3,000,000 セッション以上であること。
12. ファイアウォール新規セッション(TCP)は 280,000/秒以上であること。
13. ファイアウォールポリシー数は 10,000 以上であること。
14. ステートフルファイアウォールによる通信制御が可能なこと。
15. SSL-VPN 機能が搭載されていること。
16. バーチャルファイアウォール（仮想システム）に追加料金なしで最大 10 システムまで対応可能なこと。
17. セキュリティ機能として通信に対する、アンチウイルス、IPS、アンチスパム、Web フィルタ、アプリケーション制御に対応していること。
18. アンチウイルスはプロキシモードとフローベースモードの方式に対応可能なこと。
19. アンチスパムは SMTP/POP3/IMAP に対応可能なこと。
20. WebUI、CLI から設定管理が可能なこと。
21. WebUI は日本語に対応可能なこと。
22. 19 インチラックに収容可能であること。
23. ログの保存を安全性の高いクラウドに自動保存できること。
24. クラウド上のログは 1 年以上保存できること。

患者用は以下の要件を満たすこと。

1. ハードウェアおよびソフトウェアが一体で提供されるアプライアンス製品であること
2. GbE RJ45 インターフェースを 18 ポート以上有すること。
3. GbE SFP インターフェースを 4 ポート以上有すること。
4. GbE RJ45 / SFP 共有メディアペアを 4 ポート以上有すること。

5. 10 GbE SFP+インターフェースを 2 ポート以上有すること。
6. シリアルコンソール用のインターフェースを 1 ポート有すること。
7. USB インターフェースを 1 ポート有すること。
8. ラックマウントに搭載可能でサイズは 1U 以内であること。
9. 重量は 3.29 kg 以下であること。
10. 最大消費電力は 40W 以下であること。
11. ファイアウォールスループットは UDP パケット 1518 バイトにおいて 20Gbps 以上、512 バイトにおいて 18Gbps 以上、64 バイトにおいて 10Gbps 以上であること。
12. ファイアウォール同時セッション(TCP)は 1,500,000 セッション以上であること。
13. ファイアウォール新規セッション(TCP)は 56,000/秒以上であること。
14. ファイアウォールポリシー数は 10,000 以上であること。
15. ステートフルファイアウォールによる通信制御が可能なこと。
16. SSL-VPN 機能が搭載されていること。
17. バーチャルファイアウォール（仮想システム）に追加料金なしで最大 10 システムまで対応可能なこと。
18. アンチウイルス、IPS、アンチスパム、Web フィルタ、アプリケーション制御に対応していること。
19. アンチウイルスはプロキシモードとフローベースモードの方式に対応可能なこと。
20. アンチスパムは SMTP/POP3/IMAP に対応可能なこと。
21. WebUI、CLI から設定管理が可能なこと。
22. WebUI は日本語に対応可能なこと。
23. 19 インチラックに収容可能であること。
24. ログの保存を安全性の高いクラウドに自動保存できること。
25. クラウド上のログは 1 年以上保存できること。

遠隔監視用は以下の要件を満たすこと。

1. 保守ベンダー以外が利用できないように認証等の仕組みを用意すること。
2. 導入ネットワーク機器メーカーが提供している保守窓口にて常時監視・リモート切り分けが実施できること。
3. 保守回線から院内の端末が参照できないように、専用の管理セグメントを用意すること。
4. 当調達で導入するネットワーク監視装置に登録し、疎通確認をはじめトラフィックなど情報を収集するように設定すること。
5. VPN ルータは、西神戸医療センター並びに保守ベンダーの施設内に設置すること。
6. 遠隔保守用回線は､IP-VPN または広域イーサネット､SD-WAN などを利用すること。
7. リモートメンテナンスにおいて障害等により機器のログ解析/収集が必要となった場合、項番 7.2（1）、（2）、（3）、（4）で導入したメーカーが直接実施すること。

8. 前項 7 .の調査結果について状況・改善内容において当院に報告できること。さらに、受注業者においては、本内容を元に当院の改善をすること。
9. リモートメンテナンスにおいては、24 時間 365 日、本調達で導入したメーカーへのエスカレーションを当院にて実施できること。また、同時に当院が受注業者への問い合わせも 24 時間 365 日できること。
10. 回線契約並びに、回線工事に関する作業を当調達に含めること。

(7) 外部との通信回線

職員用および患者用の通信回線は、既存の回線を流用すること。ただし、遠隔保守用回線は受託者が準備すること。

・ 遠隔保守用回線

遠隔保守用通信回線費用は 5 年間の保守契約に含めること。

(8) 無線 LAN コントローラ

以下の機能を満たすこと。

1. 無線アクセスポイントの設定一元管理機能を有すること。
2. 無線アクセスポイントの設定一元管理機能を有し、状態監視が可能なこと。
3. 無線アクセスポイントの通信制御機能を有すること。
4. 機器や認証によるログを閲覧可能なこと。
5. 有線 LAN ポートは、1000BASE-T 対応であること。
6. SNMP に対応していること。
7. 受託者が調達するアクセスポイントの台数を収容可能なこと。

その他

1. 機器を導入する場合は、アプライアンスまたはサーバとし、ラックマウント型とすること。ただし、サービス提供型により一元管理する場合はその限りではないが、無線アクセスポイントの状態を機構内から閲覧できること。
2. 当調達で導入するネットワーク監視装置に登録し、疎通確認をはじめトラフィックなど情報を収集するように設定すること。

(9) ネットワーク機器監視

無線アクセスポイントおよびネットワーク機器の監視は、機構内から把握できる仕組みを有し、当調達で導入するネットワーク監視装置に登録し、以下の機能を満たすこと。

1. 当調達で導入したネットワーク機器を一元的に行えること。
2. 200 台以上の機器を監視できること。
3. 標準的なネットワーク管理プロトコル（SNMP、trap など）に対応していること。
4. 標準 MIB-2 とエンタープライズ MIB に対応していること。
5. 死活監視のタイミングを任意のタイミングで実効できること。

6. ソフトウェアをアップデートする機能を有し、バージョンアップができること。
7. WEB インターフェース機能を有し、GUI での操作が可能なこと。
8. 管理画面を表示中でも障害時に情報表示を行う機能を有すること。
9. 機器のデータを収集・蓄積し、グラフ表示が可能なこと。
10. ツリー上の監視対象と条件を指定することで、リアルタイム表示やトラフィック情報、状態チェックができる機能を有すること。
11. 管理サーバへのログインに使用するユーザ権限とユーザ種別が設定できること。また、ホストに対するアクセス権の設定ができること。
12. 障害時にメール等による通知ができること。
13. 障害通知の詳細情報は、ユーザで定義できること。
14. 管理機器のバックアップが可能なこと。
15. 帯域制限が可能なこと
16. 電波干渉検知可能なこと
17. 管理画面は日本語に対応していること。
18. アプリケーションの統計情報を取得できること。
19. スループット測定を行う機能を有すること
20. 無線コントローラ一体型でもかまわない

機器を導入する場合は、アプライアンスまたはサーバー（ラックマウント型）とし、ハードウェアの要件は以下を満たすこと。

1. アプライアンス機器を導入する場合は、下記の要件を満たすこと。

| | スペック |
|---|---|
| CPU | デュアルコア ARM プロセッサ　以上 |
| HDD | SSD 250GB 以上 |
| ネットワーク・インターフェース | 1000BASE-T×4 以上 |

2. サーバ機が必要な場合は、以下の要件を満たすこと。

| | スペック |
|---|---|
| OS | Linux 系 or Windows Server |
| CPU | Xeon 2GHz（デュアルコア）×1　以上 |
| メモリ | 32GB　以上 |
| HDD | 300GB　RAID1 以上 |
| サイズ | 2U 以内 |
| ネットワーク・インターフェース | 1000BASE-T×2 以上 |

(10) DNS サーバ

1. 西神戸医療センターにて稼働している機器と同等以上の機能を有する後継機種を DNS サーバとして 2 台接続すること。

2. レコード数は、プライマリ、セカンダリともに 5,000 以上であること。
3. DNS 性能は、23,000 クエリー/秒であること。
4. ゾーン数は、200 以上であること。
5. SNMP、NTP、Syslog 出力に対応していること。
6. 中央市民病院に設置している DNS サーバをセカンドとして参照出来るようにすること。
7. すべての操作は web 管理画面より日本語にて操作設定可能なこと。
8. アクセス先が危険・悪性サイトの場合は IP アドレスを応答しない機能を有すること。

(11) 無停電電源装置

1. 停電や落雷などの電源障害に対応できるように、導入機器に対し無停電電源装置を設置すること。
2. 本調達の機器でサーバ室のラックに搭載する機器をすべて収容できる容量の機器を選定すること。
3. 電源障害時には導入機器を安全に停止するように設定すること。
4. 常時インバータ給電方式を採用し、電源障害時にはラック内の機器に対し 5 分間以上の電源供給が行えること。

(12) その他

1. 無線 LAN コントローラやネットワーク監視装置を、監視センターにて一元管理する場合は、施設間の回線についても当調達に含めること。
2. ネットワーク機器は、管理用セグメントに配置し各ネットワークと分離すること。

# 8 保守

## 8.1 保守概要

当調達において導入したネットワーク機器を一元的に管理し、障害時の対応・問合せ窓口を用意すること。

## 8.2 保守条件

(1) 受付は、24 時間 365 日対応可能な窓口であること。(電話での受付)

(2) 機器の監視は 24 時間 365 日対応可能とし、障害を検知した場合は、導入する遠隔監視・操作システムにより状況を判断し、保守内容に応じて対応を行うこと。

(3) オンサイトは、受付後原則 3 時間以内に現場に到着させる体制であること。

(4) 以下の保守対象機器一覧の★印については、24 時間 365 日とすること。
また、☆印については、平日の 9 時から 1 7 時のオンサイト保守とする、もしくは

工場出荷状態の機器を設定することなく自動復旧ができる機能を有する場合はその限りではない。

無線アクセスポイント及び患者用認証装置については、先出センドバックとするが、予め交換が可能なように設定済みの予備機を受託者で準備しておくこと。

職員用認証装置については、冗長構成とするため先出センドバックも可とする。

(5) 本仕様書で新たに構築するシステムおよび配線・機器を保守対象とすること。

(6) ハード保守費及びライセンスは以下の表に基づき、5 年契約を契約すること。

(7) 5 年保守に対応した機器を導入すること。

また、使用するライセンスを含めて 5 年間追加費用が発生しないように本調達に含めること。

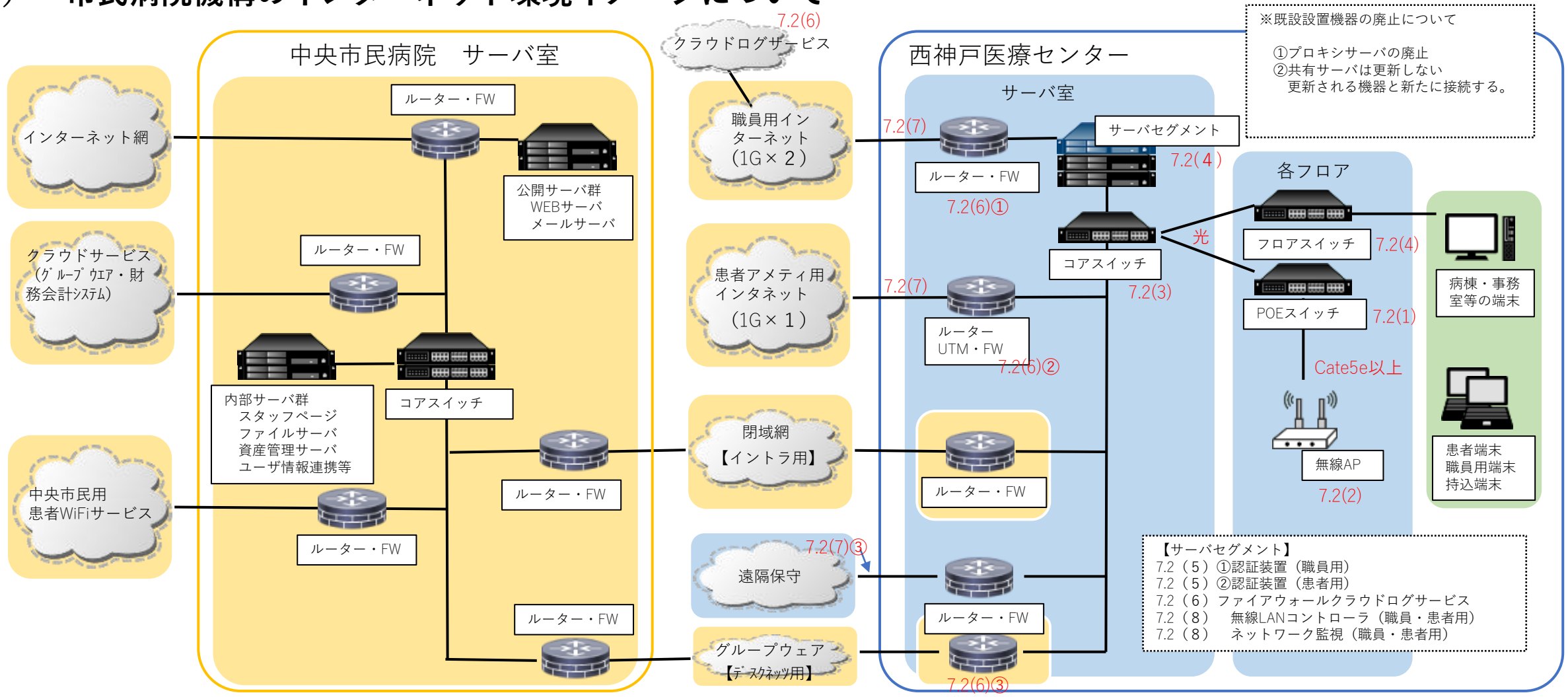
(8) サービス提供型の場合は、障害発生時に予め受託者が準備した予備機と入れ替え接続し、自動復旧できる場合、これらの限りではない。また、設定済みの予備機を受託者にて準備しておくこと。もしくは、障害発生時に、機器入れ替え接続のみで自動復旧可能であること。

**保守対象機器一覧**

| 項番 | 用途 | 用途 | 注 | | 備考 |
|---|---|---|---|---|---|
| 7.2(1) | PoE スイッチ | | ☆ | 平日の９時から１７時のオンサイト保守 | 機器を導入する場合<br>※サービス型の場合は利用料等が発生する場合は、提示すること |
| 7.2(2) | 無線 AP | | | 先出センドバックとするが、予め交換が可能なように設定済みの予備機を受託者で準備 | |
| 7.2(3) | コアスイッチ（L3） | | ★ | 24 時間 365 日 | |
| 7.2(4) | ｻｰﾊﾞｽｲｯﾁ・ﾌﾛｱｽｲｯﾁ（L2） | | ☆ | 平日の９時から１７時のオンサイト保守 | |
| 7.2(6) | ルータ・FW（職員用） | 職員用 | ★ | 24 時間 365 日 | |
| 7.2(6) | ルータ・FW（患者用） | 患者用 | ★ | 24 時間 365 日 | |
| 7.2(6) | ルータ・FW（遠隔監視用） | 遠隔監視用 | ☆ | 平日の９時から１７時のオンサイト保守 | |
| 7.2(5) | 認証装置 | 職員用 | | ・先出センドバックとするが、予め交換が可能なように設定済みの予備機を受託者で準備<br>・職員用認証装置については、冗長構成とするため先出センドバックも可 | |
| 7.2(5) | 認証装置 | 患者用 | | | |
| 7.2(8) | 無線コントローラ | 職員用・患者用 | ☆ | 平日の９時から１７時のオンサイト保守 | |
| 7.2(9) | ネットワーク監視装置 | 職員用・患者用 | ☆ | | |
| 7.2(10) | DNS サーバ | 職員用 | ☆ | | ※中央市民病院にある DNS サーバは保守対象外 |
| 7.2(11) | 無停電電源装置 | 職員用・患者用 | ☆ | オンサイト保証付きモデル | |

以上

# （1）　市民病院機構のインターネット環境イメージについて




◆西神戸から中央へ
- ■ 中央の内部・公開サーバ群、クラウドサービスに対し通信させる。メールは閉域網を使って送受信する
- ■ クライアント用セュリティパターンファイルは、各施設のインターネットから取得

◆中央から西神戸へ
- ■ 西神戸のサーバセグメント、ネットワーク機器に対し、管理セグメントを利用して通信させる。

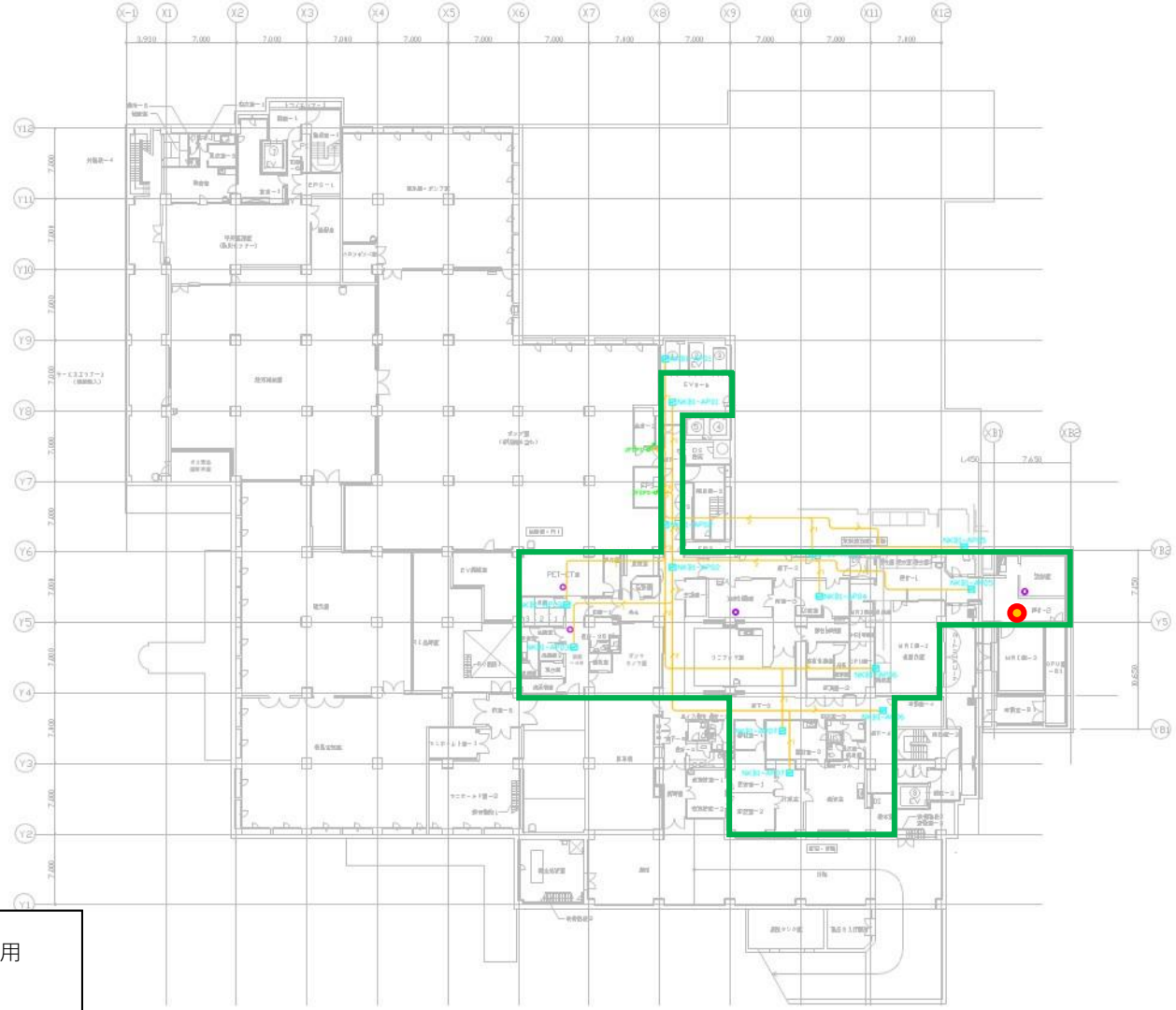
◆ 調達範囲および各機器の設定については、以下の色分けにて確認すること

青色： 受託者の調達範囲及び設定範囲

黄色：既存ベンダーが、必要な機器に対して設定変更を行う

※　既存機器の設定変更および新規に調達する機器の設定が、その調達範囲をまたぐ場合は相互に協力し作業を進めること。

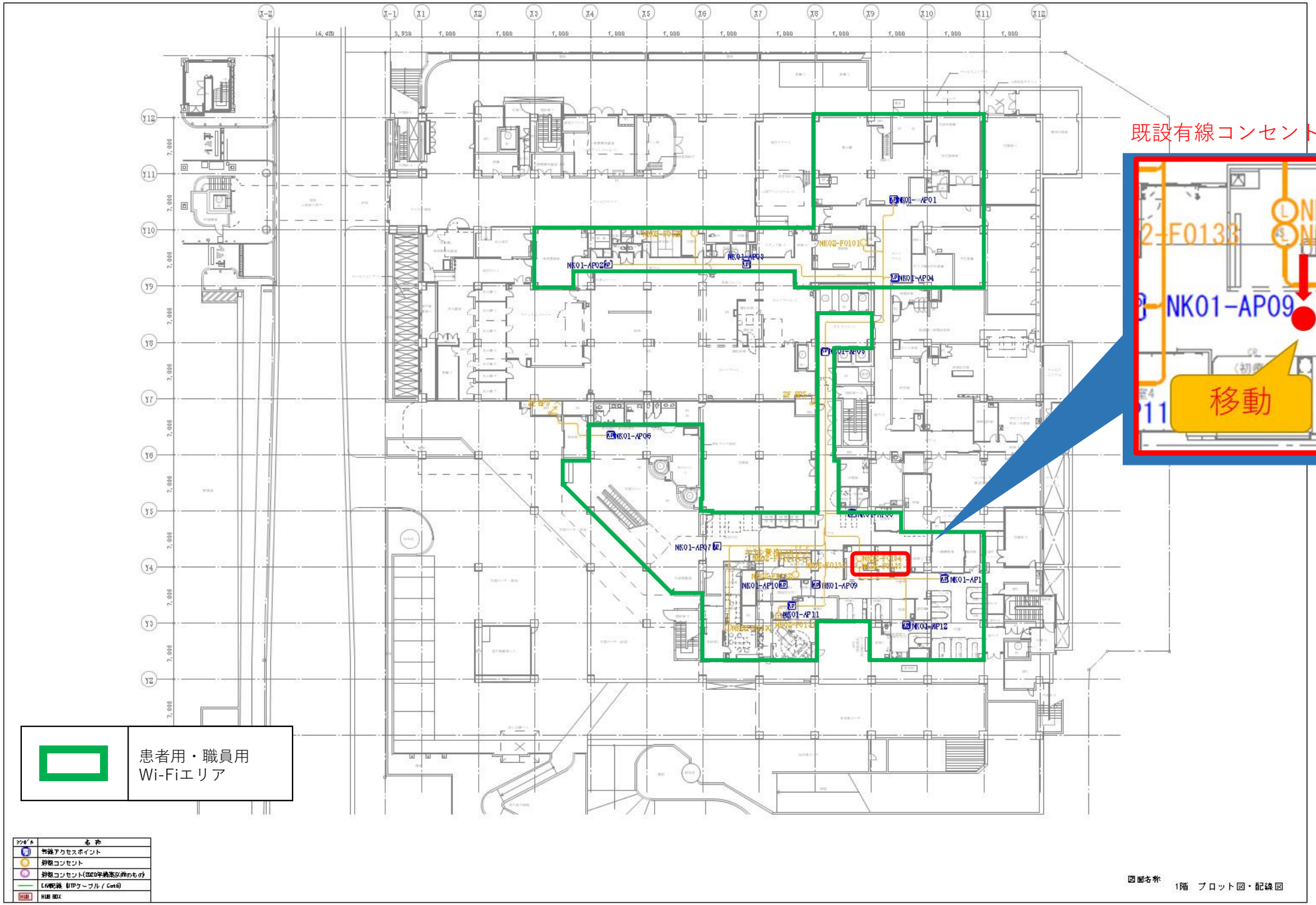
神戸市立西神戸医療センターネットワーク基盤更新業務仕様書【別紙１】ネットワーク整備図面

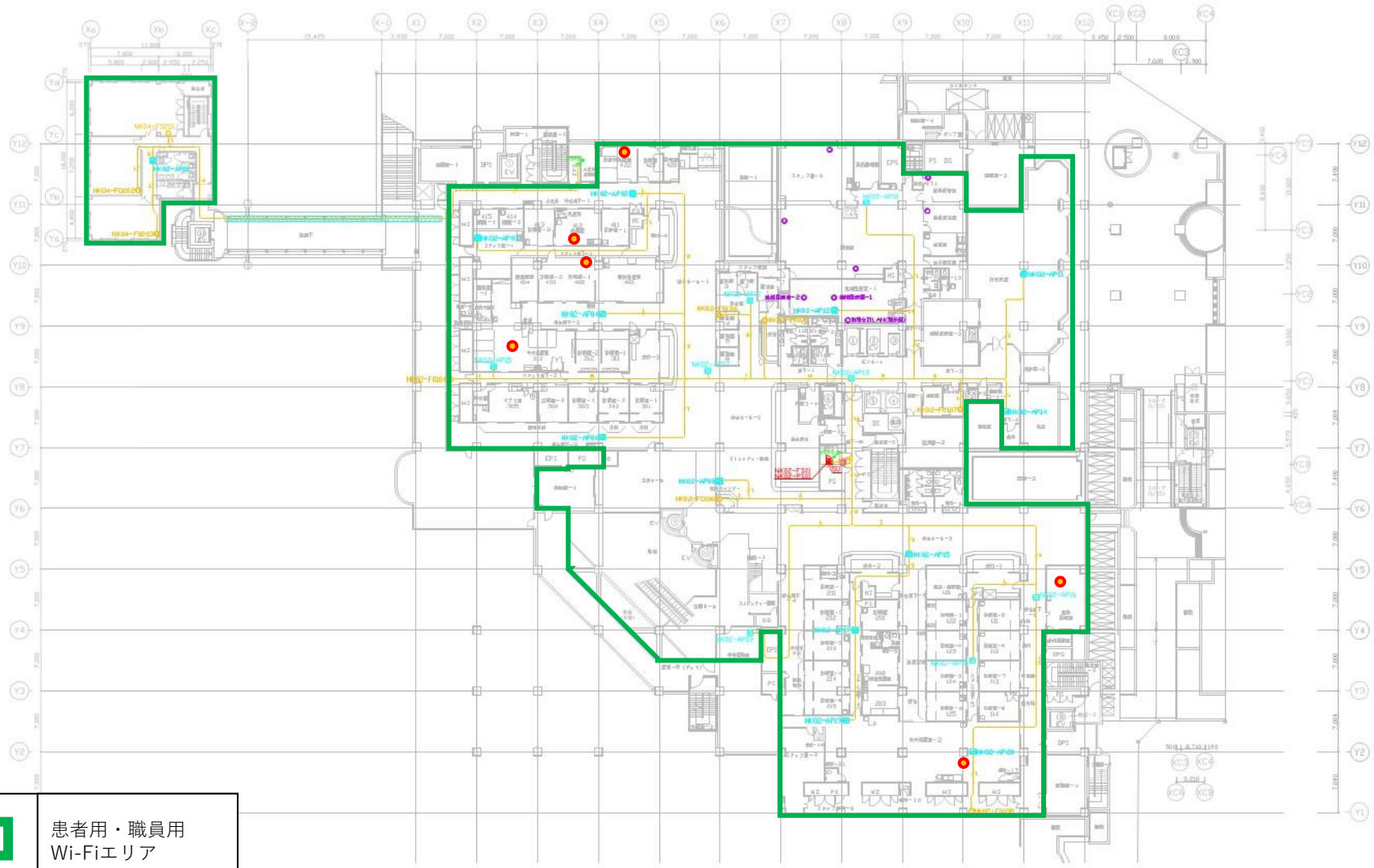


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |
| | 有線コンセント追加<br>（１箇所） |

| 記号 | 名称 | 記号 | 名称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント（埋込み型） | | 屋外用壁面 PF20 |
| | 既存 情報コンセント（埋込み型） | | HUBボックス |
| | 新規 情報コンセント（露出型） | | LAN配線（UTPケーブル/Cat6） |
| | 既存 情報コンセント（露出型） | | 光配線（光ケーブル / OM3 G1 8C） |
| | 立上りルート | | 絶体貫通部 |
| | 引下げルート | | |

図面名称　地下1階　配線図


既設有線コンセントの移動（2箇所）
NK02-F0134
NK02-F0135
NK01-AP09
移動
患者用・職員用
Wi-Fiエリア
図面名称
1階　プロット図・配線図

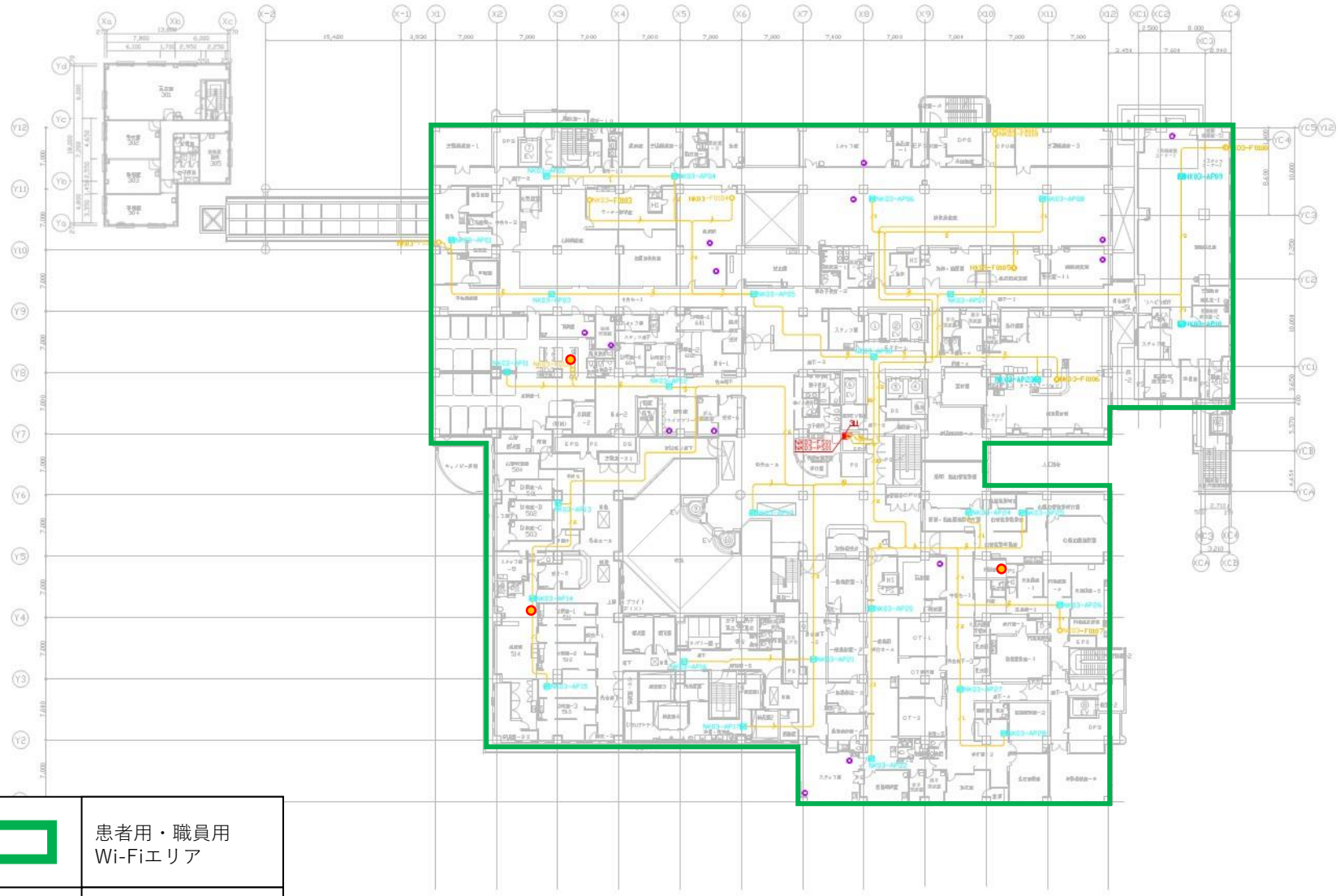


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |
| | 有線コンセント追加<br>（６箇所） |

情報通信配管凡例

| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント [埋込みﾀｲﾌﾟ] | | 屋外用警報 PF28 |
| | 既存 情報コンセント [埋込みﾀｲﾌﾟ] | | HUBボックス |
| | 新規 情報コンセント [露出ﾀｲﾌﾟ] | | LAN配線 [UTPケーブル/Cat5] |
| | 既存 情報コンセント [露出ﾀｲﾌﾟ] | | 光配線 [光ケーブル / OM3 G1 8C] |
| | 立上りルート | | 避雷突針 |
| | 引下げルート | | |

図面名称　2階　配線図

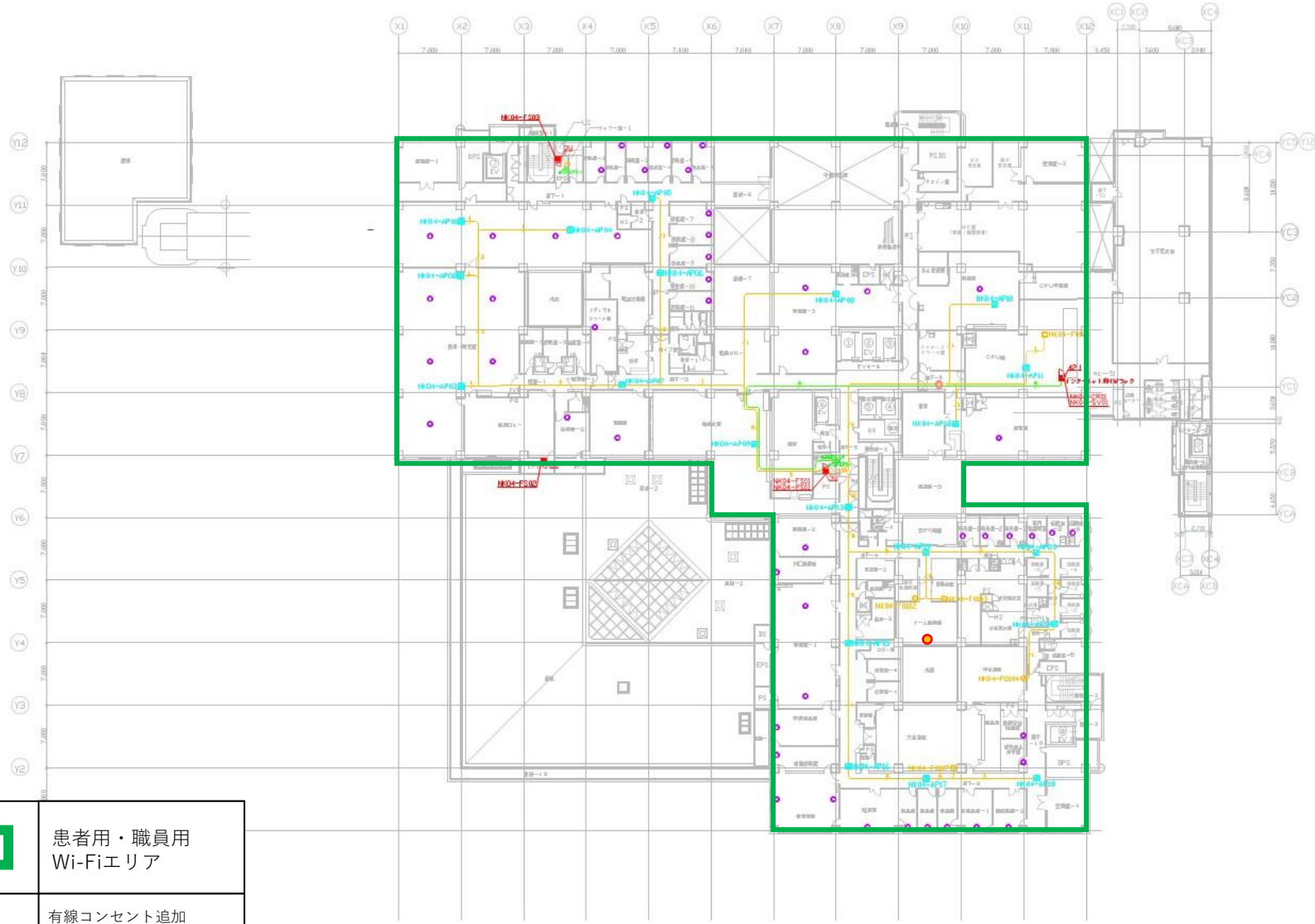


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |
| | 有線コンセント追加<br>（３箇所） |

情報通信配管凡例

| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配管 |
| | 新規 情報コンセント［埋込みﾀｲﾌﾟ］ | | 露出用金属 PF28 |
| | 既存 情報コンセント［埋込みﾀｲﾌﾟ］ | | HUBボックス |
| | 新規 情報コンセント［露出ﾀｲﾌﾟ］ | | LAN配線［UTPケーブル/Cat5］ |
| | 既存 情報コンセント［露出ﾀｲﾌﾟ］ | | 光配線［光ケーブル / OW3 G1 8C］ |
| | 立上りルート | | 磁性表示体 |
| | 引下げルート | | |

図面名称　3階　配線図

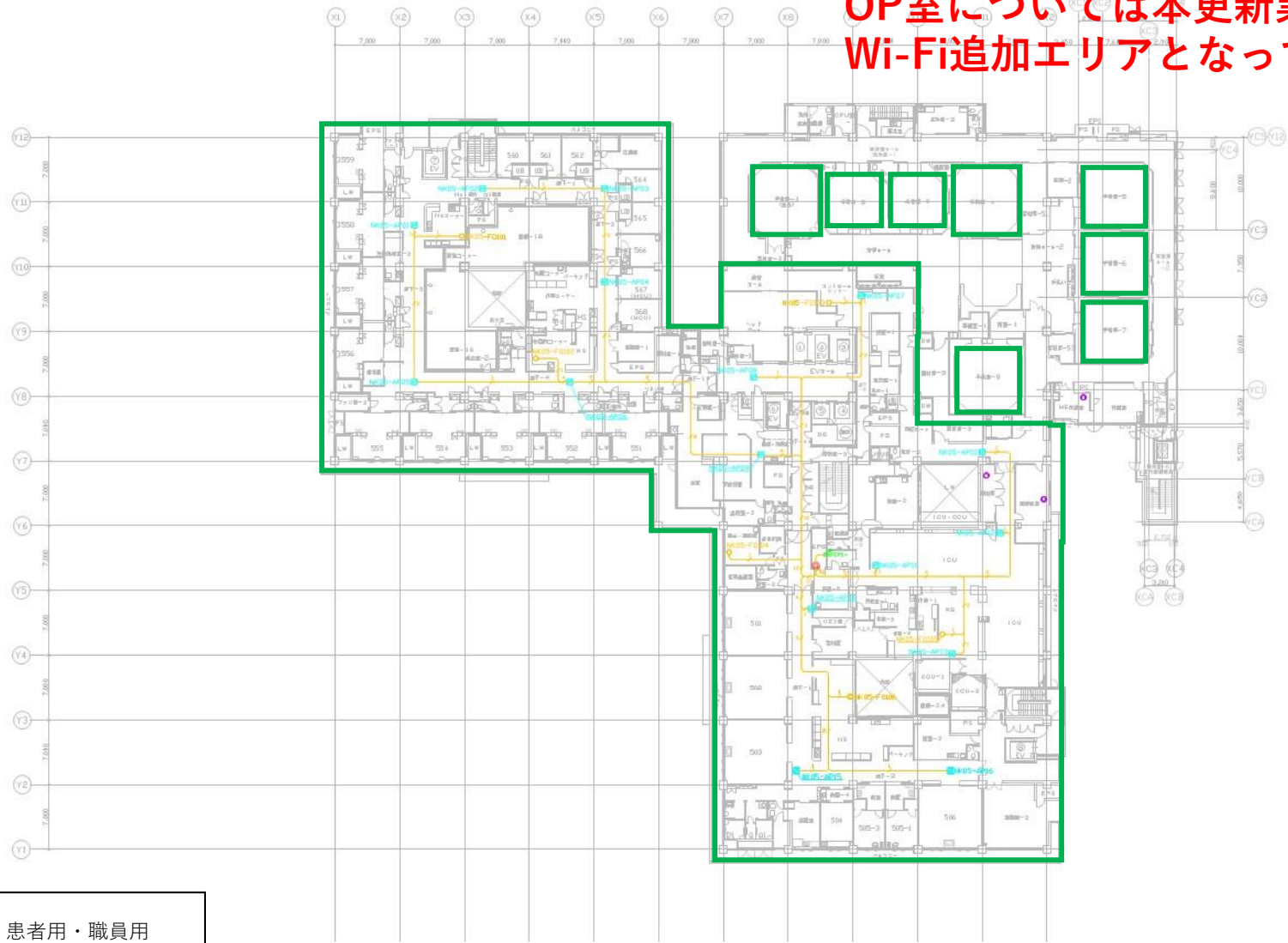


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |
| | 有線コンセント追加<br>（１箇所） |

| 記号 | 名称 | 記号 | 名称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント［埋込み型］ | | 屋外用装置 PF28 |
| | 既存 情報コンセント［埋込み型］ | | HUBボックス |
| | 新規 情報コンセント［露出型］ | | LAN配線［UTPケーブル/Cat5e］ |
| | 既存 情報コンセント［露出型］ | | 光配線［光ケーブル / OM3 G1 8C］ |
| | 立上りルート | | 避雷突針 |
| | 引下げルート | | |

図面名称　4階　配線図

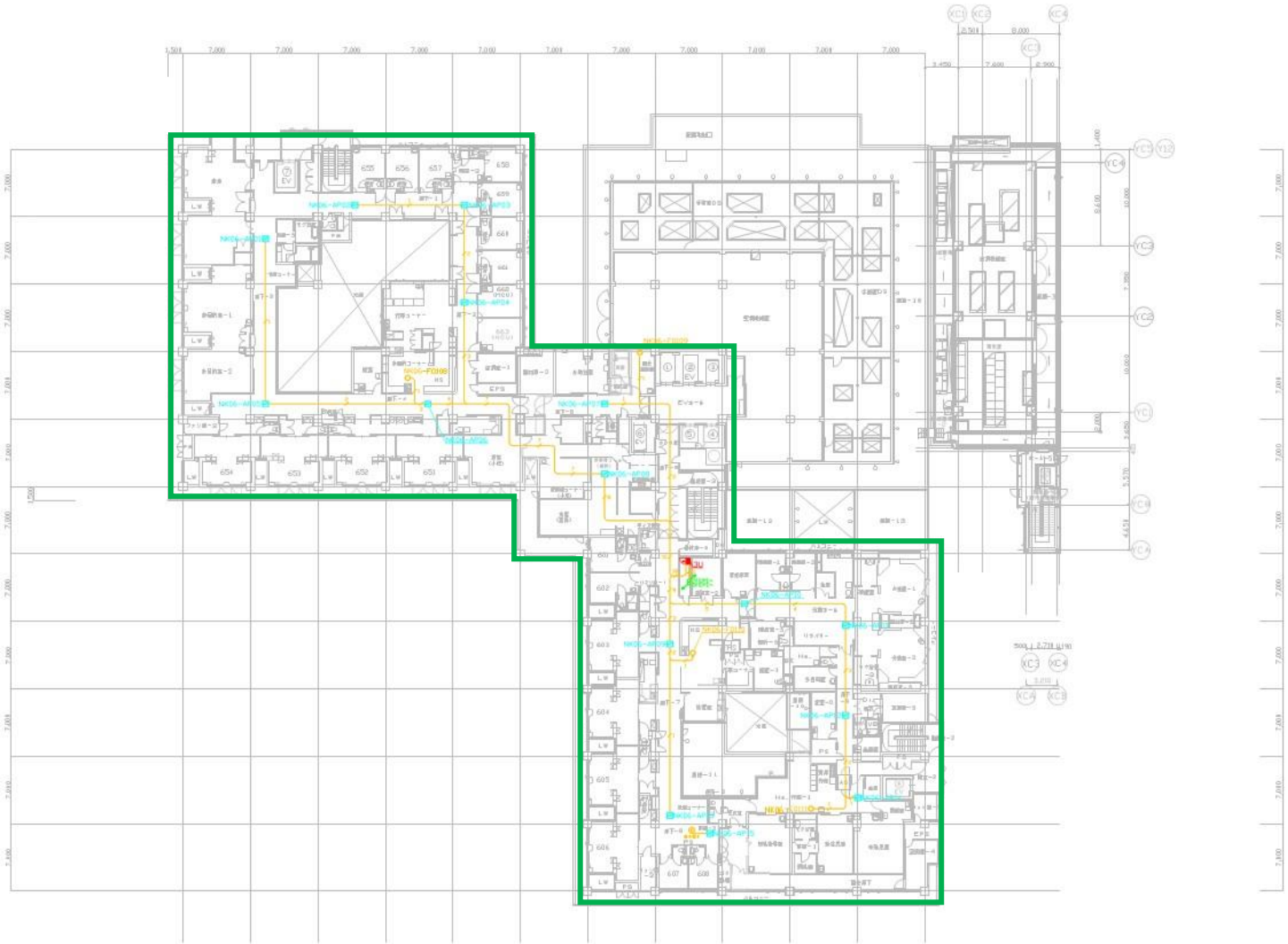
**OP室については本更新業務にて**
**Wi-Fi追加エリアとなっています**



| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |

| 情報通信記号凡例 | | | |
|---|---|---|---|
| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント（埋込み型） | | 屋外用電話 PF28 |
| | 既存 情報コンセント（埋込み型） | | HUBボックス |
| | 新規 情報コンセント（露出型） | | LAN配線（UTPケーブル/Cat5E） |
| | 既存 情報コンセント（露出型） | | 光配線（光ケーブル / OM3 G1 8C） |
| | 立上りルート | | 絶縁貫通部 |
| | 引下げルート | | |

図面名称　5階　配線図

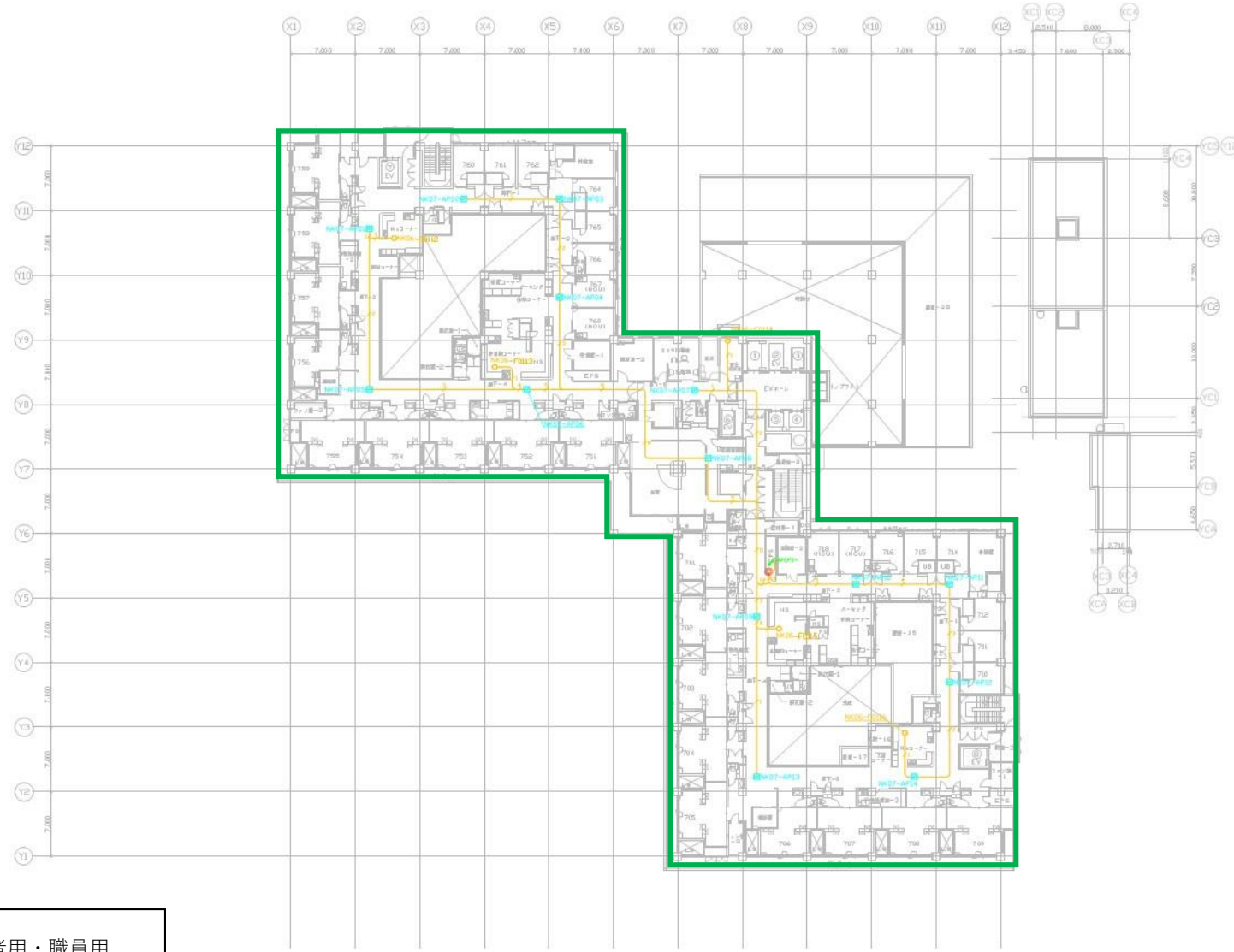


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |

情報通信配管凡例図

| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント [埋込み型] | | 屋外用露器 PF28 |
| | 既存 情報コンセント [埋込み型] | | HUBボックス |
| | 新規 情報コンセント [露出型] | | LAN配線 [UTPケーブル/Cat5] |
| | 既存 情報コンセント [露出型] | | 光配線 [光ケーブル / OM3 G1 8C] |
| | 立上りルート | | 絶縁貫通孔 |
| | 引下げルート | | |

図面名称　8階　配線図

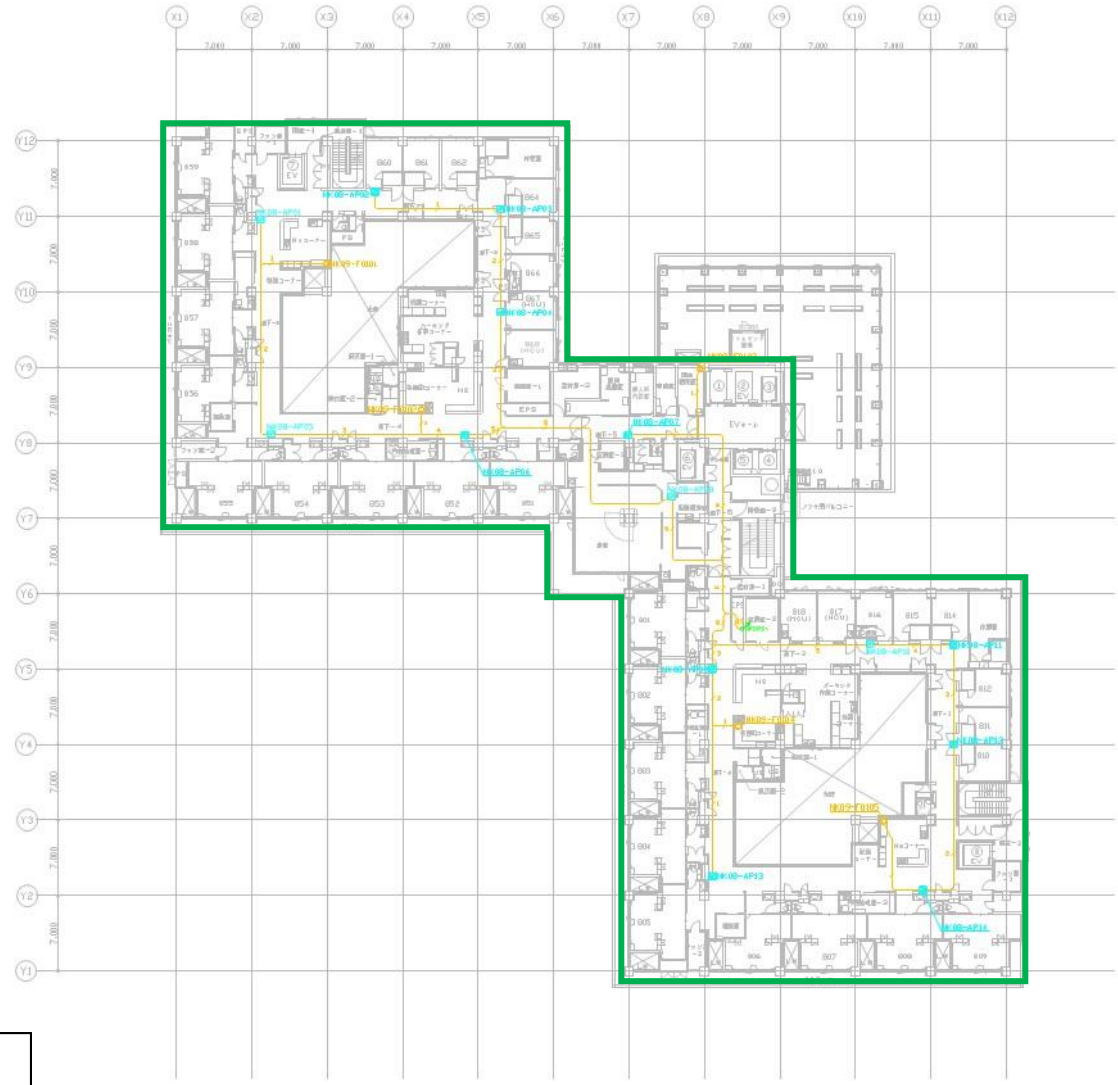


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |

情報通信配管凡例

| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配管 |
| | 新設 情報コンセント（埋込み型） | | 屋外用電線 PF28 |
| | 既存 情報コンセント（埋込み型） | | HUBボックス |
| | 新設 情報コンセント（露出型） | | LAN配線（UTPケーブル/Cat5E） |
| | 既存 情報コンセント（露出型） | | 光配線（光ケーブル / OM3 G1 8C） |
| | 立上りルート | | 絶縁貫通孔 |
| | 引下げルート | | |

図面名称　7階　配線図

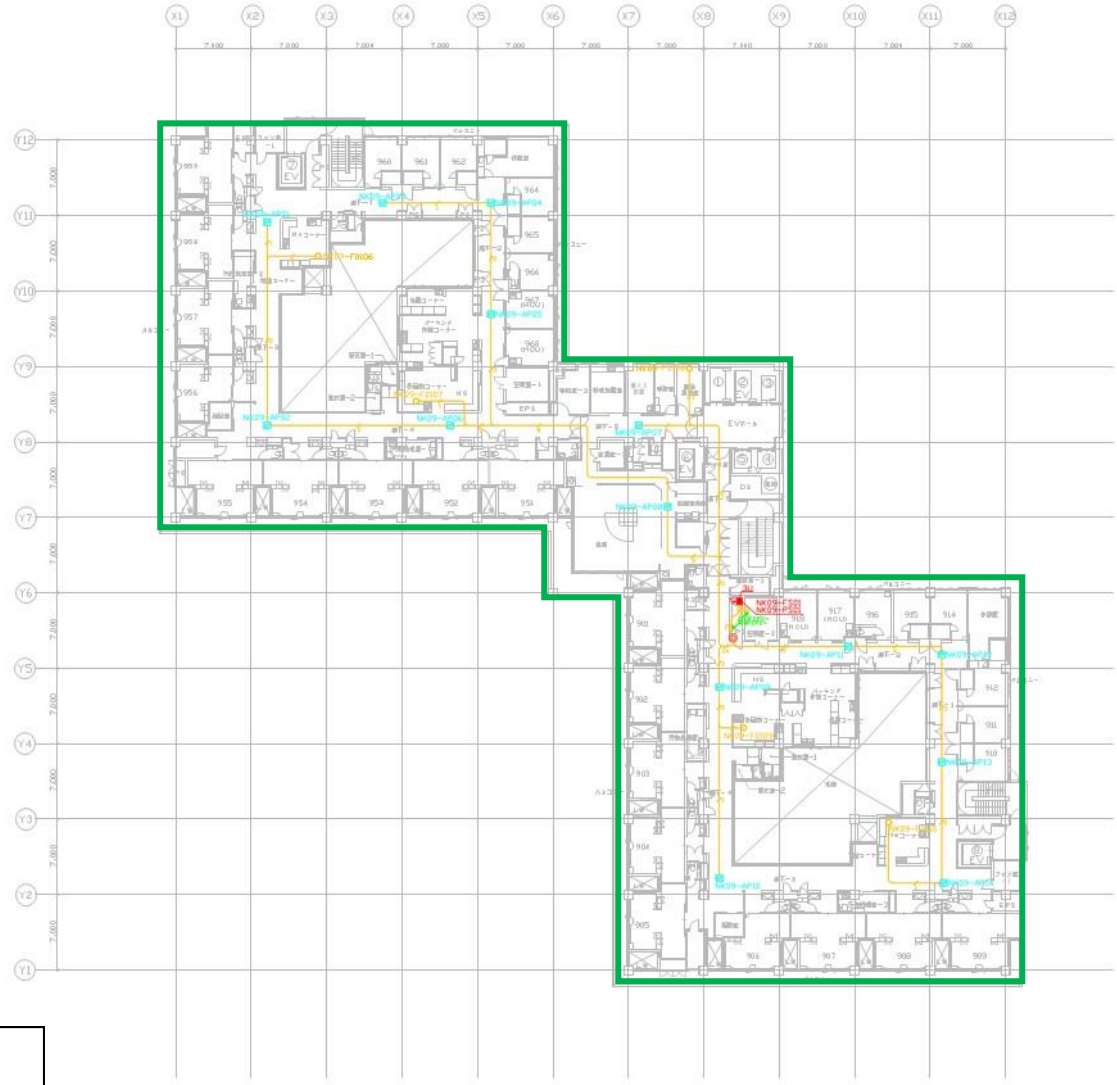


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |

情報通信配管凡例

| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント（埋込み型） | | 屋外用電路 PF28 |
| | 既存 情報コンセント（埋込み型） | | HUBボックス |
| | 新規 情報コンセント（露出型） | | LAN配線（UTPケーブル/Cat5） |
| | 既存 情報コンセント（露出型） | | 光配線（光ケーブル / OW3 G1 8C） |
| | 立上りルート | | 絶縁貫通孔 |
| | 引下げルート | | |

図面名称　8階　配線図

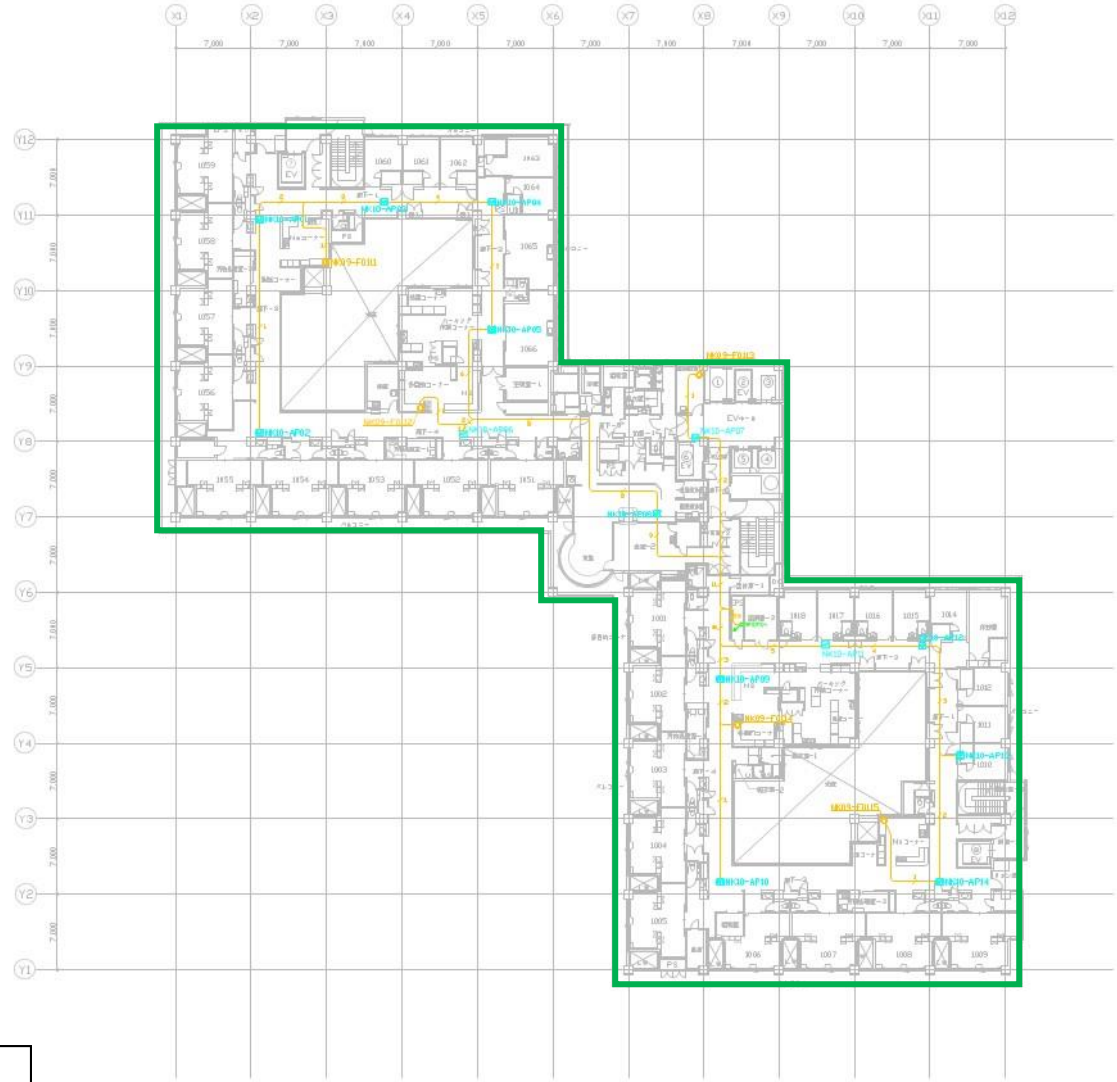


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |

情報表種記号凡例用

| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント（埋込み型） | | 屋外用壁面 PF2G |
| | 既存 情報コンセント（埋込み型） | | HUBボックス |
| | 新規 情報コンセント（露出型） | | LAN配線（UTPケーブル/Cat5E） |
| | 既存 情報コンセント（露出型） | | 光配線（光ケーブル / OM3 G1 8C） |
| | 立上りルート | | 絶縁貫通金 |
| | 引下げルート | | |

図面名称　9階　配線図

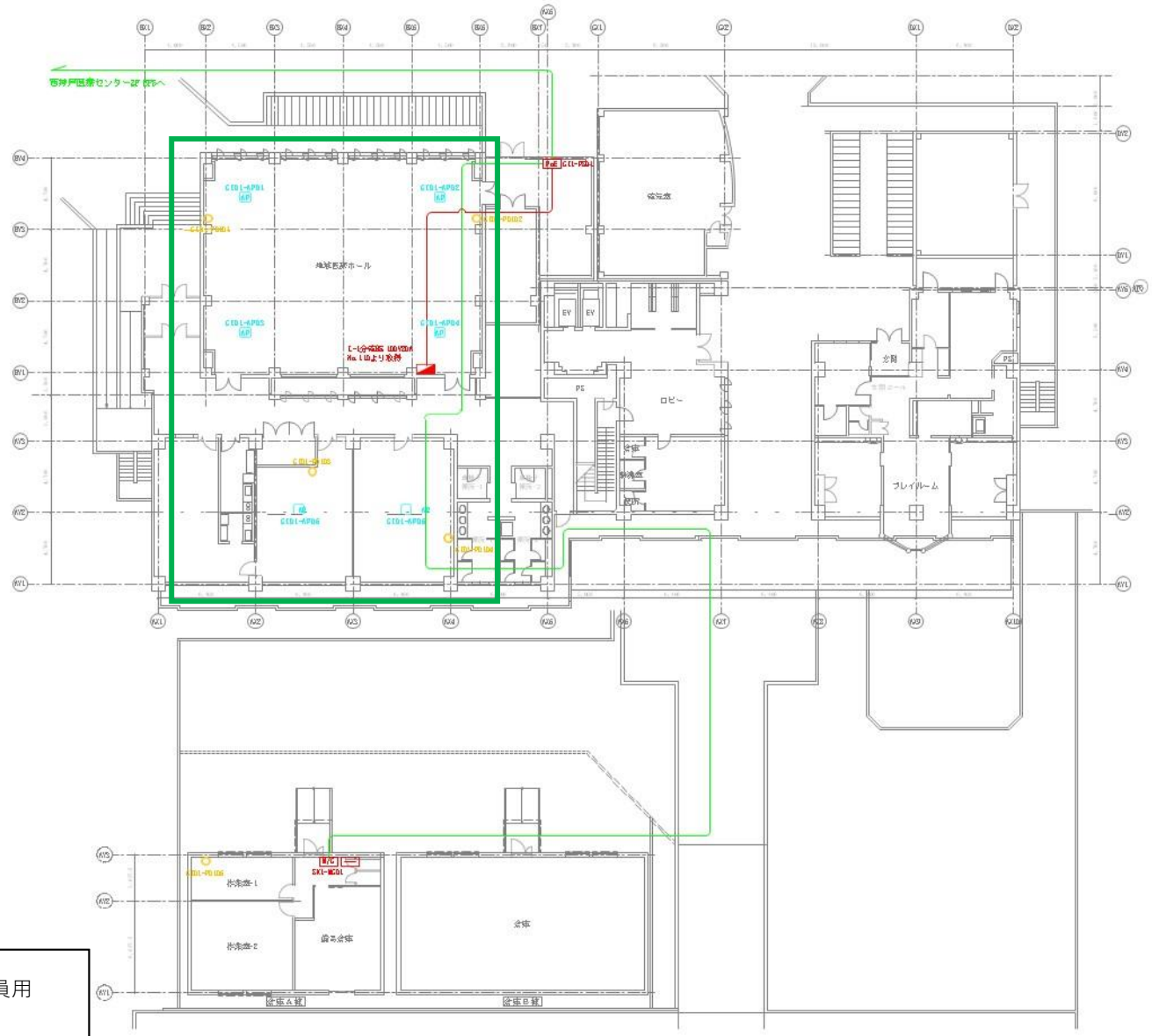


| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |

情報通信配管凡例

| ｼﾝﾎﾞﾙ | 名　称 | ｼﾝﾎﾞﾙ | 名　称 |
|---|---|---|---|
| | 無線アクセスポイント | | 天井内隠蔽配線 |
| | 新規 情報コンセント（埋込み型） | | 屋外用電線 PF28 |
| | 既存 情報コンセント（埋込み型） | | HUBボックス |
| | 新規 情報コンセント（露出型） | | LAN配線（UTPケーブル/Cat5E） |
| | 既存 情報コンセント（露出型） | | 光配線（光ケーブル / OM3 G1 8C） |
| | 立上りルート | | 絶体貫通部 |
| | 引下げルート | | |

図面名称　10階　配線図




| | |
|---|---|
| | 患者用・職員用<br>Wi-Fiエリア |

| ｼﾝﾎﾞﾙ | 名 称 | ｼﾝﾎﾞﾙ | 名 称 | ｼﾝﾎﾞﾙ | 名 称 |
|---|---|---|---|---|---|
| | 無線アクセスポイント | PoE | PoEスイッチ | | LAN配線（UTPケーブル/Cat6A） |
| | 分電盤コンセント | 集広 | メディアコンバータ | | 光配線（光ケーブル/OM4 4C） |
| | | | 多機能端子板 | | |
| | | | 分電盤 | | |

図面名称　地域医療ホール・倉庫　機器プロット・配線図

# 情報セキュリティ遵守特記事項

（趣旨）

第１条 この契約で定める情報セキュリティ遵守特記事項（以下「特記事項」という。）は、委託契約約款又は製造その他請負契約約款の特記条項として、個人情報を取り扱う業務又はネットワーク又は情報システムの開発、保守又はデータ処理その他情報処理に係る業務（ただし、業務遂行のための連絡用ツールとしてクラウドサービス等の外部サービスを利用する場合は除く。以下「情報処理業務」という。）の委託契約および請負契約（以下、「委託契約等」という。）に関する情報の取扱いについて、必要な事項を定めるものである。

（定義）

第２条 この特記事項において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 個人情報

個人情報の保護に関する法律（平成 15 年法律第 57 号）第２条第１項に規定する個人情報をいう。

(2) 特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）第２条第８項に規定する特定個人情報をいう。

(3) 第１号及び前号以外の秘密等に係る情報

法令の規定により秘密を守る義務を課されている情報、部外に知られることが適当でない法人その他の団体に関する情報及び部外に漏れた場合に信頼を著しく害するおそれのある情報をいう。

(4) 重要情報

第１号から前号までに規定する情報及び神戸市民病院機構（以下「甲」という。）が指定する情報をいう。

(5) 情報

重要情報及び重要情報以外の情報をいう。

（基本的事項）

第３条 この契約により甲から業務を受託または請負し情報を取り扱う者（以下「乙」という。）は、個人情報の保護に関する法律（平成 15 年法律第 57 号）、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）、神戸市個人情報保護法の施行等に関する条例（令和４年 12 月条例第 17 号）及び神戸市民病院機構情報セキュリティポリシーその他関係法令を遵守し、この契約による業務（以下「委託業務等」という。）を通じて知り得た情報の保護の重要性を認識し、委託業務等を履行するために必要な情報の取扱いにあたっては、甲の業務に支障が生じることがないよう、適正に取り扱わなければならない。

２　乙は、委託業務等を通じて知り得た情報を正当な理由なく他人に知らせ、又は不当な目的に使用してはならない。
３　乙は、委託業務等を履行するにあたって、情報の漏えい、滅失、き損及び改ざんの防止その他情報の適正な管理のために必要な措置を講じなければならない。

（管理体制の整備等）
第４条　乙は、情報の適正な管理を実施する者として業務責任者を選定して管理組織を整備するとともに、前条第３項の措置に係る管理規程又は情報の具体的な取扱い内容を規定しなければならない。
２　乙は、前項に定める管理体制を書面により速やかに甲に通知しなければならない。管理体制を変更するときも同様とする。
３　乙は、情報処理業務を行う場所及び情報を保管する施設その他情報を取り扱う場所において、入退室の規制及び防災防犯対策その他必要な情報セキュリティ対策を講じなければならない。

（従事者の監督）
第５条　乙は、乙の業務責任者に、乙の従業員その他委託業務等に従事する者（以下「従事者」という。）に対し、委託業務等を通じて知り得た重要情報を正当な理由なく他人に知らせ、又は不当な目的に使用しないよう、並びに委託業務等に関する重要情報を安全に管理するよう、必要かつ適切な監督を行わせなければならない。この契約が終了し、又は解除された後においても同様とする。

（教育の実施）
第６条　乙は、乙の業務責任者及び従事者に対し、委託業務等に関する情報を取り扱う場合に遵守すべき事項、関係法令に基づく罰則の内容及び民事上の責任その他委託業務等の適切な履行のために必要な事項に関する研修等の教育を実施しなければならない。

（作業場所及び従事者の届出）
第７条　乙は、委託業務等に関する仕様書において委託業務等の履行に係る作業場所が定められていない場合、当該作業場所を書面により速やかに甲に届け出なければならない。作業場所を変更するときも同様とする。
２　乙は、委託業務等を履行するにあたって、作業場所ごとに従事者の所属（特定個人情報を取り扱う場合は従事者の氏名及び役職も必要）その他必要な事項を書面により速やかに甲に届け出なければならない。従事者を変更するときも同様とする。

（収集の制限）
第８条 乙は、委託業務等を履行するにあたって情報を収集するときは、委託業務等を履行するために必要な範囲内で、適正かつ公正な手段により収集しなければならない。

（目的外利用及び第三者への提供の禁止）
第９条 乙は、委託業務等を履行するにあたって知り得た情報を、甲の書面による事前の承諾を得ることなく委託業務等を履行する目的以外の目的で利用し、又は第三者に提供してはならない。

（複写及び複製の禁止）
第 10 条 乙は、委託業務等を履行するにあたって甲から貸与された重要情報が記載又は記録された文書及び資料その他ファイル等を、甲の指示又は承諾を得ることなく複写し、又は複製してはならない。

（重要情報の管理）
第 11 条 乙は、委託業務等に関する重要情報を安全に管理するため、次の各号に定める事項を遵守しなければならない。
(1) 重要情報を作業場所以外に持ち出さないこと。やむを得ず持ち出さなければならないときは、甲の承諾を得たうえで行い、持ち出しの状況に関する記録を作成し、確実に保管すること。
(2) 重要情報が記載された文書が第三者の利用に供されることのないよう施錠管理すること。また、重要情報が格納された電子計算機又は電磁的記録媒体が第三者の利用に供されることのないよう、記憶領域の暗号化又はファイルへのパスワード設定を施したうえで施錠管理すること。
(3) 重要情報の格納又は処理を行うにあたって、個人のパーソナルコンピュータ等の電子計算機又は電磁的記録媒体を使用しないこと。
(4) 重要情報を処理する電子計算機について、ウイルス対策ソフトウェアの導入及び最新のウイルス定義ファイルへの更新を行うこと。

（再委託先等の監督等）
第 12 条 乙は、委託業務等を遂行するために得た重要情報を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、甲の書面による事前の承諾を得た場合は、この限りではない。
２ 乙は、前項ただし書の規定により重要情報を取り扱う業務を第三者に再委託または下請負（以下「再委託等」という。）する場合、当該再委託等を受ける者（以下「再委託先等」という。）に対し、この契約に基づく一切の義務を遵守させなければならない。

3　乙は、再委託先等の当該業務に関する行為及びその結果について、乙と再委託先等との契約（以下「再委託契約等」という。）の内容にかかわらず、甲に対して責任を負うものとする。
4　乙は、第２項の再委託等を行う場合、再委託契約等において、再委託先等が委託契約約款及び製造その他請負契約約款並びに特記事項を遵守するために必要な事項その他甲が指示する事項を規定するとともに、再委託先等に対する必要かつ適切な監督、重要情報に関する適正な管理及び情報セキュリティ対策について、具体的に規定しなければならない。
5　乙は、第２項の再委託等を行った場合、再委託先等による当該業務の履行を監督するとともに、甲の求めに応じて、履行の状況を甲に対して適宜報告しなければならない。
6　乙は、再委託先等に対し、甲の書面による事前の承諾なくして、重要情報をさらなる委託等（以下「再々委託等」という。）により第三者（以下「再々委託先等」という。）に取り扱わせることを禁止し、その旨を再委託先等と約定しなければならない。
7　第１項から前項までの規定は、前項の規定による甲の承諾を得て重要情報を取り扱う業務を再々委託等する場合について準用する。

（提供文書等の返還及び廃棄等）
第 13 条　乙は、委託業務等を履行するにあたって甲から貸与され、又は乙が収集し、複製し、若しくは作成した重要情報が記載又は記録された文書及びファイル等を善良な管理者の注意をもって管理し、この契約が終了し、又は解除された後直ちに甲に返還し、又は引き渡さなければならない。ただし、甲が別に指示したときは、当該方法によるものとする。
2　前項ただし書の場合において、重要情報が記録されたファイル又はファイルが格納された電磁的記録媒体（以下「ファイル等」という。）の廃棄等を甲が指示した場合、乙は、ファイル等からすべての情報を消去し、復元不可能な状態にする措置を講じなければならない。また、甲は、職員による立ち会い又は証拠書面の提出により当該措置の履行確認を確実に行わなければならない。
3　第１項の場合において、乙が乙の電子計算機を使用して重要情報を処理し、同項ただし書の規定により当該電子計算機（以下「機器」という。）に格納された当該重要情報の消去を甲が指示した場合、乙は、機器からすべての情報を消去し、復元不可能な状態にする措置を講じなければならない。また、甲は、職員による立ち会い又は証拠書面の提出により当該措置の履行確認を確実に行わなければならない。

（報告及び検査）
第 14 条　甲は、乙に対し、納品検査時に委託業務等に関する情報の管理状況及び情報セキュリティ対策の実施状況についての報告書を提出させなければならない。又、必要があると認めるときは、検査をすることができる。

２ 甲は、必要があると認めるときは、乙に対し、委託業務等である情報処理業務を行う場所及び情報を保管する施設その他情報を取り扱う場所で検査することができる。
３ 乙は、甲から前２項の指示があったときは、速やかにこれに従わなければならない。

（事故発生時等における報告等）
第 15 条 乙は、甲の提供した情報並びに乙、再委託先等又は再々委託先等が委託業務等の履行のために収集した情報について、火災その他の災害、盗難、紛失、漏えい、改ざん、破壊、コンピュータウイルスによる被害、不正な利用、不正アクセスその他の情報セキュリティ事故が発生したとき、又は発生するおそれがあることを知ったときは、速やかに甲に報告し、甲の指示に従わなければならない。
２ 乙は、前項の場合において、次の各号に定める事項を行わなければならない。
(1) 直ちに被害を最小限に抑えるための措置を講じること。
(2) 甲の求めに応じて、当該事故の原因を分析すること。
(3) 甲の求めに応じて、当該事故の再発防止策を策定し、実施すること。
(4) 甲の求めに応じて、当該事故の経緯等の記録を書面で提出すること。
３ 乙は、第１項の場合に備え、同項及び前項に定める報告等必要な事項を速やかに行うことができるよう、緊急時連絡体制を整備しなければならない。

（契約の解除及び損害の賠償）
第 16 条 甲は、次の各号のいずれかに該当するときは、乙に対してこの契約の解除及び損害賠償の請求をすることができる。
(1) 委託業務等を履行するために乙、再委託先等又は再々委託先等が取り扱う重要情報について、
乙、再委託先等又は再々委託先等の責に帰すべき理由による漏えい、滅失、き損又は改ざんがあったとき。
(2) 前号に掲げる場合のほか、特記事項に違反し、委託業務等の目的を達成することができないと認められるとき。

| 外部サービス名称 | | | 記入日 | | | |
|---|---|---|---|---|---|---|
| 外部サービス提供者名称 | | | 記入者 | | | |
| 区分 | | 要件 | 取扱情報が機密性2以上の場合 | | | |
| | | | 要否 | 適用状況 | 備考 | |
| 1.外部サービス要件（機密性2以上） | | | | | | |
| 1.1. | セキュリティ評価制度 | 利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））への登録が行われていること。 | 任意 | はい | 「はい」の場合は登録番号を記入ください<br>⇒ | |
| | | 1.1でISMAPへの登録が行われていない場合 | | | | |
| 1.2. | | 利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度「ISMAP-LIU」（ISMAP for Low-Impact Use）への登録が行われていること。 | 任意 | | | |
| 1.3. | SLA | サービスレベルの保証が定められていること。<br>SLAには以下のような内容が定められていること。<br>・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順及び情報セキュリティインシデントの対応等の取り決め<br>・外部サービス利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得、保持し、定期的にレビューできること。<br>・利用する外部サービス又はシステムの技術的脆弱性に関する情報は、公表された後に速やかにクラウドサービス利用者が入手できるようになっていること。 | 任意 | | | |
| 1.4. | クラウドサービス情報開示認定制度 | 利用しようとする外部サービス（アプリケーション）が一般社団法人日本クラウド産業協会(ASPIC)クラウドサービス情報開示認定制度への登録が行われていること。 | 任意 | | | |
| 1.5. | 生成AIを利用したサービスにおける入力情報の取扱 | 外部サービスが生成AIを利用したサービスに該当する場合においては、同サービスへの入力情報が、法人の許可なく生成AIの学習に用いられたり、サービスを提供する事業者による監査の対象にならないことが確認できること。 | 必須 | | | |
| 1.1.でISMAPへの登録が行われている場合、1.2.でISMAP-LIUへの登録が行われている場合、または1.4.でASPICへの登録が行われている場合、以下の要件は不要 | | | | | | |
| 1.6. | 資格・認証<br>※アプリケーション提供事業者 | サービス提供を行う組織が、ISO/IEC 27001：2013認証を取得していること。 | 任意 | | | |
| 1.7. | 資格・認証<br>※クラウドサービスプロバイダー | サービス提供を行う組織が、ISO/IEC 27001：2013認証を取得していること。 | 必須 | | | |
| 1.8. | | サービス提供を行う組織が、ISO/IEC 27017：2015認証もしくはPCI DSSを取得していること。 | 必須 | | | |
| 1.9. | | サービス提供を行う組織が、ISO/IEC 27018：2014認証を取得していること。 | 任意 | | | |
| 1.10. | データの所在・適用法と裁判管轄 | サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。 | 必須 | | | |
| 1.11. | | サービス提供事業の実施場所（事務所、運用場所）（地域（リージョン）が特定できるようにすること）を情報提供すること。提供にあたっては文書にて内容を確約すること。 | 必須 | | | |
| 1.12. | | 準拠法、裁判管轄を国内に指定できること。 | 必須 | | | |
| 1.13. | | 法人が登録したデータは、法人に確実に提供でき、提供後のデータの所有権・管理権は、法人が保有すること。また、法人が登録したデータは、本契約に明示的に定められているところを除き、法人の承諾なく、利用できないものとすること。 | 任意 | | | |
| 1.14. | データセンター要件 | データセンターは、日本データセンター協会が制定するデータセンターファシリティスタンダードのティア3相当の基準を満たした設備とすること。 | 必須 | | | |
| 1.6 と 1.9の認証を取得している場合、以下の要件は不要 | | | | | | |
| 1.15. | セキュリティ対策・体制 | サービス提供業務の遂行のために提供する情報（契約等の手続に付随して外部サービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。 | 必須 | | | |
| 1.16. | | サービス提供を行う組織若しくはその従業員、再委託先又はその他の者によって、法人の意図しない変更が加えられないための管理体制について提示すること。 | 必須 | | | |
| 1.17. | | 情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。 | 必須 | | | |
| 1.18. | | 障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。 | 必須 | | | |
| 1.19. | データ暗号化 | 機密性の高いデータ等については、暗号化等によって蓄積・伝送データを保護できること。 | 必須 | | | |
| 1.20. | ログ取得 | 外部サービス上におけるアクセスログ等の証跡に係る保存期間について、1年間以上の保存が可能であること。その手法について提示すること。 | 必須 | | | |
| 1.21. | 脆弱性対策 | 外部サービス上の脆弱性を発見する方法があり、実施可能であること。その手法について提示すること。 | 必須 | | | |
| 1.22. | 不正アクセス対策 | 通信内容を監視する等により、不正アクセスや不正侵入を検知及び通知できること。 | 必須 | | | |
| 1.23. | 機器停止 | 機器に異常があった場合、検知できること。<br>また、機器を死活監視し、停止した場合、検知できること。 | 必須 | | | |
| 1.24. | データ取扱い時の権限管理 | データの取り扱いについて、権限管理及びアクセス制御ができること。 | 必須 | | | |
| 1.25. | 保守端末 | 保守端末は、認証管理、持出管理、施錠管理、ログ管理等によりセキュリティを確保していること。 | 必須 | | | |
| 1.26. | データ消去 | データを消去する際は、ISO27001に準拠してデータを復元できないように電子的に完全に消去又は廃棄すること。また、データを消去又は廃棄した証明書を提示すること。<br>なお、ISO27001にデータ消去が未規定の場合、サービス終了までに規定し、認証を受けること。 | 必須 | | | |
| 1.27. | セキュリティ監査 | 情報セキュリティ監査の受入れが行われていること。 | 任意 | | | |