

ネットワーク一式 仕様書

2026年10月

近江八幡市立総合医療センター

近江八幡市立総合医療センター ネットワーク式

仕様書 目次

- A 基本要件
- B 役務・保守他
- C ネットワーク

項番	機能要件	配点
A	基本要件	—
A.1	共通要件	—
A.1.1	本仕様書は、近江八幡市立総合医療センター(以下「当センター」という。)に導入するネットワーク一式および7年間の保守委託業務について規定するものである。	○
A.1.2	納入場所は、滋賀県近江八幡市土田町1379 近江八幡市立総合医療センター内とすること。	○
A.1.3	当センターの良質な医療を効率的に運営するために、より低価格で、より良い総合医療情報システムを調達するという目的に沿った提案を行うこと。	○
A.1.4	本調達は仕様書だけではなく、別表等の他資料の要件も含めて応札すること。	○
A.1.5	ネットワークは稼働後、7年間はサポートができる機器・役務を提供すること。具体的には保守および法令改訂等による機能追加、修正、更新ができること。	○
A.1.6	ネットワークは、導入後7年利用するため、全国的な導入実績を持つ機器を提供すること。また、ネットワークの陳腐化を防ぎ、常に最新の機能やセキュリティ基準を維持できるよう、計画的なアップデート(機能向上プログラムの適用)が継続的に提供されること。	○
A.1.7	応札技術仕様書で対応可能と回答した機能要件を満たすための費用は、全て本調達に含めること。	○
A.1.8	仕様書の必須項目は、完全に実現できなければならない要件であるが、部分的にできない内容やネットワーク上の機能が異なる場合は、その旨を記載してネットワーク上又は運用上での回避方法を明記すること。その提案が合理的であると当センターが判断すれば、仕様を満たしていると判断することもある。ただし、提案内容が不十分であれば、失格となる場合があるので十分に注意すること。	○
A.1.9	提出された資料について、当センターが不明確であると判断した場合は、技術的要件を満たしていない資料とみなす場合があるので十分に注意すること。	○
A.1.10	仕様書に記載されていない機能を最新標準機能として搭載している場合は、その利用を前提として機能を提供すること。	○
A.1.11	応札者は、ネットワークの明細書(ハードウェア・ソフトウェア・導入作業費用・保守費用等の品名、数量、標準価格、提供価格が記載された明細書)を提示すること。	○
A.1.12	本調達のネットワークが2027年10月1日までに確実に稼働する状態で納入すること。また、稼働スケジュールは、落札後、当センターと協議の上で決定すること。	○
A.1.13	導入スケジュールは当センターと十分協議し、導入にあたっては通常業務への影響を最小限にとどめ、病院業務に混乱を起こさず、且つ、当センター職員の負荷が増大しないよう配慮できるよう仕組みを提供すること。	○
A.1.14	受注者又は実作者の責めに帰すべき理由により、当センターと協議により決定した稼働期日に対して遅延が発生した場合は、遅延期間の現行システム継続利用に係る費用を受注者が全額負担すること。	○
A.1.15	基本的な要件(基本要件、役務・保守他)は、本調達の全てのシステムを包含する要件として実現できること。また、各章にまたがる要件がある場合は、互いの仕様に準拠すること。	○
A.1.16	受注者の自社製品だけで仕様を満たさない場合は、他社製品を使って仕様を満たしてもよい。ただし、受注者は、他社製品を用いて満たす要件も含めて、本仕様書の全要件の内容を把握し、各章にまたがる要件を整理の上、他社製品導入者との役割・業務分担や機能範囲を明確にすること。	○
A.1.17	提案するネットワークに関してハード、ソフトを納入でき、責任を持って構築できる体制を整えること。	○
A.1.18	円滑なネットワーク本稼働を実現するために、他病院において導入経験のあるネットワークエンジニア(以下NE)による開発体制を整備すること。	○
A.1.19	他病院で生じたネットワークトラブルの事例を整理しており、システム化していること。トラブル発生時は全国の各ネットワークサポートの拠点に通知し、同一原因によるトラブルの再発を防止する体制を有すること。	○
A.1.20	仕様書に記載のない機能要件で、標準機能で有する有用で革新的な機能がある場合は、その機能を資料で提示すること。	○
A.2	システム	—
A.2.1	基本要件	—
A.2.1.1	当センターは10年以上に渡り電子カルテを運用しており、多くの患者の診療記録が蓄積されている。電子カルテの膨大な診療データが存在する前提において、システム更新後もデータの蓄積量に依存せず、画面展開や患者検索等のレスポンスタイムが、現行ネットワーク同等以上の快適な動作速度を維持できるネットワークを提供すること。	○
A.2.1.2	デファクトスタンダードを追求したシステム構築を基本とし、システムのOS・通信プロトコル等は国際標準・業界標準を積極的に採用すること。	○
A.2.1.3	汎用性とシステムの安定性を考慮し、サーバおよびクライアントのOSは最新又は同等以上の性能・機能を有すること。	○
A.2.1.4	「医療情報システムの安全管理に関するガイドライン」(2026年9月末時点の最新版)および厚生労働省標準規格の最新版(2026年9月末時点の最新版)に準拠していること。	○
A.2.1.5	提案に参加する全ベンダーは、仕様書の全ページを確認し内容を理解したことを示す確認書を取得し提出すること。	○
A.2.1.6	各章にまたがる要件がある場合は、互いの仕様に準拠すること。	○
A.2.1.7	受注者の自社製品だけで仕様を満たさない場合は、他社製品を使って仕様を満たしてもよい。ただし、受注者は、他社製品を用いて満たす要件も含めて、本仕様書の全要件の内容を把握し、各章にまたがる要件を整理の上、他社製品導入者との役割・業務分担や機能範囲を明確にすること。	○
A.2.1.8	本調達ネットワークに接続が必要な既存システムおよび機器は全て接続すること。	○
A.2.1.9	別紙. ネットワーク構成図・配置図等に記載の既存システムや機器側の接続費用は、本調達に含めること。部門ベンダー自社のリモートアクセス環境、ファイアウォールおよび端末接続は対象外とする。また、リモート集約化に含むことができない部門ベンダーが発生する場合は作業対象外とする。	○

A. 2. 1. 10	ネットワーク間やネットワークと機器間のデータ連携に関する要件は各章に記載するが、連携対象ネットワークの双方の要件に同一内容の記載がなくても、その要件を実現すること。	○
A. 2. 1. 11	疑義がある場合には、入札前に質問事項として当センターに提出し、その回答に従うこと。	○
A. 2. 1. 12	提案するネットワークに関し、ハード・ソフトを納入でき、責任を持って構築できる体制を整えること。	○
A. 2. 1. 13	円滑なネットワーク本稼働を実現するために、他病院において開発経験のあるSEによる体制を整備すること。	○
A. 2. 1. 14	一病院で生じたシステムトラブルの事例を全国の各ネットワークサポートの拠点に通知し、同原因によるトラブルの再発を防止する体制を有すること。	○
A. 2. 1. 15	医療機関で行うべき重要ポイントも、過去の事例に従い詳細に資料に記載して提出すること。	○
A. 2. 1. 16	本システムの構成が理解できるように、ハードウェア・ソフトウェア等の構成図を提出すること。	○
A. 2. 2	情報セキュリティ	—
A. 2. 2. 1	受注者は、本調達仕様書の内容を踏まえた上で、納入するネットワークのセキュリティ設計、環境構築等にかかる作業を主体的に実施すること。本調達において、以下の要件を満たすセキュリティ管理を実施すること。その他、環境設計する上で必要な要件は契約締結後に当センターと協議すること。	○
A. 2. 2. 2	受注者は、情報セキュリティ管理体制を有し、セキュリティ管理責任者を設けること。	○
A. 2. 2. 3	「政府機関等のサイバーセキュリティ対策のための統一基準」の最新版および当センターの情報セキュリティポリシーに準拠していること。なお、当センターの情報セキュリティポリシーが原則的に優先するが、統一基準にある記載内容を考慮したものであることが必要である。	○
A. 2. 2. 4	当センターが提供する情報(資料等)は、情報セキュリティ管理体制の下、第三者への漏えいや目的外利用が行われないよう、適切に管理すること。なお、原則として貸出しによるものとし、本契約終了時まで担当職員の指示に従い、当センターに返却すること。また、当該資料の複写はしないこと。	○
A. 2. 2. 5	当センターが提供した情報の第三者への漏えいや目的外利用、委託業務以外の情報への不正アクセス等、情報セキュリティに問題が生じたときは、直ちに当センターへ報告し、必要な対策を講じること。	○
A. 2. 2. 6	ネットワーク導入の各工程において、当センターの意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされること。	○
A. 2. 2. 7	当センターの意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類(例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図)を提出すること。第三者機関による品質保証体制を証明する書類等が提出可能な場合は、提出すること。	○
A. 2. 2. 8	ネットワークに当センターの意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、当センターと連携して原因を調査し、排除するための手順および体制(例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、要求された場合には提出できるなど)を整備していること。また、当該手順および体制が妥当であることを証明するための書類を提出すること。	○
A. 2. 2. 9	当センターの許可なく、作業の一部又は全部を第三者(再委託先)に請け負わせてはならない。ただし、当センターが許可した場合には、受注者は、当センターとの契約上受注者に求められる水準と同等の情報セキュリティ水準を再委託先においても確保すること。また、受注者は、再委託先が実施する情報セキュリティ対策およびその実施状況について、当センターに報告すること。	○
A. 2. 2. 10	委託業務において取り扱う情報について、再委託先が閲覧することがないように、受注者は情報を厳重に管理すること。やむを得ず、再委託先において委託業務に係る情報を閲覧する必要がある場合には、受注者は、事前に当センターの担当者と調整し、その指示に従うこと(再委託先における情報の取扱いを含む包括的な秘密保持契約を締結する、作業の都度情報の取扱いについて調整するなど)。	○
A. 2. 2. 11	ネットワーク導入進捗報告会や運用開始後の定例報告会等を用いて、情報セキュリティ対策の履行状況(例えば、情報の受渡しや返却の実績および受け渡した情報の管理状況等)を報告すること。情報セキュリティ対策の履行が不十分と当センターが指摘した場合には、是正計画を当センターへ報告し、当センターが了承した後に是正処置を行うこと。	○
A. 2. 2. 12	ネットワーク機器、その他のネットワーク上で稼働させるソフトウェアは、本稼働時点で最新の修正プログラムやセキュリティパッチを適用の上でシステム動作試験を行い、正常に動作することを検証すること。	○
A. 2. 2. 13	総合医療情報システム以外との通信は発生した際、それらの通信記録を全て定期的に当センターへ報告すること。	○
A. 2. 3	基本機能	—
A. 2. 3. 1	ネットワークは、データのセキュリティ保護と、患者のプライバシー保護のための対策が講じられていること。	○
A. 2. 3. 2	ID・パスワード認証方式により、アクセス管理ができること。また、職種に応じてデータ参照範囲・データ入力範囲に関するセキュリティレベルを設定できること。なお、ログインパスワードは、「大文字・小文字・数字・記号」の4種類のうち、3種類以上を用いて8文字以上で作成できること。	○
A. 2. 3. 3	ネットワークのアクセスログや操作履歴の管理ができ、必要に応じて閲覧やデータ出力ができること。	○
A. 3	高可用性	—
A. 3. 1	故障や停電等の障害発生時においても、病院業務の遂行に支障を及ぼす影響を極小化し、復旧時の保守管理操作も容易なシステムを提供すること。	○

項番	機能要件	配点
B	役務・保守他	—
B.1	役務	—
B.1.1	本調達ネットワーク機器更新後の7年間総額の保守費用を別途見積り提示すること。7年間の保守費用総額により加点する。	●
B.2	役務	—
B.2.1	プロジェクト管理	—
B.2.1.1	管理手法	—
B.2.1.1.1	管理業務の遂行にあたり、PMBOK(Project Management Body Of Knowledge)又はこれに類するプロジェクト管理体系に準拠したプロジェクト管理を行うこと。	○
B.2.1.1.2	プロジェクト計画書を策定し、当センターに説明すること。	○
B.2.1.2	進捗管理	—
B.2.1.2.1	作業計画に基づき、各タスクの状況把握およびスケジュール管理を行うこと。	○
B.2.1.2.2	各タスクの進捗状況に関するプロジェクト会議を開催し、当センターに作業状況を報告すること。	○
B.2.1.2.3	プロジェクト会議では、対象とする作業期間に予定していた全タスクについて作業進捗を報告すること。	○
B.2.1.2.4	計画から遅れが生じた場合は原因を調査し、要員の追加および担当者の変更等の体制の見直しを含む改善策を提示し、当センターの承認を得た上でこれを実施すること。	○
B.2.1.3	品質管理	—
B.2.1.3.1	プロジェクト計画書に基づき、設計工程完了時の品質指標を測定した上で、プロジェクト内で評価し、評価結果を当センターに報告すること。	○
B.2.1.3.2	プロジェクト内に、品質管理を担当する担当者が存在すること。	○
B.2.1.3.3	上記、品質管理担当者による品質レビューを定期的実施すること。	○
B.2.1.4	コミュニケーション管理	—
B.2.1.4.1	作業工程ごとにコミュニケーション計画を策定し、当センターの承認を受けること。なお、コミュニケーション計画では、会議体の目的、開催頻度および対象者等を明確にすること。	○
B.2.1.4.2	策定したコミュニケーション計画に基づき、設計工程における各種作業に関する打合せ、成果物等のレビュー、進捗確認および課題共有等を行うために、当センター職員が出席するプロジェクト会議を開催すること。	○
B.2.1.4.3	各会議が開催される都度、受注者が議事録を作成し、原則5営業日以内に提示の上で当センターの承認を受けること。なお、議事録にはワーキングで意思決定を行った当センター担当者を明記し、ネットワーク稼働後に仕様の検討経緯や決定者の遡及確認が行えるように留意すること。	○
B.2.1.5	課題管理	—
B.2.1.5.1	プロジェクト遂行上様々な局面で発生する各種課題について、課題の認識、対応案の検討、解決および報告のプロセスを明確にすること。	○
B.2.1.5.2	課題管理にあたり以下の内容を一元管理することとし、その他必要と考えられる項目についても管理する仕組みとすること。・ 課題内容 ・ 影響 ・ 優先度 ・ 発生日 ・ 担当者 ・ 対応状況 ・ 対応策 ・ 対応結果 ・ 対応完了日	○
B.2.1.5.3	積極的に課題の早期発見に努め、迅速にその解決に取り組むこと。	○
B.2.1.5.4	本業務の推進に影響を与えるような重大な課題が発生した場合は、速やかに当センターに報告し、対応策について協議すること。	○
B.2.1.6	構成・変更管理	—
B.2.1.6.1	ネットワークの整合性を維持し、プロジェクト環境の変更に対するトレーサビリティを確保すること。	○
B.2.1.6.2	構成管理対象(仕様書および設計書等)を特定し、管理レベル(参照・更新権限および保存方法・期間等)を定めること。	○
B.2.1.6.3	要件と構成管理対象の変更について、双方向に追跡可能な仕組みを確立すること。また、定期的に監査・評価し、その結果を反映・報告すること。	○
B.2.1.7	リスク管理	—
B.2.1.7.1	技術的観点、進捗的観点、人間的観点や、本ネットワークと類似する案件で発生した問題等から、プロジェクトの遂行に影響を与えるリスクを識別し、その発生要因、発生確率および影響度等を整理すること。また、発生確率および影響度に基づき、リスクの優先度を決定し、それに応じた対策を行うこと。	○
B.2.1.7.2	上記で整理したリスクおよび各内容について定期的に監視・評価し、その結果を反映・報告すること。	○
B.2.1.7.3	リスクを顕在化させないための対応策(対応手順、体制等)を策定すること。	○
B.2.2	体制・導入	—
B.2.2.1	体制	—
B.2.2.1.1	受注者決定後、1か月以内には導入を開始できる体制とすること。構築時のネットワークの人員体制は、当センターの稼働を十分にサポートできるようにすること。仮に、当センターがサポートが不十分と判断した場合は、相談により人員体制を強化すること。	●
B.2.2.1.2	受注者決定後、速やかにワーキンググループ構成およびメンバー案を当センターへ提示するなど、当センター側の出席者の調整に配慮すること。	○
B.2.2.1.3	作業開始から稼働までのマスタスケジュール表を当センター役割とベンダー側役割に分けて、詳細な作業分担表を提示すること。なお、作業内容にはネットワーク構築やデータ移行をはじめとした、ネットワーク導入に不可欠な内容を十分に盛り込むこと。	●
B.2.2.1.4	開札後、2週間以内に、詳細なスケジュールとネットワーク概要の説明を行うこと。別日程で、院内(情報管理課)向けに再度全体のスケジュールの説明を受注者が行うこと。	○
B.2.2.1.5	SE・営業・CE	—

B. 2. 2. 1. 5. 1	ネットワーク構築のプロジェクトマネージャーは実務経験5年以上であり、3件以上の医療機関でプロジェクトマネジメントの経験を有すること。また、これまでの経歴および実績医療機関名を記載して提出すること。また、当センターの必要に応じて、実績医療機関に問合せができるように協力すること。	●
B. 2. 2. 1. 5. 2	ネットワーク構築の営業責任者は実務経験5年以上であり、ネットワーク構築プロジェクトの担当経験を有すること。また、これまでの経歴および実績医療機関名を記載して提出すること。	●
B. 2. 2. 1. 5. 3	ネットワーク構築の主担当NEは実務経験5年以上であり、400床以上の医療機関で主担当NEの経験を有すること。担当NEの担当経歴を記載すること。	●
B. 2. 2. 1. 5. 4	ネットワーク構築の主担当CEは実務経験5年以上であり、400床以上の医療機関で主担当CEの経験を有すること。また、担当CEの保守経歴を記載すること。	●
B. 2. 2. 1. 5. 5	担当のSE・CEは、事前に当センターに届け出てネットワーク構築・保守にあたること。	○
B. 2. 2. 1. 5. 6	ネットワークの支援組織体制表を当センターへ提示すること。	○
B. 2. 3	導入作業	—
B. 2. 3. 1	受注者は構築にあたり、ワーキンググループを開催して当センターの現状の運用を調査し、導入ネットワークの説明を行うこと。また、ネットワーク導入後の運用は、患者目線に沿い、効率性・経済性に優れた提案を行い、当センターと協議の上決定すること。決定に際しては、具体的な運用フローを記載した書面をもって、決定の承認を得ること。	○
B. 2. 3. 2	ネットワークベンダーが現行から変更になった場合は、当センターの運用変更が予想される。その際は、他院での事例を示しながら、当センターの立場に立ち真摯に運用方法の検討を行うこと。	○
B. 2. 3. 3	ネットワークの構築期間中に、当センター・受注者が、いつまでに何を行うのか明確にした詳細スケジュールを提示すること。	○
B. 2. 3. 4	導入時や機能追加・変更時の設計書等のドキュメントを提出すること。	○
B. 2. 3. 5	セキュリティ・情報保護の観点から、ネットワーク構築に携わるSEは全員、院内の出入りに際し、IDの提示又は名札を着用すること。また、ネットワーク構築に携わるSE全員に対して提供ベンダーの責任で、病院内の行動に関する倫理・道徳・社会常識的な指導を行うこと。指導方法はマニュアル化し、全員の承諾を得ること。	○
B. 2. 3. 6	受注者はプロジェクト会議を定期的に行い、導入の過程・進捗状況・課題対応状況を当センターに報告すること。また、プロジェクト会議には当センター職員を参加させ、その意見の中で適切なものは採用すること。	○
B. 2. 3. 7	ネットワーク導入における設計・構築・テスト等の各工程の完了は、当センター職員も参加するレビュー会議を開催して当センターの承認を得ること。レビュー会議で指摘された内容を真摯に受け止めて迅速に対応すること。	○
B. 2. 3. 8	ネットワークの稼働は、当センターの確認および承認によって行うこと。	○
B. 2. 3. 9	作業にあたっては、別途当センターが指定する作業場所を使用すること。なお、作業用機や椅子等は、当センターが余剰品で用意するが、不足する分は受注者が用意すること。また、指定する作業場所以外のスペースは提供が困難であるため、作業場所が不足する場合は受注者の事業所等での作業を前提とすること。なお、リモート作業を行う場合は、受注者の事業所等での作業を前提とすること。	○
B. 2. 3. 10	本ネットワークの稼働が確認された後は、保守等の作業に必要な機器等を除き、速やかに撤収して原状に復すること。ただし、既存システム機器は、対象外とする。	○
B. 2. 3. 11	作業に伴う各室への立入り時には、当センター担当者経由で各部署の責任者に確認を取り、その許可を受け、当センターの業務に支障を来さないように、且つ、患者への迷惑とならないように配慮すること。	○
B. 2. 3. 12	作業場所は、常に整理整頓し、定期的に清掃を行うこと。また、ゴミやダンボールの廃棄は当センターの指示に従うこと。	○
B. 2. 3. 13	作業場所を返却する際は、受注者が原状復帰させること。	○
B. 2. 3. 14	病院情報システム専用ネットワークで仮設配線が必要となる場合は、作業にあたって当センター担当者との協議に応じること。	○
B. 2. 3. 15	導入時に必要となる本業務作業室（開発室やマシン室等）のネットワーク機器と配線は、全て本調達に含めること。	○
B. 2. 3. 16	新システムにおけるIPアドレスの設計・管理は受注者で行うこと。システム稼働後は、当センター職員又はそれに準ずるオペレータ要員等へ引継ぎを行うこと。	○
B. 2. 4	その他	—
B. 2. 4. 1	障害時対応	—
B. 2. 4. 1. 1	障害時にリモートデスクトップ、Telnet、ssh、GUI等いずれかにて対応ができること。	○
B. 2. 5	ハードウェア設置作業	—
B. 2. 5. 1	サーバ設置調整作業（サーバは、本調達により導入する機器を示す。）	—
B. 2. 5. 1. 1	サーバ機器等の設置作業の日程と体制を事前に当センターに提示し、当センター担当者と協議を行いその指示に従うこと。	○
B. 2. 5. 1. 2	サーバ機器等の搬入・設置作業にあたっては、病院業務への妨げや、患者への迷惑とならないように、且つ、施設を毀損することのないように十分な注意を払うとともに、受注者が必ず立ち会うこと。	○
B. 2. 5. 1. 3	当センターとの協議内容・導入機器等の設置場所・作業内容に関して、それぞれ完了後に書面で報告し、当センターの承認を受けること。	○
B. 2. 5. 1. 4	サーバ機器等の設置の際に、2次側のブレーカ以降の電源配線、ネットワーク配線部材の費用は、本調達に含めること。また、当センターが用意すべき2次側のブレーカを示すこと。	○
B. 2. 5. 2	端末機器・ネットワーク機器・その周辺装置の設置調整作業（端末機器・その周辺装置は、本調達で導入する機器を示す。）	—
B. 2. 5. 2. 1	端末機器・ネットワーク機器・その周辺装置の設置にあたり、当センター職員の立会いの下あらかじめ設置場所の下見を行い、当センターが提供する建屋図面へのプロットを行うこと。その際に、当センターの準備する電源や机に不備がある場合は、助言すること。	○

B. 2. 5. 2. 2	端末機器・ネットワーク機器・その周辺装置の配置は現状を基本とするが、若干の変更(微調整)の可能性があるので柔軟に対応すること。下見による結果の差異を当センター担当者へ報告し、その指示に従うこと。	○
B. 2. 5. 2. 3	端末機器・ネットワーク機器・その周辺装置の設置作業日程と体制を事前に当センターに提示し、当センター担当者と協議を行いその指示に従うこと。	○
B. 2. 5. 2. 4	端末機器・ネットワーク機器・その周辺装置とネットワークとの間は、情報コンセント又はスイッチングハブから、UTPケーブルを用いて接続すること。ネットワーク配線部材の費用および必要となる電源タップの費用は、本調達に含めること。	○
B. 2. 5. 2. 5	手術室など、有線LAN接続の端末機器を移動する必要がある場所ではLAN配線の取り回しや接続部の保護に配慮すること。	○
B. 2. 5. 2. 6	入出力機器との接続は、UTPケーブル又はUSB 3.0以上のケーブルを用いて接続すること。なお、ケーブル等の費用は、本調達に含めること。	○
B. 2. 5. 2. 7	作業に伴う各室への立入り時には、当センター担当者経由で各部署の責任者に確認を取り、その許可を受け、当センターの業務に支障を来さないように、且つ、患者への迷惑とならないように配慮すること。	○
B. 2. 5. 2. 8	当センターとの協議内容・導入機器等の設置場所・作業内容に関して、それぞれ完了後に書面で報告し、当センターの承認を受けること。	○
B. 2. 5. 2. 9	端末機器・ネットワーク機器・その周辺装置には、機器管理名称を明示すること。なお、手書きによる記載は、これを認めない。	○
B. 2. 5. 2. 10	現行ネットワーク機器の撤去を行い、当センターが指定する場所に集積すること。ただし、現有機器を継続利用する場合もあるので、当センターの指示に従うこと。	●
B. 2. 5. 2. 11	端末機器・ネットワーク機器・その周辺装置の配置については、指示された箇所に提供ベンダーの要員が設置すること。必要に応じて当センター職員が立ち会うが、設置作業・動作確認作業は受注者で行うこと。	○
B. 2. 5. 3	機器接続調整・動作確認作業	—
B. 2. 5. 3. 1	接続にあたっての相互接続調整作業費用および必要となる部材等の費用は、本調達に含めること。	○
B. 2. 5. 3. 2	当センターとの協議内容・作業内容に関して、それぞれ完了後に書面で報告し、当センターの承認を受けること。	○
B. 2. 5. 4	動作確認作業	—
B. 2. 5. 4. 1	本調達で導入する全ての機器について動作確認を行うこと。	○
B. 2. 5. 4. 2	ネットワークを構成する機器のうち、相互通信が必要である装置間の接続に関して通信テストを含む動作確認を行うこと。	○
B. 2. 5. 4. 3	本ネットワークと接続を行った、各既存装置との通信テストを含む動作確認を行うこと。	○
B. 2. 5. 4. 4	設置する機器の接続テスト・機能テストは、必ず当センター職員の立会いの下に行い、その評価を受けること。	○
B. 2. 5. 4. 5	協議内容・作業内容の結果を書面で報告し、当センターの承認を受けること。	○
B. 2. 6	ソフトウェアインストール作業	—
B. 2. 6. 1	サーバソフトウェアのインストール作業	—
B. 2. 6. 1. 1	サーバごとの基本ソフトウェア・アプリケーションソフトウェアをインストールし、動作確認を行うこと。	○
B. 2. 6. 1. 2	協議内容・作業内容・動作確認の結果をそれぞれ書面で報告し、当センターの承認を受けること。	○
B. 2. 6. 2	端末機器・ネットワーク機器・その周辺装置ソフトウェアのインストール作業	—
B. 2. 6. 2. 1	端末機器・ネットワーク機器・その周辺装置ごとの基本ソフトウェア・アプリケーションソフトウェアをインストールし、動作確認を行うこと。	○
B. 2. 6. 2. 2	協議内容・作業内容・動作確認の結果をそれぞれ書面で報告し、当センターの承認を受けること。	○
B. 2. 6. 2. 3	サーバ・端末のOSや、その他の端末上で稼働させるシステムの動作に必要なソフトウェアは、本稼働時点で最新の修正プログラムを適用の上で、システム正常動作を確認すること。	○
B. 2. 7	稼働後の立会体制	—
B. 2. 7. 1	稼働後は、最低でも7営業日は診療現場での立会いを行うこと。また、立会日程・立会終了日は当センターとの協議の上決定すること。	○
B. 2. 7. 2	新ネットワーク稼働直後は、各種の不具合や課題が発生することが想定される。稼働後数日間は、当センターと受注者による連絡会議を開催し、不具合や課題に対する対応方針を協議する機会を設けること。	○
B. 2. 8	その他	—
B. 2. 8. 1	稼働するネットワークに合わせて病院情報システム運用管理規程および関連するドキュメントの改訂が必要な際は、その作業を支援すること。	○
B. 3	運用	—
B. 3. 1	運用管理	—
B. 3. 1. 1	サーバ監視	—
B. 3. 1. 1. 1	サーバハードウェアの監視を行うこと。また、エラー等の通報を受注者側で受け、ハードウェア保守担当に出動依頼を行うこと。	○
B. 3. 1. 1. 2	ネットワークに関する業務アプリケーションの監視(具体的には「サーバプロセス起動・稼働監視」「定期業務実行監視(日次・月次)」等)を行うこと。具体的な監視項目は当センターと協議の上決定すること。	●
B. 3. 1. 1. 3	サーバパフォーマンスの監視(具体的には「DISK容量」「DB容量」「メモリ使用量」等の監視)を行うこと。具体的な監視項目は当センターと協議の上決定すること。	○
B. 3. 1. 1. 4	これらの受付・監視は24時間・365日行い、各監視状況を報告すること。	○
B. 3. 1. 1. 5	各システム間のI/Fを監視し、止まっているなどのエラーが発生した場合は、自動で管理者に通報できること。	○
B. 3. 1. 2	リモート保守センターに関わる設備・人員・実績	—

B.3.1.2.1	ネットワークで、緊急対応ができる業務スキルを保有した要員との連絡が、当センターから取れる体制を有すること。	●
B.3.1.2.2	これらリモート保守におけるネットワークのサポートを医療機関に対して提供している実績を有すること。	○
B.3.1.2.3	ハードウェア・アプリケーションに関するコールを一元的に受付するサポート窓口を設けること。また、サポート窓口担当者には、病院業務とネットワークに精通したSEを配置していること。その実績を有する場合は、実績を提示すること。	●
B.3.1.3	障害発見時の通報体制	—
B.3.1.3.1	ネットワークから自動的に障害情報が通知され、緊急性が高いと判断された場合は、その時点で当センター担当者に連絡すること。	○
B.3.1.3.2	受注者による電話対応は、留守番電話ではなく常時受付体制を有すること。	○
B.3.1.3.3	機器障害時に当該箇所の特定後は、原則4時間以内に復旧作業を開始できる体制を有すること。	○
B.3.1.4	障害発生時の対応	—
B.3.1.4.1	当センターからの障害通知又はベンダーの障害発生把握から、原則2時間以内に当センターに到着又はリモートでの対応ができる体制を構築すること。	○
B.3.1.4.2	障害発生時は、復旧後1週間以内に障害対応報告書を当センターに提出し、その承認を受けること。ただし、障害の過失度合いや影響程度によっては、メール等での簡易な報告を認める。	○
B.3.1.5	計画停電時の対応	—
B.3.1.5.1	2年に1回の計画停電を実施している。計画停電時にはサーバ管理・ネットワーク管理の視点で立ち合いを実施すること。	○
B.3.1.5.2	計画停電は保守費用で実施すること。	○
B.4	その他	—
B.4.1	ネットワーク稼働後検証	—
B.4.1.1	ネットワーク稼働後の1か月目に本仕様書の技術要件を満たしているかの確認を行う。確認作業の前には、開発ベンダーとしての稼働認識を仕様書の各技術要件に関し、「●(稼働)」又は「×(未稼働)」を記載して提出すること。	○
B.4.1.2	上記内容で、当センター担当者が了承の下「×(未稼働)」としたものは、了承者およびその経緯が確認できる会議議事録等の補足資料を併せて提示すること。	○
B.4.1.3	ネットワークの稼働状況の検収にあたり、システム概要をよく理解しているSEが同席してネットワークの説明を行い、確認作業の支援を行うこと。	○
B.4.1.4	ネットワークの外観や操作により稼働確認が行えない技術要件は、当センターから根拠資料の追加提示を求める場合があるため、必要な資料を準備して提出すること。	○
B.4.1.5	技術要件を満たしていない項番に対しては、その対応をいつまでに行うかを回答すること。	○

項番	機能要件	配点
C	ネットワーク	—
C.1	ネットワーク構成設計上の基本要件	—
C.1.1	基本要件	—
C.1.1.1	本ネットワークは総合医療情報システム（電子カルテや部門システム）が稼働する診療系ネットワークとインターネット接続が可能なインターネット系のネットワークに分離し、適切な通信制御を行うこと。	○
C.1.1.2	物理的には1つのネットワーク上に各系統のネットワークを構築すること。	○
C.1.1.3	各系統は論理的に分離され、各系統間の通信制御はアクセスコントロールリストによる制御ではなくルーティングテーブルの分離の仕組みを用いること。	○
C.1.1.4	ネットワークスイッチは、コアスイッチ、フロアスイッチ、エッジスイッチまたはPoEスイッチで構成される3階層構成であること。ただし、3階層が必要でない判断できる箇所は、病院と協議の上、2階層も可とする。	●
C.1.1.5	コアスイッチとフロアスイッチ間は光ケーブル接続とすること。エッジスイッチと情報コンセントまでのUTPケーブルは流用すること。	○
C.1.1.6	コアスイッチとフロアスイッチ間の接続は1Gbps以上かつ冗長化構成とすること。その他各機器間の通信帯域は現状と同等以上とすること。	○
C.1.1.7	フロアスイッチとPoEスイッチ間は1Gbps以上の回線で冗長構成とすること。	○
C.1.1.8	各系統で無線LANを提供するための無線アクセスポイントを設置すること。	○
C.1.1.9	無線LANシステムは無線LANコントローラーによる集中管理型とすること。	○
C.1.1.10	無線アクセスポイントへの給電はPoEスイッチからの給電もしくはパワーインジェクタによる給電とすること。	○
C.1.1.11	各フロアに設置する無線アクセスポイントは1台で各ネットワーク系の通信を実現し、かつセキュリティを確保できること。 ※セキュリティを確保するとは、無線アクセスポイントを共有しても異なる系統間の端末が通信できない状態を表す。	○
C.1.1.12	診療系ネットワークシステムでサーバ室及び各EPSに設置する機器は、無停電電源装置に接続すること。無停電電源装置はネットワーク接続し監視すること。	○
C.1.1.13	ネットワークの可用性及び拡張性を考慮して、コアスイッチは、2台以上でのスタック構成とすること。また、コアスイッチについては筐体内で電源部を2重化すること。サーバスイッチ、フロアスイッチは、筐体を2重化すること。なお、フロアスイッチに関しては影響範囲を鑑み、筐体2重化が必須でない箇所については、病院と協議の上、冗長化構成でなくても可とする。	●
C.1.1.14	コアスイッチ、サーバスイッチ、フロアスイッチの冗長化は、複数の筐体を論理的に1台に見せるスタック構成とすること。	○
C.1.1.15	ネットワークの可用性及び拡張性を考慮して、無線LANコントローラ、認証装置は筐体を2重化すること。ただし、業務通信に影響が出ない場合はこの限りではない。	○
C.1.1.16	当センターが利用する電子カルテシステムで検証済みのネットワーク機器を選定すること。	○
C.1.1.17	ネットワークに接続できる無線端末は許可された端末であること。	○
C.1.1.18	導入以降に機器は増加するものと考え、IPアドレスに十分な余裕を持たせること。	○
C.1.1.19	ネットワークの導入に際しては、現場業務に支障をきたさないよう、職員との打合せを実施し、スムーズな構築を図ること。	○
C.1.1.20	現行のサーバ室を継続で利用する前提で構築を行うこと。	○
C.1.1.21	診療系ネットワーク構築は、統一したネットワーク構築とし、部門システム独自のローカルネットワーク構築等は行わないこと。	○
C.1.1.22	納品する機器は、最新のOS・ファームウェアで設定を行い、検証後に導入すること。	○
C.1.2	セキュリティ	—
C.1.2.1	本ネットワークの有線、無線に接続するパソコン、医療機器等のすべてのデバイスはネットワーク認証をして接続を許可すること。	○
C.1.2.2	総合医療情報システムの無線端末は、あらかじめ許可されたネットワーク系統のみに接続を可能とすること。	○
C.1.2.3	総合医療情報システムの端末を認証するためのデータベースとして、認証サーバの構築を設計に含むこと。なお、認証等に必要なライセンス等についても費用に含めること。	○
C.1.2.4	医療情報システムの無線端末のネットワーク認証はIEEE802.1x(電子証明書)や、MACアドレス認証が実現可能なこと。	○
C.1.3	プロジェクト管理要件	—
C.1.3.1	本業務にあたっては、適正なプロジェクト管理を実施すること。	○
C.1.3.2	契約後速やかにプロジェクト計画書を提出すること。	○
C.1.3.3	本仕様書に定める設計構築業務におけるスケジュールと進捗管理方法にもとづく進捗管理を実施すること。	○
C.1.3.4	本業務に当たっては、必要なスキルを有する要員を配置すること。	○
C.1.3.5	スケジュールはWBSを作成し、作業内容について明らかにすること。	○
C.1.3.6	原則として各作業について計画工数を明示し、作業までの連絡体制および、作業時の連絡体制表を事前に提出すること。	○
C.1.3.7	本プロジェクト遂行における課題やスケジュール、各種承認事項等のやり取りに進捗会議を設けて行うこと。	○
C.1.3.8	本ネットワークの契約期間中、稼働期間中は月1回を原則として当センター指定の場所で定期的に連絡会議を行うこと。なお具体的開催日時は当センター担当者と協議を行い決定すること。	○
C.1.3.9	進捗会議の議事録は受注者にて作成し、会議開催後5営業日以内に当センターへ提示すること。	○
C.1.3.10	本業務とは別に電子カルテ側プロジェクト、当センター全体のプロジェクトにおいて必要に応じて会議に参加し報告を行うこと。	○
C.1.4	設計構築要件	—
C.1.4.1	本仕様に沿って要件定義を行うこと。	○

C.1.4.2	ネットワーク基本設計を行うこと。基本設計では物理設計、論理設計、冗長設計、無線LAN設計、監視設計、移行設計、運用設計を行うこと。	○
C.1.4.3	ネットワーク詳細設計を行うこと。詳細設計では導入するシステムのパラメータ設計をおこなうこと。	○
C.1.4.4	詳細設計に従い、機器の構築を行うこと。	○
C.1.4.5	構築では、単体試験、結合試験、総合試験を行い、試験成績書を提出すること。	○
C.1.5	システムベンダとの連携に関する要件	—
C.1.5.1	診療系ネットワークに電子カルテ及び部門システムが接続される。各システムが確実に接続できるように支援を行うこと。	○
C.1.5.2	電子カルテシステムベンダー及び部門システムベンダーへネットワークに関する要望をヒアリングし、各ベンダの要求する診療系ネットワークを準備すること。	●
C.1.5.3	総合医療情報システムのリハーサル及び本番切り替え時にネットワークベンダとして立ち合い、必要な対処を行うこと。	●
C.1.5.4	システムベンダと連携して行う作業費用については本調達に含めること。	●
C.1.5.5	電子カルテシステム、部門システムの要件に変更が発生した場合はそれに伴う費用も電子カルテシステムベンダー、部門システムベンダーと調整のうえ積算し本調達に含めること。	●
C.1.6	教育要件	—
C.1.6.1	本業務で導入する診療系ネットワークシステムについて設計書を用いて情報システム部門管理者への説明会を実施すること。	○
C.1.6.2	説明会では運用管理マニュアルや実機を用いて説明すること。	○
C.1.6.3	情報システム部門管理者宛に説明会を実施すること。	○
C.2	ネットワーク工事の作業範囲	—
C.2.1	ネットワークシステムに関わる工事の作業範囲について、以下のとおりとする。	—
C.2.1.1	LAN幹線系配線工事(既設配線の不足箇所のみで、既設利用前提) 必ず下見を申し入れ入札前に行い、不足箇所があった際には新規配線費用についても本調達に含めること。	○
C.2.1.2	LAN支線系配線工事(既設配線の不足箇所のみで、既設利用前提) 必ず下見を申し入れ入札前に行い、不足箇所があった際には新規配線費用についても本調達に含めること。	○
C.2.1.3	LANケーブル成端(フルーク試験含む)	○
C.2.1.4	無線LAN設備工事(AP設置施工配線等)	○
C.2.1.5	サーバ室内ネットワーク機器用電源の二次側工事	○
C.2.1.6	サーバ室に設置するネットワーク機器用のネットワークラックの設置工事 既設流用でも可とするが、必ず事前下見を入札前に行い、当センターの承認を得ること。また、流用するに伴い、ラックを空ける為に現行機器の移動等の必要がある場合は、提案者側で対応すること。	○
C.2.1.7	新サーバスイッチ～各サーバまでの配線工事 既設流用でも可とするが、必ず事前下見を入札前に行い、当センターと協議し、承認を得ること。	○
C.3	ネットワーク構成	—
C.3.1	ネットワーク構成機器	—
C.3.1.1	診療系ネットワークの提案に際しては、以下の製品構成を「基準」とする。ネットワークシステム全体として下記で示す機器をシステムの安定稼働に必要な数備えること。	●
C.3.1.2	「別紙.ネットワーク構成図・配置図等」に現行状況に関して提示できる範囲で資料を提示している為、それらを必ず確認した上で提案を行うこと。	○
C.3.1.3	以下に記載した1)～17)の中で、(※)に記載した項目に関しては、右記H列の「機能要件に対するコメント・変更希望理由」に提案数量を必ず記載すること。	○
C.3.1.4	保守に関しては、ネットワーク機器、保守役務含めて7年間を費用に含めること。	○
C.3.1.5	ネットワーク機器に付随するライセンスや構築、運用に必要なライセンスについては、必要分を全て本調達に含めること。	○
C.3.1.6	1) L3コアスイッチ :2台以上	○
C.3.1.7	2) サーバスイッチ① :6台 サーバスイッチ② :2台以上	○
C.3.1.8	3) フロアスイッチ① :2台 フロアスイッチ② :5台 フロアスイッチ③ :25台	○
C.3.1.9	4) PoEスイッチ① :17台 PoEスイッチ② :1台	○
C.3.1.10	5) 部門系スイッチ① :1台 部門系スイッチ② :15台 部門系スイッチ③ :2台 部門系スイッチ④ :5台 部門系スイッチ⑤ :2台	○
C.3.1.11	6) 管理棟スイッチ① :3台 管理棟スイッチ② :2台	○
C.3.1.12	7) 無停電電源装置 :必要数(※)	○
C.3.1.13	8) 無線LANコントローラー :1式(2台)	○
C.3.1.14	9) 無線LANアクセスポイント :173台	○
C.3.1.15	10) 認証サーバ :1式	○
C.3.1.16	11) インターネット系ファイアウォール :1式	○
C.3.1.17	12) 診療系ファイアウォール :1式	○
C.3.1.18	13) ネットワーク監視サーバ :1式	○
C.3.1.19	14) ネットワーク監視ソフトウェア :1式	○

C.3.1.20	15) Syslogサーバ	:1式	○
C.3.1.21	16) パトランプ	:2式	○
C.3.1.22	17) ネットワークラック	:必要数(※)	○
C.4	ネットワーク移行(切替)要件		—
C.4.1	移行要件		—
C.4.1.1	ネットワークシステムの移行は移行前後のネットワーク構成や設計、新旧ネットワークで使われるプロトコル等十分検討したうえで実施すること。		○
C.4.1.2	総合医療情報システム更新前にネットワーク機器の更新を終わらせること。		○
C.4.1.3	ネットワーク切替えに伴う現行ネットワークの停止時間帯等を含めた切替計画は、本番移行の3か月以上前には当センターと合意すること。		○
C.4.1.4	ネットワーク移行に伴い、受注者は他施設における対応事例を複数提示し、当センターの切替運用計画の立案を支援し、スムーズな移行となるよう十分に協力すること。		○
C.4.1.5	ネットワーク移行までに当センターで事前に検討や準備をすべき重要ポイントを資料に記載し、提出すること。		○
C.4.1.6	電子カルテシステムと部門システムの通信の確認を行うこと。通信の確認にて電子カルテシステムベンダーおよび部門システムベンダー側に発生する作業費用に関しては、電子カルテベンダーから取得し、見積を本調達に含むこと。		●
C.4.1.7	システム更新前においては、稼働中の総合医療情報システム(医事等の電子カルテを含む)及び、各部門サーバのネットワーク接続要件を満たすこと。接続に伴い発生する既設システム側の作業費用は、電子カルテベンダーから取得し、見積を本調達に含むこと。		●
C.4.1.8	電子カルテシステム及びそれに連携する部門システム側の動作確認において、ネットワークシステム側に不具合が認められた場合は速やかに調査及び対応をすること。その際に必要な費用については見積に含むこと。		●
C.4.1.9	ネットワーク移行時は極力通信断が発生しない方法で移行すること。通信が発生する場合でもできる限り短い時間になるように設計すること。		○
C.4.1.10	ネットワーク移行時に当センター職員や電子カルテ等の総合医療情報システムに影響がある場合は速やかに提示すること。		○
C.4.1.11	ネットワーク移行に関しては既存ネットワーク構築業者と十分な協議の上、具体的な移行計画を提出すること。また、その費用も見積に含むこと。		●
C.4.1.12	ネットワーク移行作業時に必要になる既存ネットワークの設定変更等は既設業者にて行うこと。また、その費用も見積に含むこと。		●
C.4.1.13	新ネットワークでも引き継ぐ必要のあるデータは移行作業をすること。また、既設業者に必要な作業がある場合は、その費用も見積に含むこと。		●
C.5	ネットワーク保守要件		—
C.5.1	保守構成		—
C.5.1.1	ネットワークに関する保守は以下の通りとすること。		○
C.5.1.2	1) L3コアスイッチ	:24時間365日オンサイト保守7年分(原則4時間以内駆け付け)	○
C.5.1.3	2) サーバスイッチ	:24時間365日オンサイト保守7年分(原則4時間以内駆け付け)	○
C.5.1.4	3) フロアスイッチ	:24時間365日オンサイト保守7年分(原則4時間以内駆け付け)※運用上支障がなければ、予備機運用でも良いが、適切な予備機提案を行うこと。	○
C.5.1.5	4) PoEスイッチ	:24時間365日オンサイト保守7年分(原則4時間以内駆け付け)※運用上支障がなければ、予備機運用でも良いが、適切な予備機提案を行うこと。	○
C.5.1.6	5) 部門系スイッチ	:24時間365日オンサイト保守7年分(原則4時間以内駆け付け)※運用上支障がなければ、予備機運用でも良いが、適切な予備機提案を行うこと。	○
C.5.1.7	6) 管理棟スイッチ	:24時間365日オンサイト保守7年分(原則4時間以内駆け付け)※運用上支障がなければ、予備機運用でも良いが、適切な予備機提案を行うこと。	○
C.5.1.8	7) 無停電電源装置	:平日8:30～17:30のオンサイト保守7年分	○
C.5.1.9	8) 無線LANコントローラー	:平日8:30～17:30のオンサイト保守7年分	○
C.5.1.10	9) 無線LANアクセスポイント	:平日8:30～17:30のオンサイト保守7年分※運用上支障がなければ、予備機運用でも良いが、適切な予備機提案を行うこと。	○
C.5.1.11	10) 認証サーバ(同等機能を有していれば、代替提案でも可とする)	:24時間365日オンサイト保守7年分 (メーカー保守/7年分のライセンス含む)	○
C.5.1.12	11) インターネット系ファイアウォール	:24時間365日オンサイト保守5年分	○
C.5.1.13	12) 診療系ファイアウォール	:24時間365日オンサイト保守5年分	○
C.5.1.14	13) ネットワーク監視サーバ	:平日8:30～17:30のオンサイト保守7年分 OSについては平日8:30～17:30製品問合せ7年分	○
C.5.1.15	14) ネットワーク監視ソフトウェア	:平日8:30～17:30製品問合せ7年分	○
C.5.1.16	15) Syslogサーバ	:平日8:30～17:30のオンサイト保守7年分	○
C.5.1.17	16) パトライト	:スポット対応	○
C.5.1.18	17) ネットワークラック	:不要	○
C.5.2	基本要件		—
C.5.2.1	24時間365日、診療系ネットワークの死活監視を行い、保守対応を行う部門へエスカレーションを行うこと。		○
C.5.2.2	監視を行うセンターは、情報セキュリティマネジメントシステム(ISMS)の国際標準規格「ISO 27001:2022」を取得していること。		○
C.5.2.3	監視を行うセンターは、自治体(都道府県・市区町村)、もしくは病院(都道府県・市区町村)において十分な運用実績があること(50団体、もしくは50病院以上)。		○
C.5.2.4	監視によりハードウェアの障害を検知した場合は、あらかじめ決められた部門へ連絡すると同時に保守対応を開始し、原則として当日対応ができること。		○

C.5.2.5	故障対応は、受注者が指定する保守会社が回復までの作業を一貫して行うことができるサービス体制を整えていること。	○
C.5.2.6	ネットワーク機器については、原則として専任担当者にて障害対応が可能であること。	○
C.5.2.7	診療系ネットワークの24時間365日安定稼働と継続的なサポートを確保するため導入するハードウェア、ソフトウェアの保守作業ができること。	○
C.5.2.8	保守業務に当たっては当センター職員と円滑な協力体制を構築できること。	○
C.5.2.9	保守作業は、システムに故障や動作不良が発生した際に、障害箇所の特定、機器交換、テクニカルサポートといった様々な手段でシステムのダウンタイムを低減し、システムの可用性を向上できること。	○
C.5.2.10	障害時の連絡対応、当センターからの連絡により迅速に対応できること。	○
C.5.2.11	不良部位の切り分け及び交換を行うとともに、必要に応じてファームウェア、ソフトウェア(事業者作業分)の回復および疎通確認及び、設定内容の変更を実施できること。	○
C.5.2.12	障害時の切り分けのため当センター職員が行う作業がある場合は、その手順を提示できること。	○
C.5.2.13	障害事象に関する対象機器の情報から、過去の発生事例や既知の問題を調査し、ナレッジによる解決策を提示できること。	○
C.5.2.14	導入するハードウェア、ソフトウェアの保守窓口は受注者の保守センターで一括管理できること(窓口を1本化できること)。	○
C.5.2.15	保守センターは24時間365日電話もしくはメール対応できること。	○
C.5.2.16	障害発生時は、保守窓口での対応を基本とするが、設計・構築担当技術者及び営業担当者も連携して障害対応に当たることができること。	○
C.5.2.17	ネットワーク構築事業者が保守対応もできること。	○
C.5.2.18	契約期間中は修理可能な製品を納品すること。	○
C.5.2.19	ネットワークの運用に関する消耗品・定期交換品・作業費等の必要経費(いわゆるランニングコスト)を試算し、具体的に記載して提出すること。	○
C.6	ファイアウォール運用	—
C.6.1	基本要件	—
C.6.1.1	本調達にて導入するファイアウォール機器について、以下に記載の運用を受注者にて対応し、対応費用も本調達に含めること。	○
C.6.1.2	全ての対象システムのプログラムのバージョンの管理を行うために、適切なツールを準備し全ての対象システムを登録すること。	○
C.6.1.3	修正プログラム適用をリモートで実施する場合、事前にリモートメンテナンス設備を現地に設置して接続確認を行うこと。	○
C.6.1.4	修正プログラム適用をリモートで実施する場合のリモートメンテナンス設備は、閉域網で接続すること。	○
C.6.1.5	適切なツールを利用し、全ての対象システムのプログラムのバージョンの管理を行うこと。	○
C.6.1.6	対象システムの製造元、CVE情報、JVN、JPCERT/CC、US-CERTから脆弱性および対応方法の情報を収集すること。	○
C.6.1.7	対象システムに関する脆弱性情報を確認した際、重大度を分類し、一定以上の重大度の場合、脆弱性情報の内容を通知すること。	○
C.6.1.8	修正プログラム適用の要望を受けたら、重大度に応じて作業日程を調整し、対象システムに対し修正プログラムを適用すること。	○
C.6.1.9	修正プログラムを適用したあと、業務確認で不具合が見受けられた場合、切り戻し作業を実施すること。	○
C.6.1.10	当センターで導入した機器について、修正プログラム適用の失敗等で機器に不具合が発生した場合、保守対応を実施すること。	○
C.7	リモート保守運用	—
C.7.1	基本要件	—
C.7.1.1	総合医療情報システム(電子カルテシステム、医事会計システムおよび各部門システム含む)のリモート保守構築作業は、ネットワーク構築業者が構築を行うこと。	○
C.7.1.2	リモート保守構築範囲として、「別紙. ネットワーク構築・配置図等」に本調達範囲を記載しているので、事前に確認を行い、総合医療情報システム提案ベンダ(電子カルテシステム、医事会計システムおよび各部門システム含む)と入札前に必ず1回以上の打合せを行った上で提案を行うこと。なお、費用は必要となる端末(踏み台等)・機器費用と稼働後7年間分の運用・回線費用を含めること。また、ネットワーク側の費用と総合医療情報システム提案ベンダ側の対応費用も本調達に含めること。	●
C.7.1.3	「別紙. ネットワーク構築・配置図等」には、「本調達外」と記載されているが、今回のネットワーク更新を機に「本調達外」のシステムのリモート保守構築をあらためて行い、「本調達対応」と「本調達外」を含めたリモート保守構築の一本化を行った場合に、「本調達対応」のみの費用、機器構成に対して、追加で必要な構築費用、追加で必要な機器構成(踏み台、NW機器等)を備考欄に記載すること。ネットワーク側の費用と「本調達内」と「本調達外」のシステムベンダ側の対応費用も本調達に含めること。	●
C.7.1.4	原則として当センターが指定する外部接続基盤(病院専用VPN、または自治体共通のセキュリティ基盤等)を介して行うように構築を行うこと。なお、当センターの許可なく当該基盤を介さない接続を行い、情報漏洩や不正アクセス等のセキュリティ事故が発生し、当センターの業務に支障が生じた場合、受注者はその復旧および損害賠償を含め、一切の責任を負うものとする。また、接続にあたっては「医療情報システムの安全管理に関するガイドライン」を遵守し、接続履歴(ログ)の保存および当センターへの報告を行うこと。	●
C.7.1.5	当センターの運用ルールを理解した上で当センター用のシステムベンダー保守運用ルールを策定し、当センターの承認を得ること。なお、各システムベンダーへの周知は受注者が行うこと。	●
C.7.1.6	リモート保守は、ランサムウェアを含むコンピュータウイルス等の脅威に対応した機器・システムを使用し、常にアップデートすること。(年2回でも可とする)	○
C.7.1.7	VPN装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、セキュリティパッチ(最新のファームウェアや更新プログラム等)を迅速に適用し、排除すること。	○

C. 7. 1. 8	委託業者とのシステム連携がある場合、セキュリティ管理体制を確認できるようにし、関連システムおよび委託業者とのネットワーク接続点（特にインターネットとの接続点）の脆弱性対策を実施し、当センターの承認を得ること。	○
C. 7. 1. 9	リモートメンテナンスは、原則として、都度、当センターの許可を得て行うこと。また、緊急あるいは頻回のリモートメンテナンスが必要な場合は定期的にその作業内容について当センターへ報告すること。	○
C. 8	運用（その他）	—
C. 8. 1	基本要件	—
C. 8. 1. 1	以下の運用業務を実施できること。なお、フロアのレイアウト変更に伴う大量の端末変更や、設計変更が必要になる変更については別途作業を手配するため対象外とする。	○
C. 8. 1. 2	電子カルテシステムや部門システム用端末、インターネット接続端末等の接続変更、追加時のアクセススイッチのVLANアサイン変更作業ができること（VLANアサイン変更に伴うコアスイッチ、フロアスイッチの変更を含む）。	●
C. 8. 1. 3	医療ガイドラインに則した対策を随時追加提案できること。	○
C. 9	機能要件	—
C. 9. 1	L3コアスイッチ	—
C. 9. 1. 1	以下、仕様を満たすL3コアスイッチを2台以上用意すること。	○
C. 9. 1. 2	2160.0 Gbps以上のスイッチング容量を持つこと。	○
C. 9. 1. 3	1,000Mpps以上の転送レートを持つこと。	○
C. 9. 1. 4	80K以上のMACアドレスを保持できること。	○
C. 9. 1. 5	16K以上のIPルート情報を保持できること。	○
C. 9. 1. 6	80K 以上のARP情報を保持できること。	○
C. 9. 1. 7	SFP+ (10G) スロットを48スロット標準搭載すること。	○
C. 9. 1. 8	SFP+ (10G) スロットは、1000BASE-T/SX/LX/ZX/BX SFP トランシーバ、10GBASE-T/SR/LR SFP+ トランシーバをサポートすること。	○
C. 9. 1. 9	QSFP28 (100G) スロットを4スロット以上標準搭載すること。	○
C. 9. 1. 10	QSFP28 (100G) スロットは、100GBASE-SR4/LR4 QSFP28 トランシーバをサポートすること。	○
C. 9. 1. 11	マネージメントポート（ファームウェアや設定ファイルを転送したり、SNMPで情報を取得する目的で使用する管理用Ethernetポート）を標準搭載すること。	○
C. 9. 1. 12	2台以上でのスタック接続に対応可能であること。	○
C. 9. 1. 13	QSFP28 (100GbE) にてスタック接続可能であること。	○
C. 9. 1. 14	スタック接続ケーブルに関して光ケーブル、もしくは専用スタックケーブルが接続可能であること。	○
C. 9. 1. 15	スタック接続ケーブルが完全に切断されてしまう障害が発生した場合に、複数の同一設定装置がネットワーク上に出現することになり、アドレス重複障害や通信障害が発生する。これを防ぐ機能を有すること。	○
C. 9. 1. 16	スタック接続時にスタックメンバー各装置のソフトウェアバージョンアップを行う際、通信停止時間を最小限に抑えつつ、スタック構成を組んだままバージョンアップできる機能を有すること。	○
C. 9. 1. 17	タグVLAN (IEEE802. 1Q) に対応していること。	○
C. 9. 1. 18	Voice VLANに対応していること。	○
C. 9. 1. 19	VLANマッピング、QinQ (802. 1Q-in-802. 1Q) に対応していること。	○
C. 9. 1. 20	最大4094のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 1. 21	2048VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 1. 22	標準搭載ポートは、Auto Negotiationに対応し、速度、全二重の固定設定が可能なこと。	○
C. 9. 1. 23	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 1. 24	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 1. 25	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 1. 26	最大9,000byte以上のジャンプフレームに対応可能であること。	○
C. 9. 1. 27	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能（ループ検出機能）を有すること。	○
C. 9. 1. 28	片方向リンクの発生（例えば光ファイバペアケーブルの一本が断線等）を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 1. 29	複数の物理リンクを束ねて1つの論理リンクとして扱う技術（リンクアグリゲーション）を有すること。Link Aggregation Control Protocol (IEEE802. 3ad) に対応していること。	○
C. 9. 1. 30	スパンニングツリー (IEEE802. 1d)、ラピッドスパンニングツリー (IEEE802. 1w)、MSTP (IEEE802. 1s)、VLAN毎に動作するスパンニングツリー (PVST+) に対応していること。	○
C. 9. 1. 31	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。 リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 1. 32	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 1. 33	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 1. 34	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 1. 35	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 1. 36	ローカルデータベースによる認証が可能なこと。	○
C. 9. 1. 37	STATIC/RIP (RIP v1/v2/ng) /OSPF (OSPF v2/v3) /BGP (BGP4/4+) ルーティング機能を有すること。	○
C. 9. 1. 38	ポリシーベースルーティング機能を有すること。	○
C. 9. 1. 39	VRRP機能を有すること。	○

C.9.1.40	BFD機能を有すること。	○
C.9.1.41	VRF-Lite(Virtual Routing and Forwarding)機能を有すること。	○
C.9.1.42	マルチキャストVLAN機能を有すること。	○
C.9.1.43	IGMP v1/v2/v3機能、IGMP v1/v2/v3スヌーピング機能を有すること。	○
C.9.1.44	MLD v1/v2機能、MLD v1/v2スヌーピング機能を有すること。	○
C.9.1.45	マルチキャストルーティングプロトコルPIM-SM、PIM-SSMをサポートすること。	○
C.9.1.46	VXLAN機能を有すること。	○
C.9.1.47	コンソールポート(CLI)による設定、状態確認が可能であること。	○
C.9.1.48	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C.9.1.49	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C.9.1.50	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C.9.1.51	NTPクライアント、NTPサーバ機能を有すること。	○
C.9.1.52	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C.9.1.53	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C.9.1.54	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C.9.1.55	RMONv1エージェント機能を有すること。	○
C.9.1.56	sFlowエージェント、もしくはNetFlowエージェント機能を有すること。	○
C.9.1.57	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C.9.1.58	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C.9.1.59	質量が17kg以下であること。	○
C.9.1.60	AC電源搭載時、90~264Vでの動作が可能であること。	○
C.9.1.61	電源の2重化が可能であること。電源を2重化しても装置が19インチラック3U以内に収まること。	○
C.9.1.62	AC最大消費電力が、1130W以下であること。	○
C.9.1.63	温度 0~45℃で動作すること。	○
C.9.1.64	19インチラック搭載金具が標準添付であること。	○
C.9.1.65	USBメモリにコンフィグやソフトウェアを保存できること。	○
C.9.1.66	VCCIクラスA、RoHS指令に対応していること。	○
C.9.1.67	L3コアシッチの拡張オプションとして、以下に記載の製品を手配すること。	○
C.9.1.68	銅線ケーブル(3m)を計6個用意すること。なお、必要に応じて長さや個数は変更可とする。	○
C.9.1.69	1port 1GBASE-SR SFP+(MM, LC)を計16個以上用意すること。	○
C.9.1.70	1port 1000BASE-SX SFP (MM, LC)を計71個以上用意すること。	○
C.9.1.71	1port 1000BASE-T SFP (RJ-45)を計2個以上用意すること。	○
C.9.2	サーバスイッチ①	—
C.9.2.1	以下、仕様を満たすサーバスイッチを6台用意すること。	○
C.9.2.2	176.0Gbps以上のスイッチング容量を持つこと。	○
C.9.2.3	130.9Mpps以上の転送レートを持つこと。	○
C.9.2.4	16,000以上のMACアドレスを保持できること。	○
C.9.2.5	512以上のIPルート情報を保持できること。	○
C.9.2.6	1,000以上のARP情報を保持できること。	○
C.9.2.7	10/100/1000BASE-Tポートを48ポート標準搭載すること。	○
C.9.2.8	SFP+スロットを4スロット標準搭載すること。	○
C.9.2.9	SFP+スロットは、1000BASE-T/SX/LX/BX SFPトランシーバ、10GBASE-T/SR/LR/ER SFP+トランシーバをサポートすること。	○
C.9.2.10	6台までのスタック接続に対応可能であること。	○
C.9.2.11	スタック接続ケーブルが完全に切断されてしまう障害が発生した場合に、複数の同一設定装置がネットワーク上に出現することになり、アドレス重複障害や通信障害が発生する。これを防ぐ機能を有すること。	○
C.9.2.12	タグVLAN(IEEE802.1Q)に対応していること。	○
C.9.2.13	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C.9.2.14	Voice VLANに対応していること。	○
C.9.2.15	VLANマッピング、QinQ(802.1Q-in-802.1Q)に対応していること。	○
C.9.2.16	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C.9.2.17	32VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C.9.2.18	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C.9.2.19	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C.9.2.20	フローコントロール(IEEE802.3X)を有すること。	○
C.9.2.21	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C.9.2.22	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C.9.2.23	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C.9.2.24	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C.9.2.25	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C.9.2.26	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol(IEEE802.3ad)に対応していること。	○
C.9.2.27	スパニングツリー(IEEE802.1d)、ラピッドスパニングツリー(IEEE802.1w)、MSTP(IEEE802.1s)、VLAN毎に動作するスパニングツリー(Per VLAN スパニングツリー)に対応していること。	○

C. 9. 2. 28	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。 リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。もしくは、高速経路切替が可能な冗長化プロトコル（REP等）を有する形でも可とする。	○
C. 9. 2. 29	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 2. 30	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 2. 31	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 2. 32	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 2. 33	輻輳制御として、Strict Priority Queueing (SP)、Weighted Round Robin (WRR) を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 2. 34	IEEE802. 1X認証/MAC認証/WEB認証/マルチステップ認証に対応のこと。	○
C. 9. 2. 35	ダイナミックVLANによるVLAN付与 (Port based/MAC based) に対応できること。	○
C. 9. 2. 36	ポートセキュリティ機能に対応のこと。	○
C. 9. 2. 37	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 2. 38	マルチキャストVLAN機能を有すること。	○
C. 9. 2. 39	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 2. 40	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 2. 41	コンソールポート (CLI) による設定、状態確認が可能であること。	○
C. 9. 2. 42	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 2. 43	GUI (WEB Console) による設定が可能であること。	○
C. 9. 2. 44	FTP/TFTPクライアントを有すること。	○
C. 9. 2. 45	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 2. 46	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C. 9. 2. 47	NTPクライアント、NTPサーバ機能を有すること。	○
C. 9. 2. 48	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 2. 49	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 2. 50	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 2. 51	RMONエージェント機能を有すること。	○
C. 9. 2. 52	sFlowエージェント機能を有すること。もしくは、NetFlow、IPFIX、または同等のトラフィック解析機能を有する形でも可とする。	○
C. 9. 2. 53	ポートミラーリング機能 (モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能) を有すること。	○
C. 9. 2. 54	Energy Efficient Ethernet (IEEE802. 3az) 機能を有すること。	○
C. 9. 2. 55	外形寸法 (Width x Depth x Height) が、19インチラックに収まること。	○
C. 9. 2. 56	質量が6. 3kg以下であること。	○
C. 9. 2. 57	AC電源を内蔵し、90～264Vでの動作が可能であること。	○
C. 9. 2. 58	最大消費電力が、487W以下であること。	○
C. 9. 2. 59	温度 0～45℃で動作すること。	○
C. 9. 2. 60	19インチラック搭載金具を標準添付すること。	○
C. 9. 2. 61	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 2. 62	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に無償にて代替品と交換する形でも可とする。	○
C. 9. 2. 63	サーバスイッチ①の拡張オプションとして、以下に記載の製品を手配すること。	○
C. 9. 2. 64	SFP+銅線ケーブル (1m) を計6個用意すること。	○
C. 9. 2. 65	1port 1GBASE-SR SFP+ (MM, LC) を計6個以上用意すること。	○
C. 9. 3	サーバスイッチ②	—
C. 9. 3. 1	以下、仕様を満たすサーバスイッチを2台以上用意すること。	○
C. 9. 3. 2	320. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 3. 3	238. 0Mpps以上の転送レートを持つこと。	○
C. 9. 3. 4	32, 000以上のMACアドレスを保持できること。	○
C. 9. 3. 5	100/1/2. 5/5/10GBASE-Tポートを14ポート標準搭載すること。もしくは、10GBASE-Tポートを48ポート標準搭載すること。	○
C. 9. 3. 6	SFP+スロットを2スロット以上を標準搭載すること。	○
C. 9. 3. 7	SFP+スロットは、1000BASE-SX/LX/ZX/BX SFPトランシーバ、10GBASE-T/SR/LR/ER SFP+トランシーバをサポートすること。もしくは、SFP+スロットは、1000BASE-SX/LX/ZX/BX SFPトランシーバ、25GGBASE-T/SR/LR/ER SFP+トランシーバをサポートすること。	○
C. 9. 3. 8	2台までのスタック接続に対応可能であること。	○
C. 9. 3. 9	スタック接続ケーブルが完全に切断されてしまう障害が発生した場合に、複数の同一設定装置がネットワーク上に出現することになり、アドレス重複障害や通信障害が発生する。これを防ぐ機能を有すること。	○
C. 9. 3. 10	スタック接続時にスタックメンバー各装置のソフトウェアバージョンアップを行う際、通信停止時間を最小限に抑えつつ、スタック構成を組んだままバージョンアップできる機能を有すること。	○
C. 9. 3. 11	タグVLAN (IEEE802. 1Q) に対応していること。	○
C. 9. 3. 12	プロトコルVLANに対応していること。もしくは、MACベースや802. 1XなどのダイナミックVLANを有していること。	○
C. 9. 3. 13	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○

C. 9. 3. 14	Voice VLANに対応していること。	○
C. 9. 3. 15	VLANマッピング、QinQ(802.1Q-in-802.1Q)に対応していること。	○
C. 9. 3. 16	最大1000のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 3. 17	1024VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。もしくは、設定可能なSVI (VLANインターフェース) の最大数は 1000まで行える形でも可とする。	○
C. 9. 3. 18	標準搭載ポートは、Auto Negotiationに対応し、速度、全二重の固定設定が可能なこと。	○
C. 9. 3. 19	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 3. 20	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 3. 21	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 3. 22	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 3. 23	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 3. 24	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 3. 25	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 3. 26	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol (IEEE802.3ad)に対応していること。	○
C. 9. 3. 27	スパニングツリー(IEEE802.1d)、ラピッドスパニングツリー(IEEE802.1w)、MSTP(IEEE802.1s)、VLAN毎に動作するスパニングツリー(Per VLAN スパニングツリー)に対応していること。	○
C. 9. 3. 28	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 3. 29	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 3. 30	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 3. 31	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrustが可能なこと。	○
C. 9. 3. 32	輻輳制御として、Strict Priority Queueing(SP)、Weighted Round Robin(WRR)を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 3. 33	IEEE802.1X認証/MAC認証/WEB認証に対応のこと。	○
C. 9. 3. 34	ダイナミックVLANによるVLAN付与(Port based/MAC based)に対応できること。	○
C. 9. 3. 35	ポートセキュリティ機能に対応のこと。	○
C. 9. 3. 36	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 3. 37	STATIC/RIP(RIP v1/v2)ルーティング機能を有すること。	○
C. 9. 3. 38	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 3. 39	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 3. 40	クラウド型、もしくはオンプレミス型の統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 3. 41	コンソールポート(CLI)による設定、状態確認が可能であること。	○
C. 9. 3. 42	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 3. 43	FTP/TFTPクライアントを有すること。	○
C. 9. 3. 44	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 3. 45	DHCPクライアント、DHCPスヌーピング機能を有すること。	○
C. 9. 3. 46	NTPクライアント、NTPサーバ機能を有すること。	○
C. 9. 3. 47	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 3. 48	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 3. 49	RMONエージェント機能を有すること。	○
C. 9. 3. 50	sFlow、もしくはNetFlowエージェント機能を有すること。	○
C. 9. 3. 51	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 3. 52	質量が8.25kg以下であること。	○
C. 9. 3. 53	温度 0~45℃で動作すること。	○
C. 9. 3. 54	19インチラック搭載金具を標準添付すること。	○
C. 9. 3. 55	USBメモリにコンフィグやソフトウェアを保存できること。	○
C. 9. 3. 56	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 3. 57	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 3. 58	サーバスイッチ②の拡張オプションとして、以下に記載の製品を手配すること。	○
C. 9. 3. 59	SFP+銅線ケーブル(1m)を計2個以上用意すること。また、構成上必要な場合は、1port 10GBASE-SR SFP+(MM, LC)を計4個以上用意すること。	○
C. 9. 4	フロアスイッチ①	—
C. 9. 4. 1	以下、仕様を満たすフロアスイッチを2台用意すること。	○
C. 9. 4. 2	20.0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 4. 3	14.8Mpps以上の転送レートを持つこと。	○
C. 9. 4. 4	16,000以上のMACアドレスを保持できること。	○
C. 9. 4. 5	10/100/1000BASE-Tポートを8ポート標準搭載すること。	○
C. 9. 4. 6	SFPスロットを2スロット標準搭載すること。	○
C. 9. 4. 7	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 4. 8	タグVLAN(IEEE802.1Q)に対応していること。	○

C. 9. 4. 9	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 4. 10	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 4. 11	Voice VLANに対応していること。	○
C. 9. 4. 12	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 4. 13	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 4. 14	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 4. 15	フローコントロール(IEEE802. 3X)を有すること。	○
C. 9. 4. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 4. 17	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 4. 18	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 4. 19	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 4. 20	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 4. 21	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 4. 22	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol(IEEE802. 3ad)に対応していること。	○
C. 9. 4. 23	スパニングツリー(IEEE802. 1d)、ラピッドスパニングツリー(IEEE802. 1w)、MSTP(IEEE802. 1s)、VLAN毎に動作するスパニングツリー(Per VLAN スパニングツリー)に対応していること。	○
C. 9. 4. 24	通信パケットのパケットフィルタ機能を有すること。入力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 4. 25	入力トラフィックの帯域制限が可能なこと。	○
C. 9. 4. 26	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 4. 27	輻輳制御として、Strict Priority(SP)、Weighted Round Robin(WRR)を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 4. 28	IEEE802. 1X認証に対応のこと。	○
C. 9. 4. 29	MACアドレス認証に対応のこと。	○
C. 9. 4. 30	マルチステップ認証に対応のこと。	○
C. 9. 4. 31	ダイナミックVLANによるVLAN付与(Port based/MAC based)に対応できること。	○
C. 9. 4. 32	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 4. 33	IGMPv1/v2/v3スヌーピング機能を有すること。	○
C. 9. 4. 34	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 4. 35	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 4. 36	コンソールポート(CLI)、WEBコンソール(WEB GUI)による設定、状態確認が可能であること。	○
C. 9. 4. 37	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 4. 38	GUI (WEB Console) による設定が可能であること。	○
C. 9. 4. 39	FTP/TFTPクライアント機能を有すること。	○
C. 9. 4. 40	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 4. 41	DHCPクライアント機能を有すること。	○
C. 9. 4. 42	NTPクライアント機能を有し、NTPサーバから時刻同期可能であること。	○
C. 9. 4. 43	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 4. 44	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 4. 45	RMONv1エージェント機能を有すること。	○
C. 9. 4. 46	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 4. 47	Energy Efficient Ethernet(IEEE802. 3az)機能を有すること。	○
C. 9. 4. 48	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 4. 49	質量が3. 53kg以下であること。	○
C. 9. 4. 50	AC電源を内蔵し、90~264Vでの動作が可能であること。	○
C. 9. 4. 51	壁掛け金具により、壁掛けが可能であること。	○
C. 9. 4. 52	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 4. 53	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 5	フロアスイッチ②	—
C. 9. 5. 1	以下、仕様を満たすフロアスイッチを5台用意すること。	○
C. 9. 5. 2	56Gbps以上のスイッチング容量を持つこと。	○
C. 9. 5. 3	41. 66Mpps以上の転送レートを持つこと。	○
C. 9. 5. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 5. 5	10/100/1000BASE-Tポートを48ポート標準搭載すること。	○
C. 9. 5. 6	SFPスロットを4スロット標準搭載すること。	○
C. 9. 5. 7	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 5. 8	タグVLAN(IEEE802. 1Q)に対応していること。	○
C. 9. 5. 9	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 5. 10	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 5. 11	Voice VLANに対応していること。	○
C. 9. 5. 12	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 5. 13	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○

C. 9. 5. 14	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 5. 15	フローコントロール(IEEE802. 3X)を有すること。	○
C. 9. 5. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 5. 17	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 5. 18	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 5. 19	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 5. 20	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 5. 21	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 5. 22	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol(IEEE802. 3ad)に対応していること。	○
C. 9. 5. 23	スパニングツリー(IEEE802. 1d)、ラピッドスパニングツリー(IEEE802. 1w)、MSTP(IEEE802. 1s)、VLAN毎に動作するスパニングツリー(Per VLAN スパニングツリー)に対応していること。	○
C. 9. 5. 24	通信パケットのパケットフィルタ機能を有すること。入力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 5. 25	入力トラフィックの帯域制限が可能なこと。	○
C. 9. 5. 26	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 5. 27	輻輳制御として、Strict Priority(SP)、Weighted Round Robin(WRR)を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 5. 28	IEEE802. 1X認証に対応のこと。	○
C. 9. 5. 29	MACアドレス認証に対応のこと。	○
C. 9. 5. 30	マルチステップ認証に対応のこと。	○
C. 9. 5. 31	ダイナミックVLANによるVLAN付与(Port based/MAC based)に対応できること。	○
C. 9. 5. 32	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 5. 33	IGMPv1/v2/v3スヌーピング機能を有すること。	○
C. 9. 5. 34	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 5. 35	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 5. 36	コンソールポート(CLI)、WEBコンソール(WEB GUI)による設定、状態確認が可能であること。	○
C. 9. 5. 37	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 5. 38	GUI (WEB Console) による設定が可能であること。	○
C. 9. 5. 39	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 5. 40	DHCPクライアント機能を有すること。	○
C. 9. 5. 41	NTPクライアント機能を有し、NTPサーバから時刻同期可能であること。	○
C. 9. 5. 42	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 5. 43	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 5. 44	RMONv1エージェント機能を有すること。	○
C. 9. 5. 45	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 5. 46	Energy Efficient Ethernet(IEEE802. 3az)機能を有すること。	○
C. 9. 5. 47	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 5. 48	質量が4. 53kg以下であること。	○
C. 9. 5. 49	AC電源を内蔵し、90~264Vでの動作が可能であること。	○
C. 9. 5. 50	最大消費電力が、54W以下であること。	○
C. 9. 5. 51	19インチラック搭載金具を標準添付すること。	○
C. 9. 5. 52	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 5. 53	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 6	フロアスイッチ③	—
C. 9. 6. 1	以下、仕様を満たすフロアスイッチを25台用意すること。	○
C. 9. 6. 2	104. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 6. 3	77. 3Mpps以上の転送レートを持つこと。	○
C. 9. 6. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 6. 5	64以上のIPルート情報を保持できること。	○
C. 9. 6. 6	256以上のARP情報を保持できること。	○
C. 9. 6. 7	10/100/1000BASE-Tポートを48ポート標準搭載すること。	○
C. 9. 6. 8	SFPスロットを4スロット標準搭載すること。	○
C. 9. 6. 9	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 6. 10	4台までのスタック接続に対応可能であること。もしくは、冗長化(アクティブ/スタンバイ)ができる形でも可とする。	○
C. 9. 6. 11	タグVLAN(IEEE802. 1Q)に対応していること。	○
C. 9. 6. 12	プロトコルVLANに対応していること。もしくは、MACベースや802. 1XなどのダイナミックVLANを有していることでも可とする。	○
C. 9. 6. 13	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 6. 14	Voice VLANに対応していること。	○
C. 9. 6. 15	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 6. 16	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○

C. 9. 6. 17	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 6. 18	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 6. 19	フローコントロール(IEEE802. 3X)を有すること。	○
C. 9. 6. 20	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 6. 21	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 6. 22	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 6. 23	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 6. 24	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 6. 25	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 6. 26	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol(IEEE802. 3ad)に対応していること。	○
C. 9. 6. 27	スパニングツリー(IEEE802. 1d)、ラピッドスパニングツリー(IEEE802. 1w)、MSTP(IEEE802. 1s)、VLAN毎に動作するスパニングツリー(Per VLAN スパニングツリー)に対応していること。	○
C. 9. 6. 28	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 6. 29	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 6. 30	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 6. 31	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 6. 32	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 6. 33	輻輳制御として、Strict Priority Queueing(SP)、Weighted Round Robin(WRR)を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 6. 34	IEEE802. 1X認証/MAC認証/WEB認証/マルチステップ認証に対応のこと。	○
C. 9. 6. 35	ダイナミックVLANによるVLAN付与(Port based/MAC based)に対応できること。	○
C. 9. 6. 36	ポートセキュリティ機能に対応のこと。	○
C. 9. 6. 37	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 6. 38	STATICルーティング機能を有すること。	○
C. 9. 6. 39	BFD機能を有すること。	○
C. 9. 6. 40	マルチキャストVLAN機能を有すること。もしくは、マルチキャストルーティングやスヌーピング機能を有する形で可とする。	○
C. 9. 6. 41	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 6. 42	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 6. 43	コンソールポート(CLI)による設定、状態確認が可能であること。	○
C. 9. 6. 44	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 6. 45	GUI (WEB Console) による設定が可能であること。	○
C. 9. 6. 46	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 6. 47	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C. 9. 6. 48	NTPクライアント機能を有すること。	○
C. 9. 6. 49	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 6. 50	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 6. 51	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 6. 52	RMONエージェント機能を有すること。	○
C. 9. 6. 53	sFlowエージェント機能を有すること。もしくは、NetFlow および Flexible NetFlowに対応する形で可とする。	○
C. 9. 6. 54	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 6. 55	Energy Efficient Ethernet(IEEE802. 3az)機能を有すること。	○
C. 9. 6. 56	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 6. 57	質量が5. 2kg以下であること。	○
C. 9. 6. 58	AC電源を内蔵し、90~264Vでの動作が可能であること。	○
C. 9. 6. 59	最大消費電力が、65W以下であること。	○
C. 9. 6. 60	19インチラック搭載金具を標準添付すること。	○
C. 9. 6. 61	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 6. 62	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形で可とする。	○
C. 9. 6. 63	機器の構成上、必要な場合に限り1port 1000BASE-SX SFP (MM, LC)を計35個等の適宜必要な数量を用意すること。	○
C. 9. 7	POEスイッチ①	—
C. 9. 7. 1	以下、仕様を満たすPOEスイッチを17台用意すること。	○
C. 9. 7. 2	56. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 7. 3	41. 6Mpps以上の転送レートを持つこと。	○
C. 9. 7. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 7. 5	64以上のIPルート情報を保持できること。	○

C. 9. 7. 6	256以上のARP情報を保持できること。	○
C. 9. 7. 7	10/100/1000BASE-T (PoE Plus給電対応) ポートを24ポート標準搭載すること。	○
C. 9. 7. 8	SFPスロットを4スロット標準搭載すること。	○
C. 9. 7. 9	SFPスロットは、1000BASE-SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 7. 10	PoE Plus (IEEE802. 3at) 規格に準拠し、1ポートあたり30W給電が可能であること。	○
C. 9. 7. 11	装置あたりの最大給電可能電力が370. 0W以上であること。	○
C. 9. 7. 12	S/Wバージョンアップなどの再起動時にも受電装置への給電が停止しないこと。	○
C. 9. 7. 13	4台までのスタック接続に対応可能であること。もしくは、冗長化 (アクティブ/スタンバイ) ができる形でも可とする。	○
C. 9. 7. 14	タグVLAN (IEEE802. 1Q) に対応していること。	○
C. 9. 7. 15	プロトコルVLANに対応していること。もしくは、MACベースや802. 1XなどのダイナミックVLANを有している形でも可とする。	○
C. 9. 7. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 7. 17	Voice VLANに対応していること。	○
C. 9. 7. 18	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 7. 19	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 7. 20	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 7. 21	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 7. 22	フローコントロール (IEEE802. 3X) を有すること。	○
C. 9. 7. 23	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 7. 24	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 7. 25	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 7. 26	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 7. 27	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブルードキャストストームを防止する機能 (ループ検出機能) を有すること。	○
C. 9. 7. 28	片方向リンクの発生 (例えば光ファイバペアケーブルの一本が断線等) を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 7. 29	複数の物理リンクを束ねて1つの論理リンクとして扱う技術 (リンクアグリゲーション) を有すること。Link Aggregation Control Protocol (IEEE802. 3ad) に対応していること。	○
C. 9. 7. 30	スパンニングツリー (IEEE802. 1d)、ラピッドスパンニングツリー (IEEE802. 1w)、MSTP (IEEE802. 1s)、VLAN毎に動作するスパンニングツリー (Per VLAN スパンニングツリー) に対応していること。	○
C. 9. 7. 31	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。 リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 7. 32	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 7. 33	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 7. 34	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 7. 35	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 7. 36	輻輳制御として、Strict Priority Queueing (SP)、Weighted Round Robin (WRR) を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 7. 37	ダイナミックVLANによるVLAN付与 (Port based/MAC based) に対応できること。	○
C. 9. 7. 38	ポートセキュリティ機能に対応すること。	○
C. 9. 7. 39	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 7. 40	最大2000ユーザの認証セッションを保持できること。	○
C. 9. 7. 41	STATICルーティング機能を有すること。	○
C. 9. 7. 42	マルチキャストVLAN機能を有すること。もしくは、マルチキャストルーティングやスヌーピング機能を有する形でも可とする。	○
C. 9. 7. 43	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 7. 44	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 7. 45	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 7. 46	コンソールポート (CLI) による設定、状態確認が可能であること。	○
C. 9. 7. 47	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 7. 48	GUI (WEB Console) による設定が可能であること。	○
C. 9. 7. 49	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 7. 50	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C. 9. 7. 51	NTPクライアント機能を有すること。	○
C. 9. 7. 52	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 7. 53	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 7. 54	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 7. 55	RMONエージェント機能を有すること。	○
C. 9. 7. 56	sFlowエージェント機能を有すること。もしくは、NetFlow および Flexible NetFlowに対応できる形でも可とする。	○
C. 9. 7. 57	ポートミラーリング機能 (モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能) を有すること。	○
C. 9. 7. 58	Energy Efficient Ethernet (IEEE802. 3az) 機能を有すること。	○
C. 9. 7. 59	外形寸法 (Width x Depth x Height) が、19インチラックに収まること。	○

C. 9. 7. 60	質量が6. 2kg以下であること。	○
C. 9. 7. 61	AC電源を内蔵し、90～264Vでの動作が可能であること。	○
C. 9. 7. 62	最大消費電力が、470W以下であること。	○
C. 9. 7. 63	19インチラック搭載金具を標準添付すること。	○
C. 9. 7. 64	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 7. 65	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 7. 66	機器の構成上、必要な場合に限り1port 1000BASE-SX SFP (MM, LC) を計26個等の適宜必要な数量を用意すること。	○
C. 9. 8	POEスイッチ②	—
C. 9. 8. 1	以下、仕様を満たすPOEスイッチを1台用意すること。	○
C. 9. 8. 2	104. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 8. 3	77. 3Mpps以上の転送レートを持つこと。	○
C. 9. 8. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 8. 5	64以上のIPルート情報を保持できること。	○
C. 9. 8. 6	256以上のARP情報を保持できること。	○
C. 9. 8. 7	10/100/1000BASE-T (PoE Plus給電対応) ポートを48ポート標準搭載すること。	○
C. 9. 8. 8	SFPスロットを4スロット標準搭載すること。	○
C. 9. 8. 9	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 8. 10	PoE Plus (IEEE802. 3at) 規格に準拠し、1ポートあたり30W給電が可能であること。	○
C. 9. 8. 11	装置あたりの最大給電可能電力が370. 0W以上であること。	○
C. 9. 8. 12	S/Wバージョンアップなどの再起動時にも受電装置への給電が停止しないこと。	○
C. 9. 8. 13	4台までのスタック接続に対応可能であること。もしくは、冗長化 (アクティブ/スタンバイ) ができる形でも可とする。	○
C. 9. 8. 14	タグVLAN (IEEE802. 1Q) に対応していること。	○
C. 9. 8. 15	プロトコルVLANに対応していること。もしくは、MACベースや802. 1XなどのダイナミックVLANを有している形でも可とする。	○
C. 9. 8. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 8. 17	Voice VLANに対応していること。	○
C. 9. 8. 18	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 8. 19	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 8. 20	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 8. 21	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 8. 22	フローコントロール (IEEE802. 3X) を有すること。	○
C. 9. 8. 23	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 8. 24	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 8. 25	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 8. 26	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能 (ループ検出機能) を有すること。	○
C. 9. 8. 27	片方向リンクの発生 (例えば光ファイバペアケーブルの一本が断線等) を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 8. 28	複数の物理リンクを束ねて1つの論理リンクとして扱う技術 (リンクアグリゲーション) を有すること。Link Aggregation Control Protocol (IEEE802. 3ad) に対応していること。	○
C. 9. 8. 29	スパニングツリー (IEEE802. 1d)、ラピッドスパニングツリー (IEEE802. 1w)、MSTP (IEEE802. 1s)、VLAN毎に動作するスパニングツリー (Per VLAN スパニングツリー) に対応していること。	○
C. 9. 8. 30	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。 リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 8. 31	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 8. 32	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 8. 33	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 8. 34	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 8. 35	輻輳制御として、Strict Priority Queueing (SP)、Weighted Round Robin (WRR) を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 8. 36	IEEE802. 1X認証/MAC認証/WEB認証/マルチステップ認証に対応のこと。	○
C. 9. 8. 37	ダイナミックVLANによるVLAN付与 (Port based/MAC based) に対応できること。	○
C. 9. 8. 38	ポートセキュリティ機能に対応のこと。	○
C. 9. 8. 39	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 8. 40	最大2000ユーザの認証セッションを保持できること。	○
C. 9. 8. 41	BFD機能を有すること。	○
C. 9. 8. 42	マルチキャストVLAN機能を有すること。もしくは、マルチキャストルーティングやスヌーピング機能を有する形でも可とする。	○
C. 9. 8. 43	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 8. 44	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 8. 45	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 8. 46	コンソールポート (CLI) による設定、状態確認が可能であること。	○
C. 9. 8. 47	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 8. 48	GUI (WEB Console) による設定が可能であること。	○

C. 9. 8. 49	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 8. 50	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C. 9. 8. 51	NTPクライアント機能を有すること。	○
C. 9. 8. 52	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 8. 53	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 8. 54	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 8. 55	RMONエージェント機能を有すること。	○
C. 9. 8. 56	sFlowエージェント機能を有すること。もしくは、NetFlow および Flexible NetFlowに対応できる形でも可とする。	○
C. 9. 8. 57	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 8. 58	Energy Efficient Ethernet(IEEE802.3az)機能を有すること。	○
C. 9. 8. 59	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 8. 60	質量が6.4kg以下であること。	○
C. 9. 8. 61	AC電源を内蔵し、90~264Vでの動作が可能であること。	○
C. 9. 8. 62	19インチラック搭載金具を標準添付すること。	○
C. 9. 8. 63	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 8. 64	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 8. 65	POEスイッチ②の拡張オプションとして、以下に記載の製品を目安として手配すること。	○
C. 9. 8. 66	1port 1000BASE-SX SFP (MM, LC)を計2個以上用意すること。	○
C. 9. 9	部門系スイッチ①	—
C. 9. 9. 1	以下、仕様を満たす部門系スイッチを1台用意すること。	○
C. 9. 9. 2	20.0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 9. 3	14.8Mpps以上の転送レートを持つこと。	○
C. 9. 9. 4	16,000以上のMACアドレスを保持できること。	○
C. 9. 9. 5	10/100/1000BASE-Tポートを8ポート標準搭載すること。	○
C. 9. 9. 6	SFPスロットを2スロット標準搭載すること。	○
C. 9. 9. 7	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 9. 8	タグVLAN(IEEE802.1Q)に対応していること。	○
C. 9. 9. 9	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 9. 10	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 9. 11	Voice VLANに対応していること。	○
C. 9. 9. 12	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 9. 13	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 9. 14	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 9. 15	フローコントロール(IEEE802.3X)を有すること。	○
C. 9. 9. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 9. 17	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 9. 18	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 9. 19	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 9. 20	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 9. 21	片方向リンクの発生(例えば光ファイバケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 9. 22	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol(IEEE802.3ad)に対応していること。	○
C. 9. 9. 23	スパニングツリー(IEEE802.1d)、ラピッドスパニングツリー(IEEE802.1w)、MSTP(IEEE802.1s)、VLAN毎に動作するスパニングツリー(Per VLAN スパニングツリー)に対応していること。	○
C. 9. 9. 24	通信パケットのパケットフィルタ機能を有すること。入力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 9. 25	入力トラフィックの帯域制限が可能なこと。	○
C. 9. 9. 26	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 9. 27	輻輳制御として、Strict Priority(SP)、Weighted Round Robin(WRR)を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 9. 28	IEEE802.1X認証に対応のこと。	○
C. 9. 9. 29	MACアドレス認証に対応のこと。	○
C. 9. 9. 30	ダイナミックVLANによるVLAN付与(Port based/MAC based)に対応できること。	○
C. 9. 9. 31	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 9. 32	IGMPv1/v2/v3スヌーピング機能を有すること。	○
C. 9. 9. 33	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 9. 34	クラウド型統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 9. 35	コンソールポート(CLI)、WEBコンソール(WEB GUI)による設定、状態確認が可能であること。	○
C. 9. 9. 36	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 9. 37	GUI (WEB Console) による設定が可能であること。	○

C. 9. 9. 38	FTP/TFTPクライアント機能を有すること。もしくは、TFTPクライアントやSCP等の機能を有する形でも可とする。	○
C. 9. 9. 39	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 9. 40	DHCPクライアント機能を有すること。	○
C. 9. 9. 41	NTPクライアント機能を有し、NTPサーバから時刻同期可能であること。	○
C. 9. 9. 42	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 9. 43	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 9. 44	RMONv1エージェント機能を有すること。	○
C. 9. 9. 45	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 9. 46	Energy Efficient Ethernet(IEEE802.3az)機能を有すること。	○
C. 9. 9. 47	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 9. 48	質量が3.53kg以下であること。	○
C. 9. 9. 49	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 9. 50	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 10	部門系スイッチ②	—
C. 9. 10. 1	以下、仕様を満たす部門系スイッチを15台用意すること。	○
C. 9. 10. 2	40.0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 10. 3	26.7Mbps以上の転送レートを持つこと。	○
C. 9. 10. 4	16,000以上のMACアドレスを保持できること。	○
C. 9. 10. 5	10/100/1000BASE-Tポートを16ポート標準搭載すること。	○
C. 9. 10. 6	SFPスロットを2スロット以上標準搭載すること。	○
C. 9. 10. 7	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 10. 8	タグVLAN(IEEE802.1Q)に対応していること。	○
C. 9. 10. 9	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 10. 10	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 10. 11	Voice VLANに対応していること。	○
C. 9. 10. 12	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 10. 13	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 10. 14	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 10. 15	フローコントロール(IEEE802.3X)を有すること。	○
C. 9. 10. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 10. 17	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 10. 18	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 10. 19	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 10. 20	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 10. 21	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 10. 22	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol(IEEE802.3ad)に対応していること。	○
C. 9. 10. 23	スパンニングツリー(IEEE802.1d)、ラピッドスパンニングツリー(IEEE802.1w)、MSTP(IEEE802.1s)、VLAN毎に動作するスパンニングツリー(Per VLAN スパンニングツリー)に対応していること。	○
C. 9. 10. 24	通信パケットのパケットフィルタ機能を有すること。入力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 10. 25	入力トラフィックの帯域制限が可能なこと。	○
C. 9. 10. 26	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 10. 27	輻輳制御として、Strict Priority(SP)、Weighted Round Robin(WRR)を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 10. 28	IEEE802.1X認証に対応のこと。	○
C. 9. 10. 29	MACアドレス認証に対応のこと。	○
C. 9. 10. 30	ダイナミックVLANによるVLAN付与(Port based/MAC based)に対応できること。	○
C. 9. 10. 31	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 10. 32	IGMPv1/v2/v3スヌーピング機能を有すること。	○
C. 9. 10. 33	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 10. 34	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 10. 35	コンソールポート(CLI)、WEBコンソール(WEB GUI)による設定、状態確認が可能であること。	○
C. 9. 10. 36	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 10. 37	GUI (WEB Console) による設定が可能であること。	○
C. 9. 10. 38	FTP/TFTPクライアント機能を有すること。もしくは、TFTPクライアントやSCP等の機能を有する形でも可とする。	○
C. 9. 10. 39	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 10. 40	DHCPクライアント機能を有すること。	○
C. 9. 10. 41	NTPクライアント機能を有し、NTPサーバから時刻同期可能であること。	○
C. 9. 10. 42	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○

C. 9. 10. 43	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 10. 44	RMONv1エージェント機能を有すること。	○
C. 9. 10. 45	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 10. 46	Energy Efficient Ethernet(IEEE802. 3az)機能を有すること。	○
C. 9. 10. 47	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 10. 48	質量が4. 35kg以下であること。	○
C. 9. 10. 49	AC電源を内蔵し、90～264Vでの動作が可能であること。	○
C. 9. 10. 50	19インチラック搭載金具により、19インチラックに搭載可能であること。	○
C. 9. 10. 51	壁掛け金具により、壁掛けが可能であること。	○
C. 9. 10. 52	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 10. 53	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形で可とする。	○
C. 9. 11	部門系スイッチ③	—
C. 9. 11. 1	以下、仕様を満たす部門系スイッチを2台用意すること。	○
C. 9. 11. 2	56. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 11. 3	41. 6Mpps以上の転送レートを持つこと。	○
C. 9. 11. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 11. 5	10/100/1000BASE-Tポートを24ポート標準搭載すること。	○
C. 9. 11. 6	SFPスロットを4スロット標準搭載すること。	○
C. 9. 11. 7	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 11. 8	タグVLAN(IEEE802. 1Q)に対応していること。	○
C. 9. 11. 9	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 11. 10	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 11. 11	Voice VLANに対応していること。	○
C. 9. 11. 12	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 11. 13	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 11. 14	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 11. 15	フローコントロール(IEEE802. 3X)を有すること。	○
C. 9. 11. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 11. 17	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 11. 18	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 11. 19	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 11. 20	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 11. 21	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol(IEEE802. 3ad)に対応していること。	○
C. 9. 11. 22	スパンニングツリー(IEEE802. 1d)、ラピッドスパンニングツリー(IEEE802. 1w)、MSTP(IEEE802. 1s)、VLAN毎に動作するスパンニングツリー(Per VLAN スパンニングツリー)に対応していること。	○
C. 9. 11. 23	通信パケットのパケットフィルタ機能を有すること。入力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 11. 24	入力トラフィックの帯域制限が可能なこと。	○
C. 9. 11. 25	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 11. 26	輻輳制御として、Strict Priority(SP)、Weighted Round Robin(WRR)を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 11. 27	IEEE802. 1X認証に対応のこと。	○
C. 9. 11. 28	MACアドレス認証に対応のこと。	○
C. 9. 11. 29	ダイナミックVLANによるVLAN付与(Port based/MAC based)に対応できること。	○
C. 9. 11. 30	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 11. 31	IGMPv1/v2/v3スヌーピング機能を有すること。	○
C. 9. 11. 32	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 11. 33	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 11. 34	コンソールポート(CLI)、WEBコンソール(WEB GUI)による設定、状態確認が可能であること。	○
C. 9. 11. 35	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 11. 36	GUI (WEB Console) による設定が可能であること。	○
C. 9. 11. 37	FTP/TFTPクライアント、FTPサーバ機能を有すること。もしくは、TFTPクライアントやSCP等の機能を有する形で可とする。	○
C. 9. 11. 38	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 11. 39	DHCPクライアント機能を有すること。	○
C. 9. 11. 40	NTPクライアント機能を有し、NTPサーバから時刻同期可能であること。	○
C. 9. 11. 41	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 11. 42	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 11. 43	RMONv1エージェント機能を有すること。	○
C. 9. 11. 44	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 11. 45	Energy Efficient Ethernet(IEEE802. 3az)機能を有すること。	○
C. 9. 11. 46	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○

C. 9. 11. 47	質量が4. 35kg以下であること。	○
C. 9. 11. 48	AC電源を内蔵し、90～264Vでの動作が可能であること。	○
C. 9. 11. 49	固定用マグネットによる設置が可能なこと。	○
C. 9. 11. 50	19インチラック搭載金具を標準添付すること。	○
C. 9. 11. 51	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 11. 52	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形で可とする。	○
C. 9. 12	部門系スイッチ④	—
C. 9. 12. 1	以下、仕様を満たす部門系スイッチを5台用意すること。	○
C. 9. 12. 2	104. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 12. 3	77. 3Mpps以上の転送レートを持つこと。	○
C. 9. 12. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 12. 5	10/100/1000BASE-Tポートを48ポート標準搭載すること。	○
C. 9. 12. 6	SFPスロットを4スロット標準搭載すること。	○
C. 9. 12. 7	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 12. 8	タグVLAN (IEEE802. 1Q) に対応していること。	○
C. 9. 12. 9	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 12. 10	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 12. 11	Voice VLANに対応していること。	○
C. 9. 12. 12	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 12. 13	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 12. 14	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 12. 15	フローコントロール (IEEE802. 3X) を有すること。	○
C. 9. 12. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 12. 17	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 12. 18	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 12. 19	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能 (ループ検出機能) を有すること。	○
C. 9. 12. 20	片方向リンクの発生 (例えば光ファイバペアケーブルの一本が断線等) を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 12. 21	複数の物理リンクを束ねて1つの論理リンクとして扱う技術 (リンクアグリゲーション) を有すること。Link Aggregation Control Protocol (IEEE802. 3ad) に対応していること。	○
C. 9. 12. 22	スパニングツリー (IEEE802. 1d)、ラピッドスパニングツリー (IEEE802. 1w)、MSTP (IEEE802. 1s)、VLAN毎に動作するスパニングツリー (Per VLAN スパニングツリー) に対応していること。	○
C. 9. 12. 23	通信パケットのパケットフィルタ機能を有すること。入力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 12. 24	入力トラフィックの帯域制限が可能なこと。	○
C. 9. 12. 25	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 12. 26	輻輳制御として、Strict Priority (SP)、Weighted Round Robin (WRR) を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 12. 27	IEEE802. 1X認証に対応のこと。	○
C. 9. 12. 28	MACアドレス認証に対応のこと。	○
C. 9. 12. 29	ダイナミックVLANによるVLAN付与 (Port based/MAC based) に対応できること。	○
C. 9. 12. 30	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 12. 31	IGMPv1/v2/v3スヌーピング機能を有すること。	○
C. 9. 12. 32	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 12. 33	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 12. 34	コンソールポート (CLI)、WEBコンソール (WEB GUI) による設定、状態確認が可能であること。	○
C. 9. 12. 35	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 12. 36	GUI (WEB Console) による設定が可能であること。	○
C. 9. 12. 37	FTP/TFTPクライアント、FTPサーバ機能を有すること。もしくは、TFTPクライアントやSCP等の機能を有する形で可とする。	○
C. 9. 12. 38	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 12. 39	DHCPクライアント機能を有すること。	○
C. 9. 12. 40	NTPクライアント機能を有し、NTPサーバから時刻同期可能であること。	○
C. 9. 12. 41	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 12. 42	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 12. 43	RMONv1エージェント機能を有すること。	○
C. 9. 12. 44	ポートミラーリング機能 (モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能) を有すること。	○
C. 9. 12. 45	Energy Efficient Ethernet (IEEE802. 3az) 機能を有すること。	○
C. 9. 12. 46	外形寸法 (Width x Depth x Height) が、19インチラックに収まること。	○
C. 9. 12. 47	質量が4. 5kg以下であること。	○
C. 9. 12. 48	AC電源を内蔵し、90～264Vでの動作が可能であること。	○
C. 9. 12. 49	最大消費電力が、54W以下であること。	○
C. 9. 12. 50	19インチラック搭載金具を標準添付すること。	○
C. 9. 12. 51	VCCIクラスA、RoHS指令に対応していること。	○

C. 9. 12. 52	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 13	部門系スイッチ⑤	—
C. 9. 13. 1	以下、仕様を満たす部門系スイッチを2台用意すること。	○
C. 9. 13. 2	104. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 13. 3	77. 3Mpps以上の転送レートを持つこと。	○
C. 9. 13. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 13. 5	64以上のIPルート情報を保持できること。	○
C. 9. 13. 6	256以上のARP情報を保持できること。	○
C. 9. 13. 7	10/100/1000BASE-T (PoE Plus給電対応) ポートを48ポート標準搭載すること。	○
C. 9. 13. 8	SFPスロットを4スロット標準搭載すること。	○
C. 9. 13. 9	SFPスロットは、1000BASE-T/SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 13. 10	PoE Plus (IEEE802. 3at) 規格に準拠し、1ポートあたり30W給電が可能であること。	○
C. 9. 13. 11	装置あたりの最大給電可能電力が370. 0W以上であること。	○
C. 9. 13. 12	S/Wバージョンアップなどの再起動時にも受電装置への給電が停止しないこと。	○
C. 9. 13. 13	4台までのスタック接続に対応可能であること。もしくは、冗長化 (アクティブ/スタンバイ) ができる形でも可とする。	○
C. 9. 13. 14	タグVLAN (IEEE802. 1Q) に対応していること。	○
C. 9. 13. 15	プロトコルVLANに対応していること。もしくは、MACベースや802. 1XなどのダイナミックVLANを有している形でも可とする。	○
C. 9. 13. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 13. 17	Voice VLANに対応していること。	○
C. 9. 13. 18	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 13. 19	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 13. 20	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 13. 21	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 13. 22	フローコントロール (IEEE802. 3X) を有すること。	○
C. 9. 13. 23	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 13. 24	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 13. 25	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 13. 26	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 13. 27	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能 (ループ検出機能) を有すること。	○
C. 9. 13. 28	片方向リンクの発生 (例えば光ファイバペアケーブルの一本が断線等) を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 13. 29	複数の物理リンクを束ねて1つの論理リンクとして扱う技術 (リンクアグリゲーション) を有すること。Link Aggregation Control Protocol (IEEE802. 3ad) に対応していること。	○
C. 9. 13. 30	スパニングツリー (IEEE802. 1d)、ラピッドスパニングツリー (IEEE802. 1w)、MSTP (IEEE802. 1s)、VLAN毎に動作するスパニングツリー (Per VLAN スパニングツリー) に対応していること。	○
C. 9. 13. 31	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 13. 32	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 13. 33	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 13. 34	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 13. 35	入出力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 13. 36	輻輳制御として、Strict Priority Queueing (SP)、Weighted Round Robin (WRR) を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 13. 37	IEEE802. 1X認証/MAC認証/WEB認証/マルチステップ認証に対応のこと。	○
C. 9. 13. 38	ダイナミックVLANによるVLAN付与 (Port based/MAC based) に対応できること。	○
C. 9. 13. 39	ポートセキュリティ機能に対応のこと。	○
C. 9. 13. 40	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 13. 41	最大2000ユーザの認証セッションを保持できること。	○
C. 9. 13. 42	STATICルーティング機能を有すること。	○
C. 9. 13. 43	マルチキャストVLAN機能を有すること。	○
C. 9. 13. 44	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 13. 45	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 13. 46	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 13. 47	コンソールポート (CLI) による設定、状態確認が可能であること。	○
C. 9. 13. 48	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 13. 49	GUI (WEB Console) による設定が可能であること。	○
C. 9. 13. 50	FTP/TFTPクライアント、FTPサーバ機能を有すること。もしくは、TFTPクライアントやSCP等の機能を有する形でも可とする。	○
C. 9. 13. 51	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 13. 52	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C. 9. 13. 53	NTPクライアント機能を有すること。	○

C. 9. 13. 54	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 13. 55	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 13. 56	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 13. 57	RMONエージェント機能を有すること。	○
C. 9. 13. 58	sFlowエージェント機能を有すること。もしくは、NetFlow および Flexible NetFlowに対応できる形でも可とする。	○
C. 9. 13. 59	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 13. 60	Energy Efficient Ethernet (IEEE802. 3az) 機能を有すること。	○
C. 9. 13. 61	外形寸法 (Width x Depth x Height) が、19インチラックに収まること。	○
C. 9. 13. 62	質量が6. 4kg以下であること。	○
C. 9. 13. 63	AC電源を内蔵し、90～264Vでの動作が可能であること。	○
C. 9. 13. 64	19インチラック搭載金具を標準添付すること。	○
C. 9. 13. 65	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 13. 66	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 13. 67	部門系スイッチ⑤の拡張オプションとして、以下に記載の製品を手配すること。	○
C. 9. 13. 68	1port 1000BASE-SX SFP (MM, LC) を計4個用意すること。	○
C. 9. 14	管理棟スイッチ①	—
C. 9. 14. 1	以下、仕様を満たす管理棟スイッチを3台用意すること。	○
C. 9. 14. 2	128. 0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 14. 3	95. 2Mpps以上の転送レートを持つこと。	○
C. 9. 14. 4	16, 000以上のMACアドレスを保持できること。	○
C. 9. 14. 5	512以上のIPルート情報を保持できること。	○
C. 9. 14. 6	1, 000以上のARP情報を保持できること。	○
C. 9. 14. 7	10/100/1000BASE-Tポートを24ポート標準搭載すること。	○
C. 9. 14. 8	SFP+スロットを4スロット標準搭載すること。	○
C. 9. 14. 9	SFP+スロットは、1000BASE-T/SX/LX/BX SFPトランシーバ、10GBASE-T/SR/LR/ER SFP+トランシーバをサポートすること。	○
C. 9. 14. 10	6台までのスタック接続に対応可能であること。もしくは、冗長化（アクティブ/スタンバイ）ができる形でも可とする。	○
C. 9. 14. 11	タグVLAN (IEEE802. 1Q) に対応していること。	○
C. 9. 14. 12	プロトコルVLAN、IPサブネットVLANに対応していること。もしくは、MACベースや802. 1XなどのダイナミックVLANを有している形でも可とする。	○
C. 9. 14. 13	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 14. 14	Voice VLANに対応していること。	○
C. 9. 14. 15	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 14. 16	32VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 14. 17	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 14. 18	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 14. 19	フローコントロール (IEEE802. 3X) を有すること。	○
C. 9. 14. 20	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 14. 21	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 14. 22	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 14. 23	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 14. 24	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○
C. 9. 14. 25	片方向リンクの発生(例えば光ファイバペアケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 14. 26	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol (IEEE802. 3ad) に対応していること。	○
C. 9. 14. 27	スパニングツリー (IEEE802. 1d)、ラピッドスパニングツリー (IEEE802. 1w)、MSTP (IEEE802. 1s)、VLAN毎に動作するスパニングツリー (Per VLAN スパニングツリー) に対応していること。	○
C. 9. 14. 28	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。 リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 14. 29	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 14. 30	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 14. 31	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 14. 32	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 14. 33	輻輳制御として、Strict Priority Queueing (SP)、Weighted Round Robin (WRR) を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 14. 34	IEEE802. 1X認証/MAC認証/WEB認証/マルチステップ認証に対応のこと。	○
C. 9. 14. 35	トリプル認証に対応のこと。	○
C. 9. 14. 36	ダイナミックVLANによるVLAN付与 (Port based/MAC based) に対応できること。	○
C. 9. 14. 37	ポートセキュリティ機能に対応のこと。	○

C. 9. 14. 38	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 14. 39	STATIC/RIP(RIP v1/v2/ng)/OSPF(OSPF v2/v3)ルーティング機能を有すること。	○
C. 9. 14. 40	ポリシーベースルーティング機能を有すること。	○
C. 9. 14. 41	VRRP機能を有すること。	○
C. 9. 14. 42	マルチキャストVLAN機能を有すること。	○
C. 9. 14. 43	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 14. 44	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 14. 45	コンソールポート(CLI)による設定、状態確認が可能であること。	○
C. 9. 14. 46	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 14. 47	GUI (WEB Console) による設定が可能であること。	○
C. 9. 14. 48	FTP/TFTPクライアント、FTPサーバ機能を有すること。もしくは、TFTPクライアントやSCP等の機能を有する形で可とする。	○
C. 9. 14. 49	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 14. 50	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C. 9. 14. 51	NTPクライアント、NTPサーバ機能を有すること。	○
C. 9. 14. 52	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 14. 53	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 14. 54	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 14. 55	RMONエージェント機能を有すること。	○
C. 9. 14. 56	sFlowエージェント機能を有すること。もしくは、NetFlow および Flexible NetFlowに対応できる形で可とする。	○
C. 9. 14. 57	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 14. 58	Energy Efficient Ethernet(IEEE802.3az)機能を有すること。	○
C. 9. 14. 59	外形寸法(Width x Depth x Height)が、19インチラックに収まること。	○
C. 9. 14. 60	質量が4.4kg以下であること。	○
C. 9. 14. 61	AC電源を内蔵し、90~264Vでの動作が可能であること。	○
C. 9. 14. 62	温度 0~45℃で動作すること。	○
C. 9. 14. 63	19インチラック搭載金具を標準添付すること。	○
C. 9. 14. 64	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 14. 65	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形で可とする。	○
C. 9. 14. 66	管理棟スイッチ①の拡張オプションとして、以下に記載の製品を手配すること。	○
C. 9. 14. 67	SFP+銅線ケーブル(1m)を計2個用意すること。	○
C. 9. 14. 68	1port 1GBASE-SR SFP+(MM, LC)を計2個以上用意すること。	○
C. 9. 15	管理棟スイッチ②	—
C. 9. 15. 1	以下、仕様を満たす管理棟スイッチを2台用意すること。	○
C. 9. 15. 2	56.0Gbps以上のスイッチング容量を持つこと。	○
C. 9. 15. 3	41.6Mpps以上の転送レートを持つこと。	○
C. 9. 15. 4	16,000以上のMACアドレスを保持できること。	○
C. 9. 15. 5	64以上のIPルート情報を保持できること。	○
C. 9. 15. 6	256以上のARP情報を保持できること。	○
C. 9. 15. 7	10/100/1000BASE-T(PoE Plus給電対応)ポートを24ポート標準搭載すること。	○
C. 9. 15. 8	SFPスロットを4スロット標準搭載すること。	○
C. 9. 15. 9	SFPスロットは、1000BASE-SX/LX/BX SFPトランシーバをサポートすること。	○
C. 9. 15. 10	PoE Plus(IEEE802.3at)規格に準拠し、1ポートあたり30W給電が可能であること。	○
C. 9. 15. 11	装置あたりの最大給電可能電力が370.0W以上であること。	○
C. 9. 15. 12	S/Wバージョンアップなどの再起動時にも受電装置への給電が停止しないこと。	○
C. 9. 15. 13	4台までのスタック接続に対応可能であること。もしくは、冗長化(アクティブ/スタンバイ)ができる形で可とする。	○
C. 9. 15. 14	タグVLAN(IEEE802.1Q)に対応していること。	○
C. 9. 15. 15	プロトコルVLANに対応していること。もしくは、MACベースや802.1XなどのダイナミックVLANを有している形で可とする。	○
C. 9. 15. 16	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 15. 17	Voice VLANに対応していること。	○
C. 9. 15. 18	VLANマッピング、QinQ(802.1Q-in-802.1Q)に対応していること。	○
C. 9. 15. 19	最大1024のVLANを同時にタグVLANで通信可能なこと。	○
C. 9. 15. 20	8VLANインタフェースを設定可能で、それぞれにIPアドレスを1つ付与できること。	○
C. 9. 15. 21	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。	○
C. 9. 15. 22	標準搭載ポートは、Auto MDI・MDIXに対応し、MDIX固定設定が可能なこと。	○
C. 9. 15. 23	フローコントロール(IEEE802.3X)を有すること。	○
C. 9. 15. 24	同一VLANであっても特定ポート以外とは通信をさせない機能を持つこと。	○
C. 9. 15. 25	各ポートから流入するBroadcast、Multicast、Unknown Unicastの通信量に一定の閾値を設け、閾値を超過したパケットを破棄する機能を有すること。	○
C. 9. 15. 26	各ポートから流入するBroadcast、Multicast、Unicastの通信量が一定の閾値を超えた場合にポートをブロック/シャットダウンしたり、SNMP trapを送信する機能を有すること。	○
C. 9. 15. 27	最大9000byte以上のジャンボフレームに対応可能であること。	○
C. 9. 15. 28	ケーブル誤接続等により、誤ってループ状態が構成された場合に自動的にポートをブロックしブロードキャストストームを防止する機能(ループ検出機能)を有すること。	○

C. 9. 15. 29	片方向リンクの発生(例えば光ファイバケーブルの一本が断線等)を検出し、検出ポートを自動的にシャットダウンする機能を有すること。	○
C. 9. 15. 30	複数の物理リンクを束ねて1つの論理リンクとして扱う技術(リンクアグリゲーション)を有すること。Link Aggregation Control Protocol (IEEE802. 3ad)に対応していること。	○
C. 9. 15. 31	スパンニングツリー(IEEE802. 1d)、ラピッドスパンニングツリー(IEEE802. 1w)、MSTP(IEEE802. 1s)、VLAN毎に動作するスパンニングツリー(Per VLAN スパンニングツリー)に対応していること。	○
C. 9. 15. 32	リング状にスイッチングハブを接続し、広帯域な冗長化ネットワークを実現するリングプロトコル機能を有すること。リング接続ケーブル、接続ノード障害時には、数秒で経路切替を行いネットワークの信頼性を確保できること。	○
C. 9. 15. 33	通信パケットのパケットフィルタ機能を有すること。入出力ポートでのフィルタリングが可能なこと。送信元/宛先MACアドレス、送信元/宛先IPアドレス、プロトコル番号、TCP/UDPの送信元/宛先ポート番号でのフィルタが可能なこと。	○
C. 9. 15. 34	IPv6アドレス付与、IPv6ルーティング機能を有すること。	○
C. 9. 15. 35	入出力トラフィックの帯域制限が可能なこと。	○
C. 9. 15. 36	入力トラフィックの分類として、ポートプライオリティの利用、入力パケットのCOS値/DSCP値のtrust/remarkが可能なこと。	○
C. 9. 15. 37	輻輳制御として、Strict Priority Queueing (SP)、Weighted Round Robin (WRR) を利用可能なこと。各ポートで8つの出力キューを利用可能であること。	○
C. 9. 15. 38	IEEE802. 1X認証/MAC認証/WEB認証/マルチステップ認証に対応のこと。	○
C. 9. 15. 39	ダイナミックVLANによるVLAN付与 (Port based/MAC based)に対応できること。	○
C. 9. 15. 40	ポートセキュリティ機能に対応のこと。	○
C. 9. 15. 41	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 15. 42	最大2000ユーザの認証セッションを保持できること。	○
C. 9. 15. 43	STATICルーティング機能を有すること。	○
C. 9. 15. 44	マルチキャストVLAN機能を有すること。	○
C. 9. 15. 45	IGMP v1/v2/v3スヌーピング機能を有すること。	○
C. 9. 15. 46	MLD v1/v2スヌーピング機能を有すること。	○
C. 9. 15. 47	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 15. 48	コンソールポート (CLI) による設定、状態確認が可能であること。	○
C. 9. 15. 49	Telnet、SSHにより装置へのリモートログインが可能であること。	○
C. 9. 15. 50	GUI (WEB Console) による設定が可能であること。	○
C. 9. 15. 51	FTP/TFTPクライアント機能を有すること。もしくは、TFTPクライアントやSCP等の機能を有する形でも可とする。	○
C. 9. 15. 52	LLDP機能を有し、隣接するマルチベンダー機器に対して自装置の機器情報をアドバタイズできること。	○
C. 9. 15. 53	DHCPクライアント、DHCPリレー、DHCPサーバ、DHCPスヌーピング機能を有すること。	○
C. 9. 15. 54	NTPクライアント機能を有すること。	○
C. 9. 15. 55	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 15. 56	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 15. 57	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 15. 58	RMONエージェント機能を有すること。	○
C. 9. 15. 59	sFlowエージェント機能を有すること。もしくは、NetFlow および Flexible NetFlowに対応できる形でも可とする。	○
C. 9. 15. 60	ポートミラーリング機能(モニタリングデバイスにてパケット解析等を行うために、特定のポートを通過するトラフィックを指定したポートにコピーする機能)を有すること。	○
C. 9. 15. 61	Energy Efficient Ethernet (IEEE802. 3az) 機能を有すること。	○
C. 9. 15. 62	外形寸法 (Width x Depth x Height) が、19インチラックに収まること。	○
C. 9. 15. 63	質量が6. 2kg以下であること。	○
C. 9. 15. 64	AC電源を内蔵し、90~264Vでの動作が可能であること。	○
C. 9. 15. 65	19インチラック搭載金具を標準添付すること。	○
C. 9. 15. 66	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 15. 67	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換できる形でも可とする。	○
C. 9. 16	NW機器用UPS①	—
C. 9. 16. 1	以下、仕様を満たすラックマウント型UPSを17台用意すること。	○
C. 9. 16. 2	運転方式は常時商用給電方式であること。	○
C. 9. 16. 3	相数は「単相2線+接地 (D種以上)」であること。	○
C. 9. 16. 4	定格入力電圧は100Vに対応していること。	○
C. 9. 16. 5	定格周波数は50/60Hzであること。	○
C. 9. 16. 6	出力電力容量は1500VA/1200W以上であること。	○
C. 9. 16. 7	発熱量は284kJ/h以下であること (急速充電時)	○
C. 9. 16. 8	入力端子はNEMA 5-15Pであること。またケーブルも添付されていること。	○
C. 9. 16. 9	出力端子はNEMA 5-15R ×6個以上であること。	○
C. 9. 16. 10	質量は28kg以下であること。	○
C. 9. 16. 11	バッテリー期待寿命は3年以上であること (周囲温度20℃平均時)	○
C. 9. 16. 12	ラックマウント用金具を添付すること。	○
C. 9. 17	NW機器用UPS②	—
C. 9. 17. 1	以下、仕様を満たすタワー型UPSを5台用意すること。	○
C. 9. 17. 2	運転方式は常時商用給電方式であること。	○
C. 9. 17. 3	相数は「単相2線+接地 (D種以上)」であること。	○
C. 9. 17. 4	定格入力電圧は100Vに対応していること。	○

C. 9. 17. 5	定格周波数は50/60Hzであること。	○
C. 9. 17. 6	出力電力容量は1500VA/980W以上であること。	○
C. 9. 17. 7	発熱量は284kJ/h以下であること（急速充電時）	○
C. 9. 17. 8	入力端子はNEMA 5-15Pであること。またケーブルも添付されていること。	○
C. 9. 17. 9	出力端子はNEMA 5-15R ×8個以上であること。	○
C. 9. 17. 10	質量は26kg以下であること。	○
C. 9. 17. 11	バッテリー期待寿命は3年以上であること（周囲温度20℃平均時）	○
C. 9. 18	無線LANコントローラ	—
C. 9. 18. 1	以下、仕様を満たす無線LANコントローラを2台用意すること。ただし、無線LANコントローラ故障時も継続して無線APが利用できる場合、この限りではない。	○
C. 9. 18. 2	100/1000BASE-Tポートを8ポート標準搭載すること。もしくは、構成上の必要数を搭載している形でも可とする。	○
C. 9. 18. 3	複数の物理リンクを束ねて1つの論理リンクとして扱う技術（リンクアグリゲーション）を有すること。	○
C. 9. 18. 4	2台までのスタック接続に対応可能であること。もしくは、冗長化（アクティブ/スタンバイ）ができる形や、無線LANコントローラ故障時も継続して無線APが利用できる場合でも可とする。	○
C. 9. 18. 5	最大500台のAPを管理できること。	○
C. 9. 18. 6	最大3000のクライアントを管理できること。	○
C. 9. 18. 7	1ラジオあたり最大16のSSIDを設定できること。	○
C. 9. 18. 8	ビーコンフレーム内にSSIDを隠し、ブロードキャストプローブ要求に応答しない技術を有すること。	○
C. 9. 18. 9	MACアドレスに基づいてWhite List/Black Listを設定できること。	○
C. 9. 18. 10	WPA/WPA2/WPA3に対応していること。	○
C. 9. 18. 11	TKIP/AESに対応していること。	○
C. 9. 18. 12	アクセスポイント間で再認証なしの高速ローミングに対応していること。	○
C. 9. 18. 13	IEEE802. 1X認証/MAC認証/マルチステップ認証に対応すること。	○
C. 9. 18. 14	ダイナミックVLANによるVLAN付与に対応できること。	○
C. 9. 18. 15	ローカルデータベース、外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 18. 16	WIDS/WIPSに対応していること。	○
C. 9. 18. 17	DFS/TPCに対応していること。	○
C. 9. 18. 18	WMM標準に基づいたQoS設定が可能なこと。	○
C. 9. 18. 19	WLANメッシュ機能に対応していること。	○
C. 9. 18. 20	統合管理サービスにより、一元的に管理が可能であること。	○
C. 9. 18. 21	STATICルーティング機能を有すること。	○
C. 9. 18. 22	GUI（WEB Console）による設定が可能であること。	○
C. 9. 18. 23	NTPクライアント機能を有すること。	○
C. 9. 18. 24	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 18. 25	アクセスログ、システムログ、エラーログ等を定期的に自装置Flashメモリに保存し、装置再起動時にも、そのログを確認できる機能を有すること。	○
C. 9. 18. 26	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 18. 27	外形寸法（Width x Depth x Height）が、440 x 436 x 44.0mm以下であること。突起部含まない形でも可とする。	○
C. 9. 18. 28	質量が6.6kg以下であること。	○
C. 9. 18. 29	最大消費電力が、110W以下であること。	○
C. 9. 18. 30	19インチラック搭載金具を用意すること。もしくは、19インチラックに搭載できること。	○
C. 9. 18. 31	USBメモリにコンフィグやソフトウェアを保存できること。	○
C. 9. 18. 32	VCCIクラスA、RoHS指令に対応していること。	○
C. 9. 18. 33	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換できる形でも可とする。	○
C. 9. 18. 34	無線アクセスポイントの導入数に合わせたライセンスを手配すること。	○
C. 9. 18. 35	電源は冗長化すること。ただし、無線LANコントローラ故障時も継続して無線APが利用できる場合、この限りではない。	○
C. 9. 19	無線LANアクセスポイント	—
C. 9. 19. 1	以下、仕様を満たす無線LANアクセスポイントを173台用意すること。	○
C. 9. 19. 2	100/1000/2.5G/5GBASE-T（PoE++受電）ポートを1ポート標準搭載すること。	○
C. 9. 19. 3	標準搭載ポートは、Auto Negotiationに対応し、速度、全半二重の固定設定が可能なこと。もしくは、全二重設定のみでも可とする。	○
C. 9. 19. 4	IEEE802. 11axに対応していること。	○
C. 9. 19. 5	2.4GHz帯、5GHz（W52/W53/W56）帯、5GHz（W52/W53）帯/6GHz帯の3つの周波数帯を同時利用できること。	○
C. 9. 19. 6	1ラジオあたりに最大16のSSIDが設定できること。	○
C. 9. 19. 7	ビーコンフレーム内にSSIDを隠し、ブロードキャストプローブ要求に応答しない技術を有すること。	○
C. 9. 19. 8	MACアドレスに基づいてWhite List/Black Listを設定できること。	○
C. 9. 19. 9	WPA/WPA2/WPA3に対応していること。	○
C. 9. 19. 10	TKIP/AESに対応していること。	○
C. 9. 19. 11	IEEE802. 1X認証/MAC認証/マルチステップ認証に対応すること。	○
C. 9. 19. 12	ダイナミックVLANによるVLAN付与に対応できること。	○
C. 9. 19. 13	ローカルデータベース、もしくは外部RADIUSサーバによる認証が可能なこと。	○
C. 9. 19. 14	DFS（Dynamic Frequency Selection）に対応していること。	○
C. 9. 19. 15	WMM標準に基づいたQoS設定が可能なこと。	○
C. 9. 19. 16	統合管理サービスにより、一元的に管理が可能であること。	○

C. 9. 19. 17	NTPクライアント機能を有すること。	○
C. 9. 19. 18	Syslogプロトコルにより、Syslogサーバに動作状況のテキストを送付可能であること。	○
C. 9. 19. 19	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 19. 20	外形寸法265 (W) × 265 (D) × 60 (H) mm (突起部含まず) 以下であること。	○
C. 9. 19. 21	質量が1.7kg以下であること。	○
C. 9. 19. 22	ACアダプタ電源入力時、90～264Vでの動作が可能であること。	○
C. 9. 19. 23	最大消費電力が、42W以下であること。	○
C. 9. 19. 24	ファンレス設計であること。	○
C. 9. 19. 25	壁/天井取り付け用ブラケットが標準添付であること。	○
C. 9. 19. 26	製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。もしくは、製品購入から5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換する形でも可とする。	○
C. 9. 20	認証サーバ	—
C. 9. 20. 1	WEB管理画面で製品を操作できること。その言語は日本語で、WEB管理画面へのアクセスは暗号化 (httpsポート有効化でも可) されていること。	○
C. 9. 20. 2	利用者向けのサービスページはカスタマイズできること。ロゴの変更や任意メッセージの挿入に対応すること。	○
C. 9. 20. 3	製品の操作マニュアル、リリースノート、その他関連文書は日本語で提供されていること。	○
C. 9. 20. 4	WEB管理ページにて、RADIUSサービス、LDAPサービスの状態が正常または異常であることを確認できること。	○
C. 9. 20. 5	WEB管理ページ上で、ファームウェアに内蔵されたマニュアルを参照できること。	○
C. 9. 20. 6	ソフトウェアとハードウェアが一体となったアプライアンス製品であること。	○
C. 9. 20. 7	EIA規格 19インチラックに固定可能であること。ラック占有は1RU以下であること。	○
C. 9. 20. 8	フラッシュメモリから起動すること。	○
C. 9. 20. 9	ネットワークインターフェイスとして、10BASE-T/100BASE-TX/1000BASE-Tポートを2つ、もしくは2つ以上有し、サービス提供用インターフェイス、管理アクセス用インターフェイス、冗長化時のデータ同期用インターフェイスとして利用可能なこと。	○
C. 9. 20. 10	本体前面に起動/停止ボタンを有し、ボタン操作のみで安全にシステムのシャットダウンを完了できること。	○
C. 9. 20. 11	電源供給開始時に、すぐに起動するモードが使用できること。	○
C. 9. 20. 12	RADIUS (Remote Authentication Dial In User Service) 機能を有し、ネットワーク機器等と連携し、認証システムを実現できること。	○
C. 9. 20. 13	認証方式として、PAP CHAP MS-CHAP MS-CHAPv2 EAP-MD5 EAP-TLS EAP-TTLS (PAP/CHAP/MSCHAP/MSCHAPv2/EAP-TLS/EAP-MSCHAPv2) EAP-PEAP (MS-CHAPv2/GTC/TLS) に対応すること。もしくは、認証方式として、EAP-MD5、EAP-PEAP (MS-CHAPv2、TLS)、EAP-TTLS (PAP、CHAP、MS-CHAPv2、EAP-MSCHAPv2、EAP-TLS)、EAP-TLS、及びPAP、CHAP、MS-CHAP、MS-CHAPv2に対応できる形でも可とする。	○
C. 9. 20. 14	認証に用いるアカウントは5,000以上登録できること。	○
C. 9. 20. 15	認証アカウント毎に最終認証成功日時を記録できること。記録した日時の情報は検索条件として利用でき、その結果はCSVファイルとしてエクスポートできること。	○
C. 9. 20. 16	パスワードの有効期限、およびパスワードの変更禁止期間を設定できること。	○
C. 9. 20. 17	利用者パスワードの期限切れと期限切れリマインダーを、管理者および利用者宛にメール通知できること。期限切れ通知の場合、アプライアンス上で期限切れが確認された際にメール通知すること。期限切れリマインダーの場合、何日前 (当日, 1週間前, 10日前, 30日前) に通知するかを指定できること。また、1度のみの通知か毎日通知かを選択できること。 もしくは、利用者パスワードの期限切れに関して、下記の通知ができる形でも可とする。 ・期限当日通知：当日にメール通知 ・事前通知：1～998日の範囲で指定した残りの日数になった日に該当日にのみ通知 ・期限切れフォロー：期限切れのアカウントに対して、指定した曜日に週1回通知	○
C. 9. 20. 18	認証に用いるアカウント、連携する認証ネットワーク機器はグループで管理できること。また両グループの組合せにより認証の結果を制御できること。	○
C. 9. 20. 19	認証連続失敗によりアカウントロックができること。アカウントロックに至る失敗回数、連続失敗カウントのリセットやロックの解除までの秒数は管理者により指定できること。 もしくは、PAPのみパスワード誤りによる認証連続失敗をトリガーとしたアカウントロックができ、連続失敗カウントのリセットは管理者から手動のみできる形でも可とする。	○
C. 9. 20. 20	同一アカウントによる多重ログオンの有無や、曜日と時間帯の組合せ、任意のチェックアイテムにより認証の成否を制御できること。 もしくは、Accountingや属性チェックにより認証制御 (同一アカウントによる多重ログオンの有無/任意のチェックアイテムにより認証の成否) を行う形でも可とする。	○
C. 9. 20. 21	アカウントは機器内のデータベースに登録するほか、外部の認証・データベースサーバの情報を利用できること。外部データベースとして、LDAP (Lightweight Directory Access Protocol) データベース、及びRADIUS認証サーバを想定する。	○
C. 9. 20. 22	ゲストユーザーアカウント登録機能を持つこと。	○
C. 9. 20. 23	利用者にゲストユーザーアカウントの登録申請をさせる機能を持つこと。	○
C. 9. 20. 24	ユーザーによるゲストユーザーアカウントの代理登録が可能であり、代理登録が可能なユーザーは、ゲスト管理権限を持つユーザーまたは正規ユーザーから選択できること。	○
C. 9. 20. 25	ゲストユーザーアカウントの有効期限を日数および時刻で設定でき、有効期限切れのゲストユーザーアカウントを自動的に削除する機能を持つこと。	○
C. 9. 20. 26	ゲストユーザーアカウント登録完了通知を利用者のメールアドレスに送信可能なこと。	○
C. 9. 20. 27	ゲストユーザー申請時に入力させる利用者情報を管理者が設定できること。	○

C. 9. 20. 28	認証連続失敗によりゲストユーザーアカウントのロックができること。アカウントロックに至る失敗回数、ロックの解除までの秒数は管理者により指定できること。 もしくは、PAP認証時のパスワード誤りによる、認証連続失敗をトリガーとするアカウントロックが可能で、管理者向けWeb管理画面からロックの解除ができる形でも可とする。	○
C. 9. 20. 29	ゲストユーザーはゲストユーザー用グループに所属することができ、ゲストユーザー用RADIUSアトリビュートを返すことができること。	○
C. 9. 20. 30	ネットワーク機器と連携し、MACアドレス認証を行う機能を有すること。なお、本調達で必要なライセンス数を含めること。	○
C. 9. 20. 31	MACアドレス情報は複数の認証サーバ間で共有(冗長化)できること。	○
C. 9. 20. 32	利用者によるMACアドレスの申請ができること。承認は、事前承認用コードによる事前承認と自動承認ができること。もしくは、承認は管理者による手動承認か自動承認から選択できる形でも可とする。	○
C. 9. 20. 33	ローカルデータベースのユーザーによるMACアドレスの代理登録ができること。	○
C. 9. 20. 34	代理登録が可能なユーザーは、MACアドレス管理者権限を持つユーザー、または正規ユーザーから選択できること。	○
C. 9. 20. 35	MACアドレス申請時に入力させる利用者情報を管理者が設定できること。	○
C. 9. 20. 36	MACアドレス登録完了通知を利用者のメールアドレスに送信できること。	○
C. 9. 20. 37	RADIUS認証時にMACアドレスの自動収集ができること。	○
C. 9. 20. 38	システム管理者が、申請・収集したMACアドレスを確認できること。	○
C. 9. 20. 39	MACアドレス毎に最終認証成功日時を記録できること。その結果はCSVファイルとしてエクスポートできること。	○
C. 9. 20. 40	ダッシュボードの画面から、本登録待ちのMACアドレス件数を確認できること。もしくは、専用のページで未登録のMACアドレスの件数表示できる形でも可とする。	○
C. 9. 20. 41	複数台の構成にて利用者情報を他のRADIUSサーバに複製する機能を持ち、複製先として動作すること。	○
C. 9. 20. 42	複製された利用者情報を参照して認証を行えること。	○
C. 9. 20. 43	EAP認証時のTLSプロトコルとしてTLS 1.3をサポートすること。	○
C. 9. 20. 44	RADIUS認証成功/失敗時に出力するログに、NAS-Identifier属性、NAS-IP-Address属性、送信元IPアドレスを出力可能であること。 もしくは、拡張ログとしてNAS-Identifier属性、NAS-IP-Address属性、送信元IPアドレスを出力できる形でも可とする。	○
C. 9. 20. 45	EAP-TLS認証成功ログに、クライアント証明書のサブジェクトとシリアル番号を出力可能であること。もしくは、コモンネームの出力ができる形でも可とする。	○
C. 9. 20. 46	全てのLANポートでRADIUSサービスを有効に出来ること。	○
C. 9. 20. 47	認証局(CA: Certificate Authority)機能を有し、X.509 version3形式のユーザー証明書、及びサーバ証明書を発行できること。	○
C. 9. 20. 48	内部に搭載されているプライベート証明機関の有効期限は最大20年、もしくは20年以上で設定できること。	○
C. 9. 20. 49	発行するデジタル証明書の有効期限は有効日数もしくは日付から選択できること。	○
C. 9. 20. 50	OCSP(Online Certificate Status Protocol)に対応し、証明書の失効状態を取得可能であること。	○
C. 9. 20. 51	発行するクライアント証明書の最大数は利用者ライセンス数の最大で2倍、もしくは4倍以上であること。	○
C. 9. 20. 52	ダッシュボードの画面、もしくは証明書申請画面から、証明書発行待ちの証明書申請の件数を確認できること。	○
C. 9. 20. 53	発行した証明書の期限切れと期限切れリマインダーを、管理者および利用者(証明書内に記載されたメールアドレス)宛にメール通知できること。期限切れ通知の場合、アプライアンス上で期限切れが確認されたタイミングでメール通知すること。期限切れリマインダーの場合、何日前(当日, 1週間前, 10日前, 30日前)に通知するかを指定できること。また、1度のみの通知か毎日通知かを選択できること。 もしくは、証明書の期限切れに関して、下記の通知できる形でも可とする。 ・期限当日通知：当日にメール通知 ・事前通知：1～998日の範囲で指定した残りの日数になった日に該当日にのみ通知 ・期限切れフォロー：期限切れのアカウントに対して、指定した曜日に週1回通知	○
C. 9. 20. 54	SCEPプロトコルによる証明書要求に応答できること。 SCEPチャレンジパスワードの確認は、チャレンジなし、固定チャレンジに対応すること。	○
C. 9. 20. 55	CA証明書の公開鍵方式は、RSA, DSA, ECCのいずれかを選択可能であること。 RSAまたはDSAを選択した場合の鍵長は、1024bits, 2048bits, 4096bits, 8192bits のいずれかを選択可能であること。ECCを選択した場合の楕円曲線は、P-256, P-384, P-521 のいずれかを選択可能であること。署名ハッシュアルゴリズムは、SHA1, SHA256, SHA384, SHA512 のいずれかを選択可能であること。 もしくは、CA証明書の公開鍵方式はRSAのみで、鍵長は1024bit、2048bit、4096bit、8192bitから選択可能な形でも可とする。	○
C. 9. 20. 56	自身のサーバ証明書の公開鍵方式は、RSA, ECCのいずれかを選択可能であること。RSAを選択した場合の鍵長は、2048bits, 4096bits のいずれかを選択可能であること。ECCを選択した場合の楕円曲線は、P-256, P-384, P-521 のいずれかを選択可能であること。署名ハッシュアルゴリズムは、SHA1, SHA256, SHA384, SHA512 のいずれかを選択可能であること。 もしくは、自身のサーバ証明書公開鍵方式はRSAのみで、鍵長は1024bit、2048bit、4096bit、8192bitから選択可能な形でも可とする。	○

C. 9. 20. 57	クライアント証明書など、CAが発行する各証明書の公開鍵方式は、RSA, DSA, ECCのいずれかを選択可能であること。RSAまたはDSAを選択した場合の鍵長は、1024bits, 2048bits, 4096bits, 8192bitsのいずれかを選択可能であること。ECCを選択した場合の楕円曲線は、P-256, P-384, P-521 のいずれかを選択可能であること。署名ハッシュアルゴリズムは、MD5, SHA1, SHA256, SHA384, SHA512 のいずれかを選択可能であること。ただし組み合わせにより指定できない値がある。 もしくは、クライアント証明書の公開鍵方式はRSAのみで、鍵長は1024bit、2048bit、4096bitから選択可能な形で可とする。	○
C. 9. 20. 58	外部CAの証明書失効リストを自動で取り込めること。	○
C. 9. 20. 59	各証明書の鍵長は4096bitsで発行できること。 CA証明書およびOCSP署名要求証明書については、工場出荷時設定が2048bitsであること。	○
C. 9. 20. 60	DHCP (Dynamic Host Configuration Protocol) サーバ機能を有し、複数の異なるネットワークに対してIPアドレスの配付ができること。	○
C. 9. 20. 61	IPアドレスの払い出し能力は500件/秒以上であること。	○
C. 9. 20. 62	リースIPアドレス数の最大は5,120以上であること。	○
C. 9. 20. 63	スコープ数の最大は128以上であること。	○
C. 9. 20. 64	登録アカウントの管理は個別のほか、CSVファイルからの一括登録・変更・削除ができること。	○
C. 9. 20. 65	利用者ページでユーザー自らパスワードの変更ができること。	○
C. 9. 20. 66	WEB管理画面からの平易な操作により設定の保存(バックアップ)と復元(リストア)が可能であること。設定の保存は手動のほか、外部サーバへの自動保存が指定できること。	○
C. 9. 20. 67	NTP(Network Time Protocol)クライアント、SNMP(Simple Network Management Protocol)エージェント機能を有すること。	○
C. 9. 20. 68	システムやRADIUS、CAサービスのログを記録できること。ログの記録先は内部のみ、もしくは内部に加え外部とする設定のいずれかより指定可能で、外部Syslogサーバへのログ出力はUDP、TCPどちらにも対応すること。	○
C. 9. 20. 69	WEB管理画面、もしくはコンソール画面からネットワーク通信状況の確認が可能であること。使用するネットワークコマンドとして、ping、traceroute、nslookup、packet captureを想定する。	○
C. 9. 20. 70	管理用コンピュータと直接コンソール接続することで、システム情報表示、設定の初期化、システムの停止、及びアクセス制御の無効化ができること。	○
C. 9. 20. 71	WEB管理画面はGoogle ChromeもしくはMicrosoft EdgeのWEBブラウザを使って操作できること。	○
C. 9. 20. 72	ダッシュボードの画面からライセンスの利用状況および認証失敗状況を確認できること。	○
C. 9. 20. 73	本サーバ自身の設置先や用途などを把握するために、機器毎にニックネームを設定し、WEB管理画面より確認できること。	○
C. 9. 20. 74	設定をサポートするために、設定画面上に配置されたボタンを選択することでヘルプを表示する機能を有すること。	○
C. 9. 20. 75	無停電電源装置 (UPS: Uninterruptible Power Supply) と連携し、USB接続またはSSH接続によるシャットダウンに対応すること。仮想版の場合はSSH接続によるシャットダウンのみ対応すること。	○
C. 9. 20. 76	4台以上の機器による冗長構成に対応すること。	○
C. 9. 20. 77	ネットワーク認証サーバへの通信に対し、機器インターフェイス、プロトコル、送信先・送信元ネットワーク情報(IPアドレス、サブネットマスク、ポート番号)の組合せにより、許可・拒否などの制御ができること。	○
C. 9. 20. 78	ユーザライセンスは1000ライセンスとし、それぞれ87ヶ月分手配すること。	○
C. 9. 21	インターネット系ファイアウォール	—
C. 9. 21. 1	ソフトウェアとハードウェアが一体となったアプライアンス製品であること。	○
C. 9. 21. 2	専用のASICを搭載し、CPUの負荷を軽減して高速処理を実現できるアーキテクチャであること。	○
C. 9. 21. 3	1000BASE-Tのポートを8ポート、5/2.5GBASE-Tのポートを8ポート以上搭載していること。	○
C. 9. 21. 4	ギガビットSFPポートを4ポート以上有していること。	○
C. 9. 21. 5	10ギガビットSFP+ポートを8ポート以上有していること。	○
C. 9. 21. 6	装置内部にログを保存するためのストレージとして、480GB以上のSSDが搭載されていること。	○
C. 9. 21. 7	コンソールポートを搭載していること。	○
C. 9. 21. 8	専用の管理インターフェースを有していること。	○
C. 9. 21. 9	IPv4ファイアウォールスルーブットは64byte UDPで26.5Gbps以上であること。	○
C. 9. 21. 10	同時セッションは、TCPで最大11,000,000以上であること。	○
C. 9. 21. 11	NAT機能を有すること。	○
C. 9. 21. 12	IEEE802.1Q VLANトランク機能を有すること。	○
C. 9. 21. 13	IEEE802.3ad リンクアグリゲーション機能を有すること (Static, LACP)	○
C. 9. 21. 14	ジャンボフレーム (9,216Bytes) をサポートすること。	○
C. 9. 21. 15	スタティック、RIP、OSPF、BGPのルーティング機能を有し、異なるルーティングプロトコルにリダイストリビューション可能なこと。	○
C. 9. 21. 16	ファイアウォールポリシーは、10000以上サポートできること。	○
C. 9. 21. 17	Active/Passiveの冗長化構成で導入できること。	○
C. 9. 21. 18	WANリンクの冗長が可能で、自動的に経路障害の検出が可能なこと。	○
C. 9. 21. 19	https対応のWEBインターフェースを有し、それ以外にSSHやTelnetによる遠隔保守が可能であること。	○
C. 9. 21. 20	GUIは一般的なWEBブラウザを利用したものであること。	○
C. 9. 21. 21	WEBUIで、CPU使用率、メモリ使用率、セッション数の推移をリアルタイムでモニタリングが可能であること。	○
C. 9. 21. 22	WEBUIは、日本語、英語、フランス語、スペイン語、ポルトガル語、中国語、韓国語に対応していること。	○
C. 9. 21. 23	WEBUI上でコマンドラインインターフェースを利用可能なこと。	○
C. 9. 21. 24	4台以上の外部Syslogサーバにログ出力可能であること。	○
C. 9. 21. 25	通信ログは、許可も拒否もログに残せること。	○
C. 9. 21. 26	仮想FW (VDM) 単位で管理者を分割することが可能なこと。	○

C. 9. 21. 27	仮想FW (VDM) ごとに設定のバックアップ・リストアが可能なこと。	○
C. 9. 21. 28	NTPクライアント機能を有すること。	○
C. 9. 21. 29	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 21. 30	消費電力が200W以下であること。	○
C. 9. 21. 31	騒音レベル55dBA以下であること。	○
C. 9. 21. 32	19インチ幅のラック搭載型として1RU以内に収納可能であること。	○
C. 9. 21. 33	冗長構成が可能であること。	○
C. 9. 22	診療系ファイアウォール非冗長	—
C. 9. 22. 1	ソフトウェアとハードウェアが一体となったアプライアンス製品であること。	○
C. 9. 22. 2	専用のASICを搭載し、CPUの負荷を軽減して高速処理を実現できるアーキテクチャであること。	○
C. 9. 22. 3	1000BASE-Tのポートを8ポート、5/2. 5GBASE-Tのポートを8ポート以上搭載していること。	○
C. 9. 22. 4	装置内部にログを保存するためのストレージとして、480GB以上のSSDが搭載されていること。	○
C. 9. 22. 5	コンソールポートを搭載していること。	○
C. 9. 22. 6	専用の管理インターフェースを有していること。	○
C. 9. 22. 7	NAT機能を有すること。	○
C. 9. 22. 8	ファイアウォールポリシーは、10000以上サポートできること。	○
C. 9. 22. 9	GUIは一般的なWEBブラウザを利用したものであること。	○
C. 9. 22. 10	WEBUIで、CPU使用率、メモリ使用率、セッション数の推移をリアルタイムでモニタリングが可能であること。	○
C. 9. 22. 11	WEBUIは、日本語、英語、フランス語、スペイン語、ポルトガル語、中国語、韓国語に対応していること。	○
C. 9. 22. 12	WEBUI上でコマンドラインインターフェースを利用可能なこと。	○
C. 9. 22. 13	4台以上の外部Syslogサーバにログ出力可能であること。	○
C. 9. 22. 14	通信ログは、許可も拒否もログに残せること。	○
C. 9. 22. 15	NTPクライアント機能を有すること。	○
C. 9. 22. 16	SNMPエージェント機能を有し、SNMPv1/v2c/v3に対応可能であること。	○
C. 9. 22. 17	消費電力が200W以下であること。	○
C. 9. 22. 18	騒音レベル55dBA以下であること。	○
C. 9. 22. 19	19インチ幅のラック搭載型として1RU以内に収納可能であること。	○
C. 9. 23	ネットワーク監視サーバ	—
C. 9. 23. 1	以下、仕様を満たすネットワーク監視サーバを1台用意すること。(物理アプライアンス製品でも可)。もしくはネットワーク監視ソフトウェアと一体型のアプライアンス監視サーバを提案する形で可とする。また、以下に記載の製品を手配すること。	○
C. 9. 23. 2	サーバは1Uラックマウント型にて選定すること。	○
C. 9. 23. 3	16GB以上のメモリを搭載すること。	○
C. 9. 23. 4	以下、仕様を満たすラックマウント型UPSを1台用意すること。なお、サーバ室設置ネットワーク機器用のUPSと共用する形で可とする。共用する場合は、以下の仕様項目は○回答で行い、コメント欄にネットワーク機器用のUPSと共用する旨を記載すること。	○
C. 9. 23. 5	運転方式は常時商用給電方式であること。	○
C. 9. 23. 6	相数は「単相2線+接地 (D種以上)」であること。	○
C. 9. 23. 7	定格入力電圧は100Vに対応していること。	○
C. 9. 23. 8	定格周波数は50/60Hzであること。	○
C. 9. 23. 9	出力電力容量は750VA/525W以上であること。	○
C. 9. 23. 10	発熱量は254kJ/h以下であること (急速充電時)	○
C. 9. 23. 11	入力端子はNEMA 5-15Pであること。またケーブルも添付されていること。	○
C. 9. 23. 12	出力端子はNEMA 5-15R ×4個以上であること。	○
C. 9. 23. 13	質量は20kg以下であること。	○
C. 9. 23. 14	バッテリー期待寿命は3年以上であること (周囲温度20℃平均時)	○
C. 9. 24	ネットワーク監視ソフトウェア	—
C. 9. 24. 1	以下、仕様を満たすネットワーク監視ソフトウェアを1個用意すること。アプライアンス製品でも可とする。	○
C. 9. 24. 2	クライアントソフトまたはWEBブラウザからGUIで管理する機能を有すること。	○
C. 9. 24. 3	監視の目的に応じた内容をまとめたダッシュボードを表示する機能を有すること。	○
C. 9. 24. 4	マップを用いて監視ができ、障害箇所が視覚的にわかること。	○
C. 9. 24. 5	マップ上のアイコンを警告や異常などの重要度に応じて表現できること。	○
C. 9. 24. 6	マップは自由にカスタマイズ可能なこと。	○
C. 9. 24. 7	GUIからの操作により、ネットワークに接続された機器の自動発見ができること。	○
C. 9. 24. 8	ネットワークを構成する機器の接続情報を収集し、物理トポロジの自動、もしくは手動描画ができる機能を有すること。	○
C. 9. 24. 9	ユーザ毎に操作権限を設定できること。	○
C. 9. 24. 10	メールやパトランプによる通報が可能なこと。	○
C. 9. 24. 11	Pingによる死活監視ができること。	○
C. 9. 24. 12	SNMPによる監視ができること。	○
C. 9. 24. 13	NW機器が出力するsyslog監視ができること。	○
C. 9. 24. 14	ベンダーMIBを追加・修正できること。	○
C. 9. 24. 15	ネットワーク機器にリモート接続して操作できること。	○
C. 9. 24. 16	性能データに対してアノマリー分析、トレンド分析をリアルタイムに行い、障害の予兆検知やキャパシティ管理ができる機能を有すること。もしくは、管理している機器のハードウェアメトリック、および、デバイスインターフェースのエラー統計に基づき障害の予兆検知やキャパシティ管理ができる機能を有する形で可とする。	○
C. 9. 24. 17	システム規模が拡張した場合もマネージャ階層化などにより、一元管理を実現できる機能を有すること。	○
C. 9. 25	Syslogサーバ	—

C. 9. 25. 1	以下、仕様を満たすSyslog管理用ソフトウェアを1個用意すること。アプライアンス製品でも可とする。	○
C. 9. 25. 2	GUIベースのシスログマネージャであること。	○
C. 9. 25. 3	受信ログのリアルタイム表示ができること。	○
C. 9. 25. 4	ログファイルの自動スプリット機能を有すること。	○
C. 9. 25. 5	UDP/TCP/SNMP受信機能を有すること。	○
C. 9. 25. 6	高負荷環境でのメッセージ受信に対応するメッセージバッファ機能を有すること。	○
C. 9. 25. 7	WEB GUI(ブラウザ)で閲覧できる機能を標準で装備していること。直近4GBまでのログを閲覧・検索できること。	○
C. 9. 25. 8	アクティビティとログ管理をスケジュール化できる機能を有すること。	○
C. 9. 25. 9	アーカイブ/クリーンアップ/プログラム実行ができるスケジューラ機能を有すること。	○
C. 9. 25. 10	複数ウィンドウによる同時ログ出力ができること。	○
C. 9. 25. 11	ログ転送時に送信元IPをそのまま保持できること。	○
C. 9. 25. 12	トレンド解析グラフを表示できること。	○
C. 9. 25. 13	統計データをメールで送信できること。	○
C. 9. 25. 14	処理速度は1時間あたり最大200万メッセージ以上であること。	○
C. 9. 25. 15	閾値によるアラート機能を有すること。	○
C. 9. 25. 16	定期的な統計レポートのメール送信(時、日、週、月)/ディスク容量監視/受信数閾値監視のアラーム機能を有すること。	○
C. 9. 25. 17	アーカイブファイルの圧縮および暗号化ができること。	○
C. 9. 25. 18	世代数指定/ログサイズ指定(B, KB, MB, GB)/時間指定(分、時、日、半日、週、月、四半期、年)ができるログローテーション機能を有すること。もしくは、監視対象装置のConfigの世代管理、世代間の比較ができる形でも可とする。	○
C. 9. 26	その他	—
C. 9. 26. 1	パトランプを2個用意すること。	○
C. 9. 27	UPS要件(サーバ室以外)	—
C. 9. 27. 1	サーバ室以外に設置されるネットワーク機器は、原則UPSからの電源供給とすること。	○
C. 9. 27. 2	設置されるネットワーク機器に十分な時間供給できるUPSを選定すること。	○
C. 9. 28	無線LANサーベイ	—
C. 9. 28. 1	無線アクセスポイントの更新及び新規無線アクセスポイントの設置が完了した時点で、無線アクセスポイントの電波調査を行うこと。	○
C. 9. 28. 2	電波調査を行った後に電波調査報告書として各周波数帯での電波強度、カバレッジエリア、外来波、不正AP等の確認結果を報告すること。	○
C. 9. 29	成果物	—
C. 9. 29. 1	以下に記載した成果品の納入は紙媒体と電子記憶媒体とする。紙媒体の書式については、A4版縦書き片面印刷(A3Z折り可)を基本とし、電子記憶媒体はCD-ROMもしくはDVD-ROMとする。	○
C. 9. 29. 2	また、電子記憶媒体は、MicrosoftWord、MicrosoftExcelとし、その他の形式は当センターの承認を得た形式とする。電子記憶媒体にはウイルスチェックを行った日時、ウイルス対策ソフト名、パターンファイルバージョンを記載すること。	○
C. 9. 29. 3	部数は2部を原則とし、これによらない場合は協議を行うこと。	○
C. 9. 29. 4	①ネットワーク設計書(基本設計、詳細設計、移行設計)	○
C. 9. 29. 5	②ネットワーク構成図(物理構成図、論理構成図)	○
C. 9. 29. 6	③導入機器一覧表	○
C. 9. 29. 7	④IPアドレス管理表、VLAN管理表	○
C. 9. 29. 8	⑤スイッチポート表(パッチパネル管理表)	○
C. 9. 29. 9	⑥アカウント一覧表	○
C. 9. 29. 10	⑦ライセンス管理表	○
C. 9. 29. 11	⑧配線図面(配線系統図、情報コンセントプロット図、無線アクセスポイントプロット図)	○
C. 9. 29. 12	⑨ラック実装図	○
C. 9. 29. 13	⑩各種試験成績書	○
C. 9. 29. 14	⑪運用管理マニュアル	○
C. 9. 29. 15	⑫UPS電源系統図、配置図	○
C. 9. 29. 16	⑬事前、事後無線サーベイ報告書	○
C. 10	次期ネットワークにおける新機能	—
C. 10. 1	NDR (Network Detection and Response)	—
C. 10. 1. 1	基本機能	—
C. 10. 1. 1. 1	監視対象として1000IP以上の監視ができること。	○
C. 10. 1. 1. 2	GUIによる解析結果表示機能を有すること。	○
C. 10. 1. 1. 3	NDRを提案する上で、必要となるハードウェア、ソフトウェアがある場合は、NDRに加えてそれらの初期費用と7年分の保守費用を全て本調達に含めること。	●
C. 10. 1. 2	ネットワークトラフィックの監視・分析に関する要件	—
C. 10. 1. 2. 1	日常的な通信パターンを機械学習し、それと異なる不審な通信を自動的に検知できること。	○
C. 10. 1. 2. 2	コマンドアンドコントロール(C&C)攻撃、ランサムウェア、違法仮想通貨マイニング、未知のマルウェア、組織内に潜む脅威などを表示、分析できること。また、脅威の情報がダッシュボードに表示できること。	○
C. 10. 1. 2. 3	通信ログ(トラフィック、ファイアウォールログ、パケット(Flow統計情報でも可))を収集・解析して、脅威の兆候を検出できること。	○
C. 10. 1. 2. 4	収集した過去の通信ログ情報を任意の条件(期間、IP、IPグループ、ポート番号、バイト数など)で検索・表示できること。	○
C. 10. 1. 2. 5	誤検知を減らす目的で、正常な通信が脅威として検出されないように、各イベントの発生閾値のチューニングが可能であること。(例:特定のIPにおいて、特定のトラフィックが発生した場合には、そのイベントをホワイトリストに登録するなどしてアラートが上がらないようにする。)	○

C. 10. 1. 2. 6	内部ネットワーク上の感染端末によるスキャン行為や脆弱性スキャンなどの偵察行動や、典型的な悪意ある振る舞いを検知できること。	○
C. 10. 1. 2. 7	SSHの連続した認証の失敗、DNSサーバへの大量のクエリ送信等、不正な活動の兆候を捉え、インシデントの発生を検知できること。	○
C. 10. 1. 2. 8	MACアドレスや端末名などにより、IPが変わっても同一端末として識別し、継続的な監視ができること。	○
C. 10. 1. 2. 9	既知のパターンマッチングやシグネチャに依存しない、未知の脅威やマルウェアへの感染や疑わしい挙動を検出できること。	○
C. 10. 1. 2. 10	通信元・通信先・通信量・時間帯などのトラフィック特性から異常を自動学習・分析し、インシデントの検出基準として用いること。	○
C. 10. 1. 2. 11	脅威を保持すると判断したPCについて検索機能を有し、特定のデバイスに関する詳細な情報を収集できること。	○
C. 10. 1. 2. 12	収集したログまたはトラフィックから、脅威と判断した情報をイベントログとして、Syslog サーバもしくは SIEM に送信可能であること。	○
C. 10. 1. 3	セキュリティ挙動検出・分析に関する要件	—
C. 10. 1. 3. 1	一般的なサンドボックス環境では検出困難な最新のマルウェアや攻撃にも対応できること。	○
C. 10. 1. 3. 2	継続的に動作する教師なし学習により、通常と異なる行動・リスクの高い挙動を自動的に識別できること。また、契約満了まで機械学習が停止することなく継続されること。	○
C. 10. 1. 3. 3	リアルタイムでの通信の監視・分析ができるだけでなく、特定端末の通信状況を最大1か月まで遡って確認できる機能を有すること。	○
C. 10. 1. 4	通信制御・ブロック機能に関する要件	—
C. 10. 1. 4. 1	特定の異常通信に対して、リセットパケットを用いることでアラートの元となった異常通信を自動的に遮断できること。もしくは、アラートの元となった異常通信の宛先を送信元を確認し、Firewall等に管理者にて通信遮断を行うための情報を提供可能な形で可とする。	○
C. 10. 1. 4. 2	この通信遮断機能は動作対象となったデバイスに対してエージェントを事前にインストールすることなく機能すること。Firewall等に管理者にて通信遮断を行うための情報を提供する場合は、この限りではない。	○
C. 10. 1. 4. 3	通信遮断の範囲は管理者にてチューニングできることとし、特定の通信の遮断からデバイスの隔離など範囲を選べること。	○
C. 10. 1. 5	SOCサービス	—
C. 10. 1. 5. 1	NDRの運用監視・リモートレスポンスサービスを7年分本調達に含めること。フォレンジック、現地対応は本調達に含まないが、NDR上のログから判明する範囲(どのIPといつ通信したか等)の調査結果はレポートに含めること。	●
C. 10. 1. 5. 2	監視時間は24時間365日とすること。	○
C. 10. 1. 5. 3	リアルタイムアラート監視として、NDRが検知したセキュリティイベントの常時監視すること。	○
C. 10. 1. 5. 4	相関分析・トリアージとして、発生したアラートが「真の脅威」か「誤検知」かをSOCアナリストが判定すること。	○
C. 10. 1. 5. 5	エスカレーションとして、危険度が高いと判断された事象の速報通知（メール・電話）を行うこと。	○
C. 10. 1. 5. 6	月次レポートの提供として、脅威傾向の分析、および検知精度向上のためのチューニング提案を行うこと。	○