

松阪市庁内ネットワーク構築及び 機器等賃貸借・運用保守業務

【別紙】 機器仕様書

令和 5 年 3 月

松阪市 企画振興部

デジタル未来戦略局 情報システム課

【目次】

1. 更新機器の調達	1
2. 基本事項	1
3. ハードウェア調達	2
3.1. コアスイッチ A	2
3.2. コアスイッチ B	6
3.3. レイヤ 3 スwitch A	9
3.4. レイヤ 3 スwitch B	11
3.5. レイヤ 2 スwitch A	13
3.6. レイヤ 2 スwitch B	15
3.7. PoE 対応レイヤ 2 スwitch	17
3.8. PoE 対応アクセスレイヤ 2 スwitch	19
3.9. アクセスレイヤ 2 スwitch	21
3.10. 外局収容ルータ	23
3.11. 外局接続用ルータ	25
3.12. 基幹ファイアウォール	27
3.13. ファイアウォール A	28
3.14. ファイアウォール B	29
3.15. ファイアウォール C	30
3.16. 無線 LAN コントローラ	31
3.17. 無線 LAN アクセスポイント A	34
3.18. 無線 LAN アクセスポイント B	36
3.19. 無線 LAN 管理サーバ	38
3.20. 無線 LAN ロケーション管理サーバ	39
3.21. ネットワーク認証サーバ	40
3.22. NAS サーバ	42
3.23. SFP	43
3.24. 仮想基盤用ラックマウントサーバ	44
3.25. バックアップサーバ	46
3.26. 共有ストレージ	49
3.27. 管理用パソコン	51
4. ソフトウェア及びライセンス調達	52
4.1. インターネット分離システム	52
4.2. メール無害化システム	55

4.3. WEB メールシステム	57
4.4. スпамメール対策システム	59
4.5. ファイル無害化システム	60
4.6. 内部ファイル交換システム	63
4.7. 外部ファイル交換システム	64
4.8. ID 連携用システム	65
4.9. 仮想化基盤ウイルス対策システム	66
4.10. バックアップシステム	67
4.11. 負荷分散装置	69
4.12. SYSLOG サーバ	72
4.13. サーバ仮想化ソフトウェア仕様	73
4.14. 各種 OS ソフトウェア	74
4.15. WEB コンテンツフィルタ	75
4.16. 資産管理システム	78
4.17. ウイルス対策システム	79
5. 光幹線工事及び各種工事部材等仕様	80
5.1. フロア機器収納ボックス	80
5.2. 光ファイバーケーブル	80
5.3. 光パッチコード	80
5.4. UTP ケーブル	80
5.5. UTP パッチコード	81
5.6. UTP 情報コンセント	81
5.7. 電源ケーブル	81
5.8. PDU・OA タップ	81
6. データセンター ハウジング	82
6.1. ハウジング環境	82

1. 更新機器の調達

以下に要求仕様及び想定する機種を示す。想定機種以外の製品を使用する場合は、指定日までに「同等品承諾願書」と同等以上の性能を有することを示した機能証明書（カタログ等）と機器選択理由を明記し（任意様式）、を松阪市（以下、「本市」という。）へ提出し承認を得ること。

2. 基本事項

1. 本仕様書に記載されていない事項で、各機器で正常に機能するために必要と思われるものは追加して装備し、仕様上、疑義や不明が生じた場合、本市の指示に従うこと。
2. 特に記載のない限り、未使用品の新品にて対応すること。

3. ハードウェア調達

以下に要求仕様及び想定する機種を示す。

3.1. コアスイッチ A

【想定機種：シスコシステムズ社製 C9500-24Y4C-A】 【数量：2 台】

1. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
2. IEEE802.1D に準拠したスパンニングツリー機能を有すること。
3. IEEE802.1w に準拠した高速スパンニングツリー機能を有すること。
4. IEEE802.1s に準拠したマルチプル・スパンニングツリー機能を有すること。
5. IEEE 802.3ad に準拠した Link Aggregation 機能を有すること。
6. ユニキャストルーティングとして、Static、RIPv1/v2、RIPng、OSPF、OSPFv3、BGPv4、IS-ISv4 に対応していること。
7. ポートにてリンクフラップ等の障害を検知した際、ポートを一時的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
8. ゲートウェイ冗長プロトコル機能を有すること。
9. IGMP Filtering、IGMP snooping 機能を有すること。
10. MLDv1/v2 snooping 機能を有すること。
11. 4,000 個以上の VLAN ID が利用可能であること。
12. スイッチ仮想インタフェースを 1,000 個以上利用可能であること。
13. 9,000 バイト以上のジャンボフレームに対応していること。
14. IPv4/IPv6 デュアルスタック機能を有すること。
15. マルチキャスト DNS(mDNS)ゲートウェイ機能をサポートし、Apple mDNS(Bonjour)プロトコルを使用して広告されるサービスを見つけることが出来ること。
16. ポートあたり 8 個のキューを有すること。
17. 設定情報レート (CIR) または最大情報レート (PIR) でレート制限が行えること。
18. トラフィックを照合し、パケットラベル (DSCP) に基づき、一致するパケットを自動的に QoS グループに割り当てる機能を有すること。
19. モジュラー型 QoS 機能を有すること。
20. Class-Based Shaping 機能を有すること。
21. Priority Queueing 機能を有すること。

22. IEEE802.1p の CoS 優先制御機能を有すること。
23. 階層型 QoS 機能を有すること。
24. ACL、IP Precedence、DSCP、COS によってトラフィックを分類する機能を有すること。
25. 輻輳回避の仕組みとして、WTD、WRED を有すること。
26. アクセスまたはトランクポートにて学習される MAC アドレスの数やアドレスにより制限する機能を有すること。
27. IEEE802.1X および IEEE802.1X-REV 認証機能を有すること。
28. VLAN、ルータ、およびポートの ACL 機能を有すること。
29. CPU（コントロールプレーン）への通信のレート・リミッタ機能を有すること。
30. 同一 VLAN 上でブロードキャストドメインの分割をし、通信制限を行うセキュリティ機能を有すること。
31. BPDU の受信時にスパニングツリーPortFast 対応インターフェイスをシャットダウンして、予期せぬトポロジループを阻止する機能を有すること。
32. ネットワーク管理者の予期しないエッジ デバイスが、スパニングツリープロトコルのルートノードになることを阻止する機能を有すること。
33. 光ファイバやツイストペアケーブルの単一方向リンク（片対障害）検出機能を有すること。
34. ARP Spoofing などの攻撃を防止するため、ARP パケットを検査する機能を有すること。
35. 管理者の想定しない DHCP サーバによる、DHCP サービスを防止するため、DHCP サービスを提供できるインタフェースを指定できること。
36. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム制御機能を有すること。
37. サブリカントとして上位スイッチにて IEEE802.1X を用いて認証される機能を有すること。
38. 日時や時間帯を指定できるアクセスリスト機能を有すること。
39. IEEE802.1X ユーザ認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
40. IEEE802.1X 未対応端末に対応するため、ゲスト VLAN 機能を有すること。
41. IEEE802.1X 認証ユーザに対し、ユーザ単位で異なるアクセスリストを適用できること。
42. 送信元/受信元 MAC アドレスの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
43. 送信元/受信元 IP アドレス、TCP/UDP ポート番号、またはこれらのフィールドの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。

44. IEEE802.1AE に準拠したレイヤ 2 フレーム暗号化機能を有すること。
45. GUI を使用して設定を行える機能を有すること。
46. シリアル接続によるコンソールポートを有すること。
47. Telnet/SSH によるリモートコンソール機能を有すること。
48. トラフィック解析のためポートのミラーリング機能を有しすること。ミラー先は同一筐体内や他の筐体へ VLAN を使いミラーリングできる機能を有すること。
49. トラフィック解析のため、他の筐体のポートを L3 を経由してミラーリングできる機能を有すること。
50. ソフトウェア及び設定情報を TFTP にてアップロード及びダウンロードが可能であること。
51. NTP クライアントとして時刻同期可能なこと。
52. Syslog サーバにメッセージを送信する機能を有すること。
53. SNMPv1/v2c/v3 による管理機能を有すること。
54. Flexible NetFlow 機能を有すること。
55. フロー情報からアプリケーションを識別する機能を有すること。
56. 隣接するデバイスの情報を取得するプロトコルを有すること。
57. ネットワークおよび機器単体の障害に備えて、詳細なデバッグ機能を有していること。
58. スイッチが接続される端末の DHCP サーバとなる機能を有すること。
59. リモートから機器内で、Wireshark 等の汎用アプリケーションで解読可能なパケットキャプチャを取得する機能を有すること。
60. 稼動中に機器動作の信頼性を維持するための総合的な自己診断機能を有すること。
61. 送信元デバイスから宛先デバイスまでのパケットの L2 パスを確認する機能を有すること。
62. 機器のアップタイム、温度、電圧とともにハードウェア関連のシステムメッセージをフラッシュに保存する機能を有すること。
63. 19 インチラックマウント可能であり、1RU 以下であること。
64. 1/10/25 ギガビットイーサネットを 24 ポート、40 ギガビットイーサネットを 4 ポート実装していること。(トランシーバは別途必要)
65. AC200V に対応していること
66. エアフローが前面吸気、背面排気に対応していること。
67. 最大 2.0Tbps の帯域幅を有すること。
68. 転送レートは、1Bpps 以上の性能を有すること。
69. MAC アドレス数は 82,000 以上に対応可能であること。
70. IPv4 の間接・直接ルート数は、256,000 以上に対応可能であること。

- 71. IPv4 のホストルート数は、90,000 以上に対応可能であること。
- 72. QoS ACL のスケールは、16,000 以上に対応可能であること。
- 73. セキュリティ ACL のスケールは、27,000 以上に対応可能であること。
- 74. VLAN ID は 4,000 以上に対応可能であること。
- 75. 構成に必要なライセンスを契約期間中有していること。

3.2. コアスイッチ B

【想定機種：シスコシステムズ社製 C9500-48Y4C-A】 【数量：2 台】

1. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
2. IEEE802.1D に準拠したスパニングツリー機能を有すること。
3. IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
4. IEEE802.1s に準拠したマルチプル・スパニングツリー機能を有すること。
5. IEEE 802.3ad に準拠した Link Aggregation 機能を有すること。
6. ユニキャストルーティングとして、Static、RIPv1/v2、RIPng、OSPF、OSPFv3、BGPv4、IS-ISv4 に対応していること。
7. ポートにてリンクフラップ等の障害を検知した際、ポートを一時的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
8. ゲートウェイ冗長プロトコル機能を有すること。
9. IGMP Filtering、IGMP snooping 機能を有すること。
10. MLDv1/v2 snooping 機能を有すること。
11. 4,000 個以上の VLAN ID が利用可能であること。
12. スイッチ仮想インタフェースを 1,000 個以上利用可能であること。
13. 9,000 バイト以上のジャンボフレームに対応していること。
14. IPv4/IPv6 デュアルスタック機能を有すること。
15. ポートあたり 8 個のキューを有すること。
16. 設定情報レート（CIR）または最大情報レート（PIR）でレート制限が行えること。
17. トラフィックを照合し、パケットラベル（DSCP）に基づき、一致するパケットを自動的に QoS グループに割り当てる機能を有すること。
18. モジュラー型 QoS 機能を有すること。
19. Class-Based Shaping 機能を有すること。
20. Priority Queueing 機能を有すること。
21. IEEE802.1p の CoS 優先制御機能を有すること。
22. 階層型 QoS 機能を有すること。
23. ACL、IP Precedence、DSCP、COS によってトラフィックを分類する機能を有すること。
24. 輻輳回避の仕組みとして、WTD、WRED を有すること。
25. アクセスまたはトランクポートにて学習される MAC アドレスの数やアドレスに

より制限する機能を有すること。

26. IEEE802.1X および IEEE802.1X-REV 認証機能を有すること。
27. VLAN、ルータ、およびポートの ACL 機能を有すること。
28. CPU（コントロールプレーン）への通信のレート・リミッタ機能を有すること。
29. 同一 VLAN 上でブロードキャストドメインの分割をし、通信制限を行うセキュリティ機能を有すること。
30. BPDU の受信時にスパニングツリーPortFast 対応インターフェイスをシャットダウンして、予期せぬトポロジループを阻止する機能を有すること。
31. ネットワーク管理者の予期しないエッジ デバイスが、スパニングツリープロトコルのルートノードになることを阻止する機能を有すること。
32. 光ファイバやツイストペアケーブルの単一方向リンク（片対障害）検出機能を有すること。
33. ARP Spoofing などの攻撃を防止するため、ARP パケットを検査する機能を有すること。
34. 管理者の想定しない DHCP サーバによる、DHCP サービスを防止するため、DHCP サービスを提供できるインタフェースを指定できること。
35. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム制御機能を有すること。
36. サブリカントとして上位スイッチにて IEEE802.1X を用いて認証される機能を有すること。
37. 日時や時間帯を指定できるアクセスリスト機能を有すること。
38. IEEE802.1X ユーザ認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
39. IEEE802.1X 未対応端末に対応するため、ゲスト VLAN 機能を有すること。
40. IEEE802.1X 認証ユーザに対し、ユーザ単位で異なるアクセスリストを適用できること。
41. 送信元/受信元 MAC アドレスの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
42. 送信元/受信元 IP アドレス、TCP/UDP ポート番号、またはこれらのフィールドの任意の組み合わせに基づくパケットフィルタを行う機能を有すること。
43. IEEE802.1AE に準拠したレイヤ 2 フレーム暗号化機能を有すること。
44. GUI を使用して設定を行える機能を有すること。
45. シリアル接続によるコンソールポートを有すること。
46. Telnet/SSH によるリモートコンソール機能を有すること。
47. トラフィック解析のためポートのミラーリング機能を有しすること。ミラー先は同一筐体内や他の筐体へ VLAN を使いミラーリングできる機能を有すること。

48. トラフィック解析のため、他の筐体のポートを L3 を経由してミラーリングできる機能を有すること。
49. ソフトウェア及び設定情報を TFTP にてアップロード及びダウンロードが可能であること。
50. NTP クライアントとして時刻同期可能なこと。
51. Syslog サーバにメッセージを送信する機能を有すること。
52. SNMPv1/v2c/v3 による管理機能を有すること。
53. Flexible NetFlow 機能を有すること。
54. フロー情報からアプリケーションを識別する機能を有すること。
55. 隣接するデバイスの情報を取得するプロトコルを有すること。
56. ネットワークおよび機器単体の障害に備えて、詳細なデバッグ機能を有していること。
57. スイッチが接続される端末の DHCP サーバとなる機能を有すること。
58. リモートから機器内で、Wireshark 等の汎用アプリケーションで解読可能なパケットキャプチャを取得する機能を有すること。
59. 稼動中に機器動作の信頼性を維持するための総合的な自己診断機能を有すること。
60. 送信元デバイスから宛先デバイスまでのパケットの L2 パスを確認する機能を有すること。
61. 機器のアップタイム、温度、電圧とともにハードウェア関連のシステムメッセージをフラッシュに保存する機能を有すること。
62. 19 インチラックマウント可能であり、1RU 以下であること。
63. 1/10/25 ギガビットイーサネットを 48 ポート、40 ギガビットイーサネットを 4 ポート実装していること（トランシーバは別途必要）
64. AC200V 及び AC100V 電源に対応していること
65. エアフローが前面吸気、背面排気に対応していること。
66. 最大 3.2Tbps の帯域幅を有すること。
67. 転送レートは、1Bpps 以上の性能を有すること。
68. MAC アドレス数は 82,000 以上に対応可能であること。
69. IPv4 の間接・直接ルート数は、256,000 以上に対応可能であること。
70. IPv4 のホストルート数は、90,000 以上に対応可能であること。
71. マルチキャストルート数は、32,000 以上に対応可能であること。
72. QoS ACL のスケールは、16,000 以上に対応可能であること。
73. セキュリティ ACL のスケールは、27,000 以上に対応可能であること。
74. VLAN ID は 4,000 以上に対応可能であること。
75. 構成に必要なライセンスを契約期間中有していること。

3.3. レイヤ 3 スイッチ A

【想定機種：シスコシステムズ社製 C9300-24P-E】 【数量：10 台】

1. スイッチング容量 208Gbps 以上を有すること。
2. スタック構成で 688Gbps 以上のスタック間のスループットを有すること。
3. 専用ケーブルで複数のスイッチを一台として管理する機能を有すること。
4. スタック上のステートフルフェールオーバー（SSO）をサポートしていること。
5. スタック内での電源共有が可能な機能を有すること。
6. 10/100/1000 イーサネットポートを 24 ポート以上実装していること。
7. 1 ギガビットイーサネット SFP を 4 ポート以上実装していること。
8. 10/100/1000 イーサネットポートを 12 ポート以上で最大 30w までサポートできる PoE+（IEEE802.3at）ポートを実装していること。
9. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
10. IEEE802.1D に準拠したスパニングツリー機能を有すること。
11. IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
12. IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
13. IEEE802.1x に準拠した認証機能を有すること。
14. IEEE802.1x 認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
15. IEEE802.3ad Link Aggregation 機能を有すること。
16. マルチシャシ・イーサチャネル（シャシを跨って、複数の Ethernet ポートを束ねて 1 つの高速なポートとして利用可能な機能）をサポートすること。
17. IEEE802.1p も優先制御機能（QoS）を有すること。
18. ユニキャストルーティングとして、Static、RIPv1/v2、OSPF Routed Access、に対応していること。
19. モジュラー型 QoS 機能を有すること。
20. 4,000 個以上の VLAN をサポートしていること。
21. ポートにてリンクフラップ等の機能を検知した際、ポートを自動的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
22. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム抑制機能を有すること。
23. ゲートウェイ冗長プロトコルに対応していること。
24. シリアル接続によるコンソールポートを有すること。
25. Telnet/SSH によるリモートコンソール機能を有すること。

- 26. NTP クライアント機能を有すること。
- 27. Syslog サーバにメッセージを送信する機能を有すること。
- 28. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
- 29. SNMPv1/v2c/v3 による管理機能を有すること。
- 30. L3 スイッチ機能で DHCP リレー機能を有すること。
- 31. トラフィック解析のためのポートをミラーリングする機能を有すること。ミラー先は同一筐体内や他の筐体へ VLAN を使いミラーリングをできる機能を有すること。
- 32. 同一筐体内で電源の二重化機能を有すること。
- 33. 19 インチラックに格納できること。
- 34. 1U 以内のラックマウント型の形状であること。
- 35. 構成に必要なライセンスを契約期間中有していること。

3.4. レイヤ 3 スイッチ B

【想定機種：シスコシステムズ社製 C9300X-12Y-E】 【数量：2 台】

1. スイッチング容量 1,000Gbps 以上を有すること。
2. スタック構成で 2,000Gbps 以上のスタック間のスループットを有すること。
3. 744.04Mpps 以上の転送レートを有すること。
4. 専用ケーブルで複数のスイッチを一台として管理する機能を有すること。
5. スタック上のステートフルフェールオーバー（SSO）をサポートしていること。
6. スタック内での電源共有が可能な機能を有すること。
7. 1/10/25 ギガビットイーサネット SFP28 を 12 ポート以上実装していること。
8. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
9. IEEE802.1D に準拠したスパニングツリー機能を有すること。
10. IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
11. IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
12. IEEE802.1x に準拠した認証機能を有すること。
13. IEEE802.1x 認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
14. IEEE802.3ad Link Aggregation 機能を有すること。
15. マルチシャーシ・イーサチャネル（シャーシを跨って、複数の Ethernet ポートを束ねて 1 つの高速なポートとして利用可能な機能）をサポートすること。
16. IEEE802.1p も優先制御機能（QoS）を有すること。
17. ユニキャストルーティングとして、Static、RIPv1/v2、OSPF Routed Access に対応していること。
18. モジュラー型 QoS 機能を有すること。
19. 4,000 個以上の VLAN をサポートしていること。
20. 9,000 バイト以上のジャンボフレームに対応していること。
21. ポートにてリンクフラップ等の機能を検知した際、ポートを自動的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
22. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム抑制機能を有すること。
23. ゲートウェイ冗長プロトコルに対応していること。
24. シリアル接続によるコンソールポートを有すること。
25. Telnet/SSH によるリモートコンソール機能を有すること。

- 26. NTP クライアント機能を有すること。
- 27. Syslog サーバにメッセージを送信する機能を有すること。
- 28. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
- 29. SNMPv1/v2c/v3 による管理機能を有すること。
- 30. L3 スイッチ機能で DHCP リレー機能を有すること。
- 31. トラフィック解析のためのポートをミラーリングする機能を有すること。ミラー先は同一筐体内や他の筐体へ VLAN を使いミラーリングをできる機能を有すること。
- 32. 同一筐体内で電源の二重化機能を有すること。
- 33. 19 インチラックに格納できること。
- 34. 1U 以内のラックマウント型の形状であること。
- 35. 構成に必要なライセンスを契約期間中有していること。

3.5. レイヤ 2 スイッチ A

【想定機種：シスコシステムズ社製 C9200-24T-E】 【数量：28 台】

1. スイッチング容量 208Gbps 以上を有すること。
2. スタック構成で 688Gbps 以上のスタック間のスループットを有すること。
3. スタック上のステートフルフェールオーバー（SSO）をサポートしていること。
4. 10/100/1000 イーサネットポートを 24 ポート以上実装していること。
5. 10 ギガビットイーサネット SFP+を 4 ポート以上実装していること。
6. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
7. IEEE802.1D に準拠したスパニングツリー機能を有すること。
8. IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
9. IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
10. IEEE802.1x に準拠した認証機能を有すること。
11. IEEE802.1x 認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
12. IEEE802.3ad Link Aggregation 機能を有すること。
13. マルチシャシ・イーサチャネル（シャシを跨って、複数の Ethernet ポートを束ねて 1 つの高速なポートとして利用可能な機能）をサポートすること。
14. IEEE802.1p も優先制御機能（QoS）を有すること。
15. ユニキャストルーティングとして、Static、RIPv1/v2、OSPF Routed Access に対応していること。
16. モジュラー型 QoS 機能を有すること。
17. 4,000 個以上の VLAN をサポートしていること。
18. 9,000 バイト以上のジャンボフレームに対応していること。
19. ポートにてリンクフラップ等の機能を検知した際、ポートを自動的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
20. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム抑制機能を有すること。
21. GUI を使用して設定を行える機能を有すること。
22. シリアル接続によるコンソールポートを有すること。
23. Telnet/SSH によるリモートコンソール機能を有すること。
24. NTP クライアント機能を有すること。
25. Syslog サーバにメッセージを送信する機能を有すること。
26. 隣接するデバイス間でトポロジ管理を行う機能を有すること。

- 27. SNMPv1/v2c/v3 による管理機能を有すること。
- 28. トラフィック解析のためのポートをミラーリングする機能を有すること。ミラー先は同一筐体内や他の筐体へ VLAN を使いミラーリングをできる機能を有すること。
- 29. 19 インチラックに格納できること。
- 30. 1U 以内のラックマウント型の形状であること。
- 31. 構成に必要なライセンスを契約期間中有していること。

3.6. レイヤ 2 スイッチ B

【想定機種：シスコシステムズ社製 C9200L-24T-4G-E】【数量：102 台】

1. スイッチング容量 56Gbps 以上を有すること。
2. 転送レートは 41.66Mpps 以上を有すること。
3. 10/100/1000 イーサネットポートを 24 ポート以上実装していること。
4. 1 ギガビットイーサネット SFP を 4 ポート以上実装可能なこと。
5. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
6. IEEE802.1D に準拠したスパンニングツリー機能を有すること。
7. IEEE802.1w に準拠した高速スパンニングツリー機能を有すること。
8. IEEE802.1s に準拠した多重スパンニングツリー機能を有すること。
9. IEEE802.1x に準拠した認証機能を有すること。
10. IEEE802.1x 認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
11. IEEE802.3ad Link Aggregation 機能を有すること。
12. IEEE802.1p も優先制御機能（QoS）を有すること。
13. ユニキャストルーティングとして、Static、RIPv1/v2、OSPF Routed Access に対応していること。
14. モジュラー型 QoS 機能を有すること。
15. 4,000 個以上の VLAN をサポートしていること。
16. 9,000 バイト以上のジャンボフレームに対応していること。
17. ポートにてリンクフラップ等の機能を検知した際、ポートを自動的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
18. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム抑制機能を有すること。
19. GUI を使用して設定変更する機能を有すること。
20. シリアル接続によるコンソールポートを有すること。
21. Telnet/SSH によるリモートコンソール機能を有すること。
22. NTP クライアント機能を有すること。
23. Syslog サーバにメッセージを送信する機能を有すること。
24. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
25. SNMPv1/v2c/v3 による管理機能を有すること。
26. トラフィック解析のためのポートをミラーリングする機能を有すること。ミラー

先は同一筐体内や他の筐体へ VLAN を使いミラーリングをできる機能を有すること。

- 27. 19 インチラックに格納できること。
- 28. 1U 以内のラックマウント型の形状であること。
- 29. 構成に必要なライセンスを契約期間中有していること。

3.7. PoE 対応レイヤ 2 スイッチ

【想定機種：シスコシステムズ社製 C9200L-24P-4X-E】 【数量：36 台】

1. スイッチング容量 128Gbps 以上を有すること。
2. スタック構成で 288Gbps 以上のスタック間のスループットを有すること。
3. 転送レートが 95.23Mpps 以上を有すること。
4. 専用のスタックポートを有し、スタックされたすべての筐体は 1 台の論理ユニットとして設定・管理できること。
5. スタック上のステートフルフェールオーバー（SSO）をサポートしていること。
6. 10/100/1000 イーサネットポートを 24 ポート以上実装していること。
7. 10 ギガビットイーサネット SFP+を 4 ポート以上実装していること。
8. 10/100/1000 イーサネットポートを 12 ポート以上で最大 30w までサポートできる PoE+（IEEE802.3at）ポートを実装していること。
9. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
10. IEEE802.1D に準拠したスパニングツリー機能を有すること。
11. IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
12. IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
13. IEEE802.1x に準拠した認証機能を有すること。
14. IEEE802.1x 認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
15. IEEE802.3ad Link Aggregation 機能を有すること。
16. マルチシャシ・イーサチャネル（シャシを跨って、複数の Ethernet ポートを束ねて 1 つの高速なポートとして利用可能な機能）をサポートすること。
17. IEEE802.1p も優先制御機能（QoS）を有すること。
18. ユニキャストルーティングとして、Static、RIPv1/v2、OSPF Routed Access に対応していること。
19. モジュラー型 QoS 機能を有すること。
20. 4,000 個以上の VLAN をサポートしていること。
21. 9,000 バイト以上のジャンボフレームに対応していること。
22. ポートにてリンクフラップ等の機能を検知した際、ポートを自動的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
23. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム抑制機能を有すること。

- 24. GUI を使用して設定変更が行える機能を有すること。
- 25. シリアル接続によるコンソールポートを有すること。
- 26. Telnet/SSH によるリモートコンソール機能を有すること。
- 27. NTP クライアント機能を有すること。
- 28. Syslog サーバにメッセージを送信する機能を有すること。
- 29. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
- 30. SNMPv1/v2c/v3 による管理機能を有すること。
- 31. トラフィック解析のためのポートをミラーリングする機能を有すること。ミラー先は同一筐体内や他の筐体へ VLAN を使いミラーリングをできる機能を有すること。
- 32. 19 インチラックに格納できること。
- 33. 1U 以内のラックマウント型の形状であること。
- 34. 構成に必要なライセンスを契約期間中有していること。

3.8. PoE 対応アクセスレイヤ 2 スイッチ

【想定機種：シスコシステムズ社製 C1000-16FP-2G-L】 【数量：28 台】

1. スイッチ帯域幅が 36Gbps 以上を有すること。
2. 転送レートが 26.78Mpps 以上を有すること。
3. ギガイーサネット PoE+ポートを 16 ポート以上実装していること。
4. アップリンクとして SFP ポートを 2 ポート以上実装していること。
5. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
6. IEEE802.1D に準拠したスパニングツリー機能を有すること。
7. IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
8. IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
9. IEEE802.1x に準拠した認証機能を有すること。
10. IEEE802.1x 認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
11. IEEE802.3ad Link Aggregation 機能を有すること。
12. IEEE802.1p の優先制御機能（QoS）を有すること。
13. 1 ポートあたり最大 8 つの出力キューに対応可能なこと。
14. Shaped Round Robin スケジューリング機能を有すること。
15. Priority Queuing 機能を有すること。
16. Weighted Tail Drop アルゴリズムによる輻輳回避機能を有すること。
17. 256 個以上の VLAN をサポートしていること。尚、VLAN ID は 4,000 以上を利用可能であること。
18. 9,000 バイト以上のジャンボフレームに対応していること。
19. ポートにてリンクフラップ等の機能を検知した際、ポートを自動的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
20. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム抑制機能を有すること。
21. GUI を使用して設定変更が行える機能を有すること。
22. シリアル接続によるコンソールポートを有すること。
23. Telnet/SSH によるリモートコンソール機能を有すること。
24. NTP クライアント機能を有すること。
25. Syslog サーバにメッセージを送信する機能を有すること。
26. 隣接するデバイス間でトポロジ管理を行う機能を有すること。

- 27. SNMPv1/v2c/v3 による管理機能を有すること。
- 28. ソフトウェア及び設定情報を TFTP にてアップロード及びダウンロードする機能を有すること。
- 29. 送信元デバイスから宛先デバイスまでのパケットロスの L2 パスを確認する機能を有すること。
- 30. 機器がリブート時でも、PoE 給電を止めない機能を有すること。
- 31. トラフィック解析のためのポートをミラーリングする機能を有すること。
- 32. ファンレスであること。
- 33. 19 インチラックに取り付け可能なこと。(必要なマウント金具は含めること)
- 34. 総 PoE 電力容量は 240W 以上であること。

3.9. アクセスレイヤ 2 スイッチ

【想定機種：シスコシステムズ社製 C1000-8T-2G-L】 【数量：124 台】

1. スイッチ帯域幅が 20Gbps 以上を有すること。
2. 転送レートが 14.88Mpps 以上を有すること。
3. ギガイーサネットポートを 8 ポート以上実装していること。
4. アップリンクとして SFP/RJ45 を各 2 ポート以上実装していること。
5. IEEE802.1Q に準拠した VLAN Tagging 機能を有すること。
6. IEEE802.1D に準拠したスパニングツリー機能を有すること。
7. IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
8. IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
9. IEEE802.1x に準拠した認証機能を有すること。
10. IEEE802.1x 認証時に、認証サーバに登録された VLAN を動的に割り振る機能を有すること。
11. IEEE802.1x、Web 認証、MAC 認証ユーザに対してユーザ単位で異なるアクセスリストを動的に割り当てる機能を有すること。
12. IEEE802.3ad Link Aggregation 機能を有すること。
13. IEEE802.1p も優先制御機能（QoS）を有すること。
14. 1 ポートあたり最大 8 つの出力キューに対応可能なこと。
15. Shaped Round Robin スケジューリング機能を有すること。
16. Priority Queuing 機能を有すること。
17. Weighted Tail Drop アルゴリズムによる輻輳回避機能を有すること。
18. 256 個以上の VLAN をサポートしていること。尚、VLAN ID は 4,000 以上を利用可能であること。
19. 9,000 バイト以上のジャンボフレームに対応していること。
20. ポートにてリンクフラップ等の機能を検知した際、ポートを自動的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。
21. ポート単位にブロードキャスト、マルチキャスト、ユニキャストのストーム抑制機能を有すること。
22. GUI を使用して設定変更が行える機能を有すること。
23. シリアル接続によるコンソールポートを有すること。
24. Telnet/SSH によるリモートコンソール機能を有すること。
25. NTP クライアント機能を有すること。
26. Syslog サーバにメッセージを送信する機能を有すること。

- 27. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
- 28. SNMPv1/v2c/v3 による管理機能を有すること。
- 29. ソフトウェア及び設定情報を TFTP にてアップロード及びダウンロードする機能を有すること。
- 30. 送信元デバイスから宛先デバイスまでのパケットロスの L2 パスを確認する機能を有すること。
- 31. トラフィック解析のためのポートをミラーリングする機能を有すること。
- 32. ファンレスであること。

3.10. 外局収容ルータ

【想定機種：シスコシステムズ社製 C8300-1N1S-6T】 【数量：2 台】

1. ギガネットイーサネットを 4 ポート以上実装していること。
2. 最大スループットが 19.7Gbps 以上であること。
3. IPv4 および IPv6 のルーティングが可能なルータ製品であること。
4. ルーティング機能として、RIPv1/v2、OSPF、EIGRP、BGP4 に対応していること。
5. マルチキャストとして、Multicast Internet Group Management Protocol (IGMPv3)、Protocol Independent Multicast sparse モード (PIM SM)、PIM Source Specific Multicast (SSM)、Distance Vector Multicast Routing Protocol (DVMRP)、IPv4-to-IPv6 マルチキャストをサポートすること。
6. カプセル化機能として Generic Routing Encapsulation (GRE)、イーサネット、802.1q VLAN、Point-to-Point Protocol (PPP)、Multilink Point-to-Point Protocol (MLPPP)、PPP over Ethernet (PPPoE) をサポートしていること。
7. 機器上に設定されたインスタンス毎にルーティングテーブルを保持する機能 (VRF) を有していること。
8. ポリシーベースルーティング機能を有していること。
9. ゲートウェイ冗長化プロトコルをサポートしていること。
10. IPSec 暗号化はハードウェアで処理されること。
11. IPSec トンネル数が 4,000 以上であること。
12. IPSec スループットが最大 1.9Gbps 以上であること。
13. システムあたりの ACL 数が 4,000 以上であること。
14. Layer2 Tunneling Protocol Version3 (L2TP) に対応していること。
15. DES、3DES、AES-128、AES-256 の暗号化プロトコルをサポートしていること。
16. 階層型 QoS に対応していること。
17. イベントをモニタし、モニタ対象イベントが発生したり、しきい値に達したりすると情報提供などの処理が単体で実施可能な機能を有すること。
18. シリアル接続によるコンソールポートを有すること。
19. Telnet/SSH によるリモートコンソール機能を有すること。
20. NTP クライアント機能を有すること。
21. Syslog サーバにメッセージを送信する機能を有すること。
22. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
23. SNMPv1/v2c/v3 による管理機能を有すること。

- 24. Telnet/SSH によるリモートコンソール機能を有すること。
- 25. ソフトウェア及び設定情報を TFTP や FTP にてアップロード及びダウンロードが可能であること。
- 26. モジュールの追加でポートの増設が可能になること。
- 27. 16GB 以上の M.2 SSD のストレージ容量を有していること。
- 28. 冗長化された電源モジュールを有すること。
- 29. 19 インチラックに実装可能で、1U 以下であること。
- 30. 構成に必要なライセンスを契約期間中有していること。

3.11. 外局接続用ルータ

【想定機種：シスコシステムズ社製 C1111-8P】 【数量：130 台】

1. 本体上に本体上に WAN 用ギガビットイーサネット(RJ-45)1 ポートと、LAN スイッチ用ギガビットイーサネット 8 ポートを有すること。
2. PoE+（30W）給電が可能なポートを 2 ポート以上有している事。
3. AC 入力電圧は 100 ～ 240 VAC（オートレンジ）に対応していること
4. IPv4,IPv6 プロトコルに対応していること。
5. ルーティング機能として RIP および RIPv2、OSPF、BGP、BGP ルータ リフレクタ、IS-IS に対応していること。
6. マルチキャストとして、Multicast Internet Group Management Protocol (IGMPv3)、Protocol Independent Multicast sparse モード（PIM SM）、PIM Source Specific Multicast（SSM）、Distance Vector Multicast Routing Protocol（DVMRP）、IPv4/IPv6 マルチキャストをサポートすること
7. Generic Routing Encapsulation（GRE）トンネル、802.1q VLAN 及び VRF Lite をサポートすること。
8. セキュリティ機能として、IPSec、L2TPv3 をサポートすること。
9. IPSec パフォーマンスが 200Mbps までサポートしていること。
10. QoS 機能として Class-Based Weighted Fair Queuing（CBWFQ）、重み付けランダム早期検出（WRED）、階層型 QoS をサポートすること
11. ポリシーベース ルーティング（PBR）をサポートしていること。
12. 暗号化アルゴリズムとして以下の仕様に対応していること
 暗号化：DES、3DES、AES-128 または AES-256（CBC および GCM モード）
 認証：RSA（748/1024/2048 ビット）、ECDSA（256/384 ビット）、整合性：MD5、SHA、SHA-256、SHA-384、SHA-512"
13. イベントをモニタし、モニタ対象イベントが発生したり、しきい値に達したりすると、情報提供などの処理が単体で実効できること。
14. シリアル接続によるコンソールポートを有すること。
15. Telnet/SSH によるリモートコンソールポートを有していること。
16. NTP クライアント機能を有すること。
17. Syslog サーバにメッセージを送信する機能を有すること。
18. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
19. SNMPv1/v2/v2c による管理機能を有すること。

20. ソフトウェア及び設定情報を TFTP/FTP にてアップロード及びダウンロードが可能であること。
21. 構成に必要なライセンスを契約期間中有していること。

3.12. 基幹ファイアウォール

【想定機種：Fortinet 社製 FG-1100E-FC】 【数量：2 台】

1. 40 GbE SFP+ インタフェースを 2 ポート以上実装していること。
2. 25 GbE SFP28 / 10 GbE SFP+ / GbE SFP インタフェースを 4 ポート以上実装していること。
3. 10 GbE SFP+ インタフェース / GbE SFP インタフェースを 4 ポート以上実装していること。
4. GbE SFP インタフェースを 8 ポート以上実装していること。
5. GbE RJ45 インタフェースを 16 ポート以上実装していること。
6. GbE RJ45 管理 / HA インタフェースを 2 ポート以上実装していること。
7. USB インタフェースを 2 ポート以上実装していること。
8. シリアル管理コンソールインタフェースを実装していること。
9. IPv4 ファイアウォールスループットは (1518 / 512 / 64 バイト UDP パケット) それぞれで 80 / 80 / 45 Gbps 以上であること。
10. IPv6 ファイアウォールスループットは (1518 / 512 / 86 バイト UDP パケット) それぞれで 80 / 80 / 45 Gbps 以上であること。
11. ファイアウォールスループットは 67.5Mpps 以上であること。
12. ファイアウォール同時セッション(TCP)は 8,000,000 以上であること。
13. ファイアウォール新規セッション / 秒 (TCP) は 500,000 以上であること。
14. ファイアウォールポリシーは 100,000 以上であること。
15. クライアント - ゲートウェイ間 IPSec VPN トンネルは 100,000 以上であること。
16. SSL インспекションスループット (IPS、avg. HTTPS) は 10Gbps 以上であること。
17. SSL インспекション CPS(IPS、avg. HTTPS) は 6,500 以上であること。
18. SSL インспекション同時セッション(IPS、avg. HTTPS)780,000 以上であること。
19. アプリケーション制御スループットは 26Gbps 以上であること。
20. 仮想 UTM は最大 250 以上であること。
21. AC 電源は 100 ～ 240 V AC、50 ～ 60 Hz に対応すること。
22. 冗長電源(ホットスワップ)に対応すること。

3.13. ファイアウォール A

【想定機種：Fortinet 社製 FG-100F-US】 【数量：4 台】

1. GbE RJ45 インタフェースを 12 ポート以上実装していること。
2. GbE RJ45 管理 / HA / DMZ インタフェースを 1 / 2 / 1 ポート以上実装していること。
3. GbE SFP インタフェースを 4 ポート以上実装していること。
4. 10 GbE SFP+ FortiLink インタフェースを 2 ポート以上実装していること。
5. GbE RJ45 WAN インタフェースを 2 ポート以上実装していること。
6. GbE RJ45 または SFP 共有インタフェースを 4 ポート以上実装していること。
7. USB インタフェースを実装していること。
8. シリアル管理コンソールインタフェースを実装していること。
9. IPv4 ファイアウォールスループットは (1518 / 512 / 64 バイト UDP パケット) それぞれで 20 / 18 / 10 Gbps 以上であること。
10. ファイアウォールレイテンシは 4.97 μ s 以下であること。
11. ファイアウォールスループットは 15 Mpps 以上であること。
12. ファイアウォール同時セッション(TCP)は 1,500,000 以上であること。
13. ファイアウォール新規セッション / 秒 (TCP) は 56,000 以上であること。
14. ファイアウォールポリシーは 10,000 以上であること。
15. SSL インスペクションスループット (IPS、avg. HTTPS) は 1Gbps 以上であること。
16. SSL インスペクション CPS(IPS、avg. HTTPS) は 1,800 以上であること。
17. SSL インスペクション同時セッション(IPS、avg. HTTPS)135,000 以上であること。
18. アプリケーション制御スループットは 2.2Gbps 以上であること。
19. 仮想 UTM は最大 10 以上であること。
20. AC 電源は 100 ~ 240 V AC、50 ~ 60 Hz に対応すること。
21. 冗長電源に対応すること。

3.14. ファイアウォール B

【想定機種：Paloart 社製 PAN-PA-460】 【数量：4 台】

1. 10/100/1000BASE-T のインターフェイスを 8 ポート以上搭載すること。
2. Firewall スループットは 4.4Gbps 以上であること。
3. Threat Prevention スループットは 2.4Gbps 以上であること。
4. 新規セッション数/秒は 73,000 以上であること。
5. 最大セッション数は 400,000 以上であること。
6. アプリケーション登録数は 3,602 個以上であること。
7. IPsec VPN の VPN スループットとして 3.0Gbps 以上であること。
8. Tap モード, Virtual wire (Layer1), Layer2 and Layer3 に対応していること。
9. 802. 1Q VLAN tagging (Virtual wire, Layer2, Layer3) に対応していること。
10. DHCP / DHCP Relay / DHCP Client に対応していること。
11. OSPF / RIPv2 / BGP に対応していること。
12. NAT に対応していること。
13. 冗長化(HA)機能として Active / Standby, Active / Active に対応していること。
14. CLI / WebUI 管理に対応していること。
15. Syslog / SNMPv2 / SNMPv3 に対応していること。
16. 管理インターフェイスとして MGT ポート(×1), RJ-45 コンソールポート(×1), microUSB コンソールポート(×1), USB ポート(×2)に対応すること。
17. 冗長電源に対応すること。
18. ラックマウント時は 1 U 以内で搭載可能なこと。

3.15. ファイアウォール C

【想定機種：Fortinet 社製 FG-60F-US】 【数量：1 台】

1. GbE RJ45 WAN インタフェースを 2 ポート以上実装していること。
2. GbE RJ45 DMZ インタフェースを実装していること。
3. GbE RJ45 LAN インタフェースを 5 ポート以上実装していること。
4. USB インタフェースを実装していること。
5. シリアル管理コンソールインタフェースを実装していること。
6. NGFW スループットは 1Gbps 以上であること。
7. ファイアウォールスループットは (1518 / 512 / 64 バイト UDP パケット) それぞれで 10 / 10 / 6 Gbps 以上であること。
8. ファイアウォールレイテンシは 3.3μ s 以下であること。
9. ファイアウォールスループットは 9 M pps 以上であること。
10. ファイアウォール同時セッション(TCP)は 700,000 以上であること。
11. ファイアウォール新規セッション / 秒 (TCP) は 35,000 以上であること。
12. ファイアウォールポリシーは 5,000 以上であること。
13. SSL-VPN スループットは 900Mbps 以上であること。
14. 同時 SSL-VPN ユーザの推奨最大値、トンネルモードは 200 以上であること。
15. SSL インスペクションスループット (IPS、avg. HTTPS) は 630Mbps 以上であること。
16. SSL インスペクション CPS(IPS、avg. HTTPS) は 400 以上であること。
17. SSL インスペクション同時セッション(IPS、avg. HTTPS)55,000 以上であること。
18. アプリケーション制御スループットは 1.8Gbps 以上であること。
19. 仮想 UTM は最大 10 以上であること。
20. AC 電源は 100 ～ 240 V AC、50 ～ 60 Hz に対応すること。

3.16. 無線 LAN コントローラ

【想定機種：シスコシステムズ社製 C9800-40-K9】 【数量：2 台】

1. IEEE802.11a、802.11b、802.11g、802.11d、WMM/802.11e、802.11h、802.11n、802.11ac をサポートすること。
2. IEEE 802.1Q をサポートすること。
3. 無線コントローラとアクセスポイントの通信が RFC で公開された CAPWAP (RFC5415)プロトコルをサポートしていること。
4. コントローラとアクセスポイント間の通信は暗号化が可能であること。
5. 隣接するデバイス間でトポロジ管理を行う機能を有すること。
6. 802.11r / 802.11k をサポートしていること。
7. mDNS 機能をサポートすること。
8. SNMP v1, v2c, v3 及び Syslog に対応していること。
9. クライアント側で意識せず、IP サブネットを跨るローミングができること。
10. 冗長構成として、環境に応じて 1 対 1 の Active-Standby 構成または、N 対 1 の Primary-Secondary 構成が出来る機能を有すること。
11. N+1 構成時にアクセスポイントをグループ化し、グループ単位でソフトウェアアップグレードすることにより、コントローラとアクセスポイントの一部が常に起動している状態で無線システムのソフトウェアアップグレードできること。
12. アクセスポイントをグループ化し、グループ単位でソフトウェアアップグレードができること。
13. コントローラを再起動せず、ソフトウェアのパッチを適用できること（再起動の必要性はパッチの種類に依存する）。
14. RF の管理機能として、ダイナミックなチャネル割り当て、カバレッジ ホールの検出と修正、出力制御ができること。
15. AP の電波状況を常に監視し、管理者に以下の情報を提供できること。
 - ・ 通信に伴う負荷の大きさ
 - ・ 電波干渉の影響度合い
 - ・ 電波雑音の大きさ
 - ・ 接続している無線 LAN クライアントの受信信号強度、信号対雑音比
 - ・ 電波到達範囲（セル）が隣接する AP の数
 - ・ 常時変動しうる電波環境に対応するため、電波管理機能は定期的に動作すること。
16. 電波干渉の発生や AP の故障などの電波状況の変化に対応して送信出力を自動的に調整する機能を有すること。

17. 初期設定を軽減できるよう、無線 LAN 電波到達範囲（セル）が隣接する AP の電波の受信信号強度、電波雑音の状況、電波干渉の状況、無線 LAN 通信量に基づきチャンネルを自動的に選択し最適化する機能を有すること。
18. Ad-hoc Network の検知、Reporting が可能なこと。
19. 管理外 AP の検知、Reporting が可能なこと。
20. 管理外 AP を SSID、RSSI、暗号化有無等のパラメータを利用してリスクに応じたルールによって分類できること。
21. 無線 LAN クライアント間の通信をブロックすることが可能であること。
22. セキュリティ機能として、WPA および IEEE 802.11i（WPA2、RSN）に対応していること。
23. 以下の暗号化をサポートすること
 - AES: CBC, CCM, CCMP
 - DES: DES-CBC, 3DES
 - SSL/TLS: RC4 128-bit, RSA 1024-bit, 2048-bit
 - DTLS: AES-CBC
 - IPsec: DES-CBC, 3DES, AES-CBC
 - 802.1AE MACsec encryption
24. IEEE802.1X 無線 LAN 認証が可能なこと。
25. Web ベース認証が可能なこと。
26. MAC 認証可能なこと。
27. 複数の RADIUS サーバと連携可能なこと。
28. 予めアップグレードするイメージをアクセスポイント側に保存することで停止時間を最小にすることができること。
29. 管理用インターフェイスとして、①Web ベース：HTTP/HTTPS ②コマンドライン インターフェイス：Telnet、Secure Shell（SSH）プロトコル、シリアルポートが利用可能であること。
30. QoS 機能を有すること。
31. アプリケーションを可視化する機能を有すること。また、それぞれのアプリケーションに対して、通信をブロックしたり、帯域を制限する機能を有すること。
32. Flexible NetFlow に対応していること。
33. 10Gbps イーサネット インタフェース SFP+を 4 つ以上有すること。
34. 最大 500 台のアクセスポイントを管理できること。
35. 最大 10,000 台の無線デバイスを管理できること。
36. スループットとして最大 40Gbps を利用できること。
37. 最大 4,096 個の VLAN ID に対応出来ること。
38. 4,096 個以上の VLAN を設定できること。

- 39. 電源は冗長構成であること。
- 40. 冗長ファン構成が出来ること。
- 41. 1RU であること。

3.17. 無線 LAN アクセスポイント A

【想定機種：シスコシステムズ社製 CW9166I-Q】 【数量：137 台】

1. IEEE 802.11 a/b/g/n/ac/ax に対応していること
2. IEEE802.11ax Wi-Fi6E 規格に対応していること
3. アップリンクとして、IEEE 802.3bz の 100/1000/2500/5000 マルチギガビットイーサネット (RJ45) に対応したポートを 1 つ有すること
4. 無線 LAN のアンテナは内蔵であること
5. WPA3-Personal, WPA3-Enterprise, WPA3-Enhanced Open (OWE)に対応していること
6. 2.4GHz/5GHz /6GHz 帯をサポートしており、それぞれ同時に利用できること (トライバンド)
7. スキャン専用 Radio を有しており、データ通信に影響なく全チャネルに対して、非 Wi-Fi の干渉源を検知・特定が可能であること
8. スキャン専用アンテナを有しており、データ通信に影響なくレーダーの検知が可能なこと
9. ビームフォーミングに対応していること
10. IEEE802.3at での 25.0W 給電の際、802.11ac/ax で 5GHz/6GHz 帯それぞれで 4(送信)x4(受信)のアンテナをサポートしていること
11. 環境センサを実装し、AP で温度、湿度、空気の品質をモニタリングできること
12. レーダー干渉時帯域幅を縮退し回避する機能を有すること
13. BLE 5.1 用のラジオを搭載していること
14. 不正アクセスポイント・クライアントを検知し、悪意ある機器 (同一の SSSID を利用など) を自動識別できること
15. 壁面や天井に設置された状態でも LED が確認でき、LED の色で稼働状態 (ブートローダーステータス、アソシエーションステータス、オペレーティングステータス、ブートローダーワーニング、ブートローダーエラー) が判別できること。
16. パワーインジェクターや PoE+など柔軟な電源環境に対応できる製品があること。
17. 以下の EAP に対応した認証が可能なこと。
 - ・ Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
 - ・ EAP-Tunneled TLS (TTLS) または Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)

- ・ Protected EAP (PEAP) v0 または EAP-MSCHAPv2
 - ・ Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
 - ・ PEAPv1 または EAP-Generic Token Card (GTC)
 - ・ EAP-Subscriber Identity Module (SIM)
18. コントローラと連携して動作可能なこと
 19. USB インターフェースを具備していること。
 20. WPA2 (Enterprise,Personal), WPA3(Enterprise,Personal), Wi-Fi 6,Wi-Fi 6 Release2 features, Wi-Fi 6E 認定が取得できていること
 21. Uplink MU-MIMO, DownLink MU-MIMO 双方に対応していること
 22. Uplink OFDMA, Downlink OFDMA 双方に対応していること
 23. チャンネル幅を 6GHz 帯において 20/40/80/160MHz の組み合わせから最適なものを自動選択できること
 24. チャンネル幅を 5GHz 帯において 20/40/80MHz の組み合わせから最適なものを自動選択できること
 25. 1 台の無線 LAN アクセスポイントで 5GHz 帯× 2 チャンネルまたは 5GHz +6 GHz チャンネルを選択可能なこと
 26. アプリケーションホスティングができること
 27. アクセスポイントが消費する電力を利用状況に応じて最適化できること（省電力）

3.18. 無線 LAN アクセスポイント B

【想定機種：シスコシステムズ社製 CW9162I-Q】 【数量：235 台】

1. IEEE 802.11 a/b/g/n/ac/ax に対応していること。
2. IEEE802.11ax Wi-Fi6E 規格に対応していること
3. アップリンクとして、IEEE 802.3bz の 100/1000/2500 マルチギガビットイーサネット (RJ45) に対応したポートを 1 つ有すること
4. DRAM 2,048MB、Flash 1,024MB を搭載すること
5. 無線 LAN のアンテナは内蔵であること
6. WPA3-Personal, WPA3-Enterprise, WPA3-Enhanced Open (OWE)に対応していること
7. 2.4GHz/5GHz /6GHz 帯をサポートしており、それぞれ同時に利用できること (トライバンド)
8. スキャン専用 Radio を有しており、データ通信に影響なく全チャネルに対して、非 Wi-Fi の干渉源を検知・特定が可能であること
9. スキャン専用 Radio を有しており、データ通信に影響なくレーダーの検知が可能なこと
10. ビームフォーミングに対応していること
11. レーダー干渉時帯域幅を縮退し回避する機能を有すること
12. BLE 5.1 用のラジオを搭載していること
13. 不正アクセスポイント・クライアントを検知し、悪意ある機器 (同一の SSSID を利用など) を自動識別できること
14. 壁面や天井に設置された状態でも LED が確認でき、LED の色で稼働状態 (ブートローダーステータス、アソシエーションステータス、オペレーティングステータス、ブートローダーワーニング、ブートローダーエラー) が判別できること。
15. パワーインジェクターや PoE+など柔軟な電源環境に対応できる製品があること。
16. 以下の EAP に対応した認証が可能なこと。
 - ・ Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
 - ・ EAP-Tunneled TLS (TTLS) または Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)
 - ・ Protected EAP (PEAP) v0 または EAP-MSCHAPv2
 - ・ Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)

- ・ PEAPv1 または EAP-Generic Token Card (GTC)
 - ・ EAP-Subscriber Identity Module (SIM)
17. コントローラと連携して動作可能なこと
 18. USB インターフェースを具備していること。
 19. WPA2 (Enterprise,Personal), WPA3(Enterprise,Personal), Wi-Fi 6,Wi-Fi 6 Release2 features, Wi-Fi 6E 認定が取得できていること
 20. UpLink MU-MIMO, DownLink MU-MIMO 双方に対応し、通信速度の向上が可能であること
 21. Uplink OFDMA, Downlink OFDMA 双方に対応し、通信速度の向上が可能であること
 22. チャンネル幅を 6GHz 帯において 20/40/80/160MHz の組み合わせから最適なものを自動選択できること
 23. チャンネル幅を 5GHz 帯において 20/40/80MHz の組み合わせから最適なものを自動選択できること
 24. アプリケーションホスティングができること
 25. アクセスポイントが消費する電力を利用状況に応じて最適化できること（省電力）

3.19. 無線 LAN 管理サーバ

【想定機種：シスコシステムズ社製 DN2-HW-APL】 【数量：1 台】

1. 指定した無線 LAN 端末の物理的な位置情報の履歴をマップ上に表示させることが可能であること。
2. 以下の物について位置情報をマップ上に表示可能であること。
 - ・ 無線 AP
 - ・ 不正 AP(管理外 AP)
 - ・ 干渉源(非無線 LAN 機器)
 - ・ RFID tag
 - ・ 無線 AP に接続しているクライアント
 - ・ 不正クライアント（管理外の AP に接続されているクライアント）
3. 上記項目において、物理位置に加え、稼働状況、実測値に基づく RF カバレッジのヒートマップ、干渉源の影響範囲を可視化できること。
4. JSON/XML のメッセージフォーマットで位置情報を外部システムに通知可能なこと。
5. 位置情報を活用したアプリケーションを容易に開発できるように REST API を利用可能なこと。
6. 記録する位置情報が膨大にならぬよう、位置情報を記録する「対象 MAC アドレス」や「最低限必要とする受信信号強度」のフィルタリングが可能であること。
7. 無線 LAN 端末の Wi-Fi 位置情報より、主な導線や時間ごとの端末滞在時間、端末数など位置情報の分析できる機能を有すること。
8. 1 RU であること。
9. 10Gb Ethernet port が 2 ポート以上あること
10. Management port として専用の 1Gb Ethernet port を有すること
11. USB3.0 ポートを有すること
12. 最大 500 台のアクセスポイントをサポートすること
13. 1 日当たり最大 10,000 台のデバイスをトラッキング可能なこと

3.20. 無線 LAN ロケーション管理サーバ

【想定機種：シスコシステムズ社製 AIR-CMX-3375-K9】 【数量：1 台】

1. 無線 LAN のレイアウト、アクセスポイントの稼働状況、実測値に基づく RF カバレッジのヒートマップ、干渉源、不正デバイスを視覚化できること。
2. 指定した接続デバイスの物理的な位置情報の履歴を MAP 上に表示させることが可能であること。
3. 不正端末、干渉源、WIFI 端末、スマートフォン、RFID タグを検知し、リアルタイムにロケーション追跡でき、過去に遡って軌跡や痕跡を把握出来ること。
4. WIFI 端末の WIFI 位置情報より、主な導線や時間ごとの端末滞在時間、端末数などロケーション分析できる機能を有すること。
5. REST API や SOAP/XML、Syslog を用いて WIFI ロケーション情報を外部にエクスポートできること。
6. クライアント端末のブラウザ上に場所ごと時間ごとにコンテンツをプッシュすることが可能であること。

3.21. ネットワーク認証サーバ

【想定機種：エイチ・シー・ネットワークス株式会社 ACP-AP5000】 【数量：2 台】

1. ソフトウェアとハードウェアが一体になったアプライアンス機であること。
2. 1U 以内に設置可能であること。
3. 管理画面は WEB ブラウザかつ日本語で表示されること。(専用のアプリケーションを必要としない)
4. 日本語のユーザインターフェースを有し、ユーザ単位に設定するユーザ情報に、日本語「2 バイト文字」が使用可能であること。
5. プログラムのバージョンアップは WEB ブラウザ操作で実施可能であること。
6. 1 日 1 回、自動的にバックアップする機能を有すること。
7. 解析に必要な情報を一括して収集できること。
8. マスターからスレーブに対してアカウント情報、RADIUS 情報、証明書情報、DHCP 情報の同期が可能であること。
9. SNMP エージェント機能、Trap 出力機能を有すること。
10. 認証ログの出力が管理画面、syslog、ファイルで可能であること。
11. ライセンス数に関わらず登録可能な Radius クライアント数に制限が無いこと。
12. IEEE802.1X 機能を有すること。(EAP-MD5、EAP-TLS、EAP-PEAP、EAP-TTLS)
13. IEEE802.1X に対応した証明書発行機能を有すること。
14. 外部認証機関が署名した証明書をインポート可能であること。
15. CSR を発行して他の認証局で発行した CA 証明書をインポートし、下位認証局(中間認証局)として動作すること。
16. クライアント証明書の一括発行、失効、ダウンロードが可能であること。
17. クライアント証明書の発行および失効時に発行/失効ログを出力すること。
18. 失効リストをダウンロードできること。
19. 1 アカウントあたり 2 枚の証明書を発行できること。
20. Radius クライアントをグルーピングできること。
21. アカウント情報を追加、修正、削除できる機能を有すること。
22. アカウント情報をタブ区切りテキストファイル形式でインポート、エクスポートできる機能を有すること。
23. アカウント作成、一覧、検索画面では、使用する管理項目、属性のみを画面に表示できること。
24. アカウント作成画面では、管理項目毎に必須入力/任意入力の指定が可能で、必須入力項目に未入力で登録しようとした場合にはエラーで登録不可となること。

25. 管理項目名、属性名は、任意にカスタマイズ表示できること。
26. 管理者がユーザのパスワードポリシーを設定できること。
27. ディレクトリ単位で管理者を設定できること。ディレクトリ管理者は、自身のディレクトリのみ管理者権限を持つこと。
28. ディレクトリに共通アトリビュートを設定し、そのディレクトリに属するアカウントに対して、共通アトリビュートを設定可能であること。
29. 最終認証日を検索条件としたアカウント検索が可能であること。
30. 最終認証日から指定した期間に認証要求が発生していないアカウントに対してネットワーク利用の停止や削除を自動で行うことが可能であること。また、有効期限が切れたアカウントに対して自動削除することも可能であること。
31. VID など Radius アトリビュート設定をグルーピングしたネットワーク属性を定義できること。
 - (ア)定義したネットワーク属性をユーザ・端末アカウントに紐づけることができること。
 - (イ)定義したネットワーク属性を Radius クライアント（グループ）に紐づけることができること。
 - (ウ)（ア）、（イ）を組み合わせ、特定の Radius クライアント（グループ）から接続したときに、特定のネットワーク属性（に設定した Radius アトリビュート）を払い出すことができること。
32. 5,000 以上のライセンスを有すること。

3.22. NAS サーバ

【想定機種：NEC 社製 iStorage NS300Rj（8TB）】 【数量：2 台】

1. 1RU 以内でラックマウント可能な筐体であること。
2. 物理容量として 8TB 以上、論理容量として 5.5TB 以上を満たすハードディスクが搭載されていること。
3. RAID5 によりディスクの冗長構成が可能なこと。
4. システム動作中にハードディスクの交換（ホットスワップ）が可能なこと。
5. 内蔵 DVD-ROM ドライブが搭載されていること。
6. ファンが冗長されていること。

3.23. SFP

本システムを構成する上で必要となる SFP については、下記を調達すること。

【想定機種：シスコシステムズ社 各種 SFP】

【想定機種：Fortinet 社 各種 SFP】

項 目	機 能	数 量
SFP	シスコシステムズ社製 ・ 40G QSFP-AOC 1M ケーブル	5
	シスコシステムズ社製 ・ 25G SFP25-AOC 3M ケーブル	11
	シスコシステムズ社製 ・ 25G SFP-25G-SR SFP モジュール	5
	シスコシステムズ社製 ・ 10G SFP+AOC 1M ケーブル	3
	シスコシステムズ社製 ・ 10GBase-SR SFP+モジュール	136
	シスコシステムズ社製 ・ 1000Base-SX SFP モジュール	28
	シスコシステムズ社製 ・ 1000Base-LX/LH SFP モジュール	19
	シスコシステムズ社製 ・ 1000Base-T SFP モジュール	19
	Fortinet 社製 ・ 10GBase-SR SFP+モジュール	8

3.24. 仮想基盤用ラックマウントサーバ

【想定機種：シスコシステムズ社製 UCSC-C220-M6S】 【数量：4 台】

1. 1RU 以内でラックマウント可能な筐体であること。
2. サーバの CPU は、動作周波数 2.0GHz、コア数 32 以上（参考：Intel 社製 Xeon Gold6338 プロセッサ）を 2 つ以上搭載すること。
3. サーバのメモリは、1 台あたり 512GB 以上の容量を有すること。
4. サーバのハードディスクは、15,000 回転以上の 2.5inchi SAS 300GB HDD を 3 本以上内蔵した RAID 構成で構成すること。（ホットスペアディスク 1 本含む）
5. PCIe Gen4.0 に対応した PCIe スロットを 2 スロット以上有すること。
6. シャーシ全面の LED でシステム、ファン、温度、ネットワーク、電源のステータスを確認できること。
7. 1G/10GBase-T (RJ45) を 2 ポート以上有すること。
8. 25GBase-SR (SFP28) ポートを 4 ポート以上有すること。
9. 16G Fiber Channel ポートを 2 ポート以上有すること。
10. 1GBase-T (RJ45) の管理専用ポートを有すること。
11. RS-232C (RJ45) のシリアルポートを 1 ポート有すること。
12. VGA ポート (DB15) を 1 ポート有すること。
13. USB3.0 2 ポート有すること。
14. ホットスワップ可能な 1,050W 以上の AC 電源モジュールを 2 個以上搭載し、冗長構成とすること。
15. AC 電源モジュールは高変換効率の 80 Plus Platinum 認定を取得していること。
16. 12G SAS RAID Controller は最大 10 個の SAS/SATA ディスクをサポートすること。また、4GB のフラッシュバック・ライトキャッシュ(FBWC)を装備し、RAID 0,1,5,6,10,50,60,SRAID, JBOD に対応すること。
17. RAID コントローラは専用スロットに装着され、PCI スロットを専有する必要のないこと
18. 10/25Gb で FCoE 対応のインタフェースを 4 個有するネットワークインタフェースカードを PCI スロットを使わない専用スロット(mLOM)にて搭載すること。ネットワークカードは 900,000 以上の IOPS 性能を持つこと。
19. ネットワークカード一枚に付きデフォルトで 4 個の vHBA (仮想ホストバスアダプタインタフェース)と 4 個の vNIC (仮想ネットワークインタフェース) が用意されており、最大 10 個の vNIC または vHBA を追加作成できること。SR-IOV を用いず、サーバ管理ソフトウェアから設定可能なこと。
20. 追加した vNIC ごとにレート制限(Rate Limit), VLAN, MAC アドレス, 優先制御

(CoS), VXLAN/GENEVE オフロードが設定可能なこと

21. 追加した vHBA ごとにレート制限(Rate Limit), WWNN, WWPN, MAC アドレス, 優先制御(CoS)が設定可能なこと
22. ネットワークカードは、usNIC 技術により 2 マイクロ秒の以下の遅延を実現可能なこと。
23. TPM2.0 (Trusted Platform Module)を装備すること
24. 設定情報を GUI ベースの管理画面からバックアップ・リストアが実行可能なこと。バックアップはネットワーク設定・電力ポリシー・BIOS パラメータ・SNMP などを取得できること。
25. サーバ管理ツールは Web ブラウザを用いてリモートからグラフィカル(GUI)インタフェースを使用可能なこと。
26. リモートから KVM コンソール（キーボード・ビデオ・マウス）を使いサーバ接続が可能なこと
27. 仮想メディア機能を有し、リモートからパソコンもしくはネットワーク上にある CD/DVD ドライブや ISO イメージにアクセスして OS のインストール等が可能なこと。
28. サーバ管理ツールはメインサーバ CPU から独立している専用のプロセッサを使用することでサーバ本体や OS の障害の影響を受けることなく管理が可能なこと。
29. IPMI に準拠した専用の管理ポートを有し、OS やハイパーバイザーが停止している状態でも当該ポートを介して IPMI を利用したネットワーク経由での操作が可能なこと。また、XML API を使用した管理も可能とすること
30. システムの起動時にハードウェアの不正な変更を検証する TPM(Trusted Platform Module)およびメーカでの製造時に付与する固有のセキュアデバイス識別子を搭載するチップを標準装備し、ハードウェアの不正改ざんを確認できること。
31. 入力電圧 100~240 VAC、50-60 Hz にて動作すること。
32. サーバ管理ツールにて以下の管理が可能なこと。
 - (ア)接続されている全てのサーバが一元的な画面で統合管理できること。
 - (イ)インベントリ情報（サーバ名・モデル・シリアル番号・CPU・メモリ・HDD・NIC）の確認が可能なこと。
 - (ウ)アラートやエラー情報などシステムの健全性を監視
 - (エ)システムエラー発生時、障害対応連絡がツール上から可能なこと。

3.25. バックアップサーバ

【想定機種：シスコシステムズ社製 UCSC-C240-M6L】 【数量：1 台】

1. 2RU 以内でラックマウント可能な筐体であること。
2. サーバの CPU は、動作周波数 2.9GHz、コア数 16 以上（参考：Intel 社製 Xeon Gold6326 プロセッサ）を 1 つ以上搭載すること。
3. サーバのメモリは、32GB 以上の容量を有すること。
4. ハードディスクはシステム領域として、SAS 接続 7,200 回転以上でハードウェアであること。
5. ハードディスクはバックアップデータ領域として、SAS 接続 7,200 回転以上のハードウェアであること。
6. システム領域はハードディスク 3 本で構成され、RAID 未構成時のディスク 1 台の容量は 2TB 有すること。（参考：7200 回転 2TB SAS HDD）ハードディスク装置故障時にシステム停止することなく交換（ホットスワップ）が可能であること。ハードディスク 3 台の内にホットスペア用ハードディスク 1 台を含める事。
7. バックアップデータ領域はハードディスク 7 本で構成され、RAID 未構成時のディスク 1 本の容量は 6TB 有すること。ハードディスク故障時にはシステム停止することなく交換（ホットスワップ）が可能であること。ハードディスク 7 本の内にホットスワップ用のハードディスクを 1 台含める事。
8. PCIe Gen4.0 に対応した PCIe スロットを 8 スロット以上有すること。
9. シャーシ全面の LED でシステム、ファン、温度、ネットワーク、電源のステータスを確認できること。
10. 1G/10GBase-T (RJ45) を 2 ポート以上有すること。
11. 25GBase-SR (SFP28) ポートを 4 ポート以上有すること。
12. 1GBase-T (RJ45) の管理専用ポートを有すること。
13. RS-232C (RJ45) のシリアルポートを 1 ポート有すること。
14. VGA ポート (DB15) を 1 ポート有すること。
15. USB3.0 2 ポート有すること。
16. ホットスワップ可能な 1050W 以上の AC 電源モジュールを 2 個以上搭載し、冗長構成とすること。
17. AC 電源モジュールは高変換効率の 80 Plus Platinum 認定を取得していること。
18. 12G SAS RAID Controller は最大 10 個の SAS/SATA ディスクをサポートすること。また、4GB のフラッシュバック・ライトキャッシュ(FBWC)を装備し、RAID 0,1,5,6,10,50,60,SRAID, JBOD に対応すること。
19. RAID コントローラは専用スロットに装着され、PCI スロットを専有する必要の

ないこと

20. 10/25Gb で FCoE 対応のインタフェースを 4 個有するネットワークインタフェースカードを PCI スロットを使わない専用スロット(mLOM)にて搭載すること。ネットワークカードは 900,000 以上の IOPS 性能を持つこと。
21. ネットワークカード一枚につきデフォルトで 4 個の vHBA (仮想ホストバスアダプタインタフェース)と 4 個の vNIC (仮想ネットワークインタフェース) が用意されており、最大 10 個の vNIC または vHBA を追加作成できること。SR-IOV を用いず、サーバ管理ソフトウェアから設定可能なこと。
22. 追加した vNIC ごとにレート制限(Rate Limit), VLAN, MAC アドレス, 優先制御 (CoS), VXLAN/GENEVE オフロードが設定可能なこと
23. 追加した vHBA ごとにレート制限(Rate Limit), WWNN, WWPN, MAC アドレス, 優先制御(CoS)が設定可能なこと
24. ネットワークカードは、usNIC 技術により 2 マイクロ秒の以下の遅延を実現可能なこと。
25. TPM2.0 (Trusted Platform Module)を装備すること
26. 設定情報を GUI ベースの管理画面からバックアップ・リストアが実行可能なこと。バックアップはネットワーク設定・電力ポリシー・BIOS パラメータ・SNMP などを取得できること。
27. サーバ管理ツールは Web ブラウザを用いてリモートからグラフィカル(GUI)インタフェースを使用可能なこと。
28. リモートから KVM コンソール (キーボード・ビデオ・マウス) を使いサーバ接続が可能なこと
29. 仮想メディア機能を有し、リモートからパソコンもしくはネットワーク上にある CD/DVD ドライブや ISO イメージにアクセスして OS のインストール等が可能なこと。
30. サーバ管理ツールはメインサーバ CPU から独立している専用のプロセッサを使用することでサーバ本体や OS の障害の影響を受けることなく管理が可能なこと。
31. IPMI に準拠した専用の管理ポートを有し、OS やハイパーバイザーが停止している状態でも当該ポートを介して IPMI を利用したネットワーク経由での操作が可能なこと。また、XML API を使用した管理も可能とすること
32. システムの起動時にハードウェアの不正な変更を検証する TPM(Trusted Platform Module)およびメーカーでの製造時に付与する固有のセキュアデバイス識別子を搭載するチップを標準装備し、ハードウェアの不正改ざんを確認できること。
33. 入力電圧 100~240 VAC、50-60 Hz にて動作すること。

34. サーバ管理ツールにて以下の管理が可能なこと。

(オ)接続されている全てのサーバが一元的な画面で統合管理できること。

(カ)インベントリ情報（サーバ名・モデル・シリアル番号・CPU・メモリ・HDD・NIC）の確認が可能なこと。

(キ)アラートやエラー情報などシステムの健全性を監視

(ク)システムエラー発生時、障害対応連絡がツール上から可能なこと。

3.26. 共有ストレージ

【想定機種：Pure Storage 社製 X20R3-ETH-22TB-22/0-EMZZ】 【数量：1 台】

1. 以下の領域で構成すること。
 物理領域 21TB 以上
 実行容量（有効容量） 12TB 以上（重複排除未考慮）
 2. 将来の拡張を考慮しシェルフの増設が可能な構成であること。
 3. フラッシュのみ（フラッシュモジュール）のみを搭載したオールフラッシュストレージであること。
 4. 16G Fiber Channel ポートをコントローラあたり 4 ポート以上有すること。
 5. ストレージ筐体のコントローラは冗長構成で、片側のコントローラで障害が発生しても性能影響のないアクティブ-スタンバイ構成であること。
 6. コントローラ障害時にも Write 性能に影響が無いように、NVRAM（Write キャッシュ）は、ストレージコントローラ外に独立し、NVRAM、コントローラ共に 2 重化以上の可用性をもつこと。
 7. コントローラ、NVRAM、SSD、電源まで全てのコンポーネントをモジュール化し、性能影響なく障害時に交換できること。
 8. インラインでの重複排除機能を有し、可変長による重複判定が可能であること。
 9. インラインでの圧縮機能に加え、バックグラウンドによる圧縮によりさらに圧縮率を高める機能を実装していること。
 10. 重複排除、圧縮、暗号化機能は常時有効であること。
 11. ストレージの暗号化機能を有すること。有効時にも性能影響がないこと。
 12. 暗号化済みドライブのデータは、当該筐体以外（別筐体に搭載）ではデータを読み出しできないこと。
 13. 1 Lun のサイズは、1MB～最大 4PB まで作成できること。
 14. 任意のタイミングでスナップショットの取得、世代管理（最大 50,000 世代）が可能であること。スナップショット取得の際に性能影響がないこと。
 15. コントローラのメンテナンスや、コントローラ障害時の IO 待機時間を低減させるために、NPIV をサポートしていること。
 16. フラッシュモジュールは、SAS 接続、NVMe 接続をサポートすること。同一筐体内で混在が可能であること。
 17. メーカーのリモート保守サービスが標準機能で提供可能であること。
- ログは機器本体より 30 秒以上・1 分以内の間隔でメーカー提供のクラウドサポート基盤にログ転送し、13 ヶ月間保持できるサービスを、保守の範囲で提供する。

18. リモート保守サービスを活用し、VMware vSphere 環境からログを取得することで仮想ディスク、仮想マシン、ESXi ホスト、データストア、ボリューム (LUN)、アレイまで、各レイヤーの性能情報をフルスタックで表示できる管理ツールを提供できること。
19. メーカーサポートエンジニアがリモートから、即時ログインできるサービスを通常の保守で提供すること。
20. グローバルで稼働している機器から送信されるログを収集し、メーカーの提供するクラウドサポート基盤内にて、ログを解析・分析し、未然に障害を防ぐ対策、通知を通常の保守にて提供すること。
21. ストレージ管理にあたり、GUI ベースの管理ツールを無償で提供すること。また、各種情報（容量、IOPS、遅延、スループット）がリアルタイムで可視化できること。
22. データの増加量およびストレージパフォーマンスの将来予測、それらのレポート機能も有すること。
23. 別途、専用管理サーバ・ソフトウェアを必要とせず、Web ベースのアクセスにて管理ができること。
24. RAID6 相当の可用性を有すること。RAID 設計は必要なく自動的に設定されること。また容量拡張時にも、フラッシュモジュールの追加、シェルフの追加の場合も同様とする。
25. Snapshot に含まれるデータも重複排除および圧縮の対象になること。
26. ランサムウェア等のマルウェア対策として、ストレージ管理者の管理権限を用いても、ストレージのスナップショット機能で取得した LUN のスナップショットを設定された期間内は完全に消去することが不可能な機能を有していること。

3.27. 管理用パソコン

【想定機種：Dell 社製 Latitude 3520 】 【数量：2 台】

項 目	機 能
機種	ノートパソコン
OS	Windows11 Pro （日本語版）
CPU	Core i3-1115G4 以上
メモリー	4GB 以上
内蔵ストレージ	SSD 256GB 以上
ディスプレイ	13 インチ HD 以上
インターフェース	<ul style="list-style-type: none"> ・有線 LAN（1000BASE-T/100BASE-TX 以上）端子 ・HDMI×1 以上 ・USB ポート×1 以上
キーボード	日本語キーボード（JIS 配列準拠）

4. ソフトウェア及びライセンス調達

以下に要求仕様及び想定する機種を示す。

4.1. インターネット分離システム

【想定機種：Sky 社製 SKYDIV SBC 構成】【500 ユーザ同時接続ライセンス】

1. 本システムは Windows ServerOS で構成すること。
2. システムの管理用画面は日本語の UI が提供されること。
3. マウスカーソルが指すボタンの簡易説明が表示される設定ができる機能を有すること。
4. システムで利用するサーバーOS については、導入される組織において、すでに利用され、運用する際に新たな知識を必要としない OS だけで構成することが可能であること。
5. システムを構成する各サーバーは、環境構築状況や問題の発生状況を正しく確認できるよう、UI 上に構成図として視覚的に表示されること。
6. アイコン上やサーバー登録一覧にアラートや異常状態の情報を表示できること。発生している一番優先順位の高いアラート項目の色で、各サーバーの状態を色付けして表示でき、アラートの詳細機能も確認できること。
7. システムを構成する各サーバーのメモリ使用率やネットワークの送信・受信量などのパフォーマンスに関する情報を、グラフで視覚的に確認できること。
8. 各サーバのシステム稼働ログやイベントログを収集し、収集したログを対象サーバ、対象期間、ログ種別、警告レベル、キーワード等の検索条件を複数指定して検索できること。また、ログの検索条件は保存できること。
9. 各サーバーのメンテナンス前に、サーバーの常時監視およびリモートデスクトップ接続の新規受付の停止を設定できること。
10. 管理画面上でサーバーごとにログオンしているユーザや仮想端末の利用状況を確認できること。また、以下の項目が設定できること。
 - ・新規リモート接続の受付停止
 - ・仮想端末のログオフ / 電源 OFF / 電源 ON / 停止
 - ・利用中のユーザに事前メッセージで通知"
11. 管理コンソールから SQL Server Express の冗長化構築を行うことができること。
12. システム上で予め設定されたアラートが発生した場合、管理者へメールで通知するよう設定できること。また、メールによる通知のタイミングは、アラートの重要度に応じて、即時／1 日に 1 回／通知なしの 3 段階に設定されていること。

13. 特権管理者として権限設定したユーザのみ以下の項目を設定する権限が与えられること。
 - ・ SQL Server 冗長化管理
 - ・ サーバーの追加 / 削除
 - ・ 管理者の追加 / 削除
 - ・ RD ライセンスの設定
 - ・ RD ライセンスサーバーの優先順位を設定（SBC(RDS)方式）
 - ・ サーバの常時監視
 - ・ リモートデスクトップ接続の新規受付の停止（SBC(RDS)方式）
14. ユーザが使用する、同一構成の仮想端末やリモート接続サーバーの作成を行いやすいよう、UI 上で仮想化の方式や設定について、イラストとヒントを用いて解説されていること。
15. 仮想化されたアプリケーションは、利用者が物理端末上のローカルアプリケーションと識別できるよう、ウインドウ上部やウインドウ上下左右にマーカーが付与され、容易に識別が可能であること。
16. 1 台の物理端末で、異なる仮想イメージを利用できるランチャーを備えていること。また、ランチャーのアイコン色を利用者ごとに任意で設定できること。
17. アカウント管理については、Active Directory 上のユーザ情報を利用して実現可能なシステムであること。
18. Active Directory 上の OU またはセキュリティグループを、本システムの部署情報として紐づけでき、OU 配下またはセキュリティグループ配下のユーザを、紐づけた部署の配下にユーザとして反映できること。"
19. RemoteFX USB リダイレクトで接続されたデバイスについて、デバイス種別ごとに使用を禁止する設定ができること。また、禁止したデバイス種別の中から特定のデバイスの禁止を除外できること。
20. ユーザが任意の URL から Web ブラウザを起動する際に、仮想環境もしくはローカル環境のいずれでブラウザを起動するかを、管理者が事前に指定できること。さらに、事前に登録した URL を、仮想環境もしくはローカル環境のいずれで起動するかについても指定できること。
21. ファイル無害化システム（参考：Opswat MetaDefender Core）との連携が可能なこと。
22. 物理端末と仮想端末間のクリップボード共有は、指定したクリップボードのデータカテゴリ別（テキスト、ファイルなど）ごとに、制限できること。また、物理端末から仮想端末へのクリップボード共有のみ / 仮想端末から物理端末へのクリップボード共有のみ許可する設定もできること。またプリセット設定を利用してクリップボード制限が行えること。

- 23. 仮想環境上の画面上で、アニメーションなどの視覚効果を減少させる事で通信量を軽減できること。
- 24. システムのソフトウェアを開発サポートする組織は、日本国内に存在し、日本国内でトラブル解決が完結するメーカーの製品であること
- 25. サポート情報や技術情報等のメーカーから提供される情報については、すべて日本語であること。
- 26. システムのアップデート・最新版へのバージョンアップが可能なこと。
- 27. 仮想環境への接続失敗や認証不可などのエラーが発生すると、問い合わせ番号が記載されたエラー画面を物理端末に表示すること。また、その問い合わせ番号から詳細や対処方法を管理画面上で確認し、メモも追記できること。

4.2. メール無害化システム

【想定機種：デジタルアーツ社製 m-FILTER】 【数量：3,000 ユーザライセンス】

1. メールフィルタリングソフト、もしくはメールフィルタリングサービスであること。
2. 国内で開発・販売されている製品で、日本語によるサポート対応が可能であること。
3. 外部からの攻撃メールを受信され場合にそのリスク情報を通知する無償のサービスを提供していること。
4. 動作環境として、Windows Server と Red Hat Enterprise Linux のいずれにも対応していること。
5. メール通信プロトコルは SMTP だけでなく POP にも対応しており、メール暗号化方式として STARTTLS にも対応していること。
6. SPF 認証の技術と独自のロジックをベースに送信元アドレスの偽装を LAN 内環境に設置した場合でも判定可能なこと。
7. 安全な差出人の「IP アドレス」と「ドメイン」をデータベースとして有し、データベースを利用して安全なメールのみを受信可能な機能を有すること。また、データベースに存在しない「IP アドレス」と「ドメイン」を収集し、精査した上でデータベースとして配信できること。
8. Web フィルタリング製品と連携し、メールの本文・添付ファイル内の悪性 URL や未カテゴリ URL を Web に自動登録が可能なこと。
9. メール本文・添付ファイル内に悪性 URL や未カテゴリ URL があった場合、当該メールを配送せずに隔離できること。
10. 添付ファイルが ZIP パスワードロックされている場合でもファイルの危険因子の判定が可能なこと。
11. 電子メールの送信元、メール本文、添付ファイル、またはメール内のリンク先それぞれの要素に対して評価基準を定め、レベル判定を行うことで偽装か否か精度よく判断することができる技術を利用していること。
12. メール本文の無害化処理(添付ファイル削除、URL 含めたリンクの無効化、HTML メールやリッチテキストメールの本文テキスト化)
13. ファイルを一旦分解した上で危険因子を除去した後、ファイルを再構築できるファイル無害化システム（参考：Opswat MetaDefender Core）と連携し、添付ファイルを自動で無害化を実施させ、無害化済のファイルを再度添付し直し、配送することが可能なこと。ファイルの埋め込み画像や埋め込みオブジェクトなどの

要素に対しても、再帰的に無害化処理をすること。

14. 異なるネットワークセグメントでファイル受け渡しを簡単にできるファイル転送ソリューションと連携し、自動で添付ファイルを連携先にアップロードし、添付ファイルの受け渡しをスムーズに行うことが可能なこと。
15. 送信メールを即時送信せず、事前に設定した任意の時間、一時保留可能なこと。
保留時間設定箇所は、宛先が社内か社外かで分かれており、社内外時間差配送が可能なこと
16. 3,000 ライセンスを有すること。

4.3. WEB メールシステム

【想定機種：クオリティア社製 DEEPMail】 【数量： 3,000 ユーザライセンス】

1. SMTP、POP3、IMAP4、Web メール、メーリングリスト機能を統合した 1 つのメール専用ソフトウェアであること。
2. システム管理者は、ドメイン毎にドメイン管理者アカウントを指定できること。
3. システム管理者は、ドメイン毎にユーザ数を制限できること。
4. 各ドメインごとにログイン URL を指定することにより、メールアドレスのローカルパートのみをログイン ID として使用できること。
5. スプールする電子メールは Maildir 形式またはこれに準ずる形式で格納すること。
6. システム管理者、及びドメイン管理者は各ユーザが設定した自動振り分け設定、転送設定、自動応答設定、モバイル設定を Web インターフェースを用いて確認・編集可能であること。
7. ユーザは Web メール画面内に用意された領域に http でファイルをアップロードし、受信者に URL を通知し、そのファイルをダウンロードさせる機能を有すること。URL を通知する際に、ダウンロード期限、ダウンロード回数、ダウンロードの為のパスワードを設定できること。
8. Web メールからメールを送信する際、任意のメールアドレスをヘッダーFrom として使用できること。
9. Web メールを表示中に新着メールがある場合、通知する機能を有すること。但し、ポップアップブロックの制限を受けないこと。
10. 新着メールのチェック間隔は、管理者が設定した最小間隔を下回らない制限内で各ユーザが自分自身で設定できること。
11. Web メールからの送信操作時に発送時刻を指定しておき、即時には送信せずにその時刻に達したときに自動的に送信する機能を有すること。
12. Web メールからのメール作成時に、住所録と送信先アドレス履歴に存在するアドレスを各宛先欄に入力する時に補完する機能を有すること。なお、システム管理者は、補完候補のアドレスが表示されはじめる文字数と表示件数を設定可能なこと。
13. Web メール画面内にオプションではなく標準機能としてメーリングリスト管理機能を備えていること。
14. メーリングリストに参加する外部ドメインユーザ向けの専用 Web インターフェースを提供すること。

15. システム管理者は、各ユーザが SMTP,POP,IMAP,Webmail でログインする際の接続元 IP アドレスについて国ごとに指定してログインを制限できること。また、その設定画面を GUI 上で備えていること。
16. システム管理者が指定した許可国以外に各ユーザがログイン可能な国を増やすことができる設定を Webmail 画面内に用意すること。
17. ユーザはメーリングリスト管理画面からメーリングリストを作成できること。ただし、管理者の承認を要する設定が可能なこと。
18. メーリングリスト参加者は、Web インターフェースを用いてアーカイブされているメールを検索・表示・取得できること。
19. システム管理者画面では、CPU 使用率、主記憶領域使用量およびハードディスク使用量について、直近の状況を表示可能であること。
20. システム管理者画面では、SMTP/POP3/IMAP4/Web メールログインの各処理について、出力されたログを Web インターフェース上で閲覧、及びダウンロードできること。
21. 管理者用 Web 画面では、グループあるいはユーザごとに、送受信できるメールサイズおよび添付サイズを制限する設定が可能なこと。
22. メールボックスを 2,000 の個人ユーザと 250 の所属（部署）ユーザが利用可能なこと。

4.4. スпамメール対策システム

【想定機種：Fortinet 社 FortiMal-VM01（1CPUcore）】 【数量：2 式】

1. ハイパーバイザー上で構築可能な仮想アプライアンス製品であること。
2. 保護されるメールドメイン数が 20 以上であること。
3. 受信者ポリシーを 60/300（ドメイン/システム）以上設定が可能なこと。
4. アンチスパム・アンチウイルス機能を搭載していること。
5. アンチスパム・アンチウイルスはシグネチャ/シグネチャレス検査可能なこと。
6. コンテンツ/フィルタタイプのフィルタリング機能が可能なこと。
7. Eメールの暗号化が可能なこと。
8. メールアーカイブ機能、システム/ユーザ隔離機能があること。
9. インバウンドとアウトバウンド通信のスキャンが可能なこと。
10. ゲートウェイモード（MTA）で導入可能なこと。
11. WebUI 及び CLI から設定管理が可能なこと。
12. WebUI は日本語に対応していること。
13. SNMPv1/v2c/v3 に対応していること。
14. Telnet、SSH によるリモートアクセス管理が可能なこと。

4.5. ファイル無害化システム

【想定機種：OPSWAT 社製 MetaDefender】 【数量：1 式】

1. ファイル交換を行う対象ストレージとして以下のストレージ内のファイルを検査して無害化等の処理を行えること。
 - ・ファイルサーバ（Windows SMB ファイルサーバなど）
2. 対象ストレージ内のフォルダにファイルが格納されたら即時検査することやスケジューラで指定して一斉
3. ストレージ内の検査については、ファイルが格納されたら即時検査する、スケジュールで一斉検査を行うなどの柔軟なタイミングの設定（月/日の単位で任意の期間）が可能なこと。
4. マルウェア検査でマルウェア判定が行われた際に以下の処理が行えること。
 - ・マルウェア判定されたファイルは別領域に保存する。
 - ・マルウェア判定されたファイルは削除する。
5. 無害化処理後のファイルについて以下の処理が行えること。
 - ・無害化されたファイルは別領域に保存する
 - ・無害化されたファイルは無害化前の元ファイルを上書きする
6. インターネット経由でファイルを LGWAN 環境に取り込む場合はスクリプトやマクロや OLE オブジェクトなどのリスクの高い因子について総務書ガイドラインの無害化処理要件を満たしたうえで取り込めること。
7. 無害化エンジンのソースファイルの拡張子の対応数については、100 種類以上を要件とすること。またその要件は一般に公開されていることを要件とする。
8. 無害化後のファイルの操作性（編集・加工）やアプリケーションの適合性を保持するため、無害化処理前と処理後で 75% 以上はファイル拡張子が変わらないことを要件とする。なお無害化処理についてはファイル構造を解析して、内部構造に含まれるファイル要素も無害化処理して再構成する処理プロセスを要件とし、この処理においてファイル拡張子が維持されることを要件とする。
9. 無害化に対応していないファイルについては、マルチスキャン処理（複数のマルウェア検査エンジンによるウイルスチェック）を行い、安全判定となった場合に無害化処理はせずにファイルのダウンロードを可能とする制御ができること。
10. 無害化に対応しないファイルに対する危険因子のないことの確認のためのマルチスキャンエンジンについては 8 つ以上のマルウェアエンジンで検査できること。
11. ファイルの拡張子だけでなく、ファイルシグネチャーやファイル構造などからファイルタイプを識別できること。また、ファイル構造が正規の仕様と異なる場合はこれを遮断もしくは正規のファイル形式への修正ができること。

12. 無害化に対応していない拡張子や拡張子を改ざんした不正なファイルの転送を遮断、または許可できること。
13. 無害化処理のポリシー設定については、アプリケーション単位にポリシー設定が可能であること。(例：Microsoft Office の場合、Word/Excel/Powerpoint などの単位)
14. 無害化結果は、そのファイルが持つ要素（Office ファイルの場合、埋め込みオブジェクトやマクロ、ハイパーリンクなど）ごとに確認が可能であること。
15. 以下のファイル（拡張子）を無害化処理できること。

<文書ファイル>

Word (doc、docx、docm)
 Excel (xls、xlsx、xlsm)
 PowerPoint (ppt、pptm、pptx、ppsm)
 Word Viewer (rtf)
 Visio(vsdx)
 一太郎文書 (jtd、jtdc)
 PDF (pdf)
 DocuWorks (xdw)

<画像ファイル>

JPEG (jpg/jpeg)、PNG(png)、TIFF(tiff)、GIF (gif)、BMP (bmp)、
 Windows Metafile(wmf/emf)

<動画ファイル>

WMV(wmv)、MPEG(mpeg)、WAV(wav)、MP3(mp3)、MP4(mp4)、
 MOV(mov)、AVI(avi)、WEBM(webm)

<圧縮ファイル>

ZIP (zip)、RAR(rar)、7Z(7z)、GZIP(gz)、XZ (xz)、LZH (lzh)

<CAD>

AutoCAD (dwg)、AutoCAD Drawing Template (dwt)、
 AutoCAD Drawing Standards (dws)、SXF Feature Comment (sfc)、
 STEP Data Model (p21)、JW CAD(jww)、
 Drawing Interchange Format(dxf)、
 Design Web Format (dwf)、3D Studio (3ds)

16. 無害化対象とする拡張子は、拡張子ごとに有効／無効が設定可能であること。
17. アクセス管理において Active Directory と連携が可能であること。
18. ログ情報を Syslog サーバに転送可能であること。
19. 無害化装置の保守サポートにあたっては国内に製品担当技術者・サポートセンターがあり日本語での問い合わせの対応が実施できること。

- 20. 利用者の端末に専用モジュールをインストールせずに、機能を提供すること。
- 21. 利用ユーザ数の増減によってライセンス費用が変化しないこと。

4.6. 内部ファイル交換システム

【想定機種：ノースグリッド社製 Proself Gateway Edition】 【数量：2 式】

1. 異なるネットワーク間でデータファイルを受け渡しが可能で、ネットワーク間のやり取りは片方向、双方向に制限可能な機能を有すること。
2. データファイルを受け取る前に任意のユーザによる承認機能を有すること。
3. 承認を行うネットワークを設定することが可能な機能を有すること。
4. 特定のファイルタイプのみ受渡可能にできるようデータの拡張子を 制限可能な機能を有すること。
5. ファイルの受け取り方法を運用によって変更できる機能を有すること。
6. データベースを別途インストールしなくても動作すること。
7. ActiveDirectory/LDAP 連携に標準対応していること。
8. CSV からユーザのインポート/エクスポート可能な機能を有していること。
9. 利用履歴と証跡を一元的に保存する機能を有していること。
10. アップロードされたファイルに自動的に保管期間が設定可能であること。
11. 画面上のすべての文言を自由に変更する機能を有すること。
12. 本仕様書に記載のファイル無害化システムと連携して受け渡しの際にファイルが無害化できること。
13. ファイルの受け渡しは双方向共に Web ブラウザを用いた方式に加え Windows のネットワーク共有フォルダを用いてエクスプローラーから行えること。
14. 暗号化 ZIP ファイルであってもパスワードを入力する仕組みを別途用意することでエクスプローラーから受け渡しすることができること。

4.7. 外部ファイル交換システム

【想定機種：ノースグリッド社製 Proself Enterprise Edition】 【数量：1 式】

1. 一時 URL を経由して利用者アカウントを持たない他人に対してファイルを送信できること。
2. 一時 URL を経由して利用者アカウントを持たない他人からファイルを受信できること。
3. 利用者アカウントをもつ複数の利用者でアクセス可能な領域を作成し、ファイルを共有できること。
4. 利用者が Web ブラウザでファイルの操作を行える Web インターフェイスを有すること。
5. データファイルを受け渡す、受け取る前に任意のユーザによる承認機能を有すること。
6. 特定のファイルタイプのみ受渡可能にできるようにデータの拡張子を制限可能な機能を有すること。
7. データベースを別途インストールしなくても動作すること。
8. ActiveDirectory/LDAP 連携に標準対応していること。
9. CSV からユーザのインポート/エクスポート可能な機能を有していること。
10. 利用履歴と証跡を一時的に保存する機能を有していること。
11. アップロードされたファイル自動的に保管期間が設定可能であること。
12. 画面上のすべての文言を自由に変更する機能を有すること。
13. SSL 通信を行うための、SSL 証明書を調達すること。

4.8. ID 連携用システム

【想定機種：ジインズ社製 ADMS Lite】 【数量：1 式】

1. ネットワーク分離されたについて Active Directory の管理についてユーザの設定作業を軽減させるため、以下機能を実現するソフトウェアを用意すること。
2. 「LGWAN 接続系」における Active Directory の組織単位 (OU)・グループ・ユーザ情報をテキスト形式で出力し、出力したテキストファイルを「インターネット接続系」で取り込み、組織単位 (OU)・グループ・ユーザ情報の追加・変更・削除、パスワード設定を行う機能を有すること。
3. 「インターネット接続系」において登録するユーザ情報は、条件を設定し絞り込みができる機能を有すること。
4. ネットワーク分離された Active Directory はドメインが異なるため、データ同期時に別ドメインへ変換する機能を有すること。
5. データの取り込み結果をログに出力する機能を有すること。
6. データを取り込む前に反映結果が確認できる、リハーサル機能を有していること。
7. 連携元 AD で変更されたパスワード情報を連携先 AD にリアルタイムで反映できる機能を有すること。

4.9. 仮想化基盤ウイルス対策システム

【想定機種：トレンドマイクロ社製 DeepSecurity Agent】【数量：1 式】

1. エージェント型であること。
2. 保護対象として、Windows/Linux をサポートしていること。
3. 不正プログラムを検知し、駆除・蚊瓜・削除する機能を有すること。
4. 不正プログラムの検知はリアルタイム、スケジュールおよび手動により実行する機能を有すること。
5. CPU の使用率によって検索の一時停止を自動で判断できる機能を有すること。
6. プロセスメモリ内の不正プログラムを検出できること。
7. 特定のフォルダや拡張子などを検索対象外にすることができること。
8. Web サイトにアクセスする際に自動的に安全性を確認する機能を有すること。
9. C&C サーバへの接続を検出し、接続をブロックできること。
10. 仮想化システムにおいて実行中の仮想マシンをホスト間で移行した場合でも、保護を継続できること。
11. Web ブラウザを使用した管理ツールにて様々な環境（物理/仮想）のセキュリティ管理を統合的に行える機能を有すること。
12. 管理ツールを介して行われたすべての操作を記録できる機能を有すること。
13. 管理ツールは、ロールベースアクセス管理、管理者権限の委譲機能を有すること。
14. 管理ツールにて、特定の情報（システム、イベント、レポート等）を迅速に確認可能な GUI 表示をカスタマイズ可能なこと。
15. 管理ツールが日本語に対応していること。
16. アラートメールを送信する機能を有すること。
17. イベントを Syslog に送信する機能を有すること。
18. イベントを SNMP Trap にて送信できる機能を有すること。
19. レポート機能を有すること。
20. セキュリティ対策の設定をテンプレート化し、同一構成の複数サーバを統一的に管理できる機能を有すること。
21. 各マシンにセキュリティ対策の設定を設定できること。
22. システムを検索し、必要なルールを自動的に選定、適用でき、不要になった場合は自動的に解除する機能を有すること。
23. パターンファイルのアップデート頻度を設定できること。
24. 70 台のサーバのウイルス対策が可能なこと。

4.10. バックアップシステム

【想定機種：Veeam 社製 Veeam Backup & Replication】【数量：1 式】

1. VMware、Hyper-V のマルチハイパーバイザをサポートしていること。
2. 全ての仮想マシンでバックアップ取得できるライセンスを有すること。
3. 仮想マシンに対してエージェントをインストールしなくともバックアップ可能であること。
4. ハイパーバイザーがサポートしているすべての OS について、バックアップが可能であること。
5. 管理サーバ、処理実行サーバを分割して配置することが可能であること。
6. バックアップ対象の仮想マシンが増えた場合も、処理実行サーバを増やすことで滞りなく処理を実行可能であること。
7. 変更点のみのバックアップが可能であること。
8. 重複排除、圧縮によりバックアップファイルのサイズ削減が可能であること。
9. バックアップ対象となる仮想マシンのディスクを指定可能であること。
10. Microsoft VSS(ボリューム・シャドウ・コピー・サービス) により、静止点の作成が可能であること。
11. 任意のスクリプトによる静止点の作成が可能であること。
12. バックアップを実施するタイミングを日付と時間で指定、実施しない時間帯を指定可能であること。
13. バックアップが指定した時間帯までに終了しなかった場合、強制停止が可能であること。
14. バックアップに対して破損チェックを実施可能であること。
15. 失敗時の再試行回数、間隔を指定可能であること。
16. ゲスト OS のページファイルやスワップファイル領域をバックアップから除外可能であること。
17. ハイパーバイザ上から削除された仮想マシンのバックアップについて、保持期間を指定可能であること。
18. 増分、差分バックアップが可能であること。
19. 2 回目以降のバックアップでは合成でのフルバックアップが作成可能であること。
20. 合成フルバックアップ時に古い世代の増分バックアップを差分バックアップに変換可能であること。
21. ファイルサイズが 2TB 以上の仮想マシンについてもバックアップ、レプリケーション可能であること。

- 22. ゲスト OS 内のファイルをバックアップから復元可能であること。
- 23. 仮想マシンの構成ファイルをバックアップから復元可能であること。
- 24. 仮想マシンのディスク単位でバックアップから復元可能であること。
- 25. バックアップから仮想マシンをリストアする際に、オリジナルの仮想マシンを上書きするか、新しい仮想マシンを作成するか選択が可能であること。
- 26. バックアップ内の仮想マシンをハイパーバイザに転送せずに直接起動が可能であること。
- 27. バックアップ等の設定情報をバックアップが可能であること。
- 28. 管理についてはユーザ単位で権限を設定可能であること。
- 29. Web ブラウザからバックアップの状況表示、実行が可能であること。
- 30. メール通知、SNMP 通知が可能であること。
- 31. 70 台の仮想マシンのバックアップを取得可能なこと。

4.11. 負荷分散装置

【想定機種：F5 社製 F5-BIG-LTM-VE-1G-V18】 【数量：1 式】

1. ハイパーバイザー上での動作がサポートされていること。
2. OVA 形式で製品イメージが提供されていること。
3. 1Gbps 以上のスループットをサポートしていること。また処理能力向上でアップグレードライセンスが提供されていること。
4. 処理能力を拡張するためのアップグレードライセンスが提供されていること。
5. L7 での負荷分散において、秒間 3,000 リクエストから秒間 2,000,000 リクエストまで対応可能であること。
6. L4 での負荷分散において、秒間 2,000 リクエストから秒間 625,000 リクエストまで対応可能であること。
7. SSL アクセラレーションにおいて、秒間 9,700 トランザクションの処理能力あること。(RSA 鍵長 2048bit 時)
8. SSL アクセラレーションにおいて、秒間 47,500 トランザクションの処理能力あること。(ECC)
9. レイヤ 4、レイヤ 7 の負荷分散が可能であること。
10. 負荷分散機能として、下記のロードバランシング方式を備えること。
Round Robin (均等)、Ratio (比率)、Least Connections (最小接続)、Fastest (最速)、Least Sessions (最小セッション)、Weighted Least Connection (重み付け最小接続)、Observed (監視)、Predictive (予測)、Dynamic Ratio (動的比率)
11. ヘルスチェック機能として、下記のモニタリング方法をサポートすること。
12. ICMP、TCP、UDP、Diameter、RADIUS、HTTP、HTTPS、FTP、IMAP、LDAP、MSSQL、MySQL、NNTP、Oracle、POP3、PostgreSQL、Real Server、SASP、RPC、SIP、SMB、SOAP、WAP、WMI、Firepass、DNS
13. ヘルスチェック機能として、スクリプトを利用した監視、外部コマンドを利用した監視が可能であること。
14. セッション維持機能として、IP アドレス情報、HTTP Cookie 情報、HTTP ヘッダ情報、SSL セッション ID 情報でのパーシステンス機能をサポートしていること。
15. レイヤ 7 のデータペイロードの情報をもとにして、トラフィック制御が可能であること。
16. HTTP ヘッダの変更/挿入/削除ができること。
17. HTTPCookie 暗号化による、なりすまし防御機能を備えること。

18. 脆弱性につながる特定の文字列（サーバの情報など）をレスポンスから遮断するリソースクローキング機能を備えること。
19. VLAN ごとにルーティングテーブルや管理ドメインを分割できる機能を備えること。
20. 分散対象サーバの IP アドレスに重複があった場合でも、サーバの IP アドレスを変更することなく、負荷分散処理が可能なこと。（ルートドメイン機能）
21. TLS1.3 にサポートしていること。
22. HTTP/2 に対応し、HTTP/2 ゲートウェイとして動作できること。
23. コンテンツキャッシュ機能と HTTP 圧縮機能を備えること。
24. スクリプトベースの柔軟なルールを定義可能であること。
25. システム状態を監視し、特定イベントが発生した場合に、自動的に処理や設定変更を行う機能を有すること。
26. パケットをミラーリング し、フォレンジック機器等へ実通信と同じパケットを送信できること。
27. L7(HTTP Cookie 等)の通信状態を冗長構成機器間で同期でき、障害切替時に通信の引き継ぎが可能であること。
28. 負荷分散対象サーバの障害時の Sorry ページ機能を有すること。
29. http request を https へリダイレクト可能であること。
30. NAT 機能を有すること。
31. SSL アクセラレーションの機能を有すること。
32. SSL ハンドシェイクの同時実行数を設定でき、SSL 通信の集中時に輻輳回避する機能を有すること。
33. SSL レコードサイズの動的変更に対応し、パケットロス時の通信再送を効率化できること。
34. SSL サーバ証明書をバックアップファイルに含めることができること。
35. バックアップファイルからリストア時に、SSL サーバ証明書も復元できること。
36. 明示及び透過型の HTTP プロキシ機能を有すること。
37. ソースアドレスの隠蔽が可能なこと。
38. アクセス先を IP アドレス/ポート制限単位で制限可能なこと。
39. クライアントの IP アドレスやサブネット単位で制限可能なこと。
40. キャッシュ機能を有すること。
41. アクセスログを出力し、保存可能なこと。
42. PAC ファイルの定義・WPAD プロトコルに対応していること。
43. 論理的に分割した複数のネットワーク構成上でも対応できること。
44. 設定情報のバックアップ及びリストア機能を有し、バックアップファイルの暗号化も可能であること。

- 45. 機器に対応が必要な異常が発生した場合、SNMP 及びメールで警告を送信できること。
- 46. Web ブラウザより HTTPS で GUI 管理/設定を行う機能を有すること。
- 47. SSH により CLI 管理・設定を行う機能を有すること。
- 48. パケットキャプチャを取得する機能を有すること。
- 49. 機器へログインするパスワード強度を高められること。

4.12. Syslog サーバ

【想定機種：SolarWinds 社製 KiwiSyslogServer】 【数量：1 式】

1. ログの保存ができること。
2. ログが CSV または XML にて出力することができること。
3. Web ブラウザでログが閲覧することができること。
4. 送信元 IP アドレス、受信日付でログファイルを自動で分割できること。
5. ログを圧縮してアーカイブすることができること。
6. 保存期間が過ぎたログを自動で削除することができること。
7. Windows Server OS 上で構築が可能なこと。

4.13. サーバ仮想化ソフトウェア仕様

サーバ仮想化ソフトウェアについては、以下の製品を調達すること。

以下の製品以外で入札する際は事前に同等品申請を行い、市の承認を得ること。

【想定機種：VMware 社 vSphere8 シリーズ
VMware 社 vCente Server8 シリーズ】

項 目	機 能	数 量
ライセン ス等	●ライセンス 型式：VS8-EPL-C 製品名：vSphere Enterprise Plus	8
	●サポートライセンス 型式：VS8-EPL-G-SSS-C 製品名：Basic SnS vSphere Server 8 STD for vSphere8 1 年	48
	●ライセンス 型式：VCS8-STD-C 製品名：vCenter Standard	1
	●サポートライセンス 型式：VCS8-STD-G-SSS-C 製品名：Basic SnS vCenter Server8 STD for vSphere8 1 年	6

4.14. 各種 OS ソフトウェア

本システムを構成する上で必要となる以下のソフトウェアを調達すること。

項 目	機 能	数 量
OS	本システムの仮想基盤用 Windows Server OS に以下のソフトウェアを調達すること ・ Windows Server 2022 Datacenter -2core License Pack	128
OS	本システムのバックアップシステム用 Windows Server OS に以下のソフトウェアを調達すること ・ Windows Server 2022 Standard -2core License Pack	8
OS	本システムのデータベース用に以下のソフトウェアを調達すること。 ・ Microsoft SQL Server 2022 Standard	10
OS	本システムの Linux サーバ用に以下のソフトウェアを調達すること。 ・ Redhat Enterprise Linux Server (2 ゲスト OS 用)	1
CAL	本システムの Active Directory 環境用に以下のライセンスを調達すること。 ・ Windows Seerver Device CAL	2,020
CAL	本システムのアプリケーション仮想化システム用に以下のライセンスを調達すること。 ・ Windows Server 2022 Remote Desktop Service	2,020
サポート	本システムの Microsoft プロフェッショナルサポートに以下を調達すること。 ・ プロフェッショナルサポート 5 インシデントパック	6

4.15. Web コンテンツフィルタ

【想定機種：デジタルアーツ社製 i-Filter】 【数量：2,020 ユーザライセンス】

1. 物理環境、仮想環境上の Windows/Linux 64bit OS に対応していること。
2. フィルタリング URL データベースを 30 億コンテンツ以上有すること。
3. フィルタリング URL データベースがユーザ定義カテゴリ10 を含む 111 カテゴリに分類されており、カテゴリはユーザが任意に設定追加することができること。
4. フィルタリング URL データベースの配信は 1 日 3 回以上行われ、緊急性を要する場合、即時に反映させる緊急配信機能を有すること。
5. 出口対策用の情報には以下の内容が含まれていること。
 - ・世界中のハニーポットや独自の探索システムで収集した実際のマルウェア挙動に基づいた情報
 - ・国内の企業、官公庁、公共団体などで「実際に確認された」マルウェアによるアクセス先情報
 - ・国内 1,000 台以上の監視センサー(FW/UTM など)のログを元に相関分析された情報
 - ・専任のセキュリティアナリストによって分析精査された情報
6. Web サービス制御データベースは 2,000 件以上の Web サービス機能を登録しており、情報漏洩の観点で 5 段階に区別されたリスクレベルを有すること。
7. Web サービス制御データベースは、登録済み Web サービスの仕様が変更・追加・削除された場合も、それらの変更を随時反映させたものであること。
8. 直観的な日本語 GUI による容易なルール設定が可能であり、特殊な設定を実現するための ACL を利用したルール設定が、複数の設定画面で可能なこと。
9. フィルタリング URL データベースは閲覧規制時のアクションをカテゴリごとに「ブロック」「許可」「パスワード解除」「警告」「監視」のアクション設定が可能であること。
10. ユーザが画面上に任意の画像表示・URL リダイレクトの設定ができ、グループ、カテゴリ、URL を条件にしたブロック画面または警告画面表示が可能なこと。
11. Web サイトへのデータ送信(POST)規制は、「パスワード解除」「警告のみ」「監視」と設定が可能なこと。
12. 「基本設定」「企業」「公共」「小学校」「中学校」「高等学校・高専」等、メーカーが推奨する規制パターンがテンプレートとして複数用意されていること。
13. 開設されたばかりでデータベースに登録されていない有害サイトであっても、適切なフィルタリングが可能であること。

14. フィルタリング技術に関して国際特許を取得しているメーカー製品であること。
15. Web サービスにログイン後のページもカテゴリー判定が可能なこと。
16. 上位のプロキシサーバーを 15 台以上指定でき、各プロキシサーバーのアクティブ/スタンバイ設定、ラウンドロビンを含む任意の転送比率指定が行えること。
17. 仮想技術を用いずに最大 4 つまでのプロセスを起動させソフトウェア的に冗長化が可能で、1 台あたりの同時接続数上限は 40,000 であること。
18. HTTP、HTTPS、FTP over HTTP、Gopher、RTSP プロトコル全てに対応していること。
19. 本サーバーに繋がる外部・内部・管理画面・設定同期の全通信で IPv4/IPv6 を自動認識し IPv6 の利用が完全に可能なこと。
20. HTTP キャッシュ（ディスク/メモリキャッシュ）利用可否をホスト単位やグループ単位で設定ができ、複数台サーバーでのキャッシュ共有が可能なこと。
21. 動画コンテンツ（WMV、MOV、MP4、Flash 等）のプログレッシブダウンロードが可能であり、動画コンテンツ向けのキャッシュサーバーとして有効なこと。
22. 「入出力 IP アドレス」を管理 GUI 上から指定可能なこと。
23. Web サービスのみ SSL デコード対象とすることができ、あわせて、グループ等のルールパーツをデコード対象や対象除外の条件として設定可能なこと。
24. グループごとに所属している全ユーザの Web 利用時間制限、各ユーザの Web 利用時間確認と私的 Web 利用状況可視化ができ、全社またはグループごとに利用時間制限除外 URL・User-Agent 設定が可能なこと。
25. グループごとに任意有効期間（開始日/終了日の両方またはいずれか）を指定し、特定日以降フィルタリング開始とするグループ事前設定や、テンポラリなグループ作成時に活用可能であること。
26. ユーザ認証の除外条件として、URL、ホスト名、ホスト IP、クライアント IP、User-Agent、ACL の指定が可能なこと。
27. 管理者画面の「POST ログ」画面上から、添付ファイル復元を含む HTTP/HTTPS データの内容確認が可能であること。
28. 管理画面にて同時接続数の状態、及び、管理者毎に管理対象グループのカテゴリー毎アクセス件数、メーカーからの重要なお知らせが確認可能なこと。
29. 設定されたフィルタリングルールをボタン操作でグループごとに CSV や PDF に出力し、印刷可能なこと。
30. アクセスログの内容を解析、検索する、汎用 DB を利用しないレポーティングソフトがフィルタリングソフトに無償で付属されており、リスクの高い Web サービスを利用しているユーザ、送信量の多いユーザの確認が可能なこと。
31. アップロードされている YouTube 動画の URL を、その動画をアップロードしたユーザ単位でリストとして抽出しインポートし、YouTube 動画の閲覧制御を可能

とすること。

- 32. 日本国内で開発、販売されている製品であること。
- 33. 日本 PTA 全国協議会推薦の製品であること。
- 34. 2020 ユーザが利用できるライセンスを有していること。

4.16. 資産管理システム

【製品指定：Sky 社製 SKYSEA Client View 】

本システムを構成する上で、下記の保守サポートを調達すること。

項 目	機 能	数 量
保守サ ポート 等	●保守サポート 型式：SKYSEA000GLT13AHK4 製品名：SKYSEA Client View(GL)サーバ L 保守 4 年(協力)	1
	●保守サポート 型式：SKYSEA000GLT13AHK1 製品名：SKYSEA Client View(GL)サーバ L 保守 1 年(協力)	2
	●保守サポート 型式：SKYSEA000GLT13KHK4 製品名：SKYSEA Client View (GL) LT クライアント L(W/M/L) (1500-1999) 保守 4 年(協力)	1,650
	●保守サポート 型式：SKYSEA000GLT13KHK1 製品名：SKYSEA Client View (GL) LT クライアント L(W/M/L) (1500-1999) 保守 1 年(協力)	1,650
	●保守サポート 型式：SKYSEA000GOL01KHK4 製品名：SKYSEA Client View (GL) 申請・承認 クライアン ト L(1500-1999) 保守 4 年(協力)	1,650
	●保守サポート 型式：SKYSEA000GOL01KHK1 製品名：SKYSEA Client View (GL) 申請・承認 クライアン ト L(1500-1999) 保守 1 年(協力)	1,650

4.17. ウイルス対策システム

【想定機種:トレンドマイクロ社製 ウイルスバスターコーポレートエディション Plus】

【数量 : 2,020 ライセンス】

1. 一元管理、集中管理が可能であること。また、管理されないスタンドアロン運用も可能であること。
2. 未知のマルウェア対策として複数年以上の期間に世界規模のユーザから収集したソフトウェアの安全性（復旧度、定着度、安定性等）に関するレピュテーション情報から、安全と確認の取れない実行ファイルを検出する技術を有すること。
3. 世界規模で展開されたウイルス解析機関を有し、ウイルス定義ファイルを 1 日に最低 1 回以上更新することができること。
4. 感染で影響を受けたレジストリやファイルの自動修復機能が標準で利用できること。
5. 仮想マシンに対しても、物理マシンと同様、アンチウイルス、ファイアウォール、ネットワーク侵入防止機能により、マルウェアからの保護が可能であること。
6. クライアント管理をグループに分けて管理でき、定義ファイルやスキャン設定、通信間隔の設定をグループ毎に設定できること。また設定情報に関しては複数グループで共有できること。
7. ネットワーク接続がない端末に対して、アンチウイルスの定義ファイルを更新する機能があり、そのためのファイルなどが日々更新され、インターネットを通じて入手できること。
8. ウイルス感染してしまったクライアント PC に対して、改ざんされたレジストリや設定ファイルの復旧、及び起動しているウイルスのプロセスを停止する機能を有すること。また、それらのファイルを自動的に更新する機能を有すること。
9. パターンファイル（シグネチャベース）に加えて、機械学習（AI 技術）型の検索機能により、マルウェア実行前（ファイル検出）および実行後（挙動監視）の検出が可能なこと。
10. インターネットに接続できないオフライン環境において、機械学習（AI 技術）を用いたファイル検索を行うことができること。
11. クライアントに対するウイルス定義ファイルなどの配信時に、ネットワークに負荷をかけないように、差分パターンファイルの配信が可能なこと。
12. ウイルス定義ファイルなどの配信をクライアント中継できる機能を有すること。また、それらが管理サーバから簡単に設定管理可能なこと。
13. 管理画面およびマニュアルが日本語に対応していること。

5. 光幹線工事及び各種工事部材等仕様

5.1. フロア機器収納ボックス

【想定機種：日東工業製 THD34-6565-BF】

1. フロア機器収納ボックスの寸法は、設置環境、ネットワーク機器及び収容するケーブル本数を考慮した仕様・サイズとすること。
2. 19 インチ機器が取り付け可能であること。
3. 天面に開口部を有すること。
4. OA タップ、棚板等のオプションは含めること。

5.2. 光ファイバーケーブル

1. 光ファイバーケーブルの芯数は、別紙の「別紙_庁舎間光幹線必要芯数表」に記載の芯数とすること。
2. 各建屋間や本庁舎内で必要となるケーブル長とすること。
3. ネットワーク機器仕様及び付設距離に合わせたコア径の光ファイバーケーブルを使用すること。
4. 帯域 10Gbps を満たすものとすること。
5. 配線施工後は、要求される規格の試験を行うこと。

5.3. 光パッチコード

1. ネットワーク機器仕様及び付設距離に合わせたコア径の光ファイバーケーブルを使用すること。
2. 帯域 10Gbps を満たすものとすること。
3. ネットワーク機器等の接続に必要な数量を用意すること。

5.4. UTP ケーブル

1. 特に記載なき場合は、エンハンスドカテゴリ 6 規格相当の性能を持つ UTP ケーブルを使用すること。
2. TIA/EIA-568B 配線パターンとすること。
3. ケーブルは撚り線を使用すること。
4. RJ コネクタは、爪折れ防止対策が取られていること。（ブーツ取り付けによる爪折れ防止は不可）
5. 配線施工後は、要求される規格の試験を行うこと。

5.5. UTP パッチコード

1. 特に記載なき場合はエンハンスドカテゴリ 6 規格相当の性能を持つ UTP ケーブルを使用すること。
2. RJ45 コネクタは、爪折れ防止対策がとられていること。(ブーツ取り付けによる爪折れ防止は不可)
3. ネットワーク機器等の接続に必要なケーブル長及び数量を用意すること。
4. コードの両端に行き先を示すラベリングを行うこと。

5.6. UTP 情報コンセント

1. エンハンスドカテゴリ 6 規格相当の性能を持つこと。
2. 情報コンセントはシャッター付とすること。
3. 情報コンセントは行き先や用途に応じた名称を付けること。

5.7. 電源ケーブル

1. ケーブルは使用電圧及び電流を考慮した仕様とすること。
2. 必要に応じて、既設分電盤から電源配線作業を行うこと。なお、既設分電盤の空回路は市で準備することとし、必要な電圧及び電流は協議すること。
3. 電源コンセントは抜け止め対策が取られていること
4. 電源コンセントは取得した分電盤回路番号などの名称を付けること。
5. 配線施工後は、要求される規格の試験を行うこと。

5.8. PDU・OA タップ

1. PDU・OA タップは、使用電圧及び電流を考慮した仕様とすること。
2. PDU・OA タップへの電源ケーブルの接続は、抜け止め対策を行った上で接続すること。
3. PDU・OA タップの 1 本あたりのコンセント数量は機器台数に合わせた数量とすること。

6. データセンター ハウジング

6.1. ハウジング環境

本システムを設置するにあたり、本市が利用しているデータセンター事業者（株式会社松阪電子計算センター）からラック利用料等の見積を取得したうえで、本案件の費用に含めること。

【担当窓口】

株式会社松阪電子計算センター

吉田 匡章

0598-51-3588

m-yoshida@matsusaka.co.jp