

松阪市広域情報ネットワーク構築及び
運用・保守委託業務
機器仕様書

松 阪 市

目 次

1. 更新機器の調達	1
1.1. コアスイッチ	1
1.2. レイヤ3スイッチA	4
1.3. レイヤ3スイッチB	6
1.4. レイヤ3スイッチC	8
1.5. レイヤ2スイッチA	9
1.6. レイヤ2スイッチB	12
1.7. PoE 対応レイヤ2スイッチ	16
1.8. アクセスレイヤ2スイッチ	18
1.9. インターネット接続用ルータ	20
1.10. WAN 回線負荷分散装置	22
1.11. 外局収容ルータ	23
1.12. 外局接続用ルータ	24
1.13. 無線 LAN コントローラ	26
1.14. 無線 LAN アクセスポイント	28
1.15. 無線 LAN 管理サーバー	30
1.16. 無線 LAN ロケーション管理サーバー	31
1.17. 無線 LAN アダプタ	32
1.18. ネットワーク認証サーバー	32
1.19. 基幹ファイアウォール	34
1.20. ファイアウォールA	36
1.21. ファイアウォールB	38
1.22. AD 兼 DHCP サーバー	42
1.23. WEB コンテンツフィルタサーバ	43
1.24. 資産管理システム	45
1.25. ウィルス対策管理サーバー	47
2. 工事部材等仕様	47
2.1. サーバラック	47
2.2. コード集合型光ファイバーケーブル	48
2.3. 光パッチコード	48
2.4. UTP ケーブル	49
2.5. UTP パッチコード	49
2.6. UTP 情報コンセント	49

2.7. 電源ケーブル.....	49
------------------	----

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導入する場合は別途定める用紙に変更する理由と要件を満たすことを示し、市の承認を得ること。

1.1. コアスイッチ

想定機種

シスコシステムズ社製 Cisco C6880-X-LE

1. ハードウェアとして、単体で 2Tbps 以上のスイッチファブリックを搭載していること。
2. 複数のスイッチを 1 つの仮想スイッチとしてクラスタ化しシステムの帯域幅容量を 4 Tbps まで拡張できること。
3. 当該スイッチは、下位装置として接続するスイッチを同じシャーシ内のラインカードと同様に扱うことが可能なアーキテクチャであること。
4. インターフェースモジュールが 4 モジュール以上搭載可能であること。
5. 10Gbps 以上が提供可能なインターフェースが取り外し可能なモジュールで 64 ポート以上有すること。
6. 本システムを構築する上で必要となる光コネクタモジュール・銅コネクタモジュール等 (SFP、SFP+) は必要数量を搭載しておくこと。
7. IEEE802.1Q VLAN Tagging に準拠していること。
8. IEEE802.1D に準拠したスパニングツリー機能を有すること。
9. 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。
10. 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。
11. IEEE802.1X に準拠した認証機能を有すること。
12. IEEE 802.3ad Link Aggregation 機能を有すること。
13. マルチシャーシ・イーサチャネル (シャーシをまたがって、複数の Ethernet ポートを束ねて 1 つの高速ポートとして利用可能な機能) をサポートすること。
14. IP ルーティング・プロトコルとして、Static、RIP、OSPF、EIGRP をサポートしていること。
15. ポリシーベースルーティング機能を有すること。
16. IPv6 ルーティングとして、Static Routing、RIPng、OSPFv3、EIGRPv6 をサポートしていること。
17. IP マルチキャストルーティングプロトコルとして、PIM-SparseMode、

PIM-DenseMode、PIM sparse-dense mode、Source Specific Multicast に対応していること。

18. 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。
19. ポートを束ねて、1つの高速ポートとして利用する機能を有すること。また、動的にポートを束ねるネゴシエーションプロトコルに対応していること。
20. ゲートウェイ冗長プロトコルに対応していること。
21. ループ防止機能としてスパニングツリープロトコル以外で Flex Link 機能を有していること。
22. 複数のルーティングテーブルを保有することができ、お互いのルーティング間で通信ができない様な閉域ネットワークを構成することができること。
23. IGMP Filtering、IPv4 IGMP snooping および IPv6 MLDv1/v2 snooping 機能を有すること。
24. IEEE802.1p の CoS および DSCP に基づきトラフィックの優先制御に対応していること。
25. IEEE802.1p の CoS および DSCP のマーキングおよび再分類に対応していること。
26. WRR アルゴリズムにてパケット優先制御が可能であること。
27. WRED アルゴリズムにより輻輳回避が可能であること。
28. IPv6 ハードウェアルーティングに対応していること。
29. 4096 個以上の VLAN をサポートしていること。尚、VLAN ID は、4094 まで利用可能であること。
30. 256,000 以上の IPv4 ユニキャスト経路をサポートできること。
31. 128,000 以上の IPv6 ユニキャスト経路をサポートできること。
32. ハードウェアとして 128,000 以上の MAC アドレスに対応可能であること。
33. 9216 バイト以上のジャンボフレームに対応していること。
34. IEEE802.1ae に準拠した MACsec 機能を有すること。
35. SFP インターフェースは、1000BASE-SX/LH/ZX に対応可能であること。
36. SFP+インターフェースは 10GBASE-LR、SR、LRM、ER に対応可能であること。
37. BPDU の受信時にスパニングツリーPortFast 対応インターフェー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。
38. ネットワーク管理者の制御下でないエッジ 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。
39. 光ファイバやツイストペアケーブルの単方向リンク（片対障害）検出機能を有すること。
40. MAC アドレスに基づいてアクセスまたはトランクポートへのアクセスを保護し、

学習される MAC アドレスの数を制限する機能を有すること。

41. 悪意のあるユーザーが ARP プロトコルのセキュリティの弱点を悪用するのを阻止し、ユーザーの整合性を保証する機能を有すること。
42. 同一 VLAN 内トラフィックに対してアクセスリストを用いたアクセス制限に対応可能なこと。
43. 送信元/受信元 MAC アドレス/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. ルーティングされないレイヤ 2 インターフェース上の IP トラフィックを制限するセキュリティ機能を有すること。
45. ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
46. 不正な IPv6 RA (Router Advertisement) を廃棄する機能を保有すること
47. 未学習の MAC アドレスを送信先とするパケットを転送せず廃棄する機能に加え、任意の転送レートに抑制する機能を有すること。
48. DoS 攻撃による CPU への影響を防ぐ機能を有すること。
49. RADIUS サーバーと連携することにより、下位スイッチを IEEE802.1X を用いて認証する機能を有すること。かつ、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。
50. IEEE802.1X に準拠し、動的なポートの利用の可否を決定する機能を有すること。
51. IEEE802.1X ユーザー認証時に、認証サーバーに登録された VLAN を動的に割り振る機能を有すること。
52. 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。
53. 2 台のスイッチを 1 台の仮想スイッチとして管理できることで管理オーバーヘッドを半減できること。
54. 仮想スイッチを構成した場合、ソフトウェアアップグレードを行う際に、ダウンタイムを最小限に抑える機能を有すること
55. シリアル接続によるコンソールポートを有すること。
56. Telnet/SSH によるリモートコンソール機能を有すること。
57. トラフィック解析のためのポートのミラーリング機能を有すること。また、レイヤ 2 およびレイヤ 3 ネットワークをまたがりリモート・ミラーリングする機能もサポートすること。
58. 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。
59. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
60. Syslog サーバーにメッセージを送信する機能を有すること。

61. SNMPv1/v2c/v3 による管理機能を有すること。
62. RMON を使った管理機能を有すること。
63. UTP ケーブル障害時に、障害原因、断線部分までの距離等の状況を検知し、管理コンソール上で情報を確認できる機能を有すること。
64. 接続した光ケーブルに対する品質診断機能を有すること。
65. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
66. L3 スイッチ機能で、DHCP Relay 機能を有すること。
67. 簡易的なパケットキャプチャ可能な機能を有すること。
68. シスログ出力などの対象となるイベントが発生した際に、そのイベントと関連づけたアクションを起こすことが可能であること。
69. 複数の LAN スイッチ間で、VLAN 情報を一元管理するためのプロトコルを実装していること。
70. VCCI クラス A に準拠していること。
71. 動作温度が 0℃～40℃に対応していること。
72. 保管温度が－20℃～65℃に対応していること。
73. 動作相対湿度は 5%～90%（結露しないこと）に対応していること。
74. ノイズ源からの影響を受ける可能性が高いため、CE マークを取得していること。
75. 同一筐体内で電源の二重化機能を有すること。
76. 起動時、稼動中など、任意のタイミングで実行できる総合的な自己診断機能を有すること。
77. 19 インチラックに格納できること。
78. 5 U 以内のラックアマウント型の形状であること。

1.2. レイヤ 3 スイッチ A

想定機種

シスコシステムズ社製 Cisco WS-C3850-12S-E

1. スイッチング容量 68Gbps 以上有すること。
2. スタック構成で 480 Gbps 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 スイッチオーバー（SSO）をサポートすること。
4. スタック内での電源共有が可能な機能を有していること。
5. 2 つのモジュール型電源および 3 つのモジュール型ファンによる冗長性を有すること。

6. モジュラー型の QoS 機能を有し最大 2 Priority 6 Queues 3 Thresh hold のキューモデルをサポートすること
7. 1Gbps 以上が提供可能なインターフェースが 12 ポート以上有すること。
本システムを構築する上で必要となる光コネクタモジュール・銅コネクタモジュール等 (SFP) は必要数量を搭載しておくこと。
8. マルチシャード・イーサチャネル (シャードをまたがって、複数の Ethernet ポートを束ねて 1 つの高速ポートとして利用可能な機能) をサポートすること。
9. 4000 個以上の VLAN をサポートしていること。
10. Gigabit Ethernet ポートを束ねて、1 つの高速ポートとして利用する機能を有すること。また、動的にポートを束ねるネゴシエーションプロトコルに対応していること。
11. IP ルーティング・プロトコルとして、Static、RIP、OSPF、EIGRP をサポートしていること。
12. IPv6 ルーティングとして、Static Routing、RIPng、OSPFv3、EIGRPv6 をサポートしていること。
13. IP マルチキャストルーティングプロトコルとして、PIM-SparseMode、PIM-DenseMode、PIM sparse-dense mode、Source Specific Multicast に対応していること。
14. ポリシーベースルーティング機能を有すること。
15. 24,000 以上の IPv4 ユニキャスト経路をサポートできること。
16. ゲートウェイ冗長プロトコルに対応していること。
17. シリアル接続によるコンソールポートを有すること。
18. Telnet/SSH によるリモートコンソール機能を有すること。
19. トラフィック解析のためのポートのミラーリング機能を有すること。
20. 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。
21. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
22. Syslog サーバーにメッセージを送信する機能を有すること。
23. SNMPv1/v2c/v3 による管理機能を有すること。
24. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
25. L3 スイッチ機能で、DHCP Relay 機能を有すること。
26. IEEE802.1Q VLAN Tagging に準拠していること。
27. IEEE802.1D に準拠したスパニングツリー機能を有すること。
28. 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。
29. 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。
30. IEEE802.1x に準拠した認証機能を有すること。

31. IEEE 802.3ad Link Aggregation 機能を有すること。
32. IEEE802.1p の優先制御機能を有すること。
33. VCCI クラス A に準拠していること。
34. 動作温度が-5℃～45℃に対応していること。
35. 保管温度が-40℃～70℃に対応していること。
36. 動作相対湿度は 5%～90%（結露しないこと）に対応していること。
37. ノイズ源からの影響を受ける可能性が高いため、CE マークを取得していること。
38. 同一筐体内で電源の二重化機能を有すること。
39. 19 インチラックに格納できること。
40. 1 U 以内のラックアマウント型の形状であること。

1.3. レイヤ 3 スイッチ B

想定機種

シスコシステムズ社製 Cisco WS-C3850-24P-S

1. スイッチング容量 92 Gbps 以上有すること。
2. スタック構成で 480 Gbps 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 スイッチオーバー (SSO) をサポートすること。
4. スタック内での電源共有が可能な機能を有していること。
5. 2 つのモジュール型電源および 3 つのモジュール型ファンによる冗長性を有すること。
6. モジュラー型の QoS 機能を有し最大 2 Priority 6 Queues 3 Thresh hold のキューモデルをサポートすること
7. 1Gbps 以上が提供可能なインターフェースが 24 ポート以上有すること。
8. 本システムを構築する上で必要となる光コネクタモジュール・銅コネクタモジュール等 (SFP) は必要数量を搭載しておくこと。
9. マルチシャシ・イーサチャネル (シャシをまたがって、複数の Ethernet ポートを束ねて 1 つの高速ポートとして利用可能な機能) をサポートすること。
10. 4000 個以上の VLAN をサポートしていること。
11. Gigabit Ethernet ポートを束ねて、1 つの高速ポートとして利用する機能を有すること。また、動的にポートを束ねるネゴシエーションプロトコルに対応していること。
12. IP ルーティング・プロトコルとして、Static、RIP、OSPF、EIGRP をサポート

していること。

13. IPv6 ルーティングとして、Static Routing、RIPng、OSPFv3、EIGRPv6 をサポートしていること。
14. IP マルチキャストルーティングプロトコルとして、PIM-SparseMode、PIM-DenseMode、PIM sparse-dense mode、Source Specific Multicast に対応していること。
15. ポリシーベースルーティング機能を有すること。
16. 24,000 以上の IPv4 ユニキャスト経路をサポートできること。
17. ゲートウェイ冗長プロトコルに対応していること。
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. トラフィック解析のためのポートのミラーリング機能を有すること。
21. 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。
22. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
23. Syslog サーバーにメッセージを送信する機能を有すること。
24. SNMPv1/v2c/v3 による管理機能を有すること。
25. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
26. L3 スイッチ機能で、DHCP Relay 機能を有すること。
27. IEEE802.1Q VLAN Tagging に準拠していること。
28. IEEE802.1D に準拠したスパニングツリー機能を有すること。
29. 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。
30. 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。
31. IEEE802.1x に準拠した認証機能を有すること。
32. IEEE 802.3ad Link Aggregation 機能を有すること。
33. IEEE802.1p の優先制御機能を有すること。
34. VCCI クラス A に準拠していること。
35. 動作温度が-5℃～45℃に対応していること。
36. 保管温度が-40℃～70℃に対応していること。
37. 動作相対湿度は 5%～90%（結露しないこと）に対応していること。
38. ノイズ源からの影響を受ける可能性が高いため、CE マークを取得していること。
39. 同一筐体内で電源の二重化機能を有すること。
40. 19 インチラックに格納できること。
41. 1 U以内のラックアマウント型の形状であること。

1.4. レイヤ 3 スイッチ C

想定機種

シスコシステムズ社製 Cisco WS-C3850-24T-S

1. スイッチング容量 92 Gbps 以上有すること。
2. スタック構成で 480 Gbps 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 スイッチオーバー (SSO) をサポートすること。
4. スタック内での電源共有が可能な機能を有していること。
5. 2つのモジュール型電源および 3つのモジュール型ファンによる冗長性を有すること。
6. モジュラー型の QoS 機能を有し最大 2 Priority 6 Queues 3 Thresh hold のキューモデルをサポートすること
7. 1Gbps 以上が提供可能なインターフェースが 24 ポート以上有すること。
8. 10Gbps 以上が提供可能なインターフェースが 4 ポート以上有すること。
9. 本システムを構築する上で必要となる光コネクタモジュール・カップーコネクタモジュール等 (SFP、SFP+) は必要数量を搭載しておくこと。
10. マルチシャーシ・イーサチャネル (シャーシをまたがって、複数の Ethernet ポートを束ねて 1つの高速ポートとして利用可能な機能)をサポートすること。
11. 4000 個以上の VLAN をサポートしていること。
12. Gigabit Ethernet ポートを束ねて、1つの高速ポートとして利用する機能を有すること。また、動的にポートを束ねるネゴシエーションプロトコルに対応していること。
13. IP ルーティング・プロトコルとして、Static、RIP、OSPF、EIGRP をサポートしていること。
14. IPv6 ルーティングとして、Static Routing、RIPng、OSPFv3、EIGRPv6 をサポートしていること。
15. IP マルチキャストルーティングプロトコルとして、PIM-SparseMode、PIM-DenseMode、PIM sparse-dense mode、Source Specific Multicast に対応していること。
16. ポリシーベースルーティング機能を有すること。
17. 24,000 以上の IPv4 ユニキャスト経路をサポートできること。
18. ゲートウェイ冗長プロトコルに対応していること。
19. シリアル接続によるコンソールポートを有すること。
20. Telnet/SSH によるリモートコンソール機能を有すること。
21. トラフィック解析のためのポートのミラーリング機能を有すること。

22. 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。
23. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
24. Syslog サーバーにメッセージを送信する機能を有すること。
25. SNMPv1/v2c/v3 による管理機能を有すること。
26. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
27. L3 スイッチ機能で、DHCP Relay 機能を有すること。
28. IEEE802.1Q VLAN Tagging に準拠していること。
29. IEEE802.1D に準拠したスパニングツリー機能を有すること。
30. 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。
31. 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。
32. IEEE802.1x に準拠した認証機能を有すること。
33. IEEE 802.3ad Link Aggregation 機能を有すること。
34. IEEE802.1p の優先制御機能を有すること。
35. VCCI クラス A に準拠していること。
36. 動作温度が-5℃～45℃に対応していること。
37. 保管温度が-40℃～70℃に対応していること。
38. 動作相対湿度は 5%～90%（結露しないこと）に対応していること。
39. ノイズ源からの影響を受ける可能性が高いため、CE マークを取得していること。
40. 同一筐体内で電源の二重化機能を有すること。
41. 19 インチラックに格納できること。
42. 1 U 以内のラックアマウント型の形状であること。

1.5. レイヤ 2 スイッチ A

想定機種

シスコシステムズ社製 Cisco WS-C2960X-24TD-L

1. 95Mpps 以上の転送パフォーマンスを実装すること。
2. 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。
3. 10 ギガビットイーサネット SFP+を 2 ポート以上実装していること。
4. IEEE802.1Q VLAN Tagging 機能を有すること。
5. IEEE802.1D に準拠したスパニングツリー機能を有すること。
6. 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。

7. 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。
8. IEEE 802.3ad Link Aggregation 機能を有すること。
9. 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。
10. 1000 個以上の VLAN に対応していること。尚、VLAN ID は 4000 以上を利用可能であること。
11. 9,216 バイト以上のジャンボフレームに対応していること。
12. ループ防止機能としてスパンニングツリープロトコル以外の機能を有し、切り替わり際には 100ms 以内で切り替わりが可能なこと。
13. IPv4 IGMPv1, v2, v3 Snooping に対応していること。
14. IPv6 MLDv1, v2 Snooping に対応していること。
15. IPv4 プロトコルによる ping、traceroute、Telnet、SSH 機能を有すること。
16. SFP+インターフェースは 10GBASE-LR、SR、LRM、CU、ACU、AOC に対応可能であること。
17. 専用のスタックポートを有し、最大 8 台までのスイッチを論理的に 1 台とするスタック接続機能を有すること。
18. 複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーションを構成可能なこと。
19. すべてのスイッチ・ポートで半二重、全二重伝送モードが自動的に選択され、帯域幅を最適化する機能を有すること。
20. ポートに接続されたケーブルのタイプ（クロスまたはストレート）が不適切な場合は、送受信ペアが自動的に調整される機能を有すること。
21. VLAN トランッキング・プロトコル機能を有すること。
22. VLAN 単位のスパンニングツリー・ベースでスパンニングツリーを高速に再コンバージェンスする機能を有すること。
23. IEEE802.1p の CoS による優先制御機能を有すること。
24. 1 ポートあたり 4 つの出力キューに対応していること。
25. Shaped Round Robin スケジューリング機能を有すること。
26. Weighted Tail Drop アルゴリズムによる輻輳回避機能を有すること。
27. スwitchをスタック構成時にスタック全体に提供される QoS を設定できる Cross-Stack QoS 機能を有すること。
28. パスワードおよび特権レベルの設定により、不正なユーザーがスイッチの構成を変更することを阻止できる機能を有すること。
29. BPDU の受信時にスパンニングツリーPortFast 対応インターフェー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。

30. 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。
31. ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること
32. IEEE802.1x に準拠した認証機能を有すること。
33. Port ACL 機能を有すること。
34. VLAN ACL 機能を有すること。
35. 送信元/受信元 MAC アドレスに基づくパケットフィルタを行う機能を有すること。
36. 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。
37. RADIUS サーバーと連携することにより、下位スイッチを IEEE802.1x を用いて認証する機能を有すること。かつ、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. 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。
39. IEEE802.1x ユーザー認証時に、認証サーバーに登録された VLAN を動的に割り振る機能を有すること。
40. マルチドメイン認証機能を有すること。
41. IEEE802.1x マルチプル認証モード機能を有すること。
42. TACACS+によるユーザー認証機能を有すること。
43. シリアル接続によるコンソールポートを有すること。
44. Telnet/SSH によるリモートコンソール機能を有すること。
45. 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すること。
46. 同一筐体内のみならず、他の筐体のポートもミラーリング機能も有すること。
47. 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。
48. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有することと。
49. Syslog サーバーにメッセージを送信する機能を有すること。
50. SNMPv1/v2c/v3 による管理機能を有すること。
51. RMON を使った管理機能を有すること。
52. 管理用の RADIUS ユーザー認証機能を有し、管理者以外が設定情報を参照、変更できないような機能を有すること。
53. 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。
54. 他のスイッチにて、OS イメージおよび設定ファイルを管理可能なこと。

55. UTP ポートにてケーブル診断(Time-domain reflectometer)機能を有すること。
56. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
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. 起動時、稼動中、トラブルシューティングなど、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。
59. スタックモジュールはホットスワップに対応していること。
60. VCCI クラス A に準拠していること。
61. 動作温度が-5℃～45℃に対応していること。
62. 保管温度が-25℃～70℃に対応していること。
63. 動作相対湿度は 10%～95%（結露しないこと）に対応していること。
64. 19 インチラックに格納できること。
65. 1 U 以内のラックアマウント型の形状であること。

1.6. レイヤ 2 スイッチ B

想定機種

シスコシステムズ社製 Cisco WS-C2960X-24TS-L

1. 71Mpps 以上の転送パフォーマンスを実装すること。
2. 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。
3. 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。
4. IEEE802.1Q VLAN Tagging 機能を有すること。
5. IEEE802.1D に準拠したスパニングツリー機能を有すること。
6. 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。
7. 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。
8. IEEE 802.3ad Link Aggregation 機能を有すること。
9. 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。
10. 1000 個以上の VLAN に対応していること。尚、VLAN ID は 4000 以上を利用可能であること。
11. 9,216 バイト以上のジャンボフレームに対応していること。
12. ループ防止機能としてスパニングツリープロトコル以外の機能を有し、切り替わりの際には 100ms 以内で切り替わりが可能なこと。

13. IPv4 IGMPv1, v2, v3 Snooping に対応していること。
14. IPv6 MLDv1, v2 Snooping に対応していること。
15. IPv4 プロトコルによる ping、traceroute、Telnet、SSH 機能を有すること。
16. SFP インターフェースは 1000BASE-T、SX、LX/LH、ZX、100BASE-LX/BX/FX、CWDM に対応可能であること。
17. 専用のスタックポートを有し、最大 8 台までのスイッチを論理的に 1 台とするスタック接続機能を有すること。
18. 複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーションを構成可能なこと。
19. すべてのスイッチ・ポートで半二重、全二重伝送モードが自動的に選択され、帯域幅を最適化する機能を有すること。
20. ポートに接続されたケーブルのタイプ（クロスまたはストレート）が不適切な場合は、送受信ペアが自動的に調整される機能を有すること。
21. VLAN トランッキング・プロトコル機能を有すること。
22. VLAN 単位のスパニングツリー・ベースでスパニングツリーを高速に再コンバージェンスする機能を有すること。
23. IEEE802.1p の CoS による優先制御機能を有すること。
24. 1 ポートあたり 4 つの出力キューに対応していること。
25. Shaped Round Robin スケジューリング機能を有すること。
26. Weighted Tail Drop アルゴリズムによる輻輳回避機能を有すること。
27. スwitchをスタック構成時にスタック全体に提供される QoS を設定できる Cross-Stack QoS 機能を有すること。
28. パスワードおよび特権レベルの設定により、不正なユーザーがスイッチの構成を変更することを阻止できる機能を有すること。
29. BPDU の受信時にスパニングツリーPortFast 対応インターフェー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。
30. 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。
31. ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること。
32. IEEE802.1x に準拠した認証機能を有すること。
33. Port ACL 機能を有すること。
34. VLAN ACL 機能を有すること。
35. 送信元/受信元 MAC アドレスに基づくパケットフィルタを行う機能を有すること。
36. 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。

37. RADIUS サーバーと連携することにより、下位スイッチを IEEE802.1x を用いて認証する機能を有すること。かつ、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. 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。
39. IEEE802.1x ユーザー認証時に、認証サーバーに登録された VLAN を動的に割り振る機能を有すること。
40. マルチドメイン認証機能を有すること。
41. IEEE802.1x マルチプル認証モード機能を有すること。
42. TACACS+によるユーザー認証機能を有すること。
43. シリアル接続によるコンソールポートを有すること。
44. Telnet/SSH によるリモートコンソール機能を有すること。
45. 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すること。
46. 同一筐体内のみならず、他の筐体のポートもミラーリング機能も有すること。
47. 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。
48. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
49. Syslog サーバーにメッセージを送信する機能を有すること。
50. SNMPv1/v2c/v3 による管理機能を有すること。
51. RMON を使った管理機能を有すること。
52. 管理用の RADIUS ユーザー認証機能を有し、管理者以外が設定情報を参照、変更できないような機能を有すること。
53. 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。
54. 他のスイッチにて、OS イメージおよび設定ファイルを管理可能なこと。
55. UTP ポートにてケーブル診断(Time-domain reflectometer)機能を有すること。
56. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
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. 起動時、稼動中、トラブルシューティングなど、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。
59. スタックモジュールはホットスワップに対応していること。
60. VCCI クラス A に準拠していること。
61. 動作温度が-5℃～45℃に対応していること。
62. 保管温度が-25℃～70℃に対応していること。

- 63. 動作相対湿度は 10%～95%（結露しないこと）に対応していること。
- 64. 19 インチラックに格納できること。
- 65. 1 U以内のラックアマウント型の形状であること。

1.7. 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 Cisco WS-C2960X-24PS-L

1. 71Mpps 以上の転送パフォーマンスを実装すること。
2. 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。
3. 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。
4. 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。
5. IEEE802.1Q 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. IEEE 802.3ad Link Aggregation 機能を有すること。
10. 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。
11. 1000 個以上の VLAN に対応していること。尚、VLAN ID は 4000 以上を利用可能であること。
12. 9,216 バイト以上のジャンボフレームに対応していること。
13. ループ防止機能としてスパニングツリープロトコル以外の機能を有し、切り替わりの際には 100ms 以内で切り替わりが可能なこと。
14. IPv4 IGMPv1, v2, v3 Snooping に対応していること。
15. IPv6 MLDv1, v2 Snooping に対応していること。
16. IPv4 プロトコルによる ping、traceroute、Telnet、SSH 機能を有すること。
17. SFP インターフェースは 1000BASE-T、SX、LX/LH、ZX、100BASE-LX/BX/FX、CWDM に対応可能であること。
18. 専用のスタックポートを有し、最大 8 台までのスイッチを論理的に 1 台とするスタック接続機能を有すること。
19. 複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーションを構成可能なこと。
20. すべてのスイッチ・ポートで半二重、全二重伝送モードが自動的に選択され、帯域幅を最適化する機能を有すること。
21. ポートに接続されたケーブルのタイプ（クロスまたはストレート）が不適切な

場合は、送受信ペアが自動的に調整される機能を有すること。

22. VLAN トランッキング・プロトコル機能を有すること。
23. VLAN 単位のスパニングツリー・ベースでスパニングツリーを高速に再コンバージェンスする機能を有すること。
24. IEEE802.1p の CoS による優先制御機能を有すること。
25. 1 ポートあたり 4 つの出力キューに対応していること。
26. Shaped Round Robin スケジューリング機能を有すること。
27. Weighted Tail Drop アルゴリズムによる輻輳回避機能を有すること。
28. スイッチをスタック構成時にスタック全体に提供される QoS を設定できる Cross-Stack QoS 機能を有すること。
29. パスワードおよび特権レベルの設定により、不正なユーザーがスイッチの構成を変更することを阻止できる機能を有すること。
30. BPDU の受信時にスパニングツリーPortFast 対応インターフェー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. 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。
32. ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること
33. IEEE802.1x に準拠した認証機能を有すること。
34. Port ACL 機能を有すること。
35. VLAN ACL 機能を有すること。
36. 送信元/受信元 MAC アドレスに基づくパケットフィルタを行う機能を有すること。
37. 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。
38. RADIUS サーバーと連携することにより、下位スイッチを IEEE802.1x を用いて認証する機能を有すること。かつ、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。
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 ユーザー認証時に、認証サーバーに登録された VLAN を動的に割り振る機能を有すること。
41. マルチドメイン認証機能を有すること。
42. IEEE802.1x マルチプル認証モード機能を有すること。
43. TACACS+によるユーザー認証機能を有すること。
44. シリアル接続によるコンソールポートを有すること。
45. Telnet/SSH によるリモートコンソール機能を有すること。

46. 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すること。
47. 同一筐体内のみならず、他の筐体のポートもミラーリング機能も有すること。
48. 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。
49. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
50. Syslog サーバーにメッセージを送信する機能を有すること。
51. SNMPv1/v2c/v3 による管理機能を有すること。
52. RMON を使った管理機能を有すること。
53. 管理用の RADIUS ユーザー認証機能を有し、管理者以外が設定情報を参照、変更できないような機能を有すること。
54. 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。
55. 他のスイッチにて、OS イメージおよび設定ファイルを管理可能なこと。
56. UTP ポートにてケーブル診断 (Time-domain reflectometer) 機能を有すること。
57. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
58. 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。
59. 起動時、稼動中、トラブルシューティングなど、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. スタックモジュールはホットスワップに対応していること。
61. VCCI クラス A に準拠していること。
62. 動作温度が -5°C \sim 45°C に対応していること。
63. 保管温度が -25°C \sim 70°C に対応していること。
64. 動作相対湿度は 10% \sim 95% (結露しないこと) に対応していること。
65. 19 インチラックに格納できること。
66. 1 U 以内のラックアマウント型の形状であること。

1.8. 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 Cisco WS-C2960C-8TC-L

1. 10Gbps 以上の転送帯域幅を有すること。
2. 10/100 イーサネットポートを 8 ポート以上実装していること。

3. 1 ギガビットイーサネット SFP または銅ポートを 2 ポート以上実装していること。
4. IEEE802.1Q VLAN Tagging 機能を有すること。
5. IEEE802.1D に準拠したスパニングツリー機能を有すること。
6. 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。
7. 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。
8. IEEE 802.3ad Link Aggregation 機能を有すること。
9. 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。
10. 250 個以上の VLAN に対応していること。尚、VLAN ID は 4000 以上を利用可能であること。
11. 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。
12. IPv4 IGMPv1, v2, v3 Snooping に対応していること。
13. IPv6 MLDv1, v2 Snooping に対応していること。
14. IPv4 プロトコルによる ping、traceroute、Telnet 機能を有すること。
15. SFP インターフェースは 1000BASE-SX、LX/LH、ZX に対応可能であること。
16. すべてのスイッチ・ポートで半二重、全二重伝送モードが自動的に選択され、帯域幅を最適化する機能を有すること。
17. ポートに接続されたケーブルのタイプ（クロスまたはストレート）が不適切な場合は、送受信ペアが自動的に調整される機能を有すること。
18. VLAN トランッキング・プロトコル機能を有すること。
19. VLAN 単位のスパニングツリー・ベースでスパニングツリーを高速に再コンバージェンスする機能を有すること。
20. IEEE802.1p の CoS による優先制御機能を有すること。
21. パスワードおよび特権レベルの設定により、不正なユーザーがスイッチの構成を変更することを阻止できる機能を有すること。
22. BPDU の受信時にスパニングツリーPortFast 対応インターフェー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。
23. 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。
24. ポート単位のブロードキャスト、マルチキャスト、およびユニキャストのストーム制御機能を有すること
25. IEEE802.1x に準拠した認証機能を有すること。
26. RADIUS サーバーと連携することにより、下位スイッチを IEEE802.1x を用いて認証する機能を有すること。

27. 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。
28. IEEE802.1x ユーザー認証時に、認証サーバーに登録された VLAN を動的に割り振る機能を有すること。
29. マルチドメイン認証機能を有すること。
30. IEEE802.1x マルチプル認証モード機能を有すること。
31. TACACS+によるユーザー認証機能を有すること。
32. シリアル接続によるコンソールポートを有すること。
33. Telnet/SSH によるリモートコンソール機能を有すること。
34. 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すること。
35. 同一筐体内のみならず、他の筐体のポートもミラーリング機能も有すること。
36. 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。
37. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
38. Syslog サーバーにメッセージを送信する機能を有すること。
39. SNMPv1/v2c/v3 による管理機能を有すること。
40. RMON を使った管理機能を有すること。
41. 管理用の RADIUS ユーザー認証機能を有し、管理者以外が設定情報を参照、変更できないような機能を有すること。
42. 他のスイッチにて、OS イメージおよび設定ファイルを管理可能なこと。
43. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
44. 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。
45. 起動時、稼動中、トラブルシューティングなど、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。
46. VCCI クラス A に準拠していること。
47. 動作温度が-5℃～45℃に対応していること。
48. 保管温度が-25℃～70℃に対応していること。
49. 動作相対湿度は 5%～95%（結露しないこと）に対応していること。

1.9. インターネット接続用ルータ

想定機種

シスコシステムズ社製 Cisco CISC02921/K9

1. IPv4 および IPv6 のルーティング可能なルータ製品であること。
2. IPv4 ルーティングとして、Static、RIP、OSPF、EIGRP のルーティング・プロトコルをサポートすること。
3. IPv6 ルーティングとして、Static、RIPng、OSPFv3、EIGRPv6 のルーティング・プロトコルをサポートすること。
4. ポリシーベースルーティング機能を有すること。
5. IP マルチキャストルーティングプロトコルとして、PIM-SparseMode、Source Specific Multicast に対応していること。
6. PPPoE に対応していること。
7. 256MB 以上の Flash を搭載していること。
8. 512MB 以上の ECC 付き DDR-SDRAM をメインメモリとして使用できること。
9. DSCP に基づきトラフィックの優先制御に対応していること。
10. 2 つ以上の 10/100/1000Base-T ポートを有すること。
11. 1 つ以上の 1000BaseX ポートポートを有すること。
12. モジュールの追加でポートの増設が可能になること。
13. 転送容量は 245.76Mbps 以上であること。
14. 転送能力は 480,000pps 以上であること。
15. 固定 USB ポートを 2 つ以上有すること。
16. Telnet/SSH によるリモートコンソール機能を有すること。
17. 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。
18. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
19. Syslog サーバーにメッセージを送信する機能を有すること。
20. DNS を参照し IP アドレスの代わりにホスト名を使用できる機能を有すること。
21. SNMPv1/v2c/v3 による管理機能を有すること。
22. RMON を使った管理機能を有すること。
23. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
24. IP アプリケーションに対するサービスレベルを測定する機能をサポートすること。
25. シスログ出力などの対象となるイベントが発生した際に、そのイベントと関連づけたアクションを起こすことが可能であること。
26. 起動時、稼動中など、任意のタイミングで実行できる総合的な自己診断機能を有すること。
27. 動作温度が 0℃～40℃に対応していること。
28. 保管温度が-40℃～70℃に対応していること。
29. 動作相対湿度は 10%～85%に対応していること。

30. VCCI クラス A に準拠していること。
31. 100BaseTX インターフェースが、IEEE 802.3u に準拠していること。
32. 1000Base-X インターフェースが、IEEE 802.3z に準拠していること。
33. 1000Base-T インターフェースが、IEEE 802.3ab に準拠していること。
34. 19 インチラックマウント可能であること。

1.10. WAN 回線負荷分散装置

想定機種

F5 社製 BIG-IP 2000s

1. ハードウェアとソフトウェアが一体となったアプライアンス機器の WAN 回線負荷分散装置であること。
2. 1Gigabit の RJ45 ポートを 8 ポート以上有すること。
3. 電源の冗長化をすること。
4. データペイロードにおけるコンテンツのどの部分においてもコンテンツの書き換えが可能であること。
5. WAN 回線のヘルスチェック方法として、ヘルスチェック先を IP アドレス又は FQDN で指定可能であること。
6. トラフィックの種類を、送信元/送信先 IP アドレスや宛先 TCP/UDP ポート番号でグループ分けし、グループ毎に宛先回線の指定が可能であること。グループに該当しない通信は複数宛先回線でラウンドロビンが可能であること。
7. 宛先回線のグループ分けが出来ること。グループ内宛先回線のラウンドロビン割合を設定できること。
8. 同時接続セッション数は 500 万セッション以上の処理能力であること。
9. 5Gbps 以上のスループットであること。
10. 管理用インターフェースとして、シリアルコンソールのほか Web ユーザーインターフェースを有すること。
11. Syslog トラップ、SNMP トラップの通知機能を有すること。E-Mail での通知機能も有することが望ましい。
12. 2 台以上で Active-Standby 構成もしくは Active-Active 構成が可能であること。
13. LACP をサポートすることが望ましい。
14. 将来、インターネットから内部へのアクセスが想定されるため、インターネットからの回線負荷分散と内部からの回線負荷分散ができるようにライセンスを含むこと。

15. SSH ターミナルアクセスが可能であること。
16. SSL 暗号化された通信で管理画面への GUI アクセスが可能であること。
17. 標準機能として、IPv4-IPv6 デュアルスタック構成が可能であること。
18. 19 インチ幅のラック搭載型とし、1RU 以内に収納可能であること。

1.11. 外局収容ルータ

想定機種

シスコシステムズ社製 CISCO 3945E-SEC/K9

1. IPv4 および IPv6 のルーティング可能なルータ製品であること。
2. IPv4 ルーティングとして、Static、RIP、OSPF、BGP4、EIGRP のルーティング・プロトコルをサポートすること。
3. IPv6 ルーティングとして、Static、RIPng、OSPFv3、EIGRPv6 のルーティング・プロトコルをサポートすること。
4. ポリシーベースルーティング機能を有すること。
5. IP マルチキャストルーティングプロトコルとして、PIM-SparseMode、Source Specific Multicast に対応していること。
6. PPPoE に対応していること。
7. 256MB 以上の Flash を搭載していること。
8. 1GB 以上の DRAM を搭載していること。
9. DSCP に基づきトラフィックの優先制御に対応していること。
10. 4 つ以上の 1G ポートを有し、その内 2 つは RJ45 ポートか SFP ポートを選択可能であること。
11. モジュールの追加でポートの増設が可能になること。
12. Layer 2 Tunneling Protocol Version 3 に対応していること。
13. IPsecVPN トンネル数が 200 以上であること。
14. トンネリングプロトコルとして GRE に対応していること。
15. Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192 及び AES 256 の各暗号化機能を有すること。
16. IPsec 暗号化はハードウェア処理で行われること。
17. IKE v1 / IPsec / PKI, IPsec/GRE, Easy VPN w/ DVTI, DMVPN, Firewall, GETVPN 機能に対応していること。
18. DSCP に基づきトラフィックの優先制御に対応していること。
19. 転送容量は 8,675Mbps 以上であること。
20. 転送能力は 2,924kpps 以上であること。

21. Telnet/SSH によるリモートコンソール機能を有すること。
22. 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。
23. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
24. Syslog サーバーにメッセージを送信する機能を有すること。
25. DNS を参照し IP アドレスの代わりにホスト名を使用できる機能を有すること。
26. SNMPv1/v2c/v3 による管理機能を有すること。
27. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
28. IP アプリケーションに対するサービスレベルを測定する機能をサポートすること。
29. シスログ出力などの対象となるイベントが発生した際に、そのイベントと関連づけたアクションを起こすことが可能であること。
30. 電源の冗長化が可能であること。
31. 動作温度が 0℃～40℃に対応していること。
32. 動作相対湿度は 5%～85%に対応していること。
33. VCCI クラス A に準拠していること。
34. 1000Base-X インターフェースが、IEEE 802.3z に準拠していること。
35. 1000Base-T インターフェースが、IEEE 802.3ab に準拠していること。
36. 19 インチラックマウント可能であり 3U 以下であること。

1.12. 外局接続用ルータ

想定機種

シスコシステムズ社製 CISC0 891FJ-K9

1. IPv4 および IPv6 のルーティング可能なルータ製品であること。
2. IPv4 ルーティングとして、Static、RIP、OSPF、BGP4、EIGRP のルーティング・プロトコルをサポートすること。
3. IPv6 ルーティングとして、Static、RIPng、OSPFv3、EIGRPv6 のルーティング・プロトコルをサポートすること。
4. ポリシーベースルーティング機能を有すること。
5. IP マルチキャストルーティングプロトコルとして、PIM-SparseMode、Source Specific Multicast に対応していること。
6. PPPoE に対応していること。
7. WAN 側インターフェースとして 1G ポートを有し、RJ45 ポートまたは SFP ポー

トを選択可能なこと。

8. WAN 側インターフェースとして ISDN ポートを 1 つ以上有すること
9. LAN 側インターフェースとして、10/100/1000BASE-T ポートを 8 ポート以上有すること。
10. IEEE802.1q に準拠した VLAN 設定が 14 以上可能なこと。
11. Firewall 機能を有すること。
12. VRF-lite 機能を有すること。
13. Layer 2 Tunneling Protocol Version 3 に対応していること。
14. IPsecVPN トンネル数が 50 以上であること。
15. トンネリングプロトコルとして GRE に対応していること。
16. Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192 及び AES 256 の各暗号化機能を有すること。
17. IPsec 暗号化はハードウェア処理で行われること。
18. DSCP に基づきトラフィックの優先制御に対応していること。
19. Telnet/SSH によるリモートコンソール機能を有すること。
20. 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。
21. NTP クライアントとして、一貫したタイムスタンプを刻む機能を有すること。
22. Syslog サーバーにメッセージを送信する機能を有すること。
23. DNS を参照し IP アドレスの代わりにホスト名を使用できる機能を有すること。
24. SNMPv1/v2c/v3 による管理機能を有すること。
25. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。
26. IP アプリケーションに対するサービスレベルを測定する機能をサポートすること。
27. シスログ出力などの対象となるイベントが発生した際に、そのイベントと関連づけたアクションを起こすことが可能であること。
28. 動作温度が 0℃～40℃に対応していること。
29. 保管温度が 0℃～60℃に対応していること。
30. 動作相対湿度は 10%～85%に対応していること。
31. 100BaseTX インターフェースが、IEEE 802.3u に準拠していること。
32. 1000Base-T インターフェースが、IEEE 802.3ab に準拠していること。
33. 19 インチラックマウント可能であり 1U 以下であること。
34. ファンレスであること。

1.13. 無線 LAN コントローラ

想定機種

シスコシステムズ社製 AIR-CT5508-250-K9

1. 無線 LAN のダウンタイムを最小化するため、無線 LAN コントローラはアクセスポイントに対するアクティブスタンバイのフェールオーバー構成を組むことが可能であること。
2. トラフィックの傾向を観察しネットワーク計画に役立てるため、無線 LAN 上に流れているアプリケーション及びその利用状況を視覚化できること。
3. 無線環境において、重要度の高い特定のアプリケーションの通信を優先させることが可能な優先制御の仕組みを有すること。
4. 無線 LAN にアクセスするためのユーザー認証として、802.1x と Web 認証を用いた 2 要素認証が可能であること。
5. 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。
6. IEEE802.1x 認証をサポートしていること。
7. IEEE 802.1X 無線 LAN 認証に対応すること。以下の EAP タイプに対応すること。
 - (ア)EAP-TLS
 - (イ)EAP-FAST
 - (ウ)PEAPv1/GTC
 - (エ)PEAPv0/MSCHAPv2
8. IEEE 802.1X 認証に 3 回連続で認証失敗した無線 LAN クライアントの無線 LAN 接続を拒否することができること。接続拒否を一定時間後に解除するか永久に継続するかを選択することができること。一定時間後に解除する場合は、その時間を 1～2147483647 秒の間で設定できること。本機能の適用は、SSID 毎に選択できること。
9. 暗号化機能として下記の機能をサポートしていること。
 - (ア)WEP および TKIP-MIC : RC4 40、104、および 128 ビット (静的キーと共有キー)
 - (イ)SSL および TLS : RC4 128 ビットと RSA 1024 および 2048 ビット
 - (ウ)AES : CBC, CCM, CCMP
 - (エ)DES : DES-CBC、3DES
 - (オ)DTLS: AES-CBC
10. 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り、かつ利用時

にラインレートがでること。

11. 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
12. 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
13. 無線 LAN コントローラとアクセスポイント間で利用するプロトコルは IETF で標準化されていること
14. 1GbE ポートを 8 つ以上有すること。
15. 1 台のコントローラで 500AP 以上のサポートが可能で、ハードウェアの追加無しにライセンス追加のみで管理可能なアクセスポイントの数を増やすことが可能であること。
16. 管理用インターフェースとして、①Web ベース : HTTP/HTTPS ②コマンドライン インターフェース : 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。
17. 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
18. 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。
 - (ア)通信に伴う負荷の大きさ
 - (イ)電波干渉の程度
 - (ウ)電波雑音の大きさ
 - (エ)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
 - (オ)電波到達範囲 (セル) が隣接する AP の数
19. 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。
20. 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。
21. 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ネルを自動的に選択し最適化する機能を有すること。
22. 無線 LAN クライアントに IP アドレス情報を提供するための DHCP サーバー機能を有すること。
23. Ad-hoc Network の検知、Reporting が可能なこと
24. OS Image のプリダウンロードができること
25. 100V AC 電源で稼動すること。
26. 440 x 539 x 44.5 mm 以下であること
27. 重量が 9.1 kg 以下であること。

1.14. 無線 LAN アクセスポイント

想定機種

シスコシステムズ社製 CAP3702E-Q-K9

1. IEEE 802.11 a/b/g/n/ac (wave1) に準拠および Wi-Fi 認定を得ていること。
2. 最大理論値 1.3Gbps まで対応可能なこと。
3. AP 自体に設定されているチャンネルだけではなく、すべてのチャンネルの電波をモニターできるモジュールが搭載できる AP であること。
4. IEEE 802.11i に準拠およびセキュリティにおける Wi-Fi 認定 (WPA (TKIP)、WPA2 (AES)) を得ていること。
5. 2.4GHz および 5GHz のワイヤレスネットワークの同時運用が可能であること。
(デュアル無線)
6. アップリンクとして、自動検知式の 10/100/1000BASE-T (RJ-45) イーサネットを有していること。
7. コンソールポートとして RJ-45 のインターフェースを有していること。
8. 無線 LAN のアンテナは外出しであること。
9. 3 空間ストリーム対応かつ 4x4 MIMO アンテナであること。
10. 壁面や天井に設置された状態でも LED が確認でき、LED の色で稼働状態などが判別できること。
11. IEEE 802.3at にて動作可能であること。
12. 外部の電源装置やパワーインジェクターなどの柔軟な電源環境に対応できる製品があること。
13. 以下の EAP に対応した認証が可能なこと。
 - (ア) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
 - (イ) EAP-Tunneled TLS (TTLS) または Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)
 - (ウ) Protected EAP (PEAP) v0 または EAP-MSCHAPv2
 - (エ) Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
 - (オ) PEAPv1 または EAP-Generic Token Card (GTC)
 - (カ) EAP-Subscriber Identity Module (SIM)
14. 非 Wi-Fi デバイスとの干渉による 20MHz, 40MHz, 80MHz におけるインパクトやネットワークのパフォーマンスを 1 つの数字で表す機能に対応すること。
15. 非 WIFI 干渉を含めた 20 種類以上の干渉を 5-30 秒以内に分類する機能を有すること。

16. RF の干渉を検出し、干渉源周囲のワイヤレス電波到達範囲を最適化する自動調整機能を有すること。
17. 802.11a/g/n/ac のクライアントに対して機能を追加せずに、DSP ベースのビームフォーミング技術によりダウンリンクのパフォーマンスを向上する機能を有すること。
18. MRC(Maximum Ratio Combining, 最大合成比)によりアップリンクのパフォーマンスを向上する機能を有すること。
19. AP において 2.4GHz 帯、5GHz 帯の双方の電波周波数帯が利用可能な場合、無線 LAN クライアントが 5GHz 帯に優先して接続するよう促す機能を有すること。
20. アクセスポイント単体の寸法 (幅×奥行×高さ) が 22.1 × 22.1 × 5.4 cm 以下であること。
21. アクセスポイント単体の重量が 1.13 kg 以下であること。
22. コントローラと連携して動作する、または連動せずに動作することを選択できること。
23. 動作温度が 0℃～40℃に対応していること。
24. 動作温度が-20℃～50℃に対応していること。
25. 金属製ハウジングで密閉筐体であること。
26. マルチキャストをユニキャストに変換する機能を有すること。
27. オーバーサブスクリプションを防止するビデオコールアドミッション制御を有すること。
28. UL2043 プレナム定格に準拠し、天井裏への設置や吊るし天井からのつり下げが可能なこと。
29. AP 固有の CPU、メモリ以外に Radio 毎に CPU、メモリを搭載していること
30. HW 上に専用のチップを内蔵し、非 Wi-Fi デバイスの干渉源を検出できる機能を有すること。
31. IEEE802.11ac/wave2 にモジュール追加で対応できるモジュールタイプの AP であること。

1.15. 無線 LAN 管理サーバー

想定機種

シスコシステムズ社製 PRIME-NCS-APL-K9

1. 管理対象機器のインターフェース、ポート、接続ホストに関する状態(CPU 利用率・メモリ利用率・VLAN 情報・ポートの UP/Down・MAC アドレス・IP アドレス)を表示することができること。
2. 無線 LAN システム全体を管理する為に、複数の無線 LAN コントローラ、アクセスポイントを一元的に管理することが可能であること。
3. 複数の LAN スイッチやルータを一元的に設定することが可能であること
4. 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を視覚化できること。
5. 無線 LAN の通信品質の視覚化とステータス評価が可能であること。
6. 管理対象機器に接続しているおけるユーザーの情報(ネットワーク認証のユーザー名、MAC アドレス、IPv4/IPv6 アドレス、接続 SSID、SNR、RSSI、VLAN、接続先 AP)が表示可能なこと。
7. 検索フォームにユーザー情報(MAC アドレス、ユーザー名、IP アドレス)を入力することで対象デバイス一覧が表示可能なこと
8. 検索フォームにデバイス情報(ホスト名、管理対象 IP アドレス)を入力することで対象デバイス一覧が表示可能なこと
9. 設定作業の容易性および設定投入の利便性を考慮し、管理対象機器向けに、設定のテンプレートの作成、割り当てることができること。
10. 設定作業の容易性および設定投入の利便性を考慮し、管理対象機器向けに、監視項目のテンプレートの作成、割り当てることができること。
11. 実際に無線 LAN アクセスポイントを導入せずに、アクセスポイントの設置に関するシミュレーションができること。
12. 指定した接続デバイスの接続先 AP や Switch の履歴を表示させることが可能であること。
13. ネットワークアクティビティ、パフォーマンス、使用状況、デバイス、インベントリ、セキュリティ、および通信品質について、様々なオンデマンドのレポートおよび自動化されたレポートを実行可能なこと。
14. レポートのデータ、タイムフレーム、および形式をカスタマイズ可能なこと。
15. レポートは CSV 形式または PDF 形式でファイル出力でき、電子メールとして通知可能なこと。

16. 無線 LAN コントローラで検知した不正 AP の情報を一元的に表示や分類することが可能なこと
17. 無線 LAN システムにおいてゲストユーザーアカウントや管理専用ゲストアカウントを作成可能なこと。
18. クライアントごとに接続性のトラブルシューティング (L2 の接続性や IP アドレスの取得状況などの確認) が可能であること
19. Management Frame Protection (MFP) による 802.11 管理フレームを監視可能であること。
20. スケジュール設定した間隔でアクセスポイントのラジオの電源のオン/オフを切り替えることによって、節電が可能なこと。
21. WEB ブラウザベースのグラフィカルユーザーインターフェースを有すること。接続は HTTP/HTTPS に対応していること。
22. SSH やコンソールによるリモートコンソール機能を有すること。
23. Syslog サーバーにメッセージを送信する機能を有すること。
24. SNMP エージェントを有すること。
25. NTP サーバーと時刻を同期する機能を有し、且つ複数の NTP サーバーを指定することが可能であること。

1.16. 無線 LAN ロケーション管理サーバー

想定機種

シスコシステムズ社製 AIR-MSE-3355-K9

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。

1.17. 無線 LAN アダプタ

想定機種

エレコム社製 WDC-433SU2M または WDC-867SU3S または WDC-433DU2H

1. USB による接続が可能なこと。
2. IEEE 802.11 a/b/g/n/ac に準拠および Wi-Fi 認定を得ていること。
3. セキュリティにおいて WPA2-PSK (AES) / WPA-PSK (TKIP) / WEP (128/64bit) に対応できること。

1.18. ネットワーク認証サーバー

想定機種

日立電線ネットワーク社製 Account@Adapter+

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 に 2 台設置可能であること。
3. 最大消費電力は 72W 以下であること。
4. 管理画面は Web ブラウザかつ日本語で表示されること。（専用アプリケーション不要）
5. 設定情報を USB メモリや外部のサーバーに自動的にバックアップする機能を有すること。
6. マスターからスレーブに対して設定情報の同期が可能であること。
7. 認証ログを管理画面で確認できること、また syslog として外部に送出可能であること。
8. Web、MAC、IEEE802.1X 認証（EAP-MD5、EAP-TLS、EAP-PEAP、EAP-TTLS）機能を有すること
9. MAC 認証の際、MAC アドレスの区切り文字やパスワードに関わらず認証成功する機能があること。
10. ライセンス数に関わらず RADIUS クライアントを最大 10000 台登録できること。
11. RADIUS 属性応答に対応していること。任意の RADIUS 属性を追加できること。
12. RADIUS クライアントをグルーピングできること。
13. RADIUS クライアント/グループ毎に応答属性を変えられること。
14. 外部の ActiveDirectory/LDAP サーバーにあるアカウント情報を参照し、認証

情報として利用することができること。

15. 複数の外部認証局と連携して認証できること。
16. RADIUS プロキシサーバーとして動作できること。
17. realm ごとに参照先 LDAP サーバーや転送先 RADIUS サーバーを指定できること。
18. RADIUS Accounting に対応していること。
19. サーバー・クライアント証明書発行機能を有すること。
20. 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。
21. 1 アカウントあたり 2 枚の有効期限が異なるクライアント証明書を発行できること。
22. 失効リストをダウンロードできること。
23. クライアント証明書と使用するクライアント端末を紐づけて管理できること。
24. 下位認証局（中間認証局）として動作すること。
25. 最大 200,000 アカウントを登録可能であること。
26. ユーザー/端末(MAC アドレス)/証明書アカウントの管理がディレクトリ単位にできること。
27. アカウント情報を登録、編集、削除できる機能を有すること。
28. アカウント作成、一覧、検索画面では、表示する管理項目をカスタマイズできること。
29. 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、管理項目名、任意にカスタマイズ表示できること。
30. 管理者がユーザーのパスワードポリシーを設定できること。
31. 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。
32. ディレクトリ単位で共通のアトリビュートを設定できること。
33. 最終認証日から一定期間認証していないアカウントや有効期限が切れたアカウントを自動無効・削除できること。
34. アカウント情報を外部のサーバーへ定期インポート/エクスポートできること。
35. 認証端末の MAC アドレスを収集する機能を有すること。
36. 利用者によるユーザー/端末/証明書アカウントを登録/編集/削除申請する Web インターフェースを有すること。利用者が申請した内容を管理者に通知し、管理者が承認する機能を有すること。
37. 登録するユーザーID/パスワードは、ユーザー任意入力および自動割り当てができること。
38. 登録する MAC アドレスは、自動入力が可能であること。
39. 登録する MAC アドレスを DHCP 端末情報として利用できること。
40. 利用者による証明書のダウンロードが可能であること。

41. 申請する際のログインアカウントには外部 LDAP アカウントを利用でき、申請項目に外部 LDAP アカウントの属性情報を自動で表示可能であること。
42. 外部 LDAP アカウントをクライアント証明書情報として利用できること。
43. パスワード期限切れメール通知ができること。利用者がパスワードを変更可能であること。
44. クライアント証明書有効期限切れメール通知ができること。利用者が証明書更新可能であること。
45. 申請、編集画面では、使用する管理項目をカスタマイズできること。
46. 申請、編集画面では、管理項目毎に必須入力/任意入力の指定が可能で、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。
47. 利用者向け Web インターフェースは、スマートデバイス専用の画面にも対応していること。

1.19. 基幹ファイアウォール

想定機種

シスコシステムズ社製 ASA5545-SSD120-K9

1. ファイアウォール機能が動作可能なこと。
2. 異なるネットワーク間のルーティングによる構成が取れること。
3. レイヤ 2 ブリッジにおけるファイアウォール機能を有し、既存の IP アドレスを変更せずに Firewall を導入できること。
4. アクセスリストによる接続の許可・拒否が可能であること。アクセスリストは以下の要素をサポートすること。
 - (ア) IPv4 送信元及び送信先のホスト、ネットワーク
 - (イ) IPv6 送信元及び送信先のホスト、プリフィックス
 - (ウ) TCP/UDP 送信元及び送信先ポート番号
5. HTTP の URL の文字列の部分一致によるアクセスリストを定義できること。
6. アクセスリストの定義において、曜日、日付、時刻によって自動的に有効化・無効化される属性を付加することが可能であること。
7. IPv4 のアドレス変換 (NAT) が可能であること。アドレス変換方式として、以下をサポートすること。
 - (ア) スタティック NAT
 - (イ) スタティックポートアドレス変換
 - (ウ) ダイナミック NAT

(エ)Dynamic PAT

8. ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェースと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護できること。
9. アプリケーション固有の検査機能を有し、アプリケーション セキュリティポリシーに基づいたアクセス制御を行えること。具体的には IPv6 および IPv4 パケットについて、下記のアプリケーションに対応していること。

(ア)Web ブラウジング (HTTP)

(イ)E メール (SMTP)

(ウ)エンタープライズ IP テレフォニー (SIP)

(エ)ファイル転送 (FTP)

10. 不正なサイトへの通信の特定は逆引き DNS をもとに行うことができること。
11. DoS 攻撃などの攻撃に関連している可能性のあるイベントを検出することができること。具体的には下記の理由にてドロップしたパケット及びセキュリティイベントの頻度を監視可能であること。
 - (ア)アクセスリストによる拒否
 - (イ)不正なパケット形式
 - (ウ)事前に定義した制限値を超えた接続
 - (エ)DoS 攻撃の検出
 - (オ)疑わしい ICMP パケットの検出
 - (カ)スキャン攻撃の検出
 - (キ)不完全セッションの検出
 - (ク)ファイアウォール関連の検査にて不適合
 - (ケ)アプリケーション検査にて不適合
 - (コ)インターフェースの過負荷

12. IP アドレスと Windows Active Directory のログイン情報の関連付けに基づいてセキュリティ ポリシーを適用可能であること。
13. 8 ポート以上の 10/100/1000T インターフェースを有すること。
14. 6 ポート以上の 1000BASE-X インターフェースを有すること。
15. USB 2.0 ポート を 2 ポート以上有すること。
16. 3Gbps 以上のファイアウォール性能を有すること。
17. 900Mbps 以上の IPS 性能を有すること。
18. 400Mbps 以上の 3DES/AES VPN 性能を有すること。
19. 300 以上の VLAN に対応すること。
20. 2500 以上の VPN コネクションが可能であること。

21. 新規接続数が毎秒 30,000 コネクション以上であること。
22. 同時接続数が 750,000 コネクション以上であること。
23. 9000 バイト以上のジャンボフレームに対応可能であること。
24. 20 以上の仮想ファイアウォールに対応可能なこと。
25. 19 インチラックにマウント可能であり、サイズは、19 インチラックにマウント可能であり、サイズは、4.24 x 42.9 x 48.4 cm 以下であること。
26. 重量が 7.63kg 以下であること、電源冗長化時は 8.61 kg 以下であること。
27. メモリが 12GB 以上であること。
28. 電源の冗長構成が可能なこと。
29. アクティブブーアクティブ、アクティブースタンバイのステートフルフェールオーバー機能に対応可能なこと。

1.20. ファイアウォール A

想定機種

シスコシステムズ社製 ASA5525-SSD120-K9

1. ファイアウォール機能が動作可能なこと。
2. 異なるネットワーク間のルーティングによる構成が取れること。
3. レイヤ 2 ブリッジにおけるファイアウォール機能を有し、既存の IP アドレスを変更せずに Firewall を導入できること。
4. アクセスリストによるコネクションの許可・拒否が可能であること。アクセスリストは以下の要素をサポートすること。
 - (ア) IPv4 送信元及び送信先のホスト、ネットワーク
 - (イ) IPv6 送信元及び送信先のホスト、プリフィックス
 - (ウ) TCP/UDP 送信元及び送信先ポート番号
5. HTTP の URL の文字列の部分一致によるアクセスリストを定義できること。
6. アクセスリストの定義において、曜日、日付、時刻によって自動的に有効化・無効化される属性を付加することが可能であること。
7. IPv4 のアドレス変換 (NAT) が可能であること。アドレス変換方式として、以下をサポートすること。
 - (ア) スタティック NAT
 - (イ) スタティックポートアドレス変換
 - (ウ) ダイナミック NAT
 - (エ) Dynamic PAT

8. ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェースと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護できること。
9. アプリケーション固有の検査機能を有し、アプリケーション セキュリティポリシーに基づいたアクセス制御を行えること。具体的には IPv6 および IPv4 パケットについて、下記のアプリケーションに対応していること。
 - (ア)Web ブラウジング (HTTP)
 - (イ)E メール (SMTP)
 - (ウ)エンタープライズ IP テレフォニー (SIP)
 - (エ)ファイル転送 (FTP)
10. 不正なサイトへの通信の特定は逆引き DNS をもとに行うことができること。
11. DoS 攻撃などの攻撃に関連している可能性のあるイベントを検出することができること。具体的には下記の理由にてドロップしたパケット及びセキュリティイベントの頻度を監視可能であること。
 - (ア) アクセスリストによる拒否
 - (イ)不正なパケット形式
 - (ウ)事前に定義した制限値を超えた接続
 - (エ)DoS 攻撃の検出
 - (オ)疑わしい ICMP パケットの検出
 - (カ)スキャン攻撃の検出
 - (キ)不完全セッションの検出
 - (ク)ファイアウォール関連の検査にて不適合
 - (ケ)アプリケーション検査にて不適合
 - (コ)インターフェースの過負荷
12. IP アドレスと Windows Active Directory のログイン情報の関連付けに基づいてセキュリティ ポリシーを適用可能であること。
13. 8 ポート以上の 10/100/1000T インターフェースを有すること。
14. USB 2.0 ポート を 2 ポート以上有すること。
15. 2Gbps 以上のファイアウォール性能を有すること。
16. 600Mbps 以上の IPS 性能を有すること。
17. 300Mbps 以上の 3DES/AES VPN 性能を有すること。
18. 200 以上の VLAN に対応すること。
19. 750 以上の VPN コネクションが可能であること。
20. 新規接続数が毎秒 20,000 コネクション以上であること。
21. 同時接続数が 500,000 コネクション以上であること。

22. 9000 バイト以上のジャンボフレームに対応可能であること。
23. 4 以上の仮想ファイアウォールに対応可能なこと。
24. 19 インチラックにマウント可能であり、サイズは、19 インチラックにマウント可能であり、サイズは、4.24 x 42.9 x 39.5 cm 以下であること。
25. 重量が 6.77kg 以下であること。
26. メモリが 8GB 以上であること。
27. アクティブ-アクティブ、アクティブ-スタンバイのステートフルフェールオーバー機能に対応可能なこと。

1.21. ファイアウォール B

想定機種

パロアルト社製 PA-3020

1. ハードウェアとソフトウェアが一体となったアプライアンス機器のファイアウォールであること。
2. 専用の管理用インターフェースを 1 ポート以上有すること。
3. 専用の HA 用インターフェースを 2 ポート以上有すること。
4. IPS、アンチウィルス、アンチスパイウェア機能を同時に使用した場合でも 1Gbps 以上の処理能力を有すること。
5. 新規セッション数が秒間あたり、50,000 セッション以上を処理可能であること。
6. 最大同時セッション数が、250,000 セッション以上を処理可能であること。
7. 消費電力が 200W 以下であること。
8. 機器内部にログや設定を保存するためのストレージとして、120GB 以上の SSD が搭載されていること。
9. 19 インチ幅のラック搭載型とし、1RU 以内に収納可能であること。
10. 管理通信処理用とデータ通信処理用でそれぞれ独立した処理プロセッサを搭載していること。
11. 設定については、候補コンフィグと実行コンフィグを分けた Commit ベースのアーキテクチャとなっていること。
12. 設定ファイルについては XML 形式でインポート/エクスポート可能であること。
13. 設定およびレポートデータを XML ベースの API を使用して外部システムと連携可能であること。
14. レポートデータを PDF 形式でエクスポートし、スケジュール機能により定期的に電子メールに添付し送付することが可能であること。

15. 本装置は TAP モード(ミラーポート接続)、L1 モード(MAC アドレスを保持しない)、L2(ブリッジ) モード、L3 (ルータ) モードに対応し、一筐体内で複数のモードの混在設定が可能なこと。
16. NAT 機能を有すること。
17. DoS 攻撃防御機能を有すること。
18. IEEE802.1Q VLAN トランク機能を有すること。
19. IEEE802.3ad リンクアグリゲーション機能を有すること。
20. ジャンボフレーム (9216Bytes) をサポートすること。
21. 本装置を通過するアプリケーションを識別し可視化する機能を有すること。
22. 1800 種類以上のアプリケーションをポート番号に依存せず識別し可視化できること。
23. 専用のアプリケーション識別エンジンを搭載しており、標準(デフォルト設定)で全てのトラフィックを対象にしたアプリケーションの識別のシグネチャが適用されていること。
24. ゾーンベースのポリシー制御が可能で、1 筐体あたり 20 以上のゾーン設定が可能なこと。
25. ゾーンベースのポリシー制御が可能で、1 筐体あたり 10 以上のゾーン設定が可能なこと。
26. ファイアウォールのポリシーは送信元/送信先とアプリケーション名を元に処理可能であること。
27. ファイアウォールのポリシー毎にウィルス・スパイウェア、URL フィルタリング等のコンテンツ検査機能を有効/無効に設定が可能であること。
28. ファイアウォールのセキュリティポリシー上で URL カテゴリーを直接指定し、URL カテゴリー毎のアクセス制御が可能であること。
29. PDF、Excel、WORD、PPT、ZIP など 70 種類以上のファイルタイプによる通信の可視化やフィルタリングが可能なこと。
30. クレジットカード番号、またはカスタマイズした文字列パターンでのデータフィルタが可能であること。
31. 脆弱性防御、アンチウィルス、アンチスパイウェア機能を有すること。
32. 脆弱性防御、アンチウィルス、アンチスパイウェア、ファイルフィルタ、データフィルタといったコンテンツスキャニング機能を、シングルエンジンで且つストリームベースで処理できること。
33. 筐体内で SSH 通信を複合化し、ポートフォワード通信を検知可能であること。
34. 筐体内で SSL/TLS1.2 に準拠した通信を復号化し、アプリケーションの識別およびコンテンツ検査のポリシーが適用可能であること。
35. 内部クライアントから外部サーバーに対する SSL 通信を筐体内で復号化した後、

復号化したトラフィックを外部システムに転送する機能を有すること。

36. 筐体内にサーバー証明書と鍵をインポートし、その証明書と鍵をもとに該当するサーバー宛での SSL 通信を複合化し、アプリケーションの識別およびコンテンツ検査のポリシーが適用可能であること。
37. URL フィルタリング機能として、75 以上のカテゴリーに分類された 2000 万件以上の URL データベースを筐体内に有すること。
38. Active Directory 等と連携し、IPv4 及び IPv6 環境に関わらずアプリケーションとユーザー情報を紐付け、可視化と制御が可能であること。
39. ポリシーベースの QoS に対応しており、アドレス、ポート番号、利用ユーザー、アプリケーションといった情報を基に帯域制御が可能であること。
40. SNMP, メール、syslog へのログ出力方式に対応していること。また、ポリシー毎にログ出力方式を指定することが可能であること。
41. 4 台以上の外部 syslog サーバーにログ出力可能であること。
42. Syslog データ転送方式として UDP に加えて TCP または SSL に対応していること。
43. ローカルシステム上でのログ保存が可能であること。
44. http および https 対応の Web インターフェースを有すること
45. telnet/ssh によるコマンドラインインターフェースを有すること。
46. SNMP プロトコルによる管理処理部のメモリ利用率、ディスク使用率、スワップ利用率、仮想システム毎のセッション利用率、およびデータ転送処理部のパケットバッファ利用率のモニタリングが可能なこと。
47. WebUI 上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し、利用頻度の多いアプリケーション、URL カテゴリー、脅威をランキング形式で表示できること。
48. 40 以上の事前に定義されたレポートテンプレートおよびカスタムレポート機能を有し、それらを PDF 形式にして設定されたスケジュールで自動メール送信可能なこと。
49. ポートやプロトコルに関わらず全てのトラフィックをモニターし、ボットネット感染が疑われる端末をリストアップするボットネットレポート機能を有すること。
50. Windows OS の実行形式のファイルや PDF ファイル、Microsoft Office ドキュメントや Java アプレット(jar., .class)、Android OS の実行形式のファイルである APK など、未知のマルウェア感染が疑われるファイルを自動的に仮想実行環境上で 100 以上の検査項目によって検査し、未知のマルウェアの早期発見と対策が可能なクラウドシステムと連携する機能を有すること。
51. インターネット経由でファームウェアならびにシグネチャファイルを製品に直接ダウンロードおよびインストール可能であること。また Proxy 経由でもこ

れが可能であること。

52. 通信量の統計情報を元に、宛先/送信元の国別で通信量を世界地図上に視覚的に表示する機能を有すること。
53. 検出/防御した脅威の統計情報を元に、宛先/送信元の国別で脅威の発生状況を世界地図上に視覚的に表示する機能を有すること。
54. 宛先/送信元の国別アドレスでポリシー制御が可能であること。
55. 候補コンフィグと実行コンフィグを分けており、設定変更が即座に反映されないような Commit ベースのアーキテクチャとなっていること。
56. RIPv2, OSPF, BGP のダイナミックルーティングに対応していること。
57. IPv4 および IPv6 の OSPF Graceful Restart に対応していること。
58. IPv6 による WebUI/CLI の管理通信に対応していること。
59. IPv6 に対してもアプリケーション識別やユーザー識別、および脆弱性防御、アンチウィルス、アンチスパイウェア、ファイルフィルタ、データフィルタといったコンテンツスキャニングが可能なこと。
60. Syslog を介して受信した外部認証サーバーのログ情報を元にしたユーザー識別機能を有すること。
61. Active/Passive、Active/Active 両方の冗長構成に対応していること。(尚、いずれの冗長構成でもアプリケーション識別や IPS 機能、アンチウィルス機能も制限なく利用可能なこと)
62. CPU 使用率のモニタリングが可能であること。
63. センサーとなる次世代ファイアウォールで補足したファイルのコピーを受け取り、サンドボックスで検査を行いマルウェアかどうかの判断が可能なこと。
64. 100 台以上のセンサーとなる次世代ファイアウォールからファイルの送信を受け付けられること。
65. センサーとなる次世代ファイアウォールの管理画面を経由して、ファイルの検査状況と詳細レポートを確認可能なこと
66. 管理クライアント端末に対する専用クライアントソフトウェアインストールを必要としないこと。
67. ssh によるコマンドラインインターフェースを有すること。
68. REST/XML の API を有し、任意の API クライアントから検体の送信ならびに検査結果の情報取得が行えること。
69. サンドボックスでの検査時、検体が動作しているプラットフォームからインターネット上にある C&C サーバーに接続させてマルウェアかどうかの判断材料にすることができること。
70. TOR クライアント機能を有し、サンドボックスからのインターネット接続時にソース IP アドレスを隠蔽できること。

71. 設定については、候補コンフィグと実行コンフィグを分けた Commit ベースのアーキテクチャとなっていること。
72. Win32 PE の他に PDF や Office ドキュメントの検査に対応していること。
73. APK ファイルの検査に対応していること。
74. 設定については、候補コンフィグと実行コンフィグを分けた Commit ベースのアーキテクチャとなっていること。
75. 設定ファイルについては XML 形式でインポート/エクスポート可能であること。
76. 次世代ファイアウォール用のアンチウイルスシグネチャ/Phone Home (C&C 通信) シグネチャ/DNS シグネチャ/URL フィルタ DB への情報フィードバックができること。
77. センサーとなる次世代ファイアウォールとは独立して非同期に動作し、お互いの死活がそれぞれの処理内容に影響を与えないこと。
78. 検体から発生した通信を記録し、その PCAP ファイルを詳細レポート画面経由で取得できること。
79. 検体を詳細レポート画面経由で取得できること。

1.22. AD 兼 DHCP サーバー

想定機種

マイクロソフト社製 Windows Server 2012 R2

1. Active Directory 機能を提供可能なこと。
2. 既存のドメイン環境にドメインコントローラーを追加し、正常稼働を確認後には既存のドメインコントローラーの Active Directory 降格作業を実施すること。
3. DNS サービスを提供可能なこと。また既存のドメインコントローラー上に構築されている DNS サーバー機能を移行すること。
4. DHCP サービスを提供可能なこと。またネットワーク機器に必要な DHCP リレー情報を開示すること。
5. 既存のドメインコントローラー上に構築されている DHCP サーバー機能を移行すること。
6. CA 局サービスを提供可能なこと。また CA 局は既存の Active Directory 証明書サービスの設定を引き継ぎ、設定を実施すること。なお、ユーザー証明書を発行する機能を有していること。

想定機種

シスコシステムズ社製 CISC0 UCSC-C220-M4S

1. CPU はインテル Xeon プロセッサーE5-2623 v3 (3GHz コア数 4) 以上を 1 つ以上搭載すること。
2. メインメモリは 16GB 以上搭載すること。
3. 拡張性として 1CPU あたり 12 枚までメインメモリが搭載可能なこと。
4. ハードディスク装置は SAS 接続、回転数 10,000rpm 以上で、ハードウェアによる RAID5 構成とし、RAID 未構成時のディスク容量は 900GB 以上、RAID 構成時で 600GB 以上有すること。
5. ハードディスク装置故障時にはシステムを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。
6. ホットスペア用のハードディスク 1 台を含めること。

1.23. Web コンテンツフィルタサーバ

想定機種

デジタルアーツ社製 i-Filter

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ー定義カテゴリ 10 を含む 111 カテゴリに分類されており、カテゴリはユーザー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。
6. ・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
7. ・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
8. ・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
9. ・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
10. 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。

11. 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。
12. 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。
13. 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。
14. ユーザー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。
15. 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。
16. 「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。
17. 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。
18. 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。
19. Web サービスにログイン後のページもカテゴリ判定が可能なこと。
20. 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。
21. 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。
22. HTTP、HTTPS、FTP over HTTP、Gopher、RTSP プロトコル全てに対応していること。
23. 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。
24. 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。
25. 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。
26. 「入出力 IP アドレス」を管理 GUI 上から指定可能なこと。
27. 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。

28. グループごとに所属している全ユーザーのWeb利用時間制限、各ユーザーの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。
29. 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。
30. ユーザー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。
31. 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。
32. 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。
33. 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。
34. 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ー、送信量の多いユーザーの確認が可能なこと。
35. 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ー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。
36. 日本国内で開発、販売されている製品であること。
37. 日本PTA全国協議会推薦の製品であること。

1.24. 資産管理システム

想定機種

スカイ社製 SkySea

1. 各クライアントコンピューターから資産情報を自動的に収集し一覧で表示できること。
2. クライアントコンピューター上のソフトウェアに関するインストール状況（Microsoft Office インストール状況、Windows 更新プログラム適用状況、ハードディスク上に存在する実行ファイル一覧を含む）等についても、自動的に収集可能であること。
3. クライアントコンピューターに関する各種情報を自動で資産情報として収集

する機能を有すること。検索条件はインベントリ情報や WindowsOS のバージョン、サービスパックなどで検索が可能であること。

4. 指定したクライアントコンピュータに対して、任意のプログラムを配布し、自動的にプログラムの実行を行う機能を有すること。また、ソフトウェアの配布日時と対象端末を設定し、配布したソフトウェアの配布状況および実行状況を確認することができること。また、配布時に利用する帯域を制限できること。
5. 指定したクライアントコンピュータに対して、Windows 更新プログラムを配布し、自動的に更新プログラムの実行を行う等のセキュリティパッチを適用する機能を有すること。配布した Windows 更新プログラムが適用されていないクライアントコンピュータを検出し、一覧化できること。
6. USB 外部ストレージをシリアルナンバーごとに管理する機能を有すること。保有 USB デバイスはシステムで台帳管理し、一覧で表示できること。なお、台帳への登録は USB デバイスをコンピュータに接続した際にデータを収集するなど自動収集できることが望ましい。
7. USB メモリ等の端末への着脱日時と記録されたファイル情報とを利用して、外部漏洩の危険性があるファイルを自動判定する機能を有すること。
8. 書き込み禁止とされた USB デバイスであっても、管理者が承認した特定のファイルのみ、書き込みを行えること。
9. クライアントコンピュータに対して行われた操作、ログオン、ログオフの日時、実行されたソフトウェアについての起動・終了時間、ファイル操作、共有フォルダへのアクセス・ファイル操作、クリップボードにコピーされた内容、USB メモリなどの記憶媒体を利用した内容および記憶媒体のシリアル情報等を記録する機能を有すること。
10. 有線/無線のネットワークカードや、Bluetooth などの通信デバイスに関して制限ができること。許可する IP 体系や無線アクセスポイントの SSID を登録することで、登録外のネットワークについては、接続を制限することができること。
(設定により指定したネットワークやアクセスポイントへの接続だけを許可し、その他の通信を制限することができること。) また、Bluetooth 接続、無線 LAN アクセスポイントへの接続および TCP/IP 通信をログとして記録する機能を有すること。
11. 収集されたファイル操作ログから、一つのファイルに対して、どのような操作(コピー・ファイル名変更、新規作成、削除など)が行われたかを抽出して表示する機能を有すること。また、Microsoft Office 製品については、名前を付けて保存(別ファイル名保存)ログを取得し、表示できること。
12. Windows 端末の 2 画面以上のディスプレイを同時に使用しているコンピュータに対してリモート操作を行う場合、操作するディスプレイを切り替えて対応

できる機能を有すること。

1.25. ウィルス対策管理サーバー

想定メーカー

シマンテック社製、トレンドマイクロ社製、マカフィー社製、カスペルスキー社製

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ーから収集したソフトウェアの“安全性”(普及度、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ィルス解析期間を有し、ウィ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、アンチウィルス、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の設定、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、アンチウィ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

2. 工事部材等仕様

2.1. サーバラック

1. 幅 800 mm、高さ 2000 mm、奥行き 1017 mmの 19 インチラックを 3 面設置すること。
2. 19 インチラックは、制振構造とすること。
3. 前後にマウントアングルが装備された EIA 規格のものとすること。
4. 前後マウントアングルは、ケージナット仕様とすること。
5. ラックの塗装色は、ブラック塗装とすること。
6. 取り付け可能なユニット数は、42U とすること。

7. 許容荷重は、500Kg 以上とすること。
8. 前面及び背面扉は、パンチング仕様とすること。
9. 棚板、L 型レール、ケーブルサポート等のオプションは含めること。

2.2. コード集合型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、2 芯とすること。
2. ネットワーク機器仕様に合わせたコネクタ形状の光ファイバーケーブルを使用すること。
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。
4. ケーブルは、環境配慮型を使用すること。

2.3. 光パッチコード

1. ネットワーク機器仕様に合わせたコネクタ形状の光ファイバーケーブルを使用すること。
2. 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。
3. ケーブルは、環境配慮型を使用すること。

2.4. 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 5 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. 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)
4. ケーブルは、環境配慮型を使用すること。

2.5. 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 5 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. 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)
5. ケーブルは、環境配慮型を使用すること。

2.6. UTP 情報コンセント

1. エンハンスドカテゴリ 5 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。

2.7. 電源ケーブル

1. ケーブルは、環境配慮型を使用すること。
2. 電源コンセントは、抜け止め対策がとられていること。

以上