14. インターネット

14. 1ネットワーク機器		
	14.1.1	アクセスポイント
	(1)	装置単体で10/100/1000BASE-Tのポートを2ポート以上搭載していること。 また、そのうち１ポート以上はIEEE 802.3at（PoE+、Power over Ethernet +）に対応していること。
	(2)	有線LANポートを2ポート以上搭載し、本装置の配下にパソコンをカスケード接続可能であること。
	(3)	アンテナ形式が内蔵であること。
	(4)	最大接続台数が127台以上であること。
	(5)	Wi-Fi規格及びIEEE 802.11a（W52/W53/W56）/802.11ac（W52/W53/W56）/802.11b/802.11g/802.11nに準拠していること。
	(6)	IEEE 802.11k（Radio Resource Measurement of Wireless LANs）、IEEE 802.11r（Fast Basic Service Set Transition）、IEEE 802.11v （Basic Service Set Transition Management Frames）に準拠したFast Roamingに対応していること。
	(7)	2.4GHz帯と2つの5GHz帯の同時使用が可能な3ラジオに対応していること。
	(8)	2空間ストリームに対応していること。
	(9)	複数アクセスポイント間のブリッジ接続を行うWDS(Wireless Distribution System)機能を有すること。
	(10)	エアタイムフェアネスに対応していること。
	(11)	IEEE 802.11ac Wave2に対応した送信ビームフォーミングに対応していること。
	(12)	自律型無線LANコントローラーによる管理時、無線AP間を無線接続することにより、LANケーブル不要で無線LANの利用エリアを拡張できること。なお、無線接続経路は冗長可能であり、障害時に自動経路切り替えできるものとする。
	(13)	無線端末間通信禁止機能を有すること。
	(14)	隣接アクセスポイントの検出機能を有すること。
	(15)	接続するクライアントに対して、周囲の電波状況を考慮し、無線端末に対して混雑していない帯域への接続を促すバンドステアリング機能を有すること。
	(16)	アクセスポイント1台で仮想的なアクセスポイントを、2.4GHz帯・2つの5GH z 帯ごとに最大で8個動作させる機能を有すること。また仮想的なアクセスポイントごとにSSIDとセキュリティーの設定を行うことや異なるVLANを関連付けることができること。
	(17)	自律型無線LANコントローラーによる管理時、無線アクセスポイント周囲の電波出力、チャンネルを常に認識し、最適化できること。
	(18)	スマートフォンやタブレットから容易に無線接続出来るための、無線設定情報を含むQRコードを生成可能であること
	(19)	SSIDごとに利用するRADIUSサーバを自由に指定できること。

	(20)	IEEE 802.1X認証に対応し、EAP-TLS / EAP-TTLS / MSCHAPv2 / PEAPv0 /EAP-MSCHAPv2 / PEAPv1 / EAP-GTC /EAP-SIM / EAP-AKA / EAP-FAST方式が使用可能なこと。
	(21)	キャプティブポータルによるWeb認証を有すること。
	(22)	認証時に、ユーザー（無線クライアント）が所属するVLANを動的に割当てる機能を有すること。
	(23)	暗号化機能としてWEP（64/128bit）及びWPA/WPA2(TKIP/CCMP)、WPA3(CCMP)が利用可能であること。
	(24)	MACアドレスフィルタリングが2,048以上設定可能なこと。
	(25)	IEEE 802.1Qに準拠したVLANが設定可能なこと。
	(26)	無線の利用状態を収集して、常に最適な電波出力とチャンネルを分析しアクセスポイントへ適用する機能を持つ自律型無線LANコントローラーにて管理ができること。
	(27)	自律型無線LANコントローラー離脱時でも無線サービスの提供を継続できること。
	(28)	時刻同期を行うためにNTPクライアント機能を有すること。
	(29)	SNMPエージェント機能を有し、SNMPv1/v2c/v3による管理が可能なこと。
	(30)	Syslogサーバーへログを転送できること。
	(31)	日本語Web GUI （HTTP/HTTPS） に対応していること。
	(32)	設定によりLEDを常時消灯させる機能を有すること。
	(33)	PoEスイッチとACアダプターの両方を同時に接続することにより、電源の冗長化が可能なこと。
	(34)	最大消費電力が20W以下であること。
	(35)	外形寸法は215（W）×215（D）×48（H）mm（突起部含まず）以下であること。
	(36)	天井・壁にレイアウト可能な専用のブラケットに対応していること。
	(37)	壁にレイアウト可能な専用のマグネットシートに対応していること。
	(38)	筐体の質量は700g以下（ブラケット含まず）であること。
	(39)	環境温度0～45℃（ACアダプター使用時）、0～50℃（PoE受電時）に対応していること。
	(40)	日本語マニュアルをインターネット上に公開していること。
	(41)	装置固有のベンダー定義MIBが存在する場合にはそのMIB仕様を公開すること。
	14.1.2	サーバスイッチ
	(1)	装置単体で10/100/1000BASE-Tのインターフェースを24ポート以上有すること。
	(2)	装置単体でSFPスロットを4つ以上有すること。
	(3)	IEEE 802.3z 1000BASE-LX/SX、IEEE 802.3ab 1000BASE-T、IEEE 802.3ah 1000BASE-BX10に準拠したSFPを搭載可能なこと。

	(4)	装置単体でスイッチングファブリックは56Gbps以上であること。
	(5)	装置単体でMACアドレス登録数は16,384以上であること。
	(6)	装置単体でIEEE 802.1Qに準拠した4,094以上のVLANを設定可能なこと。
	(7)	VLANの種類として、ポートベースVLAN、IEEE 802.1Qタグベース VLAN、IPサブネットベースVLAN、プロトコルベースVLAN、マルチプルVLAN、Voice VLANの各VLANに対応可能なこと。
	(8)	IEEE 802.1AX-2008 に準拠したLink Aggregation (static and dynamic) 機能を有すること。
	(9)	IEEE 802.1D-2004およびIEEE 802.1Q-2005準拠のスパニングツリー機能を有すること。
	(10)	ポートミラーリング、リモートミラーリング機能を有すること。
	(11)	RFC3619に準拠したレイヤー2のリング型冗長化機能を有すること。
	(12)	DHCPクライアント機能を有すること。
	(13)	特殊フレームの送受信によりループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせるなど設定した動作を自動実行可能なこと。
	(14)	ループを検出した際の動作に付随して、ポートLEDを点滅させることにより、視覚的に知らせる機能を有すること。
	(15)	製品間で管理専用ネットワークを自動構成し、ネットワークの管理・保守作業を効率化する機能を有しており、メンバーノードとして動作可能であること。
	(16)	メンバーノードの機器交換時に、バックアップデータからファームウェア、コンフィグ、スクリプトなどを自動復元する機能を有すること。なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(17)	異なる機種間での機器交換時に、バックアップデータからコンフィグを自動復元する機能を有すること。 なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(18)	ネットワーク仮想化機能に対応していない機器の情報をメンバーノードで収集し、マスターノードに通知可能であること。
	(19)	脅威検知アプリケーションからの通知をマスターノードと共有し、マスターノード配下のメンバー機器で脅威を検知した通信を遮断可能であること。
	(20)	Telnet（クライアント/サーバー）機能およびSecure Shell（クライアント/サーバー）機能を有すること。
	(21)	Web GUI を実装し、Webブラウザーを利用した保守・管理が可能なこと。
	(22)	時刻同期を行うためにNTP（クライアント/サーバー）機能を有すること。また他のNTPサーバーに同期していない場合であっても、装置単体で権威のあるNTPサーバーとして動作することが可能なこと。
	(23)	PTPトランスペアレントクロック(IEEE1588v2)に準拠した時刻同期機能を有すること。(但しライセンス適用は可とする)
	(24)	SNMPエージェント機能を有し、SNMPv1/v2c/v3による管理が可能なこと。
	(25)	Syslogサーバーへログを転送できること。
	(26)	外部メディア（SDカード）へログを転送できること

	(27)	決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。
	(28)	SDカードにファームウェアやコンフィグファイルを直接アップロード/ダウンロード可能なこと。
	(29)	短時間でリンクダウン/アップを繰り返すポートフラッピング現象を検出し、当該ポートの自動シャットダウンが可能なこと。
	(30)	TDR (Time-Domain Reflectometry) 方式のカッパーケーブル診断機能を有すること。
	(31)	光ファイバーケーブルの受信光レベルを常時監視し、任意のしきい値を下回った場合に当該ポートのシャットダウンおよびSNMPトラップ通知が可能であること。
	(32)	装置内にファームウェアを複数保存可能なこと。
	(33)	複数の設定ファイルを異なる名前で保存可能なこと。また、それらを必要に応じて切り替えて使用することが可能なこと。
	(34)	設定ファイルを直接編集するエディター機能を有すること。
	(35)	最大消費電力が26W以下であること。
	(36)	外形寸法は341（W）×231（D）× 44（H）mm（突起部含まず）以下であり、19インチラックに収容可能であること。
	(37)	筐体の質量は2.4kg以下であること。
	(38)	動作時温度0～50℃に対応していること。
	(39)	装置前面にSD/SDHCカードスロットおよびコンソールポートを各1つ以上有すること。
	(40)	日本語取扱説明書および日本語コマンドリファレンスをインターネット上に公開していること。
	(41)	装置固有のベンダー定義MIBが存在する場合にはそのMIB仕様を公開すること。
	14.1.2	フロアスイッチ＃1
	(1)	装置単体で10/100/1000BASE-Tのインターフェースを48ポート以上有すること。
	(2)	装置単体でSFPスロットを4つ以上有すること。
	(3)	IEEE 802.3z 1000BASE-LX/SX、IEEE 802.3ab 1000BASE-T、IEEE 802.3ah 1000BASE-BX10に準拠したSFPを搭載可能なこと。
	(4)	装置単体でスイッチングファブリックは336Gbps以上であること。
	(5)	装置単体でMACアドレス登録数は16,384以上であること。
	(6)	装置単体でIEEE 802.1Qに準拠した4,094以上のVLANを設定可能なこと。
	(7)	VLANの種類として、ポートベースVLAN、IEEE 802.1QタグベースVLAN、IPサブネットベースVLAN、プロトコルベースVLAN、マルチプルVLAN、Voice VLANの各VLANに対応可能なこと。
	(8)	IEEE 802.1AX-2008 に準拠したLink Aggregation (static and dynamic) 機能を有すること。
	(9)	IEEE 802.1D-2004およびIEEE 802.1Q-2005準拠のスパニングツリー機能を有すること。

	(10)	ポートミラーリング、リモートミラーリング機能を有すること。
	(11)	RFC3619に準拠したレイヤー2のリング型冗長化機能を有すること。
	(12)	ITU-T G.8032 に準拠したレイヤー2のリング型冗長化機能を有すること。（但しライセンス適用は可とする）
	(13)	IEEE 802.1ag に準拠したイーサネットCFM機能を有すること。（但しライセンス適用は可とする）
	(14)	DHCPクライアント機能を有すること。
	(15)	特殊フレームの送受信によりループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせるなど設定した動作を自動実行可能なこと。
	(16)	ループを検知したポートLEDの点滅と全てのポートLEDの点滅を繰り返すことで、ループ検知を視覚的に知らせる機能を有すること。
	(17)	製品間で管理専用ネットワークを自動構成し、ネットワークの管理・保守作業を効率化する機能を有しており、メンバーノードとして動作可能であること。
	(18)	メンバーノードの機器交換時に、バックアップデータからファームウェア、コンフィグ、スクリプトなどを自動復元する機能を有すること。なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(19)	異なる機種間での機器交換時に、バックアップデータからコンフィグを自動復元する機能を有すること。 なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(20)	ネットワーク仮想化機能に対応していない機器の情報をメンバーノードで収集し、マスターノードに通知可能であること。
	(21)	脅威検知アプリケーションからの通知をマスターノードと共有し、マスターノード配下のメンバー機器で脅威を検知した通信を遮断可能であること。
	(22)	IEEE 802.3af準拠のPoE、およびIEEE 802.3at準拠のPoE+機能を持ったポートを48ポート以上搭載していること。
	(23)	1ポートあたり30W以上、装置全体で740W以上のPoE給電が可能であること。
	(24)	PoE給電を停止せず機器の再起動が可能であること。（但しライセンス適用は可とする）
	(25)	Telnet（クライアント/サーバー）機能およびSecure Shell（クライアント/サーバー）機能を有すること。
	(26)	Web GUI を実装し、Webブラウザーを利用した保守・管理が可能なこと。
	(27)	時刻同期を行うためにNTPクライアント機能を有すること。
	(28)	SNMPエージェント機能を有し、SNMPv1/v2c/v3による管理が可能なこと。
	(29)	Syslogサーバーへログを転送できること。
	(30)	外部メディア（USBメモリ）へログを転送できること
	(31)	決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。
	(32)	USBメモリにファームウェアやコンフィグファイルを直接アップロード/ダウンロード可能なこと。

	(33)	短時間でリンクダウン/アップを繰り返すポートフラッピング現象を検出し、当該ポートの自動シャットダウンが可能なこと。
	(34)	TDR (Time-Domain Reflectometry) 方式のカッパーケーブル診断機能を有すること。
	(35)	光ファイバーケーブルの受信光レベルを常時監視し、任意のしきい値を下回った場合に当該ポートのシャットダウンおよびSNMPトラップ通知が可能であること。
	(36)	装置内にファームウェアを複数保存可能なこと。
	(37)	複数の設定ファイルを異なる名前で保存可能なこと。また、それらを必要に応じて切り替えて使用することが可能なこと。
	(38)	設定ファイルを直接編集するエディター機能を有すること。
	(39)	最大消費電力が1100W以下であること。
	(40)	最大消費電力が1100W以下であること。
	(41)	外形寸法は441（W）×359（D）×44（H）（突起部含まず）以下であり、19インチラックに収容可能であること。
	(42)	筐体の質量は5.8kg以下であること。
	(43)	動作時温度0～50℃に対応していること。
	(44)	装置前面にUSBポートおよびコンソールポートを各1つ以上有すること。
	(45)	日本語取扱説明書および日本語コマンドリファレンスをインターネット上に公開していること。
	(46)	装置固有のベンダー定義MIBが存在する場合にはそのMIB仕様を公開すること。
	14.1.3	フロアスイッチ＃2
	(1)	装置単体で10/100/1000BASE-Tのインターフェースを48ポート以上有すること。
	(2)	装置単体でSFPスロットを4つ以上有すること。
	(3)	IEEE 802.3z 1000BASE-LX/SX、IEEE 802.3ab 1000BASE-T、IEEE 802.3ah 1000BASE-BX10に準拠したSFPを搭載可能なこと。
	(4)	装置単体でスイッチングファブリックは336Gbps以上であること。
	(5)	装置単体でMACアドレス登録数は16,384以上であること。
	(6)	装置単体でIEEE 802.1Qに準拠した4094以上のVLANを設定可能なこと。
	(7)	VLANの種類として、ポートベースVLAN、IEEE 802.1QタグベースVLAN、IPサブネットベースVLAN、プロトコルベースVLAN、マルチプルVLAN、Voice VLANの各VLANに対応可能なこと。
	(8)	IEEE 802.1AX-2008 に準拠したLink Aggregation (static and dynamic) 機能を有すること。
	(9)	IEEE 802.1D-2004およびIEEE 802.1Q-2005準拠のスパニングツリー機能を有すること。
	(10)	ポートミラーリング、リモートミラーリング機能を有すること。

	(11)	RFC3619に準拠したレイヤー2のリング型冗長化機能を有すること。
	(12)	ITU-T G.8032 に準拠したレイヤー2のリング型冗長化機能を有すること。（但しライセンス適用は可とする）
	(13)	IEEE 802.1ag に準拠したイーサネットCFM機能を有すること。（但しライセンス適用は可とする）
	(14)	DHCPクライアント機能を有すること。
	(15)	特殊フレームの送受信によりループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせるなど設定した動作を自動実行可能なこと。
	(16)	ループを検知したポートLEDの点滅と全てのポートLEDの点滅を繰り返すことで、ループ検知を視覚的に知らせる機能を有すること。
	(17)	製品間で管理専用ネットワークを自動構成し、ネットワークの管理・保守作業を効率化する機能を有しており、メンバーノードとして動作可能であること。
	(18)	メンバーノードの機器交換時に、バックアップデータからファームウェア、コンフィグ、スクリプトなどを自動復元する機能を有すること。なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(19)	異なる機種間での機器交換時に、バックアップデータからコンフィグを自動復元する機能を有すること。 なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(20)	ネットワーク仮想化機能に対応していない機器の情報をメンバーノードで収集し、マスターノードに通知可能であること。
	(21)	脅威検知アプリケーションからの通知をマスターノードと共有し、マスターノード配下のメンバー機器で脅威を検知した通信を遮断可能であること。
	(22)	Telnet（クライアント/サーバー）機能およびSecure Shell（クライアント/サーバー）機能を有すること。
	(23)	Web GUI を実装し、Webブラウザーを利用した保守・管理が可能なこと。
	(24)	時刻同期を行うためにNTPクライアント機能を有すること。
	(25)	SNMPエージェント機能を有し、SNMPv1/v2c/v3による管理が可能なこと。
	(26)	Syslogサーバーへログを転送できること。
	(27)	外部メディア（USBメモリ）へログを転送できること
	(28)	決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。
	(29)	USBメモリにファームウェアやコンフィグファイルを直接アップロード/ダウンロード可能なこと。
	(30)	短時間でリンクダウン/アップを繰り返すポートフラッピング現象を検出し、当該ポートの自動シャットダウンが可能なこと。
	(31)	TDR (Time-Domain Reflectometry) 方式のカッパーケーブル診断機能を有すること。
	(32)	光ファイバーケーブルの受信光レベルを常時監視し、任意のしきい値を下回った場合に当該ポートのシャットダウンおよびSNMPトラップ通知が可能であること。
	(33)	装置内にファームウェアを複数保存可能なこと。

	(34)	複数の設定ファイルを異なる名前で保存可能なこと。また、それらを必要に応じて切り替えて使用することが可能なこと。
	(35)	設定ファイルを直接編集するエディター機能を有すること。
	(36)	最大消費電力が54W以下であること。
	(37)	最大消費電力が54W以下であること。
	(38)	外形寸法は441（W）×323（D）×44（H）mm（突起部含まず）以下であり、19インチラックに収容可能であること。
	(39)	筐体の質量は4.5kg以下であること。
	(40)	動作時温度0～50℃に対応していること。
	(41)	装置前面にUSBポートおよびコンソールポートを各1つ以上有すること。
	(42)	日本語取扱説明書および日本語コマンドリファレンスをインターネット上に公開していること。
	(43)	装置固有のベンダー定義MIBが存在する場合にはそのMIB仕様を公開すること。
	14.1.4	メインスイッチ
	(1)	装置単体で10/100/1000BASE-Tのインターフェースを24ポート以上有すること。
	(2)	装置単体でSFP/SFP+スロットを4つ以上有すること。
	(3)	IEEE 802.3z 1000BASE-LX/SX、IEEE 802.3ab 1000BASE-T、IEEE 802.3ah 1000BASE-BX10に準拠したSFPを搭載可能なこと。
	(4)	IEEE 802.3ae 10GBASE-ER/LR/SR、IEEE 802.3an 10GBASE-Tに準拠したSFP+(Small Form-factor Pluggable+)を搭載可能なこと。
	(5)	IEEE 802.3ae 10GBASE-Rに準拠した最大伝送距離80kmのSFP+(Small Form-factor Pluggable+)を搭載可能なこと。
	(6)	装置単体でスイッチングファブリックは253Gbps以上であること。
	(7)	装置単体でMACアドレス登録数は16,384以上であること。
	(8)	装置単体でIEEE 802.1Qに準拠した4,094以上のVLANを設定可能なこと。
	(9)	VLANの種類として、ポートベースVLAN、IEEE 802.1Qタグベース VLAN、IPサブネットベースVLAN、プロトコルベースVLAN、マルチプルVLAN、Voice VLANの各VLANに対応可能なこと。
	(10)	IEEE 802.1AX-2008 に準拠したLink Aggregation (static and dynamic) 機能を有すること。
	(11)	IEEE 802.1D-2004およびIEEE 802.1Q-2005準拠のスパニングツリー機能を有すること。
	(12)	ポートミラーリング、リモートミラーリング機能を有すること。
	(13)	RFC3619に準拠したレイヤー2のリング型冗長化機能を有すること。
	(14)	ITU-T G.8032 に準拠したレイヤー2のリング型冗長化機能を有すること。（但しライセンス適用は可とする）

	(15)	IEEE 802.1ag に準拠したイーサネットCFM機能を有すること。（但しライセンス適用は可とする）
	(16)	ソフトウェアを変更することなく、スタティックルーティング、RIPv1/v2、RIPng、OSPFv2、OSPFv3、PIM-SSMv4、PIM-SMv4、PIM-DMv4、PIM-SMv6、、PIM-SSMv6、BGP機能を有すること。（但しライセンス適用は可とする）
	(17)	DHCPサーバー機能を有すること。
	(18)	DHCPリレー機能を有すること。
	(19)	スタックケーブルで機器間(最大8台)を接続することにより、仮想的に1台の装置として扱うことができる、スタック機能(以下、スタック)を有すること。
	(20)	スタック接続されている装置間では、コンフィグ、FDB、ARPテーブル、IPルーティングテーブル等の各種情報を同期することが可能なこと。
	(21)	スタック接続した際は装置間の帯域を80Gbps（双方向）以上有すること。
	(22)	最大80kmの長距離スタックが可能なこと。
	(23)	スタック構成時、状態確認用の予備リンク(レジリエンシーリンク)を構成できること。
	(24)	特殊フレームの送受信によりループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせるなど設定した動作を自動実行可能なこと。
	(25)	ループを検出した際の動作に付随して、ポートLEDを点滅させることにより、視覚的に知らせる機能を有すること。
	(26)	製品間で管理専用ネットワークを自動構成し、ネットワークの管理・保守作業を効率化する機能を有しており、メンバーノードとして動作可能であること。
	(27)	メンバーノードの機器交換時に、バックアップデータからファームウェア、コンフィグ、スクリプトなどを自動復元する機能を有すること。なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(28)	異なる機種間での機器交換時に、バックアップデータからコンフィグを自動復元する機能を有すること。 なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。
	(29)	ネットワーク仮想化機能に対応していない機器の情報をメンバーノードで収集し、マスターノードに通知可能であること。
	(30)	脅威検知アプリケーションからの通知をマスターノードと共有し、マスターノード配下のメンバー機器で脅威を検知した通信を遮断可能であること。
	(31)	Telnet（クライアント/サーバー）機能およびSecure Shell（クライアント/サーバー）機能を有すること。
	(32)	時刻同期を行うためにNTP（クライアント/サーバー）機能を有すること。また他のNTPサーバーに同期していない場合であっても、装置単体で権威のあるNTPサーバーとして動作することが可能なこと。
	(33)	SNMPエージェント機能を有し、SNMPv1/v2c/v3による管理が可能なこと。
	(34)	Syslogサーバーへログを転送できること。
	(35)	外部メディア（USBメモリ）へログを転送できること
	(36)	決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。

	(37)	インターネットに接続された環境において、ライセンスをオンラインで更新可能なこと。
	(38)	USBメモリにファームウェアやコンフィグファイルを直接アップロード/ダウンロード可能なこと。
	(39)	短時間でリンクダウン/アップを繰り返すポートフラッピング現象を検出し、当該ポートの自動シャットダウンが可能なこと。
	(40)	TDR (Time-Domain Reflectometry) 方式のカッパーケーブル診断機能を有すること。
	(41)	光ファイバーケーブルの受信光レベルを常時監視し、任意のしきい値を下回った場合に当該ポートのシャットダウンおよびSNMPトラップ通知が可能であること。
	(42)	装置内にファームウェアを複数保存可能なこと。
	(43)	複数の設定ファイルを異なる名前で保存可能なこと。また、それらを必要に応じて切り替えて使用することが可能なこと。
	(44)	設定ファイルを直接編集するエディター機能を有すること。
	(45)	最大消費電力が43W以下であること。
	(46)	固定式冗長電源を有しており、電源の冗長が可能なこと。
	(47)	外形寸法は441（W）×323（D）×44（H）mm（突起部含まず）以下であり、19インチラックに収容可能であること。
	(48)	筐体の質量は4.4kg以下であること。
	(49)	動作時温度0～50℃に対応していること。
	(50)	装置前面にUSBポートおよびコンソールポートを各1つ以上有すること。
	(51)	日本語取扱説明書および日本語コマンドリファレンスをインターネット上に公開していること。
	(52)	装置固有のベンダー定義MIBが存在する場合にはそのMIB仕様を公開すること。
	14.1.5	ネットワーク統合管理ソフトウェア
	(1)	Windows 10 Pro（64ビット版）、Windows 10 Pro Education（64ビット版）、Windows Server 2016 日本語版（Standard、Datacenterエディションのみサポート）、Windows Server 2019 日本語版（Standard、Datacenter、Essentialsエディションをサポート）のOS上で動作可能であること。
	(2)	Microsoft Windows Server 2016 Hyper-V、Microsoft Windows Server 2019 Hyper-Vに対応可能なこと。
	(3)	VMware vSphere ESXi 6.5/6.7の仮想化環境に対応可能なこと。
	(4)	サブネット上のSNMPエージェントを自動探索し、ツリーによる接続構成表示、機器の一覧表示、機器/ポート状態の周期監視（ポーリング）、監視対象機器の追加/削除が可能であること。
	(5)	ループ検出などによるトラップ通知をネットワーク仮想化機能のトポロジーマップ上に表示し、視覚的に把握可能であること。

	(6)	統計情報を折れ線グラフとして表示し、MIB変数の折れ線の表示/非表示を切り替えることが可能なこと。また、折れ線グラフの任意の点にマウスポインターを置くと、該当時点の日時とMIB変数の参照値がポップアップ表示されること。
	(7)	起動時コンフィグをバックアップし、バックアップしたコンフィグの内容の差分を比較することができること。
	(8)	ネットワーク機器が生成・送信するSyslog情報を収集し、リスト表示可能なSyslogサーバー機能を有していること。ただし追加ライセンスは不可とする。
	(9)	ネットワーク仮想化機能に障害が発生した場合に、サーバーのローカル環境からSNMP管理機能のWeb管理画面に直接アクセス可能な、スタンドアローンモードに対応していること。
	(10)	ネットワーク仮想化機能で管理しているスイッチ、ルーターを自動認識し、トポロジーマップの自動生成が可能であること。
	(11)	マップ上のノードを最大3階層のサイトで分類したり、表示/非表示の切り替えが可能なこと。
	(12)	ネットワーク仮想化機能で管理しているスイッチ、ルーターへのCLI接続が可能なこと。
	(13)	ネットワーク仮想化機能で管理しているスイッチ、ルーターに異常が発生した際は、管理者へ視覚的に通知できること。
	(14)	ネットワーク仮想化機能で管理しているスイッチ、ルーターの一覧表示および検索が可能であること。
	(15)	ネットワーク仮想化機能で管理している機器のVLAN情報の設定と可視化を可能にするVLANマップ機能を有すること。
	(16)	ネットワーク仮想化機能で管理しているスイッチに、ループガード機能の設定が可能なこと。また、1度に10台までの機器を選択して同時に設定が可能なこと。
	(17)	ネットワーク仮想化機能で管理している機器間のリンク速度やトラフィック量を可視化するトラフィックマップ機能を有すること。また通信プロトコルごとに帯域利用状況を把握できること。
	(18)	センタールーターと複数拠点ルーターが相互接続している環境において、ネットワーク仮想化機能で管理している機器間のWANトラフィック量を監視し、拠点側からセンター側へのトラフィックが集中した場合に自動的に帯域を制御することができること。
	(19)	ネットワーク仮想化機能で管理しているルーターに対し、ネットワークマップ上からルーター間を線で結ぶような簡単な操作で当該箇所にVPNトンネルを構成することができること。
	(20)	ネットワーク仮想化機能で管理しているルーターに対し、WAN通信のアプリケーション毎の通信優先度が設定可能なこと。
	(21)	ネットワーク仮想化機能で管理しているルーターに対し、アプリケーションごとにインターネットブレークアウトの要否を設定することが可能であること。また、管理下のルーターで判定されたDPIの結果を、同じく管理下にある対向のルーターと共有できること。
	(22)	ネットワーク仮想化機能で管理しているルーターに対し、業種を指定するだけで、業種ごとの推奨セキュリティ設定を設定可能なこと。
	(23)	ネットワーク仮想化機能で管理している無線LANアクセスポイントの機器交換時に自動復元する機能を有すること。
	(24)	無線LANアクセスポイントを実際の環境に応じてフロアマップ上に配置させ、表示することで視覚的に管理できること。

	(25)	無線チャンネルの表示（色によってチャンネル種別を表現）や無線電波出力の表示（大きさによって出力を表現）が可能であること。
	(26)	フロアマップ上で接続無線クライアントの一覧および位置情報含めた詳細表示、接続無線クライアントの履歴管理が可能なこと。
	(27)	ヒートマップの3D表示が可能であり、無線の電波強度を多次元的に管理できること。
	(28)	無線LANアクセスポイントの一覧表示および検索が可能であること。
	(29)	管理下の無線LANコントローラー機能を内蔵しているスイッチおよびルーターと連携し、無線LANコントローラー機能を内蔵しているスイッチおよびルーターからMACアドレスに基づいて接続可能な無線クライアントを管理する機能を有すること。
	(30)	電波出力・チャンネル自動調整機能にて、管理対象無線アクセスポイント周囲の無線利用状態を収集し、常に最適なチャンネル/電波出力を分析し、分析結果をアクセスポイントに適用する機能を有すること。
	(31)	セル型とブランケット型の無線LANサービスを同時利用可能であること。
	(32)	ブランケット型運用時において、互いに電波干渉しない複数の無線端末は、異なる無線LANアクセスポイントを利用して同時に通信が可能なこと。
	(33)	事前登録済みの無線LANアクセスポイントを設置して電源を入れるだけで利用でき、LANケーブルを接続せずに設置や増設が可能なこと。
	(34)	無線LANアクセスポイント間の無線接続は、自動的に冗長経路が構成され、無線経路がダウンしても、すばやく冗長経路に切り替えが可能なこと。
	(35)	チャンネル自動調整に使用する選択候補のチャンネルを設定変更できること。
	(36)	管理対象アクセスポイントのチャンネルおよび電波出力が自動調整、固定設定が混在している場合でも最適化可能なこと。
	(37)	電波出力・チャンネルの分析結果の適用は、スケジュール登録による任意のタイミングでの調整実施可能なこと。
	(38)	管理対象とする無線LANアクセスポイントの登録のほか、ログインユーザー名/パスワードなどを直接設定できること。また、複数台の無線LANアクセスポイントをCSVファイルで一括して登録できること。
	(39)	無線LANアクセスポイントの設定情報の一部を共通化して管理できること。共通設定を無線LANアクセスポイントへ一括適用することで誤設定の防止や、設定工数の削減ができること。
	(40)	無線LANコントローラ再起動の場合など、無線LANコントローラと無線LANアクセスポイント間で通信が一時的に不通になったとしても、無線サービスの提供を継続することが可能であること。
	(41)	通信スピードに関わらず接続されている全てのクライアントに同じ通信時間（エアタイム）を提供できる機能を有すること。
	(42)	2.4GHz・5GHz帯の両方をサポートしている無線クライアントに対して、適切な帯域への接続を優先するように促す機能を有すること。
	(43)	無線LANアクセスポイントに接続するクライアント端末に対し、MAC アドレス認証を行えること。
	(44)	無線LANアクセスポイントに接続するクライアント端末に対し、WPA/WPA2/WPA3 Enterprise認証を行えること。

	(45)	無線LANアクセスポイントに接続するクライアント端末に対し、キャプティブポータルによる認証が可能なこと。
	(46)	事前に定義した時間帯に、設定の変更やファームウェアのバージョンアップが行えるスケジューリング機能を有し、スケジュールされたタスクの自動実行ができること。
	(47)	管理外の無線LANアクセスポイントの検知および当該外来波の情報をGUI上で確認できること。
	(48)	無線LANアクセスポイントに接続しているクライアントの接続状況が把握できること。
	(49)	無線アクセスポイントが検知したクライアントの推定位置情報をGUI上に表示できること。
	(50)	無線LANアクセスポイントの基本情報、使用チャンネル、送信出力、接続無線クライアント数、統計情報などを表示できること。
	(51)	複数の無線LANアクセスポイントに対し、緊急時用として設定されているSSIDの一括での有効化/無効化が可能な機能を有すること。
	(52)	MACアドレスリストを利用したMACアドレスフィルタリング機能(MAC認証とは排他利用)を有すること。
	(53)	不正な無線APからのSSID Spoofing/Security Spoofingの検出、不正な無線クライアントの検出、De-Authentication Attackに対応していること。
	(54)	日本語/英語の言語選択が可能なこと。
	(55)	ユーザーの作成、削除、閲覧可能エリアの指定、最終ログイン日時表示が可能なこと。
	(56)	有線ネットワークおよび無線ネットワークをグラフィカルに集約して一元管理が可能なこと。
	(57)	システムのバックアップ、リストア、初期化が可能なこと。
	(58)	管理している無線LANアクセスポイントのログ表示が可能であること。また、ログはCSV形式で出力可能なこと。
	(59)	SNMPエージェントに対応する機器の詳細情報を取得して、統計情報のグラフ表示が可能であること。
	(60)	指定したサブネット内のネットワーク機器を自動的に探索、接続構成ツリーを作成できること。また、ホスト名やIPアドレスを指定してデバイスを手動で追加可能であること。
	(61)	ネットワークの構成要素（サブネット、デバイス、ポートなど）をツリー形式で階層的に表示、アイコンにより各要素の種類や状態を一目で把握可能であること。
	(62)	イベントフィルターによるアクション設定（メール送信、コマンド（外部アプリケーション）の実行）が可能であること。
	(63)	特定のイベント発生時に指定したアクション(メール通知及びマップ上でのアラーム表示)を実行できること。
	(64)	無線LANアクセスポイントは、最大3000台まで管理可能なこと。
	(65)	SNMPエージェントは、最大2000台まで管理可能なこと。
	(66)	初回使用時に90日間、全機能を利用可能な試用ライセンスを適用可能なこと。
	(67)	ソフトウェア製品であること。
	(68)	日本語マニュアルをインターネット上に公開していること。

14．2ソフトウェア		
	14.2.1	ソフトウェア
	(1)	国産製品であること
	(2)	ホームページの改竄やマルウェア感染の疑いのあるお客様へ通知する無償サービスを提供していること
	(3)	情報セキュリティやITマナーなどの情報教育の支援機能を有すること
	(4)	社内通達や法令遵守啓発等の告知をブラウザー上に表示するインフォメーション機能を有すること
	(5)	安全なWebサイトにのみアクセスできるホワイト運用が可能なDBを搭載していること
	(6)	DBのURL登録数が150億以上あること
	(7)	ファイルの拡張子をリスク別にダウンロード制限が可能であり、Webサイトにアクセスしただけでマルウェアに感染してしまう攻撃の対策ができること。なお、OSやアプリケーションのアップデートなどに利用されるサイトのダウンロードは許可でき、利便性を損なわずにセキュリティを担保できること。
	(8)	安全を確認できていないURLにクレデンシャル（認証情報）を送信することをブロックでフィッシングサイト対策ができること
	(9)	出口対策用のDBを有し、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 ・専任のセキュリテイアナリストよって分析精査された情報
	(10)	出口対策用のDBを有し、以下の内容が含まれていること ・メーカー独自に収集した、改ざんが行なわれている脆弱なWebサイトのIPアドレス/URLリスト
	(11)	脅威情報への通信が発生した際に、管理者にメール通知が可能なこと
	(12)	脅威情報以外に、IT不正技術カテゴリなど、メール通知したいカテゴリを設定できること
	(13)	任意のルールでクライアント端末をインターネット利用できないように隔離することが可能なこと
	(14)	デコードなしでSSLセッションを張っている怪しい通信を一定期間で自動切断することが可能なこと
	(15)	Webサービスを機能ごと・組織ごとに制御する機能を有すること
	(16)	Webサービスごとに「ログイン、書き込み、アップロード」等の機能を制御でき、設定画面上で簡潔に設定できること
	(17)	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
	(18)	管理者画面の二段階認証を行うことで不正ログイン防止を強化できること
	(19)	企業アカウントと個人アカウントが異なるWebサービスの場合に、個人アカウントでの利用を制御できること
	(20)	Webサイトへのデータ送信(POST)規制ができること
	(21)	データ送信(POST)規制は、「パスワード解除」「警告のみ」「監視」と併用して設定が可能なこと

	(22)	必要に応じてPOSTされた添付ファイルを復元し、どのURLにどんなファイルをPOSTしたか調べることができること
	(23)	POSTのログが一括エクスポートできること
	(24)	FQDNだけでなく下位のページのURLでもフィルタリングが可能であり、ログに残ること
	(25)	セーフサーチ（検索エンジンによる検索結果制御機能）の強制的な設定が可能であること
	(26)	セーフサーチの対象サイトがDB配信され、対象サイトの仕様変更があった場合でも、製品をバージョンアップすることなく継続的に強制化が可能であること
	(27)	PICS規格のラベル情報を含んでいる場合のPICSレベル閾値設定が可能
	(28)	メーカーが推奨するフィルタリング設定のテンプレートが用意されていること
	(29)	日本の組織に応じたグループ・ユーザー管理ができそれを基にフィルタリグルールの設定ができること
	(30)	URLリストをインポートすると、URLが整理された状態で、ユーザー毎に登録可能なURLカテゴリとして利用可能であること
	(31)	ACLでのフィルタリグルールの設定ができること
	(32)	ブロック画面をカスタマイズできること
	(33)	クライアント端末の言語設定を自動判定してブロック画面の言語を切り替えられること
	(34)	SSLデコード対象をWebサービスに限定し、ルールパーツで条件設定が可能なこと
	(35)	Windows UpdateなどのSSLデコードが必要ないURLをDB配信でき管理者の負荷軽減が可能なこと
	(36)	HTTP/HTTPSキャッシュ（ディスク/メモリキャッシュ）の利用可否をホスト単位やグループ単位で設定でき、複数台サーバーで共有可能なこと
	(37)	HTTP/認証/DNS等のキャッシュを管理GUI上で削除でき、メモリキャッシュはホスト単位でのキャッシュクリアにも対応していること。また、SSL Adapter利用時にSSL代理証明書キャッシュを、保存期間の指定により削除が可能なこと
	(38)	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
	(39)	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
	(40)	難読レベルを調整可能なCAPTCHA認証を利用できること
	(41)	ユーザーアカウントへの辞書攻撃の防止を目的とした、認証エラー時のロック機能を有すること
	(42)	管理画面にアクセスするパスワードのポリシー（英数字や大文字の組合せなど）、パスワードの有効期間、複数回パスワードエラー時にロックするなどが設定可能なこと
	(43)	アクセスログの出力フォーマットがカスタマイズ可能で、ポリシーごとに適用するフォーマットも変更できること
	(44)	アクセスしたWebサイトのページタイトルをアクセスログ上に表示可能なこと
	(45)	レポート機能が無償で付属されており、外部DBを用意せず利用可能なこと

	(46)	ドリルダウン操作により、複数の条件を掛け合わせた任意のレポートを表示可能なこと
	(47)	グループごとに有効期間が指定でき、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、テンポラリのグループ作成が可能なこと
	(48)	多段構成の場合でも、下位プロキシのIPアドレスに加え、接続元であるクライアント端末のIPアドレス/識別子でグルーピングが可能なこと
	(49)	ユーザーのWeb利用の時間制限ができること
	(50)	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
	(51)	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
	(52)	Outgoing IPを個社ごとに専有IPアドレスに固定化できること
14. 3ネットワーク構築作業		
	14.3.1	ネットワーク構築作業
	(1)	構築するネットワークの構成は、現行の構成を踏襲すること。
	(2)	導入するアクセスポイントは電子カルテ用として使用するが、現行の情報系用の光回線を経由してインターネットへ接続できるような設定にすること。
	(3)	各ベンダーがリモートメンテナンスを行える環境を構築すること。
14. 4保守		
	14.4.1	ネットワーク機器保守
	(1)	導入するネットワーク機器にはすべて保守を付帯すること。また保守対応時間は、平日の9時から17時とすること。
	(2)	メンテナンス保守費用を含むこと。保守対応時間は平日の9時から17時30分までとすること。