

(別紙2)

常総市情報通信ネットワーク機器賃貸借  
機器仕様書

令和8年5月

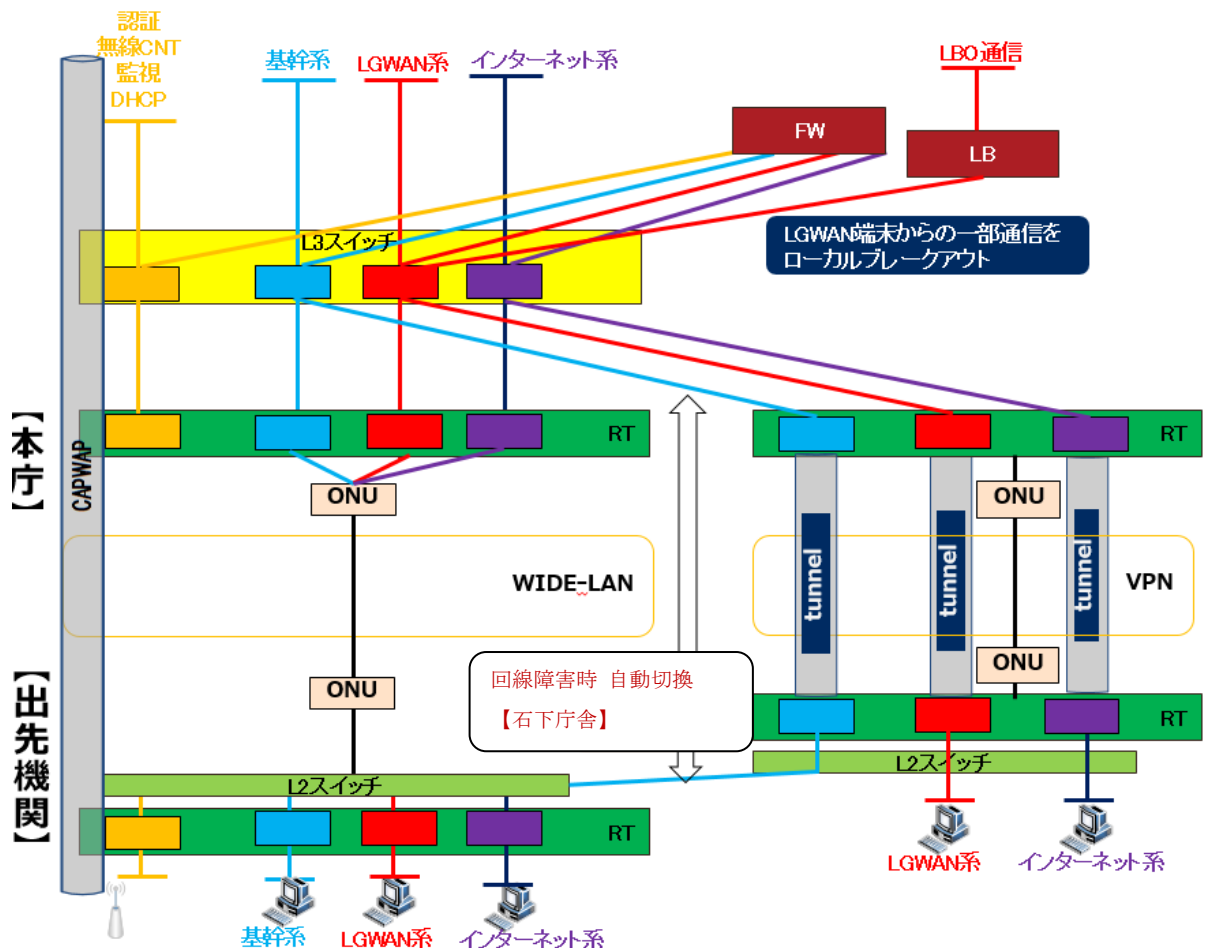
常総市

#### <ネットワークの構成>

- ・ ギガビットイーサネットをバックボーンとするネットワークを構築するものとする。
- ・ 基幹系・LGWAN系・インターネット系の3系統とし、論理的に分割したネットワークとして構築するものとする。
- ・ 基幹系・LGWAN系・インターネット系のそれぞれの構成は、基本的にセンタースイッチ・フロアスイッチ・エッジスイッチの構成とする。
- ・ 本庁舎及び一部出先機関のLGWAN系・インターネット系に、無線LANを導入する。
- ・ 無線LANアクセスポイントは、POEスイッチより給電し、コンセント工事を不要とする。
- ・ センタースイッチに接続する各スイッチ間は、光ケーブル又はUTPを用いた複数のリンクで接続するものとする。
- ・ センタースイッチはサーバ室に設置し、各スイッチからの配線を収容するものとする。
- ・ フロアスイッチはセンタースイッチに接続し、各フロア又はその一部に設置し、エッジスイッチを収容するものとする。
- ・ エッジスイッチはフロアスイッチに接続し、各端末を収容するものとする。
- ・ ネットワーク障害を防止する機能（ループ接続防止機能等）を搭載するものとする。また、ネットワーク監視障害検知及び通報する仕組みを構築するものとする。
- ・ 基幹系については、停電時でも業務が継続できるよう、ネットワーク機器及びクライアントPCの一部に、無停電電源装置を導入するものとする。
- ・ ネットワークのセグメントは、基幹系・LGWAN系・インターネット系・戸籍系・国保連合会系・広域連合系・教育系の7系統とし、論理的に分割するものとする。
- ・ 戸籍系・国保連合会系・広域連合系・教育系のネットワークは、他事業者で提供・管理されており、今回構築するネットワーク内を通じ、必要な場所にL2延伸させるものとする。
- ・ 全てのLGWAN系クライアントPCは、IBBN（茨城ブロードバンドネットワーク）経由でインターネットへ接続できるものとする。なお、基幹系・戸籍系・国保連合会系・広域連合系は、インターネットへの接続を認めないものとする。
- ・ 今後のクラウド利用の増加に伴いネットワーク負荷増大対策として特定通信をインターネットにアクセスできるようにセキュリティゲートウェイを導入する。
- ・ サーバ室と石下庁舎間はバックアップ回線を準備しており、障害発生時には、自動でバックアップ回線に切替えができる仕組みを構築するものとする。
- ・ センタールータは、基幹系・LGWAN系・インターネット系に対し、論理分割を維持しながら、1台で収容できるものとする。
- ・ 出先ルータは、基幹系・LGWAN系・インターネット系に対し、論理分割を維持しながら、1台で収容できるものとする。
- ・ 基幹系・LGWAN系・インターネット系をまたぐ通信は、特定通信として限定的に許可できる仕組みを構築するものとする。なおこの仕組みは、1か所で対応可能とすること。
- ・ 今年度中に水道課にIBBN経由にて県庁NWを導入の必要があるため、NW移行作業前に既存のNWに設定変更を行うこと。必要な場合既存事業者よりNW設定変更の見積依頼を行うこと。既存NW事業者の見積依頼窓口は、要求がある場合市より連絡するものとする。

## ＜全体構成＞

○全体の構成例を以下に示す。



## ＜無線 LAN の更新＞

- ・ 本庁舎（議会棟・第 2 分庁舎・第 3 分庁舎を含む。）及び一部出先機関（石下庁舎・保健センター・水道事業所・図書館・豊岡学校給食センター・玉学校給食センター・きぬふれあいセンター）の LGMAN 系とインターネット系に無線 LAN を導入し、LGMAN 系クライアント PC とインターネット系クライアント PC が、無線 LAN を利用できる環境を構築するものとする。
- ・ 無線 LAN アクセスポイントコントローラーによる、無線 LAN アクセスポイントの集中管理が可能となる仕組みを構築するものとする。
- ・ 無線 LAN アクセスポイントコントローラーは、運用工数を考慮しアプライアンス製品とする。
- ・ 無線出力を周囲の環境に応じて、自動で調整できるものとする。
- ・ 無線チャンネルを周囲の環境に応じて、自動で調整できるものとする。
- ・ 無線 LAN アクセスポイントは、IEEE802.11ax/ac/n/a/g/b/に対応するものとする。
- ・ 本庁舎・議会棟・石下庁舎・図書館に設置されている、既存の公衆無線 LAN 用のアクセスポイントの更新を行うものとする。

#### <監視機能の導入>

- ネットワーク機器の障害検知を可能とする仕組みを構築するものとする。
- 障害検知は、パトライト等で通報できるものとする。
- 死活監視を実施し、ネットワーク機器の障害に備えるものとする。
- SNMPトラップにより、ネットワーク機器のインターフェース障害に備えるものとする。
- 標準 MIB およびプライベート MIB 情報があらかじめテンプレート化されていて、Web GUI 画面上での操作によって容易に設定し情報収集が可能であること。
- 監視項目の設定については、予めツールによって定義された監視項目の優先度をもとに自動登録する機能を有すること。
- Web GUI による各種設定やグラフ情報の確認が可能であること。また、操作画面は日本語および英語表示が可能であること。
- 監視対象ホストはすべてのネットワーク機器（公衆無線 LAN 用アクセスポイントを除く。）の死活監視を実施するものとする。
- 監視対象ホストのトラフィックやインターフェイス（エラー値/パケット数等）情報を SNMP で監視可能であること。対象ホストの MIB 情報が対応している場合は、リソース情報(CPU/メモリー値 等)も含めるものとする。
- 監視間隔は監視項目単位にて、1 分～10 分の間で任意に変更ができること。

#### <ネットワークのセキュリティ>

- インターネット向け通信のセキュリティ強化として、ファイアウォールの UTM 機能（アンチウィルス・IPS）を利用し、不正な通信を遮断し、より高度なセキュリティ対策を実施するものとする。
- 無線 LAN における暗号化方式として「CCMP（AES）」を採用し、高セキュリティな無線ネットワークを構築するものとする。
- 有線 LAN における認証方式として LGWAN 系では「EAP-TLS」を採用する。  
プリンタなどの証明書インストールが不可の機器に関しては MAC アドレス認証を採用する。
- ネットワーク認証（IEEE802.1X 認証）には、電子証明書を用いたセキュリティレベルの高い「EAP-TLS」を採用するものとする。
- 無線 LAN を利用する各クライアント PC は、認証装置（NetAttest EPS）により、認証されたもののみ接続できるよう構築するものとする。
- 基幹系・LGWAN 系・インターネット系間の特定通信が発生した場合は、情報漏洩防止の観点で、ファイアウォール機能による通信制御を行うものとする。

#### <セキュリティゲートウェイの導入>

- LGWAN 系端末から特定のクラウドへセキュアな通信を可能とすること
- LBO 通信（Microsoft365 系）通信対象 URL を自動取り込みが可能なこと。
- セキュリティゲートウェイを経由する LBO 通信（Microsoft365 系）はテナント制限を実施し常総市ドメインのみ接続可能とすること。

#### <ネットワークの必要最低限の冗長化>

- サーバ室に設置するセンタースイッチは、2 台のスタック接続等により、冗長化を図るものとする。

- ・ サーバ室に設置するファイアウォールは、HA 構成で冗長化を図るものとする。
- ・ 無線 LAN アクセスポイントコントローラーは 2 台で冗長化し、1 台の無線 LAN アクセスポイントコントローラーに障害が生じた場合でも、無線 LAN が継続して稼働するものとする。
- ・ DHCP サーバは 2 台で冗長化し、1 台の DHCP サーバに障害が生じた場合でも、端末に IP アドレスの払い出しが行われるものとする。
- ・ サーバ室に設置するセンタースイッチとルータの間は、リンクアグリゲーションによる、LAN の冗長化を図るものとする。
- ・ サーバ室に設置するセンタースイッチとファイアウォールの間は、リンクアグリゲーションによる、LAN の冗長化を図るものとする。

#### ＜機器仕様＞

##### ○センター（メイン）スイッチ

- ・ 10/100/1000BASE-T を 24 ポート有すること。
- ・ 10GbE SFP+スロットを 4 ポート有すること。
- ・ コンソールポートを有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 9 台であること。
- ・ 802.1x 認証に対応すること。
- ・ VRF 機能を有すること。

##### ○サーバスイッチ

- ・ 10/100/1000BASE-T を 48 ポート有すること。
- ・ 10GbE SFP+スロットを 4 ポート有すること。
- ・ コンソールポートを有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 6 台であること。
- ・ 802.1x 認証に対応すること。

##### ○基幹系フロアスイッチ（本庁舎）

- ・ 現行の幹線 LAN を利用し構築すること。
- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 10GbE SFP+スロットを 4 ポート有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 6 台であること。

##### ○基幹系フロアスイッチ（議会棟・第 3 分庁舎）

- ・ 現行の幹線 LAN を利用し構築すること。
- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 4 台であること。

##### ○基幹系エッジスイッチ（本庁舎内各課）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 4 台であること。

○基幹系フロアスイッチ（石下庁舎）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 4 台であること。

○基幹系エッジスイッチ（石下庁舎）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 4 台であること。

○基幹系エッジスイッチ（出先機関 ※石下庁舎以外）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。

○OLGWAN 系フロアスイッチ（本庁舎・議会棟・第 3 分庁舎）

- ・ 現行の幹線 LAN を利用し構築すること。
- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 802.1X 認証及び、MAC アドレス認証に対応していること。
- ・ SFP スロットを 2 ポート以上有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ IRF スタック最大数は 4 台であること。
- ・ 1 ポートあたりの最大供給電力が 30.0W 以上であること。ただし、供給ポート数は装置あたりの最大電力によるものとする。

○OLGWAN 系エッジスイッチ（本庁舎・議会棟・第 3 分庁舎内各課）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 802.1X 認証及び、MAC アドレス認証に対応していること。

○OLGWAN 系フロアスイッチ（石下庁舎）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック最大数は 4 台であること。
- ・ 1 ポートあたりの最大供給電力が 30.0W 以上であること。ただし、供給ポート数は装置あたりの最大電力によるものとする。

○OLGWAN 系エッジスイッチ（石下庁舎）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 802.1X 認証及び、MAC アドレス認証に対応していること。

○OLGWAN 系エッジスイッチ（出先機関 ※石下庁舎以外）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること。
- ・ 802.1X 認証及び、MAC アドレス認証に対応していること。

○OLGWAN 系 POE スイッチ（出先機関 ※保健センター・水道事業所・図書館・豊岡学校給食センター・玉学校給食センター・きぬふれあいセンター）

- ・ 現行を収容できる 10/100/1000BASE-T ポート有すること

- 802.1X 認証及び、MAC アドレス認証に対応していること。
- 1 ポートあたりの最大供給電力が 30.0W 以上であること  
ただし、供給ポート数は装置あたりの最大電力によるものとする

#### ○センタールータ

- 10/100/1000BASE-T を 8 ポート有すること。
- シリアルコンソールポートを有すること。
- VRF 機能を有すること。
- IPsec 機能を有すること。
- IPsec 対地数 128 であること。
- IKEv2 に対応していること。

#### ○センタールータ（選挙用）

- 10/100/1000BASE-T を 4 ポート有すること。
- シリアルコンソールポートを有すること。
- VRF 機能を有すること。
- IPsec 機能を有すること。
- IPsec 対地数 128 であること。
- IKEv2 に対応していること。

#### ○出先ルータ（広域イーサ拠点：8）

- 10/100/1000BASE-T を 4 ポート有すること。
- シリアルコンソールポートを有すること。
- VRF 機能を有すること。
- IPsec 機能を有すること。
- IPsec 対地数 128 であること。
- IKEv2 に対応していること。
- 802.1X 認証及び、MAC アドレス認証に対応していること。

#### ○出先ルータ（VPNワイド拠点：11）

- 10/100/1000BASE-T を 4 ポート有すること。
- シリアルコンソールポートを有すること。
- VRF 機能を有すること。
- IPsec 機能を有すること。
- IPsec 対地数 128 であること。
- IKEv2 に対応していること。
- 802.1X 認証及び、MAC アドレス認証に対応していること。

#### ○出先ルータ（選挙用：1）

- 10/100/1000BASE-T を 4 ポート有すること。
- シリアルコンソールポートを有すること。
- VRF 機能を有すること。
- IPsec 機能を有すること。
- IPsec 対地数 128 であること。
- IKEv2 に対応していること。

- ・ 802.1X 認証及び、MAC アドレス認証に対応していること

#### ○出先ルータ（学校用 17 拠点）

- ・ 10/100/1000BASE-T を 4 ポート有すること。
- ・ シリアルコンソールポートを有すること。
- ・ VRF 機能を有すること。
- ・ IPsec 機能を有すること。
- ・ IPSec 対地数 128 であること。
- ・ IKEv2 に対応していること。
- ・ 802.1X 認証及び、MAC アドレス認証に対応していること。

#### ○ファイアウォール

- ・ 10/100/1000BASE-T インターフェースを 16 ポート有すること。
- ・ GbE RJ45 HA インターフェースを 2 ポート有すること。
- ・ GbE RJ45 WAN インターフェースを 2 ポート有すること。
- ・ シリアルコンソールポートを有すること。
- ・ 仮想 UTM（VDM）を最大で 10 個構築できること。
- ・ 同時セッション数は 1000 万以上であること。
- ・ 脅威に対抗する機能を使用した状態で 6Gbps 以上の性能を有すること。
- ・ HA 機能を有すること。
- ・ リンクアグリゲーション機能を有すること。

#### ○無線コントローラ

- ・ 10/100/1000BASE-T インターフェースを 8 ポート有すること。
- ・ シリアルコンソールポートを有すること。
- ・ マネジメントポートを搭載していること。
- ・ コントローラでアクセスポイントを一元管理できること。
- ・ 最大 384 台のアクセスポイントを管理できること。
- ・ 専用モジュールなしでスタック構成が可能なこと。
- ・ スタック機能による冗長構成に対応していること。
- ・ IEEE802.1x 認証に対応していること。
- ・ 暗号化方式は、TKIP/AES に対応していること。
- ・ 自動チャネル調整に対応していること。

#### ○アクセスポイント

- ・ 10/100/1000BASE-T を 1 ポート有すること。
- ・ 100/1000BASE-T/2.5G BASE-T の受電ポートを 1 ポート有すること。
- ・ AC アダプターでも給電可能なこと。
- ・ IEEE802.11ax/ac/n/a/g/b/に対応していること。
- ・ 無線 LAN コントローラで集中管理可能なこと。

#### ○監視装置

- ・ 本監視システムに必要なアプリケーションをマネージャサーバにインストールし、またはアプライアンス装置にて Web から閲覧・設定をおこなうことで各種機能を実現すること。
- ・ ネットワーク機器を自動発見し、構成マップを自動描画できること。



- Web GUI による各種設定やグラフ情報の確認が可能であること。また、操作画面は日本語および英語表示が可能であること。
- あらかじめ定義したコマンドを、スケジュール指定でネットワーク機器に実行できること。
- 機器の死活監視, SNMP トラップ監視, MIB 閾値チェックなどにより, ネットワーク上の障害を検出できること。
- 特定アラート発生時に, 電子メールやパトランプ等で通報できる機能を有すること。

#### ○ファイアウォールアナライザ

- ログ処理の容量が 25GB/日以上であること。
- 最新分析日数が 20 日以上可能であること。
- ストレージ容量が 4TB 以上であること。
- 日本語の GUI に対応していること。

#### ○DHCP サーバ

- 最大同時払出アドレス数が 2500 であること。
- 冗長構成が可能なこと。

#### ○セキュリティゲートウェイ

- 19 インチラックに収容でき、1U に収まること。
- 1000BASE-T インターフェースを 7 ポート有すること。
- 10G Fiber を 4 ポート以上搭載可能なこと
- 外部から取得した Microsoft Office365 及び Google Workspace の URL 一覧を条件としたトラフィックの振り分けができること
- 2 台での冗長構成であること。
- 1 台でリバースプロキシ、フォワードプロキシの両方を構成できること また、それぞれ ID 管理基盤と連携し、認証・認可やアクセス制御機能を提供できること（認証サーバや認証サービスと連携し、Kerberos 認証/SAML 認証/LDAP 認証/RADIUS 認証等のユーザー認証やそれに基づく認可ができること）
- 利用ユーザー数は 2,000 人以上、同時セッション数は 100,000 まで使用できること。
- ソース IP、Cookie、SSL Session ID によるセッション維持機能に対応していること
- 2 台での冗長構成に対応していること
- 日本語 GUI に対応していること／CLI でも設定が可能なこと
- 負荷分散方式として、ラウンドロビン、最小コネクション数、最速応答時間を含め、25 種類以上の方式に対応していること

#### ○公衆無線 LAN 用アクセスポイント（公衆無線 LAN 用の個別回線がある）

- 公衆無線 LAN を使用可能にできること。
- SSID を設定できること。
- 10/100/1000BASE-T を 1 ポート有すること。
- 100/1000BASE-T/2.5G BASE-T の受電ポートを 1 ポート有すること。 -
- AC アダプターでも給電可能なこと。
- IEEE802.11ax/ac/n/a/g/b/に対応していること。
- 無線 LAN コントローラで集中管理可能なこと。

以上