

仙台市統合ネットワーク再構築

基本計画書

Ver1.0

令和2年 3月10日

仙台市

目次

1.	はじめに.....	1
2.	本市の現状.....	3
3.	統合NWの再構築による課題解決.....	29
4.	統合NW構成・要件.....	33
5.	テスト要件.....	41
6.	運用保守要件.....	43
7.	費用対効果.....	47
8.	移行計画及び再構築スケジュール.....	49

別冊資料

1. 調査報告書
 1. 1 現状調査・分析報告書
 1. 2 動向調査報告書
2. 要求定義書
3. 必要経費積算表
4. 要件定義書

1. はじめに

1. 1 統合NW再構築の背景・目的

1. はじめに

仙台市統合ネットワーク再構築基本計画を策定するにあたり、統合ネットワーク（以下「統合NW」と記載）の現状調査・分析と動向調査の結果を踏まえて課題を抽出し、課題を解決するために必要となる要求事項を定義した。要求定義を元を実施した情報提供招請（RFI）の結果を踏まえ、再構築に必要な要件を精査し、基本計画として本書に纏めた。

1. 1 統合NW再構築の背景・目的

仙台市（以下「本市」という。）では庁舎間内線電話のV o I P (Voice over Internet Protocol) 化を行い、データ通信と音声電話の庁舎間の通信回線（以下「通信回線」という。）を統合した仙台市統合NWを平成22年度に整備し、その後、各種システムの通信回線の統合を順次進めてきた。

平成27年度には本市職員がインターネットやEメール、文書管理・庶務事務システム等に供する端末（行政情報ネットワークシステム（以下「庁内LAN」という。））の通信回線の一部についても統合NWに切替を行い、一定の成果を成し遂げている。

本市では、今後も必要に応じて各種システムの通信回線を統合する想定であるが、統合NWが使用している広域イーサ中継網の帯域が上限値に迫っており、現在の仕組みでは、これ以上の通信回線の統合が難しいことから、令和4年度までに統合NWの再構築を行うことを検討する必要がある。

しかしながら、ネットワーク構築に求められる要件整理や解決すべき課題が多いため、長期的に有効なネットワークを構築するためには、現状の緻密な分析を実施したうえで、最新の情報化技術の動向を踏まえた設計を行うことが不可欠である。

また、統合NWの再構築にあたっては、庁舎内における無線LANの導入や外部からのリモートアクセスについても検討する必要がある。

これらのことから、ICT分野における専門的かつ高度な見識を有する事業者に委託した仙台市統合ネットワーク再構築基本計画策定支援業務を行うことで、統合NWの再構築に向けた基本計画を策定し、その基本計画に基づく要件を十分に反映した統合NWに再構築することを目的とする。

2. 本市の現状

2. 1 現行統合NWの概要

2. 2 現行統合NWの調査・分析結果

2. 3 現行統合NWの課題

2. 本市の現状

本章では、現行統合NWの現状、現行統合NWの調査・分析結果、及び現行統合NWの課題について記載する。現状調査・分析の結果、及び動向調査の結果については、別冊資料「現状調査・分析報告書」「動向調査報告書」を参照のこと。

2. 1 現行統合NWの概要

(1) 統合NW

統合NWは音声電話V o I P用の通信回線を基本に構成し運用されている。各種システムや庁内LAN（主回線）に対して拠点間ネットワークを提供しているが、あくまで通信サービスの位置づけであり、ネットワーク的には別々に運用されている。

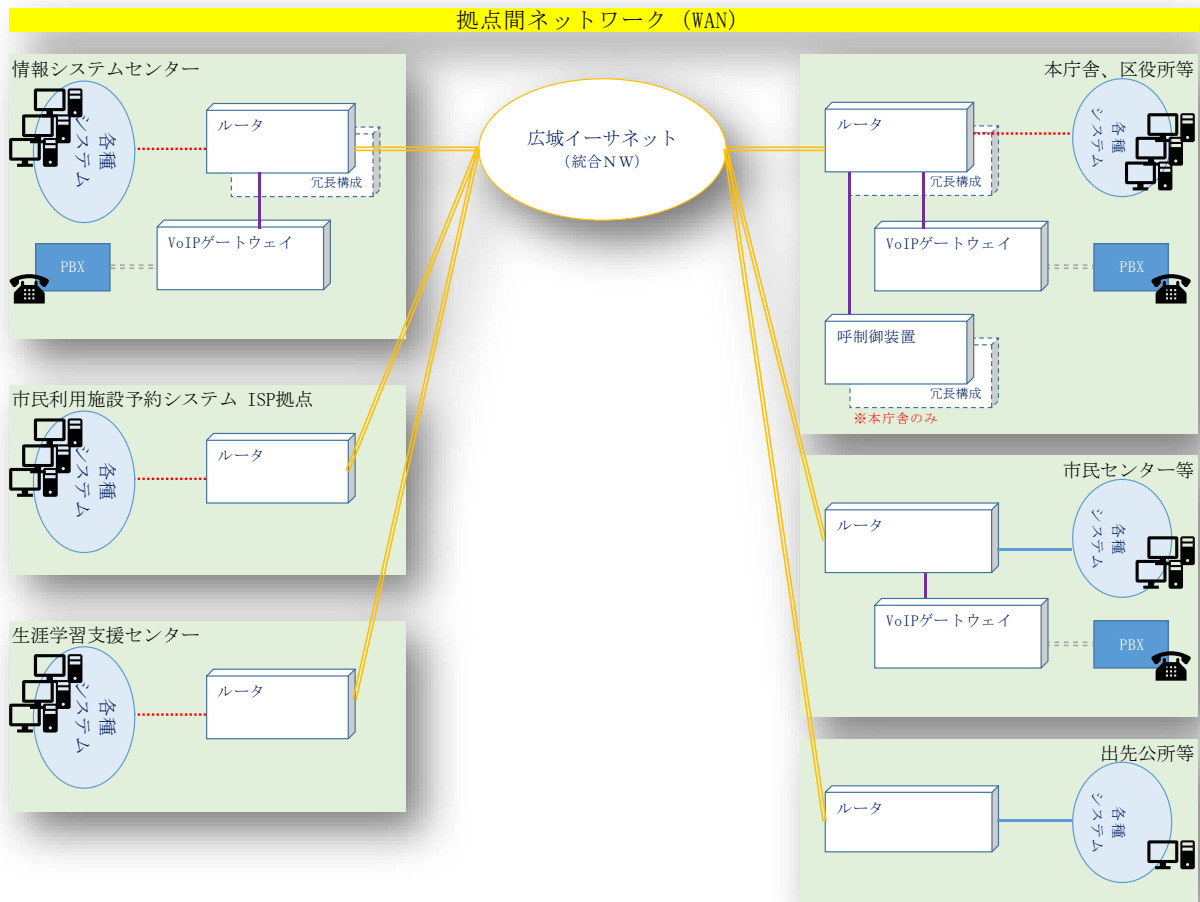


図2. 1-1 統合ネットワーク概要

(2) 統合NW以外のネットワーク

本市における統合NW以外のネットワークは、基幹系NW、庁内LAN（フレッツ回線、VDSL 接続）等があり、統合NWとは別々に構成し運用されている。

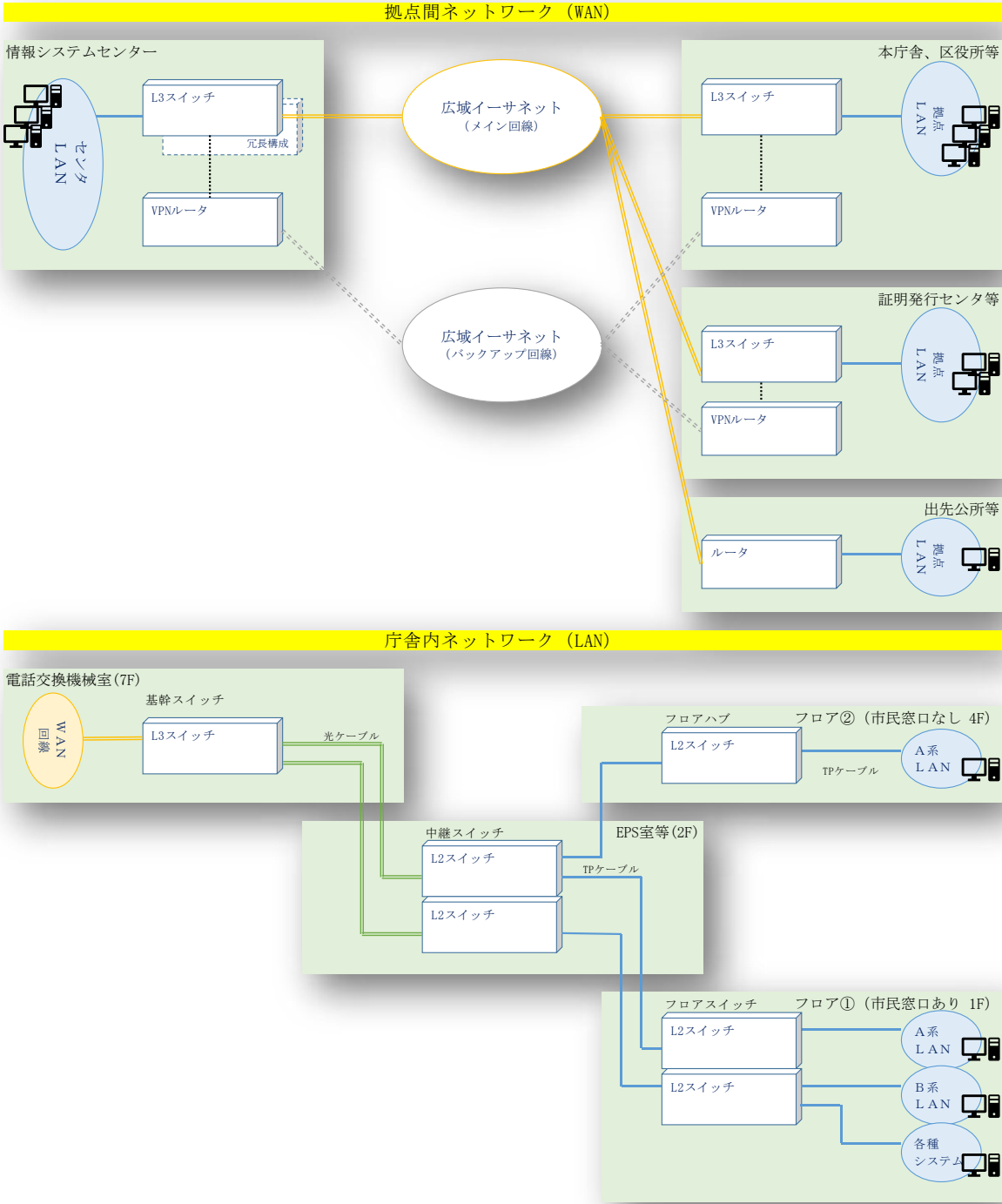


図2. 1-2 基幹系ネットワーク概要

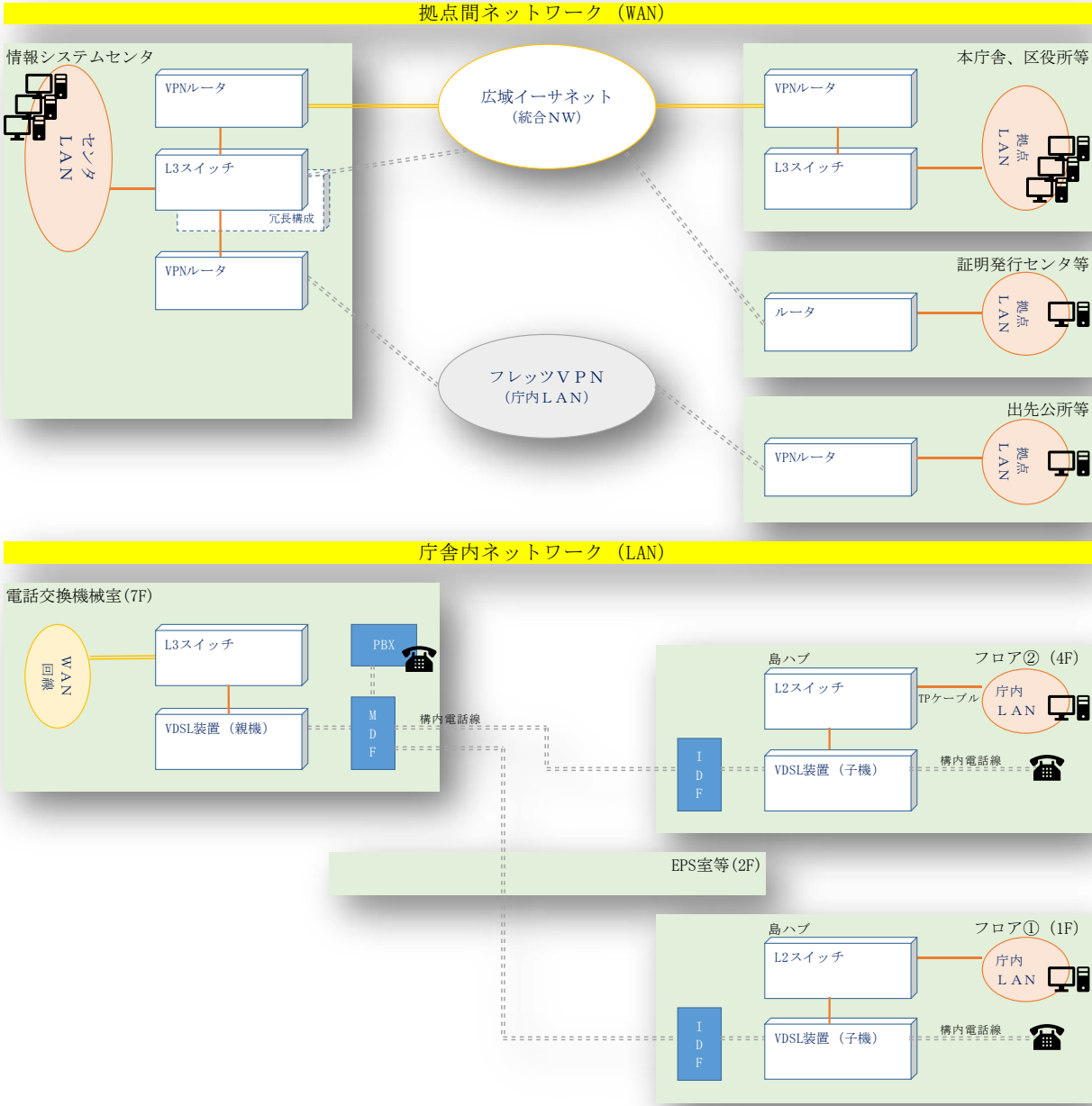


図2. 1-3 庁内LANネットワーク概要

2. 2 現行統合NWの調査・分析結果

現行統合NWの現状を把握し課題の抽出と検討を行うため、以下の観点から調査・分析を行った。

- ・回線種別（帯域・QoS等）・機能・機器等、及び情報セキュリティ状況
- ・ネットワーク運用
- ・統合NW以外のネットワーク

(1) 回線種別（帯域・QoS等）・機能・機器等、及び情報セキュリティ状況

調査・分析の結果について「表2. 2-1 回線種別（帯域・QoS等）・機能・機器等、及び情報セキュリティ状況」に示す。

表2. 2-1 回線種別（帯域・QoS等）・機能・機器等、及び情報セキュリティ状況

#	調査対象	調査・分析結果（概要）
1	回線種別 (帯域・QoS等)	<p>① メイン回線（イーサネット専用線サービス（L2））</p> <ul style="list-style-type: none"> ・全ての拠点がメイン回線を利用。 ・県外の拠点である東京事務所については県間中継回線を利用。 ・保守ベンダの監視センターとの接続はフレッツ回線を利用。 <p>② 帯域</p> <ul style="list-style-type: none"> ・拠点の規模（端末台数、用途）に応じて、アクセス回線の帯域制限（サービス品目）を500Mbps、100Mbps、10Mbps、1Mbpsから選定。 <p>③ QoS</p> <ul style="list-style-type: none"> ・VoIP接続や各種システムの有無に応じて、拠点のアクセス回線の帯域を最大値として、統合NWのNW機器（ルータ）によるQoS制御（帯域制御・優先制御）を実施。

#	調査対象	調査・分析結果（概要）
2	機能 (VoIP 機能)	<p>① 音声ゲートウェイ機能</p> <ul style="list-style-type: none"> ・アナログ電話網と IP 電話網の中継を行う。 ・呼制御装置と連動して通話相手の電話番号から通話対象の音声ゲートウェイへの発信処理を行う。 ・通話相手の音声ゲートウェイからの着信処理を行う。 <p>② 呼制御機能</p> <ul style="list-style-type: none"> ・アナログ電話網の電話番号と IP 電話網の音声ゲートウェイ IP アドレスの紐付け管理を行う。 ・音声ゲートウェイと連動して通話状態の管理を行う。 <p>③ VoIP 機能を利用している拠点数</p> <ul style="list-style-type: none"> ・センタ拠点（呼制御装置） 1 拠点（本庁舎） ・利用拠点（音声ゲートウェイ） 48 拠点（本庁舎を含む）
3	機能 (データ通信機能)	<p>① L3 中継機能</p> <ul style="list-style-type: none"> ・各種システムに拠点間ネットワーク（L3）接続を提供し拠点間での IP 通信を可能とする。 ・拠点毎に IP ゲートウェイ機能を提供する。 ・拠点間のルーティング機能を提供する。 <p>② QoS 機能</p> <ul style="list-style-type: none"> ・各種システムごとに QoS による帯域制御を提供する。 (拠点ごとに最低保証帯域を設定する) <p>③ データ通信機能を利用している各種システムと利用拠点数</p> <ul style="list-style-type: none"> ・児童扶養手当システム 8 拠点 ・市民利用施設予約システム 115 拠点 ・学習情報レファレンスシステム 59 拠点 ・道路占用料システム 9 拠点 ・生活衛生システム 11 拠点 ・生活保護システム 8 拠点 ・母子保健システム 9 拠点 ・庁内 LAN 38 拠点

#	調査対象	調査・分析結果（概要）
4	機能 (運用監視)	<p>① NW 監視機能</p> <ul style="list-style-type: none"> ・対象ノードの疎通、死活監視を行う。 ・不正接続検出等の監視を行う。 <p>② 性能管理機能</p> <ul style="list-style-type: none"> ・ネットワークトラヒック等の測定を行う。 ・ネットワークトラヒック等の分析を行う。 <p>③ ログ管理機能</p> <ul style="list-style-type: none"> ・サーバやNW 機器からのログ収集を行う。 ・収集したログ情報の管理を行う。 <p>④ 遠隔操作機能</p> <ul style="list-style-type: none"> ・サーバやNW 機器の遠隔操作を行う。
5	機器 (VoIP 機器)	<p>① 呼制御装置</p> <ul style="list-style-type: none"> ・CiscoSystems 製 呼制御装置 2 台 <p>② 音声ゲートウェイ</p> <ul style="list-style-type: none"> ・CiscoSystems 製 ルータ 82 台 (予備機 17 台を含む)
6	機器 (データ通信機器)	<p>① WAN 接続ルータ</p> <ul style="list-style-type: none"> ・CiscoSystems 製 ルータ 109 台 (予備機 3 台を含む) <p>② L3 スイッチ</p> <ul style="list-style-type: none"> ・CiscoSystems 製 L3 スイッチ 2 台 <p>③ L2 スイッチ</p> <ul style="list-style-type: none"> ・CiscoSystems 製 L2 スイッチ 32 台 (予備機 8 台を含む)
7	機器 (運用監視機器)	<p>① シスログサーバ</p> <ul style="list-style-type: none"> ・HP 製サーバ 1 台 ・JTC-i 製 ソフトウェア 1 式 <p>② NW 監視サーバ</p> <ul style="list-style-type: none"> ・HP 製 サーバ 1 台 ・日立製 ソフトウェア 1 式 <p>③ NW 監視端末</p> <ul style="list-style-type: none"> ・HP 製 PC 2 台 ・MS 製 ソフトウェア 2 式

#	調査対象	調査・分析結果（概要）
8	情報セキュリティ状況	<p>① 外部ネットワークとの接続を持たないクローズドネットワーク（閉域網）であり、外部ネットワークからの脅威に対して堅牢な構成。</p> <p>② 統合NWの各機器は、コンソール接続のパスワード設定やリモート接続のアクセス制限が設定されており、機器に対する不正なログインを防止。</p> <p>③ 各種システムで外部ネットワークとの接続を持つものがあるが、統合NWのVRF（仮想化）によるネットワーク分離により、統合NWと外部ネットワークとの通信ができない構成。</p> <p>④ 外部ネットワークと各種システム間のセキュリティ対策については、各種システム側のポリシーで実施。</p> <p>⑤ 統合NWにおける各種システムの通信経路は暗号化されていないため、通信経路の秘匿性については、各種システム側のポリシーに依存。</p>

（2） ネットワーク運用

調査・分析の結果について「表2. 2-2 ネットワーク運用」に示す。

表2. 2-2 ネットワーク運用

#	調査対象	調査・分析結果（概要）
1	管理者用機能 (障害監視)	<p>① NW 監視</p> <ul style="list-style-type: none"> ・対象ノードの疎通、死活を監視する ・不正接続検出を監視する ・監視センタへの通報を行う <p>② WAN 回線監視</p> <ul style="list-style-type: none"> ・通信事業者がWAN回線の正常性を監視する ・通信事業者が管理者への通報を行う

#	調査対象	調査・分析結果（概要）
2	管理者用機能 (性能管理)	① 性能情報の測定 ・ネットワークトラフィック情報の測定 ・サーバリソース情報の測定 ② 性能情報の評価 ・ネットワークトラフィック情報の評価 ・サーバリソース情報の評価 ③ 性能評価レポート ・性能評価レポートの作成
3	管理者用機能 (ログ管理)	① ログ情報の収集 ・システムログの収集 ・アクセスログの収集 ② ログ情報の管理 ・システムログの管理 ・アクセスログの管理 ③ ログ情報の分析 ・システムログの分析 ・アクセスログの分析 ④ ログ分析レポート ・ログ分析レポートの作成
4	運用状況	① 障害の監視や障害対応 ② 定期的なトラフィック分析 ③ 定例会での報告 ④ 定期点検や設定変更等の対応

(3) 統合NW以外のネットワーク

通信回線統合の可能性を検討するため、以下の統合NW以外のネットワークについて調査・分析を行った。

- ・基幹系NW（基幹系ネットワーク）
- ・庁内LAN（行政情報ネットワーク）

調査・分析結果について「表2. 2-3 他ネットワーク概要」に示す。

表2. 2-3 他ネットワーク概要

#	調査対象	調査・分析結果（概要）
1	基幹系NW (回線種別)	<p>① メイン回線（広域イーサネット網サービス（L2））</p> <ul style="list-style-type: none"> ・アクセス回線の帯域毎の回線数： <ul style="list-style-type: none"> 1Gbps 1回線 100Mbps 10回線 10Mbps 34回線 ・網内の帯域制限：無し ・保守条件：回線監視 有り、故障通知 有り、SLA 有り <p>② バックアップ回線（広域イーサネット網サービス（L2））</p> <ul style="list-style-type: none"> ・アクセス回線の帯域毎の回線数： <ul style="list-style-type: none"> 100Mbps 1回線 10Mbps 10回線 1Mbps 11回線 ・網内の帯域制限：有り ・保守条件：回線監視 有り、故障通知 有り、SLA 有り <p>③ 開発ネットワーク（広域イーサネット網サービス（L2））</p> <ul style="list-style-type: none"> ・アクセス回線の帯域毎の回線数： <ul style="list-style-type: none"> 100Mbps 4回線 ・網内の帯域制限：無し ・保守条件：回線監視 有り、故障通知 有り、SLA 有り <p>④ 住基ネット拠点回線（広域イーサネット網サービス（L2））</p> <ul style="list-style-type: none"> ・アクセス回線の帯域毎の回線数： <ul style="list-style-type: none"> 100Mbps 1回線 10Mbps 9回線 ・網内の帯域制限：無し ・保守条件：回線監視 有り、故障通知 有り、SLA 有り

#	調査対象	調査・分析結果（概要）
2	基幹系NW （各種システムで個別に利用している回線）	① 住基システム ・住基ネット 住基ネット回線（県） ・コンビニ交付 LGWAN 回線 ・法務省連携 LGWAN 回線 ② 戸籍システム ・コンビニ交付 LGWAN 回線 ・法務省連携 LGWAN 回線 ③ 国保システム ・国保総合 独自 WAN 回線 ・後期高齢 独自 WAN 回線 ・特定検診 独自 WAN 回線 ・ねんきんネット 独自 WAN 回線 ④ 税システム ・コンビニ交付 LGWAN 回線 ・eLTAX LGWAN 回線、独自 WAN 回線

#	調査対象	調査・分析結果（概要）
3	庁内LAN (回線種別)	<p>① メイン回線（統合NW（VPN/L3））</p> <ul style="list-style-type: none"> ・帯域毎の拠点数： 500Mbps 2 拠点 100Mbps 13 拠点 10Mbps 29 拠点 ・網内の帯域制限：有り ・保守条件：統合NWに準ずる <p>② フレッツ回線（VPN サービス（VPN/L3））</p> <ul style="list-style-type: none"> ・グループ毎の拠点数： FVW① 40 拠点 FVW② 31 拠点 FVW③ 50 拠点 ・網内の帯域制限：有り ・保守条件：回線監視 無し、故障通知 無し、SLA 無し <p>③ インターネット</p> <ul style="list-style-type: none"> ・アクセス回線：宮城県ハイパーウェブ（L2） ・アクセス回線の帯域：300Mbps ・上位ネットワークセンタ（NOC）： 宮城県自治体情報セキュリティクラウド ・ファイアウォール：仙台市管理の機器を設置 <p>④ LGWAN</p> <ul style="list-style-type: none"> ・アクセス回線：宮城県ハイパーウェブ（L2） ・アクセス回線の帯域：100Mbps ・上位ネットワークセンタ（NOC）：LGWAN（宮城県 NOC） ・ファイアウォール：仙台市管理の機器を設置

2. 3 現行統合NWの課題

(1) 課題の抽出と改善策の検討

現行統合NWの調査・分析により以下の課題を抽出し、改善策（案）の検討を行った。

- ・ 中継網の帯域不足
- ・ 通信回線の可用性
- ・ 拡張性
- ・ LAN 配線の重複
- ・ 内線電話のあり方

表 2. 3 - 1 現行統合NWの課題

#	課題	調査結果	改善策（案）
1	中継網の帯域不足	<p>【概要】統合NWが使用している広域イーサ中継網の帯域が上限値に迫っていることから、これ以上 WAN 回線の統合が困難である。</p> <p>【詳細】各種システムの統合NW接続を進める過程で、市内LANの大規模で通信量の多いネットワーク（使用帯域 10M～100Mbps）を収容したことにより、中継網の帯域に余裕が無い状態にあることを確認した。</p> <p>また、市民利用施設予約システムでは、端末更新（Windows10 導入）に伴い、当初に想定したシステム利用通信（使用帯域 1Mbps～）の他に、OS のセキュリティパッチ配信等で大量の通信が発生することが想定され、中継網の帯域不足が課題となっている。</p>	<p>案① 統合NWのWAN回線を複数の回線サービスに分割して契約する。</p> <p>案② 仙台市の他ネットワークのWAN回線を共同利用する。</p>

#	課題	調査結果	改善策（案）
2	通信回線の可用性	<p>【概要】統合NWは通信回線が冗長化されていないため、可用性の面で課題がある。</p> <p>【詳細】統合NWのセンター拠点である本庁舎のWAN回線は冗長化されているが、情報システムセンターや区役所等の主要拠点であってもWAN回線が冗長化されていないことを確認した。</p> <p>WAN回線は通信事業者のSLAにより回復時間などの保守条件が設定できるが、内線電話網のVoIP中継を行っていることを考慮すると、区役所等の主要拠点についてはWAN回線の冗長化が必要である。バックアップ回線はメイン回線と別の通信事業者または別の回線サービスを利用する必要がある。</p>	<p>案① 統合NWで新たにバックアップ回線を契約する。</p> <p>案② 仙台市の他ネットワークをバックアップ回線として共同利用する。</p>

#	課題	調査結果	改善策（案）
3	拡張性	<p>【概要】統合NWは、外部から接続出来ない仕組みであり、情報漏えいやサイバー攻撃を阻止するためには有効な仕組みであるものの、市民サービスの向上や事務の効率化を含めた業務改善や働き方改革等を推進するにあたり、外部からの接続環境の整備やモバイル端末の活用を検討する必要がある、拡張性の面で課題がある。</p> <p>【詳細】統合NWをWAN回線として利用している各種システムの構成を調査したところ、インターネットやLGWAN等の外部ネットワークとの接続については、ほとんどが庁内LAN系のシステムで運用されていることを確認した。</p> <p>現状、統合NWとして市民や職員にサービスを提供している機能がないことや、複数の外部ネットワークとの接続を持つことがセキュリティのリスクを増大させる要因になることを考慮すると、外部からの接続環境の整備やモバイル端末の活用については、庁内LANも含めた拡張性として検討する必要がある。</p>	関連する技術について調査を行い、動向調査報告書に整理した。

#	課題	調査結果	改善策（案）
4	LAN 配線の重複	<p>【概要】 各種システムが統合NWを利用する際、各庁舎における統合NW側の設備と各種システム側の設備の間の LAN 配線は各種システムを所管する部署で敷設している。そのため、統合NW側の設備と各種システム側の設備が別の階にある場合、縦系配線がシステムごとに必要であることから、LAN ケーブルの重複による建物の配線スペースの課題と、各種システムごとに LAN 配線を敷設することによる、費用の重複が課題である。</p> <p>【詳細】 統合NWを WAN 回線として利用している各種システムの構成を調査したところ、各種システムごとに LAN ケーブルを敷設し運用していることを確認した。また、他ネットワークの構成を調査したところ、統合NWと同様に他ネットワークごとに LAN ケーブルを敷設し運用していることを確認した。区役所等の縦系配線は電話交換機械室を起点として端末設置階の EPS を経由して敷設されており、この間については LAN 配線の重複を確認した。</p>	<p>案① 仙台市の他ネットワークと縦系の LAN 配線を一元的に管理する</p> <p>案② 仙台市の他ネットワークと縦系の LAN 配線を統合する</p>

#	課題	調査結果	改善策（案）
5	内線電話のあり方	<p>【概要】内線の VoIP 化にあたり、SIP サーバと VoIP ゲートウェイを統合NWの設備として整備しているため、内線電話拠点の増設による番号計画の変更、VoIP ゲートウェイの増設等の費用面の課題や、構内電話交換機、SIP サーバ、VoIP ゲートウェイの管理等、ネットワークインフラとしてのあり方について検討する必要がある。</p> <p>【詳細】統合NWのデータ通信機能の運用管理は一般的な NW スキルで対応できる。各種システムの変更も新しい各種システムを接続したり利用拠点を増やす場合など限定的である。</p> <p>VoIP 機能の運用管理は PBX や番号計画等より専門的なスキルが必要とされる。内線電話網の変更は組織改正や人事異動など定期的な作業が想定される。</p> <p>ネットワークインフラ運用の観点から、VoIP 機能とデータ通信機能の管理は分離して行うことが可能である。特に内線電話網の VoIP 機能と各種システムのデータ通信機能で主管部署が異なる場合には、それぞれで管理することが望ましい。</p>	<p>案① VoIP 機能と機器（呼制御装置、VoIP ゲートウェイ）の管理を分離する</p> <p>案② 将来的な IP 電話機の導入を検討する</p>

(2) 通信回線統合の可能性

課題の解決策である「他ネットワークとの共同利用」の実現性を検証するため、統合NWと他ネットワークとの通信回線統合の方式（案）を検討した結果、WAN回線とLAN配線を共同利用することで将来的に通信回線を統合できる可能性を確認した。

WAN回線統合のイメージについて「図2.3-1 WAN回線統合のイメージ（現状）」「図2.3-2 WAN回線統合のイメージ（移行中）」「図2.3-3 WAN回線統合のイメージ（移行後）」「図2.3-4 WAN回線統合のイメージ（論理的な統合）」に示す。

LAN配線統合のイメージについて「図2.3-5 LAN配線統合のイメージ（現状）」「図2.3-6 LAN配線統合のイメージ（移行中）」「図2.3-7 LAN配線統合のイメージ（移行後）」に「図2.3-8 LAN配線統合のイメージ（論理的な統合）」に示す。

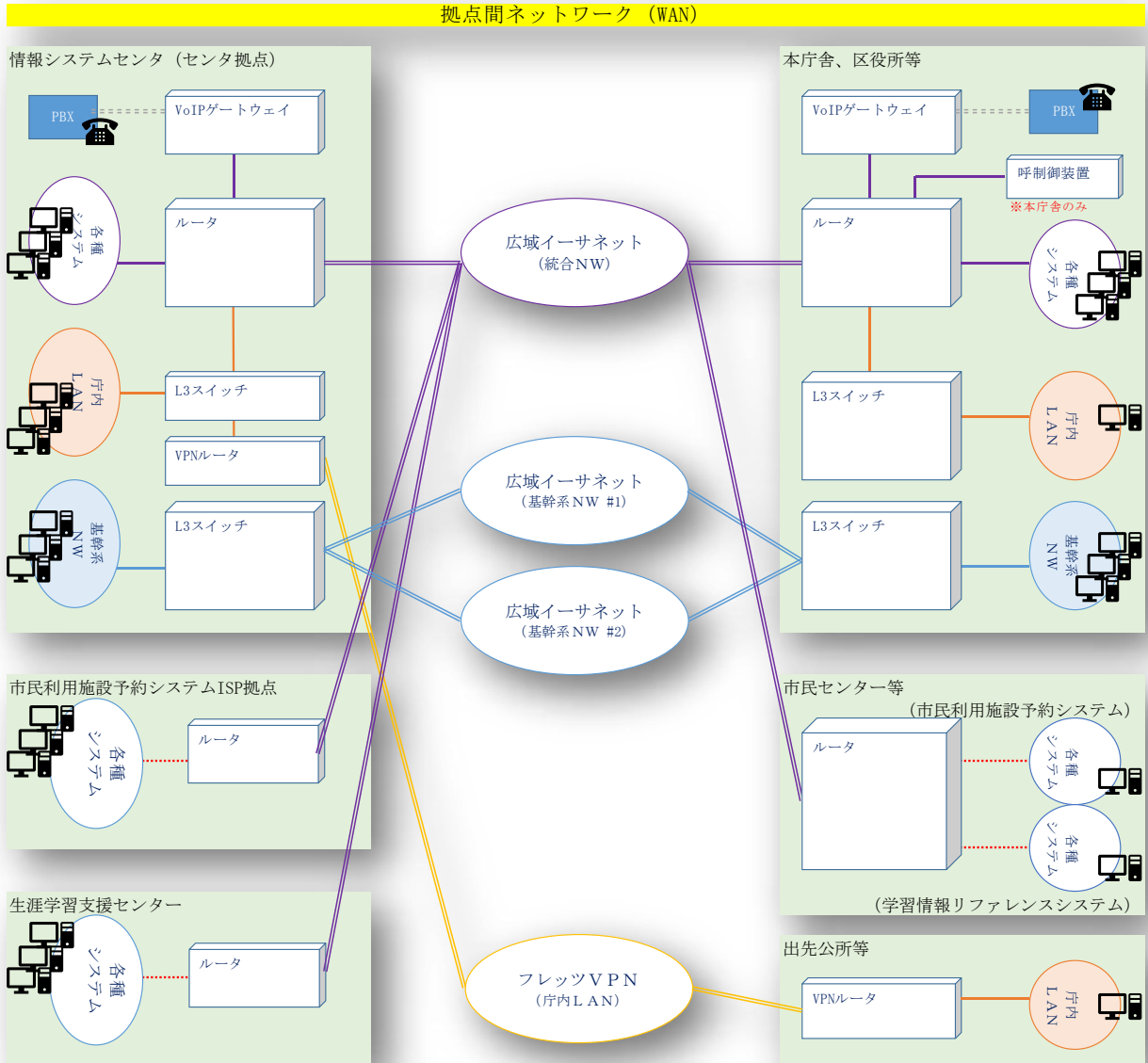


図 2. 3-1 WAN 回線統合のイメージ (現状)

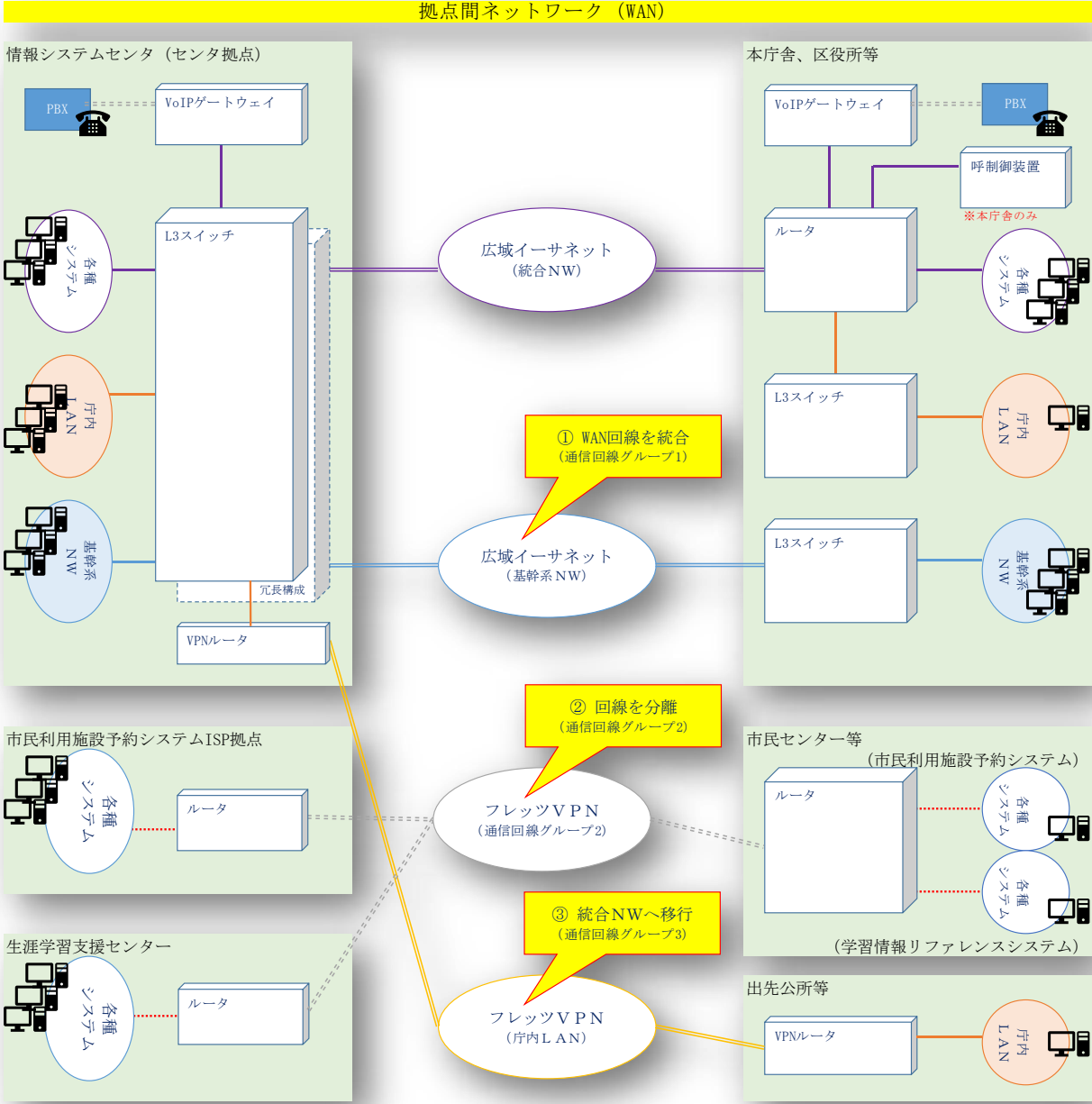


図 2. 3 - 2 WAN 回線統合のイメージ (移行中)

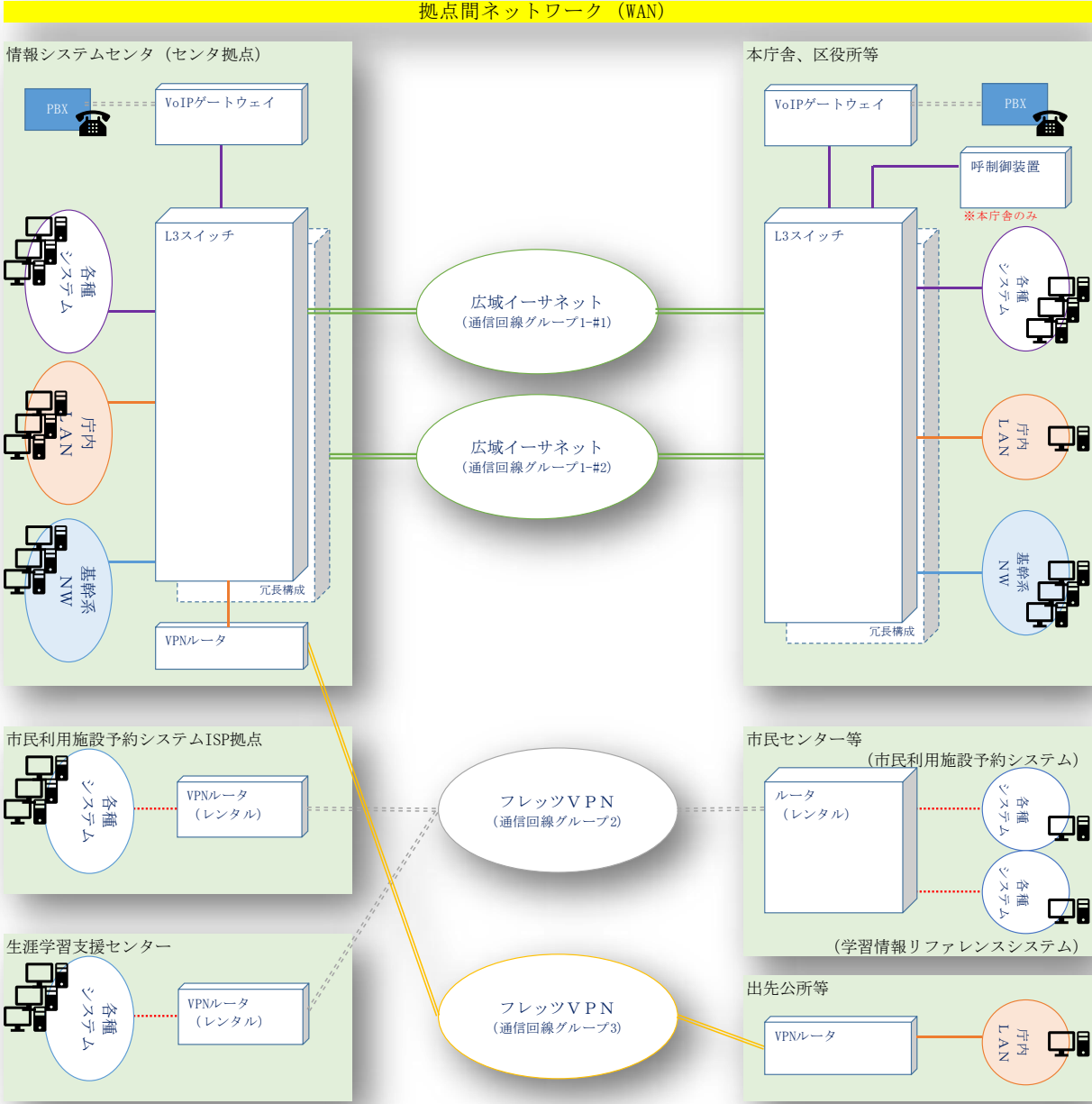


図 2. 3 - 3 WAN 回線統合のイメージ (移行後)

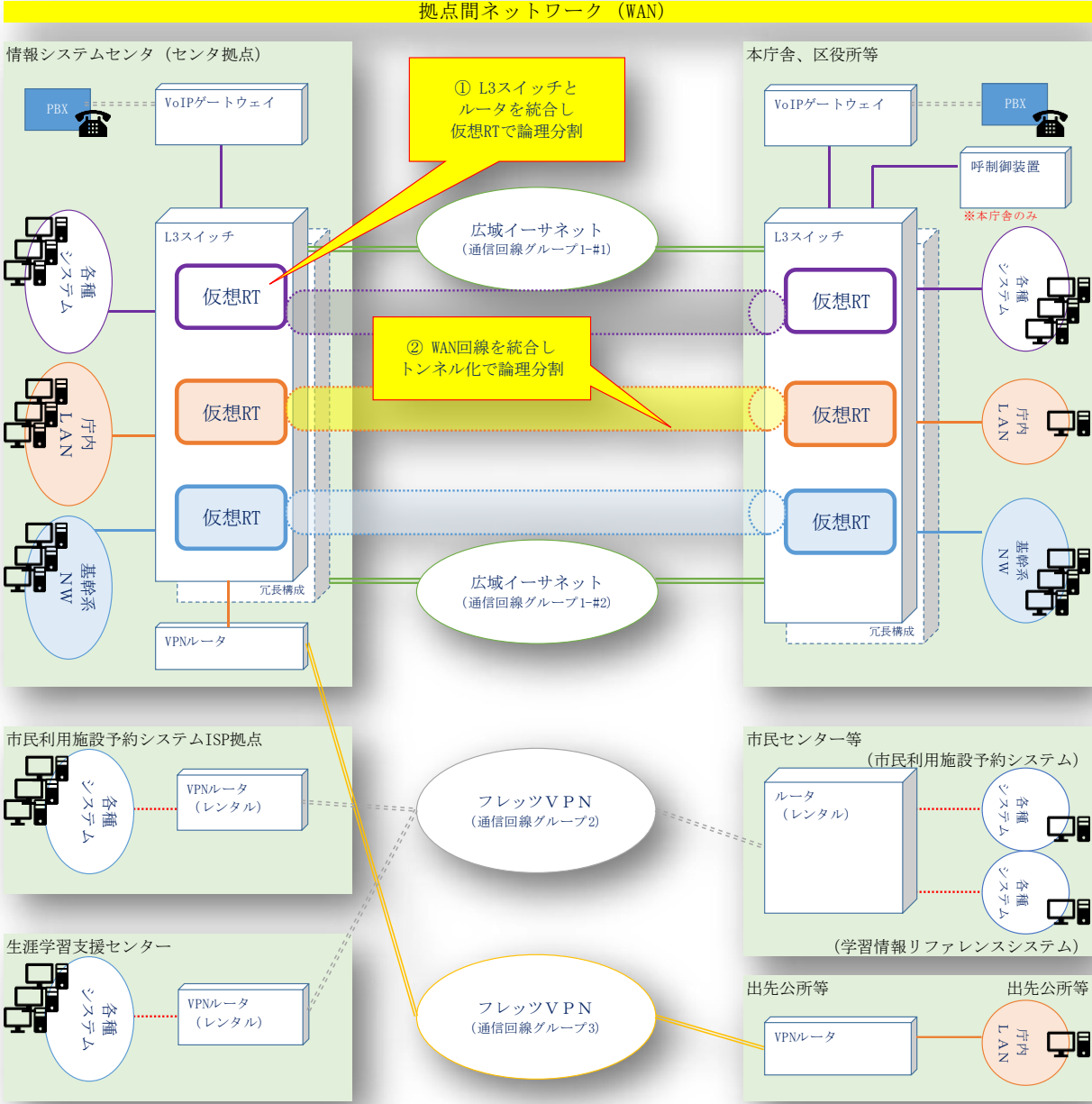


図 2. 3-4 WAN 回線統合のイメージ (論理的な統合)

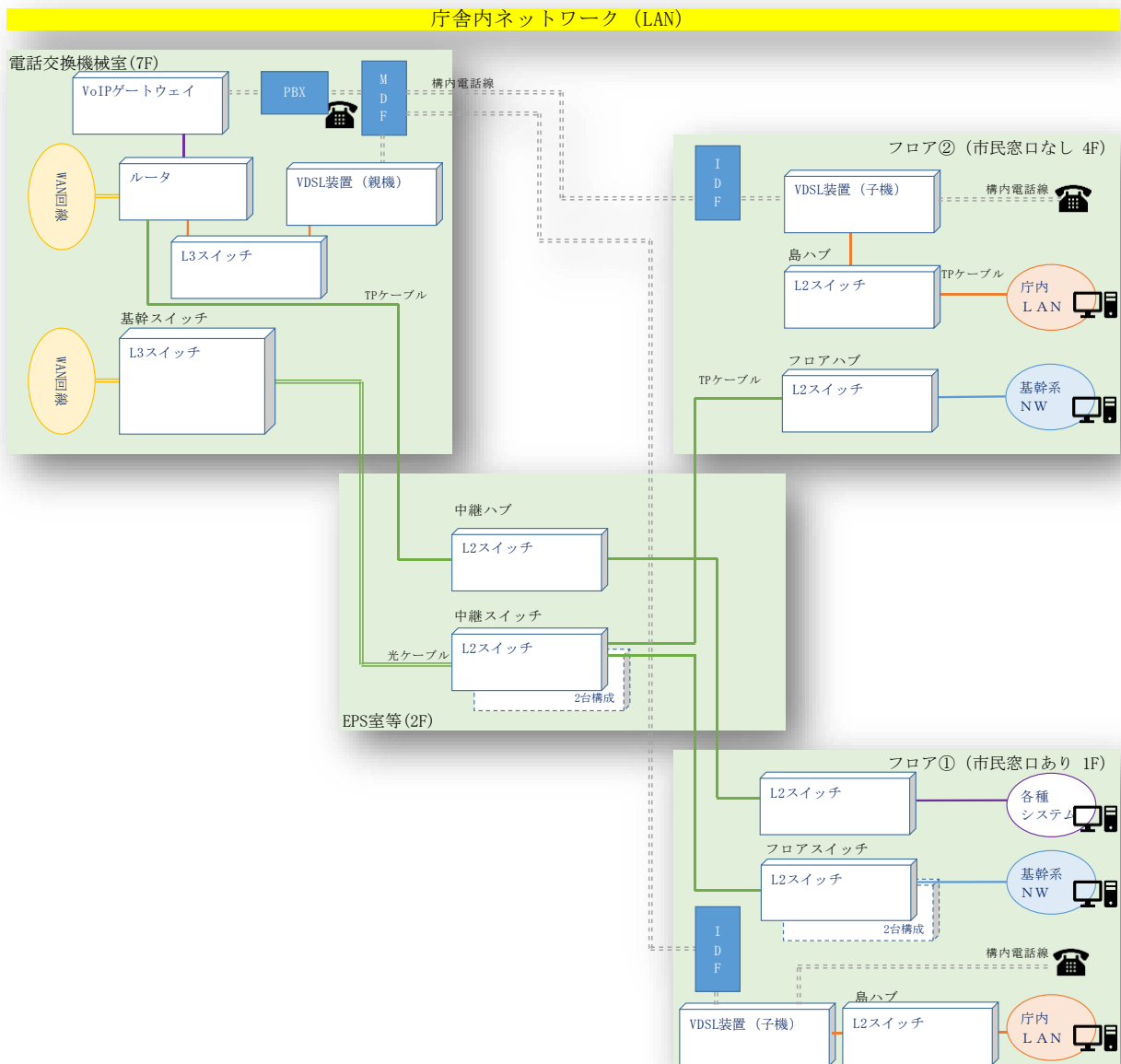


図 2. 3-5 LAN 配線統合のイメージ (現状)

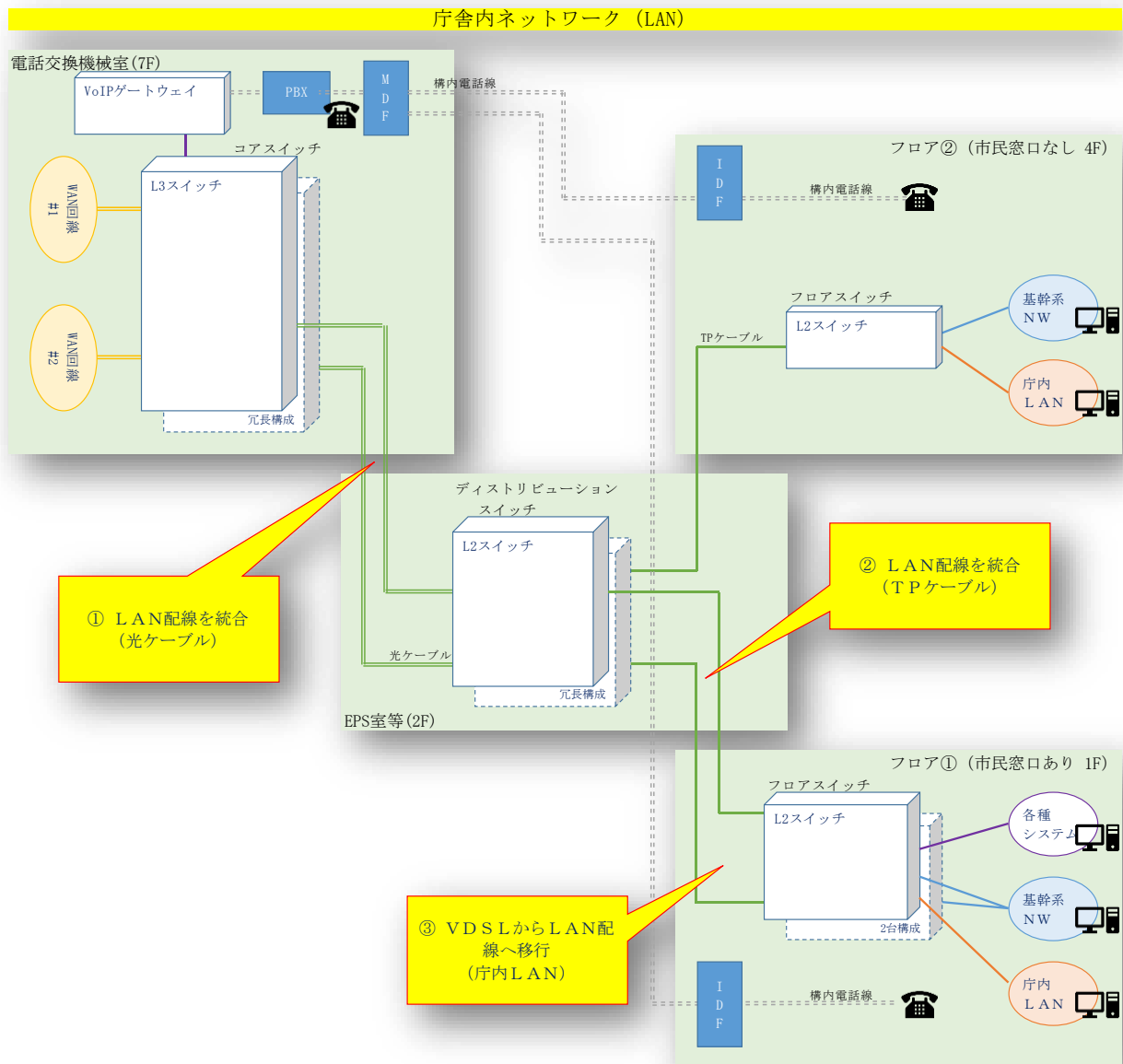


図2. 3-6 LAN配線統合のイメージ (移行中)

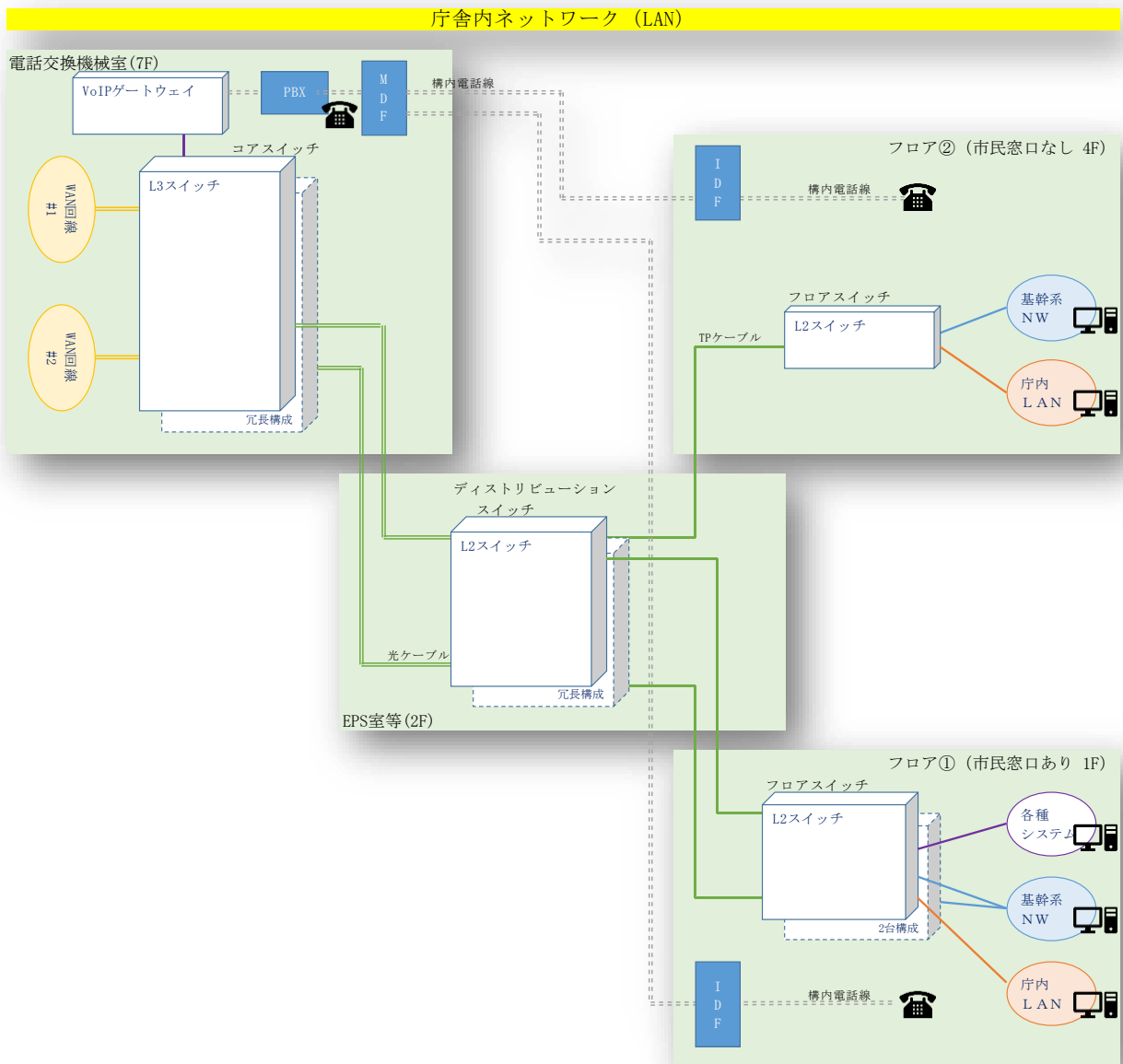


図 2. 3-7 LAN 配線統合のイメージ (移行後)

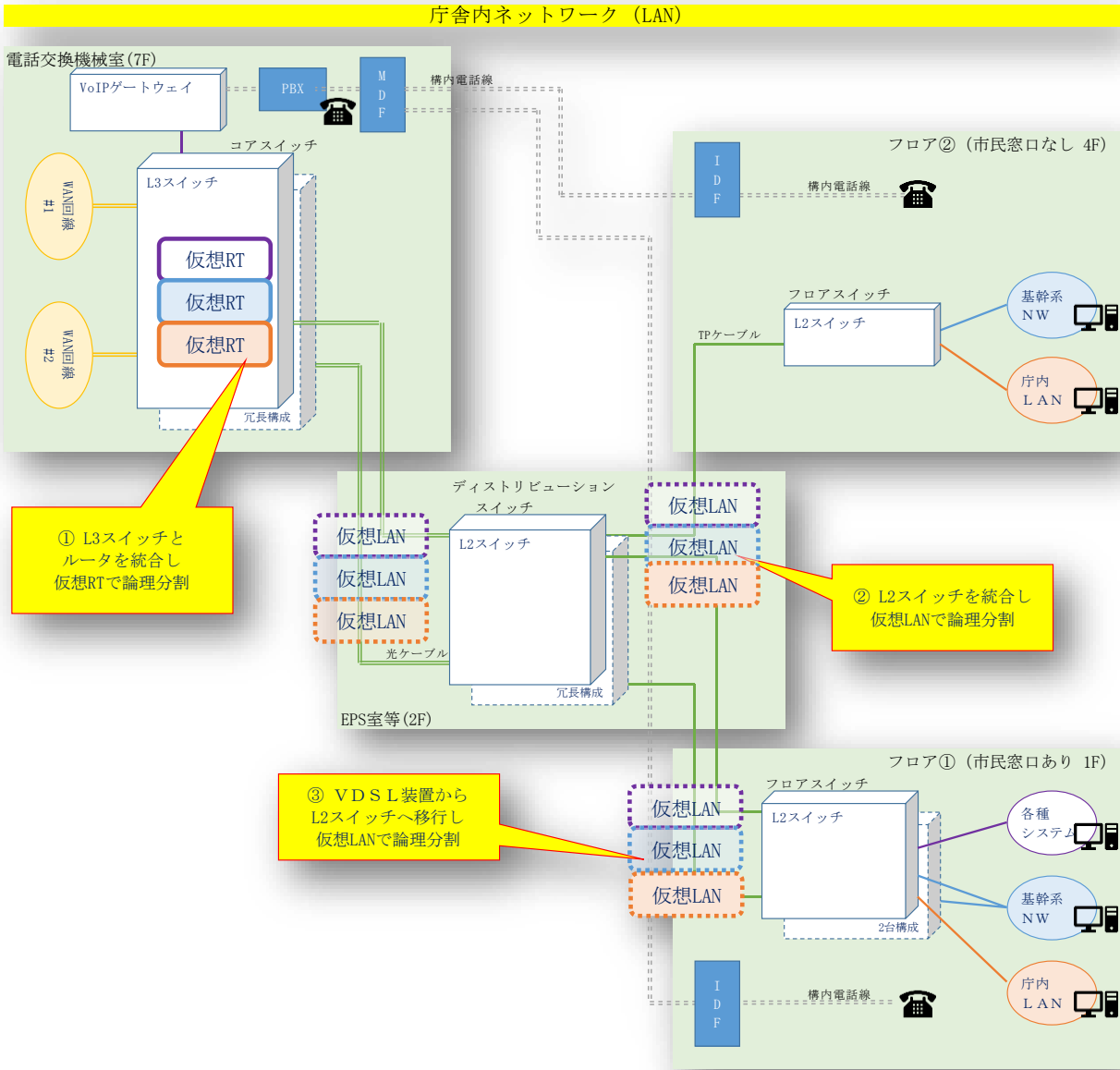


図 2. 3 - 8 LAN 配線統合のイメージ (論理的な統合)

3. 統合NWの再構築による課題解決

3. 1 新たな統合NWのあるべき姿

3. 2 統合NW再構築基本方針

3. 3 再構築対象範囲

3. 4 期待される効果

3. 統合NWの再構築による課題解決

本章では、統合NWの再構築により解決される課題と解決策を踏まえ、新たな統合NWのあるべき姿、統合NW再構築基本方針、再構築対象範囲、期待される効果について記載する。

【現状の統合NWの課題】

- ・ 中継網の帯域不足
- ・ 通信回線の可用性
- ・ LAN 配線の重複
- ・ 拡張性
- ・ 内線電話のあり方



【再構築による課題の解決】

- ・ 通信回線の統合により帯域を増強
- ・ 通信回線の統合により回線を冗長化
- ・ 通信回線の統合により LAN 配線を共用
- ・ 将来的な拡張性を考慮した再構築を実現
- ・ 将来的な内線電話用V o I Pの分離に向けた協議

3. 1 新たな統合NWのあるべき姿

統合NWの再構築により、統合NWは本市の標準的なネットワーク基盤として位置づけられ、将来的に更なるネットワークサービスの拡充が期待される。

- ・ 内線電話の IP 電話化（フル IP 化）
- ・ 庁舎内無線 LAN の導入
- ・ 庁舎外からのリモート接続による庁内サービスの利用

長期的に安定したネットワークサービスを提供するためには、ネットワーク基盤に特化した運用が求められる。インターネットやL G W A N等の外部接続の運用と同様に、内線電話用V o I Pの運用については、統合NWとの分離に向けて内線電話主管部門との協議を進めることが求められる。

3. 2 統合NW再構築基本方針

新たな統合NWを本市の標準的なネットワーク基盤と位置づけ、現行統合NWを通信回線として利用しているV o I Pや各種システムに加えて、基幹系NWと庁内L A Nの通信回線を統合する。また、庁舎内のLANについても統合を進めることで、全庁的な統合NWの利用を実現する。なお、V o I Pについては移行期間の内線電話網への影響を考慮し、現行の構成を踏襲して移行する。

3. 3 再構築対象範囲

統合NW再構築の対象範囲は、現行統合NWの全拠点、基幹系NWの全拠点と庁舎内のLAN、庁内L A Nの一部拠点と庁舎内のLANとする。対象拠点の詳細については、別冊資料「要件定義書」を参照のこと。

3. 4 期待される効果

統合NWの再構築を進めることによって、通信回線やネットワークの運用保守にかかる費用の低減が期待できる。本市のネットワークが一元的に管理されることで、本市職員のネットワーク管理者としての業務負担の軽減も期待できる。

4. 統合NW構成・要件

4. 1 回線要件

4. 2 ハードウェア等要件

4. 3 ネットワーク要件

4. 4 セキュリティ要件

4. 統合NW構成・要件

本章では、再構築後の統合NWに求められる、回線要件、ハードウェア等要件、ネットワーク要件、セキュリティ要件について記載する。各要件の詳細については、別冊資料「要件定義書」を参照のこと。

4. 1 回線要件

回線要件は、以下のパターンに分類し定義する。

- ・通信回線グループ1 : 通信帯域を保証する回線を利用。一部の拠点は冗長構成。
- ・通信回線グループ2 : 通信帯域を保証しない回線を利用。拠点間でVPNを構成。
市民利用施設予約システム、学習情報リファレンスシステムの拠点を対象。
- ・通信回線グループ3 : 通信帯域を保証しない回線を利用。拠点間でVPNを構成。
庁内LANの一部の拠点を対象。

回線要件の概要について「表4. 1-1 回線要件」に示す。

表4. 1-1 回線要件

#	カテゴリ	要件
1	通信回線グループ1	① 回線種別：広域イーサネットサービス (L2) <ul style="list-style-type: none"> ・他の回線ユーザとのセキュリティが確保されていること。 ・県外の拠点と接続できること。(東京事務所) ・24時間365日の保守サービスに対応し、復旧時間のSLAがあること。 ② 帯域 <ul style="list-style-type: none"> ・拠点毎にアクセス回線の帯域制限(サービス品目)を選択できること。 (1Gbps、500Mbps、100Mbps、10Mbps、1Mbps) ③ 冗長構成 <ul style="list-style-type: none"> ・回線の冗長化にあたり、別々の通信事業者を選定すること。

#	カテゴリ	要件
2	通信回線グループ2	<p>① 回線種別：フレッツ VPN (L3)</p> <ul style="list-style-type: none">・アクセス回線毎に PPPoE のユーザ認証ができること。・VPN グループ毎に指定した IP アドレスを利用できること。 <p>② アクセス回線</p> <ul style="list-style-type: none">・フレッツ光の回線サービスを利用できること。 <p>③ マルチセッション</p> <ul style="list-style-type: none">・同一のアクセス回線を用いて、複数のフレッツ VPN を利用できること。
3	通信回線グループ3	<p>① 回線種別：フレッツ VPN (L3)</p> <ul style="list-style-type: none">・アクセス回線毎に PPPoE のユーザ認証ができること。・VPN グループ毎に指定した IP アドレスを利用できること。 <p>② アクセス回線</p> <ul style="list-style-type: none">・フレッツ光の回線サービスを利用できること。 <p>③ マルチセッション</p> <ul style="list-style-type: none">・同一のアクセス回線を用いて、複数のフレッツ VPN を利用できること。

4. 2 ハードウェア等要件

ハードウェア等要件は、以下のパターンで分類し定義する。

- ・ネットワーク機器 : データ通信を行う NW 機器の仕様
- ・VoIP 機器 : VoIP 通信を行う VoIP 機器等の仕様
- ・監視機器 : 運用監視を行う監視機器、ソフトウェアの仕様
- ・ネットワークラック : 各機器を収容するラック等の仕様

ハードウェア等要件の概要について「表 4. 2-1 ハードウェア要件」に示す。

表 4. 2-1 ハードウェア要件

#	カテゴリ	要件
1	ネットワーク機器	<p>① 機器種別</p> <ul style="list-style-type: none"> ・L3 スイッチ① (センタ拠点用) ・L3 スイッチ② (タイプ A 拠点用) (全ポート SFP) ・L3 スイッチ③ (タイプ A 拠点用) (SFP 4 ポート程度) ・L3 スイッチ④ (タイプ B~D 拠点用) ・ルータ (タイプ F 拠点用) (LAN 8 ポート) ・ルータ (タイプ F 拠点用) (生涯学習支援センター及び市民利用施設予約システム ISP 拠点用) ・L2 スイッチ① (ディストリビューション) (24 ポートスタック対応) ・L2 スイッチ② (ディストリビューション) (48 ポートスタック対応) ・L2 スイッチ③ (フロア) (24 ポートファンレス) ・L2 スイッチ④ (フロア) (16 ポートファンレス) ・L2 スイッチ⑤ (フロア) (8 ポートファンレス) ・VoIP ゲートウェイ ・音声モジュール① (OD トランクインターフェース用) ・音声モジュール② (COT トランクインターフェース用) <p>② 仕様項目</p> <ul style="list-style-type: none"> ・モデル、冗長構成、インターフェース、仮想化、スイッチング機能、ルーティング機能、ネットワーク機能、性能、外形、備考 (保守条件等)
		※次ページに続く

#	カテゴリ	要件
	※前ページから続き	③ 必要台数 ・拠点別機器一覧にて、必要台数、光モジュール数等を示す。
2	VoIP 機器	① 機器種別 ・呼制御装置 ・コンソール（呼制御装置用） ・UPS（呼制御装置用） ② 仕様項目 ・モデル、機能・性能、外形、備考（保守条件等） ③ 必要台数 ・拠点別機器一覧にて、必要台数等を示す。
3	監視機器	① 機器種別 ・NW 監視サーバ ・シスログサーバ ・コンソール（サーバ用） ・UPS（サーバ用） ・NTP サーバ ・ファイアウォール（遠隔監視用） ・外付け HDD（サーバのバックアップ用） ・監視端末（業務受注者用、本市管理者用） ② 仕様項目 ・モデル、ソフトウェア仕様、機能・性能、外形、備考（保守条件等） ③ 必要台数 ・拠点別機器一覧にて、必要台数等を示す。
4	ネットワークラック	① 機器種別 ・フルラック ・ハーフラック ・キャビネット① ・キャビネット② ② 仕様項目 ・規格、収容サイズ（ユニット数）、外形サイズ、備考（オプション等） ③ 必要台数 ・拠点別機器一覧にて、必要台数等を示す。

4. 3 ネットワーク要件

ネットワーク要件は、機器仕様の検討や設計構築の積算に必要となる項目のみを定義し、詳細は設計業務にて検討し定義することとする。

ネットワーク要件の概要について「表 4. 3-1 ネットワーク要件」に示す。

表 4. 3-1 ネットワーク要件

#	カテゴリ	要件
1	ネットワーク要件	<p>① IPアドレス</p> <ul style="list-style-type: none"> ・IPアドレスv4を利用する。(IPv6は利用しない)。 <p>② プロトコル</p> <ul style="list-style-type: none"> ・TCP、UDP、IP、ARP、ICMP、SNMPを利用する。 <p>③ トポロジ</p> <ul style="list-style-type: none"> ・WAN：回線網を中心としたスター型トポロジで構成する。 ・LAN：L3スイッチ/ルータを頂点としたスター型トポロジで構成する。 <p>④ ルーティング</p> <ul style="list-style-type: none"> ・拠点間WAN：BGP等を用いたダイナミックルーティングを利用する。 (拠点をASとしてBGPによるAS間ルーティングを行う) ・拠点LAN：L3スイッチ/ルータをゲートウェイとしたスタティックルーティングを利用する。 <p>⑤ 仮想スイッチ</p> <ul style="list-style-type: none"> ・L3スイッチ/ルータを仮想化し論理的に分離するネットワークパーティション(VRF)を利用する。 <p>⑥ 仮想LAN</p> <ul style="list-style-type: none"> ・拠点LANの接続を仮想化し論理的に分離するVLANを利用する。

4. 4 セキュリティ要件

セキュリティ要件は、現行統合NWの要件を踏襲する。詳細な方式は設計業務にて検討し定義することとする。

セキュリティ要件の概要について「表 4. 4-1 セキュリティ要件」に示す。

表 4. 3-1 セキュリティ要件

#	カテゴリ	要件
1	セキュリティ要件	<p>① ネットワーク</p> <ul style="list-style-type: none"> ・統合NWは閉域ネットワークであり、直接的に外部ネットワークとの接続は行わない。(インターネット、LGWAN との接続は庁内LAN側で管理し、専用のセキュリティ機器を介して接続される) <p>② 機器管理</p> <ul style="list-style-type: none"> ・NW 機器の管理に利用するユーザ ID、パスワードを機器の稼働中に変更することができる。 ・ログイン/ログアウトの履歴を内部メモリやシスログサーバに記録することができる。 <p>③ 脆弱性対策</p> <ul style="list-style-type: none"> ・NW 機器の OS (ファームウェア) に重大な脆弱性が発見され更新版の OS が提供された場合に、遠隔操作で OS の更新作業ができる。

5. テスト要件

5. 1 テスト要件

5. テスト要件

本章では、統合NWの再構築にあたり必要となるテスト要件について記載する。

5. 1 テスト要件

統合NWの再構築は、現行統合NWとの並行稼働を行い、本番稼働中のV o I Pや基幹系NW、庁内LAN、及び各種システムの移行を安全かつスムーズに行うため、事前検証や構築時、移行時のテストを確実に実行し評価する必要がある。詳細なテスト方式は設計業務にて検討し定義することとする。テスト要件の概要について「表5. 1-1 テスト要件」に示す。

表5. 1-1 テスト要件

#	カテゴリ	要件
1	事前検証	<ul style="list-style-type: none"> ・統合NWの主要な拠点（構成）を想定した検証環境を構築する。 ・設定した機器を検証環境に接続し、事前検証による動作確認を行い、機器が設計した通りに動作することを確認する。 ・問題が発生した場合には、設計へのフィードバックを行い、再度、検証を実施する。
2	動作確認	<ul style="list-style-type: none"> ・拠点へ機器を設置した際に、動作確認を行い、機器が設計した通りに動作することを確認する。 ・正常時テスト、異常時テストの両方を行う。
3	運用テスト	<ul style="list-style-type: none"> ・統合NWの本番環境への移行を行う前に、運用保守で必要となる各種手順について、運用テストによる評価を行う。 ・正常時、異常時の手順だけでなく、変更作業の手順についても評価を行う。 ・遠隔監視の接続テストや通報テストを行う。
4	連携テスト	<ul style="list-style-type: none"> ・各種システムの統合NWへの移行にあたり、連携テストによる動作確認を行い、移行した各種システムが、問題なく動作することを確認する。

6. 運用保守要件

6. 1 運用要件

6. 2 保守要件

6. 3 S L A要件

6. 運用保守要件

本章では、再構築後の統合NWに求められる、運用要件、保守要件、SLA要件について記載する。各要件の詳細については、別冊資料「要件定義書」を参照のこと。

6. 1 運用要件

統合NWの運用要件を以下に示す。

(1) 現行運用との並行運用を行う。

現統合NW運用期間： 現在～令和4年3月

新統合NW運用期間： 令和3年12月～令和9年3月

並行運用期間： 令和3年12月～令和4年3月（4ヶ月間）

(2) 端末の通信異常時は、基幹系NWや庁内LANの運用（ヘルプデスク）で一次切り分けを行い、必要に応じて統合NWの運用者へエスカレーション（障害連絡）する。

(3) 障害連絡を受付けてから2時間以内に障害対策に着手し、サービスレベルに応じた時間内で障害を復旧する（仮対策による復旧を含む）。

・サービスレベル 高 : 着手から2時間以内に復旧（受付から4時間）

中 : 着手から4時間以内に復旧（受付から6時間）

低 : 着手から6時間以内に復旧（受付から8時間）

— : 着手から翌平日開庁日までに復旧

・受付からの経過時間が夜間休日となる場合は協議のうえで対策時間を決定する。

(4) 新統合NWの運用拠点は情報システムセンターとする。

現統合NW運用拠点： 本庁舎（運用監視機器を設置、予備機を保管）

新統合NW運用拠点： 情報システムセンター（運用監視機器を設置、予備機を保管）

(5) 運用者不在時の異常に備え、常時遠隔監視を行う。

運用監視機器で検出した異常を監視センタに通報し、運用者へ電話やメールによる障害連絡を行う。

6. 2 保守要件

統合NWの保守要件を以下に示す。

(1) ハードウェア保守の条件は、機器パターン毎に設定する。

オンサイト保守： センタ拠点及びタイプA 拠点の NW 機器、並びに呼制御装置及びサーバ機器

予備機交換： センタ拠点及びタイプA 拠点以外の NW 機器、並びにその他の機器
(交換後に先出しセンドバック保守)

(2) オンサイト保守の対応時間は、サービスレベルに応じた時間内とする。

- ・サービスレベル 高 : 着手から2時間以内に復旧（受付から4時間）
- 中 : 着手から4時間以内に復旧（受付から6時間）
- 低 : 着手から6時間以内に復旧（受付から8時間）
- : 着手から翌平日開庁日までに復旧

・受付からの経過時間が夜間休日となる場合は協議のうえで対策時間を決定する。

6.3 SLA要件

統合NWの安定稼働を実現するために、稼働状況を継続的に評価し運用改善を行うために、SLAを定義する。詳細なSLA項目は設計業務にて検討し定義することとする。

SLAを検討する上で必要となるサービスレベル（可用性）の考え方について「表6.3-1 サービスレベル（可用性）概要」に示す。

表6.3-1 サービスレベル（可用性）概要

#	カテゴリ	要件
1	サービスレベル	<p>拠点パターン毎にサービスレベルを設定する。</p> <ul style="list-style-type: none"> ・センタ拠点 : 高（サーバ：有） ・タイプA拠点 : 高（窓口端末：有 内線電話：利用 利用者：多） ・タイプB拠点 : 中（窓口端末：有 内線電話：利用 利用者：少） ・タイプC～G拠点 : 低（窓口端末：無 内線電話：一部 利用者：少）
2	許容ダウンタイム	<p>拠点パターン毎に許容ダウンタイム（最短）を設定する</p> <ul style="list-style-type: none"> ・センタ拠点 : WAN（数十秒） LAN（数秒） ・タイプA拠点 : WAN（数十秒） LAN（数秒） ・タイプB拠点 : WAN（数時間） LAN（数時間） ・タイプC～G拠点 : WAN（数時間） LAN（数時間） <p>※休日開庁拠点は翌平日開庁日</p>
3	冗長構成	<p>拠点パターン毎に冗長構成（フェールオーバー時間）を設定する</p> <ul style="list-style-type: none"> ・センタ拠点 : WAN（二重化：数十秒） LAN（二重化：数秒） ・タイプA拠点 : WAN（二重化：数十秒） LAN（二重化：数秒） ・タイプB拠点 : WAN（不要） LAN（不要） ・タイプC～G拠点 : WAN（不要） LAN（不要） <p>※タイプB拠点の仙台駅前SCはWANのみ二重化する。</p>

7. 費用対効果

7. 1 費用試算

7. 2 導入効果

7. 費用対効果

本章では、統合NWの再構築に必要となる、費用試算と導入効果について記載する。費用試算の詳細については、別冊資料「必要経費積算表」を参照のこと。

7. 1 費用試算

(1) 現行費用の試算

現行の統合NWと基幹系NW、庁内LANについて、それぞれが独立して更新した場合の設計構築、機器、運用保守にかかる概算費用と回線費用について試算を行い、現行費用とした。

(2) 再構築費用の試算

情報提供招請（RFI）により各社から提案された概算費用を基に、設計構築、機器、運用保守にかかる費用の試算を行った。回線費用については、現行統合NWの回線費用を参考に試算を行った。

7. 2 導入効果

現行費用と再構築費用の試算結果について比較し、費用面での導入効果の検討を行った。

回線費用については、回線統合により4,700万円程度の削減効果がある。

この削減効果を見込むためには、ネットワーク再構築が必要となるが、設計・構築、通信回線、機器費用、運用保守の全てを含めても1,139,320千円（RFI回答の最小見積り額）の費用となり、現行費用と比較して266,085千円の削減効果が見込める。

8. 移行計画及び再構築スケジュール

8. 1 移行計画

8. 2 再構築スケジュール

8. 移行計画

本章では、統合NW再構築の移行計画と再構築スケジュールについて記載する。

8. 1 移行計画

統合NW再構築の移行時に求められる要求事項を定義する。詳細な移行計画については設計業務にて検討することとする。

- (1) 新統合NWの構築終了時点で新統合NWの構成を完成する。
 - ・ 現統合NWと並行で構築する
(新規 WAN 回線を併設し、現ネットワークと相互接続する)
 - ・ VoIP 機能も並行で構築する (音声ゲートウェイ間の通信テストまで行う)

- (2) 他ネットワークとの段階的な統合を行う。
 - ・ 基幹系NWとの WAN 共同利用 (現行の WAN 回線を運用しつつ移行する)
 - ・ 基幹系NWとの拠点 LAN 共同利用 (庁内 LAN の VDSL を廃止する)
 - ・ 庁内 LAN の統合NW用 VPN を廃止する (統合NWでルーティングする)

- (3) 各種システムは並行稼働期間で移行を行う。
 - ・ システム毎に移行計画策定の上、拠点毎に現ネットワークから新ネットワークへ移行する

8. 2 再構築スケジュール

統合NWの再構築は、令和2年度から令和3年度にかけて2年間で実施する。

1年目は設計期間、2年目は構築期間を想定しているが、詳細なスケジュールについては設計業務にて検討し決定することとする。想定する再構築スケジュールについて「図8. 2-1 再構築スケジュール」に示す。

#	作業工程	令和2年度												令和3年度												令和4年度～令和8年度				
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	～	1月	2月	3月
1	設計業務																													
	基本設計																													
	詳細設計																													
2	構築業務																													
	事前検証																													
	事前設定																													
	環境構築・テスト																													
	移行																													
3	仮稼働(並行稼働)																													
4	本稼働																													
5	撤去準備・撤去																													

図8. 2-1 再構築スケジュール

仙台市統合ネットワーク再構築

現状調査・分析報告書

Ver1.0

令和元年 7月25日

仙台市

目次

1.	はじめに.....	1
2.	回線種別（帯域・QOS等）・機能・機器等及び情報セキュリティ状況.....	3
3.	ネットワーク運用フロー.....	11
4.	現行の統合NWにおける課題等.....	17
5.	通信回線統合の可能性について.....	25
6.	まとめ.....	41

1. はじめに

1. 1 現状の調査・分析の目的

1. 2 現状の調査・分析の範囲

1. はじめに

1. 1 本書の目的

本書は、仙台市統合ネットワーク再構築基本計画を策定するにあたり、統合ネットワーク（以下「統合NW」と記載）の現状について調査・分析を行い、担当者からのヒアリングを通して内容を整理し報告書に記載することを目的とする。

1. 2 現状の調査・分析の範囲

現状の調査・分析の範囲は以下の通りである。

(1) 回線種別（帯域・QoS等）・機能・機器等及び情報セキュリティ状況

① 回線種別

② 機能

③ 機器等

④ 情報セキュリティ状況

(2) ネットワーク運用フロー

① 管理者機能

② 管理フロー

③ 運用状況

(3) 現行の統合NWにおける課題等

① 中継網の帯域不足

② 通信回線の冗長化

③ 将来の拡張性

④ その他

(4) 通信回線統合の可能性について

① 通信回線統合の可能性

2. 回線種別（帯域・QoS等）・機能・機器等 及び情報セキュリティ状況

2. 1 回線種別

2. 2 機能

2. 3 機器等

2. 4 情報セキュリティ状況

2. 回線種別（帯域・QoS等）・機能・機器等及び情報セキュリティ状況

本章では、統合NWの回線種別・機能・セキュリティ状況について、構成管理資料をもとに調査・分析を行い、担当者からのヒアリングを行った結果を踏まえて整理した内容を記載する。

2. 1 回線種別（帯域・QoS等）

統合NWのWAN回線は、イーサネット専用線サービス（L2）を利用しており、一つのWAN回線サービスに全ての拠点に接続している。県外の拠点である東京事務所については県間中継回線を利用している。保守ベンダの監視センターとの接続はフレッツ回線を利用している。

WAN回線の帯域は、拠点の規模（端末台数、用途）に応じて、アクセス回線の帯域制限（サービス品目）を500Mbps、100Mbps、10Mbps、1Mbpsから選定している。

WAN回線のQoSは、VoIP接続や各種システムの有無に応じて、拠点のアクセス回線の帯域を最大値として、統合NWのNW機器（ルータ）によるQoS制御（帯域制御・優先制御）を行っている。

2. 1. 1 回線種別の概要

WAN回線の概要を「表2. 1 WAN回線サービス概要」に、帯域・QoSの概要を「表2. 2 帯域・QoS概要」に示す。

表2. 1 WAN回線サービス概要

項目	内容	備考
回線種別	広域イーサネット網サービス（L2） （NTT東日本：ビジネスイーサ ワイド）	
県外接続	有り（NTT東日本ワイドタイプ） （NTTコミュニケーションズ：e-VLAN）	東京事務所
網内の帯域制限	有り（アクセス回線のサービス品目）	
保守条件	回線監視：有り、故障通知：有り、SLA：有り	
外部接続	無し（各種システムからの外部接続は除く）	
保守ベンダ監視	有り（フレッツ回線）	

表 2. 2 帯域・QoS 概要

項目	内容		備考
帯域制限対象の回線数	500Mbps	2 回線	
	100Mbps	18 回線 (本庁舎 x1 を含む)	
	10Mbps	104 回線	
	1Mbps	20 回線 (本庁舎 x2 を含む)	
	合計	144 回線	
QoS 対象の回線数	500Mbps	2 回線	
	100Mbps	16 回線 (本庁舎 x1 を含む)	
	10Mbps	10 回線	
	1Mbps	20 回線 (本庁舎 x2 を含む)	
	合計	48 回線	
QoS の種別	<ul style="list-style-type: none"> ・シェーピング (WAN 回線帯域制御) ・LLQ、PQ、帯域保証 (VoIP 音声) ・LLQ、最低帯域保証 (VoIP 制御、NW 監視) ・CBWFQ、最低帯域保証 (各種システム) 		

【用語説明】

※シェーピング：NW機器からの送信時に指定した帯域まで通信量を絞る方式。

※LLQ (LowLatencyQueuing)：特定の通信パケットを優先させ通信の遅延を抑えるキューイング方式。

※PQ (PriorityQueuing)：通信パケットにプライオリティ (優先度) を設定し優先的に通信させる方式。

※CBWFQ (ClassBasedWFQ)：通信パケットをクラスごとに分類し、クラスに指定された帯域制御を行うキューイング方式。

WFQ (WeightedFairQueuing)：動的なキューを用いて通信パケットを均等に通信させるキューイング方式。

2. 2 機能

本書では、統合NWの機能をその用途や構成により3つの機能として分類した。1つ目は内線電話の中継を行う「VoIP 通信機能」。2つ目は各種システムに拠点間のネットワーク接続を提供する「データ通信機能」。3つ目は統合NWの運用監視を行う「運用監視機能」である。

2. 2. 1 機能の概要

各機能の概要を「表2. 3 VoIP 機能概要」「表2. 4 データ通信機能概要」「表2. 5 運用監視機能概要」に示す。

表2. 3 VoIP 機能概要

項目	内容		備考
音声ゲートウェイ機能	<ul style="list-style-type: none"> ・アナログ電話網と IP 電話網の中継を行う。 ・呼制御装置と連動して通話相手の電話番号から通話対象の音声ゲートウェイへの発信処理を行う。 ・通話相手の音声ゲートウェイからの着信処理を行う。 		
呼制御機能	<ul style="list-style-type: none"> ・アナログ電話網の電話番号と IP 電話網の音声ゲートウェイ IP アドレスの紐付け管理を行う。 ・音声ゲートウェイと連動して通話状態の管理を行う。 		
VoIP 機能を利用している拠点数	<ul style="list-style-type: none"> ・センタ拠点（呼制御装置） ・利用拠点（音声ゲートウェイ） 	1 拠点（本庁舎） 48 拠点（本庁舎を含む）	

表2. 4 データ通信機能概要 (1/2)

項目	内容	備考
L3 中継機能	<ul style="list-style-type: none"> ・各種システムに拠点間ネットワーク（L3）接続を提供し拠点間での IP 通信を可能とする。 ・拠点毎に IP ゲートウェイ機能を提供する。 ・拠点間のルーティング機能を提供する。 	
QoS 機能	<ul style="list-style-type: none"> ・各種システムごとに QoS による帯域制御を提供する。（拠点ごとに最低保証帯域を設定する） 	

表 2. 4 データ通信機能概要 (2/2)

項目	内容		備考
データ通信機能を利用している各種システムと利用拠点数	① 児童扶養手当システム	8 拠点	
	② 市民利用施設予約システム	115 拠点	
	③ 学習情報レファレンスシステム	59 拠点	
	④ 道路占用料システム	9 拠点	
	⑤ 生活衛生システム	11 拠点	
	⑥ 生活保護システム	8 拠点	
	⑦ 母子保健システム	9 拠点	
	⑧ 庁内 LAN	38 拠点	

表 2. 5 運用監視機能概要

項目	内容	備考
NW 監視機能	<ul style="list-style-type: none"> 対象ノードの疎通、死活監視を行う。 不正接続検出等の監視を行う。 	
性能管理機能	<ul style="list-style-type: none"> ネットワークトラヒック等の測定を行う。 ネットワークトラヒック等の分析を行う。 	
ログ管理機能	<ul style="list-style-type: none"> サーバや NW 機器からのログ収集を行う。 収集したログ情報の管理を行う。 	
遠隔操作機能	<ul style="list-style-type: none"> サーバや NW 機器の遠隔操作を行う。 	

2. 3 機器等

本書では、統合NWの機器等をその役割や機能により3つの種別に分類した。VoIP通信機能を構成する音声ゲートウェイ、呼制御装置。拠点間ネットワークとデータ通信機能を構成するWAN接続ルータ、L3スイッチ、L2スイッチ。運用監視機能を構成するNW監視サーバ、シスログサーバ等である。

各機器のメーカーと形名、台数までを整理し、機器の詳細な仕様についての記載は行わないものとする。

2. 3. 1 機器等の概要

各機器の概要を「表2. 6 VoIP機器概要」「表2. 7 データ通信機器概要」「表2. 8 運用監視機器概要」に示す。

表2. 6 VoIP機器概要

項目	内容		備考
呼制御装置	CiscoSystems 製 呼制御装置		予備機なし
	・ BE6H-M4-K9= (CiscoBusinessEdition6000)	2台	
	合計	2台	
音声ゲートウェイ	CiscoSystems 製 ルータ		
	・ CISC02901-V/K9	54台	
	・ CISC02911-V/K9	11台	
	合計	65台	
予備機	CiscoSystems 製 ルータ		音声ゲートウェイ機能を持つためVoIP機器として集計する
	・ CISC02901-V/K9	4台	
	・ CISC02911-V/K9	1台	
	・ ISR4331-V/K9	12台	
	合計	17台	

表 2. 7 データ通信機器概要

項目	内容		備考	
WAN 接続ルータ	CiscoSystems 製 ルータ			
	・ CISC03925/K9	8 台		
	・ ISR4321/K9	3 台		
	・ C891FJ-K9	93 台		
	合計	104 台		
WAN 接続ルータ (音声ゲートウェイ機能を持つ機器)	CiscoSystems 製 ルータ		主用途が WAN 接続ルータのためデータ通信機器として集計する	
	・ CISC02901-V/K9	1 台		
	・ CISC02911-V/K9	1 台		
	合計	2 台		
L3 スイッチ	CiscoSystems 製 L3 スイッチ		予備機なし	
	・ WS-C3650-48TS-E	2 台		
	合計	2 台		
L2 スイッチ	CiscoSystems 製 L2 スイッチ			
	・ WS-C2960+24TC-L	10 台		
	・ WS-C2960C-8TC-L	10 台		
	・ WS-C2960CPD-8TT-L	4 台		
	合計	24 台		
予備機	CiscoSystems 製 ルータ		音声ゲートウェイ機能を持つ機器は表 2. 6 に VoIP 機器として記載する	
	・ CISC03925/K9	1 台		
	・ ISR4321/K9	2 台		
		合計	3 台	
	CiscoSystems 製 L2 スイッチ			
	・ WS-C2960+24TC-L	2 台		
	・ WS-C2960C-8TC-L	3 台		
	・ WS-C2960CPD-8TT-L	3 台		
	合計	8 台		

表 2. 8 運用監視機器概要

項目	内容		備考
シスログサーバ	HP 製サーバ、JTC-i 製 ソフトウェア		予備機なし
	・ HP DL320e Gen8 v2 (Windows Server 2012 R2 Std)	1 台	
	・ KiwiSyslogServer/KiwiLogViewer	1 式	
NW 監視サーバ	HP 製 サーバ、日立製 ソフトウェア		予備機なし
	・ HP DL160 Gen9 (Windows Server 2012 R2 Std)	1 台	
	・ 日立 JP1/Cm2/NNMi	1 式	
NW 監視端末	HP 製 PC、MS 製 ソフトウェア		二日町第三仮庁舎 x1 台 監視センタ x1 台 予備機なし
	・ N4P96AV-ADDU (Windows 10 Home (64bit))	2 台	
	・ Microsoft Office Personal 2013	2 式	

2. 4 情報セキュリティ状況

統合NWは、インターネットやL GWAN等の外部ネットワークとの接続を持たないクロードネットワーク（閉域網）であるため、外部ネットワークからの脅威に対しては堅牢な構成である。統合NWの各機器は、コンソール接続のパスワード設定やリモート接続のアクセス制限が設定されており、機器に対する不正なログインを防止する対策が取られている。

各種システムにおけるデータ通信では外部ネットワークとの接続を行っているものがあるが、統合NWのNW機器でVRF（仮想化）によるネットワーク分離を行っているため、統合NWと外部ネットワークは直接的な通信ができない構成となっている。

外部ネットワークと各種システム間のセキュリティ対策については、各種システム側のポリシーで実施している。統合NWにおける各種システムの通信経路は暗号化されていないため、通信経路の秘匿性については、各種システム側のポリシーに依存する。

3. ネットワーク運用フロー

3. 1 管理者機能

3. 2 管理フロー

3. 3 運用状況

3. ネットワーク運用フロー

本章では、統合NWのネットワーク運用フローについて、構成管理資料（運用管理資料等）をもとに調査・分析を行い、担当者からのヒアリングを行った結果を踏まえて整理した内容を記載する。

3. 1 管理者用機能

本書では、統合NWの管理者用機能について、運用管理業務の観点から「障害監視機能」「性能管理機能」「ログ管理機能」の3項目に分類した。

管理者機能の項目と概要までを整理し、各作業の詳細な手順等についての記載は行わないものとする。

3. 1. 1 管理者用機能の概要

管理者用機能の概要について「表3. 1 障害監視機能概要」「表3. 2 性能管理機能概要」「表3. 3 ログ管理機能概要」に示す。

表3. 1 障害監視機能概要

項目	内容	備考
NW 監視	<ul style="list-style-type: none"> ・対象ノードの疎通、死活を監視する ・不正接続検出を監視する ・監視センタへの通報を行う 	
WAN 回線監視	<ul style="list-style-type: none"> ・WAN 回線の正常性を監視する ・管理者への通報を行う 	通信事業者

表 3. 2 性能管理機能概要

項目	内容	備考
性能情報の測定	<ul style="list-style-type: none">・ネットワークトラフィック情報の測定・サーバリソース情報の測定	
性能情報の評価	<ul style="list-style-type: none">・ネットワークトラフィック情報の評価・サーバリソース情報の評価	
性能評価レポート	<ul style="list-style-type: none">・性能評価レポートの作成	

表 3. 3 ログ管理機能概要

項目	内容	備考
ログ情報の収集	<ul style="list-style-type: none">・システムログの収集・アクセスログの収集	
ログ情報の管理	<ul style="list-style-type: none">・システムログの管理・アクセスログの管理	
ログ情報の分析	<ul style="list-style-type: none">・システムログの分析・アクセスログの分析	
ログ分析レポート	<ul style="list-style-type: none">・ログ分析レポートの作成	

3. 2 運用フロー

統合NWの運用フローについて、運用管理業務の観点から「監視・障害対応」「性能管理」「設定変更対応」の3つの運用フローについて調査・分析を行った。

各運用フローで想定されるシナリオについてフロー概要を整理し、全ての運用フローの記載は行わないものとする。

3. 2. 1 監視・障害対応のフロー概要

監視・障害対応のフロー概要について「図3. 1 監視・障害対応フロー概要」に示す。

【想定シナリオ】 死活監視の異常を検知し障害対応を行う。

仙台市	← →	統合NW運用管理 受託業者
		<ul style="list-style-type: none"> ・監視システムより死活監視の異常を検知。 ・障害状況の調査を実施。 (影響範囲を特定)
<ul style="list-style-type: none"> ・障害報告を受理 (影響範囲を把握) 	←	<ul style="list-style-type: none"> ・障害状況を報告。 (影響範囲を提示)
		<ul style="list-style-type: none"> ・情報収集、切り分けを実施。 (原因を特定、対策案を検討)
<ul style="list-style-type: none"> ・障害報告を受理 (原因と対策案を把握) 	←	<ul style="list-style-type: none"> ・障害状況を報告。 (原因と対策案を提示)
<ul style="list-style-type: none"> ・対策案を承認 	→	<ul style="list-style-type: none"> ・対策案の承認を受理。
		<ul style="list-style-type: none"> ・対策案により復旧作業を実施。 (疎通確認での復旧を確認)
<ul style="list-style-type: none"> ・対策結果を受理 (復旧したことを把握) 	←	<ul style="list-style-type: none"> ・対策結果を報告。 (復旧状況を提示)
		<ul style="list-style-type: none"> ・障害報告書を作成。 (対策状況を整理)
<ul style="list-style-type: none"> ・障害報告書を受理 (対策状況を把握) 	←	<ul style="list-style-type: none"> ・障害報告書を送付。 (対策状況を提示)

図3. 1 監視・障害対応フロー概要

3. 2. 2 性能管理のフロー概要

性能管理のフロー概要について「図3. 2 性能管理フロー概要」に示す。

【想定シナリオ】定期的にネットワークトラフィック等の分析を行う。

仙台市	← →	統合NW運用管理 受託業者
		<ul style="list-style-type: none"> 性能情報の測定・評価。 性能評価レポートの作成
<ul style="list-style-type: none"> 性能評価レポートを受理 (評価結果を把握) 	←	<ul style="list-style-type: none"> 性能評価レポートの送付 (評価結果を提示)
<ul style="list-style-type: none"> 性能評価レポートを承認 	→	<ul style="list-style-type: none"> 性能評価レポートを保管 (参照可能な状態とする)

図3. 2 性能管理フロー概要

3. 2. 3 設定変更等対応のフロー概要

設定変更等のフロー概要について「図3. 3 設定変更等フロー概要」に示す。

【想定シナリオ】設定変更の依頼により設定変更を行う。

仙台市	← →	統合NW運用管理 受託業者
<ul style="list-style-type: none"> 設定変更を依頼 (変更内容を指示) 	→	<ul style="list-style-type: none"> 設定変更の依頼を受理 (変更内容を確認)
		<ul style="list-style-type: none"> 変更手順の作成
<ul style="list-style-type: none"> 変更手順を受理 (作業内容を把握) 	←	<ul style="list-style-type: none"> 変更手順の送付 (作業内容を提示)
<ul style="list-style-type: none"> 変更手順を承認 	→	<ul style="list-style-type: none"> 変更手順の承認を受理
		<ul style="list-style-type: none"> 変更手順により変更作業を実施。 (変更後の正常性を確認)
<ul style="list-style-type: none"> 作業報告を受理 (作業結果を把握) 	←	<ul style="list-style-type: none"> 作業報告を送付 (作業結果を報告)

図3. 3 設定変更等フロー概要

3.3 運用状況

統合NWの運用状況について、運用管理仕様書の業務内容をもとに担当者からヒアリングした結果、障害の監視や障害対応、定期的なトラフィック分析や定例会での報告、定期点検や設定変更等の対応について、問題なく運用できていることを確認した。

4. 現行の統合NWにおける課題等

4. 1 中継網の帯域不足

4. 2 通信回線冗長化

4. 3 将来の拡張性

4. 4 LAN 配線

4. 5 内線電話

4. 現行の統合NWにおける課題等

本章では、統合NWにおける課題等について、業務委託仕様書に記載の課題を中心に調査・分析を行い、担当者からのヒアリングを行った結果を踏まえて整理した内容を記載する。仕様書に記載の課題は以下の通りである。

- (1) 中継網の帯域不足
- (2) 通信回線が冗長化されていない
- (3) 将来の拡張性について
- (4) LAN 配線
- (5) 内線電話

4. 1 中継網の帯域不足

【課題】

統合NWが使用している広域イーサ中継網の帯域が上限値に迫っていることから、これ以上WAN回線の統合が困難である。

【調査結果】

各種システムの統合NW接続を進める過程で、庁内LANの大規模で通信量の多いネットワーク（使用帯域10M～100Mbps）を収容したことにより、中継網の帯域に余裕が無い状態にあることを確認した。

また、市民利用施設予約システムでは、端末更新（Windows10導入）に伴い、当初に想定したシステム利用通信（使用帯域1Mbps～）の他に、OSのセキュリティパッチ配信等で大量の通信が発生することが想定され、中継網の帯域不足が課題となっている。

【改善策（案）】

案① 統合NWのWAN回線を複数の回線サービスに分割して契約する

複数のWAN回線に中継網が分離されるため帯域に余裕を持つことができる。

ただし、通信費用が現状と比較して大幅に増額となることが想定される。統合NWの運用コストも増額となるため十分な検討が必要である。

案② 仙台市の他ネットワークの WAN 回線を共同利用する

他ネットワークと同一の拠点で異なる WAN 回線を利用しており、他ネットワーク側の中継帯域にも余裕がある場合には、WAN 回線を共同利用することで通信量の分散を図ることができきる。

ただし、ポリシーの異なるネットワーク間を接続することになるため、双方で構成変更を行う必要があり、相互接続の条件や WAN 回線の通信費用の負担等、ネットワーク管理部門間での十分な協議が必要となる。WAN 回線の通信費用は増加しないが、構成変更による設計費用が発生する。

4. 2 通信回線の冗長化

【課題】

統合NWは通信回線が冗長化されていないため、可用性の面で課題がある。

【調査結果】

統合NWのセンター拠点である本庁舎の WAN 回線は冗長化されているが、情報システムセンターや区役所等の主要拠点であっても WAN 回線が冗長化されていないことを確認した。

WAN 回線は通信事業者の SLA により回復時間などの保守条件が設定できるが、内線電話網の VoIP 中継を行っていることを考慮すると、区役所等の主要拠点については WAN 回線の冗長化が必要である。バックアップ回線はメイン回線と別の通信事業者または別の回線サービスを利用する必要がある。

【改善策（案）】

案① 統合NWで新たにバックアップ回線を契約する。

メイン回線に障害が発生した場合でもバックアップ回線を経由して通信を継続することが可能となる。構成によってはバックアップ回線を利用して通信量の分散を図ることが可能となる。

ただし、通信費用が現状と比較して増額となることが想定される。メイン回線の障害等でバックアップ回線を利用する場合は各種システムの通信制限を行う等の縮退運用を検討する必要がある。

案② 仙台市の他ネットワークをバックアップ回線として共同利用する

他ネットワークと同一の拠点で異なる WAN 回線を利用しており、他ネットワーク側の通信帯域に余裕がある場合には、他ネットワーク側の WAN 回線をバックアップ回線として共同利用することができる。

ただし、ポリシーの異なるネットワーク間を接続することになるため、双方で構成変更を行う必要がある。相互接続の条件や WAN 回線の通信費用の負担等、ネットワーク管理部門間での十分な協議が必要となる。WAN 回線の通信費用は増加しないが、構成変更による設計費用が発生する。

4. 3 将来の拡張性

【課題】

統合NWは、外部から接続出来ない仕組みであり、情報漏えいやサイバー攻撃を阻止するためには有効な仕組みであるものの、市民サービスの向上や事務の効率化を含めた業務改善や働き方改革等を推進するにあたり、外部からの接続環境の整備やモバイル端末の活用を検討する必要がある、拡張性の面で課題がある。

【調査結果】

統合NWを WAN 回線として利用している各種システムの構成を調査したところ、インターネットや LGWAN 等の外部ネットワークとの接続については、ほとんどが庁内 LAN 系のシステムで運用されていることを確認した。

現状、統合NWとして市民や職員にサービスを提供している機能がないことや、複数の外部ネットワークとの接続を持つことがセキュリティのリスクを増大させる要因になることを考慮すると、外部からの接続環境の整備やモバイル端末の活用については、庁内 LAN も含めた拡張性として検討する必要がある。

関連する技術については、本業務で調査を行う動向調査報告書に記載することとする。

4. 4 LAN 配線

【課題】

各種システムが統合NWを利用する際、各庁舎における統合NW側の設備と各種システム側の設備の間のLAN配線は各種システムを所管する部署で敷設している。そのため、統合NW側の設備と各種システム側の設備が別の階にある場合、縦系配線がシステムごとに必要であることから、LANケーブルの重複による建物の配線スペースの課題と、各種システムごとにLAN配線を敷設することによる、費用の重複が課題である。

【調査結果】

統合NWをWAN回線として利用している各種システムの構成を調査したところ、各種システムごとにLANケーブルを敷設し運用していることを確認した。また、他ネットワークの構成を調査したところ、統合NWと同様に他ネットワークごとにLANケーブルを敷設し運用していること確認した。区役所等の縦系配線は電話交換機械室を起点として端末設置階のEPSを経由して敷設されており、この間についてはLAN配線の重複を確認した。

【改善策（案）】

案① 仙台市他ネットワークと縦系のLAN配線を一元的に管理する

統合NWの各種システムや他ネットワークで管理している縦系のLAN配線を一元的に管理することで、配線スペース（配管）の共同利用や予備配線の共同利用が可能となる。

ただし、敷設時の条件や管理方針の異なるLAN配線を一元的に管理することになるため、LAN配線に障害が発生した場合の対応やケーブル新設時の工事費用の負担等、ネットワーク管理部門間での十分な協議が必要となる。

案② 仙台市他ネットワークと縦系のLAN配線を統合する

統合NWの各種システムや他ネットワークで管理している縦系のLAN接続をNW仮想化の技術（タグVLAN等）を用いて統合することで、LANケーブル等の配線設備やL2スイッチ等のNW機器も含めた共同利用が可能となる。新たな端末設置階に中継用のL2スイッチが設置されている場合は、L2スイッチの設定変更を行いL2スイッチを起点として端末設置場所までの横系のLAN配線を敷設するだけで端末のネットワーク利用が可能となる。

ただし、ポリシーの異なるネットワーク間を接続することになるため、双方で構成変更を

行う必要がある。相互接続の条件や NW 機器に障害が発生した場合の対応等、ネットワーク管理部門間での十分な協議が必要となる。縦系 LAN 配線の工事費用は発生しないが、構成変更による設計費用が発生する。

4. 5 内線電話

【課題】

内線の VoIP 化にあたり、SIP サーバと VoIP ゲートウェイを統合 NW の設備として整備しているため、内線電話拠点の増設による番号計画の変更、VoIP ゲートウェイの増設等の費用面の課題や、構内電話交換機、SIP サーバ、VoIP ゲートウェイの管理等、ネットワークインフラとしてのあり方について検討する必要がある。

【調査結果】

統合 NW のデータ通信機能の運用管理は一般的な NW スキルで対応できる。各種システムの変更も新しい各種システムを接続したり利用拠点を増やす場合など限定的である。

VoIP 機能の運用管理は PBX や番号計画等より専門的なスキルが必要とされる。内線電話網の変更は組織改正や人事異動など定期的な作業が想定される。

ネットワークインフラ運用の観点から、VoIP 機能とデータ通信機能の管理は分離して行うことが可能である。特に内線電話網の VoIP 機能と各種システムのデータ通信機能で主管部署が異なる場合には、それぞれで管理することが望ましい。

【改善策（案）】

案① VoIP 機能と機器（呼制御装置、VoIP ゲートウェイ）の管理を分離する

VoIP 機能は統合 NW の各種システムと同様に別システムとして構成し運用する。音声通信は低遅延の通信が求められるため L3 通信機能や QoS 機能は、これまでと同等のレベルで提供することが必要である。

SIP サーバや VoIP ゲートウェイ間の通信インターフェースは規格化されているため、他ベンダ製の機器でも相互接続が可能である。拠点側の内線電話機器の保守を考慮すると、VoIP ゲートウェイは PBX 側の機器として管理する。SIP サーバは将来的な IP 電話機の導入も考慮して内線電話網の主管部門が管理することが望ましい。

案② 将来的な IP 電話機の導入を検討する

現状は拠点の PBX 間を VoIP ゲートウェイで相互に接続する VoIP ゲートウェイ方式を利用している。構内電話線の耐用年数は LAN ケーブルと比較して長いものの、フロア内のレイアウト変更を行う場合には、内線電話機（構内電話線）と PC（LAN ケーブル）の双方で配線作業を行う必要がある。

将来的な市役所新庁舎の建設や拠点設備の老朽化対策に対応するためにも、拠点内において内線電話機と PC で LAN ケーブルを共同利用することのできる IP 電話機（フル IP 方式）の導入を検討することを推奨する。IP 電話機を導入することで、SIP サーバのクラウド利用や IP セントレックス等のサービス利用の検討も可能となる。

災害等による停電時の直通電話等、アナログ電話利用のメリットもあるが、非常用電源がある拠点では PoE（Power Over Ethernet）による給電により IP 電話機の利用も可能である。将来的な IP 電話機の導入にあたっては十分な検討が必要である。

5. 通信回線統合の可能性について

5. 1 他ネットワークの調査

5. 2 通信回線統合の検討

5. 3 通信回線統合の可能性

5. 通信回線統合の可能性について

本章では、統合NWと他ネットワークとの通信回線統合の可能性を検討するにあたり、他ネットワークの調査・分析を行い、担当者からのヒアリングを行った結果を踏まえて整理した内容を記載する。

5. 1 他ネットワークの調査

統合NWと同様に拠点ネットワークを構築し運用している「基幹系ネットワーク」と「庁内LAN」の2つのネットワークを調査対象とした。現状の課題である「LAN配線」についても検討を行うため、WAN回線のみではなく庁舎内の縦系LAN配線や各種システムについて調査を行った。庁内LANについては外部ネットワーク接続について調査を行った。

5. 1. 1 基幹系ネットワーク概要

基幹系ネットワークの概要を「表5. 1 基幹系ネットワーク WAN回線サービス概要」「表5. 2 基幹系ネットワーク 各種システム概要」「図5. 1 基幹系ネットワーク 拠点WAN概要」「図5. 2 基幹系ネットワーク 拠点LAN概要」に示す。

表5. 1 基幹系ネットワーク WAN回線サービス概要 (1/4)

項目	内容		備考
回線種別① メイン回線	広域イーサネット網サービス (L2) (東北インテリジェント通信：V-LAN Limited)		
網内の帯域制限	無し (アクセス回線の帯域まで利用可能)		
保守条件	回線監視：有り、故障通知：有り、SLA：有り		
外部接続	無し (各種システムからの外部接続は除く)		
保守ベンダ監視	有り (IP-VPN サービス/フレッツ回線)		統合監視
アクセス回線の 帯域毎の回線数	1Gbps	1 回線	
	100Mbps	10 回線	
	10Mbps	34 回線	
	合計	45 回線	

表 5. 1 基幹系ネットワーク WAN 回線サービス概要 (2/4)

項目	内容		備考
回線種別② バックアップ回線	広域イーサネット網サービス (L2) (NTT 東日本: ビジネスイーサ ワイド)		
網内の帯域制限	有り (アクセス回線のサービス品目)		
保守条件	回線監視: 有り、故障通知: 有り、SLA: 有り		
外部接続	無し		
保守ベンダ監視	有り (IP-VPN サービス/フレッツ回線)		統合監視
アクセス回線の 帯域毎の回線数	100Mbps	1 回線	
	10Mbps	10 回線	
	1Mbps	11 回線	
	合計	22 回線	

表 5. 1 基幹系ネットワーク WAN 回線サービス概要 (3/4)

項目	内容		備考
回線種別③ 開発ネットワーク	広域イーサネット網サービス (L2) (東北インテリジェント通信: V-LAN Limited)		開発ルーム拠点
網内の帯域制限	無し (アクセス回線の帯域まで利用可能)		
保守条件	回線監視: 有り、故障通知: 有り、SLA: 有り		
外部接続	無し		
保守ベンダ監視	無し		
アクセス回線の 帯域毎の回線数	100Mbps	4 回線	
	合計	4 回線	

表 5. 1 基幹系ネットワーク WAN 回線サービス概要 (4/4)

項目	内容		備考
回線種別④ 住基ネット	広域イーサネット網サービス (L2) (東北インテリジェント通信: V-LAN Limited)		住民情報システム
網内の帯域制限	無し (アクセス回線の帯域まで利用可能)		
保守条件	回線監視: 有り、故障通知: 有り、SLA: 有り		
外部接続	無し (各種システムからの外部接続は除く)		
保守ベンダ監視	無し		
アクセス回線の 帯域毎の回線数	100Mbps	1 回線	
	10Mbps	9 回線	
	合計	10 回線	

表 5. 2 基幹系ネットワーク 各種システム概要 (1/4)

項目	内容		備考
住基システム	自動交付機	・基幹系ネットワークを利用	法務省連携 は暗号化の ため VPN を 構築
	住基ネット	・住基ネット WAN 回線を利用	
	コンビニ交付	・LGWAN 接続を利用	
	法務省連携 (外国人)	・LGWAN 接続を利用 ・庁内 LAN (VPN) を利用	

表 5. 2 基幹系ネットワーク 各種システム概要 (2/4)

項目	内容		備考
戸籍システム	戸籍端末	・基幹系ネットワーク (VPN) を利用	戸籍端末は 暗号化のため VPN を構築
	コンビニ交付	・LGWAN 接続を利用	
	法務省連携 (副本)	・LGWAN 接続を利用	

表 5. 2 基幹系ネットワーク 各種システム概要 (3/4)

項目	内容		備考
国保システム	国保総合 後期高齢 特定健診	・独自 WAN 回線を利用 (東北インテリジェント通信： 光回線イーサネットアクセス)	
	ねんきんネット	・独自 WAN 回線を利用 (NTT 東日本：フレッツ光 HF)	

表 5. 2 基幹系ネットワーク 各種システム概要 (4/4)

項目	内容		備考
税システム	コンビニ交付	・LGWAN 接続を利用	
	eLTAX	・LGWAN 接続を利用 ・独自 WAN 回線を利用 (東北インテリジェント通信： 専用回線)	

※上記以外で基幹系ネットワークのみを利用している各種システムについては記載しないこととする。

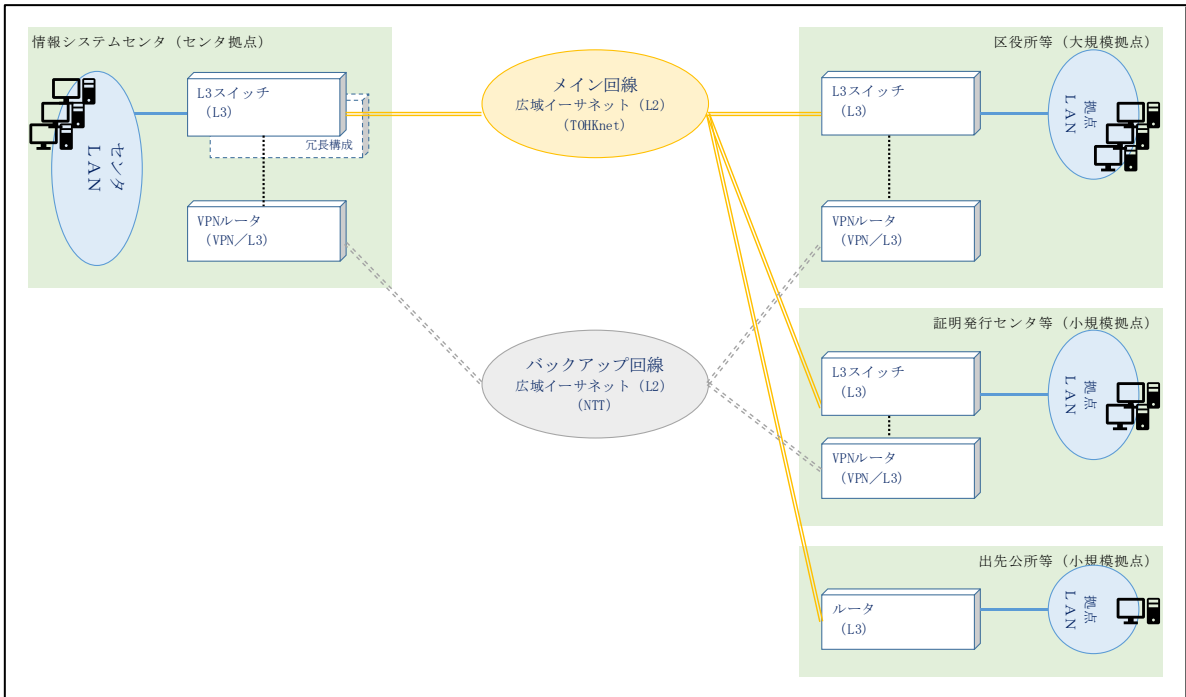


図 5. 1 基幹系ネットワーク 拠点 WAN 概要

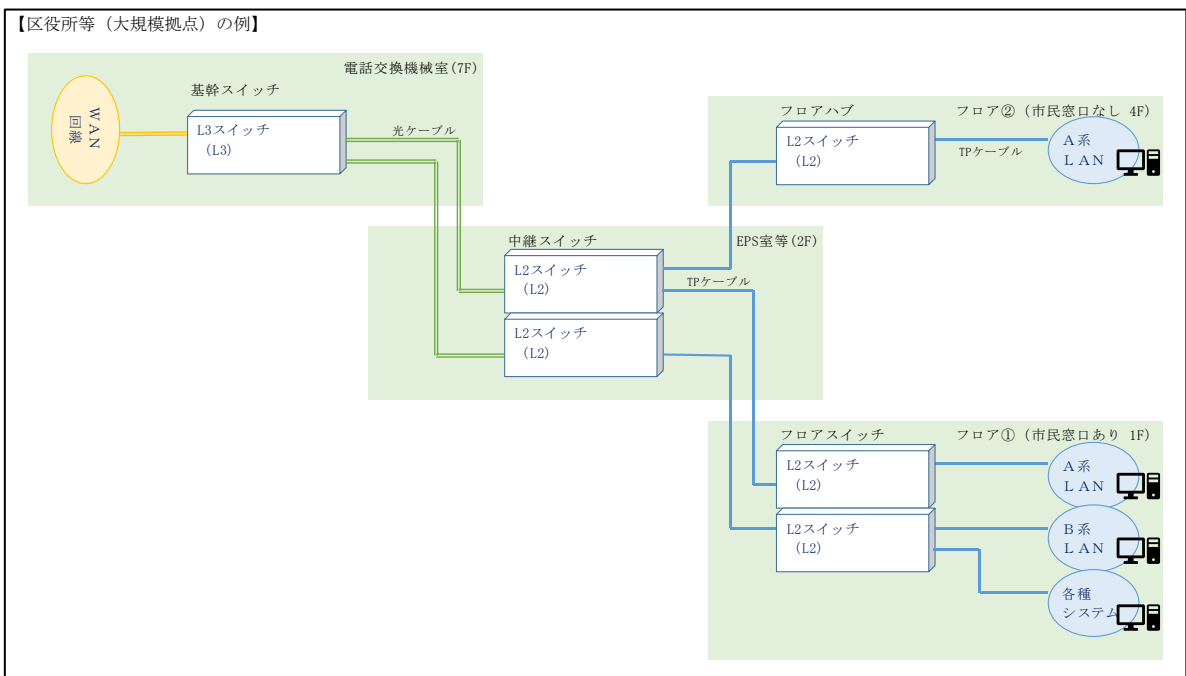


図 5. 2 基幹系ネットワーク 拠点 LAN 概要

5. 1. 2 庁内 LAN 概要

庁内 LAN の概要を「表 5. 3 庁内 LAN WAN 回線サービス概要」「表 5. 3 庁内 LAN 外部ネットワーク接続概要」「図 5. 3 庁内 LAN 拠点 WAN 概要」「図 5. 3 庁内 LAN 拠点 LAN 概要」に示す。

表 5. 3 庁内 LAN WAN 回線サービス概要 (1/2)

項目	内容		備考
回線種別① 統合NW	統合NW (VPN/L3) (統合NWの L3 中継機能を利用)		L2 通信のため VPN を構築
網内の帯域制限	有り (統合NWの QoS 機能による帯域制御)		
保守条件	統合NWに準ずる		
外部接続	・インターネット (宮城県自治体情報セキュリティクラウド経由) ・LGWAN		
保守ベンダ監視	無し		
帯域毎の拠点数	500Mbps	2 拠点	水道局本庁舎を含む
	100Mbps	13 拠点	
	10Mbps	29 拠点	
	合計	44 拠点	

表 5. 3 庁内 LAN WAN 回線サービス概要 (2/2)

項目	内容		備考
回線種別② F V W	VPN サービス (VPN/L3) (NTT 東日本：フレッツ VPN ワイド)		ルーティングのため VPN を構築
県外接続	有り (東日本エリア)		東京事務所
網内の帯域制限	無し (ベストエフォート)		
保守条件	回線監視：無し、故障通知：無し、SLA：無し		
外部接続	無し		
保守ベンダ監視	無し		
VPN グループ毎の拠点数	FVW①	40 拠点	ガス局、交通局、市立病院を含む
	FVW②	31 拠点	
	FVW③	50 拠点	
	合計	121 拠点	

表 5. 4 庁内 LAN 外部ネットワーク接続概要 (1/2)

項目	内容		備考
インターネット	アクセス回線	宮城県ハイパーウェブ (L2) (東北インテリジェント通信 : イーサネット回線サービス)	
	アクセス回線の帯域	300Mbps	
	上位ネットワークセンター (NOC)	宮城県自治体情報セキュリティクラウド	
	ファイアウォール	仙台市管理の機器を設置	

表 5. 4 庁内 LAN 外部ネットワーク接続概要 (2/2)

項目	内容		備考
LGWAN	アクセス回線	宮城県ハイパーウェブ (L2) (東北インテリジェント通信 : イーサネット回線サービス)	
	アクセス回線の帯域	100Mbps	
	上位ネットワークセンター (NOC)	LGWAN (宮城県 NOC)	
	ファイアウォール	仙台市管理の機器を設置	

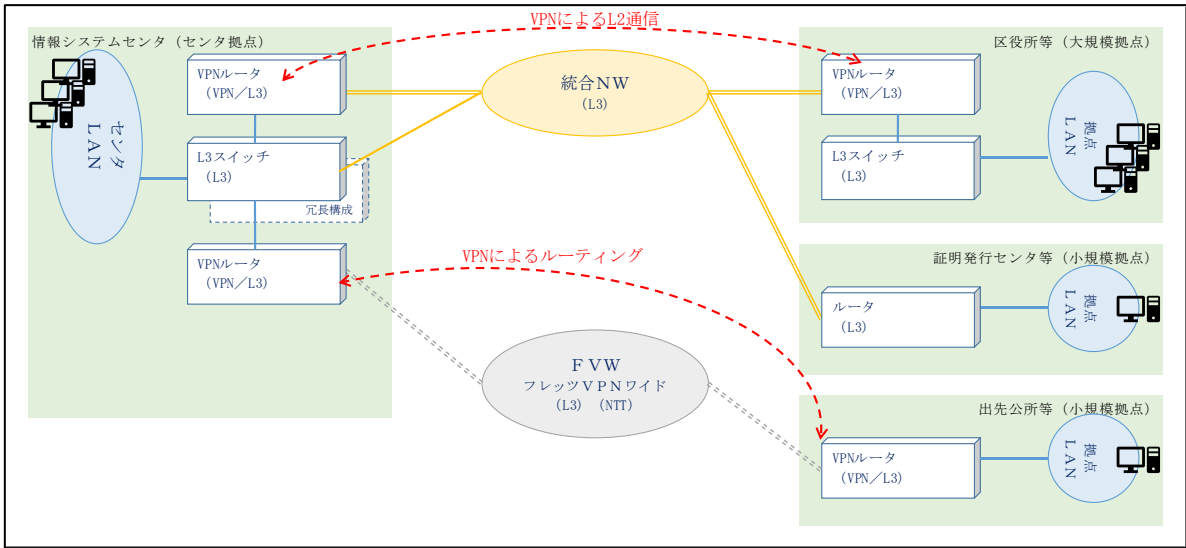


図5.3 庁内LAN 拠点WAN概要

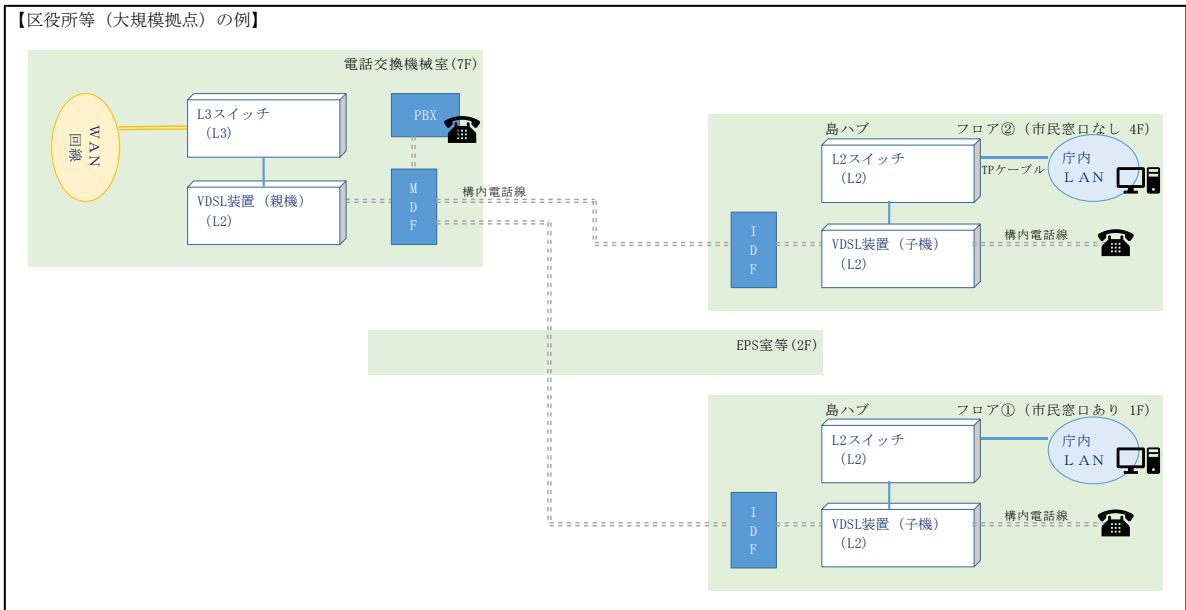


図5.4 庁内LAN 拠点LAN概要

5. 2 通信回線統合の検討

他ネットワークの調査結果を踏まえて、統合NWと他ネットワークの比較分析を行い、通信回線統合の方式（案）を検討した。統合NWは現状の課題を解決する観点から、基幹系ネットワークはバックアップ回線を共同利用する観点から、庁内 LAN は L2 通信のための VPN を不要とする観点から検討を行い、2つの方式（案）を策定した。また、将来的な構成（案）についても検討を行ったが詳細については本業務の基本計画（案）策定にて検討するものとする。

(1) WAN 回線を統合する方式（案）

(2) LAN 配線を統合する方式（案）

5. 2. 1 WAN 回線を統合する方式（案）

WAN 回線を統合する方式（案）のポイントを「表 5. 5 WAN 回線の統合のポイント」「図 5. 5 WAN 回線の統合のイメージ」に示す。

表 5. 5 WAN 回線の統合のポイント

対象 ネットワーク	ポイント（主な変更点）	備考
統合NW	① 基幹系ネットワークと相互に接続する。 （WAN 接続ルータと基幹系：VPN ルータ） ② 基幹系を経由するバックアップ経路を構築する。 ③ 基幹系ネットワークにバックアップ経路を提供する。	基幹系のバックアップ回線の利用拠点
基幹系 ネットワーク	④ 統合NWと相互に接続する。 （VPN ルータと統合NW：WAN 接続ルータ） ⑤ 統合NWを経由するバックアップ経路を構築する。 ⑥ 統合NWにバックアップ経路を提供する。	バックアップ回線の利用拠点
庁内 LAN	⑦ 現状どおり統合NWの各種システムとして運用する。 （バックアップ経路での縮退運用について検討する）	

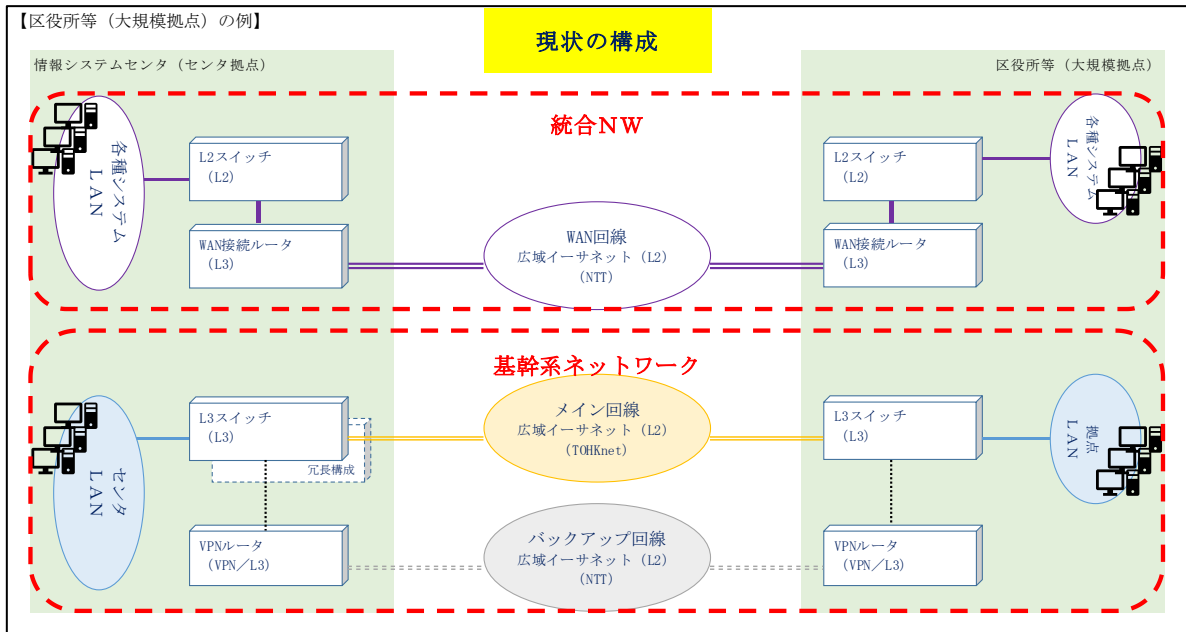


図 5. 5 WAN 回線の統合のイメージ (1/3)

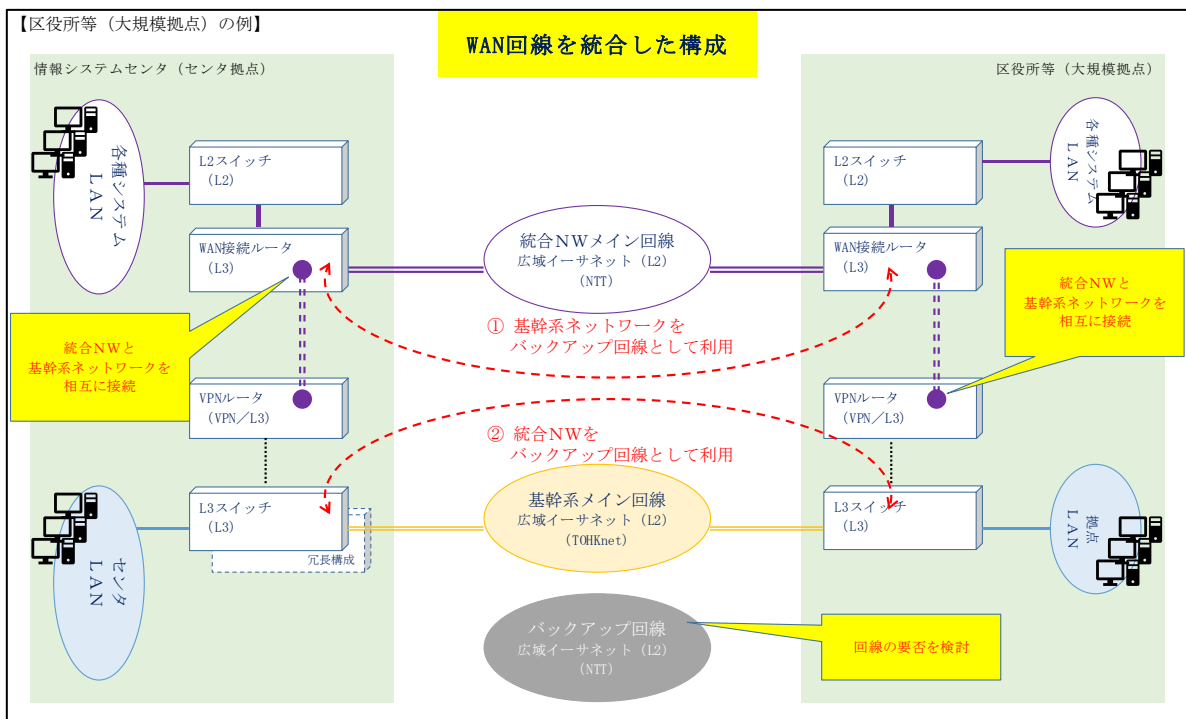


図 5. 5 WAN 回線の統合のイメージ (2/3)

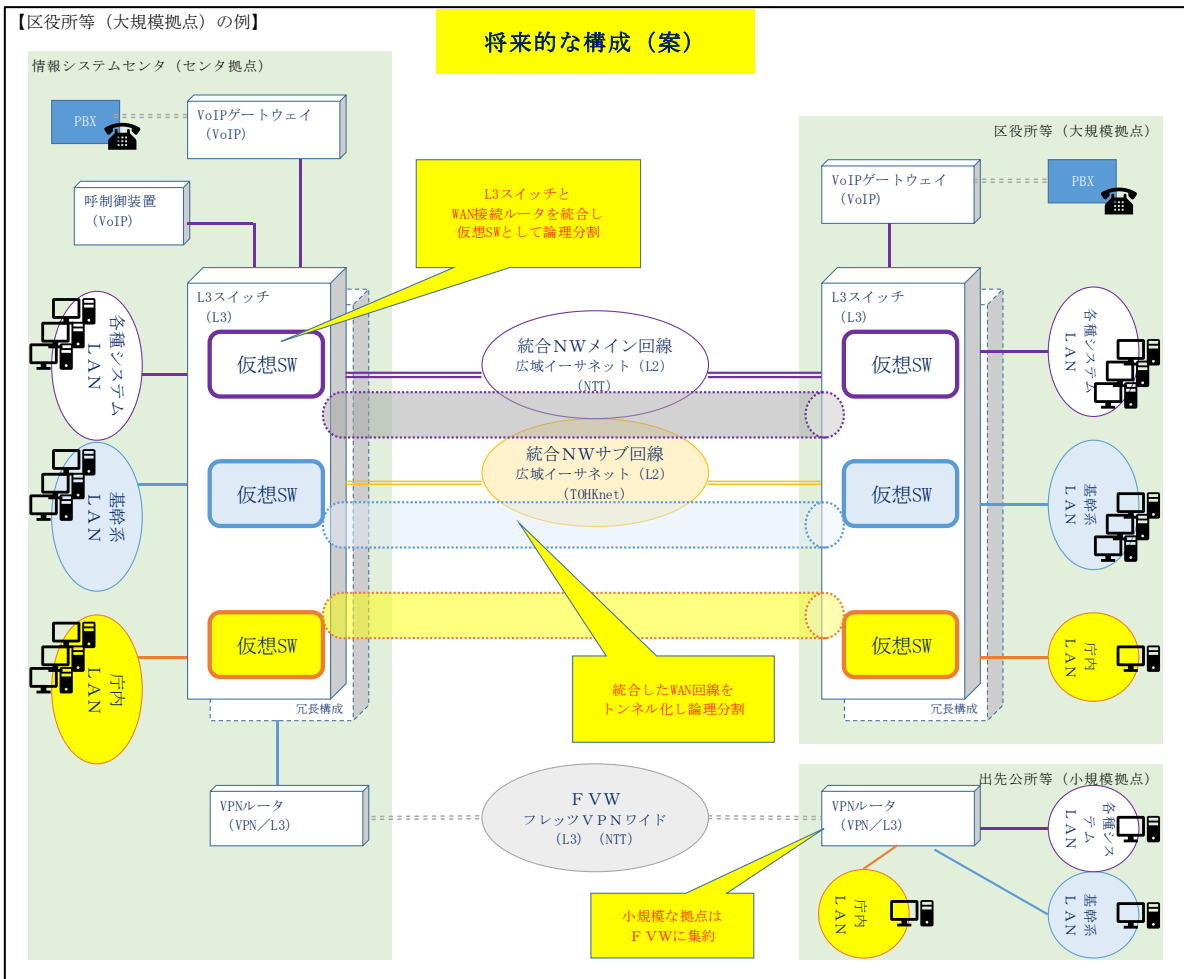


図 5. 5 WAN 回線の統合のイメージ (3/3)

5. 2. 2 LAN 配線を統合する方式 (案)

LAN 配線を統合する方式 (案) のポイントを「表 5. 6 LAN 配線の統合のポイント」「図 5. 6 LAN 配線の統合のイメージ」に示す。

表 5. 6 LAN 配線の統合のポイント

対象ネットワーク	ポイント (主な変更点)	備考
統合NW	<ul style="list-style-type: none"> ① 基幹系ネットワークと相互に接続する。 (L2 スイッチと基幹系 : L3 スイッチ) ② 縦系 LAN 配線の接続を基幹ネットワーク経由にする。 (各種システムと基幹系 : フロアスイッチ) 	各種システム の縦系 LAN 配 線
基幹系 ネットワーク	<ul style="list-style-type: none"> ③ 統合NWと相互に接続する。 (L3 スイッチと統合NW : L2 スイッチ、 フロアスイッチと統合NW : 各種システム) ④ 庁内 LAN と相互に接続する。 (L3 スイッチと庁内 LAN : L3 スイッチ フロアスイッチと庁内 LAN : 島ハブ) ⑤ 統合NW、庁内 LAN 用の経路を提供する。 (VLAN 設定、接続ポート) 	同一フロアに 統合NW、庁 内 LAN の LAN 配線があるフ ロア
庁内 LAN	<ul style="list-style-type: none"> ⑥ 基幹系ネットワークと相互に接続する。 (L3 スイッチと基幹系 : L3 スイッチ) ⑦ 縦系 LAN 配線の接続を基幹ネットワーク経由にする。 (島ハブと基幹系 : フロアスイッチ) 	VDSL 接続の LAN 配線

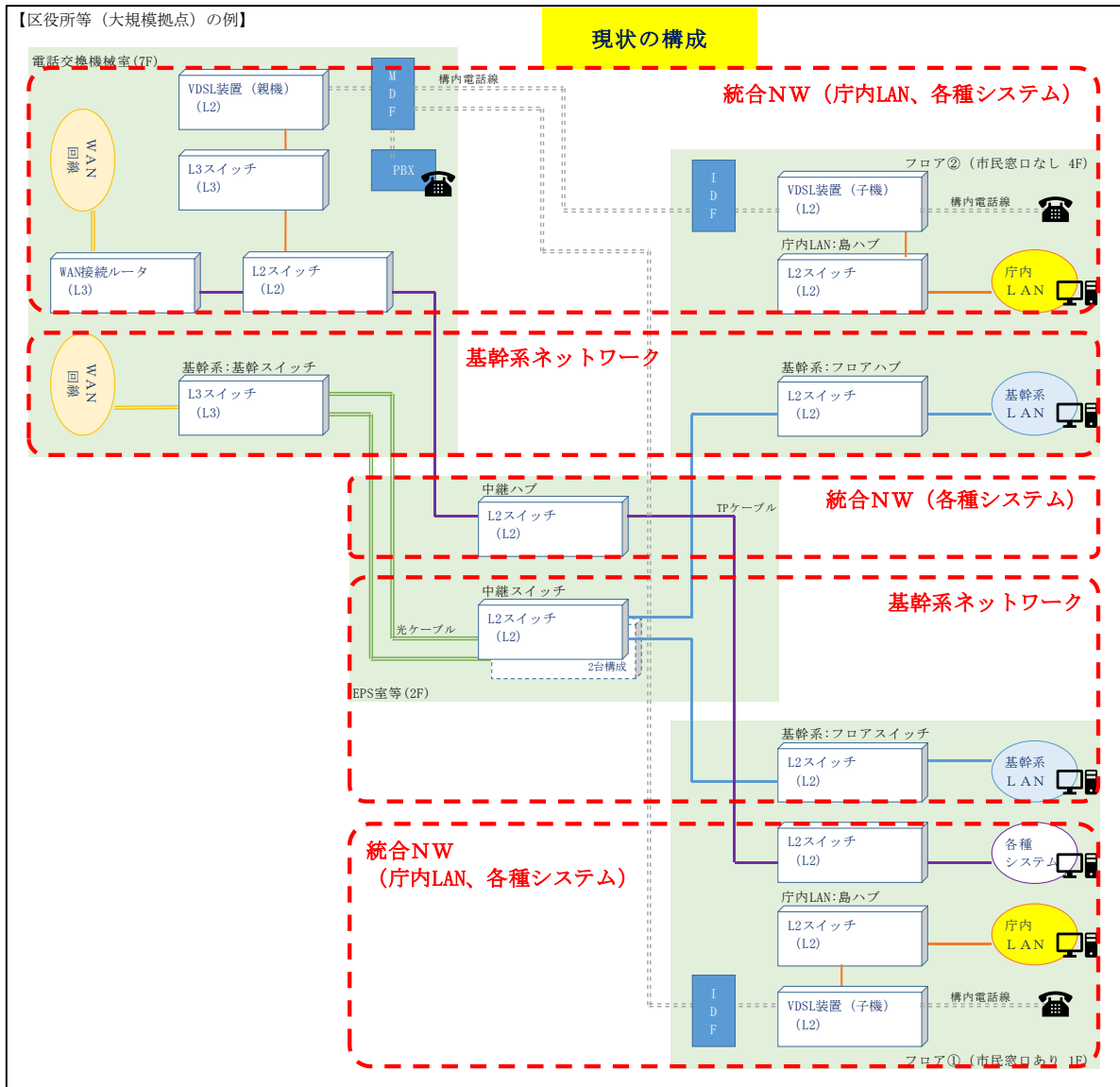


図5. 6 LAN配線の統合のイメージ (1/3)

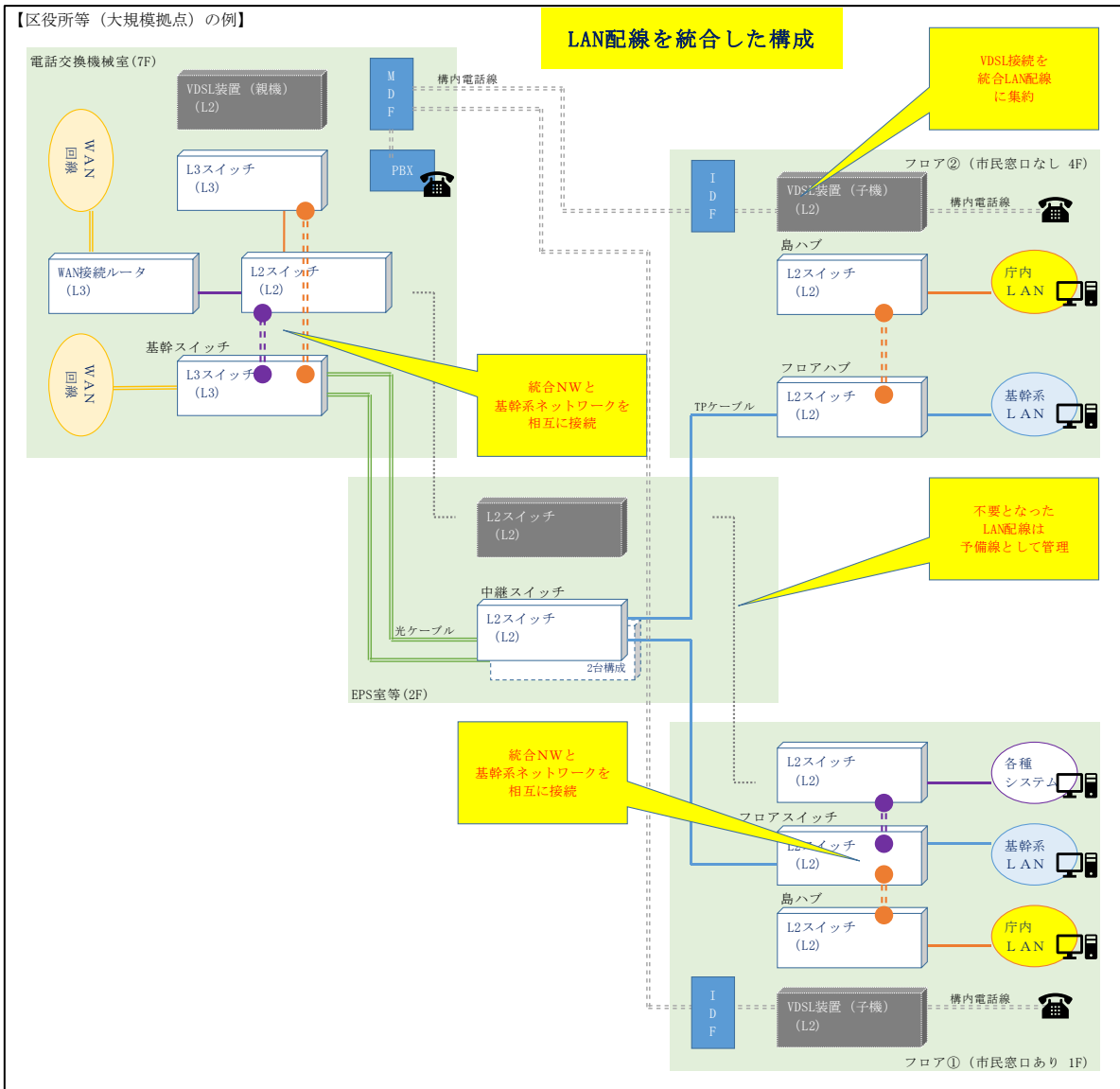


図5. 6 LAN配線の統合のイメージ (2/3)

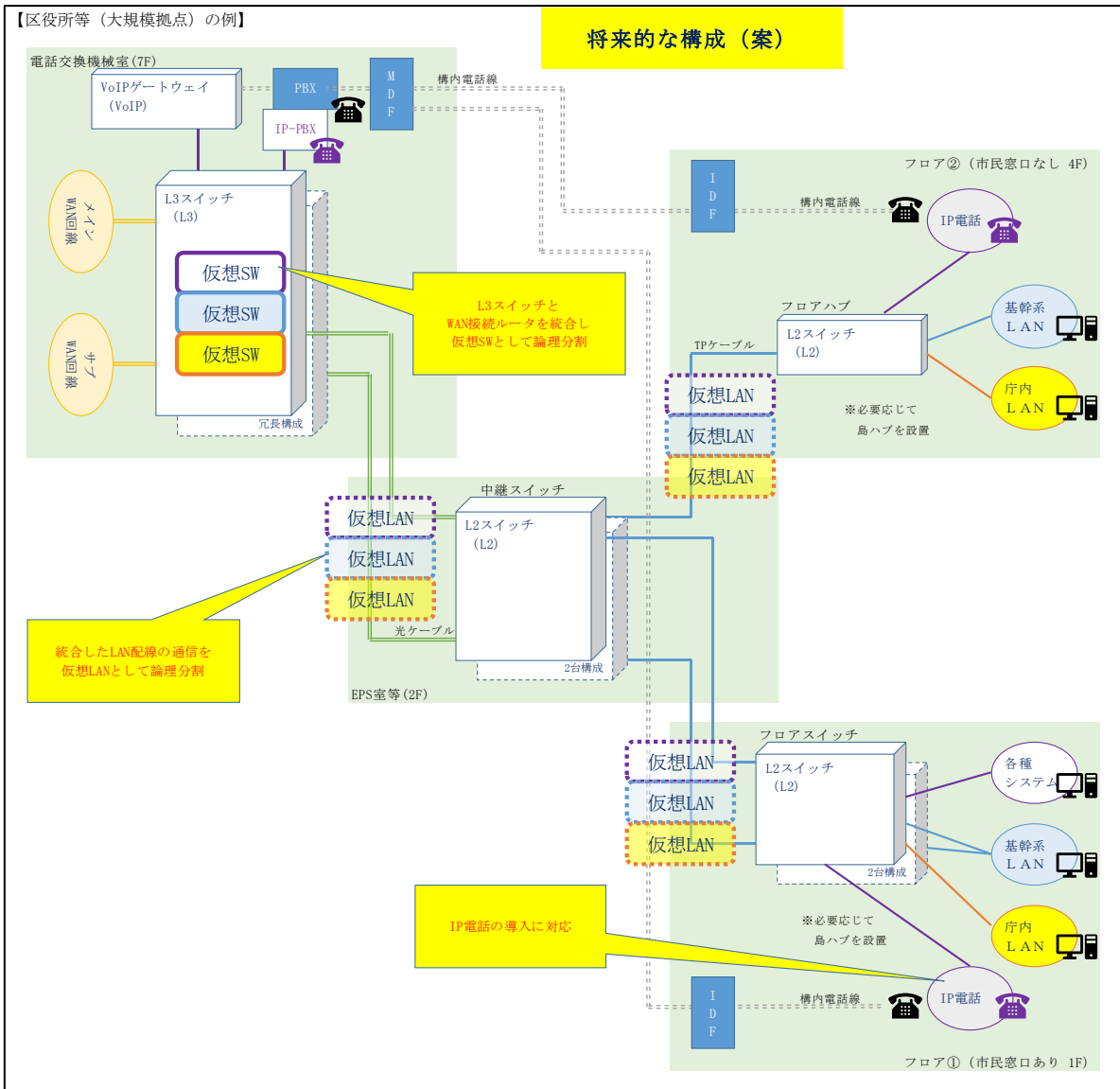


図5. 6 LAN配線の統合のイメージ (3/3)

5. 3 通信回線統合の可能性

統合NWと他ネットワークとの通信回線統合の方式（案）を検討した結果、WAN回線とLAN配線を共同利用することで段階的に通信回線を統合できる可能性を確認した。

本書では、通信回線統合の最初の段階であるWAN回線とLAN配線を共同利用する方式（案）までを検討し、将来的な構成（案）やネットワーク全体のあり方については、本業務の基本計画（案）策定にて検討することとする。

6. まとめ

6. 1 まとめ

6. まとめ

6. 1 まとめ

本書は、統合NWの現状について、構成管理資料や追加提供資料をもとに調査・分析を行い、担当者からのヒアリングを通して整理した内容をまとめた報告書である。

本業務において仙台市統合ネットワーク再構築基本計画を策定するうえでの検討資料とする。

仙台市統合ネットワーク再構築

動向調査報告書

Ver1.0

令和元年 7月25日

仙台市

目次

1.	はじめに.....	1
2.	仮想化技術.....	3
3.	無線 LAN.....	9
4.	リモートアクセス.....	13
5.	まとめ.....	17

1. はじめに

1. 1 動向調査の目的

1. 2 動向調査の範囲

1. はじめに

1. 1 動向調査の目的

本書は、仙台市統合ネットワーク再構築基本計画を策定するにあたり、新たな統合NW（以下「統合NW」と記載）の調達・構築・運用の検討に必要な各種技術動向や事例等について、調査・整理した内容を報告書に記載することを目的とする。

1. 2 動向調査の範囲

動向調査の範囲は以下の通りである。

(1) 仮想化技術

仮想化技術（サーバ仮想化・ネットワーク仮想化（WANの論理分割も含む）等）に関すること。

(2) 無線LAN

庁舎内で利用する無線LANに関すること。

(3) リモートアクセス

SSL-VPNや各種認証による外部から庁内ネットワークへのセキュアなアクセスに関すること。

2. 仮想化技術

2. 1 ネットワークの仮想化

2. 2 ネットワーク機器の仮想化

2. 3 通信経路の仮想化

2. 4 ネットワーク管理の仮想化

2. 仮想化技術

本章では、仮想化技術の技術動向について調査を行い、担当者からのヒアリングを行った結果を踏まえて整理した内容を記載する。

2. 1 ネットワークの仮想化

ネットワークの仮想化に関する技術から統合NWの再構築基本計画に関連するものとして、ネットワーク機器の仮想化、通信経路の仮想化、ネットワーク管理の仮想化の3つについて調査した。ネットワークの仮想化のイメージを「図2. 1 ネットワーク機器と通信経路の仮想化のイメージ」に示す。

2. 2 ネットワーク機器の仮想化

ネットワーク機器の仮想化は、機器を論理的に分割する方式と複数の機器を一元的に構成する方式がある。

(1) 機器を論理的に分割する方式

機器を論理的に分割する方式はネットワークパーティションとも呼ばれ、VRF (**V**irtual **R**outing and **F**orwarding) 方式が主流となっており、統合NWでもVRFを利用している。

VRFではL3通信に必要となるIPアドレス情報やルーティング情報を、同一機器の中で複数のインスタンスとして管理する。本来、ネットワーク毎に必要なルータやL3スイッチを1台の機器に集約して構成することができる。

複数のネットワークを扱うデータセンタでのネットワーク機器の集約化や、ネットワーク機器の台数を減らすことによる経費削減に利用されることが多い。

(2) 複数の機器を一元的に構成する方式

複数の機器を一元的に構成する方式は、従来、隣接するボックス型の機器を専用ケーブルで接続し1台の機器として構成するスタック方式が主流だった。

最近では、ネットワーク上の隣接しない機器をデータ通信のネットワーク経由で接続し1台の機器として構成する方式を利用するネットワークが増えてきた。従来は全ての機器を1台ずつ操作する必要があったが、この方式ではマスタとなる1台の機器を操作すること

で、ネットワーク全体の機器のコンフィグ情報を更新したりバックアップ情報やログ情報を収集できる。

管理するネットワーク機器の台数が多い大規模なネットワークでの運用管理にかかる工数を低減できる等の導入効果が期待されている。ただし、ほとんどがメーカー独自の技術で構成されるため、機器の選定においては十分な検討が必要である。

2. 3 通信経路の仮想化

通信経路の仮想化は、仮想化される通信経路の種類によって、LAN 通信経路を仮想化する方式と WAN 通信経路を仮想化する方式に分類できる。

(1) LAN 通信経路を仮想化する方式

LAN 通信経路を仮想化する方式は、L2 通信（フレーム）に ID タグを付与することにより機器間の通信経路を仮想的に多重化するタグ VLAN が主流である。IEEE802.1q として標準規格化されており、異なるメーカー間の機器でも互換性があるのが特徴である。ただし、同一セグメントで ID タグが一意である必要があり ID 範囲が最大 4094 個に限られている。

更に多くの VLAN を扱う方式としてタグ VLAN 通信（フレーム）に二重の ID タグを付与しタグ VLAN の中にタグ VLAN を通信させる方式がある。QinQ やダブルタグ VLAN と呼ばれる技術であり、元々は通信事業者の L2 サービス提供のために利用されることが多かった。最近では複数ネットワークを統合する方式として利用されることもある。

(2) WAN 通信経路を仮想化する方式

WAN 通信経路は主に通信事業者の回線サービスを利用する。回線サービスには機器間に L3 通信を提供する IP 網サービス、機器間に L2 通信を提供するイーサネット網サービスに分類される。統合NWの通信回線はイーサネット網サービスを利用している。

IP 網サービスで WAN 通信経路を仮想化する方式として、VPN (Virtual Private Network) がある。VPN は IP 網サービス上に仮想的なネットワークのトンネルを構築し、その中でプライベートな通信を行うことができる。

VPN ではトンネル内の通信経路を暗号化することが可能である。通信経路の暗号化を前提とした回線サービスを IP-VPN サービスと呼び、主に金融サービス等の秘匿性が求められる

WAN 回線で利用されることが多い。

VPN ではトンネル内の通信経路で L2 通信を行うことが可能である。L2TP と呼ばれる方式では先に取り上げたタグ VLAN を経由させることができる。庁内 LAN では統合 NW 上に L2TP によるトンネルを構築し L2 通信を行っている。

イーサネット網サービスで WAN 通信経路を仮想化する方式として、タグ VLAN を利用する方式が主流である。ただし、通信事業者の設備でタグ VLAN を利用しているため、QinQ やダブルタグ VLAN 等による通信経路の仮想化は利用できない場合が多い。

最近では VXLAN (Virtual eXtensible LAN) と呼ばれる仮想化技術により、ID タグではなく VXLAN_ID と呼ばれる新たな ID を用いた VPN 技術により、イーサネット網サービス上に VXLAN トンネルを構築し、複数のタグ VLAN による通信を行うことができる。また、VXLAN は IP 網サービスでも利用することができるが、通信性能は IP 網の性能に依存するため導入にあたっては十分な検討が必要である。

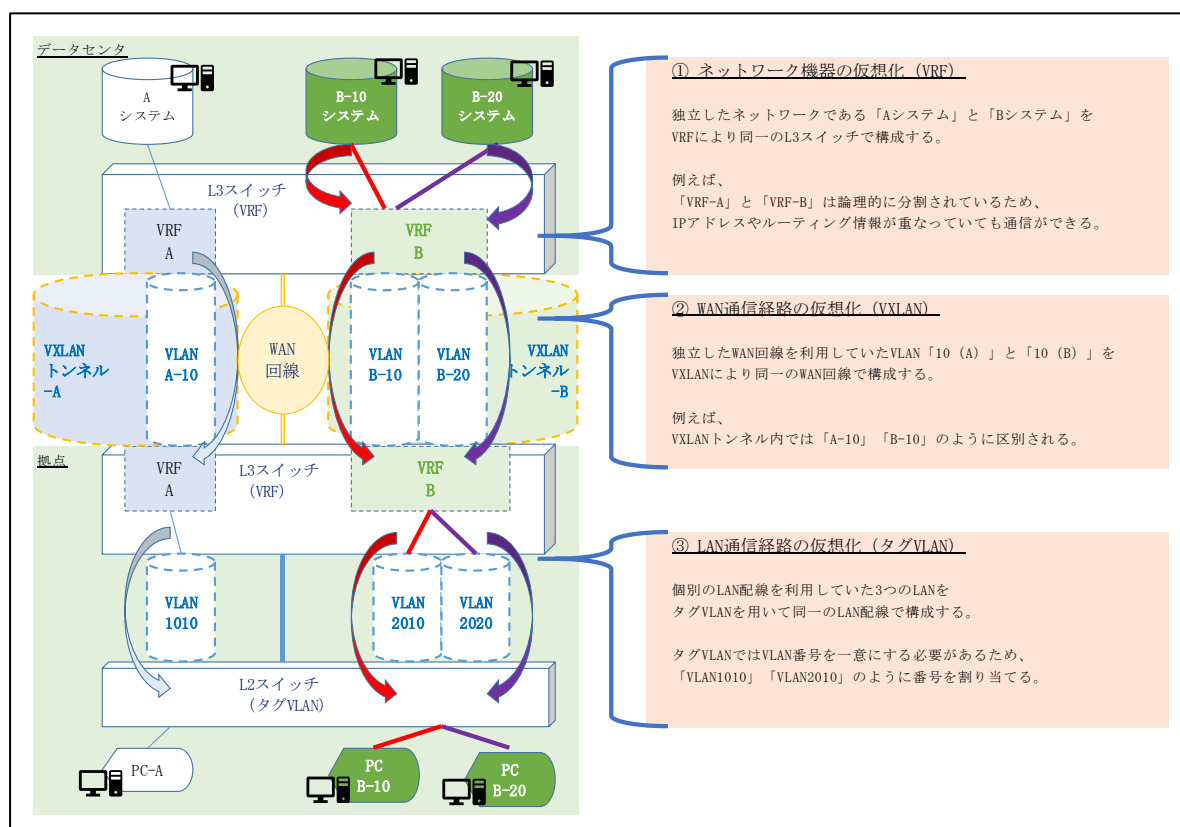


図2. 1 ネットワーク機器と通信経路の仮想化のイメージ

2. 4 ネットワーク管理の仮想化

ネットワーク管理の仮想化は、ネットワーク機器管理の仮想化とネットワーク管理サーバの仮想化に分類できる。ネットワーク管理の仮想化に対応した製品について「表 2. 1 ネットワーク管理仮想化の対応製品（例）」に示す。

(1) ネットワーク機器管理の仮想化

従来のネットワーク機器の管理は、機器 1 台ごとにコンソール接続を行うことで設定情報の変更や機器故障時の設定リストア作業を行う必要があった。

最近ではマスタとなる機器や管理サーバ上で全ての機器の構成情報を一元的に管理することで、関連する設定情報を一斉に変更したり、機器故障時にハードウェアを交換するだけで自動的に設定情報をリストアすることができる製品がある。

広域で拠点数が多いネットワークの保守性を向上し、保守費用を低減する目的で導入される場合が多い。ただし、ほとんどがメーカー独自の技術で構成されるため、機器の選定においては十分な検討が必要である。

(2) ネットワーク管理サーバの仮想化

ネットワーク管理サーバは、一般的に専用のサーバ機器にサーバ OS やネットワーク管理ソフトウェアを導入して運用する。統合 NW でも専用サーバを運用している。

ネットワークの正常を監視し継続的にトラフィック情報を収集する等の重要な役割を持つサーバであるが、専用のサーバ機器を利用するため費用面等の理由から冗長構成が取られていないことが多い。また、管理サーバは管理する機能ごとにサーバを構築するため、システム管理者は複数のサーバを管理する必要がある。サーバの故障時にはネットワーク機器と同様にサーバ 1 台ごとの回復作業が必要であり、運用面の課題となる場合が多い。

サーバの仮想化技術を用いてネットワーク管理サーバを仮想化することで、サーバ機器のハードウェア故障時におけるサーバの可用性を向上させることができるほか、システムのバックアップやリストア等の運用面での簡易化も期待できる。

従来は仮想サーバ上でサーバ OS や管理ソフトウェアを構築し物理サーバと同様に運用することが主流であった。最近では、仮想サーバ上で運用されることを前提にした VA (Virtual Appliance) 版の管理製品もあり、管理サーバ導入時の選択肢が広がっている。

表 2. 1 ネットワーク管理仮想化の対応製品（例）

メーカー	内容		備考
CiscoSystems	Cisco DNA 製品群 (IOS XE 製品)		ソフトウェア製品、ハードウェア機能
	Cisco Prime 製品群 (IOS 製品)		
	コンフィグ情報の一元管理	一部の製品のみ対応	
	ファームウェアの一元管理	一部の製品のみ対応	
	設定変更の支援機能	一部の製品のみ対応	
	機器故障時の自動回復	未対応	
アラクサラネットワークス	AX-Network-Manager 製品群		ソフトウェア製品、ハードウェア機能
	コンフィグ情報の一元管理	AX シリーズ	
	ファームウェアの一元管理	AX シリーズ	
	設定変更の支援機能	AX シリーズ	
	機器故障時の自動回復	一部の製品のみ対応	
アライドテレシス	AT-Vista Manager 製品群		ソフトウェア製品、ハードウェア機能
	Autonomous Management Framework (AMF) 機能		
	コンフィグ情報の一元管理	AMF 対応機種	
	ファームウェアの一元管理	AMF 対応機種	
	設定変更の支援機能	AMF 対応機種	
	機器故障時の自動回復	AMF 対応機種	
ApresiaSystems	APRESIA Network Resource Center (ANRC) 製品群		ソフトウェア製品、ハードウェア機能
	VirtualBoxCore (VB) 機能		
	コンフィグ情報の一元管理	Apresia シリーズ	
	ファームウェアの一元管理	Apresia シリーズ	
	設定変更の支援機能	Apresia シリーズ	
	機器故障時の自動回復	未対応	

3. 無線 LAN

3. 1 庁舎内での無線端末利用

3. 2 無線 LAN 通信の概要

3. 3 無線 LAN 技術の動向

3. 無線 LAN

本章では、無線 LAN の技術動向について調査を行い、担当者からのヒアリングを行った結果を踏まえて整理した内容を記載する。無線 LAN 通信のイメージを「図 3. 1 無線 LAN 通信のイメージ」に示す。

3. 1 庁舎内での無線端末利用

庁舎内での無線端末利用は、職員による会議等での PC 端末利用によるペーパーレス化や、来庁した市民へ情報提供を行うためのタブレット端末等の利用が想定される。

また、執務室のフリーアドレス化に伴い庁内 LAN 端末の無線 LAN 化も想定される。

3. 2 無線 LAN 通信の概要

無線 LAN 通信は、無線通信の基地局となるアクセスポイント（無線 AP）と無線 LAN 端末から構成される。L2 通信の経路であり有線 LAN と同様の通信が可能である。通信方式は IEEE802.11 として規格化されており一般的には Wi-Fi の名称で呼ばれている。

無線 LAN 通信は電波を用いる通信方式であり通信信号が周囲に拡散される。有線 LAN と比べて情報漏えいのリスクが大きくセキュリティ対策が必須となる。主なセキュリティ対策としては、無線 LAN 端末を認証する接続認証と無線 LAN 通信の秘匿性を確保する暗号化がある。

接続認証では、ESSID と呼ばれる無線 AP の ID とパスワードによる認証が基本となる。内部ネットワークでの無線 LAN 利用では不正接続を防止する対策が必要であり、無線 LAN 端末の MAC アドレスを用いた MAC 認証やデジタル証明書を用いた証明書認証、ユーザ認証基盤（AD、LDAP 等）と連動したユーザ認証を行うことが推奨される。

無線 LAN の暗号化は、接続認証と合わせて暗号化方式を選択する。従来は WEP（Wired Equivalent Privacy）と呼ばれる方式が主流であったが、通信方式に脆弱性がある等の理由から、最近では WPA（Wi-Fi Protected Access）方式が主流となっており、更なる強度を持った方式も開発されている。無線 LAN の暗号化方式は脆弱性等の発見により度々強化されている。無線 AP を古い暗号化方式のままで利用し続けているとセキュリティのリスクが増大するため注意が必要である。

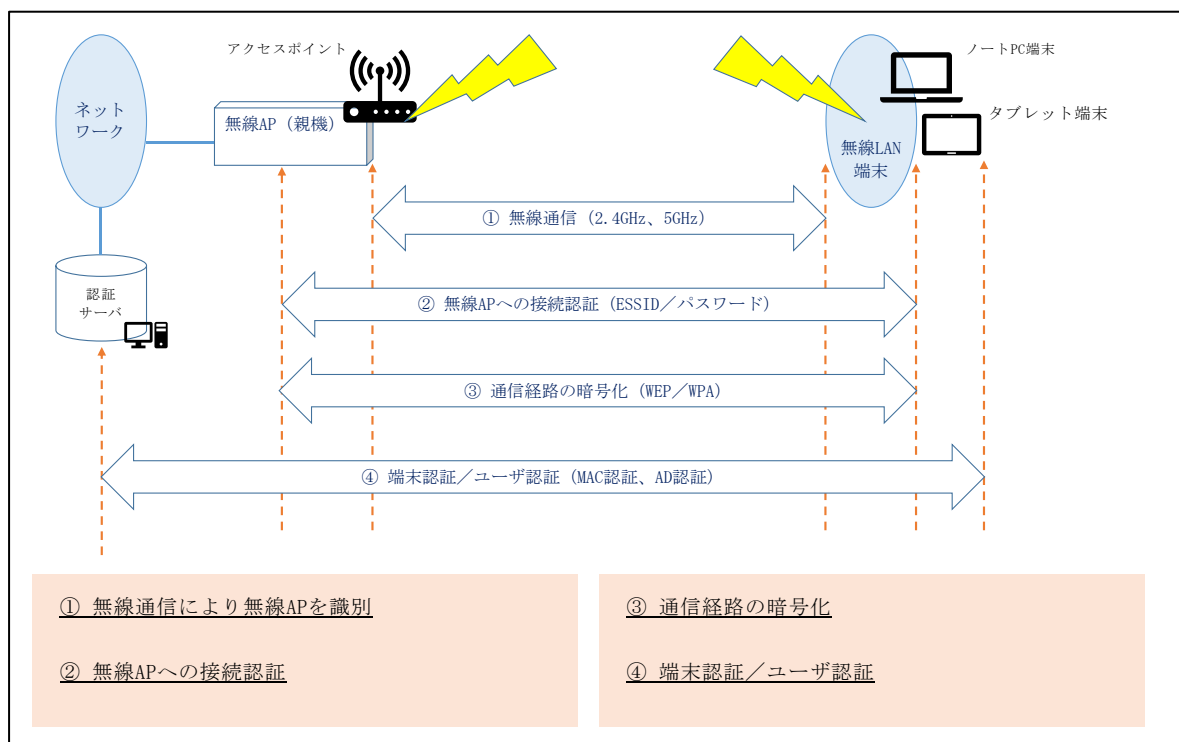


図 3. 1 無線 LAN 通信のイメージ

3. 3 無線 LAN 技術の動向

無線 LAN (Wi-Fi) を利用できる携帯端末等の普及によるセキュリティの強化やデジタルコンテンツの大容量化、リアルタイム通信の必要性から新しい無線 LAN 規格が開発されている。IEEE802.11ax として規格化され Wi-Fi6 (第 6 世代 Wi-Fi) と呼ばれている。

【Wi-Fi6 の特徴】

- (1) より高速な無線 LAN 通信が可能 (コンテンツの大容量化に対応)
- (2) より低遅延な無線 LAN 通信が可能 (リアルタイム通信の必要性に対応)
- (3) 弱い受信電波での通信が可能 (無線 LAN 通信距離の拡大)
- (4) より省電力での通信が可能 (無線 LAN 端末の省電力化)

庁舎内での無線 LAN 端末の業務利用においては、大容量でリアルタイム性が必要な通信を行うケースは少ないと考えられる。無線 LAN 技術の動向は、将来的なネットワーク利用のあり方を検討する上で必要な情報である。

4. リモートアクセス

4. 1 庁舎外での業務端末利用

4. 2 リモートアクセス通信の概要

4. 3 リモートアクセス技術の動向

4. リモートアクセス

本章では、リモートアクセスの技術動向について調査を行い、担当者からのヒアリングを行った結果を踏まえて整理した内容を記載する。リモートアクセス通信のイメージを「図4. 1 リモートアクセス通信のイメージ」に示す。

4. 1 庁舎外での業務端末利用

庁舎外での業務端末利用は、緊急時における遠隔からの庁舎内へのメッセージ配信やシステム状態の確認等での利用が想定される。また、出張先に紙媒体を持参する業務について、リモートアクセスで庁舎内の業務システムを参照することで、紙媒体を紛失する情報漏えいのリスクを低減できるが、モバイル端末を紛失するリスクも考慮する必要がある。

4. 2 リモートアクセス通信の概要

リモートアクセス通信は、外部からのアクセスを受付けるリモートアクセスゲートウェイと外部からアクセスを行うモバイル端末で構成される。従来は発信元が特定できる電話回線によるアクセスが主流だった。その後インターネット環境の普及に合わせて、インターネット経由でのアクセスが主流となり、通信回線も無線 LAN (Wi-Fi) が主流となっている。インターネット経由でのリモートアクセスは VPN (Virtual Private Network) 方式が利用される。

VPN 方式は、その接続形態から IPsec と SSL-VPN に分類できる。IPsec は L3 通信の IP パケットを暗号化する方式であるが、接続元と接続先の双方で固定グローバル IP アドレスが必要であるほか、通信経路上のアドレス変換 (NAT) に対応できないものがあるため、主に拠点間の VPN 接続で利用される。SSL-VPN は Web サーバ等へのアクセスで利用される SSL 通信

(https) を利用して VPN を構築する方式である。Web サーバへ接続できるインターネット環境があれば利用できるほか、通信経路上のアドレス変換 (NAT) に対応していることから、モバイル端末で利用されることが多い。

SSL-VPN の接続は、はじめに Web サーバの SSL 通信 (https) と同様にリモートアクセスゲートウェイに対して SSL 接続を行う。リモートアクセスゲートウェイは SSL の認証と暗号化に必要なサーバ証明書を送信しモバイル端末との間で SSL 通信が確立される。次に ID/パスワードによるユーザ認証が行われる。ユーザ認証では二要素認証としてデバイス認証やクライアント証明書による認証を行うことでセキュリティを強化することができる。最後に VPN 通信

(IP トンネル)を開始する。IP トンネルではモバイル端末からの全通信をVPN 経由とする(フルトンネリング)ことで、内部ネットワークと同等の通信を行うことが可能である。また、特定の内部ネットワーク宛て通信のみをVPN 経由とする(スプリットトンネリング)ことで、インターネット経由でクラウド上のサービスを利用しながら、VPN 経由で内部ネットワークのサービスを利用することができる。

SSL-VPN の接続では Web サーバと同じ https 通信を利用しているため内部から外部ネットワークへ向けた SSL-VPN の構築も簡単にできる。利用者が意図せずにバックドア(セキュリティホール)を作ってしまうことが想定されるため、内部ネットワーク側で Web フィルタリングやプロキシサーバ認証等、十分なセキュリティ対策を行うことが必要である。

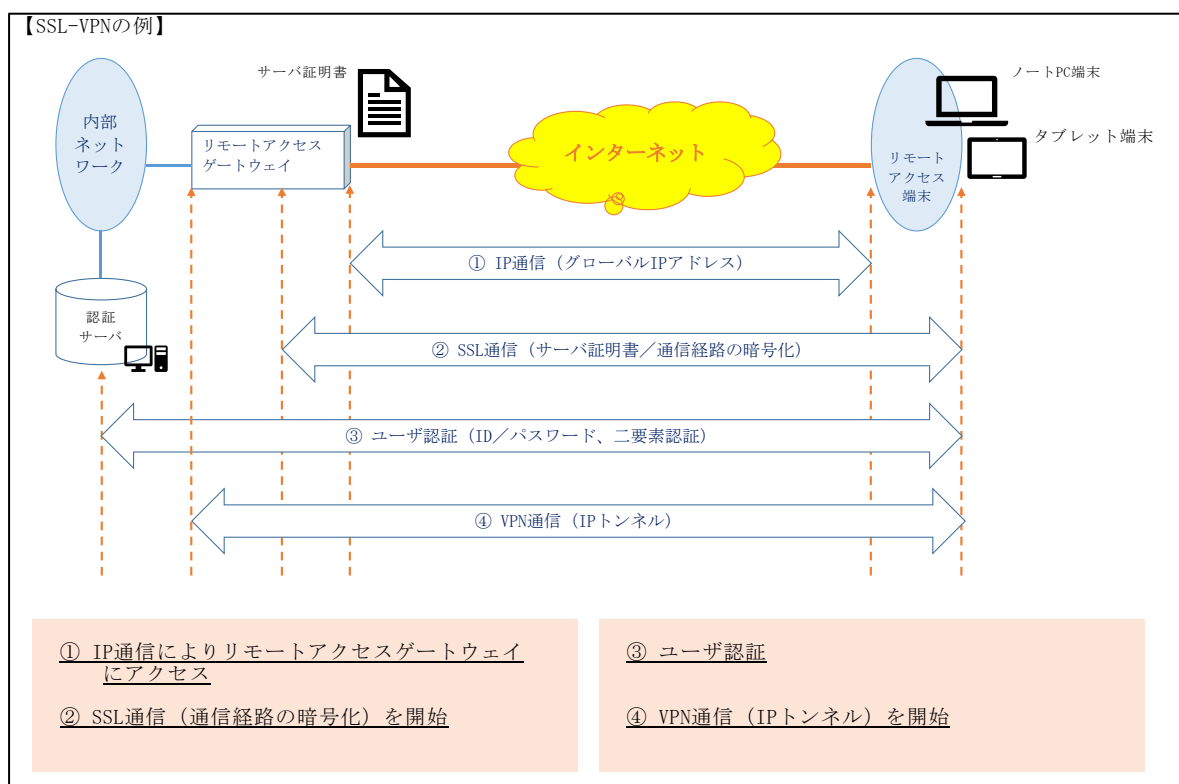


図4. 1 リモートアクセス通信のイメージ

4. 3 リモートアクセス技術の動向

リモートアクセスを行うためにはモバイル端末と通信回線が必要である。従来は持ち出し専用の PC (HDD を暗号化、データ出力不可等のセキュリティ対策を施したもの) を携帯し、通信先が限定されたデータ通信カード (通信事業者の VPN サービスに接続) を利用することが主流であった。

最近ではタブレット端末やスマートフォン等の携帯端末の業務利用や出張先での Wi-Fi 環境を利用したリモートアクセスの利用が主流になってきた。

タブレット端末は持ち出し専用 PC のようなセキュリティ対策が難しいため、モバイル端末にポリシーによる利用制限を適用しネットワーク経由で遠隔から管理するエンタープライズモビリティ管理 (EMM: **E**nterprise **M**obility **M**anagement) という管理方式が利用されている。EMM により、モバイル端末へのデータ保存やデータ出力、利用できるアプリを制限できるほか、GPS 位置情報を利用してモバイル端末の移動履歴を記録することで、モバイル端末の紛失時の対策を行うことができる。

通信回線は出張先での Wi-Fi 環境を利用するため必然的にインターネット経由でのリモートアクセスとなる。

また、個人所有のモバイル端末から業務を利用する BYOD (**B**ring **Y**our **O**wn **D**evice) という考え方がある。個人所有のモバイル端末を EMM で管理することは出来ないため、リモートアクセス時にモバイル端末のセキュリティ状態をチェックし、一定の条件を満たした場合のみアクセスを許可する等の対策が必要となる。

庁舎外からのリモートアクセスによる端末の業務利用を行うには、端末の管理方針や情報漏えいのセキュリティ対策等、導入にあたっては十分な検討が必要である。リモートアクセス技術の動向は、将来的なネットワーク利用のあり方を検討する上で必要な情報である。

5. まとめ

5. 1 動向調査の結果

5. まとめ

5. 1 まとめ

本書は、新たな統合NWの調達・構築・運用の検討に必要となる各種技術動向や事例等について調査を行い整理した内容をまとめた報告書である。

本業務において仙台市統合ネットワーク再構築基本計画を策定するうえでの検討資料とする。

仙台市統合ネットワーク再構築

要求定義書

Ver1.1

令和元年 10月10日
仙台市

目次

本書の目的.....	1
1. 統合ネットワーク概要.....	2
2. 機能要件.....	6
3. 非機能要件.....	8
4. 移行要求.....	12
5. 運用保守要求.....	13

本書の目的

本書は、仙台市統合ネットワーク再構築基本計画を策定するにあたり、統合ネットワーク（以下「統合NW」と記載）の現状調査・分析と動向調査の結果を踏まえ、新たな統合NWに必要な要求事項を取りまとめて整理した内容を要求定義書に記載したものである。

要求定義の範囲を以下に示す。

- ① 統合ネットワーク概要
- ② 機能要件
- ③ 非機能要件
- ④ 移行要求の具体化
- ⑤ 運用保守要求の具体化

1. 統合ネットワーク概要

統合NWの概要として、全体構成、統合対象通信回線、ネットワーク機器設置環境、ハードウェア要件、ソフトウェア要件、ネットワーク要件を記載する。

1. 1 全体構成

統合NWの全体構成を、別紙「図 1. 1 ネットワーク概要構成図」に示す。
概要構成図は、以下のパターンで構成する。

- ① WAN： ネットワークの全体構成を示す。
拠点の構成により以下のパターンに分類する。
 - センタ拠点： 情報システムセンター
 - タイプ A 拠点： 統合するシステム数が多く、WAN 回線を冗長化する拠点
 - タイプ B 拠点： 市民向けの窓口端末があり、WAN 回線を冗長化する拠点
 - タイプ C 拠点： 市民向けの窓口端末がなく、WAN 回線を冗長化しない拠点
 - タイプ D 拠点： ベストエフォート型 WAN 回線で VPN を構成する拠点
- ② タイプ C 拠点詳細： タイプ C 拠点の詳細パターンを示す。
- ③ LAN： タイプ A 拠点の LAN 構成を示す。

1. 2 統合対象通信回線

統合対象とする通信回線の一覧を、別紙「表 1. 1 統合対象通信回線」に示す。
通信回線の一覧は、以下のパターンで構成する。

- ① ギャランティ型 WAN 回線
通信帯域を保証する WAN 回線を利用する。一部の拠点で WAN 回線を冗長化する。
- ② ベストエフォート型 WAN 回線
通信帯域を保証しない WAN 回線を利用する。拠点間で VPN を構成する。

1. 3 ネットワーク機器設置環境

ネットワーク機器設置環境を、別紙「図 1. 2 ネットワーク機器設置環境」に示す。

ネットワーク機器の設置環境は、以下のパターンで分類する。

- ① フラック： シャーシ型の NW 機器やサーバ等を搭載する。
- ② ハブボックス： ボックス側の NW 機器を搭載する。
- ③ 机上設置： ゴム足やマグネットで設置する。

1. 4 ハードウェア要件

機器パターン毎のハードウェア要件を、別紙「表 1. 2 ハードウェア要件」に示す。

ハードウェア要件は以下のパターンで構成する。

- ① データ通信機器 (WAN)： 拠点間のデータ通信を行う。
- ② データ通信機器 (LAN)： 拠点内のデータ通信を行う。
- ③ VoIP 機器： 内線電話の VoIP 通信を行う。
- ④ 運用監視機器： ネットワークの運用監視を行う。

1.5 ソフトウェア要件

運用監視機器のソフトウェア要件を、「表 1.3 ソフトウェア要件」に示す。

表 1.3 ソフトウェア要件

項目	内容
NW 監視サーバ OS	WindowsServer2019 相当とする。
NW 監視ソフトウェア	NNM (NetworkNodeManager) ソフトウェア ・ ICMP、SNMP を用いて NW 機器を自動的に検出し、監視用のマップを自動的に生成できる。 ・ 対象ノードの生存監視を行い、異常時には外部コマンドによるアラート通知ができる。 ・ Web コンソールが利用でき、ネットワーク経由で管理できる。 ・ 日本語での GUI 表示ができる。 ・ 500 ノードの機器を管理できるライセンスを有している。
シスログサーバ OS	・ WindowsServer2019 相当とする。
SYSLOG ソフトウェア	SyslogServer ソフトウェア ・ 200 台以上の機器からの Syslog 転送を受信し記録できる。 ・ ログ送信元の IP アドレスを元にフィルタリングできる。 ・ 記録したログデータを自動的にアーカイブできる。 ・ Web コンソールが利用でき、ネットワーク経由で管理できる。
監視端末 OS	・ Windows10/Pro 相当とする。
Office ソフトウェア	・ OfficePersonal2019 相当とする。

1. 6 ネットワーク要件

統合NWのネットワーク要件を、「表1. 4 ネットワーク要件」に示す。

表1. 4 ネットワーク要件

項目	内容
IP アドレス	• IP アドレス v4 を利用する。(IPv6 は利用しない)。
プロトコル	• TCP、UDP、IP、ARP、ICMP、SNMP を利用する。
トポロジ	• WAN : 回線網を中心としたスター型トポロジで構成する。 • LAN : L3 スイッチ/ルータを頂点としたスター型トポロジで構成する。
ルーティング	• 拠点間 WAN : BGP 等を用いたダイナミックルーティングを利用する。 (拠点を AS として BGP による AS 間ルーティングを行う) • 拠点 LAN : L3 スイッチ/ルータをゲートウェイとしたスタティックルーティングを利用する。
仮想スイッチ	• L3 スイッチ/ルータを仮想化し論理的に分離するネットワークパーティション (VRF) を利用する。
仮想 LAN	• 拠点 LAN の接続を仮想化し論理的に分離する VLAN を利用する。

2. 機能要件

機能要件として、データ通信機能、VoIP 機能、運用監視機能を記載する。

2. 1 データ通信機能

データ通信機能の要件を、「表 2. 1 データ通信機能の要件」に示す。

表 2. 1 データ通信機能の要件

項目	内容
L3 中継機能	<ul style="list-style-type: none"> 各システムに拠点間ネットワーク（L3）接続を提供し拠点間での IP 通信を可能とする。 拠点毎に IP ゲートウェイ機能を提供する。 拠点間のルーティング機能を提供する。
QoS 機能	<ul style="list-style-type: none"> 各システムごとに QoS による帯域制御を提供する。 (拠点ごとに最低保証帯域を設定する)

2. 2 VoIP 機能

VoIP 機能の要件を、「表 2. 2 VoIP 機能の要件」に示す。

表 2. 2 VoIP 機能の要件

項目	内容
音声ゲートウェイ機能	<ul style="list-style-type: none"> アナログ電話網と IP 電話網の中継を行う。 呼制御装置と連動して通話相手の電話番号から通話対象の音声ゲートウェイへの発信処理を行う。 通話相手の音声ゲートウェイからの着信処理を行う。
呼制御機能	<ul style="list-style-type: none"> アナログ電話網の電話番号と IP 電話網の音声ゲートウェイ IP アドレスの紐付け管理を行う。 音声ゲートウェイと連動して通話状態の管理を行う。

2.3 運用監視機能

運用監視機能の要件を、「表 2.3 運用監視機能の要件」に示す。

表 2.3 運用監視機能の要件

項目	内容
NW 監視機能	<ul style="list-style-type: none">・対象ノードの疎通、死活監視を行う。・不正接続検出等の監視を行う。
性能管理機能	<ul style="list-style-type: none">・ネットワークトラヒック等の測定を行う。・ネットワークトラヒック等の分析を行う。
ログ管理機能	<ul style="list-style-type: none">・サーバや NW 機器からのログ収集を行う。・収集したログ情報の管理を行う。
遠隔操作機能	<ul style="list-style-type: none">・サーバや NW 機器の遠隔操作を行う。

3. 非機能要件

非機能要件として、可用性、性能・拡張性、運用・保守性、移行性、セキュリティを記載する。

3.1 可用性

可用性の要件を、「表3.1 可用性の要件」に示す。

表3.1 可用性の要件

項目	内容
サービスレベル	拠点パターン毎にサービスレベルを設定する。 ・センタ拠点 : 高 (サーバ: 有) ・タイプA拠点: 高 (窓口端末: 有 内線電話: 利用 利用者: 多) ・タイプB拠点: 中 (窓口端末: 有 内線電話: 利用 利用者: 少) ・タイプC拠点: 低 (窓口端末: 無 内線電話: 一部 利用者: 少) ・タイプD拠点: - (窓口端末: 無 内線電話: 無 利用者: 少)
許容ダウンタイム	拠点パターン毎に許容ダウンタイム (最短) を設定する ・センタ拠点 : WAN (数十秒) LAN (数秒) ・タイプA拠点: WAN (数十秒) LAN (数秒) ・タイプB拠点: WAN (数十秒) LAN (数秒) ・タイプC拠点: WAN (数時間) LAN (数時間) ・タイプD拠点: WAN (翌開庁日) LAN (翌開庁日) ※休日開庁拠点は翌平日開庁日
冗長構成	拠点パターン毎に冗長構成 (フェールオーバー時間) を設定する ・センタ拠点 : WAN (二重化: 数十秒) LAN (二重化: 数秒) ・タイプA拠点: WAN (二重化: 数十秒) LAN (二重化: 数秒) ・タイプB拠点: WAN (二重化: 数十秒) LAN (不要) ・タイプC拠点: WAN (不要) LAN (不要) ・タイプD拠点: WAN (不要) LAN (不要)

3. 2 性能・拡張性

性能・拡張性の要件を、「表 3. 2 性能・拡張性の要件」に示す。

表 3. 2 性能・拡張性の要件

項目	内容
トラフィック性能	<ul style="list-style-type: none"> ・WAN 回線の通信帯域の範囲で各システム毎の通信帯域を設定し、WAN 機器の QoS 等により優先制御と帯域制限を行うことで、各システム毎のトラフィック性能を確保する。 ・LAN 配線の通信帯域の範囲で最大トラフィック性能を確保する。ただし、システム毎の優先制御や帯域制限は行わない。
仮想システム数 (VRF 数)	<p>データ通信機器 (WAN) で想定する仮想システム数 (VRF) を設定する。</p> <ul style="list-style-type: none"> ・センタ拠点 : 20 以上 ・タイプ A 拠点 : 20 以上 ・タイプ B 拠点 : 10 以上 ・タイプ C 拠点 : 5 以上 ・タイプ D 拠点 : 不要
仮想 LAN 数 (VLAN 数)	<p>データ通信機器 (LAN) で想定する仮想 LAN 数 (VLAN) を設定する。</p> <ul style="list-style-type: none"> ・センタ拠点 : 40 以上 ・タイプ A 拠点 : 40 以上 ・タイプ B 拠点 : 20 以上 ・タイプ C 拠点 : 10 以上 ・タイプ D 拠点 : 不要

3. 3 運用・保守性

運用・保守性の要件を、「表 3. 3 運用・保守性の要件」に示す。

表 3. 3 運用・保守性の要件

項目	内容
稼働統計情報	・ NW 機器の機能ステータスや通信カウンタ等の稼働統計情報を取得できる。
設定回復方法	・ NW 機器の設定情報をコンフィグファイルとして装置外に取得できる。 ・ 取得したコンフィグファイルを利用して設定情報の回復ができる。 ・ コンフィグファイルはテキスト形式ファイルとして閲覧・編集ができる。
CLI 操作	・ NW 機器に遠隔でログインし CLI 操作により管理できる。

3. 4 移行性

移行性の要件を、「表 3. 4 移行性の要件」に示す。

表 3. 4 移行性の要件

項目	内容
移行時のルーティング	・ WAN 機器を現ネットワーク（統合NW、基幹系 NW、庁内 LAN）と接続し、相互にルーティング情報を交換することで通信ができる。
移行時の VLAN 間通信	・ LAN 機器を現ネットワーク（統合NW、基幹系 NW、庁内 LAN）と接続し、相互に VLAN 間通信ができる。
移行時の VoIP 通信	・ 音声ゲートウェイが現統合NWに接続し、現行の呼制御装置、音声ゲートウェイと相互に VoIP 通信できる。 ・ 音声ゲートウェイを PBX に接続し、内線電話の通信ができる。

3.5 セキュリティ

セキュリティの要件を、「表3.5 セキュリティの要件」に示す。

表3.5 セキュリティの要件

項目	内容
ネットワーク	<ul style="list-style-type: none">・統合NWは閉域ネットワークであり、直接的に外部ネットワークとの接続は行わない。（インターネット、LGWAN との接続は庁内 LAN 側で管理し、専用のセキュリティ機器を介して接続される）
機器管理	<ul style="list-style-type: none">・NW 機器の管理に利用するユーザ ID、パスワードを機器の稼働中に変更することができる。・ログイン/ログアウトの履歴を内部メモリやシスログサーバに記録することができる。
脆弱性対策	<ul style="list-style-type: none">・NW 機器の OS（ファームウェア）に重大な脆弱性が発見され更新版の OS が提供された場合に、遠隔操作で OS の更新作業ができる。

4. 移行要求

移行時に求められる要求事項について具体化した内容を記載する。

- ① 新統合NWの構築終了時点で新統合NWの構成を完成する。
 - ・ 現統合NWと並行で構築する（新規 WAN 回線を併設し、現ネットワークと相互接続する）
 - ・ VoIP 機能も並行で構築する（音声ゲートウェイ間の通信テストまで）

- ② 他ネットワークとの段階的な統合を行う。
 - ・ 基幹系 NW との WAN 共同利用（現行の WAN 回線を運用しつつ移行する）
 - ・ 基幹系 NW との拠点 LAN 共同利用（庁内 LAN の VDSL を廃止する）
 - ・ 庁内 LAN の統合NW用 VPN を廃止する（統合NWでルーティングする）

- ③ 各種システムは並行稼働期間で移行を行う。
 - ・ システム毎に、現ネットワークから新ネットワークへ移行する
 - ・ SS システム、GJ システムは独立した WAN へ移行する

5. 運用保守要求

運用保守時に求められる要求事項について具体化した内容を記載する。

① 現行運用との並行運用を行う。

現統合NW運用期間： 現在～令和4年3月

新統合NW運用期間： 令和3年12月～令和9年3月

並行運用期間： 令和3年12月～令和4年3月（4ヶ月間）

② 端末の通信異常時は、基幹系や庁内LANの運用（ヘルプデスク）で一次切り分けを行い、必要に応じて統合NWの運用へエスカレーション（障害連絡）する。

③ 障害連絡を受付けてから2時間以内に障害対策に着手し、サービスレベルに応じた時間内で障害を復旧する（仮対策による復旧を含む）。

- ・サービスレベル 高 : 着手から2時間以内に復旧（受付から4時間）
- 中 : 着手から4時間以内に復旧（受付から6時間）
- 低 : 着手から6時間以内に復旧（受付から8時間）
- : 着手から翌平日開庁日までに復旧

- ・受付からの経過時間が夜間休日となる場合は協議のうえで対策時間を決定する。

④ 新統合NWの運用拠点は情報システムセンターとする。

現統合NW運用拠点： 本庁舎（運用監視機器を設置、予備機を保管）

新統合NW運用拠点： 情報システムセンター（運用監視機器を設置、予備機を保管）

⑤ 運用拠点不在時の異常を遠隔監視にて通報する。

運用監視機器で検出した異常を監視センタに通報し、電話やメールによる障害連絡を行う。

⑥ ハードウェア保守の条件は、機器パターン毎に設定する。

オンサイト保守： シャーシ型 NW 機器、呼制御装置、サーバ機器

予備機交換： ボックス型 NW 機器、その他の機器（交換後に先出し SEND バック保守）

以上

図 1. 1 ネットワーク概要構成図 (WAN)

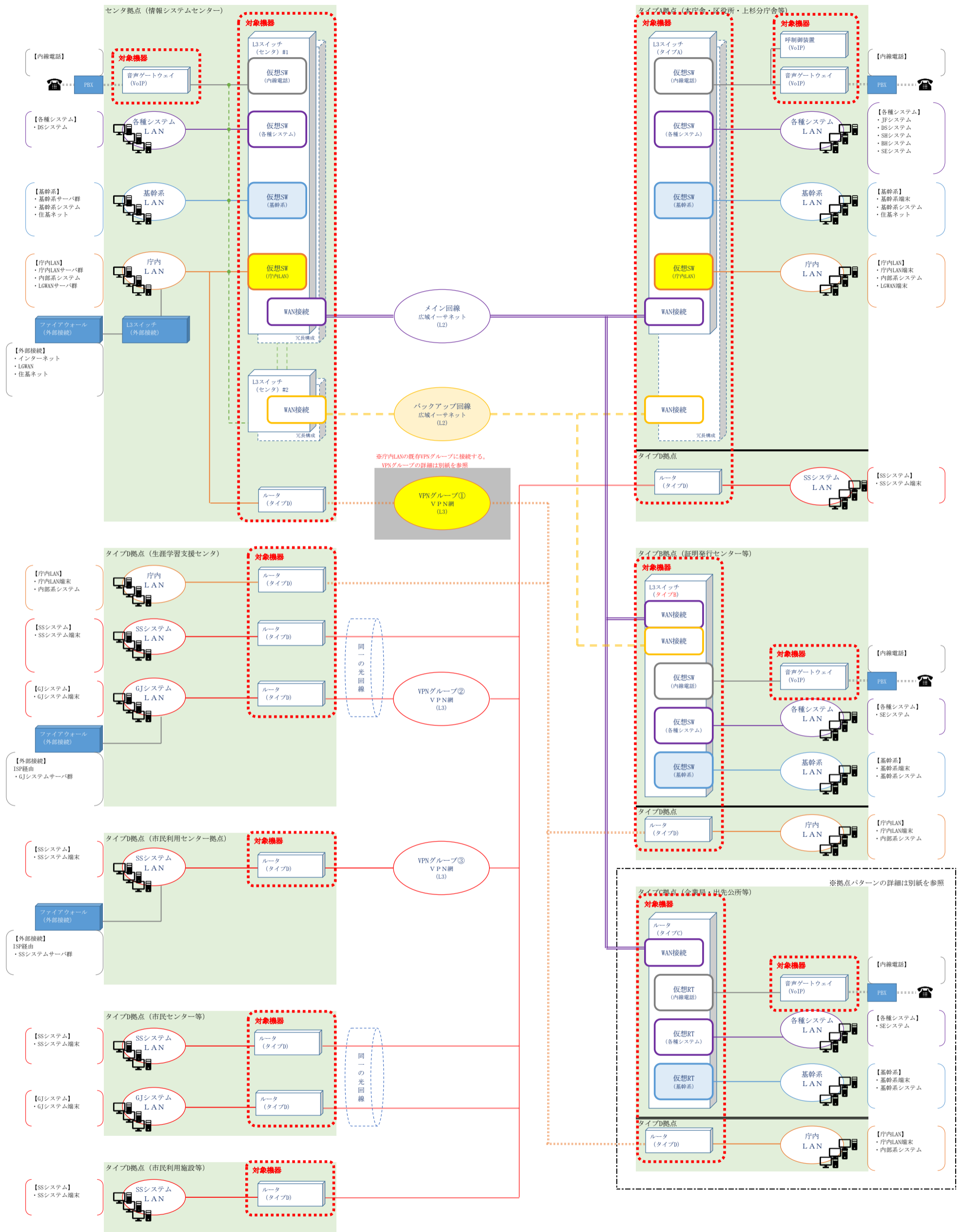


図1.1 ネットワーク概要構成図(タイプC拠点詳細)

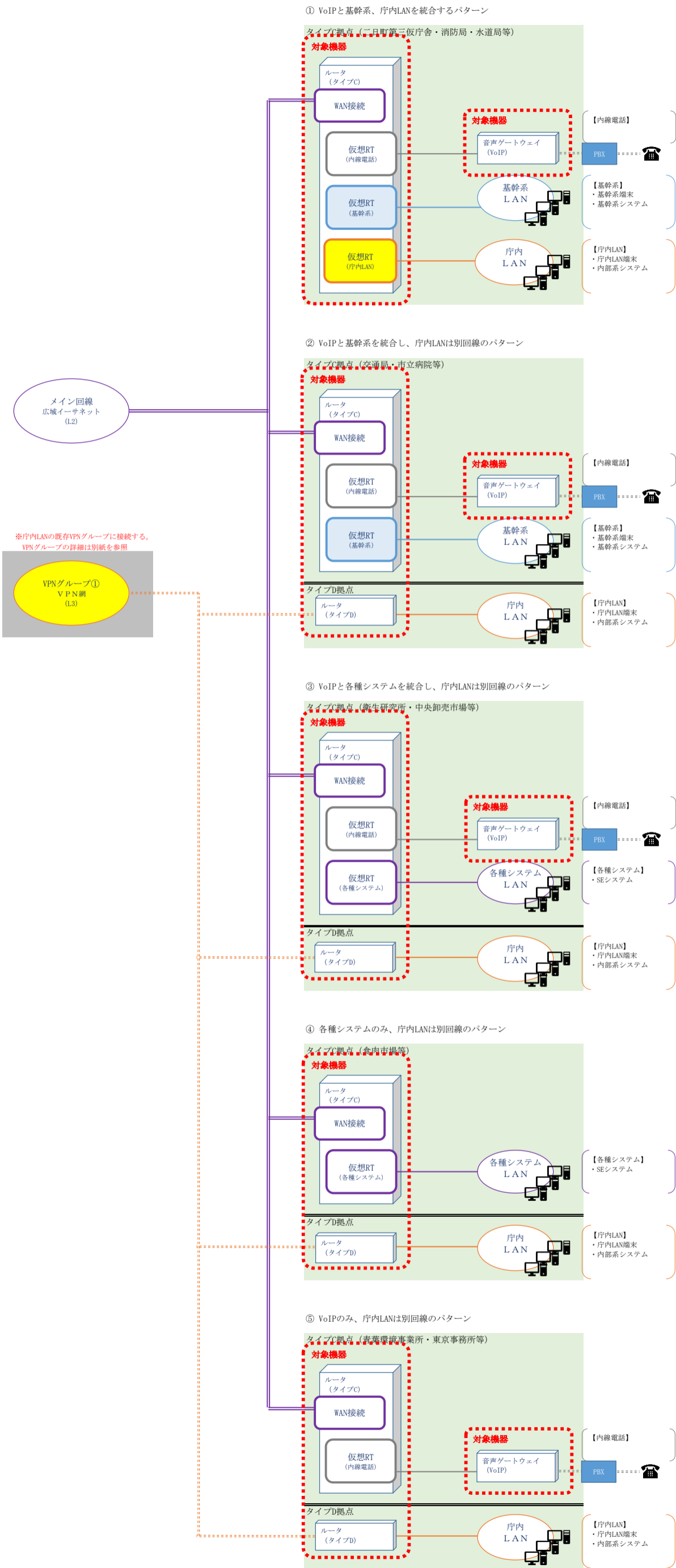
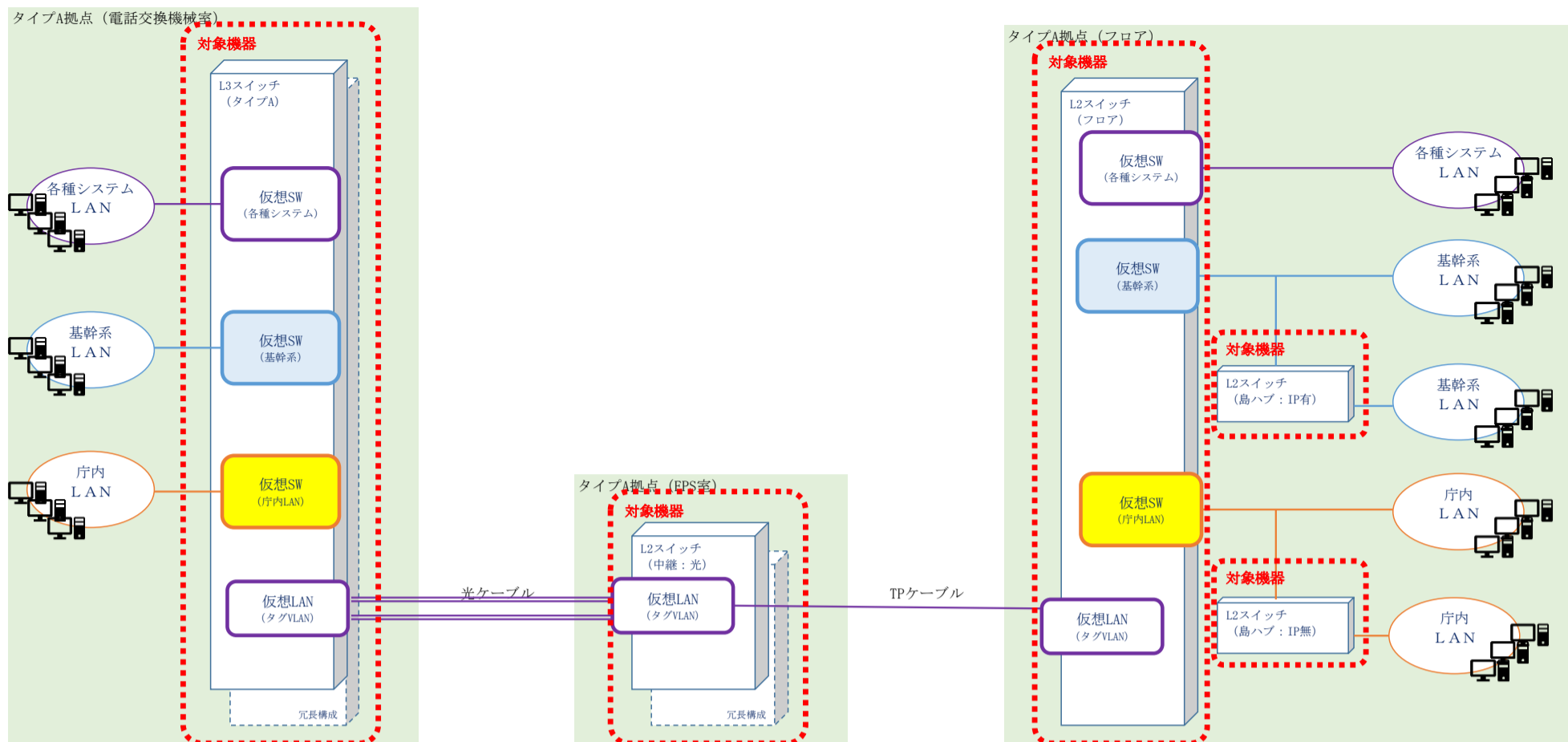


図 1. 1 ネットワーク概要構成図 (LAN)

① 幹線を光ケーブルで接続するパターン



② 幹線をTPケーブルで接続するパターン

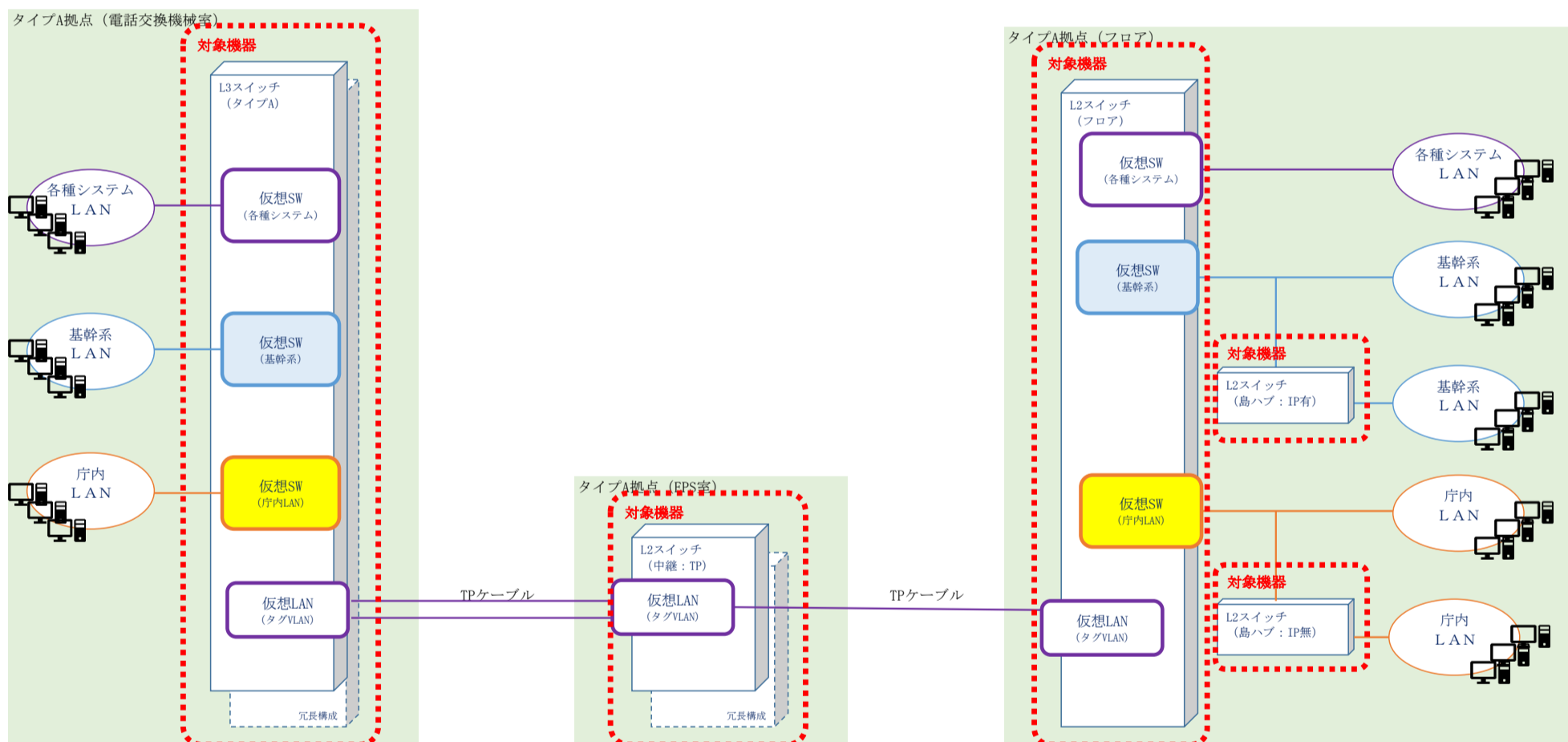


表1. 1 統合対象通信回線（ギャランティ型WAN回線）

拠点 No.	拠点名（統合NW）	拠点 パターン	WAN回線冗長化 の有無	VoIP	各種 システム	基幹系	庁内LAN
1	本庁舎	タイプA	○	○	○	○	○
2	北庁舎	タイプA	○	—	—	○	○
3	二日町分庁舎	タイプC	—	○	—	○	—
4	錦町庁舎	タイプC	—	○	—	—	—
5	表小路仮庁舎	タイプC	—	○	—	—	○
6	二日町第二仮庁舎	タイプC	—	○	—	○	○
7	二日町第三仮庁舎	タイプB	—	○	—	○	○
8	二日町第四仮庁舎	タイプC	—	○	—	○	○
9	上杉仮庁舎	タイプC	—	○	—	○	○
10	上杉分庁舎	タイプA	○	○	○	○	○
11	情報システムセンター	センタ	○	○	○	○	○
12	青葉区役所	タイプA	○	○	○	○	○
13	宮城野区役所	タイプA	○	○	○	○	○
14	若林区役所	タイプA	○	○	○	○	○
15	太白区役所	タイプA	○	○	○	○	○
16	泉区役所	タイプA	○	○	○	○	○
17	宮城総合支所	タイプA	○	○	○	○	○
18	秋保総合支所	タイプA	○	○	○	○	○
19	消防局	タイプB	—	○	—	○	○
20	水道局	タイプC	—	○	—	○	○
21	ガス局	タイプC	—	○	—	—	—
22	交通局	タイプC	—	○	—	○	—
23	仙台市立病院	タイプC	—	○	—	○	—
24	精神保健福祉総合センター	タイプC	—	○	—	○	—
25	健康増進センター	タイプC	—	○	—	○	—
26	南部発達相談支援センター	タイプC	—	○	—	○	—
27	消費生活センター	タイプC	—	○	—	—	—
28	衛生研究所	タイプC	—	○	○	—	—
29	青葉環境事業所	タイプC	—	○	—	—	—
30	宮城野環境事業所	タイプC	—	○	—	—	—
31	若林環境事業所	タイプC	—	○	—	—	—
32	下水道南管理センター	タイプC	—	○	—	—	—
33	泉環境事業所	タイプC	—	○	—	—	—
34	今泉工場	タイプC	—	○	—	—	—
35	葛岡工場	タイプC	—	○	—	—	—
36	松森工場	タイプC	—	○	—	—	—
37	中央卸売市場	タイプC	—	○	○	—	—
38	八木山動物園	タイプC	—	○	—	—	—
39	下水道北管理センター	タイプC	—	○	—	—	—
40	水質管理センター	タイプC	—	○	—	—	—
41	南蒲生浄化センター	タイプC	—	○	—	—	—
42	設備管理センター	タイプC	—	○	—	—	—
43	仙台市コールセンター	タイプC	—	○	—	—	—
44	情報・産業プラザ（AER）	タイプB	○	—	—	○	—
45	児童相談所	タイプC	—	—	—	○	—
46	吉成証明発行センター	タイプB	○	—	—	○	—
47	高砂証明発行センター	タイプB	○	—	—	○	—
48	岩切証明発行センター	タイプB	○	—	—	○	—
49	六郷証明発行センター	タイプB	○	—	—	○	—
50	七郷証明発行センター	タイプB	○	—	—	○	—
51	生出証明発行センター	タイプB	○	—	—	○	—
52	中田証明発行センター	タイプB	○	—	—	○	—
53	根白石証明発行センター	タイプB	○	—	—	○	—
54	南光台証明発行センター	タイプB	○	—	—	○	—
55	食肉市場（食肉検査場）	タイプC	—	—	○	—	—
56	東京事務所	タイプC	—	○	—	—	—

表 1. 1 統合対象通信回線（ベストエフォート型WAN回線）

拠点 No.	拠点名（統合NW）	統合する VPNグループ （庁内LAN）	統合する VPNグループ （GJシステム）	統合する VPNグループ （SSシステム）	庁内LAN	GJ システム	SS システム
57	錦町庁舎	グループ①	—	グループ③	○	—	○
58	健康増進センター	グループ①	—	グループ③	○	—	○
59	南部発達相談支援センター	グループ①	—	—	○	—	—
60	消費生活センター（エルパーク仙台）	グループ①	—	グループ③	○	—	○
61	衛生研究所	グループ①	—	—	○	—	—
62	葛岡工場（葛岡温水プール）	—	—	グループ③	—	—	○
63	中央卸売市場（食品監視センター）	グループ①	—	—	○	—	—
64	情報・産業プラザ（エル・ソーラ仙台）	グループ①	—	グループ③	○	—	○
65	市民会館	—	—	グループ③	—	—	○
66	戦災復興記念館	—	グループ②	グループ③	—	○	○
67	仙台市体育館	—	—	グループ③	—	—	○
68	青葉区中央市民センター	—	グループ②	グループ③	—	○	○
69	柏木市民センター	—	グループ②	グループ③	—	○	○
70	北山市民センター	—	グループ②	グループ③	—	○	○
71	福沢市民センター	—	グループ②	グループ③	—	○	○
72	旭ヶ丘市民センター	—	グループ②	グループ③	—	○	○
73	三本松市民センター	—	グループ②	グループ③	—	○	○
74	片平市民センター	—	グループ②	グループ③	—	○	○
75	水の森市民センター	—	グループ②	グループ③	—	○	○
76	貝ヶ森市民センター	—	グループ②	グループ③	—	○	○
77	中山市民センター	—	グループ②	グループ③	—	○	○
78	折立市民センター	—	グループ②	グループ③	—	○	○
79	宮城西市民センター	—	グループ②	グループ③	—	○	○
80	大沢市民センター	—	グループ②	グループ③	—	○	○
81	落合市民センター	—	グループ②	グループ③	—	○	○
82	吉成市民センター	—	グループ②	グループ③	—	○	○
83	木町通市民センター	—	グループ②	グループ③	—	○	○
84	生涯学習支援センター	—	グループ②	グループ③	—	○	○
85	高砂市民センター	—	グループ②	グループ③	—	○	○
86	岩切市民センター	グループ①	グループ②	グループ③	○	○	○
87	鶴ヶ谷市民センター	—	グループ②	グループ③	—	○	○
88	榴ヶ岡市民センター	—	グループ②	グループ③	—	○	○
89	東部市民センター	—	グループ②	グループ③	—	○	○
90	幸町市民センター	—	グループ②	グループ③	—	○	○
91	田子市民センター	—	グループ②	グループ③	—	○	○
92	福室市民センター	—	グループ②	グループ③	—	○	○
93	七郷市民センター	グループ①	グループ②	グループ③	○	○	○
94	荒町市民センター	—	グループ②	グループ③	—	○	○
95	六郷市民センター	グループ①	グループ②	グループ③	○	○	○
96	沖野市民センター	—	グループ②	グループ③	—	○	○
97	若林市民センター	—	グループ②	グループ③	—	○	○
98	生出市民センター	グループ①	グループ②	グループ③	○	○	○
99	中田市民センター	グループ①	グループ②	グループ③	○	○	○
100	西多賀市民センター	—	グループ②	グループ③	—	○	○
101	八本松市民センター	—	グループ②	グループ③	—	○	○
102	八木山市民センター	—	グループ②	グループ③	—	○	○
103	山田市民センター	—	グループ②	グループ③	—	○	○
104	茂庭台市民センター	—	グループ②	グループ③	—	○	○
105	東中田市民センター	—	グループ②	グループ③	—	○	○
106	柳生市民センター	—	グループ②	グループ③	—	○	○
107	富沢市民センター	—	グループ②	グループ③	—	○	○
108	湯元市民センター	—	—	グループ③	—	—	○
109	秋保市民センター	—	グループ②	グループ③	—	○	○
110	泉区中央市民センター	—	グループ②	グループ③	—	○	○
111	根白石市民センター	グループ①	グループ②	グループ③	○	○	○
112	南光台市民センター	グループ①	グループ②	グループ③	○	○	○
113	黒松市民センター	—	グループ②	グループ③	—	○	○
114	将監市民センター	—	グループ②	グループ③	—	○	○
115	加茂市民センター	—	グループ②	グループ③	—	○	○
116	高森市民センター	—	グループ②	グループ③	—	○	○
117	松陵市民センター	—	グループ②	グループ③	—	○	○
118	寺岡市民センター	—	グループ②	グループ③	—	○	○
119	長命ヶ丘市民センター	—	グループ②	グループ③	—	○	○
120	松森市民センター	—	グループ②	グループ③	—	○	○
121	桂市民センター	—	グループ②	グループ③	—	○	○
122	南中山市民センター	—	グループ②	グループ③	—	○	○
123	広瀬文化センター（広瀬市民センター）	—	グループ②	グループ③	—	○	○
124	宮城広瀬総合運動場（宮城広瀬体育館）	—	—	グループ③	—	—	○
125	宮城野区文化センター（宮城野区中央市民センター）	—	グループ②	グループ③	—	○	○
126	若林区文化センター（若林区中央市民センター）	—	グループ②	グループ③	—	○	○
127	太白区文化センター（太白区中央市民センター）	—	グループ②	グループ③	—	○	○
128	泉文化創造センター（イゾミティ21）	—	—	グループ③	—	—	○
129	仙台国際センター	—	—	グループ③	—	—	○
130	青年文化センター	—	—	グループ③	—	—	○

拠点 No.	拠点名 (統合NW)	統合する VPNグループ (庁内LAN)	統合する VPNグループ (GJシステム)	統合する VPNグループ (SSシステム)	庁内LAN	GJ システム	SS システム
131	仙台文学館	-	-	グループ③	-	-	○
132	福祉プラザ	-	-	グループ③	-	-	○
133	シルバーセンター	-	-	グループ③	-	-	○
134	秋保・里センター	-	-	グループ③	-	-	○
135	せんだいメディアテーク	-	-	グループ③	-	-	○
136	大倉ふるさとセンター	-	-	グループ③	-	-	○
137	青葉体育館	-	-	グループ③	-	-	○
138	川内庭球場	-	-	グループ③	-	-	○
139	陸上競技場	-	-	グループ③	-	-	○
140	新田総合運動場 (宮城野体育館)	-	-	グループ③	-	-	○
141	新田総合運動場 (市民球場)	-	-	グループ③	-	-	○
142	出花体育館	-	-	グループ③	-	-	○
143	若林体育館	-	-	グループ③	-	-	○
144	今泉運動場	-	-	グループ③	-	-	○
145	中田温水プール	-	-	グループ③	-	-	○
146	茂庭荘 (茂庭庭球場)	-	-	グループ③	-	-	○
147	秋保体育館	-	-	グループ③	-	-	○
148	泉総合運動場 (体育館)	-	-	グループ③	-	-	○
149	泉サッカー場	-	-	グループ③	-	-	○
150	屋内グラウンド(シェルコム仙台)	-	-	グループ③	-	-	○
151	泉海洋センター	-	-	グループ③	-	-	○
152	北中山コミュニティグラウンド	-	-	グループ③	-	-	○
153	根白石温水プール	-	-	グループ③	-	-	○
154	公園緑地協会	-	-	グループ③	-	-	○
155	青葉山公園庭球場	-	-	グループ③	-	-	○
156	卸町東二丁目公園庭球場	-	-	グループ③	-	-	○
157	湯元公園野球場	-	-	グループ③	-	-	○
158	七北田公園(体育館)	-	-	グループ③	-	-	○
159	七北田公園(庭球場)	-	-	グループ③	-	-	○
160	泉総合運動場(泉庭球場)	-	-	グループ③	-	-	○
161	海岸公園	-	-	グループ③	-	-	○
162	市民利用センター拠点 (ISP)	-	-	グループ③	-	-	○

図1.2 ネットワーク機器設置環境

1. フルラック (センタ拠点)



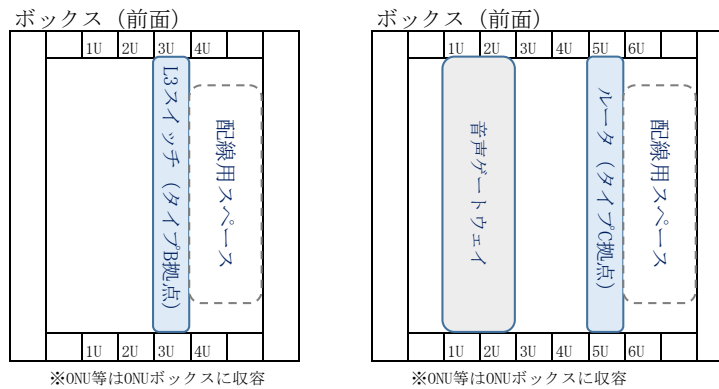
2. フルラック (タイプA拠点: 本庁舎)



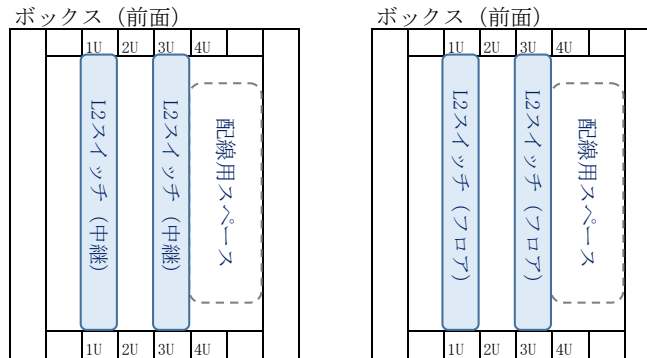
3. フルラック (タイプA拠点：区役所等)



4. ハブボックス (タイプB拠点/タイプC拠点)



5. ハブボックス (拠点LAN中継/フロア)



6. 机上設置 (タイプD拠点/島ハブ)



表 1. 2 ハードウェア要件 データ通信機器 (WAN)

1. L3スイッチ (センタ)

モデル	<ul style="list-style-type: none"> ・L3スイッチ、シャーシ型
冗長構成	<ul style="list-style-type: none"> ・単体冗長構成 (FT) 制御部 (ホットスワップ)、電源部 (ホットスワップ) インターフェース部 (複数モジュール)
インターフェース	<ul style="list-style-type: none"> ・10/100/1000BASE-T最大96ポート以上 ・SFP/SFP+ 8ポート以上
仮想化	<ul style="list-style-type: none"> ・ネットワークパーティション (VRF) ・仮想LAN (VLAN)
スイッチング機能	<ul style="list-style-type: none"> ・タグVLAN ・VXLAN または QinQ ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	<ul style="list-style-type: none"> ・OSPF ・BGP4
ネットワーク機能	<ul style="list-style-type: none"> ・QoS ・VRRP
性能	<ul style="list-style-type: none"> ・最大スイッチング容量 (800Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (96K)
外形	<ul style="list-style-type: none"> ・ラックマウント (8U以内、奥行700mm以内)
備考	

または、以下の仕様とする。

モデル	<ul style="list-style-type: none"> ・L3スイッチ、ボックス型
冗長構成	<ul style="list-style-type: none"> ・スタック冗長構成 スタックメンバ (ホットスワップ)
インターフェース	
仮想化	
スイッチング機能	
ルーティング機能	
ネットワーク機能	
性能	
外形	<ul style="list-style-type: none"> ・ラックマウント (2台以上で8U以内、奥行700mm以内)
備考	

2. L3スイッチ (タイプA拠点)

モデル	・L3スイッチ、シャーシ型
冗長構成	・単体冗長構成 (FT) 制御部 (ホットスワップ)、電源部 (ホットスワップ) インターフェース部 (複数モジュール)
インターフェース	・10/100/1000BASE-T最大48ポート以上 ・SFP/SFP+ 8ポート以上
仮想化	・ネットワークパーティション (VRF) ・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・VXLAN または QinQ ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	・OSPF ・BGP4
ネットワーク機能	・QoS ・VRRP
性能	・最大スイッチング容量 (800Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (96K)
外形	・ラックマウント (5U以内、奥行700mm以内)
備考	

または、以下の仕様とする。

モデル	・L3スイッチ、ボックス型
冗長構成	・スタック冗長構成 スタックメンバ (ホットスワップ)
インターフェース	
仮想化	
スイッチング機能	
ルーティング機能	
ネットワーク機能	
性能	
外形	・ラックマウント (2台以上で8U以内、奥行700mm以内)
備考	

3. L3スイッチ (タイプB拠点)

モデル	・L3スイッチ、ボックス型
冗長構成	・電源部 (ホットスワップ)
インターフェース	・10/100/1000BASE-T最大24ポート以上
仮想化	・ネットワークパーティション (VRF) ・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・VXLAN または QinQ ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	・OSPF ・BGP4
ネットワーク機能	・QoS ・VRRP
性能	・最大スイッチング容量 (288Gbps) ・最大パケット処理性能 (214Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (96K)
外形	・ラックマウント (1U以内、奥行400mm以内)
備考	

4. ルータ (タイプC拠点)

モデル	・ルータ
冗長構成	—
インターフェース	・10/100/1000BASE-T最大10ポート以上
仮想化	・ネットワークパーティション (VRF) ・仮想LAN (VLAN)
スイッチング機能	・タグVLAN
ルーティング機能	・OSPF ・BGP4
ネットワーク機能	・QoS ・VRRP
性能	・最大スイッチング容量 (2Gbps) ・最大パケット処理性能 (384Kpps) ・最大ルーティング経路 (4K)
外形	・ラックマウント (1U以内、奥行300mm以内)
備考	・ファンレス、電源内蔵

5. ルータ (タイプD拠点)

モデル	・ルータ
冗長構成	—
インターフェース	・10/100/1000BASE-T最大5ポート以上
仮想化	—
スイッチング機能	—
ルーティング機能	・スタティック
ネットワーク機能	<ul style="list-style-type: none"> ・QoS ・IPsec ・L2TP ・PPPoEマルチセッション
性能	<ul style="list-style-type: none"> ・最大スイッチング容量 (2Gbps) ・最大パケット処理性能 (384Kpps) ・最大ルーティング経路 (4K)
外形	—
備考	・ファンレス、電源内蔵

表 1. 2 ハードウェア要件 データ通信機器 (LAN)

1. L2スイッチ (中継)

モデル	・L2スイッチ、ボックス型
冗長構成	・スタック構成
インターフェース	・10/100/1000BASE-T最大24ポート以上 ・SFP 4ポート以上
仮想化	・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	ー
ネットワーク機能	ー
性能	・最大スイッチング容量 (56Gbps) ・最大パケット処理性能 (41Mpps) ・最大MACアドレス数 (32K)
外形	・ラックマウント (1U以内、奥行300mm以内)
備考	・ファンレス

2. L2スイッチ (フロア)

モデル	・L2スイッチ、ボックス型
冗長構成	・スタック構成
インターフェース	・10/100/1000BASE-T最大24ポート以上 ・SFP 4ポート以上
仮想化	・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	ー
ネットワーク機能	ー
性能	・最大スイッチング容量 (56Gbps) ・最大パケット処理性能 (41Mpps) ・最大MACアドレス数 (16K)
外形	・ラックマウント (1U以内、奥行200mm以内)
備考	・ファンレス

3. L2スイッチ（島ハブ：IP有）

モデル	・L2スイッチ
冗長構成	－
インターフェース	・10/100/1000BASE-T最大8ポート以上
仮想化	・仮想LAN（VLAN）
スイッチング機能	・タグVLAN ・L2ループ検知
ルーティング機能	－
ネットワーク機能	－
性能	・最大スイッチング容量（20Gbps） ・最大パケット処理性能（14Mpps） ・最大MACアドレス数（8K）
外形	－
備考	・ファンレス、電源内蔵

4. L2スイッチ（島ハブ：IP無し）

モデル	・L2スイッチ
冗長構成	－
インターフェース	・10/100/1000BASE-T最大8ポート以上
仮想化	－
スイッチング機能	・EAP透過
ルーティング機能	－
ネットワーク機能	－
性能	・最大スイッチング容量（8Gbps） ・最大パケット処理性能（11Mpps） ・最大MACアドレス数（4K）
外形	・マグネット付
備考	・ファンレス、電源内蔵

表 1. 2 ハードウェア要件 VoIP機器

1. 呼制御装置

モデル	・呼制御装置、ラックマウント型
機能・性能	・呼制御 ・最大ユーザ数 (1000) ・最大デバイス数 (2500) ・最大共有アプリケーション数 (8)
外形	・ラックマウント (2U以内、奥行1000mm以内)
備考	・Cisco Business Edition 6000相当

2. コンソール

モデル	・ラックマウント型
機能・性能	・呼制御装置の画面表示、キーボード/マウス操作ができること
外形	・ラックマウント (2U以内、奥行1000mm以内)
備考	

3. UPS

モデル	・ラックマウント型
機能・性能	・瞬停時に呼制御装置に電源供給できること
外形	・ラックマウント (2U以内、奥行1000mm以内)
備考	

4. 音声ゲートウェイ (E/M)

モデル	・ルータ、ラックマウント型
機能・性能	・音声ゲートウェイ ・E/Mインターフェース数 (8以上)
外形	・ラックマウント (2U以内、奥行400mm以内)
備考	・ISR4331-V/K9相当

5. 音声ゲートウェイ (FXS)

モデル	・ルータ、ラックマウント型
機能・性能	・音声ゲートウェイ ・FXSインターフェース数 (2以上)
外形	・ラックマウント (2U以内、奥行400mm以内)
備考	・ISR4331-V/K9相当

表 1. 2 ハードウェア要件 運用監視機器

1. NW監視サーバ

モデル	・ラックマウント型
機能・性能	・WindowsServer2019の推奨動作環境を満たしていること ・NW監視ソフトウェアの推奨動作環境を満たしていること ・UPSと連動し安全にシャットダウンできること
外形	・ラックマウント（2U以内、奥行1000mm以内）
備考	

2. シスログサーバ

モデル	・ラックマウント型
機能・性能	・WindowsServer2019の推奨動作環境を満たしていること ・SYSLOGソフトウェアの推奨動作環境を満たしていること ・UPSと連動し安全にシャットダウンできること
外形	・ラックマウント（2U以内、奥行1000mm以内）
備考	

3. コンソール

モデル	・ラックマウント型
機能・性能	・NW監視サーバ、シスログサーバの画面表示、キーボード/マウス操作ができること
外形	・ラックマウント（2U以内、奥行1000mm以内）
備考	

4. UPS

モデル	・ラックマウント型
機能・性能	・NW監視サーバ、シスログサーバと連動しシャットダウン制御できること
外形	・ラックマウント（2U以内、奥行1000mm以内）
備考	

5. 外付けHDD

モデル	・USB-HDD
機能・性能	<ul style="list-style-type: none"> ・NW監視サーバ、シスログサーバと接続しデータ保存ができること ・USB3.0対応 ・最大容量(2TB以上)
外形	—
備考	

6. NTPサーバ

モデル	・ボックス型
機能・性能	<ul style="list-style-type: none"> ・時刻情報を受信し、ネットワーク経由で時刻同期ができること ・FM方式に対応していること
外形	—
備考	

7. 監視端末

モデル	・デスクトップ型
機能・性能	<ul style="list-style-type: none"> ・Windows10/Proの推奨動作環境を満たしていること ・Officeソフトウェアの推奨動作環境を満たしていること ・ディスプレイと一体型であること
外形	—
備考	

必要経費積算表

1. 現行費用 (概算)

※ 12ヶ月運用する年度を基準年度とする。

(単位:千円)

	設計・構築期間		運用期間 (機器更新後)					機器更新全費用	備考
	n-2年度	n-1年度	n年度	n+1年度	n+2年度	n+3年度	n+4年度		
運用月数	0	3	12	12	12	12	9		
庁内LAN	設計・構築	10,500	10,500					21,000	
	通信回線		4,500	18,000	18,000	18,000	13,500	90,000	1,500/月 (フレック回線、ハイパーウェブ含まず)
	機器費用		2,880	11,520	11,520	11,520	8,640	57,600	960/月
	運用保守		120	480	480	480	360	2,400	40/月
庁内LAN合計	10,500	18,000	30,000	30,000	30,000	22,500	171,000		
統合NW	設計・構築	50,300	2,700					53,000	内線網機器更新実績
	通信回線	20,100	5,405					25,505	市民センター機器更新実績
	機器費用		9,585	38,340	38,340	38,340	28,755	191,700	3,195/月
	運用保守		6,390	25,560	25,560	25,560	19,170	127,800	2,130/月
統合NW合計	70,400	27,806	78,804	78,804	78,804	59,103	472,525	1,242/月	
基幹系NW	設計・構築	6,000	49,500					55,500	リプレース想定費用
	通信回線(N)		6,300	25,200	25,200	25,200	18,900	126,000	2,100/月
	通信回線(B)		1,158	4,632	4,632	4,632	3,474	23,160	386/月
	機器費用		13,998	55,992	55,992	55,992	41,994	279,960	4,666/月(後継機標準価格×80%)
運用保守		11,556	46,224	46,224	46,224	34,668	231,120	3,852/月(後継機保守価格×90%)	
基幹系NW合計	6,000	84,819	141,276	141,276	141,276	105,957	761,880	769/月	
全合計	設計・構築	86,900	68,105					155,005	
	通信回線		21,543	86,172	86,172	86,172	64,629	430,860	
	機器費用		34,824	139,296	139,296	139,296	104,472	696,480	
	運用保守		6,153	24,612	24,612	24,612	18,459	123,060	
全合計	86,900	130,625	250,080	250,080	250,080	187,560	1,405,405		

2. RFI回答比較 (概算)

※ 12ヶ月運用する年度を基準年度とする。

(単位:千円)

	設計・構築期間		運用期間 (機器更新後)					パターン1 全費用	備考	パターン2 差額費用	パターン1 現行費用差額
	令和2年度	令和3年度	令和4年度	令和5年度	令和6年度	令和7年度	令和8年度				
運用月数	0	3	12	12	12	12	9				
A社	設計・構築	51,000	34,280					85,280		720	-69,725
	通信回線		19,170	76,680	76,680	76,680	57,510	383,400	6,390/月(3,195/月 x2回線)	0	-47,460
	機器費用		460,640	0	0	0	0	460,640	令和3年度に一括	190,360	-235,840
	運用保守		17,666	37,272	37,272	37,272	43,246	210,000		0	86,940
合計	51,000	531,756	113,952	113,952	113,952	105,756	1,139,320		191,080	-266,085	
現行費用差額:	-35,900	401,131	-136,128	-136,128	-136,128	-136,128	-86,804		-266,085		

費用比較

設計・構築費用: 現行費用との差額-69,725千円
 機器費用: 現行費用との差額-235,840千円
 運用保守: 現行費用との差額+86,940千円
 合計: 現行費用との差額-266,085千円

	設計・構築期間		運用期間 (機器更新後)					パターン1 全費用	備考	パターン2 差額費用	パターン1 現行費用差額
	令和2年度	令和3年度	令和4年度	令和5年度	令和6年度	令和7年度	令和8年度				
運用月数	0	3	12	12	12	12	9				
B社	設計・構築	43,331	97,284					140,614		8,330	-14,391
	通信回線		19,170	76,680	76,680	76,680	57,510	383,400	6,390/月(3,195/月 x2回線)	0	-47,460
	機器費用		625,507	38,706	38,706	38,706	38,706	819,036		48,999	122,556
	運用保守		55,029	84,128	84,128	84,128	123,114	514,652	令和3年度に現行撤去有	9,440	391,592
合計	43,331	796,989	199,513	199,513	199,513	219,329	1,857,702		66,769	452,297	
現行費用差額:	-43,570	666,364	-50,567	-50,567	-50,567	-50,567	31,769		452,297		

費用比較

設計・構築費用: 現行費用との差額-14,391千円
 機器費用: 現行費用との差額+122,556千円
 運用保守: 現行費用との差額+391,592千円
 合計: 現行費用との差額+452,297千円

	設計・構築期間		運用期間 (機器更新後)					パターン1 全費用	備考	パターン2 差額費用	パターン1 現行費用差額
	令和2年度	令和3年度	令和4年度	令和5年度	令和6年度	令和7年度	令和8年度				
運用月数	0	3	12	12	12	12	9				
C社	設計・構築	38,160	48,600					86,760		2,160	-68,245
	通信回線		19,170	76,680	76,680	76,680	57,510	383,400	6,390/月(3,195/月 x2回線)	0	-47,460
	機器費用		554,411	85,130	85,130	85,130	85,130	980,061		8,588	283,581
	運用保守		7,720	23,160	23,160	23,160	23,160	133,020		200	9,960
合計	38,160	629,901	184,970	184,970	184,970	184,970	1,583,241		10,948	177,836	
現行費用差額:	-48,740	499,276	-65,110	-65,110	-65,110	-65,110	-12,260		177,836		

費用比較

設計・構築費用: 現行費用との差額-68,245千円
 機器費用: 現行費用との差額+283,581千円
 運用保守: 現行費用との差額+9,960千円
 合計: 現行費用との差額+177,836千円

	設計・構築期間		運用期間 (機器更新後)					パターン1 全費用	備考	パターン2 差額費用	パターン1 現行費用差額
	令和2年度	令和3年度	令和4年度	令和5年度	令和6年度	令和7年度	令和8年度				
運用月数	0	3	12	12	12	12	9				
D社	設計・構築	105,105	210,980					316,085		0	161,080
	通信回線		19,170	76,680	76,680	76,680	57,510	383,400	6,390/月(3,195/月 x2回線)	0	-47,460
	機器費用	414,784	65,596	601	1,413	601	601	484,197	令和2年度から費用有	0	-212,283
	運用保守		18,000	36,000	36,000	36,000	36,000	79,456		241,456	118,396
合計	519,889	313,746	113,281	114,093	113,281	113,281	137,567	1,425,138		0	19,733
現行費用差額:	432,989	183,121	-136,799	-135,987	-136,799	-136,799	-49,993		19,733		

費用比較

設計・構築費用: 現行費用との差額+161,080千円
 機器費用: 現行費用との差額-212,283千円
 運用保守: 現行費用との差額+118,396千円
 合計: 現行費用との差額+19,733千円

共通事項

- ①通信回線の費用は、現行費用の統合NW用回線の2倍(2回線分)として積算する。
- ②パターン1は拠点間通信を暗号化しない構成
- ③パターン2は拠点間通信を暗号化する構成

必要経費積算表

3. まとめ (概算)

設計・構築、通信回線、機器費用、運用保守の現行費用(1,405,405千円)とRFI回答の最小見積り額(1,139,320千円)の比較から266,085千円の削減効果がある。

【現行費用】

(単位：千円)

	設計・構築期間		運用期間 (機器更新後)					機器更新全費用
	n-2年度	n-1年度	n年度	n+1年度	n+2年度	n+3年度	n+4年度	
運用月数	0	3	12	12	12	12	9	
設計・構築	86,900	68,105						155,005
通信回線		21,543	86,172	86,172	86,172	86,172	64,629	430,860
機器費用		34,824	139,296	139,296	139,296	139,296	104,472	696,480
運用保守		6,153	24,612	24,612	24,612	24,612	18,459	123,060
合計	86,900	130,625	250,080	250,080	250,080	250,080	187,560	1,405,405

【RFI回答の最小見積り費用】

(単位：千円)

	設計・構築期間		運用期間 (機器更新後)					機器更新全費用	現行費用との差額
	令和2年度	令和3年度	令和4年度	令和5年度	令和6年度	令和7年度	令和8年度		
運用月数	0	3	12	12	12	12	9		
設計・構築	51,000	34,280						85,280	-69,725
通信回線		19,170	76,680	76,680	76,680	76,680	57,510	383,400	-47,460
機器費用		460,640	0	0	0	0	0	460,640	-235,840
運用保守		17,666	37,272	37,272	37,272	37,272	43,246	210,000	86,940
合計	51,000	531,756	113,952	113,952	113,952	113,952	100,756	1,139,320	-266,085

仙台市統合ネットワーク再構築

要件定義書

Ver1.0

令和2年 3月12日

仙台市

目次

本書の目的.....	1
1. 統合ネットワーク概要.....	2
2. 機能要件.....	7
3. 非機能要件.....	9
4. 移行要件.....	13
5. テスト要件.....	14
6. 運用保守要求.....	15

本書の目的

本書は、「仙台市新統合ネットワーク設計・構築・運用保守業務」に関する情報提供招請(RFI)の結果、基本計画を策定し、統合NW再構築に必要な要件を整理した内容を要件定義書として記載したものである。

要件定義の範囲を以下に示す。

- ① 統合ネットワーク概要
- ② 機能要件
- ③ 非機能要件
- ④ 移行要件
- ⑤ テスト要件
- ⑥ 運用保守要件

1. 統合ネットワーク概要

統合NWの概要として、全体構成、統合対象通信回線、ネットワーク機器設置環境、ハードウェア要件、ソフトウェア要件、ネットワーク要件を記載する。

1. 1 全体構成

統合NWの全体構成を、別紙「図 1. 1 ネットワーク概要構成図」に示す。
概要構成図は、以下のパターンで構成する。

- ① WAN： ネットワークの全体構成を示す。
拠点の構成により以下のパターンに分類する。
 - センタ拠点： 情報システムセンター
 - タイプ A 拠点： 本庁舎や区役所、総合支所等、統合するシステムが多い拠点
 - タイプ B 拠点： 仙台駅前サービスセンターや証明発行センター
 - タイプ C 拠点： 各仮庁舎等、窓口業務がなく回線帯域が 100Mbps の VoIP 拠点
 - タイプ D 拠点： 企業局（水道局以外）やその他拠点で、回線帯域が 10Mbps の VoIP 拠点
 - タイプ E 拠点： VoIP のみの拠点
 - タイプ F 拠点： ベストエフォート型 WAN 回線で通信回線グループ 2 の拠点
 - タイプ G 拠点： ベストエフォート型 WAN 回線で通信回線グループ 3 の拠点
- ② タイプ C～G 拠点詳細： タイプ C～G 拠点の詳細パターンを示す。
- ③ LAN： タイプ A 拠点の LAN 構成を示す。

1. 2 統合対象通信回線

統合対象とする通信回線の一覧を、別紙「表 1. 1 統合対象通信回線」に示す。
通信回線の一覧は、以下のパターンで構成する。

- ① ギャランティ型 WAN 回線
通信帯域を保証する WAN 回線を利用する。一部の拠点で WAN 回線を冗長化する。
通信回線グループ 1 に分類する。

④ ベストエフォート型 WAN 回線

通信帯域を保証しない WAN 回線を利用する。拠点間で VPN を構成する。
通信回線グループ 2 及び通信回線グループ 3 に分類する。

1. 3 ネットワーク機器設置環境

ネットワーク機器設置環境を、別紙「図 1. 2 ネットワーク機器設置環境」に示す。

ネットワーク機器の設置環境は、以下のパターンで分類する。

- ① フラック : NW 機器 (L3 スイッチ) やサーバ等を搭載する。
- ② ハーフラック : NW 機器 (L3 スイッチ) を搭載する。
- ③ キャビネット : NW 機器 (L3 スイッチや L2 スイッチ) を搭載する。
- ④ 机上設置 : ゴム足やマグネットで設置する。

1. 4 ハードウェア要件

機器パターン毎のハードウェア要件を、別紙「表 1. 2 ハードウェア要件」に示す。

ハードウェア要件は以下のパターンで構成する。

- ① ネットワーク機器 : 拠点間のデータ通信を行う。
- ② VoIP 機器 : 内線電話の VoIP 通信を行う。
※VoIP ゲートウェイはネットワーク機器に含める。
- ③ 運用監視機器 : ネットワークの運用監視を行う。
- ④ ネットワークラック : ネットワーク機器等を収容する。

1. 5 ソフトウェア要件

運用監視機器のソフトウェア要件を、「表 1. 3 ソフトウェア要件」に示す。

表 1. 3 ソフトウェア要件

項目	内容
NW 監視サーバ OS	<ul style="list-style-type: none">• NW 監視ソフトウェアの推奨動作環境を満たしている。
NW 監視ソフトウェア	<p>NW 監視ソフトウェア</p> <ul style="list-style-type: none">• NNM (NetworkNodeManager) 機能を有している。• ICMP、SNMP を用いて NW 機器を自動的に検出し、監視用マップを自動的に生成できる。• 対象ノードの生存監視を行い、異常時にはアラート通知ができる。• Web コンソールが利用でき、ネットワーク経由で管理できる。• 日本語での GUI 表示ができる。• 700 ノードの機器を管理できるライセンスを有している。
シスログサーバ OS	<ul style="list-style-type: none">• SYSLOG ソフトウェアの推奨動作環境を満たしている。
SYSLOG ソフトウェア	<p>SYSLOG ソフトウェア</p> <ul style="list-style-type: none">• 700 台以上の機器から Syslog 転送を受信し記録できる。• ログ送信元の IP アドレスを元にフィルタリングできる。• 記録したログデータを自動的にアーカイブできる。
監視端末 OS	<ul style="list-style-type: none">• Windows10/Pro 相当とする。
Office ソフトウェア	<ul style="list-style-type: none">• OfficePersonal2019 相当とする。

1. 6 ネットワーク要件

統合NWのネットワーク要件を、「表1. 4 ネットワーク要件」に示す。

表1. 4 ネットワーク要件

項目	内容
IP アドレス	• IP アドレス v4 を利用する。(IPv6 は利用しない)。
プロトコル	• TCP、UDP、IP、ARP、ICMP、SNMP を利用する。
トポロジ	• WAN : 回線網を中心としたスター型トポロジで構成する。 • LAN : L3 スイッチ/ルータを頂点としたスター型トポロジで構成する。
ルーティング	• 拠点間 WAN : BGP 等を用いたダイナミックルーティングを利用する。 (拠点を AS として BGP による AS 間ルーティングを行う) • 拠点 LAN : L3 スイッチ/ルータをゲートウェイとしたスタティックルーティングを利用する。
仮想スイッチ	• L3 スイッチ/ルータを仮想化し論理的に分離するネットワークパーティション (VRF) を利用する。
仮想 LAN	• 拠点 LAN の接続を仮想化し論理的に分離する VLAN を利用する。

2. 機能要件

機能要件として、データ通信機能、VoIP 機能、運用監視機能を記載する。

2. 1 データ通信機能

データ通信機能の要件を、「表 2. 1 データ通信機能の要件」に示す。

表 2. 1 データ通信機能の要件

項目	内容
L3 中継機能	<ul style="list-style-type: none"> 各システムに拠点間ネットワーク（L3）接続を提供し拠点間での IP 通信を可能とする。 拠点毎に IP ゲートウェイ機能を提供する。 拠点間のルーティング機能を提供する。
QoS 機能	<ul style="list-style-type: none"> 各システムごとに QoS による帯域制御を提供する。 (拠点ごとに最低保証帯域を設定する)

2. 2 VoIP 機能

VoIP 機能の要件を、「表 2. 2 VoIP 機能の要件」に示す。

表 2. 2 VoIP 機能の要件

項目	内容
音声ゲートウェイ機能	<ul style="list-style-type: none"> アナログ電話網と IP 電話網の中継を行う。 呼制御装置と連動して通話相手の電話番号から通話対象の音声ゲートウェイへの発信処理を行う。 通話相手の音声ゲートウェイからの着信処理を行う。
呼制御機能	<ul style="list-style-type: none"> アナログ電話網の電話番号と IP 電話網の音声ゲートウェイ IP アドレスの紐付け管理を行う。 音声ゲートウェイと連動して通話状態の管理を行う。

2.3 運用監視機能

運用監視機能の要件を、「表 2.3 運用監視機能の要件」に示す。

表 2.3 運用監視機能の要件

項目	内容
NW 監視機能	<ul style="list-style-type: none">・対象ノードの疎通、死活監視を行う。・不正接続検出等の監視を行う。
性能管理機能	<ul style="list-style-type: none">・ネットワークトラヒック等の測定を行う。・ネットワークトラヒック等の分析を行う。
ログ管理機能	<ul style="list-style-type: none">・サーバや NW 機器からのログ収集を行う。・収集したログ情報の管理を行う。
遠隔操作機能	<ul style="list-style-type: none">・サーバや NW 機器の遠隔操作を行う。

3. 非機能要件

非機能要件として、可用性、性能・拡張性、運用・保守性、移行性、セキュリティを記載する。

3.1 可用性

可用性の要件を、「表3.1 可用性の要件」に示す。

表3.1 可用性の要件

項目	内容
サービスレベル	<p>拠点パターン毎にサービスレベルを設定する。</p> <ul style="list-style-type: none"> ・センタ拠点 : 高 (サーバ:有) ・タイプA拠点 : 高 (窓口端末:有 内線電話:利用 利用者:多) ・タイプB拠点 : 中 (窓口端末:有 内線電話:利用 利用者:少) ・タイプC~G拠点: 低 (窓口端末:無 内線電話:一部 利用者:少)
許容ダウンタイム	<p>拠点パターン毎に許容ダウンタイム (最短) を設定する。</p> <ul style="list-style-type: none"> ・センタ拠点 : WAN (数十秒) LAN (数秒) ・タイプA拠点 : WAN (数十秒) LAN (数秒) ・タイプB拠点 : WAN (数時間) LAN (数時間) ・タイプC~G拠点 : WAN (数時間) LAN (数時間) <p>※休日開庁拠点は翌平日開庁日</p>
冗長構成	<p>拠点パターン毎に冗長構成 (フェールオーバー時間) を設定する</p> <ul style="list-style-type: none"> ・センタ拠点 : WAN (二重化:数十秒) LAN (二重化:数秒) ・タイプA拠点 : WAN (二重化:数十秒) LAN (二重化:数秒) ・タイプB拠点 : WAN (不要) LAN (不要) ・タイプC~G拠点 : WAN (不要) LAN (不要) <p>※タイプB拠点の仙台駅前SCはWANのみ二重化する。</p>

3. 2 性能・拡張性

性能・拡張性の要件を、「表 3. 2 性能・拡張性の要件」に示す。

表 3. 2 性能・拡張性の要件

項目	内容
トラフィック性能	<ul style="list-style-type: none"> • WAN 回線の通信帯域の範囲で各システム毎の通信帯域を設定し、WAN 機器の QoS 等により優先制御と帯域制限を行うことで、各システム毎のトラフィック性能を確保する。 • LAN 配線の通信帯域の範囲で最大トラフィック性能を確保する。ただし、システム毎の優先制御や帯域制限は行わない。
仮想システム数 (VRF 数)	<p>データ通信機器 (WAN) で想定する仮想システム数 (VRF) を設定する。</p> <ul style="list-style-type: none"> • センタ拠点 : 20 以上 • タイプ A 拠点 : 20 以上 • タイプ B~D 拠点 : 10 以上 • タイプ E 拠点 : 5 以上 • タイプ F~G 拠点 : 不要
仮想 LAN 数 (VLAN 数)	<p>データ通信機器 (LAN) で想定する仮想 LAN 数 (VLAN) を設定する。</p> <ul style="list-style-type: none"> • センタ拠点 : 40 以上 • タイプ A 拠点 : 40 以上 • タイプ B~D 拠点 : 20 以上 • タイプ E 拠点 : 10 以上 • タイプ F 拠点 : 2 以上 (ポート VLAN) • タイプ G 拠点 : 不要

3. 3 運用・保守性

運用・保守性の要件を、「表 3. 3 運用・保守性の要件」に示す。

表 3. 3 運用・保守性の要件

項目	内容
稼働統計情報	・ NW 機器の機能ステータスや通信カウンタ等の稼働統計情報を取得できる。
設定回復方法	・ NW 機器の設定情報をコンフィグファイルとして装置外に取得できる。 ・ 取得したコンフィグファイルを利用して設定情報の回復ができる。 ・ コンフィグファイルはテキスト形式ファイルとして閲覧・編集ができる。
CLI 操作	・ NW 機器に遠隔でログインし CLI 操作により管理できる。

3. 4 移行性

移行性の要件を、「表 3. 4 移行性の要件」に示す。

表 3. 4 移行性の要件

項目	内容
移行時のルーティング	・ WAN 機器を現ネットワーク（統合NW、基幹系NW、庁内LAN）と接続し、相互にルーティング情報を交換することで通信ができる。
移行時のVLAN間通信	・ LAN 機器を現ネットワーク（統合NW、基幹系NW、庁内LAN）と接続し、相互にVLAN間通信ができる。
移行時のVoIP通信	・ 音声ゲートウェイが現統合NWに接続し、現行の呼制御装置、音声ゲートウェイと相互にVoIP通信できる。 ・ 音声ゲートウェイをPBXに接続し、内線電話の通信ができる。

3.5 セキュリティ

セキュリティの要件を、「表3.5 セキュリティの要件」に示す。

表3.5 セキュリティの要件

項目	内容
ネットワーク	<ul style="list-style-type: none">・統合NWは閉域ネットワークであり、直接的に外部ネットワークとの接続は行わない。（インターネット、LGWANとの接続は庁内LAN側で管理し、専用のセキュリティ機器を介して接続される）
機器管理	<ul style="list-style-type: none">・NW機器の管理に利用するユーザID、パスワードを機器の稼働中に変更することができる。・ログイン/ログアウトの履歴を内部メモリやシスログサーバに記録することができる。
脆弱性対策	<ul style="list-style-type: none">・NW機器のOS（ファームウェア）に重大な脆弱性が発見され更新版のOSが提供された場合に、遠隔操作でOSの更新作業ができる。

4. 移行要件

移行時に求められる移行要件について記載する。

- ① 新統合NWの構築終了時点で新統合NWの構成を完成する。
 - ・ 現統合NWと並行で構築する（新規 WAN 回線を併設し、現ネットワークと相互接続する）
 - ・ VoIP 機能も並行で構築する（音声ゲートウェイ間の通信テストまで）

- ② 他ネットワークとの段階的な統合を行う。
 - ・ 基幹系NWとの WAN 共同利用（現行の WAN 回線を運用しつつ移行する）
 - ・ 基幹系NWとの拠点 LAN 共同利用（庁内 LAN の VDSL を廃止する）
 - ・ 庁内 LAN の統合NW用 VPN を廃止する（統合NWでルーティングする）

- ③ 各種システムは並行稼働期間で移行を行う。
 - ・ システム毎に移行計画策定の上、拠点毎に現ネットワークから新ネットワークへ移行する

5. テスト要件

統合NWの再構築にあたり必要となるテスト要件について記載する。

統合NWの再構築は、現行統合NWとの並行稼働を行い、本番稼働中のV o I Pや基幹系NW、庁内LAN、及び各種システムの移行を安全かつスムーズに行うため、事前検証や構築時、移行時のテストを確実に実行し評価する必要がある。詳細なテスト方式は設計業務にて検討し定義することとする。テスト要件の概要について「表5. 1 テスト要件」に示す。

表5. 1 テスト要件

#	カテゴリ	要件
1	事前検証	<ul style="list-style-type: none"> ・統合NWの主要な拠点（構成）を想定した検証環境を構築する。 ・設定した機器を検証環境に接続し、事前検証による動作確認を行い、機器が設計した通りに動作することを確認する。 ・問題が発生した場合には、設計へのフィードバックを行い、再度、検証を実施する。
2	動作確認	<ul style="list-style-type: none"> ・拠点へ機器を設置した際に、動作確認を行い、機器が設計した通りに動作することを確認する。 ・正常時テスト、異常時テストの両方を行う。
3	運用テスト	<ul style="list-style-type: none"> ・統合NWの本番環境への移行を行う前に、運用保守で必要となる各種手順について、運用テストによる評価を行う。 ・正常時、異常時の手順だけでなく、変更作業の手順についても評価を行う。 ・遠隔監視の接続テストや通報テストを行う。
4	連携テスト	<ul style="list-style-type: none"> ・各種システムの統合NWへの移行にあたり、連携テストによる動作確認を行い、移行した各種システムが、問題なく動作することを確認する。

6. 運用保守要件

運用保守時に求められる要件について記載する。

- ① 現行運用との並行運用を行う。

現統合NW運用期間： 現在～令和4年3月

新統合NW運用期間： 令和3年12月～令和9年3月

並行運用期間： 令和3年12月～令和4年3月（4ヶ月間）

- ② 端末の通信異常時は、基幹系や庁内LANの運用（ヘルプデスク）で一次切り分けを行い、必要に応じて統合NWの運用へエスカレーション（障害連絡）する。

- ③ 障害連絡を受付けてから2時間以内に障害対策に着手し、サービスレベルに応じた時間内で障害を復旧する（仮対策による復旧を含む）。

- ・サービスレベル 高 : 着手から2時間以内に復旧（受付から4時間）
- 中 : 着手から4時間以内に復旧（受付から6時間）
- 低 : 着手から6時間以内に復旧（受付から8時間）
- : 着手から翌平日開庁日までに復旧

- ・受付からの経過時間が夜間休日となる場合は協議のうえで対策時間を決定する。

- ④ 新統合NWの運用拠点は情報システムセンターとする。

現統合NW運用拠点： 本庁舎（運用監視機器を設置、予備機を保管）

新統合NW運用拠点： 情報システムセンター（運用監視機器を設置、予備機を保管）

- ⑤ 運用者不在時の異常に備え、常時遠隔監視を行う。

運用監視機器で検出した異常を監視センタに通報し、電話やメールによる障害連絡を行う。

⑥ ハードウェア保守の条件は、機器パターン毎に設定する。

オンサイト保守： センタ拠点及びタイプ A 拠点の NW 機器、呼制御装置及びサーバ機器

予備機交換： センタ拠点及びタイプ A 拠点以外の NW 機器、並びにその他の機器

(交換後に先出しセンドバック保守)

図1. 1 ネットワーク概要構成図 (WAN)

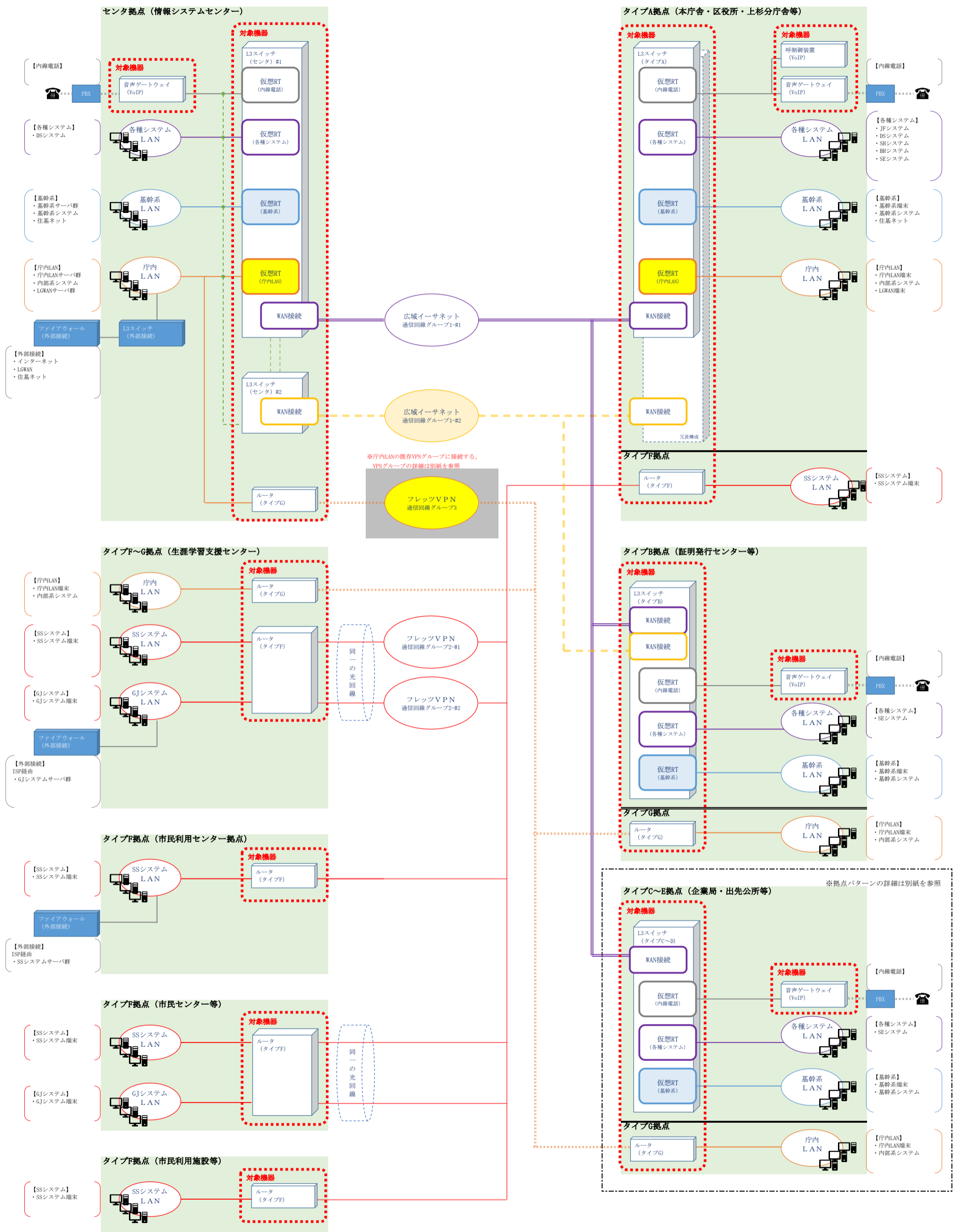


図 1. 1 ネットワーク概要構成図 (タイプC~E拠点詳細)

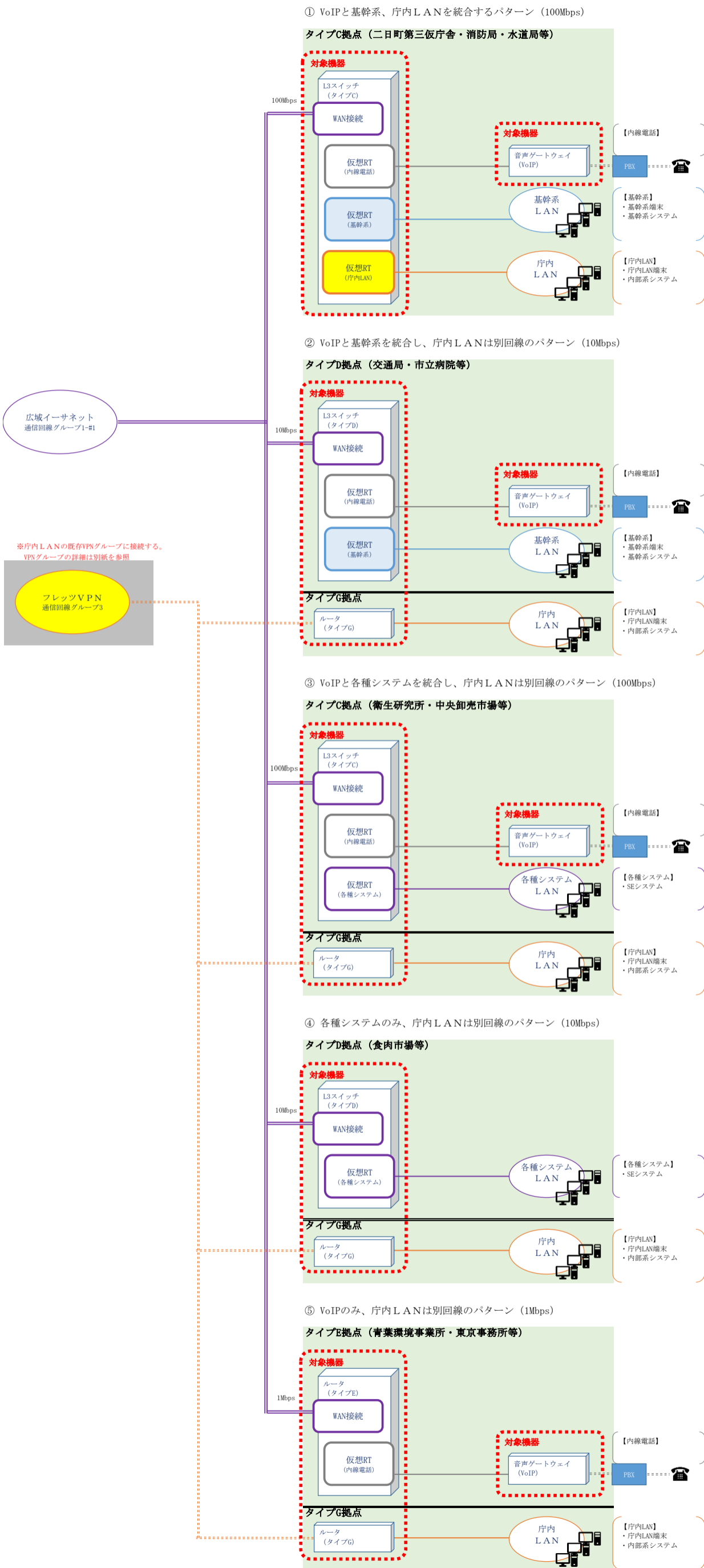
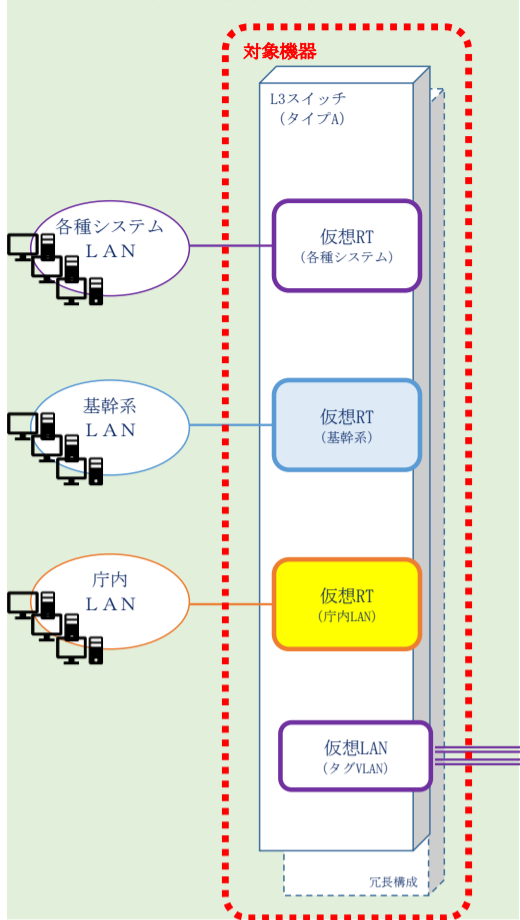


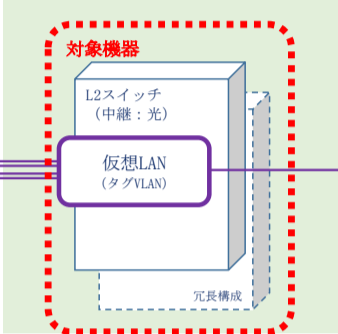
図1.1 ネットワーク概要構成図 (LAN)

① 幹線を光ケーブルで接続するパターン

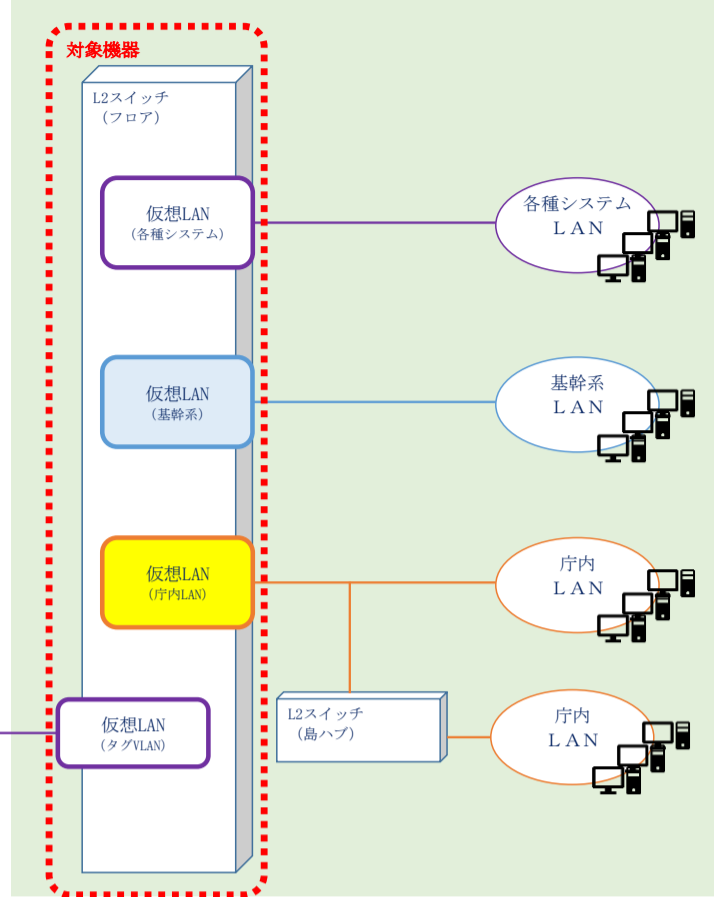
タイプA拠点 (電話交換機械室)



タイプA拠点 (EPS室)



タイプA拠点 (フロア)

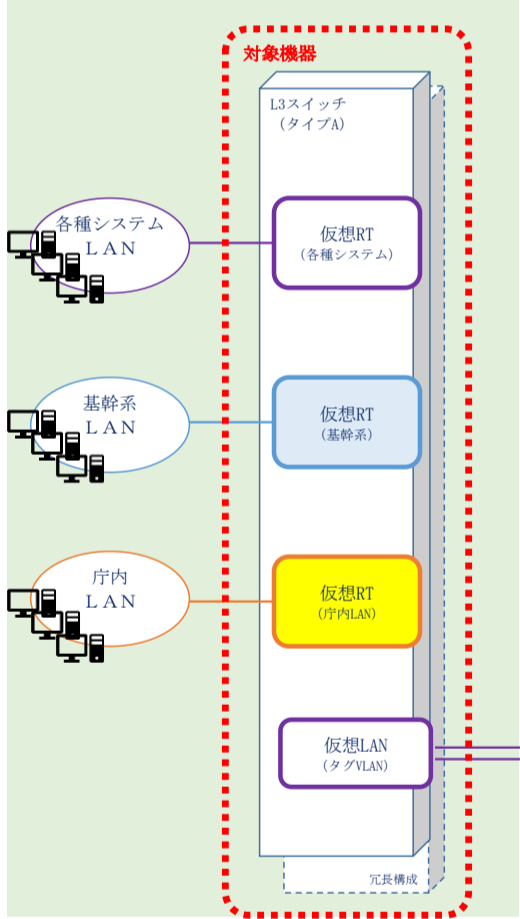


光ケーブル

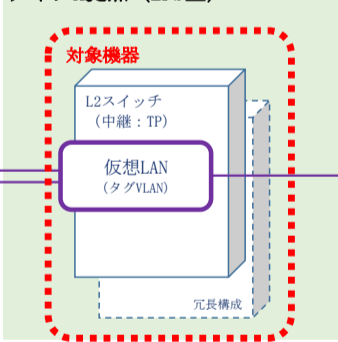
TPケーブル

② 幹線をTPケーブルで接続するパターン

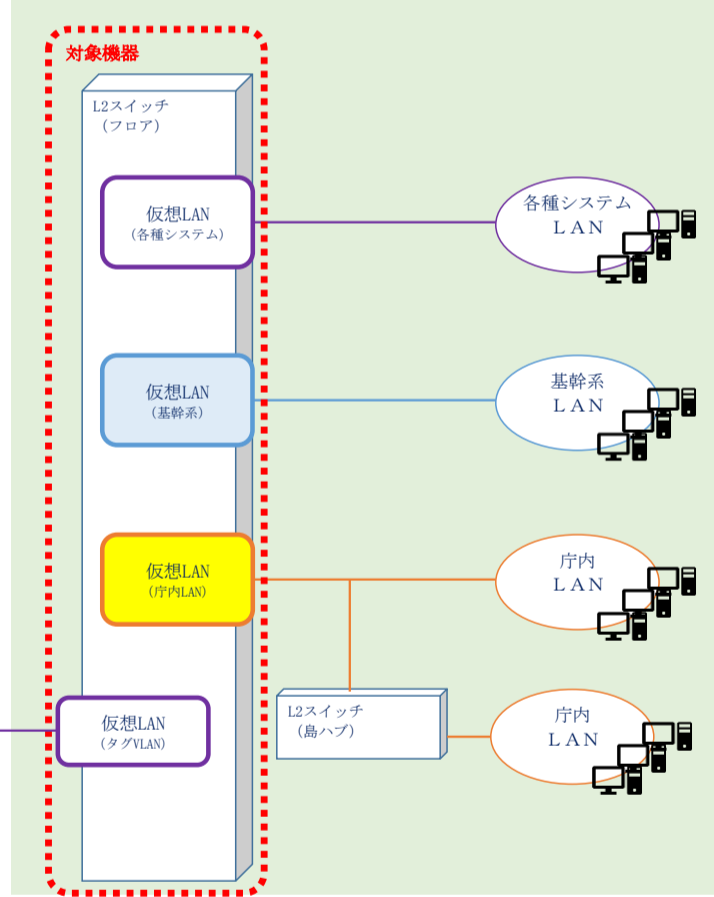
タイプA拠点 (電話交換機械室)



タイプA拠点 (EPS室)



タイプA拠点 (フロア)



TPケーブル

TPケーブル

表1. 1 統合対象通信回線 (ギャランティ型WAN回線)

拠点No.	拠点名 (統合NW)	通信回線グループ	拠点パターン	WAN回線冗長化の有無	VoIP	各種システム	基幹系	庁内LAN
1	情報システムセンター	グループ1	センタ	○	○	○	○	○
2	本庁舎	グループ1	タイプA	○	○	○	○	○
3	北庁舎	グループ1	タイプA	○	—	—	○	○
4	上杉分庁舎	グループ1	タイプA	○	○	○	○	○
5	青葉区役所	グループ1	タイプA	○	○	○	○	○
6	宮城野区役所	グループ1	タイプA	○	○	○	○	○
7	若林区役所	グループ1	タイプA	○	○	○	○	○
8	太白区役所	グループ1	タイプA	○	○	○	○	○
9	泉区役所	グループ1	タイプA	○	○	○	○	○
10	宮城総合支所	グループ1	タイプA	○	○	○	○	○
11	秋保総合支所	グループ1	タイプA	○	○	○	○	○
12	情報・産業プラザ (AER)	グループ1	タイプB	○	—	—	○	—
13	吉成証明発行センター	グループ1	タイプB	○	—	—	○	—
14	高砂証明発行センター	グループ1	タイプB	○	—	—	○	—
15	岩切証明発行センター	グループ1	タイプB	○	—	—	○	—
16	六郷証明発行センター	グループ1	タイプB	○	—	—	○	—
17	七郷証明発行センター	グループ1	タイプB	○	—	—	○	—
18	生出証明発行センター	グループ1	タイプB	○	—	—	○	—
19	中田証明発行センター	グループ1	タイプB	○	—	—	○	—
20	根白石証明発行センター	グループ1	タイプB	○	—	—	○	—
21	南光台証明発行センター	グループ1	タイプB	○	—	—	○	—
22	二日町第二仮庁舎	グループ1	タイプC	—	○	—	○	○
23	二日町第三仮庁舎	グループ1	タイプC	—	○	—	○	○
24	二日町第四仮庁舎	グループ1	タイプC	—	○	—	○	○
25	表小路仮庁舎	グループ1	タイプC	—	○	—	—	○
26	衛生研究所	グループ1	タイプC	—	○	○	—	—
27	健康増進センター	グループ1	タイプC	—	○	—	○	—
28	中央卸売市場	グループ1	タイプC	—	○	○	—	—
29	消防局	グループ1	タイプC	—	○	—	○	○
30	水道局	グループ1	タイプC	—	○	—	○	○
31	二日町分庁舎	グループ1	タイプD	—	○	—	○	—
32	上杉仮庁舎	グループ1	タイプD	—	○	—	○	○
33	精神保健福祉総合センター	グループ1	タイプD	—	○	—	○	—
34	南部発達相談支援センター	グループ1	タイプD	—	○	—	○	—
35	食肉市場 (食肉検査場)	グループ1	タイプD	—	—	○	—	—
36	児童相談所	グループ1	タイプD	—	—	—	○	—
37	交通局	グループ1	タイプD	—	○	—	○	—
38	仙台市立病院	グループ1	タイプD	—	○	—	○	—
39	錦町庁舎	グループ1	タイプE	—	○	—	—	—
40	東京事務所	グループ1	タイプE	—	○	—	—	—
41	消費生活センター	グループ1	タイプE	—	○	—	—	—
42	青葉環境事業所	グループ1	タイプE	—	○	—	—	—
43	宮城野環境事業所	グループ1	タイプE	—	○	—	—	—
44	若林環境事業所	グループ1	タイプE	—	○	—	—	—
45	泉環境事業所	グループ1	タイプE	—	○	—	—	—
46	葛岡工場	グループ1	タイプE	—	○	—	—	—
47	今泉工場	グループ1	タイプE	—	○	—	—	—
48	松森工場	グループ1	タイプE	—	○	—	—	—
49	八木山動物園	グループ1	タイプE	—	○	—	—	—
50	下水道北管理センター	グループ1	タイプE	—	○	—	—	—
51	下水道南管理センター	グループ1	タイプE	—	○	—	—	—
52	設備管理センター	グループ1	タイプE	—	○	—	—	—
53	南蒲生浄化センター	グループ1	タイプE	—	○	—	—	—
54	水質管理センター	グループ1	タイプE	—	○	—	—	—
55	ガス局	グループ1	タイプE	—	○	—	—	—
56	仙台市コールセンター	グループ1	タイプE	—	○	—	—	—

表 1. 1 統合対象通信回線（ベストエフォート型WAN回線）

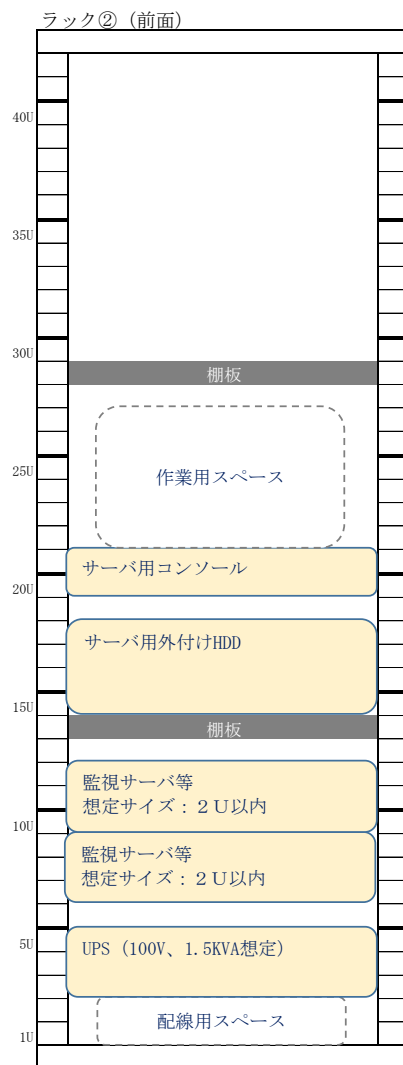
拠点 No.	拠点名（統合NW）	通信回線 グループ	拠点 パターン	GJ システム	SS システム
57	情報システムセンター	グループ2	タイプF	—	○
58	本庁舎	グループ2	タイプF	—	○
59	錦町庁舎	グループ2	タイプF	—	○
60	青葉区役所	グループ2	タイプF	—	○
61	宮城野区役所	グループ2	タイプF	—	○
62	若林区役所	グループ2	タイプF	—	○
63	太白区役所	グループ2	タイプF	—	○
64	泉区役所	グループ2	タイプF	—	○
65	宮城総合支所	グループ2	タイプF	—	○
66	秋保総合支所	グループ2	タイプF	—	○
67	消費生活センター（エルパーク仙台）	グループ2	タイプF	—	○
68	市民会館	グループ2	タイプF	—	○
69	戦災復興記念館	グループ2	タイプF	○	○
70	仙台市体育館	グループ2	タイプF	—	○
71	葛岡工場（葛岡温水プール）	グループ2	タイプF	—	○
72	情報・産業プラザ（エル・ソーラ仙台）	グループ2	タイプF	—	○
73	表小路仮庁舎	グループ2	タイプF	—	○
74	二日町第三仮庁舎	グループ2	タイプF	—	○
75	二日町第四仮庁舎	グループ2	タイプF	—	○
76	上杉分庁舎	グループ2	タイプF	—	○
77	青葉区中央市民センター	グループ2	タイプF	○	○
78	柏木市民センター	グループ2	タイプF	○	○
79	北山市民センター	グループ2	タイプF	○	○
80	福沢市民センター	グループ2	タイプF	○	○
81	旭ヶ丘市民センター	グループ2	タイプF	○	○
82	三本松市民センター	グループ2	タイプF	○	○
83	片平市民センター	グループ2	タイプF	○	○
84	水の森市民センター	グループ2	タイプF	○	○
85	貝ヶ森市民センター	グループ2	タイプF	○	○
86	中山市民センター	グループ2	タイプF	○	○
87	折立市民センター	グループ2	タイプF	○	○
88	宮城西市民センター	グループ2	タイプF	○	○
89	大沢市民センター	グループ2	タイプF	○	○
90	落合市民センター	グループ2	タイプF	○	○
91	吉成市民センター	グループ2	タイプF	○	○
92	木町通市民センター	グループ2	タイプF	○	○
93	生涯学習支援センター	グループ2	タイプF	○	○
94	高砂市民センター	グループ2	タイプF	○	○
95	岩切市民センター	グループ2	タイプF	○	○
96	鶴ヶ谷市民センター	グループ2	タイプF	○	○
97	榴ヶ岡市民センター	グループ2	タイプF	○	○
98	東部市民センター	グループ2	タイプF	○	○
99	幸町市民センター	グループ2	タイプF	○	○
100	田子市民センター	グループ2	タイプF	○	○
101	福室市民センター	グループ2	タイプF	○	○
102	七郷市民センター	グループ2	タイプF	○	○
103	荒町市民センター	グループ2	タイプF	○	○
104	六郷市民センター	グループ2	タイプF	○	○
105	沖野市民センター	グループ2	タイプF	○	○
106	若林市民センター	グループ2	タイプF	○	○
107	生出市民センター	グループ2	タイプF	○	○
108	中田市民センター	グループ2	タイプF	○	○
109	西多賀市民センター	グループ2	タイプF	○	○
110	八本松市民センター	グループ2	タイプF	○	○
111	八木山市民センター	グループ2	タイプF	○	○
112	山田市民センター	グループ2	タイプF	○	○
113	茂庭台市民センター	グループ2	タイプF	○	○
114	東中田市民センター	グループ2	タイプF	○	○
115	柳生市民センター	グループ2	タイプF	○	○
116	富沢市民センター	グループ2	タイプF	○	○

拠点 No.	拠点名 (統合NW)	通信回線 グループ	拠点 パターン	GJ システム	SS システム
117	湯元市民センター	グループ2	タイプF	—	○
118	秋保市民センター	グループ2	タイプF	○	○
119	泉区中央市民センター	グループ2	タイプF	○	○
120	根白石市民センター	グループ2	タイプF	○	○
121	南光台市民センター	グループ2	タイプF	○	○
122	黒松市民センター	グループ2	タイプF	○	○
123	将監市民センター	グループ2	タイプF	○	○
124	加茂市民センター	グループ2	タイプF	○	○
125	高森市民センター	グループ2	タイプF	○	○
126	松陵市民センター	グループ2	タイプF	○	○
127	寺岡市民センター	グループ2	タイプF	○	○
128	長命ヶ丘市民センター	グループ2	タイプF	○	○
129	松森市民センター	グループ2	タイプF	○	○
130	桂市民センター	グループ2	タイプF	○	○
131	南中山市民センター	グループ2	タイプF	○	○
132	広瀬文化センター(広瀬市民センター)	グループ2	タイプF	○	○
133	宮城広瀬総合運動場(宮城広瀬体育館)	グループ2	タイプF	—	○
134	宮城野区文化センター(宮城野区中央市民センター)	グループ2	タイプF	○	○
135	若林区文化センター(若林区中央市民センター)	グループ2	タイプF	○	○
136	太白区文化センター(太白区中央市民センター)	グループ2	タイプF	○	○
137	泉文化創造センター(イズミティ21)	グループ2	タイプF	—	○
138	仙台国際センター	グループ2	タイプF	—	○
139	青年文化センター	グループ2	タイプF	—	○
140	仙台文学館	グループ2	タイプF	—	○
141	福祉プラザ	グループ2	タイプF	—	○
142	シルバーセンター	グループ2	タイプF	—	○
143	秋保・里センター	グループ2	タイプF	—	○
144	せんだいメディアテーク	グループ2	タイプF	—	○
145	大倉ふるさとセンター	グループ2	タイプF	—	○
146	青葉体育館	グループ2	タイプF	—	○
147	川内庭球場	グループ2	タイプF	—	○
148	陸上競技場	グループ2	タイプF	—	○
149	新田総合運動場(宮城野体育館)	グループ2	タイプF	—	○
150	新田総合運動場(市民球場)	グループ2	タイプF	—	○
151	出花体育館	グループ2	タイプF	—	○
152	若林体育館	グループ2	タイプF	—	○
153	今泉運動場	グループ2	タイプF	—	○
154	中田温水プール	グループ2	タイプF	—	○
155	茂庭荘(茂庭庭球場)	グループ2	タイプF	—	○
156	秋保体育館	グループ2	タイプF	—	○
157	泉総合運動場(体育館)	グループ2	タイプF	—	○
158	泉サッカー場	グループ2	タイプF	—	○
159	屋内グラウンド(シェルコム仙台)	グループ2	タイプF	—	○
160	泉海洋センター	グループ2	タイプF	—	○
161	北中山コミュニティグラウンド	グループ2	タイプF	—	○
162	根白石温水プール	グループ2	タイプF	—	○
163	公園緑地協会	グループ2	タイプF	—	○
164	青葉山公園庭球場	グループ2	タイプF	—	○
165	御町東二丁目公園庭球場	グループ2	タイプF	—	○
166	湯元公園野球場	グループ2	タイプF	—	○
167	七北田公園(体育館)	グループ2	タイプF	—	○
168	七北田公園(庭球場)	グループ2	タイプF	—	○
169	泉総合運動場(泉庭球場)	グループ2	タイプF	—	○
170	海岸公園	グループ2	タイプF	—	○
171	市民利用センター拠点(ISP)	グループ2	タイプF	—	○

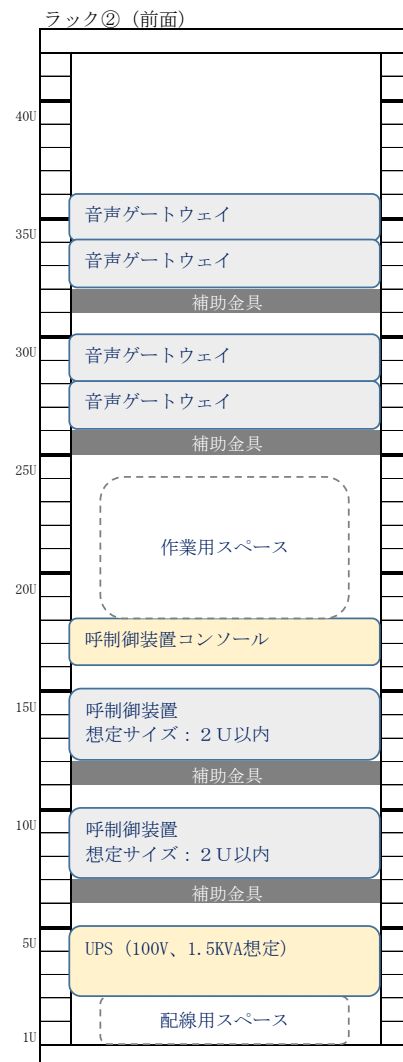
※通信回線グループ3(タイプG拠点)は現行回線からの変更がないため省略する。

図 1. 2 ネットワーク機器設置環境

1. フルラック (センタ拠点)



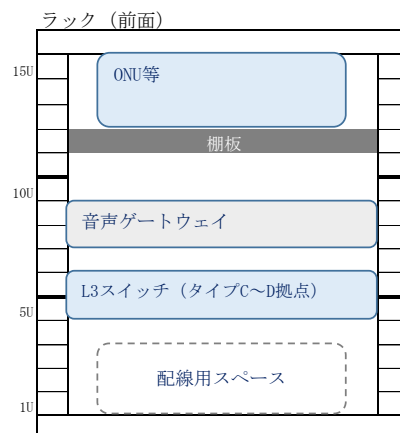
2. フルラック (タイプA拠点: 本庁舎)



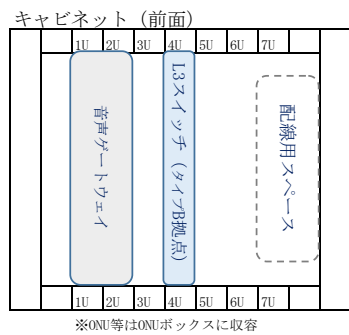
3. フルラック (タイプA拠点：区役所等)



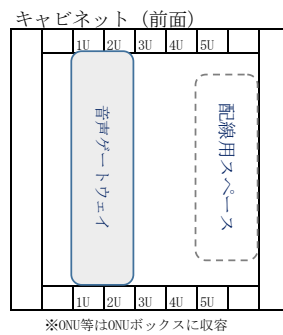
4. ハーフラック (タイプC～D拠点)



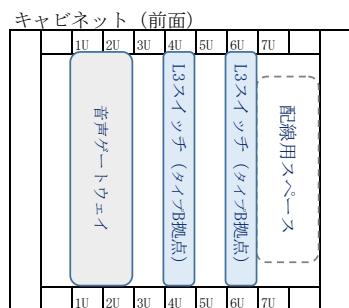
5. キャビネット (タイプB拠点: 証明発行センター等)



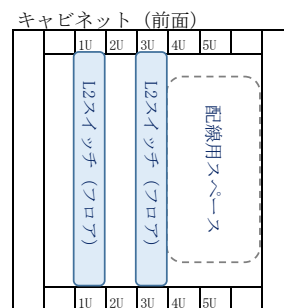
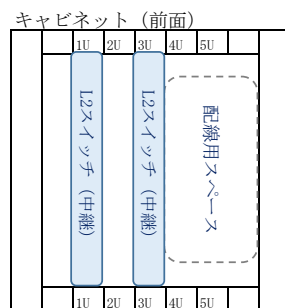
7. キャビネット (タイプE拠点)



6. キャビネット (タイプB拠点: 仙台駅前SC)



8. キャビネット (拠点LAN中継/フロア)



9. 机上設置 (タイプF~G拠点/島ハブ)



表1. 2 ハードウェア要件 ネットワーク機器

1. L3スイッチ① (センタ拠点用)

モデル	<ul style="list-style-type: none"> ・L3スイッチ 	
冗長構成	<ul style="list-style-type: none"> 単体冗長構成 ・冗長部分がホットスワップに対応 	<ul style="list-style-type: none"> スタック冗長構成 ・スタックメンバがホットスワップに対応
インターフェース	<ul style="list-style-type: none"> 冗長構成の合計として以下のインターフェースを利用可能なこと 冗長部分の故障時にケーブルを接続変更して運用できるポート数とする ・10/100/1000BASE-T 96ポート以上 ・SFP/SFP+ 24ポート以上 	<ul style="list-style-type: none"> スタックメンバ1台あたりの構成として以下のインターフェースを利用可能なこと スタックメンバの故障時に他のスタックメンバにケーブルを接続変更して運用できるポート数とする ・10/100/1000BASE-T 48ポート以上 ・SFP/SFP+ 12ポート以上
性能	<ul style="list-style-type: none"> ・最大スイッチング容量 (240Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (64K) 	<ul style="list-style-type: none"> スタックメンバ1台あたり以下の性能を満たすこと ・最大スイッチング容量 (120Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (64K)
仮想化	<ul style="list-style-type: none"> ・ネットワークパーティション (VRF) ・仮想LAN (VLAN) 	
スイッチング機能	<ul style="list-style-type: none"> ・タグVLAN ・VXLAN または QinQ ・L2ループ検知 ・LinkAggregation (LAG) 	
ルーティング機能	<ul style="list-style-type: none"> ・OSPF ・BGP4 	
ネットワーク機能	<ul style="list-style-type: none"> ・QoS ・VRRP 	
外形	<ul style="list-style-type: none"> ・ラックマウント (冗長構成で8U以内、奥行700mm以内) 	
備考	<ul style="list-style-type: none"> ・保守：24時間365日オンサイト 	

2. L3スイッチ② (タイプA拠点用) (全ポートSFP)

モデル	<ul style="list-style-type: none"> ・L3スイッチ 	
冗長構成	<ul style="list-style-type: none"> 単体冗長構成 ・冗長部分がホットスワップに対応 	<ul style="list-style-type: none"> スタック冗長構成 ・スタックメンバがホットスワップに対応
インターフェース	<ul style="list-style-type: none"> 冗長構成の合計として以下のインターフェースを利用可能なこと 冗長部分の故障時にケーブルを接続変更して運用できるポート数とする ・SFP/SFP+ 24ポート以上 	<ul style="list-style-type: none"> スタックメンバ1台あたりの構成として以下のインターフェースを利用可能なこと スタックメンバの故障時に他のスタックメンバにケーブルを接続変更して運用できるポート数とする ・SFP/SFP+ 24ポート以上
性能	<ul style="list-style-type: none"> ・最大スイッチング容量 (144Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (32K) 	<ul style="list-style-type: none"> スタックメンバ1台あたり以下の性能を満たすこと ・最大スイッチング容量 (120Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (32K)
仮想化	<ul style="list-style-type: none"> ・ネットワークパーティション (VRF) ・仮想LAN (VLAN) 	
スイッチング機能	<ul style="list-style-type: none"> ・タグVLAN ・VXLAN または QinQ ・L2ループ検知 ・LinkAggregation (LAG) 	
ルーティング機能	<ul style="list-style-type: none"> ・OSPF ・BGP4 	
ネットワーク機能	<ul style="list-style-type: none"> ・QoS ・VRRP 	
外形	<ul style="list-style-type: none"> ・ラックマウント (冗長構成で8U以内、奥行700mm以内) 	
備考	<ul style="list-style-type: none"> ・保守 : 24時間365日オンサイト 	

3. L3スイッチ③ (タイプA拠点用) (SFP 4ポート程度)

モデル	<ul style="list-style-type: none"> ・L3スイッチ 	
冗長構成	<ul style="list-style-type: none"> 単体冗長構成 ・冗長部分がホットスワップに対応 	<ul style="list-style-type: none"> スタック冗長構成 ・スタックメンバがホットスワップに対応
インターフェース	<ul style="list-style-type: none"> 冗長構成の合計として以下のインターフェースを利用可能なこと 冗長部分の故障時にケーブルを接続変更して運用できるポート数とする ・10/100/1000BASE-T 48ポート以上 ・SFP/SFP+ 8ポート以上 	<ul style="list-style-type: none"> スタックメンバ1台あたりの構成として以下のインターフェースを利用可能なこと スタックメンバの故障時に他のスタックメンバにケーブルを接続変更して運用できるポート数とする ・10/100/1000BASE-T 48ポート以上 ・SFP/SFP+ 4ポート以上
性能	<ul style="list-style-type: none"> ・最大スイッチング容量 (144Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (32K) 	<ul style="list-style-type: none"> スタックメンバ1台あたり以下の性能を満たすこと ・最大スイッチング容量 (120Gbps) ・最大パケット処理性能 (240Mpps) ・最大ルーティング経路 (13K) ・最大MACアドレス数 (32K)
仮想化	<ul style="list-style-type: none"> ・ネットワークパーティション (VRF) ・仮想LAN (VLAN) 	
スイッチング機能	<ul style="list-style-type: none"> ・タグVLAN ・VXLAN または QinQ ・L2ループ検知 ・LinkAggregation (LAG) 	
ルーティング機能	<ul style="list-style-type: none"> ・OSPF ・BGP4 	
ネットワーク機能	<ul style="list-style-type: none"> ・QoS ・VRRP 	
外形	<ul style="list-style-type: none"> ・ラックマウント (冗長構成で8U以内、奥行700mm以内) 	
備考	<ul style="list-style-type: none"> ・保守 : 24時間365日オンサイト 	

4. L3スイッチ④ (タイプB~D拠点用)

モデル	<ul style="list-style-type: none"> L3スイッチ 	
冗長構成	—	仙台駅前SC <ul style="list-style-type: none"> スタック冗長構成 スタックメンバがホットスワップに対応
インターフェース	<ul style="list-style-type: none"> 10/100/1000BASE-T 24ポート以上 	スタックメンバ1台あたりの構成として以下のインターフェースを利用可能なこと スタックメンバの故障時に他のスタックメンバにケーブルを接続変更して運用できるポート数とする <ul style="list-style-type: none"> 10/100/1000BASE-T 24ポート以上
性能	<ul style="list-style-type: none"> 最大スイッチング容量 (48Gbps) 最大パケット処理性能 (214Mpps) 最大ルーティング経路 (13K) 最大MACアドレス数 (32K) 	スタックメンバ1台あたり以下の性能を満たすこと <ul style="list-style-type: none"> 最大スイッチング容量 (48Gbps) 最大パケット処理性能 (214Mpps) 最大ルーティング経路 (13K) 最大MACアドレス数 (32K)
仮想化	<ul style="list-style-type: none"> ネットワークパーティション (VRF) 仮想LAN (VLAN) 	
スイッチング機能	<ul style="list-style-type: none"> タグVLAN VXLAN または QinQ L2ループ検知 LinkAggregation (LAG) 	
ルーティング機能	<ul style="list-style-type: none"> OSPF BGP4 	
ネットワーク機能	<ul style="list-style-type: none"> QoS VRRP 	
外形	<ul style="list-style-type: none"> ラックマウント (冗長構成で2U以内、奥行500mm以内) 	
備考	<ul style="list-style-type: none"> 保守：平日先出 SEND バック 	

5. ルータ（タイプF拠点用）（LAN 8ポート）

モデル	・ルータ
冗長構成	－
インターフェース	・10/100/1000BASE-T 8ポート以上
性能	・最大パケット処理性能（384Kpps） ・最大ルーティング経路（4K）
仮想化	－
スイッチング機能	・ポートVLAN
ルーティング機能	・スタティック
ネットワーク機能	・IPsec ・L2TP ・PPPoEマルチセッション
外形	－
備考	・電源内蔵 ・保守：平日先出センドバック

6. ルータ（タイプF拠点用）（生涯学習支援センター及び市民利用施設予約システムISP拠点用）

モデル	・ルータ
冗長構成	－
インターフェース	・10/100/1000BASE-T 5ポート以上
性能	・最大パケット処理性能（384Kpps） ・最大ルーティング経路（4K）
仮想化	－
スイッチング機能	・ポートVLAN
ルーティング機能	・スタティック
ネットワーク機能	・IPsec ・L2TP ・PPPoEマルチセッション
外形	－
備考	・電源内蔵 ・保守：平日先出センドバック

7. L2スイッチ① (ディストリビューション) (24ポートスタック対応)

モデル	・L2スイッチ
冗長構成	・スタック冗長構成 ・冗長部分がホットスワップに対応
インターフェース	スタックメンバ1台あたりの構成として以下のインターフェースを利用可能なこと スタックメンバの故障時に他のスタックメンバにケーブルを接続変更して運用できるポート数とする ・10/100/1000BASE-T 24ポート以上 ・SFP/SFP+ 4ポート以上
性能	・最大スイッチング容量 (56Gbps) ・最大パケット処理性能 (41Mpps) ・最大MACアドレス数 (32K)
仮想化	・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	—
ネットワーク機能	・MAC認証
外形	・ラックマウント (冗長構成で2U以内、奥行500mm以内)
備考	・保守：平日先出センドバック

8. L2スイッチ② (ディストリビューション) (48ポートスタック対応)

モデル	・L2スイッチ
冗長構成	・スタック冗長構成 ・冗長部分がホットスワップに対応
インターフェース	スタックメンバ1台あたりの構成として以下のインターフェースを利用可能なこと スタックメンバの故障時に他のスタックメンバにケーブルを接続変更して運用できるポート数とする ・10/100/1000BASE-T 48ポート以上 ・SFP/SFP+ 4ポート以上
性能	・最大スイッチング容量 (104Gbps) ・最大パケット処理性能 (77Mpps) ・最大MACアドレス数 (32K)
仮想化	・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	—
ネットワーク機能	・MAC認証
外形	・ラックマウント (冗長構成で2U以内、奥行500mm以内)
備考	・保守：平日先出センドバック

9. L2スイッチ③ (フロア) (24ポートファンレス)

モデル	・L2スイッチ
冗長構成	—
インターフェース	・10/100/1000BASE-T 24ポート以上
性能	・最大スイッチング容量 (56Gbps) ・最大パケット処理性能 (41Mpps) ・最大MACアドレス数 (16K)
仮想化	・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	—
ネットワーク機能	・MAC認証
外形	・ラックマウント (1U以内、奥行200mm以内)
備考	・ファンレス ・保守：平日先出 SENDバック

10. L2スイッチ④ (フロア) (16ポートファンレス)

モデル	・L2スイッチ
冗長構成	—
インターフェース	・10/100/1000BASE-T 16ポート以上
性能	・最大スイッチング容量 (32Gbps) ・最大パケット処理性能 (29Mpps) ・最大MACアドレス数 (16K)
仮想化	・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	—
ネットワーク機能	・MAC認証
外形	
備考	・ファンレス ・保守：平日先出 SENDバック

1 1. L2スイッチ⑤ (フロア) (8ポートファンレス)

モデル	・L2スイッチ
冗長構成	—
インターフェース	・10/100/1000BASE-T 8ポート以上
性能	・最大スイッチング容量 (16Gbps) ・最大パケット処理性能 (14Mpps) ・最大MACアドレス数 (8K)
仮想化	・仮想LAN (VLAN)
スイッチング機能	・タグVLAN ・L2ループ検知 ・LinkAggregation (LAG)
ルーティング機能	—
ネットワーク機能	—
外形	
備考	・ファンレス ・保守：平日先出 SENDバック

1 2. VoIPゲートウェイ

モデル	・ISR4331-V/K9相当
機能・性能	・音声ゲートウェイ ・E/Mインターフェース数 (8以上)
外形	・ラックマウント (1U以内、奥行600mm以内)
備考	・PVDM4-32以上 ・保守：平日先出 SENDバック

1 3. 音声モジュール①

モデル	・Cisco NIM-4E/M 相当
機能・性能	・OD トランクインターフェース
備考	・保守：平日先出 SENDバック

1 4. 音声モジュール②

モデル	・Cisco NIM-2FXSP 相当
機能・性能	・COT トランクインターフェース
備考	・保守：平日先出 SENDバック

表 1. 2 ハードウェア要件 VoIP機器

1. 呼制御装置

モデル	・呼制御装置、ラックマウント型
機能・性能	・呼制御 ・最大ユーザ数 (1000) ・最大デバイス数 (2500)
外形	・ラックマウント (2U以内、奥行800mm以内)
備考	・Cisco Business Edition 6000相当 ・保守：24時間365日オンサイト

2. コンソール

モデル	・ラックマウント型
機能・性能	・呼制御装置の画面表示、キーボード/マウス操作ができること ・17 インチTFT 液晶 (最大1920×1080 の解像度) ・タッチパッド付キーボード (106 キーボード相当)
外形	・ラックマウント (1U以内、奥行1000mm以内)
備考	・保守：24時間365日オンサイト ・呼制御装置接続に必要なスイッチ/ケーブル含む

3. UPS

モデル	・ラックマウント型
機能・性能	・呼制御装置のシャットダウン制御できること ・ネットワーク経由で電源制御ができること ・ネットワーク管理ソフトウェアで管理できること
外形	・ラックマウント (2U以内、奥行1000mm以内)
備考	・保守：24時間365日オンサイト

表 1. 2 ハードウェア要件 監視機器

1. NW監視サーバ

モデル	・ラックマウント型
OS	・NW監視ソフトウェアの推奨動作環境を満たしていること
ソフトウェア	NW監視ソフトウェア ・NNM (NetworkNodeManager) 機能を有していること。 ・ICMP、SNMP を用いてNW 機器を自動的に検出し、監視用マップを自動的に生成できること。 ・対象ノードの生存監視を行い、異常時にはアラート通知ができること ・Web コンソールが利用でき、ネットワーク経由で管理できること ・日本語でのGUI 表示ができること ・700 ノードの機器を管理できるライセンスを有していること
機能・性能	・NW 監視ソフトウェアの推奨動作環境を満たしていること ・UPS と連動し安全にシャットダウンができること
外形	・ラックマウント (2U以内、奥行800mm以内)
備考	・保守：24時間365日オンサイト ・ソフトウェアサポート：平日9～17時

2. シスログサーバ

モデル	・ラックマウント型
OS	・SYSLOGソフトウェアの推奨動作環境を満たしていること
ソフトウェア	SYSLOG ソフトウェア ・700 台以上の機器からSyslog 転送を受信し記録できること ・ログ送信元のIP アドレスを元にフィルタリングできること ・記録したログデータを自動的にアーカイブできること
機能・性能	・SYSLOGソフトウェアの推奨動作環境を満たしていること ・UPS と連動し安全にシャットダウンができること
外形	・ラックマウント (2U以内、奥行800mm以内)
備考	・保守：24時間365日オンサイト ・ソフトウェアサポート：平日9～17時

3. コンソール

モデル	・ラックマウント型
機能・性能	・サーバの画面表示、キーボード/マウス操作ができること ・17 インチTFT 液晶 (最大1920×1080 の解像度) ・タッチパッド付キーボード (106 キーボード相当)
外形	・ラックマウント (1U以内、奥行1000mm以内)
備考	・保守：24 時間365 日オンサイト ・サーバ接続に必要なスイッチ/ケーブル含む

4. UPS

モデル	・ラックマウント型
機能・性能	・NW 監視サーバ、シスログサーバのシャットダウン制御できること
外形	・ラックマウント（2U以内、奥行700mm以内）
備考	・保守：24時間365日オンサイト

5. NTPサーバ

モデル	・TS-2220相当
機能・性能	・時刻情報を受信し、ネットワーク経由で時刻同期ができること ・GPS方式に対応していること
外形	・ラックマウント（2U以内、奥行700mm以内）
備考	・保守：平日先出 SEND バック

6. ファイアウォール

モデル	・ボックス型
インターフェース	10/100/1000BASE-T 8 ポート以上
機能・性能	・ファイアウォールパフォーマンス（ラージパケット700Mbps 以上） （IMIX 200Mbps 以上） ・VPN パフォーマンス（3DES+SHA-1 100Mbps 以上） ・セキュリティポリシー（384 以上）
外形	・ラックマウント（1U以内、奥行700mm以内）
備考	・保守：平日先出 SEND バック

7. 外付けHDD

モデル	・USB-HDD
機能・性能	・NW 監視サーバ、シスログサーバのデータ保存ができること ・USB3.0 対応（サーバ接続用） ・最大容量（2TB 以上）
外形	—
備考	・保守：平日先出 SEND バック

8. 監視端末

モデル	・デスクトップ一体型またはノート型
OS	・Microsoft Windows10/Pro
ソフトウェア	・Microsoft OfficePersonal2019
機能・性能	・Windows10/Pro の推奨動作環境を満たしていること ・OfficePersonal2019 の推奨動作環境を満たしていること
外形	—
備考	・情報システム課設置はノート型に限定 ・保守：平日9～17時オンサイト

表 1. 2 ハードウェア要件 ネットワークラック

1. フルラック

規格	・EIA
高さ	・42U
横幅	・800mm
奥行	・1000mm
備考	・転倒防止対策を行うこと ・センタ拠点用及び本庁舎用は2連結とする

2. ハーフラック

規格	・EIA
高さ	・15U
横幅	・700mm
奥行	・1000mm
備考	・転倒防止対策を行うこと

3. キャビネット①

規格	・EIA
高さ	・600mm
横幅	・7U（機器を縦方向に搭載）
奥行	・600mm
備考	・キャスタ付とする

4. キャビネット②

規格	・EIA
高さ	・600mm
横幅	・5U（機器を縦方向に搭載）
奥行	・600mm
備考	・キャスタ付とする