我孫子市第２期庁内 ICT インフラ基盤グランドデザイン

（第１版）



令和８年 11 月

我孫子市　企画総務部　デジタル戦略課

目　次

第 1 章　グランドデザインの概要と構成 1
1-1. 本グランドデザインの目的と基本理念 1
1-1-1. 策定背景と次期 12 年（6 年+6 年）の基本コンセプト 1
①境界型防御の限界と「ZTNA ハイブリッド β モデル」への進化 1
②財政的持続性と安全性の両立 1
1-1-2. ドキュメント体系と役割 1
①本グランドデザインのドキュメント構成 1
②本章が果たす 2 つの核心的役割 2
1-2. 本市が直面する主要課題と解決アプローチ 2
1-2-1. 現行 ICT インフラ基盤の構成規模 2
1-2-2. 三層分離と ZTNA を融合した「ハイブリッド型ネットワーク」の構築/第 2 章 .. 4
① 完全 ZTNA における構造的リスクと業務継続性の確保 4
②高度なネットワーク構成の実現（三層分離×庁内 ZTNA） 4
1-2-3. サプライチェーン・リスク対策とハードウェア調達方法の見直し/第 3 章 5
①2026 年のサーバ価格異常高騰の教訓と特定メーカー依存の脱却 5
②大手メーカーの許容と特定メーカー依存の排除 5
③後期契約時の価格高騰に対応できるマルチベンダー切替体制の必須化 5
④ベンダーに求める先回り提案力と適応力 5
1-2-4. 仮想化ソフトウェア価格高騰への対抗策と OSS 活用原則/第 3 章 6
①大手メーカーのハイパーバイザへの依存からの脱却 6
②Proxmox VE および Accops による本市 PoC 結果の公表 6
③提案者自身のナレッジ・独自検証要件 6
1-3. 各章の個別技術のアーキテクチャ・サマリー 7
1-3-1. ネットワーク（アクセス制御、証明書認証、ネットワーク分離）/第 2 章 7
①電子証明書認証に基づく庁内 ZTNA の確立と主要拠点への Wi-Fi 導入 7
②島 HUB 混在環境に対する強固な複合防御（IPSG・定期再認証） 7
③ZTNA ハイブリッド β モデルによる 10 セグメント論理分離 7
1-3-2. 仮想基盤（3Tier・マルチ OS 対応 VDI・脱ベンダーロックイン）/第 3 章 8
①3Tier アーキテクチャの維持と既存高機能ストレージ資産の活用 8
②マルチ OS 対応 VDI 接続管理基盤の採用 9
③目的別 VDI 基盤の区分と最適化 9
1-3-3. システム（無害化・多層防御・セキュリティ連携）/第 4 章 9
①多段プロキシ構成と Web・ファイル無害化処理の徹底 9
②メールセキュリティと上長承認ワークフロー 10
③エンドポイント防護（EPP+EDR）と境界型自動暗号化 10
④身体特性・運用リスクを考慮した二要素認証選定 10

1-3-4. 端末管理（ハイブリッド端末戦略・統合 AD・M365 最適化）/第 5 章 11
①コストとセキュリティを両立するハイブリッド端末配置戦略 11
②Active Directory（AD）統合 2 ドメイン構成と運用自動化（SSOT） 12
③Chrome Enterprise Upgrade（CEU）によるデバイスの集中管理 12
④Microsoft 365（M365）ライセンスの全体最適化（約 1,600 アカウント） 12
1-3-5. 外部通信（公的接続・LBO・マルチベンダー保守）/第 6 章 13
①公的クラウド基盤（セキュリティクラウド・ガバメントクラウド）への接続 13
②テレワーク基盤（専用 VM 不要・VDI 直接接続） 13
③NGN 網内 DDNS/VPN を活用した低コスト・マルチベンダー保守基盤 14
1-3-6. 保守・運用サポート（包括的サポート・ハイブリッド運用）/第 7 章 14
①包括的保守サポート原則（原則包含アプローチ）の導入 14
②保守内容・実績の事前開示と過大見積の防止 14
③オンサイトとリモートを融合させたハイブリッド保守体制 14
④月次保守定例会によるガバナンスと運用管理 15
1-4. 調達・選定評価・契約方式 15
1-4-1. 前・後期合計 12 年間の提案・分割契約モデル 15
①評価・競争範囲（12 年間） 15
②前期・後期の積算手法 16
③契約形式（前期のみ締結と随意契約の位置づけ） 16
1-4-2. 全体調達・事業工程 16
1-4-3. 契約関連規定および付属書の扱い 18
①契約付属書の規定 18
②解釈および適用における優先順位 18
1-4-4. 契約満了時の機器取扱い・データ消去規定 18
①ハードウェア無償譲渡および市資産化選択権 18
②不要機器の安全な廃棄とデータ破壊における分担体制 19
1-5. 成果連動型 SLA（サービスレベル合意）と運用評価 19
1-5-1. SLA の導入目的 19
①安定稼働の確保と継続的運用改善の促進 19
②受託者提案型 SLA 方式による価格転嫁の防止 19
1-5-2. ペナルティポイントとインセンティブポイントの相殺評価 20
①障害・品質低下に伴うペナルティポイント 20
②改善・課題解決に伴うインセンティブポイント 20
③ポイントの相殺メカニズムと運用貢献度の定量的評価 20
1-5-3. 金銭的処置（減額・清算）の適用基準 20
①累積ペナルティに対する清算措置と緊張感のある運用維持 20
②代替措置（物・作業による清算）の選択可能性と双方協議 21
第 2 章　ネットワーク 22
2-1. ネットワーク設計の基本方針：庁内 ZTNA の構築 22

2-1-1. 境界型防御から「庁内ゼロトラスト」への転換 22
2-1-2. 属性と状態に基づく厳格なアクセス制御 22
2-1-3. 物理的制約の排除と柔軟なワークスタイルの両立 22
2-1-4. 可用性を重視したハイブリッド・セキュリティ 22
2-2. 認証ベースのアクセス制御とネットワークセキュリティ 23
2-2-1. 端末認証による不正接続の構造的排除 23
2-2-2. 電子証明書による多階層の端末識別 24
①系統に応じた証明書の付与 24
②端末属性管理の徹底 24
2-2-3. D-VLAN による動的なネットワーク構成 24
①自動的なセグメント割り当て 24
②ロケーションフリーの実現 24
③アンマネージド HUB 混在環境における制御（IPSG・DHCP スヌーピング） 24
2-2-4. ネットワークが混在する場所への対応 25
①IP ソースガード（IPSG）による固定 IP 直打ちの完全遮断 26
②定期的な再認証による「なりすまし」の構造的無力化 26
2-2-5. 未許可デバイスの完全遮断と証明書認証の導入 26
①本庁舎周辺および主要拠点における庁内 Wi-Fi の導入と ZTNA の高度化 26
2-3. 次期ネットワークアーキテクチャ（ZTNA ハイブリッド β モデル） 27
2-3-1. ネットワーク・セグメントの定義 27
2-3-2. アドレッシング体系の特徴 28
2-3-3. 論理分離による安全性と独立性 29
2-4. 通信制御ポリシーと SASE の戦略的活用 29
2-4-1. SASE の導入検討（インターネット ASP） 29
①導入の目的 29
②運用方針 29
2-4-2. 単一障害点（SPOF）の回避と可用性の確保 29
①SASE 適用外とする重要基盤（対象外サービス） 30
②制御手法とレジリエンスの確保 30
2-5. ネットワーク運用の高度化 30
2-5-1. QoS 制御の徹底による通信品質の担保 30
①優先制御の実装 30
②帯域不足時のパケロス防止 30
2-5-2. セグメント間の完全分離と横断通信の遮断 31
①用途別分離の徹底 31
②VDI を経由しないアクセスの遮断 31
③セキュリティ境界の維持 31
2-5-3. ネットワークの可視化と動的な運用管理 31
①認証ログとトラフィックの相関分析 31

②運用負荷の軽減 31
第 3 章　仮想基盤 32
3-1. 仮想基盤設計の基本方針：脱ベンダーロックインとコストの最適化 32
3-1-1. 仮想化市場の構造変化と財政的リスクへの対応 32
3-1-2. オープンソースおよび新興ベンダーの戦略的活用 32
3-1-3. 調達における競争性の確保と機器選定の裁量権 32
3-2. 次期ハイパーバイザおよび仮想デスクトップ管理基盤の選定 33
3-2-1. ハイパーバイザ選定における調達リスクと経済性の評価 33
①商用製品の調達リスク排除 33
②総保有コスト（TCO）の最適化要件 33
③オープンソースソフトウェア（OSS）の戦略的志向 33
④技術的信頼性の担保と提案資格要件 34
3-2-2. 仮想デスクトップ（VDI）接続管理基盤に求められる機能要件 34
①特定商用製品からの脱却 34
②エンドポイントのマルチ OS 対応（必須要件） 35
③接続管理基盤における技術的信頼性の担保と提案資格要件 35
3-2-3. 代替方式「リモート PC アレイ」の検証 36
①リモート PC アレイの基本仕組み 36
②集約率の低さに伴う筐体数の膨大化 36
③ファシリティ面の限界（電源・ラック・工事コスト） 36
④全量移行の困難性と部分的導入の現実的妥当性 37
3-3. ハードウェア選定およびクラスタ構成（3Tier アーキテクチャ） 37
3-3-1. 特定メーカーに依存しないホストマシン選定 37
①経済情勢に伴う調達価格高騰への対策 37
②汎用・独立系サーバの視野投入とロックインの打破 38
3-3-2. クラスタ構成の定義（2 つの仮想基盤） 38
①セキュリティ用仮想基盤（約 130～150 台規模） 38
②VDI 用仮想基盤（総数約 1,700 台規模） 38
3-3-3. 3Tier 構成の維持と既存資産の継続利用に関する方針 39
①HCI 構成の不採用と 3Tier アーキテクチャの維持 39
②既存ストレージ資産の活用とベンダー交代への備え 39
3-4. クラウド移行における構造的リスクとオンプレミスの妥当性 39
3-4-1. クラウドの経済的実態と試算の不確実性 39
①資産非保有化とトータルコストの乖離 39
②隠れたコストと積算の困難さ 40
③従量課金制度に伴う予算管理の不確実性 40
3-4-2. 単一障害点（SPOF）と物理回線のボトルネック 40
①物理回線の構造的限界と共用経路のリスク 40
②セキュリティ基盤の障害による業務全停止リスク 41

3-4-3. 出戻り不能（クラウドロックイン）のリスク 41
①庁舎側ファシリティの喪失による再移行の困難さ 41
②データアウト課金による経済的ロックイン 41
3-5.【比較表】オンプレミス vs クラウドのメリット・デメリット 42
3-5-1. 比較評価の目的 42
3-5-2. 評価軸に基づく詳細比較 42
3-5-3. 本市における選定の妥当性と今後の検討方針 43
①現時点における結論の回避と評価の慎重性 43
②RFI（情報提供依頼）を通じた定量的データの収集 43
③表面的な一般論の排除と厳正な比較検討の重要性 44
第 4 章 セキュリティ・システム 45
4-1. Web セキュリティおよび情報無害化基盤の構成 45
4-1-1. 多段プロキシによる Web フィルタリングと SSL デコード要件 45
①ディレクトリサービス連携による認証とログ管理 45
②細分化されたフィルタルール制御 46
③SSL デコード機能と独自認証局の運用方針 46
4-1-2. セキュアブラウザによる Web ページ無害化と例外運用 46
①多段プロキシ構成によるネットワーク防御 46
②表示不具合への対応と例外運用の明確化 47
4-1-3. ダウンロードファイルに対するサニタイズ（ファイル無害化） 47
①セキュアブラウザと連動した自動サニタイズ 47
②原本保持・取り出し機能の排除による最適化 48
4-2. メールシステムおよびメールセキュリティの設計 48
4-2-1. 内部メールサーバの配置とアラート連携 48
①メール配信経路における位置付けと基本役割 48
②システムアラート受信用ゲートウェイとしての通信要件 48
4-2-2. 多層的なメールセキュリティと誤送信防止・冗長承認の徹底 49
①受信メールの多層検知と無害化処理 49
②送信制御による誤送信防止と上長による冗長承認 49
③送信元ドメイン（系統）別のマルチポリシー制御要件 50
4-3. エンドポイント管理・セキュリティおよびデータ保護 50
4-3-1. 資産管理の高度化と勤怠連携・ログ管理 50
①ソフトウェア資産管理とリモート配信・制御 50
②登録制外部デバイス制御によるマルウェア混入防止と VDI リダイレクトの検証 50
③ログイン・ログアウトログの収集と勤怠管理連携 51
4-3-2. ファイル持ち出し制御とファイル自動暗号化の連動設計 51
①外部持ち出し制御ワークフローと厳格な承認体系 52
②境界型自動暗号化の採用と運用の単純化 53
4-3-3. 次期エンドポイント対策（EPP および EDR の導入） 53

①EPP と EDR による多層防御体系の構築 53
②インシデント発生時の即時隔離と追跡能力 53
4-4．インフラ監視および共有リソースの最適化 54
4-4-1．ネットワーク・サーバ監視と重要サービスの死活監視要件 54
①全庁インフラに対する多層的な死活監視の適用 54
②重要システムに対するサービス・プロセス監視基準の定義 54
4-4-2．仮想基盤リソースを活用したファイルサーバ設計と AD 連携 54
①共有ストレージリソースを活用した 3Tier 連動型設計 54
②Active Directory 連携によるアクセス権限の自動設定 55
4-5．コミュニケーションおよび認証基盤の要件 55
4-5-1．グループウェア調達戦略（一括調達と別調達の評価） 55
①標準的機能の明確化と費用対効果の検証 55
②RFI（情報提供依頼）を通じた調達区分の評価方針 55
4-5-2．身体的特徴・運用特性を考慮した二要素認証の選定基準 56
①適用範囲の限定と運用の最適化 56
②身体的影響を受ける認証方式の除外 56
③実用性と確実性を兼ね備えた二要素認証技術の定義 56
第 5 章　端末構成・管理 58
5-1．クライアント端末構成およびネットワーク・セグメントの設計 58
5-1-1．端末形態（FAT/シンクライアント）と OS 戦略の定義 58
5-1-2．大規模 VDI に代わる代替方式（FAT 端末）の許容と解決すべき技術要件 58
① 大規模 VDI のコスト課題と代替提案の許容 58
② セキュア FAT・データレス PC 提案においてクリアすべき技術的課題 58
③ 評価方針 59
5-1-3．クライアント端末および VDI ライセンスの予定数量 59
5-1-4．三層分離ネットワークにおける端末割り当てと Chromebook 活用方針 60
①三層分離ネットワークにおける接続定義 60
②二要素認証の要件に基づく OS の分岐設計 60
③Chromebook 全面移行に向けた柔軟な設計思想 61
④インターネット Wi-Fi 接続と専用 FAT 端末の分離運用 61
5-1-5．クライアント端末の配備・運用方針（1 人 1 台個別貸与の導入検討） 61
①共有方式から「1 人 1 台個別貸与方式」への移行 61
②「6 年間携行」の原則と管理責任の明確化 62
③人事異動時の端末携行と、系統違い（NM 系／LG 系）に伴う例外ルール 62
④1 人 1 台・携行化がもたらす変革効果 63
5-1-6．端末調達におけるコスト最適化とメーカー選定の多様化 63
① 独立系メーカーおよび BTO（Build To Order）ブランドの積極的活用 63
② 長期保守と国内サポート体制の必須化 64
③ 調達事業者への柔軟な提案要求 64

5-2. ディレクトリサービスおよびデバイス・アカウント統合管理 64
5-2-1. Active Directory（AD）の統合・ドメイン分割構成 64
5-2-2. ユーザーアカウント設計と人事異動自動化（情報連携） 65
①アカウント運用原則 65
②所属・役職情報をマスターとした運用自動化 65
5-2-3. ユーザープロファイル管理の高度化（FSLogix 等の導入検討） 65
① 従来方式の課題とプロファイルコンテナ技術の検討 65
② VDI 環境における起動負荷軽減と安定稼働の実現 66
③ FAT 端末（代替方式含む）における通信帯域圧迫の解消 66
④ ライセンス体系および RFI における検証方針 66
5-2-4. Chrome Enterprise Upgrade によるクラウドデバイス管理 66
5-3. 端末アップデート管理および Microsoft 365 最適化 67
5-3-1. 資産管理基盤と連携した Windows 端末・VDI の一元更新管理 67
5-3-2. M365 ライセンスプランの選定とグループウェア統合の費用対効果検証 68
①現行ライセンス運用の評価と見直し 68
②RFI/RFP における提案要件と費用対効果の検証方針 68
5-4. 印刷基盤（プリンタサーバ）の集約とセキュアクロスセグメント印刷 69
5-4-1. 系統間（LGWAN 系・番号利用系）共有プリンタ設計 69
5-4-2. プリンタ専用セグメントの通信制御とセキュリティ強化 69
①独立したプリンタ専用セグメントの配置 69
②通信プロトコルの厳格な絞り込み 69
5-4-3. AD ログオンスクリプトによる論理プリンタの動的自動割り当て 70
①中央集約型論理プリンタ管理 70
②所属情報と連動した自動セットアップ（ノータッチ運用） 70
第 6 章 外部通信 71
6-1. ガバメントクラウドおよびセキュリティクラウド接続 71
6-1-1. 千葉県情報セキュリティクラウドを介したインターネット接続 71
①セキュリティクラウドへの通信集約 71
②標準経路としてのトラフィック制御 71
6-1-2. LGWAN 回線を介したガバメントクラウド（標準化基幹システム）接続設計 .. 71
①ガバメントクラウド運用の前提と回線経路 71
②庁内「番号利用系セグメント」からのアクセス制御 71
6-1-3. LGWAN ゲートウェイ基盤の構成と運用 72
①庁内 LAN と LGWAN の接合構成と機能の集約 72
② メール配送の振り分けとドメイン変換ルール 72
③ ドメイン変換テーブルのメンテナンス体制 73
6-2. ローカルブレイクアウト（LBO）の最適化と通信制御 73
6-2-1. 高速光回線（フレッツ 光クロス）を活用した LBO の対象範囲と適用拡張 .. 73
①LBO 導入の目的と回線構成 73

②LBO 対象通信の厳格な制御と適用拡張 73
6-2-2. 運用中の LBO 通信チューニングと保守運用境界の明確化 74
6-2-3. 閉域 SIM 環境と庁内 LAN の接合およびアクセス制御 75
①既存閉域 SIM 環境と次期庁内 LAN との相互接続設計 75
②最小権限原則に基づく厳格な ACL（アクセス制御）設計 76
③端末セキュリティと適用業務の維持 76
6-3. テレワークおよびマルチベンダー・リモート保守基盤 76
6-3-1. テレワーク用リモートアクセス基盤（固定 IP・VDI 連携） 76
①アクセス方式と専用 VM を必要としない構成 76
②庁内 VDI 環境との連携によるデータ持ち出し防止 77
6-3-2. NGN 網内 DDNS/VPN を活用した低コスト・マルチベンダー保守回線 77
①NGN 網内 DDNS/VPN を活用した通信構成 77
②回線コストの圧縮とベンダー間セキュリティの独立確保 77
6-4. 将来の回線分離・WAN 構造変化への適応設計 78
6-4-1. 回線多目的利用からの将来的な分離・拡張 78
①NGN 網内 DDNS による自動追従と VPN 自動確立の仕組み 78
②WAN 側変化（IPv6 アドレス・回線変更）の完全隠蔽と LAN 側影響ゼロ化 78
第 7 章　保守・運用サポート 80
7-1. 保守・運用サポートの基本方針と契約境界の定義 80
7-1-1.「別途契約事項の明示」による曖昧さの排除 80
①従来の契約における課題と認識齟齬の防止 80
②明示的リスト方式によるサポート範囲の適正化（包括的保守契約） 80
7-1-2. 新規参入リスク費用の抑制（実績頻度データの開示方針） 80
①包括的保守契約に伴う参入障壁および価格高騰リスクの解消 80
②依頼実績および頻度データの開示 80
7-1-3. 保守体制とオンサイト・リモートハイブリッド運用要件 81
①完全リモート保守の禁止とオンサイト要件の維持 81
②オンサイトとリモートを組み合わせたハイブリッド運用の確立 81
7-2. 通常契約に含まれる保守・運用サポート範囲 81
7-2-1. システム・インフラ管理および設定変更作業 81
7-2-2. システム保守・パッチ適用・適宜チューニング 82
7-2-3. 障害対応および予防保全（SLA 要件） 82
7-2-4. 主要機器のメーカー保守要件（構築 1 年＋運用 6 年） 82
①「計 7 年間」のメーカー保守体制の確保 82
②運用途中のサポート終了（EOL）の排除 83
7-2-5. エンドポイント（端末）管理・保守および修理手配 83
①ソフトウェア保守および年度更新 83
②物理保守および修理手配（オンサイト対応） 83
③過失破損時の動産保険活用 84

④Microsoft 365（M365）ライセンス対応 84
7-2-6. 運用管理・月次定例会（SLA・課題管理） 84
7-3.【参考情報】日常運用における本市からの依頼作業実績と想定頻度 85
7-3-1. 本市依頼作業の性質と提示の目的 85
①本市依頼作業（SE 対応依頼）の定義 85
②実績データの開示目的と効果 85
7-3-2. 想定作業内容と年間実績頻度データ 85
①主な個別依頼作業項目と想定発生頻度 85
②SLA およびインセンティブ評価との連携 87
7-4. 別途契約（当初契約対象外）とする要件と実績事例 87
7-4-1. 過去に別途契約として実施した環境変更実績 87
①過去の別途契約事例提示の趣旨 87
②主な過去の別途契約実績事例 87
7-4-2. 次期契約において明確に「別途契約」と規定する要件 88
①別途契約となる明確な区分基準の定義 88
②別途契約対象となる具体要件 88

第 1 章　グランドデザインの概要と構成

1-1. 本グランドデザインの目的と基本理念

1-1-1. 策定背景と次期 12 年(6 年+6 年)の基本コンセプト

①境界型防御の限界と「ZTNA ハイブリッド β モデル」への進化

本市では、令和 14 年 1 月に予定している、次期 12 年（前期 6 年・後期 6 年）を見据えた庁内 ICT インフラ基盤の刷新にあたり、従来の「内部ネットワークは安全である」という前提に立った境界型防御（α'モデル）からの脱却を図る。近年、クラウドサービスの普及や LGWAN-ASP の高度化、多様な働き方の進展に伴い、物理的な境界のみに依存したセキュリティ体系は限界を迎えており、特定通信の許可の繰り返しは、ネットワーク構造を複雑化させ、セキュリティの形骸化を招くリスクとなっている。

これに対し本市では、電子証明書に基づく IEEE 802.1X 認証や IP ソースガード（IPSG)、DHCP スヌーピング等の動的なネットワークアクセス制御（庁内 LAN ゼロトラスト）と、仮想デスクトップ（VDI）を高度に融合させた「ZTNA ハイブリッド β モデル」を確立する。端末の属性やセキュリティを「常に検証し、決して信頼しない」原則を適用しつつ、インターネット系と LGWAN 系を安全に架け渡すことで、高度なセキュリティと職員の業務利便性・ロケーションフリーな働き方を効率的に両立させる。

②財政的持続性と安全性の両立

市場におけるソフトウェアのサブスクリプション化や価格高騰、半導体不足や為替変動に伴うハードウェア調達コストの増大は、自治体の財政運営において深刻なリスク要因となっている。

次期 ICT インフラ基盤においては、特定の大手メーカーの製品の価格設定やライセンス形態に追従せざるを得ない構造的リスク（ベンダーロックイン）を可能な限り排除する。汎用・独立系ハードウェアの積極活用やオープンソースソフトウェア（OSS）の選択肢を獲得し、健全な競争環境を形成することで、変化の激しい社会情勢下であってもコストの最適化(TCO の抑制）とシステムの安全・安定稼働を持続的に達成する ICT インフラ戦略を展開する。

1-1-2. ドキュメント体系と役割

①本グランドデザインのドキュメント構成

本グランドデザインは、次期 ICT インフラ基盤の全体像と調達・運用の方針を提示する包括的ドキュメントであり、「本章」および各専門領域を定義した個別技術編（「ネットワーク」「仮想基盤」「セキュリティ・システム」「端末管理」「外部通信」「保守・運用サポート」）を各章として構成される。

②本章が果たす 2 つの核心的役割

全体を統括する本章は、以下の 2 つの役割を担う。

【各章の個別技術編の横断的統合・サマリー機能】

「ネットワーク」「仮想基盤」「セキュリティ・システム」「端末管理」「外部通信」「保守・運用サポート」として詳細に記述する各専門領域の基本的事項・設計思想の核心部分を横断的に集約・可視化する。これにより、仕様を検討する者や検討ベンダーが個別技術の詳細情報の概要をスムーズに理解でき、ICT インフラの全体像とアーキテクチャ相互の連動性を容易に把握することを可能とする。

【全体共通方針および調達・運用管理の枠組みの定義】

特定の技術や製品に縛られない、システム全体に共通する重要なポイントとして、「本市が直面する主要課題に対する解決のアプローチ」「12 年（6 年+6 年）を見据えた分割契約・プロポーザル等の調達戦略」「PoC 結果の公開と選定評価・契約要件」「長期運用スケジュール」「SLA および運用評価制度」など、調達・契約およびプロジェクト全体の共通ルールと評価基準を定義する。

1-2. 本市が直面する主要課題と解決アプローチ

1-2-1. 現行 ICT インフラ基盤の構成規模

本市が直面する構造的課題と解決アプローチを検討する前提として、現行 ICT インフラ基盤（第 1 期）の主要な構成規模を以下に示す。

これら大規模なハードウェア群および仮想デスクトップ（VDI）、セキュリティ等を安定的に稼働・維持していくためには、アーキテクチャを刷新し特定製品の価格変動リスクを排除し、持続可能で柔軟な調達構造へ転換することが不可欠となっている。

【機器の内訳】

機器区分	項　　目	現在の数量
サーバ	セキュリティ用仮想基盤ホスト	4 台
	VDI 用仮想基盤ホスト	14 台
	管理用物理サーバ	1 台
ストレージ	仮想基盤用ストレージ	2 台
	庁内バックアップ用ストレージ	1 台
	遠隔地バックアップ用ストレージ	1 台

機器区分	項　　目	現在の数量
仮想デスクトップ	業務用 VDI（個人番号利用系）	331 台
	業務用 VDI（LGWAN 系）	151 台
	個人用 VDI	1075 台
仮想サーバ	各種業務システム・管理用等	130 台
FAT 端末	個人番号利用系 PC	37 台
	LGWAN 系 PC	78 台
	インターネット系 PC	35 台
	デジタル戦略課用 BTO	8 台
	テレワーク・リモート用 PC	15 台
	リモート保守用	1 台
シンクライアント端末	番号利用系（二要素認証あり）	312 台
	LGWAN 系	634 台
ネットワーク機器	UTM	2 台
	コアスイッチ	2 台
	その他マシン室内スイッチ	7 台
	フロアスイッチ・L2 スイッチ	24 台
	その他小規模なスイッチ・FW 機器	9 台
	出先機関ルーター	34 台
	無線 LAN 用 AP	32 台
	無線 LAN 用 PoE	7 台
プリンタ	モノクロレーザー	121 台
	モノクロレーザー（中速機）	1 台

【各フロア・出先機関等】

建物区分	フロア数・箇所数	備　　考
本庁舎	3 フロア	部署毎にセグメントを分割し、5 つに分割
議会棟	2 フロア	本庁舎 2 階と同一セグメント
分館	2 フロア	建物全体で 1 セグメント
東別館	2 フロア	建物全体で 1 セグメント
西別館	4 フロア	建物全体で 1 セグメント
出先機関	28 カ所	建物ごとに 1 セグメント

【回線帯域と数量】

本庁舎・水道局・アビスタ・クリーンセンター・水の館・保健センター・消防本部については 100Mbps（ギャランティ）の広域イーサで接続している。

なお、本庁舎については、RAG2 回線による 200Mbps である。
その他の出先機関 22 カ所は、10Mbps（ギャランティ）である。
回線については、調達には含めないものとする。

1-2-2. 三層分離と ZTNA を融合した「ハイブリッド型ネットワーク」の構築/第 2 章

① 完全 ZTNA における構造的リスクと業務継続性の確保

すべての通信制御をクラウド型セキュリティや単一の認証基盤へ全面的に委ねる「完全な ZTNA（Zero Trust Network Access）」への移行は、自治体インフラにおいて極めて深刻な単一障害点（SPOF）リスクを内包する。万が一、中核となる認証サーバ等が停止した場合、庁内すべてのネットワーク通信が遮断され、全業務が停止する事態を招く。

特に、SASE（Secure Access Service Edge）等のパブリッククラウド基盤に全面的に依存した ZTNA 構成では、本庁舎のインターネット回線障害のみならず、過去に発生したような世界規模の主要なクラウド事業者や CDN サービスの障害が発生した際、認証そのものが通過しなくなり、庁内オンプレミスシステムや LGWAN-ASP を含めたあらゆる業務へのアクセスが不可能となる。

また、本市のような職員 1,500 人規模のネットワーク環境においては、トラフィック制御や帯域管理、影響範囲の限定化の観点から、適切なセグメントの分離（VLAN・VRF による論理分離）は不可欠である。

したがって、ZTNA へ全面的に寄せてしまう設計は自治体の業務継続性の観点から非常にリスクが高い。「庁内 ZTNA」と「三層分離（境界防御）」を高度に融合させた本市のハイブリッド構成であれば、万が一 ZTNA 認証基盤やクラウド側で深刻な障害が発生した場合であっても、一時的にネットワーク側の認証処理をバイパス（不要化）する非常時運用へ切り替えることで、三層分離による論理セグメントのセキュリティ隔離を維持したまま通信を継続させ、市役所機能の全停止を回避することができる。

②高度なネットワーク構成の実現（三層分離×庁内 ZTNA）

総務省のセキュリティガイドラインに準拠した「三層分離（番号利用系・LGWAN 系・インターネット系）」による高度な機密性を維持しつつ、現代の多様な働き方やクラウド利用に対応するため、動的なアクセス制御技術を組み合わせた高度な「ハイブリッド型ネットワーク」を構築する。

端末の電子証明書に基づく IEEE 802.1X 認証（D-VLAN）や IP ソースガード（IPSG）、DHCP スヌーピング等の厳格な認証・制御メカニズムを実装し、物理ポートの制約がないロケーションフリーな環境を実現する。さらに、VDI 基盤と連動した「ZTNA ハイブリッド β モデル（10 セグメント分離）」により、各セグメント間を論理的に完全分離することで、万が一のマルウェア侵入時にも横断移動をブロックする、堅牢かつ柔軟な「庁内

ZTNA（ゼロトラスト)」を完成させる。

1-2-3. サプライチェーン･リスク対策とハードウェア調達方法の見直し/第 3 章

①2026 年のサーバ価格異常高騰の教訓と特定メーカー依存の脱却

2026 年に顕在化した世界的な半導体およびパソコン、サーバの異常な価格高騰は、特定の大手メーカーに依存した ICT インフラ調達モデルの脆弱性を浮き彫りにした。従来のように世界シェア上位の大手ブランドメーカー（DELL、HP 等）のみに機器選定を固定化する手法は、メーカー側の価格改定やサプライチェーンの目詰まりによる納期遅延、予算の大幅超過のリスクをダイレクトに受ける構造となっている。

第 2 期 ICT インフラ基盤においては、この教訓を生かし、特定のメーカーに依存しない柔軟なハードウェア調達構造へと変換する。

②大手メーカーの許容と特定メーカー依存の排除

本市の方針は、DELL や HP 等の大手メーカー製ハードウェアの採用を一切排除するものではない。提案時（前期契約時）において価格が安定しており、経済性、信頼性、および性能の観点から総合的に妥当であると判断される場合には、これらのメーカーを採用した構成の提案は可能である。しかし、特定のメーカー製品しか取り扱い・提案ができない事業者、あるいは代替構成の選択肢を持たない事業者については、将来的なリスク回避の観点から本 ICT インフラにおける受託者として採用しない方針とする。

③後期契約時の価格高騰に対応できるマルチベンダー切替体制の必須化

前期契約において大手メーカーを採用してスタートした場合であっても、受託者は後期契約に向けて、市場の動向に応じ他の優れたメーカー(第 3 のメーカー等）を選定・切り替えできる技術的体制および調達ノウハウを保持していなければならない。

6 年後の後期契約（更新・継続）のタイミングにおいて、大手メーカー製品が再び価格高騰を起こした際、他社メーカーへの切り替えができずに高騰した製品を使わざるを得ない事態は絶対に回避する必要がある。当初提案で大手メーカーを採用する場合であっても、後期契約の締結時点までには、市場第 3 位以下のコストパフォーマンスに優れた独立系・汎用メーカー（Supermicro 等）を柔軟に選定・調達・運用できる体制を確立できることを、本 ICT インフラ調達における必須の評価・適応要件として定義する。

④ベンダーに求める先回り提案力と適応力

単に提示された仕様どおりに機器を導入するだけでなく、将来的な市場変動や価格高騰に対し、受託者が主体的にリスクを回避できる機動力を要

件とする。

具体的には、市場動向を常時予測し、「採用メーカーが高騰した際、更新時に他社メーカーへと構成変更を行う代替プランの事前準備」や「供給状況に応じた先回りした構成変更提案」を柔軟かつ迅速に行える技術力と提案ノウハウを備えた事業者を選定する。

1-2-4. 仮想化ソフトウェア価格高騰への対抗策と OSS 活用原則/第 3 章

①大手メーカーのハイパーバイザへの依存からの脱却

現行 ICT インフラで採用されている VMware をはじめ、主要な仮想化ソフトウェア関連の市場では、ライセンス体系のサブスクリプション化に伴う著しい価格高騰やライセンス体系の変更が相次いでいる。これにより、製品を継続利用すること自体が、コストにおける重大なリスクと負担になっている。

第 2 期 ICT インフラ基盤においては、既存製品（VMware）の継続利用を前提とせず、また代替案の選択肢が特定製品（Nutanix）のみに固定化し、コスト削減効果が薄れる事態を回避する。この課題に対応するために必要なことは、OSS(オープンソースソフトウェア)の活用と選択肢を持つことであり、脱ベンダーロックインを進め、中長期的なトータルコストの増大を構造的に抑制する。

②Proxmox VE および Accops による本市 PoC 結果の公表

高価なソフトウェア依存からの脱却を具体化するため、本市では独自に OSS である「Proxmox VE」およびコストパフォーマンスに優れた VDI 基盤「Accops」を用いた概念実証（PoC）を実施する。

本 PoC において検証された機能性・安定性・運用性に関する技術的知見やデータは、調達前に広く公開する。これにより、高価な大手パッケージ製品に頼らず、オープンで費用対効果に優れる技術を活用した選択肢のある提案を事業者から積極的に募る環境を整える。

③提案者自身のナレッジ・独自検証要件

OSS 等の新しい技術を活用した柔軟かつ経済的な提案を広く歓迎する一方で、システム構築・運用の確実性を担保するため、提案者に対するナレッジ・実績要件を厳格に定義する。

【本市 PoC の扱い】

本市が公開する PoC 結果を参照・参考にすること自体は一切制限しない。

（令和 10 年 4 月、令和 11 年 4 月の 2 回に分けて公開予定）

【独自検証・導入実績の義務付け】

本市の PoC 結果のみを根拠とし、提案者に技術的ノウハウや検証実績がない状態での提案は不可とする。提案にあたっては、提案者自身や協業する企業が独自に技術検証（PoC）を行っていること、または官公庁・地方公共団体・国内企業等において該当技術の導入・構築・運用保守の実績を有していることを要件として明確化する。

1-3. 各章の個別技術のアーキテクチャ・サマリー

1-3-1. ネットワーク（アクセス制御、証明書認証、ネットワーク分離）/第 2 章

①電子証明書認証に基づく庁内 ZTNA の確立と主要拠点への Wi-Fi 導入

本市の次期ネットワークアーキテクチャにおいては、従来の「内部ネットワークは安全である」という境界型防御の思想を完全に排し、アクセス元を常時検証・制御する「庁内 ZTNA」を構築する。

本庁舎周辺および主要な出先機関に対しては、庁内無線 LAN（Wi-Fi）の導入を戦略的に推進し、電子証明書認証（EAP-TLS 等）と組み合わせた強固なアクセス制御基盤を確立する。

有線・無線のすべてのアクセスポイントにおいて、正規の証明書を保持しない未許可デバイスは接続を拒否するとともに、認証に成功した端末に対しては、認証サーバ（RADIUS）とネットワーク機器が連動して属性に応じた VLAN ID を動的に割り当てる「ダイナミック VLAN（D-VLAN)」を実装する。これにより、庁内のどのフロア・会議室から接続しても、自動的に必要なセグメントへ繋がるロケーションフリーな環境を実現する。

②島 HUB 混在環境に対する強固な複合防御（IPSG・定期再認証）

小規模出先機関等の有線 LAN 環境において、D-VLAN が前提とする「1 物理ポート＝1 端末」の原則が適用できない島 HUB（アンマネージドスイッチ）の混在環境に対しては、未許可端末の共連れや「なりすまし」による不正侵入を防ぐ複合的な防御を適用する。

エッジスイッチ側において、電子証明書認証と連動した IP ソースガード（IPSG）や DHCP スヌーピング等の機能を有効化し、正規の認証を経て払い出された「MAC アドレス＋IP アドレス」のペアのみを動的ホワイトリストとして保持・許可する。これにより、固定 IP アドレスの直打ちによる不正アクセスを物理破棄し、さらにバックグラウンドでの定期的な再認証により、端末切断後の偽装割り込みを即座に検知・遮断する運用を徹底する。

③ZTNA ハイブリッド β モデルによる 10 セグメント論理分離

総務省が推進する「βモデル」の基本骨格（Chromebook 等からの直接インターネット利用および画面転送による LGWAN 利用）をベースとしつつ、庁内 ZTNA および三層分離の高度なセキュリティ要件を融合させた本市独

自の「ZTNA ハイブリッド β モデル」を採用する。
本モデルにおいては、ネットワーク全体を役割とセキュリティレベルに応じた以下の「10 のセグメント」に細分化して論理分離する。

【分離対象セグメント】
○インターネット系
○プリンタ系
○番号利用系
○LGWAN 系
○サーバ・管理系
○シンクラ LG 系（LGWAN 系 VDI のみに接続する）
○シンクラ MN 系（LGWAN 系 VDI および番号利用系 VDI に接続）
○LGWAN 系 VDI
○MN 系 VDI（番号利用系 VDI）
○IP 電話系

各セグメント間は、VRF（Virtual Routing and Forwarding）によってルーティングテーブル自体を独立させ、最上位 UTM のアクセス制御リスト（ACL）によってセグメント間の通信を厳格に制御する。物理端末セグメントから VDI 環境（画面転送プロトコル）を経由せずに重要セグメントへアクセスする、横断通信を構造的に遮断し、万が一マルウェアに感染した場合でも被害の拡大を局所内に封じ込める。

1-3-2. 仮想基盤（3Tier・マルチ OS 対応 VDI・脱ベンダーロックイン）/第 3 章

①3Tier アーキテクチャの維持と既存高機能ストレージ資産の活用

次期仮想基盤の設計においては、特定のソフトウェアのライセンス体系変更や価格高騰リスクに対抗する「脱ベンダーロックイン」および「中長期的な TCO（総保有コスト）の最適化」を最優先方針とする。
近年トレンドとなっている HCI（ハイパーコンバージドインフラ）構成は、計算リソースとストレージ領域が一体化しているため、いずれか一方のリソース不足した場合でもユニット毎増強する不要な買い増しが発生しやすく、中長期のコスト制御が困難となる課題がある。このため、本市ではホストサーバと外部ストレージを独立させた従来の「3Tier アーキテクチャ」を維持する。
ホストサーバには汎用・独立系サーバ製品を導入しつつ、ストレージ基盤には本市が保有する Everpure 社（旧 Pure Storage 社の Evergreen サブスクリプション）の継続利用を視野に入れる。これにより、新規ハードウェア調達費用を大幅に圧縮するとともに、将来のベンダー交代時においてもストレージとサーバを個別に最適に調達できる柔軟性を担保する。

②マルチ OS 対応 VDI 接続管理基盤の採用

仮想デスクトップ（VDI）環境の管理基盤（セッションブローカー）については、従来の製品（Horizon）に依存する構成から脱却を図り、他の製品の選択肢を持つ。

選定にあたっては、接続元の OS を限定しない「マルチプラットフォーム（マルチ OS）対応」を必須条件とする。Windows ベースのシンクライアント端末のみならず、軽量かつ安価な ChromeOS（Chromebook）からの接続を一元的に制御・識別できる接続管理基盤を採用することで、将来的な端末構成の汎用化・低価格化に適応できる仮想基盤環境を確立する。

③目的別 VDI 基盤の区分と最適化

職員が利用する総数約 1,700 台規模の VDI 環境については、リソース消費特性およびセキュリティ要件に応じて「2 つの区分」を設ける。

【職員個人用 VDI（約 1,200 台)】

全職員の日常的な事務処理・文書作成等を担う環境であり、ストレージ容量の消費を大幅に抑制しパッチ適用の一括化を図るため、マスターイメージを共有する「非永続型（リンククローン相当)」方式にて構築・運用する。

【業務システム用 VDI（約 500 台)】

特定の業務アプリケーションや専門ソフト等を個別に実行する環境であり、データの永続性とアプリケーションの独立性を担保するため、個別にディスクを割り当てる「永続型（フルクローン相当)」方式で構築・運用する。

1-3-3. システム(無害化・多層防御・セキュリティ連携)/第 4 章

①多段プロキシ構成と Web・ファイル無害化処理の徹底

インターネット通信における脅威の遮断と安全な Web 利用を実現するため、「Web フィルタリングプロキシ」と「セキュアブラウザ用プロキシ」を多層に配置する「多段プロキシ構成」を構築する。

すべての Web アクセスは、Active Directory（AD）と連携したプロキシ認証を受け、ユーザー単位の行動ログを漏れなく保持するとともに、暗号化通信内部に潜む脅威を検知する「SSL デコード検査」を原則適用する。その上で、セキュアブラウザプロキシを通じて Web ページのソースコード（HTML/CSS/JavaScript 等）をサーバ側で要素分解・再構築し、画面転送形式で描画する「Web ページ無害化」を実行することで、未知の脆弱性を突いたブラウザ攻撃を無力化する。

また、Web 経由でファイルをダウンロードする際は、セキュアブラウザと連動した「サニタイズ（ファイル無害化)」を行い、Office ファイル内のマクロや画像に埋め込まれた不正コード等のリスク因子を剥離・除去し、安全なファイルのみを庁内へ取り込む。本無害化機能においては、原本ファイルからの感染リスクを根本排除するため、原本保持・引き出し機能は不要とし、原本の取得が必要な業務は、インターネット系 FAT 端末に限定する運用とする。

②メールセキュリティと上長承認ワークフロー

庁内で受信する外部メールに対しては、スパム・標的型攻撃フィルタリングに加え、HTML メールのプレーンテキスト化および添付ファイルの自動削除を行う「メール無害化」を適用し、内部ネットワーク環境へ悪意あるプログラムが到達することを構造的に防ぐ。

一方、外部へのメール送信に際しては、誤送信による情報漏洩を防ぐ自動変換（複数外部アドレスの強制 BCC 化等）および再確認ダイアログを適用する。さらに、ファイルを添付した外部宛メールの送信時には、システム上で所属長（管理職）による確認・許可を必須条件とし、人為的ミスや不正なデータ持ち出しを水際で防ぐ。

③エンドポイント防護（EPP+EDR)と境界型自動暗号化

端末管理・セキュリティの高度化として、個体識別情報（VID および PID 等）に基づき許可された指定デバイス以外の接続を物理拒否する「登録制外部デバイス制御」を実装する。また PC のログイン/ログアウト確定時刻を勤怠管理システムと連動させる打刻収集機能を実装する。

ファイル持ち出し制御においては、庁内ネットワーク内でのファイル運用を平文として業務利便性を保ちつつ、信頼された領域からファイルを移動するタイミングで自動的に暗号化を施す「境界型自動暗号化」を採用する。持ち出し承認フローを経ずに取り出したデータは閲覧不能となり、信頼領域内では、暗号化による運用負荷をかけずに強固な漏洩防止策を確立する。

エンドポイントセキュリティの核としては、既知のマルウェアをブロックする「EPP（Endpoint Protection Platform)」に加え、侵入後の不審な挙動をリアルタイムに検知・追跡する「EDR（Endpoint Detection and Response)」を組み合わせる。ゼロデイ攻撃等の侵入を検知した際は、該当端末をネットワークから自動的に論理隔離し、侵入経路・被害範囲をログから可視化・特定を可能とする体制を構築する。

④身体特性・運用リスクを考慮した二要素認証選定

マイナンバー等の特定個人情報を取り扱う「番号利用系セグメント」へ

のログイン時に義務付けられる二要素認証（多要素認証）については、職員の身体特性や季節的要因による失敗リスクを排除するための選定基準を定義する。

冬季の乾燥や手荒れ、多汗症等により読み取りエラーが多発し業務遅延を招く「指紋認証」方式は、採用対象から明確に除外する。代わりに、マスク・眼鏡着用時にもスムーズな「高精度顔認証」、皮膚表面の状態に影響を受けない「静脈認証（手のひら・指）」、あるいはパターン記憶等を活用した「トークンレス認証（画面上完了型）」を二要素認証の方式として定義する。なお、スマートフォン等を利用した BYOD(私有端末の業務利用）による認証コード送信方式は、情報セキュリティ方針の観点から不許可とする。

1-3-4. 端末管理（ハイブリッド端末戦略・統合 AD・M365 最適化）/第 5 章

①コストとセキュリティを両立するハイブリッド端末配置戦略

本市におけるクライアント端末配置においては、一律の単一 OS 運用ではなく、業務特性・セキュリティ要件・コストパフォーマンスに応じた「ハイブリッド端末戦略」を展開する。

【一般事務用「Chromebook（シンクラ LG 系：640 台）」】

一般事務処理、Web 会議、SaaS 利用、および VDI 経由の LGWAN 業務を担う標準機として配備する。安価なハードウェアコストと効率的なクラウド管理を行い、総保有コスト（TCO）の圧縮を図る。なお、提案者が Windows 端末を選定すること排除するものではない。（Windows による提案も可）

【番号利用事務用「Windows（シンクラ MN 系：330 台）」】

二要素認証デバイスのドライバ適合性が要求される番号利用系セグメント接続用に「Windows シンクライアント（シンクラ MN 系：330 台）」を配置する。

インターネット接続が必要な Chromebook から番号利用系への接続は、認められないため。Windows のシンクライアントに限定する。

なお、将来的に ChromeOS 上で二要素認証が完全に動作・成立した段階で、すべてのシンクライアント端末を Chromebook へ一元化できるよう、柔軟な拡張性を保持した設計とする。

【専用業務用「Windows（FAT：140 台）」】

専用周辺機器の使用やローカルでの特殊処理が必要な特定業務（LGWAN 系 90 台、番号利用系 30 台、インターネット系 20 台）に対し、「Windows FAT 端末（計 140 台）」を必要な部署にのみ配備する。なお、LGWAN 系 FAT は、個人用 VDI へと接続するシンクラ LG 系としても利用可能とする。

②Active Directory（AD）統合 2 ドメイン構成と運用自動化（SSOT）

Active Directory（AD）は、独立性が求められる「番号利用系ドメイン」と、一元管理を行う「LGWAN 系・インターネット系統合ドメイン」の 2 ドメイン構成とする。

AD 内に保持する所属・役職情報を「唯一の信頼できる情報源（SSOT：Single Source of Truth）」として定義し、人事異動時には AD の属性更新のみで以下の運用が自動で追随する仕組みを確立する。

【アクセス権限の自動同期】

ファイルサーバの部署別共有フォルダ権限の自動切替・消去。

【外部連携の自動同期】

グループウェアや各種業務システムに対する LDAP/SAML 連携経由でのユーザー情報の自動更新や SSO への対応を行う。

【動的プリンタ割り当て】

ログオン時のスクリプト実行による、異動先部署近接の最適論理プリンタの自動セットアップ。

③Chrome Enterprise Upgrade（CEU）によるデバイスの集中管理

Chromebook を導入する場合は、「Chrome Enterprise Upgrade（CEU）」を管理基盤として必須化し、Google 管理コンソールから全端末の一元管理を行う。

工場出荷状態の端末をネットワークへ接続するのみで設定を完了させる「ゼロタッチ・キッティング」、USB 接続制限やブラウザセキュリティ等の「一括ポリシー適用」、万が一の端末紛失・盗難時に外部からのデータ流出を物理遮断する「リモートロックおよびリモートワイプ」をクラウド上で一括運用する。

④Microsoft 365（M365）ライセンスの全体最適化（約 1,600 アカウント）

全職員（VDI・物理端末利用を含む約 1,600 アカウント）が使用する「Microsoft 365」ライセンスについて、現行プラン（Apps for enterprise）の更新にとどまらない、必要かつ適切なライセンスの提案を求める。

調達・評価プロセスにおいて、専用グループウェア（メール、スケジュール等）を廃止して M365 機能へ集約する場合の費用対効果や、M365 の上位ライセンスプラン（E3/E5 等）を採用することで、サードパーティ製の ID 管理・資産管理・セキュリティツール群を標準機能へ統合・代替できるか、提案による評価を実施し、全体の支出を最も抑制できるライセンス体

系を選定する。

1-3-5. 外部通信（公的接続・LBO・マルチベンダー保守）/第 6 章

①公的クラウド基盤（セキュリティクラウド・ガバメントクラウド）への接続

本市から外部へ向かう通信においては、セキュリティレベルおよび通信目的に応じ、以下のとおり接続ルートを使い分けて運用する。

【千葉県情報セキュリティクラウド】

一般的なインターネット接続（Web 閲覧・メール等）については、市役所からセキュリティクラウドまでを専用線（閉域網）で接続し、セキュリティクラウド側で高度なセキュリティ対策を一括適用した上で外部インターネットへ接続する。

【ガバメントクラウド（LGWAN 経由・非インターネット）】

標準化業務システムが稼働するガバメントクラウドへのアクセスは、LGWAN 接続回線を経由して接続する。

【高速光回線（フレッツ 光クロス／OCN）を活用した最適化 LBO】

セキュリティクラウドへのトラフィック集中による通信遅延や、暗号化デコード等の相性問題により正常に表示・利用できない特定 Web サイトの課題に対処するため、市側の高速光回線（フレッツ 光クロス／OCN）から直接インターネットへ接続（LBO）させる迂回ルートを適用する。

具体的には、M365 認証通信、Google 関連通信（Chromebook 用）、安全性が確認され且つ大量の通信を行うサイトおよびセキュリティクラウド経由では利用できないサイト等の通信のみを、最上位 UTM のポリシーベースルーティング（PBR）や PAC ファイルを用いてピンポイントで LBO へ誘導する。

②テレワーク基盤（専用 VM 不要・VDI 直接接続）

在宅勤務や出張先からの安全なリモートアクセス環境として、LBO 用に設置する専用 UTM や VPN 機器のアプライアンス機能を直接活用したセキュア基盤を構築する。庁外の専用 PC から接続エージェント等を用いて、市の固定グローバル IP 宛てに SSL-VPN 接続を確立し、UTM から庁内の個人用 VDI へ接続する。

仮想基盤上に専用のテレワーク用 VM（仮想マシン）を配する必要がなく、リソースおよびライセンスコストを一切消費しない。業務処理は VDI 内部で完結し、外部 PC へは暗号化された画面転送データのみが送信されるため、ローカル保存を許さない、データ持ち出し防止策を講じる。

③NGN 網内 DDNS/VPN を活用した低コスト・マルチベンダー保守基盤

本市 ICT インフラシステム群および庁内オンプレミス業務システム群に対するリモート保守を一体的に実現するため、NTT の「NGN 網内ダイナミック DNS（DDNS）機能」を活用した VPN 接続方式を構築する。

インターネットを経由せず、NGN 網内の名前解決により各保守事業者の拠点と直接暗号化 VPN を確立する。従来システム毎に個別に契約していた保守用回線を廃止し、本市が提供する 1 本の「フレッツ光クロス」回線を全保守事業者で論理共有することで、月額回線維持費を大幅に削減する。回線終端（ONU）配下に各保守事業者が用意した VPN 機器を個別配置し、最上位 UTM およびコアスイッチ側で VLAN 分離とアクセス制御（ACL）を徹底することで、他系統や他ベンダー領域への横断通信を遮断した高セキュリティなマルチベンダー保守環境を実現する。

1-3-6．保守・運用サポート（包括的サポート・ハイブリッド運用）/第 7 章

①包括的保守サポート原則（原則包含アプローチ）の導入

従来の保守契約において多発していた、軽微な設定変更や調査作業のたびに受託者から「契約範囲外につき都度見積・追加費用が必要」と主張され協議が遅延する問題を根本的に排除する。

次期保守契約においては、「明確に別途契約と規定した事項以外は、すべて原契約内の保守・運用サポート範囲に含まれる」という包括的保守契約（原則包含アプローチ）を採用する。日常運用で発生するスイッチ・UTM・AD・VDI 等のパラメータ変更、パッチ適用、障害切り分け、および各種チューニング作業をすべて追加費用なしで迅速に遂行する体制を確立する。

②保守内容・実績の事前開示と過大見積の防止

全作業を包括する契約形態においては、新規参入事業者が作業負荷を予測できず、リスク費用の過剰積算やプロポーザル辞退を招く事態が想定され、これを防止する。

本市では、現状の契約おいて受託者へ依頼した SE 対応作業（VLAN 作成、UTM ルール追加、PAC ファイル修正、例外設定等）の具体的な内容および年間発生頻度の状況を調達資料上で事前に開示する。これにより、参入ベンダーが客観的な根拠に基づく適正な価格積算を行える環境を整え、特定のベンダーが有利とならない透明で公正な競争環境を実現する。

③オンサイトとリモートを融合させたハイブリッド保守体制

保守体制においては、迅速な障害対応、物理トラブル解決、各種設定の確認・変更、および市の情報管理部門との確実な意思疎通を担保するため、リモートのみの保守体制を不許可とする。

運用期間を通じて「最低でも週 1 日以上のオンサイト（市役所庁舎への

来庁）訪問保守」を必須要件とする。定期来庁日には現場での保守対応を重点実施し、非来庁日には暗号化された閉域網経由のセキュアなリモートアクセスを活用して監視や日常設定変更を行う、高品質とコスト効率を両立した「ハイブリッド保守運用」を要件とする。

④月次保守定例会によるガバナンスと運用管理

オンサイト・リモート保守作業とは別に、定期的な管理・合意形成の場として、受託者と本市による「月次保守定例会」を開催する。

月次保守定例会においては、受託者から以下の報告および協議を行い、システム全体の健全性維持と課題の早期解決を図る。なお、定例会についてはペーパーレスおよびオンライン会議等の効率的な手段の活用し、終了後は受託者が速やかに議事録を作成して発注者との合意形成を図るものとする。

【リソース・ログ稼働状況報告】

CPU・メモリ・ストレージの利用実績、ならびにセキュリティログ等の分析結果の提示。

【イベントスケジュール確認】

予定されている機器メンテナンス、機能更新、および全庁的なイベントスケジュールの共有。

【課題管理（タスク管理)】

発生している運用上の課題、設定変更リクエスト、および障害復旧プロセス等の進捗管理。

【SLA 実績確認】

達成されたサービスレベルの評価ポイントの客観的検証と運用改善に向けた協議。

1-4. 調達・選定評価・契約方式

1-4-1. 前・後期合計 12 年間の提案・分割契約モデル

①評価・競争範囲(12 年間)

庁内 ICT インフラの調達・受託者選定(プロポーザル公募)においては、前期 6 年間および後期 6 年間の計 12 年間を通じた、トータル的なシステム構成・運用提案および費用積算により評価・選定を実施する。評価においては、12 年間の総額および総合提案の内容を評価対象とすることで、提案者間の健全な競争を促し、最良の提案を行う受託者を特定する。

②前期・後期の積算手法

提案における費用積算は、前期と後期でそれぞれ以下の考え方に基づき実施させる。

【前期（6 年間)】

実際の設計・構築・移行および稼働を前提とした、具体的かつ確定的なシステム構成と実用価格に基づき積算する。

【後期（6 年間)】

機器やライセンスの市場価格変動およびライセンス携帯は予測困難であるため、プロポーザル提案時点の構成および単価をベースとした現時点価格にて積算する。

③契約形式（前期のみ締結と随意契約の位置づけ）

実際の契約締結手続および履行管理においては、以下のとおり分割した契約を行う。

【当初契約（前期 6 年間)】

契約締結時は、まず「前期 6 年間(令和 14 年 1 月～令和 19 年 12 月末)」の事業を対象とした契約を締結する。

【後期契約の更新要件】

後期着手前（令和 18 年度中）において、前期における受託者の履行成績（SLA 達成状況等）が良好であり、かつ社会情勢の大幅な変動や本市の基本方針における著しい変更がない場合に限り、前期契約事業者と継続して後期（6 年間）の契約を締結する。

【随意契約手続の位置づけ】

本手続における後期の随意契約の締結は、特定の 1 社と競争せずに随意契約を行うものではない。公募段階（最初のプロポーザル）において、全期間（12 年間）を評価対象として公正に特定された受託者との間で手続を進める「プロポーザル選定結果に基づく随意契約手続の後半部分」という正当な理由と位置づけおよび解釈のもとで実施する。

1-4-2. 全体調達・事業工程

本 ICT インフラ基盤の調達・構築および運用に関する全体工程は、以下の計画を想定する。

時　期	実施項目 マイルストーン	概要・詳細
令和 8 年度 後期	本グランドデザイン公開	意見募集を実施（個別回答は行わず、必要に応じ随時改定）
令和 8 年度 後期～令和 10 年度末	PoC（概念実証）の実施	Proxmox VE、Accops 等を用いた仮想化・VDI の技術検証
令和 10 年 4 月	PoC 結果公表（中間報告）	技術検証の中間実績を外部へ広く公開
令和 10 年 4 月～6 月	第 1 回 RFI（情報提供依頼）	技術動向、構成案、概算費用に関する第 1 次市場調査
令和 11 年 4 月	PoC 結果公表（最終報告）	最終的な検証結果・構成要件を外部公表
令和 11 年 4 月～6 月	第２回 RFI（情報提供依頼）	仕様の精緻化および最終積算に向けた第 2 次市場調査
令和 11 年 10 月～12 月	RFC（コメント募集）	プロポーザル仕様書（案）を公開し、事業者からの意見を募集
令和 11 年 11 月	事業費積算期限	予算要求に向けた最終的な事業費用の要求
令和 12 年 3 月	予算成立	議会承認および次期 ICT インフラ予算の成立
令和 12 年 4 月～6 月	プロポーザル公募（募集期間 3 ヶ月）	提案募集の開始。十分な検討期間（3 ヶ月）を確保
令和 12 年 7 月	受託候補者選定	プレゼンテーション・審査による最優秀提案者の決定
令和 12 年 7 月～中期	契約協議	費用・契約条件に関する細部要件の確定協議
令和 12 年 中期	前期契約締結	前期（6 年分）の契約締結
令和 12 年 中期～令和 13 年末	設計・構築・移行期間	詳細設計、機器調達、環境構築、データ移行、事前リハーサル、端末展開
令和 14 年 1 月	運用開始（前期本稼働）	前期 ICT インフラ基盤の運用開始(～令和 19 年 12 月末)
令和 18 年 4 月	前期履行成績評価および後期契約の決定	前期事業における受託者の履行成績および後期契約に向けた方針決定
令和 18 年 4 月～7 月	後期契約要件の調整および事業費確定	社会情勢・技術動向の確認、機器構成の見直し(価格高騰時における第 3 のメーカー選定等の協議を含む)、および後期契約金額の確定。

時　期	実施項目 マイルストーン	概要・詳細
令和 18 年 9 月	9 月議会補正予算	予算要求
令和 18 年 10 月	後期契約締結	後期（6 年分）の契約締結
令和 18 年 11 月～令和 19 年 12 月	後期構成の詳細設計・機器調達・構築・移行	後期向け機器の調達、環境構築、データ移行、事前リハーサル等の移行作業期間
令和 19 年 12 月末	前期契約の満了	前期運用期間の完了および機器切り替え
令和 20 年 1 月	後期運用開始	後期（6 年分：～令和 25 年 12 月末）の運用開始
令和 25 年 12 月末	後期契約の満了	全期運用期間の完了

1-4-3. 契約関連規定および付属書の扱い

①契約付属書の規定

本調達において、本市が提示した「プロポーザル調達仕様書」、「プロポーザル質疑回答書」、受託者が提出した「提案書」、「選定時のデモンストレーションの議事録」、選定後の契約協議過程において作成された「協議議事録」は、すべて本契約書の不可分の付属書として扱う。

これら付属書に記載された機能要件、運用条件、支援体制、および協議決定事項は、契約本文と同等の法的拘束力を有するものとし、発注者および受託者はこれらを完全に履行する義務を負う。

②解釈および適用における優先順位

契約の履行過程において、契約本文および各付属書間の記述に相違、食い違い、または解釈の矛盾が生じた場合は、以下の優先順位に従い解釈・適用を行う。

(1) 契約書（仕様書を含む）
(2) 受託者特定後の契約協議議事録
(3) プロポーザル質疑回答書および選定時デモンストレーション議事録
(4) プロポーザル仕様書および提案書

1-4-4. 契約満了時の機器取扱い・データ消去規定

①ハードウェア無償譲渡および市資産化選択権

契約期間満了時において、本 ICT インフラ基盤を構成する物理ハードウェア機器群については、受託者から本市への無償譲渡を可能とする規定を調達仕様に設ける。

本市は、満了時における機器の老朽化状況、保守継続性、および再利用の要否を精査し、必要と判断した機器のみを選択的に本市の公有財産（資産）へ組み替える権利を有する。これにより、運用の継続性確保や既存資産の有効活用における柔軟な選択肢を保持する。

②不要機器の安全な廃棄とデータ破壊における分担体制

契約満了に伴い本市への譲渡を行わず不要となった機器については、受託者の責任および費用負担において、関係法令に則り安全かつ適正に廃棄処分を行うものとする。

廃棄に際して生じる記憶媒体（HDD、SSD 等）内のデータ破壊処理作業については、情報漏洩リスクを構造的に排除するため、以下のとおり本市と受託者における役割分担を定義する。

【受託者の役割（主体作業）】

対象機器からの記憶媒体の取り外し、データ消去・破壊作業の実施、および破砕証明書等の提出を含む一連の処分手続を主導・実施する。

【本市の役割（物理的協力）】

データセキュリティの確実性を高めるため、可能な範囲で物理的な作業協力を分担・実施する（例：受託者が機器から取り外した HDD 等に対し、本市が破砕・破壊処理を直接執り行う等）。

1-5. 成果連動型 SLA（サービスレベル合意）と運用評価

1-5-1. SLA の導入目的

①安定稼働の確保と継続的運用改善の促進

本 ICT インフラ基盤における SLA（Service Level Agreement）の導入目的は、受託者に対するペナルティの付与や契約金額の「減額・清算」そのものを主目的とするものではない。

本制度の根幹は、システムの安定稼働を最優先事項として確保しつつ、日々の運用現場で生じる課題の早期解決やシステム品質の自主的・継続的な改善活動を受託者側から積極的に引き出し、動機付けするための評価システムとして運用することにある。本市と受託者が双方で合意したサービス水準を客観的に評価・可視化し、高い運用品質を維持するためのインセンティブ構造として本制度を位置付ける。

②受託者提案型 SLA 方式による価格転嫁の防止

SLA の設計にあたっては、発注者（本市）側から画一的かつ厳格な数値要件を一方的に提示・強制する方式は採用しない。受託者が SLA の未達成リスクを過度に懸念し、そのリスク費用を提案価格に転嫁させる事態を構

造的に防止するためである。

プロポーザル段階においては、本市から SLA に関する基本概念、現状の SLA、および評価の考え方（概要）を示すにとどめ、具体的な管理項目、達成基準値、および評価ポイントの考え方については、提案者のノウハウに基づく主体的な提案を求める。最終的な SLA（サービスレベル合意書）の確定および正式な合意については、プロポーザル選定後の契約締結時、または契約締結後の協議において、受託者と本市との間で十分な調整を行った上で合意する方式とする。

1-5-2. ペナルティポイントとインセンティブポイントの相殺評価

①障害・品質低下に伴うペナルティポイント

システム障害の発生時の業務影響度や復旧所要時間等をはじめ、アプリケーション品質の低下、レスポンス遅延等の不具合に対し、あらかじめ定義された評価基準に基づき「ペナルティポイント」を課す。障害の発生そのもののみならず、初動対応の遅れや二次障害の誘発等も評価対象とし、運用の緊張感を維持する。

②改善・課題解決に伴うインセンティブポイント

一方で、本市からの個別 SE 対応依頼に対する迅速かつ正確な遂行実績や、システムの安定稼働・効率化に向けた自主的な運用改善提案、トラブルの未然防止策（予防保全）、ならびに本市の業務課題解決に著しく寄与した取組に対し、「インセンティブポイント」を積極的に付与する。

③ポイントの相殺メカニズムと運用貢献度の定量的評価

月次および期末の保守定例会において、該当期間内に累積されたペナルティポイントとインセンティブポイントを合算（相殺）評価する仕組みを導入する。

相殺後の評価ポイントに基づき、受託者の総合的な運用貢献度を客観的かつ定量的に算定する。単なる減点主義に陥ることなく、優れた運用改善活動を正当に評価してペナルティを相殺できる構造とすることで、受託者による主体的な品質向上・改善意欲の持続を促進する。

1-5-3. 金銭的処置（減額・清算）の適用基準

①累積ペナルティに対する清算措置と緊張感のある運用維持

ポイント相殺を一定期間（年次または期末等）ごとに行い、その結果、事前に合意された基準値を超えるペナルティポイントが累積した場合には、SLA 規定に基づき、委託料の減額や清算等の金銭的措置を執行する。

本措置は単なる懲罰を目的とするものではなく、適度なインセンティブとペナルティの相反構造を機能させることで、受託者側に常時適切な緊張

感を持たせ、万が一の障害時にも迅速な復旧と再発防止策の徹底を強制する構造的なサービス品質維持メカニズムとして運用する。

②代替措置（物・作業による清算）の選択可能性と双方協議

累積したペナルティポイントに基づく清算にあたっては、金銭による清算手法のほか、受託者側の SE による追加的な稼働提供、あるいは本 ICT インフラに資する有用な機器・ライセンス等の現物提供による清算を選択できる仕組みを設ける。

ただし、本市にとって不要または運用上不適合な物品・役務をもって清算に代えることは認めないものとする。金銭による清算、現物支給、または追加作業のいずれの方法により清算を実施するかについては、一方的な決定とせず、双方協議のうえで決定する運用とする。

第 2 章　ネットワーク

2-1. ネットワーク設計の基本方針：庁内 ZTNA の構築

2-1-1. 境界型防御から「庁内ゼロトラスト」への転換

本市における次期ネットワークは、従来の「内部ネットワークは安全である」という前提に立った「境界型防御（α’モデル）」から、場所や端末を問わず「常に検証し、決して信頼しない」ことを原則とする「庁内 ZTNA（Zero Trust Network Access）」へと転換する。

近年のクラウドサービス利用の拡大や働き方の多様化により、庁舎の内外という物理的な境界線でセキュリティを担保する手法は限界を迎えている。次期 ICT インフラ基盤では、庁内 LAN そのものをゼロトラスト化し、ネットワーク接続のあり方を根本から再定義する。

2-1-2. 属性と状態に基づく厳格なアクセス制御

すべての端末に対し、その属性（端末種別、用途、証明書の種類）に応じた厳格な認証と動的なアクセス制御を適用する。

具体的には、電子証明書を用いた IEEE 802.1X 認証による接続制限を実装する。これにより、正規の証明書を持たない持ち込み PC 等の未許可デバイスによるネットワーク侵入を構造的に遮断する。また、認証結果に基づいて最適なセグメント（インターネット系、LGWAN 系、番号利用系等）を自動的に割り当てることで、情報の機密性を確保する。

2-1-3. 物理的制約の排除と柔軟なワークスタイルの両立

D-VLAN、IPSG（IP ソースガード）、DHCP スヌーピング等の技術の導入により、特定の業務を行うために特定の LAN ポートに接続しなければならないという「物理ポートの制約」を排除する。

庁内のどの場所、どのネットワークポートに接続しても、認証によって適切なネットワーク環境が自動的に構成されるため、組織改編に伴う配線工事の削減や、フリーアドレス化を強力に推進することが可能となる。これは、強固なセキュリティを維持しつつ、業務の機密性と職員の利便性を両立させるための基盤となる。

2-1-4. 可用性を重視したハイブリッド・セキュリティ

クラウド型のセキュリティ基盤である SASE（Secure Access Service Edge）の導入を検討する一方で、単一障害点（SPOF）のリスクを徹底的に排除する。

インターネット ASP 等の通信には、利用実績が多い場合 SASE を活用した高度な脅威保護の実現を検討するが、ガバメントクラウド、庁内オンプレミスシステム、および LGWAN-ASP といった基幹業務に関わる通信については、SASE を経由させない直接制御（論理分離と ACL と認証）を維持する。このハイブリッドな構成により、インターネットや SASE の障害時においても市

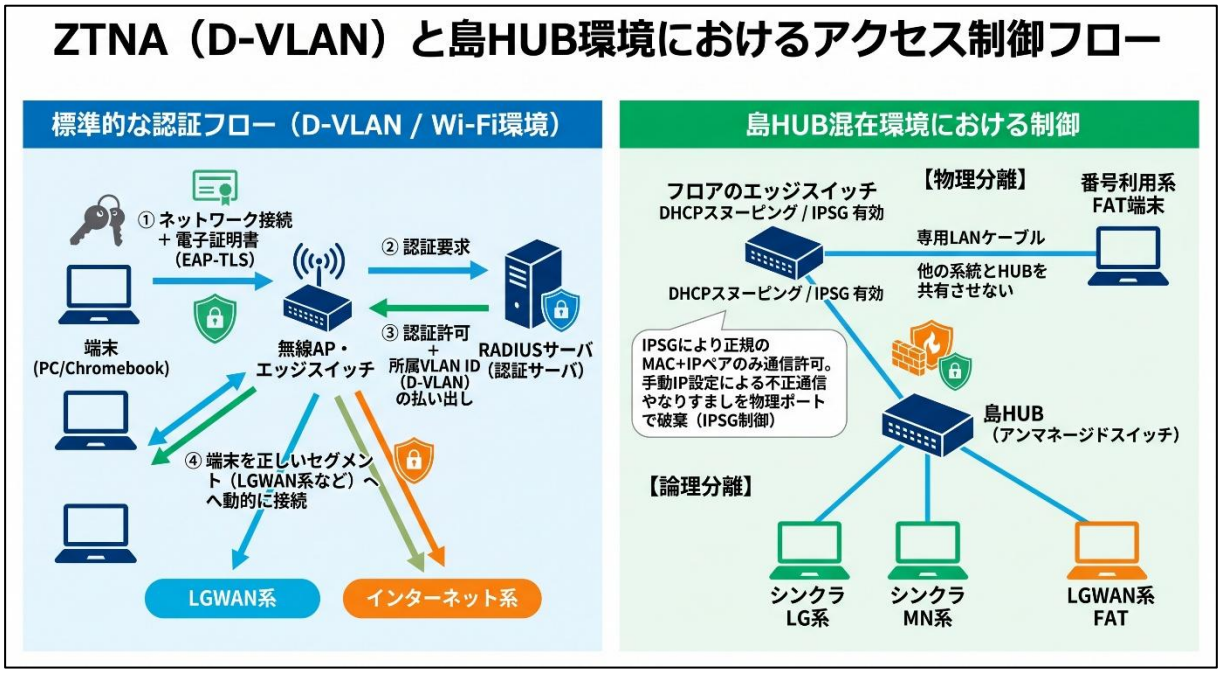
役所機能が全停止するリスクを回避し、自治体としての業務継続性を担保する。

2-2. 認証ベースのアクセス制御とネットワークセキュリティ

本節では、次期ネットワークにおけるアクセス制御の要となる「認証ベースのセキュリティ」について定義する。

原則として、すべての有線・無線 LAN 環境において電子証明書を用いた動的 VLAN（D-VLAN）による自動制御を推進するが、物理的な制約等により島 HUB（アンマネージドスイッチ）が混在する環境においても、IPSG（IP ソースガード）等を用いた論理分離と物理分離を併用し、全庁的なゼロトラスト（ZTNA）の理念を破綻させることなく実装する。

標準的な認証フローと、島 HUB 環境におけるアクセス制御の対比は以下の図のとおりである。



2-2-1. 端末認証による不正接続の構造的排除

次期ネットワーク基盤においては、物理的な LAN ポートの場所や接続ポイントに依存する従来の境界防御を廃止し、端末の認証を起点としたアクセス制御を導入する。これにより、組織内ネットワークへの物理的な侵入や、持ち込み PC 等の未許可デバイスによる不正接続を構造的に排除し、ネットワークの安全性を抜本的に強化する。正当な電子証明書を保有しないデバイス（私物 PC、スマートフォン、外部持ち込み機器等）に対しては、ネットワークへの接続そのものを拒否し、L2 レベルでの通信も許可しないことで、マルウェアの感染拡大や内部情報の窃取リスクを入口で封鎖する。

2-2-2. 電子証明書による多階層の端末識別

すべてのシンクライアント端末および FAT 端末に対し、用途に応じた電子証明書を配布して厳格なアクセス制御を実施する。

①系統に応じた証明書の付与

「インターネット系」「LGWAN 系」「番号利用系」といった各系統の属性情報を電子証明書に紐付ける。これにより、端末が「どの業務系統に属する権限を持っているか」をネットワーク接続時に動的に識別する基盤を構築する。

②端末属性管理の徹底

端末がシンクライアントか FAT 端末かといった機材種別の判別も証明書に基づき実施する。これにより、エンドポイントのセキュリティ状態や端末の役割に合わせた柔軟かつ正確なアクセス制御ポリシーの適用を可能とする。

2-2-3. D-VLAN による動的なネットワーク構成

IEEE 802.1X 認証と RADIUS サーバ（認証サーバ）を密に連携させた「ダイナミック VLAN（D-VLAN)」を実装する。

①自動的なセグメント割り当て

端末がネットワークに接続した際、認証サーバが端末内の証明書を検証する。認証成功後、その端末の権限に応じた VLAN ID がネットワーク機器（スイッチ・AP）へ即座に通知され、適切なネットワーク・セグメントへ動的に配属される。

②ロケーションフリーの実現

認証ベースでセグメントが決定されるため、庁内のどの LAN ポート、どのフロアの Wi-Fi から接続しても、職員は常に自身の業務に必要なネットワーク環境へ自動的に接続される。これは、物理的な配線管理コストの削減および庁内フリーアドレス化の基礎となる。

③アンマネージド HUB 混在環境における制御（IPSG・DHCP スヌーピング）

D-VLAN は「1 物理ポート＝1VLAN」の割り当てを基本原則とするため、フロアスイッチの配下にアンマネージド HUB（島 HUB）が接続されている場合、最初に接続・認証された端末のセグメント（VLAN ID）にスイッチポート全体（HUB 配下全体）が固定されてしまうという構造的課題が存在する。

島 HUB の配下には、異なる電子証明書やアクセス権限を持つ複数台の端

末が、同時に接続される運用が想定されるため、ポート全体が特定の VLAN に固定される D-VLAN 単体での制御方式は適用できない。

このため、島 HUB が介在し D-VLAN の適用が妥当ではない有線ネットワーク領域においては、D-VLAN ではなく DHCP スヌーピングおよび IP ソースガード（IPSG）等の技術を組み合わせたアクセス制御を採用する。具体的には、正規の認証を経て適切な IP アドレスが払い出された端末の「MAC アドレス＋IP アドレス」の組み合わせのみをスイッチのハードウェア上にホワイトリストとして動的に生成し、認証を経ない未許可デバイスの割り込みや、固定 IP 直打ちによる不正侵入を L2/L3 レベルで完全に遮断する構成とする。同様の機能は、認証サーバの機能で実現できる可能性がある。

なお、情報セキュリティポリシーが求める三層分離の原則と、庁舎内の物理的な配線制約とのバランスを考慮し、島 HUB 配下における端末の接続・混在運用ルールについては以下のとおり定義する。

【番号利用系 FAT 端末の物理分離】

特定個人情報等のデータを直接取り扱う「番号利用系 FAT 端末」については、情報漏洩リスクを極小化するため、他の業務系統と同一の島 HUB への混在接続を一切許可せず、専用の物理結線による分離を徹底する。

【シンクライアント等の混在許容と代替措置の提案要件】

一方で、「シンクライアント端末（シンクラ LG 系およびシンクラ NM 系）」および「LGWAN 系 FAT 端末」については、実務運用の制約上、同一の島 HUB 配下での混在接続を許容する。ただし、受託者は、同一 L2 セグメント内に異なる業務系統の端末が混在する状態においても、端末間での不正通信やパケット盗聴リスクを遮断するための論理的なセキュリティ対策（パーソナルファイアウォールの厳格化、エンドポイント制御等）を検討すること。

2-2-4. ネットワークが混在する場所への対応

庁舎内において多用されている既存の島 HUB（ノンインテリジェントスイッチ）環境は、D-VLAN が前提とする「1 物理ポート＝1 端末」の原則と物理的に矛盾し、同一物理空間内での未許可端末の共連れ（フリーライド）や、誰か 1 人のログアウトに伴う巻き添え切断といった運用・セキュリティ上の脆弱性を生じさせる要因となる。これに対し、機器の全面刷新を伴わない現実的な移行措置として、フロアスイッチ側で以下の複合防御アプローチ（マルチ認証モード）を実装する。

①IP ソースガード（IPSG）による固定 IP 直打ちの完全遮断

証明書認証と連動した DHCP スヌーピングを有効化し、正式に払い出された「MAC アドレスと IP アドレスのペア」のホワイトリストをスイッチのハードウェア（TCAM）上に動的生成する。これにより、認証を経ずに手動で固定 IP を直打ちして侵入を試みる未許可デバイスのパケットを、スイッチ本来の通信速度を犠牲にすることなく、物理ポートの入り口で完全に破棄する。

②定期的な再認証による「なりすまし」の構造的無力化

正規端末が島 HUB から抜去されたことをスイッチ側が検知できないという島 HUB 特有の弱点を突き、正規端末の MAC アドレスおよび IP アドレスを完全に模倣（ダブル偽装）して割り込む高度な「なりすまし」に対し、IEEE 802.1X の定期的な再認証機能を実装する。数分～十分間隔で電子証明書の提示（チャレンジ＆レスポンス）をバックグラウンドで要求することにより、物理的な入れ替わりが発生した場合でも即座に認証エラーを発生させ、ホワイトリストから偽装ペアを排除して全遮断する。

2-2-5. 未許可デバイスの完全遮断と証明書認証の導入

大量の端末が存在するフロア等において、1 ポート 1 端末の原則を実直に適用した場合、フロアスイッチの必要台数や OA フロア下の配線コストが爆発的に増大し、財政的・空間的制約に直面する。この「コストとセキュリティのジレンマ」を解決し、本市が目指す「庁内 ZTNA」を完成させるためのロードマップを以下のとおり定義する。

①本庁舎周辺および主要拠点における庁内 Wi-Fi の導入と ZTNA の高度化

フロア無線化の進展に合わせ、本市ネットワークの完成形を見据え、主要拠点におけるアクセス制御の主軸を無線セクションへ移行する。

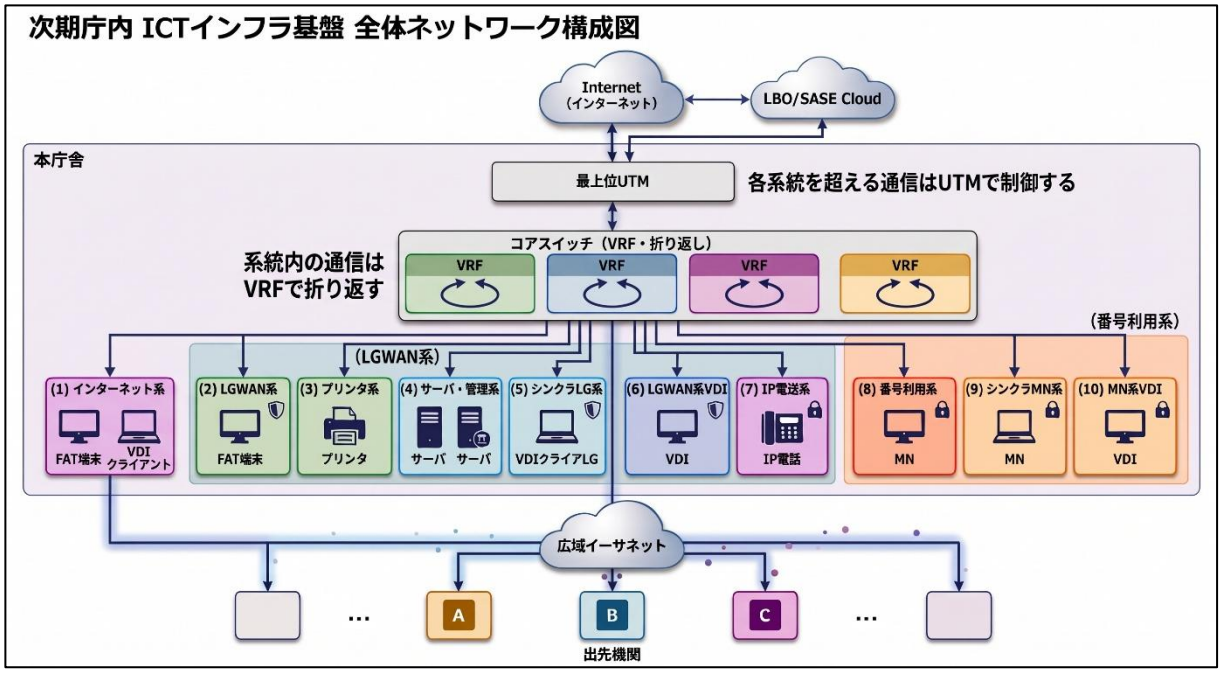
無線 AP が備える「クライアント・アイソレーション機能（端末間通信の禁止）」等により、たとえ同じ空間（SSID）に複数の端末が同居していても、電波の暗号化キーを端末ごとに個別に生成し、空間内でのパケット盗聴等を遮断する。これにより、有線 D-VLAN で必要であった「1 物理ポート＝1 端末」の縛りや、高度なエッジスイッチ設定（IPSG 等）の運用負荷からも解放され、高強度のセキュリティと柔軟なフリーアドレス環境を両立した「庁内 ZTNA」の完成形を実現する。

ただし、次期 ICT インフラにおいては費用対効果（アクセスポイントの機器費用やライセンス・保守費用の増大）を考慮し、全拠点の一律な全面無線化は求めない。導入エリアは、職員の移動や会議が頻繁に発生し機動的なアクセスが求められる「本庁舎、東別館、西別館、分館、議会棟」の本庁舎周辺エリア全域、および一定規模の出先機関を必須要件とする。

一方で、職員数が限られる小規模な出先機関については、Wi-Fi 化は行わず、既存の有線 LAN 環境（IPSG や物理分離等）の運用を継続することで、インフラ投資コストとセキュリティ要件の全体最適化を図る。

2-3. 次期ネットワークアーキテクチャ（ZTNA ハイブリッド β モデル）

本市の次期ネットワークアーキテクチャにおける全体的な論理構成、および各セグメント間のトラフィック制御経路は以下の図のとおりである。



2-3-1. ネットワーク・セグメントの定義

次期構成においては、三層分離の原則を維持しつつ、エンドポイントの多様化とセキュリティの高度化に対応するため、ネットワークの設計思想を大幅に進化させた「ZTNA ハイブリッドβモデル」を採用する。本モデルでは、端末の役割や通信要件に基づき、ネットワークを以下の 10 個のセグメントに論理分離する。

各セグメントの役割、アドレッシング体系、およびおよび接続端末の定義は下表のとおりである。

番号	セグメント名	IP 体系(例)	端末種別	主な役割･通信先
①	インターネット系	172.16.**.0/24	ChromeOS Win FAT	直接インターネット接続、原本ファイルの保持･管理
②	プリンタ系	172.23.**.0/24	プリンタ	プリンタサーバ経由での共有(各系統から印刷利用可)
③	番号利用系	172.24.**.0/24	Win FAT	地方税･住民基本台帳等の重要情報を取り扱う業務
④	LGWAN 系	172.25.**.0/24	Win FAT	LGWAN-ASP、庁内オンプレミスシステムの直接利用
⑤	サーバ･管理系	172.26.**.0/24	サーバ系	システム管理用、および特殊な用途のセグメント
⑥	シンクラ LG 系	172.27.**.0/24	ChromeOS	インターネット接続、および LGWAN 系 VDI(⑧)への接続
⑦	シンクラ MN 系	172.28.**.0/24	Win Thin	各種 VDI(⑧および⑨)への接続専用端末
⑧	LGWAN 系 VDI	172.29.**.0/22	仮想デスクトップ	個人用･業務システム用。仮想基盤内に論理的に存在
⑨	MN 系 VDI	172.30.**.0/22	仮想デスクトップ	番号利用系･ガバメントクラウド接続用。仮想基盤内に存在
⑩	IP 電話系	10.53.**.0/24	IP 電話機	クラウド PBX と通信。現状は PC と直鎖上に接続いている。

2-3-2. アドレッシング体系の特徴

本体系では、現行の設計思想を継承しつつ、第２オクテットによって用途（系統）を厳格に分離している。第３オクテットはロケーション（本庁舎フロア、出先機関、教育委員会等）を識別するために割り当てる。

特に、VDI セグメント（⑧・⑨）については、物理的な拠点とは別に、仮想基盤そのものを一つの巨大な拠点（ロケーション）と見立てた広域なサブネットマスク（/22）を適用する。これにより、将来的な VDI 台数の増大に

も柔軟に対応可能な拡張性を確保する。

2-3-3. 論理分離による安全性と独立性

各セグメントは VRF（Virtual Routing and Forwarding）によって論理的に独立しており、系統を跨ぐ通信はすべて最上位の UTM にて厳密に制御される。

特に「シンクラ LG 系（⑥）」から「LGWAN 系 VDI（⑧）」へ接続する際や、「シンクラ MN 系（⑦）」から「MN 系 VDI（⑨）」へ接続する際は、画面転送プロトコルのみを許可し、物理端末と重要データが存在する VDI 環境との間の直接的なデータ通信を遮断することで、強固なセキュリティ境界を構築する。

2-4. 通信制御ポリシーと SASE の戦略的活用

2-4-1. SASE の導入検討（インターネット ASP）

クラウドサービスの利用拡大および多様化に対応するため、インターネット経由で利用する各種 ASP サービスを対象として、SASE（Secure Access Service Edge）の導入を検討する。しかし、これは費用対効果の観点から、一定の規模の数であり、かつ重要なシステムをインターネット上のクラウドサービスで運用する場合に検討するものである。

①導入の目的

本市が推進するロケーションフリーな働き方（テレワークや出先機関での業務等）において、庁外からのリモートアクセス時にも、庁内と同等かつ一貫したセキュリティポリシーを適用することを目的とする。また、クラウドトラフィックの可視化と制御を高度化し、データ漏洩リスクの低減を図る。

②運用方針

クラウド利用の進展度合いに合わせ、トラフィックの最適化（クラウドへの直接接続等）と、サンドボックスや CASB（Cloud Access Security Broker）による高度な脅威保護をクラウド上で一元的に実現する。これにより、将来的なトラフィック増大に伴う庁内ネットワーク機器の負荷増大を抑制する。

2-4-2. 単一障害点（SPOF）の回避と可用性の確保

SASE をはじめとするクラウド型セキュリティ基盤は、極めて利便性が高い一方、その障害が全業務の停止を招く「単一障害点（SPOF）」となるリスクを孕んでいる。

本市では、自治体としての業務継続性を最優先事項とし、以下のとおり

「SASE を通さない通信」を明確に定義する。

①SASE 適用外とする重要基盤（対象外サービス）

a. ガバメントクラウド：住民情報や基幹系業務が稼働する最重要基盤。
b. 庁内オンプレミスシステム：庁内のサーバ上で動作する業務システム。
c. LGWAN-ASP：LGWAN を通じて提供される行政専用サービス。

②制御手法とレジリエンスの確保

これらの重要通信については、SASE を経由させない直接制御を維持する。具体的には、物理的なネットワーク分離をベースとした従来の VRF（仮想ルーティング）および、最上位 UTM による厳密な ACL（アクセス制御リスト）に基づいた直接通信ルートを固定する。

このハイブリッドな制御方針により、万が一クラウド上の SASE 基盤に大規模な障害が発生した場合でも、住民情報の処理や LGWAN 連携といった市役所の核心的な業務機能が全停止する事態を回避する。利便性と安全性のバランスを保ちつつ、いかなる状況下でも市民サービスを継続できる堅牢なインフラを構築する。

2-5. ネットワーク運用の高度化

2-5-1. QoS 制御の徹底による通信品質の担保

音声通信（IP-PBX）および仮想デスクトップ（VDI）の画面転送トラフィックは、遅延やパケットロスに対して極めて敏感であり、これらが業務継続性に直結する。次期ネットワークでは、物理回線を共有する多様なトラフィックに対し、高度な QoS（Quality of Service）制御を適用し、通信品質の最適化を図る。

①優先制御の実装

音声パケットおよび VDI の画面転送パケットを最優先クラスとして定義し、L2 スイッチの CoS（Class of Service）および L3 ルータの DSCP（Differentiated Services Code Point）等を用いて、ネットワーク全域で一貫した優先制御を実施する。

②帯域不足時のパケロス防止

特に本庁舎と各出先機関を結ぶ拠点間回線において、大容量ファイルの転送等による突発的なトラフィック増大が発生した場合でも、音声の途切れや VDI の操作遅延を招かないよう、キューイングアルゴリズムを最適化し、重要通信の帯域を動的に確保する。

2-5-2. セグメント間の完全分離と横断通信の遮断

本構想の核心である「ZTNA ハイブリッドβモデル」を成立させるため、仮想デスクトップ（VDI）セグメントと物理端末セグメントの間には、論理的な用途の共通性に関わらず、厳格なルーティング分離を適用する。

①用途別分離の徹底

「LGWAN 系 VDI（⑧）」と「物理 LGWAN 系（④）」、および「MN 系 VDI（⑨）」と「物理番号利用系（③）」は、それぞれ取り扱う情報の性質は同一であるが、ルーティング上は全く別の系統として定義する。

②VDI を経由しないアクセスの遮断

「シンクラ LG 系（⑥）」や「シンクラ MN 系（⑦）」のエンドポイント端末から、VDI を介さずに物理端末セグメント（④・③）へ直接通信を行う「横断通信」を、コアスイッチおよび UTM のフィルタリングによって完全に遮断する。

③セキュリティ境界の維持

この分離により、エンドポイント端末が万が一マルウェアに感染した場合でも、攻撃者が VDI という「画面の壁」を越えて庁内中核ネットワーク（オンプレミスサーバや重要端末群）へ直接侵入することを構造的に防止する。

2-5-3. ネットワークの可視化と動的な運用管理

D-VLAN および ZTNA の導入に伴い、ネットワークの状態をリアルタイムで可視化する管理体制を構築する。

①認証ログとトラフィックの相関分析

「誰が」「どの端末で」「どのセグメントに」接続しているかを認証ログによって常時把握し、異常な通信パターンや未許可デバイスの接続試行を即座に検知する。

②運用負荷の軽減

物理的な構成変更を伴わないソフトウェアイメージベースの管理（SDN 的機能）を導入することで、人事異動や組織改編に伴うネットワーク設定変更の工数を大幅に削減し、迅速かつ低コストの運用を実現する。

第 3 章　仮想基盤

3-1. 仮想基盤設計の基本方針：脱ベンダーロックインとコストの最適化

3-1-1. 仮想化市場の構造変化と財政的リスクへの対応

本市の次期 ICT インフラ基盤における仮想基盤の基本方針の策定にあたり、最も重視すべきは「財政的な持続可能性」である。

近年の情報システム市場においては、主要な商用仮想化ソフトウェアのライセンス体系が永続ライセンスからサブスクリプション方式へと急激に移行し、運用コストの大幅な高騰を招き、今後も価格高騰のリスクが顕在化している。さらに、為替レートの変動に伴うハードウェア調達価格の上昇や、世界的な半導体供給不足に起因する製品価格の高騰リスクなど、外部要因による予算圧迫の不確実性は常に存在している。

このような背景から、従来の「特定の特定メーカーが提供する商用製品」に依存し続けるインフラ設計は、本市の財政運営において極めて高いリスクとなる。次期基盤では、これまでの設計思想を抜本的に見直し、特定メーカーへの依存（ベンダーロックイン）を排除した柔軟なアーキテクチャへの転換を図る。

3-1-2. オープンソースおよび新興ベンダーの戦略的活用

コスト高騰リスクへの具体的な対抗策として、オープンソースソフトウェア（OSS）やコストパフォーマンスに優れた新興ベンダーの技術を戦略的に組み合わせる。

商用パッケージ製品が提供する多機能・高付加価値な機能の中から、本市の業務実態において本当に必要な要件を厳格に見極め、過剰な機能への投資を削減する。ライセンス費用そのものを極小化、あるいは固定化できるソフトウェアを選定することで、中長期的な総保有コストの最適化を最優先で追求する。

3-1-3. 調達における競争性の確保と機器選定の裁量権

次期 ICT インフラへの移行にあたっては、保守期限の満了に伴い、ホストサーバ等のハードウェア基盤を全面的かつ一斉に刷新する。現行契約のすべてが更新対象となるため、機器の段階的な更新やスライド移行を前提としない、完全な新規調達として設計を行う。

この一斉刷新においてコストを抑制するためには、特定のメーカーや特定のシステムインテグレーターに依存しない「競争性の高い調達環境」の構築が不可欠である。特定のメーカーに縛られない標準的かつ汎用的なハードウェア・ソフトウェア構成を採用することで、入札におけるベンダー間の競争を促し、調達コストの最適化を図る。

また、現在稼働している高性能なストレージ機器(Everpure)については、投資抑制の観点から、可能な限り継続利用することを基本とする。ただし、

選定の結果によって受託者が変更となる状況を想定する。そのため、既存資産の継続利用を絶対条件とせず、受託者の交代時にはストレージも含めた一括刷新にも柔軟に対応できるよう、システムの独立性と互換性を担保した設計を進める。

3-2. 次期ハイパーバイザおよび仮想デスクトップ管理基盤の選定

3-2-1. ハイパーバイザ選定における調達リスクと経済性の評価

①商用製品の調達リスク排除

現在使用している VMware は、ライセンス体系の急激な変更やそれに伴う利用コストの著しい高騰、さらには特定のリセラーによる提供条件や販売経路の制限などが顕在化している。これにより、自治体が中長期にわたって安定かつ合理的な価格で調達を継続することが極めて困難な状況にある。

本市においては、財政的な持続可能性および調達の安定性を最優先とするため、次期 ICT インフラ基盤の設計にあたり、VMware の導入は原則として想定しない方針とする。

②総保有コスト（TCO）の最適化要件

その他のハイパーバイザ（Nutanix、Hyper-V 等）の導入については、一律に排除するものではなく、調達における想定の範囲内とする。しかし、これらの製品についても、将来的なライセンスのサブスクリプション化の進展や、特定のハードウェアとソフトウェアの互換性の強制などにより、中長期的な総保有コスト（TCO）が想定を超えて増大する懸念が常に存在する。

したがって、VMware 以外の製品を選定対象とする場合には、初期構築費用のみならず、将来の更新時や運用保守を含めた 6 年、12 年スパンでの総保有コストが本市の財政状況に合致し、コスト高騰のリスクを限りなく低く抑えることが必須の条件となる。

③オープンソースソフトウェア（OSS）の戦略的志向

本市が直面するコスト高騰のリスクを根本的に回避し、予算の最適化を図るための有力な選択肢として、「オープンソースソフトウェア（OSS）をベースとした仮想化技術」の活用を強く想定する。

OSS をベースとしたアーキテクチャは、ライセンス費用そのものを極小化できるだけでなく、特定のメーカーに依存しない柔軟なシステム構成を可能にする。ただし、特定の製品名を仕様書等に明記することは、公募調達における公平性および競争性を損なう恐れがある。そのため、実際の調達にあたっては特定の製品を指定せず、あくまで「汎用かつオープンな技術体系を備え、特定の商用ライセンスに依存しない仮想化環境」という機

能要件として定義し、広く事業者からの提案を可能とする環境を整える。

④技術的信頼性の担保と提案資格要件

OSS の活用を具現化するにあたっては、机上の検討にとどまらず、本市の業務要件や既存 ICT インフラとの親和性を事前に深く検証することが不可欠である。そのため、本市は独自に概念実証（PoC：Proof of Concept）を実施し、機能面、性能面、および運用面における実現可能性を評価する。なお、この PoC によって得られた知見や検証結果については、調達の透明性を高めるため、広く外部に公開する予定である。

本調達において、事業者が提案できるシステム構成および製品は、技術的な安定性と確実な保守体制を担保するため、次のいずれかの条件を満たすものに限定する。

【本市検証済み製品とサポート体制の保有】

本市が実施した PoC において検証対象となった製品であり、かつ、当該製品の構築および運用保守サポートに関する十分なノウハウと体制を有していること。

【官公庁への導入実績とサポート体制の保有】

他の官公庁（国または地方公共団体等）において、一定の導入・稼働実績がある製品であり、かつ、当該製品の構築および運用保守サポートに関する十分なノウハウと体制を有していること。

※上記のいずれの場合においても、提案者単独での対応に限らず、再委託先や外部の専門組織を含めた「協力ベンダー体制」によって十分なサポート品質が実証できる場合は、これを認めるものとする。

3-2-2. 仮想デスクトップ（VDI）接続管理基盤に求められる機能要件

①特定商用製品からの脱却

現行の仮想デスクトップ環境において利用している管理基盤（VMware および Horizon）に依存した構成を全面的に見直し、中長期的な財政負担を大幅に軽減する。ライセンス費用および運用保守コストの双方において、コストパフォーマンスに極めて優れた代替製品・技術の選定を最優先で進める。

なお、ハイパーバイザの選定方針と同様に、特定の代替製品名を仕様書等に明記することは調達の公平性を欠くため行わない。あくまで本市が求める機能要件を基準とし、広くベンダーから最適かつ経済的な提案を募る方針とする。

②エンドポイントのマルチ OS 対応（必須要件）

本市の次期端末においては、従来の Windows ベースのシンクライアント端末にとどまらず、ライセンス費用やハードウェア調達コストが安価であり、かつ運用管理が軽量な「ChromeOS」の活用を検討する。

このエンドポイント戦略を具現化するため、仮想デスクトップ（VDI）接続管理基盤（セッションブローカ等）の選定にあたっては、Windows 環境のみに依存・限定される製品の導入は不可とする。

接続管理基盤の必須要件として、接続元となるエンドポイント端末が Windows であるか、あるいは ChromeOS であるかを問わず、それら複数の OS 環境を一元的に制御・識別し、目的の VDI へと接続できる「マルチプラットフォーム対応能力」を有していることを絶対条件として定義する。これにより、将来的な端末の汎用化・低価格化に柔軟に対応できるインフラ基盤を確立する。

③接続管理基盤における技術的信頼性の担保と提案資格要件

マルチ OS 環境における仮想デスクトップへの接続管理基盤の導入にあたっては、クライアント端末（Windows、ChromeOS 等）との親和性や各種認証基盤との連携における確実性を事前に検証することが不可欠である。そのため、本市は独自に PoC を実施し、異種 OS 混在環境下での動作安定性および運用性の実現可能性を評価する。この検証結果については、広く外部に公開する予定である。

本調達において、ベンダーが提案できる接続管理基盤製品およびその体制は、安定稼働と確実な保守サポートを担保するため、次のいずれかの条件を満たすものに限定する。

【本市検証済み製品とサポート体制の保有】

本市が実施した PoC において、マルチ OS 接続検証の対象となった製品であり、かつ、当該製品の構築および運用保守サポートに関する十分なノウハウと体制を有していること。

【官公庁への導入実績とサポート体制の保有】

他の官公庁（国または地方公共団体等）において、マルチ OS 環境、あるいは一定規模以上の仮想デスクトップ接続管理としての導入・稼働実績がある製品であり、かつ、当該製品の構築および運用保守サポートに関する十分なノウハウと体制を有していること。

※上記のいずれの場合においても、ベンダー単独での対応に限らず、再委託先や外部の専門組織を含めた「協力ベンダー体制」によって十分なサポート品質が実証できる場合は、これを認めるものとする。

3-2-3. 代替方式「リモート PC アレイ」の検証

これまで本章では、ハイパーバイザ（仮想化ソフトウェア）上で展開する標準的な VDI（仮想デスクトップ）基盤の選定や脱ベンダーロックインについて記述してきた。しかし、商用ハイパーバイザのライセンス高騰リスクを根本から回避する「ハイパーバイザフリー」の選択肢として、従来の仮想化とは毛色の異なる物理集約型ソリューションである「リモート PC アレイ」についても、検討の土台に上る手法の一つとして技術的・設備的検証を行う。

①リモート PC アレイの基本仕組み

リモート PC アレイは、1 台の専用筐体内に 20～30 台程度の超小型物理 PC 基板（カートリッジ）を高密度に搭載したハードウェア製品である。

ハイパーバイザによる仮想化処理を行わず、職員は接続管理基盤（VDI セッションブローカー）を介して、筐体内の個々の物理 PC へリモートデスクトップ接続を行う。全職員分の物理 PC を個別配置するのではなく、同時接続数を考慮した必要最小限の台数をアレイとして配備し、共有リソースとして制御する仕組みである。ハイパーバイザのライセンス料が発生しないため、ソフトウェア単体の調達費用を大きく抑えられる可能性がある。

②集約率の低さに伴う筐体数の膨大化

一見すると費用対効果が高く見える本方式であるが、導入にあたっては「集約率の低さ」という構造的課題に注意が必要である。

ハイパーバイザを用いた現在の本市 VDI 基盤では、1 台（1U）の高性能物理サーバ上に 100 台以上の仮想マシンを集約しており、全体で 14 台の物理サーバで運用している。これに対し、リモート PC アレイは 1 台あたり 20～30 台程度しか物理 PC を集約できない。仮に本市の VDI 環境（総数約 1,700 台規模）の全量をリモート PC アレイへ置き換えた場合、必要な機器台数は約 57 台～85 台にまで跳ね上がることになる。

③ファシリティ面の限界（電源・ラック・工事コスト）

機器台数が 57～85 台規模に膨らむことで、庁舎内サーバ室の物理的ファシリティ（設備環境）の限界を超える。

【電源容量と UPS の不足】

リモート PC アレイは 1 台あたり最大で 600W 弱の電力を消費する。数十台を一斉稼働させる場合、既存の電源容量を大幅に超過するため、分電盤からの新たな電源回路の引き込み工事が不可欠となる。また、停電時に稼働を維持する無停電電源装置（UPS）の容量も不足するため、UPS の増設が必要となる。

【物理スペースと工事費用】

機器を収容するためのサーバラックが新たに 2 本必要となり、設置工事や配線処理、

スペースの確保、空調設計の見直しも含めた大掛かりな工事が発生する。

④全量移行の困難性と部分的導入の現実的妥当性

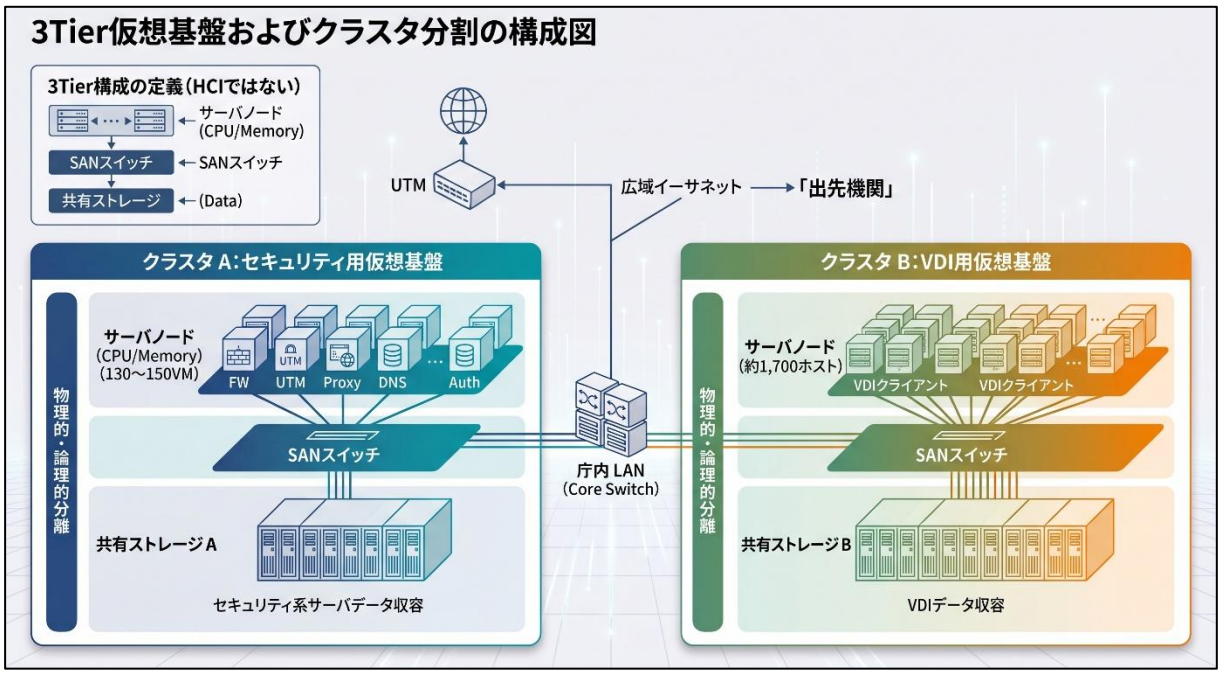
検証の結果、リモート PC アレイはソフトウェアライセンス費用を削減できる一方で、全量導入を図った場合は集約率の悪さに起因する「ファシリティ構築・改修費用」が膨れ上がり、かえって全体コストを悪化させるリスクが高い。

したがって、本市の全 1,700 台規模の VDI 基盤をすべてリモート PC アレイに置き換えることは、技術的・設備的な観点から非常に難易度が高いと判断せざるを得ない。本方式を活用する場合、例えば特定業務に特化した「業務用 VDI（約 500 台規模）」などの一部環境へ局所的に適用するに留めることが、コスト抑制とファシリティ制約の双方を成立させる現実解となる可能性がある。

3-3. ハードウェア選定およびクラスタ構成（3Tier アーキテクチャ）

次期仮想基盤においては、拡張性と保守性の観点から HCI ではなく「3Tier 構成（サーバノード＋SAN スイッチ＋共有ストレージ）」を採用する。また、高セキュリティ領域のサーバ群を収容する「セキュリティ用仮想基盤（クラスタ A）」と、全庁の約 1,700 ホストにおよぶデスクトップ環境を収容する「VDI 用仮想基盤（クラスタ B）」の 2 つのクラスタに物理的・論理的に分割し、リソース競合を防いだ分離設計とする。

本基盤における 3Tier 構成およびクラスタ分割の全体像は以下の図のとおりである。



3-3-1. 特定メーカーに依存しないホストマシン選定

①経済情勢に伴う調達価格高騰への対策

ハードウェア市場における需給逼迫や経済情勢の変動に起因するサー

バ製品の価格高騰リスクは、ICT インフラ構築における大きな財政的懸念事項である。従来のように、世界的なシェアを占める特定の大手ブランドメーカー製サーバに固定して調達を進める手法は、メーカー側の価格政策やサプライチェーンの状況に大きな影響を受けやすく、大幅な予算の超過を招くリスクがある。

②汎用・独立系サーバの視野投入とロックインの打破

次期 ICT インフラにおいては、特定のメーカーに固定した調達（ベンダーロックイン）を排除する。同等のプロセッサやメモリ、アーキテクチャを搭載し、同等の性能・信頼性を担保できるのであれば、コストパフォーマンスに優れた国内外の独立系メーカーの汎用サーバも広く選定視野に含める。これにより、ハードウェアの調達コストそのものを大幅に抑制し、市場の価格高騰リスクを最小限に抑える。

3-3-2. クラスタ構成の定義（2 つの仮想基盤）

ホストサーバ群は、システムの重要度、セキュリティ要件、およびリソースの消費特性を考慮し、「セキュリティ用仮想基盤」と「VDI 用仮想基盤」の 2 つの独立したクラスタに分離して構成する。

①セキュリティ用仮想基盤（約 130～150 台規模）

本クラスタは、庁内 ICT インフラの根幹を支えるセキュリティシステムやネットワーク監視、システム・インフラ用の管理サーバを統合収容する。さらに、庁内で利用する内部事務系の業務システムなどの仮想マシン群も包括的に集約する。

運用規模としては、現行の約 130 台の稼働実績を踏まえ、次期運用期間中の拡張性を見据えた 130～150 台規模の仮想マシンを安定稼働させる性能を確保する。

②VDI 用仮想基盤（総数約 1,700 台規模）

職員が日々の業務で利用する仮想デスクトップ環境を収容するクラスタであり、総数約 1,700 台規模の VDI を想定する。本基盤内は、運用の目的とコスト効率を最適化するため、次の 2 系統に分けて管理する。

なお、個人用 VDI と LGWAN 系の業務システム用 VDI は、共に LGWAN 系であり、同一のユーザー名でログインするため、ユーザーに紐づくプロファイル環境（従来の移動プロファイル、または第 5 章「5-2-3」にて検討する FSLogix 等のプロファイルコンテナ方式）は共通のものを使用する。

【職員個人用 VDI（約 1,200 台）】

主に一般的な事務処理やブラウザ、事務用ソフトを利用する。ストレー

ジ容量の消費を徹底的に抑え、パッチ当てや管理の効率性を最優先とするため、マスターイメージを共有する「リンククローン（または非永続型）」に相当する方式を採用する。

【業務システム用 VDI（約 500 台）】
特定の基幹業務システムや個別システムを使用する業務に利用する。データとソフトウェアの独立性と永続性を担保するため、個々に独立したディスク領域を割り当てる「フルクローン（または永続型）」方式で構築する。

3-3-3. 3Tier 構成の維持と既存資産の継続利用に関する方針

①HCI 構成の不採用と 3Tier アーキテクチャの維持

昨今のトレンドである HCI（ハイパーコンバージドインフラ）構成は、計算リソース（CPU/メモリ）とストレージリソースが一体化しているため、いずれか一方が不足した場合でもユニットごと買い増す必要があり、本市のような大規模環境では中長期的なコスト最適化が難しい。そのため、次期基盤においても、計算基盤（サーバホスト）と外部ストレージ基盤を独立させた従来の「3Tier 構成」を維持する。

②既存ストレージ資産の活用とベンダー交代への備え

3Tier 構成を維持する最大のメリットは、サーバとストレージの調達を分離できる点にある。

本市では、Everpure 社（旧 Pure Storage 社）のストレージを採用しており、Evergreen Storage による保守・サブスクリプションにより、リプレースが不要なエコシステムを実現している。費用抑制の観点から、可能な限り Everpure を継続利用することを基本思想とし、新規調達コストの大規模な削減を目指す。

ただし、次期インフラの選定結果によっては、受託者が入れ替わる可能性が十分にあるため、Everpure の継続利用を絶対条件として仕様を縛ることはせず、新たな受託者への交代時にはストレージも含めた一括刷新へ柔軟に対応できるよう考慮する。

3-4. クラウド移行における構造的リスクとオンプレミスの妥当性

3-4-1. クラウドの経済的実態と試算の不確実性

①資産非保有化とトータルコストの乖離

システムをパブリッククラウドへ移行する利点として「ハードウェア資産を保有しないことによる費用の平準化」が頻繁に挙げられる。しかし、これが必ずしも中長期的なトータルコスト（TCO）の削減に直結するとは限らない。クラウドサービスは、利用期間が長期に及ぶほど累積する利用

料がオンプレミスの減価償却費を上回る可能性があり、さらにはサービスベンダー側の価格改定や為替変動リスクによるコスト増大を自治体側でコントロールできないという構造的課題を抱えている。

②隠れたコストと積算の困難さ

クラウドへの全面移行を前提とした正確なコスト積算を行うためには、サーバ費用とクラウド利用料の比較だけでなく、ICT インフラ全体を包含したネットワーク構成を念頭に置くことが不可欠である。

具体的には、クラウド環境と庁舎を安全に結ぶための専用線費用や、接続拠点の帯域拡張費用、さらには全通信をクラウド上で防御・制御するための SASE（Secure Access Service Edge）等のセキュリティライセンス費用などをすべて合算する必要がある。これらが未確定の段階では、クラウド移行による真の財政負担を見極めることは不可能である。

③従量課金制度に伴う予算管理の不確実性

多くのクラウドサービスが採用している「従量課金」は、データ転送量やストレージの I/O（入出力）回数、稼働時間など、一時的なリソース消費に応じて動的に費用が変動する。クラウド移行前にこれらの費用を積算することは、極めて困難であり、現行の仮想基盤およびネットワーク機器などに対して、特殊な方法で長期間計測し、クラウド移行後の費用の参考とする必要がある。

現状の詳細な調査により、具体的な積算ができたとしても、住民サービスや突発的な行政需要によって通信量や処理データ量が予測を超えて増大した場合、実際の月額・年額費用がどの程度まで膨らむか事前に見当をつけることは極めて困難である。また、ドル建てでなければ支払いができないサービスもあり、為替変動の影響をダイレクトに受ける。

これらの不確実性は、厳格な予算管理と定額での運用が求められる自治体の財政運営において、大きなリスク要因となる。

3-4-2. 単一障害点（SPOF）と物理回線のボトルネック

①物理回線の構造的限界と共用経路のリスク

クラウドへの依存は、本庁舎および出先機関からクラウド基盤へと至る通信回線が最大の単一障害点（SPOF）となることを意味する。

本市庁舎周辺における光ファイバー網の敷設環境を考慮すると、その多くは特定の通信事業者が管轄するダークファイバー等の物理インフラに依存せざるを得ない。そのため、信頼性を高める目的で複数の回線事業者と個別に契約を交わし、論理的なルートの冗長化を図ったとしても、最終的に同じ収容局を通過したり、同一管路を経由したりしているケースが極めて多い。これは、災害や交通事故等によって物理的な切断事故が発生し

た場合、すべての回線が同時に不通となり、冗長構成が機能しないリスクを常にはらんでいる。

②セキュリティ基盤の障害による業務全停止リスク

すべての通信や認証を SASE などのクラウド型セキュリティ基盤に依存させた場合、回線そのものが健全であっても、該当セキュリティ基盤の不具合や輻輳（アクセス集中による通信遅延）によって市役所機能が全停止する恐れがある。

過去には、大手クラウドベンダーによるネットワークの設定誤りや、世界規模の CDN・セキュリティ配信サービスの障害により、世界中で広範なシステムへの接続や認証が不可能となった実例が複数存在する。基盤の運用を完全に外部へ委ねるクラウド環境においては、こうしたベンダー側の過失や大規模障害が発生した際、自治体側で主体的な復旧手段を講じることができず、ただ復旧を待つのみとなる脆弱性がある。

3-4-3. 出戻り不能（クラウドロックイン）のリスク

①庁舎側ファシリティの喪失による再移行の困難さ

一度オンプレミス環境のすべてのシステムを廃止してクラウドへ完全移行すると、将来的にコストやセキュリティ上の理由から再度オンプレミスへ環境を戻そう（出戻り）としても、事実上不可能となるリスクが存在する。クラウド移行に伴い、庁舎内のサーバ室に備わっていた電源容量の削減、空調・冷却設備の停止、サーバラックの撤去などが行われるためである。これら一度失われたインフラファシリティを再度構築し直すには、莫大な初期投資と期間が必要となり、財政的にも物理的にもオンプレミスへの再回帰は極めて困難となる。

②データアウト課金による経済的ロックイン

自治体が保有する住民情報や各種行政データは、中長期的に膨大な量へと蓄積されていく。これらの大容量データをクラウド上に保管した場合、別のクラウドサービスへ引っ越しをする際、あるいは自庁内のサーバへとデータを書き戻す際に、クラウドからデータを外部へ搬出するための「データ転送料（データアウト課金）」が莫大な規模で発生する可能性がある。

このデータ移行コストは、実際の移行時にどれだけの費用が発生するか、事前予測が極めて困難である。この経済的なリスクにより、特定のクラウドサービスに事実上永続的に拘束される「クラウドロックイン」を引き起こす要因となる。

3-5.【比較表】オンプレミス vs クラウドのメリット・デメリット

3-5-1. 比較評価の目的

本市における次期仮想基盤の選定にあたり、意思決定層が財政、運用、およびレジリエンス（業務継続性）の観点から客観的な判断を行えるよう、「オンプレミス」と「クラウド」の特性をコスト・運用・リスクの 3 軸から比較・整理した。

3-5-2. 評価軸に基づく詳細比較

オンプレミスとクラウドの両アーキテクチャのメリットおよびデメリットの比較は下表のとおりである。

評価軸	オンプレミス	クラウド
コスト面	【メリット】 ・運用コスト（ライセンス・保守等）が固定化され、中長期の財政見通しが立ちやすい。 ・データアウト課金（データ移行費用）等の費用が発生しない。	【メリット】 ・初期のハードウェア資産購入が不要（一部の費用の平準化）。
	【デメリット】 ・構築時にハードウェアの初期調達費用が一括して発生する。（ただし、転リース、リースバック等により、平準化が可能）	【デメリット】 ・為替レートの変動や従量課金（データ転送量、I/O 数）により、月額・年額の予算変動リスクが大きい。 ・構築時から本稼働と同等の利用料が発生する。 ・利用期間が長期化するほどコストが増大する傾向がある。
運用面	【メリット】 ・機器構成、設計、メーカー選定において市側に完全な裁量権（コントロール権）がある。 ・仕様書の工夫次第で、特定のベンダーロックインを構造的に排除できる。	【メリット】 ・物理ハードウェアの保守やライフサイクル管理をクラウド事業者側に一任できる。

評価軸	オンプレミス	クラウド
	【デメリット】 ・ハードウェアの保守管理、パッチ適用、物理的な障害対応を市（または受託者）の責任ですべて実施する必要がある。	【デメリット】 ・インフラ内部の構造がブラックボックス化し、市側でのトラブルシューティングや個別カスタマイズが困難となる。 ・事業者から提示されたメニューと規約に従う以外の選択肢がない。
リスク面	【メリット】 ・外部回線が途絶した場合でも、庁内オンプレミスシステムや VDI 基盤、庁内 LAN は独立して動作を継続できる（回線断に強い）。	【メリット】 ・事業者の高度なデータセンター群により、物理的な災害に対する堅牢性が高い。
	【デメリット】 ・庁舎の被災（停電、水害等）時における物理的な事業継続対策を独自に講じる必要がある。	【デメリット】 ・庁舎周辺の物理回線断やクラウド、SASE 側の障害、輻輳が発生した際、認証やシステム接続が不可能となり、市役所機能が全停止する。 ・一度移行するとオンプレミス環境（電源・空調等）の維持が難しく、他のクラウド環境への再移行や庁内への移行（出戻り）が極めて困難（経済的、技術的ロックイン）。

3-5-3. 本市における選定の妥当性と今後の検討方針

①現時点における結論の回避と評価の慎重性

比較結果が示すとおり、オンプレミスとクラウドは、コスト・運用・リスクのいずれの面においても一長一短があり、それぞれが異なる構造的課題を内包している。したがって、現段階においていずれか一方のアーキテクチャのみを「本市にとって最善の決断」と断定することは早計であり、慎重な判断が必要である。

②RFI（情報提供依頼）を通じた定量的データの収集

クラウドの採用には、予算管理の不確実性や回線切断時の業務停止とい

った重大なリスクが存在することは確かである。しかし、これらのリスクの大きさを理由に検討の初期段階でクラウドを選択肢から排除するべきではない。

今後は、RFI（情報提供依頼）等の調達準備を通じて、クラウド環境によるインフラ構築を提案する事業者から、具体的なシステム構成や回線費用、セキュリティ対策も含めた網羅的な見積・積算データを収集する。これにより、机上の一般論ではなく、本市の固有要件に即した具体的な積算に基づき、双方のコストパフォーマンスと実現性を厳正に分析・比較する。

③表面的な一般論の排除と厳正な比較検討の重要性

次期 ICT インフラ基盤の決定において最も警戒すべきは、「クラウドは資産を持たないため安価である」といった表面的な一般論や、具体的な検証を欠いた安易なクラウド移行である。同様に、過度なリスク懸念からオンプレミスへ盲目的に固執することも回避しなければならない。

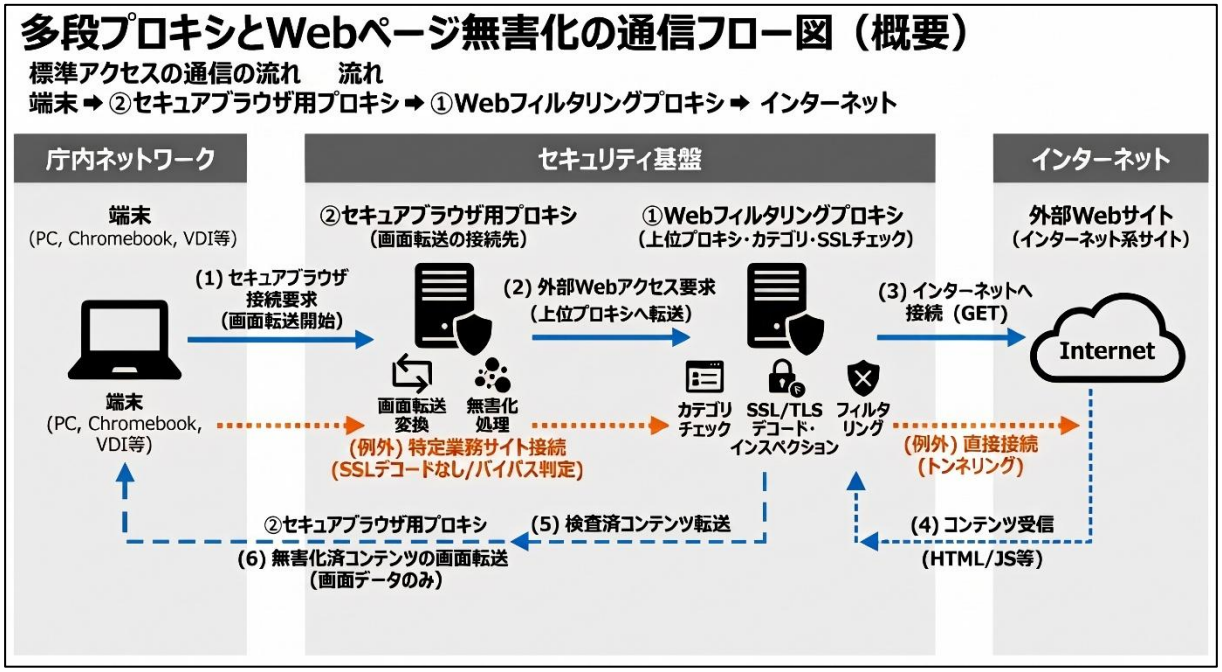
自治体としての財政的持続可能性と、いかなる災害時にも市民サービスを継続するレジリエンス（業務継続性）を両立させるためには、双方が抱える見えづらいコストや固有のリスクを完全に洗い出し、定量的に把握することが不可欠である。その上で、オンプレミスとクラウドの双方を同一の評価指標のもとでフラットに比較検討し、本市にとって真に最適なグランドデザインを最終決定していくことが重要である。

4-1. Web セキュリティおよび情報無害化基盤の構成

本節では、次期ネットワークにおける Web アクセス時のセキュリティ対策および情報無害化の仕組みについて定義する。

インターネットへの標準的なアクセスは、まず画面転送・無害化処理を担う「セキュアブラウザ用プロキシ」へ接続し、さらにカテゴリ判定や SSL/TLS の検査を担う「Web フィルタリングプロキシ」を上位プロキシとして経由する多段構成を基本とする。一方で、事前登録された特定の業務サイト等、無害化処理を経由することで業務に支障をきたす通信については、安全性を確認した上で、例外として直接通信（バイパス）を許可する。

端末からインターネットへ至る多段プロキシの標準的な通信フロー、および例外ルートの概要は以下の図のとおりである。



4-1-1. 多段プロキシによる Web フィルタリングと SSL デコード要件

①ディレクトリサービス連携による認証とログ管理

本市における Web アクセスの制御および監視は、ディレクトリサービス（Active Directory：AD）と連携したプロキシサーバを中心に行う。

職員がインターネット接続を行う際、AD に登録されたユーザー情報に基づくプロキシ認証を必須とする。これにより、匿名アクセスを排除し、Web サイトへのアクセス、ファイルアップロード、書き込み、各種 Web サービスの利用といったインターネット上のすべての行動ログをユーザー単位で確実に取得・保管する。取得したログは、情報漏洩発生時の監査ログとして機能させるだけでなく、不正な通信の早期発見と原因究明に活用する。

②細分化されたフィルタルール制御

Web フィルタリング機能においては、不正なサイトや業務に不適切なサイトへのアクセスを防止するため、「ホワイトリスト（許可リスト）」と「ブラックリスト（拒否リスト）」の双方の機能を併用したハイブリッド制御を導入する。

フィルタリングは、システムベンダーにより提供される、カテゴリに応じたポリシーを適用し、業務上不必要なサイトの閲覧を防止する。

SSL のデコードにより接続できないサイトで、安全性が確認できるものについては、ホワイトリストを適用し、確実なアクセスを保証する。一方で、必要に応じてブラックリストによるブロックを行う。さらに、サイトの種類や危険度、業務上の必要性に応じて「完全ブロック」「閲覧回数制限」などのフィルタルールを URL 単位やカテゴリ単位で細かくチューニングし、運用の実態に即した柔軟かつ厳格なルール変更を可能とする。

③SSL デコード機能と独自認証局の運用方針

インターネット上のトラフィックの大半が暗号化（HTTPS 化）されている現状を踏まえ、暗号化通信の内部に隠蔽されたマルウェアや不正なデータ持ち出しを検知するため、SSL デコード機能を原則として有効化する。

プロキシサーバが暗号化通信を一時的に復号（デコード）してコンテンツの検査を行い、再度暗号化してクライアント端末へ配送する仕組みを構築する。この機能を実現するため、プロキシサーバで生成した自己証明書を AD のグループポリシー等を通じてすべての VDI および FAT 端末へ一斉配布・自動適用する。

4-1-2. セキュアブラウザによる Web ページ無害化と例外運用

①多段プロキシ構成によるネットワーク防御

インターネットから庁内へのマルウェア侵入を防御するため、セキュアブラウザ用プロキシの外側（インターネット側）に Web フィルタリングプロキシを配置する「多段プロキシ構成」とする。

端末からのすべての Web アクセスは、まず外側に位置する Web フィルタリングプロキシによってチェックと認証を受け、許可された通信のみが内側のセキュアブラウザ用プロキシへと中継される。この多層的な防御構成により、悪意あるサイトへのアクセスを入口で遮断するとともに、無害化処理を担うセキュアブラウザ用プロキシにはフィルタリング済みの通信のみが到達するため、サーバの処理負荷を大幅に低減させる。

セキュアブラウザ用プロキシにおいては、閲覧対象の Web ページに含まれる HTML、CSS、JavaScript などのソースコードをサーバ側で一度完全に要素分解し、悪意あるスクリプト等を無効化した上で安全な形に再構築してユーザーの画面へ転送（レンダリング画面転送等）する「Web ページ無

害化」を実装する。

これにより、未知の脆弱性を突いたブラウザ攻撃やダウンロードによるマルウェア感染のリスクを構造的に排除する。なお、この無害化処理の過程において、サーバと端末間における安全な画面転送とセッション維持を行うため、Web フィルタリングサーバには、セキュアブラウザ専用の証明書を登録する必要がある。

②表示不具合への対応と例外運用の明確化

Web ページの無害化処理は極めて安全性が高い一方、高度なスクリプトを多用した最新の Web サイトや業務用 SaaS において、表示の崩れや一部機能(ボタンの反応や動的コンテンツの動作)の不全といった表示不具合、閲覧そのものができないという問題が生じる場合がある。

これらの事象により業務に著しい支障を来す特定サイトに対しては、原則インターネット専用の端末から接続するか、LGWAN 系シンクライアントの端末からの接続とする。(接続先の VDI からではなく、接続元 PC から直接閲覧)

本市で構築したサイトなど、安全性が確認できるサイトの場合、もしくは、万が一改ざんされてもサイトを直ちに停止できるなど、本市が管理できるサイトについては、無害化対象外とすることが可能である。

これら、例外運用については、情報管理部門が精査した上で、無害化処理を通さずに直接閲覧を許可する「例外設定（バイパス設定)」の運用ルールを明確に定義する。例外設定を行うとしても、すべてのセキュリティをバイパスするのではなく、可能な限り Web フィルタリングプロキシによるログ取得と SSL デコード検査などのセキュリティ対策は継続し、セキュリティレベルの局所的な低下を最小限に留める。

4-1-3．ダウンロードファイルに対するサニタイズ(ファイル無害化)

①セキュアブラウザと連動した自動サニタイズ

外部の Web サイトから庁内ネットワークへファイルをダウンロードする際のリスクを排除するため、セキュアブラウザと密に連動した「ファイル無害化（サニタイズ)」機能を統合する。

職員が Web ブラウザを通じて PDF、Microsoft Office 製品(Word、Excel、PowerPoint 等)、画像ファイル等の各種ファイルをダウンロードしようとした際、システムは自動的にそのファイルを検知し、庁内に取り込む前にサニタイズ処理を実行する。具体的には、Office ファイル内に埋め込まれたマクロ（VBA)、非可視領域のメタデータ、画像に埋め込まれた不正な埋め込みコード、実行形式のファイルなどのリスク因子を自動的に剥離・除去する。対象ファイルは、安全なデータ部分のみを抽出して新しくファイルを再生成した上で、職員の端末へのダウンロードを許可するか、リスク

のあるデータを含むファイルそのものをブロックする。

②原本保持・取り出し機能の排除による最適化

本無害化機能の設計における重要な特徴として、無害化を施す前の「原本ファイル」をシステム内に一時保存したり、後から原本を取り出したりする仕組みは、あえて不採用とする。

原本の保持および引き出し機能を実装した場合、悪意のあるファイルを直接取り込むリスクが生じるため、原本は、インターネット専用環境からのみダウンロードする方式が妥当である。

原本ファイル（無害化前データ）の取得が必要な業務については、本システムとは物理的・論理的に分離された「①インターネット系(Win FAT)」端末をスポット的に利用する運用とすることで、リスク管理と利便性の最適化を両立させる。また「⑥シンクラ LG 系(ChromeOS)」は、インターネット用 SSID に接続することで、インターネット専用端末として使用できるため(この場合 VDI へは接続不可)、これを利用することも可能である。

4-2. メールシステムおよびメールセキュリティの設計

4-2-1. 内部メールサーバの配置とアラート連携

①メール配信経路における位置付けと基本役割

内部メールサーバ（SMTP、POP、IMAP）は、全庁的なメール配送経路において最も内側（インフラ基盤内）に配置される。本サーバは、主にグループウェアのメール機能専用の受信サーバとして位置付けられ、庁内で利用するすべての個人のメールアカウントおよびメーリングリストの一元的な登録・管理を担う。

なお、本サーバはグループウェアにおける送受信の提供を主目的とするものであり、本サーバ自体にセキュリティ機能を持たない。

②システムアラート受信用ゲートウェイとしての通信要件

本サーバは、職員間の一般的なメール受信用途にとどまらず、庁内ネットワークに接続された各種業務システム、仮想化基盤上のサーバ群、スイッチやルーター等のネットワーク機器の監視システム、ならびに NAS をはじめとするストレージ製品から発信される「システム障害・運用アラートメール」を統合的に集約する受信ゲートウェイとして機能する。

このため、本サーバはグループウェアとの通信のみならず、庁内各セグメントに存在するインフラ機器およびシステムからの内部 SMTP 接続を確実に受け入れる通信許可ポリシーを設定し、重要システムからの異常通知が途切れることなく管理者に届く環境を整備する。

4-2-2. 多層的なメールセキュリティと誤送信防止・冗長承認の徹底

①受信メールの多層検知と無害化処理

外部ネットワークから庁内へ配送される受信メールに対しては、未知の脅威や標的型攻撃から内部環境を防護するため、多層的なセキュリティチェックと無害化処理を適用する。

本サーバは、上記の内部メールサーバとは、別のシステムである。

【多角的なフィルタリング検知】

スパムメール、迷惑メール、フィッシングメールに加え、差出人のなりすましや悪意あるリンクが含まれる標的型攻撃メールを高度なフィルタリングエンジンにより検知・遮断する。

【メールの完全無害化】

庁内（グループウェア）に到達するメールに対しては、スクリプト実行リスクを排除するため、HTML メールのプレーンテキスト化を行う。さらに、マルウェアの感染源となりやすい「添付ファイルの自動削除（剥離）」を実施し、脅威を構造的に排除した安全なテキスト本文のみを職員へ配送する。

②送信制御による誤送信防止と上長による冗長承認

職員による外部へのメール送信に際しては、人為的ミス（うっかりミス）に起因する情報漏洩を防御するための自動制御機能と承認ワークフローを実装する。

【誤送信防止機能の自動適用】

複数の外部宛先へ一括送信する際の強制 BCC 変換や、送信ボタン押下時の「宛先・添付ファイル再確認ダイアログなどを自動的に適用し、BCC 指定漏れや宛先間違いを未然に防ぐ。

【添付ファイル送信時の上長承認】

添付ファイルを伴う外部向けメールの送信に対しては、システム上で所属上長（管理者）による確認・承認を必須とする「送信承認ワークフロー」を強制適用する。上長による内容確認と明示的な承認手続きが完了しない限り、添付ファイル付きメールが外部へ送信されない仕組みとすることで、故意・過失による重要データの流出を水際で封鎖する。

なお、ファイルの持ち出し制御やグループウェアの機能で上長承認が行える場合もあり、どのタイミングで承認を必要とするかは運用面から検討する。

③送信元ドメイン(系統)別のマルチポリシー制御要件

本メールセキュリティシステムは、インターネット系からのメールのみならず、LGWAN を経由して届くメールについても一元的に通過・制御する。

接続するネットワーク系統や送信元ドメイン(インターネット、LGWAN、特定連携先等)の信頼性レベルに応じて、フィルタリングの検知強度や無害化処理の適用範囲(HTML テキスト化の要否、添付ファイル削除の例外設定等)を柔軟に切り替えられる「マルチポリシー制御機能」を実装する。これにより、高いセキュリティ水準を維持しつつ、安全性が担保された組織間通信における業務効率の低下を防ぐ。

4-3. エンドポイント管理・セキュリティおよびデータ保護

4-3-1. 資産管理の高度化と勤怠連携・ログ管理

①ソフトウェア資産管理とリモート配信・制御

各種エンドポイント端末(Windows FAT、VDI 等)の安全性を維持するため、インストールされているすべてのソフトウェアのバージョン、ライセンス状態、およびセキュリティパッチの適用状況を中央でリアルタイムに可視化・管理する仕組みを構築する。

各種アプリケーションの更新プログラムや新たなインストーラーを、エンドポイントへリモートで一括配布および強制適用・実行する機能を実装する。これにより、脆弱性が発見されたソフトウェアを放置することなく、庁内全体のセキュリティレベルを常に最新かつ均一な状態に保持する。

②登録制外部デバイス制御によるマルウェア混入防止と VDI リダイレクトの検証

近年増加している USB メモリ等の記憶媒体を媒介とした大規模なマルウェア混入・感染事案を鑑み、単なる「USB メモリ使用禁止」という一律の運用制限にとどまらず、ハードウェアの個体識別情報に基づく厳格なデバイス接続制御を導入する。

具体的な制御手法として、あらかじめシステムに正規登録され、安全性が確認できた特定デバイスのみの接続を許可する「ホワイトリスト方式」を徹底する。デバイスの識別にあたっては、ベンダーID (VID)、プロダクト ID (PID)、およびハードウェア固有のシリアル番号 (Serial Number) を組み合わせた識別・制御を必須要件とする。登録されていない私物 USB メモリや出所の不明な記憶媒体が物理的に接続された場合であっても、アクセスを完全に拒否し、悪意あるプログラムの内部侵入を構造的に遮断する。

また、本市におけるシンクライアント端末から仮想デスクトップ(VDI)へ接続する環境においては、ローカル端末側のポート制御だけでなく、VDI セッション内へ USB デバイスを透過・転送させる「リダイレクト方式(USB リダイレクト等)」との技術的適合性を確保する必要がある。

資産管理ソフトウェアやデバイス制御ツールが持つ USB 制御機能と、VDI 接続用クライアント基盤（セッションブローカー等）における USB リダイレクト通信処理との間で相性不整合が発生した場合、VDI 側で正常にデバイスが制御できない、あるいはリダイレクトそのものが正常に機能しないといった運用上の問題を引き起こす恐れがある。このため、調達・構築にあたっては、資産管理ソフト側のデバイス制御機能と VDI リダイレクト方式との組み合わせ・相性等についてあらかじめ十分に検証し、シンクライアント経由の VDI 利用時においても厳格かつ安定したデバイス制御が確実に成立する設計・導入を必須要件とする。

③ログイン・ログアウトログの収集と勤怠管理連携

エンドポイント端末におけるログインおよびログアウトの確定時刻、ならびに操作ログを漏れなく収集・蓄積する。

取得したログイン・ログアウトログは、職員の労働時間管理システムや勤怠管理システムとの連携を想定し、「出退勤の打刻データ」の補正・裏付け資料として活用する。これにより、自己申告に基づく打刻と実際の PC 稼働時間の乖離を可視化し、過重労働の抑止や不適切なサービス残業の防止といった人事労務管理の適正化・透明化にも寄与させる。

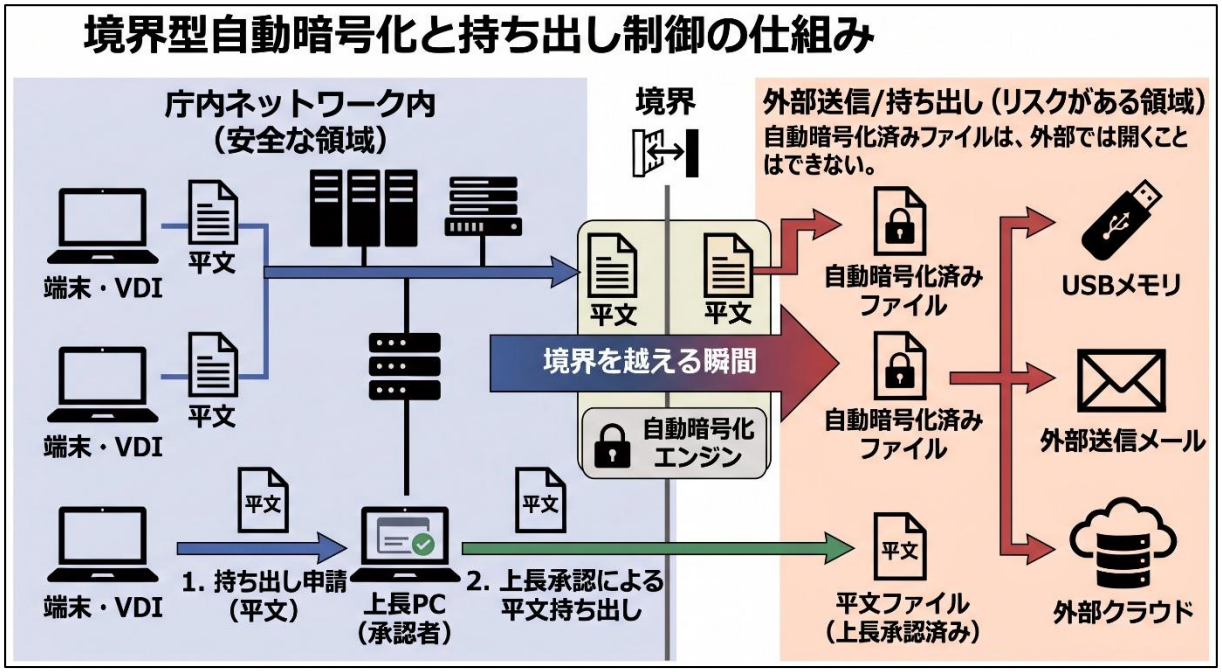
4-3-2. ファイル持ち出し制御とファイル自動暗号化の連動設計

本節では、業務の利便性を損なわずに情報漏洩リスクを極小化するための「境界型自動暗号化」および「持ち出し制御」の連動メカニズムについて定義する。

庁内ネットワーク（安全な領域）においては、業務効率を優先し、端末や VDI 上のファイルは平文のまま取り扱う。一方で、USB メモリへの保存、外部へのメール送信、クラウドストレージへのアップロード等、ファイルが庁内のネットワーク境界を越える瞬間に、自動暗号化エンジンが強制的に暗号化処理を実行する。自動暗号化されたファイルは外部の環境では開くことができない状態となり、万が一の流出時にも情報漏洩を確実に防止する。

ただし、正当な業務上の理由で外部とのファイル共有が必要な場合は、システム上の上長承認フロー（持ち出し申請）を経ることで、例外的に平文でのファイル持ち出しを許可する仕組みとする。

この一連のファイル持ち出し制御と自動暗号化の基本フローは以下の図のとおりである。



①外部持ち出し制御ワークフローと厳格な承認体系

庁内ネットワーク領域（共有フォルダやローカルストレージ等）に存在するファイルを外部へ持ち出す際のあらゆる経路（許可された外部記憶媒体への保存、外部ネットワーク共有への転送、Web サイトへのファイルアップロード、メールへの添付等）に対し、上長承認による明示的な許可を要する「持ち出し制御機構」を実装する。

持ち出し申請に対する承認権限は、各セグメントの重要性に応じて以下のとおり段階的に適用する。

【インターネット系】

このセグメントは、機密情報を扱わないため、上長承認は不要とする。担当者の権限で持ち出しを可能とする。

【LGWAN 系】

このセグメントは、マイナンバーや特定個人情報を含まない機密情報を扱うため、所属部署の管理職による審査・承認を必須とする。

【番号利用系】

このセグメントは、マイナンバー等特定個人情報を取り扱うため、取扱情報の極めて高い機密性に鑑み、所属部署の管理職による一次承認に加え、情報管理部門の職員による二次承認を必須条件とする。二重のチェックプロセスを経ない限り、物理的・論理的なデータの移動を許可しない仕組みとする。

なお、番号利用系から LGWAN 系へのデータの移動も同様とする。

②境界型自動暗号化の採用と運用の単純化

庁内ネットワーク内の全ファイルを常時暗号化する運用は、各種業務アプリケーションとの互換性問題や無数の例外設定が発生し、結果として運用負荷の増大や大量のバックドアによるセキュリティの形骸化を招く恐れがあるため不採用とする。

次期基盤においては、庁内ネットワーク（信頼された領域）内ではファイルを「平文」で保管・利用し、その信頼された領域からファイルが外部へ出るタイミングでのみ自動的に暗号化を施す「境界型自動暗号化」を採用する。

持ち出し承認フローを経ずに不正に持ち出されたファイルや漏洩したデータは自動的に暗号化され、専用の復号環境がなければ閲覧不能となる。一方で、上長等の正規承認を得て持ち出されたファイルについては、自動暗号化の対象外として平文のまま持ち出しを可能とする。この単純かつ明確な境界型制御により、職員の日常業務の利便性を損なうことなく、万が一の流出事故における情報漏洩リスクを確実に防ぐ。

4-3-3. 次期エンドポイント対策（EPP および EDR の導入）

①EPP と EDR による多層防御体系の構築

現在は、従来のエンドポイントセキュリティで主流であった、パターンファイルに基づき既知のマルウェアをブロックする「EPP（Endpoint Protection Platform)」のみの対策を実施しており、「EDR（Endpoint Detection and Response)」は導入していない。

次期 ICT インフラにおいては、未知の脅威やゼロデイ攻撃、ファイルレス攻撃など、EPP の防御をすり抜けて端末内部に侵入してくる最新の脅威に対抗するため、端末内の挙動を常時監視・分析する EDR を組み合わせた構成とする。

また、初期化によってデータが消失する非永続型（リンククローン）VDI 環境においても、再起動やログオフに伴う証拠隠滅・ログ消失を防ぐため、EDR のテレメトリ（挙動ログ）をリアルタイムで管理サーバへ転送・保全する仕組みが必要である。

②インシデント発生時の即時隔離と追跡能力

万が一、マルウェアや攻撃者が端末に侵入した場合、EDR は不審なプロセスや異常な通信挙動を即座に検知し、該当端末をネットワークから自動的に論理隔離する。

隔離と同時に、攻撃が「どこから侵入し」「どのファイルに触れ」「どの範囲まで感染が広がったか」という侵入ルートおよび被害範囲のタイムラインをログから迅速に追跡・可視化できる環境を整備する。これにより、

インシデント発生時の初動対応を極めて短時間で完了させ、全庁的な被害拡大を最小限に食い止める。

4-4. インフラ監視および共有リソースの最適化

4-4-1. ネットワーク・サーバ監視と重要サービスの死活監視要件

①全庁インフラに対する多層的な死活監視の適用

庁内 ICT インフラを構成する全ネットワーク機器(UTM、コアスイッチ、フロアスイッチ、出先ルーター、無線アクセスポイント等）および物理・仮想サーバ群に対し、ICMP（Ping）プロトコルや SNMP polling 等を用いた基本的な死活監視（稼働状態の常時監視）を全網羅的に実施する。

ネットワーク障害やハードウェア障害が発生した際は、管理コンソールへの即時警報表示およびシステム管理者へのアラートメール通知を自動で行う仕組みを確立し、インシデントの早期検知と初動対応の迅速化を図る。

②重要システムに対するサービス・プロセス監視基準の定義

単なる Ping 監視のみでは、OS やミドルウェアのハングアップ、特定サービスの停止といった「ネットワークは疎通するが業務が停止している」状態を検知できない。このため、大規模障害や市民サービスの停止、行政業務の麻痺に直結する「重要インフラ・業務システム」を事前に定義し、より深い階層（サービス等）の監視を実施する。

【適用対象の定義】

AD（Active Directory)、DNS、DHCP、認証基盤（RADIUS)、電子証明書発行基盤（PKI)、グループウェア、ファイルサーバ、およびその他セキュリティ関連システム等。

【監視手法の定義】

対象システムに対し、個別のミドルウェア・プロセス(HTTP/HTTPS、SMTP、SQL、特定の Windows サービス等）の稼働状態を直接確認する「プロトコル・サービス監視」、ならびに CPU・メモリ・ディスク使用率の閾値（しきい値）監視を導入する。これにより、リソース枯渇の兆候や一部サービスの機能停止を未然に把握し、大規模障害への発展を防止する。

4-4-2. 仮想基盤リソースを活用したファイルサーバ設計と AD 連携

①共有ストレージリソースを活用した 3Tier 連動型設計

ファイルサーバの構築にあたっては、非常に高価なファイルサーバ専用の物理 NAS や独立した外部ストレージ機器を個別に調達する手法は採用しない。

仮想化基盤（3Tier）の共有ストレージ領域から必要なディスク容量を切り出し、仮想マシンの Windows Server へ割り当てる設計とする。これにより、重複データを排除したファイルサーバが構築でき、専用ストレージを調達しないことで費用を大幅に低減できる。将来的なデータ容量の増加に対しても、仮想基盤上の共有ストレージから柔軟にディスク容量を拡張できる高い拡張性を確保する。

②Active Directory 連携によるアクセス権限の自動設定

ファイルサーバ内の各部署用共有フォルダに対するアクセス権限管理は、AD(Active Directory）に登録されている職員の所属情報と完全に連動・同期させる運用とする。

定期的な人事異動や組織改編の際、個別のフォルダやファイルに対して手動でアクセス権限を再設定する運用は、莫大な管理負荷を生むだけでなく、権限の設定漏れや消し忘れによる不要なアクセス権の残留（情報漏洩リスク）を引き起こす要因となる。

本設計では、AD 上の職員の所属属性を変更するだけで、各部署の共有フォルダへのアクセス権が自動的に追加・切除される「権限管理の自動化」を要件化する。これにより、情報管理部門の運用工数を極小化しつつ、人事異動初日から正確かつ安全なファイルアクセス環境を整備する。

4-5. コミュニケーションおよび認証基盤の要件

4-5-1. グループウェア調達戦略（一括調達と別調達の評価）

①標準的機能の明確化と費用対効果の検証

グループウェアの選定にあたっては、メール、スケジュール管理、掲示板、設備予約等、日常業務に不可欠な基本機能を確実に備えた標準的なシステムを対象とする。

近年普及が進む大手パブリッククラウドサービス（Microsoft 365、Google Workspace 等）の導入については、利便性の向上や高度な連携機能が期待できる一方で、ライセンス費用がサブスクリプション型として継続的に発生し、価格も頻繁に改訂され、中長期的な財政負担が増大する懸念がある。また、従来の専用パッケージ製品をオンプレミス環境やプライベートクラウド上で運用する形態との間には、コスト構造やセキュリティ管理の面で大きな差異が存在する。そのため、本市が求める機能の範囲とコストとのバランスを厳密に見極め、導入および運用における費用対効果を多角的に検証する。

②RFI（情報提供依頼）を通じた調達区分の評価方針

ICT インフラ基盤の刷新にあたり、グループウェアを次期 ICT インフラ全体基盤と合わせた一括調達とするか、あるいはシステム特性や運用更新

周期の差異を考慮して、独立した単独調達とするかについては、調達の柔軟性と経済性に直結する重要な判断要素となる。

このため、今後の RFI（情報提供依頼）手続きにおいて、グループウェアの提供形態、コスト構造、インフラ連携の親和性等について、市場ベンダーへ広く情報提供を求め、一括調達と別調達の双方におけるメリット・デメリットを比較評価する。この分析結果に基づき、調達における競争性を最大限に引き出し、本市にとって最も経済的合理性の高い調達手法を最終決定する。

4-5-2. 身体的特徴・運用特性を考慮した二要素認証の選定基準

①適用範囲の限定と運用の最適化

地方公共団体におけるセキュリティガイドラインを踏まえ、強固な本人確認が求められる、番号利用系セグメントへのログイン時の二要素認証（多要素認証）の導入を必須とする。

全業務セグメント（LGWAN 系、インターネット系等）へ一律に二要素認証を課す運用は、現場職員の業務効率を悪化させ、ログイン時のトラブルや運用コストの増加を招くため行わない。リスクの高さに応じたピンポイントの適用により、セキュリティの確保と業務利便性の維持を両立させる。

②身体的影響を受ける認証方式の除外

生体認証技術の選定にあたっては、職員の身体的特徴や季節的要因によって認証不能となる事象を回避することを最優先条件とする。

具体的には、「指紋認証」方式を採用対象から明確に除外する。指紋認証は、冬季の乾燥や手荒れによって指紋の隆線が欠損するケースや手掌多汗症等によって、読み取りセンサーが正しく反応しないケースが生じることが知られており、認証失敗によるログイン遅延の深刻化や別の認証方式が必要になるなど、運用課題が生じる。

③実用性と確実性を兼ね備えた二要素認証技術の定義

本市が番号利用系セグメントに導入する二要素認証としては、職員の日常運用を妨げず、かつ高いなりすまし防止性能を有する技術を要件とする。対象として以下のいずれか、またはこれらを組み合わせた方式を定義する。

【高精度顔認証方式】

写真や動画による成りすましを検知・防止する偽装判定機能を備え、かつ感染症対策等による「マスク着用時」や「眼鏡着用時」であっても再登録や取り外しを要することなくスムーズに認証を完了できる方式。

【静脈認証方式（手のひら静脈・指静脈)】
皮膚表面の状態（手荒れ、乾燥、汗等）に左右されにくく、体内の静脈パターンを非接触または軽微な接触で読み取ることで、本人認識率の高さと偽造困難性を両立した、十分な運用実績を有する方式。

【トークンレス認証方式（スマートフォン利用不可)】
物理トークンやカード等の持ち歩き・配布・管理を不要とし、画面上のパターンや位置記憶等を活用して端末単体で二要素認証を完結させる方式（マトリクス認証やパターン認証等)。
なお、トークンレス認証において一般的に用いられる、スマートフォンの認証アプリ（Push 通知）や SMS 送信等を活用する方式については、本市では情報セキュリティおよび管理方針の観点から BYOD（私有端末の業務利用）を一切認めないため、スマホ等を利用した認証方式は採用不可とする。

第 5 章　端末構成・管理

5-1. クライアント端末構成およびネットワーク・セグメントの設計

5-1-1. 端末形態（FAT/シンクライアント）と OS 戦略の定義

本市における次期クライアント端末の構成にあたっては、セキュリティの確保、情報漏洩リスクの最小化、および運用管理工数の抑制を最優先課題とし、端末の形態を「シンクライアント」および「FAT 端末」の 2 種類に大別して適材適所で配備する。

基本原則として、日常的な事務処理、文書作成、メール送受信、および各種システムへのアクセスは、端末側にデータを一切残さない「シンクライアント環境」を標準とする。一方で、ハードウェア固有の特殊な周辺機器を接続して制御する必要がある業務や特定の専用アプリケーション（例：大容量データを直接処理するローカルアプリや特定の伝送ソフト等）の稼働が業務上必須となる一部の部門については、「FAT 端末」をピンポイントで配置する方針とする。これにより、不自由な運用を避けつつ、セキュリティと業務継続性の双方を合理的に満たす構成とする。

5-1-2. 大規模 VDI に代わる代替方式（FAT 端末）の許容と解決すべき技術要件

① 大規模 VDI のコスト課題と代替提案の許容

本市の次期インフラにおいては、情報漏洩対策と運用管理の最適化、利便性の向上を目的に VDI を主要な基盤として運用しており、次期 ICT インフラにおいても同様の方式を想定している。しかし、大規模の VDI 環境の構築・維持には、仮想化基盤や各種ライセンスに多額の経費が必要となる。

このため、調達におけるコスト最適化の観点から、VDI の導入規模を最小限に抑え、エンドポイント側で処理を行う「セキュア FAT」や「データレス PC」を全面的に導入する提案も考えられ、本市として最初から選択肢として排除するものではない。

② セキュア FAT・データレス PC 提案においてクリアすべき技術的課題

本市のネットワーク環境および運用体制において全面的な FAT 方式を導入する場合、以下の固有課題が強く懸念される。代替方式を提案する事業者は、これらの課題に対し明確で実効性のある解決策を提案に含めなければならない。

【始業時等のネットワーク負荷集中とアップデート対策】

ユーザープロファイルの同期やダウンロード等により、始業時に通信トラフィックが集中し、回線帯域の細い出先機関や、庁内 Wi-Fi 環境において深刻な通信遅延を招くリスクがある。

また、大容量化する Windows のフィーチャーアップデート（機能更新プログラム）について、将来的な WSUS の廃止を見据え、全庁のネットワー

ク帯域を圧迫することなく、確実かつ効率的に配信・適用できる仕組みが必要である。

【端末故障時のデータ喪失リスクの排除】
秘密分散技術等を用いて、データを PC 本体とサーバに断片化・暗号化して分散保存する方式の場合、PC の物理的故障に伴い、PC 側に保持されていた断片データが失われ、結果として元のデータが復元不能となる構造的リスクが存在する。端末故障時においても、ユーザーのデータが確実に保全され、代替機等で直ちに業務復旧できる仕組みが担保されていなければならない。

③ 評価方針

上記の「ネットワーク負荷の課題」および「データ保全性の課題」に対して、技術的根拠に基づいた合理的な解決策が提示され、VDI 構成と同等かそれ以上の可用性・運用性が確保されるのであれば、本市は全面的なセキュア FAT 等の導入提案を有効な選択肢として受け入れ、コスト優位性を含めて積極的に評価する。

5-1-3. クライアント端末および VDI ライセンスの予定数量

本市における次期基盤の調達・構築にあたっては、以下の予定数量を想定し、ハードウェア選定、VDI リソース設計およびライセンス調達を行う。

区分	機種・OS / 接続系統	数量	主な想定用途・備考
シンクライアント端末	シンクラ LG 系（Chromebook）	640 台	一般事務用。インターネット接続および LGWAN 系 VDI 接続用
	シンクラ MN 系（Windows 等）	330 台	番号利用系 VDI 接続用（二要素認証対応）
FAT 端末（物理 PC）	LGWAN 系 FAT	90 台	専用ソフト・特殊周辺機器接続が必要な特定業務（LGWAN 系）
	MN 系 FAT	30 台	地方税・住民基本台帳等の専用処理・伝送用（番号利用系）
	インターネット系 FAT	20 台	専用伝送ソフト等のローカル処理用（インターネット系）
仮想デスクトップ(VDI)	個人用 VDI	1,200 台	全職員の日常事務用（容量削減・効率重視の非永続型/リンククローン相当）
	LGWAN 系 VDI	170 台	LGWAN 系業務システム専用（永続型/フルクローン相当）

区分	機種・OS / 接続系統	数量	主な想定用途・備考
	MN 系 VDI	330 台	番号利用系業務システム・ガバメントクラウド接続用 VDI 環境
Office ライセンス	Microsoft 365 ライセンス	1,600	全職員（物理端末・VDI 利用者含む）用の Office 利用

5-1-4. 三層分離ネットワークにおける端末割り当てと Chromebook 活用方針

①三層分離ネットワークにおける接続定義

次期 ICT インフラ基盤では、前掲のネットワーク設計（ZTNA ハイブリッド β モデル）に基づき、庁内ネットワークを「LGWAN 系」「番号利用系」「インターネット系」の 3 つの系統を軸に厳格に論理分離する。各エンドポイント端末は、その役割や接続するセグメントに応じて、前掲のネットワーク・セグメント定義（2-3-1.ネットワーク・セグメントの定義）に基づき、適切な分類と割り当てを行う。

②二要素認証の要件に基づく OS の分岐設計

シンクライアント端末の OS については、「Windows」と「ChromeOS（Chromebook)」の 2 種類を想定し、接続する業務系統および求められるセキュリティ要件に応じて使い分ける設計とする。

【LGWAN 系シンクライアント（Chromebook)】

LGWAN 系シンクライアントおよびインターネット系 FAT については、ハードウェアコストが安価で、かつ Google Enterprise Upgrade による強固なクラウド管理と高いセキュリティ耐性を備えた「Chromebook」を主力として採用する。

【番号利用系シンクライアント（Windows)】

地方税や住記、福祉情報等の極めて高い機密性を取り扱う、番号利用系セグメントへの接続を伴う端末については、現行のサードパーティ製二要素認証ツールとの適合性や専用ドライバの動作要件を考慮し、当面の間は「Windows ベースのシンクライアント」を想定する。

この背景として、番号利用系セグメントへのアクセス時にはセキュリティガイドラインに基づく厳格な二要素認証が必須となるが、現時点の仕様において、一部のサードパーティ製二要素認証製品や生体認証デバイスとの連携において ChromeOS が十分なサポートを有していない可能性があるためである。

また、ChromeOS は、インターネットとの通信が必須であり、番号利用系

セグメントにアクセスする端末が常時インターネットへ接続することは不適当である。

③Chromebook 全面移行に向けた柔軟な設計思想

ただし、本設計は Windows シンクライアントへの固定化を意図するものではない。今後の市場動向や、次期二要素認証製品（顔認証、静脈認証、またはトークンレス認証等）の ChromeOS へのネイティブ対応、あるいは Web 標準規格（WebAuthn 等）を通じた認証基盤の進化を見据え、ChromeOS 上で二要素認証が完全に成立し、実用に耐え得ることが確認できた段階で、すべてのシンクライアント端末を Chromebook へ一本化（置換）することを視野に入れた、柔軟な拡張性を持つ設計思想とする。これにより、将来的なハードウェア調達コストおよびライセンスコストの大幅な圧縮の余地を常に確保する。

ただし、インターネットへの通信が必要であるという課題については、十分に検討が必要である。

④インターネット Wi-Fi 接続と専用 FAT 端末の分離運用

Chromebook（シンクラ LG 系端末）を運用する「シンクラ LG 系セグメント」においては、VDI への画面転送通信に加え、OS の稼働およびデバイス管理（CEU 等）に必須となる Google 系通信、ならびに M365 認証通信等についてのみ、LBO（ローカルブレイクアウト）経由でインターネットへの直接通信を許可する。

一方で、汎用的な Web ブラウジング等、完全なインターネットアクセスが必要な場合は、端末の接続先を「インターネット専用 Wi-Fi（インターネット系セグメント)」へ切り替えて利用する運用とする。当該 Wi-Fi に接続されている状態においては、セキュリティ上のポリシーに基づき、庁内の仮想デスクトップ(VDI)環境へはアクセスできない仕様(SSID と VLAN による明示的な切り離し）とし、シンクライアントとしてではなく、インターネット専用端末として機能させる。

また、前述のとおり、インターネット系ネットワークにおいて業務上どうしても特別なローカルアプリケーション（専用の伝送ソフト等）の常時稼働が必要となる特定の部署・用途に対しては、Windows の FAT 端末を専用機として必要最小限の規模で配置し、専用のセグメントにて運用を行う。

5-1-5. クライアント端末の配備・運用方針（１人１台個別貸与の導入検討）

①共有方式から「１人１台個別貸与方式」への移行

現状（第 1 期）においては、各部署の出勤者数や席数等に基づき、最適化した台数を「部署共用端末」として、所属職員の数よりも少ない配置・運用をしている。しかし、この方式は端末の一時的な不足が生じ、複数人

が同一端末をランダムに利用するため、柔軟な働き方の阻害や管理責任の曖昧化が課題となっている。

第 2 期においては、フリーアドレス等による機動的な働き方の実現、セキュリティ管理の高度化、使用する職員の管理責任の明確化などを進め、「職員 1 人 1 台の個別貸与方式」への移行を検討する。

②「6 年間携行」の原則と管理責任の明確化

個別貸与されたモバイル端末等は、原則として調達周期（ライフサイクル）である「6 年間」同一の端末を職員個人が占有して継続使用する。

【人事異動時の端末携行（原則）】

人事異動の際にも、一度貸与された端末は元の部署へ返却せず、職員自らが新しい配属先（職場）へ「携行」してそのまま使用することを原則とする。

【紛失・破損リスクの低減】

「自分専用の端末」として長期間にわたり占有・管理させることで、共用時に生じがちであった取り扱いの不徹底や放置、しまい込みを防止し、端末の紛失・破損といった管理上のリスクを低減させる。

③人事異動時の端末携行と、系統違い（NM 系／LG 系）に伴う例外ルール

原則携行とする一方で、セキュリティセグメント（ネットワーク系統）が異なり、使用する端末の種類自体が変化する部署間での人事異動に際しては、例外的に端末の交換（回収および再貸与）を行う。

【シンクラ NM 系とシンクラ LG 系の仕様差異】

本市が採用する番号利用系の「シンクラ NM 系」は Windows OS に二要素認証を組み合わせた構成であり、LGWAN 系の「シンクラ LG 系」は Chromebook を採用している。このように、部署や業務によって必要となる端末仕様（OS および認証方式）が根本的に異なる。

【交換・再設定の運用】

NM 系 VDI が必要な部署と、それ以外の部署との間での人事異動においては、使用する端末の種類そのものが異なるため、例外的に「端末の携行は不可」とし、異動先部署の仕様に合わせた端末交換を行う。

一方で、NM 系同士、または LG 系同士の異動であれば、端末の変更は生じないため、そのまま端末を携行して使用する。

なお、本市が導入するシンクライアント端末は、ローカル環境に個人ごとの個別データや設定を保持しない仕様を想定しているため、異動に伴う

端末交換が発生した場合であっても、端末の初期化や個別データの移行、個別再設定といった煩雑な作業は一切不要であり、スムーズな回収と再貸与が可能な運用を実現する。

④1 人 1 台・携行化がもたらす変革効果

この「1 人 1 台個別貸与・携行運用」の確立により、以下の効果を創出する。

【フリーアドレス化の促進】

自席に縛られることなく、庁内のどの場所（フリーアドレスエリア・会議室等）からでも、自身に最適化された環境で即座に業務を行える。

【テレワーク・モバイルワークへの柔軟な拡張性】

現時点において、テレワークやモバイルワークは小規模な実施にとどまっており、今後の具体的な実施規模や運用方針等の詳細は検討段階にある。そのため、将来的な方針決定やニーズの拡大に対し、システム側の軽微な変更のみで容易かつ柔軟に対応できるシステム構成を、あらかじめ設計思想として織り込んでおく必要がある。

将来的にテレワークを推進する際、1 人 1 台貸与端末をそのまま活用するか、あるいは別途専用端末を調達するかは今後の検討事項である。しかし、日常的に使用している貸与端末をそのままテレワーク等へも転用・適応可能とする設計にしておくことで、将来のテレワーク対象者の増加時にも、専用端末の追加導入行わずに、迅速かつ経済的に対応できる選択肢を確保する。

これにより、端末使用の事前申請や貸出調整といった業務を最小限に抑え、将来的な働き方の変化へ機動的に適応できるインフラ基盤としての拡張性を担保する。

5-1-6. 端末調達におけるコスト最適化とメーカー選定の多様化

近年の円安進行や半導体不足、グローバルなサプライチェーンの混乱等により、端末の市場価格は高騰傾向にあり、2 期の調達時においてコストの最適化は不可欠である。

本市の端末調達においては、特定の国内・海外大手 PC メーカーの製品のみを前提とする従来の選定基準を見直し、以下の方針に基づき、要求仕様および長期保守要件を満たす多様なメーカー・ブランドの製品を積極的に評価・採用する。

① 独立系メーカーおよび BTO（Build To Order）ブランドの積極的活用

大手メーカー製 PC に限定せず、国内の PC 専門店やシステムインテグレ

ーターが独自に企画・製造・展開する「法人・ビジネス向けオリジナルブランド PC（BTO パソコン等）」や、グローバル市場で確かな実績を持つ独立系メーカーの製品も、同等の選択肢として調達要件に含める。

これにより、ハードウェアの性能に対するコストパフォーマンスを最大化する。

② 長期保守と国内サポート体制の必須化

価格競争力を重視する一方で、安価であっても品質やサポート体制に懸念がある海外の無名ブランド等は採用しない。

本市の端末運用は 6 年間を想定しており、最低でも 5 年間の長期ハードウェア保守（部品提供および修理サポート）が確約できること、および国内に迅速な修理・サポート拠点を有していることを必須要件とする。

③ 調達事業者への柔軟な提案要求

次期 ICT インフラ構築を担う提案事業者に対しては、あらかじめ指定された大手メーカーの機器を前提とした画一的な提案ではなく、上記の条件（国内拠点による長期保守の確約と高いコストパフォーマンス）を満たす最適な PC メーカーやブランドを調査・選定し、本市にとって最も経済的優位性の高い端末構成を提案することを求める。

5-2. ディレクトリサービスおよびデバイス・アカウント統合管理

5-2-1. Active Directory（AD）の統合・ドメイン分割構成

現行のドメイン構造を踏襲し、管理性の向上とセキュリティの厳格化を両立させるため、ディレクトリサービス（Active Directory：AD）を 2 ドメイン構成へ集約・最適化する。これにより、全体としてのドメイン管理コストや運用負荷を軽減しつつ、番号利用系における厳格な分離性を維持する。本ドメイン構成のもと、庁内の全 Windows マシン（物理 FAT/シンクライアント）、仮想デスクトップ（VDI）、およびユーザーアカウントを一元管理する。

【番号利用系 AD ドメイン】

極めて高い機密性と独立性が求められる「番号利用系セグメント」専用のドメインとして完全に独立させて配置する。他系統からの物理的・論理的影響を排除し、アクセス制限やグループポリシーを個別に集中管理する。

【LGWAN 系・インターネット系統合 AD ドメイン】

従来どおり「LGWAN 系」と「インターネット系」の領域については、同一の統合 AD ドメイン配下で一元管理する。

5-2-2. ユーザーアカウント設計と人事異動自動化（情報連携）

①アカウント運用原則

本市においてインフラを利用する全職員（正職員、再任用職員、会計年度任用職員等を含む約 1,500 名）に対し、原則として個人識別が可能な「個人用アカウント」を発行・割り当てる。これにより、操作ログの追跡性と個別の権限設定を可能とする。

ただし、派遣会社や外部委託事業者が常駐して業務を行う窓口等、業務の性質上個人アカウントの運用が馴染まない特定の運用環境については、限定的に例外として厳格な管理のもとで「共用アカウント」の利用を認める定義とする。

②所属・役職情報をマスターとした運用自動化

統合管理の核心的機能として、AD 内に保持する「所属情報」「役職情報」「職員属性」等のマスターデータを全庁的な権限制御の信頼できる唯一の情報源（SSOT/Single Source of Truth）として位置付ける。

人事異動や組織改編の際、情報管理部門が AD 上の属性情報を更新するだけで、以下の関連システムやサービスにおける権限変更および環境設定が、自動的に反映される仕組み（運用自動化）を要件とする。

【ファイルサーバのアクセス権自動追随】

各部署の共有フォルダに対するアクセス権限を AD の所属オブジェクトと連動させ、異動と同時に旧部署の権限切除および新部署の権限付与を自動的に完了させる。

【外部システム・LDAP 連携の同期】

グループウェア、認証基盤、各種業務システム等の外部システムに対し、LDAP/SAML 等の連携プロトコルを介して最新の所属・役職情報を同期・自動更新する。

【プリンタの動的自動割り当て】

職員が PC や VDI へログインした際、AD のスクリプトが動的に実行され、移動先の部署や配属場所に最適な論理プリンタを自動セットアップする。

5-2-3. ユーザープロファイル管理の高度化（FSLogix 等の導入検討）

① 従来方式の課題とプロファイルコンテナ技術の検討

従来の移動ユーザープロファイルを用いた運用では、ログイン時に大量のファイルがネットワーク経由で一斉に読み込みされるため、始業時のトラフィック集中やログイン処理の遅延、プロファイル破損といったトラブルが生じやすい構造的課題がある。

次期 ICT インフラ基盤においては、これらの課題を根本的に解消するため、ユーザープロファイルを仮想ディスク（VHD/VHDX 等）として集約し、ログイン時にネットワーク経由で動的にマウントするプロファイルコンテナ技術（Microsoft 社の FSLogix 等）の導入を検討する。

② VDI 環境における起動負荷軽減と安定稼働の実現

約 1,700 台規模の VDI 環境（特に非永続型・リンククローン方式を採用する個人用 VDI）においてプロファイルコンテナ技術を適用することで、ログイン・起動時のファイル転送量およびストレージ I/O 負荷を大幅に削減できる。これにより、始業時のログイン遅延やプロファイル読み込み失敗に起因するトラブルを未然に防ぎ、安定したデスクトップ起動と高い操作レスポンスの確保が期待できる。

③ FAT 端末（代替方式含む）における通信帯域圧迫の解消

第 5 章「5-1-2」にて挙げたセキュア FAT・データレス PC の導入課題である、ログイン時のユーザープロファイルダウンロードに伴うネットワーク帯域の圧迫に対しても、プロファイルコンテナ技術は有効な解決策となり得る。ログイン時にプロファイル全体を一括ダウンロードするのではなく、仮想ディスクをマウントして必要なデータブロックのみを読み書きする仕組みにより、回線帯域の細い出先機関や庁内 Wi-Fi 環境における始業時の通信負荷を大幅に抑制できる可能性がある。

ただし、FAT 端末および無線 LAN 環境での適用にあたっては、一時的なネットワーク瞬断やオフライン状態への耐性（キャッシュ機能の活用等）を含めた実用性の検証が必要である。

④ ライセンス体系および RFI における検証方針

FSLogix 等の利用にあたっては、Windows Enterprise / VDA ライセンスや Microsoft 365(M365)の上位プラン等に利用権が含まれる場合がある。このため、「5-3-2. M365 ライセンスプランの選定」と合わせて、追加ライセンス費用の有無やファイルサーバ側のストレージ要件を含めた費用対効果を RFI 等を通じて総合的に検証する。

5-2-4. Chrome Enterprise Upgrade によるクラウドデバイス管理

端末戦略において Chromebook（シンクライアント端末）を採用する場合は、集中管理基盤として、「Chrome Enterprise Upgrade」を必須要件とする。

Windows 端末がグループポリシーによって制御されるのと同様に、Chromebook および Google アカウントの管理をクラウド上の Google 管理コンソールへ統合し、以下の端末管理機能を一括運用する。

【ゼロタッチ・キッティング】
新規導入時や端末交換時において、工場出荷状態の端末に電源を投入してネットワークへ接続することで、自動的に本市のドメイン管理下へと組み込まれ、必要なポリシーや証明書が即座に配布・適用される事前設定環境を確立する。

【統一的なセキュリティポリシーの強制適用】
USB メモリの接続制限、外部 SSID への接続制限、インストール許可アプリの制御、ブラウザセキュリティ設定等をクラウドから一括で更新・強制適用し、管理の漏れを防止する。

【紛失・盗難時のリモート制御】
端末の紛失や盗難、不正持ち出しが発生した際、管理者コンソールから該当端末を遠隔で即座にロック（無効化）し、端末内のキャッシュデータを「リモートワイプ（遠隔全消去）」することで、端末からの情報流出リスクを物理的に遮断する。

5-3. 端末アップデート管理および Microsoft 365 最適化

5-3-1. 資産管理基盤と連携した Windows 端末・VDI の一元更新管理

本市におけるすべての Windows 環境（物理 FAT 端末、Windows シンクライアント端末、および約 1,700 台規模の VDI）を対象として、Windows Update における品質更新プログラムおよび機能更新プログラムの一元的な配信・適用管理基盤を構築する。

なお、従来利用されてきた Windows Server Update Services（WSUS）については、Microsoft 社による今後の製品展開方針やサポート終了（非推奨化）の動向を踏まえ、採用しない。代わりに、本市が導入する統合資産管理・エンドポイント管理基盤のアップデート管理機能を活用し、確実かつ効率的な一元管理を実現する。

本管理基盤の導入・運用にあたっては、以下の制御および配信運用を必須要件とする。

【更新パッチの事前検証と段階的適用】
個人用 VDI 環境については、業務への影響を最小限に抑えつつ、計画的に適宜アップデートを実施する運用とする。

一方、物理 FAT 端末および業務システム用 VDI 環境に対しては、対象端末群へ段階的に適用（グループ分け配信）する運用を実施する。

【ネットワーク帯域の保護と負荷分散】

多数の端末がインターネット上の更新サーバへ個別にアクセスすることに伴う外線帯域（インターネット回線）の逼迫を回避するため、管理基盤によるキャッシュ配信機構や帯域制御機能を活用する。

さらに、庁内 LAN における配信時間帯の制御（夜間・休日等のスケジュール配信）や配布速度の制限を行うことで、パッチ適用に伴うネットワークの混雑・遅延を防止し、通常業務の安定稼働を確実に担保する。

5-3-2. M365 ライセンスプランの選定とグループウェア統合の費用対効果検証

①現行ライセンス運用の評価と見直し

本市では現在、全職員・端末の Office アプリケーションの利用を目的として「Microsoft 365（現行：Apps for enterprise)」を約 1,500 ライセンス運用しており、将来的には 1,600 ライセンスへの増加を見込んでいる。次期 ICT インフラ基盤の構築にあたっては、単に現行ライセンス（Apps for enterprise）を同規模で継続更新するだけでなく、グループウェアやセキュリティ基盤などシステム全体の構成変更を踏まえたライセンスプランの最適化を図る。

②RFI/RFP における提案要件と費用対効果の検証方針

今後の RFI（情報提供依頼）および RFP（提案依頼）においては、提案事業者に対して特定のライセンス固定を前提とせず、システム全体のトータルコスト削減と利便性向上を両立させる「全体最適の組み合わせ提案」を求める方針とする。提案事業者による検証の主な軸は以下のとおりである。

【グループウェア統合によるコスト削減シナリオ】

専用グループウェア（メール、スケジュール、施設管理、掲示板等）を導入せず、M365 群が提供するクラウド機能へ全面的に集約・統合する場合のライセンス追加費用と、グループウェア導入・保守・運用費の削減額を対比・評価する。

【上位プラン採用による他ツール置換効果の検証】

Microsoft365(M365)の上位プラン（E3 や E5、あるいは各種オプション等）へシフトした場合に、従来個別に調達していた資産管理、ID 管理、セキュリティ対策ソフト等のサードパーティ製ソリューションを M365 の機能へ統合・代替できるか検証する。単体のライセンス単価の増額のみで判断せず、代替される周辺システムの削減費用を含めた、トータルコストの観点から最も経済的合理性の高いプランを選定する。

5-4. 印刷基盤(プリンタサーバ)の集約とセキュアクロスセグメント印刷

5-4-1. 系統間(LGWAN 系・番号利用系)共有プリンタ設計

ネットワークの三層分離に基づき、系統ごと(LGWAN 系・番号利用系等)に個別の物理プリンタを配置・運用する構成は取らず、物理プリンタの設置台数を最小限に抑えつつ利便性を担保するプリンタ統合モデルを構築する。

本設計では、「LGWAN 系」および「番号利用系」の異なる業務系統（VDI および物理端末）から、同一の物理プリンタへ相互に安全な印刷出力を可能とする。ネットワークの物理・論理的な分離状態を維持しながら、プリンタサーバを介して印刷指示を集約・仲介することで、庁内機器調達コストおよび出力管理の運用負担を大幅に削減する。

5-4-2. プリンタ専用セグメントの通信制御とセキュリティ強化

①独立したプリンタ専用セグメントの配置

ネットワーク構成（ZTNA ハイブリッドβモデル）に基づき、全庁の複合機およびプリンタ群を独立した「プリンタ系セグメント)」へ集約・配置する。

各業務端末（VDI や物理 PC 等）からプリンタ群への直接の IP 通信は拒否し、中央の「プリンタサーバ」との通信のみを許可するアクセス制御(ACL)を最上位 UTM またはコアスイッチにて適用する。これにより、プリンタを足がかりとしたネットワーク間での不適切なアクセスを防止する。

②通信プロトコルの厳格な絞り込み

プリンタ系セグメントにおける通信制御は、印刷および機器管理に必要な最小限のプロトコルのみを許可し、不要な通信を遮断する。

【許可プロトコル】

印刷処理に必要なスプール系プロトコル（LPR/LPD、RAW/Port 9100、IPP/IPPS 等)、稼働監視および管理用の ICMP (Ping)、Web 管理コンソール接続用の HTTP/HTTPS のみに限定する。

【不正通信の遮断】

SMB（ファイル共有プロトコル）等のファイル転送用プロトコルや不要な広域ブロードキャスト通信は許可せず、プリンタを介したファイルの隠蔽・持ち出し等を不可能とする。

【インターネット系からの印刷制御】

セキュリティの観点から、「インターネット系セグメント」からの印刷出力は原則として不許可とする。

5-4-3. AD ログオンスクリプトによる論理プリンタの動的自動割り当て

①中央集約型論理プリンタ管理

プリンタサーバ上に庁内すべての物理プリンタに対応する「論理プリンタ」を作成・共有化し、ドライバ管理や印刷キューの一括制御を管理サーバ側で行う。

②所属情報と連動した自動セットアップ（ノータッチ運用）

職員が端末（VDI 環境および物理 PC）へログインした際、AD(Active Directory）に保持されている職員の所属情報を元に、AD のログオンスクリプトを自動実行する。

職員の配属部署や配置場所に最適な近接の論理プリンタがバックグラウンドで自動的に追加・デフォルトプリンタ設定される仕組みを確立する。これにより、人事異動や組織改正の際にも、手動でのプリンタ追加設定やドライバの個別インストール作業を一切不要とし、管理工数の削減とユーザー利便性の最大化を両立させる。

第 6 章　外部通信

6-1. ガバメントクラウドおよびセキュリティクラウド接続

6-1-1. 千葉県情報セキュリティクラウドを介したインターネット接続

①セキュリティクラウドへの通信集約

国が推進する自治体情報セキュリティ対策の取組に基づき、本市から外部インターネットへ向けた一般的な Web アクセスおよびメール等の通信については、原則として「千葉県情報セキュリティクラウド」へ接続する通信経路を標準構成とする。

本接続形態により、県内すべての自治体と同等水準の高度なセキュリティ監視、Web フィルタリング、スパム対策、および未知の脅威に対するサンドボックス検知機能等が統合的に適用される。これにより、インターネット経由でのマルウェア感染や C2 サーバ（コマンド＆コントロールサーバ）との不正通信といった脅威を県域の境界部分（水際）で遮断し、本市インフラ全体の安全性を維持する。

②標準経路としてのトラフィック制御

インターネット系セグメントおよびシンクラ LG 系セグメントからの外部インターネット通信は、最上位 UTM およびコアスイッチにおけるデフォルトルートとして千葉県情報セキュリティクラウド宛てにルーティングされる。ただし、全通信を一律にセキュリティクラウド経由とすることで生じる帯域の圧迫や応答遅延（レスポンス低下）、セキュリティの相性不整合による web アクセスの不具合等の課題に対しては、後述するローカルブレイクアウト(LBO)技術を組み合わせて選択的に分散配置することで、セキュリティ強度の維持と良好な通信の品質確保を両立させる。

6-1-2. LGWAN 回線を介したガバメントクラウド（標準化基幹システム）接続設計

①ガバメントクラウド運用の前提と回線経路

地方公共団体情報システム標準化基本方針に基づき、本市の住民基本台帳、地方税、福祉関連等の基幹業務システム群は、国が整備するガバメントクラウド上へ移行し、安全かつ高可用な運用を行っている。

ガバメントクラウドへのアクセス経路については、独自の専用線ではなく、LGWAN 接続回線を経由して接続を行う。

②庁内「番号利用系セグメント」からのアクセス制御

ガバメントクラウド上で稼働する各種標準化基幹システムは、取り扱う情報の極めて高い機密性に鑑み、すべて庁内ネットワークにおける「番号利用系」のシステムとして位置付ける。

これに伴い、庁内 LAN 側の通信設計においては、以下の番号利用系セグメント群からガバメントクラウド宛ての通信が安全・確実に疎通できるよ

う、専用のルーティングおよびアクセス制御（ACL）を定義する。
最上位の UTM およびコアスイッチにおいては、その他のセグメント（インターネット系や通常 LGWAN 系等）からガバメントクラウド上のデータベースや管理領域への直接通信を厳格に遮断し、三層分離の原則に則ったセキュアな境界防御を維持する。

【番号利用系 FAT 端末】
専用機器等が接続された物理 FAT 端末から、LGWAN 回線上のガバメントクラウド接続用ゲートウェイ宛ての直接アクセスを許可する。

【番号利用系 VDI】
仮想化基盤内に構築された MN 系 VDI 環境から、VDI 画面転送通信とは物理的・論理的に分離された業務通信ルートを通じて、ガバメントクラウド上の対象データベースおよびアプリケーションサーバへ接続を行う。

6-1-3. LGWAN ゲートウェイ基盤の構成と運用

①庁内 LAN と LGWAN の接合構成と機能の集約

庁内 LAN と LGWAN（総合行政ネットワーク）を接続するゲートウェイ基盤については、安定した運用実績と業務継続性を考慮し、次期 ICT インフラにおいても現行と同様の方式とする。
物理的な接続ポイントには、冗長化された UTM（2 台）および L2 スイッチ（2 台）を配置し、仮想化基盤上に構築した 1 台の LGWAN ゲートウェイサーバによって通信を制御する構成とする。
本ゲートウェイサーバは、1 台の VM で DNS、NTP、メール、プロキシの各中継・制御機能を複合的に担う。また、各種設定変更等の運用保守をコマンドラインに依存せず、市職員が視覚的かつ確実に行えるよう、GUI ベースの管理ツールである Webmin を継続して利用する。

② メール配送の振り分けとドメイン変換ルール

本ゲートウェイを経由するメールの送受信においては、LGWAN とインターネット間のドメインの差異を吸収し、適正なルーティングを行うため、以下のドメイン変換（city.abiko.lg.jp と city.abiko.chiba.jp）を実施する。

【受信メールの変換・転送】
外部からのメール受信は、LGWAN 経路からの通信のみを許可する。受信したメールの宛先ドメイン「city.abiko.lg.jp」を庁内用ドメイン「city.abiko.chiba.jp」へ変換した上で、内部の庁内メールサーバへ転送する。

【送信メールの自動振り分けと変換】

庁内から外部への送信時は、宛先アドレスに応じて「インターネット向け」と「LGWAN 向け」の通信をシステムが自動で振り分ける。このうち、LGWAN 宛ての送信メールについてのみ、送信元のドメインを「city.abiko.chiba.jp」から「city.abiko.lg.jp」へ自動変換して送信する。

③ ドメイン変換テーブルのメンテナンス体制

各行政機関における「LGWAN ドメイン」および「インターネットドメイン」の対応情報は、国から随時更新・提供される。これに伴うゲートウェイサーバ上の変換用テーブルの修正および設定反映作業については、保守対応とせず、次期運用においても引き続き市職員の手により随時対応・メンテナンスを行う運用とする。

6-2. ローカルブレイクアウト(LBO)の最適化と通信制御

6-2-1. 高速光回線(フレッツ 光クロス)を活用した LBO の対象範囲と適用拡張

①LBO 導入の目的と回線構成

千葉県情報セキュリティクラウドへのトラフィック集中による回線帯域の圧迫や通信遅延の回避に加え、セキュリティクラウド側で実施される高度な暗号化通信検査やフィルタリング機能等との相性問題により、特定の Web サイトへ正常に接続できない事象に対処するため、特定の通信を庁内から直接インターネットへ迂回させる「ローカルブレイクアウト(LBO)」技術を適用する。

LBO 用の回線として、超高速・大容量通信に対応した「フレッツ光クロス」を市側で準備し、プロバイダには固定グローバル IP アドレスを提供する「OCN」を使用する。固定グローバル IP を保持することにより、外部サービスへの市のグローバル IP のみ許可した制限や後述するテレワーク・リモート保守のセキュアな通信としての機能を担保する。

②LBO 対象通信の厳格な制御と適用拡張

全トラフィックを無条件に LBO へ逃がす運用はセキュリティの低下を招くため、事前に許可された特定のドメインおよび IP アドレス宛ての通信のみを厳格に選別して LBO 経路へ振り分ける設計とする。

【Microsoft 365（M365）通信】

現行運用において大量のセッションと帯域を消費する M365 の認証通信（Entra ID 等）および各種クラウドサービス通信を LBO の主たる対象として適用する。

【Google サービス通信（将来的な Chromebook 本格導入対応)】

今後の端末戦略に基づき Chromebook を導入した場合、Google Workspace や端末管理（Chrome Enterprise Upgrade）に関わる各種クラウド通信についても、LBO 経路へ選択的に振り分ける拡張を行える設計とする。ただし、通信する情報の性質を考慮し、安易にすべてを LBO 経路とするのではなく適切なセキュリティ対策を実施する。

これらの振り分け制御は、最上位 UTM のポリシーベースルーティング（PBR）や Web 自動構成ファイル（PAC ファイル）の厳格なチューニングによって実現し、必要な通信のみをピンポイントで LBO へ誘導する。

6-2-2. 運用中の LBO 通信チューニングと保守運用境界の明確化

①動的な LBO 通信チューニング運用

セキュリティクラウドを経由する標準経路においては、通信帯域の逼迫や遅延だけでなく、セキュリティクラウド側の各種セキュリティ制御（SSL/TLS 復号検査、各種フィルタリング等）と対象サイトとの相性によって、「特定の行政 ASP サービスや Web サイトに接続できない」「画面が正しく表示されない」「セッションが途中で断絶する」といった運用上の不具合が発生する場合がある。

このようなセキュリティの相性等に起因する接続不可・不具合が発生した Web サービスについては、情報管理部門と受託者にて対象サービスの安全性を確認・審査する。セキュリティ上問題がないと判断されたものについては、LBO の適用対象として評価し、運用の中で随時、UTM のルーティングテーブル、アクセス制御リスト（ACL)、および PAC ファイルを修正して LBO 経路へ動的に迂回させる「通信チューニング」を迅速に遂行する体制を確立する。

②LBO 回線を巡る責任分界の明確化

LBO 回線（フレッツ光クロス）は、LBO 通信のみならず、後述するテレワーク接続や複数ベンダーによるリモート保守の共通回線としても多目的に活用される。運用時のトラブルや設定変更における責任範囲の曖昧さを防止するため、本インフラにおける保守の責任分界を以下のとおり明確に定義する。

【各業務システムベンダーの管轄（本庁内 ICT インフラ保守の対象外)】

LBO 回線上に配置・接続される、各業務システムベンダーが所有する VPN ルーター等のハードウェア機器調達、物理設置、パラメータ設定および保守管理は、それぞれのベンダーの責任と費用において実施（本庁内 ICT インフラ契約の対象外）する。

【本インフラ受託者の管轄（本庁内 ICT インフラ保守の範囲内）】

上記ベンダー機器との接続に伴い発生する、庁内コアスイッチや最上位 UTM 等におけるルーティング設定、アクセス制御リスト（ACL）の追加・変更・削除、VLAN 制御および PAC ファイルの修正等の設定変更作業は、すべて本庁内 ICT インフラの通常保守・運用サポートの範囲内として実施する。

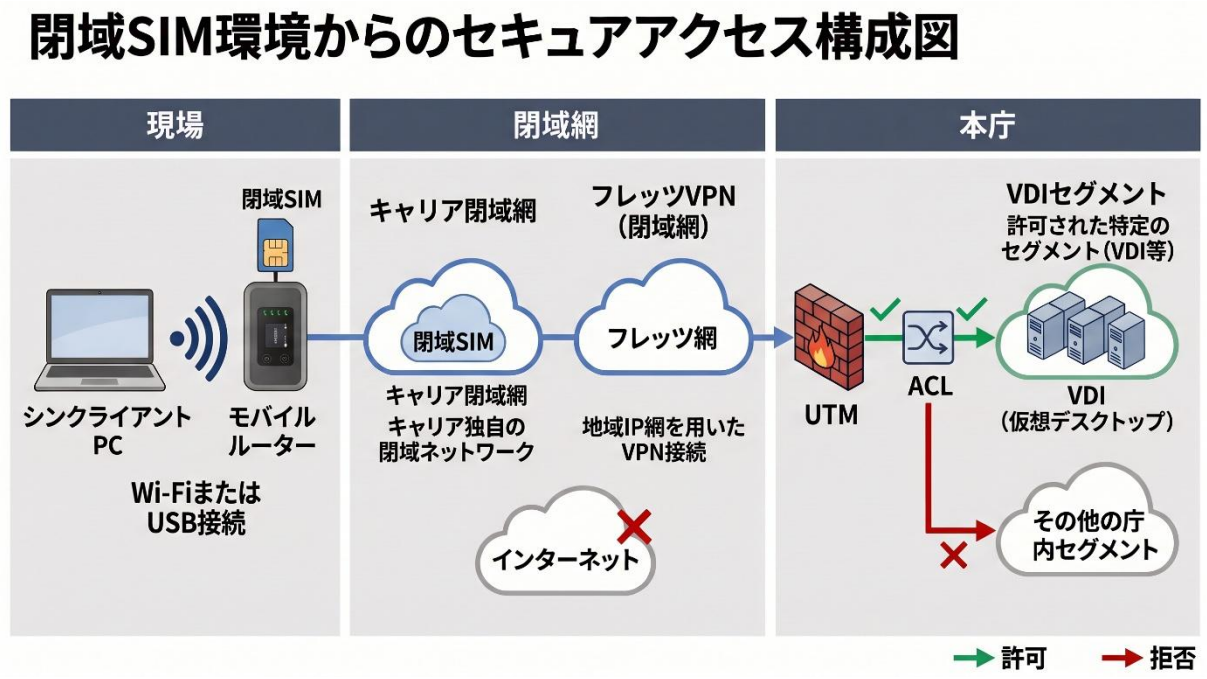
6-2-3. 閉域 SIM 環境と庁内 LAN の接合およびアクセス制御

本節では、出先機関や屋外などの現場環境から庁内ネットワークへ安全に接続するための、閉域 SIM を用いたリモートアクセス環境の構成要件を定義する。なお、本構成は、既に利用している環境を記載するものである。

現場に携行するモバイルルーターからの通信は、情報漏洩や外部からの攻撃リスクを排除するため、インターネットを一切経由させないものとする。具体的には、キャリア独自の閉域ネットワークからフレッツ網（VPN 接続）をとおり、直接本庁の UTM へと到達する閉域経路とする。

また、本庁へ到達した通信に対しては、UTM および ACL（アクセスコントロールリスト）によって厳密なアクセス制御を実施する。VDI（仮想デスクトップ）などの事前に許可された特定セグメントへの通信のみを許可し、その他の庁内セグメントへのアクセスはすべて拒否する設計とする。

この閉域 SIM 環境からのセキュアな経路およびアクセス制御の全体像は以下の図のとおりである。



①既存閉域 SIM 環境と次期庁内 LAN との相互接続設計

本市において既に運用している「閉域 SIM 環境（訪問先、工事現場、期

日前投票所等からの可搬型庁内アクセス基盤)」を次期 ICT インフラ基盤へ円滑に統合・接合するため、最上位 UTM およびコアスイッチ群において適切なルーティングおよびアクセス制御リスト（ACL）を構築する。

本接続においては、公衆インターネットを一切経由せず、キャリアの閉域モバイル網から NTT のフレッツ・VPN 基盤を経由して庁内ネットワーク境界へ引き込まれる構成を維持する。最上位 UTM 側において、閉域 SIM 網からの流入トラフィックを識別・集約し、次期 ICT インフラの各論理セグメントへ適切にルーティングするネットワーク設計を実施する。

②最小権限原則に基づく厳格な ACL(アクセス制御)設計

閉域 SIM を経由して接続される端末群から庁内リソースへのアクセス制御においては、ゼロトラストの思想に基づき「最小権限の原則」を徹底した ACL を定義・適用する。

【業務・セグメント別の通信許可制限】

接続端末がアクセス可能な宛先を、各現場業務（介護認定調査、工事打合せ、選挙管理システム等）に必要な特定のサーバ・VDI セグメントのみに限定する。不要なセグメント（番号利用系、管理系、他業務 VDI 等）への横断通信は ACL により制限する。

【ポートおよびプロトコルの限定】

VDI 画面転送プロトコルや特定のセグメント、IP アドレス、ポートのみを許可し、その他の IP 疎通を許可しない設計とする。

③端末セキュリティと適用業務の維持

本接続環境において利用する端末については、従来とおりシンクライアント（Chromebook 等）または専用端末を基本とし、ローカル環境へのデータ保存を許可しない無痕跡運用を徹底する。これにより、可搬型モバイルルーター（Wi-Fi 接続）を介した現場運用（介護認定訪問調査、現場写真・図面共有、期日前投票所の投票事務等）における高度なデータ保護と利便性を両立させる。

6-3. テレワークおよびマルチベンダー・リモート保守基盤

6-3-1. テレワーク用リモートアクセス基盤(固定 IP・VDI 連携)

①アクセス方式と専用 VM を必要としない構成

在宅勤務や出張先等の庁外から安全に業務を遂行するためのテレワーク基盤として、新たな専用の仮想マシン（VPN アクセスサーバ等の VM）を仮想基盤上に構築することなく、LBO 用に設置する UTM または VPN 機器の機能を活用したセキュアなリモートアクセス環境を構築する。

庁外からのアクセスにあたっては、専用に設計された「テレワーク専用PC」を用い、クライアントソフトウェアから本市の固定グローバル IP アドレス（「フレッツ光クロス／OCN」回線）宛て、SSL-VPN 接続を確立する。

本構成により、テレワーク専用の認証サーバや VDI ゲートウェイ用の仮想マシン（VM）を個別に保持・維持管理する必要がなく、仮想基盤側の CPU・メモリリソースおよびソフトウェアライセンス等のコストを一切消費しない、シンプルで強固なリモート構成を実現する。

②庁内 VDI 環境との連携によるデータ持ち出し防止

VPN 認証および端末認証が成功した後、通信は UTM を経由して直接庁内 LAN の「LGWAN 系 VDI」へと引き継がれる。接続ユーザーは、庁内 LAN で通常のシンクライアント端末を利用する際と同一の運用フローにより、自身の「個人用 VDI 環境」へログインして業務を行う。

実際の業務処理およびデータ保存はすべて仮想基盤上の VDI 内部で完結し、庁外の専用 PC へは画面の描画データ（画面転送プロトコル）のみが暗号化されて送信される。これにより、専用 PC 側へのファイルダウンロードやローカルストレージへの保存を構造的に遮断し、端末の紛失・盗難が発生した場合であっても情報流出を 100%防止する安全な小規模運用を最小限のコストで確立する。

6-3-2. NGN 網内 DDNS/VPN を活用した低コスト・マルチベンダー保守回線

①NGN 網内 DDNS/VPN を活用した通信構成

本市 ICT インフラ基盤自体のリモート保守をはじめ、庁内オンプレミス環境で稼働する各種業務システムに対するリモート保守を一体的に実現するため、NTT の「NGN 網内ダイナミック DNS（DDNS）機能」を活用した VPN 接続基盤を構築する。

本方式は、インターネットを経由させることなく、NGN 網内で提供される名前解決機能（DDNS）を用いて、各保守ベンダー拠点と本市との間で直接セキュアな VPN トンネルを構築する手法である。

なお、各業務システムのリモート保守のための VPN 機器の調達と設定は、業務システムベンダーが行う。

②回線コストの圧縮とベンダー間セキュリティの独立確保

従来のように、システムベンダーごとに独立した保守用物理回線を個別に契約・導入する方式を廃止し、本市が提供する 1 本の物理回線（フレッツ光クロス）をすべての保守ベンダーで論理的に共有する方式とする。

これにより、毎月発生する回線維持費（ランニングコスト）を大幅に圧縮し、コストの最適化を実現する。回線共有に伴うセキュリティリスクに対しては、回線終端装置（ONU）配下に各ベンダーが調達する専用 VPN 機

器を個別に配置（接続）させるとともに、庁内コアスイッチおよび最上位 UTM において VLAN 分離とアクセス制御（ACL）を厳格に適用する。

さらに、対象システムのサーバと VPN 機器も庁内 LAN 内で VPN 接続することで、各ベンダーは自社の担当する対象システムへのみアクセスが許可され、他の業務システムや別ベンダーの保守領域への横断通信は L2/L3 レベルで遮断される。この方式により、コスト削減と極めて高度なセキュリティの確保を両立したマルチベンダー保守基盤を実現する。

6-4. 将来の回線分離・WAN 構造変化への適応設計

6-4-1. 回線多目的利用からの将来的な分離・拡張

①NGN 網内 DDNS による自動追従と VPN 自動確立の仕組み

NTT の NGN 網の環境においては、フレッツ回線に割り当てられる IPv6 アドレスは半固定（動的）であり、VPN 機器の更新や NTT 収容局内の構成変更等によって割り当てアドレスが変動する特性を持つと考えられる。これに対し、本 ICT インフラのリモート保守基盤等で採用する「NGN 網内 DDNS（ダイナミック DNS)」サービスは、固定のドメイン名（ホスト名）と動的に変化する IPv6 アドレスを、NGN 網内の DNS サーバ上で自動的に紐付け・同期させる仕組みである。

対向する VPN ルーター等の装置は、NGN 網に接続された時点で自身の最新 IPv6 アドレスを網内 DDNS サーバへ自動登録・更新する。VPN 接続時には IP アドレスの直接指定ではなく設定済みのドメイン名を宛先として名前解決を行うため、WAN 側の IPv6 アドレスがどのように変動しようとも、自動的に最新アドレスが特定され、装置間で暗号化 VPN トンネルが即座に確立・維持される。

②WAN 側変化（IPv6 アドレス・回線変更）の完全隠蔽と LAN 側影響ゼロ化

この NGN 網内 DDNS および網内折り返し VPN の自動追従機能により、将来的な通信量増大に伴い LBO 用・テレワーク用・リモート保守用などの回線を物理的に分離・増設した場合や別のフレッツ回線へ繋ぎ替えて WAN 側の IPv6 アドレスが変更された場合であっても、以下のとおり庁内 LAN 側への影響を完全に抑えることができる。

【動設定変更の完全不要化】

網内 DDNS が WAN 側の IPv6 アドレス変動や回線変更をリアルタイムで自動的に検知し更新するため、WAN 側の変化に伴って UTM やコアスイッチ側のルーティングポリシーを手動で修正・再設定する必要がない。

【庁内 LAN 側への影響の抑止】

VPN トンネル内部を通過する庁内 LAN 側の通信（IPv4/IPv6 プライベー

ト IP 体系）はカプセル化されて伝送されるため、内部ネットワーク（コアスイッチ、VLAN、各エンドポイント端末、VDI 環境等）からは WAN 側の IPv6 アドレスの変更や回線切り替えの事実そのものが全く見えず、影響も一切受けない。

第 7 章　保守・運用サポート

7-1. 保守・運用サポートの基本方針と契約境界の定義

7-1-1.「別途契約事項の明示」による曖昧さの排除

①従来の契約における課題と認識齟齬の防止

情報システム調達の保守・運用サポートにおいて、「軽微な設定変更や作業は保守範囲に含める」といった曖昧な文言で契約を締結した場合、受託者側が「当該作業は原契約の範囲外である」と解釈し、発注者側との間で認識の齟齬が生じるケースがこれまでも繰り返されてきた。

現実的に、すべての想定作業を契約書に記載することは不可能であり、あらゆる作業を想定した曖昧な文言にならざるを得ない。このような曖昧さは、軽微な運用作業であるにも関わらず、高額な追加費用の発生や、作業の実施可否を巡る不要な協議・手続きによる時間の浪費を招き、行政サービスの継続性に著しい支障を及ぼすリスクとなる。

②明示的リスト方式によるサポート範囲の適正化（包括的保守契約）

次期 ICT インフラ基盤における保守・運用サポート契約においては、こうした曖昧さを根本から排除するため、設計思想を一新する。具体的には、「明確に別途契約と規定した事項（契約対象外事項の明示）以外は、すべて原契約内の保守・運用サポート範囲に含まれる」という、原則保守・サポートに包含するという要件を定める。

本方式により、原契約に明記された保守作業項目のみならず、日常運用の中で発生する各種設定変更や調査・調整作業を原契約の範囲内として確実にカバーし、発注者・受託者双方にとって契約解釈の揺らぎがない強固かつ明朗な運用管理体制を構築する。

7-1-2. 新規参入リスク費用の抑制（実績頻度データの開示方針）

①包括的保守契約に伴う参入障壁および価格高騰リスクの解消

「明示された別途契約事項以外のすべての運用作業を原契約に含める」という包括的な契約形態を採用した場合、既存ベンダー以外の新規参入事業者にとっては、「契約期間中にどの程度の作業負荷や設定変更作業が発生するか予測がつかない」という過度なリスクを負うことになる。その結果、リスク回避のために想定作業費用（リスク費）の過大な積算を招いたり、プロポーザルへの参加辞退によって競争性が低下したりする懸念が生じる。

②依頼実績および頻度データの開示

本市においては、公平・公正かつ透明性の高い競争環境を維持し、新規参入事業者が適正な価格を見積もることができるよう、本市が日々の運用の中で保守ベンダーへ依頼している「実際の作業内容とその発生頻度」に

関する定量的データ（参考情報）を仕様書および調達資料において明確に開示する方針とする。

これにより、既存ベンダーのみが知る情報の偏りを解消し、参入意欲を持つすべての事業者に対して客観的な根拠に基づくリスク積算を可能とさせることで、適正な価格競争と費用の最適化を実現する。

7-1-3. 保守体制とオンサイト・リモートハイブリッド運用要件

①完全リモート保守の禁止とオンサイト要件の維持

保守・運用サポート体制の構築にあたっては、庁内ネットワークやサーバ基盤の即時復旧、物理トラブル対応、および情報管理部門との密接な意志疎通を確保するため、「完全リモート（非対面）のみによる保守体制」は不可とする。

常駐による保守までは求めないものの、運用期間中を通じて「最低でも週 1 日以上のオンサイト（市役所庁舎への来庁）保守」を継続・維持することを必須要件として定義する。

②オンサイトとリモートを組み合わせたハイブリッド運用の確立

定期的なオンサイト訪問日においては、対面による定例打ち合わせ、対面での運用改善協議、物理機器や配線の状況確認、および庁内環境でしか行えない作業等を重点的に実施する。

一方で、定期訪問日以外の日常的な監視、問い合わせ対応、ソフトウェア設定変更、および緊急時の障害一次対応については、暗号化された専用回線を介した「リモート保守環境」を有効活用する。このオンサイトとリモートを融合させたハイブリッド保守運用を確立することで、保守品質とコスト効率の双方を両立させる。

7-2. 通常契約に含まれる保守・運用サポート範囲

本項では、前項に記載した「包括的保守契約」に基づき、次期 ICT インフラ基盤の運用において契約の範囲内として受託者が恒常的に提供すべき保守・運用サポートの具体的な内容を定義する。

7-2-1. システム・インフラ管理および設定変更作業

庁内 ICT インフラを構成する、すべてのシステムおよびネットワーク環境に対する日々の管理、ならびに運用上必要となる設定変更作業を網羅的にサポートする。

具体的には、ネットワーク機器群（コアスイッチ、フロアスイッチ、ルーター、UTM 等）のパラメータ変更、VLAN の追加・変更・削除等の論理ネットワーク構成の管理、Wi-Fi 環境（アクセスポイント等）の稼働管理および設定調整を含む。また、Active Directory（AD）におけるユーザー・

グループ・ポリシーの管理、および仮想デスクトップ（VDI）基盤のリソース割り当てや展開・構成変更など、インフラ基盤全体の中核となる管理業務および設定変更作業を契約の範囲内として確実に実施する。

7-2-2. システム保守・パッチ適用・適宜チューニング

ICTインフラ基盤のセキュリティレベルと稼働安定性を恒久的に維持するため、各種システムおよび機器の定期的な保守作業を実施する。

対象となるすべてのネットワーク機器、サーバOS、ミドルウェア、および仮想化ソフトウェアに対するバージョンアップ検証および計画的なパッチ（更新プログラム）適用作業を含む。さらに、日々の監視データやリソース稼働状況に基づき、システムのレスポンス低下やボトルネックの発生を未然に防ぐためのパフォーマンス調整（適宜チューニング）を定常的に実施し、常に最適なシステム状態を保持する。

7-2-3. 障害対応および予防保全（SLA要件）

システム障害やネットワーク切断等のインシデントが発生した際の迅速な復旧対応、および障害を未然に防ぐための予防措置を契約範囲内の業務として実施する。

障害発生時には、アラート検知および市からの申告に基づき、即座に障害箇所の一次切り分け（ハードウェア、ソフトウェア、ネットワークのいずれに起因するかの特定）および各種ログの解析を行う。ハードウェア故障と判定された場合は、迅速にメーカーや保守ベンダーへの修理手配・交換対応を主導する。また、事後的な障害対応にとどまらず、システムの劣化兆候や異常ログを事前に検知し、部品の予防交換や設定見直し等の「予防保全（定期点検）」を実施することで、業務への影響を最小化する（SLA達成要件）。

なお、障害原因が責任分界の範囲外の可能性があった場合でも、庁内ICTインフラが原因である可能性がある場合は、一次切り分けのための調査を実施する。

7-2-4. 主要機器のメーカー保守要件（構築１年＋運用６年）

次期ICTインフラ基盤を構成するサーバ（ホストマシン）、ストレージ、および各種ネットワーク機器（コアスイッチ、UTM、ルーター等）の主要ハードウェアについては、本市が想定するシステム・ライフサイクル全体を通じて、メーカーによる正規のサポートが継続されることを必須の要件とする。

①「計７年間」のメーカー保守体制の確保

前・後期の契約における事業工程は、「構築・移行期間（1年間）」およ

び「本稼働・運用期間（6 年間）」で構成される。したがって受託者は、これらを合算した「計 7 年間」にわたり、メーカーによるハードウェア保守（代替部品の供給・修理）およびソフトウェア保守（ファームウェア・セキュリティパッチの提供）が受けられる機器を選定しなければならない。

②運用途中のサポート終了（EOL）の排除

コスト圧縮を目的として、6 年間の運用期間中にメーカーサポートが終了（End of Life）する製品、または最大保守年数が 7 年に満たない製品を選定することは禁止する。万が一、受託者の選定した機器が期間途中でサポート終了となった場合においても、本市に対する「ベストエフォート（可能な範囲での保守）」による責任回避は認めず、受託者の責任と費用負担において、有償修理または同等以上の性能とサポートを有する機器へ無償で交換・対応する義務を負うものとする。

7-2-5. エンドポイント（端末）管理・保守および修理手配

全庁に配備される端末（シンクライアント、FAT 端末等）のライフサイクル全般に関わるソフトウェア的・物理的な保守管理を包括的に実施する。

①ソフトウェア保守および年度更新

端末の各種設定変更、OS およびクライアントに導入済みのソフトウェアのアップデート・パッチ適用作業を実施する。また、年度初めに行われる大規模な人事異動や組織改編に伴う、ユーザーの所属情報や権限変更等の「年度更新処理」を実施する。

②物理保守および修理手配（オンサイト対応）

全端末に対し、「5 年間・翌営業日オンサイト修理対応」を基本要件とする。日常的な利用で発生しやすい「キーボードのキートップ外れ」「LAN ケーブル差込口（NIC）の爪折れ」「電源（AC）アダプタ不良」といった軽微な物理損傷についても、保守の対象範囲に含め、無償での部品交換や修理対応を行う。なお、翌営業日オンサイト修理対応とはいっても、修理部品の状態により修理日数がかかる場合があるため、事前に予備機の準備は必須である。特に番号利用系については、業務の非効率化への影響が大きいため、故障時に確実に予備機を配置できるよう機器を整備する必要がある。

メーカーのオンサイト修理対応の上限が 5 年間であることを踏まえ、「運用開始 6 年目」に発生した端末の物理故障については、受託者による無償保守の対象外とする。運用 6 年目における故障機器への対応については、本市の費用負担に基づく個別のスポット有償修理、予備機との交換、または部分的な機器更新（買い替え）のいずれかの措置を講じることで業務を継続する。

③過失破損時の動産保険活用

落下や水濡れ等、職員の過失に起因する破損事故が発生した場合は、リース会社が付保している動産総合保険を活用するための事故報告書の作成支援、リース会社との折衝、および修理手配等の手続き一式を保守業務の一環として代行する。

④Microsoft 365(M365)ライセンス対応

M365 ライセンス自体は別途入札により調達する予定であるが、インフラ保守受託者は、当該ライセンス落札者と緊密に連携・調整を行う義務を負う。ライセンスのシームレスな引き継ぎや、庁内インフラと M365 を連携させるためのネットワーク・AD 等の設定変更作業は、本インフラ保守契約の範囲内として確実に実施する。

7-2-6. 運用管理・月次定例会(SLA・課題管理)

日常の保守作業に加え、インフラ基盤全体の健全性や運用上の課題を市と受託者間で共有・解決するため、定期的な運用管理業務および「月次定例会」の開催を行う。

月次定例会においては、以下の項目を網羅した月次報告書（レポート）を提出・報告する。なお、月次定例会の開催形式については、業務効率化および環境配慮の観点から、オンライン会議システムを用いたリモート開催、ならびに電子データ（PDF 等）を用いたペーパーレスでの実施を推奨する。また、定例会終了後には受託者が速やかに議事録を作成し、市と合意形成を図るものとする。

【保守内容の報告】

当月に実施した設定変更、パッチ適用、障害対応等の作業実績。

【リソース状況の報告】

CPU、メモリ、ストレージ、セキュリティログ等の各種リソースの利用状況と将来予測。

【イベントスケジュール】

翌月以降に予定されているメンテナンス、機能更新、および ICT インフラ関連の全体スケジュール。

【課題管理】

現在発生しているシステム上・運用上の課題とその解決に向けた対応方針・進捗管理。

【SLA 報告】
事前に合意した SLA(サービスレベル合意書)の達成状況の客観的評価。

7-3.【参考情報】日常運用における本市からの依頼作業実績と想定頻度

7-3-1. 本市依頼作業の性質と提示の目的

①本市依頼作業(SE 対応依頼)の定義

システムが正常かつ安定的に稼働し続けるために、当然発生する日常的な監視やハードウェアの維持管理等の「通常稼働に必要な保守作業」は、受託者が提供すべき標準業務として契約に含まれる。

本章で開示する「本市依頼作業」とは、こうした標準業務となる保守作業とは異なり、日々の運用の中で本市の業務内容の変更、新規事業の開始、組織・システムの追加、新たな機器の追加による設定変更、その他チューニング等、市職員では対応が困難な高度な技術的作業について、本市から受託者の技術者へ個別に依頼・実施を要請する作業項目を指す。

②実績データの開示目的と効果

前述のとおり、「包括的保守契約」のもとで保守契約を締結する際、新規参入事業者が過去の実際の作業負荷を把握できず、リスク費用を過大に積算することを防止する目的で現在の状況を開示する。

本市からの個別依頼に基づく、主だった作業内容と過去の定量的頻度の情報を事前に公開することで、提案者が実態に即した適正なリソース配置とコスト積算を行える環境を整え、特定の現行ベンダーに有利とならない公平かつ透明性の高い調達を実現する。

7-3-2. 想定作業内容と年間実績頻度データ

①主な個別依頼作業項目と想定発生頻度

過去の運用実績および次期 ICT インフラ基盤の運用想定に基づき、本市から受託者へ依頼する可能性の高い SE 対応作業の具体的な内容および想定発生頻度は、下表のとおりである。

依頼作業項目	具体的な作業内容・範囲	想定発生頻度 (参考実績)
新規 VLAN およびルーティングの作成・保守	特定の業務や機器接続のために新たなネットワークセグメントを定義し、コアスイッチや UTM へ VLAN 設定およびルーティングを設定・適用する作業。	年 1～2 回程度
UTM 内簡易プロキシ・DNS プロキ	UTM 内部に搭載されている簡易プロキシ機能や DNS プロキシ機能等に関する各	5 年間で 1～2 回程度

依頼作業項目	具体的な作業内容・範囲	想定発生頻度（参考実績）
シ等の作成･保守	種設定の新規作成、パラメータ変更、および保守作業。	
UTM セキュリティルールの追加･削除	業務アクセス制限の見直しや新たな外部サービス連携に伴う、UTM のアクセス制御リスト（ACL）やファイアウォールルールの追加・修正・削除作業。	年 5 回程度
市購入の L2 スイッチおよびルーター等への設定	市が独自に新規購入または移設した L2 スイッチやルーター等に対し、本市ネットワーク環境（VLAN、QoS、D-VLAN･IPSG 等）に適合させるためのパラメータ設定・投入作業。	5 年間で 1～2 回程度
Active Directory（AD）設定変更	人事異動の時期以外の随時発生する端末・ユーザーの個別追加、運用変更に伴うグループポリシー（GPO）およびログオンスクリプトの作成・適用、新たなセキュリティグループの追加作成作業。	年 12 回程度（月 1 回程度）
PAC ファイルの修正	Web アクセス時のプロキシ自動構成ファイル（PAC ファイル）における記述内容の修正、振り分けルールの変更・適用作業。	年 5 回程度
Web アクセス等の例外設定	セキュアブラウザや Web フィルタリングにおいて、無害化処理やブロック処理の対象から特定の業務サイト等を外すための例外アクセスルールの追加･調整作業。	年 12 回程度（月 1 回程度）
新規システム導入に伴う NW 設定および VM デプロイ	新たな業務システムやネットワーク機器の庁内導入に伴うインフラ側の設定変更･追加、および仮想基盤上への OS 標準状態（プレーン）の仮想マシン（VM）のデプロイ（展開）作業。	年 1～2 回程度
Microsoft Entra ID 利用のための設定	Salesforce の認証を Entra ID と紐づけるため、専用仮想サーバを構築し、端末の証明書の取得設定を行った	5 年に 1 回程度
職員のミス等によるネットワーク障害の原因調	職員が誤ってループを起こすなど瑕疵による障害を発生させた場合、障害発生時の原因調査・復旧作業	年 1～3 回程度

依頼作業項目	具体的な作業内容・範囲	想定発生頻度（参考実績）
査・復旧		
IP 電話の品質低下による原因調査・対策	庁内 LAN 上で運用している IP 電話の品質に問題がある場合、パケットキャプチャおよびデータ解析を行う。また、原因が判明しない場合でも、想定される対策を検討し、市と協議の上実施する。	5 年で 3 回程度

※上記に記載のない作業であっても、次項で明示する「別途契約（当初契約対象外）要件」に該当しない作業については、すべて原契約内の保守・運用サポート範囲として取り扱うものとする。なお、軽微な作業は、市職員が実施する場合がある。

②SLA およびインセンティブ評価との連携

本市から受託者へ依頼するこれらの作業については、単に作業の遂行を求めるだけでなく、依頼から作業完了までの対応速度、設定の正確性、ならびに事前・事後の連絡調整の確実性、実施した内容の効果などを総合的に考慮し評価対象とする。

具体的には、上記依頼作業の迅速かつ確実な遂行実績およびその効果を本 ICT インフラにおける「SLA（サービスレベル合意書）のインセンティブ評価ポイント」の対象項目として組み入れる。優れた対応を実施した受託者に対しては SLA 上の評価インセンティブを付与する評価基準を導入することで、運用期間中の保守品質の維持および受託者の改善意欲の向上を構造的に促進する。

どのような作業をインセンティブの対象とするかは、協議の上決定する。

7-4. 別途契約（当初契約対象外）とする要件と実績事例

7-4-1. 過去に別途契約として実施した環境変更実績

①過去の別途契約事例提示の趣旨

本章で定めた「包括的保守契約」に基づき、次期 ICT インフラ基盤の運用においては、明確に別途契約と規定した事項以外の作業は、すべて原契約の保守・運用サポートの範囲に含まれる。受託者が事前にその費用負担やリスク範囲を正しく予見できるよう、過去の ICT インフラ運用においてどのような規模・内容の環境変更作業が原契約から切り離され、別途見積・別途契約として実施されたか、その具体的事例を提示する。

②主な過去の別途契約実績事例

過去に原契約の範囲を超えて、個別調達および別途契約により実施した

主な構築・改修事例は以下のとおりである。

【全庁 LAN の無線化工事】
全庁舎への無線アクセスポイント（AP）の新規調達・設置工事、認証基盤（RADIUS 等）の新規構築・調達、それに伴う全庁的な新たな VLAN の設計、LAN 配線・物理取り付け工事および全配備端末への接続設定変更作業一式。

【クラウド PBX 導入に伴う専用ネットワークの全庁追加】
全庁的なクラウド PBX 導入(IP-PBX の更改)に伴い、既存ネットワーク内に独立した「IP 電話系セグメント」を新規に全庁規模で設計・追加し、専用ルーター・スイッチの調達および調整を行った作業。

【専用線の更新・切り替えに伴う段階的なルーティング変更作業】
本庁舎と出先機関等を結ぶ広域イーサネット・専用線の回線サービス変更に伴い、回線切り替えの工程に合わせて複数日程にわたりルーティング情報やパラメータを順次更新・変更していった大規模な切り替え作業。

【教育情報ネットワーク（学校系）との境界セキュリティ設置・構築】
教育情報ネットワーク（学校系）と庁内 LAN の境界部に、相互通信のためのファイアウォール（FW）およびネットワークストレージ（NAS）を新規設置した際における FW 機器の調達およびポリシー設計・設定作業（※庁内 LAN 側の既存スイッチ設定変更については通常保守の範囲内として実施し、NAS の調達・設定は市が直接実施）。

7-4-2. 次期契約において明確に「別途契約」と規定する要件

①別途契約となる明確な区分基準の定義

次期 ICT インフラ保守契約においては、受託者と本市との間で「どこまでが通常保守で、どこからが別途契約か」の判断基準を明確にするため、原契約の対象外とし、別途の見積および個別契約締結を必要とする要件をリスト化し明確に規定する。

なお、契約に当たっては、別途契約または変更契約のいずれかの方式とする。

以下の 5 つに条件に直接該当しない作業・対応については、その規模の軽微・重大に関わらず、すべて原契約内の保守・運用サポートの範囲として実施するものとする。

②別途契約対象となる具体要件

(1)全庁に渡る新たなセグメント・ネットワーク構造の設計および大規模追加

クラウドPBX全庁導入や全庁無線化と同等規模の事業であり、庁内LAN全体の設計思想の変更や全庁規模での新たなネットワーク系統（VRF・セグメント）の新規設計・構築を伴う大規模な環境変更作業。

ネットワーク変更であっても、部分的なVLANやルーティングの追加などは、通常保守の範囲内で作業を行う。

(2)新たなネットワーク機器本体の購入費用

スイッチ、ルーター、UTM、アクセスポイント等の機器本体の調達（新規購入）費用。ただし、単発・小規模で追加設置される機器に対する設定作業や上記(1)のようなネットワーク全体の設計思想の変更が部分的であり、設定やパラメータ投入作業の場合、この設定作業は、機器の調達ルートに関わらず通常保守の範囲内で作業を行う。

(3)追加端末の物理購入費用および大規模キッティング費用

事業拡大や職員増員に伴うクライアント端末（PC、シンクライアント等）の新規本体購入費用、および数十台規模を一括構築するためのマスター作成・キッティング作業費用。ただし、少数の端末追加であり、個別の設定登録等で対応可能な小規模対応（キッティング作業を伴わないもの）については、通常保守の範囲内で作業を行う。

(4)原契約に含まれていない未想定の新しいソリューションの新規導入･構築費用

原契約の調達仕様書に含まれていない、全く新しいカテゴリのセキュリティソリューションや運用管理ソフトウェア等を変更契約により新規に導入・構築する費用。

(5)国の交付金･補助金を活用して実施する特定事業

国からの交付金や補助金を財源として、特定目的にて実施されるシステム構築・改修事業。ただし、この場合の別途契約金額の上限は、国が定める補助対象事業費の範囲内とする。なお、特別交付税措置の事業は別途契約の対象とするが、普通交付税の算定基礎に入る事業については、特定事業の対象とはしない。