延岡市サーバルーム整備運用業務

委託仕様書

延 岡 市

４．２　ハウジング対象が想定されるシステム----------20
４．３　監視・基本オペレーション----------22
４．３．１　監視サービス----------22
４．３．２　オペレーションサービス----------22
４．４　バックアップ作業----------22
４．５　利用ラック数の想定----------22

第５章　スケジュール
５．１　IT 機器移設スケジュール ----------23
５．２　必須要件----------23

第６章　IDC における管理体制
６．１　必要な管理機能----------24
６．２　管理体制イメージ----------24
６．３　監査----------25

第７章　コンピュータルームセキュリティポリシーについて
７．１　目的----------26
７．２　コンピュータルームに関する指針----------26
７．２．１　対象者----------26
７．２．２　対象システム----------26
７．２．３　コンピュータルームの定義----------26
７．２．４　コンピュータルームの物理的セキュリティ----------26
７．２．５　コンピュータルームの運用----------27
７．３　物理的対策に関する指針----------27
７．３．１　対象者----------28
７．３．２　対象システム----------28
７．３．３　遵守事項----------28
７．４　クライアント PC における接続条件の指針----------29
７．４．１　対象者----------29
７．４．２　遵守事項----------29
７．４．３　クライアント PC の他者への利用制限----------30
７．５　媒体の取扱に関する指針----------30
７．５．１　対象者----------30
７．５．２　対象システム----------30
７．５．３　遵守事項----------30
７．６　例外事項----------31
７．７　罰則事項----------31

第８章　IDC 使用に伴う管理手順書について
８．１　管理手順書----32
８．２　管理手順書の必要性----32
８．３　管理手順書の内容----32
８．４　管理手順書の更新----40

第９章　SLA の概略
９．１　SLA について ----41
９．１．１　目的----41
９．１．２　検討方針----41
９．２　SLA の概略構造 ----41
９．３　SLA のサイクル ----42
９．４　IDC における SLA 分類 ----44
９．５　SLA の留意点 ----44
９．５．１　ペナルティについて----44
９．５．２　免責事項----54

第１０章　SLA 評価項目と設定値
１０．１　ホスティング----45
１０．２　セキュリティ----47
１０．３　ネットワーク----49
１０．４　ハウジング----50
１０．５　サービスサポート----58
１０．６　SLA 関連提出資料 ----59

第1章　概要

1.1　目的

2001年のe－JAPAN戦略に始まり、e－JAPAN戦略Ⅱ、2006年のIT新改革戦略と次々と政府はIT戦略を展開しており、延岡市においても、CATV網整備による市内全域ブロードバンド化実現に代表される、高度情報化の推進と情報ネットワークシステムの整備が着々と進められている。

本事業は、共同利用サーバルームを整備・運用することによって、これまで各システムごとに独自に購入し運用していたハードウェア類及び設備を共同利用化し、各システムを一元管理・運営することにより、高いセキュリティレベルの確保と、施設設備整備及び管理運営コストの重複投資を抑制することを目的としている。

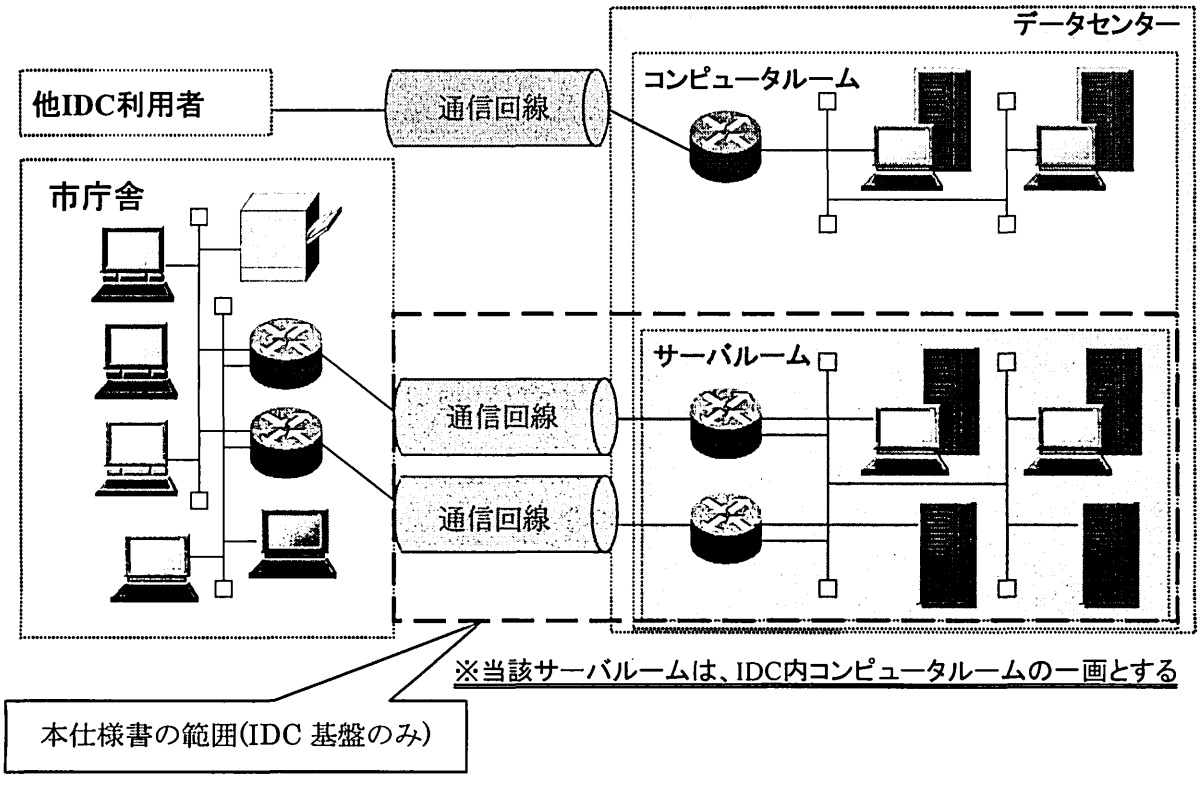
当該サーバルームは、高度なセキュリティ対策・堅牢なファシリティを有する民間インターネットデータセンター（以下「IDC」という。）内のコンピュータルームの区画されたスペースに整備することを想定している。

本仕様書は、IDCの機能要件を整理した上で、評価・運営・管理におけるSLAの検討についても記しており、各社はそれらを遵守した形で具体的な計画立案を提出すること。

1.2　全体イメージ

本仕様書にて想定されているシステムの全体イメージは以下のとおりである。

図表1.2　全体イメージ図



第2章　基本方針

2.1　IDC の構成要素の検討

IDC へサーバルームをアウトソーシングするにあたり、運用における安定性・信頼性を確保するために、下記項目について検討が必要となる。なお、アプリケーションに関しては業務ごとに検討が必要であるため、今回の検討の対象外とする。

① ホスティングサービス
② セキュリティサービス
③ ネットワークサービス
④ ハウジングサービス
⑤ サービスサポート

第3章　IDC 基盤に係る要求仕様

3.1　ホスティングの検討

本事業でのホスティングによる機器提供サービスについては運用に関する機器のみを想定している。ホスティングサービスとは、IDC 所有の資産（ハードウェア・ソフトウェア）の提供及び利用者(延岡市)の資産であるサーバ類の情報システムのオペレーション・バックアップサービスを提供するものである。

3.1.1　基本的な考え方

IDC で利用されるサーバは、利用形態によって必要なサーバの種類や諸元が異なる。したがって妥当な水準の仕様を個別に検討する必要がある。

現状想定している以下の機器については市側での個別運用負荷をかんがみ、IDC の共通性の高さから、IDC からのホスティングサービスとしての提供を想定している。

3.1.2　ホスティング対象範囲

以下の（1）～（5）については、IDC 事業者の基盤サービスとして提供されることを想定している。「3.1.3 対象サービス」については、IDC に導入するシステムに対し共通的に利用可能なサービスとしての提供を想定している。

（1）運用管理サーバ

IDC 内の各運用管理業務における機能を提供する。

①機器情報管理

機器の型名、ソフトウェア名・バージョン、各機器の OS・インストールソフトウェア・バージョン、パッチ等作業履歴を管理できること。

②インシデント管理

問い合わせ申告・履歴、障害申告内容・履歴、障害対応経過・履歴を管理できること。

③その他

入館管理、ラック実装管理、評価室の予約管理を行うこと。

運用管理サーバを複数台準備することにより、障害発生時は、他の運用管理サーバにより継続利用が可能なこと。

④システムコンフィグレーション等のバックアップについては以下のルールのもとで実施すること。

a) コンフィグレーション情報

ルール：各種設定変更やパッチ等のコンフィグレーション情報の設定・変更時にフルバックアップを実施。

b) データ

ルール：日次で実施。

（２）運用監視サーバ

①サービスを運用するネットワーク機器およびサーバに対して、サーバの死活監視、システムリソース監視、メッセージ監視、プロセスの死活監視、トラフィック監視を行うこと。

②運用監視サーバを複数台準備することにより、障害発生時は他の運用監視サーバにより継続利用が可能なこと。

③システムコンフィグレーション等のバックアップについては以下のルールのもとで実施すること。

a）コンフィグレーション情報

ルール：各種設定変更やパッチ等のコンフィグレーション情報の設定・変更時にフルバックアップを実施。

b）データ

ルール：日次で実施。

（３）監視用ターミナルサーバ（TS）

①IDC 基盤の各ネットワーク機器、各種サーバのメンテナンス用として使用すること。

②コールドスタンバイ機を準備し、障害発生時には、コールドスタンバイ機により運転再開可能なこと。

（４）管理コンソール

①オペレータが運用管理を行うための汎用的な PC コンソールを用意すること。

②管理コンソールを複数台準備することにより、障害発生時は、他の管理コンソールにより継続利用が可能なこと。

（５）リブーター

①予め登録した任意のスケジュールにて、市庁舎よりサーバの定期シャットダウンとサーバの定期リブートが可能な機器を用意すること。（例：月～金 6：00 起動 22：00 終了）

3.1.3 対象サービス

ホスティングはアプリケーション毎に業者が異なることが想定されるため、サービス要件に関しては業者毎に個別に運用ルールを規定する。

（１）機器提供サービス

ホスティングサービスを実施するにあたり、ホスティング業者資産のハードウェアを提供し、監視を実施する。

機器提供サービスにおいては、障害監視、サービス時間、レポーティングといった要件を定める必要がある。

①機器種別

パフォーマンス要件、稼働要件に合致する、サーバ、ワークステーション、ネットワーク機

器を選択・構成する。システムの必要性に応じて、高可用性、高パフォーマンス、負荷分散環境も選択する。

②障害監視

Pingによる応答確認、監視ツールによる障害監視を行う。

③サービス時間

機器のサービス時間を規定する。設備、ネットワーク等の点検、保守のための計画停止時間、計画停止通告期間・方法、稼働率を規定する。

④レポーティング

障害時、発生した障害への対応状況（インフラ、サーバに発生した障害の内容、発生理由、対応経緯、実施作業等）を報告する。

なお、問題状況報告は、予め設定した重要度、緊急度の高いものに適用する。

（2）ソフトウェア提供サービス

ホスティングサービスを実施するにあたり、ホスティング業者資産のソフトウェアを提供し、ホスティング業者が監視を実施する。

ソフトウェア提供サービスにおいては、障害監視、サービス時間、レポーティングといった要件を定める必要がある。

①ソフトウェア種別

パフォーマンス要件、稼働要件に合致する、OS、ミドルウェアを選択・構成する。システムの必要性に応じて、高可用性、高パフォーマンス、負荷分散環境も選択する。

②障害監視

監視ツールによる障害監視を行う。

③サービス時間

ソフトウェアのサービス時間を規定する。設備、ネットワーク等の点検、保守のための計画停止時間、計画停止通告期間・方法、稼働率を規定する。

④レポーティング

障害時、発生した障害への対応状況（インフラ、サーバに発生した障害の内容、発生理由、対応経緯、実施作業等）を報告する。

なお、問題状況報告は、予め設定した重要度、緊急度の高いものに適用する。

（3）オペレーションサービス

ホスティングサービスを実施するにあたり、運用に必要な定期／不定期の作業代行、機器の稼働監視と予備機への交換を実施する。オペレーションサービスにおいては、定期作業代行、不定期作業代行、機器交換、機器稼働監視といった要件を定める必要がある。

①定期作業代行

サービス利用者が提出した作業手順書に基づき、定期的な作業を実施する。

②不定期作業代行

トラブル対応を行うため、サービス利用者の指示に基づき、不定期な作業を実施する。

③機器交換

機器故障、トラブルシューティングの一環として、予備機への交換を行う。但し、利用者（延岡市）資産を除くものとする。機器交換に際しては、ハードウェア、OS までの復旧をサービス範囲として実施する。

④機器稼働監視

サービス対象機器に対し、運用手順書に基づき、Ping による活性／非活性監視を実施、またオペレータによる LED ランプの確認を実施する。また、サーバ運用に関する監視手順書を作成して提出する。

（4）バックアップ／リストアサービス

災害等によって情報資産を損失する可能性もあるため、データのバックアップ対策について検討し、バックアップ媒体・頻度・保管場所・データ損失の際の復旧対応策等について確認しておく必要がある。また、大規模地震などの広域災害による被害が発生し、行政サービスの業務の継続が困難な場合、代替センタへ切り替えることも考えておく必要がある。代替センタ検討の際は、活断層を越えた地理的に離れた地方自治体同士で、お互いの公共 IDC 同士を補完し合うことも検討する必要がある。

また、データストレージを共有する場合、アプリケーションのデータベースへのアクセスレスポンスやバックアップのタイミングなど、アプリケーションの運用面も考慮し検討する必要がある。

①バックアップ

サービス利用者からの指示に基づき、予め調整した周期、時間にて定期バックアップを実施する。

②リストア

サービス利用者からの指示に基づき、指定されたエリアにリストア作業を実施する。

3.2　セキュリティの検討

セキュリティサービスについてはすべてのサービスレイヤに存在するが、ここでは他のサービスに含まれないセキュリティサービスに関しての検討を行うこととし、対象としては IDC 所有の資産（サーバ・端末）を想定している。但し、運用全般におけるセキュリティ及び監査においては利用者（延岡市）の資産であるサーバ類の情報システムについても対象機器とする。

3.2.1　サーバセキュリティ

（1）ウイルスチェック（サーバ）

サーバ上で扱われる全てのファイルについてウイルス感染のリスクがあり、ウイルス感染ファイルを検知しそこで感染を食い止めるために、ウイルスチェックを行う必要がある。

サービス要件は以下の通りとする。

①専用ソフトによりサーバ上で扱われる全てのファイルに対してウイルスチェックを実施する。
②緊急対応が必要な場合、サービス利用組織の代表者（または窓口担当者）への情報提供及び対応指示を行う。緊急対応が必要な場合の連絡方法、対応方法等をあらかじめ規定する。
③ウイルスチェックサーバの管理は、決められた代表者のみが実施可能とする。
④チェック稼働時間帯はメンテナンスに必要な停止時間を除き端末稼働時間全てとする。
⑤ウイルスパターンファイルのタイムリーな更新を行う。
⑥定期的または不定期なメンテナンスログの提出をあらかじめ規定する。

評価項目は以下の通りとする。
・ウイルスパターンファイルの更新間隔（例）
①ベンダリリースから 24 時間以内
②ベンダリリースから 24 時間以降 3 日以内
③規定しない

注）上記に示した SLA 評価項目と SLA 設定値（例）は、サービス要件「ウイルスチェック」の総合的なサービスレベルを規定するものではなく、その一部を評価するものであり、SLA における取扱には注意が必要である。

（2）OS、ミドルウェアのセキュリティパッチ管理

OS、ミドルウェアにおいてサプライヤーより提供されるセキュリティパッチを適用する。

サービス要件は以下の通りとする。
①OS、ミドルウェアにおいて、サプライヤーより提供されるセキュリティパッチのタイムリーな適用を行う。
②サービス提供事業者は、サービス利用組織の代表者（または窓口担当者）に対しセキュリティパッチ適用に関わる情報提供を行う。

評価項目は以下の通りとする。
・パッチ試験間隔（例）
①ベンダリリースから 24 時間以内にパッチ試験環境を整備の上、パッチ試験を開始。
②ベンダリリースの 24 時間以降 3 日以内にパッチ試験環境を整備の上、パッチ試験を開始。
③規定しない

（3）サーバ上のデータ管理

サービス要件は以下の通りとする。
・サーバ上のデータにつき、漏洩や改ざんを防止し、適正に管理する。
・データの破壊、改ざん、消去等の不測の事態を想定し、定期的にデータのバックアップを取得する技術的な仕組みを備える。
・データ管理に関する運用方法について、あらかじめ取り決める。特に契約終了時のデータの消去や変換方法について取り決める。

評価項目については、本 SLA では規定しない（サービス要件を満たした運用を行うことのみ、合意の対象とする）。

3.2.2 端末セキュリティ

（1）ウイルスチェック

全てのファイルについて、ウイルスチェックを実施する。

（2）認証

本人が使用していることの認証を行う。

3.2.3 運用管理

（1）レポーティング

セキュリティサービスの提供状況（運用状況）に関し、レポーティングを行う。

サービス要件は以下の通りとする。

・サービス提供事業者は、定期的または（要求された場合等）随時に、サービス利用者（延岡市）の代表者（または窓口担当者）へのレポーティングを行う。
・レポートの内容、フォーマット、提出期限等について、あらかじめ取り決める。

（2）媒体や紙に出力した情報等の適正な管理

媒体の管理、処分方法などの取扱手順、またシステムより出力した紙の書類等の情報媒体について、運用に関する詳細な規則を作成し、外部業者と取り交わす。

サービス要件は以下の通りとする。

・情報媒体の運用に関して詳細な規則を作成し、外部業者と取り交わす。
・運用管理に関して、規則が遵守されているか必要に応じて監査を実施し、モラルの維持を図る。

（3）コンピュータルームセキュリティ運用管理手順書

延岡市で定めたセキュリティポリシーに沿って、運用に関する詳細なルールを整理して提出する。

（4）管理手順書の更新

環境などの変化に合わせて、常に更新をする。

3.2.4 セキュリティの確保

情報システムのセキュリティ対策と同様に情報を適切に管理される施策が採られていること。客観的評価として公的基準に準拠していることが望ましい。

（例）ISMS 認証取得

3.2.5 監査

発注者側の監査に対応してSLAの遵守状況を必要時に提出する。

3.3 ネットワークの検討

本事業において、市庁舎～IDC間のネットワークについては、重要なIDC構成要素であり、今回の調達範囲に含むものとする。また、ネットワーク構築する上でIDC側として、必要な受入機器等を整備すること。

3.3.1 市庁舎～IDC間のネットワーク接続

市庁舎～IDC間のネットワークについては、県がIT化推進の政策として構築している宮崎情報ハイウェイ21を延岡市庁舎とIDC間の接続回線として使用することを想定しても構わない。ただし、接続回線については冗長構成が必須条件であり、宮崎情報ハイウェイ21を使用しない別途回線を整備することとする。

（1）サービス要件

①帯域

接続回線の帯域は、100Mbps以上とする。

②冗長

接続回線については、万一の障害に備えて、冗長構成とする。回線についてはバックアップ回線を利用する。

③監視・通報

ネットワークを監視し、障害を通報する時間帯（例:24時間365日）

④拡張性

接続する回線の帯域を増やしたい場合等に、サービス提供事業者が対応可能な期間（例：帯域増速対応を1ヶ月以内で実施）。

3.3.2 バックアップ回線

バックアップ回線についても、今回の調達範囲とし、「3.4.1市庁舎～IDC間のネットワーク接続」において述べたメイン回線とは異なるルートを利用するものとする。

（1）サービス要件

①帯域

接続回線の帯域は、100Mbps以上とする。

②構成

メイン回線とは異なるルートを利用するものとする。

③監視・通報

ネットワークを監視し、障害を通報する時間帯（例:24時間365日）

④拡張性

接続する回線の帯域を増やしたい場合等に、サービス提供事業者が対応可能な期間（例：帯域増速対応を１ヶ月以内で実施）。

3.3.3 その他の接続について

本基本設計において、下記の接続における検討は予定していないが、今後接続の可能性を考慮するため、記述する。

（１）LGWAN との接続

①IDC には、LGWAN 提供設備を設置し、LGWAN - ASP サービスを利用できること。

②IDC は、「LGWAN-ASP」としての条件を満たすこと。

③市庁舎との接続回線は高い信頼性を確保できること。

注：LGWAN においては、アプリケーションが追加された場合、レスポンスにおける問題を考慮する必要がある。

（２）認証基盤との接続

①証明書検証（失効情報の確認）を行うために必要となる。認証サービス（公的個人認証サービス、商標登記に基づく電子認証サービス、電子調達サービスにおいて企業を認証するための民間認証サービス、LGPKI）において「証明書有効性検証局（VA:Validation Authority)」との疎通を図ること。

3.4 ハウジングの検討

本事業では延岡市の情報システムを IDC にハウジングすることを想定している。ハウジングとは、利用者(延岡市)の資産であるサーバ類の情報システムを IDC で預かり、設置スペースや電力・空調などのファシリティを提供するものである。

3.4.1 建築物

耐震性については建築基準法で規定されているが、これは最低基準での耐震性であり、建築基準法に遵守していれば地震に対して安全というわけではない。IDC として使用する建築物は、少なくとも新潟中越地震や阪神・淡路大震災クラスの地震に耐え得る耐震性を備えるべきと考える。また、地震の揺れを吸収し、建物内に収容する機器・装置等の倒壊といった致命的損害を与えない免震構造（免震床など）や制震構造であること。

床荷重については、ストレージを設置する場合を想定して、500kg/㎡以上であり、フロア有効高は、天井下にケーブルトレイを敷設するならば高い方が望ましい。内装は不燃材で施工し、サーバルーム内の床については静電気対策された部材を使用すべきである。

（1）住所

延岡市が保管しているデータを主体的にコントロールすることのできる権限が及ぶ範囲内及び地元の産業育成の観点よりサーバルーム設置場所は宮崎県内にあること。

（2）ビル耐震構造

建築基準法における「新耐震基準」に適合し、震度7クラスの地震に耐え得ることを必須条件とする。

（3）免震構造

地震の揺れを吸収し、建物内に収容する装置等に致命的な損害を与えない耐震性能を保持する方法として、免震構造（免震床など）・制震構造であること。

（4）水害対策

サーバルーム及びそれに関連する施設は、水害を考慮し、防水・排水設備の完備や高床式建築などの構造をとる必要がある。また、建物および内部の IT 機器に影響の及ぼさないような排水設備を完備することが望ましいこと。

（5）床荷重

ラックエリア 500kg/㎡以上の十分な床荷重を有すること。

（6）内装材

フロア内の内装材は不燃材が使用されていること。

（7）駐車場

サーバルームへの入室者の交通手段が主に車であることを想定し、駐車スペースが確保されていること。

3.4.2 スペース提供サービス

（1）IT 機器設置スペース

本件で対象となるサーバ群が設置されるスペースは、同一区画であること。

（2）スペース有効高さ

IT 機器及び収納ラック等をスペースに設置した上で空調効率を保持できる高さがあること。

（3）収容スペースの拡張性

延岡市が計画している対象アプリケーションの増加に対応していること。また、終期（47システム分±α）の利用想定に対応できること。

（4）照明及び非常灯

作業に必要な照明と非常灯が建築基準法・消防法に準拠して整備されていること。

（5）防塵

室内の防塵対策（防塵塗装、空調対策等）を行っていること。

（6）避難経路

建築基準法・消防法に準拠した避難経路が確保されていること。

（7）ウィスカ対策

床下部材の亜鉛から生じるウィスカの発生対策がなされていること。

（8）作業用スペース

サーバルームへのシステム・機器導入、メンテナンスに伴う技術者の作業用スペースをコンピュータルーム内、もしくは近接した場所に確保可能なこと。

3.4.3 電源提供サービス

受電方法については障害時の電源確保のため、2系統以上の受電方式があり、商用電源の停止時に、電源供給可能なバックアップ電源を提供できることが必要である。特に、法定点検、工事等によってビル内電力供給が停止している間も機器類を停止することのない十分な容量の無停電電源装置（UPS）を用意すること、また商用電源停止時に電源を供給することのできる非常用電源装置を有することが必要である。非常用発電機は少なくともサーバルームの全設備へ供給できる能力が必須であり、発電機の故障に備え、また保守点検を勘案して予備機を考慮する必要がある。燃料の備蓄量は補給までの所要時間が最大の決定要因であるが、広域災害など燃料補給を期待できない最悪の事態を想定し、データの保存と代替センタへの移行の所要時間も考慮する必要がある。

（1）受電方法

障害時の電源確保のため、2系統以上の受電方式があること。

（2）変電所ルート

同一変電所における障害を避けるため、異なる給電ルートを選択可能であることが望ましい。

（3）受電容量

受電容量は将来の収容計画に基づいて決めること。（サーバルームの電源容量、運用機器電源容量、施設設備電源容量）例えば750W/m²以上（力率0.8で見積もった場合）。

（4）冗長性

法定点検や工事等の際にも電力の供給を止めることなく、サーバルーム内に電力を供給できる冗長構成であること。ただし、法定点検に伴うサーバルーム内への電力供給の計画停止は、

年間の保守計画に計上し、実際に停止する2ヶ月前までに延岡市に連絡・協議し、日程を決めるものとする。

（5）無停電電源装置（バッテリ）

設置システムが動作するために必要な電力容量(10 分以上供給可能な能力)を確保すること。

（6）非常用電源（発電機）

非常用に自家発電設備を設け、サーバルームの電源容量、運用機器電源容量、施設設備電源容量以上の電源容量について、24 時間以上の稼働が可能な燃料を確保すること。

（7）電力設備監視

電力設備は集中監視していること。

3.4.4 空調提供サービス

設置されているIT機器による発熱を抑えることができる容量の空調であること、24時間365日連続して空調稼働できること、サーバなどの増設に対応して空調能力を増強可能なことが望ましい。

また、1 台が故障しても全体に影響を与えないように、必要数＋1 以上の構成をとることが望ましい。

（1）空調容量

設置されているIT機器による発熱を抑えるのに十分な容量の空調を提供すること。

（2）空調稼働時間

24 時間 365 日連続して空調稼働できること。

（3）温度・湿度調整

ラック外の周囲温度を適正に保ち、誤動作せず、かつ四季を問わず結露の発生しない適正温度・湿度の維持ができること。

（4）空調タイプ（送風方法）

ラック下吹き出し、上吸い込みであること。

（5）空調設備監視

空調設備の集中監視が可能であること。

（6）予備空調（冗長性）

1 台が故障しても全体に影響を与えないシステム構成であること。（必要数＋1 以上の構成）

（7）水漏れ検知システム

空調機及び排水管周りに漏水検知システムを設置する。

3.4.5　消火設備提供サービス

消防法により、特定の建築物に対して消防設備の設置が義務付けられている。消火剤の種類により水系消火設備とガス系消火設備に分けられるが、サーバルームは、水による消火を極力避けるためガス消火システムであることは必須であり、ガスの種類は地球環境を考慮しハロン代替消火剤が望ましい。運用面では、消防設備の起動前に無人になったことを確認する必要がある。火災報知システム、延焼防止システム、火災予兆検知システム等を有し、建築基準法・消防法基準での点検スケジュールを実施できること。

（1）サーバルーム内消火設備

放水による IT 機器の損傷を防ぐため、サーバルーム内はスプリンクラー等の水系消火設備は設けず、ガス系消火設備を設けること。

（2）事務所エリア消火設備

スプリンクラー、消火器等の消火設備を設けること。

（3）火災感知・報知システム

火災を自動的に検出する方法として、熱感知器、煙感知器等があり、かつ人が発見して通報する手動通報といったものを備えること。

また、非常放送設備、防火防排煙設備、各種消火設備と連動していること。

（4）消火設備監視

消火設備の集中監視が可能であること。

3.4.6　避雷・静電気対策設備提供サービス

避雷針だけでは、雷電流の接地からの回り込みや誘導により電源線や通信線を伝わる雷サージによる電気設備の被害までは防ぐことができないといわれている。

ハウジングしている IT 機器の被害を防ぐため避雷器、耐雷トランスなどが必要であり、これらと避雷針及び接地を含めた十分に配慮する必要がある。

（1）直撃雷対策

国内の建築設備設計基準上、ビル構造によっては屋上に避雷針の義務付けがなされている。避雷針と大地とのアース接続、または保護したい設備機器に雷対策装置を取り付け、大地とのアース接続を十分配慮した対策を講じること。また電気設備、弱電設備、通信設備、セキュリティ設備の電源火災に対しても、耐雷電圧の査定を十分考慮した対策を講じること。

（２）誘導雷対策

直撃雷が無くとも、遠隔地の稲妻の影響で生じる過電流・過電圧対策を行うこと。

① 電源系統は全て誘導雷を受けにくい施工方法を採用、もしくは電力会社から受電するポイント（受電点）に避雷器（最大放電サージ電流 40kA 以上）を設置すること。

② サーバルームの設備機器を守るため、誘導雷を受けない施工方法を採用、もしくはコンピュータルームの分電盤に避雷器(最大放電サージ電流 40kA 以上)を設置すること。

③ 雷が近隣に落雷すると大地電圧が上昇し建物への回り込みが想定され、接地系統からの雷ノイズ侵入対策として接地線用避雷器を設置する。また雷ノイズ侵入時に共通接地方式に切り換えられるようにすること。変電設備、分電盤に雷サージ電流が流れても破壊されない対策を行うこと。

④ 弱電設備の雷ノイズ対策として、電話回線用ケーブルの引き込み部には弱電用避雷器（保安器）が設置されていること。また、ネットワーク通信ケーブルに関しても、保安器を設置し、雷の影響を受けにくい光ケーブルにて引き込みを行うこと。

（備考）

電気設備技術基準に基づき、上記①については接地抵抗値 10Ω以下、②～④については接地抵抗値 100Ω以下であることを前提とする。

（３）静電気対策

オペレータや関係者が帯電した静電気（数千 V～1 万 V）を機器に放電することは、雷が機器に直撃した現象と等しく、機器に被害を与える恐れがある。静電気対策リストバンドの着用、空調機器による対策（加湿）、タッチバー等による静電気除去対策、静電気床対策、静電気対策シューズを使用するなどの対策をとること。また、そのルールを徹底するための作業手順書を明示すること。

3.4.7　ラック提供サービス

機器の搭載ラックは EIA 規格の 19 インチラック仕様であり、各開閉口に施錠ができ第三者が開閉できない仕組みであること、ラック搭載型でない機器をラックに搭載できる棚板が準備されていること、40U 以上(EIA 規格：1U＝1.75 インチ)の搭載スペースを確保できること、そして AC100V 及び AC200V の機器への給電が可能であること。

（１）内寸

ラック搭載型の IT 機器の搭載が可能な内寸であること。

（２）規格

EIA 規格準拠 19 インチラックであること。

（３）搭載重量

350kg 程度であること。

（4）棚板

ラック搭載型でないIT機器等をラックに搭載できる棚板を使用できること。またその重量に耐え得る棚板であること。

（5）コンセント・形状

NEMA5-15相当のコンセント形状であること。

（6）ラック施錠

ラックは施錠ができ、サービス利用者又は許可されたものから申し出がない限り開錠できないように管理すること。また、管理方法を明確にして、鍵の置き場所、利用者の制限などを鍵管理手順書に明示する。

3.4.8 ビル管理におけるセキュリティサービス

セキュリティゾーンを設定し、入退室にあたっては、有人対応によるチェック、監視カメラ、ICカードやバイオメトリクス等個人認証システム等により複数の入退室チェックを行い、あらかじめ入退室を許可された人のみに制限すること。監視カメラ等の監視により、サーバルーム内での不審行動者を監視すること。

IC カードやバイオメトリクス認証等の対象となる個人については、契約時に登録を行い、責任が明確になるようにすること。また、担当者等の入れ替わりについては、随時追跡調査を行い、登録者リストのメンテナンスを行うこと。

（1）入退館・入退室管理

建物入口には人員を配置し、24時間365日、監視を行うこと。入退室については、入退室記録、ICカード式ゲートシステムやバイオメトリクス認証等の個人認証システムにより、入退室を許可された人のみに制限すること。ベンダ等の作業者が事前に登録を行うことにより、入館・入室を可能にすること。IDCに入退室をする全ての委託業者について、氏名管理まで行うこと。また、委託業者氏名名簿は、発注者に提出すること。かつ、担当者の変更があった際には、速やかに報告すること。ICカードの貸借は厳禁とすること。また、入退室の記録については、2年間データとして保持するものとする。なおかつ、発注者側からデータを要求された場合は、常に提出可能なこととする。

（2）鍵管理

入退室などの鍵管理については、管理方法を明確にして、利用者の制限などを鍵管理手順書に明示すること。

（3）入館可能時間

24時間365日であること。

（4）モニタ監視

24時間365日であること。

（５）監視映像記録（保存期間）

1ヶ月以上の保存が可能であること。

（６）監視カメラカバー率

追尾式監視カメラや固定カメラを活用することで、入口から事務室、サーバルームまでの監視範囲がほぼ100%のカバー率であること。

（７）入室ドア

入室ドアそのものが容易に破壊されないような対策、窓なしとする等外部から容易に見とおせない対策が施されていること。

（８）オペレータ常駐時間

24時間365日であること。

（９）オペレータ常駐対応

常駐オペレータ用仮眠・休憩室を用意すること。

（１０）前室

セキュリティドアは、共連れ・機器持出し防止の対策がなされ、バイオメトリクス認証によるチェックを行うこと。

（１１）媒体保管

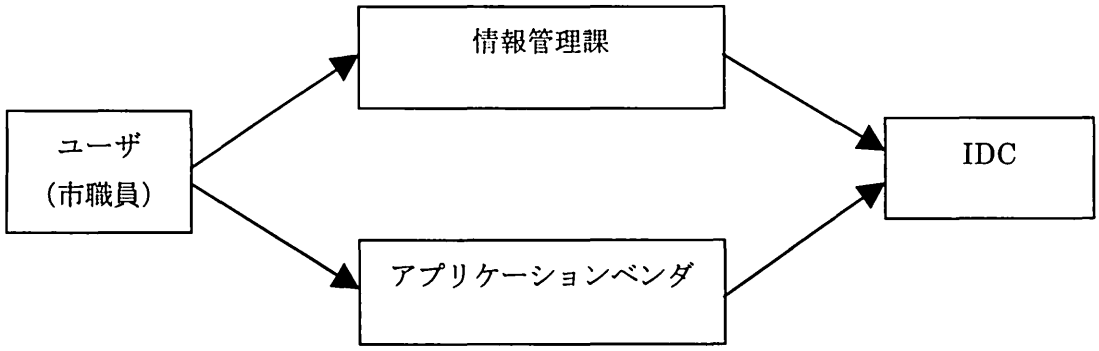
磁気テープや光ディスクなどのデータメディア類および情報が記載されているペーパー等の保管場所の構造は、サーバルームと同等以上に堅牢な構造とし、空調設備、ガス消火設備を備えること。入退室に関しては、ICカードやバイオメトリクス等個人認証システムを使用するなどセキュリティの徹底を図ること。データメディア類そのものの保管については、保管庫内に鍵付きの防火金庫を設置し保管すること。但し、防火金庫の鍵の管理については、別途定めるセキュリティ運用手順に準ずること。媒体を取扱う委託業者に関しては、その都度氏名を管理すること。

3.5　サービスサポートの検討

サービスサポートには発注者（市職員）からの問い合せ等に対応するIDC単体のサービスサポートがある。

想定される問い合わせルートは下記のとおりである。

図表 3.5.1　想定される問い合わせルート



3.5.1　必要な運用機能

システムの運用に必要な機能は、運用管理、セキュリティ管理、基盤運用保守、監視・オペレーションと考える。システムの安定稼働のためには、運用機能の全体範囲に対応する運用体制を構築することが重要となる。

3.5.2　サービスサポートメニュー

サービスサポートのサービスメニューについては次の２つのサービス種別に分類される。

（１）運用体制

サービスサポートを提供する上で運用体制の確立は必要条件となる。したがって運用サービスとして提供される運用は、下記の体制を維持管理した上で提供する。また、運用サービスを提供する担当者のスキル確認については定期的に実施する。

・常駐オペレータ１名以上
・システム技術者１名
・管理者１名

（２）障害対応サービス

各サービスに関する障害対応を行うサービス。障害発生から運用要員における検知から一時対応及び障害報告のエスカレーションを確実に実施する。また、障害検知時、エスカレーションが必要な場合や障害の継続による経過連絡の実施の可用性を維持する。

（3）問合せ対応サービス

各サービスに関する問合せ対応を行うサービス。運用規定に定められた要件における問合せ対応の完全性及び可用性を確実にする。

第4章　IDC へハウジングされるシステムの検討

4.1　今後のシステム運用方針

現在、延岡市庁舎内には各課に独自で導入された25のクライアント/サーバ系システム、汎用機（ホスト系システム）と多岐にわたった形態により運用・管理されている。この25システム及びホスト系システム（平成22年度更新に伴い、クライアント/サーバ系システムへ移行予定）を効率的かつ安全性の高い運用を実現することを目的としている。

4.2　ハウジング対象が想定されるシステム

平成20年度移設予定の８サーバ（７システム）の要件は以下のとおりとする。

年度	機種	OS	システム数	サーバ数	備考
20年度	PRIMERGY RX300	Windows 2003 Server	５システム	６サーバ	バックアップ交換　：１サーバ 自動サーバリブート：２サーバ
	PRIMERGY RX100	Windows 2003 Server	１システム	１サーバ	—
	POWER EDGE 850	Windows 2003 Server	１システム	１サーバ	—

平成 21 年度以降の移設予定のサーバについては下記のとおりとする。なお、サーバ要件については現在利用中のものを記載している。したがって、システム更新に伴い、移設時期、サーバ数、サーバ要件等については変更となる場合がある。

年度	機種	OS	システム数	サーバ数	備考
21年度	PRIMERGY TX200相応	Windows系	２システム	２サーバ	バックアップ交換　：１サーバ 自動サーバリブート：１サーバ
	PRIMERGY RX100相応	Windows系	１システム	１サーバ	自動サーバリブート：１サーバ
	PRIMERGY P250相応	LINUX	１システム	１サーバ	—
	POWER EDGE 1950相応	Windows系	１システム	１サーバ	—
	PRIMEPOWER 200相応	UNIX	２システム	２サーバ	バックアップ交換　：２サーバ 自動サーバリブート：２サーバ
	EXPRESS5800 /110Ee相応	Windows系	１システム	１サーバ	バックアップ交換　：１サーバ 自動サーバリブート：１サーバ
22年度	PRIMERGY RX200相応	LINUX	ホスト系システム	７サーバ	バックアップ交換　：７サーバ 自動サーバリブート：７サーバ
	PRIMERGY RX300相応	LINUX		３サーバ	バックアップ交換　：３サーバ 自動サーバリブート：３サーバ
	PRIMERGY ES320相応	Windows系	１システム	１サーバ	—
	PRIMERGY RX300相応	Windows系	１システム	１サーバ	—
	HA8000 /130相応	Windows系	１システム	３サーバ	バックアップ交換　：３サーバ 自動サーバリブート：３サーバ

年度	相応機種	OS	システム数	サーバ数	備考
23年度	PRIMERGY RX300相応	Windows系	2システム	3サーバ	バックアップ交換　：2サーバ 自動サーバリブート：2サーバ
	PRIMERGY TX200相応	Windows系	2システム	3サーバ	バックアップ交換　：3サーバ 自動サーバリブート：2サーバ
	PRIMERGY C200相応	Windows系	1システム	1サーバ	バックアップ交換　：1サーバ 自動サーバリブート：1サーバ
	EXPRESS5800 /110Ee相応	Windows系	1システム	1サーバ	—
24年度	EXPRESS5800 /120Rh相応	Windows系	1システム	7サーバ	バックアップ交換　：1サーバ 自動サーバリブート：7サーバ
	FMV-W5210相応	Windows系	1システム	1サーバ	自動サーバリブート：1サーバ

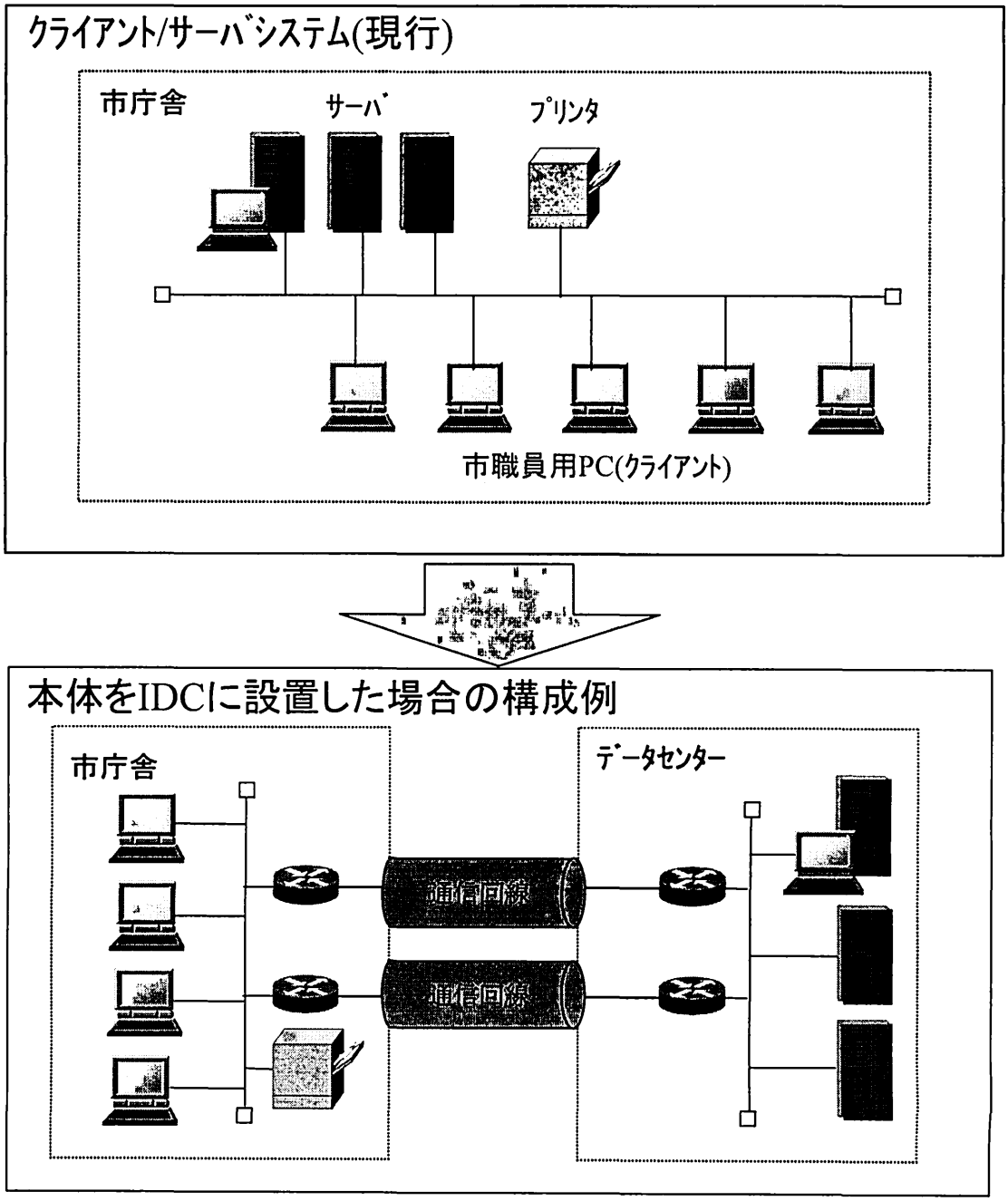


図 4.2 クライアント/サーバシステムの構成

4.3　監視・基本オペレーション

4.3.1　監視サービス

監視サービスについては、今回ハウジングされた全てのシステムに対して死活監視のみを定期的に実施する。

4.3.2　オペレーションサービス

（1）LED ランプ確認

今回ハウジングされた全てのシステムの LED ランプの確認を行う。

（2）障害対応支援（サーバリブートなど）

今回ハウジングされた全てのシステムについて障害発生時の際にサーバリブート作業を実施する。

（3）レポーティング

障害履歴、作業報告を月次レポートとして提出する。

4.4　バックアップ作業

（1）媒体交換

今回ハウジングされたシステムのうち約２５サーバ（最終年度）に対して週１回のペースで媒体交換を実施する。

（2）媒体保管

媒体保管数は、①媒体交換対象サーバ 1 台につき 3 本程度（DAT）、②今回ハウジングされない市庁舎にあるホスト系システムバックアップのみ４０本程度（CMT）を想定している。

（3）媒体搬送

上記（2）②における媒体については、月 2 回程度の媒体搬送を実施する。

4.5　利用ラック数の想定

平成 20 年度からサーバルームのラックを利用する予定である。今後 5 年間のサーバ導入数及び利用ラック数の想定は下表のとおりである。

図表 4.5　年度別想定利用ラック数

	H20 年度	H21 年度	H22 年度	H23 年度	H24 年度	最終サーバ及びラック数
サーバ導入予定数	8	8	１５	8	8	４７±α
ラック導入予定数	1	1	1	1	1	５±α

第5章　スケジュール

5.1　IT 機器移設スケジュール

市庁舎内にある既存設備を IDC に移設するには以下のスケジュールを想定している。

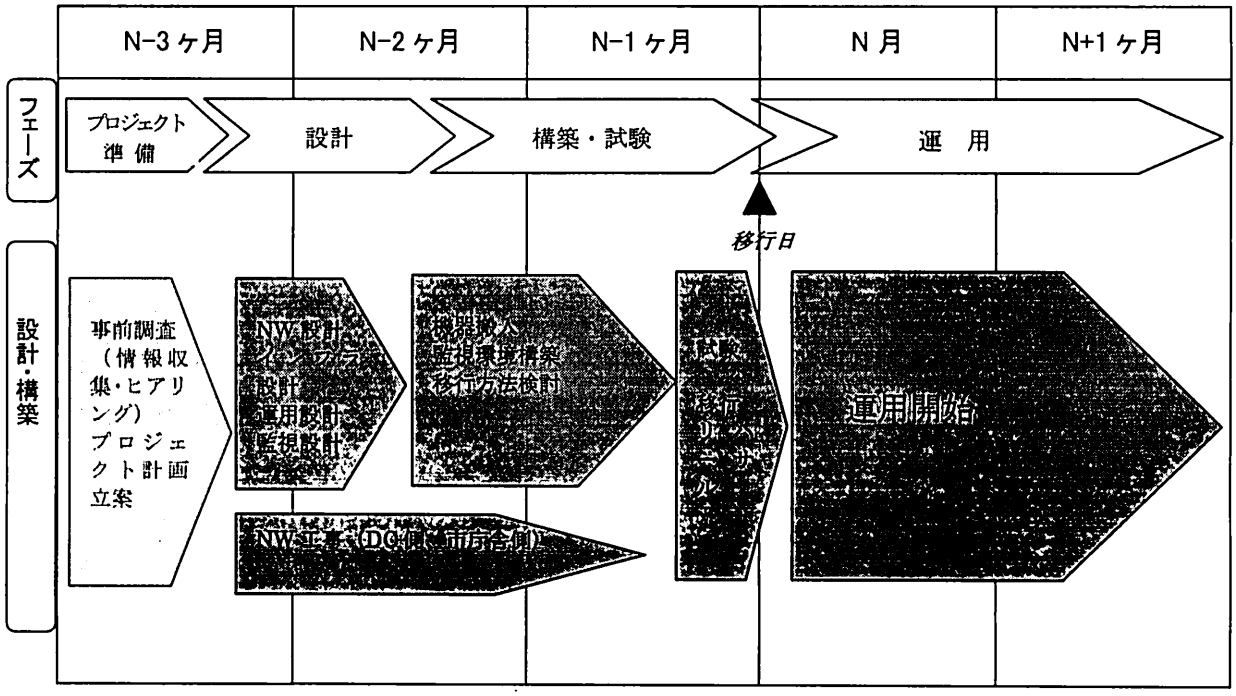


図 5.1 既存システム移設・運用スケジュール

5.2　必須要件

本基本設計書 5.1 記載のスケジュールで、回線手配、ネットワーク構築、ファシリティ構築、監視設備構築など、サーバルームとして必要な機能の構築が可能なことが必須要件である。

平成 20 年度で約 8 システムの移設を想定しており、以後 5 年間で累計（平成 20 年度分含む）47 システム±α（5 ラック±α）の利用を想定しているため、今後 5 年間で最大 47 システム±α（5 ラック±α）の受入が可能であることが必須要件である。

第6章　IDC における管理体制

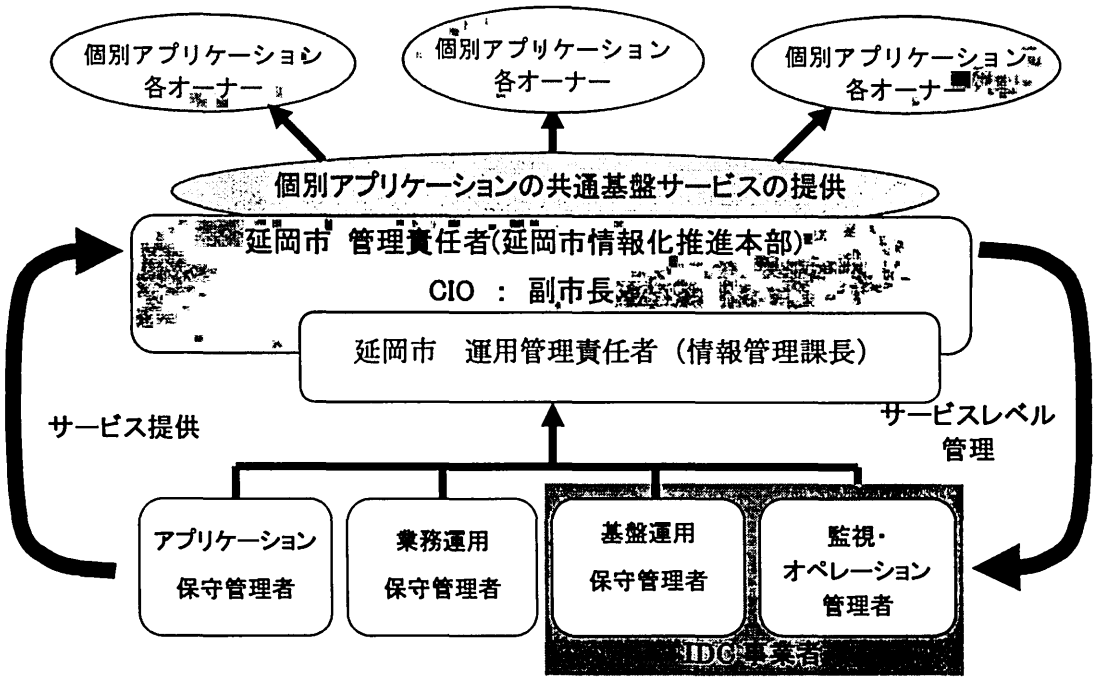
6.1　必要な管理機能

システムの運用に必要な管理機能としては、システム運用の委託元である延岡市側の管理機能と、委託先側の管理機能の両方と考える。システムの安定稼働のためには、両者の管理機能に対応する管理体制を構築することが重要となる。

6.2　管理体制イメージ

延岡市には、管理責任者を設定する。その管理の元で、IDC 事業者が個別アプリケーションの業者側に対して、個別アプリケーション運用の共通基盤サービスを提供する。また、IDC 事業者は、管理者に対し、サービスレベルに関する報告を定期的に行う。延岡市の管理責任者は、サービスレベルの管理を実施し、問題があれば改善の方策を委託先と協議する。

延岡市の管理責任者は、技術者知識や IDC 運用の経験ノウハウを補完するために、外部の専門家に運用管理のサポートを委託することがある。



図表 6.2　管理体制イメージ図

図表 6.2 の各管理者については以下のとおり。

①アプリケーション保守管理者	個別アプリケーションの作成ベンダの保守管理者
②業務運用保守管理者	業務に関する問合せを管理する
③基盤運用保守管理者	IDC における基盤（ファシリティ・NW等）の保守管理を行う
④監視・オペレーション管理者	監視・オペレーションの管理を行う

6.3 監査

契約時に締結したSLA及びSLAに組み込まれていないセキュリティに関するルールなどについては、運用試験時及び稼働後に必要に応じて監査の必要がある。また、必要に応じ第三者機関による監査も実施するので、受託者はこれに対応すること。

第7章　コンピュータルームセキュリティポリシーについて

7.1　目的

延岡市は「延岡市情報セキュリティポリシー」(平成 16 年 3 月)を策定済であり、サーバルームを設置する場合は、基本的にはそのセキュリティポリシーを遵守して運営するものとする。但し、今回のサーバルームは、IDC 内コンピュータルームの区画されたスペースに設置されるのでコンピュータルームの運営上いくつか留意点がある。したがって、「延岡市情報セキュリティポリシー」より抜粋した下記 4 項目において記載する。

①コンピュータルームに関する指針
②物理的対策に関する指針
③クライアント PC における接続条件の指針
④媒体の取扱に関する指針

7.2　コンピュータルームに関する指針

コンピュータルームの設置によってサーバ等を保護し、それらに格納する情報の安全性を確保することを目的とする。

7.2.1　対象者

コンピュータルームの設置と利用に係る全ての関係者。

7.2.2　対象システム

コンピュータルームに設置するコンピュータ及びその他の機器。

7.2.3　コンピュータルームの定義

①コンピュータルームの定義は「重要度の高い情報資産が格納されているコンピュータがまとめて設置される部屋」とする。
②電子化されたデータとして保存する重要度の高い情報資産は、「７．４　クライアント PC 等における接続条件の指針」および「７．５　媒体の取扱に関する指針」に基づいて管理される場合を除き、コンピュータルームに設置するコンピュータでのみ保存されなければならない。

7.2.4　コンピュータルームの物理的セキュリティ

①コンピュータルームは独立した部屋として設置し、一般オフィスとの共用や他社オフィスと

の隣接は避けなければならない。

②コンピュータルームは、危険物保管場所、火気施設、水道設備等、災害のリスクの大きい場所からは遠ざけて設置しなければならない。

③コンピュータルームの外観は目立ちにくいものとし、室名表示等も最小限にとどめなければならない。

④コンピュータルームの出入り口は原則1ヶ所に限定し、施錠設備を設けなければならない。

⑤コンピュータルームに窓を設けることは極力避け、設ける場合は網付きガラス・強化ガラス等を用いなければならない。

⑥コンピュータルームには設置する機器・設備の重要度に応じて、防犯カメラ、侵入報知機等の防犯設備の設置を検討しなければならない。

⑦コンピュータルームには必要に応じて、非常電話、非常ベル等の非常用連絡設備の設置を検討しなければならない。

⑧コンピュータルームにはコピー・FAX等、情報の複写や送信のための設備を設置してはならない。

⑨その他のコンピュータルームの物理的セキュリティについては「7．3　物理的対策に関する指針」でのセキュリティ区画の扱いに準ずる。

7.2.5　コンピュータルームの運用

①コンピュータルームは関係者不在時には施錠しなければならない。

②コンピュータルームおよびその鍵の管理については管理責任者を置かなければならない。

③コンピュータルームへの入室は、受付または認証装置（入館カード、パスワード入力、生体認証）等によって特定の登録メンバに制限されなければならない。

④コンピュータルームへの未登録者の入室および作業実施については管理責任者の許可と登録メンバの同伴がなければならない。

⑤コンピュータルームに入室可能な登録メンバは定期的に見直さなければならない。

⑥コンピュータルームに入室不要となった登録メンバは速やかに登録を解除し、入室のための認証を無効にしなければならない。

⑦コンピュータルームへの入退室は記録しなければならない。

⑧コンピュータルーム内で長時間作業を行う場合は監視カメラ等による監視または、一人で実施せず、必ず同伴者を伴わなければならない。

⑨コンピュータルーム内で管理責任者の許可なく撮影・録音を行ってはならない。

⑩コンピュータルームには作業に必要のないものを置いてはならない。もし置いてあった場合は速やかに撤去しなければならない。

⑪コンピュータルーム内の環境（機器・設備の有無、配置、利用状況等）は定期的に点検しなければならない。

⑫その他のコンピュータルームの運用については「7．3　物理的対策に関する指針」でのセキュリティ区画の扱いに準ずる。

7.3　物理的対策に関する指針

敷地・建物・機器・設備等を保護し、それらの損傷や利用の妨害、許可されていないアクセスを防止することを目的とする。

7.3.1　対象者

IDCの設備又は利用に直接的又は間接的に関わる全ての関係者。

7.3.2　対象システム

IDCに設置する全ての情報システム（サーバ、クライアントPC、ネットワーク通信機器等により構成されるシステム）

7.3.3　遵守事項

（1）セキュリティ区画の設定

①重要度の高い機器・設備を設置する場所にはその重要度に応じたセキュリティ区画が設定されなければならない。

②セキュリティ区画はその範囲を明確にしていなければならない。

③セキュリティ区画の管理については管理責任者を置かなければならない。

④セキュリティ区画には施錠設備を設けなければならない。

⑤セキュリティ区画は区画およびそこに設置する機器・設備等に関するセキュリティ上の各種のリスクを評価した上で必要な対策を実施しなければならない。リスクの要素には以下のものがある。（盗難、破壊、地震、火災、水害、ほこり、振動、化学作用、電源事故、電磁波、静電気等）

（2）セキュリティ区画の運用

①セキュリティ区画は従業員不在時には施錠しなければならない。

②セキュリティ区画への入場は、管理責任者の許可を受けて登録した特定のメンバに制限されなければならない。

③セキュリティ区画への未登録者の入場については必ず入退場を記録し、登録メンバが同伴しなければならない。

④セキュリティ区画に入場する外部からの来訪者には区画内での注意事項を事前に説明しておかなければならない。

⑤セキュリティ区画に入場可能な作業者などは、「３．４．８（１）入退館・入退室管理」の記述に従う。

⑥セキュリティ区画に入場するものは身分証明となるカードあるいはバッジ等を常に明示しておかなければならない。また従業員は身分証明の明示がない入場者の相互確認を行わなければならない。

（３）機器・設備の保護

①機器・設備の設置位置については、不正な操作が実施しにくく、不用意な操作ミス（間違いや見落とし）が起こりにくいように配慮しなければならない。

②重要度の高い機器・設備は他のものと分離して設置しなければならない。

③機器を設置する場合、落下や損傷の防止措置をとらなければならない。

④機器周辺では飲食・喫煙等を行ってはならない。

（４）電源・空調の保護

①電源・空調室およびその設備には耐震、耐火、耐水などの防災対策を実施しなければならない。

②電源は、安定化装置の導入、負荷変動機器との配電隔離等によって電源容量と品質を確保しなければならない。

③電源は過電流・漏電等による機器への障害に対する保護措置をとらなければならない。

④電源には避雷設備を設置しなければならない。

⑤重要度の高い機器・設備に対する電源には、無停電装置、バックアップ電源等を設置しなければならない。

⑥空調設備は機器・設備を適切に運転するために十分な温度・湿度の調整能力を確保しなければならない。

⑦重要度の高い機器・設備に対する空調設備については予備装置を確保しなければならない。

（５）ケーブルの保護

①ケーブルは、損傷や回線の盗聴を避けるため、保護用の電線管・カバーの使用や、敷設経路に対する配慮などの対策を行わなければならない。

②干渉防止のため、電源ケーブルと通信ケーブルは分離しなければならない。

③重要度の高いケーブルについては代替経路を準備しなければならない。

④ケーブルおよび端子については、未認可の機器・設備の接続や設置に対する監視または定期的チェックを行わなければならない。

7.4　クライアントPCにおける接続条件の指針

クライアントPC上の機密性・完全性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

7.4.1　対象者

クライアントPCを利用する全ての関係者。

7.4.2　遵守事項

①延岡市の業務において、関係者が使用できるクライアントPCは、延岡市が支給・貸与また

は延岡市が認めたクライアントPCのみとする。
②いかなる場合でも、延岡市システム環境に私物PC を接続・利用してはならない。

7.4.3 クライアントPCの他者への利用制限

①席を離れる場合、第三者が無断でPC を利用できないようにクライアントPC にロックを掛けなければならない。
②クライアントPCに対するパスワード管理を徹底しなければならない。
③クライアントPCでは、基本認証以外にもBIOS上での認証を行うようにしなければならない。

7.5 媒体の取扱に関する指針

PC 等の修理時、並びに媒体の処分時に関するルールを定め、機密性の高い情報の漏洩を未然に防ぐことを目的とする。

7.5.1 対象者

①PC 等の修理を依頼する全ての関係者。
②媒体の使用、処分を行う全ての関係者。

7.5.2 対象システム

延岡市の業務で使用する全てのPC 等及び媒体を対象とする。
媒体とは、フロッピーディスク、MO、CD、DVD、磁気テープ、ハードディスク等、情報が保存できるものを対象とする。

7.5.3 遵守事項

（1）PC 等の修理
①PC 等の修理を依頼する関係者は、機密性の高い情報が読み出し可能な状態で保管されていないことを確認した上で修理を依頼しなければならない。故障の状況により、保管されている情報の確認や保護が実施できない場合には、ハードディスク等の情報が保管されている装置を取り外して修理を依頼しなければならない。
②外部業者がコンピュータルームに立ち入って修理を行う場合、「７．２．５．コンピュータルームの運用」、「７．３　物理的対策に関する指針」に基づいて対応しなければならない。

（2）媒体の保管
①機密性の高い情報を媒体に保存する者は、権限のない者が保管された情報にアクセスできないよう、暗号化を行うか、媒体を鍵のかかる場所に保管し、鍵は容易に持出しが出来ない場所に保管しなければならない。

（３）媒体の移動

①全ての関係者は、機密性の高い情報を保管した媒体を、その情報の管理責任者の許可なく社外へ持ち出してはならない。但し、管理責任者の許可がある場合においても、セキュリティが確保された手段で送付しなければならない。

（４）媒体の再使用

①全ての関係者は、機密性の高い情報が保存されている媒体を再利用する前に、保存されていた情報を、再生できない方法で消去しなければならない。

（５）PC 等と媒体の廃棄

①PC 等の廃棄を行う者は、延岡市にデータ消磁証明書を提出しなければならない。

②PC 等の廃棄を行う者は、機密性の高い情報が保管されたハードディスク等を取り外してから、指定された場所に廃棄しなければならない。取り外したハードディスク等は、延岡市が指定する場所に持ち込むか、または廃棄証明書を提出しなければならない。

③機密性の高い情報が保管された媒体の廃棄を行う者は、延岡市が指定する場所に持ち込むか、または廃棄証明書を提出しなければならない。

④機密性の高い情報が保管されているかどうかが確認できない場合には、機密性の高い情報が保管されているものとして取り扱わなければならない。

⑤媒体の処分を外部業者に委託する場合、秘密保持及び、処分依頼品の再利用の禁止を契約文書に含めなければならない。

7.6　例外事項

業務都合等により、コンピュータルームセキュリティポリシーの遵守事項を守れない状況が発生した場合は、延岡市から例外の適用承認を受けなければならない。

7.7　罰則事項

コンピュータルームセキュリティポリシーの遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。

第8章　IDC 使用に伴う管理手順書について

8.1　管理手順書

管理手順書は、規定（ポリシー、管理要綱、管理基準など）に基づく活動の実施方法が記述される。複雑な業務でも、手順化することにより一定の品質を維持することが可能と考える。

8.2　管理手順書の必要性

サーバルームに設置されるコンピュータには、大量かつ重要な情報が保管される。そのため、セキュリティ事件・事故を未然に防ぐための管理手順書は必須と考える。そこで、サーバルームの委託先の選定にあたっての条件として、「１０．６　SLA 関連提出資料」内で指定する資料を提案時に提出すること。

8.3　管理手順書の内容

（1）コンピュータルームセキュリティ運用管理手順書の内容

コンピュータルームのセキュリティ運用管理手順書の例を下記に示す。

１．目的

コンピュータルームに設置されるサーバにおける、不正アクセス、データ改ざんなどセキュリティ上の脅威に対する対策（管理策）についての具体的な手順を記述する。

２．本書の位置付け

本書は、コンピュータルームの管理策を実施（運用）する際の具体的な手続き、手順、その実施責任、及び関連する作業手順等を示すものである。

３．詳細管理策

３．１　通信及び運用管理

３．１．１　運用手順及び責任

① 操作手順書

情報システムの操作方法及び障害発生時の対応方法について定めた「運用マニュアル」等に従う。

② 運用変更管理

情報処理施設の変更は「各種マニュアル」「運用仕様書」等の申請手続きに従う。

③ 事件・事故管理手順

「コンピュータルームコンテンジェンシープラン」に従う。

④ 職務の分離

システム管理者、オペレータは、基本的には職務を分離し、責任の範囲を明確にする。

⑤ 開発環境と運用環境との分離

情報システムのテストの環境は、テスト機もしくはソフト的に本番環境と分離する。

⑥ 外部委託による施設管理

リスク分析結果を元に規定の各種契約書にて契約を締結する。

3．1．2　システムの計画作成及び受入

① 容量・能力の計画作成

運用仕様書等に従う。

② システムの受入

情報システムの新規導入あるいは変更は、品質マニュアルに基づきテスト、及び受入審査を実施する。

3．1．3　悪意のあるソフトウェアからの保護

① 悪意のあるソフトウェアに対する管理策

管理策は個別の運用仕様書に従う。利用者へはISMS対策の教育を実施する。

3．1．4　システムの維持管理

① 情報のバックアップ

個別の運用仕様書に従う。

② 運転の記録

運転記録は業務毎に定める「チェックシート」に記録し、運用責任者はその状況を把握する。

③ 障害記録

障害の原因に応じて定められた方法で運用責任者に報告する。

3．1．5　ネットワークの管理

① ネットワーク管理策

問題が発見された場合、業務担当者はネットワーク管理者へ報告し、ネットワーク管理者は早急に対策を行う。

3．1．6　媒体の取扱及びセキュリティ

① コンピュータの取外し可能な付属媒体の管理

データ保管室で厳重に保管する。

② 媒体の処分

保管中のデータ等の廃棄は、センタ管理責任者の許可を受け、定められた方法で廃棄する。

③ 情報の取扱手順

重要なデータ等の選定基準・保管方法・取扱方法は定められた通りの方法で実施し、個別の指定は運用責任者が行う。

④ システムに関する文書のセキュリティ

システムに関する文書（運用仕様書、運用マニュアル等）、及び電子データは、所定のセキュリティ区画以外への持出し及び放置を禁止する。

3．1．7　情報及びソフトウェアの交換

① 情報及びソフトウェアの交換契約

情報及びソフトウェアの交換契約を行う場合には、定められた契約を取り交わす。

② 搬送中の媒体のセキュリティ

移送中の媒体を許可されないアクセス誤用及び改ざんから保護するため、堅牢なケースで移送する。

③ 電子メールのセキュリティ

電子メールの使用に関して規定する使用規準に従う。

④ 電子オフィスシステムのセキュリティ

電子オフィスシステムとは、コンピュータ（モバイル含む）、電子メール、グループウェア、電話（携帯含む）、FAX、コピー機等とし、使用については定められた規定に従う。

⑤ 公開されているシステム

ホームページの運営、利用に関しては、定められた規定に従う。

⑥ 情報交換のその他の方式

電話やFAXを使用しての情報交換の際は、定められた規定に従う。

３．２　アクセス制御

３．２．１　アクセス制御に関する業務上の要求事項

情報へのアクセス制御は、定められた規定に従う。

３．２．２　利用者のアクセス管理

① 利用者登録

ユーザIDの発行、更新、削除は定められた規定に従う。

② 特権管理

システム管理者、及びオペレータの情報システム及びファイルへのアクセスの資格、権限は、明確に定める。

③ 利用者のパスワードの管理

管理主体はアプリケーション管理者とする。

④ 利用者アクセス権の見直し

管理主体はアプリケーション管理者とする。

３．２．３　利用者の責任

① パスワードの使用

運用仕様書等に従う。

② 利用者領域にある無人運転の装置

無人運転の装置は設置しない。

３．２．４　ネットワークのアクセス制御

ネットワークについては、「サーバルーム技術的セキュリティ管理要領」に従う。

３．２．５　オペレーティングシステムのアクセス制御

① 自動の端末識別

サーバではアプリケーション管理者が端末の設定を実施している為、端末の自動認証機能は備えない。

② 端末のログオン手順

管理主体はアプリケーション管理者とする。

③ 利用者の識別及び認証

管理主体はアプリケーション管理者とする。

④ パスワード管理システム

パスワードを管理する担当者と行使する担当者は事前に氏名を登録し、報告するものとする。また、パスワードの貸借は厳禁とし、パスワードの貸借が難しいワンタイムパスワードなどの方法をとるものとする。

⑤ システムユーティリティの使用

運用仕様書等に従う。

⑥ 利用者を保護するための脅威に対する警報

入退室管理、カメラによる常時監視、オペレータ 24 時間常駐化、定期巡回監視、アクセス監視（サーバ監視ログ、侵入検知システムログ）を実施し、物理的又はネットワークを介して侵入することによる直接的な脅威を遮断する。

⑦ 端末のタイムアウト機能

管理主体はアプリケーション管理者とする。

⑧ 接続時間の制限

管理主体はアプリケーション管理者とする。

3．2．6　業務用ソフトウェアのアクセス制御

① 情報へのアクセス制限

ユーザ ID とパスワードにより制限する。

② 取扱に慎重を要するシステムの隔離

セキュリティ区画として管理されたマシン室に隔離する。ルータ及びファイアウォールにより、アクセス権限者を特定する。

3．2．7　システムアクセス及びシステム使用状況の監視

① 事象の記録

セキュリティ関連イベント等の監査ログは、「運用仕様書」等アプリケーション管理者との取り決めに従う。

② システム使用状況の監視

情報システムの状態監視に関しては、「運用仕様書」等に従う。

③ コンピュータ内の時計の同期

時刻同期のためのサーバを、サーバルーム内に設置する。

3．2．8　移動型計算処理及び遠隔作業

① 移動型計算処理

モバイルコンピュータを使用するにあたり、定められた規定を遵守する。

② 遠隔作業

遠隔作業を行うにあたり、定められた規定を遵守する。

（2）コンピュータルーム入退館管理手順書の内容

コンピュータルームの入退館管理手順書の例を下記に示す。

1．総則

1．1　目的

本規定はコンピュータルームの安全を維持し、犯罪の未然防止を目的とし、コンピュータルームに出入りする関係者の入退館管理を行う。

1．2　適用範囲

本規定はコンピュータルームの入退館者の全員に対して適用する。

2．資格の付与

2．1　入館・入室資格の付与

① 入館・入室資格の付与

所定の手続きにより申請を行い、センタ管理責任者の許可の元、写真入りの入館証を交付する。

② 資格の付与対象者

定められた関係者に限定する。

③ 資格の付与対象者以外

必要と認められる運用スタッフ、見学者、運搬業者、工事業者、システム保守業者

④ 入館証、入館バッチの着用

入館証または入館バッチを第三者から見やすい部位に常時着用する。

2．2　入館証、IDカード申請（登録／削除／変更）

IDカードの申請手続きは、別途定められた通りとする。

2．3　資格の点検

センタ管理責任者は、定期的に発行済みの入館証、IDカードの所有確認を行う。

2．4　入館証及びIDカードの取扱

入館証及びIDカードは第三者への貸与を禁止する。また、紛失・破損の場合は、速やかに定められた方法に従う。

3．入退館管理

3．1　入退館手続きの場所

手続きは受付において行う。

3．2　訪問者の入退館手続き

入館者は、定められた手続きに従い、入退館申請を行う。

3．3　見学時の入退館手続き

見学者は、定められた手続きに従い、入退館手続きを行う。

3．4　荷物搬出入時の入退館手続き

「訪問者の入退館手続き」と同様とする。

3．5　入退室管理システム異常時の運用

定められた代替措置に従う。

３．６　持込みの制限

危険物、可燃物、燃焼器具類等の持込みは、原則として禁止する。また、強い電磁波を放出し情報システムに影響を与える可能性のある機器の持込みを禁止する。

３．７　持出しの制限

コンピュータルームで管理する装置、情報、及びソフトウェアの持出しは、原則として禁止する。

（３）サーバ運用監視手順書の内容

サーバ運用監視手順書の例を下記に示す。

１．運用対象機器

運用対象機器,台数,OS 種別,パッチのリビジョンを一覧表で記載。

２．ネットワーク構成図

ネットワーク構成図を添付。

３．システム構成管理

システム構成情報として、ハードウェア構成一覧、ソフトウェア構成一覧を添付。

４．サービス提供時間

４．１　サービス時間

24 時間 365 日等、サーバのサービス時間を記載。

４．２　イベントタイムチャート

データバックアップ・サーバ再起動など、各サーバのイベントタイムチャートを記載。

５．システム運用

５．１　サービス内容一覧

５．２　以降で記載する監視運用サービスの中で、実施対象とするサービスを記載。

５．２　死活監視

サーバ／ネットワーク機器の死活監視を行う。

対象サーバ名、IP アドレスの一覧表を記載。

５．３　サーバ再起動完了確認・障害時サーバ再起動

障害発生時にアプリケーション管理者からの指示に基づき、次の手順書に記載された手順でサーバ／ネットワーク機器の再起動を行う。

再起動手順書の文書番号を指定。

５．４　障害通報

障害一次切り分け、障害報告、および障害復旧後の連絡についての作業手順を記載。

５．５　SNMP 監視

SNMP トラップ通知を監視する。対象サーバ名、SNMP トラップ名の一覧表を記載。

５．６　Web 応答監視

指定 URL へアクセスし Web サービスの稼働監視を行う。対象 URL、検知文字列、監視間隔を記載。

５．７　閾値監視

サーバリソースの閾値監視を行う。CPU,DISK の閾値を記載。

５．８　サービス・プロセス監視

サービス（もしくはプロセス・デーモン）の稼働状況を監視する。

対象プロセスを記載。

５．９　システムログ監視

指定のイベントログ・メッセージの発生を確認する。指定のメッセージの ID とソースを記載。

５．１０　APログ監視

任意のAPログの指定文字列の発生を監視する。

指定のログファイル名、メッセージを記載。

５．１１　構成管理

受入を完了したシステムの仕様書にて、記載された内容を構成情報として管理する。構成情報を管理する旨記載する。

５．１２　障害対応

受入を完了した次の手順書にて、障害発生時の一次切り分け、オペレーション作業を実施する。

障害対応マニュアルの文書番号を記載。

５．１３　バックアップ状態監視

指定時間に指定されたアラート通知によるバックアップ処理完了確認を行う。指定アラートはイベントログまたは指定文字列で指定する。

５．１４　バックアップ媒体交換

指定する頻度で媒体の交換を行う。媒体交換頻度、クリーニング頻度、媒体交換手順書の文書番号を記載する。

５．１５　定期リブート確認

サーバ別タイムチャートに従い、自動リブートの実行結果完了確認を実施する。

５．１６　媒体保管

ラック内に保管しない媒体およびマニュアル類を耐火金庫（エリア提供）にて保管する。

５．１７　運用報告

定めた報告様式により、月１回の運用状況報告書を作成する。

５．１８　性能レポート

コンピュータのリソース状況を収集し、グラフ化して報告する。

５．１９　障害時の復旧作業

受入を完了した次の手順書にて、既知の障害の復旧作業を実施する。個別オペレーション手順書の文書番号を記載。

５．２０　個別オペレーション作業

受入を完了した次の手順書にて、個別オペレーション作業を実施する。個別オペレーション手順書の文書番号を記載。

６．連絡体制

６．１　緊急連絡網

緊急連絡網を記載する。

６．２　障害対応（原因究明）担当部門表

障害対応（原因究明）担当部門表を記載する。

６．３　サーバアカウント設定情報

OSログオン認証情報とWeb認証情報を記載する。

8.4　管理手順書の更新

管理手順書は、一旦作成すればそれで終わりという事は無く、環境の変化などに合わせて、常に更新される必要がある。

第9章　SLA の概略

9.1　SLA について

9.1.1　目的

SLA（Service Level Agreement）とは、サービスを利用する側（ユーザ）と提供する側（プロバイダー）の間で、目標とするサービスのレベルを設定し、サービス対象となる項目とサービス内容（サービスメニュー・サービス要件・サービス内容・SLA 評価項目・SLA 設定値）を明示する契約である。

サーバルームアウトソーシングにおいては、延岡市役所の中枢をつかさどる情報通信システムを IDC に外部委託するため、それを安全確実に維持運用することが最重要とされている。利用者が安心してシステムを委託するためには、当該事業者が信頼できることを知る必要がある。しかし、ハードウェア機器・装置のように形のあるものと異なり、サービスの安心と信頼性（品質）が、目に見えないが、利用者は、上記のサービス要件や SLA 設定値によって事前に知ることが可能になる。曖昧で主観的な尺度で IDC を選択することがないように、また稼働後の品質が約束通り提供されるように SLA を適切に運用することが重要になる。

ここでは IDC を活用する上での SLA の役割と構造を明確にし、利用者に安心と信頼を提供するための設定・運用方法について記述する。

9.1.2　検討方針

SLA の検討においては、総務省「公共 IT におけるアウトソーシングに関するガイドライン」（平成 15 年 3 月）を参考にし、このガイドラインを基本とする。

9.2　SLA の概略構造

SLA は、サービスを高いレベルで保証する場合には、それに伴いサービス料金も高くなる。そのため、契約する側も予算に応じて SLA を設定する必要がある。

SLA においては、基本的にどこまで達成できたのかを数値で明示したレポートが求められる。したがって、SLA では取り決めたサービスが実施されていることが定量的に把握できることが非常に重要であるため、提供者は利用者に報告することが義務付けられる。

利用者にとってサービスレベルが達成か未達成かを定量的に計測可能であることが重要であり、SLA 設定値のあるものは必ず計測が可能である必要がある。また提供者にとってはサービスレベルが制御可能であることも重要である。

サービスが SLA 設定値を達成できなかった場合の補償や、更には係争時の調停においても SLA は重要な役割を担う。

9.3 SLA のサイクル

IDC 事業は新分野であり、利用者と提供者で協議して決定するが、はじめから完全な SLA を実現することは極めて困難であり、時間の経過と共に利用者の要求水準も市場や技術も変化する。そのため、当初設定を行う SLA は暫定的なものと認識し、ライフサイクルの視点から変更を考慮しておく必要がある。その際、SLA を変更するのにファシリティからシステム、運用体制に至るまで見直し、逆に、ファシリティなどの改善・変更が SLA の見直しに繋がる、という二面あることに注意しなければならない。このことから、SLA を固定的に捉えてペナルティの対象とするのでなく、利用者と提供者が協力して実現する目標、という考え方が重要となる。

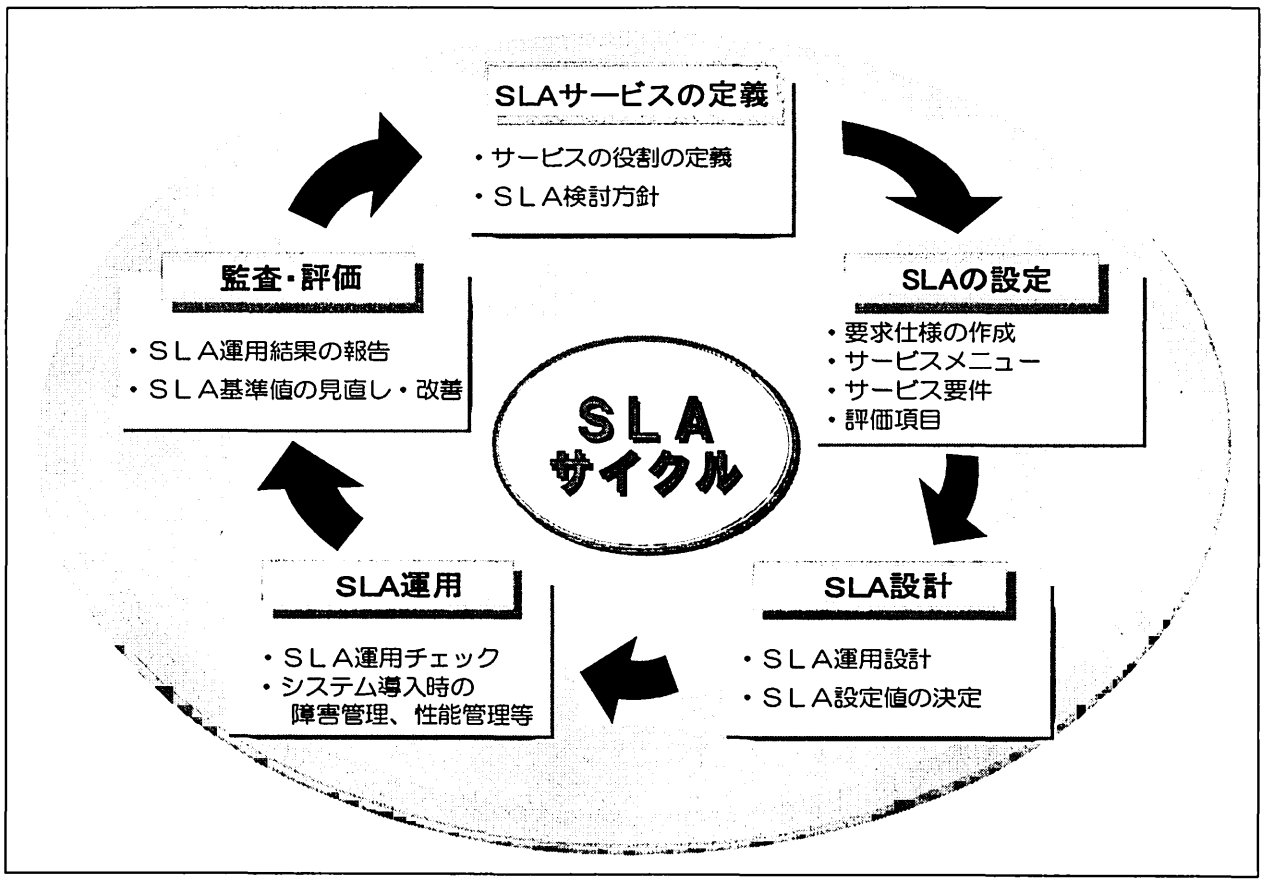
SLA をライフサイクルの視点で管理するには実績データの分析が必須である。SLA の根拠となる数値データを具体的に計測するとき、現状測定可能な技術として以下のような項目が検討される。

・可用性
・パフォーマンス監視
・サービス時間
・サポートレベル
・レスポンスタイム
・機能
・セキュリティ
・認証　　等

また、上記の項目に対して、随時、定期的なレポートや緊急時の対応手続きレビュー、サービスレベルの定義と参照などを行う。もちろんこの項目全てが網羅されている必要はなく、先に述べた費用や柔軟性、維持の面から選択する必要がある。また技術の発展に伴い、運用監視ツールなどで測定可能なデータが一般化することも考えられる。更に、ネットワーク監視やハードウェア、ミドルウェアなど基盤周りの監視ツールの機能向上によって、新たな測定可能なデータを運用に活用できるようになるなども意識してサービスレベルと SLA の見直し、検討を常に行うのが望ましい。

これらを踏まえて、SLA サービスレベルを定義・合意し、運用を行い、定期的にレビューをするなど一連のサイクルとすると、図表９．３のように表すことが出来る。

この過程で監査と評価が重要なポイントとなるが、監査と評価は第三者による委員会等で実施することが望ましい。



図表 9.3　SLA のサイクル

9.4 IDC における SLA 分類

SLA の枠組みを以下の分類で示すこととする。

①ホスティング
②セキュリティ
③ネットワーク
④ハウジング
⑤サービスサポート

ホスティングはサーバおよびストレージなどの各機器・装置の動作確認や性能管理、障害時の対応などに関する SLA となる。システムとしての可用性や能力に関する SLA は、利用者およびアプリケーションによる差異が大きいので、SI ベンダとの個別契約で規定する SLA となる。

セキュリティ（ファイアウォール運用など）はプロフェショナルサービスの範疇に含まれ、個別契約上で規定する SLA となる。

ネットワークは、インターネット回線や専用回線などの回線の提供が基本的なサービスである。主にキャリア側の SLA となるが、スイッチなどの動作確認や性能管理、障害時の対応なども含まれる。

ハウジングは全サービスの基盤であり、特にハウジング（コロケーション）サービスとしてラック提供（ケージサービスなど）とスペース提供が基本的なサービスである。

サービスサポートは利用者との接点にあり、IDC の運用に関わる事項全てを統括する位置付けにある。

9.5 SLA の留意点

9.5.1 ペナルティ

契約書及びサービスレベル協定書で定める。

9.5.2 免責事項

契約書及びサービスレベル協定書で定める。

第10章　SLA 評価項目と設定値

ここで記述するSLAはIDCに関連したものであり、表中に値がないものであっても、アプリケーション構築時毎に追加検討する場合もある。また、定期的に発注者側が監査を実施する際に、下記のSLAの中で要求されたものは、指定された時期に提出するものとする。

10.1　ホスティング

SLA評価項目と設定値は以下の通りである。

図表 10.1(1)　ホスティングにおけるSLA評価項目と設定値（1）

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
機器提供サービス	機器種別	パフォーマンス要件、稼働要件に合致する、サーバ、ワークステーション、ネットワーク機器を選択・構成する。システムの必要性に応じて、高可用性、高パフォーマンス、負荷分散環境も選択する。	—	—
	障害監視	Pingの応答、監視ツールによる障害監視を行う。	死活監視	1回／5分
	サービス時間	機器のサービス時間を規定する。設備、ネットワーク等の点検、保守のための計画停止時間、計画停止通告期間・方法、稼働率を規定する。	・インフラ保守時間 ・稼働率	・提案による ・99%以上（アプリケーションサービスの規定以上の値に設定すること）
	レポーティング	障害時、発生した障害への対応状況（インフラ、サーバに発生した障害の内容、発生理由、対応経緯、実施作業等）を報告する。なお、問題状況報告は、予め設定した重要度、緊急度の高いものに適用する。	報告タイミング	対応後1日以内 遵守率 99.9%
ソフトウェア提供サービス	ソフトウェア種別	パフォーマンス要件、稼働要件に合致する、OS、ミドルウェアを選択・構成する。システムの必要性に応じて、高可用性、高パフォーマンス、負荷分散環境も選択する。	—	—
	障害監視	監視ツールによる障害監視を行う。	死活監視	1回／5分
	サービス時間	ソフトウェアのサービス時間を規定する。設備、ネットワーク等の点検、保守のための計画停止時間、計画停止通告期間・方法、稼働率を規定する。	・インフラ保守時間 ・稼働率	・提案による ・99%以上（アプリケーションサービスの規定以上の値に設定すること）
	レポーティング	障害時、発生した障害への対応状況（インフラ、サーバに発生した障害の内容、発生理由、対応経緯、実施作業等）を報告する。なお、問題状況報告は、予めホスティング業者と設定した重要度、緊急度の高いものに適用する。	報告タイミング	対応後1日以内 遵守率 99.9%

図表 10.1 (2)　ホスティングにおける SLA 評価項目と設定値 (2)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
オペレーションサービス	定期作業代行	延岡市が提出した作業手順書に基づき、定期的な作業を実施する。	—	—
	不定期作業代行	トラブル対応を行うため、サービス利用者の指示に基づき、不定期な作業を実施する。	オペレータスキル	提案による
	機器交換	機器故障、トラブルシューティングの一環として、予備機への交換を行う。但し、利用者(延岡市)資産を除くものとする。機器交換に際しては、ハードウェア、OS までの復旧をサービス範囲として実施する。	—	—
	機器稼働監視	サービス対象機器に対し、Ping により、活性／非活性監視を実施する。	死活監視	1 回／5 分
		サービス対象機器に対し、運用手順書に基づき、LED ランプ確認を実施する。	LED ランプ確認	巡回実施率 100%
		サーバ運用監視手順書を明示する。	サーバ運用監視手順書	—
バックアップ／リストアサービス	バックアップ	延岡市からの指示に基づき、予め調整した周期、時間にて定期バックアップを実施する。	—	—
	リストア	延岡市からの指示に基づき、指定されたエリアにリストア作業を実施する。	—	—

10.2 セキュリティ

SLA 評価項目と設定値は以下の通りである。

図表 10.2(1) セキュリティにおける SLA 評価項目と設定値 (1)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
サーバセキュリティ	ウイルスチェック(サーバ)	ファイルアクセス時に全てのファイルについて、ウイルスチェックを実施する。	パターンファイルの更新間隔	ベンダリリースから24時間以内／24時間～3日以内、等
	OS、ミドルウェアのセキュリティパッチ管理	OS、ミドルウェアのセキュリティパッチ管理・適宜実装を実施する。	—	ベンダリリースから24時間以内にパッチ試験開始／24時間～3日以内にパッチ試験開始、等
	サーバ上のデータ管理	サーバ上のデータにつき、漏洩や改ざんを防止し、適正に管理する。	—	—
端末セキュリティ	ウイルスチェック	全てのファイルについて、ウイルスチェックを実施する。	パターンファイルの更新間隔	ベンダリリースから24時間以内／24時間～3日以内、等
	認証	本人が使用していることの認証を行う。	—	—

図表 10.2(2)　セキュリティにおける SLA 評価項目と設定値（2）

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
運用管理	レポーティング	定期的もしくは随時にセキュリティサービス運用状況についての報告を行う。	—	—
		ウイルス侵入など問題を発見した場合、随時連絡を行う。	報告	報告 30 分以内/対処時間は協議して決める
	媒体や紙に出力した情報等の適正な管理	盗難紛失や情報漏洩等を防ぐために、管理運用方法について、あらかじめ取り決め、提出する。	媒体や紙に出力した情報の管理手順書	—
	コンピュータルームセキュリティ運用管理手順書	延岡市で定めるセキュリティポリシーの基本方針に従い、運用に関する詳細な運用管理手順書を作成し提出する。	コンピュータルームセキュリティ運用管理手順書	—
	管理手順書の更新	環境などの変化に合わせて、常に更新をする。	見直し期間	1 年
監査	監査体制の整備	発注者が実施する監査に対応して、SLA の遵守状況を必要時に提出する。	—	—

10.3　ネットワーク

ネットワークにおけるSLA評価項目と設定値は以下の通りである。

図表 10.3　ネットワークにおけるSLA評価項目と設定値

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
IDCから庁舎間ネットワーク接続サービス	帯域	帯域を保証するタイプの回線接続サービスの場合の接続回線の帯域	帯域保証	100Mbps 以上
	冗長	接続回線については、万一の障害に備えて、冗長構成とする。回線についてはバックアップ回線を利用する。	—	—
	監視・通報	ネットワークを監視し、障害を通報する時間帯	通報時間	検知後 60 分以内の連絡 遵守率:99.9%
	拡張性	接続する回線の帯域を増やしたい場合等に、サービス提供事業者が対応可能な期間		
バックアップ回線接続サービス	帯域	帯域を保証するタイプの回線接続サービスの場合の接続回線の帯域	帯域保証	100Mbps 以上
	構成	メイン回線とは異なるルートを利用する	—	—
	監視・通報	ネットワークを監視し、障害を通報する時間帯	通報時間	検知後 60 分以内の連絡 遵守率:99.9%
	拡張性	接続する回線の帯域を増やしたい場合等に、サービス提供事業者が対応可能な期間		

10.4　ハウジング

ハウジングにおけるSLA評価項目と設定値は以下の通りである。

図表 10.4(1)　ハウジングにおけるSLA評価項目と設定値（1）

サービスメニュー	サービス要件	説明	SLA評価項目	SLA設定値
建築物	住所	延岡市が保管しているデータを主体的にコントロールすることのできる権限が及ぶ範囲内及び地元の産業育成の観点より、設置場所は宮崎県内であること。	住所	宮崎県内
	ビル耐震構造	建築基準法における「新耐震基準」に適合すること。震度7クラスの地震に耐え得ることを必須とする。	適用耐震基準 耐震数値	昭和56年6月改正以降の新耐震基準に適合 震度7
	免震構造	地震の揺れを吸収し建物内に収容する装置等に致命的な損害を与えない免震構造（免震床等）や制震構造であること。	免震構造または制震構造	あり
	水害対策	サーバルーム及びそれに関連する施設は、水害を考慮し、防水・排水設備の完備や高床式建築などの構造をとること。	防水・排水設備の完備等	—
	床荷重	ストレージ等の設置を考慮した荷重に耐え得る構造とする。	最大床荷重	ラックエリア500kg/㎡以上
	内装材	フロアの内装材は不燃材を使用する。	不燃材	—
	駐車場	駐車スペースが確保されていること。	—	—

図表 10.4(2)　ハウジングにおける SLA 評価項目と設定値 (2)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
スペース提供サービス	IT機器設置スペース	本件で対象となるサーバ群が設置されるスペースは、同一区画であること。	—	—
	スペース有効高	IT機器及び収納ラック等をスペースに設置した上で、空調効率を保持できる高さを提供する。	—	—
	収容スペースの拡張性	延岡市が計画しているアプリケーションの増加に対応可能なこと。	増設可能な設置スペース	5＋α
	照明及び非常灯	作業に必要な照明、非常時の非常灯を提供する。	—	—
	防塵	室内の防塵対策(防塵塗装、空調対策等)を実施し、提供する。	—	—
	避難経路	建築基準法・消防法に準拠した避難経路を確保し提供する。	—	—
	ウィスカ対策	床下部材の亜鉛から生じるウィスカの発生対策がなされていること。	ウィスカ対策	—
	作業用スペース	システム・機器導入・メンテナンスに伴う技術者の作業用スペースを確保すること。	—	—

図表 10.4(3)　ハウジングにおける SLA 評価項目と設定値 (3)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
電源提供サービス	受電方法	障害時の電源確保のため、2 系等の受電ルートを有する。	受電方法	2 回線受電方式以上
	受電容量	受電容量は将来の収容計画に基づいて決めること。(サーバエリアの電源容量、運用機器電源容量、施設設備電源容量)例えば 750W/㎡以上(力率 0.8 で見積もった場合)	受電容量	750W/㎡以上(力率 0.8 で見積もった場合)
	冗長性	法定点検や工事等の際にも電力の供給を止めることなく、サーバルーム内に電力を供給できる冗長構成であること。ただし、法定点検に伴うサーバルーム内への電力供給の計画停止は、年間の保守計画に計上し、実際に停止する 2 ヶ月前までに延岡市に連絡・協議し、日程を決めるものとする。	—	—
	無停電電源装置(バッテリ)	設置システムが動作するために必要な電力容量を 10 分以上供給可能な能力を確保できること。	電力供給時間	10 分以上
	非常用電源(発電機)	非常用に自家発電設備を設け、サーバエリアの電源容量、運用機器電源容量、施設設備電源容量異常の電源容量について、24 時間以上の稼働が可能な燃料を確保すること。	連続稼働時間	24 時間以上
	電力設備監視	電力設備の集中監視が可能であること。	集中監視	あり

図表 10.4 (4)　ハウジングにおける SLA 評価項目と設定値 (4)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
空調提供サービス	空調容量	設置されているIT機器による発熱を抑えるのに十分な容量の空調を提供する。	空調容量	総発熱量の115%以上
	空調稼働時間	24 時間連続して空調を提供する。	稼働時間	24 時間連続運転
	温度・湿度調整	ラック外の周囲温度を適正に保ち、誤動作せず、かつ四季を問わず結露の発生しない設定温度、適正湿度の維持ができること。	—	—
	空調タイプ（送風方法）	ラック下吹き出し、上吸い込み型。	ラック下吹き出し、上吸い込み型の空調	あり
	空調設備監視	空調設備の集中監視が可能であること。	集中監視	あり
	予備空調（冗長性）	空調設備1台が故障しても全体に影響を与えないシステム構成とする。（必要数＋1以上の構成）	予備空調	1 台以上
	水漏れ検知システム	空調機からIT機器設置スペースへの水漏れがないよう、空調機および配水管周りに漏水検知システムを設置する。	漏水検知システム	あり
消火設備提供サービス	サーバルーム内消火設備	スプリンクラーの放水による汚損を防ぎ、通電時の火災防止のためガス系消火設備を設けること。	消火設備	ガス系消火設備
	事務所エリア消火設備	スプリンクラー、消火器等の消火設備を設置する。	消火設備	あり
	火災感知・報知システム	火災を自動的に検出する方法として、熱感知器、煙感知器、炎感知器等があり、かつ人が発見して通報する手動通報といったものを備えること。また、非常放送設備、防火防排煙設備、各種消火設備と連動していること。	火災検知システム	あり
	消火設備監視	消火設備の集中監視が可能であること。	集中監視	あり

図表 10.4 (5)　ハウジングにおける SLA 評価項目と設定値 (5)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
避雷・静電気対策設備提供サービス	直撃雷対策	国内の建築設備設計基準上、ビル構造によっては屋上に避雷針の義務付けがなされている。避雷針と大地とのアース接続、又は保護したい設備機器に雷対策装置を取り付け、大地とのアース接続を十分配慮した対策を講じること。	左記直撃雷対策	あり
	誘導雷対策	電気設備技術基準に基づき、以下の対策を講じること。 ① 高圧電源系統対策として、電源系統は全て誘導雷の影響を受けない施工方法を採用するか、もしくは架空線引き込みの場合は電力会社から受電するポイント(受電点)に避雷器を設置すること。 ②サーバルームの設備機器対策として、誘導雷の影響を受けない施工方法を採用するか、もしくはサーバルームの分電盤に避雷器を設置すること。 ③ 雷が近隣に落雷すると大地電圧が上昇し建物への回り込みが想定され、接地系統からの雷ノイズ侵入対策として接地線用避雷器を設置する。また、雷ノイズ侵入時に接地極間の電位差をなくす対策がとられていること。 ④ 弱電設備の雷ノイズ対策として、電話回線用ケーブルの引き込み部に保安器を設置する。また、ネットワーク通信ケーブルに関しても保安器を設置し、雷の影響を受けにくい光ケーブルにて引き込みを行うこと。	①誘導雷の影響を受けない施工方法(地中線引き込み等)の有無、もしくは架空線引き込みの場合、避雷器の最大放電サージ電流規格値 ②誘導雷の影響を受けない施工方法(地中線引き込み等)の有無、もしくは分電盤に設置する避雷器の最大放電サージ電流規格値 ③接地系統からの雷ノイズ対策の有無 ④弱電設備の雷ノイズ対策の有無	①誘導雷の影響を受けない施工方法・・・有もしくは架空線引き込みの場合、避雷器の最大放電サージ電流規格値・・・40kA 以上 ②誘導雷の影響を受けない施工方法・・・有もしくは架空線引き込みの場合、避雷器の最大放電サージ電流規格値・・・40kA 以上 ③接地系統からの雷ノイズ対策の有無・・・有 ④弱電設備の雷ノイズ対策の有無・・・有
	静電気対策	静電気対策リストバンドの着用、空調機器による対策、タッチバー等による静電気除去対策、静電気床対策、静電気対策シューズを使用するなどの対策をとる。また、作業者の静電気対策に関する作業手順書を明示する。	静電気対策作業手順書	—

図表 10.4 (6)　ハウジングにおける SLA 評価項目と設定値 (6)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
ラック提供サービス	内寸	ラック提供サービスとして、ラック搭載型の IT 機器の搭載が可能な内寸で提供する。	—	—
	規格	EIA 規格準拠 19 インチラックを提供する。	—	—
	搭載重量	ラック提供サービスとして、IT 機器等の総重量搭載可能なものを提供する。	最大重量	350kg 程度
	棚板	ラック提供サービスとして、ラック搭載型でない IT 機器等をラックに搭載できる棚板を提供する。	—	—
	コンセント・形状	NEMA5-15 相当のコンセント形状で提供する。	形状	NEMA5－15
	ラック施錠	ラックは施錠ができ、サービス利用者又は許可されたものから申し出がない限り開錠できないように管理すること。また、管理方法を明確にして、鍵の置き場所、利用者の制限などを鍵管理手順書に明示する。	鍵管理手順書	—

図表 10.4 (7)　ハウジングにおける SLA 評価項目と設定値 (7)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
ビルにおけるセキュリティサービス	入退館・入退室管理	ビルにおけるセキュリティサービスとして、入退室記録と監視カメラ、IC カードやバイオメトリクス等個人認証システムにより、入退室を許された人のみに制限する。	入退室記録 監視カメラ 個人認証システム	あり あり あり
		オペレータ・清掃などの委託業者については氏名管理まで行うこと。氏名の名簿は発注者側に提出すること。かつ、担当者の変更があった場合は、すみやかに報告すること。	委託業者の氏名管理	あり
		コンピュータルーム入退館・入退室管理に関する手順書を明示すること。	コンピュータルーム入退館・入退室管理手順書	あり
		入退室の記録については、2 年間データとして保持するものとする。なおかつ、発注者側から要求された場合は、常に提出可能なこととする。	入退室記録	2 年間
	鍵管理	コンピュータルームの鍵(緊急時使用)、ラックの鍵、情報媒体管理庫等の鍵管理手順書を作成する。サービス利用者又は許可された者から申し出がない限り開錠できないように管理すること。また、管理方法を明確にして、鍵の置き場所、利用者の制限などを鍵管理手順書に明示する。なお、鍵担当者の氏名を発注者へ提出し担当が変更された時は必ず書類にて報告すること。	鍵管理手順書	—
	入館可能時間	24 時間 365 日とする。	入館可能時間	24 時間 365 日
	モニタ監視	監視カメラ等の監視により、24 時間 365 日の監視を行う。	稼働時間	24 時間 365 日
	監視映像記録(保存期間)	1 ヶ月以上の保存が可能であること。	保存期間	1 ヶ月以上

図表 10.4 (8)　ハウジングにおける SLA 評価項目と設定値 (8)

サービスメニュー	サービス要件	説明	SLA 評価項目	SLA 設定値
ビルにおけるセキュリティサービス	監視カメラカバー率	追尾式監視カメラや固定カメラを活用することで、入口から事務室、サーバルームまでの監視範囲がほぼ 100%のカバー率であること。	監視範囲	ほぼ 100%
	コンピュータルーム	ドアそのものが破壊されない対策をとること。窓なしとする等外部から見とおせない対策をとること。	破壊対策ドア	あり
	オペレータ常駐時間	オペレータの常駐時間を 24 時間 365 日とする。	常駐時間	24 時間 365 日
	オペレータ常駐対応	常駐オペレータ用 仮眠・休憩室	仮眠・休憩室	あり
	前室	共連れ・機器持出し防止の対策がなされ、バイオメトリクス認証によるチェックを行う。	前室	あり
	媒体保管	磁気テープや光ディスクなどデータメディア類の保管場所の構造は、空調設備、ガス消火設備を備えた保管庫を利用すること。	空調設備 ガス消火設備	あり あり
		入退室に関しては、IC カードやバイオメトリクス等個人認証システムを使用するなどセキュリティの徹底を図ること。	個人認証システム	あり
		データメディア類そのものの保管については、保管庫内に鍵つきの防火金庫を設置し保管すること。	防火金庫	あり
		媒体及び媒体保管に関する管理手順を明示すること。	媒体や紙に出力した情報の管理手順書	あり

10.5 サービスサポート

サービスサポートにおけるSLA評価項目と設定値は以下の通りである。

図表10.5 サービスサポートにおけるSLA評価項目と設定値

サービスメニュー	サービス要件	説明	SLA評価項目	SLA設定値
運用体制	運用体制の確立	運用サービスとして提供される運用は、下記の体制を維持管理した上で提供する。 ・常駐オペレータ1名以上 ・システム技術者1名 ・管理者1名	人員の確保 担当者スキルの確認の実施	100% 年2回以上
オペレーション	障害対応 (検知)	障害発生から運用要員における検知から一時対応及び障害報告のエスカレーションを確実に実施する。	障害検知時間 初期動作または一時対応 エスカレーション(初期連絡)	5分以内の認知 99%以上 24時間365日 5分以内実施 99.9%以上 5分以内実施 99.9%以上
		障害検知時、エスカレーションが必要な場合や障害の継続による経過連絡の実施の可用性を維持する。	障害経過報告	30分毎実施
	問合せ対応	運用規定に定められた要件における問合せ対応の完全性及び可用性を確実にする。	放棄率 バックログ率 Mail返信率	全要求の5%未満 全要求の5%未満 30分以内 99%以上

10.6 SLA 関連提出資料

サーバルームアウトソーシングに関連する SLA の設定提出資料は以下の通りである。

図表 10.6-1 SLA 関連提出資料(1)

	項目	内容	提出時期	コメント	SLA 記載ページ
1	コンピュータルームセキュリティ運用管理手順書	延岡市で定めたセキュリティポリシーに沿って、運用に関する詳細なルールを整理して提出する。	提案時	コンピュータルームセキュリティ運用管理手順書・コンピュータルーム入退館・入退室管理手順書・サーバ運用監視手順書・鍵管理手順書は一つに取りまとめて提出する	P48
2	コンピュータルーム入退館・入退室管理手順書	入退館・入退室管理に関する手順書を作成して提出する。 オペレータ・清掃業者などの委託業者については、氏名管理表を作成し発注者へ提出すること、また氏名等の管理を行い変更された時は必ず報告すること。入退室記録に関しては、発注者側から要求があった場合提出する。	提案時	同上	P56
3	サーバ運用監視手順書	サーバ運用に関する監視手順書を作成し提出する。	提案時	同上	P46
4	鍵管理手順書	・コンピュータルームの鍵(緊急時使用) ・ラックの鍵 ・情報媒体管理庫 ・・等の 鍵の運用・管理手順書を作成する。 サービス利用者又は許可された者から申し出がない限り開錠できないように管理すること。また、管理方法を明確にして、鍵の置き場所、利用者の制限などを鍵管理手順書に明示する。なお、鍵担当者の氏名を発注者へ提出し担当が変更された時は必ず書類にて報告する。	提案時	同上	P55、P56

図表 10.6-2　SLA 関連提出資料(2)

	項目	内容	提出時期	コメント	SLA 記載ページ
5	媒体や紙に出力した情報の管理手順書	媒体・紙による盗難・紛失、情報漏洩等を防ぎ、適正に管理するための管理・運用方法について書類にて提出する。	提案時	—	P48、P57
6	静電気対策作業手順書	作業者の静電気対策に関する作業手順書を提出する。	提案時	—	P54
7	利用約款	IDC 利用約款を提出する。	提案時	—	—
8	SLA 遵守状況報告	全ての SLA について遵守状況を整理して提出する。	監査時 要求時	—	—
9	IDC 構築詳細設計書	ネットワーク、ハードウェア・ソフトウェア構成、ホスティング等の詳細設計書を提出する。	設計終了時	—	—
10	運用管理計画書	1 月ごとに翌月の運用管理計画書を作成し、提出する。	毎月指定日	—	—
11	実績報告書等	委託業務に係る実績報告書を 1 月ごとにまとめて作成し、提出する。また、委託業務に係る運用の日報及び月報を併せて提出する。	毎月指定日	—	—
12	成果報告書	各年度の成果報告書を作成し、提出する。	各年度終了後速やかに	—	—

備考：この委託仕様書については、技術の変遷や時代の推移とともに内容見直しの必要性が生じる可能性がある。その際には、発注者側・業者側とで打ち合わせを行い、見直しを行う。

【参考文献】

・総務省「公共 IT におけるアウトソーシングに関するガイドライン」平成 15 年 3 月
・総務省「地方公共団体情報セキュリティ監査ガイドライン」平成15年12月
・宮崎県「サーバルーム整備基本計画等作成業務委託事業報告書」平成 16 年 3 月
・特定非営利活動法人 ASP インダストリ・コンソーシアム・ジャパン「ASP 白書」平成 15 年 4 月
・自治日報社「公共 XSP 活用のアウトソーシングとリスクマネジメント」平成 15 年 6 月
・NPO 日本ネットワークセキュリティネットワーク協会
「情報セキュリティポリシーサンプル（0.92a 版）」平成 15 年 3 月