RDクラウドFS　運用設計書

第1.1版 2025年●●月●●日

富士フイルムソフトウエア株式会社

ネットワークソリューショングループ

貴社発注番号：　PO1207837

当社見積番号：　EA24030664

改版履歴

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版 | 日付 | 箇所 | 改訂内容 | 担当者 |
| 1.0 | 2025/03/18 |  | 初版 | 加藤 |
| 1.1 | 2025/●●/●● |  | 用語定義等を修正 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目次

[1. はじめに 5](#_Toc202274381)

[2. 用語定義 5](#_Toc202274382)

[3. 運用体制 6](#_Toc202274383)

[3.1. 運用体制図 6](#_Toc202274384)

[3.2. 運用スケジュール 8](#_Toc202274385)

[3.2.1. 週間スケジュール 8](#_Toc202274386)

[3.2.2. 月間スケジュール 8](#_Toc202274388)

[3.2.3. 年次スケジュール 9](#_Toc202274389)

[3.2.4. 運用時間 9](#_Toc202274390)

[4. 運用対象 10](#_Toc202274391)

[4.1. 運用対象システム 10](#_Toc202274392)

[5. 運用業務 11](#_Toc202274393)

[5.1. 運用業務一覧 11](#_Toc202274394)

[5.2. システム変更運用 12](#_Toc202274395)

[5.2.1. 運用方針 12](#_Toc202274396)

[5.2.2. 作業一覧 12](#_Toc202274397)

[5.3. アカウント運用 13](#_Toc202274398)

[5.3.1. 運用方針 13](#_Toc202274399)

[5.3.2. アカウント種別 13](#_Toc202274400)

[5.3.3. アカウント運用方式 13](#_Toc202274401)

[運用アカウント対象：「‎4.1運用対象システム」に記載の範囲で作成されるアカウント対象とする。 13](#_Toc202274402)

[5.3.4. パスワード利用・変更ポリシー 13](#_Toc202274403)

[5.3.5. 作業一覧 14](#_Toc202274404)

[5.4. ジョブ/スクリプト運用 15](#_Toc202274405)

[5.4.1. 運用方針 15](#_Toc202274406)

[5.4.2. ジョブ/スクリプト実行方式 15](#_Toc202274407)

[5.4.3. 作業一覧 15](#_Toc202274408)

[5.5. 監視運用 16](#_Toc202274409)

[5.5.1. 運用方針 16](#_Toc202274410)

[5.5.2. 監視方針 16](#_Toc202274411)

[5.5.3. 監視対象 16](#_Toc202274412)

[監視種別と概要および監視対象を以下の通り記載する。 具体的なメトリクス、ログの監視実装内容は「‎‎5.5.3.1](#_Toc202274413)**[監視メトリクス](#_Toc202274413)**[」および「‎5.5.3.2‎ 監視ログ」に記載する。 16](#_Toc202274413)

**[5.5.3.1. 監視メトリクス](#_Toc202274414)** [17](#_Toc202274414)

**[5.5.3.2. 監視ログ](#_Toc202274415)** [17](#_Toc202274415)

[5.5.4. 作業一覧 18](#_Toc202274416)

[5.6. ログ運用 19](#_Toc202274417)

[5.6.1. 運用方針 19](#_Toc202274418)

[5.6.2. ログ収集・管理方式 19](#_Toc202274419)

[5.6.3. 作業一覧 19](#_Toc202274420)

[5.7. バックアップ/リストア運用 20](#_Toc202274421)

[5.7.1. 運用方針 20](#_Toc202274422)

[5.7.2. バックアップ方式 20](#_Toc202274423)

[5.7.3. リストア方式 20](#_Toc202274424)

[5.7.4. 作業一覧 21](#_Toc202274425)

[5.8. 保守契約管理 22](#_Toc202274426)

[5.8.1. 運用方針 22](#_Toc202274427)

[5.8.2. 作業一覧 22](#_Toc202274428)

[5.8.3. 保守機器一覧 22](#_Toc202274429)

[5.9. パッチ適用 23](#_Toc202274430)

[5.9.1. 運用方針 23](#_Toc202274431)

[5.9.2. パッチ適用方式 23](#_Toc202274432)

[5.9.3. 作業一覧 23](#_Toc202274433)

[5.10. 請求管理運用 24](#_Toc202274434)

[5.10.1. 運用方針 24](#_Toc202274435)

[5.10.2. 運用方式 24](#_Toc202274436)

**[5.10.2.1.](#_Toc202274437)** [24](#_Toc202274437)

[5.10.3. 作業一覧 24](#_Toc202274438)

[5.11. 障害対応 25](#_Toc202274439)

[5.11.1. 障害対応方針 25](#_Toc202274440)

[5.12. 問合せ対応 25](#_Toc202274441)

[5.12.1. 問合せ対応方針 25](#_Toc202274442)

[5.13. 計画メンテナンス対応 25](#_Toc202274443)

[5.13.1. 計画メンテナンス対応方針 25](#_Toc202274444)

1. はじめに

本書は、FFシステム研究開発部門(以降、RD部門とする)にて利用しているクラウドファイルサーバ基盤(以降、本システムとする)の運用設計を記載した文書である。

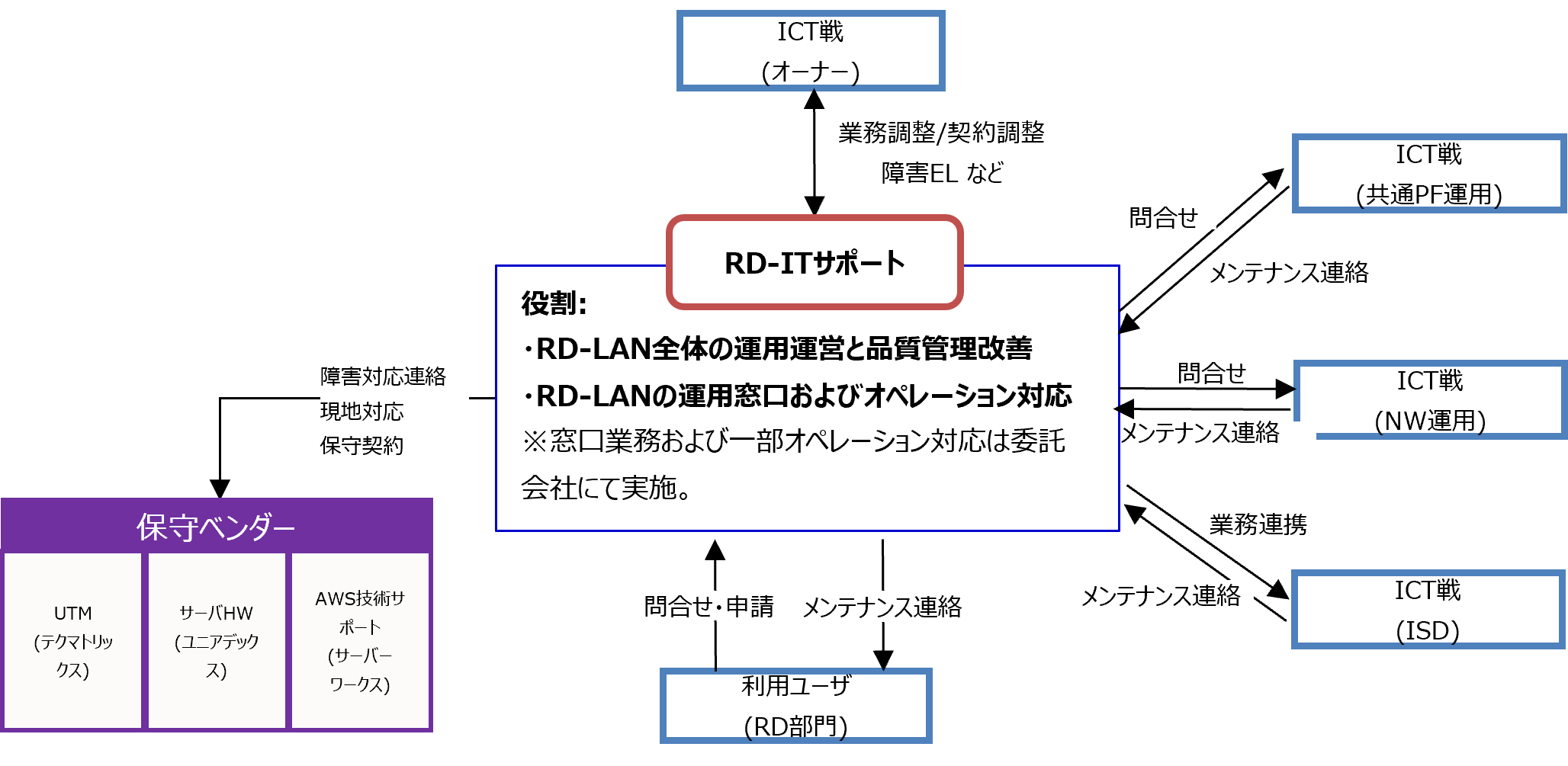
1. 用語定義

本書における用語を以下に定義する。

|  |  |
| --- | --- |
| 略称 | 説明 |
| FH | 富士フイルムホールディングス株式会社の略称。 |
| FF | 富士フイルム株式会社の略称。 |
| ICT戦 | 富士フイルムホールディングス株式会社ICT戦略部の略称。全社インフラを主管している組織。 |
| ISD | ICT戦のもと全社インフラのシステムヘルプデスクを担っている部隊。インフラサービスデスクの略称。 |
| OA | FF標準PCが一般オフィス業務を行う環境のことを指す。OAで利用するNWをOA系NWと呼ぶ。 |
| RD | 研究開発業務を行う環境のことを指す。RDで利用するNWをRD系NWと呼ぶ。 |
| RD-WAN | RD各拠点-共通PF間のWAN回線の略称。 |
| 共通PF | 「All-Fujifilm共通プラットフォーム」の略称。富士フイルムホールディングスICT戦略部が、社内ITシステムを構築する各社・各組織に対し、稼働環境を提供するための社内向けプライベートクラウド基盤のことを指す。本システムでは共通PFのAWS環境を利用する。 |
| FSx | Amazon FSx for Windows File Serverの略称。 |
| S3 | AWS S3の略称。本システムでは、「S3 Standard」、「S3 Glacier Deep Archive」を利用する。 |
| ホストサーバ | RD各拠点に設置する物理サーバのこと。 |
| キャッシュサーバ | RD各拠点のホストサーバ上の仮想サーバであり、仮想アプライアンス(FileGateway)が実装されている。 |
| 運用管理サーバ | RD各拠点のホストサーバ上の仮想サーバであり、FTP、DHCP、DNSサーバが実装されている。 |

1. 運用体制
   1. 運用体制図

　本システムの運用業務の全体像とそれに関わる主要な組織・担当者の役割を以下に定義する。



|  |  |
| --- | --- |
| 役割 | 役割概要 |
| RD-ITサポート | ・本システムのインフラ運用/保守  　- 「‎5.1‎5.1運用業務一覧」に記載の業務 |
| ICT戦(オーナー) | ・本システムのオーナーであり、システム全体とシステム上で行われる全ての活動に対する責任者 |
| ICT戦(共通PF運用) | ・共通PF(AWS)の運用/保守 |
| ICT戦(NW運用) | ・RD-WANに関する運用/保守 |
| ICT戦(ISD) | ・FF研究開発拠点のOA系NWに関する運用/保守 |
| 利用ユーザ(RD部門) | ・本システムの利用者 |
| 保守ベンダー | ・本システムが利用するハードウェアおよびソフトウェアの保守を行う会社であり、以下の領域ごとに各ベンダーが実施する。  　- テクマトリックス：UTM  　- サーバHW：ユニアデックス  　- サーバーワークス：AWS |

* 1. 運用スケジュール

本システムにおいて、必要となる運用スケジュールを定義する。

* + 1. 週間スケジュール

1週間の繰り返しスケジュールとなる。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **項目** | **対象** | **実施のタイミング** | | | | | | |
| **月** | **火** | **水** | **木** | **金** | **土** | **日** |
| システムフルバックアップ | ホストサーバ | 2:00 | 2:00 | 2:00 | 2:00 | 2:00 | 2:00 | 2:00 |
| システムフルバックアップ | 運用管理サーバ | 1:00 | 1:00 | 1:00 | 1:00 | 1:00 | 1:00 | 1:00 |
| データバックアップ | FSx | 0:00 12:00 | 0:00 12:00 | 0:00 12:00 | 0:00 12:00 | 0:00 12:00 | 0:00 12:00 | 0:00 12:00 |
| 週次報告会 | 本システム運用 |  |  |  |  | 11:00 |  |  |
| DHCPサーバMACアドレス同期 | 開成、足柄、吉田南、小田原DHCPサービス | 10分毎 | | | | | | |
| 定期パッチ適用 | FSx |  |  |  |  |  |  | 0:30 |
| キャッシュサーバ |  |  |  |  |  |  | 0:30 |
| ログ転送 | EventBridge | 0:05 | 0:05 | 0:05 | 0:05 | 0:05 | 0:05 | 0:05 |
| サーバ再起動 | FSx |  |  |  |  |  |  | 0:30 |

* + 1. 月間スケジュール

1か月の繰り返しスケジュールとなる。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **項目** | **対象** | **実施のタイミング** | | | | | | | | | |
| **月** | **火** | **水** | **木** | **金** | **土** | **日** | | **その他** | |
| 定期パッチ適用 | ホストサーバ |  |  | 第二水曜日4:00 |  |  |  |  | |  | |
| 運用管理サーバ |  |  | |  | |
| サーバ再起動 | ホストサーバ 運用管理サーバ | 第三月曜日4:00 |  |  |  |  |  |  | |  | |
| パターンファイル更新 |  |  |  |  |  |  |  |  | | 初旬 | |
| サーバ再起動 |  |  |  |  |  |  |  |  | | 10日 0:30 | |

* + 1. 年次スケジュール

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **項目** | **対象** | **実施のタイミング** | | | | | | | | | | | |
| **4月** | **5月** | **6月** | **7月** | **8月** | **9月** | **10月** | **11月** | **12月** | **1月** | **2月** | **3月** |
| アカウント棚卸 | ･ホストサーバ ･運用管理サーバ ･キャッシュサーバ ･UTM | 初旬 |  |  |  |  |  |  |  |  |  |  |  |
| 請求運用 | ･クラウドストレージ |  |  |  |  |  | 初旬 |  |  |  |  |  | 初旬 |

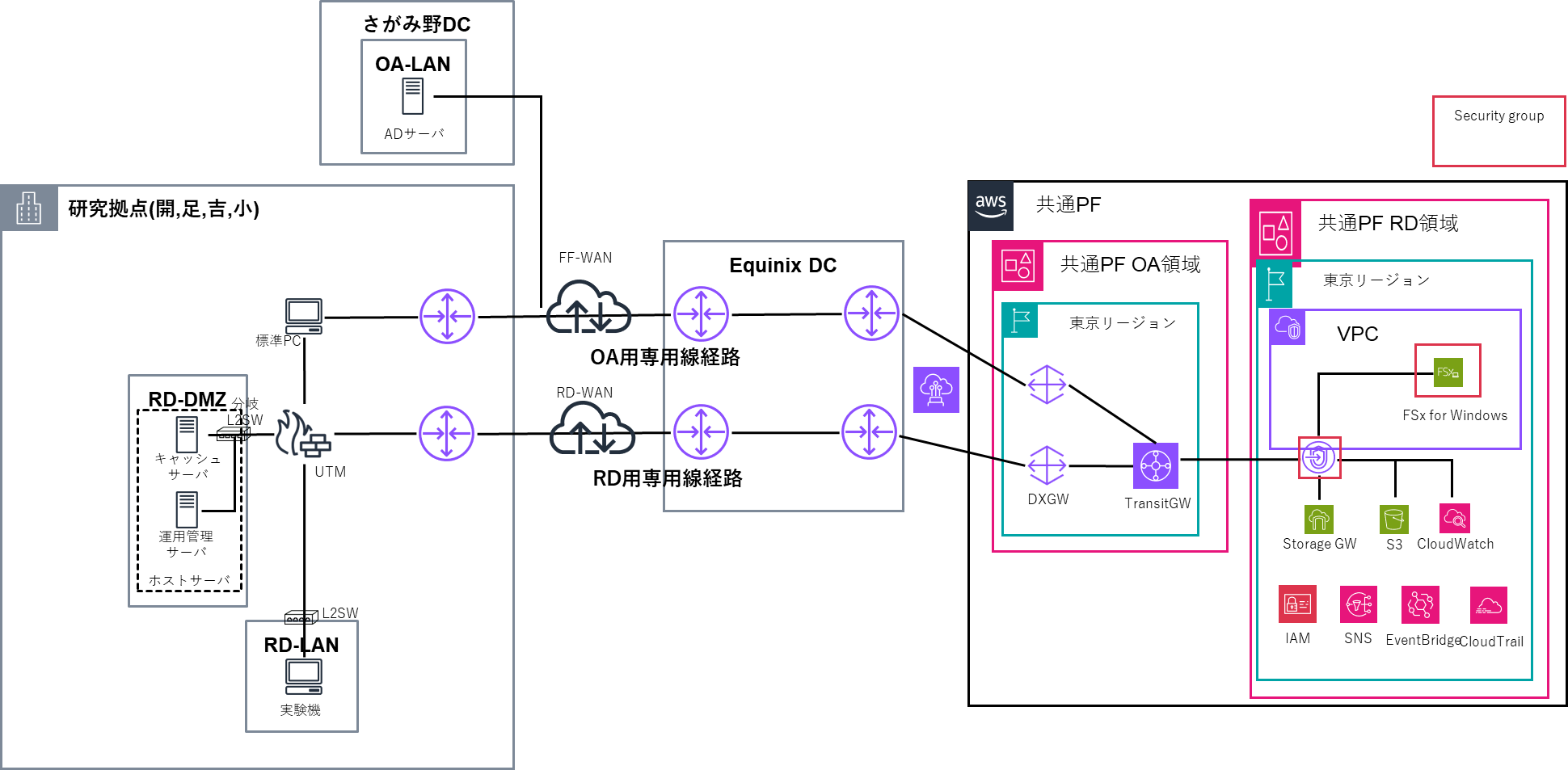
* + 1. 運用時間

本システムは24時間365日稼働する。運用時間は以下の通りとする。

|  |  |  |
| --- | --- | --- |
| 項目 | 時間帯 | 備考 |
| サービス提供時間 | 24時間365日 | 各システムメンテナンス期間を除く |
| 運用業務 | RD-ITサポート営業時間　平日 8:20～16:45 | 現状FFS(開成地区)営業時間帯平日8:20～16:45 有休付与日、休暇奨励日は除く |

1. 運用対象
   1. 運用対象システム

本システムにおける運用は以下を対象とする。

* + RD各拠点(開成、足柄、吉田南、小田原)
    - RD-DMZ上のサーバ・ネットワークスイッチ
    - RD-LAN上のネットワークスイッチ・実験機
    - UTM
  + 標準PC
  + ADサーバ
  + OA用専用線経路
  + RD用専用線経路
  + 共通PF OA領域内のリソース
  + 共通PF RD領域内のリソース

1. 運用業務
   1. 運用業務一覧

本システムの運用業務を以下に記載する。

|  |  |
| --- | --- |
| 運用項目 | 内容 |
| システム変更運用 | サービス提供を行う上で必要なネットワーク、サーバ、ストレージに関する設定変更依頼を受け付け、RD-ITサポートにて設定内容を取りまとめ、設定手順書に基づいた変更作業を行う |
| アカウント運用 | 運用担当者のアカウント管理および定期的な運用アカウントの棚卸を行う |
| ジョブ/スクリプト運用 | スケジューリングされているスクリプトの実行管理を行う。また、新しいジョブ/スクリプトの登録や既存ジョブの修正を行う |
| 監視運用 | 監視アラートを検知して、一次対応、切り分け・エスカレーションを実施する。また、監視システムの設定変更を行う |
| ログ運用 | サーバOSのシステムログ、AWSの各種リソースログ等を収集し保管する |
| バックアップ/リストア運用 | データの定期的なバックアップを行い、障害時に迅速にリストアできる体制を整える。対象データには、システム設定ファイル、ユーザデータが含まれる |
| 保守契約管理 | 保守契約の内容、期間、問合せ先などの情報更新を行う。保守ベンダーへの発注に必要な処理を行う |
| パッチ適用 | 本システムを安定稼働させるため、セキュリティ確保のため、定期的・緊急のパッチ適用を行う |
| 請求管理運用 | 本システムにおいて 各部門に適正な請求を実施する |
| 障害対応 | 本システムで発生した障害を迅速に復旧する。また、復旧ができる体制を整える |
| 問合せ対応 | 本システムに関する問合せを管理し、一次回答およびエスカレーションを行う |
| 計画メンテナンス対応 | 本システムに関連するシステムのメンテナンス発生時に、本システムへのサービス影響を最小限にする |

* 1. システム変更運用
     1. 運用方針

本システムのサービス提供を実施するため以下のシステム変更運用を定義する。

* + 対象：「‎4.1‎運用対象システム」を参照とする。
  + 方式：利用ユーザからの申請及び各RD部門管理者からの依頼もしくはRD-ITサポートが必要と判断した内容を元に対応内容の合理性を判断し、変更作業を実施する。
  + 実施手順：運用対象システムの特性とベンダー公開情報を組み合わせた検証済み手順。
  + 注意事項：停止を要する変更作業およびメンテナンス作業が発生する場合、原則2週間以上前にポータルサイトおよびメールにて利用ユーザに通知する。

* + 1. 作業一覧

|  |  |  |  |
| --- | --- | --- | --- |
| **運用項目** | **運用作業** | **内容** | **実施トリガー** |
| NW/セキュリティ運用 | RD-LAN登録/変更/削除 | 測定器等をRD-LANへ接続するための申請作業を実施する。 | 利用ユーザが申請書にて実施 |
|  | 通信制御設定変更 | 依頼要件に基づいて以下のパラメータを変更する。 対象は以下とする。 ①UTM ②セキュリティグループ | 変更要件発生時 |
| ファイルサーバ運用 | FSx設定変更 | クラウドストレージ(FSx)の以下設定変更作業を実施する。 ･ストレージ容量追加 ･FSx増設 ･FSx閉鎖 | 変更要件発生時 |
|  | キャッシュサーバ増設 | キャッシュサーバを増設する。 | 変更要件発生時 |
|  | キャッシュサーバ容量拡張 | キャッシュサーバのストレージ容量を拡張する。 | 変更要件発生時 |
|  | ファイルのアーカイブ作業 | 長期間アクセスのないファイルに対して部門側の要求に応じて手動アーカイブを実施する。 | 部門依頼発生時 |
|  | ファイルのアーカイブ復元作業 | アーカイブされたファイルに対して部門側の要求に応じて手動復元を実施する。 | 部門依頼発生時 |
|  | 部門アカウント追加対応 | 新規で部門アカウントが追加された場合、クラウドストレージ、キャッシュサーバの追加対応を実施する。 | 部門アカウント追加発生時 |

※作業内容詳細は別紙に記載

* 1. アカウント運用
     1. 運用方針

本システムを運用するために使用するアカウントは以下の方針に基づいて運用管理を実施する。

* + 適正な権限の付与：必要な人が必要な権限で操作・利用できる状態にする。
  + アカウントの可視化：現在利用しているアカウントを常に把握できる状態にする。

* + 1. アカウント種別

本システムを運用するために使用するアカウントは次の通り。

|  |  |
| --- | --- |
| アカウント | 対象 |
| 共通PF RD領域内ログイン用(運用者向け)アカウント | 共通PF内の各サービスおよびリソース |
| 監視システム(CloudWatch)利用向けアカウン | 共通PFのAWS IAM |
| サーバログイン用アカウント | ホストサーバ、運用管理サーバ、UTM |

* + 1. アカウント運用方式

運用アカウント対象：「‎4.1運用対象システム」に記載の範囲で作成されるアカウント対象とする。

* 運用方式：アカウント保有者の変更発生タイミングで、RD-ITサポートおよび利用ユーザからの申請に基づきアカウントの追加・変更・削除を実施する。年次でアカウントの棚卸を実施する。
  + 1. パスワード利用・変更ポリシー

|  |  |  |
| --- | --- | --- |
| アカウント | パスワード利用ポリシー | パスワード変更ポリシー |
| 共通PF RD領域内ログイン用(運用者向け)アカウント | 共通PF内の利用ルールに従う  （FF社内ドメインユーザ、鍵認証を用いた認証） | 共通PF内の利用ルールに従う |
| 監視システム(CloudWatch)利用向けアカウン | 共通PF内の利用ルールに従う  （FF社内ドメインユーザ、鍵認証を用いた認証） | 共通PF内の利用ルールに従う |
| サーバログイン用アカウント | パスワードポリシーの最小要件として以下とする。  ・長さは12文字以上とする。  ・次の4つのカテゴリ全てが使用されているものとする。  英大文字(AからZ)  英小文字(aからz)  数字(0から9)  アルファベット以外の文字(!、$、#、%など) | 定期的なパスワード変更は行わない。ただしインシデント発生、セキュリティリスク発生時に変更は実施する。 |

* + 1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| クラウドサービス(FF社内ユーザ)アカウント追加/削除 | 共通PF RD領域内へログインするユーザを追加/削除する。  ※本作業はICT戦オーナーにて実施する。 | 新規メンバーがRD-ITサポートに参画時、退職時等 |
| サーバOSアカウント追加/変更/削除 | サーバ(運用管理サーバ、キャッシュサーバ)のOSアカウントの追加/変更/削除を実施する。 | 新規メンバーがRD-ITサポートに参画時、退職時等 |
| アカウント棚卸 | 定期的にサーバ(運用管理サーバ、キャッシュサーバ)のアカウントの追加/変更/削除を実施する。 | 定期(年次) |
| アカウントPW変更 | パスワードポリシーの要件に基づきアカウントのPW変更を実施する。 | セキュリティインシデント発生時 |

* 1. ジョブ/スクリプト運用
     1. 運用方針

本システムで実行するジョブ/スクリプトは以下の方針に基づいて実施する。

* + 自動化：スクリプトを定期的なタスクへ設定し、自動化することで手動作業の負担を軽減し。効率的な業務を実現する。
  + 時間の有効利用：システムのリソースを有効活用するため、夜間など利用者が少ない時間帯にスクリプトを実行し、システムパフォーマンスの影響を最小限にする。
    1. ジョブ/スクリプト実行方式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| スクリプト機能 | 内容 | 実行日時 | 実行対象 | 実行ツール |
| サーバ再起動 | サーバの再起動を実施する。 | 毎月、第3月曜日 4:00 | ･ホストサーバ  ･運用管理サーバ | タスクスケジューラ |
| MACアドレスフィルター同期 | 開成拠点のDHCPサーバからフィルターリストを同期する。 | 10分毎 | ･運用管理サーバ(足柄・吉田南・小田原拠点) | タスクスケジューラ |
| バックアップ(Hyper-V) | Hyper-Vのエクスポート機能を使用したイメージバックアップを実施する。 | 毎日1:00 | ･運用管理サーバ | タスクスケジューラ |
| バックアップコピー | イメージバックアップをS3にコピーする。 | 毎日2:30 | ･ホストサーバ  ･運用管理サーバ | タスクスケジューラ |

* + 1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| スケジュールの追加/変更/削除 | 実行ツールにスケジュールの追加/変更/削除を実施する。 | スケジュールの追加等の変更要件発生時 |
| スクリプトの追加/変更/削除 | 実行スクリプトの追加/変更/削除を実施する。 | スクリプトの追加等の変更要件発生時 |

* 1. 監視運用
     1. 運用方針

本システムの監視運用は以下の方針に基づいて実施する。

* + 迅速な対応および障害予兆検知：迅速な一次対応とエスカレーションを行えるように障害の予兆検知を実現する。
  + 監視設定の柔軟な管理：監視設定および通知先のパラメータを状況に応じて柔軟に追加・変更・削除を実現する。

* + 1. 監視方針

本システムの運用監視は以下の実現方式に基づいて実装する。

* + アラート検知方法：Amazon CloudWatchのアラーム機能を使用する。
  + 通知方法：Amazon SNSおよびUTMのメール通知機能を用いてメール通知を行う。
  + 通知先：各RD部門管理者、RD-ITサポート
  + 監視時間：24時間365日

* + 1. 監視対象

監視種別と概要および監視対象を以下の通り記載する。  
具体的なメトリクス、ログの監視実装内容は「‎‎5.5.3.1**監視メトリクス**」および「‎5.5.3.2‎ 監視ログ」に記載する。

|  |  |  |
| --- | --- | --- |
| 監視種別 | 概要 | 監視対象 |
| 死活監視 | 監視対象の予期せぬ停止やネットワーク障害による通信不能状態を検知する ※Ping疎通での死活監視は行わずCloudWatchメトリクスが定期的に取得されていることで監視を行う | ・ホストサーバ ・運用管理サーバ |
| ディスク使用率監視 | ディスク使用率のしきい値の状態を検知する | ・ホストサーバ  ・FSx |
| ログ監視 | ログファイルをリアルタイムで監視し、パターンマッチした場合に通知 | ・運用管理サーバ ・キャッシュサーバ ・FSx ・CloudTrail |
| プロセス監視 | サーバ内のプロセス稼働監視を行い、プロセス停止を障害として検知する | ・ホストサーバ ・運用管理サーバ |
| セキュリティイベント監視 | 検出ルールに基づいた、アンチウイルス等の外部脅威リスクを検出と通知 | ・UTM |

* + - 1. **監視メトリクス**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 監視対象 | 監視種別 | 監視データ種別 | 監視間隔 | 監視方法 |
| ホストサーバ | 死活監視 | CloudWatchメトリクスの正常取得 | 5分 | CloudWatch Agent→CloudWatch |
|  | ディスク使用率監視 | ディスク使用率 | 5分 | CloudWatch Agent→CloudWatch |
|  | プロセス監視 | 以下サービスプロセス ･CloudWatch Agent ･Hyper-V | 5分 | CloudWatch Agent→CloudWatch |
|  | ログ監視 | 「‎5.5.3.2監視ログ」に記載のログ | 随時 | CloudWatch Agent→CloudWatch Logs |
| 運用管理サーバ | 死活監視 | CloudWatchメトリクスの正常取得 | 5分 | CloudWatch Agent→CloudWatch |
|  | プロセス監視 | 以下サービスプロセス ･DHCP ･DNS ･FTP ･CloudWatch Agent | 5分 | CloudWatch Agent→CloudWatch |
|  | ログ監視 | 「‎5.5.3.2監視ログ」に記載のログ | 常時 | CloudWatch Agent→CloudWatch Logs |
| キャッシュサーバ | ログ監視 | 「‎5.5.3.2監視ログ」に記載のログ | 常時 | Storage Gateway→CloudWatch Logs |
| FSx | ディスク使用率監視 | ディスク使用率 | 5分 | FSx→CloudWatch |
|  | ログ監視 | 「5.5.3.2監視ログ」に記載のログ | 常時 | FSx→CloudWatch Logs |
| CloudTrail | ログ監視 | 「5.5.3.2監視ログ」に記載のログ | 常時 | CloudTrail→CloudWatch Logs/S3 |
| UTM | セキュリティイベント監視 | ウイルス検知ログ | 常時 | UTM |

* + - 1. **監視ログ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 監視対象 | 取得ログ | 取得方法 | ログ保存場所と保持期間 | 保管用途 | 備考 |
| ホストサーバ | ･システムイベントログ | ①CloudWatch Agent→CloudWatch Logs  ②CloudWatch Logs→EventBridge→S3 | ①過去14日まで： CloudWatch Logs  ②180日まで：S3 | ①監視  ②障害調査・監査 |  |
| 運用管理サーバ | ･システムイベントログ ･ミドルウェア(DHCP/DNS/FTP)ログ | ①CloudWatch Agent→CloudWatch Logs  ②CloudWatch Logs→EventBridge→S3 | ①過去14日まで： CloudWatch Logs  ②180日まで：S3 | ①監視  ②障害調査・監査 |  |
| キャッシュサーバ | アクセスログ | ①Storage Gateway→CloudWatch Logs  ②CloudWatch Logs→EventBridge→S3 | ①過去14日まで： CloudWatch Logs  ②180日まで：S3 | ①監視  ②障害調査・監査 | 本システム上に蓄積されたファイルおよびフォルダの意図しない一括削除/リネームの監視 |
| FSx | アクセスログ | ①FSx→CloudWatch Logs  ②CloudWatch Logs→EventBridge→S3 | ①過去14日まで： CloudWatch Logs  ②180日まで：S3 | ①監視  ②障害調査・監査 |  |
| S3 | アクセスログ | S3 | 180日まで：S3 | 監視・障害調査 |  |
| VPC | トラフィックログ | VPC Flow Log→S3 | 180日まで：S3 | 障害調査・監査 |  |
| CloudTrail | AWS操作/設定変更ログ(管理イベントログ) | CloudTrail→S3 | 180日まで：S3 | 障害調査・監査 |  |
| UTM | トラフィックログ | UTM | 過去14日まで：UTM | 障害調査 |  |
|  | 設定変更ログ | UTM | 180日まで：UTM | 障害調査・監査 |  |
|  | ウイルス検知ログ | UTM | 過去30日まで：UTM | 監視・障害調査 |  |

* + 1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| 監視対応 | 障害アラートを検知して、一次切り分け、ICT戦オーナーエスカレーションを実施する。 | アラート検知時 |
| セキュリティインシデント対応 | ウイルスやマルウェアなどのアラートを検知した場合、一次対応を実施する。 | アラート検知時または共通PF運用者から連絡時 |
| 監視設定追加/変更/削除 | 監視システムのパラメータを追加/変更/削除を実施する。 | ･FSx作成時 ･ICT戦からパラメータ追加等の依頼発生時 |

※作業内容詳細は別紙に記載

* 1. ログ運用
     1. 運用方針

運用要件で定められた期間に本システムのログを保管し、必要な時(障害調査、監査対応)に参照・取得できるようにするため、ログ運用管理を行う。

* + 1. ログ収集・管理方式
  + 集約ツール：CloudWatch LogsおよびS3を用いてログの集約・管理を行う。
  + 取得/管理対象：「‎‎5.5.3.2監視ログ」を参照。
    1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| ログ収集・提出 | セキュリティインシデント等の調査、または監査対応で必要なログ提出依頼を受け付け、手順書に基づいたログ収集・提出を行う。  ※保守ベンダーに対する、障害調査に必要なログの収集・提出も含む | ログ提出の提出依頼発生時 |

* 1. バックアップ/リストア運用
     1. 運用方針

運用要件で定められた対象のバックアップを実施し、必要な時(障害発生に伴う迅速なリカバリー)に復旧できるようにするため、以下の方針に基づいてバックアップ/リストア運用を行う。

* + 定期的なデータ保全：システムとデータのバックアップを定期的に取得し、データの保全性を向上する。
  + 迅速な復旧：障害発生時には取得したバックアップを使用して迅速かつ確実なリストアを実施し、システムのダウンタイムを最小限に抑える。
  + 柔軟なファイル復旧：特定のファイルやデータの復元が必要な場合、迅速な対応を実現する。
    1. バックアップ方式

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 取得対象 | 頻度 | バックアップ種別 | 手法 | 保持期間（世代） | 保存先 | 備考 |
| ホストサーバ | 毎日1回 | システムバックアップ | 自動フルバックアップ (Windows Server Backup) | 1世代 | S3 | ･Windows Server Backupの機能で実施 |
| 運用管理サーバ | 毎日1回 | システムバックアップ | 自動フルバックアップ (Hyper-V) | 1世代 | S3 | ･Hyper-Vのエクスポート機能をスクリプトで実行 |
| FSx | 毎日2回 | データバックアップ | 自動バックアップ (ボリュームシャドウコピー) | 32日 | S3 |  |
| S3 | ファイル変更発生時 | データバックアップ | バージョニング機能 | 変更分 | S3 |  |

* + 1. リストア方式

|  |  |  |
| --- | --- | --- |
| リストア対象 | 手法 | 実施トリガー |
| ホストサーバ | バックアップイメージ(Windows Server Backup)から復元 | ･サーバ故障時 ･OS障害発生時 |
| 運用管理サーバ | バックアップイメージ(Hyper-V)から復元 | ･サーバ故障時 ･OS障害発生時 |
| キャッシュサーバ | 仮想アプライアンスイメージから復元 | ･サーバ故障時 ･OS障害発生時 |
| FSx | ボリュームシャドウコピーから復元 | 各RD部門にて実施 |
| S3 | バージョニングから復元 | 各RD部門依頼発生時 |

* + 1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| 自動バックアップ(ホストサーバ) | Windows標準機能(Windows Server Backup)を使用してシステムフルバックアップを取得する。 | 定期(毎日2:00) |
| 自動バックアップ(運用管理サーバ) | 仮想基盤(Hyper-V)のエクスポート機能を使用してシステムフルバックアップを取得する。 | 定期(毎日1:00) |
| 自動バックアップ(FSx) | ボリュームシャドウコピーを使用してデータバックアップを取得する。 | 定期(毎日0:00、12:00) |
| 自動バックアップ(S3) | バージョニング機能を使用してデータバックアップを取得する。 | ファイル変更発生時 |
| リストア(ホストサーバ) | 取得したバックアップを使用してリストアを実施する。 | サーバ障害、OS障害発生時 |
| リストア(運用管理サーバ) | 取得したバックアップを使用してリストアを実施する。 | サーバ障害、OS障害発生時 |
| リストア(キャッシュサーバ) | 仮想アプライアンスイメージを使用して作成する。 | サーバ障害、OS障害発生時 |
| ファイルデータリストア(FSx) | 各部門フォルダ配下にあるファイルデータを復元する必要がある場合、ボリュームシャドウコピーからファイルデータリストアを実施する。 | 各RD部門にてファイルデータ復元要件発生時 |
| ファイルデータリストア(S3) | 各部門フォルダ配下にあるファイルデータを復元する必要がある場合、バージョニングからファイルデータリストアを実施する。 | 各RD部門依頼発生時 |

* 1. 保守契約管理
     1. 運用方針

機器故障時に迅速な対応を実現できるよう、以下の方針に基づいて本システムの保守契約更新に必要な処理を実施する。

* + 契約情報の最新化：保守契約の内容・期間・問合せ等の情報を常に最新の状態に保ち、適切に管理する。
  + 契約更新の適時対応：製品の安定した継続利用のため、保守契約期間終了前に適時見積取得を行い、ICT戦が契約更新できる状態を実現する。

* + 1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| 保守契約の更新 | ･保守、ライセンス期間終了が近づいた際に保守、ライセンス契約更新の見積の取得を実施し、必要情報をICT戦に提供する。  ･保守契約の内容・期間・問合せ等の情報を常に最新の状態に保ち、適切に管理する。  ※保守契約の更新作業自体はICT戦にて実施する。 | 契約更新時期 |
| ライセンス適用 | ･入手したライセンス情報をもとにライセンス更新を実施する。 | ライセンス更新時期 |

* + 1. 保守機器一覧

|  |  |  |
| --- | --- | --- |
| 対象 | 保守 | ライセンス |
| ホストサーバ | HW保守  ・平日オンサイト保守 | Windows Server ライセンス |
| UTM | HW保守  ・メーカサポート  ・平日オンサイト保守 | サブスクリプションライセンス  ・Threat prevention subscription |
| ネットワークスイッチ  ※新規SW購入時 | HW保守  ・平日オンサイト保守 | サブスクリプションライセンス |

* 1. パッチ適用
     1. 運用方針

本システムのセキュリティホールを迅速に改善できるよう、以下の方針に基づいてパッチ適用を実施する。

* 定期的なシステム保全：定期的にパッチを適用し、システムのリスク最小化を実現する。
  + 1. パッチ適用方式

適用対象

* ハードウェア：ホストサーバ、運用管理サーバ、UTM
* ソフトウェア：DHCP、DNS、FTP、Hyper-V

※クラウド事業者がパッチ適用を行うものは設計対象外とする。

適用方式：

* ハードウェア：WSUSによるセキュリティパッチ自動適用で実現する。UTMについてはベンダーの指示に従い対応する。
* ソフトウェア：適用対象のソフトウェアはWindows OS標準搭載のものであるため、ハードウェアと同様の適用方式とする。
  + 1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| 定期パッチ適用 | 定期的にシステム基盤に対してパッチ適用を実施する。 | 定期(週次、月次) |
| 緊急パッチ適用 | システムに重大な影響を与えるパッチがリリースされた際に、緊急でシステム基盤に対してパッチ適用作業を実施する。 | 社内通知やベンダーからの連絡を受けて実施 |

* 1. 請求管理運用
     1. 運用方針

本システムにおいて各部門に適正な請求が実施できるよう請求管理運用を実施する。

* + 1. 運用方式

実施方式：

* Cost Explorerを使用して、負担部門コードごとのクラウドFS利用料を集計し、台帳更新を行う。
* 部署への付け替え先の負担部門コードの確認を行う。
* 更新後の台帳をICT戦へ送付する。
  + 1. 作業一覧

|  |  |  |
| --- | --- | --- |
| 運用作業 | 内容 | 実施トリガー |
| クラウドFS利用料集計 | 共有フォルダの負担部門コード単位の利用料を集計し、台帳更新を実施。 上期分集計時期：3月初旬、利用費集計期間2月～7月 下期分集計次期：9月初旬、利用費8月～1月 | 定期(半期) |
| 負担部門コード確認 | 部署管理者に対して、付け替え先の負担部門コードの確認を実施し、変更があれば台帳更新を実施。 | 定期(半期) ※クラウドFS利用料集計完了後 |
| 付け替え処理依頼 | 更新後の台帳をICT戦へ送付し、ICTに付け替え処理を依頼する。 | 定期(半期) ※負担部門コード確認完了後 |

* 1. 障害対応
     1. 障害対応方針

本システムにおいて障害が発生した場合は、以下の基本方針に基づいて対応を実施する。

* 運用体制に基づいた対応：障害発生時には、「‎3.1運用体制図」に従い、迅速に一次対応および順次エスカレーションを実施する。
* 実施手順：別紙「障害対応手順書.xlsx」を参照し、適切な障害対応および障害復旧を実施する。
* 連絡先：別紙「連絡先一覧.xlsx」を参照し、適切な関係者へ連絡を行う。
  + 障害復旧目標：本システムにおける障害復旧目標を1日以内とする。
  1. 問合せ対応
     1. 問合せ対応方針

本システムに対する問合せ対応業務の方針は以下とする。

* 受付時間：問合せ受付時間は以下の通り、FFS営業時間内とする。

受付時間：FFS営業日 8:20~16:45

* 連絡先：問合せ連絡先は以下の通り、メールおよび電話で受け付ける。

メールアドレス：shm-ffs-rd-it-support@fujifilm.com

電話番号：090-2762-2456

* 一次回答目安：問合せ受付後、2営業日以内を目安に一次回答を行う。ただし、至急の場合を除き、ベストエフォートとする。

* 1. 計画メンテナンス対応
     1. 計画メンテナンス対応方針

本システムに対する計画メンテナンス対応業務の方針は以下とする。

* 対象：「‎4.1‎4.1運用対象システム」を参照とする。
* 方式：対象機器(※)および対象拠点、AWS(共通PF)環境、RD-WAN回線のメンテナンススケジュールに応じて、各RD部門管理者およびICT戦(共通PF運用)、ICT戦(NW運用)に対して周知を行い、サービス影響を最小限にした上で、メンテナンス作業を実施する。※OSバージョンアップを含む。
* 実施手順：
  + 運用対象システムの特性とベンダー公開情報を組み合わせた検証済み手順。
* 注意事項：停止を要する作業が発生する場合、原則2週間以上前に関係各所にポータルサイトおよびメールにて通知する。

以上