

A R アドバンステクノロジー株式会社

cnaris-MSP サービス仕様書

目次

1 サービス概要	4
1-1 サービス説明	4
1-2 サービス提供条件	4
1-3 サービス提供イメージ	5
1-4 サービス構成	6
1-5 サービスプラン	6
1-6 サービス導入の流れ	7
2 初期導入	8
2-1 コミュニケーションツール	8
2-2 監視ツール	9
2-3 運用・監視回線	9
2-4 マネジメント対象	10
2-5 監視項目の設定	11
2-6 障害対応手順	11
2-7 通知情報	11
3 基本サービス	13
3-1 サービス品質目標	13
3-2 WEB モニタ	13
3-3 問い合わせ窓口	15
4 監視仕様	16
4-1 外部監視	16
4-2 内部監視	17
4-3 監視ツールについて	17
4-4 クラウドサービス監視	19
5 オペレーション仕様	20
5-1 モニタリング	20
5-2 自動通知	21
5-3 有人通知	24
5-4 チャットシステムへの通知	25
5-5 大規模障害発生時の対応方針	26
5-6 障害一次対応	26
5-7 障害二次対応	28
5-8 定期作業	30

5-9 依頼作業 30

5-10 静観依頼受付 33

6 付則..... エラー! ブックマークが定義されていません。

1 サービス概要

本サービスは弊社から外部委託先によるサービス提供を含んでおります。

1-1 サービス説明

お客様の環境で稼働している IT サービスが常時安定稼働の継続ができるように、運用監視専用の拠点（以降「コントロールセンター」）から 24 時間 365 日の自動検知・制御システムを駆使しながら運用監視を行うサービスです。

お客様が抱える日々の運用監視をアウトソースいただくことにより、IT サービスの品質を維持しながら運用の負荷とコストを軽減し、お客様本来の業務に専念していただくことを目的とします。

本サービスは下記の特徴を有するサービスです。

- オンプレミスからパブリッククラウドまで幅広い環境への運用監視に対応
- 監視ツールに依存しない柔軟な監視運用サービスを提供
- コントロールセンターは情報セキュリティマネジメントシステム「ISO27001」の認証を取得し、安全で信頼性の高いサービスを提供

1-2 サービス提供条件

本サービスをご利用いただくにあたって下記の条件があります。

- 提供言語は原則日本語となります。（英語での対応は別途でご相談ください）
- 有人での対応はリモートのみとなります。現地へ作業員を派遣し対応を行うオンサイト作業のサービス提供はありません。

1-3 サービス提供イメージ

本サービスは外部委託先指定のコントロールセンターで提供するサービスです。コントロールセンターは外部委託先正社員のエンジニアが24時間365日常駐する運用拠点です。

本サービスは、弊社指定の自動監視ツール(以下「指定ツール」)による監視が標準となります。内部監視は監視対象サーバに指定ツールエージェントをインストールし実現します。監視データを収集するデータサーバはコントロールセンターに設置されており、エージェントからHTTPSを利用したアウトバウンド通信(Port#443から外部への通信許可が必要)となります。指定ツールの詳細情報につきましては、契約時に提供する別紙「監視サービス仕様書」を参照ください。

また、監視ツールは、お客様指定のツールも利用可能です。指定ツール以外の監視ツールからのアラートをメールで送信できる必要があります。詳細につきましては、後述の「4-3 監視ツールについて」を参照ください。

1-4 サービス構成

本サービスの構成要素は下記のとおりです。内容によって対応可能時間が異なります。

項目	実施内容	対応可能時間
障害の検知・通知	監視ツールによる障害検知	24時間 365日
	障害発生時のエスカレーション	24時間 365日
障害対応	障害発生時の一次対応	24時間 365日
	障害発生時の二次対応	24時間 365日
運用作業	定期的に行われる運用作業の代行	24時間 365日
	依頼に基づく運用作業の代行	平日 9:30 - 17:30
監視データ閲覧	Web モニタの提供 - サービスのリソース状況の確認 - 監視レポートの閲覧	24時間 365日

1-5 サービスプラン

本サービスは、下記の4つのプランをご用意しております。お客様の要望に合わせてプランを選択いただけます。

- Basic プラン
- Standard プラン
- Professional プラン
- Full Management プラン

各プランでの対応内容は下記の通りとなります。

対応内容	Basic	Standard	Professional	Full Management
障害の検知・通知	○	○	○	○
障害一次対応	—	○	○	○
障害二次対応	—	—	○	○
定期作業	—	—	—	○
月次運用レポート	—	○	○	○※1

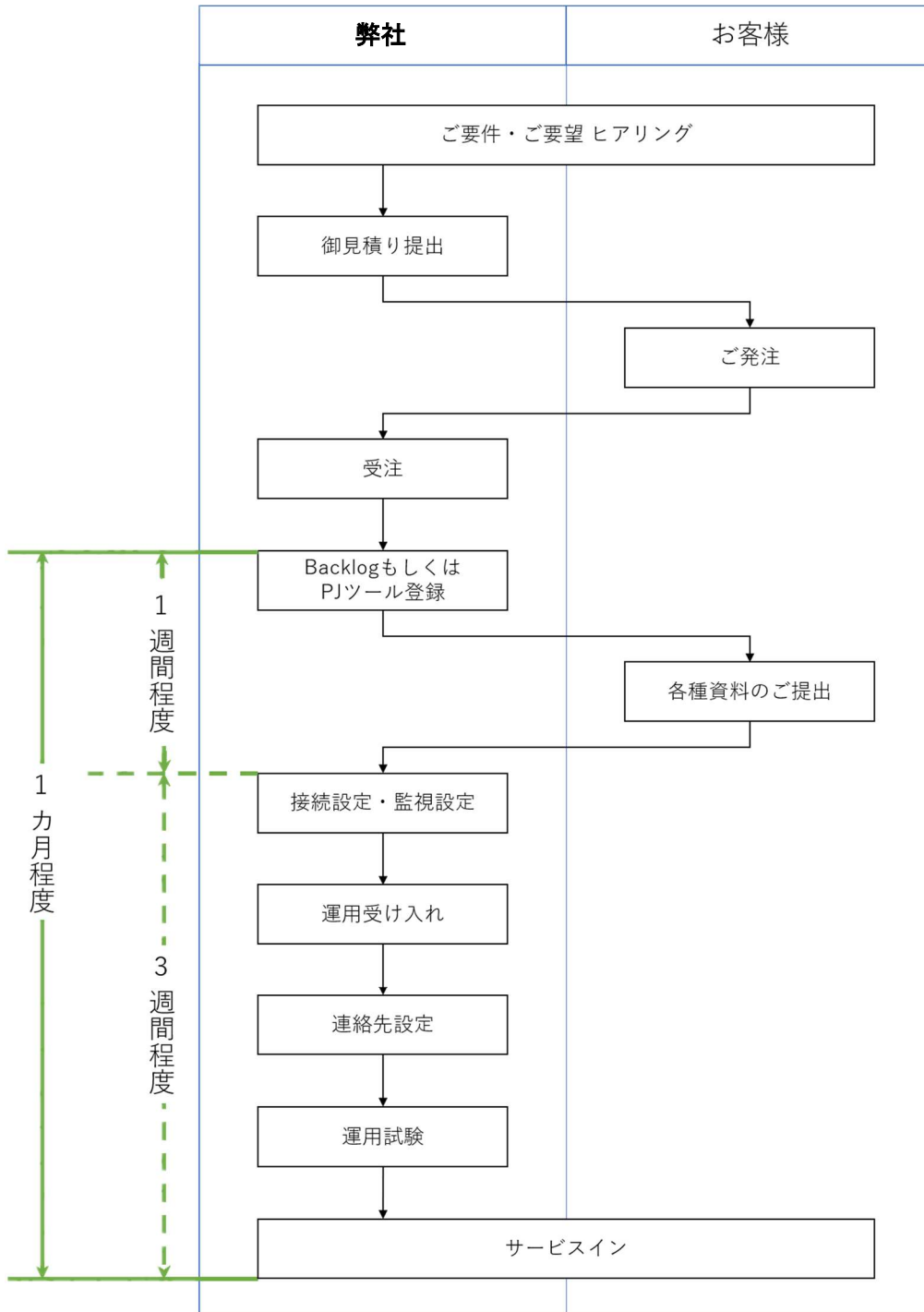
○：対応可、—：対応不可

※1 ご要望に応じて月次報告会を開催

対応内容の詳細は後述の「5 オペレーション仕様」を参照ください。

1-6 サービス導入の流れ

サービスのご提供までは約1カ月が目安となります。但し、運用監視のご要件やボリュームによって変動いたします。サービス導入の流れは概ね下図の通りとなります。



2 初期導入

本サービスを導入にあたり、必要な環境の準備や取り決めに定義します。

2-1 コミュニケーションツール

初期導入からサービス導入後の各種設定の変更や問い合わせ、運用のご依頼などのやり取りを管理するため、弊社では Backlog を採用しております。また、弊社用意の Backlog 以外にお客様ご指定のコミュニケーションツールをご希望の場合は別途ご相談ください。

2-1-1 弊社用意の Backlog について

1) ログイン方法

ご契約後に弊社 Backlog へ招待する方のお名前、メールアドレスをお伺いします。その後、送信される招待メールにログイン URL が記載されます。

2) 弊社への連絡方法

「課題の追加」から内容を記載いただき、担当者に「JIG-SAW サポートチーム」を指定ください。

2-1-2 制限事項

- お客様ご指定のコミュニケーションツールの管理主体はお客様となります。
- コミュニケーションツールのリアルタイムチャット機能の受入れは不可となります。
- コミュニケーションツールが障害などの何らかの理由で利用できない場合はメールでの連絡に代用となります。

2-2 監視ツール

本サービス標準の監視ツールは自社で独自開発を行っている監視ツール「指定ツール」となります。また、お客様のご希望される監視ツールをご利用いただくことも可能です。但し、指定ツール以外の監視ツールを利用する場合、下記の制限があります。

- 監視ツールの管理はお客様となります。
- 監視ツールの導入および設定、変更などの作業はお客様で行っていただきます。

監視ツールの違いによる、弊社とお客様の役割分担としては下記となります。

項目	指定ツール	指定ツール以外の監視ツール
監視ツールの導入	弊社 ※	お客様
監視ツールの設定・変更	弊社	お客様
監視ツールの管理	弊社	お客様

※ 監視対象へリモート接続できない場合はお客様にて監視エージェントのインストールをご対応いただく場合があります。

2-3 運用・監視回線

本サービスの通信回線は通常、弊社インターネット回線の利用となります。VPN 接続などインターネット回線以外をご希望の場合も受け入れ可能です。(別途ご相談ください)

2-3-1 通信回線仕様

弊社通信回線は、運用と監視で完全に独立しており、それぞれ3経路インターネット回線を保有しております。平時は全経路並列で利用し、可用性を高めています。通信断が発生した場合は、他回線にて継続して監視サービスを提供可能です。但し、全経路での運用・監視を保証するものではありません。

2-3-2 インターネット回線以外の受け入れ

ご希望される場合は、インターネット回線以外の受け入れもご相談により対応可能です。但し、VPN 機器や回線費用はお客様のご負担となります。

1) 回線の役割分担について

回線の違いによる、弊社とお客様の役割分担は下記の通りとなります。

回線	弊社インターネット回線	お客様指定の回線
機器・回線のご用意	JIG-SAW	お客様
回線の管理	JIG-SAW	お客様

2) 回線受け入れのために事前に必要な情報

- 回線種別（IPsec-VPN など）
 - お客様側機器の機種情報（製造メーカ、製品名、型番など）
 - お客様側のネットワークアドレス情報
- ※ なお、回線や機種によっては受け入れをお断りする場合があります。

2-4 マネジメント対象

「マネジメント対象」とは本サービスの契約に基づくサービス適用対象となります。マネジメント対象の情報はヒアリングシート「マネジメント対象一覧」にお客様にて記載いただきます。

マネジメント対象一覧に記載いただく情報の例

システム名	対象のシステム名（ホスト名）
IP アドレス	対象の IP アドレス
ユーザー／パスワード／認証方式	対象へ接続する際に利用する情報
接続方法	対象への接続方法
権限変更方法	管理者権限への変更方法
オートスケール	クラウドサービス機能によるオートスケール有無
計画停止	メンテナンスなどの計画停止時間
サービス名	クラウドサービス名
システム ID	クラウドサービスの識別 ID

2-5 監視項目の設定

2-5-1 指定ツール利用の場合

弊社で監視項目の設定を行います。設定値はカスタマイズ可能でヒアリングシート「指定ツール監視設定一覧」をお客様にて記載いただきます。弊社エンジニアで一般的な監視項目を提案、設定することも可能です。

2-5-2 指定ツール以外の監視ツールの場合

監視ツールから弊社の監視用メールアドレスへアラートを送信いただきます。アラートの件名、本文とのマッチ条件により、検知・対応いたしますのであらかじめマッチ条件を定義します。

定義したマッチ条件は「指定ツールメール監視設定書」として弊社エンジニアがとりまとめを行います。

2-6 障害対応手順

障害発生後の一次対応として作業実施をご希望の場合、事前に共有いただいた作業手順書の受け入れを行います。作業手順書をお持ちでない場合はご相談により弊社エンジニアにて作成の支援も可能です。

また作業手順書の受け入れには下記の制限があります。

- ※ 着手から完了まで15分以内に収まる手順であること
- ※ 作業に分岐がある場合、判断基準が明確であること

2-7 通知情報

2-7-1 通知方法

アラート検知後のお客様への通知方法を定義します。通知方法は下記から選択いただけます。また、複数の通知方法を併用可能です。

- 電話
- メール
- チャットツール (Slack、Chatwork、Teams に対応)
- ※ チャットツールへの通知はコントロールセンターからの一方向発信のみで弊社エンジニアとのリアルタイムチャットには対応しません。

2-7-2 通知設定情報

通知設定を行うにあたり、下記情報を準備いただく必要があります。

通知方法	準備いただく情報
電話	<ul style="list-style-type: none"> ・通知先担当者の情報 <ul style="list-style-type: none"> - 会社名 - 担当者名 - 担当者の電話番号 ・通知先担当者への連絡順
メール	<ul style="list-style-type: none"> ・通知先担当者の情報 <ul style="list-style-type: none"> - 会社名 - 担当者名 - 担当者のメールアドレス
チャットツール ※	<ul style="list-style-type: none"> ・通知先チャットツールの情報 <ul style="list-style-type: none"> - 通知先チャンネル - 通知時にメンションが必要なアカウント ・通知用の弊社アカウントのご用意

※ 通知先チャットツールはお客様のご用意となります。

2-7-3 運用試験

サービスイン前に運用試験を実施します。運用試験項目はお客様と協議のうえ決定します。主な試験項目は下記です。

1) アラート検知テスト

監視ツールからテストアラートを発報し、コントロールセンターで正しく検知できるかを試験します。

2) 通知テスト

設定した通知リストへ正しく通知が可能かを試験します。

3) 手順書リハーサル

受け入れする手順書通りに作業が完了できるかを試験します。

3 基本サービス

24 時間 365 日の有人による運用監視サービスです。サービスは全てリモートでの提供となります。本章では全てのサービスプランでご利用頂ける内容について記載します。

3-1 サービス品質目標

弊社では障害検知から初動対応を行うまでの時間にサービス品質目標 (Service Level Objective) を設けています。コントロールセンターでの障害検知後 15 分以内に初動対応を着手することを目標時間とします。初動対応は下記のいずれかとなります。

- 電話通知 (手動/自動)
- メール通知 (手動/自動)
- 事前に取り決められた障害復旧対応

3-2 Web モニタ

月次の監視レポートの閲覧、および收拾した監視データの閲覧が可能なリソースモニタ機能です。Web モニタは主に下記の機能を有します。機能は随時アップデートされ本書に記載のない機能や、詳細な仕様は Web モニタ上から参照できるヘルプページを参照ください。

3-2-1 ログイン URL

ログイン URL はご契約時に開示、ログイン ID、パスワードは契約時に発行されます。

3-2-2 ヘルプページ URL

各機能の詳細な仕様が記載されたヘルプページとなります。Web モニタ機能について本書とヘルプページで記載が異なる場合はヘルプページを正とします。URL はご契約時に開示されます。

3-2-3 Web モニタの機能（一部）

お知らせ	Web モニタの機能に関するアップデート／バージョンアップ情報などが掲載されます。
ダッシュボード	最新のサーバステータスと発生警報統計などが表示できます。
リソースモニタ	指定の日時から遡った期間の監視データがグラフで表示できます。
監視設定一覧	各種監視項目における警報対象およびその設定値が表示できます。表示される設定情報は最新の設定値となります。
監視レポート	毎月過去 1 カ月分の監視の発生状況が出力できます。
発生中警報一覧	発生中の警報が一覧でご確認いただけます。
静観設定	サーバのメンテナンス等であらかじめ警報が発生することが予測される場合に、指定した期間に発生した警報を静観(抑止)する機能です。

3-3 問い合わせ窓口

3-3-1 契約に関する窓口（営業）

契約、請求に関する問い合わせ、サービスに関する問い合わせ窓口となります。

窓口時間	弊社営業日 10:00~18:00
連絡方法	電話、メール
連絡先	担当営業

3-3-2 障害状況の確認窓口

発生した障害に関する問い合わせを受け付けます。

窓口時間	24 時間 365 日
連絡方法	電話、メール
連絡先	コントロールセンター

3-3-3 監視内容の変更窓口

監視設定の変更や、アラート抑止に関する問い合わせを受け付けます。証跡を残すためメールまたはコミュニケーションツールでの受け付けとなります。

窓口時間	24 時間 365 日
連絡方法	メール、コミュニケーションツール
連絡先	コントロールセンター

3-3-4 依頼作業に関する窓口

各種システムへの設定追加・変更等、ご依頼を契機に実施する作業に関する問い合わせを受け付けます。

窓口時間	平日 9:30~18:30
連絡方法	コミュニケーションツール
連絡先	コントロールセンター

4 監視仕様

4-1 外部監視

監視対象サーバに対して、外部のサーバからアクセスを行いサービスの死活、レスポンスを監視する方式となります。

4-1-1 通信仕様

コントロールセンターからインターネット経由にて監視対象サーバにアクセスし監視を行います。コントロールセンターの接続元 IP セグメントから監視対象サーバに対してインバウンドの接続が必要となります。詳細は「指定ツール監視サービス仕様」を参照ください。

4-1-2 監視周期

外部監視の監視周期は3分となります。詳細は「指定ツール監視サービス仕様」を参照ください。

4-1-3 外部監視項目

監視可能な項目の一例です。詳細は「指定ツール監視サービス仕様」を参照ください。

監視項目	概要
ICMP	ICMP の「echo request」パケットを送信し、「echo reply」パケットが返ってくるかを監視します。
URI	指定した URI に対して HTTP リクエストを送信し、レスポンスが返ってくるか、またレスポンスの内容を監視します。
SSL 証明書有効期限	指定した FQDN または IP アドレス、ポート番号に対して SSL でアクセスし、取得した SSL 証明書の有効期限残日数を監視します。
汎用 TCP ポート	指定した FQDN または IP アドレスの指定ポートに対して TCP 接続を行い、接続可能かどうかを監視します。
SMTP	指定した FQDN または IP アドレスの指定ポートに対して、SMTP 接続を行い、接続可能かどうかを監視します。
POP3	指定した FQDN または IP アドレスの指定ポートに対して、POP3 接続を行い、接続可能かどうかを監視します。
IMAP	指定した FQDN または IP アドレスの指定ポートに対して、IMAP 接続を行い、接続可能かどうかを監視します。
SSH	指定した FQDN または IP アドレスの指定ポートに対して、SSH 接続を行い、接続可能かどうかを監視します。
Oracle	指定した FQDN または IP アドレスの指定ポートに対して、ODBC 接続を行い、指定したデータベースに対して任意の SQL を実行し、正しいレスポンスが返ってくるかどうかを監視します。

MySQL	指定した FQDN または IP アドレスの指定ポートに対して、MySQL 接続を行い、指定したデータベースに対して任意の SQL を実行し、正しいレスポンスが返ってくるかどうかを監視します。
PostgreSQL	指定した FQDN または IP アドレスの指定ポートに対して、PostgreSQL 接続を行い、指定したデータベースに対して任意の SQL を実行し、正しいレスポンスが返ってくるかどうかを監視します。
Sybase	指定した FQDN または IP アドレスの指定ポートに対して、Sybase 接続を行い、指定したデータベースに対して任意の SQL を実行し、正しいレスポンスが返ってくるかどうかを監視します。
MSSQL	指定した FQDN または IP アドレスの指定ポートに対して、MSSQL 接続を行い、指定したデータベースに対して任意の SQL を実行し、正しいレスポンスが返ってくるかどうかを監視します。
SNMP 応答	指定した FQDN または IP アドレスに対して、SNMP 接続を行い、指定したコミュニティ、OID に対するレスポンスを監視します。 レスポンスの結果が期待した結果とならない場合にエラーとすることも可能です。
SNMP リソース	指定した FQDN または IP アドレスに対して、SNMP 接続を行い、指定したコミュニティ名でリソース情報を収集します。

4-2 内部監視

内部監視は監視対象となるサーバにエージェントプログラムをインストールします。エージェントプログラムがサーバ内のデータを収集し、外部のデータ収集サーバにネットワーク経由でデータを送信する方式です。

4-3 監視ツールについて

弊社では自社開発した監視ツール「指定ツール」を提供しております。指定ツールの導入には監視対象にエージェントプログラムをインストールいただきます。

また、お客様で導入済みの「指定ツール以外の監視ツール」も受け入れ可能です。

4-3-1 指定ツールでの監視

1) 通信仕様

監視対象サーバからコントロールセンターに設置されたデータ収集サーバに対してアウトバウンドのインターネット通信が必要です。接続先ポート番号は 443 です。通信は TLS 接続により暗号化 (AES256) されます。詳細は「指定ツール監視サービス仕様」を参照ください。

また、直接インターネットに接続できない環境では、CONNECT メソッドに対応した Web proxy サーバ(認証なし)経由で接続や、弊社監視ネットワークとの拠点間 VPN(IPsec) 接続も可能ですが、通信仕様につきましては別途ご相談ください。

2) 監視周期

内部監視の監視周期は3分となります。詳細は「指定ツール監視サービス仕様」を参照ください。

3) 内部監視項目

監視可能な項目の一例です。詳細は「指定ツール監視サービス仕様」を参照ください。

監視	概要
リソース監視	CPU 使用率、メモリ使用率、ディスク使用率、ロードアベレージなどのリソース情報を収集します。
ネットワーク使用率監視	受信バイト数、送信バイト数から使用率を計算します。
プロセス監視	指定のプロセスの死活を監視します。
ログ監視	監視対象サーバ上の指定したログファイルに指定したパターンのログが出力された場合に、そのログとマッチした行数を収集します。
Windows サービス監視	service control manager(SCM)を利用してサービスの状態監視を行います。

4-3-2 指定ツール以外の監視ツール

指定ツール以外の監視ツールは「アラートメールを弊社宛てに送信できる」システムであれば、受け入れ可能です。アラートメールを弊社で受信し各種対応を行います。また、指定ツールとの併用は可能です。

1) 制限事項

- 監視できる内容は使用するツールまたはシステムに準じます。
- 監視ツールまたはシステムの管理はお客様となり、監視ツールまたはシステム自体のトラブルにおいて弊社は責任を負いません。
- 監視設定はお客様にて実施いただきます。
- 監視ツールまたはシステムを弊社環境下には設置できません。お客様管理下に設置することを前提とします。
- Web モニタは利用できません。

4-4 クラウドサービス監視

指定ツールではクラウドサービスで提供される監視サービスとの API 連携によりデータ収集を行うことが可能です。

※ クラウド基盤側の障害等に起因する対処については後述の「5-5 大規模障害発生時の対応方針」を参照ください。

4-4-1 AWS CloudWatch

Amazon Web Service の監視サービスである CloudWatch API から情報を取得して監視します。下記は対応する監視の一例です。詳細は「指定ツール監視サービス仕様書」を参照ください。

監視項目	概要
RDS	リソース情報やコネクション数などのメトリクスを監視可能です。
ALB/ELB/NLB	ヘルスチェックやエラー数のメトリクスを監視可能です。
ElastiCache	リソース情報やキャッシュ接続回数などのメトリクスを監視可能です。
CloudFront	各リクエストのエラーコード率や全体のエラー発生率などのメトリクスを監視可能です。
Aurora	リソース情報やソース DB クラスターからレプリカ DB クラスターまでの遅延などのメトリクスを監視可能です。
EC2	CPU クレジット数やステータスチェックなどのメトリクスを監視可能です。
DynamoDB	キャパシティーユニットの数やアカウントが使用する、プロビジョニングされた読み取りキャパシティーユニットの割合などのメトリクスを監視可能です。
Elasticsearch	リソース情報やクラスターノードのストレージ容量やクラスターステータスなどのメトリクスを監視可能です。
Lambda	関数コードが実行された回数や関数エラー数などのメトリクスを監視可能です。
APIGateway	クライアントまたはサーバ側エラー数やレスポンス遅延などのメトリクスを監視可能です。
ECS	クラスターやサービスで仕様されているリソース割合などのメトリクスを監視可能です。
AutoScaling グループ	AutoScaling グループの最小・最大サイズなどのメトリクスを監視可能です。

5 オペレーション仕様

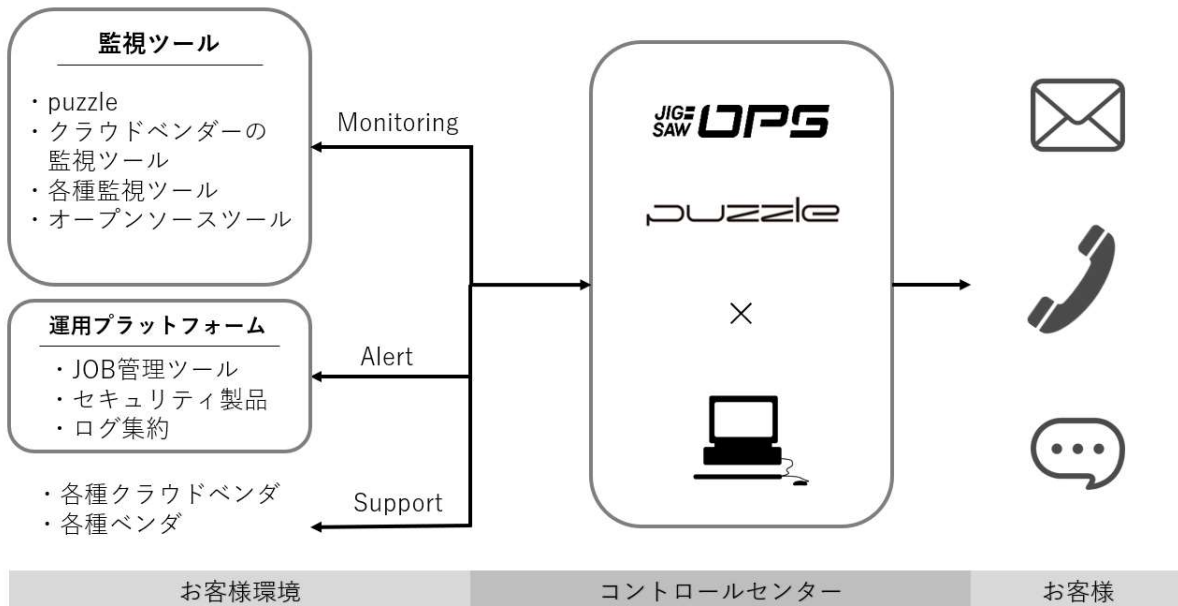
コントロールセンターの各オペレーション対応について記載します。有人対応以外にコントロールセンターのシステム上で自動処理される内容も含まれます。前述のサービスプランによって対応可否が異なるため、下記アイコンにて対応するサービスプランを示します。

アイコン	プラン
B	Basic
S	Standard
P	Professional
F	Full Management

5-1 モニタリング

監視ツールから発報された障害アラートはコントロールセンターで検知します。検知後は、導入時に取り決めた内容に応じた対応(通知や障害対応)を実施します。

下図は基本となるモニタリングイメージです。



5-2 自動通知

対応プラン： **B** **S** **P** **F**

監視ツールからのアラート検知後の通知対応を自動処理します。弊社エンジニアを介さずに実施可能なので、迅速な通知が必要かつ、有人による障害の確認などが不要な場合に利用可能です。

5-2-1 自動メール通知

通知先メールアドレスおよびアラートメールの件名、本文がカスタマイズ可能です。

1) 通知メールフォーマット

Subject: 【サーバ名】 <警報名>警報発生のご連絡
ご担当者様

お世話になっております。JIG-SAW コントロールセンターです。
サーバの警報についてご連絡いたします。

【サーバ名】

【初回発生時刻】

【警報検知時刻】

【警報内容】

<警報名>を検知しました。

【警報レベル】

【リソース使用率】

以上、ご連絡させていただきます。

2) 制限事項

- ・ 通知メールが通知先メールアドレスへの到達性を保証するものではありません。

5-2-2 自動架電通知（オートコール）

合成音声の架電です。架電リストへの順次架電と一斉架電が選択可能です。コール受電後はキーパッド操作が必須です。受電後はキーパッドの「1」を押すことによりコール成功の判定となります。押されないまま通話が終了した場合はコール失敗と判定され次の架電先へ架電されます。架電先リストの全員に繋がらなかった場合は、繋がらなかった旨をメール送信して終了となります。また、一部機能がカスタマイズ可能です。

1) キーパッド操作一覧

キーパッド	アクション
1	コール成功
3	再度メッセージを確認
*	通話が中断され、コール失敗
2、4～9	「3」と同様に再度メッセージの確認

2) カスタマイズ可能な設定

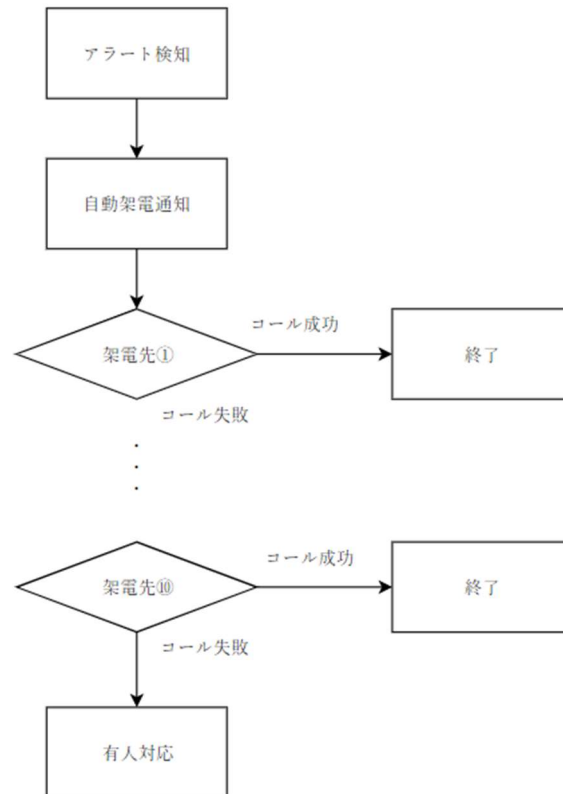
項目	内容	規定値	設定可能範囲
スキップ間隔 (分)	アラート多発時の連続架電を抑止する間隔です。架電対象者が同じであれば異なるアラートでもこの間隔は架電されません。	60	3 - 1440
リトライ回数	架電リスト上の全ての番号に繋がらない場合のリトライ回数です。	0	0 - 10
応答待ち時間 (秒)	コール時間です。この時間内に電話に出るか、留守電に切り替わらない場合は、次の架電対象者へ架電します。	30	1 - 180

制限事項

- 受電後の最大通話時間は2分となります。2分を超過すると通話終了でコール失敗の判定となります。
- 通知リストへの登録電話番号数は最大10件までとなります。
- 留守番電話にメッセージを残す機能はありません。
- 留守番電話になった場合はキーパッド操作が確認できない限りコール失敗の判定となります。

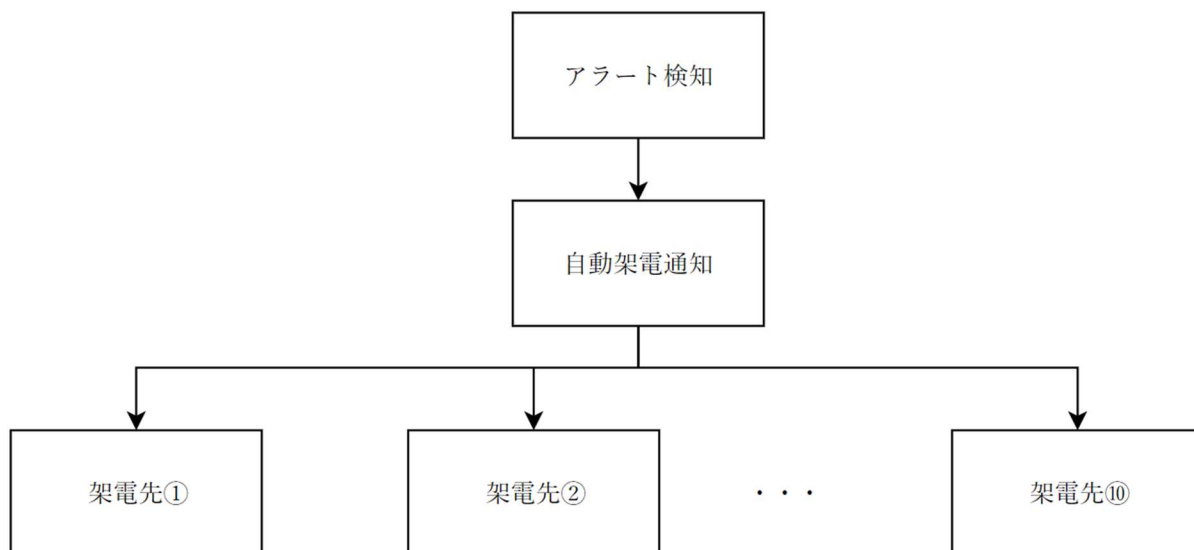
3) 順次架電フロー

通知先リストの優先順位に沿って順番に架電します。最初にキーパッドの「1」が押された時点でコール成功となり下位の通知先へ架電はされません。



4) 一斉架電フロー

通知先リストに登録の番号へ同時にコールが可能です。架電先いずれかで最初にキーパッドの「1」が押された時点でコール成功となり通知が終了となります。



5-3 有人通知

対応プラン： B S P F

弊社エンジニアがアラート内容を確認し必要に応じて通知を行います。一次対応として障害の切り分けや復旧対応が必要な場合に利用可能です。

5-3-1 有人メール通知

コントロールセンターシステム上から手動でメール送信します。メールフォーマットは前述の自動メール通知と同様となり件名や本文のカスタマイズが可能です。

5-3-2 有人架電通知

アラートの種別および発生時間帯(営業時間内/営業時間外)に応じて、最大5件までの連絡先リストに優先順位に従い順次架電いたします。最初の1名に繋がった時点で通知対応は終了します。連絡先リストの1巡目でどなたにも繋がらない場合は最大2巡目まで対応します。2巡でどなたにも繋がらない場合はメールを送信し通知対応を終了します。

通話内容は、電話対応品質向上のため録音をしています。

5-4 チャットシステムへの通知

対応プラン： **B** **S** **P** **F**

システムからお客様がご利用しているチャットシステムに任意のメッセージを通知します。
Slack, Chatwork, Teams へのアラート発生時の自動通知、または有人での通知が可能です。

1) 通知フォーマット

<発生イベント> <ノード名> <警報名> <検知データ> <警報レベル> <検知時間> <ログのサマリ>

項目	内容
発生イベント	アラートのステータス ※発生、継続中、復旧の3種。
ノード名	アラート発生ノード
警報名	監視項目名
検知データ	監視ツールが収集した実測値
警報レベル	複数段階閾値が設定されている場合の警報レベル ※低、中、高の3種。
検知時間	アラートの検知時刻
ログのサマリ	検出したログ(1024文字まで) ※ログ監視の場合のみ出力されます。

2) 制限事項

- 対応するチャットシステムは Slack, Chatwork, Teams のみです。
- チャットツールへの通知はコントロールセンターからの一方向発信のみで弊社エンジニアとのリアルタイムチャットには対応しません。

5-5 大規模障害発生時の対応方針

1) クラウド事業者側の大規模障害に起因する場合

大量のアラート検知により通常のオペレーション対応が不可能とコントロールセンターが判断した際は、ご指定頂いた緊急通知先に設定されているメールアドレスに対して弊社の対応状況を一齐配信します。

2) 単一システム内での大量アラート検知

コントロールセンターが通常のオペレーション対応が不可能と判断した際は、アラート通知先に設定されている連絡先へ電話連絡のうえ、対応をお客様と協議いたします。連絡がつかない場合はアラートの発生順に順次対応しますがベストエフォートとなります。

5-6 障害一次対応

対応プラン： **S** **P** **F**

障害検知後あらかじめ取り決めた手順書に基づいて障害の切り分け、または復旧作業などを有人で対応します。作業後に障害が復旧しない場合は通知先リストへエスカレーションとなります。

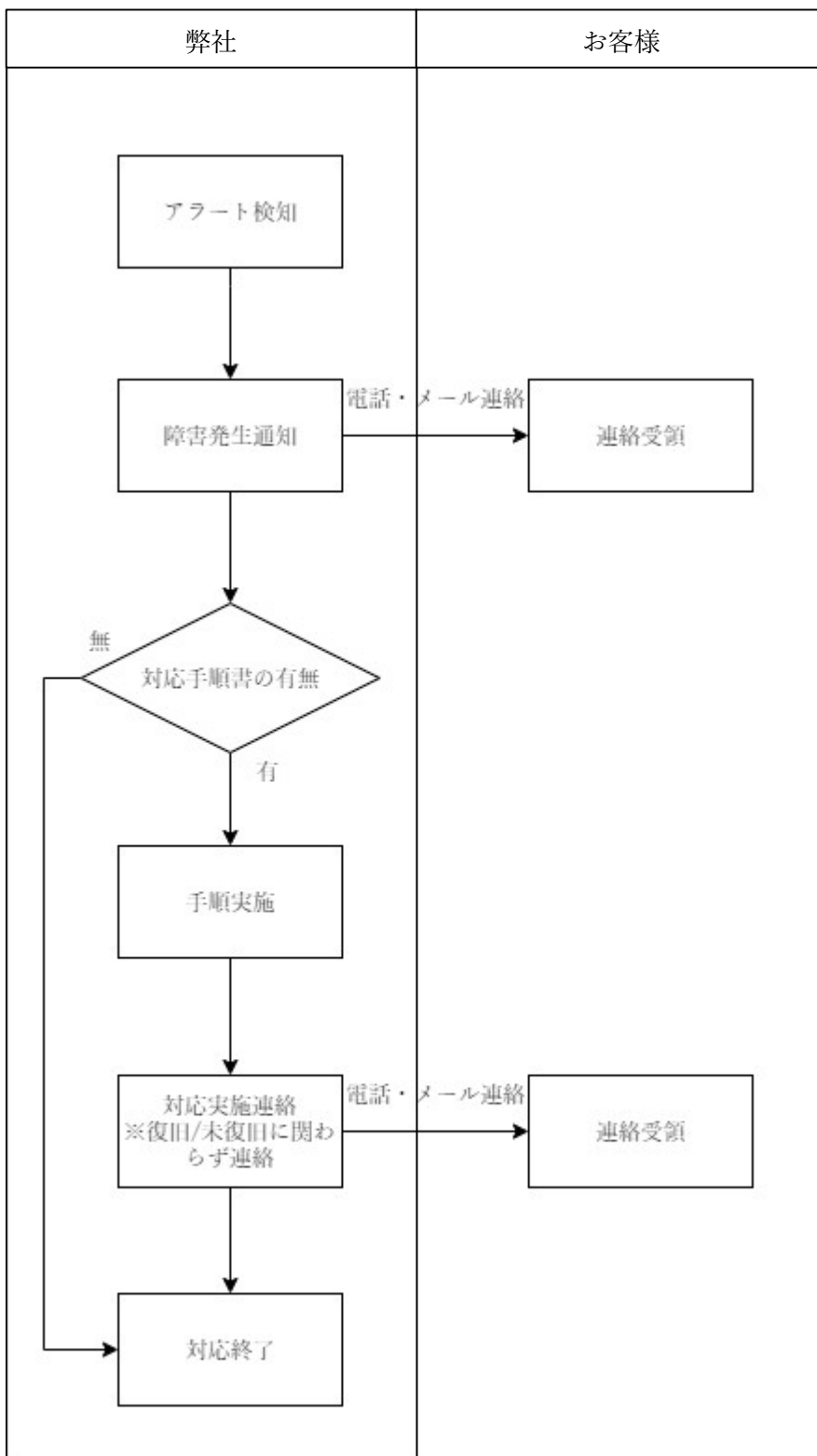
項目	内容
作業対象	マネジメント対象のみとなります。契約のない対象への作業は実施できません。
1回の作業時間	着手から完了まで1回15分以内の作業が対応可能です。
障害の原因調査	即時性を求めない作業は障害一次対応には含まれません。障害の原因調査、ログの収集等のお客様との連携、時間を要する作業は障害二次対応となります。
作業判断	手順書は複雑な分岐が無く、判断基準が明確である必要があります。

1) 実施作業例

下記にない作業の対応可否については弊社エンジニアへご相談下さい。

項目	内容
プロセス停止／起動	プロセスの停止と起動を行い、復旧を確認します。
サーバ再起動	サーバやインスタンスの再起動を行います。
ジョブ再実行	指定ジョブの再実行を行います。
ロードバランサー復旧	ロードバランサー下のインスタンスの切り離しと切り戻しを行います。

2) 障害一次対応標準フロー



5-7 障害二次対応

対応プラン： **P** **F**

障害一次対応実施後、復旧しなかった際にお客様と協議の上、作業を実施いたします。また、一次対応で復旧した場合の原因調査もご希望により対応します。

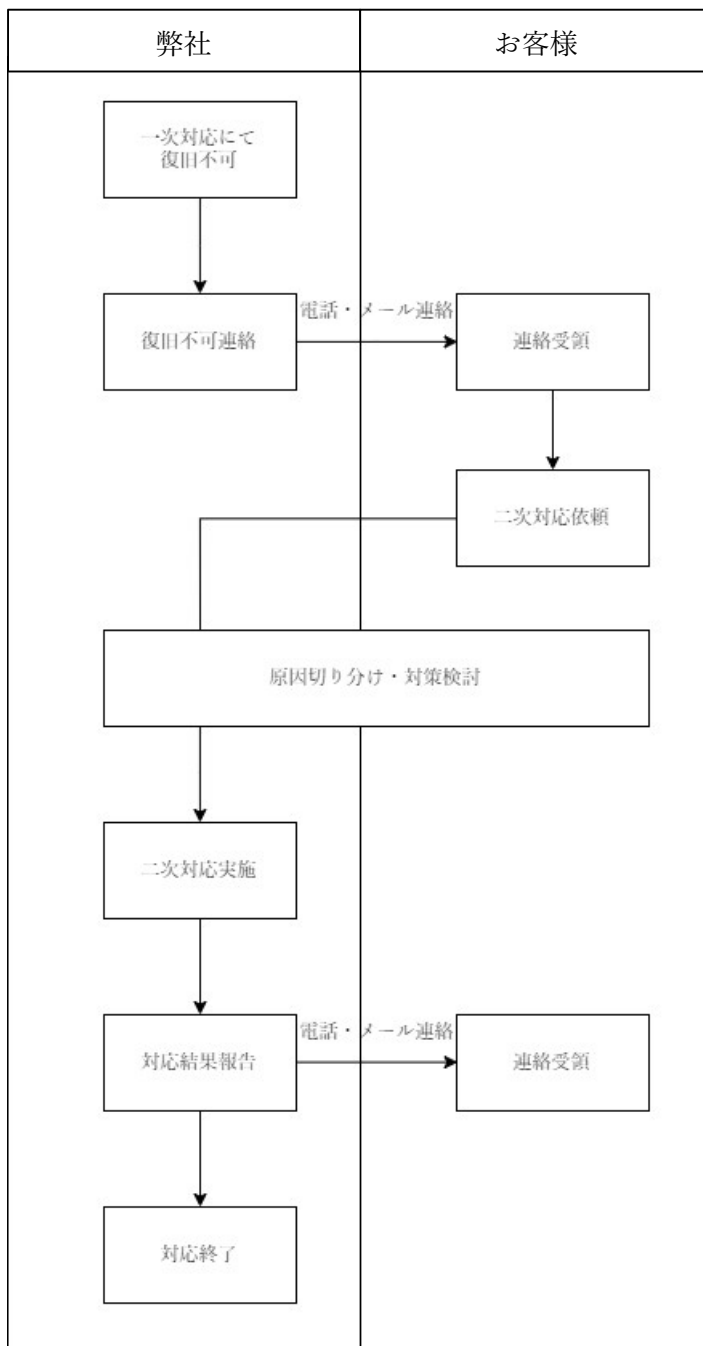
項目	内容
作業対象	マネジメント対象のみとなります。契約のない対象への作業は実施できません。
対応時間	相談・受付は 24 時間 365 日対応となります。作業は内容によって実施時間を調整させていただく場合があります。
実施可否	あらかじめ取り決めのない二次対応についてはお客様と協議の上、実施可否を判断いたします。
連絡手段	電話、メール、コミュニケーションツール(Backlog 等)

1) 実施作業例

下記にない作業の対応可否については弊社エンジニアへご相談下さい。

項目	内容
仮想マシンのリストア	スナップショットやマシンイメージから仮想マシンの復旧を行います。
IP 制限の実施	特定の IP アドレスからの接続が多く、接続元が海外であった場合、該当 IP アドレスをブロックするようにチューニングを行います。
ログによる障害原因調査	予期せぬ障害(ミドルウェアの起動失敗等)が発生した際に、ログから障害原因の調査を行います。 但し原因の解明をコミットするものではありません。
DB の長時間クエリの切断	DB の処理が重い場合にログ調査を行い、長時間実行されているクエリがあれば、該当クエリの切断を行います。
Apache のチューニング	ログを調査し、スレッド数の調整や接続の保持時間の調整を行います。
ミドルウェアの再起動	停止したミドルウェアの再起動を行います。
メーカーへのお問い合わせ代行	原因不明の障害が発生した際は、クラウドベンダや各メーカーへの問い合わせを代行します。

2) 障害二次対応標準フロー



5-8 定期作業

対応プラン： **F**

事前に取り決めた日時で定期的に作業を行います。

項目	説明
作業対象	マネジメント対象のみとなります。契約のない対象への作業は実施できません。
対応可能時間	24時間365日となります。作業は内容によって実施時間を調整させていただく場合があります。
1回の作業時間	着手から完了まで1回30分以内の作業が対応可能です。
作業内容	手順書の無い作業は実施できません。事前にお客様にて用意いただいた手順の受け入れが必要です。

5-9 依頼作業

対応プラン： **F**

ご依頼を契機に作業を行います。

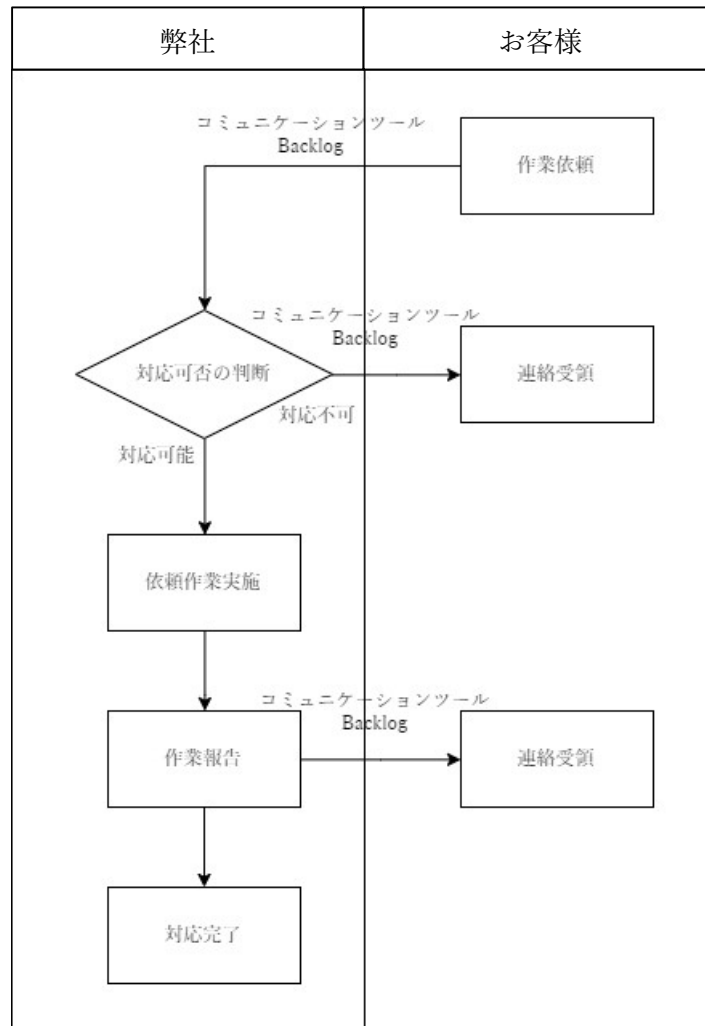
項目	説明
作業対象	マネジメント対象のみとなります。契約のない対象への作業は実施できません。
対応可能時間	平日 9:30~18:30 の時間帯になります。 上記時間帯以外は実施日の5営業日以上前にご相談ください。
1回の作業時間	着手から完了まで1回30分以内の作業が対応可能です。
作業内容	手順書の無い作業は実施できません。事前にお客様にて用意いただいた手順の受け入れが必要です。 内容によって作業後の最終確認はお客様に実施いただく場合があります。
依頼方法	コミュニケーションツール(Backlog等)でのご依頼ください。 電話やチャットツールでの依頼は受け付けておりません。
リードタイム	ご依頼から作業完了まで最大3営業日のリードタイムをいただきます。

1) 実施作業例

下記にない作業の対応可否については弊社エンジニアへご相談下さい。

作業	内容	分類
システム停止、起動	仮想マシン、サービスの停止・起動	依頼
アカウント作成、削除	OSに必要なアカウント作成・削除	依頼
アカウントパスワード変更	アカウントのパスワード更新	依頼
ミドルウェアの各種設定変更	Apache,PHP,MySQL など ※設定項目と値を明示的に指示して頂き設定変更	依頼
OS 設定変更	ホスト名、IP アドレスの変更 ※設定項目と値を明示的に指示して頂き設定変更	依頼
NTP 時刻同期設定変更	NTP/chronyd の時刻同期設定	依頼
SSL 証明書対応	CSR 作成、証明書設置	依頼
ログローテーション設定変更	Logrotate の間隔、世代数の変更	依頼
セキュリティパッチ適用	仮想マシン、ミドルウェアのセキュリティパッチ適用 ※アプリケーション動作確認は対象外 ※対応可能なミドルウェア ・yum/rmp/deb でインストール/アップデート可能なミドルウェア(Linux) ・WindowsUpdate の範囲内	定期/依頼
クラウドベンダへの問い合わせ	各クラウドベンダへの問い合わせ代行	依頼
スケールイン/アウト	クラウド上の仮想マシンに対して手動でスケールイン/アウト作業	依頼
インスタンスタイプの変更	インスタンスタイプの変更	依頼
PaaS のパラメータ変更	各クラウドでの各種 PaaS のパラメータ変更 ※設定項目と値を明示的に指示して頂き設定変更	依頼
DNS サーバ設定変更	レコード追加 ※設定項目と値を明示的に指示して頂き設定変更	依頼
バックアップ設定変更	バックアップ取得日時、世代数の設定	依頼
IAM 設定変更	IAM ユーザーの作成、権限設定	依頼

2) 依頼作業のフロー



5-10 静観依頼受付

対応プラン： B S P F

作業等であらかじめ、アラートの検知が見込めるものに対して静観設定を行うことでお客様へ通知、一次対応を実施いたしません。静観設定の受付は原則1営業日前までとなります。静観受付下記を利用していただく必要があります。

1) Web モニタ(※指定ツール利用に限る)

対象サーバから静観設定を選択し、静観期間を入力すると対象サーバで検知するアラート全てに対して静観とすることができます。

2) メール

メールにて静観の依頼を受け付け可能です。依頼先メールアドレスはご契約時に提供します。

下記メールフォーマットに沿ってご依頼ください。

【件名】

監視静観依頼

【本文】**【会社名・案件名】** お客様名やシステム名を記載**【対象サーバ名】** 対象のサーバ名を記載**【期間】** 静観の開始時間および終了時間を記載**【作業概要】** 作業内容を記載(可能であれば)

※ メンテナンス実施など

【対象警報】 静観対象警報(サービス監視、URL 応答監視等)を記載

※ サービス停止や再起動の場合は対象のサービス名を記載

※ サーバの停止や再起動の場合は「すべての警報」と記載

5-1 1 その他

1) 脆弱性情報アナウンス

対応プラン： B S P F

OS/ミドルウェアの脆弱性情報を提供します。

2) 監視モニタ/レポート

対応プラン： S P F

稼働状況などを月次報告書として提供します。

3) S3 バケットレポート

対応プラン： S P F

S3 サービスの監視をご利用のお客様に対して、ご要望に応じて S3 パケットの簡易レポートを提供します。詳細レポートをご希望の場合は有償)となります。

2023年8月1日 制定

2025年3月31日 改訂