サービス仕様

目次

1. 変更履歴

変更日	変更内容
2018/11/22	初版リリース
2019/05/01	価格改定

2. サービス概要

2.1. 監視サービス概要

- 本サービスは各種 AWS リソースを対象とした監視サービスです。
- 障害検知の方法として、数値データに対してはしきい値を、文字列データに対しては条件文を設定し、障害を検知できます
- 障害検知時のアラート通知としては、メール、チャット（※1）、電話を利用できます
- 障害などのイベントについては、WEB画面にて参照、管理ができます（※2）
- 取得した数値データについては、WEB画面にてグラフ形式で参照ができます（※2）

（※1）利用できるチャットサービスについては「3.3. アラート通知機能」を参照してください
（※2）WEB 画面の詳細については、Mackerelの仕様を参照してください

2.2. 対象とするお客様

- AWS を利用しており、各種 AWS サービスと AWS 上で稼働しているアプリケーションの監視を行いたい
- 独自の監視システムの構築や CloudWatch の細かな設定などのコストを省きたい
- アラート通知の方法を柔軟に選択したい（例：メールだけでなく電話やチャットも）
- 複数の AWS アカウントでの監視を統合して管理したい（※3）

（※3）詳細については、Mackerelの仕様を参照してください

2.3. サービス範囲

- サービス範囲については、「3. サービス仕様」記載の通りとします
- 監視システムの動作保証範囲としては、初期導入時の設定状態とします
- 障害検知後の原因調査や復旧対応はサービス範囲外となります

3. サービス仕様

3.1. 監視機能

本サービスで提供する監視機能は以下の通りです。

- 死活監視
- AWSサービス監視 (EC2、RDS、ELB、Redshift、CloudFront、Lambda)
- URL外形監視
- TCPポート監視
- アプリケーションログ・プロセス監視 (EC2 のみ)

注意

- 以下の項目の監視には、mackerel-agent（および同プラグイン）の導入が必要となります。
    - 「死活監視」-「connectivity」
    - 「AWSサービス監視」-「Filesystem Usage」
    - 「AWSサービス監視」-「Memory Utilization」
    - 「TCP接続監視」
    - 「アプリケーションログ・プロセス監視」
- Mackerel および mackerel-agent の設定は、各お客様で自由に変更が可能です。ただし、本仕様を超えたご利用をされた範囲のサポートはベストエフォートでのご提供とさせて頂きます。

3.2. 監視項目

各監視対象における監視項目を下表に記載します。

3.2.1. 死活監視

監視項目名	説明	mackerel-agent	監視しきい値（デフォルト値）	通知方法（デフォルト値）
connectivity	対象の mackerel-agent からデータが定期的に送信されてくることを確認します	必要	（※1）	メール + 電話

Status Check Failed（※2）	EC2インスタンスが正常に稼働していることを確認します	ー	> 0（異常時には1を示す）	メール + 電話

（※1） connectivity の監視しきい値は Mackerel の内部的に決定されており、変更はできません。詳細は下記ヘルプドキュメントをご参照ください。

- FAQ・Mackerelの死活監視はどのような仕組みで動いていますか？ - Mackerel ヘルプ

（※2）Status Check Failed による監視は、後述する EC2 サービス監視中の項目と同じものです

3.2.2. AWSサービス監視

3.2.2.1. Amazon EC2

EC2 の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- インスタンスの利用可能な CloudWatch メトリクスのリスト表示 - Amazon Elastic Compute Cloud
- AWSインテグレーション - EC2 - Mackerel ヘルプ

監視項目名	統計値	説明	mackerel-agent	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
CPU Utilization	平均	割り当てられた EC2 コンピュートユニットのうち、現在インスタンス上で使用されているものの比率 (※1)	ー	%	> 90	メール
Status Check Failed	最大値	インスタンスが過去 1分間にインスタンスのステータスチェックとシステムステータスチェックの両方に合格したかどうかを報告します	ー	0（合格） or 1（失敗）	> 0	メール + 電話
Filesystem Usage	計測値	EC2 インスタンスに取り付けられたファイルシステムの使用率 (※2)	必要	%	> 90	メール
Memory Utilization	計測値	EC2 インスタンスの物理メモリに対する使用率	必要	%	> 90	メール

（※1）複数のコアが搭載されているインスタンスの場合は、全 CPU コアの平均値となります。

（※2）複数のファイルシステムが存在する場合は最も高い使用率を取得します。

3.2.2.2. Amazon RDS

RDS の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- Amazon RDS のモニタリングの概要 - Amazon Relational Database Service

- [AWSインテグレーション - RDS - Mackerel ヘルプ]

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
CPU Utilization	平均	CPU 使用率	%	> 90	メール
Free Storage Space	平均	使用可能なストレージ領域の容量	Byte	< 500 MB	メール
Replica Lag	平均	ソース DB インスタンスからリードレプリカ DB インスタンスまでのラグ	秒	> 60	メール
Swap Usage	平均	DBインスタンスで使用するスワップ領域の量	Byte	> 100 MB	メール

対象の RDS が Aurora の場合は、下記も監視されます

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
Replica Lag	平均	Aurora レプリカについて、プライマリインスタンスからアップデートをレプリケートするときの遅延時間の量	ミリ秒	> 100	メール
Commit Latency	平均	コミットされたトランザクションのレイテンシー時間	ミリ秒	> 50	メール
DML Latency	平均	挿入、更新、削除のレイテンシー時間	ミリ秒	> 50	メール
Free Local Storage	平均	DB インスタンスが一時テーブルとログのために使用できるストレージの量	Byte	< 5G	メール

3.2.2.3. ELB (Elastic Load Balancing) - CLB

ELB(CLB) の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- Classic Load Balancer の CloudWatch メトリクス - Elastic Load Balancing
- AWSインテグレーション - ELB (CLB) - Mackerel ヘルプ

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
Healthy Host Count	平均	ロードバランサーに登録された、正常なインスタンスの数	台	< 1	メール + 電話
UnHealthy Host Count	平均	ロードバランサーに登録された、異常なインスタンスの数	台	> 0 メール	メール
HTTPCode Backend 5XX	合計	登録されたインスタンスによって生成された HTTP 応答コードの数。 ロードバランサーによって生成される応答コードは含まれません	回	> 0	メール
HTTPCode ELB 5XX	合計	リスナーが HTTP または HTTPS プロトコルを使用するよう設定されている場合、ロードバランサーによって生成される HTTP 5XX サーバーエラーコード数。 登録されたインスタンスによって生成される応答コードは含まれません	回	> 0	メール
Spillover Count	合計	キューがいっぱいなため、拒否されたリクエストの総数	回	> 0	メール
Surge Queue Length	最大	登録されたインスタンスへの送信が保留中のリクエストの合計数	ー	> 500	メール

3.2.2.4. ELB (Elastic Load Balancing) - ALB

ELB(ALB) の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- Application Load Balancer の CloudWatch メトリクス - Elastic Load Balancing
- AWSインテグレーション - ALB - Mackerel ヘルプ

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
HTTPCode Backend 5XX	合計	登録されたインスタンスによって生成された HTTP 5XX サーバーエラーコード数	回	> 10	メール
HTTPCode ELB 5XX	合計	リスナーが HTTP またはHTTPSプロトコルを使用するよう設定されている場合、ロードバランサーによって生成された HTTP 5XX サーバーエラーコード数	回	> 5	メール
Target Response Time	平均	リクエストがロードバランサーから送信され、ターゲットからの応答を受信するまでの経過時間	秒	> 5	メール
Rejected Connection Count	合計	ロードバランサーが接続の最大数に達したため、拒否された接続の数	回	> 10	メール
Client TLS Negotiation ErrorCount	合計	クライアントにより開始され、ロードバランサーとのセッションを確立しなかった、TLS 接続の数	回	> 10	メール
TargetGroup Healthy Host Count	平均	正常と見なされるターゲットの数	台	< 1	メール + 電話
TargetGroup Unhealthy Host Count	平均	異常と見なされるターゲットの数	台	> 0	メール
HTTPCode Target 5XX Count	合計	ターゲットによって生成された HTTP 5XX サーバーエラーコード数	回	> 10	メール
Target Connection Error Count	合計	ロードバランサーとターゲット間で正常に確立されなかった接続数	回	> 10	メール
Target TLS Negotiation ErrorCount	合計	ロードバランサーにより開始され、ターゲットとのセッションを確立しなかった、TLS 接続の数	回	> 10	メール

3.2.2.5. ELB (Elastic Load Balancing) - NLB

ELB(NLB) の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- Network Load Balancer の CloudWatch メトリクス - Elastic Load Balancing
- AWSインテグレーション - NLB - Mackerel ヘルプ

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
TCP ELB Reset Count	合計	ロードバランサーによって生成されたリセット (RST) パケットの数	回	> 10	メール
TargetGroup Healthy Host Count	平均	正常と見なされるターゲットの数	台	< 1	メール + 電話
TargetGroup Unhealthy Host Count	平均	異常と見なされるターゲットの数	台	> 0	メール

3.2.2.6. Amazon Redshift

Redshift の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- Amazon Redshift のパフォーマンスデータ - Amazon Redshift
- AWSインテグレーション - Redshift - Mackerel ヘルプ

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
Database Connections	平均	クラスターへのデータベース接続の数	—	> 24	メール
Health Status	最小	クラスターの状態を示します。クラスターは毎分データベースに接続し、簡単なクエリを実行します。この操作を正しく実行できる場合、クラスターは正常な状態であると見なされます。 ただし、メンテナンスタスクのためクラスターを利用できなかったとしても、クラスターでは正常な状態が維持されています	1 or 0	< 1	メール + 電話
Percentage Disk Space Used	最大	使用中のディスク容量の割合	%	> 80（コンピューティグノード）	メール

3.2.2.7. Amazon CloudFront

CloudFront の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- CloudWatch を使用した CloudFront アクティビティの監視 - Amazon CloudFront
- AWSインテグレーション - CloudFront - Mackerel ヘルプ
-

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
5xx Error Rate	平均	HTTP ステータスコードが 5xx であるすべてのリクエストの割合	%	> 1	メール

3.2.2.8. AWS Lambda

AWS Lambda の CloudWatch 各種メトリックスの詳細については以下を参照してください。

- AWS Lambda のメトリクス - AWS Lambda
- AWSインテグレーション - Lambda - Mackerel ヘルプ

監視項目名	統計値	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
Error Count	合計	関数 (応答コード 4XX) エラーが原因で失敗した呼び出しの回数	回	> 1	メール
Throttle Count	合計	同時実行数制限を超えた Lambda 関数の呼び出し試行の回数	回	> 1	メール

3.2.3. URL外形監視

監視項目名	説明	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
External Http Monitor	対象の URL へ HTTP 接続を 60 秒間隔で試み、異常 (※1)と判断された回数	回	2	メール + 電話

(※1) 本監視では、下記の条件に合致した場合を「異常」と判断します。

- HTTP レスポンスのステータスコードが 4xx または 5xx の場合（404、503 等）
- 15秒以内に応答が無かった場合（タイムアウト）
- SSL 証明書が不正だった場合（期限切れなど）

その他、Mackerel のもつ監視機能のオプションを活用可能です。詳細は下記ドキュメントを参照ください。

- URL外形監視をおこなう - Mackerel ヘルプ

3.2.4. TCP接続監視

check-tcp プラグインを利用した監視となります。

監視項目名 (※1)	説明	mackerel-agent	単位	監視しきい値（デフォルト値）	通知方法（デフォルト値）
TCP Connections Monitor	対象のポートへ TCP 接続を試み、時間内に接続が確立できることを確認します	必要 (※2)	秒	10（タイムアウト値）	メール + 電話

（※1）監視項目名は対象ホスト内で一意である必要があります。特に指定が無い場合は下記のように設定いたします。

- tcp_<監視対象ホスト名 or IPアドレス>_<ポート番号>
- ex) tcp_localhost_25

（※2） 監視対象の EC2 上で動作する mackerel-agent に check-tcp プラグインを設定して監視を行います。

- 設定項目
    - 監視対象のホスト名 or IP アドレス（localhost、x.x.x.x 等）
    - 監視対象 TCP ポート番号（ 80 等）
    - その他詳細は下記ドキュメント、あるいは「check-tcp -h」の実行結果をご参照ください
        - go-check-plugins/check-tcp at master · mackerelio/go-check-plugins

3.2.5. アプリケーションログ監視

3.2.5.1 Linuxの場合 / 監視対象のログがテキストファイルである場合

check-logプラグインを利用した監視となります。

監視項目名 (※1)	説明	mackerel-agent	監視しきい値（デフォルト値）	通知方法（デフォルト値）
Application Logs Monitor	対象のログファイルをウォッチし、指定の文字列をフィルタします	必要(※2)	指定の文字列を検出した場合	メール

（※1）監視項目名は対象ホスト内で一意である必要があります。特に指定が無い場合は下記のように設定いたします。

- log_〈監視対象ファイル名〉_〈キーワード等、重複回避かつ識別可能なもの〉
- ex) log_var_log_messages_ERROR

（※2） 監視対象の EC2 上で動作する mackerel-agent に check-log プラグインを設定して監視を行います。

- 設定項目
    - 監視対象のログファイル名（ /var/log/messages 等）
    - 監視する正規表現（「ERROR|FATAL」など）
    - 大文字・小文字の区別
    - 文字列エンコード（UTF-8、Shift_JIS など）
    - その他詳細は下記ドキュメント、あるいは「check-log -h」の実行結果をご参照ください
        - go-check-plugins/check-log at master · mackerelio/go-check-plugins

3.2.5.2 Windowsの場合 / 監視対象がイベントログである場合

check-windows-eventlog プラグインを利用した監視となります。

監視項目名 (※1)	説明	mackerel-agent	監視しきい値（デフォルト値）	通知方法（デフォルト値）
Application Logs Monitor	EventLogをウォッチし、指定の文字列をフィルタします	必要(※2)	指定の文字列を検出した場合	メール / メール + 電話 (※3)

（※1）監視項目名は対象ホスト内で一意である必要があります。特に指定が無い場合は下記のように設定いたします。

- eventlog_〈キーワード等、重複回避かつ識別可能なもの〉

- ex）eventlog_failed

（※2） 監視対象の EC2 上で動作する mackerel-agent に check-windows-eventlog プラグインを設定して監視を行います。

- 設定項目
    - 監視する文字列（「failed」など）
    - その他詳細は下記ドキュメント、あるいは「check-windows-eventlog.exe /?」の実行結果をご参照ください
        - go-check-plugins/check-log at master · mackerelio/go-check-plugins
- サンプル設定
    - 下記内容を mackerel-agent.conf に追記してください
    - [plugin.checks.eventlog_failed]
    - command = "check-windows-eventlog.exe /message-pattern:failed /r"

（※3）出力されたイベントログのレベルに依存します（エラーレベル = メール + 電話、警告レベル = メールのみ）。

3.2.6 プロセス監視

check-proc プラグインを利用した監視となります。

た監視となります。

監視項目名 (※4)	説明	mackerel-agent	監視しきい値（デフォルト値）	通知方法（デフォルト値）
Application Process Monitor	対象のプロセスが稼働していることを確認します	必要(※5)	対象のプロセスがダウンしていた場合	メール

（※4）監視項目名は対象ホスト内で一意である必要があります。特に指定が無い場合は下記のように設定いたします。

- process_〈監視対象プロセス名 + キーワード等、重複回避かつ識別可能なもの〉
- ex）process_postfix

（※5） 監視対象の EC2 上で動作する mackerel-agent に check-procs プラグインを設定して監視を行います。

- 設定項目
    - 監視対象のプロセス名（ postfix 等）

    - その他詳細は下記ドキュメント、あるいは「check-procs -h」「check-procs /?」の実行結果をご参照ください
        - go-check-plugins/check-procs at master · mackerelio/go-check-plugins

- サンプル設定
    - 下記内容を mackerel-agent.conf に追記してください
    - **Linuxの場合**
    - [plugin.checks.process_postfix]

      command = "check-procs -p postfix -C 0"
    - **Windowsの場合**
    - [plugin.checks.process_AmazonSSMAgent]

      command = "check-procs.exe /p amazon-ssm-agent /C 0

3.3. アラート通知機能

閾値超過時のアラート通知の手段は電話通知、メール通知、チャット通知、と3つ存在します。またアラート通知対象がEC2の場合は、EC2インスタンスの再起動指示を行う（停止、起動を順次行う）というアクションを行うことができます。

本サービスで提供するアラート通知機能は下表の通りです。

通知方法	障害発生時の挙動
メール	● 事前に指定したメールアドレスに対し、メールを送信します ● 複数のメールアドレスを指定することも可能です
電話	● 事前に指定した電話番号に対し、電話を発信します ● 複数の電話番号を指定することが可能です（最大10件まで） ● 設定された順番に従って、電話が繋がるまで発信します ● 電話が繋がった場合、その番号以降に指定されている電話番号には発信されません また、誰も出なかった場合でも再電話はされません ● 通知対象がEC2の場合、ダイアルパッド操作により再起動を指示することが可能です
チャット	● 事前に指定したチャットサービスにメッセージを送信します ● 対応しているチャットサービスは以下になります（'18/10時点 : Mackerelのサービスによる） ○ Slack ○ Chatwork ○ HipChat ○ TypeTalk ○ Yammer ○ LINE

4. サービス提供条件

4.1. AWS環境要件

- **AWS アカウントのメンバーズ契約が必要** です
- 対象の AWS アカウントに監視サービス提供に必要なIAM Roleの作成が必要です
- インターネットとの接続がないプライベートネットワークに配置されたサーバーでは、一部の監視機能がご利用頂けません
- 監視対象サーバーの環境要件はこちらを参照してください

4.2. 利用準備

- Mackerel のコンソールにログインするためのアカウントが必要となります。新規に作成する場合は、アカウント用のメールアドレスをご用意ください。
- 障害検知時のアラート通知用にメールアドレスが最低1つ必要になります（メーリングリスト推奨）
- 電話通知を行う場合は通知先の電話番号が最低1つ必要になります
- チャット通知を行う場合はお客様にて対応するチャットサービスのご準備をお願いします
- クライアント端末の環境要件はこちらを参照してください

4.3. サービス提供時間

サービス項目	対応時間	備考
サービスお申込み受付	営業日9:00～18:00	ー
監視初期導入	営業日9:00～18:00	作業スケジュールについては調整が必要になります
監視サービス	24時間×365日	ー
本サービスに関するお問い合わせ	営業日9:00～18:00	ー
障害（アラート通知事象）に関するお問い合わせ	24時間×365日	メンバーズのサポート窓口に準じます

4.4. サービス停止時間

本サービスには下記のサービス停止時間が存在します。

4.4.1. メンテナンスによるサービス一時停止

監視システムのメンテナンス時（AWS インフラ環境を含む監視設備やサービスプログラムのメンテナンスなど）に一時的にサービスを停止します。

メンテナンス実施の際は、事前にメール等にてご連絡いたします。

4.4.2. 障害発生によるサービス一時停止

AWS や Mackerel にて障害発生等の予期せぬ理由にて、サービスを提供できなくなる場合があります。

その場合におけるサービス状況につきましては、メール等にてご連絡いたします。

5. サービス費用

5.1. 初期費用

導入に際し、監視対象1台（ホスト）あたり 10,000円の初期費用が発生いたします。

5.2. 月額費用

監視対象のホスト数に準じて費用が発生します。

監視機能	費用	備考
死活監視	0円	EC2に含まれる
AWSサービス監視（EC2）	5,000円／スタンダードホスト (200メトリクス)	※1
AWSサービス監視（RDS、ELB、Redshift、CloudFront、Lambda）	2,000円／マイクロホスト (30メトリクス)	※1
TCP接続監視	0円	EC2に含まれる
アプリケーションログ・プロセス監視	0円	EC2に含まれる
URL外形監視	5,000円／20個	※1 ※2

監視対象のホスト（スタンダードホスト、マイクロホスト）数の計算方法については以下を参照してください。

- FAQ・ホスト数の計算方法について - Mackerel ヘルプ
- FAQ・プラン上限超過時のホスト台数換算について - Mackerel ヘルプ

※1 URL外形監視やメトリクスについては、一定数を超えると追加ホストとしてカウントされますのでご注意ください

※2 スタンダードホストの利用が 1 ホスト以上あった場合は、最初の20URLまでは追加料金なしでご利用可能です

5.3 電話通知回数超過料金

1ヶ月の電話通知回数が一定回数を超過した場合、超過分の電話通話料が発生します。

項目	費用	備考
電話通知（通話料）	100円／回	**1ヶ月あたり50回まで電話通知費用は発生しませんが、51回目以降の電話通知については1回あたり左記の費用が発生します。** ※電話のコールに出なかった場合（出られなかった場合も同じ）は、電話通知回数に含めません。受電が成功した場合のみ電話通知の回数として数えます。 ※電話通知回数は、対象監視サーバーが所属しているAWSアカウント毎に数えます。 ⇒あるお客様がAWSアカウントX、AWSアカウントYを保有しており、それぞれのアカウントのサーバー起因の事象により40回、30回の電話通知があった場合、アカウント毎に数えると50回以下なので電話通知費用は発生しません。

6. その他

6.1. セキュリティ対策

6.1.1. 情報セキュリティ

お客様から提供いただいた各種情報は、ISMSの情報資産管理規定に則り、適切に管理いたします。

6.1.2. 監視システムのセキュリティ

- CloudWatch エンドポイントへアクセスするための権限は IAM Role で管理しています。また、サーバーの起動・停止・再起動の権限についても同様です（サーバー削除の権限は有しておりません）
- 監視システムの監視サーバーと CloudWatch エンドポイント間の通信は HTTPS で暗号化されています。また、ブラウザによる監視サービスWEB画面（ダッシュボード）への通信についても HTTPS で暗号化されています
- 監視システムへのログインアカウントは、弊社内での徹底した管理と運用を実施しております