Engineer

ログ記録

起きたことを、その都度書き残すこと

どのようなものか

ログ記録は、イベントログ記録とも呼ばれ、プログラムが自らの動作を継続的に記録することです。処理したリクエスト、拒否したパスワード、再試行、異常終了など、一つのイベントに一つの記録を残します。ログ行、またはログレコードという各記録は、少なくとも時刻とメッセージを持ち、後から何がどの順に起きたかを再構成できます。OpenTelemetryプロジェクトは、ログを、任意のメタデータを伴う、構造化または非構造化の時刻付きテキストレコードと定義し、テレメトリーの信号の中で、最も大きな既存の蓄積があると述べます。

その蓄積には標準があります。イベントメッセージを収集先に送る古くからのプロトコルsyslogは、2009年3月のRFC 5424で標準化され、以前のRFC 3164を置き換えました。各メッセージに、0のEmergencyから7のDebugまで、八段階の重大度を付けます。大半のログライブラリーは、同じ考えを短くしたdebug、info、warning、errorを持ちます。OpenTelemetryのログデータモデルは、それらをすべて、TRACEからFATALまで六つの帯に分けた1から24の数値に対応させます。

非構造化の行は、自由な文章です。人には読みやすい一方、機械が分解するには、その文言専用の正規表現が必要です。構造化したログ行は、決まった構造に従い、すべての記録が、同じ名前、型、意味のフィールドを持ちます。OpenTelemetryは、本番では構造化ログを推奨し、見落としやすい注意も加えます。JSONとして解析できるだけでは、構造化されたことにはなりません。構造化を成り立たせるのは、安定した構造です。ここでは複数行で示しますが、ディスク上では一行です。

```
{
    "time": "2026-09-14T03:12:07.412Z",
    "severity": "WARN",
    "service": "checkout",
    "event": "payment.retry",
```

```
    "attempt": 3,
    "trace_id": "4bf92f3577b34da6a3ce929d0e0e4736"
}
```

一緒に集めることが多い信号が、メトリクスとトレースです。メトリクスは、時間を追って採取する数値で、保存費用が小さく、頻度を表すのに向きます。トレースは、一つのリクエストが通るすべてのサービスを追います。ログは、個々のイベントの詳細を残すため、アラートの後に原因を調べるときに読みます。OpenTelemetryは、実行中のトレースとスパンのIDを各ログレコードに付け、ログとトレースを結び付けます。

概念を判断に生かす

「ログ記録とは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 障害が小さいうちに知らせる監視とアラートを整え、安定した状態をどれだけ維持できているかを数値で示します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 社内初のオブザーバビリティダッシュボードを構築 — 社内システムの状態を初めて可視化

社内初のオブザーバビリティダッシュボードを構築 お問い合わせ →

なぜ重要なのか

大半のシステムでは、ログが過去について残す唯一の記録です。メトリクスは、03:12にエラーが増えたと示せます。ログは、どのリクエストが、どのサービスから、どの値を伴って届き、プログラムが次に何をしたかを示します。夜中に壊れ、朝には回復していた場合も、ログという証拠は残ります。

記録には、三種類の負担が伴います。各行は、ディスク、入出力、プロセッサー時間を使います。中央の保存先に送れば、さらに費用がかかり、ホスト型サービスは、通常、取り込んだ量で請求します。各行は、誰かについて保有するデータでもあります。Webサーバーのアクセスログには、アクセスした全員のアドレスとブラウザーが残ります。そして各行を守る必要があります。OWASPのLogging Cheat Sheetは、各イベントについて「いつ、どこで、誰が、何を」を記録し、ログ自体を改ざん、不正なアクセス、変更、削除から保護するよう求めます。個人情報など、機密性のある情報を含む可能性があるからです。

組織規模では、Karen KentとMurugiah Souppayaによる、2006年9月刊行のNIST特別刊行物800-92、Guide to Computer Security Log Managementが、ログ管理を、一つのプログラムの設定ではなく、全社で運用する基盤と手順として扱います。

ログも、数値と一緒に使うと力を発揮します。Prometheusプロジェクトの計装ガイドは、ログを出すコードの各行にカウンターを設け、注目するメッセージが現れたとき、どれほどの期間に何回起きたかが分かるようにすることを勧めます。info、warning、errorの行数を、リリース間で比べることも勧めます。

実際の活用例

このサイト自身のアクセスログは、プライバシーのページで、一行ずつ説明しています。各リクエストは、ページと時刻、応答の状態、ブラウザーが自称する情報、参照元サイト名、一部をぼかしたネットワークアドレスを記録します。アドレスの末尾は、行を書く時点で、ディスクに届く前にゼロに置き換えます。一行の寿命は約三十日です。サーバーソフトウェアは、一日一回、または約10 MBに達した時点で先にファイルを閉じ、閉じてから二十八日後に削除します。毎晩の検査は、すべてのファイルを読み返し、三十日より古い行があれば不合格にします。問題は二度あり、両方をページに記録しています。2026年9月には、通信が少ないアドレスのファイルが10 MBに達するのが遅すぎ、一度も閉じられず、記録開始以来の全行が残っていたため、毎日閉じるジョブを追加しました。2026年10月26日には、ログを残す十三のアドレスのうち七つが、そのジョブが閉じたと扱うファイルに書き続け、一つは四十七日前の、既に閉じたファイルを保持していました。そのジョブは廃止し、今はサーバーソフトウェア自身がファイルを閉じ、削除します。

macOSアプリケーションの全テスト実行で、コアのログが610,996行記録されました。大量に発生したコアのログイベントを、上限のない主ストリームに保持し、そのイベントを使わない消費側の購読ストリームにもコピーしていました。インシデント記録は、36 GBのマシンで圧縮ページが111 GBになった診断報告と、接続の再試行ループ中にメモリー使用量が毎秒約41 MB増えた別の採取結果を記載します。上限付きのバッファー、イベント種別で絞る購読、ログ頻度の予算で、そのイベント経路に対処しました。記録にある全テスト実行の比較では、コアのログは1,411行に減りました。本番のベンチマークでも、修正後に測ったメモリー使用量でもありません。予算は、意図的に情報を捨てます。診断イベントの繰り返しを落とし、無制限に保持する代わりに、影響を受けた状態を取り直す場合があります。終了時に別途起きたタイムアウトには、別の修正が必要でした。

本番ホストでsystemdの十三ユニットを堅牢化した際には、三つのユニットテンプレートで、それらの構成管理ロールが存在した当初から、一つのディレクティブの綴りが間違っていたと分かりました。サービスマネージャーは、知らないキーを受け取ると、その事実をログに書き、それでもユニットを起動します。した

がって、唯一の手掛かりはログの警告で、ユニットを書き直す途中で発覚しました。今は、設定を収束させるたびに、すべてのユニットをサービスマネージャー自身の検証器にかけ、同じ誤記で実行を失敗させます。

問題が起きるところ

システムが壊れかけたときほど、ログが急増します。 再試行を毎回書くループは、普段は数行でも、悪い日には毎秒何千行も書き、余裕のないシステムから、ディスク、メモリー、プロセッサー時間を奪います。OWASPは、ディスクを埋めるなど、ログ記録を資源枯渇の手段にできないか確認するよう求めます。頻繁に通る各経路に予算を設け、同じメッセージは回数付きの一行にまとめ、横にカウンターを置きます。行を落としても、発生頻度は残ります。

秘密と個人情報を書いてしまいます。 リクエストを丸ごと記録すれば、その中身もすべて残ります。OWASPが、通常はログに入る前に除去、マスク、ハッシュ化、暗号化すべきものとして挙げるのは、セッションID、アクセストークン、パスワード、データベース接続文字列、暗号鍵、決済カード情報です。前述のアクセスログがアドレスに対して行うように、書く時点で処理します。誰かが掃除するころには、バックアップやアーカイブにも行が入っている可能性があります。

外部の入力が、偽の行を書き込みます。 利用者が渡した値に、復帰文字や改行が含まれ、それをエスケープせずテキストログに書くと、アプリケーション自身が書いたのと見分けのつかない新しい行を始められます。OWASPは、これをログインジェクションと呼び、そのような文字を無害化し、書き込む形式に合わせてデータを符号化するよう求めます。各値を、エスケープしたJSON文字列として出す構造化ロガーなら、仕組み自体で実現します。

ログが静かになっただけなのに、正常と判断します。 ディスク満杯、ローテーション後に開き直さなかったファイル、停止した収集器は、外からは同じに見えます。行が届かなくなります。OWASPは、ログ記録が止まったことを検出する方法を求めます。発生元ごとに毎分の行数を数え、ゼロになったら通知します。そうすれば、ログの空白自体がアラートになります。

参考資料

- ログ — OpenTelemetryによるログの定義、構造化を推奨する理由、トレースとの関係です。
- ログデータモデル — ログレコードのフィールド、二つの時刻、1から24の重大度です。

- RFC 5424：Syslogプロトコル — syslogメッセージの形式と八段階の重大度です。
- NIST SP 800-92 — コンピューターセキュリティーのログ管理ガイドです。
- Logging Cheat Sheet — 記録するイベント、除外するデータ、結果の保護についてのOWASPの指針です。
- 計装 — ログを含む、コードの計装についてのPrometheusの実践です。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「ログ記録とは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く 連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/logging/