

# FALCON LOGSCALE

あらゆるログデータと、リアルタイムのインサイトを、すべて1か所に。

## 課題：

拡張性のないロギングプラットフォームほど高価なものはない

IT インフラストラクチャが毎秒毎秒ビジネスのあらゆる側面で実行される際、システムの健全性、パフォーマンス、セキュリティに関連するデータも同時に作成されています。ログデータとして知られるこの情報は、インフラストラクチャがどのように機能しているか、そしてそれらの資産がどの程度安全であるかを理解しようとする SecOps、ITOps、DevOps チームにとって不可欠です。

しかし、ログデータを取得しようとする、必然的に規模とコストの問題に直面します。従来のログ管理プラットフォームでは、すべてをログに記録しようとする、法外なコストがかかります。さらに、これらのプラットフォームはインデックススペースであるため、データ量が増加するとインデックスのサイズが大きくなって検索クエリが滞ることになり、侵害が発生した場合に攻撃者を追跡したり、停止の原因を発見したりするのが困難になります。

最小限の予算とリソースで業務を行う DevOps、SecOps、ITOps の担当者は、どのログをどのくらいの期間収集するかという点で妥協を余儀なくされています。その結果、必然的に収集されないログが発生し、デジタル資産の健全性とセキュリティポスチャに盲点が生じることとなります。その代償は何でしょうか？それは、調査の遅れと攻撃リスクの増大です。

## ソリューション：

リアルタイムのスピードとスケールですべてを記録

CrowdStrike Falcon LogScale は、組織が IT 環境のパフォーマンス、セキュリティ、レジリエンスについてデータに基づいた意思決定を行えるようにする、一元化されたログ管理プラットフォームです。世界で最もスケーラブルなログ管理プラットフォームである Falcon LogScale は、重要なログ情報をすばやく簡単に探索し、死角をなくしてインシデントの根本原因を見つけることで、すべてのログおよびイベントデータのオプザーバビリティを向上させます。Falcon LogScale は、IT 組織に、すべてのログおよびイベントデータをペタバイト規模で保存、分析、保持できる単一のプラットフォームを提供し、ログデータの取り込み、検索、変換、保持に必要なコンピューティングおよびストレージリソースを最小限に抑えます。その結果、従来のプラットフォームよりも低い総所有コストで、今日の複雑な IT インフラストラクチャに必要なパワーとスピードを提供します。

## 主な利点

### 現代の企業のために構築

分散システム全体に完全なオプザーバビリティを提供し、どのログを取り込み保持するかというコスト面での譲歩が不要

1日あたり1+PBのライブクエリのベンチマークを持つ、あらゆる規模でのストリーミングデータの取り込み

データバーストと超高速検索を可能にするインデックスフリーアーキテクチャ

業界最高水準のデータ圧縮率とクラウドストレージオプションにより、ログ管理プロセスにおいてより多くのデータを取り込み、管理することが可能

あらゆる構成に対応する柔軟でスケーラブルな展開：オンプレミス、クラウド、ハイブリッド

# 主な機能

## ペタバイト規模での最新のログ管理

- **すべてをログに記録** : Falcon LogScale を使用することで、さまざまなソースからの大量のストリーミングログデータをペタバイト規模で保存、分析、保持できます。
- **最新のアーキテクチャ** : 独自のインデックスフリーアーキテクチャと、ハードウェア要件を最小限に抑えるために設計された高度な圧縮技術により、ついにすべてのログをオブザーバビリティプログラムに取り込むことが可能となりました。
- **長期間のデータ保存** : Falcon LogScale は1年以上にわたりデータを保持するため、ユーザーは脅威ハンティングとトラブルシューティングのために、前例のない速度と規模でより完全な履歴データとリアルタイムデータにアクセスできます。

## 瞬時に検索結果を取得

- **すべてのデータを検索** : Falcon LogScale は、リアルタイムのストリーミングとインデックスフリー検索を提供し、DevOps、ITOps、SecOps チームが最も複雑なクエリに対しても瞬時に回答を受け取ることが可能です。
- **継続的な改善を推進** : 1秒以下で検索結果を取得できるため、より迅速なインシデントからの復旧や問題の根本的な原因の把握が可能となります。
- **単一のインターフェース** : 分散したデータを一箇所でシームレスに収集、分析、検索できるため、環境に関する単一の包括的なビューを得ることができます。

## 総所有コストを削減

- **高度な圧縮技術** : Falcon LogScale はデータを6～80倍に圧縮し、インデックススペースのロギングプラットフォームで見られる高額なストレージコストを大幅に削減します。
- **全体的なコストの削減** : Falcon LogScale は、従来のログ管理プラットフォームよりもはるかに低いTCOを提供し、組織がすべてのログデータを取り込み、保持、検索する費用効果の高い方法を提供します。
- **高い費用対効果** : 2022年のForrester Consulting Total Economic Impact™ 調査によると、Falcon LogScale は3年後のROIが210%であると報告されています。

## クラウドストライクについて

CrowdStrike(Nasdaq: CRWD)、は、サイバーセキュリティのグローバルリーダーであり、エンドポイント、クラウドワークロード、アイデンティティ、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームにより、現代のセキュリティを再定義しています。

CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud およびワールドクラスの AI を搭載し、リアルタイムの攻撃指標、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリを活用して、超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けられた脆弱性のオブザーバビリティを提供します。

Falcon プラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンス、複雑さの低減、迅速な「Time to Value」を実現します。

CrowdStrike: **We stop breaches**

詳細はこちら :

<https://www.crowdstrike.jp/>

ソーシャルメディア : [ブログ](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2023 CrowdStrike, Inc.  
無断複製禁止。

