

解析は、 未来への布石。

統合ログ管理プラットフォーム



問題解決、意思決定、すべての行動にデータを活用するための
総合ログ管理プラットフォーム

このようなお悩みはありませんか？

【課題】

大量のログやデータを
検索可能な状態で保存したい。

リアルタイムにログやデータを
解析(確認)したい。

大量のログやデータから表やグラフを
簡単に作成し、関係者で共有したい。

【解決】

Splunkは1日あたり数TBにおよぶ
ログやデータでも、効率よく
読み込み・解析・保存できます。

Splunkはログやデータを監視し、
解析した結果を
リアルタイムでアラート通知することができます。

Splunkはログやデータの検索結果を
柔軟に集計し、ダッシュボード機能ですばやく
関係者と共有できます。

「Splunk」は、サーバー・ネットワーク機器・業務システム・センサーなど、さまざまなマシンからログ・データを収集し、リアルタイムな検索・分析・可視化を行える統合ログ管理プラットフォームを提供します。セキュリティインシデントの検出をはじめとしたIT運用の効率化・向上だけでなく、将来に向けたビジネスの分析など、さまざまな分野で活用できます。

Splunk <3つのポイント>

POINT 01

SECURITY
セキュリティ

ネットワーク機器などのログを一元管理、分析し、セキュリティインシデントを検出

POINT 02

IT OPERATION
IT運用

局所的な問題からシステム全体の影響を早期発見し、被害の最小化に貢献。

POINT 03

BUSINESS ANALYSIS
ビジネス・アナリティクス

高度で柔軟な検索・集計機能により、ログやデータをビジネスのヒントに。

活用事例 **POINT 02**
IT OPERATION
IT運用

膨大なログやデータの解析を通じてITシステム全体に与える影響を早期発見し、運用の高度化を支援します。

課題

- エンジニアによるシステム管理工数を削減したい
- 予兆検知できず障害発生後の対応に追われている
- システム全体を俯瞰して状況を把握できるようにしたい

効果

- ログ情報の自動収集と一元管理により調査効率を向上
- 複数のログ情報を横断的に分析し、障害を予測
- サービス視点でIT環境の状態を可視化し、障害発生時に影響範囲と重大性を特定

お客様システム
サーバー OS
ネットワーク
APP
アプリケーション

ログを収集

分析
・ログの相関分析
・リアルタイム解析

splunk>

運用ログ
・イベント

アラート通知

運用担当者

ダッシュボード参照

重要
・障害検知ルール
・サービスレベル低下検知ルール

早期対策
・状況の把握、判断

活用事例 **POINT 01**
SECURITY
セキュリティ情報イベント管理

さまざまなシステムログを一元的に収集・分析・可視化することで、脅威の早期発見と被害の最小化に貢献します。

課題

- インシデント発生時の調査と分析に時間と工数が掛かる
- 機器やシステムごとに管理や調査方法が異なり限界を感じている

効果

- さまざまな機器やシステムの情報を一元管理し調査を効率化
- 誤検知を削減し、対応すべきインシデントにリソースを集中
- 複数ログを横断して分析し、ダッシュボード上に可視化

お客様システム
業務システム
端末
セキュリティシステム

ログを収集

分析
・ログの相関分析
・リアルタイム解析

splunk>

セキュリティログ
・イベント

アラート通知

運用担当者

ダッシュボード参照

重要
・内部不正検知ルール
・サイバー攻撃検知ルール

早期対策
・状況の把握、判断

活用事例 **POINT 03**
BUSINESS ANALYTICS
ビジネス・アナリティクス

人事情報・勤怠管理・経費などのログを分析し、働き方に関連する情報をダッシュボード化。働き方改革の指標として活用できます。

課題

- リモートの従業員は問題なくシステムを利用できているか
- 各従業員の働き過ぎやパフォーマンスの管理の必要性

効果

- VPNや認証システムの情報から従業員の業務状況を把握
- 勤怠情報やアクセス情報などを一元管理して問題を把握

【リモートワークでの分析の例】

従業員システム
端末
ネットワーク
APP
アプリケーション

ログを収集

分析
・ログの相関分析
・リアルタイム解析

splunk>

人やアプリケーションの稼働情報・ログ・イベント

ダッシュボード参照

人事担当者

早期対策
・状況の把握、判断

日立ソリューションズだからできること

SOLUTION 01

関連商品との組み合わせで利用用途が多彩。

日立ソリューションズの関連商品との組み合わせによって、Splunkの役割をさらに広げることができます。解析精度の向上や業務効率化など、最適なソリューションを提供します。

SOLUTION 02

豊富な実績とノウハウを活用し、お客様の課題を解決。

長年にわたって蓄積してきたシステム開発・構築の経験があり、お客様の課題に合わせて柔軟な提案が可能です。Splunkをハブとし、さまざまなシステム間の情報連携を実現していきます。

SOLUTION 03

日立グループの力を結集した“One Hitachi”のSI力。

要件定義から運用まで、プロジェクトをワンストップで支援。自社の運用管理コンサル担当との連携のほか、グループ各社の知見を活用した“One Hitachi”体制で幅広く対応します。

まずは、ダウンロードしてすぐに使える評価版をお試しください！

評価版ダウンロード > <http://www.hitachi-solutions.co.jp/splunk/>

紹介動画サイト > <http://www.hitachi-solutions.co.jp/splunk/#movie>



最新の情報【Splunk社サイト】

<http://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements>

提供製品

- オンプレミスライセンス「Splunk Enterprise」と、サービス「Splunk Cloud」を選択可能
- よりSplunkを活用できる、各種プレミアムソリューションも提供
- オブザーバビリティソリューション「Splunk Observability」を提供

| | | |
|----------------------|---|-----------------|
| Splunk コア製品 | splunk > enterprise | splunk > cloud™ |
| プレミアム ソリューション | ■ セキュリティ: Splunk Enterprise Security、Splunk User Behavior Analytics、Splunk SOAR ■ IT運用/オブザーバビリティ: Splunk IT Service Intelligence | |
| オブザーバビリティ ソリューション | Splunk Observability | |

※Splunkは、Splunk Inc.の米国およびその他の国における商標または登録商標です。※その他、本カタログ中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記していません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。※本カタログ中の情報は、カタログ作成時点のものです。

◎ 株式会社 日立ソリューションズ

www.hitachi-solutions.co.jp



本カタログ掲載商品・サービスの詳細情報

www.hitachi-solutions.co.jp/splunk/

S13S-36-03

2023.02