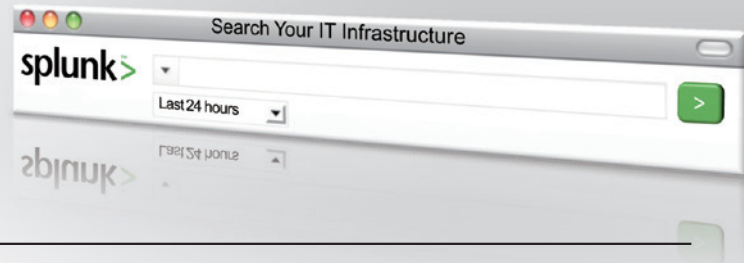




The IT Search Engine.



膨大なITデータを取り扱うシステム管理者の運用効率を飛躍的に向上!

ITインフラのための高速“ITサーチエンジン”

検索エンジンなしでインターネットを使う、なんて想像できますか?

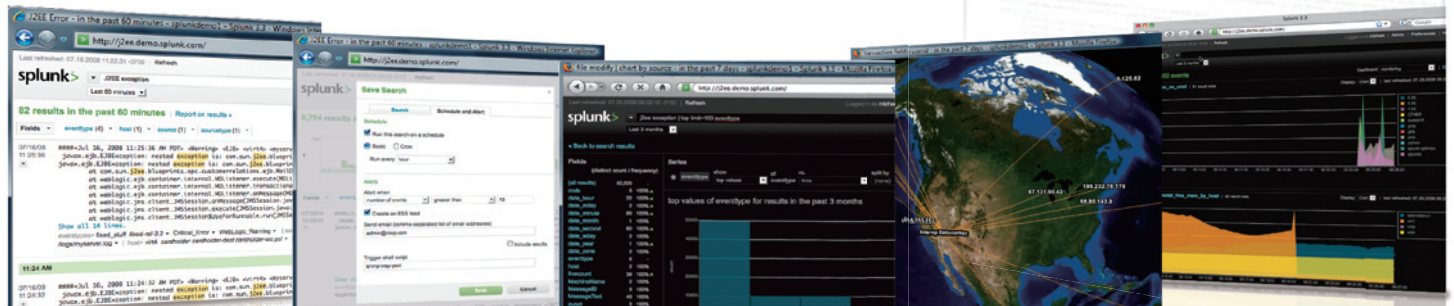
インフラが毎日生成するログデータなど、ITデータの中には運用管理に必要な価値ある情報が埋もれています。膨大な情報の中から、欲しい情報をどうやって見つけ出していますか?

SplunkはITインフラに対する拡張性と高速性を兼ね備えた、革新的なインデックス作成機能(インデキシング)と検索技術を提供することにより、インターネットの検索と同じような感覚で必要なITデータ・ログを見つけて出し、収集することができます。

Splunkは、いかなるアプリケーション、サーバ、ネットワーク機器が生成するデータであっても、インデックスを作成し、リアルタイムの検索とナビゲートを可能にするソフトウェア製品です。ログ、コンフィグレーションファイル、メッセージ、トラップ、アラート、スクリプト、コマンドの実行結果など、およそマシンが生成するデータであれば、Splunkはほぼ全てを取り込むことができます。

ネットワークエンジニア、システム管理者、セキュリティ及びコンプライアンス担当者、開発担当、カスタマーサポート、ヘルプデスクスタッフなどの方が、ITインフラの中で起きていることを、その起きた瞬間に知ることができるようになります。

数百の大手企業、サービスプロバイダ、政府機関などが既にSplunkをITデータの運用管理、セキュリティ、コンプライアンス、ビジネスインテリジェンスなどのサポートに使用しています。



検索

アラート

レポート

共有

可視化

アプリケーション
プラットフォーム

認証とセキュリティ機能

データ入力

- ファイル
- ネットワーク
- データベース
- リモートインターフェース
- API
- スクリプト

ユニバーサル
インデキシング

多次元検索

ナレッジ
マネジメント

データ
マネジメント

データルーティング

アーカイブ/リストア

- ローカルディスク
- SAN
- NAS
- DAS

データ保存

Splunkは、ダウンロードしてインストールすれば、すぐに使い始めることができる画期的でパワフルな検索・分析機能を持つ、ITインフラ運用管理ソリューションです。

機能

ユニバーサル リアルタイム インデキシング

- あらゆるフォーマット、あらゆる種類のITデータを認識
- データ取り込みのためのファイルやディレクトリのモニタリング、ファイルシステムへのクロウリング
- syslog、OPSEC LEA、SNMP、JMX/JMS、SQL/DBI、WMI、Windowsレジストリなどの直接入力
- スクリプトとネットワークリスナーポートによる独自データ入力の定義
- タイムスタンプと複数行に渡るイベントを自動的に検出
- 独自アルゴリズムでイベントとソースを分類
- オリジナルのイベントにある各項目の緻密なインデキシング
- 生データとインデックスをサーバのファイルシステム内に保持

アドホックな(特定目的のための)検索とナビゲーション

- タイプahead(先行入力)機能付きフリーフォーム検索
- 検索結果はその場で瞬時に表示
- 時間やキーワード、複雑な相関関係から関連イベントをナビゲート
- 様々な要素を複合的に組み合わせたビュー(表示、参照)を可能にするイベントの抽出・グループ化機能

インタラクティブなアラートとレポート

- 検索時に動的にフィールドを抽出し、レポート生成に使用
- インタラクティブなグラフ作成、レポート作成インターフェース
- 多彩なグラフ、チャート
- パワフルな統計、相関操作
- 全ての検索をアラート設定付きで保存可能
- 電子メール、RSS、SMS、SNMP、syslog、カスタムスクリプトによるアラート通知

知識の確保と共有

- 検索、アラート、レポート、タグの保存と共有
- Splunkコミュニティでの共有と学習

拡張性

- 必要なものをすべて備えた自己完結型ソフトウェアパッケージ、豊富な動作プラットフォーム
- クラスターと分散による拡張
- データルーティングとクロウニング
- 集中管理するために組み込まれた展開サーバ

セキュアなデータ管理

- Splunkインスタンス間のセキュアなSSL通信
- セキュアなユーザアクセス、ロールベースの認証、細分化されたアクセスコントロールのためのLDAP連携
- 管理者とユーザに対する監査
- 圧縮された生データの長期保存
- ポリシーベースのデータアーカイブ、リタイア及びリストア

オープンアーキテクチャ

- ブラウザツールバーでウェブベースアプリからSplunkを起動
- REST API
- TCPを用いてリアルタイムでデータを他のシステムにルーティング
- スクリプトベースでの入力と出力

フリー版とエンタープライズ版の違い

	フリー	エンタープライズ
1日あたりの最大インデキシングボリューム	500MB	ライセンスによる
ユニバーサル リアルタイム インデキシング	✓	✓
アドホックな検索とナビゲーション	✓	✓
アラートとレポート	✓	✓
知識の確保共有	✓	✓
Splunk コミュニティアクセス	✓	✓
開発用 API	✓	✓
データクロウニングとルーティング	✓	✓
他の Splunk サーバからのデータの受信	✓	✓
分散サーチ		✓
アクセスコントロールと複数ユーザアカウント		✓
展開用サーバ		✓

システム要件

サーバオペレーティングシステム

- UNIX** : 主要な Linux ディストリビューション 2.6+ カーネル/x86_64 または x_86 ; Solaris (8,9,10) /SPARC ; Solaris (9,10) /x86 ; FreeBSD 6.1 以降 /x86, AIX 5.2/5.3
- Windows (32-bit)** : Windows 2000, XP, Windows Server 2003, Vista, Windows Server 2008
- Windows (64-bit)** : Windows Server 2003, Vista, Windows Server 2008
- MAC** : Mac OSX (10.4+)/PPC または Intel

サーバハードウェア

- 1x1.4GHz CPU, 1GB メモリ (最少)、2x3.4GHz CPU, 4GB メモリ (推奨) 以上 非 Windows プラットフォーム
- Pentium4 同等 CPU, 2GHz, 2GB メモリ (最少)、マルチコア Xeon 同等 CPU, 3GHz, 4GB メモリ (推奨)

ストレージ

- インデキシングの密度とデータソースに応じて生データサイズの 12-48%

ブラウザ

- AIX, BSD** 及び **Linux** : Firefox 1.5 または 2.0; Adobe Flash 9 以降
- Mac OS X** : Firefox 1.5 または 2.0; Adobe Flash 9 以降
- Windows** : Internet Explorer 6 または 7、Firefox 1.5 または 2.0; Adobe Flash 9 以降

最新の製品情報・詳細は

www.ssl.fujitsu.com/products/sysope/splunk/ をご覧ください。

■ Splunk 製品に関するお問い合わせ先

Email : ssl-info@cs.jp.fujitsu.com



マクニカネットワークス株式会社

本社 〒222-8562 横浜市港北区新横浜 1-5-5
 TEL.045-476-1973 FAX.045-476-1976
 大阪営業所 〒532-0003 大阪市淀川区宮原 3-4-30 ニッセイ新大阪ビル 17階
 TEL.06-6397-1055 FAX.06-6397-1056

株式会社 富士通ソーシアルサイエンスラボラトリ

マーケティング本部 ソリューション推進部

〒211-0063 川崎市中原区小杉町1-403 武蔵小杉タワープレイス

TEL:044-739-1251

E-mail: ssl-info@cs.jp.fujitsu.com

2009年3月 ©Macnica Networks Corp.
 ● このカタログに掲載のある社名および製品名は、各社の商標または登録商標です。
 ● 仕様は予告なく変更する場合があります。