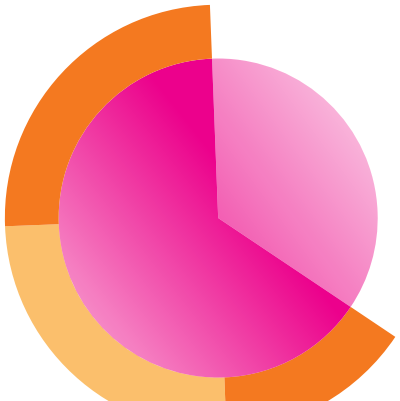
インフラデータ・マシンデータ
エッセンシャルガイド

splunk>
turn data into doing™

時系列データ
ストリーミングデータ
ダークデータ

世界中の多くの組織でデータが過小評価され、十分に活用されていないことは今や周知の事実です。データに基づく意思決定のメリットが盛んにうたわれているにもかかわらず、あらゆる規模の組織が、ユーザー、ネットワークデバイス、外部リソースなどから日々生成される大量のデータを捕捉して活用するための効果的な方法を見出せずにいます。実際、ビジネス部門やIT部門の多くの意思決定者が、**組織内のデータの55%がダークデータである**(存在が把握されていないか十分に活用されていない)と推定しています。

これによって失われる機会は膨大です。これらのデータの中には、IT、セキュリティ、組織に関する重要なインサイトが眠っています。また、これらのデータには、顧客、ユーザー、トランザクション、アプリケーション、サーバー、ネットワーク、モバイルデバイスなどのすべてのアクティビティや行動が明確に記録され、設定から、API、メッセージキュー、診断結果、産業システムのセンサーデータまで、あらゆる重要情報が埋もれています。これらを活用しない手はありません。



適切なアプローチを使用してデータを活用すれば、以下のメリットが簡単に得られます。

- ビジネスのあらゆる面について、情報に基づくより的確な意思決定を行う
- 業務の効率を向上させる
- ユーザーエクスペリエンスやカスタマーエクスペリエンスを最適化する
- 不正行為の痕跡を見つける、または不正行為を未然に防ぐ
- 障害の兆候を検出して未然に防ぐ
- 競争優位を獲得するために役立つ隠れたトレンドを発見する
- 困っている人を助けてヒーローになる

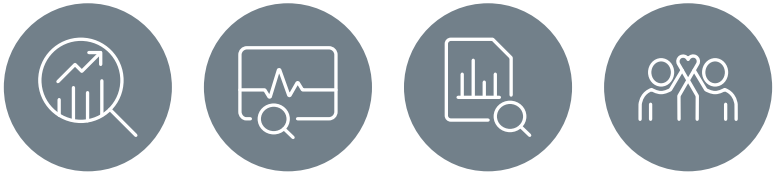
ほかにもたくさんあります。

多くの組織が抱える大量データを活用するための課題は、データの形式がばらばらで、従来のデータ監視ツールや分析ツールでは処理できないことです。多くのツールは、多様なデータ構造、ソース、時間尺度に対応していません。しかも、対象となるのはマシンデータだけではありません。とはいえ、データを活用して得られるメリットは計り知れません。そこで活躍するのがSplunkです。

Splunkなら、組織内の問題解決、意思決定、ビジネス戦略にデータを活用して、有意義な成果を得ることができます。他のプラットフォームとは異なり、Splunkでは言葉のとおりあらゆるソースからデータを取り込み、アクションにつなげて、ITインフラから、セキュリティ監視、DevOps、アプリケーションパフォーマンス監視/管理まで、ビジネスに幅広く活用できます。

Data-to-Everythingの実践

データの用途：



データの価値を最大限に引き出すには、さまざまなタイプのデータを収集し、関連付けて、求める答えを導き出せるようにする必要があります。しかし、取り込むべきデータがわからなければ何も始まりません。

まずは、セキュリティ、IT運用、ビジネスアナリティクス、DevOps、IoTなどの一般的なユースケースと、それぞれに関係するデータタイプやソースを知ることが、次のステップにつながります。

たとえば次のような状況が発生したとします。

1. お客様の注文が処理されなかった
2. お客様がサポート窓口に電話をして、問題を解決しようとした
3. しかし電話がなかなかつながらず、お客様はあきらめて、この会社に対する不満をツイッターで訴えた

マシンデータはどのように見えるか？

図1：データは数多くのデータソースから取得できます。一見すると、これらのデータは互いに関連性のないテキスト情報のように思われます。

重要なインサイトを含むマシンデータ

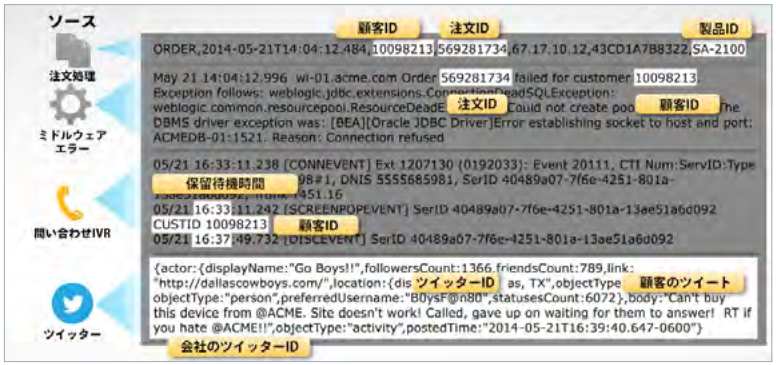


図2：データの価値は、この一見互いに関連性がないように見えるテキスト情報の中に眠っています。

重要なインサイトを含むマシンデータ

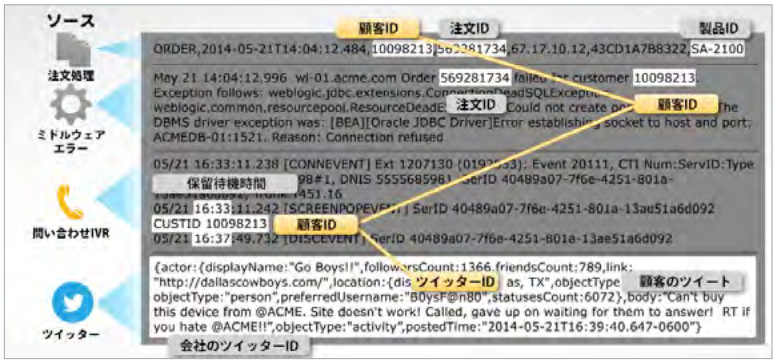


図3：多種多様なデータを相互に関連付けることで、インフラ状況について真のインサイトを獲得したり、セキュリティ脅威を発見したりできます。さらに、このインサイトを活用することで、より適切なビジネス意思決定を下せます。

この場合、このプロセスに関係するすべてのデータ(受注処理、ミドルウェア、対話型音声応答システム、ツイッターの情報)を総合すれば、カスタマーエクスペリエンスの問題の全体像を把握できます。

インフラデータ

このガイドでは、通常の業務中に仮想インフラや物理インフラで生成されるデータから得られる価値について、その概要を説明します。このデータを利用すれば、クラウド環境の監視、侵入の形跡の検出、脆弱性の排除など、さまざまなユースケースに対応できます。

組織のニーズやデータソースは、その組織が利用するベンダー、製品、インフラによってさまざまです。このガイドでは、探すべきデータの種類と場所、およびそのデータがIT、セキュリティ、IoT、ビジネスアナリティクスの各ユースケースにもたらす価値について説明します。

このガイドに記載されているデータソースの多くは、複数のユースケースに対応できます。このこと自体、マシンデータのもたらす大きな価値と言えるでしょう。

セキュリティと
コンプライアンス

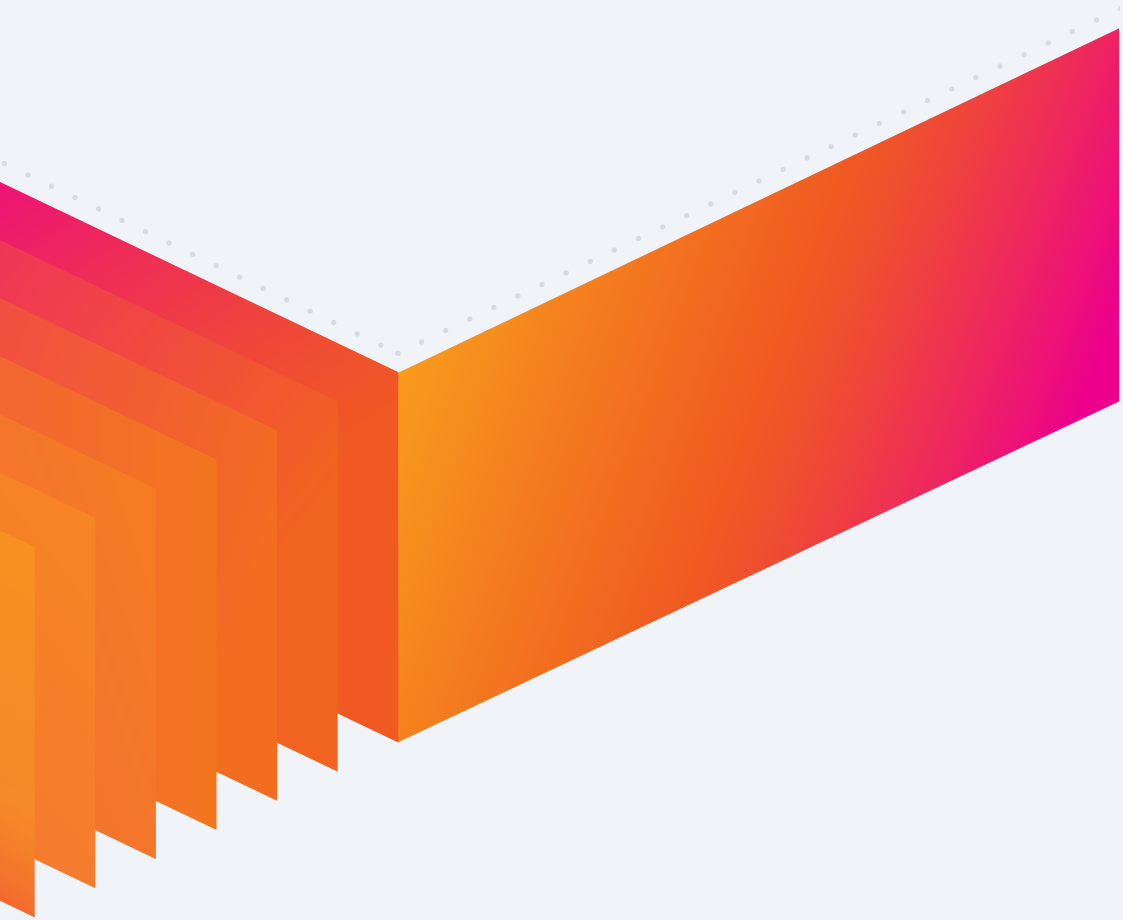
IT運用、アプリケーションデリバリー、DevOps

IoT

ビジネスアナリティクス

目次

仮想インフラのデータ



AWSサービス

ユースケース：セキュリティとコンプライアンス、IT運用

例：CloudTrail、CloudWatch、Config、S3

アマゾンウェブサービス (AWS)は、最も規模が大きく、最も広く利用されているパブリッククラウドインフラで、オンデマンドのコンピューティング、ストレージ、データベース、ビッグデータ、アプリケーションサービスを、従量制料金で提供するものです。AWSを従来のエンタープライズ仮想サーバーインフラの代わりに利用すれば、ソフトウェアを仮想マシン(VM)上で動かしたり、複数のAWSサービスで構成されたクラウドネイティブのアプリケーションをホストしたりできます。AWSには、サービス管理、自動化、セキュリティ、ネットワーク、監視のためのさまざまなサービスがあり、AWS環境、サブスクリプション、およびホステッドアプリケーションのデプロイ、スケーリング、使用停止、監査、管理に使用できます。

ユースケース

セキュリティとコンプライアンス：AWSサービスのセキュリティデータには、ログインとログアウトのイベントと試行、API呼び出し、ネットワークログ、Webアプリケーションファイアウォールのログなどがあります。

IT運用：AWSサービスは、従来のITインフラと同じようなタイプのシステムデータとサービスデータを提供していますが、その多くがCloudWatchサービスによって統合されています。ユーザーは、他のAWSリソースやアプリケーションによって生成されたメトリクス、ログ、イベントに対して、ダッシュボードを利用してサービスの監視やアラームの設定が可能です。主なイベントや測定値には、インスタンスが開始および停止された日時、CPU使用率、ネットワークトラフィック、ストレージ消費量などがあります。

Google Cloud Platform (GCP)

ユースケース：セキュリティとコンプライアンス、IT運用

例：Stackdriver

GCPは、人気が高く、広く利用されているクラウドインフラで、オンデマンドのコンピューティング、ストレージ、データベース、ビッグデータ、アプリケーションサービスを、従量制料金で提供するものです。GCPを従来のエンタープライズ仮想サーバーインフラの代わりに利用すれば、ソフトウェアをVM上で動かしたり、複数のGCPサービスで構成されたクラウドネイティブのアプリケーションをホストしたりできます。GCPには、サービス管理、自動化、セキュリティ、ネットワーク、監視のためのさまざまなサービスがあり、GCP環境、サブスクリプション、ホステッドアプリケーションのデプロイ、スケーリング、使用停止、監査、管理に使用できます。

ユースケース

セキュリティとコンプライアンス：GCPサービスのセキュリティデータには、ログインとログアウトのイベントと試行、API呼び出し、ネットワークログ、Webアプリケーションファイアウォールのログなどがあります。

IT運用：GCPサービスは、従来のITインフラと同じようなタイプのシステムデータとサービスデータを提供していますが、その多くがStackdriverによって統合されています。ユーザーは、他のGCPリソースやアプリケーションによって生成されたメトリクス、ログ、イベントに対して、ダッシュボードを利用してサービスの監視やアラームの設定が可能です。主なイベントや測定値には、インスタンスが開始および停止された日時、CPU使用率、ネットワークトラフィック、ストレージ消費量などがあります。

Microsoft Azure

ユースケース：セキュリティとコンプライアンス、IT運用

例：WADログ、WADイベントログ、WADパフォーマンスカウンター、WAD診断インフラ

Azureは、人気が高く、広く利用されているクラウドインフラで、オンデマンドのコンピューティング、ストレージ、データベース、ビッグデータ、アプリケーションサービスを、従量制料金で提供するものです。Azureを従来のエンタープライズ仮想サーバーインフラの代わりに利用すれば、ソフトウェアをVM上で動かしたり、複数のAzureサービスで構成されたクラウドネイティブのアプリケーションをホストしたりできます。Azureには、サービス管理、自動化、セキュリティ、ネットワーク、監視のためのさまざまなサービスがあり、Azure環境、サブスクリプション、ホステッドアプリケーションのデプロイ、スケーリング、使用停止、監査、管理に使用できます。

ユースケース

セキュリティとコンプライアンス：セキュリティチームは、Azureのサービスログを使用し、定義済みのポリシーに基づいてコンプライアンスを監査および実証することが可能です。また、不正アクセスの兆候をアクセスログから発見したり、リソースや設定の変更に関するイベントを追跡したり、ホストやファイアウォールの脆弱性を特定したりするといったインシデントフォレンジック分析にも、ログデータが大いに役立ちます。

IT運用：Azureサービスは、テクノロジースタック、VM、コンテナ、ストレージ、アプリケーションサービス全体でインフラを監視するための詳細なメトリクスとログを提供するものです。このデータは、アプリケーションデリバリーの品質とサービスレベルを維持し、ユーザーの行動を測定し、リソースの使用量を把握して、容量計画とコスト管理を行うのに役立ちます。

仮想インフラのデータ

Pivotal Cloud Foundry (PCF)

ユースケース：IT運用、DevOps

例：Loggregator、PCF Healthwatch

Pivotal Cloud Foundryは、開発者がクラウドネイティブアプリケーションを簡単にデプロイ、運用、スケーリングできるPaaS (Platform-as-a-Service)で、オープンソースのクラウドコンピューティングプラットフォーム、Cloud Foundryに構築されています。Cloud Foundryでは多くのクラウドフレームワークとアプリケーション言語がサポートされているため、パッケージングから、デプロイ、実行までのアプリケーションライフサイクル全体を管理できます。PCFでは、インフラの管理とプロビジョニング、OSのパッチ適用、コンテナのオーケストレーション、セキュリティなどの機能により、クラウドネイティブアプリケーションのインストールと管理を簡単に実行できます。

ユースケース

IT運用とDevOps：運用チームは、PCFメトリクスを活用して、デプロイの健全性、キャパシティの需要、アプリケーションの健全性に関するインサイトを得ることで、パフォーマンスの低下がエンドユーザーに影響を及ぼす前に問題に対応できます。これらのメトリクスの多くはLoggregator Firehoseを介して統合されます。DevOpsチームは、PCFを利用することにより、任意のクラウドでアプリケーションの運用をすばやく開始し、オンデマンドでスケーリングできます。そのため、PCFデータを活用して、ライフサイクル全体をエンドツーエンドで可視化するとともに、個々のコンポーネント間でのやり取りを可視化することが重要になります。大規模なPCF環境を運用する場合、パフォーマンスを把握するには、アプリケーション、コンテナ、さらに大きなアーキテクチャ内の各種レイヤー間の依存関係を理解する必要があります。

仮想インフラのデータ

VMwareのサーバーログ、設定データ、パフォーマンスメトリクス

ユースケース：セキュリティとコンプライアンス、IT運用

例：vCenter、ESXi

VMware vSphere ESXiは、最もよく利用されているエンタープライズサーバー仮想化プラットフォームです。VMwareの管理プラットフォームは、vSphere製品またはスタンドアロンのハイパーバイザーに関するさまざまなデータを生成しますが、それらのデータは主に次の4つに分類されます。

- **vCenterログ：**vCenterはvSphere環境の「コントロールセンター」です。vCenterログには、変更を行うためにログインしたユーザー、変更を行ったユーザー、認証エラーなどの情報が表示されます。
- **ESXiログ：**すべてのvSphere環境には1つまたは複数のESXiハイパーバイザーが含まれており、仮想マシンをホストするシステムとして動作しています。ESXiログには、ハードウェアの問題や設定の問題のトラブルシューティングに役立つ情報が表示されます。
- **インベントリ情報：**vCenter環境は、ハイパーバイザー、仮想マシン、データストア、クラスターなど、さまざまなアイテムに関する設定を追跡します。これには、各アイテムの設定やアイテム間の関連性に関する情報が含まれます。この情報は、vCenterサーバーとESXiサーバーのどちらのログファイルにも表示されません。この情報を表示するには、vSphereクライアントを使用するか、vSphere APIを使用してこの情報を取り出す必要があります。どちらの場合も、情報はvCenterサーバーから取り出されます。
- **パフォーマンス情報：**vCenterサーバーは、構成アイテムごとにさまざまなパフォーマンスメトリクスを追跡します。データストアのレイテンシー、仮想または物理CPUの使用率など100を超えるメトリクスがこのカテゴリに分類されます。インベントリ情報と同じく、この情報はログファイルに表示されないため、vSphereクライアントから表示するか、vSphere APIから取り出す必要があります。

ユースケース

セキュリティとコンプライアンス：仮想サーバーと基盤の物理ハードウェアはそれぞれ独立した存在であるため、インシデント調査、容量分析、変更追跡、セキュリティレポートに複雑な問題をもたらす場合があります。VMwareデータのセキュリティでよくあるユースケースは、vCenterログに関するもので、vSphereインターフェイスを利用するユーザーのアクティビティを監視し、VMware環境内でユーザー権限を割り当て直します。

IT運用：運用チームは、VMwareのデータを使用して、ハイパーバイザー環境と基盤のゲストオペレーティングシステム全体の健全性を測定できます。管理者はこのデータを使用することで、容量計画の策定や、データストアのレイテンシーなどパフォーマンスにまつわる問題のトラブルシューティングの実行が可能です。

また、このデータに記録されるハードウェアリソースの使用量を確認して、サーバープール全体のVMデプロイを最適化することで、どのサーバーのワークロードも過大になることなく、リソースを最大限に活用できます。

仮想インフラのデータ

物理インフラのデータ

バックアップ

ユースケース：IT運用

データ複製によって、システム、データベース、およびファイルストアのミラーリングが行われるようになった今でも、データバックアップは重要なIT機能です。この機能のおかげで、保全に関する法規制要件に基づいて、多くの価値ある情報をアーカイブとして長期間保存できます。また、バックアップ機能を使って、さまざまなバージョンのシステムイメージやデータを保存することも可能です。これにより、変更されたデータ、誤って消去されたデータ、破損したデータをすばやく復旧したり、システムやデータベースを以前の正常な状態に戻したりできるようになります。バックアップソフトウェアでは、データのニーズに応じてさまざまな種類のストレージメディアを使用できます。たとえば、利用中のデータを保存する外部ディスクや仮想テープライブラリ、および長期的にデータを保管するテープ、光ディスク、クラウドサービスなどです。

ユースケース

IT運用：バックアップシステムは、アクティビティやシステムの状態を定期的にログに記録します。具体的には、ジョブの履歴、エラー状態、バックアップターゲット、コピーされたファイルやボリュームの詳細なリストなどです。運用チームは、このデータを利用して、バックアップシステム、ソフトウェア、およびジョブの健全性を監視できます。また、エラー発生時にアラートを生成したり、バックアップエラーのデバッグを支援したりすることが可能です。さらに、リカバリが必要になった場合に、特定のデータが保存されている可能性がある場所を見つけ出せるようになります。

環境センサー

ユースケース：IoT、ビジネスアナリティクス

例：Bosch Sensortec、Mouser Electronics、Raritan、Schneider Electric、TSI、Vaisala

環境センサーは、気圧、湿度、周囲温度、大気質に関するデータを提供します。環境汚染対策から、ガス漏れの検知、データセンターの過熱防止まで、幅広い用途に利用されています。

ユースケース

IoT：環境センサーは、環境を監視するように最適化されたスマートメーターの一種です。データセンターなどでは、温度設定や熱流を自動的に調整するために、環境センサーからのデータが利用されています。

ビジネスアナリティクス：小売業界では、環境センサーのデータを利用して、悪天候がモールの来店者数にどう影響するかといった予測が可能です。

ICS(産業用制御システム)

ユースケース：セキュリティとコンプライアンス、IoT、ビジネスアナリティクス

例：ABB、Emerson Electric、GE、日立、Honeywell、Rockwell Automation、Siemens、東芝

ICSは、プログラマブルロジックコントローラー (PLC)を利用してデータを取得して監視機能を実行する、製造業向けのシステムです。製造施設で導入されるプロセスオートメーションの多くは、ICSによって実現されています。

ユースケース

セキュリティとコンプライアンス：ICSは、世界中の産業や自治体にサービスを提供する上で重要な役割を果たします。これらのシステムは、従来のITインフラ上に構築され、通常は企業のITシステムから切り離されますが、デジタルトランスフォーメーションの取り組みの中で他のシステムと接続する事例が増え、攻撃を受けるリスクが高まっています。これらのシステムは、セキュリティ対策の盲点になりがちです。ICSに対する攻撃や感染を防ぐには、ICSデバイスのデータを収集して可視性を確保するとともに、データを分析して悪意のあるアクティビティや潜在的な脅威を特定する必要があります。可視性を確保すれば、影響やリスクを測定して、ビジネスプロセスと関連付けることができます。

IoT：ICSから収集したマシンデータを利用すれば、重要な資産のアップタイムと可用性をリアルタイムで可視化できます。これにより、問題を検出し、根本原因分析を実行して、今後のイベント発生に対する予防策をとることができます。また、ICSのマシンデータを利用して、これらのミッションクリティカルな資産を保護することもできます。

ビジネスアナリティクス：ICSで生成されたマシンデータに機械学習アルゴリズムを適用して、生産性、アップタイム、可用性の向上に役立てることができます。ICSデータによって複雑な製造プロセスを可視化して、ボトルネックや非効率なプロセスを特定することもできます。

物理インフラのデータ

メインフレーム

ユースケース：IT運用

メインフレームは、初めて登場した企業向けコンピューターで、複数のプロセッサー、システムメモリ(RAM)、I/Oコントローラーを内蔵した大規模な集中型システムとして構成されています。メインフレームが登場したのは60年も前のことですが、ミッションクリティカルなアプリケーション(特にトランザクション処理)で今も広く利用されています。メインフレームは基本的に専用OSで動作していますが、仮想化を行えばUnixやLinuxを動かすことが可能で、アドオンのプロセッサーカードを使えばWindows Serverを動かすことも可能です。メインフレームは、冗長性の高いハードウェアと厳しいテストを経た回復力の高いソフトウェアのおかげで、信頼性と安全性が非常に高い点が評価されています。そのため、複数のワークロードを少数のシステムに統合し、信頼性と汎用性を高めたいと考えている組織にとって効果的です。

ユースケース

IT運用：メインフレームは他のサーバーと同じく、現在の状態、設定、および全体的な健全性を示すさまざまなシステムパラメーターを測定し、ログに記録するものです。多くのメインフレームのサブシステムは冗長性を備えているため、システムログには、致命的ではないハードウェア障害やエラーの兆候を示す異常な動作も記録されます。メインフレームは重要なアプリケーションに利用されるため、多くの場合、メモリー使用率、I/Oとトランザクションのスループット、プロセッサーの使用率、ネットワークアクティビティなどのアプリケーションパフォーマンスに関わるデータが記録されます。

医療機器

ユースケース：IoT、ビジネスアナリティクス

例：Abbott Laboratories、Apple、Baxter、Boston Scientific、GE、Siemens、St. Jude Medical

集中治療室からウェアラブルデバイスまで、あらゆる医療機器がさまざまなタイプのマシンデータを生成します。実際、病院内外での患者ケアのほぼすべての面を医療機器で測定できます。一番の目的は患者の命を救うことですが、必要な通院回数と入院期間を減らして医療コストを削減することも重要な目的の1つです。

ユースケース

IoT：病院内の多くの機器は、院内監視アプリケーションに接続されています。一方、自宅療養の患者を監視するシステム(ウェアラブルデバイスなど)と通信するセンサーを使用すれば、患者の状況をリモートで監視することもできます。

ビジネスアナリティクス：マシンデータを利用すれば、医療専門家が、地理的に分散した広範な地域を対象に患者データと匿名データを簡単に分析できます。たとえば、特定の疾患のかかりやすさに地域差があるかどうかを検証できます。

メトリクスラインプロトコル

ユースケース：IT運用、アプリケーションデリバリー、IoT

例：collectd、statsd

メトリクスは、システム上で実行されているプロセスによって生成される測定値で、CPU使用率など特定の測定基準について一定間隔のデータポイントを示すものです。通常、メトリクスデータソースは以下の項目で構成されており、一定の間隔で測定値を生成します。

- タイムスタンプ
- メトリクス名
- 測定値(データポイント)
- ディメンション(多くの場合、メトリクスをフィルタリングまたはソートするために必要となるホストやインスタンス、およびその他の属性を示す)

メトリクスを生成するのは通常、サーバー (OS)、コンテナ、アプリケーションで実行されるデーモン(プロセス)です。各データ測定値は、UDPやHTTPなどのネットワークプロトコル経由でサーバーに送られ、そこで情報のインデックス化と分析が行われます。

メトリクスは、監視に用いると特に有効です。たとえば、患者の心拍数を定期的に確認する心拍モニターのように、インフラやアプリケーションのパフォーマンスと可用性に影響する傾向や問題についてのインサイトを、メトリクスから得ることができます。ただし、心拍モニターは、患者の心拍数に突然問題が生じた理由を教えてはくれません。原因をすばやく特定して患者の容態を安定させるには、別の方法が必要です。同じことは、マシンデータにも該当します。他のデータソース(通常はログ)と統合することで、起こっている問題とその原因の両方に関するインサイトを取得できるのです。

メトリクスラインプロトコルの例：

collectd：collectdは、特定の属性を測定してその情報を定義済みの宛先に送信するように構成されたサーバー上で実行されるエージェントを含むプロトコルです。collectdは拡張性に優れた測定エンジンであり、幅広いデータを収集できます。現在、collectdが最もよく利用されているのは、サーバーやその他のインフラコンポーネントのワークロード、メモリー使用率、I/O、ストレージに関するインサイトなど、主要インフラを監視するためのインサイトの取得です。collectdはオープンソースとして開発されています。collectdについて詳しくは、**http://collectd.org**をご覧ください。

statsd：statsdは、Node.js上で実行されるネットワークデーモンです。Windowsの管理者やアプリケーションパフォーマンスの専門家の間で人気があります。statsdの機能を利用すると複数のメトリクスをまとめて提供できることと、信頼性が低いUDPネットワークを利用するものの配備が簡単なことから、多くの管理者に人気があるのです。collectdとほとんど同じように、statsdはメトリクスを収集することに重点を置いています。たいていの場合、このメトリクスはアプリケーションとコンポーネントの使用状況とパフォーマンスを含んでおり、そのような情報を収集して分析できるツールに向けてネットワーク経由で送信されます。

ユースケース

IT運用とアプリケーションデリバリー：メトリクスラインプロトコルは、オペレーティングシステム、ストレージデバイス、アプリケーション、およびITインフラの他のコンポーネント全体を対象とした、使用状況、パフォーマンス、可用性に関するデータを提供します。メトリクスが特に役立つのはIT運用とアプリケーションデリバリーを監視する場合であり、トレンドを調べることで、問題が発生している場所を特定できます。トレンドやしきい値がパフォーマンスの問題を示していることが判明すれば、多くの場合、他のデータソースを関連付けることで問題の根本原因を特定できます。

IoT：デバイスのインテリジェント化が進むにつれて、メトリクスベースの測定値の利用も増えるでしょう。メトリクスラインプロトコルは、このようなデバイスの状態やパフォーマンスを知るための効果的な手段を提供します。

物理インフラのデータ

パッチログ

ユースケース：セキュリティとコンプライアンス、IT運用

最新のバグ修正プログラムやセキュリティパッチを適用して、オペレーティングシステムとアプリケーションを最新の状態に保つことは、予定外のダウンタイム、アプリケーションの突然のクラッシュ、セキュリティ侵害を防止するためにきわめて重要です。市販のアプリケーションやオペレーティングシステムは通常、パッチを適用するためのソフトウェアを内蔵しています。しかし、組織によっては、独自のパッチ管理ソフトウェアを利用してパッチ管理を統合し、すべてのアプリケーションにパッチが確実に適用されるようにしたり、自社のカスタムアプリケーションに対してパッチジョブが実行されるようにしたりしている場合があります。

パッチ管理ソフトウェアでは、利用可能なアップデートのデータベースを使用してパッチのインベントリを作成し、組織がインストールしたソフトウェアと照合することが可能です。また、パッチのスケジュール設定、インストール後のテストと検証、必要なシステム設定とパッチ適用手順の文書化などの機能もあります。

ユースケース

セキュリティとコンプライアンス：セキュリティチームはパッチログを使用することで、システムの更新を監視し、パッチのエラーや古いパッチのため危険にさらされる可能性がある資産を確認できます。

IT運用：運用チームは、パッチログを使用することで、スケジュール設定されたパッチが、適切なタイミングで適切なアプリケーションに適用されたことを確認します。また、パッチが未適用のシステムやアプリケーションを特定し、パッチ処理のエラーに関する警告を発信します。エラーをパッチログと関連付けることで、そのエラーがパッチに起因するのかを確認できます。

物理カードリーダー

ユースケース：セキュリティとコンプライアンス

ほとんどの組織は、自動化されたシステムを使用して、施設への物理的なアクセスを管理しています。そのために、従来はシンプルな磁気ストライプ付きの社員バッジを使用していましたが、セキュリティ要件の厳しい場所では、生体認証リーダーやデジタルキーのようなものを使用している場合があります。どのようなテクノロジーのシステムでも、ユーザーの個人情報をデータベースと照合し、そのユーザーの入館許可が確認されればドアを解錠する仕組みです。デジタルシステムであるバッジリーダーには、ユーザー IDや入館日時が記録されるだけでなく、入館時の写真などの情報が記録されることもあります。

ユースケース

セキュリティとコンプライアンス：ITセキュリティチームにとって、カードリーダーから提供される物理的な場所へのアクセスに関するデータは、ネットワークファイアウォールのログと同じような情報です。このデータを利用すれば、侵入が試みられた形跡を見つけ出し、その情報をシステムログやネットワークログと関連付けることで、潜在的な内部脅威を特定し、全体の状況を把握できるようになります。また、通常では考えられない時間や場所でのアクセスや、長時間にわたるアクセスを検出できるようになります。

POS

ユースケース：セキュリティとコンプライアンス、IoT、
ビジネスアナリティクス

例：IBM、LightSpeed、NCR、Revel Systems、Square、東芝、Vend

POSシステムといえば、通常、小売店で生成されるトランザクションを連想しますが、モバイルPOSソリューションの普及によって、地域の催しや学校の行事など、一時的なイベントでもPOSシステムが使われ始めています。

一般的なPOSシステムには、PCまたは組み込みシステムベースのキャッシュレジスター、モニター、レシートプリンター、ディスプレイ、バーコードスキャナー、デビット/クレジットカードリーダーが含まれます。POSシステムで生成されるマシンデータから、売れた商品から、トランザクションごとの売上金額、使用された支払方法まで、すべてのトランザクションに関するインサイトをリアルタイムで取得できます。

ユースケース

セキュリティとコンプライアンス：通常、POSシステムは金融取引に使用され、その中で口座、決済、財務情報がやり取りされるため、攻撃の標的になりやすい面があります。POSトランザクションに攻撃者が特に欲しがる情報が含まれるだけでなく、POS自体がネットワークに侵入するための入口として利用できるため、POSシステムの保護は非常に重要です。さらに、POSシステムには通常、管理者がおらず、その基盤ではオペレーティングシステムが実行され、バージョン管理や監視はITチームの監視対象外にあるため、セキュリティがさらに複雑になります。POSシステムとそのデータを可視化して分析すれば、財務情報の保護、不正行為の検出、脆弱性の悪用防止に役立つ重要なインサイトを得ることができます。

IoT：以前は、POSシステムをネットワークに一切接続しないか、専用のプライベートネットワークにのみ接続するのが一般的でした。しかし、IoTが普及して以来、POSシステムをクラウドプラットフォームに直接接続して、中央の場所からリモートで簡単に管理できるようになりました。これによってITスタッフが現地に赴いて各システムを1つずつ手動で更新する必要がなくなります。これは、障害対応においても重要な点です。POSシステムに障害が発生すると、顧客を待たせることになり、顧客の満足度が低下するばかりか、収入減につながることもあります。競争の激しい小売業界では、カスタマーエクスペリエンスの低下は顧客離れにすぐにつながります。

ビジネスアナリティクス：POSシステムには、売れた商品、支払方法、商品の売れ行きなどの情報が詰まっています。このデータを利用すれば、売上をリアルタイムで監視して、対面販売の改善、商品レイアウトと売れ行きの追跡、不審なトランザクションのリアルタイムでの検出などに役立てることができます。このようなリアルタイムのビッグデータ分析をうまく活用すれば、クロスセルやアップセルの機会を増やすことができます。また、POSデータは、人気のクーポンや、一緒に買われることの多い商品の組み合わせを調べるなど、カスタマーエクスペリエンスの可視化にも役立ちます。地理位置データと組み合わせれば、地域別にデータを分析することで、より価値のあるインサイトを得ることもできます。

物理インフラのデータ

RFID/NFC/BLE

ユースケース：IoT、ビジネスアナリティクス

例：Alien Technology、BluVision、CheckPoint Systems、Gimbal、MonsoonRF、Radius Networks、STMicroelectronics、TAGSYS RFID、ThingMagic

今日、小売店で商品の追跡や顧客とのやり取りに使用される主なワイヤレス方式には2つあり、それぞれ異なるワイヤレス通信技術が使用されています。そのうち最もよく知られているのがRFID(Radio-Frequency IDentification)です。この方式では、商品の詳細や出荷状況などの情報を保存できるタグが使用されます。

このほかに、他のデバイスに信号を送信できるBLE (Bluetooth Low Energy)ワイヤレス接続ソリューションもよく使用されます。BLEは、小売店が買い物客のスマートフォンにセールス情報を通知したり、スポーツイベントで今後のイベント情報をファンに発信したりするためのビーコンとしてよく使用されます。

ユースケース

IoT：RFIDは、IoTアプリケーションの初の実用例と言ってよいでしょう。RFIDタグは、従来のバーコードリーダーの代わりとして、商品の出荷から家畜の追跡まで、幅広い用途に使用されています。IoTを導入してRFIDデータを収集すれば、RFIDタグを付けた対象が関係するイベントを簡単に追跡できます。RFIDデータからのインサイトは、サプライチェーン全体、注文処理、在庫管理などの改善に役立ちます。

一方、BLEでは、特定の範囲内を移動する顧客との接点を深めると同時に、そこから収集したデータをカスタマーエクスペリエンスの最適化に役立てることができます。

ビジネスアナリティクス：RFIDタグを使用して在庫を追跡する場合でも、特定の範囲内を移動する顧客や従業員を把握する場合でも、RFIDやBLEに対応したデバイスで生成されるデータを新しい分析アプリケーションで分析することによって、実用的なビジネスインサイトをほぼリアルタイムで獲得できます。小売店は、買い物客の購買率が最も高い場所の周辺に在庫を陳列するなど、このデータをさまざまな方法で活用できます。

物理インフラのデータ

センサーデータ

ユースケース：セキュリティとコンプライアンス、IT運用、IoT、ビジネスアナリティクス

例:MQTT、AMQP、およびCoAPブローカーのスイッチ状態、温度、圧力、周波数、フローなどを示すバイナリ値や数値、HTTPイベントコレクター

産業機器やセンサーなどのデバイスは基本的にプロセッサーやネットワーク機能を搭載しており、稼働状態に関するさまざまな情報を記録、送信することが可能です。どのようなデバイスであっても、デバイスのデータには、パフォーマンスパラメーターやアノマリに関する新たな情報が詳しく記録されています。こうした情報は、デバイスが故障しかけているとか、他のシステムに起因する問題が発生しているといった、より大きな問題を示している可能性があります。複数のデバイスやサブシステムからデータを収集して関連付けを行うことで、デバイス、システム、工場、施設のパフォーマンスに関する全体像を把握できるのです。

ユースケース

セキュリティとコンプライアンス：センサーデータを使って、システムのパフォーマンスや、マシンや人を危険にさらす可能性のあるセットポイントを可視化することで、ミッションクリティカルな資産や産業システムをサイバーセキュリティの脅威から守ることができます。また、コンプライアンスレポートの要件に対応するためにセンサーデータを利用することも可能です。

IT運用：データセンターの運用チームが監視すべき最も重要なパラメーターとして、温度、湿度、通気、電圧調節といった環境条件が挙げられます。このような測定値は、サーバーやネットワークデバイスからも入手できます。これらのデータを関連付けることで、故障を招く可能性がある施設や設備の問題を明らかにできるのです。

その他のユースケース

予防的メンテナンスと資産ライフサイクル管理：センサーデータを利用すると、資産の配置、稼働率、リソースの使用量に関するインサイトを獲得できます。また、運用データを利用すれば、長期的な資産管理、メンテナンス、およびパフォーマンスに対してプロアクティブな取り組みを行うことが可能です。

監視と診断：センサーを監視することで、現場にあるデバイスやシステムの予定外の中断を監視、追跡して、意図したとおりにデバイスを動作させるといった取り組みが可能になります。また、このようなデータを利用することで、デバイスの障害の原因を把握して、効率性や可用性を向上させたり、デバイスの製造や配備で発生した異常や問題を特定したりできます。

物理インフラのデータ

サーバーログ

ユースケース：セキュリティとコンプライアンス、IT運用、アプリケーションデリバリー

サーバーのオペレーティングシステムは、運用、セキュリティ、エラー、およびデバッグに関するさまざまなデータを定期的に記録しています。これには、ブート時にロードされたシステムライブラリ、開始されたアプリケーションプロセス、ネットワーク接続、マウントされたファイルシステム、システムメモリの使用率などが含まれます。データの詳細度はシステム管理者が設定できますが、稼働中のシステムアクティビティの全体像を効率的に把握できるオプションも利用可能です。サブシステムでも、サーバーログがシステム、ネットワーク、ストレージ、およびセキュリティチームにとって役立つ場合があります。

ユースケース

セキュリティとコンプライアンス：サーバーログには、ローカルのファイアウォールなどのセキュリティサブシステム、ログインの試行、ファイルアクセスエラーのデータが記録されます。セキュリティチームは、これらのデータを利用して、侵入の形跡を見つけたり、システムに侵入した攻撃者を追跡したり、脆弱性を排除したりできます。ファイルアクセス、認証、アプリケーションの使用状況などのサーバーログは、インフラのコンポーネントを保護するのに有効です。

IT運用とアプリケーションデリバリー：サーバーログには、システム全体の健全性が詳しく記録されるだけでなく、エラーやアノマリの正確な発生日時に関するフォレンジック情報が記録されます。このような情報は、システムの問題の根本原因を見つけ出すのに欠かせません。

スマートメーター

ユースケース：IoT、ビジネスアナリティクス

例：ABB、GE、Google、eMeter、IBM、Itron、Schneider Electric、Siemens

スマートメーターは、電力の消費量、水の使用量、天然ガスの使用量を記録して、情報を継続的に処理および共有できるようにするための装置です。スマートメーターでは、通常、特定のタイプの計測器を調整するためのリアルタイムの双方向通信が可能です。

ユースケース

IoT：スマートメーターは、電力会社、ガス会社、水道会社などの大規模ユーティリティ企業の基幹システムに導入されます。これらのシステムは社会インフラの生命線であり、障害が発生すると壊滅的な被害をもたらす可能性があります。スマートメーターをリアルタイムで監視すれば、障害をリモートからより詳細に分析して、電線やガス管、水道管などの障害をリモートで検出できます。それと同じくらい重要なのが、悪質な攻撃やデータ漏えいにつながる可能性のある改ざんからデバイスを保護することです。

さらに、エネルギー会社や水道会社は、スマートセンサーを幅広く活用して、石油の備蓄量や水道水の品質など、あらゆる状態を追跡することもできます。

ビジネスアナリティクス：スマートメーターで収集されるデータは、幅広い業界で分析され、サービスの最適化に利用されています。たとえば現在、石油会社やガス会社では、作業員が検針のために実際に現場に行かなくても、燃料の消費量や残量をリアルタイムで把握できます。

スマートメーターは将来、最新の交通管制システムから、社会インフラを守るための防御システムまで、あらゆるシステムに利用されるでしょう。スマートメーターからのデータを集約すれば、ユーティリティ企業は需要に関する重要なインサイトを得ることができます。規制の厳しいユーティリティ企業は、デマンドレスポンス(DR)イベント時に適切なSLAを満たすことを求められます。スマートメーターのマシンデータを利用すれば、現在の対応状況を可視化できます。

ストレージ

ユースケース：IT運用

例：EMC、NetApp、IBM、Amazon EBS

データセンターのストレージは、主に2つの方法でプロビジョニングされます。1つは、ストレージをサーバーに組み込み、さまざまなネットワークストレージプロトコルを使用して共有する方法で、もう1つは、専用のストレージアレイを使用する方法です。後者の場合は、ストレージ容量が統合され、複数のアプリケーションが、専用のストレージエリアネットワーク(SAN)またはイーサネットLANファイル共有プロトコル経由でその容量を利用できるようになります。サーバーベースの内部ストレージでは、アクティビティがシステムログに記録されるのが普通です。一方、ストレージアレイでは、内部コントローラーやストレージプロセッサーがストレージ向けに最適化されたOSを実行し、運用、エラー、利用状況に関する膨大なデータをログに記録します。多くの組織は複数のアレイを利用しているため、ストレージ管理システムを利用してログを統合し、アクティビティと容量に関するレポートをまとめて作成できるようにしています。

ユースケース

IT運用：共有ストレージのログには、システム全体の健全性(ハードウェアとソフトウェアの両方を含む)、エラーの状態(コントローラー、ネットワークインターフェイス、ディスクの障害など)、および利用状況(各ボリュームが利用している容量と、ファイルまたはボリュームへのアクセス)が記録されます。これらの情報をまとめることで、運用チームは、問題の発生、追加容量のニーズ、パフォーマンスのボトルネックに関する警告を受け取れるようになります。

ユニファイドコミュニケーション

ユースケース：IT運用

例：Cisco Unified Communications Manager、ShoreTel、Twilio

リアルタイムのビジネスコミュニケーションに利用できるサービスは、従来の基本電話サービスによって提供される音声通話サービスだけではありません。今や、音声、ビデオ、テキストメッセージ、およびWeb会議の機能が、既存のエンタープライズネットワークでIPアプリケーションとして提供されています。ユニファイドコミュニケーションなどのコミュニケーションアプリケーションは、従来のクライアントサーバー型やWebアプリケーションとは異なり、サービスのネットワーク品質、レイテンシー、パケットロスに関する要件は厳格なものです。そのため、サービスの品質と信頼性は、ネットワークの状態やサーバーの応答時間の影響をはるかに受けやすくなっています。従来の基本電話サービスでは、電話をかければ発信音がすぐに鳴ることやノイズやエコーがないことが当然視されています。しかし、IPユニファイドコミュニケーションではこうした問題が起こる可能性があるため、システムインフラやサポートインフラを注意深く監視および管理し、品質と信頼性を確保する必要があるのです。

ユースケース

IT運用：VoIPと同じく、ユニファイドコミュニケーションのログには、システムの健全性の概要が表示されるとともに、トラブルシューティングや使用状況に関するデータが、他のネットワークアプリケーションと同じように表示されます。また、詳細情報として、音声/ビデオ通話、Web会議、およびテキストメッセージの発信元、発信先、時間、長さに加えて、通話品質に関するメトリクス(パケットロス、レイテンシー、音声品質/ビットレートなど)、エラーの状態、Web会議のユーザーの出席状況などが表示されます。発信元/発信先のアドレスに関するユニファイドコミュニケーションの記録を、ADやLDAPなどの従業員データベースやDHCPデータベースと統合することで、通話記録を実際のユーザー IDに関連付けたり、IPアドレスを実際の場所に関連付けたりできます。このような情報は、トラブルシューティングや請求処理に役立ちます。また、ログを使用して、輻輳やその他のパフォーマンスの問題が起こっているネットワークセグメントを見つけ出すこともできます。そうすれば、デバイスの問題やアップグレードの必要性を確認できます。

物理インフラのデータ

輸送

ユースケース：IoT、ビジネスアナリティクス

例：Boeing、BMW、Ford、GE、General Motors、Daimler-Benz、John Deere、Volkswagen

あらゆるサイズ、あらゆるタイプの乗り物が、日々大量のマシンデータを生成しています。これらのデータは、資産の健全性とパフォーマンスをリアルタイムで可視化し、予測的メンテナンスを行うために役立ちます。航空機メーカーや自動車メーカーは、これらのデータを利用して、「マニュアルどおり」ではなく、データに基づいてメンテナンスを実施できます。

さらに、そこから得た情報を活用して、可用性や信頼性の向上、利用頻度の低い車両の延命、摩耗しやすい部品の交換などに役立てることができます。

ユースケース

IoT：自動車メーカーは今日、使用するすべての機械と電子部品にセンサーを取り付けています。そのデータを利用することで、資産の状態を総合的に把握して、運用の問題をすばやく特定および診断し、計画外のダウンタイムを監視、追跡、回避できます。これは、機器が意図したとおりに動作していることを確認するためにも役立ちます。また、異常や正常動作からの逸脱を検出し、是正措置を講じることにより、アップタイム、資産の信頼性を向上させ、その耐用年数を延ばすこともできます。

ビジネスアナリティクス：マシンデータを分析することで、自動車メーカーはビジネスモデルの根本的な見直しが可能になります。今後は、自動車を販売するよりも、従量課金制でリースすることに重点を置くメーカーが増えるでしょう。車両の稼働率が上がれば、リースサービスによる収益も上がります。こうしたタイプのサービスで利益率を上げるには、収集したすべての集計データに高度な分析を適用することが重要です。

ウェアラブル

ユースケース：IoT、ビジネスアナリティクス

例：ARM、Intel、Lenovo、Microsoft、Samsung

健康管理機能を備えたスマートウォッチから、医師がバイタルデータをリモート監視できる医療機器まで、ウェアラブルデバイスは私たちの生活にすでに浸透しています。ウェアラブルデバイスは、私たちの最も身近にあるIoTの1つです。

ユースケース

IoT：最新のスマートウォッチは、単にスマートフォンと同期するだけでなく、アプリケーションを通じて位置情報システムとAPIを利用し、現在地と時刻に基づく最適なエクスペリエンスを提供します。

近い将来には、VR (仮想現実)ヘッドセットから最新式の組み込みセンサーまで、あらゆるものを活用してまったく新しい体験ができるウェアラブルデバイスが登場するでしょう。

ビジネスアナリティクス：ウェアラブルデバイスを介したデータ共有に抵抗を感じないユーザーが増えたことで、多くの人が分析のメリットを直接享受できるようになりました。ウェアラブルデバイス向けアプリケーションの開発者は、分析結果に基づいて、健康増進の方法から良いレストランまで、あらゆるお勧め情報を提供しています。ウェアラブルデバイスのデータ分析は、ユーザーエクスペリエンスの改善や画期的な製品の開発にも役立ちます。たとえば、ユーザーがデバイスをどのように使用しているかを分析して、より使いやすい機能を開発することができます。

物理インフラのデータ

Splunkについて

Splunkは、Data-to-Everythingプラットフォームを通じてデータを行動につなげます。Splunkのテクノロジーは、データをあらゆる規模で調査、監視、分析、活用することを目的に設計されています。すでに何百万人ものユーザーがSplunkをお使いです。無料版をぜひお試しください。

無料トライアル版

splunk>

20-13476-SPLK-Essential-Guide-to-Data-Infrastructure-Data-JA-202009