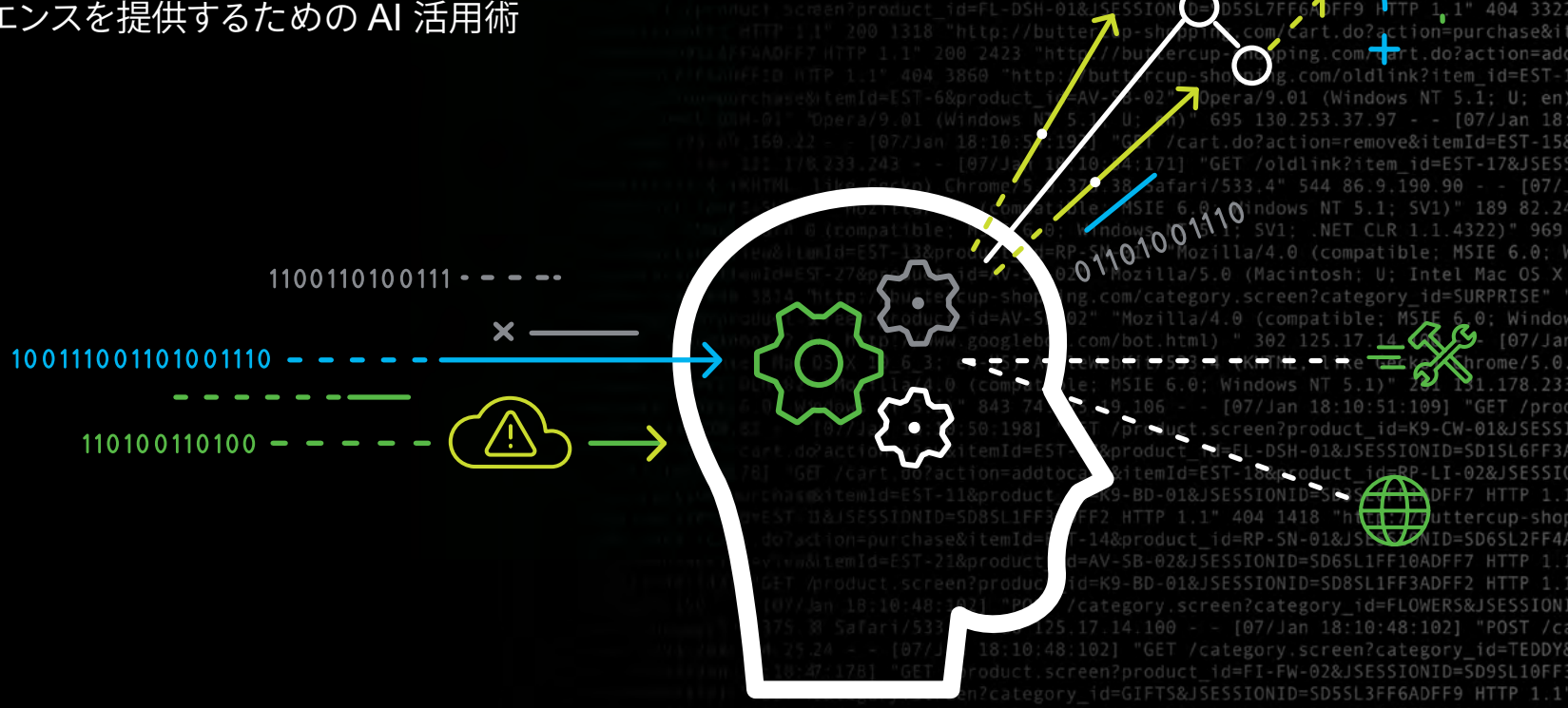
splunk>

Predictive IT:
予測技術を用いた IT 運用

よりよいカスタマーエクスペリエンスを提供するための AI 活用術



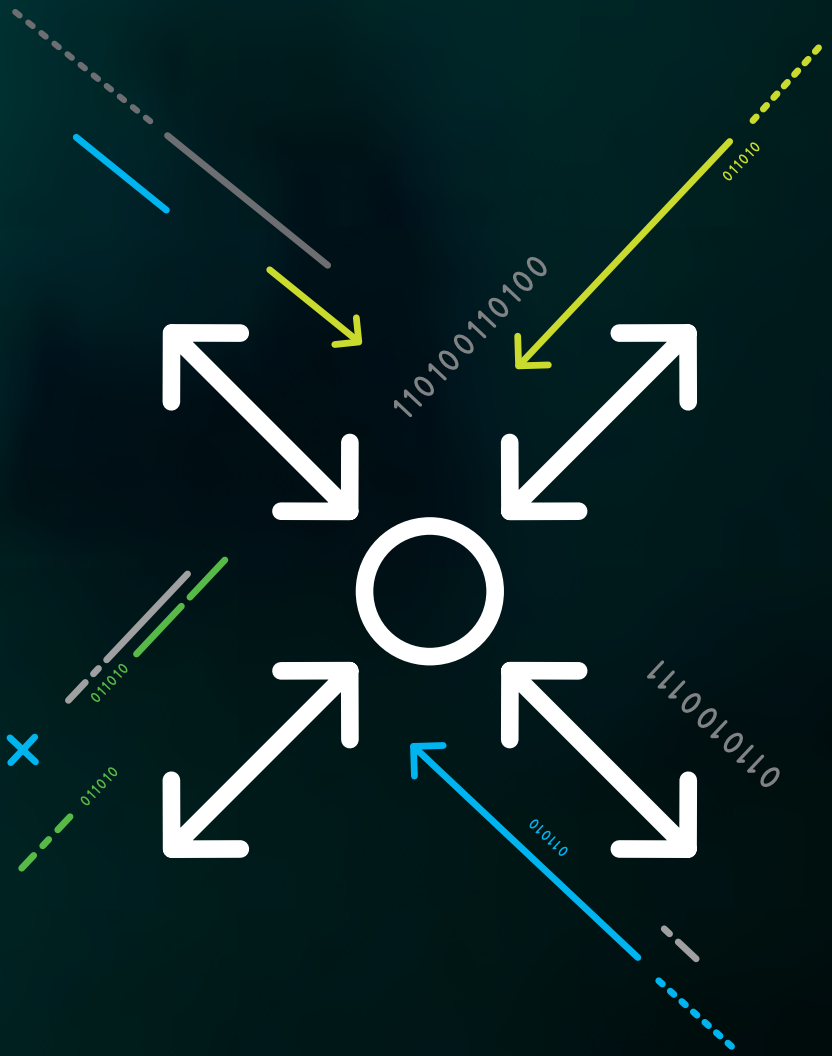
リアクティブな IT 運用は もはや時代遅れ

世界中のあらゆる業界で、IT 運用チームは複雑な問題に直面しています。大量のイベント、複雑に関連し合うサービス、サイロ化した組織、厳しい SLA への対応など、IT の運用管理を困難にしている要因を挙げたらきりがありません。しかも、システム障害、特にカスタマーエクスペリエンスに悪影響を及ぼす可能性がある障害の防止については、全ての組織が IT チームを頼りにしています。

すでに一歩進んでいる IT 部門は、こうした混沌とした状況を乗り越え、問題の原因を突き止めて迅速に解決しています。
それだけではありません。取り組みの早い IT 部門は、機械学習を利用して異常な行動を予測し、障害の発生前に対応しています。そのために活用しているのが、Splunk IT Service Intelligence (ITSI) です。

ITシステムの障害、運用 の課題をどのように予測、防止、そしてトラブルシューティングしているのでしょうか。各社の事例をご覧ください。

- → Leidos 社
- → ENGIE Global Markets 社
- → Micron Technology 社
- → Econocom 社
- → CenturyLink 社
- → TransUnion 社



イベント管理の向上：
LEIDOS 社の Splunk ITSI 活用事例

イベントノイズを 97% 削減

「20 年以上にわたって IT 管理に携わってきましたが、このように強力な製品は今までありませんでした。Splunk はあらゆるデータに対応し、すべてを同じ方法で検索できるため、今になって初めて、さまざまなテクノロジーから成る IT 環境全体を真の意味で監視できるようになりました」

- Leidos 社、パフォーマンス管理担当ディレクター、**Don Mahler 氏**

Leidos 社は Fortune 500 に名を連ねる科学技術ソリューションの大手企業であり、防衛、インテリジェンス、医療などの市場におけるグローバルな課題の解決に注力しています。一方で、顧客が同社のサービスを常時利用できる状態にしなければならないという課題を抱えていました。

課題

Leidos 社のパフォーマンス管理担当ディレクターである Don Mahler 氏は、以下のような課題に対応するため、関連する部署、IT 部門、組織内のサイロを一つにまとめ、120 以上の IT サービスで発生する大量のイベントをトリアージできるソリューションを必要としていました。

- → 顧客が 24 時間 365 日アクセスできるように監視および対応する
- → サイロ化による IT 部門の分断を解消する
- → 何千件ものアラートとイベントを削減する

ビジネスへの効果

同社では、種類の異なる IT 環境で発生するイベントを統合し、重複するアラートを検出して抑制し、解決済みのアラートを消去して対応すべきイベントのみを抽出するといった基本的な機能に加え、一定期間が経過した後に自動でアラートをあげる機能や、デバイスを意図的にオフラインにしたときはアラートを出さない機能なども必要としていました。Leidos 社は Splunk ITSI を使用してこれらのすべてを実現することができました。Mahler 氏は次のように述べています。「Splunk ITSI が膨大なイベントの優先順位付けを行ってくれます。アラート画面では問題が発生しているものだけでなく、影響を受けているものについても、インサイトを得ることができます」

また Mahler 氏によると、Splunk のプラットフォームを使用するもう 1 つの大きな利点は、チームがサービススタック全体のデータを共有できるようになり、サイロを崩すことができるということです。現在、Microsoft System Center Configuration Manager (SCCM) や SolarWinds ネットワーク管理ツールをはじめとする約 20 の管理システム、そして世界 240 拠点、120 の IT サービスに関連する 4,500 を超える構成アイテム (Configuration Items) のデータが Leidos 社の Splunk ITSI にフィードされています。その結果、ネットワークおよびデータセンターオペレーションで対応しなければならないアラート件数は 1 日あたり 3,500 ～ 5,000 件から約 50 件にまで減少しました。また、CMDB 情報を Splunk ITSI に渡すことで、スタッフごとに必要な範囲のアラートが表示されるようになりました。つまり、より関連性の高いデータに簡単にアクセスして、最も重要な問題に専念できるようになったのです。

Splunk の確実性

重要な販売アプリケーションのパフォーマンス

ENGIE Global Markets 社の事例

ビジネスに影響を与える問題を迅速に解決

「Splunk ITSI の機械学習を利用すると、各サーバーのパフォーマンスを測定するために、手動でしきい値を設定する必要がありません。予想されるパフォーマンスの差異を把握して動的に調整することが可能です。これにより、頻繁な設定や調整にかかる手間を省けるので、カスタマーエクスペリエンスに影響が及ぶ前に、実際のインシデントに優先順位を付けて対応することができます」

- ENGIE Global Markets 社、インフラストラクチャ部門の責任者

ENGIE グループの中核をなす ENGIE Global Markets (EGM) 社は、ガス、電力、エネルギーサービスを提供する世界的なエネルギー販売事業者です。同社は、クリティカルな販売アプリケーションの確実な稼働をリアルタイムで一元的に把握することによって、トラブルシューティングを迅速化し、パフォーマンスを確保する必要がありました。

課題

アプリケーションの確実な稼働は非常に重要であり、EGM 社の IT チームはその稼働状況を一元的なリアルタイムのビューで把握し、システムパフォーマンスに関する情報を迅速かつ簡単に関係者に提供する機能を必要としていました。しかし、分散したグリッドシステム上にアプリケーションが構築されているため、容易にはできていませんでした。同社は次のような課題にも直面していました。

- 重要な販売アプリケーションのパフォーマンスと可用性を確保する必要がある
- システムの健全な稼働状況を一元的かつリアルタイムに可視化する必要がある
- 分散グリッドシステムにより、自社開発ソリューションが複雑になり、パフォーマンスに影響を及ぼしている

ビジネスへの効果

Splunk プラットフォームを導入する前は、開発チームとインフラストラクチャチームはそれぞれ独自の監視ツールをそれぞれ使用しており、問題解決のために多くのやり取りをする必要がありました。Splunk ソフトウェアを使用することで、チーム間のコラボレーションを向上させることができ、インシデントの解決時間が短縮されました。

EGM 社では Splunk ITSI の導入により、IT スタック全体でのデータの相関付けが簡単になり、インシデント解決の効率性が改善されました。同社のインフラストラクチャ部門の責任者は次のように述べています。「問題が発生したとき、Splunk ITSI は素早く解決すべき箇所を示してくれます。Splunk ITSI の機械学習を利用すると、各サーバーのパフォーマンスを測定するために、手動でしきい値を設定する必要がありません。予想されるパフォーマンスの上昇と下降の差異を把握して動的に調整することが可能です。これにより、頻繁に監視システムのチューニングを行うコストを削減でき、カスタマーエクスペリエンスに影響が及ぶ前に、適確にインシデントの優先順位付けをして対応することができます」

分析主導型のアプローチで IT 運用を変革

Micron Technology 社の事例

ビジネスに影響を与える IT インシデントを **50%** 削減

IT 担当者が重大なインシデントを解決するまでの時間を **32%** 短縮

重大な IT インシデント数を **23%** 削減

「大きなインシデントが発生してしまった場合、最初に確認するのは Splunk ITSI です。「ITSI は問題の特定に役立ったのか」と常に振り返るようにしていますが、答えはいつも「イエス」です。その事からも私たちの監視用の KPI が正しく設定され、適切なサービスと関連性が定義されていることがわかります」

-Micron Technology 社、IT ディレクター、**Brian Best 氏**

最先端の半導体システムのグローバルリーダーであり、幅広いメモリソリューションポートフォリオを誇る Micron Technology 社は、優れたカスタマーエクスペリエンスの確保と競争力維持のために不可欠な高いサービス品質を追求しています。

課題

Micron 社の IT ディレクターである Brian Best 氏によると、これまで製造系 IT 部門では IT 運用を全社的に把握することができませんでした。業界での競争力を保持するため、Micron 社はサービス品質を維持し、IT 運用戦略を見直して以下の課題に対応する必要がありました。

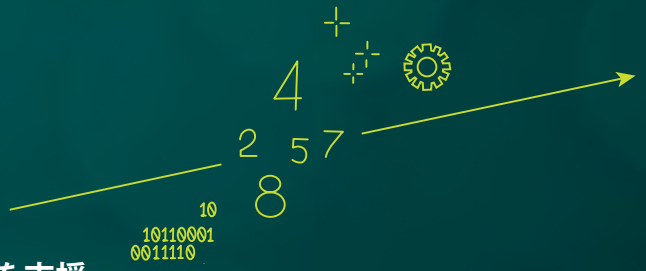
- → データのサイロ化のせいで、IT の問題を確実に特定、解決、防止することができない
- → IT 監視に関してリアクティブなアプローチをとっていると、事業上の重要なミッション (製造施設においてシステムの中断や予期しない影響を引き起こすことなく、確実に半導体の生産および出荷を行う) への障害影響を防止できない

ビジネスへの効果

今では、Micron Technology 社は、イベント管理、アラート生成、インシデント管理から変更管理に至るまで、すべてを Splunk ITSI で管理しています。このソリューションは、Micron 社が必要とするリアルタイムの可視化を実現するだけでなく、時間を節約し、IT インシデントがビジネスに与える影響を抑えるのにも役立っています。全体として、Splunk ITSI を使用することで同社はビジネスに影響を与える IT インシデントを 50% 以上削減し、解決までの平均所要時間を 32% 短縮し、重大な IT インシデントの件数を 23% 削減できました。Best 氏は次のように述べています。「ネットワークエンジニアに電話をしてネットワークが正常かどうか確認する必要がなくなりました。自分たちで確認できるようになったからです」

毎朝、Splunk ITSI データによって提供されるカスタムレポートに基づいて、Best 氏とそのチームは、過去 24 時間でアラートを出した KPI (通常はトップ 10) のレポートを受け取ります。一定量のアラートが発生している場合は、その KPI への対処をすぐに開始できます。Best 氏は、問題が発生した場合は、すべてのチームが参加して重要なことを見逃していないか確認することができると述べています。また、Splunk ITSI を使用することで製造系 IT チームは IT 環境の全体像を示すダッシュボードを簡単に作成できるようになりました。

econocom



イベント分析で ECONOCOM 社を支援

お客様により良いサービスを提供

「Splunk ITSI の統合された機械学習のおかげで処理するインベント数が減り、効率的な分析ワークフレームによってイベントの処理時間を平均で 8 分短縮できました。これは、SLA に照らすと 15% のパフォーマンス 向上となります」

-Econocom 社、インフラストラクチャ管理サービス、テクニカルディレクター、**Laurent Amouroux 氏**

SLA に照らしたパフォーマンスが 15% 向上

イベントの総数を 60% 削減

10 倍

システムパフォーマンスの問題が原因で発生したイベントの削減量

19 カ国に 1 万人の従業員を有し、25 億ユーロの収益をあげている Econocom 社は、企業向けのデジタルトランスフォーメーションソリューションの設計、費用対効果の監督を行っており、サービスに関連する厳格な SLA を満たすことが同社にとって非常に重要になります。

課題

Splunk を導入する以前、Econocom 社の IT 運用チームは約 12 種類の監視およびイベントコンソールを使用していました。しかも同社の IT 運用担当者には以下の能力が不足していました。

- 複数のデータソースを統合して分析を行い、インシデント調査を迅速化する
- ビジネスサービスのコンテキストに基づいてデータを視覚化し、適切な容量計画を行う
- 複数のサイロでイベントが発生した状態でも、SLA を適切に測定できる

ビジネスへの効果

同社はわずか数週間で Splunk ITSI の導入を完了し、現在は IT 部門内のさまざまなチームが使用しています。Splunk ITSI を使用することで、サイロ化したさまざまなソリューションのイベントをすべて単一のソリューションで一元管理できるようになりました。Splunk ITSI のイベント分析により、顧客のインフラストラクチャイベントに優先順位を付け、迅速に対応して、より良いサービスを提供することができます。また、イベント管理処理から誤検知と見なされるイベントを除外できるようになったので、イベントの総数が 60% 削減され、IT 運用担当者は本当に重要なイベントに注力できるようになりました。

その結果、システムパフォーマンスの問題によって発生したイベントの削減量が 10 倍になりました。Econocom 社のアプローチでは、Splunk ITSI の柔軟なしきい値を使用しています。これは統合された機械学習を利用して正常動作を学習するというものです。以前は、CPU が急上昇した場合、それが本当に問題を示しているかにかかわらず、しきい値を超えたとして問題と扱われていました。現在では、Splunk ITSI を使用することで、特定の状況下における正常な急上昇を見極めて、しきい値を超えたことだけでの問題発生を回避できるようになり、生成されるイベント数が削減されました。

CenturyLink

スイッチボードからダッシュボードまで

通信業界のリーダーが新しいソリューションを採用

平均特定時間 (MTTI) と 平均解決時間 (MTTR)を 大幅に短縮

「CenturyLink 社ではカスタマーエクスペリエンスに重点を置いています。Splunk を使用することで、エンドユーザーは常にサービスチームと満足のいくやり取りができるようになりました。Splunk Enterprise と Splunk IT Service Intelligence によって、アプリケーションの確実な稼働状況を経営幹部層向けにリアルタイムに可視化することができます。これにより、当社の担当者はお客様にいつでも重要な情報を提供できるようになりました」

- CenturyLink 社、システムエンジニアリンググループ、**Tim Kerrigan 氏**

1930 年に地方の電話会社として創業した CenturyLink 社は、全米および世界各地で個人と企業向けにブロードバンド、セキュリティ、IT サービス、クラウドサービスを提供する企業へと成長しました。

課題

買収の結果、CenturyLink 社は自社製および他社製のアプリケーションについてリアルタイムなサービス監視を行う必要が生じました。同社の各コールセンターでは買収後、システムのパフォーマンスだけではなく、問い合わせの混乱や、オーダーを完了または修正するまでの時間がかかるようになったことが課題になっていました。CenturyLink 社は以下のような課題も抱えていました。

- さまざまなサイロや古いアプリケーションからの情報を統合する必要がある
- IT 運用とビジネス運用を経営幹部レベルで可視化する必要がある
- コールセンターやその他の部門が部門内の問題を独力で評価せずに IT 部門に丸投げする

ビジネスへの効果

Splunk Enterprise を導入したことで、IT 部門に電話で問い合わせなくても、リアルタイムでダッシュボードを使用して他のセンターと比較しながらパフォーマンスを確認できるようになりました。システムエンジニアリンググループのマネージャーである Tim Kerrigan 氏は「障害切り分け作業に 30 ～ 50 の人員を投じる前に、手順の変更がなかったか自分たちで確認してもらうことができます」と語っています。CenturyLink 社では、すでにほぼすべての部門に Splunk Enterprise が導入され多くのユーザーが使用していましたが、最近 Splunk ITSI を追加したことで、エグゼクティブがレビューするための業績評価指標と詳細情報を収集できるようになりました。

現在のところ、Splunk ITSI の監視対象には、XenApp およびその他の Citrix デスクトップおよびサーバー製品、そして複数の外部アプリケーションと課金システムを連携させる重要な API が含まれます。2017 年の 1 カ月を前年の同じ月と比較すると、監視の改善により IT の機能停止、MTTI、および MTTR が減少しています。

TransUnion

TransUnion 社が
Splunk ソリューションに投資

エンタープライズ監視と機械学習

インシデントの根本原因調査が
数時間から数分に短縮され、
誤検知によるアラート数も減少

「顧客が直面するあらゆる状況を理解することは、ビジネスにとって重要なことです。例えば、トラフィック状況の異常を検知するとアラートが生成されます。このようなSplunk の機械学習機能を利用すれば早期の調査が可能となり、シームレスなカスタマーエクスペリエンスを実現できます」

- TransUnion 社 Splunk 開発 Lead、**Steve Koelpin 氏**

30 を超える国と地域でグローバルに事業を展開する TransUnion 社は、企業のリスク管理を支援する一方で、消費者が自らの信用情報や個人情報を管理する手助けも行っています。

課題

TransUnion 社は、一流金融機関を含む 10 億以上の消費者および企業顧客に対して、消費者レポート、リスクスコア、分析サービスなどを提供しています。TransUnion 社で監視と運用のシニアアーキテクトを務める Edward Bailey 氏は以下について改善方法を模索していました。

- → 外部の顧客トラフィックのパフォーマンス監視
- → 大量の顧客トランザクション

ビジネスへの貢献

TransUnion 社の Web サイトはトラフィックサイクルが変動しやすく、1 日または 1 週間の中でトランザクションが増える特定の時間帯があります。自動化と機械学習アルゴリズムを導入したことで、同社はこれらのトラフィックサイクルとトランザクションを監視する新しい方法を手に入れました。TransUnion 社は Splunk ITSI を使用して複数のアプリケーションから取り込まれたマシンデータの可視化と集約を行い、エンドツーエンドのトランザクションフローをモニタリングしています。Bailey 氏は次のように語ります。「Splunk ITSI を使用すると、各アプリの稼働状況を新しい方法で可視化できます。そのおかげで根本原因の特定にかかる時間を短縮し、問題を迅速に解決できました」

TransUnion 社のアナリストは最近、顧客である大手銀行のトラフィックにおけるトラブルシューティングを行なった際に Splunk ダッシュボードを活用しました。1 日の特定の時間帯に予想されるトラフィックの情報が蓄積されており、そのデータから外れたトラフィックは異常と見なされ、アラートが生成されました。Koelpin 氏は次のように述べています。「顧客が経験するあらゆるパターンを理解することは、ビジネスにとって重要なことです。トラフィック状況の異常を検知するとアラートが生成されます。Splunk の機械学習なら、早期の調査でシームレスなカスタマーエクスペリエンスを実現できます」

SPLUNK ITSI

Splunk ITSI は IT サービスやビジネスサービス全体の可視性を高める監視と分析のソリューションであり、AI (機械学習) を活用して、IT 環境へのアプローチをリアクティブなものから、予測的で予防的なアプローチに変えることができます。AI (機械学習) を使用することで、Splunk ITSI は障害が発生する前にサービスへの影響を予測し、イベントノイズを低減することができるため、ビジネスの俊敏性を高め、競争力を手に入れることが可能になります。

Splunk ITSI の体験版をご希望される場合は、オンラインサンドボックスにご登録ください。Splunk ITSI がイベント削減などの 課題の解決や、データからのビジネスインテリジェンスの抽出に役立つことが体験できます。

さまざま業界のお客様が Splunk ソフトウェアを利用し、ビジネス上のあらゆる課題に取り組んでいます。事例については、当社の Web サイトをご覧ください。

Splunk ITSI による予測と防止

→ **詳細はこちら**

splunk>

www.splunk.com/ja_jp

EB-Splunk-ITSI-V2-screen-JA-201908