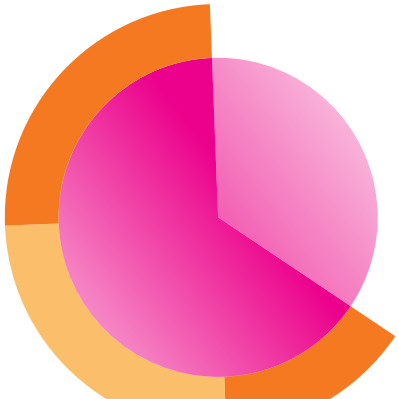
# セキュリティデータ
## エッセンシャルガイド

splunk>

# 時系列、ストリーミング、急増するデータ

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。しかし、サイバー犯罪者は時としてデータが石油よりも価値があることに気付いています。石油と同じように、データも精度を高め、商品化することで、高額な値段で販売できる可能性があるからです。セキュリティチームは、データの急増や組織内の境界の拡大のみならず、巧妙なサイバー攻撃の高まりにも対処しなければなりません。そのため、オンプレミス、ハイブリッド、マルチクラウドの環境全体にわたって、セキュリティインシデントを効果的に調査し対応するための、可視性とコンテキストに基づくインサイトが必要です。

実際、73%の組織が、分析ツールで他のデータソースを使用してセキュリティ分析を強化しています。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
- 不正行為を検出する、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の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、時間軸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。

# ハイブリッド環境に最適なデータプラットフォーム

## データの用途：

調査　監視　分析　実行

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成功への扉を開くことができません。

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

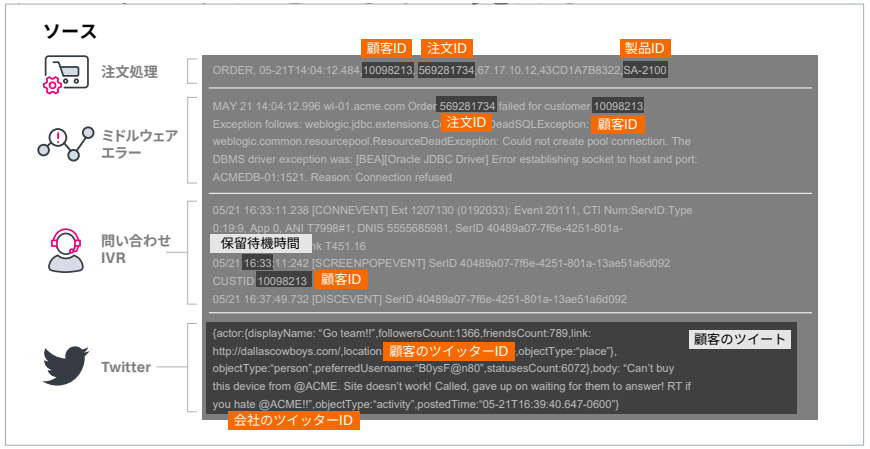



**図2:**データの価値は、この一見互いに関連性がないように見えるテキスト情報の中に眠っています。

**重要なインサイトを含むマシンデータ**

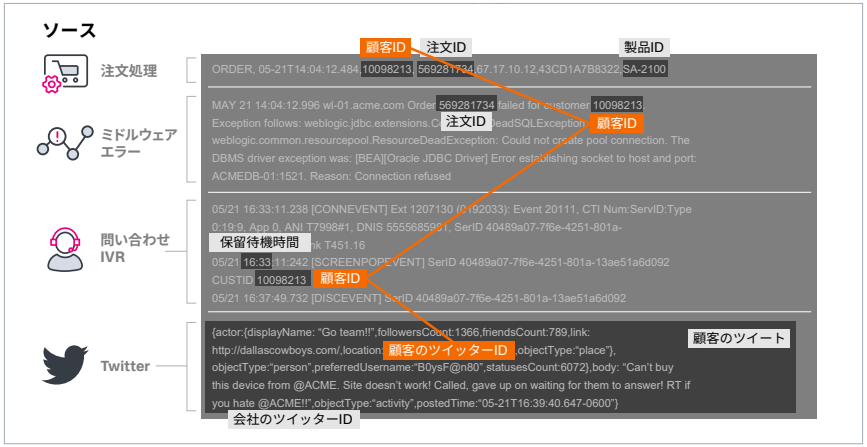



**図3：**多種多様なデータを相互に関連付けることで、インフラ状況について真のインサイトを獲得したり、セキュリティ脅威を発見したりできます。さらに、このインサイトを活用することで、より適切なビジネス意思決定を下せます。

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。

# セキュリティデータ

高度な脅威は持続性があり、マルウェアはネットワーク全体を容易に麻痺させ得るため、組織がサイバー攻撃に先んじるには、利用可能なすべてのリソースをもって立ち向かわなければなりません。しかし、セキュリティアナリストは絶え間なく届く大量のセキュリティアラートの対応で疲弊しています。毎日すべてのアラートに対処できないため、どうしても調査や対応に遅れが生じてしまいます。また、有能なセキュリティアナリストが世界規模で不足しており、SOCは人手不足に陥っている状況です。

あらゆることがデジタル化される世界で、こうした課題は増大する一方です。クラウド移行は複雑化し、ネットワークは4Gから5Gへの転換を迎え、コネクテッドデバイス数は800億台に及びます。また、自動化も私たちの生活に組み込まれつつあります。

データは、セキュリティに関する課題の解決に利用できる非常に重要なリソースでありながら、見過ごされていることが少なくありません。増え続けるデータは、最新のサイバー脅威に対抗するために積極的に活用することができるのです。

現在のトランスフォーメーションの力と、生成されているデータを有効に活用できれば、企業は効率性、収益性、イノベーションを向上させることができ、ひいてはセキュリティを強化できます。

このガイドでは、データを活用して最新のサイバー脅威から組織を守るとともに、IT運用、IoT、DevOps、ビジネスアナリティクスの課題に対応している3社の企業の事例をご紹介します。

**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**

# 目次

# Intel社：データインテリジェンスの革新によりセキュリティ態勢を刷新

### 業種

- テクノロジー

### Splunkのユースケース

- セキュリティ
- サイバーセキュリティインシデント対応管理
- セキュリティ監視
- アプリケーション監視

### 課題

- データ中心のビジネスモデルに転換するとデータの価値が高まる一方で脆弱性も大きくなる
- 従来型のSIEMが目的に合わなくなっている
- チーム間の連携に欠けデータが孤立してサイロ化したことでデータ分析の解釈に不整合が生じる

### ビジネス効果

- 情報セキュリティの管理と統制を変革
- 数日～数週間かかっていた高度な脅威の検出時間を数分～数時間に短縮
- サイバーセキュリティに対するコラボレーション型の統合的なアプローチを確立
- 社内InfoSecチーム共通のサイバーインテリジェンスプラットフォームを構築

### Splunk製品

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence (ITSI)
- VictorOps
- Splunk Mission Control

**“そこには可能性があります。可能性があるからこそ、私たちは時間と労力とリソースを投資しているのです。私たちはSplunkの成功を望んでいます。Splunkは弊社のミッション達成に欠かせないと考えています”**

**— Intel社最高情報セキュリティ責任者、Brent Conran氏**

## 概要

Intel社のテクノロジーが社会に与える影響と重要性は計り知れません。同社のエンジニアリング技術は、何十億ものデバイスをつなぐと同時にその安全性と利便性を確保し、すべてが有機的に結び付くスマート社会を実現するインフラを支えています。そして同じく計り知れない価値を持つのが、組織が最も厳重に保護する資産、セキュリティデータです。

Intel社のITチームは、Splunk®とApache Kafkaを基盤として、情報セキュリティに対するアプローチを一変させる新しいプラットフォーム「Cyber Intelligence Platform」を構築し、以下の成果を達成しました。

- データ分析を迅速化して、高度な脅威の検出と対応にかかる時間を短縮
- 言語と作業環境を統一してコラボレーションを促進
- ストリーム処理と機械学習ツールにより、セキュリティ運用やシステム健全性といった新しい領域にもビジネス価値を提供

## データドリブンへの転換

PC中心の企業だったIntel社は、データドリブンの組織へと変貌を遂げました。今日では革新的な方法で新製品を開発し、新しい市場に参入し、顧客と接しています。

「データがすべてです。すべてはデータに基づきます。データは弊社のビジネスに力を与えています。データはあらゆるものの原動力です」と、Intel社の最高情報セキュリティ責任者Brent Conran氏は言います。「データは従来型の産業もクラウド生まれの産業も変貌させています。データからインサイトを引き出せるかどうかが、ビジネスの勝敗を分けるのです」

よりデータに重きを置くデータ中心の組織へと移行するにあたり、同社のInfoSec、情報セキュリティチームは包括的な「多層防御」戦略を策定し、管理する必要がありました。さまざまなレベル(境界、ネットワーク、エンドポイント、アプリケーション、データ層など)で脅威防止/検出ツールを自動化し、その結果、社内環境で発生する脅威の99%に対処できるようになりました。

## 残り1%の捕獲

高度な脅威は発生頻度が高まるとともに巧妙さを増し続けています。Intel社が当時使用していた従来型のSIEMはもはや組織のニーズに合わなくなっていました。この従来型SIEMの操作を熟知しているのは一握りの担当者のみで、新しいタイプのデータに対応する必要が高まっていても、それに応じて拡張することもできませんでした。

同社のInfoSecチームは、社内環境に侵入しようとする高度な脅威を検出するため、「1%の捕獲」と呼ばれる戦略を策定しました。そしてこの戦略が、SplunkとApache Kafkaを含む最新テクノロジーを中心としたプラットフォーム「Cyber Intelligence Platform (CIP)」の開発につながりました。Intel® Xeon® Platinumプロセッサ、Intel 3D NAND SSD (ソリッドステートドライブ)、Intel® Optane™ SSDを搭載した高性能サーバーで構成されるCIPプラットフォームには、1日あたり12テラバイト以上のデータが取り込まれ、15ペタバイトに及ぶデータが保存されています。数百のソースから収集されたデータは、Kafkaメッセージバスを介してSplunkプラットフォームに送られ、そこでは1週間あたり130万回以上のサーチがユーザーによって実行されています。

InfoSecチームは、SplunkのData-to-Everything™プラットフォームと数百のサードパーティツールによって、データを豊富なコンテキストとともに可視化し、作業環境を統一して、チーム全体の生産性を向上させました。これにより、脅威を検出して対応するまでに、以前は数週間から数時間かかっていましたが、現在は数時間から数分にまで短縮されました。

## Cyber Intelligence Platformの拡張

Intel社では、CIPの導入により、データソースが増え、新しいユースケースが開拓され、多数の新しいデータモデルが作成されました。また導入後まもなく、脆弱性管理チーム、コンプライアンス・エンフォースメントチーム、リスク管理チームなどの他チームもCIPを使用するようになりました。その結果、インフラ需要が高まり、処理能力とストレージの増強が必要になりました。しかし、

**“1日あたり数十テラバイト、最終的には数百テラバイトのデータを処理し、数百人のユーザーがアドホックサーチやスケジュールサーチを実行し、データモデルを高速化して、機械学習モデルを作成できることを目標にCIPを構築しました。パフォーマンスを最大化するために、IntelのXeon Scalableプロセッサと Intel SSDを搭載したサーバーを用意して、処理能力とストレージを強化する必要がありました。『Intelの進化を安全に加速する』というミッションにおいては、秒単位の差が大きな違いを生みます”**

— Intel社セキュリティソリューションアーキテクト、Jac Noel氏

プラットフォームのパフォーマンスを最大化するには、同社のセキュリティソリューションアーキテクトとエンジニアが、SplunkプラットフォームとIntelテクノロジーについてもっと理解する必要がありました。

そこでSplunkとIntel社のチームは共同で、最新のIntel製品とテクノロジーを利用してCIPの処理能力、メモリー、ストレージを拡張するためのガイドとなるリファレンス構成を開発しました。現在、SplunkとIntel社はその成果を他のIT企業とも共有して、より多くの企業がSplunkとApache Kafkaによる基盤を拡張し、Rawデータを有用なインテリジェンスに変換して、運用、ビジネス、セキュリティに活用できるようにしています。

## 現在と将来の価値を創造

Intel社のInfoSecチームによるSplunkとKafkaの使用は拡大しています。アナリストとデータサイエンティストはストリーム内のデータに対し、変換や補強、結合、フィルタリング、操作を行っています。また、チームは機械学習ツールを追加して、インシデント対応から運用とシステムの健全性の確認、ワークフローオーケストレーションとアラートまで、あらゆる処理に活用しています。Intel社はSplunkと協力しながら、現在だけでなく将来にも役立つ価値を生み出し続けています。

「弊社の情報セキュリティはかつてない俊敏性を誇ります」とConran氏は言います。「私たちは最新のSplunkデータレイクを導入し、既存のツールをモダナイズしました。適切なデータの提供と従業員の再教育が相乗効果を生んでいます。そして機械学習を活用することにより、サイバーインテリジェンスは深みとスピードを増しています」

# NewYork-Presbyterian病院：Splunkでオピオイド危機に立ち向かう

### 業種

- ヘルスケア

### Splunkのユースケース

- セキュリティ

### 課題

- 違法と疑われる目的に医薬品が流用されていないかどうかを確認するために、電子カルテ、規制薬物の電子処方箋プラットフォーム、薬局の調剤システム、その他のソースからのデータを追跡する必要がある
- 電子PHIへのアクセスをリアルタイムで監視できないため、セキュリティと患者記録の保護に懸念が生じる

### ビジネス効果

- オピオイドや高額な医薬品(価格が1カ月あたり数万ドルに及ぶこともある抗がん剤など)の流用を防止
- ITセキュリティ運用を監視して、規制薬物やその他の医薬品が違法に使用または処方されていないことを確認
- 他の病院が同じ監視手法と流用対策を取り入れることのできる環境を整備

### データソース

- 監査ログ
- アプリケーションデータ
- EPIC
- Cerner
- Allscripts
- athenahealth

### Splunk製品

- Splunk Enterprise
- Splunk Enterprise Security (ES)

## 概要

NewYork-Presbyterian病院は、米国屈指の包括的かつ統合的な医療提供システムを誇る大学病院の1つとして、ニューヨーク都市圏の患者に、国内のみならず世界的にも最高レベルの医療と心のこもったケアを提供することに専心しています。その医学教育、画期的な研究、患者中心の革新的な臨床ケアは常に高く評価されています。

同院は、Splunkのテクノロジーを活用することで、規制薬物やその他の医薬品を厳重に管理するためのプラットフォームを構築し、最終的にその恩恵は院内にとどまらず、より大きなヘルスケアコミュニティに広まっています。SplunkによってNewYork-Presbyterian病院は以下の成果を実現しました。

- 患者記録へのアクセスを監査し、許可されたユーザーとデータを共有してインサイトを収集
- オピオイドやその他の規制薬物の流用防止に貢献
- HIPAA (医療保険の相互運用性と説明責任に関する法律)やその他の開示要件に準拠
- PHI (保護対象保健情報)データと患者のプライバシーを保護

## 患者のデータとプライバシーを守る

NewYork-Presbyterian病院では当初、フィッシング攻撃の防止、アカウントのセキュリティ強化、重要なセキュリティワークフローの自動化など、さまざまなセキュリティユースケースにSplunkを利用していました。「数カ月があっという間に過ぎた頃、私たちはSOC (セキュリティオペレーションセンター)の構築に取り掛かりました」と、同院でシニアバイスプレジデント兼最高情報セキュリティ責任者を務めるJennings Aske氏は説明します。「現在は6人のチームで、セキュリティ管理に必要なデータがすべて統合されているダッシュボードや画面を終日監視しています」

しかしそれは始まりに過ぎませんでした。「SOCを構築する過程で、患者のプライバシーに関するビジネス上の問題について考える必要があることに気付きました。特に、記録の不正閲覧や過度な閲覧、アクセスミスによる不必要な開示が起きないようにするためのプラットフォームが必要でした」とAske氏は続けます。「そこで私の提案により、Splunkに相談して、当院や他のSplunkユーザーのために、EPICなどの臨床システムと統合できるプライバシープラットフォームの構築を手助けしてもらうことにしました」

NewYork-Presbyterian病院とSplunkは協力してこの構想の実現に取り組み、患者記録への不適切なアクセスがあったときにプライバシー担当者に警告して、ただちに調査できるプラットフォームを開発しました。さらに、同院はすぐに、このプラットフォームの潜在能力が当初の想定をはるかに超えていることに気付きました。

## 世界規模でのオピオイドとの戦い

NewYork-Presbyterian病院はすぐに、患者記録プラットフォームを支えるSplunkの相関付けと機械学習機能が、米国を襲うオピオイド蔓延の重大な原因であるオピオイド流用を特定するためにも役立つ可能性があることに気付きました。

「オピオイド危機と病院の関係について考えた場合、実はオピオイドへの依存は一般人よりも病院の従業員の割合が高いのです」とAske氏は説明します。「CDCの統計を見ると、いくつかの時点で、市中に不正に出回る一部の薬物の主要な供給源が病院であることがわかります。ある年には、市中のオキシコドンの25%が病院からのものでした。ですから、手動の監査に頼るのではなく、潜在的な流用の防止に役立つプラットフォームを構築することは、病院側の倫理的および道徳的な義務だと思います」

このミッションを遂行するには、電子健康記録(EHR)、規制薬物の電子処方箋(EPCS)プラットフォーム、薬局の調剤システム、その他のソースからのデータを追跡して、医薬品の流用に関するインサイトを収集できる、投薬分析プラットフォームが必要です。たとえば、医師が病院の治療を受けていない患者に規制薬物を処方した場合や、特定の薬剤師が他の薬剤師よりも頻繁に自動調剤棚を使用している場合に、病院側にただちに警告するようなプラットフォームです。

**“Splunkを基盤にすれば、最終的に、全国の関係医療機関がこのプラットフォームを簡単に利用できるようになると考えました。Splunkは、U.S. Newsによる優れた病院ランキングの20位までに入るすべての病院で導入されていると言って差し支えないでしょう。この普及率は、このプラットフォームが医療と公衆衛生の改善に果たし得る役割の大きさを示しています”**

**— NewYork-Presbyterian病院シニアバイスプレジデント兼最高情報セキュリティ責任者、Jennings Aske氏**

「投薬分析プラットフォームについて考えると、自分または家族から親族を6人たどれば誰かしらがこの問題の影響を受けているという事実に思い当たります」とAske氏は言います。「歯茎の手術でオピオイドを処方され、結局使わなかったときのことも思い出します。私には小さい娘がいますが、娘がオピオイドを処方されたときは、それが正しい判断であり、薬が流用されることはないという確信を持てるようでいたいですね」

## 将来への期待

NewYork-Presbyterian病院は、心のこもったケアを世界中で提供しながら、医療事務での問題の迅速な検出や、却下された償還請求の詳細調査など、病院システムを改善するSplunkの新しいユースケースを模索しています。「Splunkプラットフォームでは、データを思いがけないかたちで活用できます」とAske氏は評価します。「保険請求に関する疑問など、Splunkから得られるインサイトを増やしていけば、数百万ドルを節約できる可能性もあります」

SplunkとNewYork-Presbyterian病院のパートナーシップについてAske氏は次のように総括します。「Splunkのおかげで院内のデータの活用方法が無限に広がっています。今後、Splunkの利用範囲をさらに広げて、このパートナーシップをより強化したいと考えています。それは、私たちだけでなく国内のすべての医療機関にとって有益です」

# 脅威インテリジェンスをセキュリティプレイブックに活用

## Recorded Future社の顧客がSplunkプラットフォームを選んだ理由

**業種**
- テクノロジー

**Splunkのユースケース**
- セキュリティ
- サイバーセキュリティ
- SOAR (セキュリティのオーケストレーションと自動化によるレスポンス)
- インシデント対応管理
- セキュリティ監視
- アプリケーション監視

**課題**
- 顧客が運用を手動で行っている
- 個々のクライアントに合わせてプロセスを再設計する必要がある

**ビジネス効果**
- 顧客側で脅威の検出時間が10%短縮
- 顧客側でイベントへの対応時間が63%短縮
- 全体的な効率が32%向上

**Splunk製品**
- Splunk SOAR
- Splunk Enterprise Security

**“自動化とオーケストレーションを取り入れなければ、企業が今日直面している課題に対処するのは難しいでしょう。課題はあまりにも多く、企業は圧倒されています。人間だけではもはや手に負えません”**

**— インテグレーション&戦略パートナーシップ担当VP、Seth Whitten氏**

世界6カ国、22の業種の約4万人のセキュリティ担当者が、Recorded Futureプラットフォームの最高レベルの脅威インテリジェンスを頼りにしています。Recorded Futureは、大量のデータを収集、分析し、そこから抽出したサイバー脅威インテリジェンスをリアルタイムで提供しています。顧客はこのインテリジェンスを活用して脅威の検出と対応の精度を向上させ、セキュリティチームの迅速な意思決定につなげています。

Seth Whitten氏は、Recorded Future社でインテグレーション&戦略パートナーシップ担当VPを務めます。同氏はSplunkとRecorded Future社のパートナーシップ、およびSplunk® SOARインテグレーションのインパクトについて次のように評価しています。「現時点で当社が最も大規模に統合しているのがSplunk® Enterpriseです。ですからSOARの導入は自然なことでした。SIEMツールで収集したイベントを有効活用したいと考えるお客様はたくさんいます」

## SOARが選ばれる理由

SOARの導入前は、Recorded Futureを利用する顧客は運用を手動で行っていました。「お客様は、自社環境で発生したアラートを調査したり問題をトリアージしたりする際に、当社のプラットフォームにアクセスして必要な情報を探し、次のステップに進むかどうかを判断する必要がありました」とSeth氏は説明します。

SOARを導入したことで、顧客はこれまで手動で行っていた定型的なセキュリティ運用タスクを自動化できるようになりました。SOARの自動化機能により、以前は解決に数分から数時間かかっていたセキュリティアラートを現在では数秒で解決できます。その結果、運用効率が向上し、セキュリティイベントの対応時間が大幅に短縮しました。

SOARについて特に気に入っているのはプレイブックの作成方法だとSeth氏は言います。「SOARでは、プロセスを再設計しなくても、お客様に適した事前定義済みのプレイブックを使って非常にすばやく対応できるので、現場での活用がとても簡単です」

## Recorded FutureとSOAR

SOARのプレイブックを使用すれば、顧客に応じてカスタマイズした再現可能なセキュリティワークフローを構築して、一連のセキュリティアクションをマシン並みのスピードで自動実行できます。たとえばプレイブックを使って、サンドボックス内でファイルを実行したり、エンドポイントセキュリティツールでデバイスを隔離したりするように指示できます。すぐに使える事前定義済みのプレイブックが100種類以上用意されているため、セキュリティ運用について再現可能かつ監査可能なプロセスをすばやく確立できます。

**“自然言語処理とAIを活用してデータを相関付け、お客様が問題解決に利用できるようにしています”**

**— インテグレーション&戦略パートナーシップ担当VP、Seth Whitten氏**

**“お客様はすべてのアラートに適切に対応したいと考えています。優先順位を判断し、適切な措置を講じて、成果を向上させたいのです。成果の向上につながるアクションを引き出せるデータを提供するために、SOARは最良の選択肢でした”**

**— インテグレーション&戦略パートナーシップ担当VP、Seth Whitten氏**

プレイブックから脅威インテリジェンスデータには、Recorded Futureとのインテグレーションを介してアクセスできます。Splunk® Enterprise Securityから、または新しいアーティファクトとして、SOARにアラートが送られると、プレイブックが呼び出され、Recorded Futureから取得したリスクスコアと関連コンテキストが自動的に追加されます。その後、プレイブックの意思決定ロジックにより、リスクのあるアラートであれば人間のアナリストにエスカレーションされ、そうでなければ無視されます。このように、SOARによってフローから誤検知を取り除くことができるため、人間のアナリストはより重要な問題への対応に時間を費やすことができます。

## 特に大きな3つのメリット

- 脅威の検出時間が10%短縮
- イベントへの対応時間が63%短縮
- 全体的な効率が32%向上

# 認証データ

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

**例とデータソース：**Active Directory、LDAP、アイデンティティ管理、シングルサインオン

認証データでは、ユーザーやアイデンティティに関するアクティビティを把握できます。一般的な認証データソースには以下のものがあります。

- **Active Directory：**組織内でユーザーとグループのアイデンティティ、セキュリティポリシー、コンテンツコントロールを定義するために使用される分散ディレクトリです。
- **LDAP：**IETF (Internet Engineering Task Force)が定めたオープン標準で、一般的にユーザー認証(ユーザー名とパスワード)に使用されます。柔軟なディレクトリ構造を持ち、フルネーム、電話番号、メールアドレス、住所、組織単位、ワークグループ、マネージャーなど、さまざまな情報を登録できます。
- **アイデンティティ管理：**デジタルリソースのユーザー (個人、IoTデバイス、システム、アプリケーション)を検証可能なオンラインIDと関連付けるためのシステムです。
- **シングルサインオン(SSO)：**単一のソースから複数のシステムに、検証および証明可能なアイデンティティを提供することで、統合的なアイデンティティ管理を実現するためのプロセスです。SSOを使用すると、ユーザー認証情報が単一のソースに紐付けられます。そのため、そのソースでユーザーの権限やアカウントの状態を変更すれば、そのユーザーがアクセスするすべてのアプリケーションやサービスに変更が反映されるため、セキュリティを大幅に強化できます。SSOは特に、多数のシステムにアクセスするシステム管理者やネットワーク管理者など、高いセキュリティ権限を持つユーザーを管理する場合に重要です。

## ユースケース

**セキュリティとコンプライアンス：**セキュリティについては、所定の時間内での複数のホストに対する複数回のログイン失敗や成功、所定の時間内での異なる場所からの操作、ブルートフォース攻撃など、ユーザーのアクティビティに関する幅広い情報が認証データから得られます。具体的には以下の情報を確認できます。

- Active Directoryドメインコントローラーのログには、特権アカウントのアクティビティや、リモートアクセスの詳細、新しいアカウントの作成、有効期限が切れたアカウントのアクティビティなど、ユーザーアカウントに関する情報が記録されます。
- LDAPのログには、システムにログインしたユーザーとその日時や場所、情報へのアクセス方法などが記録されます。
- アイデンティティ管理のデータには、ユーザー、グループ、職務(CEO、管理者、通常のユーザーなど)ごとにアクセス権限が示されます。このデータはアクセスに関する異常の検出に役立ちます。アクセスの異常は脅威につながる可能性があります。たとえば、セキュリティが低いネットワークデバイスにCEOがアクセスしたことや、ネットワーク管理者がCEOのアカウントにアクセスしたことを検出できます。

**IT運用とアプリケーションデリバリー：**認証データは、IT運用チームが認証の問題を解決するときに役立ちます。たとえば、アプリケーションサポートをログインと関連付けることで、ユーザーがアプリケーションに円滑にログインできているかどうかを確認できます。Active Directoryを使用している場合は、Active Directoryのトラブルシューティングや健全性の確認にログを使用できます。



ユーザーデータ

# ウイルス対策

**ユースケース：**セキュリティとコンプライアンス

**例：**Kaspersky、McAfee、Norton Security、F-Secure、Avira、Panda、Trend Micro

組織のセキュリティにおける最大の弱点は人です。ウイルス対策は、ユーザーが不注意で有害な操作をしてしまうのを防ぐ方法の1つです。ウイルス対策ソフトウェアを導入すれば、怪しいWebリンクを開く、悪質なソフトウェアをダウンロードする、マルウェアが仕込まれた文書を開く(何も知らない同僚から転送されることもよくあります)といった操作の多くを防止したり、その被害を緩和または回復したりできます。

一般に「APT」と呼ばれる高度な脅威の多くは、1台の感染したコンピューターを踏み台にして、そのコンピューターが接続する信頼できるネットワークに侵入します。ウイルス対策ソフトウェアでは、すべてではありませんが一般的な多くの攻撃手法を検知し、脅威が拡散する前に阻止できます。

## ユースケース

**セキュリティとコンプライアンス：**ウイルス対策ログは、マルウェアや、ホスト、ノートPC、サーバーの脆弱性を分析したり、不審なファイルパスを監視したりするために活用できます。また、以下の問題も特定できます。

- ファイルシステムやレジストリ内で新たに検出されたバイナリ、ファイルハッシュ、ファイル
- バイナリ、ハッシュ、レジストリが脅威インテリジェンスと合致した日時
- パッチ未適用のオペレーティングシステム
- 既知のマルウェアのシグネチャ

# メールサーバー

**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：**Exchange、Office 365

電子メールは多くの組織で今日でも主要なコミュニケーション方法として利用されています。そのため、メールサーバーのデータベースとログも非常に重要なビジネス記録です。メールデータは量が多く、しかも増え続けるため、その管理においては、データの保持期間とアーカイブに関するポリシーを定めて重要なデータのみを保持し、普段使用しないデータは低コストのストレージに移動するのが一般的です。

## ユースケース

**セキュリティとコンプライアンス：**メールサーバーデータは、悪質な添付ファイル、悪質なドメインへのリンクとリダイレクト、既知の悪質なドメインからのメール、未知のドメインからのメールを特定するために役立ちます。また、サイズが異常または過剰なメッセージや、不自然な時間帯のメール操作を検出することもできます。

**IT運用：**組織の情報セキュリティ、保持期間、規制コンプライアンスプロセスを確保するために、メールメッセージとアクティビティログが必要になることがあります。メールサーバーのトランザクションログとエラーログは、ITの問題を解決するために欠かせないデバッグツールであり、従量課金の計算にも使用できます。

# 脆弱性スキャン

**ユースケース：**セキュリティとコンプライアンス

**例：**ncircle IP360、Nessus

セキュリティホールを見付けるための効果的な方法は、攻撃者の視点でインフラを調査することです。脆弱性スキャンでは、組織のネットワークを綿密に調査して、外部の第三者からの侵入経路になり得るソフトウェアの既知の欠陥を検出できます。スキャンを実行すると、特定のシステムやネットワーク全体への侵入に悪用される可能性のあるオープンポートやIPアドレスに関するデータが生成されます。

システムでは、どのサーバーでも使われていないネットワークサービスがデフォルトで稼動していることがよくあります。稼動しているにもかかわらず監視対象になっていないサービスは、最新のセキュリティ更新プログラムが適用されていないOSを標的にするような外部からの攻撃で、踏み台として悪用されます。脆弱性スキャンを広範囲に実行すれば、内部ネットワーク全体への侵入に悪用される可能性のあるセキュリティホールを探り出すことができます。

## ユースケース

**セキュリティとコンプライアンス：**脆弱性スキャンを実行すると、特定のシステムやネットワーク全体への侵入に悪用される可能性のあるオープンポートやIPアドレスに関するデータが生成されます。このデータを調査して以下の問題を特定できます。

- セキュリティの脆弱性につながるシステム設定のミス
- パッチの未適用
- 不要なネットワークサービスポート
- ファイルシステム、ユーザー、アプリケーションの設定ミス
- システム設定の変更
- ユーザー、アプリケーション、ファイルシステムの権限の変更

アプリケーションデータ

# Webサーバー

**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

**例：**Java J2EE、Apache、アプリケーション使用ログ、IISログ、nginx

Webサーバーは、すべてのWebサイトのバックエンドとして機能し、クライアントのブラウザーに表示されるコンテンツを配信するアプリケーションです。静的なHTMLページを表示し、さまざまな言語で記述されたアプリケーションスクリプトを実行して、動的なコンテンツを生成したり、ミドルウェアなどのアプリケーションを呼び出したりします。

Webサーバーの種類は数多く存在しますが、一例として以下のような種類があります。

- **Java – J2EE：**Javaは、その汎用性、使いやすさ、開発者ツールエコシステムの充実度から、最も人気のあるプログラミング言語です。API、プロトコル、SDK、オブジェクトモジュールを提供するJ2EEプラットフォームを基盤として、Webアプレット、中間層のビジネスロジック、グラフィックフロントエンドなどのエンタープライズアプリケーションを実装するために広く使用されています。JavaはAndroidネイティブのモバイルアプリケーションの開発にも使用されます。

- **Apache：**Apacheは、インターネット上で最も古くから最もよく使用されているWebサーバーの1つで、何百万もの企業、政府機関、公共のWebサイトを支えています。Apacheでは、すべてのトランザクションの詳細な記録が保持されます。ブラウザーからWebページがリクエストされるたびに、日時、リモートIPアドレス、ブラウザーの種類、リクエストされたページなどの情報がログに記録されます。また、リクエストされたファイルが見つからない、アクセスしようとしているファイルに対する適切な権限がない、Apacheのプラグインモジュールに問題があるといったエラー状態も記録されます。Apacheのログは、Webアプリケーションや Webサーバーの問題の修正に不可欠です。また、トラフィック統計の生成、ユーザーの行動の追跡、不正侵入やDDoSなどのセキュリティ攻撃の検知にも利用できます。

- **アプリケーション使用ログ：**Apache Webログと同様に、アプリケーション使用ログを収集することで、開発者、ITチーム、セールス/マーケティングチームは重要な情報が得られます。測定の精度によっては、開発者がアプリケーションの使用状況を追跡することにより、使用頻度の高い機能と低い機能や、ユーザーが操作しづらい機能を判別して、将来の機能改善に活かすことができます。顧客向けアプリケーションの場合、セールス/マーケティングチームは、使用ログを利用して、オンラインやアプリケーション内の販売チャネルとプロモーションの有効性、セルスルーやカート放棄、クロスセールスプロモーションの可能性などに関するインサイトを得ることができます。

## ユースケース

**セキュリティとコンプライアンス：**Webログには、適切な権限のないファイルへのアクセス要求などのエラー状態が記録され、ユーザーアクティビティを追跡することで、不正侵入やDDoSなどのセキュリティ攻撃の兆候を察知できます。また、SQLインジェクションを特定したり、不正なトランザクションを相関付けたりする場合にも役立ちます。

- Javaアプリケーションはネットワークサービスや機密性の高いデータベースに頻繁にアクセスするため、セキュリティチームはログデータを調査することで、J2EEアプリケーションの完全性を確認し、アプリケーションの不審な動作や脆弱性を特定できます。
- Apache Webログを使用すれば、不正侵入、XSS、バッファオーバーフロー、DDoSなどのセキュリティ攻撃の兆候を検知して警告できます。
- Webログと同様に、一般的なアプリケーションの使用ログも、リソースの消費量が異常に多い、不自然な時間帯にアプリケーションを使用しているなど、不正アクセスを警告する場合に活用できます。

**IT運用とアプリケーションデリバリー：**Webログは、Webアプリケーションや Webサーバーの問題の修正に不可欠です。また、キャパシティプランニングに役立つトラフィック統計の生成にも使用できます。Webサーバーデータからは、IT運用に役立つ以下のような情報が得られます。

- 運用チームは、J2EEのデータを使用することで、Webサーバー、ミドルウェアサーバー、データベースサーバー間のやり取りを含む3層アプリケーションの問題を診断できます。
- Apache Webログでは、Webサービスのアクティビティ全般を把握できます。また、詳細を確認することで、インフラのボトルネックやダウンストリームの問題を特定できます。
- さらに、アプリケーション使用ログに記録されたリソース消費の詳細を利用して、インフラのキャパシティプランニング、最適化、負荷分散、従量課金の計算を行えます。



ミドルウェアデータ

# ファイアウォール

**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：**Palo Alto、Cisco、Check Point

ファイアウォールは、セキュリティポリシーの異なるゾーンを区切るために使用されます。ネットワークのいわば門番としてネットワークトラフィックの流れを制御する役割を果たすため、他の場所では収集できないような貴重なデータを収集できます。また、セキュリティポリシーを適用して、異常なプロトコルや許可されていないプロトコルを使用するアプリケーションの通信を阻止することもできます。

## ユースケース

**セキュリティとコンプライアンス：**ファイアウォールのログには、ネットワークセグメント間のトラフィックが詳細に記録されます。送信元と宛先のIPアドレス、ポート、プロトコルなどが含まれますが、いずれもセキュリティインシデントの調査には欠かせません。また、ログからセキュリティポリシーのギャップを特定し、ファイアウォールルールをより厳しく設定して、そのギャップを解消することもできます。ファイアウォールデータは以下の問題の検出に役立ちます。

- ラテラルムーブメント(横展開)
- C&C (コマンドアンドコントロール)のトラフィック
- DDoSのトラフィック
- 悪質なドメインのトラフィック
- 未知のドメインのトラフィック
- 未知の場所のトラフィック

**IT運用：**ネットワークアプリケーションで通信に問題があるときは、ネットワークセキュリティポリシーが原因である可能性があります。ファイアウォールデータを使ってブロックされているトラフィックと許可されているトラフィックを調査すると、アプリケーションの問題とネットワークの問題を切り分けることができます。

# IDS/IPS (侵入検知/防止システム)

**ユースケース：**セキュリティとコンプライアンス

**例：**Tipping Point、Juniper IDP、Netscreen Firewall、Juniper NSM IDP、Juniper NSM、Snort、McAfee IDS

IDSとIPSは、ファイアウォールを補助する、類似した機能を持つ相互補完的なセキュリティシステムです。IDSは、ファイアウォールを通過したネットワーク攻撃やサーバー攻撃を検知し、IPSは、高度な攻撃に対する防御を強化します。IDSは、一般的にネットワーク境界にあるファイアウォールのすぐ内側に配置しますが、組織によっては、すべての攻撃についてより幅広い情報を得るためにファイアウォールの外側に配置することもあります。IPSも、通常はネットワーク境界に配置しますが、ネットワーク内や個々のサーバーなど、他の階層に配置することもあります。IPSの機能は、一般的に、問題のあるパケットを破棄し、ネットワーク接続をリセットして、特定のIPアドレスやアドレス範囲をブラックリストに追加することです。

## ユースケース

**セキュリティとコンプライアンス：**IDSログには、セキュリティチームにとって有用な、攻撃に関する詳細が記録されます。タイプ、送信元、宛先、ポートなどの情報から、全体的な攻撃シグネチャを特定できます。特定のシグネチャについて、アラートを送信したり緩和策を実行したりすることもできます。IPSでは、同じ攻撃シグネチャデータを収集できるほか、不正なネットワークパケットの脅威分析を行ったり、ラテラルムーブメント(横展開)を検出することもできます。このデータから、C&C (コマンドアンドコントロール)のトラフィック、DDoSのトラフィック、悪質なドメインや未知のドメインのトラフィックを検出することもできます。

# NAC (ネットワークアクセスコントロール)

**ユースケース：**セキュリティとコンプライアンス

**例：**Aruba ClearPass、Cisco ACS

NAC (ネットワークアクセスまたはアドミッションコントロール)は、ローカルにインストールされたソフトウェアエージェントを使用して、保護されたネットワークへの接続を事前認証する、クライアント/エンドポイントセキュリティの一種です。NACでは、クライアントデバイスを調査して、既知のマルウェアに感染していないかどうかや、承認されたOSを使用して最新のパッチを適用するなどのセキュリティポリシーが守られているかどうかを検証します。NACの検証に合格しなかったクライアントは、検出された問題を修正するまで、隔離されたネットワークにしかアクセスできなくなります。

## ユースケース

**セキュリティとコンプライアンス：**NACソフトウェアでは、クライアントにインストールされているすべてのソフトウェア、セキュリティポリシーへの準拠状況、OSやアプリケーションのパッチのバージョン、リモートクライアントからのアクセスの可否、保護されたネットワークへのユーザーアクセスなど、接続するクライアントに関するデータが収集されます。セキュリティチームは、NACのログを調査することで、クライアントの状態とアクティビティを詳細に把握できます。ログには未許可のデバイス接続の詳細も記録され、そのユーザーまたはIPアドレスをネットワークの位置情報と関連付けることもできます。

# ネットワークスイッチ

**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：**イーサネットスイッチ、仮想スイッチ

スイッチは、ネットワークセグメント間をつなぎ、パケットが行き交う、いわばネットワークの交差点です。基本的には特定のIPサブネット内で機能し、レイヤー 3パケットのネットワーク間ルーティングはできません。最近のデータセンター設計では、エッジのサーバーやストレージアレイに接続するトップオブラック(ToR)スイッチと、ネットワークコアに接続するアグリゲーションスイッチ(スパインスイッチ)で構成される、2層のスイッチ階層が使用されます。一般に普及しているのはイーサネットスイッチですが、SAN (ストレージエリアネットワーク)やHPC (ハイパフォーマンスコンピューティング)の相互接続にファイバーチャネルまたはInfiniBandを使用している組織では、それに応じた独自のタイプのスイッチも使用されます。

## ユースケース

**セキュリティとコンプライアンス：**通常、スイッチデータはNetFlowレコードとして収集され、高度な脅威(APT)の検出、トラフィックフローの分析による異常なアクティビティの特定、データ漏えいの兆候の検知に欠かせない重要なデータソースです。スイッチの統計情報は有線レベルのデータソースであり、なりすましがほぼ不可能です。そのためセキュリティデータとしては重要なソースです。このデータを使用して、ユーザーまたはIPアドレスをネットワークの位置情報と関連付けることもできます。

**IT運用：**運用チームは、スイッチログを調査して、送信元と宛先、サービスのクラス、輻輳の原因などのトラフィックフローの状態を確認できます。ログにはトラフィックの統計も記録されるため、ポートごとの集計や、クライアントごとの集計、特定のポートで輻輳、障害、機能停止が生じていないかどうかを確認することもできます。

ネットワークデータ

# プロキシ

**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：**Blue Coat、Fortinet、Juniper IDP、Netscreen Firewall、Palo Alto Networks、Palo Alto Networks config、Palo Alto Networks system、Palo Alto Networks threat、Palo Alto Networks traffic、nginx

ネットワークプロキシは、Webアプリケーションのアクセラレーターやインテリジェントトラフィック制御、アプリケーションレベルのファイアウォール、コンテンツフィルターなど、ITインフラ内のさまざまな用途に使用されます。透過的(BITW)な仲介役として機能し、レイヤー 7のネットワークプロトコルスタック全体を認識するため、アプリケーション固有のトラフィックの管理やセキュリティポリシーを実装できます。

## 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にとっては、アプリケーション層のファイアウォールとして機能するプロキシが重要です。この場合、プロキシレコードを調査して、ネットワーク制御ポイントを通過するコンテンツの詳細を確認できます。たとえば、ファイル名、タイプ、送信元と宛先のほか、プロキシの実装方法に応じて、OS署名、アプリケーション、ユーザー名/IDなど、要求元クライアントに関するメタデータを取得できます。このデータは、C&C (コマンドアンドコントロール)のトラフィック、悪質なドメインのトラフィック、未知のドメインのトラフィックの検出にも役立ちます。

Webプロキシと一部の次世代ファイアウォールは、透過モードまたは明示モードでクライアントの代わりにHTTP(S)サーバーと通信します。この場合、いくつかの関連技術を使用すれば、要求と応答を調査し、ユーザーの役割、サイトやリソースのカテゴリ、攻撃インジケーターなどに基づいて通信を許可またはブロックできます。このイベントログに記録されるデータは相関関係の調査にも役立ちます。

**IT運用：**運用チームは、高度なレイヤー 7対応ロードバランサーであるアプリケーションデリバリーコントローラー (ADC)に組み込まれたプロキシを使用することがよくあります。この場合、プロキシログで、受信要求や、利用可能なリソース間でのトラフィック分散に関する情報を確認できます。

# システムログ

**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

**例：**Unix、Windows、Mac OS、Linux

どのOSでも、OS自体の動作状況やエラーが詳細に記録されます。これらのログにはタイムスタンプが付けられ、システムテレメトリとして基本的かつ信頼できるソースとして使用できます。OSによっては、定期的な情報更新、システムエラー、ブートローダーの記録、ログインの試行、デバッグ出力など、イベントのクラスごとにログが作成されることもあります。通常、エラーログには複数のサブシステム、OSサービス、デーモンからの記録が集約されるため、トラブルシューティングに欠かせません。

## ユースケース

**セキュリティとコンプライアンス：**システムログには、ログインの試行、ファイルアクセス、システムファイアウォールの動作など、セキュリティに関連するさまざまな情報が記録されます。これらの情報は、ネットワーク攻撃、セキュリティの脅威、ソフトウェア侵害の発生時のアラートに利用できます。また、セキュリティインシデントのフォレンジック分析にも非常に役立ちます。たとえば、システム設定の変更や、ユーザーまたは特権ユーザーが実行したコマンドを特定できます。

**IT運用とアプリケーションデリバリー：**多くの場合、OS、ハードウェア、各種のI/Oインターフェイスなど、システムの問題に対処するときに運用チームが最初に確認するのがシステムログです。1つの問題が複数のサブシステムのエラーにつながることが多いため、特定しづらいシステム障害の根本原因を究明するにはログエントリーを相関付けることが効果的です。

# 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、システムメモリー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、稼動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

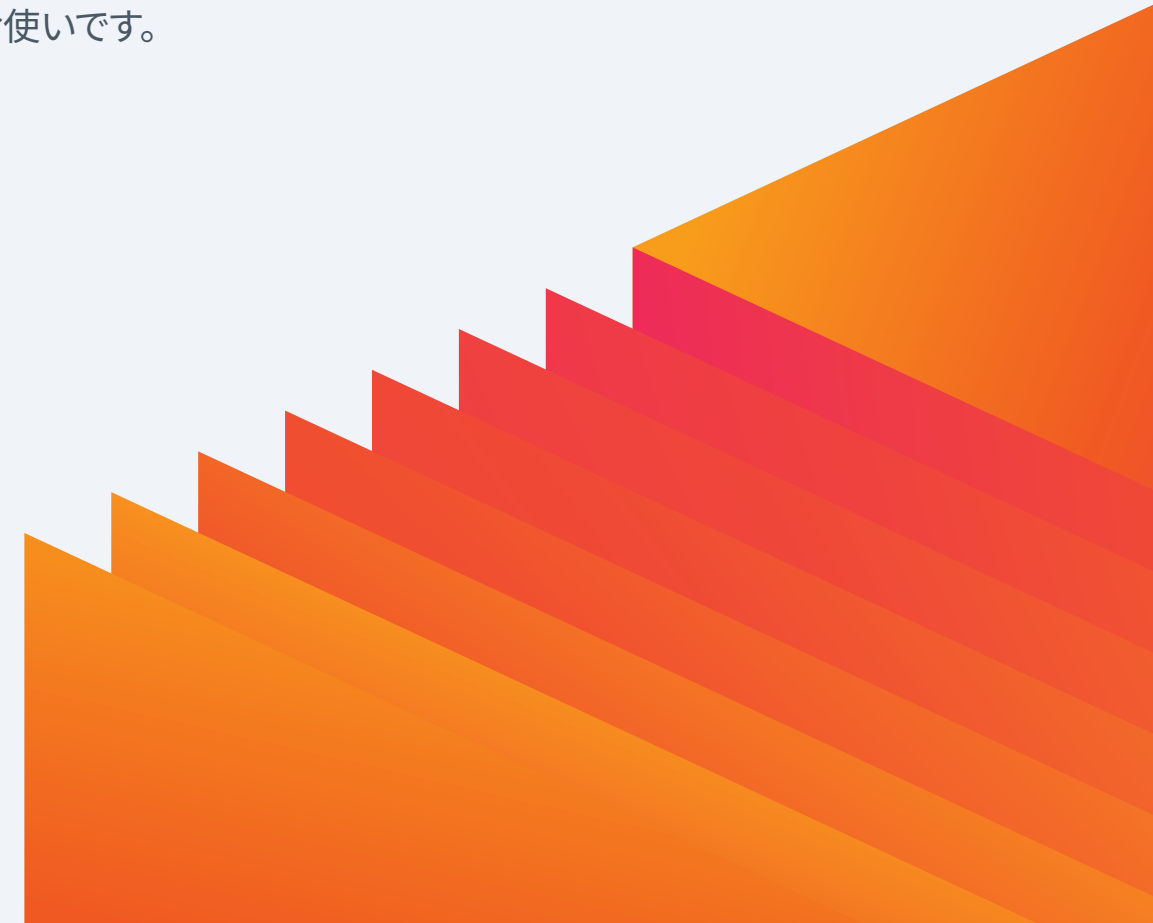
**セキュリティとコンプライアンス：**サーバーログには、ローカルのファイアウォールなどのセキュリティサブシステム、ログインの試行、ファイルアクセスエラーのデータが記録されます。セキュリティチームは、これらのデータを利用して、侵入の形跡を見付けたり、システムに侵入した攻撃者を追跡したり、脆弱性を排除したりできます。ファイルアクセス、認証、アプリケーションの使用状況などのサーバーログは、インフラのコンポーネントを保護するのに有効です。

**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。

# Splunkについて

Splunkは、セキュリティとオブザーバビリティの統合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、活用するため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>



23-251635-Splunk-theessentialguidetosecuritydata-EB-JA-202405