

ロンドン警視庁：データドリブンなガバナンスで信頼を構築

主な課題

ロンドン警視庁の新たな取り組み「Connect」で重大な課題が生じていました。それは、データの悪用を阻止して市民からの信頼を維持するために、組織全体でデータを監視、監査、統制することです。

主な成果

Splunkの導入により、ロンドン警視庁は組織内の不正行為をプロアクティブに特定して対処し、問題が深刻化する前に対応できるようになりました。説明責任と効率性を両立させたのです。



製品：保管時の暗号化、[Splunk Enterprise](#)、[プロフェッショナルサービス](#)、[サポート](#)

ソリューション：
[Splunk Cloud Platform](#)、
[Splunkプラットフォーム](#)

ロンドン警視庁は市民の安全を守るため、まず組織内部で説明責任を確立

グレーターロンドンの大部分を管轄するロンドン警視庁の活動は非常に大規模かつ複雑で、他の警察組織ではほとんど類を見ないほどです。地域の警備からテロ対策まで幅広い任務を担う同庁が首都ロンドンの安全を守るには、さまざまな専門分野、システム、チーム間のシームレスな連携が欠かせません。

ロンドン警視庁は2022年、Connectと呼ばれる大規模な取り組みを開始しました。これは断片化されたシステムを統合して犯罪データをより効率的に可視化するために立案されたものです。これによって犯罪通報の迅速化と連携強化の基盤を築きました。しかし、Connectによって新たなレベルの可視化が実現した一方で、大きな死角も生じるようになりました。あらゆる種類の機密データにオンラインでユーザーが簡単にアクセスできるようになったものの、同庁ではデータがどのように利用されているのかを効果的に監視、監査、統制する機能が不足していたのです。つまり、リスクは外部ではなく、内部に存在していました。機密情報への不適切なアクセスや誤ったアクセスなど、潜在的な不正行為が大規模に検出することは不可能な状況でした。

成果

- **298件：**ConnectでのICTの侵害を特定
- **4,768時間：**業務時間の削減
- **16時間短縮(平均)：**監査調査時間について手動との比較
- **8名の職員が解放され、**他の付加価値創出に従事

リアクティブな調査からプロアクティブな検出へ

ロンドン警視庁特有のリスク環境に対応するため、Splunkは内部脅威、コンプライアンス、データの悪用に対処できるよう設計されたカスタムソリューションを提供しました。正式な入札プロセスの結果、この製品は他の汎用的な各種ソリューションよりはるかに勝っていました。セキュリティツールとしてだけでなく、ロンドン警視庁が抱える重要課題に対処するのに役立つデータプラットフォームとして優れていたのです。

「顧客としての当庁のニーズにこれほど寄り添い、意欲的に連携してくれるテクノロジー企業に出会えたのは得難いことです」と、巡査部長のGraham Wenn氏は述べています。さらに、「Splunkによって得られるインサイトと確実性は、ロンドン警視庁の健全性を内部から保護するうえで欠かせないものです。複雑なデータを実用的なインテリジェンスに転換することで、倫理的な警察活動を支え、市民からの信頼の獲得をサポートしてくれるのです」と、警部のJake Ellis氏は付け加えます。

SplunkのインテリジェントデータプラットフォームとSplunk Cloudを基盤とするこのカスタムソリューションは、今やConnectの中核を担っています。これにより、ロンドン警視庁は膨大な運用データをほぼリアルタイムで獲得して分析し、対応に乗り出せるようになりました。組織内活動を監視する方法が、組織全体にわたって大きく変化したのです。

重要なのは、当初は調査ツールと考えられていたものが急速に成長して、包括的でプロアクティブなインテリジェンス機能になったことです。警察官や職員による機密システムの利用を一層詳細に監視できるようになったため、異常な動作や不適切な活動が発生した際に迅速な検出がしやすくなりました。また、極めて重要な点として、専門チームだけでなく、インサイトの創出や新たなユースケースの開発に関するトレーニングを受けた約150名の職員が、データにアクセスできるようになりました。

こうしたことはすべて、ロンドン警視庁がリアクティブな調査を脱却してプロアクティブなリアルタイム監視へと移行する原動力となりました。従来の調査は通常、通報を受けてから開始され、膨大な手作業が必要でした。しかし今では、以前よりもはるかに早く、かつ強い確信を持って不正アクセスやシステムの悪用を検出できるようになっています。

注目すべき成果を確保

最初の12カ月間でSplunkは、ConnectでのICTの侵害298件に加えて、その他のデータシステムで発生した149件の技術的侵害をロンドン警視庁が特定するのに貢献しました。

こうした監視体制の強化により、業務の効率は大幅に向上しています。かつては数日、あるいは数週間かかっていたプロセスを数分で完了できるようになりました。その結果、以前ならはるかに多くのリソースを必要としていた作業に、少人数で対応できます。1件の監査調査にかかる平均時間は、手動の場合と比べて16時間短縮されました。デジタルアナリストと警察官、合わせて8名の時間が解放され、付加価値の高い他の業務に注力できるようになりました。

Wenn氏は次のように説明します。「Splunkがなければ、データをこれほどの規模で処理することは不可能だったでしょう。毎日毎日、何十億行ものコードが生成されているのですから」

ロンドン警視庁は同時に、コンプライアンスとガバナンスに関する取り組みを強化しました。監視能力とデータ利用状況の可視化能力の向上は、規制要件への準拠だけでなく、内部基準の遵守にも役立ちます。「(Splunkは)単に業務遂行を支援してくれるアドオンというだけではありません。私たちの職務をより効果的に遂行できるよう、実際に変革しているのです」と、Wenn氏は述べています。

ここで重要なのは、Splunkのソリューションが非常に使いやすいものとして多忙な職員に受け入れられている点です。直感的なダッシュボードとワークフローのおかげで、あらゆるチームにすばやく導入でき、ほとんどのユーザーは30分もすれば活用できています。

最も重要なことは、こうした改善が、内部の説明責任と市民からの信頼を強化するのに役立っていることです。不正行為や汚職の兆候を早期に察知することにより、ロンドン警視庁はより迅速に対処が行えます。問題が深刻化する前に食い止め、透明性の向上を通じて信頼を強化できます。



これまでの手作業では、
内部脅威の監査に1週間
かかることもありました。
今では、ボタンをクリック
すれば10分で完了します。

ロンドン警視庁巡査部長、
デジタル搾取対策チーム(DET)
汚職・不正対策司令部、
Graham Wenn氏

警察活動インテリジェンスの新たな基準を確立

Splunkのソリューションによってすでに、ロンドン警視庁の警察活動戦略におけるテクノロジーの役割は高まっていますが、そこで止まっているわけではありません。

同庁は、Connectに統合するデータソースを増やして、より包括的な情報の全体像を把握できるようにすることで、データ収集と分析の能力をさらに引き上げる計画です。さらに、Wenn氏と担当チームは、AIドリブンの分析など最新のテクノロジーによってプロアクティブな脅威検出を促進する方法についても、検討を進めることにしています。

また、部門を超えた連携にも重点が置かれることになります。ロンドン警視庁は、歳入関税庁やBAE Systems社といった組織との緊密な連携を通じて、ベストプラクティスを共有しながら取り組みを加速しています。「私たちの取り組みは、公共部門と民間企業がどのように協力して正しい目標を達成できるのかを示す、実にすばらしい事例です」と、Wenn氏は述べています。

対象はさらに拡大し、同庁は英国の警察活動のより広範な変革に貢献するところです。英国内務省は、ロンドン警視庁とSplunkの提携に触発され、他のチームのモデルとして適用可能なデータ分析手法の検討を進めています。ロンドン警視庁は、変革につながる実証済みの運用フレームワークの提供を通じて、小規模な警察組織における高度なデジタル機能の迅速かつ効果的な導入を支援することになるでしょう。

Splunkで地域営業マネージャーを務めるLinda Walesは、最後にこう述べています。「ロンドン警視庁と協力して進めた取り組みは、素晴らしい成果を達成した一例です。データの透明性、プロアクティブなリスク管理、および市民からの信頼を獲得する強い意志をデジタルトランスフォーメーションの基盤としたときに、どんなことが実現できるのかを示しています」

Splunkを無料でダウンロードするか、[Splunk Cloudの無料トライアル](#)をお試ください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわらず、お客様のニーズに最適な導入モデルでご利用いただけます。



お問い合わせはこちら：
https://www.splunk.com/ja_jp/talk-to-sales.html

[www.splunk.com/ja_jp
jp_marketing_splunk@cisco.com](https://www.splunk.com/ja_jp/jp_marketing_splunk@cisco.com)