



**CISO, SOC, CSIRT及びセキュリティ担当者に！**  
**セキュリティ対策コストを圧倒的に削減！**



**他に類を見ない「ワイヤデータ」と最新のAI機能を**  
**駆使したリアルタイムセキュリティ解析・対策ソリューション！**



今後5年の間に、アベイラビリティ及びパフォーマンス管理のためのデータの最も重要なソースであることが証明されるのは、データを根本的に再考し、新しい方法で使用される **ワイヤデータ** である。

\*出典:Gartner、「将来の可用性とパフォーマンス管理への**ワイヤデータを重視したデータと分析中心のプロセスの使用**」  
Vivek BhallaとWill Cappelli, 2016年3月

既に10年以上にわたり、ワイヤデータ分析技術では業界トップの、**ExtraHop Networks社** (アメリカ、シアトル) が開発した最新のAIとMLテクノロジーを駆使した**“Reveal(x)”** は、これまでにない可視性能 / 高度な挙動解析 / 自動化調査によりインシデントレスポンスやセキュリティ対処に要する時間を圧倒的に削減します！

**Reveal(x)** は、従来のソリューションとは異なり、潜在的な問題に単にフラグを立てるのではなく、「発見・相関・調査」を自動化した「3-in-1ワークフロー」を用いてセキュリティオペレーションを加速化し、ExtraHop Networks社が誇る**ワイヤデータと最新のAI技術を駆使**して、重要資産に影響を及ぼす挙動をリアルタイム解析します。

### **旧来のソリューションでは不可能な、企業のリアルタイム可視性能！**

暗号化トラフィック、不正ノード、IoTデバイス、及びBYODシステムをネットワーク上で通信している瞬間に特定することによって、盲点を排除、ビジネスに影響を及ぼす前に環境内の問題や脅威を明らかにします。この状況インテリジェンスにより、ネットワークは、全てがリアルタイムで利用可能な、最も包括的で高忠実度のデータソースになります。

- エージェントやログが対処しないセグメントを含む、全ての接続されたデバイスを自動的に発見・分類
- データベース、AAAサーバ及びDNSサーバ、エグゼクティブラップトップ、R&Dシステムなどの重要資産に特に注意を払うことが容易
- 1つのイベントにおける、コンテキスト及び層間の依存性を含めた、トランザクションのL2~7データの完全なセットにアクセス
- 40以上のプロトコルを解析し、SSLやPFS (perfect forward secrecy) トラフィックを解読

### **「ワイヤデータに基づく全ての異常インシデント」に対する自動化調査ダッシュボード(業界初！)**

The screenshot shows the ExtraHop Reveal(x) dashboard interface. At the top, there are navigation tabs for Dashboards, Alerts, Detections, Metrics, Records, and Packets. A search bar and 'LAUNCH GUIDES' button are also visible. The main area displays a 'Timeline' view of detections. A filter is set to 'Any Source'. The 'Group by' is set to 'None', and 'Sort by' is 'Most Recent'. A 'Security Category' filter is set to 'Any'. The dashboard shows 15 detections found. A specific alert is highlighted: 'Data Exfiltration on AccountingLaptop' at 13:00. The alert description states: 'This device sent an unusually large amount of data to an external IP address. Investigate for a potential data exfiltration attack, where a compromised device transfers unauthorized information to an attacker. This device exfiltrated data to the following endpoint: 34.208.247.6 via SSH: 1.1GB'. A table below shows network metrics for 'AccountingLaptop', including 'External Bytes Out' at 1.11 GB, which is 111,078% above the expected range of 0 B-1 KB. Another alert is shown at 12:00: 'Suspicious CIFS Client File Share Access on AccountingLaptop', with a description: 'This device sent an excessive number of read requests over the Common Internet File System (CIFS) protocol. This anomaly indicates that the device might be compromised and is preparing files for data exfiltration.'

このデバイスから異常に大量のデータが外部のIPアドレスに送られました。侵害されたデバイスが(不正情報を攻撃者へ送る)データの窃盗攻撃の可能性がありますので調べてください。このデバイスは下記のエンドポイントへデータを窃盗しました。

経理のLapTop からデータの窃盗がありました！

データの窃盗

経理のLapTop に疑わしいCIFS Client File Share

このデバイスはCIFS (Common Internet File System) プロトコルで過剰なReadリクエストを送りました。通常、これはそのデバイスが侵害されている可能性を示し、データの窃盗のためファイルの準備をしていることを示します。

詳細資料は右記よりお問い合わせ下さい

**資料請求**

コーネットソリューションズ株式会社  
Cornet Solutions (TEL) 03-5817-3655 (代)  
www.cornet-solutions.co.jp