



**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！**



**Reveal(x)**

**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 사용되는 **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, Anomalies, and Metrics. A search bar is present on the right. The main area displays a 'Timeline' chart showing 7 anomalies found between 12:00 and 17:00. Below the chart, a list of anomalies is shown, including 'Data Exfiltration on AccountingLaptop (10.10.5.121)' and 'Suspicious CIFS Client File Share Access on AccountingLaptop (10.10.5.121)'. Callout boxes provide detailed information about these anomalies, such as the amount of data exfiltrated and the specific endpoints involved.

**1月16日16:00**  
**データの窃盗**  
 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。

**1月16日16:00**  
**Data Exfiltration on AccountingLaptop (10.10.5.121)**  
 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:  
 • ec2-51-213-121-46.us-west-2.compute.amazonaws.com (51.213.121.46) via SSH: 1.3GB

経理のLapTop (10.10.5.121)からデータの窃盗がありました！

**1月16日15:00**  
**Suspicious CIFS Client File Share Access on AccountingLaptop (10.10.5.121)**  
 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**

日本コーネット・テクノロジー株式会社  
**CORNET (TEL) 03-5817-3655 (代)**  
 TECHNOLOGY www.nihon-cornet.co.jp