

# Arbor Sightline with Insight

ビッグデータを瞬時に解析し、より速いネットワーク分析を行うとともに、ビジネス上の意思決定をスマートに

## 主な機能と特長

### 既存のArbor Sightlineプラットフォームを拡張/強化

Arbor Sightlineの価値が拡張、強化され、解析済みのフローの生データを高品質のまま長期間保管したり、多次元のビジュアル解析を実行したりすることが可能になります。

### ビッグデータレイクからネットワークトラフィックの正確なメモリーを取得

顧客が必要とする限り、ネットワーク上のあらゆるフローの生データは、カスタマイズされた解析データおよびメタデータと共に保管され、リアルタイムまたは過去の非構造化解析に用いられます。

### 単一のUIから素早く解析を実行

複雑なクエリーや普段の調査の状況が、単一のUIからグラフィック形式または表形式で視覚化されます。

### 高度なフォレンジック調査が可能に

複数の画面やいくつかのレポート処理に振り回されることなく、比較的短い時間で過去データを自由かつ直感的に閲覧できるので、攻撃や標的、痕跡について把握できる情報が増加します。

### フィルターボックスの新設計

ネットワークトラフィックにおける関連性の傾向が把握しやすくなりました。表示フィルターを通じて、関連性の高い複数の側面の組み合わせや、側面毎の高いバリューを表示することができます。

Arbor Sightline with Insightは、ネットワーク可視化プラットフォームとして業界をリードするArbor Sightlineをベースとするプロダクトです。Sightline with Insightのビッグデータ機能は、情報を付加されたNetflowを蓄積する事で、ネットワークトラフィックデータを正確に保存することができます。また、新たなビジュアル解析ツールにより、スマートかつ迅速にネットワークを調査しやすくなります。さらに、Arbor Sightline独自のフロー解析やその他の豊富な機能を活用し、ネットワークポロジ、顧客、およびトラフィックパターンを前述のビッグデータとマッチングさせ、さらに無制限のフィルタリングで生データおよび加工データの多次元検索を素早く実行できるようになります。加えて、長期にわたるきめ細かなデータメンテナンス、過去に遡っての詳細なドリルダウン、グラフから数値データへと表示形式を簡単に変換できるピボットなどの優れた機能も用意されています。

### 視認性を深め、瞬時に明確な状況の把握を実現

Arbor Sightline with Insightでは、Arbor Sightlineとビッグデータ技術を基盤として、ネットワークトラフィックアクティビティの正確な保管が可能です。これにより、詳細かつ広範囲な解析や、アドホックなレポートの新規作成が可能です。生データおよび加工データの多次元検索を素早く実行し、さらに解析結果やメタデータも活用することで、全体像と詳細の両面から把握できるようになります。ビッグデータの高速解析により、状況を素早く洞察し、ビジネス上の意思決定をスマートに行うことが可能です。

### 考える速さで調査が可能に

Arbor Sightline独自のフロー解析とその他の豊富な機能を活用し、ネットワークポロジ、顧客、およびトラフィックパターンを前述のメモリーとマッチングさせることで、コンテキストが生成されます。これによって、対象のイベントおよび期間を保持しながら、無制限のフィルタリングで生データおよび加工データの多次元検索を素早く実行できます。また、長期にわたるきめ細かなデータメンテナンス、過去に遡っての詳細なドリルダウン、グラフィックから表へと表示形式を簡単に変換できるピボットなどの機能も使用可能です。

### Arbor Sightlineプラットフォームの運用価値を拡張/強化

Arbor Sightlineの価値が拡張、強化され、解析済みのフローの生データを高品質のまま長期間保管したり、多次元のビジュアル解析を実行したりすることが可能になります。ネットワークトラフィックの状況を把握すれば、ビジネスの発展につながったり、ネットワークのアップタイムを維持するための高度なフォレンジック調査を実行したりすることができます。このように、Arbor Sightline with Insightは既存のArbor Sightlineプラットフォームの機能を拡張し、強化します。

### ネットワークの拡大に伴い、Arbor Sightline with Insightは不可欠に

データセンターや大規模ネットワークの運用者は、ネットワーク全体の視認性や、DDoS攻撃の検知、トラフィックエンジニアリング、高度なピアリング/トランジット分析のために、Arbor Sightlineプラットフォームを採用しています。ピーク時のサービスパフォーマンスや可用性の維持、ネットワーク容量のインテリジェントの拡大、運用コストの把握、新たなサービス機会の発見が、Arbor Sightlineによってすべて容易になることがその理由です。そのようなArbor Sightlineの機能をさらに拡張、強化するのがArbor Sightline with Insightです。

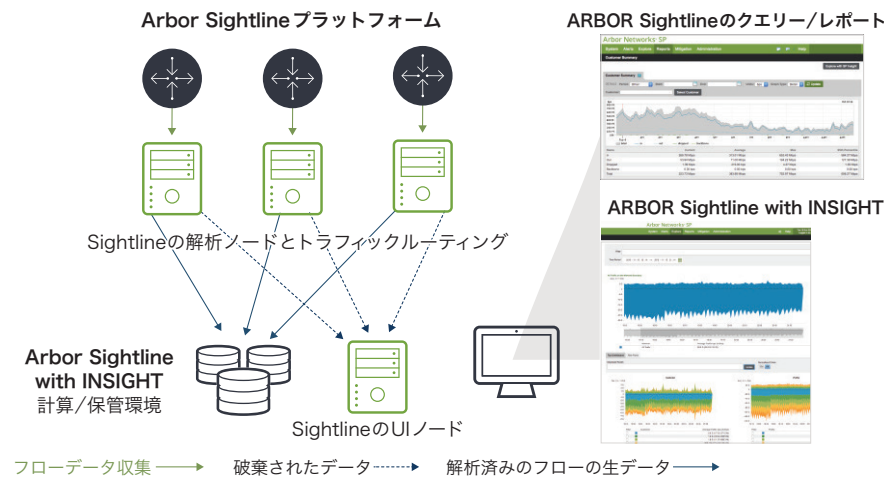
## Arbor SightlineとArbor Sightline with Insightの機能比較

Arbor Sightline with Insightは、Arbor Sightlineの機能とワークフローを強化するために設計されました。ネットワーク運用者が両者を併用すれば、ネットワークの視認性が一層高まり、破棄されたデータや解析済みのフローの生データに対して、多次元のビジュアル解析を素早く実行できます。

	レポート	フィルタリング	Accessing Data
<b>Arbor Sightline</b>	<ul style="list-style-type: none"> <li>体系的ワークフロー</li> <li>事前に設定済み</li> <li>2個のフィルターの組み合わせ</li> </ul>	<ul style="list-style-type: none"> <li>最大2個</li> <li>組み合わせはレポートの形式に依存</li> <li>体系的調査</li> </ul>	<ul style="list-style-type: none"> <li>破棄されたデータ (MOに依存)</li> <li>高速クエリー、高速検出</li> </ul>
<b>Arbor Sightline with Insight</b>	<ul style="list-style-type: none"> <li>アドホック、インタラクティブ</li> <li>フィルターの組み合わせが無制限</li> </ul>	<ul style="list-style-type: none"> <li>フィルター表示が無制限</li> <li>時間範囲指定の表示が無制限</li> <li>直感的な組み合わせが可能</li> </ul>	<ul style="list-style-type: none"> <li>ユーザーの保管ニーズに依存</li> <li>詳細クエリー</li> <li>フローの生データ</li> </ul>

## Arbor Sightline with InsightでArbor Sightlineはビッグデータレイクへと変貌

Arbor Sightline with Insightは、Arbor Sightlineプラットフォームに対するアドオンとして導入します。ネットワーク上のあらゆるフローの生データは、Arbor Sightlineからの解析データおよびメタデータと共にお客様の用意したストレージに送信され、リアルタイムまたは過去の高度な非構造化ビジュアル解析に用いられます。



### システム要件

- Arbor Sightline v8.1 (FLEXライセンスが必要)
- Arbor Sightline with Insightは、Arbor Sightlineの拡張ソフトウェアオプションです。外部データベース用の計算/保管インフラストラクチャは、お客様にご用意いただく必要があります。
- 計算/保管に必要なハードウェア環境の規模は、以下の条件によって異なります。
  - ネットワークのフローレート
  - 必要となる過去のフローデータの保管量
  - 必要となるクエリーの回数および量

**NETSCOUT**

### 米国本社

NETSCOUT Systems, Inc.  
Westford, MA 01886-4105  
TEL : +1 978-614-4000  
www.netscout.com

### アーバーネットワークス株式会社

101-0063 東京都千代田区神田淡路町2-105  
ワテラスアネックス13階  
TEL : 03-3525-8040  
EMAIL : japan@arbor.net  
WEB : jp.arbornetworks.com

NETSCOUTは、世界32カ国以上の国々で製品、サポート、サービスを提供しています。各国の事業拠点所在地、電話番号などのお問い合わせ先は、NETSCOUTのWebサイトでご参照ください。  
www.netscout.com/company/contact-us

## 主な機能と特長(続き)

### 側面の関連性のビジュアル解析

構造化されていない、破棄されたデータおよび解析済みのフローの生データを自由に時間範囲を設定して調査し、高トラフィックの側面のクエリーについてサンキーダイアグラムで見やすく表示することができます。

### トラフィックの計算

トラフィックは、期間を設定して調べることができます。最後に記録されたトラフィックに関する期間のトラフィック、全トラフィックの平均値、全トラフィックの最大値、および全トラフィックの95パーセンタイルを確認できます。

## Arbor Sightline with Insightのメリット

- Arbor Sightline with Insightでは、ビッグデータ技術を基盤として、ネットワークトラフィックアクティビティの正確なメモリーを作成できます。これにより、詳細で広範なトラフィックの解析が可能です。
- Arbor Sightline独自のフロー解析および豊富な機能(管理対象オブジェクト)を活用し、ネットワークポロジ、顧客、およびトラフィックパターンを前述のメモリーとマッチングさせることで、Arbor Sightline with Insightでコンテキストが生成されます。
- Arbor Sightline with Insightでは、ネットワークの視認性が強化され、DDoS攻撃に対するフォレンジックなユースケースも高度化します。そのため、サービスの可用性の確保や、運用コストの削減、新たなサービス機会の発見につながります。