Ennetix

AI-Powered User Performance Analytics

アプリケーション・インフラの性能分析　――　ＡＩＯＰＳ

１．課題

今日、 パブリック・クラウド、データセンター、バーチャリゼーション、ＳＤＮ，多種多様のセキュリティの普及に伴い、アプリケーション・インフラは急速に変わってきています。 その結果、アプリケーション利用時の応答性能や品質の分析は、分散型ネットワークサービスやハイブリッドクラウド、さらにはマルチクラウドに展開される第三者のサービスに依存して複雑化しています。

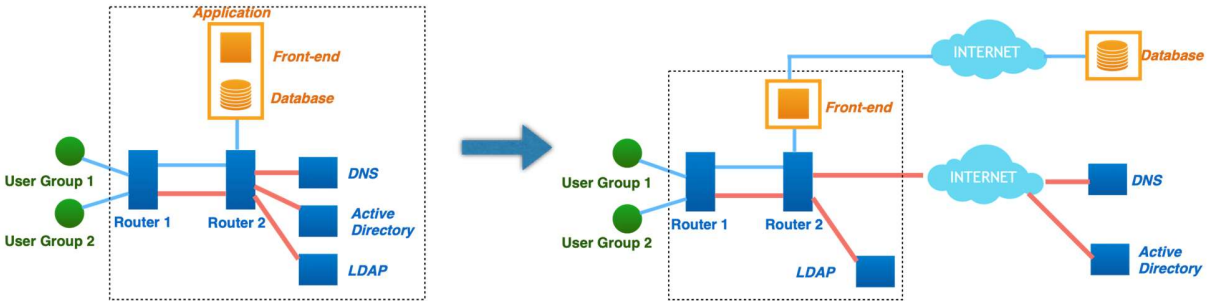


図１：オンプレミス（左）からクラウド（右）へのアプリケーション・アクセス・インフラの変遷

図１に示すように、クラウド時代には、多くのアプリケーションコンポーネントがクラウドでホスティングされたり、データセンタに置かれたアプリケーションを利用するケースが主流を占めるようになってきています。 そして、アプリケーションデリバリーをサポートするネットワーク機能（DNS、Active Directory、LDAP など）もデータセンタに移行されています。 また、アプリケーションを利用するクライアントも本社、支社、支店など地理的に分散しています。それらのクライアントがアプリケーションを利用するとき、そのパフォーマンスは、

（1）クラウドでバーチャライズされているネットワークサービス（DNS,LDAP など）、

（2）アプリケーションサーバやネットワークサービスまでのネットワーク経路、および

（3）第三者やデータセンタが提供するバーチャル・サーバーやＳａａＳサービスなどに依存しています。

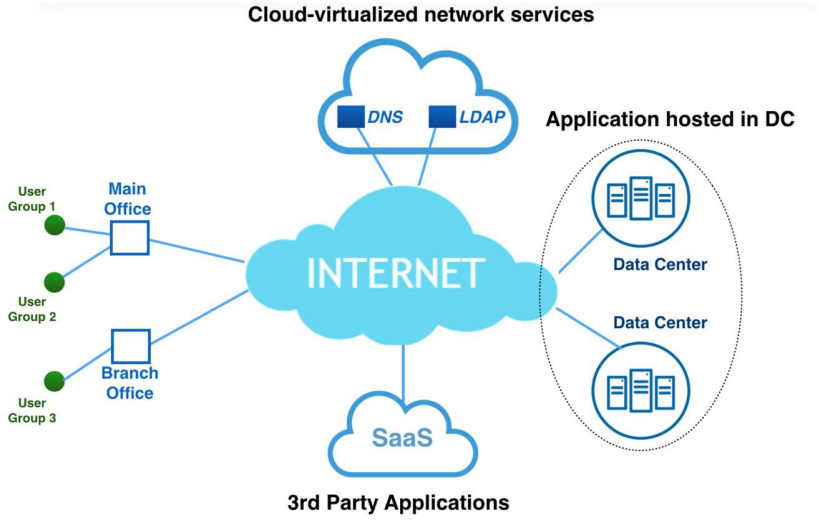


図２：クラウド仮想化アプリケーション・アクセス・インフラストラクチャ

このような環境下で、運用部門はクライアントにとってミッションクリティカルなアプリケーションに関して、頻繁に苦情を受けたり、問題を見逃しているケースもあります。（1）Sharepoint が機能していない、（2）Office 365 が停止している、（3）Webex / Skype / Zoom が不安定になっている、（4）仮想デスクトップが遅いなど、（５）ＩＣＴとはこのようなものだと遅いレスポンスや品質の悪さにあきらめている。そして、これらの問題が深刻化してきています。 多くのアプリケーションとそれをサポートするインフラがクラウド仮想化しているため、さらに問題が複雑化してきています。 従来のパフォーマンス分析ツールは、アプリケーション層またはネットワーク層のみを分析・可視化しています。そのために応答性能などのパフォーマンスの問題に対処するため、部門間での調整が必要だったりで、分析に多大な作業工数と時間がかかったりしています。もはや従来の手法とプロセスでは効果的な問題処置が出来なくなってきています。新しい時代の AIOPS*(Artificial Intelligence for IT Operations)*が必要とされている所以です。

２．ソルーション

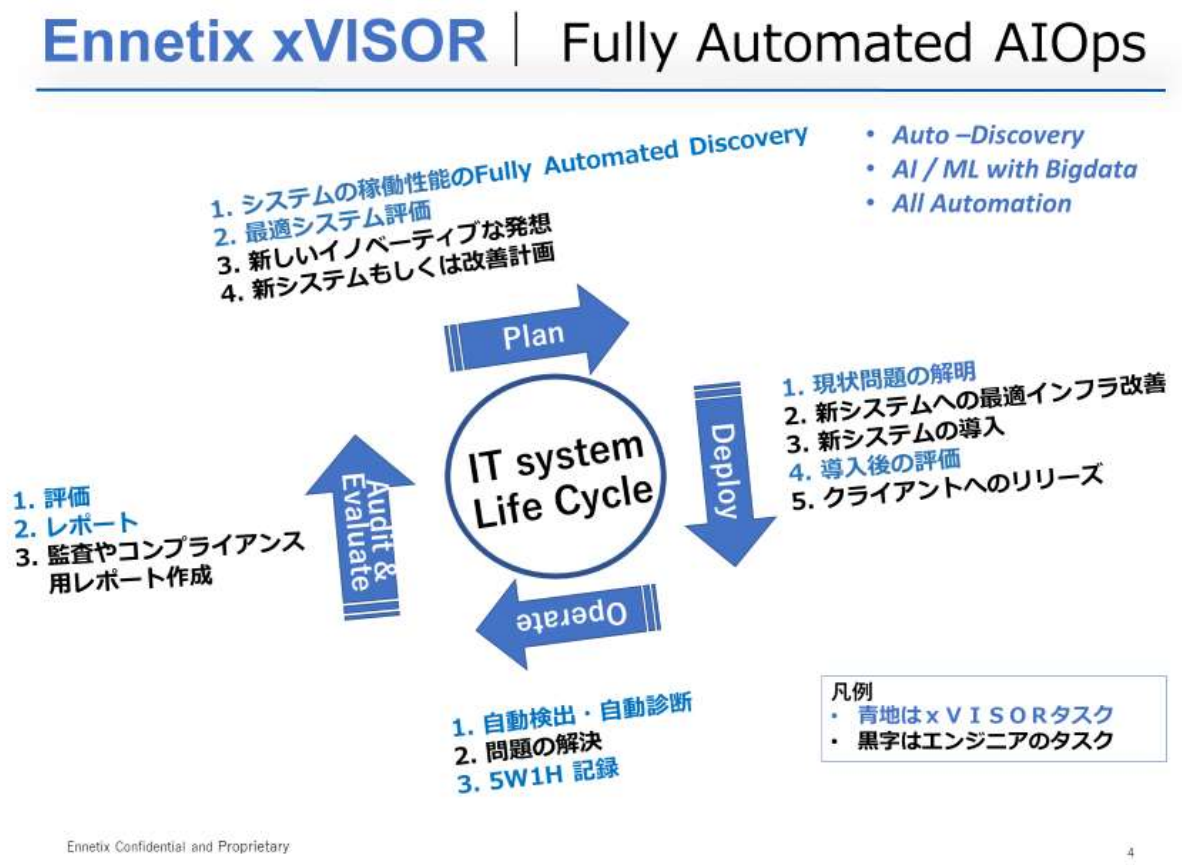
Ennetix の xVISOR はクラウド・バーチャリゼーション時代の AIOPS コンポーネント/ツールで、複数の有名顧客サイトで既に検証されています。クライアント-サーバ型アプリケーションのエンド・ツー・エンドの応答品質のみならず、アプリケーションアクセスに依存する一連のネットワークサービスなどもマッピングしてパフォーマンス分析するなど、全方位からデータ収集・分析して可視性を提供します。 xVISOR は性能・品質問題をリアルタイムで特定し、問

題のあるインシデントを迅速にトリアージする実用的なフォレンジック情報を提供します。
xVISOR は、そのクライアントとアプリに固有の詳細レベルのアプリケーションパフォーマンスを全方位（３６０度）から分析するために AI 駆動の推論エンジンを利用しています。

xVISOR は 1 時間程度で導入・展開でき、アプリケーション運用部門は次のようなメリッが得られます。

1. 問題がアプリケーション、ネットワーク、ネットワークサービスのいずれにあるかをリアルタイムで診断し、可視化。
2. 実際に起こしている問題/箇所を正確に特定化。（例：アプリのトランザクションエラー、輻輳したネットワークリンク、DNS トランザクションの遅延、認証エラーなど）。
3. インシデント診断時間を数時間のレベルから 5 分間に短縮。

AIOｐｓというと運用部門のツールと思われるかもしれません。しかしながら、現在のＩＣＴシステムの全体を自動発見する xVISOR はプラニング（計画）のためにも重要な役割を果たします。例えば、現行 ICT システムの改善やリプーレースを提案する企画部やシステム・インテグレータにとって、現状の静的・動的な状況を理解する必要があります。xVISOR はこれらの情報を各コンポーネット・レベルまで自動発見します。レイヤー２からレイヤー７（L2~L7）までの状況、DNS,LDAP,アップ・サーバーのレスポンス時間、各ルーターの遅延やロスなどをすべて自動発見します。もちろん、社員がどのようなサーバーをどのくらい使用しているかなども自動発見します。また、逆にアプリ・サーバーをどのクライアントがどのくらい使用しているかも自動発見します。これらの状況を把握したうえで、改善の提案や新システムのリプレースを企画・提案すべきと考えます。また、現状を把握することで、知識だけに頼らない思わぬイノベーション的なアイデアが浮かぶ可能性も高まります。
さらに xVISOR は現状の静的・動的な状況をビジブル（可視化）できるため、コンプライアンスや監査のイノベーティブな ICT 資料の作成に役立ちます。



3． xVISOR アーキテクチャ

xVISOR は SaaS（Software-as-a-Service）ソリューションです。特にシステム・インテグレータやデータセンター事業者の SaaS ビジネスに新しいプラットフォームを提供します。これらを Ennetix 社が提供することもできますが、Ennetix 社は　これらの SaaS プラットフォーム・ソフトウェアをシステム・インテグレータやデータセンター事業者に提供します。

図 3 に示すように、xVISOR アーキテクチャには 2 つの主要コンポーネントがあります。

（a）**XOME**（スマート・センサー）：顧客ネットワークに配置されるデータ・コレクタであり、分析のためにエンド・ツー・エンドのデータを収集して正規化します。

（b）**ENNETIX xVISOR CLOUD**：データをクラウド上に格納・保管し、AI 分析などの中核的役割を果たします。XOME によって収集されたデータを複数の観点から分析し、 Web ベースの xVISOR ダッシュボードで可視化します。

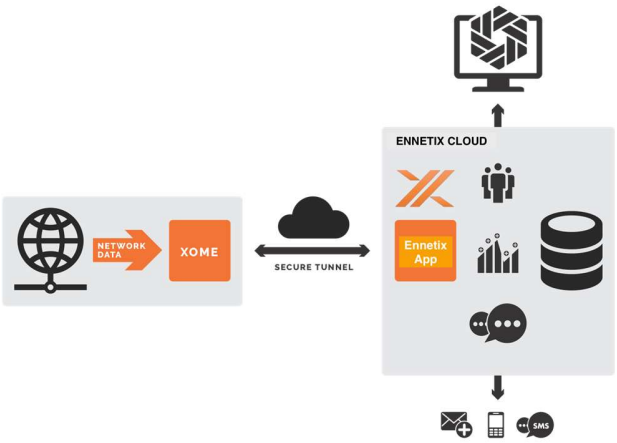


図 3：xVISOR アーキテクチャの概要

アプリ・インフラの運用部門（ユーザー）は、xVISOR が提供する Web ベースのダッシュボードをコンソール・マシーン（ＰＣなど）からクラウド経由でアクセスしてアプリ・インフラ全体の状況が把握できます。 ダッシュボードの詳細は第４項で説明します。

３．１．XOME（スマート・センサー）の導入方法

図４に示すように、XOME はクライアントの企業ネットワーク内（例えば本社、支社、支店など）にインストールされます。 XOME はコンテナ化されたソフトウェアとして設計されています。 そのため、コンテナをサポートしている任意のホスト OS 環境で実行できます。 XOME アーキテクチャの詳細はセクション 3.2 で説明します。 XOME は、本社、支社、支店などのボーダールータ（ミラー/タップポート）に直接接続するか、もしくはクライアントネットワークのバーチャル・マシーン（ERSPAN プロトコル利用）にインストールするかのどちらかを選択できます。 図４に示すように、XOME はパッシブなデータ（フロー、SNMP、ログなど）の収集ならびにプローブを送信することでアクティブにデータを収集します。 XOME によって収集されたデータは、正規化後、分析のために xVISOR クラウドプラットフォームにセキュア・トンネルを介して送信されます（図４）。

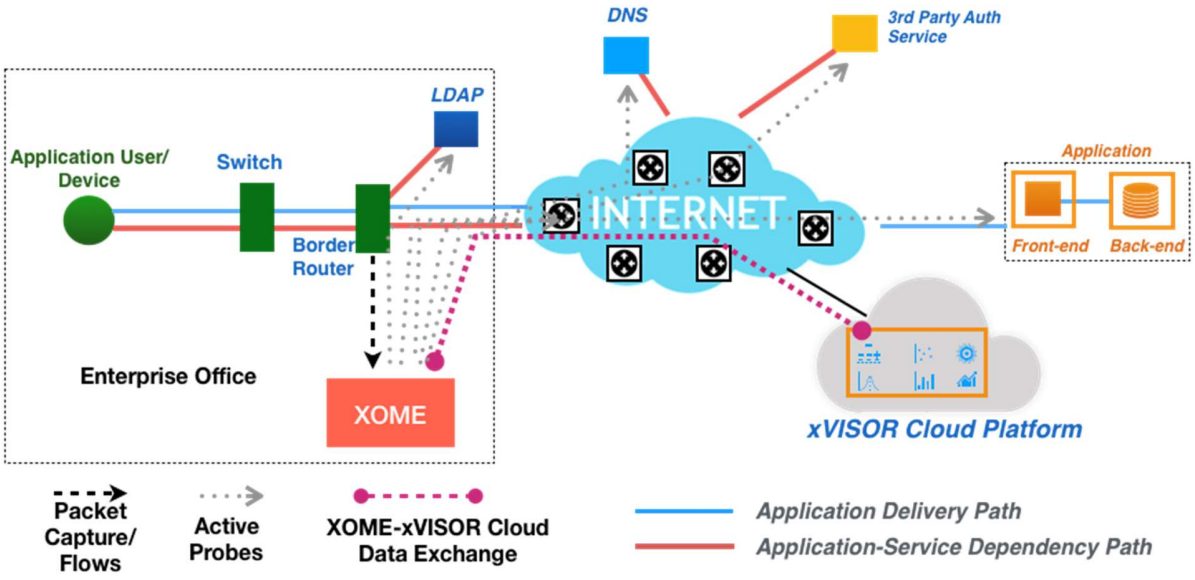


図 4：XOME の実行展開とデータ収集

XOME は、ボーダールータからのポートミラーリングにより、パケット・レベルのデータ、フローデータ（NetFlow、SFlow、IPFIX など）およびルータからの SNMP / syslog をパッシブに収集・蓄積します。 これらの収集されたパッシブ・データから、xVISOR はクライアント、アプリ・サーバー、ネットワークサービス・サーバ（DNS、LDAP、認証など）及び　クライアントがそれらのサーバーをアクセルするパスとパス上のルーターをデスカバーします。
XOME は、デスカバーされた宛先（イントラネットやインターネットのルータ、アプリケーションサーバ、ネットワークサービスサーバなど）にアクティブプローブを送信して、ホップ・バイ・ホップ、セグメント・バイ・セグメント、およびエンド・ツー・エンドのパフォーマンスデータ（遅延、損失、ジッタ、利用可能な帯域幅など）を収集します。さらに XOME データ収集の詳細はセクション 3.2 でも説明しています。

3．2． XOME アーキテクチャ

前述のように、XOME は Docker コンテナとして、ホスト OS /デバイスに導入されます（図 5）。もし XOME にアップデート/パッチが必要な場合には Ennetix クラウドリポジトリからの新しいアップデート/パッチで自動的にアップデートされます。
XOME は、重要なシステムログを xVISOR クラウドにエキスポートして、その正常性やその他の重要なシステムパラメータを xVISOR クラウドに報告します。 XOME はコンテナ環境に導

入されるので、コンテナをサポートしている任意の OS にデプロイすることができ、それによってさまざまなホスティング環境に導入可能になります。

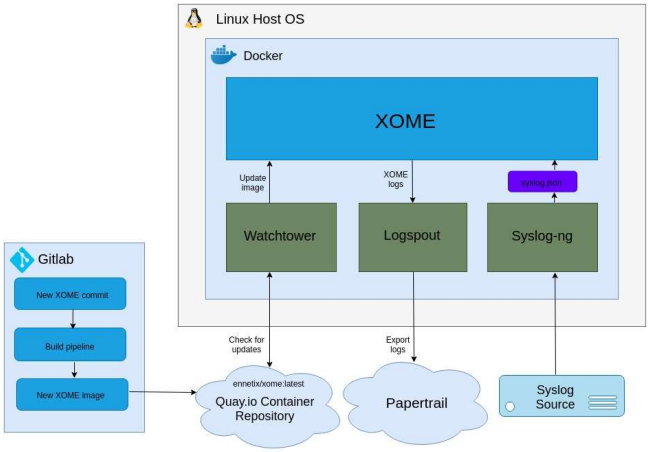


図 5：Linux ホスト上の XOME コンテナキテクチャ

次に、XOME アーキテクチャのブロック図を図 6 に示します。 図 6 に示すように、XOME は Passive Listener(パッシブリスナー)を通してフローデータ（NetFLow / SFlow など）、トラフィック、トランザクションデータや syslog などを収集します。 Passive collectors（パッシブコレクタ）はテーブルからデータを引き出し、データを分析し、データをデータバッファに集約します。

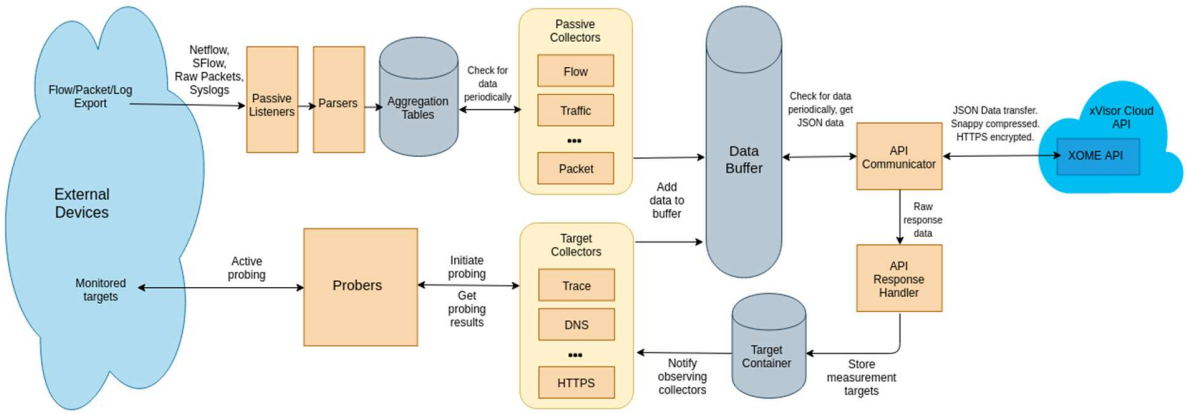


図 6：XOME アーキテクチャのブロック図

xVISOR クラウドは Ennetix 独自のＡＩ／ＭＬアルゴリズムにより、収集されたパッシブデータからアプリケーション・サービス・トポロジを学習し、ターゲット（たとえば、アプリケーションサーバ、ネットワーク・サービス・サーバ、ルータなど）をデスカバーします。

XOME Active collectors（アクティブコレクター）は、xVISOR クラウドからターゲット・コンテナを通じてターゲット情報を通知され、それぞれのプローブクラスに応じたプロービングを開始します。XOME は定期的に（５分間隔とか）これらのアクティブプローブを送信し、アクティブデータを収集します。

XOME 上の API Communicator は、モニターおよびコンフィギュレーションのリクエストがあったときに xVISOR クラウドと通信します。 また、API Communicator はバッファーのサマリーデータを継続的にチェックし、それらを JSON でフォーマットし、セキュア・トンネルを介して xVISOR クラウドに送信します。

XOME アクティブ・データ収集プロセス：XOME は、ルータ、リンク/パス、およびサーバのパフォーマンス特性を検出するためにアクティブ測定プロセスを実行します。 XOME は、Ennetix 独自のパケット・トレイン・テクノロジを使用して、これらのパフォーマンス特性をデスカバーします。 パケット・トレインには：

（１）ＴＣＰ ＳＹＮ ／ ＡＣＫ、ＵＤＰ、ＩＣＭＰエコー要求、アプリケーション・レイヤ・パケット（ＨＴＴＰ、ＨＴＴＰＳ、ＤＮＳ、ＬＤＡＰなど）を使用して、ｘＶＩＳＯＲデータ収集用に設計したプローブパケットを使います。

（２）プローブパケットがクライアントからのパケットと同じ経路をたどるためにクライアントと同じパケット・シグネチャを使用します。

（3）サーバ側には何のインストルメンテーションも必要としません。

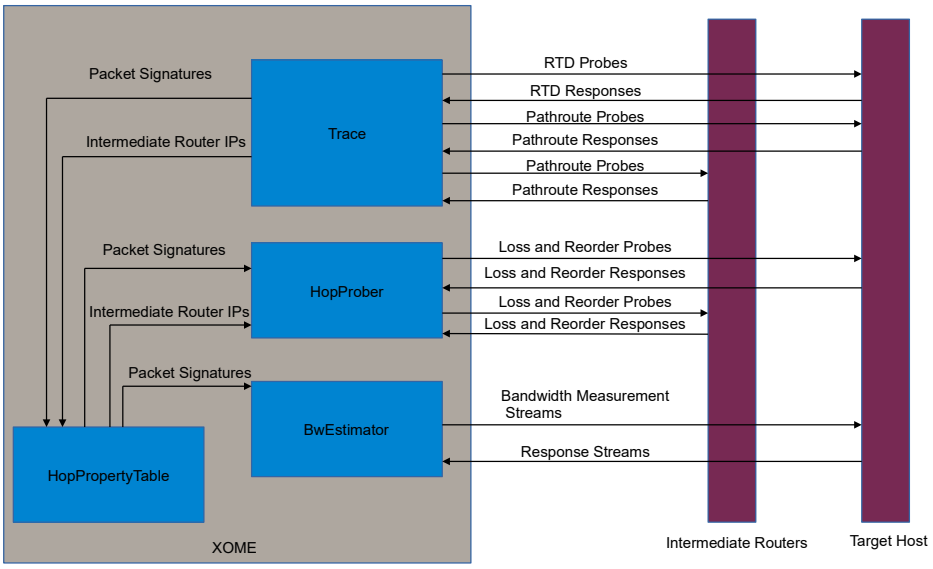


図 7：XOME アクティブ測定プロセス

図 7 はアクティブ測定プロセスの主要コンポーネントを示します。XOME は宛先タイプに応じたパケット・タイプでプローブの送信を開始して、さまざまなパフォーマンス特性を収集します。 XOME は以下を収集します。

(a) **Pathroute**：XOME は、プローブの TTL フィールドを変更させることによって、介在するルータからの応答の ICMP 時間を監視して、ターゲットホスト（アプリケーションサーバなど）への経路のトポロジーをデスカバーします。XOME は、マルチパス・ルーティングが存在する場合でも正確なルート・トポロジを理解するためにパケット・シグネチャの履歴を管理しています。 XOME は、MPLS ラベルスタックのプローブに対する ICMP 応答を調べることによって、MPLS トンネルも検出します。 このプロセスでデスカバーされたイントラネット、インターネット、およびデータセンタ・ネットワーク内の中間ルータは、その後、リンクごとのパフォーマンスデータを収集するためにプローブされます。

(b) **ラウンド・トリップ遅延**：XOME は、ターゲットホストへのプローブを定期的に送信し、そのホストの応答から、クライアント-サーバ間（エンド・ツー・エンド）のラウンド・トリップ遅延を測定します。

(c) **リンクごとの損失と遅延**：XOME はパスルート中に見つけたパケットシグネチャを使用して、検出した各ルータへのパケット損失率と遅延を測定します。 各リンクの

損失率（または遅延）は、そのポイント間の損失率（または遅延）の差から算定します。

(d) **使用可能帯域幅**：プローブのストリームを所定のレートでターゲットに送信し、応答のパケット間到着時間を分析することによって、XOME はそのレートがエンド・ツー・エンドの使用可能帯域幅より大きいか小さいかを判断できます。 このプロセスをいくつかの異なるレートで繰り返すことにより、XOME はホストへのパスのエンド・ツー・エンドの使用可能帯域幅の上限と下限を見つけ出しています。

(e) **ホスト・パフォーマンス**：XOME は、クライアント・リクエストとして模倣したプローブパケットをホスト（アプリケーションサーバやネットワークサービス）に送信することによって、ホスト固有の測定値も収集します。 収集されるホスト固有の測定値には、次のようなものがあります。

- HTTP / S の Web ページロード時間、ならびに名前検索、接続、SSL、応答、フェッチ時間などの要素を含む遅延を計測します。
- DNS と LDAP のパフォーマンス（リゾルーション時間、成功/失敗率）

以上のように XOME はプローブパケットとそのレスポンスの特性（タイミング、レスポンスコードなど）の両方を使用して、さまざまなパフォーマンス特性（リンクごと、エンド・ツー・エンド）を測定します。

３．３　xVISOR クラウドアーキテクチャ

図 8 に xVISOR クラウドのブロック図を示します。 XOME は、ｘＶＩＳＯＲクラウドの API Instances に接続します。API Instances は負荷分散された拡張性の高い仕掛けですので、xVISOR クラウドへの大規模なデータ取り込みが出来ます。 xVISOR のユーザ（運用部門スタッフ）は xVISOR が提供するダッシュボードを使用して、アプリケーションインフラの状態を検証できます。ダッシュボードへのアクセスは負荷分散された Web インスタンスでサポートされています。

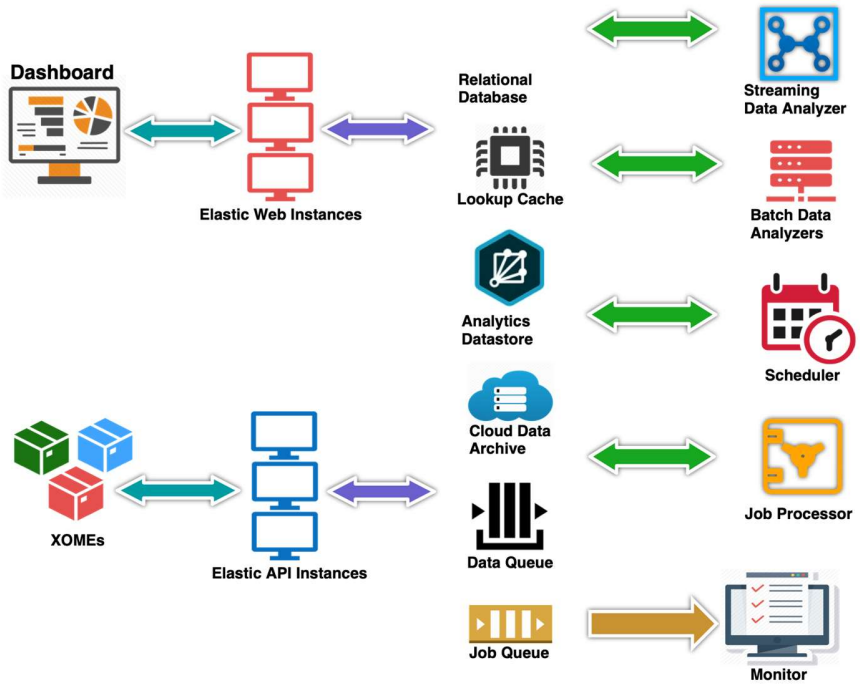


図 8：xVISOR クラウドブロック図

xVISOR クラウドは、Ennetix Cloud インフラ上にコンテナ環境としてデプロイされ、Kubernetes コンテナ・オーケストレーションによって管理されています。 xVISOR Cloud のバックエンドには、AI / ML アルゴリズムを使用したデータ分析と、データの長期保存をサポートするモジュールがあります。

- **Data Queue:** 拡張可能で、テラビット規模のデータ取り込みを処理できるストリーミング・データ・キュー・クラスタ構造にしています。
- **Job Queue:** ジョブを順番に格納するためのキューで、ジョブプロセッサによって処理されます。
- **Streaming Data Analyzer:** フォールトトレラント、そしてスケーラブルなリアルタイム分析用のストリーミング分析クラスタで構成しています。
- **Batch-Data Analyzer:** 大量のデータを大規模に処理するジョブで定期的に実行します。
- **ＡＩ／ＭＬアルゴリズムに基づくカスタムメイドの分析**：
    - リアルタイム分析ジョブは、Streaming Data Analyzer で実行します。
    - 長時間実行されるバッチジョブは、Batch Data Analyzer で実行します。

- **Job Scheduler/Processor:** オンデマンドおよびスケジュールされたジョブを処理するための Ennetix 独自のジョブスケジューラ/プロセッサです。
- **Data Store:** 複数の種類のデータを処理するためのデータストア・テクノロジを使っています。 分析データは Analytics Datastore に送られます。 長期アーカイブデータは Cloud Data Archive に送られます。 Lookup Cache はキャッシュ・データ用です。そしてクライアント/ユーザ/アプリケーションのデータは SQL ベースのストレージで管理されます。 これらのデータストアは、スケーラブルで、高速検索ができるように設計されています。

4． xVISOR Dashboard

前述のように、xVISOR は SaaS ソリューションです。 アプリ・インフラの運用部門スタッフ（ユーザー）は、URL https://app.ennetix.com から Ennetix ダッシュボード（コンソールなど）にアクセスできます。 xVISOR のログインページを以下に示します。

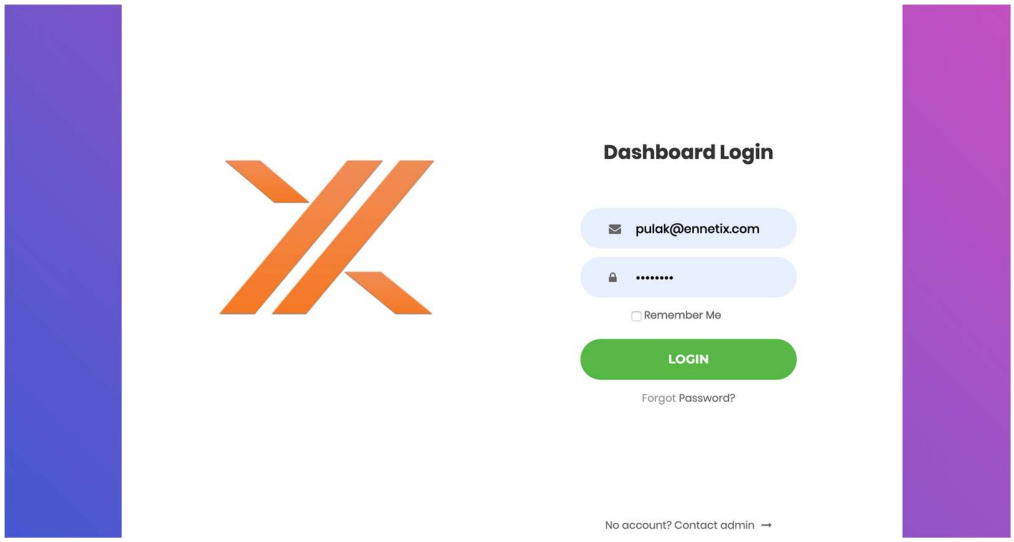


Figure 9: xVISOR ログインページ.

４．１．ｘＶＩＳＯＲダッシュボード機能

４．１．１．分析主導の 360 度の可視性

クラウド上の監視対象アプリケーションに対して、xVISOR は（a）アプリケーション、（b）ネットワーク、および（c）サービスの 3 次元でパフォーマンスを分析し、可視化します。図 10（a）および 10（b）では、例としてあるクライアントの SMB アプリケーション・トランザクションのパフォーマンス（エラー、遅延、カウント数、ボリュームなど）を 5 分間隔で表示しています。またネットワーク状態（TCP 再送信、TCP RTT などのレイヤ 4 パフォーマンス、遅延、損失、ジッタ、帯域幅などの L-3 パフォーマンスパラメータ）を同時に表示しています。さらにクライアントからアプリ・サーバーに接続しているパスルートも表示しています。 xVISOR は、同じ 5 分間におけるサービスレベルのアクセスパフォーマンス（トランザクションエラー、遅延、損失など）も示します。図１０（ｂ）はＤＮＳへのサービスレイヤーアクセス性能を示しています。もちろん、DNS のみならず LDAP、AD、SSH、その他の第三者のサービスやアプリケーションなど、あらゆるものに対応できます。

このようにアプリケーションにアクセスするためのすべてのコンポーネントの状態を測定して、ユーザパフォーマンスを表示します。このため、アプリケーション運用管理者はパフォーマンス問題に関するトラブルシューティングやパフォーマンス問題の関連付けを簡単に実現できます。

さらに、動的な ML / AI アルゴリズムを使用した xVISOR は、問題を診断し、それを特定の箇所にピンポイントすることができます。図 10（a）の例では、クライアントが直面している問題は、複数のトランザクションエラーが発生しているアプリケーション・レイヤのケースです。

図 10（a）：アプリケーションアクセスのパフォーマンス：パート 1

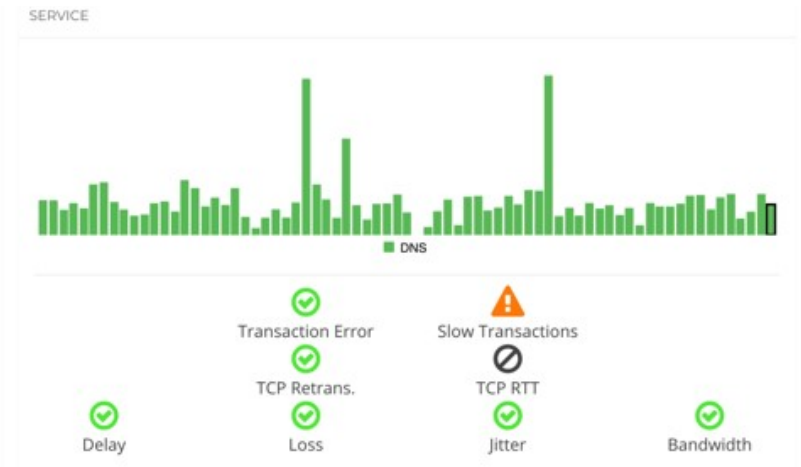


図 10（b）：アプリケーションアクセスのパフォーマンス：パート 2

４．１．２　アプリケーション・インフラ・トポロジの自動検出と可視化

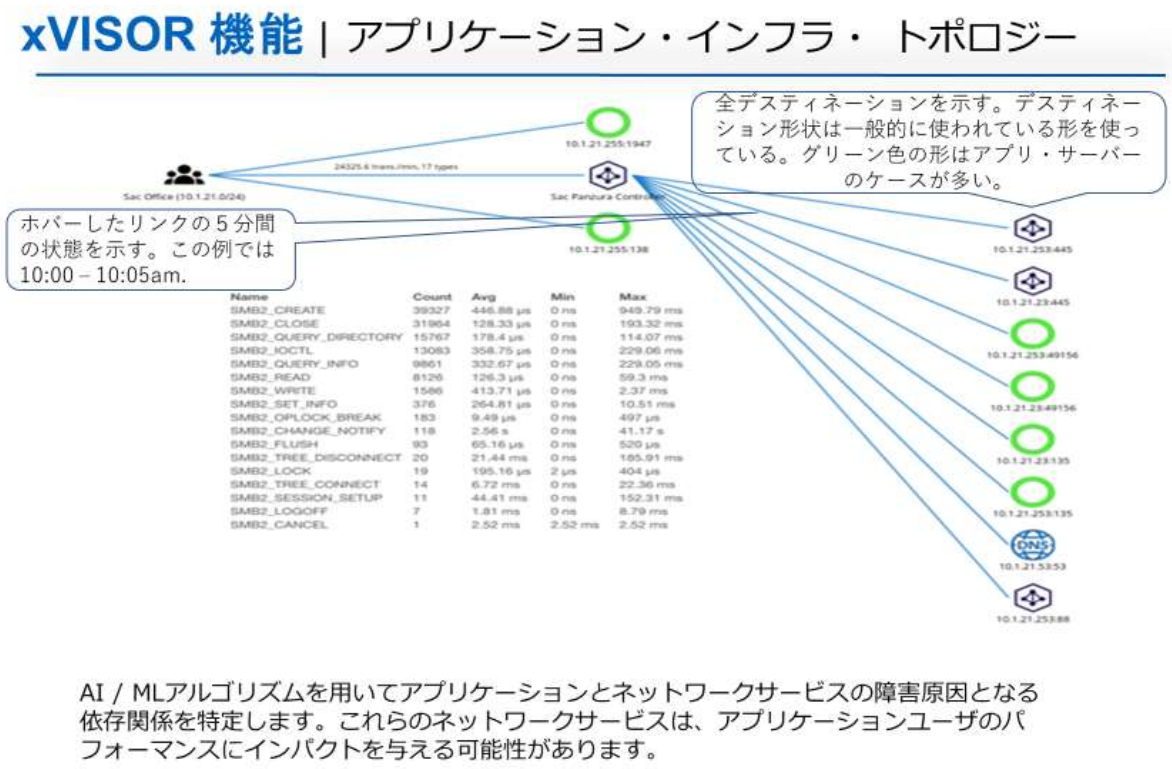


図 11：アプリケーション・インフラのトポロジー

xVISOR は AI / ML アルゴリズムを使用して、クライアントがアプリケーションにアクセスするためのすべてのコンポーネントをデスカバーします。例えば、クライアントがクラウドにあるアプリにアクセスする場合に、まずはクラウド上のＤＮＳサーバをアクセスします。また、クライアントの認証をするためにクラウド上のＬＤＡＰサーバにもアクセスします。その後、アプリ・サーバをアクセスすることになります。これらすべてのアクセスがスムーズの行われなければ、クライアントの満足は得られません。

ＤＮＳサーバの性能やクライアントからＤＮＳサーバまでへの経路、それからＬＤＡＰサーバの性能やその経路までへの ネットワークサービスの性能は、クライアントがアプリケーションをアクセスするときのパフォーマンスに影響を与える可能性があります。 したがって、アプリ

へのアクセスのみならず、ネットワークサービスのアクセスをデスカバーすることが重要です。それらすべてのコンポーネントとその性能・品質を測定・把握することでクライアントのパフォーマンスと問題の全体像が初めて分かります。
それらは 図１０（ａ）および図１０（ｂ）で、アプリケーション、ネットワーク、およびサービスの全体的な相関と因果的依存関係を示して、運用部門が全体像から思わぬデスカバリーを可能にします。 Ennetix xVISOR は、このような 360 度の可視性を提供する市場で唯一のソリューションです。

４．１．３．パス（経路）パフォーマンスに関する自動的なマッピング

XVISOR は、XOME のアクティブ測定技術を通じて、アプリケーションやサービスの経路トポロジー上の各パスのホップごと、セグメントごと、およびエンド・ツー・エンドのパフォーマンスを収集・可視化することができます。 図 12 で示すようにアプリケーションインフラであるイントラネットとインターネットの両方のネットワークインフラが一目で分かります。ホップ、ルータ/スイッチ、アプリケーションサーバ、ネットワークサービスのパフォーマンスの劣化を自動的に検出し、アプリケーションアクセスのパフォーマンス上の問題として特定化します。以上のように xVISOR は、自動的にパフォーマンスのベースライン状態を検出・表示し、運用部門のユーザが的確な診断と処置をするためのサポートが出来ます。

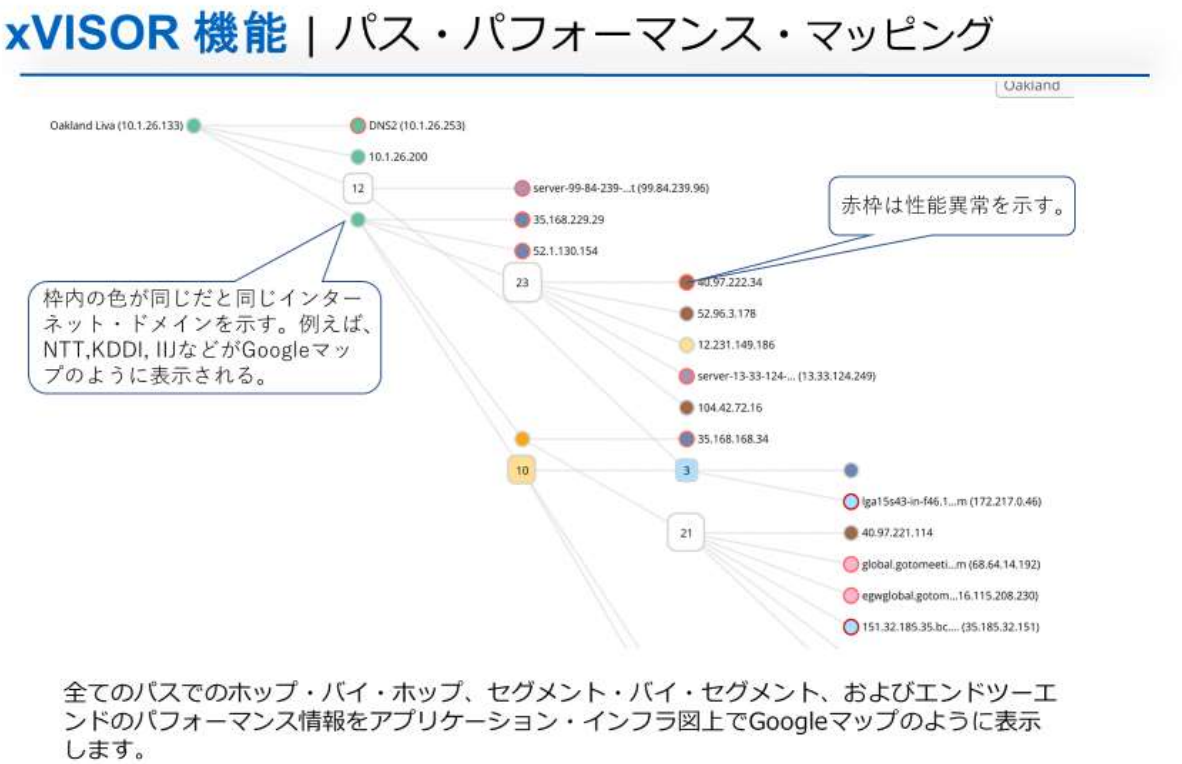


図 12：アプリケーションインフラのマップ・ビュー

４．１．４．自動異常検出とパターン認識

xVISOR は、監視対象アプリケーションのパフォーマンスと異常な動作を自動的に検出します（図 13 および図 14）。 これらの異常を推測するためにＡＩ ／ ＭＬアルゴリズム（例えば、パラメトリック回帰、クラスタリング、モデルベースのヘルス・スコアリング、ランダム決定フォレストなど）を使用しています。 これらのアルゴリズムは、アプリケーション/ネットワーク運用管理者がアラートを処理するのに大いに役立つものと考えられます。 また、相関分析によって、管理者はパフォーマンスのホットスポットと診断を正確に特定できます。 レガシーの監視ツールはパフォーマンスの問題検出のために閾値ベースのポリシーを必要としていますが、xVISOR は自動化された異常検出と警告によって、管理者の閾値の設定作業の負担を軽減します。

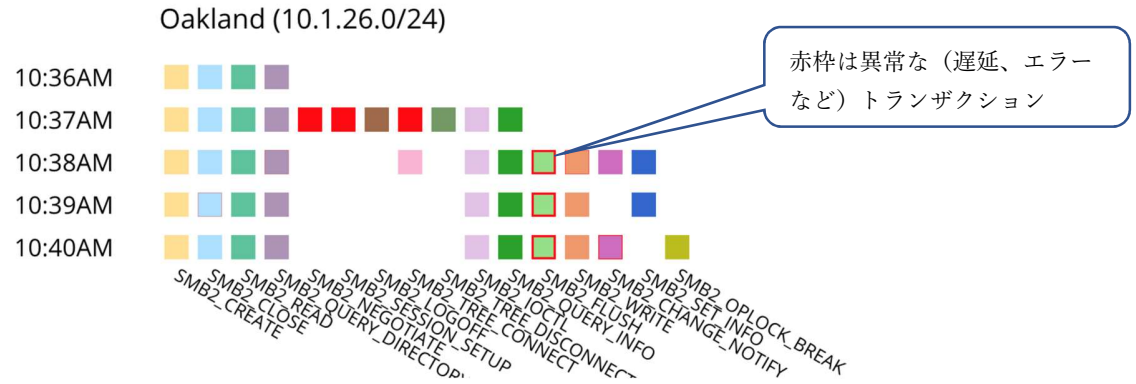


図１３；異常を示すためのアプリケーション・トランザクション・ヒートマップ

４．１．５．アプリケーション固有のユーザビヘイビア分析

xVISOR は AI / ML アルゴリズムを使用して、アプリケーションにアクセスしている間の各ユーザのトラフィック動作のベースラインを作成します。 これらのアルゴリズムは、クライアントからの苦情を先取りして異常な動作を自動的にデスカバーし、アプリケーション管理者が修正措置を取れるようにサポートします。

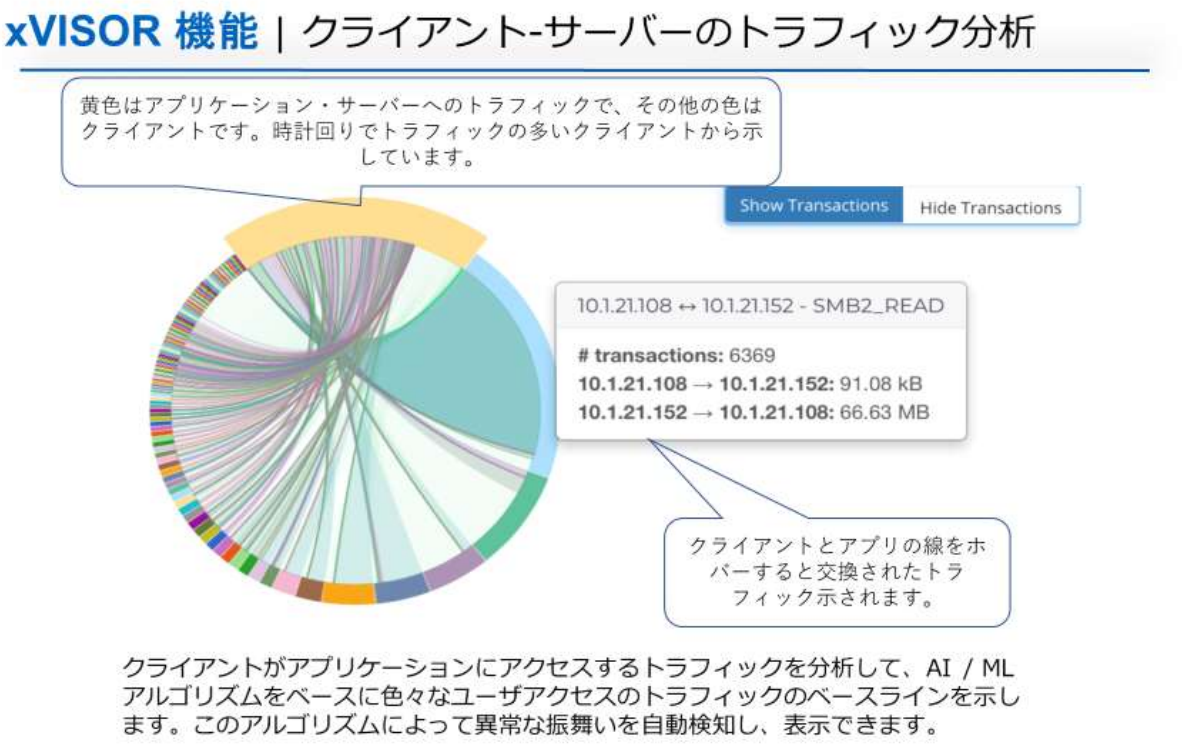


図 14：クライアントとアプリ間の異常なトラフィックを特定するための容量分析

４．１．６．ヒストリカルな観察とフォレンジックス

xVISOR を使用すると、アプリケーション管理者は、スライダー（図 10（a）の上部に表示）とタイムウィンドウを使用して、5 分間隔でパフォーマンス履歴を確認することもできます。ヒストリカル（時間経緯的）な観察とフォレンジックのために、xVISOR は最大 1 か月まで 5 分間隔での各ユーザのパフォーマンスデータを保持できます。 必要に応じて、さらに長い期間のデータを保持できます。 また、長期的なパフォーマンスレポートを作成して傾向と要約を特定することができます。