業界初!!

ネットワークやシステムパフォーマンスの可視化から現在の商品在庫や売れ筋までをリアルタイム解析！

ExtraHop

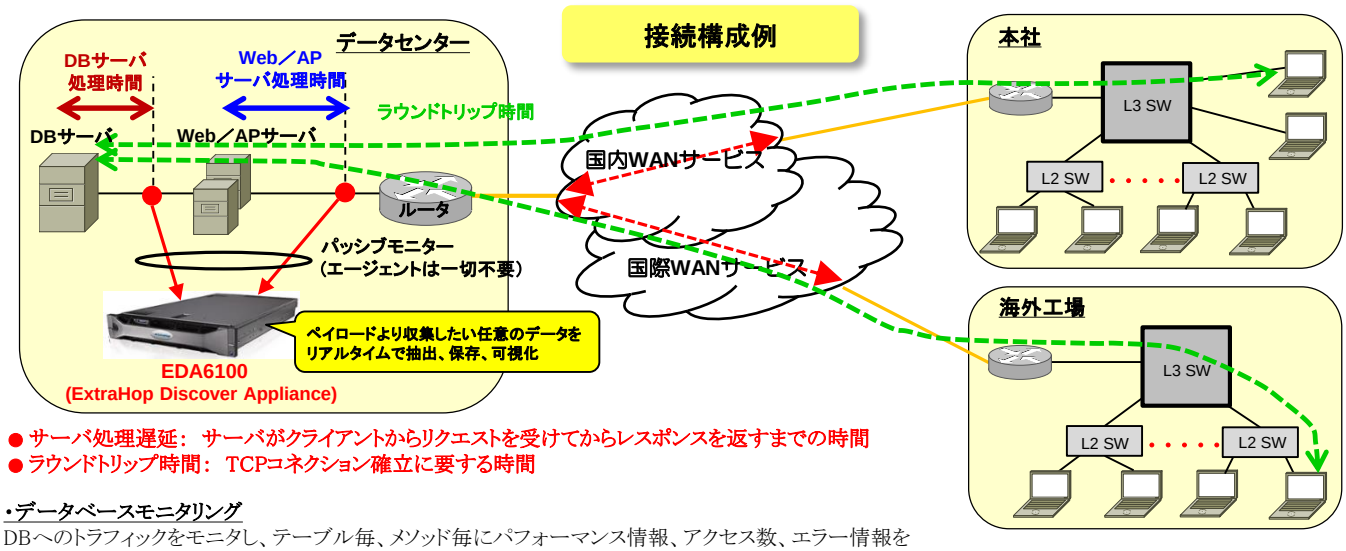
処理能力40Gbps
EDA9100

ExtraHop Networks社（アメリカ、シアトル）が開発した“ExtraHopアプライアンス”は回線上の実トラフィックを**パッシブ**にモニタリングし、ネットワークレベルから、アプリケーション(Web、DB等)のトランザクションレベルまでを**リアルタイム可視化！ダッシュボードを一目見るだけで、現状把握が可能です！**

更に、他に類を見ないペイロード解析機能により、時間毎に変化する在庫や商品の出入りを商品番号毎に分類・表示、「今日の売れ筋商品」をリアルタイムに、マーケティング部や経営層に自動報告します！

ExtraHop社のソリューションは従来製品とは以下の点で大きく異なっています。

- 実トラフィックをL2からL7までリアルタイムに解析、更に**ペイロードの特定部分を抽出、解析、保存**する事で経営上の意思決定にも貢献！
- アプリケーション検査トリガ機能により、**振る舞い監視**を実現。パフォーマンス監視だけでなく、ブルートフォース攻撃やデータベース不正アクセスの監視等、セキュリティ監視も可能。（アプリケーション検査トリガ：監視・測定項目をユーザ自身で設定できるExtraHop独自の機能）
- パッシブモニターアーキテクチャで**エージェントは一切不要**、監視対象機器に対する追加設定は一切不要です。（AWS環境を除く）



- サーバ処理遅延： サーバがクライアントからリクエストを受けてからレスポンスを返すまでの時間
- ラウンドトリップ時間： TCPコネクション確立に要する時間

・データベースモニタリング

DBへのトラフィックをモニタし、テーブル毎、メソッド毎にパフォーマンス情報、アクセス数、エラー情報を可視化します。（Oracle、DB2、MS-SQL、MySQL、PostgresSQL等）

・HTTPモニタリング

Webサーバへのトラフィックをモニタし、サーバ毎、URI毎にパフォーマンス情報、アクセス数、エラー情報を可視化します。

主な導入メリット

● ビジネスインテリジェンス／ビッグデータ

従来のビジネスインテリジェンス(BI)やビッグデータアプローチと違い、ExtraHopのソリューションはシンプルにネットワーク上のトラフィックからリアルタイムにペイロード内の分析対象データ（商品コード、販売数、購入された時間等）を抽出、保存、可視化する事で、より早く、安価に実現。更に、アプリケーション検査トリガーを使ってワイヤデータから任意の特定部分を抽出する事で商品やサービスの販売傾向を把握するだけでなく、他のビッグデータストアへ送る事で他のデータ・ソースとの相関解析も可能です。

● 広範なセキュリティ監視とコンプライアンス

ExtraHopによる回線上の実トラフィックのリアルタイム解析は、ふるまいの異常なクライアント等を見つける事が可能です(午後10時に普通より20パーセント多くのファイルにアクセスしている特定のクライアントがいる、データベースからの受信データが1MBより大きい、等)。
IDSまたはIPSシステムとは異なり、ExtraHopのワイヤー・データ解析はシグネチャに依存せず、ネットワーク上で通信している全てのシステム又はクライアントのふるまいをリアルタイムに観察し、分析可能です。

● プロアクティブモニタリングと問題解決

ExtraHopプラットフォームは、自社ネットワークを流れる全てのクライアント、アプリケーション、およびインフラストラクチャ間の関係を含む完全なトランザクション・レベルでの可視化を行い、深い洞察を可能にし、システムに潜む問題を顕在化する前に対処する事が可能です。

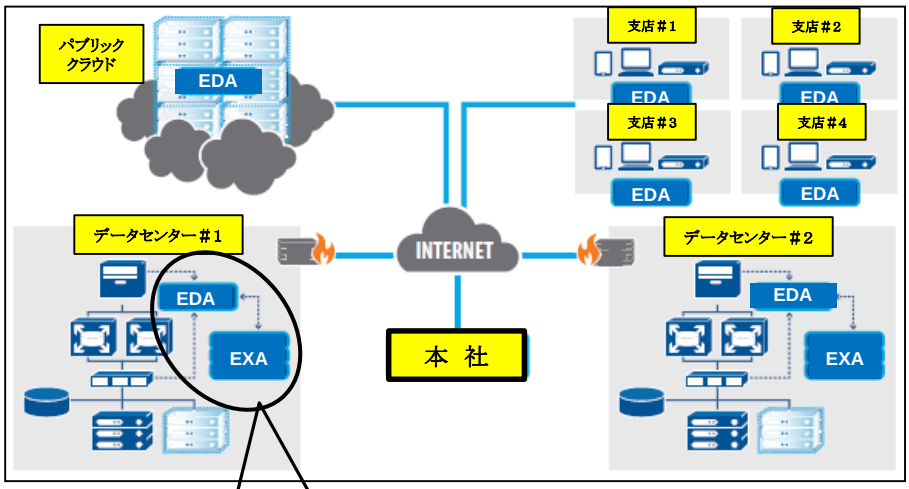
● 最適化と継続的改善

ExtraHopを用いて、強化すべきサーバ、引退もしくはクラウドへの移行が可能なアプリケーションやシステム、TCPの最適化等を推測や仮定でなく、解析データに基づいて判断する事により継続的な設備及び運用コストの削減が可能です。またIT投資の正当性を証明するデータを入手可能です。自社システム環境内の全ての要素の利用状況と相互依存性を理解する事で過剰投資を防ぎ、より正確な情報に基づいた適切なIT投資を実現します。

CORNET TECHNOLOGY 日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2　〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp

ExtraHop
See IT run.

● ExtraHopターンキーソリューション

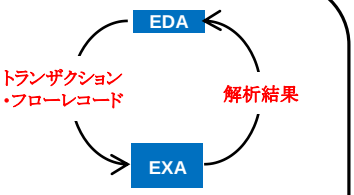


EDA (ExtraHop Discover Appliance)

ExtraHop Discovery Appliance（EDA）は、ExtraHopプラットホームの要となる製品です。タップまたはミラーポートよりネットワーク・トラフィックを収集し、非常にスケーラブルなリアルタイムITおよびビジネス分析のためにパケットを体系化されたワイヤー・データに変えます。Web、ミドルウェア、データベース、ストレージ、VDI等主要なTCPまたはUDPベースのアプリケーションのプロトコルをサポートします。

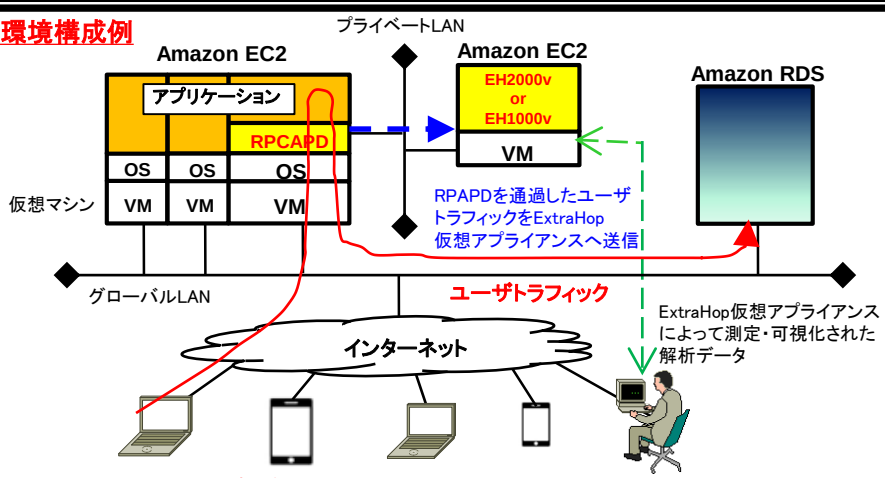
EXA (ExtraHop Explore Appliance)

ExtraHop Explore Appliance（EXA）はDiscover Appliance（EDA）からトランザクションとフローレコードを受け取り、多次元分析に備えそれらのレコードにインデックスを付けて保存します。ユーザはいつでも単純なクエリー言語で、それらから捜す、調査する、ピボットする、そして洞察を抽出することができます。ExtraHop プラットホームのビジュアルクエリー言語による多次元分析 を通してより多くのトランザクションとフローレコードを調査することができます。



EXAはEDAからトランザクション・フローレコードを受け取り、EDAよりも更に詳細な解析を行い、その結果をEDAに返します。
これによりEDAユーザはアプリケーション検査トリガを使う(プログラムを作成する）事無く、詳細解析結果を容易に入手可能となります。

●AWS環境構成例



RPCAPD（ExtraHop社より提供されるプログラム）
EC2上のアプリケーションで発生するトラフィック（ユーザからのアクセス、DBとの通信等）をキャプチャして、EC2上のExtraHop仮想アプライアンス（EH1000v or EH2000v）へ送信する機能を提供。

主な機能

● アプリケーション検査トリガ

ExtraHopアプライアンスが標準でサポートしない測定項目やフィルター条件をユーザ自身が定義し、追加でき、自社システムのニーズに合わせたカスタマイズが容易に行えます。

● Webアプリケーションの詳細解析

・Web(HTTP,HTTPs)アプリケーションのアクセス数、処理遅延、トラフィック量、エラー状況等をURI単位で可視化可能。

● データベースの詳細解析と情報漏えい対策

・データベースのアクセス数やエラー、処理遅延をテーブル毎、メソッド毎に可視化し、レスポンスタイム悪化の原因特定を迅速に実行
・データベースへのアクセスを常時監視し、疑わしい振る舞い（大量データ取得、特定テーブルへの長時間接続等）の検出・通知、アクセスレコードの編集、ログサーバへの保存が可能。

● 業界初！AWS環境の可視化をサポート

CloudWatchでは提供されないパフォーマンス情報や課金のベースとなるデータ量、リージョン毎のトラフィックやトランザクションの片寄りなど、AWSの運用に必要なパフォーマンス情報だけでなく、最適化に有効な情報まで提供！

● Splunkとの連携

・収集したパフォーマンス情報やエラー情報をSplunk上で統計グラフとして作成可能。
・アプリケーション検査トリガでフィルターを設定する事で、Splunkへ渡すデータを必要最小限に減らし、利用コストの削減が可能。

● 振る舞い監視によるセキュリティ脅威の識別

アクセスユーザの振る舞いを監視し、IPS、IDS等では検出できないシグネチャが無い脅威を識別。

● 外部で取得したPCAPファイルをオフライン解析

遠隔拠点での障害調査において、ExtraHopを遠隔拠点に持ち運ぶ事無く、現地で取得したPCAPファイルをインポートする事で原因調査が可能！

● 実環境に一切影響を与えないパッシブモニター

● 設定不要で簡単導入

CORNET TECHNOLOGY 日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2　〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp