

# Why We Monitor Networks but Still Don't Understand Them

Exploring the gap between metrics and understanding  
A journey through behavioral analysis and intelligent augmentation

# 監視しているのに、 なぜ理解できないのか？

## AIで原因まで解明

メトリクス（数値指標）と真の理解との間にあるギャップを探る  
行動分析とインテリジェントな拡張（AI活用）を通じた探求の旅

# Who We Are

- Luca is the founder of ntop a European company (Italy and Switzerland) established 25+ years ago that develops open-source network security and visibility tools.

He is the contributor to various open-source software tools (e.g. Wireshark and Suricata) and a lecturer at the CS Department of the University of Pisa, Italy.



- Gabriele is a master student at the CS Department of the University of Pisa and a junior network engineer at ntop. He is passionate about AI, network monitoring, and large data analysis.



# 自己紹介

## Luca

25年以上前に設立されたヨーロッパの企業であるntop（イタリアおよびスイスに拠点）の創業者です。同社は、オープンソースのネットワークセキュリティおよびネットワーク可視化ツールの開発を行っています。

また、LucaはWiresharkやSuricataをはじめとするさまざまなオープンソースソフトウェアプロジェクトへの貢献者であり、イタリアのピサ大学コン

**Gabriel**サイエンス学部の講師も務めています。

イタリアのピサ大学コンピュータサイエンス学部に在籍する修士課程の学生であり、ntopのジュニアネットワークエンジニアとしても活動しています。

AI、ネットワーク監視、大規模データ分析に強い関心と情熱を持っています。



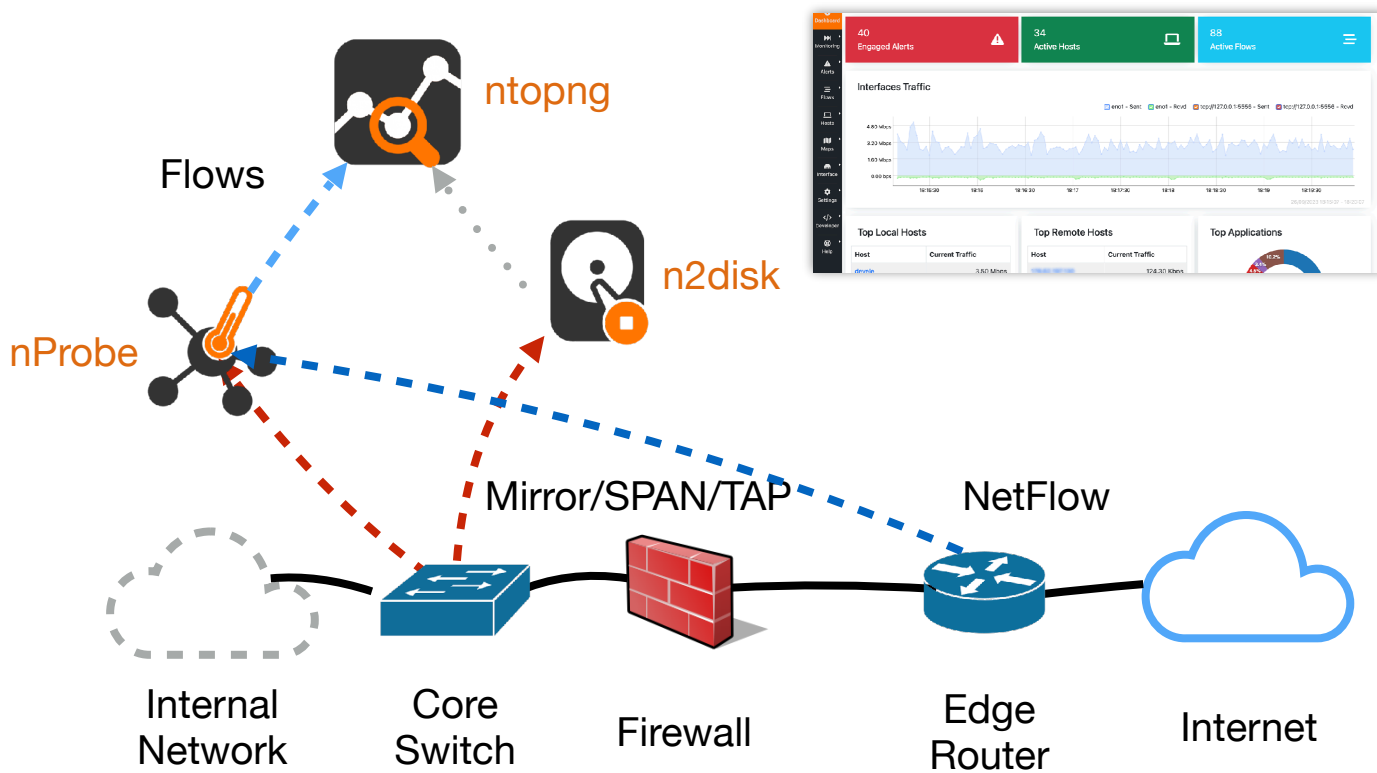
# ntop and Jupiter Technology

- Jupiter Technology Corporation (ジュピターテクノロジー株式会社) is a prominent Japanese IT company that specializes in localizing, distributing, and supporting advanced international software solutions for the Japanese market.
- Jupiter serves as the primary official partner and distributor in Japan for ntop.
- Our partnership focuses on delivering ntop tools to enterprise and SME networks in Japan.
- This event has been possible thanks to the support of Jupiter Technology.

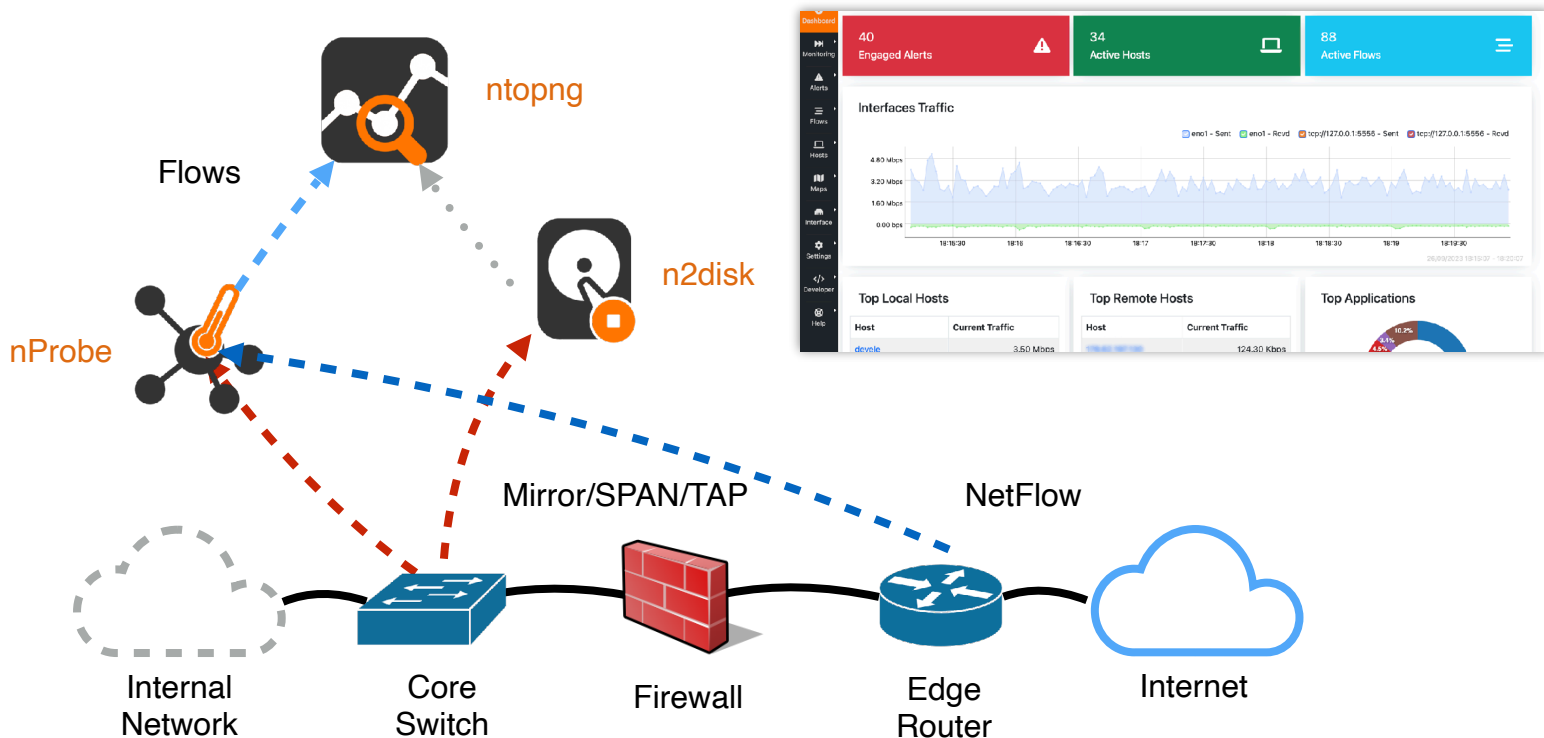
# ntopとジュピターテクノロジー

- ジュピターテクノロジーは、海外の先進的なソフトウェア製品を日本市場向けにローカライズし、販売・サポートを提供する日本の有力なIT企業です。
- ジュピターテクノロジーは、ntop製品の日本国内における主要な公式パートナーおよびディストリビューターを務めています。
- 両社のパートナーシップを通じて、日本国内の大企業から中小企業まで幅広いお客様へntop製品を提供しています。
- 本イベントは、ジュピターテクノロジーのご支援により実現しました。

# The ntop Ecosystem



# ntop製品群・関連ソリューション群



# The ntop Vision

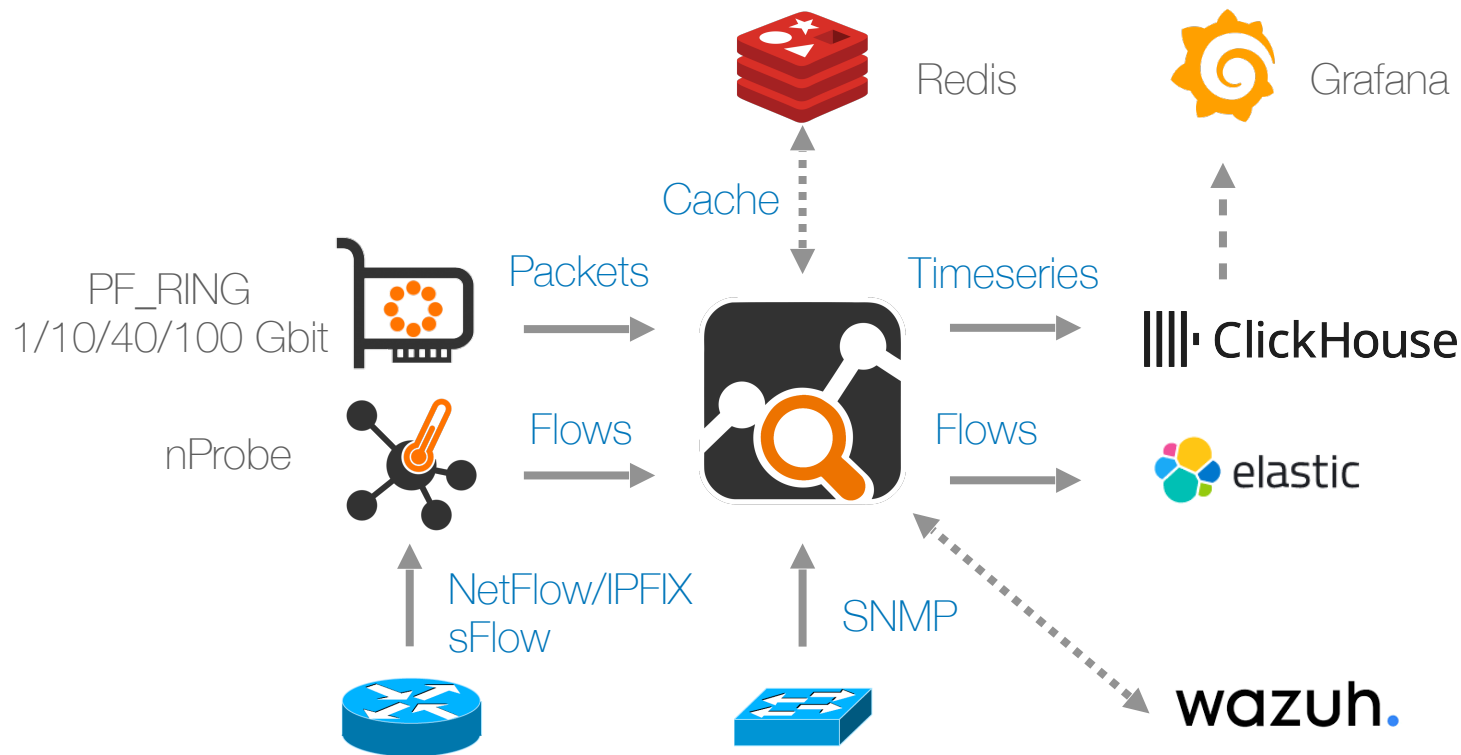
- We have developed components that can fulfill various requirements:
  - Traffic visibility and security (DPI, L7-protocol support).
  - Large networks monitoring via distribute probes.
  - Data retention and troubleshooting (n2disk).
  - Graphical console for network monitoring (ntopng).
  - Multi-10/100 Gbit support (RX+TX), balancing, filtering....
  - DDoS Mitigation
  - 100 Gbit traffic monitoring (QoS + QoE)
- In essence, we're working towards a **toolkit for commodity hardware systems**, able to satisfy most network visibility needs.

# ntopのビジョン

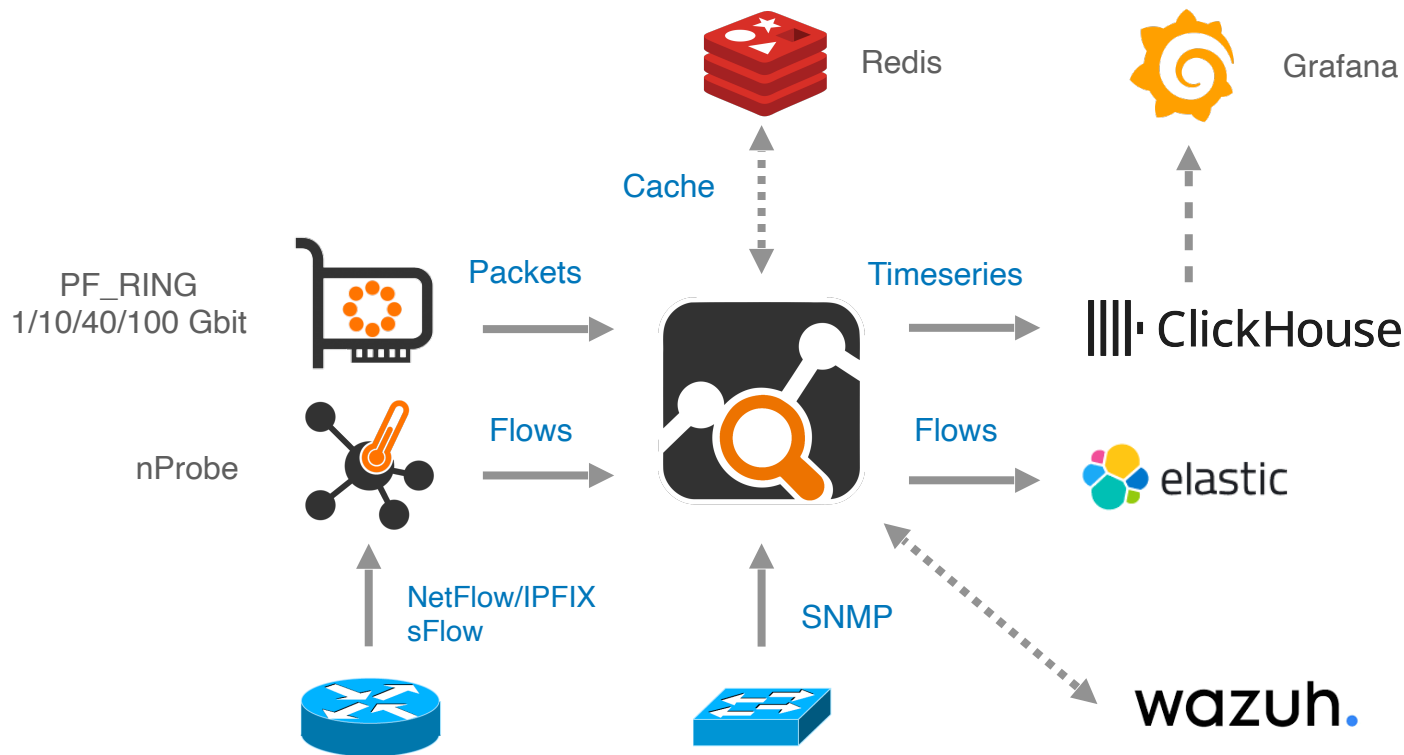
当社は、さまざまな要件に対応できるコンポーネント群を開発してきました。

- トラフィックの可視化とセキュリティ (DPI、L7プロトコル対応)
- 分散プローブによる大規模ネットワーク監視
- データ保存とトラブルシューティング (n2disk)
- ネットワーク監視向けグラフィカルコンソール (ntopng)
- マルチ10Gbps/100Gbps環境対応 (送受信対応)、負荷分散、フィルタリング
- **DDoS攻撃対策**  
つまり私たち 一般的なサーバーハードウェア上で動作し、ネットワーク可視化に関する
- **100Gbps環境におけるトンネルネットワーク監視 (n2disk)** の実現を目指しています。

# ntopng Architecture



# ntopng アーキテクチャ



# The Visibility Gap and The Modern Challenge

- Executive Focus  
High financial investments in monitoring tools frequently fail to decrease Mean Time to Resolution (MTTR).
- Technical Focus  
Standard dashboards display thousands of disparate time-series charts without behavioral correlation: more doesn't mean better.
- Key Point  
Data abundance creates operational noise. True visibility requires structural synthesis, data correlation and intelligence.



# 可視化のギャップと現代の課題

- 経営層の視点

監視ツールへの多額の投資を行っているにもかかわらず、平均復旧時間（MTTR）の短縮につながらないケースが少なくありません。

- 技術者の視点

一般的なダッシュボードには、相互の関連性がない数千もの時系列グラフが表示されます。しかし、情報量が多いことが必ずしも優れた可視化を意味するわけではありません。

- 重要なポイント

データが増えれば増えるほど、運用現場にはノイズが生まれます。

真の可視化を実現するには、データの構造化・相関分析・インテリジェンス（知能化）が不可欠です。



# The Death of the Perimeter

- The Reality

Modern networks are highly fragmented with hybrid-cloud and remote workforces, Firewalls and edge proxies can no longer see the critical lateral east-west traffic inside your infrastructure.



- The Consequence

Modern visibility blind spots are exactly where advanced threats, misconfigurations, and performance bottlenecks live.

- The Requirement

Continuous, deep-network visibility must occur *everywhere*, not just at the network border.

# 境界防御の終焉



- **現実**

現代のネットワークは、ハイブリッドクラウドやリモートワークの普及により高度に分散化されています。

その結果、ファイアウォールやエッジプロキシだけでは、インフラ内部で発生する重要な東西トラフィックを把握できなくなっています。

- **影響**

現代のネットワークにおける可視化の死角こそが、高度なサイバー攻撃、設定ミス、そして性能ボトルネックが潜む場所となっています。

- **求められること**

継続的かつ詳細なネットワーク可視化は、ネットワーク境界だけではなく、ネットワーク全体のあらゆる場所を実施されなければなりません。

# Why Traditional Flow Monitoring Fails

- The Problem

Legacy sampling models (like 1:1000 packet sampling typical of NetFlow/IPFIX/sFlow) or coarse 1-minute granularities iron out anomalies.

- The Blind Spot

Transient spikes, micro-bursts, and highly targeted low-and-slow cyber attacks completely disappear. This is because NetFlow/IPFIX/sFlow rely on packet sampling and averaged counters.

- The Shift

Moving from statistical guessing models to deterministic traffic capture with near-realtime detailed counters stored on timeseries databases for drill-down and analytical analysis.

# 従来型フローモニタリングが限界を迎えている理由

- **課題**

NetFlow/IPFIX/sFlowで一般的な1:1000パケットサンプリングなど

従来のサンプリング方式や、1分単位の粗い集計粒度では、重要な異常が平滑化されてしまいます。

- **見落とされるもの**

瞬間的なトラフィックスパイク、マイクロバースト、そして標的型の低速・潜伏型サイバー攻撃（Low-and-Slow Attack）は、監視データ上から完全に消えてしまいます。これは、NetFlow/IPFIX/sFlowがパケットサンプリングや平均化されたカウンタ値に依存しているためです。

- **求められる変化**

統計的な推測に基づく監視モデルから脱却し、詳細なトラフィック情報をほぼリアルタイムで収集・保存する決定論的なトラフィックキャプチャへ移行する必要があります。そして、それらのデータを時系列データベースに蓄積し、ドリルダウン分析や高度な分析を可能にすることが重要です。

# ntopng: Next-Gen Network Visibility

- Vision

Network traffic analysis using high-resolution, application and security oriented (DPI) probes able to parse packets into *human-oriented intelligence*.

- Core Philosophy

Building an open, highly flexible platform that doesn't just log packets but continuously analyzes their underlying operational intent.

- Key Value

Designed to sit natively inside your infrastructure to provide instant operational answers.

# ntopng:次世代ネットワーク可視化の実現

- **ビジョン**

アプリケーションやセキュリティを意識した高解像度のDPIプローブを用いてネットワークトラフィックを分析し、パケットデータを**人が理解しやすいインテリジェンス**へと変換します。

- **基本思想**

単にパケットを記録するだけでなく、その背後にある通信の目的や意図を継続的に分析する、オープンで高い柔軟性を持つプラットフォームを構築することを目指しています。

- **提供価値**

お客様のネットワークインフラ内部にネイティブに配置され、運用上の疑問に対する答えを即座に提供できるよう設計されています。

# Engineering for Large-Scale Networks

- Technical Focus

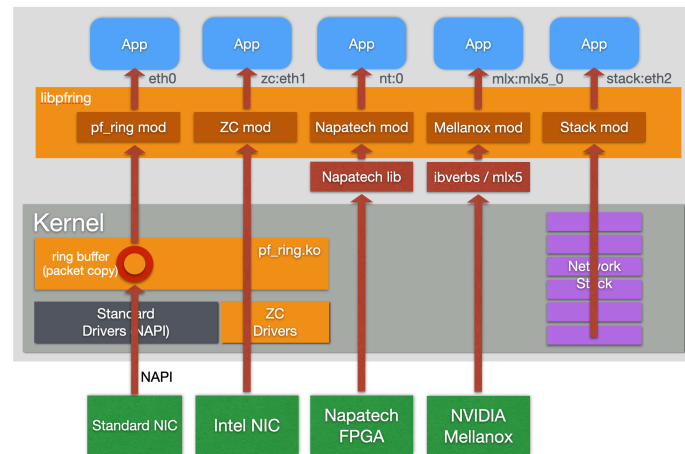
Line-rate processing across 10G/40G/100G+ interfaces without CPU starvation or dropped packets.

- Scale Capability

Handling hundreds of thousands of concurrent active flows across vast enterprise fabrics.

- Distribution and Precision

Collect rich monitoring data across large networks with high precision (no just packets and bytes) measurements with continuous sub-second metrics tracking.



[https://github.com/ntop/PF\\_RING/](https://github.com/ntop/PF_RING/)

# 大規模ネットワークに対応する技術

- 技術的な特長

10Gbps、40Gbps、100Gbpsを超える高速インターフェース環境においても、CPUリソースの枯渇やパケットロスが発生させることなく、ラインレートでの処理を実現します。

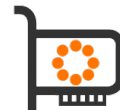
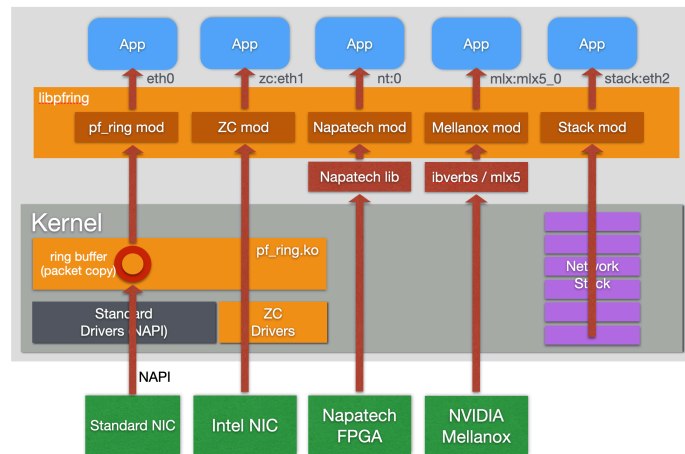
- スケーラビリティ

大規模なエンタープライズネットワークにおいて、数十万規模のアクティブフローを同時に処理できます。

- 分散性と精度

広範なネットワーク全体から豊富な監視データを収集し、高精度な分析を実現します。

単なるパケット数やバイト数だけでなく、さまざまな指標を継続的に収集し、サブ秒単位での詳細なメトリクス追跡を行います。



PF\_RING

[https://github.com/ntop/PF\\_RING/](https://github.com/ntop/PF_RING/)

# Deep Packet Inspection (DPI) with nDPI

- The Challenge  
Over 90% of enterprise traffic is encrypted. Traditional inspection breaks down without risky decryption proxies.
- The Engine  
Leveraging the open-source nDPI engine natively within ntop tools: 14 years of developments, the only open DPI toolkit available on the market, developed by ntop.
- Protocol Mastery  
Over 500 different application protocols recognized out of the box.
- The Objective  
Moving beyond port-based identification (e.g., assuming port 443 is safe HTTPS traffic) to true behavior payload classification, and cybersecurity metadata extraction.



nDPI

<https://github.com/ntop/nDPI>

# ディープパケットインスペクション(DPI) with nDPI

- 課題

企業ネットワークトラフィックの90%以上は暗号化されています。従来のトラフィック検査手法は、リスクの高い復号プロキシ（SSL/TLSインスペクション）を導入しない限り十分に機能しません。



nDPI

<https://github.com/ntop/nDPI>

- エンジン

ntop製品群には、オープンソースのDPI（Deep Packet Inspection）エンジンである

nDPIがネイティブに組み込まれています。nDPIは14年以上にわたり開発が継続されており、

- **プロトコル識別能力** 市場で利用可能な唯一の本格的なオープンソースDPIツールキットとして、ntopによって開発・提供されています。500種類以上のアプリケーションプロトコルを標準で認識できます。

- 目的

「ポート番号ベースの識別」（例えば、TCP/443番ポートの通信を単純に安全なHTTPS通信とみなすこと）から脱却し、実際の通信内容や振る舞いに基づく高度なアプリケーション分類、およびサイバーセキュリティに有用なメタデータの抽出を実現することです。

# Next-Gen Cyber Detection in ntopng

- Continuous Auditing  
Real-time behavioral detection heuristics running simultaneously with packet processing.
- Identified Vectors  
Port scanning, lateral movement indicators, out-of-hours data bursts, and rogue asset discovery.
- Context Preservation and Drill Down  
Every security alert is automatically linked back to the exact historical flow, application, and device involved.

# ntopngが実現する次世代サイバー攻撃検知

- **継続的監査**

パケット処理と並行して、ルールベースの異常検知エンジンがリアルタイムに動作します。

- **検知対象**

ポートスキャン、ラテラルムーブメントの兆候、業務時間外の大量データ転送、および不正デバイスの発見。

- **コンテキスト保持とドリルダウン分析**

すべてのセキュリティアラートは、自動的に関連する過去の通信フロー、アプリケーション、およびデバイスと紐付けられます。

# Summary: The Three Pillars of Rich Visibility

- Pillar 1  
High-Performance Scale (Capture everything without loss).
- Pillar 2  
High-Definition Granularity (Zero blind spots for transient anomalies).
- Pillar 3  
Application-Aware Depth (DPI and behavioral context).

まとめ：

## 高度なネットワーク可視化を支える3つの中核技術

1

### 高性能なトラフィック収集

---

瞬間的な異常も見逃さない

2

### 高解像度なネットワーク可視化

---

すべての通信をロスなく取得

3

### アプリケーションレベルの詳細分析

---

DPIと振る舞い分析による深い洞察

# Stop Building Monitoring Islands: We're Open !

- The Problem

When infrastructure breaks down, teams spend time pointing fingers at each other because their tools don't talk.

- The Open Philosophy

Networks do not exist in a vacuum; your traffic monitoring tool must actively feed the broader enterprise security and operations ecosystem.

- Open Code and Data

Open source code guarantees you transparency, no vendor lock-in, business continuity and costs stability overtime. Open data promotes sharing, analysis with third-party tools, and ability to analyze it with artificial intelligence (AI) tools.

# 監視ツールを孤立させない – オープンな監視基盤の重要性

## 課題

インフラ障害が発生すると、ツール同士が連携していないため、チーム間で責任の押し付け合いに時間を費やしてしまいます。

## オープンな思想

ネットワークは単独で存在するものではありません。

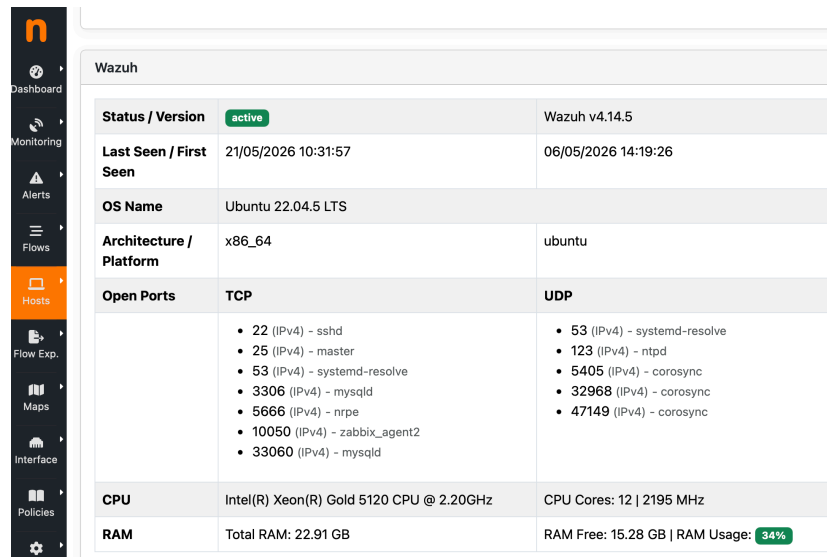
トラフィック監視ツールは、企業全体のセキュリティおよび運用エコシステムと積極的に連携すべきです。

## オープンソースとオープンデータ

- オープンソースコードは、透明性の確保、ベンダーロックインの回避、事業継続性の向上、そして長期的なコストの安定化を実現します。
- オープンデータは、他社製ツールとのデータ共有や分析を促進し、さらにAI（人工知能）を活用した高度な分析を可能にします。

# ntopng and Wazuh Integration

- The Connection  
Correlating network telemetry (wire data) directly with host-based telemetry (endpoint logs and active processes).
- The Power  
Detecting that an endpoint is communicating with an anomalous external IP (via ntopng) and instantly identifying which local process ID initiated that specific flow (via Wazuh).



The screenshot shows the ntopng interface with a sidebar on the left containing navigation options: Dashboard, Monitoring, Alerts, Flows, Hosts, Flow Exp., Maps, Interface, and Policies. The main content area displays the Wazuh integration status and details.

| Wazuh                   |  |  |
|-------------------------|--|--|
| Status / Version        | active   | Wazuh v4.14.5  |
| Last Seen / First Seen  | 21/05/2026 10:31:57  | 06/05/2026 14:19:26  |
| OS Name                 | Ubuntu 22.04.5 LTS   |  |
| Architecture / Platform | x86_64   | ubuntu   |
| Open Ports              | TCP  | UDP  |
|                         | <ul style="list-style-type: none"><li>• 22 (IPv4) - sshd</li><li>• 25 (IPv4) - master</li><li>• 53 (IPv4) - systemd-resolve</li><li>• 3306 (IPv4) - mysqld</li><li>• 5666 (IPv4) - nrpe</li><li>• 10050 (IPv4) - zabbix_agent2</li><li>• 33060 (IPv4) - mysqld</li></ul> | <ul style="list-style-type: none"><li>• 53 (IPv4) - systemd-resolve</li><li>• 123 (IPv4) - ntpd</li><li>• 5405 (IPv4) - corosync</li><li>• 32968 (IPv4) - corosync</li><li>• 47149 (IPv4) - corosync</li></ul> |
| CPU                     | Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz   | CPU Cores: 12   2195 MHz   |
| RAM                     | Total RAM: 22.91 GB  | RAM Free: 15.28 GB   RAM Usage: 34%  |

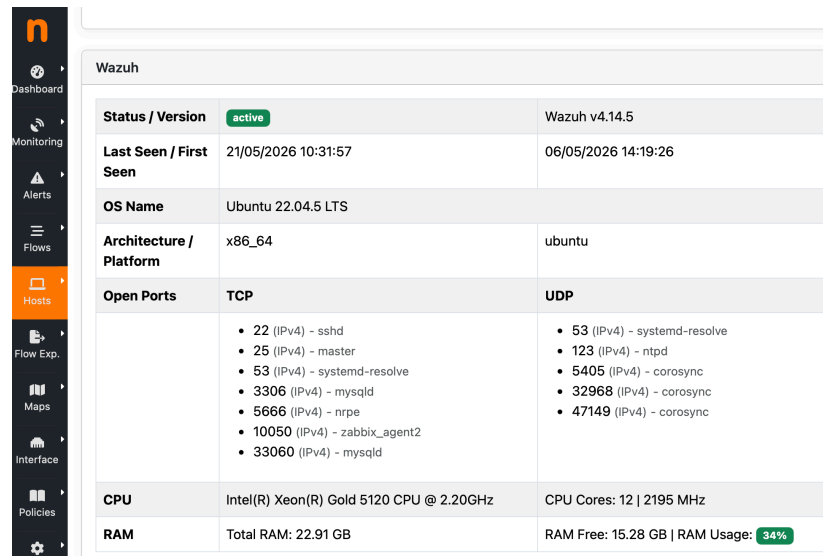
# ntopngとWazuhの連携

## 連携

ネットワークテレメトリ（通信データ）と、ホストベースのテレメトリ（エンドポイントログや実行中プロセス）を直接関連付けます。

## 効果

エンドポイントが異常な外部IPアドレスと通信していることを検知（ntopng）し、その通信フローを開始したローカルプロセスIDを即座に特定（Wazuh）できます。



| Wazuh                   |  |  |
|-------------------------|--|--|
| Status / Version        | active   | Wazuh v4.14.5  |
| Last Seen / First Seen  | 21/05/2026 10:31:57  | 06/05/2026 14:19:26  |
| OS Name                 | Ubuntu 22.04.5 LTS   |  |
| Architecture / Platform | x86_64   | ubuntu   |
| Open Ports              | TCP  | UDP  |
|                         | <ul style="list-style-type: none"><li>22 (IPv4) - sshd</li><li>25 (IPv4) - master</li><li>53 (IPv4) - systemd-resolve</li><li>3306 (IPv4) - mysqld</li><li>5666 (IPv4) - nrpe</li><li>10050 (IPv4) - zabbix_agent2</li><li>33060 (IPv4) - mysqld</li></ul> | <ul style="list-style-type: none"><li>53 (IPv4) - systemd-resolve</li><li>123 (IPv4) - ntpd</li><li>5405 (IPv4) - corosync</li><li>32968 (IPv4) - corosync</li><li>47149 (IPv4) - corosync</li></ul> |
| CPU                     | Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz   | CPU Cores: 12   2195 MHz   |
| RAM                     | Total RAM: 22.91 GB  | RAM Free: 15.28 GB   RAM Usage: 34%  |

# Eliminating Vendor Traps

- The Stand  
Monitoring data is your corporate property. You shouldn't be penalized or forced into a single ecosystem to analyze it.
- Open Standard Compliance  
Utilizing open JSON outputs, open REST APIs, and open-source foundations across the entire pipeline.
- Flexibility  
Giving organizations the freedom to switch or append visualization and storage tiers at any point.
- Core Takeaway  
True infrastructure visibility is collaborative, open-ended, and completely decoupled from proprietary constraints.

# ベンダーロックインからの脱却

## 考え方

監視データは企業の資産です。

その分析のために、特定ベンダーのエコシステムへ縛られたり、不利益を被ったりするべきではありません

### オープン標準への準拠

オープンなJSON形式の出力、REST API、そしてオープンソース基盤を活用し、システム全体で相互運用性を実現します。

### 柔軟性

可視化ツールやデータ保存基盤を、必要に応じて自由に追加・変更できる柔軟性を提供します。

## 重要なメッセージ

真のインフラ可視化とは、オープンで協調的であり、特定ベンダーの制約から完全に独立していることです。

# Shift from Filtering to Understanding

- The Core Advantage

AI in traffic analysis is not about generating random code; it is about rapid structural synthesis, data correlation and reasoning.

- Cognitive Relief

Moving the operational burden away from tedious manual triage (operators fatigue) and grep scripts: from experience to AI skills.

- The Result

Elevating junior engineers to perform advanced behavioral analysis safely and instantly, time saved, use engineers for advanced tasks and not continuously repeating unpleasant activities.

# フィルタリングから理解へ

- **中核となる強み**

トラフィック分析におけるAIの価値は、単にコードを生成することではありません。  
データの構造的な整理、相関分析、そして推論を高速に行うことにあります。

- **運用負荷の軽減**

経験や勘に頼った調査、煩雑なgrepスクリプトによる解析といった運用負荷を軽減します。  
運用担当者の疲弊を抑え、経験依存の運用からAIを活用した効率的な運用へと移行できます。

- **得られる効果**

若手エンジニアでも、安全かつ迅速に高度な振る舞い分析を実施できるようになります。  
調査時間を大幅に短縮し、エンジニアを単純な繰り返し作業ではなく、より高度で価値の高い業務に集中させることができます。

# Networks Tell Everything but Operators Have no Time To Understand It

- The Issue  
The real problem isn't visibility, it's interpretation,
- Monitoring Facts  
TBs of data per day, thousands of alerts, metrics and actionable data available to analysts: analysts spend hours investigating them or do not use them at all due to lack of time.
- Wrong Answers to Good Needs  
Most tools answer: what, not why.

ネットワークはすべてを語っている。

## しかし、運用者にはそれを理解する時間がない

- **課題**

本当の問題は、可視化ではなく「解釈」にあります。

- **監視の現実**

1日にTB単位のデータ、数千件のアラート、メトリクス、分析担当者が活用できるデータが存在します。しかし、分析担当者はそれらの調査に何時間も費やすか、時間がないためにまったく活用できていません。

- **良いニーズに対する間違った答え**

多くのツールが答えるのは「何が起きたか」であり、「なぜ起きたか」ではありません。

# From Observability to Understanding

| Today's Monitoring   | AI-based Analysis     |
|----------------------|-----------------------|
| Dashboards           | Explanations          |
| Alerts               | Prioritized incidents |
| Queries              | Grounded Answers      |
| Manual Investigation | Automated reasoning   |

# 可観測性を超えて、本当の理解へ

| 今日の監視   | AIによる分析     |
|---------|-------------|
| ダッシュボード | 説明          |
| アラート    | 重要なインシデント   |
| クエリー    | 事実に裏付けられた回答 |
| 自力による調査 | 自動推論        |

# AI in ntopng

- nDPI acts as a specialized features extractor (i.e. protocol metadata information) reported in JSON to tools sitting on top of it.
- nProbe acts as a high-precision, high definition traffic measurement sensor able to deliver data in open format to ntop/non-ntop consumers.
- ntopng acts as a telemetry engine and data source for network analysis.
- The REST API returns structured, AI-friendly JSON.
- Live and historical telemetry data is inserted into the LLM prompts.
- The LLM orchestrates the analysis using data provided by the analytics platform.

# ntopngのAI機能

- nDPI が通信の特徴を抽出する
- nProbe が高精度なネットワークテレメトリを収集する
- ntopng がテレメトリデータを統合・分析する
- REST API がAIに最適化されたJSONデータを提供する
- LLM がリアルタイムおよび履歴データを基に推論を実施する
- AI Analyst が根拠に基づく分析結果（Grounded Answers）を生成する



この流れは、


**Traffic → Telemetry → Analytics → Automated Reasoning → Grounded Answers**

(トラフィック → テレメトリ → 分析 → 自動推論 → 根拠に基づく回答)

# Using ntopng with an AI Assistant [1/2]

```
deri@iMacM1.local 206> claude
Claude Code v2.1.154

Welcome back ntop!



Sonnet 4.6 · Claude Pro · claude@ntop.org's
Organization
~/tmp/interop

Tips for getting started
Ask Claude to create a new app or clone a repository

What's new
Auto mode is now available on Bedrock, Vertex, and
Plugins in `.claude/skills` directories are now available
Added `claude plugin init <name>` to scaffold a new plugin
/release-notes for more

Opus 4.8 is now available! · /model to switch

/mcp
└─ MCP dialog dismissed
```

夜間に最も多くのクエリを実行した上位10のホストはどれですか？

夜間（22:00～06:00）に最もクエリを実行したホストを調べます。まずテーブル構造を確認します。

Called ntopng (ctrl+o to expand)

`flows` テーブルの構造を確認してから、夜間のクエリ集計を実行します。

Called ntopng (ctrl+o to expand)

`17_protocols` テーブルで DNS プロトコル ID を確認しながら、夜間（22:00～06:00）のDNSクエリを集計します。

Called ntopng (ctrl+o to expand)

タイムゾーン名を修正して再クエリします（CEST → Europe/Berlin）。

Called ntopng (ctrl+o to expand)


夜間（22:00～06:00 CEST）に最も多くのDNSクエリを実行した上位10ホスト

| 順位 | ホスト / IPアドレス  | DNSクエリ数    |
|----|---------------|------------|
| 1  | 89.31.72.65   | 12,439,913 |
| 2  | 194.242.61.65 | 9,120,377  |

# AIアシスタントを活用したntopngの利用 [1/2]

```
deri@iMacM1.local 206> claude
Claude Code v2.1.154

Welcome back ntop!



Sonnet 4.6 · Claude Pro · claude@ntop.org's
Organization
~/tmp/interop

Tips for getting started
Ask Claude to create a new app or clone a repository

What's new
Auto mode is now available on Bedrock, Vertex, and
Plugins in `.claude/skills` directories are now available
Added `claude plugin init <name>` to scaffold a new plugin
/release-notes for more

Opus 4.8 is now available! · /model to switch

/mcp
└─ MCP dialog dismissed
```

夜間に最も多くのクエリを実行した上位10のホストはどれですか？

夜間（22:00～06:00）に最もクエリを実行したホストを調べます。まずテーブル構造を確認します。

Called ntopng (ctrl+o to expand)

`flows` テーブルの構造を確認してから、夜間のクエリ集計を実行します。

Called ntopng (ctrl+o to expand)

`17_protocols` テーブルで DNS プロトコル ID を確認しながら、夜間（22:00～06:00）のDNSクエリを集計します。

Called ntopng (ctrl+o to expand)

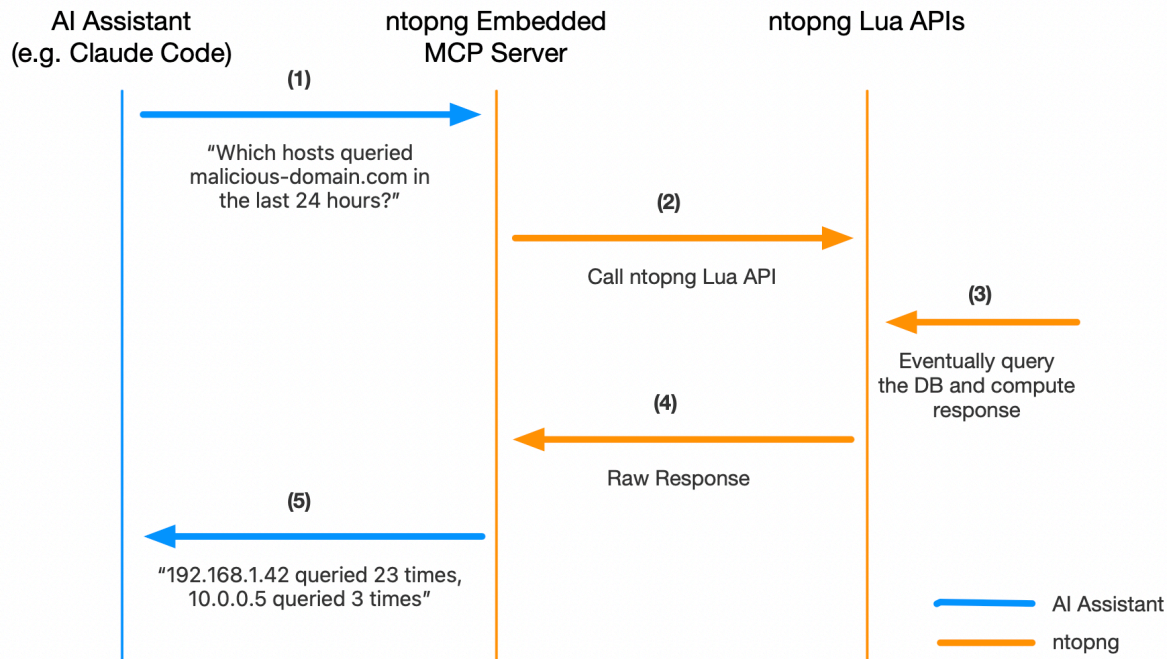
タイムゾーン名を修正して再クエリします（CEST → Europe/Berlin）。

Called ntopng (ctrl+o to expand)

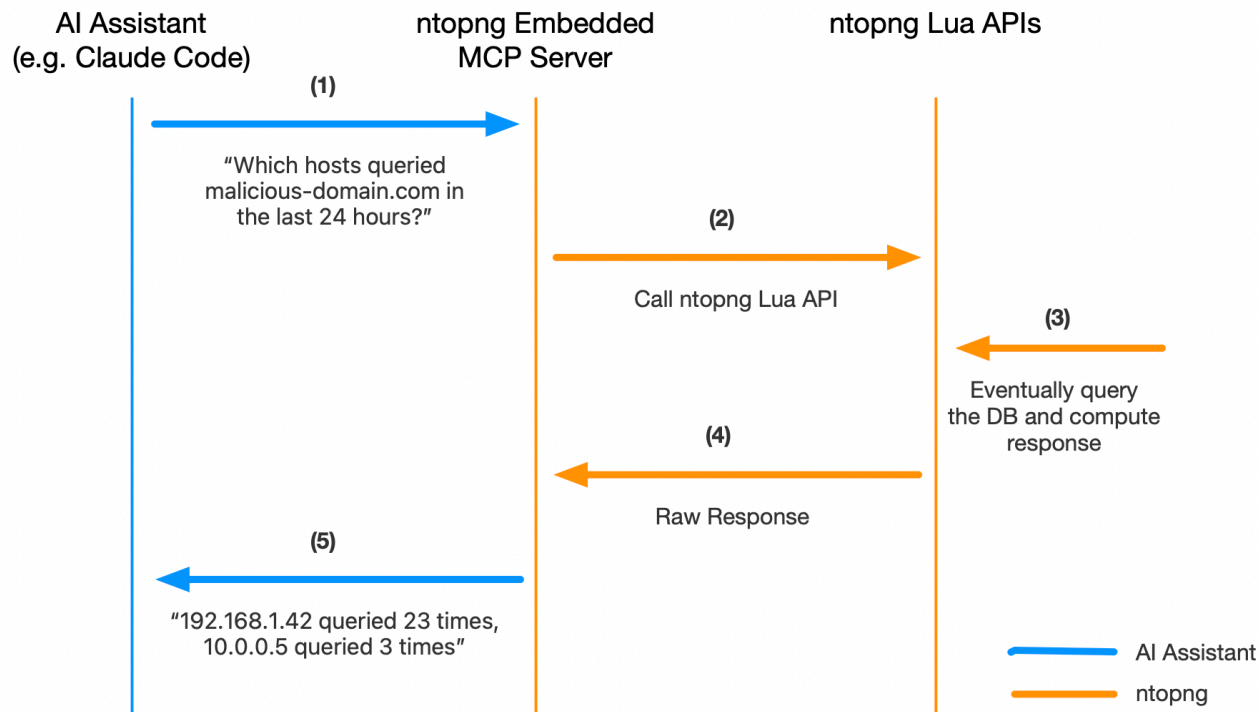
夜間（22:00～06:00 CEST）に最も多くのDNSクエリを実行した上位10ホスト

| 順位 | ホスト / IPアドレス  | DNSクエリ数    |
|----|---------------|------------|
| 1  | 89.31.72.65   | 12,439,913 |
| 2  | 194.242.61.65 | 9,120,377  |

# Using ntopng with an AI Assistant [2/2]



# AIアシスタントを活用したntopngの利用 [2/2]



# The Protocol Blueprint: MCP Tools vs. Resources

- MCP Resources (Static/Read-Only): Exposing structured, real-time datasets.
  - `ntopng://interfaces/list` -> Returns operational states, link speeds, and active configurations.
  - `ntopng://alerts/active` -> Streams the current high-priority cyber and performance alert queues.
- MCP Tools (Dynamic/Executable): Function schemas that external AI engines use to run targeted diagnostics.
  - `get_host_telemetry(ip, timespan)`
  - `get_top_talkers(interface_id, metric)`
  - `ntopng_inspect_crypto_fingerprint(suspect_ip, destination_ip)`

# MCPアーキテクチャ解説：ToolsとResourcesの役割

## MCP Resources

- `ntopng://interfaces/list`

稼働状態、リンク速度、および現在有効な設定情報を返します。

- `ntopng://alerts/active`

現在の高優先度サイバーセキュリティおよびパフォーマンスアラートキューをストリーミング配信します。

静的 / 読み取り専用  
構造化されたリアルタイムデータセットを公開

## MCP Tools

- `get_host_telemetry(ip, timespan)`

- `get_top_talkers(interface_id, metric)`

- `ntopng_inspect_crypto_fingerprint(suspect_ip, destination_ip)`

動的 / 実行可能  
外部AIエンジンが対象を絞った診断を  
実行するために利用する関数スキーマ

# Introducing nAnalyst: From Data to Answers

- What  
nAnalyst is an autonomous network intelligence layer that explains what is happening in your network and why.
- How  
Natural language queries, in your language.
- nAnalyst does the heavy lifting:
  - Query and correlate monitoring data.
  - Visualize results in charts.
  - Propose network policies and generate alert(s) on violation.
  - Add actionable items to correct problems (e.g. enable an active monitoring script to check services uptime).

# nAnalystの紹介：データから答えへ

## What

nAnalystは、ネットワーク内で何が起きているのか、そしてなぜそれが起きているのかを説明する自律型ネットワークインテリジェンスレイヤーです。

## How

自然言語による問い合わせに対応。しかも、あなたの言語で利用できます。

## ▽ nAnalyst does the heavy lifting:

- 監視データの照会と相関分析を実施。
- 分析結果をグラフとして可視化。
- ネットワークポリシーを提案し、違反時のアラートを生成。
- 問題を解決するための具体的なアクションプランを提案(レポートを有効化)

# nAnalyst User Experience [1/2]

The screenshot displays the nAnalyst dashboard with a sidebar on the left containing navigation options: Dashboard, Monitoring, Alerts, Flows, nAnalyst (highlighted), Hosts, Maps, Interface, Policies, and Settings. The main interface shows a search bar with 'eno1' and network statistics (7.50 Kbps / 77.80 Kbps). Below the search bar, a 'HISTORY' panel is visible. The main content area features a chat window with a question: '夜間に最も多くのクエリを実行した上位10のホストはどれですか?' (Which are the top 10 hosts that performed the most queries during the night?). The chat response includes a title '夜間 (22:00 - 06:00) のDNSクエリ上位ホスト' and a table of results.

夜間に最も多くのクエリを実行した上位10のホストはどれですか?  
10:34 AM

夜間 (22:00 - 06:00) のDNSクエリ上位ホスト  
夜間に最も多くのクエリを実行した上位10のホストはどれですか?

2026年5月30日 22:00 から 2026年5月31日 06:00 までの期間で、最も多くのDNSクエリを実行したホストは以下の通りです。

| 順位 | IPアドレス          | クエリ数 |
|----|-----------------|------|
| 1  | 83.149.128.88   | 110  |
| 2  | 104.218.164.192 | 3    |
| 3  | 151.243.11.37   | 1    |
| 4  | 51.158.205.203  | 1    |
| 5  | 138.68.43.38    | 1    |
| 6  | 204.76.203.15   | 1    |
| 7  | 141.98.83.48    | 1    |

**83.149.128.88** が突出して多くのクエリ (110件) を実行しています。他のホストは1~3件です。  
10:34 AM · 22s · 84 tok/s  
Show Evidence

# nAnalystユーザーエクスペリエンス [1/2]

The screenshot displays the nAnalyst web interface. On the left is a vertical sidebar with navigation icons for Dashboard, Monitoring, Alerts, Flows, nAnalyst (highlighted), Hosts, Maps, Interface, Policies, and Settings. The main content area shows a search bar with 'Local LLM Qwen3.6-72B' selected. Below the search bar, a notification bubble asks '夜間に最も多くのクエリを実行した上位10のホストはどれですか?' (Which are the top 10 hosts that executed the most queries at night?). The search results show a card for the query '夜間に最も多くのクエリを実行した上位10のホストはどれですか?' with a timestamp of 10:34 AM. The card title is '夜間 (22:00 - 06:00) のDNSクエリ上位ホスト' (Top DNS Query Hosts at Night (22:00 - 06:00)). The text below the title states: '2026年5月30日 22:00 から 2026年5月31日 06:00 までの期間で、最も多くのDNSクエリを実行したホストは以下の通りです。' (During the period from 2026 May 30 22:00 to 2026 May 31 06:00, the hosts that executed the most DNS queries are as follows.) A table follows with columns for Rank (順位), IP Address (IPアドレス), and Query Count (クエリ数). The table lists 7 hosts, with the first host (83.149.128.88) having 110 queries. Below the table, a note states: '83.149.128.88 が突出して多くのクエリ (110件) を実行しています。他のホストは1~3件です。' (83.149.128.88 is executing many queries (110 items) prominently. Other hosts are 1-3 items.) The timestamp '10:34 AM · 22s · 84 tok/s' and a 'Show Evidence' link are also visible.

| 順位 | IPアドレス          | クエリ数 |
|----|-----------------|------|
| 1  | 83.149.128.88   | 110  |
| 2  | 104.218.164.192 | 3    |
| 3  | 151.243.11.37   | 1    |
| 4  | 51.158.205.203  | 1    |
| 5  | 138.68.43.38    | 1    |
| 6  | 204.76.203.15   | 1    |
| 7  | 141.98.83.48    | 1    |

# nAnalyst User Experience [2/2]

The screenshot displays the nAnalyst interface. On the left is a sidebar with a 'HISTORY' tab, a 'New Chat' button, and navigation options for 'All', 'Live Flows', and 'Historical'. The main chat area shows a conversation with 'Local LLM Qwen3.6-27B'. The user's message is in Japanese: '83.149.128.88 が突出して多くのクエリ (110件) を実行しています。他のホストは1~3件です。' (83.149.128.88 is executing many queries (110 items). Other hosts are 1-3 items). The AI's response includes a 'Describe Table' section explaining the user's need for the top 10 hosts and a 'SQL Query' section providing a SQL query to filter for DNS traffic (L7\_PROTO = 5) during a 'night' period (2026-05-30 22:00:00 to 2026-05-31 06:00:00) and aggregate by source IP.

HISTORY ×

+ New Chat

All Live Flows Historical

nAnalyst

🔊 夜間に最も多くの...

Local LLM Qwen3.6-27B

83.149.128.88 が突出して多くのクエリ (110件) を実行しています。他のホストは1~3件です。

10:34 AM · 22s · 84 tok/s

Hide Evidence

**Q Describe Table**

The user wants to find the top 10 hosts that executed the most queries during the night. 'Queries' typically refers to DNS queries. I need to identify the table that contains DNS flow data. The 'flows' table is the primary source. I need to check its schema to understand how to filter for DNS traffic (L7\_PROTO) and how to aggregate by host. I also need to define 'night'. Usually, this might be 22:00 to 06:00. I will first describe the 'flows' table.

**Q SQL Query**

I have the schema for the 'flows' table. I need to find the top 10 hosts that performed the most DNS queries during the night. 'Night' is typically defined as 22:00 to 06:00. I will filter for L7\_PROTO = 5 (DNS) and aggregate by source IP. I'll use the current day and the previous day to cover a full night cycle if necessary, but usually 'night' implies the most recent night. Given the current time is 2026-05-31 10:34:28, the most recent 'night' would be from 2026-05-30 22:00:00 to 2026-05-31 06:00:00. I will construct a query to count DNS flows per source IP during this window.

```
SELECT
  IPv4NumToString(IPV4_SRC_ADDR) AS src_ip,
  count(*) AS query_count
FROM flows
WHERE
  L7_PROTO = 5
  AND FIRST_SEEN >= '2026-05-30 22:00:00'
  AND FIRST_SEEN <= '2026-05-31 06:00:00'
GROUP BY src_ip
ORDER BY query_count DESC
LIMIT 10
```

# nAnalystユーザーエクスペリエンス [2/2]

The screenshot displays the nAnalyst web interface. On the left is a sidebar with a 'HISTORY' tab, a 'New Chat' button, and navigation options for 'All', 'Live Flows', and 'Historical'. The main area shows a chat window with a 'Local LLM' header (Qwen3.6-27B). The chat content includes a system message in Japanese, a user query, and an LLM response. The response contains a natural language description of the user's intent and a corresponding SQL query.

**83.149.128.88**が突出して多くのクエリ（110件）を実行しています。他のホストは1~3件です。

10:34 AM · 22s · 84 tok/s

Hide Evidence

**Q Describe Table**

The user wants to find the top 10 hosts that executed the most queries during the night. 'Queries' typically refers to DNS queries. I need to identify the table that contains DNS flow data. The 'flows' table is the primary source. I need to check its schema to understand how to filter for DNS traffic (L7\_PROTO) and how to aggregate by host. I also need to define 'night'. Usually, this might be 22:00 to 06:00. I will first describe the 'flows' table.

**Q SQL Query**

I have the schema for the 'flows' table. I need to find the top 10 hosts that performed the most DNS queries during the night. 'Night' is typically defined as 22:00 to 06:00. I will filter for L7\_PROTO = 5 (DNS) and aggregate by source IP. I'll use the current day and the previous day to cover a full night cycle if necessary, but usually 'night' implies the most recent night. Given the current time is 2026-05-31 10:34:28, the most recent 'night' would be from 2026-05-30 22:00:00 to 2026-05-31 06:00:00. I will construct a query to count DNS flows per source IP during this window.

```
SELECT
  IPv4NumToString(IPV4_SRC_ADDR) AS src_ip,
  count(*) AS query_count
FROM flows
WHERE
  L7_PROTO = 5
  AND FIRST_SEEN >= '2026-05-30 22:00:00'
  AND FIRST_SEEN <= '2026-05-31 06:00:00'
GROUP BY src_ip
ORDER BY query_count DESC
LIMIT 10
```

# Query Pipeline

- Ask nAnalyst a question using natural language:  
夜間に最も多くのクエリを実行した上位10のホストはどれですか？  
(What are the top 10 hosts that made most queries during night hours?)
- An agent is started
  - Agent gathers data using the registered functions and endpoints
  - Additional evidence is collected from flows, hosts, asset inventory, SNMP and alerts.
  - Evidence is visualized and persisted across sessions (context).

# 質問から回答までの処理フロー

- 自然言語でnAnalystに質問します：

「夜間に最も多くのクエリを実行した上位10のホストはどれですか？」

- エージェントが起動されます

- エージェントは登録済みの関数およびエンドポイントを使用してデータを収集します。
- フロー、ホスト、資産インベントリ、SNMP、およびアラートから追加の根拠情報を収集します。
- 根拠情報は可視化され、セッションをまたいでコンテキストとして保持されます。

# nAnalyst Unique Proposition [1/2]

- It easily integrates with nDPI - ntopng - nProbe
- Works with a local LLM mode, Anthropic, OpenAI and any OpenAI compatible inference server.
- Privacy and explainability in mind, no black box, interpretable results.
- Cost tracking and audit log ready (SOC2 style evidence).
- Domain specific tools embedded into ntopng: this is not a prompt or LLM wrapper.

# nAnalystの独自価値 [1/2]

- nDPI、ntopng、nProbeと容易に統合できます。
- ローカルLLMモード、Anthropic、OpenAI、およびOpenAI互換の推論サーバーに対応しています。
- プライバシー保護と説明可能性を重視して設計されており、ブラックボックスではなく、解釈可能な結果を提供します。
- コスト追跡および監査ログに対応しており、SOC2監査向けの証跡として活用できます。
- ntopngにドメイン特化型ツールを組み込んでおり、単なるプロンプトやLLMラッパーではありません。

# nAnalyst Unique Proposition [2/2]

| Differentiator         | nAnalyst   | Generic Agent Assistant |
|------------------------|--|-------------------------|
| Purpose built tools    | 25 network specific tools and counting (open source) | Generic web search      |
| Evidence transparency  | Full reasoning steps, tools called and SQL.          | Black box               |
| Audit trail            | Full audibility on actions taken                     | None                    |
| Privacy                | Fully on premise                                     | Cloud only              |
| Cost Tracking          | Per user, per model, per tool call                   | NA                      |
| ntopng and nDPI native | Yes  | No nDPI                 |

# nAnalystの独自価値 [2/2]

| 差別化要素              | nAnalyst                                       | 汎用AIエージェント |
|--------------------|--|------------|
| 目的特化型ツール           | 25種類のネットワーク特化ツールを提供<br>(オープンソース、さらに増加中)        | 一般的なWEB検索  |
| 根拠の追跡透明性           | Full reasoning steps,<br>tools called and SQL. | ブラックボックス   |
| 監査証跡               | Full audibility on actions taken               | なし         |
| プライバシー             | Fully on premise                               | クラウドのみ     |
| コスト追跡              | Per user, per model, per tool call             | NA         |
| ntopngとnDPIネイティブ統合 | 統合済み   | nDPIなし     |

# Advantages for Net- and SecOps

- Investigation time from hours to seconds.
- Less alert fatigue.
- Less false positives and noise.
- Faster incident response.
- Ability to replicate analysis by creating skills that distillate human experience into repeatable actions.

# NetOpsおよびSecOpsにおけるメリット

- 調査時間を数時間から数秒へ短縮。
- アラート疲れ（Alert Fatigue）を軽減。
- 誤検知（False Positive）やノイズを削減。
- インシデント対応を迅速化。
- 人間の経験やノウハウをスキルとして定義し、  
再活用可能なアクションへ変換することで、  
分析手法の標準化・再現を実現。

# nAnalyst Live Demo



# nAnalystライブデモ

# The Financial Reality of Network-Scale AI

- The Token Explosion

A standard corporate network generates millions of network events every minute. Feeding this high-velocity flow data to a commercial public cloud LLM via traditional APIs results in thousands of dollars in token fees daily.

- The Compute Efficiency

High-end reasoning models are built to compose poetry, debug massive codebases, and answer general knowledge. They are overly bloated for infrastructure triaging.

- The Local Optimization

ntopng works with compact, quantized local models specifically fine-tuned for networking semantics, protocol diagnostics, and security telemetry.

- The Bottom Line

Run complex automated diagnostics 24/7 on an adjacent, fixed-cost local edge engine rather than paying metered, unpredictable utility bills to cloud providers.

# ネットワーク規模AIの経済的現実

## トークン数の爆発的増加

一般的な企業ネットワークでは、毎分数百万件のネットワークイベントが生成されます。

このような大量かつ高速なフローデータを、従来のAPI経由で商用クラウドLLMへ送信すると、トークン利用料だけで1

ロに数億ドル規模のコストが発生します。

## 計算効率の課題

高性能な推論モデルは、詩の作成、大規模コードベースのデバッグ、一般知識への回答などを目的として設計されています。そのため、インフラ運用における障害切り分けやトリアージ用途には過剰な性能を持っています。

## ローカル最適化

ntopngは、ネットワーク運用の意味理解、プロトコル診断、セキュリティテレメトリ解析向けに特別にチューニングされた、コンパクトかつ量子化されたローカルモデルと連携して動作します。

## 結論

クラウドAIプロバイダーへ従量課金かつ予測困難な利用料金を支払うのではなく、

固定コストのローカルエッジ環境で24時間365日の高度な自動診断を実行できます。

# Local Architecture vs. Public Cloud AI

|                            | Public Cloud AI Pipelines  | ntopng Secure Local AI Architecture  |
|----------------------------|--|--|
| <b>Data Leakage Risk</b>   | <b>High</b> Leakage Risk (Network maps, topologies, and sensitive payloads leave the building)                 | <b>Zero</b> (All data remains contained within local memory buffers)   |
| <b>API Costs</b>           | <b>Variable &amp; Scalable</b> (Per-token costs explode under continuous network traffic telemetry ingestion). | <b>Fixed &amp; Predictable</b> (Leverages existing compute infrastructure; no operational subscription dependencies) |
| <b>Triage Latency</b>      | <b>Slow</b> (Network state must be packaged, scrubbed, exported, and uploaded to the cloud)                    | <b>Instantaneous</b> (Direct in-memory access via the local MCP server layer)  |
| <b>Regulatory Standing</b> | <b>Non-Compliant</b> (Directly violates strict regional privacy directives like GDPR, HIPAA, and NIS2)         | <b>Fully Compliant</b> (Maintains total operational isolation within corporate data boundaries)                      |

# ローカルAIアーキテクチャとパブリッククラウドAI

|          | パブリッククラウドAI   | ntopng<br>セキュアなローカルAIアーキテクチャ                               |
|----------|---|--|
| データ漏洩リスク | <b>データ漏えいリスク：高</b><br>(ネットワークマップ、トポロジ情報、および機密性の高いペイロードが組織外へ送信される)     | <b>ゼロ</b><br>(すべてのデータはローカルメモリバッファ内に保持される)                  |
| APIコスト   | <b>変動型コスト</b><br>(継続的なネットワークトラフィックテレメトリの取り込みにより、トークン利用料金が急増する)        | <b>固定かつ予測可能</b><br>(既存のコンピューティング基盤を活用し、運用上のサブスクリプション依存がない) |
| 障害切り分け時間 | <b>低速</b><br>(ネットワーク状態を収集・加工・匿名化し、クラウドへ送信する必要がある)                     | <b>瞬時</b><br>(ローカルMCPサーバーレイヤーを介したメモリ内データへの直接アクセス)          |
| 規制対応力    | <b>コンプライアンス非準拠</b><br>(GDPR、HIPAA、NIS2などの厳格な地域別プライバシー規制に直接抵触する可能性がある) | <b>完全準拠</b><br>(企業のデータ境界内で完全な運用分離を維持する)                    |

# Conclusion: True Network Understanding Achieved

- The Shift Complete  
Moving permanently away from unreadable text-heavy logging dumps to instantaneous, clear contextual analysis.
- The Vision  
Scaling your physical network footprint without expanding your engineers' mental workload or compromising data privacy.
- Unique Proposition  
nAnalyst is not another dashboard. It's the layer that finally explains your network and let you automate actions through agent pipelines.

# 結論： 真のネットワーク理解を実現

- 変革の完了

読みづらく大量のテキストで構成されたログの解析から脱却し、即座に理解できる明確なコンテキスト分析へ移行します。

- ビジョン

エンジニアの認知負荷を増やすことなく、またデータプライバシーを損なうことなく、ネットワーク基盤の拡大に対応します。

- 独自価値

nAnalystは単なるダッシュボードではありません。ネットワークで何が起きているのかを説明し、さらにエージェントパイプラインを通じてアクションの自動化を実現するレイヤーです。

