

CODEBLUE2024 OpenTalks

# AIエージェントを活用した サイバー脅威インテリジェンス生成

2024年11月14日

日本電気株式会社

サイバーセキュリティ戦略統括部

サイバーインテリジェンスグループ

# 本日のアジェンダ

1. サイバー脅威インテリジェンス
2. AIエージェント
3. NECで開発したアプリケーション
4. Advanced Search
5. ユースケース例(社内)
6. まとめ

# 本日のアジェンダ

1. サイバー脅威インテリジェンス
2. AIエージェント
3. NECで開発したアプリケーション
4. Advanced Search
5. ユースケース例(社内)
6. まとめ

# サイバー脅威インテリジェンス

インテリジェンスとは  
意思決定のために  
情報を収集・分析し得られた**知見・有用な情報**

サイバー脅威インテリジェンスとは  
サイバー脅威に関する情報を  
収集・分析することで生成された  
**知見・有用な情報**

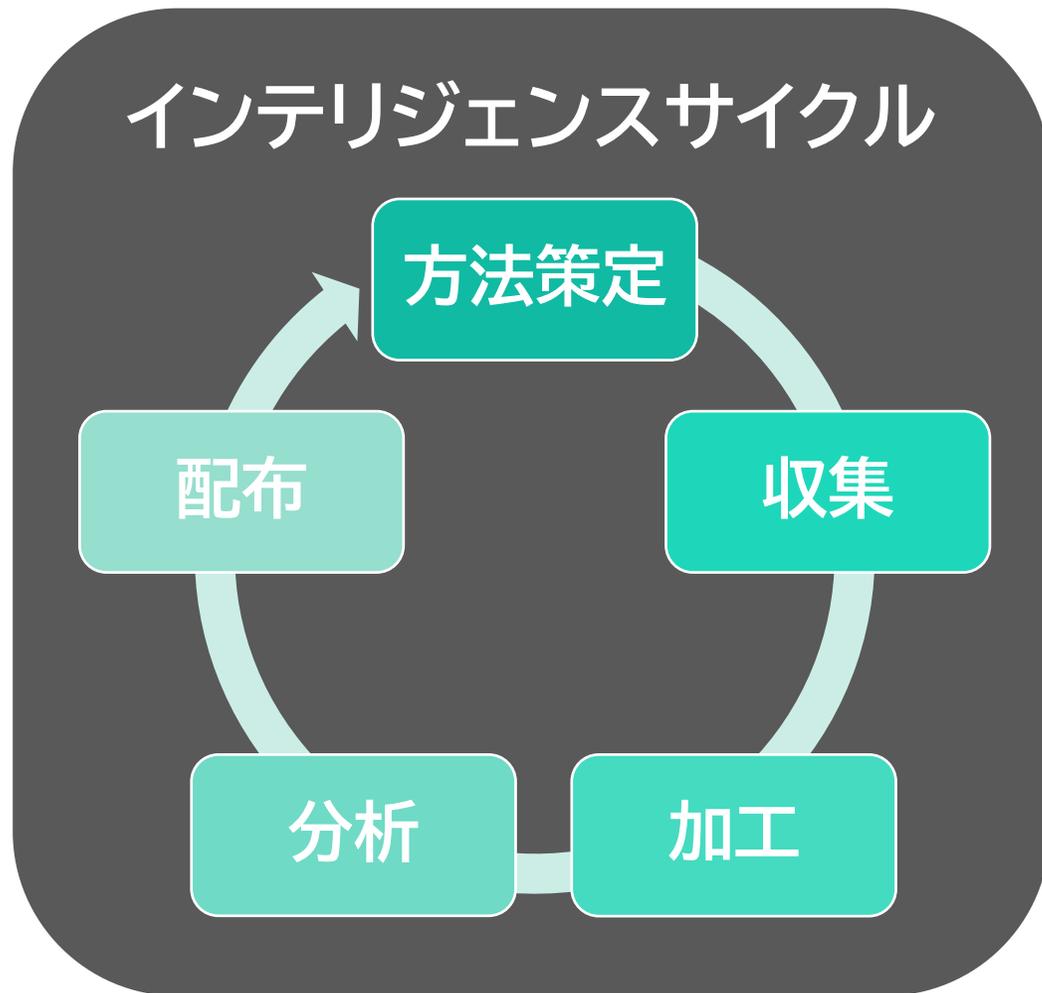
# サイバー脅威インテリジェンス

サイバー脅威インテリジェンスとは  
サイバー脅威に関する情報を  
収集・分析することで生成された  
知見・有用な情報

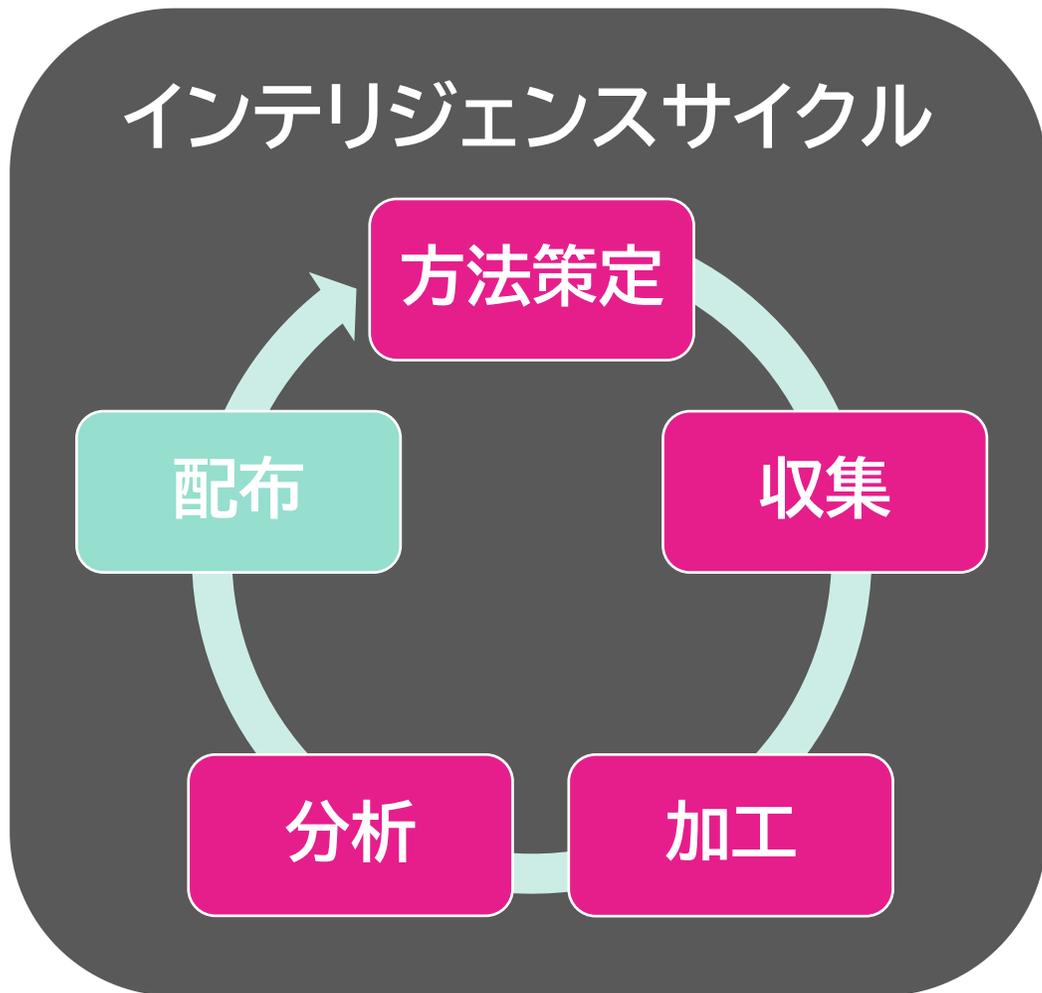


**IPアドレス・URLなどの攻撃者の侵害痕跡**(戦術インテリジェンス)  
**攻撃者の攻撃手法を活用した攻撃予測**(運用インテリジェンス)  
**世界情勢**(戦略インテリジェンス)

# サイバー脅威インテリジェンス



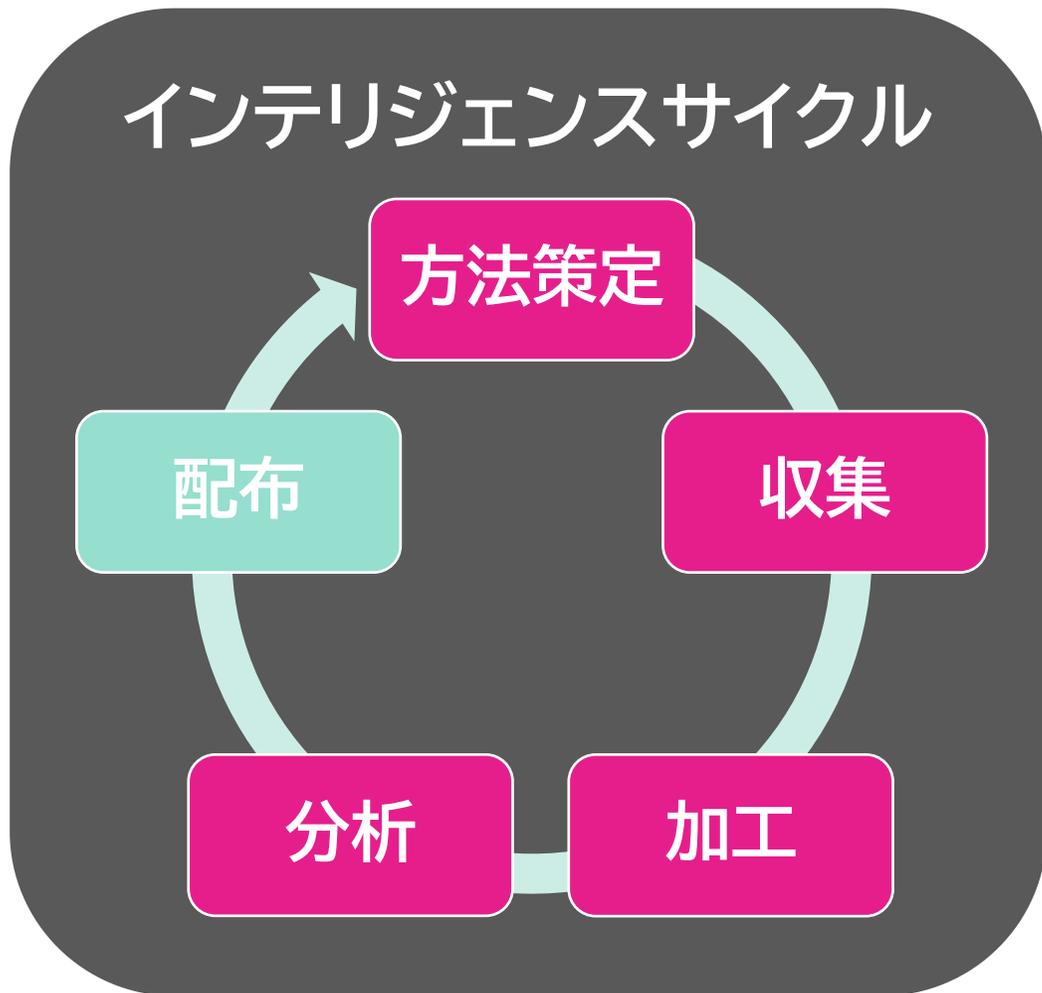
# サイバー脅威インテリジェンス



## 現状の課題

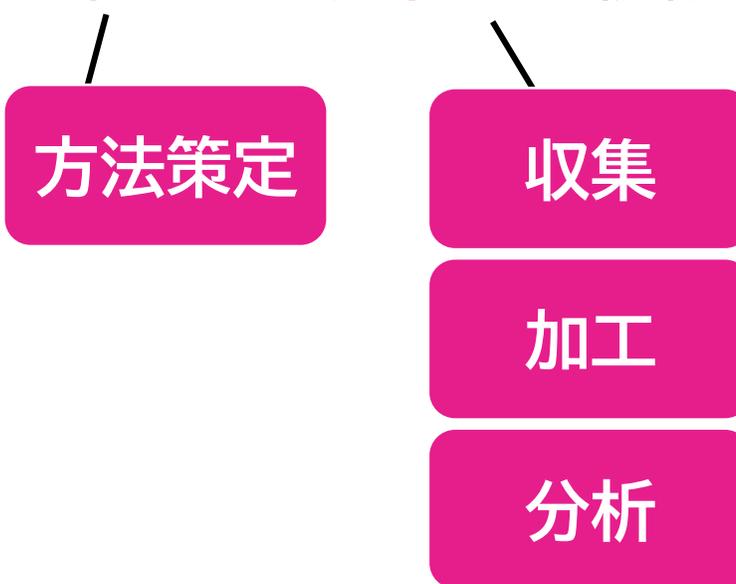
- インテリジェンスの品質がリサーチャーの調査方法や能力に依存している

# サイバー脅威インテリジェンス

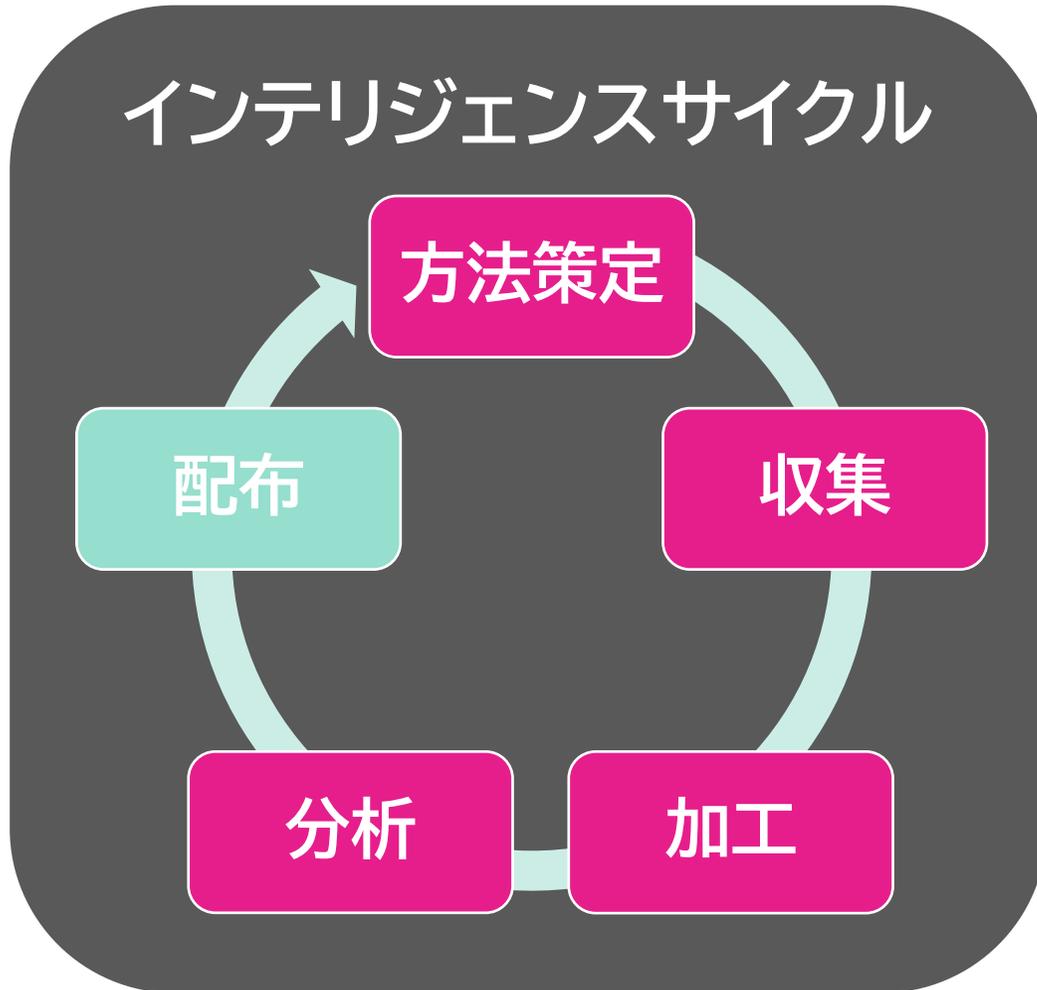


## 現状の課題

- インテリジェンスの品質がリサーチャーの調査方法や能力に依存している



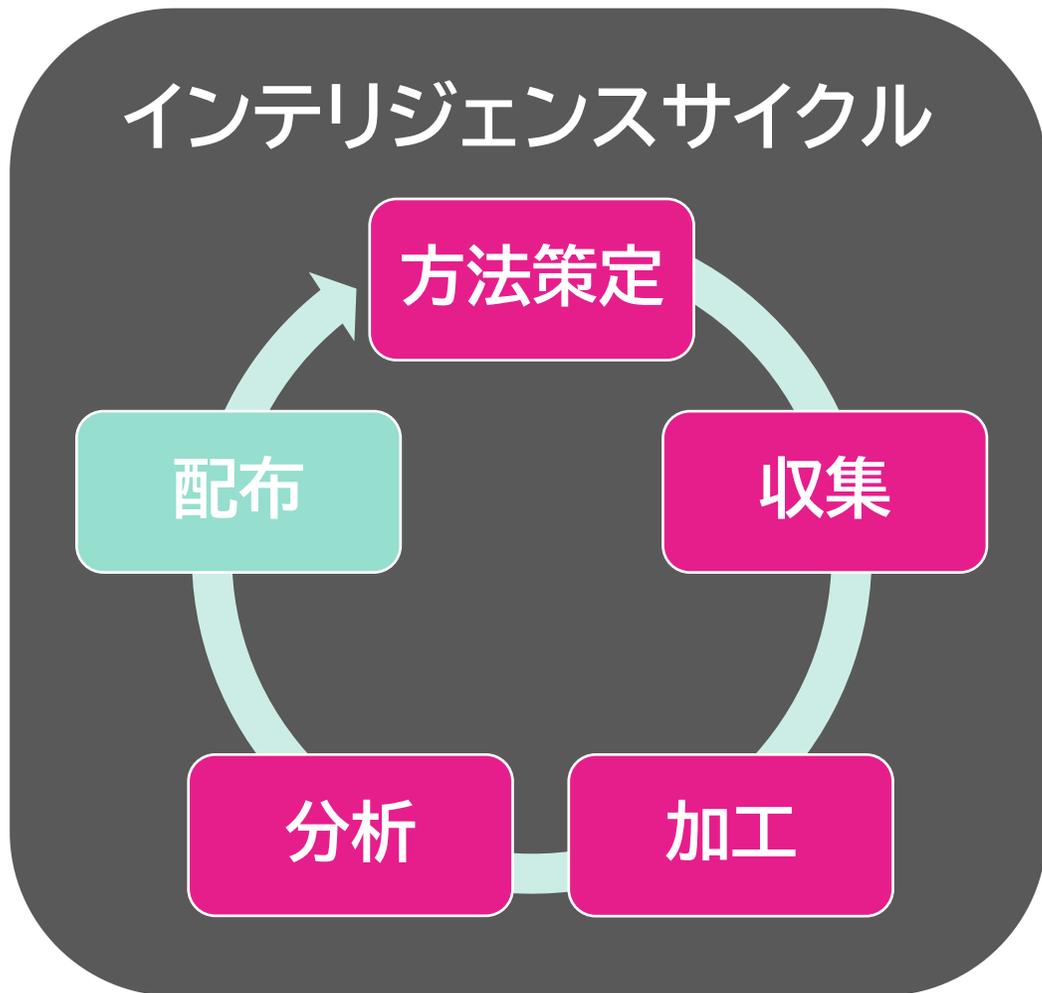
# サイバー脅威インテリジェンス



## 現状の課題

- インテリジェンスの品質がリサーチャーの調査方法や能力に依存している
- 情報**収集**や関連の高い情報の**判断**に時間がかかる

# サイバー脅威インテリジェンス

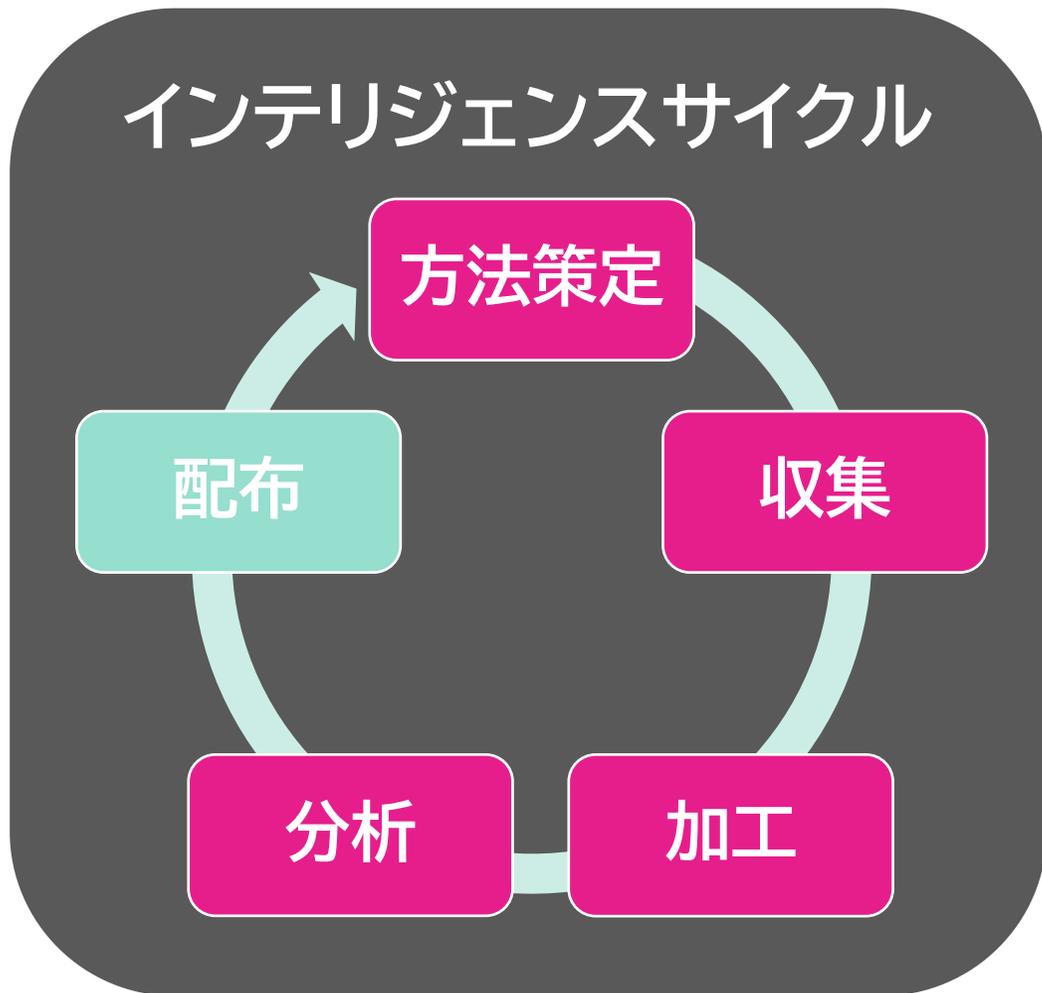


## 現状の課題

- インテリジェンスの品質がリサーチャーの調査方法や能力に依存している
- 情報**収集**や関連の高い情報の**判断**に時間がかかる



# サイバー脅威インテリジェンス



## 現状の課題

- インテリジェンスの品質がリサーチャーの調査方法や能力に依存している
- 情報収集や関連の高い情報の判断に時間がかかる



**AIエージェント**によって  
サイバー脅威インテリジェンスの  
効率化・品質向上を目指す

# 本日のアジェンダ

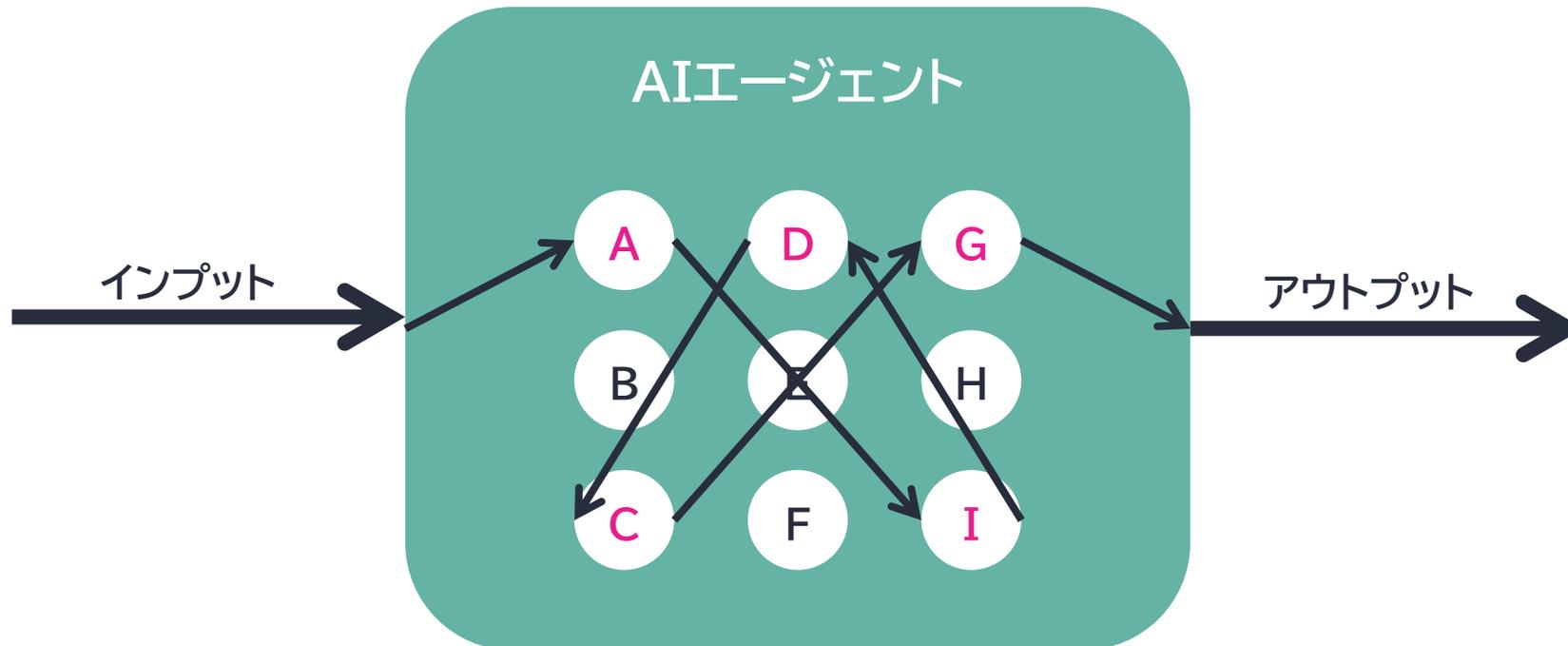
1. サイバー脅威インテリジェンス
2. AIエージェント
3. NECで開発したアプリケーション
4. Advanced Search
5. ユースケース例(社内)
6. まとめ

# AIエージェント

AIエージェントとは

最適なアクションをAIエージェントが自律的に決定し  
事前に決めた目的を達成するための枠組み

参考:<https://aws.amazon.com/jp/what-is/ai-agents/>, <https://speakerdeck.com/masahiro.nishimi/llmdekiru-shi-eru-sheng-cheng-aieziento?slide=9>



# 本日のアジェンダ

1. サイバー脅威インテリジェンス
2. AIエージェント
- 3. NECで開発したアプリケーション**
4. Advanced Search
5. ユースケース例(社内)
6. まとめ

# NECで開発したアプリケーション

## アプリケーション概要

- **AIエージェント**を活用したアプリケーション
- サイバー脅威インテリジェンスを**効率的に生成**する
- LLM(GPT3.5/GPT4/GPT4o)を処理の一部として活用

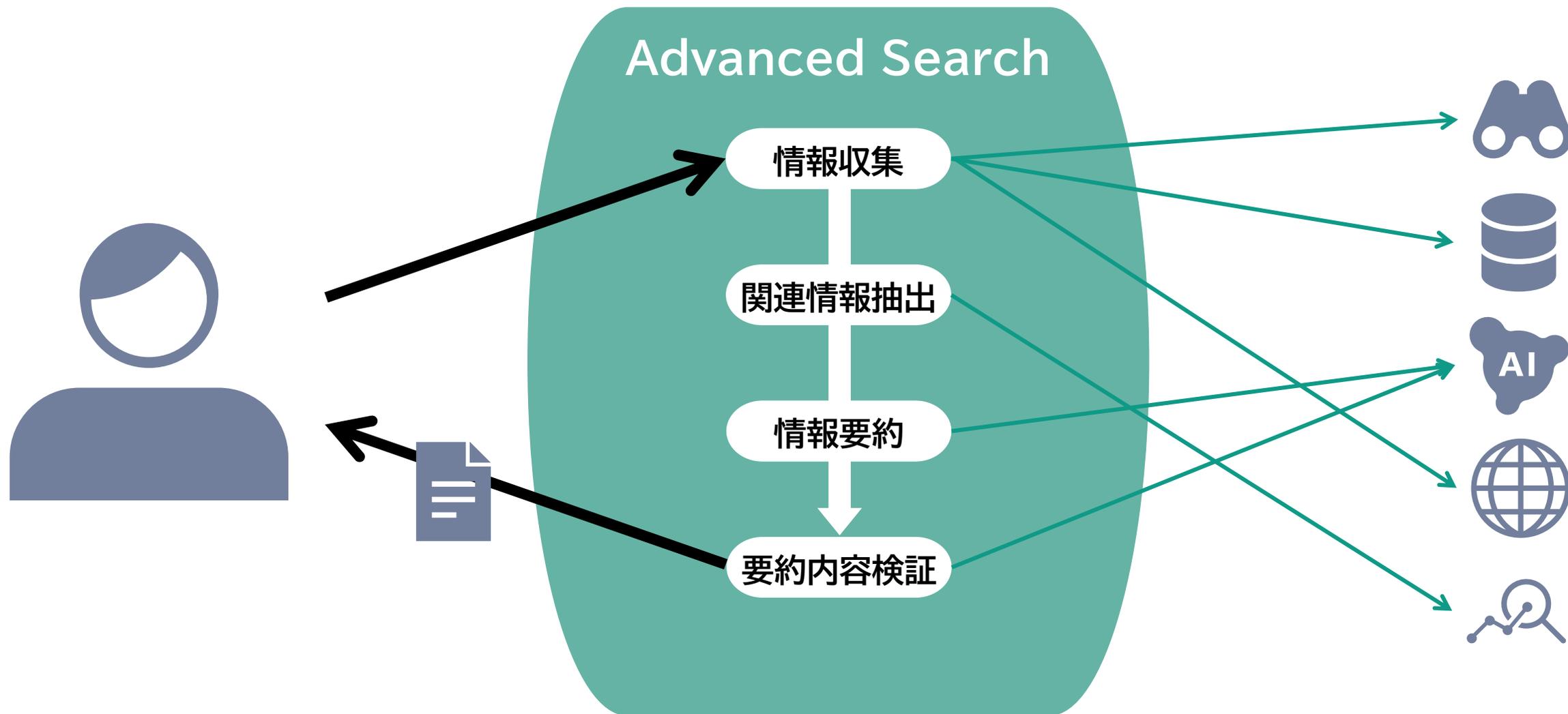
## 機能

Summarize	:サイバーニュースや調査レポートの <b>抽出・要約</b> ※URLやテキストのインプットに対し回答
<b>Advanced Search</b>	:サイバー脅威情報の <b>収集・抽出・要約・分析</b> ※自然言語の質問に対し回答

# 本日のアジェンダ

1. サイバー脅威インテリジェンス
2. AIエージェント
3. NECで開発したアプリケーション
4. Advanced Search
5. ユースケース例(社内)
6. まとめ

# Advanced Search



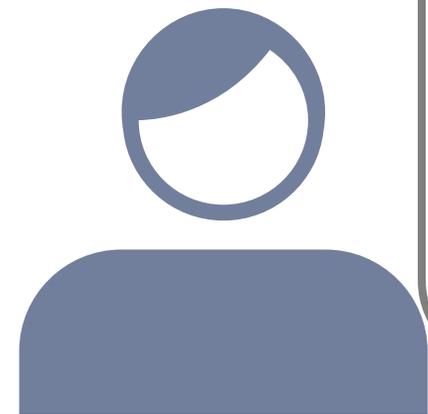
# Advanced Search

## Advanced Search

### ポイント

- RAGによりリアルタイム情報を収集
- 生成AIを要約や検証で活用することでハルシネーションを低減

要約内容検証



# Advanced Search

## Advanced Search

### ※注意点

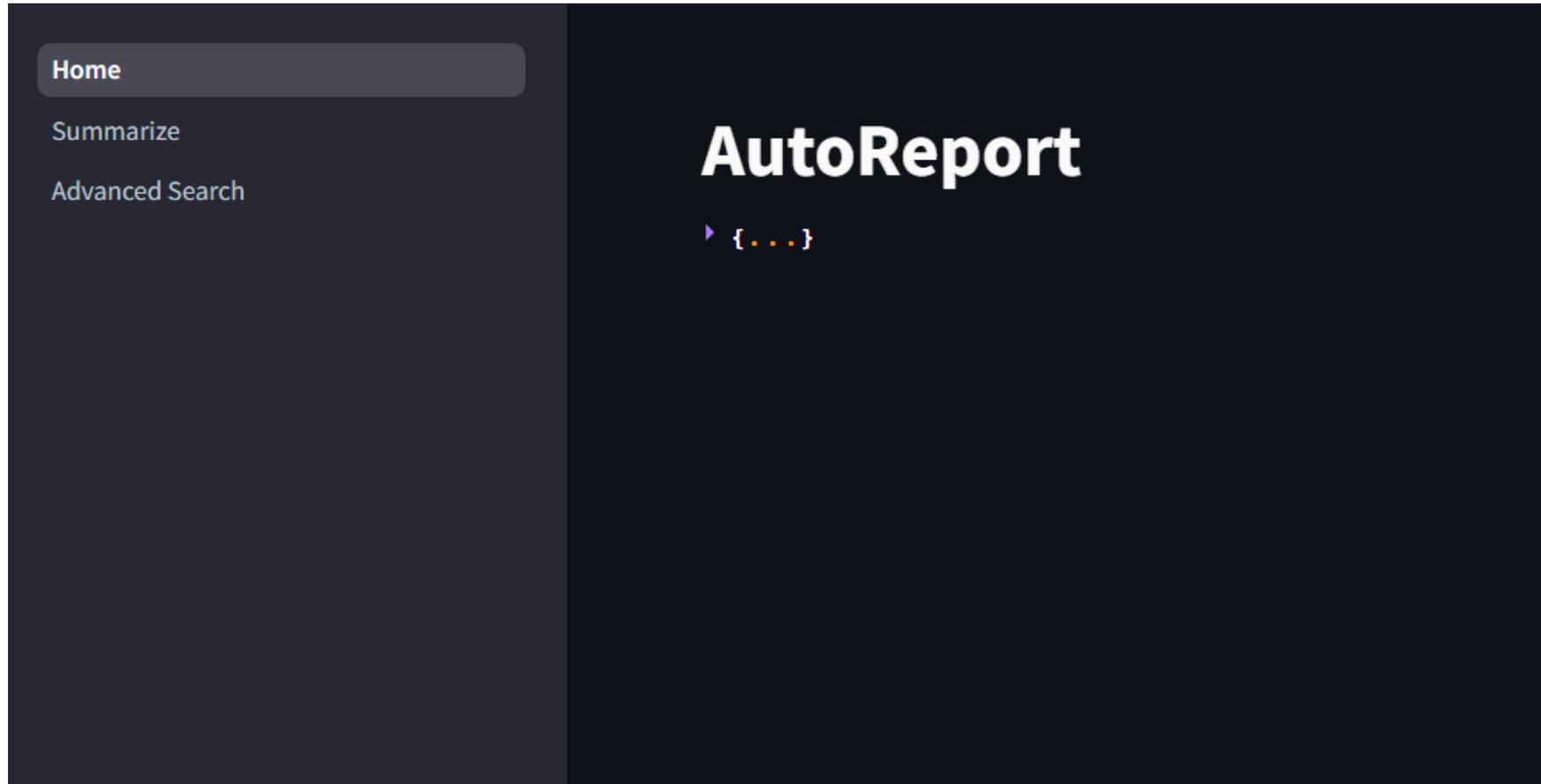
本アプリケーションはAIエージェントによる  
アプリ開発の最初の取り組みとして、現状、  
**最適なアクションを事前に定義**している

要約内容検証



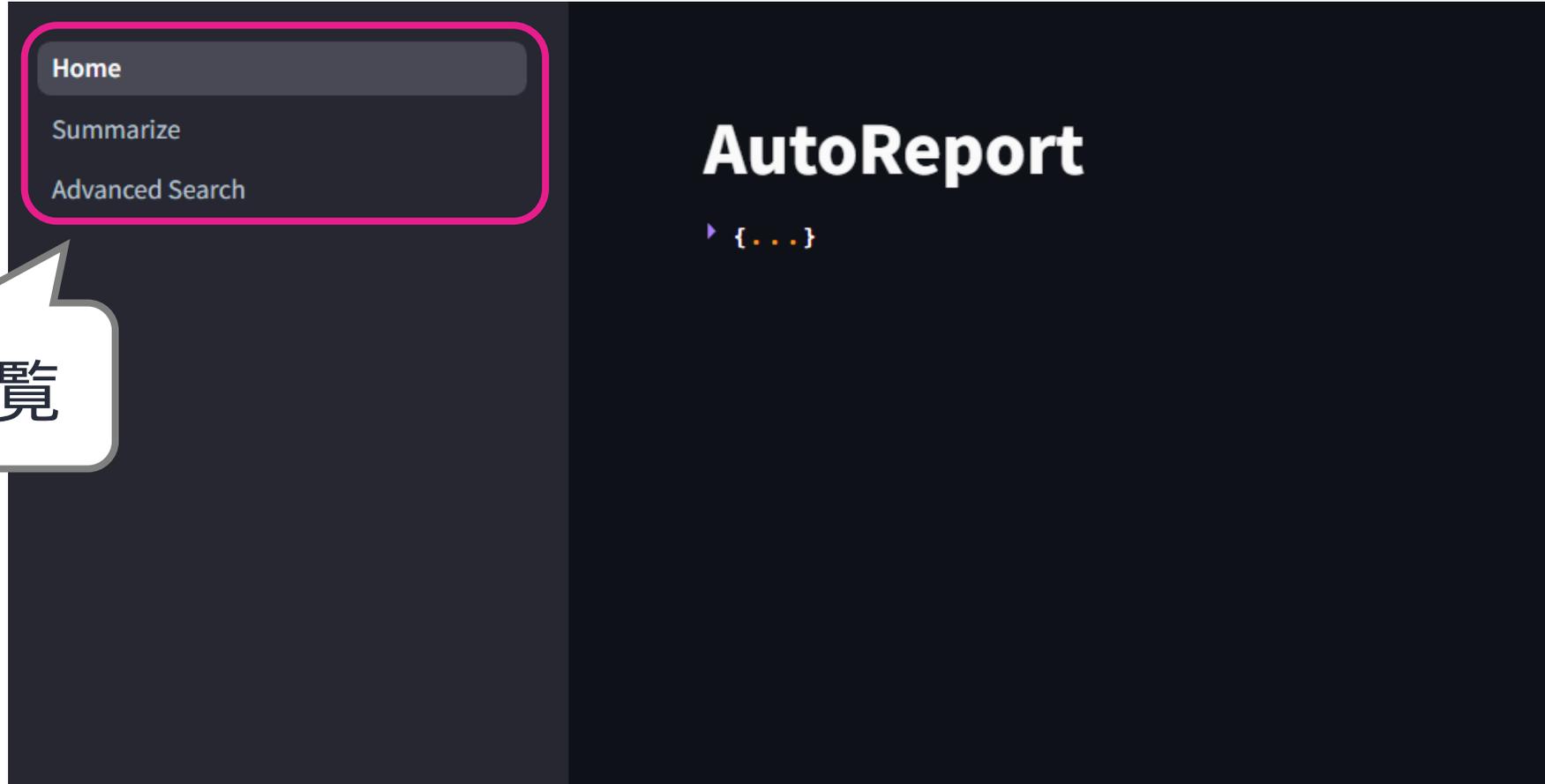
# Advanced Search

## TOP画面



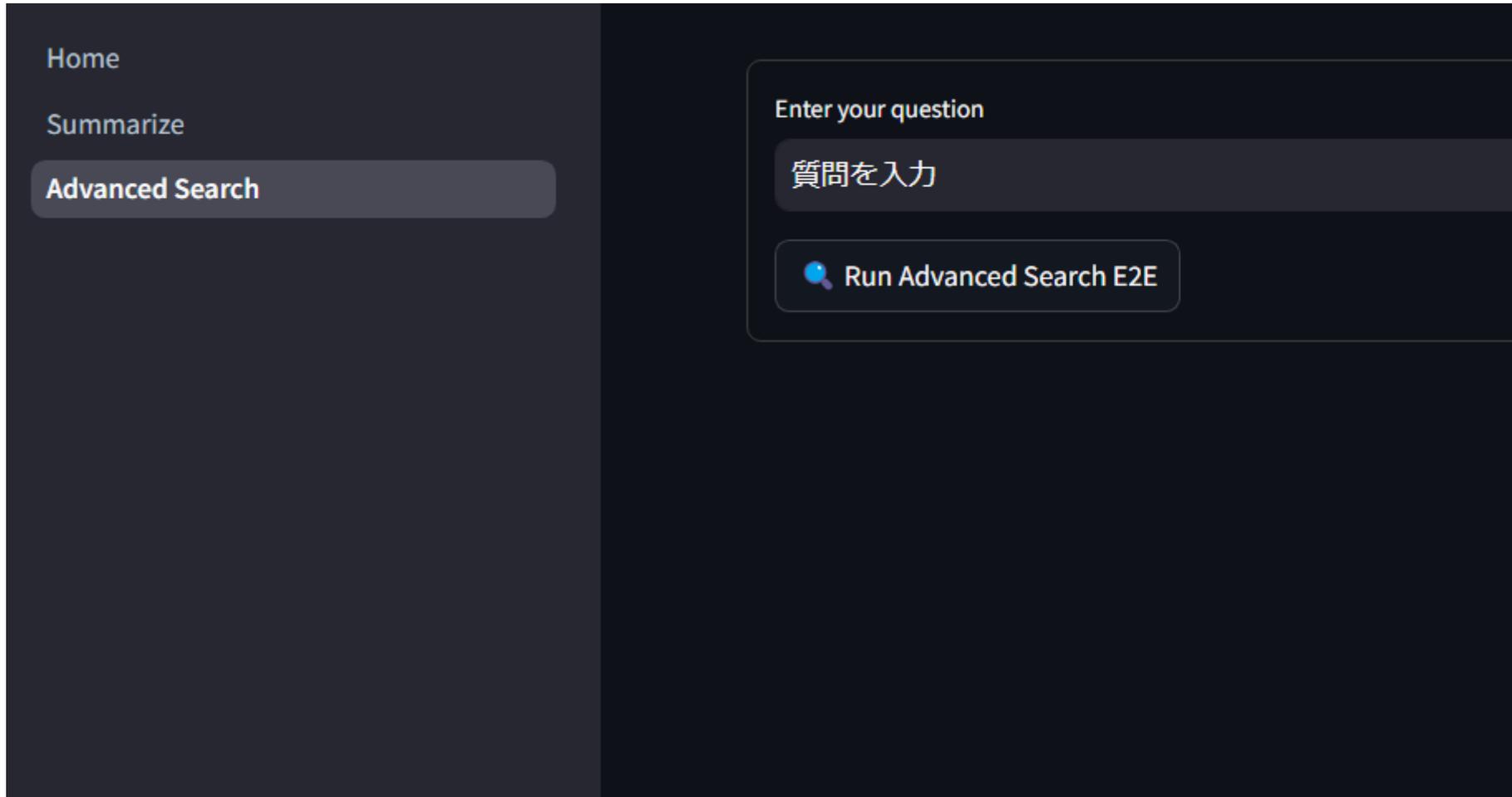
# Advanced Search

## TOP画面



# Advanced Search

## Advanced Search画面



# Advanced Search

## 質問:2023 年のサイバー攻撃の種類はどのくらいですか？

### 2023 年の主なサイバー攻撃

の種類 2023 年の主なサイバー攻撃の種類には、DDoS、フィッシング、ランサムウェア、暗号通貨関連の攻撃、内部脅威、マルウェア、データ侵害、さまざまな ID ベースの攻撃が含まれます。これらの中には、明確な傾向と新しい展開が見られました。

1. **DDoS 攻撃:** 特にアプリケーション層の DDoS 攻撃が 15% 増加しました。
2. **フィッシング:** 依然として蔓延しており、組織の 57% が毎週または毎日フィッシング攻撃を受けています。FBI の IC3 はフィッシング詐欺に重点を置いており、2023 年の全苦情の約 34% を占めています。
3. **ランサムウェア:** 2023年3月の発生件数は前年比でほぼ倍増しました。
4. **暗号通貨関連の攻撃:** 2023 年第 1 四半期に 600% 増加し、特に暗号通貨企業を標的としています。
5. **内部脅威:** 意図的および非意図的を問わず、すべての侵害の 43% を占めています。
6. **マルウェア:** コンピュータの機能を盗んだり、暗号化したり、乗っ取ったりする能力があることで知られており、フィッシングキャンペーンや詐欺メッセージを通じて侵入されることが多いです。
7. **データ侵害:** オーストラリアの重要なインフラに影響を及ぼすサイバーセキュリティインシデント全体の 13% を占めています。
8. **アイデンティティベースの攻撃:** SIM スワッピング、MFA バイパス、盗まれた API キーの使用などの戦術により、大幅な増加が見られました。

侵害されたアカウント、侵害されたインフラストラクチャ、ビジネスメール詐欺 (BEC)、サービス拒否 (DoS) 攻撃などの追加の種類は、2023 年のサイバー脅威の多様な状況にさらに貢献しました。

**出典:** [' <https://www.varonis.com/blog/cybersecurity-statistics> ', ' <https://www.varonis.com/blog/data-breach-statistics> ', ' <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023> ', ' <https://www.proofpoint.com/us/resources/threat-reports/human-factor> ', ' <https://blog.checkpoint.com/research/checkpoint-research-2023-the-year-of-mega-ransomware-attacks-with-unprecedented-impact-on-global-organizations/> ', ' <https://www.fbi.gov/news/stories/elder-fraud-in-focus> ', ' <https://www.crowdstrike.com/global-threat-report/> ']

# Advanced Search

## 質問: USAの大統領選挙で懸念すべきサイバー攻撃は？

### 米国大統領選挙へのサイバー脅威

2024年の米国大統領選挙をめぐるには、さまざまな攻撃タイプ、手法、標的、脅威アクターが重大なリスクをもたらすサイバー脅威がいくつか特定されています。

1. **偽情報キャンペーン:** ロシア、中国、イランなどの外国の脅威アクターは、生成型人工知能 (AI) を利用して誤解を招くコンテンツを拡散しています。これらのキャンペーンは、国家レベルのメディアを模倣し、有償のインフルエンサーを使用することで、民主的プロセスの完全性に疑問を投げかけ、党派間の不和を煽ることを目的としています。(出典: CISA、FBI)
2. **ブルートフォース攻撃とパスワードスプレー攻撃:** イランのサイバー攻撃者は2023年10月以降、これらの手法を使用して重要なインフラ分野のユーザーアカウントを侵害しており、継続的な警戒の必要性が浮き彫りになっています。(出典: CISA)

3. **フィッシング:** イランの攻撃者は、米国大統領選挙運動を標的として、フ

8. **データの盗難と漏洩:** Ransomed.vc シンジケートなどの脅威アクターは、個人識別情報 (PII) を盗み、漏洩させて有権者の信頼を損ないます。(出典: Resecurity)

9. **商用マルウェア:** 選挙関連のIT インフラストラクチャや有権者登録システムを標的とした、悪意のある活動のための PowerShell の使用や、パッチが適用されていない脆弱性の悪用など。(出典: CISA)

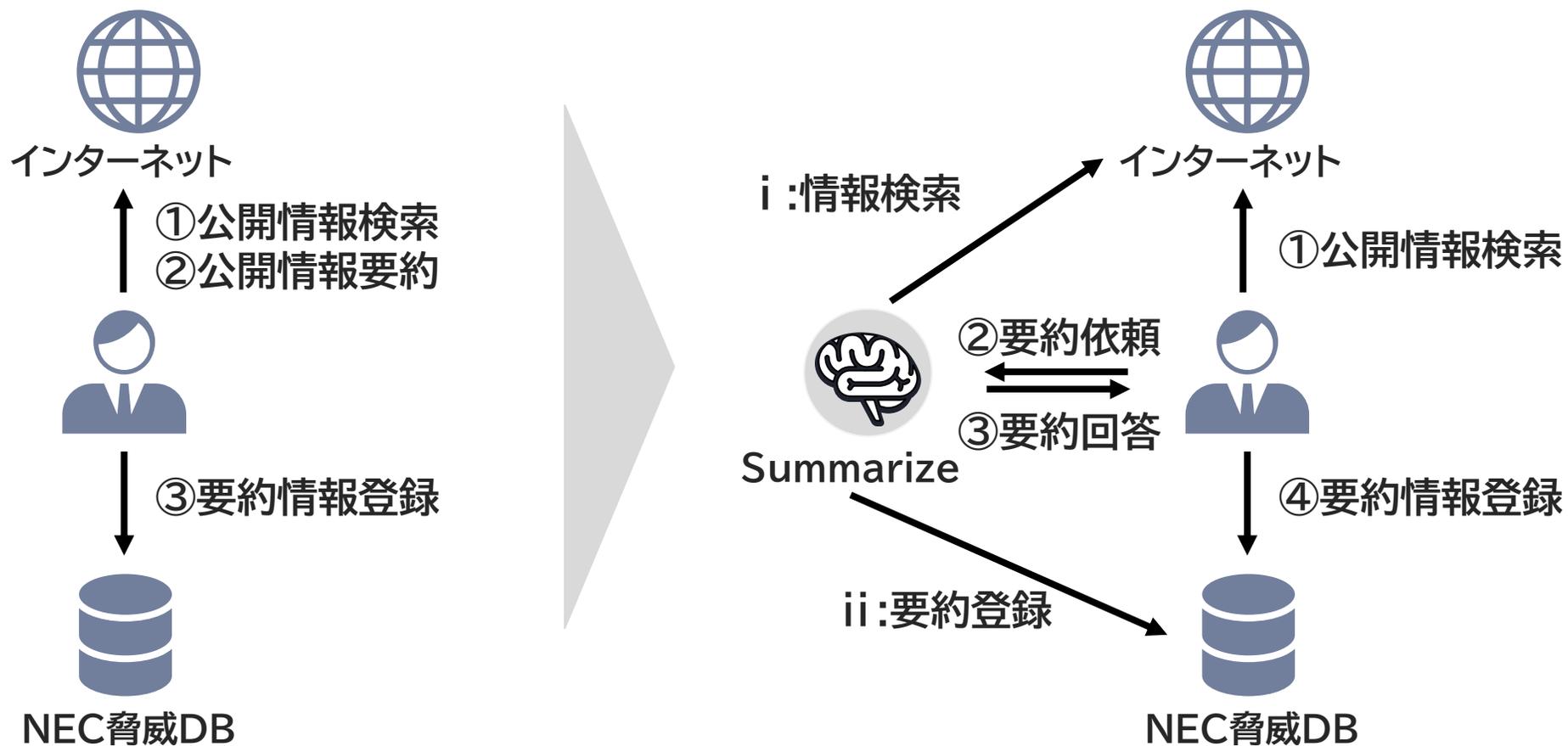
出典: [' <https://www.cisa.gov/> ', ' <https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us> ', ' <https://www.cisa.gov/topics/election-security/protect2024> ', ' <https://www.cisa.gov/news-events/news/fbi-and-cisa-issue-public-service-announcement-warning-tactics-foreign-actors-targeting-2024-us-federal-elections-incidents> ']

# 本日のアジェンダ

1. サイバー脅威インテリジェンス
2. AIエージェント
3. NECで開発したアプリケーション
4. Advanced Search
5. ユースケース例(社内)
6. まとめ

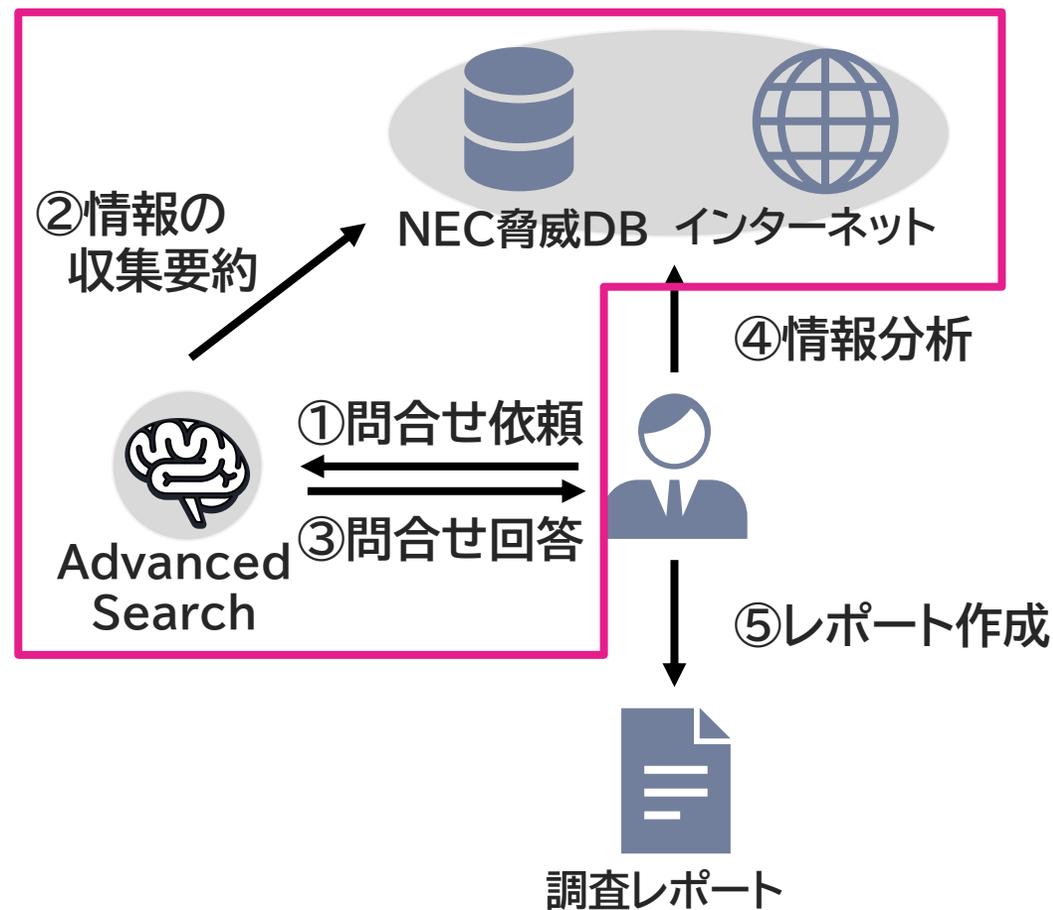
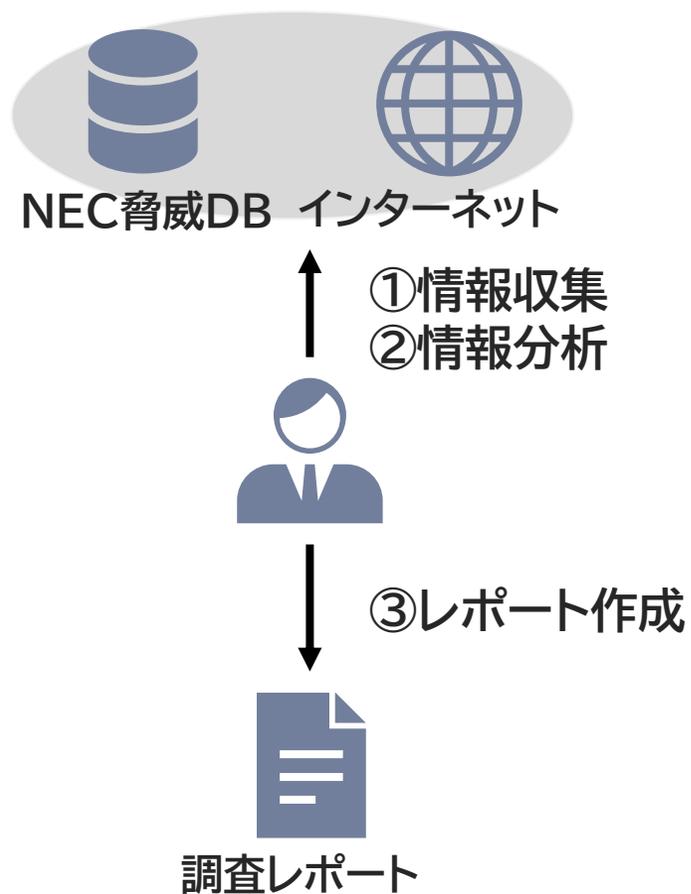
# ユースケース例(Summarize)

## 脅威情報要約業務の業務時間を約50%削減



# ユースケース例(Advanced Search)

特定テーマ調査業務の脅威情報収集時間を約**50%削減**



# 本日のアジェンダ

1. サイバー脅威インテリジェンス
2. AIエージェント
3. NECで開発したアプリケーション
4. Advanced Search
5. ユースケース例(社内)
6. まとめ

# まとめ

サイバー脅威インテリジェンスの生成には  
個人の能力差や時間的な課題がある

NECはAIエージェントによって業務の効率化を目指しており  
AIエージェントは生成AIの課題を低減できる可能性がある

NECでAIエージェント化を目指し開発したアプリケーションにより  
脅威情報要約業務や特定テーマの調査業務の情報収集時間を  
約50%削減した

本取り組みについて2024年3月のNEC技報で公開している  
➤ NEC技報-サイバー脅威インテリジェンス生成自動化  
<https://jpn.nec.com/techrep/journal/g23/n02/230207.html>



**NEC**

\Orchestrating a brighter world