

Hardening Designers Conference 2024 Day2

# AIエージェントによる サイバー脅威インテリジェンス生成

2024年7月5日(金)

NEC 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

# \Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、  
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

# 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機能
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

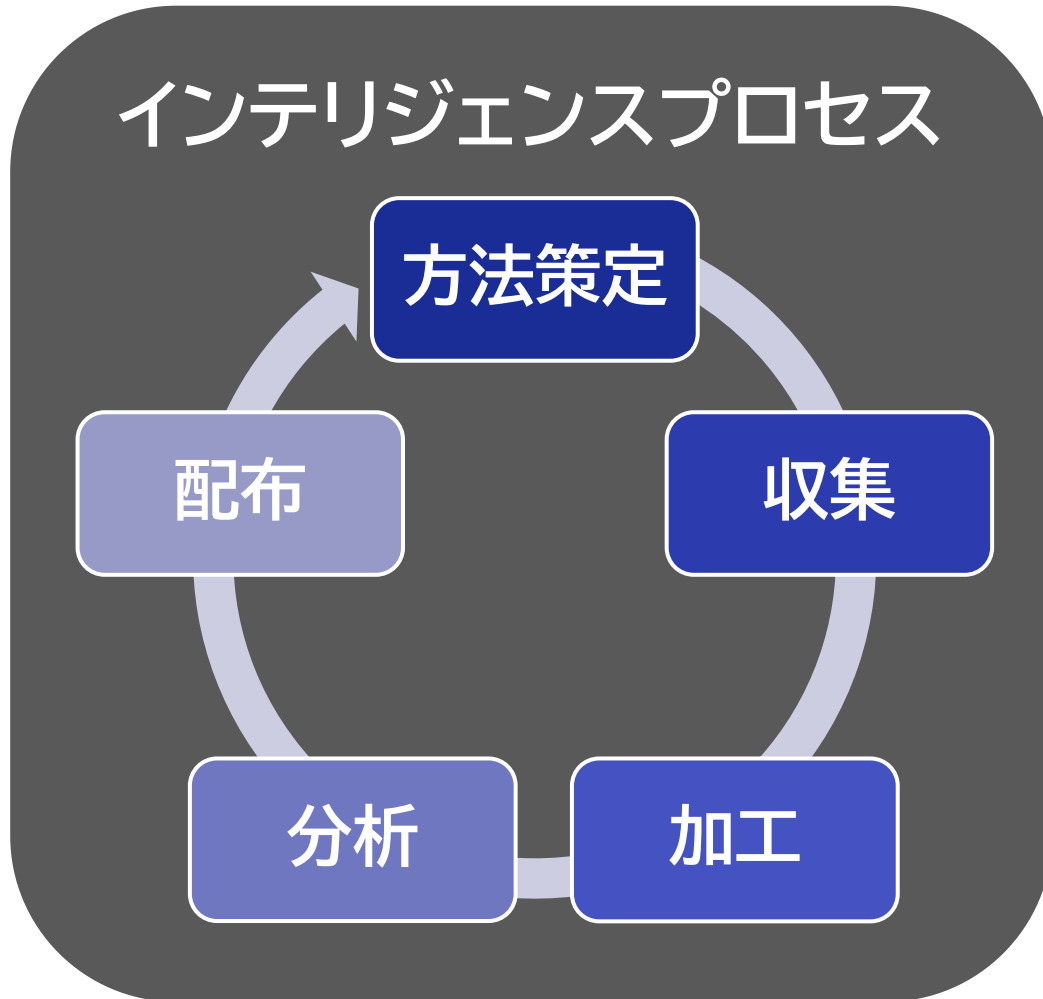
# サイバー脅威インテリジェンス

---

サイバー脅威インテリジェンスとは

→サイバー攻撃に関する情報を収集・分析する

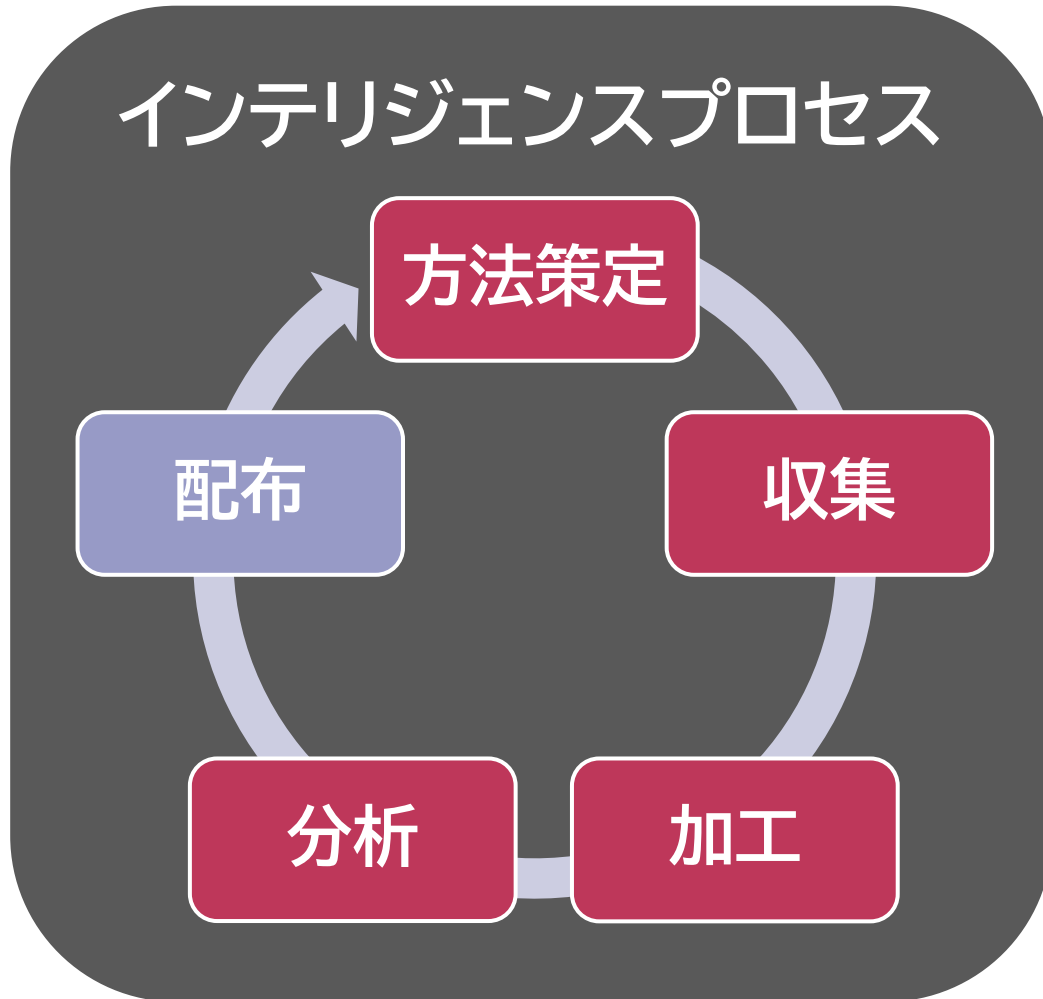
# サイバー脅威インテリジェンス



## 現状の課題

- インテリジェンスの品質が作業者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作業者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

生成AIを活用した  
AIエージェントで  
インテリジェンス業務の  
効率化・品質向上を目指す

# AIエージェント



# AIエージェント

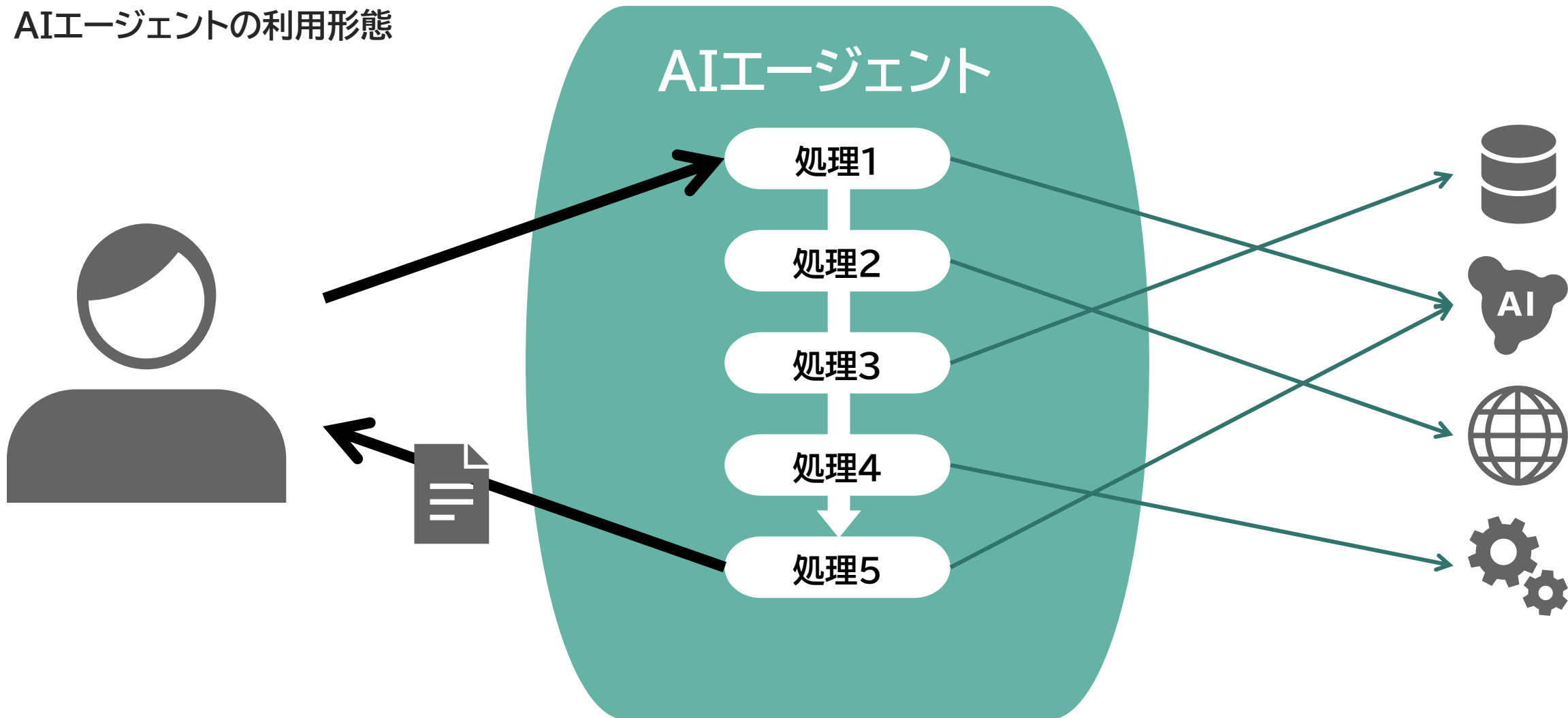
---

## AIエージェントとは？

→特定の業務に特化した処理を生成AI/LLMによって決定したコードまたはメカニズムを指します。

# AIエージェント

## AIエージェントの利用形態

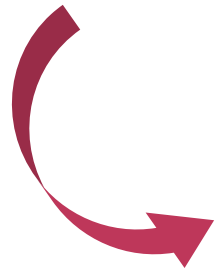


# AIエージェント

なぜAIエージェントか？

→ 生成AIの課題

- ハルシネーション(嘘の回答)
- 最新情報の読み込み



**AIエージェントで生成AIの課題を解決**

# NECで開発したアプリケーション

# NECで開発したアプリケーション

## アプリケーション概要

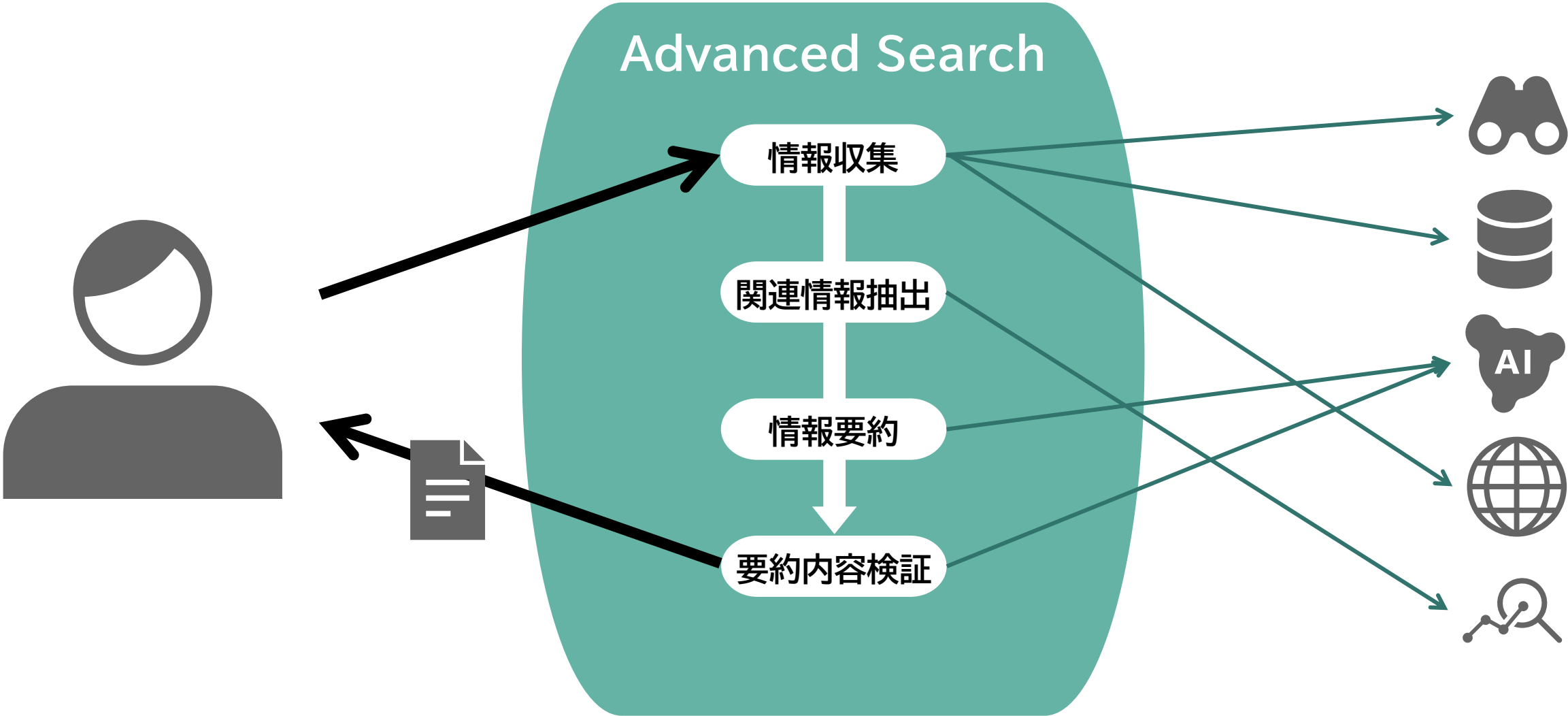
→サイバー脅威インテリジェンス業務を効率化するため  
NEC欧州研究所と協力し開発中のAIエージェント

## 機能

• Summarize	:情報要約機能・情報抽出機能
• Advanced Search	:サイバー脅威情報の収集・分析要約機能

# Advanced Search機能

# Advanced Search機能



# Advanced Search機能

## TOP画面

The screenshot shows a dark-themed user interface. On the left is a vertical sidebar menu with the following items: 'Main Page' (highlighted with a dark background), 'Summarize', 'Advanced Search', 'Feeds', 'Timeline', 'TICP Posting monitoring', 'TICP Deduplication check', and 'TICP Async queue monitoring'. Below the menu is a small upward-pointing arrow. The main content area on the right features the text 'AutoReport - Main page' in a large, bold, white font, followed by a red balloon icon with a white string.



# Advanced Search機能

## TOP画面

Main Page

Summarize

Advanced Search

Feeds

Timeline

TICP Posting monitoring

TICP Deduplication check

TICP Async queue monitoring

AutoReport - Main page 

Main page 

機能一覧

# Advanced Search機能

## Advanced Search画面

The screenshot displays the 'Advanced Search' interface. On the left is a dark sidebar menu with the following items: 'Main Page', 'Summarize', 'Advanced Search' (highlighted with a red border), 'Feeds', 'Timeline', 'TICP Posting monitoring', 'TICP Deduplication check', and 'TICP Async queue monitoring'. The main content area is titled 'AutoReport - Advanced Search' and contains the following fields and controls:

- Input field: 'Insert query keyword (Google Search style)'
- Radio buttons: 'Select sources for Advanced Search' with options 'AutoReport Sources' (selected) and 'TICP knowledge base'.
- Input field: 'Insert question (e.g. What is Grandoreiro malware?)'
- Radio buttons: 'Search mode' with options 'Q&A' and 'Research' (selected).
- Button: 'Query'

# Advanced Search機能

## AutoReport - Advanced Search

Insert query keyword (Google Search style)

Select sources for Advanced Search

AutoReport Sources  TICP knowledge base

Insert question (e.g. What is Grandoreiro malware?)

Search mode

Q&A  Research

Query

インターネット上で情報を  
検索するためのキーワードを入力

質問内容を入力

# Advanced Search機能

## インプット

Insert query keyword (Google Search style)

Emotet

Select sources for Advanced Search

AutoReport Sources  TICP knowledge base

Insert question (e.g. What is Grandoreiro malware?)

Emotet malwareとは何ですか?

Search mode

Q&A  Research

Query

## アウトプット

### Final Answer

Emotetは、他のマルウェアのダウンローダーやドロPPERとして機能する高度なトロイの木馬で、フィッシングメールの添付ファイルやリンクを通じて広がります。一度インストールされると、犯罪者が追加の有害なソフトウェアをコンピュータにロードすることを可能にします。Emotetは、ネットワーク全体に感染を広げる「ワームのような」特性と、その能力を逐次進化させ更新するためのモジュラー型のダイナミックリンクライブラリを使用するため、対処が難しいとされています。また、Emotetは、自動起動レジストリキーとサービスを含む、持続性を維持するためのいくつかの方法を持っています。さらに、Emotetは仮想マシンに対応しており、仮想環境で実行されると偽の指標を生成することができます。Emotetは、銀行、電子商取引、医療、学術、政府、技術などの重要な産業を対象とするマルウェアの一種です。

==== Refs =====

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a>
- <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>
- <https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware>
- <https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation>
- <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor>
- <https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121>
- <https://unit42.paloaltonetworks.com/new-emotet-infection-method/>
- <https://unit42.paloaltonetworks.com/emotet-thread-hijacking/>
- <https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/>

# Advanced Search機能

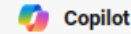
## Advanced Search機能とCopilotの比較(質問:Emotetとは何か?)

### Final Answer

Emotetは、他のマルウェアのダウンローダーやドロPPERとして機能する高度なトロイの木馬で、フィッシングメールの添付ファイルやリンクを通じて広がります。一度インストールされると、犯罪者が追加の有害なソフトウェアをコンピュータにロードすることを可能にします。Emotetは、ネットワーク全体に感染を広げる「ワームのような」特性と、その能力を逐次進化させ更新するためのモジュラー型のダイナミックリンクライブラリを使用するため、対処が難しいとされています。また、Emotetは、自動起動レジストリキーとサービスを含む、持続性を維持するためのいくつかの方法を持っています。さらに、Emotetは仮想マシンに対応しており、仮想環境で実行されると偽の指標を生成することができます。Emotetは、銀行、電子商取引、医療、学術、政府、技術などの重要な産業を対象とするマルウェアの一種です。

==== Refs =====

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a>
- <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>
- <https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware>
- <https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation>
- <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor>
- <https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121>
- <https://unit42.paloaltonetworks.com/new-emotet-infection-method/>
- <https://unit42.paloaltonetworks.com/emotet-thread-hijacking/>
- <https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/>



Copilot

✓ 回答を生成しています...

\*\*エモテット (Emotet) \*\*は、2014年に発見された非常に強力な感染力を持つマルウェアです。このマルウェアは、不正なメールの添付ファイルを介して感染を広げます。以下に、エモテットの特徴と攻撃手法、対策について詳しく解説します。

### エモテットの特徴・攻撃手法

#### • 正規メールの返信を偽装する巧妙な攻撃手法:

1. Emotetが侵入した端末のOutlookから、メール情報を盗みます。
2. 取引先や顧客になりすまし、マクロ付きのOfficeファイルを添付した偽装メールを送信します。
3. 偽装メールのタイトルに「Re:」を付け、業務関係の文面を装って受信者にOfficeファイルの開封を促します。
4. Officeファイルを開封すると、「コンテンツの有効化」を要求され、受信者が実行することで端末にEmotetが侵入します。

#### • プラットフォームとしての役割:

- Emotetは単体で動作するのではなく、他のマルウェアを感染させるプラットフォームとしての役割を持ちます。
- ウイルス対策ソフトに検知されないマクロなど正規の機能を悪用して端末に侵入するため、感染しやすい特性があります。

#### • 感染拡大と他のマルウェアへの感染:

- Emotetは自己増殖が可能な「ワーム」機能を持ち、社内ネットワークへ感染を広げる恐れがあります。
- 他のマルウェアをダウンロード・実行してしまうため、ランサムウェアなどの強力なマルウェアに感染するリスクも高まります。

詳細情報

1 cybersecurity-jp.com

2 nttpc.co.jp

3 hitachi-systems-es.co.jp

4 skyseaclientview.net

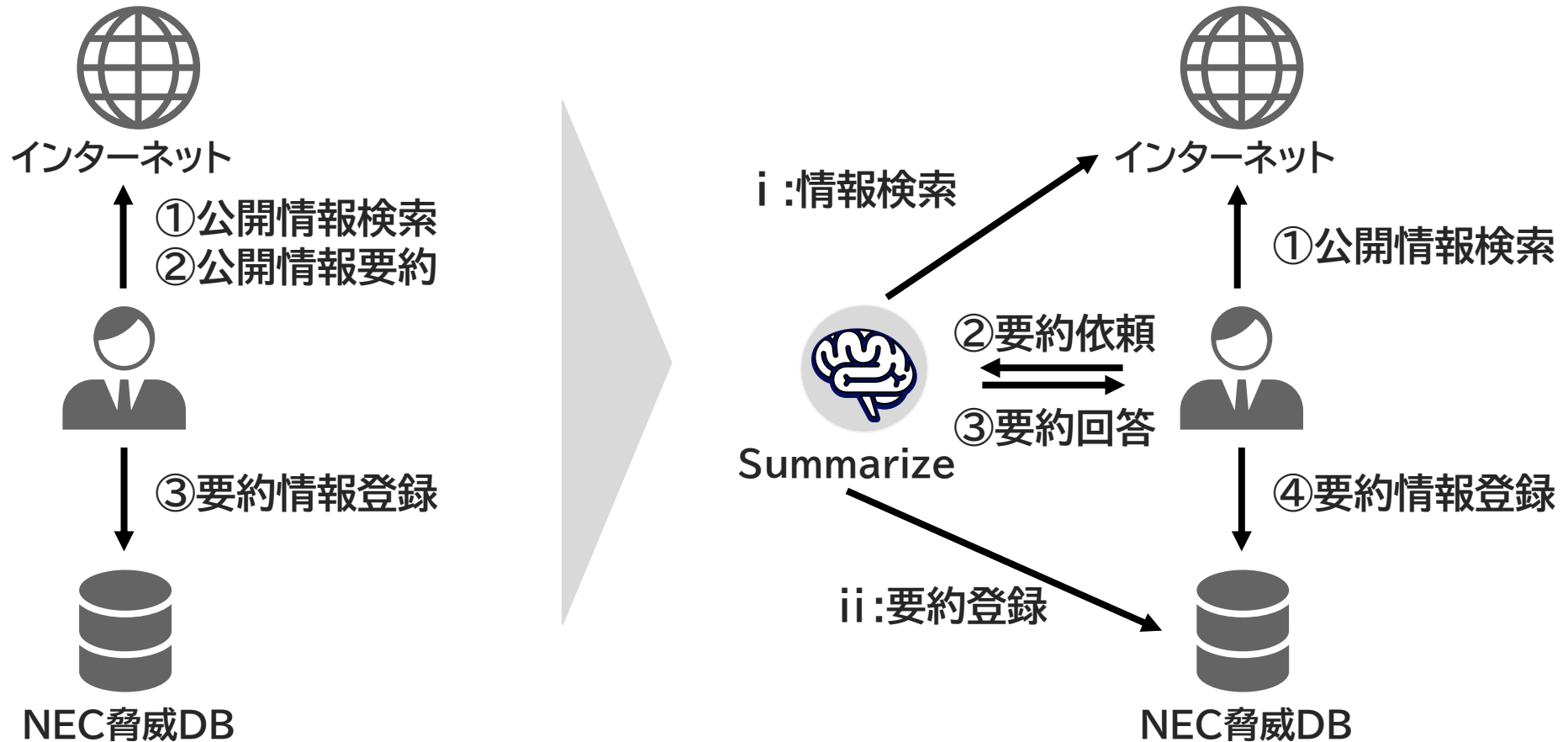
5 ntt.com

← 表示を減らす

# ユースケース例(社内)

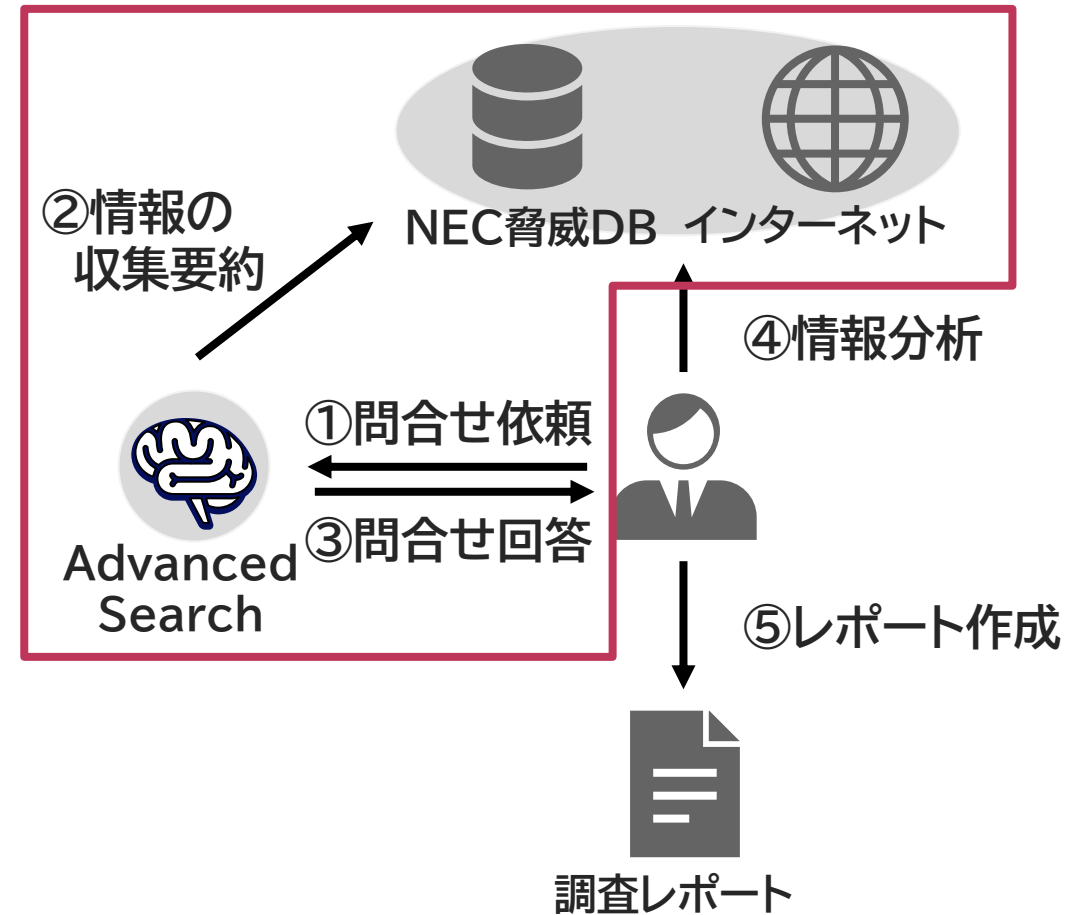
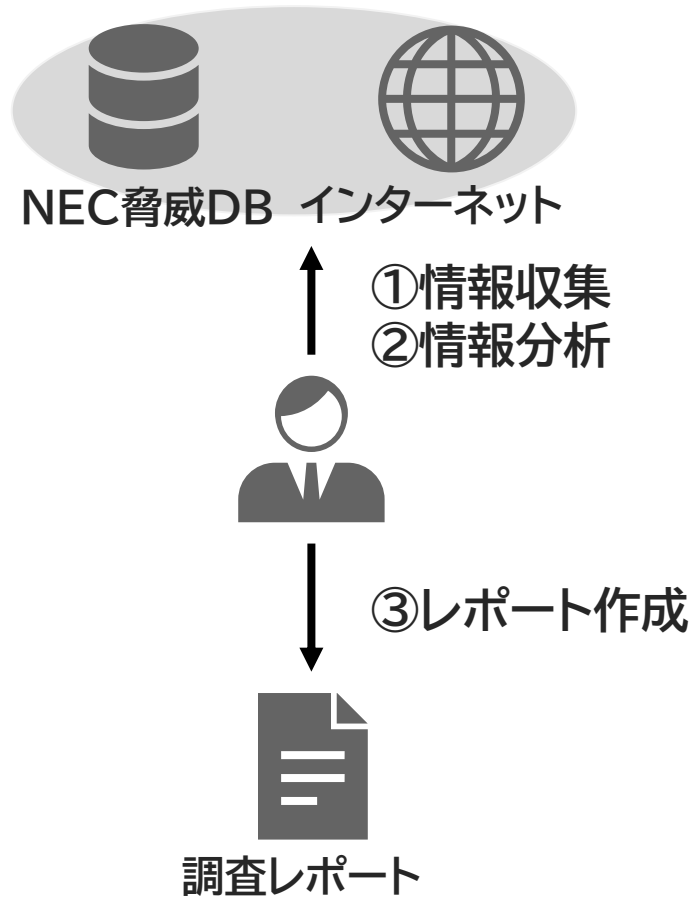
# ユースケース例(Summarize)

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**





# まとめ

# まとめ

- ◆ インテリジェンスプロセス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>

\ Orchestrating a brighter world

**NEC**