Recorded Future®

脅威インテリジェンスは次の段階へ

Autonomous Threat Operations（ATO）とは

レコーデッドフューチャージャパン株式会社
Shingo Anraku | Senior Sales Engineer

本日のアジェンダ

01 **AIを活用した攻撃の現状**
AIの脅威動向と脅威インテリジェンスの進化

02 **ATOの機能と4つのユースケース**
ATOによる運用変革と現場への適用シーン

03 **直近のインシデント事例**
Axios攻撃 / Recorded Futureが実現できること

04 **まとめ**

Recorded Future会社概要

	US本社	日本法人
名称	Recorded Future, Inc.	レコーデッド・フューチャー・ジャパン株式会社
設立	2009年	2018年
所在地	本社：ボストン グローバル拠点： ワシントンDC、ロンドン、ヨーテボリ、シンガポール、東京、ドバイ	〒100-7014 東京都千代田区丸の内二丁目7番2号 JPタワー14F
経営陣	Co-Founder：Christopher Ahlberg Ph.D. CEO：Colin Mahony	Country Manager：柿澤 光郎
従業員数	1000名～	25名～
導入社数	1,900以上	100以上の企業、団体
導入業界	各国政府機関（40カ国以上）、防衛警察機関、 金融業界、重要インフラ、食品小売業、製造業、ITサービス、 エンタメ、製薬等	中央省庁、大手金融機関、大手小売業、製薬業界、大学、大手製造業（電機メーカー、自動車業界、半導体関連、重工業、等）

Recorded Futureが保有するセキュリティ認証 SOC 2 Type 2, ISO 27001, ISO 27701, and ISO 9001 SOC 3
https://www.recordedfuture.com/faq/security

サイバーセキュリティに関するあらゆる情報を収集

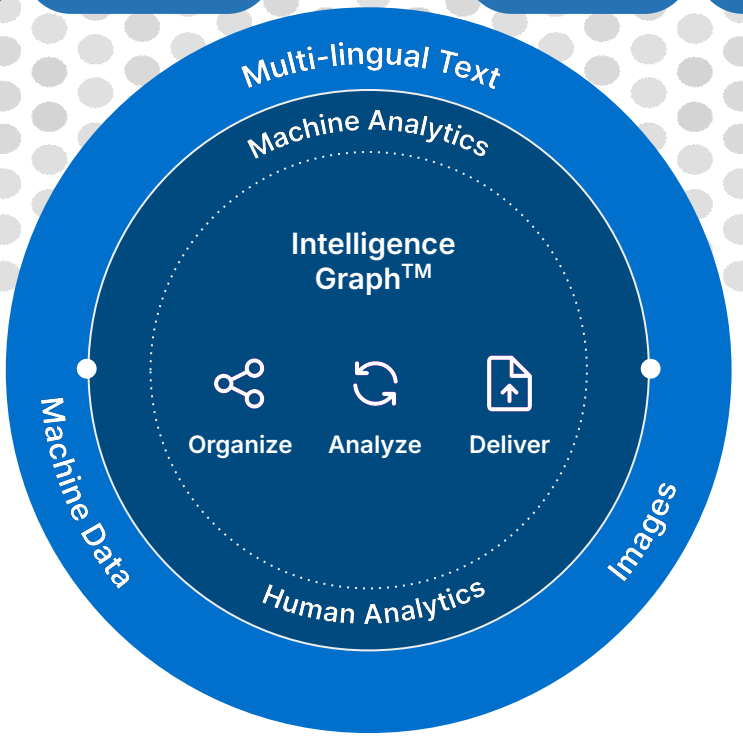
Powered by the Intelligence Graph®: AI-Driven & built for Internet scale

Recorded Future Intelligence

OSINT | Dark Web | Network Intelligence | Malware Intelligence | Insikt Group® Research

Customer Telemetry

SIEM/SOAR | EDR | Network Security | IAM | Other Detection Tools/Feeds



- **Intelligence Graph -**

  独自の分析エンジンにより、
  あらゆる言語の、
  大量のデータセットを、
  リアルタイムに相関分析し、
  AIを用いたアクショナブルなワークフローを実現

世界最大のインテリジェンスグラフ:
100TB以上のテキスト、画像、技術データから構築

自然言語処理によってタグ付けされた、サイバーおよび地政学分野最大のOSINT

世界最大の犯罪ダークウェブおよびメッセージングデータを保有

世界最大のグローバル企業サイバーオントロジー
(インターネット上のアタックサーフェス)

世界最大のインテリジェンスユーザーコミュニティ

Modules | **Integrations & APIs** | **Recorded Future AI**

AIを活用した攻撃の現状

数字で見る AI脅威のリアル

1,265%

フィッシング攻撃増加率

ChatGPT公開後（Q4 2022→2023末）

10倍

ディープフェイク詐欺の増加

2022→2023年、北米で1,740%急増

$2,500万

香港ディープフェイク被害額

ビデオ会議で経営陣を偽装し送金指示

300%

合成ID詐欺の増加

AI生成の実在しないIDが急増（2025 Q1）

Insikt Groupの評価：AI脅威の成熟度

AI Malware Maturity Model（AIM3）

Lv.1	→	Lv.2	→	Lv.3	→	Lv.4
実験段階		導入段階		最適化段階		自律段階

現在の大半の攻撃はここ（ Lv.1〜3）

「人の判断を騙す攻撃」

完全自律型のAI攻撃はまだ来ていない。
しかし、AIが作る偽メール・偽声・偽顔は
すでに人間が見抜けるレベルを超えている。

AIは攻撃者の力を増幅し、速度・精度・規模すべてを拡大させている。
今は「準備期間」— 自律型攻撃が本格化する前に防御側の自律化を。

出典: Recorded Future Insikt Group — AIM3 Framework / 2025 Annual Report / State of TI Report 2025

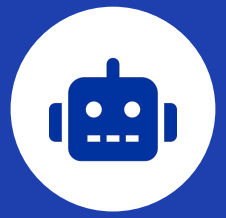
脅威インテリジェンスの進化

Phase 1
知る

「可視化」

Phase 2
現在地

「コンテキスト」



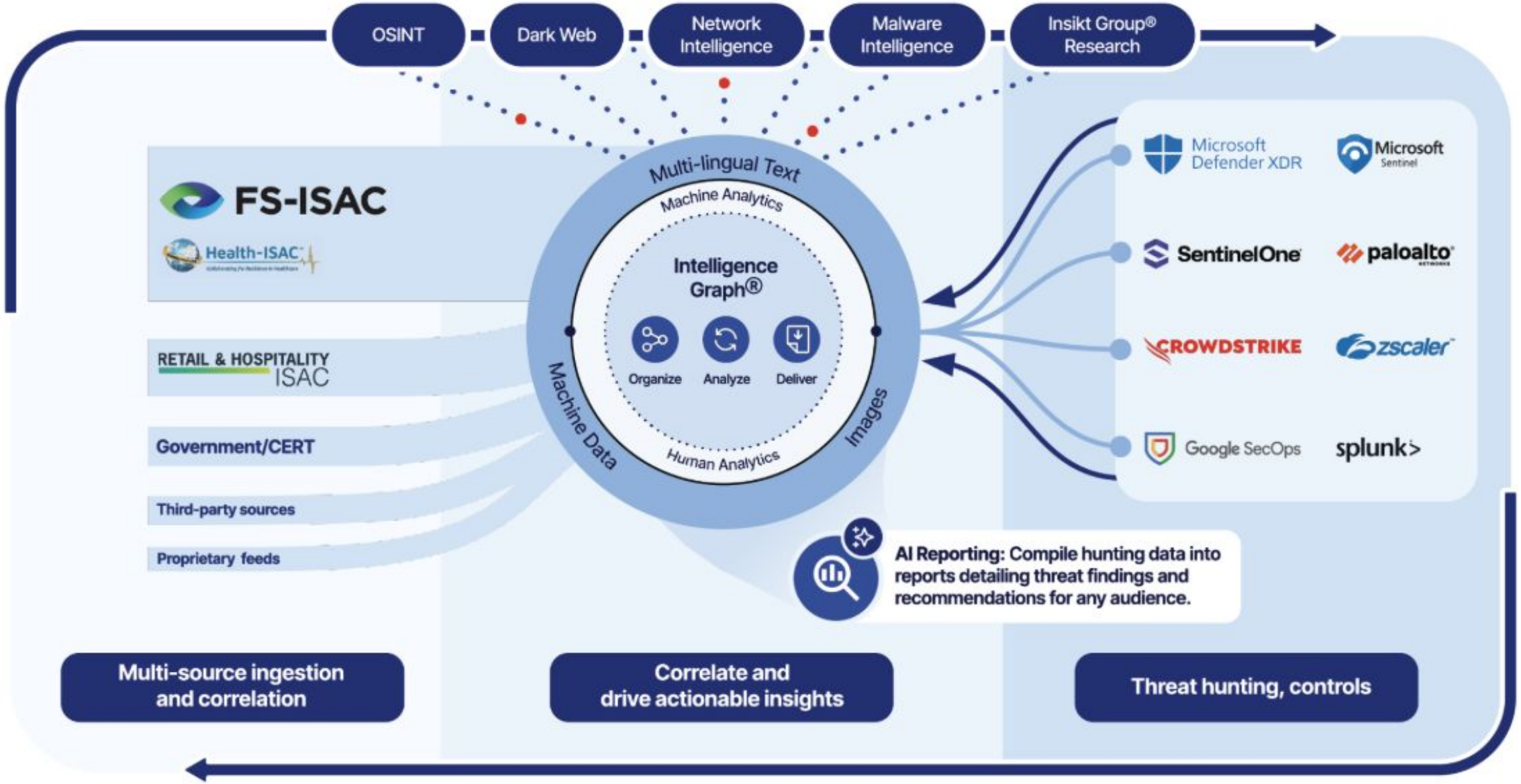
Phase 3
次の一手

「運用」

Autonomous Threat Operations = インテリジェンスを端緒としたアクションをAIエージェントが自律的に実行

“Autonomous Threat Operations”は何を変えるか

Intelligence Graph を活用し、AIの支援により人の介入を最小限に抑え、自律的サイバー防御を実現します。



現場の疲弊：手動プロセスが生み出す　4つの「ボトルネック」

ケース① 情報収集（Collection）

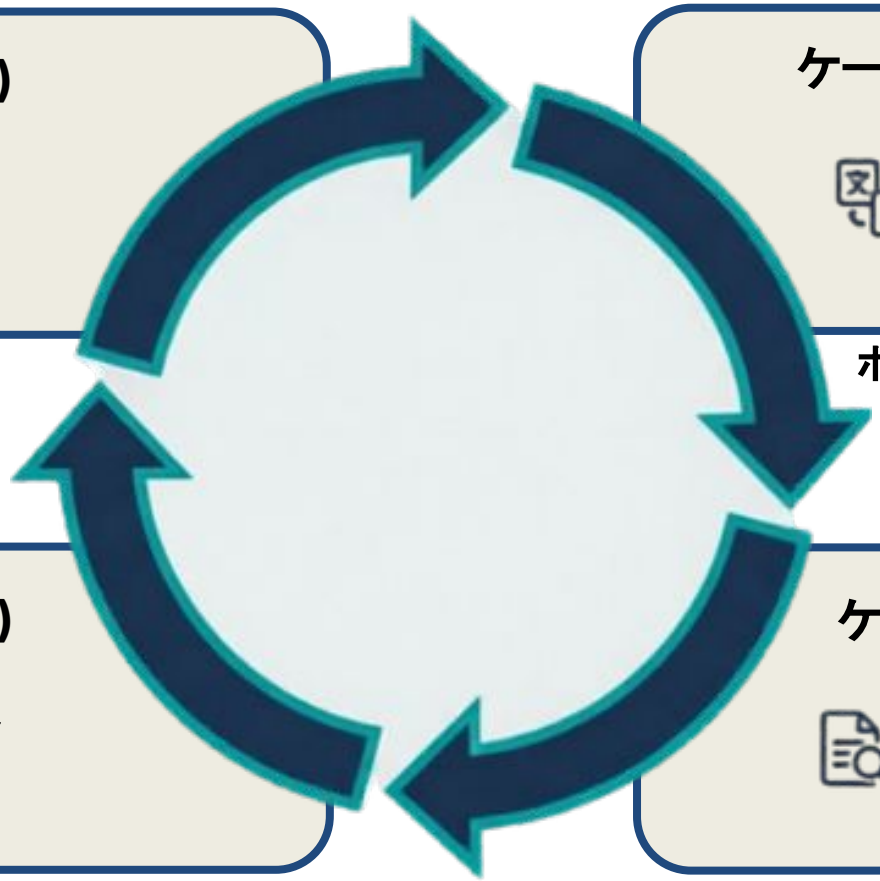
ISACやJ-CSIP等からの情報を
Excel等で手作業で整理

ボトルネック：「コピペ地獄」による疲弊

ケース② ルール変換（Translation）

Sigma&YARAルールから
自社SIEM/EDR言語へ手動修正

ボトルネック：数時間～数日の展開遅延



ケース③ ハンティング（Hunting）

スキルフル人材依存の手動ハント
還流がされない人海戦術

ボトルネック：属人化、再度手動対応

ケース④ レポート（Reporting）

情報の取捨選択、読者別書き分け、
正確性の担保。。

ボトルネック：収集・見直しの工数多大

優秀なアナリストの貴重な時間が、「分析」ではなく「情報の整理と定型作業」に浪費されている

ケース①②：ISAC自動連携とSigma&YARA→製品別クエリ自動変換、即時防御へつなぐ

①ATOによってISACは「読むもの」から「防御エンジンの入力データ」に変わる

② Recorded Futureの提供Sigma&YARAルールを、Integration AppがSIEM/EDR等環境に合わせ 自動変換・展開

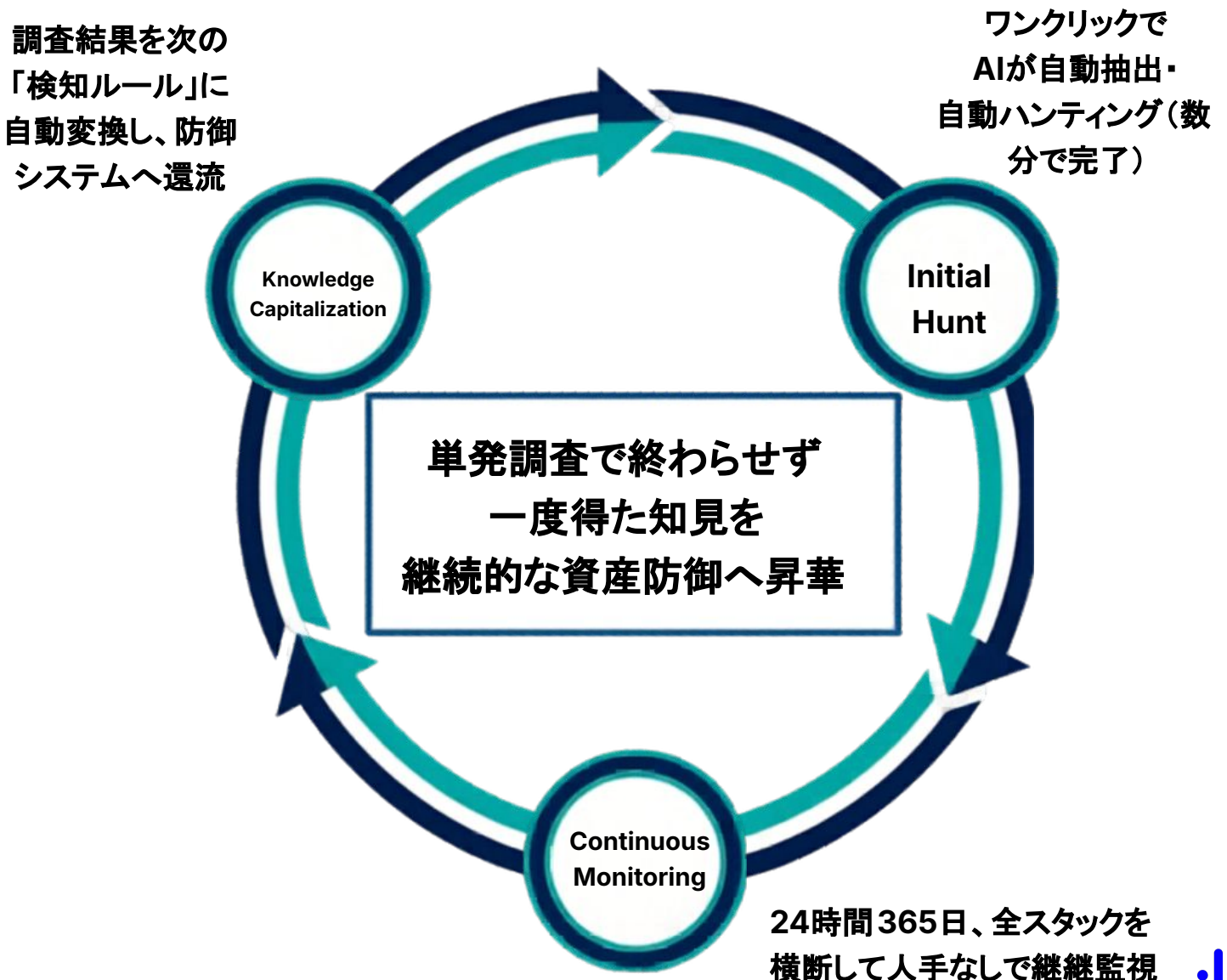
情報整理の属人化を解消、手作業負担なく「マシンスピードの検知力」に直接変換します

ケース ③: 自律型脅威ハンティングによる知見の資産化

Scenario: サプライチェーン攻撃
（例：Axios乗っ取りに関する調査）

- **従来の限界：** CISOからの指示で単発の手動調査を実施。結果はレポート化されて終了。数週間後に同じTTPsで攻撃されても気づかない。
（知見活用の断絶）

- **ATOの介入：** AIがレポートからIOC/TTPを自動抽出。



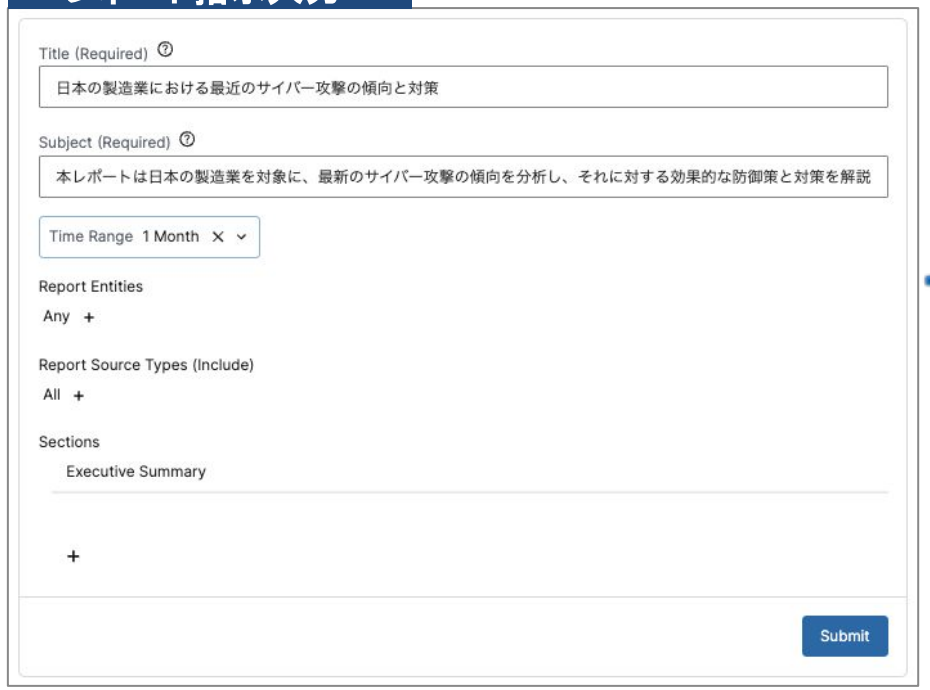
ケース ④：Recorded Future AIによるレポート生成

ATO summary Report：ハンティング後、検出・対処件数が膨大でも AIが自動でダイジェストに集約

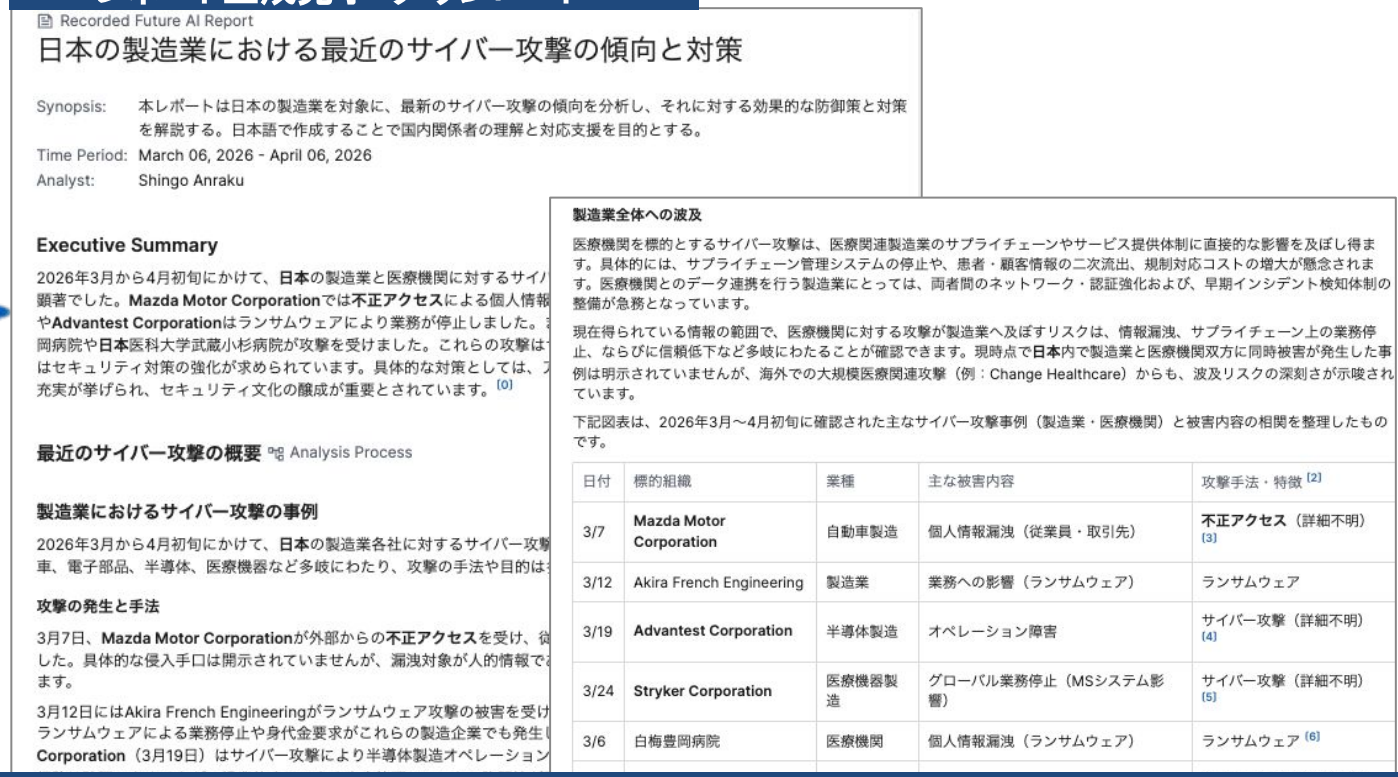
Custom Report：特定の関心事や報告形式に合わせ、AIが高度な分析書を即座に作成

[Custom Reprt 作成イメージ]

レポート指示入力



レポート生成完了・ダウンロード


Recorded Future AI Report

日本の製造業における最近のサイバー攻撃の傾向と対策

Synopsis: 本レポートは日本の製造業を対象に、最新のサイバー攻撃の傾向を分析し、それに対する効果的な防御策と対策を解説する。日本語で作成することで国内関係者の理解と対応支援を目的とする。

Time Period: March 06, 2026 - April 06, 2026

Analyst: Shingo Anraku

Executive Summary

2026年3月から4月初旬にかけて、**日本**の製造業と医療機関に対するサイバー攻撃が顕著でした。**Mazda Motor Corporation**では**不正アクセス**による個人情報漏洩が発生し、**Advantest Corporation**はランサムウェアにより業務が停止しました。[1] 岡病院や**日本**医科大学武蔵小杉病院が攻撃を受けました。これらの攻撃はセキュリティ対策の強化が求められています。具体的な対策としては、充実が挙げられ、セキュリティ文化の醸成が重要とされています。[0]

最近のサイバー攻撃の概要 Analysis Process

製造業におけるサイバー攻撃の事例

2026年3月から4月初旬にかけて、**日本**の製造業各社に対するサイバー攻撃が車、電子部品、半導体、医療機器など多岐にわたり、攻撃の手法や目的は

攻撃の発生と手法

3月7日、**Mazda Motor Corporation**が外部からの**不正アクセス**を受け、した。具体的な侵入手口は開示されていませんが、漏洩対象が人的情報で ます。

3月12日にはAkira French Engineeringがランサムウェア攻撃の被害を受け ランサムウェアによる業務停止や身代金要求がこれらの製造企業でも発生 **Corporation**（3月19日）はサイバー攻撃により半導体製造オペレーション

製造業全体への波及

医療機関を標的とするサイバー攻撃は、医療関連製造業のサプライチェーンやサービス提供体制に直接的な影響を及ぼし得ます。具体的には、サプライチェーン管理システムの停止や、患者・顧客情報の二次流出、規制対応コストの増大が懸念されます。医療機関とのデータ連携を行う製造業にとっては、両者間のネットワーク・認証強化および、早期インシデント検知体制の整備が急務となっています。

現在得られている情報の範囲で、医療機関に対する攻撃が製造業へ及ぼすリスクは、情報漏洩、サプライチェーン上の業務停止、ならびに信頼低下など多岐にわたることが確認できます。現時点で**日本**内で製造業と医療機関双方に同時被害が発生した事例は明示されていませんが、海外での大規模医療関連攻撃（例：Change Healthcare）からも、波及リスクの深刻さが示唆されています。

下記図表は、2026年3月～4月初旬に確認された主なサイバー攻撃事例（製造業・医療機関）と被害内容の相関を整理したものです。

日付	標的組織	業種	主な被害内容	攻撃手法・特徴 [2]
3/7	**Mazda Motor Corporation**	自動車製造	個人情報漏洩（従業員・取引先）	**不正アクセス**（詳細不明） [3]
3/12	Akira French Engineering	製造業	業務への影響（ランサムウェア）	ランサムウェア
3/19	**Advantest Corporation**	半導体製造	オペレーション障害	サイバー攻撃（詳細不明） [4]
3/24	**Stryker Corporation**	医療機器製造	グローバル業務停止（MSシステム影響）	サイバー攻撃（詳細不明） [5]
3/6	白梅豊岡病院	医療機関	個人情報漏洩（ランサムウェア）	ランサムウェア [6]

ATO Summary Report →「SOCリーダーが 毎朝の状況を 1分で把握 するため」

Custom Report →「マネジメント層 への報告や、特定の インシデントへの深い洞察 を伝えるため」

Axiosへのサプライチェーン攻撃：3時間の空白がもたらした重大な脅威

Target

1億DL/1週間
HTTPクライアントライブラリ「Axios」

Impact

- 悪意あるバージョン（1.14.1 / 0.30.4）公開
- CI/CD パイプラインを標的
- Windows / macOS / Linux クロスプラットフォーム
- RAT感染リスク

約3時間

npmスキャナーが15分で検出するも、レジストリからの完全削除まで3時間を要した。この空白時間にインストールされた全環境が危険に晒された。

脅威アクタープロファイル

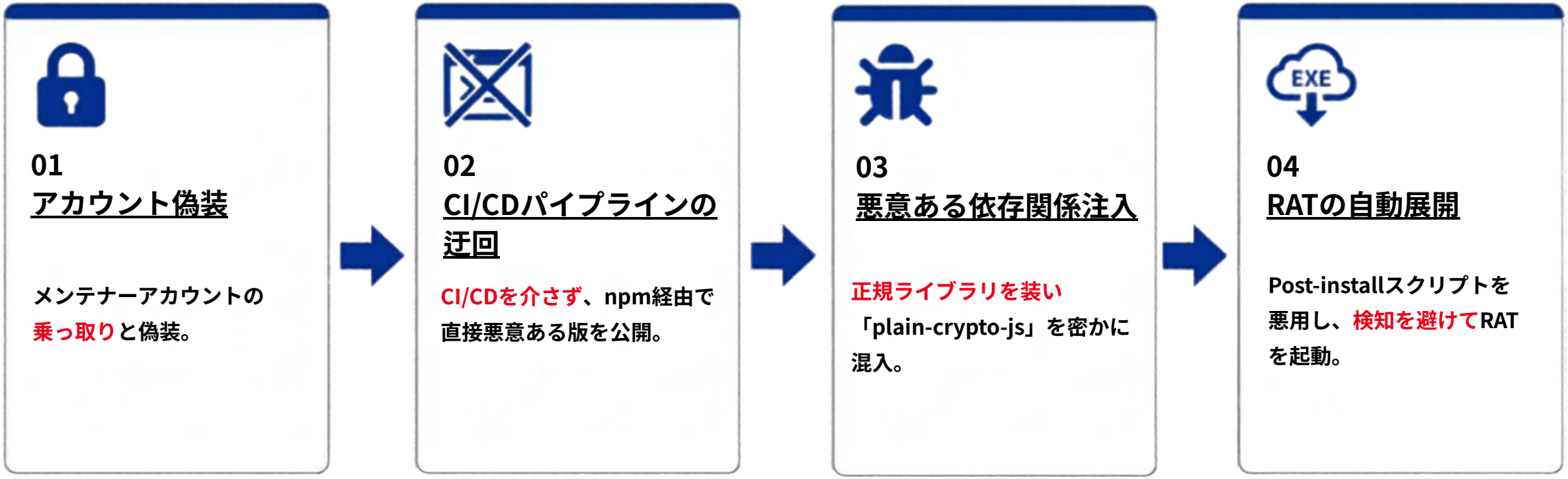
・アクター：UNC1069

・暗号通貨の窃取およびインテリジェンス収集

・サプライチェーン攻撃とOSSメンテナーのアカウント乗っ取りに特化

・「WAVESHAPER」に類似したマルウェアを使用

正規プロセスを悪用した巧妙な攻撃メカニズムと検知回避手法

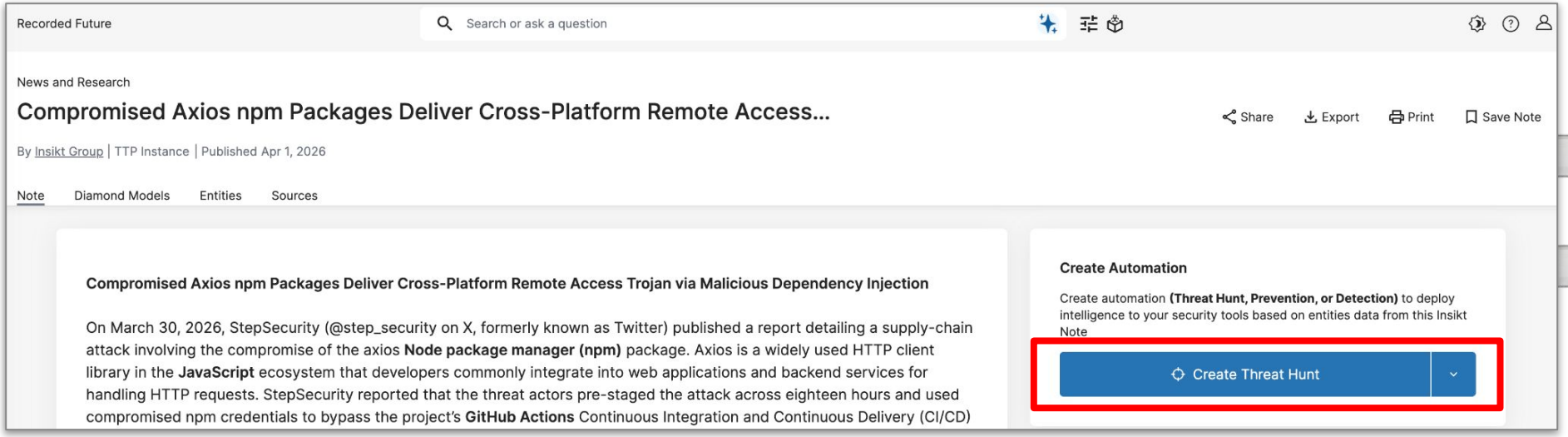


正規のライブラリアップデートとして実行されるため、
従来のエンドポイント防御（EDR）や境界防御では初期検知が極めて困難。

ATO：インシデント対応を「数日」から「数分」へ

	現在の運用（Manual）	ATO導入後（Autonomous）
初動対応	1, レポート確認 2, IoCの手動抽出 3, ルールの手作業作成 4, EDR/SIEMへの展開 所要時間：数時間～数日 高度なスキルが必要	1, ボタンクリック 2, AIが自動抽出 3, ハンティングルール自動作成、適用 所要時間：数分 高度スキルは不要
継続監視	単発の手動確認 継続追跡しないと脅威を見逃すリスク	インテリジェンスグラフと連動 24/7 自動ハンティング実施

既存セキュリティスタックとのシームレスな統合 (連携ツールへ送信前にフィルタも可能)



Microsoft Sentinel

CROWDSTRIKE

Malware Intelligenceの威力：高度な解析スキルを不要にするルールの自動生成

社内環境のハンティングにおける課題

膨大なログとの格闘

毎日出る山のようなログから、怪しい動きを見つけ出すのが非常に大変。

専門スキルの不足

ファイル(ハッシュ値)から自力でYARA、SIGMAの検知ルールを作成するには、高度な解析スキル、多く時間が必要。

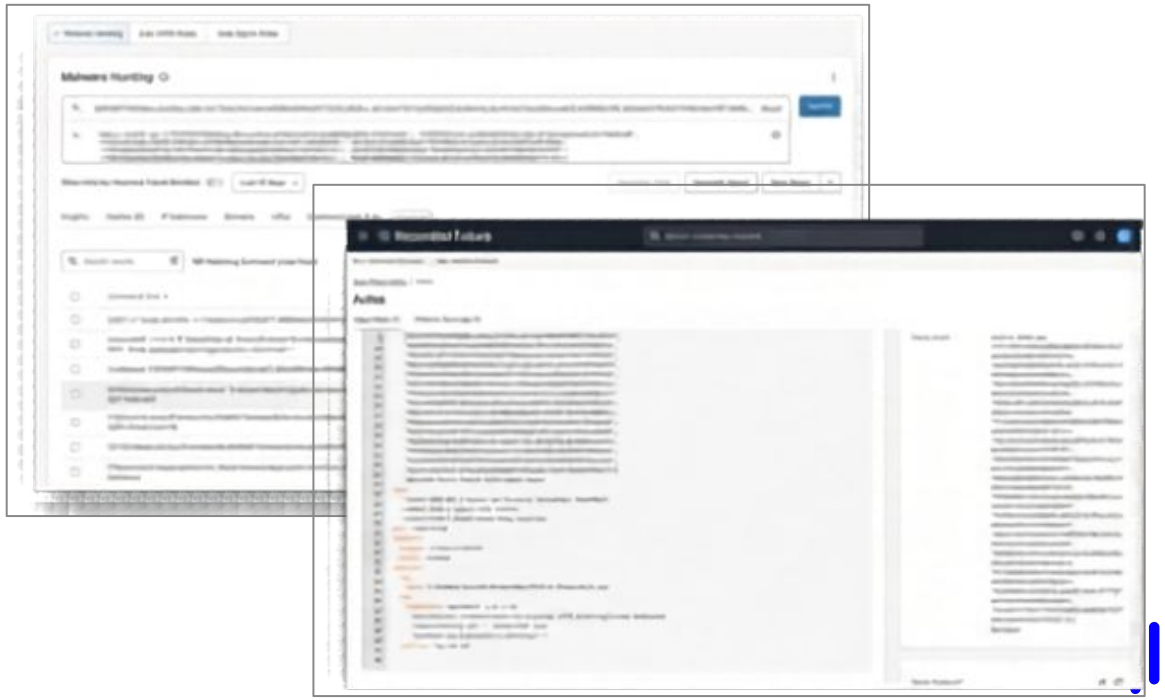
数日が数分へ：AIによる自動生成

1, ハッシュ値を入力

2, AIがそのマルウェアの特徴を分析

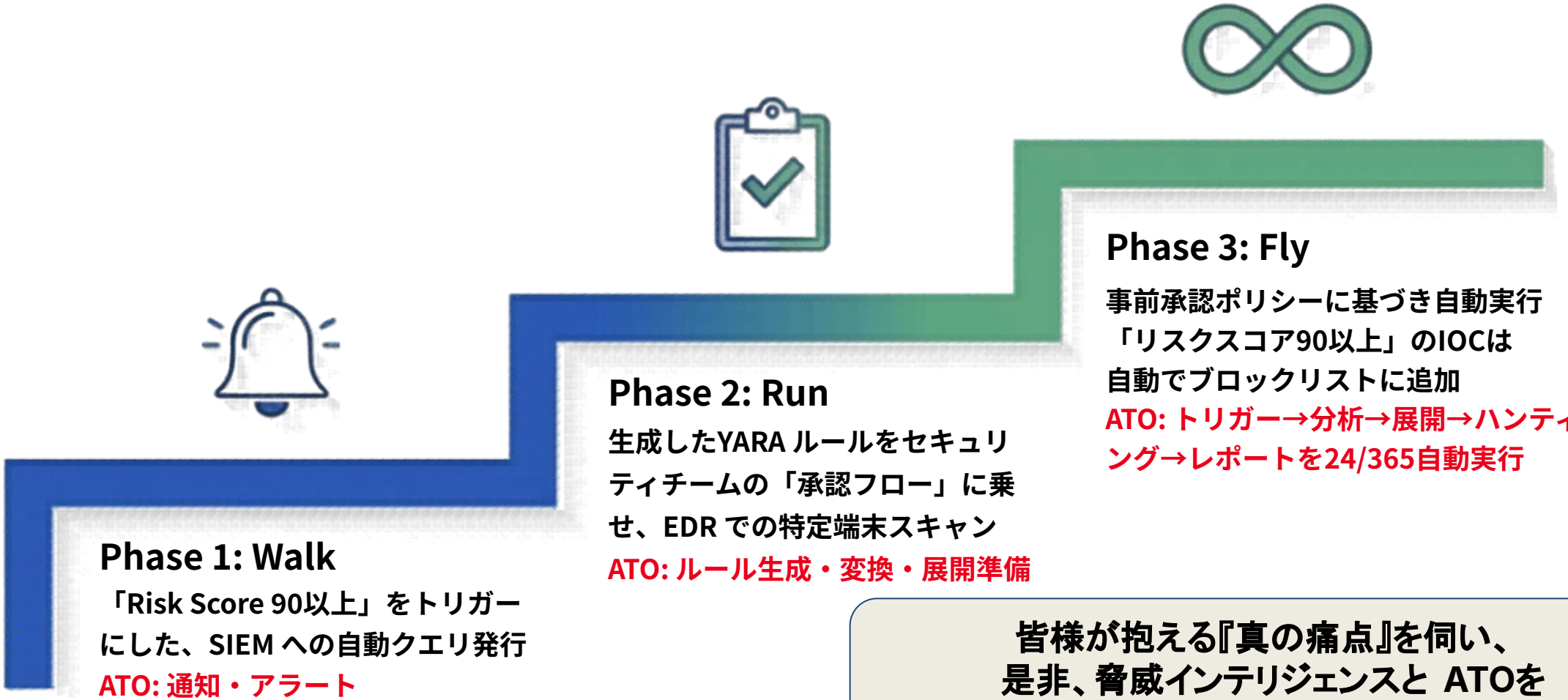
3, 検知用ルールを自動作成

→ 数日かかる作業が数分で終わります。



ATO 実務導入へのロードマップ

完璧な自動化を初日から目指す必要はありません。
実務の成熟度に合わせた3つのフェーズで、段階的に自律運用を組み込みます。



Phase 1: Walk

「Risk Score 90以上」をトリガーにした、SIEM への自動クエリ発行

ATO: 通知・アラート

Phase 2: Run

生成したYARA ルールをセキュリティチームの「承認フロー」に乗せ、EDR での特定端末スキャン

ATO: ルール生成・変換・展開準備

Phase 3: Fly

事前承認ポリシーに基づき自動実行
「リスクスコア90以上」のIOCは
自動でブロックリストに追加

ATO: トリガー→分析→展開→ハンティング→レポートを24/365自動実行

皆様が抱える『真の痛点』を伺い、
是非、脅威インテリジェンスと ATOを
ご体感いただく機会を設けさせてください。

まとめ：人間とAIの協調による、次世代のサイバー防御

非対称性の克服	AIで武装した攻撃者に、マシンスピードの自律防御で対抗。
運用の自律化	手作業・属人化を排除、情報収集から検知反映までを即時化。
知見の資産化	調査結果を組織の防御力として継続的に蓄積・還流。

AIがスピードとスケールを担当し

人間が戦略を指揮する運用へ

まず一歩を一緒に始めませんか

Thank you.