遠藤レポート：AIがソフトウェア産業に与えるインパクト（3）

IT運用へのAI適用の課題

株式会社 NTT データ
技術革新統括本部　技術開発本部
Technology Strategist　遠藤 宏

本レポートでは前回、ソフトウェア開発へのAI適用の事例を紹介した。今回はIT運用にAIを適用する取り組み事例について紹介する。サイバーセキュリティ分野ではAI適用が当たり前になってきているが、業務アプリケーションが載ったITシステムの運用にAIを適用するのは、ソフトウェア開発へのAI適用と同様に「緒に就いたばかり」とご理解いただきたい。

AIを利用したIT運用自動化

Arago社はIT運用自動化を実現するソフトウェアサービス「HIRO」を提供する企業で、本社はドイツのフランクフルトにある。

「HIRO」はルールベースと機械学習を組み合わせている。RPA（Robotic Process Automation）が構造化された異なるセットの情報を接続するのとは対照的に、「HIRO」は環境に動的に対応し、ナレッジを取得してコード化し問題解決するのが特徴である（図1）。

「HIRO」を使っている具体的事例として、Arago社とルフトハンザ航空で、飛行機のMRO(Maintenance, Repair and Overhaul: 保守・修理・分解検査）の最適化を狙う取り組みが始まっている。

NTTデータSMSのIT運用自動化への挑戦

NTTデータグループの中でお客様の情報システムの運用管理業務を担っている株式会社NTTデータSMSでは、運用業務にAIを利用して問題検知から解決までの工程全体を高度化できないかという視点で、有望企業・有望技術のひとつとしてArago社のツールの調査及び評価検証を続けている。

従来のIT運用自動化製品は、事前に定めた問題解決フローのみ実行可能で、新たなフローが必要になる都度開発が必要であった。すなわちスクリプトなどを開発して

①故障検知から被疑箇所の切り分けと特定
②故障の復旧方法の決定と実行

など、故障対応全体の流れを都度定義する必要があった。

この作業はおおむね1～3カ月

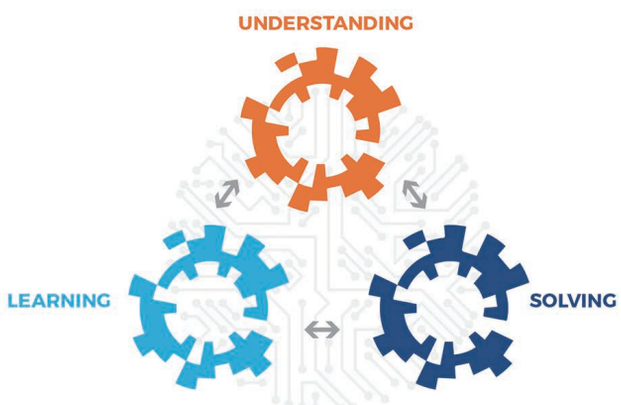

図1　HIROの学習と推論（Source: Arago社）

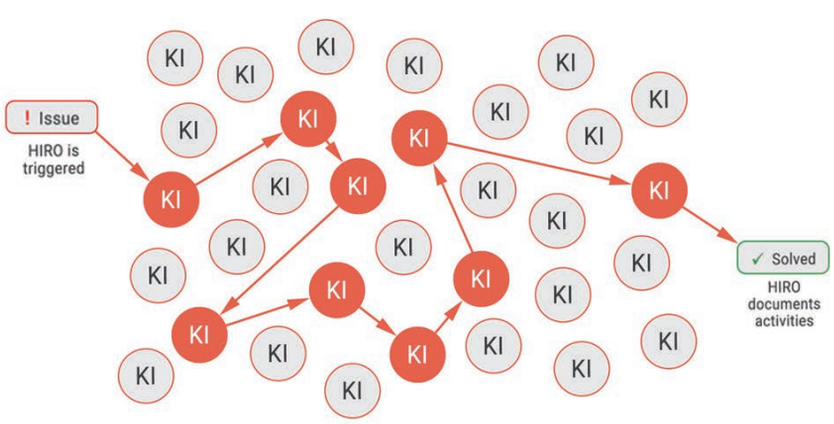

図2　予め定義された作業手順の選択・実行による問題解決（Source: Arago社）

程度の開発・試験期間を経て商用環境に展開されるが、該当するインシデントの発生頻度や一回あたりの対応時間を考えると、開発成果物の再利用性が上がらず、また自動化される故障範囲を広げるにもコストがかかるので費用対効果に課題があった。

「HIRO」の自動化対象は、IT運用においてネットワーク経由で作業出来る範囲の問題検知から解決までの全工程のシステム故障対応で以下の情報を使い問題解決する。

①監視ツールや運用管理製品から発行されるアラートやチケット
②システム構成要素(APソフト、OS、ハード等)
③KI(Knowledge Item:情報取得コマンド実行などエンジニアの知見に基づく簡易な作業手順)

「HIRO」は、故障発生時にAIが対応作業の実行順序を考案し、問題解決にあたる。最終的に故障復旧や適切な関係者への連絡を自動的に実行する（図2）。

KIは汎用性が高く、従来の自動化ツールより開発成果物の再利用性を高めることが期待できる。

サイバーセキュリティとAI及びDevSecOps

IT運用の話と密接な関係にあるセキュリティ対策に関して、NTTテクノクロス株式会社が公開している「サイバーセキュリティトレンド2018」から2点紹介する。

1点めは、**「AIを悪用した攻撃技術とAIを活用した防御技術がしのぎを削り、マシン戦争時代に突入する」**

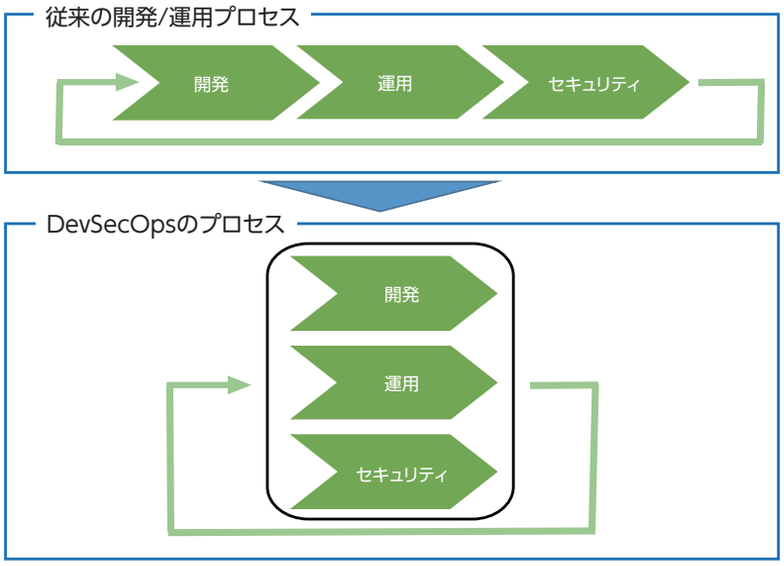

図3　DevSecOpsのイメージ（Source：NTTテクノクロス）

AIはセキュリティ分野で未知のマルウェア対策、攻撃に対する防御、脆弱性検出など様々な用途で応用が期待されている。しかし、AIを活用するのは防御側だけでなく攻撃側もAIを活用する。攻撃側、防御側双方がお互いの機能や振る舞いを学習する世界になりつつある[1]。

2点めは、**「加速するビジネススピードに対して継続的なセキュリティ確保も必須となる」**

ソフトウェア開発/運用のDevOpsの手法にセキュリティを加えたDevSecOpsの概念が提唱されている。セキュリティ関連の動きがAIにより良くも悪くも速くなっているので、ソフトウェアの各開発工程でセキュリティ要件定義～設計～実装を同時実行することが必要になってくる（図3）[2]。

IT運用とAI

多くのアプリケーションを含む商用システムのIT運用にAIを組み込んで稼働させるには、前半で紹介したAragoに限らず各種AIの現場での運用実績が重要となる。現状のIT運用においては、様々な機器・ツールがアラートを検出し、運用者が事象を判断し適切なアクションに繋げている。アラートとアクションの実績を踏まえ、「この環境下でこういう事象が発生したので、このアクションをすべき」とAIが推奨した場合に、「AIの判断を正しいとして自動的にアクションを実行する」と信頼するためにはひとつひとつ実績を積み重ねていくしかない。

ネットワークセキュリティ対応を運用者の人手に頼るのは限界があるので、AIの活用は必至であるが、アプリケーションまで含めたIT運用全体での「AI使いこなし」のためには現場での多くの運用実績と時間を必要とすると思われる。

※[1]、[2]の引用元
NTTテクノクロス株式会社
「サイバーセキュリティトレンド2018」
https://www.ntt-tx.co.jp/products/cs-trend/

＜お問い合わせ先＞
endouhr@nttdata.co.jp