2 Cycle-Ops

LLMを用いた次世代サイバーセキュリティオペレーション技術

社会情報研究所では、セキュリティ人材の世界的な不足に備えたセキュリティプロセス技術「Cycle-Ops」に取り組んでいる。人々が蓄積してきた不定形な情報をもLLMが知識として学習し、人間に寄り添いながらさまざまなセキュリティプロセスの代行・補助を行うことをめざしている。

進化するサイバー脅威とセキュリティ人材の不足

サイバー攻撃は日々成長する最新技術を取り込むことで進化し続けており、企業や組織が考慮すべき脅威もまた、24時間365日絶え間なく増え続けている。その一方で世界的に見てもセキュリティ人材が約400万人不足しているという深刻な状況がある。最新の脅威に対抗するためには、脅威の特定から防御、検知、対応、そして復旧に至るまでのセキュリティプロセスを効果的に連携させ、現状のセキュリティ人材により高度化させていくことが不可欠だ。しかし、そのためには、セキュリティプロセスに関する、幅広く深い専門知識が必要である。さらに、業務システムは組織ごとに異なり、自社ポリシなどが複雑に絡み合っているため、高度化されたセキュリティプロセスを実現しても、それが他の企業や組織にフィットするとは限らない。

日本電信電話株式会社
社会情報研究所
社会イノベーション研究プロジェクト
（左）主幹研究員　**今野 俊一** 氏
（右）研究主任　**山中 友貴** 氏

未来のサイバーセキュリティプロセス技術：Cycle-Ops

Cycle-Opsは、この問題を解決する技術として考案された（図1）。この技術は、LLMを核としており、軽量なLLMを用いて、サイバーセキュリティプロセス全体を低コスト

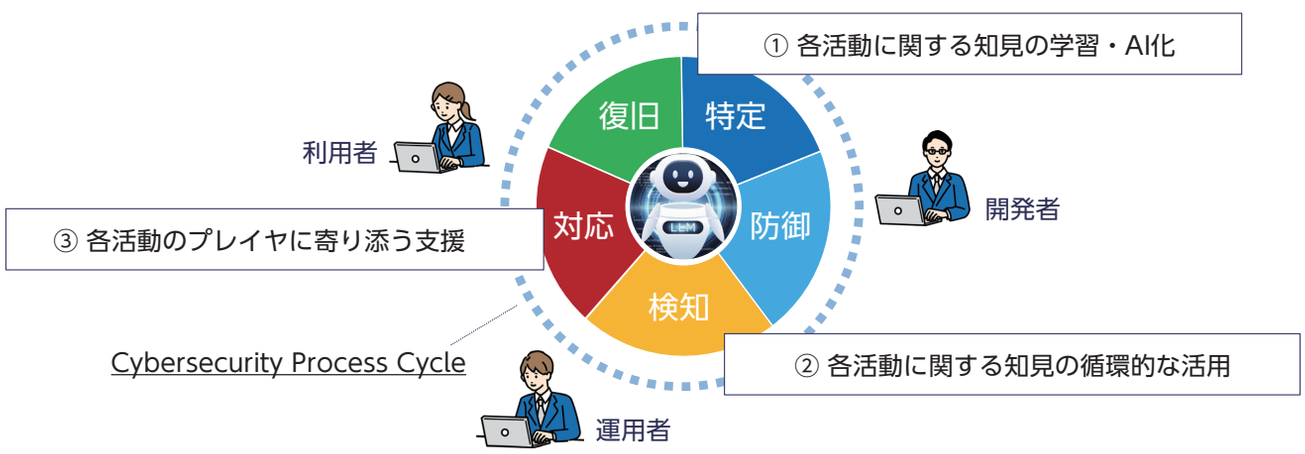

図1　Cycle-Opsの概要

で学習し、各プロセスの効率化と高度化を実現する。Cycle-Ops は、脅威の特定から復旧までのセキュリティプロセスのすべてを AI が主導または支援することで、必要な時に即座に対応できるように設計されている。また、AI は各プロセスにおけるセキュリティ運用の知見のさらなる蓄積と、それらの知見の循環的な活用を自律的に行う。例えば、AI が社内でのインシデント対応に関わる一連の流れを学ぶことで、被害者から適切なタイミングで必要な情報を収集しながら、最適な対応策を指示することが可能となる。

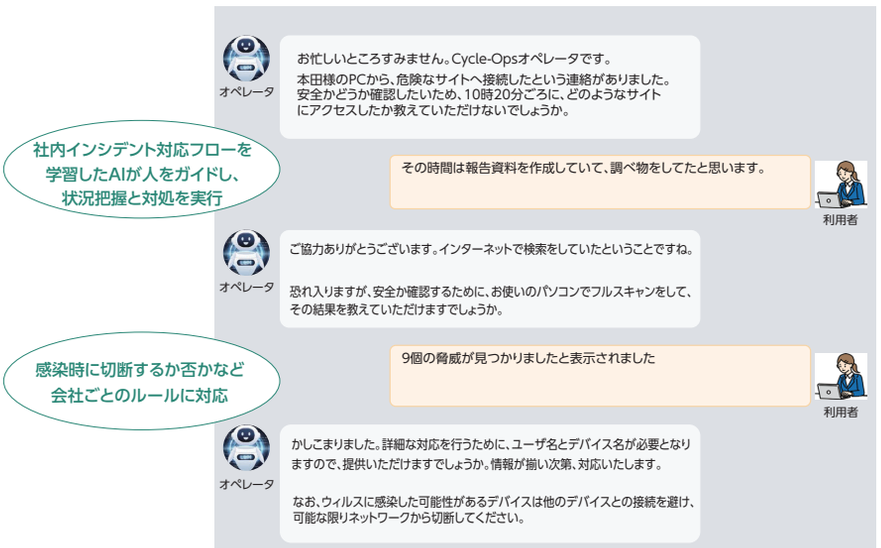

図 2　インシデントレスポンスの高度化事例

人に寄り添うセキュリティ AI

Cycle-Ops では、セキュリティ運用領域における人と AI の最適な在り方を提案している。具体的には、AI が脅威の特定や防御に必要な基本的な調査・分析や対策を代行し、人は AI を監督する役割を担う。これにより、セキュリティ担当者はより優先度の高い業務や、高度な脅威への対策に集中できるようになる。また、インシデントが発生した場合の対応では、AI がヒアリングやフォレンジックを補助することで、インシデントハンドリングがスムーズかつ適切に進むようになる。Cycle-Ops のもう一つの特徴は、AI が人のスキルや知識に合わせて柔軟に対応を代行、補助することだ。例えば、サイバー攻撃の被害者がセキュリティに詳しくない場合、AI はより具体的な選択式の質問や具体的な端末操作の誘導を行うことで情報収集を行う。これにより、人と AI の双方がセキュリティの知見を学習し、使えば使うほど対応が高度化、効率化する仕組みを実現している。このような自律的な仕組みは、現代のサイバーセキュリティが直面する複雑で多様な課題に対して極めて有効な対策となり得る。

具体的なユースケース：インシデントレスポンス

Cycle-Ops の具体的なユースケースの 1 つとして、インシデントレスポンスの例を紹介する（図 2）。Cycle-Ops は、自身の持つセキュリティ知識と社内のセキュリティポリシーや社内に蓄積された過去のインテリジェンスを活用し、ユーザーの誘導を行う。具体的にはまず、端末などで不審な動作があった場合、自動的にログ情報などを取得しアラートを通知。次に、アラートの種別に応じて、社内ポリシの何を確認すべきか、その会社では過去どのように対応したかを推論し、さまざまな情報を分析し必要なアクションを決定する。その後、アクションに基づき具体的な質問文を生成し、ユーザーと自然にやりとりを行い、インシデントのクローズまで誘導する。このように、Cycle-Ops は今まで人々が蓄積してきたログや自然言語などによる不定形な情報を AI により活用し、セキュリティオペレーションの精度向上・効率化を実現する。

事業適用をめざしたフィールド実証

私たちは、早期の実フィールド実証を計画している。各社で異なるセキュリティポリシーや運用ルールといった組織的側面、システムやセキュリティ機器といった技術的側面に対して、Cycle-Ops をいかに適合させ、実フィールドにおける本格運用に耐えられる技術へと発展させることが目的だ。Cycle-Ops は「人に寄り添うセキュリティ AI」を標榜している。実際のユーザーの方々の声に寄り添い、安心・安全に使える技術に磨き上げてゆくためにも、パートナーと共に検討を深めていきたい。