URL https://journal.ntt.co.jp/article/36080
DOI https://doi.org/10.60249/25095106

主 役 登 場

生成AIがもたらすセキュリティ運用の未来

山中 友貴 Yuki Yamanaka

NTT社会情報研究所
社会イノベーション研究プロジェクト
研究主任

最近，仕事でも日常生活でも，私は生成AI（人工知能），特に大規模言語モデル（LLM）を使い倒しています．コーディングから論文の翻訳，アイデア出しなど，今やLLMなしの生活は考えられません．しかしその一方で，複雑なタスクになると，こちらの意図を正確にLLMに伝え，思ったとおりに使いこなすのはまだ難しいと感じることがあります．特に，専門的な分野の情報や微妙なニュアンスを扱う必要があるときは，もう少し踏み込んだ工夫が必要だと実感しています．

現在私が取り組んでいるCycle-Ops（サイクロプス）という技術は，まさにそのLLMを用いて，高度な専門性に根差したサイバーセキュリティの運用プロセスを大幅に改善することをめざしています．Cycle-Opsという名前は，米国国立標準技術研究所（NIST）が策定したサイバーセキュリティフレームワーク（CSF）の特定・防御・検知・対応・復旧という各運用サイクルをLLMを用いて高度化・効率化し，運用サイクル全体を循環的に強化するオペレーションを実現したいという思いから名付けられました．

サイバー攻撃の手法は日々巧妙化し，多様化しています．その一方で，サイバーセキュリティを担う人材は世界的に不足しており，このギャップが大きな課題となっています．サイバーセキュリティ運用の現場では，複雑で膨大な知識と経験が必要とされ，人間の負担が非常に大きくなっています．

Cycle-Opsは，この人間の負担を軽減し，人とAIが高度に協調して運用サイクル全体を強化することに貢献します．セキュリティ運用のプロセスには，CSFに定義されるとおり多くのステップがあります．これらの各ステップでは，専門家による豊富なノウハウと経験が活かされて運用が行われていますが，その知識は暗黙知として個人に蓄積されがちで，組織全体での共有や継承が困難な状況となっています．Cycle-Opsでは，これらの各ステップにおける人間の専門知識を生成AIに学習・継承させ，AIによる自律的な運用知識の蓄積・循環を実現します．

Cycle-Opsの重要なコンセプトの1つに「セキュリティ運用にかかわる専門家の暗黙知を抽出・活用する」という点があります．専門家が持つ高度な判断力や直感，経験に基づく知見など，従来はなかなか言語化・共有が難しかった暗黙知を生成AIにより抽出・体系化することで，それらを継続的に活用できるようになります．この結果，人間が持つ貴重なノウハウが組織全体に広まり，セキュリティ運用の質が向上するとともに，専門家に依存しすぎない持続可能なセキュリティ体制が構築されます．

例えば，Cycle-Opsがめざすインシデントレスポンスでは，不審な動作が検知された端末のログをAIが自動収集・分析し，即座に必要な対応策を提示することを想定しています．さらに，ユーザに対して具体的な選択式の質問を提示し，情報収集を支援することで，専門知識がないユーザでもスムーズにインシデント対応ができる仕組みを提供します．また，AIが過去の事例やポリシーを踏まえて企業ごとに最適な対応を判断し，自然言語でユーザとコミュニケーションを取りながら，インシデントの解決までをサポートすることを実現したいと考えています．

このようにCycle-Opsでは，AIが基本的な調査や分析，定型的な対応を代行し，人間はAIが提示した高度な脅威への対応策を監督・判断する役割を担います．このような役割分担によって，人間はより重要な判断や複雑な問題の対応に専念できるようになります．セキュリティのもっとも弱い部分はシステム自体よりも人間の部分であり，この人間の部分をサポートし，運用サイクルを強化することは非常に重要だと考えています．

私たちは現在，Cycle-Opsの技術をより実用的なものへと発展させるべく取り組んでいます．企業ごとに異なるセキュリティポリシーや運用ルールに柔軟に適応し，実運用に耐える技術として磨き上げることが目標です．そのためには，実際のセキュリティ現場のニーズを深く理解することが不可欠です．より良い技術の実現に向けて，皆様からのさまざまなご意見をお待ちしています．

生成AIは日常生活のあらゆる場面で活用が進んでいます．私たちは，サイバーセキュリティ分野においても人間とAIが高度に協調し，運用サイクルを強化することで，より安全で安心な社会をつくっていきます．セキュリティ専門家がより高度な業務に集中できる環境を整備し，私たちが安心してネットワークを利用できる未来をCycle-Opsを通じて実現していきます．