AI時代のITおよびセキュリティ人材
育成の課題と展望

情報通信研究機構（NICT）サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター長
園田道夫（そのだ　みちお）

セキュリティ人材の需給状況

セキュリティ人材の不足が叫ばれて久しいが、その状況は一向に改善しないままである。大学、高等専門学校、専門学校などの人材輩出力も徐々に増強されてきてはいるが、その伸びは緩やかで、不足とされる11万人を埋め切るには数十年かかってしまう。DXの流れは、社会や組織に生産性向上という恩恵をもたらし始めてはいるが、一方でIT人材不足に拍車をかけてしまっている。希少種であるセキュリティエンジニアは奪い合いで、採用コストは右肩上がり。労働市場が逼迫（ひっぱく）する中でもセキュリティ人材の不足は突出していて、人材関連会社のレポート[注1]によれば、2025年12月時点のセキュリティ関連職種の中途採用の求人倍率は42・6倍に達している。

そうした状況を踏まえ、システムや人材の内製化に乗り出す企業も増えている。社内向け教材を内製している企業がそれを公開する例もあるし、動画を主とするプラットフォーム型の教育コンテンツや教育サービスも増えつつある。書籍やウェブの技術記事も含め、システム内製化の需要に応えるコンテンツも増えており、これらが人材内製化の流れを後押ししている。

システム開発における生成AI活用の主流化

システム開発周り、セキュリティ関連でいえばさらに、生成AIによる大波が押し寄せつつある。生成AIを用いてプログラミングからデバッグ、脆弱性のチェックまで行うことで、システム開発の生産性とセキュリティ面の品質は驚異的なまでに向上するとみられ、今後、主流の方法論になると予想される。現状、新規に登録される脆弱性数は年間4万5000個に上るが、AIによって脆弱性をあぶり出す力がより強まれば、この激減すらあり得る。世の中のサイバー攻撃の原因の多くを占めるのが、この脆弱性という代物なので、これが激減すればサイバー攻撃を職業的に行う犯罪者たちにとっては相当の痛手になるだろう。

とはいえ、人間が指示をしなければ生成AIは何も生み出せない。今後はこの指示を、日本語、英語というAIとの「コミュニケーションツール」を用いて的確に行うノウハウを、蓄積・研磨していく必要がある。現在それを確実に実行できるのは、皮肉なことにプログラミングのメカニズムを理解したエキスパートに限られている。生成AIが人間からプログラミングの仕事を「奪う」一方、プログラミングをよく知るエキスパートのみがそれを使いこなせる、という図式だ。

エキスパート人材の育成に向けた課題

現在構築されているシステムは、開発効率やコスト、ビジネス自体のスピードやスケーリングを追求した結果、従来よりも格段に複雑化している。したがって、生成AIに適切な指示を出すには、現在の複雑化したシステムの仕組みを一定の解像度で把握している必要がある。例えば、アプリを入れる〝箱〟であるコンテナ、その箱を自動で整理するオーケストレーター、必要なときだけ動くサーバーレス、機能を小さく分けて作るマイクロサービスなど、役割や流れを踏まえなければ指示は難しい。システム開発周りの今後の人材育成では、これらの資質を持ったエキスパートをどう育成するか、というところがポイントになるだろう。当機構が主催するSecHack365という若手人材育成のプログラムでは、現代の複雑な基盤のうえでのものづくり力（＝エキスパートに近いものづくり力）とセキュリティ資質をあわせ持った人材を輩出しているが、今後はそのような育成の仕組みを社会として増強する必要がある。

また、組織が人材を「内製」する場合にも、そのプロセスの中に生成AIを使いこなす力とセキュリティ力の育成を溶け込ませることが今後は求められるだろう。開発・構築したシステムを運用管理する側面でも、生成AIの影響は徐々に出始めている。生成AIのコアはLLM（Large Language Model）だが、文字通り大規模なデータの処理に長けている仕組みなので、膨大な量のログやアラートの分析などにも適任といえる。巨大容量化し続ける記録装置（ハードディスクやSSDなど）に悩まされていたデジタル・フォレンジック[注2]も含め、情報収集・分析という側面では大きな福音をもたらす可能性がある。ここでも、使いこなすためにはエキスパートの存在が重要であり、そのエキスパートになるためのプロセスをAIに実務的に奪われる中、そうした人材をどう育てるか、が課題となってくる。

人間独自の検知能力を組織的に鍛えるべし

システム開発のセキュリティ面も含む品質が向上し、運用管理面の分析力が向上したとして、サイバー攻撃被害は激減するだろうか。残念ながらそう簡単にはいかないだろう。世の中の全てのシステムやそれを構成するパーツが一気に最新化することはあり得ないし、調査分析力向上の恩恵も簡単には行き渡らないだろう。まず、セキュリティの宿命ともいえるが、何事も起きていない平時には予算をつけてもらいにくいという事情がある。また残念ながら、相当痛い目に遭ってからでなければ、システムやかかわる人材の大幅刷新、とはならないだろう。となると、世の中に広い意味での「脆弱性」は残り続け、サイバー攻撃によるインシデント（事件・事故）は絶えない、と見る方が現実的である。

インシデントの対応についても生成AIは入り込んでくるだろう。例えば、インシデントを認知してからの組織的な動きなどは、業務プロセスを学習したAIがサポートしやすい部分だといえる。当機構のインシデントの初動対応をテーマとする演習CYDERも、今後の演習シナリオのあり方について、そうした変化を視野に入れて検討を始めている。全てをAIに任せられるわけではないので、人間そのもの、特に能動的サイバー防御という側面からは、例えば人間の認知や異常検知の能力を組織的に鍛える必要性は多く残ると見ているが、鍛え方の確立や効率化は今後の重要な課題であるという認識である。

（注1）レバテック「IT人材の正社員転職市場動向」2026年1月29日公表

（注2）デジタル・フォレンジック：コンピューターやスマートフォン、サーバーなどに記録されたデータを科学的手法で回収・解析し、事件・事故・不正行為の真相を明らかにするための調査技術