KEIZAI DOYUKAI

Claude Mythos に端を発するセキュリティ課題対応について

2026 年 5 月 1 日
公益社団法人 経済同友会
代表幹事　山口　明夫

2026 年 4 月、米 Anthropic 社の次世代 AI モデル「Claude Mythos」をめぐる動きを契機として、高性能 AI 全般において、ソフトウェア脆弱性の発見・攻撃能力が飛躍的に向上していることが明らかになりました。代表幹事として、会員各位に以下のメッセージをお届けします。

1. 現状の危機に対する共通認識

これまでの「人間による検知と対応」のスピードでは、もはや AI による攻撃の勢いを防ぐことは困難です。実際、以下のような事象が発生しています。

（未知の脆弱性の爆発的増加）

私たちが利用する主要なオペレーティングシステムやソフトウェアにおいて、過去に類を見ない速度で脆弱性が特定されています。

（攻撃の高度な連鎖）

ネットワークや業務システムといったシステム全体の環境を考慮し、それぞれに存在する複数の脆弱性を高度かつ高速に連鎖させることで、防御側の死角を突く極めて巧妙な攻撃が現実のものとなっています。

2. 全社的な対応方針

この脅威に対し、私たちは守りを一段と高いレベルへ引き上げなければなりません。

（基盤対策の徹底と迅速化）

各種データのバックアップ取得をはじめとする従来型の対策を、これまで以上のスピード感をもって確実に実施することが重要です。これは「後回しにできない経営課題」と言えます。

（「副次的障害」に対する経営判断）

脆弱性への迅速な対応（パッチ適用等）により、既存システムに一時的な不具合が発生する場合（副次的障害）があります。しかし、これからは、「攻撃による致命的な被害」を防ぐことを最優先し、代替防御手段がない場合はパッチ適用等による副次的障害によるシステムリスクを許容した上での対応も必要と考えます。

3. 役員・リーダー層に対するメッセージ

セキュリティは IT 部門だけの問題ではありません。各部門のリーダーは、システムの停止や不具合が事業に与える影響をあらかじめ想定し、有事の際に「守るための決断」を躊躇なく行える準備を整えることが重要です。

AI の進化は止まりません。私たちはその進化に対応できる強靭な組織へと変革していく必要があると考えます。貴社の組織全体でこの新たな挑戦に向き合っていただきますよう、お願い申し上げます。

以 上