事務連絡
令和８年５月 18 日

各府省庁情報セキュリティ担当者 各位

AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について

内閣官房国家サイバー統括室

AI 技術は急速に進展・普及しており、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加する等、サイバーセキュリティにおける脅威に直面している。

特に、本年４月７日に米国 Anthropic 社が公表した Claude Mythos Preview を始めとするフロンティア AI モデルによる、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に備えた対応が必要不可欠である。

サイバーセキュリティ性能のより高い AI（高性能 AI）は、開発・利用するプログラム等における脆弱性の発見・修正等や各政府機関等[1]における検知・対応等のサイバーセキュリティ対策に活用することにより、我が国のサイバー対処能力の更なる強化が期待できる。特に脆弱性に関しては、高性能 AI により、脆弱性の発見・修正等が高速化することが考えられる。一方で、高性能 AI が攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われるおそれがあるため、悪用リスクを前提として、対策強化を早急に進めていくことが必要である。

このため、各政府機関等においては、以下のとおり、高性能 AI の悪用リスクに備え、政府統一基準に基づく基本的な対策を徹底するとともに、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策の強化を図られたい。

１．高性能 AI の悪用リスクに備え、政府統一基準に基づき、資産管理、リスクアセスメント、脆弱性対策、アカウント管理・認証・アクセス制御、バックアップの確保、ログの取得・管理、監視・分析、インシデントへの対応及び復旧等、基本的な対策を徹底すること[2,3]。

２．特に、情報システムを構成する機器等へのセキュリティパッチの速やかな適用は非常に重要であり、高性能 AI の悪用などのサイバー攻撃の高度化、自動化等を踏まえ、必要に応じて、セキュリティパッチ等の対策用ファイルの適時の適用を前提とした運用設計（パッチマネジメント（管理））を見直すこととするほか、機器等で利用するソフトウェアに関する脆弱性情報を入手し脆弱性対策計画を策定し実施する場合においても、こう

した技術や脅威の動向を踏まえて、迅速な対策が必要であるかどうかを見極めた上で[4]、実施の要否、実施時期等を判断することとするなど、脆弱性対策の強化を図ること。

3．これらの実施状況については、実効的な対応を継続的に行うべく、各政府機関等で実施する情報セキュリティ監査において機動的に確認すること。なお、国家サイバー統括室による監査においても当該実施状況について確認を行う。

なお、国家サイバー統括室においては、巧妙化・高度化を遂げる組織的なサイバー攻撃につき、初期段階から把握し、被害の防止につなげるため、インシデント情報等のサイバーセキュリティ関連情報を分野横断的に集約・分析し、各政府機関等に対する適切な形での情報提供やサイバー対処能力強化法等に基づく措置を含む能動的な防御・抑止に取り組むこととしている。そのため、各政府機関等においては、インシデントやその予兆等を確認した場合には、国家サイバー統括室まで速やかに報告願いたい。

---

[1] 国の行政機関（26 機関）、独立行政法人（86 法人）及び指定法人（10 法人）をいう。

[2] 英国 AISI による Claude Mythos Preview に関する評価においても、セキュリティアップデートの定期的な適用、堅牢なアクセス制御、構成管理、包括的なログ監視といったサイバーセキュリティの基本の重要性が改めて示されている。（英国 AISI　Our evaluation of Claude Mythos Preview's cyber capabilities https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities）また、米国 CISA による重要インフラのレジリエンス強化のためのガイダンスにおいても、外部ネットワークとの接続を能動的に遮断し通信が制限された状態でも重要インフラ・サービスの提供を継続する運用の確保（隔離）や隔離状態のまま侵害された重要システムを迅速に復旧させるための計画や手順の策定、訓練等（復旧）の重要性が示されている。（米国 CISA　CI Fortify: Strengthening Resilience Across Critical Infrastructure https://www.cisa.gov/topics/industrial-control-systems/ci-fortify）

[3] 特に、攻撃の端緒となりやすいインターネットへの露出領域を最小限にするとともに、閉域網について過信することなく管理の徹底をはかること。

[4] 横断的アタックサーフェスマネジメント事業等をとおして GSOC から情報提供している脆弱性については、リスクベースを評価した上で通知しており、参考とされたい。