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
（重要インフラ事業者等に対する注意喚起）

2026 年 5 月 18 日
内閣官房国家サイバー統括室、内閣府政策統括官（経済安全保障担当）
警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省、防衛省

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ます。

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す。

サイバーセキュリティ性能のより高い AI（高性能 AI）は、ベンダ等における脆弱性の発見・修正等や重要インフラ事業者等[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ます。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ます。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、高性能 AI を積極的にサイバー防御に活用していくことも含め、対策強化を早急に進めていくことが必要です。

このため、重要インフラ事業者等においては、経営層のリーダーシップの下、高性能 AI の悪用リスクに備えたサイバーセキュリティ対策の実施や、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強化をお願いします。

1．経営層のリーダーシップの下でのサイバーセキュリティ対策

サイバーセキュリティ対策は、企業活動におけるコストや損失を減らすために必要な投資（将来の事業活動・成長に必須な費用）と位置付けることが重要です。特に重要インフラ・サービスの機能停止が経済社会にもたらす影響の大きさは言うまでもありません。「サイバーセキュリティ経営ガイドライン」[2]（経済産業省・IPA[3]）も参照し、組織のリスクマネジメントの責任を担う経営層のリーダーシップの下で、リスク対策の実施方針の検討、予算や人

[1] 本文書では、「重要インフラのサイバーセキュリティに係る行動計画」に基づく重要インフラ事業者等（重要インフラ事業者及びその組織する団体並びに地方公共団体）、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）第 50 条第 1 項に規定する特定社会基盤事業者及び防衛産業の事業者をいいます。

[2] 経済産業省　サイバーセキュリティ経営ガイドラインと支援ツール
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[3] 独立行政法人情報処理推進機構

材の確保・割当、実施状況の確認や問題の把握・対応等のサイバーセキュリティ対策の実施をお願いします。

2．基本的なサイバーセキュリティ対策の確実な実施及び更なる対策の強化

英国 AISI による Claude Mythos Preview に関する評価[4]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、構成管理及び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を改めて示されております。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[5]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おります。

今後策定される「重要インフラのサイバーセキュリティ対策のための統一基準」（重要インフラ統一基準）[6]や各分野の安全基準等も参照しつつ、資産管理、リスクアセスメント、脆弱性管理、アカウント管理・認証・アクセス制御、バックアップの確保、監視・分析、事業継続計画の策定、インシデントへの対応及び復旧、組織の壁を越えたサプライチェーン・リスクへの対応等、基本的な対策の確実な実施をお願いします。これらの実施状況については、実効的な対策を継続的に行うべく、今後、関係省庁・関係機関を通じて機動的に確認しますのでご協力をお願いします。

加えて、更なるサイバーセキュリティ対策水準の向上のため、内部・外部を問わず全てのアクセスを信頼せず継続的に検証する「ゼロトラスト」の考え方に基づくシステム設計・運用への移行、侵害を前提として組織内の不審な活動や攻撃痕跡等を能動的に検知・分析する取組（脅威ハンティング等）の強化、高性能 AI を活用したサイバーセキュリティ対策の強化[7]（例：脅威検知・インシデント対応・脆弱性発見等）等、更なる取組の検討・実施を推奨します。また、各分野におけるセキュリティ対策を実践する人材の育成の観点から、NICT[8]による実践的サイバー防御演習「CYDER」[9]や、IPA 産業サイバーセキュリティセンターに

---

[4] 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

[5] 米国 CISA　CI Fortify: Strengthening Resilience Across Critical Infrastructure
https://www.cisa.gov/topics/industrial-control-systems/ci-fortify

[6] 2026 年 4 月「重要インフラ統一基準（案）」に関する意見の募集について
https://www.cyber.go.jp/policy/group/infra/report.html

[7] 高性能 AI の活用にあたっては、情報漏えいや意図しない学習への流用等のリスクを適切に管理する必要があることに留意。

[8] 国立研究開発法人情報通信研究機構

[9] NICT 実践的サイバー防御演習「CYDER」　https://cyder.nict.go.jp/

よる「中核人材育成プログラム」[10]等の活用も検討ください。

また、国家サイバー統括室は、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、被害防止に向け、必要とする主体に適切な形での情報提供に取り組みます。そのため、重要インフラ事業者等においては、インシデントやその予兆等を確認した場合には、所管省庁等を通じて国家サイバー統括室まで連絡[11]をお願いします[12]。

3．高性能 AI により高速化する脆弱性の発見・修正等への対応

ベンダ等による高性能 AI の活用により、脆弱性の発見・修正等が高速化することが考えられます。また、高性能 AI が攻撃者に悪用されることにより、脆弱性の発見から悪用までの時間が極めて短くなるとともに、多数の脆弱性への対応が必要となります。こうした蓋然性が高まっていることを前提に、既知の未処理脆弱性のリスクを改めて検証し対応を行うとともに、資産管理を徹底した上で、脆弱性情報を積極的に収集し、発見された脆弱性のリスク評価及びリスクに応じた対応（修正プログラムの適用やリスク緩和措置等）を速やかに行うことをお願いします。また、多数の脆弱性への対応を同時並行で求められる可能性が高まることから、脆弱性の影響度、悪用リスク、事業継続への影響等を踏まえた優先順位付けを行うことも重要です。

その際、迅速に行われるべきリスク評価及びリスクに応じた対応は、事業継続等の観点も踏まえた総合的な判断となり得ることから、あらかじめそのプロセス・体制等を構築し、業界団体や事業所管省庁とも情報交換を図ることが推奨されます。

---

[10] IPA　中核人材育成プログラム 事業内容
https://www.ipa.go.jp/jinzai/ics/core_human_resource/about.html

[11] 「重要インフラのサイバーセキュリティに係る行動計画」では、重要インフラ事業者等は重要インフラ所管省庁及びセプターを経由して内閣官房へ情報連絡を行い、内閣官房は重要インフラ所管省庁及びセプターを経由して重要インフラ事業者等へ情報提供を行うことを基本としています。

[12] 警察では、各都道府県警察や重要インフラ事業者等で構成される「サイバーテロ対策協議会」等の枠組みを通じて情報提供・注意喚起等を実施しているところ、実空間における対応もあり得ることから、重要インフラ事業者等においては、警察にも相談等をお願いします。