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
～Project YATA-Shield～

2026 年 5 月 18 日

内閣官房国家安全保障局、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）、内閣府科学技術・イノベーション推進事務局、
警察庁、金融庁、デジタル庁、総務省、外務省、
文部科学省、厚生労働省、経済産業省、国土交通省、防衛省

1．背景・課題認識

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など、サイバーセキュリティにおける脅威に直面している状況である。

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て、重要インフラ事業者等[1]への対応と脆弱性の発見・修正等に関する対応の双方に、サイバー安全保障の観点から、危機感を持って迅速に取り組むことが必要不可欠である。

こうした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、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ある。

このため、重要インフラ事業者等においては、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行うとともに、ベンダ等においては、高性能 AI の活用を含め、より早期の脆弱性の発見・修正等の実施が求められる。

---

[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う。

こうした喫緊の課題に対して、関係省庁・関係機関の緊密な連携の下、政府一体となって対応するため、「Project YATA-Shield」と題して、ここに関係省庁・関係機関による施策を取りまとめることとし、関係省庁・関係機関は、これら施策を迅速かつ的確に実施することとする。

2．実施する施策

1）重要インフラ事業者等及び政府機関等への対応

①重要インフラ事業者等への注意喚起等

［国家サイバー統括室、重要インフラ所管省庁等、内閣府］

重要インフラ事業者等において、経営層のリーダーシップの下、基本的なサイバーセキュリティ対策の確実な実施や、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が速やかに実施されるよう、注意喚起を行う。

また、国家サイバー統括室は、重要インフラ事業者等からのインシデント報告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、被害防止に向けて、必要とする主体に適切な形で情報提供する。そのため、重要インフラ事業者等からのインシデント情報の収集に取り組む。

加えて、重要インフラ所管省庁は、重要インフラ機能の確保の観点から、重要インフラ役務の提供上重大な脆弱性が認められる場合等には、国家サイバー統括室等との連携の下、重要インフラ事業者に対し必要な対応を行う。

②金融分野等での先行的な取組の実施及び他分野への展開

［国家サイバー統括室、重要インフラ所管省庁］

金融分野では、4 月 24 日に、民間企業・政府等が共通理解を持って必要な対応を検討・実施するための官民連携の枠組みが設置された。また、経済産業省の所管分野においても、５月１日に、官民での認識共有を図るための意見交換が行われた。引き続き、各重要インフラ分野において、その分野特性も踏まえて必要な対応を検討・実施できるよう、官民連携を推進する。

③人材育成支援［総務省、経済産業省、文部科学省、関係省庁］

重要インフラ事業者等のサイバーセキュリティ人材を育成し、サイバー対処能力強化に繋

げるため、NICT[2]による実践的サイバー防御演習「CYDER」や、IPA[3]産業サイバーセキュリティセンター等による人材育成支援、リ・スキリング等を含む大学・専修学校等におけるサイバーセキュリティ人材育成機能の強化を推進する。

④政府機関等[4]の情報システムにおける対応

［国家サイバー統括室、デジタル庁、関係省庁］

民間事業者のみならず、政府機関等に対しても基本的なサイバーセキュリティ対策の確実な実施や、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応強化が速やかに実施されるよう、注意喚起を行う。また、政府機関等の情報システムにおいても、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を進める。

２）脆弱性の発見・修正等の対応

①外国政府機関や AI 開発者等との更なる連携［国家サイバー統括室、外務省、関係省庁］

これまでにも外国政府機関や AI 開発者等との情報交換等を積み重ねているところ。我が国のサイバー対処能力強化を図る観点から、重要インフラ事業者等やベンダ等のニーズも踏まえつつ、外国政府機関や AI 開発者等との更なる連携を図り、高性能 AI へのアプローチも含め、必要な情報収集・対応を行う。

②ソフトウェア・ベンダへの注意喚起［経済産業省、国家サイバー統括室］

ソフトウェア・ベンダ[5]が、セキュア・バイ・デザインの原則に基づき、高性能 AI も活用しながら、ソフトウェア開発ライフサイクル全体において脆弱性の早期発見・対応に率先して取り組むよう注意喚起を行う。これを通じて、脆弱性を低減させた上でのソフトウェアのリリースや、残存する脆弱性の修正プログラムの作成・提供等を促す。

③AISI[6]による技術支援等［内閣府、国家サイバー統括室］

AISI により、フロンティア AI モデルのサイバーセキュリティ性能や悪用等を迅速かつ的確に把握するための情報収集・評価の実施及びこれを踏まえた情報提供、ガイドラインの策定等、これらを実施するための評価方法・環境等の構築、英国 AISI を始めとする諸外国 AISI

---

[2] 国立研究開発法人情報通信研究機構

[3] 独立行政法人情報処理推進機構

[4] 国の行政機関、独立行政法人及びサイバーセキュリティ基本法（平成 26 年法律第 104 号）第 13 条に規定される指定法人をいう。

[5] ソフトウェアを開発・提供・運用する主体

[6] AI セーフティ・インスティテュート

との連携を行う。

④技術開発の推進［内閣府、経済産業省、総務省、文部科学省］

経済安全保障重要技術育成プログラムや NICT によるビッグテック等との共同研究、研究機関等による技術開発を通じて、我が国の脆弱性の発見・修正等の AI 技術の高度化を図る。

⑤高性能 AI を活用したサイバー対処能力の強化［国家サイバー統括室、警察庁、防衛省］

高性能 AI を悪用したサイバー攻撃の増加を念頭に、サイバー関連データの国家サイバー統括室への集約の推進や、機密性の高いデータの取扱い、これらを踏まえた迅速な意思決定を行う上での AI 活用の考え方等の検討・具体化、AI を活用した資機材の導入等、AI を活用したサイバー対処能力の向上・強化に努める。その上で、サイバー対処能力強化法[7]に基づく協議会の枠組みの下、IPA・AISI と連携し情報共有等の取組を強化する等、AI セキュリティに関する官民連携の強化を図る。

3．フォローアップ

AI を巡る動向が急速に変化する中においても、より実効的な対応を継続的に行うべく、関係省庁・関係機関はこれら施策の実施状況を機動的に確認し、追加的な対応を不断に検証・実施する。

[7] 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和 7 年法律第 42 号）