AMT/NEWSLETTER
Cyber & AI Security

2026 年 9 月 28 日

OpenAI や Google、Anthropic など 100 社超の IT・セキュリティ企業、共同書簡

―「サイバー防御に向けた共同行動の呼びかけ」を公開―

弁護士 清水 亘 / 弁護士 石川 雅人

Contents

Ⅰ. 概要

OpenAI や Google、Anthropic など 100 社超の IT・セキュリティ企業は、2026 年 8 月 31 日、AI サイバー攻撃の急増に警鐘を鳴らす目的で、サイバー防御を世界規模で強化するための共同書簡「サイバー防御に向けた共同行動の呼びかけ」を公表した[1]（以下「本書簡」という。）。

本書簡によれば、今後数か月で、世界中のモデルの能力が高まるにつれ、AI を利用したサイバー攻撃ははるかに広範かつ高度になると予想される。病院や浄水場からインターネットを支えるインフラまで、地域社会が依存する企業や公共サービスが危険にさらされているといえる。

そして、本書簡は、現在の AI の進歩を踏まえて、長年蓄積してきた脆弱性を修正する新たな手段を、防御担当者はす

1 https://openai.com/ja-JP/collective-cyberdefense/（日本語版）

でに得ていることから、断固として行動すれば、防御側に与えられたこの機会を生かし、デジタル世界をはるかに安全なものにできる、と述べている。以下、本書簡の内容を紹介する[2]。

II. 3 つの原則

本書簡は、次の 3 つの原則を提案している。

1. 従来どおりのセキュリティでは不十分だと認識すること

長年放置されたバグ、過剰な権限、設定ミス、安全でない未修正のソフトウェア、脆弱な認証、レガシーシステムの技術的負債により、システムは危険にさらされている。特に重要インフラのセキュリティチームは、以前からリソースが不足しており、ツールと資源の大幅な増強を必要としている。

2. より多くの防御担当者に、サイバー対応能力を備えた AI を提供すること

AI は、より多くの防御担当者が専門技能を活用できるようにし、中核的なセキュリティ業務をより速く、低コストで、効果的にすることができる。ツール、実践的な知識、検証済みの修正を共有すれば、ある組織の取り組みを多くの組織の保護に役立てることができる。

3. 共同対応を推進すること

サイバー能力は世界中で進歩しており、これは全体として好ましいことであるが、未来を一社だけが支配すべきではなく、同時に、世界規模の対応が必要であることも意味している。セキュリティ基準を引き上げ、新たなサイバー脅威への新しい解決策を見いだすには、新たな連携が必要である。

本書簡によれば、あらゆる組織、サイバーセキュリティ企業、テクノロジーパートナー、政府、フロンティア AI 企業には重要な役割がある。特に予算が限られる重要インフラ組織に対し、ツール、資金、実践的な支援を提供し、防御側の優先課題への対応を加速することが必要である。

III. 次に必要だと考える取り組み

そして、本書簡は、それぞれの組織について、次に必要だと考える取り組みを示している。

1. すべての組織

サイバー防御を経営陣の最優先課題として直ちに位置付けることが必要である。セキュリティ基準を引き上げ、重要な事業運営を除くすべてに優先するインシデントと同等の緊急性と連携体制で、その基準を満たす。最もリスクの高い脆弱性を修正し、不可欠なサービスを中断せずに結果を検証する。また、AI 生成コードを含め、調達、構築、導入するものに求めるセキュリティ基準を引き上げる。最小権限、強固なアクセス制御、多層防御を組み込むため、システムをアップグレードまたは入れ替える。広範な保護には高性能で低コストのモデルを使用し、最も難しい課題にはフロンティア能力を活用する。不可欠なサービスを中断せずにパッチを適用できないシステムには、代替統制を適用して検証する。

---

2 本書簡（日本語版）（前掲注 1）の用語・表現を基本的にそのまま使用している。

2. サイバーセキュリティ企業とテクノロジーパートナー

フロンティアレベルのサイバー能力に対して防御策を継続的にテストし、既存ツールを AI で強化し、テクノロジーパートナーと連携して現時点の防御の穴を埋めるなど、AI を利用した継続的な攻撃への対応を主導する。重要インフラ事業者が AI による防御を利用・導入できるようにし、ツールの導入や修正の検証を実践的に支援する。また、重要インフラのサプライチェーンに属するメーカーやシステムインテグレーターと連携して、パッチの適用と暫定的なガイダンスの提供を進める。脅威インテリジェンスと検証済みの手順書を共有し、保護できた組織の数、攻撃を封じ込める速さ、修正の有効性によって進捗を測る。

3. 政府

地域、国、国際の各レベルでサイバー防御を連携させる。政府と産業界の既存の連携経路を強化して、対処に役立つ脅威インテリジェンスを共有し、最も深刻なリスクを優先するとともに、世界各地のインシデント対応と復旧を調整する。まず、対応する人員や予算が不足している不可欠なサービスを対象に、サイバー防御へ資金を提供する。特に重要インフラのサプライチェーンを対象に、信頼できるアクセスプログラムの拡充を加速し、ほかの防御担当者にも防御機能の利用を広げる。信頼できるセキュリティ事業者やパートナーを通じて、病院、水道事業者、地方自治体が、高性能な防御用 AI、許可を得たテスト、実践的な支援を利用できるようにする。攻撃者に代償を負わせる。

4. フロンティア AI 企業

特にリソースが不足している重要インフラの防御担当者に対し、責任あるモデル利用、十分な資金、トレーニング、実践的な支援を提供する。可観測性とセキュリティのためのツールを構築し、エージェントのアイデンティティを追跡可能かつ説明責任を負えるものにするとともに、継続的な監視のベストプラクティスを共有する。許可を得たテスト、非公開での脆弱性報告、検証済みの修正に投資し、政府、セキュリティパートナー、オープンソースのメンテナーとツール、手順書、信頼できる脅威評価を共有して、備え、対応、復旧を強化する。

Ⅳ. 産業界と政府のリーダーへの呼びかけ

最後に、本書簡は、産業界と政府のリーダーに対し、技術、資源、専門知識を総動員して、この取り組みに臨むよう呼びかけている。この書簡は、まず不可欠なサービスを守るチームに、サイバー対応能力を備えた AI を届けるとしている。また、この書簡は、最も危険な脆弱性を修正して結果を検証し、有効な対策を共有することで、他の組織もそれを基盤に改善できるようにすると述べている。そして、この書簡は、力を合わせれば、現在の AI の進歩を、すべての人に恩恵をもたらす持続的なセキュリティ向上につなげられるとし、デジタルインフラを、より安全なものにすることを呼びかけている。

Ⅴ. おわりに

本書簡は、業界や政府のさまざまな組織とともに、サイバー防御に向けた緊急の連携を呼びかけている。

AI の急速な進化に対し、2026 年 9 月 12 日、Anthropic の CEO ダリオ・アモデイ氏は、2026 年の夏ごろから AI の進化が劇的に加速していると指摘し、セキュリティ対策が追い付く時間を確保するため、AI 開発を遅らせる必要があると指摘した。この指摘には、OpenAI のサム・アルトマン氏や、自身も AI 開発を手掛けるイーロン・マスク氏も賛同している。AI の進化に伴うサイバーセキュリティの重要性がますます高まっており、企業としても対策が急務である。

以上

■ 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

■ 本ニュースレターの執筆者は、以下のとおりです。

弁護士 清水 亘 wataru.shimizu[at]amt-law.com
弁護士 石川 雅人 masato.ishikawa[at]amt-law.com
※メールを送信する際には、[at]を@に変更してお送りください。

■ ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

■ ニュースレターのバックナンバーは、こちらにてご覧いただけます。