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
（ソフトウェア・ベンダに対する注意喚起）

令和８年５月 18 日
内閣官房国家サイバー統括室、経済産業省

足下で、ソフトウェア※の脆弱性発見について高い能力を有する AI（高性能 AI）の開発が進んでいる。こうした高性能 AI は、未知の脆弱性の早期発見や是正によりセキュリティ向上に役立つ一方で、仮に悪意ある者に使われた場合には、サイバーセキュリティ上のリスクが一気に高まるおそれがある。

このため、政府全体としては、内閣官房国家サイバー統括室を中心に 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関する対策パッケージ「Project YATA-Shield」をとりまとめたところである。経済産業省としても、高性能 AI を活用したサイバーセキュリティ産業の育成も重要との観点の下、引き続き、国内のサイバーセキュリティ対策の実装を支える高度な人材育成や、研究開発などサイバーセキュリティ産業の育成・振興等の各種施策の企画・実行を推進していく予定である。

こうした政府の取組も念頭に置きつつ、広く産業界で用いられているソフトウェアを開発・提供・運用する主体（ソフトウェア・ベンダ）の皆様におかれては、セキュア・バイ・デザインの原則に基づき、以下のとおりソフトウェア開発ライフサイクル（SDLC）全体において高性能 AI も活用しながら脆弱性の早期発見・対応に率先して取り組むことをお願いしたい。なお、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されたい。

１．リリース前のソフトウェアについては、高性能 AI を積極的に活用し、リリース後の脆弱性発見の可能性を低減させた上で、リリースをする。

２．リリース後のソフトウェアについては、自ら高性能 AI を積極的に活用して自らがリリースしたソフトウェアの脆弱性の把握に努めるとともに、脆弱性関連情報の収集・早期把握に努めつつ、脆弱性が発見された場合には（必要に応じ高性能 AI も活用して）パッチを早急に作成し、顧客に速やかに提供する。

※　ソフトウェアには、製品として顧客に提供されるソフトウェアのほか、クラウドサービスなど顧客が直接利用する IT サービスであるソフトウェアサービス、システム・サービスの構成要素として提供されるソフトウェアも含まれる。

＜参考資料＞

- 国家サイバー統括室「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年 10 月）
- 経済産業省／国家サイバー統括室「サイバーインフラ事業者に求められる役割等に関するガイドライン」（令和８年３月）
- 経済産業省「産業界へのメッセージ」（令和８年４月）
- 独立行政法人情報処理推進機構「情報セキュリティ早期警戒パートナーシップガイドライン」（最終更新：令和８年４月）