IoT セキュリティ観点における
ChatGPT に対する考察

一般社団法人セキュア IoT プラットフォーム協議会

理事長　辻井 重男

２０２３年5月

1. はじめに

昨今、OpenAI 社の AI チャットボット ChatGPT を中心に AI の活用について、その効用と課題が広く議論されているのは周知のことである。例えば ChatGPT により、幅広い領域での業務の効率化が期待される一方で、その生成される結果の正確性・信頼性の保証や生産物の著作権の所在、機密情報の漏洩などの脅威も想定され、その使い方について議論が進められている。また知識や経験に乏しくとも、ChatGPT を活用することにより、エキスパートと同等の結果を導く可能性さえ出てきており、その悪用も懸念されるところである。

2. サイバーセキュリティ上の脅威

サイバーセキュリティの観点で考えると、いままで専門知識をもつ人間や組織しか開発できなかったマルウェアなどの悪意を持ったプログラムの生成に活用される可能性を含んでいることを憂慮する。その結果、今まで以上にマルウェアが広く生成、流布され、犯罪に悪用される脅威があることは無視できない。ChatGPT にはそのような悪用を防ぐために、不適切な問いには回答を拒否するセキュリティフィルタなどの安全上の制限がかけられているが、残念ながらそれをかいくぐるような手段も研究をされ、対策に限界もあるのが現状である。

つまり IoT システムにおいても、悪意を持ったコードが生成され、それが気づかれないうちに機器に混入・実装される可能性があるということである。そのような IoT 機器が産業用途で活用され、M2M で何らかのインタラクションが発生した場合に、予期せぬ結果がもたらされたり、機密情報や知財の漏洩に繋がることが懸念される。またコンシューマ用途で利用される機器に混入した場合もプライバシー侵害や情報漏洩に繋がることは否定できないのである。

3. ソフトウェアサプライチェーンの安全性強化

このような環境変化を前提に、悪意を持ったプログラムの混入を防ぐためには、ソフトウェアサプライチェーンの安全性を強化することが喫緊の課題であると考える。
具体的な対策としては、生成されたプログラムをコード署名により安全性を担保することやソフトウェアの部品表ともいえる SBOM(Software Bill of Material)による管理が必要であると考える。

これは当協議会が会員企業と共に、2022 年の夏より進めてきた Linux Foundation/OpenSSF(Open Source Security Foundation)との連携によるソフトウェアセキュリティに対する取組みともつながるものである。いまや重要インフラも含む多くの IoT システムで利用されるオープンソースについて、 Log4j 問題に代表される重大かつ広範囲なインシデントに対応する為、米国政府と連携し、活動する Linux Foundation/OpenSSF の動きに注目すべきということは以前にリリースしたドキュメントでも述べたとおりである。その活動の中でも Sigstore による電子署名サービスや SBOM を活用したソフトウェアサプ

ライチェーン管理が重要な施策として取り上げられている。

さらに ChatGPT を使って、偽の SBOM を生成されることさえ考えられる。そのため確実な本人性確認と、署名対象の真贋を立証できることが重要となることも忘れてはならない。

※参考資料：

「経済安全保障への対応～オープンソースセキュリティの動向～」(2022/ 8 /25)
https://www.secureiotplatform.org/wp-content/uploads/report_20220825.pdf

「経済安全保障への対応～国際連携におけるサイバーセキュリティ対策の推進～」(2023/1/12)
https://www.secureiotplatform.org/wp-content/uploads/report_20230112.pdf

4. まとめ

ChatGPT の出現により、当協議会が会員企業と連携し進めてきたソフトウェアサプライチェーン管理の重要性がさらに拡大し、IoT システムの安全性確立に向けての動きをさらに加速する必要が高まってきたと考える。

日本政府としても 2023 年 5 月 9 日に、岸田文雄首相より「AI 戦略会議」を立ち上げ、ChatGPT も含めて AI に関わる課題について、政府関係者と有識者で議論を開始する旨が発表された。この中でも当協議会でも取り組む SBOM の導入も含めたソフトウェア安全基準を整備することも含まれると想定される。

以前よりセキュア IoT プラットフォーム協議会では、国際安全基準に基づくものづくりにおいて、IoT 機器の真正性担保、製造から破棄に至るライフサイクルマネジメント、および IoT 機器に組み込まれるソフトウェアのサプライチェーン管理により、IoT システム全体の安全性担保に対して研究を行ってきた。

当協議会では、引き続き会員の皆様の力を結集し、安心安全な IoT 社会の構築に向けて、取り巻く環境変化をいち早く捉え、国際安全基準や日本政府の施策を基に、セキュリティ対策の推進に取り組んでいく所存である。特に多くの IoT システムにおいてオープンソースが活用されていることを考慮すると、産業界のみならずコミュニティと連携したセキュリティ対策支援に力を入れていくことが重要であると考える。