オープンソースにおけるサプライチェーン攻撃

○八田真行（Masayuki Hatta）
Keywords：オープンソース、ソフトウェア開発、セキュリティ、コミュニティ

1　目的

本研究の目的は、オープンソース・ソフトウェア開発におけるサプライチェーン攻撃について事例の分析を行い、そこから近年におけるオープンソースの変質を浮き彫りにすることである。

ソフトウェアが巨大化、複雑化し、相互に依存することが常となった現在、一部を食い破ることでシステム全体を不安定化させる攻撃は「サプライチェーン攻撃」と呼ばれて非常に懸念されている。オープンソースによるバザール型開発は、「目玉の数さえ十分あればどんなバグも怖くない」と称されるようにこの種の攻撃に強いとされてきたが、2024 年 3 月に発覚した XZ Utils へのバックドア混入事例は、必ずしもそうとは言えないことを示した。

本研究では、こうしたオープンソースにおけるサプライチェーン攻撃について非オープンソースの事例も含めて分析し、特に最近の事例は単なる技術的問題に留まらず、近年のオープンソース自体の変質と密接な関係があることを明らかにしたい。

2　方法

本研究の調査・分析方法は事例研究である。サプライチェーン攻撃に関して非オープンソースの事例に加え、ケン・トンプソン・ハック（1984 年）、Debian における mICQ のコード混入（2003 年）、OpenSSL における Heartbleed 問題（2014 年）といったオープンソースにおける類似の事例を分析し、最近の XZ Utils の事例をオープンソースの歴史的な文脈の中に位置づける。

3　結果

サプライチェーン攻撃に関して、オープンソース固有の問題の所在を明らかにすることができた。

4　結論

サプライチェーン攻撃に対して Reproducible Builds などオープンソース側の（技術的）対策を示すとともに、最近の事例はメンテナの疲弊や金銭を含めたリソース配分の失敗など、いわばオープンソース神話そのものの綻びに起因すること、すなわち技術的な問題であると同時に、極めて組織的、経営的課題であることを主張する。

【主要参考文献】

Hatta, M. (2022). The Nebraska problem in open source software development. Annals of Business Administrative Science, 21(5), 91-102. https://doi.org/10.7880/abas.0220914a

Ladisa, P., Plate, H., Martinez, M., & Barais, O. (2023). SoK: Taxonomy of Attacks on Open-Source Software Supply Chains. 2023 IEEE Symposium on Security and Privacy (SP), 1509-1526. https://doi.org/10.1109/SP46215.2023.10179304