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～

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

２０２２年８月

1. はじめに

いまやオープンソースソフトウェアは重要インフラを中心としたIoT環境でも利用され、その脆弱性を突かれた重大インシデントも発生しており、大きな課題となっています。

特にボランティアベースで開発やプロジェクトが推進されるオープンソースは、脆弱性対策やリスク発生時の対応対策が十分とは言えないという課題があり、特に社会的にも大きな影響を与えたLog4jの脆弱性問題は記憶に新しいところです。

この課題は、セキュア IoT プラットフォーム協議会が注目する、日本の経済安全保障においても、グローバル環境での安全なサプライチェーン構築を考えると、非常に重要な課題だと考えます。

その対応策として、全世界で 2,950 以上の組織をメンバーとする Linux Foundation が2020年に設立した「Open Source Security Foundation (OpenSSF)」の動向は着目すべきだと考えます。

２．OpenSSFの動向

Linux Foundation/OpenSSFの動きは米国政府と緊密に連携しており、2022年1月にホワイトハウスが、セキュリティ関連の政府機関や米国を代表する民間企業を集めて開催したソフトウェアセキュリティに関する会議を受け、「Alpha-Omega Project」を開始しました。

「Alpha-Omega Project」はオープンソースのセキュリティ強化と安全性を確保するプロジェクトであり、2022年5月には、NSC(米国国家安全保障会議)、CISA(米国サイバーセキュリティ・社会基盤安全保障庁)、NIST(米国国立標準技術研究所)などの米国政府機関やAWS、Google、Intel、Microsoft、VMWareなど民間企業が参画し、オープンソースのセキュリティを強化する3つの目標とリスク評価、SBOM、セキュリティ教育などを含む10項目の動員プラン(対策指針)を発表しています。

3. OpenSSFが提唱する3つの目標と10項目の動員プラン

●3つの目標

・セキュアなOSSの作成

・脆弱性の検出と修復の強化

・エコシステムのパッチ応答時間を短縮

●10項目の動員プラン

・セキュリティ教育

・リスク評価
・デジタル署名
・メモリの安全性
・インシデントへの対応
・スキャン機能の向上
・コード監査
・データ共有
・SBOM の普及
・サプライチェーンの改善

4. 今後の対応

米国政府とも連動して推進されるこの動きは、グローバルサプライチェーンの中に組み込まれて活動をする以上、日本の企業にも無視できるものではありません。特に我が国で推進されている経済安全保障推進の流れとも、緊密に連携する動きであると認識すべきだと考えます。その流れを受け日本においても 2022 年 8 月 23 日に Linux Foundation が「Open Source Security Summit Japan」を開催し、情報発信を行いました。

セキュア IoT プラットフォーム協議会が運営を担当する JAPANSecuritySummit 2022 (2022/10/24～11/6 開催)においても、そのオープニングデイのキーノートとして、Open SSF の代表(General Manager)である Brian Behlendorf 氏を招へいし、オープンソースに関するグローバル視点でのセキュリティ動向と問題提起を行う準備を進めています。

当協議会では経済安全保障の推進に向けて、オープンソースのセキュリティ実装に着目し、今後も継続的に Linux Foundation /OpenSSF との連携による情報発信を進めてまいります。