

# 令和元年度イノベーション戦略策定事業の成果概要

## － オープンソースソフトウェアの脆弱性情報管理に関する戦略策定 －

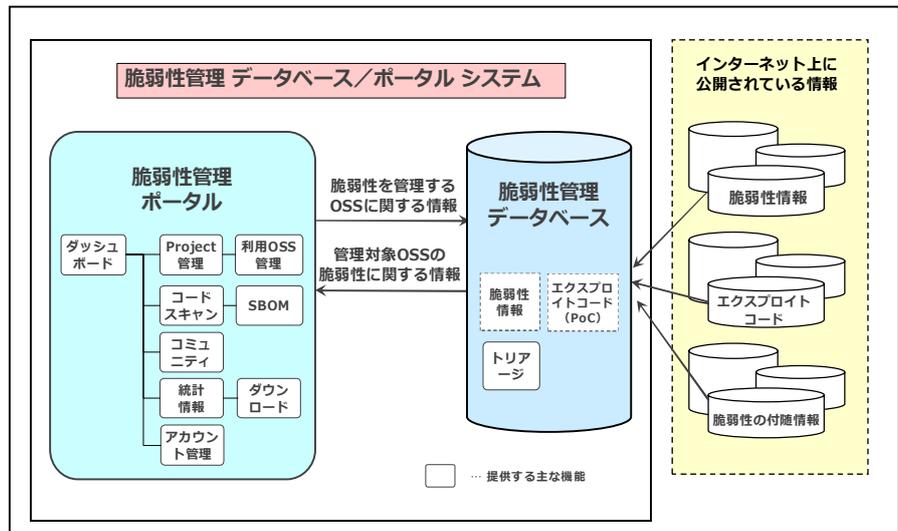
令和2年5月

(一財) 機械システム振興協会

令和元年度イノベーション戦略策定事業の5テーマの1つとして、(一社) コンピュータソフトウェア協会に委託して、「オープンソースソフトウェアの脆弱性情報管理に関する戦略策定事業」を、次の通り実施しました。

### 【事業の目的】

昨今のソフトウェアの開発においては、オープンソースソフトウェア(OSS)を用いることがほとんどです。そのため、情報セキュリティ対策の面においても、OSSに着目して、ソフトウェアのサプライチェーン全体のセキュリティ対策を行う必要があります。



このため、ソフトウェア ISAC (Information Sharing and Analysis Center) の事業化に向けて、OSS の脆弱性情報管理に関する戦略を策定しました。

### 【令和元年度事業の概要と主要成果】

コンピュータソフトウェア協会に産学官の専門家から成る戦略策定委員会を設置し、ソフトウェア開発における OSS の利用状況を調査して、その現状及びソフトウェア ISAC の必要性を明らかにするとともに、脆弱性情報管理に必要なデータベース及びポータルの設計 (要件定義) を行いました。その主要な成果は次の通りです。

#### ① OSS の利用状況に係るヒアリング調査

我が国のソフトウェア開発事業者 21 社からヒアリング調査を行い、次のことなどが分かりました。

- i) ソフトウェア開発に当たっては、約 7 割の事業者が外部委託を行っており、約 8 割が OSS を使用している。
- ii) バイナリ納品の割合が高く (ソースコード納品が約 3 割、バイナリ納品が約 7 割)、SBOM (Software Bill of Material) に代表されるコンポーネント管理が適切に行われていない。(注: バイナリは 1,0 の機械語のプログラムで、人が読めない。SBOM

は部品の管理表。)

- iii) PSIRT (Product Security Incident Response Team) が必要との認識は高まっているが、「ヒト」の問題があって PSIRT を構築している社は少ない (14%)。

このように、我が国のソフトウェア開発においては脆弱性管理が十分ではなく、エンジニア個人での管理、企業の努力のみに任せているのはサプライチェーンの根本的な問題が残り、ソフトウェア ISAC が個々の企業を支援する必要性が明らかになりました。

## ② ソフトウェア ISAC の情報システムの設計 (要件定義)

OSS の脆弱性情報については、国内では (独法) 情報処理推進機構 (IPA) や (一社) JPCERT コーディネーションセンターが、国際的には米国国立標準技術研究所 (NIST) などがインターネット上に公開していますが、情報が膨大なため、ソフトウェア ISAC において、トリアージ情報とともに脆弱性管理データベースで管理する必要があります。また、ソフトウェア ISAC の利用企業 (ソフトウェア開発を行う企業) に対して、プロジェクト管理やアカウント管理などができるように、ポータルを用意する必要もあります。

これらの情報システムは、特に高いセキュリティレベルにして、ソフトウェアの開発への攻撃から防御する必要がありますし、ソフトウェア開発のサプライチェーン全体を通じた脆弱性管理のために、発注企業と受注企業との連携を可能にすることなども大切になります。このため、戦略策定委員会において、これらの情報システムのあり方を検討するとともに、その検討を踏まえた要件定義書を外注により作成しました。

## ③ OSS 対応に関するソフトウェア ISAC の戦略策定

現在、コンピュータソフトウェア協会にソフトウェア ISAC の組織 (その中のタスクフォースが今回のプロジェクトを実施) が構築されており、その今後の活動のあり方をソフトウェア ISAC の戦略として取りまとめました。その中で、脆弱性管理の情報システムの構築・運用のみならず、セキュリティテストを行う脆弱性検証センターを整備することや、コンポーネント管理の重要性をソフトウェア業界に情報発信する重要性も記述しました。

### 【今後の展開】

今後、(一社) コンピュータソフトウェア協会においては、国に働きかけて、公的資金により脆弱性管理の情報システムを構築し、ソフトウェア ISAC の活動を展開していくこととしております。また、今回のヒアリング結果を公開し、OSS のセキュリティ対策の普及啓発も行うこととしております。

### 【問い合わせ先】

イノベーション戦略策定事業全般：(一財) 機械システム振興協会 Tel: 03-6848-5036

本調査開発の詳細：(一社) コンピュータソフトウェア協会 e-mail: security\_info@csaj.jp