HITACHI
Inspire the Next

OpenSSFのサプライチェーンセキュリティ関連プロジェクトのご紹介

2023/10/31

中村 雄一
日立製作所　OSSソリューションセンタ

自己紹介

HITACHI
Inspire the Next

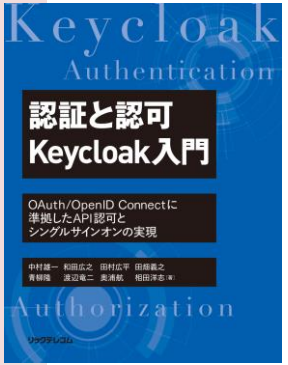
中村 雄一
株式会社　日立製作所　OSSソリューションセンタ、博士(工学)

～2008年

- SELinuxのコミュニティ活動、ビジネス開発
  - パッチ書いたりツール公開、情報家電向けSELinuxの開発
  - 執筆(書籍・雑誌記事・学術論文)・国内外講演多数
  - 研究をまとめ岡山大学にて博士（工学）の学位取得

現在

- Keycloak関連ビジネスやコントリビューション活動の立ち上げ
  API管理・認証関連サービス立上げ
  Keycloakメンテナを育成
  Keycloak書籍執筆：　認証と認可Keycloak入門（リックテレコム）
- OSSコミュニティ活動
  「OSSセキュリティ技術の会」の会長として勉強会開催や学術界との連携
  The Linux Foundation BoardとしてOpenSSFやCNCF加入に携わる



OpenSSFの概要

2020年設立のThe Linux Foundation傘下の団体
「OSSのセキュリティ全般（OSSの開発側, OSSを使う側双方）」が活動のスコープ。

2021年末のlog4jのインシデント(*)を受けサプライチェーンセキュリティにおけるOSSの懸念が高まり、
米国政府の要請で、OpenSSFがOSSセキュリティ実行計画(10 streams)を取りまとめ、
メンバ加入や活動が加速。

- 参考： https://www.jpcert.or.jp/newsflash/2021122401.html

現在、100社以上が加入。最上位のPremierには、
主要ベンダ(Amazon, MS, Google, IBM, Oracle, Cisco等)の他、
金融系のユーザ企業(Citi, CaptitalOne等)も加入。
2023年4月には弊社も加入。

OpenSSFの活動状況

HITACHI
Inspire the Next

項目	状況
OSSプロジェクトの支援	重要なOSSプロジェクトを特定し、ファンディング含めた支援を継続。OSSコミュニティ運営上のセキュリティベストプラクティスを定め、認定プログラム(Best Practice Badge)を通じて、多くのOSSプロジェクトに広がっている。
脆弱性情報の取り扱い	OSSコミュニティにおけるインシデントレスポンスチームの形成や脆弱性フォーマットの議論等が行われているが大きな動きはまだ。
サプライチェーンセキュリティの確保	ソフトウェアサプライチェーンの完全性を確保するSLSA、ソフトウェア署名ツールsigstore、リファレンスモデルFRSCA、SBOM可視化ツールGuac等活発。SLSAについては、CNCFで必須になるなどOSS開発に広がり始めている。Google, MS,Citi, スタートアップ(kusari,chainguard)がメインプレーヤー
セキュリティツールの開発	Fuzzingツール、SBOM生成ツールの議論が行われているが、まだ目立った成果は出てきていない

サプライチェーンセキュリティの取り組みについて本日はご紹介

HITACHI
Inspire the Next

- **SLSA(Supply Chain Levels for Software Artifacts)とは**
  ・ソフトウェアサプライチェーンにおける完全性確保のためのフレームワーク・ガイドライン。
  ・ソフトウェア開発から実装までのプロセスに注目して、どの段階でも「確実に真正であること＝第3者によって破壊されていないこと」を実証することで、すべてのプロセスが意図された通りに開発、ビルド、パッケージ、デプロイされたことを確認するためのフレームワーク。元々はGoogleが開発。
  ・2023年4月19日　OpenSSFがSLSA Version 1.0を公開、Google,IBM,Verison等が貢献中。

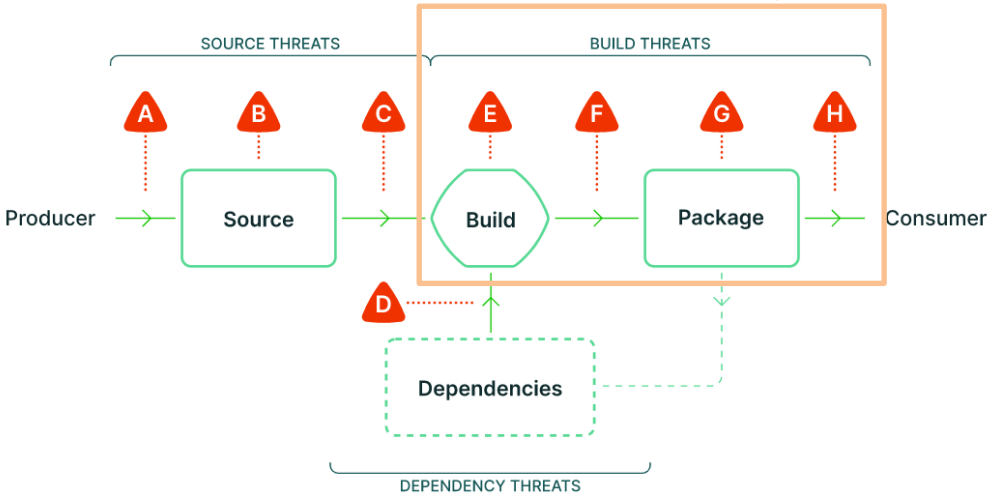
- **1～3のレベル**（v0.1では1～4までレベルが分かれていた。4はv1.0では未実装）
  L1：パッケージがどのように構築されたかを示すprovenance(来歴)　→間違い防止
  L2：ホストされたビルドプラットフォームによって生成された署名付きの来歴　→ビルド後の改ざん防止
  L3：L2に加え、強化されたビルドプラットフォーム　→ビルド中の改ざん防止
  　・同じプロジェクト内であっても実行が互いに影響を与えない
  　・来歴の署名に使用される秘密マテリアルがユーザー定義のビルドステップからのアクセス不可

SLSAを身近なもので例えると
成分リストの信頼性を高めるための食品安全取り扱いガイドライン。クリーンな工場環境の基準から、食料品店の棚に置かれた商品の中身を誰も変更しないようにする蓋の改ざん防止シールの要件など

HITACHI
Inspire the Next

●サプライチェーンにおける脅威

V1.0での対応箇所



SOURCE THREATS
- A Submit unauthorized change
- B Compromise source repo
- C Build from modified source

DEPENDENCY THREATS
- D Use compromised dependency

BUILD THREATS
- E Compromise build process
- F Upload modified package
- G Compromise package repo
- H Use compromised package

出典： https://slsa.dev/spec/v1.0/threats-overview

- SLSAの焦点はサプライチェーンの**整合性**(ソースやビルドの整合性)と**可用性**

- それぞれの脅威へのSLSAでの対策
  A：2人によるレビューで不正な変更を発見
  B：適切に保護する
  C：SLSA準拠のビルドサーバーで改ざんを検出する
  D：出所を見て対処する
  E： SLSA準拠のビルドサーバーを使う
  F･G：アーティファクトの出所を確認する
  H：直接対処はしない

HITACHI
Inspire the Next

- **SLSAがカバーしていない部分**
  コードの品質：安全なコーディング方法をとっているかは保証していない
  作成者の信頼：信頼できる組織に提供しているが、内部の人物までは保証していない
  依存関係にあるアーティファクトの信頼：アーティファクトのSLSAレベルはそれに関連するもののレベルを保証していない
- **SLSAツール**
  https://github.com/slsa-framework/slsa-github-generator
- **Provenance(来歴)とは**
  どのように作成されたかに関する情報、メタデータ
  in-totoという形式に基づいて記述される
  slsa-github-generatorで、コンテナ、go、java、rustなどのアーティファクトに対応したビルドプロセスから来歴を生成

どのソースコード、ビルドシステム、ビルドステップが使用されたか、誰が、なぜビルドを開始したかに関する情報など

CNCFのprojectではgraduationのためにSLSAへの対応が必須になっている

https://github.com/in-toto/attestation

- **in-totoとは**
  ソフトウェアサプライチェーンの完全性を保護するためのフレームワーク

  ソフトウェア製品の製造開始からエンドユーザーへのインストールまでの**整合性**を確保するように設計
  整合性はソフトウェア・ライフサイクル上のどのステップが、誰によって、どの順序で、実行されたかの記録を署名付きで保存することで実現している
  米国国立科学財団(NSF)、国防高等研究計画局(DARPA)、空軍研究所(AFRL)、Linux Foundationによって支援されているCNCFのincubating project

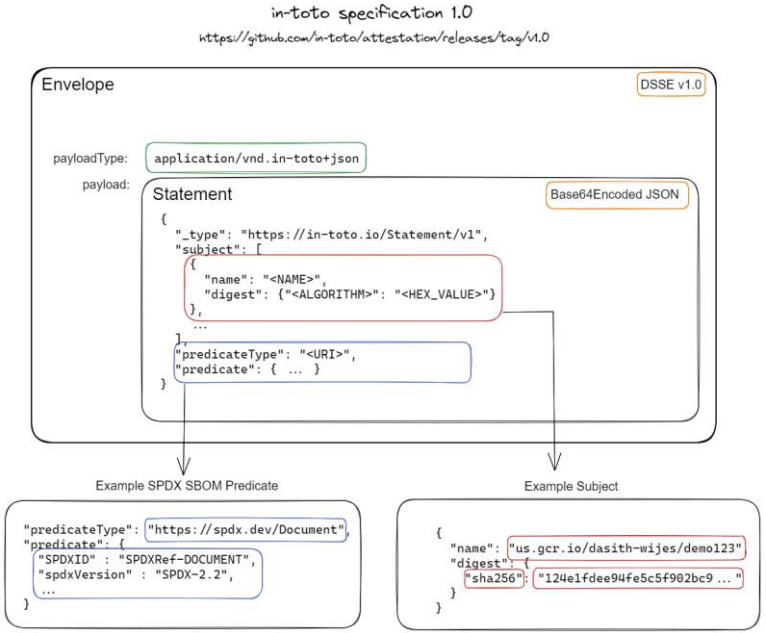
in-toto attestation framework

https://github.com/in-toto/attestation
https://slsa.dev/blog/2023/05/in-toto-and-slsa

HITACHI
Inspire the Next

SPDXやCycloneDXなどのBOMや、
SCAIレポートなどに適応している

- **in-toto attestation**
  ソースがレビューされたか、(SLSA準拠の)ビルドプロセスを経たかなど、ソフトウェアサプライチェーンの実行に関する情報を伝えるための「Statement」を定義している



出典： https://github.com/in-toto/attestation/tree/main/spec

4つのレイヤー

- Statement：証明書の中間層。証明書を特定のsubjecに紐づけて、Predicateのタイプを明確に識別する
- Predicate：証明書の一番内側。Statementのsubject内のアーティファクトに関するメタデータを含んだスキーマを定義。柔軟にカスタムできる
- Envelope：認証とシリアル化(json化など)を実行する
- Bundle：複数の証明書をまとめる方法を定義する

S2C2F

HITACHI
Inspire the Next

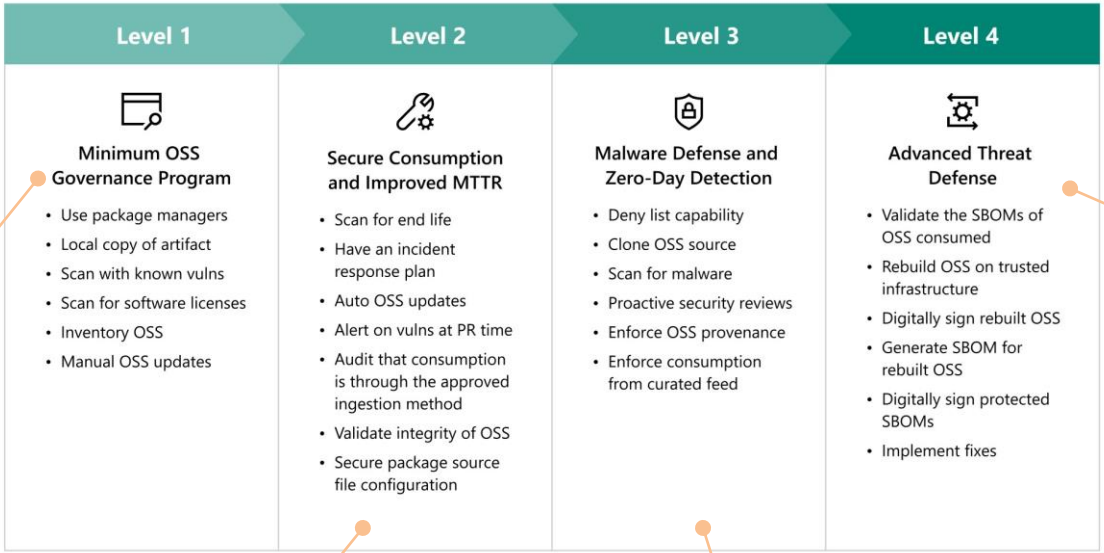
- **Secure Supply Chain Consumption Framework (S2C2F)とは**
  - ・OSSの依存関係を開発者のワークフローに安全に取り込む方法を概説および定義する
  - ・マイクロソフトによるOpen Source Software-Supply Chain Security (OSS-SSC) Frameworkが元
- ・OpenSSFのSupply Chain Integrity Working Group内に採用され、独自のSpecial Initiative Group(SIG)に編成された　→S2C2F SIGと呼ばれる

- https://github.com/ossf/s2c2f　2023年4月22日時点ではv1.1
- NSA Enduring Security Framework (ESF)がS2C2Fのガイダンスに沿った業界仕様を出す予定

OpenSSFのセキュリティフレームはSLSAとS2C2Fの2つ
SLSAはProducer、S2C2FはConsumerが対象

S2C2F

出典： https://github.com/ossf/s2c2f/blob/main/specification/framework.md



Level1
OSSのインベントリ作成、既知の脆弱性のスキャン、OSSの依存関係の更新、といった従来の方法

Level4
最も巧妙な攻撃を緩和する管理策で、大規模な実装が最も困難な管理策でもある

GitHub Advanced Security(GHAS)とGHAS on Azure DevOps(ADO)はレベル2を達成するのに役立つ一連のセキュリティ ツールを提供

Level2
OSSの脆弱性の平均修復時間(MTTR)を改善する技術を活用し、敵が操作できるよりも早くパッチを適用する

Level3
危険なOSSや悪意のあるOSSを誤って使用してしまうことを防ぐための予防的な管理策を組み合わせる

SLSAほどは活発ではない

Sigstore https://www.sigstore.dev/ https://github.com/sigstore

HITACHI
Inspire the Next

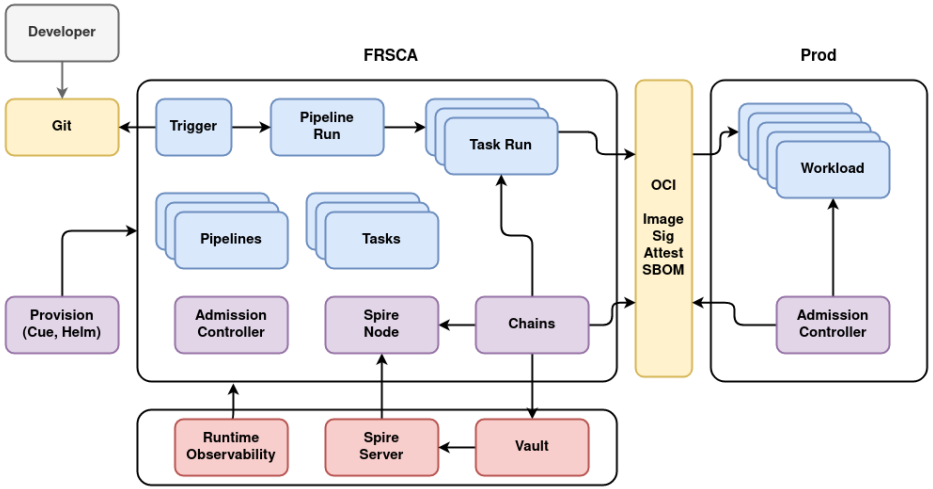
- 目的： ソフトウェアサプライチェーン攻撃からの保護を強化すること
- 内容： ソフトウェアを署名、検証するためのツールを提供
- 構成要素
  ・sigstore server：デジタル署名を作成および検証するためのサーバー
  ・cosign：署名されたコンテナイメージを検証するためのツール
  ・rekor：透過的なログ管理システム
  ・gitsign：Gitコミットに署名するツール
  ・fulcio：クラウドネイティブなPKI。オンラインでのセルフサービス証明書管理、CRLの公開、OCSPステータスのオンライン検証など

- 特長
  通常の公開鍵・秘密鍵ベースの署名の他、OpenID Connectの認証サーバを用いた「キーレス署名」をサポート。K8sプロジェクトで用いられ、OSSコミュニティでの採用が急速に広がっている。SLSAやFRSCAでは、ソフトウェアのみならず、SBOMやSLSA provenanceにデジタル署名が必須であり、署名ツールとしてsigstoreがよく用いられている

FRSCA(Factory for Repeatable Secure Creation of Artifacts)

- CNCFのベストプラクティスに基づいたセキュアなビルドパイプラインのリファレンス実装
  https://github.com/buildsec/frsca　サンプルのパイプラインはSLSA Level 3対応 (ただしv0.1)
- 元々はCitiが開発し、OpenSSFに寄贈したもの。現在はスタートアップのKusariやGoogle,Citi等がメンテ

- 下記のツールを利用
  (K8s前提)
  - CIパイプライン: Tekton
  - SBOM生成: trivy
  - AttestationやSBOM等の署名: sigstore
  - ワークロードの識別: SPIFFE(規格)・SPIRE(実装)



出典： https://buildsec.github.io/frsca/docs/getting-started/architecture/

まとめ

OpenSSFでは、サプライチェーンセキュリティ確保のための取り組みが活発に行われている。

- 特に注目すべきはSLSAとsigstore。CNCFとも連携し、OSSコミュニティでの利用が広がっている。
  OSSコミュニティでは、SBOMだけでなく、ビルド来歴であるSLSAのprovenanceを
  sigstoreの署名付きで流通することになりそう。

- SLSAに対応した開発を容易にするためのツールやOSSの開発も進んでいくと思われる。

他社商品名、商標等の引用に関する表示

・Linuxは，Linus Torvalds氏の日本およびその他の国における登録商標または商標です。
・Google is registered trademarks of Google LLC in the United States and other countries.

その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。


Hitachi Social Innovation is
POWERING GOOD