HITACHI
Inspire the Next

OSSコミュニティ活動とOpenSSFの紹介

2023/07/11

日立製作所　OSSソリューションセンタ
中村 雄一

自己紹介

HITACHI
Inspire the Next

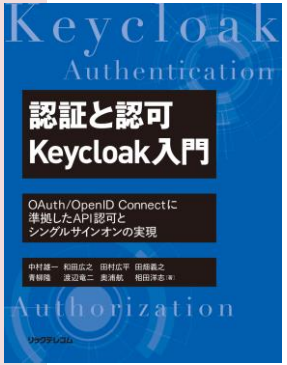
中村 雄一
株式会社　日立製作所、博士(工学)

～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

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



アジェンダ

HITACHI
Inspire the Next

1．OSSコミュニティ活動の事例

2．OpenSSFのご紹介

１．OSSコミュニティ活動の事例

事例１：　SELinuxとは

HITACHI
Inspire the Next

- SELinux (Security-Enhanced Linux)
  - NSA (National Security Agency)が開発、2001年OSS公開し話題に

- OSレベルでアクセス制御機能を強化
  - 「セキュアOS」技術
  - 不正アクセスの被害を最小限に封じ込める

- その後Linuxカーネル標準オプションになり、RHELやAndroid等にも標準搭載

SELinuxのコミュニティ活動をはじめたきっかけ

HITACHI
Inspire the Next

- 2000年代初頭入社。研究開発部門に配属。
  当時出たての技術として、
  「SELinux」の論文と「SAML」の論文を並べられ、
  「どっちがいい？」と言われて、
  もともとOSSに興味があったため、「SELinux」を選んだのがきっかけ。

- 技術評価を行い課題を洗い出し、「設定がとんでもなく難しい」ことに着目。

最初の活動
- 日本語情報源が全くなかったため、記事のネタを出版社に持ち込んだら、あっさり採用。
  ↓
- 研究し、設定ツール「SELinux Policy Editor」を開発、論文発表。
  ↓
- 事業部が関連する某省庁の研究開発プロジェクトも受注し、支援。

SELinuxコミュニティ活動の広がり

HITACHI
Inspire the Next

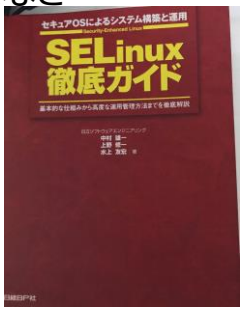
国内コミュニティ立ち上げ

「SELinuxユーザ会」立ち上げ、多数の仲間を獲得。

OSS開発活動

- SELinux Policy Editorを当時の所属としては、初めてOSS公開。
  商用distroにも採用。
- 組込み向けにSELinuxをチューニングし数々contribute。
- 開発者に会いに渡米。
- Ottawa Linux Symposium、Embedded Linux Conference, USENIX LISAなど
  様々な場所で成果を発表。

執筆活動



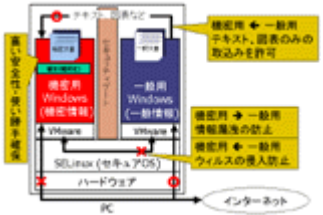
- 当時世界初のSELinux書籍「SELinux徹底ガイド」を日経BPから出版。
- 複数の出版社で連載・特集執筆、講師としても多数お呼ばれした。

まさに順風満帆

ビジネスの壁

- 最初は国プロなので、文句を言われない。
- その後しばらくは「元気な若手」として見守って頂けたが…
- **ビジネス化しないと研究予算つかないことをある時に気づく！**

- 色々なアイデアを考えて提案



二系統Windows

https://enterprise.watch.impress.co.jp/cda/software/2005/03/24/4898.html

情報家電向けSELinux

Android SELinux

https://xtech.nikkei.com/it/article/NEWS/20071114/287229/

https://xtech.nikkei.com/it/article/NEWS/20080530/305495/

その他色々ネタを出して動き回った

しかしSELinuxは当時の自社ビジネスとして厳しかった…

- 技術開発しても商用distro・機器ベンダが自力で使うだけで会社にお金落ちない
  「個人」に声はかかるが(執筆とか講師とか)、組織が食える規模の仕事は取れず。

→ 活動原資がつかなくなり、断念し、しばらく別の分野でビジネス含めて修行。

SELinuxの事例からの学び

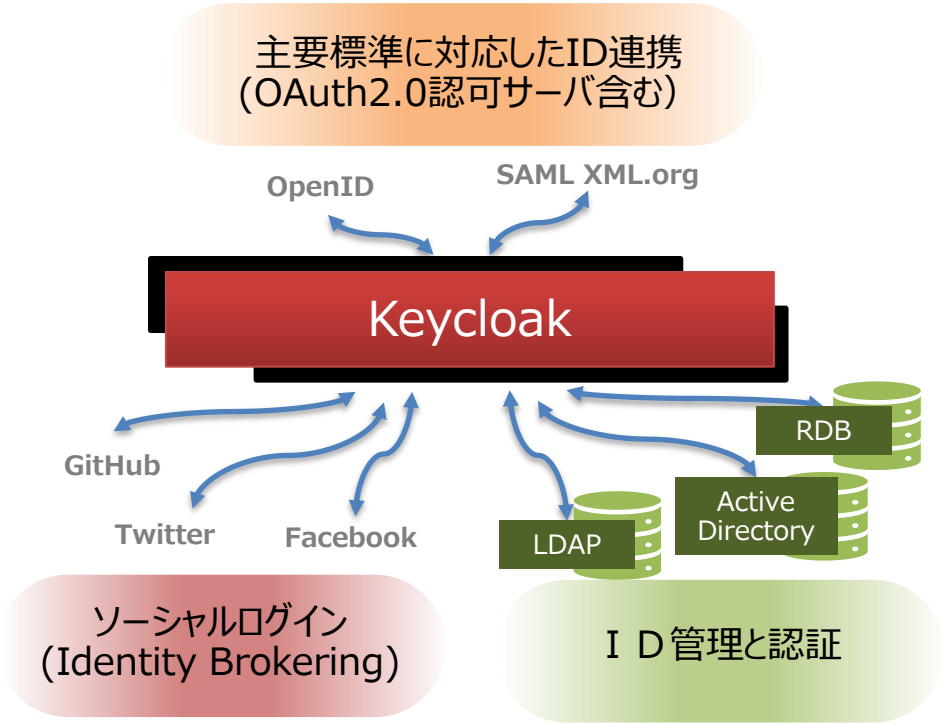
HITACHI
Inspire the Next

- 業務でコミュニティ活動をやる場合の注意点
  - コミュニティ活動だけなら、一定の成果を出すことはできる。
    多くのコミュニティでは人手不足であり、貢献は歓迎されるため。
  - 社外に仲間ができて盛り上がると、うまく行っているように錯覚してしまう。
    時折冷静に振り返る必要。
  - 所属組織のビジネスと結び付け、自身のミッションとして評価される形でないと長続きしない

- 何が残ったか？　：　技術とOSS経験は残った。
  - ContributeしたパッチはAndroid SELinux適用の礎に
  - 学術論文も残り、学位取得できた
  - コミュニティ活動の回し方は分かった

事例２：Keycloakとは？

Keycloakは、Red Hat社を中心に開発されるID管理OSS。
シングルサインオンやOAuth2.0に対応したAPIの認可認証サーバーの機能を提供。
2023年4月にCNCFのIncubating Projectとして承認



HITACHI
Inspire the Next

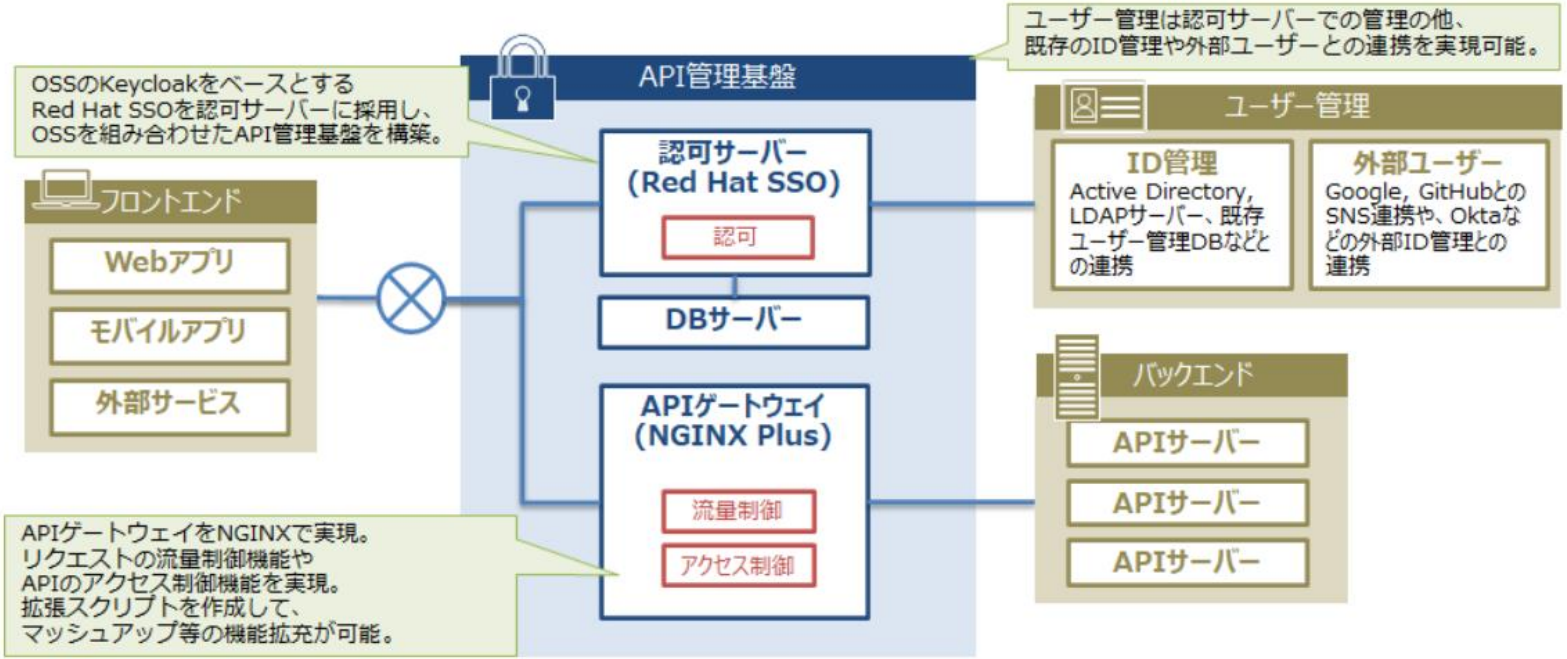
「Keycloakありき」ではじめたわけではないところがポイント

- 自社のソリューションに必要
  新規ビジネスを検討したところ、Keycloakがコアとなる部材として必要だった

- OSSコントリビューションも、「必要だから行う」
  - バグ、非機能改善
  - 将来、お客様が必要になる機能を先んじて入れ込み

Keycloakの自社ビジネスでの活用例：ベーシックAPI管理モデル

課題：　APIをセキュアに公開したい、しかしセキュリティには高度な専門知識が必要
ソリューション：　KeycloakやOSS・クラウドサービスを活用してAPIセキュリティを確保



出典：https://www.hitachi.co.jp/products/it/oss/solution/basic_api_mgmt_model/index.html

コミュニティ活動

HITACHI
Inspire the Next

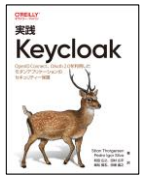
ビジネスの中でコミュニティ活動を実施してきました（参考：日立のKeycloakへの取組み）

執筆講演: Keycloakや技術者の知見を知って頂く

■Keycloakや認証認可分野についてのWeb連載記事を掲載
- ThinkIT: Keycloakで実現するAPIセキュリティ
  https://thinkit.co.jp/series/9721
- ThinkIT: KeycloakのFAPI1.0対応で実現する高度なAPIセキュリティ
  https://thinkit.co.jp/article/18829

■国内外の著名なカンファレンスでの講演
- APIdays Paris(2022/12)
  “Securing APIs in Open Banking –FAPI implementation to OSS”
- Open Identity Summit 2022(2022/07)
  “Flexible Method for Supporting OAuth 2.0 Based Security Profiles in Keycloak”
- APIsecure 2022(2022/04)
  “Why Assertion-based Access Token is preferred to Handle-based one?”

■Keycloakの書籍執筆
- 「認証と認可 Keycloak入門」(2022/1)
- 「実践Keycloak」(2022/10)



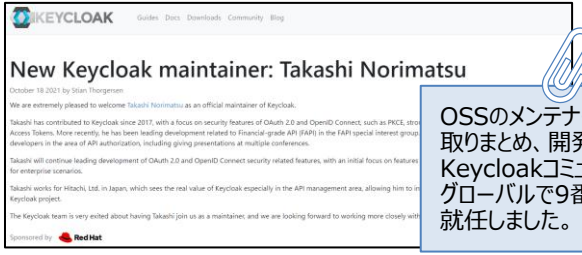
開発貢献： 必要な機能を入れ込む

■最新のAPIセキュリティ仕様への準拠をリード
- RFC7636(PKCE)対応 (v3.1,v6.0)、Holder of Key対応 (v4.0)
  強固な署名アルゴリズム対応 (v4.5)、トークン暗号化(v7.0) 、OAuth 2.0 Device Authorization Grant対応(v13.0)、 CIBA対応(v13.0)、FAPI対応(v14.0)、FAPI-CIBA対応(v15.0)

■ その他主要機能を開発
- パスワードレス認証(WebAuthn)対応(v8.0)
- クライアント設定のためのフレームワーク(Client Policies) (v13.0)

■日本市場からのニーズに対してパッチ投稿

■Keycloakメンテナーに日立社員が就任
https://www.hitachi.co.jp/products/it/oss/news/20211026.html



OSSのメンテナーは、コミュニティの開発プロジェクトを取りまとめ、開発方針などをリードする責任者です。Keycloakコミュニティには、日立社員の乗松さんがグローバルで9番目、日本では初のメンテナーとして就任しました。

1.まとめ：　持続的なコミュニティ活動のために

HITACHI
Inspire the Next

コミュニティ活動と自社・顧客ビジネスの循環を回すのが理想

HITACHI
Inspire the Next

2．OpenSSFのご紹介

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コミュニティ運営の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

OpenChainには、サプライチェーンセキュリティの取り組みが関連すると思われる

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。

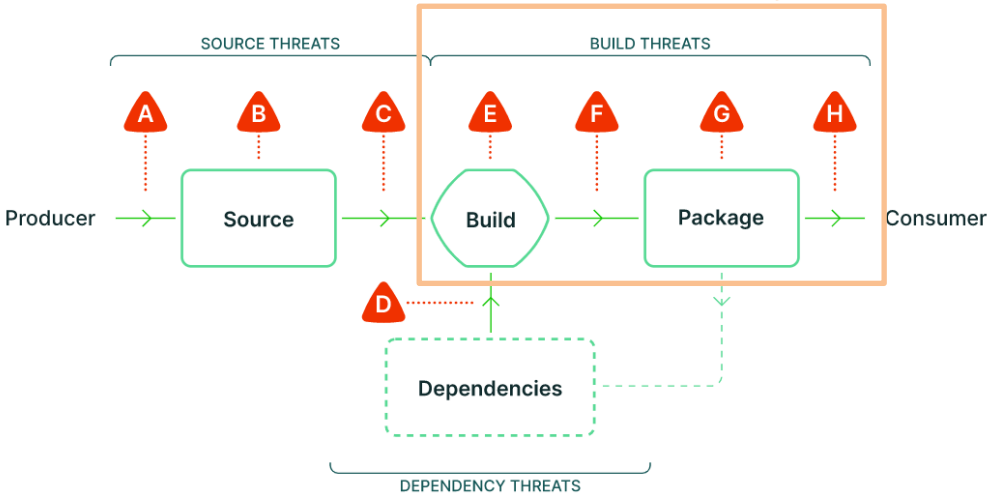
- **1～3のレベル**（v0.1では1～4までレベルが分かれていた。4はv1.0では未実装）
  L1：パッケージがどのように構築されたかを示すprovenance(来歴)　→間違い防止
  L2：ホストされたビルドプラットフォームによって生成された署名付きの来歴　→ビルド後の改ざん防止
  L3：L2に加え、強化されたビルドプラットフォーム　→ビルド中の改ざん防止
  　・同じプロジェクト内であっても実行が互いに影響を与えない
  　・来歴の署名に使用される秘密マテリアルがユーザー定義のビルドステップからのアクセス不可

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**

- <u>それぞれの脅威へのSLSAでの対策</u>
  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

S2C2F

HITACHI
Inspire the Next

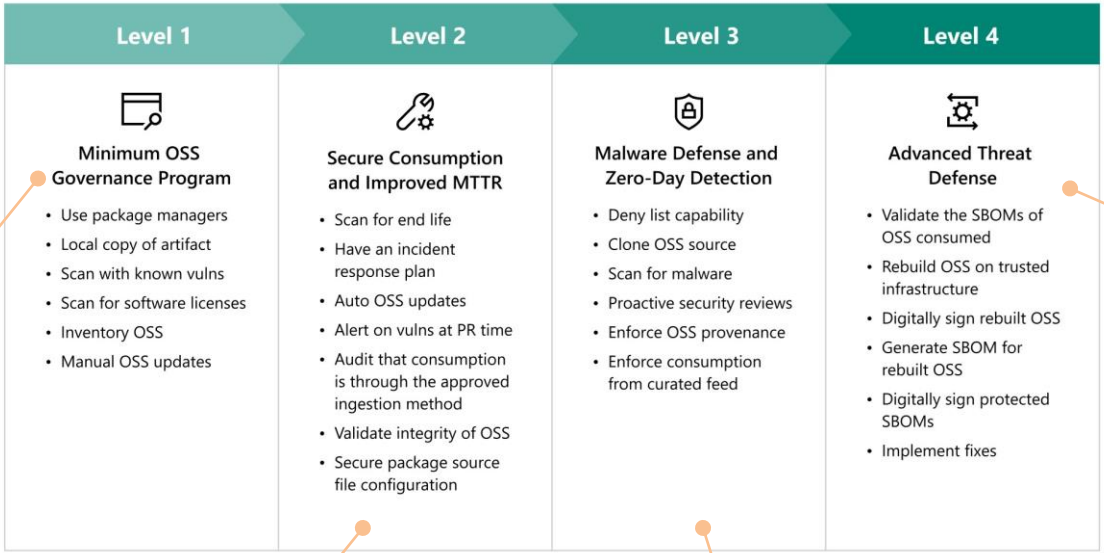
- **Secure Supply Chain Consumption Framework (S2C2F)とは**
  - ・OSSの依存関係を開発者のワークフローに安全に取り込む方法を概説および定義する
  - ・マイクロソフトによるOpen Source Software-Supply Chain Security (OSS-SSC) Frameworkが元
- ・OpenSSFのSupply Chain Integrity Working Group内に採用され、独自のSpecial Initiative Group(SIG)に編成された　→S2C2F SIGと呼ばれる

- 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

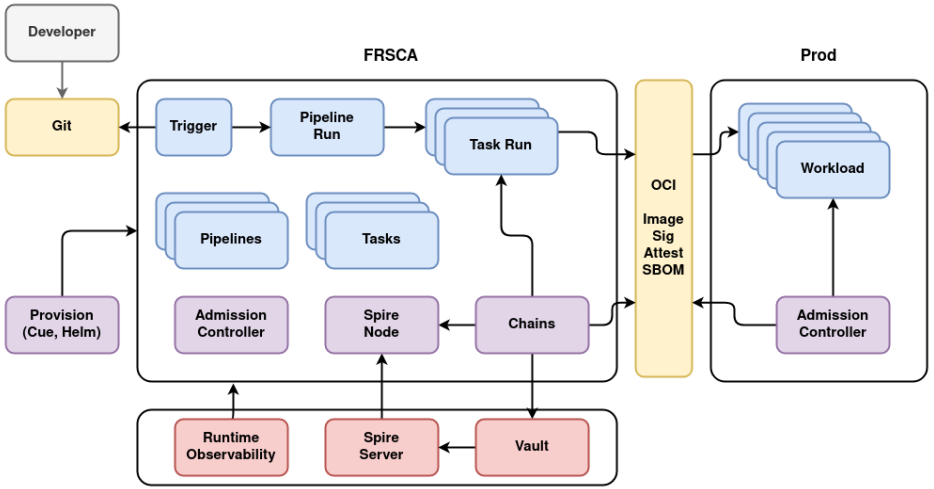
Sigstore https://www.sigstore.dev/ https://github.com/sigstore

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
- Kusari社はFRSCAを活用したビジネスを行っている模様
- 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/

2. 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

・Facebookは、Facebook,Inc.の登録商標です。
・AndroidはGoogle,LLCの登録商標です。
・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。
・Red Hat is registered trademarks of Red Hat, Inc. in the United States and other countries.
・OpenID is a trademark or registered trademark of OpenID Foundation in the United States and other countries.
・NGINXは、NGINX,Inc.の登録商標です。
・Twitterは、Twitter,Inc.の登録商標です。

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