コンテナセキュリティスキャン

コンテナスキャンには, 大きく分けて以下の2つがある

- **静的スキャン** : コンテナイメージをスキャンする
- **動的スキャン** : 動作中のコンテナへの攻撃を検知する

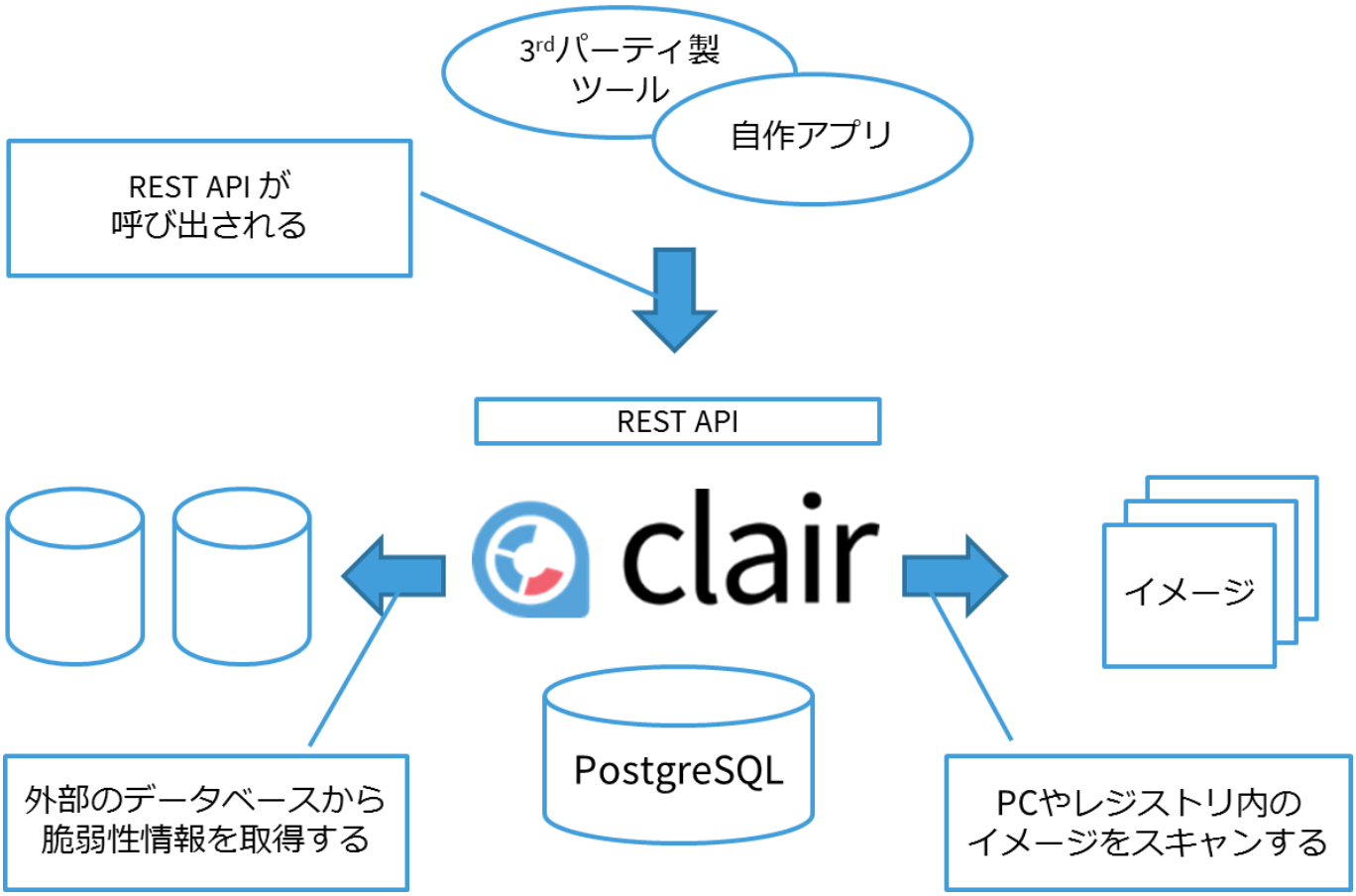
k8s完全ガイド P11で紹介されているスキャンサービスは, 静的スキャン

コンテナの静的スキャン

- コンテナホストに対する脆弱性スキャン
    - コンテナホストで実行されるカーネル／コンテナを実行するデーモンにバグがあると、コンテナがセキュアでも外部から攻撃を受ける場合がある
- コンテナイメージに対する脆弱性スキャン

コンテナホスト／コンテナの脆弱性スキャンでは、マシン内で使用しているアプリケーション／ライブラリを始めとした実行形式に脆弱性がないかを確かめる

静的スキャンサービスの例1 : Clair(クレア)



概要

- 既知の脆弱性情報からイメージをスキャンした結果を結びつけてイメージにどのような脆弱性があるのかを発見する仕組み

- パッケージ管理されていないソフトウェアの脆弱性を検出しない(自力でtarファイルを展開してツールをインストールした場合、そのツールはイメージに含まれていてもスキャンされず、脆弱性も検出されない)
- つまり検出するのは、イメージの構成要素のうち、パッケージ管理システムで管理されたパッケージに存在する、既知の脆弱性のみ
- 実行には, PostgreSQLが必要

静的スキャンサービスの例2: trivy

概要

- 作成者はもともと日本人
- OSのパッケージの脆弱性を検知
- DBが不要のためインストールが容易なのでお勧めされている
- **アプリケーションの依存ライブラリの脆弱性を検知**
  - pip（Python）などのアプリケーションの依存性解決ツールでinstallされるライブラリの脆弱性をスキャン

他脆弱性スキャンサービスとの比較

Scanner	OS Packages	Application Dependencies	Easy to use	Accuracy	Suitable for CI
Trivy	✅	✅ (7 languages)	⭐ ⭐ ⭐	⭐ ⭐ ⭐	⭐ ⭐ ⭐
Clair	✅	×	⭐	⭐ ⭐	⭐ ⭐
Anchore Engine	✅	✅ (4 languages)	⭐ ⭐	⭐ ⭐	⭐ ⭐ ⭐
Quay	✅	×	⭐ ⭐ ⭐	⭐ ⭐	×
Docker Hub	✅	×	⭐ ⭐ ⭐	⭐	×
GCR	✅	×	⭐ ⭐ ⭐	⭐ ⭐	×

参考文献

https://thinkit.co.jp/article/17525 https://www.ogis-ri.co.jp/otc/hiroba/technical/clair/part2.html
https://qiita.com/MahoTakara/items/47d9c4ecd67f82977ca8
https://qiita.com/knqyf263/items/dc179f9223fc31b5a51c