SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

クラウドアプリケーションの完全性を保証するKubernetesマニフェストの署名検証手法

Kubernetes manifest signing and verification method for cloud application integrity

北原 啓州 * 渡邊 裕治 *
Hirokuni Kitahara Yuji Watanabe

キーワード クラウドアプリケーション, Kubernetes マニフェスト, 完全性

あらまし

システムやアプリケーションを機能ごとに細分化するマイクロサービスが浸透するにつれ，クラウドでコンテナを稼働させることでマイクロサービスを実現する方式が普及してきている．特に，クラウドの管理システムとして，オープンソースソフトウェアの Kubernetes が広く利用されており，本稿では Kubernetes のアプリケーションの完全性を保証するための手法について提案および議論する．一般的な Kubernetes のアプリケーションは，1) コンテナイメージ，2)Kubernetes リソース，という 2 つの要素に大別することができる．コンテナイメージはアプリケーションで実行される処理とその実行環境，Kubernetes リソースはアプリケーションを実行するための設定，を定義するためにそれぞれ用いられ，Kubernetes のアプリケーションの完全性のためには，両者の完全性が保たれる必要がある．1) のコンテナイメージについては，コンテナイメージに電子署名を付与しコンテナが起動する前に署名検証を行う手法や，起動中のコンテナを監視して変更を検知する手法などが完全性を保証するための手法として知られている．2) の Kubernetes リソースについては，アプリケーション開発者が定義するものとクラウド上にデプロイされたリソースには様々な要因により差異が存在するため，アプリケーションの振る舞いに詳しい者が，リソースの一部分の設定のみを指定し，その部分についてのみ完全性を検証するという方法が採られてきた．しかし，一般に，クラウド上では様々なアプリケーションが同時に動作しており，すべてのアプリケーションの振る舞いを把握することは難しく，アプリケーション設定の完全性を検証する方法として現実的ではない．本稿では，個別のアプリケーションの振る舞いについて事前知識が一切不要な Kubernetes リソースの完全性の検証手法として，クラウド上でリソースが変更されていても署名検証が可能な署名手法および検証手法を提案し，さらに実際のクラウド環境における実用性についての検証結果を報告する．

* IBM 東京基礎研究所, 東京都中央区日本橋箱崎町 19-21, IBM Research - Tokyo, 19-21 Nihonbashi Hakozakicho, Chuo City, Tokyo