OpenStackにおけるインスタンス認証

ヤフー株式会社 藤代大介

自己紹介

藤代 大介

ヤフー株式会社 COOバーティカル統括本部

2014年12月 中途入社

2014年12月 ~ 2017年9月

ウェブ検索のバックエンドエンジニアとして従事

2017年10月 ~ 2021年3月

プライベートクラウドの開発・運用に従事

2021年4月 ~

COOバーティカル統括本部へ

アジェンダ

1. Yahoo! JAPANのプライベートクラウドの紹介
2. OpenStackのインスタンス認証について

アジェンダ

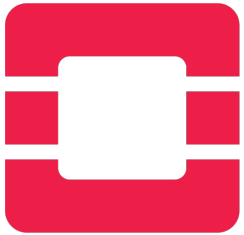
1. Yahoo! JAPANのプライベートクラウドの紹介
2. OpenStackのインスタンス認証の構成

OpenStack

OSSのクラウド基盤

マイクロサービス化された複数のコンポーネントで構成される

Yahoo! JAPANではOpenStackでサービス開発者にインスタンスを提供



openstack®

Yahoo! JAPANのOpenStack

稼働時期: 2013年~

OpenStack version: Grizzly~Rocky

クラスタ数: 200+

運用人数: 20+ (全員が開発との兼任)

HV数: 21,000+

VM数: 170,000+

ラック数: 1,000+

クラウド利用目的の変化

2013年~

既存のベアメタルをインスタンスへ置き換えたい

2014年~

クラウドネイティブなアーキテクチャを採用したい

2015年~

システム毎の要件にマッチするようなOpenStackクラスタがほしい

2016年~

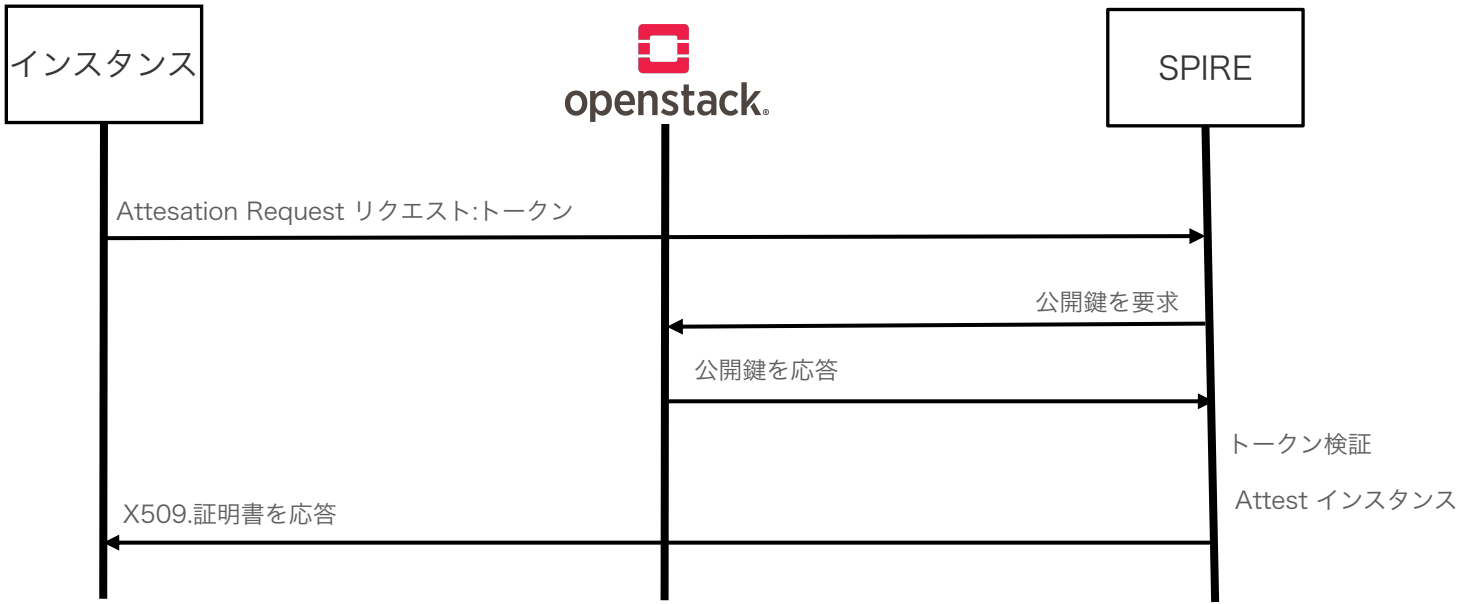
プラットフォームの基盤として使いたい

アジェンダ

1. Yahoo! JAPANのプライベートクラウドの紹介
2. OpenStackのインスタンス認証について

SPIREの導入にむけて

Node Attestationには自身の身元を証明するためのトークンが必要



身元を証明するためのトークン

Yahoo! JAPANのOpenStackは、インスタンスの身元を証明するために利用できるデータがない。

OpenStack IIDを実装して、身元を証明するデータとして利用するようにした。

OpenStack IIDとは

OpenStack Instance Identity Documents（IID） はOpenStackによって作られるインスタンスが自身の身元を証明するためのトークンであり、IIDは検証可能なインスタンスメタデータであり、インスタンスのみが参照可能な情報として提供する。

OpenStack IIDはJSON Web Token（JWT）の形式である。

IID APIとは

インスタンスの起動の際にOpenStack IIDの発行処理を受けるAPIである。

IIDの発行があった場合は、インスタンスごとに秘密鍵を生成して、OpenStackのAPIから必要な情報を取得して、IID（JWT形式）を生成後、公開鍵はデータベース（DB）で保存して、署名鍵は破棄して、IIDを応答する。

アーキテクチャ概要