クラウドのセキュリティー・ポリシー自動診断「Vulnerability Advisor」「Policy Manager」

DevOpsにおけるセキュリティーとコンプライアンス遵守を簡単確実に

多様なビジネスがクラウド上のサービスとして提供されるようになってきた近年では、クラウド上でのサービスのセキュリティーとコンプライアンス遵守がますます重要な課題となっています。東京基礎研究所はワトソン研究所と共同で「IBM Containers」のセキュリティーおよびコンプライアンス機能である「Vulnerability Advisor」を開発しました。

Vulnerability Advisorと、そのポリシー管理機能「Policy Manager」の自動診断機能により、クラウド・サービスのセキュリティー・コンプライアンス遵守に要する作業を大幅に削減するとともに、自社のクラウド・サービスを他社と明確に差別化することができます。

1.「IBM Containers」のセキュリティー機能

2015年6月22日IBMは、「DockerCon」というイベントで、「Docker」をベースとしたコンテナー・サービス「IBM Containers」を発表しました[1]。Dockerは素早く簡単なコンテナー技術として最近注目を集めており、IBM Containersは、「IBM Bluemix」のサービスの一部として提供されています。

まず、Dockerについて、簡単に説明しておきましょう。Dockerはコンテナー型の仮想化技術で、コンテナーと呼ばれる区画ごとに異なる環境を動かすことができ、サーバー構成をイメージとして保管することができます。ユーザーはそのイメージから作成したコンテナーを、自分のノートパソコンやクラウド環境などさまざまなコンテナー実行環境で起動させることができます。実際のコンテナーが起動している場所を意識することなく、さまざまなサーバーをコンテナーで実現することができるため、近年ますます複雑なサーバー構成での開発を求められるようになったアプリケーション開発者にとっては、開発を加速させるための強力なツールとなっています[2]。

イメージを手元からプッシュしてクラウド上で実行できる機能は、アプリケーション開発者にとって非常に有用です。その一方で、セキュリティー脆弱性が含まれるイメージがプッシュされた場合には、それに基づいて起動されたコンテナーにも脆弱性が含まれることになり、セキュリティー上の非常に大きな脅威になってしまいます。

そこで、IBM Containersは、安全なコンテナー実行環境を実現する機能として、「Vulnerability Advisor」を他社に先駆けて発表しました。Vulnerability Advisorは、コンテナーやイメージのセキュリティー脆弱性やセキュリティー・ポリシー違反を警告し、ポリシーに反するイメージに基づくコンテナーを起動させないように制御します。これにより、アプリケーション開発者がアプリケーション開発時に発生するセキュリティー対応に要する労力を大幅に低減できます[3][4]。

Vulnerability Advisorを利用するために、ユーザーのイメージに特別な機能を組み込んだり、エージェントを起動させたりする必要はありません。IBM Containers

で起動するすべてのコンテナーのDevOpsライフサイクルにVulnerability Advisorによるセキュリティー監視機能が自動的に統合されます。

Vulnerability Advisorによるイメージの状態監視により、以下のようなイメージの自動診断と制御が可能となります。

- ユーザーのイメージ内にインストールされているパッケージ一覧を自動作成し、既知の脆弱性を含むバージョンのパッケージがないかをチェックする
- 既知の脆弱性を含むパッケージのリストと、脆弱性の修正方法を参照できるページへのリンクを提供する
- ユーザーのセキュリティー・ポリシーに基づいて、イメージのセキュリティー脆弱性を評価する
- コンテナーを起動する際は、元となるイメージに対する評価結果に基づいてその可否を判断し、問題がある場合は起動をブロックする

このように、ユーザーが意識しなくとも、セキュリティー・ポリシーに違反するイメージに基づくコンテナーは起動されない仕組みが組み込まれています。これは安全なクラウドのDevOps環境を実現する非常に重要な機能です。

このVulnerability Advisorの特筆すべき重要な特長は以下の通りです[5]。

- IBM Bluemixクラウド・プラットフォームに組み込まれているため、特別なセットアップが不要
- イメージやコンテナーでのエージェント起動や特別なアクセス権の設定などが不要
- プラットフォーム・レベルで、イメージからの情報収集を制御するため、不正に情報が操作され、セキュリティー脆弱性のチェックに影響を及ぼすことがない
- イメージをプッシュし、コンテナーを起動するプロセスの一部として、イメージの脆弱性検証がほぼリアルタイムに行われる
- 一目でわかるシンプルな画面で、脆弱性検証の結果が表示される

特にクラウドをビジネス・プラットフォームとして利用する場合には、セキュリティー・コンプライアンス遵守が必須となります。IBM Containersで提供されているユーザー視点でのセキュリティー・ポリシー自動診断機能は、他のクラウドと一線を画す最新テクノロジーです。この後の章では、IBM Bluemix上でVulnerability Advisorと、そのポリシー管理機能「Policy Manager」によって、イメージとコンテナーのセキュリティーがどのように自動診断され、制御されるのかをご紹介します。

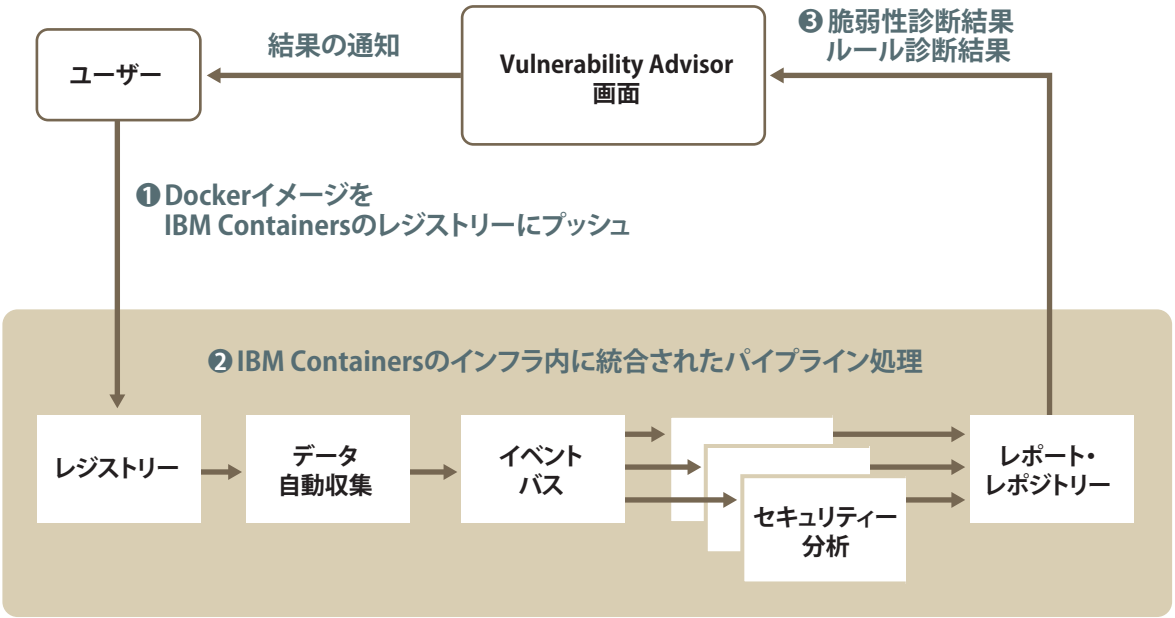

図1. Vulnerability Advisorの処理の流れ

2. Vulnerability Advisor イメージのセキュリティー自動診断機能

Vulnerability AdvisorによるセキュリティーIBM Containersの基盤に組み込まれており、ユーザーが特別な事前設定をせずに利用することが可能です。

図1にVulnerability Advisorがどのように動作するのかを紹介します。

①ユーザーが独自のイメージを作成し、IBM Bluemix上のレジストリーにプッシュします。

②セキュリティー分析に必要な情報はレジストリー内のイメージから自動抽出され、イベントバスを通じて複数のセキュリティー分析モジュールに受け渡され並行処理されます。

③結果はレポート・レポジトリーに格納され、Vulnerability AdvisorをIBM Bluemixコンソール上にフィードバックされます。

この一連の処理はパイプライン化されており、イメージをプッシュした直後には、IBM Bluemixのカタログ上に新たにプッシュしたイメージが追加されるのを確認できます。また、イメージに対するセキュリティー・ポリシー自動診断結果は、カタログ上のイメージのアイコンの上にマウスオーバーするとポップアップ表示されます(**図2**)。そのポップアップには、診断結果に応じて、

- ●Safe to Deploy(安全にコンテナーを起動可能)
- ●Deployment Blocked(コンテナー起動は不可)
- ●Deploy with Caution(コンテナー起動可能だが警告付)

の3種類のメッセージが表示されます。Vulnerability Advisorの自動診断結果は、セキュリティー脆弱性や設定違反の状況に応じて事前に決められたポリシーに基づき判定されます。このポリシーは後述のPolicy Managerで定義・変更可能です。

イメージごとの詳細な検出結果を確認することもできます。「Vulnerable Packages(脆弱性のあるパッケージ)」タブ(**図3**)には、

- ●スキャンしたパッケージ数
- ●脆弱性の発見されたパッケージ数
- ●対象のセキュリティー脆弱性一覧

が表示されます。これにより、イメージに含まれる脆弱性をイメージを実行する前に検出でき、イメージの修正を行うことができます。

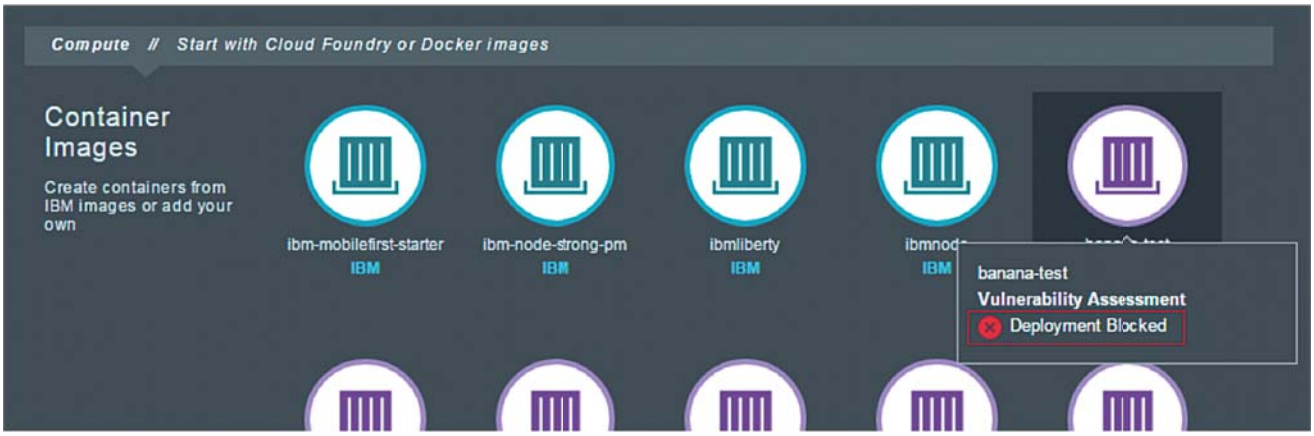

図2. IBM Bluemix上のイメージカタログと自動診断結果の表示例

また、「Policy Violations（ポリシー違反）」タブ（**図4**）には、

- セキュリティー・チェック項目総数
- セキュリティー違反項目数
- 検出されたセキュリティー違反の一覧

が表示されます（セキュリティー・チェック項目は今後拡張可能となる予定です）。

このように、イメージをプッシュすると直ちにセキュリティー・ポリシーに基づく診断が行われるのが大きな特徴です。この診断プロセスによりユーザーのコンテナー利用におけるパフォーマンスが低下することのないように設計されており、コンプライアンス要件として定義されるセキュリティー・ポリシーを遵守するためにDevOpsにおける開発効率が悪化することはありません。IBM ContainersではDevOps開発とセキュリティー・コンプライアンス遵守の両立を実現します。

ユーザーが遵守すべきセキュリティー・ポリシーは、ユーザーの所属組織や開発対象および環境などによって異なることは当然考えられることです。Vulnerability Advisorでは、セキュリティー・ポリシーをカスタマイズするPolicy Managerを提供しています。次章では、Policy Managerの機能について詳しくご紹介します。

3. Policy Manager ポリシーに基づくコンテナーのライフサイクル制御

Vulnerability Advisorによってレジストリー上のイメージにセキュリティー上の問題が発見されたとき、そのイメージからコンテナーを作ることはシステム管理の観点でリスクとなります。Vulnerability Advisorの一機能として提供されるPolicy Managerは、ポリシーに基づいてコンテナーのライフサイクルを制御できるようにします（**図5**）。Policy Managerはシステム管理者に対して、組織に属するコンテナーに対するポリシーを一元的に定義できる仕組みを提供します（**図5-❶**）。ユーザーがあるイメージを元にコンテナーを起動しようとすると（**図5-❷**）、Policy Managerは、Vulnerability Advisorでチェックされたそのイメージに含まれる脆弱性やセキュリティー・ポリシー違反の結果を受けて（**図5-❸**）、問題がある場合にはユーザーに対し警告を出したり、コンテナーの起動をブロックするか許可するかを判定します（**図5-❹**）。

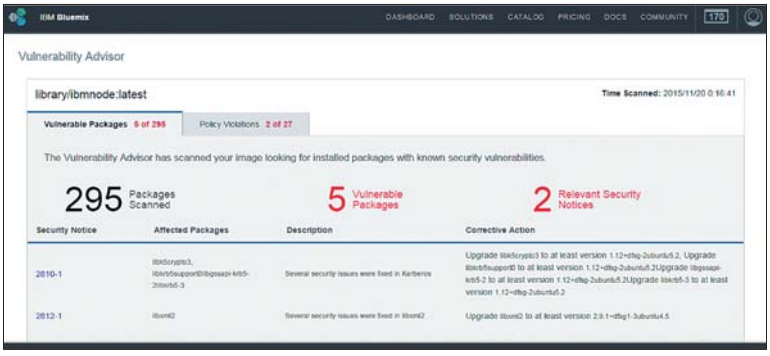

図3. Vulnerable Packages（脆弱性のあるパッケージ）タブ

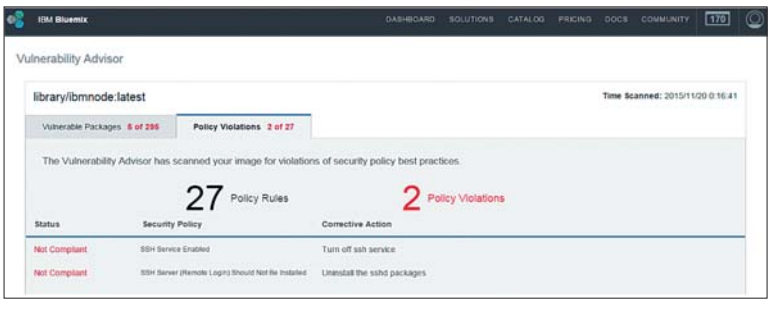

図4. Policy Violations（ポリシー違反）タブ

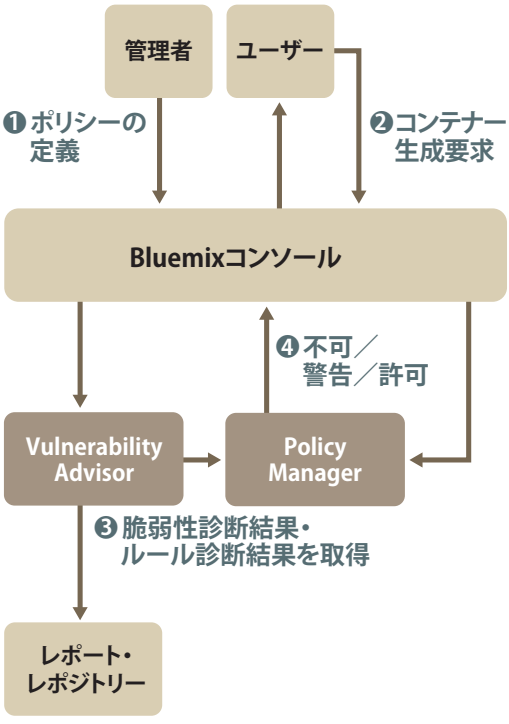

図5. Policy Managerによるコンテナーのライフサイクル制御の流れ

Policy Managerの設定画面（**図6**）は、イメージが脆弱性を持っていた場合のアクションを設定する部分（**図6左側**）と、その設定結果からどのイメージがコンテナー起動の際に警告、またはブロックを受けるのかを一覧表示する部分（**図6右側**）で構成されています。

アクション設定部分には、以下の3つの判定条件があらかじめ設定されています。

- ●脆弱性を持つパッケージがインストールされている
- ●リモート・ログインが可能になっている
- ●リモート・ログインが可能、かつ第三者が容易に想像できるパスワードを使用している

そしてこれらの条件に当てはまるイメージに対して、コンテナー起動時に「警告を出す」、もしくは「ブロックする」というアクションを設定できます。将来的には新規条件が追加・変更できるようになります。

例えば、組織Aの管理者が、前述した3つの条件いずれかに当てはまるイメージがプッシュされた場合には、常にコンテナー起動をブロックすると設定したとします。組織Aの開発者が自分で作成したイメージをIBM Bluemix上のイメージのカタログページに登録してインスタンス化をしようとすると、コンテナー生成ページ（**図7**）でのVulnerability Assessment結果が「ブロック」になっており、コンテナーの生成ボタンが押せません。そこで開発者はPolicy Managerへのリンクをクリックし、Policy Managerの画面で自分が生成したイメージが組織の判定条件に違反していたためにコンテナー生成ができなかったということを理解します。そして自分が生成したイメージを安全な設定になるように変更します。

このように、Policy Managerを用いることで無意識に（もしくは悪意を持って）開発者が脆弱性をもったイメージを組織のレポジトリーにプッシュし、他の開発者が知らない間にそのイメージを使用してしまうという事態を防ぐことができます。

4. 終わりに

本稿では、クラウドのビジネス利用における最大の関心事の一つであるセキュリティーおよびコンプライアンス遵守に開発者が要する労力を、Vulnerability Advisorの自動診断機能によって大幅に削減できることを示しました。この自動診断機能を活用することで、クラウド・サービスの初期開発時のみならず、運用フェーズでも一定水準のセキュリティーおよびコンプライアンス遵守へ

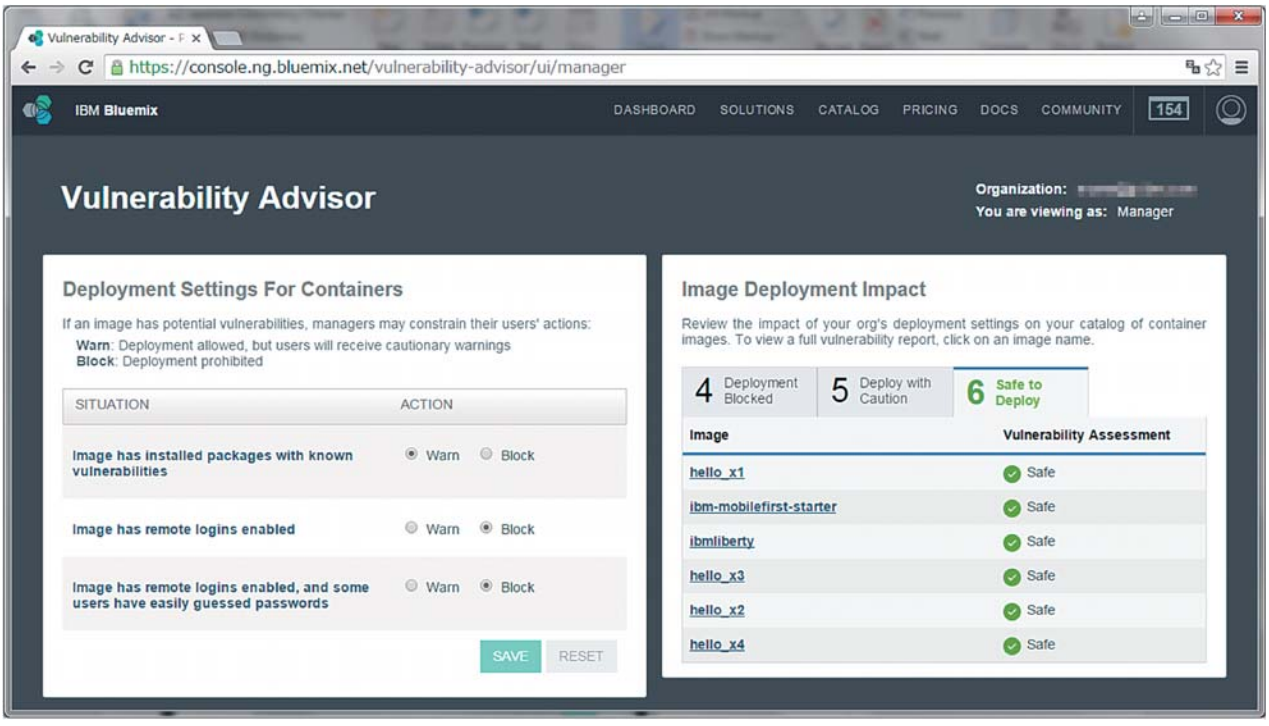

図6. Policy Manager設定画面

の対応を自動化することができます。

IBMが業界で初めて実現した本機能は、IBM Containerを利用するIBM Bluemixのユーザーであれば、誰でも体験することができます。ぜひIBMの最新テクノロジーでコンテナーのセキュリティーおよびコンプライアンス遵守を実現し、お客様のビジネスやサービスをより信頼性のあるものにするための一助としてご活用ください。

[参考文献]

[1] IBM Press Release:IBM Delivers Docker Based Container Services Developers, http://www-03.ibm.com/press/us/en/pressrelease/47165.wss

[2] Jason McGee:Containers: the Answer to Modern Development Demands, IBM Cloud, https://www.ibm.com/cloud/resourcecenter/content/85

[3] Tamar Eilam:IBM Containers - Achieve agility without sacrificing quality, Platform as a Service Magazine, http://www.paasmag.com/2015/07/09/ibm-containers-achieve-agility-without-sacrificing-quality/

[4] Tamar Eilam:IBM Containers - Achieve agility without sacrificing quality, IBM Bluemix Developers Community, https://developer.ibm.com/bluemix/2015/07/09/containers-for-agility-and-quality/

[5] Jim Doran:Is your Docker container secure? Ask Vulnerability Advisor!, IBM Bluemix Developers Community, https://developer.ibm.com/bluemix/2015/07/02/vulnerability-advisor/

日本アイ・ビー・エム株式会社
東京基礎研究所
クラウド＆セキュリティー担当

佐藤 史子
Fumiko Satoh

2001年日本IBM入社、以来同東京基礎研究所にて、Webサービスのセキュリティー、クラウドのプラットフォーム技術に関する研究開発に従事。現在はクラウドのセキュリティー・コンプライアンスやセキュリティー・インテリジェンスの研究を推進。博士(工学)。

日本アイ・ビー・エム株式会社
東京基礎研究所
クラウド＆セキュリティー

渡邊 裕治
Yuji Watanabe

2001年日本IBM入社、以来同東京基礎研究所にて、セキュリティー・プライバシー保護、コンプライアンスに関する研究開発に従事。近年はクラウド上のセキュリティーの設計開発プロジェクトを担当。東京工業大学大学院非常勤講師。博士(工学)。

日本アイ・ビー・エム株式会社
東京基礎研究所
クラウド＆セキュリティー

石田 愛
Ai Ishida

2006年日本IBM入社、以来同東京基礎研究所にて、Webサービスセキュリティー、ビジネスプロセス分析に関する研究開発に従事。現在はクラウド上のセキュリティーに関する研究開発のプロジェクトを担当。

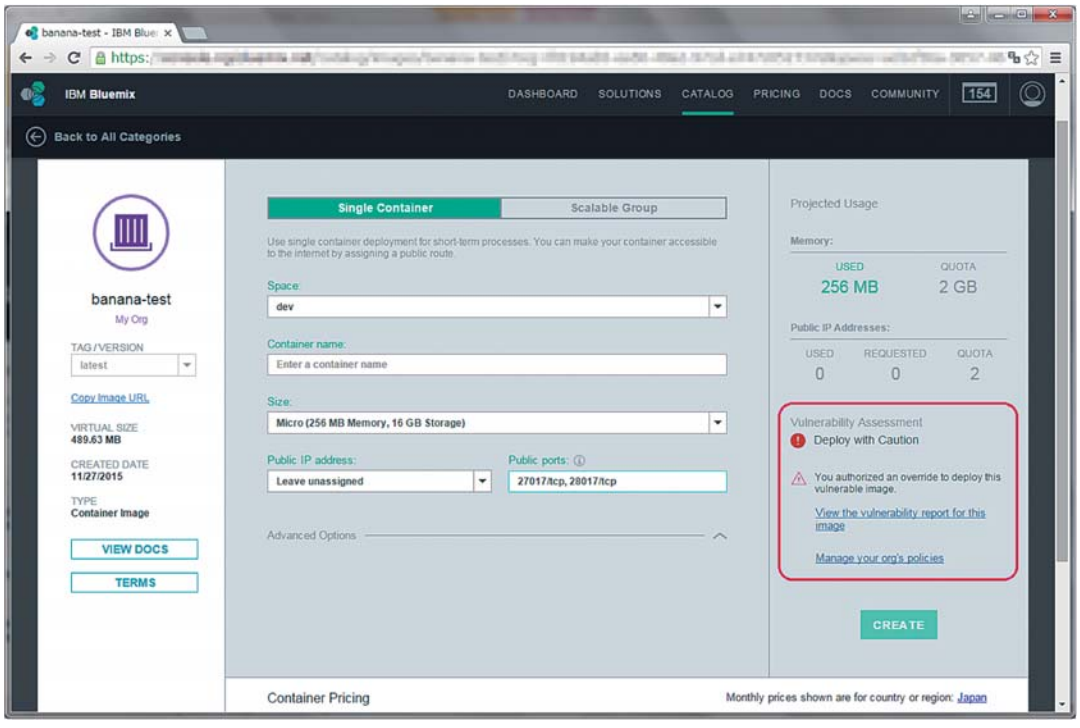

図7. コンテナー生成ページ