

SmartCloud DevaaS® 2.0セミナーレポート

DevSecOpsサイクルを実現する
開発環境クラウドDevaaS® 2.0

迅速なリリースとセキュリティの両立をめざして



デジタルトランスフォーメーション (DX) への取り組みが進むなか、DevOpsやアジャイル開発への関心が一層高まっています。しかし安全性を保ちつつ、高速なアプリケーション開発を実現するには、何が必要なのでしょう。2019年2月27日、NTTコムウェアは、「進化し続ける、開発環境クラウドDevaaS® 2.0 お客さまのDevSecOpsサイクルを実現」をタイトルに掲げ、「SmartCloud DevaaS® 2.0セミナー」を開催しました。ガートナージャパン シニアディレクターアナリストである桂島 航様をゲストスピーカーに迎えての基調講演の後、開発の高速性とセキュリティを両立する開発環境クラウド『DevaaS® 2.0』など、さまざまな角度からDevOpsの進化に向けた取り組みを紹介しました。

評価が高まる開発環境クラウド「DevaaS® 2.0」

DevaaS® 2.0は、開発に必要なハードウェア、ソフトウェア、管理の仕組みを提供するクラウドサービスです。その特長としては、DevOps推進のためのサポート体制、CI/CD (継続的インテグレーション/継続的デリバリー) に必要なすべてを含んだプラットフォームの2点が挙げられます。

ネットワーククラウド事業本部 担当部長 増田 良平は、DevaaS® 2.0のサポートについて「これからDevOpsが本格的に進むと期待される日本市場において特に重要です」と説明しました。NTTコムウェアではDevOpsサービスセンターを設立し、DevaaS® 2.0のサポートはもとより、オープンソースソフトウェアのツールなどの問い合わせにも対応して、DevOpsそのものの推進を強化しています。

CI/CDツールの充実度も、DevOpsには重要な観点です。DevaaS® 2.0では、30を超えるツールが利用できます。増田は「DevaaS® 2.0は、あたかもカセットを取り換えるように、豊富なラインアップから使いたいツールを利用できます。インストールやセットアップも必要ありません」とDevaaS® 2.0だけでDevOpsが実現できる利点を解説しました。

これらの取り組みにより、NTTコムウェア社内におけるDevaaS®の稼働率は右肩上がりで見られ、今ではほぼすべてのプロジェクトで利用しています。社外でも、**みずほ情報総研様のようにパートナー企業との協創にDevaaS® 2.0を活用している事例**もあります。

DevOpsプラットフォームとしての評価も高く、Red Hat主催のRed Hat Forumでは、クラウド・インフラストラクチャ部門で「Red Hat Innovation Awards APAC 2018」を、公益社団法人企業情報化協会 (IT協会) からは「IT特別賞 (DevOps賞)」を受賞しています。



増田 良平
NTTコムウェア株式会社
ネットワーククラウド事業本部
担当部長

SmartCloud DevaaS® 2.0セミナーレポート
DevSecOpsサイクルを実現する開発環境クラウドDevaaS® 2.0

NTTコムウェアでは、Webブラウザによるロケーションフリーの開発環境を提供する「クラウドIDE」や、開発環境からさまざまなクラウドへのリリースを可能にする「DataSkywalker®」、セキュリティ診断を組み込んだ「DevSecOps」など、さらなるDevOps推進に向けて積極的に取り組んでいます。

スピーディーなDevSecOpsサイクルを実現するために

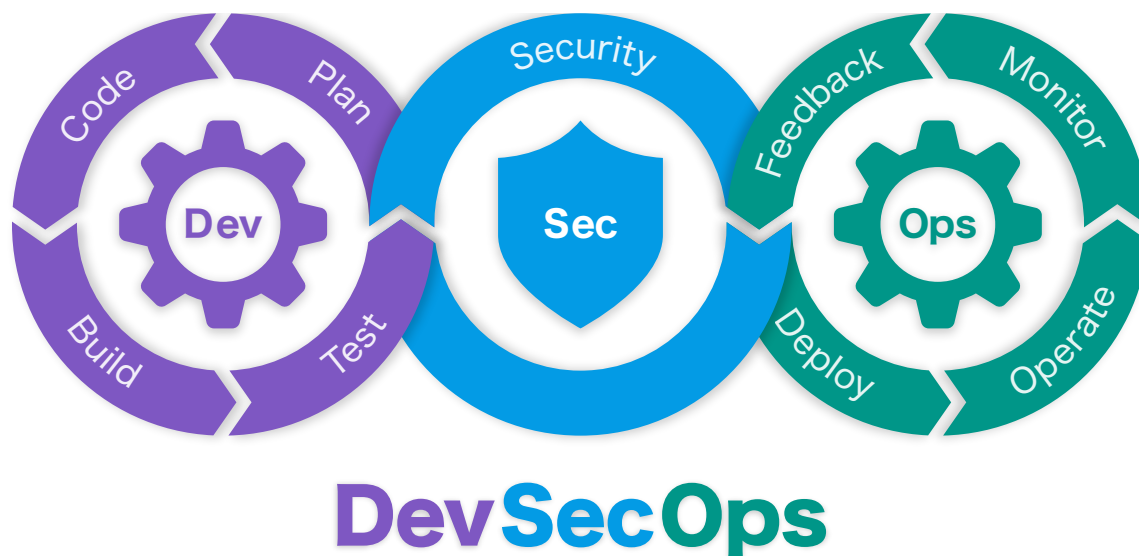
アプリケーションの開発では、セキュリティの担保は欠かせません。万が一脆弱性が潜んでいるとそこから情報漏えいなどのリスクが発生します。それを回避するために、開発チームの多くは、アプリケーションのリリースが近づくとセキュリティチームへ診断を依頼して、脆弱性の有無などのチェックを行います。しかし、その段階でセキュリティ上の大きな問題が発見された場合、リリースまでに対応が間に合わない可能性も生じます。

「セキュリティ診断とその後の対応に時間がかかっては、スピーディーにDevOpsサイクルを回すことが不可能です」と、ネットワーククラウド事業本部 アソシエイト エバンジェリスト (DevOps)の山田 恭子は、DevOpsとセキュリティの両立の難しさを解説します。

その両立をめざすのがDevSecOpsです。これは開発と運用を連携させるDevOpsにセキュリティを組み合わせた概念で、NTTコムウェアでは「開発チーム自身でセキュリティに責任を持って開発サイクルを回すこと」と定義しています。



山田 恭子
NTTコムウェア株式会社
ネットワーククラウド事業本部
アソシエイト エバンジェリスト
(DevOps)

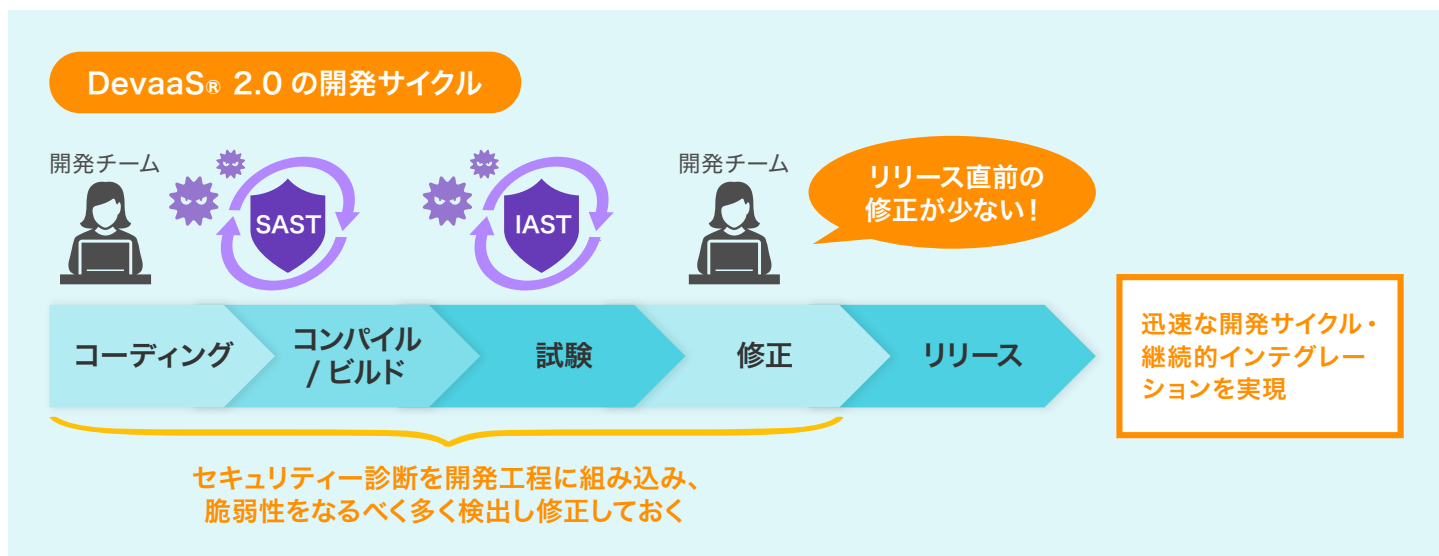
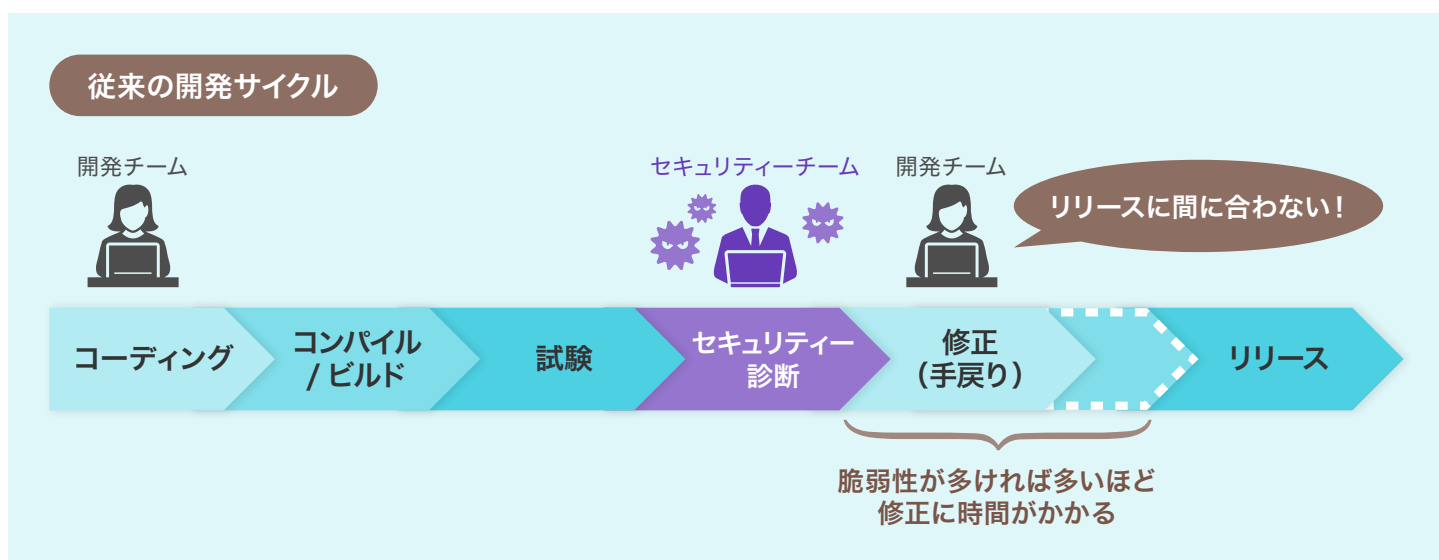


ではDevSecOpsを実現するには何が必要なのでしょう。山田は「リリース直前にセキュリティ専門家が診断するのではなく、開発中に、開発チーム自身でセキュリティ診断を行うこと」とポイントを説明した後、「開発工程終了前に多くの脆弱性を検知して修正できれば、リリース直前の修正を最小限に抑え、迅速にリリースできるようになります」とDevSecOpsの利点にも言及しました。

SmartCloud DevaaS® 2.0セミナーレポート
DevSecOpsサイクルを実現する開発環境クラウドDevaaS® 2.0

セキュリティ診断を開発工程に組み込むと、開発作業はどのように変わるのでしょうか。DevSecOpsに対応したDevaaS® 2.0では、SAST (Static Application Security Testing) と呼ばれる診断ツールの提供を予定しており、開発者がコードを保存した段階でソースコードの記述をチェックする静的診断が自動的に働きます。脆弱性につながる記述があれば該当する行を指摘するため、開発者はすぐに対応できます。

また、アプリケーションのリスクには「動かしてみても初めて判明する脆弱性」もあります。DevaaS® 2.0では、IAST (Interactive Application Security Testing) という新しいタイプの診断ツールも提供予定です。IASTを試験サーバーに組み込んでおけば、機能試験と同時にセキュリティの動的診断が働き、リスクの有無が開発者に通知されます。導入方法も容易で、DevaaS® 2.0のポータル画面からIASTを選択し、エージェントとして登録するだけです。



SmartCloud DevaaS® 2.0セミナーレポート
DevSecOpsサイクルを実現する開発環境クラウドDevaaS® 2.0

「開発者には、どの行にどういうリスクがあるか、そして具体的にソースをどのように修正すればよいか、セキュリティ診断の経験がない開発者にとっても見やすく、分かりやすい形で通知されます。診断に準備や手間がかからないため、開発者はアプリケーションの開発に専念して、スピーディーなDevSecOpsサイクルが実現できます」と解説しました。

最後に山田は、「DevaaS® 2.0がめざしているビジョンは、デジタルトランスフォーメーション時代に対応した「Intelligent DX Platform」です。その実現に向けて、DevaaS® 2.0は今後も機能拡充を進めていきます。」と締めくくりました。

コンテナを迅速に商用クラウドに移行するコンポーザブルインフラ

現在のビジネスのインフラを巡る状況について、日本ヒューレット・パッカートの伊藤 光裕氏は、「ビジネスではサービスのスピードとコスト削減が同時に迫られています。ITインフラに期待されているのは、この2つを両立させることです」と分析します。

そこで求められているのは、ITインフラの自動化です。人の手が介在しない完全な自動化が図られないと、高速、高品質、かつ低コストのITインフラを提供できません。しかし従来、サーバー機器の導入（設置作業、ハードウェアの設定など）と、ソフトウェアの導入（OSやミドルウェアの導入、サービスの設定など）には、部分的な手作業が必要でした。

ところがヒューレット・パッカートのコンポーザブルインフラである「HPE Synergy」は、それらの完全自動化を達成しています。伊藤氏は「コンポーザブルインフラで重要になるのはAPIです」と述べ、「APIが窓口となることで、指令を受け取ったシステムが適切に実行して、自動化を実現します」と説明しました。

例えばDevaaS® 2.0で開発されたコンテナを動かしているHPE Synergyに展開すれば、そのまま商用環境クラウドへ展開できます。つまり、コンテナを利用したDevOpsサイクルの完全な自動化が可能となります。

伊藤氏は最後に「ITインフラの提供の完全な自動化の実現には、HPE Synergyが最適です。DevaaS® 2.0で開発したアプリケーションの商用サービスへの展開などにぜひご利用ください」とまとめました。



伊藤 光裕氏
日本ヒューレット・パッカート株式会社
ハイブリッドIT事業統括
クラウドプラットフォーム統括本部
技術本部
ビジネスソリューション部
シニアITスペシャリスト

SmartCloud DevaaS® 2.0セミナーレポート
DevSecOpsサイクルを実現する開発環境クラウドDevaaS® 2.0

開発者自身がセキュリティ・テストを実施するために

DevOpsにセキュリティを実装したDevSecOpsの導入には、乗り越えなくてはならないさまざまな課題があります。DevOpsを達成している企業では、1日に数十回という数のデプロイを実現しています。その速度を落とすことなく、迅速なセキュリティ診断が可能になれば、DevSecOpsは実現できません。

日本シノプシスの吉井 雅人氏は、従来のセキュリティ診断に時間がかかる理由として「開発者とセキュリティ担当者の考え方が大きく異なる点」を挙げました。「従来型のセキュリティ診断ツールでも、CI/CDツールに乗せて自動化することは可能でした。しかし、レビューやフィードバックなどにかかる時間が考慮されておらず、リリースまでに時間がかかってしまいます。それらのフローの自動化ができないので、DevSecOpsの実現は困難でした」と吉井氏は説明します。

「DevSecOpsを取り入れるには、そのような環境を変える必要がある」と口にした吉井氏は、「私たちは、開発者が日々の開発過程の真っ只中でもセキュリティを実装できるようなツールを提供しています」と述べたうえで、3種類の診断方法を解説しました。

第1の方法は静的診断です。これは、ソースコードを分析して診断するもので、「DevSecOpsとの相性はよい」と吉井氏は説明します。

第2の方法は、ソフトウェアコンポジション解析です。Webアプリケーションには数多くのオープンソースソフトウェア (OSS) が利用されていますが、実際にどれだけのOSSが使用されているかを正確に洗い出し、「バージョンごとの脆弱性」はもちろん、「OSSのコミュニティが縮小傾向に向かっていないのか」「ソース開示が必要となるOSSを組み合わせた使い方をしていないか」といったリスクも検出します。

第3の方法が動的解析です。静的解析とソフトウェアコンポジション解析はソースコードなどを見て診断を実施しますが、アプリケーションには実際に動かしてみないと発見できない脆弱性も存在します。それを検知するのが動的診断です。

動的診断には従来DAST (Dynamic Application Security Testing) という種類のツールが一般的でした。これはセキュリティの専門家用のツールであり、開発者が診断結果を見ても対応するのは難しく、そもそもクリティカルではない処理が誤検知されることも多く、開発者にとって使いやすいツールとはいえません。またCI/CDツールとの連携ができないため、DevOpsサイクルに組み込むこともできません。

しかし、日本シノプシスのSeeker IASTは、開発者にも分かりやすい診断結果を示しながら、CI/CDツールとの連携もでき、DevSecOpsを実現しやすい動的診断ツールといえます。



吉井 雅人氏
日本シノプ시스合同会社
ソフトウェア インテグリティ グループ
シニア・セールス・エンジニア

SmartCloud DevaaS® 2.0セミナーレポート
DevSecOpsサイクルを実現する開発環境クラウドDevaaS® 2.0

通常、Webアプリケーションを開発する際の機能テストを走らせている背後で、Seeker IASTが稼働し、脆弱性などのセキュリティリスクを検出します。新たにセキュリティ診断用のサーバーを用意する必要もなく、通常の機能テストを実施する環境をそのまま使った診断が可能です。試験サーバーに対してXSS攻撃を実施するような試験の必要がなくなりますし、優秀な技術者がソースコードレビューに忙殺されるといった状況から開放することも可能です。脆弱性には詳しくない開発者でもコーディングの一環でソースを修正できます。

吉井氏は「これまでDevOpsにセキュリティを組み込めば、リリースが遅くなるという問題を抱えていました。しかし、これらのセキュリティ診断ツールをDevOpsサイクルに組み込むことで、スピードとセキュリティを両立したDevSecOpsを実現できます」といい、締めくくりました。

※ 商品およびサービスの内容は、予告なく変更する場合がありますので、あらかじめご了承ください。

※ 「SmartCloud(スマートクラウド)」、「SmartCloud」ロゴ、「DevaaS」、「DataSkywalker」は、NTTコムウェア株式会社の登録商標です。

※ その他、記載されている社名、商品名などは、各社の商標または登録商標である場合があります。

※ 所属部署、役職等については、取材当時のものです。

