【DevSecOps とは？】

入門者向けにメリットなどの概要をわかりやすく解説

システム開発において「DevSecOps」というキーワードが注目されています。本ページでは、「DevSecOps とは何ですか？」や「DevSecOps とはどういう意味ですか？」についてシステム開発に携わる関係者が共通の理解を深めるために、DevSecOps の特徴などの概要、開発の流れ、実現方法の順で説明します。

DevSecOps とは

DevSecOps の概要を以下の順で解説します。

- 登場背景と重要性
- 定義
- DevOps との違い
- 必要性とメリット
- 市場規模から考える注目度
- 導入の課題

登場背景と重要性

今までは、ウォーターフォールモデルによるシステム開発が一般的でした。
しかし、近年、様々な企業がデジタル技術を用いるようになり、ビジネス環境の激しい変化や不確実性が増しています。それにより、ビジネス環境の変化に素早く対応する必要がある場合、新しい機能やサービスをできるだけ速く提供できる DevOps が求められるようになりました。

DevOps は、開発チームと運用チームが協力しあうシステム開発です。そのため、開発チームがシステムで必要とされる機能をいち早く知ることができたり、機能が必要とされる時期を事前に把握できたりします。また、開発中に開発チームから運用チームへの新機能に対する教育を実施できます。このような協力関係を築くことで、ビジネスの状況を見ながら、システムの安定稼働を維持しつつ必要な時に必要な機能を素早く提供できます。

また、近年、ランサムウェアなどの新しいサイバー攻撃が次々と生まれ、被害が増加しています。さらに DevOps によるシステムの素早い変化も起こっています。このような早い変化に追従しつつ、サイバー攻撃による被害を最小限にすることも求められています。
それを実現するために、DevOps にセキュリティを組み込んだ DevSecOps というシステム開発があります。

ちなみに、DevSecOps の起源は、世界有数のリサーチ&アドバイザリ企業である Gartner が 2012 年 1 月に提唱し始めたと言われています。その際は、DevOpsSec と説明されていました。

- DevOpsSec: Creating the Agile Triangle（Gartner のオフィシャルページへ）
  https://www.gartner.com/en/documents/1896617

定義

DevSecOps(読み方：デブセックオプス)とは、DevOps と Security を合わせた造語です。ちなみに、DevOps とは、ソフトウェア開発の手法のひとつで、開発チーム（Development）と運用チーム（Operations）が協力しあってシステムを開発・運用することで、ビジネスの価値を高めるための様々な取り組みを示す概念です。

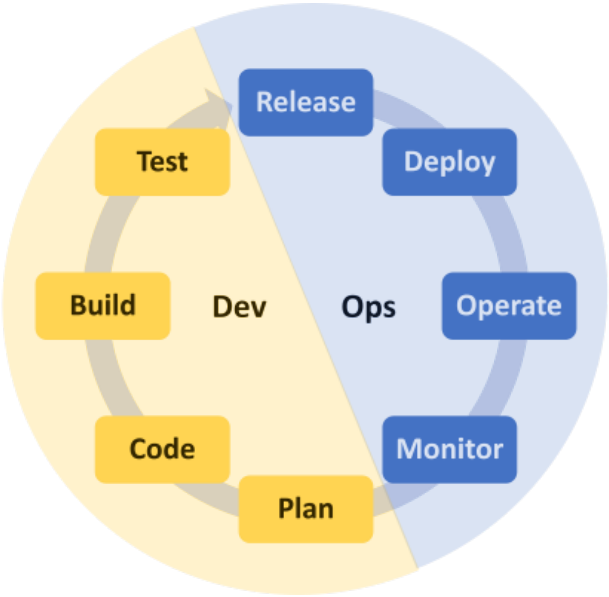

図 1：DevOps の全体像

DevOps の取り組みに対して、DevSecOps ではセキュリティ観点の要素が付与されます。すなわち、DevSecOps とは、開発、運用、セキュリティを密に連携させ、シフトレフト(ある工程を通常よりも前倒しで実施すること)の考えのもと、DevOps で開発後に実施していたセキュリティ対策を前倒しで実施することで、問題の早期検出による対応コストを削減できる取り組みのことです。脆弱性などのセキュリティ観点でのリスクを早期発見するために、システムの開発と運用の各工程でセキュリティ対策を実施します。工程ごとのセキュリティ対策に関しては、本記事の後半で解説します。

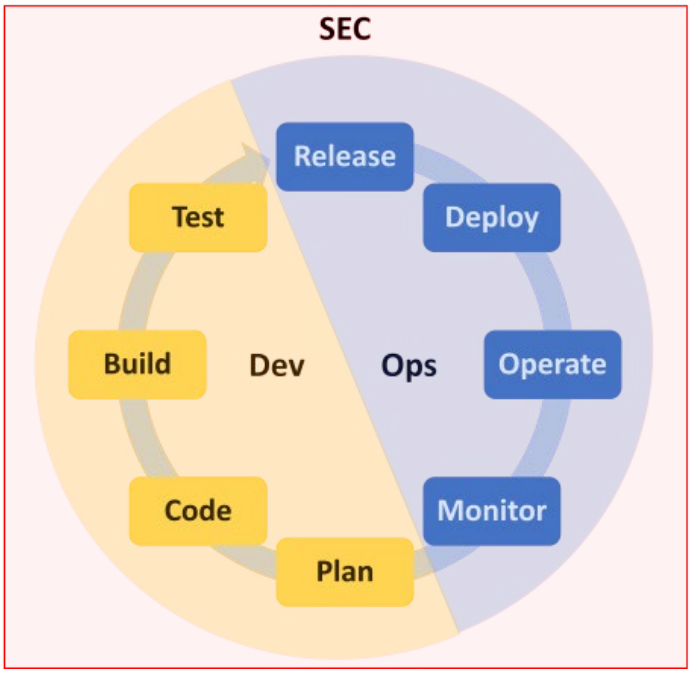

図 2：DevSecOps の全体像

DevOps との違い

DevOps と DevSecOps の違いとして、「期待できる効果」があります。DevOps と DevSecOps の効果を以下の表にまとめます。

表 1 DevOps と DevSecOps の効果

効果	DevOps	DevSecOps
短期間での製品リリース	あり	あり
製品の品質向上	あり	あり
開発や運用にかかるコスト削減	あり	あり
セキュリティ事故による企業価値低下の抑止	一部あり	あり

DevOps と DevSecOps の期待できる効果において、「セキュリティ事故による企業価値低下の抑止」という点が異なります。
DevOps では開発後にセキュリティ対策を実施します。それにより、最適なタイミングや対処の細分化がされていなかったため、セキュリティ対策の長期化や手戻りなどが発生していました。

一方の DevSecOps では、ソフトウェア開発の各段階で行うべきセキュリティ対策や観点を明確に型化するため、毎回同じレベルのセキュリティを確保できます。さらに、DevOps に型化したセキュリティ対策を組み込んだことにより、優先する機能を高セキュリティに保ったまま提供できたり、その時に優先するべきセキュリティ課題に迅速に対応できたりします。

必要性とメリット

DevOps は開発と運用を組み合わせることで開発速度を向上させます。ただし、セキュリティに関しては細分化されていないため脆弱性などの早期対処が困難という課題があります。
そこで、DevOps の各工程にセキュリティ観点を組み込んだ DevSecOps では、初期段階で脆弱性などのセキュリティリスクを検出し、セキュリティの脅威を最小限に抑えることができます。これにより、脆弱性などのセキュリティリスクの低減と開発速度の維持を実現できます。

市場規模から考える注目度

2020 年のグローバル DevSecOps 市場規模は 27.9 億ドルであり、2021 年から 2028 年までの年平均成長率（CAGR）は 24.1%で拡大することが予想されています。さらに、アジア太平洋地域は、最も高い DevSecOps 市場の成長を説明すると推定されています。
市場規模が年々拡大していることから、将来性があり注目度が高い技術分野となります。

- Global DevSecOps Market Share Report, 2021-2028（MarketsandMarkets のオフィシャルページへ）
  https://www.grandviewresearch.com/industry-analysis/development-security-operation-market-report

導入の課題

DevSecOps の課題として、「組織」「ツール」「データ」の 3 つの観点があります。

組織に関する課題

DevSecOps を実現するためには、開発・運用・セキュリティチームが密に連携できる組織形成が必要です。密に連携できない組織形成である場合、組織形成から変えていく必要があります。
また、組織の既存ルール(例：ある判定結果の脆弱性には必ず対応する)を DevSecOps の全工程に適用した結果、開発速度が低下す

る危険性もあります。よって、組織の既存ルールを DevSecOps に適したものに変更する必要があります。
さらに、DevSecOps を実現する上で、セキュリティの内製化が望ましく、段階的にでも内製化に取り組まない場合、開発速度の低下に繋がります。密に連携できるチームにセキュリティ有識者がいない場合、セキュリティ有識者の人材確保に取り組む必要があります。

以上のように組織観点では、「組織形成」「組織の既存ルール」「セキュリティ人材の確保」の 3 つの課題があります。

ツールに関する課題

DevSecOps では、開発や運用の各工程で適切なセキュリティ対策を実施します。開発や運用の速度を維持するためにも、高速なセキュリティ対策の適用が求められます。
その 1 つの方法として、セキュリティ対策を自動で実施するテストツールの導入が考えられます。
今まで使っていたテストツールが、手作業で行うものであった場合、「人手が必要」、「終了まで長時間必要」、「繰り返し何度も実施が困難」などの課題が挙がります。また、不適切なテストツールを導入した場合、「脆弱性の過検知」や「未知の脅威を検出不可能」などの課題が発生します。よって、組織の情報セキュリティポリシーを満たす自動テストツールの導入が必要です。

以上のように「テストツール選定の難しさ」という課題があります。

データに関する課題

DX 時代ではデータドリブン経営が主となり、エンタープライズ(企業や事業)領域でもシステム開発の短期間化が求められています。その際に DevSecOps の適用により、新しいデータ処理やそれを基にした新サービスの早期リリースを実現できます。
DevSecOps におけるアプリケーション観点でのセキュリティを考慮する方法については様々なウェブメディアで言及されています。しかし、DevSecOps におけるデータに対する情報セキュリティ(機密性、完全性、可用性)を考慮する方法についてはあまり言及されていません。

近年、データを起点としたランサムウェアなどのセキュリティ事故が多発しているため、DevSecOps におけるデータに対する情報セキュリティも考慮が必要です。本記事では、データ格納場所であるデータベースに対する情報セキュリティに関しても解説します。

DevSecOps での開発の流れ

DevSecOps は、8 つの工程で構成されます。さらに各工程でセキュリティ対策も実施します。以降で、各工程の概要と実施するセキュリティ対策に関して説明します。

8 つの工程

DevSecOps は、4 つの開発工程と 4 つの運用工程で構成されます。各工程の概要を以下の表にまとめます。

表 2 DevSecOps の工程

種類	工程	実施内容
開発工程(Dev)	Plan	プロジェクト全体のタスク管理や開発要件を定義します。
	Code	開発要件に沿って、ソースコードの作成をします。
	Build	ソースコードからアプリケーションを作成します。
	Test	開発環境や検証環境でビルドしたものに不具合がないかを確認します。本工程を踏むことで、開発物の品質を担保できます。
運用工程(Ops)	Release	開発物を本番環境に適用するスケジュールや手順を決めます。
	Deploy	ビルドしたアプリケーションを本番環境に配備し、現在稼働中のアプリケーションから切り替えます。
	Operate	本番環境のアプリケーションやインフラの監視、保守作業やトラブル対応を行います。
	Monitor	運用やユーザーから得られた情報(性能値、評価、要望など)を確認し次の Plan に繋げます。

各工程でのセキュリティ対策と自動化ツール

DevSecOps の各工程でのセキュリティ対策を「アプリケーション観点」と「データベース観点」に分けて以下の表にまとめます。

表 3 DevSecOps でのセキュリティ対策

工程	アプリケーション観点でのセキュリティ対策	データベース観点でのセキュリティ対策	自動化に利用できるツールの例
Plan	—	セキュリティポリシー策定、基盤選択、コンプライアンスチェック、DBMS 設計	データベース：Fujitsu Enterprise Postgres
Code	静的アプリケーション・セキュリティ・テスト（SAST）	データベースの定義資材の作成、プログラミング	SAST：GitHub(シークレットスキャン)、Coverity、SonarQube
Build	ソフトウェア・コンポジション解析（SCA）	資源の一元管理、分散管理	SCA：Black Duck、GitHub(コードスキャン)、Prisma Cloud
Test	動的アプリケーション・セキュリティ・テスト（DAST）、インタラクティブ・アプリケーション・セキュリティ・テスト（IAST）、ペネトレーションテスト	業務テスト、ペネトレーションテスト	• DAST：Contrast Assess、VEX • IAST：Contrast Assess、Seeker • データベース：Fujitsu Enterprise Postgres
Release	—	—	—
Deploy	—	セットアップ	データベース：Fujitsu Enterprise Postgres
Operate	—	起動・停止、バックアップ・リカバリー、計画切り替え、トラブル対処	データベース：Fujitsu Enterprise Postgres
Monitor	システム監視、アプリケーション／ネットワーク監視、可視化、異常監視	容量監視、性能監視、アクセス監視、セキュリティ障害の通知	• システム監視：Nagios, Ganglia • アプリケーション／ネットワーク監視：StatsD、Prisma Cloud • 可視化：Graphite • 異常監視：Kale、Prisma Cloud • データベース：Fujitsu Enterprise Postgres

各工程で実施するデータベース観点でのセキュリティ対策の詳細に関しては、以下の記事で紹介しています。

- 【DevSecOps を導入する】データベース観点でのセキュリティ対策

DevSecOps の実現方法

DevOps 形成後に段階的に DevSecOps に移行することで、効率よく DevSecOps を適用できます。

DevOps 形成後、3 ステップに分けて段階的に DevSecOps へ移行できます。

1. 現在のセキュリティ対策の評価

脅威モデリングを実施し、現在のセキュリティ対策を評価しましょう。脅威モデリングとは、開発したシステムやソフトウェアを分析して脆弱性などのセキュリティリスクを明確化するプロセスのことです。脅威モデリングは、以下の 5 ステップから構成されます。

1. システム構造図
2. データフローライン
3. データフローラインをたどる
4. 脅威の洗い出し
5. シナリオ数分繰り返し

各ステップの詳細に関しては、以下 IPA のオフィシャルページをご覧ください。

- 脅威モデリングの手順（IPA のオフィシャルページへ）
  https://warp.ndl.go.jp/info:ndljp/pid/12446699/www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c101.html

2. 開発工程におけるセキュリティを統合

Plan から Test までの開発工程に、表 3 に掲載したセキュリティ対策を組み込みます。その際に、適切な自動テストツールを組み込むことにより、混乱を最小限にした統合を実現できます。

3. 運用工程におけるセキュリティを統合

運用中の製品やシステムにおいて、セキュリティ上の懸念を継続的に監視できるようにしましょう。脆弱性が検出された場合、迅速な対応ができるように事前に検出内容ごとの対策プランを明確化しておきましょう。

近年、ビジネス環境の変化が激しく、様々なサイバー攻撃も多発しています。そのような環境下で、迅速かつ安心安全にソフトウェア開発する方法の一つとして、DevSecOps があることを説明しました。
また、「組織」「ツール」「データ」の課題を解消した上で段階的に DevOps から移行することで、DevSecOps を円滑に適用できると解説しました。
データの課題に対しては、古くからデータベースミドルウェアが取り組んでおり、データベースミドルウェアである Fujitsu Enterprise Postgres を使うことでデータの課題を解消できます。例えば、Fujitsu Enterprise Postgres の機密管理支援機能を使うことで、データの情報セキュリティに関して内製化しやすくなります。DevSecOps を適用するために、Fujitsu Enterprise Postgres の活用をぜひご検討ください。
お問い合わせは本ページに表示されているお問い合わせボタンから、または本ページ下部に記載のお問い合わせ先からご連絡ください。

2023 年 6 月 29 日