金融サービスでの
DevSecOpsを正しく理解する

はじめに

銀行、投資会社、保険会社などの金融サービス機関は、サイバーセキュリティを継続的に強化しつつソフトウェアリリースのスピード向上を強く求められています。一見するとこの2つの目標は相反するように見えますが、金融サービス企業にとってこの相反する目標を実現する方法があります。それがDevSecOpsなのです。

DevSecOpsとはSDLC（ソフトウェア開発ライフサイクル）全体にわたる開発、セキュリティ、運用チームをエンドツーエンドで連携させて、それぞれのタスクを自動化し、モバイルアプリ、Webサービス、API、IoTネットワークといったデジタルビジネスを支えるソフトウェアの頻繁かつ安全なリリースをすることです。

本書では以下について説明します。

- SDLCのセキュリティと俊敏性を向上させようとする際に
  金融サービス事業者が直面する主な課題
- DevSecOpsがどのように企業のデジタルビジネスを守り
  競争力を向上するのか
- バイナリ管理がDevSecOps戦略の鍵となる理由とバイナリ構成を理解する上での
  ソフトウェア部品表（SBOM）の重要な役割

金融業界の課題

どの業界の企業もソフトウェアパイプラインのスピード向上とセキュリティ強化に努めている一方で金融サービス企業は顕著な業界特有の課題に直面しています。

サイバー犯罪者に狙われやすい業界

銀行をはじめとする金融サービス企業は、個人情報や財務情報の宝庫であるため、サイバー犯罪者の主要なターゲットとなっています。ハッカーたちは銀行に侵入すると、個人や法人のお客様情報、銀行のプロセス、財務記録など機密データにアクセスできるようになります。その結果、これらの機関は最新かつ最も洗練されたあらゆる方法で激しく絶え間ない攻撃を受けています。

銀行はDDoS（Distributed Denial of Service 分散サービス拒否）攻撃、ランサムウェア攻撃、フィッシング詐欺、ゼロデイ脆弱性攻撃、APT（高度な継続的脅威）、マルウェア感染、マンインザミドル攻撃、クロスサイトスクリプティング、IoT侵害、**サプライチェーン侵害**といった攻撃を特定のタイミングで受ける可能性があります。

重い規制の負荷

金融サービスは最も規制の厳しい業界の1つであり、世界中で膨大で複雑な一連の義務と政府の規制の対象になっています。DevOpsチームにとって、従業員、お客様、パートナーにリリースするすべてのソフトウェアが、企業がビジネスを行っているすべての国や地域で増え続ける複雑かつ時には多くの混乱を招く規制に準拠してるかを確認しなければならないことは、明らかに負担となります。失敗すれば重い罰金、法的責任、評判の低下、ビジネスの損失につながる可能性があります。

規制の一例

- **強力な顧客認証（SCA）**：金融系アプリでは少なくとも2つの形式でユーザ認証が要求されるヨーロッパの規制

- **支払いカード業界のデータ・セキュリティ標準（PCI DSS）**：クレジットカード会員情報の収集、保存、処理、送信を保護するための世界的な業界標準

- **金融商品市場司令（MiFID）**：投資家を保護することを目的とした欧州の規制
- **改正決済サービス指令（PSD2）**：電子決済のセキュリティと透明性を向上を目的とした欧州の規制
- **SOX法／サーベンス・オクスリー法**：企業や会計の不正や汚職を抑止・処罰し、労働者や株主を保護することを目的とした米国連邦法
- **ドット・フランク法**：EU居住者のプライバシーと個人データの保護を目的とする金融業界固有ではないヨーロッパの規制
- **一般データ保護規制（GDPR）**：EU居住者のプライバシーと個人データを保護することを目的とする金融業界固有ではないヨーロッパ規制
- **国家のサイバーセキュリティの改善に関するホワイトハウスの大統領令**：金融業界に特化したものではありませんが、米国政府と米国の民間企業に影響を与える**サイバーインシデントの予防と対応**の強化を目的とした米国の大統領令

制限が多いデジタル環境

金融サービス業界のITインフラは他のどの業界よりも、エアギャップ・システム、強化されたアクセス制御、最小限のチーム間コラボレーション、変更管理と承認の遅さ、厳格な監査とガバナンス、開発者の柔軟性の制限といった俊敏性を妨げる厳しい制限があるのが特徴です。

さらにこの分野のITインフラでは、従来のオンプレミスのデータセンターから**マイクロサービスアーキテクチャとコンテナ**を備えた最新のハイブリッドクラウドのデプロイに至るまで複雑・大規模で異種混在の傾向があるという事実も問題を複雑にしています。またスマートフォン、ATM、POS端末など幅広く多様なエンドポイントをサポートする必要があります。

技術革新による重圧

金融業界は目まぐるしい技術革新に対応し、破壊的なスタートアップ企業や確立した影響力の高い既存企業の両方に対して競争力を維持する必要があるため絶えず重圧を背負っています。最近の「FinTech」の進歩にはロボアドバイザー、ネット専門銀行、暗号通貨、ブロックチェーン、AIベースのサービスのカスタマイズ、P2Pのトランザクションがあります。

つまり金融サービス企業はデジタルサービスを継続的に強化するために、新しいソフトウェアやソフトウェアのアップデートを頻繁にリリースする必要があることを意味します。これらは脆弱性や設定ミス、その他のセキュリティやコンプライアンスの欠如を含むソフトウェアデプロイ時のリスクが高まるためつい10年ほど前からこれらの企業が回避してきた変化とも言えます。

エスカレートする顧客要求

金融サービス事業者のデジタル体験に対するお客様の期待値は増大し続けています。お客様は携帯電話、PC、タブレット端末を利用したデジタルチャネルによる銀行業務、株取引、支払い、退職金管理などの利便性を求めています。これらのサービスはますますパーソナライズされ、機能が豊富かつ高速になり、常に利用可能であることを期待されています。そして当然のことながら、すべてのデジタルトランザクションの安全性も期待されます。

金融サービスのデジタル化により、お客様は銀行やその他の事業者をこれまでになく簡単に変更できます。そのため、これらの企業はお客様のデジタル体験を継続的に改善することが急務となっています。

SDLCを保護し高速化するDevSecOps

では、これらの課題にどう対応すればいいのでしょうか。セキュリティを犠牲にすることなく、ソフトウェアのリリース速度と革新性をどのように維持すればいいのでしょうか。まずはIT環境がオンプレミス、クラウド、またはその両方であるかに関わらず、SDLC（ソフトウェア開発ライフサイクル）プロセスが俊敏かつ安全であるか確認することにフォーカスするべきです。そしてDevSecOpsがそれを可能にします。

DevSecOpsの採用がもたらす人材、プロセス、テクノロジーの変化により**金融サービス機関**では次のことが可能になります

- SDLCに関わるすべてのチームメンバーとステークホルダー（主に開発、運用、セキュリティだけでなく、QA・テスト、ビジネスリーダー、GRC、上級管理職）の間でオープンなコミュニケーション、コラボレーション、説明責任を共有する文化を確立します。

- できるだけ多くのセキュリティとコンプライアンスのチェックを含むタスクを自動化することでSDLCのスピードと敏捷性を高め、設計段階から始まるすべてのステップにネイティブに組み込み、問題を早期かつ頻繁に検出して修正できるようにします。

- SDLC全体でソフトウェア・バイナリをきめ細かく管理・追跡するため、深刻な脆弱性やコンプライアンスの問題が含まれていることが判明した場合は、それらが使用されている場所を特定し「深刻な影響が及ぶ範囲」を理解した上で問題を迅速に修正できます。

- SDLCを通じて生成されたすべてのアーティファクトの信頼性を検証することで、開発者や運用メンバーはパイプラインによって作成されたビルドに欠陥のあるアーティファクトが含まれていないことを確認できます。

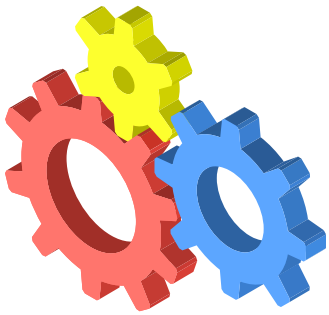
DevSecOpsの中心となるバイナリ管理

ビルドの段階でソースコードがバイナリにコンパイルされるとすぐに、バイナリはDevOpsパイプラインの重要な資産になります。なぜなら開発者がビルド、テスト、プロモート、本番環境にリリースするといった一連の流れを通過した**唯一の情報源**になるからです。このため、バイナリフローを管理することはソフトウェアビルドの整合性と再現性、ひいてはアプリケーションの品質と安全性を確保するための重要な鍵となります。

高速で安全なソフトウェアリリースを実現するために必要なコアな要素は、あらゆる種類のソフトウェアパッケージに対応したリポジトリマネジャーを中核とするエンドツーエンドで拡張可能な**DevOps Platform**です。このPlatformはREST APIを介してすべてのサードパーティのDevOpsツールと簡単に統合でき、本番環境でのソフトウェアのセキュリティスキャン、配布、監視のためのコンポーネントが含まれている必要があります。

Platformのリポジトリでは、社外から入手したものであるか、社内のものであるかに関わらずすべてのバイナリを保存し、ユニークに識別する必要があります。これにより、金融サービス企業が潜在的な脅威に対応するために使用できる唯一の正しい情報源を提供でき、それに応じてルールとポリシーを作成し、以下のようなバイナリに対する特定のアクションをトリガーできます。

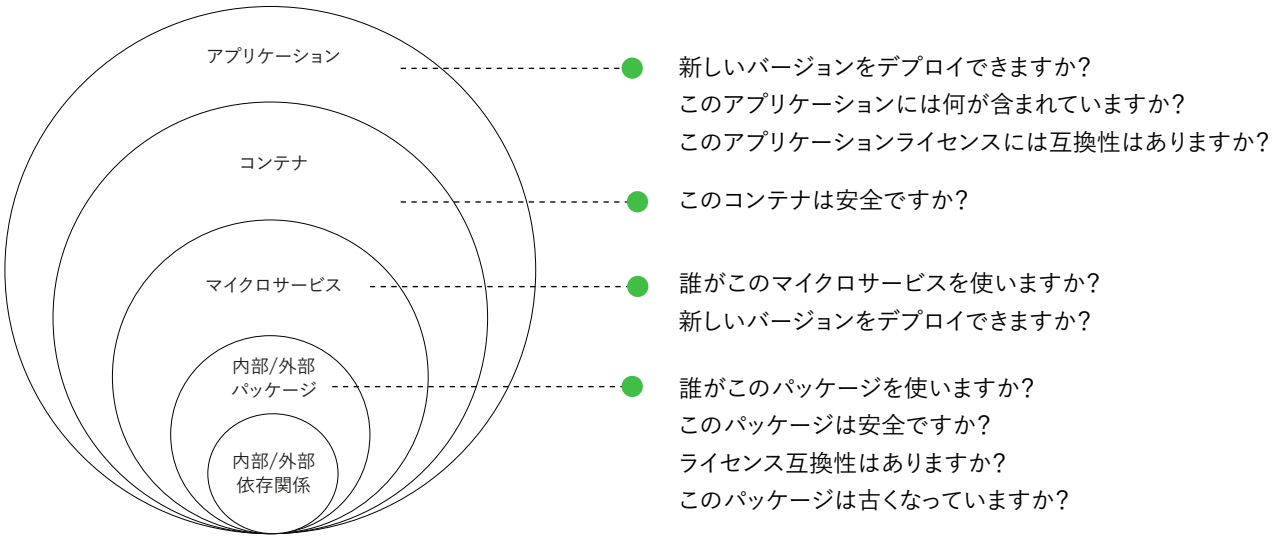
- 問題を検知した際に利用できないようブロック
- フラグを立てる
- 新しいメタデータの追加
- 二次プロセスの開始
- 適切なチームメンバーへの通知



金融セクターのDevOpsチームにとって重要な機能は、**エアギャップ環境**、つまりインターネットに接続されていない環境のサポートです。通常、開発組織は**Docker Hub**などのリモートパブリックリソースにアクセスしてビルドの依存関係をダウンロードします。しかし金融機関は多くの場合その運用をインターネット上に公開できないという厳しい要件があるため、このエアギャップのシナリオをサポートするDevOps Platformを用意することが必要不可欠となります。

金融サービス企業はまた、サードパーティの相互依存関係、特にアプリケーションコードのベースの90%以上を占めることが多いAPI、ライブラリ、ベースOSなどのオープンソースコンポーネントでは、バイナリの詳細な可視性が求められます。

バイナリ構成を理解するために、DevOps Platformはリリース、配布、デプロイするすべてのソフトウェアの**ソフトウェア部品表（SBOM）**を生成する必要があります。SBOMにはオープンソースか商用ライセンスのあるソフトウェアに限らず、ライブラリやモジュールなど、ビルドプロセス中に使用される開発ツールやCI環境に関するソフトウェアの部品を構成するすべての「コンポーネント」のリストが含まれています。

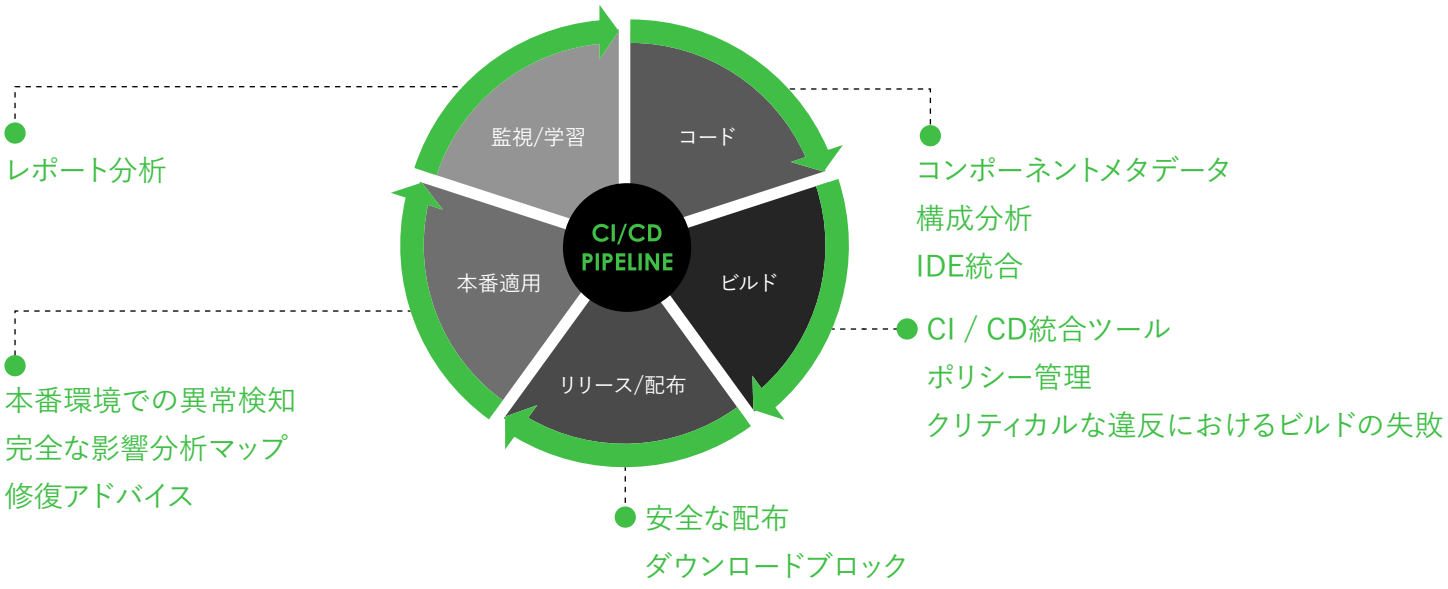


SBOMを見ていくことで、ソフトウェアがいつ構成されたか、開発、QA、ステージング、本番といったSDLCのどの段階を経ているか、また**セキュリティとコンプライアンス**のどの問題が検出され修正されたかという情報を説明できます。

この情報はDevSecOpsへの取り組みを強化し、さまざまなユースケースでセキュリティやコンプライアンスを維持する役目をしています。例えばSBOMはアプリケーションとさまざまなバージョンで使用されているすべての上位コンポーネントの詳細を表示します。これによりアプリケーションに影響を与える脆弱性が検知されたときに、影響を受けるバージョンとその対処法を簡単に検出できます。

また、PlatformはSDLCフェーズ全体で脆弱性、ライセンスコンプライアンスの問題、その他の問題を検出して修正するためにすべてのソフトウェアコンポーネントを継続的にスキャンする必要があります：

- コード：コンポーネントのメタデータのキャプチャ、構成分析の実行、組織のIDE（総合開発環境）との統合
- ビルド：CI/CDシステムとの統合、ポリシー管理の実施、クリティカルな違反を伴う場合にビルドを失敗とする
- リリース・配布：ソフトウェアの安全な配布とダウンロードのブロック
- 本番環境：違反の検知、完全な影響分析マップの生成、修正アドバイスの提供を含む
- 監視：レポートの作成や分析の生成を含む



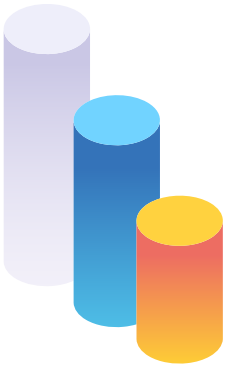
要約すると、ネイティブのセキュリティとコンプライアンス機能を備えた**エンドツーエンドのDevOps Platform**を使用することで、金融サービス機関はバイナリの完全な説明責任、トレーサビリティ、監査可能性を確保できます。そのためバイナリで問題が発生した場合には、正確で迅速な根本原因の分析を実施し、適切なアクションを実行できます。

結論

本書では、DevSecOpsの採用が金融サービス業界にとって必須である理由を説明しました。DevSecOpsはソフトウェアリリースのペースを落とさずSDLCを適切に保護するのに役立ちます。

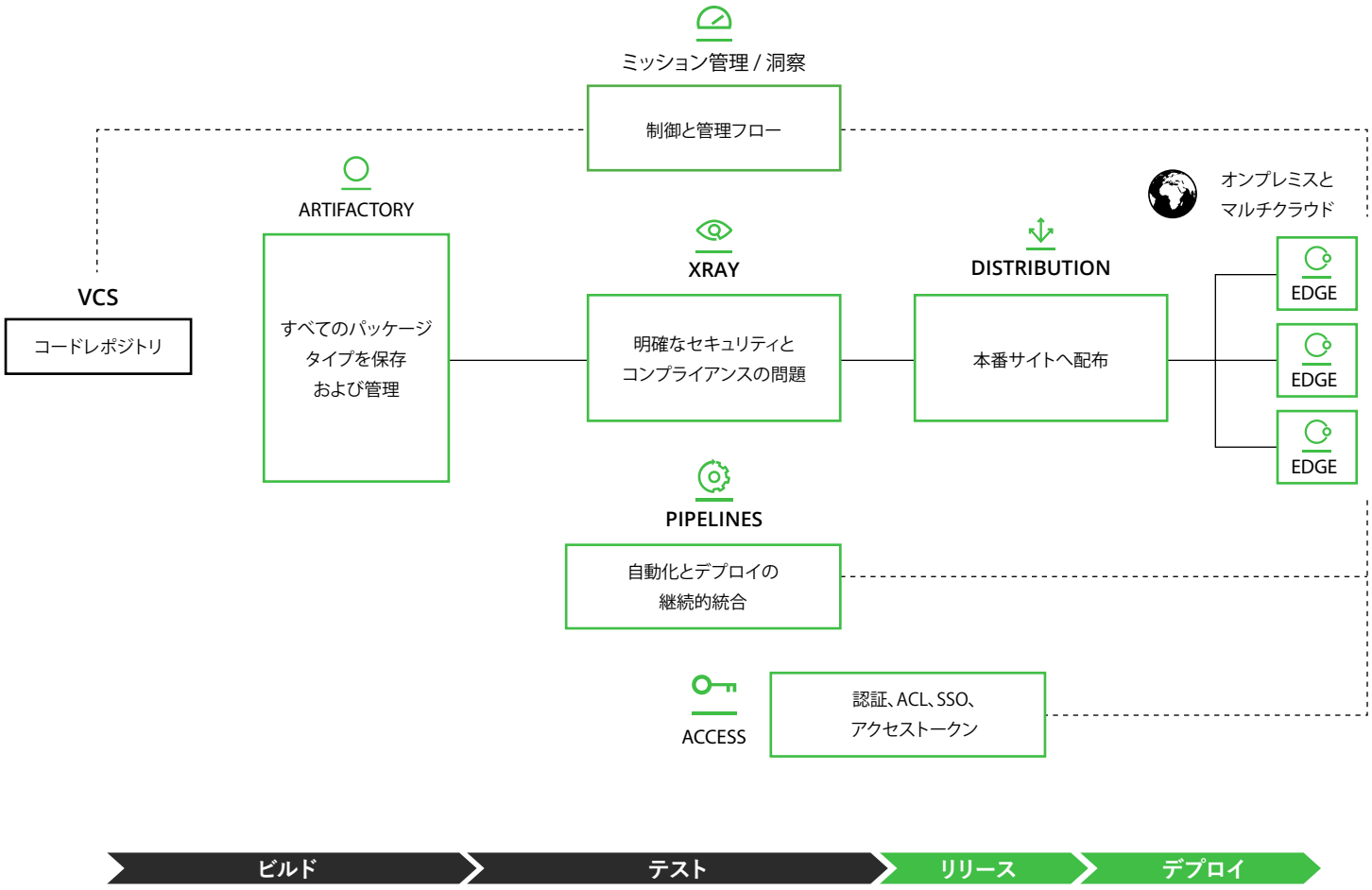
銀行やその他金融サービス事業者にとってDevSecOpsの主なメリットは次のとおりです：

- SDLCをエンドツーエンドで保護
- ソフトウェアリリースの加速
- 開発、運用、セキュリティチームの生産性の向上
- チーム間のコミュニケーションとコラボレーションの増加
- デジタルサービスの品質、パフォーマンス、信頼性、革新性の向上
- 以下のようなビジネスの成長と拡大
    - 収益の増加
    - よりよい顧客維持
    - コスト削減
    - カスタマーエクスペリエンスの向上



金融サービスでDevSecOpsをうまく採用する方法に関する詳細については**こちらのデモをご覧ください。**JFrog DevOps Platformにはセキュアでコンプライアンスに準拠したソフトウェアを迅速かつ頻繁にリリースするエンドツーエンドのDevOpsパイプラインをデプロイするのに役立つすべての特徴と機能を備えています。

THE JFROG PLATFORM



JFrog Japan 株式会社

〒 100-0004 東京都千代田区大手町1-9-2 Global Business Hub Tokyo | TEL: 03-4243-1049 | Webサイト:jfrog.com/ja/ | ブログ:jfrog.com/ja/blog/
お問い合わせ:jfrog.com/ja/contact-us/

EB202210-D