企業のDXにおける新たなサイバーセキュリティ

アジャイル開発でのセキュリティ実装
セキュリティ担当者の役割

PwCコンサルティング合同会社　シニアマネージャー　山田 素久

ビジネスのスピードが加速しシステム開発にスピードが求められるようになった昨今、アジャイル開発はスタートアップ企業だけではなく、成熟した大企業でも採用されるようになりつつあります。組織の規模が大きな企業では、一般的にインフラ部門とシステム・アプリケーション開発部門は分離されており、企画・開発・運用を独自に行っているケースが多く見られます。

一方、アジャイル開発においては開発側と運用側が協力して継続的に開発を行うDevOpsが取り入れられ、部門の垣根が曖昧になりつつもあります。また、コンテナ技術やサーバーレスアーキテクチャの発展により、インフラは、これまでのようにインフラ担当者に事前に用意されてアプリケーション層とは切り離されてメンテナンスされる存在ではなく、アプリケーションの一部としてデプロイされるようになっています。

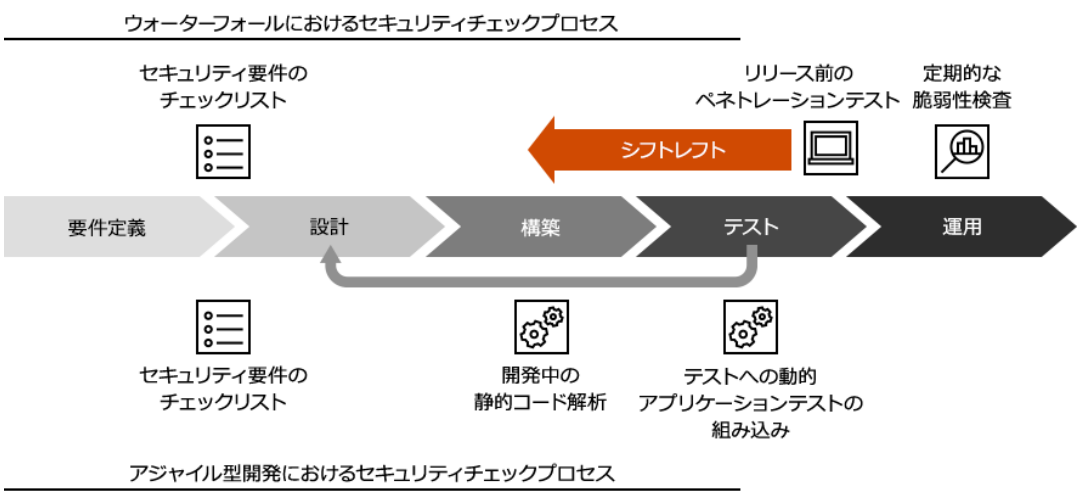
このように刻々と変化する状況で適切なセキュリティを確保するためには、アプリケーション開発者、インフラ担当者およびセキュリティ担当者のそれぞれが、変わっていく自らの役割を意識し、これまでとは異なるアプローチを取る必要があります。本稿では特に大企業におけるセキュリティ担当者とインフラ担当者の役割の変化に注目することで、アジャイル開発に必要なセキュリティの実装についての留意点をまとめます。

アジャイル開発におけるセキュリティの確保は「シフトレフト」が鍵を握る

大企業においては、アジャイル開発が急激に全てのプロジェクトに採用されるということは少なく、プロジェクトの性質に合わせて徐々に浸透していくことがほとんどです。アジャイル開発はその性質上、セキュリティのための修正にもスピードが要求されるので、手戻りをなくすために問題の早期発見がより重要となります。したがってセキュリティのレビューも、ウォーターフォール型開発で一般的な、完成後のセキュリティレビューやペネトレーションテストではなく、開発時におけるコードレビューや静的コードスキャンを自動的に行う、いわゆる「シフトレフト」が求められます。DevOpsにこうした自動的なセキュリティチェックを取り入れた、DevSecOpsの概念が提唱されていますが、本稿では自動化やツールの導入の観点ではなく、こうしたセキュリティチェックをも自動化した開発においてセキュリティ担当者が果たすべき役割について説明します。

図表1：セキュリティチェックのシフトレフト

・従来のウォーターフォール型開発では各フェーズの終了時にセキュリティのチェックを行っていたが、
アジャイル開発では構築中に都度チェックを行う必要がある。
チェックが前工程（左）に移行していくことから、シフトレフトと呼ばれる。



セキュリティ担当者は「ゲートキーパー」から「アジャイルの輪の中への参加」を

アジャイル開発におけるセキュリティ担当者の役割の変化をまとめると、以下の3点になります。

1. 開発者の啓蒙と教育
2. 適切なセキュリティチェックプロセスとツールの導入
3. Trust, but Verify

1. 開発者の啓蒙と教育

開発されるアプリケーションのセキュリティは、開発者によるコーディングに大きく依存します。しかし、高度に自動化され、高速なリリースが要求されるアジャイル開発においては、全てのコードをセキュリティ担当者がレビューするのは不可能です。したがって、通常はセキュリティに疎遠な開発者を啓蒙し、教育することが、セキュリティ担当者の重要な役割の1つとなります。これまではゲートキーパーとしてリリース前の判定会議でしか顔を合わせないという関係性だったとしても、開発現場に足を運んでアジャイル開発の輪の中に入り、啓蒙活動を行うという変化が求められます。

2. 適切なセキュリティチェックプロセスとツールの導入

DevSecOpsというとどうしてもツールの導入が先行する印象がありますが、いきなりツールを導入することはおすすめできません。使い慣れないツールや結果を生かせないツールを入れても開発者に利用されず、無駄な投資になる恐れがあるからです。まずは自社の開発するアプリケーションや開発者のレベル、開発体制などを俯瞰した上で効果的なセキュリティチェックプロセスの策定を行い、その上で必要な箇所にツールを実装するアプローチが望ましいと考えます。多種多様なアプリケーション開発環境において常に最適なプロセスやツールは無いため、原則とリスクの受容を使い分ける判断ができる関係を築いておくことも重要です。

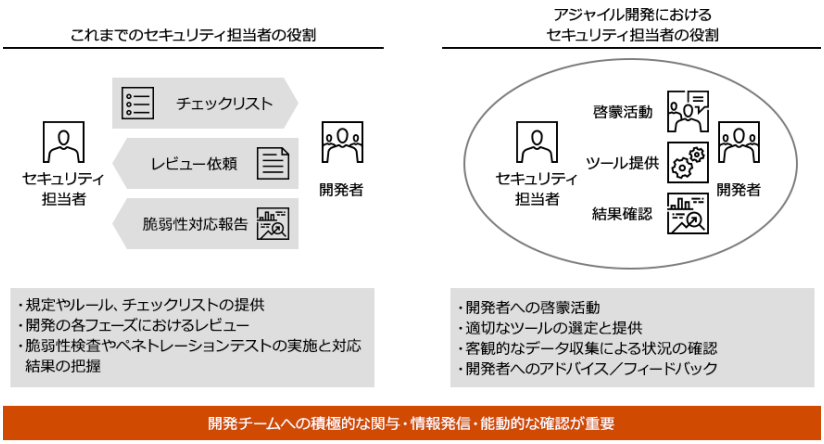
3. Trust, but Verify

前述の通り、アジャイル開発ではアプリケーション開発者が担う役割が大きく、セキュリティ担当者が全てをチェックする事はできません。基本的にはアプリケーション開発者を信じる（Trust）ことが重要ですが、結果を常に確認する（Verify）ことも重要です。チェックリストを作って自己申告してもらった結果を確認するのではなく、静的解析ツールの実行結果および修正状況やペネトレーションテストの実施結果など、客観的なデータを確認し、状況を常に把握することが必要となります。

本稿では、大企業でのアジャイル開発におけるセキュリティ担当者の役割の変化について述べました。大企業でアジャイル開発に取り組む場合、これまでアプリケーション開発を担っていたベンダー／協力会社とは異なる企業と協業して開発を行う事例も多く、そうした新規の協力会社は社内のレビュープロセスなどに関する知識も少ないため、どうしてもセキュリティ担当者の目が行き届かなくなりがちです。アジャイル開発が広まっていくに連れ、セキュリティ担当者はこれまで以上に現場に飛び込んでいかなくてはならないことを理解し、実践していただきたいと思います。

図表2：セキュリティ担当者の役割の変化

・セキュリティ担当者は開発フェーズにおけるゲートキーパーからアジャイル開発のアドバイザーに役割を変化させなければならない。



お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com

© 2020 PwC. All rights reserved. PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.