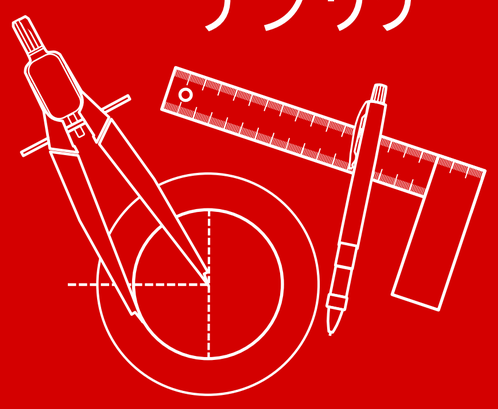
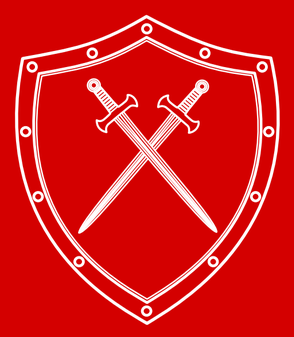
ほとんどの攻撃はインフラストラクチャセキュリティソリューションが有効でないアプリケーション層で発生する。残念ながら
アプリケーション開発では設計によるセキュリティ(Security by Design)とハードニングはまだ一般的ではない。それを変えよう！

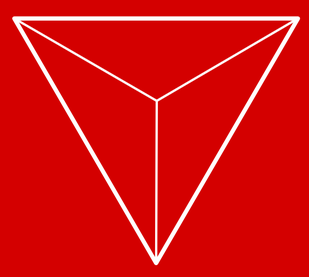
アプリケーションセキュリティを促進するための3つの便利な概念



「シフトレフト」



「Security by Design」



「DevSecOps」
継続セキュリティハードニング

「IT現場」と「ビジネストップ」を結ぶセキュリティストーリー

シフトレフト:
アプリケーション・ライフサイクル全体において運用効率をアップさせる思想
(リスクとコストのコントロール)

「シフトレフト (Shift Left)！」

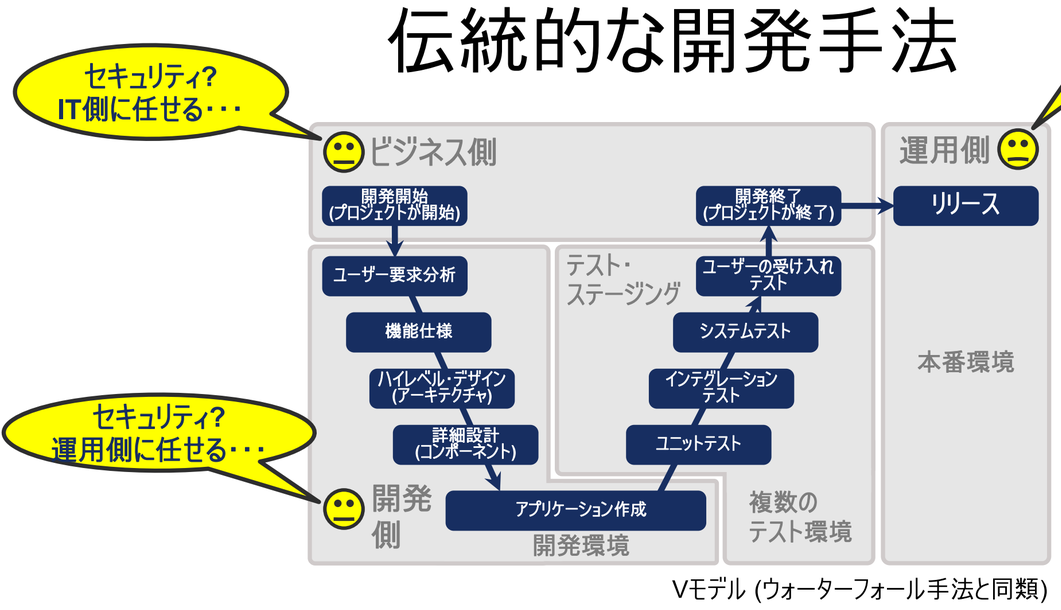
欠陥早期発見と訂正はコストとリスクを抑える作戦！
アプリケーションセキュリティにおいても有利なセキュリティ対策！

アプリケーション・ライフサイクル全体

リスクとコスト:
時間が経つとセキュリティリスクと欠陥の訂正コストが高くなる

トップダウンが必要:
組織内のトップ経営層は「シフトレフト」、「設計によるセキュリティ」と「DevSecOps」に関する現場の状況を理解する必要がある

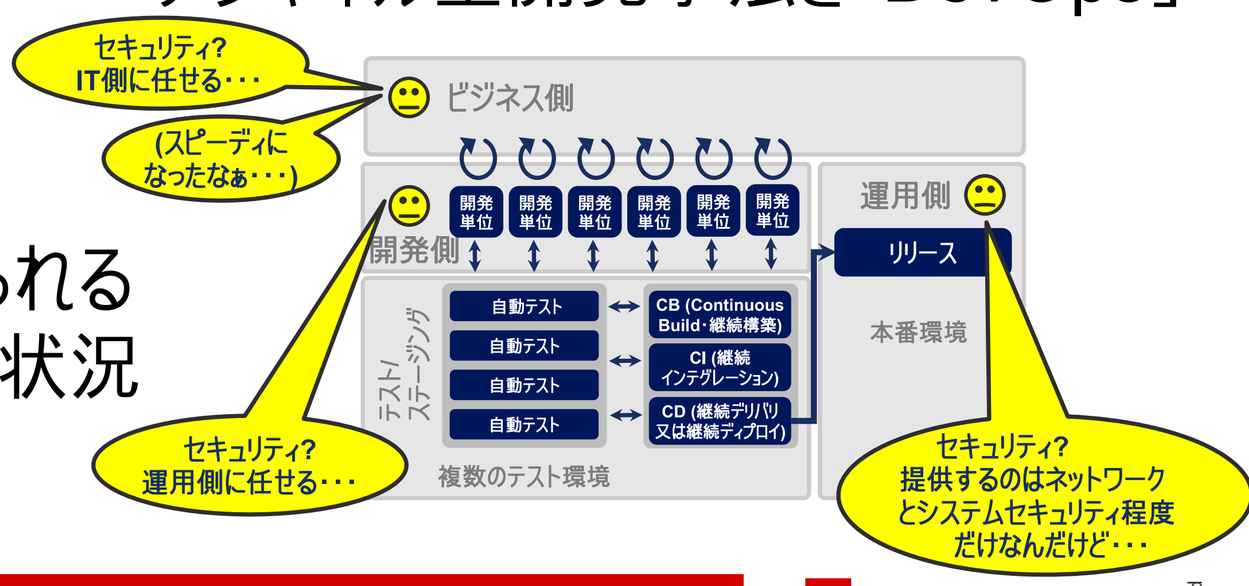
伝統的な開発手法



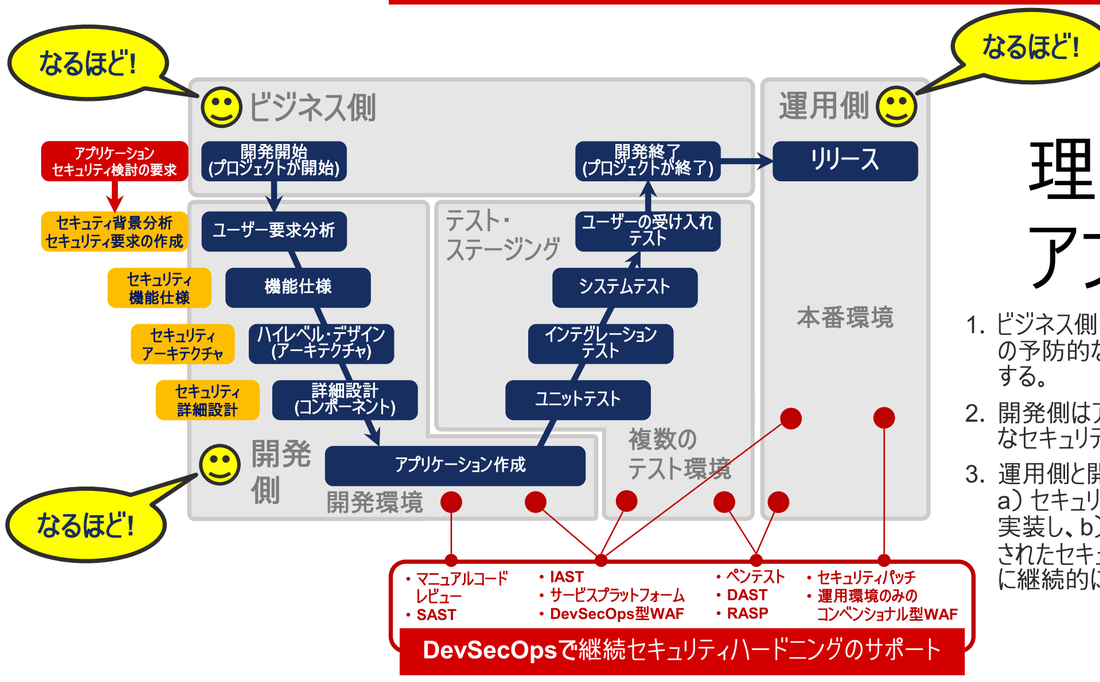
Vモデル (ウォーターフォール手法と同類)

よく見られる現場の状況

アジャイル型開発手法と「DevOps」

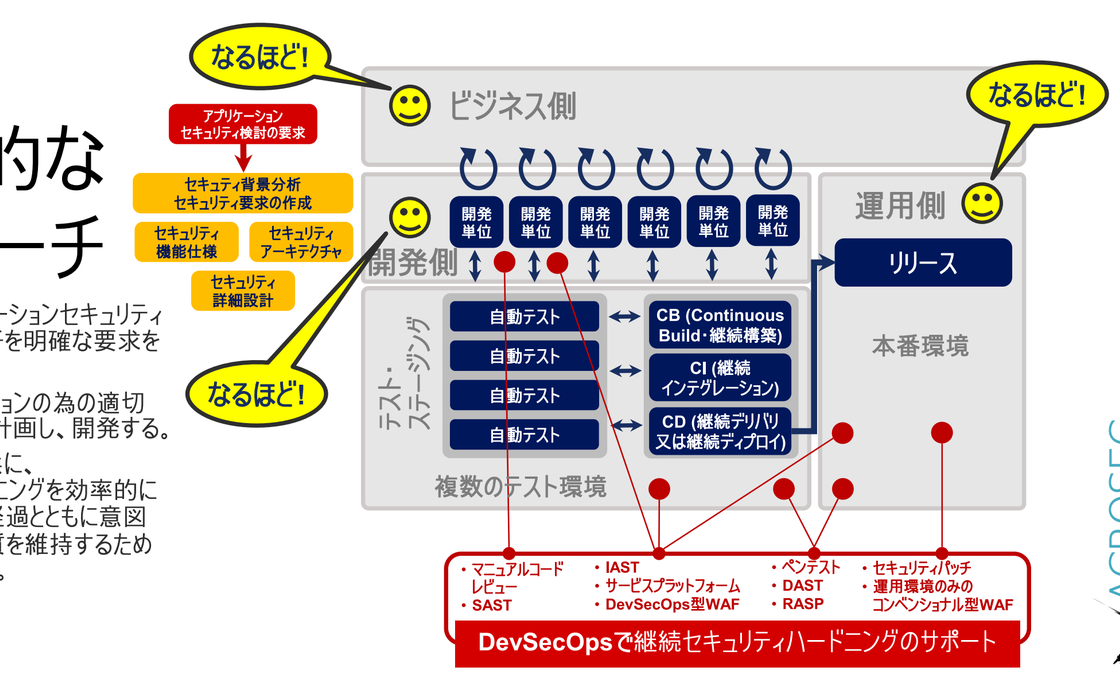


「Security by Design」&「DevSecOps」の導入



理想的なアプローチ

1. ビジネス側はアプリケーションセキュリティの予防的なアプローチを明確な要求をする。
2. 開発側はアプリケーションの為の適切なセキュリティ設計を計画し、開発する。
3. 運用側と開発側は共に、a) セキュリティハードニングを効率的に実装し、b) 時間の経過とともに意図されたセキュリティ品質を維持するために継続的に協力する。



ACROSEC
株式会社 アクロセック
https://www.acrosec.jp