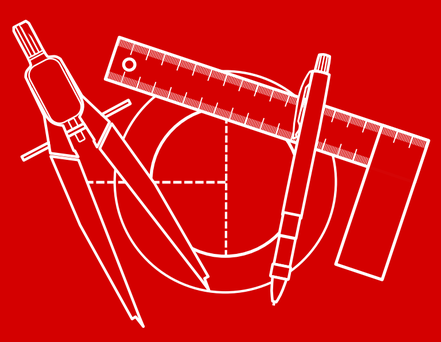
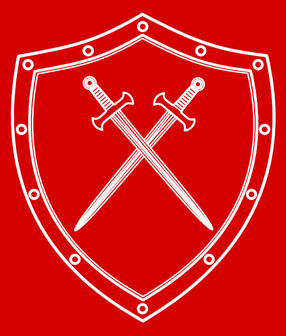
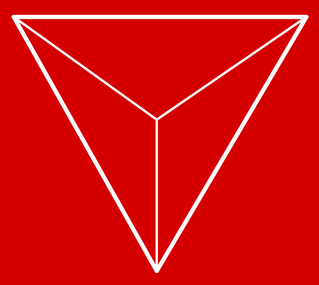
数多くの攻撃はインフラストラクチャセキュリティソリューションが有効でないアプリケーション層で行われる。しかしながら
アプリケーション開発の段階で設計によるセキュリティ(Security by Design)とハードニングはまだ一般的ではない。それを変えよう！



アプリケーションセキュリティ維新の三傑：「シフトレフト」



「Security by Design」



「DevSecOps」継続的なハードニング

「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テストの強化で運用効率をアップさせる発想(リスクとコストのコントロール)

「シフトレフト（Shift Left）！」

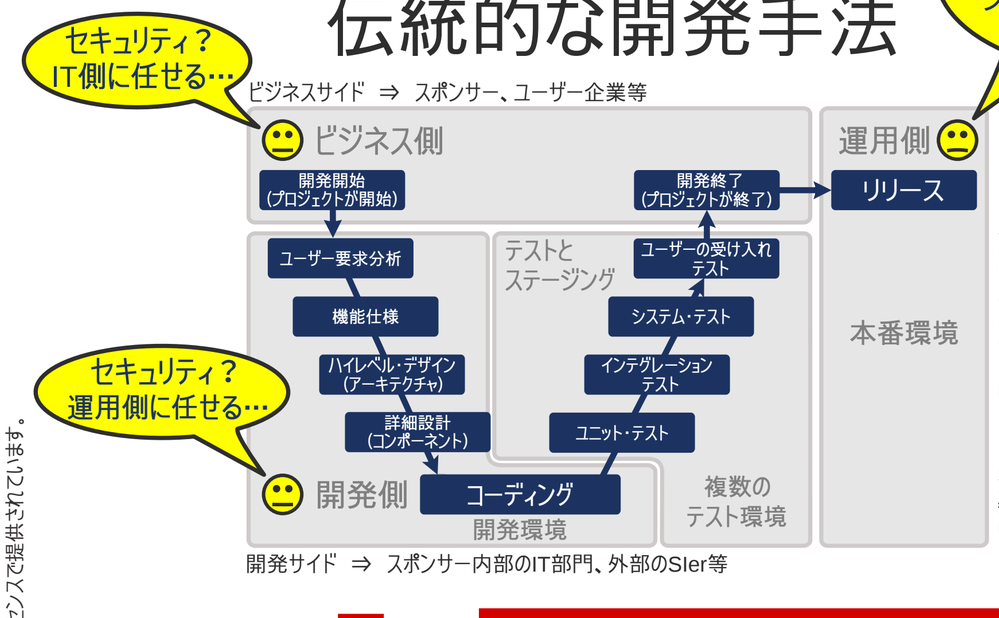
欠陥の早期発見と修正はコストとリスクを抑える作戦！
品質改善や安全管理のように有利なアプローチ

トップダウンサポートが必須：
経営トップの強力なサポートがなければ、効率的なアプリケーション・セキュリティは不可能！

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修正コストが高くなる

経営者サイドの役割：
組織内の経営者は「Shift Left」、「Security by Design」と「DevSecOps」に関する現場の状況を理解する必要がある！

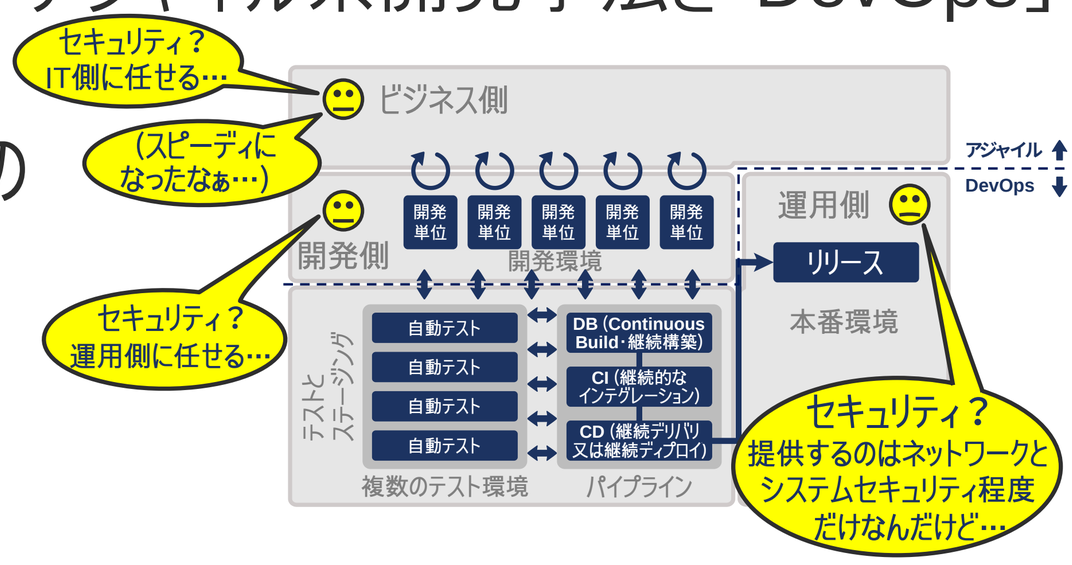
伝統的な開発手法



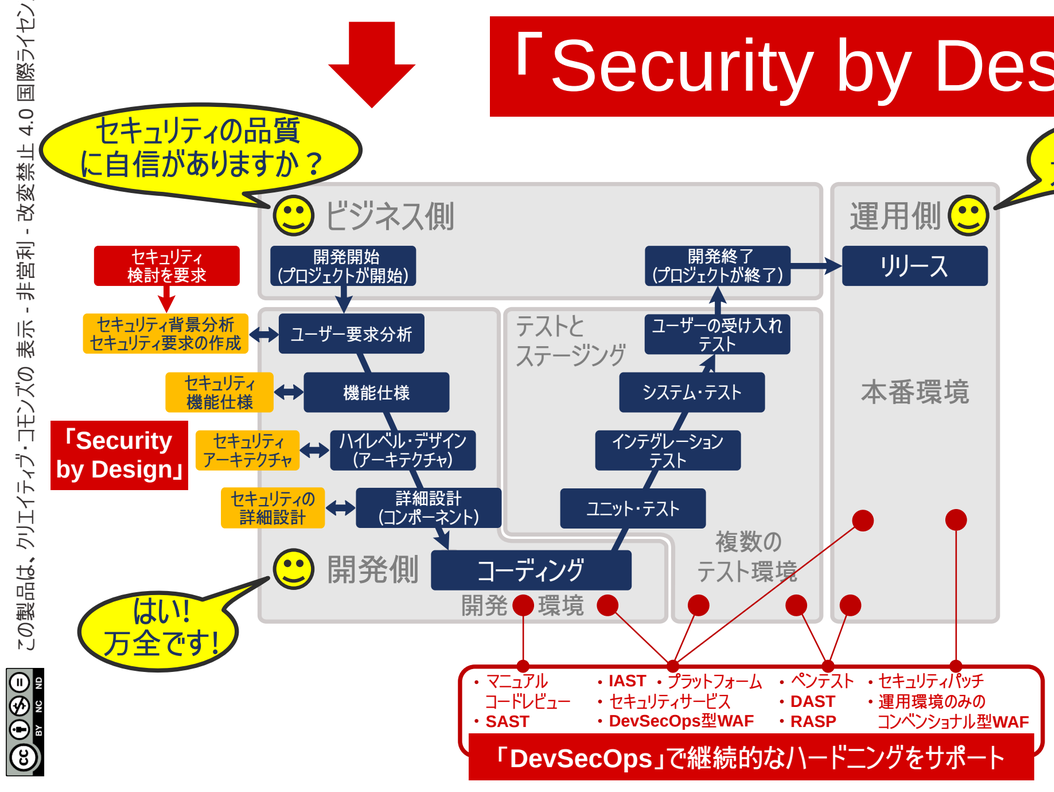
VモデルVモデル(ウォーターフォール手法と同類)

IT現場の悲劇
(よく見られる現場の状況)

アジャイル系開発手法と「DevOps」

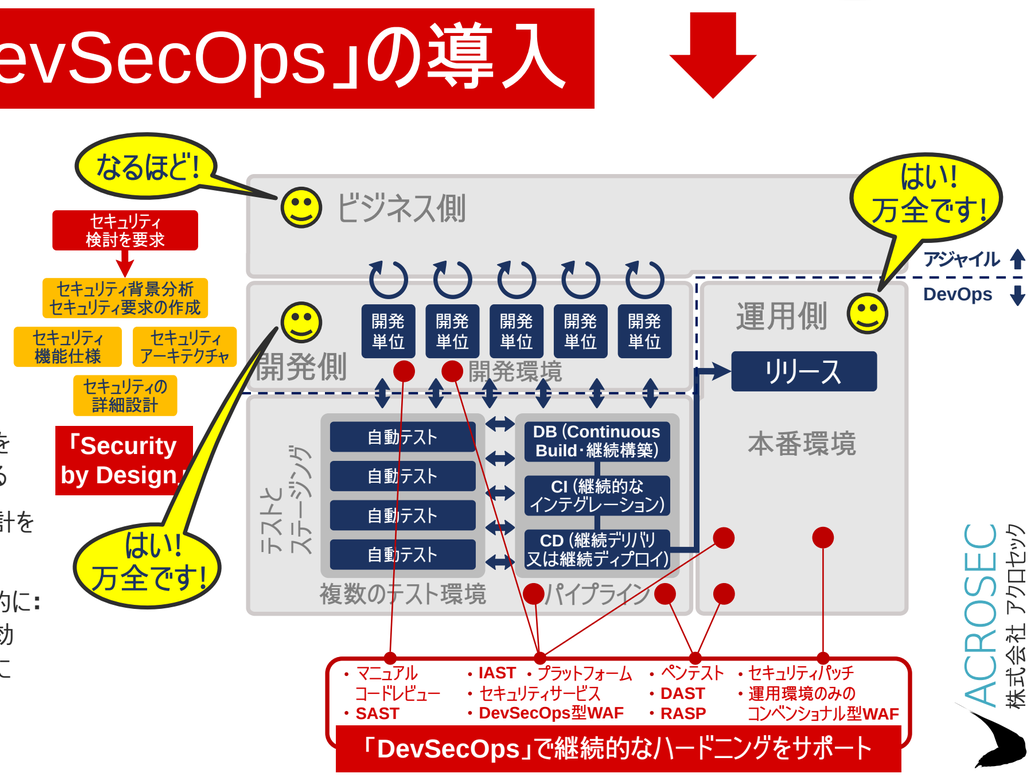


「Security by Design」＆「DevSecOps」の導入



理想的なアプローチ

1. ビジネス側は明確にセキュリティを要求し、適切な予算を提示する
2. 開発側は適切なセキュリティ設計を行い、製品を開発する
3. 運用側と開発側はともに継続的に：
   a) セキュリティハードニングを実効
   b) セキュリティ品質維持のために協力する



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