ソフトウェア・セキュリティに科学的アプローチを適用

ソフトウェア環境が刻々と変化する中、　　にも変化が求められます。

- 開発スピードの上昇
- 自動化によって駆動されるアプリケーション・ライフサイクル管理プロセス
- エンジニアリング主導のソフトウェア・セキュリティ対策
- コンテナ、マイクロサービス、仮想環境へのシフト
- マルチクラウド・デプロイメント戦略の競合
- 「Everything as Code」（あらゆるものをコード化）
- 新しいアプリケーション・アーキテクチャ

概要

ソフトウェア・セキュリティの変化がアジャイル、CI/CD、DevOps といったエンジニアリング・チームの新しい取り組みから生まれているにせよ、中央のソフトウェア・セキュリティ・グループ（SSG）からトップダウン式に発生しているにせよ、リスク管理を成功させるにはソフトウェア・セキュリティ・イニシアティブ（SSI）の成熟度を高めることが鍵となります。しかし自社の SSI の現状を可視化するデータがなければ、改善への戦略を立てることも SSI の改革に優先順位を付けることもできません。

こうした問題を解決するのが、セキュア開発成熟度モデル（BSIMM）です。BSIMM はこれまで 10 年間にわたる SSI の調査結果を独自の業界モデルとしてまとめたもので、SSI を測定する唯一の基準として利用されています。BSIMM はさまざまな組織で実施されているアクティビティを定量化し、これら組織にどのような共通点と相違点があるのかを記述します。BSIMM スコアカードは、SSI の現状を診断し、目標とのギャップを見つけ、今後の改革の優先順位を付け、リソースをどの部分にどれだけ投入すれば即座の改善が見込めるかを判断する上での材料となります。

　　を使ってできること

現実のデータに即してソフトウェア・セキュリティ・イニシアティブ（　　）を開始する。

まだ SSI を実施し　　BSIMM を利用することで、企業の業種や規模、デプロイメント・モデル、コンプライアンス要件を問わず、成功を収めている SSI が共通して実施している中心的アクティビティを知ることができます。

. 同じ業界の企業と自社の間で　　を比較する。

BSIMM は、自社の SSI の広がりと深さを繰り返し測定できる唯一にして最高の方法です。SSI を開始したら、BSIMM を利用することで SSI の改善を毎年継続的に測定できます。また、自社の SSI がどれだけ効果を上げているかを幹部チームや取締役会に示すための具体的な詳細情報も BSIMM によって得られます。