SYNOPSYS®

セキュア開発成熟度モデル
（BSIMM）

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、SSI 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。

BSIMM を使ってできること

1. 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（SSI）を開始する。

まだ SSI を実施していない場合、早急に開始する必要があります。SSI を開始したら、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。

2. 同じ業界の企業と自社の間で SSI を比較する。

BSIMM は、自社の SSI を測定してさまざまな業界の企業との間で結果を比較できる現在唯一の評価ツールです。目標が明確になれば、現在地から目標地点までの距離を容易に把握できます。

3. 繰り返し測定して SSI の成長を追跡する。

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。

4. 成熟度の高い SSI から得られた教訓を自社の SSI 改善に活かす。

BSIMM には成熟度の高い組織が現在実施している実証済みアクティビティが掲載されており、SSI を構築および改善していく上で何が効果的なのかを知ることができます。自社の SSI の診断結果、BSIMM のアクティビティ、自社の目標に基づいて、真の改善に向けた戦略と優先度を設定できます。

5. 同じ問題に直面している他のプロフェッショナルとの交流を図る。

BSIMM の調査結果以外にも、BSIMM コミュニティ専用のコンテンツとしてニュースレター、特別ウェビナー、年次カンファレンス（アメリカ、イギリス）、RSA Conference の交流イベント、活発なオンライン・コミュニティにアクセスできます。

カスタマイズしたレポートをご提供

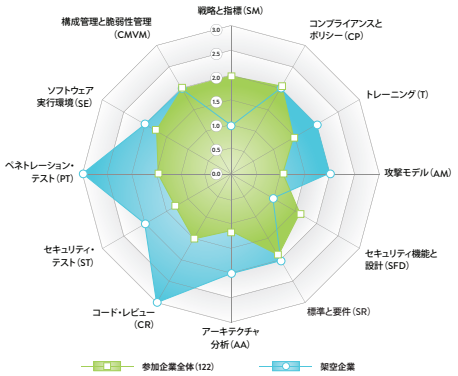
BSIMM の診断を受けると、自社の SSI の優れた部分と改善の余地がある部分を指摘した詳細なレポートを受け取ることができます。また、幹部や取締役会への報告資料として、以下のものも利用できます。

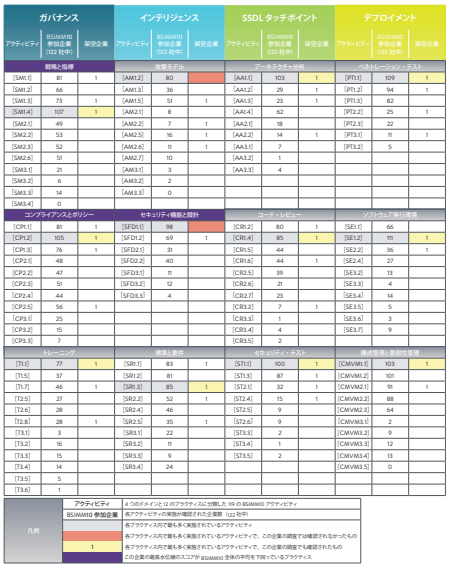
カスタマイズしたレーダーチャート。他社と比較して進んでいる部分、遅れている部分を一目で把握できます。BSIMM を測定ツールとして使用する段階から SSI 立案ツールとして使用する段階へ移行すると、これらの結果を客観的なフィードバックとして利用して進捗状況を追跡できます。

BSIMM スコアカード。他社の SSI と比較して、自社の SSI の現状を捉えることができます。これを利用して、自社の SSI 全体の経年変化、個々の事業部門、ビジネス・パートナー、および取引先ベンダーを検討できます。

価値を引き出す

「2008 年以降、BSIMM は世界最先端のセキュリティ・チームを含む多種多様な組織がどのようにソフトウェア・セキュリティ戦略を実施しているのかを理解するための効果的なツールとして利用されてきました。最新の BSIMM データからは、リリース・サイクルの短縮、自動化の進行、ソフトウェア定義インフラストラクチャなど、開発およびデプロイメントの手法の最新動向に合わせて多くの組織がアプローチを適合させていることがうかがえます」—MassMutual 社エンタープライズ情報リスク管理責任者、Jim Routh 氏





シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質のソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や欠陥を迅速に見つけて修正します。業界をリードするツール、サービス、専門知識を組み合わせることで、シノプシスは DevSecOps におけるセキュリティと品質を最大化し、ソフトウェア開発のライフサイクル全体にわたって組織を支援します。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス

TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software