SYNOPSYS®

Black Duck 監査

**ソフトウェアに潜む
ライセンス、セキュリティ、
品質に関するリスクを
迅速に洗い出す専門
サービスをオンデマンドで**

概要

Black Duck 監査は、M&A および社内コンプライアンス向けのオープンソース・デューデリジェンス・ソリューションとして 15 年以上にわたり業界屈指の高い信頼を得ています。

コードの中身は、知らなかったで済まされることではありません。アプリケーションに含まれるオープンソースに見落としがあると、ライセンス違反が生じて高い代償を払うことになります。また、プロプライエタリ、オープンソース、サードパーティを問わず、ソフトウェアに潜むセキュリティの欠陥が自社のソフトウェア資産の価値に重大な悪影響を与える可能性もあります。

Black Duck 監査は、以下のサービスをご提供します。

- ライセンスが不明なオープンソース・ソフトウェアおよびサードパーティ製コードを洗い出し、訴訟リスクを軽減します。
- オープンソースのライセンス不一致やセキュリティ脆弱性をはじめ、ソフトウェア資産の価値に影響するさまざまなリスクを検出します。
- ソフトウェア・セキュリティ脆弱性を特定およびテストし、プロプライエタリ・ソフトウェアに潜むセキュリティ・ギャップを明らかにします。
- ソフトウェア品質、およびソフトウェア開発の管理が全体的に良好かどうかを可視化します。

Black Duck 監査は、買収先企業または自社のソフトウェアに潜む多様なリスクを迅速に診断できるよう、必要な情報をご提供します。オープンソースのライセンス取得状況、およびアプリケーション・セキュリティとコード品質に関するリスクの全体像を把握することで、情報に基づいた確かな意思決定が可能になります。

「買収手続きを進める際には、Black Duck 監査の多岐にわたるサービスを利用しています。必要な第三者監査をワンストップでカバーできるので助かります。おかげで、新しいテクノロジを自社のポートフォリオに加える前のリスク確認の手間が大いに軽減されました。」

—PointClickCare 社

オープンソース / サードパーティ・ソフトウェア監査

オープンソース / サードパーティ・コード監査

コードベースに含まれるすべてのオープンソース・コンポーネントを完全な部品表として提示し、それぞれのライセンス取得状況 / 不一致の解析結果を示します。

オープンソース・リスク評価

既知のセキュリティ脆弱性やメンテナンス・リスクなど、コードベースに内在するオープンソースのリスクを包括的に可視化します。調査および修正の優先度を決定するハイレベルの行動計画として役立ちます。

Web サービスと API リスク監査

アプリケーションで使用している外部 Web サービスの一覧を作成し、法的リスクやデータ・プライバシー・リスクの可能性を指摘します。ガバナンス、データ・プライバシー、品質の 3 つの主要なカテゴリごとに、Web サービスのリスクをすばやく評価できます。

アプリケーション・セキュリティ監査

ペネトレーション・テスト監査

実際に動作中のアプリケーションに侵入を試みて、ソフトウェアのセキュリティに関する堅牢性を評価します。セキュリティ・コントロール（WAF、入力値検証など）を回避し、ビジネス・ロジックおよびユーザー認可の誤用を試みるリスク分析により、ハッカーがどのような方法で不正にアクセスして損害を与えるかを明らかにします。

静的アプリケーション・セキュリティ・テスト（SAST）監査

ツールによる自動スキャンとソースコード・レビューを組み合わせることにより、SQL インジェクションやクロスサイトスクリプティング、バッファ・オーバーフローなどの OWASP Top 10 を含め、重大なソフトウェア・セキュリティ脆弱性を検出します。

セキュリティ・コントロール・デザイン分析

パスワードの保管、アイデンティティ / アクセス管理、暗号の使用など主要なセキュリティ・コントロールのデザインを業界のベスト・プラクティスに照らし合わせて評価し、これらに設定のミス、弱点、誤用、不足がないかどうかをチェックします。アプリケーション設計におけるセキュリティ・コントロールに関するシステム不具合を見つけるもので、アプリケーションやコードに対するテストや解析は行いません。

コード品質監査

定量的コード品質監査

静的解析ツールとマニュアル・コード・レビューを併用し、コード品質を分析します。また、業界ベンチマークとの比較により、プロプライエタリ・コードの品質、再利用性、拡張性、保守性を診断します。コード品質改善のための提案も示します。

定性的コード品質監査

ソフトウェア開発ライフサイクル（SDLC）のプロセスとプラクティスを分析します。主要な担当者への聞き取り調査を通じ、これらプロセスの品質と成熟度を診断します。コストを削減しながらコード品質を高めるための提案も示します。

暗号監査

プロプライエタリ、オープンソース、およびその他のサードパーティ・ソフトウェア・コンポーネントで使用されている暗号機能を特定します。これにより、輸出規制への法令遵守に伴う政府機関への情報開示が容易になり、輸出制限を回避できます。また、製品に含まれる暗号コードが社内のセキュリティ要件を満たしているかどうかも確認できます。

任せて安心の専門サービス

リスクの大きい M&A の世界では、スピードと正確性が何より重視されます。買収先企業の評価額に占めるソフトウェア資産の割合が大きい場合は特に、高度なツールを駆使した経験豊富な専門監査サービスにお任せいただくことをお勧めします。

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

SYNOPSYS®
Silicon to Software™

©2019 Synopsys, Inc. All rights reserved. Synopsys は Synopsys, Inc. の米国およびその他の国における登録商標です。
Synopsys の商標に関しては、こちらをご覧ください。http://www.synopsys.com/copyright.html その他の会社名および商品名は各社の商標または登録商標です。
04/03/19.ds-bd-odsig.