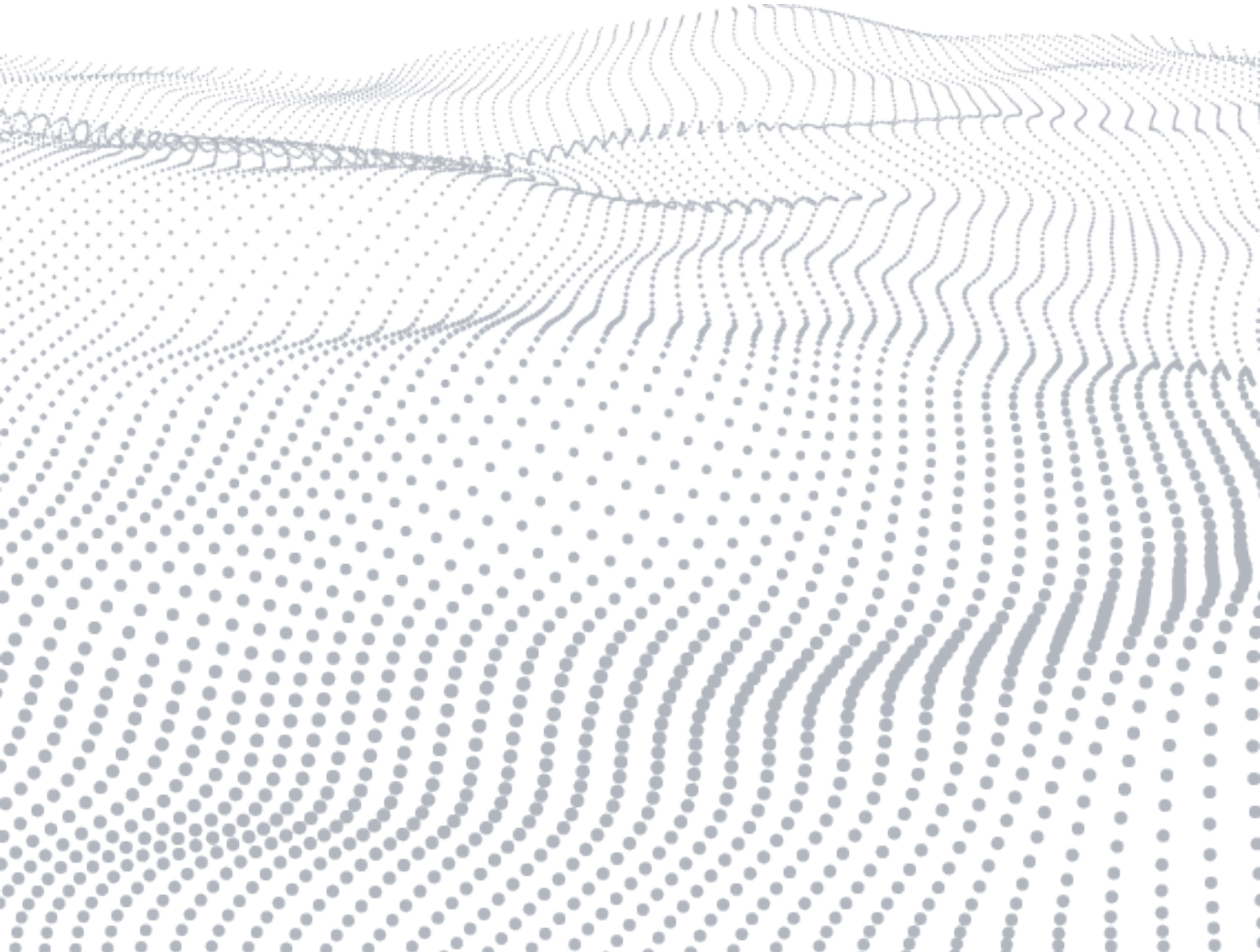
BLACKDUCK®

ホワイトペーパー

セキュリティを問う―金融サービス業界における オープンソース・セキュリティの現状



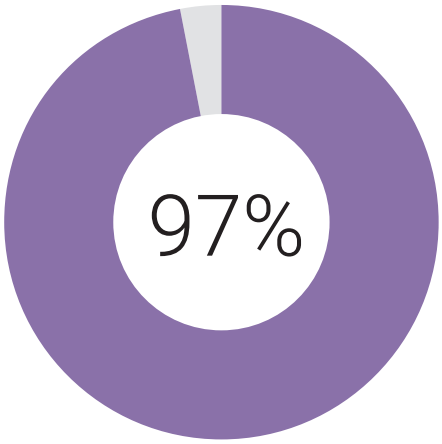
ブラック・ダック サイバーセキュリティ・リサーチセンター（CyRC）は、企業がセキュアで高品質なソフトウェアを開発、利用できるようにセキュリティ・アドバイザリおよびリサーチを発行することを設立目的としています。CyRC は毎年、オープンソース・セキュリティの現状を詳細に分析しており、その結果をフィードバックすることによって、幅広い業界でのセキュリティに関する意思決定の改善を図っています。

最新の年次レポートを作成するに当たり、CyRC は 17 の業種を対象に 1,500 を超えるコードベースを分析しました。そこから見えてくるのは、過去のレポートで繰り返し指摘してきたこと、すなわちすべての業種のほとんどすべてのアプリケーションでオープンソース・ライブラリの利用が拡大しているという事実です。しかしオープンソースの隆盛を語る上で最も重要なのは、オープンソースの管理が不適切または不十分であるとリスクが生じるという点です。

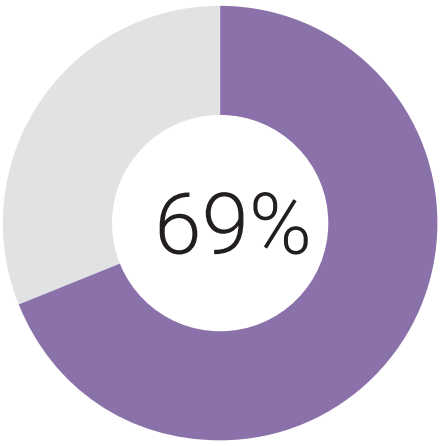
この問題は、金融サービス業界（FSI）で使用されるアプリケーションでは特に大きな意味を持ちます。FSI アプリケーションには機微なデータの管理と利用が委ねられるため、アプリケーション・セキュリティ（AppSec）に対する包括的なアプローチが求められます。本稿は、金融サービス業界に関する重要な調査結果を紹介することを目的に、「2021 年オープンソース・セキュリティ & リスク分析レポート（OSSRA）」から FSI 関連の内容を抜き出して要約したものです。これらの調査結果を詳しく見ていくことにより、FSI アプリケーションのセキュリティ担当者に対し、どのような点に重点的に取り組むべきかを示していきます。

金融サービス業界におけるオープンソース脆弱性に関する調査結果

オープンソースは業界の垣根を越えて爆発的に利用が拡大しています。今回の調査でスキャンした 162 の金融サービス /FinTech アプリケーションのうち、97% に何らかのオープンソースが含まれていました。また、FSI アプリケーションの全コードベースに占めるオープンソースの割合は 69% でした。



今回の調査でスキャンした
FinTech アプリケーションのうち、
オープンソースを含むものの割合



全コードベースに占める
オープンソースの割合

懸念されるのは、スキャンした FSI コードベースのうち、62% にオープンソース脆弱性が見つかったことです。これほど多くの脆弱性が存在しているということは、間違いなく金融サービス業界にはオープンソースのセキュリティについて考え直し、是正策をとる必要があることを示唆しています。調査した全業種の中で、FSI アプリケーションは脆弱性の総数が 3 番目に多いという結果が出ています。

この年次レポートで毎年指摘しているように、調査で見つかった脆弱性のほとんどは容易に修正が可能であるか、ずいぶん前から既知の修正方法が存在しているかのどちらかです。今年も例外ではありません。今回の調査でも、CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）の上位 10 の脆弱性がすべて検出されています。CVE は、一般向けにリリースされているソフトウェアで非常によく見られる脆弱性に一意に付けられた識別子で、CVE データベースに情報が登録されており、開発者が容易にアクセスできるリポジトリを提供しています。今回の調査で、最も一般的な上位 10 の脆弱性がすべて検出されたということは、単純でよく知られた脆弱性さえも修正できていないという事実を示しています。

既知の脆弱性が修正されずに残っていること、そして FSI アプリケーションで実に多くの脆弱性が見つかったことは、オープンソースの管理がいかに難しいかを物語っています。開発チームが特に難しいと感じているのが、オープンソース・セキュリティ・リスクに特有の動的な性質への対処です。金融サービス業界では機微なデータを扱うため、このことは特に深刻な問題となります。

毎年、何千ものオープンソース脆弱性が新たに報告されています。商用ソフトウェアとは異なり、オープンソースの場合は特定のベンダーがこれらの脆弱性についてユーザーに情報を提供したり、セキュリティ・チームに最新のセキュリティ・アップデートの適用を促したりすることはありません。

オープンソースの利用が拡大している中で、オープンソースの脆弱性およびエクスプロイトも広く報告されており、脆弱性が発見されたその日にエクスプロイトが報告されることも少なくありません。これでは、ハッカーが機先を制して何千ものアプリケーションや Web サイトに攻撃を加える可能性があります。Heartbleed や Equifax 社の情報漏洩が示すように、わずか 1 つのオープンソース脆弱性だけでも、ハッカーは数千ものアプリケーションへの鍵を手にすることができます。

脆弱性が公開されたその瞬間から、企業は無防備な状態に置かれます。セキュリティ・チームにとって、攻撃を受ける前にアプリケーションに含まれるオープンソースの脆弱性を特定して修正することが重要となります。ソフトウェア・コンポジション解析（SCA）ツールのようなソリューションは、使用中のオープンソースの完全な可視化と、新たに発見された脆弱性に関するタイムリーな報告に役立ちます。オープンソースの使用は企業の全体的なリスクに影響を与えるため、ビジネスへの悪影響を軽減するには、オープンソースの管理に対して包括的かつ戦術的なアプローチをとる必要があります。

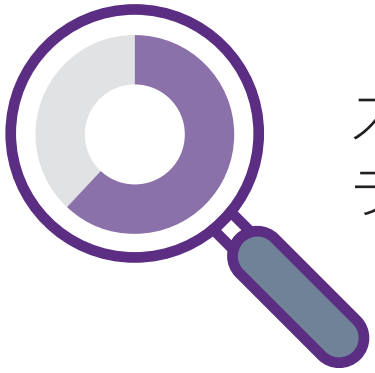
ライセンス条件の競合に関する調査結果

「オープンソース・セキュリティ & リスク分析レポート」では、オープンソースのライセンス管理に対する意識向上の必要性を毎年指摘しています。ライセンスのリスク、そしてそれが企業の全体的なリスク状況にどのような影響を与えるかを理解することは非常に重要な点です。最も寛容なオープンソース・ライセンスでさえ、ソフトウェアの使用と引き換えにユーザーが負う義務が規定されています。オープンソース・ライセンスに関する訴訟が増加傾向にある中、ライセンスの懸念には特別な注意を払う必要があります。ライセンスに違反すると、訴訟による巨額の費用が発生したり、価値ある知的財産権が危険にさらされたりする可能性があるため、企業はこうしたライセンス違反を特定できるツールやソリューションを活用し、オープンソースの追跡と管理に努める必要があります。今回の調査では、スキャンした FSI コードベースの 62% にライセンス条件の競合が見つかっています。

もちろん、オープンソースを利用する企業はライセンス管理の必要性を理解していますが、今回の調査結果を見ると、ライセンス条件の競合に適切に対処できている企業はほとんどないことを示しています。オープンソース・コンポーネントに適用されるオープンソース・ライセンスの種類は多岐にわたり、往々にしてこれらライセンスの内容は非常に複雑で難解です。特に、一部のライセンスは技術的で複雑な条件が設定されており、十分に注意しないとコンプライアンスの問題が生じます。

オープンソース・ライセンスの最も大きな課題は、これらのライセンスが主観的なものであるという点です。その解釈は、ライセンスを受けたソフトウェアを技術的にどのように使用するかによっても変わってきます。ライセンスがどのような法的リスクをもたらすのかを判断しづらいのは、ここに理由があります。しかもその解釈は、法律の知識がほとんどない開発者に委ねられているのが現状です。

したがって、ライセンスを管理するには、法的コンプライアンスに対してどのようなリスクがあるかに基づいて、ライセンスを大まかに分類する必要があります。これは非常に骨の折れる作業ですが、SCA ツールには競合や問題の箇所を容易に特定し、主要なライセンス条件の競合に優先順位を付ける機能があり、容易に自動化できます。



スキャンした FSI コードベースの 62% にライセンス条件の競合が見つかりました

運用面のリスクに関する調査結果

オープンソースを常に最新の状態に維持するために積極的な活動を続けることは、多くの企業のセキュリティ・チームにとって運用面での大きな負担となっています。Black Duck® 監査サービスが 2020 年に調査した 1,500 以上のコードベースのうち、過去 2 年間に開発活動実績のなかったオープンソース・プロジェクトを依存ファイルとして少なくとも 1 つ含んでいるものが 91% もありました。つまり、コードベースの 91% は、過去 2 年の間に一度も機能のアップグレード、コードの改良、必要なセキュリティ不具合の修正が行われていないことを意味しています。

金融サービス業界に限って言えば、スキャンした 162 のコードベースのうち、過去 2 年間に開発活動実績がなかったオープンソース・コンポーネントを含むものが 10% ありました。そしてそのすべてにおいて、4 年以上前の旧バージョンのオープンソース・コンポーネントが検出されました。10% という数字は特に高いわけではありませんが、これほど長期間にわたって放置されたコンポーネントを使い続けているのは、好ましいことではありません。

スキャンした 162 の FSI コードベースのうち、過去 2 年間に開発活動実績がなかったオープンソースを含むものが 10% あり、そのすべてにおいて 4 年以上前の旧バージョンのオープンソースが検出されました

オープンソースが人気を博している理由の 1 つは、オープンソースが多くの人によって支えられていること、つまり有志によるコミュニティが継続的にコードをアップデートして脆弱性に対処しているということにあります。しかしそれが無保証で行われていることが、このモデルの問題点です。コミュニティがオープンソース・プロジェクトを効果的、効率的に最新の状態に維持できているのか、コードを適切にメンテナンスできるだけのスキルとリソースがコミュニティにあるのか、といったことを確認するすべがありません。

金融サービス企業がこの問題を解決するには、オープンソース・コードを特定して効果的に管理できるようにするソリューションを導入する必要があります。自社のコードに含まれるコンポーネントを追跡するのに最も適しているのが、SCA ツールです。オープンソース・コードを適切に追跡していないと、セキュリティと運用の面で悪夢のシナリオが起こりうる可能性があります。セキュリティ面では、パッチ未適用の脆弱性が悪用されるのを防ぐことが困難になります。運用面では、自社のアプリケーションの開発に使用しているオープンソース・プロジェクトが今後も存続するかどうかの確証を持つことが難しくなります。

強力な SCA ツールがあれば、脆弱性や最新でないコンポーネントを容易に特定できます。また、部品表（BOM）を生成してアプリケーション内のコンポーネントを特定できるのも SCA ツールの便利な機能です。なぜなら、存在に気付いていないものは管理や保護のしようがないためです。

まとめ

オープンソースの利用にはリスクが伴います。それは、アプリケーションに含まれるオープンソースの数や種類を容易に特定できるツールやプラクティスを企業が導入していないのが主な理由です。自社のすべてのアプリケーションに含まれるオープンソース、および関連するライセンス義務および脆弱性を完全に可視化できない限り、企業は訴訟やセキュリティ攻撃、さらには自社ソフトウェアの所有権を危険にさらす可能性など、大きなリスクを抱えることになります。

今回のオープンソース分析の結果から言えるのは、オープンソース管理は業界を問わずすべての企業にとって大きな課題であり続けているという事実です。これは、過去のオープンソース分析でも毎年指摘している点でもあります。

また、オープンソースのセキュリティ・リスクを容易に軽減できるセキュリティ・プラクティスやソリューションが存在することも、毎年指摘しているとおりです。強力なオープンソース・セキュリティ・プログラムを導入することへセキュリティ・チームのリソースと関心を集中させることで、オープンソース・コミュニティに依存していただけでは決して得られないセキュリティ面での安心が得られます。適切なソリューションとプラクティスを優先的に導入すれば、ライセンス条件の競合を見落とすことによって生じる潜在的な脅威も容易に回避できます。

ブラック・ダックの Black Duck SCA のようなソリューションを利用すると、開発、セキュリティ、およびリスク管理チームはオープンソース脆弱性、ライセンス条件の競合、および運用上のリスクに関する情報を把握できます。Black Duck のようなツールを活用することにより、チームは情報に裏付けられた行動を起こし、アプリケーション・セキュリティを効果的に高めることができます。

Black Duck SCA の詳細は、ブラック・ダックの Web サイトをご覧いただくか、最近のウェビナーをご視聴ください。

今回の調査結果の全容は、「オープンソース・セキュリティ & リスク分析レポート」をお読みください。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。

詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp