BIZREACH

PRESS RELEASE

2019 年 8 月 27 日
株式会社ビズリーチ

サイバー攻撃が深刻化するなか、IT エンジニアによるシステム開発の生産性向上を目指す

オープンソース脆弱性管理ツール「yamory」をリリース

株式会社ビズリーチ（所在地：東京都渋谷区/代表取締役社長：南 壮一郎）は、オープンソース脆弱性管理ツール「yamory（ヤモリー）」（URL：https://yamory.io）を 2019 年 8 月 27 日にリリースしました。

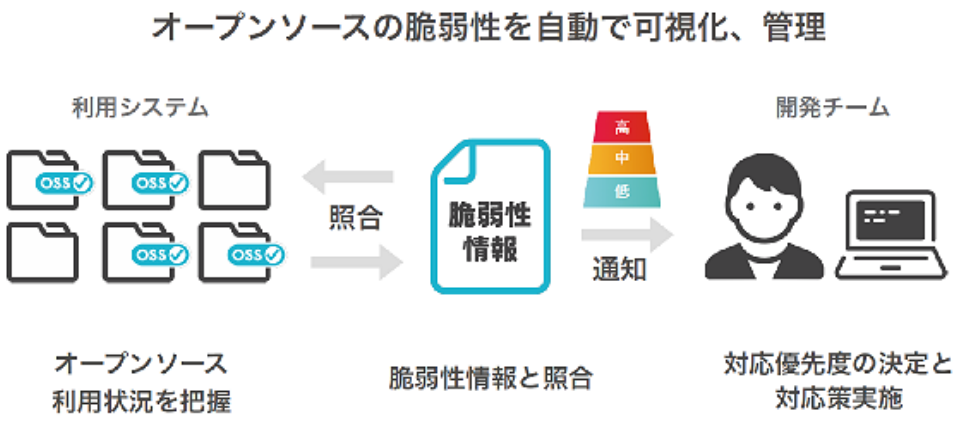
■商用アプリの 96%がオープンソースを利用、そのうち 78%に脆弱性が含まれる（米国調査）

近年、IT の利活用が進み、国内民間企業の IT 市場規模が急拡大するなか、サイバー攻撃の関連通信量が 2018 年までの 10 年間で 21.8 倍に達する (注 1) など、サイバー攻撃が深刻化しています。なかでも、オープンソースの脆弱性（プログラムの不具合や設計上のミスが原因となって発生した欠陥）を突いた攻撃によって個人情報の漏えいなどの大きな被害が続出しています。オープンソースは、ソースコードが公開され、利用者による利用・改変・再配布が可能なソフトウエアです。無料で利用ができる便利なオープンソースの普及により、システムやアプリを生産性高く開発できるようになりました。その結果、米国の調査結果では、2018 年時点で商用アプリの 96% (注 2) においてオープンソースが利用されています。しかし、オープンソースを利用している商用アプリのうち、78%にオープンソースの脆弱性が含まれていると報告されており (注 2)、サイバー攻撃の危険にさらされているのが現状です。

この状況に対し、yamory はオープンソースの脆弱性を管理することで、セキュリティ対策にかかる工数を削減し、IT エンジニアのシステム開発の生産性向上を目指します。

■yamory の機能：オープンソースの脆弱性を自動で可視化し、管理

yamory は、オープンソースの利用状況を自動で把握し、脆弱性の管理・対策ができるサービスです。まず、システムにおいて利用されているオープンソースを抽出し、その利用状況を把握します。同時に、yamory が有する最新の脆弱性情報のデータベース（オープンソースの脆弱性情報と攻撃用コードを収集）と照合し、脆弱性を可視化します。そして、サイバー攻撃の危険度などをもとに、対応優先度を分類（オートトリアージ機能 ※特許出願中）、その対応策と対応優先度を開発チームごとに通知し、それぞれのチームの脆弱性対応の管理を可能にします。それにより、これまでセキュリティ担当者などが手動で行っていた一連の対応を、自動化できます。

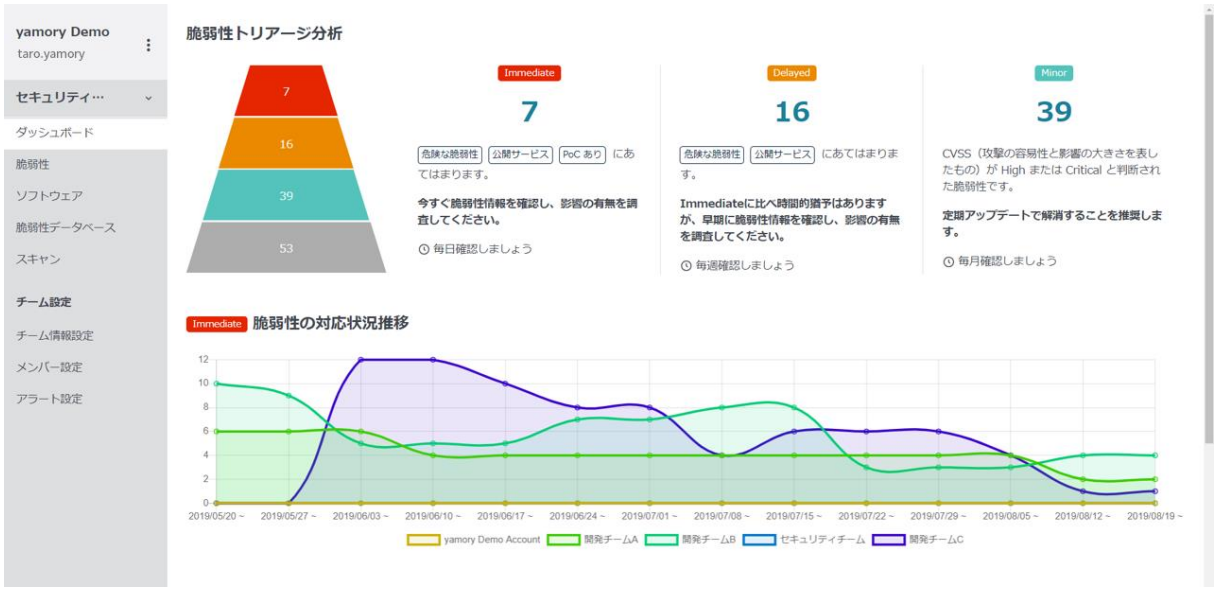


■現状の課題：サイバーセキュリティ対策への意識の低さ、専門人材の不足

日本と海外の企業（従業員 300 名以上）を対象に実施したサイバーセキュリティ投資額の調査によると、「投資額が 5,000 万円以上」と回答した企業は、米国が 70.7%に対し、日本は 31.7%と半分以下にとどまりました (注 3)。また、ウイルス感染・サイバー攻撃が発生した場合の事前の被害額推定の実施状況について、「行っている」という回答をした企業は、米国が 79.3%に対し、日本は 50.9%で (注 3)、日本企業のサイバーセキュリティに対する意識と投資額の低さの実態が浮き彫りとなりました。また、IT 人材の需要が高まり続けるなか、国内の情報セキュリティ人材の不足は年々深刻化しており、その不足数は 2016 年の 13.2 万人から 2020 年には 19.3 万人に増加すると予想されています (注 4)。このようななか、半数以上の企業は、専門部署を設置していないのが現状です (注 3)。多くの企業では、システムの脆弱性管理を手動で行い、高度な知識と膨大な工数を必要としていました。

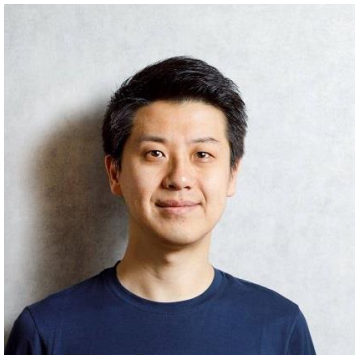
■yamory 利用のメリット：セキュリティ対策の工数を大幅に削減、サイバー攻撃のリスクを軽減

yamory は、セキュリティ担当者の代わりとなり、オープンソースの利用状況の把握、脆弱性などの情報収集と照合、対応の優先順位付け、対応策の通知を自動的に行うため、高度なセキュリティの専門知識がない方でも簡単にオープンソースの脆弱性を管理できます。これにより、セキュリティ対策の工数を大幅に削減します。また、yamory の利用企業はオープンソースの脆弱性対策ができ、サイバー攻撃のリスクを格段に軽減できます。



ユーザーの利用画面：対応優先度の分類と脆弱性の対応状況の推移

株式会社ビズリーチ 取締役 CTO 兼 CPO　竹内 真　コメント



近年、オープンソースの普及に伴い、サイバーリスクが急激に増大し、オープンソースの脆弱性を突いた深刻なサイバー攻撃が続出しています。弊社もさまざまな IT サービスを提供し、オープンソースを利用するなか、オープンソースの脆弱性管理に膨大な工数を要していました。そして、同じ悩みを抱える企業様が多くいることを知り、多くのエンジニアの方の役に立てたらと考え、このたび、yamory をリリースしました。yamory を利用することで、現場のエンジニアの方は膨大なタスクから解放され、サービス開発に集中

できます。yamory は、未来を創るエンジニアが安心してテクノロジーを活かし、生産性高く開発できる世界を目指します。

■yamory の名前の由来

生き物のヤモリに由来しています。ヤモリは、壁や窓、屋根裏など家の隅々まで行くことができ、人間にとっての害虫を食べてくれる、縁起のいい生き物とされています。家を守るとされ、漢字では「守宮」「家守」とも表されます。また、環境により皮膚の色を変幻自在に変える、臨機応変さを持つ存在でもあります。ヤモリのこれらの特徴から、それぞれの状況に合わせて大切なものを守ってくれる存在という思いを込めて、yamory と名付けました。

yamory ロゴ

注 1）国立研究開発法人情報通信研究機構「NICTER 観測レポート 2018」（2019 年 2 月）
注 2）Synopsys Center for Open Source Research and Innovation “2018 Open Source Security and Risk Analysis”
注 3）独立行政法人情報処理推進機構「企業の CISO や CSIRT に関する実態調査 2017－調査報告書－」（2017 年 4 月）
注 4）総務省「我が国のサイバーセキュリティ人材の現状について」（2018 年 12 月）

■株式会社ビズリーチについて https://www.bizreach.co.jp/

「インターネットの力で、世の中の選択肢と可能性を広げていく」をミッションとし、2009 年 4 月より、社会や産業の未来を支えるさまざまなインターネットサービスを運営。東京本社のほか、大阪、名古屋、福岡に拠点を持つ。即戦力人材と企業をつなぐ転職サイト「ビズリーチ」や、挑戦する 20 代の転職サイト「キャリトレ」、人材活用クラウド「HRMOS（ハーモス）」、求人検索エンジン「スタンバイ」、事業承継 M&A プラットフォーム「ビズリーチ・サクシード」などを展開。