PRESS RELEASE

2021年8月26日
Visionalグループ

国内初、脆弱性とオープンソースライセンス違反の一元管理を実現
脆弱性管理クラウド「yamory」、
OS、ミドルウェア・開発言語への対応と、ライセンス違反検知を開始

Visionalグループのビジョナル・インキュベーション株式会社（所在地：東京都渋谷区/代表取締役社長：村田 聡）が運営する脆弱性管理クラウド「yamory（ヤモリー）」（https://yamory.io/）は、ITシステムのOS（オペレーティングシステム）とミドルウェア・開発言語の脆弱性を自動で検知し管理・対策ができる機能、およびオープンソースのライセンス情報を可視化しライセンス違反を検知する機能を、2021年8月26日（木）に提供開始します。

yamoryは、ITシステムに潜む脆弱性を自動で検知し、管理・対策ができるクラウドサービスです。これまでは、アプリケーション内で利用されているライブラリ・フレームワークにおける脆弱性を対象としてきました。新機能により、ITシステムの脆弱性とオープンソースのライセンス違反を一元管理できる国内初（※1）のサービスとなります。脆弱性の管理・対策をすることでサイバー攻撃から身を守り、ITシステムからの情報漏洩とオープンソースライセンス違反による法的リスクの軽減を実現します。

■DXが加速するなか、高まるサイバー攻撃リスク

近年のテクノロジーの急速な進化にコロナ禍の影響も重なり、さまざまな場面でDXが進むなか、ITの利活用が加速している一方で、サイバー攻撃は深刻化しています。2020年に観測されたサイバー攻撃の関連通信は、2019年の約1.5倍、約10年前の110倍にのぼり（※2）、サイバー攻撃による情報漏洩などのリスクが高まり続けているのが現状です。これらの多くは、既知の脆弱性（すでに公開されている脆弱性情報）を悪用した攻撃（※3）であり、脆弱性情報を事前に把握し、適切な対応をすることで未然に防ぐことが可能です。実際に、サイバー攻撃の85%は、最もよく知られた脆弱性の上位10件を悪用したものであることが分かっています（※4）。

■ITシステムは多様化し、属人的な対応はますます困難に

既知の脆弱性に対するサイバー攻撃のリスクに対して十分な対応ができていない背景には、ITシステムの多様化と管理者による属人的な対応が挙げられます。

新しい技術が次々に生まれ、会社や事業、サービスごとに最適な開発環境が変わり続けているため、ITシステムの多様化が進んでいます。そんななか、開発、運用、セキュリティのそれぞれの担当者が、ITシステムの利用状況を把握したうえで、それらに含まれる脆弱性情報を属人的に収集しているケースが多いため、網羅的に適切な管理・対策をすることが難しいのが現状です。

■脆弱性管理クラウド「yamory」サービス概要

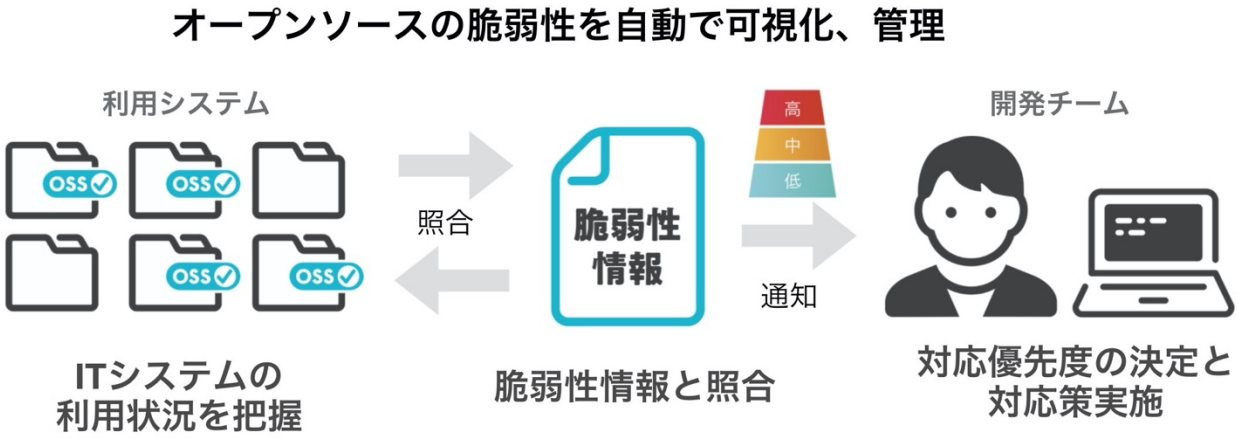
yamoryは、複数のITシステムの脆弱性とオープンソースライセンス違反をクラウド上で一元管理することで、サイバー攻撃やオープンソースライセンス違反から自社サービスを守り、ITシステムからの情報漏洩と法的リスクの軽減を目指します。

特徴（1）　独自で構築した脆弱性のデータベースを使い、危険度のレベルを算出

常に最新の脆弱性情報と攻撃用コードをyamory独自で収集し、ITシステムの利用状況と照合し、脆弱性を可視化します。

特徴（2）　対応の優先度を自動で判断するオートトリアージ機能（特許取得済み）を搭載

オートトリアージ機能（特許取得済み）は、脆弱性ごとに流通している攻撃コードを収集することで、悪用される可能性の高い脆弱性をリスクの大きさに応じて自動で分類する機能です。これにより、ITシステムが抱える多くの脆弱性のなかから、緊急度が高く直ちに対策すべき脆弱性を可視化し、漏れなくスピーディーに対応することが可能です。



■OSとミドルウェア・開発言語への対応と、ライセンス違反検知を開始。国内初、脆弱性の一元管理を実現

新機能（1）　OSとミドルウェア・開発言語への対応

ITシステムはOS、ミドルウェア・開発言語、ライブラリ・フレームワークなどのレイヤーで構築されています。これまでyamoryは、アプリケーション内で利用されているライブラリ・フレームワークにおける脆弱性に対応していましたが、新機能ではOS、ミドルウェア・開発言語の脆弱性も自動検知し、管理・対策ができるようになります。

新機能（2）　オープンソースライセンス違反の検知

オープンソースは誰でも自由に無償で入手できるメリットがある一方、それぞれのオープンソースで利用時のライセンス（ソフトウェアの利用許諾契約書）が定められています。これらのソフトウェアの利用条件を把握せずに、意図せず著作権を侵害してしまうリスクが存在しており、損害賠償やソースコードの公開を請求されるなど、経営上の大きな損失につながるケースが多数発生しています。yamoryでは、ITシステムのオープンソースの利用状況とともに、それぞれのライセンス情報も管理することで、違反を防ぐことが可能です。

これまでは、管理者が属人的にITシステムの利用状況を把握し、それらにおける脆弱性やオープンソースライセンス違反を管理・対策する必要がありましたが、新機能により、開発、運用、セキュリティのそれぞれの担当者がyamory上でITシステムの脆弱性とオープンソースライセンス違反を一元管理することが可能となります。

■yamory新機能利用企業コメント（企業名の五十音順）

エムスリー株式会社 エンジニアリンググループ グループリーダー　岩佐 淳史 氏

エムスリーは2000年創業の会社で、「インターネットを活用し、健康で楽しく長生きする人を１人でも増やし、不必要な医療コストを１円でも減らすこと」を目指しています。「m3.com」を中心とするプラットフォームを活用し、多様な医療系サービスを展開しています。

OSSのライブラリ利用が開発の基本となっていること、およびセキュリティの重要性が年々上がっていることもあり、以前からyamoryを導入し、Webアプリケーションが抱えている脆弱性を一覧化することで、セキュリティアップデートの計画と実施に活用させていただいていました。

このたび、OS・ミドルウェアのスキャン機能をリリースしていただいたことにより、今までカバーできていなかった部分への対応も広がりました。

実際にオンプレミスで運用している数百台のサーバーのOS・ミドルウェアの脆弱性を検出し、数千件のセキュリティアップデートを実施しています。

セキュリティは、「どこまでやればいいのか？」「どれだけコストをかければよいのか？」という基準がわかりにくかったのですが、yamoryがカバー範囲を広げてくれることで、今後もコストパフォーマンスのよいセキュリティを実現できそうです。

freee株式会社 CIO　土佐 鉄平 氏

freeeは「スモールビジネスを、世界の主役に。」をミッションに、「freee会計」を中心とする統合型経営プラットフォームを開発・提供しています。

yamoryを導入したことで、安全なプラットフォームの提供にセキュリティは欠かせないものとして、日夜セキュリティ向上に取り組むことができています。

yamoryの検出項目にはCVEだけではなく関連情報も集約されているため、個々に情報収集する必要がなく、その分の工数削減が実現できました。また実際に攻撃可能なコードも収集してくれるため、具体的にどういった脅威があるのかを把握でき、セキュリティチームで実施しているリスク判定に活用し、対策しなければいけない脆弱性に注力できています。yamoryを運用していくことでライブラリの脆弱性対策について各プロダクトで分散することなく一定のベースラインを引けるようになりました。現在、弊社が抱える課題として、開発者の脆弱性対策に対する「モチベーション低下」が挙がっており、それ

に対するアプローチとしてCIのなかにyamoryを組み込むことを考えているため、機能拡張に期待しています。また、弊社はさまざまな場面でコンテナを利用しているケースがほとんどであり、新機能であるコンテナスキャナがどういったものになるのか注目しています。世に出ているOSSスキャナからの乗り換えを検討できるような機能になることを期待しています。

■ビジョナル・インキュベーション株式会社 yamory事業責任者　高橋 則行 コメント

yamoryは、「情報漏洩リスクをゼロにする」を目指しており、今回、企業がDXを推進するうえで、何が必要で、どのような種類のセキュリティが求められているかを考え、新機能追加に至りました。

これまでは、開発、運用、セキュリティのそれぞれの担当者が、属人的にセキュリティ担保を行ってきましたが、DXが進み、世の中にITシステムが激増する今後は、属人的な管理や、手間のかかる脆弱性診断だけでは、対応が追いつかなくなるでしょう。

yamoryはこのような時代の変化を見据えて、セキュリティ対策を自動的に運用できる世界を目指しています。企業様からのさまざまなお声のなかで、管理が容易かつ使いやすいクラウドベースで、さらに脆弱性リスクからライセンス違反まで一元管理したいというご要望を多くいただいていました。今後はコンテナや、各社IaaS（Infrastructure as a Service）のセキュリティまでも含めた一元管理ができるソリューションに発展させていく予定です。

セキュリティ対策においては、境界防御だけでは、高度な防御を構築していても、小さな抜け穴から決壊する危険性があります。全てのITシステムの脆弱性対策を行う必要があり、属人的な対応への依存は限界を迎えています。yamoryを活用していただき、お客様のITシステムの脆弱性を自動で検知し、管理・対策を強化することで、TCO（Total Cost of Ownership）の削減、情報漏洩リスクの軽減に加えて、お客様のDXの推進に寄与していきます。

※1：当社調べ
※2：国立研究開発法人情報通信研究機構「NICTER観測レポート2020」（2021年2月）
※3：ソフトウェアの脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広めるメリットがある。一方、その情報を攻撃者に悪用され、当該ソフトウェアに対する脆弱性対策を行っていないシステムを狙った攻撃が行われている。近年では脆弱性情報の公開後、攻撃コードが流通し、攻撃が本格化するまでの時間が短くなっている。
※4：ZDNet Japan「サイバー攻撃の85％は良く知られた脆弱性を悪用したもの--ベライゾン調査」（2016年6月）

■9月2日開催、企業の情報セキュリティレベル向上を目指すオンラインセミナー「Visional Security Lounge」（参加費無料）概要

Visionalグループは、情報セキュリティの強化に積極的に取り組む企業の事例やセキュリティ責任者の考えを知ることで、自社や自身の課題解決のヒントになる機会を創出し、企業の情報セキュリティレベルの向上を目指すオンラインセミナー「Visional Security Lounge（セキュリティ ラウンジ）」を2021年9月2日（木）に開催します。※参加費無料

＜お申し込みURL＞
connpass：https://d-cube.connpass.com/event/221920/
Peatix：https://visional-security-lounge-vol1.peatix.com

【脆弱性管理クラウド「yamory（ヤモリー）」について】

「yamory」は、ITシステムの脆弱性を自動で検知し、管理・対策ができるクラウドサービスです。独自で構築した脆弱性のデータベースを使い、危険度のレベルを算出し、対応の優先度を自動で判断するオートトリアージ機能（特許取得済み）を搭載しています。ITシステムのライブラリ・フレームワーク、ミドルウェア・開発言語、OSの脆弱性、および、オープンソースのライセンス違反を一元管理できる国内初のサービスです。脆弱性を管理・対策することでサイバー攻撃から身を守り、ITシステムからの情報漏洩と、ライセンス違反による法的リスクの軽減を実現します。

URL：https://yamory.io/

※30日間の無料トライアルが可能です。詳細は上記URLからご確認ください。

【Visionalについて】

「新しい可能性を、次々と。」をグループミッションとし、HR Tech領域を中心に、産業のデジタルトランスフォーメーション（DX）を推進するさまざまな事業を展開。「ビズリーチ」をはじめとした採用プラットフォームや、人財活用プラットフォーム「HRMOS」シリーズを中心に、企業の人材活用・人材戦略（HCM）エコシステムの構築を目指す。また、事業承継M&A、物流DX、サイバーセキュリティ、Sales Techの領域においても、新規事業を次々に立ち上げている。

URL：https://www.visional.inc/ja/index.html

【ビジョナル・インキュベーション株式会社について】

「新しい可能性を、次々と。」をミッションとするVisionalグループの新規事業開発を担う。事業承継M&Aプラットフォーム「ビズリーチ・サクシード」、脆弱性管理クラウド「yamory（ヤモリー）」、クラウド活用と生産性向上の専門サイト「BizHint（ビズヒント）」を運営。2020年2月、グループ経営体制への移行にともない、株式会社ビズリーチの新規事業開発組織を分社化し新設。

URL：https://visional.inc/visional-incubation/

本件に関するお問い合わせ先
Visionalグループ 広報　担当：本田 沙貴子
Email：visional-pr@bizreach.co.jp