BLACKDUCK®

“セキュリティ対策の内製化”を進めるには “アジャイル開発”に適した「脆弱性対策」を みらい翻訳が実現した方法

MiraiTranslate
みらい翻訳


みらい翻訳　山口真親氏


みらい翻訳　金 重逸氏

開発サイクルを短期間で回すアジャイル開発には、従来の脆弱性対策の手法が適さない場合がある。自社の翻訳サービスのセキュリティ対策に力を入れるみらい翻訳の事例から、アジャイル開発と脆弱性対策のポイントを探る。

NTT ドコモグループのみらい翻訳は、“言語の壁を超える”というビジョンを掲げ、異なる言語を話す人が自由にコミュニケーションできる世界を目指し、AI（人工知能）自動翻訳サービス「Mirai Translator」をはじめとするさまざまなサービスを開発、提供している。

Mirai Translator はビジネスシーンでの活用を想定していることが特徴だ。翻訳のベースとなる対訳のデータに良質なものを選び、AI に学習させることで、専門用語を含んだ文章でも高品質な翻訳を可能にしている。

法人向けのサービスとして、みらい翻訳が積極的に取り組むのが Mirai Translator のセキュリティ対策だ。同サービスは法律や製薬といった専門領域もカバーするサービスのため、ユーザー企業は機密データの翻訳に利用する場合がある。ユーザー企業が求めるセキュリティ水準が高まる中、同社はどのようにセキュリティの確保に取り組んでいるのか。

開発と脆弱性診断、2 つのライフサイクルの違いが課題に

「『英語のネイティブスピーカーではない人たちが、英語を母語とする方々と同じような自然な言語体験を得られる体験』を提供したいという思いで、Mirai Translator を開発しています」と、みらい翻訳の山口真親氏（プラットフォーム開発部 エンジニアリングマネージャー）は話す。

みらい翻訳が法人向けの翻訳サービスを提供する上で特に重視しているのが、自社サービスのセキュリティ対策だ。Mirai Translator は、ユーザー企業の機密データがみらい翻訳の従業員を含む第三者の目に触れないようすることを、セキュリティポリシーとして掲げている。システム面でも機密性を保ち、「ISO 27001」などの認証を取得してセキュリティ対策に努めてきた。

Web アプリケーションのセキュリティ対策のために、みらい翻訳は社内で「セキュリティチェックシート」を整備し、SQL インジェクションをはじめとする深刻な脆弱性が作り込まれないよう、QA（品質保証）チームが主導してセルフチェックを実施している。それに加えて、年に 1 回は外部のセキュリティ企業に依頼し、脆弱性診断も実施する。

しかし外部の診断サービスを使うには相応のコストがかかる。さらに進化が速い AI 技術をベースに Web サービスを展開し、素早いペースで機能改善を加えるみらい翻訳の開発プロセスと、年に 1 回の脆弱性診断とでは、ライフサイクルがなかなか合わないと感じるようになっていった。

“外部診断頼り”の脆弱性診断では限界に　その解決策とは

みらい翻訳は、アプリケーションの開発者に加え、テストを通して品質保証に責任を持つ QA 担当も含めた 5 人前後でスクラムチームを組み、アジャイル開発に取り組んでいる。チームによって異なるが、1、2 週間単位で目標を立て、機能追加や改善に取り組んでいる。

一方で脆弱性診断のスケジュールや工程は全く異なる。「診断対象のアプリケーションができていない 2、3 カ月前から見積もりを依頼し、どの範囲を診断するかを検討していかなければなりません。実際の診断そのものにも 1 カ月かそれ以上の期間を要し、場合によってはさらに時間をかけて再診断を実施することになります。窓口担当はもちろん、開発チームのリソースをそこに割くことに負担を感じていました」（山口氏）

診断中に対象アプリケーションに変更を加えることは望ましくない。このため開発やデプロイ作業を一時的に停止したり、場合によっては別の開発用インフラをもうワンセット用意して開発を継続したりするといった手間が掛かっていた。

こうして手間や時間を掛けて診断しても、その翌週や翌月には Web アプリケーションに変更が加わることは珍しくない。「診断からある程度時間がたち、大規模な改修があったタイミングで『今、セキュリティは大丈夫か』を定量的に証明する方法がないことも課題でした」と山口氏は話す。

ステージング環境に Continuous Dynamic を適用し、診断を毎日実施

山口氏は次のように話す。「セキュリティを気にされるお客さまから、年に 1 回ではなく、できれば月次でセキュリティ診断ができないかといった要望をいただくことがありました」。みらい翻訳にも、ユーザー企業に自社サービスを提案するときに「このような仕組みで、こういった頻度でセキュリティ診断を実施するため、安心して利用できる」と提示できる体制を整えたいという思いがあった。

こうした背景から、みらい翻訳がアプリケーションの開発ライフサイクルに合わせたセキュリティ診断を実現するために採用したのが、ブラック・ダックの動的解析ツール（DAST）の「Continuous Dynamic ™」だ。

Continuous Dynamic はもともと NTT Application Security が提供していたツールで、ブラック・ダックは同社の買収によって Continuous Dynamic を自社の製品・サービス群の一つに加えた。AI を活用してアプリケーションを実際に動作させ、主要な脆弱性に加え、アプリケーションの設定不備などを検出できる。これにより、ソースコードを解析する手法である SAST（静的アプリケーション・セキュリティ・テスト）を補完することが可能だ。

みらい翻訳の開発ライフサイクルに即したセキュリティ検査が実現できることに加え、客観的な診断結果をより高い頻度で得られることが、同社での Continuous Dynamic の採用を後押しした。

こうして 2021 年春ごろから Continuous Dynamic を試験導入し、2022 年 4 月から本格的な運用を開始した。みらい翻訳では、本番環境と同一構成で構築されたステージング環境を対象に、Continuous Dynamic による診断を実施している。

みらい翻訳の金 重逸氏（プラットフォーム開発部 QA チーム QA エンジニア）は次のように話す。「ステージング環境にアプリケーションをデプロイすると、その日の夜の間にスキャンできます。翌日出社したときには、今回のデプロイで脆弱性が検出されたかどうかを確認できます。Continuous Dynamic の API（アプリケーションプログラミングインタフェース）を活用し、何かあったらチャットツールの『Slack』のチャンネルに通知する仕組みにしています」

導入後に重大な脆弱性は検出されていないが、深刻度が中程度以上の脆弱性が報告された場合は QA チームが確認した上で部内に周知し、チームの開発者が対処するフローにしている。

Continuous Dynamic の導入によって、みらい翻訳は Web アプリケーションの脆弱性診断の頻度を年に 1 回から 1 日 1 回に変更し、脆弱性がないことを定量的に確認できるようになった。年に 1 回外部に診断を依頼する場合よりも、コストを抑えられるという効果もあった。以前は窓口担当者や開発者のストレスになっていた、診断のための事前調整が不要になったことも利点の一つだ。「年に 1 回の診断のために、2、3 カ月ほどを要する準備に悩まなくてもよくなりました」（山口氏）

山口氏は次のように説明する。「開発者がセキュリティ診断のことを気にせず、日々の開発を進めながら診断ができることも大きなメリットです。開発プロセスの効率化も実現できました」。既存の開発フローを変更したり、開発者に負担を掛けたりすることなく導入・運用できているため、QA チーム以外の開発者は Continuous Dynamic を意識せずに開発できている状況だ。セキュリティ確保に関する意識をより高めながら開発することがこれからの課題だという。

QA チームにも相乗効果が生まれた。「自分たちで検査の仕組みを構築し、脆弱性を自ら調査するようになったことで、QA チームのセキュリティに対する意識や脆弱性に関する知見が向上しました」と山口氏は話す。

他のツールとも組み合わせ、さらなるセキュリティの強化を模索

Continuous Dynamic の導入によって、脆弱性診断の頻度を高めながら、アプリケーションの開発スピードを向上させたみらい翻訳。次の課題は開発段階のさらなるセキュリティ強化だ。現状はアプリケーションをデプロイした後、ステージング環境で Continuous Dynamic を実行し、診断している。CI/CD（継続的インテグレーション／継続的デリバリー）ツールに SAST を組み込み、自動的にソースコードをチェックする仕組みを構築することで、開発プロセスの早期段階からソースコード内部に潜む脆弱性を検査できる。これにより、さらに効率的にセキュリティの強化を図れると同社は見込む。「Continuous Dynamic を取り入れたセキュリティ対策の手法を Mirai Translator 以外のサービスに適用する施策も推進し、より安心して言語の壁を越えたコミュニケーションができるようにしたいと考えています」（金氏）

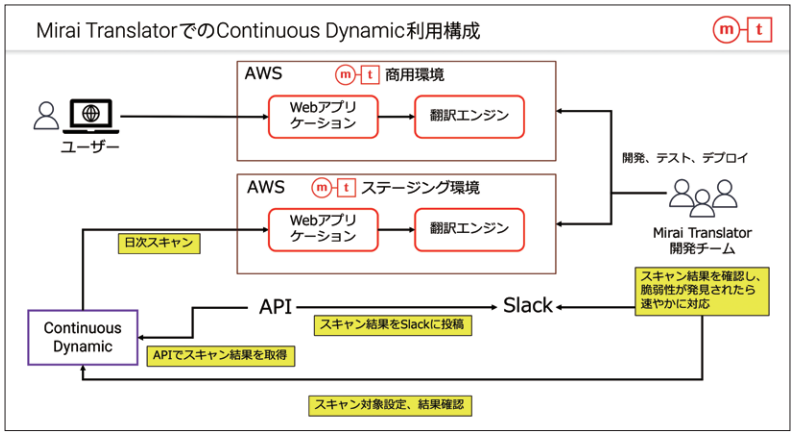

図　みらい翻訳の Continuous Dynamic 利用時の構成図（出典：みらい翻訳資料）

※この冊子は、TechTarget ジャパン（https://techtarget.itmedia.co.jp/）に 2023 年 10 月に掲載されたコンテンツを再構成したものです。
https://techtarget.itmedia.co.jp/tt/news/2310/17/news03.html

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