GitLab | SOURCENEXT

外部開発パートナーを含む開発プロセスをGitLabによるオールインワン開発環境に統合し最適化

- 3つの開発環境を1つに統合
- セキュリティを開発プロセスに取り込む
- Deploy工程の自動化

ソースネクスト株式会社（以下、ソースネクスト）は、社内にあるECを含む最も大きなシステムの開発・運用プロジェクトにおいて、GitLabのすべての機能を有効に活用し、DevSecOpsを実現しました。社内の開発メンバーと外部の開発パートナー企業がGitLabをひとつの開発プラットフォームとして駆使し、プロセスの厳格化によるビジネスリスク低減に成功。同時に、Deploy工程の9割を自動化するなどの工数削減効果を得て、生産性250%アップという成果に結びつけることができました。

業種
システム・ソフトウエア

規模
単体131名
連結166名

本拠地
日本、東京

ソリューション
パソコン・スマートフォンソフトウェアおよびハードウェア製品の企画・開発・販売

Deploy工程の9割を自動化

生産性250%アップ

まずはDevSecOpsというコンセプトを理解すること。そして、それに共感するのであれば、いちはやくスタートすることをおすすめしています。

高沢 冬樹 氏
ソースネクスト株式会社 CIO

3つの開発環境をGitLabでひとつに統合

ソースネクストは、パソコン・スマートフォンソフトウェアおよびハードウェア製品の企画・開発・販売を行う東証プライム市場上場企業です。「製品を通じて、喜びと感動を、世界中の人々に広げる」という創業以来の思いから、消費者とメーカーにとって最適なプライシング戦略が強み。近年はIoT製品の取り扱いを広げ、AIを活用した取り組みも積極化させるなど、最新テクノロジーをうまくビジネスに取り入れながら成長を続けています。

同社では、ソフトウェア開発において、少数精鋭の社内エンジニアと外部開発パートナー企業との協業体制を取っています。長年一緒にやる中で関係性は深まり、優れたチーム同士が役割分担しながらシステムをブラッシュアップしてきました。しかし、セキュリティとガバナンスが大きな経営課題としてクローズアップされる中、より密にチーム同士を連携させ、一貫した厳格な開発プロセスへと移行とすることで、ビジネスへのリスクを極小化したいというニーズが出てきました。

同社 CIO 高沢 冬樹氏は、「開発環境刷新の対象としたシステムを担当する外部開発パートナーは2社で、どちらもスキルが高く、信頼できるメンバーがそろっている企業です。ただ、以前の開発プロセスは、社内のものと2社のものが同時に走る状態で、いわば3つのDevOpsが並立していたようなイメージだったのです」と話します。

これら3つの開発環境を統合するとともに、セキュリティを開発プロセスに取り込むDevSecOps*へと昇華させたい――。高沢氏も経営層も意見は同じでしたが、管理を厳格化すると現場がやらなければならないことが増え、結果として現場に負担を強いることになります。そこで、DevSecOpsを定着させて経営の求める厳格な開発プロセスへと移行しながら、同時に現場を楽にする自動化をやり遂げ、負担をトレードオフするという発想が生まれました。

オールインワン開発環境のGitLabをフルに使ってやってみる

DevSecOpsを検討するにあたり、ソースネクストは株式会社トレンドソリューションズ（以下、トレンドソリューションズ）に協力を依頼しました。そして、市場にあるDevSecOpsソリューションの中から、GitLabを本格的に調査することになりました。検討初期において、GitLabの最大の魅力は強力な脆弱性スキャン能力でした。ただ、DevSecOpsのコンセプトを深く理解するようになるにつれ、「1つの製品でDevSecOpsのすべてのプロセスに対応できる」ことと、「豊富なドキュメント系の機能を備えていて、振り返りをしやすい仕組み」こそが、求めている仕様にマッチしていることがわかってきたといいます。

「GitLabだけがあればDevSecOpsを実現できる、というトータルソリューションになっている点は、初めて取り組む上で重要でした。開発コードのセキュリティスキャン、CI/CDなど開発リリース時に必須の個別プロセスに対応できるツールを組み合わせて“DevSecOpsのDIY”をするというアプローチもあるのかもしれませんが、詳細な機能比較をするにしても、だれも体感したことのない機能に優劣をつけようがありません。ですから、まずはGitLabをフルに使ってやりたいことを

* DevSecOps とは
開発と運用を統合する DevOps にセキュリティを加え、運用を視野に入れながら開発とセキュリティを同時に進め、安心・安全なソフトウェアを迅速にリリースするというコンセプト。

すべてやってみて、どうしても足りなければそのときに考えようという方向で意見が一致しました」（高沢氏）
今回のプロジェクトで対象となったのは、社内で最も大きなECを含むフロントエンドシステムです。高沢氏は、「スモールスタートでテストしたかったわけではありません。最も難しいところからスタートしたのは、動機が“DevSecOpsを使ってみたい”ではなく、“ビジネスの品質を高めたい”という真剣なものだったから。最初から成果が求められました」と振り返ります。
GitLabの採用を決め、半年をかけてじっくりと新たな開発プロセスを整備していきました。経験豊富なトレンドソリューションズのスペシャリストがプロジェクトをリードし、社内エンジニアが外部開発パートナーを巻き込んで議論を重ね、さまざまな決めごとをクリアしていったのです。
具体的には、GitLabとDevSecOpsのコンセプト理解および共有からスタートし、to beモデルを作成。それに向けた課題をリスト化し、順次プロセスの中に落とし込んでいくイメージです。ワークフローの整備やCI/CDの仕様策定など、専門的な知見が生きる分野はトレンドソリューションズが主導したことで、プロジェクトはスムーズに進みました。
巨大で複雑なシステムであるために、苦労した点もありました。Microsoft Azureベースのシステムであり、「自動化のための呪文（笑）を唱えるとうまくいくところ」（高沢氏）を切り抜ける必要がありました。システムの中にCMSパッケージがあり、その部分と連携するシステム開発においてサーバ側で独特な手法を取りながら自動化するという調整も実施しました。AzureとCMS、GitLabのすべてを深く理解しているメンバーはおらず、最適な着地点を見い出すために全員がプロジェクトの成功にコミットして知識を持ち寄る必要もありました。
プロジェクトメンバーは、これらの課題に立ち向かい、稼働時にはGitLabを使う新たな開発プロセスへと移行することができました。プロジェクト初期から、課題管理にGitLabのイシュー機能を利用したことも、スムーズな移行に役立ちました。これはトレンドソリューションズがGitLab導入プロジェクトでよく使う手法で、初期からすべてのメンバーが仕事の中でGitLabを使う習慣が自然と身につくという点で価値は高かったといいます。

Deploy工程の９割を自動化、生産性は250%アップ

実は、無理をして自動化しなかった部分や、あえて手作業を残した部分もあります。たとえば、CI/CDを工夫し、一部に手作業を加えることでよりセキュアな開発をできるようにしました。Deployにかかわる全工程は、現状で９割の自動化にとどめています。
高沢氏は、「Deploy部分は、もっと自動化しようと思えばできます。ただ、実務を考えると自動化しない部分を残しておいた方が良いと判断したケースもあるのです。たとえば、最後の検証作業はパフォーマンスチェックも含むので、自動化したとしても結局は目視することになります。やろうと思えば95%までならいけるのですが、やめておいた方がより良さそう、というせめぎあいです。もう少し慣れてくると、現場と相談して自動化部分を増やすかもしれません。ただ、現場がやりやすい開発プロセスを目指すなら、９割くらいが最適解かもしれませんし、９割は十分に良い数字だと自負しています」と話しています。
GitLabの稼働後、そのほかにも多くの成果が顕在化しています。エラー検知とセキュリティ診断がプロセスに取り込まれた上に自動化されたことで、作業効率を高めながらプロセスを厳格化することに成功しました。手作業でやっていった際には時間のかかっていたパッケージングプロセスは完全に自動化できました。これらを含め、トータルな作業負荷を低減できたため、エンジニアの生産性は250%以上アップしている感覚があるといいます。
これまでの“３つのDevOps”は、“ひとつのDevSecOps”になり、自社が担当する部分と開発パートナーに任せる部分をすべてソースコードレベルから、イシューを含めて管理できます。これにより、初期開発時の思想を含めてすべての情報を管理できるようになりました。また、以前は時間を要していた組織をまたいだマージリクエスト処理でも、“組織”という壁はもはやありません。

GitLab

「気づいていないリスク」を可視化する価値

高沢氏は、「開発における最大の課題は、“気づいていないリスク”です」と話します。あらゆるシステムは、「将来にわたって絶対にリスクがない」と言えませんが、それ以上に、「今リスクがあるのかどうかも不確かであり、確かめようがなかった」のです。「例えば、サードパーティのJSライブラリを、ユーザー体験をより良くするためにWebサイトのごく一部で使っていた、などのケースはよくあることです。これらは存在すら見つけにくい上に、コールするライブラリの先の先にリスクが潜んでいる場合もあります。ソースコードチェックだけでリスク発見することはほぼ不可能です」。

GitLabで一貫したDevSecOpsを実現したことで、コールするライブラリの先の先までを自動検証し、リスクを避けることができます。目指していた姿は、「100%安全なシステムはありえないけれど、“ここまできちんとやっている”と自信を持って説明できる状態」（高沢氏）です。そして、それを実現することができました。今回の成功を受けて、販売する製品別のシステム開発プロジェクトや、社内業務システムの開発・運用プロジェクトにも、今後GitLabを展開する計画も出てきました。

ソースネクストがDevSecOpsを推進している、という噂は、IT関係者に伝わり始めているようです。そのため、高沢氏は各社のCIOが集まる場で意見を求められるケースが増えてきたといいます。

高沢氏は、「DevSecOpsは国内企業からも大きな注目を集めていて、私たちがGitLabを使ってシフトレフト*に全力で取り組んでいるという話をすると、みなさん興味津々です。ただ、実際に取り組んでいる企業の数となるとまだまだかもしれません。ですから、まずはDevSecOpsというコンセプトを理解すること。そして、それに共感するのであれば、いちはやくスタートすることをおすすめしています」と話してくれました。

* シフトレフトとは
開発の各フェーズにセキュリティ対策を組み込み、開発効率を向上させながらセキュリティリスクを低減しようとする考え方。GitLab はコード解析、脅威モデリング、テストなどシフトレフトに役立つ機能を提供している。

※本内容は2024年8月取材当時の情報をもとに制作しております。