



The Liquid Software Company

GitHub & JFrog インテグレーションについて

JFrog Japan株式会社

東京都千代田区丸の内2-2-1 7F

Alex Wang

2025/08/20



1

Copyright © 2022 JFrog Inc. All Rights Reserved.

自己紹介

戦略コンサル時代、様々な業界に対して、アジャイル、DevSecOpsのコーチとして開発環境構築、CI/CD構築などのプロジェクトをリードしてきました。

現在、JFrogでDevSecOpsやLiquid Softwareを日本への展開・普及を行っています。



<https://www.linkedin.com/in/alex-wang-662290150/>



EXIN DevOps Professional

PMI Project Management Professional

PCI DSS Member

Aoyamagakuin-MBA

Fortune100のうち、90社採用。本社アメリカ、国内100社以上導入実績

10/10

TOP
TECHNOLOGY

10/10

TOP
FINANCE

9/10

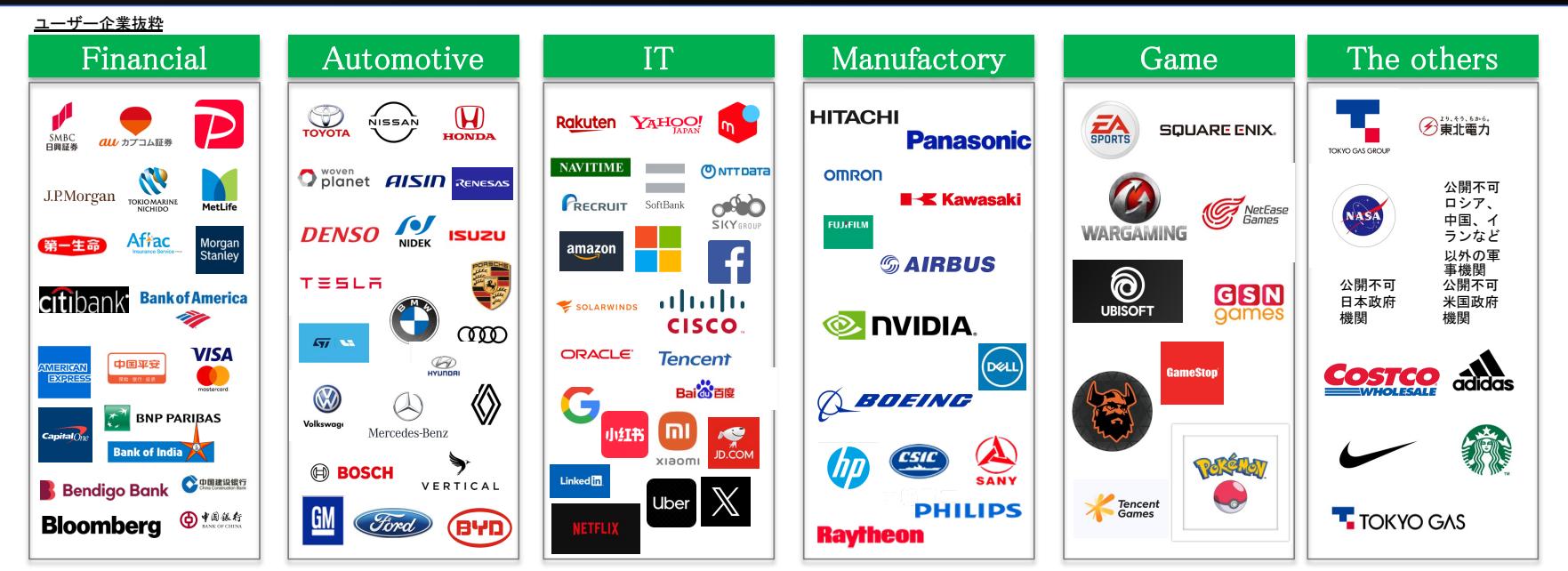
TOP
HEALTHCARE

8/10

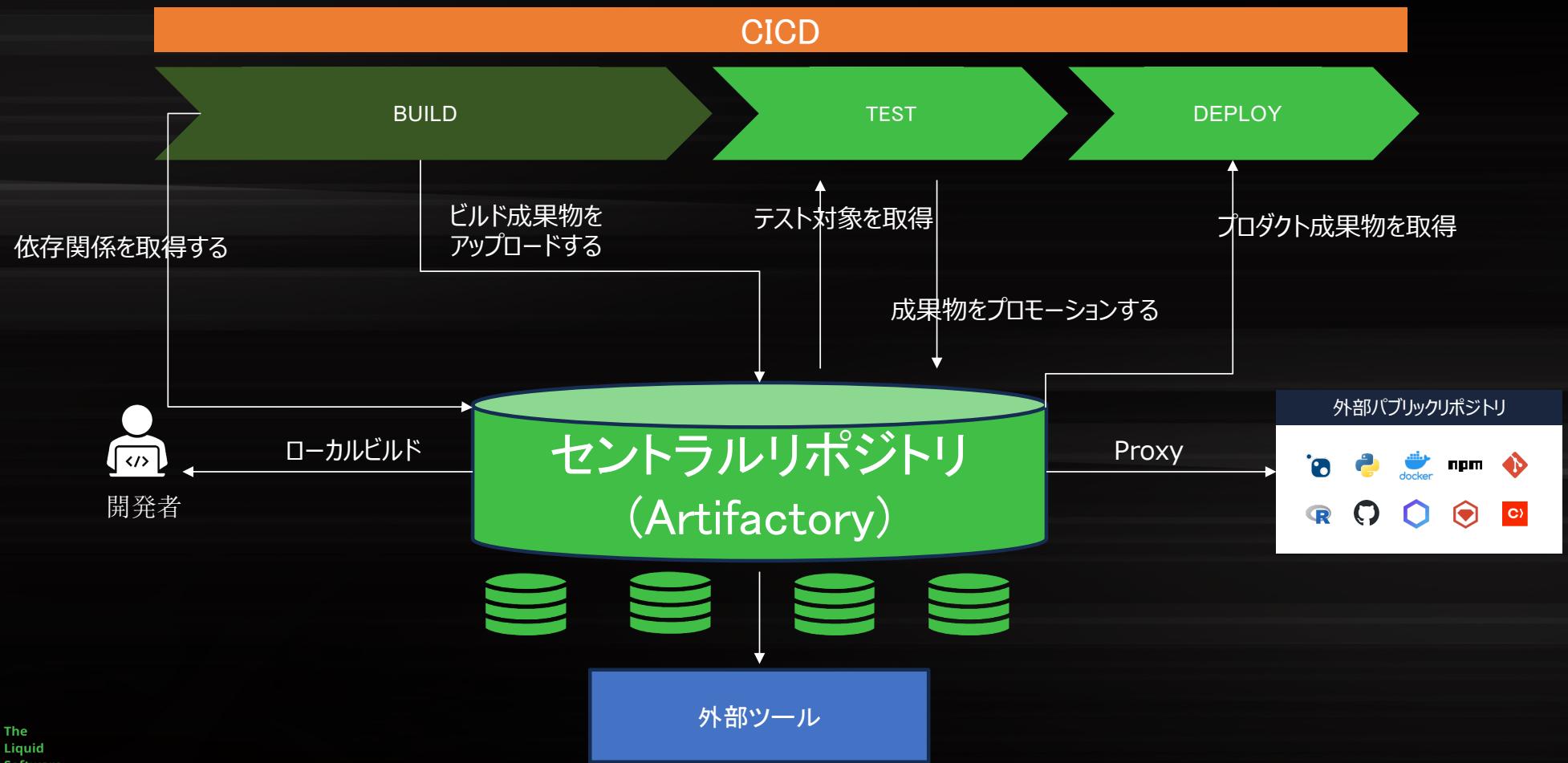
TOP
RETAIL

8/10

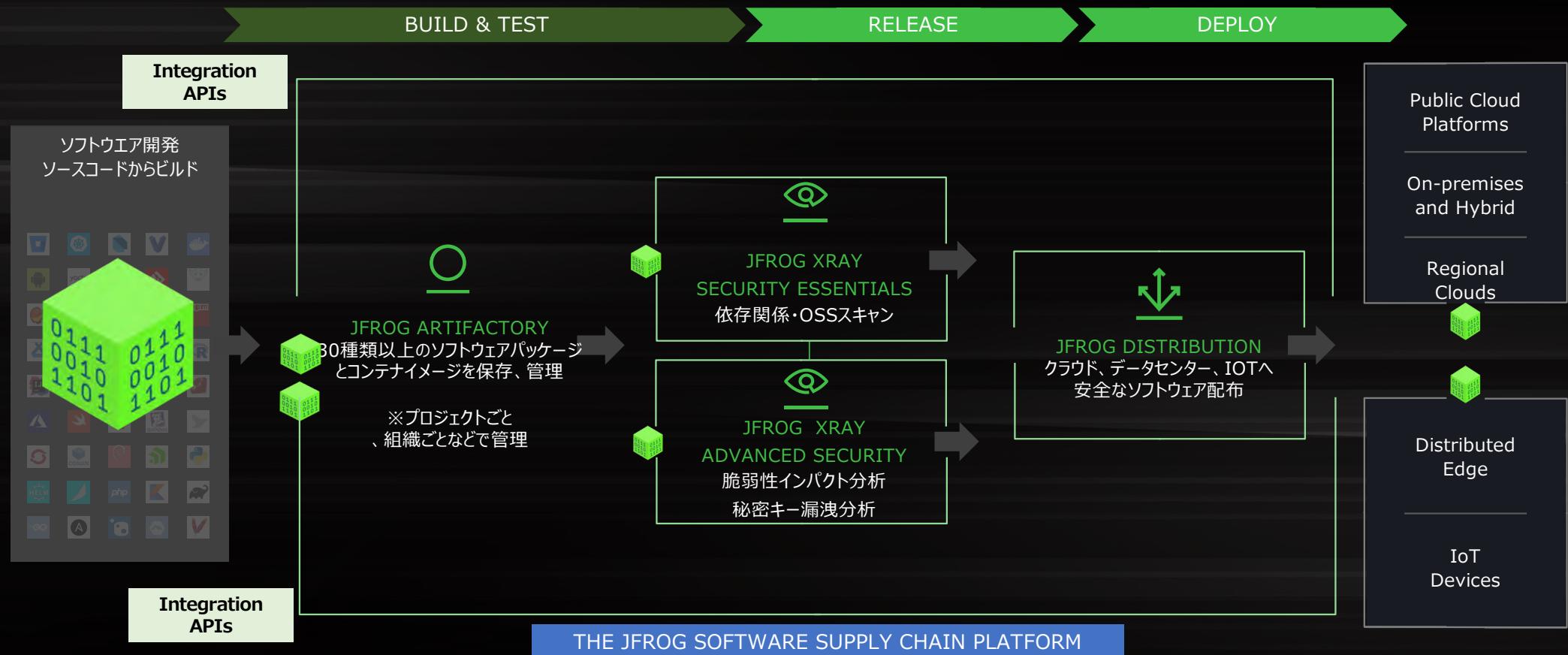
TOP
TRANSPORTATION



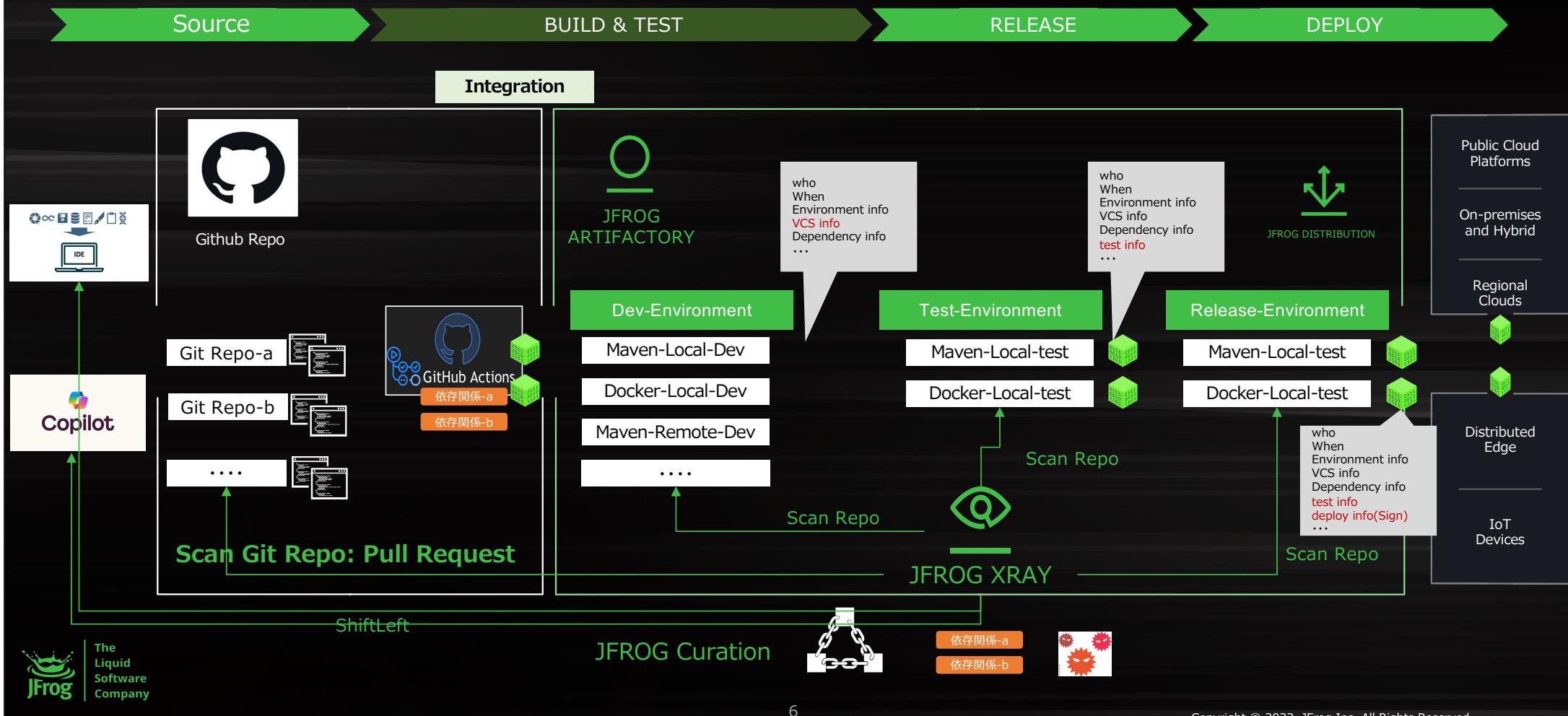
Artifactory : セントラルリポジトリとは



JFrog プラットフォームについて

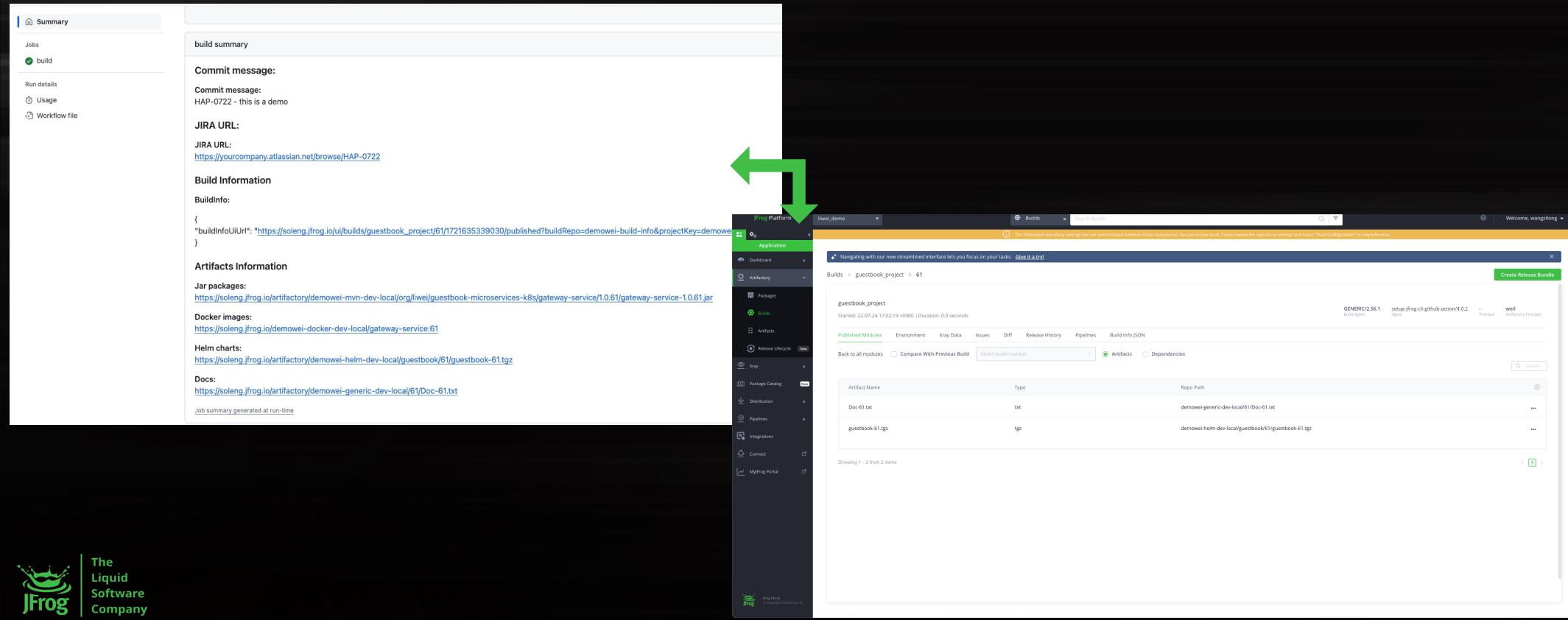


ex: Github + JFrog 開発～リリースProcess



双方向のコードとパッケージのリンクとCI統合

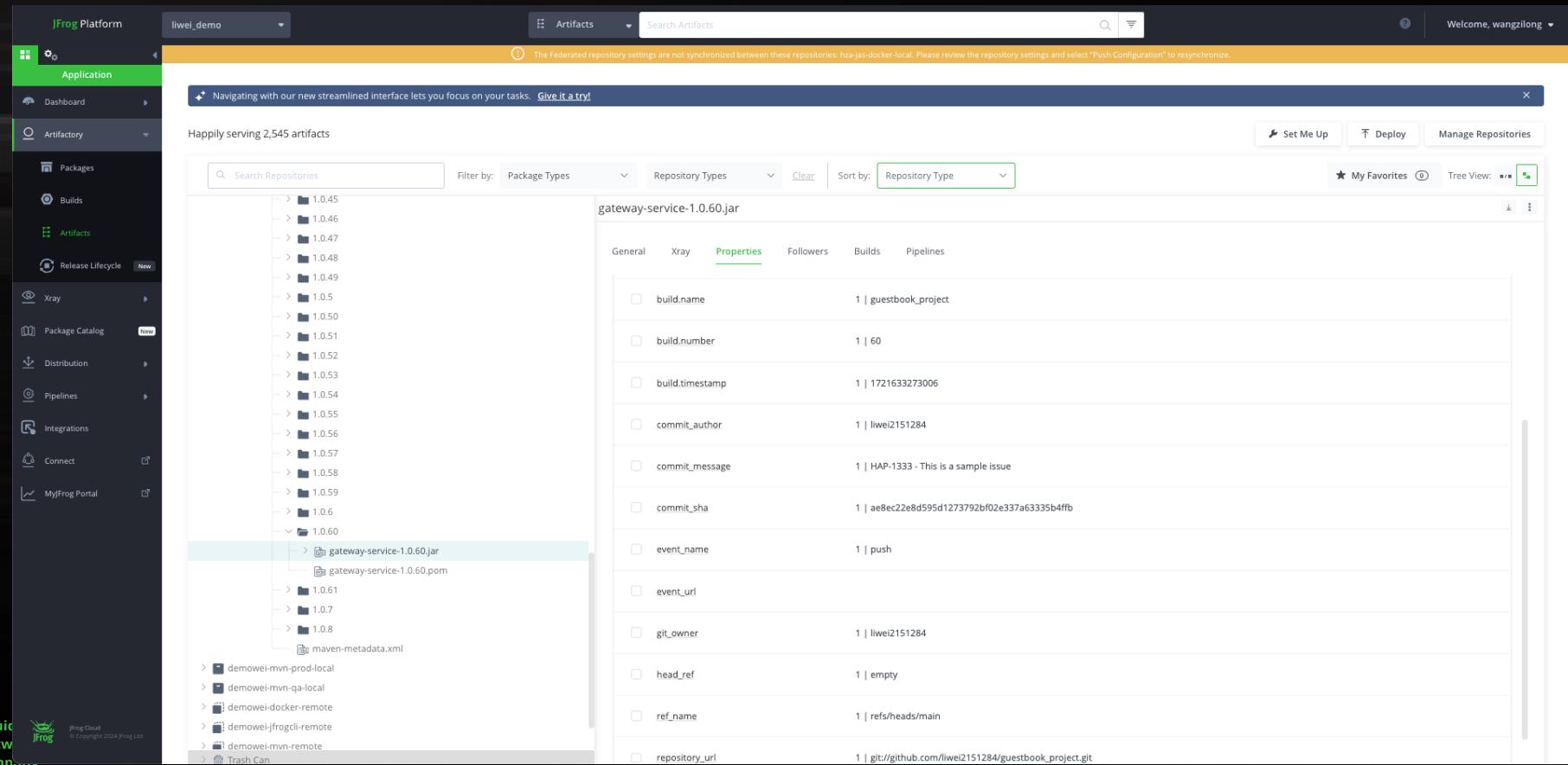
成果物だけではなく、ビルト時の環境情報、metaデータなどがJFrogに入る、ソースコードとバイナリの情報リンク



The screenshot shows the JFrog Artifactory interface. On the left, a sidebar titled 'Summary' displays 'Jobs' (1), 'build' (selected), 'Run details', 'Usage', and 'Workflow file'. The main content area is titled 'build summary' and contains sections for 'Commit message', 'Run details', 'JIRA URL', 'Build information', and 'Artifacts Information'. The 'Build information' section shows a JSON snippet for 'BuildInfo'. The 'Artifacts Information' section shows 'Jar packages' and 'Docker images'. A green double-headed arrow is overlaid on the screenshot, pointing between the 'build summary' section and the 'Artifacts' table on the right. The 'Artifacts' table lists two items: 'Doc-61.txt' (Type: txt, Repo Path: demowei-generic-dev-local/61/Doc-61.txt) and 'guestbook-61.tgz' (Type: tgz, Repo Path: demowei-helm-dev-local/guestbook/61/guestbook-61.tgz). The right side of the interface shows a 'Builds' tab for 'guestbook_project' with a build number of 61, and a 'Build Info JSON' tab.

ビルドインフォとバージョン管理について

例：このJarファイルに対して、PJ name、ビルドNo.、ビルドの人（Git Owner）、ビルド時間、Git repoなど確認できる



The screenshot shows the JFrog Platform interface for the repository 'liwei_demo'. The left sidebar is the navigation menu. The main area displays the artifact 'gateway-service-1.0.60.jar' with its properties. The properties table includes:

| Property | Value |
|-----------------|---|
| build.name | 1 guestbook_project |
| build.number | 1 60 |
| build.timestamp | 1 1721633273006 |
| commit_author | 1 liwei2151284 |
| commit_message | 1 HAP-1333 - This is a sample issue |
| commit_sha | 1 ae8ec22e8d595d1273792bf02e337a63335b4ffb |
| event_name | 1 push |
| event_url | |
| git_owner | 1 liwei2151284 |
| head_ref | 1 empty |
| ref_name | 1 refs/heads/main |
| repository_url | 1 git://github.com/liwei2151284/guestbook_project.git |

ビルドインフォについて

また、以前のビルド成果物とのDiffを取れる

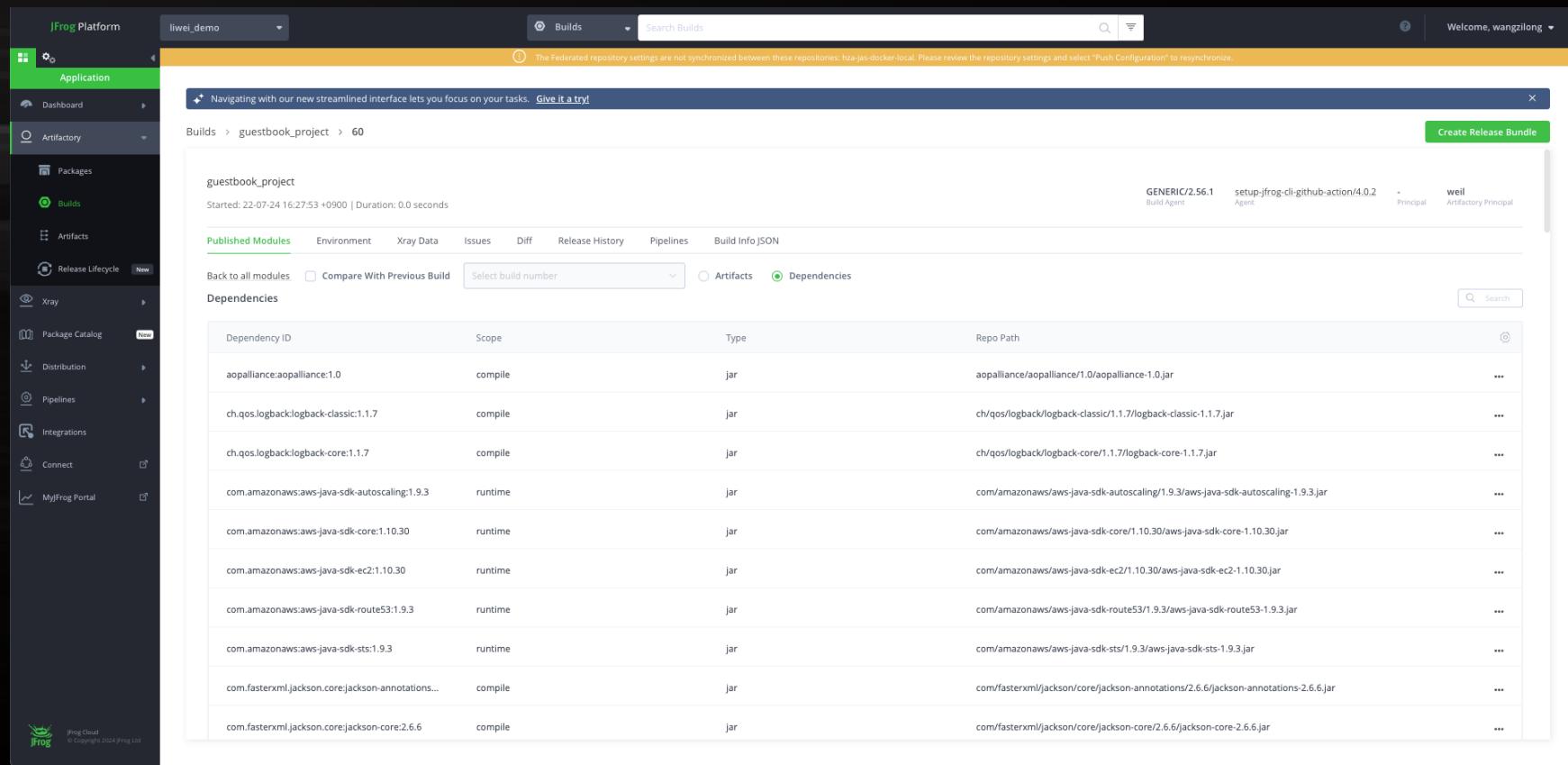
The screenshot shows the JFrog Platform interface with the following details:

- Header:** JFrog Platform, liwei_demo, Builds, search Builds, Welcome, wangzilong.
- Left Sidebar:** Application (Dashboard, Artifactory, Packages, Builds, Artifacts, Release Lifecycle), Xray, Package Catalog, Distribution, Pipelines, Integrations, Connect, MyFrog Portal.
- Current View:** Builds > guestbook_project > 60
- Toolbar:** Create Release Bundle.
- Content Area:**
 - Message: "Navigating with our new streamlined interface lets you focus on your tasks. Give it a try!"
 - Message: "The Federated repository settings are not synchronized between these repositories: h2a-jenkins-local. Please review the repository settings and select 'Push Configuration' to resynchronize."
 - Table: Comparison of build variables between build 59 and build 58. The table includes columns for Variable, Value (Build # 59), Value (Build # 58), and Status.

| Variable | Value (Build # 59) | Value (Build # 58) | Status |
|---|--|---------------------------------------|-----------|
| buildInfo.env.ACCEPT_EULA | Y | | Unchanged |
| buildInfo.env.ACTIONS_RUNNER_ACTION_ARCHIVE_CACHE | /opt/actionarchivecache | | Unchanged |
| buildInfo.env.AGENT_TOOLSDIRECTORY | /opt/hostedtoolcache | buildInfo.env.AGENT_TOOLSDIRECTORY | Unchanged |
| buildInfo.env.ANDROID_HOME | /usr/local/lib/android/sdk | buildInfo.env.ANDROID_HOME | Unchanged |
| buildInfo.env.ANDROID_NDK | /usr/local/lib/android/sdk/ndk/25.2.9... | buildInfo.env.ANDROID_NDK | Unchanged |
| buildInfo.env.ANDROID_NDK_HOME | /usr/local/lib/android/sdk/ndk/25.2.9... | buildInfo.env.ANDROID_NDK_HOME | Unchanged |
| buildInfo.env.ANDROID_NDK_LATEST_HOME | /usr/local/lib/android/sdk/ndk/26.3.1... | buildInfo.env.ANDROID_NDK_LATEST_HOME | Unchanged |
| buildInfo.env.ANDROID_NDK_ROOT | /usr/local/lib/android/sdk/ndk/25.2.9... | buildInfo.env.ANDROID_NDK_ROOT | Unchanged |
| buildInfo.env.ANDROID_SDK_ROOT | /usr/local/lib/android/sdk | buildInfo.env.ANDROID_SDK_ROOT | Unchanged |
| buildInfo.env.ANT_HOME | /usr/share/ant | buildInfo.env.ANT_HOME | Unchanged |

依存関係について

すべての依存関係を一覧できる



The screenshot shows the JFrog Platform interface for a build named 'guestbook_project' (Build ID: 60). The build was started on 2022-07-24 at 16:27:53 and completed in 0.0 seconds. The build is associated with a Build Agent named 'well' and an Artifactory Principal named 'well'. The interface displays the 'Published Modules' tab, showing the build's environment, Xray data, issues, diff, release history, pipelines, and build info JSON. The 'Dependencies' tab is selected, listing the following dependencies:

| Dependency ID | Scope | Type | Repo Path |
|---|---------|------|--|
| aopalliance:aopalliance:1.0 | compile | jar | aopalliance/aopalliance/1.0/aopalliance-1.0.jar |
| ch.qos.logback:logback-classic:1.1.7 | compile | jar | ch/qos/logback/logback-classic/1.1.7/logback-classic-1.1.7.jar |
| ch.qos.logback:logback-core:1.1.7 | compile | jar | ch/qos/logback/logback-core/1.1.7/logback-core-1.1.7.jar |
| com.amazonaws.aws-java-sdk-autoscaling:1.9.3 | runtime | jar | com/amazonaws/aws-java-sdk-autoscaling/1.9.3/aws-java-sdk-autoscaling-1.9.3.jar |
| com.amazonaws.aws-java-sdk-core:1.10.30 | runtime | jar | com/amazonaws/aws-java-sdk-core/1.10.30/aws-java-sdk-core-1.10.30.jar |
| com.amazonaws.aws-java-sdk-ec2:1.10.30 | runtime | jar | com/amazonaws/aws-java-sdk-ec2/1.10.30/aws-java-sdk-ec2-1.10.30.jar |
| com.amazonaws.aws-java-sdk-route53:1.9.3 | runtime | jar | com/amazonaws/aws-java-sdk-route53/1.9.3/aws-java-sdk-route53-1.9.3.jar |
| com.amazonaws.aws-java-sdk-sts:1.9.3 | runtime | jar | com/amazonaws/aws-java-sdk-sts/1.9.3/aws-java-sdk-sts-1.9.3.jar |
| com.fasterxml.jackson.core:jackson-annotations... | compile | jar | com/fasterxml/jackson/core/jackson-annotations/2.6.6/jackson-annotations-2.6.6.jar |
| com.fasterxml.jackson.core:jackson-core:2.6.6 | compile | jar | com/fasterxml/jackson/core/jackson-core/2.6.6/jackson-core-2.6.6.jar |

脆弱性とSBOMについて

脆弱性の確認とSBOMの両方に対応

The Federated repository settings are not synchronized between these repositories: h2a/jas.docker-local. Please review the repository settings and select "Push Configuration" to resynchronize.

| Severity | CVSS v3 | ID | Contextual Analysis | JFrog Research | Component | Fix Version | CWE |
|----------|------------------|----------------|---------------------|--|------------------------|--------------|-----|
| 9.8 | CVE-2013-7285 | Applicable | Critical | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.11, 1.4.7 | CWE-77 (+1) | |
| 9.8 | CVE-2022-1471 | Applicable | Critical | org.yaml:snakeyaml:1.16 | 2.0 | CWE-502 (+2) | |
| 10.0 | CVE-2021-44228 | Applicable | Critical | org.apache.logging.log4j:log4j-core:2.13.0 | 2.12.2, 2.15.0, 2.3.1 | CWE-917 (+3) | |
| 9.8 | CVE-2021-21344 | Applicable | Critical | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.16 | CWE-434 (+1) | |
| 9.9 | CVE-2021-21345 | Applicable | Critical | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.16 | CWE-94 (+1) | |
| 9.8 | CVE-2021-21346 | Applicable | Critical | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.16 | CWE-434 (+1) | |
| 9.8 | CVE-2021-21347 | Applicable | Critical | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.16 | CWE-502 (+1) | |
| 9.8 | CVE-2021-21350 | Applicable | Critical | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.16 | CWE-434 (+1) | |
| 9.1 | CVE-2021-21351 | Applicable | Critical | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.16 | CWE-502 (+1) | |
| 9.1 | CVE-2021-21342 | Applicable | High | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.16 | CWE-502 (+1) | |
| 9.8 | CVE-2019-10173 | Applicable | | com.thoughtworks.xstream:xstream:1.4.2 | 1.4.11 | CWE-502 (+1) | |
| 9.8 | CVE-2022-22965 | Not Applicable | Critical | org.springframework:spring-beans:4.2.6.RELEASE | 5.2.20.RELEASE, 5.3.18 | CWE-94 (+1) | |
| 9.8 | CVE-2022-22965 | Not Applicable | Critical | org.springframework:spring-webmvc:gav://org.springframework... | 5.2.20, 5.3.18 | CWE-94 | |
| 9.8 | CVE-2016-1000027 | Not Applicable | Critical | org.springframework:spring-web:4.2.6.RELEASE | 6.0.0 | CWE-502 | |

統合セキュリティ：SASTとSCA

Frogbotを利用して、Github上でSASTとSCAもできる

The screenshot displays the JFrog Xray interface, specifically the 'Code scanning' section for a GitHub repository named 'liwei2151284 / WebGoat-frogbot'. The interface is split into two main panes.

Left Pane (Code scanning): Shows a list of vulnerabilities. The first item is a critical alert for [CVE-2023-34034] org.springframework.security:spring-security-config 6.1.0, detected in pom.xml:1. It includes a link to the alert detail page and a snippet of the XML code.

| Severity | Tool | Branch | Rule | Severity |
|----------|---------------|--------|------------------|---|
| Critical | JFrog Frogbot | main | [CVE-2023-34034] | org.springframework.security:spring-security-config 6.1.0 |

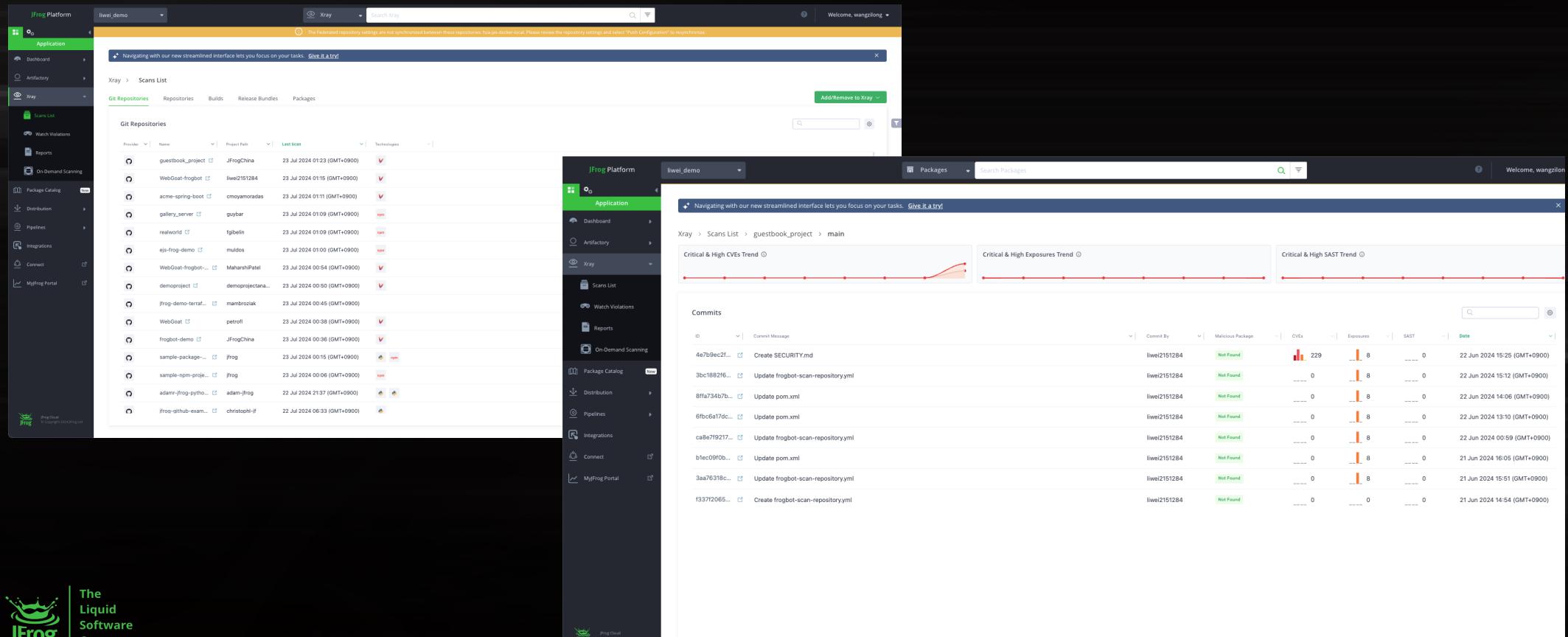
Right Pane (Code scanning alerts): A detailed view of the [CVE-2023-34034] alert. It shows the alert status (Open), the affected file (pom.xml:1), and the XML code snippet. It also includes a 'Severity' section (Critical), a 'Affected branches' section (main), and a 'Tool' section (JFrog Frogbot) with the rule ID CVE-2023-34034_org.springframework.security:spring-security-config_6.1.0.

| Severity Score | Direct Dependencies | Fixed Versions |
|----------------|---|---|
| 9.8 | org.springframework.boot:spring-boot-starter-security 3.1.0 | [5.6.12], [5.7.10], [5.8.5], [6.0.5], [6.1.2] |

Bottom Left: The JFrog logo and tagline 'The Liquid Software Company'.

統合セキュリティ：Git RepoのScan確認

JFrog UI上でGit repoのScan結果を確認できる



The screenshot displays the JFrog Platform UI, specifically the Xray and Packages sections, for a Git repository named "liwei_demo".

Xray Section:

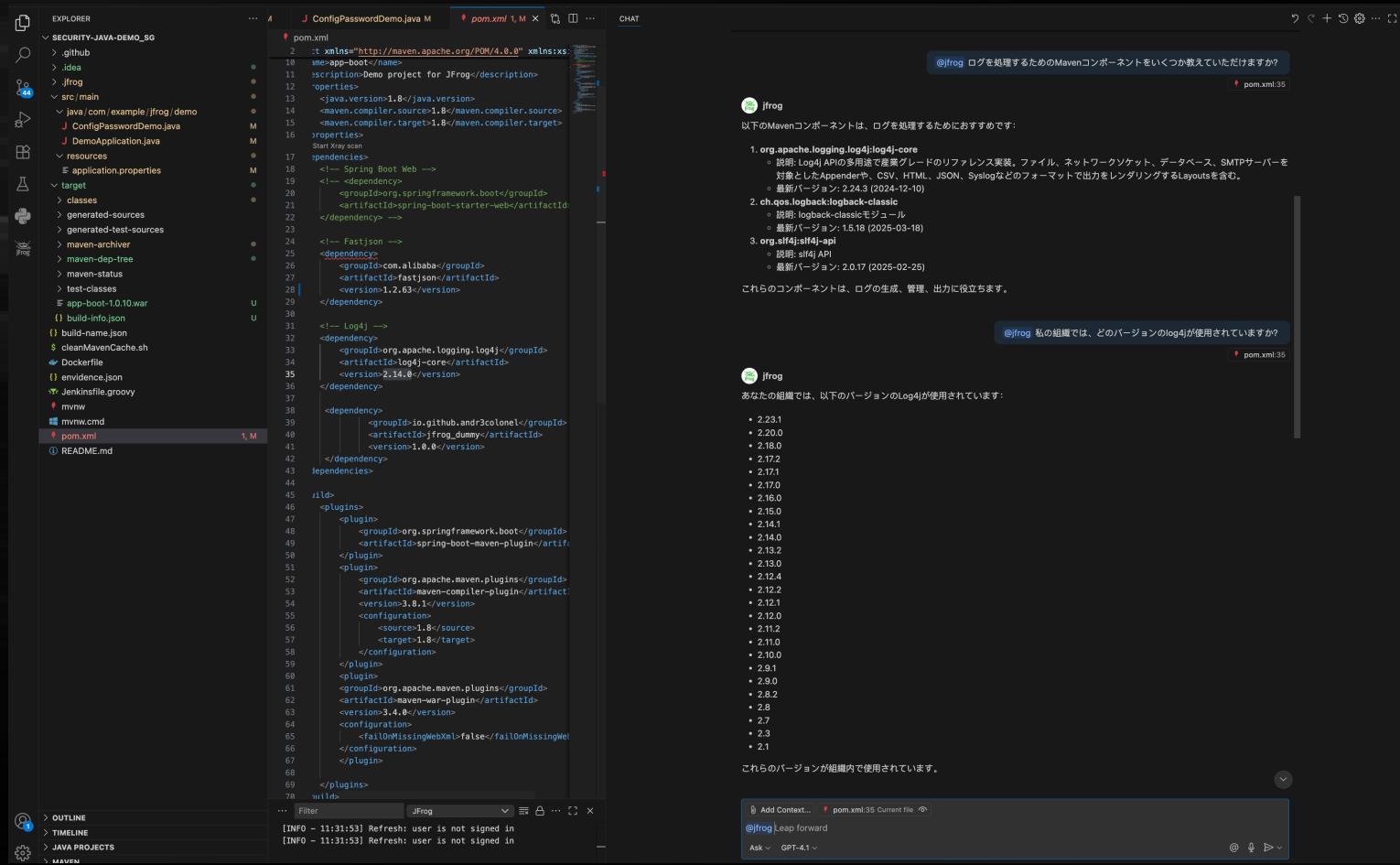
- The main header shows "liwei_demo" and "Xray".
- The sub-header "Scans List" is selected.
- The "Git Repositories" tab is active.
- A list of repositories is shown, including "guestbook_project", "WebGoat-frogbot", "acme-spring-boot", "gallery_server", "realworld", "eji-fog-demo", "WebGoat-frogbot-", "demoproject", "jfrog-demo-terraf-", "WebGoat", "frogbot-demo", "sample-package-", "sample-npm-project", "adam-jfrog-python-", and "jfrog-github-exam-". Each entry includes a provider icon, repository name, last scan date, and a red "Scan" button.

Packages Section:

- The main header shows "liwei_demo" and "Packages".
- The sub-header "Scans List" is selected.
- The "guestbook_project" repository is selected.
- The "main" branch is selected.
- Three trend charts are displayed: "Critical & High CVEs Trend", "Critical & High Exposures Trend", and "Critical & High SAST Trend".
- The "Commits" table lists recent commits:

| Commit Message | Commit By | Malicious Package | CVEs | Exposures | SAST | Date |
|---|--------------|-------------------|------|-----------|------|------------------------------|
| 4e7b9ec2f... Create SECURITY.md | liwei2151284 | Not Found | 229 | 8 | 0 | 22 Jun 2024 15:25 (GMT+0900) |
| 3bc188216... Update frogbot-scan-repository.yml | liwei2151284 | Not Found | 0 | 8 | 0 | 22 Jun 2024 15:12 (GMT+0900) |
| 8ff734b7b... Update pom.xml | liwei2151284 | Not Found | 0 | 8 | 0 | 22 Jun 2024 14:06 (GMT+0900) |
| 6fbcd6a17dc... Update pom.xml | liwei2151284 | Not Found | 0 | 8 | 0 | 22 Jun 2024 13:10 (GMT+0900) |
| ca8e79217... Update frogbot-scan-repository.yml | liwei2151284 | Not Found | 0 | 8 | 0 | 22 Jun 2024 00:59 (GMT+0900) |
| b1ec09f0b... Update pom.xml | liwei2151284 | Not Found | 0 | 8 | 0 | 21 Jun 2024 16:05 (GMT+0900) |
| 3aa7631bc... Update frogbot-scan-repository.yml | liwei2151284 | Not Found | 0 | 8 | 0 | 21 Jun 2024 15:51 (GMT+0900) |
| f337f2065... Create frogbot-scan-repository.yml | liwei2151284 | Not Found | 0 | 0 | 0 | 21 Jun 2024 14:54 (GMT+0900) |

CopilotでShiftLeft



The screenshot shows a Java project named "SECURITY-JAVA-DEMO_SG" in an IDE. The project structure includes a "src/main" folder containing "ConfigPasswordDemo.java" and "DemoApplication.java", and a "resources" folder with "application.properties". The "target" folder contains "classes", "generated-sources", "generated-test-sources", "maven-archiver", "maven-dep-tree", "maven-status", "test-classes", and "app-boot-1.0.10.war". The "pom.xml" file is open in the editor, showing Maven configuration for dependencies like Spring Boot and JFrog Dummy, and build plugins like Spring Boot Maven Plugin and Maven War Plugin.

The Chat window on the right shows a conversation with JFrog AI:

- Q: @jfrog ログを処理するためのMavenコンポーネントをいくつか教えていただけますか?
- A: 以下のMavenコンポーネントは、ログを処理するためにおすすめです:
 - 1. org.apache.logging.log4j:log4j-core
 - 説明: Log4j APIの多用途で産業グレードのリファレンス実装。ファイル、ネットワークソケット、データベース、SMTPサーバーを対象としたAppenderや、CSV、HTML、JSON、Syslogなどのフォーマットで出力をレンダリングするLayoutsを含む。
 - 最新バージョン: 2.24.3 (2024-12-10)
 - 2. ch.qos.logback:logback-classic
 - 説明: logback-classicモジュール
 - 最新バージョン: 1.5.18 (2025-03-18)
 - 3. org.slf4j:slf4j-api
 - 説明: slf4j API
 - 最新バージョン: 2.0.17 (2025-02-25)
- Q: これらのコンポーネントは、ログの生成、管理、出力に役立ちます。
- Q: @jfrog 私の組織では、どのバージョンのlog4jが使用されていますか?
- A: あなたの組織では、以下のバージョンのLog4jが使用されています:
 - 2.23.1
 - 2.20.0
 - 2.18.0
 - 2.17.2
 - 2.17.1
 - 2.17.0
 - 2.16.0
 - 2.15.0
 - 2.14.1
 - 2.14.0
 - 2.13.2
 - 2.13.0
 - 2.12.4
 - 2.12.2
 - 2.12.1
 - 2.12.0
 - 2.11.2
 - 2.11.0
 - 2.10.0
 - 2.9.1
 - 2.9.0
 - 2.8.2
 - 2.8
 - 2.7
 - 2.3
- Q: これらのバージョンが組織内で使用されています。

CopilotでShiftLeft

JFrog Platformについて

SaaS版(AWS、Azure、GCP)

利用量(Storage、Transfer)に応じて価格設定

365×24サポート
日本国内サポート

SLA 99.9%

ユーザー数、リポジトリ数、保存量無制限

Selfhosted版

ライセンス数に応じて購入

365×24サポート
日本国内サポート

HA機能でSLA保証

ユーザー数、リポジトリ数、保存量無制限

無料トライアル版があるので、
ぜひ弊社ホームページ上で
試してみてください