OpenText™ Fortify SAST

ユーザガイド

Version 26.4

PDF Generated on 2026年11月17日

© Copyright 2026 Open Text

Table of Contents

ユーザガイド 10
1 変更ログ 10
2 はじめに 17
2.1 OpenText Fortify SAST 17
2.1.1 アナライザについて 18
2.2 ライセンス 20
2.3 有効期限が切れたライセンスの更新 20
2.4 OpenText Application Security Content 21
2.5 Fortify ScanCentral SAST 21
2.6 OpenText Application Security Tools 21
2.7 サンプルプロジェクト 22
2.8 関連ドキュメント 22
3 システム要件 24
3.1 ハードウェア要件 24
3.1.1 サンプルスキャン 26
3.2 サポートされているプラットフォームとアーキテクチャ 28
3.3 ソフトウェア要件 29
3.4 AIを活用したSASTの要件 31
3.4.1 構成可能なLLM 32
3.4.2 データベース要件 33
3.5 言語の互換性 34
3.5.1 ライブラリ、フレームワーク、およびテクノロジ 37
3.5.2 AIを活用したSASTの言語の互換性 43
3.6 サポートされるビルドツール 44
3.7 サポートされているコンパイラ 45
3.8 OpenText Application Security Content 46
3.9 仮想マシンのサポート 46
3.10 ソフトウェアの取得 46
3.11 ソフトウェアのダウンロードの確認 48
4 Fortify SASTのインストール 49
4.1 Fortify SASTのインストールについて 49
4.1.1 Fortify SASTのインストール 50
4.1.2 Fortify SASTのサイレントインストール 51
4.1.3 Windows以外のプラットフォームでテキストベースモードでのFortify SASTのインストール 53
4.1.4 OpenText Application Security Contentの手動インストール 54
4.2 Dockerを使用したFortify SASTのインストールと実行 54
4.2.1 OpenText SASTをインストールするDockerfileの作成 54
4.2.2 コンテナの実行 55
4.3 Fortify SASTのアップグレード 56
4.4 Fortify SASTのアンインストールについて 56
4.4.1 Fortify SASTのアンインストール 57

4.4.2 Fortify SASTのサイレントアンインストール 57
4.4.3 Windows以外のプラットフォームでテキストベースモードでのFortify SASTのアンインストール 57
4.5 インストール後のタスク 58
4.5.1 インストール後処理ツールの実行 58
4.5.2 プロパティファイルの移行 58
4.5.3 ロケールの指定 58
4.5.4 Fortify Security Contentの更新の設定 59
4.5.5 Application Securityへの接続の設定 59
4.5.6 プロキシサーバ設定の削除 60
4.5.7 信頼された証明書の追加 60
5 分析プロセスの概要 60
5.1 スキャンの基本 61
5.2 変換フェーズ 61
5.3 分析フェーズ 62
5.4 変換フェーズと分析フェーズの検証 62
5.5 問題の深刻度のランク付け 63
6 AIを活用したSASTによる分析 64
6.1 LLMの構成 64
6.1.1 AIを活用したSASTへのAWS Bedrockの使用 64
6.1.2 AIを活用したSASTへのAzureの使用 65
6.1.3 AIを活用したSASTへのGoogle Cloudの使用 66
6.1.4 AIを活用したSASTへのOpenAI APIの使用 66
6.2 データベースへの接続 67
6.3 dbToolの使用 69
6.4 AIを活用したSASTによるサンプル分析 70
6.5 AIを活用したSASTの構成オプション 70
6.6 レート制限 84
6.7 pwtoolを使用した機密性の高い値の暗号化 84
7 Java、Kotlin、およびJSPプロジェクトの分析 85
7.1 Gradleとの統合 85
7.1.1 Gradle統合の使用 85
7.1.2 Gradle統合のトラブルシューティング 86
7.1.3 Gradleプラグインの使用 86
7.2 Mavenとの統合 88
7.2.1 Fortify Mavenプラグインのインストールと更新 88
7.2.2 Fortify Mavenプラグインのインストールのテスト 88
7.2.3 Fortify Mavenプラグインの使用 89
7.3 Bazelとの統合 90
7.3.1 Java Bazelの統合例 90
7.4 Antとの統合 91
7.5 JavaおよびKotlinの手動変換構文 91
7.5.1 Java、Kotlin、およびJSPのコマンドラインオプション 92
7.5.2 Javaのコマンドライン例 95
7.5.3 Kotlinコマンドラインの例 95

7.6 Kotlinスクリプトの分析 96
7.7 KotlinとJavaの変換相互運用性 96
7.8 Javaの警告の処理 96
7.9 Jakarta EE (Java EE)アプリケーションの分析 97
7.9.1 Javaファイルの変換 97
7.9.2 JSPプロジェクト、環境設定ファイル、および展開ディスクリプタの変換 97
7.9.3 Jakarta EE (Java EE)変換の警告 97
7.10 Javaバイトコードの分析 97
7.11 Java、Kotlin、およびJSP変換および分析に関する問題のトラブルシューティング 98
8 Androidプロジェクトの分析 99
8.1 Androidプロジェクト変換の前提条件 99
8.2 Androidコード分析のコマンドライン構文 99
8.3 Androidレイアウトファイルで検出されたフィルタリングの問題 99
9 Groovyコードの分析 99
9.1 Groovy分析の前提条件 100
9.2 Groovyの変換構文 100
10 Scalaコードの分析 100
11 Visual Studioプロジェクトの分析 101
11.1 Visual Studioプロジェクト変換の前提条件 101
11.2 Visual Studioプロジェクトのコマンドライン構文 101
11.3 Visual Studioプロジェクトの変換に関する特殊なケースの処理 102
11.3.1 スクリプトからの変換の実行 102
11.3.2 プレーンな.NETおよびASP.NETプロジェクトの変換 102
11.3.3 C/C++およびXamarinプロジェクトの変換 103
11.3.4 空白を含む設定を持つプロジェクトの変換 103
11.3.5 Visual Studioソリューションの単一プロジェクトの変換 103
11.3.6 複数の実行可能ファイルをビルドするプロジェクトの分析 103
11.4 Visual Studioプロジェクトを変換する別の方法 103
11.4.1 Visual Studioソリューション用の別の変換オプション 103
11.4.2 Fortify SASTを明示的に実行せずに変換する 104
12 JavaScriptおよびTypeScriptコードの分析 105
12.1 ピュアJavaScriptプロジェクトの変換 106
12.2 依存関係の除外 106
12.3 NPM依存関係の除外 106
12.4 NPMの依存関係 107
12.4.1 NPM依存関係の除外の例 107
12.5 HTMLファイルを使用したJavaScriptプロジェクトの変換 108
13 DartおよびFlutterコードの分析 108
13.1 DartおよびFlutter変換の前提条件 108
13.2 DartおよびFlutterのコマンドライン構文 109
13.3 DartおよびFlutterのコマンドライン例 109
14 PythonおよびJupyter Notebookの分析 109
14.1 Bazelとの統合 110
14.1.1 Python Bazelの統合例 110
14.2 Python変換コマンドライン構文 110

14.2.1 Pythonコマンドラインオプション 111
14.2.2 Pythonのコマンドライン例 113
14.3 仮想環境でのPythonの変換 113
14.4 インポート済みのモジュールとパッケージを含める 113
14.5 ネームスペースパッケージを含める 114
14.6 DjangoとFlaskの変換 114
15 iOSおよびXcodeプロジェクトの分析 115
15.1 iOSプロジェクト変換の前提条件 115
15.2 iOSコード分析のコマンドライン構文 115
16 CおよびC++コードの分析 116
16.1 CおよびC++コード変換の前提条件 116
16.2 Makeとの統合 116
16.3 CMakeとの統合 117
16.4 Gradleとの統合 117
16.5 CおよびC++の手動変換構文 117
16.6 C/C++のプリコンパイル済みヘッダファイル 118
16.7 他のコンパイラの使用 118
17 Rustコードの分析 119
17.1 Rust分析の前提条件 119
17.2 Rustの変換構文 119
18 Fortranコードの分析 120
18.1 Fortran分析の前提条件 120
18.2 Fortranの変換構文 120
19 AIエージェント指示ファイルの分析 120
19.1 AIエージェント指示ファイル分析の前提条件 120
19.2 AIエージェント指示ファイルの変換構文 120
20 Goコードの分析 121
20.1 Goコマンドライン構文 121
20.2 Goコマンドラインオプション 121
20.3 カスタムGoビルドタグを含める 123
20.4 依存関係の解決 123
21 PHPコードの分析 124
21.1 PHPコマンドラインオプション 124
22 Perlコードの分析 124
22.1 Perl分析の前提条件 124
22.2 Perlの変換構文 125
23 Rubyコードの分析 125
23.1 Rubyの変換構文 125
24 Adaコードの分析 126
24.1 Ada分析の前提条件 126
24.2 Adaの変換構文 126
25 Delphiコードの分析 126
25.1 Delphi分析の前提条件 126
25.2 Delphiの変換構文 126
26 Elixirコードの分析 127

26.1 Elixir分析の前提条件 127
26.2 Elixirの変換構文 127
27 Erlangコードの分析 127
27.1 Erlang分析の前提条件 128
27.2 Erlangの変換構文 128
28 Luaコードの分析 128
28.1 Lua分析の前提条件 128
28.2 Luaの変換構文 128
29 Kornshellコードの分析 129
29.1 Kornshell分析の前提条件 129
29.2 Kornshellの変換構文 129
30 Salesforce ApexおよびVisualforceコードの分析 129
30.1 ApexおよびVisualforce変換の前提条件 129
30.2 ApexおよびVisualforceのコマンドライン構文 130
31 ABAPコードの分析 130
31.1 ソースファイルのダウンロードについて 130
31.1.1 INCLUDEの処理 131
31.2 移送依頼のインポート 131
31.3 Fortify SASTのお気に入りリストへの追加 131
31.4 Fortify ABAP Extractorの実行 132
31.5 Fortify ABAP Extractorのアンインストール 135
32 COBOLコードの分析 136
32.1 COBOLソースファイルとコピーブックファイルの変換準備 136
32.2 COBOLのコマンドライン構文 137
32.2.1 ファイル拡張子を持たないCOBOLソースファイルの変換 137
32.2.2 任意のファイル拡張子を持つCOBOLソースファイルの変換 137
32.2.3 COBOLコマンドラインオプション 137
32.3 レガシーCOBOL変換の使用(非推奨) 138
32.3.1 レガシーCOBOL変換コマンドラインオプション 138
33 SQLの分析 139
33.1 PL/SQLのコマンドライン例 140
33.2 T-SQLのコマンドライン例 140
34 コードとしてのインフラストラクチャ(IaC)の分析 140
35 JSONの分析 142
36 YAMLの分析 142
37 Dockerfileの分析 142
38 Bashコードの分析 142
38.1 Bash分析の前提条件 143
38.2 Bashの変換構文 143
39 PowerShellコードの分析 143
39.1 PowerShell分析の前提条件 143
39.2 PowerShellの変換構文 143
40 Rコードの分析 144
40.1 R分析の前提条件 144
40.2 Rの変換構文 144

41 Solidityコードの分析 144
42 その他の言語および設定の分析 145
42.1 FlexおよびActionScriptの分析 145
42.1.1 FlexおよびActionScriptコマンドラインオプション 145
42.1.2 ActionScriptのコマンドライン例 147
42.1.3 解決の警告の処理 147
42.2 ColdFusionコードの分析 147
42.2.1 ColdFusionコマンドライン構文 148
42.2.2 ColdFusion (CFML)コマンドラインオプション 148
42.3 ASP/VBScript仮想ルートの分析 148
42.4 Classic ASPのコマンドライン例 150
42.5 VBScriptのコマンドライン例 150
43 ライブラリコードの分析 150
44 シークレットのスキャン 151
44.1 正規表現分析 151
45 PQCの問題のスキャン 152
46 結果の最適化 152
46.1 分析へのスキャンポリシーの適用 152
46.2 フィルタファイルによる問題の除外 154
46.2.1 フィルタファイルの例 157
46.3 フィルタセットを使用した問題の除外 158
46.4 FortifyRemoveコメントを使用したフィルタ 158
46.5 Fortify Java注釈 160
46.5.1 データフローの注釈 160
46.5.2 フィールドと変数の注釈 162
46.5.3 その他の注釈 162
47 パフォーマンスの最適化 163
47.1 ウィルス対策ソフトウェア 163
47.2 ハードウェアに関する考慮事項 163
47.3 チューニングオプション 164
47.4 クイックスキャン 165
47.5 短縮ダイヤルを使用したスキャン速度の設定 166
47.6 コードベースの分割 167
47.7 アナライザと言語の制限 168
47.7.1 アナライザの無効化 168
47.7.2 言語の無効化 168
47.8 FPRファイルの最適化 169
47.8.1 フィルタファイルの使用 169
47.8.2 フィルタセットの使用 169
47.8.3 FPRからのソースコードの除外 170
47.8.4 FPRファイルサイズの削減 170
47.8.5 大きなFPRファイルを開く 171
47.9 長時間実行されているスキャンの監視 172
47.9.1 SCAStateツールの使用 172
47.9.2 JMXツールの使用 173

47.9.2.1 JConsoleの使用 173
47.9.2.2 Java VisualVMの使用 173
48 モバイルビルドセッションの使用 173
48.1 モバイルビルドセッションバージョンの互換性 174
48.2 モバイルビルドセッションの作成 174
48.3 モバイルビルドセッションのインポート 174
49 トラブルシューティング 175
49.1 終了コード 175
49.2 メモリのチューニング 176
49.2.1 Javaヒープの枯渇 176
49.2.2 ネイティブヒープの枯渇 176
49.2.3 スタックオーバーフロー 177
49.3 複雑な関数のスキャン 177
49.3.1 Dataflow Analyzerのリミッタ 178
49.3.2 制御フローおよびNullポインタアナライザのリミッタ 178
49.4 問題の非決定性 179
49.5 ログファイルの場所の確認 179
49.6 ログファイルの設定 180
49.7 問題の報告と機能拡張の要求 181
50 コマンドライン参照 181
50.1 ファイルとディレクトリの指定 181
50.2 ディレクティブ 182
50.2.1 LIMライセンスディレクティブ 184
50.3 変換オプション 185
50.4 分析オプション 188
50.5 出力オプション 192
50.6 その他のオプション 195
51 環境設定オプション 197
51.1 プロパティファイル 198
51.1.1 プロパティファイルの形式 198
51.1.2 設定の上書き 198
51.2 fortify-sca.properties 199
51.2.1 変換と分析フェーズのプロパティ 200
51.2.2 正規表現分析のプロパティ 210
51.2.3 LIMライセンスのプロパティ 211
51.2.4 ルールのプロパティ 213
51.2.5 JavaおよびKotlinのプロパティ 215
51.2.6 Visual StudioおよびMSBuildプロジェクトのプロパティ 218
51.2.7 JavaScriptおよびTypeScriptのプロパティ 219
51.2.8 Pythonのプロパティ 221
51.2.9 Goのプロパティ 223
51.2.10 Rubyのプロパティ 224
51.2.11 COBOLのプロパティ 224
51.2.12 PHPのプロパティ 226
51.2.13 ABAPのプロパティ 226

51.2.14 FlexおよびActionScriptのプロパティ 226
51.2.15 ColdFusion (CFML)のプロパティ 227
51.2.16 SQLのプロパティ 228
51.2.17 出力のプロパティ 228
51.2.18 モバイルビルドセッション(MBS)のプロパティ 231
51.2.19 プロキシプロパティ 231
51.2.20 ログプロパティ 232
51.2.21 デバッグのプロパティ 232
51.3 fortify-sca-quickscan.properties 234
51.4 fortify-rules.properties 237
52 コマンドラインツール 246
52.1 OpenText Application Security Contentの更新について 247
52.1.1 OpenText Application Security Contentの更新 247
52.1.2 fortifyupdateコマンドラインオプション 248
52.2 SCAStateを使用したスキャンステータスの確認 251
52.2.1 SCAStateコマンドラインオプション 251
53 インストールおよびアップグレードに関する注意 253

ユーザガイド

このセクションでは、OpenText™ Fortify SASTを使用して、ほとんどの主要なプログラミングプラットフォームでコードをスキャンする方法について説明します。このセクションは、セキュリティ監査とセキュアコーディングを担当するユーザを対象にしています。

1. 変更ログ

次の表は、このガイドに加えられた変更をまとめたものです。改訂版は、変更が製品の機能に影響を与える場合に、ソフトウェアリリース間で発行されます。

ソフトウェアリリース/ ドキュメントのバージョン	変更点

26.4.0	追加: • 新しいAlmaLinux、SUSE Linux Enterprise Server、およびmacOSのバージョン。詳細については、「サポートされているプラットフォームとアーキテクチャ」を参照してください。 • 新しいNet (Core)、C#、Go、Kotlin、Swift、およびT-SQLサーバのバージョン。詳細については、「言語の互換性」を参照してください。 • gcc、Swift、LLVM Clangの新バージョンのサポート。詳細については、「サポートされているコンパイラ」を参照してください。 • 新しいMSBuild、dotnet、およびxcodeのバージョン。詳細については、「サポートされているビルドツール」を参照してください。 • AIを活用したSASTをサポートする言語としてのKornShell。詳細については、「Kornshellコードの分析」を参照してください。 • 正規表現分析中に最小化されたJavaScriptファイルとTypeScriptファイルをスキャンするための `-regex-scan-minified` オプションと `com.fortify.sca.regex.ScanMinifiedJS` プロパティ。詳細については、「正規表現分析のプロパティ」を参照してください。 • 環境変数を使用してデータベース接続プロパティを構成するためのサポート。詳細については、「データベースへの接続」を参照してください。 • 異なるモデルが使用された場合にキャッシュされたLLM結果を再生成するための `com.fortify.sca.ai.cache.missOnNewModel` プロパティ。詳細については、「AIを活用したSASTの構成オプション」を参照してください。 更新: • 従来のCOBOLアナライザを使用するには、 `-cobol-legacy` オプションを指定するか、 `com.fortify.sca.CobolLegacy=true` プロパティを設定します。詳細については、「レガシーCOBOL変換」を参照してください。 • Application Default Credentials (ADC)を含めるための、AIを活用したSASTにおけるGoogle Cloud認証ガイダンス。詳細については、「AIを活用したSASTへのGoogle Cloudの使用」を参照してください。 • 組み製品名の変更 削除: • macOS 15、26.3、26.4およびCPU arch x64のサポート • .Net Framework 4.6、Java (Androidを含む) 7、およびT-SQLサーババージョン2005、2008、および20012のサポート • Maven 3.8.x、xcode 16.x、Bazel 6.xのサポート

	• compiler gcc 14のサポート • compiler LLVM Clang 17.0.6のサポート

26.3.0	追加: • AIを活用したSASTを対象とした、Microsoft Azureを介した新しいClaudeモデル (「サポート対象のLLM」を参照) • AIを活用したSASTを対象としたサポートプロバイダーとしてGoogle Cloudを追加 (「サポート対象のLLM」と「AIを活用したSASTへのGoogle Cloudの使用」を参照) • 必要な権限があるIAMロールを使用するAmazon EC2インスタンスでスキャンを実行し、AWS認証用のBedrock Bearerトークンを指定するためのサポートを追加 (「AIを活用したSASTへのAWS Bedrockの使用」を参照) • Azure Foundryリソース名を使用してMicrosoft Foundry展開用にAzure OpenAIエンドポイントを構成するためのサポートを追加 (「AIを活用したSASTへのAzureの使用」を参照) • `com.fortify.sca.ai.model` プロパティ用のMicrosoft Azureを介した新しいClaudeモデル名のサポートを追加 (「AIを活用したSASTの構成オプション」を参照) • AWSベンダー構成プロパティに新しい `com.fortify.sca.ai.aws.inferenceProfile` および `com.fortify.sca.ai.aws.bearerTokenBedrock` プロパティを追加 (「AIを活用したSASTの構成オプション」を参照) • Azureベンダー構成プロパティに新しい `com.fortify.sca.ai.azure.resource` プロパティを追加 (「 AIを活用したSASTの構成オプション」を参照) • macOS®istered trademark;の新しいバージョンを追加 (「サポートされているプラットフォームとアーキテクチャ」を参照) • ファイル構成プロパティのセクションを追加 (「AIを活用したSASTの構成オプション」を参照) • GoとSwiftの新しいバージョンを追加 (「言語の互換性」を参照) • Gradle(ビルド統合)とxcodebuildの新しいバージョンを追加 (「サポートされるビルドツール」を参照) • LLMV Clang、Apple Clang、Swiftc用の新しいコンパイラバージョンを追加 (「サポートされているコンパイラ」を参照) • C/C++コードの分析時のカスタムコンパイラの使用に関するページを追加 (「他のコンパイラの使用」を参照) • `com.fortify.sca.fileextensions.<language>` プロパティの新しい拡張子タイプを追加 (「変換と分析フェーズのプロパティ」を参照) • 名前がピリオドで始まるファイルとディレクトリが非表示として扱われるプラットフォームでも、名前がピリオドで始まるファイルとディレクトリがデフォルトで含まれるのを回避するための新しい

	`com.fortify.LegacyHiddenGlobSyntax` プロパティを追加 (「変換と分析フェーズのプロパティ」と 「ファイルとディレクトリの指定」を参照) 更新: • 組み製品名の変更 • *OpenText SAST*の記載をすべてFortify SASTに変更 • `com.fortify.sca.ai.model` プロパティでのAWS推論プロファイルIDまたは推論プロファイルARNの指定に関する説明を更新 (「AIを活用したSASTの構成オプション」を参照) • `-cp <paths>` | `-classpath <paths>` プロパティの説明を更新 (「Java、Kotlin、およびJSPコマンドラインオプション」を参照)。 削除: • CentOS、Red Hat®istered trademark; Enterprise Linux®istered trademark; 7.2、Ubuntu®istered trademark; 20.04.1 LTS、Microsoft Windows®istered trademark; Server 2019を削除 • `com.fortify.sca.FilterSet` プロパティをfortify-sca-quickscan.propertiesから削除

26.2.0	追加: • AIを活用したSASTに対応した新しいLLMプロバイダー(サポート対象のLLM) • AIを活用したSASTを使用してCOBOL、Fortran、AIエージェント指示ファイルを分析するためのサポートを追加しました (「AIを活用したSASTの言語の互換性」を参照)。 • 「COBOLコードの分析」、「Fortranコードの分析」、「AIエージェントルールファイルの分析」の各セクションを追加しました。 • AIを活用したSASTを使用するためのデータベース要件に関するセクション(データベース要件) • 「AIを活用したSASTへのAzureの使用」に関するセクション • 「AIを活用したSASTへのOpenAI APIの使用」に関するセクション • AzureおよびOpenAIのベンダー構成プロパティ (「AIを活用したSASTの構成オプション」を参照) • 「pwtoolを使用した機密性の高い値の暗号化」のAzureとOpenAIの機密性の高いプロパティ • C++、Kotlin、Swift、PHPの新しいバージョンを追加しました (「言語の互換性」を参照) • MSBuildとxcodebuildの新しいバージョンを追加しました (「サポートされるビルドツール」を参照) • Microsoft Windows®istered trademark;およびmacOS®istered trademark;の新しいバージョンを追加しました (「サポートされているプラットフォームとアーキテクチャ」を参照) 更新: • Akkaライセンスファイルに関する注意事項を追加しました (「Scalaコードの分析」を参照) 削除: • Microsoft Windows®istered trademark;バージョン10、macOSバージョン14、 IBM AIXバージョン7.1を削除しました • .NET (Core)バージョン2.x～4.xを削除しました • .NET Frameworkバージョン2.0～4.5を削除しました • C#バージョン5を削除しました • Swiftバージョン5.10～6.0を削除しました • MSBuildバージョン14.xを削除しました • Xcodebuildバージョン15.3、15.4を削除しました • Rubyのローカル変換を削除しました (「Rubyコードの分析」を参照) • `com.fortify.sca.ruby.legacy.enabled` プロパティが `fortify-sca.properties` ファイルから削除されました (「Rubyのプロパティ」を参照) • 「*Rubyコマンドラインオプション*」、「*ライブラリの追加*」、「*Gemパスの追加*」の各トピックがこのドキュメントから*削除されました*

	トピック「*外部JavaScriptまたはHTMLを変換に含める*」がこのドキュメントから削除されました • `fortify-sca-quickscan.properties` ファイル内の `com.fortify.sca.FilterSet` プロパティが非推奨となり、次回のリリースで `fortify-sca-quickscan.properties` ファイルから削除されます
26.1.0	追加: • AIを活用したSAST (「AIを使用した分析」を参照) • 新しいPythonバージョンを追加しました (「言語の互換性」を参照) • 新しいxcodebuildバージョンを追加しました (「サポートされるビルドツール」を参照) • AI支援型分析でサポートされる言語のフレームワークを追加しました (「ライブラリ、フレームワーク、およびテクノロジ」を参照) 削除: • Antバージョン1.9.xおよびXcodeビルドバージョン15.3～15.4を削除しました (「サポートされるビルドツール」を参照)

2. はじめに

このセクションでは、次のトピックについて説明します。

- OpenText Fortify SAST
- ライセンス
- 有効期限が切れたライセンスの更新
- OpenText Application Security Content
- Fortify ScanCentral SAST
- OpenText Application Security Tools
- サンプルプロジェクト
- 関連ドキュメント

2.1. OpenText Fortify SAST

Fortify SAST (Fortify Static Code Analyzer)は、さまざまな言語でセキュリティ固有のコーディングルールおよびガイドラインの違反を検索する一連のソフトウェアセキュリティアナライザです。Fortify SASTでは、よりセキュアなソフトウェアを提供し、セキュリティコードレビューの効率性、一貫性、および完全性を向上させるのに役立つ分析情報が生成されま す。お客様固有のセキュリティルールを組み込むことのできる設計になっています。

サポートされている言語、ライブラリ、コンパイラ、およびビルドツールのリストについては、「システム要件」を参照してください。

Fortify　SASTを使用してアプリケーションを分析するには、次の方法があります。

- 次のSecure Code Pluginsのいずれかを使用して、IDEから直接分析を実行します: Visual Studio用のFortify Extension、Eclipse用のFortify Plugin、およびIntelliJ IDEAおよびAndroid Studio用のFortify Analysis Plugin)。この分析は、Fortify Audit Workbenchを使用して実行することもできます。
  セキュリティ脆弱性分析の結果をIDEおよびFortify Audit Workbenchで表示したり、結果をFortify Software Security Centerにアップロードすることもできます。ツールの説明については、「OpenText Application Security Tools」を参照してください。

- 分析をビルドシステムに統合するか、またはコマンドラインから分析を実行します。このガイドでは、分析のこの実行方法を主に説明します。

2.1.1. アナライザについて

Fortify SASTは、8つの脆弱性アナライザ(Buffer、Configuration、Content、Control Flow、Dataflow、Null Pointer、Semantic、およびStructural)で構成されています。各アナライザでは、実行された分析に対応するタイプに必要な情報を提供するために特別にカスタマイズされた別のタイプのルールが受諾されます。ルールは、ソースコード内のセキュリティの脆弱性や安全でない状態が発生する可能性がある要素を特定する定義です。次の表では、各アナライザについて説明します。

アナライザ	説明(Description)
Dataflow	Dataflow Analyzerでは、テイントデータ(ユーザ制御入力またはプライベートデータ)の潜在的に危険な使用が発生する潜在的な脆弱性が検出されます。Dataflow Analyzerは、プロシージャ間テイント伝播分析を使用して、ユーザ入力(またはプライベートデータ)のサイトから、アプリケーションを通って、危険な関数呼び出しや操作に至るデータの流れを検出します。たとえば、Dataflow Analyzerは、ユーザが制御する入力文字列がHTML (クロスサイトスクリプティング)を動的に生成するかどうかを検出し、ユーザが制御する文字列がSQLクエリを構成するかどうか(SQLインジェクション)を検出します。
Control Flow	Control Flow Analyzerでは、一連の危険な操作が検出されます。プログラムで制御フローパスを分析すると、Control Flow Analyzerで一連の操作が特定の順序で実行されているかどうかが判断されます。たとえば、Control Flow Analyzerは、チェックの時刻/使用時刻の問題や競合状態を検出し、XMLリーダーなどのユーティリティが使用前に適切に設定されているかどうかをチェックします。
Buffer	Buffer Analyzerでは、バッファに保持できる以上のデータの書き込みまたは読み取りが発生するバッファオーバーフローの脆弱性が検出されます。バッファはスタックで割り当てられるか、ヒープで割り当てられます。Buffer Analyzerでは、制限付きのプロシージャ間分析を使用して、バッファオーバーフローが発生する原因になる状態であるかどうかが判断されます。バッファへの実行パスが原因でバッファオーバーフローが発生する場合は、 Fortify SASTでバッファオーバーフローの脆弱性としてレポートされ、オーバーフローの原因になる可能性がある変数が指摘されます。バッファオーバーフローの発生原因となる変数の値が汚染(ユーザ制御)されている場合は、その値もFortify SASTでレポートされ、どのように変数が汚染されているのかを示すデータフロートレースが表示されます。Buffer Analyzerは、バッファアンダーリード状態およびバッファアンダーフロー状態も検出します。
Structural	Structural Analyzerでは、プログラムの構造または定義の潜在的に危険な欠陥が検出されます。Structural Analyzerでは、変数および関数の宣言と使用の両方を含む幅広い範囲が網羅されるため、プログラムの構造を理解することで、検査による検出が難しい場合が多いセキュアなプログラミング手法や技術の違反も特定されます。たとえば、Structural Analyzerは、ハードコードされたシークレット、コード内でのCookieの誤設定、および暗号化の弱点を検出します。

アナライザ	説明(Description)
Configuration	Configuration Analyzerでは、アプリケーション展開環境設定ファイルの間違い、弱点、およびポリシー違反が検索されます。たとえば、Configuration Analyzerでは、Webアプリケーションでユーザセッションに適切なタイムアウトがチェックされます。Configuration Analyzerでは、正規表現分析も実行されます(「正規表現分析」を参照)。
Semantic	Semantic Analyzerでは、プロシージャ内レベルで関数とAPIの潜在的に危険な使用が検出されます。
Content	Content Analyzerでは、HTMLコンテンツのセキュリティ問題とポリシー違反が検索されます。Content Analyzerでは、静的なHTMLページに加えて、動的なHTMLを含むファイル(PHP、JSP、従来のASPファイルなど)でも、これらのチェックが実行されます。
Null Pointer	Null Pointer Analyzerでは、null値が割り当てられたポインタ変数の逆参照が検出されます。Null Pointer Analyzerの検出は、プロシージャ内レベルで実行されます。問題は、null割り当て、逆参照、およびこれらの間のすべてのパスが単一の関数内で発生した場合にのみ検出されます。

2.2. ライセンス

Fortify SASTでは、セキュリティ分析の変換フェーズと分析(スキャン)フェーズの両方を実行するためにライセンスが必要です(これらのフェーズの詳細については、「分析プロセス」を参照)。

ご使用の製品のFortifyライセンスファイルをソフトウェアライセンスおよびダウンロード(SLD)ポータルからダウンロードする必要があります。カスタマサポートがアクセス用に提供した資格情報を使用します。

Fortify SASTをインストールするには、Fortifyライセンスファイル(`fortify.license`)が必要です。オプションで、Fortify License and Infrastructure Managerを使用してFortify SASTの同時ライセンスを管理できます。LIMで管理される同時ライセンスを使用すると、複数のFortify SASTのインストールで単一のライセンスを共有できます。Fortify SASTのライセンスでLIMを設定する方法については、『*OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド*』を参照してください。Fortify SASTからLIMライセンスを管理する方法については、「LIMライセンスディレクティブ」を参照してください。



Note

Fortify SASTの同時ライセンスを管理するためにOpenText™ Fortify License and Infrastructure Manager (LIM)を使用するには、LIMバージョン21.2.0以降が必要です。

2.3. 有効期限が切れたライセンスの更新

Fortify SASTのライセンスは1年ごとに有効期限が切れます。

有効期限が切れたライセンスを更新するには:

- 更新されたFortifyライセンスファイルを、Fortify SASTがインストールされているルートディレクトリに入れます。

有効期限が切れたLIMで管理される同時ライセンスを更新する方法については、『*OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド*』を参照してください。

2.4. OpenText Application Security Content

Fortify SASTでは、ルールのナレッジベースを使用して、静的分析用のコードベースにセキュアなコーディング標準が強制的に適用されます。OpenText Application Security Contentは、変換と分析の両方に必要です。Fortify SASTのインストール時に、セキュリティコンテンツをダウンロードしてインストールできます(「Fortify SASTのインストール」を参照)。また、インストール後のタスクとしてfortifyupdateコマンドラインツールを使用して、OpenText Application Security Contentをダウンロードしたり、あらかじめダウンロードしておいたものをインポートしたりすることもできます(「OpenText Application Security Contentの手動インストール」を参照)。

OpenText Application Security Contentは、Fortify Secure Coding Rulepacksおよび外部メタデータで構成されます。

- Fortify Secure Coding Rulepacksには、一般的な言語およびパブリックAPIに対する一般的なセキュアコーディングのイディオムが記述されています。
- 外部メタデータには、Fortifyカテゴリから代替カテゴリ(CWE、OWASP Top 10、PCIなど)へのマッピングが含まれています。

OpenTextは、Fortify SASTとFortify Secure Coding Rulepacksの機能に追加する、カスタムルールを記述する機能を提供します。たとえば、場合によっては、専有セキュリティガイドラインを適用したり、すでにFortify Secure Coding Rulepacksの対象ではないサードパーティのライブラリや事前コンパイルされたその他のバイナリを使用するプロジェクトを分析したりする必要があります。また、外部メタデータをカスタマイズして、さまざまな分類体系(内部アプリケーションのセキュリティ基準や追加のコンプライアンス義務など)にFortifyの問題をマップすることもできます。独自のカスタムルールまたはカスタムの外部メタデータを作成する方法については、『OpenText™ Static Application Security Testingカスタムルールガイド』を参照してください。

OpenText™ Fortify SASTには、カスタムルールやルールパックの作成、修正、および検証に役立つFortify SAST Rules Skillも含まれています。このスキルは、オーサリングルールXMLだけでなく、データフロー、構造、制御フロー、構成、テイント分析ルールの開発などのタスクをサポートします。

セキュリティコンテンツを定期的に更新することが推奨されています。`fortifyupdate`を使用すると、最新のセキュリティコンテンツを取得できます。詳細については、「セキュリティコンテンツの更新」を参照してください。

2.5. Fortify ScanCentral SAST

OpenText™ ScanCentral SASTを使用すると、Fortify SASTの分析フェーズをビルドコンピュータから、この目的のためにプロビジョニングされたコンピュータのコレクションにオフロードすることでリソースを管理できます。ほとんどの言語では、Fortify ScanCentral SASTで変換フェーズと分析(スキャン)フェーズの両方を実行できます。Fortify Software Security Centerのユーザは、FPRファイルをサーバに直接出力するようにFortify ScanCentral SASTに指示できます。Fortify SASTのインストール時にFortify ScanCentral SASTクライアントをインストールすることもできます。

次の2つの方法のいずれかでコードを分析できます。

- Fortify ScanCentral SASTの変換でサポートされている言語でアプリケーションが記述されている場合は、分析の変換フェーズと分析(スキャン)フェーズをFortify ScanCentral SASTにオフロードできます。
- ローカルビルドコンピュータ上で変換フェーズを実行し、モバイルビルドセッション(MBS)を生成します。MBSファイルを使用して、Fortify ScanCentral SASTでスキャンを開始します。このプロセスでは、ビルドコンピュータを解放することに加えて、必要に応じてリソースを追加することで、ビルドプロセスを中断することなく、システムを拡張することができます。MBSの詳細については、「モバイルビルドセッション」を参照してください。

変換でサポートされている特定の言語と、Fortify ScanCentral SASTの設定および使用方法については、『*OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド*』を参照してください。

2.6. OpenText Application Security Tools

OpenTextでは、Fortify SAST、Fortify ScanCentral SAST、およびFortify Software Security Centerと統合するアプリケーションとツール(Secure Code Pluginsを含む)が用意されています。次の表では、OpenText Application Security Toolsインストーラを使用してインストールできるアプリケーションについて説明します。OpenText Application Security Toolsのインストール方法については、『*OpenText™Application Security ツールガイド*』を参照してください。

アプリケーション	説明(Description)
OpenText™ Fortify Audit Workbench	開発者がセキュリティ上の欠陥を迅速に修正できるように分析結果を整理、調査、および優先順位付けするのに役立つグラフィカルユーザインタフェースを提供するアプリケーション。
OpenText™ Fortify Plugin for Eclipse	プロジェクトのコードベース全体をスキャンして分析し、Eclipse IDEからJavaコードの脆弱性を特定するソフトウェアセキュリティルールを適用する機能を追加します。結果とともに、個々のセキュリティ問題の説明とそれらの解消に関する提案が表示されます。
OpenText™ Fortify Analysis Plugin for IntelliJ IDEAおよびAndroid Studio	プロジェクトのコードベース全体でスキャンを実行し、IntelliJ IDEAおよびAndroid Studioからコード内の脆弱性を識別するソフトウェアセキュリティルールを適用する機能を追加します。
OpenText™ Fortify Extension for Visual Studio	ソリューションおよびプロジェクトのセキュリティ脆弱性をスキャンして見つけ、Visual Studioにスキャン結果を表示する機能を追加します。結果には、見つかった問題のリスト、各問題が表す脆弱性のタイプの説明、それらの修正方法に関する提案が含まれます。この拡張機能には、Fortify Software Security Centerサーバに保存された監査結果を使用する修正機能も含まれています。
OpenText™　Fortifyカスタムルールエディタ	カスタムルールを作成および編集するためのアプリケーション。
Fortify Scan Wizard	(ローカルまたはFortify ScanCentral SASTを使用してリモートで)コードをスキャンするスクリプトを準備し、必要に応じて結果をFortify Software Security Centerにアップロードできるグラフィカルユーザインタフェースを提供します。
BIRTReportGenerator ReportGenerator	FPRファイルから問題レポート(BIRT)およびレガシーレポートを生成するコマンドラインツール。

2.7. サンプルプロジェクト

OpenTextでは、個別にダウンロードできるサンプルプロジェクトが `OpenText_SAST_Fortify_Samples_<version>.zip` パッケージで提供されています。

このZIPファイルには、 `basic` ディレクトリと `advanced` ディレクトリの2つが含まれています。各コードサンプルには、Fortify SASTでコードをスキャンしてその結果をFortify Audit Workbenchに表示する方法について説明する `README.txt` ファイルが含まれています。

`basic` ディレクトリには、簡単な言語固有のコードサンプルのセットが含まれています。 `advanced` ディレクトリには、より高度なサンプルが含まれています。

2.8. 関連ドキュメント

このトピックでは、OpenText Application Security Software製品に関する情報を提供しているドキュメントについて説明します。

すべての製品

以下のドキュメントには、すべての製品に関する一般情報が記載されています。特に明記されている場合を除き、これらのドキュメントは各製品の製品マニュアルのWebサイトで利用できます。

ドキュメント/ファイル名	説明(Description)
OpenText Application Security Softwareについて appsec-docs-n-<*version*>.pdf	このドキュメントでは、OpenText Application Security Softwareのドキュメントにアクセスする方法について説明しています。 **Note** このドキュメントは、製品のダウンロードにのみ含まれています。
OpenText Application Security Softwareリリースノート appsec-rn-<*version*>.pdf	このドキュメントでは、OpenText Application Security Softwareのこのリリースで行われた変更の概要と、他の製品ドキュメントには記載されていない重要な情報について説明します。

Fortify SAST

以下のドキュメントには、Fortify SAST (Fortify Static Code Analyzer)に関する情報が記載されています。特に明記されている場合を除き、これらのドキュメントは、製品マニュアルのWebサイト(www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools)で入手できます。

ドキュメント/ファイル名	説明(Description)
OpenText™ Fortify SASTユーザガイド sast-ugd-<*version*>.pdf	このドキュメントでは、多くの主要なプログラミングプラットフォームにFortify SASTをインストールし、コードをスキャンするために使用する方法について説明します。これは、セキュリティ監査とセキュアコーディングを担当するユーザを対象にしています。
OpenText™ Fortify SASTカスタムルールガイド sast-cr-ugd-<*version*>.zip	このドキュメントでは、Fortify SASTのカスタムルールを作成するために必要な情報について説明します。このガイドには、ルール作成の概念を実際のセキュリティ問題に適用する例が含まれています。 **Note** このドキュメントは、製品のダウンロードにのみ含まれています。
OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド lim-ugd-<*version*>.pdf	

OpenText Application Security Tools

次のドキュメントには、OpenText Application Security Toolsに関する情報が記載されています。これらのドキュメントは、製品ドキュメントのWebサイト(https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools)で入手できます。

ドキュメント/ファイル名	説明(Description)
OpenText™ Application Security ツールガイド sast-tgd-<*version*>.pdf	このドキュメントでは、Application Security Toolsのインストール方法について説明します。Fortify SASTを使用してコードのスキャン、分析結果の確認、分析結果ファイルの操作などを行うことのできるアプリケーションとコマンドラインツールの概要を提供します。
OpenText™ Fortify Audit Workbench ユーザガイド awb-ugd-<*version*>.pdf	このドキュメントでは、Fortify Audit Workbenchを使用して、ソフトウェアプロジェクトをスキャンして分析結果を監査する方法について説明します。このガイドには、バグトラッカとの統合方法、レポートの作成方法、共同監査の実行方法も記載されています。
OpenText™ Fortify Plugin for Eclipse ユーザガイド ep-udg-<*version*>.pdf	このドキュメントでは、Fortify Plugin for Eclipseをインストールして、コードを分析および監査するために使用する方法について説明しています。
OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studioユーザガイド iap-udg-<*version*>.pdf	このドキュメントでは、Fortify Analysis Plugin for IntelliJ IDEA and Android Studioをインストールして、コードを分析し、必要に応じて分析結果をFortify Software Security Centerにアップロードするために使用する方法について説明しています。
OpenText™ Fortify Extension for Visual Studio ユーザガイド vse-ugd-<*version*>.pdf	このドキュメントでは、Fortify Extension for Visual Studioをインストールおよび使用して、コードを分析、監査、修復し、ソリューションとプロジェクトのセキュリティに関する問題を解決する方法について説明します。

3. システム要件

このセクションでは、システム要件、サポートされている言語、ビルドツール、コンパイラ、およびFortify SASTソフトウェアパッケージの取得方法について説明します。

- ハードウェア要件
- サポートされているプラットフォームとアーキテクチャ
- ソフトウェア要件
- AIを活用したSASTの要件
- 言語の互換性
- サポートされるビルドツール
- サポートされているコンパイラ
- OpenText Application Security Content
- 仮想マシンのサポート
- ソフトウェアの取得
- ソフトウェアのダウンロードの確認

3.1. ハードウェア要件

CPU、メモリ、ストレージなどのシステムリソースは、プロジェクトの全体的な分析時間に大きな影響を与える可能性があります。全体的なコードサイズ、構成、言語、コードの複雑さなど、ターゲットプロジェクトのコードベースに関連する多くの要因に依存します。次のガイドでは、多数の異なる実際のアプリケーションをスキャンした経験に基づいて、一般的な開始点について説明します。

アプリケーションのサイズと複雑さ	CPUコア数	RAM (GB)	説明(Description)
小さくシンプル	4	16	サーバまたはデスクトップ上で実行される小規模なスタンドアロンシステム(バッチジョブやコマンドラインツールなど)。以下を含みます: • 10,000未満の関数
小さくシンプル (動的言語)	8	32	複雑なコンピュータモデルで動作するスタンドアロンシステム(税額計算システムやスケジューリングシステムなど)。以下を含みます: • 10,000未満の関数 • 主にJavaScript、TypeScript、Python、PHP、Rubyなどの動的言語
Medium	16	64–128	トランザクションデータ処理を備えた3階層ビジネスシステム(財務システムや商用Webサイトなど)。以下を含みます: • 100,000未満の関数 • 100万行以上のコード
大規模で複雑	32	256	コンテンツを配信するシステム(アプリケーションサーバ、データベースサーバ、コンテンツ管理システムなど)。以下を含みます: • 100万以上の関数 • 数百万行のコード

Fortify SASTは、システムで利用可能なすべてのCPUコアを利用して、大規模なプロジェクトのスキャン時間を短縮します。Fortify SASTを実行すると、スキャンに使用できるハードウェアの全リソースが使用されると想定されるため、Fortify SASTの実行時にCPUを大量に消費する他のプロセスは実行しないようにしてください。

システムリソースの調整に関するその他の考慮事項:

- **仮想システム**—仮想化では、ワークロード内の未使用のリソースを特定し、他のワークロードに再割り当てすることで、ハードウェアリソースをスケールできます。Fortify SAST分析は一般的に長期にわたるリソース集約型プロセスであるため(特に、大規模かつ複雑なプロジェクトで)、リソースのスワッピングを減らすために、仮想化層での専用リソースを推奨しています。

- **CPU**—全体的な処理能力は、分析に必要な合計時間に大きな影響を与える可能性があります。高速クロック速度(コアあたりのGHz)を備える高性能プロセッサを推奨しています。システムで使用可能なコア数と必要なメモリ容量との間には相関関係があることに注意が必要です。
- **メモリ**—最適なパフォーマンスを得るために必要なメモリの量を決定する方法の詳細については、「メモリチューニング」を参照してください。JavaScript、TypeScript、Python、PHP、Rubyなどの動的言語の分析では、スキャンフェーズで他の言語よりも多くのメモリが必要です。
- **ディスクI/O**—プロジェクトの変換とスキャンは、大量のデータをシリアル化し、より高速なストレージから利益を得るI/O集約型のアクティビティです。可能な限り高速なSSDストレージで分析を実行することが推奨されています。
- **関数の数**— `-debug` オプションを使ってスキャンを実行し、サポートログファイルで `NameTable.funs: ###` の値が最後に出現した箇所を探すことで、分析中にモデル化された関数の数を確認できます。

3.1.1. サンプルスキャン

これらのサンプルスキャンメトリクスは、クラシックスキャンポリシーを適用した専用仮想マシン上で、Fortify SASTバージョン26.3を使用して収集されました。これらのスキャンは、OpenText Application Security Content 26.1 Updateで実行されました。次の表は、いくつかの一般的なオープンソースプロジェクトで期待できるスキャン時間を示しています。

言語	プロジェクト名	変換時間 (mm:ss)	分析(スキャン)時間 (mm:ss)	問題の合計数	LOC	システム設定
.NET (C#)	SharpZipLib	00:55	14:37	632	31843	Windows Server 2022 (4個のCPUコアと32GBのRAM)
ABAP	abap2UI5	00:11	00:48	11	59141	Linux (alma 9) (8個のCPUコアと64GBのRAM)
C/C++	nasm 0.98.38	00:34	02:36	796	35997	8個のCPUと32GBのRAMを搭載したLinux (Centos 7)
Java	WebGoat 8	0:14	01:05	457	23662	Linux (alma 9) (8個のCPUコアと64GBのRAM)
Java	WordPress for Android	00:07	01:24	777	35377	Linux (alma 9) (8個のCPUコアと64GBのRAM)
JavaScript	three.js	04:39	11.22	288	636355	Linux (Alma 9) (4個のCPUコアと32GBのRAM)
PHP	CakePHP	00:15	4:54	5190	136621	Linux (alma 9) (8個のCPUコアと64GBのRAM)
PHP	phpBB3	01:03	03:04	1495	206802	Linux (alma 9) (8個のCPUコアと64GBのRAM)

Python 3	numpy-1.13.3	1:56	07:14	430	563487	Linux (alma 9) (8個のCPUコアと64GBのRAM)
Swift	MediaBrowser	00:09.39	00:20.2	25	17699	4個のCPUと16 GBのRAMを搭載したmacOS
TypeScript	rxjs-7.8.1	02:14	07:19	56	204587	4個のCPUと32GBのRAMを搭載したLinux (Alma 9)

3.2. サポートされているプラットフォームとアーキテクチャ

Fortify　SASTは、次の表に示すプラットフォームとアーキテクチャをサポートしています。

オペレーティングシステム	プラットフォーム	配布パッケージとバージョン	メモ
Microsoft Windows®istered trademark;	x64	Windows 11 Windows Server 2022、2025	
Linux®istered trademark;	x64 ARM	• AlmaLinux 8.6, 9.x, 10.x • Red Hat®istered trademark; Enterprise Linux®istered trademark; 8.x (8.2以降)、9.x、10.x • SUSE®istered trademark; Linux®istered trademark; Enterprise Server 15、16 • Ubuntu®istered trademark;22.04.1 LTS	
macOS®istered trademark;	M series ARM	26, 27	Xcodeバージョン26.2以降にはmacOS®istered trademark; 15.6以降が必要です。
IBM®istered trademark; AIX®istered trademark;	Power ISA	7.3	**Important** IBM XL C/C++ for AIX 16.1ランタイム環境パッケージがインストールされている必要があります。

3.3. ソフトウェア要件

Fortify　SASTのインストールには、ソフトウェアが必要とする組み込みOpenJDK/JREバージョン21が含まれています。Java 21をインストールする必要はありません。

Note

Fortify SASTは、インストールにバンドルされているJREで動作確認およびサポートされています。Fortify SASTは他のJava 21 JRE実装と互換性がある場合がありますが、OpenTextでは互換性を保証しておらず、バンドルされていないJREを使用した場合に直接発生する問題のサポートを提供していません。

社内ポリシーとセキュリティ要件を満たすために、組織でJREのアップグレードが必要になることがある場合をOpenTextでは認識しています。バンドルされていないJREを使用する際に問題が発生した場合は、カスタマーサポートに連絡する前に、バンドルされているJREに戻し、その問題がJRE構成に固有であるかどうかを確認します。

Fortify SASTを使用するには、Fortify SASTインストールディレクトリに対する読み込みおよび書き込み権限が必要です。

次の表は、特定のプロジェクトタイプの分析に必要なソフトウェア要件を示しています。

言語	ソフトウェア	オペレーティングシステム	変換要件	スキャン要件
Visual Studio、MSBuild、または.NETプロジェクト	.NET Framework 4.8以降(MSBuildのみ)	Windows	はい	なし
	.NET SDK 10.0	Windows, Linux	はい	なし
ABAP®istered trademark;/BSP	Fortify ABAP Extractorは、ABAP Platform 2023 / ABAPバージョン7.58で動作するシステム上でサポートされています。	All	なし	なし
Bicep	.NET SDK 10.0	Windows, Linux	なし	はい
Scala	Akkaコンパイラプラグインは、Maven Central Repositoryで利用できます。	All	はい	なし
Solidity	関連するSolidityコンパイラのバージョン スキャンマシンがインターネットに接続されている場合、Fortify SASTは必要なSolidityコンパイラをダウンロードしようとします。 このような場合、スキャン前にスキャンマシンにSolidityコンパイラは必要ありません。	All	なし	はい

AI支援型分析を利用するには、 PostgreSQLデータベースバージョン12.0以降が必要です。詳細については、「AIを活用したSASTの要件」を参照してください。

3.4. AIを活用したSASTの要件

このセクションでは、AIを活用したSASTの要件について説明します。

AWS　Bedrockによってホストされる LLMを使用するための要件

- Amazon Web Services (AWS)アカウントが必要です。
- AWS Bedrockへのリクエストに使用するAWS IAMユーザーまたはロールには、以下のAPIを呼び出す権限が必要です。
  - `Bedrock Runtime: InvokeModel`
  - `Bedrock: GetInferenceProfile` (モデルIDとしてアプリケーション推論プロファイルを使用する場合にのみ必要)

AWS Identity and Access Managementの詳細については、*AWSのドキュメント*を参照してください。

Azure上でMicrosoft Foundryがホストするllmを使用するための要件

- Azureアカウントが必要です。
- Microsoft Foundryデプロイメントを作成する必要があります。
- (省略可)Microsoft Entra ID認証を使用している場合、Microsoft Entra IDのプリンシパルには、Microsoft Foundryデプロイメントを含むスコープに対する `Azure AI User` ロールを割り当てる必要があります。

  AzureとMicrosoft Foundryの詳細については、*Azureのドキュメント*を参照してください。

Google Cloud上でAgent Platformがホストするllmを使用するための要件

- Google Cloudアカウントが必要です。
- 関連するプリンシパルを `Agent Platform User` ロールに付与する必要があります。
- Agent PlatformのModel Gardenで目的のモデルを有効にする必要があります。
- `vertexai.allowedPartnerModelFeatures` 制約に対して目的のモデルの `structured_outputs` 機能を許可する必要があります。

OpenAIがホストするllmを使用するための要件

- OpenAIアカウントが必要です。
- APIキーを作成する必要があります。

その他の要件

- LLM結果のキャッシュを有効化するには、PostgreSQLデータベースバージョン12.0以降が必要です。



Note

データベースを使用して結果をキャッシュしない場合、LLMのコストが増加する可能性があります。

データベース要件の詳細については、「データベース要件」を参照してください。

- (省略可) `fortify-sca.properties` ファイルに保存したりコマンドラインで使用したりする前に機密性の高い値を難読化したい場合は、OpenText Application Security Toolsと一緒にインストールされているpwtoolがあることを確認します。詳細については、次を参照してください。

サポート対象のLLM

データベース要件

3.4.1. 構成可能なLLM

ソースコードファイルを分析するために、Fortify SASTに対して以下のいずれかのLLMを指定できます。

プロバイダー	モデル
AWS	Claude Sonnet 4.6(検証済み) Claude Opus 4.6
Azure	Claude Sonnet 4.6(検証済み) Claude Opus 4.6 GPT-6.0 GPT-5.4 GPT-5.2 GPT-5.2
Google Cloud	Claude Sonnet 4.6(検証済み)
OpenAI	GPT-6.0 GPT-5.4 GPT-5.2

Important

*検証済み*ラベルが付いているモデルは、 OpenTextの品質要件を満たしていることがテストで確認されており、十分な結果品質が保証されています。

3.4.2. データベース要件

以下のデータベース要件を考慮してください。

- PostgreSQLデータベースバージョン12.0以降が必要です。
- PostgreSQLのデータベースとユーザを作成する必要があります。
- 必要に応じてスキーマを作成することも、デフォルトの `public` スキーマを使用することもできます。
- データベースユーザには以下の権限が必要です。
  - データベース上に対するCONNECT
  - データベーススキーマに対するCREATE、USAGE。

    Note

    デフォルトのスキーマは `public` です。JDBC接続URLの `currentSchema` でパラメータを使用してスキーマを指定できます。

    Example

    `jdbc:postgresql://host:5432/db?currentSchema=myschema` .

  - スキーマ内の全テーブルに対するSELECT、INSERT、UPDATE、DELETE。
  - スキーマ内のすべてのシーケンスに対するUSAGE。

例: ユーザ、データベースの作成、および権限の付与

以下の例を考慮してください。

- データベースユーザを作成する

Example

```
CREATE USER <user> WITH PASSWORD '<password>';
```

- データベースを作成してデータベースに接続する

Example

```
CREATE DATABASE <database>;
\c <database>
```

- 必要に応じて、カスタムスキーマを作成するか、デフォルトの `public` スキーマを使用する

Example

```
CREATE SCHEMA <schema>;
```

- 必要な権限を付与する

Example

```
GRANT CONNECT ON DATABASE <database> TO <user>;
GRANT CREATE, USAGE ON SCHEMA <schema> TO <user>;
GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA <schema> TO <user>;
GRANT USAGE ON ALL SEQUENCES IN SCHEMA <schema> TO <user>;
```

- 複数のデータベースユーザがデータベースに接続する場合、各ユーザが他のユーザが作成したオブジェクトにアクセスできるようデフォルト権限を構成する

Note

```
ALTER DEFAULT PRIVILEGES FOR ROLE <other_user> IN SCHEMA <schema>
GRANT SELECT, INSERT, UPDATE, DELETE ON TABLES TO <user>;
ALTER DEFAULT PRIVILEGES FOR ROLE <other_user> IN SCHEMA <schema>
GRANT USAGE ON SEQUENCES TO <user>;
```

3.5. 言語の互換性

Fortify SASTは、次に示す言語バージョンとの互換性を検証します。これらのバージョンはテスト済みですが、OpenText SASTは柔軟性を念頭に置いて設計されており、明示的に検証されていない他のバージョンを正常にスキャンできます。

ユーザには、Fortify SASTの最新バージョンにアップグレードし、互換性を判断するためにスキャンを実行するようお勧めします。新しい未確認のバージョンのスキャンで問題が発生した場合や、現在サポートされていない言語をスキャンする場合には、OpenTextサポートに問い合わせてください。

下記のリストに加えて、AIを活用した分析を利用できる言語のセットがあり、各言語のすべてのバージョンとフレームワークに対応しています。詳細については、「AI支援型分析の言語の互換性」を参照してください。

言語/フレームワーク	検証済みの互換性
.NET (Core)	7.x-11.x (プレビュー版)
.NET Framework	4.6.2–4.8.1
ABAP/BSP	6.x, 7.x
ActionScript	3.0
Apex	55–61
Bicep	0.12.x–0.15.31
C#	6–15 (プレビュー版)
<C>	C11、C17、C23 (「コンパイラ」を参照)
C++	C++11、C++14、C++17、C++20、C++23 (「 コンパイラ」を参照)
クラシックASP (VBScriptを使用)	2.0, 3.0
COBOL	AIを活用したSASTによってサポートされているすべての方言とバージョン。詳細については、「AI支援型分析の言語の互換性」を参照してください。
ColdFusion	8–10
Dart™	2.12-3.8
Docker®istered trademark; (Dockerfiles)	任意
Go™プログラミング言語	最大1.27
HCL	2.0 **Note** HCLの言語サポートは、Terraformおよびサポートされるクラウドプロバイダのコードとしてのインフラストラクチャ(IaC)構成に固有のものです。
HTML	5以前

Java（Androidを含む）	1.8–25
JavaScript	ECMAScript®istered trademark; 2015–2024
JSON	ECMA-404
JSP	1.2、2.1
Kotlin	1.3–2.4
MXML (Flex®istered trademark;)	4
Objective-C/C++	2.0 (「コンパイラ」を参照)
PHP	7.3–8.5
PL/SQL	8–23
Python®istered trademark;	2.6–3.14 Jupyter Notebook内のPythonもスキャン可能です。
Ruby	AI支援型分析でサポートされているすべてのバージョン。詳細については、「AI支援型分析の言語の互換性」を参照してください。
Scala	2.11–2.13, 3.3–3.6
Solidity	0.4.12–0.8.21
Swift®istered trademark;	6.1～6.4(サポートされているswiftcバージョンについては、「コンパイラ」を参照)
T-SQL	SQL Server 2014、2016、2017、2019、2022、2025
TypeScript	3.6–5.4
VBScript	2.0, 5.0
Visual Basic (VB.NET)	15.0–16.9
Visual Basic	6.0
XML	1.0, 1.1

YAML	1.2

3.5.1. ライブラリ、フレームワーク、およびテクノロジ

Fortify SASTは、このセクションに記載されているライブラリ、フレームワーク、および技術をサポートしており、専用のFortify Secure Coding Rulepacksと、主要なサポート対象言語を超えた脆弱性カバレッジを提供しています。

Note

AIを活用したSAST言語の場合、すべてのライブラリとフレームワークがデフォルトでサポートされています。

Java

Adobe Flex Blaze DS	Apache Slide	iBatis	Mozilla Rhino	Spring AI
Ajanta	Apache Spring Security (Acegi)	IBM MQ	MyBatis	Spring MVC
Amazon Web Services (AWS) SDK	Apache Struts	IBM WebSphere	MyBatis-Plus	Spring Boot
Android	Apache Tapestry	Jackson	Netscape LDAP API	Spring Data Commons
Android Jetpack	Apache Tomcat	Jakarta Activation	OkHttp	Spring Data JPA
Apache Axiom	Apache Torque	Jakarta EE Core	OpenCSV	Spring Data MongoDB
Apache Axis	Apache Util	Jakarta EE (Java EE)	Oracle Application Development Framework (ADF)	Spring Data Redis
Apache Beam	Apache Velocity	Jasypt	Oracle BC4J	Spring for GraphQL
Apache Beehive NetUI	Apache Wicket	Java Annotations	Oracle JDBC	Spring HATEOAS
Apache Catalina	Apache Xalan	Java Core	Oracle OA Framework	Spring JMS
Apache Cocoon	Apache Xerces	Java Excel API	Oracle tcDataSet	Spring JMX
Apache Commons	ATG Dynamo	JavaMail	Oracle XML Developer Kit (XDK)	Spring Messaging
Apache ECS	Azure SDK	JAX-RS	OWASP Enterprise Security API (ESAPI)	Spring Security
Apache Hadoop	Bouncy Castle	JAXB	OWASP HTML Sanitizer	Spring Webflow
Apache HttpComponents	Castor	Jaxen	OWASP Java Encoder	Spring WebSockets
Apache Jasper	表示タグ	JBoss	Plexus Archiver	Spring WS
Apache Log4j	Dom4j	JDesktop	Realm	Stripes
Apache Lucene	Fortify Javaの注釈	JDOM	Restlet	Sun JavaServer Faces (JSF)
Apache MyFaces	GDS AntiXSS	Jetty	SAP Web Dynpro	Tungsten
Apache OGNL	Google Cloud	JGroups	Saxon	Weblogic
Apache ORO	Google Dataflow	json-simple	SnakeYAML	WebSocket
Apache POI	Google Guava	JTidy Servlet	Spring	XStream
Apache SLF4J	Google Web Toolkit	JXTA		YamlBeans
	gRPC	JYaml		ZeroTurnaround ZIP
	Gson	J2EE Core		Zip4J
	Hibernate	Liferay Portal		
		MongoDB		

Kotlin

Kotlinのサポートには、Java用にカバーされるすべてのライブラリと、次のKotlinライブラリが含まれています。

Kotlin Core

Scala

Scalaのサポートには、Java用にカバーされるすべてのライブラリと、次のScalaライブラリが含まれています。

Akka HTTP Scala Core	Scala Play Scala Slick

.NET

.NET Framework、.NET Core、および.NET Standard ADO.NET Entity Framework ADODB Amazon Web Services (AWS) SDK ASP.NET Core ASP.NET MVC ASP.NET SignalR ASP.NET Web API Azure SDK	Castle ActiveRecord CsvHelper Dapper DB2 .NET Provider DotNetZip Entity Framework Core fastJSON gRPC Hot Chocolate	IBM Informix .NET Provider Json.NET Log4Net Microsoft .NET WebSockets Microsoft ApplicationBlocks Microsoft My Framework Microsoft Practices EnterpriseLibrary Microsoft Web Protection Library MongoDB	MySql .Net Connector NHibernate NLog Npgsql Open XML SDK Oracle Data Provider for .NET OWASP AntiSamy Saxon SharePoint Services	SharpCompress SharpZipLib SQLite .NET Provider SubSonic Sybase ASE ADO.NET Data Provider Xamarin Xamarin Forms YamlDotNet

<C>

ActiveDirectory LDAP Apple System Logging (ASL) C Core	CURL Library GLib JNI	MySQL Netscape LDAP ODBC	OpenSSL POSIX Threads SQLite	Sun RPC WinAPI

C++

CPPCore Boost Smart Pointers MFC	STL WMI

SQL

SQLCore Microsoft T-SQL	Oracle ModPLSQL Oracle PL/SQL Core

PHP

ADOdb Advanced PHP Debugging CakePHP PHPCore PHP Debug	PHP DOM PHP Extension PHP Hash PHP JSON PHP Mcrypt	PHP Mhash PHP Mysql PHP OCI8 PHP OpenSSL PHP PostgreSQL	PHP Reflection PHP Simdjson PHP SimpleXML PHP Smarty PHP Sodium	PHP WordPress PHP XML PHP XMLReader PHP Zend PHP Zip

JavaScript/TypeScript/HTML5

Angular AngularJS Anthropic Apollo Server Bluebird child-process-promise	Express GraphQL.js Google Gemini Google Vertex AI Handlebars Helmet	iOS JavaScript Bridge JavaScript (ECMAScript)/HTML5 Core jQuery JS-YAML LangChain Mustache	Node.js Azure Storage Node.js Core OpenAI React React Native React Native Async Storage	React Router SAPUI5/OpenUI5 Sequelize Underscore.js Vue

PythonとJupyter Notebook

aiopg Amazon Web Services (AWS) Lambda Amazon SageMaker Anthropic AutoGen Azure Functions Boto3 Django Faiss FastAPI	FastAPI-FastMCP FastMCP Flask Google Cloud Graphene gRPC httplib2 Hugging Face Jinja3 LangChain	libxml2 lxml memcache-client _mysql MySQL Connector/Python MySQLdb OpenAI oslo.config Pandas Paramiko	psycopg2 pycrypto PyCryptodome pycurl pylibmc PyMongo PySpark Python Core PyYAML requests	simplejson six Starlette TensorFlow Twisted Mail urllib3 WebKit

Objective-C

AFNetworking Apple AddressBook Apple AppKit Apple CFNetwork Apple ClockKit Apple CommonCrypto Apple CoreData	Apple CoreFoundation Apple CoreLocation Apple CoreServices Apple CoreTelephony Apple Foundation Apple HealthKit Apple LocalAuthentication	Apple MessageUI Apple Network Apple os Apple Security Apple Social Apple UIKit Apple UserNotifications	Apple WatchConnectivity Apple WatchKit Apple WebKit Hpple Objective-Zip Realm SBJson	SFHFKeychainUtils SSZipArchive ZipArchive ZipUtilities ZipZap

Swift

Alamofire Apple AddressBook Apple CFNetwork Apple ClockKit Apple CommonCrypto Apple CoreData Apple CoreFoundation	Apple CoreLocation Apple CryptoKit Apple Foundation Apple HealthKit Apple LocalAuthentication Apple MessageUI Apple Network	Apple os Apple Security Apple Social Apple SwiftUI Apple System Apple UIKit Apple UserNotifications	Apple WatchConnectivity Apple WatchKit Apple WebKit Realm SQLite SSZipArchive Swift Core	Zip ZipArchive ZIPFoundation ZipUtilities ZipZap

Go

Go Core Gin GORM	logrus gRPC

Dart

Dart SDK Flutter

Salesforce Apex/Visualforce

Salesforce Apex/Visualforce Core

Configuration

.NET Configuration Adobe Flex (ActionScript) Configuration Ajax Frameworks Amazon Web Service (AWS) Ansible AWS CloudFormation Azure Resource Manager (ARM) Build Management	Docker Configuration (Dockerfiles) GitHub Actions Google Android Configuration iOS Property List J2EE Configuration Java Apache Axis Java Apache Log4j Configuration Java Apache Spring Security (Acegi)	Java Apache Struts Java Apache Tomcat Configuration Java Blaze DS Java Hibernate Configuration Java iBatis Configuration Java IBM WebSphere Java MyBatis Configuration	Java OWASP AntiSamy Java Spring and Spring MVC Java Spring Boot Java Spring Mail Java Spring Security Java Spring WebSockets Java Weblogic Kubernetes Mule	OpenAPI Specification Oracle Application Development Framework (ADF) PHP Configuration PHP WordPress Silverlight Configuration Terraform (AWS, Azure, GCP) WS-SecurityPolicy XML Schema

コードとしてのインフラストラクチャ: Amazon Web Services

API Gateway App Mesh AppSync Athena Aurora Backup Batch Certificate Manager CloudFormation CloudFront CloudTrail CloudWatch CodeBuild CodeCommit CodeStar Cognito	Config ConfigurationRecorder Database Migration Service (DMS) DataSync DocumentDB DynamoDB EC2 Elastic Block Store (EBS) Elastic Container Registry (ECR) Elastic Container Service (ECS) Elastic File System (EFS) Elastic Kubernetes Service (EKS)	Elastic Load Balancing (ELB) ElastiCache EMR FinSpace FSx Global Accelerator Glue GuardDuty HealthLake Identity and Access Management (IAM) Image Builder Key Management Service (KMS) Kinesis Kinesis Video Streams	Lightsail Location Service Lookout for Equipment Mainframe Modernization Managed Streaming for Apache Kafka (MSK) MemoryDB for Redis MQ Neptune OpenSearch Service Quantum Ledger Database (QLDB) RDS Redshift Rekognition Route 53	SageMaker Secrets Manager Simple Notification Service (SNS) Simple Queue Service (SQS) Simple Storage Service (S3) Step Functions Systems Manager Timestream Transfer Family VPC VPC Lattice WorkSpaces Family

コードとしてのインフラストラクチャ: Microsoft Azure

App Service Application Gateway Automation Microsoft Entra Domain Services Azure Health Data Services Azure Kubernetes Service (AKS) Batch Blob Storage	Cache for Redis Cognitive Search Container Registry Cosmos DB Database for MariaDB Database for MySQL Database for PostgreSQL Databricks Data Box	Data Factory Defender for Cloud Event Hubs Front Door Grafana Hostname Binding IoT Central IoT Hub Key Vault Logic Apps	Machine Learning MariaDB Media Services Monitor NetApp Files Private Cloud ポリシー Portal SignalR Service	Site Recovery Spring Apps SQL Storage Accounts Virtual Machine Scale Sets Virtual Machines Web PubSub

コードとしてのインフラストラクチャ: Google Cloud

Access Context Manager AlloyDB Apigee API Management App Engine Artifact Registry	Backup for GKE BigQuery Cloud Bigtable Cloud DNS Cloud Functions Cloud Key Management	Cloud Load Balancing Cloud Logging Cloud Spanner Cloud SQL Cloud Storage Compute Engine	Filestore Google Cloud Platform Google Kubernetes Engine (GKE) Identity and Access Management (IAM)	Media CDN Memorystore Pub/Sub Secret Manager Workflows

Secrets

.netrc	Defined	HashiCorp (Terraform, Vault)	New Relic	Sendbird
1Password	DES	Heroku	npm	SendGrid
Actually Good Encryption (AGE)	DigitalOcean	HexChat	NuGet	Sentry
Adafruit	Docker	HubSpot	Okta	SHA1
Adobe	Doppler	Intercom	OpenVPN	SHA256
Airtable	Droneci	Java	Password in comment	SHA512
Algolia	Dropbox	JFrog (Artifactory)	Password in connection string	Shippo
Alibaba (Aliyun)	Duffel	JSON Web Token	Password in PowerShell script	Shopify
Amazon (AWS, MWS)	Dynatrace	KDE Wallet (Kwallet)	Password in URI	Sidekiq
Apple (macOS)	EasyPost	KeePass	Password Safe	Slack
Apache HTTP	Encryption key	Kraken	PayPal (Braintree)	SonarQube
Asana	Etsy	Kucoin	Pidgin	Square
Atlassian	Facebook	LaunchDarkly	Plaid	Squarespace
Authress	Fastly	Linear	Planetscale	StackHawk
基本アクセス認証	Finicity	LinkedIn	PostgreSQL	Stripe
bcrypt	Finnhub	Lob	Postman	Sumologic
Beamer	Flickr	Mailchimp	Prefect	Telegram
Bearer token	Flutterwave	Mailgun	Pulumi	Travis
Bitbucket	Frame.io	Mapbox	PuTTY	Trello
Bittrex	Freshbooks	Mattermost	PyPI	Twilio
Brevo (Sendinblue)	Git	MD5	RapidAPI	Twitch
Clojars	GitHub	MessageBird	Readme	Twitter
Code Climate	GitLab	Microsoft (Azure App Storage、Cosmos DB、 Functionsと Bitlocker、 PowerShell、 RDP、 VBScript)	RSA Security	Typeform
Codecov	Gitter	Microsoft (Outlook)	Ruby (Ruby on Rails, RubyGems)	Yandex
Coinbase	GNOME	Mutt	Sauce Labs	Zendesk
Confluent	GNU (Bash)	MySQL	Secret key	
Contentful	GoCardless	Netlify	Secure Shell Protocol (SSH)	
Databricks	Google (API, Google Cloud, OAuth)			
Datadog	Grafana			

3.5.2. AIを活用したSASTの言語の互換性

AIを活用したSASTでは以下の言語がサポートされています。

- AIエージェントルールファイル
- AI Instructionsファイル
- Ada
- Bash
- COBOL*
- Delphi

- Elixir
- Erlang
- Fortran
- Groovy
- KornShell
- Lua
- Perl
- PowerShell
- <R>
- Ruby**
- Rust

*AIを活用したSASTと従来のSASTの両方を使用できます。より良い結果を得るために、OpenTextではAIを活用したSASTの使用を推奨しています。

**AIを活用したSASTが従来のローカルSAST分析に取って代わりました。

3.6. サポートされるビルドツール

Fortify　SASTは、次の表に示すビルドツールをサポートしています。

ビルドツール	バージョン	メモ
Apache Ant™	1.10.x	
Bazel	7.x	Bazel統合はJavaとPythonをサポートしています。
dotnet	7.x - 11.x (プレビュー版)	
Gradle (ビルド統合)	6.6–9.x	Fortify SAST Gradle統合は、Java、Kotlin、およびC/C++をサポートしています。
Gradle (Gradleプラグイン)	6.6–8.5	Fortify SAST Gradle Pluginは、JavaおよびKotlinをサポートしています。
Apache Maven™ Software	3.9.x	
MSBuild	15.x–18.x	Fortify SAST MSBuild 18統合は、.NET 7.0以降および.NET Framework 4.7.2以降と互換性があります。 これらのバージョンはテスト済みですが、Fortify SASTは柔軟性を念頭に置いて設計されており、明示的に検証されていないMSBuildのバージョンを正常にスキャンできます。ユーザには、Fortify SASTの最新バージョンにアップグレードし、互換性を判断するためにスキャンを実行するようお勧めします。MSBuildの新しいバージョンまたは未検証のバージョンで問題が発生した場合は、OpenTextサポートにお問い合わせください。
xcodebuild	16～16.4、26.0～26.6	

3.7. サポートされているコンパイラ

Fortify　SASTは、次の表に示すコンパイラをサポートしています。

コンパイラ	バージョン	オペレーティングシステム
gcc	GNU gcc 6.x– 14	Windows, Linux, macOS, AIX
gcc	GNU gcc 4.9–5.x	Windows, Linux, macOS, AIX
g++	GNU g++ 6.x– 13	Windows, Linux, macOS
	GNU g++ 4.9–5.x	Windows, Linux, macOS, AIX
OpenJDK javac	9, 10, 11, 12, 13, 14, 17, 21, 24, 25	Windows, Linux, macOS, AIX
Oracle javac	7, 8, 9	Windows, Linux, macOS
cl (MSVC)	2015, 2017, 2019, 2022	Windows
LLVM Clang	19.1.4, 19.1.5, 21.1.6	Windows, Linux, macOS, AIX
Apple Clang	17.0.0, 21.0.0	macOS
Swiftc	6.1 - 6.4	macOS

1Fortify　SASTは、次のXcodeバージョンで構築されたアプリケーションをサポートします:

16～16.4、26.0～26.6

.

3.8. OpenText Application Security Content

Fortify Secure Coding Rulepacksは、サポートされているすべてのバージョンのFortify SASTと後方互換性があります。これにより、現在サポートされているFortify　SASTインストールにおいて、Rulepackの更新によって不具合が生じないようにします。

3.9. 仮想マシンのサポート

OpenText Application Security Software製品は、仮想マシン環境で承認済みのオペレーティングシステムで実行できます。最小限のハードウェア要件を満たす専用のCPUおよびメモリリソースを提供する必要があります。推奨される処理リソース、メモリリソース、およびディスクリソースで、ネイティブ環境では再現できない問題を見つけた場合は、仮想環境のプロバイダと一緒に作業して問題を解決する必要があります。

Note

VM環境でOpenText Application Security Software製品を実行する場合は、パフォーマンスの低下を避けるため、CPUおよびメモリリソースをVMに完全にコミットしておくことを強く推奨します。

3.10. ソフトウェアの取得

Fortify SAST(Static Code Analyzer)は、電子的なダウンロードとして利用できます。ソフトウェアライセンスおよびダウンロード(SLD)ポータルからソフトウェアをダウンロードする方法については、［**お問い合わせ先/セルフヘルプ(Contact Us / Self Help)**］をクリックしてビデオと『*クイックスタートガイド*』を確認してください。

次の表に、使用可能なパッケージを一覧表示してそれぞれの内容を説明します。

File Name	説明(Description)
OpenText_SAST_Fortify_Windows_<*version*>.zip	Windows用のFortify SASTパッケージ このパッケージには次の内容が含まれています。 • 次のコンポーネントを含む、Fortify SASTインストーラ • Fortify License and Infrastructure Managerインストーラ • Fortify SASTカスタムルールガイドバンドル • OpenText Application Security Softwareについて **Note** OpenText Application Security Content (ルールパックおよび外部メタデータ)は、インストール時にダウンロードできます。
OpenText_SAST_Fortify_Windows_<*version*>.zip.sig	Fortify SAST Windowsパッケージの署名ファイル
OpenText_SAST_Fortify_Linux-ARM_<*version*>.tar.gz	ARM上のLinux用のFortify SASTパッケージ このパッケージには次の内容が含まれています。 • 次のコンポーネントを含む、Fortify SASTインストーラ • Fortify SASTカスタムルールガイドバンドル • OpenText Application Security Softwareについて **Note** OpenText Application Security Content (ルールパックおよび外部メタデータ)は、インストール時にダウンロードできます。
OpenText_SAST_Fortify_Linux-ARM_<*version*>.tar.gz.sig	ARMパッケージ上のFortify SAST Linuxの署名ファイル
OpenText_SAST_Fortify_Linux_<*version*>.tar.gz	Linux用のFortify SASTパッケージ このパッケージには次の内容が含まれています。 • 次のコンポーネントを含む、Fortify SASTインストーラ • Fortify SASTカスタムルールガイドバンドル • OpenText Application Security Softwareについて **Note** OpenText Application Security Content (ルールパックおよび外部メタデータ)は、インストール時にダウンロードできます。

OpenText_SAST_Fortify_Linux_<*version*>.tar.gz.sig	Fortify SAST Linuxパッケージの署名ファイル
OpenText_SAST_Fortify_Mac-ARM_<*version*>.tar.gz	macOS-ARM用のFortify SASTパッケージ このパッケージには次の内容が含まれています。 ◆ 次のコンポーネントを含む、Fortify SASTインストーラ ◆ Fortify SASTカスタムルールガイドバンドル ◆ OpenText Application Security Softwareについて **Note** ◆ OpenText Application Security Content (ルールパックおよび外部メタデータ)は、インストール時にダウンロードできます。 ◆ x86インストーラが必要な場合は、カスタマサポートにお問い合わせください。
OpenText_SAST_Fortify_Mac-ARM_<*version*>.tar.gz.sig	Fortify SAST macOS-ARMパッケージの署名ファイル
OpenText_SAST_Fortify_AIX_<*version*>.tar.gz	AIX用のFortify SASTパッケージ このパッケージには次の内容が含まれています。 ◆ Fortify SASTインストーラ ◆ Fortify SASTカスタムルールガイドバンドル ◆ OpenText Application Security Softwareについて
OpenText_SAST_Fortify_AIX_<*version*>.tar.gz.sig	Fortify SAST AIXパッケージの署名ファイル
OpenText_SAST_Fortify_Samples_<version>.zip	Fortify SASTの使用法を学ぶのに役立つコードサンプル
OpenText_SAST_Fortify_Samples_<version>.zip.sig	Fortify SASTコードサンプルの署名ファイル

3.11. ソフトウェアのダウンロードの確認

このトピックでは、カスタマサポートWebサイトからダウンロードした署名ファイルのデジタル署名を検証する方法について説明します。検証により、ダウンロードしたパッケージが署名されてサイトにポストされた後に改ざんされていないことが保証されます。検証に進む前に、OpenText Application Security Software製品ファイルおよび関連する署名(`*.sig`)ファイルをダウンロードします。ソフトウェアを使用するためにパッケージを検証する必要はありません。ただし、セキュリティ上の理由から、組織で必要になる場合があります。

デジタル署名検証のためのシステムの準備

電子メディア検証用にシステムを準備するには、次の手順を実行します。

1. GnuPGのWebサイトに移動します。
2. GnuPG Privacy Guardをダウンロードしてインストールします。
3. 次のように、秘密鍵を生成します。
    1. 次のコマンドを実行します(Windowsシステムでは、 `$` プロンプトなしでコマンドを実行します)。
    `$ gpg --gen-key`

2. キータイプのプロンプトが表示されたら、［ DSA and Elgamal ］を選択します。
3. キーサイズのプロンプトが表示されたら、［ 2048 ］を選択します。
4. キーが有効である必要がある時間の長さのプロンプトが表示されたら、［ key does not expire ］を選択します。
5. ユーザ識別の質問に回答し、秘密鍵を保護するパスフレーズを入力します。

4. OpenText GPG公開鍵(圧縮されたtarファイル)を https://mysupport.microfocus.com/documents/10180/0/MF_public_keys.tar.gzからダウンロードします。
5. 公開鍵を抽出します。
6. 次のコマンドを使用して、ダウンロードした各キーをGnuPGでインポートします。
   `gpg --import <path_to_key>/<key_file>`

4. Fortify SASTのインストール

このセクションでは、Fortify SASTのインストール方法とアンインストール方法について説明します。このセクションでは、インストール後の基本的なタスクについても説明します。システムがハードウェアおよびソフトウェアの最小要件を満たしていることを確認するために、「システム要件」を参照してください。

- Fortify SASTのインストールについて
- Dockerを使用したFortify SASTのインストールと実行
- Fortify SASTのアップグレード
- Fortify SASTのアンインストールについて
- インストール後のタスク

4.1. Fortify SASTのインストールについて

このセクションでは、Fortify SASTをインストールする方法について説明します。いくつかのコマンドラインツールがFortify SASTと一緒に自動的にインストールされます(「コマンドラインツール」を参照)。必要に応じて、Fortify ScanCentral SASTクライアントとFortify Software Security Center fortifyclientユーティリティをFortify SASTのインストールに含めることができます。Fortify ScanCentral SASTの詳細については、『OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド』を参照してください。

インストール用のFortifyライセンスファイルと、オプションでLIMライセンスプール資格情報を指定する必要があります。次の表に、Fortify SASTをインストールする方法を示します。

インストール方法	手順
標準インストールウィザードを使用してインストールを実行する	Fortify SASTおよびアプリケーションのインストール
サイレント(無人)でインストールを実行する	Fortify SASTのサイレントインストール
Windows以外のシステムでテキストベースのインストールを実行する	Windows以外のプラットフォームでテキストベースモードでのFortify SASTとアプリケーションのインストール
Dockerを使用してインストールを実行する	Dockerを使用したFortify SASTのインストールと実行

パフォーマンスを最適にするには、スキャンするコードが存在するローカルファイルシステムにFortify SASTをインストールします。

Note

Windows以外のシステムでは、書き込み権限があるホームディレクトリを持っているユーザとしてFortify SASTをインストールする必要があります。ホームディレクトリを持ってないルート以外のユーザとしてFortify SASTをインストールしないでください。

インストールが完了したら、「インストール後のタスクについて」を参照して、システムのセットアップを完了するために実行できる追加のステップを確認します。また、インストールされた環境設定ファイルを更新して、ランタイム分析、出力、およびFortify SASTのパフォーマンスを設定することもできます。Fortify SASTの環境設定オプションについては、「環境設定オプション」を参照してください。

4.1.1. Fortify SASTのインストール

Fortify SASTをインストールするには:

1. オペレーティングシステムのインストーラファイルを実行して、Fortify SASTセットアップウィザードを起動します。
   - Windows: `OpenText_SAST_Fortify_windows-x64_<version>.exe`
   - Linux: `OpenText_SAST_Fortify_linux-x64_<version>.run` または `OpenText_SAST_Fortify_linux-arm64_<version>.run`
   - macOS: `OpenText_SAST_Fortify_osx-arm64.app.zip`
     APPインストーラファイルを実行する前に、ZIPファイルを展開します。
   - AIX: `OpenText_SAST_Fortify_aix-ppc64_<version>.run`

   ここで、*<version>*はソフトウェアリリースのバージョンです。次に、［次へ(Next)］をクリックします。
2. ライセンス契約を確認して受諾し、［**次へ(Next)**］をクリックします。
3. (オプション)インストールするコンポーネントを選択して、［次へ(Next)］をクリックします。
4. 一部のタイプのプロジェクト分析に必要な最小限のソフトウェアがシステムに含まれていないことがインストーラによって検出された場合、不足している要件と、その要件を必要とするプロジェクトが「**システム要件**」ページに表示されます。［次へ(Next)］をクリックします。

   すべてのソフトウェア要件については、「ソフトウェア要件」を参照してください。
5. Fortify SASTのインストール先を選択し、［**次へ(Next)**］をクリックします。
   手順3で、Fortify ScanCentral SASTクライアントをインストールに含めることを選択した場合は、パスにスペースを含まない場所を指定する必要があります。

   Important

   OpenText™ Application Security Toolsのインストール先と同じディレクトリにFortify SASTをインストールしないでください。
6. `fortify.license` ファイルへのパスを指定し、［**次へ(Next)**］をクリックします。
7. (オプション)［**LIMライセンス**］ページで［**はい**］を選択して、Fortify LIM (License and Infrastructure Manager)の同時ライセンスを管理し、［**次へ**］をクリックします。

   Note

   Fortify SASTでライセンスが必要なタスクが実行されたら、アプリケーションでライセンスプールからのLIMリースの取得が試みられます。LIMサーバとの通信上の問題があるためにFortify SASTでライセンスの取得に失敗した場合は、Fortifyのライセンスファイルが使用されます。この動作を変更するには、`com.fortify.sca.lim.WaitForInitialLicense` ファイル内で `fortify-sca.properties` を使用します(「LIMライセンスのプロパティ」を参照)。

   1. LIM APIのURL、ライセンスプール名、およびライセンスプールパスワードを入力します。
   2. ［次へ(Next)］をクリックします。
      ［**LIM Proxy Settings**］ページが開きます。
   3. LIMサーバへの接続にプロキシサーバが必要な場合は、プロキシホスト(プロキシサーバのホスト名またはIPアドレス)とポート番号(省略可能)を入力します。

4. ［次へ(Next)］をクリックします。

8. インストールのセキュリティコンテンツを更新するには:

> **Note**
> インストール時にインターネットにアクセスできない展開環境の場合、fortifyupdateコマンドラインツールを使用してセキュリティコンテンツを更新できます。「Fortify Software Security Contentの手動インストール」を参照してください。

   1. 更新サーバのWebアドレスを入力します。
      セキュリティコンテンツの更新にFortify Rulepack更新サーバを使用するには、Webアドレスを `https://update.fortify.com` のままにします。Fortify Software Security Centerをアップデートサーバとして使用することもできます。
   2. (オプション)更新サーバへの接続にプロキシサーバが必要な場合は、プロキシホストとポート番号を入力します。
   3. セキュリティコンテンツを手動で更新する場合は、［**インストール後にセキュリティコンテンツを更新する(Update security content after installation)**］チェックボックスをオフにします。
   4. ［次へ(Next)］をクリックします。

9. システム上の以前のインストールから移行するかどうかを指定します。
   以前のインストールから移行すると、Fortify　SASTアーティファクトファイルが保持されます。詳細については、「Fortify　SASTのアップグレードについて」を参照してください。

> **Note**
> `scapostinstall` コマンドラインツールを使用してアーティファクトを移行することもできます。インストール後のツールを使用して以前のインストールから移行する方法については、「プロパティファイルの移行」を参照してください。

   以前のインストールからアーティファクトを移行するには、次の手順に従います。
   1. ［**Fortify SAST (Fortify) の移行(Migration)**］ページで［**はい(Yes)**］を選択して、［**次へ(Next)**］をクリックします。
   2. システム上の既存のインストール場所を指定し、［**次へ(Next)**］をクリックします。

   以前のリリースからのアーティファクトのマイグレーションをスキップするには、移行の選択を［**いいえ(No)**］のままにして、［**次へ(Next)**］をクリックします。

10. ［**インストール準備(Ready to Install)**］ページで［**次へ(Next)**］をクリックして、Fortify SAST、選択したコンポーネント、およびFortify Software Security Contentをインストールします。
    セキュリティコンテンツの更新を選択した場合は、［セキュリティコンテンツ更新の結果(Security Content Update Result)］ウィンドウにセキュリティコンテンツ更新の結果が表示されます。
11. ［**完了(Finish)**］をクリックして、セットアップウィザードを閉じます。

4.1.2. Fortify　SASTのサイレントインストール

サイレントインストールを使用すると、ユーザプロンプトを表示せずにインストールを完了できます。サイレントでインストールするには、インストーラに必要な情報を提供するオプションファイルを作成する必要があります。サイレントインストールを使用して、複数のコンピュータにインストールパラメータを複製できます。

> **Important**
> OpenText™ Application Security Toolsのインストール先と同じディレクトリにFortify SASTをインストールしないでください。

Fortify SASTをサイレントでインストールすると、デフォルトでは、インストーラによってFortify Software Security Centerがダウンロードされません。オプションファイルでFortify Software Security Contentのダウンロードを有効にするか、Fortify Software Security Contentを手動でインストールすることができます(Fortify Software Security Contentの手動インストールを参照)。

Fortify　SASTをサイレントでインストールするには:

1. オプションファイルを作成します。
    1. 次の行を含むテキストファイルを作成します。

        ```
        fortify_license_path=<license_file_locat　　ion>
        ```

        ここで、<*license_file_location*>は　fortify.license　ファイルへのフルパスです。
    2. LIMライセンスサーバを使用するには、LIMライセンスプール資格情報を含む次の行をオプションファイルに追加します。

        ```
        lim_url=<lim_url>lim_pool_name=<license_pool_name>lim_pool_password=<license_pool_pwd>
        ```

    3. Fortify Software Security Contentの更新で、デフォルトの　　とは異なる場所を使用するには、次の行を追加します。

        ```
        update_server=<updat e_server_url>
        ```

    4. Fortify　Software　Security　Contentのダウンロードにプロキシサーバが必要な場合は、次の行を追加します。

        ```
        update_proxy_server=<proxy_server>update_proxy_port=<port　　_number>
        ```

    5. Fortify Software Security Contentのダウンロードを有効にするには、次の行を追加します。
    update_security_content=1
    6. 必要に応じて、オプションファイルにインストール指示を追加します。
    オプションファイルに追加できるインストールオプションのリストを取得するには、コマンドプロンプトを開き、インストーラファイル名と　--help　オプションを入力します。このコマンドでは、使用可能な各コマンドラインオプションの前に二重ダッシュが付けられ、使用可能なパラメータが角括弧で囲まれます。たとえば、インストールの進行状況をコマンドラインに表示する場合は、オプションファイルに　unattendedmodeui=minimal　を追加します。

        メモ:

        - コマンドラインオプションでは大文字と小文字が区別されます。
        - インストールオプションは、サポートされているすべてオペレーティングシステムで同じではあるとは限りません。 --help　を使用してインストーラを実行して、オペレーティングシステムで使用可能なオプションを確認します。

        次のWindowsオプションファイルの例では、ライセンスファイルの場所、Fortify Software Security Centerサーバの場所とFortify Software Security Contentを取得するためのプロキシ情報、以前のリリースからの移行要求、およびFortify SASTのインストールディレクトリの場所を指定しています。

        ```
        fortify_license_path=C:¥Users¥admin¥Desktop¥fortify.license
        update_server=https://my_ssc_host:8080/ssc　　update_proxy_server=webproxy.abc.company.com
        update_proxy_port=8080　migrate_sca=1　install_dir=C:¥Fortify
        ```

        次のオプションファイルの例は、LinuxおよびmacOS®istered　trademark;用です。

        ```
        fortify_license_path=/opt/Fortify/fortify.license　　update_server=https://my_ssc_host:8080/ssc
        update_proxy_server=webproxy.abc.company.com　update_proxy_port=8080　migrate_sca=1
        install_dir=/opt/Fortify
        ```

2. オプションファイルを保存します。
3. オペレーティングシステムのサイレントインストールコマンドを実行します。

Note
場合によっては、インストーラを実行する前に、管理者としてコマンドプロンプトを実行する必要があります。

Windows	`OpenText_SAST_Fortify_windows-x64_<version>.exe --mode unattended --optionfile <full_path_to_options_file>`

Linux	`./OpenText_SAST_Fortify_linux-x64_<version>.run --mode unattended --optionfile <full_path_to_options_file>`
	または
	`./OpenText_SAST_Fortify_linux-arm64_<version>.run --mode unattended --optionfile <full_path_to_options_file>`

macOS®istered trademark;	コマンドを実行する前に、ZIPファイルを展開する必要があります。
	`OpenText_SAST_Fortify_osx-x64_<version>.app/Contents/MacOS/installbuilder.sh --mode unattended --optionfile <full_path_to_options_file>`
	または
	`OpenText_SAST_Fortify_osx-arm64_<version>.app/Contents/MacOS/installbuilder.sh --mode unattended --optionfile <full_path_to_options_file>`

AIX	`./OpenText_SAST_Fortify_aix-ppc64_<version>.run --mode unattended --optionfile <full_path_to_options_file>`

インストールが完了すると、インストーラのログファイルが作成されます。このログファイルは、オペレーティングシステムに応じて次の場所に保存されます。

Windows	`C:\Users\<*username*>\AppData\Local\Temp\OpenTextSASTFortify-<*version*>-install.log`
Windows以外	`/tmp/OpenTextSASTFortify-<*version*>-install.log`

4.1.3. Windows以外のプラットフォームでテキストベースモードでのFortify　SASTのインストール

コマンドラインでテキストベースのインストールを実行します。インストール時に、インストールを完了するために必要な情報の入力を求めるプロンプトが表示されます。Windowsシステムではテキストベースのインストールがサポートされていません。

Important
OpenText™ Application Security Toolsのインストール先と同じディレクトリにFortify SASTをインストールしないでください。

Fortify SASTのテキストベースのインストールを実行するには、次の表に示すように、オペレーティングシステム用のテキストベースのインストールコマンドを実行します。

Linux	`./OpenText_SAST_Fortify_linux-x64_<version>.run --mode text`
	または
	`./OpenText_SAST_Fortify_linux-arm64_<version>.run --mode text`

MacOS	コマンドを実行する前に、提供されたZIPファイルを展開する必要があります。
	`OpenText_SAST_Fortify_osx-x64_<version>.app/Contents/MacOS/installbuilder.sh --mode text`
	または
	`OpenText_SAST_Fortify_osx-arm64_<version>.app/Contents/MacOS/installbuilder.sh --mode text`

AIX	`OpenText_SAST_Fortify_aix-ppc64_<version>.run --mode text`

4.1.4. OpenText Application Security Contentの手動インストール

OpenText Application Security Content (Fortify Secure Coding Rulepacksとメタデータ)は、インストール時に自動的にインストールできます。ただし、Fortify Rulepack更新サーバからOpenText Application Security Contentをダウンロードしてから、fortifyupdateコマンドラインツールを使用してインストールすることもできます。このオプションは、インストール時にインターネットにアクセスできない展開環境のために提供されています。

リモートサーバまたはローカルにダウンロードされたファイルからOpenText Application Security Contentをインストールするには、fortifyupdateを使用します。

セキュリティコンテンツをインストールするには、次の手順に従います。

1. コマンドウィンドウを開き、 `<sast_install_dir> /bin/` に移動します。
2. コマンドプロンプトで「 `fortifyupdate` 」と入力します。

以前にFortify Rulepack更新サーバからOpenText Application Security Contentをダウンロードした場合は、 `fortifyupdate` オプションと、ZIPファイルをダウンロードしたディレクトリへのパスを使用して `-import` を実行します。

この同じツールを使用して、OpenText Application Security Contentを更新することもできます。fortifyupdateコマンドラインツールの詳細については、「セキュリティコンテンツの更新」を参照してください。

4.2. Dockerを使用したFortify SASTのインストールと実行

DockerイメージにFortify SASTをインストールしてから、Fortify SASTをDockerコンテナとして実行できます。

> **Note**
>
> Fortify SASTは、Dockerでサポートされ ているLinuxプラットフォームでのみ実行できます。

- OpenText SASTをインストールするDockerfileの作成
- コンテナの実行

4.2.1. OpenText SASTをインストールするDockerfileの作成

このトピックでは、DockerイメージでFortify SASTをインストールするDockerfileを作成する方法について説明します。

Dockerfileには、次の命令が含まれている必要があります。

1. ベースイメージに使用されるLinuxシステムを設定します。
   サポートされているプラットフォームとアーキテクチャの詳細については、「サポートされるプラットフォームとアーキテクチャ」を参照してください。

> **Note**
> Fortify SASTの実行時にビルドツールを使用する場合は、イメージに必要なビルドツールがインストールされていることを確認します。サポートされているビルドツールの使用については、「サポートされるビルドツール」を参照してください。

2. COPY命令を使用して、Fortify SASTインストーラ、Fortifyライセンスファイル、およびインストールオプションファイルをDockerイメージにコピーします。
   インストールオプションファイルの作成方法については、「Fortify SASTのサイレントインストール」を参照してください。
3. RUN命令を使用してFortify SASTインストーラを実行します。
   インストーラは無人モードで実行する必要があります。詳細については、「Fortify SASTのサイレントインストール」を参照してください。
4. RUN命令を使用して、runifyupdateを実行してFortify Software Security Contentをインストールします。

   > **Important**
   > Fortify SASTでプロジェクトの分析を実行するには、Fortify Software Security Contentのインストールが必要です。次の例では、イメージの構築中にダウンロードしたローカルファイルから、Fortify Software Security Contentをインストールします。fortifyupdateツールを使用したFortify Software Security Contentのダウンロードとインストールの詳細については、「Fortify Software Security Contentの手動インストール」を参照してください。

5. Fortify SASTを実行できるようにイメージを設定するには、ENTRYPOINT命令を使用して、インストールされたsourceanalyzer実行可能ファイルの場所にエントリポイントを設定します。
   sourceanalyzerのデフォルトのインストールパスは `/opt/Fortify/OpenText_SAST_Fortify_<version>/bin/sourceanalyzer` です。

Fortify SASTをインストールするDockerfileの例は、次のとおりです。

```
FROM ubuntu:18.04 WORKDIR /app ENV APP_HOME="/app" ENV RULEPACK="MyRulepack.zip" COPY fortify.license ${APP_HOME} COPY OpenText_SAST_Fortify_linux-x64_25.4.0.run ${APP_HOME} COPY optionFile ${APP_HOME} COPY ${RULEPACK} ${APP_HOME} RUN ./OpenText_SAST_Fortify_linux-x64_25.4.0.run --mode unattended ¥ --optionfile "${APP_HOME}/optionFile" && ¥ /opt/Fortify/OpenText_SAST_Fortify_25.4.0/bin/fortifyupdate -import ${RULEPACK} && ¥ rm OpenText_SAST_Fortify_linux-x64_25.4.0.run optionFile ENTRYPOINT ["/opt/Fortify/OpenText_SAST_Fortify_25.4.0/bin/sourceanalyzer"]
```

現在のディレクトリからDockerfileを使用してdockerイメージを作成するには、docker buildコマンドを使用する必要があります。例:

```
docker buildx build -f <docker_file> -t <image_name> "."
```

4.2.2. コンテナの実行

このトピックでは、Fortify SASTイメージをコンテナとして実行する方法について説明し、変換およびスキャン用のDocker実行コマンドの例を示します。

> **Note**
> コンテナでFortify SASTを実行する際に、特にランタイムコンテナ保護も利用する場合は、Fortify SASTにビルドコマンド(javacなど)を実行するための適切な許可があることを確認します。

Fortify SASTイメージをコンテナとして実行するには、ホストファイルシステムからコンテナに次の2つのディレクトリをマウントする必要があります。

- 分析するソースファイルが含まれるディレクトリ。

- 変換フェーズとスキャンフェーズの間にFortify SASTビルドセッションを保存し、出力ファイル(ログとFPRファイル)をホストと共有するための一時ディレクトリ。
  このディレクトリは、Fortify SASTの変換コマンドとスキャンコマンドの両方で `-project-root` コマンドラインオプションを使用して指定します。

次のコマンドの例では、 `/sources` に入力ディレクトリ `/src` をマウントし、 `/scratch_docker` に一時ディレクトリをマウントします。この例のイメージ名は `fortify-sast` です。

変換およびスキャン用のDocker実行コマンドの例

次の例では、一時ディレクトリとソースディレクトリをマウントし、変換フェーズ用にコンテナからFortify SASTを実行します。

```
docker run -v /scratch_local/:/scratch_docker -v /sources/:/src -it fortify-sast -b MyProject -project-root /scratch_docker [<sca_options>] /src
```

次の例では、一時ディレクトリをマウントし、分析フェーズ用にコンテナからFortify SASTを実行します。

```
docker run -v /scratch_local/:/scratch_docker -it fortify-sast -b MyProject -project-root /scratch_docker -scan [<sca_options>] -f /scratch_docker/MyResults.fpr
```

`MyResults.fpr` 出力ファイルがホストの `/scratch_local` ディレクトリに作成されます。

4.3. Fortify SASTのアップグレード

Fortify SASTをアップグレードするには、現在のバージョンがインストールされている場所とは異なる場所に新しいバージョンをインストールし、以前のインストールから設定を移行します。この移行では、 `<sast_install_dir>/Core/config` ディレクトリにあるアーティファクトファイルが保持および更新されます。

以前のリリースから設定を移行しない場合は、次のデータが変更されていれば、バックアップを保存することが推奨されています。

- `<sast_install_dir>/Core/config/rules` folder
- `<sast_install_dir>/Core/config/customrules` folder
- `<sast_install_dir>/Core/config/ExternalMetadata` folder
- `<sast_install_dir>/Core/config/CustomExternalMetadata` folder
- `<sast_install_dir>/Core/config/server.properties` file
- `<sast_install_dir>/Core/config/scales` folder

新しいバージョンをインストールしたら、以前のバージョンをアンインストールできます。詳細については、「Fortify SASTのアンインストールについて」を参照してください。



Note

以前のバージョンがインストールされたままにしておくこともできます。同じシステムに複数のバージョンがインストールされている場合は、コマンドラインからコマンドを実行すると、最近インストールされたバージョンが使用されます。

4.4. Fortify SASTのアンインストールについて

このセクションでは、Fortify SASTをアンインストールする方法について説明します。標準インストールウィザードを使用することも、Fortify SASTをサイレントでインストールすることもできます。Windows以外のシステムでは、テキストベースのアンインストールを実行することもできます。

このセクションでは、次のトピックについて説明します。

- Fortify SASTのアンインストール
- Fortify SASTのサイレントアンインストール
- Windows以外のプラットフォームでテキストベースモードでのFortify SASTのアンインストール

4.4.1. Fortify　SASTのアンインストール

Fortify　SASTをアンインストールするには:

1. インストールディレクトリに移動します。
2. 次の表で説明するように、ご使用のオペレーティングシステム用のアンインストールコマンドを実行します。

OS	アンインストールコマンド
Windows	`Uninstall_OpenTextSASTFortify.exe` または、Windowsインタフェースからアプリケーションをアンインストールすることもできます。手順については、Microsoft Windowsのドキュメントを参照してください。
Linux AIX	`./Uninstall_OpenTextSASTFortify`
macOS®istered trademark;	`Uninstall_OpenTextSASTFortify.app`

3. アプリケーション全体を削除するか、個々のコンポーネントを削除するかを指定するよう求めるメッセージが表示されます。どちらかを選択し、［**次へ(Next)**］をクリックします。
   特定のコンポーネントをアンインストールする場合は、［**アンインストールするコンポーネントの選択(Select Components to Uninstall)**］ページで削除するコンポーネントを選択し、［**次へ(Next)**］をクリックします。
4. すべてのアプリケーション設定を削除するかどうかを指定するよう求めるメッセージが表示されます。次のいずれかを実行します。
   - アンインストールするFortify SASTのバージョンと一緒にインストールされたコンポーネントのアプリケーション設定を削除するには、［**はい(Yes)**］をクリックします。
     Fortify SAST（ `sca<version>`)アプリケーション設定フォルダは削除されません。
   - ［**No**］をクリックして、アプリケーション設定をシステムに保持します。

4.4.2. Fortify　SASTのサイレントアンインストール

Fortify　SASTをサイレントでアンインストールするには、次の手順に従います。

1. インストールディレクトリに移動します。
2. 次の表で説明するように、ご使用のオペレーティングシステム用のアンインストールコマンドを実行します。

OS	アンインストールコマンド
Windows	`Uninstall_OpenTextSASTFortify.exe --mode unattended`
Linux AIX	`./Uninstall_OpenTextSASTFortify --mode unattended`
macOS®istered trademark;	`Uninstall_OpenTextSASTFortify.app/Contents/MacOS/installbuilder.sh --mode unattended`



Note

Windows、Linux、およびmacOS®istered trademark;の場合、アンインストールするFortify SASTのバージョンと一緒にインストールされたコンポーネントのアプリケーション設定はアンインストーラによって削除されます。

4.4.3. Windows以外のプラットフォームでテキストベースモードでのFortify　SASTのアンインストール

テキストベースモードでFortify　SASTをアンインストールするには、

1. インストールディレクトリに移動します。

2. 次の表で説明するように、ご使用のオペレーティングシステム用のアンインストールコマンドを実行します。

OS	アンインストールコマンド
Linux AIX	`./Uninstall_OpenTextSASTFortify --mode text`
macOS®istered trademark;	`Uninstall_OpenTextSASTFortify.app/Contents/MacOS/installbuilder.sh --mode text`

4.5. インストール後のタスク

インストール後のタスクでは、Fortify　SASTの使用を開始する準備をします。

- インストール後処理ツールの実行
- プロパティファイルの移行
- ロケールの指定
- Fortify Security Contentの更新の設定
- Application Securityへの接続の設定
- プロキシサーバ設定の削除
- 信頼された証明書の追加

4.5.1. インストール後処理ツールの実行

インストール後処理コマンドラインツールを使用すると、Fortify　SASTの以前のバージョンのプロパティファイルの移行、Fortify Software Security Contentの更新設定、およびFortify Software Security Centerへの接続設定を行うことができます。

インストール後処理ツールを実行するには:

1. `<sast_install_dir>/bin/` に移動します。
2. コマンドプロンプトで「`scapostinstall`」と入力します。
3. 次のいずれかを入力します。
    - 設定を表示するには、「`s`」を入力します。
    - 前のプロンプトに戻るには、「`r`」を入力します。
    - ツールを終了するには、「`q`」を入力します。

4.5.2. プロパティファイルの移行

以前のバージョンのFortify SASTから、システムにインストールされている現在のバージョンにプロパティファイルを移行するには、次の手順に従います。

1. `<sast_install_dir>/bin/` に移動します。
2. コマンドプロンプトで「`scapostinstall`」と入力します。
3. 「`1`」と入力して、`Migration` を選択します。
4. 「`1`」と入力して、`Static Code Analyzer Migration` を選択します。
5. 「`1`」と入力して、`Migrate from an existing Fortify installation` を選択します。
6. 「`1`」と入力して、`Set previous Fortify installation directory` を選択します。
7. 以前のインストールディレクトリを入力します。
8. 「`s`」と入力して、設定を確認します。
9. 「`2`」と入力して、移行を実行します。
10. 「`y`」と入力して、確認します。

4.5.3. ロケールの指定

Fortify　SASTインストールのデフォルトロケールは英語です。

Fortify　SASTインストールのロケールを変更するには、次の手順を実行します。

1. `<sast_install_dir>/bin/` に移動します。

2. コマンドプロンプトで「 scapostinstall 」と入力します。
3. 「 2 」と入力して、 Settings を選択します。
4. 「 1 」と入力して、 General を選択します。
5. 「 1 」と入力して、 Locale を選択します。
6. 次のいずれかのロケールコードを入力します。
    - en (英語)
    - es (スペイン語)
    - ja (日本語)
    - ko (韓国語)
    - pt_BR (ポルトガル語(ブラジル))
    - zh_CN (簡体字中国語)
    - zh_TW (繁体字中国語)

4.5.4. Fortify Security Contentの更新の設定

Fortify Software Security Contentを取得する方法を指定します。サーバに接続する必要がある場合は、プロキシ情報を指定する必要もあります。

Fortify Security Content更新の設定を指定するには、次の手順に従います。

1. <sast_install_dir>/bin/ に移動します。
2. コマンドプロンプトで「 scapostinstall 」と入力します。
3. 「 2 」と入力して、 Settings を選択します。
4. 「 2 」と入力して、 Fortify Update を選択します。
5. Fortify Rulepack更新サーバのURLを変更するには、「 1 」と入力してから、URLを入力します。
   Fortify Rulepack更新サーバのデフォルトのURLは https://update.fortify.com です。
6. Fortify Software Security Content更新用のプロキシを指定するには、次の手順に従います。
    1. 「 2 」と入力して Proxy Server を選択してから、プロキシサーバの名前を入力します。
       プロトコルとポート番号を除外します(例: some.secureproxy.com)。
    2. 「 3 」と入力して Proxy Server Port を選択してから、プロキシサーバのポート番号を入力します。
    3. (オプション)プロキシサーバのユーザ名(オプション 4)とパスワード(オプション 5)を指定することもできます。

4.5.5. Application Securityへの接続の設定

Fortify Software Security Centerへの接続方法を指定します。ネットワークでFortify Software Security Centerへのアクセスにプロキシサーバが使用されている場合は、プロキシ情報を指定する必要があります。

Fortify Software Security Centerへの接続の設定を指定するには、次の手順に従います。

1. <*sast_install_dir*>/bin/ に移動します。
2. コマンドプロンプトで「 scapostinstall 」と入力します。
3. 「 2 」と入力して、 Settings を選択します。
4. 「 3 」と入力して、 Software Security Center Settings を選択します。
5. 「 1 」と入力して Server URL を選択してから、Fortify Software Security CenterサーバのURLを入力します。
6. 接続のプロキシ設定を指定するには、次の手順に従います。
    1. 「 2 」と入力して Proxy Server を選択してから、プロキシサーバの名前を入力します。
       プロトコルとポート番号を除外します(例: some.secureproxy.com)。
    2. 「 3 」と入力して Proxy Server Port を選択してから、プロキシサーバのポート番号を入力します。
    3. プロキシサーバのユーザ名とパスワードを指定するには、ユーザ名のオプション 4 とパスワードのオプション 5 を使用します。
7. (オプション)次を指定することもできます。
    - Fortify Software Security CenterサーバからFortify Software Security Contentを更新するかどうか(オプション 6)
    - Fortify Software Security Centerユーザ名(オプション 7)

4.5.6. プロキシサーバ設定の削除

以前にFortify Rulepack更新サーバまたはFortify Software Security Centerのプロキシサーバ設定を指定し、不要になった場合は、それらの設定を削除できます。

Fortify Software Security Contentの更新を取得したり、Fortify Software Security Centerに接続したりするためのプロキシ設定を削除するには:

1. `<sast_install_dir>/bin/` に移動します。
2. コマンドプロンプトで「`scapostinstall`」と入力します。
3. 「`2`」と入力して、`Settings` を選択します。
4. 「`2`」を入力して`Fortify Update`を選択するか、「`3`」を入力して`Software Security Center Settings`を選択します。
5. 削除するプロキシ設定に対応する番号を入力し、マイナス記号(`-`)を入力して設定を削除します。
6. 削除するプロキシ設定ごとに手順5を繰り返します。

4.5.7. 信頼された証明書の追加

Fortify SASTから他のOpenText Application Securityソフトウェア製品および外部システムに接続するために、HTTPS経由の通信が必要になる場合があります。次に例をいくつか示します。

- Fortify SASTのデフォルトでは、ライセンス管理にLIMサーバと通信するために、HTTPS接続が必要です。`com.fortify.sca.lim.RequireTrustedSSLCert` プロパティでは、LIMサーバとの接続に信頼されたSSL証明書が必要であるかどうかが決定されます。このプロパティの詳細については、「LIMのプロパティ」を参照してください。
- fortifyupdateコマンドラインツールでは、Windowsシステムのインストール時に自動的に、または手動で(「Fortify Software Security Contentの手動インストール」を参照)、HTTPS接続を使用してFortify Software Security Contentが更新されます。
- Fortify ScanCentral SASTセンサとして設定されたFortify SASTでは、HTTPS接続を使用してコントローラと通信します。

HTTPSを使用している場合、Fortify SASTとそのアプリケーションは提示されたSSLサーバ証明書に標準チェックをデフォルトで適用します。これには、証明書が信頼されているかどうかを確認するチェックが含まれます。組織が独自の認証局 (CA)を運営し、そのCAから発行された証明書がサーバで提示される接続がFortify SASTで信頼される必要がある場合は、そのCAを信頼するようにFortify SASTを設定する必要があります。さもないと、HTTPS接続の使用に失敗する可能性があります。

CAの信頼された証明書をFortify SASTキーストアに追加する必要があります。Fortify SASTキーストアは、`<sast_install_dir>/jre/lib/security/cacerts` ファイルにあります。keytoolコマンドを使用すると、信頼された証明書をキーストアに追加できます。

信頼された証明書をFortify SASTキーストアに追加するには、次の手順に従います。

1. コマンドプロンプトを開き、次のコマンドを実行します。

   ```
   <sast _inst all_dir>/jre/bin/keytool -importcert -alias <alias_name> -cacerts -file <cert _file>
   ```

   ここで:
   - `<alias_name>` は、追加する証明書に固有の名前です。
   - `<cert_file>` は、PEM形式またはDER形式の信頼されたルート証明書を含むファイルの名前です。
2. キーストアパスワードを入力します。

   > **Note**
   > デフォルトのパスワードは `changeit` です。

3. この証明書を信頼するように求めるプロンプトが表示されたら、[**yes**]を選択します。

5. 分析プロセスの概要

- スキャンの基本

- 変換フェーズ
- 分析フェーズ
- 変換フェーズと分析フェーズの検証
- 問題の深刻度のランク付け

5.1. スキャンの基本

コードを変換および分析するためのコマンドの基本的なシーケンスを以下に示します。

1. 指定したビルドIDの既存のFortify SAST一時ファイルをすべて削除します。

   ```
   sourceanalyzer -b MyProject -clean
   ```

   以前に使用したビルドIDを持つプロジェクトを分析するには、常に、このステップで分析を開始してください。
2. プロジェクトコードを変換します。可能な場合には、ビルド統合を使用して、ソースファイルの選択と変換設定の正しい設定を自動化することをお勧めします。
   通常、ビルド統合には次の形式が使用されます。

   ```
   sourceanalyzer -b MyProject ... <build_command>
   ```

   または、手動で操作を行います。

   ```
   sourceanalyzer -b MyProject <files_to_analyze> <options_specific_to_language>
   ```

   変換の詳細については、分析しようとしているプログラミング言語のセクションを参照してください。
3. プロジェクトコードを分析し、結果をFortify Project Results(FPR)ファイルに保存します。

   ```
   sourceanalyzer -b MyProject -scan -f MyResults.fpr
   ```

   詳細については、「分析フェーズ」を参照してください。
   また、OpenText™ ScanCentral SASTを介して簡素化したり、リモートで実行したりもできます。詳細については、『*OpenText™ Fortify ScanCentral SASTインストール、設定、および使用ガイド*』を参照してください。

5.2. 変換フェーズ

通常どおりにコンパイルされているプロジェクトを正常に変換するには、プロジェクトをビルドするために必要な依存関係があることを確認します。特定の要件がある言語については、特定のソースコードタイプのセクションを参照してください。

分析プロセスの最初のステップ(ファイルの変換)を実行するための基本的なコマンドライン構文は、次のとおりです。

```
sourceanalyzer -b <build_id> ... <files>
```

または

```
sourceanalyzer -b <build_id> ... <compiler_command>
```

変換フェーズは、`sourceanalyzer` コマンドを使用した1回以上のFortify SASTの呼び出しで構成されます。Fortify SASTでは、ビルドID(`-b` オプション)を使用して呼び出しが相互に関連付けられます。後続の `sourceanalyzer` の呼び出しでは、ビルドIDに関連付けられたファイルリストに新しく指定されたソースファイルまたは環境設定ファイルが追加されます。

変換後に `-show-build-warnings` ディレクティブを使用して、変換フェーズで発生した警告やエラーのリストを表示できます。

```
sourceanalyzer -b <build_id> -show-build-warnings
```

ビルドIDに関連付けられたファイルを表示するには、 `-show-files` ディレクティブを使用します。

```
sourceanalyzer -b <build_id> -show-files
```

変換フェーズに関する特別な考慮事項

プロジェクトで変換フェーズを実行する前に、次の特別な考慮事項を検討してください。

- 動的言語(JavaScript/TypeScript、PHP、Python、Ruby)を変換する場合は、1回の呼び出しですべてのソースファイルを同時に指定する必要があります。Fortify SASTでは、後続の呼び出し時にビルドIDで関連付けられたファイルリストに新しいファイルを追加する機能はサポートされていません。
- 生成されるコードは、スクリプト、または解析ツールなどのツールによって、自動的に生成されます。このコードは最適化され、最小化されることもあれば、大きく複雑になることもあります。したがって、このコードでFortify SASTから報告される脆弱性をすべて修正するのは困難なことがあるため、変換から除外することをお勧めします。 `-exclude` コマンドラインオプションを使用して、このタイプのコードを変換から除外してください。
- ビルドマシン上でプロジェクトを変換し、パフォーマンスの高いシステムでスキャンを実行するには、「モバイルビルドセッションの使用」を参照してください。

5.3. 分析フェーズ

分析フェーズでは、変換時に作成された中間ファイルがスキャンされ、脆弱性結果ファイル(FPR)が作成されます。

このフェーズは、 `sourceanalyzer` の1回の呼び出しで構成されます。ビルドIDを指定し、 `-scan` ディレクティブを他の必要な分析オプションまたは出力オプションとともに含めます (「分析オプション」および「出力オプション」を参照)。

次の例は、分析フェーズを実行し、結果をFPRファイルに保存するコマンドライン構文を示しています。

```
sourceanalyzer -b MyProject -scan -f MyResults.fpr
```

Note

デフォルトでは、Fortify SASTのFPRファイルのソースコードが含まれています。

複数のビルドを単一のスキャンコマンドと組み合わせるには、コマンドラインに追加のビルドを追加します。

```
sourceanalyzer -b MyProject1 -b MyProject2 -b MyProject3 -scan -f MyResults.fpr
```

AI支援型分析を使用してコードを分析するには、LLM接続を構成するためにPostgreSQLデータベースを設定し、 `fortify-sca.properties` ファイルでデータベースを構成する必要があります。これらのプロパティはコマンドラインで指定することも可能ですが、結果のキャッシュが回避されるため、追加コストが発生する可能性があります。AI支援型分析の詳細については、「AIを使用した分析」を参照してください。

AI支援型分析を必要とする言語を分析していて、LLMまたはデータベース接続を構成しない場合、それらのファイルはシークレットスキャンによってのみスキャンされます。

5.4. 変換フェーズと分析フェーズの検証

Fortify Audit Workbenchの証明書には、スキャンによるコード分析が完了し、有効であるどうかが示されます。Fortify Audit Workbenchのプロジェクト概要には、Fortify SASTでスキャンされたコードに関する次の特定の情報が表示されます。

- スキャンされたファイルのリスト(ファイルサイズとタイムスタンプ付き)
- 変換に使用されるJavaクラスパス(該当する場合)
- 分析に使用されるRulepack
- Fortify SASTのランタイム設定とコマンドラインオプション
- 変換時または分析時に発生したエラーまたは警告
- コンピュータおよびプラットフォームの情報

> **Note**
> 結果証明書を取得するには、分析フェーズの出力形式にFPRを指定する必要があります。

結果証明書情報を表示するには、Fortify Audit WorkbenchでFPRファイルを開き、［**Tools**］>［**Project Summary**］>［**Certification**］の順に選択します。詳細については、*OpenText™ Fortify Audit Workbench ユーザガイド*を参照してください。

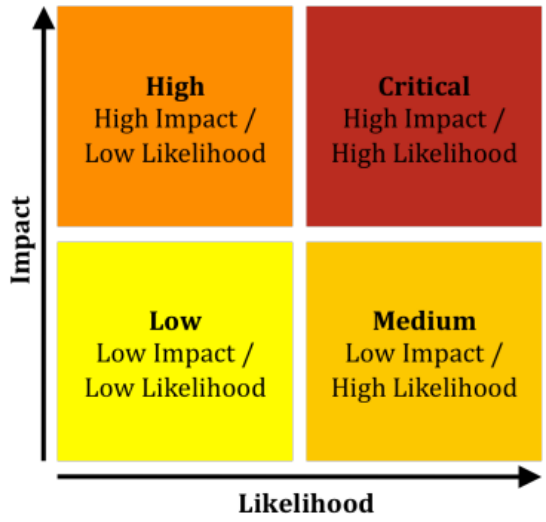
5.5. 問題の深刻度のランク付け

Fortify SASTでは、Fortify Priority Orderを使用して各問題の深刻度を計算します。

Fortify SASTでは、以下のデフォルトの深刻度バケットを使用します。

- 重大
- High
- Medium
- Low

次の図に示すように、Fortify SASTでは問題の影響と見込みに基づいて問題を評価する4象限モデルを採用しています。



問題は、**影響**と**見込み**に基づいて、**重大、高、中、低**の4段階で分類されます。

影響とは、専門のリサーチチームが現在のセキュリティ状況を評価したうえで割り当てているスコアです。

見込みの計算には以下の式が用いられます。

`Likelihood = (Accuracy × Probability × Confidence) / 25`

見込みがどのように決定されるかを理解するには、**精度**、**可能性**、**信頼度**を理解することが重要です。

精度

リサーチチームでは、ルールを作成する際に、そのルールに精度スコアを割り当てます。このスコアは、脆弱性を特定するための新しい技術が導入されることで、将来のバージョンで上下する可能性があります。
精度の範囲は `1.0 to 5.0` です。

可能性

可能性スコアは、
*「この問題が現実に存在する場合、攻撃者がそれを悪用する可能性はどの程度あるか？」*という問いに対する回答を反映しています。
この値はリサーチチームによって提供されたものであり、業界で新たな悪用手法や防御メカニズムが登場するにつれて、時間の経過とともに変化する可能性があります。
可能性の範囲は `1.0 to 5.0` です。

信頼度

信頼度スコアはFortify SASTによって生成され、ルールが正確であると仮定した場合に、モデリングの信頼性と問題を特定するために必要だった仮定の数を示しています。計算方法はアナライザごとに異なり、分析エンジンの進化に伴って変化する可能性があります。詳細については、「アナライザについて」を参照してください。
信頼度の範囲は `1.0 to 5.0` です。

6. AIを活用したSASTによる分析

Fortify SASTでは、AIを活用したSASTを使用して、特定の言語のソースファイルを構成済みの大規模言語モデル(LLM)にガイダンスとルールとともに渡すことで分析し、数十種類の脆弱性カテゴリーを特定します。

AIを活用したSASTは既存の分析を補完し、通常であればネイティブサポートの提供に多大な時間を要する言語のスキャンを可能にします。

オフクラウドユーザーは自分でLLMインスタンスをプロビジョニングし、独立して維持管理するPostgreSQLデータベースを通じて構成する必要があります。詳細については、「AIを活用した分析の要件」と「サポート対象のLLM」を参照してください。

このセクションでは、次のトピックについて説明します。

- LLMの構成
- データベースへの接続
- dbToolの使用
- AIを活用したSASTによるサンプル分析
- AIを活用したSASTの構成オプション
- レート制限
- pwtoolを使用した機密性の高い値の暗号化

6.1. LLMの構成

プロバイダーとモデルを指定することで、AIを活用したSASTを有効にします。

```
com.fortify.sca.ai.provider=<provider> com.fortify.sca.ai.model=<model, deployment, or inference profile identifier>
```

Example

```
com.fortify.sca.ai.provider=aws com.fortify.sca.ai.model=us.anthropic.claude-sonnet-4-5-20250929-v1:0
```

サポートされているLLMプロバイダーとモデルに関する詳細については、「LLMリクエスト構成」と「サポート対象のLLMを参照してください。

特定のLLMプロバイダーへのアクセスの構成に関する詳細情報は、以下のトピックを参照してください。

- AIを活用したSASTへのAWS　Bedrockの使用
- AIを活用したSASTへのAzureの使用
- AIを活用したSASTへのGoogle　Cloudの使用
- AIを活用したSASTへのOpenAI　APIの使用

6.1.1. AIを活用したSASTへのAWS　Bedrockの使用

Fortify SASTでは、AWS BedrockにAPIリクエストを送信するためにAWS SDK for Java(バージョン2)を使用します。AWS SDKでは、これらのリクエストを認証および許可するための資格情報が必要です。資格情報は複数の方法で指定できます。

- **SDKのデフォルトのプロバイダーチェーン**
  SDKは、デフォルトの認証情報プロバイダーチェーンを使用して、認証情報を自動的に検出するよう試みます。認証情報は、デフォルトの認証情報プロバイダーチェーンに含まれるいずれかの認証情報プロバイダー方式を通じて提供できます。詳細については、*AWSのドキュメント*を参照してください。

認証プロバイダー方式には以下のものがありますが、これらに限定されません。

- **認証情報ファイル:**
  AWSアクセスキー、AWSシークレットキー、およびオプションのAWSセッショントークンをAWS `credentials` ファイルで指定できます。`credentials` ファイルはLinuxまたはmacOSの場合は `<HOME_DIR>/.aws/credentials` に、Windowsの場合は `C:\Users\USERNAME\.aws\credentials` にあります。`credentials` ファイルの構成の詳細については、*AWSのドキュメント*を参照してください。
- **環境変数を構成する**
  AWSアクセスキー、AWSシークレットキー、およびオプションのAWSセッショントークンをシステム環境変数として指定できます。環境変数の構成の詳細については、*AWSのドキュメント*を参照してください。
- **EC2インスタンスのIAMロール**
  適切な権限があるIAMロールでEC2インスタンスに対してスキャンを実行できます。

- **Bedrock Bearerトークン**
  `com.fortify.sca.ai.aws.bearerTokenBedrock` プロパティを使用するか、`AWS_BEARER_TOKEN_BEDROCK` システム環境変数を設定することで、Bedrock Bearerトークン(APIキー)を提供できます。
- **PostgreSQLデータベースに認証情報を保存する**

dbToolを使用することで、AWSアクセスキー、AWSシークレットキー、およびオプションのAWSセッショントークンを指定されたデータベースに直接保存できます。詳細については、「dbToolの使用」を参照してください。

- `fortify-sca.properties` **ファイルに認証情報を追加する**

AWSアクセスキー、AWSシークレットキー、およびオプションのAWSセッショントークンは、Fortifyプロパティとして `fortify-sca.properties` ファイル内で明示的に設定できます。`-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。特定のプロパティに関する詳細については、「AWSの構成プロパティ」を参照してください。

-

6.1.2. AIを活用したSASTへのAzureの使用

Fortify SASTはAzureに対してHTTPリクエストを送信します。

認証

認証方法は複数存在しています。

- **Microsoft Entra ID**
  Fortify SASTでは、`DefaultAzureCredentialBuilder` を使用して認証情報を自動的に解決しているため、`DefaultAzureCredentialBuilder` でサポートされている任意のプロバイダー方式を使用して認証を構成できます。詳細については、*Azure Entraのドキュメント*を参照してください。
- **APIキー**
  以下のいずれかの方法を使用して、Microsoft Foundryデプロイメントの APIキーを指定できます。
  - dbToolを使用して `com.fortify.sca.ai.azure.apiKey` プロパティをデータベースに保存します。詳細については、「dbToolの使用」を参照してください。
  - `FORTIFY_AI_AZURE_API_KEY` システム環境変数を設定します。
  - `fortify-sca.properties` ファイル内で `com.fortify.sca.ai.azure.apiKey` プロパティを設定します。`-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。

Azure OpenAIエンドポイントの指定

ベースURLかリソースを使用して、Microsoft FoundryデプロイメントのAzure OpenAIエンドポイントを指定する必要があります。

- 以下のいずれかの方法でベースURLを指定します。
  - dbToolを使用して `com.fortify.sca.ai.azure.baseUrl` プロパティをデータベースに保存します。詳細については、「dbToolの使用」を参照してください。
  - `FORTIFY_AI_AZURE_BASE_URL` システム環境変数を設定します。
  - `fortify-sca.properties` ファイル内で `com.fortify.sca.ai.azure.baseUrl` プロパティを設定します。`-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。
- 以下のいずれかの方法でリソースを指定します。

- dbToolを使用して `com.fortify.sca.ai.azure.resource` プロパティをデータベースに保存します。詳細については、「dbToolの使用」を参照してください。
- `FORTIFY_AI_AZURE_RESOURCE` システム環境変数を設定します。
- `fortify-sca.properties` ファイル内で `com.fortify.sca.ai.azure.resource` プロパティを設定します。 `-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。

-

6.1.3. AIを活用したSASTへのGoogle　Cloudの使用

`fortify-sca.properties` ファイルではdbToolを使用して、コマンドラインでは `-D` オプションを使用して、データベース内で次のプロパティを設定できます。

- `com.fortify.sca.ai.google.project` プロパティをGoogle　CloudプロジェクトのIDに設定します。
- `com.fortify.sca.ai.google.location` プロパティを、使用しているモデルに対して選択したGoogle　Cloudリージョンに設定します。

AIを活用したSASTでは、Application Default Credentials (ADC)チェーンを使用してGoogle Cloud資格情報を自動的に検出するため、ADCがサポートするあらゆる方法で資格情報を提供できます。 `com.fortify.sca.ai.google.credentialsFile` プロパティを使用してGoogle資格情報ファイルの場所を指定することもできます。

6.1.4. AIを活用したSASTへのOpenAI　APIの使用

Fortify　SASTはOpenAIに対してHTTPリクエストを送信します。

認証

以下のいずれかの方法でAPIキーを指定する必要があります。

- dbToolを使用して `com.fortify.sca.ai.openai.apiKey` プロパティをデータベースに保存します。詳細については、「dbToolの使用」を参照してください。
- `OPENAI_API_KEY` システム環境変数を設定します。
- `fortify-sca.properties` ファイル内で `com.fortify.sca.ai.openai.apiKey` プロパティを設定します。 `-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。

(省略可)ベースURLを指定する

以下のいずれかの方法でベースURLを指定できます。

- dbToolを使用して `com.fortify.sca.ai.openai.baseUrl` プロパティをデータベースに保存します。詳細については、「dbToolの使用」を参照してください。
- `OPENAI_BASE_URL` システム環境変数を設定します。
- `fortify-sca.properties` ファイル内で `com.fortify.sca.ai.openai.baseUrl` プロパティを設定します。 `-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。

(省略可)組織IDを指定する

以下のいずれかの方法で組織IDを指定できます。

- dbToolを使用して `com.fortify.sca.ai.openai.organization` プロパティをデータベースに保存します。詳細については、「dbToolの使用」を参照してください。
- `OPENAI_ORG_ID` システム環境変数を設定します。
- `fortify-sca.properties` ファイル内で `com.fortify.sca.ai.openai.organization` プロパティを設定します。 `-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。

(省略可)プロジェクトIDを指定する

以下のいずれかの方法でプロジェクトIDを指定できます。

- dbToolを使用して `com.fortify.sca.ai.openai.project` プロパティをデータベースに保存します。詳細については、「dbToolの使用」を参照してください。
- `OPENAI_PROJECT_ID` システム環境変数を設定します。
- `fortify-sca.properties` ファイル内で `com.fortify.sca.ai.openai.project` プロパティを設定します。 `-D` オプションを使用して、コマンドラインでプロパティを指定することもできます。

6.2. データベースへの接続

Fortify SASTをPostgreSQLデータベースに接続するように構成することで、以下の機能を有効にすることをおすすめします。

- LLMの結果をキャッシュして、コストを削減してスキャン時間を短縮する。
- LLMへの接続やAIを活用したSASTの動作の構成に使用する集中管理型構成プロパティを保存する。
- `sourceanalyzer` の複数のインスタンス間で分散型レート制限を有効化する。
- LLMトークン使用データを保存する。

データベースに接続するには、以下のJDBC接続プロパティをfortify-sca.propertiesファイル内で、またはコマンドライン引数として指定します。

プロパティ	説明(Description)
com.fortify.sca.ai.db.url	データベースのJDBC接続URLを指定します。  **Example** `jdbc:postgresql:my.domain.com:5432/ai_sast_db?currentSchema=ai_sast_schema` URLの `currentSchema` クエリパラメータを使用して、PostgreSQLスキーマを指定できます。スキーマが指定されていない場合は、デフォルトのスキーマ `public` が使用されます。 `FORTIFY_AI_DB_URL` システム環境変数を設定することもできます。
com.fortify.sca.ai.db.prop.username	データベースへの接続に使用するユーザ名を指定します。 `FORTIFY_AI_DB_PROP_USERNAME` システム環境変数を設定することもできます。
com.fortify.sca.ai.db.prop.password	データベースへの接続に使用するパスワードを指定します。 これは機密性の高いプロパティです。ユーザーは、`pwtool` を使用して値を難読化することで、プロパティファイルに平文で保存したり、コマンドライン引数として使用したりすることを避けることができます。 `FORTIFY_AI_DB_PROP_PASSWORD` システム環境変数を設定することもできます。

com.fortify.sca.ai.db.prop.*	PostgreSQL　JDBC接続プロパティは、先頭に「`com.fortify.sca.ai.db.prop.`」を付けることで設定できます。
	たとえば、SSLを使用した認証を有効にするには、以下のプロパティを設定します。
	`com.fortify.ai.db.prop.ssl=true`
	`com.fortify.ai.db.prop.sslmode=verify-full`
	`com.fortify.ai.db.prop.sslcert=my/dir/postgresql.crt`
	`com.fortify.ai.db.prop.sslkey=my/dir/postgresql.pk8`
	`com.fortify.ai.db.prop.sslrootcert=my/dir/root.crt`
	利用可能なPostgres JDBC接続プロパティの詳細については、*PostgreSQLのドキュメント*を参照してください。
	SSLキーと証明書を提供するように、`FORTIFY_AI_DB_PROP_SSL_CERT`、`FORTIFY_AI_DB_PROP_SSL_KEY`、`FORTIFY_AI_DB_PROP_SSL_ROOT_CERT` の各システム環境変数を設定することもできます。

詳細については、「データベース構成プロパティ」を参照してください。

6.3. dbToolの使用

dbToolは、データベース内の構成値のプロビジョニングと更新に使用されます。

dbToolはFortify SASTと一緒にインストールされており、 *<sast_install_directory>/bin* ディレクトリにあります。

dbToolを呼び出す際は、必要なデータベース接続プロパティを指定する必要があります。

Example

```
dbTool --com.fortify.sca.ai.db.url=<ai-db-url> --com.fortify.sca.ai.db.prop.username=<ai-db-username> --com.fortify.sca.ai.db.prop.password=<ai-db-password>
```

dbTool を使用して、 `--store=<property>=<value>` 引数を指定してプロパティ値をデータベースに保存します。

Example

```
--store="com.fortify.sca.ai.provider=aws" --store="com.fortify.sca.ai.model=us.anthropic.claude-sonnet-4-5-20250929-v1:0"
```

dbToolを使用して、 `--storeFile=<path to .properties file>` 引数を指定してプロパティファイルからプロパティのコレクションを保存します。

Example

```
--storeFile=/path/to/my.properties
```

プロパティファイルには、 `key=value` 形式を使用して各行に1つのプロパティが必要です。

Example

```
com.fortify.sca.ai.provider=aws
com.fortify.sca.ai.model=us.anthropic.claude-sonnet-4-5-20250929-v1:0
```

機密性の高いプロパティの値をデータベースに保存する前に暗号化するために、base64でエンコードされたAES 256暗号化キーを提供できます。暗号化されたプロパティ値を復号化するには、ファイルのスキャン時に暗号化キーを sourceanalyzer に提供する必要があります。

暗号化キーまたは暗号化キーファイルを指定するには、以下のプロパティ値を使用できます。

- `com.fortify.sca.ai.config.encryptionKey`
- `com.fortify.sca.ai.config.encryptionKeyFile`

Example

```
--com.fortify.sca.ai.config.encryptionKey="ZWm2HqvK3Jjrqb12ne1Wu/pU8qla/CHQcSBxKa/7qrU="
```

Note

暗号化キーまたは暗号化キーファイルを指定しない場合、dbToolは機密性の高いプロパティ値を難読化し、データベースに平文で保存されないようにします。

以下はdbToolの使い方の一例です。

Example

```
dbTool --com.fortify.sca.ai.db.url=jdbc:postgresql:my.domain.com:5432/sast-ai-db --
com.fortify.sca.ai.db.prop.username=ai-db-username --com.fortify.sca.ai.db.prop.password=ai-
db-password --store="com.fortify.sca.ai.provider=aws" --
store="com.fortify.sca.ai.model=us.anthropic.claude-sonnet-4-5-20250929-v1:0" --
storeFile="/path/to/file.properties" --
com.fortify.sca.ai.config.encryptionKey="ZWm2HqvK3Jjrqb12ne1Wu/pU8qIa/CHQcSBxKa/7qrU="
```

6.4. AIを活用したSASTによるサンプル分析

AIを活用したSASTでソースファイルを有効にする方法については、関連する言語のセクションを参照してください。

スキャンフェーズ中にデータベース内でLLMプロパティを設定した場合、基本的なコマンドライン構文は以下の通りです。

Example

```
sourceanalyzer -b <build_id> -scan <database_connection_properties> <other_scan_options>
```

データベース接続プロパティを `<SAST_INSTALL_DIR>/Core/config/fortify-sca.properties` ファイルで構成する場合、スキャン時にデータベース接続プロパティを指定する必要はありません。

スキャン時にすべてのLLMプロパティを指定し、デフォルトの認証情報プロバイダーチェーンを使用して認証情報を取得するか、関連する認証情報を `fortify-sca.properties` ファイルまたはコマンドラインで設定することも可能です。

AIを活用したSASTを使用するには、データベースに接続するための構成の提供は厳密に必要というわけではありません。データベースを使用せずにAIを活用したSASTで分析を行う場合は、以下の基本的なコマンドライン構文を使用します。

Example

```
sourceanalyzer -b <build_id> -scan <AI_configuration_properties> <other_scan_options>
```

Caution

結果のキャッシュが不可能になり、追加コストが発生する可能性があるため、データベースを使用せずにAIを活用したSASTを利用することをOpenTextでは推奨していません。

以下の例は、AIを活用したSASTを使用してサンプルErlangソースファイルを解析する際の、基本的なコマンドライン構文を示しています。

Example

```
sourceanalyzer -b myProject -clean sourceanalyzer -b myProject <file_path>/sample.erl
sourceanalyzer -b myProject -scan -Dcom.fortify.sca.ai.provider=aws -
Dcom.fortify.sca.ai.model="us.anthropic.claude-sonnet-4-5-20250929-v1:0" -f my_AI_results.fpr
```

6.5. AIを活用したSASTの構成オプション

以降のセクションでは、AIを活用したSASTの構成で使用できるプロパティについて説明します。dbToolを使用してデータベースにプロパティを保存するか、`fortify-sca.properties` ファイル内でプロパティを設定するか、または `-D` オプションを使用してコマンドラインでプロパティを指定します。

LLMリクエスト構成

プロパティ	説明(Description)
com.fortify.sca.ai.enabled	falseに設定すると、AIを活用したSASTが無効になります。 **Important** このプロパティは `fortify-sca.properties` で設定するか、コマンドライン引数として渡します。dbToolを使用してデータベース内のプロパティを構成しても、効果は得られません。 **デフォルト**: true
com.fortify.sca.ai.provider	必須です。LLMベンダーを指定します。 **デフォルト**: null **サポートされている値:** • azure • openai • aws

com.fortify.sca.ai.model	必須です。LLMを指定します。 **デフォルト**: null **Azureの場合:** 以下のモデル名を受け付けます。 ◆ claude-sonnet-4-6 ◆ claude-opus-4-6 ◆ claude-sonnet-4-5 ◆ gpt-5.4 ◆ gpt-5.2(検証済み) ◆ gpt-5.2-Codex ◆ gpt-5.1 ◆ gpt-5.1-Codex ◆ gpt-5 ◆ gpt-5-Codex **Google Cloudの場合:** モデル名を受け付けます。任意のAnthropic Claudeモデルを受け付けます。使用可能なモデルについては、Google Cloudのマニュアルを参照してください。 例: claude-sonnet-4-6 **OpenAIの場合:** 以下のモデル名を受け付けます。 ◆ gpt-5.4 ◆ gpt-5.2(検証済み) ◆ gpt-5.2-Codex ◆ gpt-5.1 ◆ gpt-5.1-Codex ◆ gpt-5 ◆ gpt-5-Codex **AWSの場合**: システム推論プロファイルまたはアプリケーション推論プロファイルの推論プロファイルIDまたは推論プロファイルARNを受け入れます。 `com.fortify.sca.ai.model` プロパティの代わりに `com.fortify.sca.ai.aws.inferenceProfile` プロパティを設定することもできます。 カスタムアプリケーション推論プロファイルを使用しており、推論プロファイルのベースとなるモデルを解決するための適切な権限を付与していない場合(Bedrock `GetInferenceProfile` APIを呼び出す権限が必要)、`com.fortify.sca.ai.model` プロパティをベースとなるモデルIDに設定し、`com.fortify.sca.ai.aws.inferenceProfile` プロパティをアプリケーション推論プロファイルARNに設定できます。 指定された推論プロファイルでは、次の基盤モデルのいずれかを使用する必要があります。 ◆ Claude Sonnet 4.6 (anthropic.claude-sonnet-4-6)

- Claude Opus 4.6 (anthropic.claude-opus-4-6-v1)
- Claude Sonnet 4.5 (anthropic.claude-sonnet-4-20250514-v1:0)
- Claude Sonnet 4 (anthropic.claude-sonnet-4-5-20250929-v1:0)

サポートされているAWSシステム推論プロファイル:

- Claude Sonnet 4.6
  - global.anthropic.claude-sonnet-4-6
  - us.anthropic.claude-sonnet-4-6
  - au.anthropic.claude-sonnet-4-6
  - eu.anthropic.claude-sonnet-4-6
  - jp.anthropic.claude-sonnet-4-6
- Claude Opus 4.6
  - global.anthropic.claude-opus-4-6-v1
  - us.anthropic.claude-opus-4-6-v1
  - au.anthropic.claude-opus-4-6-v1
  - eu.anthropic.claude-opus-4-6-v1
- Claude Sonnet 4.5(検証済み)
  - global.anthropic.claude-sonnet-4-5-20250929-v1:0
  - us.anthropic.claude-sonnet-4-5-20250929-v1:0
  - au.anthropic.claude-sonnet-4-5-20250929-v1:0
  - eu.anthropic.claude-sonnet-4-5-20250929-v1:0
  - jp.anthropic.claude-sonnet-4-5-20250929-v1:0
- Claude Sonnet 4
  - global.anthropic.claude-sonnet-4-20250514-v1:0
  - us.anthropic.claude-sonnet-4-20250514-v1:0
  - apac.anthropic.claude-sonnet-4-20250514-v1:0
  - eu.anthropic.claude-sonnet-4-20250514-v1:0



Note

システム推論プロファイルは、そのプロファイルがサポートするAWSリージョンで使用する必要があります。



Example

`us.anthropic.claude-sonnet-4-5-20250929-v1:0` は `us-east-1` リージョンで使用できますが、 `eu-west-1` リージョンでは使用できません。

com.fortify.sca.ai.llm.parallelism	同時LLMリクエストの最大数。 **デフォルト**: 4 x 利用可能なプロセッサ
com.fortify.sca.ai.llm.rateLimiter.enabled	LLMリクエストレートリミッターが有効かどうかを指定します。 **デフォルト**: true
com.fortify.sca.ai.llm.rateLimiter.updateDistributedLimits	指定された `requestsPerMinute` と `tokensPerMinute` によって、データベース内の既存の制限が更新されるかどうかを指定します。 trueに設定すると、データベース内の制限が更新されます。falseに設定すると、既存の制限は更新されず、指定された制限は無視されます。 **デフォルト**: false データベース内で分散レート制限を設定するために `dbTool` を使用することをOpenTextでは推奨しています。
com.fortify.sca.ai.llm.requestsPerMinute	1分間に許可されるLLMリクエストの最大数を指定します。このプロパティでは、同じデータベースに接続されている `sourceanalyzer` のすべてのインスタンスの合計制限を設定します。 データベースが構成されていない場合、このプロパティでは単一の `sourceanalyzer` インスタンスの最大制限を設定します。 **デフォルト**: 200
com.fortify.sca.ai.llm.tokensPerMinute	1分間に許可されるLLMリクエストの入力および出力トークンの最大数を指定します。このプロパティでは、同じデータベースに接続されている `sourceanalyzer` のすべてのインスタンスの合計制限を設定します。 データベースが構成されていない場合、このプロパティでは単一の `sourceanalyzer` インスタンスの最大制限を設定します。 **デフォルト**: 200,000
com.fortify.sca.ai.llm.maxRequestCount	1回のスキャンで実行可能なLLMリクエストの最大数。 このプロパティにより、ユーザーが誤って大きなプロジェクトをスキャンしてしまったことによって高額な請求が発生するのを防ぐことができます。LLMリクエストを送信する前に、必要なリクエストの数を計算します。必要なリクエストの数が上限を超えた場合、LLMリクエストを行わずにスキャンは中断されます。 **デフォルト**: 10,000

com.fortify.sca.ai.fileChunkSize	LLMへのリクエストで許可される最大文字数。ファイルがこの文字数を超えた場合、ファイルは複数のファイルチャンクに分割されます。 チャンクサイズを変更すると、チャンクサイズの変更によって関連ファイルの内容が変わる場合、一部のキャッシュエントリが古くなる可能性があります。影響を受けたファイルチャンクについては、新たなLLMリクエストが必要となります。 **デフォルト**: 50,000

ベンダー構成

プロパティ	説明(Description)
AWS構成プロパティ	
com.fortify.sca.ai.aws.inferenceProfile	プロファイルのIDまたはARNを使用してBrock推論プロファイルを指定します。 `com.fortify.sca.ai.model` プロパティの代わりにこれを設定できます。 カスタムアプリケーション推論プロファイルを使用しており、推論プロファイルのベースとなるモデルを解決するための適切な権限を付与していない場合(Bedrock `GetInferenceProfile` APIを呼び出す権限が必要)、`com.fortify.sca.ai.model` プロパティをベースとなるモデルIDに設定し、 `com.fortify.sca.ai.aws.inferenceProfile` プロパティをアプリケーション推論プロファイルARNに設定できます。
com.fortify.sca.ai.aws.region	LLMリクエストを実行するAWSリージョンを指定します。 **デフォルト**: null 以下の方法でも指定できます。 • 環境変数: `AWS_REGION` • AWS構成または認証情報ファイル: `region`
com.fortify.sca.ai.aws.profile	AWS `config` ファイルまたは `credentials` ファイル内のどのプロファイルを使用して AWSで認証するかを指定します。 **デフォルト**: null **環境変数**: `AWS_PROFILE`
com.fortify.sca.ai.aws.accessKeyId	AWSでの認証時に使用するAWSアクセスキーを指定します。 設定する場合は、 `com.fortify.sca.ai.aws.secretAccessKey` と `com.fortify.sca.ai.aws.sessionToken` も設定する必要があります(短期認証情報を使用する場合)。 **デフォルト**: null 以下の方法でも指定できます。 • 環境変数: `AWS_ACCESS_KEY_ID` • AWS構成または認証情報ファイル: `aws_access_key_id`

com.fortify.sca.ai.aws.secretAccessKey	AWSでの認証時に使用するAWSシークレットアクセスキーを指定します。 設定する場合は、`com.fortify.sca.ai.aws.secretAccessKey` と `com.fortify.sca.ai.aws.sessionToken` も設定する必要があります(短期認証情報を使用する場合)。 **デフォルト**: null 以下の方法でも指定できます。 • 環境変数: `AWS_SECRET_ACCESS_KEY` • AWS構成または認証情報ファイル: `aws_secret_access_key` これは機密性の高いプロパティです。値はログ内でマスクされます。ユーザーは、`pwtool` を使用して値を難読化することで、プロパティファイルに平文で保存したり、コマンドライン引数として使用したりすることを避けることができます。
com.fortify.sca.ai.aws.sessionToken	AWSでの認証時に使用するAWSセッショントークを指定します。 設定する場合は、`com.fortify.sca.ai.aws.accessKeyId` と `com.fortify.sca.ai.aws.secretAccessKey.` も設定する必要があります。 以下の方法でも指定できます。 • 環境変数: `AWS_SESSION_TOKEN` • AWS構成または認証情報ファイル: `aws_session_token` これは機密性の高いプロパティです。値はログ内でマスクされます。ユーザーは、`pwtool` を使用して値を難読化することで、プロパティファイルに平文で保存したり、コマンドライン引数として使用したりすることを避けることができます。
com.fortify.sca.ai.aws.bearerTokenBedrock	AWSでの認証に使用できるBedrock Bearerトークンを指定します。 `AWS_BEARER_TOKEN_BEDROCK` システム環境変数を設定することで指定することもできます。 これは機密性の高いプロパティです。値はログ内でマスクされます。ユーザーは、`pwtool` を使用して値を難読化することで、プロパティファイルに平文で保存したり、コマンドライン引数として使用したりすることを避けることができます。
Azure構成プロパティ	

com.fortify.sca.ai.azure.deployment	Microsoft Foundryのデプロイメントの名前を指定します。 デプロイメントの名前が `com.fortify.sca.ai.model` に指定されたモデルの名前と同じでない場合にのみ必要です。
com.fortify.sca.ai.azure.resource	Azure Foundryリソース名を指定します。 `com.fortify.sca.ai.azure.resource` と `com.fortify.sca.ai.azure.baseUrl` のいずれかを指定しますが、両方は指定しないでください。 `FORTIFY_AI_AZURE_RESOURCE` システム環境変数を設定することで指定することもできます。
com.fortify.sca.ai.azure.baseUrl	Microsoft FoundryデプロイメントのAzure OpenAIエンドポイントを指定します。 `com.fortify.sca.ai.azure.baseUrl` と `com.fortify.sca.ai.azure.resource` のいずれかを指定しますが、両方は指定しないでください。 `FORTIFY_AI_AZURE_BASE_URL` システム環境変数を設定することで指定することもできます。
com.fortify.sca.ai.azure.apiKey	Microsoft Foundryデプロイメントでの認証に使用するシークレットAPIキーを指定します。 **環境変数**: `FORTIFY_AI_AZURE_API_KEY`
Google Cloud構成プロパティ	
com.fortify.sca.ai.google.project	Google CloudプロジェクトIDを指定します。
com.fortify.sca.ai.google.location	モデルが展開されるGoogle Cloudのリージョンまたはロケーションを指定します。 **例**: us-east5またはグローバル。
com.fortify.sca.ai.google.credentialsFile	Google Cloud資格情報JSONファイルへのパスを指定します。 必須ではありません。資格情報が標準のApplication Default Credentials (ADC)チェーンからは検出できない場合にのみ設定します。ほとんどの環境では、これを設定せずにそのままにしておき、ADCに資格情報の自動解決を任せてください。
OpenAI構成プロパティ	
com.fortify.sca.ai.openai.apiKey	OpenAIでの認証に使用するシークレットAPIキーを指定します。 **環境変数**: `OPENAI_API_KEY`

com.fortify.sca.ai.openai.organization	OpenAI組織の識別子を指定します。 複数の組織に所属している場合にのみ必要です。 **環境変数**: OPENAI_ORG_ID
com.fortify.sca.ai.openai.project	OpenAIプロジェクトの識別子を指定します。 レガシーユーザAPIキーを使用してプロジェクトにアクセスする場合にのみ必要です。 **環境変数**: OPENAI_PROJECT_ID
com.fortify.sca.ai.openai.baseUrl	OpenAIサービスに接続するために使用するベースURLを指定します。 OpenAIサーバに直接接続しない場合にのみ必要です。 デフォルトでは本番環境(https://api.openai.com/v1)です。 **環境変数**: OPENAI_BASE_URL

データベース構成

プロパティ	説明(Description)
データベース接続プロパティ	
com.fortify.sca.ai.db.url	データベースのJDBC接続URLを指定します。  **Example** `jdbc:postgresql:my.domain.com:5432/ai_sast_db?currentSchema=ai_sast_schema` LLM結果のキャッシュ、集中型構成、分散レート制限、LLMリクエスト使用状況データのために、データベースに接続するのに必要です。 URLの `currentSchema` クエリパラメータを使用して、PostgreSQLスキーマを指定できます。スキーマが指定されていない場合は、デフォルトのスキーマ `public` が使用されます。 詳細については、*PostgreSQLのドキュメント*を参照してください。 **デフォルト**: null
com.fortify.sca.ai.db.prop.username	データベースへの接続に使用するユーザ名を指定します。 LLM結果のキャッシュ、集中型構成、分散レート制限、LLMリクエスト使用状況データのために、データベースに接続するのに必要です。 **デフォルト**: null
com.fortify.sca.ai.db.prop.password	データベースへの接続に使用するパスワードを指定します。 これは機密性の高いプロパティです。値はログ内でマスクされます。ユーザーは、 `pwtool` を使用して値を難読化することで、プロパティファイルに平文で保存したり、コマンドライン引数として使用したりすることを避けることができます。 **デフォルト**: null

com.fortify.sca.ai.db.prop.*	PostgreSQL　JDBC接続プロパティは、先頭に「`com.fortify.sca.ai.db.prop.`」を付けることで設定できます。
	デフォルト: null
	たとえば、SSLを使用した認証を有効にするには、以下のプロパティを設定します。
	`com.fortify.ai.db.prop.ssl=true`
	`com.fortify.ai.db.prop.sslmode=verify-full`
	`com.fortify.ai.db.prop.sslcert=my/dir/postgresql.crt`
	`com.fortify.ai.db.prop.sslkey=my/dir/postgresql.pk8`
	`com.fortify.ai.db.prop.sslrootcert=my/dir/root.crt`
	利用可能なPostgres JDBC接続プロパティの詳細については、*PostgreSQLのドキュメント*を参照してください。

データベース動作プロパティ	
com.fortify.sca.ai.cache.enabled	LLM結果キャッシュを有効にするかどうかを指定します。無効にすると、キャッシュの読み取りと書き込みの両方が無効になります。 **デフォルト**: true より具体的なプロパティである`com.fortify.sca.ai.cache.read.enabled`と`com.fortify.sca.ai.cache.write.enabled`が設定されている場合は、これらのプロパティが優先されます。
com.fortify.sca.ai.cache.read.enabled	LLM結果キャッシュからの読み取りを有効にするかどうかを指定します。 **デフォルト**: true
com.fortify.sca.ai.cache.write.enabled	LLM結果キャッシュへの書き込みを有効にするかどうかを指定します。 **デフォルト**: true
com.fortify.sca.ai.cache.missOnNewModel	キャッシュされた結果で使用されているLLMモデルが現在のリクエストのモデルと異なる場合、キャッシュ内のLLM結果をキャッシュミスとみなすかどうかを指定します。 つまり、これをtrueに設定すると、新しいモデルが使用された場合に、キャッシュされた結果が削除されます。 デフォルト: false

com.fortify.sca.ai.cache.missOnNewPrompt	キャッシュされた結果で使用されているLLMプロンプトが現在のリクエストのプロンプトと異なる場合、キャッシュ内のLLM結果をキャッシュミスとみなすかどうかを指定します。 つまり、これをtrueに設定すると、関連するルールパックが更新された場合に、キャッシュされた結果が削除されます。 **デフォルト**: true
com.fortify.sca.ai.cache.maxSize	LRU削除前にキャッシュされるLLM結果の最大数。 **デフォルト**: 1,000,000
com.fortify.sca.ai.cache.ttl.day	使用されていないLLM結果がキャッシュから削除されるまでの日数。 **デフォルト**: 30
com.fortify.sca.ai.remoteConfig.enabled	接続されたデータベースから構成プロパティを取得できるかどうかを指定します。 **デフォルト**: true
com.fortify.sca.ai.config.encryptionKey	データベースに保存されている機密性の高いプロパティの値を暗号化および復号化するために使用される、オプションのbase64でエンコードされたAES-256対称暗号化キー。 データベースから機密性の高い構成を取得するには、暗号化キーをすべての `sourceanalyzer` インスタンスに配布する必要があります。暗号化キーは、KMS、OSキーストア、パスワードマネージャーなどを使用して配布できます。 **Caution** 暗号化キーを紛失した場合、そのキーを使用して暗号化された構成値は復元できなくなります。 `com.fortify.sca.ai.config.encryptionKey` と `com.fortify.sca.ai.config.encryptionKeyFile` のいずれかを通じて暗号化キーが指定されていない場合、データベースに保存される機密性の高いプロパティの値は難読化され、平文で保存されなくなります。 これは機密性の高いプロパティです。値はログ内でマスクされます。ユーザーは、 `pwtool` を使用して値を難読化することで、プロパティファイルに平文で保存したり、コマンドライン引数として使用したりすることを避けることができます。 **デフォルト**: null

com.fortify.sca.ai.config.encryptionKeyFile	データベースに保存されている機密性の高いプロパティの値を暗号化および復号化するために使用される、base64でエンコードされたAES-256対称暗号化キーを含むオプションのファイルパス。 データベースから機密性の高い構成を取得するには、暗号化キーをすべての `sourceanalyzer` インスタンスに配布する必要があります。暗号化キーは、KMS、OSキーストア、パスワードマネージャーなどを使用して配布できます。 **Caution** 警告: 暗号化キーを紛失した場合、そのキーを使用して暗号化された構成値は復元できなくなります。 `com.fortify.sca.ai.config.encryptionKey` と `com.fortify.sca.ai.config.encryptionKeyFile` のいずれかを通じて暗号化キーが指定されていない場合、データベースに保存される機密性の高いプロパティの値は難読化され、少なくとも平文では保存されなくなります。 **デフォルト**: null
com.fortify.sca.ai.usage.enabled	使用状況テーブルへの書き込みが有効かどうかを指定します。 **デフォルト**: true

ファイル構成

プロパティ	説明(Description)
com.fortify.sca.ai.exclude.directories	指定された、セミコロンで区切られた正規表現パターンの1つに名前が一致する、ディレクトリ内にネストされたファイルを除外します。 デフォルト値: `test;tests;__tests__;testing;testcases;spec;example;examples;sample;samples;demo;demos;doc;docs;documentation`
com.fortify.sca.ai.exclude.fileNames	指定された、セミコロンで区切られた正規表現パターンの1つに名前が一致するファイルを除外します。 デフォルト値: `.*Test\..*;.*_test\..*;.*\.test\..*;.*\.spec\..*;.*Tests\..*;.*_spec\..*`

pwtool構成

プロパティ	説明(Description)
com.fortify.sca.ai.pwtool.encryptionKeyFile	pwtoolによって生成される暗号化キーファイルへのパス。ユーザがpwtoolを使用して難読化された機密性の高いプロパティの値を指定する場合に必要です。 **デフォルト**: null

6.6. レート制限

サービスの信頼性とリソースの公平な配分を実現するために、LLMプロバイダーはリクエストレート制限とトークンレート制限を設けています。これらの制限を超えるとスロットリングが発生することがあります。リクエストがスロットリングされた場合、Fortify SASTでは一時的にリクエストレートを低下させ、スロットリングされた各リクエストを最大試行回数まで再試行します。散発的なスロットリングはスキャン結果にほとんど影響を与えませんが、過度なスロットリングはスキャン時間の増加や、一部のファイルが分析されないことによる結果の欠落を引き起こす可能性があります。

スロットリングの問題は以下のいずれかの方法で解決できます。

- 使用しているモデルのリクエストレート制限とトークンレート制限の引き上げを、LLMプロバイダーに申請できます。
- Fortify SASTがLLMプロバイダーに対してリクエストを送信するレートを調整するために、クライアント側のレート制限を設定できます。接続されたデータベースを使用している場合は、 dbTool を使用して com.fortify.sca.ai.llm.requestsPerMinute プロパティと com.fortify.sca.ai.llm.tokensPerMinute プロパティを設定し、データベースに接続されているすべてのFortify SASTインスタンス間で分散レート制限を有効にします。

  または、 com.fortify.sca.ai.llm.rateLimiter.updateDistributedLimits をtrueに設定し(接続されたデータベースを使用している場合)、 com.fortify.sca.ai.llm.requestsPerMinute プロパティと com.fortify.sca.ai.llm.tokensPerMinute プロパティを fortify-sca.properties ファイル内で、またはコマンドラインで -D オプションを使用して設定します。

6.7. pwtoolを使用した機密性の高い値の暗号化

機密性の高いプロパティ値の暗号化された値を生成するにはpwtoolを使用できます。暗号化された値はプレーンテキスト値の代わりに使用できます。これにより、機密性の高い値をプレーンテキストで fortify-sca.properties ファイルに保存したり、コマンドライン引数としてプレーンテキストで渡したりする必要がなくなります。

pwtoolを使用して以下のプロパティを暗号化できます。

- com.fortify.sca.ai.azure.apiKey
- com.fortify.sca.ai.openai.apiKey
- com.fortify.sca.ai.db.prop.password
- com.fortify.sca.ai.aws.secretAccessKey
- com.fortify.sca.ai.aws.sessionToken
- com.fortify.sca.ai.config.encryptionKey

機密性の高いプロパティ値を暗号化するには:

1. コマンドプロンプトで以下のコマンドを実行します。

   ```
   <tools_install_dir>/bin/pwtool <pwtool_keys_file>
   ```

2. プロンプトが表示されたら、機密性の高い値を入力して**Enter**キーを押します。
3. pwtoolでは、ステップ1で指定されたパス上のファイルに保存される新しいキーを生成するか、指定されたパス上に存在する既存のファイルを再利用します。pwtoolでは、入力された機密性の高い値を暗号化するためにキーを使用します。
4. 暗号化されたシークレットをコピーし、 fortify-sca.properties ファイル内にプロパティの値として、またはコマンドライン引数として貼り付けます。

5. 機密性の高いプロパティ値をさらに暗号化するには、暗号化したいプロパティ値ごとにステップ1から4を繰り返します。
6. `fortify-sca.properties` ファイルで以下のプロパティを設定するか、コマンドライン引数として渡します。
`com.fortify.sca.ai.pwtool.encryptionKeyFile=<pwtool_keys_file>`

7. Java、Kotlin、およびJSPプロジェクトの分析

このセクションでは、Java、Kotlin、JSPプロジェクト、およびこれらの言語を組み合わせて使用するプロジェクトを変換する方法について説明します。

Fortify SASTでは、Jakarta EE (Java EE)アプリケーション(JSPファイル、環境設定ファイル、展開デスクリプタを含む)、Javaバイトコード、およびLombokアノテーション付きJavaコードの分析をサポートしています。

- Gradleとの統合
- Mavenとの統合
- Bazelとの統合
- Antとの統合
- JavaおよびKotlinの手動変換構文
- Kotlinスクリプトの分析
- KotlinとJavaの変換相互運用性
- Javaの警告の処理
- Jakarta EE (Java EE)アプリケーションの分析
- Javaバイトコードの分析
- Java、Kotlin、およびJSP変換および分析に関する問題のトラブルシューティング

7.1. Gradleとの統合

Fortify SASTは、Gradleでビルドされたプロジェクトとの変換統合を提供します。ビルドスクリプトを変更せずに統合するか、タスクを使用してFortify SASTを起動するFortify SAST Gradleプラグインを使用できます。

- Gradle統合の使用
- Gradle統合のトラブルシューティング
- Gradleプラグインの使用

7.1.1. Gradle統合の使用

`build.gradle` ファイルを変更せずに、Gradleを使用してビルドされたプロジェクトを変換できます。ビルドが実行されると、Fortify SASTでソースファイルがコンパイル時に変換されます。代わりに、Fortify SAST Gradle Pluginを使用して Gradle ビルドスクリプト内から分析を実行できます (「Fortify SAST Gradleプラグインの使用」を参照)。

Gradle統合で特定的にサポートされているプラットフォームおよび言語については、「ビルドツール」を参照してください。プロジェクト内のファイルは、Gradleの統合でサポートされていない言語では変換されません(エラーもレポートされません)。したがって、これらのファイルは分析されず、既存の潜在的な脆弱性は検出されない可能性があります。

Fortify SASTをGradleビルドに統合するには、`sourceanalyzer` 実行可能ファイルがPATH環境変数に含まれていることを確認します。プロジェクトをビルドするすべてのGradleコマンドに対して、システムパスの `sourceanalyzer` 実行可能ファイルを常に使用します。

> **Note**
> Fortify SASTが複数インストールされている場合、Gradleプロジェクトに使用するバージョンは、PATH環境変数内の他のすべてのバージョンのFortify SASTより前に定義されている必要があります。

次のように、Gradleコマンドラインの前に `sourceanalyzer` コマンドを追加します。

```
sourceanalyzer -b <build_id>
```

<sca_options>

gradle [<*gradle_options*>] <*gradle_tasks*>

Gradle統合の例

```
sourceanalyzer -b MyProject gradle clean build sourceanalyzer -b MyProject gradle --info assemble
```

ビルドファイル名が `build.gradle` と異なる場合は、次の例に示すように、ビルドファイル名に `--build-file` オプションを付けます。

```
sourceanalyzer -b MyProject gradle --build-file sample.gradle clean assemble
```

次の例に示すように、Gradle Wrapper (`gradlew`)を使用することもできます。

```
sourceanalyzer -b MyProject gradlew [<gradle_options>]
```

プロジェクトを変換し、変換からファイルを除外する場合:

```
sourceanalyzer -b MyProject -exclude "src\test\**\*" gradlew build
```

アプリケーションでXMLまたはプロパティ環境設定ファイルが使用されている場合は、これらのファイルを個別の `sourceanalyzer` コマンドを使って変換します。プロジェクトファイルで使用したときと同じビルドIDを使用します。次に例を示します。

```
sourceanalyzer -b MyProject <path_to_xml_files> sourceanalyzer -b MyProject <path_to_properties_files>
```

Fortify SASTがgradleまたはgradlewを使ってプロジェクトを変換した後、次の例に示すように分析フェーズを実行して、結果をFPRファイルに保存できます。

```
sourceanalyzer -b MyProject -scan -f MyResults.fpr
```

7.1.2. Gradle統合のトラブルシューティング

Fortify SASTGradle統合を使用したGradleビルドで設定キャッシング(`--configuration-cache` オプション)を使用した場合、ビルドは次のメッセージをレポートします。

```
Configuration cache problems found in this build.
```

次のようなメッセージが表示される場合もあります。

```
FAILURE: Build failed with an exception...
```

このメッセージは、Fortify SAST変換に関しては無視して構いません。プロジェクトが変換されているからです。プロジェクトが変換されていることは、 `-show-files` オプションを使用して確認できます。例:

```
sourceanalyzer -b mybuild -show-files
```

7.1.3. Gradleプラグインの使用

Fortify SASTのインストールには、 `<sast_install_dir>/plugins` GradleにあるGradleプラグインが含まれています。Fortify SAST Gradleプラグインを使用するには、まずJavaまたはKotlinプロジェクト用にプラグインを設定してから、そのプラグインを使用してプロジェクトを分析する必要があります。Gradleプラグインは、分析用に3つのFortify SASTタスク(sca.clean、sca.translate、およびsca.scan)を提供しています。特にFortify SAST Gradleプラグイン用にサポートされているプラットフォームと言語については、「ビルドツール」を参照してください。

Note

Fortify SASTが複数インストールされている場合、Gradleプロジェクトに使用するバージョンは、PATH環境変数内の他のすべてのバージョンのFortify SASTより前に定義されている必要があります。

Fortify SAST Gradleプラグインを設定するには:

1. Gradle設定ファイルを編集して、プラグインへのパスを指定します。
   Groovy DSL (`settings.gradle`):

   ```
   pluginManagement { repositories { gradlePluginPortal() maven { url = uri("file://<sast_plugin_path>") } } }
   ```

   Kotlin DSL (`settings.gradle.kts`):

   ```
   pluginManagement { repositories { maven(url = uri("file://<sast_plugin_path>")) gradlePluginPortal() } }
   ```

2. 以下の例に示すように、ビルドスクリプトにエントリを追加します。
   Groovy DSL (`build.gradle`):

   ```
   id 'com.fortify.sca.plugins.gradlebuild' version '26.4'
   ```

   および

   ```
   SCAPluginExtension { buildId = "MyProject" options = ["-encoding", "utf-8", "-logfile", "MyProject.log", "-debug-verbose"] }
   ```

   または次のエントリの例では、変換からファイルが除外されます。

   ```
   SCAPluginExtension { buildId = "MyProject" options = ["-encoding", "utf-8", "-logfile", "MyProject.log", "-debug-verbose", "-exclude", "src/test/**/*"] }
   ```

   Kotlin DSL (`build.gradle.kts`):

   ```
   plugins { id ("com.fortify.sca.plugins.gradlebuild") version "26.4" ... }
   ```

   および

   ```
   SCAPluginExtension { buildId = "MyProject" options = listOf("-encoding", "utf-8", "-logfile", "MyProject.log", "-debug-verbose") }
   ```

   または次のエントリの例では、変換からファイルが除外されます。

   ```
   SCAPluginExtension { buildId = "MyProject" options = listOf("-encoding", "utf-8", "-logfile", "MyProject.log", "-debug-verbose", "-exclude", "src/test/**/*") }
   ```

3. Gradle設定ファイルとGradleビルドファイルを保存して閉じます。

次のコマンドシーケンスを使用して、JavaまたはKotlinプロジェクトを分析します。

- 既存のJavaまたはKotlinプロジェクトビルドの既存のFortify SAST一時ファイルをすべて削除するには、次のコマンドを実行します。

  ```
  gradlew sca.clean
  ```

- 設定済みのJavaまたはKotlinプロジェクトの変換フェーズを実行するには、次のコマンドを実行します。

  ```
  gradlew sca.translate
  ```

- 設定済みのJavaまたはKotlinプロジェクトを分析するには、次のコマンドを実行します。

  ```
  gradlew sca.scan
  ```

  このタスクは、Fortify SASTによってプロジェクトがFortify SAST Gradleプラグインを使用してすでに変換されている場合に、正常に実行されます。

サブプロジェクトを持つJavaまたはKotlinプロジェクトの操作

JavaまたはKotlinマルチプロジェクトビルド(サブプロジェクトを含む)がある場合は、Fortify SAST Gradleプラグインを `allprojects` ブロックを使用して設定する必要があります。以下に例を示します。

Groovy DSL (`build.gradle`)

```
allprojects { apply plugin: "com.fortify.sca.plugins.gradlebuild" SCAPluginExtension { buildId = "MyProject" options = ["-encoding", "utf-8", "-logfile", "MyProject.log", "-debug-verbose"] ... } }
```

Kotlin DSL (`build.gradle.kts`):

```
allprojects { apply(plugin = "com.fortify.sca.plugins.gradlebuild") SCAPluginExtension { buildId = "MyProject" options = listOf("-encoding", "utf-8", "-logfile", "MyProject.log", "-debug-verbose") ... } }
```

7.2. Mavenとの統合

Fortify SASTには、Mavenプロジェクトのビルドに次の機能を追加する方法を提供するMavenプラグインが含まれています。

- Fortify SASTで消去、変換、スキャンする
- 変換されたプロジェクトのモバイルビルドセッション(MBS)をFortify SASTからエクスポートする
- 変換されたコードをFortify ScanCentral SASTに送信する
- Fortify Software Security Centerに結果をアップロードする

プラグインを直接使用することも、プラグインの機能をビルドプロセスに統合することもできます。

- Fortify Mavenプラグインのインストールと更新
- Fortify Mavenプラグインのインストールのテスト
- Fortify Mavenプラグインの使用

7.2.1. Fortify Mavenプラグインのインストールと更新

Fortify Mavenプラグインは、 `<sast_install_dir>/plugins/maven` に配置されています。このディレクトリには、バイナリバージョンとソースバージョンのプラグインがzipアーカイブとtarballアーカイブの両方で含まれています。プラグインをインストールするには、使用するバージョン(バイナリまたはソース)を抽出し、付属の `README.TXT` ファイルの指示に従います。アーカイブを展開したディレクトリでインストールを実行します。

Mavenのサポートされているバージョンについては、「ビルドツール」を参照してください。

以前のバージョンのFortify Mavenプラグインがインストールされている場合は、最新バージョンをインストールします。

Fortify Mavenプラグインのアンインストール

Fortify Mavenプラグインをアンインストールするには、 `<maven_local_repo>/repository/com/fortify/ps/maven/plugin` ディレクトリからすべてのファイルを手動で削除します。

7.2.2. Fortify Mavenプラグインのインストールのテスト

Fortify Mavenプラグインをインストールしたら、付属のサンプルファイルのいずれかを使用して正しくインストールされていることを確認します。

Eightballサンプルファイルを使用してFortify Mavenプラグインをテストするには、次の手順に従います。

1. `sourceanalyzer` 実行可能ファイルを含むディレクトリをパス環境変数に追加します。例
   :

   ```
   export set PATH=$PATH:/ <sast_install_dir> /bin
   ```

   または

   ```
   set PATH=%PATH%; <sast_install_dir> /bin
   ```

2. 「 `sourceanalyzer -version` 」と入力してパスの設定をテストします。
   パスの設定が正しい場合は、Fortify SASTにバージョン情報が表示されます。
3. サンプルのEightballディレクトリ(`<root_dir>/samples/EightBall`)に移動します。
4. 次のコマンドを入力します。

   ```
   mvn  com.fortify.sca.plugins.maven:sca-maven-plugin:<ver>:clean
   ```

   ここで、 `<ver>` は使用しているFortify Mavenプラグインのバージョンです。バージョンが指定されていない場合 は、ローカルリポジトリにインストールされている最新バージョンのFortify Mavenプラグインが Mavenで使用されます。

   > **Note**
   > Fortify Mavenプラグインのバージョンを表示するには、テキストエディタで `pom.xml` に抽出した `<root_dir>` ファイルを開きます。Fortify Mavenプラグインのバージョンは、 `<version>` 要素で指定されます。

5. ステップ4のコマンドが正常に完了した場合は、Fortify Mavenプラグインが正しくインストールされています。次のメッセージが表示された場合は、Fortify Mavenプラグインが正しくインストールされていません。

   ```
   [ERROR] Error resolving version for plugin 'com.fortify.sca.plugins.maven:sca-maven-plugin' from the repositories
   ```

   Mavenのローカルリポジトリをチェックし、Fortify Mavenプラグインの再インストールを試みます。

7.2.3. Fortify Mavenプラグインの使用

Mavenプロジェクトでは、次の2つの方法で分析を実行します。

- Fortify SASTビルド統合時
  この方法では、プロジェクトをビルドするために使用されるMavenコマンドの前に `sourceanalyzer` コマンドとFortify SASTオプションを追加します。Fortify SASTのビルド統合の一環としてファイルを分析するには、次の手順に従います。
  1. 以前のビルドを消去します。

     ```
     sourceanalyzer -b MyProject -clean
     ```

  2. コードを変換します。

     ```
     sourceanalyzer -b MyProject [
     ```

     <*sca_options*>] [<*mvn_command_with_options*>]

例:

```
sourceanalyzer -b MyProject mvn package
```

```
sourceanalyzer -b MyProject -exclude "**/Test/*.java" mvn clean install
```

使用可能なFortify SASTオプションについては、「コマンドラインインタフェース」を参照してください。

3. 次の例に示すように、スキャンを実行して結果をFPRファイルに保存します。

```
sourceanalyzer -b MyProject [<sca_scan_options>] -scan -f MyResults.fpr
```

- Mavenプラグインとして
  この方法では、`mvn`コマンドを使用して分析タスクを目標として実行します。たとえば、次のコマンドを使用してソースコードを変換します。

```
mvn com.fortify.sca.plugins.maven:sca-maven-plugin:26.4:translate
```

たとえば、次のコマンドを使用してソースコードを変換し、テストファイルを除外します。

```
mvn -Dfortify.sca.exclude="**/Test/*.java" com.fortify.sca.plugins.maven:sca-maven-plugin:26.4:translate
```

この方法でコードを分析するには、Fortify Mavenプラグインに付属のドキュメントを参照してください。次の表では、Fortify Mavenプラグインをインストールした後にドキュメントが置かれる場所について説明します。

パッケージタイプ	ドキュメントの場所
バイナリ	`<root_dir>/docs/index.html`
ソース	`<root_dir>/sca-maven-plugin/target/site/index.html`

7.3. Bazelとの統合

Bazelのビルドと統合するために、Fortify SASTはソースファイルをコンパイル時に変換します。したがって、Bazelのビルドの前提条件は、Bazelのビルドが正常に実行されることです。サポートされているBazelのバージョンについては、「ビルドツール」を参照してください。

Bazelと統合するには、Bazelのワークスペースディレクトリに移動し、構築するBazelのターゲットでs sourceanalyzerを実行します。次のように、変換のための他のsourceanalyzerオプションを指定できます。

```
sourceanalyzer -b <build_id> <sca_options> bazel build <target>
```

プロジェクトを変換し、変換からファイルを除外する場合:

```
sourceanalyzer -b MyProjectC -exclude C:¥test¥MY-JAVA-APP¥src¥proj¥content.py bazel build //projc:my-python-prj
```

7.3.1. Java Bazelの統合例

特定のターゲットのプロジェクトを変換する場合:

```
sourceanalyzer -b MyProjectA bazel build //proja:my-prj
```

パッケージ `proja/abc` 内のターゲット `abc` を変換する場合:

```
sourceanalyzer -b MyProjectA bazel build //proja/abc
```

または

```
sourceanalyzer -b MyProjectA bazel build //proja/abc:abc
```

パッケージ `proja/abc` 内のすべてのターゲットを変換する場合:

```
sourceanalyzer -b MyProjectA bazel build //proja/abc:all
```

`projb/` ディレクトリ内のすべてのターゲットを変換する場合:

```
sourceanalyzer -b MyProjectB bazel build //projb/...
```

変換に特定のJDKバージョンを指定する場合:

```
sourceanalyzer -b MyProjectC -jdk 17 bazel build //projc:my-java-prj
```

プロジェクトを変換し、変換からファイルを除外する場合:

```
sourceanalyzer -b MyProjectC -exclude C:¥test¥MY-JAVA-APP¥src¥main¥java¥com¥example¥HelpContent.java
bazel build //projc:my-java-prj
```

Fortify SASTとBazelの統合では、複数のターゲットおよび関連アクション(ターゲットの除外など)はサポートされていません。

7.4. Antとの統合

Antビルドファイルを使用するプロジェクト用に、Javaソースファイルを変換できます。この統合は、Antの `build.xml` ファイルを変更せずにコマンドラインに適用できます。ビルドが実行されると、Fortify SASTで `javac` タスクの呼び出しがすべて傍受され、Javaソースファイルがコンパイル時に変換されます。プロパティはすべて、ANT_OPTS環境変数に追加して、Antに渡すようにします。sourceanalyzerコマンドには含めないでください。

> **Note**
>
> アプリケーションの一部であるJSPファイル、環境設定ファイル、またはJava以外のソースファイルを個別のステップで変換する必要があります。

Antの統合を使用するには、 `sourceanalyzer` 実行可能ファイルがPATH環境変数に入っていることを確認します。

次のように、Antコマンドラインの前に `sourceanalyzer` コマンドを追加します。

```
sourceanalyzer -b <build_id> [ <sca_options> ] ant [<ant_options>]
```

たとえば、Javaプロジェクトを変換し、変換からファイルを除外するには、次のようにします。

```
sourceanalyzer -b MyProjectA -logfile MyProjectA.log -exclude src/module-info.java ant
```

7.5. JavaおよびKotlinの手動変換構文

JavaまたはKotlinコードを手動で変換するには、すべてのソースファイルをコマンドラインに含め、.jarファイル、.classファイル、またはソースファイルを介してすべての依存関係を提供します。依存関係を提供しない場合、スキャン結果が最

適でない可能性があります。

KotlinからJavaへの相互運用性では、 –sourcepath オプションで提供されるKotlinファイルをサポートしません。 –sourcepath オプションの詳細については、「Javaコマンドラインオプション」を参照してください。

JavaまたはKotlinコードを変換するための基本的なコマンドライン構文を次の例に示します。

```
sourceanalyzer -b <build_id> -cp <classpath> [<translation_options>] <files> | <file_specifiers>
```

ここで:

- <translation_options> は、コンパイラに渡されるオプションです。
- -cp <classpath> ではJavaおよびKotlinシンボルの解決に使用するクラスパスを指定します。
  プロジェクトをビルドするために通常使用されるJAR依存関係を含めます。複数のパスはセミコロン(Windows)またはコロン(Windows以外)で区切ります。
  javacと同様に、Fortify SASTではクラスをクラスパスに出現する順序でロードします。リスト内に同じ名前のクラスが複数ある場合、Fortify SASTでは最初にロードされたクラスを使用します。次の例では、 A.jar と B.jar の両方に MyData.class という名前のクラスが含まれる場合、Fortify SASTでは MyData.class からの を使用します。

  ```
  sourceanalyzer -cp A.jar:B.jar myfile.java
  ```

  -cp オプションで重複するクラスを使用しないように強く推奨します。
  Fortify SASTではJARファイルを次の順序でロードします。
  1. -cp オプションから
  2. jre/lib. から
  3. <sast_install_dir> /Core/default_jars. から

  これにより、 -cp オプションで指定したJARに同様の名前のクラスを含めることで、ライブラリクラスを上書きできます。

使用可能なすべてのJava固有のコマンドラインオプションの詳細については、「Java/J2EEコマンドラインオプション」を参照してください。

Javaコードを使用すると、Fortify SASTはさらにコンパイラをエミュレートして、カスタムビルドスクリプトに容易に統合できます。

Fortify SASTでコンパイラをエミュレートするには、次のコマンドを入力します。

```
sourceanalyzer -b <build_id> javac [<translation_options>]
```

7.5.1. Java、Kotlin、およびJSPのコマンドラインオプション

次の表では、Javaコマンドラインオプション(Java SEおよびJakarta EE用)について説明します。

Java、Kotlin、またはJakarta　EEのオプション	説明(Description)
`-appserver weblogic` | `websphere`	JSPファイルを処理するアプリケーションサーバを指定します。 **同等のプロパティ名:** `com.fortify.sca.AppServer`
`-appserver-home <dir>`	アプリケーションサーバのホームを指定します。 • Oracle®istered trademark; WebLogic®istered trademark;の場合、これは `server/lib` ディレクトリを含むディレクトリへのパスです。 • IBM®istered trademark; WebSphere®istered trademark;の場合、これは `JspBatchCompiler` スクリプトを含むディレクトリへのパスです。 **同等のプロパティ名:** `com.fortify.sca.AppServerHome`
`-appserver-version <version>`	アプリケーションサーバのバージョンを指定します。 **同等のプロパティ名:** `com.fortify.sca.AppServerVersion`

`-cp <paths>` |
`-classpath <paths>`
	JavaまたはKotlin依存関係の解決に使用するクラスパスを指定します。形式はjavacに似ており、ディレクトリとファイルのセミコロン区切り(Windows)またはコロン区切り(Linux/macOS)リストで構成されています。
	`-classpath` または `-cp` は `-classpath` がjavacおよびjavaと連携するのと同様に動作します。
	• `-cp "<dir>"` では指定されたディレクトリで `.class` ファイルを検索します。
	• `-cp "<dir>/*"` | `-cp "<dir>/*.jar"` では指定されたディレクトリで `.jar` ファイルを検索します。
	Caution
	意図しないシェル展開を回避するには、classpathの値を引用符で囲みます。
	次の例に示すように、Fortify SASTファイル指定子を使用することもできます。
	`-cp "build/classes:lib/*.jar"`
	同等のプロパティ名:
	`com.fortify.sca.JavaClasspath`

`-extdirs <dirs>`	javac `extdirs` オプションと同様に、ディレクトリのセミコロン区切りまたはコロン区切りリストを使用できます。これらのディレクトリにあるJARファイルは、クラスパスに暗黙的に含まれます。 **同等のプロパティ名:** `com.fortify.sca.JavaExtdirs`
`-java-build-dir <dirs>`	コンパイル済みJavaソースを含む1つ以上のディレクトリを指定します。
`-source <version>` | `-jdk <version>`	JavaまたはKotlinコードを記述するJava™ Development Kit (JDK)バージョンを示します。サポートされているバージョンについては、「サポートされる言語」を参照してください。デフォルトはバージョン11です。 **同等のプロパティ名:** `com.fortify.sca.JdkVersion`
`-custom-jdk-dir`	JDKを含むディレクトリを指定します。Fortify SASTインストール(*<sast_install_dir>* `/Core/bootcp/`)に含まれていないバージョンを指定するには、このオプションを使用します。サポートされているバージョンについては、「サポートされる言語」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.CustomJdkDir`
`-show-unresolved-symbols`	変換されたJavaソースファイルで参照されている未解決のタイプ、フィールド、および関数が、変換の最後に表示されます。リストされるのは、レシーバータイプが解決済みJavaタイプであるフィールドおよび関数参照のみです。各クラス、フィールド、および関数が、コード内で最初に変換された出現箇所のソース情報とともに表示されます。この情報はログファイルにも書き込まれます。 **同等のプロパティ名:** `com.fortify.sca.ShowUnresolvedSymbols`
`-sourcepath <dirs>`	スキャンに含まれていないが名前解決に使用されるソースコードを含むディレクトリのリストをセミコロン区切りまたはコロン区切りで指定します。ソースパスはクラスパスに似ていますが、解決にはクラスファイルではなくソースファイルが使用されます。ターゲットファイルリストによって参照されるソースファイルのみが変換されます。 **同等のプロパティ名:** `com.fortify.sca.JavaSourcepath`

`-jvm-default <mode>`	本体がKotlinインターフェイスに入っているメソッドの `DefaultImpls` クラスの生成を指定します。*<mode>*の有効な値は: • `disable` —本体を持つメソッドが含まれている各インターフェイスに対して、 `DefaultImpls` クラスを生成するように指定します。 • `all` —インターフェイスに `DefaultImpls` の注釈が付く場合に、 `@JvmDefaultWithCompatibility` クラスを生成するように指定します。 • `all-compatibility` —インターフェイスに `DefaultImpls` の注釈が付かない限り、 `@JvmDefaultWithoutCompatibility` クラスを生成するように指定します。 **同等のプロパティ名:** `com.fortify.sca.KotlinJvmDefault`

JavaおよびKotlinのプロパティ

7.5.2. Javaのコマンドライン例

クラスパスとして `MyServlet.java` が指定された1つのファイル `javaee.jar` を変換するには、次のコマンドを入力します。

```
sourceanalyzer -b MyServlet -cp lib/javaee.jar MyServlet.java
```

`` ディレクトリ内のすべての `` ファイルをクラスパスとして使用して `` ディレクトリ内のすべてのJARファイルを変換するには、次のコマンドを入力します。

```
sourceanalyzer -b MyProject -cp "lib/*.jar" "src/**/*.java"
```

javacコンパイラを使用して `MyCode.java` ファイルを変換およびコンパイルするには、次のコマンドを入力します。

```
sourceanalyzer -b MyProject javac -classpath libs.jar MyCode.java
```

7.5.3. Kotlinコマンドラインの例

クラスパスとして `MyKotlin.kt` が指定された1つのファイル `A.jar` を変換するには、次のコマンドを入力します。

```
sourceanalyzer -b MyProject -cp lib/A.jar MyKotlin.kt
```

`` ディレクトリ内のすべての `` ファイルをクラスパスとして使用して `` ディレクトリ内のすべてのJARファイルを変換するには、次のコマンドを入力します。

```
sourceanalyzer -b MyProject -cp "lib/**/*.jar" "src/**/*.kt"
```

gradlewを使用してgradleプロジェクトを変換するには、次のコマンドを入力します。

```
sourceanalyzer -b MyProject gradlew clean assemble
```

`src` ディレクトリおよびサブディレクトリ内の `src/java` およびすべてのJARファイルのJava依存関係をクラスパスとして使用して `lib` ディレクトリ内のすべてのファイルを変換するには、次のコマンドを入力します。

```
sourceanalyzer -b MyProject -cp "lib/**/*.jar" -sourcepath "src/java" "src"
```

7.6. Kotlinスクリプトの分析

Fortify SASTでは、試験的なスクリプトのカスタマイズを除くKotlinスクリプトの変換をサポートしています。スクリプトのカスタマイズには、外部プロパティの追加、静的または動的な依存関係の提供などがあります。スクリプト定義(テンプレート)はカスタムスクリプトの作成に使用され、テンプレートは *.kts 拡張子に基づいてスクリプトに適用されます。 Fortify SASTでは *.kts ファイルを変換しますが、これらのテンプレートは適用されません。

7.7. KotlinとJavaの変換相互運用性

プロジェクトにJavaコードを参照するKotlinコードが含まれている場合、別のKotlinファイルを参照するKotlinファイルの場合と同じ方法で、Javaファイルを変換ツールに渡すことができます。変換されたプロジェクトソースの一部として、または –sourcepath パラメータとして渡すことができます。

プロジェクトにKotlinコードを参照するJavaコードが含まれている場合、JavaコードとKotlinコードが同じFortify SASTインスタンスに変換され、Kotlin要素へのJava参照が正しく解決されるようにしてください。KotlinからJavaへの相互運用性では、 –sourcepath オプションで提供されるKotlinファイルをサポートしません。 –sourcepath オプションの詳細については、「Java、Kotlin、およびJSPコマンドラインオプション」を参照してください。

7.8. Javaの警告の処理

変換中に生成されたすべての警告を表示するには、スキャンフェーズを開始する前に次のコマンドを入力します。

```
sourceanalyzer -b <build_id> -show-build-warnings
```

Java変換の警告

Javaコード変換に次の警告が表示される場合があります。

警告	解決策
`Unable to resolve type... Unable to resolve function... Unable to resolve field... Unable to locate import... Unable to resolve symbol...`	これらの警告は通常、リソースが不足している場合に発生します。たとえば、アプリケーションのビルドに必要な一部の .jar および .class ファイルが指定されていない可能性があります。 これらの警告を解決するには、アプリケーションが使用する必要なファイルをすべて含める必要があります。
`Multiple definitions found for class...`	この警告は通常、Javaファイル内でクラスが重複している場合に発生します。 これらの警告を解決するには、警告に表示されているソースファイルは同一のファイルが重複して変換対象のソースファイルに複数回含められているものではないことを(たとえば、同じプロジェクトの2つのバージョンが含まれていることを)確認します。重複が存在する場合は、変換するファイルからその1つを削除します。そうすると、Fortify SASTで使用するクラスのバージョンを決定できるようになります。 この警告は、クラスが欠落している可能性も示しています。これを解決するには、必要なすべてのJARファイルをクラスパスに追加してください。

7.9. Jakarta EE (Java EE)アプリケーションの分析

Jakarta EEアプリケーションを変換するには、Fortify SASTでJavaソースファイルおよびJakarta EEコンポーネント(JSPファイル、展開デスクリプタ、および環境設定ファイルなど)を処理します。Jakarta EEアプリケーション内のすべての関連ファイルを1ステップで処理することができますが、プロジェクトでは、ビルドプロセスに統合したり、組織内のさまざまな利害関係者のニーズを満たしたりするために、手順をコンポーネントに分割する必要が生じることがあります。

- Javaファイルの変換
- JSPプロジェクト、環境設定ファイル、および展開ディスクリプタの変換
- Jakarta EE (Java EE)変換の警告

7.9.1. Javaファイルの変換

Jakarta　EEアプリケーションを変換するには、Javaファイルの変換に使用したものと同じ手順を使用します。たとえば、「Javaのコマンドライン例」を参照してください。

7.9.2. JSPプロジェクト、環境設定ファイル、および展開ディスクリプタの変換

Jakarta EE (Java EE)アプリケーションのJavaファイルを変換するほかに、JSPファイル、環境設定ファイル、および展開デスクリプタの変換が必要になることがあります。JSPファイルは、Webアプリケーションアーカイブ(WAR)の一部である必要があります。ソースディレクトリがすでにWARファイル形式で構成されている場合は、ソースディレクトリからJSPファイルを直接変換できます。そうでない場合は、アプリケーションを展開し、展開ディレクトリからJSPファイルを変換する必要があります。

例:

```
sourceanalyzer -b MyJavaApp "/**/*.jsp" "/**/*.xml"
```

ここで、`/**/*.jsp`はJSPプロジェクトファイルの場所を参照し、`/**/*.xml`は環境設定ファイルおよび展開ディスクリプタファイルの場所を参照します。

7.9.3. Jakarta EE (Java EE)変換の警告

Jakarta　EEアプリケーションの変換で次の警告が表示される場合があります。

```
Could not locate the root (WEB-INF) of the web application. Please build your web application and try
again. Failed to parse the following jsp files: <list_of_jsp_files>
```

この警告は、Webアプリケーションが標準のWARディレクトリ形式で展開されていないか、必要なライブラリの完全なセットが含まれていないことを示します。この警告を解決するには、Webアプリケーションが開かれたWARディレクトリ形式であり、アプリケーションに必要なすべての`WEB-INF/lib`ファイルおよび`WEB-INF/classes`ファイルが正しい`.jar`および`.class`ディレクトリに格納されていることを確認してください。また、すべてのタグのすべての`TLD`ファイル、およびそれらのタグの実装に対応するJARファイルが存在することも確認してください。

7.10. Javaバイトコードの分析

JavaバイトコードとJSP/Javaコードを同じ`sourceanalyzer`呼び出しで変換しないことをお勧めします。同じビルドIDを持つ複数の`sourceanalyzer`呼び出しを使用して、バイトコードとJSP/Javaコードの両方を含むプロジェクトを変換します。

バイトコードを変換するには:

1. `fortify-sca.properties`ファイルに次のプロパティを追加します(または、`-D`オプションを使用してコマンドラインにこれらのプロパティを含めます)。
   `com.fortify.sca.fileextensions.class=BYTECODE`
   `com.fortify.sca.fileextensions.jar=ARCHIVE`
   これは、Fortify SASTで`.class`および`.jar`ファイルを処理する方法を指定します。
2. 次のいずれかを実行します。
   - Fortify SASTでバイトコードクラスを通常のJavaファイルに逆コンパイルして変換に含めることを要求します。
     `fortify-sca.properties`ファイルに次のプロパティを追加します。

```
com.fortify.sca.DecompileBytecode=true
```

または、 `-D` オプションを使用して、変換フェーズのコマンドラインにこのプロパティを含めます。

```
sourceanalyzer -b MyProject -Dcom.fortify.sca.DecompileBytecode=true -cp "lib/*.jar"
"src/**/*.class"
```

- Fortify SASTで逆コンパイルせずにバイトコードを変換することを要求します。
  最善の結果を得るため、完全なデバッグ情報(`javac -g`)を使用してバイトコードをコンパイルすることを推奨しています。
  変換するJavaバイトコードファイルを指定することで、変換フェーズにバイトコードを含めます。最善のパフォーマンスを得るため、スキャンが必要な `.jar` または `.class` ファイルだけを指定します。次の例では、 `.class` ファイルが変換されています。

  ```
  sourceanalyzer -b MyProject -cp "lib/*.jar" "src/**/*.class"
  ```

7.11. Java、Kotlin、およびJSP変換および分析に関する問題のトラブルシューティング

次のセクションでは、Java、Kotlin、およびJSP分析に関するトラブルシューティング情報について説明します。

多くのJavaソースファイルが変換されていない

スキャン結果から一部のファイルが見つからない場合にJavaプロジェクトを変換する場合、次のプロパティを fo sca.properties ファイルに追加することで、マルチファイルJava解析を無効にできます。

```
com.fortify.sca.JavaParseMultipleFiles=false
```

一部のJSPを変換できない

Fortify SASTでは、組み込みコンパイラまたは特定のアプリケーションサーバJSPコンパイラを使用して、分析のためにJSPファイルをJavaファイルに変換します。Fortify SASTでJSPファイルをJavaファイルに変換する際にJSPパーサで問題が発生すると、次のようなメッセージが表示されます。

```
Failed to translate the following jsps into analysis model. Please see the log file for any errors from
the jsp parser and the user manual for hints on fixing those <list_of_jsp_files>
```

これは通常、次の1つ以上の理由で発生します。

- Webアプリケーションが適切な展開可能WARディレクトリ形式でレイアウトされていない
- アプリケーションに必要なJARファイルまたはクラスの一部が見つからない
- アプリケーションのタグライブラリまたはそれらの定義(TLD)の一部が見つからない

問題の詳細を取得するには、次の手順を実行します。

1. エディタでFortify SASTログファイルを開きます。
2. 次の文字列を検索します。
   - `Jsp parser stdout:`
   - `Jsp parser stderr:`

JSPパーサではこれらのエラーを生成します。エラーを解決してFortify SASTを再実行します。

Jakarta EEアプリケーションの分析方法の詳細については、「Jakarta EE (Java EE)アプリケーションの変換」を参照してください。

JSP関連カテゴリで問題の数が増加した

分析結果に含まれるクロスサイトスクリプティングなどのJSP関連カテゴリの脆弱性数が以前のFortify SASTバージョンと比較して大幅に増加している場合は、分析フェーズで `-legacy-jsp-dataflow` オプションを指定できます(`-scan` オプションも指定します)。このオプションを使用すると、JSP関連のデータフローに対する追加のフィルタリングが有効になり、検出される偽陽性が減少します。

`fortify-sca.properties` ファイルで指定できるこのオプションと同等のプロパティは `com.fortify.sca.jsp.LegacyDataflow` です。

8. Androidプロジェクトの分析

このセクションでは、Androidアプリケーションの Javaソースコードを変換する方法について説明します。Fortify SASTを使用して、次のいずれからでもGradleでコードをスキャンできます。

- オペレーティングシステムのコマンドライン
- Android Studioで実行中のターミナルウィンドウ

Gradleの使い方はどちらの方法でも同じです。



Note

Fortify Analysis Plugin for IntelliJ IDEA and Android Studioを使用すると、Android StudioからAndroidコードを直接スキャンすることもできます。詳細については、*OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio ユーザガイド*を参照してください。

- Androidプロジェクト変換の前提条件
- Androidコード分析のコマンドライン構文
- Androidレイアウトファイルで検出されたフィルタリングの問題

8.1. Androidプロジェクト変換の前提条件

Androidプロジェクトを変換するための前提条件は次のとおりです。

- Android　Studioと関連するAndroid　SDKは、スキャンを実行するシステムにインストールされます。
- Androidプロジェクトでは、ビルドにGradleを使用します。
  Gradleを使用しない古いプロジェクトがある場合は、関連付けられているAndroid StudioプロジェクトにGradleサポートを追加する必要があります。
  Androidプロジェクトの作成に使用するバージョンのAndroid Studioに付属するGradleと同じバージョンを使用します。
- アプリケーションのプロジェクトのAndroidコードをビルドするために必要なすべての依存関係が用意されていることを確認します。
- Android Studio内に表示されないコマンドウィンドウからAndroidコードを変換するには、Gradle Wrapper (`gradlew`)がシステムパスで定義されている必要があります。

8.2. Androidコード分析のコマンドライン構文

Androidプロジェクトをスキャンするには、gradlewを使用します。これは、Gradle Wrapperを使用する点以外はGradleを使用することに似ています。Gradle Wrapperを使用してAndroidプロジェクトを変換する方法については、Gradleの統合を参照してください。

8.3. Androidレイアウトファイルで検出されたフィルタリングの問題

Androidプロジェクトにレイアウトファイル(ユーザインタフェースの設計に使用)が含まれている場合、プロジェクトファイルにはAndroid Studioによって自動的に生成される `R.java` ソースファイルが含まれている可能性があります。プロジェクトをスキャンすると、Fortify SASTでこれらのレイアウトファイルに関連する問題を検出できます。

レイアウトファイルでレポートされた問題を標準的な監査に含めて、これらの問題が誤検出かどうかを慎重に判断できるようにすることをお勧めします。関心がないレイアウトファイルで問題を特定した後は、「結果の最適化」の説明に従って、問題をフィルタで除外できます。インスタンスIDに基づいて問題をフィルタできます。

9. Groovyコードの分析

このセクションでは、Groovyプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Groovy分析の前提条件

- Groovyの変換構文

9.1. Groovy分析の前提条件

現在、GroovyコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Groovyコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

9.2. Groovyの変換構文

AIを活用したSASTを使用して分析対象にGroovyコードを含めるには、分析対象のすべてのソースファイルを含めます。

Groovyコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.groovy"
```

Important

Groovyソースファイルでサポートされているファイル拡張子は `.groovy` 、 `.gvy` 、 `.gy` 、 `gsh` です。

10. Scalaコードの分析

Scalaコードの変換に必要なものは次のとおりです。

- Akkaコンパイラプラグイン
  このプラグインは、Maven Central Repositoryからダウンロードできます。
- Akka(以前のLightbend)ライセンスファイル
  このライセンスファイルは、Fortify SASTのインストールに含まれ、 `<sast_install_dir>/plugins/lightbend` ディレクトリにあります。

Caution

新しいバージョンにアップグレードすると、既存のAkkaライセンスファイルが失効したり、無効になったりする可能性があります。

アップグレード後にこのような問題が発生した場合:

1. 新しいバージョンのライセンスをリクエストするには、カスタマーサポートにお問い合わせください。
2. 更新されたライセンスを受け取ったら、古いライセンスファイルを削除し、サポートから提供された新しいライセンスをインストールしてください。

ライセンスの設定方法およびScalaコードの変換方法については、Akkaドキュメント『Fortify SCA for Scala』を参照してください。

Important

プロジェクトに、Scala以外のソースコードが含まれている場合は、分析フェーズを実行する前にScala Fortifyコンパイラプラグインを使用してScalaコードを変換してから、同じビルドIDでsourceanalyzerを使用してその他のソースコードを変換する必要があります。

11. Visual Studioプロジェクトの分析

Fortify SASTでは、次のタイプのVisual Studioプロジェクトの変換をサポートするためのビルド統合を提供しています。

- C/C++プロジェクト
- .NET Frameworkと.NET Coreをターゲットとする C#プロジェクト
- ASP.NETフレームワークとASP.NET Coreをターゲットとする ASP.NETアプリケーション
- Android™およびiOSプラットフォームをターゲットとするXamarinアプリケーション

関連するプログラミング言語およびフレームワークと、Visual StudioおよびMSBuildのサポートされているバージョンの一覧については、「サポートされる言語」および「サポートされるビルドツール」を参照してください。

- Visual Studioプロジェクト変換の前提条件
- Visual Studioプロジェクトのコマンドライン構文
- Visual Studioプロジェクトの変換に関する特殊なケースの処理
- Visual Studioプロジェクトを変換する別の方法

11.1. Visual Studioプロジェクト変換の前提条件

変換する各プロジェクトを完成させ、エラーなしでビルドできる環境で変換を実行することをお勧めします。ソフトウェア環境要件のリストについては、「ソフトウェア要件」を参照してください。完全なプロジェクトには、次の要素が含まれます。

- 必要なすべてのソースコードファイル(C/C++、C#、またはVB.NET)。
- 必要なすべての参照ライブラリ。
  これには、関連するフレームワークの参照ライブラリ、NuGetパッケージ、およびサードパーティ製ライブラリが含まれます。
- C/C++プロジェクトの場合は、Visual StudioまたはMSBuildインストールに属していない必要なすべてのヘッダファイルを含めます。
- ASP.NETおよびASP.NET Coreプロジェクトの場合は、必要なすべてのASP.NETページファイルを含めます。
  サポートされているASP.NETページのタイプは、ASAX、ASCX、ASHX、ASMX、ASPX、AXML、BAML、CSHTML、Master、RAZOR、VBHTML、およびXAMLです。

11.2. Visual Studioプロジェクトのコマンドライン構文

Visual Studioソリューションまたはプロジェクトを変換する基本的な構文では、Fortify SAST変換コマンドの一部として、プロジェクトの対応するビルドオプションを指定します。そのようにすると、ソリューションおよびプロジェクトファイルを分析し、適切な変換ステップを自動的に実行するビルド統合が開始されます。Visual Studioソリューション(`.sln` または `.slnx`)に含まれるすべてのプロジェクトがFortify SASTによって変換されます。セミコロンで区切ったプロジェクトのリストを指定して、1つ以上の特定のプロジェクトを変換することもできます。

> **Important**
>
> 適切なプロジェクト依存関係とリソースのすべてをビルド統合が間違いなく取得できるようにするため、Fortify SASTコマンドはビルドの環境設定にアクセスできるコマンドプロンプトから実行する必要があります。変換に最適な環境を確保するために、Visual Studioの開発者コマンドプロンプトからこのコマンドを実行するよう強く推奨します。

次の例では、Visual Studioソリューション `Sample.sln` に含まれるすべてのプロジェクトがFortify SASTによって変換されます。

デフォルトでは、テストプロジェクトは変換から除外されます。NUnit、xunit、またはMSTestを参照するソリューション内のプロジェクトは、テストプロジェクトと見なされます。テストプロジェクトを変換に含めるには、MSBuildオプション `/p:ScaForceTranslateTestProjects=True` を `sourceanalyzer` コマンドに追加します。

- WindowsまたはLinux上の.NET 6.0以降のソリューションの場合は、次のコマンドを使用してソリューションを変換します。
  1. 必要に応じて次のコマンドを実行し、以前のプロジェクトビルドから中間ファイルを削除します。

```
dotnet clean Sample.sln
```

2. 必要に応じて次のコマンドを実行し、必要なすべての参照ライブラリがダウンロードされ、プロジェクトにインストールされるようにします。次のコマンドをプロジェクトの最上位フォルダから実行します。

```
dotnet restore Sample.sln
```

3. プロジェクトのビルドの実装方法に応じて、次のFortify SASTコマンドのいずれかを実行します。このコマンドには、追加のビルドパラメータを含めることができます。

```
sourceanalyzer -b MyProject dotnet msbuild Sample.sln
```

または

```
sourceanalyzer -b MyProject dotnet build Sample.sln
```

- Windows上のC、C++、および.NET Frameworkソリューション(4.8.x以前)の場合は、次のコマンドを使用してソリューションを変換します。

```
sourceanalyzer -b MyProject msbuild /t:rebuild [<msbuild_options>] Sample.sln
```



Note

Visual Studioの開発者コマンドプロンプトではなくWindowsのコマンドプロンプトからFortify SASTを実行する場合は、環境を設定し、プロジェクトのビルドに必要なMSBuild実行可能ファイルへのパスをPATH環境変数に含める必要があります。

変換が完了したら、次の例に示すように、分析フェーズを実行して結果をFPRファイルに保存します。

```
sourceanalyzer -b MyProject -scan -f MyResults.fpr
```

11.3. Visual Studioプロジェクトの変換に関する特殊なケースの処理

- スクリプトからの変換の実行
- プレーンな.NETおよびASP.NETプロジェクトの変換
- C/C++およびXamarinプロジェクトの変換
- 空白を含む設定を持つプロジェクトの変換
- Visual Studioソリューションの単一プロジェクトの変換
- 複数の実行可能ファイルをビルドするプロジェクトの分析

11.3.1. スクリプトからの変換の実行

スクリプトなどの非対話型モードで変換を実行するには、Fortify SAST変換を実行する前に次のコマンドを実行して、変換に最適な環境を確立してください。

```
cmd.exe /k <vs_inst all_dir>/Common7/Tools/VSDevCmd.bat
```

ここで、*<vs_install_dir>*はVisual Studioをインストールしたディレクトリです。

11.3.2. プレーンな.NETおよびASP.NETプロジェクトの変換

プレーンな.NETおよびASP.NETプロジェクトは、Windowsコマンドプロンプトおよび Visual Studio環境から変換できます。Windowsコマンドプロンプトから変換する場合は、プロジェクトのビルドに必要なMSBuild実行可能ファイルへのパスがPATH環境変数に含まれていることを確認してください。

11.3.3. C/C++およびXamarinプロジェクトの変換

C/C++およびXamarinプロジェクトは、Visual Studioの開発者コマンドプロンプトまたはFortify Extension for Visual Studioから変換する必要があります。

> **Note**
>
> Xamarinプロジェクトでは、対応するネイティブAndroid APIのルールがFortify Secure Coding Rulepacksに存在する場合、Xamarin.Android APIのカスタムルールを使用する必要はありません。使用すると、重複した問題が報告される可能性があります。

11.3.4. 空白を含む設定を持つプロジェクトの変換

空白を含む環境設定またはその他の設定ファイルを使用してプロジェクトがビルドされている場合は、設定値を引用符で囲む必要があります。たとえば、環境設定 `Sample.sln` を使用してビルドされたVisual Studioソリューション `My Configuration` を変換するには、次のコマンドを使用します。

```
sourceanalyzer -b MySampleProj msbuild /t:rebuild /p:Configuration="My Configuration" Sample.sln
```

11.3.5. Visual Studioソリューションの単一プロジェクトの変換

Visual Studioソリューションに複数のプロジェクトが含まれている場合は、ソリューション全体ではなく1つのプロジェクトを変換することもできます。プロジェクトファイルには、 `proj` で終わるファイル名拡張子(`.vcxproj` や `.csproj` など)が付いています。1つのプロジェクトを変換するには、MSBuildコマンドのパラメータとしてソリューションの代わりにプロジェクトファイルを指定します。

次の例では、 `Sample.vcxproj` プロジェクトファイルを変換します。

```
sourceanalyzer -b MySampleProj msbuild /t:rebuild Sample.vcxproj
```

11.3.6. 複数の実行可能ファイルをビルドするプロジェクトの分析

Visual StudioまたはMSBuildプロジェクトで複数の実行可能ファイル(ファイル名拡張子 `*.exe` を持つファイルなど)をビルドする場合は、分析結果の誤検知の問題を避けるため、実行ファイルごとに個別に分析フェーズを実行することを強くお勧めします。これを行うには、分析フェーズの実行時に `–binary-name` オプションを使用して、実行可能ファイル名または .NETアセンブリ名をパラメータとして指定します。

次の例は、Sample1 (.NETアセンブリ名が関連付けられていないC++プロジェクト)とSample2 (.NETアセンブリ名 `Sample.sln` を持つ.NETプロジェクト)という2つのプロジェクトで構成されるVisual Studioソリューション `Sample2` を変換して分析する方法を示しています。各プロジェクトは、それぞれ別個の実行可能ファイル(`Sample1.exe` と `Sample2.exe`)をビルドします。分析結果は `Sample1.fpr` ファイルと `Sample2.fpr` ファイルに保存されます。

```
sourceanalyzer -b MySampleProj msbuild /t:rebuild Sample.sln sourceanalyzer -b MySampleProj -scan -binary-name Sample1.exe -f Sample1.fpr sourceanalyzer -b MySampleProj -scan -binary-name Sample2.exe -f Sample2.fpr
```

`-binary-name` オプションについて詳しくは、分析オプションを参照してください。

11.4. Visual Studioプロジェクトを変換する別の方法

このセクションでは、Visual Studioプロジェクトを変換する別の方法について説明します。

- Visual Studioソリューション用の別の変換オプション
- Fortify SASTを明示的に実行せずに変換する

11.4.1. Visual Studioソリューション用の別の変換オプション

Visual Studioソリューションでのみ使用できる変換方法には、次の2種類があります。

- Fortify Extension for Visual Studioを使用する
  Fortify Extension for Visual Studioは、変換および分析(スキャン)フェーズを1ステップで実行します。

- Fortify SASTコマンドにdevenvコマンドを追加する
  次のコマンドは、Visual Studioソリューション `Sample.sln` を変換します。

  ```
  sourceanalyzer -b MySampleProj devenv Sample.sln /rebuild
  ```

  Fortify SASTはdevenvの呼び出しを同等のMSBuildの呼び出しに変換するため、この場合、このコマンドを使用するソリューションはdevenvツールではなくMSBuildによってビルドされます。

11.4.2. Fortify SASTを明示的に実行せずに変換する

Fortify SASTを直接起動せずにVisual Studioプロジェクトを変換するオプションがあります。これには、 `DotNet` および `Framework` ディレクトリ内の *<sast_install_dir>\Core\private-bin\sca\MSBuildPlugin* にある Fortify.targets ファイルが必要です。プロジェクトをビルドするビルドコマンドラインで絶対パスまたは相対パスを使用してファイルを指定できます。使用しているビルドコマンド(`Dotnet` または `Framework`)に応じて、それぞれ `dotnet.exe` ディレクトリまたは `MSBuild.exe` ディレクトリを含むパスを使用します。例:

```
dotnet.exe msbuild /t:rebuild /p:CustomAfterMicrosoftCommonTargets= <sast_install_dir\Core\private-bin\sca\MSBuildPlugin\Dotnet\Fortify.targets Sample.sln>
```

または

```
msbuild.exe /t:rebuild /p:CustomAfterMicrosoftCommonTargets= <sast_install_dir>\Core\private-bin\sca\MSBuildPlugin\Framework\Fortify.targets Sample.sln
```

プロジェクトの変換を設定するために設定できる環境変数は複数あります。これらの変数の多くはデフォルト値を持ち、Fortify SASTでは変数が設定されていない場合に使用されます。これらの変数を次の表に示します。

環境変数	説明(Description)	デフォルト値
FORTIFY_MSBUILD_BUILDID	変換のFortify SASTビルドIDを指定します。この値は必ず設定してください。 これは、Fortify SAST `-b` オプションと同じです。	なし
FORTIFY_MSBUILD_DEBUG	デバッグモードを有効にします。これは、Fortify SAST `–debug` オプションと同じです。	False
FORTIFY_MSBUILD_DEBUG_VERBOSE	冗長デバッグモードを有効にします。これは、Fortify SAST `–debug-verbose` オプションと同じです。両方がtrueに設定されている場合は、FORTIFY_MSBUILD_DEBUGよりも優先されます。	False
FORTIFY_MSBUILD_MEM	変換のメモリ要件をJVM `-Xmx` オプションの形式で指定します。たとえば、 `-Xmx2G` になります。	システムで使用可能な物理メモリに基づいて自動割り当て
FORTIFY_MSBUILD_SCALOG	Fortify SASTログファイルの場所(絶対パス)を指定します。 これは、Fortify SAST `-logfile` オプションと同じです。	`%LOCALAPPDATA%/Fortify/sca/log/sca.log`

12. JavaScriptおよびTypeScriptコードの分析

JavaScript、TypeScript、JSX、およびTSXソースファイルが含まれるJavaScriptプロジェクト、およびHTMLファイルに埋め込まれているJavaScriptを分析できます。

一部のJavaScriptフレームワークは、平文のJavaScriptにトランスパイルされ(ソースからソースへのコンパイル)、これが生成されるコードになります。このタイプのコードを除外するには、 `-exclude` コマンドラインオプションを使用してください。

JavaScriptコードおよびTypeScriptコードを変換する場合は、すべてのソースファイルを1回の呼び出しで一緒に指定してください。Fortify　SASTでは、後続の呼び出し時にビルドIDで関連付けられたファイルリストに新しいファイルを追加する機能はサポートされていません。

Fortify　SASTでは、圧縮されたJavaScript　(*.min.js)を変換しません。

> **Note**
> 変換から除外する圧縮されたJavaScriptファイルには、Fortify SASTで自動的に検出できないタイプがあります。これらのファイルは、 `-exclude` コマンドラインオプションを使用して直接除外してください。

- ピュアJavaScriptプロジェクトの変換
- 依存関係の除外
- NPM依存関係の除外
- NPMの依存関係

- HTMLファイルを使用したJavaScriptプロジェクトの変換

12.1. ピュアJavaScriptプロジェクトの変換

JavaScriptを変換する基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer –b <build_id><js_file_or_dir>
```

ここで、 <js_file_or_dir> は変換するJavaScriptファイルの名前、または複数のJavaScriptファイルを含むディレクトリのいずれかです。 *.js に <js_file_or_dir> を指定して、複数のファイルを変換することもできます。

Vue 3プロジェクトの分析(プレビュー版)

Vue 3プロジェクトを翻訳してスキャンするには、翻訳とスキャンの両方でコマンドライン指示内に -flight-js オプションと -vue3 オプションを含めます。

```
sourceanalyzer -b <build_id> -flight-js -vue3 <vue_files_or_dir> sourceanalyzer -b <build_id> -flight-js -vue3 -scan -f results.fpr
```

12.2. 依存関係の除外

特定の依存関係の変換を回避するには、 fortify-sca.properties ファイル内の適切なプロパティ設定に追加します。次のプロパティで指定されたファイルは変換されません。

- com.fortify.sca.skip.libraries.ES6
- com.fortify.sca.skip.libraries.jQuery
- com.fortify.sca.skip.libraries.javascript
- com.fortify.sca.skip.libraries.typescript

各プロパティには、ファイル名(パス情報なし)のカンマまたはコロン区切りリストを指定します。

これらのプロパティで指定されたファイルは、ローカルファイルとインターネット上のファイルの両方に適用されます。たとえば、JavaScriptコードに次のローカルファイル参照が含まれるとします。

```
<script  src="js/jquery-ui.js"  type="text/javascript"  charset="utf-8"></script>
```

デフォルトでは、 ファイル内の プロパティに が含まれるため、Fortify SASTでは前の例に示したファイルを変換しません。

ファイル名には正規表現を使用できます。Fortify SASTでは '(-?\d+\.\d+\.\d+)?' プロパティ値に含まれる各ファイル名の .min.js または .js の前に正規表現 com.fortify.sca.skip.libraries.jQuery を自動的に挿入します。

> **Note**
>
> -exclude コマンドラインオプションを使用して、ローカルファイルまたはディレクトリ全体を除外することもできます。このオプションの詳細については、変換オプションを参照してください。

詳細な分析を行うために、依存関係の言語が -disable-language オプションで無効になっている場合でも、依存関係ファイルが変換に含まれます。言語を無効にするオプションの詳細については、「変換オプション」を参照してください。

12.3. NPM依存関係の除外

デフォルトで、Fortify SASTではコードにインポートされたNPM依存関係のみを変換します。この動作は、次の2つのプロパティで変更できます。

- com.fortify.sca.follow.imports プロパティは、インポートされたファイルを解決して変換に含めることをFortify SASTに指示します。
  このプロパティは、デフォルトで有効になっています。このプロパティの値をfalseに設定すると、コマンドラインに明示的に含まれていないNPM依存関係は変換に含まれません。

- com.fortify.sca.exclude.unimported.node.modules プロパティは、com.fortify.sca.follow.imports プロパティによって特定的にインポートされたファイルを除き、node_modulesディレクトリ内のすべてのファイルを変換から除外することをFortify SASTに指示します。
  このプロパティはデフォルトで有効になっています。これは、ビルドシステムにのみ必要な依存関係など、最終プロジェクトには必要ない依存関係の変換を避けるためです。

12.4. NPMの依存関係

デフォルトでは、Fortify SASTはNPM依存関係(node_modules ディレクトリ内のファイル)の問題を報告しません。この設定は、 com.fortify.sca.exclude.node.modules プロパティで設定されます。このプロパティは、デフォルトで true に設定されています。



Note

com.fortify.sca.exclude.node.modules が true に設定されている場合には、-excludeオプションを使用してノードモジュールを除外することをお勧めしません。結果の品質が変わる可能性があるためです。

- NPM依存関係の除外の例

12.4.1. NPM依存関係の除外の例

次の例は、NPM依存関係を除外する3つの異なるシナリオを示しています。これらの例では、次のディレクトリ構造を使用します。

```
./ RootProjectDir innerSrcDir node_modules innerProjectReferencedModule index.ts
moduleNotReferencedByProject index.ts innerProject.ts (contains import from innerProjectReferencedModule)
node_modules projectReferencedModule index.ts moduleNotReferencedByProject index.ts projectMain.ts
(contains import from projectReferencedModule)
```

例1

この例は、 com.fortify.sca.exclude.unimported.node.modules が false に設定された状態で、ファイルが変換される場合を示しています。この場合、 com.fortify.sca.follow.imports と com.fortify.sca.exclude.unimported.node.modules が両方とも true に設定されています。

```
sourceanalyzer -Dcom.fortify.sca.exclude.node.modules=false RootProjectDir/
```

例1の変換には、次のファイルが含まれます。

```
./RootProjectDir/innerSrcDir/innerProject.ts
./RootProjectDir/innerSrcDir/node_modules/innerProjectReferencedModule/index.ts
./RootProjectDir/projectMain.ts ./RootProjectDir/node_modules/projectReferencedModule/index.ts
```

例2

この例は、プロジェクトによって参照されているモジュールに加えて、解決中に見つかったがプロジェクトによって参照されていないモジュールも変換に含める場合を示しています。

```
sourceanalyzer -Dcom.fortify.sca.exclude.unimported.node.modules=false RootProjectDir/
```

例2の変換には、次のファイルが含まれます。

```
./RootProjectDir/innerSrcDir/innerProject.ts
./RootProjectDir/innerSrcDir/node_modules/innerProjectReferencedModule/index.ts
./RootProjectDir/innerSrcDir/node_modules/moduleNotReferencedByProject/index.ts
./RootProjectDir/projectMain.ts          ./RootProjectDir/node_modules/projectReferencedModule/index.ts
./RootProjectDir/node_modules/moduleNotReferencedByProject/index.ts
```

例3

この例は、-excludeオプションを使用して、任意の node_modules ディレクトリ内のすべてのファイルを除外する場合を示しています。 -exclude オプションは、 com.fortify.sca.follow.imports および com.fortify.sca.exclude.unimported.node.modules プロパティの設定に基づくモジュールの解決策を上書きします。

```
sourceanalyzer  RootProjectDir/  -exclude  "**/node_modules/*.*"
```

例3の変換には、次のファイルが含まれます。

```
./RootProjectDir/innerSrcDir/innerProject.ts    ./RootProjectDir/projectMain.ts
```

12.5. HTMLファイルを使用したJavaScriptプロジェクトの変換

プロジェクトにJavaScriptファイルに加えてHTMLファイルが含まれている場合は、次の例に示すように、 com.fortify.sca.EnableDOMModeling ファイルまたはコマンドラインで fortify-sca.properties プロパティをtrueに設定します。

```
sourceanalyzer  -b  MyProject  <js_file_or_dir>  -Dcom.fortify.sca.EnableDOMModeling=true
```

プロパティをtrueに設定すると、DOM関連のクロスサイトスクリプティングの問題など、DOM関連の攻撃に関する偽陰性レポートを減らすことができます。



Note

このオプションを有効にすると、Fortify SASTではHTMLファイル内のDOMツリー構造をモデル化するJavaScriptコードが生成されます。分析フェーズの時間が長くなる場合があります(分析する変換済みコードが多くなるため)。

com.fortify.sca.EnableDOMModeling プロパティを true に設定した場合は、Fortify SASTがDOMモデリングに含める追加のHTMLタグを com.fortify.sca.DOMModeling.tags プロパティで指定することもできます。デフォルトで、Fortify SASTはHTMLタグ body 、 button 、 div 、 form 、 iframe 、 input 、 head 、 html 、および p を含めます。

たとえば、HTMLタグ ul および li をDOMモデルに追加で含めるには、次のコマンドを使用します。

```
sourceanalyzer  -b  MyProject  <js_file_or_dir>  -Dcom.fortify.sca.DOMModeling.tags=ul,li
```

13. DartおよびFlutterコードの分析

このセクションでは、DartおよびFlutterコードを変換する方法について説明します。Fortify SASTでは、WindowsおよびLinux上のDartおよびFlutterコードの分析をサポートしています。

- DartおよびFlutter変換の前提条件
- DartおよびFlutterのコマンドライン構文
- DartおよびFlutterのコマンドライン例

13.1. DartおよびFlutter変換の前提条件

DartプロジェクトとFlutterプロジェクトを変換するための前提条件は次のとおりです。

- サポートされているDart SDK (Dart専用プロジェクトの場合)およびFlutter SDK (Flutterプロジェクトの場合)がシステムにインストールされている必要があります。サポートされているDartおよびFlutter SDKのバージョンについては、「サポートされている言語」を参照してください。
- 次のいずれかのコマンドを実行して、プロジェクトの依存関係をダウンロードします。
  - Flutterプロジェクトの場合は、 `flutter pub get` を使用します。
  - Dart専用プロジェクトの場合は、 `dart pub get` を使用します。

  たとえば、プロジェクトルートが `myproject` のFlutterプロジェクトの依存関係をダウンロードするには、次のコマンドを実行します。

```
cd myproject flutter pub get
```

> **Important**
> プロジェクトに、 `pubspec.yaml` ファイルが異なるネストされたパッケージが含まれている場合は、パッケージルートごとに `dart pub get` または `flutter pub get` を実行する必要があります。

> **Important**
> プロジェクトディレクトリに次のものが含まれている必要があります。
>
> - `pubspec.yaml` ファイル。このファイルは依存関係を指定します
> - `.dart_tool` ディレクトリ。このディレクトリには、 `pub` ツールによって自動的に生成される `package_config.json` ファイルが含まれます

13.2. DartおよびFlutterのコマンドライン構文

DartおよびFlutterのコードを変換する基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id> <translation_options> <dirs> sourceanalyzer -b <build_id>
<translation_options> <files>
```

13.3. DartおよびFlutterのコマンドライン例

`my_app` プロジェクトルートディレクトリを使用してDartプロジェクトまたはFlutterプロジェクトを変換するには:

```
sourceanalyzer -b MyProject my_app/
```

`a_widget.dart` プロジェクトルートディレクトリ内の `my_app` ファイルを変換するには、次のコマンドを使用します。

```
sourceanalyzer -b MyProject my_app/a_widget.dart
```

`my_dart_proj` ディレクトリ内のすべてのdartソースファイルを変換するには:

```
sourceanalyzer -b MyProject "my_dart_proj/**/*.dart"
```

14. PythonおよびJupyter Notebookの分析

Fortify SASTはPythonアプリケーションを変換し、 `.py` 拡張子を持つファイルをPythonソースコードとして処理します。拡張子が `.ipynb` のファイルはJupyter Notebookとして認識されます。Fortify SASTは、Jupyter NotebookとDjangoおよびFlaskフレームワークの変換をサポートしています。

- Bazelとの統合
- Python変換コマンドライン構文
- 仮想環境でのPythonの変換

- インポート済みのモジュールとパッケージを含める
- ネームスペースパッケージを含める
- DjangoとFlaskの変換

14.1. Bazelとの統合

Bazelのビルドと統合するために、Fortify SASTはソースファイルをコンパイル時に変換します。したがって、Bazelのビルドの前提条件は、Bazelのビルドが正常に実行されることです。サポートされているBazelのバージョンについては、「ビルドツール」を参照してください。

Bazelと統合するには、Bazelのワークスペースディレクトリに移動し、構築するBazelのターゲットでs sourceanalyzerを実行します。次のように、変換のための他のsourceanalyzerオプションを指定できます。

```
sourceanalyzer -b <build_id> <sca_options> bazel build <target>
```

プロジェクトを変換し、変換からファイルを除外する場合:

```
sourceanalyzer -b MyProjectC -exclude C:¥test¥MY-JAVA-APP¥src¥proj¥content.py bazel build //projc:my-python-prj
```

14.1.1. Python Bazelの統合例

特定のターゲットのプロジェクトを変換する場合:

```
sourceanalyzer -b MyProjectA bazel build //proja:my-prj
```

パッケージ `proja/abc` 内のターゲット `abc` を変換する場合:

```
sourceanalyzer -b MyProjectA bazel build //proja/abc
```

または

```
sourceanalyzer -b MyProjectA bazel build //proja/abc:abc
```

パッケージ `proja/abc` 内のすべてのターゲットを変換する場合:

```
sourceanalyzer -b MyProjectA bazel build //proja/abc:all
```

`projb/` ディレクトリ内のすべてのターゲットを変換する場合:

```
sourceanalyzer -b MyProjectB bazel build //projb/...
```

変換にPythonプロジェクトの依存関係を指定する場合:

```
sourceanalyzer -b MyProjectD -python-path /usr/local/lib/python3.6/ bazel build //projd:my-python-app
```

Fortify SASTとBazelの統合では、複数のターゲットおよび関連アクション(ターゲットの除外など)はサポートされていません。

14.2. Python変換コマンドライン構文

Pythonコードを変換する基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id> -python-version <python_version> -python-path <dirs> <files>
```



Note

Pythonコードを変換する場合は、すべてのソースファイルを1回の呼び出しで一緒に指定してください。Fortify SASTでは、後続の呼び出し時にビルドIDで関連付けられたファイルリストに新しいファイルを追加する機能はサポートされていません。

14.2.1. Pythonコマンドラインオプション

次の表では、Pythonオプションについて説明します。

Pythonオプション	説明(Description)
`-python-version <version>`	スキャンするPythonソースコードのバージョンを指定します。`<version>`の有効な値は、`2`および`3`です。デフォルト値は`3`です。 **同等のプロパティ名:** `com.fortify.sca.PythonVersion`
`-python-no-auto-root-calculation`	モジュールおよびパッケージのインポートに使用する、すべてのプロジェクトソースファイルの共通ルートディレクトリの自動計算を無効にします。 **同等のプロパティ名:** `com.fortify.sca.PythonNoAutoRootCalculation`
`-python-path <dirs>`	追加のインポートディレクトリのセミコロン区切り(Windows)またはコロン区切り(Windows以外)リストを指定します。`-python-path`オプションを使用して、パッケージまたはモジュールのインポートに使用するパスを指定できます。このオプションを使用してネームスペースパッケージディレクトリのすべてのパスを含めてください。Fortify SASTでは、インポートされるファイルごとに指定されたパスを順番に検索し、最初に検出されたファイルを使用します。 **同等のプロパティ名:** `com.fortify.sca.PythonPath`
`-django-template-dirs <dirs>`	Djangoテンプレートを含むディレクトリのセミコロン区切り(Windows)またはコロン区切り(Windows以外)リストを指定します。Fortify SASTでは、Djangoテンプレートファイルごとに指定されたパスを順番に検索し、最初に検出されたテンプレートファイルを使用します。 **同等のプロパティ名:** `com.fortify.sca.DjangoTemplateDirs`
`-django-disable-autodiscover`	Fortify SASTでDjangoテンプレートを自動検出しないことを指定します。 **同等のプロパティ名:** `com.fortify.sca.DjangoDisableAutodiscover`
`-jinja-template-dirs <dirs>`	Jinja2テンプレートを含むディレクトリのセミコロン区切り(Windows)またはコロン区切り(Windows以外)リストを指定します。Fortify SASTでは、Jinja2テンプレートファイルごとに指定されたパスを順番に検索し、最初に検出されたテンプレートファイルを使用します。 **同等のプロパティ名:** `com.fortify.sca.JinjaTemplateDirs`

Pythonオプション	説明(Description)
-disable-template-autodiscover	Fortify SASTでDjangoまたはJinja2テンプレートを自動検出しないことを指定します。 **同等のプロパティ名:** com.fortify.sca.DisableTemplateAutodiscover

Pythonのプロパティ

14.2.2. Pythonのコマンドライン例

WindowsでPython 3コードを変換する場合:

```
sourceanalyzer -b Python3Proj -python-path "C:¥Python312¥Lib;C:¥Python312¥Lib¥site-packages" src/*.py
```

WindowsでPython 2コードを変換する場合:

```
sourceanalyzer -b MyPython2 -python-version 2 -python-path "C:¥Python27¥Lib;C:¥Python27¥Lib¥site-packages" src/*.py
```

Windows以外でPython 3コードを変換する場合:

```
sourceanalyzer -b Python3Proj -python-path /usr/lib/python3.12:/usr/local/lib/python3.12/site-packages src/*.py
```

Windows以外でPython 2コードを変換する場合:

```
sourceanalyzer -b MyPython2 -python-version 2 -python-path /usr/lib/python2.7:/usr/local/lib/python2.7/site-packages src/*.py
```

14.3. 仮想環境でのPythonの変換

このセクションでは、仮想環境でPythonプロジェクトを変換する方法について説明します。プロジェクトのすべての依存関係が仮想環境にインストールされていることを確認してください。仮想環境でPythonプロジェクトを変換するには、プロジェクトの依存関係を指定する -python-path オプションを含めます。

Python仮想環境の例

仮想環境名が myenv で、プロジェクトの依存関係が myenv/lib/python<version>/site-packages ディレクトリにインストールされているPythonプロジェクトを変換するには、次のように入力します。

```
sourceanalyzer -b mybuild -python-path "myenv/lib/python<version>/site-packages/" myproject/
```

conda環境の例

conda環境名が myenv で、プロジェクトの依存関係が *<conda_install_dir>*/envs/myenv/lib/python*<version>*/site-packages ディレクトリにインストールされているPythonプロジェクトを変換するには、次のように入力します。

```
sourceanalyzer -b mybuild -python-path "<conda_inst all_dir>/envs/myenv/lib/python<version>/site-packages/" myproject/
```

14.4. インポート済みのモジュールとパッケージを含める

Pythonアプリケーションを変換してスキャンに備えるため、Fortify SASTではアプリケーションが使用するインポート済みのモジュールおよびパッケージを検索します。Fortify SASTでは、Pythonランタイムシステムがインポート済みのモジュールとパッケージを検索するために使用する PYTHONPATH 環境変数を考慮しません。

Fortify SASTでは、次の順序でディレクトリのリストを使用して、インポート済みのモジュールとパッケージを検索します。

1. すべてのプロジェクトソースファイルの共通ルートディレクトリ。Fortify SASTが自動的に計算します。たとえば、2つのプロジェクトディレクトリ `PrimaryDir/project1/*` および `PrimaryDir/project2/*` が存在する場合、共通ルートディレクトリは `PrimaryDir` です。
   インポート済みモジュールおよびパッケージの検索ターゲットである共通ルートディレクトリを削除するには、変換コマンドに `-python-no-auto-root-calculation` オプションを含める必要があります。
2. `-python-path` オプションで指定されたディレクトリ。
   Fortify SASTでは、標準Pythonライブラリのモジュールのサブセットを変換に含めます(「builtins」モジュール、もともとCで記述されたすべてのモジュールなど)。Fortify SASTでは最初にFortify SASTに含まれるセットで標準Pythonライブラリモジュールを検索し、次に `-python-path` オプションで指定されたパスで検索します。Fortify SASTで見つからないモジュールをPythonコードでインポートすると、警告が表示されます。標準Pythonライブラリのすべてのモジュールが見つかるようにするには、`-python-path` リストで標準Pythonライブラリへのパスを追加します。
3. 変換中のファイルを含むカレントディレクトリ。たとえば、Fortify SASTで `PrimaryDir/project1/a.py` を変換すると、インポート済みモジュールおよびパッケージを検索する最後のディレクトリとしてディレクトリ `PrimaryDir/project1`が追加されます。

14.5. ネームスペースパッケージを含める

ネームスペースパッケージを変換するには、`-python-path` オプションを使用してネームスペースパッケージディレクトリへのすべてのパスを含める必要があります。たとえば、複数のフォルダにネームスペースパッケージ `package_name` の2つのサブパッケージが含まれている場合は:

```
/path_1/package_name/subpackageA
/path_2/package_name/subpackageB
```

Sourceanalyzerコマンドラインに、`/path_1;/path_2` オプションとともに `-python-path` を含めます。

14.6. DjangoとFlaskの変換

デフォルトでは、Fortify SASTはプロジェクトのルートディレクトリ内のDjangoおよびJinja2テンプレートの検出を試みます。検出されたDangoおよびJinja2テンプレートはすべて自動的に変換に追加されます。Sourceanalyzerコマンドに `-django-template-dirs` または `-jinja-template-dirs` オプションを追加して、DjangoまたはJinja2テンプレートファイルの追加の場所を指定できます。

Fortify SASTでDjangoおよびJinja2テンプレートを自動的に検出しないようにする場合には、`-disable-template-autodiscover`オプションを使用します。プロジェクトにDjangoまたはJinja2テンプレートが必要なのに、テンプレートが予期しない場所にあるようにプロジェクトが設定されている場合には、次のWindows以外の例に示されているように、`-disable-template-autodiscover` オプションに加えて `-django-template-dirs` または `-jinja-template-dirs` オプションを使用して、テンプレートを含むディレクトリを指定します。

```
sourceanalyzer -b djangoProj -python-path /usr/lib/python3.12:/usr/local/lib/python3.12/site-packages
djangoProj -django-template-dirs djangoProj/templatedir1:/djangoProj/dir2 -disable-template-autodiscover
```

```
sourceanalyzer -b flaskProj -python-path /usr/lib/python3.12:/usr/local/lib/python3.12/site-packages
flaskProj -jinja-template-dirs flaskProj/templatedir1:/flaskProj/dir2 -disable-template-autodiscover
```

次の例では、Windows上でDangoテンプレートとJinja2テンプレートを組み合わせて使用するPythonプロジェクトを変換します。

```
sourceanalyzer -b pythonProj -python-path "C:¥Python312¥Lib;C:¥Python312¥Lib¥site-packages" flaskProj -
django-template-dirs "C:¥djangoProj¥templatedir1;C:¥djangoProj¥dir2" -jinja-template-dirs
"C:¥flaskProj¥templatedir1;C:¥flaskProj¥dir2" -disable-template-autodiscover
```

15. iOSおよびXcodeプロジェクトの分析

このセクションでは、iOSアプリケーションのSwift、Objective-C、およびObjective-C++ソースコードを変換する方法について説明します。プロジェクトのソースファイルを識別するために、Fortify SASTは自動的にXcodeコマンドラインツールのXcodebuildに統合されます。

- iOSプロジェクト変換の前提条件
- iOSコード分析のコマンドライン構文

15.1. iOSプロジェクト変換の前提条件

iOSプロジェクトを変換するための前提条件は次のとおりです。

- Objective-C++プロジェクトは、非脆弱なObjective-Cランタイム(ABIバージョン2または3)を使用する必要があります。
- Appleの `xcode-select` コマンドラインツールを使用して、Xcodeパスを設定します。Fortify SASTでは、システムグローバルなXcode設定を使用して、Xcodeツールチェーンとヘッダを検索します。
- 正常なXcodeビルドに必要なすべてのソースファイルが提供されていることを確認します。 `-exclude` オプションを使用して、分析からファイルを除外できます(iOSコード分析のコマンドライン構文を参照)。
- プロジェクトをビルドするために必要な依存関係が用意されている必要があります。
- Swiftコードを変換するには、CocoaPodsを含むすべてのサードパーティモジュールを使用できることを確認します。ブリッジヘッダも使用可能である必要があります。ただしXcodeでは、通常、ビルド中にこれらのファイルを自動的に生成します。
- プロジェクトにバイナリ形式のプロパティリストファイルが含まれる場合は、先にファイルをXML形式に変換する必要があります。これを行うには、Xcodeの `putil` コマンドを使用できます。
- Objective-Cプロジェクトを変換するには、サードパーティライブラリのヘッダが使用可能な必要があります。
- WatchKit®istered trademark;アプリケーションを変換するには、iPhoneアプリケーションターゲットとWatchKit Extensionターゲットの両方を変換してください。

15.2. iOSコード分析のコマンドライン構文

次のコマンドライン構文を使用して、iOSコードを変換できます。

```
sourceanalyzer -b <build_id> xcodebuild [<compiler_options>]
```

ここで、 `<compiler_options>` はXcodeコンパイラに渡される、サポートされているオプションです。何らかの `build` を指定した `<compiler_options>` オプションを含める必要があります。Fortify SAST Xcodebuildの統合では、 `xcodebuild archive` などの代替ビルドコマンドの出力形式はサポートされていません。



Note

このコマンドを実行すると、xcodebuildによってソースコードがコンパイルされます。

分析からファイルを除外するには、 `-exclude` オプションを使用します(変換オプションを参照)。ファイルがXcodeのビルドに含まれている場合でも、除外指定に一致するすべてのソースファイルが変換されません。次に例を示します。

```
sourceanalyzer -b MyProject -exclude "**/TestFile.swift" xcodebuild clean build
```



Note

`-exclude` オプションでは、除外パターンでファイルが明示的に指定されている場合でも、Xcodeビルド統合中に生成またはダウンロードされたSwiftソースファイル(たとえば、 `**/DerivedData/**` の下のファイル)が除外されません。

アプリケーションがプロパティリストファイル(たとえば `<file>.plist`)を使用している場合は、これらのファイルを別の `sourceanalyzer` コマンドで変換します。プロジェクトファイルの変換に使用したものと同じビルドIDを使用します。次に例を示します。

```
sourceanalyzer -b MyProject <path_to_plist_files>
```

プロジェクトでCocoaPodsを使用している場合は、 `-workspace` を含めてプロジェクトをビルドします。例:

```
sourceanalyzer -b DemoAppSwift xcodebuild clean build -workspace DemoAppSwift.xcworkspace -scheme
DemoAppSwift -sdk iphonesimulator
```

変換が完了したら、次の例に示すように、分析フェーズを実行して結果をFPRファイルに保存できます。

```
sourceanalyzer -b DemoAppSwift -scan -f MyResults.fpr
```

16. CおよびC++コードの分析

このセクションでは、CおよびC++コードを変換する方法について説明します。Fortify SASTは標準のANSI CおよびC++をサポートしており、すべての非標準のC++構成をサポートしているとは限りません。

> **Important**
>
> このセクションでは、Visual StudioまたはMSBuildプロジェクトの一部 *ではない* CおよびC++コードを変換する方法について説明します。Visual StudioまたはMSBuildプロジェクトの変換方法については、「Visual StudioおよびMSBuildプロジェクトの変換」を参照してください。

- CおよびC++コード変換の前提条件
- Makeとの統合
- CMakeとの統合
- Gradleとの統合
- CおよびC++の手動変換構文
- C/C++のプリコンパイル済みヘッダファイル
- 他のコンパイラの使用

16.1. CおよびC++コード変換の前提条件

プロジェクトをビルドするために必要な依存関係(サードパーティ製ライブラリのヘッダを含む)があることを確認してください。Fortify SAST変換では、オブジェクトファイルと静的/動的ライブラリのファイルは必要ありません。

16.2. Makeとの統合

Fortify SASTをmakeと統合するには、ビルドプロセスのために `sourceanalyzer` とMakeを組み合わせて実行します。次のビルドコマンドを使用してプロジェクトを構築する場合の例:

```
make clean make make install
```

次のサンプルコマンドを使用して、プロジェクト全体を同時に変換およびコンパイルできます。

```
make clean sourceanalyzer -b MyProject make make install
```

ビルド統合の代替方法として、ビルドスクリプトを変更して、各コンパイラ、リンカ、およびアーカイバ操作の前に `sourceanalyzer` コマンドを追加することもできます。たとえば、makefileでは、これらのツールの名前に変数が定義されることが多いです。

```
CC=gcc
CXX=g++
LD=ld AR=ar
```

makefile内のツール参照の前に、 sourceanalyzer コマンドと適切なオプションを付加できます。

```
CC=sourceanalyzer -b MyProject gcc CXX=sourceanalyzer -b MyProject g++ LD=sourceanalyzer -b MyProject ld
AR=sourceanalyzer -b MyProject ar
```

各操作に同じビルドIDを使用する場合は、Fortify SASTで自動的に、個別に変換された各ファイルが変換された単一のプロジェクトに結合されます。

16.3. CMakeとの統合

Windows以外のシステムでは、Fortify SASTコマンドにJSONコンパイルデータベースを組み込むことによって、CMakeを使用してビルドされたプロジェクトを変換できます。これは、MakefileジェネレータとNinjaジェネレータでのみサポートされています(詳細については、『CMake Reference Documentation』を参照してください)。

Fortify SASTをCMakeビルドと統合するには:

1. CMakeプロジェクト用の compile_commands.json ファイルを生成します。
   -DCMAKE_EXPORT_COMPILE_COMMANDS=yes 設定コマンドに cmake を追加します。例:

   ```
   cmake -G Ninja -DCMAKE_EXPORT_COMPILE_COMMANDS=yes
   ```

2. 次のようにして、 sourceanalyzer コマンドにJSONコンパイルデータベースを含めます。

   ```
   sourceanalyzer -b <build_id> compile_commands.json
   ```

16.4. Gradleとの統合

Gradle統合には、C++アプリケーションプラグインに関する前提条件があります。Gradleファイルに次のいずれかの形式で追加してください。

```
apply plugin: 'cpp'
```

```
plugins { id 'cpp-application' }
```

Gradleの統合は、Gradleまたはgradlewのコマンドラインにコマンドを前に付加するだけで、次のように簡単にできます。

```
sourceanalyzer -b <build_id><sca_options> gradle [<gradle_options>] <gradle_tasks>
```

詳細なガイドについては、「JavaとKotlinの統合: Gradle統合の使用」を参照してください。

16.5. CおよびC++の手動変換構文

コンパイラに渡されるコマンドラインオプションは、プリプロセッサの実行に影響を与え、言語の機能や拡張機能を有効または無効にすることができます。Fortify SASTでコンパイラと同じようにソースコードを解釈するには、C/C++ソースコードの変換フェーズで完全なコンパイラコマンドラインが必要です。元のコンパイラコマンドの前に sourceanalyzer コマンドとオプションを指定します。

1つのファイルを変換する基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id> [<sca_options>] <compiler> [<compiler_options>] <file>.c
```

ここで:

- *<sca_options>* Fortify SASTに渡されるオプションです。

- *<compiler>* 使用するC/C++コンパイラの名前(gcc 、 g++ 、 cl など)です。サポートされているC/C++コンパイラのリストについては、「サポートされる言語」を参照してください。
- *<compiler_options>* C/C++コンパイラに渡されるオプションです。
- *<file>*.c ASCIIまたはUTF-8エンコーディング形式である必要があります。



Note

Fortify SASTのすべてのオプションをコンパイラオプションの前に指定する必要があります。

コンパイラコマンドは、単独で実行したときに正常に完了する必要があります。コンパイラコマンドが失敗する場合は、コンパイラコマンドの前に指定したFortify SASTコマンドも失敗します。

たとえば、次のコマンドを使用してファイルをコンパイルするとします。

```
gcc -I. -o hello.o -c helloworld.c
```

この場合、次のコマンドを使用してこのファイルを変換できます。

```
sourceanalyzer -b MyProject gcc -I. -o hello.o -c helloworld.c
```

Fortify SASTは、変換フェーズの一部として元のコンパイラコマンドを実行します。前のコマンド例では、スキャンに適した変換済みのソースと、 hello.o を実行して得られるオブジェクトファイル gcc の両方が生成されます。Fortify SAST -nc オプションを使用して、コンパイラの実行を無効にすることができます。

16.6. C/C++のプリコンパイル済みヘッダファイル

一部のC/C++コンパイラは、コンパイルのパフォーマンスを向上させるプリコンパイル済みヘッダファイルをサポートしています。コンパイラによっては、この機能の実装によって微妙な副作用が発生します。この機能を有効にすると、コンパイラが警告やエラーなしで誤ったソースコードを受け入れる可能性があります。その結果、Fortify SASTで変換エラーが報告されてもコンパイラでは報告されないという矛盾が発生する可能性があります。

コンパイラのプリコンパイル済みヘッダ機能を使用する場合は、プリコンパイル済みヘッダを無効にしてから、完全ビルドを実行してソースコードが正しくコンパイルされるのを確認してください。

16.7. 他のコンパイラの使用

サポートされていないCコンパイラアダプタには、GCCやMSVCなどの標準コンパイラを使用できない場合の代替手段が用意されています。

Configuration

カスタムコンパイラとリンカを登録するには、次のエントリを fortify-sca.properties ファイルに追加します。

```
com.fortify.sca.compilers.mycompiler = com.fortify.sca.util.compilers.ConfigurableCompiler
com.fortify.sca.compilers.mylinker = com.fortify.sca.util.compilers.LdCompiler
```

mycompiler と mylinker をコンパイラおよびリンカ実行ファイルの実際の名前に置き換えます。

分析の実行

アダプタを構成した後、標準コマンドで sourceanalyzer を実行します。

アダプタでは、GCCスタイルのプローブを使用して、システムincludeディレクトリをコンパイラに対してプローブします。プローブが失敗すると、次の警告が表示されます。

```
No system includes found for compiler mycompiler. Translation will not be able to find system include
directories.
```

これは、エンジンがシステムヘッダ(iostream 、 vector 、 stdio.h など)を見つけられないことを意味します。

これを解決するには、 com.fortify.sca.ctran.clang-args プロパティを使用してincludeディレクトリを手動で指定します。

```
-Dcom.fortify.sca.ctran.clang-args="-isystem /my/system/dir -isystem /my/other/system/dir"
```

非標準構文の処理

非標準のC/C++構成の中には、エンジンによる変換の停止の原因となるものがあります。

認識されないカスタムプリプロセッサディレクティブをコードで使用する場合は、 FORTIFYSCA マクロを使用して条件付きブロックでラップします。

```
#ifdef FORTIFYSCA #include "myinclude.h" #else #includetag* "myinclude.h" #endif // FORTIFYSCA
```

次に、マクロ定義を com.fortify.sca.ctran.clang-args プロパティ経由で渡します。

```
-Dcom.fortify.sca.ctran.clang-args="-DFORTIFYSCA"
```

Fortify SASTでは標準の #include ディレクティブを使用しますが、コンパイラでは引き続きネイティブ構文を使用します。

Clang引数リファレンス

com.fortify.sca.ctran.clang-args プロパティは、C/C++変換中にエンジンで使用するClangフロントエンドに直接引数を渡します。

サポートされている引数の完全なリストについては、Clangコマンドラインリファレンスを参照してください。

17. Rustコードの分析

このセクションでは、Rustプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Rust分析の前提条件
- Rustの変換構文

17.1. Rust分析の前提条件

現在、RustコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Rustコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

17.2. Rustの変換構文

AIを活用したSASTを使用して分析対象にRustコードを含めるには、分析対象のすべてのソースファイルを含めます。

Rustコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。



Example

```
sourceanalyzer -b <build_id>"**/*.rs"
```

18. Fortranコードの分析

このセクションでは、Fortranプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Fortran分析の前提条件
- Fortranの変換構文

18.1. Fortran分析の前提条件

現在、FortranコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Fortranコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

18.2. Fortranの変換構文

AIを活用したSASTを使用して分析対象にFortranコードを含めるには、分析対象のすべてのソースファイルを含めます。

Fortranコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。



Example

```
sourceanalyzer -b <build_id> "**/*.f"
```



Important

Fortranソースファイルでサポートされているファイル拡張子は、`.f`、`.for`、`.ftn`、`.f90`、`.f95`、`.f03`、`.f08`、`.f15`、`.f18` です。

19. AIエージェント指示ファイルの分析

このセクションでは、AIエージェント指示ファイルを分析する方法について説明します。

このセクションでは、次のトピックについて説明します。

- AIエージェント指示ファイル分析の前提条件
- AIエージェント指示ファイルの変換構文

19.1. AIエージェント指示ファイル分析の前提条件

現在、AIエージェント指示ファイルの分析はAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

19.2. AIエージェント指示ファイルの変換構文

AIを活用したSASTを使用して分析対象にAIエージェント指示ファイルを含めるには、分析対象のすべてのAIエージェント指示ファイルを含めます。

AIエージェント指示ファイルを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.md"
```

Important
AIエージェント指示ファイルでサポートされているファイル拡張子は .md 、 .mdc 、 .cursorrules 、 .windsurfrules です。

20. Goコードの分析

このセクションでは、Goコードを変換する方法について説明します。Fortify SASTでは、Windows、Linux、およびmacOS®istered trademark;上のGoコードの分析をサポートしています。

- Goコマンドライン構文
- Goコマンドラインオプション
- カスタムGoビルドタグを含める
- 依存関係の解決

20.1. Goコマンドライン構文

最善の結果を得るには、プロジェクトがコンパイル可能で、必要なすべての依存関係を利用できる必要があります。次のエンティティは、変換(およびスキャン)から除外されます。

- ベンダフォルダ
- サブフォルダ内の任意の go.mod ファイルによって定義されたプロジェクト(%PROJECT_ROOT%の下にある go.mod ファイルによって定義されたプロジェクトを除く)
- _test.go サフィックスが付くすべてのファイル(ユニットテスト)

Goコードを変換する基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id> [-gopath <dir>] [-goroot <dir>] <files>
```

最善の結果を得るために、すべてのGoプロジェクトにGoモジュールを使用し、Goコードを1つずつモジュールに変換するようお勧めします。sourceanalyzerコマンドの*<files>*パラメータの値が、 go.mod ファイルを含むディレクトリ内に存在するようにしてください。これは、プロジェクトをビルドするために go build コマンドを実行するディレクトリと同じです。プロジェクトが複数のモジュールで構成されている場合には、sourceanalyzerコマンドを同じ*<build_id>*値で複数回実行して、すべてのモジュールの変換結果をまとめることができます。

ビルド用のGOPATH開発モードの使用は引き続きサポートされますが、これは、2つのスキャンをFireify Audit WorkbenchやFortify Software Security Centerなどのツールで比較しようとする場合に問題を引き起こす可能性があります。モジュールの固定識別子パスを定義する go.mod ファイルがない場合、Go言語システムは各モジュールをローカルファイルシステム上の絶対パスで識別します。したがって、異なるサブディレクトリや異なるマシンから同じモジュールを2回スキャンすると、異なるモジュール識別子が生成されるため、マッチング問題が2つのスキャン間で正しく関連付けられません。 GOPATH開発モードは、Goコンパイラおよびsdkに対して非推奨となり、今後のGo 1.xxリリースで削除される予定です。

20.2. Goコマンドラインオプション

次の表では、Goコード変換専用のコマンドラインオプションについて説明します。

Goオプション	説明(Description)
`-gotags <go_build_tags>`	Goプロジェクトのカスタムビルドタグのカンマ区切りリストを指定します。これは、`go` コマンドの `-tags` オプションに相当します。詳細については、「カスタムGoビルドタグを含める」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.gotags`

`-gopath <dir>`	Goプロジェクトの変換に使用するGOPATH環境変数の値を指定します。このオプションを指定しない場合、Fortify SASTではGOPATHシステム環境変数の既存の値が使用されます。
	gopathディレクトリは絶対パスとして指定する必要があります。次の例は、`<dir>` に有効な値です。
	`/home/projects/go_workspace/my_proj`
	`C:¥projects¥go_workspace¥my_proj`
	次の例は、`<dir>` に無効な値です。
	`go_workspace/my_proj`
	このオプションとGOPATHシステム環境変数が設定されていない場合、gopathのデフォルトは、ユーザのホームディレクトリにある `go` という名前のサブディレクトリです(Linuxの場合は `$HOME/go`、Windowsの場合は `%USERPROFILE%\go`)。ただし、そのディレクトリにGoディストリビューションが含まれている場合を除きます。
	モジュールを使用する場合、GOPATH環境変数でパッケージのインポートを解決する必要はありません。ただし、不足しているモジュールの依存関係をダウンロードするときに使用する出力ディレクトリは、引き続きGOPATHによって決定されます。
	Note
	Fortify SASTでは、パッケージのインポートを解決するためにGOPATH環境変数のみに依存する古いGoプロジェクトを完全にはサポートしていません。
	同等のプロパティ名:
	`com.fortify.sca.GOPATH`

Goオプション	説明(Description)
`-goroot <dir>`	Goインストールの場所を指定します。このオプションを指定しない場合は、GOROOTシステム環境変数が使用されます。 このオプションが指定されず、GOROOTシステム環境変数が設定されていない場合、Fortify SASTではFortify SASTインストールに含まれるGoコンパイラを使用します。 **同等のプロパティ名:** `com.fortify.sca.GOROOT`
`-goproxy <url>`	1つ以上のプロキシURLをカンマ区切りで指定します。また、`direct`または`off`(ネットワークの使用を無効化)を指定することもできます。 このオプションが指定されず、GOPROXYシステム環境変数が設定されていない場合、Fortify SASTは`https://proxy.golang.org,direct`を使用します。 **同等のプロパティ名:** `com.fortify.sca.GOPROXY`

Goのプロパティ

20.3. カスタムGoビルドタグを含める

Goプロジェクトにカスタムビルドタグを必要とするファイルが含まれる場合には、`-gotags`オプションを使用して、これらのビルドタグをFortify SAST変換に含めることができます。例:

```
sourceanalyzer -b MyProject -gotags release "src/**/*.go"
```

Fortify SAST `-gotags`オプションでは、オペレーティングシステム、アーキテクチャ、またはGoバージョン(`//go:build linux`、`//go:build arm`、`//go:build go1.21`など)の自動ビルドタグの上書きを許可しません。Goプロジェクトを別のオペレーティングシステムまたはアーキテクチャ向けに変換するには、GOOSおよびGOARCH環境変数で適切なクロスコンパイルターゲットを設定します。特定のGoバージョンを設定するには、GOROOT環境変数または`-goroot`オプションで、Go SDKバージョンのパスを指定します。

20.4. 依存関係の解決

Fortify SASTでは、Goに組み込む2つの依存関係管理システムをサポートしています。

- モジュール
  モジュールを使用するGoプロジェクトを変換するには、必要な依存関係を指定する`go.mod`ファイルと、ダウンロードした依存関係を検証するための対応する`go.sum`ファイルを、プロジェクトに含める必要があります。
  sourceanalyzerコマンドで、`go.mod`ファイルを含むディレクトリをプロジェクトルートとして指定します。
  Fortify SASTでは、ネイティブのGoツールチェーンを使用して必要なすべての依存関係をダウンロードします。
  Fortify SASTを実行するコンピュータでインターネットへのアクセスが制限されている場合は、次のいずれかを実行します。
  - Artifactoryなどのアーティファクト管理システムを使用している場合には、GOPROXY環境変数を設定するか、「Goコマンドラインオプション」で説明されている`-goproxy`オプションを使用します。
  - モジュールとベンダを使用して、必要なすべての依存関係をダウンロードします。
    手動ベンダを使用する場合には、変換を開始する前に、GOFLAGS環境変数を`-mod=vendor`に設定します。
- GOPATHの依存関係の解決
  depなどのサードパーティの依存関係管理システムを使用している場合は、変換を開始する前に、すべての依存関係をダウンロードする必要があります。

GOPATH開発モードでは、ローカルファイルシステム上の絶対パスを使用して依存関係を識別します。この場合、異なるサブディレクトリや異なるマシンからのスキャンを相互に関連付けるときに問題が発生する可能性があります。詳細については、「Goコマンドライン構文」を参照してください。

21. PHPコードの分析

`MyPHP.php` という名前の単一のPHPファイルを変換する構文を次の例に示します。

```
sourceanalyzer -b <build_id> MyPHP.php
```

ソースまたは `php.ini` ファイルエントリに相対パス名が含まれる(`./` または `../` で始まる)ファイルを変換するには、次の例に示すようにPHPソースルートを設定します。

```
sourceanalyzer -php-source-root <path> -b <build_id> MyPHP.php
```

`-php-source-root` オプションの詳細については、「PHPコマンドラインオプション」の説明を参照してください。

PHPコードを変換する場合は、すべてのソースファイルを1回の呼び出しで一緒に指定してください。Fortify SASTでは、後続の呼び出し時にビルドIDで関連付けられたファイルリストに新しいファイルを追加する機能はサポートされていません。

- PHPコマンドラインオプション

21.1. PHPコマンドラインオプション

次の表では、PHP固有のコマンドラインオプションについて説明します。

PHPオプション	説明(Description)
`-php-source-root <path>`	プロジェクトルートディレクトリへの絶対パスを指定します。相対パス名は最初にカレントディレクトリから展開されます。ファイルが見つからない場合は、指定したPHPソースルートディレクトリからパスが展開されます。 **同等のプロパティ名:** `com.fortify.sca.PHPSourceRoot`
`-php-version <version>`	PHPのバージョンを指定します。デフォルトのバージョンは8.2です。有効なバージョンのリストについては、「サポートされる言語」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.PHPVersion`

22. Perlコードの分析

このセクションでは、Perlプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Perl分析の前提条件
- Perlの変換構文

22.1. Perl分析の前提条件

現在、PerlコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Perlコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

22.2. Perlの変換構文

AIを活用したSASTを使用して分析対象にPerlコードを含めるには、分析対象のすべてのソースファイルを含めます。

Perlコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.pl"
```

Important

Perlソースファイルでサポートされているファイル拡張子は `.pl` と `.pm` です。

23. Rubyコードの分析

このセクションでは、Rubyコードを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

- Rubyの変換構文

23.1. Rubyの変換構文

RubyはAIを活用したSASTにのみ対応しています。

Note

AIを活用したSASTが構成されていない場合、Rubyコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

AIを活用したSASTを使用してRubyコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id> <files> | <file_specifiers>
```

たとえば、ファイルを個別に指定します。

```
sourceanalyzer -b <build_id> file1.rb file2.rb file3.erb
```

ワイルドカードやディレクトリを使用して、複数のファイルをより簡単に指定することもできます。

```
sourceanalyzer -b <build_id> "src/**/*.rb" "templates/
```

AIを活用したSASTのスキャンの構成に関する詳細については、以下のトピックを参照してください。

- AIを活用したSASTの要件
- AIを活用したSASTによる分析

24. Adaコードの分析

このセクションでは、Adaプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Ada分析の前提条件
- Adaの変換構文

24.1. Ada分析の前提条件

現在、AdaコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Adaコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

24.2. Adaの変換構文

AIを活用したSASTを使用して分析対象にAdaコードを含めるには、分析対象のすべてのソースファイルを含めます。

Adaコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.ada"
```

Important

Adaソースファイルでサポートされているファイル拡張子は `.ada` 、 `.adb` 、 `.ads` です。

25. Delphiコードの分析

このセクションでは、Delphiプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Delphi分析の前提条件
- Delphiの変換構文

25.1. Delphi分析の前提条件

現在、DelphiコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Delphiコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

25.2. Delphiの変換構文

AIを活用したSASTを使用して分析対象にDelphiコードを含めるには、分析対象のすべてのソースファイルを含めます。

Delphiコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.pas"
```

Important
Delphiソースファイルでサポートされているファイル拡張子は `.pas` 、 `.dpr` 、 `.dpk` です。

26. Elixirコードの分析

このセクションでは、Elixirプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Elixir分析の前提条件
- Elixirの変換構文

26.1. Elixir分析の前提条件

現在、ElixirコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Elixirコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

26.2. Elixirの変換構文

AIを活用したSASTを使用して分析対象にElixirコードを含めるには、分析対象のすべてのソースファイルを含めます。

Elixirコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.ex"
```

Important
Elixirソースファイルでサポートされているファイル拡張子は `.ex` と `.exs` です。

27. Erlangコードの分析

このセクションでは、Erlangプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Erlang分析の前提条件
- Erlangの変換構文

27.1. Erlang分析の前提条件

現在、ErlangコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Erlangコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

27.2. Erlangの変換構文

AIを活用したSASTを使用して分析対象にErlangコードを含めるには、分析対象のすべてのソースファイルを含めます。

Erlangコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。



Example

```
sourceanalyzer -b <build_id> "**/*.erl"
```



Important

Erlangソースファイルでサポートされているファイル拡張子は `.erl` と `.hrl` です。

28. Luaコードの分析

このセクションでは、Luaプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Lua分析の前提条件
- Luaの変換構文

28.1. Lua分析の前提条件

現在、LuaコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Luaコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

28.2. Luaの変換構文

AIを活用したSASTを使用して分析対象にLuaコードを含めるには、分析対象のすべてのソースファイルを含めます。

Luaコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。



Example

```
sourceanalyzer -b <build_id> "**/*.lua"
```

29. Kornshellコードの分析

このセクションでは、Kornshellプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Kornshell分析の前提条件
- Kornshellの変換構文

29.1. Kornshell分析の前提条件

現在、KornshellコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Kornshellコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

29.2. Kornshellの変換構文

AIを活用したSASTを使用して分析対象にKornshellコードを含めるには、分析対象のすべてのソースファイルを含めます。

Bashコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id> <files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。



Example

```
sourceanalyzer -b <build_id> "**/*.ksh"
```

30. Salesforce ApexおよびVisualforceコードの分析

- ApexおよびVisualforce変換の前提条件
- ApexおよびVisualforceのコマンドライン構文

30.1. ApexおよびVisualforce変換の前提条件

ApexプロジェクトやVisualforceプロジェクトを変換するには、スキャンするすべてのソースコードが、Fortify SASTをインストールしたのと同じマシン上で使用可能である必要があります。

カスタムSalesforce®istered trademark;アプリをスキャンするには、そのアプリを開発して展開したSalesforce組織(org)からローカルコンピュータにダウンロードします。ダウンロードしたアプリは次の要素で構成されています。

- `.cls` 拡張子を持つファイル内のApexクラス
- `.page` 拡張子を持つファイル内のVisualforce Webページ
- `.trigger` 拡張子を持つファイルに含まれている、データベースの「trigger」関数と呼ばれるApexコードファイル
- `.component` 拡張子を持つファイル内のVisualforceコンポーネントファイル
- `.object` 拡張子を持つファイル内のオブジェクト

Salesforce Webサイトで入手できるAnt移行ツールを使用して、Salesforceクラウド内の組織からローカルコンピュータにアプリをダウンロードします。プロジェクトマニフェストファイルが、`build.xml` ファイル内の指定したターゲットに対して正しく設定されていることを確認します。たとえば、次の `package.xml` マニフェストファイルは、Fortify SASTに、すべてのクラス、カスタムオブジェクト、ページ、およびコンポーネントを提供します。

```
<?xml version="1.0" encoding="UTF-8"?> <Package xmlns=http://soap.sforce.com/2006/04/metadata> <types>
<members>*</members> <name>ApexClass</name> </types> <types> <members>*</members>
<name>ApexTrigger</name> </types> <types> <members>*</members> <name>ApexPage</name> </types> <types>
<members>*</members> <name>ApexComponent</name> </types> <types> <members>*</members>
<name>CustomObject</name> </types> <version>55.0</version> </Package>
```

Ant移行ツールのドキュメントを使用して、取得ターゲットを設定します。AppExchangeのアプリを組織で使用している場合、それらのアプリはパッケージ化されたターゲットとしてダウンロードされる必要があります。

30.2. ApexおよびVisualforceのコマンドライン構文

ApexおよびVisualforceのコードを変換する基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id> <files>
```

ここで、 *<files>* はApexまたはVisualforceのファイルまたはソースファイルへのパスです。

Important

ソースファイルでサポートされているファイル拡張子は、 .cls 、 .component 、 .trigger 、 .object 、および .page です。

31. ABAPコードの分析

ABAPコード変換では、SAP®istered trademark;データベースからコードを抽出してスキャン用に準備するための追加の準備手順が必要です。詳しくは、移送依頼のインポートを参照してください。このセクションは、SAPとABAPの基本を理解していることを前提としています。

- ソースファイルのダウンロードについて
- 移送依頼のインポート
- Fortify SASTのお気に入りリストへの追加
- Fortify ABAP Extractorの実行
- Fortify ABAP Extractorのアンインストール

31.1. ソースファイルのダウンロードについて

ABAPコードを変換するために、Fortify ABAP Extractorプログラムはソースファイルをプレゼンテーションサーバにダウンロードし、必要に応じてFortify SASTを開始します。 ファイルをローカルシステムにダウンロードしてオペレーティングシステムのコマンドを実行するには、アクセス許可を持つアカウントを使用する必要があります。

Extractorプログラムはオンラインで実行されるため、抽出するために選択されたソースファイルのボリュームが許容されるプロセス実行時間を超えた場合は、 max dialog work process time reached メッセージを受信することがあります。これを回避するには、大規模なプロジェクトを連続する小さいExtractorタスクとしてダウンロードします。 たとえば、プロジェクトが4つの異なるパッケージで構成されている場合、各パッケージを同じプロジェクトディレクトリに個別にダウンロードします。 例外が頻繁に発生する場合は、SAP Basis管理者と協力して最大時間制限(rdisp/max_wprun_time)を大きくします。

ABAPからパッケージが抽出されたら、Fortify ABAP Extractorは TDEVC からパッケージ名と一致する parentcl フィールドを持つすべてを抽出します。次に、 TDEVC から抽出したものと同じ parentcl フィールドを持つ残りのすべてを TDEVC から再帰的に抽出します TDEVC から抽出されるフィールドは<code>devclass</code>です。 TDEVC から抽出されるフィールドは devclass です。

devclass の値はプログラム名のセットとして扱われ、指定できるプログラム名と同様に処理されます。

TRDIR からプログラムを抽出するには、名前フィールドを次のいずれかと比較します。

- 選択画面で指定したプログラム名
- TDEVC から抽出された値のリスト(パッケージが提供された場合)

TRDIR の行は名前フィールドに指定したプログラム名を含む行であり、式 LIKE programname を使用して行が抽出されます。

この最終的な名前のリストを READ REPORT で使用して、SAPシステムからコードを取得します。このメソッドは、レコードに対して単に REPORTS だけでなく、クラスとメソッドも読み込みます。

READ REPORT を呼び出すたびに、ローカルシステムの一時フォルダにファイルが作成されます。Fortify SASTは、この一連のファイルを変換およびスキャンしてFPRファイルを作成します。FPRファイルは、Fortify Audit Workbenchを使用して開きます。

ABAPのプロパティ

31.1.1. INCLUDEの処理

ソースコードがダウンロードされると、Fortify ABAP Extractorはソース内の INCLUDE ステートメントを検出します。検出すると、分析のためにincludeのターゲットをローカルコンピュータにダウンロードします。

31.2. 移送依頼のインポート

ABAPコードをスキャンするには、Fortify ABAP Extractorの移送依頼をSAPサーバにインポートする必要があります。移送依頼は *<sast_install_dir>*/Tools/SAP_Extractor.zip にあります。

Fortify ABAP Extractorのパッケージ(SAP_Extractor.zip)には次のファイルが含まれています。

- K900*<release_number>*.*<system_id>*
- R900*<release_number>*.*<system_id>*

これらのファイルが、ローカル移送ドメインの外部からSAPシステムにインポートする必要があるSAP移送依頼の構成要素です。SAP管理者または移送依頼をシステムにインストールする権限を持つ個人に、移送依頼をインポートしてもらってください。これらのファイルには、プログラム、トランザクション(YSCA)、およびプログラムユーザインタフェースが含まれています。これらをシステムにインポートした後、SAPデータベースからコードを抽出してFortify SASTスキャン用のコードを作成できます。

インストールに関する注意事項

移送依頼のインポートエラー(Install release does not match the current version)が発生した場合には、移送依頼のインストールが失敗しました。サポートされているABAPバージョンについては、「ソフトウェア要件」を参照してください。

この問題を解決するには、次の手順を実行します。

1. 移送依頼のインポートを再実行します。
   ［Import Transport Request］ダイアログボックスが開きます。
2. ［**Options**］タブを選択します。
3. ［**Ignore Invalid Component Version**］チェックボックスをオンにます。
4. インポート手順を完了します。

それでも問題が解決しない場合や、異なるテーブル構造を持つSAPバージョンがシステムで実行されている場合には、Fortify SASTがABAPコードをスキャンできるように、独自の技術を使用してABAPファイル構造をエクスポートすることをお勧めします。

31.3. Fortify SASTのお気に入りリストへの追加

Fortify SASTのお気に入りリストへの追加はオプションですが、追加すると、Fortify SASTスキャンにすばやくアクセスしてスキャンを開始できます。次の手順では、日常業務でユーザメニューを使用すると仮定しています。別のメニューから作業を行う場合は、使用するメニューにお気に入りリンクを追加します。Fortify SASTのエントリを作成する前に、SAPサーバが実行中であり、WebベースのクライアントのSAP Easy Accessエリアにアクセスしていることを確認してください。

Fortify SASTをお気に入りリストに追加するには、次の手順を実行します。

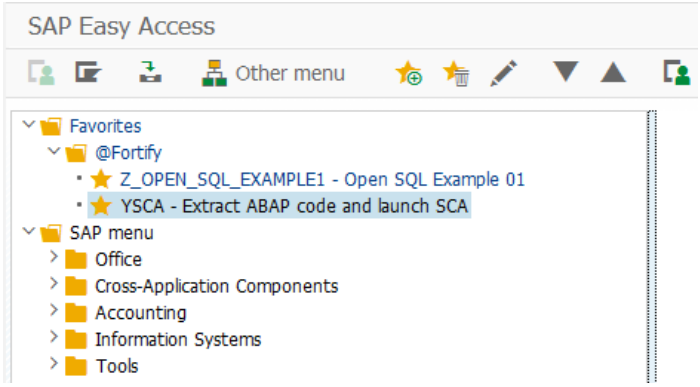
1. ［**SAP Easy Access**］メニューから、トランザクションボックスに「 S000 」と入力します。
   ［**SAP Menu**］が開きます。
2. ［**Favorites**］フォルダを右クリックし、［**Insert transaction**］を選択します。
   ［**Manual entry of a transaction**］ダイアログボックスが開きます。
3. ［**トランザクションコード(Transaction Code)**］ボックスに「 YSCA 」と入力します。

4. 緑色のチェックマークアイコンをクリックします。
［お気に入り(Favorites)］リストに［ABAPコードを抽出してSCAを起動する(Extract ABAP code and launch SCA)］という項目が表示されます。
5. ［ABAPコードを抽出してSCAを起動する(Extract ABAP code and launch SCA)］リンクをクリックしてFortify ABAP Extractorを開始します。

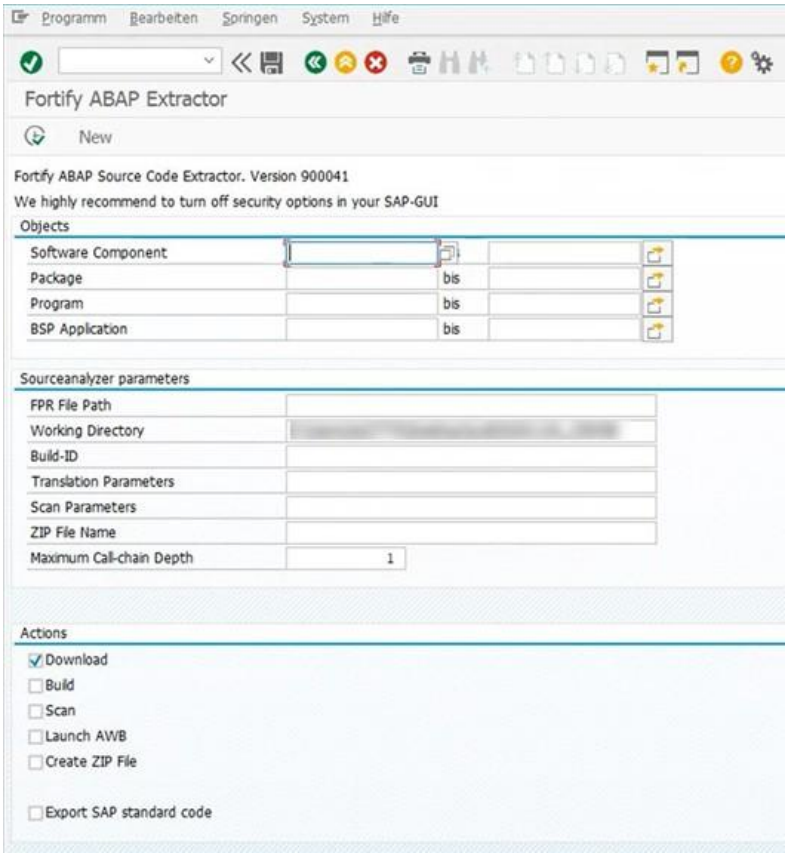
31.4. Fortify ABAP Extractorの実行

Fortify ABAP Extractorを実行するには、次の手順を実行します。

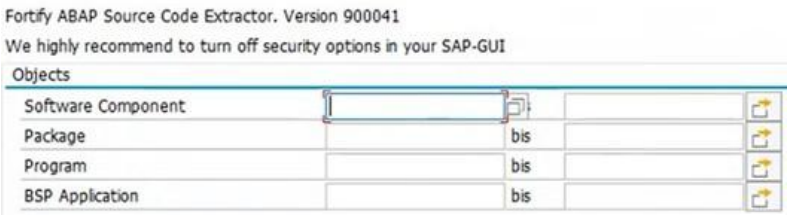
1. ［**お気に入り(Favorites)**］リンクまたはトランザクションコードからFortify ABAP Extractorを起動するか、手動でExtractorオブジェクトを起動します。



これにより、Fortify ABAP Extractorが開きます。

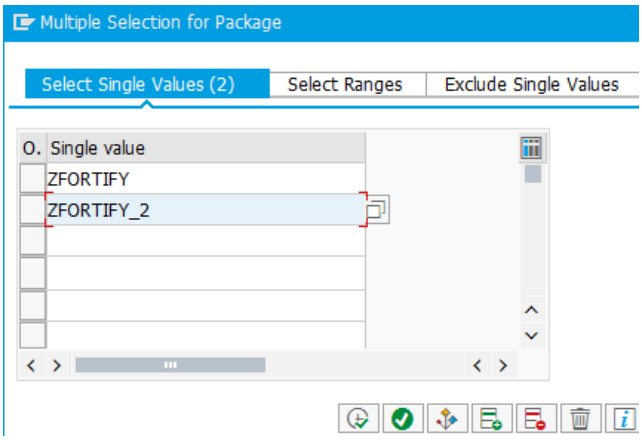


2. ダウンロードするコードを選択します。
スキャンするソフトウェアコンポーネント、パッケージ、プログラム、またはBSPアプリケーションの範囲を開始名と終了名で指定します。



Note

複数のオブジェクトまたは範囲を指定できます。



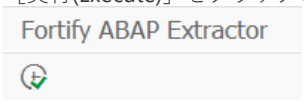
3. 次の表に示すFortify　SAST固有のパラメータを指定します。

フィールド	説明(Description)
FPR File Path	(オプション)スキャン結果ファイル(FPR)を保存するディレクトリを入力または選択します。FPRファイルの名前をパス名に含めてください。抽出プロセスを実行している同じコンピュータにダウンロードしたコードを自動的にスキャンするには、FPRファイルパスを指定する必要があります。
作業ディレクトリ(Working Directory)	抽出したソースコードを保存するディレクトリを入力または選択します。
Build-ID	(オプション)スキャンのビルドIDを入力します。Fortify SASTでは変換されたソースコードを識別するためにビルドIDを使用します。これはコードをスキャンするために必要です。抽出プロセスを実行している同じコンピュータにダウンロードしたコードを自動的に変換するには、ビルドIDを指定する必要があります。
変換パラメータ(Translation Parameters)	(オプション)追加のFortify SASTコマンドライン変換オプションを入力します。抽出プロセスを実行している同じコンピュータにダウンロードしたコードを自動的に変換したり、変換オプションをカスタマイズしたりするには、変換オプションを指定する必要がありま す。
スキャンパラメータ(Scan Parameters)	(オプション)Fortify SASTコマンドラインスキャンオプションを入力します。抽出プロセスを実行している同じコンピュータにダウンロードしたコードを自動的にスキャンしたり、スキャンオプションをカスタマイズしたりするには、スキャンオプションを指定する必要があります。
ZIPファイル名(ZIP File Name)	(オプション)圧縮パッケージで出力する場合は、ZIPファイル名を入力します。
Maximum Call-chain Depth	グローバルSAP関数Fは、Fが明示的に選択されていない限り、または明示的に選択されたコードで始まる関数呼び出しのチェーンを介してFに到達可能で、そのチェーンの長さがこの数以下である場合を除き、ダウンロードされません。カスタマサポートの指示がない限り、2より大きい値を指定しないことを推奨します。

4. 次の表に示すアクション情報を指定します。

フィールド	説明(Description)
Download	SAPデータベースから抽出したソースコードをFortify SASTでダウンロードするには、［ダウンロード(Download)］チェックボックスをオンにします。
ビルド(Build)	Fortify SASTでダウンロード済みのすべてのABAPコードを変換し、指定したビルドIDを使用してそのコードを保存するには、［ビルド(Build)］チェックボックスをオンにします。このアクションを実行するには、Fortify ABAP Extractorを実行しているコンピュータにFortify SASTのインストール済みバージョンが必要です。多くの場合、Fortify SASTがインストールされているシステムにダウンロードしたソースコードを移動する方が簡単です。
スキャン(Scan)	指定したビルドIDのスキャンをFortify SASTで実行するには、［スキャン(Scan)］チェックボックスをオンにします。このアクションでは、変換(ビルド)アクションが以前に実行されている必要があります。このアクションを実行するには、Fortify ABAP Extractorを実行しているコンピュータにFortify SASTのインストール済みバージョンが必要です。多くの場合、ダウンロードしたソースコードを事前定義されたFortify SASTコンピュータに移動する方が簡単です。
Launch AWB	Fortify Audit Workbenchを起動して指定したFPRファイルを開くには、［AWBの起動(Launch AWB)］チェックボックスをオンにします。
ZIPファイルの作成(Create ZIP File)	出力を圧縮するには、［ZIPファイルの作成(Create ZIP File)］チェックボックスをオンにします。また、ソースコードをSAPデータベースから抽出した後で、出力を手動で圧縮することもできます。
Export SAP standard code	カスタムコードに加えてSAP標準コードもエクスポートするには、［SAP標準コードのエクスポート(Export SAP standard code)］チェックボックスをオンにします。

5. ［実行(Execute)］をクリックします。



31.5. Fortify ABAP Extractorのアンインストール

ABAP　Extractorをアンインストールするには、次の手順を実行します。

1. ABAP Workbenchで、Object Navigatorを開きます。
2. Y_FORTIFY_ABAPパッケージを選択します。
3. ［**Programs**］タブを展開します。
4. 次の要素を右クリックして、［**Delete**］を選択します。
    - プログラム: Y_FORTIFY_SCA

32. COBOLコードの分析

COBOLは、AIを活用したSASTまたは従来型のSASTを使用してスキャンできます。AIを活用したSASTとデータベース接続が指定されていない場合、Fortify SASTではCOBOLソースファイルのローカル分析を実行する状態に自動的に戻ります。

> **Note**
>
> AIを活用したSASTは単一ファイルの解析であり、LLMベースの解析とはその他の点で異なるため、AIを活用したSASTでスキャンした場合、従来のローカルスキャンと同じ結果が得られない可能性があります。

他のファイルに対してAIを活用したSASTを有効にしていて、COBOLソースファイルのローカル分析も引き続き確実に実行されるようにするには、変換フェーズと分析フェーズの両方で次のプロパティが設定されていることを確認する必要があります。

```
com.fortify.sca.cobol.legacy.enabled=true
```

ローカルのトラディショナルSASTでは、COBOL翻訳を使用して最新のCOBOL方言をサポートします。プラットフォームを問わず使用できるものの、対応している方言が少ない、従来のローカルSASTレガシーCOBOL変換（「レガシーCOBOL変換の使用」を参照）も用意しています。

COBOLコードの変換でサポートされている技術のリストについては、「サポートされる言語」を参照してください。Fortify SASTは、現時点ではCOBOLアプリケーションのカスタムルールをサポートしていません。

32.1. COBOLソースファイルとコピーブックファイルの変換準備

COBOLプログラムを分析する前に、Fortify SASTを実行するシステムに次のプログラムコンポーネントをコピーします。

- COBOLソースコード
  COBOLソースコードファイルには、拡張子 `.CBL` 、 `.cbl` 、 `.COB` 、または `.cob` を使用することを強く推奨しています。ソースコードファイルに拡張子がないか、拡張子が標準以外のものである場合は、「ファイル拡張子を持たないCOBOLソースファイルの変換」および「任意のファイル拡張子を持つCOBOLソースファイルの変換」の手順に従う必要があります。
- COBOLソースコードで使用しているすべてのコピーブックファイル
  これには、COBOLソースコードで参照するすべてのSQL INCLUDEファイル(SQL INCLUDEファイルは技術的にはコピーブックファイル)が含まれます。

  > **Important**
  >
  > ローカル分析の場合、コピーブックファイルには拡張子 `.CPY` または `.cpy` を使用する必要があります。AIを活用したSASTを使用する場合、コピーブックファイルでは拡張子 `.copy` 、 `.cobcopy` 、 `.copybook` も使用できます。

  COBOLソースコードに次が含まれている場合:

  ```
  COPY FOO
  ```

  または

  ```
  EXEC SQL INCLUDE FOO END-EXEC
  ```

  `FOO` はCOBOLコピーブックの名前で、対応するコピーブックファイルは名前が `FOO.cpy` または `FOO.CPY` になります。

ローカル分析を使用する場合、COBOLソースコードファイルを `sources` という名前のディレクトリに、コピーブックファイルを `copybooks` という名前のディレクトリに配置することをOpenTextでは推奨しています。これらのディレクトリは同じレベルで作成してください。

32.2. COBOLのコマンドライン構文

AIを活用したSAST

AIを活用したSASTを使用してCOBOLコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer –b <build_id><path>
```

AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

ローカル変換(非推奨)

1つのCOBOLソースコードファイルを変換するために使用される基本的な構文は次のとおりです。

```
sourceanalyzer -b <build_id><path>
```

変換されたCOBOLプログラムをスキャンして、分析結果をFPRファイルに保存するために使用される基本的な構文は次のとおりです。

```
sourceanalyzer -b <build_id> -scan -f <results>.fpr
```

詳細については、「ファイルとディレクトリの指定」を参照してください。

32.2.1. ファイル拡張子を持たないCOBOLソースファイルの変換

メインフレームからCOBOLソースファイル(コピーブックファイルではなく)を取得し、これに `.COB` や `.CBL` のファイル拡張子がない場合(COBOLファイル名としては一般的です)、変換コマンドラインに次の項目を含める必要があります。

```
-noextension-type  COBOL
```

次のコマンドの例では、ファイル拡張子を持たないCOBOLソースコードを変換します。

```
sourceanalyzer –b MyProject –noextension-type COBOL –copydirs copybooks sources
```

32.2.2. 任意のファイル拡張子を持つCOBOLソースファイルの変換

任意の拡張子(`.xyz`)を持つCOBOLソースファイルがある場合は、変換コマンドラインに次の項目を含める必要があります。

```
-Dcom.fortify.sca.fileextensions.xyz=COBOL
```

ファイルまたはディレクトリ指定子を使用する場合は、式 `*.xyz` も含める必要があります(ファイルとディレクトリの指定を参照)。

32.2.3. COBOLコマンドラインオプション

次の表では、COBOLコマンドラインオプションについて説明します。レガシーCOBOL変換を使用するには、「レガシーCOBOL変換コマンドラインオプション」を参照してください。

COBOLオプション	説明(Description)
-copydirs <dirs>	Fortify SASTでコピーブックファイルを検索する、1つ以上のディレクトリをセミコロン区切りで指定します。 **Note** このオプションでは、ワイルドカードは使用できません。 **同等のプロパティ名:** com.fortify.sca.CobolCopyDirs

32.3. レガシーCOBOL変換の使用(非推奨)

次のいずれかの条件に当てはまる場合は、レガシーCOBOL変換を使用してください。

- Windows以外のオペレーティングシステムでFortify　SASTを実行している。
  サポートされているWindows以外のプラットフォームおよびアーキテクチャについては、「プラットフォームとアーキテクチャ」を参照してください。
- 使用しているCOBOL方言が、デフォルトのCOBOL変換でサポートされているものとは異なる (「COBOLコマンドラインオプション」の -dialect オプションを参照)。

「COBOLソースファイルとコピーブックファイルの変換準備」の説明に従ってCOBOLソースコードファイルとコピーブックファイルを準備し、「COBOLのコマンドライン構文」で説明されているコマンドライン構文を使用します。レガシー COBOL変換では、ファイル拡張子の有無に関係なく、コピーブックファイルを受け入れることにご注意ください。コピーブックファイルにファイル拡張子がある場合は、 -copy-extensions コマンドラインオプションを使用します (「レガシー COBOL変換コマンドラインオプション」を参照)。

32.3.1. レガシーCOBOL変換コマンドラインオプション

次の表では、レガシーCOBOL変換のコマンドラインオプションについて説明します。

レガシーCOBOLオプション	説明(Description)
`-cobol-legacy`	レガシーCOBOL変換を使用したCOBOLコードの変換を指定します。このオプションは、レガシーCOBOL変換を有効にする場合に必要です。 **同等のプロパティ名:** `com.fortify.sca.CobolLegacy`
`-copydirs <dirs>`	Fortify SASTでコピーブックファイルを検索する、1つ以上のディレクトリをセミコロン区切りまたはコロン区切りで指定します。 **同等のプロパティ名:** `com.fortify.sca.CobolCopyDirs`
`-copy-extensions <ext>`	1つ以上のコピーブックファイル拡張子をセミコロン区切りまたはコロン区切りで指定します。 **同等のプロパティ名:** `com.fortify.sca.CobolCopyExtensions`
`-fixed-format`	すべてのコード行のカラム8〜72の間のソースコードのみを検索するようFortify SASTに指示する、固定形式のCOBOLを指定します。デフォルトはフリーフォーマットです。 IBM®istered trademark; Enterprise COBOLコードは通常、固定形式です。以下の場合は、`-fixed-format`オプションが必要になる可能性があります。 • COBOL変換が無期限にハングする可能性がある • Fortify SASTによりCOBOL変換で多数の解析エラーが報告される **同等のプロパティ名:** `com.fortify.sca.CobolFixedFormat`

33. SQLの分析

Windows (および.NETプロジェクトの場合に限り、Linuxも)のFortify SASTでは、`.sql`拡張子を持つファイルはPL/SQLではなくT-SQLであることを前提とします。Windowsで`.sql`拡張子を持つPL/SQLファイルを使用する場合は、PL/SQLとして扱われるようにFortify SASTを設定する必要があります。

PL/SQLを変換およびスキャンするための基本的な構文は次のとおりです。

```
sourceanalyzer -b <build_id> -sql-language PL/SQL <files> sourceanalyzer -b <build_id> -sql-language PL/SQL -scan -f <results>.fpr
```

または、`.sql`拡張子を持つファイルのデフォルトの動作を変更できます。`fortify-sca.properties`ファイルで、`com.fortify.sca.fileextensions.sql`プロパティを`PLSQL`に設定します。

T-SQLを変換およびスキャンするための基本的な構文は次のとおりです。

```
sourceanalyzer -b <build_id> -sql-language TSQL <files> sourceanalyzer -b <build_id> -scan -f <results>.fpr
```

33.1. PL/SQLのコマンドライン例

次のコマンド例では、2つのPL/SQLファイルを変換してスキャンします。

```
sourceanalyzer -b MyProject -sql-language PL/SQL x.pks y.pks sourceanalyzer -b MyProject -sql-language PL/SQL -scan -f MyResults.fpr
```

次のコマンド例では、 `sources` ディレクトリ内のすべてのPL/SQLファイルを変換してスキャンします。

```
sourceanalyzer -b MyProject -sql-language PL/SQL "sources/**/*.pks" sourceanalyzer -b MyProject -sql-language PL/SQL -scan -f MyResults.fpr
```

33.2. T-SQLのコマンドライン例

次の例では、2つのT-SQLファイルを変換します。

```
sourceanalyzer -b MyProject x.sql y.sql
```

次の例では、 `sources` ディレクトリ内のすべてのT-SQLファイルを変換します。

```
sourceanalyzer -b MyProject "sources¥**¥*.sql"
```

Note

この例は、 `fortify-sca.properties` 内の `com.fortify.sca.fileextensions.sql` プロパティが、プロパティのデフォルト値である `TSQL` に設定されていることを想定しています。

34. コードとしてのインフラストラクチャ(IaC)の分析

Fortify SASTは、Azure Resource Manager (ARM)、Bicep、AWS CloudFormation、およびHCLテンプレートを理解します。

Note

HCLの分析サポートは、Terraformおよびサポートされるクラウドプロバイダのコードとしてのインフラストラクチャ(IaC)構成に固有のものです。

最適な結果を得るには、テンプレートファイルの展開が有効であることを確認してください。テンプレートには次が含まれていてはなりません。

- 静的であり、ローカルで検出可能な検証エラー(タイプエラーや未定義の変数または関数への参照など)。
- テンプレートの解釈中、ただしリソースが展開または変更される前に発生する、展開前エラー(無効な配列のインデックス付け操作など)。
- クラウドで発生する展開エラー(存在しないリソースの動的参照など)。

AWS CloudFormationのファイル名拡張子を `.json` 、 `.yaml` 、 `.template` 、または `.txt` にすることが推奨されています。 Fortify SASTでは、他の言語やファイルタイプでそれらの拡張子が一般的に使用されていない場合にのみ、他の拡張子をサポートしています(.java や .html など)。

デフォルトで、Fortify SASTでは、HCL拡張子 `.hcl` および `.tf` を持つファイルを変換します。

ARM変換コマンドラインの例

ARMテンプレートを変換する場合:

```
sourceanalyzer -b MyProject ArmTemplate.json
```

ディレクトリ内のすべてのARMテンプレートを変換する場合:

```
sourceanalyzer -b MyProject "src/**/*.json"
```

Bicep変換コマンドラインの例

1つのBicepテンプレートを変換する場合:

```
sourceanalyzer -b MyProject BicepTemplate.bicep
```

ディレクトリ内のすべてのBicepテンプレートを変換する場合:

```
sourceanalyzer -b MyProject "src/**/*.bicep"
```

Important
最適な結果を得るために、Bicepではスキャンマシン上でインターネット接続を行い、依存関係をダウンロードする必要があります。インターネットに接続せずにスキャンマシンを使用すると、最適な結果が得られない場合があります。

AWS CloudFormation変換コマンドラインの例

異なる拡張子を持つAWS CloudFormationテンプレートを変換する場合:

```
sourceanalyzer -b MyProject CFTemplateA.template CFTemplateB.yaml CFTemplateC.json CFTemplateD.customext
```

`.template` 拡張子を持つディレクトリ内のすべてのAWS CloudFormationテンプレートを変換する場合:

```
sourceanalyzer -b MyProject "src/**/*.template"
```

`.json` または `.yaml` の拡張子を持つディレクトリ内のすべてのAWS CloudFormationテンプレートを変換する場合:

```
sourceanalyzer -b MyProject "src/**/*.json" "src/**/*.yaml"
```

HCL変換コマンドラインの例

異なる拡張子を持つ2つのHCLテンプレートを変換する場合:

```
sourceanalyzer -b MyProject HCLTemplateA.hcl HCLTemplateB.tf
```

ディレクトリ内のすべてのHCLテンプレートを変換する場合:

```
sourceanalyzer -b MyProject "src/**/*.tf" "src/**/*.hcl"
```

Important
最適な結果を得るために、Terraformではスキャンマシン上でインターネット接続を行い、依存関係をダウンロードする必要があります。インターネットに接続せずにスキャンマシンを使用すると、最適な結果が得られない場合があります。

JSONの変換

YAMLの変換

35. JSONの分析

デフォルトで、Fortify SASTでは、JSON拡張子 `.json` を持つファイルをJSONとして変換します。次の例では、1つのJSONファイルを変換します。

```
sourceanalyzer -b MyProject x.json
```

次の例では、 `sources` ディレクトリ内のすべてのJSONファイルを変換します。

```
sourceanalyzer -b MyProject "sources/**/*.json"
```

36. YAMLの分析

デフォルトで、Fortify SASTでは、YAML拡張子 `.yaml` および `.yml` を持つファイルを変換します。次の例では、異なるファイル拡張子を持つ2つのYAMLファイルを変換します。

```
sourceanalyzer -b MyProject x.yaml y.yml
```

次の例では、 `sources` ディレクトリ内のすべてのYAMLファイルを変換します。

```
sourceanalyzer -b MyProject "sources/**/*.yaml" "sources/**/*.yml"
```

37. Dockerfileの分析

デフォルトでは、Fortify SASTは、ファイル名が `Dockerfile*` 、 `dockerfile*` 、 `*.Dockerfile` 、および `*.dockerfile` のいずれかの形式のファイルをDockerfileとして認識します。



Note

`com.fortify.sca.fileextensions` プロパティを使用して、Dockerfileを検出するために使用されるファイル名拡張子を変更できます。「変換と分析フェーズのプロパティ」を参照してください。

Fortify SASTでは、Dockerfile内のエスケープ文字としてバックスラッシュ(`\`)とバッククォート(`` ` ``)を受け付けます。Dockerfileでエスケープ文字が設定されていない場合、Fortify SASTではバックスラッシュがエスケープ文字と見なされます。

Dockerfileを含むディレクトリを変換する構文を次の例に示します。

```
sourceanalyzer -b <build_id> <dir>
```

Dockerfileの形式が正しくない場合、Fortify SASTはログファイルにエラーを書き込んでファイルを解析できないことを示し、そのDockerfileの分析をスキップします。ログに書き込まれるエラーの例を次に示します。

```
Unable to parse dockerfile ProjA.Dockerfile, error on Line 1:20: mismatched input '¥n' expecting
{LINE_EXTEND, WHITESPACE} Unable to parse config file
C:/Users/jsmith/MyProj/docker/dockerfile/ProjA.Dockerfile
```

38. Bashコードの分析

このセクションでは、Bashプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- Bash分析の前提条件

- Bashの変換構文

38.1. Bash分析の前提条件

現在、BashコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Bashコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

38.2. Bashの変換構文

AIを活用したSASTを使用して分析対象にBashコードを含めるには、分析対象のすべてのソースファイルを含めます。

Bashコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.sh"
```

Important

Bashソースファイルでサポートされているファイル拡張子は `.sh` と `.bash` です。

39. PowerShellコードの分析

このセクションでは、PowerShellプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- PowerShell分析の前提条件
- PowerShellの変換構文

39.1. PowerShell分析の前提条件

現在、PowerShellコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、PowerShellコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

39.2. PowerShellの変換構文

AIを活用したSASTを使用して分析対象にPowerShellコードを含めるには、分析対象のすべてのソースファイルを含めます。

PowerShellコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.ps1"
```

Important

PowerShellソースファイルでサポートされているファイル拡張子は `.ps1`、`.psm1`、`.psd1`、`.psd1xml` です。

40. Rコードの分析

このセクションでは、Rプロジェクトを分析する方法について説明します。他のファイルと組み合わせたプロジェクトについては、対応する言語の該当するセクションを参照してください。

このセクションでは、次のトピックについて説明します。

- R分析の前提条件
- Rの変換構文

40.1. R分析の前提条件

現在、RコードはAIを活用したSASTにのみ対応しています。AIを活用したSASTのスキャンの構成に関する詳細については、「AIを活用したSASTによる分析」を参照してください。

AIを活用したSASTが構成されていない場合、Rコードは正規表現分析でのみスキャンされ、ユーザーは不十分な結果しか得られない可能性があります。

40.2. Rの変換構文

AIを活用したSASTを使用して分析対象にRコードを含めるには、分析対象のすべてのソースファイルを含めます。

Rコードを分析するには、以下の基本的なコマンドライン構文を使用します。

```
sourceanalyzer -b <build_id><files> | <file_dir_specifiers>
```

詳細については「ファイルとディレクトリの指定」を参照してください。

Example

```
sourceanalyzer -b <build_id> "**/*.r"
```

Important

Rソースファイルでサポートされているファイル拡張子は `.r` と `.R` です。

41. Solidityコードの分析

Solidityコードを変換およびスキャンするための基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id><files> sourceanalyzer -b <build_id> -scan -f <results>.fpr
```

依存関係のインポート

Fortify SAST変換では、相対パスと絶対パスで指定したファイルのインポートステートメントのみがサポートされます。ライブラリのインポートステートメントはサポートされません。

コンパイラのバージョンの管理

Fortify SASTは、pragmaステートメントを使用してコード内で参照されているコンパイラを、Solidityコンパイラリポジトリからダウンロードします。デフォルトでは、Fortify SASTはSolidityコンパイラを ${flight.workdir}/solidity にダウンロードします。

ファイルにpragmaステートメントが含まれていない場合は、 ^0.8.0 の既定値が使用されます。分析で使用する別のデフォルトコンパイラバージョンを指定するには、コマンドラインに flight.solidity.defaultCompilerVersion プロパティを含めることができます。指定するバージョンは、Solidityコンパイラリポジトリに存在する必要があります。例:

```
sourceanalyzer -b MyProject ./ sourceanalyzer -b MyProject -scan -Dflight.solidity.defaultCompilerVersion=0.8.16 -f MyResults.fpr
```

Solidityコンパイラをダウンロードするための接続にプロキシが必要な場合は、 -Dhttps.proxyHost および -Dhttps.proxyPort を使用してプロキシ情報を含めてください。例:

```
sourceanalyzer -b MyProject ./ sourceanalyzer -b MyProject -scan -Dhttps.proxyHost=MyProxyHost -Dhttps.proxyPort=1234 -f MyResults.fpr
```

flight.solidity.defaultCompilerVersion は、 fortify-sca.properties ファイルに追加できます。

42. その他の言語および設定の分析

- FlexおよびActionScriptの分析
- ColdFusionコードの分析
- ASP/VBScript仮想ルートの分析
- Classic ASPのコマンドライン例
- VBScriptのコマンドライン例

42.1. FlexおよびActionScriptの分析

ActionScriptを変換するための基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id> -flex-libraries <libs> <files>
```

ここで:

<libs> は、セミコロンで区切られた(Windows)またはコロンで区切られた(Windows以外)「リンク」するライブラリ名のリストで、 *<files>* は変換するファイルです。

42.1.1. FlexおよびActionScriptコマンドラインオプション

Flexファイルを変換するには、次のコマンドラインオプションを使用します。この情報は、各説明に記載されているproperties環境設定ファイル(fortify-sca.properties)でも指定できます。

FlexおよびActionScriptオプション	説明(Description)
-flex-sdk-root <*dir*>	有効なFlex SDKのルートの場所を指定します。このディレクトリには、flex-config.xmlファイルを含むフレームワークフォルダが含まれている必要があります。MXMLC実行可能ファイルを含むbinフォルダも含まれている必要があります。 **同等のプロパティ名:** com.fortify.sca.FlexSdkRoot
-flex-libraries <*libs*>	リンクするライブラリ名をセミコロン区切り(Windows)またはコロン区切り(Windows以外)のリストで指定します。ほとんどの場合、このリストにはflex.swc、framework.swc、playerglobal.swc(通常、Flex SDKルートのframeworks/libs/にある)が含まれています。 **Note** SWCファイルまたはSWCファイルをFlexライブラリとして指定できます(SWZは現在サポートされていません)。 **同等のプロパティ名:** com.fortify.sca.FlexLibraries
-flex-source-roots <*dirs*>	MXMLソースが保存されているルートディレクトリをセミコロン区切り(Windows)またはコロン区切り(Windows以外)のリストで指定します。通常、これらにはcomという名前のサブフォルダが含まれます。 たとえば、指定されたFlexソースルートがfoo/bar/srcである場合、foo/bar/src/com/fortify/manager/util/Foo.mxmlはcom.fortify.manager.util.Fooという名前のオブジェクト(パッケージFoo内のcom.fortify.manager.utilという名前のオブジェクト)に変換されます。 **同等のプロパティ名:** com.fortify.sca.FlexSourceRoots

Note

-flex-sdk-rootおよび–flex-source-rootsオプションは主にMXML変換用であり、純粋なActionScriptをスキャンする場合は省略可能です。–flex-librariesはすべてのActionScriptリンク済みライブラリを解決するために使用します。

Fortify SASTではMXMLファイルをActionScriptに変換し、ActionScriptパーサを介して実行します。生成されたActionScriptは簡単に分析でき、Flexランタイムモデルのように厳密な正解を示すものではありません。その結果、MXMLファイルで解析エラーが発生する可能性があります。たとえば、XML解析が失敗し、ActionScriptへの変換が失敗し、結果の ActionScriptの解析も失敗する可能性があります。元のソースコードに対して明確な接続がないというエラーが発生した場合は、カスタマサポートまでお知らせください。

FlexおよびActionScriptのプロパティ

42.1.2. ActionScriptのコマンドライン例

次の例では、ActionScriptを変換するためのコマンドライン構文を示します。

例1

次の例は、1つのMXMLファイルと1つのMXMLライブラリ(MyLib.swf)のみを含む単純なアプリケーションの例です。

```
sourceanalyzer -b MyFlexApp -flex-libraries lib/MyLib.swf -flex-sdk-root /home/myself/flex-sdk/ -flex-source-roots . my/app/FlexApp.mxml
```

これにより、含めるライブラリの場所、Flex SDK、およびFlexソースルートの場所が識別されます。 /my/app/FlexApp.mxml にある1つのMXMLファイルは、 my.app という1つのActionScriptクラスとしてMXMLアプリケーションの変換になり、 FlexApp パッケージに入れられます。

例2

次の例は、ソースファイルが src ディレクトリに対して相対的であるアプリケーションの例です。1つのSWFライブラリ MyLib.swf と、Flex SDKのFlexライブラリとフレームワークライブラリを使用します。

```
sourceanalyzer -b MyFlexProject -flex-sdk-root /home/myself/flex-sdk/
-flex-source-roots src/ -flex-libraries lib/MyLib.swf "src/**/*.mxml" "src/**/*.as"
```

この例では、Flex SDKを見つけ、ファイル指定子を使用して、 .as ファイルと .mxml ファイルを src フォルダに含めます。この例では、 .SWC にある –flex-sdk-root ファイルを明示的に指定する必要はありません。ただし、この例では例示のために明示的に指定しています。Fortify SASTにより、指定したFlex SDKルート内にあるすべての .SWC ファイルが自動的に検索され、ActionScriptまたはMXMLファイルの変換に使用されるライブラリであると見なされます。

例3

この例では、Flex SDKルートとFlexライブラリがプロパティファイルで指定されています。これは、sourceanalyzerを実行するたびに情報を入力するのは時間がかかり、データが頻繁には変わらないためです。アプリケーションを2つのセクションに分割し、mainセクションフォルダとmodulesフォルダに保存します。各フォルダには、パスの起点になる src フォルダが含まれています。ファイル指定子には、両方の .mxml フォルダ内にあるすべての .as および src ファイルを選択するワイルドカードが含まれています。 main/src/com/foo/util/Foo.mxml 内の MXML ファイルは、たとえば次のようにソースルートを指定して、 com.foo.util パッケージ内の Foo という名前のActionScriptクラスとして変換されます。

```
sourceanalyzer -b MyFlexProject -flex-source-roots main/src:modules/src "./main/src/**/*.mxml" "./main/src/**/*.as" "./modules/src/**/*.mxml" "./modules/src/**/*.as"
```

42.1.3. 解決の警告の処理

変換中に生成されたすべての警告を表示するには、スキャンフェーズを開始する前に次のコマンドを入力します。

```
sourceanalyzer -b <build_id> -show-build-warnings
```

ActionScriptの警告

次のようなメッセージが表示される場合があります。

```
The ActionScript front end was unable to resolve the following imports: a.b at y.as:2. foo.bar at somewhere.as:5. a.b at foo.mxml:8.
```

このエラーは、Fortify SASTで必要なすべてのライブラリが見つからないときに発生します。Fortify SASTで分析を完了するために、(-flex-libraries オプションまたは com.fortify.sca.FlexLibraries プロパティを使用して)追加のSWCライブラリまたはSWC Flexライブラリを指定する必要がある場合があります。

42.2. ColdFusionコードの分析

CFMLページ内の未定義の変数を汚染されているものとして扱う場合は、 <*sast_install_dir*>/Core/config/fortify-sca.properties の次の行をコメント解除します。

```
#com.fortify.sca.CfmlUndefinedVariablesAreTainted=true
```

これは、register-globalsスタイルの脆弱性に注意するようにDataflow Analyzerに指示します。ただし、このプロパティを有効にすると、インクルードページ内の変数がそれ以前に発生したインクルードページの汚染された値に初期化されることがDataflow Analyzerで判明した場合に支障があります。

42.2.1. ColdFusionコマンドライン構文

ColdFusionソースコードを変換するための基本的なコマンドライン構文は次のとおりです。

```
sourceanalyzer -b <build_id> -source-base-dir <dir> <files> | <file_specifiers>
```

ここで:

- *<build_id>* プロジェクトのビルドIDを指定します
- *<dir>* Webアプリケーションのルートディレクトリを指定します
- *<files>* | *<file_specifiers>* はCFMLソースコードファイルを指定します
  <file_specifiers> の使用方法については、「ファイルの指定」を参照してください。



Note

Fortify SASTは、
-source-base-dirディレクトリを起点として各CFMLソースファイルの相対パスを計算します。Fortify SASTでは、インスタンスIDを生成するときに、これらの相対パスを使用します。アプリケーションソースツリー全体を別のディレクトリに移動する場合、 -source-base-dir オプションに適切なパラメータを指定すると、Fortify SASTで生成されるインスタンスIDは同じままです。

42.2.2. ColdFusion (CFML)コマンドラインオプション

次の表では、CFMLオプションについて説明します。

ColdFusionのオプション	説明(Description)
-source-base-dir *<web_app_root_dir>* *<files>* | *<file_specifiers>*	Webアプリケーションのルートディレクトリ。 **同等のプロパティ名:** com.fortify.sca.SourceBaseDir

ColdFusion (CFML)のプロパティ

42.3. ASP/VBScript仮想ルートの分析

Fortify SASTでは、ASP仮想ルートを処理できます。物理ディレクトリにマップするエイリアスとして仮想ディレクトリを使用するWebサーバの場合、Fortify SASTを使用するとエイリアスを使用できます。

たとえば、 Include および Library という名前の仮想ディレクトリがあり、それぞれ物理ディレクトリ C:\WebServer\CustomerOne\inc および C:\WebServer\CustomerTwo\Stuff を参照しているとします。

次の例では、*virtual*インクルードを使用するアプリケーションのASP/VBScriptコードを示しています。

```
<!--#include      virtual="Include/Task1/foo.inc"-->
```

この例で、前述のASPコードは次の物理的な場所にあるファイルを参照します。

```
C:¥Webserver¥CustomerOne¥inc¥Task1¥foo.inc
```

この例では、実際のディレクトリが仮想ディレクトリ名 Include に置き換わります。

仮想ルートへの対応

各仮想ディレクトリのマッピングをFortify SASTに提供するには、次の例に示すように、Fortify SASTコマンドライン呼び出しで com.fortify.sca.ASPVirtualRoots.name_of_virtual_directory プロパティを設定する必要があります。

```
sourceanalyzer -Dcom.fortify.sca.ASPVirtualRoots.<virtual_directory>=
<full_path_to_corresponding_physical_directory>
```



Note

Windowsでは、物理パスにスペースが含まれている場合は、プロパティ設定を引用符で囲む必要があります。

```
sourceanalyzer "-Dcom.fortify.sca.ASPVirtualRoots.<virtual_directory>=
<full_path_to_corresponding_physical_directory>"
```

前のセクションの例で展開するには、次のプロパティ値をFortify SASTに渡します。

```
-Dcom.fortify.sca.ASPVirtualRoots.Include="C:¥WebServer¥CustomerOne¥inc" -
Dcom.fortify.sca.ASPVirtualRoots.Library="C:¥WebServer¥CustomerTwo¥Stuff"
```

これにより、 Include は C:\WebServer\CustomerOne\inc に、 Library は C:\WebServer\CustomerTwo\Stuff にマップされます。

Fortify SASTで #include ディレクティブが出現する場合:

```
<!-- #include virtual="Include/Task1/foo.inc" -->
```

Fortify SASTでは、プロジェクトに という名前の物理ディレクトリが含まれているかどうかを特定します。このような物理ディレクトリがない場合、Fortify SASTはそのランタイムプロパティを調べて、 -Dcom.fortify.sca.ASPVirtualRoots.Include= "C:\WebServer\CustomerOne\inc" 設定を見つけます。その後、Fortify SASTでは、 C:\WebServer\CustomerOne\inc\Task1\foo.inc ファイルを探します。

または、 fortify-sca.properties にある <*sast_install_dir*>\Core\config ファイルでこのプロパティを設定できます。次の例に示すように、物理ディレクトリのパス内のバックスラッシュ文字(\)をエスケープする必要があります。

```
com.fortify.sca.ASPVirtualRoots.Library=C:¥¥WebServer¥¥CustomerTwo¥¥Stuff
com.fortify.sca.ASPVirtualRoots.Include=C:¥¥WebServer¥¥CustomerOne¥¥inc
```



Note

以前のバージョンのASPVirtualRootプロパティは引き続き有効です。Fortify SASTコマンドラインで次のように使用できます。

```
-Dcom.fortify.sca.ASPVirtualRoots=C:\WebServer\CustomerTwo\Stuff;
C:\WebServer\CustomerOne\inc
```

これはFortify SASTに対し、virtualインクルードディレクティブの解決時に、指定した順序でリストされているディレクトリを検索するように促します。

仮想ルートの使用例

次のファイルがあります。

```
C:¥files¥foo¥bar.asp
```

このファイルを指定するには、次のインクルードを使用します。

```
<!-- #include virtual="/foo/bar.asp">
```

次に、 sourceanalyzer コマンドで仮想ルートを次のように設定します。

```
-Dcom.fortify.sca.ASPVirtualRoots=C:¥files¥foo
```

これにより、仮想ルートの前から /foo がストライプされます。 を プロパティで指定しない場合、Fortify SASTでは C:\files\bar.asp を探して失敗します。

仮想ルートを指定するシーケンスは次のとおりです。

1. ソースのパスの最初の部分を削除します。
2. パスの最初の部分を、コマンドラインで指定した仮想ルートに置き換えます。

42.4. Classic ASPのコマンドライン例

VBScriptで記述された、 MyASP.asp という名前の単一ファイルのClassic ASPを変換するには、次のように入力します。

```
sourceanalyzer -b mybuild "MyASP.asp"
```

42.5. VBScriptのコマンドライン例

myApp.vb という名前のVBScriptファイルを変換するには、次のコマンドを入力します。

```
sourceanalyzer -b mybuild "myApp.vb"
```

43. ライブラリコードの分析

ライブラリコードは、他のアプリケーションに統合するように設計された再利用可能なソフトウェアコンポーネントまたはモジュールを指します。特定のプログラムのビジネスロジックとエントリポイントを含むアプリケーションコードとは異なり、通常、ライブラリコードは次の通りになります。

- 複数のプロジェクトにわたって汎用的で再利用可能
- メインエントリポイント(main()メソッドなど)がない
- 他のアプリケーションが使用する機能(ユーティリティクラス、フレームワーク、SDKなど)を提供します。

ライブラリコードは他のアプリケーションコードから呼び出されることを想定しているため、通常は、ユーザが制御できるデータ自体のインタフェースは提供されず、SAST技術が通常見つけ出せる結果は最小限に抑えられます。

ライブラリコードとアプリケーションコードの比較

機能	アプリケーションコード	ライブラリコード
エントリポイント	通常は「あり」	なし
目的	ビジネスロジックの実装	再利用可能な機能の提供
使用	スタンドアロンまたは展開	他のアプリに組み込まれている
分析の焦点	プログラムの完全な動作	APIの開示と使用パターン

ライブラリコードの効果的な分析

ライブラリコードを効果的にスキャンするには、コードをライブラリとして扱うFortify SASTを設定する必要があります。

言語に合わせた通常の方法でコードを変換します。適切な言語の分析の詳細については、このユーザガイドの該当するセクションを参照してください。

スキャンの準備ができたら、スキャンステップ中に次のプロパティを設定します。

```
com.fortify.sca.rules.IsLibrary=true
```

このプロパティを有効にすると、分析エンジンは外部アプリケーションがライブラリコードを呼び出す呼び出しを模倣して、より詳細な分析を提供します。

その他の使用事例

ライブラリに加えて、アプリケーションコードをライブラリコードに似たように見せる宣言型エンドポイントフレームワークも多く存在します。

ご使用のWeb APIが現在カバーされていないフレームワークを使用している場合(「サポートされている技術」を参照)、このプロパティを有効にすると、フレームワークのカバレッジが模倣されることもありますが、誤ったフローがさらに生じることもあります。



Note

この機能は現在Javaコードでのみサポートされています。



Caution

このプロパティを有効にすると、外部のコードがアプリケーションに呼び込むのを模倣し、攻撃対象面が大幅に増加して、問題が目立って増え、より多くのリソースを使用する可能性があります。指定されたユースケースや指示がない限り、通常はこれをアプリケーションコードで有効化すべきではありません。また、Spring BootやJAX-RSなど、すでにカバーされている多数の宣言エンドポイントフレームワークをサポートするために、このプロパティを有効にする必要はありません。

44. シークレットのスキャン

Fortify SASTスキャンは一連のアナライザで構成されており、そのうちの1つはあらゆるファイル形式にわたる情報を一般的に検出できます。これにより、Fortify SASTは、シークレットなどのプレーンビューに隠された情報や、不可視制御文字を含む攻撃の使用など、プログラミング言語にかかわらず脆弱な弱点を見つけることができます。

この設定方法の詳細については、「正規表現の分析」を参照してください。

44.1. 正規表現分析

正規表現(regex)分析では、正規表現ルールを使用して、ファイルコンテンツとファイル名の両方の脆弱性を検出できます。この分析では、プロジェクトファイル内の脆弱なシークレット(パスワード、キー、資格情報など)を検出できます。



Important

Regex分析は言語に依存しないため、Fortify SASTが公式にはサポートしていないファイルタイプの脆弱性を検出する可能性があります。

正規表現分析では、変換フェーズに含まれるすべてのファイルパスとパスパターンが再帰的に検査されます。見つかったすべてのファイルは、特に除外されていない限り分析されます。正規表現分析に含まれているファイルを管理するには、次のオプションを使用します。

- 変換フェーズで `-exclude` オプションを使用してファイルまたはディレクトリを除外します。
  このオプションの詳細については、変換オプションを参照してください。
- デフォルトでは、正規表現分析から検出可能なバイナリファイルがすべて除外されます。分析にバイナリファイルを含めるには、次のプロパティを `fortify-sca.properties` ファイルに追加します(または、 `-D` オプションを使用して、このプロパティをコマンドラインに含めます)。

```
com.fortify.sca.regex.ExcludeBinaries = false
```

- デフォルトでは、スキャン時間が許容可能になるように、10 MBを超えるファイルが正規表現分析から除外されます。次のプロパティを使用して、最大ファイルサイズ(メガバイト単位)を変更できます。

```
com.fortify.sca.regex.MaxSize = <max_file_size_mb>
```

正規表現分析はデフォルトで有効になっています。正規表現分析を無効にするには、次のプロパティを `fortify-sca.properties` ファイルに追加するか、コマンドラインに含める必要があります。

```
com.fortify.sca.regex.Enable = false
```

45. PQCの問題のスキャン

Fortify SASTはPQC（Post Cryptographicm Cryptography)の問題のスキャンをサポートしています。PQC攻撃に対して回復力を持たない暗号化アルゴリズムが使用されている場所を特定する場合に特に便利です。

PQCの懸念事項はすべての業界に適用されるわけではないため、デフォルトではこれらが無効になっています。これらを有効にするには、次のプロパティを指定します:

```
com.fortify.sca.rules.enablePQCRules=true
```

`fortify-sca.properties` 内、または `-Dcom.fortify.sca.rules.enablePQCRules=true` を使用してスキャン時にコマンドラインで。

使用しているルールパックに基づいて、どのライブラリおよび言語がサポートされているのかについては、OpenText SASTのセキュリティコンテンツリリース情報を参照してください。

46. 結果の最適化

このセクションでは、Fortify SASTで多様なコードベースを分析する際に結果を最適化するためのガイドラインとヒントについて説明します。

46.1. 分析へのスキャンポリシーの適用

分析(スキャン)フェーズでは、最も深刻な脆弱性を特定してコードを迅速に修復できるようにするために、スキャンポリシーを指定できます。次の表で、提供されている3つのスキャンポリシーについて説明します。

ポリシー名	説明(Description)
security	これはデフォルトのスキャンポリシーであり、コード品質に関連する問題、一般的に信頼されるソースからのデータフロー、および通常はノイズと見なされる問題を分析結果から除外します。セキュリティ問題のコード修正に重点を置く場合はこのポリシーを使用します。
devops	このスキャンポリシーは、ノイズと見なされる可能性が高い追加の問題を除外し、優先度の低い問題を減らすことで、セキュリティポリシーを拡張します。このスキャンポリシーは、スキャン速度を優先して、開発者が結果を(中間監査なしで)直接レビューする場合に使用します。このスキャンポリシーを適用した後に残る問題は、修正が必要な重大なセキュリティ問題である可能性があります。 **Note** ローカルのsecurityスキャンポリシーに加えたカスタマイズが、このdevopsスキャンポリシーに自動的に組み込まれることはありません。
classic	このスキャンポリシーでは、問題は除外されません。このスキャンポリシーを使ってすべての問題を確認できますし、隠れた問題を見つけやすくするためにプロジェクトテンプレートで問題をフィルター処理する方法もおすすめです。

分析用のスキャンポリシーを指定するには、次の例に示すように、分析フェーズに `-scan-policy` (または `-sc`)オプションを含める必要があります。

```
sourceanalyzer -b MyProject -scan -scan-policy devops -f MyResults.fpr
```

または、`com.fortify.sca.ScanPolicy` ファイルの `fortify-sca.properties` プロパティを使用してスキャンポリシーを指定することもできます。例:

```
com.fortify.sca.ScanPolicy=devops
```

Note
分析用のスキャンポリシー設定に加えて、フィルタファイルを適用できます(「フィルタファイルによる問題の除外」を参照)。この場合、Fortify SASTによってスキャンポリシーとフィルタファイルの両方が分析に適用されます。

カスタムスキャンポリシーの作成

スキャンポリシーファイルは、 `<sast_install_dir>/Core/config/scales` ディレクトリにあります。スキャンポリシーごとに1つのファイルがあります。これらのポリシーファイルの設定を変更してスキャンポリシーをカスタマイズしたり、独自のス

キャンポリシーファイルを作成することができます。スキャンポリシーファイルに使用される構文については、「フィルタファイルによる問題の除外」を参照してください。

カスタムスキャンポリシーファイルを作成するには:

1. `<sast_install_dir>/Core/config/scales/` に移動します。
2. テキストエディタを開き、 `scan-policy-<name>.txt` という名前のファイルを作成します。ここで、*<name>*はカスタムスキャンポリシーの名前です。
3. フィルタを `scan-policy-<name>.txt` ファイルに追加して保存します。
4. 分析にカスタムスキャンポリシーを使用するには、次の例に示すようにコマンドを入力します。この例では、スキャンポリシーファイル名は `scan-policy-myscanpolicy.txt` です。

   ```
   sourceanalyzer -b MyProject -scan -scan-policy myscanpolicy -f MyResults.fpr
   ```

   または、 `fortify-sca.properties` ファイルにカスタムスキャンポリシーを指定できます。詳細については、「変換と分析フェーズのプロパティ」を参照してください。

46.2. フィルタファイルによる問題の除外

`sourceanalyzer` コマンドを実行すると、特定の脆弱性インスタンス、ルール、および脆弱性カテゴリをフィルタ処理するファイルを作成できます。 `-filter 分析オプション`を使用してファイルを指定します。

フィルタファイルは、任意のテキストエディタで作成できるテキストファイルです。このファイルで必要 ないフィルタ項目のみを指定します。

> **Note**
>
> このセクションで説明するフィルタタイプは、フィルタファイルとスキャンポリシーファイルの両方に適用されます(「分析へのスキャンポリシーの適用」を参照)。

次の表に、使用可能なフィルタタイプとそれぞれの例を示します。

フィルタタイプ	メモ	例
Category	カテゴリのみを指定すると、すべてのサブカテゴリがフィルタで除外されます **Note** Fortify SASTでは、分析が実行される前の初期化フェーズでカテゴリフィルタが適用されます。	`Poor Error Handling` `J2EE Bad Practices: Leftover Debug Code`
インスタンスID	特定の問題のインスタンスID **Note** Fortify SASTでは、分析フェーズの後にインスタンスIDフィルタが適用されます。	`6291C6A33303ED270C269917AA8A1005`
ルールID	特定の問題のレポートを生成するルールID **Note** Fortify SASTでは、分析が実行される前の初期化フェーズでルールIDフィルタが適用されます。	`823FE039-A7FE-4AAD-B976-9EC53FFE4A59`
Priority1	優先度の値は、昇順で、`low`、`medium`、`high`、`critical`です。 詳細については、「問題の深刻度のランク付け」を参照してください。	`priority <= low` `priority < medium`

テイントフラグ	テイントフラグ式を括弧で囲みます。式を指定するには、`&&`、`||`、および`!`論理演算子を使用します。テイントフラグの一覧については、『*OpenText™ Fortify SASTカスタムルールガイド*』を参照してください。	`(SYSTEMINFO || EXCEPTIONINFO)`
		`(WEB || (DATABASE && PRIVATE))`
		`(NETWORK && !XSS)`

Impact1	詳細については、「問題の深刻度のランク付け」を参照してください。	`impact < 0.5`

Likelihood1	詳細については、「問題の深刻度のランク付け」を参照してください。	likelihood <= 1.5
Confidence1	詳細については、「問題の深刻度のランク付け」を参照してください。	confidence < 1.8
Probability1	詳細については、「問題の深刻度のランク付け」を参照してください。	probability <= 1.2
Accuracy1	詳細については、「問題の深刻度のランク付け」を参照してください。	accuracy <= 1.0
min_virtual_call_confidence1	特定の問題のトレース内のすべての仮想呼び出しに基づいてエンジンによって計算された、総合的な信頼度値。 confidence スコアリング内で使用されますが、よりきめ細かいフィルタリングにも使用できます。これは0.4から1.0の間の値です。	min_virtual_call_confidence <= 0.75
アナライザ	有効な値は、 buffer 、 content 、 configuration 、 controlflow 、 dataflow 、 scripted 、 semantic 、 structural です。	
ファイルタイプ	有効なファイルタイプの値は、 ABAP 、 ACTIONSCRIPT 、 ADA 、 APEX 、 ASPNET 、 ASP 、 ASPX 、 BYTECODE 、 C 、 CFML 、 CLOUDFORMATION 、 COBOL 、 CPP 、 CSHARP 、 DART 、 DELPHI 、 DOCKERFILE 、 ELIXIR 、 ERLANG 、 GO 、 GROOVY 、 HCL 、 HOCON 、 HTML 、 INI 、 JAVA 、 JAVA_PROPERTIES 、 JAVASCRIPT 、 JINJA 、 JSON 、 JSP 、 JSPX 、 JUPYTER 、 KOTLIN 、 LUA 、 MSIL 、 MXML 、 OBJC 、 OBJCPP 、 PERL 、 PHP 、 PLSQL 、 POWERSHELL 、 PYTHON 、 R 、 RUBY 、 RUST 、 SCALA 、 SOLIDITY 、 SWIFT 、 SWC 、 SWF 、 SQL 、 TERRAFORM 、 TLD 、 TSQL 、 TYPESCRIPT 、 VB 、 VB6 、 VBSCRIPT 、 VISUAL_FORCE 、 VUE 、 XML 、 YAML です。	

1優先度フィルタとメタデータフィルタには、「未満」(<)または「以下」(<=)を使用します。

複合フィルタ

異なる行にフィルタを指定すると、Fortify SASTは各フィルタ行を一度に1行ずつ適用します。また、これらの演算子を1行に結合し、ブール論理演算子(&&、||、!)と中カッコ { } を使用して式をグループ化すると、より高度なフィルタを作成できます。

たとえば、Cross-Site Scriptingの問題をフィルタで除外したい場合に、問題に4.0未満のconfidenceがあり、テイントフラグにDATABASEまたはLDAPが含まれているとします。

次のフィルタを使用できます:

```
{ Cross-Site Scripting && confidence < 4.0 } && ( DATABASE || LDAP )
```

複合フィルタの一部が、事後スキャンのみを実行できるフィルタタイプである場合、通常は事前スキャンをフィルタする項目がある場合でも、事後スキャンが実行されます。

> **Note**
>
> 中括弧に関係なく、テイントフラグフィルタは丸括弧で囲む必要があります。

フィルタファイルの例

46.2.1. フィルタファイルの例

たとえば、次の出力はEightBall.javaサンプルのスキャンによる出力です。このサンプルプロジェクトは、OpenText_SAST_Fortify_Samples_<*version*>.zipディレクトリ内のbasic/eightballアーカイブに含まれています。

次のコマンドは、分析結果を生成するために実行されます。

```
sourceanalyzer -b eightball EightBall.java sourceanalyzer -b eightball -scan
```

次の結果は、検出された5つの問題を示しています。

```
[F7A138CDE5235351F6A4405BA4AD7C53 : low : Unchecked Return Value : semantic ] EightBall.java(12) :
Reader.read() [6291C6A33303ED270C269917AA8A1005 : high : Path Manipulation : dataflow ]
EightBall.java(12) : ->new FileReader(0) EightBall.java(8) : <=> (filename) EightBall.java(8) : <-
>Integer.parseInt(0->return) EightBall.java(6) : <=> (filename) EightBall.java(4) : ->EightBall.main(0)
[176CC0B182267DD538992E87EF41815F : critical : Path Manipulation : dataflow ] EightBall.java(12) : ->new
FileReader(0) EightBall.java(6) : <=> (filename) EightBall.java(4) : ->EightBall.main(0)
[E4B3ACF92911ED6D98AAC15876739EC7 : high : Unreleased Resource : Streams : controlflow ]
EightBall.java(12) : start -> loaded : new FileReader(...) EightBall.java(14) : loaded -> end_of_scope :
end scope : Resource leaked EightBall.java(12) : start -> loaded : new FileReader(...) EightBall.java(12)
: java.io.IOException thrown EightBall.java(12) : loaded -> loaded : throw EightBall.java(12) : loaded ->
end_of_scope : end scope : Resource leaked : java.io.IOException thrown [BB9F74FFA0FF75C9921D0093A0665BEB
: low : J2EE Bad Practices : Leftover Debug Code : structural ] EightBall.java(4)
```

次の処理を実行するフィルタファイルの例を次に示します。

- J2EE Bad Practiceカテゴリに関連する結果をすべて削除する
- インスタンスIDに基づいてパス操作を削除する
- 特定のルールIDから生成されたデータフローの問題を削除する

```
#This is a category to filter from scan output
J2EE Bad Practices #This is an instance ID of a specific issue to be filtered #from scan output
6291C6A33303ED270C269917AA8A1005 #This is a specific Rule ID that leads to the reporting of a #specific
issue in the scan output: in this case the #dataflow sink for a Path Manipulation issue.
823FE039-A7FE-4AAD-B976-9EC53FFE4A59
```

フィルタ処理された出力をテストするには、このテキストをコピーし、 test_filter.txt という名前でファイルに貼り付けます。

test_filter.txt ファイルにフィルタ処理を適用するには、次のコマンドを実行します。

```
sourceanalyzer -b eightball -scan -filter test_filter.txt
```

フィルタ処理された分析では、次の結果が生成されます。

```
[176CC0B182267DD538992E87EF41815F : critical : Path Manipulation : dataflow ] EightBall.java(12) : ->new
FileReader(0) EightBall.java(6) : <=> (filename) EightBall.java(4) : ->EightBall.main(0)
[E4B3ACF92911ED6D98AAC15876739EC7 : high : Unreleased Resource : Streams : controlflow ]
EightBall.java(12) : start -> loaded : new FileReader(...) EightBall.java(14) : loaded -> end_of_scope :
end scope : Resource leaked EightBall.java(12) : start -> loaded : new FileReader(...) EightBall.java(12)
: java.io.IOException thrown EightBall.java(12) : loaded -> loaded : throw EightBall.java(12) : loaded ->
end_of_scope : end scope : Resource leaked : java.io.IOException thrown
```

46.3. フィルタセットを使用した問題の除外

Fortify Audit Workbenchで作成した問題テンプレートでフィルタセットを使用して、分析結果から問題をフィルタできます。分析フェーズ中に問題を非表示にするフィルタセットを適用すると、Fortify SASTはその非表示の問題をFPRに書き込みません。これを行うには、Fortify Audit Workbenchを使用してフィルタセットを作成し、そのフィルタセットと、そのフィルタセットが含まれている問題テンプレートを使用してFortify SASTスキャンを実行します。Fortify Audit Workbenchでフィルタとフィルタセットを作成する方法について詳しくは、『*OpenText™ Fortify Audit Workbench ユーザガイド*』を参照してください。

次の例では、FPRから問題を削除するために、問題テンプレート内でフィルタを作成して使用する方法の基本的な手順について説明します。

1. OWASP Top 10 2021を使用し、この標準のカテゴリに分類された問題のみを表示するとします。Fortify Audit Workbenchで、 OWASP_Filter という名前の新しいフィルタセットを作成します。
2. Fortify Audit Workbenchで、 OWASP_Filter フィルタセット内に表示フィルタを作成します。

   ```
   If [OWASP Top 10 2021] does not contain A Then hide issue
   ```

   このフィルタは、問題を検索して、名前に「A」を含むOWASP Top 10 2021のカテゴリに問題がマップされない場合は、それを非表示にします。OWASP Top 10 2021のカテゴリはすべて「A」(A01、A02、...、A10)で始まるため、文字「A」を含まないカテゴリはOWASP Top 10 2021に存在しません。このフィルタによって、問題はFortify Audit Workbenchのビューに表示されなくなりますが、FPRには残ったままになります。
3. Fortify Audit Workbenchで、問題テンプレートを IssueTemplate.xml という名前のファイルにエクスポートします。
4. Fortify SASTを使用し、次のコマンドを指定して、分析フェーズでフィルタセットを指定します。

   ```
   sourceanalyzer -b MyProject -scan -project-template IssueTemplate.xml -
   Dcom.fortify.sca.FilterSet=OWASP_Filter -f MyFilteredResults.fpr
   ```

フィルタセットで問題をフィルタすると、FPRのサイズは削減されますが、通常、スキャン時間は短縮されません。Fortify SASTは、問題を計算してFPRファイルに書き込むかどうかを判断した後で、フィルタセットを調べます。フィルタセット内のフィルタによって、Fortify SASTがロードするルールタイプが決まります。

46.4. FortifyRemoveコメントを使用したフィルタ

リンター、コンパイラ、静的解析ツールがIDEに直接組み込まれているように、開発者はこれらのツールの結果をコードから直接制御することに慣れています。同様に、Fortify SASTによって引き起こされる問題を管理するために、インラインコメントを必要に応じて使うこともできます。開発者は、問題を引き起こすルールID、または検索結果のカテゴリを FortifyRemove() に指定して、問題が報告されるのを防ぐことができます。

コメント付きで問題が削除されると、Fortify SASTは削除された問題をその場所やカテゴリを含めてログに記録します。

Note
この機能は、JavaおよびC#コードでデフォルトで利用可能かつ有効にされています。この機能は、`com.fortify.sca.rules.EnableRuleComments=false` を設定することで `fortify-rules.properties` で無効にできます。詳細については、「fortify-rules.properties」を参照してください。

基本的なコメント

たとえば、次のような `Java Hello World` アプリケーションがあるとします。

```
public class MyClass { public static void main(String[] args) { System.out.println("Hello World"); } }
```

*J2EE Bad Practices: Leftover Debug Code*として*メイン関数*でトリガされる、`625EEE1F-464F-42DC-85D6-269A637EF747` のIDを持つルールがある場合を考えます。

開発者が同意せず、この問題を今後表示したくない場合は、次のいずれかの設定により、問題が表示されなくなります。

```
public class MyClass { // FortifyRemove(ID="625EEE1F-464F-42DC-85D6-269A637EF747") public static void main(String[] args) { System.out.println("Hello World"); } }
```

または

```
public class MyClass { // FortifyRemove(Category="J2EE Bad Practices: Leftover Debug Code") public static void main(String[] args) { System.out.println("Hello World"); } }
```

注: 文字列引数には「"」または「'」のいずれかを使用できます。

ワイルドカード

ワイルドカード(`*`)を使用して、カテゴリを展開し、複数のサブカテゴリまたは複数の一致するカテゴリをカバーできます。
例:

```
// FortifyRemove(Category="Cross-Site Scripting: *")
```

クロスサイトスクリプティングに関する問題のバリアントはすべて削除されます。
一方:

```
// FortifyRemove(Category="Cross-Site *")
```

クロスサイトスクリプティングに関する問題のすべてのバリアントと、「クロスサイト」で始まるカテゴリ(たとえば「クロスサイトリクエスト偽造」)も削除します。

複数の条件

ワイルドカードを使用する以外に、文字列の配列を取る `Categories` プロパティまたは `IDs` プロパティを使用して、それぞれ、複数のカテゴリまたは複数のルールIDを指定できます。
例

```
// FortifyRemove(Categories=["Cross-Site Scripting: Reflected", "Cross-Site Scripting: Persistent"])
```

`Cross-Site Scripting: Reflected` または `Cross-Site Scripting: Persistent` の問題が次の行に表示されるのを防ぎます。

```
// FortifyRemove(IDs=["A", "B", "C", "D"]
```

`A`、`B`、`C`、または `D` のルールが次の行でトリガされるのを防ぎます。
また、複数の条件をセミコロン(`;`)で区切って指定することもできます。

例:

```
//  FortifyRemove(Category="SQL  Injection";  ID="ABCD-1234")
```

これにより、 の問題が次の行で発生しないようにし、ルールID からトリガされる問題も防げます。

正当な理由の追加

問題は、 FortifyRemove のコメント付きで、削除済みとして記録されます。削除情報と共にログに記録される文字列を受け入れる justification プロパティを指定することで、なぜ問題が削除されるのかを詳しく説明できます。
例:

```
// FortifyRemove(Category="Cross-Site Scripting: *"; Justification="We remove XSS here because we're
using custom framework XYZ that automatically protects against the attack")
```

46.5. Fortify Java注釈

OpenTextでは、2つのバージョンのFortify Java注釈ライブラリが提供されています。

- 保持ポリシーがCLASS (FortifyAnnotations-CLASS.jar)に設定された注釈。
  このバージョンのライブラリでは、コンパイル時にFortify Java注釈がバイトコードに反映されます。
- 保持ポリシーがSOURCE (FortifyAnnotations-SOURCE.jar)に設定された注釈。
  このバージョンのライブラリでは、Fortify Java注釈が使用されるコードがコンパイルされた後にバイトコードに反映されません。

OpenText Application Security Software製品を使ってアプリケーションのバイトコードを分析する場合(たとえばOpenText™ Core Application Security評価を使う場合)、注釈保持ポリシーがCLASSに設定されたバージョンを使用してください。OpenText Application Security Software製品を使ってアプリケーションのソースコードを分析する場合は、いずれかのバージョンのライブラリを使用できます。ただし、保持ポリシーがSOURCEに設定されているライブラリを使用することが強く推奨されています。

Important

コード内の潜在的なセキュリティ上の問題に関する情報が漏洩する可能性があるため、Fortify Java注釈を運用コードに残すのはセキュリティ上のリスクになります。保持ポリシーがCLASSに設定されている注釈は内部の分析にのみ使用し、アプリケーションの運用ビルドでは決して使用しないことが推奨されています。

このセクションでは、使用可能な注釈の概要を示します。サンプルアプリケーションは、OpenText_SAST_Fortify_Samples_<*version*>.zip ディレクトリ内の advanced/javaAnnotations アーカイブに含まれています。ディレクトリに含まれている README.txt ファイルには、サンプルアプリケーション、アプリケーションから発生する可能性がある問題、およびこれらの問題をFortify Java注釈を使用して解決する方法が記述されています。

Fortify Javaの注釈には、次の2つの制限があります。

- 各注釈は1つの入力または1つの出力のみ(あるいはその両方)を指定できます。
- 同じターゲットには各タイプの注釈を1つのみ適用できます。

OpenTextでは、次の主要な3つのタイプの注釈が提供されています。

- データフローの注釈
- フィールドと変数の注釈
- その他の注釈

独自のカスタム注釈がサポートされるルールを作成することもできます。詳細については、カスタマサポートにお問い合わせください。

46.5.1. データフローの注釈

データフローの注釈には、データフロールールと同様に、ソース、シンク、パススルー、検証の4種類があります。すべてがメソッドに適用され、パラメータ名または文字列 this および return によって入力、出力、またはその両方を指定しま

す。また、データフローのソースおよびシンク注釈を関数の引数に適用することもできます。

ソース注釈

注釈パラメータで使用できる値は、`this`、`return`、または関数パラメータ名です。たとえば、ターゲットメソッドの出力に汚染を割り当てることができます。

```
@FortifyDatabaseSource("return") String [] loadUserProfile(String userID) { ... }
```

たとえば、ターゲットメソッドの引数に汚染を割り当てることができます。

```
void retrieveAuthCode(@FortifyPrivateSource String authCode) { ... }
```

特定のソース注釈に加えて、OpenTextには という名前の、汎用の*信頼できない*汚染ソースが用意されています。

ソース注釈の完全なリストを次に示します。

- `FortifySource`
- `FortifyDatabaseSource`
- `FortifyFileSystemSource`
- `FortifyNetworkSource`
- `FortifyPCISource`
- `FortifyPrivateSource`
- `FortifyWebSource`

パススルー注釈

パススルー注釈では、ターゲットメソッドの入力から出力にすべての汚染が転送されます。`FortifyNumberPassthrough` および `FortifyNotNumberPassthrough` の場合は、出力から汚染を割り当てたり、削除したりすることもできます。 `in` 注釈パラメータで使用できる値は、`this` または関数パラメータ名です。`out` 注釈パラメータで使用できる値は、`this`、`return`、または関数パラメータ名です。

```
@FortifyPassthrough(in="a",out="return") String toLowerCase(String a) { ... }
```

データが純粋に数値であることを示すには、 `FortifyNumberPassthrough` を使用します。数値データは、ソースに関係なく、クロスサイトスクリプティングなどの特定のタイプの問題を引き起こす可能性があります。 `FortifyNumberPassthrough`を使用すると、このタイプの誤検出が減少します。プログラムで文字データを数値型(intやint[]など)に分解する場合は、`FortifyNumberPassthrough` を使用できます。プログラムで数値データを文字または文字列データに連結する場合は、`FortifyNotNumberPassthrough` を使用します。

パススルー注釈の完全なリストを次に示します。

- `FortifyPassthrough`
- `FortifyNumberPassthrough`
- `FortifyNotNumberPassthrough`

シンク注釈

シンク注釈では、適切なタイプの汚染がターゲットメソッドの入力に到達したときに問題が報告されます。注釈パラメータで使用できる値は、 `this` または関数パラメータ名です。

```
@FortifyXSSSink("a") void printToWebpage(int a) { ... }
```

関数の引数または戻りパラメータに注釈を適用することもできます。次の例では、汚染が引数 に到達したときに問題が報告されます。

```
void printToWebpage(int b, @FortifyXSSSink String a) { ... }
```

シンク注釈の完全なリストを次に示します。

- FortifySink
- FortifyCommandInjectionSink
- FortifyPCISink
- FortifyPrivacySink
- FortifySQLSink
- FortifySystemInfoSink
- FortifyXSSSink

検証注釈

検証注釈では、ターゲットメソッドの出力から汚染が削除されます。注釈パラメータで使用できる値は、this 、 return 、または関数パラメータ名です。

```
@FortifyXSSValidate("return") String xssCleanse(String a) { ... }
```

検証シンク注釈の完全なリストを次に示します。

- FortifyValidate
- FortifyCommandInjectionValidate
- FortifyPCIValidate
- FortifyPrivacyValidate
- FortifySQLValidate
- FortifySystemInfoValidate
- FortifyXSSValidate

46.5.2. フィールドと変数の注釈

これらの注釈は、フィールドと変数(ほとんどの場合)に適用できます。

パスワードとプライベートの注釈

パスワードとプライベートの注釈を使用して、ターゲットのフィールドまたは変数がパスワードであるのか、プライベートデータであるのかを示します。

```
@FortifyPassword String x; @FortifyNotPassword String pass; @FortifyPrivate String y; @FortifyNotPrivate
String cc;
```

この例では、「x」という文字列がパスワードとして識別され、プライバシー違反およびハードコーディングされたパスワードがチェックされます。「pass」という文字列は、パスワードとして識別されません。注釈がない場合は、誤検知が発生する可能性があります。 FortifyPrivate および FortifyNotPrivate の注釈も同様に機能しますが、プライバシー違反の問題は発生しません。

負でない注釈と0以外の注釈

これらの注釈を使用して、ターゲットのフィールドまたは変数で許可されていない値を指定します。

```
@FortifyNonNegative int index; @FortifyNonZero double divisor;
```

この例では、 index に負の値が割り当てられているか、 divisor にゼロが割り当てられている場合に問題がレポートされます。

46.5.3. その他の注釈

戻り値チェックの注釈

FortifyCheckReturnValue 注釈を使用して、戻り値をチェックする必要がある関数のリストにターゲットメソッドを追加します。

```
@FortifyCheckReturnValue int openFile(String filename) { ... }
```

危険の注釈

FortifyDangerous 注釈を使用すると、ターゲット関数、フィールド、変数、またはクラスの使用がレポートされます。注釈パラメータに使用できる値は、CRITICAL、HIGH、MEDIUM、または LOW です。これらの値は、Fortify Priority Order の値に基づいて問題を分類する方法を示しています。

```
@FortifyDangerous("CRITICAL") public class DangerousClass { @FortifyDangerous("HIGH") String
dangerousField; @FortifyDangerous("LOW") int dangerousMethod() { ... } }
```

47. パフォーマンスの最適化

このセクションでは、Fortify SASTでさまざまな種類のコードベースを分析する際に、メモリ使用量とパフォーマンスを最適化するためのガイドラインとヒントについて説明します。

- ウィルス対策ソフトウェア
- ハードウェアに関する考慮事項
- チューニングオプション
- クイックスキャン
- 短縮ダイヤルを使用したスキャン速度の設定
- コードベースの分割
- アナライザと言語の制限
- FPRファイルの最適化
- 長時間実行されているスキャンの監視

47.1. ウィルス対策ソフトウェア

ウィルス対策ソフトウェアを使用すると、Fortify SASTのパフォーマンスが悪影響を受ける可能性があります。スキャン時間が長い場合に、ウィルス対策ソフトウェアスキャンから内部のFortify SASTファイルを一時的に除外することが推奨されています。ソースコードが存在するディレクトリでも同じ操作を実行できますが、分析時のパフォーマンスの影響は内部ディレクトリの場合よりも小さいです。

デフォルトでは、Fortify SASTの内部ファイルが次の場所に作成されます。

- Windows: c:\Users\<*username*>\AppData\Local\Fortify\sca<*version*>
- Windows以外: <*userhome*>/.fortify/sca<*version*>

ここで、<*version*>は使用しているFortify SASTのバージョンです。

47.2. ハードウェアに関する考慮事項

さまざまなソースコードがあるため、メモリ使用量やスキャン時間を正確に予測することはできません。次のさまざまな要因によってメモリ使用量やパフォーマンスが影響を受けます。

- コードのタイプ
- コードベースのサイズと複雑さ
- 使用される補助言語(JSP、JavaScript、HTMLなど)
- 脆弱性の数
- 脆弱性のタイプ(使用されるアナライザ)

OpenTextでは、実際のアプリケーションスキャンの結果に基づいて、次の「最適な推測」というハードウェアの推奨事項が開発されました。次の表には、アプリケーションの複雑性に基づいた推奨事項のリストを示します。一般に、使用可能なコアの数を増やすと、スキャン時間が短縮される可能性があります。

アプリケーションの複雑さ	CPUコア数	RAM (GB)	平均スキャン時間	説明(Description)
単純	4	16	1時間	サーバまたはデスクトップ上で実行されるスタンドアロンシステム(バッチジョブやコマンドラインツールなど)。
Medium	8	32	5時間	複雑なコンピュータモデルで動作するスタンドアロンシステム(税額計算システムやスケジューリングシステムなど)。
複雑	16	128	4日間	トランザクションデータ処理を備えた3階層ビジネスシステム(財務システムや商用Webサイトなど)。
非常に複雑	32	256	7日間以上	コンテンツを配信するシステム(アプリケーションサーバ、データベースサーバ、コンテンツ管理システムなど)。



Note

TypeScriptスキャンおよびJavaScriptスキャンでは、分析時間が大幅に長くなります。アプリケーション内のコード行の合計がTypeScriptまたはJavaScriptの20%を超える場合は、2番目に高い推奨事項を使用します。

システム要件については、「ハードウェア要件」を参照してください。ただし、大規模で複雑なアプリケーションの場合は、Fortify SASTでより高い能力を持つハードウェアが必要です。その内容は次のとおりです。

- **ディスクI/O** - Fortify SASTはI/O集中型であるため、ハードドライブが高速になるほど、多くのI/Oトランザクションが節約されます。7,200 RPMドライブが推奨されていますが、10,000 RPMドライブ(WD Raptorなど)またはSSDドライブの方が適切です。
- **メモリ** - 最適なパフォーマンスを得るために必要なメモリの量を決定する方法の詳細については、「メモリチューニング」を参照してください。
- **CPU**—2.1　GHz以上のプロセッサが推奨されています。

47.3. チューニングオプション

Fortify SASTでは、複雑なプロジェクトの処理に長い時間がかかる場合があります。次のようにさまざまなフェーズで時間が費やされます。

- 変換
- 分析

Fortify SASTでは、大きな分析結果ファイル(FPR)が生成される可能性があります。その結果、監査とFortify Software Security Centerへのアップロードに長い時間がかかる場合があります。このフェーズは、次のように呼ばれます。

- 監査/アップロード

次の表では、時間のかかるさまざまなフェーズでパフォーマンスを向上させる方法に関するヒントを示します。

フェーズ	オプション	説明(Description)	詳細情報
変換	-export-build-session -import-build-session	さまざまなコンピュータでの変換とスキャン	モバイルビルドセッション
分析	-quick	クイックスキャンの実行	クイックスキャン
分析	-scan-precision	スキャン精度の設定	短縮ダイヤルを使用したスキャン速度の設定
分析	-bin	バイナリに関連するファイルのスキャン	コードベースの分割
分析	-Xmx<*size*>M | G	最大ヒープサイズの設定	メモリのチューニング
分析	-Xss<*size*>M | G	各スレッドのスタックサイズの設定	メモリのチューニング
分析 監査/アップロード	-filter <*file*>	フィルタファイルを使用したフィルタの適用	フィルタファイルの使用
分析 監査/アップロード	-disable-source-bundling	FPRファイルからのソースファイルの除外	FPRからのソースコードの除外

47.4. クイックスキャン

クイックスキャンモードを使用すると、プロジェクトを高速にスキャンして、重大な問題や優先度の高い問題を特定できます。Fortify SASTは、分析の深さを減らすことでスキャンを高速に実行します。さらに、Quick Viewフィルタセットも適用されます。クイックスキャン設定は設定可能です。クイックスキャンモードの設定について詳しくは、fortify-sca-quickscan.propertiesを参照してください。

クイックスキャンは、評価を通じて多くのアプリケーションを取得し、問題をすばやく見つけて修復を開始できるようにするための最適な方法です。パフォーマンスがどの程度向上するかは、アプリケーションの複雑さとサイズによって異なります。このスキャンはフルスキャンよりも高速ですが、結果セットの堅牢性は劣ります。可能な限りフルスキャンを実行することをお勧めします。

リミッタ

Fortify SASTの分析の深さは、利用可能なリソースに依存する場合があります。Fortify SASTは、複雑性のメトリックを使用して、これらのリソースと検出可能な脆弱性の数のバランスを取ります。このため、Fortify SASTが十分なリソースを使用できないと見なされる場合は、特定の機能を実行しないことがあります。

Fortify SASTでは、ユーザがFortify SASTのリミッタプロパティを使用して「カットオフ」ポイントを制御できます。アナライザごとに異なるリミッタが用意されています。クイックスキャンを使用して、これらのリミッタの事前定義されたセットを実行できます。リミッタについて詳しくは、fortify-sca-quickscan.propertiesを参照してください。

クイックスキャンモードを有効にするには、-quickオプションとともに-scanオプションを使用します。クイックスキャンモードを有効にすると、Fortify SASTは標準の<*sast_install_dir*>/Core/config/fortify-sca-quickscan.propertiesファイルに加えて<*sast_install_dir*>/Core/config/fortify-sca.propertiesファイルのプロパティを適用します。fortify-sca-quickscan.propertiesファイルを編集して、Fortify SASTが使用するリミッタを調整できます。fortify-sca.propertiesを変更すると、クイックスキャンの動作にも影響します。クイックスキャンモードでパフォーマンスを調整し、正確なスキャンを実行するためにフルス

キャンをデフォルト設定のままにすることを推奨します。クイックスキャンモードのプロパティの詳細については、「Fortify　SASTのプロパティファイル」を参照してください。

クイックスキャンとフルスキャンの使用

- **フルスキャンを定期的に実行する** - フルスキャンは、クイックスキャンモードでは検出されない問題を検出できる可能性があるため、定期的に実行することが重要です。ソフトウェアのイテレーションごとに、少なくとも1回はフルスキャンを実行します。可能であれば、週末など、開発ワークフローが中断されないタイミングで定期的にフルスキャンを実行します。
- **クイックスキャンとフルスキャンを比較する** - クイックスキャンの正確な影響を評価するには、同じコードベースでクイックスキャンとフルスキャンを実行します。Fortify Audit Workbenchでクイックスキャンの結果を開き、それをフルスキャンにマージします。問題を**新しい問題**でグループ化して、フルスキャンで検出されたがクイックスキャンでは検出されなかった問題のリストを生成します。
- **クイックスキャンとFortify Software Security Center** — フルスキャンの結果が上書きされるのを防ぐため、デフォルトではFortify Software Security Centerは、クイックスキャンモードでスキャンされてアップロードされたFPRファイルを無視します。ただし、Fortify Software Security Centerのアプリケーション版は、クイックスキャンでスキャンされたFPRファイルを処理するように設定できます。詳しくは、*OpenText™ Application Securityユーザガイド*の分析結果の処理ルールを参照してください。

47.5. 短縮ダイヤルを使用したスキャン速度の設定

分析フェーズの精度レベルを指定して、スキャンの速度と深さを設定できます。これらの精度レベルを使用して、たとえば、パイプラインに適合するようにスキャン時間を調整すると、開発者がコードの作業を続けながら一連の脆弱性をすばやく見つけ出すことができます。短縮ダイヤル設定を使用したスキャンは、フルスキャンよりも高速ですが、結果セットの堅牢性は劣ります。可能な限りフルスキャンを実行することをお勧めします。

精度レベルでは、設定プロパティを各レベルに関連付けることで、スキャンの深さと精度を制御します。各レベルの設定プロパティファイルは、 `<sast_install_dir>/Core/config/scales` ディレクトリにあります。レベルごとに1つのファイル(`level-<precision_level>.properties`)があります。これらのファイルの設定を変更して、独自の精度レベルを作成できます。

メモ:

- Fortify Software Security Centerでは、4未満の精度レベルで作成され、アップロードされた分析結果がデフォルトでブロックされます。ただし、これらの精度レベルでスキャンされ、アップロードされた監査プロジェクトが処理されるように、Fortify Software Security Centerのアプリケーションバージョンを設定できます。
- 短縮ダイヤルスキャンをフルスキャンとマージすると、アプリケーションに残っている以前のスキャンの問題が削除される場合があります(フルスキャンを実行すると再び検出されます)。

スキャンの短縮ダイヤル設定を指定するには、次の例に示すように、スキャンフェーズに `-scan-precision` (または `-p`)オプションを含める必要があります。

```
sourceanalyzer -b MyProject -scan -scan-precision <level> -f MyResults.fpr
```



Note

短縮ダイヤル設定と `-quick` オプションを同じスキャンコマンドで使用することはできません。

次の表では、4つの精度レベルについて説明します。

精度レベル	説明(Description)
1	これは最も高速なスキャンであり、数個のファイルをスキャンするのにお勧めします。この精度レベルのスキャンでは、Buffer Analyzer、Control Flow Analyzer、Dataflow Analyzer、およびNull Pointer Analyzerがデフォルトで無効になります。
2	この精度レベルのスキャンでは、すべてのアナライザがデフォルトで有効になります。リミッタを減らして実行すると、スキャンの実行速度が向上します。その結果、検出される問題の数が少なくなります。
3	この精度レベルでは、中間開発スキャンの速度が最大50%向上します(報告される問題も減少します)。具体的には、このレベルではJavaやC/C++などの型付け言語のスキャン時間が向上します。
4	これはフルスキャンと同じです。

`com.fortify.sca.PrecisionLevel` ファイルの `fortify-sca.properties` プロパティを使用してスキャン精度レベルを指定することもできます。例:

```
com.fortify.sca.PrecisionLevel=1
```

47.6. コードベースの分割

大規模なプロジェクトを独立したモジュールに分割すると、効率が向上します。たとえば、ポータルアプリケーションを構成する複数のモジュールが互いに独立しているか、モジュール間のやり取りが少ない場合は、モジュールを個別に変換およびスキャンできます。ただし、何らかのやり取りがある場合は、データフローの問題を検出できない可能性があることに注意する必要があります。

C/C++の場合は、 `–bin` オプションとともに `–scan` オプションを使用すると、スキャン時間が短縮される可能性があります。バイナリファイルをパラメータとして渡す必要があります(`-bin <filename>.exe -scan` または `-bin <filename>.dll -scan` など)。Fortify SASTでは、バイナリに関連するファイルが検索され、スキャンされます。これは、makefileに複数のバイナリがある場合に便利です。

次の表は、コードベースを分割する際に役立つFortify SASTコマンドラインオプションのリストです。

オプション	説明(Description)
-bin <*binary*>	スキャンするソースファイルのサブセットを指定します。ビルド時に名前付きバイナリにリンクされたソースファイルのみがスキャンに含められます。このオプションを複数回使用すると、スキャンに複数のバイナリが含まれるように指定できます。
-show-binaries	他のバイナリの生成時に作成されたが、使用されていないオブジェクトが表示されます。ビルドに完全に統合されている場合は、作成されたバイナリがすべて表示されます。
-show-build-tree	-bin オプションとともに使用すると、バイナリを作成するために使用されるファイルと、それらのファイルをツリーレイアウトで作成するために使用されるファイルがすべて表示されます。-bin オプションが存在しない場合、Fortify SASTではバイナリごとにツリーが表示されます。

47.7. アナライザと言語の制限

場合によっては、1つのアナライザの実行や特定の言語の分析に膨大な時間が費やされることがあります。このアナライザや言語は、セキュリティ要件にとって重要ではない可能性があります。実行するアナライザとFortify SASTで変換する言語を制限できますが、その結果は最適とは言えない場合があります。

- アナライザの無効化
- 言語の無効化

47.7.1. アナライザの無効化

特定のアナライザを無効にするには、スキャン時にFortify SASTに -analyzers オプションを追加して、有効にするアナライザのカンマ区切りまたはコロン区切りリストを指定する必要があります。-analyzers オプションの有効なパラメータ値は、buffer content configuration 、 controlflow 、 dataflow 、 nullptr 、 semantic 、および structural です。

たとえば、Dataflow、Control Flow、およびBufferアナライザのみを含むスキャンを実行するには、次のスキャンコマンドを使用します。

```
sourceanalyzer -b MyProject -analyzers dataflow:controlflow:buffer -scan -f MyResults.fpr
```

Fortify SASTのプロパティファイル(com.fortify.sca.DefaultAnalyzers)に <sast_install_dir>/Core/config/fortify-sca.properties を設定して、同じ操作を実行することもできます。たとえば、前のスキャンコマンドと同等の結果を得る場合は、プロパティファイルに次の値を設定します。

```
com.fortify.sca.DefaultAnalyzers=dataflow:controlflow:buffer
```

47.7.2. 言語の無効化

特定の言語を無効にするには、除外する言語のリストを指定する -disable-language オプションを変換フェーズに含めます。有効な言語の値は次のとおりです。

abap 、 actionscript 、 apex 、 cfml 、 cobol 、 configuration 、 cpp 、 dart 、 dotnet 、 golang 、 objc 、 php 、 python 、 ruby 、 swift 、および vb 。

たとえば、設定およびPHPファイルを除外する変換を実行するには、次のコマンドを使用します。

```
sourceanalyzer -b MyProject <src_files> -disable-language configuration:php
```

Fortify SASTのプロパティファイル(com.fortify.sca.DISabledLanguages)で <sast_install_dir>/Core/config/fortify-sca.properties プロパティを設定して、言語を無効にすることもできます。たとえば、前の変換コマンドと同等の結果を得る場合は、プロパティファイルに次の値を設定します。

```
com.fortify.sca.DISabledLanguages=configuration:php
```

で使用できない言語については、 オプションを使用します。詳細については、「変換オプション」を参照してください。

47.8. FPRファイルの最適化

このセクションでは、監査結果(FPR)ファイルに関連するパフォーマンスの問題を処理する方法について説明します。これらのトピックでは、スキャン時間の短縮方法、FPRファイルサイズの削減方法、および大きなFPRファイルを開くためのヒントについて説明します。

- フィルタファイルの使用
- フィルタセットの使用
- FPRからのソースコードの除外
- FPRファイルサイズの削減
- 大きなFPRファイルを開く

47.8.1. フィルタファイルの使用

ファイルを使用して、特定の脆弱性インスタンス、ルール、および脆弱性カテゴリを分析結果から除外できます。特定の問題カテゴリまたはルールが特定のスキャンに関連していないと判断した場合は、それらをFPRに追加しないように Fortify SAST を設定できます。フィルタファイルを使用すると、スキャン時間と分析結果ファイルのサイズの両方を削減できます。

たとえば、指定したファイルを読み取るだけの単純なプログラムをスキャンする場合、パス操作の問題は機能の一部として計画されていない可能性が高いため、あまり見たくないかもしれません。パス操作の問題をフィルタで除外するには、次の1行を含むファイルを作成します。

```
Path Manipulation
```

このファイルを filter.txt という名前で保存します。次の例に示すように、分析フェーズで -filter オプションを使用します。

```
sourceanalyzer -b MyProject -scan -filter filter.txt -f MyResults.fpr
```

の分析出力には、パス操作カテゴリの問題は含まれません。フィルタファイルの詳細と例については、「フィルタファイルによる問題の除外」を参照してください。

47.8.2. フィルタセットの使用

問題テンプレートのフィルタによって、Fortify SASTの結果の表示方法が決まります。フィルタに加えてフィルタセットを使用すると、同時に使用するフィルタを選択できます。各FPRには、関連付けられた問題テンプレートがあります。フィルタセットを使用すると、問題テンプレートのフィルタで指定した条件に基づいて問題の数を減らすことができます。これにより、FPRのサイズを大幅に削減できます。

これを行うには、Fortify Audit Workbenchを使用してフィルタセット内にフィルタを作成してから、そのフィルタセットと、そのフィルタセットが含まれている問題テンプレートを使用してFortify SASTスキャンを実行します。フィルタセットの作成方法の詳細と基本的な例については、「フィルタセットによる問題の除外」を参照してください。



Note

フィルタセットで問題をフィルタリングすると、FPRのサイズは削減されますが、通常、スキャン時間は短縮されません。Fortify SASTは、問題を計算してFPRファイルに書き込むかどうかを判断した後で、フィルタセットを調べます。フィルタセット内のフィルタによって、Fortify SASTがロードするルールタイプが決まります。

47.8.3. FPRからのソースコードの除外

FPRからソースコード情報を除外することで、FPRファイルのサイズを削減できます。これは、大きなソースファイルやコードベースの場合に特に便利です。通常、この方法を使用しても、小さなソースファイルのスキャン時間は短縮されません。

Fortify SASTでFPRにソースコードが含まれないようにするために使用できるプロパティがあります。`<sast_install_dir>/Core/config/fortify-sca.properties` いずれのプロパティもファイル内で設定するか、コマンドラインでオプションを指定することができます。次の表では、これらの設定について説明します。

プロパティ名	説明(Description)

`com.fortify.sca.FPRDisableSourceBundling=true`
 	
コマンドラインオプション:
`-disable-source-bundling`
	FPRからソースコードを除外します。

`com.fortify.sca.FVDLDisableSnippets=true`
 	
コマンドラインオプション:
`–fvdl-no-snippets`
	FPRからコードスニペットを除外します。

次のコマンドライン例では、両方のオプションを使用して、FPRからソースコードとコードスニペットの両方を除外しています。

```
sourceanalyzer -b MyProject -disable-source-bundling -fvdl-no-snippets -scan -f MySourcelessResults.fpr
```

47.8.4. FPRファイルサイズの削減

FPRファイルのサイズを減らすには、いくつかの方法があります。結果に影響を与えずにこれを実現する最も簡単な方法は、「FPRからのソースコードの除外」で説明されているように、FPRからソースコードを除外することです。また、マージされたFPRのサイズをFPRUtilityで削減することもできます(『*OpenText™ Application Security ツールガイド*』を参照)。

FPRから除外する項目を選択するために使用できるプロパティが他にもいくつかあります。これらのプロパティを`<sast_install_dir>/Core/config/fortify-sca.properties`ファイルで設定するか、分析(スキャン)フェーズのコマンドラインでオプションを指定することができます。

プロパティ名	説明(Description)
com.fortify.sca.FPRDisableMetatable=true **コマンドラインオプション:** -disable-metatable	FPRからメタテーブルを除外します。Fortify Audit Workbenchは、メタテーブルを使用して関数ビューに情報をマップします。
com.fortify.sca.FVDLDisableDescriptions=true **コマンドラインオプション:** -fvdl-no-descriptions	FPRからルールの説明を除外します。カスタムの説明を使用しない場合は、Fortify Taxonomy (https://vulncat.fortify.com)の説明が使用されます。
com.fortify.sca.FVDLDisableEngineData=true **コマンドラインオプション:** -fvdl-no-enginedata	FPRからエンジンデータを除外します。これは、Fortify Audit Workbenchでファイルを開くときにFPRに多くの警告が含まれている場合に便利です。 **Note** FPRからエンジンデータを除外する場合は、FPRをFortify Software Security Centerにアップロードする前に、ローカルでFPRを現在の監査プロジェクトとマージする必要があります。FPRにはFortify SASTのバージョンが含まれていないため、Fortify Software Security Centerはサーバ上でFPRをマージできません。
com.fortify.sca.FVDLDisableProgramData=true **コマンドラインオプション:** -fvdl-no-progdata	FPRからプログラムデータを除外します。これにより、Fortify Audit Workbenchの関数ビューから汚染されたソースの情報が削除されます。通常、このプロパティがFPRファイルの全体的なサイズに及ぼす影響は最小限です。

47.8.5. 大きなFPRファイルを開く

大きなFPRファイルをFortify Audit Workbenchで開くのに必要な時間を短縮するために、<sast_install_dir>/Core/config/fortify.properties ファイルにいくつかのプロパティを設定できます。これらのプロパティについて詳しくは、『*OpenText™ Application Security ツールガイド*』を参照してください。次の表は、大きなFPRファイルを開く時間を短縮するために使用できるプロパティについて説明しています。

プロパティ名	説明(Description)
com.fortify.model.DisableProgramInfo=true	Fortify Audit Workbenchのコードナビゲーション機能の使用を無効にします。
com.fortify.model.IssueCutoffStartIndex=<num> (包括的) com.fortify.model.IssueCutoffEndIndex=<num> (排他的)	問題カットオフの開始インデックスと終了インデックスを設定します。 IssueCutoffStartIndex プロパティ(包括的)と IssueCutoffEndIndex (排他的)で、表示する問題のサブセットを指定できます。たとえば、最初の100個の問題を表示するには、次のように指定します。 com.fortify.model.IssueCutoffStartIndex=0com.fortify.model.IssueCutoffEndIndex=101 IssueCutoffStartIndex はデフォルトで 0 なので、このプロパティを指定する必要はありません。
com.fortify.model.IssueCutoffByCategoryStartIndex=<num> (包括的) com.fortify.model.IssueCutoffByCategoryEndIndex=<num> (排他的)	問題カットオフの開始インデックスをカテゴリ別に設定します。これら2つのプロパティは、前のカットオフプロパティと似ていますが、カテゴリごとに指定する点が異なります。たとえば、各カテゴリの最初の5つの問題を表示するには、次のように指定します。 com.fortify.model. IssueCutoffByCategoryEndIndex=6
com.fortify.model.MinimalLoad=true	FPRからロードされるデータを最小化します。関数ビューの使用も制限され、Fortify Audit WorkbenchがFPRからソースをロードできなくなる場合があります。
com.fortify.model.MaxEngineErrorCount=<num>	FPRからロードする、Fortify SASTによって報告される警告の数を指定します。スキャンの警告が多いプロジェクトでは、この数をデフォルトの3000から減らすと、大きなFPRファイルのロード時間を短縮できます。
com.fortify.model.ExecMemorySetting	Fortify Audit Workbenchでiidmigratorやfortifyupdateなどの外部コマンドラインツールを開始するためのJVMヒープメモリサイズを指定します。

47.9. 長時間実行されているスキャンの監視

Fortify SASTの実行中に大規模で複雑なスキャンを実行すると、完了までに長い時間がかかることがよくあります。スキャン中に、状況を常に把握できるとは限りません。デバッグログをカスタマサポートチームに提供することが推奨されていますが、Fortify SASTで実行されている操作とそのパフォーマンスをリアルタイムで確認するには、いくつかの方法があります。

- SCAStateツールの使用
- JMXツールの使用

47.9.1. SCAStateツールの使用

SCAStateコマンドラインツールを使用すると、分析フェーズ中に最新の状態分析情報を確認できます。SCAStateツールは <sast_install_dir>/bin ディレクトリにあります。分析のライブビューに加えて、Fortify SASTが分析フェーズ中にどこで時間

を費やしているかを示すタイマとカウンタのセットも用意されています。SCAStateの使用法の詳細については、「*Fortify SASTスキャンステータスの確認*」を参照してください。

47.9.2. JMXツールの使用

ツールを使用すると、JMXテクノロジでFortify SASTを監視できます。これらのツールでは、長期間にわたってFortify SASTのパフォーマンスを追跡する方法が提供されます。これらのツールの詳細については、Oracle®istered trademark;のドキュメントを参照してください。

> **Note**
> これらはサードパーティのツールであり、OpenTextでは提供もサポートもされていません。

- JConsoleの使用
- Java VisualVMの使用

47.9.2.1. JConsoleの使用

JConsoleは、JMX仕様に準拠した対話型のモニタリングツールです。JConsoleの欠点は、出力を保存できないことです。

JConsoleを使用するには、最初に追加のJVMパラメータをいくつか設定する必要があります。次の環境変数を設定します。

```
export SCA_VM_OPTS="-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=9090 -
Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false"
```

JMXパラメータを設定したら、スキャンを開始します。スキャン時に次のコマンドを使用して、JConsoleを起動してFortify SASTをローカルまたはリモートで監視します。

```
jconsole <host_name>:9090
```

47.9.2.2. Java VisualVMの使用

Java VisualVMでは、JConsoleと同じ機能が提供されています。また、JVMに関する詳細情報も提供され、監視情報をアプリケーションスナップショットファイルに保存できます。これらのファイルは保存して、後でJava VisualVMで開くことができます。

JConsoleと同様に、Java VisualVMを使用する前に、「JConsoleの使用」の説明と同じJVMパラメータを設定する必要があります。

JVMパラメータを設定したら、スキャンを開始します。次のコマンドを使用すると、Java VisualVMを起動してスキャンをローカルまたはリモートで監視できます。

```
jvisualvm <host_name>:9090
```

48. モバイルビルドセッションの使用

Fortify SASTモバイルビルドセッション(MBS)を使用すると、あるコンピュータでプロジェクトを変換し、別のコンピュータでスキャンできます。この機能の一般的なユースケースとしてスキャン時間を短縮することが挙げられます。つまり、リソースの少ないビルドコンピュータで変換を行い、その後、より高性能なコンピュータをスキャンに利用できます。

> **Note**
> Fortify ScanCentral SASTやOpenText Core Application Security (Fortify on Demand) を利用する際にも、特定のプロジェクトタイプではこれが必要となります。

MBSを使用することで、1台のマシンで変換を行い、以下のいずれかを実行できます。

- Fortify ScanCentral SASTクライアントを使用して、分析のためにMBSをセンサに移動します(「Fortify ScanCentral SAST」を参照)。

- ビルドセッション(MBSファイル)を、Fortify SASTがインストールされている別のコンピュータに移動し、MBSをインポートして(「モバイルビルドセッションのインポート」を参照)、それから分析を実行します。
- 分析のために、MBSファイルをOpenText Core Application Security (Fortify on Demand) に提供します。

変換を実行するシステムと分析を実行するシステムの両方に同じバージョンのFortify Software Security Content (Rulepack) がインストールされている必要があります。



Note

スキャンマシンは特定のタイプのプロジェクトに対して依存関係を持っている場合があり、プラットフォーム非依存ではない場合があります。スキャンマシンに必要となる可能性がある依存関係の詳細については、「ソフトウェア要件」を参照してください。
Bicep、Solidity、Terraform (HCL)の各プロジェクトでは、最適な結果を得るためにインターネット接続が別途必要となります。

- モバイルビルドセッションバージョンの互換性
- モバイルビルドセッションの作成
- モバイルビルドセッションのインポート

48.1. モバイルビルドセッションバージョンの互換性

変換コンピュータ上のFortify SASTバージョンと分析コンピュータ上のFortify SASTバージョンに互換性がある必要があります。バージョン番号の形式は、<*major*>.<*minor*>.<*patch*>.<*build_number*> (26.3.0140など)です。変換コンピュータと分析コンピュータの両方でFortify SASTの<*major*>および<*minor*>部分が一致している必要があります。たとえば、26.3.0と26.3.xには互換性があります。Fortify SASTのバージョン番号を確認するには、コマンドラインで「`sourceanalyzer -v`」と入力します。

次のコマンドを使用してMBSファイルからビルドIDとFortify SASTバージョンを取得できます。

```
sourceanalyzer -import-build-session <file>.mbs -Dcom.fortify.sca.ExtractMobileInfo=true
```

48.2. モバイルビルドセッションの作成

変換を実行したコンピュータで次のコマンドを発行して、モバイルビルドセッションを生成します。

```
sourceanalyzer -b <build_id> -export-build-session <file>.mbs
```

ここで、`<file>.mbs` はFortify SASTのモバイルビルドセッションに指定するファイル名です。

48.3. モバイルビルドセッションのインポート

スキャンを実行するコンピュータに`<file>.mbs`ファイルを移動したら、モバイルビルドセッションをFortify SASTのプロジェクトルートディレクトリにインポートできます。

モバイルビルドセッションをインポートするには、次のコマンドを入力します。

```
sourceanalyzer -import-build-session <file>.mbs
```

Fortify SASTのモバイルビルドセッションをインポートしたら、分析フェーズに進むことができます。変換に使用されたときと同じビルドIDでスキャンを実行します。

複数のモバイルビルドセッションを単一のMBSファイルにマージすることはできません。エクスポートされたビルドセッションごとに、一意のビルドIDが必要です。ただし、同じFortify SASTのインストール時にすべてのビルドDがインポートされたら、 `-b` オプションを使用して1回のスキャンで複数のビルドDをスキャンできます(「分析フェーズ」を参照)。

Note
スキャンマシンは特定のタイプのプロジェクトに対して依存関係を持っている場合があります。スキャンマシンで必要となる可能性のある依存関係については、「ソフトウェア要件」を参照してください。
BicepおよびTerraform　(HCL)プロジェクトでは、最適な結果を得るためにインターネット接続が別途必要となります。

49. トラブルシューティング

- 終了コード
- メモリのチューニング
- 複雑な関数のスキャン
- 問題の非決定性
- ログファイルの場所の確認
- ログファイルの設定
- 問題の報告と機能拡張の要求

49.1. 終了コード

次の表に、取り得るFortify　SAST終了コードを示します。

終了コード	説明(Description)
0	成功
1	一般的な障害
2	入力ファイルが不正です (これは、Fortify SASTでサポートされていない拡張子を持つファイルの変換が試みられたことを示す場合があります)
3	プロセスがタイムアウトしました
4	分析が完了し、番号付きの警告メッセージがコンソールまたはログファイルに書き込まれました
5	分析が完了し、番号付きのエラーメッセージがコンソールまたはログファイルに書き込まれました
6	スキャンフェーズで問題の結果を生成できませんでした
7	有効なライセンスを検出できないか、または実行時にLICライセンスが期限切れになりました

デフォルトで、Fortify　SASTでは終了コード0、1、2、3、または7だけが返されます。

`com.fortify.sca.ExitCodeLevel` ファイル内の `<sast_install_dir>/Core/Config/fortify-sca.properties` プロパティを設定することで、デフォルトの終了コードオプションを拡張できます。

有効な値は次のとおりです。

- `nothing` —デフォルトの終了コード(0、1、2、3、または7)を返します。
- `warnings` —デフォルトの終了コードに加えて、終了コード4と5を返します。
- `errors` —デフォルトの終了コードに加えて、終了コード5を返します。
- `no_output_file` —デフォルトの終了コードに加えて、終了コード6を返します。

49.2. メモリのチューニング

スキャンに必要な物理RAMの量は、コードの複雑さによって異なります。デフォルトでは、システムで使用可能な物理メモリに基づいて、Fortify SASTにより使用するメモリが自動的に割り当てされます。通常はこれで十分です。出力オプションで説明するように、-Xmxコマンドラインオプションを使用してJavaヒープサイズを調整できます。

このセクションでは、分析中にOutOfMemoryエラーが発生した場合の解決方法について説明します。



Note

このセクションで説明するメモリ割り当てオプションを設定し、 `SCA_VM_OPTS` 環境変数を設定してすべてのスキャンに対して実行することができます。

- Javaヒープの枯渇
- ネイティブヒープの枯渇
- スタックオーバーフロー

49.2.1. Javaヒープの枯渇

Javaヒープの枯渇は、Fortify SASTスキャン時に発生する可能性のある最も一般的なメモリの問題です。これは、Fortify SASTでコードのスキャンに使用するJava仮想マシンに割り当てるヒープスペースが少なすぎるために発生します。次の症状からJavaヒープの枯渇を識別できます。

症状

これらのメッセージの1つ以上がFortify SASTログファイルとコマンドライン出力に出現します。

```
There is not enough memory available to complete analysis. For details on making more memory available, please consult the user manual. java.lang.OutOfMemoryError: Java heap space java.lang.OutOfMemoryError: GC overhead limit exceeded
```

解決策

Javaヒープの枯渇の問題を解決するには、スキャンの開始時にFortify SAST Java仮想マシンに多くのヒープ領域を割り当てます。ヒープサイズを大きくするには、Fortify SASTスキャンの実行時に `-Xmx` コマンドラインオプションを使用します。たとえば、 `-Xmx1G` は1GBを使用できるようにします。このパラメータを使用する前に、Javaヒープ領域で許容される最大値を決定してください。最大値は、使用可能な物理メモリによって異なります。

32 GB～48 GBのヒープサイズは、内部JVMの実装上推奨されていません。この範囲のヒープサイズでは、32 GBよりもパフォーマンスが低下します。32GB未満のヒープサイズはJVMによって最適化されます。スキャンで32GBを超えるサイズが必要な場合は、64GB以上が必要になります。ガイドラインとして、メモリを大量に消費するその他のプロセスが実行されていないと仮定すると、使用可能なメモリの2/3を超えて割り当てないでください。

システムがFortify SAST実行専用の場合は、変更する必要があります。ただし、メモリを大量に消費するその他のプロセスとシステムリソースが共有されている場合は、それらの他のプロセスの許容値を差し引いてください。



Note

常駐していても(Fortify SASTの実行中に)アクティブではないプロセスは、オペレーティングシステムがディスクにスワップする可能性があっても考慮する必要はありません。環境内で使用可能なメモリよりも多くの物理メモリをFortify SASTに割り当てると、「スラッシュ」が発生する可能性があります。この場合、通常はシステム上の他の機能とともにスキャンの速度が低下します。

49.2.2. ネイティブヒープの枯渇

ネイティブヒープの枯渇はまれなシナリオで、Java仮想マシンが起動時にJavaメモリ領域を割り当てできるものの、ネイティブ操作(ガーベジコレクションなど)のために残されたリソースがあまりに少なくなります。最終的には、プロセスが即座に終了する致命的なメモリ割り当てエラーが発生します。

症状

ネイティブヒープの枯渇は、Fortify SASTプロセスの異常終了およびコマンドラインでの次の出力により識別できます。

```
# A fatal error has been detected by the Java Runtime Environment: # # java.lang.OutOfMemoryError:
requested ... bytes for GrET ...
```

これは致命的なJava仮想マシンエラーであるため、通常は、作業ディレクトリにファイル名 hs_err_pidNNN.log で作成されたエラーログが伴います。

解決策

この問題はプロセス内で過大な負荷が発生していることが原因であるため、Javaメモリ領域(Javaヒープ)に使用されるメモリの量を減らすことが解決策です。この値を小さくすると、負荷の問題が減り、スキャンを正常に完了させることができます。

49.2.3. スタックオーバーフロー

Javaアプリケーションのスレッドごとに独自のスタックがあります。スタックには、戻りアドレス、関数/メソッド呼び出しの引数などが保持されます。スレッドが再帰的アルゴリズムを使用して大規模な構造体を処理する傾向がある場合、すべての戻りアドレスのために大きなスタックが必要になる場合があります。JVMでは、 -Xss オプションを使用してそのサイズを設定できます。

症状

通常、このメッセージはFortify　SASTログファイルに出現しますが、コマンドライン出力にも表示される場合があります。

```
java.lang.StackOverflowError
```

解決策

デフォルトのスタックサイズは16MBです。スタックサイズを大きくするには、 -Xss コマンドに sourceanalyzer オプションを渡します。たとえば、 -Xss32M を使用するとスタックが32MBに増えます。

49.3. 複雑な関数のスキャン

スキャン中に、Dataflow　Analyzerで分析を完了できない関数が出現し、次のメッセージをレポートする場合があります。

```
Function <name> is too complex for <analyzer> analysis and will be skipped (<identifier>)
```

ここで:

- <name> は、ソースコード関数の名前です。
- <analyzer> は、アナライザの名前です。
- <identifier> は、複雑性のタイプであり、次のいずれかになります。
  - l : 個別の場所が多すぎる
  - m : メモリ不足
  - s : スタックサイズが小さすぎる
  - t : 時間がかかりすぎる分析
  - v : 関数アクセス数が制限を超えた

Fortify SASTによる分析の深さは、利用可能なリソースに依存する場合があります。Fortify SASTは、複雑性のメトリックを使用して、これらのリソースと検出可能な脆弱性の数のバランスを取ります。このため、Fortify SASTが十分なリソースを使用できないと見なされる場合は、特定の関数の分析を中止することがあります。これは通常、「Function too complex」メッセージが表示される場合です。

このメッセージが表示されても、Fortify　SASTでプログラム内の機能が完全に無視されたことを意味するわけではありません。たとえば、Dataflow Analyzerでは通常、分析を完了するまでに何度も関数にアクセスするため、それまでのアクセスではこの複雑性の限界に達していない可能性があります。この場合、結果には、前回の訪問で学習した情報がすべて含まれます。

リミッタと呼ばれるFortify　SASTプロパティを使用して、「中止」ポイントを制御できます。アナライザごとに異なるリミッタが用意されています。

次のセクションでは、この問題の解決方法について説明します。

- Dataflow Analyzerのリミッタ
- 制御フローおよびNullポインタアナライザのリミッタ

49.3.1. Dataflow Analyzerのリミッタ

Dataflow Analyzerには、次の3種類の複雑性識別子があります。

- `l` : 個別の場所が多すぎる
- `m` : メモリ不足
- `s` : スタックサイズが小さすぎる
- `v` : 関数アクセス数が制限を超えた

`s` で識別される問題を解決するには、 `-Xss` を16MBを超える値に設定してスタックサイズを増やします。

複雑性識別子 `m` を解決するには、Fortify SASTの物理メモリを増やします。

複雑性識別子 `l` を解決するには、Fortify SASTプロパティファイル `<sast_install_dir>/Core/config/fortify-sca.properties` またはコマンドラインで次のリミッタを調整できます。

プロパティ名	デフォルト値
`com.fortify.sca.limiters.MaxTaintDefForVar`	1000
`com.fortify.sca.limiters.MaxTaintDefForVarAbort`	4000
`com.fortify.sca.limiters.MaxFieldDepth`	4

`MaxTaintDefForVar` リミッタは関数の複雑性を表すディメンションレス値ですが、 M は上限を示します。 `MaxFieldDepth` リミッタを使用して、Dataflow Analyzerが特定のオブジェクトを分析する際の精度を測定します。Fortify SASTは常に可能な限り最高の精度でオブジェクトの分析を試みます。

指定された関数が指定された精度で `MaxTaintDefForVar` 制限を超える場合、Dataflow Analyzerはその関数を(`MaxFieldDepth` リミッタを減らすことによって)低い精度で分析します。精度を低下させると、分析の複雑性が軽減されます。精度をさらに下げることができない場合、Fortify SASTは、分析が終了するか複雑性が `MaxTaintDefForVarAbort` リミッタを超えるまで、最低の精度で分析を続行します。言い換えれば、Fortify SASTでは関数から少なくとも何らかの結果を得るために、最低の精度で最善を尽くそうとします。Fortify SASTが `MaxTaintDefForVarAbort` リミッタに達すると、関数の分析が完全に中止され、「Function too complex」(関数が複雑すぎる)という警告が表示されます。

複雑性識別子 `v` を解決するには、 `com.fortify.sca.limiters.MaxFunctionVisits` プロパティを調整できます。このプロパティは、テイント伝播アナライザから関数にアクセスする最大回数を設定します。デフォルトは `50` です。

49.3.2. 制御フローおよびNullポインタアナライザのリミッタ

制御フローアナライザとNullポインタアナライザには、次の2種類の複雑性識別子があります。

- `m` : メモリ不足
- `t` : 時間がかかりすぎる分析

Dataflow Analyzerが関数の複雑性を処理する方法により、無限に時間がかかるという問題はありません。ただし、Control Flow AnalyzerとNull Pointer Analyzerは、複雑な関数を分析する際に非常に長い時間がかかる場合があります。そのため、Fortify SASTではこのような場合に分析を中止する方法が用意されていて、複雑性識別子 `t` で「Function too complex」というメッセージが表示されます。

これらのアナライザで関数分析に費やす最大時間を変更するには、Fortify SASTプロパティファイル `<sast_install_dir>/Core/config/fortify-sca.properties` またはコマンドラインで次のプロパティ値を調整できます。

プロパティ名	説明	デフォルト値
com.fortify.sca.CtrlflowMaxFunctionTime	単一の関数に制御フロー分析の時間制限(ミリ秒)を設定します。	600000 (10分)
com.fortify.sca.NullPtrMaxFunctionTime	単一の関数にNullポインタ分析の時間制限(ミリ秒)を設定します。	300000 (5分)

複雑性識別子 m を解決するには、Fortify SASTの物理メモリを増やします。

Note

これらのリミッタや時間設定を増やすと、複雑な関数の分析にかかる時間が長くなります。リミッタ/時間の特定の値における正確なパフォーマンスへの影響を具体的に示すのは、当該関数に依存するため困難です。「Function too complex」という警告を表示しないようにする場合は、リミッタ/時間を極めて高い値に設定できます。ただし、スキャン時間が許容できないものになる可能性があります。

49.4. 問題の非決定性

並行分析モードで実行すると、問題の非決定性が発生する可能性があります。問題が発生した場合は、カスタマサポートに問い合わせ、並行分析モードを無効にしてください。並行分析モードを無効にすると逐次分析になり、処理速度は大幅に低下しますが、複数回のスキャンで決定論的な結果が得られます。

並行分析モードを無効にするには、次の手順を実行します。

1. fortify-sca.properties ディレクトリにある <sast_install_dir>/Core/config ファイルをテキストエディタで開きます。
2. com.fortify.sca.MultithreadedAnalysis プロパティの値を false に変更します。

```
com.fortify.sca.MultithreadedAnalysis=false
```

49.5. ログファイルの場所の確認

今後、システム要件のドキュメントとリリースノートで -debug 、 -verbose 、および -debug-verbose オプションが非推奨となる予定です。GUIツールチームは、これらのオプションをツールで使用します。したがって、GUIツールチームにも知らせる必要があります。>>

デフォルトでは、Fortify SASTによって次の場所にログファイルが作成されます。

- Windows: C:\Users\<*username*>\AppData\Local\Fortify\sca<*version*>\log
- Windows以外: <*userhome*>/.fortify/sca<*version*>/log

ここで、 <*version*> は使用しているFortify SASTバージョンです。

次の表で、Fortify SASTのデフォルトのログファイルについて説明します。

ファイル名	説明(Description)
sca.log scaX.log	標準ログには、sourceanalyzerの実行時に発生した情報メッセージ、警告、およびエラーのログが記録されます。
sca_FortifySupport.log scaX_FortifySupport.log	Fortify SASTサポートログには、次の機能があります。 • 標準ログファイルと同じログメッセージに、詳細を追加 • 標準ログファイルに含まれていない追加の詳細メッセージ このログファイルは、カスタマサポートまたは開発チームが問題をトラブルシュートする場合に役立ちます。

コマンドラインでログファイルを指定するには、「その他のオプション」を参照してください。

解決できない警告またはエラーが発生した場合は、Fortify SAST Supportログファイルをカスタマサポートにお送りください。

49.6. ログファイルの設定

Fortify SASTでログファイルに書き込む情報を設定するには、ログプロパティを設定(「 ログプロパティ」を参照)し、*<sast_install_dir>*/Core/config/log4j2.xml ファイルを更新します。次のログファイル設定を指定できます。

- ログファイルの場所と名前
  プロパティ: com.fortify.sca.LogFile
- ログレベル(ログレベルについてを参照)
  プロパティ: com.fortify.sca.LogLevel
- sourceanalyzerを実行するごとにログファイルを上書きするかどうか
  プロパティ: com.fortify.sca.ClobberLogFile
  コマンドラインオプション: -clobber-log

log4j2.xml ファイルに変更を加える方法については、https://logging.apache.org/log4j/2.x/manual/index.html を参照してください。

ログレベルについて

選択したログレベルでは、そのレベルと同等以上のすべてのログメッセージが出力されます。次の表は、ログレベルを最低から最高の順に示しています。たとえば、デフォルトのログレベルであるINFOには、INFO、WARN、ERROR、および FATAL レベルのログメッセージが含まれます。 com.fortify.sca.LogLevel ファイル内の *<sast_install_dir>*/Core/config/fortify-sca.properties プロパティ、またはコマンドラインで -D オプションを使用して、ログレベルを設定できます。

ログレベル	説明(Description)
DEBUG	カスタマサポートまたは開発チームが問題のトラブルシューティングに使用できる情報を含む
INFO	変換またはスキャンプロセスに関する基本的な情報
WARN	変換またはスキャンが停止しなかったが、正確な結果を得るために注意が必要になる可能性がある問題に関する情報
ERROR	注意が必要になる可能性がある問題に関する情報
FATAL	変換またはスキャンが中止したエラーに関する情報

49.7. 問題の報告と機能拡張の要求

フィードバックは、この製品の成功に不可欠です。機能拡張やパッチを要求したり、問題を報告したりするには、カスタマサポート(https://www.microfocus.com/support)にアクセスしてください。

カスタマサポートに連絡する場合は、次の情報を含める必要があります。

- 製品: Fortify SAST
- Fortify SASTのバージョン番号および任意の独立したFortify SASTモジュール: バージョン番号を特定するには、次のコマンドを実行します。
  `sourceanalyzer -version`
- プラットフォーム: (たとえば、Red Hat Enterprise Linux <*version*>)
- オペレーティングシステム: (Linuxなど)

機能拡張を要求する場合は、機能拡張の説明を含めてください。

問題を報告する場合は、サポートが問題を再現できるよう十分な詳細を入力してください。説明が詳しくなるほど、サポートが問題を分析して解決するまでの時間を短縮できます。問題が発生したときのログファイル、またはログファイルで関連する部分も含めてください。

50. コマンドライン参照

このセクションでは、一般的なFortify SASTのコマンドラインオプションと分析対象のソースファイルを指定する方法について説明します。特定の言語に固有のコマンドラインオプションについては、その言語のセクションで説明します。

- ファイルとディレクトリの指定
- ディレクティブ
- 変換オプション
- 分析オプション
- 出力オプション
- その他のオプション

50.1. ファイルとディレクトリの指定

ファイル指定子は、ワイルドカード文字を使用して長いファイルリストまたはディレクトリをFortify SASTに渡すことができる式です。Fortify SASTでは、2種類のワイルドカード文字が認識されます。単一のアスタリスク文字(*)はファイル名の一部に一致し、二重のアスタリスク文字(**)はディレクトリに再帰的に一致します。1つ以上のファイル、1つ以上のファイル指定子、またはファイルとファイル指定子の組み合わせを指定できます。複数のファイル指定子はセミコロン (Windows) またはコロン(Windows以外)で区切ります。

ワイルドカードパターンを使用する場合、名前がピリオドで始まるファイルとディレクトリは、これらのエントリを非表示として扱うプラットフォームでもデフォルトで含まれます。これらのファイルとディレクトリが含まれないようにするには、明示的な除外を追加するか、 `com.fortify.LegacyHiddenGlobSyntax=true` を設定します。

```
<files> | <file_dir_specifiers>
```

Windowsおよび多くのLinuxのシェルでは、アスタリスク文字(*)を含むパラメータが自動的に展開されます。そのため、ファイル指定子の式を引用符で囲む必要があります。また、Windowsでは、スラッシュ(/)の代わりにバックスラッシュ(\)をディレクトリ区切り文字として使用することもできます。



Note

ファイル指定子は、コンパイラやビルド統合を必要とする言語には適用されません。

次の表には、ファイルおよびディレクトリ指定子の例を示します。

ファイルまたはディレクトリ指定子	説明(Description)
<dir> "*<dir>*/**/*"	名前付きディレクトリと任意のサブディレクトリ内またはディレクトリパラメータで使用時の名前付きディレクトリ内のすべてのファイルに一致します。
"*<dir>*/**/Example.java"	名前付きディレクトリまたは任意のサブディレクトリ内で見つかった Example.java という名前の任意のファイルに一致します。
"*<dir>*/*.java" "*<dir>*/*.jar"	名前付きディレクトリ内で見つかった指定した拡張子付きの任意のファイルに一致します。
"*<dir>*/**/*.kt" "*<dir>*/**/*.jar"	名前付きディレクトリまたは任意のサブディレクトリ内で見つかった指定した拡張子付きの任意のファイルに一致します。
"*<dir>*/**/beta/**"	パスに beta が含まれている(ファイル名として beta を含む)名前付きディレクトリ内で見つかったすべてのディレクトリおよびファイルに一致します。
"*<dir>*/**/classes/"	名前付きディレクトリおよび任意のサブディレクトリ内で見つかった classes という名前のすべてのディレクトリとファイルに一致します。
"**/test/**"	パスに test 要素が含まれている(ファイル名として test を含む)現在のディレクトリツリー内のすべてのファイルに一致します。
"**/test/**/*;**/build/**/*" または "**/test/**/*:**/build/**/*"	パスに test または build 要素が含まれている(ファイル名として test または build を含む)現在のディレクトリツリー内のすべてのファイルに一致します。
"**/webgoat/*"	現在のディレクトリツリーにある任意の webgoat ディレクトリ内のすべてのファイルに一致します。 一致する: • /src/main/java/org/owasp/webgoat • /test/java/org/owasp/webgoat 一致しない(assignments ディレクトリが一致しない) • /test/java/org/owasp/webgoat/assignments

50.2. ディレクティブ

一度に1つのディレクティブのみを使用します。ディレクティブを変換コマンドや分析コマンドと組み合わせて使用しないでください。次の表で説明するディレクティブを使用して、以前の変換コマンドに関する情報のリストを表示します。

ディレクティブ	説明(Description)
-clean	すべてのFortify SAST中間ファイルとビルドレコードを削除します。ビルドIDを指定すると、そのビルドIDに関連するファイルとビルドレコードのみが削除されます。
-show-binaries	他のバイナリの生成時に使用されていない、作成済みのすべてのオブジェクトが表示されます。ビルドに完全に統合されている場合は、作成されたバイナリがすべて表示されます。
-show-build-ids	既知のすべてのビルドIDのリストが表示されます。
-show-build-tree	-bin オプションを使用してスキャンすると、バイナリの作成に使用されたファイルと、それらのファイルの作成に使用されたファイルをすべてツリーレイアウトで表示します。-bin オプションが存在しない場合は、バイナリごとにツリーが表示されます。 **Note** このオプションを使用すると、大量の情報が生成される可能性があります。
-show-build-warnings	-b オプションを指定して使用すると、変換フェーズで発生したエラーおよび警告がコンソールに表示されます。 **Note** Fortify Audit Workbenchでは、これらのエラーおよび警告が結果証明書タブにも表示されます。
-show-files	指定したビルドIDに含まれているファイルが表示されます。-bin オプションが存在する場合は、バイナリに渡されたソースファイルのみが表示されます。
-show-loc	-b オプションを指定して使用すると、変換されたコードの行数が表示されます。
-regex-scan-minified	正規表現分析中に最小化されたJavaScriptファイルとTypeScriptファイルをスキャンするように、正規表現アナライザに指示します。デフォルトでは、最小化されたJavaScriptファイルおよびTypeScriptファイルは正規表現アナライザによってスキャンされません。

50.2.1. LIMライセンスディレクティブ

Fortify SASTでは、LIMライセンスの使用状況を管理するためのディレクティブが提供されています。LIMのライセンスプール資格情報を保存またはクリアできます。指定したライセンスプールでデタッチされたリースが許可されている場合は、オフライン分析用にデタッチされたリースを要求(およびリリース)することもできます。



Note

デフォルトでFortify SASTはLIMサーバにHTTPS接続する必要があり、信頼された証明書が必要です。詳細については、「信頼された証明書の追加」を参照してください。

次の表で説明するディレクティブは、LIMで管理されるライセンスに使用します。

LIMディレクティブ	説明(Description)

`-store-license-pool-credentials "<lim_url>|<lim_pool_name>|<lim_pool_pwd>|<proxy_url>|<proxy_user>|<proxy_pwd>"`	Fortify SASTでライセンスにLIMが使用されるように、LIMのライセンスプール資格情報を保存します。プロキシ情報はオプションです。Fortify SASTでは、このディレクティブで指定されたプールパスワードとプロキシ資格情報が `fortify-sca.properties` ファイルに暗号化されたデータとして保存されます。Fortify SASTのインストール後にライセンスプール資格情報が変更された場合は、このディレクティブを再度実行して新しい資格情報を保存できます。
	例:
	`sourceanalyzer -store-license-pool-credentials "`
	https://<*ip_address*>:<*port*>
	`|TeamA|mypassword"`
	関連付けられたプロパティ名:
	`com.fortify.sca.lim.Url`
	`com.fortify.sca.lim.PoolName`
	`com.fortify.sca.lim.PoolPassword`
	`com.fortify.sca.lim.ProxyUrl`
	`com.fortify.sca.lim.ProxyUsername`
	`com.fortify.sca.lim.ProxyPassword`

`-clear-license-pool-credentials`	LIMのライセンスプール資格情報を `fortify-sca.properties` ファイルから削除します。ライセンスプール資格情報が変更された場合は、このディレクティブを使用して削除してから、 `-store-license-pool-credentials` ディレクティブを使用して新しい資格情報を保存できます。
`-request-detached-lease <duration>`	このシステムで指定した期間(分単位)に排他的に使用されるように、LIMのライセンスプールからデタッチされたリースを要求します。これにより、企業のイントラネットから切断されている場合でもFortify SASTを実行できます。 **Note** このディレクティブを使用するには、デタッチされたリースが許可されるようにライセンスプールが設定されている必要があります。
`-release-detached-lease`	デタッチされたリースをライセンスプールに戻します。

50.3. 変換オプション

次の表は、ほとんどの変換コマンドで使用できる一般的な変換オプションについて説明しています。

変換オプション	説明(Description)
`-b <build_id>`	ビルドIDを指定します。Fortify SASTでは、ビルドIDを使用して、ビルドの一環としてコンパイルおよび結合されたファイルが追跡され、後でそれらのファイルがスキャンされます。 **同等のプロパティ名:** `com.fortify.sca.BuildID`
`-disable-language <languages>`	変換フェーズから除外する言語のコロン区切りリストを指定します。有効な言語の値は次のとおりです。 `abap`、`actionscript`、`apex`、`cfml`、`cobol`、`configuration`、`cpp`、`dart`、`dotnet`、`golang`、`objc`、`php`、`python`、`ruby`、`swift`、および`vb`。 **同等のプロパティ名:** `com.fortify.sca.DISabledLanguages`
`-enable-language <languages>`	変換する言語のコロン区切りリストを指定します。有効な言語の値は次のとおりです。 `abap`、`actionscript`、`apex`、`cfml`、`cobol`、`configuration`、`cpp`、`dart`、`dotnet`、`golang`、`objc`、`php`、`python`、`ruby`、`swift`、および`vb`。 **同等のプロパティ名:** `com.fortify.sca.EnabledLanguages`

`-exclude <file_specifiers>`	変換から除外するファイルを指定します。変換から除外されたファイルはスキャンもされません。複数のファイルパスはセミコロン(Windows)またはコロン(Windows以外)で区切ります。次の例では、任意の`Test`サブディレクトリ内のすべてのJavaファイルを除外します。
	`sourceanalyzer -b MyProject –cp "**/*.jar" "**/*" -exclude "**/Test/*.java"`
	ファイル指定子の使い方について詳しくは、ファイルとディレクトリの指定を参照してください。
	同等のプロパティ名:
	`com.fortify.sca.exclude`

-encoding <encoding_name>	ソースファイルのエンコーディングタイプを指定します。Fortify SASTでは、エンコードの異なるソースファイルを含むプロジェクトをスキャンできます。マルチエンコーディングされたプロジェクトを使用するには、Fortify SASTで最初にソースコードファイルが読み込まれる際に、変換フェーズで -encoding オプションを指定する必要があります。Fortify SASTでは、このエンコーディングがビルドセッションで記憶され、FVDLファイルに反映されます。 有効なエンコーディング名は java.nio.charset.Charset です。 通常、エンコーディングタイプを指定しないと、Fortify SASTではエンコーディングパラメータなしで file.encoding コンストラクタから java.io.InputStreamReader が使用されます。一部のケース(ActionScriptパーサの場合など)では、Fortify SASTのデフォルトは UTF-8 エンコーディングです。 **同等のプロパティ名:** com.fortify.sca.InputFileEncoding
-nc	コンパイラのコマンドラインの前に指定すると、Fortify SASTでソースファイルが変換されますが、コンパイラは実行されません。
-noextension-type <file_type>	拡張子がないソースファイルにファイルタイプを指定します。有効なファイルタイプの値は ABAP 、ACTIONSCRIPT 、 APEX 、 APEX_OBJECT 、 APEX_TRIGGER 、 ARCHIVE 、 ASPNET 、 ASP 、 ASPX 、 BITCODE 、 BSP 、 BYTECODE 、 CFML 、 COBOL 、 CSHARP 、 DART 、 DOCKERFILE 、 FLIGHT 、 GENERIC 、 GO 、 HCL 、 HOCON 、 HTML 、 INI 、 JAVA 、 JAVA_PROPERTIES 、 JAVASCRIPT 、 JINJA 、 JSON 、 JSP 、 JSPX 、 JUPYTER 、 KOTLIN 、 MSIL 、 MXML 、 OBJECT 、 PHP 、 PLSQL 、 PYTHON 、 RUBY 、 RUBY_ERB 、 SCALA 、 SWIFT 、 SWC 、 SWF 、 TLD 、 SQL 、 TSQL 、 TYPESCRIPT 、 VB 、 VB6 、 VBSCRIPT 、 VISUAL_FORCE 、 VUE 、 XML 、 YAML です。 .
-disable-compiler-resolution	ソースファイルとして変換中に、ビルドツールと同じ名前(gradlewなど)を持つビルドスクリプトファイルを含める場合に指定します。 **同等のプロパティ名:** com.fortify.sca.DisableCompilerName

`-project-root`	変換および分析フェーズで生成された中間ファイルを保存するディレクトリを指定します。Fortify SASTでは、このプロジェクトのルートディレクトリにある中間ファイルを広く活用します。場合によっては、このディレクトリをネットワークドライブではなくローカルストレージに配置すると、分析のパフォーマンスが向上します。 **同等のプロパティ名:** `com.fortify.sca.ProjectRoot`

50.4. 分析オプション

次の表では、一般的な分析オプション(通常は `-scan` を使用)について説明します。

分析オプション	説明(Description)
`-b <build_id>`	前の変換コマンドで使用されるビルドIDを指定します。 **同等のプロパティ名:** `com.fortify.sca.BuildID`
`-scan`	Fortify SASTで、指定したビルドIDのセキュリティ分析が実行されます。
`-scan-policy <policy_name>` | `-sc <policy_name>`	分析のためのスキャンポリシーを指定します。有効なポリシー名は、`classic`、`security`、および`devops`です。詳細については、「分析へのスキャンポリシーの適用」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.ScanPolicy`
`-analyzers <analyzer_list>`	アナライザのコロン区切りリストまたはカンマ区切りリストで有効にするアナライザを指定します。有効なアナライザ名は、`buffer`、`content`、`configuration`、`controlflow`、`dataflow`、`nullptr`、`semantic`、および`structural`です。このオプションを使用して、セキュリティ要件に必要ないアナライザを無効にすることができます。 **同等のプロパティ名:** `com.fortify.sca.DefaultAnalyzers`
`-p <level>` | `-scan-precision <level>`	短縮ダイヤルを使用して、スキャン精度レベルを指定してプロジェクトをスキャンします。スキャン精度レベルが低いほど、スキャンのパフォーマンスは高速になります。有効な値は、`1`、`2`、`3`、および`4`です。詳細については、「スキャン速度の設定」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.PrecisionLevel`
`-project-root`	変換および分析フェーズで生成された中間ファイルを保存するディレクトリを指定します。Fortify SASTでは、このプロジェクトのルートディレクトリにある中間ファイルを広く活用します。場合によっては、このディレクトリをネットワークドライブではなくローカルストレージに配置すると、分析のパフォーマンスが向上します。 **同等のプロパティ名:** `com.fortify.sca.ProjectRoot`

`-project-template <file>`	スキャンに使用する問題テンプレートファイルを指定します。これにより、ローカルコンピュータのスキャンのみが影響を受けます。FPRをFortify Software Security Centerにアップロードする場合は、アプリケーションバージョンに割り当てられた問題テンプレートが使用されます。 **同等のプロパティ名:** `com.fortify.sca.ProjectTemplate`
`-quick`	`fortify-sca-quickscan.properties` ファイルを使用してプロジェクトのクイックスキャンを実行し、重大な問題や優先度の高い問題がないか調べます。この方法では、分析の詳細さは低下します。デフォルトでは、クイックスキャンの場合、Buffer AnalyzerとControl Flow Analyzerが無効になります。さらに、Quick Viewフィルタセットも適用されます。詳細については、「クイックスキャン」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.QuickScanMode`
`-filter <file>`	結果フィルタファイルを指定します。詳細については、「結果の最適化」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.FilterFile`
`-bin <binary>` | `-binary-name <binary>`	スキャンするソースファイルのサブセットを指定します。ビルド時に名前付きバイナリにリンクされたソースファイルのみがスキャンに含められます。このオプションを複数回使用すると、スキャンに複数のバイナリが含まれるように指定できます。 **同等のプロパティ名:** `com.fortify.sca.BinaryName`
`-disable-default-rule-type <type>`	カスタムルールをテストするために使用します。デフォルトのRulepackで指定されたタイプのルールをすべて無効にします。このオプションを複数回使用すると、複数のルールタイプを指定できます。 `<type>` パラメータは、XMLタグからサフィックス `Rule` を除いた値です。たとえば、DataflowSourceRule要素の場合は `DataflowSource` を使用します。また、特性化ルールの特定のセクション(`Characterization:Control flow` 、`Characterization:Issue` 、 `Characterization:Generic` など)を指定することもできます。 `<type>` パラメータでは、大文字と小文字が区別されません。

`-no-default-issue-rules`	カスタムルールをテストするために使用します。問題が直接発生するデフォルトのRulepackでルールを無効にします。Fortify SASTでは、関数の動作を特徴付けるルールは引き続きロードされます。 **Note** これは、DataflowSink、Semantic、Controlflow、Structural、Configuration、Content、Statistical、Internal、Characterization:Issueルールタイプを無効にした場合と同等です。 **同等のプロパティ名:** `com.fortify.sca.NoDefaultIssueRules`
`-no-default-rules`	カスタムルールをテストするために使用します。デフォルトのRulepackからルールがロードされないようにします。Fortify SASTでは、説明要素と言語ライブラリのRulepackが処理されますが、ルールは処理されません。 **同等のプロパティ名:** `com.fortify.sca.NoDefaultRules`
`-no-default-source-rules`	カスタムルールをテストするために使用します。デフォルトのRulepackでソースルールを無効にします。 **Note** 特性化ソースルールは無効になりません。 **同等のプロパティ名:** `com.fortify.sca.NoDefaultSourceRules`
`-no-default-sink-rules`	カスタムルールをテストするために使用します。デフォルトのRulepackでシンクルールを無効にします。 **Note** 特性化シンクルールは無効になりません。 **同等のプロパティ名:** `com.fortify.sca.NoDefaultSinkRules`
`-rules <file>` | `<dir>`	カスタムのルールパックまたはディレクトリを指定します。このオプションを複数回使用すると、複数のRulepackファイルを指定できます。ディレクトリを指定すると、Fortify SASTでは、そのディレクトリ内の `.bin` および `.xml` の拡張子を持つすべてのファイルが含められます。 **同等のプロパティ名:** `com.fortify.sca.RulesFile`

`-regex-scan-minified`	正規表現分析中に最小化されたJavaScriptファイルとTypeScriptファイルをスキャンするように、正規表現アナライザに指示します。デフォルトでは、最小化されたJavaScriptファイルおよびTypeScriptファイルは正規表現アナライザによってスキャンされません。 **同等のプロパティ名:** `com.fortify.sca.regex.ScanMinifiedJS`

50.5. 出力オプション

次の表では、出力オプションについて説明します。これらのすべてのオプションを分析フェーズで適用します(`-scan` オプションも指定します)。 `build-label` 、 `build-project` 、および `build-version` オプションは、変換フェーズで指定できます。分析フェーズで再度指定すると、それらのオプションは上書きされます。

出力オプション	説明(Description)
`-f <file>` | `-output-file <file>`	分析結果が書き込まれるファイルを指定します。出力ファイルを指定しない場合は、Fortify SASTから端末に出力が書き込まれます。 **同等のプロパティ名:** `com.fortify.sca.ResultsFile`
`-format <format>`	出力形式を制御します。有効なオプションは、`fpr`、`fvdl`、`fvdl.zip`、`text`、および`auto`です。デフォルトは`auto`であり、`-f`オプションで指定されたファイルのファイル名拡張子に基づいて出力形式が選択されます。 FVDLは、Fortify SASTの詳細な分析結果が含まれるXMLファイルです。これには、脆弱性の詳細、ルールの説明、 コードスニペット、スキャン時に使用されるコマンドラインオプション、スキャンのエラーまたは警告が含まれています。 FPRは、FVDLファイル、およびスキャン時に使用されるソースコードのコピー、外部メタデータ、カスタムルール (該当する場合)などの追加情報が含まれる分析結果のパッケージです。Fortify Audit Workbenchは、自動的に .fpr 拡張子に関連付けられます。 **Note** 結果証明書を使用する場合は、`fpr`形式を指定する必要があります。結果証明書については、『*OpenText™ Fortify Audit Workbenchユーザガイド*』を参照してください。 一部の情報がFPRファイルまたはNFDLファイルに含まれないようにすると、スキャン時間や出力ファイルサイズを改善できます。この表のその他のオプション、および「FPRファイルの最適化」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.Renderer`

出力オプション	説明(Description)
-append	-f オプションで指定されたファイルに結果を追加します。結果のFPRファイルには、以前のスキャンによる問題と現在のスキャンによる問題が含まれています。ビルド情報およびプログラムデータ(ソースとシンクのリスト)セクションもマージされます。このオプションを使用するには、出力ファイルの形式を fpr または fvdl にする必要があります。 -format 出力オプションについては、この表の説明を参照してください。 (分析中のプログラムに関する情報とは異なり) Fortify Software Security Contentの情報、コマンドラインオプション、システムプロパティ、警告、エラー、Fortify SASTの実行に関するその他の情報を含むエンジンデータはマージされません。エンジンデータは -append オプションを使用してマージされないため、OpenTextでは、 -append で生成された結果が証明されません。 このオプションを指定しない場合は、Fortify SASTで新しい結果がFPRファイルに追加され、 previous の結果として古い結果にラベルが付けられます。 一般に、同時にアプリケーション全体を分析できない場合にのみ、 -append オプションを使用します。 **同等のプロパティ名:** com.fortify.sca.OutputAppend
-build-label <*label*>	分析結果に含めるプロジェクトのラベルを指定します。このオプションは、変換フェーズや分析フェーズ中に含めることができます。Fortify SASTでは、このラベルはコード分析に使用されません。変換と分析の両方にこのオプションを指定した場合、最後に指定したラベルだけが分析結果に渡されます。 **同等のプロパティ名:** com.fortify.sca.BuildLabel
-build-project <*project_name*>	分析結果に含めるプロジェクトの名前を指定します。このオプションは、変換フェーズや分析フェーズ中に含めることができます。Fortify SASTでは、この名前はコード分析に使用されません。 **同等のプロパティ名:** com.fortify.sca.BuildProject
-build-version <*version*>	分析結果に含めるプロジェクトのバージョンを指定します。このオプションは、変換フェーズや分析フェーズ中に含めることができます。Fortify SASTでは、このバージョンはコード分析に使用されません。 **同等のプロパティ名:** com.fortify.sca.BuildVersion

出力オプション	説明(Description)
-disable-source-bundling	ソースファイルを分析結果ファイルから除外します。分析結果にはスニペットが含まれます。 **同等のプロパティ名:** com.fortify.sca.FPRDisableSourceBundling
-fvdl-no-descriptions	Fortify Software Security Contentの説明を分析結果ファイルから除外します。 **同等のプロパティ名:** com.fortify.sca.FVDLDisableDescriptions
-fvdl-no-enginedata	エンジンデータを分析結果ファイルから除外します。エンジンデータには、Fortify Software Security Contentの情報、コマンドラインオプション、システムプロパティ、警告、エラー、およびFortify SASTの実行に関するその他の情報が含まれています。 **同等のプロパティ名:** com.fortify.sca.FVDLDisableEngineData
-fvdl-no-progdata	プログラムデータを分析結果ファイルから除外します。これにより、Fortify Audit Workbenchの関数ビューからテイントソース情報が削除されます。 **同等のプロパティ名:** com.fortify.sca.FVDLDisableProgramData
-fvdl-no-snippets	コードスニペットを分析結果ファイルから除外します。 **同等のプロパティ名:** com.fortify.sca.FVDLDisableSnippets

50.6. その他のオプション

次の表では、その他のオプションについて説明します。

その他のオプション	説明(Description)
`@<file>`	指定したファイルからコマンドラインオプションを読み込みます。プレーンテキストの*<file>*にはオプションとパラメータが含まれ、それぞれが各行に分離されています。 たとえば、`sourceanalyzer -b my_build_id -source 17 -cp lib.jar Test.java` コマンドを実行する代わりに、`sourceanalyzer @optfile.txt` を実行できます。ここで、`optfile.txt` は以下を含むファイルです: `"-b" "my_build_id" "-source" "17" "-cp" "lib.jar" "Test.java"`
`-h` | `-?` | `-help`	コマンドラインオプションの概要を出力します。
`-debug`	Fortify SAST Supportログファイルにデバッグ情報を含めます。この情報は、カスタマサポートによるトラブルシューティングにのみ役立ちます。 **同等のプロパティ名:** `com.fortify.sca.Debug`
`-debug-verbose`	これは `-debug` オプションと同じですが、特に解析エラーに関する詳細が含まれています。 **同等のプロパティ名:** `com.fortify.sca.DebugVerbose`
`-debug-mem`	パフォーマンス情報をFortify SAST Supportログの中に含めます。 **同等のプロパティ名:** `com.fortify.sca.DebugTrackMem`
`-verbose`	詳細ステータスメッセージをコンソールとFortify SAST Supportログファイルに送信します。 **同等のプロパティ名:** `com.fortify.sca.Verbose`
`-logfile <file>`	Fortify SASTで作成されるログファイルを指定します。デフォルトのログファイルの場所については、「ログファイルの場所」を参照してください。 **同等のプロパティ名:** `com.fortify.sca.LogFile`

その他のオプション	説明(Description)
`-clobber-log`	sourceanalyzerが実行されるたびにログファイルを上書きするようにFortify SASTに指示します。このオプションを指定しない場合は、Fortify SASTでログファイルに情報が追加されます。 **同等のプロパティ名:** `com.fortify.sca.ClobberLogFile`
`-quiet`	コマンドラインの進行状況情報を無効にします。 **同等のプロパティ名:** `com.fortify.sca.Quiet`
`-version` | `-v`	Fortify SASTのバージョンと、Fortify SASTと一緒に含まれているさまざまな独立したモジュールのバージョンが表示されます(その他の機能はすべて、Fortify SASTに含まれています)。
`-autoheap`	システムで使用可能な物理メモリに基づいて、メモリの自動割り当てを有効にします。これはデフォルトのメモリ割り当て設定です。
`-Xmx<size>M` | `G`	Fortify SASTで使用されるメモリ使用量の最大値を手動で指定します。 **Note** このオプションで最大メモリを手動で指定する代わりに、`-autoheap` で定義されたデフォルトのメモリ割り当て設定を使用するようにお勧めします。 32 GB～48 GBのヒープサイズは、内部JVMの実装上推奨されていません。この範囲のヒープサイズでは、32 GBよりもパフォーマンスが低下します。JVMでは、32 GB未満のヒープサイズが最適化されます。スキャンで32GBを超えるサイズが必要な場合は、64GB以上が必要になります。ガイドラインとして、メモリを大量に消費するその他のプロセスが実行されていないと仮定すると、使用可能なメモリの2/3を超えて割り当てないでください。 このオプションを指定する場合は、パフォーマンスが低下するため、物理的に使用可能なメモリよりも多く割り当てないでください。ガイドラインとして、メモリを大量に消費するその他のプロセスが実行されていないと仮定すると、使用可能なメモリの2/3を超えて割り当てないでください。

51. 環境設定オプション

Fortify SASTインストーラでは、一連のプロパティファイルがシステムに保存されます。プロパティファイルには、Fortify SASTのランタイム分析、出力、およびパフォーマンスに環境設定可能な設定が含まれています。

- プロパティファイル
- fortify-sca.properties
- fortify-sca-quickscan.properties
- fortify-rules.properties

51.1. プロパティファイル

プロパティファイルは、 <sast_install_dir>/Core/config ディレクトリに配置されています。インストールされたプロパティファイルには、デフォルト値が含まれています。プロパティファイルのプロパティを変更する前に、プロジェクトリーダーに相談することが推奨されています。環境設定ファイル内のプロパティはいずれも、任意のテキストエディタで変更できます。 -D オプションを使用して、コマンドラインでプロパティを指定することもできます。

次の表に、Fortify SASTプロパティファイルを示します。Fortify SASTアプリケーションおよびツールのプロパティファイルについては、『*OpenText™ Application Security ツールガイド*』を参照してください。

プロパティファイル名	説明(Description)	詳細情報
fortify-sca.properties	Fortify SAST環境設定プロパティを定義します。	fortify-sca.properties
fortify-sca-quickscan.properties	Fortify SASTのクイックスキャンに適用される環境設定プロパティを定義します。	fortify-sca-quickscan.properties
fortify-rules.properties	ルールの動作を決定する環境設定プロパティを定義します。	fortify-rules.properties

51.1.1. プロパティファイルの形式

プロパティファイルの各プロパティは、文字列のペアで構成されます。1番目の文字列はプロパティ名、2番目の文字列はプロパティ値です。

```
com.fortify.sca.fileextensions.htm=HTML
```

上記のように、プロパティでは .htm ファイルで使用される変換が設定されます。プロパティ名は com.fortify.sca.fileextensions.htm であり、値は HTML に設定されています。

Note

Windowsシステムのパスをプロパティ値として指定する場合は、バックスラッシュ文字(\)をバックスラッシュでエスケープする必要があります(例: com.fortify.sca.ASPVirtualRoots.Library=C:\\WebServer\\CustomerA\\inc)。

無効なプロパティは、プロパティファイルからコメントアウトされています。これらのプロパティを有効にするには、コメント記号(#)を削除してから、プロパティファイルを保存します。次の例では、プロパティファイルで com.fortify.sca.LogFile プロパティが無効であり、環境設定の一部ではありません。

```
# default location for the log file
#com.fortify.sca.LogFile=${com.fortify.sca.ProjectRoot}/sca/log/sca.log
```

51.1.2. 設定の上書き

Fortify SASTでは、プロパティ設定が特定の順序で使用されます。以前に設定したプロパティは、指定した値で上書きできます。プロパティファイルを変更する際は、この順序に注意してください。

次の表には、Fortify　SASTプロパティの優先順序を示します。

順序	プロパティの指定	説明(Description)
1	`-D` オプション付きのコマンドライン	コマンドラインで指定されたプロパティの優先度は最高であり、任意のスキャンで指定できます。
2	Fortify SASTのクイックスキャン環境設定ファイル	**Note** クイックスキャンとスキャン精度レベルのいずれかを指定できます。したがって、これらのプロパティ設定の優先度はどちらも2番目です。 クイックスキャン環境設定ファイル(`fortify-sca-quickscan.properties`)で指定されたプロパティの優先度は2番目ですが、 `-quick` オプションを付けてクイックスキャンモードが有効になっている場合に限られます。
	Fortify SASTのスキャン精度プロパティファイル	スキャン精度プロパティファイルで指定されたプロパティの優先度は2番目ですが、 `-scan-precision` オプションを付けてスキャン精度が有効になっている場合に限られます。
3	Fortify　SAST環境設定ファイル	Fortify SAST環境設定ファイル(`fortify-sca.properties`)で指定されたプロパティの優先度は最低です。すべてのスキャンでより永続的にプロパティ値が変更されるように、このファイルを編集します。

また、Fortify　SASTは内部でデフォルト値が定義されている一部のプロパティに依存します。

51.2. fortify-sca.properties

次のセクションでは、 `fortify-sca.properties` ファイルで使用できるプロパティについて説明します。このプロパティファイルで使用できるその他のプロパティについては、fortify-sca-quickscan.propertiesを参照してください。各プロパティの説明には、値の型、デフォルト値、同等のコマンドラインオプション(該当する場合)、および例が含まれます。

- 変換と分析フェーズのプロパティ
- 正規表現分析のプロパティ
- LIMライセンスのプロパティ
- ルールのプロパティ
- JavaおよびKotlinのプロパティ
- Visual　StudioおよびMSBuildプロジェクトのプロパティ
- JavaScriptおよびTypeScriptのプロパティ

- Pythonのプロパティ
- Goのプロパティ
- Rubyのプロパティ
- COBOLのプロパティ
- PHPのプロパティ
- ABAPのプロパティ
- FlexおよびActionScriptのプロパティ
- ColdFusion（CFML)のプロパティ
- SQLのプロパティ
- 出力のプロパティ
- モバイルビルドセッション(MBS)のプロパティ
- プロキシプロパティ
- ログプロパティ
- デバッグのプロパティ

51.2.1. 変換と分析フェーズのプロパティ

次の表に示す `fortify-sca.properties` ファイルのプロパティは、変換フェーズや分析(スキャン)フェーズに適用される一般的なプロパティです。

プロパティ名	説明(Description)
変換とスキャン	
com.fortify.sca.BuildI D	ビルドのビルドIDを指定します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -b
com.fortify.sca.CmdlineOptionsFileEncoding	@<filename> で指定されたコマンドラインオプションファイルのエンコードを指定します (「その他のオプション」を参照)。たとえば、このプロパティを使用して、オプションファイルでUnicodeのファイルパスを指定できます。有効なエンコード名は java.nio.charset.Charset で定義されています。 このプロパティは fortify-sca.properties ファイルでのみ有効であり、 fortify-sca-quickscan.properites ファイルや -D オプションでは機能しません。 **値の型:** 文字列 **デフォルト:** JVMシステムのデフォルトエンコーディング **例:** com.fortify.sca.CmdlineOptionsFileEncoding=UTF-8
com.fortify.sca.DISabledLanguages	変換フェーズから除外する言語のコロン区切りリストを指定します。有効な言語の値は次のとおりです。 abap 、 actionscript 、 apex 、 cfml 、 cobol 、 configuration 、 cpp 、 dart 、 dotnet 、 golang 、 objc 、 php 、 python 、 ruby 、 swift 、 および vb 。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -disable-language
com.fortify.sca.EnabledLanguages	変換する言語のコロン区切りリストを指定します。有効な言語の値は次のとおりです。 abap 、 actionscript 、 apex 、 cfml 、 cobol 、 configuration 、 cpp 、 dart 、 dotnet 、 golang 、 objc 、 php 、 python 、 ruby 、 swift 、 および vb 。 **値の型:** 文字列 **デフォルト:** com.fortify.sca.DISabledLanguages プロパティで明示的に除外しない限り、指定したソース内のすべての言語が変換されます。 **コマンドラインオプション:** -enable-language

com.fortify.sca.DisableCompilerName	trueに設定すると、Fortify SASTには、ソースファイルとして変換中に、ビルドツールと同じ名前(gradlewなど)を持つビルドスクリプトファイルが含められます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -disable-compiler-resolution
com.fortify.sca.ProjectRoot	変換および分析フェーズで生成された中間ファイルを保存するディレクトリを指定します。Fortify SASTでは、このプロジェクトのルートディレクトリにある中間ファイルを広く活用します。場合によっては、このディレクトリをネットワークドライブではなくローカルストレージに配置すると、分析のパフォーマンスが向上します。 **値の型:** 文字列(パス) **デフォルト(Windows):** ${win32.LocalAppdata}/Fortify ${win32.LocalAppdata}は、Windowsのローカルアプリケーションデータシェルフォルダをポイントする変数です。 **デフォルト(Windows以外):** $home/.fortify **コマンドラインオプション:** -project-root **例:** com.fortify.sca.ProjectRoot=C:\Users\<username>\AppData\Local\
変換	

com.fortify.sca.fileextensions.java

com.fortify.sca.fileextensions.cs

com.fortify.sca.fileextensions.js

com.fortify.sca.fileextensions.py

com.fortify.sca.fileextensions.rb

com.fortify.sca.fileextensions.aspx

com.fortify.sca.fileextensions.php

これは部分的なリストです。完全なリストについては、プロパティファイルを参照してください。

ビルド統合を必要としない言語の特定のファイル名拡張子を変換する方法を指定します。有効な拡張子の種類は、 ABAP 、 ACTIONSCRIPT 、 ADA 、 AI_RULES_FILES 、 APEX 、 APEX_OBJECT 、 APEX_TRIGGER 、 ARCHIVE 、 ASPNET 、 ASP 、 ASPX 、 BASH 、 BICEP 、 BITCODE 、 BSP 、 BYTECODE 、 CFML 、 CLOUDFORMATION 、 COBOL 、 CSHARP 、 DART 、 DELPHI 、 DOCKERFILE 、 ELIXIR 、 ERLANG 、 FLIGHT 、 FORTRAN 、 GENERIC 、 GO 、 GROOVY 、 HCL 、 HOCON 、 HTML 、 INI 、 JAVA 、 JAVA_PROPERTIES 、 JAVASCRIPT 、 JINJA 、 JSON 、 JSP 、 JSPX 、 JUPYTER 、 KOTLIN 、 LUA 、 MARKDOWN 、 MSIL 、 MXML 、 OBJECT 、 PERL 、 PHP 、 PLSQL 、 POWERSHELL 、 PYTHON 、 R 、 RUBY 、 RUBY_ERB 、 RUST 、 SCALA 、 SOLIDITY 、 SWIFT 、 SWC 、 SWF 、 TLD 、 SQL 、 TSQL 、 TYPESCRIPT 、 VB 、 VB6 、 VBSCRIPT 、 VISUAL_FORCE 、 VUE 、 XML 、 YAML です。

値の型: 文字列(有効な言語タイプ)

既定: 完全なリストについては、 fortify-sca.properties ファイルを参照してください。

例:

com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.cs=CSHARP
com.fortify.sca.fileextensions.js=TYPESCRIPT
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.swift=SWIFT
com.fortify.sca.fileextensions.razor=ASPNET
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.tf=HCL

oracle:<path_to_script> の値を指定して、言語タイプをプログラムで指定することもできます。指定した拡張子と一致するファイル名のコマンドラインパラメータを1つ受け入れるスクリプトを指定します。このスクリプトは、有効なFortify SASTファイルの種類(前のリストを参照)をstdoutに書き込み、戻り値0で終了する必要があります。ゼロ以外の戻りコードが返された場合、またはスクリプトが存在しない場合、このファイルは変換されず、ログファイルにFortify SASTの警告が書き込まれます。

例:
com.fortify.sca.fileextensions.jsp=oracle:<path_to_script>

com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter これは部分的なリストです。完全なリストについては、プロパティファイルを参照してください。	カスタム名のコンパイラを指定します。 **値の型:** 文字列(コンパイラ) **デフォルト:** 完全なリストについては、fortify-sca.properties ファイルの「Compilers」セクションを参照してください。 **例:** 「my-gcc」がgccコンパイラであることをFortify SASTに知らせるには、次のようにします。 com.fortify.sca.compilers.my-gcc=com.fortify.sca.util.compilers.GccCompiler • **メモ:** • コンパイラ名の先頭または末尾をアスタリスク(*)にして、0個以上の文字と一致させることができます。 • clang/clang++の実行は、gcc/g++コマンド名ではサポートされていません。次のように指定できます。 com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.UseAntListener	trueに設定すると、Fortify SASTによってコンパイラオプションに com.fortify.dev.ant.SCAListener が追加されます。 **値の型:** ブール値 **デフォルト:** false
com.fortify.sca.exclude	変換から除外するファイルを1つ以上指定します。複数のファイルはセミコロン(Windows)またはコロン(Windows以外)で区切ります。ファイル指定子の使い方について詳しくは、ファイルとディレクトリの指定を参照してください。 **値の型:** 文字列 **デフォルト:** 無効 **コマンドラインオプション:** -exclude **例:** com.fortify.sca.exclude=file1.x;file2.x

com.fortify.sca.InputFileEncoding	ソースファイルのエンコーディングタイプを指定します。Fortify SASTでは、異なる形式でエンコードされたソースファイルを含むプロジェクトをスキャンできます。マルチエンコーディングされたプロジェクトを使用するには、Fortify SASTで最初にソースコードファイルが読み込まれる際に、変換フェーズで -encoding オプションを指定する必要があります。Fortify SASTでは、このエンコーディングがビルドセッションで記憶され、FVDLファイルに反映されます。 通常、エンコーディングタイプを指定しないと、Fortify SASTではエンコーディングパラメータなしで file.encoding コンストラクタから java.io.InputStreamReader が使用されます。一部のケース(ActionScriptパーサの場合など)では、Fortify SASTのデフォルトは UTF-8 です。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -encoding **例:** com.fortify.sca.InputFileEncoding=UTF-16
com.fortify.sca.RegExecutable	Windowsプラットフォームでは、 reg.exe システムユーティリティへのパスを指定します。Cygwin内からFortify SASTを実行する場合でも、Cygwin構文ではなくWindows構文でパスを指定します。バックスラッシュをエスケープする場合は、バックスラッシュを追加します。 **値の型:** 文字列(パス) **デフォルト:** reg **例:** com.fortify.sca.RegExecutable=C:\\Windows\\System32\\reg.exe
com.fortify.sca.xcode.TranslateAfterError	xcodebuildサブプロセスがゼロ以外の終了コードで終了した場合にxcodebuildタッチレスアダプタが変換を続行するかどうかを指定します。falseに設定すると、xcodebuildでゼロ以外の終了コードが発生した後で変換が中止され、同じ終了コードでFortify SASTタッチレスビルドが停止します。trueにすると、Fortify SASTタッチレスビルドによってxcodebuildが終了する前に識別されたビルドファイルの変換が実行され、(他のエラーが発生しない限り)終了コード0でFortify SASTが終了します。 この設定に関係なく、ゼロ以外のコードでxcodebuildが終了した場合は、xcodebuildの終了コード、stdout、およびstderrがログファイルに書き込まれます。 **値の型:** ブール値 **デフォルト:** false
スキャン	

com.fortify.sca.AddImpliedMethods	trueに設定すると、Fortify　SASTで、継承による実装が発生した場合に暗黙的なメソッドが生成されます。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.alias.Enable	trueに設定すると、エイリアス分析が有効になります。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.analyzer.controlflow.EnableTimeOut	Control Flow Analyzerのタイムアウトを有効にするかどうかを指定します。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.BinaryName	スキャンするソースファイルのサブセットを指定します。ビルド時に名前付きバイナリにリンクされたソースファイルのみがスキャンに含められます。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -bin または -binary-name
com.fortify.sca.DefaultAnalyzers	実行する分析タイプのカンマまたはコロン区切りリストを指定します。このプロパティの有効な値は、buffer、content、configuration、controlflow、dataflow、nullptr、semantic、および structural です。 **値の型:** 文字列 **デフォルト:** このプロパティはコメントアウトされ、すべての分析タイプがスキャンで使用されます。 **コマンドラインオプション:** -analyzers
com.fortify.sca.DisableFunctionPointers	trueに設定すると、スキャン時に関数ポインタが無効になります。 **値の型:** ブール値 **デフォルト:** false
com.fortify.sca.EnableAnalyzer	デフォルトのアナライザに加えて、スキャンに使用するアナライザのカンマまたはコロン区切りのリストを指定します。このプロパティの有効な値は、buffer、content、configuration、controlflow、dataflow、nullptr、semantic、および structural です。 **値の型:** 文字列 **デフォルト:** (なし)

com.fortify.sca.EnableSubtraceFiltering	trueに設定した場合、問題が特定の問題のサブトレースである部分重複をフィルタで除外します。 たとえば、エンジンがトレースに関して2つの同様の問題を見つけた場合は、次のようになります。 A -> B -> C -> D B -> C -> D 2番目の問題は、1番目のサブトレースの重複として削除され、より長い問題だけが残されます。これは全体的に、より正確な問題です。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.ExitCodeLevel	デフォルトの終了コードオプションを拡張します。終了コードとこのプロパティの有効な値については、終了コードを参照してください。
com.fortify.sca.FilterFile	スキャンのフィルタファイルのパスを指定します。詳しくは、フィルタファイルについてを参照してください。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -filter
com.fortify.sca.FilteredInstanceIDs	フィルタファイルを使用して除外するIIDのカンマ区切りリストを指定します。 **値の型:** 文字列 **デフォルト:** (なし) **例:** com.fortify.sca.FilteredInstanceIDs=CA4E1623A2424919B98EC19FCA279FFA,4418B3DC072647158B3758E6183C14CD
com.fortify.sca.FilteredRuleLanguages	ルールを削除する言語のカンマ区切りリストまたはコロン区切りリストを指定します。有効な言語の値は次のとおりです。 abap、actionscript、apex、cfml、cobol、configuration、cpp、dart、dotnet、golang、objc、php、python、ruby、swift、および vb。 **値の型:** 文字列 **デフォルト:** (なし) **例:** com.fortify.sca.FileredRuleLanguages=apex:php
com.fortify.sca.MaxPassthroughChainDepth	関数呼び出しの入力パラメータと出力パラメータ間のテイントパスの長さを指定します。 **値の型:** 整数 **デフォルト:** 4

com.fortify.sca.MultithreadedAnalysis	Fortify SASTを並行分析モードで実行するかどうかを指定します。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.Phase0HigherOrder.Languages	高次分析を実行する言語のカンマ区切りリストを指定します。高次解析は、現代の動的言語で一般的に用いられる高次コードを通じて、データフローを追跡する能力を向上させます。有効な値は、 python 、 swift 、 ruby 、 javascript 、および typescript です。 **値の型:** 文字列 **デフォルト:** python,ruby,swift,javascript,typescript
com.fortify.sca.Phase0HigherOrder.Timeout.Hard	高次分析の合計時間(秒)を指定します。ハードタイムアウト制限に達すると、アナライザはすぐに終了します。 何らかの問題で分析時間が長くなりすぎる場合に備えて、このタイムアウト制限が推奨されています。固定ポイントのパスリミッタまたはソフトタイムアウトのいずれかが先に発生するように、ハードタイムアウトをソフトタイムアウトより約50%長く設定することをお勧めします。 **値の型:** 数値 **デフォルト:** 2700
com.fortify.sca.PrecisionLevel	スキャンの精度を指定します。スキャンの精度を下げると、実行速度が向上します。有効な値は、 1 、 2 、 3 、および 4 です。 **値の型:** 数値 **デフォルト:** (なし) **コマンドラインオプション:** -scan-precision | -p
com.fortify.sca.ProjectTemplate	スキャンに使用する問題テンプレートファイルを指定します。これにより、ローカルコンピュータのスキャンのみが影響を受けます。FPRをFortify Software Security Centerにアップロードする場合は、アプリケーションバージョンに割り当てられた問題テンプレートが使用されます。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -project-template **例:** com.fortify.sca.ProjectTemplate=test_issuetemplate.xml

com.fortify.sca.QuickScanMode	trueに設定すると、Fortify　SASTでクイックスキャンが実行されます。Fortify SASTでは、fortify-sca-quickscan.properties設定ファイルの代わりにfortify-sca.propertiesの設定が使用されます。 **値の型:** ブール値 **デフォルト:** (無効) **コマンドラインオプション:** -quick
com.fortify.sca.ScanPolicy	レポートされた脆弱性の優先順位を決めるためのスキャンポリシーを指定します(「分析へのスキャンポリシーの適用」を参照)。有効なスキャンポリシー値は、classic、security、およびdevopsです。 **値の型:** 文字列 **デフォルト:** security **コマンドラインオプション:** -scまたは-scan-policy
com.fortify.sca.ThreadCount	並行分析モードのスレッド数を指定します。リソース制約のために使用するスレッド数を減らす必要がある場合にのみ、このプロパティを追加します。スキャン時間の増加やスキャンに関する問題が発生した場合は、使用するスレッド数を減らして問題を解決できます。 **値の型:** 整数 **デフォルト:** (使用可能なプロセッサコア数)
com.fortify.sca.TypeInferenceFunctionTimeout	1つの関数の分析で型推論に使用できる時間(秒)。0に設定した場合、または指定しなかった場合は、無制限になります。 **値の型:** 倍精度 **デフォルト:** 60
com.fortify.sca.TypeInferenceLanguages	型推論を使用する言語のカンマまたはコロン区切りのリスト。この設定により、動的に型付けされた言語の分析精度が向上します。 **値の型:** 文字列 **デフォルト:** javascript,python,ruby,typescript
com.fortify.sca.TypeInferencePhase0Timeout	フェーズ0 (プロシージャ間分析)で型推論に使用できる合計時間(秒)を指定します。0に設定した場合、または指定しなかった場合は、無制限になります。 **値の型:** 倍精度 **デフォルト:** 300

com.fortify.sca.UniversalBlacklist	すべてのアナライザから隠す関数のコロン区切りリストを指定します。 **値の型:** 文字列 **デフォルト:** .*yyparse.*
com.fortify.LegacyHiddenGlobSyntax	* や ** などのファイル指定子にワイルドカードを使用して、Windows以外のプラットフォーム上の隠しファイルと隠しディレクトリを含めるかどうかを指定します。 以前のレガシ製品バージョンでは、名前がピリオド(.)で始まるLinuxのファイルとディレクトリは、コマンドラインで明示的に指定しない限り、一致とみなされませんでした。従来の動作を再有効化するにはこのプロパティを使用します。 デフォルトでは、現在の動作では、問題を引き起こすか不要なデータを追加することが分かっているため、除外するファイルとディレクトリを除くすべてのファイルとディレクトリが含まれます。 値の型: ブール値 デフォルト: false

51.2.2. 正規表現分析のプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、正規表現分析に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.regex.Enable	trueに設定すると、正規表現分析が有効になります。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.regex.ExcludeBinaries	trueに設定すると、正規表現分析からバイナリファイルが除外されます。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.regex.MaxSize	正規表現分析でスキャンされるファイルの最大サイズ(メガバイト単位)を指定します。この最大ファイルサイズを超えるファイルは正規表現分析から除外されます。 **値の型:** 数値 **デフォルト:** 10
com.fortify.sca.regex.ScanMinifiedJS	正規表現分析中に最小化されたJavaScriptファイルとTypeScriptファイルをスキャンします。デフォルトでは、Fortify SASTでこれらのファイルが正規表現分析から除外されます。 **値の型:** ブール値 **デフォルト:** False

正規表現分析

51.2.3. LIMライセンスのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、LIMでのライセンスに適用されます。

プロパティ名	説明(Description)
com.fortify.sca.lim.Url	LIMサーバのAPI URLを指定します。この値をテキストエディタで直接編集しないでください。この値を変更するには、コマンドラインオプションを使用します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -store-license-pool-credentials **例:** https://<*ip_address*>:<*port*>
com.fortify.sca.lim.PoolName	LIMライセンスプールの名前を指定します。この値をテキストエディタで直接編集しないでください。この値を変更するには、コマンドラインオプションを使用します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -store-license-pool-credentials
com.fortify.sca.lim.PoolPassword	LIMライセンスプールのパスワード(暗号化)を指定します。この値をテキストエディタで直接編集しないでください。この値を変更するには、コマンドラインオプションを使用します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -store-license-pool-credentials
com.fortify.sca.lim.ProxyUrl	LIMサーバへの接続に使用するプロキシサーバを指定します。 **値の型:** 文字列 **デフォルト:** (なし) **例:** http://proxy.example.com:8080 https://proxy.example.com **コマンドラインオプション:** -store-license-pool-credentials
com.fortify.sca.lim.ProxyUsername	LIMサーバに接続するためのプロキシ認証用の暗号化されたユーザ名を指定します。この値をテキストエディタで直接編集しないでください。この値を変更するには、コマンドラインオプションを使用します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -store-license-pool-credentials

プロパティ名	説明(Description)
com.fortify.sca.lim.ProxyPassword	LIMサーバに接続するためのプロキシ認証用の暗号化パスワードを指定します。この値をテキストエディタで直接編集しないでください。この値を変更するには、コマンドラインオプションを使用します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -store-license-pool-credentials
com.fortify.sca.lim.RequireTrustedSSLCert	trueに設定すると、信頼された証明書がない状態でLIMサーバに接続しようとしたときに失敗します。このプロパティをfalseに設定すると、信頼された証明書がない状態でLIMサーバに接続しようとしたときにメッセージが表示されます。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.lim.WaitForInitialLicense	trueに設定し、LIMライセンスプールの資格情報が保存されている場合、Fortify SASTではLIMライセンスが使用可能になるのを待機してから変換またはスキャンが開始されます。このプロパティをfalseに設定すると、LIMライセンスを取得できない場合にFortify SASTが中止します。 **値の型:** ブール値 **デフォルト:** true

LIMライセンスディレクティブ

51.2.4. ルールのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、ルール(およびカスタムルール)とRulepackに適用されます。

プロパティ名	説明(Description)
com.fortify.sca.DefaultRulesDir	OpenTextによって提供される暗号化ルールファイルの検索時に使用するディレクトリを設定します。 **値の型:** 文字列(パス) **デフォルト:** ${com.fortify.Core}/config/rules
com.fortify.sca.RulesFile	カスタムのルールパックまたはディレクトリを指定します。ディレクトリを指定すると、そのディレクトリ内の .bin および .xml 拡張子を持つすべてのファイルが含められます。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -rules
com.fortify.sca.CustomRulesDir	カスタムルールの検索時に使用するディレクトリを設定します。 **値の型:** 文字列(パス) **デフォルト:** ${com.fortify.Core}/config/customrules
com.fortify.sca.RulesFileExtensions	ルールファイルのファイル拡張子のリストを指定します。このリストに拡張子が含まれている <*sast_install_dir*>/Core/config/rules (または -rules オプションで指定されたディレクトリ)内のファイルが含められます。 .bin 拡張子は、このプロパティの値に関係なく常に含められます。このプロパティの区切り記号は、システムパスのセパレータです。 **値の型:** 文字列 **デフォルト:** .xml
com.fortify.sca.NoDefaultRules	trueに設定すると、デフォルトのルールパックのルールがロードされません。Fortify SASTでは、説明要素と言語ライブラリのルールパックが処理されますが、ルールは処理されません。 **値の型:** ブール値 **デフォルト:** (なし) **コマンドラインオプション:** -no-default-rules

プロパティ名	説明(Description)
com.fortify.sca.NoDefaultIssueRules	trueに設定すると、問題の直接の原因となるデフォルトのルールパックのルールが無効になります。Fortify SASTでは、関数の動作を特徴付けるルールは引き続きロードされます。これは、カスタムの問題ルールを作成するときに役立ちます。 **値の型:** ブール値 **デフォルト:** (なし) **コマンドラインオプション:** -no-default-issue-rules
com.fortify.sca.NoDefaultSourceRules	trueに設定すると、デフォルトのルールパックのソースルールが無効になります。これは、カスタムのソースルールを作成するときに役立ちます。 **Note** 特性化ソースルールは無効になりません。 **値の型:** ブール値 **デフォルト:** (なし) **コマンドラインオプション:** -no-default-source-rules
com.fortity.sca.NoDefaultSinkRules	trueに設定すると、デフォルトのルールパックのシンクルールが無効になります。これは、カスタムのシンクルールを作成するときに役立ちます。 **Note** 特性化シンクルールは無効になりません。 **値の型:** ブール値 **デフォルト:** (なし) **コマンドラインオプション:** -no-default-sink-rules

51.2.5. JavaおよびKotlinのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、JavaおよびKotlinコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.JavaClasspath	JavaまたはKotlinソースコードの分析時に使用するクラスパスを指定します。複数のパスはセミコロン(Windows)またはコロン(Windows以外)で区切ります。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -cp または -classpath
com.fortify.sca.JdkVersion	JavaまたはKotlin変換用のJavaソースコードのバージョンを指定します。 **値の型:** 文字列 **デフォルト:** 11 **コマンドラインオプション:** -jdk または -source
com.fortify.sca.CustomJdkDir	Fortify SASTインストール(*<sast_install_dir>*/Core/bootcp/)に含まれていないJDKバージョンを格納しているディレクトリを指定します。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -custom-jdk-dir
com.fortify.sca.JavaSourcepath	スキャンに含まれていないがネームレゾリューションに使用されるJavaまたはKotlinソースファイルディレクトリのセミコロン(Windows)またはコロン(Windows以外)区切りリストを指定します。ソースパスはクラスパスに似ていますが、解決にはクラスファイルではなくソースファイルが使用されます。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -sourcepath
com.fortify.sca.Appserver	JSPファイルを処理するアプリケーションサーバを指定します。有効な値は、 weblogic または websphere です。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -appserver

プロパティ名	説明(Description)
com.fortify.sca.AppserverHome	アプリケーションサーバのホームディレクトリを指定します。WebLogicの場合、これは server/lib を含むディレクトリへのパスです。WebSphereの場合、これは JspBatchCompiler スクリプトを含むディレクトリへのパスです。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -appserver-home
com.fortify.sca.AppserverVersion	WebLogicまたはWebSphereアプリケーションサーバのバージョンを指定します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -appserver-version
com.fortify.sca.JavaExtdirs	WebLogicおよびWebSphereアプリケーションサーバのクラスパスに暗黙的に含めるディレクトリを指定します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -extdirs
com.fortify.sca.JavaSourcepathSearch	trueに設定すると、Fortify SASTで、ターゲットファイルリストによって参照されるJavaソースファイルのみが変換されます。それ以外の場合、Fortify SASTではソースパスに含まれるすべてのファイルが変換されます。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.DefaultJarsDirs	一般的に使用されるJARファイルのディレクトリのセミコロンまたはコロン区切りリストを指定します。これらのディレクトリにあるJARファイルは、クラスパスオプション(-cp)の最後に追加されます。 **値の型:** 文字列 **デフォルト:** default_jars
com.fortify.sca.DecompileBytecode	trueに設定すると、Javaバイトコードが変換用に逆コンパイルされます。 **値の型:** ブール値 **デフォルト:** false

プロパティ名	説明(Description)
com.fortify.sca.jsp.UseSecurityManager	trueに設定すると、JSPパーサでJSPセキュリティマネージャが使用されます。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.jsp.DefaultEncoding	JSPのエンコードを指定します。 **値の型:** 文字列(エンコーディング) **デフォルト:** ISO-8859-1
com.fortify.sca.jsp.LegacyDataflow	trueに設定すると、JSP関連のデータフローに対する追加のフィルタリングが有効になり、誤検出の量が減少します。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -legacy-jsp-dataflow
com.fortify.sca.KotlinJvmDefault	本体がKotlinインターフェイスに入っているメソッドのDefaultImplsクラスの生成を指定します。有効な値は次のとおりです。 • disable — 本体を持つメソッドが含まれている各インターフェイスに対して、DefaultImplsクラスを生成するように指定します。 • all — インターフェイスにDefaultImplsの注釈が付く場合に、@JvmDefaultWithCompatibilityクラスを生成するように指定します。 • all-compatibility — インターフェイスにDefaultImplsの注釈が付かない限り、@JvmDefaultWithoutCompatibilityクラスを生成するように指定します。 **値の型:** 文字列 **デフォルト:** disable
com.fortify.sca.ShowUnresolvedSymbols	trueに設定すると、変換されたJavaソースファイルで参照されている未解決のタイプ、フィールド、および関数が、変換の最後に表示されます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -show-unresolved-symbols

Java、Kotlin、およびJSPプロジェクトの分析

51.2.6. Visual　StudioおよびMSBuildプロジェクトのプロパティ

次の表に示すfortify-sca.propertiesファイルのプロパティは、.NETプロジェクトおよびソリューションの変換に適用されます。

プロパティ名	説明(Description)
WinForms.TransformDataBindings WinForms.TransformMessageLoops WinForms.TransformChangeNotificationPattern WinForms.CollectionMutationMonitor.Label WinForms.ExtractEventHandlers	さまざまな.NETオプションを設定します。 **値の型:** ブール値および文字列 **デフォルトと例:** WinForms.TransformDataBindings=true WinForms.TransformMessageLoops=true WinForms.TransformChangeNotificationPattern=true WinForms.CollectionMutationMonitor.Label=WinFormsDataSource WinForms.ExtractEventHandlers=true
com.fortify.sca.ASPVirtualRoots.<*virtual_path*>	使用する仮想ルートへのフルパスのセミコロン区切りリストを指定します。 **値の型:** 文字列 **デフォルト:** (なし) **例:** com.fortify.sca.ASPVirtualRoots.Library=c:\\WebServer\\CustomerTwo\\Stuff com.fortify.sca.ASPVirtualRoots.Include=c:\\WebServer\\CustomerOne\\inc
com.fortify.sca.DisableASPExternalEntries	trueに設定すると、スキャンのASP外部エントリが無効になります。 **値の型:** ブール値 **デフォルト:** false

Visual StudioおよびMSBuildプロジェクトの変換

51.2.7. JavaScriptおよびTypeScriptのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、JavaScriptおよびTypeScriptコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.EnableDOMModeling	trueに設定すると、Fortify SASTで、変換フェーズ中にHTMLファイルによって生成されたDOMツリーをモデル化するJavaScriptコードが生成され、DOM関連の問題(クロスサイトスクリプティング(XSS)の問題など)が特定されます。変換するコードに、埋め込みまたは参照先のJavaScriptコードを含むHTMLファイルが含まれている場合は、このプロパティを有効にしてください。 このプロパティを有効にすると、変換時間が増える可能性があります。 **値の型:** ブール値 **デフォルト:** false
com.fortify.sca.DOMModeling.tags	com.fortify.sca.EnableDOMModeling プロパティをtrueに設定した場合は、Fortify SASTのDOMモデリングに含める追加のHTMLタグ名をカンマ区切りで指定できます。 **値の型:** 文字列 **デフォルト:** body 、 button 、 div 、 form 、 iframe 、 input 、 head 、 html 、および p 。 **例:** com.fortify.sca.DOMModeling.tags=ul,li
com.fortify.sca.JavaScript.src.domain.whitelist	Fortify SASTで参照先のJavaScriptファイルをスキャン用にダウンロードできる信頼されたドメイン名を指定します。URLの区切り記号として縦棒を使用します。 **値の型:** 文字列 **デフォルト:** (なし) **例:** com.fortify.sca.JavaScript.src.domain.whitelist=http://www.xyz.com|http://www.123.org
com.fortify.sca.DisableJavascriptExtraction	trueに設定すると、JSP、JSPX、PHP、およびHTMLファイルに埋め込まれたJavaScriptコードは抽出されず、スキャンされません。 **値の型:** ブール値 **デフォルト:** false
com.fortify.sca.EnableTranslationMinifiedJS	trueに設定すると、圧縮されたJavaScriptファイルの変換が有効になります。 **値の型:** ブール値 **デフォルト:** false

プロパティ名	説明(Description)
com.fortify.sca.skip.libraries.ES6 com.fortify.sca.skip.libraries.jQuery com.fortify.sca.skip.libraries.javascript com.fortify.sca.skip.libraries.typescript	変換されないJavaScriptまたはTypeScript技術ライブラリファイルのカンマまたはコロン区切りリストを指定します。ファイル名には正規表現を使用できます。'(-\d\.\d\.\d)?' プロパティ値に含まれる各ファイル名の .min.js または .js の前に、正規表現 com.fortify.sca.skip.libraries.jQuery が自動的に挿入されます。 **値の型:** 文字列 **デフォルト:** • ES6: es6-shim.min.js,system-polyfills.js,shims_for_IE.js • jQuery: jquery.js,jquery.min.js, jquery-migrate.js,jquery-migrate.min.js, jquery-ui.js,jquery-ui.min.js, jquery.mobile.js,jquery.mobile.min.js, jquery.color.js,jquery.color.min.js, jquery.color.svg-names.js, jquery.color.svg-names.min.js, jquery.color.plus-names.js, jquery.color.plus-names.min.js, jquery.tools.min.js • javascript: bootstrap.js,bootstrap.min.js,typescript.js,typescriptServices.js • typescript: typescript.d.ts,typescriptServices.d.ts
com.fortify.sca.follow.imports	trueに設定すると、importステートメントで組み込まれたファイルが変換に含められます。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.exclude.node.modules	trueに設定すると、node_modulesディレクトリ内のファイルは分析フェーズから除外されます。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.exclude.unimported.node.modules	node_modulesディレクトリ内のソースコードを除外するかどうかを指定します。trueに設定すると、インポートされたnode_modulesのみが変換に含められます。 このプロパティは、 com.fortify.sca.exclude.node.modules プロパティの値がfalseに設定されている場合にのみ適用されます。 **値の型:** ブール値 **デフォルト:** true

JavaScriptおよびTypeScriptコードの変換

51.2.8. Pythonのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、Pythonコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.PythonPath	追加のインポートディレクトリのセミコロン区切り(Windows)またはコロン区切り(Windows以外)リストを指定します。Fortify SASTでは、Pythonランタイムシステムでインポートファイルの検索に使用されるPYTHONPATH環境変数は考慮されません。このプロパティを使用して、追加のインポートディレクトリを指定します。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -python-path
com.fortify.sca.PythonVersion	スキャンするPythonソースコードのバージョンを指定します。有効な値は、2および3です。 **値の型:** 数値 **デフォルト:** 3 **コマンドラインオプション:** -python-version
com.fortify.sca.PythonNoAutoRootCalculation	trueに設定すると、モジュールとパッケージのインポートに使用するすべてのプロジェクトファイルに共通のルートディレクトリの自動計算が無効になります。詳しくは、「インポート済みのモジュールとパッケージを含める」を参照してください。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -python-no-auto-root-calculation
com.fortify.sca.DjangoTemplateDirs	Djangoテンプレートのディレクトリのセミコロン区切り(Windows)またはコロン区切り(Windows以外)リストを指定します。Fortify SASTでは、Djangoの settings.py ファイルのTEMPLATE_DIRS設定は使用されません。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -django-template-dirs
com.fortify.sca.DjangoDisableAutodiscover	Fortify SASTでDjangoテンプレートを自動検出しないことを指定します。 **値の型:** ブール値 **デフォルト:** (なし) **コマンドラインオプション:** -django-disable-autodiscover

プロパティ名	説明(Description)
com.fortify.sca.JinjaTemplateDirs	Jinja2テンプレートのディレクトリのセミコロン区切り(Windows)またはコロン区切り(Windows以外)リストを指定します。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -jinja-template-dirs
com.fortify.sca.DisableTemplateAutodiscover	Fortify SASTでDjangoまたはJinja2テンプレートを自動検出しないことを指定します。 **値の型:** ブール値 **デフォルト:** (なし) **コマンドラインオプション:** -disable-template-autodiscover

Pythonコードの変換

51.2.9. Goのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、Goコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.gotags	Goプロジェクトのカスタムビルドタグを指定します。これは、 go コマンドの -tags オプションに相当します。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** - -gotags
com.fortify.sca.GOPATH	プロジェクト/ワークスペースのルートディレクトリを指定します。 **値の型:** 文字列 **デフォルト:** (GOPATHシステム環境変数)
com.fortify.sca.GOROOT	Goインストールの場所を指定します。 **値の型:** 文字列 **デフォルト:** (GOROOTシステム環境変数)
com.fortify.sca.GOPROXY	1つ以上のプロキシURLをカンマ区切りで指定します。 direct または off を指定することもできます。 **値の型:** 文字列 **デフォルト:** (GOPROXYシステム環境変数)

Goコードの変換

51.2.10. Rubyのプロパティ

次の表に示す `fortify-sca.properties` ファイルのプロパティは、Rubyコードの変換に適用されます。

プロパティ名	説明(Description)
`com.fortify.sca.RubyLibraryPaths`	Rubyライブラリを含むディレクトリへのパスを1つ以上指定します。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** `-ruby-path`
`com.fortify.sca.RubyGemPaths`	RubyGemsの場所へのパスを1つ以上指定します。プロジェクトにスキャンするgemが関連付けられている場合は、この値を設定します。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** `-rubygem-path`

Rubyコードの変換

51.2.11. COBOLのプロパティ

次の表に示す `fortify-sca.properties` ファイルのプロパティは、COBOLコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.cobol.legacy.enabled	trueに設定すると、ローカルCOBOL変換が有効になり、AI COBOLは無効になります。 falseに設定すると、ローカルCOBOL変換が無効になり、AI COBOLが有効になります。 設定されていない場合、com.fortify.sca.ai.provider または com.fortify.sca.ai.db.url が設定されていればAI COBOLが有効になります。それ以外の場合は、ローカルCOBOL変換が有効になります。 **デフォルト**: null
com.fortify.sca.CobolCopyDirs	Fortify SASTでコピーブックファイルを検索する、1つ以上のディレクトリをセミコロン区切りまたはコロン区切りで指定します。 **値の型**: 文字列(パス) **デフォルト**: (なし) **コマンドラインオプション**: -copydirs
com.fortify.sca.CobolDialect	COBOLの方言を指定します。方言の有効な値は、COBOL390 または MICROFOCUS です。方言の値では、大文字と小文字を区別しません。 **値の型**: 文字列 **デフォルト**: COBOL390 **コマンドラインオプション**: -dialect
com.fortify.sca.CobolCheckerDirectives	1つ以上のCOBOLチェッカディレクティブをセミコロン区切りで指定します。 **値の型**: 文字列 **デフォルト**: (なし) **コマンドラインオプション**: -checker-directives
com.fortify.sca.CobolLegacy	trueに設定すると、レガシーCOBOL変換が有効になります。 **値の型**: ブール値 **デフォルト**: false **コマンドラインオプション**: -cobol-legacy
com.fortify.sca.CobolFixedFormat	trueに設定すると、固定形式のCOBOLが指定され、すべてのコード行のカラム8〜72のソースコードのみを検索するようにFortify SASTに指示されます(レガシーCOBOL変換のみ)。 **値の型**: ブール値 **デフォルト**: false **コマンドラインオプション**: -fixed-format

プロパティ名	説明(Description)
com.fortify.sca.CobolCopyExtensions	1つ以上のコピーブックファイル拡張子をセミコロン区切りまたはコロン区切りで指定します(レガシーCOBOL変換のみ)。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -copy-extensions

COBOLコードの変換

51.2.12. PHPのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、PHPコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.PHPVersion	PHPのバージョンを指定します。有効なバージョンのリストについては、「サポートされる言語」を参照してください。 **値の型:** 文字列 **デフォルト:** 8.2 **コマンドラインオプション:** -php-version
com.fortify.sca.PHPSourceRoot	PHPのソースルートを指定します。 **値の型:** ブール値 **デフォルト:** (なし) **コマンドラインオプション:** -php-source-root

PHPコードの変換

51.2.13. ABAPのプロパティ

次の表に示すプロパティは、ABAPコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.AbapDebug	trueに設定すると、Fortify SASTでメッセージをデバッグするためにABAPステートメントが追加されます。 **値の型:** ブール値 **デフォルト:** (なし)
com.fortify.sca.AbapIncludes	Fortify SASTでABAPのINCLUDEディレクティブが検出されたときに、名前付きディレクトリが検索されます。 **値の型:** 文字列(パス) **デフォルト:** (なし)

51.2.14. FlexおよびActionScriptのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、FlexおよびActionScriptコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.FlexLibraries	「リンク先」のライブラリをセミコロン(Windows)またはコロン(Windows以外)で区切って指定します。このリストには、flex.swc、framework.swc、およびplayerglobal.swcを含める必要があります(これらは通常、Flex SDKルートのframeworks/libsディレクトリにあります)。このプロパティは、主にActionScriptを解決するために使用します。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -flex-libraries
com.fortify.sca.FlexSdkRoot	有効なFlex SDKのルートの場所を指定します。このフォルダには、flex-config.xmlファイルを含むフレームワークフォルダが含まれている必要があります。bin実行可能ファイルを含むmxmlcフォルダも含まれている必要があります。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -flex-sdk-root
com.fortify.sca.FlexSourceRoots	Flexプロジェクトの追加のソースディレクトリを指定します。複数のディレクトリはセミコロン(Windows)またはコロン(Windows以外)で区切ります。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -flex-source-root

51.2.15. ColdFusion (CFML)のプロパティ

次の表に示すfortify-sca.propertiesファイルのプロパティは、CFMLコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.CfmlUndefinedVariablesAreTainted	trueに設定すると、Fortify SASTでCFMLページ内の未定義の変数が汚染されたものとして処理されます。これは、register-globals-style脆弱性を監視するDataflow Analyzerに対するヒントとして機能します。ただし、このプロパティを有効にすると、インクルードページ内の変数がそれ以前に発生したインクルードページ内の汚染された値に初期化されるデータフローの検出に支障をきたします。 **値の型:** ブール値 **デフォルト:** false
com.fortify.sca.CaseInsensitiveFiles	trueに設定すると、大文字と小文字を区別しないファイルシステムを使用して開発され、大文字と小文字が区別されるファイルシステム上でスキャンされたアプリケーションでは、CFMLファイルの大文字と小文字が区別されなくなります。 **値の型:** ブール値 **デフォルト:** (無効)
com.fortify.sca.SourceBaseDir	ColdFusionプロジェクトのベースディレクトリを指定します。 **値の型:** 文字列(パス) **デフォルト:** (なし) **コマンドラインオプション:** -source-base-dir

ColdFusionコードの変換

51.2.16. SQLのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、SQLコードの変換に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.SqlLanguage	SQL言語のバリアントを指定します。有効なSQL言語タイプの値は、 PLSQL (Oracle PL/SQLの場合)および TSQL (Microsoft T-SQLの場合)です。 **値の型:** 文字列 **デフォルト:** TSQL **コマンドラインオプション:** -sql-language

SQLの変換

51.2.17. 出力のプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、分析出力に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.ResultsFile	結果が書き込まれるファイル。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -f **例:** com.fortify.sca.ResultsFile=MyResults.fpr
com.fortify.sca.Renderer	出力形式を制御します。有効な値は、fpr、fvdl、text、および auto です。auto のデフォルトでは、-f オプションで指定されたファイルの拡張子に基づいて出力形式が選択されます。 **値の型:** 文字列 **デフォルト:** auto **コマンドラインオプション:** -format
com.fortify.sca.OutputAppend	trueに設定すると、Fortify SASTで既存の結果ファイルに結果が追加されます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -append
com.fortify.sca.ResultsAsAvailable	trueに設定すると、Fortify SASTで使用可能になった結果が出力されます。これは、(出力ファイルを指定するための) -f オプションを指定せずに、stdoutに出力する場合に役立ちます。 **値の型:** ブール値 **デフォルト:** false
com.fortify.sca.BuildLabel	スキャンされたプロジェクトのラベルを指定します。Fortify SASTでは、このラベルは使用されませんが、結果に含められます。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -build-label
com.fortify.sca.BuildProject	スキャンされたプロジェクトの名前を指定します。Fortify SASTでは、この名前は使用されませんが、結果に含められます。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -build-project

プロパティ名	説明(Description)
com.fortify.sca.BuildVersion	スキャンされたプロジェクトのバージョンを指定します。Fortify SASTでは、このバージョン番号は使用されませんが、結果に含められます。 **値の型:** 文字列 **デフォルト:** (なし) **コマンドラインオプション:** -build-version
com.fortify.sca.MachineOutputMode	情報をインタラクティブに出力せずに、スクリプトまたはFortify SASTツールで使用できる形式で出力します。スキャンの進行状況を1行で表示せずに、コンソールの前の行の下に新しい行を出力して、更新された進行状況を表示します。 **値の型:** ブール値 **デフォルト:** (無効) **コマンドラインオプション:** -machine-output
com.fortify.sca.SnippetContextLines	問題の周囲に表示するコードの行数を設定します。スニペットでは常に、エラーが発生した行の両側にある2行のコードが含められます。デフォルトでは、5行のコードが表示されます。 **値の型:** 数値 **デフォルト:** 2
com.fortify.sca.FVDLDisableDescriptions	trueに設定すると、分析結果ファイル(FVDL)からFortify Software Security Centerの説明が除外されます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -fvdl-no-descriptions
com.fortify.sca.FVDLDisableEngineData	trueに設定すると、分析結果ファイル(FVDL)からエンジンデータが除外されます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -fvdl-no-enginedata
com.fortify.sca.FVDLDisableLabelEvidence	trueに設定すると、分析結果ファイル(FVDL)からラベル証拠が除外されます。 **値の型:** ブール値 **デフォルト:** false

プロパティ名	説明(Description)
com.fortify.sca.FVDLDisableProgramData	trueに設定すると、分析結果ファイル(FVDL)から ProgramData セクションが除外されます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -fvdl-no-progdata
com.fortify.sca.FVDLDisableSnippets	trueに設定すると、分析結果ファイル(FVDL)からコードスニペットが除外されます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -fvdl-no-snippets
com.fortify.sca.FVDLStylesheet	分析結果のスタイルシートの場所を指定します。 **値の型:** 文字列(パス) **デフォルト:** ${com.fortify.Core}/resources/sca/fvdl2html.xsl

51.2.18. モバイルビルドセッション(MBS)のプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、MBSファイルに適用されます。

プロパティ名	説明(Description)
com.fortify.sca.MobileBuildSessions	falseに設定すると、Fortify SASTはソースファイルをビルドセッションディレクトリにコピーしません。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.ExtractMobileInfo	trueに設定すると、Fortify SASTでモバイルビルドセッションからビルドIDとFortify SASTのバージョン番号が抽出されます。 **Note** Fortify SASTでは、このプロパティを使用してもモバイルビルドは抽出されません。 **値の型:** ブール値 **デフォルト:** false

モバイルビルドセッション

51.2.19. プロキシプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、プロキシ設定に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.https.proxyHost	プロキシホスト名を指定します。 **値の型:** 文字列 **デフォルト:** (なし)
com.fortify.sca.https.proxyPort	プロキシポート番号を指定します。 **値の型:** 数値 **デフォルト:** (なし)

51.2.20. ログプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、ログファイルに適用されます。

プロパティ名	説明(Description)
com.fortify.sca.LogFile	デフォルトのログファイルの名前と場所を指定します。 **値の型:** 文字列(パス) **デフォルト:** ${com.fortify.sca.ProjectRoot}/log/sca.log および ${com.fortify.sca.ProjectRoot}/log/sca_FortifySupport.log **コマンドラインオプション:** -logfile
com.fortify.sca.LogLevel	両方のログファイルの最小ログレベルを指定します。有効な値は、DEBUG、INFO、WARN、ERROR、および FATAL です。詳しくは、ログファイルへのアクセスおよびログファイルの設定を参照してください。 **値の型:** 文字列 **デフォルト:** INFO
com.fortify.sca.ClobberLogFile	trueに設定すると、Fortify SASTでsourceanalyzerを実行するたびにログファイルが上書きされます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -clobber-log
com.fortify.sca.PrintPerformanceDataAfterScan	trueに設定すると、Fortify SASTでスキャンの完了後にパフォーマンス関連のデータがFortify SAST Supportログファイルに書き込まれます。デバッグモードでは、この値は自動的にtrueに設定されます。 **値の型:** ブール値 **デフォルト:** false

ログファイルの設定

51.2.21. デバッグのプロパティ

次の表に示す fortify-sca.properties ファイルのプロパティは、デバッグ設定に適用されます。

プロパティ名	説明(Description)
com.fortify.sca.Debug	Fortify SAST Supportログファイルにデバッグ情報を含めます。この情報は、カスタマサポートによるトラブルシューティングにのみ役立ちます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -debug
com.fortify.sca.DebugVerbose	これは com.fortify.sca.Debug プロパティと同じですが、特に解析エラーに関する詳細が含まれています。 **値の型:** ブール値 **デフォルト:** (無効) **コマンドラインオプション:** -debug-verbose
com.fortify.sca.Verbose	trueに設定すると、Fortify SAST Supportログファイルに詳細メッセージが含められます。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -verbose
com.fortify.sca.DebugTrackMem	trueに設定すると、追加のパフォーマンス情報がFortify SAST Supportログに書き込まれます。 **値の型:** ブール値 **デフォルト:** (無効) **コマンドラインオプション:** -debug-mem
com.fortify.sca.CollectPerformanceData	trueに設定すると、パフォーマンスを追跡する追加のタイマが有効になります。 **値の型:** ブール値 **デフォルト:** (無効)
com.fortify.sca.Quiet	trueに設定すると、コマンドラインの進行状況情報が無効になります。 **値の型:** ブール値 **デフォルト:** false **コマンドラインオプション:** -quiet
com.fortify.sca.MonitorSca	trueに設定すると、Fortify SASTのメモリ使用量が監視され、JVMガーベッジコレクションが過剰に発生したときに警告が表示されます。 **値の型:** ブール値 **デフォルト:** true

51.3. fortify-sca-quickscan.properties

Fortify SASTでは、クイックスキャンと呼ばれるより詳細なスキャンが提供されています。このオプションでは、[redacted]/-sca-quickscan.properties ファイルのプロパティ値を使用して、プロジェクトがクイックスキャンモードでスキャンされます。デフォルトでは、クイックスキャンによって分析の深さが減少し、Quick Viewフィルタセットが適用されます。Quick Viewフィルタセットでは、優先度の高い重大な問題のみが提供されます。



Note

このファイルのプロパティは、スキャンのコマンドラインで -quick オプションを指定した場合にのみ使用されます。

次の表には、2つのデフォルト値セット(クイックスキャンのデフォルト値と通常スキャンのデフォルト値)を示します。デフォルト値が1つのみ表示されている場合は、通常スキャンとクイックスキャンの両方の値が同じです。

プロパティ名	説明(Description)
com.fortify.sca.CtrlflowMaxFunctionTime	単一の関数に制御フロー分析の時間制限(ミリ秒)を設定します。 **値の型:** 整数 **クイックスキャンのデフォルト:** 30000 **デフォルト:** 600000
com.fortify.sca.DisableAnalyzers	スキャン時に無効にするアナライザのカンマ区切りリストまたはコロン区切りリストを指定します。有効なアナライザ名は、buffer、content、configuration、controlflow、dataflow、nullptr、semantic、および structural です。 **値の型:** 文字列 **クイックスキャンのデフォルト:** controlflow:buffer **デフォルト:** (なし)
com.fortify.sca.FPRDisableMetatable	Fortify Audit Workbenchで関数ビューの情報を含むメタテーブルの作成を無効にします。このメタテーブルでは、ソースウィンドウで変数を右クリックして宣言を表示できます。C/C++のスキャンに非常に長い時間がかかる場合は、このプロパティをtrueに設定すれば、スキャン時間が数時間短縮される可能性があります。 **値の型:** ブール値 **クイックスキャンのデフォルト:** true **デフォルト:** false **コマンドラインオプション:** -disable-metatable
com.fortify.sca.FPRDisableSourceBundling	FPRファイルにソースコードが含まれることを無効にします。スキャン時にFortify SASTでマーク付きのソースコードファイルが生成されないようにします。クイックスキャンの結果として生成されるFPRファイルをFortify Software Security Centerにアップロードする場合は、このプロパティを false に設定する必要があります。 **値の型:** ブール値 **クイックスキャンのデフォルト:** true **デフォルト:** false **コマンドラインオプション:** -disable-source-bundling
com.fortify.sca.NullPtrMaxFunctionTime	単一の関数にNullポインタ分析の時間制限(ミリ秒)を設定します。標準のデフォルトは5分間です。この値を短い制限に設定すると、スキャン時間全体が短縮されます。 **値の型:** 整数 **クイックスキャンのデフォルト:** 10000 **デフォルト:** 300000

プロパティ名	説明(Description)
com.fortify.sca.TrackPaths	制御フロー分析のパストラッキングを無効にします。パスパストラッキングでは、問題に関するより詳細なレポートが提供されますが、より長いスキャン時間が必要です。これをJSPでのみ無効にするには、NoJSPに設定します。すべての関数を無効にするには、Noneを指定します。 **値の型:** 文字列 **クイックスキャンのデフォルト:** (なし) **デフォルト:** NoJSP
com.fortify.sca.limiters.ConstraintPredicateSize	Buffer Analyzerで複雑な計算にサイズ制限を指定します。スキャン時間を改善するためにBuffer Analyzerで指定されたサイズ値より大きい計算をスキップします。 **値の型:** 整数 **クイックスキャンのデフォルト:** 10000 **デフォルト:** 500000
com.fortify.sca.limiters.MaxChainDepth	Dataflow Analyzerでデータが追跡される呼び出しの最大深さを制御します。この値を大きくしてデータフロー分析の範囲を拡大すると、スキャン時間が長くなります。 **Note** 呼び出しの深さは、プログラムのエントリポイント(main() など)からの呼び出しの深さではなく、テイントソースとシンク間にあるデータフローパス上の呼び出しの最大深さを示します。 **値の型:** 整数 **クイックスキャンのデフォルト:** 3 **デフォルト:** 5
com.fortify.sca.limiters.MaxFunctionVisits	テイント伝播アナライザから関数にアクセスされる回数を設定します。 **値の型:** 整数 **クイックスキャンのデフォルト:** 5 **デフォルト:** 50

プロパティ名	説明(Description)
com.fortify.sca.limiters.MaxPaths	単一のデータフロー脆弱性についてレポートするパスの最大数を制御します。この値を変更しても、検出される結果は変更されません。個々の結果で表示されるデータフローパスの数のみが表示されます。 **Note** このプロパティを 5 より大きい値に設定することは、スキャン時間が長くなる可能性があるため、推奨されていません。 **値の型:** 整数 **クイックスキャンのデフォルト:** 1 **デフォルト:** 5
com.fortify.sca.limiters.MaxTaintDefForVar	Dataflow Analyzerに複雑さの制限を設定します。データフローでは、この複雑さメトリックを特定の精度レベルで超える関数の分析精度が徐々に減少します。この値は、変数チェーンに対して追跡されるテイントの量を制御します。 **値の型:** 整数 **クイックスキャンのデフォルト:** 250 **デフォルト:** 1000
com.fortify.sca.limiters.MaxTaintDefForVarAbort	関数の複雑さにハード制限を設定します。関数の複雑性が最小精度レベルでこの制限を超える場合は、アナライザで関数の分析がスキップされます。 **値の型:** 整数 **クイックスキャンのデフォルト:** 500 **デフォルト:** 4000

51.4. fortify-rules.properties

このトピックでは、 fortify-rules.properties ファイルで使用できるプロパティについて説明します。

結果の改善

これらのプロパティを使用して、新しいルールセットの有効化、ルールのフィルタリング、またはOpenText DASTによる結果の相関関係の有効化など、スキャン結果の動作を変更します。

プロパティ名	説明(Description)
com.fortify.sca.rules.EnableRuleComments	trueに設定すると、// FortifyRemove() コメントを使用して、結果に問題が表示されるのを阻止できます。詳細については、「FortifyRemoveコメントを使ったフィルタリング」を参照してください。 **値の型:** ブール値 **デフォルト:** true
com.fortify.sca.rules.IsLibrary	trueに設定すると、すべてのパブリック関数変数にWEB、XSS、およびPRIVATEテイントを追加する新しいエントリポイントルールがコードで有効になります(特定の除外が適用されます)。(現在のところ、JavaおよびJVM言語のみ適用されます) **値の型:** ブール値 **デフォルト:** false
com.fortify.sca.rules.enablePQCRules	trueに設定すると、Post-Cryptographicの脅威に関連する問題を特定するルールが有効になります。サポートされている言語やライブラリなど、詳細については、セキュリティコンテンツの更新とドキュメントを参照してください。 **値の型:** ブール値 **デフォルト:** false

DASTの相関関係と検証

プロパティ名	説明(Description)
com.fortify.sca.rules.enable_wi_correlation	trueに設定し、サポートされているフレームワークを持つアプリケーションをFortify SASTでスキャンすると、OpenText™ Dynamic Application Security Testingにインポートして結果を改善できる結果ファイルが生成されます。 **値の型:** ブール値 **デフォルト:** false

Google Cloud Functionの統合

Google Cloud Functionsをスキャンすると、JSONまたはYAMLのクラウドビルド設定ファイルを提供するか、以下の表のプロパティを設定して結果を最適化します。

プロパティ名	説明(Description)
com.fortify.sca.rules.GCPFunctionName	JSON/YAMLのCloud Build設定ファイルが存在しない場合に呼び出されるサーバレス関数の名前。 **値の型:** 文字列 **デフォルト:** (なし)
com.fortify.sca.rules.GCPHttpTrigger	trueに設定した場合、スキャンされるクラウド関数はHTTPトリガです。 **値の型:** ブール値 **デフォルト:** false

正規表現をカスタマイズするプロパティ

コード内の脆弱性を特定するために多くの手法が使われますが、コード内の識別子を見つけるために正規表現に頼るルールもあり、これらは多くの場合、プロパティによって設定できます。次の表は、ルールで使用される正規表現を変更するために使用できるプロパティのリストを示しています。

正規表現とシェル構文の衝突を防ぐため、コマンドラインに直接設定するのではなく、 fortify-rules.properties ファイル内でこれらの設定を行うことが勧められています。

プロパティ名	説明(Description)
com.fortify.sca.rules.password_regex.global	言語固有のルールプロパティが設定されている場合を除き、すべての言語のパスワード識別子に一致する正規表現。 **値の型:** 文字列 **デフォルト:** (?i)(s|_)?(user|usr|member|admin|guest|login|default|new|current|old|client|server|proxy|sql|server|my|mysql|mongo|mongodb|db|database|ldap|smtp|email|email(_)?smtp)?(_|\.)?pass(wd|word|phrase)|secret)
com.fortify.sca.rules.password_regex.abap	ABAPコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.actionscript	ActionScriptコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.apex	Salesforce Alesコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.cfml	ColdFusion（CFML)コードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (なし)
com.fortify.sca.rules.password_regex.cobol	COBOLコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)

com.fortify.sca.rules.password_regex.config	XMLのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。正規表現修飾子は使用しないでください。この値では、大文字と小文字が区別されません。 **値の型:** 文字列 **デフォルト:** (s|_)?(user|usr|member|admin|guest|login|default|new|current|old|client|server|proxy|sqlserver|my|mysql|mongo|mongodb|db|database|ldap|smtp|email|email(_)?smtp)?(_|\.)?pass(wd|word|phrase)
com.fortify.sca.rules.password_regex.cpp	CおよびC++コードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.dart	Dartコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.dotnet	.NETコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.docker	Dockerfileのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** .*pass(wd|word|phrase).*
com.fortify.sca.rules.password_regex.golang	Goコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)

com.fortify.sca.rules.password_regex.java	Javaコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.javascript	JavaScriptおよびTypeScriptコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.json	JSONのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (?i).*pass(wd|word|phrase).*
com.fortify.sca.rules.password_regex.jsp	JSPコードのパスワード識別子に一致するために使用される正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.objc	Objective-CおよびObjective-C++コードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (?i)(s|_)?(user|usr|member|admin|guest|login|default|new|current|old|client|server|proxy|sql|server|my|mysql|mongo|mongodb|db|database|ldap|smtp|email|email(_)?smtp)?(_|\.)?(token|pin|pass(wd|word|phrase))
com.fortify.sca.rules.password_regex.php	PHPコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)

com.fortify.sca.rules.password_regex.powershell	PowerShellファイル内のパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (?i)([a-z_]*|\{.*)(pass(wd|word|phrase)|pwd)(.*\}|[a-z_]*)
com.fortify.sca.rules.password_regex.properties	プロパティファイルのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.python	Pythonコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.ruby	Rubyコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.sql	SQLコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.swift	Swiftコードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (?i)(s|_)?(user|usr|member|admin|guest|login|default|new|current|old|client|server|proxy|sqlserver|my|mysql|mongo|mongodb|db|database|ldap|smtp|email|email(_)?smtp)?(_|\.)?(token|pin|pass(wd|word|phrase))

com.fortify.sca.rules.password_regex.vb	VB6コードのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.password_regex.global の値)
com.fortify.sca.rules.password_regex.yaml	YAMLのパスワード識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現パスワードルールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (?i).*pass(wd|word|phrase).*
com.fortify.sca.rules.key_regex.global	言語固有の正規表現キールールプロパティが設定されている場合を除き、すべての言語のキー識別子に一致する正規表現。 **値の型:** 文字列 **デフォルト:** (?i)((enc|dec)(ryption|rypt)?|crypto|secret|private)(_)?key
com.fortify.sca.rules.key_regex.abap	ABAPコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.actionscript	ActionScriptコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.cfml	CFMLコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.cpp	CおよびC++コードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)

com.fortify.sca.rules.key_regex.golang	Goコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.java	Javaコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.javascript	JavaScriptおよびTypeScriptコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.jsp	JSPコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.objc	Objective-CおよびObjective-C++コードのキー識別子と照合するために使用する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.php	PHPコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.python	Pythonコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)

com.fortify.sca.rules.key_regex.ruby	Rubyコードのキー識別子と照合するために使用される正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.sql	SQLコードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.swift	Swiftコードのキー識別子と照合するために使用される正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)
com.fortify.sca.rules.key_regex.vb	Visual Basic 6コードのキー識別子に一致する正規表現。このプロパティを設定すると、グローバル正規表現キールールプロパティが上書きされます。 **値の型:** 文字列 **デフォルト:** (com.fortify.sca.rules.key_regex.global の値)

52. コマンドラインツール

Fortify SASTコマンドラインツールを使用すると、Fortify Software Security Contentの管理、インストール後の設定、スキャンの監視を実行できます。これらのツールは、 <sast_install_dir>/bin にあります。Windows用のツールは、 .bat または .cmd ファイルとして提供されます。次の表では、Fortify SASTと一緒にインストールされるコマンドラインツールについて説明します。



Note

デフォルトでは、Fortify SASTツールのログファイルは次のディレクトリに書き込まれます。

- Windows: C:\Users\<username>\AppData\Local\Fortify\<tool_name>-<version>\log
- Windows以外: <userhome>/.fortify/<tool_name>-<version>/log

ツール	説明(Description)	詳細情報
fortifyupdate	インストールされているセキュリティコンテンツを現在のバージョンと比較し、必要に応じてアップデートします	Fortify Software Security Contentのアップデートについて
FPRUtility	このツールを使用すると、次の処理を実行できます。 • 監査されたプロジェクトをマージする • FPR署名を検証する • FPRファイルからの情報を表示する • ソースコードファイルと監査プロジェクトをFPRファイルに結合または分割する • FPRを変更する	*OpenText™ Application Security ツールガイド*
scapostinstall	このツールを使用すると、Fortify SASTの以前のバージョンのpropertiesファイルを移行したり、ロケールを指定したり、セキュリティコンテンツの更新やFortify Software Security Centerに使用するプロキシサーバを指定したりできます。	インストール後処理ツールの実行
SCAState	分析フェーズ中にJVMに関する状態分析情報を提供します。	SCAStateを使用したスキャンステータスの確認

- OpenText Application Security Contentの更新について
- SCAStateを使用したスキャンステータスの確認

52.1. OpenText Application Security Contentの更新について

fortifyupdateコマンドラインツールを使用して、最新のFortify Secure Coding RulepacksとメタデータをOpenTextからダウンロードできます。

fortifyupdateツールは、Fortify SASTインストールに含まれている既存のセキュリティコンテンツに関する情報を収集し、この情報を使用してFortify Rulepack更新サーバに問い合わせます。サーバは新しいセキュリティコンテンツまたは更新されたセキュリティコンテンツを返し、古いセキュリティコンテンツをFortify SASTインストールから削除します。インストールが最新の場合は、その旨のメッセージが表示されます。

- OpenText Application Security Contentの更新
- fortifyupdateコマンドラインオプション

52.1.1. OpenText Application Security Contentの更新

fortifyupdateコマンドラインツールを使用して、セキュリティコンテンツをダウンロードするか、セキュリティコンテンツのローカルコピーをインポートします。このツールは *<sast_install_dir>*/bin ディレクトリにあります。

このツールのデフォルトの読み込みタイムアウトは180秒です。タイムアウト設定を変更するには、rulepackupdate.SocketReadTimeoutSeconds 環境設定ファイルに server.properties プロパティを追加します。詳細については、『*OpenText™ Application Security ツールガイド*』を参照してください。

fortifyupdateの基本的なコマンドライン構文を次の例に示します。

```
fortifyupdate [<options>]
```

Fortify Rulepack更新サーバからの最新のFortify Secure Coding Rulepacksおよび外部メタデータを使用してFortify SASTインストールを更新するには、次のコマンドを入力します。

```
fortifyupdate
```

ローカルシステムからセキュリティコンテンツを更新するには、次のコマンドを入力します。

```
fortifyupdate -import <my_local_rules>.zip
```

資格情報を使用してFortify Software Security Centerサーバからセキュリティコンテンツを更新するには、次のコマンドを入力します。

```
fortifyupdate -url <ssc_url> -sscUser <username> -sscPassword <password>
```

52.1.2. fortifyupdateコマンドラインオプション

次の表では、fortifyupdateオプションについて説明します。

fortifyupdateオプション	説明(Description)
-acceptKey	公開鍵を受諾する場合に指定します。このオプションを指定すると、公開鍵の入力を求めるプロンプトは表示されません。-urlオプションを使って非標準の場所からFortify Software Security Contentを更新する場合は、このオプションを使用して公開鍵を受諾します。
-acceptSSLCertificate	サーバによって提供されるSSL証明書を使用する場合に指定します。
-import <*file*>.zip	セキュリティコンテンツを含むZIPファイルをインポートします。デフォルトでは、Rulepackが<*sast_install_dir*>/Core/config/rulesディレクトリにインポートされます。
-coreDir <*dir*>	fortifyupdateで更新が保存されるコアディレクトリを指定します。このオプションが指定されていない場合、fortifyupdateによる更新は<*sast_install_dir*>で実行されます。 **Important** <*sast_install_dir*>/config/keysフォルダのコンテンツをコピーして、このディレクトリ内のconfig/keysフォルダに貼り付けしてから、fortifyupdateを実行してください。
-includeMetadata	外部メタデータのみを更新することを指定します。
-includeRules	ルールパックのみを更新することを指定します。

fortifyupdateオプション	説明(Description)
-locale <*locale*>	ロケールを指定します。指定したロケールにセキュリティコンテンツが存在しない場合は、英語がデフォルトです。有効な値は次のとおりです。 • en (英語) • es (スペイン語) • ja (日本語) • ko (韓国語) • pt_BR (ポルトガル語(ブラジル)) • zh_CN (簡体字中国語) • zh_TW (繁体字中国語) **Note** この値では、大文字と小文字を区別しません。 または、 fortify.properties 環境設定ファイルでセキュリティコンテンツ更新のデフォルトロケールを指定できます。詳細については、『*OpenText™ Application Security ツールガイド*』を参照してください。
-proxyhost <*host*>	プロキシサーバのネットワーク名またはIPアドレスを指定します。
-proxyport <*port*>	プロキシサーバのポート番号を指定します。
-proxyUsername <*username*>	プロキシサーバが認証を必要とする場合、ユーザ名を指定します。
-proxyPassword <*password*>	プロキシサーバが認証を必要とする場合、パスワードを指定します。
-showInstalledRules	現在インストールされているRulepackを、カスタムルールとカスタムメタデータを含めて表示します。
-showInstalledExternalMetadata	現在インストールされている外部メタデータを表示します。
-url <*url*>	セキュリティコンテンツをダウンロードするURLを指定します。デフォルトのURLは、 https://update.fortify.com 、または server.properties 環境設定ファイル内の rulepackupdate.server プロパティに設定された値です。 server.properties 環境設定ファイルの詳細については、『*OpenText™ Application Security ツールガイド*』を参照してください。 Fortify Software Security Center URLを指定することで、Fortify Software Security Centerサーバからセキュリティコンテンツをダウンロードできます。

fortifyupdateオプション	説明(Description)
-urlオプションを使ってFortify Software Security Centerからセキュリティコンテンツを更新する場合には、次のいずれかのタイプの資格情報を指定します。	
-sscUsername -sscPassword	ユーザ名とパスワードでFortify Software Security Centerユーザアカウントを指定します。
-sscAuthToken	タイプがUnifiedLoginToken、CIToken、またはToolsConnectTokenのFortify Software Security Center認証トークンを指定します。

52.2. SCAStateを使用したスキャンステータスの確認

SCAStateツールを使用して、分析フェーズ中に最新の状態分析情報を確認します。状

態を確認するには:

1. スキャンを開始します。
2. 別のコマンドウィンドウを開きます。
3. コマンドプロンプトで次のコマンドを入力します。

```
SCAState [<options>]
```

SCAStateコマンドラインオプション

52.2.1. SCAStateコマンドラインオプション

次の表では、SCAStateオプションについて説明します。

SCAStateオプション	説明(Description)
`-a` | `--all`	使用可能なすべての情報を表示します。
`-debug`	SCAStateの振る舞いをデバッグする場合に役立つ情報を表示します。
`-ftd` | `--full-thread-dump`	各スレッドのスレッドダンプを出力します。
`-h` | `--help`	SCAStateツールのヘルプ情報を表示します。
`-hd <filename>` | `--heap-dump <filename>`	ヒープダンプの書き込みファイルを指定します。このファイルはリモートスキャンの作業ディレクトリを基準に解釈されます。これは必ずしもSCAStateを実行しているディレクトリとは限りません。
`-liveprogress`	実行中のスキャンの現在のステータスを表示します。これはデフォルトです。可能であれば、この情報は別の端末ウィンドウに表示されます。
`-nogui`	別のウィンドウではなく、現在の端末ウィンドウにFortify SASTの状態情報を表示します。
`-pi` | `--program-info`	スキャン中のソースコードに関する情報(含まれるソースファイルと関数の数など)が表示されます。
`-pid <process_id>`	現在実行中のFortify SASTプロセスIDを指定します。複数のFortify SASTプロセスが同時に実行されている場合は、このオプションを使用します。 Windowsシステム上でプロセスIDを取得するには、次の手順を実行します。 1. コマンドウィンドウを開きます。 2. コマンドプロンプトで「`tasklist`」と入力します。プロセスのリストが表示されます。 3. リスト内で`java.exe`プロセスを見つけ、PIDをメモします。 Linuxシステム上でプロセスIDを取得するには、次の手順を実行します。 • コマンドプロンプトで「`ps aux | grep sourceanalyzer`」と入力します。
`-progress`	コマンドが発行された時点までのスキャン情報を表示します。これには、経過時間、分析の現在のフェーズ、および取得済みの結果数が含まれます。

SCAStateオプション	説明(Description)
`-properties`	環境設定を表示します(パスワードなどの機密情報は含まれません)。
`-scaversion`	現在実行中のsourceanalyzerのFortify SASTバージョン番号を表示します。
`-td` | `--thread-dump`	メインスキャンスレッドのスレッドダンプを出力します。
`-timers`	Fortify SASTで計測されるタイマおよびカウンタからの情報を表示します。
`-version`	SCAStateバージョンを表示します。
`-vminfo`	JVM標準MXBeansで提供される、ClassLoadingMXBean、CompilationMXBean、GarbageCollectorMXBeans、MemoryMXBean、OperatingSystemMXBean、RuntimeMXBean、およびThreadMXBeanに関する統計情報を表示します。
<none>	スキャン進行状況情報を表示します(これは `-progress` と同じです)。

Note

Fortify SASTでは、Javaプロセス情報をTMPシステム環境変数の場所に書き込みます。Windowsシステムでは、TMPシステム環境変数の場所は `C:\Users\<username>\AppData\Local\Temp` です。別の場所を指すようにこのTMPシステム環境変数を変更した場合、SCAStateは `sourceanalyzer` Javaプロセスを見つけ出せず、予期された結果を返しません。この問題を解決するには、新しいTMPの場所に一致するようにTMPシステム環境変数を変更します。SCAStateをWindows管理者として実行することを推奨します。

53. インストールおよびアップグレードに関する注意

Fortify SASTのインストール方法の詳細については、*OpenText SASTユーザガイド*を参照してください。

- デフォルトのスキャンポリシーが更新され、低精度バッファオーバーフローの問題のフィルタリングが改善されました。スキャンポリシーにコメントが追加され、フィルタ対象とその変更がいつ導入されたかに関する詳細がわかるようになりました。
- バージョン26.3から、Fortify SASTでは新しいKotlinトランスレータが使用されています。
  新しいトランスレータで問題が発生した場合は、`-use-k1` コマンドラインオプションで従来のKotlinトランスレータを有効にし、問題をカスタマサポートに報告できます。

© Copyright 2026 Open Text

For more info, visit https://docs.microfocus.com