



CxSAST 9.5.0 GA 版(HF2を含む)をリリース！

アプリケーションに潜むセキュリティ上の脆弱性を検出するうえで役立つ

新機能や機能改善が追加されました。

概要

今回のリリースにより、Checkmarx の包括的 AppSec ソリューションがさらに強化されました。Checkmarx はこれからも、ユーザーの皆様がセキュアなソフトウェアを開発できるよう、新機能の追加や機能向上を図っていきます。CxSAST 9.5.0 で実装された主な新機能や機能改善は以下の通りです。

- ・ **言語カバレッジの強化とフレームワークの更新**
- ・ **コアエンジンの強化**
- ・ **様々なアプリケーションの機能強化**
- ・ **アクセス制御の強化**

CxSAST 9.5.0 GA 版（HF2を含む）の入手について

新しいバージョンの入手についてご不明な点がある場合は、こちら（東陽テクニカ
ソフトウェア・ソリューション技術サポート係 ss_support@toyo.co.jp）まで
お問い合わせください。

リリース内容の詳細

・言語カバレッジの向上とフレームワークの更新

CxSAST 9.5.0 では、言語とフレームワークが大幅に強化されました。

CxSAST 9.4.0 のエンジンパック (9.4.1、9.4.2、9.4.3、9.4.4 および 9.4.5) でサポートされていた言語およびフレームワークはすべて、CxSAST 9.5.0 に含まれています。

- ・ Python フレームワーク Django と Flask
- ・ プリセット「MISRA C 2012」の改良 (※)
- ・ RPG と Scala (および Finagle フレームワーク) を新たにサポート
- ・ Swift サポートの改善
- ・ TypeScript 4.5
- ・ Angular 11 および 12
- ・ Kotlin 1.5 および 1.6
- ・ Java フレームワークの改善: Struts、Spring、JSP、および JSF
- ・ .NET Core 5 および 6 の最新バージョンをサポートするための C# クエリの改善
- ・ コンプライアンスの改善 (プリセットとスタンダード)

※プリセット MISRA C の改良

従来のエンジンパックで C 言語用に追加されていた、プリセット「MISRA C 2012」(コーディングスタンダード用) が改良され、追加ルールに対応しました。

CxSAST 9.5.0 でサポートされているプログラミング言語とフレームワークの一覧リストについては、[Checkmarx ナレッジセンター](#)でご確認いただけます。

・コアエンジンの強化

・新しいフローのスキャン設定

新しいフローでは、誤検出と検出漏れを減らすことにより、スキャンの精度を向上させました。また、スキャン時間やメモリ消費量などのスキャン性能も向上しています。新しいフローでは、必要な場合にのみ、クエリのフェーズでフロー計算が実行されるため、パフォーマンスが向上しています。CxSAST 9.5.0 では、改善された新しいフローへの移行（従来方式との並行時期）が完了し、すべてのプロジェクト（既存/新規）およびすべての言語が、新しいフローでスキャンされるようになりました。

・エンジン設定とログのリファクタリング

設定キーの数を約 10% 減らし、いくつかのキーの名前を変更。各キーの説明も見直すことで、使用感と保守性を向上させました。

・エンジンのモダナイゼーション

パフォーマンス、メモリ使用量、スキャンの高速化など、さまざまな面でエンジンを改善するための継続的な取り組みを行いました。

・利用可能なディスク容量の確認

利用可能なディスク容量を超えた場合、エンジンをオフラインにする新しい閾値が追加されました。

・以前のバージョンのエンジンをブロック

エンジンのバージョン（メジャー、マイナー、およびリビジョン）が、インストールされた最新のエンジンパックのバージョンと異なる場合、エンジンは「オフライン」とマークされます。

・様々なアプリケーションの機能強化

- ・ REST API の新規追加、既存 REST API の改良
- ・ パーミッションの強化
- ・ ソースプルに関するパフォーマンスの改善 - ネットワーク接続型ストレージ (NAS) を使用した場合のソースプル フローステップの実行時間が改善されました。
- ・ 結果ビューアのパフォーマンス改善 - 結果ビューアのグリッドのパフォーマンスが改善され、特に複数の結果を扱う場合の読み込みとナビゲーションの時間が最大 75% 短縮されました。
- ・ ユーザー設定の保存 - ポータルページでユーザーが定義した設定が保存され、異なるビューに切り替えたときに適用されるようになりました。
- ・ コード変更なしでの強制スキャン - コードの変更がなくても、バージョンアップやセキュリティポリシーの変更のような、スキャン結果に影響を与えるような環境の変更があった場合に、スキャンが実行されます。
- ・ プロジェクトブランチの詳細 - ポータルでプロジェクトがブランチされた場合、プロジェクト画面の一般タブに、元のプロジェクト名とブランチされたスキャンID の情報を含む詳細が表示されます。
- ・ 結果ビューアの改善 - 結果ビューアに類似度 (Similarity Id) に関する情報が追加されました。
- ・ ポストスキャンアクションの改善 - スキャン結果に含まれる脆弱性の深刻度によって、ポストスキャンアクション実行の有無を決められるようになりました。ユーザーが指定した深刻度以上の脆弱性が、スキャン結果に新たに含まれた場合のみ実行するように設定することができます。オプションで、ポストスキャンアクションの追加引数をプロジェクトの設定レベルで指定することができます。
- ・ トラブルシューティングログ - アプリケーションログに基づいた Kibana ダッシュボードが利用できるようになりました。スキャンのさまざまなフェーズについてより詳細な情報を提供することで、トラブルシューティングの取り組みを改善し、より効率的な根本原因の分析を実現します。
- ・ サービスの可用性 - 各マシン上で動作している CXSAST サービスの状態をモニタリングできるようになりました。

・アクセス制御の強化

セキュリティ向上のため、パスワードの長さを 10 文字以上としました。この変更は、既存のユーザーには影響せず、新規ユーザーまたは既存ユーザーのパスワード更新時のみ適用されます。

・追加情報

- ・新バージョンおよびホットフィックス (HF) は <https://www.checkmarx.com/downloads> からダウンロードできます。
- ・詳細については、東陽テクニカ ソフトウェア・ソリューション 技術サポート ss_support@toyo.co.jp までお問い合わせいただくか、Checkmarx 社の Web サイトで公式の[リリースノート](#)をご参照ください。

Checkmarx

商標について

本書内に記載されている会社名、システム名、製品名には各社の登録商標または商標が含まれます。本文および図表中には、「TM」および「(R)」を明記していません。