



報道関係者各位

2021年5月18日

Contrast Security Japan 合同会社

**Contrast Security がクラウドネイティブ・コンピューティング・
ファウンデーション (CNCF) と Linux Foundation に加入
～クラウドネイティブアーキテクチャとオープンソースソフトウェアにおけるセキュリティ
のベストプラクティスと標準化を推進～**

Contrast Security は、安全で最新の拡張可能な開発環境を提供し
Web アプリケーションの迅速な構築およびその実行を促進します。

アプリケーションセキュリティにおけるイノベーションリーダーである Contrast Security は本日、Cloud Native Computing Foundation (CNCF) と Linux Foundation にシルバー会員として加入したことを発表しました。これにより、世界の大手企業、エンドユーザーおよびベンダーが協力し、クラウドネイティブアーキテクチャとオープンソーステクノロジーの活用がさらに促進されます。CNCF は、Kubernetes、Prometheus、Envoy など、最も急速に成長している多くのオープンソースプロジェクトベンダーを中立的な立場で支援しています。Contrast は CNCF 会員になることにより CNCF のイベント、プロジェクト、コミュニティへの積極的な参加を通じて、クラウドネイティブアーキテクチャとオープンソースソフトウェアにおける増大するリスク対策とそのメリットの活用について業界をサポートおよび啓蒙していく事を目指しています。

サードパーティのオープンソースソフトウェア (OSS) の活用は、過去数年間で大幅に増加しています。OSS とは、開発者が社内で開発した独自のコードを補強し、リリースまでの時間を短縮するために使用、変更、共有出来るパブリックドメイン内のアプリケーションコンポーネント (フレームワークやライブラリなど) を指します。昨今、OSS は広く採用され、ウォルマート、JP モルガン・チェース、さらにはマイクロソフトなどの大手企業などで使用されています。同時に Contrast Security は、企業のソフトウェアに潜在する脆弱性、オープンソースコードに対する標的型攻撃、知的財産であるライセンスなどのリスクを発生させずに、OSS を安全に活用出来るよう企業を支援しています。DevOps で OSS を安全に活用することは、ワークフローの課題でもあります。



クラウドネイティブアプリケーションは、クラウドで実行される従来のアプリケーションに比べて、企業にさまざまなメリットをもたらします。クラウドネイティブアプローチは、ビジネスおよび開発サイクルの高速化という2つの異なる領域に分類されます。組織においてクラウドネイティブコンポーネントの採用が急速に拡大しています。例えば Forrester のレポート[※]によると、わずか1年後には、開発者の30%が定期的にクラウドコンテナを使用し、25%がサーバーレスコンピューティングを使用されると予測しています。市場が急速に進化し企業が非常に短い期間でアプリケーション開発や影響の大きい変更を加える必要性が高まるにつれ、これらの数値が増加していく可能性を強く示しています。ただし、クラウドネイティブアプリケーションのメリットを最大限に活用するには、組織が適切なセキュリティテクノロジーとプロセスを導入する必要があります。

Contrast Security の最高戦略責任者である Surag Patel は、次のように述べています。「API、Kubernetes、サーバーレス機能、クラウドネイティブアーキテクチャ、オープンソースコード等の、デジタルトランスフォーメーションを加速するためのコミュニティのコア基盤の多くは、リスクを飛躍的に増大させます。Contrast Security は、企業がこれら全ての最新のアプローチを安全に活用できるよう支援しており、デジタルトランスフォーメーションを遅らせることなく、生じ得るリスクを削減します。我々は、セキュリティの可観測性に特化した機能がコミュニティに利益をもたらすと信じるとともに、市場に関する独自のノウハウを提供します。」

CNCF への加入以前に、Contrast Security は OSS のセキュリティに関する 2021 年版のレポートにおいて、アプリケーションで検出されたサードパーティ・ライブラリの 38%がアクティブで、アクティブなライブラリのクラスのうち 31%しか呼び出されていないことを明らかにしました。従来のソフトウェア構成分析 (SCA) ソリューションでは、アプリケーションに含まれる全てのオープンソースコードを分析しなければなりません。これは、リスクが無い脆弱性を調査するために膨大な時間とリソースの浪費に繋がります。しかしながら、呼び出されるサードパーティのコードにはリスクが内在しています。ライブラリの平均使用年数は 2.6 年で、アプリケーションには平均 34 個の CVE(共通脆弱性識別子) が含まれると言われてます。

また同レポートによると、多くのアプリケーションにリスクの高いライセンスの問題が含まれており、このようなアプリケーションをリリースする可能性があることも判明しました（例、35%のアプリケーションに少なくとも1つはコピーレフトライセンスが含まれていると言われてます）。CNCF の会員企業は、Contrast Security の提供するアプリケーションセキュリティプラットフォームを活用することでアプリケーション内部からセキュリティを確認出来る様になり、その脆弱性検出結果や Contrast が提供するその他の調査報告書を参照および活用頂くことが出来ます。



Contrast は、ビルドパックを含む様々な CNCF プロジェクトを既にサポートしており、独自のセキュリティ技術を全てのワークロードイメージに自動構成します。全てのワークロードはアプリケーションセキュリティに関する見解と組み合わせられ、分散された Web アプリケーション環境に大規模なセキュリティを展開します。CNCF の会員として、Contrast は引き続き他の会員企業様と連携しながらベストプラクティスについて CNCF にフィードバックしていきます。

※出典：「Predictions 2021」Forrester（2020 年 10 月）

Contrast Security について

Contrast Security はアプリケーションセキュリティにおけるリーディングカンパニーです。Web アプリケーションの開発段階でアプリケーションに潜む脆弱性を高精度で解析し、本番環境では外部からの攻撃を迅速に検知しブロックすることが出来ます。特許取得済み技術「ディープセキュリティ・インスツルメンテーション」により、企業はソフトウェア開発ライフサイクル（SDLC）への展開を簡単且つ迅速に実現します。従来の非効率的なアプリケーションセキュリティ（SAST、DAST および WAF）から完全に置き換えることにより、時間やコストを消費する脆弱性スキャンの排除やインフラ業務、セキュリティエンジニアのリソースを軽減します。Contrast のアプリケーションセキュリティは、SDLC を加速し、未知の脅威からアプリケーションを保護しながらビジネスの成長を促進します。