Nomura Research Institute Group

NEWS RELEASE

2019 年 11 月 21 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、日本で初めてコンテナオーケストレーションに特化したセキュリティ診断サービスを提供開始

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：小田島 潤、以下「NRI セキュア」）は、日本で初めて[1]、コンテナオーケストレーション[2]を採用したシステム向けの、情報セキュリティ診断サービス（以下「本サービス」）の提供を本日、開始します。

第一弾として、コンテナオーケストレーションを行うための代表的なツールである、「Kubernetes（クーベネティス）」[3]を使用したシステムを、診断の対象とします。

DX（デジタルトランスフォーメーション）が加速する昨今、システム開発においても、従来に比べ柔軟性やスピードが求められるようになり、それらを支える設計思想やインフラ技術も目まぐるしく進化しています。中でも、アプリケーションをサービスや機能などで細かく分割して開発するマイクロサービスアーキテクチャ[4]をはじめ、クラウドネイティブ[5]、サーバレス[6]を前提にしたシステム開発が一般的になりつつあります。

それらを支える技術領域の一つが、コンテナと呼ばれる、アプリケーションの実行環境です。コンテナのデプロイ（運用環境への配置）やスケーリング（拡張）などを、自動的に行うコンテナオーケストレーションツールが登場したことにより、システムを構築する上でコンテナを採用する傾向がますます広がってきました。

一方で、コンテナは新しい技術領域であることから、セキュリティ対策が十分に整備されておらず、脆弱な設定のままでシステムを稼働させてしまう可能性が高い状況にあります。ますます激しくなるサイバー空間上の脅威や攻撃に対して、コンテナ自体の脆弱性対策だけではなく、システムのアーキテクチャ全体の視点で、アクセス管理や権限設定などのセキュリティ対策も適切に行うことが求められます。

本サービスでは、コンテナオーケストレーションの技術を採用したシステムに対して、設定ファイルなどを読み解く“静的解析”と、疑似攻撃などを試みる“動的解析”の双方の観点から、セキュリティ診断を行います。診断では、コンテナオーケストレーションに精通したエンジニアによるマニュアル検査をベースとし、補助的に複数の検査ツールを利用します。設定ファイルなどの情報および、オーケストレーション

によって生成されたアーキテクチャの設定の有効性を確認して、セキュリティ上の問題点を検出します。

設定ファイルごとに単独で行う検査だけではなく、アーキテクチャ全体を俯瞰した上で、適切な設定状態であるかどうかを確認するため、網羅的かつ高精度の診断を実施します。このため、検査ツールのみでは見落とされがちな、設計段階での問題点も検出可能です。

今後、Kubernetes 以外のコンテナオーケストレーションツールについても、診断の対象に加えていく予定です。サービスの詳細については、下記の Web サイトをご覧ください。

https://www.nri-secure.co.jp/service/assessment/container

NRI セキュアは、今後も時代のトレンドや脅威の動向を捉え、企業・組織の情報セキュリティ対策を支援するさまざまな製品・サービスを提供し、社会における安全・安心な DX の推進に貢献していきます。

---

[1] 日本で初めて：

日本において中堅・大手セキュリティベンダーが提供する、コンテナオーケストレーションを対象とした初のセキュリティ診断サービス（2019 年 11 月 21 日現在、NRI セキュア調べ）。

[2] コンテナオーケストレーション：

コンテナは、より少ないコンピュータリソースで仮想化を実現するために、OS 上に構築されたアプリケーション実行環境を指す。コンテナ型の仮想環境を構築するための代表的なツールに、Docker（ドッカー）がある。

コンテナオーケストレーションは、コンテナのデプロイ（運用環境への配置）やスケーリング（拡張）などを、自動的に行うこと。

[3] Kubernetes（クーベネティス）：

オープンソースのコンテナオーケストレーション用のツール。現在利用されているコンテナオーケストレーションツールの中でも、多くのシェアを持つ代表的なツールとなっている。Kubernetes を利用する場合は、マスターノード（クラスタ全体の管理を行うノード）やワーカーノード（マスターノードからの指示に従ってコンテナの管理等を行うノード）に含まれる各コンポーネントや、Pod（共有のストレージまたはネットワークを持つ 1 つ以上のコンテナ、およびコンテナを実行する方法についての仕様）の設定など、ツール特有のアーキテクチャや機能を熟知していないと、セキュリティ上の脆弱性が発生する可能性がある。

[4] マイクロサービスアーキテクチャ：

ソフトウェアアーキテクチャの一つ。アプリケーションをビジネス機能に沿って、複数の小さいサービス（マイクロサービス）に分割して開発を行う。サービスのデプロイやスケーリングにおいて、柔軟性が高いなどの特徴がある。

[5] クラウドネイティブ：

クラウドサービスの活用を前提とした、システム開発および運用方式のこと。

[6] サーバレス：

クラウドサービスを利用しているシステムにおいて、クラウド事業者が、事前にサーバリソースを割り当てることなく、任意のイベントをトリガーにリソースを割り当て、コード実行を行うこと。利用者側は、インフラ管理にかかるコストを抑えることが可能となる。

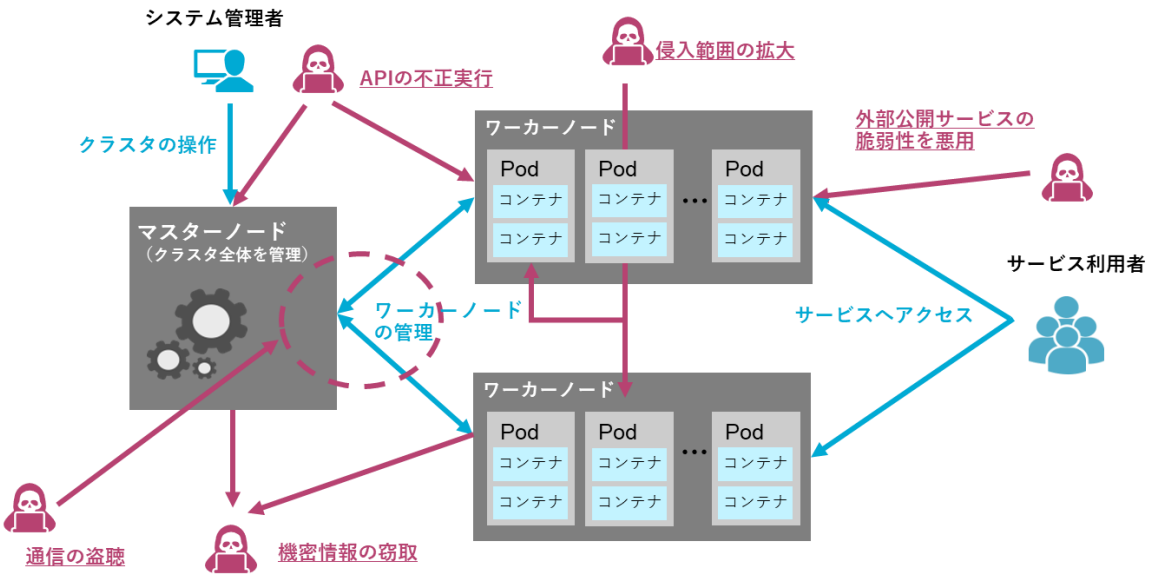
【ニュースリリースに関するお問い合わせ先】

NRI セキュアテクノロジーズ株式会社　広報担当

TEL：03-6706-0622　E-mail：info@nri-secure.co.jp

【ご参考】

■ Kubernetes を利用したコンテナオーケストレーションの概要図と、サイバー空間上の脅威例



※一般的なKubernetesアーキテクチャを簡略化して示しています。

※サイバー脅威となるケースは、下線付き赤字で表示しています。本図で示す脅威は、あくまで例示です。