kaspersky BRING ON THE FUTURE

DevOps に最適な Kaspersky Hybrid Cloud Security

DevOps の取り組みは、常にスピード、精度、革新性が要求されるプレッシャーの下にあります。このような背景から、DevOps を進める上ではセキュリティ要件が抵抗要素とみなされることがあります。しかし、DevOps の重要なプロセスからセキュリティを除外することは解決策にはなりません。DevOps と情報セキュリティ間のギャップを解消するソリューションが必要なのです。

プラットフォームのサポート

オペレーティングシステム：
- Windows
- Linux

IaaS：
- Google Cloud Platform
- AWS
- Microsoft Azure

コンテナ化プラットフォーム：
- Docker
- Windows コンテナー

仮想プラットフォーム：
- VMWare vSphere と NSX
- Microsoft Hyper-V
- Citrix XenServer と Citrix Virtual Apps and Desktops
- KVM（カーネルベースの仮想マシン）
- Nutanix AHV

オーケストレーションと CI/CD パイプライン：
- Jenkins
- TeamCity

インターフェイス：
- CLI
- Open API

DevOps と情報セキュリティ間のギャップを解消

現在、DevOps の導入が急速に進んでおり、ビジネスニーズを満たし、製品化までの時間を短縮し、俊敏性と柔軟性を高め、自動化を実現することに重点がおかれるようになっています。一方で、これらを達成する上でセキュリティに対する考えの違いが足かせとなっているケースも多く見られます。DevOps では、KPI を達成するには、セキュリティの考慮を最小限にするか、またはまったく考慮しないことが必要であると考えられる場合があるようですが、IT の観点からすると、動的に拡大を続けるシャドー IT（従業員が個人所有のスマートフォンやパソコンなどの情報端末を、会社の許可なく使用すること）の全容を明らかにして、社内セキュリティの管理下に入れることが必要になります。

両者が抱えるさまざまな懸念事項によって、このギャップはさらに広がっています。使用する専門用語や、設定した KPI が異なることがネックになって、状況の改善が難しくなっているのです。

Kaspersky Hybrid Cloud Security は、DevOps が「コードとしてのセキュリティ（security as code）」アプローチを最大限に活用するために必要な機能がすべて揃ったツールセットとインターフェイスを提供することで、DevOps と IT セキュリティ間のギャップを解消し、DevOps から DevSecOps へ変わる取り組みをサポートします。

IT のニーズ	DevOps のニーズ
情報リスク管理	トータルなコンフィギュアビリティ
オーバーヘッドを最小限に抑制	セキュリティも含めた「あらゆるもののコード化（everything as code）」アプローチ
管理ツール数の妥当な増加	各種プラットフォームのサポート
ポジティブな「ビジネスイネーブラー」のイメージ	パフォーマンスに対する影響を最小限に抑制
	動的であること – エンティティのライフサイクルは分単位または秒単位にもなる

「Security as code」で DevSecOps を実現

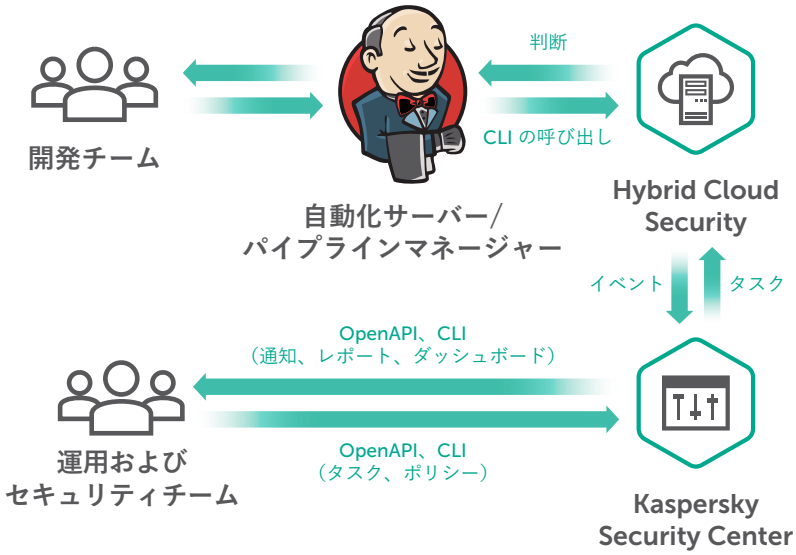
Kaspersky Hybrid Cloud Security は、効率性に優れ、高度なコンフィギュアビリティを備えたセキュリティツールセットです。以下のことを実現し、企業が真の DevSecOps カルチャーを確立できるようにします。

- Linux と Windows のプラットフォーム、仮想インフラとパブリッククラウドサーバーのインフラ、および Docker と Windows コンテナーを保護して、攻撃者が脆弱なまたは悪意のあるコンテナーコンポーネントを組織のインフラの侵入口として利用することを防止する
- セキュリティを管理および可視化し、リスクを管理するためのツールを IT 部門と IT セキュリティ管理者に提供する
- 充実したレポート機能を提供し、ポリシーベースの運用を実現する

Kaspersky Hybrid Cloud Security による「Security as code」の実現：

- コンテナ化プラットフォームのランタイムおよびメモリの保護
- デフォルトでセキュアな設定 - リポジトリ、フレームワーク、ライブラリのテスト
- 以下の自動化と実現：
  - SAST：静的アプリケーションセキュリティテスト
  - DAST：動的アプリケーションセキュリティテスト
  - IAST：対話型アプリケーションセキュリティテスト
  - BAST：ふるまいベースのアプリケーションセキュリティテスト
- ASTO：ポリシーベースのアプリケーションセキュリティテストオーケストレーション
- 「シフトレフト」：CI/CD パイプラインの開発段階でセキュリティ対策を統合
- 「Everything-as-code」アプローチをサポートする充実した統合機能

- 自動化とパイプライン構築に対する統合インターフェイスを提供し、DevOps が社内リポジトリを常にクリーンな状態に保ち、パブリックリポジトリから取得したエンティティをサニタイズする



充実した統合オプション

Kaspersky Hybrid Cloud Security では、安全かつ制御された方法でプロセスのスピードを落とすことなく、リーンな（無駄のない）ソフトウェアプラクティスとジャストインタイムのアプリケーションのビルド、パッケージ化、デリバリを組み合わせることができます。

- CI/CD プラットフォームの統合（Jenkins など）により、パイプラインの構築と自動化を簡素化する
- コンテナー、イメージ、およびローカルやリモートのリポジトリに対するオンアクセススキャン（OAS）とオンデマンドスキャン（ODS）により、開発のニーズに応じてサニタイズされたリポジトリを容易にメンテナンスできるようにする
- 名前空間の監視、マスクベースの柔軟なスキャン範囲の制御、異なるレイヤーのコンテナーに対するスキャン機能によって、開発を安全に進めるためのベストプラクティスを適用する

製品情報：
Security for DevOps - www.kaspersky.co.jp/enterprise-security/devops-security
Hybrid Cloud Security - www.kaspersky.co.jp/enterprise-security/cloud-security
ご購入相談窓口：
jp-sales@kaspersky.com

www.kaspersky.com

Kaspersky は、実証された独立した企業で、透明性が確保されています。Kaspersky は、テクノロジーによって私たちのより良い生活、より安全な世界の構築に取り組んでいます。そのため Kaspersky は、テクノロジーがもたらす無限の機会をすべての人がすべての場所で享受できるよう、そのテクノロジーを守ります。より安全な未来に向けて、サイバーセキュリティを実現します。

詳しくはこちら：kaspersky.com/transparency

Proven.
Transparent.
Independent.