

# クラウドのセキュリティを向上させる 4つの方法

## Red Hat OpenShift クラウドサービスでセキュリティ重視のアプローチを採用

多くの企業が、競争力を維持するためにテクノロジーとプロセスをモダナイズしています。しかしそれによって、クラウド環境の維持とセキュリティ保護が困難になることがあります。クラウドセキュリティの責任はクラウドプロバイダーと共有され、エンドユーザーがベストプラクティスに従わないと、往々にしてセキュリティに穴があくことになります。組み込みセキュリティ機能を備えたマネージド・クラウドサービスなら、モダナイゼーションの作業の単純化に役立ちます。

以下で紹介する 4 つの方法を使用して、組織のクラウドセキュリティの大幅な改善に役立ててください。

## 1 統合セキュリティで 実装を迅速化する

クラウド環境全体でセキュリティを優先します。セキュリティの作業を開発サイクルの早期段階に移行してサイクル全体で実施し、セキュアなソフトウェア・サプライチェーン、自動化された DevSecOps プラクティス、ランタイム時のアプリケーション・セキュリティを実現します。

Red Hat® OpenShift® クラウドサービスは組み込みセキュリティ機能を備え、以下のことを支援します。

- ▶ セキュリティの自動メンテナンス、継続的な監視、予防的な修復をフルマネージドサービスに組み込んで、ソフトウェア・デプロイメントを単純化し、運用の複雑性を低減します。
- ▶ Kubernetes プラットフォーム構成を評価し、統合プラットフォーム構成とライフサイクル管理、ID およびアクセス管理、プラットフォームデータのセキュリティ、接続されたストレージを使用して、自動デプロイメントポリシーによってセキュリティ保護します。
- ▶ DevOps ベストプラクティスと内部統制をセキュリティ・プラットフォームの構成チェックに取り入れます。

## 2 リスク管理を権限委任して 生産性を向上させる

チームの焦点をより価値が高い業務に振り向けて、効率を向上させてアプリケーション開発のスピードを上げます。責任が共有されるので、セキュリティとインフラストラクチャ管理の負担が軽減され、以下のことが実現します。

- ▶ アプリケーション開発とデプロイが最大で 70% 短縮され、チームはアプリケーションをすばやくスケールアップして継続的に発展させられます。<sup>1</sup>
- ▶ DevOps チームの業務からインフラストラクチャの管理を外して、運用効率を向上させます。
- ▶ 開発者がアップデートを小さな部分に分割できるよう支援し、限られた期間内で広範なテストを行わなければならないというプレッシャーを軽減します。
- ▶ ハイブリッドクラウド環境全体で一貫性があり、キュレートされた開発エクスペリエンスを生み出します。

<sup>1</sup>Forrester Consulting, Red Hat 後援、[「The Total Economic Impact™ of Red Hat OpenShift Cloud Services」](#)、2022 年 1 月。

### 3 自動化とプロアクティブな管理でリスクを低減する

アプリケーション・プラットフォーム専任のセキュリティエキスパートを雇用する必要性をなくし、クラウド環境の維持に必要なコストとリソースを削減します。フルマネージド型のクラウドサービスは、以下のことに役立ちます。

- ▶ 価値主導で成長に関連するタスクに集中する。セキュリティのアップデートやパッチを適用する負担はなくなり、こうした作業は [Red Hat SRE](#) (サイト信頼性エンジニアリング) によって管理されます。
- ▶ インハウスでのインフラストラクチャ管理の必要性を低減する。インハウスで管理した場合、開発チームのワークロードに大きな責任やリスクが付加されてしまいます。OpenShift クラウドサービスを使用する組織は、開発者の時間の 20% を回復しています。<sup>1</sup>
- ▶ Kubernetes およびコンテナ・プラットフォームの構成ミスを削減する。IT 専門家によると、構成ミスはサイバー攻撃の [3 倍近く](#) も懸念される問題とされています。

### 4 セキュリティに実績があるプロバイダーを選ぶ

Amazon Web Services (AWS)、Microsoft Azure、IBM Cloud、Google Cloud など、あらゆる大手クラウドプロバイダーと連携する設計の、一貫した信頼できるユーザーエクスペリエンスを維持します。

オープンソース・セキュリティに深く根ざした Red Hat は、以下の機能により、ライフサイクル全体、インフラストラクチャ、アプリケーションスタックのすべてにセキュリティを統合する支援をします。

- ▶ デフォルトで [ゼロトラストポリシー](#) を採用する多層防御戦略、およびセキュリティの原則を拡大する [パートナー・エコシステム](#)
- ▶ 人、プロセス、テクノロジーを対象とする、セキュリティとコンプライアンスを維持するインフラストラクチャを管理、自動化、適応させる統合セキュリティ
- ▶ アプリケーション・プラットフォーム、管理、データサービスの管理とセキュリティを提供する、年中無休のグローバル SRE
- ▶ 金銭的補償付きで 99.95% の SLA を活かして停止とシステム障害を最小化する、クラウド・セキュリティサービス

#### 今すぐ始める

[Red Hat OpenShift クラウドサービス](#)の信頼性について、「[Red Hat OpenShift セキュリティガイド](#)」でご確認ください。

<sup>1</sup>Forrester Consulting、Red Hat 後援、「[The Total Economic Impact™ of Red Hat OpenShift Cloud Services](#)」、2022 年 1 月。



#### Red Hat について

Red Hat は、[受賞歴のある](#) サポート、トレーニング、コンサルティングサービスを通じて、組織の環境全体の標準化、クラウドネイティブ・アプリケーションの開発、複雑な環境の統合、自動化、保護、および管理を支援します。

[fb.com/RedHatJapan](#)  
[twitter.com/RedHatJapan](#)  
[in.linkedin.com/company/red-hat](#)

jp.redhat.com  
#F31854\_202207

**アジア太平洋**  
+65 6490 4200  
apac@redhat.com

**オーストラリア**  
1800 733 428

**インド**  
+91 22 3987 8888

**インドネシア**  
001 803 440 224

**日本**  
0120 266 086  
03 5798 8510

**韓国**  
080 708 0880

**マレーシア**  
1800 812 678

**ニュージーランド**  
0800 450 503

**シンガポール**  
800 448 1430

**中国**  
800 810 2100

**香港**  
800 901 222

**台湾**  
0800 666 052

Copyright © 2022 Red Hat, Inc. Red Hat、Red Hat ロゴ、および OpenShift は、米国およびその他の国における Red Hat, Inc. またはその子会社の商標または登録商標です。Linux® は、米国およびその他の国における Linus Torvalds 氏の登録商標です。