セキュリティとコンプライアンスのための自動化

防衛関連企業のコンプライアンスを満たし、維持して、検証する

セキュリティとコンプライアンスの自動化のための Red Hat ソリューション：

- Red Hat Enterprise Linux
- Red Hat Ansible Automation Platform
- Red Hat Insights
- Red Hat Smart Management
- Red Hat OpenShift
- Red Hat Advanced Cluster Management for Kubernetes
- Red Hat Quay

防衛関連企業におけるセキュリティ上の課題

米国防総省 (DoD) の請負業者は、以下のような多くの緊急課題に直面しています。

- **サイバーセキュリティ態勢を成熟させる**：急速に進化する脅威に打ち勝つために、組織は全体的なリスクプロファイルをより深く理解する必要があります。
- **サイバーセキュリティの制御とプロセスの実装を検証する**：構成ドリフトを継続的に検出および修正し、ヒューマンエラーを低減するために、これらの基準が必要です。
- **機能を追加しながら費用を抑える**：膨大なコストをかけずにコンプライアンスを満たし、維持し、継続的に検証することが課題となっています。
- **セキュリティに対する包括的なアプローチを採用する**：組織は、直線的なウォーターフォール型のプロジェクト管理と手動によるセキュリティチェックから、アジャイルな DevSecOps と自動化された診断と緩和策に移行する必要があります。

コンプライアンスを検証し、技術要件で情報を保護する

機密情報の保護は、DoD や公的機関において最重要課題です。先進的なサイバーセキュリティモデルは、以下のような方法でこの課題に取り組んでいます。

- **サイバーセキュリティのリスクを測定する**：他の情報よりも機密性が高いため、より高度なセキュリティ管理が必要な情報があります。
- **セキュリティに対する包括的なアプローチへと移行する**：ネットワークセキュリティは、脅威アクターを拡大する境界内に侵入させないようにするだけでは十分とは言えません。情報を保護するためには、標準化されたプロセスやセキュリティに配慮した行動が不可欠です。
- **サードパーティを介して継続的なコンプライアンス準拠を検証する：**組織はサプライチェーン内の企業に対し、独立したサードパーティによる検証作業を通じてコンプライアンス準拠を証明するよう求めることがあります。

Red Hat を選ぶ理由

- **セキュリティの強化**：Red Hat のソリューションは、連邦政府の厳しいセキュリティ要件を満たしてます。
- **コストの削減**：Red Hat のサブスクリプションはプロプライエタリー・ソフトウェア・ライセンスよりも安価で、政府との契約をサポートします。
- **パートナーエコシステム**：Red Hat は、Red Hat® テクノロジーで動作するようテスト、サポート、認定された何千もの製品およびサービスからなるパートナーエコシステムを維持しています。
- **オープンソースリーダー**：Red Hat はオープンソースソフトウェアの主要な支持者であり、開発者でもあります。Red Hat はオープンソース・コミュニティと密接に協力して、お客様の組織の成功を支援するソリューションを提供します。
- **豊富な経験**：Red Hat は、米国内の政府機関と協力してアプリケーション開発プロセスのモダナイズに取り組んできたことから、豊富な専門知識を有しています。

効果的な自動化されたセキュリティおよびコンプライアンス戦略の構築

Red Hat テクノロジーは可視性と制御を実現し、コンプライアンスの単純化、加速化、コスト削減を支援します。[1] Red Hat は、信頼、認定、サポートされている安定したエンタープライズ向けオープンソース・ソフトウェアを提供し、クラウド、ネットワーク、ストレージのエコシステム企業と提携して統合を容易にします。Red Hat のポートフォリオは、技術的なセキュリティ要件を満たしてコンプライアンスを維持するのに役立つツールを備えており、明確なライフサイクルと共にオープンソースで構築された製品を完備しています。

変化し続けるサイバーセキュリティのダイナミクスには、セキュリティへの包括的なアプローチが必要とされており、これにはセキュリティとコンプライアンス戦略の重要要素としての自動化を伴います。

Red Hat テクノロジーは、セキュリティ要件への準拠と維持をサポートします。

インフラストラクチャ・ソフトウェア

Red Hat Enterprise Linux® はセキュリティ重視のオペレーティングシステムで、Security Content Automation Protocol (SCAP) など、組織の環境の保護を支援する組み込みツールを備えています。2008 年以来、Red Hat は、米国国立標準技術研究所 (NIST) が認定するオペレーティング環境のセキュリティ強化ソリューションである SCAP[2] の定義とツールの構築を行うオープンソース・コミュニティをリードしてきました。SCAP は、PCI DSS、DISA STIG、HIPAA[3] などの業界標準に準拠するための、**事前ビルド済み**のセキュリティプロファイルを備えており、また、カスタムプロファイルを構築する機能も備えています。

Red Hat Enterprise Linux は自動化のための安定した信頼できる基盤であり、システムユーザー、アプリケーション、プロセス、およびファイルのアクセス制御を定義する Security-Enhanced Linux (SELinux) が含まれています。

ネットワークやセキュリティおよびネットワークの各種ツールの設定を、共通言語で行うことができます。

自動化と運用管理

Red Hat Ansible® Automation Platform は、システム、アプリケーションからツール、プロセスに至るまで、お客様の環境のためのシンプルで柔軟かつエージェントレスな自動化言語を提供します。設定変更を行える担当者を制御し、誰がいつ変更したかを簡単に確認することができます。Ansible Automation Platform では、既存のセキュリティ・ソリューションやツールを置き換えるのではなく、それらを統合できます。Ansible Automation Platform はハイブリッド・マルチクラウド環境におけるセキュリティ・テクノロジーの統合と相互運用性を可能にします。

Red Hat Insights は、Red Hat Enterprise Linux 環境をプロアクティブに評価し、運用とセキュリティに対するリスクを特定して、これらのリスクがより大きな問題に発展する前に、迅速に解決する方法に関するガイダンスを提供します。

Red Hat Smart Management は、完全なライフサイクル管理を実現する Red Hat Satellite と Red Hat Insights の機能をグラフィカル・ユーザー・インタフェース (GUI) と組み合わせ、物理マシンからハイブリッド・マルチクラウドまで Red Hat Enterprise Linux がサポートするあらゆる環境をより安全に管理できるようにします。

コンテナ・プラットフォーム

Red Hat OpenShift® と Red Hat Advanced Cluster Management for Kubernetes により、デプロイ、アップグレード、パッチ適用、セキュリティ監査などの標準化されたワークフローで、グローバルに分散されたアプリケーション・プラットフォームの管理が可能になります。

Red Hat Quay コンテナ・イメージ・レジストリでストレージを提供し、暗号化された署名付きコンテナのビルド、分散、デプロイを可能にします。イメージリポジトリのセキュリティを、自動化、認証、承認システムで強化します。

[1] Red Hat 概要、「Red Hat と OpenSCAP によるコンプライアンスの向上と自動化」、2019 年 10 月。

[2] Red Hat ブログ、「Red Hat OpenSCAP、SCAP 1.2 NIST 標準を満たすために評価段階に」、2013 年 3 月 13 日。

[3] Payment Card Industry Data Security Standard (PCI DSS)、Defense Information Systems Agency (DISA)、セキュリティ技術導入ガイド (STIG)、Health Insurance Portability and Accountability Act (HIPAA)。

サービスとサポート

Red Hat は、規制が厳しく、セキュリティ意識の高いお客様のために、トレーニング、サポート、コンサルティング・サービスも提供しています。これらのサービスにより、テクノロジーへの投資を最大化できるよう支援します。

詳細はこちら

自動化、コンテナ化、インフラストラクチャのライフサイクル管理、プロアクティブな運用環境評価を活用することにより、DoD の請負業者は進化し続けるコンプライアンスの課題に対処することができます。

Red Hat がお客様のシステムのセキュリティ、プライバシー、安定性を維持するためにどのような支援ができるかについて、詳しくは redhat.com/gov をご参照ください。

その他の資料

Red Hat ATO Pathways

コードとしてのコンプライアンスに対応した Red Hat 公式 Ansible Roles

Common Criteria、FIPS 140-2、STIG、USGCB、USGV6 (DoD IPv6)、Section 508 などに関する Red Hat ナレッジベース

Open Vulnerability and Assessment Language (OVAL) の定義を含む Red Hat のセキュリティデータ

アジア太平洋 +65 6490 4200
apac@redhat.com
オーストラリア 1 800 733 428
インド +91 22 3987 8888
インドネシア 001 803 440 224
日本 03 4590 7472
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

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

Red Hat について

エンタープライズ・オープンソース・ソフトウェア・ソリューションのプロバイダーとして世界をリードする Red Hat は、コミュニティとの協業により高い信頼性と性能を備える Linux、ハイブリッドクラウド、コンテナ、および Kubernetes テクノロジーを提供しています。Red Hat は、新規および既存 IT アプリケーションの統合、クラウドネイティブ・アプリケーションの開発、Red Hat が提供する業界トップレベルのオペレーティングシステムへの標準化、複雑な環境の自動化、セキュリティ保護、運用管理を支援します。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提供する Red Hat は、フォーチュン 500 企業に信頼されるアドバイザーです。クラウドプロバイダー、システムインテグレーター、アプリケーションベンダー、お客様、オープンソース・コミュニティの戦略的パートナーとして、Red Hat はデジタル化が進む将来に備える企業を支援します。

O-F26829