Red Hat 製品で金融サービスのセキュリティとコンプライアンスを自動化する

「チームの取り組みが加速し、コラボレーションの効果が全社的に高まり、より多くの時間をイノベーションに使えるようになりました。この取り組みは、お客様のために正しいことをするという当社の社是の実現に大きく貢献してくれました」[1]

Ally Financial
クラウド自動化およびエンジニアリング担当
シニアディレクター
James Hixon 氏

はじめに

デジタル化の普及が進むにつれて、関連するインフラストラクチャの複雑さも増しています。この傾向は金融サービス分野で特に顕著です。この分野は従来から、技術と規制の両面の制約が強く、リスクを嫌い、変化に抵抗感を示す傾向があります。金融機関は、アプリケーションをデプロイし、求められているセキュリティを備えた一貫性のある分散アーキテクチャを構築するための自動化機能を必要としています。パッチや構成に一貫性がないと、Windows や Linux® オペレーティングシステム、仮想インフラストラクチャ、パブリッククラウドおよびプライベートクラウド・インフラストラクチャ、コンテナが混在する環境での管理が困難になります。

このような混在環境が拡大していくと、可視性と制御力の低下によりリスクが増加し、手動でのセキュリティおよびコンプライアンスの監視はますます困難になります。さらに、開発、運用、セキュリティチームがうまく連携できておらず、セキュリティ担当者が構成上の変更や問題について最後まで知らされない、というケースも珍しくありません。

脆弱性が特定されても問題の解決や修復の自動化には時間がかかり、問題が長引けば組織への悪影響が懸念されます。そして、特定された脆弱性からは、また別の問題が生じます。最終的に修復が適用されても、次には「誰がいつ、何を修復したか」を文書化するための苦労があります。銀行、決済プロバイダー、保険会社、およびその他の金融サービス機関は、Payment Card Industry Data Security Standard (PCI DSS) や、コンプライアンスを維持するために厳格な追跡、レポート作成、文書化を要求する一般データ保護規則 (GDPR) などのセキュリティ規格にも準拠する必要があります。

セキュリティおよびコンプライアンス対策の自動化

セキュリティおよびコンプライアンスの問題に対処するため、金融サービスプロバイダーは環境全体におけるデータ駆動型の IT/ネットワークプロセス自動化に注目しています。この自動化には以下の要素が含まれます。

- オペレーティングシステム (OS)
  - パッケージ管理
  - パッチ管理
  - プロビジョニング時点でセキュリティ・コンプライアンス・ベースラインに対応した一貫性と OS 不変性を持たせるための OS 強化
- Infrastructure as Code および Security as Code
  - 繰り返し、共有、検証する機能。セキュリティおよびコンプライアンス監査による補助
  - 組織内の全員が同じスクリプト/プログラミング言語を使用できるので操作性が向上

1 Red Hat お客様導入事例、「Ally Financial、クラウド・プラットフォームと DevOps を導入して市場投入時間を短縮」、2019 年 5 月。

- システムのプロビジョニング
  - IT サービス管理 (ITSM) との統合
  - ストレージのプロビジョニング
- ワークフロー
  - サービス管理の単純化
- Day 2 セキュリティ運用による継続的なセキュリティと監視
  - パッチ管理
  - 脆弱性特定と管理 (ヘルスチェックなど)
  - セキュリティ、制御、およびコンプライアンス・ポリシーのプロアクティブなガバナンス
  - 対策：修正プログラムの生成と自動化

セキュリティおよびコンプライアンス自動化の課題

セキュリティとコンプライアンスの状況を手作業で確認することには、多くの理由から問題があります。

- 時間がかかり、単調
- 人的ミスが避けられない
- 不適切なアクションや単純な構成変更に関する監査証跡情報が残らない
- 繰り返し、共有、検証が不可能
- 変更ログ情報が不完全で一貫性がないため、監査に合格しにくい
- 運用チームとセキュリティチーム間のコミュニケーションが効果的ではない、またはコミュニケーションがない

金融商品およびサービスを提供する企業は、適切な自動化戦略を見極めるにあたって、まずはどのような場面と頻度で手作業のタスクが行われているのかを特定する必要があります。また、将来的な要件の変化に対応していくためには、柔軟な自動化テクノロジーに注目すべきです。そして、ネットワーク機器とサービスへ迅速に実装して拡張していくためには、適切な自動化テクノロジーを選択することが重要となります。

Red Hat によるインテリジェントなセキュリティ自動化

Red Hat® のテクノロジーは、エンドツーエンドのソフトウェアスタックにより自動化戦略をサポートします。セキュリティ強化されたオペレーティングシステムや自動化ソフトウェアから、多数のベンダーとのインテグレーション (AWS、シスコ、ジュニパー、VMware など) に至るまで、IT 自動化とネットワーク自動化の両方のニーズに対応します。

スタック全体を Red Hat テクノロジーで統一する必要はありませんが、Red Hat 製品を組み合わせることで、セキュリティおよびコンプライアンス自動化の効力をさらに強化することができます。セキュリティおよびコンプライアンス自動化の場合、Red Hat Enterprise Linux、Red Hat Ansible® Automation Platform、Red Hat Satellite、Red Hat Insights の組み合わせが特に効果的です。

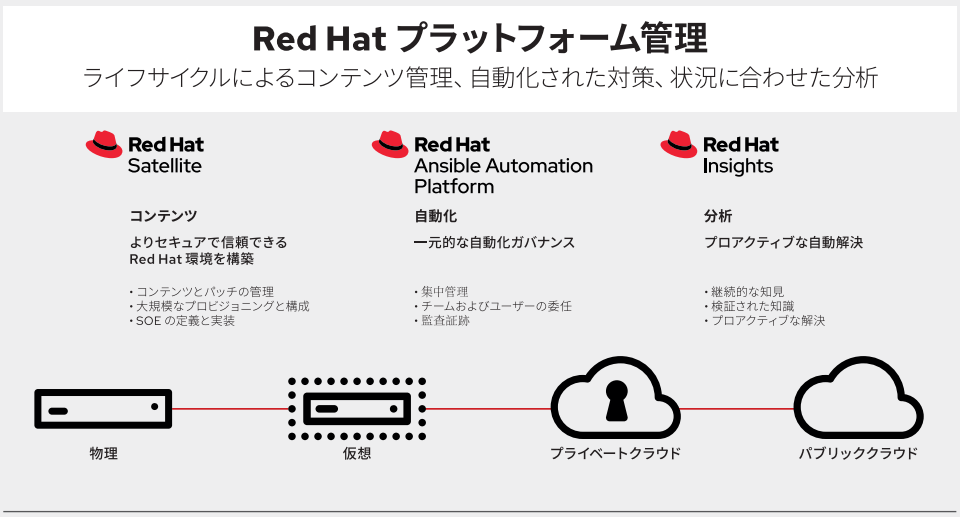


図 1. セキュリティとコンプライアンスを強化するための Red Hat テクノロジーの組み合わせ

これらの Red Hat テクノロジーが連携することで、さらなるセキュリティおよびコンプライアンス上のメリットを得られます。

Red Hat Enterprise Linux

Red Hat Enterprise Linux は、脆弱性に対処し、データを保護し、規制へのコンプライアンスを遵守するためのセキュリティ・テクノロジーを提供します。OpenSCAP により、システム全体とコンテナ内で規制コンプライアンスとセキュリティ構成の対策措置を自動化できます。これは、Red Hat の National Institute of Standards and Technology (NIST) 認定スキャナーで、以下のような脆弱性および構成のセキュリティ・ベースラインに対するチェックと対策を行います。

- PCI DSS
- Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)
- Criminal Justice Information Services (CJIS) セキュリティポリシー
- Commercial cloud services (C2S)
- Health Insurance Portability and Accountability Act (HIPAA)
- NIST 800-171
- Operating System Protection Profile (OSPP) v4.2
- Red Hat Corporate Profile for Certified Cloud Provide

ハイブリッド・コンピューティングの多様なセキュリティニーズにより適切に対処できるよう、Red Hat Enterprise Linux では、ソフトウェア・セキュリティ自動化を強化し、OpenSCAP と Red Hat Ansible Automation Platform との統合によってリスクを低減します。この統合は、事前生成された Ansible Playbook (Red Hat 提供のもの、またはサポート対象のもの) の適用を支援してシステムに対策措置を適用し、セキュリティ・ベースラインへのコンプライアンス、特定のセキュリティプロファイルからの Ansible Playbook の新規作成、OpenSCAP スキャンからの Ansible Playbook の直接作成を実現します。これらを使用すると、より迅速かつ一貫した方法で、ハイブリッド IT 環境の全体に対して対策措置を適用できます。

Red Hat Enterprise Linux システムのロールは、セキュリティ自動化にも役立ちます。Ansible ロールとモジュールのコレクションを活用することで、Red Hat Enterprise Linux 6.10 およびそれ以上のバージョンをリモート管理するための安定した一貫性のある構成インタフェースを提供します。たとえば、Security-Enhanced Linux (SELinux) システムロールを使用すると、Red Hat Enterprise Linux システム上で一貫した SELinux を正しく構成できます。

また、一般的な管理タスクを自動化すると、ホストにスーパーユーザーとして直接アクセスする必要があるユーザーが減るので、攻撃対象となりうる領域が減少します。さらに、SELinux を使用することで、自動化された個別のタスクに固有の特権を割り当てられるので、特権エスカレーションのバグへの対策になります。

Red Hat Ansible Automation Platform

Red Hat Ansible Automation Platform (Red Hat Ansible Tower を含む) は、シンプルかつ強力なエージェントレス IT 自動化テクノロジーであり、組織全体に共通の自動化プラットフォームを提供するとともに、セキュリティおよびコンプライアンスに関する以下のメリットを提供します。

- コンプライアンスのトレーサビリティと反復性
- 繰り返し作業にかかる時間を大幅に短縮
- 一貫したインフラストラクチャ管理アプローチにより、ダウンタイム発生のリスクを低減
- 分析、検出、解決の自動化により、体系的なミスのリスクを最小化
- テクノロジーを迅速に提供して収益実現までの時間を短縮
- 人的ミスのリスクを低減
- IT プロセスの迅速化 (所要時間が数日から数分へと短縮される場合もあり)
- マルチベンダー環境での一貫した構成と管理
- ポリシーのロールアウトやネットワーク全体でのシステムおよびファイアウォールの更新を含む、デプロイ、構成、構成ライフサイクル管理の自動化
- サービスカタログ構成情報を使用した、フィールド問題の迅速な複製
- RESTful API (Representational State Transfer Application Programming Interface) を使用して Ansible Automation Platform を既存のセキュリティツールとプロセスに組み込む能力
- アクセス制御、認証情報ボールト、ジョブおよびワークフローのスケジューリング、ソース制御統合、グラフィカルなインベントリー管理による監査などを含む極めてスケーラブルな自動化ソリューションで、すべてのコンポーネントの表現を単純化し、すべての自動化アクティビティの状況を把握可能

Ansible Automation Platform には、Splunk (SIEM)、Snort (侵入検知および防止)、Checkpoint (エンタープライズ・ファイアウォール) などのセキュリティベンダーおよびセキュリティソリューションとの統合に特化して作成されたモジュールとロールが含まれています。

Red Hat Satellite

Red Hat Satellite は、最新の状態でなく既知の脆弱性が存在するシステムを特定するなど、環境内の Red Hat システムの情報を IT チームに提供します。組織は Satellite を使用することで、サブスクリプションやコンテンツの管理、セキュリティに準拠したホストのプロビジョニング、構成管理、パッチ管理を行うことができます。Ansible Automation Platform は Satellite と連携して、ソフトウェア構成のデプロイと管理を自動的に実行し、ライフサイクル全体を通じてシステムとアプリケーションの管理と制御をエンドツーエンドで自動化し、セキュリティ、コンプライアンス、監査証跡の維持をサポートします。

Red Hat Satellite には以下の機能があります。

- 標準運用環境 (SOE) の定義と適用
- Ansible Automation Platform を使用して Red Hat Enterprise Linux システムのロールをデプロイし、SOE に Red Hat Insights をインストールする
- SOE からの構成ドリフトを特定し、Ansible Automation Platform を使用してドリフトの問題を修復する
- Insights を通じてセキュリティ、パフォーマンス、安定性、可用性に関するリスクを特定し、Ansible Playbook を動的に生成し、Satellite から直接実行してリスクへの対策措置を適用する
- Satellite からプロビジョニングされたシステムは、Ansible Tower にコールバックを実行してプロビジョニング後に Playbook を実行可能
- Ansible Automation Platform を使用することで、Red Hat Enterprise Linux システムロールをインポートして使用
- 動的なインベントリーにより、Ansible Tower は Satellite を動的インベントリーソースとして使用
- Ansible Automation Platform を使用して Satellite 内から Insights をデプロイ可能

Red Hat Insights

Red Hat Insights は Red Hat Satellite に付属し、Red Hat Enterprise Linux のアドオンとして単体で機能することもできます。Insights の予測分析は具体的に実行可能な対策を提供するほか、Ansible Tower と連携させることで、Playbook を自動的に生成して対策措置を適用するように設定可能です。Ansible Tower は Insights API を使用し、サイト全体に対策措置を適用するジョブを支援します。Insights の検出および対策機能は外部システムまたはスクリプトとの統合が可能で、運用チームはガイドに基づく対策措置の適用を組織全体までスケールできるようになります。

Ansible Tower は、Insights API に接続して情報を取得するように設定できます。たとえば、Ansible Tower は Red Hat Insights のカスタマーポータル版で使用される Ansible Playbook を取得でき、これらの Playbook を Ansible Tower から直接起動すれば、問題への対策措置を自動で実行することができます。

図 2. Red Hat によるセキュリティとコンプライアンスの自動化

ユースケース：パッチ管理の自動化

Red Hat Satellite、Red Hat Insights、Red Hat Ansible Automation Platform は、互いに連携しながら Red Hat Satellite で管理されるホストへのリスクをシームレスに検出し、発見された問題の多くを Red Hat Ansible Automation Platform Playbook を使用して修復します。また、繰り返し可能な修復プランを作成し、プランに沿って処置を行い、レポート情報を監査担当者に提出することができます。さらに、Satellite に送信される情報のタイプを制御するように Insights を設定すると、転送されたデータを確認して管理できるようになります。

1. Insights を使用して、パッチ適用が必要なシステムを特定します。
2. 実行する Playbook と Playbook を実行するシステムについて、Insights のプランを作成します。
3. Insights プランの実行をスケジュールするか、手動で実行します。
4. Insights プランから提供された情報に従って行動します。Insights はインテリジェンスやデータが追加されるたびに学習し、分析の精度が向上していきます。関連する知見を自動的に検出し、カスタマイズした次のアクションをプロアクティブに推奨し、さらにタスクを自動化することも可能です。
5. Insights プランの実行により、統合された監査証跡情報を作成、提供します。この情報には、プランを実行した担当者、開始時間と終了時間、タスクレベルの実行が含まれています。

まとめ

金融ネットワークが進化してプログラマビリティを備え、アプリケーションの複雑さが増していく中、IT およびネットワーク環境の管理には自動化が極めて重要となります。Red Hat の自動化およびコンプライアンス・ソリューションは、IT とネットワークをエンドツーエンドで自動化し、金融サービスプロバイダーの悩みに応えます。

Red Hat Satellite でセキュリティに準拠するシステムのプロビジョニングと設定を行う場合や、Red Hat Insights のデータを使用してプロアクティブにセキュリティ問題への対策を行う場合、またはシンプルな自動化を使用してクラウドをデプロイ、管理、アップグレードする場合、いずれの場面においても、Red Hat Ansible Automation Platform はエンドツーエンドの自動化を実現するために必要な、自動化のための共通言語、運用レイヤー、公開 API を提供します。このアプローチは、全体的なセキュリティに対してデバイス固有およびアプリケーション固有のニーズがある組織に特に効果的です。Red Hat Ansible Automation Platform は、環境情報の検出を含め、Red Hat Enterprise Linux 環境全体で自動化を実現し、組織のポリシーに従い、このポリシーに基づいて構成の変更を処理します。

すべての Red Hat 製品は特定のベンダーに依存しないよう設計されているため、重要なレガシー・アプリケーションおよびプロセスを置き換えることなく利用中の IT 環境をサポートでき、さまざまなデバイス、プラットフォーム、ベンダーに対するセキュリティ関連のタスクとプロセスの統合およびオーケストレーションを可能にします。そして、Red Hat が重要なセキュリティ自動化をサポートし、サービス管理を単純化することで、ユーザー組織の人員はイノベーションの実現に集中できるようになります。

次のステップ

- セキュリティおよびコンプライアンスの自動化を開始または拡張するには、まず Red Hat のディスカバリー・セッションで IT 環境を分析し、自動化が可能な領域を特定します。Red Hat サービスでは、セキュリティおよび信頼性のワークフローを自動化する、より包括的なサービスも提供しており、Red Hat Insights、Red Hat Satellite、Red Hat Ansible Tower を組み合わせて、既存のギャップまたは Insights で特定された潜在的に問題がある構成を特定します。サービスによって提供されるスケーラブルなフレームワークで、Insights が提供する Playbook を使用およびカスタマイズするほか、顧客の Playbook を使用およびデプロイし、脆弱性を修復して IT 環境で監査証跡を提供します。

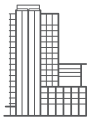
- Red Hat のセキュリティ管理テクノロジーで金融機関のインフラストラクチャにおけるリスクを低減する方法については、金融機関向けセキュリティおよびコンプライアンスの Web セミナーにご参加ください。

Red Hat ソリューションの詳細について

Red Hat Satellite、Red Hat Insights、Red Hat Ansible Automation Platform は、Red Hat OpenShift® クライアントなど、Red Hat ポートフォリオのセキュリティ管理と制御を強化します。

他の Red Hat テクノロジーはセキュリティとコンプライアンスの主な問題に特化して対処する機能を提供します。Red Hat では、今日の常に変化する環境ではエンドツーエンドのセキュリティ、コンプライアンス、監査のオーケストレーションが必要であると認識しており、管理と制御に必要なプラットフォームとツールを提供しています。

ご質問やその他の情報については、Red Hat の担当者にお問い合わせになるか、金融サービスの自動化に関する詳細をご覧ください。



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、Fortune 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。

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
0120 266 086
03 5798 8510

韓国
080 708 0880

マレーシア
1 800 812 678

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

jp.redhat.com
#F23392_0420