渡邊 悠貴
アマゾン ウェブ サービス ジャパン
ソリューションアーキテクト
2020/2/17作成

AWS INNOVATE 2020 オンラインカンファレンス

「システム管理で使えるデータ分析ハンズオン：システム構成情報の収集と可視化」のクイズおよび解答

AWS INNOVATE 2020のセッションの視聴およびアンケートにご記入頂きありがとうございます。本資料が「**システム管理で使えるデータ分析ハンズオン：システム構成情報の収集と可視化**」で出題されたクイズの解答になります。

Q1: 今回のハンズオンではシステムの構成情報の収集と可視化を行いました。さらにもう一歩進んで、次のようなことまで実現する場合、どのAWSサービスをどのように組み合わせればよいでしょうか。

- **社内で利用が禁止されているソフトウェアがインストールされたことを検知して、管理者に通報したりそのインスタンスを自動的に停止したい**

解答1: AWS Config を使用して、今回のハンズオンで構築したマネージドインスタンスのソフトウェアインベントリの変更を記録できます。AWS Config ルールを使用して、ソフトウェアの設定変更をモニタリングし、変更がルールに準拠しているかいないかの通知を受け取ることができます。AWS Configが提供するAWS マネージドルールの「ec2-managedinstance-applications-blacklisted」を利用することで、ブラックリストに指定した（つまり利用が禁止されている）アプリケーションがインスタンスにインストールされていないことを確認できます。マネージドルールにて利用が禁止されているアプリケーションがインストールされたことを検知した場合には、CloudWatch Eventsを経由して管理者に通知を行うことが可能です。CloudWatch Eventsで [Config Rules Compliance Change (設定ルールのコンプライアンス変更)] のイベントをトリガーすることで、コンプライアンスチェックが失敗したときに通知を受け取れます。また、Configルールの「修復アクション」を利用してSSM Automationを実行することでインスタンスの停止を行うことが可能です。次ページの図1.構成例をご参照ください。

渡邊 悠貴
アマゾン ウェブ サービス ジャパン
ソリューションアーキテクト
2020/2/17作成

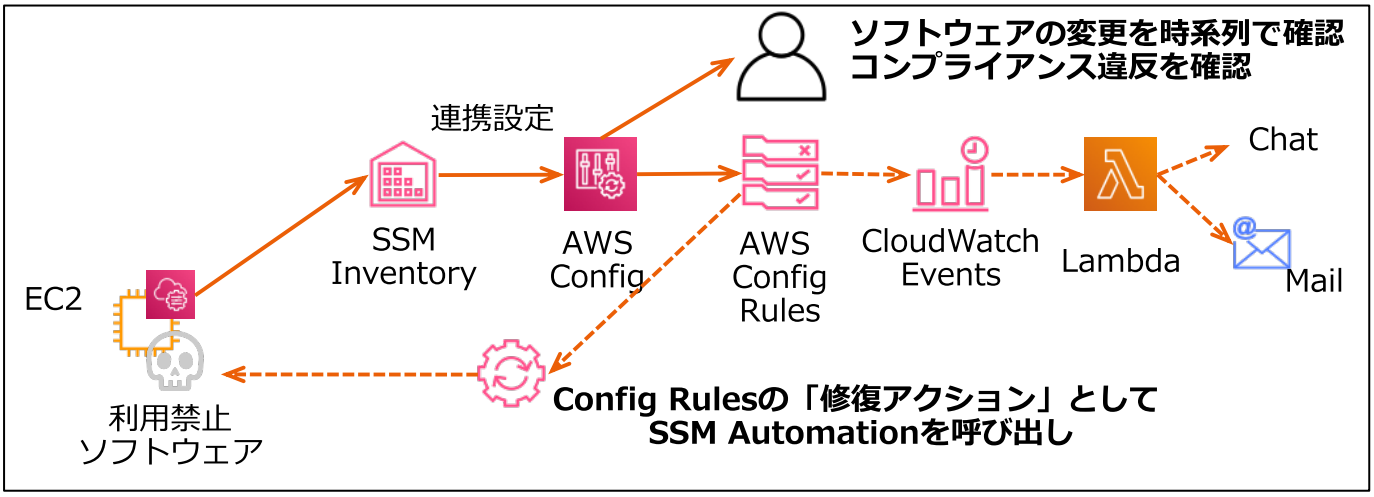

図1. 構成例

ご参考リンク

- マネージドインスタンスのソフトウェア設定の記録

  https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/recording-managed-instance-inventory.html
- ec2-managedinstance-applications-blacklisted

  https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/ec2-managedinstance-applications-blacklisted.html
- Amazon CloudWatch Events を使用した AWS Config のモニタリング

  https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/monitor-config-with-cloudwatchevents.html
- AWS Config ルールによる非準拠の AWS リソースの修復

  https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/remediation.html