AnsibleによるOWASP演習環境構築マニュアル（Amazon Linux 2023 / Let's Encrypt対応）

■ 概要

本書は、AWS EC2 (Amazon Linux 2023) 上にOWASP Top10対応の演習環境を自動構築するためのAnsibleプレイブックの使い方をまとめたものです。

■ 構成

本プレイブックは以下のロールで構成されています。

ロール名	機能
common	基本パッケージの導入とfirewalld設定
docker	DockerおよびComposeのインストールと演習環境展開
nginx	Nginxによるリバースプロキシ設定
certbot	Let's Encrypt証明書の自動取得と更新設定

■ 環境前提条件

- 対象OS: Amazon Linux 2023 - Python3 / Ansibleインストール済み - 対象EC2にSSH接続可能（pemキー利用） - ポート: 80, 443を開放済み

■ 実行手順

1. ZIPファイル(ansible-vulnlab.zip)を任意の作業ディレクトリに展開 2. inventories/production にEC2情報を記入 3. group_vars/all.yml にドメイン名と管理者メールを設定 4. 接続確認: ```bash ansible -i inventories/production vulnlab -m ping ``` 5. プレイブック実行: ```bash ansible-playbook -i inventories/production site.yml ``` 6. 完了後、HTTPSでサイトにアクセス

■ 成果物

- /home/ec2-user/vuln-lab-extended に演習環境が展開されます。 - Nginxが80番ポートで受け、内部8080のFlaskコンテナへ転送します。 - Let's Encrypt証明書はCertbotで自動取得し、cronで更新されます。

■ 保守ポイント

- 証明書更新確認: `sudo certbot renew --dry-run` - コンテナ更新: `docker-compose pull && docker-compose up -d` - Nginx設定変更時: `sudo systemctl reload nginx`

■ 注意事項

- EC2のセキュリティグループはSSH(22)を限定してください。 - Let's Encrypt利用には正しいDNS設定が必要です。 - 本環境は教育目的であり、本番運用には非推奨です。