# セキュリティ・アクション・ラボ 教育コンテンツの利用方法について

本ドキュメントはセキュリティ・アクション・ラボの IT システム関係社員向けサイバーセキュリティ研修の研修環境構築時及び研修時における本 GitHub 上の各ファイルの参照方法についてまとめたものである。

## I. プロジェクト概要

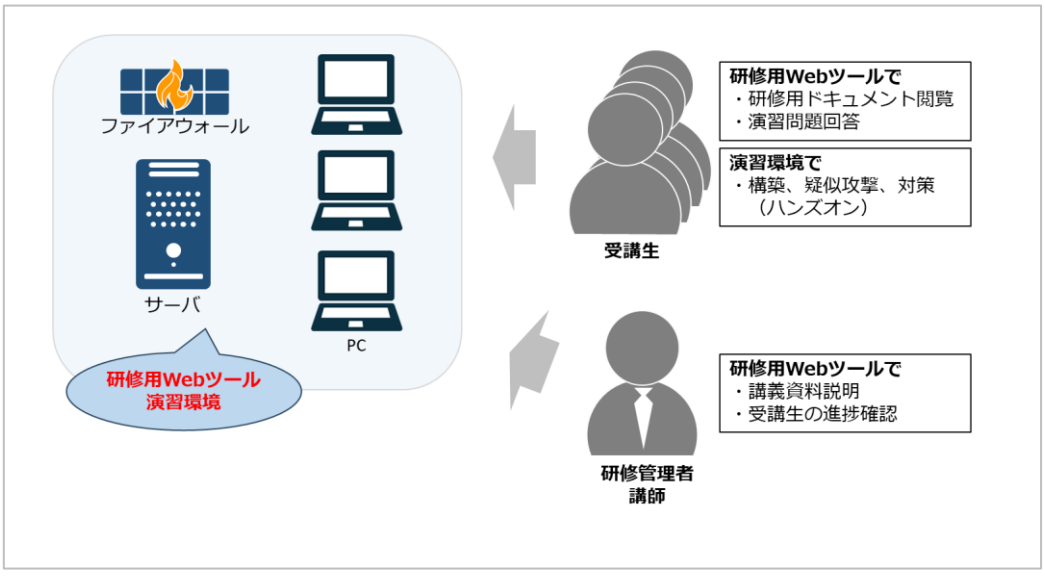
昨今、世界で、とりわけ日本ではサイバーセキュリティ人材が不足していると言われている。「サイバーセキュリティ体制構築・人材確保の手引き」[1]によると、必要なセキュリティ人材には「サイバーセキュリティ対策を主たる目的とする業務に従事する人材」だけでなく、「サイバーセキュリティ以外を主目的とする業務を遂行する中でサイバーセキュリティ対策に関わる人材」も含まれており、最近では後者の重要性が増してきている。つまり、セキュリティ統括や CSIRT などのセキュリティを主たる業務とする社員だけでなく、IT システム関係の業務に従事する社員は皆サイバーセキュリティに関する意識・知識を向上させていくことが求められている。

しかし、事業者の IT システム関係社員は IT システムの直に触れる機会が少なく、システム自体の動作原理を深く理解できていないため、サイバー攻撃の動作原理を理解できずに自ら必要な対策を検討・決定していくことができていない可能性がある。

そのため本プロジェクトでは、環境構築から疑似サイバー攻撃、対策まで実機を使用した研修を行うことで世の中の IT システム関係社員のサイバーセキュリティに関する意識・知識を向上させることを目的として IT システム関係社員向け研修「セキュリティ・アクション・ラボ」を作成した。

## II. 研修概要

III「研修環境構築」に従って研修環境を構築し、IV「研修実施」に従って研修を行うことで、受講生は研修用 Web ツールを使って研修用ドキュメント閲覧や演習問題の回答を、演習環境を使って構築・疑似攻撃・対策をハンズオン形式で行うことができる。また、研修の管理者・講師側は同じ研修用 Web ツールで講義の進行や受講生の進捗確認を行うことができる。




[1] 経済産業省・独立行政法人情報処理推進機構 「サイバーセキュリティ体制構築・人材確保の手引き」 http://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

III. 研修環境構築

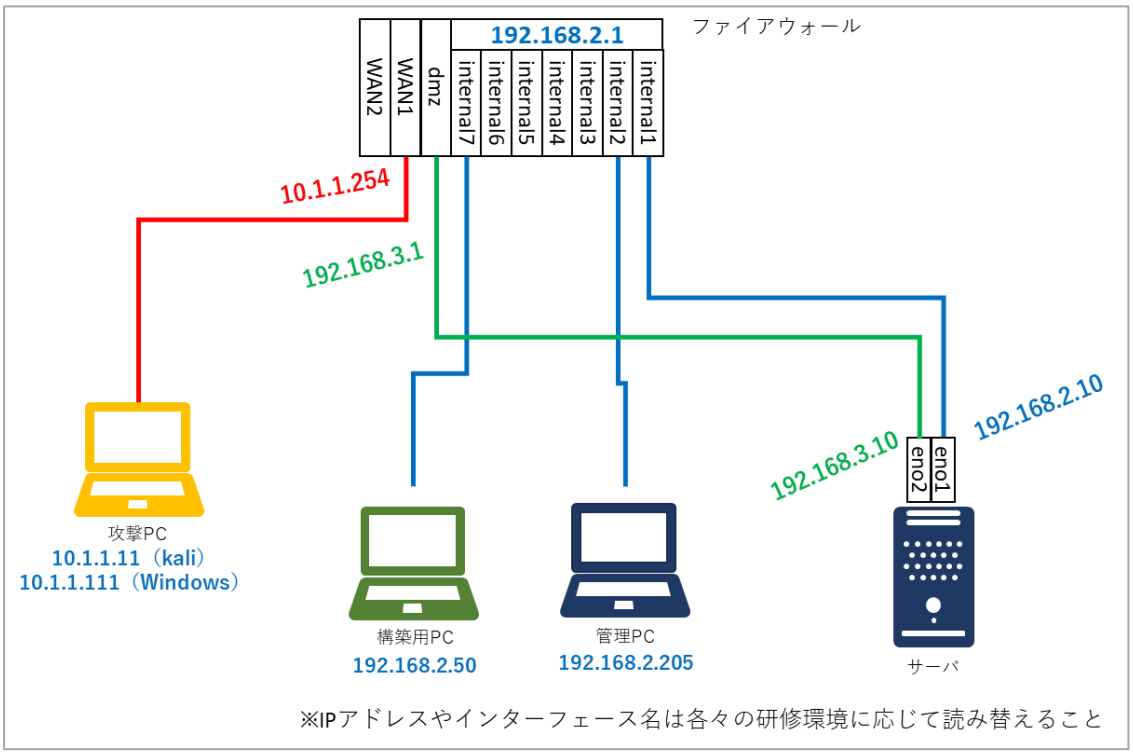
【https://github.com/sal-project/sal-setup-document】にアクセスして環境構築を行う。

1. 研修に必要なハードウェアを用意する（参考：HW.md）
2. ファイアウォールの設定を行う（参考：FW.md）
3. サーバ上にハイパーバイザ（proxmox）をインストールする（参考：Hypervisor.md）
4. DNS サーバの構築を行う（参考：DNS.md）
5. AD サーバの構築を行う（参考：AD.md）
6. ファイルサーバの構築を行う（参考：FS.md）
7. プロキシサーバの構築を行う（参考：Proxy.md）
8. Web サーバの構築を行う（参考：Web.md）
9. 研修用 Web ツール環境（以下、Secfarm）の構築を行う（参考：Secfarm.md）

IV. 研修実施

研修シナリオは「業務システム」と「Web システム」の 2 種類用意している。それぞれの研修実施に向けた準備は以下の通り。

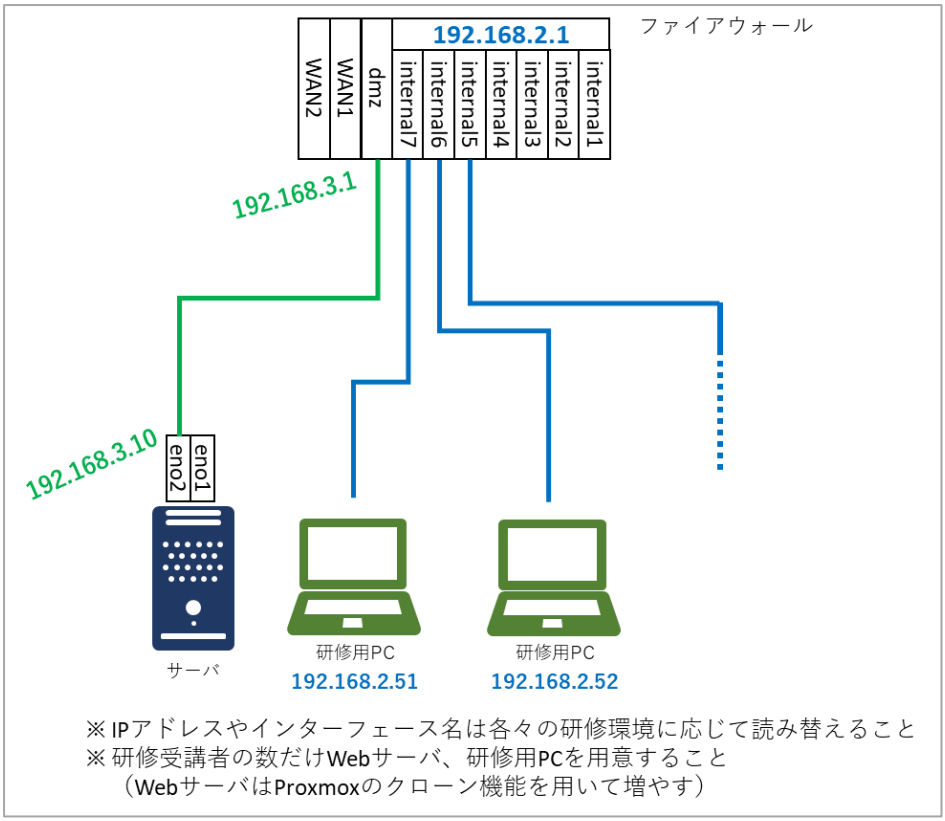
1. 業務システムシナリオ
   ① 以下の図の通り配線を行う。




   ② Secfarm に管理者アカウントでログインし、研修グループ分のユーザ作成及び研修権限付与を行う。

2. Web システムシナリオ

① 以下の図の通り配線を行う。




② Secfarm に管理者アカウントでログインし、研修グループ分のユーザ作成及び研修権限付与を行う。