MALWARE CONTAINMENT

事前学習資料

ストーリー

組織の端末がマルウエア（= コンピュータウィルス）に感染した !?
専門家の持つ特殊能力を駆使して、感染している端末を見つけ出せ !!

ある日、組織の端末がマルウエア（コンピュータウイルス）に感染しており、ハッカーによって遠隔操作されていることが分かった。

コンピュータセキュリティに関する問題に対応するため、CSIRT（シーサート）の一員であるプレイヤーは、仲間と協力して、遠隔操作をされている端末を探し出し、その端末を封じ込めなければならない。果たして、無事に封じ込めることができるのか？！

CSIRT とは

コンピュータセキュリティに関する問題（インシデント）に対応するため、専門家によって結成されたチーム。攻撃者は、気づかれないように組織の端末を悪用しようと狙っているため日ごろの通信を監視したりするほか、実際に問題が発生した際に、迅速に対応するため、調査方針や指示など調整を行ったりもする。

何をするゲーム？

インシデントにおける「初動対応」を再現したゲームです。端末がマルウエアに感染した場合、組織内の別の端末に感染が広がる場合や、組織内の機密情報が窃取される恐れがあります。それを防ぐために、**感染した端末を、ネットワークから切り離すことで、その端末がどこからも、どこへもアクセスできない状況にする（「封じ込め」と言われる）作業**を行います。

人物相関図

4日後には説明会だから、早く調査してくれ！

経営層

CSIRT

コマンダー

チームの全体統括と状況把握を行う。経営層と情報を連携し意思決定を支援する

フォレンジックエンジニア

実際に感染の疑いのある端末を保全する。また、マルウェアにどんな機能があるか解析ができる

リサーチャー

セキュリティ対策製品の出すアラートなどをログから分析したり、情報収集を得意とする

ノーティフィケーション

自組織内を調整し、各担当部署への情報発信を行うなど、情報連携を得意としている