1ZF-06

# サイバーセキュリティ演習システム CyExec 対応の IoT セキュリティ応用演習コンテンツ開発

渡辺 嶺†‡1,石川 大輔‡1, 駒野 勝己‡1, 盛 宸‡1, 畑谷 成郎‡1, 牧 宣彰‡1, 慎 祥揆‡2, 瀬戸 洋一‡1

公立大学法人首都大学東京 産業技術大学院大学 産業技術研究科

## 1. はじめに

IoT システムが普及するとともに, IoT システムを対象としたサイバー攻撃が行われ, 国内外で業務・サービス障害, 情報漏えい, 金銭被害が発生し, 経済の発展や生活の安全・安心が脅かされている[1].

産業技術大学院大学では, 実践的セキュリティ教育の普及のため, VirtualBox および Docker を利用した仮想環境からなる低コストかつ柔軟性のあるサイバーセキュリティ演習システム CyExec(Cyber Security Exercise System)を開発した[2].

今回 IoT システムに関するセキュリティを実践的に学ぶことができる演習コンテンツを開発し CyExec に実装した.

本発表では,IoT システムに関する応用演習について説明する.

## 2. CyExec 概要

### 2.1. CyExec アーキテクチャ

CyExec は, 高等教育機関や中小企業での導入を想定した, OSS(Open Source Software)で構成するサイバー攻撃と防御の基礎技術を学ぶ演習システムである. 図 1 は CyExec のアーキテクチャを示す[2].

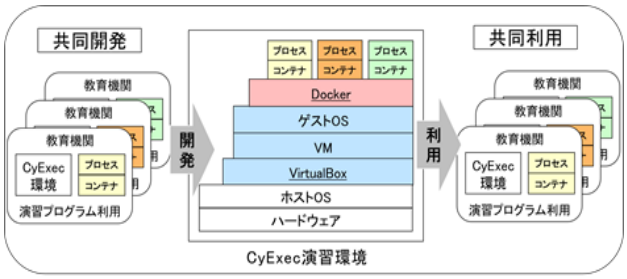


図 1 CyExec のアーキテクチャ

以下にその特徴を示す.

(1) 低コストで実現する移植性の高い演習環境

(2) 共同開発・利用の容易な演習環境

CyExec は, エコシステムの考えに基づき, 複数の組織が共同開発・利用し, 演習コンテンツを発展させることができる.

### 2.2. 演習コンテンツ

図 2 は, IoT セキュリティ演習コンテンツの構成を示す[4].

CyExec の演習コンテンツ構成は, 法と倫理, 基礎演習および応用演習からなる.

演習の受講者が学んだ攻撃技術を悪用しないよう, 最初に法と倫理の教育を実施する. 基礎演習は脆弱性の知識と検出方法の基本を学ぶ. 応用演習は, 仮想環境に再現した IoT システムを使用し, 実践的な技量を学ぶ[3]. 基礎演習には, WebGoat および Metasploitable/Kali Linux, 2 つの演習コンテンツを利用する. 応用演習は, 3.で紹介する.

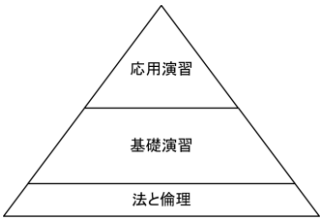


図 2 IoT セキュリティ演習コンテンツの構成

## 3. 応用演習の開発

応用演習としてデジタルサイネージとネットワークカメラの 2 つの演習コンテンツを開発した. 仮想マシンと IoT 機器を模擬した端末からなる演習環境で演習課題を実施し, 攻撃と防御技術を修得する.

### 3.1. デジタルサイネージ演習

ネットワークに接続した複数のディスプレイからなるデジタルサイネージシステムを想定する. ネットワークに接続され管理者が遠隔ログイン, 表示内容を HTTP 通信により変更するシステムである. 攻撃は, Web アプリケーションの脆弱性を利用した攻撃 CSRF(Cross-Site Request Forgeries)である. 演習時の動作から攻撃と脆弱性の原理および対策の必要性を学習する.

#### 3.1.1. システム構成

CyExec に WebWolf(攻撃者用ツール)のコンテナを実装し, Docker 上で動作させる. WebWolf は, 攻撃者が作成した攻撃ファイルを設置する罠サーバと, 使用者(デジタルサイネージ管理者)に送付する攻撃ファイルへのリンクの役割を担う.

デジタルサイネージは別途構築した Raspbian の仮想マシンに搭載し指定した画像をディスプレイ(VNC(Virtual Network Computing))に出力する.

#### 3.1.2. 演習シナリオ

演習のシナリオを以下に示す.

(1) 通常操作の確認

- 使用者(管理者)はデジタルサイネージの Web アプリケーションに ID とパスワードを入力しログイン
- パスワード変更の操作を行い意図したとおりにパスワードが変更されること,および, 画像のアップロードを行いディスプレイに意図した画像が表示されることを確認

---

Development of IoT security exercise contents in Cyber Security Exercise System

†Watanabe Ryo

‡1Advanced Institute of Industrial Technology

‡2Tokai University School of Information Science



Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.

(2) CSRF 攻撃シナリオ

図 3 は攻撃演習の概要を示す.

攻撃者は, OWASP ZAP を起動し, 上記(1)のパスワード変更, 画像アップロードの際にブラウザからデジタルサイネージに送られるリクエストを傍受

- 傍受した内容を元に攻撃用ファイルを作成, CSRF 攻撃を実現するコードを JavaScript で記述
- WebWolf を用いて攻撃用ファイルを罠サーバにアップロード, 使用者(管理者)がリンクをクリックすることにより攻撃が発動, 使用者(管理者)が意図しないパスワード変更と, 画像のアップロード・ディスプレイの表示変更を実行

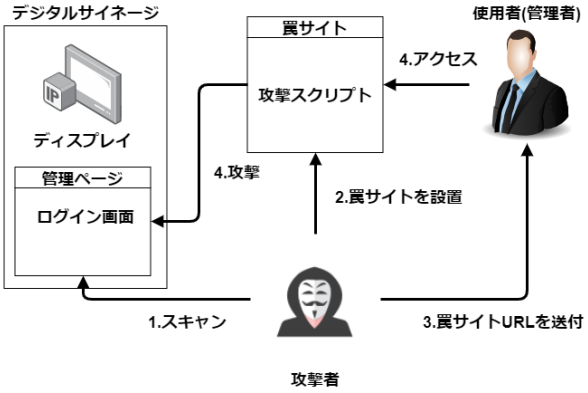


図 3 攻撃演習の概要

### 3.2. ネットワークカメラ演習

ネットワークに接続した監視ロボットのカメラを対象とし, 推測可能および強度が低いパスワードが設定されている状況を想定した. 攻撃は, SSH のパスワードに対する類推攻撃と, 総当たり攻撃である. 演習時の動作からパスワードの脆弱性および対策の効果を学習する.

#### 3.2.1. 演習環境

CyExecに攻撃ツール xHydra と VNC クライアント Reminna を実装する. 攻撃演習の操作は CyExec 上の xHydra から, 防御演習の操作は Reminna から実施する.

RaspberryPi に監視ロボットのネットワークカメラ機能を実装し, Raspberry Pi と CyExec を LAN ケーブルで接続する. 安全のため Raspberry Pi および CyExec のインターネットへの接続は無効化する.

#### 3.2.2. 演習シナリオ

図 4 は演習の概要を示す. 演習のシナリオを以下に示す.

(1) 攻撃シナリオ

- 攻撃者は, ネットワークカメラに使用されている機器が Raspberry Pi であることを目視で確認し, 検索エンジンなどで既定の ID/パスワードを調査, SSH でログインを試行
- 使用者(監視ロボット管理者)のパスワードの変更に対し脆弱性検査ツール xHydra による総当たり攻撃を実施, パスワードを解読
- 使用者(管理者)のパスワード変更に対し, 再度攻撃を実施, パスワードが容易に解読できないよう対策されたことを確認

(2) 防御シナリオ

- 使用者(管理者)は, 既定のパスワードを数字 3 桁のパスワードに変更
- 使用者(管理者)は, パスワードを強度の低い数字 3 桁より, 強度の高い数字 6 桁に変更

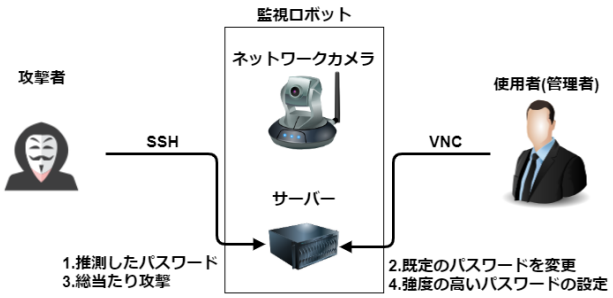


図 4 攻撃と防御演習の概要

## 4. おわりに

IoT システムを対象としたサイバー攻撃が増加し, 様々なサービスに被害が発生している.このためサービス提供者・利用者の意識と技術的改善が急務である.

サイバーセキュリティ演習システム CyExec に対し, IoT セキュリティに関する脆弱性の検出と防御技術を学べる 2 つの演習コンテンツを開発した. 一つはデジタルサイネージ, 他はネットワークカメラ演習である. これにより, 高等教育機関や中小企業で, IoT システムに対する攻撃と防御演習が可能となった.

## 謝辞

本研究は JSPS 科研費 JP16K 19K03006 の助成を受けたものである.

## 参考文献

[1]情報処理推進機構:情報セキュリティ白書 2019,2019 年 8 月.
[2]豊田真一,瀬戸洋一ほか: エコシステムで構成するサイバー攻撃と防御演習システム CyExec, CSS2018, 2018 年 10 月.
[3]渡辺嶺,瀬戸洋一ほか: IoT セキュリティ演習コンテンツの開発とサイバーセキュリティ演習システム CyExec への実装, SCIS2020,2020 年 1 月
[4] Nobuaki Maki, Yoichi Seto, et.al.: An Effective Cybersecurity Exercises Platform CyExec and its Training Contents, AEIT2020, 2020.1



Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.