E4-2

気象観測システムを題材としたペネトレーションテスト訓練教材開発

Development of Penetration Test Training Materials Using a Weather Observation System as a Subject

高井 遥香[*1]，小山慎哉[*2]
Haruka TAKAI[*1], Shinya OYAMA[*2]
[*1] 専攻科生産システム工学専攻，[*2] 生産システム工学科
[*1]Advanced Course of Production Systems Engineering, [*2]Department of Production Systems Engineering[*2]
[*1] [*2] 函館工業高等専門学校
[*1] [*2]National Institute of Technology, Hakodate College
Email: 23708@hakodate.kosen-ac.jp

あらまし：情報社会の急速な発展に伴い、業務の効率化やシステム開発などにおいて IT 技術の導入が盛んになってきている．IT 技術の導入の際には、悪意のある第三者からのサイバー攻撃に備えるための十分な対策を講じる必要があり、システムの危険性の理解と防衛体制の整備が今後の技術者に不可欠なスキルである．本研究では、「気象観測システム」を題材としペネトレーションテストが可能なサイバーレンジ環境を構築した．この環境で脆弱性を確認し、セキュリティ対策をまとめ、教材として提供することで適切な対策が行えるよう支援することを目的としている．
キーワード：サイバー攻撃，セキュリティ，ペネトレーションテスト

1. はじめに

昨今、情報技術の急速な進展により、作業の自動化、システムの構築など、多岐に渡る技術革新が進んでいる．しかし、このような発展が進む中サイバーセキュリティへの関心や成熟度は個人だけでなく、組織全体においても十分でないと言われている．ネットワーク技術の導入では、悪意のある第三者からのサイバー攻撃に備えるため十分な対策が必要であり、そのためには危険性の理解と周知、防衛体制の整備が今後の技術者に不可欠なスキルとなる．同時に、実際の利用者であるユーザーがセキュリティ対策の重要性を理解する環境も同様に整備されるべきである．本研究では、鶴岡高専で開発された『気象観測システム』[(1)]を利用している．このシステムは、IT に詳しくない農業従事者にも導入されているが、簡単に導入できるため、インターネットに接続しているシステムが常にサイバー攻撃の危険にさらされていることについて、ユーザーの理解が低い可能性があり、攻撃されていても気付かない懸念がある．また、こういうシステムを開発する側がセキュリティ対策にいて深く理解し、システムの設計段階からセキュリティを考慮できるような教育も重要である．

2. 本研究の目的

本研究の目的は、この「気象観測システム」へのサイバー攻撃耐性を検証するためのペネトレーションテストが可能なサイバーレンジ環境を構築し、技術者がサイバー攻撃に対する適切なセキュリティ対策を学んでもらうことである．またユーザーのセキュリティを高める必要性を理解してもらうための環境も構築する．

3. 気象観測システム

気象観測システムのシステム構成図を図 1 に示した．このシステムは、以下の 7 項目を観測している．

・気温　・風向　・湿度　・雨量
・気圧　・日射量　・風量

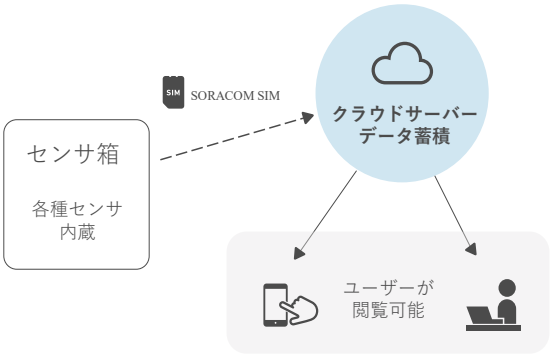

図 1 気象観測システム構成図

まずは、センサを内蔵した箱(図 2)を観測地に設置する．センサ箱内には Wio という LTE ボードが装着されており、SORACOM SIM の SORACOM Beam というデータ転送サービスを使用して、センサデータを一定時間ごとにクラウドサーバーへ転送する．その後、クラウドサーバーでデータを蓄積し、ユーザーは PC やスマートフォンを利用して観測データを閲覧することができる．

図 2 センサ内蔵箱

3.1 開発環境

この気象観測システムはJavaで開発されているが、本研究では疑似的なサイバー攻撃を模擬するために、脆弱性を持つシステムを作りやすいという観点からPHP で再実装を行っている．開発環境は以下の通りである．

サーバ OS：Ubuntu 22.02
サーバサイド：PHP Version 8.1.2
データベース：MariaDB 10.6.16

3.2 データ閲覧

蓄積した観測データの閲覧、観測項目別のデータ閲覧､年月指定の絞り込みが可能な画面を作成した．さらに、観測項目ごとに日付指定を行い一日のデータの変化が確認できるグラフ表示が可能である．

4. ペネトレーションテスト教材

独立行政法人情報処理推進機構(IPA)から提供されている､「安全なウェブサイトの作り方 改訂第 7 版のチェックリスト」(3) に基づき、以下の 5 項目の攻撃手法のシナリオを用意し､Web アプリ開発者が、脆弱性の体験と脆弱性を排除するための方法について学ぶ教材を開発する．

① SQL インジェクション
1. フォーム入力値をそのまま用いて SQL 文を組み立てるように実装
2. SQL インジェクション攻撃による脆弱性の存在の確認
3. プレースホルダを利用して再実装
4. SQL インジェクションが防御されたことを確認

②OS コマンド・インジェクション
1. シェルを起動できるようにプログラムを組んでおく
2. OS コマンド・インジェクション攻撃により、ls などの OS コマンドが実施できることを確認
3. シェルを起動できないように再実装
4. 防御確認

③ディレクトリ・トラバーサル
1. 外部からのパラメータにウェブサーバー内のファイル名を直接指定
2. ディレクトリ・トラバーサル攻撃
3. 外部からのパラメータにウェブサーバー内のファイルを直接指定せず再実装
4. 防御確認

その他､クロスサイト･スクリプティングや HTTP ヘッダ・インジェクションに関しても、同様のシナリオを用意し、教材化する予定である．

5. ユーザー用疑似フィッシングサイト

ユーザーにインターネットに接続されたシステムの危険性を理解してもらい、セキュリティ意識を高めてもらうためにユーザー側に考えられる攻撃手法の再現を行う．本研究では、フィッシングサイト利用したサインイン情報の搾取を想定した環境を構築した．疑似的なフィッシングサイトを体験してもらい、フィッシング対策を促す目的である．シナリオとしては以下の流れに沿い体験してもらう．

1. サイトのログイン画面をユーザー側画面に表示し、ユーザーはログイン情報を入力
2. しかしログインはできず、ユーザーは状況がわからない
3. この時点で攻撃者側の DB に搾取したログイン ID とパスワードが蓄積される
4. 攻撃者側の DB を確認し、ログイン情報が抜き取られていることを確認してもらう

6. まとめ

Web アプリ開発者は、技術革新と共にセキュリティ意識を高め、ユーザーと協力して安全なシステムを構築・運用することが必要である．このように、セキュリティの理解と対策を包括的に強化することが、情報技術の発展に伴う新たな課題への対応策となると考えており、この教材がその一助となることを目指す．

参考文献

(1) Jeyeon Kim, Daichi Minagawa, Daiki Saito, Shinichiro Hoshina and Kazuya Kanda: “Development of KOSEN Weather Station and Provision of Weather Information to Farmers” , Biennial State-of-the-Art Sensors Technology in Japan 2019-2020 (2020)
(2) Peter Kim:サイバーセキュリティテスト完全ガイド ~Kali Linux によるペネトレーションテスト,マイナビ出版(2016)
(3) 安全なウェブサイトの作り方 改訂第 7 版~ウェブアプリケーションのセキュリティ実装とウェブサイトの安全性向上のための取り組み, 独立行政法人情報処理推進機構(IPA) セキュリティセンター(2021)