G-52

無線 LAN 利用者のセキュリティ意識向上を目的とした 無線 LAN セキュリティリスク体験型学習システムの開発

Aiming to raise security awareness among wireless LAN users Development of a Wireless LAN Security Risk Experiential Learning System

塩田 晃平* 谷口 義明†, ‡ 井口 信和†, ‡
Kohei Shiota Yoshiaki Taniguchi Nobukazu Iguchi

1. 序論

スマートフォンやタブレット等の携帯端末の普及により，無線 LAN を利用する機会が増加している．無線 LAN の利点として，ネットワーク技術に精通していない人でも簡単に設定を施し利用することができる．これは大きい利点であるが，無線 LAN のセキュリティ対策をせずに利用した場合，様々なセキュリティリスクが存在する．

無線 LAN 利用者側のセキュリティリスクとして，通信内容の盗聴，改ざん，なりすまし，偽装の危険性が挙げられる[1][2]．これらのセキュリティリスクが存在しているが，総務省が無線 LAN 利用者 1，400 人に対してアンケートを取ったところ，HTTPS 通信を確認している人が 56．2%しかいない．また，暗号化方式を確認している人が 36．7%しかおらず，無線 LAN の暗号化方式の有無やその種類を知らない，もしくは分からない人が 31．0%も存在することが判明している[3]．このことから，無線 LAN 利用者のセキュリティ意識は高くないことが分かる．そのため，無線 LAN に対するセキュリティ対策が必要となってくる．

しかし，無線 LAN 利用者側のセキュリティ対策として攻撃を検知できる技術は存在するが，特殊なハードウェアが必要となる[4]．また，これは確実に検知できるものではない．現状のセキュリティ対策では無線 LAN 利用者の負担が大きくなると考えられ，利用者側のセキュリティ対策としては好ましくない．このことから，無線 LAN 利用者に対するセキュリティ対策ではなく，利用者のセキュリティ意識を向上させる必要があると考えるに至った．

そこで本研究では，無線 LAN 利用者のセキュリティ意識向上を目的に，無線 LAN セキュリティリスク体験型学習システム(以下，本システム)を開発する．本システムにより，無線 LAN のセキュリティリスクを体験することで，利用者のセキュリティ意識向上と利用時の知識不足を改善することが期待できる．また，本システムは学習用アクセスポイント(以下，AP)上で構築するため，実運用されているネットワークやサーバに影響を及ぼさずに学習をすることができる．

＊ 近畿大学大学院総合理工学研究科，
Graduate School of Science and Engineering Research，Kindai University．
† 近畿大学理工学部情報学科，
Department of Informatics，Faculty of Science and Engineering，Kindai University．
‡ 近畿大学情報学研究所，
Cyber Infomatics Research Institute．

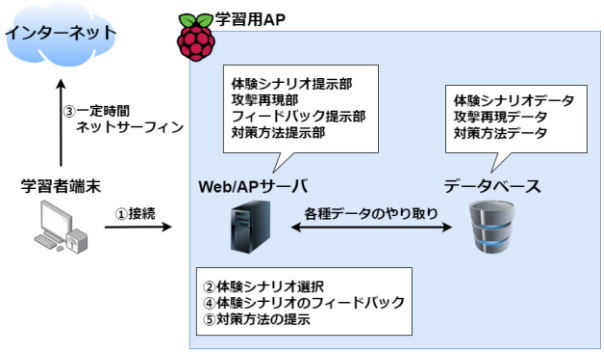


図 1:システム構成図

2. 関連研究

本研究のようにネットワークセキュリティ学習システムに関連した研究として，福山らの仮想マシンを活用したネットワークセキュリティ学習支援システム[5]がある．福山らのシステムは，仮想マシンを仮想的なネットワーク機器として動作させる．そして，ホストやルータ等の機器同士を仮想的に相互接続することで，1 台の PC 上に実機を使用した場合と同様のネットワークセキュリティ演習環境を構築する．これにより，ネットワークセキュリティの演習を低コストかつ安全，手軽に実施することができる．しかし，仮想技術の仕様上，仮想機器間で無線 LAN を利用した通信の実現が困難である．このことから，福山らのシステムでは，学習項目から無線 LAN に関するセキュリティの学習項目が対象外となっている[6]．

次に，八代らの体験型サイバーセキュリティ学習システムがある[7]．八代らのシステムは，クラウド上に演習環境と学習支援システムが構築されている．クラウド上に構築することで，時間・場所を問わずセキュリティインシデントを演習することができる．さらに，演習内容の概要及び演習をする上で必要な知識を学習することもできる．しかし，無線 LAN のセキュリティに関する演習は用意されていない．

3. 研究内容

3.1. システム構成

本システムの構成を図1に示す．本システムは新人研修や社内研修，無線 LAN に不安を覚えている人を対象に，無線 LAN のセキュリティリスクを体験できるシステムである．Rasberry Pi 4B(以下，ラズパイ)を AP 化し，学習用 AP として動作させる．Web/AP サーバの OS には，Ubuntu 20.04 LTS，Web サーバソフトウェアには，Nginx 1.20.0，Web アプリケーションフレームワークには，

Django 3.2.4 を使用する．データベースには，PostgreSQL 13.0 を使用する．

体験シナリオ提示部では，学習者に体験する無線 LAN のセキュリティリスクを一覧で表示する．

攻撃再現部では，主に中間者攻撃に関する無線 LAN のセキュリティリスクを再現する機能を持つ．再現する例として，ARP スプーフィング攻撃や Evil Twins 攻撃等の無線 LAN のセキュリティリスクを再現する．ARP スプーフィング攻撃とは，ARP の応答を偽装することによって，ルータのなりすましをする攻撃のことである．この攻撃により，LAN から WAN に流れる通信内容がすべて盗聴される危険性がある．Evil Twins 攻撃とは，安全な AP と見せかけ，接続した通信機器の通信内容を盗聴する攻撃のことである．この攻撃では，盗聴以外にもマルウェアやボットネットといった不正なペイロードを接続している通信機器にダウンロードさせる危険性もある．

フィードバック提示部では，学習者が無線 LAN のセキュリティリスクを体験後，無線 LAN のセキュリティリスクに沿ったフィードバック内容を保持する機能を持つ．

対策方法提示部では，体験した無線 LAN のセキュリティリスクの対策方法と，フィードバック提示部から得た情報を元に対策方法を提示する機能である．

データベースには体験するセキュリティリスク，再現する攻撃，対策方法といった情報を格納する．

3.2. 学習手順

まずはじめに，学習者は学習用 AP であるラズパイに接続し，学習用 AP 上にある本システムに接続する．その後，体験シナリオ提示部で体験する無線 LAN のセキュリティリスクを選択し，一定時間ネットサーフィンをしてもらう．一定時間経過後，学習者はフィードバック画面に接続し，体験した無線 LAN のセキュリティリスクのフィードバックを確認する．最後に，無線 LAN のセキュリティリスクの危険性を確認してもらった後，対策方法提示部で体験した無線 LAN のセキュリティリスクの対策方法を学習してもらう．以上が本システムの学習手順となる．フィードバックの例として，図 2 に ARP スプーフィング体験後のフィードバック画面を示す．画面には盗聴した情報，インターネットの利用方法に関する評価，対策方法，HTTP 通信と HTTPS 通信の見分け方を表示している．

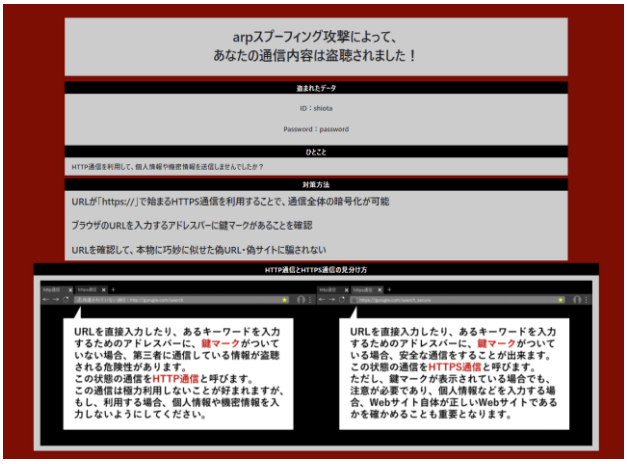


図 2:フィードバック画面

4 実験

実験は普段無線 LAN を利用している人物を対象に，無線 LAN のセキュリティ意識向上と無線 LAN のセキュリティリスクに関する理解度を増加できるかを確認する．実験の手順として，まず実験対象者には，無線 LAN のセキュリティに関する事前アンケート・テストを実施する．事前アンケート・テスト実施後，本システムで再現する無線 LAN セキュリティリスクを体験してもらう．無線 LAN のセキュリティリスク体験後，事後テスト・アンケートを実施する予定である．最後に，事前・事後テストの結果を開示し，事前・事後テストの結果，事前・事後アンケートの結果から本システムが無線 LAN 利用者のセキュリティ意識向上と無線 LAN のセキュリティリスクに関する理解度が増加できているかを確認する予定である．

5 結論

本研究では，無線 LAN 利用者のセキュリティ意識向上を目的に，無線 LAN セキュリティリスク体験型学習システムを開発した．本システムを使用することで，利用者のセキュリティ意識向上と利用時の知識不足を改善することが期待できると考えられる．

今後の予定として，本システムで体験できる無線 LAN のセキュリティリスクの追加をすることで，利用者のセキュリテイ意識がより向上できるようにする予定である．

参考文献

[1] Suroto，WLAN Security: Threats And Countermeasures，International Journal On Informatics Visualization，Vol. 2，No. 4(2018), pp. 232-238.

[2] Yeshwanth Valaboju，A Comprehensive Overview of WLAN Security Attacks，International Journal ofScientific Research & Engineering Trends，Vol.7，Issue 1，Jan-Feb-2021.

[3] 総務省:Wi-Fi 利用者向け簡易マニュアル，入手先<https://www．soumu．go．jp/main_content/000690266．pdf>(参照 2021-07-02)

[4] 保安隆明，ネットワーク情報を利用した無線 LAN 不正アクセスポイント判定手法，法政大学大学院紀要.理工学・工学研究科編，57 巻，pp. 1-8，2016-03-24.

[5] 福山和生，谷口義明，井口信和，仮想マシンを活用したネットワークセキュリティ学習支援システムの実装と評価，情報処理学会論文誌，Vol. 57，No. 3，pp. 931-935，2016-03-15.

[6] 福山和生，谷口義明，井口信和，仮想マシンを活用したネットワークセキュリティ学習支援システムにおける攻撃エージェントの実装と評価，インターネットと運用技術シンポジウム 2015 論文集，2015 巻，pp. 73-78，2015-11-26.

[7] 八代哲，田邉一寿，斎藤裕太，斎藤孝道，体験型サイバーセキュリティ学習システムの提案と構築，情報処理学会コンピュータセキュリティシンポジウム 2017 論文集，2017 巻，2 号，2017-10-16.