7ZH-01

ゴールベースシナリオ理論に基づいた 無線 LAN のセキュリティリスク学習システムの開発

塩田晃平* 谷口義明†‡ 井口信和†‡
近畿大学大学院総合理工学研究科* 近畿大学理工学部情報学科† 近畿大学情報学研究所‡

1 序論

スマートフォンやタブレットといった携帯端末の普及により，無線 LAN 利用者が増加している．無線 LAN は有線 LAN のような物理的制約が少ない．また，簡単な設定で利用できるため，公共施設における公衆無線 LAN 等，様々な場所の通信環境として用意されている．しかし，セキュリティ対策をせずに無線 LAN を利用した場合，様々なセキュリティリスクが存在する．

無線 LAN のセキュリティリスクとして，通信内容の盗聴や改ざんといった Man In The Middle（以下，MITM）攻撃や不正なアクセスポイントの設置といった危険性がある[1][2][3]．これらの技術的対策として，暗号強度の高い暗号化方式の設定や特別な製品を利用することが挙げられるが，全ての公衆無線 LAN で十分な技術的対策がされているわけではない．そのため，技術的対策だけでなく利用者のセキュリティ意識の向上も重要である．しかし，総務省の調査[4]によると公衆無線 LAN 利用者のセキュリティ意識は高いとはいえない．このことから，利用者のセキュリティ意識を向上させる仕組みが必要である．

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，ゴールベースシナリオ（以下，GBS）理論に基づいた無線 LAN のセキュリティリスク学習システム（以下，本システム）を開発する．GBS とは，「失敗することにより学ぶ」経験を疑似的に与えるための学習環境として，物語を構築する理論である[5]．

本システムにより，無線 LAN のセキュリティリスクを体験的に学習することで，無線 LAN のセキュリティに対する意識向上と利用時における知識不足を改善することが期待できる．本システムは学習用のアクセスポイント（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できる．

2 提案システム

本システムは，社内研修や無線 LAN に不安を覚える人（以下，学習者）が自己学習をする場合等に利用することを想定する．本システムにより，無線 LAN のセキュリティリスクを学習できる．

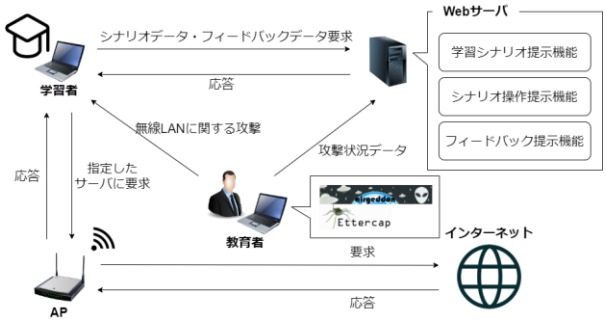

図 1：システム構成

2.1 システム概要

GBS 理論に基づいて作成した教材の設計を表 1 に示す．学習者には，架空企業に勤務し，公共施設でテレワークを実施している従業員という役割を持たせる．この従業員に対して，企業が指定するサイトにログイン操作し，個人情報が記載されたファイルを送信する使命を与える．シナリオ操作では，無線 LAN を選択しインターネットへの接続やログイン，ファイル送信といった操作をしてもらう．シナリオ操作のフィードバックでは，操作した結果に応じて詳細な解説を提示する．また，危険性をより体感してもらうために，学習者自身が実際に攻撃されている様子を動画で表示する．情報源では，シナリオ進行に支障がないように画面の操作方法や無線 LAN の基礎的な知識を提示する．

このような学習を実施するために設計した本システムの構成を図 1 に示す．本システムは，学習者 PC と教育者 PC，Web サーバで構成する．学習者 PC の OS は指定しない．教育者 PC には，Kali Linux 2021.3 と MITM 攻撃に特化したソフトウェアである Ettercap，偽の AP を作成できる Airgeddon を導入する．また，Monitor モード機能を持つ無線 LAN アダプタを使用する．Web サーバは，Node.js の Web フレームワークである Express で作成する．

以下，本システムで実装を予定している 3 つの機能について述べる．

2.2 学習シナリオ提示機能

本機能は，学習者に無線 LAN のセキュリティリスクに関する学習シナリオを提示する機能である．本システムで学習できる無線 LAN のセキュリティリスクとして，ARP Spoofing 攻撃や sslstrip 攻撃，Evil Twins 攻撃がある．ARP Spoofing 攻撃は，ARP

Development of a Security Risk Learning System for Wireless LANs Based on Goal Based Scenario Theory
*Kohei SHIOTA †, ‡Yoshiaki TANIGUCHI, Nobukazu IGUCHI
*Graduate School of Science and Engineering Research, Kindai University.
†Faculty of Science and Engineering, Kindai University.
‡Cyber Informatics Research Institute, Kindai University.

表 1：設計した GBS 教材

GBS 要素		GBS 教材
シナリオ文献	使命	公衆無線 LAN を選択し，特定のサイトに個人情報を記載したファイルを送信する作業をする．
	カバーストーリー	テレワークを実施している架空企業の従業員として勤務している場面を想定する．
	役割	個人情報を記載したファイルを特定のサイトに送信する．
学習目標		無線 LAN 利用者のセキュリティ意識の向上
シナリオ操作		特定のサイトでログイン操作やファイルを送信する．
シナリオ構成	フィードバック	操作した結果に応じて，詳細な解説を提示する．
	情報源	画面の操作方法や無線 LAN に関する基礎的な情報を提示する．

テーブルを不正に書き換え，通信内容を盗聴する攻撃である．sslstrip 攻撃は，MITM 攻撃によって SSL の機能を無効にする攻撃である．Evil Twins 攻撃は，公衆無線 LAN において偽の AP を設置し，気付かずに接続した利用者の通信内容を盗聴する攻撃である．本機能では，これらに関するシナリオを提示する．

2.3 シナリオ操作提示機能

本機能は，支障なくシナリオを進行できるよう，学習者にシナリオの操作方法を提示する機能である．教育者に対しては，シナリオ開始時に攻撃の様子が録画できるように画面キャプチャを促す．また，シナリオの進行具合に沿って，ARP Spoofing 攻撃や sslstrip 攻撃といった攻撃を実行させるように促す．

2.4 フィードバック提示機能

本機能は，シナリオを操作した結果に応じた詳細な解説や対策方法を学習者に提示する機能である．また，無線 LAN のセキュリティリスクをより体感してもらうために，学習者に対して実際に攻撃している様子を動画で表示する．表示する動画として，教育者が画面キャプチャしたファイルを使用する．

3 実験

実験は，本稿で設計した GBS 教材の評価実験と利用評価実験を実施する予定である．

GBS 教材の評価実験では，根本ら[5]が作成したチェックリストを使用する．このチェックリストは GBS 理論を構成する 7 つの要素ごとにチェック項目が存在しているため，教材を改善するための良い情報となる．そこで，設計した GBS 教材を使用する利点と改善点を明確にするために，このチェックリストで GBS 教材の評価をする予定である．

利用評価実験では，普段無線 LAN を利用している実験協力者 10 名を対象に，本システムが無線 LAN のセキュリティ意識向上とセキュリティリスクに関する理解度を増加できるか確認する．現在，対象とする実験協力者の選定方法を検討中である．実験手順として，はじめに実験協力者に無線 LAN のセキュリティに関する事前アンケートとテストを実施する．なお事前テストの結果は最後に開示する．これは事前テストの結果を復習することの影響を排除するためである．事前アンケートと事前テストの実施後，実験協力者に，本システムで設計した GBS 教材のシナリオに沿って，無線 LAN のセキュリティリスクを学習してもらう．シナリオの学習後，事後テストと事後アンケートを実施する．これらの結果から，本システムを用いることにより，無線 LAN 利用者のセキュリティ意識向上と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確認する予定である．

4 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，GBS 理論に基づいた無線 LAN セキュリティリスク学習システムを検討した．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が期待できる．

今後，GBS 教材や無線 LAN のセキュリティリスクの学習項目を追加する予定である．

参考文献

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

[2] Yeshwanth Valaboju, A Comprehensive Overview of WLAN Security Attacks, International Journal of Scientific Research & Engineering Trends, Vol.7, No.1, pp.244-251, 2021.

[3] Ibrahim Ghafir, Konstantinos G. Kyriakopoulos, Francisco J. AParicio-Navarro, Sangarapillai Lambotharan, Basil Assadhan, Hamad Binsalleeh, A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection, IEEE Access, Vol.6, pp.40008-40023, 2018.

[4] 総務省, Wi-Fi 利用者向け簡易マニュアル, 2020. <https://www.soumu.go.jp/main_content/000690266.pdf> (参照 2021-12-17)

[5] 根本淳子, 鈴木克明, ゴールベースシナリオ(GBS)理論の適応度チェックリストの開発, 日本教育工学会論文誌, Vol.29, No.3, pp.309-318, 2005.