G-49

失敗体験から学習する 無線 LAN のセキュリティリスク学習システムの開発

Development of a Learning System for Security Risks of Wireless LANs from Failure Experiences

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 は物理的な制約が少なく，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．

代表的な無線 LAN のセキュリティリスクとして MITM (Man in the Middle)攻撃が挙げられる．MITM 攻撃は，攻撃者が 2 者間で通信をしているところに割り込み，通信内容の盗聴や改ざんをする攻撃のことである．MITM 攻撃の種類として，ARP Spoofing 攻撃や DNS Spoofing 攻撃，sslstrip 攻撃が挙げられる．ARP Spoofing 攻撃は，被害者の ARP テーブルを不正に書き換え通信内容を盗聴する攻撃のことで，個人情報や機密情報を漏洩する危険性がある．DNS Spoofing 攻撃は，被害者の DNS 情報を不正に書き換え，攻撃者が用意した偽サイトに誘導させる攻撃のことで，個人情報の漏洩や不正な JavaScript を注入される危険性がある．sslstrip 攻撃は，HTTPS 通信を HTTP 通信に書き換える攻撃のことで，ARP Spoofing 攻撃と組み合わさることで個人情報を漏洩する危険性がある．

これらの対策として，arpwatch や適切なファイアウォールの設定，脆弱性に対する定期的なパッチの適用[1]，HSTS (HTTP Strict Transport Security)といったものが存在する．しかし，ARP Spoofing 攻撃には完全な解決策が存在しない[2]．DNS Spoofing 攻撃においても，全ての公衆無線 LAN 環境下で適切なネットワーク設定が施されているとは限らない．また，HSTS を回避する攻撃方法も提案されており[3]，これらの攻撃は未だ危険性のある攻撃となっている．

技術的な対策以外では，暗号化方式の確認や HTTPS 通信の確認，正しい URL か確認するといった利用者側の対策も考えられる．しかし，総務省が公衆無線 LAN 利用者 1,400 名に調査を実施したところ，暗号化方式を確認している人は 36.7%，HTTPS 通信を確認している人は 56.2%しかいない[4]．このことから，無線 LAN 利用者のセキュリティ意識は高いとはいえない．そのため，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 理論[5]は，「失敗することにより学習する」ことであり，現実的な場面を想定して学習環境を構築する理論である．GBS 理論を構成するためには，「使命」，「役割」，「カバーストーリー」，「シナリオ操作」，「学習目標」，「フィードバック」，「情報源」の 7 つの構成要素を含む必要がある．本システムで使用する学習シナリオは，この 7 つの構成要素に基づいて作成している．

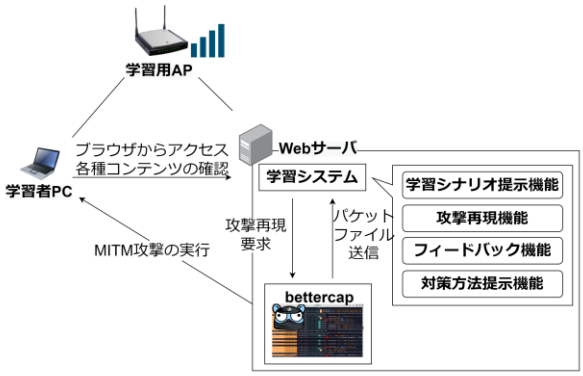

図 1:システム構成図

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の向上と理解度の向上を促進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)を用意して動作させる．そのため，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. 関連研究

本研究の関連研究として，実践型，体験型のネットワークセキュリティ学習システムが提案，開発されている[6][7]．また，sslstrip 攻撃を学習できるシステムを様々な角度から調査したところ，sslstrip 攻撃に関する研究[8][9][10]はあるが，sslstrip 攻撃を学習できるシステムは著者らが調べる限りなかった．

福山らの研究[6]では，セキュリティ人材の育成を目的に，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を開発している．福山らのシステムは，仮想マシンを活用して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．また，演習内容として ARP Spoofing 攻撃や DNS Spoofing 攻撃等，計 7 つの演習内容が用意されている．これに対して，本システムでは無線 LAN 利用者に着目した学習システムとなっており，福山らの学習支援システムにはない sslstrip 攻撃について学習することができる．

八代らの研究[7]では，クラウド上に演習環境と学習支援システムを構築することで，時間・場所を問わずセキュリティインシデントに関する演習をすることができる．八代らのシステムでは，演習項目として標的型攻撃と SQL インジェクションが用意されている．しかし，クラウド上に演習環境を構築するため，無線 LAN に関する演習を仮想的に用意することは困難である．

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

図 2:シナリオの進行方法を提示する画面の一例

これに対して，本システムでは学習用の AP を動作させ，学習環境を構築することで，無線 LAN に関する学習項目を用意している．

3. 提案システム

3.1. システム構成

本システムは，以下の項目に 1 つでも該当する人物を本システムの利用者（以降，学習者)として想定する．

- フリーWi-Fi の危険性は認識している
- 暗号強度が十分で脆弱性のない無線 LAN は安全であると認識している
- HTTPS 通信や URL を常に確認しない
- 無線 LAN に不安を感じている

本システムの構成を図1に示す．本システムは，学習用の AP と学習者 PC，Web サーバから構成する．学習用の AP は，Buffalo 製の WSR-1166DHPL2/N を使用した．Web サーバの OS には，Kali Linux 2022 Customised by zSecurity[1]，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，データベースは，SQLite 3.36.0 を使用した．また，Web サーバ内には，無線 LAN のセキュリティリスクを学習するために，学習シナリオ提示機能，攻撃再現機能，フィードバック提示機能，対策方法提示機能を実装した．

本システムでは，無線 LAN に対する MITM 攻撃の危険性を学習できる．学習できる項目は以下のとおりである．

- ARP Spoofing 攻撃による通信内容の盗聴
- DNS Spoofing 攻撃による偽サイトへの誘導
- sslstrip 攻撃による機密情報の搾取

これらの MITM 攻撃による危険性を学習できるように，MITM 攻撃の検証に利用できるペネトレーションツールの bettercap を Web サーバの OS である Kali Linux に導入した．

3.2. 学習シナリオ提示機能

学習シナリオ提示機能は，学習者に学習できる無線 LAN のセキュリティリスクの提示と学習シナリオの手順を提示する機能である．図 2 に学習シナリオの手順を示した画面の一例を示す．学習者は図 2 の画面を閲覧しながら学習シナリオを進めていく．また，画面右にある完了というチェックボタンを押下することで，実施済みの手順をグレーアウトにすることができる．これにより，現在どの手順を実施しているか一目でわかるようにしている．また，シナリオ進行に支障が出ないように情報源

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets 192.168.186.129
arp.spoof on
set net.sniff.local true
net.sniff on
```

図 3:ARP Spoofing 攻撃を自動化するスクリプト

として，手順の詳細な情報や無線 LAN に関する用語についての説明を適宜提示する．

3.3. 攻撃再現機能

攻撃再現機能は，無線 LAN に関する MITM 攻撃を再現する機能である．攻撃の再現には，bettercap を使用して，ARP Spoofing 攻撃や DNS Spoofing 攻撃，sslstrip 攻撃を再現した．再現するにあたって，bettercap で動作させる上記の攻撃を自動化するスクリプトを実装した．図 3 に bettercap 用の ARP Spoofing 攻撃を自動化したスクリプトを示す．このスクリプトを bettercap の起動オプションに加えることで，bettercap を操作することなく本システムで学習できる MITM 攻撃を実施できる．また，学習者のみで無線 LAN のセキュリティリスクの学習が完結できるように，Python の subprocess モジュールを使用した．これにより，学習者がボタンを押下するだけで，本システムで学習できる MITM 攻撃を再現できるようにした．

3.4. フィードバック提示機能

フィードバック提示機能は，bettercap から送信されるパケットを解析し，学習者にシナリオを操作した結果に応じて解説を提示する機能である．パケットの解析には pyshark を使用した．pyshark は Python ライブラリの一種であり，キャプチャファイルまたはリアルタイムでパケットを分析することができる．本機能では，盗聴したパケットを成型して，学習者に分かりやすい情報で表示するために使用している．学習者に提示する内容を以下に示す．

- 盗聴した ID や Email，パスワード
- 情報漏洩が発生したサイトの URL
- HTTPS 通信となっているか確認したか
- 正しい URL かどうか確認したか

実際に無線 LAN のセキュリティリスクの危険性を体験し，危険性を学習することで無線 LAN のセキュリティ意識の向上を促進することが期待できる．

3.5. 対策方法提示機能

対策方法提示機能は，本システムで学習できるセキュリティリスクの対策方法を提示する機能である．対策方法の一例を以下に示す．

- セキュリティが保証されていない場所では機密情報を入力しない
- HTTPS 通信か常に確認する
- 情報を入力して送信する場合，正しい URL を確認する
- 端末を常に最新のファームウェアにする[11]
- 正しいサイトをブックマークする[12]

本システムで無線 LAN のセキュリティリスクを学習した後，本機能を使用することで無線 LAN のセキュリティリスクに関する理解度の向上を促進することが期待できる．

3.6. 学習手順

学習者には，GBS 理論に基づいた学習シナリオを学習してもらう．学習内容として，ある企業に勤務する従業員としてテレ

[1] https://zsecurity.org/download-custom-kali/

ワークを実施している場面を想定 (カバーストーリー)してもらい，合計 3 つの作業 (使命，シナリオ操作)をこなしてもらう．1 つ目は，機密情報をまとめたファイルを指定するサーバにログイン後，送信する作業である．2 つ目は，仕事で使用する資料を共有ファイルサーバからダウンロードし，一部を編集してアップロードする作業である．3 つ目は，企業の広報活動のために特定のサイトにログインし，簡単な企業 PR をしてもらう作業である(役割)．また，シナリオ進行に支障が出ないように，シナリオ進行に関する用語を確認することが出来る (情報源)．学習者は全ての作業終了後，フィードバック提示機能からシナリオ操作の評価を受ける (フィードバック)．フィードバック結果から，無線 LAN のセキュリティリスクの危険性を確認してもらい，対策方法提示機能で体験した無線 LAN のセキュリティリスクの対策方法を学習する．これにより，学習者は無線 LAN のセキュリティリスクに対する理解度を向上することができる (学習目標)．また，3 つの作業内容には MITM 攻撃により機密情報の漏洩といった失敗を誘発する手順を含める．

4 実験

実験は，動作検証実験と利用評価実験を実施する予定である．

動作検証実験では，実装した各機能が意図した通りに動作するか確認する．本検証では，ログイン操作やファイル送信といった手順を含む sslstrip 攻撃の学習シナリオと DNS Spoofing 攻撃の学習シナリオを動作させる．学習シナリオを進行し，フィードバックを受ける時に sslstrip 攻撃や DNS Spoofing 攻撃によって正しくログイン情報が盗聴できているか確認する．また，攻撃により盗聴したパケットが成型され，学習者に分かりやすい情報で表示されているか確認する．

利用評価実験では，基本情報技術者試験所有者もしくは同等のスキルを所有する実験協力者 10 名を対象に，無線 LAN のセキュリティに対する意識の向上と理解度の向上を促進できるか確認する．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．事前アンケートと事前テストの実施後，実験協力者に，本システム上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．最後に学習者にテスト結果を開示する．これはセキュリティリスクの体験による理解度の定着かテスト結果を復習したことによる理解度の定着か判断できないからである．これらの結果から，本システムを使用することで，無線 LAN のセキュリティに対する意識の向上と理解度の向上を促進することができているか確認する．

アンケートやテストの内容は，総務省が発行している Wi-Fi 利用者向け簡易マニュアル[4]や IPA が実施している基本情報技術者試験の過去問を基に作成する．

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，失敗体験から学習する無線 LAN のセキュリティリスク学習システムを開発した．GBS 理論に基づいて学習する本システムを使用することで，無線 LAN のセキュリティに対する意識の向上と理解度の向上を促進することが期待できる．

今後の予定として，MITM 攻撃以外に WEP や WPA/WPA2 といった無線 LAN の暗号化規格に関するセキュリティリスクを学習できるようにする予定である．また，GBS 理論に基づいた学習シナリオの追加や動作検証実験，利用評価実験を実施する予定である．

参考文献

[1] I. M. M. Dissanayake, "DNS Cache Poisoning: A Review on its Technique and Countermeasures," 2018 National Information Technology Conference (NITC), 2018, pp. 1-6, doi: 10.1109/NITC.2018.8550085.

[2] B. Prabadevi, N. Jeyanthi, "A framework to mitigate ARP sniffing attacks by cache poisoning", Int. J. Adv. Intell. Paradigms, 10, pp.146-159.

[3] 瀬戸崎喬, 松尾和人, HSTS による対策を回避可能な sslstrip 攻撃, 情報処理学会コンピュータセキュリティシンポジウム 2016 論文集, 第 2016 巻, pp.733-740, 2016-10-04.

[4] 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 2022-07-07)

[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.

[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者エージェントの実装と評価, 情報処理学会インターネットと運用技術シンポジウム 2015 論文集 2015 (2015), pp.73-78.

[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.

[8] A. Amiruddin, D. A. P. Yusa and R. A. Rofiq, "Conformity Analysis of HTTP Strict Transport Security (HSTS) Configuration and Implementation Using Bettercap Tools," 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS, 2021, pp. 13-18, doi: 10.1109/ICIMCIS53775.2021.9699358.

[9] S. Duddu, A. Rishita sai, C. L. S. Sowjanya, G. R. Rao and K. Siddabattula, "Secure Socket Layer Stripping Attack Using Address Resolution Protocol Spoofing," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 973-978, doi: 10.1109/ICICCS48265.2020.9120993.

[10] H. A. S. Adjei, M. T. Shunhua, G. K. Agordzo, Y. Li, G. Peprah and E. S. A. Gyarteng, "SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection), " 2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021, pp. 187-193, doi: 10.23919/ICACT51234.2021.9370460.

[11] A. Alina and S. Saraswat, "Understanding Implementing and Combating Sniffing and ARP Spoofing," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), 2021, pp. 235-239, doi: 10.1109/RDCAPE52977.2021.9633635.

[12] MITM using SSLStrip & Mitigation Methods,入手先< https://krishnamanas.files.wordpress.com/2015/03/mitm-using-sslstrip-and-mitigation-methods2.pdf> (参照 2022-07-07).