無線 LAN の安全性について

1 研究の動機・目的

予てより情報系の分野に興味を持っており、2 年次で行ったフロンティアタイムでの研究の一部として取り上げた、無線 LAN についてより深く研究したいと考えた。この研究を通して、公衆化が進む無線 LAN を安全に利用するにはどうしたらよいかを示していきたい。

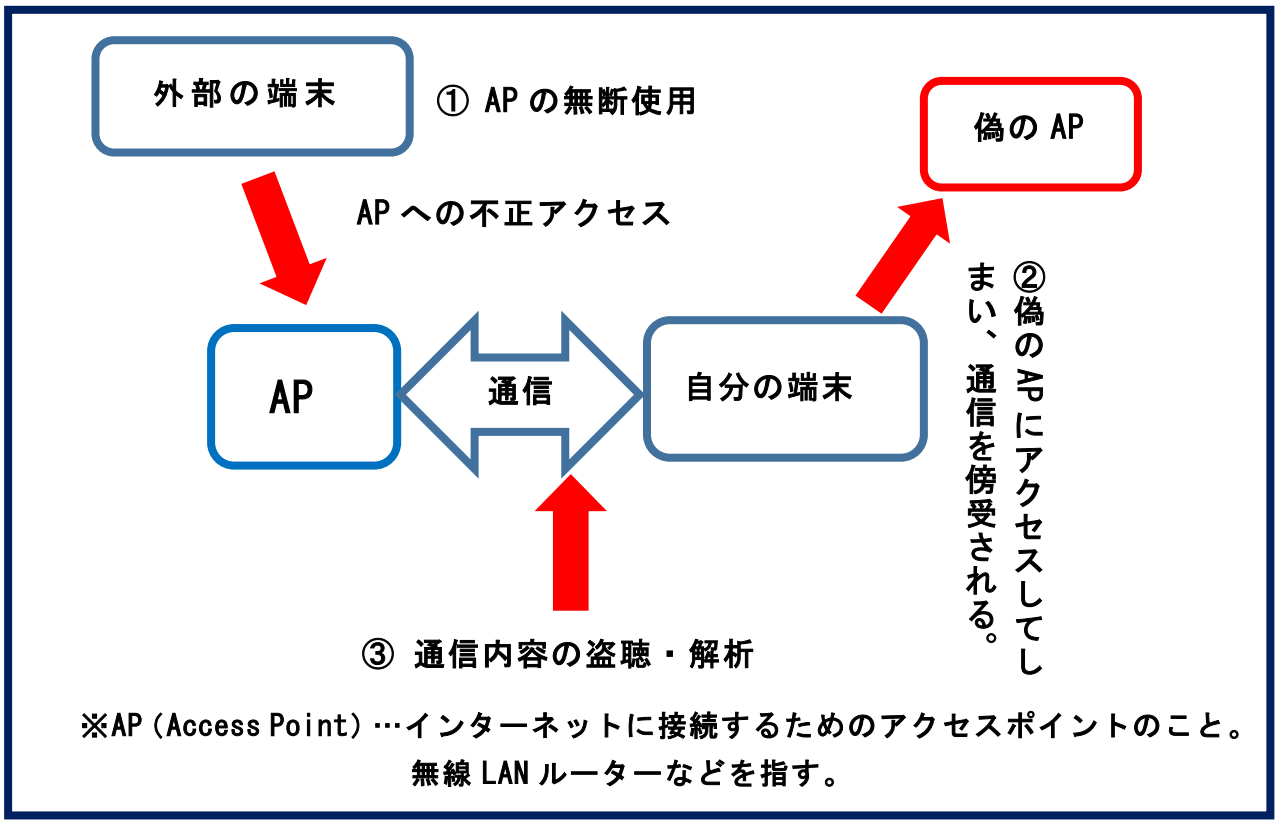
2 研究の方法・過程

まず無線 LAN の概要や通信の基本的な仕組み、身近に潜んでいる様々な危険性やその対策について書籍、インターネットで調べる。

その浮上した「通信内容の傍受・解析」の危険性に焦点を当て、自宅のインターネット環境を用いて検証実験を行いその結果について考察する。

3 研究の成果

●無線 LAN の危険性について



①AP の無断使用

家庭でも使用している人も多いであろう無線 LAN ルーターだが、しっかりと暗号化（パスワードを入力しないと使えなくする）しないと、様々な危険が伴う。

例えば AP の無断使用だ。家でスマホやパソコンで無線 LAN を使うとき、隣の家のルータ

ーの電波まで受信しているのを目にした経験はないだろうか。普通はそこから自宅のものを選び、ルーターの裏などに記載されているパスワードを入力（最近ではスイッチを押すだけで使えるものもある）してネットに接続する。パスワード（もしくはルーターのスイッチを押す動作）がなければネットに接続できないのだが、ルーターが暗号化されていないとそれらが必要なくなり、誰でも使い放題になってしまう。ただルーターが使用されるだけなら危険がないように思えるが、犯罪予告などの書き込みや不正アップロード（ダウンロード）をされると、気づかないうちに犯罪に加担することになってしまうのだ。

このような危険を回避するために、ルーターの暗号化は必要不可欠である。しかし、暗号化方式によっては全く意味を為さない場合がある。それが WEP（Wired Equivalent Privacy）という一昔前までは主流だった暗号化方式だ。その名の通り、有線ネットワークと同等のレベルの安全性を提供しようとするものであり、そこには解析が容易であるなどの様々な問題が存在する。昨年のグループ研究で、WEP で暗号化されたパスワードの解析実験を行い成功し、パソコンやインターネットに詳しい専門家でなくても、容易に突破できてしまうほど WEP は軟弱な暗号化方式であることが確認できた。実際に NTT DoCoMo が提供している公衆線 LAN サービスでは WEP を順次廃止し、よりセキュリティの強度が高いものへと移行している。自宅でも WEP のままだと危険なので、WPA2 などのセキュリティの強度が高い暗号化方式に変更する必要がある。

②偽の AP へのアクセス

外出先などで暗号化されていない AP を見つけたとしても､それは悪意がある者が構築したいわば“餌”である可能性があるので、安易にアクセスしてはいけない。故意に暗号化をせずに構築された AP に利用者がおびき寄せられ、通信の内容を盗聴されて ID やパスワードを入手されたり、ブラウザ（インターネットでサイトを閲覧するためのソフト）の脆弱性を突いた攻撃を仕掛けられたりする可能性がある。AP の名前が大手企業のものであったりすると、うっかり信頼してしまいそうになるが、使用する際には十分注意しなければならない。また、スマートフォンなどで Wi-Fi のモードを常にオンにしていると、自動的に接続できるアクセスポイントを探し､気がつかないうちに危険な AP を利用してしまう可能性があるので、そちらも注意が必要だ。

③通信内容の盗聴・解析

②で述べた偽の AP を使用した場合以外でも通信の内容を盗聴される危険がある｡そこで、実際に通信の内容を盗聴しその危険性を確かめる実験を行った。

■中間者攻撃を用いたパケット盗聴実験

･概要

③で述べた「通信内容の盗聴・解析」の危険性について、実際に自宅のインターネット環境と iPhone を用いて検証実験を行った。今回の実験では iPhone とルーターを行き交うパケットを盗聴する手段として、インターネットでの調査で挙がった中間者攻撃の一種である ARP スプーフィングを用いた。

・ARP スプーフィングとは

対象の端末の通信を傍受するための技術であり、IP アドレスに対応した MAC アドレス（ネットワーク上の機器を特定するアドレス）を特定するために使われている ARP というプロトコル（通信の手順や約束事）を悪用した攻撃方法。端末同士の ARP による通信を傍受し、悪意のある攻撃者の端末になりすました MAC アドレスを返信することで実行される。

攻撃時

```
Sender MAC address: LiteonTe_fd:d3:a8 (20:16:d8:fd:d3:a8)
Sender IP address: 192.168.11.1 (192.168.11.1)
Target MAC address: Apple_d6:8f:0e (b8:e8:56:d6:8f:0e)
Target IP address: 192.168.11.3 (192.168.11.3)
```

通常時

```
Sender MAC address: Buffalo_39:a1:80 (10:6f:3f:39:a1:80)
Sender IP address: 192.168.11.1 (192.168.11.1)
Target MAC address: Apple_d6:8f:0e (b8:e8:56:d6:8f:0e)
Target IP address: 192.168.11.3 (192.168.11.3)
```

上の画像が攻撃を仕掛けている時の、下の画像が通常時の ARP についての通信のやりとりのデータである。傍線で示したように MAC アドレスの送り主が異なっていることが分かる。通常時は某社のルーターから送信されているが攻撃時はそうではない。このように端末とルーターとの通信の間に割り込み、パケットを盗聴していくのだ。

・実験環境

iPhone5s, ノート PC, 無線 LAN ルーターを使用。

ARP スプーフィングには Nighthawk、パケットの閲覧には Wireshark という専用のソフトウェアを使用した。

実験対象の iPhone にだけ攻撃を仕掛けるように十分に注意して行った。

・実験手順

1　iPhone とルーターを接続させる。

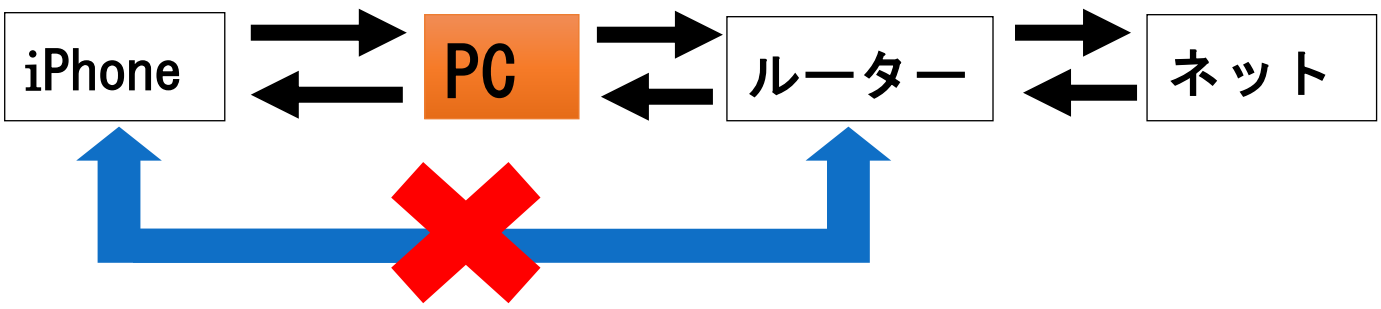
2　PC 上で Nighthawk を使用し、iPhone に ARP スプーフィングを仕掛ける。

3　PC 上で Wireshark を使用し、iPhone とルーターの間を行き交うパケットを閲覧する。

※暗号化方式での違いを確認するため、暗号化方式を WEP と WPA2 の 2 種類で行った。

また、PC とルーターが接続されていない状態でも同様に実験を行った。

・中間者攻撃のイメージ

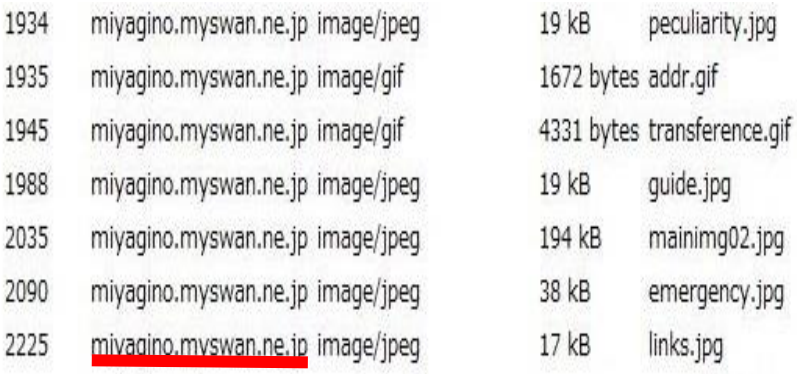


iPhone とルーターの通信の間に PC を経由させて、
iPhone が行った通信内容を専用のソフトウェア使用することで盗聴する。

・実験結果　iPhone 画面の一部　　Wireshark の画面の一部

図 1

図 2



PC で iPhone に ARP スプーフィングを仕掛けた状態で、iPhone で宮城野高校の HP にアクセスした(図 1)ところ、盗聴している PC の画面上でその通信の内容が確認できた(図 2)。画像にあるのはほんの一部だが、アクセスしたサイトの URL やそれに含まれる画像、通信した端末が iPhone でありそのバージョンが 8.2 であること（実際に 8.2)、どのサーバーを使っているか、Cookie など様々な情報が得られた。また、ARP スプーフィングを中断するとパケットの盗聴も中断されたため、ARP スプーフィングがパケットの盗聴に有効に作用したことが確認できた。なお、暗号化方式を WEP,WPA2 の 2 つに分けて実験を行ったが、どちらもパケットを傍受することができた。ノート PC とルーターの接続を絶つと、パケットの盗聴は止まり、iPhone もルーターに接続できなくなってしまった。

・実験結果を受けての考察

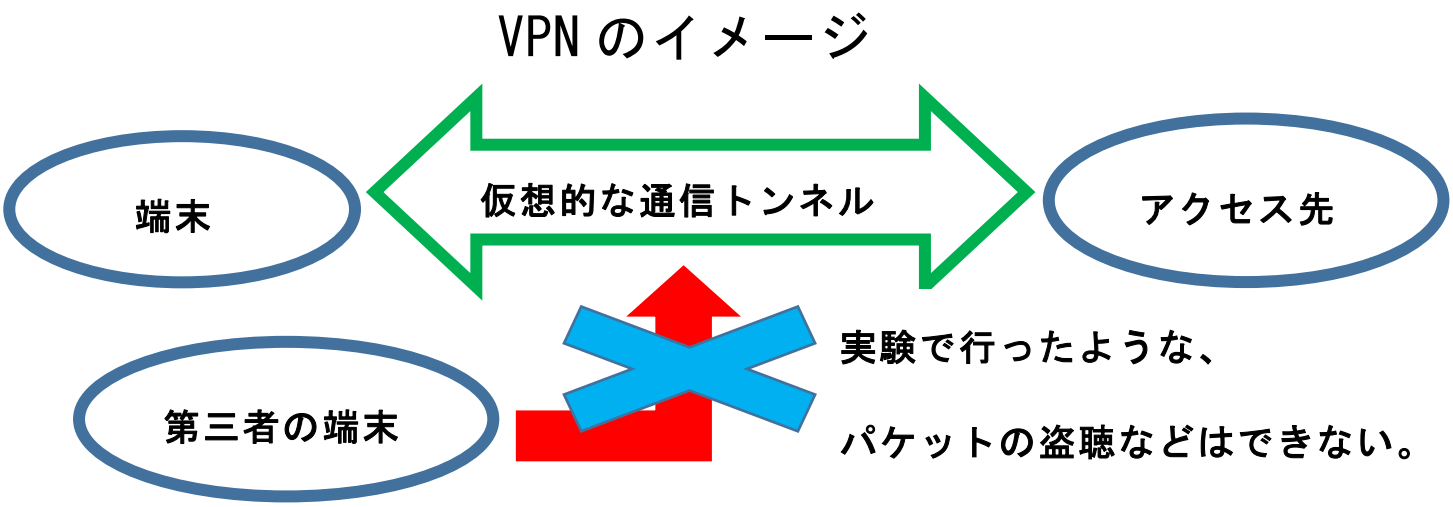
２つの暗号化方式の両方でパケットを盗聴できたことは、パケットを傍受しているノート PC が、iPhone の接続先であるルーターと同じく接続されているため、暗号化方式に関わらず通信が盗聴されてしまったのだと考えられる。また、PC とルーターの接続を絶った際にパケットの盗聴が停止したことは、PC とルーターの接続が確立できなくなったからであり、それが iPhone とルーターとの接続にも影響したと考えられる。

これらの結果から、通信を傍受するには、対象の端末が接続している AP に接続していることが必要であることが分かった。よって、誰でも AP に接続できてしまうような公衆無線 LAN だと、容易に通信が傍受されてしまう。これを悪用されると、ID やパスワードなどの大切な情報が漏洩してしまったり、電子メールの中身を見られたりするなどの危険がある。実際に成田、関西、神戸の 3 空港が提供している無料の公衆無線 LAN サービスでインターネットを利用した際、閲覧したサイトの URL や電子メールの中身が他人に盗聴され得る状態であったことが、神戸大大学院の森井昌克教授の調査で確認されたというニュース

があった（2014/8/26 日本経済新聞より）。しかし、正規の利用者しか接続できずかつセキュリティの強固な暗号化方式（WPA2 など）を用いているような AP であれば、外部から不正に接続される可能性は低く、通信を傍受される心配はほとんどないことも実験結果から分かった。

●その他の対策—VPN（Virtual Private Network）

高セキュリティな AP を使用する他にも有効な対策がある。それは、仮想的にプライベートなネットワークを作る VPN というものだ。トンネリングと暗号化によって第三者がアクセスできず、安全な通信をすることができる。



VPN のイメージは上のようになる。名前の通りプライベートな通信になるので、第三者は通信にアクセスできずパケットの盗聴などもできないので、安全な通信をすることができる。暗号化されていない AP でも VPN を使えば、通信を暗号化してくれるので安全に利用できる。最近では個人向け VPN サービスもあり、今後も公衆無線 LAN の普及とともにその数も増え、安全性も高まっていくと考えられる。AP 提供者の暗号化などのセキュリティへの配慮も大切だが、我々利用者もこのようなサービスを利用して、自らの通信の安全は自らが守るという姿勢を持つことが重要だ。

●実験・調査を通しての考察・感想

本研究では、パケットの盗聴実験などを通して無線 LAN の安全性について検証し、安全に利用するための方法を調査した。パケットの詳細な解析はできなかったが、実際に起こり得るパケットの傍受の危険性を示せたと思う。研究を通して感じたことは、無線 LAN 利用者のセキュリティに対する意識の向上が、今後の情報社会を安全に生き抜く為には必要だということだ。総務省は 2020 年の東京五輪に向けて、国内外の観光客のための公衆無線 LAN 環境の充実が求められるとしている。実際に公衆無線 LAN 環境の整備を行う地方公共団体に対し、その事業費の一部を補助する「観光・防災 Wi-Fi ステーション整備事業」という取り組みも始まっている。よって今後公衆無線 LAN を利用できる機会が増え、安全な利用方法について考えなくてはならなくなる。そこで、インターネット利用者一人ひとりが情報セキュリティへの意識を向上させ、先で挙げたような危険性を理解し、安全な利用

方法を実践することが可能になれば、より安全で安心な情報社会になっていくと私は考える。

4 今後の研究課題

大学では高校で行ってきた研究活動での経験を基に、ネットワークシステムのセキュリティ確保には不可欠である、外部からの盗聴からデータを守る安全な暗号理論の研究をしたい。そして将来、大学で学び、研究したことを活かして企業などのセキュリティ管理の中枢を担う技術者として活躍し、社会に貢献していきたい。

5 参考文献

・『無線 LAN セキュリティの教科書 2013』(白夜ムック)
・岡嶋裕史 『ハッカーの手口 ソーシャルからサイバー攻撃まで』(PHP 新書)
・JON ERICKSON 著 村上雅章 訳
『HACKING:美しき策謀 脆弱性攻撃の理論と実際 第 2 版』(オライリー・ジャパン)
・サイバーセキュリティ・ピックアップ (1):無線 LAN にまつわるセキュリティの課題を再確認しよう- @IT http://www.atmarkit.co.jp/ait/articles/1504/22/news002.html
・無線ＬＡＮのメール丸見え 成田・関西・神戸の３空港:日本経済新聞
http://www.nikkei.com/article/DGXLASDG2600E_W4A820C1CR0000/
・ネットワーク入門サイト - Wireshark の使い方
http://beginners-network.com/wireshark.html
・「危ない Wi-Fi」からデータを守る、充実し始めた個人向け VPN サービス
http://pc.nikkeibp.co.jp/article/trend/20140512/1130123/
・総務省｜地域情報化の推進｜地方自治体における公衆無線ＬＡＮ整備について
http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/local_support/ict/musenlan.html
・ARP スプーフィングとは ｜ 日立ソリューションズの情報セキュリティブログ
http://securityblog.jp/words/618.html

資料番号 1

プロジェクト・スタディ
における個人研究

「無線 LAN の
安全性について」

宮城県宮城野高等学校
松山優気