LAB LETTER

株式会社 **デザインラボ**
代表取締役　藤原　康孝

第199回　Welcome Board の制作

オフィスの入り口に来客向けのウエルカムボードを置くことがありますが、来客者に合わせてコンテンツを入れ替えることがあります。そのような用途には下記の方法があります。

1. ノートパソコンをモニタに繋ぎ、PowerPoint などでコンテンツを用意して表示。
2. USB メモリにコンテンツを保存し、USB メモリから直接画像を表示させる機能を持つモニタ、TV を繋いで表示。

以上の方法では、ノートパソコンを専用に用意する、あるいは少々高価なモニタ、TV を用意する必要があります。昨今では、右図のようなシングルボードコンピュータが安価で販売されていますので今回これを利用して作成してみました。

右図の製品は「Raspberry Pi（ラズベリーパイ）」と呼ばれているボードですが、他にも「Arduino」、「ASUS Tinker Board」など多くのボードが市販されています。

これらのボードの多くは機器への組込開発用、あるいは学習用として開発されており、様々な機能を追加することができますが、IoT（Internet of Things）やロボット向け利用としてのニーズがこの数年高まっています。有名どころでは日本の秋月電子通商の WEB サイト（http://akizukidenshi.com/）では、利用できる様々なセンサーや基盤が販売されており、電子工作が好きな方には楽しいサイトです。

OS は、主に Linux や IoT 用の Windows IoT が利用できますが、いずれも無償で利用できます。今回は Linux（Raspberry Pi 用には、Raspbian という名称になります）を利用しました。

1. OS のダウンロードとインストール
   https://www.raspberrypi.org/downloads/raspbian/ からダウンロードし、microSD カードに保存し起動するとインストール画面が出ますので、画面に従ってインストールします。

2. 「**f**rame**b**uffer **i**mageviewer/fbi」のインストール
   画像ファイルを予め設定した秒間隔で切り替える為のアプリケーションをインストールします。これは Raspbian をインストールしてネットワーク接続を行い、インターネットに繋いだ後に、Raspbian 上でダウンロード検索ができ、無償でダウンロードできます。

3. ここから先は若干ハードルが上がりますが、共有フォルダの設定(Samba)、fbi の自動起動の設定を Raspbian 上で行います。設定が終わり、パソコンからネットワークを介して Raspberry Pi 上の共有フォルダへアクセスし、表示したい画像ファイルをコピーします。(前ページの下図)

4. 後は Raspberry Pi をケースに入れモニタに繋ぎ、起動すると下図のように予め設定した秒間隔で画像が切り替わります。

画像を変更したい場合には、上記 3 に戻りネットワーク経由で共有フォルダにある画像ファイルを差し替え、Raspberry Pi を再起動するだけです。LAN ケーブルあるいは無線 LAN いずれにも対応していますので、設置場所にまで向かう必要はありません。

この機能を使えば、ウエルカムボード以外にも下記の用途に利用できます。

1) 工場の各所に余ったモニタを設置して来客用に生産設備の案内を行う。

2) 工場の各生産機器の側に運用マニュアルを画面表示させる。サーバーやデータベースと連携させ、ライン毎に異なる画像を異なるタイミングで自動切り替え表示させる。

3) 「デジタルサイネージ」として飲食店の店頭でメニュー案内や広告を表示。

今回、Raspberry Pi を利用しましたが、シングルボードコンピュータは IoT のデバイスとしても既に広く利用されています。工場内では設備の稼働状況、温度、湿度などの計測データの集計などに利用されたり、趣味の分野では手作りのドライブレコーダー、音声認識デバイスと組み合わせて、遠隔操作による屋内の電気電源オンオフツール、あるいは監視カメラを開発するなどの用途で利用できます。

(御参考まで)

LAB LETTER

株式会社 デザインラボ
代表取締役 藤原 康孝

第 200 回 無線 LAN の脆弱性

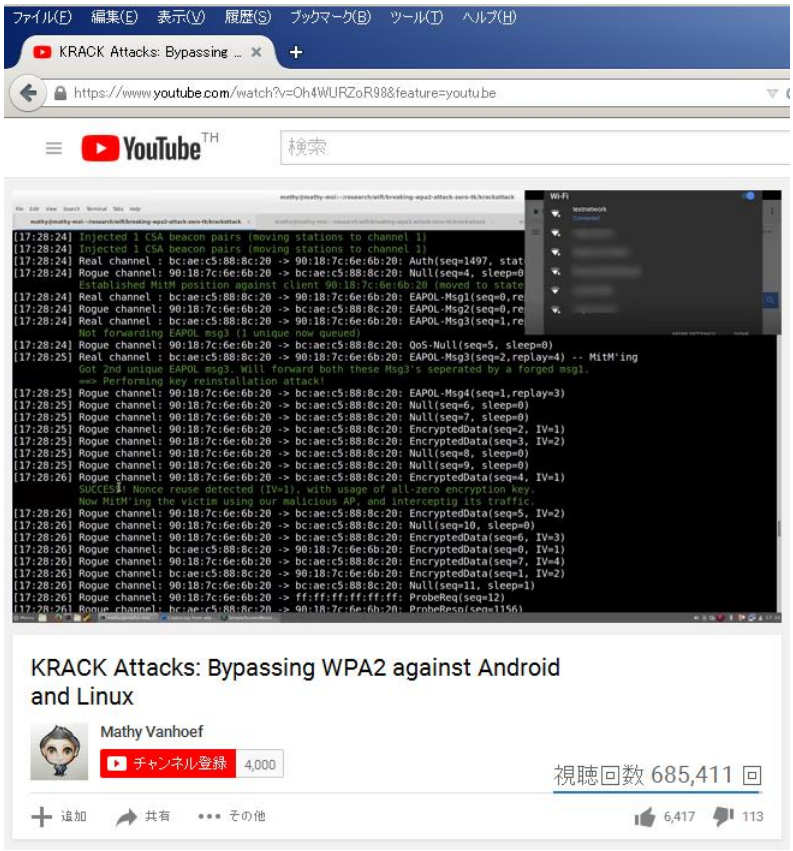
10 月 17 日に TV 並びに新聞でも報道されましたが、現在主流となっている無線 LAN の暗号化の規格に脆弱性が見つかったとニュースになっています。

無線 LAN の暗号化の規格には、古くから利用されている WEP を始め、WPA、WPA2 などの規格がありますが、現在主流となっている WPA2 に脆弱性が見つかったとのことです。WEP については暗号解読ソフトウエアが出回るなどして悪意あるユーザーにより無線 LAN 接続パスワードが解読されてしまうと 2000 年代前半に問題になりました。

その後、WPA、WPA2 が主流となり、企業向けには WPA2-Personal と WPA2-Enterprise の 2 つのモードのいずれかが利用されて来ました。今回日本の総務省は 10 月 18 日付けで「無線 LAN（Wi-Fi）暗号化における脆弱性について（注意喚起）」として下記の WEB サイトで周知しています。

http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000274.html

今回の脆弱性は、2017 年 5 月 19 日にベルギーの大学研究者が発見し、「KRACKs」と名前をつけています。その後 7 月から 8 月にかけて、ネットワーク機器製造メーカーへ周知され、10 月 16 日に無線 LAN 製品の業界団体である「Wi-Fi Alliance」がソフトウエアのアップデートで対応可能であると発表したことから今回ニュースになりました。



暗号の解読のデモが右図のように Youtube に上げられています。暗号化を解読された場合、無線 LAN アクセスポイントとクライアント側（パソコン、スマートフォンなど）の両方に攻撃を受ける可能性があります。

KRACK Attacks: Bypassing WPA2 against Android and Linux

https://www.youtube.com/watch?v=Oh4WURZoR98&feature=youtu.be

しかし攻撃者は無線 LAN の届く範囲内にいる必要があり、インターネット経由での攻撃はできないとのことですので、無線 LAN アクセスポイント

製造メーカーのソフトウエア(ファームウエア)のアップデートがリリースされた後に、アップデートを行えば大きな問題にはならないと思われます。

ただこの機会に、以前 WEP、WPA などの古い規格で無線 LAN 接続されている場合には、新たに設定し直すことがお勧めです。発見者によると今回発見の WPA2 の脆弱性を回避する為に、WEP を一時的にでも利用することの方がより危険とのことです。

2017 年 10 月 20 日現在の各社の対応状況は下記の通りです。

1. Microsoft
   10 月 16 日(18 日更新)のセキュリティーアップデートで対応可能。

2. Google Android OS
   現時点で未対応。数週間以内に対応予定。

3. Apple iPhone、Buffalo、D-Link、Zyxel
   現時点で未対応。今後対応。

4. Cisco
   該当製品の調査中、確認済みの機種は順次アップデート公開中。

5. Fortinet
   アップデートにて対応可能

6. TP-Link
   確認済みの機種は順次アップデート公開中。残りは数週間以内に対応予定。

無線 LAN に関わる機器は該当しますので、生産機器などで無線 LAN を利用している場合も個別にメーカーへ確認がお勧めです。

また、インターネット経由で社内の無線 LAN への侵入に関しては該当しませんが、当地でも TOT、TRUE、3BB 社など電話会社が提供している公衆の無線 LAN が多々ありますので、社外での無線 LAN 接続はしばらくの間は避けた方が確実です。

(御参考まで)

LAB LETTER

株式会社 デザインラボ
代表取締役 藤原 康孝

第 201 回 メールが送信できない。受信できない。

今年後半はメールの送受信についてトラブルが頻発しています。原因には様々なケースがありますが、最近の特徴としてブラックリストに送信側、受信側のメールサーバーやインターネット接続時の IP アドレスが登録されていることが多くなっています。今回は送信と受信に分けて原因と対策を御案内します。

1. 送信不可

メール送信後に、即時あるいは 1～2 日経過してから下記のようなメールが届いて宛先に届いていないことがわかります。

```
<xxx@gmail.com>: host gmail-smtp-in.l.google.com[74.125.200.26]
said: 554 5.7.1 This message has been blocked because ASE reports it
as spam.  (in reply to end of DATA command)
```

上記のメッセージでは、ASE(Anti Spam Engine)というスパムフィルターがメールをブロックしたことがわかります。ブロックされた理由は、メール件名。本文にスパムメールでよく使われる文言や添付ファイルがウイルスに感染しているケースなどがありますが、まずは、下記の IP アドレスがブラックリストに登録されているかどうかを確認したいところです。

1) 送信者のインターネット接続時の IP アドレス
2) 送信者の送信メールサーバーの IP アドレス

「送信者のインターネット接続時の IP アドレス」については、「https://www.iplocation.net/」を開いていただくと右図のようなサイトが開きますがここの「Your public IP Address is」に表示されている IP アドレスが該当します。

「送信者の送信メールサーバーの IP アドレス」についてはご利用のメールホスティング会社に問い合わせていただければわかります、あるいはメールサーバーの URL、例えば、mail.company.com のようなサーバー名を直接右図サイトへ入力していただいても検索可能です。

上記、IP アドレスあるいは URL を控えておき、次ページの 2 つのサイトに入力してみます。

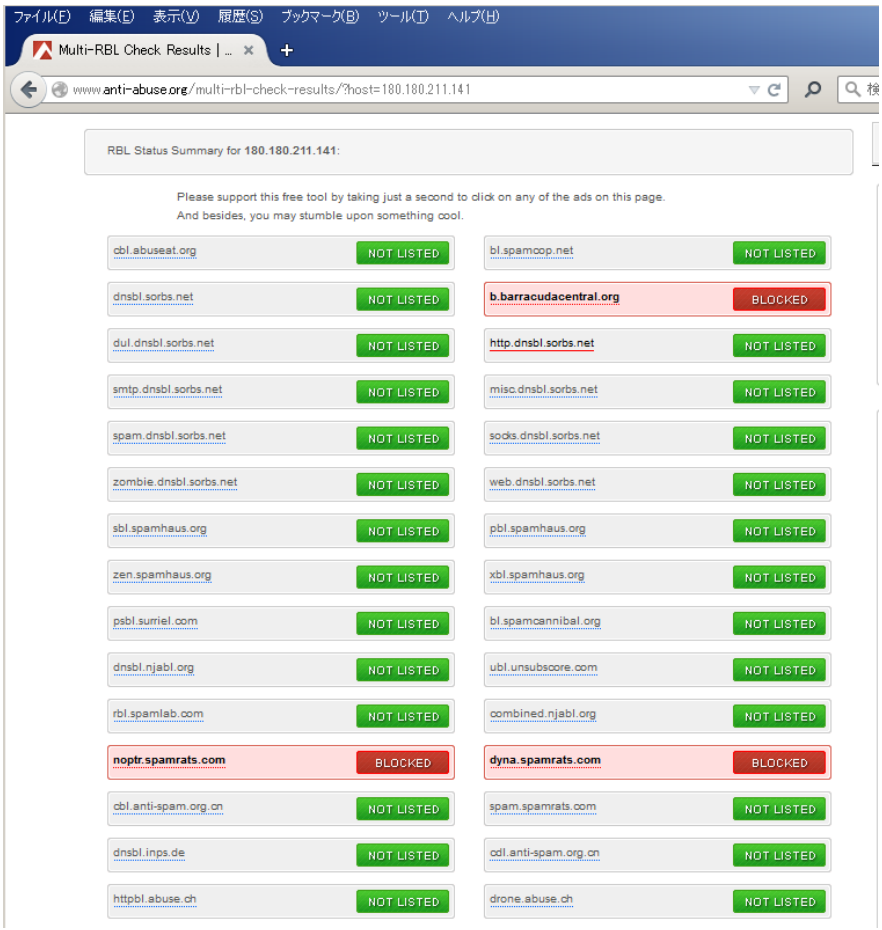
http://www.fortinet.co.jp/support/fortiguard_services/antispam.html
http://www.anti-abuse.org/multi-rbl-check/

もしブラックリストに載っている場合は、上記 Fortinet のサイトの場合は、「"xxx.xxx.xxx.xxx" is blacklisted in the IP reputation database.」と表示され、その下にブラックリストから解除を依頼する場合の入力項目が表示されます。

前ページの anti-abuse.org のサイトの場合には、右図のように 46 社のブラックリストからまとめて検索した結果が表示され、ブラックリストに載っていない場合には、「NOT LISTED」、載っている場合には、「BLOCKED」と表示されます。

「BLOCKED」と表示されている場合には、個別の各社の WEB サイト上から解除申請を行う必要があります。

すべてのメールが右図のすべてのブラックリストで検閲を受けるわけではありませんが、複数のブラックリストに登録されている場合、メール送受信ができなくなる可能性が高く、自社で利用している IP アドレスが一旦ブラックリストに載ると非常に面倒なことになります。



代表的なブラックリストは右図の 46 社になりますが、例えば、ファイヤーウォールメーカー独自のブラックリストやインターネットプロバイダー各社毎の独自のブラックリストもありますので、メールが送信できなかった場合、自動返信されてきたメッセージから判断する必要があります。

（次回に続く）

LAB LETTER

株式会社 デザインラボ
代表取締役 藤原 康孝

第 202 回 メールが送信できない。受信できない。(2)

今年後半はメールの送受信についてトラブルが頻発しています。原因には様々なケースがありますが、最近の特徴としてブラックリストに送信側、受信側のメールサーバーやインターネット接続時の IP アドレスが登録されていることが多くなっています。今回は前回の続編として受信できない原因と対策を御案内します。

2. 受信不可

受信できない原因は大きく分けて 2 つあります。

1）使っているパソコンに原因がある場合には下記のようなケースがあります。

1. 受信トレイが満杯

Outlook、Windows Live Mail などメール送受信ソフトウエアにはそれぞれ受信容量に限界が設定されています。一昔前の Outlook Express では受信フォルダが 2GB を超えると受信できなくなり頻繁に再設定する必要がありました。現行のソフトウエアでは数十 GB まで受信できますが、最後には満杯になりますので、その場合には他のフォルダに振り分け、受信フォルダの再構築が必要です。

2. 自動振り分け設定で想定外のフォルダに受信されている。

お客様からメールを受信した際に、自動的にフォルダに振り分けをするように設定していることがあります。数多くの設定を行った場合、設定したことを忘れ受信しているにも関わらず受信できていないように思えることがあります。意外と盲点です。

3. 受信方法には POP3 と IMAP の 2 方式あり、IMAP の場合、メールサーバーとの同期が正常に行われず受信するまでに時間が掛かる。

Outlook のクラウド版、Outlook 365 にて時折発生する事象です。アップデートを行うか、可能であれば、Outlook のプリインストール版ではなく、企業向けのボリュームライセンス版を利用すると問題解決します。

4. Windows Update やアンチウイルスソフトウエアの直近のアップデートが正常に終了していない。

Windows 10 では標準設定では自動アップデートされますが、アップデート中に回線が切れる、あるいはパソコンの電源が切れた場合、正常にアップデートが完了しないことがあります。念のため再度アップデートし直す必要があります。

2） ネットワーク上に原因がある場合

1. 受信側・送信側のインターネット接続の IP アドレスあるいはメールサーバーの IP アドレスがブラックリストに載っており、受信側・送信側のいずれかで止まってしまう。

   前月号に記載のブラックリストに自社の IP アドレスがブラックリストに載っている場合、送信側で止まってしまうことがあります。解除するには送信側のファイヤーウォールなどに設定をしていただくか、ブラックリストから登録を削除してもらうようにリスト先に個別に手続きをする必要があります。

   手続きしても直ぐに解除されないことがありますので、ブラックリストに載らないよう予め対策しておくことが非常に大事です。

   また当地の場合、自社に問題なくとも、自社で利用しているインターネット回線の IP アドレスが知らない内にブラックリストに登録されていることがあります。企業でインターネット回線を利用する際には、必ず「固定 IP アドレス」が割り当てられるサービスに申し込んでおくことが必須です。

2. 受信側のファイヤーウォールの受信拒否条件に適合して受信できない。

   上記1、2のように IP アドレスだけでなく、特定のスパム、ウイルス関連キーワードなどに引っかかり受信できないことがあります。最近特に「qq.com」という中国のフリーメールからの送信を会社業務に利用されているケースがあり、届かないことがありますが、「qq.com」は膨大なスパムメールの送信元でもありますので、解除するかは要検討です。

3. メールサーバーの受信者アカウントが満杯。

   特に、受信方法で IMAP 方式を利用している場合（一般的にはメールクラウドサービスを利用している場合）、メールサーバーの受信トレイの容量制限を超えると受信できなくなります。1～2 年で満杯になってしまうことがありますので、予め満杯になった場合の対策を確認しておく必要があります。

本年もお陰様で弊社社員一同無事に過ごすことができました。ありがとうございました。新年も引き続きご指導ご鞭撻お願い申し上げますと共に月報ご購読者皆様の益々のご発展をお祈り申し上げます。ありがとうございました。