IT21 の会（平成 20 年 11 月）第 125 回議事録

日　時：2008 年 11 月 7 日（金）18 時 40 分～20 時 35 分
場　所：日本技術士会　葦手第二ビル　５階Ａ会議室
出席者：14
配布資料

- 0811-0 （社）日本技術士会 CPD 行事　参加票
- 0811-1 あなたのその無線 LAN，安全ですか　（椎名高之氏）
- 0811-2 .NET の功罪／USB による計測機器の落とし穴　（加納幸博氏）
- 0811-3 情報工学部会 CPD 行事「ソフトウェアテスト :理論から実践まで」　（黒澤兵夫氏）

議　事

１．議事および資料確認　椎名高之氏

２．あなたのその無線 LAN，安全ですか　椎名高之氏

「2008 年度第 1 回情報セキュリティに関する驚異に対する意識調査」(IPA) によると，およそ 44%のユーザは無線 LAN のセキュリティ対策を実施していないか自覚していないとのことである。その危険性と対策を調査した。

無線 LAN 規格は，IEEE802.11 に規定されている。通信方式は IEEE802.11b/g/a/n/j がある。b/g/a が普及しており，次世代として n が期待されている。802.11n では従来 54Mbps であった通信速度が最大 600Mbps まで高速化されるほか，通信範囲も 2 倍程度に広がる。現在はドラフト版に対応した製品が発売されている。購入する場合は，認定ロゴ付きの製品を勧める。2009 年 9 月に標準化の見通しである。b/g/a との互換であり，2.4/5GHz 帯に対応するが，5GHz 帯では 802.11a と同様に屋外での利用ができない。セキュリティは 802.11i に規定されており，これを基に Wi-Fi アライアンスは WPA2 を策定した。WPA2 に対応すれば 802.11i に準拠していることになる。

かつて無線 LAN セキュリティと言えば，SSID／MAC アドレスフィルタリング／WEP の御三家であった。それぞれ，以下の問題がある。

- SSID は本来アクセスポイントの識別をするものであってセキュリティを目的としたものではない。フリーソフトでも参照することができる。また，SSID を指定せず最も電界の強いアクセスポイントに接続する ANY という設定が可能である。ANY 接続を拒否する機能もあり，ステルス機能とも呼ばれるが，クライアント側からの SSID は隠せず，十分ではない。
- MAC アドレスフィルタリングについても，MAC アドレスの変更が容易な上，通信暗号化においても宛先である MAC アドレス自体は隠せないことから有効性は高くないと言える。
- WEP は暗号プロトコルであり，これを傍受する行為自体は電波法の罰則対象である。しかし，IV(Initialization Vector)が 24bit だけであり，Weak IV と呼ばれるパケットを収集することでキーの推測ができてしまう。また、通常環境のパケット取得により 10 秒でも破ることが可能な方法が新たに発表されたことから，総務省としても注意喚起している。

現在は,802.11i に準拠した WPA2(Wi-Fi Protected Access2)がセキュリティの標準である。Personal mode と Enterprise mode があり，前者は家庭向けで事前共有キー(PSK)を設定し，後者は企業向け認証サーバを必要とする。暗号方式に AES をサポートすることで，安全性を高めている。PSK を利用するに当たっては，キーは 21 文字以上に設定するとよい。20 文字以下であれば解けるという論文がある。

セキュリティ設定は一般に敷居が高いため，Wi-Fi アライアンスでは WPS という簡単に設定するための仕様を策定した。PC のほかゲーム端末等においても対応するよう，いくつかの仕組みが用意されている。最近ではゲーム機器も多くが無線 LAN に対応している。Nintendo DS は WEP であったが，今月発売された DSi は WPA2 に対応した。

まずは自宅の無線 LAN の設定を見直すことを強く勧める。

３．.NET の功罪／USB による計測機器の落とし穴　　加納幸博氏

まず，マイクロソフト社の.NET Framework 環境での開発した経験を報告する。

2002 年から.NET への移行がはじまった。開発環境としては，Visual Basic 6.0 以前と VisualBasic.NET 2002 以降では大きく変わった。従来からの開発者は戸惑いが大きいが，Java の経験者にとっては似ているため容易だと思われる。従来環境（アンマネージ）の映像データを.NET（マネージ環境）へコピーするにあたり，オブジェクト指向のためフレームメモリー等の単純なメモリーコピーができず，処理速度が低下する問題が見られた。

つづいて，USB による計測機器接続の落とし穴を紹介する。

計測機器は GPIB が使われてきたが，USB2.0 の登場とともに USB 上で GPIB エミュレーションを行う仕様(USBTMC-USB488 クラス)が制定された。これに対応する PC 側のソフトウェアとして VISA が定義されている。しかし，複数の計測機器を VISA で接続すると，競合が発生することがある。また USB は VISA で OPEN する際，ベンダー ID，プロダクト ID，シリアル番号の固有の ID を指定する必要があるため代替機を使用する場合，使い辛い。それを回避するためには VISA COM を使用することにより機器接続リストから曖昧検索が可能である。

４．行事に関するディスカッション　　古瀬勉氏

2 月以降に合宿を予定しているが，委員の立候補者がいない状態に対して，募集ならびに今後の進め方の議論を行った。最近の参加状況から 1 泊 2 日の時間に対して講演者を募ることへの不安の声があった。委員の立候補がでないことはニーズがないのではないかとの見解もあり，期限を設けて再度の委員募集を行い，いない場合は今期開催なしと判断することとなった。

５．情報工学部会からのお知らせ　　黒澤兵夫氏

11 月 15 日に開催する情報工学部会と情報処理学会の CPD コラボレーション行事が紹介された。ソフトウェアテストをテーマとして，ワークショップ形式で実施する。

６．その他連絡事項

- 初参加者なし。
- 加納氏より,ホームページで会員向けに公開している講演 PowerPoint に音声を同期させた配信サービスの現状が紹介された。再生位置のジャンプもできるとのこと。

以 上（記載者：中嶋幸宏　記）