IT21 の会（平成 22 年 3 月）第 141 回議事録

日 時：平成 22 年（2010 年）3 月 12 日(金)　18 時 30 分ー20 時 30 分

場 所：日本技術士会　葺手第二ビル　５階 C・D 会議室

出席者：8 名

配布資料

- 1003-0　（社）日本技術士会　CPD 行事　参加票
- 1003-1　レガシーな通信技術(音声帯域モデム、HDLC プロトコル)の現状と今後(山下茂雄氏)
- 1003-2　ＲＳＡ暗号鍵のポイント（佐野庄一氏）

議　事

１．議事案内および資料確認（山下氏）

２．講演（山下氏）資料 1003-1

テーマ：レガシーな通信技術(音声帯域モデム、HDLC プロトコル)の現状と
今後について、以下の説明と質疑が行われた。
山下氏は、公共システム関連の案件で、昨年、音声帯域 FSK モデム、HDLC プロト
コルを使ったモジュールを新規開発した。背景は、公共システム関連の案件では、
標準仕様書に音声帯域、HDLC 仕様が残っており、その仕様で製造されるテレメータ
装置などは 20 年の供用が要求され、いまでも製造され続けている一方で、
HDLC 通信制御 LSI は、主力機種であったμPD72001 は廃型となり、かつ、
既設品と互換を保たせるためには、他社類似品が利用できなったことである。

解決策として、μPD72001 互換 IP（Intellectual Property）コアを
ライセンス購入し、互換性確認を行った上で FPGA に実装した。
また、DSP、周辺回路、AD/DA、フィルタ、アンプ等で構成される
開発委託元のモデムモジュールを利用した。

今後の問題点としては、今後も 20 年間保守を継続する必要があると考えるが、
現行 FPGA が廃型となっても VHDL で記述しているので、新 FPGA には再コンパイル

すれば実装できる。FGPA はピンコンパチではない懸念はあるが、FPGA が廃型になることはあまりない。

　仮に新規開発をするとなれば、音声帯域 FSK モデム部分については、最近の技術の組み合わせとして、ARM7 の IP コア上にΔΣ1 ビット D/A と,A/D の IP コアを組み合わせることにより、D/A コンバータ無しで実現できる。

質疑応答

Ｑ：被監視場所は無人か？

Ａ：平日日中は有人。24 時間は居ない。（宿直は居る。）

Ｑ：当該システムの通信は自営か？

Ａ：電力会社は自営、（電力以外の）ダムは NTT 専用線。

Ｑ：IP 化の方向にあるのか？

Ａ：電力会社はその方向。国交省は不明である。
ダム仕様書に IP もあるが、国電通仕には本講演テーマの仕様がある。

Ｑ：昨今の高速な汎用プロセッサーでも実現可能ではないか？

Ａ：可能だが、それだけコストをかけるかが問題。

Ｑ：μPD72001 互換 IP コアの仕様の互換性確認にはどのくらいかかったか？

Ａ：約１～２ヶ月

Ｑ：FPGA の継続供給の見通しは？

Ａ：20 年は無理だが 10 年は持つと思う。

Ｑ：FPGA でプロトコル制御の層も実現できるのか？

Ａ：モデム部と合わせて１チップでできる。

Ｑ：外販はしないのか？

Ａ：契約上困難

Ｑ：μPD72001 と日立など現在入手可能な類似品とは
　　ハード的には互換性はあるのか？

Ａ：レジスタが全く違う。状態遷移が微妙に違う。

Ｑ：（最近の技術の組み合わせ案に対して）デジタルを介すと
　　問題が出るのでは。

Ａ：確かに、帯域全体で圧縮があればまだよいが、傾いているとやっかい。
また、一旦トレーニング／ネゴシエーションが終わったあとに傾きが変わると再トレーニングが始まってしまう問題がある。

３．講演（佐野氏）資料 1003-2

テーマ　公開鍵暗号化の一つである RSA (Rivest Shamir Adleman)
方式のポイントについて、新規の技術ではないが判りやすく要約しておくことを
主旨として、説明と質疑が行われた。

一旦秘密鍵が判明してしまうと暗号が解かれてしまう共通鍵暗号方式に対して、
素数の積を基にした２つの鍵（公開鍵、秘密鍵）を用いる RSA 方式があり、
共通鍵暗号方式と組み合わされて広く使われている。
RSA 方式は、原理的には、200～300 桁の２つの素数の積を求めるのは簡単だが、
積を元の素数に因数分解するのは困難であることを利用している。
しかし、昨今、コンピュータの計算速度が上がったことで、現状の鍵の長さでの
安全性の低下が懸念されている。

４．初参加の方の自己紹介　１名

以上(記載者：内藤　雄介)