雑記 3 題

JJ1SXA 池

暗号-2

以前にも暗号についての記事を書きましたが、今回は、暗号の現状と課題、日本の「2013 年問題」ということについてです。

その昔はアナログが全盛でしたが、今やデジタル全盛です、アナログ時代の暗号は、外国の大使館と本国間の連絡に使う無線・有線、後は軍隊の通信手段に必要不可欠だったが、一般の人には、ほとんど無関係なものでした。

今や、日常生活の中に入り込んだ、暗号技術は、ソフトウエアやインターネット上のデータ通信から、携帯電話、IC カード、自動車の認証などに応用分野が広がり、電子機器や情報システムの基盤技術といえるものになっています。

暗号の応用分野が広がるにしたがって、それを利用する技術者には、目的に合った方式による最適設計が求められるようになりました。

かつては処理の高速性が重視されていましたが、携帯機器の広まりと共に、低電力かつ低コストの暗号技術が利用されるようになっています。

このような暗号設計技術の発展とともに、暗号解読技術も日々進歩しています。

これまで広く利用されてきた暗号に欠点が見つかったために、米国では 2010 年までに次世代暗号へのシフトが求められ、日本でも 2013 年までに対策が求められることになりました、いわゆる「暗号の 2013 年問題」です。

さらに最近は、暗号処理 LSI に流れる電流や動作タイミングなどを見ることによって、LSI 内部の秘密情報を非破壊で盗み出す「サイドチャネルアタック」が話題となっており、暗号技術者にとってその対策が重要になっています。

また、ハードウエアでセキュリティを強化する PUF（Physical Unclonable Function）という手法も注目を浴びています。

暗号設計技術と、暗号解読技術は常に追いかけっこ、私のような凡人には、ただただ驚愕の世界でしかありません。

先日、八百長問題で大揺れの角界で、メールの復元がテレビで話題になっていましたが、結構な有名人達が、メールは削除されていなかったのか、削除すれば良かった等の話題を出していました。

以前から、押収したパソコンからデータを復元したという話題は何度も出ていると思いますが、HDD 等の記録メディアを物理的に破壊するか、ソフトを使ってランダムの上書きで復元不能にするかしなければ、見かけ上の削除では、データは復元できるということを知らない人がいかに多いかということを再認識した次第です。

まあ、そのくらいは知っているだけでもましかと、自分を慰めています hi

間もなく春分

年が改まったと思ったら、早や 3 月です、月日の過ぎ行くスピードに驚きです。

24 節季も、小寒、大寒、立春、雨水も終わり、この号が発行される頃には、啓蟄も過ぎて、240 の総会が終われば、もうすぐ春分(3 月 21 日)です。

啓蟄は、「暦便覧」で「陽気地中にうごき、ちぢまる虫、穴をひらき出れば也」とあるように、大地が暖まり冬眠をしていた虫が穴から出てくる頃のことのようです。

春分は、「暦便覧」に「日天の中を行て昼夜等分の時なり」と記されているとおり、春分では昼夜の長さがほぼ同じになると言われています。

然し、実際には、昼の方が夜よりも長いそうで、日本付近では、年により差があるが、平均すれば昼が夜よりも約 14 分も長いようです。

「彼岸」は雑節の一つで、春分・秋分を中日とし、前後各 3 日を合わせた 7 日間のことで、俗に、中日に先祖に感謝し、残る6 日は、悟りの境地に達するのに必要な6 つの徳目、六波羅蜜を 1 日に 1 つずつ修めるためとされています。

＊「暦便覧」は天明七年(1787 年)初版、寛政十年(1798 年)に再版された暦の解説書です(太玄斎著)。

なお現物の「暦便覧」は貴重書で、現在国立国会図書館及び東京大学が収蔵しています、国会図書館の蔵書では「和古書・漢籍」に分類されていいて、マイクロフィルム記録版が閲覧出来るようです。

＊彼岸とは、煩悩を脱した悟りの境地のことで、煩悩や迷いに満ちたこの世を、こちら側の岸「此岸」(しがん)と言うのに対して、向う側の岸「彼岸」というようです。

＊六波羅蜜とは、ブッダを目指す菩薩が修めなくてはならない、6 つの実践徳目のことです。

雑節(二十四節気以外に、季節の変化の目安とする特定の日の総称)の一つである、土用のことですが、夏の土用の丑の日には鰻を食べる習慣があるのは、周知のとおり、土用とは、五行に由来する暦の雑節であり、1 年のうち不連続な 4 つの期間で、四立(立夏・立秋・立冬・立春)の直前約 18 日間のことのようです。

しかし、土用といえば、夏の土用の丑の日しか、頭に浮かびません、しかも鰻が大写しで浮かびます、見るに堪えない体型も考えず、相変わらず食い意地の張っている自分に気付き、我ながら呆れています。hi

体型について、一言弁解すると、ある病気のためホルモン療法を続けていますが、これの副作用も大きく関わっています、週 1 回、ボウリング、プールでの運動、ストレッチ体操、後の 4 日は、約 1 時間強(5 キロ～6 キロ)のウオーキング、これでは、副作用と食欲に比し、まだまだ運動量が足りないようです、ダイエットのため、食欲を押さえ、運動量を増やすのは、死ぬ気にならないと無理のようです。(一寸大袈裟か？)

国際シンボルマーク

この記事は、HP に載っているものを若干書き換えたものです、高齢運転者標章のデザインが一新されましたが、本年 1 月で私もいよいよこの対象になりました。

標章は一応準備しましたが(2 枚で 1.1k 円)、まだ車に貼る勇気(？)がありません、然し、取締りを受けると、高齢運転者標識表示義務違反で、違反点・1点、反則金・4k 円(普通自動車)が課せられます。

健康保険証も、後期高齢者医療保険証に変わります、現実を突きつけられて悲しくなっています。

それはさておき、標章を表示しないで運転すれば、本人の表示義務違反ですが、標章を表示して運転している普通自動車には、危険防止のため、やむを得ない場合を除き、進行している当該車両へ「側方に幅寄せ」や「割込み」をした場合には、道路交通法違反になりますので気をつけてください。

道交法で定める標章は、高齢運転者標章の他、初心運転者標章・聴覚障害者標章・身体障害者標章があることはご存知かと思いますが、表示が任意となっているので、あまり見かけない身体障害者標章と間違えられている標識があります。

国際シンボルマークのことです、これも別のところで書きましたが、このマークは、「障害者が利用できる建築物、施設」であることを明確に示す世界共通のシンボルマークで、このマークが持つ意味は「障害者が利用できる建築物、 施設であること」となっています、具体的には、「建築物 」「建築物の部分」ということで、細かく基準が示されています、後は 「公共輸送機関」にも使用が認められています。

この標章を貼っている自家用車を結構見かけますが、カー用品店等で、簡単に入手できるためにアクセサリーとしてとか、身障者を装ってとか、実際の身障者が間違ってとか等で貼っているいるようです、公共輸送機関では無い自家用車に貼ることは認められていません、これを貼っていれば駐車禁止を大目に見てもらえるなどと思ったら大間違いです、駐車禁止場所で、駐車して良いのは「駐車禁止除外指定車標識」を掲出している車両だけです、「駐車禁止除外指定車標識」は、身体に歩行困難等の障害があり、一定の基準に該当する場合、申し込みをして交付を受けます。

ちなみに、この標章を出していても、「法定駐車禁止場所」、「無余地駐車となる場合」等の駐車は、一般車両と同じく取り締まり対象となります。

道交法で定める標章は、下の 4 つ、離れて右の3つが国際シンボルマーク

(後ろ2つの国際シンボルマークは、視覚障害者用と聴覚障害者用)