Qtech Hide & View におけるアクセスキーの安全性評価

READme-QtechHV-v011aj には、アクセスキーとしては“1～16 個の英数小文字列”を設定するように説明されていますが、実際には、もう少し長くて多様な文字列でも構わないようになっています。具体的には、「1～32 個から成る印刷可能な半角文字列」であれば何でもアクセスキーとして使うことが出来ます。
例えば、8 文字、16 文字、32 文字から成る

{09>&MC_　　30W:!?#&,boy¥794　　@*$RTnb~^<qKV*38142jJ+-][/..|GjR

などもアクセスキーとして OK です。一般には、なるべく長い文字列の方がより安全だと言えます。

以上のことを前提に、Qtech-HV のアクセスキーの安全性を“バイナリ・パスワード換算”で評価してみましょう。
通常のコンピュータのキーボードには 47 種の文字キーがあり、Shift-Key の操作で「上段」「下段」に使い分けれらます。
更に、Qtech-HV では〝空白〟もアクセスキーの文字列に含めることが可能です。（但し、アクセスキーの先頭に空白を入れるにはちょっとした工夫が必要です。）
以上のことから、長さ 32 のアクセスキーの種類は 95^{32} となります。
これに相当する“バイナリ・パスワードの長さ”を x とすると、等式

$$2^x = 95^{32}$$

が成り立ちますが、このような x の値は、対数計算により簡単に

$$x = 210.7188\cdots$$

と求められます。
このことから、「Qtech-HV のアクセスキーの安全性は、210 bit のバスワードと同等以上」であると言えます。

＜考察＞ 総当たり探索（Exhaustive Search）による Qtech-HV のアクセスキーの探索時間

先ず、32 文字長のアクセスキーの総数は

$$95^{32} \fallingdotseq 1.9371 \times 10^{63}$$

と計算できます。
或る 32 文字長のキーが正しいものかどうかを判定するには、実際に PC を使って Qtech HV (Extracting Component)を動作させ、その結果を（人によって）見極めざるを得ません。これに要する平均的な時間を1秒程度だと仮定します。
ここでは、そのようなPCを100万台使い、チェック作業が重複しないように、それぞれの分担を割振っておくものとします。このようなシステムは 1 秒間に 100 万個のキーをチェック出来る 高速コンピュータ を使うことに相当します。そして、1 年間では

$$10^6 \times 60 \times 60 \times 24 \times 365 = 3.1536 \times 10^{13}$$

個のキーがチェックできます。 従って、全てのキーをチェックし終える年数（K）は次の通りです。

$$K \fallingdotseq (1.9371 \times 10^{63}) / (3.1536 \times 10^{13}) \fallingdotseq 6.1425 \times 10^{49}$$

Big Bang 以降の宇宙の歴史が 1.382×10^{10} 年程度であると考えられていることから、このような総当たり探索でアクセスキーを発見するのは明らかに不可能です。たとえキーの文字長を 10 に縮めたとしても、およそ 200 万年程度かかります。

なお、英数文字だけ（62 種）を使った 長さ16文字のキーの場合は　1.5117×10^7 億年
長さ 8文字のキーの場合は　6.9235　年
となります。

最終更新日： 2019 年 11 月 27 日（河口英二）