ICF3 ピアパーク展示計画案 Rev.2　by 平山直紀

本計画案の目的

本計画案の目的は平山 直紀の父、嘉一の即死確率のある手術を回避し、嘉一の寿命を延ばすことだが、家族や他人の寿命を縮めるような本末転倒なことを起こさないこと。平山 嘉一が日本道路公団の北陸自動車道の建設局、所長だった時代の功績といわれている「親不知ピアパーク」に ICF3 のレプリカを展示することでピアパークの増収、高速道路料金の増収につなげる。レプリカの展示・管理のコストが非常に低コストに行えることが本計画を後押しすると思われる。具体的にはピアパーク内のヒスイ展示館に展示されているヒスイの石の隣にレプリカの**石**(半導体チップ)を置くだけ。本稿は一般の人でも読める文章にしているつもりですが ICF3 について数ページで語ることは不可能であり、ここに書かれている記述のみで ICF3 を判断することは難しい。
可能であればインターネットで本稿の最後にある参考 URL で調べていただけるようにお願いします。

ICF3 とは

ICF3 は 1999 年に日立製作所が開発した IBM メインフレーム互換機の暗号装置の半導体チップ。米国の暗号輸出規制のため IBM が売りそびれていた時に日立が互換機を発売したため欧州など世界に良く売れた。当時、日立製作所に勤務していた平山 直紀(本計画案作成者)が ICF3 を開発している。平山 直紀は 1997 年、米国シリコンバレーに 3 か月出張後、ICF1(1997 年)のリーダーとして開発がスタートした。ICF2(1998 年)には東大卒の小国氏が参画、ICF3(1999 年)では小国氏がリーダーとなった。このため平山 直紀はリーダーから暗号プロセッサ(主に RSA 暗号)の担当設計者になった。また ICF3 の SHA-1 演算器の設計原案も平山 直紀が作成している。
ICF3 は、それまで世界一だった FastMap を抜いて RSA 暗号演算時間で世界一ですが**学術的にも非常に価値のある石(半導体チップ)です。**マイナンバーカードで使われている公開鍵暗号は RSA ですが **RSA の高速化は難しく驚くほど、いろいろな方法がある。**また研究論文も多数あります。方法の一つにモンゴメリ乗算がありますが、ICF3 はモンゴメリ乗算を採用した世界初の石(チップ)です。商用化されたものでは、恐らく世界初。米国の巨大企業 IBM のメインフレームの互換機として ICF3 は開発されていますが、この IBM の仕様がモンゴメリ乗算の採用を難しくしていた。さらに **ICF3 は世界最古の巨大整数四則演算器**でもある。公開鍵安全性の根拠として巨大整数が役立つ世界となれば世界最古の巨大整数四則演算器が世界のコンピュータの歴史により深く刻まれる

ICF3 チップのレプリカ

日本では ICF3(1999 年)は外務省などに納品されている。そして設計上は電源を落とせば ICF3 チップ内の秘密鍵は消える。しかしチップ製造工場で魔改造されていないとも限らない。展示には ICF3 チップのレプリカ推奨。チップ内の画像をパネルにしたものであれば平山直紀が作成可能。しかしパネルでは集客力が低いため日立製作所にある売れ残れを後付けでもいいから入手する案も考えられる。ピアパークに何故、レプリカ(or パネル)が展示されているのかをネタにして集客力を向上させるしかない。ICF3 の設計者の平山直紀がピアパークの創業時の日本道路公団の北陸自動車道にある建設局の所長の長男であるということがネタになるのではないだろうか。

参考 URL

親不知ピアパーク：https://e-oyasirazu.com/
note 記事「暗号プロセッサ ICF3 について、その未来」： https://note.com/spinlock/n/n3123aa855fb6
OpenICF3 公式サイト：　https://openicf3.idletime.tokyo/