ディジタルの傘

吉　田　真　紀*

A digital umbrella

Key Words: Akashi Kaikyo Bridge, Zero Knowledge, Every Evil Under the Sun, Umbrella Leaf

1．はじめに

晴れた空の下，今日もディジタルの傘が開きます．

このように書き出してみましたが，まだディジタルの傘はないと思います．それどころか言葉の意味も定義されないまま，なおざりとなっていそうです．情報科学分野に関わって以来，目前で様々な情報技術が発明され，発展していきました．それに携わった様々な方の話も聞いてきました．そして，何度も意表を突かれました．ディジタルの傘という言葉は，この原稿を書くことが決まった後しばらくしてから聞いた言葉のうち，最も意表を突いたものでした．次の章以降では，大学に入学してから助手となった現在までの間に，意表を突かれた結果，新鮮な感慨をもつことができたエピソードについて，過去から遡って書いてみたいと思います．

2．夢ではない

大学に入学したとき，原口忠次郎博士が創設者である原口育英会の奨学生となり，それが縁で，明石海峡大橋に興味をもちました．原口博士は大正７年に京都帝国大学土木工学科を卒業し，内務省技師として従事したのち，神戸市長となり神戸の発展に寄与して“土木屋市長”の名をほしいままにした技術屋です．一方，明石海峡大橋は，橋長3,910メートル，吊橋の規模を表す中央支間長が1,990メートルの世界最大の吊橋です(正確にいうと，阪神淡路大震災による地盤のずれで0.8メートル伸びました)．明石海峡への架橋は，そもそも「鳴門海峡架橋構想」として昭和15年，原口博士が内務省時代に打ち出したものでした．橋を道の一部ととらえ，阪神，淡路，四国，九州を最短距離で直結させ，地域，さらには日本の発展に活かすことを目的としたものです．時節柄，旧海軍の猛反対を受け，立ち消えとなりましたが，原口博士は諦めることなく，後の昭和32年，神戸市長時代に市の予算編成で架橋調査費を計上しました．

毎年夏に，原口育英会の奨学生相互の親睦をはかるため，夏の会が開催されます．奨学生OBの方が手配して下さったこともあり，完成間近に明石海峡大橋の建設現場を見学することができました．まず，現場作業着とヘルメットを着用し，本州四国連絡橋公団(以降，本四公団)の船に乗り込み，明石海峡から橋を見上げました．その後，ケーブルの張力を支えるアンカレッジの内部をエスカレータで移動し橋桁の下に出ました．そして，60メートル下に広がる海面に足をすくませつつ橋桁の上に登り，夏空に伸びる主塔を仰ぎ見ました．東京タワー(約333メートル)の約一割引の高さ(約300メートル)をもつ超高層の構造物です．

その際に明石海峡の架橋についたニックネームを教えてもらいました．「夢のかけ橋」です．それだけ聞くと良いニックネームではないかと思ったのですが，実は予想以上の猛反対を受けたときに逆の意味でつけられたものでした．「市長は白昼に夢を見ているのではないか」とまで言われ，それに対し，原口博士が「人生，すべからく夢なくては」と言い放った結果ついたということです．

ある奨学生OBの方が，原口博士の著書に書いてあったエピソードを紹介して下さったことを，いまや夢ではなくなった大橋の姿と共にしばしば思い出します．ある河には幾本かの橋が架橋されていたそ

* Maki YOSHIDA
1974年４月生
2001年大阪大学・大学院基礎工学研究科・情報数理系専攻修了
現在，大阪大学 情報科学研究科 マルチメディア工学専攻 セキュリティ工学講座，助手，博士(工学)，情報セキュリティ
TEL 06－6850－6563
FAX 06－6850－6564
E-Mail maki-yos@ist.osaka-u.ac.jp

うです．その橋を地震が襲い，多くが落橋した中で，一本の橋だけは健全だったそうです．その橋の設計者が「唯一つ落橋しなかった橋を設計したこと」を自慢したところオーバストロング(Over-strong)だと非難されたそうです．設計強度を超える地震が襲ったにも関わらず落橋しない橋を造ったということは，社会から託された資材や資金等を無駄(過剰)に使用したことになる，そのために他の必要物の建造を妨げたことになるというのです．その奨学生OBの方は，ここまで話されると，「技術者として当然の非難の対象になる」という原口博士の指摘を，技術者が常に維持しておくべき視座の一つだと思っていると，結ばれました．

明石海峡大橋は，架橋地点から150キロメートル離れた太平洋プレート境界で発生するマグニチュード8.5の大地震や，架橋地点周辺で150年に一度程度発生が予想されるあらゆる地震に耐えるように設計されました．工事期間中に起きた阪神淡路大震災では，大橋直近でマグニチュード7.3，震度7という激震に見舞われながら，本体構造にはほとんど損傷を受けませんでした．一連の本四連絡橋(明石海峡大橋を含む)の建設にかかった費用は巨額で，現時点では回収の見込みがつかないとのことですが，明石海峡大橋が大震災を乗り越えることができたことは，上の意味で非難の対象とはならず，賞賛に値するのだと信じています．

3．知識ゼロとゼロ知識

大学院に入ってから，情報セキュリティの研究をしています．その内容は暗号理論(技術)とその応用です．「知識」と「ゼロ」の二つを組み合わせるとき，「知識ゼロ」ではなく，その逆，「ゼロ知識(Zero knowledge)」にした途端，それは暗号理論の専門用語となります．一般に，ゼロ知識の後には「証明」がつきます．ゼロ知識証明は，認証の道具として有効なことが示され，一躍注目されました．その後，様々な応用先が見つかり，多くの暗号関連研究者の間で，究極の技術と認識されています．

ゼロ知識証明とは，自分が秘密を知っていることを，相手にそれに関する知識を与えずに(ゼロ知識で)，相手に納得させる(証明する)ための方法です．初めてこの説明を聞いたとき，そんなことができるのか，と思いました．例え話で，そのゼロ知識証明の醍醐味を一部でも伝えたいと思います．学生に何か問題を出題したとします．その問題が間違っていないこと(正解があること)は，正解を教えれば納得してもらえますが，それでは出題した意味がありません．ここで，もし，その問題にゼロ知識証明があれば，正解を明かすことなく学生に納得させることができるのです．つまり，秘密によっては，自分が知っている秘密を「相手が知る」ことと，自分が知っていることを「相手が納得する」ことは別でありうることを明確に示した技術なのです．

暗号関連の国際会議のうち，もっとも大きな会議の一つ，CRYPTOが，1997年に開催されたとき(CRYPTO'97)，参加者にお土産として，Tシャツが渡されました．そこには，過去3000年に及ぶ暗号歴史の中で公になっている出来事や研究成果の代表例として，約20件がプリントされていました．

ゼロ知識は，その中でも，暗号歴史において近代と呼ばれる公開鍵暗号発明以降から選ばれた，五つのトピックに含まれています．

ちなみに，暗号歴史の先頭を飾るのは，有史上，最古の暗号文とみなされた，1900BCのNon-standard hieroglyphicsです．古代エジプトで，ある書記が標準外のヒエログリフ(象形文字)を使ったことをさしています．さらに，五つのトピックとは，公開鍵暗号(1976 Public-key cryptography)，秘密分散(1979 Secret sharing)，ゼロ知識(1985 Zero knowledge)，差分解読法(1990 Differential cryptanalysis)，線形解読法(1994 Linear cryptanalysis)です．最後に挙げられている線形解読法の考案者は，第三世代携帯電話の無線通信区間に利用する唯一の国際標準暗号として採用された国産暗号KASUMIの開発者の一人です．

4．いつか来た道通る道

この世の どんな悪いことにも
なおす手立ては あるかないか どちらかです
もしあれば 見つかるまでさがすこと
もしなければ 気にしないこと
(マザーグース“For every evil under the sun”)

研究を始めてから(＝大学院に入ってから)，「正解なんてものはない」ということを痛感しています．学部の科目であるProblem based learning(PBL)で，教官の立場から「大学時代に何を学ぶべきか」

を考える機会がありました．そのときは「問題解決能力」だと思っていましたが，今は「どんな状況になっても，考えることを放棄しないこと」だと思っています．

なぜこういう思いに至ったかといいますと，会社で製品開発に携わっている友人も同じ思いをもっていると聞いたからです．その友人の話をまとめるとこのような感じです：会社に入って製品を作るとき，最初は「こういう仕様のものを作れ」という指示が来た．しかし，そのうち「仕様」は与えられなくなる．要求と作業量と時間と性能を考えて，できる範囲のものが「仕様」になる．実際，納期時点のもの＝仕様，になることが多かった．状況が変化したとき，「その作業・機能は当初の予定ではなかった」という意見は正しい．正しいけれど，なにも産み出さない．結局，我々は「勝たなければ」いけない．現状が予想外の状況になってしまったとき，状況を嘆いても何も生まれない．分析も後回しで，いかに「次善の策」を実現できるかを考えなくてはならない．学生時代にちゃらんぽらんに見えた(失礼…)同輩が，社会に出てしっかりと仕事をしているのは，そのときに思考停止せずに考えることができているからだと思う…．

友人の話を少し変えて，「製品を作る」を「問題を解決する」に，「仕様」は「解」とすれば(あるいは，「仕様が与えられる」を「問題が与えられる」とすれば)，研究やその他の様々な状況に通じます．心のどこかで「今のままではまずいかも?」と，薄々思ってはいても，勉強していることを隠れ蓑にしてしまっていないか，勉強していれば誰からも責められないから，楽で，そこに安住していないか…，早い段階で正解がないことを体で知っておくことが肝要だと思います．

格好の良いことを書いていますが，振り返ってみて自分自身が，これを書く資格があるほど，常にしっかりとしているかどうか，怪しいものです．その意味で，言動が一致していないかもしれませんが，こう思ったことは本当ですし，今でも思い続けています．実際，学生のとき原稿締め切り直前に，指導教官と一緒に次善の策を考えた体験は，大切な財産です．そして現在，研究で予想外の状況に突入したとき，どうしているかといいますと，本章冒頭のマザーグースの最後の行を次のように変えてロずさむようにしています．

もしなければ，それを証明すること．

「最後の策」として「存在しないことの証明」が控えているから大丈夫，という意味です(それが一番大変そうですが)．

5．遭　　遇

今年の梅雨に入った第一週目，おりから降り出した小糠雨の中，サイバーメディアセンターへ移動した時のことです．研究室は基礎工G棟にあるのですが，雨足が強くなかったため，傘も持たずそのまま歩きだしました．基礎工H棟脇の駐車場を通り，曲り角を抜けた転瞬，とっさに認識できないものが視界に入りました．傘の代わりに，葉っぱをさした学生です．その葉は学生の両肩を覆い，遠くからでも見える産毛は雨粒をしっかり弾いていました．

梅雨に入ったばかりです．傘の備えをしていなかったのか，備えていないからといって葉っぱで雨をしのぐのか，しのぐとしても傘になるような，あんな大きな葉をどこで入手したのか．そこまで考えた段階で，ようやく周囲の人を確認しました．表向きは，誰も気にしていない様子でした．白昼夢はありえませんから，改めて，葉とその学生を目で追いました．

結局，あと少しで，葉っぱの傘に手が届くかというところまで近付いたのですが，そこで学生は向きを変え，基礎工B棟に入ってしまいました．件の葉はB棟入口に大切に立てかけられていましたが，自分の立場(5分後には，吹田キャンパスの研究室と共同で行う遠隔授業が始まる)を思い出し，少しほっとして，それ以上の追跡を打ち切りました．

サイバーメディアセンター内の会議室で，授業開始を待つ学生達に言ったところ，一瞬きょとんとした後，激しい反応を返してくれました．

「本当ですか．」

「森へのパスポートですよ，先生．」

「特急の止まらない駅のホームの端に，是非立ってほしいところですね．」

その中で，ここまで黙っていた学生が，穏やかな笑顔を変えず，言いました．

「そういえば，これだけ情報技術が進んだのに，いまだ傘はディジタルになっていませんよね，何故でしょう．」

他の学生共々，意表をつかれました．確かにディ

ジタルになっていません，聞いたこともありません．しかし，なぜというより，ディジタルになるとはどういうことかという疑問よりむしろ，「葉っぱ」から「ディジタル」が出た思考の飛躍に驚きました．

傘には色々な言葉がつきます．雨傘，折り畳み傘，核の傘，そして最近ならば情報の傘でしょうか．傘がディジタルになることが，何を意味するのか想像もつきませんが，閉じるのも惜しくなってしまうではないか，と思わせて欲しいものです．

6．おわりに

葉っぱの傘に遭遇した次の日，葉がどこから来たのか確かめに出かけました．遭遇前後の状況から学生の心理を推測し，記憶にある豊中キャンパス内の植生地から範囲を絞り込み，探索をしました．その結果，10分もしないうちに発見することが出来ました．件の葉は，木の葉ではなく草の葉(の大きくなり過ぎたもの)でした．草とはいえ，その茎の太さは小ぶりな木の幹ぐらいありました．そこに，葉をちぎり取った跡が真新しく残っており，ここが出発点であることが確認できました．

それ以来，構内を移動する道すがら葉の様子を見に行っています．一度，周辺の雑草と共にごっそりと刈り取られましたが，根が残っていたのか，小猫用の傘までは大きくなっています．この勢いですと，来年の梅雨の時期には人間用の傘として機能するはずです．豊中キャンパス内を歩いてみた結果，他の多くの場所でも生えていました．確認していませんが，吹田キャンパスにも生えていると思います．葉っぱの傘が，梅雨時期の阪大風物詩になるのも面白いのではないでしょうか．