松井氏インタビュー：「これからの暗号の主流は絶対こうなると思ったんです」

三菱電機（株）の松井充氏に，第 3 世代携帯電話で日本人の多くが利用している MISTY 暗号に関して，その発明までの研究開発と標準化の経緯，さらに暗号研究のマネージメントやビジネスとの連携や乖離まで，幅広くお話をうかがいました．暗号研究の世界的第一人者が実践してきたことの一端をお伝えします．

アタックからの暗号研究スタート

DP（大蒔・村上・寺田・平田）：今日はお忙しいところ，どうもありがとうございます．まず，松井さんのプロフィールから教えていただけますか．

松井（写真）：京都大学の数学科で純粋数学をやっていまして，修士課程まで進みました．しかしさすがに数学者になる才能はないなと思い，メーカを希望し三菱電機に 1987 年に入社しました．最初に誤り訂正と暗号をやっている研究所のチームに配属されました．当時，誤り訂正に関連する仕事が沢山あって，光磁気ディスクの国際規格が決まり，私はそのための LSI 開発をやることになり，ハードウエアエンジニアとしてスタートしました．そして，私の横にいた暗号研究者 2 人の内の 1 人が，今回論文を一緒に書いた近澤さんでした．当時の上司は，暗号というのは将来役立つから，今の内からやっておこうという考えをもっていました．

私はプロパーで誤り訂正の仕事を 2 年ぐらいやりましたが，その間，プリペイドカードの磁気データをスクランブルするとか，暗号の仕事もちょこちょこ引き受けていました．

暗号に真剣に取り組むようになったきっかけは，’90 年にイスラエルの研究者（Biham と Shamir）が差分解読法という画期的な暗号解読の手法を発表して，当時としては日本の標準ともいえる NTT の FEAL 暗号を破ったという大ニュースが飛び込んできたんです．じゃあどんな手法だろうと思って論文を取り寄せて，それを読んでみました．いろんな暗号を破ったような方法とのことだから，さぞかしすごく難しいことがその論文に書いてあるだろうと思っていたのですが，ものすごく当たり前のことが書いてあってスラスラ読めるんです．それが非常に面白くて．

DP：京大時代の数学の素養が役に立ったとか．

松井：直接的には京大でやっていた純粋数学がどれぐらい役に立っているかというと，まあ 10%か 20%ぐらいでしょうか．ただ，抽象的に物を論理だけで組み立てていくという訓練はされているので，そういう意味では役立ったと思います．これだったら自分も追いつけるんじゃないかと思ってその手法をまねして，ほかの暗号に適用したらどうなるかみたいなことをやっている内に，だんだんと暗号にはまっていきました．

DP：’90 年代前半に大学で暗号の講義とかあったんでしょうか．

松井：全然ありませんでした．大学で暗号の講義がされるなんていうのはごく最近じゃないですか．大学で暗号技術の講義をすると，学生が「それ，授業で習いました」とか言うから，「えっ，こんなこと授業でやってんの？」と，それはもう隔世の感があります．

いずれにせよ入社当時は 1 人 1 台のパソコンなんていう時代ではさらさらなく，もちろん携帯電話もない時代なので，暗号の仕事は何もない暇な時代でした．それに世の中全体がやっぱり今と比べて，のどかな時代でした．今みたいに，研究所が，企業収益に直接的なかたちで貢献を求められることも少なかったし，僕らメインストリームじゃない研究者が窓際で論文を読んでるというようなことが結構許される時代だったんです（笑）．

そんな自由な環境の中で論文を読み，いろいろ好きなことをやっている内に，’93 年に線形解読法というオリジナルなアイデアが出てきて，暗号解読の実験をしたりしていく内に，暗号の専門家になっていきました．

DP：既存の暗号を解読する方からこの道に入られたんですね．

松井：そうなんです．私はアタックから入りました．線形解読法で，当時のアメリカ標準の DES という暗号が破れるんじゃないかと思って，’93 年の夏から秋にかけて実際に 12 台のワースステーションを 2〜3 カ月間回しました．ただ，それは暗号を破るほうの研究なんで，企業としてはそんなことをしても全然ビジネスにはならないわけです．ただ当時の上司はこの成果をとても高く評価してくれ、これはとても励みになりました．

DP：例えば，暗号を破ったということは研究成果として学会で発表されるんでしょうか．

松井：されます．暗号解読というのは暗号研究の非常に重要なテーマですから．

暗号研究こそオープンに

DP：そもそも暗号って，人に見られたくない何かを隠すために暗号化するというものなので，その暗号技術を学会で発表することに少し違和感を覚えます．

松井：確かに暗号というのは歴史的には軍事外交から来ている技術なので，60 年代ぐらいまで，特にアメリカでは暗号技術を学会発表するなんてことはあり得ませんでした．ところが 70 年代になってエポックメーキングなことが 2 つ起こったんです．

1 つは，アメリカ政府が自国の標準暗号を一般から公募したんです．それで IBM が応募したものがアメリカの連邦政府標準暗号になりました．もちろん軍は別です．アメリカはさすが先見の明があったと思います．そうやって暗号をオープンにすると安くなるし，相互接続性が保証されます．70 年代頃から暗号の学会ができ始めました．

もう 1 つは，公開鍵暗号という全く新しいタイプの暗号が発明されたのも 70 年代です．それまで基本的には 1 対 1 の通信が前提だった暗号が，公開鍵暗号で多対多の暗号化ができるようになったのです．インターネットのような不特定多数を相手にする状況で使えるので，それからわっとみんなが研究に参入してきました．

暗号の方式を秘密にしていると「自分だけが暗号を解ける仕組みをその方式の中にこっそり埋め込んでいるんじゃないの」というふうに疑われかねません．新しい暗号を設計したら学会でオープンにして，いろんな研究者から叩いてもらって，もし問題があれば修正していきましょうというのが学会のコンセンサスになってきたんです．実は秘密の罠が仕掛けられていて，悪い人だけがその暗号を解読できるというのが最悪のシナリオなのです．

DP：逆説的で面白いですね．

松井：暗号の研究は，大きく解読と設計に分かれていますが，私は自分が暗号解読からスタートしてすごく良かったと思っています．というのは，ただ単に「何か良いものを作りましょう」といっても，まず「良いとは何か？」という問いに答えなければなりません．今すでにある物差しの上で新しいものを作って他の研究と差別化できるような成果を上げるのはなかなか難しい．暗号解読をしたということは，結果的に暗号の強さを測る新しい物差しを作ったということと同じなんです．新しい評価軸ができたら，その評価軸でより良いものを作る．すると今までとは違う新しいものが作れます．

私が最初に読んだ論文に書いてあった差分解読法とか，私のオリジナルである線形解読法でも解けない暗号はどうしたら作れるだろうか．そんな新しい評価軸に沿って研究を進めていって，それで MISTY という暗号を作ったのが入社 8 年目の’95 年でした．

DP：松井さんは’93 年に，今お話に出てきた DES 暗号の線形解読法を提案した論文で，電子情報通信学会から情報とセキュリティシンポジウム(SCIS)論文賞を受賞されていますね．あのお仕事は 1 人でやられたんですか．

松井：アルゴリズムは 1 人で考えました．もちろん計算機を貸したりとかで協力して下さった方々は何人かいらっしゃいます．

DP：DES 暗号化の方式は当時すでに公開されていたのでしょうか．

松井：はい，すでに完全公開されていました．暗号解読というのはどういうゲームかというと，まず暗号化する前の元の文（平文），暗号化されたあとの文（暗号文），暗号化アルゴリズムの仕様が解読者の手元にあるという仮定を置きます．しかし暗号化した時のパスワードが分からない．ではどれぐらいの手間をかければ，暗号文と平文の情報からパスワードが求まるかという問題なんです．パスワード破りにちょっと似ていますね．

DP：パスワードを求めるんですか．

松井：そう，パスワード．一度パスワードが分かったら，後はどんな暗号文だって解読できちゃいますよね．これが暗号解読の標準的な問題設定です．

DP：問題として，平文は手に入らないと仮定するものだと思っていました．

松井：一見，そう思われるかも知れません．平文が手に入るなら，何のために暗号解読する必要があるのかと思われがちですが，良く考えてみると，暗号解読では暗黙の内に平文を必ず仮定しています．暗号文だけから平文を求めるということはそもそも不可能なんです．というのは，平文に関する情報量がゼロだと，暗号文を適当なパスワードで元に戻したものが平文だと言うことができ

て，それ以上のことは何も言えないからです．

DP : なるほど．求める答えは平文の方ではないんですね．

松井 : そうです．例えば，元の平文は日本語であるというような何かしらの情報があれば，試しにあるパスワードで解読してみて，もし解読結果が日本語でなかったら，そのパスワードは間違いだったとなるわけです．この調子で，解読者により大きなパワーを与えて，それでも破れない暗号を作りましょうというのが暗号研究の考え方なのです．最近ではパスワードさえも殆ど分かっているような仮定を置いたりするんですよ．

MISTY の発明

DP : 線形解読法の翌年に MISTY を提案されましたね．

松井 : MISTY を報道発表したのは'95 年 9 月でした．MISTY の最大の特徴は，差分解読法や線形解読法をそのまま適用したのでは絶対解けませんという数学的な証明を付けた点です（証明可能安全性，Provable Security）．

実は，差分解読法が提案されたすぐ後に，差分解読法では解けない暗号を作る方法論に関する論文が出て，それを見た私は絶対これだと思ったんです．差分解読法みたいなすごいパワフルなアタックでも解けないということが証明できるんだから，新しい暗号の設計をやるならこの方法論しかない．さらに線形解読法にも同様の方法論が適用できたので，差分解読法でも線形解読法でも解けない暗号が設計できる．それから証明可能安全性に基づいた暗号をいろんな人が設計して提案してくる．これからの主流は絶対こうなると思ったんですけど，意外とね…．誰もやらなかったので，自分でやろうと思ってできたのが MISTY なんですよ．

MISTY は証明可能安全性を持つ世界初の実用暗号であるということをアピールして発表したら，暫くして証明可能安全性に注目が集まるようになりました．ただ，MISTY は，当時の他の暗号と違い、高速化と小型化を両立させるためにハード化にも力をいれました．その点については，やっぱりメーカで開発できた点が良かったと思っています．

DP : 高速化にはハードとソフトの 2 通りありますよね．

松井 : DES 暗号が発表された 70 年代はハードウェアで暗号を実現する時代で，ソフトで暗号を実装できるような時代じゃなかった．それが 80 年代から少しずつソフトウエア化されるようになってきた．'95 年は Pentium プロセッサが出始めた頃で，パソコンはどんどん安くなっていくし，性能も指数的に上昇するしで，ソフトウェア万能の時代になっていました．

ハードで暗号を作ろうとすると試作に何百万円もかかるのに対して，ソフトなら手軽にプログラムを組んですぐ暗号を実装できます．これからはもうソフトの時代だと．暗号をハードで組むなんてナンセンス位の雰囲気すらありました．その結果'95 年頃は，パソコンでこんな速い暗号ができましたというテーマの暗号研究が多かったです．

ところが，当社の半導体の技術者と話をすると，昔も今もとにかく「小さい物を作る」を目標にしています．サイズが小さいことで，チップの単価が下がる，消費電力も下がる，スピードは上がりますから．なので MISTY は，証明可能安全性という理論的に良い性質を持ち，ハードで小型高速処理を実現するという 2 つの利点を兼ね備えるよう設計しました．ハード重視というのは今となっては珍しくないのですが，ソフトウェア全盛の当時としてはむしろ変わり種でした．

DP : 論文に書かれているように，このハード化が，3GPP（第 3 世代移動体通信システムの標準化プロジェクト）の時に生きてくるんですね．

松井 : そんなことになるとは当時は夢にも思わなかったんですけど，そう，生きてきたんです．世の中では'90 年半ばからダウンサイジングの波が押し寄せていました．世の中の通信機器は手のひらに乗るくらい小さくなって．そうすると消費電力が一番問題になります．今でも，携帯電話の電池がもたないというのがクリティカルな技術課題になっています．声も文章も全部暗号化しているので，暗号ハードはとにかくのべつ幕無しに動作しています．それが無駄に電力を消費するなんて許されません．さらに暗号の回路には，携帯電話の通信用 LSI の中の 2 ミリ四方くらいの面積しか与えられないのです．とにかく小さくて低消費電力が求められます．たまたま MISTY はハードが小さかったので，適しているということになりました．

暗号は付加価値である

松井 : MISTY を提案したのと，たまたま同じ年に研究所の組織が変わって，今私が所属している情報技術総合研究所が誕生して，暗号研究者 12 人だけの所長直轄のグループが 1 つ発足し，暗号でビジネスすることがミッションになりました．

DP : 暗号でビジネスすると言っても，具体的にどんなビジネスをされたのでしょうか．

松井 : 当時我々が持っていたのは論文に書かれたアルゴリズムだけでした．製品があるわけでもない．当時の部長は，日本のマーケットは小さいからアメリカに行くぞと言って，3〜4 人ぐらいで，ネットスケープなどその当

時に暗号を使っている会社を幾つか回りました．まずは暗号の紹介をして「こういう暗号があるんだけど，何かに使ってみない？」みたいな（笑）．みんな話は聞いてくれるんだけど，大体「ありがとう」で終わりですね．今から考えたら本当に笑い話みたいなもんですけど，そういうのが続いて…

DP：売り込む時に，オンライン決済する時に使ってくださいとか言ったりしたんですか．

松井：当時は「この応用に」ってなかなか言えなかったですね．後になってわかったことですが，暗号って儲からないんですよ．より正確には，暗号だけで儲けようというのはかなり難しいというか，間違っているとさえ思う時があります．暗号って付加価値だと思うんです．だって一般消費者の皆さんは，暗号だけ買うことはないですよね，

DP：最近では，携帯電話に暗号が入ってたり，パソコンを落とした時に中のデータを見られないために入ってたり…

松井：そうですね．今や暗号は当たり前で，IC カード，車のドアを開け閉めする車のキーなど，暗号を使わずに１日を過ごすということが難しいぐらいの世の中になりました．でも暗号そのものを消費者は買っているわけじゃなくて，すでにあるモノに必須の機能として暗号が入っているんです．暗号とはそれ自体を売るような技術ではくて，その暗号によって元の製品の価値をどれだけ高められるかという技術なんです．だから暗号からの収益は幾らなのか，暗号はどれ位の規模の事業なのかと質問されますが，良くも悪くも，それを数値的に表現するのはほとんど不可能なんです．後になって，暗号のビジネスにはそういう難しさがあるということがだんだん分かってくるんですけど．

MISTY の無償化

DP：MISTY は最初から無償だったんですか．

松井：’95 年に発表して無償にしたのは’98 年でした．最初から暗号は無償提供すべしという意見はありました．ただ，無償にするにもいろいろ社内準備が必要ですし，ある程度自分達でもの作りを進めて先行者となってから無償公開したかったということもあります．

DP：発表された論文を見れば誰でもプログラムが書けるようになっているんじゃないのですか．

松井：ある意味ではそうですけども，そこから製品と言えるぐらいの品質のものを作るためには，やはりそれなりのリソースが必要となります．他人の作った，標準でもない MISTY に，そこまでのリソースを投入する人はなかなか現れないとは思いますが．

あるいは，試験的に MISTY を解読してやろうという人はプログラムを書くでしょうけども，それは解読のためのプログラムであり，製品とは全然別物です．

DP：どんな製品を作られたのでしょうか．

松井：ソフトウエアライブラリを一生懸命作りました，ある程度，物ができてきた段階で，皆さんに使ってもらうために特許ライセンス料を無償にしようと進言しました．そうすれば，他の人が MISTY を使って製品を作り商売することもできるけれども，皆が MISTY を使うということは回り回って当社製品が売れることにもつながるだろう．またアメリカでは政府標準暗号の多くを無償にしているという事情もあります．しかし研究所が独断で MISTY を無償化できないので，事業部門に対して「いいですか」とお伺いを立てた所，案外すんなりと OK が出ました．

DP：すぐにですか．

松井：ええ，割とすぐ．その時，暗号は殆どビジネスになっていなかったからで，もし暗号が売れていたら無償化は絶対に OK されなかったでしょう．（笑）

DP：今でも「本当に暗号で儲かっているの？」と言われるのですか．

松井：言われます．苦労して原価低減して製品を作って売っている方々から見たら，特許を無償にするなんてと思われるでしょう．でも暗号から得られる利益はどうしても間接的なものなんです．

無償にしたことによって国際標準という名誉を獲得できました．そうすると当社は暗号に強いと世間に認知され，結果的に三菱電機は他社より情報セキュリティに関するビジネスを有利に進められます．商談の時など，じゃあこれからセキュリティはちょっと三菱電機に任せてみようとか，そういうのは結構あります．それと，特許を無償にするといっても製品まで無償にするわけではありません．当社の製品に三菱電機の暗号が入っているということで付加価値になります．他社も同じ標準を使えば他社製品も売れるでしょうけど，当社製品も売れるでしょう．

いずれにしろ数値化するのは難しいですけど，社内では，暗号は三菱電機が強い技術の 1 つとして事業に役立っていると認めてもらっています．

MISTY の標準化

DP：そしていよいよ MISTY の標準化となるわけですが，近澤さん松井さんの論文を拝見して驚いたのは，ここに，3GPP の会議に行かれたらエディタの方が辞めちゃって

いて，「雰囲気に呑まれ，エディタを引き受けてしまった」と書いてあったことです.

松井：これは著者 2 名の内，近澤さんの話です．（笑）主語はほぼ近澤さんだと思います.

DP：この，雰囲気に呑まれ，引き受けてしまったというのは，もともとあまり引き受ける気はなかったということなんですか.

松井： 標準化ってすごく骨が折れる仕事なんです．地理的なギャップもあれば，言語的なギャップもある．日本では，その技術を開発した技術者が標準化の会議にも出席することが多いですが，欧米では標準化というのをメイン業務にしている人が標準化の会議に出席するようです．日本人にとっては，技術者が自分の技術開発しながら同時に売り込みもするみたいな構図になります.

DP：それまでは論文を読んで，プログラムを書いて，ハードウェアチップを作っていたのに，突然標準化の会議に駆り出されるわけですね.

松井：はい，近澤さんのケースはそうでした．近澤さんが出席していた 3GPP の会議は，多分月 1 回以上のペースでヨーロッパで開かれていたと思います．でも近澤さんは海外出張が好きなので，標準化に向いていたように感じます．（笑）

DP：松井さんは標準化にどのようにかかわったのですか.

松井：'98 年 12 月に 3GPP が設立されて，日本からは ARIB が，ヨーロッパからは ETSI がメンバとして参加していて，近澤さんはその 3GPP の会議に行っていました．3GPP の会議には，端末メーカ，キャリアなどが参加しています．ETSI の下部組織として SAGE という暗号専門家のグループがあって，私は'99 年にその SAGE に参加しました.

DP：SAGE は何人の組織なんですか.

松井：10 名ちょっとぐらいです．ドイツテレコム，フランステレコム，ブリティッシュテレコム，ボーダフォン，スウェーデンのテリアとか，大体はヨーロッパの通信キャリアの暗号技術者です．でも，そうでないといけないという規則はないので，著名な暗号研究者のいるノキアのような端末メーカと，あと私は多分異例だと思うけど日本人でしかも三菱電機.

ヨーロッパの通信暗号標準化のやり方は少し変わっていて，伝統的に SAGE という専門家グループに委託して暗号規格を作らせるのです．そうなった背景には，昔はフランスなど暗号に関する厳しい法規制を持つ国があったので，各国が一堂に会して全員でオープンに議論しにくかったんでしょう．そこで，特権的な組織を作り，そこに暗号標準化を全部任せようというような仕組みができたんだと思います．それが今に至るまで続いてきたと.

近澤さんが参加されていた 3GPP の会議そのものは，どのような暗号にするかを決めるわけではありません．SAGE という専門家グループに対して，こういう暗号を作って下さいと注文を出すんです.

DP：暗号回路は 10 キロゲート以内じゃないといけないと論文の中に書いてありましたね.

松井：例えば端末メーカから見て具体的な要求仕様を示す．SAGE はそれを見て，ではどんな暗号を作ればいいかを考え始めます.

SAGE は 1 年ぐらいかけてそのような暗号作りに携わることになりました．ただ，1 年間というのは，ゼロから暗号を作り上げるには短すぎたので，既存の何かをベースにしましょうとなりました．その時，3GPP にいた近澤さんが，MISTY は無償だし，ハードウエアのサイズは 6 キロゲートで小さいし，どうですかとタイミング良く推薦して下さいました．SAGE では，すんなりとじゃあ MISTY を使おうかということになりました．3GPP は会議を重ねて'99 年 8 月の第 5 回会合で MISTY が第 3 世代の携帯電話の暗号アルゴリズムのベースとなることが内定されます.

すごく早いペースですが，その間に SAGE は MISTY を携帯電話用にするため変更を加えました．それに KASUMI という名前をつけて標準にしました．KASUMI のドキュメントも全部ネットに載っているので誰でもその仕様を見て作れます．同時，三菱電機は，KASUMI に関しても無償で使用許可しますということを宣言しました.

DP：ということは御社の儲けはないと.

松井：特許に関してはゼロです．それはもう標準化と引きかえなんです．でもここでライセンス料を取りますと言っていたら MISTY は絶対に標準になっていませんでした．結果的に，標準化にありがちな組織間のバトルに巻き込まれなくて非常にラッキーだったと思います.

暗号はどこでも役立つ

DP：暗号が一番役立っているというか，今社会に貢献している分野とか，将来有望な応用はどういうところだとお考えでしょうか.

松井：もう何でもですよ．まずどういう所に暗号が必要かというと，それは経済的価値を持つ情報をやりとりする所はすべて．つまりお金に関わる情報です．プライバシー情報だって，プライバシー情報がお金になるから守らなくてはならないのです．今は無線通信で暗号がかかってないほうが少ないんじゃないでしょうか.

DP : プライバシーや個人情報の保護，電子認証，著作権などの権利保護は分かりますが，その他はできるだけ暗号をかけないほうがいいのではないかと思うんですが．

松井 : 世の中としてはそうかも知れません．暗号が必要になるということは，世の中に悪い人がいるからであって，本当は暗号なんか不要な世の中になるのが望ましいことですね．

今，カーエレクトロニクスのセキュリティに注目が集まっています．もともと車には何十個もマイコンが搭載されていて，それらがネットワーク化されてます．世の中，そういう車を改造する人が一杯いまして，変な改造をされると命にかかわりますから，暗号化が必要になります．あとスマートグリッドでの電力情報の扱いにもセキュリティが必要ですし，クラウドでももちろん必要です．

DP : 以前，私の勤務する研究所にもクラウドを導入しようと働きかけたことがあったんですが，そうすると会計表とか人事の情報とか見られたら困るような情報が，自分の手元ではなく違う場所に置かれるわけですね．もしアメリカに渡ったらもっと困るなとか….

松井 : 今クラウドの一番の阻害要因がセキュリティですよね．どこに情報があるのか分かりませんからね．

DP : 結局, それが理由で研究所を説得できませんでした．

松井 : 今「クラウド暗号」というクラウド向けの新しい暗号がいろいろ提案されているんですけれども，これは従来の暗号とは全然違ったメカニズムですごく複雑な数学を駆使しているんです．実用化にむけた研究開発が急速に進んでいます．

暗号研究のマネージメント

DP : 今，松井さんの部には何人ぐらいメンバがいらっしゃるのでしょうか．

松井 : 40 人ぐらいです．

DP : その 40 人が全員，暗号をやっているんですか．

松井 : はい，三菱電機の暗号に関してはほとんど全て私の部でやっています．三菱電機の研究所の特徴は，論文を書くことがメインの基礎的な人から，製品開発に近いことをやってる人までが同じ部の中にいることですね．

他社のことは良く分かりませんが，基礎研と応用研が別々になっていたり，通信のレイヤに合わせて組織が分かれていたりするようです．三菱電機では，少なくとも暗号に関しては下から上まで，情報セキュリティも私の部が担当しています．アルゴリズム屋さんが考えたことを，5 メートル 10 メートル先にいるインプリメント屋さんがソフトウエア化・チップ化します．

DP : '87 年には 2 人だったのが…

松井 : '95 年に今の新しい研究所ができて 12 人になって，一番多い時は 50 人ぐらいでした．

DP : その 40 人の部の中には，アタック専門の研究者もいるんですか．

松井 : 普通は解読も設計も両方やります．昔はアタッカとデザイナというのがはっきり分かれてましたけど，今は暗号技術の非常に良い教科書もできて，いろいろ勉強できるようになったので，大体ひとりで両方できます．自分の設計した暗号は，その安全性とか品質保証のために必ず解読に関する評価をするので，ある意味アタックしてない設計者というのはいないです．

DP : '95 年から 16 年経ちますが，そうやって社内に築き上げてきた暗号研究文化の継承とか後進の育成とか，どのように考えていますか．

松井 : その点については前々から意識していました．付加価値としての暗号が良いか悪いかなんて専門家以外の人には分かってもらえないので，その人の名前が世間で広く知られているスターのような人物が欲しいです．技術者という意味でかなり優秀な人は何人もいるので，そういう面ではあまり心配してないんですけども．暗号を分かってもらうためのデモもとても難しいんです．

DP : 暗号のデモって，どのようにするんですか．

松井 : ここに花の絵があるとします．暗号をかけました，砂あらしになりました．復号しました，花の絵に戻りました．というようなのを昔はやっていました．でもそれ以上のことをやってもなかなか分かってもらえません．これが音声や画像なら，音がきれい汚いとか，ノイズが多い少ないとか人間の感覚にすぐ訴求できます．また，暗号の仕組みを理解してもらうことも難しいです．分かるのは, せいぜい速い遅いということくらいでしょうか．

だから尚更イメージが大切なのです．何かわからないけどスゴい．そういう時に国際標準というのは非常に大きかった．ただでさえ日本は外圧に弱いですから，まず外国で名を上げると，日本には割とすっと入って来られるのです．MISTY がまさにそうでした．

暗号研究の潮流

DP : ネットワークが遅いと，暗号がボトルネックになっていると言われることが多いですよね．

松井 : そうなんです．でも，昔はそのうち 8 割は濡れ衣で，暗号と全然違うところがボトルネックになっていたんです. だけどでも 2 割は確かに暗号のせいだったので，あんまり偉そうなことは言えませんでしたが．今では，MISTY とか RSA のような昔から良く使われてきている

暗号を使う限り,もう相当に機器も実装技術も進歩して,暗号がボトルネックになることは殆どなくなりました.

DP : だけど,暗号のスピードは重要だと思います.個人情報保護とかで暗号が複雑になればなるほど,だんだんじれったくてしょうがなくなる.

松井 : 仰る通りです.そういう課題に対して,軽量暗号(lightweight cryptography)という動きがあります.最も小さい暗号を作るために,その要求事項は何で,どうやってクリアするかを考えるんです.しかし,暗号の強度に関しては研究者の動いている行動原理と市場で必要とされるものの間にはしばしばギャップがあって,研究者は研究で飯を食っていかないといけないので,だんだん論文を書けることだけにテーマが移ってきてしまうんです.

DP : だんだん論文を書けることだけにテーマが移ってくると,何が起きるのでょうか.

松井 : 研究者はひたすら非常に強い暗号を追い求めてかすり傷一つも許しません.ところが実用側から見たらそんなかすり傷程度は実際の製品として全然関係無かったりするのです.実用側からは理論屋の遊びにさえ見えてしまう.しかし理論屋の宿命というか,どうしても世界に認めてもらうには理論的に完璧なより強い暗号を求めてしまうんです.そういう傾向は暗号だけではないのかも知れませんが.

DP : 最初は現実的な課題から始まっていたのに.

松井 : ところが一方では今は昔と違って,暗号の論文を書いても理論が面白いだけでは論文は採録されないんです.どれぐらいのスピードで動くのかとか,ある程度実用的なことが言えないとダメなんです.時代がそうなったのですね.なので,ある程度モノ作りのセンスもないと,研究成果として認められるのは難しくなってきています.そういう意味で,暗号って産業界のほうが人材の層が厚くて強いと思います.

先ほど言ったように,暗号研究ルールの流れは,アタッカにどんどん大きなパワーを与えていって,それでも解けない暗号を作ろうという方を向いていて,その流れがずっと続いてきています.暗号アルゴリズムは 1 回作って発表したら改良はそんなに容易ではなくて,その意味では暗号設計者はまな板の鯉です,なにせゲームのルールが勝手に厳しい方に変わっていくのですから.

もちろん新しいゲームのルール下で安全な暗号を作ろうと思ったら,当然ロジックは複雑にならざるを得ません.しかし一方で実用的なアルゴリズムとしてはどんどん小さいものが求められています.ここに乖離が存在します.世界で認められるためには,この強くて小さいという 2 つの要求を同時に満たさないといけません.難しい時代になったと思います.

DP : 実用という話ですと,住基ネットの本人 ID というのはなぜ普及しないのでしょうか.

松井 : それは暗号屋のせいではないと思います.(笑)

DP : 本人 ID の安全性を保証する部分はもう既に準備完了していますからね.

松井 : 住基ネットが始まった時,住基ネットのセキュリティが問題になりましたが,セキュリティに絶対ということはないんです.暗号に関して言えば、特殊な例を除けば絶対に解けない暗号というものはありません.今の暗号は,計算量的な安全性という考え方をしています.実際,無限の計算能力を持った敵を仮定すると、パスワードが有限長ならば,全パスワードを総当たりでチェックすれば,どんな暗号だって解けちゃいます.それなら例えば世界中のコンピュータを集めて 100 億年かければ解読できる暗号を,弱くて使えない暗号と言うかというと、普通言わないですよね.つまり,ものすごい計算パワーがなければ解けないような暗号は解読できないと見なすという考え方です.解けるか解けないかを厳密に言ってしまうと,すべての暗号は「解ける」です.

だから,コンピュータの進歩と暗号の強さというのは相関関係があるんです.将来コンピュータ技術が進んで,もちろん暗号解読の手法も進むと,今は解読されない暗号が解読されてしまう危険性がゼロではないんです.ただ,ゼロではないということをもって危険だから使えないというと技術の進歩はないわけで,どんな技術だって安全だ,絶対大丈夫ということはありません.むしろこの点のリスクをどう見積もるかというところが重要なんです.

DP : パスワードを総当たりで調べられないようにするには,暗号化アルゴリズムをある程度重たくする方向もあるのではないでしょうか.するとまた暗号がボトルネックになってしまうけど(笑).

松井 : パスワードそのものの暗号化は暗号アルゴリズムが少々重たくても,たいしたオーバーヘッドにはなりません.また,パスワードの長さが十分に長ければ,例えば 128 ビットを全部総当たりすると 2 の 128 乗かかるわけですよね.2 の 128 乗ってとんでもない数なんですよ.全数探索はもう 128 ビットもあれば,今のテクノロジではほとんど不可能な数なんです.量子コンピューターができれば別ですけれども.

共通鍵暗号と公開鍵暗号

DP : 共通鍵暗号と公開鍵暗号とを比較すると,どこがどう違うのでしょうか

松井：共通鍵暗号というのは基本的に 1 対 1 の暗号なんですが，公開鍵暗号に比べて小さくて高速だから，使い勝手がいい暗号なんです．ただ，共通鍵暗号でやれることというのは限られていて，例えば一般の通信の秘匿とか文章の秘匿とか認証とか．

公開鍵暗号というのは，1 対多のネットワークが組めるすばらしい暗号で，ものすごく応用が広いんです．公開鍵暗号は例えば電子署名，電子マネーを可能にします．そのかわりスピードが遅くてコストが高くつくという欠点があるので，もし公開鍵暗号で共通鍵暗号並みに高速なものが現れたら，共通鍵暗号なんて使われなくなるでしょう．今でも共通鍵暗号が生き延びている唯一の理由は，公開鍵暗号に比べて大体 3 桁位スピードが速いということなのです．

DP：松井さんは，共通鍵の DES 暗号を解読されたわけですが，公開鍵の RSA 暗号を解読しようとは思わなかったのですか．

松井：たまたま自分が最初に読んだ論文が，共通鍵暗号を差分解読法で解読する内容だったので本当に成り行きでそっちの方へ行ってしまいました．もし最初に読んだ論文が公開鍵だったらそちらの方に進んでいたかも知れません．NTT フェローの岡本龍明さんは，公開鍵の方に取り組んでおられる世界的研究者でいらっしゃいますね．

DP：暗号は無償というのは，もう世界の常識なんでしょうか．

松井：実は共通鍵暗号と公開鍵暗号とでは少し状況が異なっていて，応用が広い公開鍵暗号とコストが低い共通鍵暗号が共存共栄している段階です．共通鍵暗号は、やや極論ですが，高い安全性と小型高速の両立を求めないのなら幾らでも作れるし，また歴史的経緯からいってほぼ無償です．共通鍵暗号は有償だと言った途端に，おとといおいでという世界です．公開鍵暗号というのはそもそもアルゴリズム設計が数学的に難しく、実用化された方式も多くないので有償でも生きてこられました．

DP：今はもう公開鍵の RSA 暗号の特許が切れているので，RSA は無償で使えるんですよね．

松井：公開鍵暗号というのは，そもそも公開鍵暗号として十分実用的に機能すると立証された数学の原理がこの 35 年間の歴史でたった 3 つしか発見されていないのです．だから，実用に耐える公開鍵暗号も世の中にそんなに多くないんです．代表的な公開鍵暗号である RSA 暗号は 70 年代に発明されて特許化されて，皆が長らく特許料を払う必要がありました．その間に世の中に RSA 暗号のインフラが整いました．今，RSA 暗号は特許が切れてパブリックドメインになりましたし，マイナーな暗号を使っても相互接続性が無いので，世の中ますます RSA になっています．有償の公開鍵暗号が今後も本当に儲かるかどうかは分かりません．

DP：暗号ってまだ意外と国境が存在していますよね．アメリカは AES だけど日本では Camellia にしたらいいんじゃないかという話もありました．国ごとに暗号選択の方針が異なるのでしょうか．

松井：そうですね．アメリカの暗号はデファクトだから，皆がそれを使えばいいという考え方と，日本は日本の暗号をできる限り使っていこうよという考え方があります．韓国はそれぞれの分野ごとに自分の国でつくった暗号を使っています．お国柄というのもあるかも知れません．

暗号そのものを売りにしてない日本のメーカからすると，暗号なんて部品ですし，別に日本の暗号を使わなくてもと考えるのは当然かもしれません．当社みたいな，暗号あるいは情報セキュリティを看板に掲げているようなところは，自分で作っていこうとしますけれど．

日本はせっかく高い暗号技術をもっているのに，その技術が十分に利用されていないというのは，個人的には残念なことだと思います．

DP：暗号はやっぱりアメリカが強いんでしょうか．

松井：そうです．アメリカは技術で世界をリードする国としてやってきますから．特に情報セキュリティとか暗号の分野では法制度も後押ししていますし，アメリカに追い付くのは大変です．論文に書かれる技術そのもののレベルでは，日本はアメリカに全然負けてないどころか，それ以上の分野も沢山あると思います．しかし実用的なレベルに落とし込んで標準化して世の中に広げていくということに関しては，アメリカは国を挙げてやっているわけだから，日本にとっては厳しい戦いですね．

最近は中国パワーもスゴいです．国際会議では中国国内から非常に沢山の論文が投稿されます．平均的なクオリティも以前に比べると確実に上がってきています．私は，今の中国では，20 年前の日本と，10 年前の韓国と同じことが起きているんだと思っています．あと 10 年もすれば日本はもう中国に手も足も出なくなるんじゃないかと心配ですね．良くも悪くも日本は豊かになり，アグレッシブさが無くなりました．

DP：草食化ですね．中国や韓国に追い付かれる前に，日本もアメリカみたいになれば解決できるんでしょうか．

松井：暗号だけの話ではなくて，日本の技術全体を上げることを考えなくてはならないでしょうね．

DP：もっと時間をいただいてお話を聞かせていただきたい所ですが残念ながら尽きてしまいました．今日は貴重なお話をどうもありがとうございました．