

日本の暗号技術の国際標準化への取り組みと社会への普及

近澤 武（独立行政法人情報処理推進機構） 松井 充（三菱電機（株））

概要 筆者らは1999年に第3世代携帯電話の標準化組織3GPP(3rd Generation Partnership Project)で国産暗号アルゴリズムを技術提案し、日本の暗号技術を初めて唯一のデファクト標準とすることに成功した。その後、ISO/IECにおいても、複数の国産暗号アルゴリズムをデジュール標準としてISO/IEC 18033 “Encryption algorithms”に掲載するに至った。本稿では、これらの取り組みを紹介すると共に、標準化された国産暗号技術が社会でどのように使用されているかについて述べる。

1. はじめに

1990年代の日本の暗号研究はレベルが高かったにもかかわらず、デファクト標準、デジュール標準のいずれにおいても、世界で活用された日本の暗号技術はほとんど無かった。筆者らは1999年に第3世代携帯電話の標準化組織3GPP(3rd Generation Partnership Project)¹⁾で暗号アルゴリズムを提案し、日本の暗号技術を初めて唯一のデファクト標準*とすることに成功した。その後、ISO/IECにおいても、複数の国産暗号アルゴリズムをデジュール標準として、ISO/IEC 18033 “Encryption algorithms”に掲載するに至った。

筆者の近澤は現在、独立行政法人情報処理推進機構で暗号技術の国際標準化活動を行っている。もう一人の筆者である松井と共に三菱電機での活動を振り返り、これら両者への取り組みを紹介する。合わせて、標準化された国産暗号技術が社会でどのように使用されているかについて述べる。

2. 携帯電話 3GPP の国際標準化での取り組み

本章では、国際標準化の第一の取り組みとして、デファクト標準である3GPPでの国際標準化の取り組みを振り返って、提案のきっかけ、提案活動、暗号アルゴリズムKASUMIの開発について紹介する。

2.1 暗号アルゴリズムの提案のきっかけ

1990年代後半、日本独自で第3世代携帯電話の技術検討が始まった。1998年に入ると、電波産業会(ARIB)²⁾では第3世代携帯電話のセキュリティについての検討会も

開催されるようになり、近澤が主査を務め、セキュリティ要件をまとめていた。

当時、世界的にも第3世代携帯電話の国際標準を策定しようという機運が高まったため、1998年12月に3GPPが設立された。3GPPは、欧州のETSI³⁾を始め、日本のARIBと情報通信技術委員会(TTC)⁴⁾、米国、韓国、後に中国の標準化団体が参加するプロジェクトである。翌1999年2月には、3GPPのサービスおよびシステムの仕様を検討するTSG-SA(Technical Specification Group – Service and System Aspects)のセキュリティワーキンググループTSG-SA WG3の第1回ロンドン会合が開催されることになった。このロンドン会合では、エディタの指名を含めて、どのようなセキュリティ関連規格を作成するべきかを検討するのが主な議題であった。

ロンドン会合の参加者は約20名で、その多くは欧州からの参加者で占められており、アジアからの参加者は、ARIBでまとめられたセキュリティ要件を紹介するために参加した近澤のみであった。

会合は第1回ということもあり、ワーキンググループの検討範囲、第3世代携帯電話におけるセキュリティの基本的考え方などのプレゼンテーションと共に、ARIBで検討を進めてきたセキュリティ要件の紹介から始まった。その後、議長から表1に示す第3世代携帯電話の規格群のタイトル案が示され、エディタを決めることとなった。

概ねどの規格もエディタがすんなり決まっていたが、「暗号アルゴリズム要件」の規格についてだけは、議長から近澤にエディタをお願いしたいという依頼が、その場であった。依頼の背景には、おそらくプレゼンテーションの内容が「暗号アルゴリズム要件」とマッチしたのに加え、エディタを欧州人だけで固めてしまうのはよく

* 「フォーラム標準」に分類する専門家もいるが、デジュール標準ではないということから、本稿ではあえてデファクト標準と呼ぶことにする。

表1 3GPP セキュリティ関連の規格群 (1999 年当時)

規格タイトル
目的と原則
脅威と要件
セキュリティアーキテクチャ
セキュリティ実装要件
暗号アルゴリズム要件
合法的傍受
3G セキュリティガイド

ないとの議長判断があったように思う。結局、雰囲気
に吞まれ、エディタを引き受けてしまったが、後にこれ
が暗号アルゴリズム提案のきっかけとなった。

帰国後、規格のドラフトを作り、第2回会合に臨んだ。
ところが、3GPP の流儀 (3GPP は ETSI を母体に作られ
ているため、規格も ETSI の規格体系を踏襲している。
このため、ETSI の流儀とも言える。) に則っていなかつ
たということもあり、規格の構成など根本的な事項から
して全くダメで、多くのコメントが各参加者から出され、
かなりの修正作業が必要となった。これを見かねた議長
が近澤にアドバイス役を一人付けてくれた。

2.2 提案活動

会合で出されたコメントを基に修正を進めたが、それ
をアドバイス役を送ると、原形をほとんど留めていない
程修正されて送り返されてきた。その修正文案を見たとき、
自分の力なさに少々落胆してしまった。この繰り返
しの中で、ふと、修正文案のあるページに目が留まった。
技術者の直感である。内容は、暗号アルゴリズムに要求
される性能についての次の記述である。

- 暗号化処理速度は 2Mbps 以上であること
- 暗号化処理回路は 10 キロゲート以下であること

これらの数値は、エディタである近澤が特定の暗号アル
ゴリズムを意識して決めたものではなく、会合で合意
されたものである。ワーキンググループでは、第2世代
携帯電話は音声や SMS (ショートメッセージサービス)
を中心とした使い方であるが、第3世代携帯電話になる
とコミュニケーション手段にマルチメディアデータが加
わることを想定し、暗号化処理速度を 2Mbps 以上と設定
した。また、第2世代携帯電話の暗号化処理回路は数キ
ロゲートであったが、第3世代携帯電話には高度な暗号
アルゴリズムを実装すべきということで、暗号化処理回

路を 10 キロゲート以下と設定した。当時の暗号技術を踏
まえると、これら両者の性能を満たすことは高い要求度
であったが、身近にこれらの要件を満たす暗号アルゴリ
ズムがあることを直感したのであった。三菱電機の暗号
アルゴリズム MISTY1⁵⁾である。MISTY1 は、差分攻撃や
線形攻撃に対して数学的に安全性を証明できており、暗
号化処理回路の規模も 6 キロゲートで実現できる特長を
持っている。しかも無償で利用できる。

近澤は、早速、上記特長を記した MISTY1 の提案文書
を作成し、暗号アルゴリズム要件の規格案と共に、第3
回会合に持参した。アドバイス役に修正してもらった規
格案は、大きな問題も無く片付いた。一方、MISTY1 の
提案文書については紹介できたものの、具体的議論には
至らなかった。

実は、暗号アルゴリズムそのものについては、ETSI
での慣習により、ETSI 傘下の暗号アルゴリズムの専門家
グループ SAGE (Security Algorithms Group of Experts) で設
計することになっていたからである。しかしながら、開
発期間が半年ということもあり、既存の暗号アルゴリ
ズムをベースにカスタマイズすることが決まっていたので、
近澤は、SAGE に対して MISTY1 を紹介する文書を入力
しつつ、MISTY1 は 3GPP の暗号アルゴリズムのベース
に最適であり、採用すべきという目的を持った提案とし
た。3GPP と SAGE はリエゾンのような形を取っていた
が、3GPP からは SAGE での議論は、リエゾン文書以外
に知ることができない。このため、提案文書が本当に
SAGE に届いたのかどうか、また届いたとしても、SAGE
の中で MISTY1 に関して議論されたかどうか全く分か
らなかった。

暫くして、SAGE から近澤にメールが届いた。MISTY1
のライセンスに関する確認である。無償と返信。その後、
SAGE からの連絡は途絶えた。

今回の MISTY1 の提案もダメだったと諦めかけていた
頃、1999 年 8 月の TSG-SA WG3 第5回会合で、第3世
代携帯電話の暗号アルゴリズムのベースは MISTY1 に内
定したことが発表された⁶⁾。これを聞いた米国企業の参
加者が慌てて自社の暗号アルゴリズムを提案しようとし
ていたが、後の祭りといったところであった。

2.3 KASUMI の開発

SAGE は MISTY1 の設計者で、筆者の一人である松井
を招聘し、MISTY1 をベースとした第3世代携帯電話向
けの暗号アルゴリズム開発のタスクフォースを設置し、
作業を開始した。タスクフォースは、設計グループと評
価グループの2つに分けられ、松井は設計グループに入

った。

MISTY1 は 2.2 節で紹介した暗号アルゴリズムの要件にそのまま合致するのだが、携帯電話に実装するため、タスクフォースはさらなる高速化、小型化を目指した。まず、暗号化処理のオーバーヘッド時間を短縮するため、MISTY1 の鍵スケジュール部を簡素化した。次に、鍵スケジュール部を簡素化することで発生する、暗号解読がしやすくなるという課題を、暗号鍵の変更頻度を上げる仕様とすることで克服した。さらに、MISTY1 の暗号化処理部を一部簡素化することで、小型化に対する性能を向上させた。

2000 年 3 月、3GPP では SAGE から提示された新暗号アルゴリズムを承認し、第 3 世代携帯電話用暗号アルゴリズムとして、MISTY1 をベースに開発された暗号アルゴリズム KASUMI が正式に採用された。これは、日本の暗号技術が初めて唯一のデファクト標準となったことから、新聞等でも大きく取り上げられた。ちなみに、KASUMI というアルゴリズム名は、MISTY の直訳である「霧のかかった」に由来している。

2.4 携帯電話への KASUMI の普及

暗号技術はネットワーク化された社会において欠かせ

ないものになってきており、一般ユーザがその暗号技術を意識せずに使用している。2.3 節で紹介した暗号アルゴリズム KASUMI は、日本でも普及している W-CDMA (Widband Code Division Multiple Access) 方式の第 3 世代携帯電話システムで使用されている。携帯電話の基地局はもとより、一般ユーザが保有している携帯電話機一台一台にも KASUMI が実装されている。

KASUMI が適用されるのは、携帯電話機と基地局間の無線区間であり、第三者にその区間を盗聴されても、KASUMI で音声やデータが暗号化されているので、漏れる心配がない(図 1)。このように一般ユーザが特に意識せずに暗号アルゴリズム KASUMI を使っていることになる。

また、欧州やアジアを中心に使用されている GSM (Global System for Mobile communications) 方式の第 2 世代携帯電話でも、携帯電話機と基地局間の無線区間の暗号化に KASUMI が使用されている。

このように、3GPP での KASUMI の採用は、日本の暗号技術が全世界の人たちに利用されるという大きな成果につながった。もちろん、日本の技術が国際的に貢献していることをアピールできたということは言うまでもない。

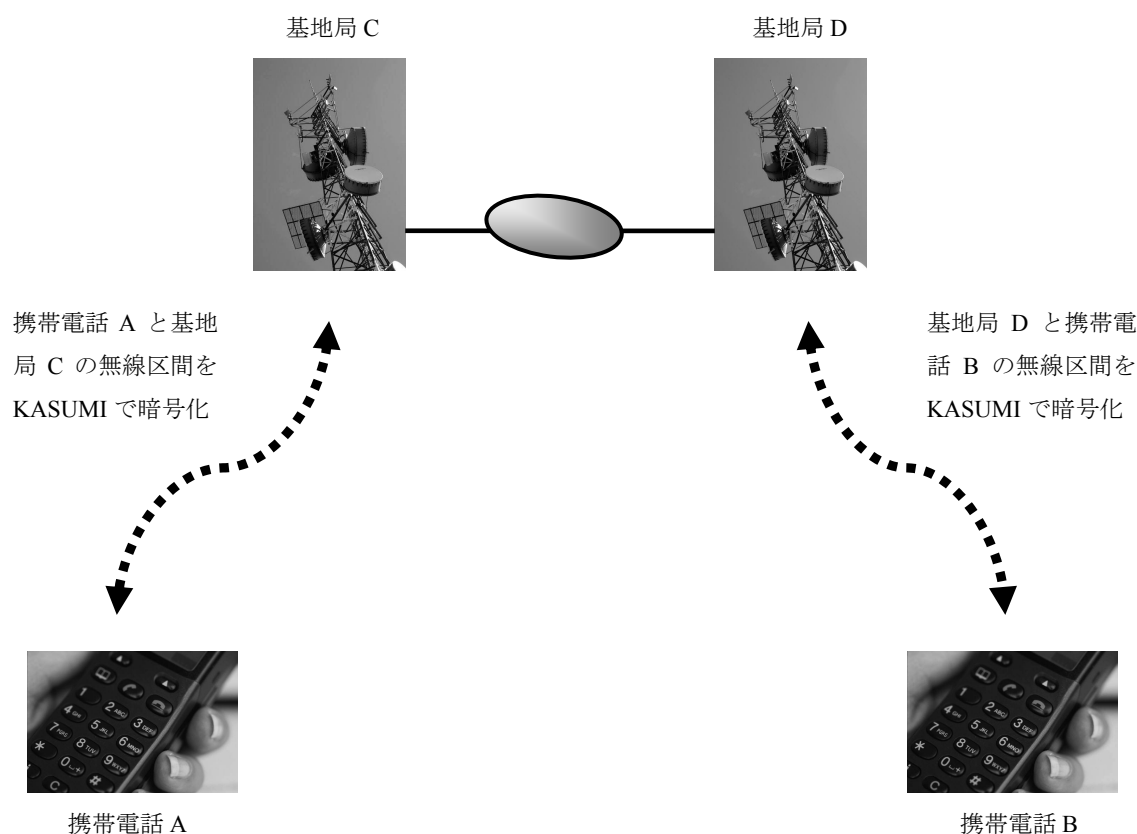


図 1 携帯電話機と基地局間の無線区間を暗号アルゴリズム KASUMI で暗号化

2.5 取り組みを振り返って

2000 年、日本の暗号技術をデファクト標準として、国際標準化することに成功した。トントン拍子で成果が出たかという、そうではない。これまで、筆者らはいくつもの国際標準化組織やコンソーシアムに暗号技術を提案してきたが、どれも却下されるばかりであった。

振り返ると、標準化作業が開始された後に、遅ればせながら参加して提案しているケースが大半であったように思う。今回は、標準化作業に最初から参画していたこと、議論の流れや各参加者の思いを把握できたことなど、自分では意識していないが、提案活動につながるチャンスを捕まえることができたと推測する。

また、過去の標準化提案の失敗経験が、今回の成功に少なからずつながったと考える。3GPP では暗号アルゴリズムを募集していたわけでもないため、何もしなければいつのまにか暗号アルゴリズムが決定され、それを知らされていたであろう。しかし、技術要件が合うと判断した時点で、募集されていないにもかかわらず、提案活動に行動を移すことができたのは、知らず知らずに標準化提案の経験値を上げていた、過去の失敗経験があったからこそである。

まさに、「失敗は成功の元」である。

「失敗は成功の元」
失敗は知らずのうち
に経験値を上げる

3. ISO/IEC での国際標準化の取り組み

本章では、国際標準化の第二の取り組みとして、デジュール標準である、ISO/IEC での国際標準化の取り組みを振り返って、国際標準化活動のきっかけ、提案活動、ISO/IEC 18033-3 ブロック暗号の策定について紹介する。

3.1 暗号アルゴリズム国際標準化のきっかけ

1980 年代、ISO/TC97/SC20 (ISO/IEC JTC1/SC27 (以下 SC27) ⁷⁾ に改組する前の前身) では、当時のデファクト標準である DES(Data Encryption Standard) ⁸⁾ のデジュール標準化を進めていた。しかし、作業途中で、提案元の米国より標準化中止の要請があり、標準化は頓挫した。標

準化された暗号アルゴリズムは攻撃的になり、安全性が脅かされると米国が考えたとも言われている。

このため、SC27 では、代替案として、暗号アルゴリズムの登録制度を開始し、書類不備がない限り、各国から暗号アルゴリズムを受け付けた。登録される暗号アルゴリズムの仕様公開は任意で、また、登録申請される暗号アルゴリズムの安全性も全く審査しないため、登録件数は増え続けた。その当時、ISO/IEC に登録された暗号であるというセールストークをする日本企業が多かったこともあり、20 を超える登録数中、日本からの登録は過半数を超えた。

1999 年、SC27 は上位組織の JTC1 の承認を得て、暗号アルゴリズム自身の標準化の解禁と、暗号アルゴリズムの国際標準化が終了した時点で、登録制度を廃止することに決定した。この背景には、米国が DES の後継となる暗号アルゴリズム AES (Advanced Encryption Standard) ⁹⁾ のオープンコンペを実施していたこと、SC27 でも暗号アルゴリズム標準化の要望が高まってきたことが挙げられる。

3.2 提案活動

SC27 は、上述の決定に沿って、2000 年の会合で、暗号アルゴリズムの規格 ISO/IEC 18033 “Encryption algorithms”を作成すること、その規格は表 2 に示す 4 つのパートから構成する方針を示した。ISO/IEC 18033 は、ISO/IEC 国際標準暗号と位置付けられるため、暗号を利用する各種 ISO/IEC 規格にとっての標準暗号となる。

表 2 ISO/IEC 18033 (暗号アルゴリズム) の規格

パート	規格タイトル
1	総論
2	非対称暗号 (公開鍵暗号)
3	ブロック暗号
4	ストリーム暗号

これを受け、日本の SC27 国内委員会では、ISO/IEC 18033 に提案する暗号アルゴリズムを募集した。

三菱電機は MISTY1 の他に、NTT と共同で開発した暗号アルゴリズム Camellia ¹⁰⁾ を保有している。MISTY1 は 64 ビットブロック暗号で、Camellia は 128 ビットブロック暗号である。三菱電機は、これまで、MISTY1 を広く使用してもらうため MISTY1 の無償利用可とすることで、3GPP でのベース暗号としての採用につなげた。さらに、MISTY1 が ISO/IEC 国際標準暗号として規格化されることになれば、利用拡大が見込まれ、国内外の暗号ならび

に情報セキュリティ業界での MISTY1 のプレゼンス向上につながると考え、MISTY1 を SC27 国内委員会に提案した。また、Camellia は、世界中でデファクト的に使われる米国の暗号アルゴリズム AES(Advanced Encryption Standard)と同じインタフェース（暗号化ブロック単位や鍵長の入出力のビット数）を持ち、AES との置き換え容易性を考慮した暗号アルゴリズムである。暗号アルゴリズムの安全性だけではなく、適用面も考慮していることから、三菱電機と NTT の共同で SC27 国内委員会に提案した。

他社からも提案があり、日本からは計 10 件の暗号アルゴリズムを ISO/IEC 18033 へ提案することになった。特に、MISTY1 および Camellia が提案されたパート 3 のブロック暗号の規格 ISO/IEC 18033-3 には各国から多くの暗号アルゴリズムが提案された（表 3）。

表 3 ISO/IEC 18033-3 へ提案された暗号アルゴリズム
(2000 年当時)

ブロック長	アルゴリズム名	提案国
64 ビット	TDEA (Triple DES)	米国
	Hierocrypt-L1	日本
	MISTY1	日本
	IDEA	スイス
	CAST-128	カナダ
	Khazad	ベルギー(2002 年)
128 ビット	AES [†]	米国
	Camellia	日本
	CIPHERUNICORN-A	日本
	Hiercrypt-3	日本
	MARS	日本
	SEED	韓国
	Xenon	韓国
	Zodiac	韓国
	RC6	スウェーデン

SC27 の会合が回を重ねる毎に暗号アルゴリズム掲載候補が減っていく中、日本の MISTY1 と Camellia が候補として残っていた。そこで、近澤は、それらの ISO/IEC 18033-3 への掲載に向け、2001 年 10 月のソウル会合に臨んだ。ところが、ブロック暗号のエディタが突然辞任したことで、ソウル会合においてブロック暗号のセッション

そのものが開催中止となってしまう雰囲気があった。今回セッションが開かれるかどうかで、規格が発行される時期が半年違ってしまう。このことから、会合に同席していた経済産業省の方と今後の対応について相談をし、日本がエディタを引き受け、MISTY1 と Camellia の標準化を推進する方針を取ることにした。そのために、まずは、ブロック暗号のセッションを開催すべく、近澤が臨時エディタに立候補し、各国コメントを処理した。さらに方針に沿って、ソウル会合中に、正式なエディタとして立候補した。

3.3 ISO/IEC 18033-3 の策定

ブロック暗号の規格のエディタへの立候補は、翌週の SC27 総会で承認されたことから、ソウルから帰国後、早速エディタ作業に取り掛かった。まず、各国から提案された暗号アルゴリズムの仕様をドラフト作成用テンプレートに取り込み、規格案を作成した。基本的には、各国から提出された技術情報をそのまま取り込む方針で進めたが、提出された暗号アルゴリズムの仕様記述がバラバラで、記述の統一感がないというコメントを踏まえ、各節の構成および用語や記号の統一の観点から非常に労力と時間をかけて技術情報を修正した。ところが、今度は提案していた国から、何故記述を変えるのだ、というクレームがあり、結局もとの記述に戻すといった二転三転があった。

規格案の作成以上に苦労したのは、掲載する暗号アルゴリズムに関する各国の意見調整であった。提案している国の多くは、自国の国内標準の暗号アルゴリズムを提案してきているので、規格に掲載したいという思いは非常に強かった。このため、提案していない国を含めて各国の意見を聞いたが、掲載すべき暗号アルゴリズムについては意見が分かれたことから、すでに掲載を合意している TDEA と AES 以外の暗号アルゴリズムについては、投票で決定することとした。投票の結果、MISTY1 と Camellia については一定の賛成票を得られ掲載が確定した。一方、カナダの暗号アルゴリズム CAST-128 と韓国の暗号アルゴリズム SEED については賛成少数であったことから再投票を行った。再投票の結果は、賛成票が僅差ながらも反対票を上回ったことから、CAST-128 と SEED も掲載が合意された。

2005 年、5 年以上の年月を費やし、ISO/IEC 18033-3 の規格が発行された。掲載された 6 つのブロック暗号のうち、2 つが国産暗号アルゴリズムである（表 4）。

[†]2000 年当時、AES は米国での候補選定コンペティション中であったことから、最終候補 5 つが提案された。翌 2001 年に最終選定が終了し、AES が決定した。

表4 ISO/IEC 18033-3 の最終的な暗号アルゴリズム
(2005 年規格発行*)

ブロック長	アルゴリズム名	提案国
64 ビット	TDEA (Triple DES)	米国
	MISTY1	日本
	CAST-128	カナダ
128 ビット	AES	米国
	Camellia	日本
	SEED	韓国

3.4 その後

MISTY1 や Camellia が ISO/IEC18033-3 の規格に掲載されたことにより、これらの暗号アルゴリズムの知名度は格段に向上した。特に、Camellia については、PKCS#11 や IETF¹¹⁾における IPsec, SSL/TLS, XML での標準暗号、ITU-T¹²⁾での NGN(Next Generation Network)用暗号など、数多くの規格に採用されるに至った¹³⁾。今後、国産暗号アルゴリズムが掲載された規格が活用され、インターネットや NGN などで使用される頻度が高まることを期待している。勿論これは、ISO/IEC における標準化活動だけではなく、CRYPTREC (Cryptography Research and Evaluation Committees)¹⁴⁾ や NESSIE (New European Schemes for Signature, Integrity and Encryption)¹⁵⁾などでの活動成果や NTT 関係者の努力もあってのことである。

また、近澤は、ブロック暗号のエディタが終了した後、約4年間の SC27/WG2 セクレタリを経て、2010 年7月には SC27/WG2 コンビーナ (国際主査) に就任した。この就任には、それまでの標準化活動が評価されたことも要因の一つではないかと考えている。

3.5 取り組みを振り返って

3GPP の活動を振り返った時と同じように、三菱電機時代の標準化活動を振り返ってみると、ISO/IEC の標準化活動は 3GPP の標準化活動とは非常に異なる、というのが第一印象である。

決定的な違いは、ISO/IEC の標準化活動は、技術論のみでは通用しないということである。各国との協調や妥協、事前の根回しも必要で、技術論ばかりで対応していると事態は進まなくなることもしばしばであった。3.3 節の後半にも記述したが、掲載に対して賛成の少ない暗号アルゴリズムについては、掲載から外したいと思って

も、提案国はしつこく掲載の妥当性を主張してくるので、標準化作業が停滞してしまうようなことがある。自分たちの提案した技術をデジュール標準として早期に完結させることを優先しなければならない場合、掲載に対して賛成の少ない暗号アルゴリズムでも掲載を受け入れるというような妥協も一つの戦略と考える。また、今回のケースではないが、「うちの国の XXX をサポートしてくれれば、他の規格で検討されている、お前の国の△△△をサポートするぞ」といった働きかけも少なからずある。

各国との協調や

根回しも必要

妥協も一つの戦略

最後に、自分の提案を推し進めたい時には、自らエディタとなって作業することをお勧めする。エディタ作業は大変であるが、標準化活動の全体の流れを見通せること、いろいろと融通が利くことから、とても良い戦略の一つであると思う。例えば、通常何も意図しなければ暗号アルゴリズムの順番というのはアルファベット順となるのが一般的である。今回、デファクト標準の TDEA の次に MISTY1 を、AES の次に Camellia を掲載した。特に、MISTY1 については、知名度のあった CAST-128 よりアピールでき、利用してもらえる機会が増えることを期待したからである。なお、デジュール標準は、規格になったからといって必ずしも利用してもらえるとは限らないので、規格化された後が普及に向けた標準化活動の本当の始まりであることを忘れないでほしい。

4. おわりに

国際標準化として、デファクト標準である 3GPP とデジュール標準である ISO/IEC における標準化活動の取り組みを紹介した。また、標準化された国産の暗号アルゴリズムが社会でどのように使われているかにも触れた。

若干筆者らの回想録的な内容になったかもしれないが、筆者らの国際標準化活動で得られたヒントが、現在国際標準化に携わっている、あるいは将来携わる方々に少しでもお役に立てれば幸いである。

謝辞 3.2 節の執筆にあたり、ご協力いただいたソニー(株)の盛合志帆氏に感謝いたします。

* 2010 年に ISO/IEC 18033-3 の第2版が出版され、表4の暗号アルゴリズムに加えて、韓国の 64 ビットブロック暗号 HIGHT が追加されている。

参考文献

- 1) 3GPP, <http://www.3gpp.org>
- 2) ARIB, <http://www.arib.or.jp>
- 3) ETSI, <http://www.etsi.org>
- 4) TTC, <http://www.ttc.or.jp>
- 5) 松井, ブロック暗号アルゴリズム MISTY, 信学技報 ISEC1996(167), 35-48, 1996
- 6) Tech Tale 暗号アルゴリズム「MISTY」の開発(最終回) たった一つの疑問から, 日経エレクトロニクス 2002 年 8 月 12 日号(2002).
<http://techon.nikkeibp.co.jp/article/FEATURE/20100114/179239/>
<http://techon.nikkeibp.co.jp/article/FEATURE/20100114/179249/>
- 7) ISO/IEC JTC1/SC27,
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27>
- 8) NIST FIPS SP800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (2008)
- 9) NIST FIPS 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES) (2001)
- 10) 青木, 市川, 神田, 松井, 盛合, 中嶋, 時田, 128 ビット ブロック暗号 Camellia, 信学技報 ISEC2000-6, 2000
- 11) IETF, <http://www.ietf.org>
- 12) ITU-T, <http://www.itu.int/ITU-T>
- 13) NTT: Camellia, <http://info.isl.ntt.co.jp/crypt/camellia/index.html>
- 14) CRYPTREC, <http://www.cryptrec.go.jp>
- 15) NESSIE, <http://www.cryptonessie.org>

投稿受付: 2011 年 6 月 16 日

採録決定: 2011 年 7 月 26 日

編集担当: 寺田真敏 (日立製作所)

近澤 武 (正会員)

E-mail: t-chika@ipa.go.jp

筑波大・第三・情報卒の後, 三菱電機(株)入社。以来, 情報セキュリティの研究開発に従事。2006 年より独立行政法人情報処理推進機構に出向。現在, 同機構技術本部セキュリティセンター暗号グループリーダー。ISO/IEC JTC1/SC27/WG2 コンビーナ(国際主査)および CRYPTREC 暗号技術検討会構成員。2010 年情報処理学会情報規格調査会国際標準化功績賞受賞。共著書「情報セキュリティハンドブック」(オーム社)など。

松井 充 (正会員)

E-mail: Matsui.Mitsuru@ab.MitsubishiElectric.co.jp

京大・理・数学卒, 同大学修士・数学専攻修了の後, 三菱電機(株)入社。以来, 暗号技術ならびに情報セキュリティ技術の研究開発に従事。現在, 同社情報技術総合研究所情報セキュリティ技術部長。CRYPTREC 暗号技術検討会構成員。2003 年新技術開発財団市村産業賞本賞, 同年発明協会全国発明表彰恩賜発明賞各受賞。電子情報通信学会, IACR 各会員。情報理工学博士(東京大学)。