標準化動向

近澤　武*

要　旨

前稿で紹介があったように，三菱電機は“MISTY１”と“Camellia”の暗号アルゴリズムを保有している。当社は，その両者を様々な標準化に提案し，高い技術レベルを示している。

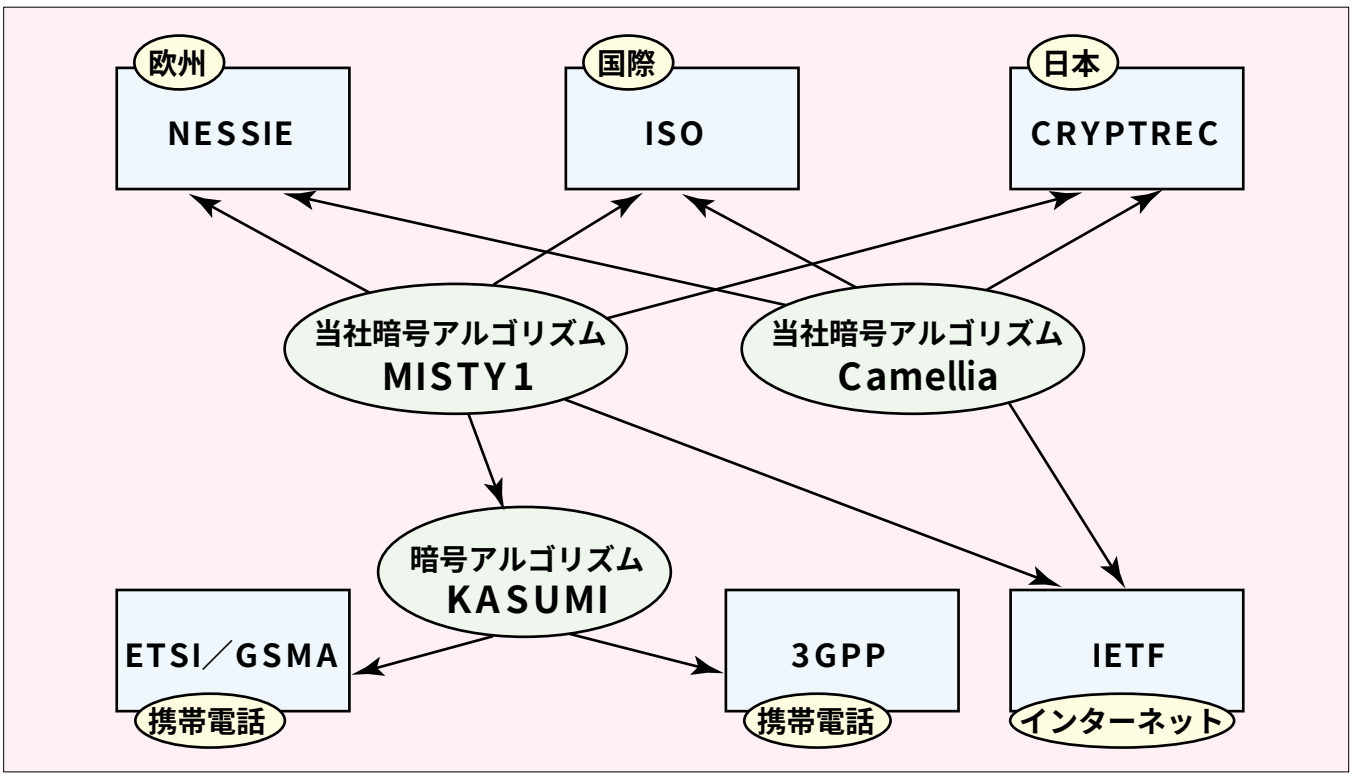
ISO（国際標準化機構）は，最近，暗号アルゴリズムの標準化を開始し，MISTY１，Camellia共に有力候補となっている。

第三世代の携帯電話の標準化を行っている３GPPにおいては，端末と基地局の無線区間の秘匿とデータ認証を行うために，“KASUMI”という暗号アルゴリズムが開発された。KASUMIは当社のMISTY１をベースに移動通信用にカスタマイズしたもので，日本発の暗号アルゴリズムをベースにしたものが唯一の国際標準になったのは日本の暗号史上初めてであり，画期的なことである。欧州の現行方式にもKASUMIをコアとする暗号が使用できるよう，欧州の標準化組織ETSIとGSM関係者の集まりのGSMAと共同で開発中である。

欧州のセキュリティプロジェクトNESSIEは，欧州産業界のための暗号部品推奨リストを作る目的で，2000年に開始された。暗号部品の候補は公募によって集められ，２段階の評価を行って最終リストを完成させることになっている。現在，第一次選考結果が発表され，ブロック暗号のカテゴリーにおいては，日本の他社からの提案アルゴリズムが落選するのに対し，MISTY１，Camellia共に合格している。

日本の電子政府のために設立されたプロジェクトCRYPTRECは，電子政府で適用可能な暗号アルゴリズムのリストを作成することを目的としている。2001年の詳細評価結果では，MISTY１，Camellia共に，安全性及び性能に関し，最高の評価を得ている。

インターネット関連技術の標準化を行っているIETFにはセキュリティに関するWGがあり，MISTY１，Camellia共にTLS WGでTLSのCipher Suiteとして提案されている。なお，MISTY１はRFC2994で参照できる。



当社の暗号アルゴリズムと標準化

当社の暗号アルゴリズムMISTY１とCamelliaは，ISO，３GPP，NESSIE，CRYPTREC，IETFなどに提案され，一部は規格化され始めている。当社の暗号アルゴリズムは高い技術レベルにあり，日本のみならず，世界に誇れる技術と言っても過言ではない。

*情報技術総合研究所