名称：「その暗号変換により特に情報漏洩観測攻撃から保護される暗号回路」事件
審決取消請求事件
知的財産高等裁判所：平成２９（行ケ）第１００５１号　判決日：平成３０年４月１２日
判決：請求棄却
特許法３６条４項１号
キーワード：実施可能要件
判決文：http://www.courts.go.jp/app/files/hanrei_jp/676/087676_hanrei.pdf

［概要］
　本願発明の技術的要求を満たす関数Ｇを構成する計算方法が、当業者の技術常識に鑑みて自明であると認めるに足りる証拠はないとして、実施可能要件に違反するとした審決には誤りはないと判断された事例。

［事件の経緯］
（１）平成２２年１月１８日（パリ条約による優先権主張外国庁受理２００９年１月２０日仏国）に特許出願された。
（２）平成２６年１月１５日付けで拒絶理由が通知されたことから、原告は、同年５月２日に手続補正書等を提出したが、同年９月４日付けで拒絶査定がされた。
（３）原告は、同年１２月２６日、特許庁に対し、拒絶査定不服審判を請求した。これに対し、特許庁は、当該審判請求を不服２０１４－２６７９２号事件として審理をし、原告に対し、平成２７年９月１７日付けで拒絶理由を通知した。これを受け、原告は、平成２８年３月２５日、特許請求の範囲の変更を内容とする別紙手続補正書を提出したが、特許庁は、同年１０月１３日、「本件審判の請求は、成り立たない。」との審決をした。
（４）原告は、審決を不服として、知財高裁に訴えを提起したが、知財高裁は、原告の請求を棄却した。

［本件発明］
【請求項１】
暗号化アルゴリズムを実行するための関数鍵ｋｃを含む暗号回路（２１）であって、前記回路は、前記回路に専用の第２の鍵ｋｉであって、前記回路のサイドチャネルを利用した攻撃から回路を保護することを可能とする第２の鍵ｋｉを含むことを特徴とする回路であって、前記関数鍵ｋｃはＸＯＲ演算によって前記２つの鍵を組み合わせることにより前記第２の鍵ｋｉによってマスクされ、入力変数ｘはマスク鍵
【数１】
$$k_c \oplus k_i$$
によって暗号化され、
前記暗号回路は、ＦＰＧＡタイプのプログラマブル回路において実現され、
前記暗号回路は、前記ＦＰＧＡタイプのプログラマブル回路のプログラミングファイル（２５）を暗号化するための第３の鍵ｋｂを含み、前記第２の鍵ｋｉはＰＵＦ（Ｐｈｙｓｉｃａｌｌｙ Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ）により生成されることを特徴とする回路。

［取消事由］
（１）本願発明１の認定の誤り
（２）本願発明１と引用発明との一致点及び相違点の認定の誤り
（３）容易想到性に関する認定の誤り
（４）実施可能要件に関する認定の誤り

（５）明確性要件に関する認定の誤り
※裁判所は、取消事由５のみ判断している。

［裁判所の判断］（筆者にて適宜抜粋）
『　・・・(略)・・・。すなわち、本願発明は、秘密情報である関数鍵ｋｃを用いて平文ｘから暗号文ｙを計算する関数をＦで表したとき、ｙ＝Ｆ（ｘ，ｋｃ）を満たす暗号文ｙを出力する暗号回路であると認められる（以下、この技術思想を「本願技術思想①」という。）。
　・・・(略)・・・。
　このような、単体の関数鍵ｋｃを直接用いずマスク鍵のみを用いることにより平文ｘから暗号文ｙを計算する関数をＧで表すと、本願発明の暗号回路は、暗号文ｙの実際の計算をｙ＝Ｇ（ｘ，ｋｃ⊕ｋｉ）によって計算するものであると認められる（以下、この技術思想を「本願技術思想②」という。）。
イ（ア）　上記本願技術思想①及び②によれば、本願発明の暗号回路を具現化するためには、暗号回路によって実際に計算された暗号文と、暗号化アルゴリズムＦに基づいて計算された暗号文とが等しいこと、すなわち
　Ｇ（ｘ，ｋｃ⊕ｋｉ）＝Ｆ（ｘ，ｋｃ）
を満たすことが要求される（以下、この要求を「本願発明の技術的要求」という。）。
　しかし、本願発明の技術的要求を満たす関数Ｇを構成する計算方法が、当業者の技術常識に鑑みて自明であると認めるに足りる証拠はない。・・・(略)・・・。
ｃ　以上のとおり、本願明細書等の図１及び２に示される回路においては、そもそもマスク鍵ｋｃ⊕ｋｉが計算されているとは認められないことから、両図の回路をもって関数Ｇ（ｘ，ｋｃ⊕ｋｉ）の具体的態様を開示したものということはできない。
ｄ　また、段落【００２８】記載の「【数２】K⊕M」は、２つの値がＸＯＲ演算されているという点で本願発明のマスク鍵と共通するものの、記号が異なることから、本願発明を説明したものとは認められない。
　仮に当該記載が本願発明を説明したものだとすると、当該記載の「秘密鍵K」は保護対象となる鍵であるから、その機能の面から本願発明の関数鍵ｋｃに該当すると解されるが、【数２】と式（A）とを比較すると、M＝Ｅ（ＲＨ（ＩＰ（ｋｉ）））であると推測されるところ、Ｅ（ＲＨ（ＩＰ（ｋｉ）））は明らかに第２の鍵ｋｉそのものとは異なる値である。したがって、当該記載は、本願発明と整合せず、やはり本願発明を説明するものということはできない。
ｅ　図１及び２に関する本願明細書等のその他の記載にも、関数Ｇの具体的態様を開示したものと見られる記載はない。
　したがって、本願明細書【００２５】～【００３６】並びに図１及び２には、関数Ｇの具体的態様が記載されているとはいえない。
（エ）　本願明細書等の記載のうち、図３及びこれに関連する段落【００３７】～【００３９】には、本願発明の関数鍵ｋｃに対応する概念が記載されていない。そうである以上、これらの記載及び図に関数Ｇ（ｘ，ｋｃ⊕ｋｉ）の具体的態様が記載されているとはいえない。
　なお、図３は図１及び２においてＦｅｉｓｔｅｌ関数ｆを示す囲みと一見類似するようにみえるけれども、図１及び２と図３にそれぞれ現れる要素の異同ないし対応関係は不明というほかなく、また、図１及び２に関する説明（【００２５】～【００３６】）に続いて「図３は別の進行方式を示す。」（【００３７】）と記載されていることに鑑みると、図１及び２と図３との間には技術的関連性はなく、相互に独立したものと見るのが相当である。このため、図１～３を総合的に見ても、関数Ｇの具体的態様は明らかでない。
ウ　以上より、本願明細書等には関数Ｇの具体的態様が記載されていないというべきである。そうである以上、本願発明を具現化して実施することはできない。
　したがって、本願明細書等の発明の詳細な説明の記載は、本願発明の属する技術の分野における通常の知識を有する者がその実施をすることができる程度に明確かつ十分に記載したも

のということはできないから、法３６条４項１号に違反する。これと同旨をいう本件審決に誤りはない。』

［コメント］

本件出願の対応ＥＰ出願ではほぼ同様の内容で登録されている。実施可能要件に関して、日本の特許法第３６条４項１号は「その発明の属する技術の分野における通常の知識を有する者がその実施をすることができる程度に明確かつ十分に、記載したものであること。」と規定され、ＥＰＣ８３条は「欧州特許出願は、当該技術の熟練者が実施することができる程度に明確かつ十分に、発明を開示しなければならない。」と規定されている。

また、日本の審査基準では「明細書及び図面に記載された発明の実施についての教示と出願時の技術常識とに基づいて、当業者が発明を実施しようとした場合に、どのように実施するかが理解できないとき（例えば、どのように実施するかを発見するために、当業者に期待しうる程度を超える試行錯誤や複雑高度な実験等を行う必要があるとき）には、当業者が実施することができる程度に発明の詳細な説明が記載されていないこととなる。」と記載されている。一方、ＥＰＣ審査便覧では「明細書には、発明の実施に不可欠な特徴について、当該技術の熟練者にとってその発明を実施する方法を明白にする程度まで十分に詳しく開示しなければならない。（中略）たとえば、非常に広範な分野であっても限られた数の実施例、又は唯一の実施例のみで十分に例示される場合もある。後者の場合に出願は、実施例の他、当該技術の熟練者が共通の一般的知識を用いて、不当な負担又は革新的な技術を必要とせずに、発明を実施することができる程度まで十分な情報を含まなければならない」と記載されている。

両者は同等の基準であると思われるが、実施可能要件違反か否かは審査官個々の判断で大きく左右されるものと思われる。本件出願の場合は、請求項で特定された構成が、具体的実施形態で特定された構成から導けないものであったことが問題であったと思われる。

明細書作成において、特許請求の範囲に係る構成要素と、具体的実施形態に記載された構成要素とは常に対応したものとすることは基本である。

以上

（担当弁理士：丹野　寿典）