認証技術特許における保護適格性判断
～Alice 判断ステップ 2 はどのように適用されるか～
米国特許判例紹介(156)

2022 年 4 月 8 日

執筆者　河野特許事務所
所長弁理士　河野 英仁

COSMOKEY SOLUTIONS GMBH & CO. KG,
Plaintiff-Appellant
v.
DUO SECURITY LLC, FKA DUO SECURITY, INC.,
Defendant-Appellee

１．概要

保護適格性に関し、米国特許法第 101 条は以下の通り規定している。

「新規かつ有用な方法，機械，製造物若しくは組成物，又はそれについての新規かつ有用な改良を発明又は発見した者は，本法の定める条件及び要件に従って，それについての特許を取得することができる。」

最高裁判所は、Alice 事件[1]において米国特許法第 101 条に関し、2 段階のテストを確立した。まず、ステップ 1 とそして抽象的なアイデア等、問題となっているクレームが保護適格性のないアイデアを対象としているか否かを判断する。その場合、ステップ 2 に進み、各クレームの要素を個別に、順序付けられた組み合わせとして検討し、追加の要素がクレームの性質を保護適格性ある出願に変換するか否かを判断する。

本事件では認証技術に関する保護適格性について、ステップ 2 の適用が争点となり、CAFC は、保護適格性なしとした地方裁判所の判決を取り消した。

２．背景

(1)特許の内容

CosmoKey Solutions 社は、認証方法と称する米国特許法第 9,246,903 号(以下、903 特許という)を所有している。903 特許は、2012 年 10 月 30 日に USPTO に出願され、2016 年 1 月 26 日に登録された。

903 特許は、複雑さが低く、セキュリティが高い認証方法を提供することを目的としている。要約では、ユーザのモバイルデバイスで認証機能をアクティブ化することを含め、端末でトランザクションを実行するユーザの ID を認証する方法について説明して

[1] *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014)

いる。

明細書は、ユーザがインターネットなどの通信チャネルを介してリモートトランザクションパートナー（例えば銀行、店舗またはセキュアなデータベース）と通信する場合、「許可されたユーザとして自分自身を識別する個人が実際に本人であることを保証することが重要である」と記載している。明細書では、ユーザの携帯電話に関連するいくつかの従来の認証方法について説明している。

明細書は先行技術に関し以下の通り開示している。認証のためにユーザのモバイルデバイスを使用することにより、従来技術は、「モバイルデバイス、例えば、携帯電話を有する人が、取引が要求された端末の場所に実際に存在する」ことを確認する。したがって、ユーザが自分のモバイルデバイスを制御している限り、認証方法は、第三者がこのユーザの識別データを偽造して、ユーザの代わりにトランザクションを実行できないことを保証する。

明細書は、これらの従来の携帯電話認証方法を改善することを意図しており、本発明によれば、「認証機能は通常非アクティブであり、トランザクションに対して予備的にのみユーザによってアクティブ化され、第２の通信チャネルからの前記応答は、認証がアクティブであるという情報を含み、認証機能は自動的に非アクティブ化される。」

明細書では、本発明の利点を以下の通り説明している。この方法では、認証機能に必要なのは、認証デバイスがこの機能がアクティブであるか否かを検出できるようにすることだけであり、認証目的でユーザに必要なアクティビティは、適切なタイミングで認証機能をアクティブにすることだけであるから、認証機能の複雑さを大幅に減らすことができる。ユーザ識別情報の送信後、特定の（好ましくは短い）時間枠内に認証機能がアクティブ化されるという、所定の時間関係がある。

明細書はまた、この方法によって提供される強化されたセキュリティを主張している。認証機能は通常非アクティブであるため、第三者が取引を開始するために不正に自分をユーザとして識別した場合、認証はほぼ確実に失敗する。その場合、認証は、真のユーザが適切なタイミングでモバイルデバイスの認証機能をアクティブ化するという非常にまれなイベントでのみ成功する。このようなまれなケースでも、不正が検出される可能性がある。したがって、複雑さが低いにもかかわらず、本発明による方法は、高レベルのセキュリティを提供する。

したがって、本明細書は、クレーム発明が、取り扱いが容易であり、複雑度の低いモ

バイルデバイスで実行できる認証方法を提供することを説明している。明細書は、「モバイルデバイスが情報をキャプチャまたは出力するための特定のハードウェアを必要としないことは、本発明の特別な利点である」と詳述している。

明細書によれば、モバイルデバイスは、一定期間アクティブ化され、ユーザの識別データにリンクされたアドレスを有するモバイルネットワークに接続することができれば十分である。次に、認証デバイスは、「アドレスが関連付けられたモバイルデバイスの認証機能がアクティブであるかどうかをチェックできる」必要がある。

ユーザが複数の通信チャネルを使用して複数の認証要素を入力することを要求する代わりに、ユーザの身元は、第１の通信チャネルを介してユーザ ID を送信し、第２の通信チャネルを介してユーザのモバイルデバイスで認証機能がアクティブ化されていることをチェックすることによって検証される。有効な認証機能をチェックすると、ユーザによる認証要素の情報の手動入力に置き換えられる。たとえば、ユーザは、モバイルデバイスをアクティブ化するか、モバイルデバイス上のアプリケーションをアクティブ化することにより、認証機能をアクティブ化できる。

争点となった 903 特許のクレーム１は以下のとおりである。

端末でのトランザクションに対してユーザを認証する方法において、

第１の通信チャネルを介して端末からトランザクションパートナーにユーザ ID を送信し、

認証デバイスが、ユーザのモバイルデバイスに実装されている認証機能をチェックするために第２の通信チャネルを使用する認証ステップを提供し、

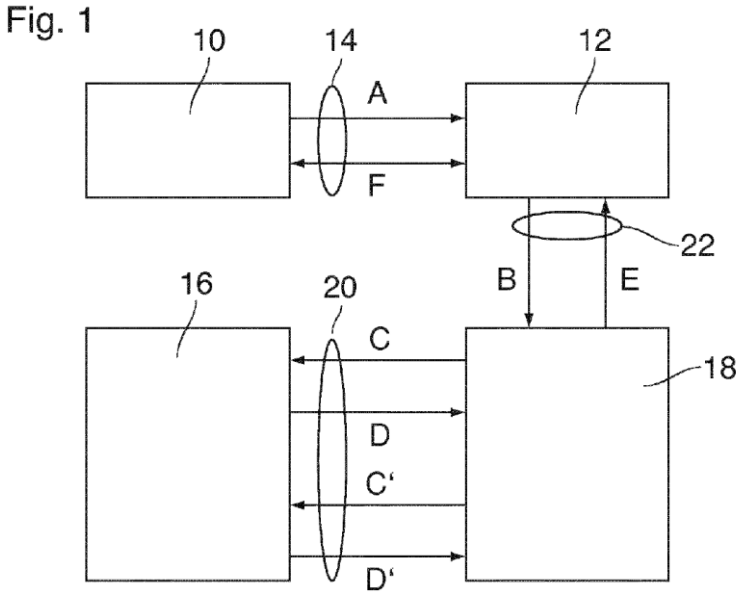
トランザクションへの認証を許可するか拒否するかを決定するための基準として、認証デバイスに、ユーザ識別情報の送信と第２の通信チャネルからの応答との間に所定の時間関係が存在するかどうかをチェックさせ、

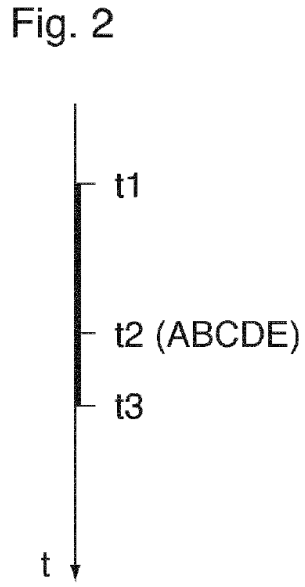
認証機能が通常は非アクティブであり、トランザクションのためにユーザによって事前にのみアクティブ化されていることを確認し、

第２の通信チャネルからの前記応答が、認証機能がアクティブであるという情報を含むことを確認し、

その後、認証機能が自動的に無効になっていることを確認する。

903 特許の図１及び図２を示す。





10 は端末、12 は銀行のトランザクションパートナー、18 は認証装置、16 はユーザのモバイルデバイスである。端末 10 による、A の認証開始から、D のユーザのモバイルデバイス 16 による非アクティブ化からアクティブ化への変更を経て、E の最終認証までが、所定時間内(t1-t3)に行われているか否かを判断する。

(2) 訴訟の経緯

2018 年 9 月、CosmoKey は 903 特許の侵害であるとして Duo Security, Inc.を提訴した。2019 年 10 月、Duo は、903 特許のすべてのクレームは米国特許法第 101 条の下では不適格であると主張した。主張によれば、クレームは認証の抽象的なアイデアを対象としており、保護適格性あるの発明概念に言及していない、というものである。地方裁判所は、2020 年 6 月 24 日に Duo の申し立てを認めた[2]。

特許適格性を判断するための Alice の 2 段階フレームワークのステップ 1 で、地方裁判所は Duo に同意し、903 特許のクレームは認証の抽象的なアイデア、つまり、トランザクションへのアクセスを許可するための ID の認証を対象としていることに同意した。

地方裁判所は、903 特許は、Prism 事件[3]で問題となっている特許と実質的に異なら

[2] *Money & Data Protection Lizenz GmpH & Co. KG, v. Duo Security, Inc.*, 468 F. Supp. 3d 674 (D. Del. 2020)

[3] *Prism Technologies LLC v. T-Mobile USA, Inc.,* 696 F. App’x 1014 (Fed. Cir.

ない」と判断した。Prism 事件で CAFC は、クレームは、リソースへのアクセスを制限するという抽象的なアイデアを対象とするため、無効であると判断した。

地方裁判所は、「903 特許の抽象的なプロセスと Prism の特許の類似性を考えると、ここで問題となっているクレームは、取引へのアクセスを許可するために身元を確認するという抽象的なアイデアを対象としている」と判断した。

アリスのステップ 2 で、地方裁判所は、903 特許は認証の抽象的な概念を実行するための汎用コンピュータ機能を単に教示しているだけであり、それゆえ Alice のステップ 2 を満たさないと結論付けた。

地方裁判所は、特許自体が「認証機能のアクティブ化の検出と、事前に決定された時間関係内での認証機能のユーザによるアクティブ化は、認証技術分野において、よく理解され、日常的で、以前に知られている従来の活動であった」と判断した。CosmoKey は判決を不服として CAFC に控訴した。

３．CAFC での争点

争点：クレーム発明が Alice のステップ２を満たすか否か

４．CAFC の判断

結論：発明概念(Inventive Concept)がありステップ２を満たす

米国特許法第 101 条は以下の通り規定している。

新規かつ有用な方法，機械，製造物若しくは組成物，又はそれについての新規かつ有用な改良を発明又は発見した者は，本法の定める条件及び要件に従って，それについての特許を取得することができる。

最高裁判所は、Alice 事件において米国特許法第 101 条に基づく特許適格性を審査するための 2 段階のテストを確立した。まず、抽象的なアイデアなど、問題となっているクレームが特許不適格の概念を対象としているか否かを判断する。その場合は、ステップ 2 に進み、「各クレームの要素を個別に、および「順序付けられた組み合わせとして」検討して、追加の要素が「クレームの性質を特許適格出願に変換する」か否かを判断する。

ステップ 2 は、「発明概念」の検証であり、「実際の特許が、不適格な概念自体をはる

2017)

かに超えることを保証するのに十分な要素または要素の組み合わせ」であるかを検証する。

Prism 事件では、クレームは「有形で（concrete）具体的な解決策」を対象としていないため、「リソースへのアクセスを制限する」という抽象的なアイデアを対象としていると判断された。クレームは、アクセスを制限するための従来のプロセスに、典型的な一般的なステップに言及しているにすぎず、ユーザ ID の「受信」、ユーザ ID の「認証」、ユーザの「承認」、およびユーザへの「アクセスの許可」を示している。ステップ 2 で、主張されたクレームは、抽象的なアイデアを特許適格発明に変換するには不十分で、慣習的な方法で使用される従来の汎用コンピューターコンポーネントを引用しているにすぎないと判断された。

また、Universal 事件[4]において、特許クレームは、金融取引を容易にするためにユーザの身元を確認するための複数の従来の認証技術を組み合わせるという抽象的なアイデアを対象としていると判断した。特許明細書は、生体認証、多要素認証、および認証に複数のデバイスを使用することは、全て従来の認証技術であることを開示していた。したがって、クレームは、これらの長年のよく知られた認証技術を組み合わせて、各技術だけで提供されるセキュリティの総和を超えないセキュリティ向上という予期された結果を達成することを目的としていた。ステップ 2 では、長年の従来の認証方法の組み合わせが、セキュリティを付加的に向上させるという予期された結果を奏するにすぎず、追加の技術的改善を示唆するものはなかったため、これらのクレームは発明概念（Inventive Concept）に言及していないと、判断された。

対照的に、Ancora 事件[5]では、以前のアプローチから脱却し、米国特許法第 101 条の下で適格性あるコンピュータ技術を改善する特定の検証方法を対象とするクレームを維持した。具体的には、認証構造をコンピュータメモリに保存することを対象とするクレームは、ハッキングに対するライセンス認証ソフトウェアの脆弱性に対処するコンピュータ機能の改善を対象としていると、判断された。そして、セキュリティの向上は、特定のコンピュータの課題を解決するための以前のアプローチとは異なる特定の手法によって行われる場合、非抽象的なコンピュータ機能の改善になる可能性がある、と判断された。

本事件において、CAFC はステップ 1 について議論することなく、ステップ 2 につい

---

[4] *Universal Secure Registry LLC v. Apple, Inc.*, 10 F.4th 1342 (Fed. Cir. 2021)

[5] *Ancora Technologies Inc. v. HTC America, Inc.* 908 F.3d 1343, 1347 (Fed. Cir. 2018).

て検討した。すなわち、ステップ 2 に移り、各クレームの要素を個別に、「順序付けられた組み合わせとして」検討し、追加の要素が「クレームの性質を特許適格出願に変換する」か否かを判断した。

コンピュータ実装発明では、コンピュータは「業界で以前から知られている、よく理解された日常的な従来の活動」以上のことを実行する必要がある。さらに、抽象的なアイデアを特許適格発明に変換する発明の概念は、抽象的なアイデア自体よりもはるかに超えるものでなければならず、単にコンピュータに抽象的なアイデアを実装または適用するための命令ではない[6]。

地方裁判所は、903 特許は、「認証の抽象的アイデアを実行するための汎用コンピュータ機能を単に教示しているだけであるため、ステップ 2 を満たさない」と判断した。地方裁判所は、明細書には以下を示していると認識した。従来技術の方法とクレームされた発明との違いは、903 特許の方法は、複雑性の低いモバイルデバイスで実行できるため、認証デバイス機能から必要とされるのは、この機能がアクティブであるか否かを検出することだけであるということであり、また、認証のためにユーザに必要なアクティビティは、トランザクションに適したタイミングで認証機能をアクティブにすることだけである。認証機能アクティビティのアクティブ化の検出と、事前に決定された時間関係内での認証機能のユーザによるアクティブ化は、認証技術分野で良く知られ、ルーチンで、日常的な従来のアクティビティであると判断した。

CAFC は地方裁判所の分析及び結論に同意しなかった。903 の特許クレームと明細書は、セキュリティを強化し、サードパーティによる不正アクセスを防止し、簡単に実装でき、複雑度の低いモバイルデバイスで有利に実行できる認証の特定の改善を示している。

地方裁判所の結論に反して、903 特許は、ネットワークとコンピュータのセキュリティ問題に対する技術的解決策を開示している。本発明の時点では、2 つの通信チャネルと携帯電話を使用したユーザの身元の認証は知られていたが、明細書には、最後の 4 つのクレームステップに関する地方裁判所の判断を裏付けるものは存在しない。
(1)トランザクションへの認証を許可するか拒否するかを決定するための基準として、認証デバイスに、ユーザ識別情報の送信と第 2 の通信チャネルからの応答との間に所定の時間関係が存在するかどうかをチェックさせ、
(2)認証機能が通常は非アクティブであり、トランザクションのためにユーザによって

[6] *BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir. 2016)

事前にのみアクティブ化されていることを確認し、
(3)第２の通信チャネルからの前記応答が、認証機能がアクティブであるという情報を含むことを確認し、
(4)その後、認証機能が自動的に無効になっていることを確認する。

これらの手順が日常的または従来型であったことを認めているとされる、コラム１の15行目から53行目への地方裁判所の依存は見当違いである。コラム１の30〜46行目は、3つの先行技術の参考文献を説明しているが、記載されているクレームの手順を教示するものはない。

それどころか、本明細書は、先行技術を以下の通り説明している。（１）トランザクションを確認するためのプロンプトをユーザに送信し、続いてユーザのモバイルデバイスが確認信号を送信する。(2) クレジットカードをアクティブ化および非アクティブ化するためにユーザのモバイルデバイスを使用する。(3) トランザクションが要求されたユーザの端末にトークンを送信し、続いてユーザのモバイルデバイスが画像をキャプチャし、2番目の通信チャネルを介して認証デバイスに送り返す。

文脈を読むと、地方裁判所によって引用された残りの部分は、クレームされたステップが発明者によって開発されたものであり、先行技術を認めておらず、記載された先行技術に対して特定の利点をもたらすことを明らかにしている。地方裁判所のこの一節の解釈には誤りがあった。

実際、特許明細書は、クレーム１のステップの特定のアレンジが、従来の認証方法に比べてどのように技術的改善を提供するかを説明している。具体的には、明細書はこれらのステップの独創的な性質を強調しており、「認証目的でユーザに必要なアクティビティはトランザクションに適したタイミングで認証機能をアクティブ化することだけである」ため、「認証機能の複雑さを大幅に軽減できる」ことを説明している。続けて、明細書は、従来技術および従来の多要素認証システムと比較して、903特許は、より少ないリソース、より少ないユーザ相互作用、およびより単純なデバイスでユーザ認証を実行することを説明している。

明細書自体が明らかにしているように、クレームは、地方裁判所によって特定された抽象的なアイデアを超え、より高いセキュリティをもたらす単純な方法を提供することによって先行技術を改善する特定の一連の順序付けられたステップを要求することによって、発明概念(Inventive Concept)を述べている。

５．結論

上記の理由により、CAFC は、903 特許のクレームは米国特許法第 101 条の下で不適格であるとした地方裁判所の判断を取り消した。

６．コメント

本事件ではステップ１について深く議論されることなく、ステップ２における判断が主要争点となった。コンピュータ実装発明において、汎用コンピュータに対し、どのような要素が追加されていれば、発明概念(Inventive Concept)があり、保護適格性ある発明に変換されるかを把握する上で重要な事件である。

多くのコンピュータ実装発明は、コンピュータ自体の改善は皆無で、汎用コンピュータ上に新たなソフトウェア上の工夫を追加して、発明概念を完成させるものである。ステップ２でこの追加の要素が、対象技術分野において「良く知られ、ルーチンで、日常的な従来のアクティビティ(well-understood and routine, conventional activities) 」であれば、ステップ２を満たさず、これをはるかに超えていればステップ２を満たすこととなる。

本事件ではシンプルな認証方法ではあったが、明細書に当該認証方法における利点が記載されており、ステップ２を満たすと判断された。従来の技術と比較してはるかに超える発明概念が付加されているか否かを判断するステップ２は、当業者が先行技術から容易に想到することができるか否かを判断する非自明性（米国特許法第 103 条）とも考えが近く、保護適格性を有するか否かの実務者の予見性を困難にしていると考える。

USPTO は、2022 年 1 月米国特許法第 101 条拒絶先延ばしパイロットプログラム(Deferred Subject Matter Eligibility Response (DSMER) pilot program)を導入すると発表した。本プログラムは 2022 年 2 月 1 日～7 月 30 日までの期間試験的に運用される。このプログラムでは、最初の拒絶理由に 101 条(主題の適格性)の拒絶およびその他の拒絶が含まれている場合、主題の適格性の拒絶に対する応答のみを先延ばしすることができる。

これは実務上、非自明性及び記載要件違反に対する補正及び反論をおこなっていれば、先行技術との差異も明確となり、自然と米国特許法第 101 条の拒絶理由が解消することも多いことに起因するものであり、ひとまず 101 条の議論はおいておき、先に主要な非自明性及び記載要件について議論を進め、審査の効率化を図るものである。米国特許

法第 101 条の判断の難しさから USPTO も審査の効率性を考慮して導入したものである。

判決日　2021 年 10 月 4 日

以上