ソフトウェア特許に対する権利侵害
～ソフトウェアモジュールがロックされている場合に侵害が成立するか～
米国特許判例紹介(87)

2011年1月13日

執筆者　弁理士　河野 英仁

Finjan, Inc.,
Plaintiff-Cross Appellant,
v.
Secure Computing Corporation, et al.,
Defendants Appellants.

１．概要

米国特許法第271条(a)[1]に規定する直接侵害が成立するためには、方法クレームの場合、イ号方法が方法クレームの全てのステップを実行する必要がある。また装置クレームの場合、イ号装置が装置クレームの全ての構成要件を具備する必要がある。

ここで、イ号装置が、装置クレームの一部の構成要件を用いずに実施するモードと、当該構成要件を用いて実施するモードとを、選択することができる場合に、特許権侵害が成立するか否かが問題となる。

同様に、イ号方法が、方法クレームの一部のステップを利用せずに実行するモードと、当該ステップを利用して実行するモードとを、選択することができる場合に、特許権侵害が成立するか否かも問題となる。

本事件においては、イ号装置は、クレームの構成要件であるソフトウェアモジュールを具備するが、販売時にはロックされており、ユーザが鍵を購入し、ロックを解除することによって初めてアクティベートされる。CAFCは、装置クレームに関してはソフトウェアモジュールに係るソースコード自体について何ら変更する必要がないから、ロックされていようとも、直接侵害が成立すると判断した。その一方で、方法クレームに対しては、実際の操作がなかったことから直接侵害は成立しないと判断した。

---

[1] 米国特許法第271条(a)の規定は以下のとおり。
(a) 本法に別段の定めがある場合を除き，特許の存続期間中に，権限を有することなく，特許発明を合衆国において生産，使用，販売の申出若しくは販売する者，又は特許発明を合衆国に輸入する者は特許を侵害する。

２．背景

(1)特許発明の内容

原告は、U.S. Patents No. 6,092,194(以下、194 特許という)、No. 6,804,780 (以下、780 特許という)、及び、No. 7,058,822(以下、822 特許という)の 3 つの特許権を所有している。

これらの特許はインターネットに接続されたコンピュータに対し脅威を与える未知のウィルスを検出及び駆除する事前(proactive)スキャン技術に関する。

(2)194 特許

194 特許は「悪意のあるダウンローダブルからコンピュータ及びネットワークを保護するためのシステム及び方法」である。クレーム 1[2]は以下のとおり。

1. コンピュータに基づく方法であり、以下のステップを含む：
クライアントをアドレスとして入ってくるダウンローダブルを、前記クライアントに対するゲートウェイとして機能するサーバにより受信する受信ステップと、
セキュリティポリシーが侵害されたか否かを決定するために、前記サーバにより、ダウンローダブルに付随するダウンローダブルのセキュリティプロフィールデータを前記セキュリティポリシーと比較するステップとを備え、
前記ダウンローダブルセキュリティプロフィールは、前記ダウンローダブルにより企てられた疑いあるコンピュータ操作リストを含み、
前記セキュリティポリシーが侵害された場合、前記クライアントによりダウンローダブルの実行を防止するステップとを備える。

問題となったクレームは、方法クレーム(クレーム 1-14, 24-30)、システムクレーム(クレーム 32-36)、及び、コンピュータでの読み取りが可能な記録媒体クレーム(クレーム

---

[2] 194 特許のクレーム 1

1. A computer-based method, comprising the steps of:
receiving an incoming Downloadable ad-dressed to a client, by a server that serves as a gateway to the client;
comparing, by the server, Downloadable secu-rity profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a [sic] suspi-cious computer operations that may be at-tempted by the Downloadable, against a security policy to determine if the security policy has been violated; and
preventing execution of the Downloadable by the client if the security policy has been violated.

65)である。

194 特許のシステムクレーム 32[3]は以下のとおりである。なお権利内容は方法クレーム 1 と実質的に同一である。
32.クライアントに対するゲートウェイとして機能するサーバにより実行されるシステムであり以下を含む：
セキュリティポリシーと、
クライアントをアドレスとして入ってくるダウンローダブルを受信するインターフェースと、
前記インターフェースに接続され、セキュリティポリシーが侵害されたか否かを決定するために、前記ダウンローダブルに付随するダウンローダブルセキュリティプロフィールデータを、前記セキュリティポリシーと比較する比較器とを備え、前記ダウンローダブルセキュリティプロフィールは、前記ダウンローダブルにより企てられた疑いあるコンピュータ操作リストを含み、
前記セキュリティポリシーが侵害された場合に、前記クライアントにより前記ダウンローダブルの実行を防止する論理エンジンを更に備える。

194 特許の記録媒体クレーム 65[4]は以下のとおり。なお権利内容は方法クレーム 1 と

---

[3] 194 特許のクレーム 32
32. A system for execution by a server that serves as a gateway to a client, the system comprising:
a security policy;
an interface for receiving an incoming Downloadable addressed to a client;
a comparator, coupled to the interface, for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against the security policy to determine if the security policy has been violated; and
a logical engine for preventing execution of the Downloadable by the client if the security policy has been violated.

[4] 194 特許のクレーム 65
65. A computer-readable storage medium storing program code for causing a server that serves as a gateway to a client to perform the steps of:
receiving an incoming Downloadable addressed to a client;
comparing Downloadable security profile data pertaining to the Downloadable against a security policy to determine if the security policy has been violated; and
preventing execution of the Downloadable by the client if the security policy has been

実質的に同一である。
65. プログラムコードを記憶したコンピュータでの読み取り可能な記録媒体であり、クライアントに対するゲートウェイとして機能するサーバに以下の処理を実行させる：
クライアントをアドレスとして入ってくるダウンローダブルを受信するステップと、
セキュリティポリシーが侵害されたか否かを決定するために、前記ダウンローダブルに付随するダウンローダブルセキュリティプロフィールデータを、前記セキュリティポリシーと比較するステップと、
前記セキュリティポリシーが侵害された場合に、前記クライアントにより前記ダウンローダブルの実行を防止するステップとを備える。

(3)780 特許

780 特許は 194 特許と同一の発明の名称であり、「キャッシング」、すなわち以前に遭遇したダウンローダブルファイルを特定する点を権利化している。クレーム 1[5]は以下のとおり。

1.ダウンローダブルを特定するためのダウンローダブル ID を生成するためのコンピュータに基づく方法であり以下を含む：
前記ダウンローダブルにより実行されるソフトウェアコンポーネントに対する一またはそれ以上の参照を含むダウンローダブルを取得し、
前記一またはそれ以上の参照により、少なくとも一つのソフトウェアコンポーネントをフェッチ[6]し、
ダウンローダブル ID を生成するために、前記ダウンローダブル及び前記フェッチされたソフトウェアコンポーネントについてハッシング関数を実行する。

194 特許と同様に、780 特許は方法クレーム(クレーム 1-6)、システムクレーム(クレーム 9-14)及びコンピュータでの読み取りが可能な記録媒体クレーム(クレーム 18)を含

---

violated.

[5] 780 特許のクレーム 1

1. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:

obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

fetching at least one software component identified by the one or more refer-ences; and

performing a hashing function on the Downloadable and the fetched soft-ware components to generate a Downloadable ID.

[6] フェッチ(fetch)とは、マイクロプロセッサが命令を実行する際、その最初の段階でメインメモリから命令コードを読み出すことをいう。小学館　デジタル大辞林

む。

(4)822 特許

822 特許は保護コードにより、潜在的に危険なダウンローダブルを「サンドボックス[7]」する点権利化している。参考図 1 は 822 特許の図 4 である。

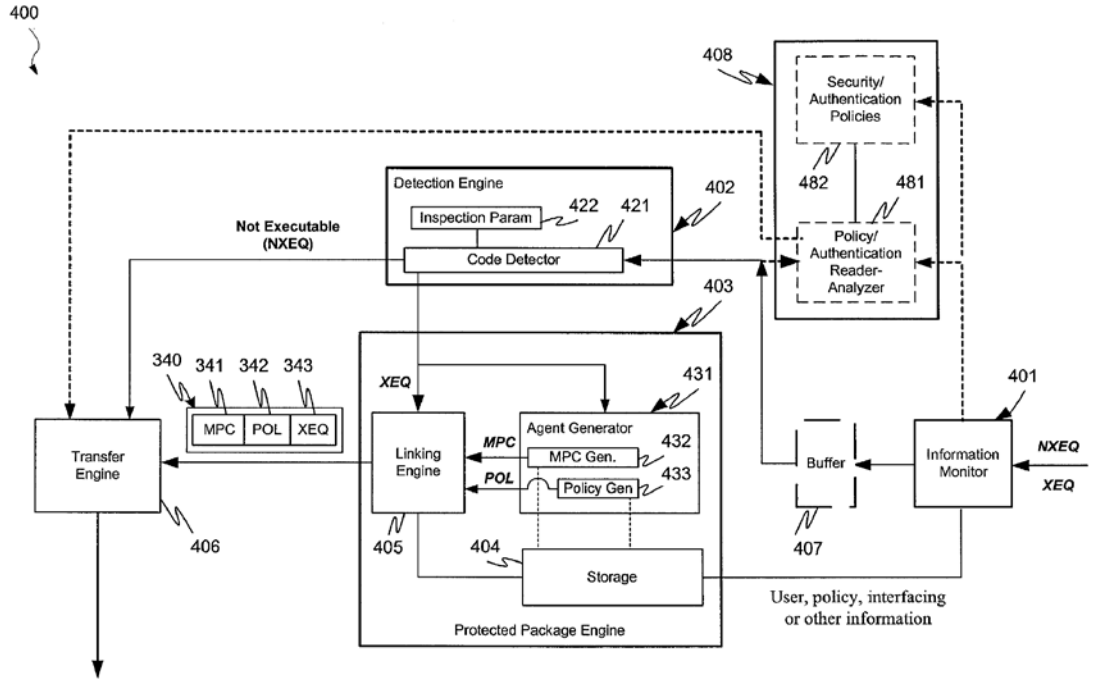

FIG. 4

参考図 1　822 特許の図 4

クレーム 4[8]は以下のとおり。

---

[7] サンドボックスとは、保護された領域内でプログラムを動作させることで、その外へ悪影響が及ぶのを防止するセキュリティモデル。このモデルでは、外部から受け取ったプログラムを保護された領域、「箱」の中に閉じ込めてから動作させる。「箱」は記憶域内の他のファイルやプロセスからは隔離され、内部から外界を操作することは禁じられている。IT 用語辞典(http://e-words.jp/)

[8] 822 特許のクレーム 4

4. A processor-based method, comprising:

receiving downloadable-information;

determining whether the downloadable-information includes executable code; and

causing mobile protection code to be com-municated to at least one information-destination of the downloadable-information, if the

4. プロセッサに基づく方法であり以下を含む：
ダウンローダブル情報を受信し、
前記ダウンローダブル情報が実行可能なコードを含むか否かを決定し、
前記ダウンローダブル情報が実行可能なコードを含むと判断した場合に、前記ダウンローダブル情報の少なくとも一つの情報宛先に、モバイル保護コードを伝達させ、
該モバイル保護コードを伝達させることは、モバイル保護コード及びダウンローダブル情報を含むサンドボックスパッケージを形成することと、サンドボックスパッケージを少なくとも一つの情報宛先へ伝達させることとを含む。

関連するクレームは「プロセッサに基づく方法」クレーム(クレーム 4,6,8)、「プロセッサに基づくシステムクレーム」(クレーム 12-13)を含む。以上のとおり、3 つの特許は全て方法クレームとそれ以外のクレームとを含む。

(5)被告の製品

被告は、以下の 3 つの製品を製造販売していた。
「Webwasher」と称するダウンロード版のソフトウェア、
「Appliance」と称するソフトウェアを含むサーバ、及び、
「Cyberguard TSP」と称するソフトウェアを含む装置

これら 3 つの製品(以下、まとめて被告製品という)全てが、クレームされた事前スキャン機能を有するソフトウェアモジュールを備えるという点には争いがない。被告製品は販売の際、当該モジュールが”ロック”されている。ユーザはモジュールを有効とする場合、別途鍵を購入しなければならない。イ号製品を購入するユーザは、コストに応じてモジュールの全て、または、いくつかを有効にでき、さらには全てのモジュールを有効としないこともできる。

(6)訴訟の開始

原告は被告が販売する上記被告製品の販売、及び、当該製品についてのテスト行為は、3 つの特許権を侵害するとしてデラウェア連邦地方裁判所に提訴した。地裁は、被告が故意に全てのクレームを文言上または均等論上侵害したと判断した[9]。そして、地裁は

---

downloadable-information is determined to include executable code,
wherein the causing mobile protection code to be communicated comprises forming a sandboxed package including the mobile protection code and the downloadable-information, and causing the sandboxed package to be communi-cated to the at least one information-destination.

[9] Finjan Software, Ltd. v. Secure Computing Corp., No. 06-CV-369 (D. Del. Aug. 18,

被告に対し永久差し止めと、＄9.18M(約 7 億 2 千万円)の損害賠償の支払いを命じた。被告はこれを不服として控訴した。

３．CAFC での争点

争点 1:一部のソフトウェアモジュールがロックされている場合に、システムクレーム及び記録媒体クレームに対する直接侵害が成立するか否か。

クレームに係る事前スキャンを特徴とするソフトウェアモジュールのソースコードは製品中に含まれている。しかしながら、当該ソフトウェアモジュールがロックされており、ユーザが鍵を購入してロックを解除しない限り、実行することができない。

このような場合に、装置クレーム及び記録媒体クレームに対する直接侵害が成立するか否かが問題となった。

争点 2:一部のソフトウェアモジュールがロックされている場合に、方法クレームに対する直接侵害が成立するか否か。

同様に、方法クレームに対して直接侵害が成立するか否かも問題となった。

４．CAFC の判断

争点 1:販売時に機能がロックされていたとしてもシステムクレーム及び記録媒体クレームについて直接侵害が成立する。

CAFC は販売時に事前スキャンモジュールがロックされていたとしても、被告製品自体には当該モジュールが備わっているから、システムクレーム及び記録媒体クレームに対する直接侵害が成立すると結論づけた。

被告は以下の 2 つの事件を挙げ、一部の機能がロックされている場合、直接侵害が成立しないと主張した。

(1)Southwest事件 [10]

Southwest 事件において特許発明は自動的に選択処理を行う点を特徴とする方法クレームであった。これに対し、イ号ソフトウェア製品は、自動選択処理を行うモジュールに加え、当該自動選択処理を避ける人手による選択をも含んでいた。CAFC は人手による選択を有することから、イ号ソフトウェア製品が自動選択処理を行うモジュールを

2009)

[10] Southwest Software, Inc. v. Harlequin Inc., 226 F.3d 1280, 1291 (Fed. Cir. 2000)

含んでいても直接侵害は成立しないと判断した。

被告は Southwest 事件を引用し、本事件においても同様に直接侵害は成立しないと主張した。しかしながら、CAFC は Southwest 事件におけるクレームは方法クレームであり、システムクレーム及び記録媒体クレームについては同様に適用できないと述べた。方法クレームはクレームされたステップの動作(パフォーマンス)を要求し、直接侵害が成立するためには実際の動作が必要とされる。

これに対し、争点となるクレームは「システム」及び「記録媒体」クレームであり、これらカテゴリーのクレームはいかなる方法のステップの動作(パフォーマンス)を要求するものではないからである。

(2)ACCO事件[11]

参考図 2 はACCO 事件において問題となったロック装置を示す説明図である。ACCO 事件で問題となった装置クレームは、盗難防止用のロック装置を権利化している。

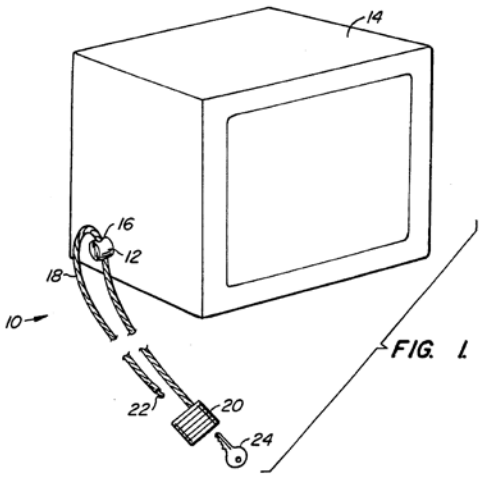

FIG. 1.

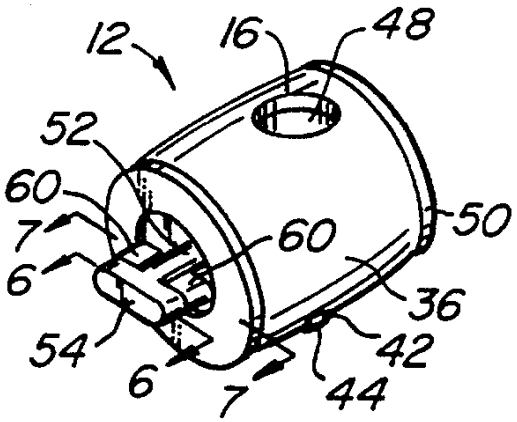

FIG. 3.

[11] ACCO Brands, Inc. v. ABA Locks Mfr. Co., 501 F.3d 1307, 1313 (Fed. Cir. 2007).

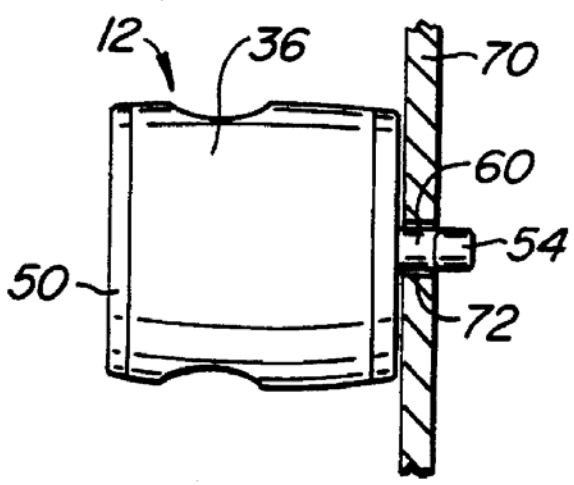

FIG. 10A.

参考図 2　ACCO 事件において問題となったロック装置を示す説明図

問題となった特許は、特殊な配置ピン 60 を、セキュリティスロット 72 を通じて突出させロックする装置である。イ号装置は 2 つのモードのいずれかにおいて操作でき、一方は侵害(侵害モード)、他方は非侵害(非侵害モード)となる。ACCO 事件において CAFC は侵害モードにて現実に誰かが実施したという証拠がないことから直接侵害は成立しないと判断した。

本事件において被告は ACCO 事件を引用し、少しでも非侵害モードにて被告ソフトウェア製品が使用されうるのであれば、直接侵害は成立しないと主張した。

CAFC は、ACCO 事件は特殊な配置が必要となるピンを必要とする点で、何ら特殊な配置が必要とされない事前スキャンモジュールとは相違すると述べた。

(3)直接侵害の成立

被告は、事前スキャン用プログラムコードが全ての被告製品に「完全に存在する」ということを認めている。また原告側証人の Gallagher 氏は、ソフトウェアモジュールがオフにされたとしても、モジュールは製品内のバイナリソースコードに存在すると証言した。

CAFC は、クレームされた機能を実行するためのソフトウェアは販売時に被告製品に

存在するということは疑いがなく、これは、自動車が停止している間も、自動車を推進するエンジンが車体に存在することと同様であると述べた。

CAFCは、Fantasy Sports事件[12]を挙げた。Fantasy事件において、特許はフットボールを仮想空間にてプレイするためのコンピュータをクレームしていた。イ号製品において、特許の機能を利用するためにはユーザがオプションによりソフトウェアの一部分にプログラムされた機能をアクティベートしなければならない。被告はアクティベートした場合にのみ侵害が成立すると主張したが、CAFCはこれを否定し、侵害が成立すると述べた。

なぜなら当該コード自体を、ユーザに変更させる必要はなく、単にアクティベートさせるだけで、ユーザに特許の機能を活用させるためのコードが被告製品中に記述されているからである。

CAFC は Fantasy 事件における考えは本事件にも適用できると述べた。問題となった事前スキャンモジュールは販売時に被告製品内に“既に存在する”。そして、ユーザがソフトウェアモジュールをアンロックするために、内在するコードを変更する必要はない。

キーを購入することにより「プログラムされた機能を有効化すること」が必要であったとしても、被告製品のクレームに対応するコード自体を何ら変更するものでもない。以上のことから CAFC はシステムクレーム及び記録媒体クレームに対する直接侵害を認めた。

争点 2：現実の実施がなければ方法クレームの直接侵害は成立しない

CAFC は米国内において事前スキャンモジュールを動作させた事実が存在しないことから、方法クレームに対する直接侵害は成立しないと判断した。

方法クレームについての直接侵害は、人がクレームされた方法の全てのステップを実行した場合に成立する[13]。原告は技術者がテストのために被告製品を動作させていることから、直接侵害が成立すると主張した。

これに対し CAFC は、当該テストは一度だけドイツで行われたものであり、米国特

---

[12] Fantasy Sports Props. v. Sportsline.com, Inc., 287 F.3d 1108, 1118 (Fed. Cir. 2002).
[13] Lucent Techs. v. Gateway, Inc., 580 F.3d 1301, 1317 (Fed. Cir. 2009).

許法第 271 条(a)にいう直接侵害は成立しないと判断した。その理由として米国特許法第 271 条(a)は「特許発明を合衆国において・・生産，使用」と規定しており、ドイツでのテスト行為では直接侵害が成立しないからである。

５．結論

CAFC は、システムクレーム及び記録媒体クレームについて直接侵害が成立するとした地裁の判断を支持した。その一方で、方法クレームについても直接侵害が成立するとした地裁の判断を無効とした。

６．コメント

被告製品が侵害モードと非侵害モードとを有する場合、方法クレームに関しては侵害モードでの実際の使用・動作があった場合にのみ、直接侵害が成立する。ソフトウェア関連発明についても同様であり、ロックの解除により非侵害モードから侵害モードとなるソフトウェア製品を販売したからといって方法クレームに対する直接侵害は成立しない。

なお、ドイツでテストを行った被告製品を米国に輸入する行為に対しては、米国特許法第 271 条(g)[14]の問題が発生するが、本事件において原告は同条(g)に基づいた主張を行わなかった。

一方、システムクレーム、装置クレーム及び記録媒体クレームについては、クレームされた発明の内容によって、結論が相違する。ACCO 事件で示されたように、侵害モードの構成とするには特殊な配置、操作、変更等が必要とされる場合、たとえ被告製品が侵害モードを有する場合でも直接侵害は成立しない。これに対して本事件及び Fantasy 事件の如く、侵害モードに関連するコード自体を変更する必要はなく、単にロックの解除またはオプション設定により非侵害モードから侵害モードへ変更可能である場合、直接侵害が成立する。

判決　2010 年 11 月 4 日

以上

---

[14] 米国特許法第 271 条(g)の規定は以下のとおり。
何人かが権限を有することなく，合衆国において特許を受けている方法によって製造された製品を合衆国に輸入する又は合衆国において販売の申出，販売若しくは使用した場合において，その製品に係る輸入，販売の申出，販売又は使用が当該方法特許の存続期間中に生じていたときは，当該人は侵害者としての責めを負うものとする。

【関連事項】
判決の全文は連邦巡回控訴裁判所のホームページから閲覧することができる[PDF ファイル]。
http://www.cafc.uscourts.gov/images/stories/opinions-orders/09-1576.pdf