FINJAN, INC.,
Plaintiff- Appellee
v.
BLUE COAT SYSTEMS, INC.,
Defendants- Appellant

2016-2520
[CAFC 2018.1.10 判決]

新横浜総合特許事務所
弁理士　山下　聡

１．概要

（１）経緯

Finjan は、Blue Coat が米国特許 6,154,844（“’844 特許”）を含む複数件の特許を侵害しているものとして、2013 年 8 月 28 日、カリフォルニア州北部地区地方裁判所（以下、地裁）に特許侵害訴訟を提起した。

地裁は、陪審員による侵害認定と損害額裁定とを支持した。また、地裁は、’844 特許が特許適格性を有すると判示した。その後、Blue Coat は、法律問題としての判決の申立（“JMOL”）と再審理の申立を行ったが、地裁は否決した。Blue Coat は、’844 特許の特許適格性を含む地裁の判決に対して控訴した。

（２）101 条の争点

ダウンロードファイルに含まれる不審コードを識別するセキュリティプロファイルをダウンロードファイルに添付する発明（争点となったのは、’844 特許のクレーム１）は、米国特許法 101 条の要件を満たすか。

’844 特許のクレーム１を以下に示す。

> 1. A method comprising:
> receiving by an inspector a Downloadable;
> generating by the inspector a first Downloadable

security profile that identifies suspicious code in the received Downloadable; and
linking by the inspector the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.

１．インスペクタによって、ダウンロード可能なものを受信し、
前記インスペクタによって、前記受信したダウンロード可能なものの中の不審コードを識別する、ダウンロード可能な第１のセキュリティプロファイルを生成し、
前記インスペクタによって、前記ダウンロード可能な第１のセキュリティプロファイルを前記ダウンロード可能なものに添付させ、ウェブサーバが前記ダウンロード可能なものをウェブクライアントに対して利用可能にさせる、
ことを特徴とする方法。

他に、侵害性、損害額についても争われた。

２．判決内容

カリフォルニア州北部地区連邦地方裁判所　No. 5;13-cv-03999-BLF, Beth Labson Freeman 裁判官からの控訴

DYK, LINN, 及び HUGHES 裁判官の面前で

DYK 裁判官

陪審員は、Blue Coat Systems, Inc.(“Blue Coat”)が Finjan, Inc.(“Finjan”)所有の４つの特許を侵害したことを認定し、損害賠償額として 3950 万ドルの合理的実施料相当額を裁決した。トライアル後、地裁は、’844 特許が合衆国法典 35 編 101 条により特許適格性を有すると判示し、トライアル後の Blue Coat による法律問題としての判決の申立（“JMOL”）と再審理の申立とを否決した。Blue Coat は控訴した。

本法廷は、’844 特許に対する地裁の特許適格性の決定には誤りはないと認定し、実質的な証拠が’844 特許と’731 特許に対する陪審員の侵害認定をサポートすることに同意する。しかし、本法廷は、侵害対象製品に関して、クレームで限定された“policy index”を実施してないため、Blue Coat に対して、’968 特許

に対する非侵害を求める JMOL の権利があると判示する。控訴の際、Blue Coat は、’633 特許を侵害するという評決に対して異議を申立てなかった。

損害額に関し、本法廷は、’731 特許と’633 特許に対する裁決を支持する。本法廷は、’968 特許の損害額に関しては、侵害はなかったものとして、損害額の裁決を取り消す。’844 特許に関し、Finjan は機能性を侵害することに対する損害額が分配されていないことと、実質的証拠からは１ユーザあたり 8 ドル分の実施料率がサポートされていないことのついての Blue Coat の主張に同意する。

したがって、本法廷は、一部支持、一部破棄、そして、’844 特許に対する損害額の更なる審理のために地裁へ差し戻す。

背景

2013 年 8 月 28 日、Finjan は、Blue Coat を被告とする、自身が所有する特許の侵害訴訟をカリフォルニア州北部地区地方裁判所に提起し、マルウェアを識別して保護する方向へ向かった。控訴の際、これらの特許のうち４件が争点となった。米国特許 6,154,844（“844 特許”）のクレーム１，７，１１，１４，および４１は、ダウンロード可能なものにセキュリティプロファイルを添付するコンピュータセキュリティを提供するシステムと方法について記載する。米国特許 7,418,731（“’731 特許”）のクレーム１，１７は、要求ファイルに関連するセキュリティプロファイルとユーザが要求したセキュリティポリシーとを比較するネットワークゲートウェイでのコンピュータセキュリティを提供するシステムと方法について記載する。米国特許 6,965,968（“’968 特許”）のクレーム１は、複数のユーザセキュリティポリシーの下、キャッシュファイルの許容可能性を示す“ポリシーベースのキャッシュマネージャ”について記載する。米国特許 7,647,633（“’633 特許”）のクレーム１４は、悪意のあるダウンロードから保護する“モバイルコードルーチンモニタリング”を用いるシステムと方法について記載する。

トライアル後、陪審員は、Blue Coat は４つの特許を侵害したと認定し、Blue Coat の侵害によって Finjan には、約 3950 万ドルの損害が発生したことを裁決した。このうち、’844 特許は 2400 万ドル、’731 特許は 600 万ドル、’968 特許は 775 万ドル、そして、’633 特許は 166 万 6700 ドルである。ベンチトライアル後、’844 特許が合衆国法典 35 編 101 条により特許適格性のある発明の主題に向けられていると地裁は判示した。

その後、地裁は、Blue Coat による、法律問題としての判決を求める申立と再審理の申立とを否決し、侵害認定と損害裁決の各々をサポートする実質的な証拠を Finjan が提出したと判示した。Blue Coat は、’844 特許の特許適格性、’844 特許と’731 特許、及び’968 特許の特許侵害、そして、’844 特許、’731 特許、’968 特許、及び’633 特許の損害額に関する地裁の判決に対して控訴した。CAFC

は、合衆国法典28編1295条(a)(1)に従って管轄権を有する。

検討

Ⅰ．’844特許の特許適格性

本法廷は、’844特許に関する特許適格性を最初に検討する。本法廷は、地裁の判決を最初（de novo）から審理する。*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1311 (Fed. Cir. 2016).

101条が提示することは、特許は、“新規かつ有用なプロセス、機械、製造物、もしくは組成物、又はそれについての新規かつ有用な改良”のために取得される、ということである。合衆国法典35編101条。しかし、最高裁が長く認識していたことは、“科学技術の基本的ツール”の占有化によって、特許システムが促進させようとしているイノベーションが抑え込まれるものとして、101条は、特許可能な発明の主題から“自然法則、自然現象、及び抽象的アイデア”を暗に排除してきた。*Alice Corp. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2354 (2014).(*Ass’n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116 (2013)を引用）; *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1294-97 (2012); *Diamond v. Diehr*, 450 U.S. 175, 185 (1981).も参照。

最高裁が判示したことは、“自然法則、自然現象、及び抽象的アイデアを請求する特許と、これらの概念に関する特許適格性のある応用を請求する特許とを区別する”ために、２ステップフレームワークを用いることである。*Alice*, 134 S. Ct. at 2355. 第１ステップで、争点となるクレームが特許適格性のある概念へ“向けられている”かどうかを決定する。Id. もし、そうであるなら、“各クレーム要素を個別に検討し、かつ、‘順序付けられた結合’として、付加的要素が‘クレームの本質を特許適格性のある応用へ変換する’かどうかを決定する。”Id. (*Mayo*, 132 S. Ct. at 1298を引用). このことは、“発明概念（inventive concept）”－クレームが抽象的アイデア自体を“遥かに超える”ことを保証するために十分なものー の探索に相当する。Id. (*Mayo*, 132 S.Ct. at 1294を引用).

第１ステップを開始する際、本法廷は、’844特許の“クレームされた進歩”を調査して、クレームが抽象的アイデアに向けられているか否かを決定しなければならない。*Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016). ソフトウェアイノベーションを含む事件では、“コンピュータ性能における特定の主張された改善、もしくは、単なるツールとしてコンピュータが実行されるための‘抽象的アイデア’としての資格を与えるプロセス”にクレームが焦点を当てているか否かにこの質問が向けられる。*Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335-36 (Fed. Cir. 2016).

’844特許は、ダウンロード可能なものをスキャンして、スキャンした結果を“セキュリティプロファイル”の形式で添付するコンピュータセキュリティを提供する方法に向けられている。’844特許のクレーム１は、地裁では101条目的で代表的なクレームと認定したが、以下のように記載する：

１．インスペクタによって、ダウンロード可能なものを受信し、

前記インスペクタによって、前記受信したダウンロード可能なものの中の不審コードを識別する、ダウンロード可能な第１のセキュリティプロファイルを生成し、

前記インスペクタによって、前記ダウンロード可能な第１のセキュリティプロファイルを前記ダウンロード可能なものに添付させ、ウェブサーバが前記ダウンロード可能なものをウェブクライアントに対して利用可能にさせる、

ことを特徴とする方法。

’844特許のcol.11 Ⅱ．11-21.　クレーム解釈において、“ダウンロード可能なもの”は、“送信元コンピュータからダウンロードされ、送信先コンピュータで実行する、実行可能なアプリケーションプログラム”を意味すると解釈されるべきことに、両当事者は合意した。さらに、“前記受信したダウンロード可能なもの中の不審コードを識別するダウンロード可能なセキュリティプロファイル”は、“悪意のある、或いは潜在的に悪意のある動作を実行する、前記受信したダウンロード可能なもの中のコードを識別するプロファイル”を意味すると、地裁は解釈した。

CAFCは、*Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1319 (Fed. Cir. 2016)事件において、“ウィルススキャン自体は既知であり、抽象的アイデアを構成する”と判示した。また、CAFCが認定したことは、－ファイルがユーザコンピュータに到着する前に、ファイルがスキャンされることを保証する－中間コンピュータ上でウィルススキャンを実行することは、“完全に従来の”アプローチの仕方であって、抽象的である。Id. At 1321.　ここで、クレームされた方法は、以前よりも良い処理方法である。

’844特許のクレーム１は、ダウンロード可能なものをスキャンし、ウィルススキャン結果を、新たに生成したファイル：“受信したダウンロード可能なもの中の不審コードを識別するセキュリティプロファイル”の形式でダウンロート可能なものに添付する。地裁のクレーム解釈において強調されたことは、この“不審コードを識別する”という限定要素が満たされるのは、“‘ダウンロード可能なものによって行われるかもしれない、潜在的な悪意あるコード操作又は不審コード操作のすべて’のような、受信したダウンロード可能なものの中の不審コードについての詳細”をセキュリティプロファイルが含む場合についてのみで

ある、ということである。*Finjan, Inc. v. Blue Coat Sys., Inc.*, No. 13-CV-03999-BLF, 2014 WL 5361976, at *9 (N.D. Cal. Oct. 20, 2014). セキュリティプロファイルには、“行動ベース”のウィルススキャンによって生成される、潜在的に悪意のある操作についての情報を含まなければならない。この操作は、伝統的な“コードマッチング”ウィルススキャンとは区別され、そのスキャンは、ダウンロード可能なものの中のコードと既知の不審コードデータベースとを比較することによって、それまで特定されたウィルスの存在を把握することに限定される。そのようなことで、論点は、’844特許におけるこの行動ベースのウィルススキャンは、コンピュータ機能の改善を構成するか否かである。本法廷は、構成すると考える。（下線部筆者）

ウィルススキャンに対する“行動ベース”のアプローチは、Finjanが先駆けであり、’844特許の特許明細書により開示された。既知のウィルスを単に探索する伝統的な“コードマッチング”システムと異なり、“行動ベース”のスキャンは、ダウンロード可能なコードを分析し、ファイルの名前を変えたり削除したりするような、潜在的に危険又は望ましくない操作を行うかどうかを決定する。セキュリティプロファイルは、行動ベースのスキャンによって利用可能な潜在的な不審コードについての詳細な情報と通信することから、これまで未知のウィルスから保護するために用いられる（下線部筆者）。セキュリティプロファイルは、コードマッチングウィルススキャンによる保護を回避するために外見上改良されたウィルスを知らせる“難読化コード”と同様である。

セキュリティプロファイルアプローチは、よりフレキシブルでよりきめ細かなウィルスフィルタリングを行うことも可能である。インスペクタがダウンロード可能なものに対するセキュリティプロファイルを生成した後、“セキュリティ*ポリシー*”がユーザと関連するものであれば何であっても、ルールに従って、そのセキュリティプロファイルを参照することで、ダウンロード可能なものにアクセスするかどうかを、ユーザコンピュータが決定することができる。管理者は、異なるセキュリティプロファイルを、異なるユーザや異なる種別のユーザに適用することで、簡単にアクセスに手を加えることができる。そして、管理者は、特定の潜在的脅威についての情報を含むセキュリティプロファイルを有することで、より高精細のルールを持つセキュリティプロファイルを手作業で作ったり、進化した脅威に応答してセキュリティポリシーを修正したりすることが可能となる。

本事件で確認することは、ソフトウェアベースのイノベーションが“コンピュータ技術に対する非抽象的な改善”をさせ、ステップ１で特許可能な発明の主題であると思わせることである。*Enfish*, 822 F.3d at 1335-36. *Enfish*事件において、例えば、裁判所が決定したことは、クレームは、新たに用いられるデー

タベースアーキテクチャに関連し、“コンピュータが通常の能力で用いられる経済的なタスクや他のタスクではなく、コンピュータ機能自体に対する改善”にクレームの焦点が当てられているため、自己参照型論理テーブルは非抽象的である、ということである。Id. at 1336.（下線部筆者）　確かに、*Enfish*事件で特許適格性があると認定された自己参照型データベースは、コンピュータに対して、より高速でより効率的な見慣れたタスクを実行させること以上のことをさせており、それは、ユーザが、新たな手法で、データベースを起動させて作成することを実際に許容している。伝統的なリレーショナルデータベースは、“様々なテーブルのより広いモデリングと構築、そして、データベースを起動する前のより広い関係性”を含むが、*Enfish*事件における自己参照型データベースは、“列コラム定義がない、あるいは列コラム定義のみ”で起動することができ、“動作中に”構築され、適用されることができる。Id. at 1333.

同様に、クレーム１の方法は、コンピュータセキュリティシステムがこれまでできなかったことをする、新しい種別のファイルを利用する。セキュリティプロファイルアプローチは、異なるユーザに適合したアクセスを許容し、ユーザコンピュータにファイルが到着する前に、脅威を識別することを保証している。セキュリティプロファイルが“不審コードを識別する”という事実は、システムに対して、新たに利用可能な、潜在的脅威についての行動ベースの情報を蓄積させ、利用させることを許容する。したがって、主張クレームは、はっきりとコンピュータセキュリティという抽象的アイデアというよりも、むしろ、コンピュータ機能に対する非抽象的な改善に向けられている。（下線部筆者）

クレームが新たなアイデアに向けられていることを認めたとしても、クレームには、そのアイデアをどのように実行するかについて十分記載されていないため、抽象的なものは残されている、ということをBlue Coatは主張した。Blue Coatは、*Apple, Inc. v. Ameranth, Inc.*事件について主張した。この事件では、第１メニューのアイテムの選択に基づいて第１メニューから第２メニューを生成することができるコンピュータシステムに関するクレームについて、CAFCは無効と判示した。842 F.3d 1229, 1240-41 (Fed. Cir. 2016).　この事件においては、特許が“ソフトウェアを特定の手法でプログラミングしたりデザインしたりすることをクレームにしているのではなく、単に得られたシステムをクレームにしているだけである”ことから、特許は抽象的アイデアに向けられているとCAFCは判示した。Id. at 1241.　Blue Coatは、*Affinity Labs*事件に依存することも主張した。この事件では、領域外の受取人に対して部分的なブロードキャストコンテンツを無線で通信することに関するクレームについて、“[アイデアを]どのように実行するかについて一切向けられておらず、むしろ、クレームはアイデアそのものを記載している”ため、抽象的であり、特許非適格である、

とCAFCは判示した。838 F.3d at 1258. そして、Blue Coatは、*Intellectual Ventures*事件についても主張した。この事件では、“どのように結果が成し遂げられかについて何ら限定がなく...メカニズム...が記載されていない”場合、クレームは、抽象的な電子メールフィルタリングへ向けられて、特許適格性がない、と判示した。838 F.3d 1307, 1316 (Fed. Cir. 2016) (*Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1348 (Fed. Cir. 2015)を引用). (下線部筆者)

*Apple*事件、 *Affinity Labs*事件、その他の類似の事件では、たとえ、イノベーティブな結果であっても、結果そのものは特許可能ではない、という基本的な特許法の原則に戻って、耳を傾けるべきである。*Corning v. Burden*, 56 U.S. 252, 268 (1853) (“有益な結果や効果そのものではなく...そのような結果や効果を生む実用的な方法や手段の発見や発明に対して”、特許が発行されることについて説明している (下線部筆者))参照；*O'Reilly v. Morse*, 56 U.S. 62, 112-113 (1853)(“その結果が、明瞭なキャラクタ、サイン、もしくは、ある距離離れた文字を作ったり印刷したりする”ための電磁気学に関するすべての使用をカバーすると主張するクレームは、“あまりに広く、法によって保証されない”ものとして無効にした).

ここで、クレームは、単なる結果以上のことについて言及する。それよりも、クレームは、特定のステップー不審コードを識別するセキュリティプロファイルを生成し、そのプロファイルをダウンロード可能なものに添付させることーについて言及し、そのステップにより望ましい結果を得ることができる (下線部筆者)。さらに、開示された唯一のことは結果であって、その結果を生む発明的な改良ではないことに争いがない。そのアイデアは、非抽象的であり、Aliceの第２ステップへ進む必要性はない。

Ⅱ. 侵害

トライアルにおいて、陪審員は、Blue Coat製品が'844特許、'731特許、及び'968特許を侵害すると認定した。地裁は、Finjanが侵害認定をサポートする実質的な証拠を提出し、陪審員の評決が証拠の重みに反していないことを認定し、Blue Coatのトライアル後の法律問題としての判決を求める申立と再審理を求める申立とを認めなかった。本法廷は、JMOLの申立を否決したことを最初からレビューし、再審理の申立についても裁量権の濫用であるかどうかについてレビューする。*Revolution Eyewear, Inc. v. Aspex Eyewear, Inc.*, 563 F.3d 1358, 1370-71 (Fed. Cir. 2009).

A. '844 特許

Blue Coat が最初に主張したことは、実質的な証拠は、陪審員の評決をサポートしていないため、'844 特許で主張されたクレームに関して非侵害であるとい

う JMOL を認めるべきである、ということである。とくに、Blue Coat が強く主張したことは、“ウェブクライアントで利用可能なダウンロード可能なものをウェブサーバが作成する前に”、セキュリティプロファイルをダウンロード可能なものに結合することが必要なクレームは、最初の場所でインターネットに公表される前に、コンテンツを評価するサーバ側の製品によってのみ、侵害とされる、ということである。Blue Coat の製品である、WebPulse は、クラウドベースのサービスであって、顧客のネットワークゲートウェイへダウンロード可能なものについての情報を提供し、特定のエンドユーザが特定のダウンロード可能なものにアクセスできるかどうかを、ネットワークゲートウェイが決定するのを助けることができる。WebPulse は、すでにインターネットで利用可能になったダウンロード可能なもののみを評価するため、Blue Coat は侵害ではない、ということを主張する。

Blue Coatは、ダウンロード可能なものがインターネットに置かれる前に、セキュリティプロファイルをダウンロード可能なものに結合することが必要であるとするクレーム解釈の要求をしなかった。Blue Coatは、トライアル後の申立において最初にクレーム解釈の争点を提起することができなかった:“JMOLの段階において、クレーム用語に関する新規でより詳細な解釈を主張したり、この新規で詳細な解釈により陪審員の評決をテストしたりすることは、あまりに遅い”。*Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1321 (Fed. Cir. 2003). このような状況において、“トライアルを行う裁判所の争点は、争点となる解釈のもと、実質的な証拠が陪審員の評決をサポートするかどうかに限定される。” *Wi-Lan, Inc. v. Apple, Inc.*, 811 F.3d 455, 465 (Fed. Cir. 2016). ここで必要とすることは、地裁が解釈するように、“ウェブクライアントにおいて利用可能なダウンロード可能なものを非ネットワークゲートウェイサーバが作成する前に、インスペクタによって、第１のダウントード可能なセキュリティプロファイルをダウンロード可能なものに結合すること”である。’844 特許, col. 11Ⅱ.18-20;J.A. 25. 陪審員は、この解釈を適用することを命じた。

クレームしたシステムにより保護される特定のウェブクライアントに言及するために、陪審員が“ウェブクライアント”を解釈することは合理的である。同様に、ダウンロード可能なものが“ウェブクライアントに利用可能...とされる”前に結合が発生することが必要であるとする限定要素は、－ダウンロード可能なものがインターネット上で利用可能とされる前の必要性ではなく－ユーザがダウンロード可能なものにアクセスすることが許容される前に、ある点で結合が発生することが必要である、と理解することが合理的である。Blue Coatが認めたことは、セキュリティプロファイルが結合される時間で、“特定のウェブク

ライアントはダウンロード可能なものを*まだ受信*することができないーしかし、ウェブサーバはそれを利用することができる、ということである。Reply Br. 9. サービス側のユーザがダウンロード可能なものを受信する前に、WebPulseが、セキュリティプロファイルをダウンロード可能なものに結合する、という争いのない事実によって、本法廷は、'844特許に対する侵害の評決は、実質的証拠によってサポートされている、と認定する。

B. '731特許

次に、本法廷が検討することは、'731特許における主張されたクレームに関して非侵害であるというJMOLの申立の権利が与えられるとする、Blue Coatの主張である。'731特許は、公的なインターネット上のウェブページで実行される悪意あるソフトウェアからプライベートイントラネットを保護するコンピュータゲートウェイに向けられている[1]。クレームにしたゲートウェイは、潜在的に悪意のあるファイルをスキャンニングし、"セキュリティプロファイル"を生成する動作を行い、各ファイルは各々、"前記ファイルが実行可能なようにプログラム化されたコンピュータコマンドのリスト"を備える。'731特許, col.4Ⅱ. 47-48. クレーム１７がさらに特定することは、セキュリティプロファイルには、"抽出ファイルが実行可能なようにプログラム化された、少なくとも１つのコンピュータコマンドのリスト"を含むことである。'731特許, col.13Ⅱ.7-8. セ

[1] '731 特許のクレーム１は以下となる：

１．イントラネットコンピュータに対するコンピュータゲートウェイにおいて、

インターネットからの着信ファイルをスキャンし、前記着信ファイルのためにセキュリティプロファイルを抽出するスキャナーであって、前記セキュリティプロファイルの各々は、コンピュータコマンドリストを備え、前記着信ファイルのうち対応するものが以下を実行可能とする：

将来アクセスのために、前記スキャナーによってスキャンされたファイルを蓄積するファイルキャッシュであって、前記蓄積ファイルの各々はファイル識別器によってインデックスが付与され、

前記スキャナーによって抽出された前記セキュリティプロファイルを蓄積するセキュリティプロファイルキャッシュであって、前記セキュリティプロファイルの各々は、前記ファイルキャッシュに蓄積された対応ファイルと関連するファイル識別器によって、前記セキュリティプロファイルキャッシュにおいてインデックスが付与され、

前記イントラネット内のイントラネットコンピュータに対するセキュリティポリシーを蓄積するセキュリティポリシーキャッシュであって、前記セキュリティポリシーは前記イントラネットコンピュータの対応する部分集合へ送信されるファイルのために限定リストを各々含む、

ことを特徴とする。

'731 特許, col. 11Ⅱ.35-55.

キュリティプロファイルが生成されると、ユーザと関連するセキュリティポリシーと比較されて、ファイルがユーザに提供されるべきかどうかを決定することができる。

Blue Coatが主張したことは、侵害被疑製品により生成された“セキュリティプロファイル”には、必要な“コンピュータコマンドリスト”が含まれていないため、’731特許は、法律問題として侵害ではない、ということである。Blue Coatは、“コマンドリスト”の用語の解釈を要求しなかったため、本法廷は、通常の意味でその用語の意味を適用する。実質的証拠は陪審員の侵害という認定をサポートしていると、本法廷は認定する。

トライアルにおいて、Finjanは、侵害被疑製品が潜在的なマルウェアを確認するために着信ファイルをスキャンするごとに、その製品が“cookie2”と呼ばれる新たなファイルを生成することを示す証拠を提出した。Cookie2は、ダウンロード可能なファイルについての様々な特徴を表す領域についての設定を備えている。Cookie2の領域７８－８０は、あるコマンドを表しており、これらのコマンドーeval(), unescape(), 及びdocument write()ーが着信ファイルとして表されているかどうかを示している。領域７８－８０において、整数は、コマンドが出現した回数を表す。Finjanの専門家、Mitzenmacher博士は、領域７８－８０に含まれるデータは、“明らかにコンピュータコマンドリストである”と証言した。 J.A. 40383.

Blue Coatは、これは十分ではないと主張し、“コマンドリスト”という限定要素は、“システムが監視すべき種類のコマンドの識別器”によって満たされることができないことも主張する。Appellant Br. 34. しかし、セキュリティプロファイルには、“着信ファイルのうち対応するものが実行可能なようにプログラム化されたコンピュータコマンドのリスト”を含むことが、クレーム用語として単純に必要としている。このことは、あらゆる特別な情報表現に対して権限を与えることではなく、ましてや、コマンドが実行可能なコードの形式でリスト化されることも必要ではない。Mitzenmacher博士がトライアルで証言したことは、領域７８－８０の整数は“明らかにコンピュータコマンドリスト”であって、その理由は、“これらの整数は、これらのコマンドがセキュリティプロファイルにあるか否かを決定する”ものだからである。J.A.40383-84. 彼は、“それがここで表現される方法を含む、[コンピュータコマンドの]リストを表現する多くの方法がある”ことも指摘した。J.A. 40384. 実質的証拠は、陪審員が暗に認定したこと、すなわち、Cookie2の領域７８－８０の整数は、“コマンドリスト”という限定要素を満たすことをサポートし、特許は侵害されている。

C. ’968特許

Blue Coatは、侵害被疑製品がクレームした“ポリシーインデックス”を実施

するという実質的証拠をFinjanが引き出すことに失敗したため、'968特許に対する非侵害に関するJMOLの申立をする権利があることを主張する。本法廷はこの意見に同意する。

'968特許は、複数のセキュリティポリシーに従ってキャッシュされたコンテンツを効率的に管理する“ポリシーベース”のキャッシュマネージャに向けられている。特許権者が同意したことは、コンテンツの一部がユーザによってアクセスされることができるかどうかを決定するルール又はルールの設定が“ポリシー”である、ということである。異なるポリシーは異なるユーザに適用され、ユーザをコンテンツにアクセスさせるかどうかの決定は、コンテンツのセキュリティプロファイルとしたがって、ユーザアクセスを管理するポリシーとを比較することで行われる。したがって、'968特許のキャッシュマネージャに基づくポリシーは、様々なポリシーのもとでコンテンツが許容されるかどうかを保持するデータ構造である。クレーム１は、単独で主張されたクレームであるが、以下のように表現されており、キーとなる用語にはアンダーラインを示す：

１．ポリシーベースのキャッシュマネージャであって、

デジタルコンテンツのキャッシュ、複数のポリシー、及び前記キャッシュコンテンツに対するポリシーインデックスを記憶するメモリであって、前記ポリシーインデックスは、複数のポリシーの各々に、キャッシュコンテンツに関するエントリと、所定のポリシーと比較して許容されていると知られているキャッシュコンテンツを表示するポリシーとを含み、

前記メモリと通信可能に接続され、受信したデジタルコンテンツをスキャンニングし、対応するコンテンツプロファイルを抽出するコンテンツスキャナーと、

前記メモリと通信可能に接続され、前記コンテンツプロファイルに基づいて、<u>所定のポリシーと比較して所定のデジタルコンテンツが許容されているかどうか</u>を決定するコンテンツ評価器であって、<u>その結果は前記ポリシーインデックスにエントリとして記憶される</u>

ことを特徴とするキャッシュマネージャ。

'968特許, col.9 Ⅱ.47-62.　クレーム解釈において、“ポリシーインデックス”は“複数のポリシーと比較してキャッシュされたコンテンツの許容可能性を表すデータ構造”を意味すると、両当事者は規定した。陪審員はこの解釈を適用することを命じた。再度、本法廷は、陪審員による侵害評決をこのクレーム用語とクレーム解釈に基づいて検査する。*Hewlett-Packard Co.*, 340 F.3d at 1320-21.

トライアルで証言されたことは、侵害被疑製品である、Proxy　SGは、コンピュータイントラネットとインターネットとの間の広い意味でのゲートウェイで

ある、ということである。ユーザがファイルを要求するごとに、Proxy SGは、ファイルを分析して、ユーザセキュリティポリシーのもとでアクセスが許容されるかどうかを決定する。Proxy SGは、ファイルを評価すると、ポリシー*内部*の個別ルールの結果をキャッシュし、その情報を用いて、最終的なポリシーを決定する処理のスピードを早くさせることができる。その分析に先立って、例えば、Proxy SGは、ファイルの“カテゴリ”をチェックし、ユーザポリシーが“カテゴリ”領域に関連するあらゆるルールをもっているかどうかを決定することができる。そして、Proxy SGは、“このカテゴリ領域を処理するルールについての一部の評価を蓄積し...あなたは、再度このような条件において再評価しなくてもよい。” J.A. 40327-28. しかし、Finjanの専門家が明確に理解するように、Proxy SGは、所定のポリシーを条件としてコンテンツがユーザにアクセスされるかどうかについての最終的な決定を記憶しない。Proxy SGは、最終的なポリシーの決定を作成することを検討する個別ルールの各々の評価を、記憶するだけである。これは、クレーム用語が必要とすることではない。’968特許でクレームにしたポリシーインデックスは、“所定のデジタルコンテンツが所定のポリシーと比較して許容可能かどうか”のコンテンツ評価器による決定の“結果”を記憶しなければならない。

サマリージャッジメントにおいて、地裁が同意したことは、ポリシーインデックスが必要とすることは、最終的な許容可能性の決定を蓄積するためであり、地裁が指摘したことは、“すべてのポリシーが複数のルール又は条件から構成されるのであれば、被告の主張が勝っているようである”、ということである。*Finjan, Inc. v. Blue Coat Sys., Inc.*, No. 13-CV-03999-BLF, 2015 WL 3630000, at *9 (N.D. Cal. June 2, 2015). それにも拘らず、地裁は、“’968特許がとくに提供することは、ポリシーはちょうど１つのルールにすることができることである”という理由で、サマリージャッジメントを認めることを否決した。Id. Proxy SGが１ルールポリシーを取りまとめるルールを適用した結果を記憶するのであれば、それは、複数ポリシーに対して最終的な許容性の決定を蓄積するだろうし、その場合は侵害になるだろう。したがって、地裁は、以下のことを証明する機会をFinjanに与えた。すなわち、“Proxy SGポリシーキャッシュは、多くの条件評価を含み、その各々は、複数の単一条件ポリシーの１つと比較してファイルが許容できるかどうかを決定するためにある。”ということである。Id.

トライアルにおいて、Finjanはこのようなことを示すことはしなかった。Proxy SGによって蓄積された条件決定が、単一ルールポリシーを管理する、ユーザに対して最終的な許容性の決定に該当することを示す証拠はなかった。確かに、Finjanの専門家が理解していたことは、Proxy SGは、最終的な許容可能性の決定を蓄積することはなく、代わりに、要求されるごとにコンテンツの許容性を

再評価しなければならない、ということである。したがって、陪審員の侵害評決が実質的証拠によってサポートされていないことは明白である。

Finjanは、侵害被疑製品が最終的な許容性の決定を蓄積するという証拠を示すことに失敗したため、Blue Coatは、非侵害であるというJMOLを申し立てる権利があった。

Ⅲ. 損害額

本法廷は、'844特許、'731特許、及び'633特許についてのBlue Coatによる損害額について検討する。スタートポイントは、合衆国法典35編284条であり、そこでは “侵害を補償するには十分な”ものに対する損害額を規定する。侵害補償に関する２つのカテゴリは、特許権者の逸失利益と、“アームレングス取引を介して受け取った合理的な実施料”とである。*Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1324 (Fed. Cir. 2009).

本事件で争点となる損害額についての唯一の判断手法は、合理的な実施料であり、それは、実施料が侵害から除外されたなら侵害者が支払うべきであろう合理的な実施料を得る機会を失ったことに対して...特許権者を補償するために請求する“ものである。*AstraZeneca AB v. Apotex Corp.*, 782 F.3d 1324, 1334 (Fed. Cir. 2015) (*Lucent Techs.*, 580 F.3d at 1325を引用).

A. '844特許

Blue Coatが最初に主張したことは、実施料ベースを計算する際に、Finjanは、侵害機能に対して損害額を配分することに失敗した、ということである。本法廷もこの意見に同意する。

侵害被疑技術が侵害被疑製品全体を組み立てることができなかったとき、配分が要求される。“実施料ベースと実施料レートの最終的な結合は、侵害被疑製品の特長を侵害することに起因する値を反映させなければならない” *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1226 (Fed. Cir. 2014); また、*Mentor Graphics v. EVE-USA*, 870 F.3d 1298, 1299 (Fed. Cir. 2017)も参照(大法廷での再ヒアリングを否定する命令)(“侵害製品が特許化された部品と特許化されていない部品との複数部品製品である場合”); *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1326 (Fed. Cir. 2014)(“実施料の形態がどのようなものであっても、特許権者は特徴を侵害することに起因する損害額についてのみ注意して請求すべきである”). このような事件において、特許権者は、“特許化された特徴と特許にされていない特徴との間の[侵害者の]利益と特許権者の損害額とを分割又は配分することを左右する証拠を提出しなければならず、このような証拠は、信頼性があり明白なものでなければならず、推測的なものや不確かなものであってはならない” *Garretson v. Clark*, 111 U.S. 120, 121 (1884). 特許権者としてのFinjanは、証拠の優位性によって、損害額を提

示する重荷を背負っている。

侵害製品であるWebPulseは、クラウドベースのシステムであって、ポルノ写真、ギャンブル、ショッピング、ソーシャルネットワーキング、そして、“疑義のある”ものー潜在的なマルウェアを見分ける意味のカテゴリであるーを含む、８０以上のカテゴリのURLと関連している。WebPulseはそれ自体では販売されていない。むしろ、Proxy SGと同様に、他のBlue Coat製品がWebPulseのカテゴリ情報を用いて、エンドユーザがアクセスしようとするURLを決定するためにある。

“動的なリアルタイム評価エンジン”であるDRTRは、カテゴリ化されていないURLの分析を担当するWebPulseの一部である。DRTRは、侵害機能も非侵害機能も双方実行する。ユーザが、WebPulseデータベースにないURLー例えば、ブランドのある新たなウェブサイトーへのアクセスを要求すると、DRTRは、コンテンツを分析し、カテゴリを割り当て又はカテゴリ化し、そして、その後に使用するためにサイトについてのメタデータを収集する。分析の一部として、DRTRは、URLに悪意のあるコードや疑義のあるコードの有無を調査し、その情報をハイライト表示した“セキュリティプロファイル”を生成し、セキュリティプロファイルを所定のURLへ“添付”させる。これは、’844特許の侵害である。しかし、DRTRの分析は、ポルノ写真からニュースまでの範囲にそのURLが含まれるか否かも評価する。このような付加的なカテゴリは、DRTRのマルウェア識別機能と無関係であるが、従業員に対して、仕事上ではあるけれどもソーシャルメディアを利用させないようにしようとする会社にとって、未だ、価値があることである。DRTRは、Blue Coatが後で使用するためのURLについてのメタデータも収集する。言い換えると、侵害機能のすべてはDRTRにおいて発生するものの、DRTRの機能の一部は侵害であり他の一部は非侵害である。

トライアルにおいて、Finjanは、侵害方法を実行するWebPulseの部品であるDRTRを介したウェブトラフィックの比率によって、WebPlusの全ユーザ数を乗算することで、侵害の増加分を実施料ベースに結び付けようとした。DRTRは、WebPulseの全ウェブリスクエストのうち約４％を処理するため、Finjanは、7500万人のWrbPlusユーザに対して４％を乗算することで実施料ベースを立証した。上述したように、DRTRは、非侵害機能を実行するけれども、Finjanは、実施料ベースの更なる配分について何も立証することはしなかった。

Finjanが主張したことは、DRTRは、発明の足跡と結びついた“最小の識別可能な技術的部品”であるため、DRTRに対する配分は適切である、ということである。Appellee Br. 49-50.　この議論は、侵害製品のうち、“最小販売可能特許実施ユニット”の配分に関するCAFCの判例から持ち出したものであるが、Finjanを助けることはできなかった。最小販売ユニットの原理は、“多数の部品を含むあらゆるケースにおいて、最小販売可能特許実施ユニットと対照的に、全体製品の需

要が特許された特徴に起因することを示すことなく、全体製品の販売量に基づいて損害額を計算することができない”、ということに向けられている。*LaserDynamics, Inc. v. Quanta Comput., Inc.*, 694 F.3d 51, 67-68 (Fed. Cir. 2012). 全体市場価値ルールは、本事件では争点ではないけれども、“最小の識別可能な技術的部品”に基づいて実施料ベースを立証したという事実は、“最終的な合理的実施料は、特許発明が最終製品に付加する増加分に基づかなければならない”という“必須要件”から孤立させることはしなかった。*Ericsson*, 773 F.3d at 1226. CAFCが*VirnetX*事件において判示するように、最小販売可能ユニットーもしくは、最小識別可能技術部品ーが、非侵害の特長を含む場合、付加的な配分は、また、必要である。*VirnetX*, 767 F.3d at 1327. (“最小販売可能ユニットが実施料ベースとして用いられる場合、ベース選択上の更なる制約は必要ない、という誤った提案をした”という陪審員に対する説示を否決した).

Finjanは、“多くの他のカテゴリは重要ではない”ことを提示して主張することで、その配分方法論に対して防御した。Appellee Br.51. しかし、クレームにした特定カテゴリの非重要性（例えば、“マーシーとショッピング”）は、マルウェアと関連しないカテゴリを識別する重要性全体に対して、言及していない。マルウェアの検出は、DRTR（及びWebPulse）の価値を運ぶ、疑いの余地のない重要なものである。例えば、トライアルにおいて、Layne-Farrar博士は、Blue Coatの内部電子メールについて指摘し、“現在、[WebFilterとWebPulse]の主要な価値は、ゼロデイ周囲からのマルウェア保護が中心である”と述べた。J.A. 40571. 彼女は、“Blue Coatを選択する５つの理由”という表題が付けられた、2012一般向け文書について言及し、２つの理由として、“否定的なデイディフェンス：ソースでマルウェアをストップすること”を掲載している。J.A. 40572-73. しかし、Blue Coatの顧客は、他のカテゴリのコンテンツを識別し、フィルタをかけるという、WebPulseの能力に価値を見出しているという事実がある。トライアルで議論されたBlue Coatのホワイトペーパーにおいて、積極的に広告していることは、“許可されたインターネット使用ポリシーを実行するために必要なビジネスとする詳細なカテゴリ制御”をWebPulseが提供するという事実である。J.A. 53136. そして、Finjanの専門家は、“ギャンブル”としてカテゴリ化したあるサイトへのアクセスを禁止したい会社についての例を利用した。“‘価値があり、重要で、もしくは本質的なものとして見られる’かどうかについて、特許の特長が分割されなければならない”。*VirnetX*, 767 F.3d at 1329. (*LaserDynamics*, 694 F.3d at 68を引用).

DRTR自体は、侵害していない特徴を含む、多数部品ソフトウェアエンジンであるため、DRTRによって制御されるウェブトラフィックの比率は、全体として、

WebPulseに対する特許技術についての増加分の代理にはならない。さらに、配分は、非特許要素の価値と比較した特許技術の価値を反映させることが必要であった。

Blue Coatは、Finjanの合理的な実施料計算において第２の誤りも確認した。'844特許の侵害に対する合理的実施料支払いの一時金にたどり着くことで、Finjanは、１ユーザあたり８ドルの実施料率による実施料まで増加させた。Blue Coatは、８ドルの実施料率には根拠がないと反論する。

本法廷は、Finjanの分析で計算した、１ユーザあたり８ドルの実施料率は、実質的な証拠によりサポートされていないことに同意する。Finjanは、比較可能なライセンスや交渉において、１ユーザあたり８ドルの料金を実際に用いたり、提案したりする証拠はない。むしろ、１ユーザあたり８ドルの料金は、Finjanの副社長であるIPライセンシングのIvan Chaperotの証言に基づいている。すなわち、彼は、ライセンス交渉における現在の“開始点”は、“８から１６％の実施料率か、又は、ユーザごとに８ドルの料金と同様に...一致する何かである”と証言した。J.A. 40489. Chaperot氏は、８－１６％は、Secure Computingに訴えを起こしたFinjanによって得られた2008年の評決に基づいている、ということも証言した。このことに基づいて、Finjanの代理人は、“Finjanがこの当時に要求したことはこれである”ため、仮説交渉において、１ユーザあたり８ドルの実施料率が用いられることを陪審員に説明した。J.A. 41654.

あらゆる合理的な実施料分析には、“概算値と不確実性の要素が必然的に含まれるが、事実に関する実験者は、合理的な実施料を決定するために、幾つかの事実の基礎となるものを持っていなければならない”。 *Unisplay, S.A. v. Am. Elec. Sign Co.*, 69 F.3d 512, 517 (Fed. Cir. 1995). １ユーザあたり８ドルの料金は、*Secure Computing*事件で立証された８－１６％実施料と“一致する”という、Chaperot氏の証言は、十分ではない。８－１６％実施料率が、１ユーザあたり８ドルの料金に対応するだろうという、Chaperot氏の証拠不十分な証言をサポートする証拠はなく、Finjanは、*Secure Computing*事件の事実を本事件の事実に適切に結び付けることに失敗した。*LaserDynamics*, 694 F.3d at 79 (“異なる技術間や異なるライセンス間でルーズな若しくは漠然とした比較を主張することは十分ではない”)参照。

*Secure Computing*事件において、'844特許は含まれなかったし、争点となった特許が経済的又は技術的に比較可能であるということを示す証拠はない。この点につきFinjanが示した証拠は、*Secure Computing*事件における侵害製品がコンピュータセキュリティ分野でもあったことと、2008年において、Secure ComputingはBlue Coatのコンペチターであったという事実に限定される。この外観における類似点は、遥かに一般的過ぎて、合理的実施料計算の基礎とするこ

とができない。どのようなケースでも、８－１６％の実施料率がライセンス交渉における*現在の出発点*であるという、Chaperot氏の証言は、2008年において、仮説のアームレングス交渉を両当事者が提案した、或いは合意したことについて、わずかに示しているだけである。そして、Finjanが示した１４－３４ドルのソフトウェアユーザ料金に関する証拠は、特許をライセンスする際に両当事者が支払った額を示すものではない。*Uniloc USA, Inc. v. Microsoft Corp.*, 632 F.3d 1292, 1317 (Fed. Cir. 2011)(“本事件で争点となる特定の仮説交渉に対しては、これまでのライセンスで使用された実施料率に関連する事実を基礎としなければならない”)を参照。すなわち、１ユーザあたり８ドルの料金は、薄い空気から引き抜かれたもののように見え、このように、合理的実施料計算の基礎とすることはできない。

Finjanは、陪審員の評決をサポートする損害額を提示することに失敗したことは明らかであるが、JMOLの破棄は、’844特許に対するBlue Coatの侵害に対して、Finjanが損害賠償金を受け取ることができない結果を生むことになる。通常、侵害が認定されたとき、特許権者が代替理論に基づく損害額の権利を放棄しないのであれば、*Promega Corp. v. Life Tech. Corp.*, No. 2013-1011, slip op. at 15 (Fed. Cir. 2017)、“地裁は、合理的実施料よりも低くならない額に相当する損害額を認めなければならない”*Dow Chem. Co. v. Mee Indus., Inc.*, 341 F.3d 1370, 1381 (Fed. Cir. 2003); *Riles v. Shell Expl. & Prod. Co.*, 298 F.3d 1302, 1313 (Fed. Cir. 2002)を参照。したがって、本法廷は、Finjanが合理的実施料損害額を立証する権利を放棄したかどうかを決定するため、そして、損害額に関する新たなトライアルを命令するかどうかを決定するため、地裁へ差し戻す。

B. ’731特許と’633特許

’731特許と’633特許に対して、Finjanの専門家は、Proxy SGに関する侵害機能と非侵害機能館の実施料ベースから構成される収入を配分した。Blue Coatは、配分は十分ではないと主張する。本法廷は、この意見に同意する。

Finjanの専門家、Layne-Farrar博士は、’731特許と’633特許の配分分析を、Blue Coatが準備した構造的ダイヤグラムに基礎づけた。ダイヤグラムは、“安全なWeb Gateway：機能”という表題であり、安全なWeb Gatewayシステムの異なる部品を表す24個のボックスについて示した。Layne-Farrar博士は、各ボックスが１つの最高級の機能を表し、各機能は同等の価値を有する、と仮定した。したがって、１つの機能は’633特許を侵害し、３つの機能が’731特許を侵害するため、彼女は、’633特許に対しては１／２４の配分、’731特許に対しては３／２４の配分を使用した。

Blue Coatが主張したことは、各ボックスが“機能”を表し、各機能は同一の

価値を有するものとして処理されるというLayne-Farrar博士の仮定をサポートする証拠がないことである。しかし、トライアルで、Layne-Farrar博士が証言したことは、その仮定は、“安全はWeb Gateway：機能”を表題が付けられたBlue Coat自身のダイヤグラムに基づいており、構造的ダイヤグラムの使用を説明し、侵害及び非侵害であるダイヤグラム内の部品を確認した、Finjanの技術的専門家である、Medovic氏と議論したことと同様である、ということである。また、Layne-Farrar博士は、Blue Coatの技術者のデポジションを信頼していることを証言し、デポジションにおいて、その技術者は、争点となっているダイヤグラムが、Secure Web Gateway機能の全範囲を表していることを述べた。このような証拠に基づいて、Layne-Farrar博士は、Blue Coatのダイヤグラムで識別された２４個の”機能“を分析し、各機能が同様の価値を有すると考えた。

Blue Coatは、Layne-Farrar博士の結論が、Blue Coatの製品部門も副社長であるShoenfeld氏の証言と矛盾することも指摘したが、Shoenfeld氏は、ダイヤグラムの各ボックスは、“背後に潜む大変多くのことを持つことができ、...、それで、これら[ボックス]には同等の重みはない...”。 J.A. 40756参照。しかし、証言矛盾の存在は、損害額認定が実質的証拠によりサポートされていないことを意味しない。陪審員は、特許権者の専門家を信じる権利がある。’731特許と’633特許の侵害に対する陪審員による損害額認定は、実質的証拠に基づくものであった[2]。

一部認容、一部破棄、そして、差し戻し。

コスト

各当事者は自身のコストを負担する。

[2] また、Blue Coat が主張したことは、Finjan の損害額専門家により提示された評価額以上の損害額を陪審員が認定したため、損害額は無効である、ということである。確かに、Finjan の損害額専門家は、’731 特許の侵害に対して、2,979,805 ドルから 3,973,073 ドルの範囲、’633 特許の侵害に対して、833,350 ドルから 1,111,133 ドルの範囲を提示した。J.A. 125. しかし、陪審員は、’731 特許に対して 6,000,000 ドル、’633 特許に対して 1,666,700 ドルを認定した。本法廷が Blue Coat の意見に同意することは、“合理的実施料と変わらない事件で”損害額を認定する法律上の方向性は、特許権者に対して、合理的証拠の認定をサポートする必要がない、という意見についてである。合衆国法典 35 編 284 条。陪審員は、記録によりサポートされたこと以上を認定することはできない。しかし、ここで、その記録には、専門家の評価額が保守的であるという証拠と、基礎となる証拠がより高い認定額をサポートするという証拠が含まれる。J.A. 40619-20, 40656.

３．101 条拒絶に対する対応策

（１）判決内容

本事件においても、Alice 判決の第１ステップ（抽象的アイデアに向けられているか否か）を判断するに際して、Enfish 判決に規範（「クレームが、コンピュータ装置の能力における特定の改善に向けられているか否か」）を用いて、特許適格性を判断している。

すなわち、CAFC は、’844 特許のクレーム１に関し、「セキュリティプロファイルには、“行動ベース”のウィルススキャンによって生成される、潜在的に悪意のある操作についての情報を含まなければならない」とし、「この操作は、伝統的な“コードマッチング”ウィルススキャンとは区別され、そのスキャンは、ダウンロード可能なものの中のコードと既知の不審コードデータベースとを比較することによって、それまで特定されたウィルスの存在を把握することに限定される」ものとして、このような「’844 特許におけるこの行動ベースのウィルススキャンは、コンピュータ機能の改善を構成するか否か」を論点と考えた。

そして、CAFC は、「セキュリティプロファイルアプローチは、異なるユーザに適合したアクセスを許容し、ユーザコンピュータにファイルが到着する前に、脅威を識別することを保証している。セキュリティプロファイルが“不審コードを識別する”という事実は、システムに対して、新たに利用可能な、潜在的脅威についての行動ベースの情報を蓄積させ、利用させることを許容する。したがって、主張クレームは、はっきりとコンピュータセキュリティという抽象的アイデアというよりも、むしろ、コンピュータ機能に対する非抽象的な改善に向けられている。」と判示した。

つまり、CAFC は、「既知のウィルスを単に探索する伝統的な“コードマッチング”システムと異なり」、クレーム１に記載した「“不審コードを識別する”」ことで、ダウンロードファイルがユーザコンピュータに到着する前に、悪意あるコードなどの脅威を識別することを保証することから、これがコンピュータ機能に対する改善に向けられている、と判断した。

したがって、CAFC は、Enfish 判決の規範を利用して、Alice ステップの第１ステップは、「NO」（＝抽象的アイデアに向けられていない）と判定されるから、第２ステップを検討するまでもなく、’844 特許のクレーム１は特許適格性あり、

と判断した。

なお、CAFCは、*Apple*事件（*Apple, Inc. v. Ameranth, Inc.* 842 F.3d 1229, 1240-41 (Fed. Cir. 2016)）や *Affinity Labs*事件（*Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016)）など、特許適格性なしと判断された過去の判例を引用して、'844 特許の特許適格性がないことを主張したBlue Coatの主張にたいしても反論した。

すなわち、CAFC は、「そのような結果や効果を生む実用的な方法や手段の発見に対して」特許が発行されている（*Corning v. Burden*, 56 U.S. 252, 268 (1853)）ことから、*Apple*事件等では、「イノベーティブな結果であっても、結果そのものは特許可能ではない。」と判示し、Blue Coatの主張を認めなかった。

（２）101条拒絶に対する対応策

本判決においても、McRO事件等と同様に、Enfish事件の規範（「クレームが、コンピュータ装置の能力において特定の改善に向けられているか否か」）により、Aliceテストの第１ステップを判断している。

とくに、本判例では、クレームのある特定部分（「不審コードを識別する」）に着目し、その部分がコンピュータ機能の改善（＝既知のウィルスを単に探索する伝統的な“コードマッチング”システムと異なり、ユーザコンピュータにファイルが到着する前に、脅威を識別する）を保証すると指摘している。

このようなコンピュータ機能の改善が特許明細書に記載されているかは、本判決からは判然としない。しかし、少なくも、101条の拒絶理由が通知された場合は、クレームのある部分に着目して、従来技術と比較して、どのように異なるのか、そして、どのような技術的改善があったのか、を具体的に主張することで、Aliceテストの第１ステップで「NO」（抽象的アイデアに向けられていない）と判定され、101条拒絶を解消できるものと思われる。

以　上