

SRI INTERNATIONAL, INC.,

*Plaintiff-Appellee*

v.

CISCO SYSTEMS, INC.,

*Defendants- Appellants*

2017-2223

[CAFC 2019. 7. 12 判決(2019. 3. 20 判決後に再審理請願が認められた後の命令)]

新横浜総合特許事務所

弁理士 山下 聡

## 1. 概要

### (1) 経緯

コンピュータネットワークのイベント監視（“EMERALD”）など、ネットワーク侵入検出技術などの開発を行う SRI International, Inc（以下、“SRI”）は、米国特許 6,484,203（以下、“’203 特許”）、6,711,615（以下、“’615 特許”）を侵害とするとして、Cisco Systems Inc（以下、“Cisco”）を被告とする特許侵害訴訟をデラウェア州連邦地方裁判所（以下、“地裁”）に提起した。’615 特許は、’203 特許の継続出願である。

訴訟提起後、Cisco は、特許非適格であること及び新規性がないことを主張するサマリージャッジメントの申立を行った。地裁は、特許非適格性についてはその申立を棄却し、新規性については新規性ありとするサマリージャッジメントを判示した。

また、地裁は、’615 特許のクレーム 1, 2, 13, 及び 14 と、’203 特許のクレーム 1, 2, 12, 及び 13 に関する侵害、有効性、及び故意侵害に関する陪審裁判を行った。陪審員は、Cisco が製造販売する製品が直接及び間接に特許を侵害し、合理的実施料率（3.5%）、填補損害賠償（23,660,000 \$）を認定した。

その後、地裁は、Cisco が申立てた、故意がないとする JMOL を棄却し、損害額を 2 倍にした。地裁は、SRI が申立てた、弁護士費用、強制実施権、及び審理

前利息についても認定した。

Cisco は、地裁が判示した、

- 1) 101 条による特許非適格性に関するサマリージャッジメントの申立の棄却、
- 2) クレーム用語“ネットワークトラフィックデータ”の解釈、
- 3) 新規性ありとするサマリージャッジメントの認定、
- 4) 法律問題として故意侵害がないという判断の否認、
- 5) 損害賠償額の増額、弁護士費用、及び継続的実施料に関する認定、

を不服として、CAFC へ控訴した。

以下では、特許適格性に絞って解説する。

## (2) 争点

トラフィックデータの分析に基づいてネットワーク上の異常行動を検出する階層的イベント監視及び分析に関するコンピュータ自動化方法に関する発明（’615 特許のクレーム 1）は、米国特許法 101 条の要件を満たすか。

’615 特許のクレーム 1 を以下に示す。

1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:  
    deploying a plurality of network monitors in the enterprise network;  
    detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};  
    generating, by the monitors, reports of said suspicious activity; and  
    automatically receiving and integrating the re-ports of suspicious activity, by one or more hierarchical monitors.

1. 企業ネットワーク内の階層的イベント監視及び分析に関するコンピュータ自動化方法であって、

前記企業ネットワーク内に複数のネットワークモニタを配置し、

前記ネットワークモニタによって、1つ以上の以下のカテゴリ：{ネットワークパケットデータ伝送コマンド、ネットワークパケットデータエラー、ネットワークパケットデータ量、ネットワーク接続要求、ネットワーク接続拒否、ネットワークパケットに含まれるエラーコード、ネットワーク接続確認、及び既知のネットワークサービスプロトコルを支持するネットワークパケット} から選択されたネットワークトラフィックデータの分析に基づいて、不審なネットワーク行動を検出し、

前記モニタによって、前記不審行動のレポートを生成し、

前記1つ以上の階層モニタによって、前記不審行動に関するレポートを自動的に受信し統合する、

ことを特徴とする方法。

## 2. 判決内容

デラウェア州連邦地方裁判所 No. 1:13-cv-01534-SLR-SRF, Sue L. Robinson  
裁判官からの控訴

担当 LOURIE 裁判官、O' Malley 裁判官、及び STOLL 裁判官

STOLL 裁判官により提出された法廷意見

LOURIE 裁判官により提出された反対意見

STOLL 裁判官

本事件は、特許事案における最終判決からの控訴である。Cisco Systems Inc (“Cisco”) は、以下に示す地裁判決に対して控訴した：(1) 101 条による特許非適格性に関するサマリージャッジメントの申立の棄却、(2) クレーム用語“ネットワークトラフィックデータ”の解釈、(3) 新規性ありとするサマリージャッジメントの認定、(4) 法律問題として故意侵害がないという判断の否認。Cisco は、損害賠償額の増額、弁護士費用、及び継続的実施料に関する地裁の認定も控訴した。

本法廷は、特許非適格性に関するサマリージャッジメントの申立を棄却した地裁の判断を支持し、“ネットワークトラフィックデータ”に関するその解釈を承認し、新規性があるとするサマリージャッジメントの判断を支持する。本法廷は、法律問題として故意侵害がないとする地裁の判断を破棄及び差し戻し、従っ

て、地裁による損害額の増額の判断についても破棄する。また、本法廷は、地裁による弁護士費用の認定も破棄し、再計算のために差し戻す。最後に、本法廷は、実際に侵害と認定されたか些細な差異しかない販売後の製品に関する継続的実施料の判断を支持する。したがって、本法廷は、一部支持し、一部破棄し、本判決と矛盾しない更なる手続のために差し戻す。

## 背景

### I

コンピュータネットワークの相互接続性は、権限あるユーザに対するアクセスを促進させる一方で、ハッカー、マルウェア、及び他のセキュリティ脅威からの攻撃に対するネットワーク感染を増加させた。あるセキュリティ脅威は、複数ソースからの情報によってのみ検出される。例えば、ハッカーは、ネットワーク内のコンピュータやモニタにログインを試みようとする。各コンピュータのログイン試行回数は、警報のトリガーとなる閾値よりも低くなる場合があり、ネットワーク内の単一のモニタ位置での様子を観察することは、このような攻撃の検出を困難にさせている。この課題を解決するために、SRI は、米国特許 6,484,203, 6,711,615 でクレームされた発明を発展させた。’615 特許（“ネットワーク監視”とのタイトル）は、’203 特許（“階層的イベント監視及び分析”とのタイトル）の継続出願である。

### II

SRI は、特許訴訟を提起する前は、ネットワーク侵入検出に関する重要なリサーチと開発を行ってきた。実際、異常な生活妨害に反応することが可能な、SRI のイベント監視（“EMERALD”）プロジェクトは、この技術分野で注意を引くものであった。EMERALD の資金を援助した米国国防高等研究計画局は、このことを、“サイバー防御の世界における宝石”、以前の技術を“超える量子跳躍的改善”と呼んだ。J.A. 1272-73 at 272:16-17, 273:7-9. SRI は、1997年11月、第20回国際情報システムセキュリティカンファレンスにおいて、“EMERALD：異常な生活妨害に反応することが可能なイベント監視”とのタイトルの論文（“EMERALD 1997”）を提出した。

EMERALD 1997 は、EMERALD システムに関する概念的な概観を表している。それは、SRI が初期にリサーチした侵入検知技術における詳細について記述しており、次世代技術の開発を概説する。*SRI Int’l Inc. v. Internet Sec. Sys., Inc.*, 647 F. Supp. 2d 323, 334 (D. Del. 2009). 両当事者は、EMERALD 1997 が合衆国法典 35 編 102 条(b)により従来技術を構成する、ということについて争わなかった。EMERALD 1997 は、表面的には、’615 特許の参考文献としてリスト化されている。

### III

2つの特許は、ほぼ同一の明細書と、1998年11月9日という優先日とを共有する。SRIは、サマリージャッジメント段階で、'615特許のクレーム1-4, 14-16, 及び18と、'203特許のクレーム1-4, 12-15, 及び17を主張した。SRIは、トライアルの段階で、主張クレームを狭め、'203特許のクレーム1, 12, 及び13と、'615特許のクレーム1, 2, 13, および14を主張した。陪審員は、この狭い範囲のクレームについてのみ審議した。

両当事者は、異なる代表クレームを確認した。Ciscoは、'203特許のクレーム1を提案する一方で、SRIは、'615特許のクレーム1を提案した。2つの特許間の僅かな相違が控訴上のあらゆる争点にとって必須ではないように、これらのクレームは実質的に相似する。そのため、本法廷は、SRIの提案を採用し、'615特許のクレーム1を代表クレーム<sup>1</sup>として使用する。そのクレームは以下のように記載する。

1. 企業ネットワーク内の階層的イベント監視及び分析に関するコンピュータ自動化方法であって、

前記企業ネットワーク内に複数のネットワークモニタを配置し；

前記ネットワークモニタによって、1つ以上の以下のカテゴリ：{ネットワークパケットデータ伝送コマンド、ネットワークパケットデータエラー、ネットワークパケットデータ量、ネットワーク接続要求、ネットワーク接続拒否、ネットワークパケットに含まれるエラーコード、ネットワーク接続確認、及び既知のネットワークサービスプロトコルを支持するネットワークパケット}から選択されたネットワークトラフィックデータの分析に基づいて、不審なネットワーク行動を検出し；

前記モニタによって、前記不審行動のレポートを生成し；及び

前記1つ以上の階層モニタによって、前記不審行動に関するレポートを自動的に受信し統合する、

ことを特徴とする方法。

'615特許、col. 15 II. 2-21

SRIがCiscoに対して'615特許と'203特許の侵害訴訟を提起した後、Cisco

---

<sup>1</sup> 2つのクレーム間の僅かの相違は、検出節である—'615特許のクレーム1は、列挙されたカテゴリの“1つ以上”から選択されたネットワークトラフィックデータを許容し、そのリストに2つの特別なカテゴリ：“ネットワーク接続確認”と“既知のネットワークサービスプロトコルを指示するネットワークパケット”を含む。Compare '203 patent col. 14 ll. 19-35 (claim 1), with '615 patent col. 15 ll. 2-21 (claim 1).

は、クレームが特許非適格、EMERALD 1997 がクレームと同一であるということを含む、幾つかの争点に関するサマリージャッジメントの申立を行ったが棄却された<sup>2</sup>。 *SRI Int’l, Inc. v. Cisco Sys., Inc.*, 179 F. Supp. 3d 339 (D. Del. Apr. 11, 2016) (“*Summary Judgment Op.*”). 地裁は、Cisco の申立を棄却し、その代わり職権で、SRI に賛成して、同一ではないというサマリージャッジメントを認定した。

地裁は、損害額と同様に、’615 特許のクレーム 1, 2, 13, 及び 14 と、’203 特許のクレーム 1, 2, 12, 及び 13 に関する侵害、有効性、及び故意侵害に関する陪審裁判を行った。陪審員が評決したことは、Cisco の侵入検知システム (“IPS”) 製品、Cisco の遠隔管理サービス、Cisco の IPS サービス、ソースファイアの IPS 製品、及びソースファイアの専門サービスは、主張クレームを、直接及び間接に侵害している、ということである。陪審員は、合理的実施料として 3.5%、填補損害賠償 (compensatory damages) として合計 23,660,000 \$ を認定した。陪審員は、Cisco による侵害が故意であるという明白で説得力のある証拠も認定した。

陪審審理後、地裁は、故意がないとする JMOL の、Cisco による再申立を棄却した。 *SRI Int’l, Inc. v. Cisco Sys., Inc.*, 254 F. Supp. 3d 680, 717 (D. Del. 2017) (“*Post-Trial Motions Op.*”). 故意であるとする評決に基づいて、地裁は、“ある強化が Cisco の訴訟行為には適切である”、“Cisco はサマリージャッジの間、全ての争点を失ったという事実”、及び“SRI とそのビジネスモデルに対して明白な侮辱”、ということを否認した。 *Id.* at 723. そして、地裁は、損害額を 2 倍にした。SRI が申し立てた弁護士費用、強制実施権、及び審理前利息についても認定した。

Cisco は、新規性あり、増額された損害額、弁護士費用、及び継続的实施料に関するサマリージャッジメントの認定と同様に、地裁のクレーム解釈、特許非適格性に関するサマリージャッジメントの棄却に対して控訴した。本法廷は、合衆国法典 28 編 1295 条 (a) (1) により管轄権を有する。

---

<sup>2</sup> 2 つの特許は、EMERALD 1997 に基づく多数の新規性に関する申立を生き延びた。特許庁は、審査手続において EMERALD 1997 を審査し、それを超える特許を発行した。 J. A. 32734 ¶ 47; J. A. 32814-15 ¶ 207. さらに、2 つの再審査において、特許庁は、EMERALD 1997 を超える主張クレームの有効性を審査し、再度、クレームは有効であることを決定した。 J. A. 32734 ¶ 47. さらに、 *SRI International Inc. v. Internet Security Systems, Inc.* 事件において、陪審員は、2 つの特許が EMERALD 1997 と同一ではないことを認定した。 647 F. Supp. 2d at 350. 地裁は、EMERALD 1997 が争点となるクレーム限定を開示しないという評決が専門家証言によりサポートされていないことを含む、JMOL を棄却した。 *Id.* 本法廷は、判決を除いて支持した。 *SRI Int’l Inc. v. Internet Sec. Sys., Inc.*, 401 F. App’x 530 (Fed. Cir. 2010).

## 検討

### I

本法廷は、クレームが特許非適格な発明の主題を記載しているか否かを最初から (de novo) レビューした。 *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1365 (Fed. Cir. 2018) (citing *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1338 (Fed. Cir. 2017)). 101条は、“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”として、特許適格性のある発明の主題を定義する。しかし、自然法則、自然現象、及び抽象的アイデアは、特許可能ではない。 *See Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 70-71 (2012) (citing *Diamond v. Diehr*, 450 U.S. 175, 185 (1981)).

特許が特許適格性のない発明の主題をクレームにしているか否かを決定するために、最高裁は、2段階フレームワークを確立した。最初に、争点となるクレームが抽象的アイデアのような特許不適格な概念に向けられているか否かを決定しなければならない。 *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). 次に、仮にクレームが抽象的アイデアに向けられている場合、本法廷は、“各クレームの構成要素を個別にかつ‘順番に結合して’、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’か否かを決定”しなければならない。 *Id.* (quoting *Mayo*, 566 U.S. at 79). 抽象的アイデアを特許適格性のある応用へ変換するために、クレームは、“‘それを適用する’用語を追加する一方で、抽象的アイデアを単純に記述すること以上のこと”をしなければならない。 *Id.* at 221 (quoting *Mayo*, 566 U.S. at 72 (internal alterations omitted)).

本法廷は、Aliceの第1ステップにおいて特許適格性争点を解決し、クレームが抽象的アイデアに向けられていないと判示する。 See *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016). 地裁が判示したことは、クレームは、インターネット上の既知のビジネス実務の実行を単純に記載すること以上に複雑であり、コンピュータネットワークの分野で特別な課題を解決するために必然的にコンピュータ技術に根付いているものとしてより良く理解される、ということである。 *Summary Judgment Op.*, 179 F. Supp. 3d at 353-54 (citing '203 patent col. 1 ll. 37-40; *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014)). (下線部は筆者が付した。以下同じ。) 本法廷は、地裁の判決に同意する。クレームは、コンピュータネットワークで発生する技術的課題ーネットワーク内でハッカーや侵入者の可能性を識別するーを解決するために、特別な技術ーネットワーク上でデータの特別な種別を分析する複数のネットワークモニタを用いて、モニタから

レポートを統合する一を用いることへ向けられている。

Ciscoの主張に反し、クレームは、複数のソースからデータを分析して不審な行動を検出することには向けられていない。その代わりに、クレームは、コンピュータネットワーク技術の改善に向けられている。確かに、代表クレーム1は、ネットワークモニタを用いて、ネットワークトラフィックデータの分析に基づいて、不審なネットワーク行動を検出し、不審な行動のレポートを生成し、階層モニタを用いてレポートを統合することについて記載する。’615 特許, col.15 II.2-21. “クレームの焦点は、コンピュータ能力において特別に主張された改善にある”一すなわち、リアルタイムでネットワークトラフィックを監視して、広範囲の攻撃を自動的に検出するネットワーク防御システムを提供することである。Enfish, 822 F.3d at 1335-36.

明細書は、クレームが技術的課題に対する技術的な解決策に向けられているという本法廷の結論を支持している。明細書で説明していることは、コンピュータネットワークが“容易で効率的な情報の交換をユーザに提供する”一方で、’615 特許, col. 1 II. 28-29, “ネットワークを価値あるものにする技術の相互利用性と複雑な統合は、ネットワークを攻撃し易いものにさせている”。Id. at col. 1 ll. 36-39. さらに、明細書が示唆することは、従来のネットワークにおいては、表面上、分散化された発動要件が広範囲に分配されたシステム上で世界的に損害の大きい効果一1980年代のARPRAネットワークや1990年代のAT&Tが衰退したように一を持つことができた。See id. at col. 1 ll. 43-47. 明細書において説明していることは、クレームにした発明は、従来のネットワークにおけるこのような弱点を解決する方向へ向けられ、“企業ネットワーク全体を横切る接続性に侵入や破壊を凶ろうとすることを含む、ドメイン間の接続に対するより世界的な脅威に対する認識に対するフレームワーク”を提供する、ということである。Id. at col. 3 ll. 44-48.

Ciscoは、クレームが3つの理由で抽象的アイデアに向けられている、ということを主張した。第1に、Ciscoが主張したことは、クレームが *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) 事件におけるクレームと類似し、データを収集及び分析するために必要とされる一般的ステップに向けられている、ということである。本法廷は、この意見には同意しない。*Electric Power* 事件のクレームは、コンピュータとコンピュータネットワーク自体の機能の改善というよりも、送電網の課題を解決する道具としてコンピュータを用いたものを記載している。Id. at 1354. 本法廷が判示することは、争点となるクレームは、DDR Holding 事件における特許適格性のあるクレームにより近い、ということである。DDR 事件において本法廷が強調したことは、“通常、期待される方法で動作するコンピュータネットワーク”に単に必要とされる



抽象的アイデア以上のものに向けられている、ということである。773 F. 3d at 1258. 争点となるクレームは、従来のコンピュータネットワークに関する通常の、期待される動作を実際には行わない。DDR 事件におけるクレームと同様に、クレームにした技術は、不審はネットワーク行動を検出し、不審行動に関するレポートを生成し、1つ以上の階層的なモニタを用いてレポートを受信及び統合することによって、“ルーチン的で従来から存在するイベント列を無効にする”。  
Id.

第2に、Ciscoは、発明が“コンピュータ機能自体に対する改善”を含まない、ということを主張している。*Enfish*, 822 F. 3d at 1336. *Alice* 事件では、最高裁は、ツールが未だ抽象的であるようなコンピュータを用いる、独立した抽象的アイデアにクレームが向けられている、と判示した。573 U.S. at 222-23. しかし、争点となるクレームは、ツールすなわち、コンピュータ上の従来から存在するアイデアを自動化することとして、コンピュータを用いたものには向けられてない。むしろ、代表クレームは、コンピュータネットワークセキュリティを改善するために特定の技術を記載することで、コンピュータとコンピュータネットワークの技術的な機能を改善する。

Ciscoは、主張クレームが一般的であるために、“人々の心の中を追加することが”できるステップを含み、主張によれば、クレームが抽象的概念に向けられていることを確認している。Appellant Br. 27-28 (citing *Capital One*, 850 F. 3d at 1340; *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F. 3d 1307, 1318 (Fed. Cir. 2016); *Cyber-Source Corp. v. Retail Decisions, Inc.*, 654 F. 3d 1366, 1371 (Fed. Cir. 2011)). 本法廷は、この主張に同意しない。争点となるクレームは、101条が除外する人間の活動に関する種別ではない。確かに、本法廷は、クレームに記載するように、ネットワークモニタを用いてネットワークパケットを分析することで不審活動を検出するための装備は人間の心にはない、というSRIの主張に同意しがちである。

本法廷は、クレームがAlice分析の第1ステップにおいて抽象的アイデアに向けられていないと判示するため、第2ステップには到達しない。*See Enfish*, 822 F. 3d at 1339. したがって、本法廷は、クレームに特許適格性があるという地裁のサマリージャッジメントを支持する。

II

(略)

III

(略)

IV

(略)

V

(略)

VI

(略)

結論

以上の理由により、本法廷は、主張クレームが特許非適格であるという、地裁のサマリージャッジメントの棄却を支持する。また、本法廷は、“ネットワークトラフィックデータ”に関する地裁のクレーム解釈に同意し、新規性があるという地裁のサマリージャッジメントの認定を支持する。本法廷は、Ciscoが主張クレームを故意に侵害しなかったという法律問題として当然の判決を求める再申立に対する地裁の棄却を破棄及び差し戻す。したがって、本法廷は、増額された損害額に関する地裁の認定を破棄する。また、本法廷は、増額された損害額と継続的实施料とを認めるという地裁の命令を支持する。最後に、本法廷は、弁護士費用に関する地裁の認定を破棄し、本争点に関する再計算のために差し戻す。

一部支持、一部破棄及び差し戻し

費用

費用は生じない。

## LOURIE 裁判官による反対意見

当裁判官は、クレームの特許適格性を判示する多数の決定に全面的に反対する。当裁判官の見解では、これらのクレームは明らかに抽象的である。実際、これらのクレームは、クレームが抽象的であると判示した *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016) 事件のクレームとほとんど変わらない。

多数の判決理由は、米国特許 6,711,615 (“615 特許”) のクレームに焦点を当てている。クレーム 1 は、以下のように記載する：

1. 企業ネットワーク内の階層的イベント監視及び分析に関するコンピュータ自動化方法であって、

前記企業ネットワーク内に複数のネットワークモニタを配置し；

前記ネットワークモニタによって、1つ以上の以下のカテゴリ：{ネットワークパケットデータ伝送コマンド、ネットワークパケットデータエラー、ネットワークパケットデータ量、ネットワーク接続要求、ネットワーク接続拒否、ネットワークパケットに含まれるエラーコード、ネットワーク接続確認、及び既知のネットワークサービスプロトコルを支持するネットワークパケット} から選択されたネットワークトラフィックデータの分析に基づいて、不審なネットワーク行動を検出し；

前記モニタによって、前記不審行動のレポートを生成し；及び

前記1つ以上の階層モニタによって、前記不審行動に関するレポートを自動的に受信し統合する、

ことを特徴とする方法。

同様に、本法廷が *Electric Power Group* 事件でレビューしたクレームは、“データを受信する”、“リアルタイムでイベントを検出及び分析する”、“イベントの分析結果とイベントの診断結果とを表示する”、“測定値を蓄積及び更新する”、及び“信頼性に関する合成指示を抽出する”ことを含む、8つのステップとともに、“広範囲に亘り相互接続された電力網上のイベントをリアルタイムで検出し、前記相互接続された電力網上のイベントを自動的に分析する方法”について記載する。 830 F.3d at 1351-52.

クレームは8つのステップを持ち、冗長であるけれども、収集、分析、及び表示のためのコンテンツまたはソースによって、情報を表示することを単に記述するだけである。 *Id.* at 1351. クレームが抽象的アイデアに向けられていると判示する際に、本法廷が論じたことは、“特定のコンテンツを限定する場合を含む情報を集めること（情報としてその特徴を変更しない）”は抽象的アイデア

である、ということである。 *Id.* at 1353. 特定の技術分野—電力網の監視—にクレームを限定することは、クレームを、抽象的アイデアに関する特許適格し得のある応用へ変換するには十分ではない。 *Id.* at 1354. 広い意味で記載したステップがコンピュータを必要とする範囲に対してのみ、そのクレームはコンピュータ技術に深く根付いていた。第2ステップにおいて、本法廷が判示したことは、クレームには、“新規なデータを生成する部品や方法に関する発明の集合”を必要とせず、“あらゆる発明的なプログラミングを実施”しなかった、ということである。 *Id.* at 1355.

本事案は、*Electric Power Group* 事件と区別することは非常に困難である。この事件のクレームは、コンピュータやコンピュータネットワークに関する機能を改善するというよりも、課題を解決するツールとしてコンピュータを用いるものとして記載されているのみであるということが多数意見において言及された。

争点となるクレームは、ネットワークモニタを配置し、異常ネットワーク行動を検出し、レポートを生成及び操作することとほとんど変わらない。異常行動の検出は、トラフィックデータの“分析”に基づいているが、クレームは、そのようなことをするための特定の手段に関して何も付加していない。クレームは、情報の移動を記載するのみである。コンピュータは、ツールとして用いられ、コンピュータ技術の改善については何も示されていない又はクレームされていない。コンピュータネットワークセキュリティを改善するために特定の技術については何も記述されていない。

当裁判官は、クレームが、ネットワークセキュリティを監視する抽象的アイデアに向けられており、Alice の第2ステップへ移行すると判示するだろう。しかしながら、*Electric Power Group* 事件のように、“クレームにおいては、明細書に照らして理解しても、既製の従来から存在する、コンピュータ、ネットワーク、及びディスプレイ技術以上のことは何も必要としない”。830 F. 3d at 1355. クレームは、“情報の種別と情報ソース”を記載するが、コンテンツやソースによる情報のこのような選択は発明概念を提供しない。 *id.* 明細書においてさらに明確になることは、クレームがコンピュータ、メモリ、プロセッサ、大容量蓄積装置を含む、汎用コンピュータ部品についてのみ依存する、ということである。 *See* ’ 615 patent, col. 14 ll. 50-57. 確かに、明細書からは、適切なメモリバス及び周辺バスを“慣用部品”と考えるだろう。 *Id.* col. 14 l. 55.

最後に、多数意見は、結果を成し遂げる手段ではなく、結果のみ記載する明細書から、言葉を引き合いに出し、かつ言い換えている。 *See, e.g., Majority Op.* at 9. しかし、クレームは、ネットワーク行動を監視することが可能なコンピュータに関する特定の方法について記載していない。 *Electric Power Group* 事

件で判示するように、本事件で争点となるような、特定の課題に対しあらゆる解決策を効果的にカバーする、結果に焦点を当てた、機能的なクレームは、しばしば、Alice テストに逆らう。830 F. 3d at 1356.

したがって、当裁判官は、Alice ステップの第2ステップで発明概念を有することなく、第1ステップで、クレームが抽象的アイデアに向けられている、と判示し、特許適格性に関する地裁の判決を差し戻すだろう。当裁判官は、争点となるクレームについて、特許適格性がないと判示するため、本事件で残った問題に到達することはないだろう。

### 3. 101 条拒絶に対する対応策

#### (1) 判決内容

CAFC は、

“We resolve the eligibility issue at *Alice* step one and conclude that claim 1 is not directed to an abstract idea. See *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016).”

と判示しました。

すなわち、争点となるクレーム（’615 特許のクレーム 1）について、Alice の第 1 ステップにおいて抽象的アイデアに向けられていないとして、特許適格性がある、と判示しました。

その理由は、

“The district court concluded that the claims are more complex than merely reciting the performance of a known business practice on the Internet and are better understood as being necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks. *Summary Judgment Op.*, 179 F. Supp. 3d at 353-54 (citing ’203 patent col. 1 ll. 37-40; *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014)). We agree. The claims are directed to using a specific technique—using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: identifying hackers or potential intruders into the network.”（下線部は筆者が付した）

すなわち、争点となるクレームが、コンピュータネットワークにおいて生じる特別な課題（ハッカーなどのネットワーク侵入者を識別すること）を解決するために、特別な技術（ネットワーク上の特別なデータ種別を各々分析する複数のネットワークモニタを用いて、モニタからのレポートを統合すること）を用いていることに向けられており、このことは、本事件のクレームと類似する DDR 事件

(*DDR Holdings, LLC v. Hotels.com, L.P.*, (Fed. Cir. 2014)) も判示している、ということです。

そして、CAFC は、

“Instead, the claims are directed to an improvement in computer network technology. Indeed, representative claim 1 recites using network monitors to detect suspicious network activity based on analysis of network traffic data, generating reports of that suspicious activity, and integrating those reports using hierarchical monitors. ’ 615 patent col. 15 ll. 2-21. The “focus of the claims is on the specific asserted improvement in computer capabilities” –that is, providing a network defense system that monitors network traffic in real time to automatically detect large scale attacks. *Enfish*, 822 F.3d at 1335-36.”、

“our conclusion that the claims are directed to a technological solution to a technological problem.”、及び

“Rather, the representative claim improves the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security.” (下線部は筆者が付した)

と判示しました。

すなわち、CAFC は、争点となるクレームが技術的な課題に対する技術的な解決策に向けられており、そのような特別な技術をクレームに記載することで、コンピュータ技術に対して特別に主張された改善（リアルタイムでネットワークトラフィックを監視して、広範囲における攻撃を自動的に検出すること）にクレームが向けられることになる、と判示しました。

CAFC は、以上の議論の結果、明確には判示しておりませんが、*Enfish* 事件 (*Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016)) で判示された枠組み (improvement in computer or other technologyがあれば、抽象的アイデアには向けられていないこと) により、争点となるクレームについては、抽象的アイデアに向けられていない、として、特許適格性を認めたものと考えます。

## (2) 101 条拒絶に対する対応策

CAFC は、争点となるクレームについて、「技術的な課題に対する技術的な解決策」に向けられて、「特別な技術」をクレームに記載していれば、或いは、「特別な課題を解決するために、特別な技術」を用いることにクレームが向けられていれば、「improving computer network security」や「improvement in computer capabilities」があることを示すことができる、と判示しています。

その際、CAFC は、明細書の記載から、「技術的な課題に対する技術的な解決策」にクレームが向けられているか否かをサポートすることも判示しております。

したがって、明細書の記載から、

- クレームが「技術的な課題に対する技術的な解決策」に向けられており、そのような課題を解決するために、「特別な技術」をクレームに記載している、又は

- クレームが、「特別な課題を解決するために特別な技術」を用いることに向けられている、

ことを示すことで、「improving computer network security」や「improvement in computer capabilities」がある、と主張することが可能となります。

そして、Enfish 事件の規範を利用して、「improvement in computer」があるから、Alice ステップの第 1 ステップで、クレームが抽象的アイデア（審査基準では“法的例外”）に向けられていない、ことを主張することが可能になります。

Enfish 事件にならって、「improvement in computer or other technology」を示せばよい、ということではなく、「技術的な課題に対する技術的な解決策」や「特別な課題を解決するために特別な技術」を用いることを示すことで、「improvement in computer or other technology」を示すことができる、という点で、本判決の意義があるものと考えます。

なお、本判決には、特許適格性について反対意見（争点となるクレームには特



許適格性がない) が提出されました。

確かに、争点となるクレームは、「分析」と「統合」が記載されていますが、具体的にどのように「分析」と「統合」を行うのかは記載されていません。

しかし、どのように「分析」と「統合」を行うことが特許になるかならないかを争うものとするれば、それは、米国特許法 102 条や 103 条で、争点とするればよいのであって、101 条で争点とすべきではないと考えます。

単に「分析」と「統合」をクレームに記載するだけのクレームであれば、102 条や 103 条によって引例を示すことで、どのように「分析」と「統合」を行わせるかを具体的に示すよう、出願人に促していく方が、建設的なように思うからです。

しかも、争点となるクレームには、ネットワークモニタを用いて「分析」と「統合」を行う、という技術的なことが記載されています。このようなクレームまで、101 条で拒絶することは、却って、米国特許商標庁に特許出願をするモチベーションが低くなり、イノベーションを促進させることにはならないと考えるからです。

以 上