侵害行為が国境をまたいで構成されるネットワーク関連発明の差し止め行為について

弁理士　湯浅　竜

要　約

クラウドサービス等のテクノロジーの進化に伴い，国境をまたいで構成されるネットワーク関連発明が増加している。日本国内で提供されるサービスにおいても，端末は日本国内にある一方で，サーバは日本国外にあるケースも多く，このようなサービスに関する発明について，特許権による保護が適切に行われることが重要となる。

国境をまたいで構成されるネットワーク関連発明については，域外適用や複数主体の観点から特許権侵害に関する議論が行われてきた。しかし，その一方で，特許権侵害が認められた場合の差し止め行為については，十分な議論が行われていない。本稿では，前半で国境をまたいで構成されるネットワーク関連発明の動向と特許権侵害に関する議論について整理を行い，後半では国境をまたいだ知的財産権侵害に関する判例等を参照する形で国境をまたいだ特許権侵害行為の差し止め行為の実現性について考察を行った。

目　次

１．はじめに

昨今，テクノロジーの進化に合わせてネットワーク関連発明が増加している。ネットワーク関連発明については，これまで特許権侵害の判断における域外適用の問題や複数主体の問題に関する議論が行われてきた(1)。

本稿では，国境をまたいで構成されるネットワーク関連発明を対象として，これまでの議論を振り返るとともに，早急な議論が必要と筆者が考える論点として「国境をまたいで実施されるネットワーク関連発明に対する権利行使の問題」について取り上げることとした。

ネットワーク関連発明が抱える問題や特許権侵害の判断に関する議論を紹介する前半部分では既存の議論を整理する中で複数主体の問題にも触れているが，本稿の主題となる「国境をまたいで実施されるネットワーク関連発明に対する権利行使」の議論に関しては，議論を単純化するため，単一主体による特許権侵害に絞って議論を行うこととする。

２．ネットワーク関連発明が抱える課題

２．１．ネットワーク関連発明の概要

はじめに，本稿における「ネットワーク関連発明」の定義を整理したい。例えば，「ネットワーク関連発明」の定義として，「ネットワークを介して接続された複数のコンピュータ（例えば，サーバ，クライアント等）の組み合わせによって実施され得る発明（物の発明と方法の発明の双方を含む。）」といった定義が行われている(2)。以下，具体的な事例をスマートフォン用アプリ（スマホアプリ）の例を挙げて説明する。

現在利用されているスマホアプリの多くは，ユーザからの入力操作の受け付けおよびユーザに対する画面表示等の出力のみをスマートフォン等のユーザ端末で行い，その他の処理をユーザ端末とネットワークで接続されたサーバで行っている。これは，ネットワークを介して接続されたユーザ端末とサーバという複数のコンピュータの組み合わせによって実施されており，前述の定義に当てはまるネットワーク関連発明である。

ネットワーク関連発明において，問題となる点の１つが冒頭で述べた複数主体の問題である。スマホアプリなどネットワークに接続するサービスを提供するサービス提供者は，自社で保有するサーバではなく，他社が保有するサーバを利用しているケースが多い。このようなサービスはクラウドサービスと呼ばれており，AmazonやMicrosoftなど大手IT企業の主力事業として近年急速に成長している。このような状況において，ネットワーク関連発明と複数主体の問題は密接に関係しているといえる。

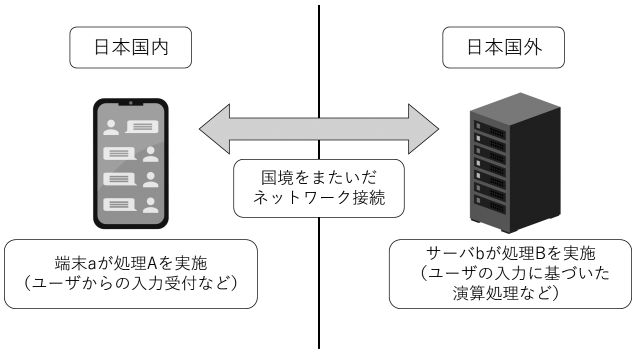
また，日本のユーザが使用するスマホアプリであっても，米国など日本以外の国に設置されたサーバを使用しているケースが頻繁に発生する。このケースが，本稿で主な論点とする「日本と海外の国境をまたいで実施されるネットワーク関連発明」となる。これは，アプリの提供者が海外法人の場合のみならず，アプリの提供者が日本法人の場合であっても同様である。

昨今のテクノロジー動向を加味すると，日本国内で利用される多くのスマホアプリやウェブサービスは，日本と海外の国境をまたいで実施されるネットワーク関連発明と捉えられる。

---

(1)　地代信幸ほか「クラウド時代に向いた域外適用・複数主体問題」パテント Vol.70 No.1（2017 年）
https://system.jpaa.or.jp/patents_files_old/201701/jpaapatent201701_039-053.pdf

(2)　平成 28 年度特許庁産業財産権制度問題調査研究報告書「ネットワーク関連発明における国境をまたいで構成される侵害行為に対する適切な権利保護の在り方に関する調査研究」
https://warp.da.ndl.go.jp/info:ndljp/pid/11064840/www.jpo.go.jp/shiryou/toushin/chousa/pdf/zaisanken/2016_11.pdf



国境をまたいだネットワーク関連発明の説明図

2．2．ネットワーク関連発明におけるサーバ設置国の特定の難しさ

日本と海外の国境をまたいで実施されるネットワーク関連発明に特有の問題として発生するのが，海外に設置されたサーバの設置国を特定する難しさである。

サービスの運用に利用されるサーバは，様々な条件によってその設置国が変更される。例えば，オンライン会議ツールの Zoom は，2020 年 4 月時点でオーストラリア，インド，ブラジル，アイルランド，カナダ，日本，中国，オランダ，ドイツ，シンガポール，香港，米国にデータセンターを設置しているが，有料アカウントのユーザはホストされるデータセンターの地域を選択可能となっている(3)。一方，無料アカウントのユーザはサービス提供者によりホストされるデータセンターを自動的に決定される。つまり，どの地域に住んでいるユーザであっても，どの地域のサーバを利用しているかが容易に特定できない状況となる。

また，データセンターなど大規模サーバの設置は雇用創出などによる経済効果を生むため，各国でサーバ設置の誘致競争が行われている。例えば，アイルランドは寒冷な気候によるサーバ冷却コストの安さ，通信インフラの安定性，データ・プライバシー保護法によるデータの安全性の確保などを強みとして，Google・Microsoft・Amazon・Apple など大手 IT 企業のデータセンターの誘致に成功している(4)。Google や Microsoft などネットワークを介して世界中にサービスを提供する企業は，今後もよりメリットの高い国や地域を適宜選択し，サーバ設置場所を変更していくと考えられる。

さらに，オリジナルのサーバに保存したデータを世界中に配置したキャッシュサーバにコピーしておくことで処理の負荷の分散を図る CDN（Content Delivery Network）などの技術を活用する場合，どの国のサーバで処理が行われているかを定義すること自体が非常に難しいという問題がある。

3．ネットワーク関連発明の侵害行為が国境をまたいで構成される場合の問題点

3．1．特許権侵害の域外適用が抱える問題の概要

特許権を始めとした知的財産権は，一般的に属地主義に基づいて運用が行われる。例えば，日本の特許権は日本における発明の実施にしか行使できず，米国の特許権は米国における発明の実施にしか行使できない，とする運用が一般的である。

また，特許権の直接侵害となる対象は，特許請求の範囲に記載された全ての構成を備えた物または方法のみに限られるのが原則である（オールエレメントルール）。請求項の構成要件のうち一部でも実施していな

(3) Zoom ヘルプセンター：ホストされるミーティングとウェビナーのデータセンター地域を選択する
https://support.zoom.us/hc/ja/articles/360042411451-%E3%83%9B%E3%82%B9%E3%83%88%E3%81%95%E3%82%8C%E3%82%8B%E3%83%9F%E3%83%BC%E3%83%86%E3%82%A3%E3%83%B3%E3%82%B0%E3%81%A8%E3%82%A6%E3%82%A7%E3%83%93%E3%83%8A%E3%83%BC%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%BB%E3%83%B3%E3%82%BF%E3%83%BC%E5%9C%B0%E5%9F%9F%E3%82%92%E9%81%B8%E6%8A%9E%E3%81%99%E3%82%8B

(4) IDA Ireland：グーグル（Google）社，アイルランド・ダブリンに 170 億円規模のデータセンターを新設
https://www.idaireland.jp/newsroom/google-data-centre-1

ければ，文言上は直接侵害にならないこととなる。

前項で説明したように，ネットワーク関連発明では，構成要件の一部（ユーザ端末での処理）がＡ国，残り（サーバでの処理）がＡ国外で実施されるケースが頻繁に発生しており，各国で登録された特許発明の構成要素の全てを実施する直接侵害が成立しにくくなっている。さらに，前述のように，サーバ設置国の特定が非常に難しい状況も発生する。

国境をまたいで構成されるネットワーク関連発明を保護するために，端末やサーバが設置される各国で特許権を取得するべきという議論もあるが，1）コストの問題で難しい，2）サーバ設置国の特定が難しい，などの問題があり，多くの企業にとっては現実的ではない。

各国で特許権を取得する以外の方法として，国内で実施させる構成要件のみで権利化すべきという議論もある（例えば，ユーザ端末で行われる処理のみで特許権を取得する）が，多くのプロセスがサーバ側で処理されることが多いサービスの場合，端末側の処理のみでは進歩性の主張が難しいケースが多い。

このような事情から，日本国内に向けて提供されるサービスにおいては，国境をまたいで構成されるケースにおいても日本の特許権で保護されるべきであり，法改正の必要性についても提言が行われている[(5)]。

表１　ネットワーク関連発明の侵害行為が国境をまたいで構成される場合の問題点の整理

	発生する問題の概要
1	属地主義に基づいた運用により，日本の特許権は日本における実施にしか行使できない。一方で，ネットワーク関連発明の多くが，一部の構成要件を日本国内，残りの構成要件を日本国外で行っているケースが多く，オールエレメントルールに基づく直接侵害にならない。
2	ネットワーク関連発明に使用される端末やサーバが設置される各国で特許権を取得すべきという議論がある。しかし，複数国で特許権を取得するためのコスト，サーバ設置国の特定が難しい，一部の構成要件のみでは進歩性の主張が難しいといった問題がある。

３．２．日本国における特許権侵害の域外適用に関する議論

（1）域外適用が直接関わる判例（インターネットナンバー事件）

日本の特許法には特許権の域外適用について言及した条項が規定されておらず，日本の特許権侵害の域外適用を争点とした判例も現時点では存在しない。

インターネットナンバー事件（知財高裁 H22.3.24）[(6)]は，地代信幸らによる論文[(7)]では，「域外適用の典型例でありながら，域外適用が争点とならなかった事件」と言及されている。本事件では韓国に設置されたサーバを利用したサービスに対して特許権侵害が認められ，サーバの除去命令が出ているが，サーバが韓国に設置されていることについては争点とならなかった。本事件の主な論点は侵害の主体が誰であるかとなっており，サーバへのアクセスを行う個別のユーザではなく，サービス提供者（韓国企業の日本法人）が権利侵害の主体となるという判断が行われており，複数主体の問題のみが議論される結果となった。

以下，同事件の判決文からポイントとなる点を引用する（下線は筆者による追加）。

> 本件発明は「アクセス」の発明ではなく，「アクセスを提供する方法」の発明であって，具体的にクライアントによるアクセスがなければ本件発明に係る特許権を侵害することができないものではない。また，本件発明に係る「アクセスを提供する方法」が提供されている限り，クライアントは，被控訴人方

(5)　地代ほか・前掲注１
(6)　インターネットナンバー事件（知財高裁 H22.3.24）
　　https://www.courts.go.jp/app/files/hanrei_jp/020/080020_hanrei.pdf
(7)　地代ほか・前掲注１

法として提供されるアクセス方法の枠内において目的の情報ページにアクセスすることができるにとどまるのであり，クライアントの主体的行為によって，クライアントによる個別のアクセスが本件発明の技術的範囲に属するものとなったり，ならなかったりするものではないから，クライアントの個別の行為を待って初めて「アクセスを提供する方法」の発明である本件発明の実施行為が完成すると解すべきでもない。
そうすると，被控訴人による「アクセスを提供する方法」が本件発明の技術的範囲に属するのである以上，被控訴人による被控訴人方法の提供行為が本件発明の実施行為と評価されるべきものである。
(3) そして，甲 60 及び弁論の全趣旨によると，平成 21 年 10 月 19 日の時点において，被控訴人は現に被控訴人方法を実施していることが認められるから，被控訴人は本件特許権を侵害する者であると認められる。したがって，控訴人は，被控訴人に対し，特許法 100 条 1 項に基づき，被控訴人方法による被控訴人サービスの提供の停止を請求するとともに，同条 2 項に基づき，被控訴人サービスに供された「NLIA サーバー」の除却及び「登録情報データベース」の消去を請求することができるといわなければならない。

(2) 複数主体の問題に関わる判例（電着画像事件，眼鏡レンズ供給システム事件，一太郎事件）

続いて，ネットワーク関連発明において，域外適用と並んで議論の対象となってきた複数主体に関連する判例を紹介する。

電着画像事件（東京地裁 H13.9.20）[8]は，「電着画像の形成方法」の特許発明に対して，構成要件の一部をユーザ（購入者）が行っているケースに関する判例である。本事件は，被告が購入者を道具として発明を実施しているとして，特許権侵害を認定した（道具理論）[9]。

以下，同事件の判決文からポイントとなる点を引用する（下線は筆者による追加）。

判示のとおり，被告が被告製品を製造・販売して，その購入者である文字盤製造業者をして被告製品を時計文字盤等へ貼付させる行為は，全体として本件特許権を侵害するものであり，また，本件特許権に無効事由があるとは認められないから，本訴請求において，原告が被告に対し，被告製品の製造・販売の差止め及び被告製品の廃棄を求める点は，理由がある。

眼鏡レンズ供給システム事件（東京地裁 H19.12.14）[10]では，レンズの発注側コンピュータと製造側コンピュータを含む権利に対して，被告は製造側コンピュータのみを管理している状態であったが，全体のシステムを支配管理しているのが被告であるという判断に基づいて，特許権侵害が認定されている（支配管理論）[11]。

以下，同事件の判決文からポイントとなる点を引用する（下線は筆者による追加）。

3) 争点 (1)（複数主体の関与）
ア ㋐本件発明 3 は，「眼鏡レンズの供給システム」であって，発注する者である「発注側」とこれに対向する加工する者である「製造側」という 2 つの「主体」を前提とし，各主体がそれぞれ所定の行為

(8) 電着画像事件（東京地裁 H13.9.20）
https://www.courts.go.jp/app/files/hanrei_jp/295/012295_hanrei.pdf
(9) 地代ほか・前掲注 1
(10) 眼鏡レンズ供給システム事件（東京地裁 H19.12.14）
https://www.courts.go.jp/app/files/hanrei_jp/513/035513_hanrei.pdf
(11) 地代ほか・前掲注 1

をしたり，システムの一部を保有又は所有する物（システム）の発明を，主として「製造側」の観点から規定する発明である。そして，「発注側」は，「製造側」とは別な主体であり，「製造側」の履行補助者的立場にもない（前提事実（3）ウ）。
㈠　この場合の特許請求の範囲の記載や発明の詳細な説明の記載は，2つ以上の主体の関与を前提に，実体に即して記載することで足りると考えられる。この場合の構成要件の充足の点は，2つ以上の主体の関与を前提に，行為者として予定されている者が特許請求の範囲に記載された各行為を行ったか，各システムの一部を保有又は所有しているかを判断すれば足り，実際に行為を行った者の一部が「製造側」の履行補助者ではないことは，構成要件の充足の問題においては，問題とならない。
㈡　これに対し，特許権侵害を理由に，だれに対して差止め及び損害賠償を求めることができるか，すなわち発明の実施行為（特許法2条3項）を行っている者はだれかは，構成要件の充足の問題とは異なり，当該システムを支配管理している者はだれかを判断して決定されるべきである。
イ　以上を前提に検討すると，被告が被告システムを支配管理していることは明らかであり，原告は，被告に対し，本件特許3に基づき，他の要件も満たす限り，被告システムの差止め及び損害賠償を求めることができる。

前記2つの判例は，いずれも複数主体に関する判例である。

本稿で着目するネットワーク関連発明では，サービス提供者とは異なる主体が提供するクラウドサーバ（Amazonが提供するAWSなど）が利用されるケースが多く，この複数主体の問題と密接に関係する。前記2つの判例を考慮すると，被告が提供するサービスにおいて，被告の所有物ではないサーバが使用される場合であっても，道具理論あるいは支配管理論が適用されると考えるのが妥当と思われる。

（3）直接侵害・間接侵害に関する判例（一太郎事件）

国内の判例紹介の最後に，ネットワーク関連発明で問題となるケースが多い直接侵害と間接侵害の議論について述べたい。

一太郎事件（知財高裁大合議H17.9.30）[12]は，被告人製品をインストールしたパソコンが特許権侵害品である場合に，被告人によるソフトウェアの提供が特許権侵害となるかが判断された事件である。本事件では，方法の発明に対して，その方法を実施することが可能な物を生産等することは間接侵害に当たると判断された一方で，その方法を実施することが可能な物を生産するために必要な物を提供することは間接侵害に当たらないと判断された。

以下，同事件の判決文からポイントとなる点を引用する（下線は筆者による追加）。

（3）本件第3発明についての特許法101条4号所定の間接侵害の成否
前記1のとおり，「控訴人製品をインストールしたパソコン」について，利用者（ユーザー）が「一太郎」又は「花子」を起動して，別紙イ号物件目録又はロ号物件目録の「機能」欄記載の状態を作出した場合には，方法の発明である本件第3発明の構成要件を充足するものである。そうすると，「控訴人製品をインストールしたパソコン」は，そのような方法による使用以外にも用途を有するものではあっても，

（12）一太郎事件（知財高裁大合議H17.9.30）
https://www.courts.go.jp/app/files/hanrei_jp/356/009356_hanrei.pdf

同号にいう「その方法の使用に用いる物…であってその発明による課題の解決に不可欠なもの」に該当するものというべきであるから，当該パソコンについて生産，譲渡等又は譲渡等の申出をする行為は同号所定の間接侵害に該当し得るものというべきである。
しかしながら，同号は，その物自体を利用して特許発明に係る方法を実施することが可能である物についてこれを生産，譲渡等する行為を特許権侵害とみなすものであって，そのような物の生産に用いられる物を製造，譲渡等する行為を特許権侵害とみなしているものではない。
本件において，控訴人の行っている行為は，当該パソコンの生産，譲渡等又は譲渡等の申出ではなく，当該パソコンの生産に用いられる控訴人製品についての製造，譲渡等又は譲渡等の申出にすぎないから，控訴人の前記行為が同号所定の間接侵害に該当するということはできない。

地代信幸らによる論文では，方法の発明を単独で実施できるサーバの製造は特許権侵害になり得るが，方法の発明を実行するためのサーバやクライアントを「製造するための」ソフトの製造や配布は間接侵害にはならないことが示唆されている(13)。

ネットワーク関連発明において，サービス全体を特許権の内容とした場合，サービス内の一部の構成要件を実行するためのサーバの製造等は間接侵害の対象とみなすが，前記サーバを動作させるためのプログラム等は，サーバを「製造するための」ソフトと同義と考えられ，間接侵害の対象とみなさないと捉えるのが妥当と思われる。

表２　日本国内の参考判例の整理

	主な論点
インターネットナンバー事件	韓国に設置されたサーバを利用したサービスに対して特許権侵害が認められ，サーバの除去命令が出された。侵害主体が外国の企業である点は論点となったが，サーバが国外にある点は論点とならなかった。
電着画像事件	構成要件の一部をユーザ（購入者）が行っているが，被告が被告製品の購入者を道具として実施していると考え，「特許発明の全構成要件に該当する全工程を被告自身により実施されている場合と同視して，本件特許権の侵害と評価すべきもの」として侵害を認定した。（道具理論）
眼鏡レンズ供給システム事件	レンズの発注側コンピュータと製造側コンピュータを含む権利に対して，被告は製造側コンピュータのみを管理しており，オールエレメントルールに従えば特許権侵害は成立しない。しかし，全体のシステムを支配管理しているのが被告であるという判断に基づいて，特許権侵害が認定されている。（支配管理論）
一太郎事件	方法の発明を単独で実施できるサーバの製造は特許権侵害になり得るが，方法の発明を実行するためのサーバやクライアントを「製造するための」ソフトの製造や配布は間接侵害にはならないことが示唆された。

３．３．海外における特許権侵害の域外適用に関する議論

（1）米国で域外適用の対応を規定した 273 条（f）

続いて，米国の判例から本稿の議論の参考となる事例を紹介する。日本の特許法との差異として，米国の特許法には，特許権侵害の域外適用について言及した第 271 条（f）が存在する。以下，日本特許庁による米国特許法第 271 条（f）の参考訳(14)を引用する。

(13) 地代ほか・前掲注 1
(14) アメリカ合衆国特許法（2015 年第 7 改正版）
https://www.jpo.go.jp/system/laws/gaikoku/document/mokuji/usa-tokkyo.pdf

米国特許法第 271 条（f）
(1) 何人かが権限を有することなく，特許発明の構成部品の全部又は要部を，当該構成部品がその全部又は一部において組み立てられていない状態において，当該構成部品をその組立が合衆国内において行われたときは特許侵害となるような方法により合衆国外で組み立てることを積極的に教唆するような態様で，合衆国において又は合衆国から供給した又は供給させたときは，当該人は，侵害者としての責めを負わなければならない。
(2) 何人かが権限を有することなく，特許発明の構成部品であって，その発明に関して使用するために特に作成され又は特に改造されたものであり，かつ，一般的市販品又は基本的には侵害しない使用に適した取引商品でないものを，当該構成部品がその全部又は一部において組み立てられていない状態において，当該構成部品がそのように作成され又は改造されていることを知りながら，かつ，当該構成部品をその組立が合衆国内において行われたときは特許侵害となるような方法により合衆国外で組み立てられることを意図して，合衆国において又は合衆国から供給した又は供給させたときは，当該人は，侵害者としての責めを負わなければならない。

米国特許法第 271 条（f）は，米国で登録となった特許発明について，米国外で組み立てるために米国内から構成部品を供給した場合に特許権侵害とみなすというものである。

（2）域外適用が直接関わる判例（ブラウザ特許事件，Blackberry 事件）

ブラウザ特許事件（Eolas Techs., Inc. v. Microsoft Corp）は，ソフトウェアコードがソフトウェア発明の構成部品に該当し，ソフトウェアコードのインストールが構成部品の組み立てに該当することを認定された事件である(15)。

被告である Microsoft は，原告が保有する特許に係る技術が搭載されたソフトウェアコードが書き込まれたディスクを米国外の OEM 企業に提供，OEM 企業がコンピュータにインストールしユーザに販売していた。本事件では，Microsoft が当該ディスクを米国外の OEM 企業に提供する行為が米国特許法第 271 条（f）のもと特許権侵害に当たると判断している。

この判例に基づき，米国で開発されたソフトウェアを他国のサーバで動作させた場合であっても，米国特許法第 271 条（f）の対象となるであろうとの示唆も行われている。具体的には，「米国においても日本企業がソフトウェア発明を権利化しておくことにより，米国の競合他社が米国内で開発した製品をもとに米国外へマーケット拡大を試みたとしても，当該日本企業の米国特許権に基づき，米国内のみならず，域外適用を認める米国特許法第 271 条（f）の規定により，日本を含む米国外のマーケット拡大をも防ぐこともできる」との見解が述べられている(16)。

Blackberry 事件では，プッシュ式で携帯電話へ配信するサーバによるメール配信システムの特許発明に対して，被告は無線で送信する配信サーバをカナダに設置し，その他のサーバおよび端末を米国に設置していた。

オールエレメントルールを厳密に適用するならば，端末で処理される要件は米国内での実施である一方で，配信サーバで処理される要件は米国外（カナダ）で行われているため，直接侵害に当たらないと考えられる。しかし，判決では，当該システムの制御が米国内で行われていること，また使用による利益を米国内で享受

(15) 河野英仁「国境を越えたソフトウェア・インターネット関連発明の法的保護」パテント Vol.58 No.5（2005 年）
https://system.jpaa.or.jp/patents_files_old/200505/jpaapatent200505_026-032.pdf
(16) 河野・前掲注 15

している点を根拠として直接侵害が成立する，との判断が行われた。本事件は，「米国における域外適用の典型的事件として挙げられる事件」と考えられている(17)。

（3）複数主体の問題に関わる判例（Akamai 事件）

Akamai 事件（Akamai Technologies, Inc. v. Limelight Networks, Inc.）米国最高裁 &CAFC（連邦巡回区控訴裁判所）は，「複数主体問題について直接侵害として認められる範囲が広がり，米国におけるネットワーク関連発明の利用性を向上させることとなった事件」である(18)。

本事件では，コンテンツをユーザに配信する方法の特許発明に対して，ステップの構成要素のうち，一部のステップを第三者であるユーザが実施しており，それ以外の構成要素を被告が行っていた。

上記状況に対して，CAFC と最高裁の間で判断が二転三転する結果となったが，最終的には被告による直接侵害であるとの判断が下された。

以下，CAFC と最高裁の判断の推移を「パテント 2017：クラウド時代に向いた域外適用・複数主体問題」より引用する（下線は筆者による追加）。

> CAFC では，一部のステップを実施し，他人に残りのステップを実施するようにしたら，一人で全ての構成要素を実施する直接侵害が成立していなくても，誘引侵害が成立するとして侵害を認めた。誘引侵害とは米国特許法第 271 条（b）「積極的に特許侵害を誘発する者は，侵害者としての責めを負わなければならない。」のことである。
>
> しかし最高裁では，全ステップを実行した直接侵害が成立していることが，誘引侵害が成立する条件である，いわば従属説を採用した。一部を実施して残りを他人に実施させたこの事件の場合，誘引侵害は成立せず，非侵害と判断した。
>
> ところが CAFC の差し戻し審では，全てのステップを被告が実施していなくても，第三者の行為に指示を出しており，指示者が利益を得ているのであれば「直接侵害」である，と判断した。

これにより，複数主体であるか否かではなく，指示者ないし利益享受者が誰であるかが侵害判断における最重要要素として考えられるようになった。

この判例を加味するならば，前述した電着事件（道具理論），眼鏡レンズ供給システム事件（支配管理論）で示唆された内容と同様に，サービス提供者とは異なる主体が提供するサーバが利用されるケースであっても，指示者ないし利益享受者が誰であるかが権利侵害の判断において重要と考えられるであろう。

(17) 地代・前掲注 1
(18) 地代・前掲注 1

表３　日本国外の参考判例の整理

	主な論点
ブラウザ特許事件	ソフトウェアコードがソフトウェア発明の構成部品に該当し，ソフトウェアコードのインストールが構成部品の組み立てに該当することを認定。Microsoft がソフトウェアコードが書き込まれたマスターディスクを米国外の OEM 企業に提供する行為が，米国特許法第 271 条（f）のもと特許侵害に当たると判断している。
Blackberry 事件	ユーザが利用する端末は米国にあるが，サービスに使用するサーバがカナダに設置されているケースでの特許侵害が問われた事件。「侵害システムの制御が米国内で行われ，使用による利益を米国内で享受している」点を根拠として「管理と使用」が米国内で行われていれば直接侵害が成立する，との判断が行われた。
Akamai 事件	全てのステップを被告が実施していなくても，被告が第三者に指示を出しており，その結果として利益を得ているのであれば「直接侵害」であるとの判断が下された。これにより，複数主体であるか否かは侵害の認定の際にそれほど大きな問題とはならず，指示者ないし利益享受者が誰であるかが侵害判断における最重要要素として考えられるようになった。

３．４．特許権侵害の域外適用のまとめ

ここまでまとめてきたように，日本では特許権侵害の域外適用について言及した条文が存在しておらず，特許権侵害の域外適用について直接見解が述べられた具体的な判例は出ていない。一方，米国では特許権侵害の域外適用に関わる判例が出てきており，オールエレメントルールにとらわれない形での判断が行われるようになってきている。

また，特許権と同じく知的財産権の一つである商標権については，WIPO から「インターネット上の商標及びその他の標識に係る工業所有権の保護に関する共同勧告」が 2001 年に出されており，インターネット上における標識の使用を特定国における使用と認めるか否かについては，「商業的効果（commercial effect）」の有無によって判断する旨が提言されている(19)。つまり，日本ユーザ向けのウェブサイトを国外のサーバで運用している場合においても，同ウェブサイトで使用される標識は日本で使用されているとみなすと考えられる。

米国の特許権侵害に関する判例や商標権に関する WIPO による共同勧告などを考慮すると，日本国においても特許権侵害の域外適用が今後認められる可能性は十分にあると考えられる。

４．ネットワーク関連発明の侵害行為が国境をまたいで構成される場合の差し止め行為に関する議論

４．１．外国における実施行為の差し止め行為の難しさ

国境をまたいで構成されるネットワーク関連発明に関しては，日本だけでなく権利保護を要する各国で特許取得を目指すべきという議論もあるが，「権利化コストが膨大にかかる」「サーバ設置国の特定の難しさにより，どの国で権利化を進めるべきかが不透明」という問題があり現実的な解決案ではない。

ここまでの議論を元にすると，日本を主な市場とするサービスへの特許権侵害に対しては，一部の構成要件が国外で実施される場合においても，日本の特許権に基づいて特許権侵害が認められる状況が望ましく，国外の特許権（米国）や特許権以外の知的財産権（商標）においては，その方向を見据えた運用が進んでいるように思われる。

これが認められた場合，特許権侵害が認められた後の権利行使，特に国外で実施される発明に対する差し止め請求の実効性に関する検討が急務であると考えられる。具体的には，国外で稼働するサーバの撤去などを行う必要があるが，前述のようにサーバ設置国の特定が難しいこと，設置国を特定しサーバが撤去できた

(19) 特許庁「インターネット上の商標及びその他の標識に係る工業所有権の保護に関する共同勧告」について
https://www.jpo.go.jp/news/kokusai/wipo/1401-037.html

としてもサーバ内で動作していたプログラムを他のサーバにコピーすることが容易で完全な撤去が難しいこと，といった問題が発生する。

4．2．外国における実施行為を差し止めるための方法に関する議論

（1）検索エンジンからの削除

ここから，国外での実施行為の差し止めを行う方法として，海外の判例から参考となる事例を紹介する。

カナダ最高裁による判決（Google 事件，Google v. Equustek）[20]は，知的財産権を侵害する製品のオンライン上での販売を差し止めるため，知的財産権侵害を行っている当該事業者ではなく，大手検索エンジンである Google に対して，当該製品の検索エンジンからの消去を命じた事件である。

元々は原告である Equustek が，同社の流通業者である Datalink を被告として侵害訴訟を行っていたが，Datalink が侵害製品の販売を継続したため，Equustek は Google に侵害製品を検索結果から削除するよう協力を求めた。Google はカナダ国内検索データベースから当該製品の販売につながるウェブサイトを削除したが，グローバル検索データベースからの削除は拒否したため，Equustek が Google を被告として裁判を起こした事件となっている。

本事件では，（1）差止行為は侵害行為の非当事者に対しても適用可能，（2）差止請求はカナダ国外に対しても適用可能，という判断がなされたことがポイントである[21]。

スマホアプリの多くは，Apple や Google が運営するアプリストアを介して提供され，両社のプラットフォームを介して課金などを行っている。カナダ最高裁の判決を考慮するならば，侵害製品へのアクセスを促す検索エンジンと同様に，Apple や Google 等のプラットフォーマーに対して差止請求を行うことにより，実質的な差止行為を行う方法が考えられるのではないか。

（2）ジオブロッキング

前項では，ユーザが知的財産権の侵害行為を行っているウェブサイトを知る機会やアクセスする機会を減らすために，検索エンジンから当該ウェブサイトを削除するという話を述べた。次に紹介するのは，より直接的にユーザが知的財産権の侵害行為を行っているウェブサイトへ接続できないようにするために，ブロッキングという技術を用いた事例である。

ブロッキングには複数の方法が存在する（検索エンジンからの削除もブロッキングとする場合もある）。例えば，ユーザが利用する DNS（Domain Name System）サーバにおいて，ブロッキング対象サイトのドメイン名に対する IP アドレスの対応付けを行わないようにする「DNS ブロッキング」や，ブロッキング対象サイトの IP アドレス向けの通信パケットを通信事業者において全て破棄してしまう「IP ブロッキング」，特定の URL への通信のみ遮断する「URL ブロッキング」などである[22]。

今回は，ジオブロッキングと呼ばれる技術を用いて所定の地域からコンテンツへのアクセスを制限することで，当該地域での知的財産権侵害を解消することにつながるのかについて，関連する判例を紹介しながら検討したい。

ジオブロッキングとは，インターネットコンテンツの配信に当たり，提供する事業者へのアクセスを試みる利用者の地理的位置により制限を加える技術である。例えば，特許権侵害を行っているサービスに対して

（20）Google Inc. v. Equustek Solutions Inc.
https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do

（21）ダニエル・アンソニー，鈴木晃治「『インターネットに国境はない』オンライン知的財産権侵害事件で Google に対する下級審の世界的差止命令をカナダ最高裁判所が支持」AIPPI Vol.63 No.2（2018 年）
https://www.smartbiggar.ca/_Archives/files/Mr_Suzuki_vol63_02.pdf

（22）Internet Society 日本支部「海賊版サイトをブロッキングするための 5 つの手法（その仕組みと限界および問題点）」（2018 年）
https://internet.watch.impress.co.jp/docs/special/1128898.html

ジオブロッキングを用いて日本からのアクセスを制限することで，国外に設置されたサーバの撤去などを行うことなく，侵害行為を差し止めることができる。

Spanski Enterprises, Inc. v. Telewizja Polska S.A. 事件[23]は，北米地域での放送権を他社が有する状況で，米国外から米国内で視聴できる形でコンテンツを配信した場合における著作権侵害が争われた事案である。

本事件では，被告である Telewizja Polska が制作したコンテンツについて原告である Spanski が北米地域での放送権を保有しており，被告がインターネット上で配信するコンテンツは北米地域からアクセスできないようにジオブロッキングをかけられていた。しかし，被告企業に在籍する社員が意図的にジオブロッキングを解除していたとして，原告が保有する当該コンテンツの米国での著作権を被告が侵害している旨の判決が下っている。

被告は北米地域へのジオブロッキングの解除によって米国での著作権侵害が認められるとすると，米国内のユーザの悪意によりジオブロッキングが回避された場合にも，被告による米国著作権の侵害となり得るとする反論を行ったが，裁判所は悪意を持つユーザに対して被告は直接的な管轄権を欠くなど，他の免責のための抗弁を主張し得るとの見解を述べた。つまり，実施者がジオブロッキングをかけているという事実を，他者が有する著作権を遵守しようとする態度とみなしたこととなる。

この解釈を特許権の侵害に転用するならば，特許権の侵害を行っている主体に対して適切な範囲のジオブロッキングを命ずることで当該国において権利侵害が行われている状態を解消し得る，と捉えることができるのではないか。

4．3．前述の方法の問題点および他の方法論の検討

（1）前述の方法の問題点

前項の「4．ネットワーク関連発明の侵害行為が国境をまたいで構成される場合の差し止め行為に関する議論」では，外国における実施行為を差し止める方法として，検索エンジンやアプリストアからの削除，ジオブロッキングによるアクセス制限を例に挙げたが，いずれの方法も完全に実施行為を差し止めることは難しい。

検索エンジンやアプリストアから特許侵害品を削除する方法は，侵害を行っている主体がウェブサイトの内容等を変更して差し止め行為を回避することが可能である。前述の Google 事件では，侵害行為を行っていた Datalink が，当該侵害製品を自社のウェブサイト内で別の新しいページに移動させ続けることで，Google が検索結果から削除する行為を妨害していた旨が報告されている[24]。

ジオブロッキングによって特許侵害品へのアクセスを防ぐ方法は，VPN（仮想プライベートネットワーク）等の技術を利用することにより回避することが可能である。前述の Spanski Enterprises, Inc. v. Telewizja Polska S.A. 事件では，ユーザの悪意によりジオブロッキングが回避される可能性を持ち出して被告が反論を行っている。

（23）Spanski Enterprises, Inc. v. Telewizja Polska, S.A.
https://www.cadc.uscourts.gov/internet/opinions.nsf/D8F6482BA5FA7E05852582440055BAEE/$file/17-7051-1720385.pdf

（24）ダニエル・アンソニーほか・前掲注 21

表４　ネットワーク関連発明の侵害行為が国境をまたいで構成される場合の差し止め方法の整理

	主な論点
検索エンジンからの削除	知的財産権の侵害を行っているサイト等自体には接続が可能だが，そこにたどり着くまでのコストを高めることで知的財産権の侵害行為を防止する。別サイトの作成などにより回避が可能。
ジオブロッキング	知的財産権の侵害を行っているサイト等自体への接続を防ぐことで知的財産権の侵害行為を防止する。VPN などの利用により回避が可能。

（2）他の方法論の一例（サイトブロッキング）

上記に鑑みて，国外での侵害を差し止める方法について，他の方法についても並行して議論を進めていくことが重要と考えられる。

他の方法の一例として，ジオブロッキングではなくサイトブロッキング（DNS ブロッキングや URL ブロッキング）を用いて，侵害行為を行っているサービス等へのアクセスを制限するという選択肢も考えられる。この方法を用いることで，差し止め行為における物理的なサーバ撤去が不要となるため，サーバ設置国の特定などが不要となる。

サイトブロッキングは憲法で規定されている通信の秘密との兼ね合いもあるが，日本でも既に DNS ブロッキングを用いる形で児童ポルノへのアクセスを防止する方法が使われており，特許権侵害行為への対応に用途を広げる可能性について議論する余地があるのではないだろうか。

５．おわりに

最後に，本稿の内容を改めて整理する。はじめに，一部の構成要素が国外で実施されるネットワーク発明が増えており，日本で取得した特許権の侵害行為が国境をまたいで行われるケースが危惧されている旨の説明を行った。続いて，国境をまたいだ特許権の侵害行為に対して，日本および米国の判例から参考となる事例を紹介し，日本を主な市場とした製品に対しては，国境をまたいだ実施行為に対しても日本で取得した特許権のみで特許権侵害を認める方向になっていく可能性がある旨を述べた。

上記を踏まえて，後半では国境をまたいだ実施行為に対する権利行使，特に差し止めの実効性に対する検討を行った。具体的には，検索エンジンやアプリストアからの削除，ジオブロッキング等の方法が差し止めの実効性としてはいずれも問題を抱えており，サイトブロッキングなど他の選択肢も合わせて検討するべきである旨の提案を行った。

本稿では一例としてサイトブロッキングを用いた差し止め行為の可能性に言及するにとどまっているが，本稿を一つのきっかけとして，他の方法も含めてさらなる議論が行われることを期待している。