クラウド時代における捜査機関によるデータの取得
――国際法的側面と国内法的側面から――

諏訪部　爽
（佐藤研究会４年）

はじめに

インターネットの普及や情報通信機器の発達に伴い、サイバー空間における犯罪が増加しており[1)]、その対策は喫緊の課題となっている。不正アクセスや電子計算機を対象とする、典型的なサイバー犯罪のみならず、通常の犯罪の実行過程においてもインターネットが利用される現状においては、あらゆる犯罪についてデータが証拠となる場合が考えられ、犯罪捜査のため、捜査機関が証拠としてデータを取得する手続を整備することが肝要になる。

欧州評議会（Council of Europe）においては、平成13年にサイバー犯罪に関する

条約[2]（convention on cybercrime、以下、「サイバー犯罪条約」又は単に「条約」という。）が採択されたところ、我が国でも、同条約締結に伴い、刑事訴訟法が改正され（以下、「平成23年改正」という。）[3]、捜査手法の情報化社会への対応がなされた。しかし、現在、サイバー犯罪条約採択の時点においてはもとより、平成23年の法改正の時点においてさえも、十分に想定されていなかった事態が生じている。クラウド・コンピューティング（以下、「クラウド」という。）の発達である。本論文では、クラウドの発達が捜査機関によるデータの取得にいかなる影響を与え、国際法及び国内法上いかなる問題が生じているのか、そして、その問題に対処するためにどのような解決策が存在するのかを明らかにする。

Ⅰ　問題の所在

1　クラウドの発達と捜査活動への影響

（1）　クラウドの意義と特徴

クラウドとは、「共有化されたコンピュータリソース（サーバ、ストレージ、アプリケーションなど）について、利用者の要求に応じて適宜・適切に配分し、ネットワークを通じて提供することを可能とする情報処理形態」[4]をいうとされ、一般的には、その利用者がスマートフォン等の端末自体にデータ処理を行うアプリケーションやデータを保存するのではなく、インターネット経由でクラウド事業者のサーバ上のアプリケーションに接続してデータ処理を実行しデータを保存することによって、任意の端末からいつでもデータにアクセスできることになるSaaSという形態のサービスが知られている[5]。

このクラウドが有する大きな特徴の一つが、「ロード・バランシング（load-balancing）」と呼ばれるシステムである[6]。これは、ユーザーのアクセスによるサーバへの負荷を軽減させ、サーバにおけるデータ処理の効率性を確保するために、自動的に単一のデータを分割し分散処理するものである。これにより、効率的なデータ処理がなされるとともに、データが単一のサーバに蔵置されないことから、ハッキングがなされにくいというセキュリティ上のメリットが生じる。

（2）　クラウドサーバに蔵置されたデータの取得に伴う問題

それでは、クラウドサービスの発達は、捜査機関によるデータの取得にいかなる影響を与えているのであろうか。

（a）押収対象となるデータ蔵置媒体の変化

クラウドの発達以前、データは被疑者等の利用している端末に保存されている場合が多く、捜査機関は、その端末を押収すれば、必要とするデータを取得することができた。しかし、データがクラウドサーバに蔵置されている場合、サーバには、アプリケーション自体や他のクラウド利用者のデータが蔵置されていることから、サーバの押収は、事業者の業務への支障が大きい上、物理的にも困難を伴う。押収後も、蔵置されている膨大なデータの分析は、捜査の効率性を阻害することになる。

（b）国家主権の侵害のおそれ

次に、Microsoft や Google 等の主要なクラウド事業者は、米国に本社を置いており、そのサーバも日本国外にあると考えられるため、我が国の捜査機関がかかるサーバにアクセスすることは、次章第１節で述べるように国際法上違法とされている執行管轄権の域外適用に当たり、サーバ所在国の国家主権を侵害する可能性がある。実際、後述する「Gmail 事件」[7] において、横浜地裁は、サーバへのアクセスは、サーバ所在国の「主権に対する侵害が問題になり得る」として「国際捜査共助を要請する方法によることが望ましい」とし[8]、控訴審である東京高裁もまた「国際捜査共助等の捜査方法を取るべきであった」として、これを違法と断じている[9]。

また、上記の海外のサーバにデータが蔵置されていることから生じる問題のほか、サーバの所在地を問わず、クラウドサーバにデータが蔵置されていること自体から生じる問題もある。それは、記録命令付差押えに応じるクラウド事業者（事業者が記録命令に応じなかった場合は、サーバの差押えに伴う刑訴110条の２第１号の処分を行う捜査機関）が、記録すべき電磁的記録にアクセスできない可能性が存在することである。米国では、いわゆるスノーデン事件以来、政府と協力関係にあった主要な米国内の IT 企業が、政府からの独立性を標榜して顧客のプライバシー保護を重視する方針へ転換したといわれている[10]。その結果、例えば、Apple と Google は、iOS8以降、暗号化の仕組みを変更し、自社自身でさえ、ロックされたスマートフォンに保存されたデータにアクセスできない仕様にした[11]。iCloud のサーバに蔵置されたデータには未だアクセスできるとされているが、そのようなデータも同様に暗号化されてしまう可能性はある[12]。その場合、記録命令付差押えや刑訴110条の２の処分を行うことはできなくなる。

（c）「ロス・オブ・ロケーション」

国家主権の侵害との関連では、「ロス・オブ・ロケーション（loss of location）」という問題もある[13]。前述のロード・バランシングによって、データが自動的に複数国間のサーバを移動し、複数国間のサーバに分割されて蔵置されるため、データの所在地を特定することが困難になる、という問題である。その結果、データの所在地が判明していることを前提とする国際捜査共助を行うことが困難となり、また、執行管轄権の範囲画定の基準となる属地主義の適用も難しくなる。そのため、事業者がデータを提出しない場合、捜査機関が直接サーバにアクセスしない限りデータの入手は不可能となる。

このように、サイバー犯罪条約及び平成23年改正では対応の困難な状況が、クラウドの発達をうけ、既に生じているのである[14]。

（3）　海外のクラウドサーバに蔵置されたデータの取得方法

上述した問題に対処するため、現在、海外のクラウドサーバに蔵置されたデータを取得する方法として、次の３つのものが考えられる。

（a）国際捜査共助

まず、第一に挙げられるのは、サーバ所在国との間の国際捜査共助である。この方法は、前記 Gmail 事件において、裁判所が推奨するものであり、国家主権の侵害の問題を生じさせないため、我が政府もこれによることが望ましいとしている[15]。もっとも、欧州評議会のサイバー犯罪条約委員会（the Cybercrime Convention Committee（T-CY））は、この方法によると、証拠の入手に通常６か月から２年を要し、非効率的だと指摘する[16]。被害者の生命の危険が存在する場合はもちろん、それ以外の場合でも、データには喪失又は破壊の危険がある以上、迅速な取得が欠かせない。したがって、国際捜査共助の手続の迅速化が進まない限り、別の方法を確立する必要がある。また、そもそも、前述した「ロス・オブ・ロケーション」の問題が存在するため、次章で説明するように、データの所在国がデータについて国家管轄権を有するとするならば、国際捜査共助を要請すべき相手国さえ確定できない事態も想定されるのである。

（b）提出命令

第二に、クラウド事業者に対する提出命令[17]（production order；条約18条）が考えられる。平成23年改正により創設された記録命令付差押え（刑訴99条の２，218条１項）は同条１項 a を担保するためのものであり[18]、我が国内法においては、

上記提出命令は記録命令付差押えに相当する。記録命令付差押えは実質的には英米法で用いられるサピーナ（subpoena）に近いとされているところ、英米法では裁判所侮辱罪による処罰という間接強制が予定されるため、実効性が確保できるのに対し[19]、記録命令付差押えは、サービス・プロバイダ等の協力的な事業者を想定しているため[20]、間接強制は規定されておらず非協力的な事業者との関係では実効性に欠けるおそれがある。もっとも、記録命令付差押えについて、間接強制の規定がないのは、被処分者が従わなかった場合には、記録媒体自体に対する、通常の差押えが予定され[21]、被処分者においてはかかる措置が取られると事業や顧客のプライバシー等に甚大な被害が及ぶため、命令に従うと期待されるからであるが[22]、国外にサーバが存在する場合には、事業者が記録命令に応じないときでも、差押えを行うことはできず、それゆえに、被処分者側の協力も期待しがたい。さらに、我が国に日本法人を設立しているクラウド事業者に対して、外国に所在するサーバに蔵置されているデータの記録命令付差押えを行うことについては、記録行為自体は命令を受けた私人によって行われるものであり、国家主権の侵害は生じない、とするのが政府見解であるが[23]、海外においては、後述するようにその適否が争われている[24]。

（c）国境を越えるアクセス

第三に、国境を越えるアクセス（transborder access；条約32条）によることが考えられる。まず、条約19条２項を受けて、平成23年改正で、電気通信回線で接続している記録媒体からの複写（以下、「リモートアクセスによる複写の処分」という。刑訴99条２項、218条２項）が規定されている[25]。もっとも、条約19条２項は「自国内にある他のコンピュータ・システム」への「捜索又はこれに類するアクセス」に関する規定であるから、「他国内にある他のコンピュータ・システム」への「捜索又はこれに類するアクセス」を認めるものではない。そのため、条約32条が、捜索・差押えを含むあらゆる捜査手法における国境を越えたデータへのアクセスが許される場合について規定している[26]。もっとも、サイバー犯罪条約は条約上規定されていない権限については承認するものでも排除するものでもなく（条約39条３項参照）[27]、同条以外の場合において他国の国家主権を侵害するか否かについては、後述するように、国際的に統一した見解があるわけではない[28]。

国境を越えるアクセスの方法による場合、まず、捜査機関がサーバに直接アクセスするのであるから、国際捜査共助におけるような非効率性や記録命令付差押えにおけるような実効性確保の問題は生じない。また、国際捜査共助を困難にす

る「ロス・オブ・ロケーション」の問題についても、捜査機関はサーバの所在地が判明していなくともアクセスすることはできるのであるから、対応することが可能になる。加えて、捜査機関は、単に被処分者のパスワードを用いて被処分者のアカウントにログインすることになるのであるから、提出命令における、被処分者のデータへのアクセス不能の問題にも対処できる。そのため、形式的に従来の執行管轄権に関する国際法上の原則に従うと国家主権の侵害のおそれがあり、また、サーバ所在国、事業者及び被処分者が知らない間に捜査機関がアクセスすることによる濫用や個人のプライバシー権等の基本的人権の侵害のおそれという[29]、それ自体として極めて重大な問題を伴うものの、国際捜査共助及び提出命令が含む問題点を克服できることに鑑みれば、クラウド時代において、国境を越えるアクセスを活用することは、なお検討に値する手段だといえる。

（4） クラウド証拠部会（CEG） 勧告

上で検討したように、海外にあるクラウドサーバに蔵置されたデータを取得するために現在考えられる方法については、いずれも検討を要する問題を含んでいる。このようなクラウド上の証拠へのアクセス方法が包含する問題の解決策を検討するため、2014年12月、T-CY 第12回総会は、クラウド証拠部会（Cloud Evidence Group（CEG））を設置した。この CEG は、2016年９月に T-CY に対して５項目からなる勧告（以下、「CEG 勧告」という。）[30] を示した。詳細については後述するが、その中には、加入者情報を対象とする提出命令に関するガイダンス・ノートの起草（勧告２）、サイバー犯罪条約第二追加議定書の起草準備（勧告５）が含まれている[31]。これらの勧告は上で検討した種々の問題の解決策として勧告されたものであることから、上記問題への対処のため、その勧告の国内法化の可能性を吟味することは欠かせないと思われる。上記勧告の内容を踏まえ、他国にあるクラウドサーバに蔵置されたデータを取得するために現在考えられる方法をいかに基礎づけ、実現を図るか、国際法、国内法双方の議論を視野に入れて検討する必要が生じているのである。

2　本論文の構成

ここまで、クラウド時代における捜査機関によるデータ取得をめぐる種々の困難と、それを克服するため、T-CY が既に解決策を講じようとしていることを示した。

CEG 勧告において示された対応は、本章第１節第３項で示した３つのデータ取得方法にそれぞれ対応させることができることから、本論文では、特に、提出命令及び国境を越えるアクセスを取り上げ、その内容について検討を試みる。国際捜査共助に関わる部分については、提出命令及び国境を越えるアクセスほどの効率化は望みにくい点、国家主権の侵害のおそれという検討されるべき重大な問題を含んでいない点並びに我が国の刑事訴訟法の解釈論及び立法論に関わらない点を考慮して、本論文では検討を割愛する。

そこで、第２章では、国際法的側面、すなわち、従来のサイバー空間における国家管轄権概念に関する判例及び学説を整理した上で、CEG 勧告に示された、他国にあるサーバに蔵置されたデータの提出命令、及び、他国にあるサーバへの国境を越えるアクセスが、その国家主権を侵害するのか、という問題について検討を加える。続いて、第３章では、国内法的側面、すなわち、提出命令及び国境を越えるアクセスの実施をめぐり、我が国刑事訴訟法上生じる問題について検討を加える。なお、結論については、第２章及び第３章において、提出命令及び国境を越えるアクセスそれぞれの項目の末尾で示すこととする。

Ⅱ　サイバー空間における国家管轄権概念

１　クラウドの発達と「国家管轄権」概念

（１）　国家管轄権の基本的理解

国家管轄権とは、国家主権の「具体的な発現形態」であり、「国家がその国内法を一定範囲の人、財産または事実に対して具体的に適用し行使する国際法上の権能」をいうとされる[32]。そして、対外関係法第３リステイトメント401節[33]は、国家管轄権を、①規律管轄権、②裁判管轄権、及び③執行管轄権の３つに分類している。そして、常設国際司法裁判所（Permanent Court of International Justice（PCIJ））は、ローチュス号事件において、いわゆるローチュス原則を判示している。すなわち、執行管轄権については、「国家は他国の領域においてその権限をいかなる態様によっても行使することができない」として、その域外適用を否定する[34]一方、規律管轄権については、「国際法は、国家に広い裁量を認めており、それは一定の場合に禁止規則によって制限されるにすぎない」とし、「それ以外の場合には、国家は自らが裁量かつ適当と考える原則を自由に採用することができる」と説示している[35]。

規律管轄権に関する原則については、管轄権行使を無制限に認める結果を導くものとして批判が強いが[36]、属地主義の他にも属人主義や客観的属地主義等が確立し、さらには米国が主張してきた効果理論もほぼ確立するなど、規律管轄権の適用範囲について国家の裁量は広いとされている。

これに対して、執行管轄権に関する原則については、学説上も争いがなく、執行管轄権の域外適用は厳格に禁止されるという理解はほとんど常識となっているといって差し支えない[37]。そのため、他国にあるサーバに蔵置されているデータの提出を、国内に所在する事業者に求める提出命令、及び、他国にあるサーバへの国境を越えるアクセスが執行管轄権の域外適用に当たるかが問題となるのである。

（2）　クラウドの発達がもたらした影響

もっとも、クラウドの発達がもたらした「ロス・オブ・ロケーション」の問題によりデータの所在地が確定できない状況が生じたことは、属地主義の適用を困難にさせ、これに伴い、領土権に根差す伝統的な国家管轄権概念の限界が明らかになりつつある。そこで、クラウドの発達した現状と、そのような伝統的な国家管轄権概念とは相容れないとして、従来の概念に根底から変化をもたらす新たな原則の確立を要する、とする「データ例外主義（data exceptionalism）」が主張されるに至っている[38]。

ただし、これに対して、クラウド上のデータは無形財産と有形財産の両方の性質を兼ね備えているものとして、それらの財産に対する属地主義の原則や国際私法の従来の適用方法をデータに対しても応用できるとする見解も存在する[39]。そのため、クラウドの発達により、国家の領土権に根差す伝統的な国家管轄権概念が変容したと一概にいうことはできず、国家の権限行使の形態ごとに検討するのが妥当であると思われる。

そこで、以下では、他国にあるサーバに蔵置されたデータの提出命令、及び、他国にあるサーバへの国境を越えるアクセスが執行管轄権の域外適用に当たり、他国の国家主権を侵害するのか、判例及び学説の動向について概観した上で、CEG 勧告の内容について評価することとする。

2　他国にあるサーバに蔵置されているデータの提出命令

（1）　判例及び学説の動向

他国にあるサーバに蔵置されているデータの提出を、国内に所在する事業者に求める提出命令については、判例及び学説上、執行管轄権の域外適用には当たらないということで、結論は一致している[40]。そこで、以下では、その理由について「データ例外主義」をめぐる議論を踏まえて紹介する。

まず、データ例外主義の立場の論者は、19世紀前半の米国連邦最高裁判事であったジョセフ・ストーリーの、①「全ての国家はその領域内において排他的な主権及び国家管轄権を有する」、② ①の帰結として、国家は「直接的に」領域外の人及び財産に影響を及ぼすことはできない、とする伝統的な領域主権原則に関する著名な見解[41] を提示した上で、「純粋に領域的な権限の行使を通じて、『間接的に』国外の人及び財産を規制することはできる」と指摘している[42]。国外の人や企業を規制するために自国内に所在するそれらの所有する財産に対して処分を執行することは、執行管轄権の域外適用には該当しない、というのである。もっとも、この見解は、執行管轄権の適用における属地主義の原則を変えるものではなく、伝統的な国家管轄権概念を確認するにとどまる。

これに対して、前述のデータ例外主義に異論を唱える立場からも、対外関係法第３リステイトメント442節１項(a)[43] 等を根拠に、データ所在国に関わらず、国家は提出命令に従わない自国内の事業者に対して自国内の財産の差押えなどをすることは従来の属地主義の原則に従って許されるものであって執行管轄権の域外適用には当たらず、データ例外主義に立たずともクラウド時代に対応できるとの主張が展開されている[44]。

また、ベルギー最高裁も、ベルギーの検察官から被疑者の加入者情報の提出要請（ベルギー刑事訴訟法46条の２第１項）を受けた米 Yahoo! 社が、その提出につき罰則を伴って義務付けられた（同条２項）事案において、ベルギーの領域内において事業を行っている事業者に対して、捜査官が国外に物理的に侵入することなく、ベルギー国内で同項を適用して罰金を科すことは執行管轄権の域外適用には当たらない、と判示している[45]。

このように、データ例外主義に立つか否かに関わらず、国外のサーバに蔵置されているデータについて提出命令によって事業者に提出を強制し、提出命令に違反したプロバイダに対して罰金を科す権限を行使することは執行管轄権の域外適

用には該当しないとされている

（a）私見

上述の締約国の国内判例及び学説における見解の一致自体は伝統的な国家管轄権概念に基づくものであることからすれば妥当といえよう。

もっとも、これらは、我が国の政府見解と同様に、プロバイダによるアクセスは私人によるアクセスであることから国家の行為ではないことを前提としているように思われるが、間接強制を伴う提出命令では、プロバイダは強制されてサーバにアクセスしているのであるから、プロバイダのアクセスを国家による行為とみなす余地があると思われるのである。すなわち、国家機関以外の行為が国家に帰属する場合として、行為者が①国に「完全に依存（complete dependence）」して当該行為者が事実上の国家機関といえる場合、又は、②「事実上国の指示に基づき、又は国による指揮若しくは支配の下で行動していた場合（in fact acting on the instructions of, or under the direction or control of, that State）」（国家責任条文草案８条）の２つの場合が国際法上認められているところ[46]、提出させる個々のデータを特定し、間接強制を伴う提出命令によって私人の国外サーバへの個々のアクセス行為に国家の「実効的支配（effective control）」が及び、少なくとも②の場合に該当する可能性を見出すことは十分可能であろう。このように、被処分者によるアクセスが国家の行為とみなされるならば、後述の国境を越えるアクセスと同様の問題状況が生じることとなり、執行管轄権の域外適用に当たり国家主権の侵害が生じるか否かは本章第３節で示す立場にかかってこよう。

（３） CEG 勧告

上記判例及び学説の動向を踏まえて、CEG 勧告の内容について紹介した後、評価を加える。

同勧告の紹介に先立ち、最初に、前提となる概念について整理しておこう。

サイバー犯罪条約上、捜査機関が入手するデータは「加入者情報（subscriber information）」（条約18条３項）、「通信記録（traffic data）」（条約１条 d）及び「通信内容（content data）」の３つに分類されている。そして、条約18条１項 a が定める「自国の領域内に所在する者[47]」に対する提出命令においては、データの種類を区別することなく「コンピュータ・データ」全般を対象としているが、同項 b が定める「自国の領域内でサービスを提供するサービス・プロバイダ」に対する提出命令においては、「加入者情報」のみを対象としている。加えて、CEG は、

これらのデータのうち「加入者情報」は、捜査上不可欠かつ最も頻繁に必要となる情報である一方で、通信記録及び通信内容に比して、プライバシーの重要性が高くないことを理由に、加入者情報の取得のための別個の制度を確立する必要性を指摘している[48]。そのため、CEG は、これらのデータの分類を前提として、提出命令制度の改善を試みている。

第一に、前述した勧告２に基づくガイダンス・ノート＃10では、加入者情報を対象とする提出命令に限定して条約18条の解釈を示している。まず、加入者情報の蔵置されているサーバが他国の領域内に所在するとしても、「自国の領域内でサービスを提供するサービス・プロバイダ」が「保有し又は管理している」限り、サイバー犯罪条約18条の適用を妨げるものではないという解釈を示し、国外サーバに蔵置された加入者情報に関する提出命令が許容されるものとしている。その上で、「自国の領域内でサービスを提供する」（同条１項ｂ）の意義について、「サービス・プロバイダが自国の領域内に所在する者に対しそのサービスを利用することを可能にし（例えば、そのようなサービスへのアクセスを遮断していない）、かつ、自国との現実的かつ実質的な連関（real and substantial connection）[49] を確立したとき」という解釈を示している[50]。これは、国外サーバにデータが蔵置されていたとしても、プロバイダへの提出命令を許容する点で判例及び学説の動向に合致している[51]。

第二に、勧告３は、「締約国及びオブザーバー参加国に加入者情報へのアクセスのための国内的手続を見直させ、それによってサイバー犯罪条約18条の完全な履行を確実にさせること」[52]、すなわち、加入者情報の重要性及びプライバシーの程度に鑑みて、加入者情報を対象とする提出命令の国内法における要件を他の種類のデータ（通信記録及び通信内容）又は他の種類の侵害的な捜査権限の発動に比して緩やかにさせることを実質的な内容とするものである[53]。これは、一部の締約国では、加入者情報の取得は警察又は検察官による命令で足りるという国内法を制定していることを背景としている[54]。

第三に、勧告４は、特に加入者情報の開示に関して、プロバイダと刑事司法当局間のより密接な協力を促進するための実践的措置をとることを内容とし、勧告５の第二追加議定書は、加入者情報の提出の要請、保全要請及び緊急要請に関する他国のプロバイダとの直接的な協力を許容する条項を含んでいる。これは、米国のプロバイダは、蔵置データ法（Stored Communications Act（SCA））の下（合衆国法典18編2702条参照）、外国の法執行機関から国際捜査共助を経ずに直接的に

データの開示要請を受けた際に「自発的な開示（voluntary disclosure）」をする運用がみられるが、現状では、条約18条がそのような要請の法的根拠となるものの、開示の基準が不明確であるため、国内的及び国際的枠組みを確立する必要性が生じていることを背景とする[55]。穏当な手法であり国家間の合意可能性が高いと思われる一方で、国際捜査共助のように相手国に対してデータの提出を要請するのではなくプロバイダとの直接的な協力によって比較的迅速なデータの取得が可能になることから、現実的な対処方法といえる。

（4）小　括

このように、他国にあるサーバに蔵置されているデータの提出命令による国家主権の侵害に関しては、判例及び学説上、これを否定するのが一般的な理解であり、CEG勧告の内容もそうした議論に沿うものであることから、国際法上の問題はほとんど生じないものと思われる[56]。その一方で、我が国ではデータの種類の区別を意識した議論はほとんどなされておらず、また、加入者情報取得の要件の緩和についても、令状主義との関係など憲法上の問題が生じ得るため、CEG勧告の実施にはなお国内法上の問題が存在している。この点については、次章において検討する。

3　国境を越えるアクセス

（1）判例及び学説の動向[57]

他国にあるサーバに国境を越えるアクセスをすることが執行管轄権の域外適用に当たるか否かについては、判例及び学説上対立があることから、以下では、まずそれぞれの内容について整理する。

（a）執行管轄権の域外適用該当性否定説

まず、他国にあるサーバへのアクセスについて、域外適用該当性を否定し、領域内における執行であるとする見解がある。このうち、限定的に域外適用該当性を否定する見解は、「当局が通常、国外に蔵置されているデータを現に画面に表示しているネットワークに接続されたコンピュータを発見した場合」には、「ディスプレイに表示されたデータはコンピュータの一時メモリに保存されており、それゆえ国内領域に蔵置されている」といえるため、ディスプレイに表示されたデータの取得は執行管轄権の域外適用ではないとする[58]。通常、コンピュータは処理するデータを必ずメインメモリに一時的に保存するところ、ディスプレイに

表示されているデータは、当該コンピュータのメインメモリに一時的に保存されているため、国内に蔵置されているといえるのである。

もっとも、この見解を前提としたとしても、捜索の着手時期をデータの取得時と解するか、データの閲覧時と解するかにより、結論に差異が生じる。すなわち、データの取得が捜索・差押えに当たり、データの取得時に捜索の着手が認められると解するのであれば、捜査機関がデータを取得する場合は域外適用に当たる。これに対して、データの閲覧が捜索・差押えに当たり、データの閲覧時を捜索の着手時期と解する立場に立つ場合、捜査機関が自らデータを取得してディスプレイに表示させたとしても、捜索の着手時においては、メインメモリに保存されており国内に所在するといえるため、当初からディスプレイに表示されていたか否かを問わず、常に域外適用に当たらなくなる。この立場は、通常の捜索においては、建造物に侵入するまで室内を捜査機関がみることはできず侵入時に捜索に着手されたと解されるところ、同様にデータの捜索についても、データを閲覧するまでデータの内容をみることはできず、捜索の着手が認められないことを根拠とする[59]。そして、実際に、捜索の対象である被疑者のコンピュータの所在地が不明な状況下で、FBI が当該コンピュータのメモリ内のデータを捜索し FBI に送信させるソフトウェアを当該コンピュータにインストールするために、捜索差押令状を請求した事案において[60]、米国政府は被疑者のコンピュータから収集された情報は裁判管轄区において初めて閲覧されるのであるから、その情報は「管轄区内に所在する物（property located within the district）」（連邦刑事訴訟規則41条（b）（1））に当たり、令状は適法に発付されると主張している。

この主張はデータの所在地を基準として領域内における執行とみている点において伝統的な国家管轄権概念と共通するが、それに対し、データ例外主義の立場からは、前述の提出命令に関する見解を類推することによって、領域内における執行とみている。すなわち、国境を越えるアクセスは、他国の領域内における伝統的な証拠物を対象とする捜索・差押え―他国の主権を侵害し許されないことに争いがない―とは異なり、むしろ、前述した、自国内から「間接的に」他国に影響を及ぼすにとどまる提出命令、及び、自国内又は国際公域から航空機、偵察衛星等を利用して物理的に他国の領域に侵入することなく当該他国内の情報収集を行う諜報・偵察活動に類似し、執行管轄権の他国内における適用ではない、とするものである[61]。これは、データの所在地が他国の領域内であっても、国家の権限の行使が領域内におけるものであることを理由に執行管轄権の域外適用に当た

らないとする点で、伝統的な国家管轄権概念と相容れない。

（b）執行管轄権の域外適用該当性肯定説

これらに対して、他国にあるサーバへのアクセスは、端的に、国外における執行であるとする見解がある。これは、外国の法執行機関によって自国にあるサーバにアクセスされることはデータ所在国が有する領域内の人及び財産を保護する利益を侵害する点で伝統的な建造物の捜索と同様の効果を有すること[62]を理由に域外適用に当たる、とするものである。前記事案において、連邦地裁は、データに対する捜索は、サーバの物理的な所在地である「住所及び地名を有する物理的な空間」で執行されるとした上で、対象物であるコンピュータ及び情報の所在地が分からない状況下における本件捜索は、「管轄区内」で執行されるとはいえない、と結論付け、前述の米国政府の主張を退けている[63]。これは、捜索の着手時期をデータの取得時と解する立場に立った上で、国境を越えるアクセスが、国外のサーバ所在地で執行されることを理由に域外適用に当たるとするものである。

もっとも、執行管轄権の域外適用に該当するとしても、伝統的な捜索・差押えを国外で行う場合と異なり、サーバへのアクセスは、捜査機関が他国の領域内に侵入することを要しないため、直ちに国家主権が侵害されると断ずるには疑問も残る。そのため、国家主権の侵害の有無を国家主権の意義に遡って検討する必要がある[64]。

この点、主権を「具体的・実質的な権利や利益を護るという必要に根差した権能」[65]と捉えることにより、国家主権が侵害される場合を限定する見解がある。この見解は、さらに二つに分かれ、まず一つは、他国内において、物理的損害が発生した場合に限り、国家主権が侵害されるとする[66]。いま一つは、物理的損害の有無にとどまらず利害関係者の利益侵害の有無を重視して、捜査機関が被処分者のアカウントのアクセス権限を適法に取得して行う国境を越えるアクセスについては、「アカウント保持者であれば問題なくアクセスが認められる範囲のデータを入手するにすぎず」「対象サーバにその本来予定している動作をさせるにすぎない」ためプロバイダの利益を害するものではなく、さらにアカウント保持者の利益についても「令状取得の際に考慮されている」ことからすれば、サーバ所在国がその領域主権に基づいて保護すべき領域内のプロバイダ及びアカウント保持者の利益は侵害されておらず、サーバ所在国の主権の侵害は認められないと説く[67]。

これに対しては、主権を「自国の領土についての一般的・抽象的支配」[68]とし

て捉えることにより、いかなる執行管轄権の域外適用も国家主権を侵害し許されないとする見解がある。この見解は、伝統的な見解に従ってローチュス原則を厳格に解釈した上で、属地主義以外の根拠に基づいて執行管轄権を適用することは許されず[69]、損害の発生の有無に関わらず単に国家が他国のサイバー・インフラストラクチャーに侵入したという事実自体が領域内の人及び財産を保護する利益を侵害し国家主権の侵害を生じさせるとするとして、前者の見解を批判する[70]一方、後者の見解に対しては、自国で犯罪を実行して他国に逃亡した被疑者について自国の方が利益を有していたとしても他国内で被疑者を捜索することが許されないのと同様に、国境を越えるアクセスを正当化するものではないと指摘している[71]。

(c) 私見

まず、データの複製がメインメモリに保存されていることを理由に、国内にデータが所在するとみる見解については、伝統的な国家管轄権概念に従っても、十分に認められるように思われる。ただし、捜索の着手時期をデータの閲覧時と解したとしても、そのことによって直ちに執行管轄権の域外適用に該当しないとはいえまい。アクセス行為が存在することは否定できないのであるから、データ所在国がその主権に基づいて保護する領域内に所在する者の権利・利益をそれによって侵害することに着目すれば、国家主権の侵害が基礎づけられると解することも可能である。また、逆に、データの取得が捜索・差押えに該当するとしても、領域内に所在する者の権利・利益を侵害しないのであれば、国家主権の侵害は認められない、ということもできる[72]。

従来、執行管轄権の域外適用が厳格に禁止されていたのは、法執行機関による他国の領域内への物理的侵入が想定され、そのことによる国家主権の侵害が当然に予定されていたからであり、領域内への物理的侵入を伴わないのであれば、国家主権の侵害が直ちに導かれるものではないように思われる。そのため、捜索の着手時期に関する見解の立場は、国境を越えるアクセスの可否について影響を及ぼすものではないというべきであり、端的にアクセス行為が国家主権を侵害するか否かを問題として取り上げる必要があろう。そして、その際、データ所在国が主権に基づいて保護する領域内に所在する者の権利・利益の侵害の有無に着目するのであれば、データに関する権利・利益がいかなる国家により強く帰属するか否かを考慮することが適切であると考える。

この点、米国議会で上程されている、米国プロバイダに送達される、データの

開示を要請する令状の効力は、データが蔵置されているアカウントの保持者が「合衆国人（United States person）[73]」であるならば、国外に蔵置されたデータにも及ぶものとする、Law Enforcement Access to Data Stored Abroad Act（LEADS Act）[74] に加えられている批判が参考になる。LEADS Act は、「合衆国人」でないアカウント保持者のデータの取得の可否を、サーバの所在地が国内か国外かで区別するが、それは伝統的な領土権を重視する点で、クラウド等の急速に変化するテクノロジーに対応するには不十分であるとの批判が加えられている。そして、このような問題点を克服するため、開示要請の可否について、データの所在地により判断するのではなく、ユーザーの国籍とデータが作成された場所に基づいて判断すべきだとする見解が提唱されている[75]。このアプローチは、データに関するアカウント保持者が自国民であるか、データが自国の領域内で作成されたならば、ロード・バランシングによって偶々他国の領域内のサーバに蔵置されたとしても、サーバ所在国ではなく当該国こそが当該データに利益を有することを根拠とするものである。このことは、国境を越えるアクセスによって取得するデータのアカウント保持者が自国民であるか、データが自国の領域内で作成されている場合においても同様であり、かかる場合には、データ所在国がその主権に基づいて保護すべき権利・利益は希薄といえ、国家主権の侵害を否定しても差し支えないといえるであろう。そして、このように解した場合には、前述した逃亡犯罪人の場合との異同が問題になるようにも思われるが[76]、そもそも、サーバへのアクセスのため、データ所在国に物理的に侵入することを要さないのであるから、逃亡犯罪人の捜索と同様に考えることはできないであろう。

これらを整理すると、第一に、自国内にある端末のメインメモリにデータが一時的に保存されている場合等、データが国内に存在するならば、その閲覧は執行管轄権の域外適用には該当しない。第二に、データ所在国がデータに関して保護する利益を有さない場合、すなわち、捜査機関が適法にアクセス権限を取得しプロバイダの利益を侵害するおそれがなく、かつ、データに関するアカウント保持者が自国民である又はデータが自国の領域内で作成されたといえる場合には、その取得は執行管轄権の域外適用に該当するとしても、国家主権の侵害は認められないことになる[77]。

（2） CEG 勧告

ここまで見てきたように、国境を越えるアクセスについては判例及び学説が対

立しており、国際的に統一された理解には至っていない。それにもかかわらず、国際捜査共助や提出命令では「ロス・オブ・ロケーション」の問題に対処できないことから、条約32条以外に保障措置を規定する国際的枠組みが存在しないまま、国際関係及び個人の人権に悪影響を及ぼすおそれのある、各国による一方的なアクセスが現実には増加している[78]。そこで、CEG は、この問題の解決のために、既存の、国境を越えるアクセスの国家実行に応じた枠組みの明確化及び保障措置の強化に関する条項を勧告５の第二追加議定書に設けることとした。

同条項では、第一に、「適法に取得した認証情報（credentials）を伴う同意を欠く国境を越えるアクセス」を規定している[79]。これは、締約国が適法な捜査活動によって認証情報を取得した場合には[80]、自国内のコンピュータを通じて、他の締約国に所在する蔵置されたデータにアクセス又は受領する他国の権限の授与なしにアクセス又は受領することを認めるものである。ただし、捜査当事国はデータ取得前、取得中又は取得後に他の締約国への通知義務を負う。これは、本節第１項で検討した、サーバ所在国内の者の実質的な権利侵害の有無に着目するという議論に沿うものといえる。

捜査当事国による通知義務の具体的内容について、CEG 勧告は言及していないが、この点、欧州委員会移民・内務総局の専門家会議による報告が参考になる。この報告では、国境を越えるアクセスについて捜査当事国による通告義務を規定しているところ、通告を受けた国家は国境を越えるアクセスを拒絶する権利を有するとしている[81]。CEG 勧告は取得中又は取得後の通告も許容していることから、通告を受けた国家による拒絶を想定していないといえるが、今後の議論によっては、事前通告を原則とし、通告を受けた国家による拒絶を認める枠組みの導入もあり得よう。

第二に、同条項は、「善意の、又は急迫した若しくはその他の状況における同意なき国境を越えるアクセス」についても規定している[82]。これらは、「適法に取得した認証情報を伴う同意を欠く国境を越えるアクセス」の例外として、捜査当事国が通知義務を負わない場合を規定するものである。もっとも、原則的な場合にも事後的な通知を許容していることに鑑みれば、少なくとも急迫時のアクセスについては国境を越えるアクセスであることを捜査機関は認識しているのであるから、事後的な通知は要求されるべきであろう。

第三に、同条項は、「関連する法的要素としての『処分権』又は『保有し若しくは管理する者』」について規定している[83]。前述のように「ロス・オブ・ロケー

ション」の状況においては、属地主義に基づいて執行管轄権の適用範囲を画定することは困難であるし、通知の対象とすべき国も特定できなくなる。そのため、領土権を離れたアプローチが必要とされるところ、領土権に代替する関連する法的要素として、「処分権」又は「保有し若しくは管理する者」を挙げているのである。そして、このような処分権に着目する考え方は、前述のアカウント保持者やデータの作成場所を基準とする考え方と軌を一にするものといえる。

（3）　小　括

このように、国境を越えるアクセスによる国家主権の侵害の問題に関しては、学説上大きな対立がみられるものの、前述した理解からは、実質的に国家主権の侵害が生じているか否かをデータの利害関係者の利益に着目して判断することが妥当であり、CEG 勧告の内容もこのような見解に即していることから、その内容が実現されれば、国家主権の侵害の問題に関する議論は整理されるものと思われる。もっとも、我が国の刑事訴訟法は、平成23年改正により設けられた、リモートアクセスによる複写の処分を規定するのみであり、かつ、リモートアクセスが実施できる場合が制限されているために、前出の Gmail 事件のような問題が生じている。次章では、この点を中心に検討する。

Ⅲ　クラウド証拠部会（CEG）勧告の国内法における実施

1　提出命令

まず、提出命令については、前章第２節における検討を踏まえると、国内法上、自国の領域内でサービスを提供するサービス・プロバイダに対する加入者情報の提出命令及び加入者情報の取得ための要件の緩和の２つの実施が必要といえる。

（1）　サイバー犯罪条約18条１項ｂの国内法化

まず、記録命令付差押えを定義する刑訴99条の２は、単に被処分者を「電磁的記録を保管する者その他電磁的記録を利用する権限を有する者」と規定するにとどまり、被処分者が「自国の領域内に所在する者」（条約18条１項ａ）か否かについては言及していない。そのため、「自国の領域内でサービスを提供するサービス・プロバイダ」（同項ｂ）に対しても適用できそうではあるが、同項の区別に従い記録させるべき電磁的記録は加入者情報に限定する必要があるため、同項ｂに

対応する規定の創設を要しよう。もっとも、従来の記録命令付差押えとの違いは、被処分者が自国の領域内に所在する者でない点及び加入者情報を他のデータと区別する点のみであり、この規定を創設することに伴い、既存の憲法及び刑事訴訟法上の原則及び規定との抵触は生じることはないものと思われる。

（2） 捜査機関による加入者情報の提出命令の創設

一方で、加入者情報を取得するための提出命令に係る要件の緩和については、加入者情報に関しては、記録命令付差押えの枠組みから除外して、検察又は警察の要請によって取得することができるとする、新たな枠組み（以下、「捜査機関による加入者情報の提出命令」という。）の創設が求められることとなろう。もっとも、捜査機関による加入者情報の提出命令については、ユーザーの通信の秘密（憲法21条２項後段）に関連して、令状主義との抵触が問題となる[84]。

（a）記録命令付差押えの意義

この点について、そもそも、捜査機関に協力的な通信事業者からデータを取得するために捜査関係事項照会（刑訴197条２項）を活用するのではなく、令状審査を経る必要のある記録命令付差押えの制度が創設されたのは、電気通信事業者には通信の秘密を保護する義務があるところ、「通信の秘密に属する事項（通信内容にとどまらず、通信当事者の住所・氏名、発受信場所、通信年月日等通信の構成要素及び通信回数等通信の存在の事実の有無を含む。）について捜査機関に提供することは原則として適当ではない」とされたからである[85]。そのため、加入者情報を提出させることは通信の秘密を制約するものであることから、少なくとも総務省のガイドラインに従う限りは、記録命令付差押えの枠組みに基づくべきであり、捜査機関がその提出を命ずることは、令状主義の制約に服すべきものといえる。

（b）保全要請と令状主義

もっとも、平成23年改正においては、記録命令付差押えに加えて、保全要請（刑訴197条３～５項）も同時に創設されている。これは、通信履歴は短期間で消去されることが多く、捜査に必要な通信履歴については、迅速に保全する必要性が大きいために規定されたものである[86]。この保全要請も司法審査を経ずに通信記録を保存させることから、通信の秘密の侵害に関連して、令状主義との抵触が問題となる。

しかし、まず、通信の秘密の侵害の点については、①保全の対象が「通信履歴」に限られており、②単にその消去しないように求めるにとどまり捜査機関に開示

されるものではなく、また、③要請に応じない場合の罰則規定も存在しないことから、通信の秘密を制約するものではないとされている[87]。さらに、このことから、通信の秘密が制約されるものではなく、憲法35条が保障する権利・利益の制約はないといえ、令状によらないとしても令状主義に反するものではないとされている[88]。このように、保全要請が、上記①ないし③の理由により、通信の秘密を制約しないとされ、したがって、令状主義にも反しないとされることからすると、捜査機関による加入者情報の提出命令についても、さしあたり、上記①ないし③の視点に即した、保全要請との比較による検討が有用だといえる。

（c）捜査機関による加入者情報の提出命令と令状主義

保全要請が令状主義の原則に抵触しないと解する根拠として指摘される、①については、通信記録に含まれる利用者のプライバシーの重要性が、通信内容に比して低いという判断が前提とされているといえる。そして、前章第２節で述べたように、CEG 勧告では、加入者情報に含まれるプライバシーの重要性が、通信記録及び通信内容のそれよりも低いことを理由として、別個の枠組みの下での取扱いを適当だとしている[89]。そのため、提出命令の対象を加入者情報に限定する、捜査機関による提出命令にも①の理由は妥当する。

また、③についても、提出命令に罰則規定を設けないのであれば、保全要請との間に異なるところはないということができる。

しかし、②については、保全にとどまらず、提出まで求めることを内容とする、捜査機関による加入者情報の提出命令には当てはまらない。そのため、提出まで求めることが通信の秘密を制約するかが問題となる。

この点、領置（刑訴221条）は、占有取得後、捜査機関の占有が強制的に維持される点は差押えの場合と同様であるが、占有取得過程に強制の要素がないので憲法35条の「押収」には当たらず、令状は要求されていないことに鑑みると、加入者情報の提出命令についても、情報を提出すべき法的義務を生じさせるものの、違反に対する罰則規定はなく、提出行為自体は被処分者の意思に基づくものであり、同様に通信の秘密を制約するものではなく令状は要しないということができよう[90]。

このように、提出命令の対象が、保全要請の対象である通信記録に比して、プライバシーの重要度が低いとみられる加入者情報に限定され、かつ、提出行為自体は被処分者の意思に基づくものであることに着目すれば、情報の保全にとどまらず提出まで求めるものであっても、令状による必要はなく、捜査機関限りの判

断に基づきこれを命ずることができる、とすることも認められるように思われる。

（3） 小　括

このように、条約18条１項ｂの国内法化及び捜査機関による加入者情報の提出命令の創設はともに、憲法及び刑事訴訟法の原則及び規定に抵触するものではなく、国内法上、立法によって実施可能といえる。そして、提出命令及び記録命令付差押えは、データが国外に所在するが国境を越えるアクセスが許されない場合においては、迅速性を欠く国際捜査共助以外に残された唯一の手段である。このことからすれば、少なくとも、国境を越えるアクセスに関する CEG 勧告の内容が実現されないのであれば、罰則規定を設け実効性を確保することも検討に値するであろう[91)]。

2　国境を越えるアクセス

次に、国境を越えるアクセスについては、前章第３節における検討を踏まえると、我が国内法上は、取得すべきデータの所在国が判明している場合と判明していない場合とを区別した上で、前者の場合には、認証情報の適法な取得及び通知義務の履行又はその例外要件の具備を、また、後者の場合には、「処分権」を有する者又は「保有し若しくは管理する者」が自国内に所在することを、それぞれ要件として、国境を越えるアクセスが認められることを法定することが必要だといえる。

もっとも、これらの要件は、国家主権の侵害の問題を生じさせないために設けられるものであり、捜査機関によるリモートアクセス自体は、平成23年改正により規定されていることから、その規定に則って実施される限り、憲法及び刑事訴訟法との抵触は生じないはずである。そこで、本節では、Gmail事件がそうであったように、リモートアクセスを、データの蔵置されている電子計算機の差押えを前提とする場合に限定して認める現行法によっては対応できない場合が生じていることを踏まえ、現行のリモートアクセス制度の限界ないし改善点について検討する。

（1） Gmail 事件

（a）事案

Gmail 事件については、すでに、その、国家主権の侵害の問題に関する判示部

分に言及したが、その判断の重点は、捜査機関が被疑者のコンピュータの検証に伴う「必要な処分」として被疑者の Gmail アカウントにアクセスしたことの適否に置かれている。

本件では、警察官が被疑者のコンピュータを「差し押さえるべき物」、メールサーバの記憶領域を「電磁的記録を複写すべきものの範囲」として記載され、リモートアクセスによる複写の処分が許可された捜索差押許可状に基づいて当該コンピュータを差し押さえたが、その際、当該コンピュータにログインするためのパスワードが判明していなかったためにログインすることができなかった。その後、パスワードが当該コンピュータの解析によって判明したため、捜査機関は当該コンピュータを「検証すべき物」と記載する検証許可状の発付を得た上で、当該コンピュータの検証に伴う「必要な処分」として Gmail アカウントにログインし、被疑者のメールアドレスに係る送受信メールをダウンロードして保存したというのが、その事案であった。

（b）原判決の内容

横浜地裁は、まず、①リモートアクセスによる複写の処分を許可する捜索差押許可状に基づいて、差押え終了後にリモートアクセスを実施することにつき、「メールサーバにアクセスすることは、当該メールサーバの管理者等の第三者の権利・利益を侵害し得るものである」ことから、現行法は「捜査の必要と第三者の権利・利益の保護の調和」を踏まえてリモートアクセスによる複写の処分を規定しているところ、「リモートアクセスによる複写の処分は、電子計算機の差押えに先立って行われるものであり、差押え終了後に行うことは想定されていない」と説示し、一般に、これを許されないものとした。

続いて、②当該コンピュータを「検証すべき物」とする検証許可状に基づいて、メールサーバに対するリモートアクセスを実施することについては、「捜査機関が検証許可状に基づいてパーソナルコンピュータの状態を検証する権限を有することとなったとしても、そのパーソナルコンピュータからインターネットに接続し、メールサーバにアクセスすることが当然に認められるものでないことは、前記のような刑事訴訟法の規定の趣旨からしても明らかである」とした上で、「本件検証は、メールサーバの管理者等の第三者の権利・利益を侵害する強制処分にほかならず、捜査機関が、このような強制処分を必要な司法審査を経ずに行ったということは、現行の刑事訴訟法の基本的な枠組みに反する違法なものであった」と断じ、本件のようなリモートアクセスもまた認められないものとした。

（c）東京高裁判決の内容

控訴審である東京高裁もまた、当該コンピュータを「検証すべき物」とする検証許可状に基づくメールサーバへのリモートアクセスの可否について、「本件パソコンの内容を複製したパソコンからインターネットに接続してメールサーバにアクセスし、メール等を閲覧、保存したものであるが、本件検証許可状に基づいて行うことができない強制処分を行ったものである」として、これを違法とする原審の判断を支持した。

（d）裁判例の意義と現行法の問題点

これらの判断は、本件捜査機関の活動の適否につき、「捜査の必要と第三者の権利・利益の保護の調和」のために刑事訴訟法218条２項がリモートアクセスを実施できる場合を限定的に定めた趣旨に反するか否かを基準としているものといえる。

これを前提とすると、まず、①については、現行法は、捜索場所にあるコンピュータ等の差押えの前段階として、リモートアクセスを許容するものであり、刑事訴訟法218条２項の文言から明らかに外れるものと言わざるを得ず、上記趣旨に反することを理由としたといえる。

続いて、②については、ここで裁判官の令状審査の対象とされたのは「検証すべき物」である被疑者のコンピュータのみであるにもかかわらず、「メールサーバ上のメール送受信履歴及び内容」まで、捜査機関が当該コンピュータの検証に伴うものとしてダウンロードすることは、被処分者の法益とは別個の法益の侵害に当たるところ[92]、実質的には、本体的処分とされる当該コンピュータの検証よりも付随的処分であるリモートアクセスを目的とした本件の検証においてリモートアクセスを行うことを許すことは、前記趣旨に反するものとしたものと解される[93]。

原判決及び東京高裁判決の結論は妥当と考えるが、刑事訴訟法218条２項の趣旨を「捜査の必要と第三者の権利・利益の保護の調和」としたことには疑問が残る。前章で述べたように「アカウント保持者がアクセスを認められる範囲のデータを入手する」場合には、「メールサーバの管理者等の第三者の権利・利益」を侵害するものではなく、「第三者の権利・利益」は「捜査の必要」に対峙する反対法益とはいえないと思われるからである[94]。被侵害利益を確定するに当たり、原判決は、リモートアクセスの被処分者を、「メールサーバの管理者等の第三者」としているが、この点は、いま少し、立ち入った検討を要するであろう。なぜな

ら、複写するのはメールサーバ全体ではなくサーバ中、当該メールアカウントによりアクセス可能な記録領域であるから、被処分者についてもメールサーバ全体ではなく、当該記録領域に限定して考える方が実態に即しているためである。

この点、通常の捜索においては、「捜索すべき場所」（刑訴107条１項、219条１項）の範囲が管理権の同一性を基準に判断され、雑居ビルなど部屋ごとに独立の排他的な管理が行われている場合には、各部屋が独立した「捜索すべき場所」となり[95]、その居住者のみが「処分を受ける者」（刑訴110条）とされている[96]。そして、通常、クラウドにおいてはユーザーによる自由なデータの送受信が前提とされ[97]、当該記録領域に蔵置されているデータに関する利益はプロバイダよりもアカウント保持者に強く帰属するものであり、また、前述のようにプライバシー意識の高まりに伴い、サーバへのアクセスがプロバイダでさえもできなくなりつつある。そうだとすれば、銀行の貸金庫が銀行とは別個の管理権に属すると解されるのと同様に[98]、サーバにおいては、各ユーザーのアカウントに対応する記録領域ごとに管理権を観念し、アカウント保持者のみを当該アカウントに対応する記録領域の管理権者として被処分者とみるべきといえる[99]。このように被処分者をアカウント保持者とみるのであれば、「捜査の必要」に対峙する反対法益は、「メールサーバの管理者等の第三者の権利・利益」ではなく「アカウント保持者の権利・利益」、すなわち、ほとんどの場合、差し押さえるコンピュータの所有者の権利・利益ということになろう。

このように、本件のような捜査は、現行法の下では許されないものであるが、リモートアクセスによる被侵害法益の理解については問題があると思われる。また、前述のとおり、捜査機関がデータ取得のために実施可能な記録命令付差押えについては間接強制が認められず、協力的でない事業者に対しては実効性を欠くことから、本件のような事案においてリモートアクセスを行う必要性はなお高い。そこで、以下では、コンピュータの差押えを前提としないリモートアクセスが現行法の下で許容されるか、その実施可能性を探ることとする。

（２）　差押えを前提としないリモートアクセス

差押えを前提としないリモートアクセスを実現するには、①サーバへのリモートアクセスが許可された、コンピュータ端末を対象とする捜索差押許可状を再度取得するか、②リモートアクセスによる、サーバを対象とする検証許可状を取得することが考えられるため[100]、以下順に検討する。

（a）リモートアクセスを許可する捜索差押許可状の（再度の）取得

別件において差押え済みの証拠物を本件の捜査のために改めて差し押さえる「二重押収」は実務上多く行われており[101]、また、刑事訴訟法218条２項自体、「当該電子計算機又は当該他の記録媒体を差し押さえることができる」と規定し、捜査機関が占有している「他の記録媒体」を差し押さえることを想定していることから[102]、捜査機関が当初の令状により既に差し押さえているコンピュータについて、改めて、リモートアクセスを許可する捜索差押許可状を取得し、これに基づく処分を実施することもまた認められるといえよう[103]。

これによって、Gmail 事件のような事案に対応できるようにはなるが、クラウドが発達した現在、捜査機関が必要とするデータは、個人の使用に係る端末にではなく、サーバに蔵置されているという事態は珍しくなくなっており、そこでは、捜査機関は、コンピュータに保存されたデータではなく、サーバ上のデータの取得を主たる目的とすることとなる[104]。そこで、個人の使用するクライアント端末ではなく、データの蔵置されている記録媒体に着目した処分を構想することが、新たな現実への、より直接的で、現実に即した対応だといえるように思われる。

（b）リモートアクセスによる検証

すでに、Gmail 事件のような事案については、クライアント端末を対象とするのではなく、サーバ自体、すなわちサーバ中の、当該メールアカウントによりアクセス可能な記録領域を対象とした検証をリモートアクセスによってすることはできるとする見解が主張されている[105]。サーバ自体を検証の対象とするならば、「アカウント保持者の権利・利益」について司法審査を経ることになり、検証に伴う「必要な処分」としてリモートアクセスを行ったとしても、「捜査の必要」と「アカウント保持者の権利・利益」の調和という刑事訴訟法218項２項の趣旨に反することにはならないように思われる[106]。

これに対して、強制処分について「いかなる内容・形態の処分類型をどのような要件と手続により正当な捜査手段として設定するかは、国民代表による国会制定法律の形式であらかじめ定め告知することにより、国民の行動の自由を民主的に担保」するという強制処分法定主義の趣旨[107] に鑑みれば、立法者は「当該手段によって確保される捜査・処罰の利益や法益侵害の質と両者の権衡、誤用・濫用の危険性等諸々の事情を勘案した上で、許そうとする行為の性質に応じた要件を設定し、さらに違法行為に関する救済の方途まで見据えて立法すべき」であり、「強制処分について要求される「特別の定」（刑訴197条１項ただし書）は、これら

の一連の考慮と規律の『パッケージ』でなければならない」とする指摘がある[108]。そして、この見解によれば、①差押えに付随しないリモートアクセスは時間的・場所的制約がなくなり捜査機関がリモートアクセスを行いやすくなること、②クライアント端末の所在地まで赴く労を省くには令状の提示（刑訴222条1項後段・110条）が不要とされる（はずである）こと、また、③検証に対する準抗告が認められておらず、不服申立てをする機会を欠くことから、現行法の下における、リモートアクセスによる検証は、刑事訴訟法の規定する検証の「パッケージ」を逸脱する可能性がある、とされるのである[109]。

もっとも、①については、クライアント端末の差押えを不要として、直接サーバにアクセスすることを認めたとしても、捜査機関はなお、認証情報を取得しなければならないのであるから、濫用のおそれが高まるといえるほどに、捜査機関がリモートアクセスによる検証を行う機会が増えるとは言い難いように思われる。また、②については、必ずしも、令状の提示を不要としてクライアント端末の所在地まで赴かなくて済む制度にする必要はなく[110]、アカウント保持者を「処分を受ける者」とした上で[111]、処分に着手する前に令状を示すことを原則とするとともに、事前に令状を示すと対象物が隠滅・破壊されるおそれがある場合等には、例外的に事後的な提示を認めるものとする[112]だけでも足りるように思われる。さらに、③については、「パッケージ論」の論者が指摘するように、電話検証に関する最高裁決定[113]は不服申立てが規定されていないことに言及しつつも電話検証を「検証」として適法としていることから、「致命傷ではない」[114]。このように考えられるとすれば、リモートアクセスによる検証が、検証の「パッケージ」を逸脱するものではないと解することも可能だと解される。

（3） 小　括

これまで検討してきたように、CEG 勧告の国内法における実施は立法によって行うことが可能だと解される。ただ、リモートアクセスによる複写の処分以外の場合の、リモートアクセスを認める必要があるところ、現行法の下においても、現行のリモートアクセスの規定又は検証の規定により実現可能であると考える。

おわりに

本論文では、クラウドの発達によって、データが、個人の使用する端末ではな

く、サーバに蔵置されることが通常の事態となりつつある状況の下、捜査機関は、データ取得の場面において、国際法上は、ロス・オブ・ロケーション等の現実がもたらす国家主権の侵害の問題、国内法上は、平成23年改正を含む現行刑事訴訟法による対応の限界の問題に直面するようになってきた。

国際法的側面については、T-CYが、領土権を基本とする伝統的な国家管轄権概念から脱し、領域への物理的侵入を伴わないデータへのアクセスという活動の性質に鑑み、国家主権の内実を実質的に捉えることにより、問題の解決を試みている。これに対し、国内に目を向けると、サイバー犯罪条約への対応を図った、平成23年の刑事訴訟法改正以後、立法の動きは見られない。前述のとおり、クラウドの発達した現状においても、現行法による対応は可能であるが、国境を越えるアクセスを関する手当ては必要となるであろうから、早急に議論を深める必要があると思われる。そのための準備作業として、本稿における検討が役立つことがあれば筆者にとり望外の喜びである。

1） 警察庁「平成29年上半期におけるサイバー空間をめぐる脅威の情勢等について」12頁（平成29年９月７日）は、平成28年のサイバー犯罪の検挙件数を8,324件としている。
2） サイバー犯罪条約の分析について、経済産業省サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」（2002年４月18日）参照。
3） 立案当局の担当官による解説として、杉山徳明＝吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について（下）」曹時64巻５号（2012年）55頁以下がある。
4） 経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013年度版）」８頁（2016年３月14日。同月26日修正）。なお、クラウドの意義と機能について、芝原邦爾ほか編『経済刑法―実務と理論』569頁〔笹倉宏紀〕（商事法務、2017年）参照。
5） 笹倉・前掲注４）566頁。
6） 笹倉・前掲注４）566-567頁、Reema Shah, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 Yale.L.Rev.543, 547-549 (2015).
7） 神奈川県警の警察官が被疑者のコンピュータの検証に伴う「必要な処分」（刑訴222条１項後段、129条）として被疑者のGmailアカウントにアクセスしたことの適否が問題となった事案である。
8） 横浜地判平成28年３月17日（LEX/DB文献番号25542385）。
9） 東京高判平成28年12月７日高刑集69巻２号５頁。
10） Shah, *supra* note 6, at 543-545.
11） Devlin Barrett & Danny Yadron, *New Level of Smartphone Encryption Alarms Law*

Enforcement, Wall Street J., Sept.22,2014, *available at* https://www.wsj.com/articles/new-level-of-smartphone-encryption-alarms-law-enforcement-1411420341

12）　Shah, *supra* note 6, at 554.

13）　Jan Spoenle, *Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?,* Aug.31, 2010, at 4–5.

14）　笹倉・前掲注４）565頁。

15）　第177回国会衆議院法務委員会議録14号（平成23年５月27日）10頁〔江田五月法務大臣答弁〕。

16）　Council of Europe Cybercrime Convention Committee (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, 123 (2013).

17）　我が国の刑事訴訟法においても裁判所による処分である提出命令（刑訴99条３項）は存在するが、本論文で提出命令という場合はサイバー犯罪条約上の提出命令をいう。

18）　杉山＝吉田・前掲注３）73頁（注４）。

19）　笹倉宏紀「サイバー空間の捜査」法教446号（2017年）39–40頁。

20）　杉山＝吉田・前掲注３）73頁（注５）。

21）　杉山＝吉田・前掲注３）72頁。

22）　指宿信「サイバースペースにおける証拠収集とデジタル証拠の確保―2011年改正法案を考える」法時83巻７号87頁。なお、同論文は、記録命令付差押えを「二次的強制処分を予定した間接強制的な性格を持つ処分」と評している。

23）　第177回国会衆議院法務委員会議録15号（平成23年５月31日）14頁〔江田五月法務大臣答弁〕、第177回国会参議院法務委員会議録15号（平成23年６月９日）10頁〔江田五月法務大臣答弁〕。

24）　本論文・第２章第２節。

25）　指宿・前掲注22）88頁。

26）　Anna-Maria Osula, *Remote search and seizure: Estonian case study*, 24 (4) IJLIT, 345 n.9 (2016).

27）　Council of Europe, *Explanatory Report – ETS 185 – Cybercrime* (*Convention)*, Nov.23, 2001, para.293.

28）　杉山＝吉田・前掲注３）100頁。

29）　Osula, *supra* note 26, at 346.

30）　Cybercrime Convention Committee (T-CY), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY (Final report of the T-CY Cloud Evidence Group)*, Sept.16,2016.

31）　*Id.* at 47.

32）　山本草二『国際法（新版）』（有斐閣、1994年）231頁。

33）　The American Law Institute, *Restatement of the Law Third: The Foreign Relations Law of the United States*, §401 (1987).

34） The Case of the SS Lotus (Fr v Turk),1927P.C.I.J (ser A) No.10 (Decision No.9), at 18.

35） *Id.* at 19. なお、訳語は、竹内真理「判批」小寺彰ほか編『国際法判例百選（第２版）』42頁に基づく。

36） 竹内・前掲注35）43頁。

37） そのため、小寺彰『パラダイム国際法―国際法の基本構成』（有斐閣、2004年）101頁は、執行管轄権の域外適用が許されるかではなく、単に「国家がどのような行為をすれば執行管轄権の域外適用に該当するか」（執行管轄権の域外適用該当性）のみが問題になるとしている。しかし、データの取得という文脈においては、後述のように執行管轄権の域外適用に該当したとしても、さらに「当該権限の行使が執行管轄権の域外適用が国家主権の侵害を生じさせるか」（執行管轄権の域外適用の可否）も問題となり得る。

38） *See*, e.g., Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313 (2013); Zachary D. Clopton, *Territoriality, Technology, and National Security*, 83 U. Chi. L. Rev. 45 (2016); Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326 (2015).

39） Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729, 763 (2016).

40） なお、これらの議論は、我が国の記録命令付差押えとは異なり、提出命令に間接強制の規定が設けられていることを前提とすることに注意を要する。

41） Joseph Story, *Commentaries on the Conflict of Laws, Foreign and Domestic, in Regard to Contracts, Rights and Remedies, and Especially in Regard to Marriages, Divorces, Wills, Successions, and Judgments*, § 18 at 19 (1841).

42） Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. Chi. Legal F. 103 (2001) at 109. なお、Woods, supra note 39, at 735 n.26は、正確には、ゴールドスミス教授は「データ例外主義」が提唱される前の「サイバーアナーキスト（cyber anarchist）」の論者であるとする。

43）「米国裁判所又は米国当局は、情報若しくは情報を保有している者が米国外にいるとしても、法律若しくは裁判所規則によって権限を与えられた場合には、文書、物若しくはその他の情報を提出するようにその者に命令する権限を有する。」

44） Woods, *supra* note 39, at 769–772.

45） Belgium v. Yahoo!, Nr. P.13.2082.N, (Hof van Cassatie van België 2015). なお、同判例の英訳として、*Case Translation: Belgium - Hof van Cassatie van België*, 13 D.E. & E.S.L.R.156 (2016) がある。

46） Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 62–65 (June 27); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), 2007 I.C.J 43 (Feb. 26).

47） Cybercrime Convention Committee (T-CY), *T-CY Guidance Note #10: Production*

orders for subscriber information (Article 18 Budapest Convention), Feb.28, 2017, at 6は、「者（person）」にはサービス・プロバイダも含まれるとしている。

48）　Cybercrime Convention Committee (T-CY), *supra* note 30, at 13.

49）　Cybercrime Convention Committee (T-CY), *supra* note 47, at 8は、その判断要素として、サービス・プロバイダがその事業活動を当該加入者に対して適応させている程度（自国内の広告や自国の言語による広告等）、事業活動を運営する上で加入者情報（若しくは関連する通信記録）を利用する程度、自国内の加入者との関連性及び自国内に設立されていると考えらえている程度を挙げている。

50）　*Id*.

51）　例えば、Cybercrime Convention Committee (T-CY), *supra* note 30, at 64は、前出ベルギー最高裁判例で問題となったベルギーの提出命令について、条約18条１項ｂに沿うものとしている。

52）　Cybercrime Convention Committee (T-CY), *supra* note 30, at 47.

53）　*Id*. at 38. なお、プライバシー権の保護の問題を含んでいるため、次章で検討する。

54）　*Id*. at 13-14.

55）　*Id*. at 24-29.

56）　もっとも、前述のように被処分者のアクセス行為が国家に帰属するのであれば、本章第３節と同様の問題状況になり得る。

57）　国境を越えるアクセスによる国家主権の侵害の問題については、Anna-Maria Osula, *Transborder access and territorial sovereignty*, 31 C.L.S.R 719 (2015) が詳しい。以下の判例及び学説の動向も同論文に基づく。

58）　Nicolai Seitz, *TRANSBORDER SEARCH: A NEW PERSPECTIVE IN LAW ENFORCEMENT?*, 7 Yale JL & Tech. 23, 28 note 6 (2004).

59）　Orin S Kerr, *SEARCHES AND SEIZURES IN A DIGITAL WORLD*, 119 Harv. L. Rev. 531, 551 (2005).

60）　In Re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d 753, 4-5 (S.D.Tex.2013).

61）　Goldsmith, *supra* note 42, at 115.

62）　Patricia L. Bellia, *Chasing Bits across Borders*, 2001 U. Chi. Legal F. 35, 77-78 (2001); Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 Fed. Comm. L.J. 117, 174 (1997).

63）　In Re Warrant to Search a Target Computer at Premises Unknown, *supra* note 61, at 5-6.

64）　井上正仁『強制捜査と任意捜査（新版）』（有斐閣、2014年）418頁。

65）　井上・前掲注64）419頁。

66）　Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 Int'l L. Stud. 123, 129 (2013). なお、後述のように同論文の著者がこのような見解に立つわけではない。

67）　山内由光「判批」研修832号（2017年）24-25頁、貴志浩平「ハイテク犯罪と捜

査手続」捜査研究564号（1998年）21頁。アクセス権限を適法に取得している場合のアクセスがプロバイダの利益を害するものではないことについては、本論文・次章第２節で詳述する。なお、クラウドの文脈においては、データが偶然データ所在国のサーバに蔵置されたにすぎない場合がほとんどであると考えられるところ、そもそもアカウント保持者を保護することにデータ所在国が利益を有さないともいえよう。

68） 井上・前掲注64）418頁。

69） Bert-Jaap Koops & Morag Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The limits and possibilities of international law*, Tilburg Law School Research Paper No. 5/2016, 61 (2014).

70） Heinegg, *supra* note 66, at 129; Bellia, *supra* note 62, at 78.

71） Bellia, *supra* note 62, at 78.

72） 本論文・前掲注67）。

73）「合衆国人」とは、市民、永住外国人又は連邦、州若しくは下部の政治単位の法にしたがって結成された組織をいう（和訳につき、堤和通「米国におけるサイバー犯罪捜査」刑ジャ51号（2017年）40頁注（33）参照）。

74） Microsoft Corp. v. United States,829 F.3d 197 (2d Cir.2016) において、米国内法上、域外的な効力を否定された電気通信におけるプライバシー保護法（Electronic Communications Privacy Act（ECPA）の一部である SCA を改正するものである。

75） Shah, *supra* note 6, at 550.

76） *See supra* note 71 and accompanying text.

77） なお、本章第２節における私見で述べたように、間接強制を伴う提出命令によるプロバイダの国外のサーバへのアクセス行為を国家の行為とみる場合にも、同様の結論になろう。

78） Cybercrime Convention Committee (T-CY), *supra* note 30, at 44.

79） *Id.* at 45.

80） そのため、他の締約国に所在するコンピュータへのハッキングにより取得された場合は含まれない等の追加の条件及び保障措置も必要とされている。

81） European Commission, *Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, Jun, 8 2017, at 26.

82） Cybercrime Convention Committee (T-CY), *supra* note 30, at 45.

83） *Id.* at 45.

84） 井上・前掲注64）62頁は、通信の秘密は通信についてのプライバシー権を保障する趣旨であることから、通信についても憲法35条による令状主義の保障が及ぶとしている。

85） 総務省「電気通信事業における個人情報保護に関するガイドライン（平成29年総務省告示第152号）解説」61-62頁（平成29年４月18日版）。

86） 杉山＝吉田・前掲注３）113頁。

87）　杉山＝吉田・前掲注３）113-114頁。

88）　杉山＝吉田・前掲注３）114頁（注２）、酒巻匡「サイバー犯罪条約の手続法規定について」法とコンピュータ21号（2003年）60頁。

89）　*See supra* note 48 and accompanying text.

90）　酒巻匡「新しい証拠収集手段―提出命令について」ジュリ1228号（2002年）130頁。なお、同論文は、加入者情報に限定しないデータ一般の提出命令について、罰則規定が付加されているとしても令状は不要だとの見解を示している。

91）　罰則規定の創設の可否については、本論文・前掲注90）、笹倉・前掲注19）39-40、川出敏裕「コンピュータ犯罪と捜査手続」曹時53巻10号（2001年）15-18頁参照。

92）　なお、河上和雄ほか編『大コンメンタール刑事訴訟法（第二版）第２巻〔第57条～第127条〕』395頁〔渡辺咲子〕（青林書店、2010年）は、刑訴111条、129条が規定する「必要な処分」は、本体的処分を実効あらしめるために必要な「新たな重要な法益を侵害する処分」も可能であることを示したものであり、第三者の法益を侵害することもできるとしており、第三者の法益を侵害する「必要な処分」も直ちに違法となるわけではない。

93）　山内・前掲注67）18-19頁参照。なお、たとえ刑事訴訟法218条２項の趣旨に反しないとしても、そもそも、令状に「検証すべき物」として記載されていないメールサーバにアクセスしたこと自体が違法であるともいえよう。

94）　山内・前掲注67）20頁。

95）　松尾浩也監『条解刑事訴訟法（第４版増補版）』220頁（弘文堂、2016年）。

96）　松尾監・前掲注95）224頁。

97）　貴志・前掲注67）20頁、長沼範良「ネットワーク犯罪への手続法的対応」ジュリ1148号（1999年）216頁参照。なお、これらの文献は、クラウドではなく企業内ネットワークにおいては、データの送受信は企業の業務目的に限られることから、サーバ管理者も被処分者に当たるとしている。

98）　河上ほか編・前掲注92）352頁〔渡辺咲子〕。

99）　このことは、リモートアクセスによる複写の処分をする場合であっても、接続先のサーバ全体の管理者に対して令状の呈示をしないであろうことにも沿う。なお、小林充「貸金庫・コインロッカーに対する捜索令状とその執行」新関雅夫ほか『増補令状基本問題（下）』227頁（判例時報社、1996年）が、貸金庫の存在する場所の管理権を有し、貸金庫の合鍵等を保管する銀行は、貸金庫全体について二次的な管理権を有するとしていることからすれば、プロバイダが被処分者のデータにアクセスできるならば、プロバイダも個々のアカウントに対応する記録領域について二次的な管理権を有するといえるだろう。

100）　笹倉・前掲注19）34-37頁。

101）　河上ほか編・前掲注92）269頁〔渡辺咲子〕。

102）　杉山＝吉田・前掲注３）108頁（注７）。

103）　笹倉・前掲注19）34頁。

104） 笹倉・前掲注19）34-35頁。
105） 井上・前掲注64）413頁、山内・前掲注67）19-20頁。
106） なお、裁判例に従って、刑訴218条２項の趣旨を「捜査の必要と第三者の権利・利益の保護の調和」と解したとしても同様であろう。
107） 酒巻匡『刑事訴訟法』（有斐閣、2015年）24-25頁。
108） 笹倉・前掲注19）35-36頁。
109） 笹倉・前掲注19）36頁。
110） 差押えを前提としないリモートアクセスを行う現状における第一の意義は、差押終了後であってもリモートアクセスを可能にすることである。また、さらには国内にサーバが所在する場合には、サーバの差押えに代わる刑訴110条の２第１号の処分を行い得ることから、国外にサーバが所在する場合に最も必要性が高い。
111） 山内・前掲注67）20頁、本論文・前掲注96）。
112） 最決平成14年10月４日刑集56巻８号507頁、長沼範良「ネットワーク犯罪への手続法的対応」ジュリ1148号（1999年）216頁参照。なお、事後的な呈示ではなく通知によるには、立法を要しよう。
113） 最決平成11年12月16日刑集53巻９号1327頁。
114） 笹倉・前掲注19）37頁。なお、同論文は、通信傍受法制定後の決定であることから、「先例としての意義を過大に評価すべきではないかもしれない」としている。