逮捕に伴う電子機器の内容確認と法的規律

――Riley 判決を契機として――

緑　　大　輔※

Ⅰ　問題の所在

刑事訴訟法上、逮捕する場合において必要があるときには、逮捕の現場で令状なく捜索差押え等を行うことが可能であり（刑訴法 220 条 1 項および 3 項）、押収品に対して、「錠をはずし、封を開き、その他必要な処分」をすることができる（同 222 条 1 項、111 条 2 項）。本稿は、これら条項の下における、逮捕時に押収された電子機器の内容確認について、その限界と規律方法を検討する。従前は、逮捕時に押収された品に付随するプライバシーには、物理的な限界が存在した。しかし、SNS や Web メールに個人の行動履歴が蓄積され、それを携帯電話等の小型端末として人々が身につけている現在、逮捕時に無令状で押収される証拠物から膨大かつ多様な情報が取得されうる。この変化に対して、従前の逮捕に伴う捜索差押えに関する議論の枠組みは、どのような帰結をもたらしうるか。そして、携帯型の電子機器におけるプライバシーを保護するために、現時点において、どのような方策が考えられるのか。本稿は、これらの問題について、アメリ

『一橋法学』（一橋大学大学院法学研究科）第 15 巻第 2 号 2016 年 7 月　ISSN 1347－0388
※　一橋大学大学院法学研究科准教授

カ合衆国の Riley 判決を契機として、刑事訴訟法の観点から検討を加える。

Ⅱ　Riley 判決

1. 事案の概要

Riley 判決は、逮捕時に被疑者が所持していた携帯電話を、捜査機関が無令状で差し押さえた上で、その内容を確認した事案である[1)]。Riley 事件と Wurie 事件が併せて審理された。

Riley 事件では、期限切れの登録証で自動車を運転していた被告人の車内から銃器が発見され、車内に銃器を隠匿・所持していた被疑事実で被告人が逮捕された。この逮捕に伴う捜索により、警察官は被告人のズボンからスマートフォンを発見し、これを押収した。警察官はその場でスマートフォンの内容を確認して、ギャングの隠語を発見した。逮捕から 2 時間後、警察署内でギャング対策専門の捜査官がスマートフォンの内容を網羅的に確認し、ギャング同士の口論の動画、数週間前の銃撃事件に関与した疑いのある車両の前に立つ被告人の写真等を発見した。その後、被告人は上記銃撃事件に関して、銃器を用いた暴行等の事実で起訴された。被告人側は、無令状で携帯電話の内容を確認した行為は修正 4 条違反にあたるとして、関連証拠の排除を主張した。事実審は申立てを斥け、控訴審はカリフォルニア州の裁判例を引き[2)]、事実審の判断を支持した。カリフォルニア

1)　*Riley v. California*, 134 S. Ct. 2473, 573 U.S. ___ (2014). 携帯電話の内容確認を合衆国の判例は「search」と表現する。以下、合衆国判例に触れる場面では、修正 4 条の適用問題として議論されていることを踏まえて、原則として「捜索」の語を当てる。本判決を紹介した文献として、成瀬剛「アメリカの刑事司法・法学教育の一断面 ── 最近の連邦最高裁判例を素材として」法学教室 411 号（2014 年）164 頁以下、柳川重規「逮捕に伴う捜索・押収の法理と携帯電話内のデータの捜索 ── 合衆国最高裁 Riley 判決の検討」法学新報 121 巻 11 = 12 号（2015 年）527 頁以下、笹倉宏紀ほか「座談会：合衆国最高裁判所 2013–2014 年開廷期重要判例概観」アメリカ法 2014–II（2015 年）290–294 頁，英米刑事法研究会「英米刑事法研究（29）アメリカ合衆国最高裁判所 2013 年 10 月開廷期刑事関係判例概観」比較法学 49 巻 1 号（2015 年）180–183 頁［洲見光男執筆］、山田哲史「新技術と捜査活動規制（1）── 合衆国最高裁 Riley 判決の検討をきっかけに」岡山法学会雑誌 65 巻 1 号（2015 年）178 頁以下、池亀尚之「判批」アメリカ法 2015–I（2015 年）144 頁以下、森本直子「被逮捕者の携帯電話の捜索と令状の必要性」比較法雑誌 49 巻 2 号（2015 年）336 頁以下。

州最高裁も被告人側の主張を退けたため、被告人側は連邦最高裁に上告した。

Wurie 事件では、警察官が被告人を薬物販売で現行犯逮捕して警察署に連行し、同署内で被告人が所持していた携帯電話２つを差し押さえた。本件争点の携帯電話は、旧式の二つ折り携帯電話であった。警察署に到着後、警察官は当該携帯電話への着信に気づき、当該携帯電話を開き、画面の壁紙に女性と乳児が写っていることと「my house」という名が登録された電話番号を確認した。これらの情報から、警察官は被告人の自宅を割り出し、当該居宅に対する捜索令状を請求し、執行した。その結果、コカイン、銃器等を発見した。被告人はその後、コカインの販売目的所持や銃器・弾薬所持で起訴された。被告人側は、修正４条に反する携帯電話の「捜索」にあたることを理由に証拠排除すべきだと主張したが、事実審（連邦地裁）はこれを斥けた。これに対して、連邦控訴裁判所は証拠排除すべきとの判断を示したため、検察側が上告した[3]。

以上の経緯を経て、２つの事件は連邦最高裁で審理された。

2. 判旨

⑴ 連邦最高裁は、ロバーツ首席裁判官による全員一致の法廷意見として、捜査機関が逮捕に伴って無令状で携帯電話の内容を確認する行為は修正４条に違反すると判断した。以下、後の検討に必要な限りで紹介する。

法廷意見は、憲法起草時には携帯電話等の取扱いに関する明確な指針がなかったとした上で、本件捜索への令状主義の適否は、個人のプライバシーに対する制約の程度と、正当な政府の利益に資する程度とを評価して判断すべきだとする。その上で、逮捕に伴う無令状捜索に関する３つの先例と対比している。

⑵ まず、逮捕に伴う捜索が無令状で許容される理由を、逮捕執行者の安全の確保および被逮捕者による証拠隠滅の防止に求めた、Chimel 判決の観点から検討している[4]。同判決は無令状捜索が許容される場所的な範囲は、被逮捕者の身体およびその直接支配下（within his immediate control）だとした[5]。本件との

2) *People v. Diaz*, 244 P. 3d 501 (Cal. 2011).
3) *United States v. Wurie*, 728 F. 3d 1 (1st Cir. 2013).
4) *Chimel v. California*, 395 U.S. 752 (1969).

関係では、無令状捜索を正当化する、逮捕執行者の安全の確保と被逮捕者による証拠隠滅の防止という利益の程度が問題になる。法廷意見によれば、逮捕執行者の安全確保について、携帯電話に蓄積されているデジタルデータそのものは、逮捕執行者に対して抵抗し、あるいは逮捕執行者から逃亡するために武器にはならない。それゆえ、携帯電話（のカバー等）に対して凶器の有無を確認できるが、携帯電話内のデータの捜索までは正当化できないとする[6]。また、検察側は、第三者の遠隔操作によるデータ消去やパスワードロックを通じた証拠隠滅の危険性を主張していた。しかし、法廷意見は、原則として捜査機関が携帯電話を差し押さえれば、被逮捕者はデータ消去等を為し得ず、データを捜索する必要性は認められないとする。また、Chimel 判決と比べて、本件は逮捕現場にいない第三者による消去行為のおそれの有無、電子機器を通じた隠滅行為の可能性の有無が問われており、同判決と事案が異なる。更に、そもそも遠隔操作によるデータ消去の実例が乏しく、押収後に当該携帯電話の電源を切り、あるいは電波を遮断する袋に当該携帯電話を封入する等して対処できると説示した。また、パスワードによるロックについても、通常、警察官が携帯電話のデータを捜索する前に、少し使用しないとすぐにロックがかかるようになっており、警察がロックされる前にデータを捜索できる場合自体が極めて例外的なものに過ぎないと指摘している。

(3)　次に、プライバシーの制約の程度につき、Robinson 判決と対比して検討している[7]。同判決は、免許停止中の被告人が自動車を運転していたのを警察官が現行犯逮捕して身体を捜索し、タバコの箱を発見してその中にあったヘロインを押収した事案において、適法な逮捕が行われた以上、捜索に別途正当化事由は要さず、一律に捜索できるとしていた[8]。検察側は、被逮捕者のプライバシーは身体拘束に比べれば付随的な制約にとどまるので一律に捜索できるという、Rob-

5)　Chimel 判決について、田宮裕「逮捕に伴う捜索・押収」判タ 248 号（1970 年）26 頁、同『捜査の構造』（有斐閣、1971 年）215 頁以下所収等参照。

6)　検察側は、被逮捕者が仲間を呼んで逮捕執行を妨害する事態を予防する必要性も主張したが、法廷意見は、検察側主張を支える証拠がない上、Chimel 判決が被逮捕者の武器の所持の有無を捜索することのみを想定しており、検察側主張のような事態まで包摂した判例ではないとして斥けた。

7)　*United States v. Robinson*, 414 U.S. 218（1973）. 緑大輔「合衆国での逮捕に伴う無令状捜索」一橋論叢 128 巻 1 号（2002 年）75 頁以下、77 頁等参照。

inson 判決の論理が本件に及ぶ、と主張していた。しかし、法廷意見は携帯電話が量的にも質的にも、被逮捕者が身につけている他の所持品とは異なり、Robinson 判決の射程は本件に及ばないとする。

量的な相違として、現在の携帯電話には膨大な情報が収集・保存されており、かつこれらの情報が携帯電話に集約されており、情報を結合して個人の私生活の状況を再現できる。しかも、それは過去に遡って行うことも可能である。したがって、携帯電話の所持が一般化した現在、携帯電話内のデータの無令状捜索を一般的に認めることと、従前の有体物への無令状捜索の許容とは意味が大きく異なるという。

また、質的な相違として、携帯電話は、有体物とは異なり、ウェブの閲覧履歴や位置情報から、個人の興味関心や動静を明らかにできる。アプリは、政治的傾向や信仰、資産状況、趣味嗜好、病歴など様々な情報を管理しており、携帯電話内のデータの捜索は、居宅の捜索以上に多くの情報を捜査機関にさらす。更に、携帯電話のクラウド機能ゆえに、捜査機関は外部サーバに保存されているデータにアクセスできる。捜査機関は携帯電話内のデータとクラウド上のデータを容易には判別できず、被逮捕者の直接支配下を越えて、外部から情報を取得する可能性があり、プライバシーの制約を大きくする[9]。

(4) 更に、検察側は Gant 判決を引いて、携帯電話内に逮捕被疑事実と関連する証拠があると考えるのが合理的である場合に、無令状捜索を許容すべきだと主張していた[10]。Gant 判決は、被逮捕者の自動車に対して逮捕時に一律に無令状捜索をなしうるか否かについて検討し、被逮捕者が身体拘束されていない状況で

8) Robinson 判決は、身体の捜索と、その後のタバコの箱の中の確認行為を分別せず、適法な捜索の過程で箱を見つけた以上はその中身を確認できるという判断も含む。

9) この問題は、個人がプロバイダー等の第三者と情報を共有している場合にはプライバシーの要保護性が低下するという第三者法理も関連するが、本判決は触れていない。それゆえ、本判決が、少なくともデジタルデータに関して、第三者法理の放棄を示唆しているとの主張もある。*See e.g.* Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L. J. F. 73 (2014), http://www.yalelawjournal.org/forum/rileys -implications-in-the-cloud.

10) *Arizona v. Gant*, 556 U.S. 332 (2009). 免許停止であるにもかかわらず運転をしていた被告人を逮捕し、同人に手錠をかけて警察車両に移動させた上で、被告人の自動車内を無令状で捜索した事案である。洲見光男「判批」アメリカ法 2010-1 号 247 頁以下参照。

車内に手が届く場合にのみ、無令状捜索が許容されると説示していた。これとは別に、逮捕被疑事実に関連する証拠が車内で見つかると信じることに合理性がある場合には、いわゆる自動車例外として無令状捜索が許容されるとも説示していた。これに対して、法廷意見は、Gant 判決が自動車におけるプライバシーの要保護性の減少や捜索の必要性の高さを前提としたものであり、携帯電話内のデータの捜索とは事案が異なるという。また、同判決の基準は自動車と携帯電話では保有する情報の性質に違いが大きく、携帯電話内のデータの捜索に対して現実的に機能しないという[11]。

また、被疑事実や被逮捕者の身元、警察官の安全に関する情報が発見されると合理的に信じることができる範囲で、携帯電話内の捜索が許容されるべきだとの検察側の主張に対しては、それを認めると結果的に膨大な情報が捜索され、実質的に捜索範囲を限定できないと指摘して斥けた。

(5)　以上の理由で、法廷意見は、逮捕に伴う場合でも、携帯電話内のデータを捜索するには予め令状を取得する必要がある旨を判示した。但し、事案によっては緊急事態例外が適用される余地がある旨が確認されている[12]。

3. 本判決が示す連邦最高裁の姿勢

アメリカの逮捕に伴う無令状捜索に関する諸判例と本判決の関係は、本稿の目的ではない[13]。ただ、本判決はその脚注において、あくまで逮捕に伴う捜索に

11)　検察側は、無令状でペンレジスターにより被告人の架電先電話番号を調べることを許容した *Smith v. Maryland*, 442 U.S. 735（1979）を引いて、携帯電話の通話履歴の確認には令状を要しないと主張していた。法廷意見は、本件が（通話履歴以外のものも含めて）携帯電話のデータを捜索したことが明らかであり、通話履歴には電話番号以外の個人の身元等も含まれるため、事案が異なるとしている。

12)　アリート裁判官の補足意見は、法廷意見の結論に賛成しつつも、(1) Chimel 判決が逮捕執行の場面での判断であって、本件のような（逮捕完遂後の）被逮捕者の身体の捜索を行う場面とは異なり本件の先例に当たらないこと、(2)法廷意見によれば、携帯電話内のデータだと無令状で捜索できず、それ以外であれば無令状で捜索できるという不均衡な結論が生じること、(3)携帯電話内のデータの捜索の規律は、司法府よりも立法府の方が適切に判断できることを指摘する。

13)　先例との関係の分析については、柳川・前掲注 1)、山本・前掲注 1)、池亀・前掲注 1）参照。*See also,* Leslie A. Shoebotham, *The Strife of Riley: The Search-Incident Consequences of Making an Easy Case Simple*, 75 LA. L. REV. 29（2014）.

ついての判断であって、その他の場面のデジタルデータの内容確認等には及ばない旨が言明している[14]。そのため、本判決がデジタルデータに対する捜査の在り方を全体的に変容させるか否かは不明確である[15]。アリート裁判官の補足意見が示唆するとおり、デジタルデータの収集に対する法的規律については、既存の判断枠組みでは司法府は充分に対応しきれず、立法府によるルール形成を経る方がよいという価値判断があるのならば[16]、連邦最高裁がデジタルデータの問題について、射程を限定して判断を積み重ねることには理由がある。

もっとも、Riley 判決が示した論理は、日本の刑事手続との関係でも示唆を与えるものと考えられる。以下では、Riley 判決の日本法への含意について、Riley 判決を契機とするアメリカの議論も適宜参照しつつ検討する。

Ⅲ　日本法に対する含意

1. 問題の位相

Riley 判決の事案では、逮捕現場で押収された後に、主として連行先の警察署で携帯電話内のデータの内容確認が行われた。そのため、Riley 判決における内容確認は、日本の刑事訴訟法に即して言えば、逮捕に伴う差押え（刑訴法 220 条 1 項）によって得られた、押収物に対する「必要な処分」（222 条 1 項、111 条 2 項）に該当する[17]。したがって、Riley 判決は、日本に置き換えれば、押収物に対する「必要な処分」に限界が存在し、携帯電話のデータの内容確認には令状を要する旨を説示したものだといえる。

14） *Riley*, 134 S. Ct., at 2489 n. 1.

15） 成瀬・前掲注 1）169 頁は、Riley 判決の脚注に触れつつ、「修正 4 条の下でのデジタルデータに対する捜査活動の全てのあり方を変える可能性を持っている」と評する。

16） 無令状で自動車の動静監視を GPS 端末で行ったことの適否を判断した、*United States v. Jones*, 132 S. Ct. 945（2012）におけるアリート裁判官補足意見も、GPS 端末による動静監視は立法での解決が望ましいとする。*Jones*, 132 S. Ct., at 964.

17） 成瀬・前掲注 1）170 頁。

2.「必要な処分」の限界

(1)　刑訴法 220 条と「必要な処分」の相関

Riley 判決は、「押収物に対する内容確認も、逮捕に伴う無令状捜索を正当化する『逮捕執行者の安全確保』『被逮捕者による証拠隠滅の予防』を実現するために行われるべきだ」という論理を前提にしている点で、特徴的といえよう。このことは、刑訴法 222 条 1 項・111 条 1 項および同条 2 項がいう「必要な処分」の趣旨が、220 条の趣旨と連動することを意味する。確かに、刑訴法 111 条の「必要な処分」は、捜索・押収を完遂するために「必要」な処分として設けられている。そうである以上、当該捜索・押収の目的を前提として処分の適否 ── 特にその必要性について ── を判断することは自然だろう。以上の理解を前提とするならば、刑訴法 220 条 1 項の趣旨について議論のあるわが国の状況に照らして、「必要な処分」の持つ意味は見解によって違いを生じうる。

(2)　緊急処分説と「必要な処分」

第 1 に、220 条の趣旨について、アメリカ合衆国の Chimel 判決と同様に「逮捕執行者の安全確保」と「被逮捕者による証拠隠滅の予防」に重点を置いて理解する、いわゆる緊急処分説（限定説）が主張されている[18]。この見解によれば、押収物の内容を確認する目的は、どのように理解されるべきか。従前さほど自覚的な議論がなされぬまま、緊急処分説の下では、押収された証拠物は証拠収集の一環として押収されたものとして理解されてきたように思われる。しかし、Riley 判決が示すように、押収された証拠物の内容確認も、逮捕に伴う差押えの趣旨と合致するように解するとすれば、111 条の処分を執行する必要性は、逮捕執行者の安全確保と被逮捕者による証拠隠滅の予防の観点から判断されるべきである。

しかし、Riley 判決が示すように、逮捕執行者の安全確保と被逮捕者による証拠隠滅の予防のために、携帯電話の外観のみならず、携帯電話内のデータを確認する必要性が認められる事態は稀であろう。差し押さえてしまえば、証拠隠滅の

18)　筆者は緊急処分説を妥当と考える。詳細は、緑大輔「逮捕に伴う対物的強制処分 ── 緊急処分説の展開」村井敏邦先生古稀記念論文集『人権の刑事法学』（日本評論社、2011 年）234 頁以下。

問題も基本的には生じないし、なお不安があるならば電波を遮断する袋に封入すればよいという説明が、ここでも意味を持つ。したがって、特段の事情がないかぎり、111 条の処分を執行する必要性が認められない。内容を確認するためには、証拠収集を目的とする令状を別途必要とする可能性が導かれよう。無論、このように内容確認に対して慎重さを期する背景には、Riley 判決法廷意見が詳述していたように、携帯電話に包蔵されている情報の「量と質」ゆえだといえよう。

まとめると、緊急処分説の下では、携帯電話内のデータを確認する必要性に乏しく、かつプライバシーの要保護性が高いため、逮捕に伴って押収された携帯電話内のデータを当然には確認できない[19]。この場合、携帯電話の差押えは、後の内容確認のための一時保全として位置づけられる[20]。これに対して、わが国では逮捕に伴う場合を除いて、アメリカ合衆国のような緊急事態に基づく無令状捜索が許されていないため、携帯電話内のデータが消去される現実的危険が生じた場合でも、捜査機関は令状を請求する必要が生じて不合理だとする批判が考えられる[21]。しかし、緊急処分説が証拠隠滅の防止を目的して掲げる以上、携帯電話内のデータが消去される現実的危険が生じた場合には、111 条の必要な処分として無令状で内容確認を執行することは許されよう。

⑶ 相当説と「必要な処分」

第 2 に、220 条の趣旨が、「逮捕現場に証拠が存在する蓋然性の高さ」を前提として逮捕現場における証拠収集にあると理解する、いわゆる相当説（合理説）が主張されている。この見解によれば、押収物の内容を確認する目的は、証拠として当該押収物から情報を取得することにあると説明されよう。したがって、111 条の処分を執行する必要性は、証拠として情報を取得する観点から判断されるべきことになる。

このような理解からは、結局のところ、捜索差押令状が発付された場合におけ

19） これに対して通常の有体物は、押収時点で一定程度に限定された範囲のプライバシーの要保護性が低下するため、証拠物として内容確認をすることが許容されると説明できる。

20） 最決平成 10 年 5 月 1 日刑集 52 巻 4 号 275 頁は、内容を確認するための一時保全を「差押え」として許容した意味を有する。緊急処分説の下での携帯電話の差押えは、この最高裁判例が認めた「差押え」に類する性質を持つといえよう。

21） 成瀬・前掲注 1）170 頁参照。

る「必要な処分」と、その性質に異なるところはない。捜索差押令状によって押収された携帯電話機内からデータを読み出す行為については、別途の令状を要さず、222 条 1 項および 111 条 2 項ないし押収の本来的効力として執行できるものと説明されている以上[22]、逮捕に伴う場合も同様に 111 条 2 項により携帯電話内のデータを確認できるという帰結を導きうる。

もっとも、相当説が一義的に上記帰結しか導きえないわけではない。携帯電話内のデータの内容確認をする必要性に対して、それを凌駕するプライバシーの要保護性を認めるならば、別途令状を要するとの立場も成り立ちうる。ただ、緊急処分説の場合とは異なり、111 条の処分の必要性は肯定する以上、プライバシーの要保護性と情報取得の必要性の間の衡量はせざるを得ない。そこで、(a)この利益衡量が事案に即して個別具体的に行われるべきか、(b)類型的にプライバシーの要保護性が高いと判断して一律に携帯電話内のデータを読み出すことはできないとするか（上述の緊急処分説と同じ帰結となる）、(c)類型的にプライバシーの要保護性が低い（ないし携帯電話の占有が剝奪された以上、プライバシーは付随的な制約に過ぎない）と判断して、一律に携帯電話内のデータを読み出すことはできるとするかについて、検討を要する。(a)を支える説明は、証拠収集の必要性の程度は事案による上、携帯電話の使用頻度や使用態様は人によって相違がある以上、類型的な判断に馴染まないというものであろう。これに対して、(b)(c)を支える説明として、相当説が明白なルール（bright line rule）を志向する立場だとの理解を基礎とするものがありえよう。相当説は、逮捕に伴う無令状捜索の場所的限界について、捜索差押令状が発付されたらその効力が及ぶであろう「場所的同一性」が認められる範囲としている。これは緊急処分説に比べて明確な範囲であり、捜査機関に明確なルールを示す点にその意義があるのだとすれば[23]、携帯電話についても類型的な判断枠組みを提供すべきだろう。その上で、携帯電話内のデータの確認が、住居の捜索に匹敵するプライバシーの制約を伴うと考えるな

22)　杉原隆行「押収した携帯電話機内のデータを読み出すための令状」別冊判例タイムズ 35 号『令状に関する理論と実務 II』（判例タイムズ社、2013 年）146 頁。

23)　緑・前掲注 7）88 頁。なお、Riley 判決が携帯電話内のデータについてカテゴリカルな判断をしたと評するものとして、池亀・前掲注 1）151 頁。

らば、(b)の理解を政策的に採用する余地はある。

まとめると、相当説においては、携帯電話内のデータを確認する必要性が認められるため、押収された携帯電話内のデータの確認は許容されうる。ただし、携帯電話内のデータのプライバシーの要保護性が高いと見積もった場合に、内容確認をする必要性と衡量して、無令状では内容確認ができないとする余地はある。

Ⅳ　内容確認とプライバシーの保護

1. 令状主義の有効性？

以上で検討したとおり、実体的なプライバシーの利益を保護する枠組みとして、ありうる選択肢の１つが、逮捕に伴って押収されたスマートフォン等の携帯電話の内容確認をする際に、令状を要求するという方法である。その場合、既に差押えが為されている以上、処分の実質は携帯電話内のデータ内容を視認することに尽きるため、現行刑訴法の下では検証令状を用いることになる[24]。

これに対して、日本では Riley 判決と同じく考える必然性はないという理解もありうる。即ち、(a)アメリカと異なり、日本では通常逮捕が主であるため、逮捕令状の審査を通じて被疑者に対する被疑事実の嫌疑の存在が担保されていること、(b)アメリカでは軽微事件でも逮捕されるため、無令状捜索差押えの問題が深刻化しやすいこと、(c)令状審査の際の疎明がアメリカでは日本よりも簡易であること、(d)アメリカでは逮捕の場合以外にも緊急事態例外が認められており、無令状で携帯電話の内容確認をする余地があることが、Riley 判決の背景の違いとして指摘されている[25]。しかし、「携帯電話内の膨大な情報に対して、その捜索範囲をどのように限定するか」という問題を両国ともに抱える。その対応策として、令状手続のコスト、被逮捕者のプライバシーの保護、捜査機関にとって必要な情報の取得の担保について均衡をとりうるならば、令状による規律も検討すべきである。

もっとも、わが国の現状の令状をデジタルデータに対してそのまま活用できるとは言い切れない。通常の捜索差押令状における目的物を特定する際には、「差

24）柳川・前掲注 1）547 頁。
25）成瀬・前掲注 1）169 頁。

し押さえようとする目的物だけに備わっている特徴を具体的に明示することが最も望ましい」とされる。しかし、現実には予め特徴まで特定することが困難であり、また、特定を厳格に求めると却って被疑者取調べによって特定した上で、対物的強制処分を行うといった「捜査の方向を歪める結果」をもたらしうるため、ある程度概括的、抽象的に記載することもやむを得ないと主張されている[26]。また、被疑事実に関わりのない個人情報が多く含まれている可能性がある電磁的記録媒体やパソコンを目的物とする場合においても、「顧客名簿が入力されている CD-R」「本件と関係のある情報が記録されたパーソナルコンピュータ」などの記載で足りるとの主張も見られる[27]。

この場合、個々の有体物の特定はなされても、当該有体物の中に膨大なデータが保有されている以上、実質的には広範なプライバシーが捜査機関にさらされる。したがって、既存の令状の特定方法では、プライバシーの保護には充分に機能しないだろう。また、逮捕に伴う押収によって得た携帯電話に対して、検証令状により内容を確認する際に、検証対象として当該携帯電話機器が明記されるにとどまるならば、やはり令状はプライバシーの保護のために充分に機能しないことになろう。

しかし、文脈は逮捕の場面に限定されないが、アメリカでは、司法府による令状主義を通じてプライバシーを保護する方が、立法よりも優れているとの主張がある。それによれば、デジタルデータの収集によるプライバシーの制約に対して、令状主義は処分範囲の最小化、処分対象の特定、令状審査による捜査機関への制御を期待しうる[28]。また、(a) 立法は必ずしも網羅的な規律ができるわけではなく、救済手段の欠如や技術の発展に対応できていない場合などがあり、(b)

26)　秋山規雄「捜索差押許可状における目的物の特定」新関雅夫ほか『増補令状基本問題・下』(一粒社、1996 年) 235 頁以下、236 頁。最大決昭和 33 年 7 月 29 日刑集 12 巻 12 号 2776 頁参照。

27)　樺清隆「被疑事実に関わりのない個人情報等が多く含まれていると予想される電磁的記録に係る記録媒体やパソコン全体を差押対象物とする捜索差押許可状発付に当たり考慮すべき事項」別冊判例タイムズ 35 号『令状に関する理論と実務 II』(判例タイムズ社、2013 年) 152 頁。池田修「判解」最判解説刑事篇平成 10 年度 78 頁以下、83 頁。

28)　Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 219 (2004).

少なくともアメリカ合衆国の場合、立法の方がプライバシーの保護の点で手続的な保障が不十分になることが多く、(c) 立法は必ずしも司法判断に比べて明確なルールを提供するわけではないという[29]。これに対して令状主義は、事後的に個別具体的な事情に応じた柔軟な対応が可能であるし、裁判所が情報技術の専門知識を必ずしも十分に有していない点は鑑定等に通じて解決可能だと主張する[30]。このように、令状主義にも有用性があるならば、それは具体的な検討に値しよう。そこで、令状を中心とした規律手法の下で、プライバシーを過剰に制約せずに、かつ被疑事実に関連する情報を取得するには、どのような法的規律を設ければよいのかについて、以下で検討を進める。

2. アメリカの最小化措置の示唆

(1) Rule 41 の 2 段階過程の最小化措置

アメリカでは、クラウド上に保存されているデータを捜査機関が取得する場合にとりうる、特殊な手続を設けている[31]。まず、捜査機関がプロバイダーに対して、取得しようと考えるアカウントの全記録を複写させる等して開示させる。その中から取得したい情報を選別する。そして、開示後 2 週間以内に、令状を執行して、取得対象となる情報のみを取得する。これにより、捜査機関の手許に保存される情報を、捜査に必要なもののみに限定する。

これは、通信傍受において行われる、犯罪関連通話の該当性判断のための傍受（通信傍受法 13 条）を実施した上で、犯罪関連通話の傍受を行うのと同様の発想だといえよう。権利利益の制約を最小化するための措置である。しかしながら、通信の場合と異なり、データの場合はファイル名などで一見明白に被疑事実との関連性を判断できるわけではなく、隠語を用いる可能性をも考慮すると、結果的

29） Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 761-771 (2005).

30） *Ibid*., at 771-772.

31） FED. R. CRIM. P. 41 (e)(2)(B). なお、Rule 41 の背景として、情報通信に関する制定法（Stored Communications Act 等）および電子メールの内容が修正 4 条の保護対象にあたると判断した *United States v. Warshak*, 631 F. 3d 466 (6th Cir. 2010) を紹介する、堀田周吾「サイバー空間における犯罪捜査とプライバシー」法学会雑誌 56 巻 1 号（2015 年）569 頁以下、582-587 頁参照。

に内容の点検を広範かつ詳密にやらざるを得ない[32]。実際、Rule 41 はそのような観点から、被疑事実との関連性を判断するための第 1 段階の開示を広範に求める形を採用したと理解できる[33]。

このことは、通信傍受法のような 2 段階の過程による最小化措置は、データに対しては必ずしも機能しない可能性を示唆する。少なくとも、捜査機関が自ら情報を精査して第 1 段階の情報選別を行う限り、プライバシーを過度に制約するとの批判は免れない。この問題を解消しうる一つの方策は、取得対象該当性を判断するために、対象となる携帯電話等にパソコンを接続し、特定の拡張子や特定の用語を含むファイルのみを拾い上げて確認できるようにしたりする等の方法が考えられる[34]。また、更に一歩進めて、複写された電子記録媒体に対して、アルゴリズムを用いて不必要な情報を自動的に削除し、選別された情報のみを捜査機関が利用できるという方式も考えられる[35]。

(2)　令状における対象期間制限・情報種類制限

これに対して、下級審で捜査機関が取得する情報の範囲を限定する動きが見られる。例えば、捜査機関が Web メールおよび無料通話ソフト Skype に存在する電子メールやインスタントメッセージ、チャットログを取得しようとして捜索令状を請求した事案において、取得するメール等の時間的な範囲について、被疑者らの共謀が開始されたと疑われる「2006 年 6 月以降」との制限を令状に付した事例がある[36]。

---

32)　井上正仁『強制捜査と任意捜査（新版）』（有斐閣、2014 年）406 頁、初出：法学教室 244 号・255 号（2001 年）。

33)　もっとも、Rule 41 における第 1 段階の開示がプライバシーの広範な制約を伴うとして、2009 年にはこの Rule 41 の適用を慎重に行うよう求めるに至った。FED. R. CRIM. P. 41 committee's notes to 2009 amendment, http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-app-federalru-dup1-rule41.pdf.

34)　Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 544-547 (2005).

35)　Note, *Data Mining, Dog Sniffs, and The Fourth Amendment*, 128 HARV. L. REV. 691, 708-712 (2014). なお、アルゴリズムを構築する初期データとして、何をどこまで収集し、どのように組み込むのか等の問題を解決する必要がある。人工知能技術を応用した、Predictive Coding によって対象情報を分別する場合も、初期学習のためのデータを要する点で、同様の課題がありうる。町村泰貴ほか編『電子証拠の理論と実務』（民事法研究会、2016 年）315 頁以下〔野崎周作〕参照。

Riley 判決が指摘したとおり、携帯電話内のデータ確認は、過去に遡って可能である点でもプライバシーの過剰な制約を伴いうる。この問題は、パソコン等を通じたクラウド上の情報の取得一般に当てはまる。このように、アカウントからアクセスして取得できる情報について、過去への遡及を限定する趣旨でメール等の取得対象となる期間を特定・明示した令状を発付することは、プライバシーの保護のためになしうる方法の一つだろう。

また、取得対象期間の特定に加えて、情報の種類について具体的な制限を加えた事例もある。銃撃事件に関して捜索令状を発付する際、SNS である Facebook 上で取得対象となる情報の開示に際して、第三者から対象アカウントに送信されたメッセージ、対象アカウントがタグ付けされた写真・動画の中で第三者が写っているもの等は対象外とする旨の特定がなされた[37]。対象アカウントのあらゆる情報の取得を認めるのでは、一般令状に等しい問題が生じると考えて、このような特定を付した旨が理由として示されている[38]。

これらの動向は、わが国の場合、逮捕に伴って既に押収された携帯電話に対する処分を行う場合は、上述の通り検証令状の記載にかかわる。検証令状による場合は、電話検証に関する最高裁平成 11 年決定が、傍受すべき通話、傍受対象となる電話回線、傍受できる期間等をできるかぎり限定するよう求めている[39]。上述のアメリカの動向は、この最高裁決定に類する記載をデジタルデータに求めるものだといえよう。逮捕が完遂された後に携帯電話内のアプリに関連する情報を取得するのであれば、被疑者取調べ等を通じて、対象の特定に資する事情を解明できる場合もあろう。そのため、上述のような特定は、通常捜索の場面に比べても、より一層可能な場合が多いだろう。但し、検証令状の場合は、情報の消去

36） *In re Target Email Accounts/Skype Accounts*, 2013 U.S. Dist. LEXIS 123129（D. Kan. Aug. 27, 2013）.

37） *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron. Alexis*, 21 F.Supp. 3d 1（D.D.C. 2013）. なお、Facebook では、写真等の投稿時に、被写体の者のアカウントが自動的にタグ付けされる。

38） 他に、疎明の際に、携帯電話内のデータの内容確認時に使用する予定のキーワード及び読出用ソフトウェアを明示するよう捜査機関に求めた事例として、*See, In re Search of Apple iPhone*, 31 F.Supp. 3d 159（D.D.C. 2014）.

39） 最決平成 11 年 12 月 16 日刑集 53 巻 1327 頁。

を求める等の不服申立手段がない点は問題であり、立法的な措置が必要であろう。

これに対して、逮捕に伴わず通常差押えに付随する処分の場合は、電気通信回線で接続している記録媒体からの複写（刑訴法 99 条 2 項）に関連して求められている、「差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって、その電磁的記録を複写すべきものの範囲の記載」（刑訴法 107 条 2 項、219 条 2 項）にかかわりうる[40]。この記載は、サーバに係るサービスの種類（メールサーバ、ファイルサーバの別など）、アクセスのための ID などによって定められる旨が主張されている[41]。これらの特定に加えて、上述のような取得対象期間の制限、あるいは取得対象となる（取得対象とならない）情報の種類の特定は、包括的なプライバシーの制約を回避するため有用だろう。日記帳等と異なり、膨大なデータを一括して容易に取得できる特殊性ゆえに、特定・明示の要請が強まると考えれば、以上のように取得データを限定する特定・明示の要請は不合理ではないだろう[42]。

(3)　フィルタリング措置

事件を担当する警察官自らが膨大な情報を取得するよりは、当該事件の捜査に直接には関与していない第三者が担当警察官とともにデータの内容確認をする方が、過剰なプライバシーの制約を回避する可能性が高まるであろう[43]。例えば、弁護人と依頼人たる被告人の間で送受信されたメールを取得対象から除外するために、フィルタリング・エージェント（a filtering agent）が付された事例がある[44]。わが国の通信傍受法における通信事業者等の立会時の意見（通信傍受法 12 条 2 項）に近いように思えるかも知れないが、令状発付裁判官によって、令

40)　電気通信回線に接続していない携帯電話の内容確認や複写を伴わない内容確認の場合、現行法の枠組みの下では、以下に示すような令状でデータの範囲の限定をするアプローチは困難であるため、プライバシー保護のためには他の方策の検討を要する。

41)　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）」法曹時報 64 巻 5 号（2012 年）109 頁。

42)　ただし、司法府への事後的な不服申立ての判断次第では、令状記載における特定・明示の効果は減殺される。

43)　*See,* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010).

44)　*See e.g., United States v. Bickle*, No. 2: 10-cr-00565-RLH-PAL, 2011 U.S. Dist.LEXIS 94921, at *59 (D. Nev. July 21, 2011).

状にフィルタリングの手続が記載され、通信事業者よりも積極的にフィルタリングに関与することが期待される。したがって、いわば条件付きの捜索令状といえよう[45]。この事件については、弁護人と依頼人の間の秘匿特権の保障に加えて、プロバイダーであったMicrosoft社が捜査機関に対して過剰に情報を開示することを防止するための措置として評価しうる[46]。

もっとも、フィルタリングを行うエージェントを誰に委ねるかは問題である。通信事業者が行うとなれば、関連情報か否かを適切に判断できない可能性が高い[47]。他方で、当該事件の担当捜査官に近い者がフィルタリングを行うほど、フィルタリングの実効性に疑義が生じる[48]。もっとも、2段階過程の最小化措置で触れたのと同様に、フィルタリングを自動化する技術が構築できるならば、エージェントの問題は解消しよう。

⑷ その他の方策

更に、プライバシー保護法制の一環として、内容を伴う情報（メールやメッセージの文面等）と内容を伴わない情報（メールの宛先や日時）に分別し、前者については修正4条の下で最小化措置を講じるべきとし、修正4条の保護対象にならない後者については、裁判所が捜査機関に命じることができる「保存利用期間の上限」を立法府が設定することによって、プライバシーの制約の限界を画する提案がある[49]。また、修正4条の保護対象となる情報か否かを問わず、マジストレイト裁判官が、捜査機関の取得したデジタルデータについて、保存利用期間

45） エージェントに事件と無関係のメールや秘匿特権にかかわるメールのフィルタリングを行わせる条件を付する点において、日本の強制採尿の最高裁判例に類する。最決昭和55年10月23日刑集34巻5号300頁は、捜索差押令状に対して、医師をして医学的に相当と認められる方法により採尿を行わせなければならない旨の条件の記載を求めた。*See also, United States v. Danielson*, 325 F. 3d 1054, 1071–72（9th Cir. 2003）.

46） Reid Day, *Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services*, 64 U. KAN. L. REV. 491, 524（2015）.

47） この問題が生じたことを示す事例として、*In re Search of Information Associated with @mac.com*, 13 F. Supp. 3d 157（D. D. C. 2014）.

48） 警察内の情報解析部門の独立性を高めて、同部門がフィルタリングを実施する方策も考えられるが、適正性の担保が課題になる。

49） Orin S. Kerr, *The Next Generation Communication Privacy Act*, 162 U. PA. L. REV. 373, 412–414（2014）.

の上限を設定すべきだとする主張もある[50]。保存利用期間の設定は、被疑事実と関連性のない情報の目的外利用を回避する効果を持ちうる。少なくとも明らかに公判立証と関連しないデータについて、上述の期限の設定は可能ではないか（刑訴法 222 条 1 項、同 123 条参照）。他方で、これを裁判官が個別事案ごとに行うことには困難があろう。この問題は、立法府がその制度的な資源を活かして検討すべきである。そして、保存利用期間を設定するとしても、情報の性質や目的ごとにルールを設定すべきだろう。他方で、公判立証と関連するデータに保管期限を一律に設定することは困難であろう。

V　おわりに

Riley 判決を契機とした本稿の主張をまとめると、以下のとおりである。第 1 に、Riley 判決の論理を踏まえれば、刑訴法 220 条の趣旨は「必要な処分」の解釈にも及ぶ。第 2 に、緊急処分説・相当説のいずれについても、逮捕に伴って差し押さえられた携帯電話内のデータを確認するために、別途検証令状を要求する論理を採用することは妨げられない。第 3 に、令状を求めるとしても、プライバシーを実効的に保護する方策が求められ、(1) 2 段階過程を踏む最小化措置の採用、(2)取得対象たる情報の特定の具体化、(3)令状執行時に被疑事実と関連性を有しない情報のフィルタリングの実施、(4)立法によるデータの保存利用期間の制限が考えられる。ただし、(1)(3)については、捜査機関自身が行うよりも、アルゴリズムを構築して自動化する方が望ましい。仮に、逮捕に伴う携帯電話内のデータの内容確認に令状を要さないと解する場合、携帯電話内のデータ量の多さを真剣に受け止めるならば、少なくとも(1)(3)(4)のいずれかについて、立法を通じて捜査機関に義務づけるべきである。しかし、現状では令状によって規律するほか手段がないというのが、本稿の評価である。なお、通常の捜索差押令状によって携帯電話などを押収し、内容確認をする場合については、更に検討を要する（本稿で示した方策を、218 条 6 項の準用等により行うこと等が考えられる）。

50)　Day, *supra* note（46）, at 524-525.

携帯電話等の端末を製造するメーカーのセキュリティの在り方と、捜査機関によるセキュリティ解除の要請への対応の要否等も、ここでの議論に影響しうる[51]。データ化されたプライバシーの保護のためには、有体物を前提として構築されたシステムを、令状主義を超えてどのように更新すべきかは、今後の研究課題である[52]。

（本論文は JSPS 科研費 15K03166 の助成を受けている。）

51） FBI が携帯端末に捜索令状を執行する際、パスコードロックを解除するよう Apple 社に命じ、同社がそれに従わなかった事案を参照。*See e.g., In re Order Requiring Apple, Inc. to Assist in the Execution of a Seach Warrant*, 2016 U.S. Dist. LEXIS 25555（E. D. N. Y. Feb. 29, 2016）.

52） 笹倉宏紀「捜査法の思考と情報プライヴァシー権」法律時報 87 巻 5 号（2015 年）70 頁参照。他に、刑訴法 197 条 2 項の照会の在り方も検討を要しよう。