経営と経済　第95巻 第３・４号　2016年３月

通信の秘密不可侵の法規範との関係における通信用端末設備の法的位置づけ及びその内包する情報に対する保護のあり方

－米国の「逮捕に伴う捜索」に関する判例法理を手がかりとして－

海　野　敦　史

Abstract

This paper clarifies the extent of government's authorized access to information on cell phones and similar communications terminal devices under Paragraph 2, Article 21 of the Constitution of Japan, which protects the " secrecy of any means of communication. " This paper considers the U.S. standard that was established by the 2014 decision, Riley v. California. In this case, it was decided that the police must obtain a search warrant before they access the digital data on a cell phone seized from a person who has been arrested. The U.S. Court decided that it would be unreasonable to allow a search without a warrant, since the amount and variety of information on a cell phone often are enough that the police are able to reconstruct much of the suspect's private life. The U.S. Court also held that the extent of a warrantless " search incident to an arrest " is limited in the sense that it is allowed to find hidden weapons or prevent the destruction of evidence, and that this doctrine does not allow warrantless searches of cell phone data after an arrest. However, it does not fully explain the difference in the relevance to privacy between data on communications terminal devices and those on other devices or commodities. In Japan, Constitutional rights for secrecy of communications do not, in principle allow the police to implement a warrantless " search incident to arrest " to the content of communications terminal devices including a cell phone or any other communications facilities, regardless of its relevancy to privacy. This norm strongly protects communications users by preventing the police or other governmental agencies from having voluntary access to the communications terminal devices and data on them. It is thus concluded that the secrecy of communications plays an important role to distinguish data on communications terminal devices from those on other devices in terms of the extent of Constitutional protection.

Keywords: Constitution of Japan, secrecy of any means of communication, terminal devices, cell-phone handset, Fourth Amendment, Riley v. California, search-incident-to-arrest

キーワード：日本国憲法，通信の秘密，端末設備，携帯電話端末，修正４条，ライリー事件判決，逮捕に伴う捜索

1 序 論

日本国憲法（以下，「憲法」という）21条２項後段は通信の秘密不可侵について規定するが，ここでいう「通信」の成立に物理的に不可欠となる有体物が電気通信設備や郵便・信書便設備といった通信設備である。とりわけ，電気通信設備については，ネットワーク構造の高度化，複雑化等に伴い，その構成要素が多様化しているが，そもそも通信の秘密不可侵の法規範との関係における通信設備の法的位置づけ及び当該設備の具体的な射程については必ずしも明確ではない。もっとも，当該射程に関して，電気通信事業者が行う情報の伝送・交換等に不可欠となる伝送路設備及びその関連設備（電気通信回線設備[1]）については，一般にもっぱら当該事業者等が支配・管理するものであり，通信設備であることに疑いはない。問題となり得るのが，通信当事者（情報の発信者及び予定された着信者）において直接利用される端末設備[2]である。「通信」の利用者が所有又は占有する端末設備については，「通信」を行うのに必要となるものとして，（電気）通信設備の一端であると言えるのだろうか。

この点に関し，立法の次元に目を向けてみると，電気通信事業法（昭和59年法律86号）が，「電気通信設備」について，「電気通信を行うための機械，器具，線路その他の電気的設備」とその所有者・占有者の帰属とは中立的に定義していること（同法２条２号）が参考になると考えられる。この定義の内実については，「通信資材を相互に結合して，電気通信が可能な状態に構成され，かつ，電気通信を行う主体が支配・管理している状態にあるもの」を指すと解されている[3]。「電気通信」には，送信・伝送・受信のそれぞれの行為が含まれることから（同法２条１号参照），ここでいう「電気通信を行う主体」については，電気通信事業者のみならず通信当事者も含まれる。それゆえ，例えば自営の端末設備についても，「利用者が設置した時点で電気通信設備となる」ものとされている[4]。実際，電気通信事業法は，端末設備

について「電気通信回線設備の一端に接続される電気通信設備」（同法52条１項）と明文の規定で位置づけており，これが通信設備の一環を占めることを明確にしている。

もとより，憲法21条２項後段にいう「通信」は，その個々の行為としては，発信者から送信された情報が予定された着信者により最終的に受信され，又は受信され得る状態におかれることにより完結する（もっとも，後述するとおり，憲法上の「通信の秘密」〔以下，単に「秘密」という〕は，個々の「通信」の完結後も保護対象となると解される）。このとき，着信者による情報の電磁的な受信が物理的に可能となるためには，一定の端末設備が必要であり，当該受信に際してそれはネットワーク（伝送路設備）に接続されることから，当該端末設備は「通信」の完結のための必須要素となると言える。この点に関しては，当初の情報の送信時における発信者側の端末設備についても同様に妥当する。したがって，前述の法律上の整理から示唆されるとおり，通信当事者の利用する端末設備については，憲法21条２項後段にいう「通信」の成立に不可欠となる通信設備の一部を構成するものと捉えることが合理的である。

このような捉え方を前提とすると，通信の秘密不可侵の法規範との関係において次に問題となるのが，以下のような論点であろう。第一に，そもそも通信当事者の利用する「通信設備としての端末設備」については，誰が支配・管理していると言えるのであろうか。第二に，端末設備及びそれを通じてアクセスされ得る情報（以下，「端末内包情報」という）については，憲法21条２項後段の規定との関係において保護されるものとなるのか。第三に，仮に端末設備及び端末内包情報が憲法21条２項後段の規定との関係において一定の保護を受けるのであれば，公権力による端末内包情報に対する任意のアクセス[5]は，憲法の予定する正当な刑事手続上のプロセスに基づく場合その他「公共の福祉」の確保のために必要と認められる場合（以下，便宜上「正当手続きに基づく場合」という）を別論とすれば，基本的に禁止されること

となると考えられるところ，仮にかかるアクセスが認められる余地があるとすれば，それはどのような場合か。

周知のとおり，端末設備は，今日の国民生活で頻繁に用いられているインターネット等に接続された電子計算機ないしパーソナルコンピュータ（PC）や携帯電話端末の例に見るまでもなく，単に伝送対象の情報を送受信するのみならず，個々の通信に関する情報（すなわち，「秘密」たる情報）ないしその記録（通信記録）の保管庫としての役割も果たしている。それらの情報の中には，各人のプライバシーに深く関わる秘匿性[6]の高いものも多分に含まれ得る。仮にそのような情報が端末設備の不具合等により通信当事者の意に反して外部に広く「流出」することとなれば，憲法が予定する「秘密」の保護は事実上骨抜きとなり得るであろう。換言すれば，通信設備の構成要素のうち，いくら伝送路設備の安全性等が確保されていたとしても，端末設備のセキュリティが極めて脆弱であれば，当該設備と不可分の端末内包情報に関する「秘密」は適切に保護されないこととなり得る。したがって，通信の秘密不可侵の法規範の内実を解明する観点から，憲法上このような「流出」の事態に対して責任を負うことが予定された者の範囲についてはもとより，「秘密」たる端末内包情報及びそれを抱える端末設備に対して予定される保護のあり方を明確にすることにも十分な意義があると考えられる。

ところが，我が国の従前の学説・判例において，通信の秘密不可侵の法規範との関係における端末設備及び端末内包情報の保護のあり方に関する議論は極めて乏しい。むしろ，当該法規範は通信の利用者のプライバシーを保護することをその主旨とするものであって[7]，少なくとも端末設備を含む通信設備それ自体の保護を要請するものではないという認識が長く席捲してきた感もある。一方，近年のアメリカ合衆国（米国）においては，やや異なる角度から，端末設備及び端末内包情報が有する固有の特質に着目しつつ，それらの法的保護のあり方を追究する興味深い議論が展開されている。そこで本稿は，憲法21条２項後段の規定の趣旨との関わりにおける端末設備及び端末

内包情報の保護のあり方に焦点を当て，その考察に資すると思われる米国の主な議論を参照しつつ，当該保護に対する要請の内実を明らかにすることを目的とする。蛇足ながら，文中の意見にわたる部分はもっぱら筆者の私見であり，その所属組織の見解とは一切無関係である。

2　憲法上の「通信」の概念及びその射程

通信設備としての端末設備及び端末内包情報の法的保護のあり方を追究するのに先立ち，まずはそもそも憲法21条２項後段にいう「通信」とは何かということについて，明らかにしておきたい。憲法上の「通信」の概念及びその射程が明確でない限り，当該保護のあり方の帰結に関しても曖昧なままとなるおそれがあるからである。

社会通念上「通信」ないしコミュニケーションと捉え得る行為については，そこでやり取りされる情報の内容・種類や通信手段の技術にかかわらず，その通信当事者及び通信の仲立ちを行う者の関わりの観点から，以下の各種類に大別することが可能であろう。すなわち，情報の発信者をＡ，当該発信者が情報の宛先として予定する着信者をＢ（特定又は不特定の者），当該情報の伝送・交換等に従事する者をＸ（複数の異なる者がこれに該当し得る）とした場合，①ＡとＢとの間の情報のやり取りをＸが一定の通信設備を用いて取り次ぐ一般的な場合（以下，「設備使用他人間通信」という），②ＡとＢとの間の情報のやり取りをＸが通信設備を用いずに取り次ぐ場合（以下，「設備不使用通信」という）[8]，③前記①の場合の中でＡとＢとが同一人である場合（Ａが自分自身に宛ててＸを介して情報を発信する場合。以下，「設備使用自自通信」という），④前記①の場合の中でＡとＸ又はＢとＸが同一人である場合（発信者又は着信者が仲立ち役を兼ねる場合。以下，「設備使用自他通信」という），⑤ＡとＢとがＸを介さずに対面の会話等により直接情報をやり取りする場合（以下，「対面コミュニケーション」という）である。

これらのうち，憲法上の「通信」に該当するのはいずれであろうか。

憲法21条２項後段の規定は「通信」に関して特段の明示的な限定を行っていないことを踏まえると，これらの行為はすべて当該「通信」に含まれるようにもみえる。実際，憲法制定当時の当該規定の制定者意思に関する調査を踏まえ，対面コミュニケーションも含め，さまざまな「意思伝達」が「通信」に含まれるものと観念すべきであるという旨を示唆する考え方も提示されている[9]。しかしながら，憲法21条２項後段の規定は「秘密」を適切に保護することをその主旨とするものであることから，当該規定の名宛人との関係を踏まえて「秘密」の保護に対する必要性の乏しいと認められるコミュニケーションについては，ここでいう「通信」に含まれないと解される。

憲法21条２項後段の規定の名宛人には，公権力及び（設備使用他人間通信における前述のＸにほぼ相当する）通信管理主体が該当すると考えられる。通信管理主体とは，「他人の需要を充足するために，一定の通信設備を用いて他人間の通信の完結に向けて能動的に関与し，それに寄与する」形での通信役務の提供を行いつつ「秘密」たる情報を取り扱う者のことであり，その多くは私人（通信事業者等）である[10]。憲法規範の名宛人として当然に予定される公権力に加えて，私人たる通信管理主体も憲法21条２項後段の規定の名宛人となると解する主な理由については，以下の各点に集約される[11]。すなわち，①通信管理主体は「秘密」たる情報に最も手近かつ正当にアクセスし得る立場にあり，「通信」の利用者にとって公権力以上の「脅威」となり得る，②仮に通信管理主体が「秘密」の保護の義務を憲法上負わないのであれば，公権力が通信当事者の知り得ないところで当該主体（の任意の協力）を介して「秘密」たる情報の提供を受けることが可能となり得る，③仮に基本的な通信役務の提供主体である通信管理主体が憲法21条２項後段の規定に何ら拘束されず，かかる通信役務を適切に提供することさえも憲法の次元では制度的に確保されない（もっぱら立法政策のあり方に委ねられる）のであれば，憲法の予定する「通信」自体が安定的に成立しなくなるおそれが生じ，

その結果として個々の「秘密」が発現する余地も乏しくなり得る，④通信の秘密不可侵の法規範との関係において，仮に通信管理主体が一般私人とまったく同列の立場にあるとすれば，当該主体が支配・管理するネットワーク全体を一種の表現媒体とした表現の自由や当該ネットワークの運営等に対する財産権又は営業の自由の行使の余地が広範な局面において生じ，その中で個別の通信に対する差別や不適正な取扱い等が行われる場合も想定されることとなり，当該通信の利用者が通信役務の健全な利用を行ううえで，憲法の次元でこれに「対抗」することが困難となり得る[12]，といった点である。

このような公権力及び通信管理主体との関係において憲法上保護されるべき「秘密」とは，プライバシーそのものと完全に同視され得るものではない。なぜなら，「秘密」たる情報の中には，利用者のプライバシーとの関わりが深いものとそうではないものとが必然的に混在し，それらが包括的に保護の対象となり得ると考えられるからである[13]。「秘密」の保護法益とはむしろ，「通信」の利用者としての国民各人が，送受信の対象となる情報の伝送・交換等の過程及びその完了後において，当該情報及びそれに付随する情報の適正な取扱い又はそれらの情報へのアクセスのあり方（原則として不接触とすること）に対して有すると認められる（客観的な）「信頼」をその中核とするものであるように思われる[14]。すなわち，「秘密」とは，万人（一般私人）との関係において保護されることが予定されたものではなく，かかる「信頼」の向かい先となると認められる公権力及び通信管理主体との関係において保護されるものである（よって，憲法上，一般私人において「秘密」を侵すという事態は予定されていない）と考えられる。なお，相手方の通信当事者については，送受信の対象となる情報の内容を全面的に認識（場合によっては利用）することが予定されているのであるから，ここでいう「信頼」の向かい先ではなく，「秘密」を侵す主体とはなり得ないと考えられる。

このような「信頼」は，その狭義においては，送受信の対象となる情報及びそれに付随する情報を合理的な理由なく知得，漏えい等しないということ

に対するものであるが，より広義においては，個々の情報が流通する通信（ネットワーク）基盤，すなわち各種通信設備の利用に関する安全性等を含む「通信」の主要な制度的利用環境が適切に確保されることに対するものと捉えることが可能であろう。なぜなら，かかる制度的利用環境が健全なものではなく，国民各人が「通信」を安全に安心して利用できないような状況に恒常的におかれている場合には，「通信」そのものが成立する機会が少なくなり，本来憲法上保護されることが予定された「秘密」も発現する余地が乏しくなる可能性が高いからである[15]。したがって，憲法上の保護の客体となる「秘密」には，利用者たる国民各人が行う個々の通信に関する情報のみならず，それが流通する通信基盤（の健全性）という意味合いも含まれていると解される[16]。

以上のような解釈を前提とした場合，まず，対面コミュニケーションについては，通信管理主体が登場しないため，通信当事者であるＡとＢとの間で生じ得る秘匿事項等に関しては，ＡやＢ自身がそれを他者に開示しないよう取り計らえばよく，公権力との関係においてはこれをプライバシーの権利（憲法13条）等の保障の問題として扱われれば足りると考えられることから，憲法上その「秘密」をあえて別に保護する必要性が乏しいと言える[17]。また，設備不使用通信についても，究極的には情報がＡからＢに伝達されるものの，ＡはＸが当該通信の事実を知ることはもとより，その内容を関知するリスクも承知していると認められることに照らすと，これは「ＡとＸとの情報のやり取り」と「ＸとＢとの情報のやり取り」とが結合して成立する行為と観念することができる。よって，この場合のＸは，通信管理主体というよりも通信当事者の一人として位置づけられ得ることから，通信管理主体との関係において保護されるべき「秘密」が存在しない。同時に，公権力との関係において設備不使用通信を通じて生じ得る秘匿事項等に関しては，対面コミュニケーションの場合と同様に，プライバシーの権利等の問題として保護されれば足りると考えられる。したがって，対面コミュニケーション及び設備不使

用通信については，憲法上保護される「通信」には含まれないと解される。

これに対し，設備使用他人間通信はもとより，設備使用自自通信及び設備使用自他通信については，少なくとも公権力との関係において，憲法上その「秘密」が適切に保護されることが要請されると考えられる。なぜなら，公権力は通信傍受その他の手段により，通信当事者（の双方又は一方）の直接のコントロールの及ばない通信設備を介して，個々の通信に関する情報を取得する物理的な可能性を有しており，当該情報をみだりに探索されない状態が確保されることが，国民各人が安心して「通信」を利用するための必要条件となり得るからである。前述のとおり，通信設備を用いた通信が行われる場合において，仮にその「秘密」が公権力及び通信管理主体の双方との関係において憲法上保護されていなければ，通信の利用者にとっては，公権力が必要に応じて通信管理主体の助力を得つつ当人の知らないところで当該設備を介して「秘密」たる情報を探索する脅威に対するリスクを払拭し切れないということになろう[18]。もっとも，さしずめ公権力との関係については措き，もっぱら通信管理主体との関係に着目すると，設備使用自他通信については，通信の仲立ち役を果たすＸが通信当事者を兼ねることから，この場合のＸは通信管理主体とは言えず，そこに保護されるべき「秘密」は生じない。これに対し，設備使用他人間通信及び設備使用自自通信については，通信管理主体による「秘密」探索の脅威からの保護の必要性が認められる。よって，設備使用他人間通信，設備使用自自通信及び設備使用自他通信のうち，設備使用自他通信に関しては，もっぱら公権力との関係において「秘密」が保護される必要性があり，設備使用他人間通信及び設備使用自自通信に関しては，これに加えて通信管理主体との関係においても「秘密」が保護される必要性があるということになる。いずれにしても，これらの通信については，国民各人がそれを健全に利用するうえでの「秘密」の保護の必要性が認められることから，憲法上の「通信」に該当すると解される[19]。

このように考えると，さまざまなコミュニケーション行為の態様のうち，

憲法上の「通信」に該当するか否かを決する重要なメルクマールは，通信設備[20]の使用の有無にあるということになる。すなわち，発信者からの情報がネットワーク（伝送路設備）その他の主要な通信設備を介してその予定する宛先（着信者）に送り届けられることが，憲法上予定される「通信」の骨格であり，そこには当該通信設備を支配・管理する者が存在する。この者は，多くの場合において通信管理主体であるが，設備使用自他通信の場合のように通信当事者（の一方）であることもある。通信管理主体は，各通信当事者の視点からみれば「信頼」の向かい先となる第三者であるが，通信設備の支配・管理に対する権限に基づき，取り扱う個々の通信に関する各種の「秘密」たる情報を正当に知り得る立場におかれていると言える。

以上の解釈を踏まえつつ，次節においては，端末設備及び端末内包情報の法的位置づけないし保護のあり方をめぐる近年の米国の議論の具体的な内容について，概観することとする。もっとも，アメリカ合衆国憲法（米国憲法）には通信の秘密不可侵に相当する明文の規定が存在しないため，当該議論に関しては，これを我が国の憲法解釈論にそのまま援用することは難しい。しかし，①今日の社会において現に利用されている端末設備及び端末内包情報の内実に関しては，日米両国においてほぼ共通すること，②端末内包情報はそれが個々の通信に関する情報である限りにおいて，我が国では「通信の秘密」たる情報に該当すると解されることなどから，端末設備及び端末内包情報の法的位置づけないしそれらの保護のあり方の考察に際して，次節において叙述する米国の議論は貴重な示唆を与えてくれるものと思われる。

3　携帯電話端末及び携帯端末内包情報の捜索等をめぐる米国の議論

3.1　逮捕に伴う捜索等をめぐる従前の主な判例法理

米国の学説・判例において端末設備の位置づけに焦点が当たることとなったのが，米国憲法修正４条（以下，単に「修正４条」という）[21]に基づく公

権力による「捜索及び拘束・押収」（以下，「捜索等」という）の客体としての携帯電話端末及び当該端末を通じてアクセス可能な電子化（デジタル化）された情報（以下，「携帯端末内包情報」という）が米国憲法上どのように保護されるのかという問題である。これは，一次的には被疑者の「逮捕に伴う捜索（search incident to arrest)」のあり方をめぐる刑事手続上の問題であるものの，今日的な携帯電話端末を手がかりとして，端末設備が本質的に有する重要な特徴を浮き彫りにしたものとも言える。もっとも，この問題をめぐる議論を的確に理解するためには，修正４条との関係における「逮捕に伴う捜索」の合理性をめぐる判例法理の主な流れについて把握する必要があると考えられるため，まずはこの点について以下に概観することとする。

周知のとおり，修正４条は，「身体，住居，書類及び所持品について，不合理な捜索及び拘束・押収を受けることのない人民の権利は，侵されない。いかなる令状も，宣誓又は確約によって支持される相当な理由に基づき，かつ，捜索されるべき場所及び拘束・押収されるべき人又は物を特に表示するものでなければ，発せられてはならない（The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.)」と規定する。これは，公権力の捜索等における令状主義の原則に関する手続的保障を定めるのみならず，プライバシーの権利等の実体的権利を米国憲法上保障し，各人の「プライバシーの合理的な期待」を保護することをその主旨とするものとして解されてきた[22]。

判例において，修正４条に基づく個別の捜索等の合憲性は，究極的にはそれが「合理的」か「不合理」かにかかっているという旨が説かれている[23]。すなわち，問題となる捜索等が合理的であると認められるためには，原則として裁判所の令状に基づくことが必要となるもの[24]，令状なくして（無令

状で）行われる捜索等が常に不合理と認められるわけではなく，一定の「令状主義の例外」に該当する場合にはその合理性が認められ得るとされている[25]。このような観点から，1914年のウィークス（Weeks）事件判決[26]の傍論において，英米法における「令状主義の例外」としての「逮捕に伴う無令状での捜索」が確認されて以来[27]，当該捜索の具体的な射程に関して長年にわたる議論が行われてきた。

この点に関しては，1969年のチャイメル（Chimel）事件判決[28]が重要な一里塚となった。すなわち，この判決の中で，捜索従事者の安全（safety）の確保及び被疑者自身による証拠の隠滅（concealment）又は破棄（destruction）の防止の必要性が，逮捕された被疑者自身及びその直接の支配の及ぶ範囲内（within his immediate control）における無令状での捜索等を「合理的」なものとするという旨が説かれることとなった[29]。

次いで，1973年のロビンソン（Robinson）事件判決[30]においては，捜索等における「被疑者から凶器を取り上げる必要性（the need to disarm the suspect）」及び「被疑者に関する証拠を保全する必要性（the need to preserve evidence on his person）」を踏まえ，「勾留付き逮捕（lawful custodial arrest）」[31]の場合，これらの必要性が常に認められることから，それに伴い行われる被疑者の身辺の捜索等については，「令状主義の例外」に相当するのみならず，修正４条に基づき「合理的」であると認められるという旨が示された[32]。この判決は，合法な勾留付き逮捕に伴う捜索等の合理性は，後日裁判所によって（「逮捕」に関する「相当な理由」とは別に）「捜索従事者の安全の確保及び被疑者自身による証拠の隠滅又は破棄の防止の必要性」に関する「相当な理由」が認められるか否かの個別判断により左右されるものではないという前提によっていた[33]。その結果，被疑者による凶器の所持や証拠の隠滅の可能性が極めて低かったにもかかわらず，当該被疑者が着用する衣服のポケットに所持していた煙草の箱を逮捕に伴い無令状で開披する行為が「合理的」な捜索であると認められることとなった[34]。

さらに，2009年のガント（Gant）事件判決[35]においては，チャイメル事件判決において認められた逮捕に伴う無令状での捜索等の正当化の根拠について，当該捜索等の客体が被疑者の逮捕時における自動車内であるときに焦点が当てられ，「被逮捕者の身柄が確保されておらず，かつ当該被逮捕者が捜索時に乗客席部分（passenger compartment）に届く距離にいる場合」に限り，当該自動車内の捜索等は「合理的」なものとなるという旨が示された[36]。同時に，この判決は，逮捕事由となる犯罪に関する証拠が自動車内に発見されると信ずることが合理的である場合には，逮捕に伴う自動車内の捜索等が正当化され得るという旨も示唆しており，ここに，もっぱら証拠収集を目的とした逮捕に伴う無令状での捜索等の可能性[37]が一定の範囲で肯定されるという解釈が導かれることとなった[38]。

3.2　ライリー事件判決の概要

以上のような議論の流れを踏まえ，2014年に示されたライリー（Riley）事件判決[39]は，逮捕に伴う被疑者の携帯電話端末及び携帯端末内包情報の捜索等に対してそれまでの判例法理がどのように適用されるかということを正面から検討し，端末設備及び端末内包情報の法的位置づけないしそれらの保護のあり方に関して一定の示唆を与えるものとなった。そこで，本項の以下においては，この判決の法廷意見の要点を概観することとしたい。

まず，総論として，ロビンソン事件判決において確認された「合法な勾留付き逮捕に伴う捜索等の合理性」については，有体物を客体とする捜索等に関しては適切な利益衡量を図ったものと言えるが，（有体物ではない）携帯端末内包情報を客体とする捜索等に関してはその限りではないとされた。ロビンソン事件判決は，チャイメル事件判決で説かれた「捜索従事者の安全の確保及び被疑者自身による証拠の隠滅又は破棄の防止の必要性」という「二要件」が「合法な勾留付き逮捕に伴う捜索等」においては当然に認められるということを前提としているが，携帯端末内包情報の捜索等に対してこれら

の必要性はそのまま当てはまるものではないという[40]。また，ロビンソン事件判決は，逮捕の事実それ自体によって被疑者のプライバシーに対する利益が著しく縮減するという前提によっているが，携帯電話端末は被疑者に関する厖大な個人的情報を内包しているため，他の物品の捜索等の場合と同視可能となるものではないとされる。したがって，ロビンソン事件判決の考え方をそのまま携帯端末内包情報の捜索等に援用することはできず，当該捜索等のためには（たとえ逮捕に伴う場合であっても）基本的に事前に令状を取得する必要があるという[41]。

次に，逮捕に伴う無令状での捜索等の可能性との関係において，ロビンソン事件判決で当該捜索等に関する「相当な理由の有無に関する個別判断」のアプローチが否定されたことを踏まえ，携帯端末内包情報という特定の類型に対する捜索等に関して，チャイメル事件判決で提示された「捜索従事者の安全の確保及び被疑者自身による証拠の隠滅又は破棄の防止の必要性」という要素が妥当する余地があるか否かという点がより具体的に検討された。その中で，「捜索従事者の安全の確保」の必要性の観点からは，①たとえどんなに小型であっても捜索従事者を殺傷させたり被疑者の逃走を補助したりするための凶器となるリスクを抱えている一般的な物品とは異なり，携帯端末内包情報についてはそれ自体としてかかるリスクを内在させるものではないこと，②携帯端末内包情報の捜索等を通じて共謀者の動向を察知するなどの手法により捜索従事者の安全性が強固に確保され得るという旨の政府の主張に関しては，これが実際の経験に基づくものであるということに対する十分な証拠が示されていないことなどから，携帯端末内包情報に対する無令状での捜索等が正当化されるものではないとされた[42]。

一方，「被疑者自身による証拠の隠滅又は破棄の防止」の必要性の観点からも，以下の各理由により，同様に携帯端末内包情報に対する無令状での捜索等が正当化されるものではないとされた。すなわち，①捜索従事者がいったん携帯電話端末を押収すれば，被疑者自身が携帯端末内包情報の消去等に

よる証拠の隠滅等を図る余地はなくなること，②第三者によるネットワーク上の遠隔操作や（パスワード等による）情報の暗号化等を通じた携帯端末内包情報の消去，隠匿等により証拠の隠滅等が図られる可能性がなお残るとしても，それは逮捕時における被疑者自身による証拠の隠滅等のおそれとは異なるうえに，当該可能性が実際に広く顕現すると信ずるに足りる十分な理由は提示されていないこと，③たとえ前記②の可能性が顕現する状況であっても，ただちに無令状での捜索等が重要となるとは言いがたく，令状を取得したうえでの通常の捜索等でも足り得ること，④前記②の可能性については，携帯電話端末に関して，その電源を切ったり，それを電磁波から隔離させるための導体性の容器に入れたりすることにより，ネットワークに接続されない状態におくことを通じて，物理的にそれを解消することが可能であること[43]，などがその主な理由である[44]。

そのうえで，被疑者の「プライバシーの合理的な期待」の保護の観点から，捜索等の客体としての携帯電話端末がもたらし得るプライバシーの侵害に対する懸念は，煙草の箱や財布等とは比較にならないものであるとされた。すなわち，①携帯電話端末は一般に質的にも量的にも厖大な情報を内包しており，その情報の保管容量の大きさも手伝って，電話のみならず，カメラ，アルバム，日記帳，地図，テレビ等の多様な機能を提供していること（情報の厖大性），②携帯電話端末はそれが内包可能な情報の量の多さと多様さ（例えば，ウェブサイト閲覧履歴，位置情報，モバイルアプリケーションの利用履歴等）から，他の独立した記録媒体ではおよそ困難な「各人の私生活の再現」を可能とし得ること（情報の私生活再現可能性），③携帯端末内包情報については端末購入時点ないしそれ以前に遡っての追跡が可能であることから，携帯電話端末は各人が通常持ち歩かないほどの多くの過去の通信に関する記録を内包するものであること（情報の遡及可能性），④携帯電話端末はプライバシーとの関わりの深い機微な情報を内包するにもかかわらず，各人が一般に始終持参することにより，利用者の所在地につきまとう性質のもの

であること（情報の利用者随伴性）などを根拠として，携帯電話端末ないし携帯端末内包情報については被疑者において通常所持される他の物品とは区別されるものと位置づけられた[45]。これは，修正４条との関係において，逮捕に伴う携帯端末内包情報の捜索等とその他の物品（所持品）の捜索等を規範的に区別し，前者については令状主義の要請を踏まえた「プライバシーの合理的な期待」の保護がより強固に及ぶということを明確化したものとして捉えることが可能であろう。

加えて，携帯端末内包情報は，厳密には必ずしも携帯電話端末それ自体に保管されたもの（以下，「携帯端末保管情報」という）ではなく，インターネット経由のクラウドコンピューティングによりアクセスされる遠隔のサーバー等[46]に保管された情報（以下，「遠隔保管情報」という）である可能性もあるという事実[47]が，問題となるプライバシーの利益の射程を複雑化させているという。すなわち，逮捕に伴う無令状での捜索等が可能となる客体の範囲は遠隔保管情報にまでは及び得ないと考えられる中で（この点については政府自身が認めているという），捜索等の対象として，携帯端末保管情報と遠隔保管情報とを物理的に区別するための明確な解決策は示されていないとされる[48]。

これらを踏まえ，以上の議論は決して携帯端末内包情報が捜索等の対象となり得ないということを意味するものではなく，当該捜索等のためにはたとえ逮捕に伴う場合といえどもあらかじめ令状を取得することが必要になるという帰結を導くものとされる[49]。また，緊急事態等，無令状での捜索等を許容し得る格別の事由が認められる場合には，それに基づく携帯端末内包情報の捜索等が妨げられるものでもないという[50]。

3.3　ライリー事件判決の考え方に関する若干の考察

ライリー事件判決は，被疑者のプライバシーの保護の観点から，逮捕に伴う捜索等の客体としての携帯端末内包情報（携帯電話端末）と一般の物品と

の間に明確な分水嶺を設けるものであるが，これはいくつかの可能性と問題点とを抱えたものであると評することができよう。まず，可能性としては，携帯電話端末に限らず，電磁的な情報を保管するあらゆる媒体（設備）の内部に対する捜索等が「プライバシーの合理的な期待」に関する強固な保護を受ける可能性が示唆されたということである[51]。このことは，ライリー事件判決が携帯電話端末を「ミニコンピュータ」として位置づけつつ，例えば通信機能を伴わないデジタルカメラ等，通信設備以外の電磁的な情報の保管媒体（以下，「その他の電磁的情報保管媒体」という）との明確な区別を図っていないということ[52]からも裏づけられる[53]。それまでの米国の判例においては，無令状での被疑者の①採血・採尿・呼気検査[54]，②裸にしたうえでの所持品検査[55]，③ＤＮＡの採取・検査[56]に対してでさえ，修正４条に違反しないという旨が示唆されてきた中で，携帯端末内包情報という電磁的な情報が令状主義との関係において一種の「別格の扱い」を受けるということの先例としての意義は小さくない。ただし，「逮捕に伴う捜索等」との関係において，携帯電話端末（携帯端末内包情報）とその他の電磁的情報保管媒体（当該媒体の保管する情報）とを区別する可能性については，なお残されている（あらゆる電磁的情報保管媒体を一律に捉えることが妥当とは言えない可能性がある）ということに留意する必要があろう。

一方，問題点として，以下の各点を指摘することができる。第一に，ライリー事件判決は，①情報の厖大性，②情報の私生活再現可能性，③情報の遡及可能性，④情報の利用者随伴性を主な理由として，携帯端末内包情報の捜索等を他の物品の捜索等と区別しているが，他の物品の中にもこれらの要件を充足するものがあり得ると考えられる。例えば，厖大な個人的情報が経時的に書き込まれた手帳をその所持者が常時持参している場合，当該所持者のプライバシーを保護する観点からは，捜索等の客体としての当該手帳の情報と携帯端末内包情報とを規範的に区別することが極めて困難となろう。

第二に，すべての携帯電話端末（携帯端末内包情報）が前述の各特徴を充

足するとは限らないと考えられる。例えば，購入したばかりの新しい携帯電話端末に関しては，たとえ物理的な情報の保管容量が大きくても，その利用者の情報や通信履歴が実際にほとんど蓄積されていない可能性もあり，その場合には，プライバシーの保護の観点から他の物品と規範的に区別する意義が乏しくなろう。また，たとえ携帯端末内包情報の情報量が厖大であるとしても，利用者が自らのプライバシーに関わる重要な（秘匿性の高い）情報を保管せずに頻繁に削除（消去）していた場合には，大半がプライバシーとの関わりの薄い「どうでも良い情報」となる可能性もある。さらに，携帯電話端末の利用者の中には，それを必ずしも常時持ち歩かない者もいると考えられる。

これらの問題点を踏まえると，携帯端末内包情報の捜索等に関する他の物品の捜索等との規範的な区別については，①その必要性を否定するか，又は②その必要性を肯定しつつもライリー事件判決が示した理由（当該必要性を肯定するための必要条件にすぎないと考えられる）とは別の理由（当該必要性を肯定するための十分条件）を提示することが不可欠となると言えるように思われる。このうち，①の方向性については，携帯電話端末に各人のプライバシーに関する多数の情報が内包されていることが多い今日の実態にかんがみると，必ずしも正鵠を射たものとは言えないであろう。他方，②の方向性については，我が国における端末内包情報に関する「秘密」の保護に関する議論とも連動し，さらなる検討の余地があるように思われる（次節参照）。

第三に，ライリー事件判決自体が認めているとおり，捜索等の客体としての携帯端末内包情報に関して，端末それ自体に保管された携帯端末保管情報（ネットワークへの接続なくしてアクセス・捜索可能なもの）と通信管理主体等の支配・管理するサーバー等に保管されている遠隔保管情報（ネットワークへの接続を介してのみアクセス・捜索可能なもの）との明確な区別が事実上放棄されている[57]。もっとも，修正４条との関係において，携帯端末保管情報と遠隔保管情報とを規範的に区別する必要性が存するのか否かとい

うことについては別途の詳細な検討が必要となり得るし，ライリー事件判決ではこれが否定的に捉えられているように見受けられる[58]。しかし，チャイメル事件判決で示された「被疑者の直接の支配の及ぶ範囲」という基準に依拠する限りにおいては，当該範囲に携帯端末保管情報が入り，「直接の支配」が及ぶとは言いがたい遠隔保管情報についてはこれに含まれないものと捉えることが合理的であろう。このとき，携帯端末内包情報のうち，携帯端末保管情報に対する捜索等については，チャイメル事件判決の考え方による限り，なお「令状主義の例外」に該当する余地が残されているということになるように思われる。このことは，プライバシーの保護との関わりにおける携帯端末内包情報について，携帯端末保管情報と遠隔保管情報とを規範的に区別することが有意となる可能性があるということを示唆するものであると言えよう。

第四に，第三の点にも関連して，携帯端末内包情報はそもそも誰が支配・管理するものなのかという問題が正面から検討されることなく，もっぱら問題となる携帯電話端末の所有者ないし占有者が利用者たる被疑者であるということをもって，そのプライバシーの保護の要請と結びついた厳格な令状主義の適用という帰結が導かれている。仮にこの帰結自体が妥当であるとしても，それを導くまでの議論の道筋においては，無令状での捜索等が例外的に認められる可能性に関する検討の一環として，遠隔保管情報を含む携帯端末内包情報への公権力による任意のアクセスに同意（承諾）を与える権限は誰が有しているのか（特に遠隔保管情報については，「被疑者の直接の支配の及ぶ範囲」を超えると考えられるにもかかわらず，被疑者自身が当該権限を有していると観念し得るのか）という点が考慮される余地もあるように思われる。

以上の各問題点は，我が国において，憲法上の通信の秘密不可侵の法規範との関係における端末設備及び端末内包情報の法的保護のあり方を考察するに当たり，貴重な示唆を与えるものであると考えられる。そこで，この点に

ついて，次節においてさらなる検討を行うこととする。

4 端末設備及び端末内包情報の憲法上の保護のあり方に関する解釈論的考察

前節で概観した米国の議論及びその考察から示唆されるのは，①携帯電話端末その他の「通信設備としての端末設備」に関しては，個人のプライバシーに関わる厖大かつ多様な情報を内包し得るものであり，公権力による捜索等（アクセス）からの要保護性が概して高いということ，②しかしながら，内包される情報の多寡については，個々の端末設備の利用実態等に応じて異なるうえに，その他の電磁的情報保管媒体（の内包する情報量）との比較においてはますます相対的なものとなるから，内包される情報の量や幅（多様性）のみをもって当然に端末設備が「別格の扱い」となると断じることは困難であるということ，③プライバシーの保護という要素を含む「秘密」の保護の観点からは，端末内包情報のうち，端末設備それ自体に保管された情報（以下，「端末保管情報」という）とそれ以外の遠隔保管情報とを規範的に区別して捉えることが有意となる可能性があるということである。これらのうち，前記②の帰結の延長線上に見え隠れするのが，通信の秘密不可侵を明示しない米国憲法とは異なり，我が国の憲法の下では，端末設備が通信設備の一環であり，そこからの公権力による端末内包情報の取得（知得）が「秘密」の侵害となり得るという点に，当該情報に対する高次の要保護性，ひいては「端末設備の不可侵性」の根源が認められるという思想である。周知のとおり，我が国の刑事手続上も，逮捕のための被疑者の捜索（刑事訴訟法〔昭和23年法律131号〕220条１項１号）や逮捕の現場における証拠物の捜索等（同項２号）が令状なくして正当に行われ得ることとなっており（同条３項。併せて，憲法35条１項参照），これらは「令状主義の例外」として広く解されている[59]。しかし，「秘密」たる情報の保護との関係における「端末設備の

不可侵性」が妥当するのであれば，端末内包情報の無令状での捜索等については，たとえそれが「逮捕の現場」において行われるものであっても，憲法21条２項後段の規定との関係において，原則として許容されないということになり得ると考えられる。

このような観点から「通信設備としての端末設備」の特徴及びそれから導かれる帰結を考えると，以下の各点を指摘することができる。第一に，端末設備は，他の通信設備と同様に，その内部に個々の通信に関する情報を内包させることが機能的に予定されていることから，その内包する情報（端末内包情報）と不可分であるという特徴を有する。すなわち，端末設備を含む通信設備は，その内部における取扱いの対象となる情報の伝送，送受信，保管等のための設備であり，当該取扱いのために不可欠の要素となるものである。しかも，端末設備に関しては，端末保管情報に加えて，遠隔保管情報へのアクセスの「入口」にもなることから，その捜索等を通じて入手可能となる情報の範囲が極めて広い。したがって，端末設備その他の通信設備へのアクセスは，基本的にそれが内包する広範な情報（端末内包情報等）の取得をも同時に意味するものと捉えられる。実際，ライリー事件判決においても，「携帯電話端末の捜索（cell phone search）」[60]と「携帯端末内包情報の捜索（searches of data on cell phones）」[61]とが明確に区別されているわけではなく，むしろ一体的に捉えられているように見受けられるが，これは両者の不可分性を象徴するものであると言えよう。

なお，憲法35条１項の規定との関係からは，同条項にいう「住居，書類及び所持品」を厳格に有体物に限定して捉える伝統的な解釈[62]を採る場合には，有体物たる端末設備の捜索と無体物たる端末内包情報の捜索とを区別する意義が認められ得るかもしれない。しかしながら，①当該「住居，書類及び所持品」という文言が捜索等の対象を厳密に有体物に限定する趣旨であると解することの妥当性については疑問であること[63]，②端末内包情報の捜索は一般に（記録媒体としての）端末設備それ自体の点検を前提として行われるこ

と[64]，③仮に無体物としての端末内包情報の捜索に憲法35条１項が直接適用されなくとも，憲法13条，21条２項後段及び31条の各規定の要請にかんがみ，実質的には当該捜索に令状主義の要請が及び得ると解し得ること[65]などの理由から，令状主義の適用との関係に着目する限りにおいても，今日において両者の捜索を厳密に区別する実益は乏しいと思われる。

第二に，通信設備としての端末設備は，通信役務の提供・利用に際して機能することが予定されており，ネットワークとの接続を通じて当該機能が実質的に発揮される（例えば，携帯電話端末は一定の通信管理主体に割り当てられる所要の周波数等から遮断された場所では十分に機能しない）という特徴を有する。そのため，端末設備は一般にネットワークを介して提供される各種の役務が利用者において適切に利用可能となるように初期設計されることとなるが，当該役務自体の大半は基本的に通信管理主体が司るものであるから，その設計に際しては多かれ少なかれ個々の通信管理主体の意思が反映されることとなる。かかる意思には，通信役務の適切な提供を総合的に管理する観点から，通信管理主体において，個々の通信に関する一定の端末内包情報（特に端末保管情報）をネットワークに接続された端末設備から取得可能となるための仕様を組み込むことも含まれ得る。その結果，個々の利用者に加え，当該利用者の「信頼」の向かい先となる通信管理主体も，（端末設備のネットワークへの接続を介して）端末内包情報に一定の範囲でアクセスし得ることとなる。とりわけ，携帯電話端末その他の移動体通信端末においては，個々の通信管理主体ごとに通信役務の提供に際して用いられる技術的要素が異なる場合が少なくないため，端末設備の設計段階において通信管理主体の個別の意思が作用する度合いが概して強く，通信管理主体がアクセス可能な端末内包情報の範囲も比較的広くなる傾向がある[66]。それゆえ，通常，遠隔保管情報を中心として，少なくとも部分的には，通信管理主体が端末内包情報の内容の知得，窃用等はもとより，その加工，改変等を行うことも物理的に可能となっている。その限りにおいて，ネットワークの一部を構成す

る端末設備については，その設計段階から一定の範囲で，通信管理主体の支配・管理に服するという側面を有しており，当該設備と不可分の関係にある端末内包情報に対してもその支配・管理が（部分的に）及び得ると言える[67]。

米国連邦政府においても，かつては端末設備及び端末内包情報に対する通信管理主体の支配・管理の及ぶ余地は乏しいという認識が一般的であったが，携帯電話端末の高度化等が進んだ今日においては，かかる認識は「時代遅れ（out of date）」であるという旨が示唆されている[68]。その背景には，端末設備（特に携帯電話端末）に一定のソフトウェア等を（その初期設計の段階で）組み込むことにより，従前よりも広範な端末内包情報を通信管理主体が取得することが技術的に可能となっているという我が国にも共通する事情がある[69]。また，我が国の立法の次元においては，ネットワーク（電気通信回線設備）に接続される端末設備の利用について，法令上の一定の制約が設けられている。それゆえ，ネットワークに接続される端末設備については，当該ネットワークを設置する電気通信事業者（通信管理主体）の支配・管理に服するという要素を内包していると言える[70]。

一方，利用者（通信当事者）が利用する端末設備それ自体は，基本的に当該利用者の所有・占有下におかれており，通信管理主体が直接占有しているわけではないことが一般的である。それゆえ，ネットワークとの接続及びそれに基づく端末内包情報へのアクセスという観点を捨象しつつ，もっぱら一有体物として端末設備を捉える限りにおいては，それは基本的に利用者の支配・管理するところとなると言える。同時に，利用者が端末内包情報に対する暗号化等の技術的措置を独自に講じることにより，通信管理主体による端末内包情報へのアクセスを一定の範囲で事実上遮断・防止する余地もある。これらの意味において，端末設備及び端末内包情報は利用者の支配・管理下におかれるという側面も併有しており，端末設備の設計・仕様が技術的に許容する範囲内で，利用者においてはあらゆる端末内包情報にアクセスし，またその加工，改変等を行うことが一般的に可能である。したがって，「通信」

の利用者において直接利用される端末設備は，基本的にそれと不可分の端末内包情報とともに，通信管理主体による支配・管理とその許容（予定）する範囲内での利用者による支配・管理との複合的なコントロールの下におかれていると言えるように思われる。

このように考えると，公権力が端末内包情報に対して任意のアクセスを行うことは，単に端末設備の利用者のプライバシーを侵害する可能性があるということにとどまらず，当該利用者の「秘密」を侵害する可能性を有する行為であるという意味合い，さらには（一定の範囲で）通信管理主体の支配・管理下におかれている通信設備及びそれと不可分の情報に対する不当な探索を通じて，その支配・管理を妨害するおそれを内包した行為であるという意味合いをも有するものと言えよう。よって，端末設備及び端末内包情報に対する公権力による任意のアクセスは，伝送路設備及びその内部を流通する情報に対する不当な探索と同様に，利用者の「秘密」を侵害する可能性と，個々の通信管理主体の通信事業の運営等に関する営業の自由又は当該設備の支配・管理に対する財産権（以下，これらを総称して「通信管理権」という）を侵害する可能性との双方を秘めていると言える[71]。換言すれば，有体物としての端末設備に対する所有権又は占有権が個々の利用者に帰属するとしても，（当該設備及び）端末内包情報の支配・管理に対する（基本権としての）通信管理権については，当該情報にネットワークを介してアクセス可能となる範囲において，そのネットワークを支配・管理する通信管理主体が享有する（ただし，利用者自身においても端末内包情報を部分的に加工，改変等し得る）ことが原則となり，公権力による任意のアクセスは，利用者の「秘密」及び通信管理主体の通信管理権の双方の基本権に対する侵害となり得ると解される。実際，米国の判例法理に基づく限り，前述のとおり遠隔保管情報については「令状主義の例外」に該当する余地が乏しい（すなわち，強固に保護され得る）と考えられるところ，その重要な理由として，当該情報が通信当事者以外の第三者たる通信管理主体等の一次的な支配・管理下におかれて

いる（通信当事者の「直接の支配の及ぶ範囲」を超えている）ということが指摘できよう。利用者の「秘密」に加えて，通信管理主体の通信管理権をも憲法上保護する必要性は，我が国における端末設備及び端末内包情報に対する捜索等が，一般の物品に対する捜索等との比較において，特に厳格な令状主義の要請に服する（不当な捜索等による基本権の侵害の可能性から強固に保護され，たとえ逮捕に伴う捜索等であっても原則として無令状では許容されない）ものと捉える解釈の妥当性を裏づける大きな根拠となるように思われる。

もっとも，端末内包情報といえども，通信管理主体の支配・管理がまったく及ばないと認められる情報（もっぱら利用者のみがアクセス可能な情報）については，通信管理権の行使の対象となるものではない。それゆえ，かかる情報に対する正当手続きに基づく場合以外の公権力によるアクセスについては，「秘密」やプライバシーの侵害の可能性を含んでいるとしても，通信管理権の侵害には該当しないと解される。一般に，端末内包情報のうち，遠隔保管情報については，当該保管先のサーバー等が通信管理主体の支配・管理下にある限りにおいて，当該主体の支配・管理下に（も）あるものと認められる。これに対し，端末保管情報については，ネットワークの接続を通じても通信管理主体がアクセスできず，かつ当該主体がその伝送等の過程で知得する余地もないものも含まれ得るところ，そのような情報に対しては，通信管理主体の通信管理権が及ぶものではない（もっぱら利用者が自ら支配・管理するところに帰する）。しかし，通信管理主体がアクセスできない端末保管情報であっても，個々の通信に関する情報として，その内容を当該主体がその伝送等の過程で知得し得た場合には，当該情報は憲法上保護される「秘密」にはなり得ると考えられる。換言すれば，端末保管情報を通信管理権との関係から大別すると，少なくとも，①個々の通信に関する情報（「秘密」たる情報）であって通信管理主体がアクセス可能な状態におかれており，その取扱いに対する当該主体の通信管理権が及ぶと認められるもの，②個々

の通信に関する情報（「秘密」たる情報）であるものの通信管理主体がアクセスできない状態におかれており，その取扱いに対する当該主体の通信管理権がもはや直接及ぶものではないと認められるもの，③個々の通信に関する情報以外の情報であるものの通信管理主体がアクセス可能な状態におかれており，その取扱いに対する当該主体の（通信管理権相当の）一定のコントロールの余地が認められるもの，④個々の通信に関する情報以外の情報であって通信管理主体がアクセスできない状態におかれており，その取扱いに対する当該主体の通信管理権が何ら及ばないと認められるもの，といった各情報が混在している様相が浮き彫りになると言える。これらのうち，前記②及び④の情報については，通信管理主体の通信管理権が及ばないという意味において，当該主体の直接の支配・管理下にあるサーバー等に保管された「秘密」たる遠隔保管情報とは規範的に区別される。ここに，端末内包情報に関して，それに対する公権力の捜索等が通信管理権の侵害となり得るか否かの観点から，端末保管情報と遠隔保管情報（通信管理主体の支配・管理するサーバー等に保管されたものに限る）とを一応峻別して捉えることに対する一定の意義が認められると考えられる。ただし，遠隔保管情報には，通信管理主体以外の者（例えば，もっぱらセキュリティ対策を行う事業者，通信管理主体とならないモバイルアプリケーションの運営者等）が支配・管理する情報（すなわち，個々の通信に関する「秘密」たる情報ではなく，通信管理主体の通信管理権が及ばないもの）も含まれ得る。それゆえ，端末保管情報と遠隔保管情報との区別が，通信管理主体の通信管理権の及ぶ客体に関する区別や当該主体との関係において保護される「秘密」であるか否かの区別にそのまま対応するわけではないということに留意する必要があろう。

第三に，ネットワークに接続された端末設備は，個々の「通信」の完結に不可欠となる通信基盤の一端であるという特徴も有している。ここで，憲法21条２項後段の規定が通信基盤の健全性の確保を要請するものであるという既述の解釈に照らせば，当該規定の名宛人となる公権力及び通信管理主体に

おいては，日頃から「通信設備の適切な管理」及びその制度的確保に努めることが求められるものと解される[72]。端末設備を含む通信設備の物理的な損傷や重大な不具合等が恒常的に生ずることとなれば，「秘密」の保護が危うくなるのはもとより，「通信」それ自体も適切に成立し得なくなるからである。このことは，憲法21条２項後段の規定に基づき，通信の利用者の「秘密」を保護する観点から，端末設備を含む通信設備からの情報の漏えい等の最大限の防止（の確保）に対する責務（努力義務）が公権力及び通信管理主体に課されているということを含意する。すなわち，端末内包情報の適切な管理については，通信管理主体の享有する通信管理権の行使のあり方の問題となると同時に，当該主体が公権力とともに負う憲法上の責務ないし努力義務の内実としての側面を有していると言うことができよう。したがって，端末設備その他の通信設備及びその内包する情報の管理に対する主観的権利としての通信管理権を通信管理主体が自由に行使可能となる範囲については，憲法内在的に相当程度において縮減されているものと解され，その分，公権力による端末内包情報への任意のアクセスが実際に通信管理権の侵害と認められる余地については限定的となると考えられる。

もっとも，電気通信の領域において，「適切な管理」が求められる通信設備については，伝送・交換等に必要となる電気通信回線設備であって，着信者による受信後の情報を持続的に内包する利用者側の端末設備についてはこの限りではないという考え方もあるかもしれない。これは，「秘密」はその伝送・交換等に際して保護されるものであって，着信者による受信完了後については別であるという思想に接合する。しかしながら，「秘密」は個々の「通信」の完了（着信者による最終的な受信の完了）と同時に消滅するものではないと考えられる[73]。仮に「秘密」が「通信」の完了と同時に保護されなくなるのであれば，それに関する情報が伝送・交換等に際してのみ保護されることの意義（価値）が乏しくなるうえに，そもそも利用者における「秘密」の保護に対する（公権力及び通信管理主体への）「信頼」は，個々の

「通信」の完了後にも及んでいるものと認められるからである。したがって，憲法上「適切な管理」が求められる通信設備には，（通信管理主体による支配・管理が及ぶと認められる範囲内において）「通信」の完了後において保管される端末保管情報等を内包する端末設備についても含まれ得ると捉えることが妥当であろう。

このように考えると，「通信設備の適切な管理」及びその制度的確保を要請する憲法21条２項後段の規定との関係においては，公権力が正当手続きに基づく場合以外で端末内包情報にアクセスすることは，通信管理主体により任意に行われる範囲でのネットワークの管理等に対する脅威となり得るだけでなく，当該情報に関する利用者の「秘密」たる情報の保護に対する要請，さらにはその前提となる通信設備の適切な管理の確保に対する客観法的要請に正面から背馳し得ると言える。それゆえ，かかるアクセス（捜索等に至らないものに限る）については，たとえ通信管理主体の同意を得ていたとしても，「秘密」の保護に対して「信頼」を有していると認められる各通信当事者の有効な同意（任意の承諾）がない限り，基本的に禁止されるものと解される（なお，刑事手続上の問題として，通信当事者の同意が得られた場合において，端末設備及び端末内包情報を無令状で強制的に点検することが，米国で認められているようないわゆる「同意捜索」[74]に該当し，憲法35条１項との関係において許容され得るか否かということについては別途の検討を要するが，ここでは措く[75]）。すなわち，通信の秘密不可侵の要請は，公権力が「秘密」たる情報を内包する他人の通信設備（端末設備を含む）にみだりに接触しないということをも含意すると言える。このような解釈に基づけば，「通信設備としての端末設備及び個々の通信に関する端末内包情報への公権力による捜索等に対しては原則として令状の事前取得が必要となる」というライリー事件判決において示された考え方の基本的な方向性については，我が国においては（憲法35条１項の要請としてのみならず）憲法21条２項後段の規定の趣旨に照らして導かれ得るものと考えられる。そして，その延長線

上には，端末設備及び端末内包情報に対する捜索等については，たとえ逮捕に伴い行われる場合であっても，憲法21条２項後段の規定に照らし，原則として無令状では行い得ないという前述の帰結が導かれることとなる。

このような帰結をやや視点を変えて捉えると，「秘密」の保護に対する憲法上の要請は，通信管理主体と通信当事者との共同的な支配・管理下にあると認められる端末内包情報について，これを実質的に「通信当事者を主とする支配・管理下」にあるものに転換させるような法的効果をもたらすということになる。すなわち，一般にある設備に内包される情報に対する公権力による（捜索等に至らない）任意のアクセスについては，当該設備を支配・管理する者（以下，「設備管理者」という）の同意を得て正当に行われ得るところ[76]，「秘密」たる端末内包情報へのアクセスに関しては，設備管理者としての役割の一端を通信管理主体が担っているにもかかわらず，その同意のみでは不十分であって，一方の設備管理者でありかつ「秘密」の「当事者」となる通信当事者の有効な同意が不可欠になるものと考えられる[77]。このとき，通信当事者の有効な同意とは，発信者及び着信者双方により明示的かつ個別的に行われる同意である必要があると考えられる[78]。すべての通信当事者の同意が必要となるのは，仮に通信当事者の一方の同意のみにより他方の通信当事者にも関わる端末内包情報が公権力のアクセス（探索）対象となるのであれば，当該他方の通信当事者の「秘密」たる情報の取扱いに対する「信頼」に背馳するものと認められ，当該当事者が安心して「通信」を利用できなくなる原因となるという理由による。

米国の場合，修正４条との関係において，「利用者の『秘密』を包括的に保護する観点から公権力による端末内包情報へのアクセスが基本的に禁止される」といった帰結は導かれる余地がないが（それゆえ，ライリー事件判決の説示に見られるように，逮捕に伴う無令状での端末設備及び端末内包情報の捜索等が原則として禁止されると解するためには，利用者のプライバシーの保護の必要性の観点等を踏まえた別途の確固たる理由が必要となる），我

が国の法の下では，基本権としての「秘密」が憲法上保護されているがゆえに，個々の通信に関する端末内包情報（端末保管情報及び遠隔保管情報の双方が含まれ得る）への公権力による任意のアクセスの可能性に対しては，当該情報が実際に有するプライバシーとの関わりの程度にかかわらず，憲法上強固に防御されることとなっていると考えられる。

もっとも，前述のとおり，端末内包情報の中には，個々の通信とは無関係に端末設備に保管された「秘密」以外の情報もあり得る。そのような「秘密」以外の端末内包情報に対しては，憲法21条２項後段の規定に基づく保護がただちに及ぶものではないため，理論的には，公権力による正当手続きに基づく場合以外でのアクセスが許容される余地もまったくないわけではない。同時に，「秘密」たる端末内包情報の中にも，不特定多数の者に向けて公開されることが予定された情報（秘匿性やプライバシーの確保に対する期待可能性が認められない情報）が混在し得る。公権力がかかる情報にアクセスしてその内容を知得したとしても，必ずしも通信当事者の「信頼」に背馳することになるとは言えず，「秘密」の侵害が認められない可能性が高いと考えられる[79]。

しかしながら，一般に公権力が端末内包情報に対して任意のアクセスを行おうとする場合，個々の通信に関する「秘密」たる情報とそれ以外の情報，あるいは公開が予定された情報とそれ以外の情報を瞬時かつ適切に区別することは事実上困難である。そのような中で，仮に正当手続きに基づく場合以外での公権力による（「秘密」以外の情報の取得を目的とした）端末内包情報へのアクセスが一律に認められるとすると，「秘密」以外の情報と同時に「秘密」たる情報も併せて不当に取得される可能性，アクセスしても「秘密」の侵害とは認められない情報と同時にアクセス自体が「秘密」の侵害となり得る情報も併せて知得される可能性が否定できず，「秘密」の保護に対する重大な脅威となる。したがって，公権力による端末内包情報への任意のアクセスについては，憲法21条２項後段の規定に基づき，包括的に禁止されるこ

とを原則とするものと解することが妥当であろう[80]。

以上のように考えると，憲法規範としての通信の秘密不可侵の効果として，通信設備としての端末設備及び端末内包情報とその他の電磁的情報保管媒体及び当該媒体の保管する情報とは，それらの設備ないし媒体及びそこに内包される情報への公権力によるアクセス（からの法的保護）のあり方に関して，規範的に区別され得るものであると言える。すなわち，「通信設備としての端末設備」の適切な管理を前提とする「秘密」の保護の要請との関係から，公権力による端末内包情報への捜索等に至らない任意のアクセスについては，その管理者としての役割を有する通信管理主体の同意があっても（各通信当事者の有効な同意がない限り）基本的に禁止されるのに対し，その他の電磁的情報保管媒体に保管された情報へのアクセスについては必ずしもその限りではなく，当該媒体の管理者（設備管理者）の有効な同意がある場合には許容される余地があるということになると考えられる。

したがって，個々の端末設備にどの程度の量の情報が実際に保管されているか，またそれらが個人の私生活を再現し得るほどのものであるか否かといったことは，通信の秘密不可侵の法規範に基づく端末設備及び端末内包情報の保護のあり方とは直接関係するものではないと言えよう。すなわち，ライリー事件判決が示した（携帯）端末内包情報に関する情報の厖大性，私生活再現可能性，遡及可能性及び利用者随伴性といった要素の有無にかかわらず，我が国の憲法の下では，通信設備としての端末設備及びそれと不可分の端末内包情報が，公権力による任意のアクセス（ないし正当手続きに基づく場合以外のアクセス）の脅威から安定的に保護されることとなっていると考えられる。同時に，通信設備としての端末設備の具体的な種類（技術的な分類）についても，通信の秘密不可侵の法規範との関係においてはただちに問題となるものではないと思われる。よって，携帯電話端末のみならず，インターネット等に接続されたPC[81]をはじめとする他の端末設備についても，それが通信設備として機能している限りにおいて，その内包する「秘密」たる情

報とともに，同様の憲法上の保護を受けるものと解される。

5 結 論

通信の秘密不可侵に関する憲法規範は，利用者の「信頼」を土台とした「秘密」たる情報の発現の前提となる個々の「通信」（の制度的利用環境）それ自体を保護することを指向しつつ，端末設備を含む通信設備及びそれが内包する「秘密」たる情報の双方の適切な保護（適切な管理又は取扱い及びそれらの制度的確保）を公権力及び通信管理主体に対して要請するものであると解される。したがって，（通信の秘密不可侵に相当する憲法規範を有しない）米国の判例において示された端末内包情報に関する情報の厖大性，私生活再現可能性，遡及可能性及び利用者随伴性といった特徴の妥当性を考慮するまでもなく，個々の通信に関する「秘密」としての端末内包情報（端末保管情報及び遠隔保管情報）については，それを擁する端末設備の種類にかかわらず，伝送路設備等の他の通信設備の内部を流通等する情報とともに，公権力及び通信管理主体により適切に保護されることが憲法上予定されているものと考えられる。

また，やや重畳的になるが，冒頭に提示した３つの論点に対しては，以下のような解答が導かれることとなる。すなわち，①「通信設備としての端末設備」及びそれが内包する情報（端末内包情報）は，原則として通信管理主体及びその利用者（通信当事者）による共同的な支配・管理下におかれる（ただし，通信当事者による支配・管理については，法令上の制約の範囲内で，かつ端末設備の設計・仕様に反映された通信管理主体の意思が許容ないし予定する範囲内にとどまる），②端末内包情報については，それが個々の通信に関する情報であると認められる限り，憲法上「秘密」として保護され（当該保護の主体は公権力及び通信管理主体である），その保護は個々の通信の完了後においても及ぶ，③かかる端末内包情報に対する公権力による捜

索等に至らない任意のアクセスが正当化されるためには，通信管理主体の同意のみでは不十分であり，基本的に各通信当事者の有効な同意が不可欠となる。

このような捉え方の帰結として，公権力において端末設備を含む通信設備全般及びそれが内包する「秘密」たる情報に対する任意のアクセスを行おうとする場合には，（プライバシーの権利の保障の問題のみにとどまらず）基本権としての「秘密」に対する侵害の可能性を伴うことから，それが伝送・交換中の情報であるか否かにかかわらず，基本的に憲法の予定する正当な手続き又は各通信当事者の有効な同意に基づくことが必要となるものと考えられる。同時に，かかるアクセスについては，通信管理主体による通信設備の管理等に関する通信管理権に対する制約にもなり得るが，通信管理主体自身が憲法21条２項後段の規定に拘束される結果，当該管理については利用者の「秘密」の保護の観点から適切に行われることが憲法上要請されるため，通信管理権の行使可能範囲自体が限定的であり，その分公権力による通信管理権の侵害が実際に認められる余地は必ずしも大きくないであろう。しかし，「秘密」の侵害の可能性に加えて通信管理権に対する侵害の可能性（又は通信設備の適切な管理の確保に関する客観法的要請に背反する可能性）をはらむということは，端末設備その他の通信設備及び当該設備が内包する情報へのアクセスを伴う公権力による捜索等については，憲法上，厳格な令状主義の要請に服するということの証左となると考えられる。他方，その他の電磁的情報保管媒体及びそれが保管する情報に対する公権力による任意のアクセスについては，憲法21条２項後段の規定に基づく要請が同様に及ぶものではない（しかも，通信管理権の保障等の問題が生じない）ことから，当該媒体の管理者の同意をもって実施し得る余地がある（もっとも，憲法13条の保障するプライバシーの権利との関係についてはなお問題となり得る一方，仮に当該アクセスが刑事手続上の捜索等の強制処分として行われる場合には，憲法35条１項の要請する令状主義との関係等が問題となり得る）と考えられる。

以上のような解釈を踏まえれば，通信の秘密不可侵の法規範は，憲法の次元において，通信設備の適切な管理の制度的な確保を要請しつつ，それに対して公権力がみだりに任意のアクセスを行う可能性から国民各人を防御する観点から，端末設備を含む通信設備をその他の電磁的情報保管媒体と規範的に区別する（通信設備に対する保護の度合いを相対的に強化する）ための役割を果たすという側面を有していると言えよう。近年の「物のインターネット（Internet of things）」や人体に装着可能なウェアラブル端末等の発展により，端末設備それ自体が著しく多様化・高度化していく中で，個々の「通信」を支える通信の秘密不可侵の法規範に基づく当該設備及びそれが内包する情報の（憲法上の）保護の必要性は，今日においてますます高まっているように思われる。

注

1　その法律上の定義につき，電気通信事業法（昭和59年法律86号）９条１項参照。電気通信回線設備とは，「送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備」のことである。

2　端末設備については，電気通信事業法52条１項において，「電気通信回線設備の一端に接続される電気通信設備であつて，一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む。）又は同一の建物内であるもの」と定義されており，本稿でも基本的にこの定義に依拠することとする。具体的には，端末設備等規則（昭和60年郵政省令31号）２条２項にいう「アナログ電話端末」，「移動電話端末」，「インターネットプロトコル電話端末」，「インターネットプロトコル移動電話端末」，「無線呼出端末」，「総合デジタル通信端末」，「専用通信回線設備等端末」のすべてが含まれる。

3　多賀谷一照ほか『電気通信事業法逐条解説』（電気通信振興会，2008年）27頁。

4　多賀谷ほか・前掲（注３）27頁。

5　本稿にいう「任意のアクセス」とは，特段の断りのない限り，刑事手続上の強制処分として行われる捜索等に至らないもの（典型的には，もっぱら行政調査等の一環として行われるもの）又は捜索等に該当しつつも憲法の予定する令状等に基づく正当な手続きによらずに行われるものを指す。

6　本稿にいう「秘匿性」とは，情報の当事者において，それを無関係の他人に知られないようにすることに対して認められる期待可能性の度合いのことを指す。

7　このような考え方に立つ代表的な学説として，芦部信喜『憲法学Ⅲ 人権各論(1)〔増補版〕』（有斐閣，2000年）542-543頁，佐藤幸治「通信の秘密」，芦部信喜編『憲法Ⅱ 人権(1)』635-669頁（有斐閣，1978年）635頁参照。

8　例えば，AがBを宛先として作成した封かん済みの書状を一般私人たるXに手渡しした後，Xがそれを直接Bに手渡しする場合がこれに該当する。

9　高橋郁夫＝吉田一雄「『通信の秘密』の数奇な運命（憲法）」，情報ネットワーク法学会編『情報ネットワーク・ローレビュー５巻』44-70頁（商事法務，2006年）67-69頁参照。

10　通信管理主体の概念の詳細について，海野敦史『「通信の秘密不可侵」の法理：ネットワーク社会における法解釈と実践』（勁草書房，2015年）３-４頁・153-179頁参照。

11　海野敦史「多様なインターネット上の役務提供者の通信管理主体性－米国における電子通信役務提供者と遠隔情報処理役務提供者との区別をめぐる議論を手がかりとして－」，『InfoCom REVIEW 66号』42-66頁（情報通信総合研究所，2016年）43頁参照。

12　法律の次元においては，電気通信事業法（昭和59年法律86号）６条が「不当な差別的取扱い」を禁止していることや，郵便法（昭和22年法律165号）５条が「差別されることがない」ことを確保していることなどが，通信管理主体による個々の通信の不適正な取扱い等に対する一定の予防措置として機能し得るであろう。これらの通信管理主体に対する行為規範となる立法が憲法上「公共の福祉」（憲法13条）の確保の必要性に基づき正当化されると解し得るとしても，通信管理主体に対して法律上禁止される「不当な差別的取扱い」や「差別」の具体的な内実・射程については一義的に明らかなものではない。したがって，仮に通信管理主体が憲法規範に何ら拘束されないと解するのであれば，各通信管理主体による個々の通信の取扱いのあり方が問題となる場合において，その合法性（前述の法律上の各規定との関係）が改めて個別に問われ得るということになる。このとき，「通信管理主体の表現の自由や財産権等」の行使の余地を十分に踏まえた形で，法律上禁止される行為の範囲を限定的に画さざるを得なくなる可能性が生じ得るであろう。

13　「このような『混在』にかかわらず，『秘密』の保護とはやはりプライバシーの保護であって，プライバシーとの関わりが乏しいものについては付随的ないし反射的に保護されるにすぎない」という考え方もあるかもしれない。確かに，「秘密」の保護の一要素として，利用者のプライバシーの保護が含まれるということは否定しがたい。しかし，仮に「秘密」をプライバシーと同視する考え方を前提とする場合，①「秘密」とは言いがたいはずのプライバシーとの関わりの乏しい情報が，なぜ「秘密」を保護の客体として明示している憲法に基づき付随的に保護されなければならないのか，②憲法13条がプラ

イバシーの権利を保障していると一般に解されている中で，なぜ憲法21条２項後段が「通信におけるプライバシー」の保護のみを改めて要請する必要があるのか（この点については注17も参照），③「通信におけるプライバシー」の保護の要請は「通信におけるネットワークのセキュリティ」の確保等の他の法益と緊張関係に立つことがあり得る中で，憲法21条２項後段はなぜプライバシーのみを明示的・優先的に保護することとしたのか，ということについて十分な説明を行うことが困難となろう。これらについては，憲法上保護される「秘密」にはプライバシーを超えた法益も含まれるものと解することにより，適切に説明することが可能となるように思われる。

14　海野・前掲（注10）128-133頁参照。

15　もっとも，憲法21条２項後段については，個々の「通信」が事実上成立し，その「秘密」が発現した場合にのみ，それが保護されることを予定した規定であると解する余地がないわけではない。しかし，少なくとも今日の社会においては，「通信」それ自体が「個人の尊厳」を支える重要な基盤となっており（海野・前掲〔注10〕10-11頁参照），かかる「尊厳」の確保のために，国民各人が「秘密」の保護を前提としつつ安全に安心して「通信」を利用できるような制度的利用環境が必要となっていると考えられること，また「通信」は本質的に個々の通信（ないしネットワークの相互接続）が多く行われれば行われるほどその効用が高まるという効果を有していることなどにかんがみると，憲法21条２項後段の規定は個々の「秘密」たる情報の保護を公権力及び通信管理主体に要請しつつ，「通信」（の制度的利用環境）そのものをも包括的に保護しようとしたものであると捉えることが合理的であるように思われる。したがって，憲法21条２項後段の規定の下では，個々の「通信」が成立した場合の「秘密」たる情報の保護のみならず，「通信」（の成立）それ自体の保護（そのために公権力及び通信管理主体において一定の作為が要請され得る）についても予定されているものと解される。

16　それゆえ，「秘密」の保護について，「私人の所持に属する文書と同様の保護を与えようとするもの」（法学協会『註解日本国憲法 上巻』〔有斐閣，1953年〕427頁，佐藤功『日本国憲法概説〈全訂第５版〉』〔学陽書房，1996年〕226頁参照）と位置づけることは，（利用者の所持に属する範囲を超えた）通信基盤の保護という意味合いが考慮されていないという点において，必ずしも正鵠を射たものとは言えないように思われる。

17　もっとも，憲法13条に基づくプライバシーの権利の保障と憲法21条２項後段に基づく通信の秘密の保護とを「一般法と特別法との関係に立つ」ものと解する場合には（井上正仁『捜査手段としての通信・会話の傍受』〔有斐閣，1997年〕12頁参照。併せて，佐藤・前掲〔注７〕636頁参照），たとえ対面コミュニケーションのプライバシーが憲法13条に

より保護されるとしても，それと重畳的に憲法21条２項後段がこれを保護するものという帰結が導かれるかもしれない。しかしながら，もっぱら対面コミュニケーション（その他の通信設備を用いないコミュニケーション）を念頭におく限り，なぜかかるコミュニケーションに関するプライバシーのみが憲法規範の中であえて重畳的・明示的に保護されなければならないのかを的確に説明することは困難となると思われる（双方又は一方の通信当事者以外の者が通信設備を用いて関与する「通信」を念頭において初めて，プライバシーの権利の保障とは別に「秘密」が憲法上明示的に保護される意義が説明可能となると考えられる）。

18　これに加え，一定の通信設備が「通信」に不可欠となる以上，当該設備を支配・管理する通信管理主体との関係において「秘密」が憲法上保護されないのであれば，通信設備それ自体の設計・構造上又は運用上の不具合等により意図せずに「秘密」たる情報が外部に漏えいするリスクとも利用者は裏腹になることとなる。

19　厳密には，これらの場合のほか，極めてまれなケースながら，⑥設備使用自自通信においてＸがＡと同一人である場合（Ａが自分自身に宛てて自ら支配・管理する通信設備を用いて情報を発信する場合。以下，「設備使用独力完結通信」という），⑦設備使用自他通信において用いられる通信設備がＡ及びＢ双方の支配・管理下にある場合（以下，「設備共用自他通信」という）も理論的には考えられる。設備使用独力完結通信については，使用される通信設備及びその内部を流通する情報がＡの同意（関与）なしには公権力がアクセスできない状態におかれている限り，公権力によりＡの意に反して通信設備を介しつつ当該情報が取得される可能性が想定されないことから，対面コミュニケーションや設備不使用通信の場合とほぼ同様に解することが可能であり，（通信設備が使用されるにもかかわらず例外的に）憲法上の「通信」に該当しないと解される。一方，設備共用自他通信については，公権力がＡの知らないところでＢの助力を得て通信設備を介して（通信傍受等により）Ａの発する情報を取得する可能性が残されており，公権力によるＡの「秘密」の侵害が想定され得ることから，憲法上の「通信」に該当すると解される。

20　ただし，ここでいう通信設備は，通信当事者の双方又は一方による支配・管理の及ばない伝送路設備等の通信設備である。

21　U.S. CONST. amend. IV.

22　Katz v. United States, 389 U.S. 347, 360-361 (1967) (Harlan, J. concurring in the judgement).

23　*See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

24 *See* Vernonia School District 47J v. Acton, 515 U.S. 646, 653 (1995).

25 *See* Kentucky v. King, 563 U.S. 452, 459-460 (2011).

26 Weeks v. United States, 232 U.S. 383 (1914).

27 *See id*. at 392.

28 Chimel v. California, 395 U.S. 752 (1969).

29 *See id*. at 763.

30 United States v. Robinson, 414 U.S. 218 (1973).

31 チャイメル事件判決においては「勾留付き逮捕」という表現は明示的に用いられていなかったが，1981年のベルトン（Belton）事件判決（New York v. Belton, 453 U.S. 454 [1981]）において，チャイメル事件判決は合法な「勾留付き逮捕」に際しての捜索を想定したものであるという旨が明確化されている。*See Belton*, 453 U.S. at 457. また，「勾留付き逮捕」に伴う捜索が合法的に行われるに際しては，逮捕に関する「相当な理由」が存在する限り，必ずしも警察関係の法規律において被疑者を勾留することが義務づけられていることを要しないという旨が（別の判例において）説かれている。*See* Gustafson v. Florida, 414 U.S. 260, 265 (1973). なお，「勾留付き逮捕」以外の逮捕関連の概念としては，「職務質問のための拘束（investigative detention）」としてのいわゆる「非勾留付き逮捕（non-custodial arrest）」や，一般私人の面前で重大な犯罪が行われた場合における「私人による逮捕（citizen's arrest）」が挙げられる。「非勾留付き逮捕」においては，捜索従事者の安全や証拠を確保する観点からの簡単な捜検（ボディチェック）を行うことが許容され得るが，「私人による逮捕」においては，目につく場所に凶器を所持しているなどの事情が認められない限り，原則としてそれに付随する捜索は許容されていない。ただし，一部の州法においては，商人が窃盗犯を逮捕する場合の「私人による逮捕」に伴う窃盗品の回収のための限定的な捜索が例外的に認められている。*See* California Penal Code § 490.5 (f)(4) (2015); Montana Code Annotated § 46-6-506 (2015).

32 *See Robinson*, 414 U.S. at 234-235. このような説示の背景には，1968年のテリー事件判決（Terry v. Ohio, 392 U.S. 1 [1968]）において，「相当な理由」を欠いても「合理的な嫌疑（reasonable suspicion）」がある場合には，警察官は相手を強制的に停止させ，職務質問することができ，その際，相手が凶器を所持し危害を及ぼすおそれがあると合理的に信じ得る場合には，凶器の捜検を行うことができるという旨が示されたことがある。*See Terry*, 392 U.S. at 24. ロビンソン事件判決は，「合法な勾留付き逮捕」の場合について，これがテリー事件判決における停止・職務質問・捜検の場合とは異なるということ

を踏まえつつ，「合理的な嫌疑」の有無にかかわらず，無条件的に無令状での被疑者の身辺の捜索を認めることとしたものと言える。テリー事件判決とロビンソン事件判決との関係の詳細につき，緑大輔「合衆国での逮捕に伴う無令状捜索：チャイメル判決以降」，『一橋論叢 128巻１号』75-93頁（一橋大学一橋学会一橋論叢編集所，2002年）77-78頁参照。

33 *See Robinson*, 414 U.S. at 235. *See also Gustafson*, 414 U.S. at 265-266. 換言すれば，合法な勾留付き逮捕に関する「相当な理由」が存在する限り，当該逮捕に伴う捜索に関する「相当な理由」も存在するということが前提とされていることになる。

34 *See Robinson*, 414 U.S. at 236. なお，ロビンソン事件判決においては，合法な勾留付き逮捕に伴う捜索等の客体の射程について，被逮捕者の身体からどこまでの範囲がこれに含まれるのかということが明らかにされていない。しかし，その後の判例においては，当該捜索等の射程については，被逮捕者自身に直接関連する（immediately associated with the person of the arrestee）私有物に限定されるという旨が示唆されている。*See* United States v. Chadwick, 433 U.S. 1, 15 (1977).

35 Arizona v. Gant, 556 U.S. 332 (2009).

36 *See id*. at 343. なお，自動車内の捜索等のあり方に関しては，前述のベルトン事件判決（注31参照）がその嚆矢となっている。当該判決においては，捜索従事者の安全の確保及び被疑者自身による証拠の隠滅又は破棄の防止の必要性が乏しかったにもかかわらず，逮捕に伴う自動車内の（無令状での）捜索等が合理的であると認められるという旨が説かれていた。また，捜索従事者は「逮捕と同時的な事象（contemporaneous incident）」として乗客席部分及び当該部分にある容器（container）を捜索することが可能であるとされた。ここでいう「容器」については，「他の物体を内包するあらゆる物体（any object capable of holding another object）」と定義されている。*See Belton*, 453 U.S. at 460-461. ガント事件判決は，自動車内の広範な捜索等を許容し得るベルトン事件判決の考え方を事実上否定し，被逮捕者の身柄が確保され，捜索従事者に対する安全上又は証拠保全上の危険が及ばないと認められる場合には，無令状での自動車内の捜索等は認められないという旨を示唆したものであると言える。

37 この証拠収集の必要性については，チャイメル事件判決において示された無令状での捜索等を可能とする要件とは別次元のものであり，携帯電話端末の捜索等のあり方をめぐる議論の争点の一つを構成することとなった（注44参照）。

38 *See Gant*, 556 U.S. at 343.

39 Riley v. California, 134 S. Ct. 2473 (2014).

40 ライリー事件判決は，無令状での捜索を認めるための一般的な判断基準として，「捜索が各人のプライバシーを制約する度合い」及び「捜索が合法的（legitimate）な政府（公共）の利益を促進するために必要となる度合い」の双方を評価（利益衡量）するという手法を示している。*See id*. at 2484. これは，携帯電話端末以外の物品の捜索においても，当該利益衡量において当事者のプライバシーを制約する度合いが過度に高いと認められる場合（ライリー事件判決が例示しているのは，被逮捕者の住居内全体の網羅的な捜索の場合。*See id*. at 2488）には，無令状での実施が認められないということを示唆するものであると言えよう。

41 *See id*. at 2484-2485. なお，フロリダ州最高裁判所の判例においても，捜索従事者が被疑者の携帯電話端末をその支配・管理下においた場合には，チャイメル事件判決において示された「二要件」が妥当しないことから，逮捕に伴う携帯電話端末の捜索等に関しては令状の取得を要するという旨が説かれている。*See* Smallwood v. State of Florida, 113 So. 3d 724, 736 (Fla. 2013).

42 *See Riley*, 134 S. Ct. at 2485-2486.

43 これらの理由に加えて，個別の事案において無令状での捜索等が不可欠となると認められる場合には，判例上確立されてきた「緊急事態（exigencies of the situation）における令状主義の例外」（*See King*, 563 U.S. at 460）によることが可能であるということも指摘されている。*See Riley*, 134 S. Ct. at 2487-2488.

44 *See Riley*, 134 S. Ct. at 2486-2487. これに加え，ガント事件判決で示された証拠収集のための逮捕に伴う無令状での捜索等の可能性については，チャイメル事件判決の考え方に基づくものではなく，その射程はもっぱら自動車内の捜索等に限定されるという旨が説かれている。*See id*. at 2484. その根拠として，自動車の場合における「縮減されたプライバシーの期待（reduced expectation of privacy）」及び「高度の法執行のニーズ（heightened law enforcement needs）」という「固有の事情（unique circumstances）」が指摘されている。*See id*. at 2492. このように，ライリー事件判決は，自動車内の捜索等を「特別視」することとする説示を通じて，証拠収集を目的とした無令状での携帯端末内包情報の捜索等の可能性を基本的に否定したものと解される。*See* Leslie A. Shoebotham, *The Strife of Riley: The Search-Incident Consequences of Making an Easy Case Simple*, 75 LA. L. REV. 29, 40 (2014). なお，学説においては，ライリー事件判決の「携帯端末内包情報の捜索等には原則として令状が必要である」という帰結を導くに当たっては，ガント事件判決で示された証拠収集のための逮捕に伴う無令状での捜索等の射程を自動車内に限定して解する必要性はなかったという旨を説くものもある。これによれば，

このような限定は，（特にチャイメル事件判決以前において）証拠収集のための逮捕に伴う無令状での捜索等が広く正当化されていた歴史的事実を無視するものであると同時に，チャイメル事件判決で示された「被疑者の直接の支配の及ぶ範囲内」という無令状での捜索等の条件と抵触する可能性を秘めたものでもあり，逮捕に伴う捜索等に関する判例法理の再構成に結びつく契機となるとされる。*See id.* at 34-35, 69-70.

45　*See Riley*, 134 S. Ct. at 2489-2490.

46　このような遠隔のサーバー等についても，ネットワークで接続されている限り，端末設備の一種である。それが各利用者の端末設備と一体的に用いられ，認知すべき事項が存在する蓋然性も共通して認められる限り，当該設備に関する端末内包情報を保管するために使用されるものとして位置づけることが可能であろう。なお，刑事訴訟法（昭和23年法律131号）においても，差押えの対象がPCや携帯電話端末等を含む「電子計算機」である場合，それを用いて作成等された電磁的記録を「保管するために使用されていると認めるに足りる状況にある」（遠隔の）記録媒体について，これがネットワーク（電気通信回線）で当該電子計算機と接続されている限り，その差押え（遠隔アクセス）の対象となるという旨が規定されているが（同法99条２項・218条２項），これは端末設備と遠隔保管情報（端末内包情報）を保管するサーバー等との一体性を前提とした考え方であると言える。すなわち，刑事訴訟法99条２項・218条２項の規定に基づく処分に関しては，端末設備たる電子計算機及びそれとネットワークで接続された遠隔のサーバー等の双方を同時にその対象として行われ得るものと解される。

47　この事実を踏まえ，ライリー事件判決においては，携帯電話端末が前述のベルトン事件判決で定義された「容器」（注36参照）に該当する可能性について，否定的に解されている。*See Riley*, 134 S. Ct. at 2491. なお，オハイオ州最高裁判所の判例においても，携帯電話端末は有体物を内包するものではないという理由から，その「容器」への該当性が否定されている。*See* State of Ohio v. Smith, 124 Ohio St. 3d 163, 167-168 (Ohio 2009).

48　*See Riley*, 134 S. Ct. at 2491. なお，ライリー事件判決は，逮捕に伴う無令状での遠隔保管情報の捜索について，「法執行機関が被疑者のポケットからその住居の鍵を見つけ，それをもって当該住居に侵入し，その捜索を行うことが許容されると主張するようなもの」と説いている。

49　ある学説は，ライリー事件判決について，令状主義の厳格な適用に関して携帯電話端末を「住居」と同視するものである（*See Riley*, 134 S. Ct. at 2491）ということを前提としたうえで，今後，生体認証の技術の発展等に伴い携帯端末内包情報へのアクセスに対する「自衛措置」が普及し，携帯電話端末の捜索等に対する令状主義の要請の必要性が

相対的に低下することとなれば，その影響は「住居」の捜索等のあり方にも波及し得るという旨を説いている。*See* George M. Dery III and Kevin Meehan, *A New Digital Divide? Considering the Implications of Riley v. California's Warrant Mandate for Cell Phone Searches*, 18 U. PA. J.L. & SOC. CHANGE 311, 331 (2015).

50 *See Riley*, 134 S. Ct. at 2493-2494.

51 この点を指摘する学説として，以下を参照：Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After Riley v. California*, 10 DUKE J. CONST. LAW & PUB. POL'Y 83, 94 (2014); H. Rick Yelton, *Riley v. California: Setting the Stage for the Future of Privacy by Distingishing between Digital and Physical Data*, 60 LOY. L. REV. 997, 1031 (2014).

52 *See Riley*, 134 S. Ct. at 2489.

53 もっとも，（ライリー事件判決後の）下級審の判例においては，被告人の住居内で発見されたデジタルカメラに対する捜索が，当該住居の捜索を許容する令状に基づいて行われ得るという旨を示唆したものがある（その前提として，携帯電話端末との比較におけるデジタルカメラの情報量の少なさが考慮されている）。*See* United States v. Miller, No. 13-20929, 2014 WL 3671062, at 2-3 (E.D. Mich. 2014).

54 Skinner v. Railway Labor Executives' Association, 489 U.S. 602, 628 (1988).

55 Florence v. Board of Chosen Freeholders of the County of Burlington, 132 S. Ct. 1510, 1523 (2012).

56 Maryland v. King, 133 S. Ct. 1958, 1980 (2013).

57 この点に関し，ある学説は，携帯電話端末が情報を保管する「収納庫（house）」としてだけではなく，（クラウドコンピューティングを用いて）情報にアクセスするための「鍵（key）」としても機能している中で，捜索等を行う公権力も利用者自身も端末保管情報と遠隔保管情報との明確な区別ができずにいると評している。*See* Dery III and Meehan, *supra* note 49, at 331。

58 ライリー事件判決は，端末保管情報と遠隔保管情報との間の区別について，基本的に「さほど重要ではない（makes little difference）」という旨を示唆している。*See Riley*, 134 S. Ct. at 2491. このような説示に照らし，当該判決は携帯電話端末の利用者が端末保管情報に対しても遠隔保管情報に対しても同程度のプライバシーの期待を有しているものと解していると説く学説もある。*See* Yelton, *supra* note 51, at 1031. 他方，一部の学説においては，第三者の支配・管理下におかれる遠隔保管情報に対して「プライバシーの合理的な期待」の強固な保護を認めることは，修正４条に関する判例法理として確立

されてきた「第三者法理（third-party doctrine）」（第三者に任意に提示された情報に対して各人は「プライバシーの合理的な期待」を有するものとは認められないと解する考え方）に抵触する可能性があるという旨が説かれている。*See* Dery III and Meehan, *supra* note 49, at 332. ここでいう第三者法理の詳細については，海野敦史「携帯電話の位置情報の法的取扱いをめぐる近年の米国の議論」，『情報通信学会誌 33巻１号』29-35頁（情報通信学会，2015年）31頁参照。

59 最大判昭和30年４月27日刑集９巻５号924頁，最大判昭和36年６月７日刑集15巻６号915頁，最決平成８年１月29日刑集50巻１号１頁参照。

60 *See Riley*, 134 S. Ct. at 2491.

61 *See id*. at 2485.

62 佐藤幸治「第35条」，樋口陽一ほか『注解法律学全集２ 憲法Ⅱ〔第21条～第40条〕』316-334頁（青林書院，1997年）319頁参照。

63 憲法35条１項において「住居」等が明示されているのは，それが「犯罪の証拠とされかねないさまざまな情報が集積されている空間・場所の代表例」であるからとしつつ，無体物たる情報の点検に対しても令状主義の要請が及ぶという旨を説く学説として，渋谷秀樹『憲法 第２版』（有斐閣，2013年）240-241頁参照。情報とそれを擁する設備との一般的な不可分性を念頭におくと，そのような不可分性が認められる限り，無体物たる情報とそれを内包する有体物たる設備とは一体的に捉えることが可能である。したがって，捜索等の対象に前者の情報が含まれることをもって，憲法35条１項の適用の余地がただちになくなるものと解することは，妥当ではないと考えられる。

64 なお，「電磁的記録に係る記録媒体」の捜索等について規定した刑事訴訟法110条の２・222条１項，前述（注46参照）の遠隔アクセスによる記録媒体等の捜索等について規定した同法99条２項・218条２項参照。

65 松井茂記『日本国憲法（第３版）』（有斐閣，2007年）532頁，井上・前掲（注17）13頁参照。

66 これに対し，自営の端末設備については，当該範囲が概して狭くなると思われるが，ネットワークとの接続を通じて一定の範囲で通信管理主体が端末内包情報にアクセス可能となるということに変わりはない。

67 例えば，携帯電話端末にSIMロック（接続先のネットワークを限定するための技術的な措置）を施す自由が通信管理主体に対して原則として認められていることは，通信設備としての当該端末の支配・管理に対する権利・利益が通信管理主体に（も）あるということを裏づけるものとなろう。なお，SIMロックの解除のあり方をめぐっては，日米

両国においてさまざまな議論があるが，その様相を米国の状況を中心に整理したものとして，海野敦史「米国における携帯電話のSIMロック解除の再合法化とその含意－通信の利用者の保護とプログラムの著作権者の保護との相克－」，『ICT World Review 7巻6号』12-38頁（マルチメディア振興センター，2015年）参照。なお，端末設備からの情報の取得可能性が当該設備の設計のあり方に左右され得るということに照らすと，端末内包情報に対して（通信管理主体のみならず）端末設備の製造・開発者による支配・管理が事実上一定の範囲で及ぶという側面も認められ得ると考えられるが，この点については本稿では措く。

68 *See* Federal Communications Commission, In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, *Declaratory Ruling* (released June 27, 2013), FCC 13-89, 28 FCC Rcd 9609, 9613.

69 *See id*. at 9615.

70 具体的には，法律上，電気通信事業者がそのネットワーク（電気通信回線設備）に利用者の端末設備を接続するための請求を受けた場合，一定の技術基準に適合しない場合等を除き，当該請求を拒否できない（すなわち，当該技術基準に適合しない端末整備への接続の請求については拒否できる）こととすることにより（電気通信事業法52条1項），端末設備の技術基準への適合性を確保することとなっている。当該技術基準については，①ネットワーク（電気通信回線設備）を損傷等しないこと，②他の利用者に迷惑を及ぼさないこと，③電気通信事業者のネットワークと利用者の端末設備との責任分界点を設けることが基本とされているが（同条2項参照），かかる規律の実際の適用（担保）方法としては，電気通信事業者による端末設備の検査の実施（同法69条1項），当該検査の省略事由を充足する端末機器（電気通信事業者により公示されたもの，一定の認定機関による技術基準適合認定を受けた〔いわゆる技適マークを有する〕端末機器）の利用（電気通信事業法施行規則〔昭和60年郵政省令25号〕32条1項4号・同項5号参照）等がある。また，利用者が端末設備を接続する際の工事の実行については，簡易なものを除いては利用者に委ねられておらず，原則として工事担任者資格者証の交付を受けている者が担当することが予定されている（電気通信事業法71条1項）。さらに，端末設備に異常がある場合等においては，電気通信事業者が利用者に対して当該設備の接続が前述の技術基準に適合するか否かの検査を受けることを求めることができ，この場合利用者においては正当な理由がある場合等を除きその請求を拒否できないこととされている（同法69条2項）。このように，法令上も，ネットワークと端末設備との間には一定の責任分界

点が設定されることが予定されつつも，端末設備の接続及びそれを通じた利用に関しては各種制約が設けられており，その限りにおいて，当該端末設備には電気通信事業者（通信管理主体）の支配・管理が部分的に及んでいると言える。換言すれば，電気通信事業法上は，利用者が所有・占有する端末設備は一次的に電気通信事業者が支配・管理するものと観念されており，各電気通信事業者においては，自らのネットワークと違法な状態の端末設備とを接続する（すなわち，電気通信事業法違反の状態を惹起する）ことのないよう，「通信設備の適切な管理に必要となると認められる範囲内において，個々の端末設備の利用実態を監視する責務」を実質的に負っているものと解される。

71　ここでいう通信管理権の詳細について，海野・前掲（注10）343-348頁参照。

72　海野・前掲（注10）195-196頁参照。ここでいう「適切な管理」の内実には，通信設備の安全性・信頼性の確保が含まれる。このような「通信設備の適切な管理」の確保に対する憲法上の客観法的要請にかんがみると，端末設備を含む通信設備及びその内包する情報に対する公権力の不当なアクセスについては，（行使可能範囲が限定的な）通信管理権の侵害というよりも，むしろ端的にかかる客観法的要請に対する違反として捉えた方が合理的な場合が少なくないであろう。

73　海野・前掲（注10）143頁参照。

74　同意捜索（consent searches）の可能性を肯定しつつ，同意の任意性を判断する方法として，状況を総合的に検討したうえでの事案ごとの判断に基づくもの（権利告知は不要）という方向性を示した米国の判例として，以下を参照：Schneckloth v. Bustamonte, 412 U.S. 218, 228-229, 233 (1973).

75　無令状での同意捜索の主な問題点については，緑大輔「合衆国における同意捜索の問題」，『修道法学 27巻１号』１-44頁（広島修道大学法学会，2004年）参照。併せて，住居等に対する同意捜索を禁止する犯罪捜査規範（昭和32年国家公安委員会規則２号）108条参照。

76　判例は，警察官の職務質問に付随して任意手段として行われる所持品検査について，「所持人の承諾を得て，その限度においてこれを行うのが原則である」と説いている。ただし，「捜索に至らない程度の行為」である限り，強制にわたらないものであれば，たとえ所持人の承諾がなくても，「具体的状況のもとで相当と認められる限度においてのみ」所持品検査として許容され得るという旨も説かれている点に留意する必要がある。最判昭和53年６月20日刑集32巻４号670頁参照。併せて，最判昭和53年９月７日刑集32巻６号1672頁参照。このような判例の考え方を基本的に支持する学説として，例えば，野中俊彦ほか『憲法Ⅰ（第５版)』（有斐閣，2012年）426頁参照。

77 なお，「公権力による任意のアクセス」とはやや異なる文脈のものであるが，同意捜索をめぐる米国の連邦最高裁判所の判例においては，ある捜索等の対象が複数の者による共同の支配・管理下におかれている場合の一方の者（被疑者以外の者）が行った任意の同意の効力に関して，これを肯定的に捉える考え方が示されている。*See* United States v. Matlock, 415 U.S. 164, 169-171 (1974)．すなわち，被疑者がその妻とともに賃借している住居の捜索に対する妻の同意が問題となった事案において，点検対象となる住居又は所持品に対して「共同の権限（common authority）を有し，又は他の十分な関係（other sufficient relationship）を有する第三者」からの同意が得られた場合には，それに基づく同意捜索が有効となるという旨が説かれている。しかしながら，「第三者」の同意に基づく同意捜索の肯定は，当該捜索を「権利の放棄」と位置づけてきた伝統的な見方に整合しないという旨が指摘されている。*See* Sharon E. Abrams, *Third-Party Consent Searches, the Supreme Court, and the Fourth Amendment*, 75 J. CRIM. L. & CRIMINOLOGY 963, 993 (1984)．また，ここでいう「共同の権限」は「単なる財産上の利益（mere property interest）」を意味するものではなく，「通常共同のアクセス又はコントロールを有する人による所有物の相互使用（mutual use of the property by persons generally having joint access or control）」の実態の有無によるものであるとされているが（*See Matlock*, 415 U.S. at 171, n.7），「他の十分な関係」の内実については極めて不明確である。*See* Abrams, *supra* note 77, at 976, n.56．一方，それに先立つカリフォルニア州最高裁判所の判例においては，複数の者による共同の支配・管理に服する住居の捜索に対して，現場を離れて逮捕された一方の者が同意したものの，その同居人である他方の者が拒否した場合に関して，当該一方の者の同意の旨が当該他方の者に伝えられていなかったこと，捜索の緊急性も認められなかったこと，前者の同意は後者の反対にもかかわらず捜索を認める趣旨のものではないことなどを主な理由として，前者の同意に基づく同意捜索は違法であるという旨が説かれている。*See* Tompkins v. The Superior Court of the City and County of San Francisco, 59 Cal. 2d 65, 68-69 (Cal. 1963)．この判例は，捜索に対する一方の者の同意がそれに対する他方の者の拒否の劣後におかれることの根拠が十分に示されたものとは言いがたいが，この判決の趣旨から，一方の者による同意が他方の者のプライバシーを侵害する効果が認められる場合には，当該同意の有効性が否定され得るという帰結が示唆されると説く学説が有力に提示されている。*See* Wayne R. LaFave, *Search and Seizure; A Treatise on the Fourth Amendment*, Vol.4 (5th Ed., West, 2012), at 207-208．このような議論を踏まえると，我が国において，（一定の情報を内包する）ある設備に対する支配・管理者が複数（さしずめ二人）存在する場合，公権力に

よる当該設備及びその内包する情報への捜索等に至らない任意のアクセスに対する一方の支配・管理者の同意の効力をどのように捉えるかということについては必ずしも一義的なものではないと思われるが，米国の同意捜索に関する前述の有力な学説の考え方をこの問題に援用する余地があるとすれば，少なくとも一方の者による同意が他方の者の基本権に関する法益（「秘密」）を侵害することとなる場合には，当該一方の者による同意の有効性は認められないと解することが可能であろう。このような考え方に基づく限り，端末内包情報を支配・管理する一方当事者たる通信管理主体による公権力のアクセスへの同意が，他方当事者たる通信当事者の「秘密」を侵害する効果をもたらすと認められる限り，当該同意単独の有効性は否定されるという帰結が導かれ得ると考えられる。

78　海野・前掲（注10）321-325頁参照。

79　この点について，海野・前掲（注10）312頁参照。

80　なお，公権力による端末内包情報への任意のアクセスに際して，一定の技術的な措置を通じて，「秘密」たる情報とそれ以外の情報とが適切に区別可能となるような例外的なケースが想定されることとなる場合には，その限りにおいて，前者の「秘密」たる情報へのアクセスについてのみ憲法21条２項後段の規定に基づき禁止され，それ以外の情報へのアクセスについては憲法13条に基づくプライバシーの権利等の保障の問題となり得るにとどまるものと解する余地が生じ得ると思われる。

81　これは，デジタルデータ伝送用の端末設備である限り，法令上は「専用通信回線設備等端末」（端末設備等規則２条２項16号及び注２参照）ないし「デジタルデータ伝送用設備に接続される端末設備」（同規則35条参照）に該当する。ただし，一定の電気通信番号を用いた音声伝送機能を有する場合には，「インターネットプロトコル電話端末」（同規則２条２項７号及び注２参照）にも該当し得る。