リモートアクセスによる差押えに伴う問題点の一考察

—— A study on the issue of a remote access seizure. ——

早乙女　宜　宏

第１　はじめに

ネットワークが発展したことにより，電子計算機（以下「コンピュータ」という。）は単体（スタンドアローン）で道具として使われる方法から，ネットワークを構成する端末の一つとして利用される形態が浸透してきた。今では，官庁・企業等の業務活動で使用されるコンピュータもさることながら，個人のコンピュータもネットワークに接続されているのがあたりまえと言えるほどに浸透している。さらには，コンピュータと言えば箱型のパーソナルコンピュータを指していた時代から，スマートフォンの登場により手のひらサイズのコンピュータが誕生し，しかも，これらは常時ネットワークに接続して，様々な情報をリアルタイムに取得，送信している。

こうしてネットワークが世界規模で発展することと対応するように，犯罪現象もネットワークが関与することが多くなってきた。コンピュータ関連犯罪は，①コンピュータを対象とする犯罪，②コンピュータを手段とする犯罪，③コンピュータが付随的役割を担う犯罪，の三種類に分類できるとされる。[(1)] 関与の形態は様々であるが，ネットワークを利用して国内外のウェブサイトから犯罪を実行するための情報を集めたり，電子掲示板やソーシャル・ネットワーク・サービス（以下「SNS」という。）を使って共犯者を集めたり，電子メールや大容量ファイル送信サービスが犯罪情報の送受信に利用されたりすることもあれば，ネットワークを利用してウイルスメールを送りつけてシステムを破壊したり，ネットワークを利用して他人のコンピュータをハッキングし，電子送金システムを不正に利用するなどの犯罪が行われているのである（いわゆる「サイバー犯罪」[(2)] などと呼ばれる。）。

これらの例はいずれも意図的にネットワークを利用した行為であるが，現代においては，ネットワークの利用が日常生活に溶け込んでいるため，ネットワークを利用しているという意識をしないままに用いている事が多い。例えば，コンピュータの文書作成ソフトで文書を作成している間に，バックグラウンドではネットワークに接続して基本ソフト（OS）のアップデート情報を取得しているし，文書ファイルを保存した際には自動的にクラウドサーバへ当該ファイルを送信して保存していることもある。スマートフォンともなれば，ポケットに入れた状態でもバックグラウンドで通信を頻繁に行い，プッシュ通知により各アプリケーションが新着情報を取得し，スマートフォン内の電磁的記録（以下「データ」という。）については，クラウド上のサーバに

(1)　川出敏裕「コンピュータ犯罪と捜査手続」法時53・10・１（法曹会，2001）。
(2)　警視庁では，「高度情報通信ネットワークを利用した犯罪やコンピュータまたは電磁的記録を対象とした犯罪等の情報技術を利用した犯罪」のことをサイバー犯罪と定義している。

送信し，バックアップとして蓄積していることもある。(3)

現代の日常生活においては，コンピュータとネットワークはいたる所に存在し，その結果，いかなる犯罪類型においても，その解明に必要な証拠となる記録や情報が，データという形でコンピュータに記録・保存され，かつ，ネットワークを経由して外部のサーバに記録・保存されていることが少なくない。

そして，これらのデータは，刑事・民事を問わず，重要な証拠となっているのが現状である。刑事事件においては，電子メールの送受信履歴が当たり前のように証拠化され，スマートフォン内に保存されている静止画・動画データは証拠化され，GPSログにより移動経過も証拠化されている。民事事件においてもSNS上での投稿記事が証拠化され，メッセージアプリ(4)の会話データが証拠として提出されることは今や一般的とさえ言ってよいだろう。スマートフォン一つ差し押さえることができれば，それを分析することで，所有者の足取りから会話内容，性的趣向から果ては信仰まで把握することができる時代である。スマートフォンは，その所有者の分身とさえいえるかもしれない。

コンピュータには様々なデータが集約されているため，捜査活動においても，収集すべき証拠がデータである場合が多くなってきていた。これらのデータは，保存場所によっては，ネットワークを通じて誰もがアクセスすることが可能であるため，従来の捜査のように人海戦術を用いて額に汗をかかずに入手し得る反面，データという性質上，移動，変更，消去することは極めて容易である。

刑事訴訟法上これらのデータを収集するには，捜査機関の管理下に置くという意味で，データの捜索・差押えということも理論上はあり得なくはない。しかし，刑事訴訟法上の差押えは，「証拠物又は没収すべき物と思料するもの」を差し押さえることができると規定し（刑事訴訟法（以下略）222条１項，99条１項），その対象が有体物に限られている(5)。債権や電気，熱などのエネルギーは差し押さえの対象とならない(6)のと同様に，無体物であるデータそのものを直接差し押さえることはできないと考えられている(7)。そこで，データを証拠とするために，データを記録した媒体としてのフロッピーディスクやCD-R等の記録媒体を対象に捜索・差押えが実施されてきたのである(8)(9)。

もっとも，このような捜索・差押えが実現可能であった背景には，コンピュータがネットワークから切り離されてスタンドアローンで利用されるという前提があってこそのもので，データも記録媒体も被疑者の管理下にあり，それらが一対一で結びついた存在だから可能な方法であった。しかも，スタンドアローンで利用されるコンピュータに保存されているデータは，通常であれば当該コンピュータの使用者たる被疑者の管理する情報が保存されているに過ぎないから，無関係の第三者の情報が大量に保存さ

(3)　自動的とはいえ，多くの場合は，使用者はデータを送信することについて事前に同意し，これに基づいてアップロードされている。
(4)　有名なアプリとしてはSkype，LINEやWeChatなどが挙げられる。
(5)　渡辺咲子『大コンメンタール刑事訴訟法』256頁（青林書院，第二版，2011）。
(6)　河上和雄『証拠法ノート１捜索・差押』10頁（立花書房，改訂版，1998）。
(7)　壇上弘文「サイバー関係をめぐる刑事訴訟法の一部改正について」刑ジャ30・42（成文堂，2011）は，現行の法解釈によっても電磁的記録を捜索・押収の対象とすることが可能であることを示唆する。
(8)　CD-R等の大量のデータを保存できる媒体は，どの範囲で差し押さえができるかという問題もある。東京地決平成10・２・27判時1637・152は，インターネット・サービス・プロバイダの支店内を捜索し，同社と通信サービス契約を結んだ400名余の顧客データを含むフロッピーディスク１枚を差し押さえた事例であるが，準抗告審において，被疑者以外のデータについては関連性を認めず，準抗告が認容された例である。
(9)　なお，サイバー犯罪条約19条では，データに対し有体物に対するのと同等の捜索・差押え権限を確立することを目的として，データそのものの捜索又はこれに類するアクセスを行う権限を与えるために必要な立法その他の措置を採ることを各国に求めている。

れていることは少なく，これらを差し押さえても，第三者の利益を侵害する可能性は低かった。

しかし，現在のようにコンピュータがネットワークに常時接続し，データは被疑者の管理下にあるコンピュータではなく，いわゆるクラウドサーバに保存され，第三者の物理的な管理下に置かれているような状態では，被疑者のコンピュータの記録媒体を差し押さえても証拠となるデータを取得することができない。また，クラウドサーバを管理する事業者の記録媒体には，顧客情報等の被疑事実とは全く関係ない第三者の情報が大量に保存されている可能性は極めて高く，スタンドアローンのコンピュータを前提としてきた時代とは利害状況が異なるのである。

そこで，「情報処理の高度化等に対処する」ことを謳った平成23年の刑事訴訟法改正（平成23年法律第74号，2012年６月施行）において，記録命令付差押え（218条１項），いわゆるリモートアクセス（同条２項），ネットワーク管理者に対する通信履歴の保全要請（197条３項～５項），処分実施の際の協力要請（222条１項，111条の２）という新たな規定が盛り込まれた。その中でも，リモートアクセスは，コンピュータとネットワークで接続された他の記録媒体に記録されているデータを，当該コンピュータまたは他の記録媒体に複写した上，これを差し押さえることができることとしたものである。(10)

もっとも，改正法の原案が答申されたのはスマートフォンが普及するより前の平成15年のことである。日本でスマートフォンが本格的に普及し始めるきっかけとなったiPhoneの発売は平成19年，Android を搭載した端末は平成21年のことであり，ネットワークや，クラウドコンピューティング(11)の利用形態が当時とは大きく異なってきており，改正法では対応できない事案が既にみられる。本稿では，この改正の中でも，リモートアクセスに焦点を当て，ネットワーク時代においてデータを証拠収集する際の問題点について若干の考察をしてみたい。

第２　平成23年刑事訴訟法改正

前述したようにコンピュータの利用はネットワークに接続した形態によるものが一般的となり，コンピュータで処理すべきデータは，ネットワークを利用することにより，物理的に離れた様々な場所にある記録媒体に送って保存し，必要なときには取り出すということが，極めて容易となるとともに一般化している。

そのため，捜査では，必要なデータが記録されている記録媒体を特定することが困難な場合も多い上，仮に特定できても様々な場所に設置された多数の記録媒体についてそれぞれ差押えを行わなければならないこととなる。特にクラウドコンピューティングにおいては，どこに所在するコンピュータによって処理されているのか把握できない場合があるし，(12) また，ひとたび強制捜査に着手すれば，被疑者に捜査を察知され得るところ，証拠となるデータを瞬時に移転することにより，容易に隠匿され得ることなどから（クラウドサーバに保存されたデータであれば，共犯者や知人に頼んでおくことで，被疑者以外の者により，データの移転や削除をすることは容易である。），コンピュータやこれに付属する記

(10)　古田佑紀「コンピュータネットワーク上の捜査と第三者の保護」芝原邦爾＝西田典之＝井上正仁編集『松尾浩也先生古稀祝賀論文集（下巻）』188頁以下（有斐閣，1998）。

(11)　米国国立標準技術研究所（NIST）の定義によると，クラウド・コンピューティングは，共用の構成可能なコンピューティングリソース（ネットワーク，サーバー，ストレージ，アプリケーション，サービス）の集積に，どこからでも，簡便に，必要に応じて，ネットワーク経由でアクセスすることを可能とするモデルであり，最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものであり，このクラウドモデルは５つの基本的な特徴と３つのサービスモデル，および４つの実装モデルによって構成される。

(12)　小野将司「クラウドコンピューティングと情報セキュリティ侵害事例」警論64・３・41（立花書房，2011）。

録媒体等を差し押さえる方法だけでは，捜査目的を達成できないことも多い。

そこで，先に述べたリモートアクセス（218条2項）という新たな規定が盛り込まれたのである。同条2項は，「差し押さえるべき物が電子計算機であるときは，当該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，当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている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ものから，その電磁的記録を当該電子計算機又は他の記録媒体に複写した上，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，差押えの形式に立っているため，その文言上，リモートアクセスは，コンピュータ等が差し押さえるべき物でなければならず（ただし，結果として差押えはしなくてもよいとされる。），かつ，差押えに先立って行われることが予定されている。また，「保管するために使用されていると認めるに足りる状況」とは，差し押さえるべきコンピュータの使用状況等から，保管するために使用されている蓋然性が認められるということであり，具体的には，差し押さえるべきコンピュータにリモート・ストレージ・サービスのアカウントとの設定がなされている場合などがこれに当たると考えられている。(13)(14)

第3　データの保管場所

改正法の原案が答申された頃と現在とで，ネットワークの利用環境が大きく異なってきたことと並行して，データの保存方法についても大きな変容を遂げており，このことは電子メールを例にすると理解しやすい。電子メールが，常にユーザのコンピュータやスマートフォンの端末内部に保存されているのかといえば，現在はそうではないことが多い。

かつて，UNIXで電子メールが始められた頃は，ユーザはUNIXホストにログインをして電子メールを読んでいた。しかし，パーソナルコンピュータが普及したことで，作業環境がパーソナルコンピュータに移行したため，電子メールが届くホスト（メールサーバ）と作業環境が分離することとなった。そのため，メールサーバに他のホスト（パーソナルコンピュータ等）からアクセスし，手元でメールを読みたいという需要が生まれ，こうして開発されたプロトコルが，POP（現在はバージョン3のためPOP 3という。Post Office Protocolの略語。）である。(15)したがって，POP 3では，電子メールをクライアント側の端末にダウンロードし，クライアント側でメールを管理する一方で，メールサーバ上のメールは削除していた。すなわち，電子メールはユーザのコンピュータ内のハードディスクに保存されているということになる。サーバにアクセスして，電子メールをダウンロードしてユーザ端末に保存するため，サーバ上の電子メールデータは削除される設計であるため，個人のコンピュータの記録媒体を差し押さえれば，電子メールデータも当該コンピュータ内に保存されているので，これを分析することが可能だった。

一方，現在主流はIMAP（Internet Message Access Protocolの略語）というプロトコルである。IMAPは，メールサーバ上にメールを保存し，必要に応じてメールソフト上に表示する。ローカルフォルダはそのホストのディスク上にメールが保存されているが，IMAPと表示されているフォルダの実体

（13）　単に閲覧し得るだけのデータも複写の対象となってしまいかねないという指摘を反映して，被処分者が変更もしくは消去できるものに限定をかけたものである（すなわち，専ら第三者が同じクラウド上に保管しているデータは対象外になるという趣旨。）。第162回国会衆議院法務委員会議事録第26号大林政府参考人発言を参照。

（14）　池田修・前田雅英『刑事訴訟法講義』181頁（第6版，東京大学出版会，2018）。

（15）　ネットワークマガジン編集部『ネットワークマガジン2007年12月号』44頁（KADOKAWA，2014）。

はサーバ側にある。[16] 基本的に電子メールデータをユーザの端末に保存しないので，端末内には電子メールデータが存在せず（もっとも数日分はキャッシュとして端末内にも保存される），サーバ上にメールデータが残る。そのため，個人のコンピュータの記録媒体を差し押さえたところで，分析できるのは端末内に残っている数日分のキャッシュされた電子メールデータだけである。すべての電子メールデータを取得するためには，ネットワークに接続されたコンピュータから，ユーザの認証情報（IDやパスワード等のこと。以下同じ。）を用いてログインをし，サーバにあるメールデータにアクセスする必要がある。[17]

電子メール以外のソフトウェアにおいても，ユーザ作成のデータをクラウドサーバに保存する場合は多いだろう。ユーザの使用するコンピュータには，最低限，クラウドサーバに正当なユーザであることを認証してもらうための認証情報が保存されているのみであり，それ以外のデータはすべてクラウドサーバに保存されているものもある。しかも，認証情報は，セキュリティの観点（情報セキュリティにおける３要素のうち「機密性の確保」）からするとユーザのコンピュータに保存しておくべきものではない。慎重なユーザであれば，クッキー[18]による認証情報の自動保存をオフにしているか，その都度削除して，認証情報は別の方法で保管しているだろう。一般にコンピュータを使用していると，一度ログインをしたことのあるウェブサイトであれば，アクセスするだけで自動的にログインをするか，または，ユーザIDとパスワードが最初から入力された状態となる場合がある。これは，ブラウザのクッキーという機能によるものである。クッキーは，ユーザの使用しているコンピュータのハードディスクに保存されており，[19] ユーザはクッキーを直接操作することはなく，意識せずに使用している。このような状態であれば，捜査機関が当該コンピュータの記録媒体を差し押さえたときに取得できるのは，認証情報のみということになる。そこから先に保存されているデータについては，これらの認証情報を用いて，クラウドサーバにアクセスして複写（ダウンロード）しなければならない。

このように，クラウドコンピューティングが発展した現在のネットワーク環境においては，被疑者であるユーザが管理しているコンピュータの記録媒体を差し押さえたとしても証拠としての価値が乏しいこともあり，[20][21] 捜査機関としては，その先にあるクラウドサーバ上のデータの入手を考えることになる。

第４　リモートアクセスによるデータの取得

１．コンピュータがネットワークに接続している環境において，データを証拠化するには，被疑者自らに有利な電子データであればユーザである被疑者自らの権限で取得すればすむことである。被疑者の立場で見れば，被疑者に有利な証拠がデータで存在するのであれば，それがどこに保存されていようと，弁護人にそれらを取得することの承諾を与え，弁護人がネットワークにアクセスして取得することには

(16)　ネットワークマガジン編集部・前掲注(15)48頁。
(17)　POP３なのかIMAPなのかを簡単に見分けるには，スマートフォンのネットワーク接続をオフにした状態で電子メールを読んでみて，閲覧できればIMAP，できなければPOP３と考えられる。
(18)　ウェブブラウザの機能の一つで，ウェブサイトにアクセスしたユーザの情報をウェブブラウザに保存し，次回アクセス以降に再利用することができる。ウェブサイト制作者の側で，保存すべき情報を選択し，組み込むことができる。
(19)　隠しフォルダであり非表示となっているため，普通にコンピュータを使用している限りは見ることはない。
(20)　前田雅英「第23講サイバー犯罪に関する法改正と捜査方法」警論64・８・159（立花書房，2011）。
(21)　認証情報そのものが被疑者と犯人を結びつけるという意味では重要なこともあろうが，ログイン後に取得できるデータの方が証拠として重要であることが多いだろう。

問題がないだろう。弁護人の視点からすれば，これまでは記録媒体そのものを差し押さえられてしまうと，たとえその中に被疑者に有利な証拠が保存されていたとしても，それを取得する術はなかった。公判前整理手続が導入されたことで証拠開示手続が充実したが，必ず公判前整理手続に付されるわけではないし，公判前整理手続になるまでは証拠開示を求める手続は法定されていない。そのため，記録媒体が差し押さえられてしまうと，その中に被疑者に有利なデータが存在していたとしても，被疑者段階での防御活動に活用することはできなかった。しかし，クラウドサーバにデータが保存されるようになると，被疑者から認証情報を聞き出し，クラウドサーバへのアクセスの承諾を得ることで，たとえ記録媒体が差し押さえられていても，同じデータを他のコンピュータからアクセスして取得することが可能となる。その意味で，弁護人の立場からすれば，クラウドコンピューティングの発展によって，被疑者段階におけるデータを活用した弁護活動を行いやすくなったことは間違いない。

一方で，捜査機関については，改正法によってリモートアクセスによるデータ取得が可能となったが，現実的にはリモートアクセスによってデータを取得することは決して容易ではないことが明らかとなったのが東京高判平28年12月７日高刑集69巻２号５頁である。

２．裁判例（東京高判平28年12月７日高刑集69巻２号５頁）

⑴　事案の概要

原判決[(22)]認定の犯罪事実の要旨は，被告人が，①いずれも行使の目的で，学生証や危険物取扱者免状，自動車運転免許証等を偽造し，②I及びJと共謀の上，某会社支店の正面玄関ガラス窓１枚をバールでたたいて損壊するなどし，某区内のビル１階車庫において，人の現住等を認識せず，ガソリンをまくなどして火を点け，天井等を焼損させた（以下「放火等事件」という。）というものである。

捜査の過程において，警察官らは，本件各公訴事実とは別件である，携帯電話通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律違反，偽造有印公文書行使幇助を被疑事実として，被告人を通常逮捕するとともに，同日，同じ事実を被疑事実とする捜索差押許可状（以下「本件捜索差押許可状」という。）に基づき，当時の被告人方（以下，単に「被告人方」という。）等を捜索し，ノート型パーソナルコンピュータ（以下「本件パーソナルコンピュータ」という。）等を差し押さえた（以下「本件捜索差押え」という。）。

本件捜索差押許可状においては，刑事訴訟法218条２項の場合に行う同法219条２項の「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」として，「メールサーバの記録領域」等が具体的に記載されており，いわゆるリモートアクセスによる複写の処分が許可されていた。しかし，捜査機関は，本件捜索差押えの時点では，本件パーソナルコンピュータにログインするパスワードが判明していなかったことから，リモートアクセスによる複写の処分を行うことができなかった。

捜査機関は，差し押さえた本件パーソナルコンピュータを解析したところ，○×に係る犯行の痕跡や○×メールアドレスのアカウント（以下「○×アカウント」という。）へのアクセス履歴の存在が認められたことから，本件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等を企図し，検証許可状の発付を得た。

そして，捜査機関は，本件パーソナルコンピュータの内容を複製したパーソナルコンピュータからインターネットに接続し，○×アカウントにログイン

(22)　横浜地判平28・３・17判時2367・115。

し，○×メールアドレスに係る送受信メールを抽出するとともに，ダウンロードし，保存した（以下，「本件検証」という。）というものである。

これに対し，弁護人は，本件検証には重大な違法があるとして，本件検証の結果及び関連する証拠は違法収集証拠として排除されるべきであると主張した。

原審は，現行法上，差し押さえた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はないこと，そのような行為は，メールサーバ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ないこと，加えて，サーバーコンピュータが他国に存在している場合にこれにアクセスすることは，その国の主権に対する侵害が問題になり得るなどとして，本件検証の違法性の程度は重大なものであり，令状主義の精神を没却すると判断した。もっとも，当該捜査から得られた派生証拠については，不可避的発見の法理や，密接な関連性がないことから証拠能力を認めて，被告人を有罪とした。被告人は控訴。

⑵　判旨

「本件検証は，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。しかも，そのサーバが外国にある可能性があったのであるから，捜査機関としては，国際捜査共助等の捜査方法を取るべきであったともいえる。そうすると，本件パソコンに対する検証許可状の発付は得ており，被告人に対する権利侵害の点については司法審査を経ていること，本件パソコンを差し押さえた本件捜索差押許可状には，本件検証で閲覧，保存したメール等について，リモートアクセスによる複写の処分が許可されていたことなどを考慮しても，本件検証の違法の程度は重大なものといえ，このことなどからすると，本件検証の結果である検証調書及び捜査報告書について，証拠能力を否定した原判決の判断は正当である。」として，本件検証には重大な違法があり証拠能力を否定するとした原判決を支持した。

さらに，本件検証から得られた派生証拠の証拠能力についても，密接な関連性がないとした原判決を支持し，証拠能力を認め，控訴を棄却した。

⑶　本判決について

本件は，検証令状にリモートアクセスの対象が明示されていなかった事案であり，「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「本件」を付していることからすると，一般論として，検証令状にリモートアクセスの対象が明示されていた場合に，検証として行うことができるかについては触れておらず，その立場は明らかでない。もっとも，218条２項によらない検証等によるリモートアクセスが排除されるものであるかは，立法過程でも明確にされたわけではない。しかしながら，218条２項がリモートアクセスの要件を課した趣旨からすると，それ以外の方法によるリモートアクセスは否定されていると解するのが相当であろう。

また，判決は検証ではできない強制処分を行ったとし，続けて，「しかも」と述べて，サーバが国外に存在した可能性を指摘して，重大な違法を導いている。サーバが国外にあり，他国の主権侵害がありうることが違法の重大性の判断に影響していると考えられる。とすると，サーバが国内にある場合については，重大な違法とまではならないと考えているとも見られる。しかし，例えばＡの自宅に対する捜索令状で，Ａの国内の別荘を捜索することはできないことを考えると，サーバの所在が国内外にあるかを重視するべきではなく，令状の効力がどこまで及んでいるかという視点から考えるべきである。

また，違法収集証拠排除法則は，国内における将来の違法捜査抑止の見地と，事後的な被処分者に対する権利侵害に対する救済措置であることに鑑みれ

ば，外国主権に対する侵害という国際法違反の違法性を，排除法則の枠内で捉えることには疑問がある。[23] 外国主権の侵害が排除法則の枠内での違法性を基礎づけるとすれば，218条２項による正規のリモートアクセスにおいても外国主権の侵害の問題はクリアできないため，排除法則の適用が問題となってしまいかねないのであり，リモートサーバの所在が国外にあることは「検証」の違法性を増大する事情ではないと考えられる。

本判決は，218条２項の趣旨に沿った判断ということができるが，上記の通り国際法違反を排除法則の違法性に取り込んだ点に疑問があることと，本件における捜査機関は，サーバの所在地を確認し国外にあるとは限らないと考えていたこと，一応検証令状を取得しており，しかも，検証令状を取得する際の疎明資料にはリモートアクセスを行う旨の記載があったことからすれば，実質的にはリモートアクセス許可の令状審査を受けていたに等しく，単に令状の形式を間違えたに過ぎないと評価できるものであるから，令状主義潜脱の意図はなく（この点は第一審判決でも認定されている。），排除法則を適用するに足りるほどの重大な違法を認定したことには疑問がある。

第５　リモートアクセスによる限界と今後の課題

１．リモートアクセスの限界

上記裁判例は，改正法が平成15年時点の技術を基準としていたこともあって，想像以上にクラウドコンピューティングが発達，浸透した現在においては技術と法律の間の齟齬が顕在化している例といえる。リモートサーバにデータを預ける形態でコンピュータを利用する態様は格段に増加しており，差押えの対象となったコンピュータには証拠価値のあるデータが全く存在しない事態も十分想定しえ，差押え対象となったコンピュータ本体を差押えただけでは証拠価値も乏しい。また，リモートサーバが「機能的一体性故に証拠となるデータの存在する蓋然性が共通して認められる」という立案当初の想定も成り立たない事態も増えつつある。[24]

上記裁判例では，もともとは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令状により，コンピュータを差押えている。本来は，ここでリモートアクセスによる複写を行うのであるが，差し押さえる予定のコンピュータを使用するための認証情報が分からなかったため，当該コンピュータを差押え後に解析して，ユーザ名，パスワードの認証情報を明らかにしてから「リモートアクセス」することを試みた。そして，その手段として，新たに検証令状を取得し，メールサーバ（これがリモートサーバにあたる）へのアクセスについては，当該コンピュータを検証するための必要な処分（222条，129条）として実施し，メールを当該コンピュータにダウンロード，保存したのである。

改正法218条２項は，リモートアクセスによる差押えは，①「差し押さえるべき物」であって，②差押えに「先立って」することが許されるとしている。①の条件がなければ，捜査機関のコンピュータから被疑者のデータが保管されるリモートサーバへリモートアクセスが可能となってしまうため，リモートアクセスが秘密裏に広く行われてしまうおそれがあること，②の条件は，本条が「変更若しくは

(23)　芝原邦爾『経済刑法-理論と実務』572頁（商事法務，2017）は，「違法な越境アクセスの効果は，国際法上の国家責任の問題であるから，日本国が国際法違反行為について負う原状回復義務の履行として主権侵害によって得られたデータの破棄を義務付けられ，したがって，国内裁判所が国内の刑事手続においてそのデータを用いた立証・事実認定もできなくなると構成すべきことになろうか」とし，国際法の解釈運用の問題であって、刑訴法の解釈の問題ではないとする。

(24)　笹倉宏紀「差押え済みのパソコンを『検証すべき物』とする検証許可状によりリモートアクセスをすることの許否」ジュリ1518・183（有斐閣，2018）。

消去をすることができることとされている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」の存在がデータの差押えを許容していることになるから，そのような状況が現存している，すなわち，コンピュータが外部に接続している状態をもって，[25] リモートアクセスの正当な理由としている。このような条文の建前になっているのは，リモートアクセスは，差押えのための付随的手段として位置づけられているに過ぎないからである。

上記裁判例が端的に示すように，コンピュータやリモートサーバへのアクセスは，ユーザ名やパスワード等によるアクセス制限が必ずかかっていると言ってよく，しかもデータは容易に移転や削除ができてしまう性質を有することから，迅速に行う必要もある。そのため，「差押えに先立って」，時間を要するユーザ名やパスワードの解除を行うことは至難の業で，現実的でないのである。

確かに，差押えの対象となっているコンピュータが，リモートアクセスのための認証情報を設定済みであったり，認証が解除してあれば，差押えに先立って，リモートアクセスによる複写は可能である。しかし，認証情報が設定済みというのは，自動ログインが設定されている場合等の限られた状況のみで，故意に犯行を行う者が，そのような安易な設定にしているとは考えられない。そうすると，捜査機関はコンピュータを解析して，過去のアクセス履歴や通信履歴などから，認証情報を抽出しなければならないが，これはもはや当該コンピュータのデータを捜索していることに等しい。しかし，捜索とは，差押えの対象物を発見するための探索行為であるから，[26] 差押え対象となるコンピュータが既に発見されているにもかかわらず，その内部のデータを捜索することは，現行法上の捜索には当たらないと考えられる。

なお，認証情報は，IDとパスワードの方式によるものから，よりセキュリティの高い指紋認証，顔認証，虹彩認証など多岐にわたる。従来のIDとパスワード方式でなく，これら生体認証方式の場合には，いかなる手続きによって生体認証情報を取得し，それをログインのために使用することができるのかについてはさらなる議論が必要だろう。

ところで，クラウドコンピューティングは多くの場合，中央集権的なシステムを前提としている。ここにきて，ビットコインに代表される非中央集権的なシステムであるブロックチェーン技術が登場してきた。このpeer to peer（P２Pとも呼ばれる。）システムは，特定のサーバ上ではなく，ネットワークとして機能するソフトウェアの形態であり，そのシステムに参加するすべての者が少しずつシステムの機能の一部を担い，システムを運営・維持するという考え方である。[27] 中央集権的な管理者が台帳を管理するのではなく，ネットワーク全体で台帳を管理しているとみることができるので，「分散型台帳」と呼ばれることもある。分散型台帳は，現在，中央集権的に管理されている不動産登記や動産譲渡・債権譲渡の登記，株主名簿などに代替することは技術的には可能であろうとされている。[28] このブロックチェーン技術のもとでは，個々のコンピュータに取引台帳が保存されることになるので，分散型台帳のシステムが広く活用されるようになれば，個々のコンピュータを差押えることで取引台帳を差押えることができるので，ブロックチェーンに馴染むデータ

(25)　指宿信「押収済みパソコンを用いて検証許状に基づき海外メールサーバにアクセスした捜査に重大な違法があるとして証拠を排除した事例」新・判例解説Watch刑事訴訟法106・３（TKC，2016）。
(26)　宇藤崇ほか『リーガルクエスト刑事訴訟法』（有斐閣，2012）108頁。
(27)　斉藤賢爾「ビットコインというシステム」法とコンピュータ33・21（法とコンピュータ学会，2015）。
(28)　小出篤「『分散型台帳』の法的問題・序論-『ブロックチェーン』を契機として」江頭憲治郎先生古稀記念『企業法の進路』（有斐閣，2017）838頁。

については，リモートアクセスによる複写という問題は解消される可能性はあると思われる。[29]

2．リモートアクセスの代替としての検証の可否

上記のとおり，リモートアクセスは現在のクラウドコンピューティング環境のもとにおいては，手続きが煩雑で現実に即していないと考えられる。そこで，現行法の解釈によって，リモートアクセス以外の方法でそれと同等の捜査をすることが可能か検討してみたい。

一つ考えられるのが検証による方法である。検証は，対象の状態を五官により感得する処分である。これまでも，磁気テープ，磁気ディスク等の電磁的記録物を証拠として検証する必要性が高いことから，捜査実務上，これらを証拠化するにあたっては，差押えあるいは検証という方法によってその入力内容をプリントアウトしてきた。さらに，プリントアウト以外にも，入力内容のみを機械的に正確に転写することも（すなわち，データをコピーすること），五官の作用をとりあえず媒体の物（捜査機関の磁気テープ）に代替させるわけであるから，検証の一方法とされてきた。[30][31] リモートにアクセスする行為は，遠隔地のサーバ等の記録領域のデータを，情報通信技術を用いて可視化して認識し，保全する行為であるから，その性質上，[32] 検証にあたるといえる。

この行為について，検証の効力の範囲内とする考えは，被疑者のコンピュータに対する管理権を捜査に必要な一定の範囲で制限することを認めた検証令状の効力の範囲内のものであると考えられることから，アクセス先のサーバを目的物とする検証令状の発付を別途必要とせず，できるとする考えがある。[33]

また，遠隔地のサーバを一体と捉える考えもある。[34] この考えは，検証対象としてのコンピュータには，同一の管理者の管理に属し，オンラインで接続され，一体的に使用されている他のコンピュータをも含むと解する。しかし，令状には，処分対象の所在地が明示されているので，明らかに別の場所にあるものまでカバーしているとは言い得ない。[35]「必要な処分」（222条１項，129条）として，サーバへのリモートアクセスを認めることもできない。[36] もっとも，この点については，「…オンラインで接続され，一体的に使用されている他のコンピュータ及び記憶媒体」という令状であれば対応できる可能性も指摘されている。[37] アメリカやヨーロッパでは，目的とするデータを直ちに保全しないと改ざんや消去の恐れがある場合は緊急処分として許されると解されている。[38] 人の身体についての捜索や検証の場合に，対象となる人さえ特定されていればよいのと同様に，物についても所在場所で特定せずそれに変わる他の要因によって特定されていればよいと考え

---

(29)　ただし，ブロックチェーンの記録からあるアドレスとある記録を結びつけることができるとしても，当該アドレスと特定の個人や法人との結びつけをどのように立証するか等の問題が存在する。森下哲朗「FinTech時代の金融法のあり方に関する序説的検討」江頭憲治郎先生古稀『企業法の進路』（有斐閣，2017）813頁。

(30)　廣畑史朗「コンピュータ犯罪と検証」警論40・11・11（立花書房，1987）。

(31)　河上和雄「強制捜査の新展開」現代刑罰法大系５・192（日本評論社，1983）。

(32)　最判平成11・12・16刑集53・９・1327は，「電話傍受は，通話内容を聴覚により認識し，それを記録するという点で，五官の作用によって対象の存否，性質，状態，内容等を認識，保全する検証としての性質をも有するということができる」とした。

(33)　貴志浩平「ハイテク犯罪と捜査手続」捜査研究564・21（東京法令出版，1998）。

(34)　稲垣隆一「情報と捜査-捜査押収の対象について」多賀谷一照＝松本恒雄編『情報ネットワークの法律実務』（第一法規，1999）5028頁は，企業内LANなどのような閉鎖的ネットワークについては，当該LANに接続されたコンピュータを一体として対象にする捜索許可上の発付の可能性を肯定する。

(35)　井上正仁「コンピュータ・ネットワークと犯罪捜査（２）」法教245・52（有斐閣，2001）。

(36)　笹倉・前掲注(24)183頁。

(37)　井上正仁『強制捜査と任意捜査（新版）』410頁（有斐閣，2014）

(38)　井上・前掲注(35)55頁。

れば（コンピュータの場合はIPアドレスになろうが，データがクラウド上で分散配置されることを考えると特定のIPアドレスで特定をすることは難しく，「クラウドの文書サーバーのうち被処分者のIDを用いてアクセス可能な記憶領域」といった記載をする他ない。[39]），できる余地はあるともされていた。[40]

ただ，このような検証による方法を許すと，被疑者のコンピュータから遠隔地にあるサーバへのリモートアクセスのみならず，捜査機関のコンピュータから直接リモートサーバへアクセスすることも検証としてできることになりかねない。[41][42][43] そうなってくると，令状呈示の問題のみならず，差押えに付随しないリモートアクセスを認めることに等しく，時間的場所的制約がなくなり，リモートアクセスがしやすくなることは間違いなく，立法者が想定したリモートアクセスを巡る対立利益の権衡状態が崩れることになるだろう。[44] このような捜査手法について，ドイツにおいては，警察や公安調査機関が被疑者・調査対象者のパソコンに侵入ソフトなどを用いて秘密侵入し，データや通信記録を取得する「オンライン捜索」について，これを認めた改定法に対して違憲確認を求める憲法異議がされ，連邦憲法裁判所は2008年（平成20年）に「情報技術システムの秘密性と完全性に対する基本権」（IT基本権）なる新たな基本権概念を根拠に，当該権限付与規定が規範明確性・規範特定性を有しておらず，かつ比例原則の要請も充たしていないとして，違憲と判断している[45]ことが参考になろう。

また，リモートサーバには被疑事実とは無関係の大量のデータが保存されているため，検証のためには，被疑事実と関連するデータを検索し，これに該当するものを抽出して認識する必要も出てくる。この検索・抽出の過程は検証すべき内容を選別するためのものであって，検証そのものではなく，いわば「検証のための捜索」であるが，現行法にそのような処分を認める規定はなく現行法上は許されない。[46][47] 加えて，検証許可状により捜査機関は自由に被処分者の認証情報を使用する権限や，コンピュータを利用できる権限を取得するわけではない。[48] これは自動車を差し押さえたからといって，捜査機関が当該自動車を乗り回すことができないのと同じである。クラウドサーバ内にあるデータへのアクセス権限は利用者たる人とサーバ事業者との間の契約に基づいて，人である当該利用者に帰属しているものであって，物であるコンピュータを対象とする強制処分により捜査機関にその権限が移転するものではない。[49]

したがって，現行法上は，ネットワーク上のデータを取得するには218条２項に基づいてする他なく，

---

(39)　笹倉宏紀「サイバー空間の捜査」法教446・35（有斐閣，2017）。
(40)　井上・前掲注(35)52頁。
(41)　令状の呈示をどのように行うかという問題がある。事後通知や第三者の立会いで可能とする余地があるとするものとして，貴志浩平「ハイテク犯罪と捜査手続き」捜査研究564・21（東京法令出版，1998）。
(42)　なお，ウェブサイトなど誰でもアクセスできるものであれば，プライバシー侵害もないため，任意捜査としてダウンロード，保存することができると解される。
(43)　芝原・前掲注(23)577頁は，リモートアクセスの趣旨は，必要な情報が外部のサーバ等に保存されているため，パソコン等の差押えが空振りに終わる事態を避けることにあるとして，捜査機関による直接のリモートアクセスも理論上は許されてよいように思われると指摘している。
(44)　笹倉・前掲注(39)446・36。
(45)　植松健一・島大法学54・１＝２・204。
(46)　長沼範良「電磁的情報に関する捜索・差押え」現刑49・47（現代法律出版，2003）。
(47)　井上・前掲注(37)404頁では，捜索と検証とを組み合わせた処分の新設を提案する。
(48)　捜査機関が被処分者のコンピュータを使用して，データをプリントアウトする限りでは被処分者にも受忍の義務があるが（河上和雄「強制捜査の新展開」現代刑罰法大系５（２）・191頁（日本評論社，1983）），それを超えてネットワークで接続されたすべてのデータに捜査機関がアクセスすることまでを受忍する義務があるとはいえないだろう。
(49)　長沼・前掲注(46)49頁。

検証としてネットワーク上のデータを取得することはできないと解さざるを得ない。(50)

3．リモートアクセスの代替としての捜索・差押えの可否

ほかに，捜索による方法も考えられる。しかし，捜索は，差押え目的物を発見するための探索行為であるところ，リモートサーバ自体は差押え対象ではないのだから（差押えの対象はあくまで被疑者の管理下にあるコンピュータ），リモートアクセスをするために捜索するということはできない。

また，いったんコンピュータを差し押さえて認証情報を解析したあとに，再度の差押えをすることも考えられる。実務上，二重押収はしばしば行われているし，事件単位説に見られるように同一人についての複数の逮捕・勾留が競合することを許容していること，記録命令付差押えや差押えの代替的執行の方法においては，捜査機関が用意した「他の記録媒体」に情報を記録した上でその「他の記録媒体」の差押えという不自然な事態を法は認めていることから，差押え済みのコンピュータを再度差し押さえることの不自然さが際立つものではない。(51) 先の裁判例で捜査機関が検証令状を取得したのには，すでに差押えた物に対する再度の差押えができないと考えたからという事情があった。仮に差押え物の再度の差押えが可能であるとすれば，218条２項のリモートアクセスによる複写を許可した差押許可状を改めて取得して執行することができることになる。

しかし，差押えによりいったん占有が移転した物について，重ねて差し押さえることは想定されていない。そうだとすると，一度所有者たる被疑者に対して還付手続きをとり，その直後に差押えをするという方法を取らざるを得ないように思われる。ただし，このような方法は迂遠であるし，結局リモートサーバの情報を取得するという当初と同一の目的で差し押えることになるので，なるべく１回目の差押えの解釈運用で行える方が訴訟経済には資するだろう。

4．リモートアクセスによる越境コンピュータ問題

218条２項に基づくリモートアクセスによっても残るのが域外捜索の問題である。ネットワークは国境を超えて接続されているから，ネットワークで繋がったコンピュータは，所在地を問わずアクセスすることが可能であるため，リモートアクセスの対象となるコンピュータが国外に所在することがある。

外国において証拠を収集する方法には２通りあり，第１は，我が国の捜査官が外国において直接収集する方法であり，第２は，我が国の捜査官が外国に証拠収集を嘱託する方法である。もっとも，捜査は任意捜査であっても国家主権の行使であるから，我が国は外国の捜査機関の本邦内における捜査活動を原則として認めておらず，実務上は第２の方法で，国際共助の方法により当該外国の捜査機関に証拠収集を依頼するのが原則である。(52)

海外サーバに保存されているデータを取得するに

---

(50)　IDとパスワードを利用者個人に付与してアクセス権限を付与した場合である。設定によっては，フィルタリングすることで当該コンピュータからは誰でもアクセスできるが，それ以外のコンピュータからは誰であってもアクセスできないような権限を与える設定もできる。メールサーバや，クラウドサーバであれば，利用者個人にアクセス権限を付与する方式でアクセス権を与えることがほとんどであろうが，企業内LANであれば企業内LANに接続しているコンピュータにのみアクセス権限を与えているような場合である（IPアドレスフィルタリングやドメイン制限をすることで特定のコンピュータにアクセスを制限することができる。）。しかしこの場合においても「アクセス権限」があるのは，「当該コンピュータを利用する者」に与えられていると考えるべきであろう。物であるコンピュータにアクセス権限を観念し得ないし（権利主体として考えられないという意味であって，コンピュータの設定上は，どのコンピュータにアクセス権限を与えるかという形で権限が想定されている。），当該コンピュータを利用する権限があるのは利用者であり，利用者がアクセス権限を行使するにあたっては当該コンピュータが道具として必要にすぎないからである（いわば，居住者にとっての鍵のようなもの）。

(51)　笹倉宏紀「サイバー空間の捜査」法教140・34（有斐閣，2017）。

(52)　山内由光「国外における捜査活動」松尾浩也ほか編『実例刑事訴訟法Ⅰ』５頁（青林書院，2013）。

あたっても，国際捜査共助や司法共助の依頼を行い，その外国政府の司法当局その他然るべき機関によって当の処分を行うのが原則となろう。しかし，捜査共助[53]を依頼するには，捜査共助要請書を起案し，これを被要請国の言語に翻訳したり，被要請国がその国の言語で作成して送付してきた証拠書類を和訳しなければならないなど手続きが煩雑で，かつ，被要請国の適当な実施機関に書類が送付されるまでの事務手続に要する時間もあり，証拠が入手できるまで最短でも数か月を要することが多い[54]。データの場合，その間に証拠の隠滅や改ざんがされるおそれがあり，それが容易であることも先に指摘したとおりである。意図的な隠滅や改ざんでないとしても，事情を知らないサーバ事業者が期間等の経過によりデータを削除してしまうことも十分考えられる。多くのサーバ事業者では，ユーザがアカウントを削除すれば，即時又は一定期間経過後にデータが削除される仕様になっているし，長期間利用されない状態が続いていれば，データが自動的に削除されることもある。

差押え対象物たるコンピュータにネットワークで接続されている記録媒体が外国に所在する場合，これらに直接アクセスしてデータを複写することが，当該外国の主権を侵害するかについては，国際的に統一した見解があるわけではない[55]。

我が国が平成13年11月23日に署名した「欧州評議会サイバー犯罪に関する条約（Council of Europe Convention on Cybercrime）」（以下，「サイバー犯罪条約」という。）は，すべてのＧ７諸国及び欧州の大多数の国が署名するなど，事実上のグローバルスタンダードとなっている。同条約32条は次のように規定している。

> サイバー犯罪に関する条約32条（訳文）[56]
>
> 蔵置されたコンピュータ・データに対する国境を越えるアクセス（当該アクセスが同意に基づく場合又は当該データが公に利用可能な場合）
>
> 締約国は，他の締約国の許可なしに，次のことを行うことができる。
>
> a　公に利用可能な蔵置されたコンピュータ・データにアクセスすること（当該データが地理的に所在する場所のいかんを問わない。）。
>
> b　自国の領域内にあるコンピュータ・システムを通じて，他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし，コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。

他国の領域内にある記録媒体を218条２項によって，リモートアクセスをすることができるかは一概に述べることができず，他国の領域にあることが判明した場合には，サイバー犯罪条約32条に該当する場合を除いては，他国の主権との関係で問題を生じる可能性もあることから，この処分を行うことは差し控え，同意を取り付けるか，捜査共助を要請することが望ましいと考えられる[57]。

もっとも，データサーバの所在地はセキュリティ

(53)　平成29年度犯罪白書によると，平成28年度において捜査共助等を要請した件数は97件，受託した件数は79件である。
(54)　山内・前掲注(52) 9 頁。
(55)　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・５・1094（法曹会，2012）。
(56)　外務省，「サイバー犯罪に関する条約」，https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf（2013）。
(57)　サイバー犯罪条約草案では「越境捜索及び証拠押収を規律するための国際合意」という目的が掲げられていたが，採択された条約では，この目的自体が柔軟な表現に変えられ，一方的な越境コンピュータ捜索は完全に外されている。王志安「越境コンピューター捜索の法的地位―サイバー犯罪条約が残した課題―」駒澤法学３・３・３（2004）。

の関係で非公表とされるのが通常である。また，国内事業者であっても，高額な電気代を避けるために，国外にサーバを設置する事業者もある。多くの情報がリモートサーバに保存されるようになった現在においては，これらのサーバから情報を取得できないことは，捜査の実効性を著しく欠くことになるだろう。計画的な犯罪者であれば，すべてのデータは意図的に国外のサーバに保存するであろう。リモートアクセスは，自国の捜査当局が，他国の領域内に物理的に乗り込んで入った場面とは異なること，ネットワークを通じて対象サーバにその本来予定している動作をさせるに過ぎないこと，(58) サイバー犯罪条約32条も同意・承諾のない一方的なリモートアクセス捜査について沈黙していることからすれば，218条２項に基づいてリモートサーバへアクセスすることは必ずしも禁止されているものとは言えないと解される。

なお，米国では，連邦法執行機関が合衆国法典第18編第2703条に基づいて，マイクロソフトの特定の顧客のアカウントに関連するすべての電子メールおよびその他の情報を開示する令状の発付をニューヨーク州連邦地方裁判所に申請し，同裁判所の下級判事により令状が発付されたが，電子メールがアイルランドのダブリンにあるデータセンターに保存されていることから，マイクロソフトは令状取消しの申立てをし，これに従わなかった。これに関し，下級判事は，マイクロソフトの申立てを棄却し，第一審も，下級判事の理由と決定を支持した。しかしながら，控訴審は，本件開示要請行為は認められていない2703条の域外適用にあたるとして第一審の判断を覆した。そして，最高裁に上告されたが，上告中にクラウド法が成立し，データが米国内外にあるかを問わずに開示ができる旨改正され，立法的に解決されている。(59) 我が国でも，域外適用に関する早期の立法を行う必要があろう。

第６　まとめに代えて

本稿では，リモートアクセス改正に伴い，実際のリモートアクセスによる複写における問題点について検討し，いくつかの法的課題の例を挙げてみたものである。本文でも指摘したとおり，立案当時に比べるとクラウドコンピューティングの利用が浸透したため，リモートアクセスの条文が現実のクラウドコンピューティングの利用形態に合致しない，又は，議論が棚上げにされたままの状況が生み出されているとの感を否めない。本稿はあくまで序論程度の問題提起にとどまるが，今後さらに研究を進めてまいりたい。

以上

（58）　貴志・前掲注(33)21頁。

（59）　United States, Petitioner v. Microsoft Corporation Supreme Court Of The United States No17-２（April 17, 2018）