資料紹介

インターネットにおける犯罪と刑事訴追

――2012年第69回ドイツ法曹大会刑事法部会（ミュンヘン）――

Straftaten und Strafverfolgung im Internet

――69. Deutscher Juristentag 2012 München――

加藤克佳＝辻本典央

Katsuyoshi Kato / Norio Tsujimoto

はじめに

第69回ドイツ法曹大会が，2012年９月18日から21日まで，ドイツ連邦共和国・ミュンヘン市の国際会議場で開催された（http://www.djt.de/die-tagungen/69-deutscher-juristentag/）。同大会は，ドイツを中心とする法曹約2,500名から3,500名が参加する大規模な学会である。紹介者両名は，会員としてこれに参加する機会を得て，主に刑事法部会に出席した。同部会のテーマは，「インターネットにおける犯罪と刑事訴追（Straftaten und Strafverfolgung im Internet）」であった。まさに、グローバル社会における刑事法分野での時代を反映するテーマが扱われたといってよい。鑑定意見書は，この課題についてのドイツの第一人者である *Ulrich Sieber*

教授（マックス・プランク外国・国際刑法研究所所長〔フライブルク〕）が執筆した。また，刑事法部会の議長は，高名な刑事弁護人である *Gunter Widmaier* 教授（カールスルーエ／ミュンヘン）が務める予定であったが，不幸にも急逝されたため，副議長の *Helmut Satzger* 教授（ミュンヘン大学）が議長を務めた。副議長は，*Ingeborg Tepperwien* 博士（元連邦通常裁判所裁判長〔ベルリン〕）であった。

このテーマは、国際的な広がりを持ち、かつ最も現代的な問題の１つでもある。特に，従来の刑事法学の諸原則との関係が正面から問題となるため，日本でも、本格的な研究が必要不可欠であり、かつ、それが極めて有益であることはいうまでもない。同大会では，慣例に従い，追って討議録が公刊される予定であり(1)，これを踏まえて分析・検討を行うのが適当であろう(2)。とはいえ，鑑定意見書等の公刊物や部会での報告・討議などからすでに一定の知見を得ることが可能であり，日進月歩の進展を見せている本テーマを，たとえ一部であっても翻訳・紹介することが時宜に適っているといってよい。そこで，本資料では，そのうち重要な柱となる「提言」（鑑定意見をはじめ，いずれも要旨である）および「決議」を紹介し，あわせて，関連文献の翻訳を付加することとした。法曹大会の際には，これを契機として多くの関連論稿が公刊されるのが通例であり，今回も同様であったが，その中でも参考となると思われるものを選択した。もとより，詳細な検討は他日を期することとしたい。

なお，本翻訳は，ドイツ刑事法学研究会（代表・加藤克佳〔名城大学法学部・大学院法務研究科教授〕）によるプロジェクトの一環として公表す

---

(1)　*Deutscher Juristentag* (*djt*), Verhandlungen des 69. Deutschen Juristentages München 2012, Bd Ⅱ/1: Sitzungsberichte—Referate und Beschlüsse, 2013, Bd Ⅱ/2: Sitzungsberichte—Diskussion und Beschlussfassung, 2013.

(2)　書記による記録として，*Dominik Brandowski*, JZ 8/2013, 401 ff. がある。

るものである。

（加藤克佳記）

第1部　刑事法部会の提言

Ⅰ．鑑定意見（*Ulrich Sieber* 教授。マックス・プランク外国・国際刑法研究所所長〔フライブルク〕）―「インターネットにおける犯罪と刑事訴追」

in: Deutscher Juristentag (djt), Verhandlungen des Deutschen Juristentages München 2012, Bd I : Gutachten/Teil C: Straftaten und Strafverfolgung im Internet, 2012.

1．総　論

情報社会の出現に対する法の対応は，多くの犯罪の広い領域と，様々な法域を対象とする。関連するルールは，現代社会が情報技術システムに強く従属し，またひどく傷つきやすい（敏感である）ことからも，大きな意義を持っている。

これに伴って必要となる情報刑法の発展は，刑法以外の（技術的，組織的，人的）解決の優先性，および，それらの実効性がしばしばより高度のものであることを，考慮しなければならない。法的規制に際して考慮されるべきであるのは，特に，情報の非物質的な性質，情報領域の国際的な性質，インターネットの匿名性，情報技術の素早い変化といったものである。これらの点は，技術に固有の規定ではなく，機能的な規定によって考慮されなければならない。インターネット犯罪に対する法的規制は，国際的な装置によって強く打ち出されている。この基準の考慮は，国際的な協力を機能化するために重要である。

ドイツ刑法は，すでに多くの改正措置によって，情報社会の新たな要請と情報技術に適合するに至っている。しかし，新たな領域においてはいまなお，情報法上の問題が，物的対象に関して展開されてきた法規定について生じている。ここでは，相当な改正が必要となっている。国際的サイバースペースにおける非物質的客体に関する新たな現象に特に対応した規定によって，規制の実効性も，市民の自由・人格の保護も，相当に改善されうるであろう。現在の改正の必要性，素材の技術的複雑さ，問題の素早い変化，規定が強く国際的な関連性を持つことなどを考えると，ドイツ法の新たな展開のために，（1980年代に類似して）学際的かつ国際的に構成された専門委員会が設置されるべきである。（そのような委員会の設置いかんにかかわらず）将来の改革作業のために，以下の準則を推奨する。

２．実体刑法

ａ）実体刑法では，情報技術システムの秘密保護・不可侵性・使用可能性に向けられたドイツの関連刑罰規定（特に刑法202ａ条，202ｂ条，202ｃ条，303ａ条，303ｂ条）を，体系的に整備しなければならない。

- ●情報の不正アクセスと不正使用の構成要件（刑法202ａ条，202ｂ条）は，１つにまとめて，そこに，内密情報の無権限使用の類型を補充すべきである。
- ●情報改ざんとコンピュータ破壊の構成要件類型（刑法303ａ条，303ｂ条）は，１つの構成要件にまとめ，損害を与えたという統一的要素によって限定すべきである。
- ●前領域の構成要件（刑法202ｃ条，263ａ条３項，303ｂ条３項，同５項）も，同一の行為客体による共通の犯罪構成要件として，新たに規定すべきである。もっとも，前領域の理論的基礎づけが異なることから，２つの異なる「道具方式」を区別すべきである。第１は，

コンピュータ・プログラムである。これは両面的な使用機能を有しており，それゆえに，所持者の犯罪意図がある場合に限り，可罰性を基礎づけうる。第2は，他者の保安コードである。それを不法に所持することは，前述のような意図的要素がなくても，可罰性を基礎づけうる。

このようなかたちで創出される不正アクセスの3つの犯罪構成要件，つまり，無権限のシステム改ざん，危険な道具および保安コードの所持および準備については，類似の加重構成要件を付加すべきである。これに加えて，組織的・営業的な実行，情報システムへの大きな侵害，相当規模の損害が惹き起こされた場合には，刑訴法100ａ条〔通信傍受〕，100ｇ条〔流通情報の収集〕による捜査措置も可能とされるべきである。関連する犯罪（現在，刑法の3つの章8つの条項に分かれて規定されている）は，1つの法律にまとめるべきである。

ｂ）情報保護法の刑罰規定は，やはり，体系化と統一化が必要である。情報保護刑法の核心領域は，中核となる刑法に定めるべきである。現在欧州連合レベルで議論されている行政的制裁は，ドイツの刑法および秩序罰規定に統合すべきである。しかし，行政的制裁および特にその手続法の法治国家的な保護は，その重さの従属性およびドイツ憲法との適合性において，刑法上の保障に合致したものでなければならない。

ｃ）著作権刑法は，実務において，組織的および営利的に行為した犯罪者に集中されなければならない。民事法上の保護システムは，執行の不十分さを是正するために，著作権法101条の回答請求権（Auskunftanspruch）の領域において改善されるべきである。その際，真正の蓄積データを必要とすることなく，権利者に各々の利用回線へのIPアドレスの割当てを容易にさせる手続も検討されるべきである。ドイツ

で現在議論されているTwo-Strikesモデルや，イングランドとフランスで実用されているThree-Strikesモデルは，少なくともその現在の形式においては，推奨されるべきものではない。

d）コンテンツ犯罪について決定的である伝統的かつ物的な情報媒体に適合した刑法11条3項の文書概念は，メディアの概念に置き換えるべきである。これは，情報媒体ではなく，関連する情報に着目する概念である。その際，所持の概念も，明確にされなければならない。多くの実行行為が重なり合うために複雑となっているポルノ構成要件は，1つにまとめる必要がある。少年保護刑法においては，可罰的コンテンツの評価は，現在のように，それが物理的媒体に記録されているのかまたはインターネットで流布されているのかという点に，左右されるものではない。

3．刑事訴訟法

刑事訴訟法は，特に，相当な範囲でまだ物的な証拠を対象とした介入権限の領域において，改正を必要とする。まとめると，以下のとおりである。

a）端末情報コミュニケーションを監視するための特別の規定。これは，技術的および法的な措置によって電話以外のコミュニケーションへのアクセスをできる限り排除し，誤って刑訴法100a条を根拠に実用されてきた，現在は憲法違反とされる「端末電話傍受（Quellen-TKÜ）」を可能にさせるものである。

b）捜索のための法的明確化。これを公然の措置として定義し，これによって，特にE-Mailプロバイダにおける継続的または隠密的な監視を，電話傍受の条件の下でのみ許すものとする。

c）情報の提出義務に関連する法制化。これは，物的客体と比較した場合の非物質的客体を提出することの特殊性を考慮したものである（例

えば，印刷，情報解読，協力といった義務)。

d）流通している情報および（拡張された）手持ちデータに対する特別の提出義務。これは，迅速なダウンロード手続において特定 IP 番号の利用者を同定することも含んでおり，連邦憲法裁判所より認められた経過期間内に創設しなければならない。

e）コンピュータ情報およびデジタル端末機の暗号解読および保護解除のための特別規定（特に開示義務と解読命令)。

f）情報の暫定的な保全のための要急手続（緊急保全)。

さらに，情報へのアクセスとその証拠としての使用のために，推奨を発展させ，刑事手続及び過料手続のための準則に導入することもできるであろう。一般的な専門教育，捜査機関および司法の特別機関の設置，ならびにそれらの協働（外国機関との関係も含めて）は，さらに強化すべきである。

4．危険への準備と予防

a）現在議論されている情報蓄積に関しての一般的推奨は，本鑑定意見の範囲では不可能である。問題がここでのテーマを大きく超えるからである。現在のところ，一般的な推奨を行うには，十分な情報基盤が欠けている。

しかし，インターネット上の解明のため本質的な情報の領域（各利用者への IP 番号の流動的付与を含む）は，明確かつ速やかに決定しなければならない。このような（介入程度の弱い）情報蓄積は，インターネット犯罪の解明のため大きな意義を持つため，流通情報および蓄積情報の「大蓄積」に関する裁判例にかかわらず，できる限り速やかに規定すべきである。

b）特定のインターネット情報を遮断するための義務づけは，否定すべ

きである。その代りに，不法な情報をその根源において消去すること，および，その著作者の捜索に向けた手続を，発展させるべきである。その際，国際的に張り巡らされたインターネットにおける住民登録も，求めるべきである。これは，不法なコンテンツに関する相応の届出をそれが蓄積されたホスト・プロバイダに転送し，プロバイダに，刑罰予告の下で関連する責任規定に基づいて情報消去を行わせるものである。

５．国際協力

インターネット犯罪の刑事訴追は，特に国内刑事訴追システムの国際的協力を必要とする。この協力を改善するために，特に以下の措置を採り入れるべきである。

ａ）国内の実体刑法および刑訴法を，地域間および国際組織間で調整すること。

ｂ）職務・司法協力のための国際協定，ならびに，インターネットに固有の国際的な捜索を許可するための国際法上の条約の締結（そのような条約がなければ，他国の主権を侵害することになる）。

ｃ）コンピュータに特殊な協助法の展開と，刑法上の協力に向けた国際的および超政府的な制度を創設し，国際的サイバースペースにおける常設的な執行権限を，そこに委ねるべきである。

Ⅱ．報　告

その１（*Constanze Kurz* 氏。カオス・コンピュータークラブ情報科学部門研究員〔ベルリン〕）

「インターネット犯罪」の概念の使用は，基本的に，検討し直すべきである。自動車犯罪，出版犯罪，信書犯罪，電話犯罪といった概念も使用に

耐えないものであるから，マスメディアおよびインターネットのような複雑な技術のシステムが犯罪現象の固有類型として特化しなければならない理由はない。

1．技術的監視

あらゆる電子的コミュニケーションの全体にわたる監視，フィルタリング，規制を導入する技術はある。例えば，シリア，リビア，サウジアラビア，白ロシアにおける実践的な投入から，現在のシステムの機能範囲と有効性が示される。

私たちが将来このような技術的に監視される国家で生きていくか否かの決定は，政策的および法律的レベルで行われるべきものである。

いったん監視およびフィルタリング権限が認められたならば，これに対する法律上および議会による規制は，おそらく十分に機能しないであろう。裁判官留保は技術的監視措置に対する実際の審査にあまり役立たないものであることは，以前から証明されている。

ネット網のフィルタリングおよび規制に向けられた著作権産業界からの要求は，いったん形成された技術的なインフラの利用の典型的な拡張に関する一例にすぎない。

法治国家の制度は，このような技術的な権力手段の規制に適したものではない。法治国家の基礎である民主的・政策的意思形成は，まさしくそのような技術的システムによって弱体化し，さらに廃止されるおそれがあるからである。

2．国家による諜報ソフト

国家によるトロイの木馬投入に際しての法的・技術的問題は，このような侵入的手段にかかわる捜査機関側からの要求が基本的に過剰であること

を示す。

トロイの木馬のような損害を与えるソフトの使用は，基本的に放棄すべきである。このような侵入的な技術的諜報手段を使用するならば，得られたデータの証明力，エクスプロイト〔訳注：コンピュータ上のソフトウェアの脆弱性に対する攻撃〕の意図的な創出，さらにエクスプロイトとの取引による闇市場の間接的な支援といった点に関して，パンドラの箱を開けることになる。私的生活形成の核心領域に強力かつ日常的な介入を受ける危険は，そのような諜報的道具が使用されるときには，非常に大きなものとなる。

それでもなお，重大犯罪のわずかな例外に関してそのような危害的ソフトを使用するべきであるというならば，「大盗聴」に関する規定を類推して行う「端末電話傍受」に際しても，そのような手続が行われる数を，厳格な法的条件によって限定すべきである。

対象者への通知は，そのような諜報的ソフトを使用した場合には常に，例外なく，遅くとも3年後には行われるべきであり，その際には，ソース・コードおよびバイナリ・コードへのアクセスも含まれるべきである。

端末電話傍受が実施されるときには，システムから得たデータの使用は許されない。侵入を受けたコンピュータ上でのトロイの木馬によるデータ操縦，ないしこれによって生じるエクスプロイトは，この点で排斥されないか，ないしは裁判で証明されるべきものではないからである（二重の使用禁止）。このことからは，「端末電話傍受」が実施されるか，または，差し押さえられたシステムからのデータの使用が計画されるとしても，双方の捜査手段の組合わせは許されない。

トロイの木馬のプログラミングおよびインストールは，基本的に，国家機関が自己の責任で行うべきである。外部発注は，ドイツではその提供者が数少なく，一部では疑わしい過去をもち，支配権限における日常的な業

務上の接触があることを考えると，支持できる選択肢ではない。

使用されるトロイの木馬は，独立機関から単独で審査され，保証を受けるべきである。これによって，少なくとも欠陥または過失による動作範囲の逸脱を最小化しなければならない。

トロイの木馬が機能するための充電機能は，基本的に許されない。

情報技術システムおよびインターネット領域での技術的に複雑な刑事法上の捜査は，明確かつ厳密な規定と，「毒樹の果実理論」の導入を要求する。これによって，許される捜査手段から得られた証拠だけが使用されるようにするためである。

その２（*Armin Nack* 判事。連邦通常裁判所裁判長〔カールスルーエ〕）

情報技術システムへのアクセスに関する現在の刑事訴訟上の介入権限は，技術に依存するものであるために，情報技術の目覚ましい発展にもはや追いついていない状況にある。したがって，そのような介入権限は，もはや介入の各技術に適合しないものとなっている。

技術に左右されない規定を優先すべきである。これは，連邦憲法裁判所の審査基準と一致して，基本権侵害の態様および程度に沿ったものである。各論の前に，総論として，４段階の保護範囲が定義される。①最も強い基本権侵害としての核心領域，②次に強い基本権侵害となるコミュニケーション内容，③間接的な基本権侵害となるコミュニケーション状況，④証言拒否権による保護，である。

保護領域が重要なものとなるほど，裁判官の留保を厳格に適用すべきである。核心領域および証言拒否権への介入が問題となるときは，合議制裁判所による。その他の場合は，単独裁判官（但し，３年以上の経験者）の管轄である。検察官の要急命令権限は，コミュニケーション状況への介入に限る。

独立した補充性条項は，刑法62条の定評あるモデルに従い，比例性原則という一般規定に置き換えることができる。この場合，各々の技術状況に合わせた基準を展開することは，裁判所の任務である。

各論として，法的保護は，介入の程度に応じて区別して規定されるべきである（刑訴法101条参照）。そこに含まれるのは，特に通知義務，そして少なくとも裁判官留保，証拠使用の規定，上告裁判所による規制である。

現在の介入命令に要求される詳細な理由づけ要件を法律に記述することが有効であるか否かも，検討の必要がある。いずれにせよ，憲法裁判所の基準が考慮されなければならないからである。

その３（*Jorg Ziercke* 氏。連邦警察局長官〔ヴィースバーデン〕）

１．サイバー犯罪の現象

「現実世界」の犯罪実行形式は，次第に，同様または匹敵するかたちで「仮想空間」でも見られるようになっている。仮想空間においても，警察は，危険阻止および刑事訴追という国家任務の目的において，現実と同様に活動的で，同様の対応ができるのでなければならない。

「サイバー犯罪」の現象領域は，特に営業的・組織的な態様で実行される限りで，個別の市民と，国家およびその施設に対する相当な潜在的危険をはらんでいる。このような危険と害悪は，技術的および社会的発展ゆえに，今後ますます大きくなっていくであろう。

サイバー犯罪の実際の規模は非常に不明な部分が多いことを考えると，害悪を厳密に見積もることは不可能であるとしても，次のことは確かである。インターネットは，犯罪者に，無数の潜在的な被害者と攻撃点を「与える」ものである。したがって，サイバー犯罪は，必然的に高度の潜在的な害悪を持った犯罪領域であり，今後もそれは変わらない。

それゆえ，行為者に視点を合わせ，そこに到達し，刑事訴追の隙間をな

くすために，国家は，法的，技術的，戦術的に戦力を高めていかなければならない。そうでなければ，国家の保護義務および刑法上の訴追権限の遂行という，場合によっては政治的問題が沸き起こるであろう。

2．実体刑法と刑訴法100ａ条のカタログ

「盗まれた」デジタルIDの取引は，現行法上の伝統的な盗品関与の構成要件を満たさない。この点で，現実世界と仮想世界とは，処罰においても，十分に同調するものではない。近年初めて司法大臣会議（Justizministerkonferenz）から推奨されているような，「データ故買」の規制に向けた発議は，この処罰の間隙を埋めるために，連邦警察局の立場からも追求すべきものである。また，営業的・組織的実行の場合には，通信傍受の機会も認められるべきである。

仮想空間で実行された犯罪については「現実の犯行場所」が欠けるため，通信傍受は，しばしば「現実時間」における唯一可能な捜査手段である。したがって，特に情報技術システムの信頼および不可侵性に対するあらゆる重大犯罪（刑法202ａ条，202ｂ条，202ｃ条，303ａ条，303ｂ条）に関しても，通信傍受の機会が開かれなければならない。

Sieber 鑑定意見で述べられているような，前述を超える犯罪構成要件および法定刑を改善するための提案は，連邦警察局の視点からは支持できるものである。しかし，それは，インターネット犯罪の現象領域における犯罪の訴追に適した必要かつ要請される権限が刑事訴追機関において欠けている限り，効果はないままであろう。

3．通信コミュニケーションにおける暗号化，端末電話傍受

利用が増加している暗号化された通信機会によって刑事訴追を免れる範囲を生じさせないためには，警察は，伝統的な通信傍受に関する相応の調

整措置を必要とする。ここでは，成果が見込まれる捜査手段（端末電話傍受）の利用が，重大犯罪に際して許されるべきである。

連邦警察局法（BKAG）201条2項には，すでに，インターネット・テロの危険回避（連邦警察局法4ａ条）の範囲で，端末電話傍受に関する厳密な権限が定められている。すでに各州の検察官の事件指揮権限の下，捜査手続においても，刑訴法100ａ条，100ｂ条により，裁判官の命令に基づいて端末電話傍受処分が実施されている。しかし，特に端末電話傍受に関する厳密な権限規定が必要であると思われる限りで，連邦および州における統一的な取扱いおよび法的安定性の理由から，刑訴法において相応の法的明確化を迅速に図らなければならない。

4．データのコード化，オンライン捜索

暗号化された通信の傍受の状況（端末電話傍受参照）以外に，対象者の側でのデータの暗号化ないしコード化（例えば，コンピュータのハード・ディスク領域のコード化）は，治安機関に，技術的な問題を提起する。個別事例においてコード化されたデータが端緒ないし証拠として利用できるようにするために，それ以外の機会はないことから，ここでも，オンライン捜索の捜査手段が成功を見込まれるであろう。前述の状況において，オンライン捜索（すでに連邦警察局法20ｋ条において，同法4ａ条による危険回避のための措置として規定されている）は，差押えの前段階において，すでにパスワードやアクセスコードなどの取得に役立ちうる。これによって，後のデータの使用が可能となる。しかし，オンライン捜索に関する憲法裁判所の判例（2008年）に照らして，介入の程度および手続の保全を考えると，特に高度の要件を設定すべきである。

5．蓄積（最低保存期間），瞬間凍結，保管命令

インターネットまたはその他の通信手段を用いた犯罪にかかわる犯罪者を，現実社会における犯罪者と同様に効率的かつ実効的に訴追できるために，データ保全に関する欧州連合準則（最低保存期間）を，憲法裁判所の基準に照らして早期に具体化することが必要である。

ホットスポットや公衆のIPsなどを通じたインターネット利用の新たな可能性に基づいて，義務づけがなされなければならない。したがって，この手続に際しても，利用者について，必要な場合には遡って訴追することが可能となる。

緊急凍結は，「蓄積データ保全措置」に代替するものではない。もはや蓄積されていないものを凍結することはできないからである。

「蓄積データ保全措置」を補充するものとしてなら，緊急凍結手続は，警察の措置にとって助けとなりうる。特に長い上訴期間に際して流通データの喪失を回避するために，保存命令に関する欧州理事会サイバー犯罪協定の第16条の規定が，国内法において具体化されるべきである。

これは，国際的な協力がなお効率的であることを示す例である。その基礎は，ここでも，国内の実体刑法および手続法の調和（Harmonisierung）である。

6．電話業者と電気通信事業者との限界の消去

新たな技術的展開によって限界はおよそ消え去っているから，電話事業者を電気通信事業者よりも優先的に保護することは，もはや正当化されない。コミュニケーションは，実際に，電気通信事業者を通じて行われることが増えている（例えば，SMS の代わりにソーシャルネットワークが利用されるなど）。したがって，存在し，流通し，利用されているデータの蓄積および加工の観点において，電話事業者と電気通信事業者との対等化

が必要である。

７．おわりに

最後に，ドイツ法曹大会は，叙述された現実に存在する可罰性および訴追の間隙を，自由と治安の緊張領域における利益の相当な考慮においてもなお甘受できるものと考えるべきであるか否か，という問題を提起しておきたい。

第２部　刑事法部会の決議

Ⅰ．総　論

１．現代社会が強く情報技術システムに依存しており，かつそれは脆弱なものであることからは，技術的な対応だけでなく，刑事法上の対応も必要である。現在の刑法上および刑事訴訟上のシステムは主として物質的な対象に合わせられており，非物質的なデータに適合しないものであるから，このような状況に基本的に適合させることが必要である。可決（賛成70：反対４：保留１〔以下，この順で数を挙げる〕）

２．その際，非常に素早い情報技術的な変化を，考慮に入れなければならない。それは，個別の技術に応じた規定によって成就されうるものではなく，機能および結果に即した規定が必要である。可決（64：５：11）

３．インターネット刑法の領域において多くの改革が必要であることから，素材の複雑さ，素早い技術的な発展，多様な国際的関連性，犯罪学上の研究の必要性といった理由から，学際的に構成された専門部会（立法者に助言を果たすべきもの）を設置すべきである。可決（71：１：７）

Ⅱ．実体刑法

1．従来は分散して規定されていた「情報に関連する」刑罰規定（情報技術システムの信頼性，不可侵性，利用可能性を保護する）は，特に前領域の行為を考慮したうえで（特に刑法202ａ条，202ｂ条，202ｃ条，303ａ条，303ｂ条），１つにまとめ，統一化し，体系的に整備して規定すべきである。可決（63：２：11）

2．重大かつ多面的な攻撃に関して，より重い法定刑を備えた加重構成要件を創設すべきである。同時に，この加重規定に際して，刑事訴追機関のための幅広い捜査手段（特に電話傍受）を創設すべきである。可決（53：12：12）

3．ａ）インターネットにおける秘密・情報保護に関する処罰の間隙をなくすために，新たな犯罪構成要件として，「データ故買罪」を導入すべきである。可決（45：16：19）

ｂ）「データ故買罪」構成要件は，もっぱら適法な業務または職業上の義務の履行のため行なわれたデータの入手を除外したものとすべきである。可決（53：９：18）

4．刑法典は，いくつかのコンテンツ犯罪に関して，伝統的な，物質的データ媒体に即した文書概念を用いている（刑法11条３項）。文書概念は，情報媒体ではなく，関連するコンテンツに焦点を合わせた規定に置き換えるべきである。同様に，文書に即した所持概念は，コンテンツに特殊な表現に置き換えるべきである。可決（61：10：７）

Ⅲ．刑事訴訟法

1．立法者は，インターネット犯罪が市民および国家ならびにその施設に対して有する高度の潜在的危険を，適切に考慮しなければならない。法治国家原理は，機能的な刑事司法に向けた利益の考慮を要求する。実効的

な刑事訴追に必要となる捜査手段および技術的な機会を刑事訴追機関に与えないままおくことは，この要請に反する。可決（45：24：10）

2．既存の技術を電子コミュニケーションの広範な監視，フィルタリング，規制のため使用することは，極めて抑制的に行うべきである。監視・フィルター権限がいったん付与されたならば，それは，司法および議会による実効的なコントロールから引き離されることになる。否決（17：50：12）

3．刑事訴訟上の監視・規制手段は，各々の介入の程度に応じて，比例性の範囲内で許容されうるものである。そのためには，立法者がこの介入をもはや物質的な証拠対象を指向するのではなく，機能に即して規定し，そのための条件を明確かつ詳細に定めることが必要である。可決（56：4：18）

4．現在の技術状況から，特に以下の重要な（抑止的）手段に関して，立法者は，法的明確性を作り出すべきである。

a）端末電話傍受

aa）抑止的な端末電話傍受を行う目的で情報技術システムに密かに侵入することは，たいていは技術的に困難な電気通信の監視に対する代替手段として，刑訴法100a条，100b条の条件に準じて可能とすべきである。可決（45：28：4）

bb）その手段のため投入されるソフトは，事前に独立して（例えば，情報保護に関して任命された者により）検定されなければならない。これによって，技術的および法的な条件を遵守し，このソフトの投入に不可避の危険を規制することを確保するためである。可決（57：11：11）

cc）個別事例で，情報保護に関して任命された者に常に事後報告するという，法的義務を課するべきである。否決（27：41：11）

b）オンライン捜索

aa）抑止的なオンライン捜索を行う目的で情報技術システムに密かに侵入することは，蓄積されたデータの暗号化の可能性に鑑みて，重要な捜査手段であり，それゆえ，憲法上の切実な介入に当たるとしても（BVerfGE 120, 274），許容されるべきである。可決（47：27： 5）

bb）その手段のため投入されるソフトは，事前に独立して（例えば，情報保護に関して任命された者により）検定されなければならない。これによって，技術的および法的な条件を遵守し，このソフトの投入に不可避の危険を規制することを確保するためである。可決（57：13： 8）

cc）個別事例で，情報保護に関して任命された者に常に事後報告するという，法的義務を創設すべきである。否決（27：44： 7）

c）接続データおよび（拡張された）在庫データに関する特別の引渡し義務を創設すべきである。これによって，技術的に可能な限りで，必要な場合にはその利用者を追跡することが可能となる。可決（52：13：11）

d）蓄積データの保存

電気通信事業者は，一般的にかつ憲法上許される限りで，欧州連合蓄積データの保存準則（RL 2006/24/EG）の基準に従って，一定の接続データを収集し，最低 6 か月間は保存するよう，義務づけられるべきである。可決（42：32： 4）

Ⅳ．国際刑法

1．インターネット犯罪は，国内領域にとどまらない。

a）インターネット犯罪に独自に対処するための執行権限を備えた，国際機関を創設すべきである。否決（ 8 ：56：14）

b）国際的なインターネット犯罪を実効的に撲滅するために，インターネット上の国際捜査を他国の同意を必要とすることなく可能とさせる，国

際法上の条約を締結すべきである。可決（33：29：14）

２．刑罰適用法の伝統的な原則によると，インターネット上では，複数の（場合によっては矛盾する）刑罰規定が適用されることが生ずる。〔この〕齟齬を避けるために，インターネット犯罪に関係する，各国家の重要な犯罪構成要件を（国際組織の範囲で）強く調和させるべきである。可決（67：４：４）

第３部　関連文献

ハンス・クートリッヒ「インターネットにおける犯罪と刑事訴追――2012年第69回ドイツ法曹大会刑事法部会の鑑定意見について――」*

Hans Kudlich, Straftaten und Strafverfolgung im Internet—zum strafrechtlichen Gutachten fur den 69. Deutschen Juristentag 2012, StV 9/2012, S. 560–566

A．はじめに

ライプツィヒで行われた前回の刑法教員大会（刑法学会）における２つの報告と同様に(1)，2012年にミュンヘンで行われる第69回ドイツ法曹大会の刑事法部会も，「刑法とインターネット」の問題に取り組む。「インターネットと刑法」に関する議論は，ほぼ15年前に少なくとも幅広い基盤において始められ，20世紀の終わりにその最初の頂点を迎えたうえで，いくつかの異なるモデルを示している。この議論は，いくつかの点ではっきりと

---

* 紹介者らは，翻訳を快諾いただいたクートリッヒ教授に謝意を表する。

(1)　この点について参照，*Schmölzer* und *Klesczewski* in ZStW 113（2011), 709 ff. bzw. 737 ff.

収束した。例えば，すでに15年前に法的に規制された[2] プロバイダ責任の問題や[3]，国際刑法に関する問題についてである[4]。しかし一部では，この間に議論が高まり，重要となったものもある。それは，特に（そして近年に至っても）刑訴法の領域にいえることである[5]。そこでは特に，インターネット技術の普及が，一方で，刑事訴追機関によるその技術の投入が増加し，そして他方で，容疑者もこの技術を使用することが（相応の伝達機会・必要性を伴って）増加するという事態を導いている。

これを背景に，ドイツ法曹大会がフライブルク・マックスプランク研究所の所長 *Ulrich Sieber*（彼は疑いなくこの領域の第１人者の１人であり[6][7]，特に情報法の先駆者でもある[8]）を鑑定意見者として得ることがで

⑵ この点でドイツにおける最初の規定化は，電話サービス法（TDG）により行われた。これは，基本的に1997年に施行された情報・コミュニケーションサービス法（BGBl. I, S. 1870 ff.）の一部であった。

⑶ 電話サービス法における当初の規定について特に参照，*Sieber*, Verantwortlichkeit im Internet, 1999. さらに多くの文献の中でも参照，*Bleisteiner*, Rechtliche Verant-wortung im Internet, 1999; *Finke*, Die strafrechtliche Verantwortlichkeit von Internet-Anbietern, 1998. アクセス仲介者の答責性という特別の問題については次も参照，*Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsprovidern (...), 2003.

⑷ 当時の議論について参照，*Cornils*, JZ 1999, 394 ff.; *Hilgendorf*, NJW 1997, 1873 ff.; *Schwarzenegger*, ZStR 118 (2000), 109 ff.; *Sieber*, NJW 1999, 2065 ff. 詳細かつ包括的な文献として，*Körber*, Rechtsradikale Propaganda im Internet-der Fall Töben, 2003, S. 131 ff.; ならびに *Lehle*, Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet, 1999; BGHSt 46, 212 (Töben). 同判決については次の評釈もある。*Hörnle*, NStZ 2001, 309 ff.; *Kudlich*, StV 2001, 397 ff.; *Lagodny*, JZ 2001, 1198 ff.

⑸ 例えば次もみよ，*Sieber*, Straftaten und Strafverfolgung im Internet-Gutachten C zum 69. Deutschen Juristentag, 2012, C 63.

⑹ 筆者は，1995年から2000年に（厳密には，私が2002年９月にブッツェリウス・ロースクールで最初の講座を受け持つまでのほぼ10年間）当時鑑定人がヴュルツブルク大学に在籍していたときの講座の助手であったため，この評価は「仲間うち」のものに過ぎないとの批判を回避するために，彼が私の学問上の先生↗

きたのは，喜ばしいことである。鑑定意見も，印象的な内容のものとなっており，刑法とインターネットのテーマに関する非凡な概観を提示するものである。本テーマは，以前の〔第68回〕法曹大会で鑑定意見者を務めた（それゆえに，ドイツ法曹大会の条件と圧迫を委ねられた）筆者を唖然とさせるほどの広がりで扱われ，刑法理論上の叙述に加えて，多かれ少なかれ詳細な実証的犯罪論，比較法，そして法政策的な部分を含むものとなっている(9)。

B．実体法および手続法の対象としての「情報」

「インターネットにおける」犯罪と刑事訴追について論じられるとき，これにより（現実社会における犯罪の効果にもかかわらず）仮想空間について語られる。仮想空間とは，現代的な情報技術によって形成され，無数の相互に通じ合う情報処理技術からなるものである。別の角度からみると，インターネットは，想像を絶するほど豊富で，「目に見えないまま提示される」(10) 情報のことである。この点で，例えば，そのような情報に対し，

↘であったとしても，鑑定人への積極的な評価は客観的かつ真摯に考えられたものであると理解されることを期待する．

(7) 例えば，*Sieber* の，本テーマに最初に詳細かつ基本的な考察を行った「国際コンピュータ網における情報交通に対する刑事法上の答責性」に関する2回の論文（1996年），JZ 1996, 429 ff., 494 ff. 参照。

(8) このことは，「インターネット刑法」だけでなく，コンピュータ刑法全体に妥当する。経済犯罪撲滅に向けた第2法律（BGBl I 1986, S. 721 ff.）によるその導入あたり，*Sieber* は，学問的に重要な役割で関与した。彼のコンピュータ犯罪と刑法に関するその博士号取得論文（第2版，1980年）のみ参照。

(9) ここで，普通の大学教員として，マックス・プランク研究所に集められた国内外からの数多くの情報は独自の組織を形成しているということは，素直に認めざるをえない。しかし，このような組織的な能力は，鑑定人の業績を貶めるものではない。なぜなら，このような情報は，的確に加工されてはじめて意義をもつものだからである。

(10) 厳密にいえば，当然ながら，これらの情報を保管するために必要なデータ記↗

サーバーを物理的に押収することによる刑事訴訟上の介入も可能である(11)。これにより，インターネットにおける犯罪と刑事訴追が問題とされるとき，「情報」は，実体上および訴訟上の規定および問題の本質的な対象となる。この情報（そして，これが大部分について素材としての「情報法」の特殊性をなし，「横断的素材」という考えをも導く）(12) は，伝統的な刑法ないし刑訴法の行為客体や証拠に対して，一連の特殊性を示すのである。この特殊性は，その非物質性(13) に始まる。このことは，多くの古典的な実行行為（例えば，奪取＝Wegnahme，破壊＝Zerstören，横領＝Zueignen など）がそのままでは適合しないこと，また，現在の訴訟上の捜査行為（特に，保全措置）が少なくとも特殊な態様に変わらざるをえないことをもたらす。さらに，極めて無限定，迅速，極めて安価に情報が多様化する機会が付け加わる。これは，「密かな」という意味で，複製された情報の所持者がそのことについてすぐには気づかない（その「オリジナル情報」は，基本的に変化しないままであるために）ということを生じさせる。情報が転送される（ここでも，極端に速やかに，費用もかからずに，大半がそれを希望してもいる）機会にも，また別の特殊性が存する。その際，刑法を常に特徴づける国家間の限界は，真摯な障壁とはならない。

Ⅰ．実体刑法

実体刑法に関する限りで，この特殊性と逸脱（特に，従来の実行行為が

↘憶装置は，物質的なものである。

(11) この点について参照，*Sieber*, Gutachten（Fn. 5), C 112 ff. そこでは，比例性原則からして，相応の情報がコピーのかたちで確保される場合には，通常，このサーバーの長期間の押収は認められない，とされている。

(12) この点について参照，*Sieber*, NJW 1989, 2569 ff.

(13) ここでは，情報自体に関係づけられるのであり，データ記憶装置に関係づけられるのではない。すでに前掲 Fn. 10 参照。

それに「適合」しないという限りで）は，特に決定的である。刑法では，民事法などの場合と異なり，迅速かつ安易に類推による解決を図ることができないからである（基本法103条2項！）。情報は重要であり，これにともなって，インターネットも，特に，（基本的に，常に実在の）2人またはそれ以上の人によって行われるコミュニケーションに着目した犯罪構成要件に際して重要となる。例えば，詐欺罪（インターネットを通じた欺罔），刑法上の「表現犯罪」などがそうである。しかし，この場合でさえ，本来伝統的な物理的伝達形式に沿った犯罪構成要件に完全に適合するかという問題が生じ(14)，いくつかの派生問題（そのような契約締結の有効性，ドイツ刑法の適用可能性(15)）も生ずるであろう。

Ⅱ．刑事訴訟法

刑訴法では，特に捜査手続において考えうる犯罪および犯罪者に関する情報の収集が問題となるが，そこでは，情報技術の凱旋行進は，例えば，監視されるべきコミュニケーションが変化を遂げ，かつ常に変化し続けるということ，そして，情報が単純に従来とは全く異なるかたちで蓄積されるというかたちで効果をあらわす(16)。しかし逆に，（情報保護団体や，「啓蒙された」メディアから常に要求される）「情報的権利」も，従来は想像できないような範囲で存在し，それゆえ，これが刑事訴追機関にとってどの程度において利用されうるのかという問題も生じている。しかしその際，

---

(14)　この点について，後掲 Fn. 22 参照。

(15)　この点について，すでに前掲 Fn. 4 ならびに再び後掲 Fn. 19 ff の本文を参照。

(16)　その際，電子的記憶装置自体は，この間，もはや新たな現象とはいえなくなった。むしろ，現在的な問題は，「外部におかれた」特殊の蓄積装置にどのように対処すべきか，というものである。「クラウド」内の捜査の問題性について，後掲 Fn. 58 参照。

「外部委託される記憶装置」[17]や，非常に小さな媒体に無数の情報を蓄積するという私人にも可能な手段は，特定の情報保持者に対する介入に際しての「過剰情報」という問題ももたらしている。このことは，一方では，目的に即した使用という実践的問題と，他方では，しばしば私人の核心領域または少なくとも第三者の秘密情報に介入する過剰捜査という危険をもたらしている。

C．法曹大会鑑定意見の対象

Sieber は，鑑定意見において，「主題」を認識させつつ，（それにもかかわらず[18]）限定された範囲に沿って驚くほど豊富な情報と非常に詳細な事柄までを扱っている。鑑定意見の対象，目標，方法について導入部分（C 9以下参照）で述べられたことによると，インターネットにおける犯罪および刑事訴追に関する現象の実証的・法現実的分析が行われる（C 18以下，C 35以下参照）。そして，この現象学の対象は，「規範的総括」と評される国際領域および現行ドイツ法に関する概観において，法的評価――但し，一見すると簡潔な――にも付される（C 40以下参照）。その際には，実体刑法，刑訴法，危険・配慮・予防法，刑事訴追の国際協力が区別される。そのような部分の叙述は，やや抑え気味で，この点ですでに情報を得ている読者にはあまり新しいことを述べるものではないが，「刑法とインターネット」にこれまではまだあまりなじみのなかった読者にとっても，彼の深い分析がよく理解できるものとなっている。ここで（C 84以下参照），前述４つの領域は，各々詳細に検討されるが，その際特に，検討されるべき改正の必要性の問題と，（これが肯定されるとして）そのような改正に向けた適切な提言が詳細に述べられる。そして，鑑定意見は，まとめの部分を

---

[17] 参照，再び Fn. 16.
[18] 参照，前掲 Fn. 9.

もって終了している（C153以下参照）。鑑定意見は，このようにして，法曹大会に向けて支持可能な簡潔な提言をまとめただけのものではなく，重要な法政策的帰結をまとめたものである。しかし，これに基づいて，ミュンヘンにおける報告との関連で多くの支持可能な提言が展開されるであろうことは，疑問の余地がないであろう。

D．重要な個別問題

前述Cですでに不完全ながら示したように，問題点（鑑定意見で扱われ，そこでもすでにわずかながら検討されている）の多さを考えると，付随的な本論文において，そのすべてに取り組むことは難しい。しかし，本稿が，すべてを検討する必要もないし，そうすべきものでもない。むしろ，いくつかの問題を選び出し，部分的に，鑑定意見における必要かつ簡潔な叙述を補足するかたちで若干深める程度にとどめるべきであろう。そのような手法は，様々な理由から，特に有益となるだろう。

Ⅰ．実体刑法

１．刑法適用法

鑑定意見は，C74以下で，若干ながら刑法適用法の問題を検討している。つまり，どのような条件の下で，インターネット上で実行された犯罪に一定の国内（ここではドイツの）刑法が適用できるか，という問題である。国際基準がどちらかといえばあまり有益ではないことから[19]，刑法３条，９条の遍在主義の射程が重要となる。その適用は難しい。それは，特に，典型的にインターネットを通じて実行される一連の犯罪（特に，伝播犯罪

---

[19]　同旨，*Sieber*, Gutachten（Fn. 5), C. 74 f. E コマース準則から刑法適用法に関してどのような帰結が導かれるかという問題について，すでに *Kudlich* HRRS 2004, 278 ff. 参照。

や発言犯罪）が抽象的危険犯である（または，少なくとも抽象的危険犯とされる個別の実行行為が含まれている）ことによる。これらに際して，結果地を特定することができるか，それはどのようにしてできるかという問題（これにより，一方では，行為が行われた以外の国でも刑法上の訴追を可能とさせ，他方では，属地主義を採るすべての刑法秩序において，インターネット上でダウンロード可能な内容に対する全面的管轄という事態が避けられる）は，いまなお未解決のままである。

20世紀末に強くなった議論（連邦通常裁判所も，その *Töben* 判決において関与している）[20]の中で，鑑定人自身は，その包括的で特にその結果において説得的な提案を示していた。これは，「Push 技術と Pull 技術」とを区別するものである[21]。この点について，見解の一致（特に国内の範囲を超えた）はまだ見られないようである。それゆえ，鑑定人の見解に対しては，特に国際的な調整をも問題としている点で，同意すべきである。逆に，*Töben* 判決の帰結として理論上は危惧されうる，ドイツ刑法の「世界警察」化といった展開はこれまでまだ生じていない。したがって，刑法適用問題は実務上も前世紀末に「机上で」考えられていたほどには切実なものとはなっていないことは，確認しておかなければならない。

2．発言犯罪における実行行為と文書概念

短い部分（C101）で，鑑定意見は，刑法11条3項による文書概念の変更を提案している。その際，「媒体」の代わりとして，「情報またはメディア」の概念を用いるべきものとする。いずれにせよ関連する構成要件をインターネットにおける伝播犯罪にも円滑に適用したいと考えるのであれば，

---

[20] 参照，BGHSt 46, 212, ならびに，ふたたび Fn. 4 で紹介した文献。

[21] 参照，*Sieber*, NJW 1999, 2065 ff. この区別がインターネット事象の明白な経験のレベル内での詳細な技術的考察に際してどれほど妥当性をもちうるかは，本稿で評価することはできない。

この意見を支持すべきであろう。すなわち，この点において，通常，「文書（刑法11条３項）が伝播」されるということが問題とされる。たしかに，関連法規定の刑法11条３項では，媒体も，文書として定義されている。しかし，この媒体は，これが物理的伝達という伝播の伝統的概念に向けられたものである場合には[22]，いずれにせよインターネット上のコミュニケーションに際して（CD-ROM の交付という場合は別として）それ自体が物理的に伝達されるものではない。「インターネットに特殊の伝播概念」は，連邦通常裁判所が展開しているものであるが[23]，それは説得的ではない[24]。それは，規定文言と適合せず，他の刑法11条３項の意味での「文書」における解釈と体系的に矛盾するというだけでなく，基礎づけること自体が困難である。なぜなら，有形的な媒体に限定された文書概念も，CDやDVD等の海賊コピーの伝達に際しても[25]，およそ適用されうるものだからである。この困難さを回避しようとするならば，刑法11条３項の調整が必要であろう。但し，そのために過剰なことが要求されるわけではない。多くの関連する構成要件において，文書の公的なアクセスも，刑罰の下におかれるからである。そのため，インターネットを通じた本来の情報保持者へのアクセスで満足することができよう。

３．児童ポルノの問題ある規定

鑑定意見（C56ならびにC102）は，欧州レベルの基準を義務づけられた児童ポルノに対する可罰性を定める刑法184ｂ条に関して，批判的である。たしかに，同条は，インターネット上の犯罪を対象とするだけではな

---

[22] 参照，多くのものを代表する *Fischer*, StGB, 59. Aufl. 2012, § 78d Rn. 4 m.w.N.

[23] 参照，基本的なものとして BGHSt 47, 55 = StV 2001, 619 m. krit. Anm. Kudlich JZ 2002, 310.

[24] 同旨，*Sieber*, Gutachten（Fn. 5), C 55.

[25] 1997年の法改正の時点ではフロッピー・ディスク，現在では USB スティックなど。

いが，これに特に重要な適用領域を有するものである。本規定は，児童ポルノについてすでに早くから妥当していた禁止対象を，14歳から18歳までの人の画像にまで広げるものであるが，これは，実際に一連の困難な問題をもたらした。ここでは，若干のみ指摘しておく[26]。

通説によると，可罰性は，例えば，いわゆる見かけ上の未成年者（すなわち，18歳未満に見えるような成人）の画像をも含む[27]。これは，児童の性的搾取および児童ポルノ撲滅に対する欧州理事会議決2004/68/JI（2003年12月22日）[28] 1ｂ条の観点で範囲決議に適合した解釈に際しても適切であり，現実の事象，現実類似の事象，その他の事象はどこで区別されるのかは，刑法184ｃ条自身における定義によって少なくとも示されている。そのような禁止の正当性が決して自明のものではない点はおくとしても，適用上重要な問題がある。それは，刑法184ｂ条において平行の「見かけ上の子供」の事案に比べて，およそ明白かつ実践的に重要な問題である。すなわち，表現者が有名な成人であるが，未成年者のように見えるときは，刑法184ｃ条が適用可能である。これに対し，表現者が有名ではなく，それゆえ未成年者であるのかまたは未成年者のような成人であるのかが判明しないのであるが，その者が見かけ上の子供という要件を満たすほどはっきりと「子供に」見えるわけではないときには，「疑わしいときは被告人の利益に（in dubio pro reo）」の原則に従い，無罪としなければならない。

㉖ 詳細は，*Kudlich*, in: Bosch/Leible（Hrsg.), Jugendmedienschutz im Informationszeitalter, 2012, S. 85 ff.

㉗ 以下のみ参照，Satzer/Schmitt/Widmaier/*Hilgendorf*, StGB, 2009, § 184b Rn. 3, 19, § 184c Rn. 6; Schönke/Schröder/*Perron/Eisele*, StGB, 28. Aufl. 2010, § 184b Rn. 3 b, § 184c Rn. 4.

㉘ ABl. L 013 vom 20.01.2004, S 44 ff. ここで対象となっているのは，「子供のような姿をもつ現実の人であり，能動的または受動的に前述のような行為に同意した者」である。

これは，いささか奇妙な結論をもたらす。表現者が著名な成人である場合には，可罰性が基礎づけられうるのに対して，無名の未成年者であるかもしれない場合には，可罰性が排除されなければならないからである[29]。

他方，「幼い未成年者」か「年長の児童」かの区別が認定できない場合，すなわち13歳か14歳かの区別が（見かけ上からは）難しい場合，刑法184ｂ条からも184ｃ条からも無罪としなければならないというのは，さほど不合理ではない。疑わしい場合には，児童であるとも，また未成年者であるとも認めることができないからである[30]。この点で，選択的認定（択一的認定）は，両規定間に匹敵性が欠けるために認められない[31]。また，「規範的段階関係」[32]の承認（少なくとも刑法184ｃ条による有罪判決を帰結するという意味で）も，基礎づけられない。このような関係が認められる場合と異なり，刑法184ｂ条の「マイナス」は，「刑法184ｃ条が適用されるもの」と合致しない。なぜなら，同条は14歳の年齢になって初めて適用されうるものだからである。

同じく，行為者が18歳未満のときに相手方の承諾を得て作成した画像を成人後も所持するという場合の（基本的には支持すべき）刑法184ｃ条４項２文による特権についても，大きな摩擦と評価矛盾の生ずることが危惧される。この規定は，象徴的に「少年恋愛特権」と呼ばれる。これによると，基本的に，構成要件該当または構成要件上意味のある相手方（未成年者）の画像であっても，その所持は許される。この問題は，法律が厳密に，

---

[29] 参照，*Palm*, Kinder-und Jugendpornographie im Internet, 2012, S. 162 f. 結論において同旨，*Hörnle*, NJW 2008, 3521, 3525.

[30] 参照，*Palm*（Fn. 29), S. 164.

[31] 的確な見解として，*Palm*（Fn. 29), S. 164.

[32] そのような段階関係の事案における「マイナス」からの有罪判決について参照，*Fischer*（Fn. 22), § 1 Rn. 21; SSW/*Satzger*,（Fn. 27), § 1 Rn. 70; Schönke/Schröder/Eser/*Hecker*,（Fn. 27), § 1 Rn. 88.

若い行為者が「相手方の承諾を得て」作成する場合だけを含んでいることによって生ずる。「行為者」が相手方自身が作成した刺激的ポーズの画像を（例えば，プレゼントとして）受け取って保持するという，重要でないとはいえない事案は，ここに含まれていない。このことは，立法上の評価においておよそ不明である。ともかくいったんは相手方の承諾によって作成されたという場合，古い画像が「生涯にわたり」所持されることとなる対象の拡張は，現在交際中にそのような画像を所持することの可罰性と比較して，所持する方が場合によっては18歳を超えたばかりであるという理由だけでは，矛盾を生むため，問題なしとはいえない。経験からは，後に複写物が作成されること（例えば，交際が終了したのちに）によって，摩擦が生じやすい。これは，立法者が刑法201ａ条３項で明白に認め，現象論的には刑法238条の規定も基礎としている現象である。なぜなら，頻発するストーカー事案は，交際が破たんした後に発生しているからである[33]。

摩擦（一部でおよそ不合理な結論となる）は，およそ同年齢の相手方の場合に想定可能な「可罰性の間隙」があることから，すでに奇妙なものである。例えば，17歳の少女が，その17歳の交際相手に，刑法184ｃ条の構成要件に該当しうる刺激的な画像を作成し，所持を許したときは，刑法184ｃ条４項２文により不可罰である。若い男がそのような「写真撮影」をやはりその彼女の承諾を得て自分が18歳の誕生日を迎えた直後に繰り返した場合（しかし，彼女の方がまだ17歳であった場合），彼は，これにより犯罪を実行したことになる。さらにその２週間後，彼女の方も18歳になってから写真を撮影した場合，再び不可罰となる。このような可罰的行為と不可罰行為とのめまぐるしい変化，そしておよそ理解困難な「可罰性の間隙」は，避けられない「限界の苦しみ」といったものではなく，構造的な問題

[33] この比較基準を的確に指摘するものとして，*Fischer*（Fn. 22），§ 184c Rn. 10 hin.

点であることを示している。明らかに，可罰性の範囲が限界に接しているか，ないしは，それ自体として実際に可罰性を評価づけるものではない要素に結び付けられているからである。

４．インターネットを通じた「伝統的な犯罪」

鑑定意見の任務に特殊なことであるが，およそ正当にも周辺的にのみ言及されているのが，インターネットを通じた一般的な犯罪である（C17以下参照）。しかし，この点については，なお補足が必要である。「インターネットに関連する」犯罪の大半は，特殊な犯罪（例えば，刑法202ａ条以下）[34]または動物ポルノや大量虐殺を否定する内容の流布といったものではなく，非常に多くの詐欺犯罪である。当然ながら，そこには，（インターネットに固有というものではないが，インターネットと関連して行われる）フィッシング攻撃や，「ナイジェリアからの手紙」〔国際詐欺団〕等も含まれている[35]。しかし，これらの攻撃の多くは，専門性に欠けるという特徴をもち，多くの利用者に危険を創設するよりも，娯楽を提供する類のものである。これに対して，大きな問題となっているのは，例えばインターネットにおける「Abo-Fallen」[36]〔インターネット上での不当広告など〕または他の詐欺行為（例えば，商品注文に際しての）である。しかし，この点で，インターネットに特殊な問題は生じない。但し，刑事訴追機関が，場合によっては，大量実行性および依然として存在するインターネット媒体に対する疑いゆえに非常に早くに可罰性を肯定し，その際に従来認められてきた可罰性の制限（構成要件要素の慎重な検討という限りでも）を考慮しないという傾向に至ることがある，という点は別としてであるが。この点で典型的であるのは，連邦通常裁判所の近時の裁判例である[37]。その

34　この点について参照，*Sieber*, Gutachten（Fn. 5), C 41 ff.

35　この点について若干参照，*Sieber*, Gutachten（Fn. 5), C 26.

36　この点について参照., *Hatz*, JA 2012, 186 ff.

37　参照，BGH ZWH 2012, 191 m. Anm. *Kudlich*.

事件では，事実審裁判所より，広告により指定されたサービスが現実かつ給付に対応する反対利益であることの可能性が十分に証明されることもなく，インターネットを通じて締結された予約購入が即座に詐欺に当たるとして有罪とされた。

5．インターネットにおける責任構造

鑑定意見は，C60以下で，この間に通信媒体法（TMG）7条以下に定められたプロバイダ責任に関する規定を指摘している。これは，相当な範囲で，1997年に作られたドイツにおける以前の規定に基づいており，その創設にあたっては，特に鑑定人も，相当な部分で関与している[38]。当時の規定および現在の規定においてもなお貫かれている，インターネット・コミュニケーションにおける複数のサービス提供者に関する段階的な責任構造という基本的な考え方は，法的な責任は基本的に技術的なコントロールの可能性と一致するという点にある。コンテンツを自ら作成した者は，それゆえに無制限の責任を負うが，大容量のデータ貯蔵領域を提供した者は，基本的に，自身が何らかの違法なコンテンツについて指摘された場合に限り（しかし，相応の消去機会があるので，およそその場合においては）責任を負う。これに対して，単なるアクセス介在者は，基本的に，そもそも責任を負わない。彼らは，実際にコントロールの機会を有していないからである。

このように期待可能であることを前提とした技術的機会に沿った責任システムは，疑いなく支持可能なものである。但し，この技術状況への指向性は，前提となる技術的条件は変化することがないのかという点について，ときおり批判的に検討されている。この点を本稿で深めることはできないが（紙幅上の理由およびその能力も欠けるために），若干の見出しのみあ

㊳　参照，再び前掲 Fn. 7 における本文。

げておく。いわゆる「位置情報システム（Geolocation）」により，インターネット利用者は，IPアドレスを手掛かりに分析され，必要とあれば，締め出されることもあるが，その際には，IPアドレスが州のリストと照合される。自動照会コントロールおよび現代のコンテンツ・コントロール技術（例えば，Perkeo＝内容に関するブロック・システム，Youtube コンテンツ ID など）によって，一定のアップロードを遮断し，単なるデータ群を少なくとも部分的には自動で探索することができる。データ網におけるトラフィック・マネージメントのための分析ツール（例えば，優先化のために投入されるものであり，鑑定意見でも言及されている Deep Paket Inspection などがこれに当たる）は，流通する情報交通も少なくとも部分的にコントロールできることを示す。流動的な IP アドレスにおける帰属の問題は，新たなインターネット・プロトコル IPv6 によって解消した。そこでは，すべての「コネクテッド・デバイス」が固有の IP アドレスを持つこととなる。このような洗練された機会は，少なくとも，技術的な支配可能性に沿った答責性のルールは「調整」の必要がないか，という問題を提起する。その際，すべてのサービス提供者に対し，彼らが自己の目的を追求するために投入する意思がある最大限の技術的コストを，いわば「他人の利益」においても用いるように期待することが法政策的に説得的である，とまでは決して断言できないであろう。

Ⅱ．刑事訴訟法

鑑定意見は，刑訴法について，多くの個別問題を扱っている[39]。それは，いくつかの情報アクセス機会から，その使用にまで及んでいる。本稿では，紙幅上の理由から，詳細な言及は次の2点にとどめる[40]：

---

(39)　参照，*Sieber*, Gutachten（Fn. 5), C 62 ff.

(40)　新たな展開に補足するものとして参照，*Kudlich*, GA 2011, 193, 204 ff.

1．コンピュータの操縦による捜査

相応の情報とともにハードウェアの押収[41]，刑訴法100ａ条を通じた現在進行中のコミュニケーションへのアクセス（この手段には問題がない），プロバイダの下に中間的に蓄積された段階での E-mail へのアクセス（十分解決されていないが，連邦通常裁判所および連邦憲法裁判所より実務を支持する裁判が下されている[42]）とならんで，被疑者・被告人ないし第三者のコンピュータの操縦を必要とする捜査手段がある。その１つは，連邦通常裁判所より，解釈論として説得的に，許されないものと判断されている。その他のものは，支配的見解からは，許容されるものと解されている。

ａ）オンライン捜索

オンライン捜索の機会，すなわち，システムへの物理的な侵入や相応のソフトを送り込むという手段で，情報の状態を捜索し，電算機がインターネットに接続している最中に必要とあれば部分的に刑事訴追機関の下へ転送させるというかたちでの，電算機への密かなオンラインによるアクセスに対して，連邦通常裁判所の捜査判事による多くの注目すべき裁判例（そして，それに続く第３刑事部の裁判例[43]）は，正当にも，解釈論として禁止を示している。そのような法的権限は，厳密には存在せず，また（正当に強調されるとおり）異なる権限の「総体」から生み出されるものでもな

---

41 参照，すでに前掲 Fn. 13 の本文，ならびに，この点を深めるものとして，*Böckenförde*, Die Ermittlung im Netz, 2003, S. 264 ff., 336 ff.

42 参照，BGH NJW 2009, 1828 m. Anm. *Gercke* StV 2009, 624 ff. 詳細な議論について，例えば LG Hanau NJW 1999, 3647; LG Hamburg wistra 2008, 116; aus der Literatur *Gaede* StV 2009, 96 ff. 対立を詳細に紹介するものとして，*Meininghaus*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, 2007, S. 249 ff., 特に S. 252 ff. まとめと区別について，SK-StPO/*Wolter*, Bd. 2, 4. Aufl. 2010, § 100a Rn. 32 ff.

43 参照，BGHSt 51, 211; 前掲 ErmR BGH JR 2007, 77 mit Anm. *Jahn/Kudlich* JR 2007, 57 ff.

い。立法論としては，刑事訴訟上のオンライン捜索は(44)，少なくとも，連邦憲法裁判所が危険回避法の範囲に関して定立した条件を満たしていなければならない(45)。その際，密かなオンライン捜索の介入の強さは相当なものであり，潜在的にその対象とされるあらゆる生活領域からなる多様な情報，およびその隠密性から導かれる介入の強さ(46)を，考慮に入れなければならない。

b）端末電話傍受

コンピュータの操縦は，被疑者・被告人が暗号化された情報を受送信する場合にも必要である。それは，例えば，インターネット電話（VoIP）の場合に該当する。プロバイダによる情報提供を伴う「通常の」通信傍受は，助けにならない。そこで得られる情報は，暗号化されているため利用できないものだからである。ここで刑事訴追機関にとって関心があるのは，利用者のシステムにあるデータについて暗号化前またはその解除後にアクセスすることである。しかも，解析データが操縦により利用者から気づかれない間に訴追機関のサーバーへ送られるという方法によってである。このようないわゆる端末電話傍受の許容性如何という問題は，（判明する限りで）最高裁ではまだ判断されておらず，下級審裁判所の間でも見解が分かれている(47)。注釈書（コンメンタール）の支配的見解は，端末電話傍受に対し，刑訴法100ａ条と関連付けて受け入れる態度を見せているが(48)，一部

(44)　連邦警察局による危険回避の領域においてすでに存在するそのような措置の機会について，連邦警察局法20ｋ条を参照。

(45)　詳細について参照，*Kudlich*, HFR 2007, 202, 205 ff.

(46)　公然のオンライン捜索を認める見解として，*Valerius* JR 2007, 275, 278 は，これはすでに解釈論として許されていると述べる。

(47)　参照，AG Bayreuth MMR 2010, 266 m. Anm. *Bär*（賛成），LG Hamburg MMR 2008, 423 m. Anm. *Bär*（反対），ならびに AG Hamburg StV 2009, 636 m. Anm. *Kudlich* JA 2010, 310 ff. まとめとして，*Buermeyer/Bäcker* HRSS 2009, 433（438）; *Becker/Meinecke* StV 2011, 50 ff.

(48)　参照，*Meyer-Goßner*, StPO, 54. Aufl. 2011, § 100a Rn 7a; *Graf/Graf*, StPO, 2010, ↗

の文献では，批判的な見解もみられる[49]。たしかに，連邦憲法裁判所は，オンライン捜索に関するその裁判例において（どちらかといえば付随的に[50]），端末電話傍受はただ基本法10条１項の基準に沿ったものでなければならない（同時に，内密性や情報技術システムの不可侵性といった「コンピュータ基本権」にも沿ったものであることは不要である），との見解を示している[51]。

しかし，この簡潔な連邦憲法裁判所の判示の具体化，さらには帰結にも，およそ問題がないわけではない。すでに基本法19条の保護範囲への関連性によっては，決して，そのような介入のために創設された刑訴法100ａ条の権限も適用されることが決定されるわけではないからである[52]。また，鑑定意見では，刑訴法100ａ条はそのことを保障しうる明確な「法的基準」をもつものではない，と強調されている。したがって，*Sieber* は，支配的注釈書および判例において広まっている見解とは異なる立場を表明し，端末電話傍受は刑訴法100ａ条によって把握されるものではないと述べている。裁判例に対するこのような解釈は，必然的なものではないと思われる。法的基準は，相応に限定された命令決定においても認めうるからである[53]。

↘ § 100a Rn 31; KK/Nack, 6. Aufl. 2008, § 100a Rn 27. 反対の見解として，SK-StPO/*Wolter*, § 100a Rn 27 ff.

[49] 参照，再び *Buermeyer/Bäcker* HRSS 2009, 433 ff.（m.w.N. S. 438）; *Bäcker/Meinecke* StV 2011, 50 ff.; *Vogel/Brodowski* StV 2009, 632 ff. まとめとして（結論として，解釈論としても許容性を認めるが，立法論として明確化を提案する）*Bratke*, Quellen-TKÜ-Grundlagen, Dogmatik, Lösungsmodelle, im Erscheinen 2012, 3. Teil.

[50] この点で，この論拠に的確に批判するものとして，*Bäcker/Meinecke* StV 2011, 50, そのような理由づけの例として，*Hornick* StraFo 2008, 281, 284 f.

[51] 参照，BVerfG NJW 2008, 822, 826（Rn 190）.

[52] 保護範囲からの権限規定へのそのような推論に反対する見解として，*Becker/Meinecke* StV 2011, 50.

[53] そのような決定を支持する提案として，*Bratke*（Fn. 49）, Teil 3 A I 2.

しかし，法治国家的には好感のもてる解釈である。補足するならば，刑訴法は特に100ｂ条3項1文においてプロバイダからの操作による通信傍受を典型としており，被疑者・被告人のコンピュータシステムへの操縦と適合させることは困難である，と指摘することができよう。但し，ここで，次の点は考慮しておかなければならない。すなわち，刑訴法100ｂ条3項に関する立法理由では，プロバイダへの「この義務づけに関する必要性」は，「通信傍受処分が効果的な形で通常ならば通信サービス事業者の協力の下でのみ行われる」ということにのみ基づくものとされているが[54]，これによって厳密に，「通信傍受処分を常に通信事業者の関与の下で行うべきことの刑事訴追機関の責任」を基礎づけるべきものではないとされている[55]。

鑑定意見と異なり，端末電話傍受事態はなおも刑訴法100ａ条により捕捉されていると解した場合でも，その技術的な準備は，法律問題として過小評価すべきものではない。例えば，ウィルスに感染した E-mail の送達により必要なソフトをインストールすることができた場合には，この点で，許される付随的処分と見なければならない。刑事訴追機関において，対象のコンピュータに都合のよい機会に（例えば，コンピュータが修理のため修理会社にあるとき，空港の税関で捜索するなどの方法で[56]）侵入することに成功した場合も同様である。これに対し，住居に侵入し，ソフトを密かにインストールするようなことは，当該処分によって把握されたものではない。第1に，通信傍受を実施するために他人の住居に立ち入ることは，非典型的な二次的処分であり，ここでは不文の付随的権限といい得ないものである。第2に，このような措置について，特に基本法13条の独立した

54　BT-Drs. 16/5846, S. 47.
55　BT-Drs. 16/5846, S. 47. 立論について詳細は，*Bratke*（Fn. 49), Teil 2 A II 6.
56　参照，*Bratke*（Fn. 49), Teil 2 B I 2 b.

制限システムはここで相応の法律の留保を置いていない，したがって，刑訴法100ａ条，100ｂ条は，そのような付随的権限をそこに含んだものであるとすると憲法違反となることからも，排除されなければならない。

２．別の新たな問題状況

刑訴法のその他の問題に関して，インターネットと関連するおよそすべての問題は，多かれ少なかれ「新しい」ものである。但し，個別の現象（例えば，プロバイダにあるE-mailへのメールボックスへのアクセスというかたちでの介入[57]）に関しては，すでに15年ほど前から争われている。しかし，ここ10年ほどの技術的および社会的発展と関連した非常に新たな問題点もある。その典型は，「クラウドにおける捜査」や，ソーシャル・ネットワークなどが，捜査処分の活動領域として挙げられる：

ａ）クラウド・コンピューティングとクラウド・ストレージ

鑑定意見では付随的に言及されているが[58]，公刊された裁判例ではまだ取り扱われたことがない問題として[59]，いわゆる「クラウド・コンピューティング」ないし（刑事訴訟上の捜査処分に関してより興味深い）「クラウド・ストレージ」が挙げられる[60]。このようなコンピュータ・サービス（特に，データ蓄積）の分散したシステムへの「アウト・ソーシング」（その柔軟性，容量，負担分散を顧客に与える）は，証拠として重要なデータがもはや処分の対象となる人（特に，被疑者・被告人）のローカルエリア

57　参照，BGH NJW 1997, 1934（メール・ボックス判決）m. Anm. *Bär* CR 1996, 490; *Kudlich*, JuS 1998, 209; *Palm/Roy*, NJW 1997, 1904. この以前の議論についてのまとめとして，例えば *Böckenforde*（Fn. 41), S. 381 ff.; *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004, S. 66 ff., 特に 90 ff.

58　参照，例えば *Sieber*, Gutachten（Fn. 5), C 36.

59　参照，学説からの指導的見解として *Gercke* CR 2010, 345 ff.; *ders*. ZUM 2009, 526, 536.

60　この点について参照，若干ながらも *Kudlich*, GA 2011, 193, 207 f.

にではなく，外部のサービス提供者の下で（そこで，場合によってはいくつかの計算機に分けられ，しばしば外国にも送られるなどして）蓄積されるという状況をもたらす。刑事訴追機関にとって，このことは，物理的な蓄積場所から利用者への必要的なデータ転送（ないし返還）は，この転送の間に刑訴法100ａ条による伝統的な通信傍受を手段として内容を認識する可能性を開く，ということを意味する[61]。また，刑訴法94条以下による介入に際して，蓄積場所の提供者は，被疑者•被告人とは異なり，例えば，データをすぐに消去・隠滅することを試みるものではない。

他方で，例えば，被疑者・被告人の住所地と物理的な蓄積場所とが離れている場合には，問題も伴う[62]。その際，現行刑訴法110条３項の形式では，たしかに，蓄積データが捜索命令に記載された場所にないという形式的な問題が解消される。もっとも，主権原理および刑訴法110条３項の立法理由を考えると，国内に蓄積されたデータに限定される。したがって，クラウド・ストレージの国際的な広がりを考えると困難さが内在しており[63]，鑑定意見ではいくつかの箇所で述べられていた国際協力の必要性が相当にあることとなる。

ｂ）ソーシャル・ネットワーク

インターネットにおける利用者の行動は，参加型ネット／Web 2.0 の標語の下，ここ10年で大きく変化した。その際，特にソーシャル・ネットワークが人気となり，捜査機関にとって関心のある情報源となっている。

61）参照，*Gercke* CR 2010, 345, 346.

62）およそ実践的には，例えば，一人の利用者がクラウド・ストレージ事業者の複数のコンピュータにデータを分割するといったまったく不可能あるいは異常とはいえないような場合に，個別事例において，物理的な記憶装置の１箇所への限定は困難となりうる（その場合，捜査機関の管轄決定も困難となる），ということによる。

63）詳細について参照，*Gercke* CR 2010, 345, 347 ff.

警察官がその際に架空名で被疑者である可能性がある者とのコミュニケーション関係を持つに至る場合，そのために必要かつ適切な法的根拠は何かという問題が生ずる[64]。その際，誰もが自由にアクセスできる内容を知るという事案は，問題がないであろう。連邦憲法裁判所と同様[65]，意図的な資料収集，蓄積，データの利用において場合によっては対象者にとって特別の危険状況が認められるとしても，この「介入」は，捜査の一般条項によって捕捉されているといってよい。このことは，事後審査されない者とのコミュニケーションが図られたという事案[66]でさえ，裁判所は事後審査が欠けるという点からコミュニケーション相手における保護されるべき信頼を認めていないことからも，なお妥当する[67]。

しかし，例えば，ソーシャル・ネットワークにおいてコミュニケーション事象に関与した人の身元確認（個別事例では異なる強さのもの）が行われたという場合には，結論が異なる。この場合，特に，捜査の一般状況に基づくべき単なる「非公然に捜査する警察官」（noeP）の投入と，刑訴法110ａ条以下に基づくべき「隠密的捜査」とをどの点で区別すべきか，という問題が生じる。その際，「左翼党」議員の「小さな質問」に基づいて，2011年に連邦政府から，連邦警察局における捜査手続に関して，刑訴法100ａ条以下による隠密的捜査官は，捜査官がソーシャル・ネットワークにおいて長期間意図的に対象者と連絡を取り合う場合に投入されている，と報告されている[68]。そうだとすると，例えば，実際にこの段階が基準となるべきか，どのような介入が刑訴法110ａ条以下の条件に即したものであるべきか，という問題が生ずる。仮名が用いられる限りで（関与者の識別が

64　この点について，*Rosengarten/Römer* NJW 2012, 1764 ff. も参照。
65　BVerfGE 120, 274［＝StV 2008, 169-Leitsatz］, 345（＝Rn. 291）.
66　典型的なニックネームを想像してみよ。
67　参照，BVerfGE 120, 274［＝StV 2008, 169-Leitsatz］, 345 f.（＝Rn. 292 f.）.
68　参照，BT-Drs. 17/6587, S. 5.

コミュニケーション関与の条件であり，少なくとも本当と推定される審査のためのデータを手掛かりとして行われる，という理由から)[69]，この領域は，隠密的捜査官に該当するというべきである。

E．おわりに

本稿は，若干の特に関心をもつべき観点，ないし現代的な観点を簡潔に叙述することにとどまった。本稿は，しばしば「刑事訴追とインターネット」の標語の下で議論される問題がどのようなものであるか，そして，これが技術的および社会的に変化する範囲条件によって現在でもなお常に変化するものであることを示した。インターネットの使用がこの間にすべての生活領域で行われるようになったことの無限の意義を考えるならば，複雑な問題であり，法曹大会の刑事法部会によりそのテーマが選ばれたことは，疑いもなく正しい判断であった。

---

[69] 参照，すでに *Kudlich* GA 2011, 193 (198 f.).