大学院研究年報　第45号　2016年２月

インターネット上の犯罪行為に関する考察

髙　良　幸　哉*

要　　旨

パーソナルコンピュータ，スマートフォンなど，情報端末が幅広く普及し，情報技術が社会生活に浸透した現代において，コンピュータやインターネットを用いた犯罪，あるいはこれらを客体としてなされる犯罪に対して，対処の必要性は増す一方であり，国際社会との関係の中で，我が国においても刑事法分野からの種々の対応がなされてきた．本稿は，サイバー犯罪をめぐる問題に関し，まず，サイバー犯罪をめぐる刑事規制について概観した上で，ネットワーク利用犯罪について，ICT技術的観点を踏まえ，検討を行なうものである．

目　　次

Ⅰ　はじめに

パーソナルコンピュータや携帯電話，スマートフォンといった，個人に利用可能な電子端末は，われわれの社会や私的生活領域に深く浸透しており，これらの利用なくしては社会生活において不便を強いられる場合も少なくない．メールによる文書の送受信，SNS（ソーシャルネットワーキングサービス）といったインターネット上のコミュニティ，個人情報の電子データ管理・利用などは社会活動の一部として組み込まれており，その利用者は小中学生から高齢者まで幅広い層に至るものである．[1)] そのような中で，コンピュータやインターネットを用いた犯罪，あるいはこれらを客体としてなされる犯罪に対して，対処の必要性は増す一方であり，国際社会との関係の中で，我が国においても刑事法分野からの種々の対応がなされてきた．たとえば，1987年の刑法改正による電子計算機使用詐欺罪（刑法246条の２）の新設や2004年の児童買春，児童ポルノにかかる行為等の規制及び処罰並びに児童の保護等に関する法律（以下児童ポルノ法）における電磁的記録提供等罪の新設（７条），2011年刑法改正によるわいせつ電磁的記録にかかる罪（175条１項），不正指令電磁的記録に関する罪（168条の２および168条の３）の追加などが，これに当たる．その他，Winny等を用いた著作権法違反行為，SMS（ショートメールサービス）やSNSを用いたセクスティングやリベンジポルノ，マイナンバー法や個人情報保護法の改正にかかる情報保護問題など，議論となる事案

＊　たから　こうや　　法学研究科刑事法専攻博士課程後期課程
2015年10月２日　推薦査読審査終了
第１推薦査読者　只木　　誠
第２推薦査読者　曲田　　統

は様々である．筆者は先に，拙稿「インターネット上のポルノグラフィについて」中央大学大学院研究年報法学研究科篇44号195頁や，拙稿「児童ポルノの単純所持規制に関する考察」比較法雑誌48巻３号277頁等，サイバー犯罪の中でもとりわけインターネットを介したポルノグラフィ犯罪について検討を加えてきた．本稿は，サイバー犯罪をめぐる問題に関し，まず，サイバー犯罪をめぐる刑事規制について概観したうえで，ネットワーク利用犯罪について，ICT技術的観点を踏まえ，検討を行なうものである．

Ⅱ　サイバー犯罪の現状

１．サイバー犯罪とは

サイバー犯罪とはいわゆるサイバースペースを介し，またはそこに存するコンピュータに対してなされる犯罪である．ここにいうサイバースペースとは，コンピュータとコンピュータが通信網を介してつながり，当該情報網上で情報を取引・共有することで形成される空間を指す．[2)]

サイバー犯罪はコンピュータおよびコンピュータ・ネットワークを標的とした加害行為と，コンピュータ・ネットワークを，伝統的犯罪を実現するための道具として用いる加害行為をいうとされ，[3)]サイバー犯罪をめぐっては，サイバー犯罪条約（Convention on Cybercrime）など国際的な取り組みがなされている．サイバー犯罪条約は，2001年に欧州評議会（EC）により発案された条約であり，日本，アメリカ合衆国，ドイツなど30か国の署名で採択され，2004年７月１日に効力が発生した．我が国においては，2004年に国会において本条約の批准が承認され，2011年の刑法改正等の法整備ののち，2012年７月３日に受諾書が欧州評議会の事務局長に寄託され，同年11月１日から本条約の効力が発生している．[4)]

サイバー犯罪条約[5)]は，サイバー犯罪から社会を保護することを目的として，コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化，コンピュータ・データの迅速な保全等にかかる刑事手続の整備，犯罪人引渡し等に関する国際協力等を規定している．本条約は，コンピュータ・データおよびシステムの機密性，完全性および可用性に対する犯罪として①違法なアクセスおよび違法な傍受（２条および３条），②データの妨害およびシステムの妨害（４条および５条），③装置の濫用（６条），コンピュータ関連犯罪として④コンピュータに関連する偽造および詐欺（７条および８条），特定の内容に関連する犯罪として⑤児童ポルノに関連する犯罪（９条），その他⑥著作権および関連する権利の侵害に関連する犯罪（10条）をサイバー犯罪とし，これらの犯罪に関する未遂および幇助又は教唆（11条）や，サイバー犯罪に関する刑事司法手続きについての締結国の協力について規定している．

我が国においてサイバー犯罪は，主に，アクセス行為の禁止等に関する法律（不正アクセス禁止法）違反，コンピュータ・電磁的記録対象犯罪，ネットワーク利用犯罪に大別される．[6)] 不正アクセス禁止法違反は，主に，情報へのアクセス権限のないものが，いわゆる「なりすまし」行為にみられるように，不正に情報を取得する行為などをいう．サイバー犯罪条約にいう上記①②がこれに当たるが，これは，個人情報等の管理に関する行為を加え，情報の保護に関する犯罪と言い換えることもできよう．コンピュータ・電磁的記録対象犯罪は，その犯罪行為の客体をコンピュータや電磁的記録とする犯罪であり，サイバー犯罪条約では上記③が該当し，我が国の立法上は主に，電子計算機使用詐欺罪やコンピュータウイルスにより電子機器を不正操作する不正指令電磁的記録に関する罪がこれに当たる．ネットワーク利用犯罪は，インターネット等ネットワークを犯罪行為の手段として用い行う犯罪であり，サイバー犯罪条約では上記⑤⑥であり，児童ポルノやわいせつ物のインターネット上での頒布・公然陳列行為，著作物の権限なき者による不正な提供行為が典型例

である．このネットワーク利用犯罪が，サイバー犯罪の中では最も多く，[7]その他，ネットワークを介した売買春，違法薬物等売買もネットワーク利用犯罪に含まれる．

サイバー犯罪をめぐっては，上記のサイバー犯罪条約にみられるように，国際的な取組がなされており，コンピュータ，インターネットが普及する中，その対策は急務である．我が国においてもサイバー犯罪の一例として挙げたいくつかの犯罪を規制する法政策がとられている．以下では，サイバー犯罪の我が国における現状と国際社会における規制について概説する．

2．我が国におけるサイバー犯罪対策の概要

我が国においては，1987年刑法改正による電子計算機使用詐欺罪の新設に始まり，2011年刑法改正による不正指令電磁的記録に関する罪の新設やわいせつ電磁的記録にかかる罪の明文化に至るまで，刑法と特別刑法を含めサイバー犯罪にかかる種々の法改正がなされている．1987年刑法改正においては，電磁的記録不正作出及び供用罪（161条の2），電子計算機損壊等業務妨害罪（234条の2），電子計算機使用詐欺罪（246条の2）といった，主にコンピュータ・電磁的記録に関する犯罪が規定された．これらは，ICT技術の発展に伴いコンピュータそのものを対象とした犯罪が増加したことを受けて規定されたものである．2001年には，支払用カード電磁的記録に関する罪（18章の2）が新設され，個人の情報の記録されたクレジットカード等についての電磁的記録の不正使用が規定された．また，2011年改正では，わいせつな電磁的記録の公然陳列や頒布にかかる事案の解決として，175条にわいせつ電磁的記録の送信に関する罪が追加され（175条1項），近時国際的な対応が要求されているいわゆるインターネットウイルスについての規制を定めた，不正指令電磁的記録に関する罪（168条の2，168条の3）新設がなされている．

また，刑法のみならず，特別刑法の分野では，まず不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）が1998年に制定され，これは1条において，「不正アクセス行為を禁止するとともに，これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより，電気通信回線を通じて行われる電子計算機にかかる犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り，もって高度情報通信社会の健全な発展に寄与することを目的」とすることを明示している．同法の2013年改正により，他人の識別記号，すなわちパスワード等を不正に取得する行為（4条），不正アクセス行為を助長する行為（5条），識別符号の入力を不正に要求する行為（6条）識別符号の入力を不正に要求する行為（7条）が新たに加えられ，いわゆるフィッシング行為のように，インターネットのウェブサイト等を通じて他人の識別記号を取得しようとする行為への対応がなされている．また，直接的にサイバー犯罪規制を定める法律ではないが，個人情報の保護に関する法律（以下個人情報保護法）や行政機関の保有する個人情報の保護に関する法律は，情報を現に利用・保管するに際しての情報の保護について規定を設け，一部罰則による対応も含めた規定がなされている．情報の保護に関しては，そもそも刑法上の保護客体性の問題がある．この点，情報の利用が商業的な価値を有するなど，情報の価値性の高まりを受けてその保護の必要性は高まっているといえる．[8]また，情報の保護という観点にとどまらず，規制対象としての電磁的記録も広い意味では情報であり，情報の客体性を明らかにする必要があろう．

そのほか，ネットワーク利用犯罪については，児童の性的搾取の防止を目的とする（児童ポルノ法1条）児童ポルノ法に関しては，児童ポルノの拡散を防止するという国際的な要請を受けて，2004年改正により，児童ポルノにかかる電磁的記録の

提供等に関する罪（７条各号）など，インターネットによる児童ポルノの拡大を防止するための規定が設置されている．これは，刑法175条のわいせつ物関連犯罪とその論点を同じくするものも多い．[9] また，現在，権利者でない者が，映像や音楽，電子化された書籍等を，インターネットを介して送信したり，動画配信サイトにアップロードしたり，あるいは，ファイル共有ソフトにより送受信するような著作権を侵害する事案が多数生じており，これに対応するために，2009年，2012年に著作権法の改正がなされている．2009年改正においては映像・音楽等のアップロード行為が処罰の対象となり，また，映像・音楽のダウンロードの禁止が規定された．2012年改正においては，当該ダウンロード行為が処罰の対象となっている．

これら，ネットワークを介した犯罪においては，たとえば，ファイル共有ソフトなどのインフラの開発者を処罰しうるかという中立的幇助の問題といった，刑法の伝統的な事案にかかる問題もあるほか，[10] インターネット特有の事案として，禁止の対象となるダウンロードとはどの範囲までの閲覧行為を意味するのかといった問題も議論の対象となっている．これらの問題に関しては本稿のⅢ章において言及したい．

３．サイバー犯罪に対する国際的対応

ここで，サイバー犯罪条約を提案した欧州連合（EU）におけるサイバー犯罪規制と情報法制についてみていきたいと思う．EUにおいては，EU加盟国間の情報や人の流通に対応するように，加盟各国におけるサイバー犯罪条約に適合する国内法による，当該犯罪に対する対応に加え，EUおよびECにおいても情報流通に関する基準の策定や，サイバー犯罪の取り締まりの強化などの対応を進めている．

たとえば，「欧州デジタルアジェンダ」（COM（2010）245 final）[11] は，EUの成長戦略「欧州2020」（2010年３月策定）に掲げた７つの主要事業のうちの１つであり，①デジタル分野の市場統合，②標準規格および相互運用性の改善，③インターネットの信頼性および安全性の向上，④インターネットアクセス確保と高速化，⑤最新技術の研究開発，⑥デジタルデバイドの解消，⑦多目的な技術開発の７つの目標を掲げている．これら７つの目標は2020年までにインターネットを基盤とする経済活動（デジタル経済）を繁栄させ，デジタル革命の恩恵を全ての人に広めることであるが，これに関しては，2012年にこれらの実施状況に鑑み，これらの目標を達成するために必要な，重要な分野の政策の特定を行っている．[12] ここにいう③のインターネットの信頼性および安全性の向上については，さらに，EUにおける情報の保護の観点においても重要となる．EUにおいては，1995年10月24日，「個人データの取扱いにかかる個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（EUデータ保護指令）を採択しており，EU加盟国に共通のデータの保護に関する指標を提供している．これは，EU加盟国からその他の国へのデータの移転について規制しており，ある一定以上の保護要件を満たしていない国との情報の流通について原則として認めていない．当該指令は，2014年３月24日に改定案が可決されており，さらなるデータの保護の規制の強化が図られている．[13]

サイバー犯罪の観点においては，サイバー犯罪条約に基づいた加盟国各国の国内法による対応がまずもって予定されるが，EUのサイバー犯罪に対する対処において，加盟国間の連携の強化が図られている．たとえば，①警察と民間の協力関係を強化するため，調査方法やサイバー犯罪の傾向などに関する知識の共有を進める，②警察と民間の両方が，情報の要求，遠隔からの捜索，犯罪者を追跡するためのサイバーパトロール，国境を越えた共同調査に対し，迅速に対応できるようにする，③違法コンテンツの掲示など，インターネット上で起こった犯罪行為を報告できる警報プラッ

トフォームを短期間内に立ち上げるといった，取締り強化策がECにおいて提案されている．[14)]

EU加盟国のドイツにおいては，ドイツ刑法典において，StGB202a条データの不正アクセス，同202b条データの不正入手，同202c条データの不正アクセス又は不正入手の準備，同263a条コンピュータ詐欺，同303a条データの改変，同303b条コンピュータの妨害が規定されている．加えて，同176条でインターネットを介して児童に対して露出行為をするような児童に対する性的虐待，同184b条，同184c条では児童ポルノや青少年ポルノの頒布・調達・所持等についてインターネットを介して行うことが規制される．これらは，従来インターネットを介さずになされていた行為態様について規定するものであり，条文上インターネットを介するということを示す文言はないが，学説，判例を含め，これらの行為がインターネットを介する場合においても適用されることを認めている．[15)] また，情報の客体性の議論と関係して，情報の個人情報の保護に関しては，1977年に個人情報保護に関する連邦データ保護法が制定され，1990年に改正がなされたほか，社会法分野や医事法分野，保険法分野などにおいて個別の法制[16)]がなされている．また，2000年には，上記1995年のEU指令を受けて，これに適合するように法改正がなされている．[17)]

4．客体としての情報

サイバースペースにおける行為を考える場合，情報それ自体が保護客体，あるいは行為客体になりうる．情報の保護をめぐっては，OECD 8 原則や上記EUの個人情報保護に関する指令，ドイツの個人情報保護法制にみられるように，個人情報保護についての国際的要請は高い．もともと，個人情報の保護は，情報が国境を越えて流通する中で経済活動をはじめとした社会活動を円滑化するために保護されてきた．我が国の個人情報保護も基本的には情報の円滑な流通を前提としている．しかしながら，現在，何らかの社会活動の円滑化のためではなく，情報それ自体が経済的価値を有するに至っている．たとえば，ビックデータの問題がこれに当たる．ビッグデータは「事業に役立つ知見を導出するためのデータ」とし，ビッグデータビジネスについて，「ビッグデータを用いて社会・経済の問題解決や，業務の付加価値向上を行う，あるいは支援する事業」と目的的に定義され，[18)] 多量性，多種性，リアルタイム性[19)]といった性質を有する．この情報は情報それ自体が企業のマーケティング等に利用されうるものであり，それ自体経済的な価値を持つ．かかる運用を担保するために，我が国の個人情報保護法はビッグデータ利用を踏まえた改正案が第189回国会で提出され提出され，[20)] いわゆる行政手続における特定の個人を識別するための番号の利用等に関する法律（以下マイナンバー法）においても，一定程度集約される個人特定情報が不当に利用されないよう規定が設けられている[21)]など，情報の要保護性は高い．

ここで，サイバー犯罪と情報の客体性に考えると，サイバー犯罪において最も割合が大きいものはネットワーク利用犯罪であるが，そこでやり取りされるのは電磁的記録を含む情報であり，犯罪行為の客体として情報を認めるかが問題となる．ここで，とりわけ問題となるのが，わいせつ物・児童ポルノ犯罪における客体性の問題である．これらいわゆるポルノグラフィ犯罪については，元来有体物を客体として想定されている．媒体に記憶されず，情報の受け手の五感のみで知覚できる情報は，固定性が弱く，それ自体として伝播性が少ないため，法益侵害性の観点においては，有体物に比べ低いとされてきた．そのような情報の伝達を問題とする犯罪としては，刑法174条の公然わいせつ罪が挙げられるが，ネットワークを介する場合，たとえばライブストリーミングなどにより露出行為を行うような場合であっても，わいせつな文書ファイルを送信する同175条の頒布のよ

うな場合であっても，ネットワーク上を伝わるものは電気信号にすぎない．そのため，両罪の区別を含め情報の行為客体性が問題となり，判例における情報化体された記憶媒体を行為客体とみる，ハードディスク説[22]や，2011年刑法改正のわいせつ電磁的記録送信罪の新設による立法による対応などがとられてきている．

以上を前提として，ネットワークを手段とする犯罪類型について，ここで問題となるいくつかの論点につき，従来型の犯罪との関係性を踏まえて検討したいと考える．

Ⅲ　ネットワーク利用犯罪

1．ネットワーク利用犯罪と従来の犯罪

インターネットやパソコン通信のように，個別のコンピュータや個々のネットワークを結びつけるネットワークの存在は，従来当該ネットワーク外でなされていた行為による法益の侵害の場を拡大させた．ネットワーク利用犯罪は，Ⅱ章でも述べたが，わいせつ物や児童ポルノの頒布・公然陳列，リベンジポルノ，公然わいせつ，著作物の提供といったネットワークの情報の伝達性を利用した犯罪や，インターネット掲示板やウェブメールサービス，SNSなどを連絡手段等に用いる，売買春，薬物事犯といったもの，ウェブサイトに他人を欺罔し錯誤に陥らせるようなプログラムを組み込んで行う，いわゆるワンクリック詐欺のような行為などが挙げられる．これらは，ネットワークやコンピュータ・プログラムといったツールを利用して犯罪行為の実現を目指すものであるが，ここで挙げた犯罪そのものは，刑法改正などにより条文上明示される行為態様もあるが，それ以前に解釈上当罰性が認められたものも多く，また，どの範囲までを実際に犯罪行為であると認めるかについては，なおも議論の余地のあるものも多い．

これらの犯罪を考慮する際には，まず，従来型の犯罪の行為態様と比して，法益の侵害性が同等程度あるのかが問題となり，当該法益侵害性を認めた上で，その行為の性質，行為客体の客体性といった個々の要素について犯罪行為であると認めるに足るものであるのか判断する必要がある．

わいせつ物・児童ポルノ犯罪についていえば，当該犯罪における行為客体である，児童ポルノにかかる情報や，わいせつ情報に客体性を認めてよいのかという議論が問題となり，加えて，わいせつ視覚情報の伝達である公然わいせつ罪との客体の区別の問題などが議論の対象となってきた．また，児童ポルノ犯罪については，ドイツにおいては，児童ポルノの調達と所持が処罰の対象となり，我が国においても2014年児童ポルノ法改正により，児童ポルノ単純所持が処罰対象となった．ここでは，インターネット上でストリーミング配信され，一時保存情報が自動的にPC内に記録される場合の閲覧が調達に当たるのか，一時情報の保管が所持に当たるのかといったネットワーク利用犯罪に特有の行為態様も問題となる．この点，それぞれの行為態様の及ぼす法益侵害性の議論と合わせて，従来の行為態様との比較検討を行う必要がある．

また，これらのネットワーク利用犯罪の犯罪行為性を認めるとして，それぞれの犯罪におけるツールを提供したものの可罰性についても検討の必要がある．たとえば，児童ポルノ犯罪を放置した場合における，インターネットサービスプロバイダ（ISP）や，ネットワークを介しての有害情報や違法情報の提供を助けるツールを開発した者の責任，有害情報，違法情報そのものではなく，当該情報にアクセスするための間接情報を提供したものの責任など，インフラ提供者の可罰性の検討も必要となる．

以下では，わいせつ物・児童ポルノ犯罪および，名誉権侵害事案，著作権法違反行為についての具体的な事案を参考に，以上の問題についての検討を行う．

2．情報の提供

(1) 諸外国の対応

ネットワーク利用犯罪の代表的なものとしては，まずもって，わいせつ物・児童ポルノ関連犯罪が挙げられる．これらの犯罪のうち，とりわけ児童ポルノに関しては，国際的な規制の動きがある．その基礎にあるものが児童の権利に関する条約（子どもの権利条約）である．子どもの権利条約は18歳未満の児童の性的・経済的な搾取をなくすことを目的としており，この条約を背景として，EUにおいては2004年に「児童の性的搾取及び児童ポルノ対策の現行枠組決定[23]」を公布し，2011年にはこの枠組み決定を廃止し，「児童の性的虐待及び性的搾取並びに児童ポルノの対策に関して定め，現行の枠組決定に代わる欧州議会及び理事会指令[24]」を公布している．この枠組み決定を受けて，ドイツにおいては2007年刑法改正（2008年施行）で，14歳以上18歳未満を対象とした青少年ポルノの頒布・調達・所持等を禁止するStGB184c条を新設したほか，当時の同184b条２項の他人のための調達行為の刑の上限を１年から５年に引き上げるなど，児童ポルノ・青少年ポルノの規制強化を図っている．[25]

StGB184b条と同184c条はインターネット上の頒布を特別に規定してはいないが，ドイツにおいても，インターネット上の頒布・公然陳列行為はこれらの条文の規制範囲に含まれると介される．これについて，BGH NStZ 2001, 596 は，被告人が，14歳未満の児童に対し，StGB176条の意味における性的虐待を行い，当該行為を記録した児童ポルノ的なデータファイルを，インターネットを通じて公開した行為につき，インターネットを通じて児童ポルノを公開する行為は，相手方のコンピュータへのデータファイルの到達をもって，StGB184条３項１号（現行StGB184b条１項頒布に該当）にいう頒布にあたり，インターネットの利用者が見聞できる状態で公開した事案につき，同４条３項２号にいう公然と陳列した行為（現行StGB184b条１項陳列に該当）に当たるとし，実際に利用者がアクセスする必要まではないとした．ここで，BGHは，データそれ自体を公然陳列の対象とはせず，児童ポルノデータの化体されたハードディスクを客体とすることにより，公然陳列を認めている．

また，アメリカ合衆国においては，児童ポルノ規制（合衆国法典2256条）と合衆国憲法第一修正条項の表現の自由[26]との関係が問題となったNew York v. Ferber[27] やその後のOsborne v. Ohio[28] のように，児童ポルノ規制については規定の合憲性が確認されている．その後，1996年児童ポルノ禁止法[29]が連邦議会で成立し，①ポルノが小児性愛者の性的欲求を刺激しかねず，また，小児性愛者が児童を性的行為に勧誘する目的で，あたかも多くの児童が同様の行為を行っているかのように当該児童に思い込ませるためにそれらを利用する可能性があり，その結果，実在の児童が性的虐待を受ける危険性を増大させる可能性があること，②実在しない児童を描写した精巧かつ写実的なポルノに規制対象を拡大することで，描写対象となっている児童の実在性に関する検察官の証明責任を軽減し，児童ポルノ規制の実効性を確保することから，非実在の児童を取り扱ったポルノについても規制対象となっていた．[30] ただしその後，Ashcroft v. Free Speech Coalition[31] において，「実在しない児童を描写するポルノの禁止は，正に表現の内容そのものを規制するものであるにもかかわらず，これを正当化する程度の重大な利益が見当たらない」として，非実在児童関する規定については違憲とされた．現在は，「当該判決を考慮した児童を誘拐及び性的搾取から保護するための法律（PROTECT法）[32]」による新たな規制がなされている．[33]

インターネットを介するポルノグラフィについては，[34] United States v. Maxwell[35] およびUnited States v. Thomas[36] があるが，これらはサイバーポルノの送信に関して合衆国連邦章典旧1465条にお

いては，データのネットワークを介した送信については明文上規定されていないものの，特にデータ自体の有体物性を問題とせずに，データの送信を「輸送（transports）」の概念に含めることでインターネット上のポルノグラフィの送信行為の可罰性を認めている．通信品位法[37]や児童オンライン保護法[38]により，ネットワークを通じて有害な情報が伝達されることで児童が悪影響を受けることを防止するための法整備がなされている．なお，通信品位法に関しては，成立後翌年には違憲判決が下されている．

以上，ドイツと米国の例を挙げたが，各国においてネットワーク上のポルノグラフィに対する規制がなされている．新法の制定のみならず，現行法の解釈により，これまでの法概念を現在的問題に適用させるという試みがなされている．この点，我が国においても同様の状況がみられる．

⑵　我が国の状況

①　わいせつ物・児童ポルノ犯罪

わいせつ物・児童ポルノ犯罪については，情報伝達の手段が紙媒体や音声や通信メディアを介さない視覚情報しかなかった時代においては，主に，当該書籍等に記載されている内容がわいせつ物に当たるのかという，憲法上の表現の自由とわいせつ概念の問題が議論の中心であり，[39] 加えて刑法175条で規定される情報発信者の行為態様である頒布・公然陳列における「公然性」が何を意味するのかという議論が中心であった．[40] メディアの発達により，これらの伝統的なわいせつ物関連犯罪をめぐる議論がなされなくなったわけではないが，[41] その公然性の議論については，ここ20年ほどで新たな問題が生じている．

わが国における公然性については，「不特定または多数のものが認識できる[42]」状態であるとする見解が一般的であり，175条においては公然陳列行為については当然であるが，頒布行為や電磁的記録の送信行為も，「特定個人」に対して提供される場合には本条には当たらず，公然性要件が要求される．これは，わいせつ物犯罪が「善良な風俗」という社会的法益保護を目的としており，固定性のある情報の伝播による社会的法益への侵害を問題とするためである．この点，同様に公然性要件を要求される保存性の無い情報の伝播である，公然わいせつ罪とは区別される．[43]

コンピュータ・ネットワークは，その情報の送信範囲の広範さや送受信の容易さから，紙媒体のように情報の伝達に媒体自体の物理的移転を要する場合に比べて，情報の伝播性が高い．国境を越えて取引される情報が我が国の法秩序に与える影響は大きい．ネットワークを介するわいせつ物・児童ポルノ犯罪に関しては，その公然陳列犯罪，頒布罪についていくつかの裁判例がある．

我が国においてネットワーク上のわいせつ物公然陳列罪の成立を初めて認めた最高裁判例である最決平成13年７月18日 刑集第55巻５号317頁は，被告人がパソコン通信を通じてサーバコンピュータ上にアップロードしたわいせつ画像等を自身の運営するするパソコンネットの会員に閲覧させた事案であるが，ここで最高裁は「わいせつ物を「公然と陳列した」とは，その物のわいせつな内容を不特定又は多数の者が認識できる状態に置くことをいい，その物のわいせつな内容を特段の行為を要することなく直ちに認識できる状態にするまでのことは必ずしも要しないものと解される」としている．この判断は，すでにわいせつな内容を記録したビデオテープを陳列した事案[44]において，再生機材を用いなければ，わいせつな内容を閲覧できないような記録媒体の陳列をも公然陳列であると認めたことと見解を同じくしている．平成13年決定は，「被告人が開設し，運営していたパソコンネットにおいて，そのホストコンピュータのハードディスクに記憶，蔵置させたわいせつな画像データを再生して現実に閲覧するためには，会員が，自己のパソコンを使用して，ホストコンピュータのハードディスクから画像データをダウンロードした上，画像表示ソフトを使用して，画

像を再生閲覧する操作が必要である」が，「そのような操作は，ホストコンピュータのハードディスクに記憶，蔵置された画像データを再生閲覧するために通常必要とされる簡単な操作にすぎず，会員は，比較的容易にわいせつな画像を再生閲覧することが可能であった」として，公然陳列の重要なファクターとして「閲覧の容易性」を取り入れている．2004年の児童ポルノ法改正や2011年刑法改正によって電磁的記録の送信行為が処罰対象として明文化された現在においても，最高裁は同様の見解に立っていると思われる．[45]

また，提供・頒布罪は公然陳列罪との行為態様の区別において，頒布・提供型事案の行為は，単に不特定または多数の者に閲覧可能な状態を作出するだけでは足りず，情報の受け手に当該情報を「得させる」ことまでを要する．[46] 頒布・提供型事案の代表的なものは「販売」であり，情報の受け手は特定されていることが多く，陳列型事案のように情報の受け手側が閲覧を容易に出来るかという受け手側の事情が問題となるのではなく，頒布・提供者が情報受け手における情報受領を担保する必要があるのである．従来の判例の立場に立てば，これを満たさない行為はそもそも提供型事案にはならず，公然陳列型事案として処理されるべきであるように思われる．

② 名誉侵害

情報の提供型の犯罪としては，名誉毀損等，名誉侵害事案が挙げられる．我が国の刑法230条の２が１項で，「公共の利害に関する事実に係り，かつ，その目的が専ら公益を図ることにあったと認める場合には，事実の真否を判断し，真実であることの証明があったときは，これを罰しない」として，「公共の利害」による特例を認めているように，名誉権を侵害する可能性のある言論であっても，それが個人の意思の表明である以上，憲法21条の表現の自由を侵害しないよう，表現の自由の尊重と名誉権の保護のバランスを考慮しなければならない．

インターネット上の言論においては，インターネットの匿名性や情報発信の容易性ゆえ，言論が過激になる場合が少なくなく，当該言論が個人の名誉を侵害する場合もありうる．表現規制については，国家の介入は最小限にすべきであると思われるが，一定の場合には法的サンクションの必要があるのは当然のことである．ただし，インターネット上の言論においては，当該名誉毀損言論に対して被侵害者側からの対抗言論機会を得ることも，従来型の紙媒体上でなされる言論に比べれば容易である．米国においては，speechに対しては言論の場においてmore speechによる対抗を行なうという，「場（フォーラム）の理論」が原則であるが，新聞等のメディアに対するアクセス能力を持つものでなくとも，ネットに接続している限り，言論活動の場に参加できるインターネット上の対抗言論についてはこの原則がより妥当しうる．[47] ただし，両者が対等の立場で言論できる状況に無く，このような対抗言論によって自身の名誉を回復できないような状況においては，やはり国家による仲介を要するであろう．

これは，名誉毀損に関する一般的なルールであるが，刑法230条の名誉毀損罪について考慮する際，このような対抗言論の理論を持ち込むべきかについては疑問が残る．[48] というのも，名誉毀損罪は抽象的危険犯であり，言論によって具体的な名誉侵害が生じていることまで要しない．とすれば，刑法上の名誉毀損は当該言論を行なった時点で，他人の名誉を害するという抽象的危険は発生しており，その後の対抗言論は結果発生後の事情であるからである．そのため，対抗言論の理論を刑法230条の問題とするかには慎重な考慮を要する．

③ リベンジポルノ

インターネット上の名誉の問題に関連して，現在リベンジポルノ[49]が問題となっている．リベンジポルノについては，私事性的画像記録の提供等による被害の防止に関する法律案（リベンジポルノ防止法）が2014年11月19日に参議院本会議にお

いて可決され成立した．リベンジポルノはインターネットの発達によって問題が顕在化し，加害者が被害者の写真等を撮影する場合に加え，携帯電話・スマートフォンなどによって自ら自身のわいせつな画像を撮影し，SMSで送信したり，SNS等にアップロードすること（いわゆるセクスティング（sexting））[50]が容易になったことも要因として，深刻化している．[51]

リベンジポルノ防止法は，「私事性的画像記録の提供等により私生活の平穏を侵害する行為を処罰するとともに，私事性的画像記録にかかる情報の流通によって名誉又は私生活の平穏の侵害があった場合」において「個人の名誉及び私生活の平穏の侵害による被害の発生又はその拡大を防止すること」を目的としている．ここにいう「記録」とは，①性交又は性交類似行為にかかる人の姿態，②他人が人の性器等（性器，肛門又は乳首）を触る行為又は人が他人の性器等を触る行為にかかる人の姿態であって性欲を興奮させ又は刺激するもの，③衣服の全部又は一部を着けない人の姿態であって，殊更に人の性的な部位（性器等若しくはその周辺部，臀部又は胸部）が露出され又は強調されているものであり，かつ，性欲を興奮させ又は刺激するもの，が記された写真・電磁的記録を意味し，かかる「記録」を「第三者が撮影対象者を特定することができる方法」で提供することが構成要件となっている．

本法にいう記録は，保護法益の観点においてみると，刑法175条にいうわいせつ電磁的記録よりも，客体性はより広く解されている．これは「第三者が撮影対象者を特定することができる」ことで撮影対象者の「名誉及び私生活の平穏」に対し深刻な影響を与えることが影響していると思われる．刑法175条のような「善良な風俗」といった社会的法益への侵害に至らないような性的な描写であっても，その提供が被害者の個人的法益を侵害する罪を構成するのである．

リベンジポルノについては，アメリカ合衆国において連邦法として，「反リベンジポルノ法」が制定されるには至っていないが，州法においてはいくつかの規制例が見られる．例えば，ニュージャージー州では2004年に発効した「ニュージャージー州法典」第2C章（刑法）第14節９条（2C:14-９）により，性的な画像や映像などをそこに写っている本人の同意を得ずに他人に公開することはプライバシーの侵害に当たり，３万ドル以下の罰金が科される．同法が，全米初の「反リベンジ・ポルノ法」とされる．また，カリフォルニア州では，2013年10月に，プライバシーの侵害について定めた「カリフォルニア刑法」647節を改正する「上院法案第255号」がJerry Brown知事によって署名された．これにより，本人の同意を得ずに，深刻な心理的負担を負わせることを目的として性的な画像や映像などをインターネット上などに公開することが軽犯罪に問われ，６か月以下の禁固刑又は1000ドル以下の罰金に処せられると定められた．ただし，同法はニュージャージー州の「反リベンジ・ポルノ法」とは異なり，撮影者が被害者自身である場合は罪に問われることがない．[52]ドイツにおいてはリベンジポルノ規制について議論はあるものの，未だ立法には至っていないのが現状である．

以上，ネットワーク利用犯罪について，情報の提供者側の行為について検討した．情報の提供者つまりは犯罪行為者の行為については，伝播性の高いネットワークシステムの利用や，その客体として本来的には電気信号にすぎない電子情報や電磁的記録を行為客体とすることによりその行為態様には議論があるが，結論としては，現実の世界において違法であることを，実際に法益侵害性がある以上，仮想空間においても違法とすべきであるという思想の下，ネットワーク上でなされる行為を従来型の行為態様に引き寄せる解釈がなされている．この点，情報を行為客体とすると，刑法174条と同175条の区別が原理上困難になるという理由から，私見はこのような解釈を妥当であると

考える．ただし，行為者ではなく，その対極にいる，情報の受け手側の行為については，従来型の行為類型の理解の枠内で把握することが困難な場合がある．以下では，ポルノグラフィ情報の受領と保管を例に，受け手側の行為について検討を加えたい．

3．情報の受領

⑴　受け手の可罰性

従来の法制上，わいせつ物や児童ポルノを購入・入手する者の行為については処罰対象外であった．この点，著作権法違反事案においても共通するところであるが，違法情報の作成・提供者と受領者によって構成される広範なブラックマーケットを規制撲滅するためには，情報発信者側のみを処罰するだけでは不十分であるとの考慮から，情報の受け手側の行為を規制する動きが活発化している．その代表例が，著作権法違反におけるダウンロード（著作権法47条６など自動公衆送信の受信）行為の処罰化（同47条ないし47条10，49条など）や児童ポルノ単純所持行為の処罰化である．これらが，現実世界で行なわれる場合，物理的な客体の受領という形であり，物理的な客体の所持であり，その行為態様において，その処罰の可否は別段，行為それ自体には議論の余地は無い．

しかしながら，ネットワークを介し記憶媒体に情報を電磁的記録として保管するような事案については，どの範囲まで可罰的な行為であると見るかには，コンピュータシステム上の問題から検討を要する．以下では，情報の閲覧と情報の保管について，その技術的側面に言及した上で，ドイツの事例を参考に検討を行なう．

⑵　情報の閲覧の技術的側面

インターネット上で情報を閲覧する場合，閲覧者側の意思としては，他人がアップロードした情報を画面に表示させ閲覧する場合と，当該情報を自身のコンピュータ上にダウンロードし閲覧する場合がある．閲覧者側にダウンロードの意思がない場合であっても，キャッシュデータのように自動でコンピュータ上に保存される場合もある．閲覧は本来的には，「書物などを調べたりみたりすること」であり，「見る」という情報の媒体への保存性を有しない行為そのものであるが，インターネット上の用語としては，「ウェブブラウザを用いてウェブページを見ること」を意味し，ネットワークやコンピュータを通じて画面に情報を表示させるに際して，単なる「見る」行為であってもそこに，記憶媒体への一定の保存性を有することになるのである．

このことは，情報の受け手側の入手行為の可罰性や，情報提供者の行為においても何をもって情報を「得させる」とするのかといった問題を考慮する際に重要な考慮要素の一つとなりえ，閲覧行為の性質を考慮するにあっては，サーバから情報の受け手への情報の廃止件形式といった，閲覧に際しての情報の技術的側面が問題となるのである．配信の方法としては，現在のところ，以下の３つに分類できよう．①アップロード画像・映像のダウンロード，②ライブ配信映像の閲覧，③ストリーミング配信映像の閲覧である．①に関しては，ウェブ掲示板掲載の画像の閲覧やWinnyなどの動画共有ソフトを利用した入手であり，閲覧によるキャッシュの自動保存の問題のように，入手・情報所持の故意の問題はあるものの，コンピュータ上の情報としては閲覧可能な，記憶媒体に固定された情報であり，ここではそれほど問題とはならない．

②のライブ配信は，ライブストリーミングとも呼ばれ，データをダウンロードしつつ同時に再生する方式であるストリーミングの一種で，映像や音声をリアルタイムで配信する方法である．リアルタイムでエンコードを行い，そのままストリーミング再生する方法である．これは，ウェブチャットなどが代表例であるが，このような配信方法においては，中継者となるサーバは元となる動画や音声の素材（クリップ）を持たないので，

一部のストリーミングのように「いったんダウンロードしてから再生する」という方式を選択することができない．そのため，映像ファイル等をダウンロードする場合のように，閲覧した情報は固定性を持たず，たとえば，ライブ配信によってリアルタイムでわいせつ行為を行い，閲覧者に見せる行為は，視覚情報を認識させる行為であり，刑法174条の公然わいせつ型事案の射程に入ると考えるべきである．著作権法におけるダウンロードの観点においては，当該ライブ配信形式の映像に関してはダウンロード行為自体が観念できないため，同法違反の射程の範囲外となろう．

ウェブ上でリアルタイム配信ではない映像を配信する方法としては，通常のウェブサーバに保存された情報をHTTP（Hyper Text Transfer Protocol）形式で配信する方法と③のストリーミングがある．[53] このHTTP形式の配信に関しては，ウェブページ上に映像再生ツールを設置するプログラムを設定し，閲覧者をしてワンクリックで映像の閲覧ができるようにした場合であっても，その仕組みとしては映像データを閲覧者のコンピュータに保存させ閲覧させるものであり，外形上ストリーミング配信と区別できない場合も多いが，仕組みとして①のダウンロードに組み込まれる．③のストリーミング配信については，基本的には上記のライブストリーミングとは別に，主に２つの形式に分かれる．

第一の方法としては，Adobe社の提唱したRTMP（Real Time Messaging Protocol）に代表される，ストリーミングサーバを経由する方法である．これはRTMPという方式で通信され，ストリームを分割して通信するものであり，Adobe社のFlashに依存するストリーミングである．ここで情報は通常のウェブサーバではなく，ストリーミングサーバを経由して配信される．ストリーミングサーバを経由する場合，映像の配信と同時に再生可能であり，映像化されたフラグメントは随時削除されるため，再生可能なデータは閲覧者側のコンピュータ上には保存されない．

第二の方法としては，Apple社の技術を用いたHLS（HTTP Live Streaming）がある．これは主にApple社製の通信端末であるiPhone等で用いられる技術であったが，その他のスマートフォンなどにも用いられている．これは，ストリーミング配信ではあるが，ストリーミングサーバを経由するのではなく，通常のウェブサーバを経由して，HHTPを用いて通信する技術である．この技術においてはm3u8と呼ばれるプレイリストファイルを最初に読み込み，そこからフラグメント化された動画ファイル（10秒毎のTSファイル）をダウンロードすることによる再生が行われる．HLSを用いたストリーミングにおいてダウンロードされるファイルの内m3u8（拡張子が„.m3u8“となる）形式のファイルは，再生情報を記録したいわゆるプレイリストにすぎず，これ自体には再生可能な情報を含まないが，HLSにおいてダウンロードされるTS（拡張子が„.ts“となる）形式のファイルは，その中に再生可能な情報を含み，再生ソフトをもちいることなどによる再生が可能である．そのため，児童ポルノとの関連では，児童ポルノの受領行為と所持行為，著作権法上のダウンロードの観点から問題となる．

⑶　情報の調達と保管

インターネット上の情報の配信をめぐる問題については，いくつかドイツにおける先例がある．また，ライブストリーミング型事案であるBGH NStZ 2009, 500 被告人は，ベルギーのオイペンからインターネットに接続していた14歳未満の児童数名に対し，インターネットのリアルタイムの動画配信システムを介して露出行為等性的行為を行ったものであり，StGB 176条４項１号は，児童の「前で（vor）」性的行為を行うことを児童に対する性的虐待であると規定しており，距離的接近性において被告人と被害児童らは対面しているとは言えないため問題となった．BGHは，児童の前で行われる性的行為に関して，児童が性的な事象

を知覚することによる，児童に対する法益侵害性を重視しており，本件においても被告人と児童が空間的距離的に直接対面していないとしても，インターネットのリアルタイムの動画配信システムを介して，性的事象を知覚していたとして，176条４項１号にいう児童の「前で」性的行為を行うことによる，児童に対する性的虐待の成立を認めている．この事案は，キャッシュデータの形で情報が自動保存されない事案について，公然わいせつ型の事案として処理したものである．

キャッシュデータの保存が，児童ポルノの所持に当たるとされた事案としては，次の二つの事案が代表的である．BGH NStZ 2007, 95は，被告人が，ネットサーフィンを通じて児童ポルノを検索し，児童ポルノデータがキャッシュとして被告人のコンピュータ上に保存された．BGHは，コンピュータのシステム上キャッシュデータが自動で削除されない限り，いつでも本件児童ポルノデータを検索することが可能であるとして，キャッシュデータの保存をStGB184b条４項にいう児童ポルノの所持に当たるとしている．また，BGH NStZ 2009, 208[54]は，被告人が，児童ポルノ的な画像を，インターネットで閲覧し，当該データファイルが被告人の認識の下自動で保存された．その１月後被告人はインターネットを介して児童ポルノ的なフィルムを自身のコンピュータ上にダウンロード[55]したものであり，LGがコンピュータ上でなされる所持罪のかすがい効果により，本件各調達行為が所為単一となると認めたのに対し，所持罪は調達行為に劣後する受け皿構成要件にすぎないとして，所持行為のかすがい効果を否定した事案である．

成人に対し公然わいせつを行う行為はStGB 183条で規定されるが，性的行為の定義規定である同184g条２項で，他人の「前で」性的な行為を行うことであるとされ，行為態様については同176条４項１号の児童に対する性的虐待同様に，インターネットを介する場合であっても183条に該当する行為は可能である．BGH NStZ 2009, 500は，176条４項１号との関連で，児童による知覚がなされることを理由に，空間的な接近を伴う対面がなくても，児童の「前で」なされた性的虐待が可能である旨述べている．ここで問題となるのは「知覚」であり，情報の移転や保存ではない．本件は，ライブストリーミング配信の技術的側面から，当該結論を導き出しているわけではないが，わいせつ物や児童ポルノ犯罪が固定性のある情報を問題とするのであれば，やはり情報の固定性を有さないライブストリーミングについては，公然わいせつ型犯罪の射程でとらえるべきである．児童ポルノについてはStGB184b条１項および３項で所持罪が規定されている．BGH NStZ 2007, 95では，ドイツにおいてはインターネットから情報受け手ないし閲覧者のコンピュータ上に児童ポルノ的なデータがすぐに閲覧できる完全な状態で保存されている場合や，データが破損していても一応それ自体で再生が可能なデータの保存されているような場合のみならず，データの一部とその参照情報のみのデータであり，それ自体では再生可能ではないようなキャッシュデータであっても，かかるデータをもとに後の参照が，キャッシュが削除されるまで可能であることから，その点に法益侵害性を認めて児童ポルノの所持を認めている．[56] また，BGH NStZ 2009, 208は，調達行為との罪数との関係においてではあるが，児童ポルノの所持行為が，調達行為の実現結果であって，受け皿規定であると述べている[57]ものであるが，本決定においても，キャッシュデータの保存を児童ポルノ所持罪の射程でとらえている．

キャッシュの保存を行為者が認識しているとして，これを行為者の頒布行為の一部である到達とみなすことは妥当であろうか．この点，ドイツにおいては，BGH NStZ 2007, 95の所持罪決定のように，キャッシュデータがコンピュータ上に記憶される場合であっても，これをデータの保存であるとするが，それ自体ではわいせつ性を発現できないデータまでも，その後の閲覧の危険性をもっ

て電磁的記録と見ることは妥当ではない.[58)]

ドイツのキャッシュ保存の2事例にみられるのは，ウェブページで閲覧した画像のキャッシュの問題であるが，例えば，ウェブページ上に組み込まれた映像の配信の場合はどうであろうか．現在映像配信の形態としては，HTTPによるダウンロードをさせる形態，RTMPを用いて再生性のあるデータを保存させない形態，HLSを用いた断片的再生データを有する形態等があるが，このうち再生可能なデータを含む2類型については，データの保存に所持を認めてよいかについては，なおも考慮の必要がある．ドイツにおいては，所持ではなく，その前段階の受領行為である調達が処罰されており，所持という結果は刑事手続き上これを補完する役割も担っており，キャッシュの保存に所持的性格を認めることにも一定の理解は出来る．しかし，児童ポルノ犯罪は過失犯規定を規定していないことに鑑みれば，キャッシュの保存を認識しておらず，故意が欠ける場合には本罪の対象とすべきではないだろう.[59)] また，ストリーミングに関して，ドイツにおいては，その技術的側面から情報が継続的に保存されず削除されるという点に鑑み児童ポルノの所持性を認めないという見解があるが,[60)] ここには現在スマートフォンを中心に拡大しつつあるHLS型のストリーミングにおいて必ずしもこの論理が当てはまらない点，考慮すべきである．

我が国においては，児童ポルノ法制において所持罪の前段階である調達行為を規制する規定はなく，検索行為等が処罰の対象とはならないことに鑑みれば，ドイツに比べキャッシュデータについて所持の客体とみる実益は小さいと思われる．また，データの再生性について，それが映像データの場合，その性質においていずれの形式のストリーミング配信であるのか，それともHTTPによるダウンロード型の映像配信であるのか，通常人において外形上は見分けがつかない場合が多く，法がその時代の通常人を対象としているという前提に立つなら，現行法が処罰対象としていない閲覧行為という，行為の形式は同様であるが，提供者側にかかる偶然の事情によって，形成される所持状態の可罰性が決定されるというのは法的安定性に欠けると思われる．少なくとも，閲覧というある種の調達行為が条文上規定されていない現状においては，キャッシュデータを所持客体とすることを一般化することはできないと思われる．ただし，再生性のあるキャッシュデータの保存を認識し，これが自動で削除されないような手段，例えば当該データをコンピュータ上の一時記憶フォルダから取り出し別フォルダに保存するなどの手段を講じた場合は，もはやそれは一時保存されるのみのキャッシュデータとはいえず，所持罪の射程に入りうるように思われる．なお，現在文化庁は，Youtubeなどの動画共有サイトの閲覧は著作権法の禁じるダウンロード行為には当たらないとの見解に立つ[61)]が，これらは厳密にはストリーミング配信ではなく，その技術的性質上，閲覧はダウンロードを伴うものである．これは現行法の文言においては本法が禁じる自動公衆送信の受信行為とは区別できない．むしろダウンロードを行うことについての認識・認容という故意の問題の射程に入るものである．このような動画配信サイトの閲覧を著作権違反行為から除外するのであれば，ダウンロード行為の再定義といった立法を要するであろう．

4．インフラ，情報ツール提供者の幇助をめぐる問題

(1) ソフトウェア開発者による幇助

ネットワーク利用犯罪について，情報の提供者の行為および情報の受領者の行為について概観し，若干の検討を行った．ただ，ネットワーク上の犯罪を考慮するに際し，これら二者に加え，これら二者が行為するに際して利用するソフトウェアなどのツールを提供する者，あるいは，情報の流通の場であるネットワークへ参加を提供する

ISPの責任や可罰性の問題である．

ネットワーク利用犯罪において用いられたソフトウェアの代表的な例としては，Winnyがある．Winnyは，サーバコンピュータを経由せずネットワークを構築するピュアP2P[62]（pure peer to peer）方式を採用する．ピュアP2P方式の通信は端末間の情報の直接のやり取りを可能とし，通信をサーバの能力に依存せずに行えるなどの利点を持つ．Winnyにおいては掲示板機能や情報検索機能などを備えており，情報の検索・入手を用意しにする機能を有していた．なお，Winnyはピュア P2P方式によりサーバを経由しないことや，別のパソコン経由でファイルを転送仕組みを備えるなど匿名性を担保するなどの仕組みを備えるソフトである．[63] このようなシステムを備えたWinnyは著作権法に違反する著作物や，児童ポルノなどの電磁的記録の授受に用いられることになった．そこで，当該ソフトの開発者の幇助が問題となった事案がいわゆるWinny事件[64),65)] である．

本件最高裁法廷意見は，適法用途にも著作権侵害用途にも利用できるファイル共有ソフトWinnyをインターネットを通じて不特定多数の者に公開，提供し，正犯者がこれを利用して著作物の公衆送信権を侵害することを幇助したとして，著作権法違反幇助に問われた事案につき，Winnyのようなソフト開発の性質に関しては，「新たに開発されるソフトには社会的に幅広い評価があり得る一方で，その開発には迅速性が要求されることも考慮すれば，かかるソフトの開発行為に対する過度の萎縮効果を生じさせないためにも，単に他人の著作権侵害に利用される一般的可能性があり，それを提供者において認識，認容しつつ当該ソフトの公開，提供をし，それを用いて著作権侵害が行われたというだけで，直ちに著作権侵害の幇助行為に当たると解すべきではない」としている．そのうえで，客観的には侵害性の認めるものの，「現に行われようとしている具体的な著作権侵害を認識，認容しながらWinnyの公開，提供を行ったものでないことは明らか」であるとし，被告人がWinnyの公開，提供に当たり，常時利用者に対しWinnyを著作権侵害のために利用することがないよう警告していたなどの事実が認定されており，「例外的とはいえない範囲の者がそれを著作権侵害に利用する蓋然性が高いことを認識，認容していたとまで認めることも困難であ」るとして，被告人には著作権法違反罪の幇助犯の故意を否定している．[66)]

以上のように最高裁は，客観面としての侵害性を認めつつも，主観面において故意の成立を否定するという，従来型の幇助犯に関する処理を行う．Winnyの技術的側面においてその後の技術開発を志向する有用性があるが，このような有用性を理由に，客観的に構成要件該当性が無いとする見解もあるが，[67)] ネットワーク上利用されるソフトウェアなどの技術は，犯罪に利用される可能性がある一方，それ自体一定以上の有用性をもつものが多く，その点を考慮すれば，ネットワーク上のツールに関しては犯罪の成立を認めることが困難になるのではないかとの疑問が残る．[68)] なお，FLマスク[69)] 事件のように，ソフトウェア開発者が，わいせつ物公然陳列の幇助犯に問われた事案もあるが，この事案は明確に公然陳列に対して加功していたものであり，本件とは状況を異にする．技術的有意性があるとはいえ，ネットワーク利用犯罪の幇助についても，その構造においては従来型の中立的行為による幇助の事案と変わらず，従来の法の枠組みの中で考慮すべき問題であろう．

(2) ISPの責任

ネットワーク利用犯罪において関与する者としては，インターネットサービスを提供するISPについても考慮すべきであろう．ISPの責任については，特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律，いわゆるプロバイダ責任制限法において，損害賠償責任の免除など，その民事上の責任を制限する規定が

設けられている．この点，刑事責任について考慮すると，インターネット上で公開されている児童ポルノや名誉棄損表現の削除などが考えられる．ただし，ISP自身が当該言論を掲載しているウェブサイト等への編集権を有している場合は別であるが，多くの場合，ISP自身はインターネット等へのアクセス可能性を提供しているにすぎず，また，ネットワーク上に膨大な情報を抱えていることに鑑みれば，そもそもこれらの削除を行うことに対する作為可能性がないのではないかとの疑問がある．また，有害情報の判断に関しては，通信情報の閲覧である．[70] ISPには憲法上の権利である通信の秘密を守る義務があり，[71] 電気通信事業法によって禁止される，知得（積極的に通信の秘密を知る行為）・窃用（通信当事者の意思に反して利用する行為）に当たる可能性がある．そのため，ISPにこれらの行為につき刑事法上の作為義務を課すことについて問題がある．現在ISPが自主的に行っている，児童ポルノサイトのブロッキングに関しても緊急避難による正当化を要するであろう．[72]

Ⅳ　おわりに

以上，サイバー犯罪規制の現状を概観し，サイバー犯罪の中で最も割合の多い，ネットワーク利用犯罪における行為について，提供型類型と受領型類型をめぐる問題を中心に検討を行った．サイバー犯罪の内，不正アクセス禁止法違反行為や，コンピュータウイルス作成などの不正指令電磁的記録関連犯罪のように，サイバー犯罪の登場で新たに導入された行為態様も存するが，ネットワーク利用犯罪の多くは，サイバー犯罪登場以前の行為態様の延長線上にある．ネットワークを介することで従来型の犯罪と同等かそれ以上の法益侵害の可能性を生じることが少なくなく，そのため，個々の行為について，学説・判例の解釈や立法により処罰範囲が拡大されてきた経緯がある．しかしながら，Ⅲ章で述べたストリーミング技術の差異によって，受領者側の行為の性質が変わる場合があるなど，情報技術との関係を踏まえた検討も必要である．サイバー犯罪にみられるように，技術的側面を踏まえつつ，現実に生じる法益保護の問題について，従来処罰対象とされてきた行為とその法益侵害性の問題との整合性のある法解釈を行うことが，新たなる法問題の対処に法的安定性を担保する方法として有用であると思料するところである．本稿では触れなかったが，情報の保存についてはクラウドコンピューティングを用いた情報の保管方法により，児童ポルノ所持罪のような情報の保管にかかる犯罪に考慮について，これまでのハードディスクへの保管と異なる考慮をすべきなのかといった問題も残る．今後，サイバー犯罪をめぐる状況の変化を勘案しつつ，検討を進めていきたい．

1）　平成25年末時点でインターネット利用者割合は，全世代平均で82.8％であり，６～12歳の73.3％，最も利用者割合の低い80歳以上でも22.3％である．総務省ホームページ「平成26年版情報通信白書」図表5-3-1-4. http://www.soumu.go.jp/johotsusin tokei/white paper/ja/h26/html/nc253120.html（2015年９月20日時点）参照.

2）　サイバースペースの用語は，SF小説である，ウィリアム・ギブソン／黒丸尚訳「ニューロマンサー」（ハヤカワ文庫SF，1986）のなかで用いられた仮想空間を示す語である.

3）　岡田好史「サイバー刑法の概念と展望」専修法学論集118号68頁参照.

4）　我が国における発効過程については，外務省ホームページ「国際組織犯罪に対する国際社会と日本の取組」http://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html（2015年９月20日現在）参照.

5）　サイバー犯罪条約については，前掲注４）および，外務省ホームページ「サイバー犯罪に関する条約」http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html（2015年９月20日現在）参照.

6）　これらは，警察庁の分類による．四方光『サイバー犯罪対策概論』（立花書房，2014）３頁参照.

7）　警察庁ウェブサイト「平成25年度中のサイバー犯罪

の検挙情報等について」http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf（2015年９月20日現在）参照.

8） いわゆるOECD８原則にみられるように，情報の流通や適正な利用，管理を実現するために国際的な取り組みがなされている．当該原則は，1980年にOECD（経済協力開発機構）で採択された，個人情報保護の基本となるガイドラインであり，我が国の個人情報保護法においても，OECD８原則がとりいれられている．総務省ウェブサイトhttp://www.soumu.go.jp/main_sosiki/gyoukan/kanri/question01.html（2015年９月20日現在）.

9） 例えばわいせつな画像をウェブページ上に表示する，公然陳列事案などについては，その行為態様を同じくする．そのため，児童ポルノ犯罪とわいせつ物関連犯罪については同様の行為態様の事案については共通する議論がなされており，判例においても，かつてのわいせつ物公然陳列事案（最決平成13年７月16日刑集55巻５号317頁いわゆる京都アルファネット事件）の見解を，児童ポルノ法違反事案（最決平成24年７月９日判時2166号140頁）においても採用している．これについて詳しくは，拙稿「判批」法学新報120巻５・６号303頁参照.

10） いわゆるWinny事件（最決平成23年12月19日刑集第65巻９号1380頁）．わいせつ物陳列罪事案におけるFLマスク事件（大阪地判平成12年３月30日公刊物未登載，園田寿「判批」捜査研究49巻５号10頁参照）などがこれに当たる.

11） 植月献二「【EU】欧州デジタルアジェンダ：2013～2014年の重点分野」外国の立法254-2号８頁.

12） 植月・前掲注11）８頁.

13） EUにおいては，外部との個人情報の流通に際しては，対象国の個人情報保護のレベルが，EUが定める「十分な保護レベル」の要件を満たす必要がある．なお，「十分な保護レベル」に達していない場合はSafe Harbor協定を結ぶことで個別的に対応することになる．なお，アメリカ合衆国については，2000年にSafe Habor協定が結ばれている．U. S. Dept. of Com., Safe Harbor Privacy Principles（2000）, http://www.export.gov/safeharbor（2015年９月20日時点）参照.

14） ECウェブサイトhttp://europa.eu/rapid/press-release_IP-15-4865_en.htm?locale=en（2015年９月20日時点）参照.

15） これを初めて認めたBGHの判断として，BGH NStZ 2001, 596がある.

16） 個人情報の保護に関しては，民間部門と公的部門それぞれに対する規制があり，加えて医学会における医者の情報の守秘義務のような各業界内の自主的基準も存する．Vgl. Marion Albers, Patientenautonomie und Patienten-vertrauen im Gesundheitsdatenschutz, Patientenautonomie: Theoretische Grundlagen - Praktische Anwendungen（2013）, S. 121ff.

17） インターネットの発達により，国際的情報交流や共働が容易かつ当然のものとなったことが，犯罪形態影響があることを鑑みた，ドイツにおける訴追機関等の実務上の保管データの捜索について解説する近時の文献として，Holger Münch, Praktische Nutzung der „Vorratsdatenspeicherung," ZRP 2015, 130がある.

18） 鈴木良介『ビッグデータビジネスの時代』（翔泳社，2011）14頁.

19） 総務省ウェブサイトhttp://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc121410.html（2015年９月20日現在）参照.

20） 個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案（第189回国会閣法34号）36条以下の第二節匿名加工情報取扱い事業者の義務などの条項がこれに当たる.

21） マイナンバー法19条など.

22） 山口厚「コンピュータ・ネットワークとネットワークと犯罪」ジュリスト1117号74頁，只木誠「判批」現代刑事法第４巻第８号79頁以下，川端博「インターネット画像とわいせつ物陳列罪の客体」研修616号10頁など.

23） 2004/68/JHA.

24） 2011/92/EU.

25） ドイツの近時の改正としては，2015年改正があるが，これについてはMeyer-Lohkamp, Schwerdtfeger, StV 2014, 772を参照．なお，2015年改正によりポージング規制が明文化されたが，このような近時の立法状況について，批判的な考察を行うものとして，Ralf Busch, Strafrechtlicher Schutz gegen Kinderpornographie und Missbrauch, NJW 2015, 977がある.

26） なお，ドイツにおいてはGG5条４項の芸術の自由との関係で議論がある.

27） New York v. Ferber, 458 U. S. 747（1982）. ここで連邦最高裁判所は，児童ポルノの製造等を禁止するニューヨーク州法の合憲性を認め，児童ポルノは合衆国憲法第一修正条項にいう表現の自由の対象に当たらないことを明らかにしている.

28） Osborne v. Ohio, 495 U. S. 103（1990）. ここで連邦最高裁は，親や監護者以外の者による児童ポルノの単純所持を禁止するオハイオ州法を合憲であるとしている.

29） Child Pornography Prevention Act of 1996, P. L. 104-208.

30） 間柴泰治「諸外国における実在しない児童を描写した漫画等のポルノに対する法規制の例」レファレンス 58巻11号47頁参照.

31） Ashcroft v. Free Speech Coalition, 535 U. S. 234.

32） Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003, P. L. 108-21. 中川かおり「短信：アメリカ：児童を誘拐及び性的搾取から保護するための法律」外国の立法217号136頁以下参照.

33） 非実在児童を扱ったものについては，合衆国法典第18編第110章による規制に留まるとされる．中川・前掲注32）136頁.

34） これについて詳細に検討するものとして，永井善之『サイバーポルノの刑事規制』（信山社，2003）29頁以下.

35） United States v. Maxwell, 42 M. J. 568.

36） United States v. Thomas, 74 F. 3d 701.

37） Communications Decency Act of 1996.これについては，1997年 6 月16日に合衆国憲法第一修正違反として違憲判決が下されている．Cannon, Robert “The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway,” Federal Communications Law Journal: Vol. 49: Iss. 1, Article 3を参照.

38） Child Online Protection Act of 1998.これは，Ashcroft v. American Civil Liberties Union, 535 U. S. 564（2002）において合衆国憲法第一修正，第四修正違反とされ，最終的には2009年 1 月21日に連邦最高裁が司法省の訴えを退けたことで，本法は施行されないことが決定した．CNET Japanウェブページ http://japan.cnet.com/news/media/20386876/（2015年 9 月20日現在）参照.

39） 最判昭和32年 3 月13日刑集11巻 3 号997頁（チャタレー事件），最判昭和44年10月15日刑集23巻10号1239頁（悪徳の栄え事件）など.

40） これは，ICT法などを扱う情報法分野においても同様であり，新聞等のメディアと表現の自由や，知る権利，報道の自由といった憲法上の自由権利の問題が伝統的な議論の対象となる.

41） インターネットの発達により，我が国においてわいせつ物と判断されうるような画像等を，海外在住者が海外のサーバコンピュータ等にアップロードし，これを日本国内在住者が閲覧するということが可能となっている．このような状況に鑑み，国内におけるわいせつ物規制を従来どおり行なうべきかについては議論の余地があろう．逆に，我が国において合法な画像が海外においては違法であるというケースもありうる．例えば，わが国において刊行されている児童を扱った写真集などが，米国・ドイツなどの基準においては違法な書籍であるとされることもありうる．犯罪地や管轄の問題と併せて，現在のようなわいせつ概念を踏襲するのか，わいせつ概念の転換を図るべきかについては，十分に議論がなされるべきである．なお，児童ポルノ性判断についても同様の問題がある．ドイツにおいては成人ポルノについては184条の対象であり，原則として提供行為は処罰の範囲外であり，児童ポルノについてとりわけ問題となる．なお，ドイツの児童ポルノ法制については，拙稿「児童ポルノの単純所持規制に関する考察」比較法雑誌48巻 3 号277頁参照のこと．ドイツにおいてはStGB176条，176a条，176b条にいう児童に対する性的虐待の描写や，児童に性的な姿態をさせこれを描写するポージング規制（184b条の2015年改正以前から性的虐待として処罰されうると解釈されている）があるが，ここにいう「虐待」の概念は広く，児童に対しする身体的な接触を有する暴力的行為に限定されるものではなく，児童ポルノの範囲は広範である．BGH NJW 2014, 1829参照のこと.

42） 最決平成13年7 月18日 刑集第55巻 5 号317頁.

43） 山口厚「サイバーポルノとわいせつ物陳列罪―最高裁判決」ジュリスト1224号166頁．なお，これを「時間的伝播性と場所的可搬性」として，固定性と管理・利用可能性の問題とするものとして，林陽一「わいせつ情報と刑法175条」現代刑事法57号10頁など.

44） わいせつ物の客体の有体物性および公然陳列概念については，再生しなければわいせつ性を認識で

きないビデオテープがわいせつ図画に当たるかが問題となった最決昭和54年11月19日刑集33巻７号754頁があり，ここで最高裁は「記録媒体そのもの自体にわいせつ性が顕在し，そのままで視覚的にわいせつ画像を見ることが出来ることを要せず，一定の操作を施すことでその物に潜在するわいせつ性が外部から認識できる程度に顕在化することで足りる」とするとしている．その後の判例も同様の見解に立っている．

45） 拙稿・前掲注９）309頁以下参照．

46） 東京高判平成25年２月22日高刑集66巻１号６頁およびその上告審である，最決平成26年11月25日刑集68巻９号1053頁．

47） 高橋和之「インターネット上の名誉棄損と表現の自由」高橋和之，松井茂記，鈴木秀美編『インターネットと法（第４版）』（有斐閣，2010）54頁以下．

48） 高橋・前掲注47）66頁以下．

49） ハンター・ムーア（Hunter Moore）氏が “IsAnyoneUp?” というウェブサイトを開設したのが最初といわれる．http://www8.cao.go.jp/youth/youth-harm/cho usa/h25/net-syogaikoku/2_16.html（2015年９月20日現在）．

50） 我が国のみならず，米国などでも問題となっている．AFPBBニュースホームページ「普遍化する10代の「セクスティング」，リスク周知でも 米国」http://www.afpbb.com/articles/-/3028612（2015年９月20日現在）．

51） 横浜地判平成27年６月12日裁判所ウェブサイト掲載（LEX/ DB:25447325）はリベンジポルノ法違反に関し，初めて判断がなされた裁判例である．

52） 内閣府ウェブサイト http://www8.cao.go.jp/youth/youth-harm/chousa/h25/net-syogaikoku/ 2_16.html（2015年９月20日現在）．

53） Adobeウェブサイトhttp://www.adobe.com/jp/devnet/rtmp.html，および，総務省ウェブサイトhttp://www.soumu.go.jp/menu_kyotsuu/media/（ともに，2015年９月20日現在）参照．

54） Appleウェブサイト「HTTPライブストリーミングの概要」http://developer.apple.com/jp/documentation/StreamingMediaGuide.pdf（2015年９月20日現在）を参照．

55） なおこのフィルムデータは完全なデータではなかったが，再生自体は可能なものであった．

56） Sven Harms, Ist das „bloße“ Anschauen von kinderpornographischen Bildern im Internet nach geltendem Recht strafbar?, NStZ 2003, S. 650．なお，キャッシュデータの客体性を否定するものとして，Tatjana Hörnle, NStZ 2010, 704.

57） Hörnle, Münchener Kommentar zum StGB, 2. Aufl. 2012, § 184b, Rn. 37.

58） 184b条の「再現」という文言によって，再生性のないキャッシュデータについては排除できるとも考えられるが，BGH NStZ 2007, 596等はあくまで「その後の検索の可能性」を判断基準とするため，所持の概念の拡大の可能性を有する．

59） ただし，認識の無い場合でも，所持罪の成立を認める裁判例も存する．

60） Vgl. Marco Gercke, Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl., § 184 StGB, Rn. 23ff., Gercke, CR 2010, 801.

61） 文化庁ウェブサイトhttp://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h21_hokaisei/（2015年９月20日現在）．

62） 日経コンピュータウェブIT PROサイトhttp://itpro.nikkeibp.co.jp/article/COLUMN/20060315/232609/（2015年９月20日現在）．

63） WinnyによりネットワークにP接続しているPCはネットワーク参加者の意図しないファイルの授受を行うため，現代的問題として情報流出のようなセキュリティリスクも有する．

64） 門田成人「判比」法学セミナー686号127頁，亀井源太郎「判比」法学研究87巻３号１頁，永井善之「判比」新・判例解説Watch11号151頁をはじめとし多くの評釈がある．

65） 本件第一審（京都地判平成18年12月13日）は，以上から，本件では，「インターネット上においてWinny等のファイル共有ソフトを利用してやりとりがなされるファイルのうちかなりの部分が著作権の対象となるもので，Winnyを含むファイル共有ソフトが著作権を侵害する態様で広く利用されており，Winnyが社会においても著作権侵害をしても安全なソフトとして取りざたされ，効率もよく便利な機能が備わっていたこともあって広く利用されていた」とし，「被告人は，そのようなファイル共有ソフト，とりわけWinnyの現実の利用状況等を認識し，新しいビジネスモデルが生まれることも期待して，Winnyが上記のような態様で利用されることを認容」していたとして，幇助犯の故意を認めている．

なお，第二審（大阪高判平成21年10月８日）は「被告人は，価値中立のソフトである本件ソフトをインターネット上で公開，提供した際，著作権侵害をする者が出る可能性・蓋然性があることを認識し，それを認容していたと認められる」としつつも，「著作権侵害の用途のみに又はこれを主要な用途として使用させるようにインターネット上で勧めて本件ソフトを提供していたとは認められない」として幇助犯の成立を否定する．

66） なお，本件反対意見は，被告人が「侵害的利用の高度の蓋然性を認識，認容していた」として故意の成立を認める．

67） 林幹人「判批」ジュリスト臨増1453号153頁など．

68） 同様の立場として亀井・前掲注64）21頁．

69） FLマスクとは，画像に対しマスク加工を施すソフトウェアであり，かつそのマスクを画像閲覧者が容易に除去できるという画像加工ソフトである．なお，FLマスクの開発者の可罰性が問題となった事件として，大阪地判平成12年３月30日公刊物未搭載がある．これは，FLマスクがダウンロード可能なFLマスク開発者が自身のウェブページ上に，FLマスクでわいせつ画像を加工していた正犯のウェブページへのリンクを設定していた事案であり，わいせつ図画公然陳列罪の幇助とされた事案である．園田寿ホームページhttp://sonoda.e-jurist.net/data/hanrei.html（2015年９月20日現在）．

70） プロバイダにはサーバ内で他人の管理する情報にアクセスする権利を認めるべきでなく，不作為による幇助を認めるための結果回避可能性がなく，そもそも危険の発生に関して先行行為に基づく作為義務等を認めることはできず，不作為犯を認める保証人的地位がない．山中敬一「インターネットとわいせつ罪」高橋和之，松井茂記，鈴木秀美編『インターネットと法（第４版）』（有斐閣，2010）113頁以下．

71） 電気通信事業法179条は，「１．電気通信事業者の取扱中にかかる通信（中略）の秘密を侵した者は，２年以下の懲役又は100万円以下の罰金に処する．２．電気通信事業に従事する者が前項の行為をしたときは，３年以下の懲役又は200万円以下の罰金に処する．」とする．

72） 赤岩順二「プロバイダによるブロッキングと他人のための緊急避難（緊急避難救助）」『刑事法学におけるトポス論の実践―津田重憲先生追悼論文集』（成文堂，2014）55頁．ここで赤岩は，ISPによるブロッキングの構造を緊急避難の構造であると認めつつ，他人のための緊急避難であるとし，その要件について本論文中で検討している．赤岩順二「プロバイダー責任制限関連ガイドラインと緊急避難論」研究報告電子化知的財産・社会基盤（EIP）５号１頁も参照．