

アメリカにおけるサイバーいじめ 対策立法の刑法的側面

西 貝 吉 晃

第1 本稿の構成

本稿ではいわゆる「サイバーいじめ」に関するアメリカにおける刑事実体法の動向を紹介する。サイバーいじめという語は、サイバーといじめの部分に分けることができる。従来から存在したいじめの語を解きほぐしたサイバーいじめの定義例を見てみると、サイバーいじめは「自身を容易に防御することができない被害者に対して、反復的及び継続的に、グループ又は個人により行われる、電子的な接触の形式を用いる意図的な攻撃的行為⁽¹⁾」と定義されている。この定義からは、当事者間の力関係や攻撃態様について一定の具体化が得られる。もっとも、いじめは学校の構成員が当事者になることが典型的であるとされるが、上記の定義では当事者の年齢や学校教育との関係が希薄であり、それでよいのかは問題である。議論の射程を確定し、類型的な議論を可能にするためには、いじめの特徴ないし要件は何か？ということを考える必要がある。

さらに、人に恐怖感、孤独感、不快感を与える行為にはいじめ以外の態様のものもあり得る。そこで、別の規制との関係をみても必要がある。サイバーいじめと重なり合いを持ち得る規制にはサイバーハラスメントやサイバーストーキングに対する規制がある。サイバーいじめの定義を、仮に当事者の年齢等を問わない等として広く考えると、サイバーいじめの規制に教育の現場における行為とは関係ない行為が

全てこれに含まれ、サイバーいじめの規制がサイバーハラスメントやサイバーストーキングの規制に接近し、結果、他の規制と同一視される可能性も生じる。まず、本稿におけるいじめの定義を考える必要がある。

一方で、いじめの定義を解きほぐすことなく、サイバーいじめを「電子的手段（インターネット、email、ブログ、ウェブサイト、チャットルーム、オンラインゲーム…）用いたいじめ⁽²⁾」と捉えることもある。電子的手段という語の意味を考えるのであれば、従来型のいじめと比較する形で、サイバー固有の特徴の議論（インターネット、email等の使用により何が変わったか？といった議論）が出てくることになるだろう。サイバーいじめが、従来型のいじめと異なり、その規制方法についても独自のものが要求されるという立論があり得るのならば、それはなぜか、という問いが生じるだろうし、また、それに応える必要が出てくる。そこでの応答の素材として、サイバーいじめの特徴論を考えておくことが必要である。

そこで、第2において、本稿なりにサイバーいじめを定義した後、第3でサイバーいじめの特徴を述べていきたい。以上の議論を経て、議論の次元や軸を整理した上で、具体的な法律や法律案の検討を行う。

- (1) Kowalski, Limber & Agatston, *Cyberbullying* second edition, 3 What is Cyberbullying (2012).
- (2) Servance, *Cyberbullying, Cyber-Harassment, and the Conflict Between Schools and the First Amendment*, 2003 *Wis. L. Rev.* 1213, 1219 (2003), Hinduja & Patchin, *Overview of Cyberbullying*, in *White Paper for the White House Conference on Bullying Prevention* 21, 21 (2011). [Stopbullying.gov](http://www.stopbullying.gov) (<http://www.stopbullying.gov/cyberbullying/what-is-it/index.html>)

第2 サイバーいじめの定義論—本稿における議論方法—

サイバーいじめの定義に関し、刑事法の観点からみて巧みな定義が

できるのであれば、サイバーいじめ罪という犯罪を他の隣接する犯罪と明確に切り分けつつ定義することが可能になるから、それを議論すれば足りる。しかし、アメリカでは、サイバーいじめを定義すること自体が難しいとされているのが現状である⁽³⁾。さらに、我が国への示唆を得るに当たり、そもそもアメリカにおける“bullying”と我が国におけるいじめとの間に概念上の差異があるかもしれない⁽⁴⁾。

そこで、ここでは法的な文脈におけるサイバーいじめのいくつかの定義を紹介しつつ、定義自体を検討したい。

まず、サイバーいじめを「電子的手段（インターネット、email、ブログ、ウェブサイト、チャットルーム、オンラインゲーム等）を用いたいじめ⁽⁵⁾」と広く捉える考え方がある。職場におけるいじめを問題視する考え方もあるが⁽⁶⁾、この広い定義によればそれをも取り込んで考えることになる。現実の立法においても、サイバーいじめを、電子的手段を用いたいじめといったように、少ない要件で広く定義する例もある。例えば、F.S.A. § 1006.147（フロリダ州）、M.G.L.A. 71 § 370(a）（マサチューセッツ州）、NRS 388.123（ネヴァダ州）、T.C.A. § 49-6-4502（テネシー州⁽⁷⁾）の各規定がそうである。

次に、上記の定義に加え、当事者の年齢をサイバーいじめの要件とする考え方がある。この考え方は、例えば加害者と被害者の双方が未成年であることを要求する⁽⁸⁾。被害者を未成年に限定することの基礎には、例えば自身を容易に防御することができない性質⁽⁹⁾といった、子供の類型的な脆弱性がある。子供達は大人と比べてより脆弱で、親や学校の管理者にいじめの報告をすることに恐怖するという主張⁽¹⁰⁾は是認されるように思われ、それゆえに、被害者としての子供達にはより手厚い保護が必要だということになる⁽¹¹⁾。一方で、加害者に対しても年齢的な要件は必要になるのだろうか。確かに、10代の子供は、しばしば自身の怒りや欲求不満を「大人」のように表現することが未成熟ゆえにできないと指摘されることもあるが⁽¹²⁾、これでは未成熟な大人による加害行為が少ないことを示していることにはならないので、

大人を加害者から除外する理由にはならない。いじめの典型かもしれない、例えば加害者が学校のクラスメートである、といった事情を重視するのであれば、加害者の年齢が重要な要素になってくるが、被害者の場合と比較し、加害者側が未成年であることをサイバーいじめの要件とする理由は未だ不明確なように思われる。

さらに、教育的文脈で行われる行為と一般の社会的文脈で行われる行為とを区別し、教育的文脈で行われる行為に限るとする説もある⁽¹³⁾。この説は、学生たる大人をも議論の対象に含めるために、教育の場に参加している者の年齢を問わない点で上記の整理とは異なる⁽¹⁴⁾。この考え方を突き詰めると、サイバーいじめの有する心理的な負の効果（憂鬱、学業不振、自殺⁽¹⁵⁾）により、教育現場における教育目的の達成が難しくなると考えれば、他の学生の教育を受ける権利の侵害が問題になり、さらには一定の水準を有するべき学校環境自体が保護されるべきだといえるかもしれない⁽¹⁶⁾。その場合には、例えば教育機関の職員に対するサイバーいじめを肯定する場合、刑を加重する要素となり得るだろう。

以上、大きく分けて3つの考え方を紹介したが、年齢や教育過程といった+ α の「要件」をサイバーいじめであるための要件として加える場合には、+ α の要件を充たさない事案を検討対象からおよそ外すことになってしまう。この手法にはサイバーいじめを広く捉える説が提示する当罰性のある類型を見落とすリスクが含まれている。

このような弊害を避けるため、本稿では、サイバーいじめの定義として最も広い定義である「電子的手段（インターネット、email、ブログ、ウェブサイト、チャットルーム、オンラインゲーム等）を用いたいじめ」を採用して議論していくことにする。もっとも、これではいじめの部分が具体化されていないので、いじめについての「自身を容易に防御することができない被害者に対して、反復的及び継続的に、グループ又は個人により行われる、電子的な接触の形式を用いる意図的な攻撃的行為⁽¹⁷⁾」という定義も重畳して採用したい。この定義中の、意図的な

行為とか反復的な行為、そして電子的手段の利用の要素は、基本的にどの論者も同様に要件にしている⁽¹⁸⁾ので議論を拾いやすい。

以上の帰結は字義通りであり、まず、反復的ないし継続的という部分は、伝統的ないじめとサイバーいじめの共通点、すなわちいじめの特徴を示した叙述に他ならず、サイバーいじめにおいて新しく争われることになったものではないといえる。また、電子的手段の利用についてもサイバーという語と対応している、と考えることができる。

もっとも、この定義は、サイバーいじめというために関与者の年齢や教育現場への関与の有無を問わないものであり、成年が関わる場合ないし成年しか関わらない場合のサイバーハラスメント、サイバーストーキングはサイバーいじめと重なりあってくる⁽¹⁹⁾。また、学校の教師が被害者になるような場合もサイバーいじめたり得ることになる⁽²⁰⁾。

一方で、この定義は若者が主たる被害者となっていることまで否定しているわけではない⁽²¹⁾。議論上のメリットもある。例えば、子供の保護をベースにしつつ、同時に学校の職員等（大人）を保護したい場合には、立法作業において客体を追記するという手法も合理的なものとしてあり得る。現にそのような立法もなされている⁽²²⁾。広い定義を用いることで定義が捕捉する範囲内で比較を行うことができるようになる。本稿の定義においては、若者が被害者となる場合はサイバーいじめの要件ではなく、法律論を展開する際の重要な考慮要素として考慮されることになる。

- (3) Phillips, Online Bullying and the First Amendment: State Cyberbullying Statutes after *People v. Marquan M.* 93 N.C. L. Rev. Addendum 179, 183 (2015). 様々な定義がなされるとする者に Cyberbullying and Other Online Safety Issues for Children: Hearing before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 111th Cong. 1 (2009). 共通の理解に基づく定義はないとする者に Brady, Criminal State Anti-Cyberbullying Statute: Does Legislative Zeal Outweigh Constitutional Considerations?, 298 Ed. Law Rep. 21, 23 (2013), Rose, From Lol To Three Months In Jail: Examining

The Validity And Constitutional Boundaries of The Arkansas Cyberbullying Act of 2011, 65 Ark. L. Rev. 1001, 1003 (2012).

- (4) 小野淳、斎藤富由起「『サイバー型いじめ』(Cyber Bullying)の理解と対応に関する教育心理学的展望」千里金蘭大学紀要5巻35頁、39頁(2008)。
- (5) Servance, *supra* note 2, at 1219, Hinduja & Patchin, *supra* note 2, at 21, Stopbullying.gov, *supra* note 2.
- (6) Lipton, Combating Cyber-Victimization, 26 Berkeley Tech. L.J. 1103, 1109-1110 (2011). 同論文でLiptonが引用するWorkplace Bullying 'Epidemic' Worse than Sexual Harassment by Jeanna Bryner (March 7, 2008 07:00pm)は、職場におけるいじめとして「継続的に (persistently) 従業員の業務を批判すること; どなること; 反復的に (repeatedly) 従業員にミス (mistake) を思い出させること; ゴシップ若しくは嘘を広めること; 従業員を無視若しくは排除すること; 及び、従業員の習慣、態度、若しくは私生活を侮辱すること」を挙げている。
- (7) 別の定義例もある。サイバーいじめではなく、bullyingの定義の中に、電子的行為(電子的手段の利用、電子的通信)を含める形式を取る例として、Ann.Cal.Educ.Code § 48900(r)(1)(カリフォルニア州)、C.R.S.A. § 22-32-109.1(1)(b)(コロラド州)、C.G.S.A. § 10-222d(a)(1)(コネチカット州)、14 Del. C. § 4112D(a)(デラウェア州)、Ga. Code Ann., § 20-2-751.4(a)(ジョージア州法、いじめにはサイバーいじめを含む)。さらに、サイバーいじめを罪名(見出し)にして、犯罪行為として書き下しているものとして、A. C.A. § 5-71-217(アーカンソー州)がある。
- (8) Stopcyberbullying.org, What is Cyberbullying, Exactly? (http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html), Barnett, Cyberbullying: A New Frontier And A New Standard A Survey of And Proposed Changes To State Cyberbullying Statutes, 27 Quinnipiac L. Rev. 579, 581 (2009).
- (9) Kowalski, Limber & Agatston, *supra* note 1, 2 Children's Experiences with Traditional Forms of Bullying.
- (10) King, Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech, 63 Vand. L. Rev. 845, 874 (2010) [若者(youth)はサイバーいじめに特にせい弱]。
- (11) What is Cyberstalking and What is Cyberharassment? (<https://www.wiredsafety.com/parry-aftabs-did-u-know---cyberstalking>).
- (12) Fertik & Thompson, Wild West 2.0: How to Protect and Restore Your Online Reputation on the Untamed Social Frontier 2, 106 (2010).
- (13) Brenner & Rehberg, "Kiddie Crime"? The Utility of Criminal Law in Controlling Cyberbullying, 8 First Amend. L. Rev. 1, 2 (2009).

- (14) Brenner & Rehberg, *supra* note 13, at 2.
- (15) Megan Meier Cyberbullying Prevention Act, H.R 1966, 111th Cong. § 2 (4), (5) (2009), Brady, *supra* note 3, at 24, Burr Richter, Cyberbullying 2.0: A “Schoolhouse Problem” Grows up, 60 DePaul L. Rev. 141, 161 (2010).
- (16) 例えば、州法の規定のうち、N.R.S. 392.915.1(c) (ネヴァダ州) は、犯罪の成立要件のうちの意図の部分で「学校の業務 (operation) を妨害する」を要件とする。
- また、例えば、一定の言論に対する校内処分の是非を巡って争われた事案である、Tinker v. Des Moines Independent Community School Dist, 89 S.Ct. 733, 738 (1969) (事案等の詳細は後掲注 139) 参照) は、処分対象となる禁止行為の遂行が、言論の自由との関係で、「『学校の運営における適切な規律の必要を実質的かつ著しく妨害する』という認定や示唆がない場合には、当該禁止は維持され得ない」と述べ、また、89 S.Ct. 733, 737 では、学校の業務に加え、他の学生の安全でいられて干渉されない (be let alone) 権利についても触れている。
- (17) Kowalski, Limber & Agatston, *supra* note 1, 3 What is Cyberbullying.
- (18) Barnett, *supra* note 8, at 580-581, Hinduja & Patchin, *supra* note 2, at 21, Stringer, Cyberbullying: Louisiana’s Solution To Confronting The Latest Strain of Juvenile Aggression, 72 La. L. Rev. 1129, 1134 (2012) 等参照。
- (19) Kowalski, Limber & Agatston, *supra* note 1, 3 What is Cyberbullying.
- (20) Shariff, Cyber-bullying, Chapter 7 Balancing free expression, Legal frameworks (2008) (Kindle version) は、サイバーいじめの一類型として anti-authority cyber-insubordination を挙げる。また、Erb, A Case For Strengthening School District Jurisdiction to Punish off-Campus Incidents of Cyberbullying, 40 Ariz. St. L.J. 257, 259 (2008) も参照。
- (21) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 1 や Henderson, High-tech Words Do Hurt: A Modern Makeover Expands Missouri’s Harassment Law To Include Electronic Communications, 74 Mo. L. Rev. 379, 381 (2009) は、大人も加害者ないし被害者になり得るが、多くの場合は子供が関わる事案であるという指摘をする。また、Rose, *supra* note 3, at 1003 は、サイバーいじめの概念自体を広く捉えつつも、どのような年齢の者に対してもサイバーいじめは起こり得るが、よくあるのが被害者が 10 代の場合だと述べる。
- (22) 例えば、罰則に関してみると、ネヴァダ州法のような、目的要件の中に生徒の横に学校の職員を追記する例 (N.R.S. 392.915 1(a))、ノースカロライナ州法のような、枝番として学校の職員が被害者になる場合を規定する例 (N.C.G.S.A. § 14-458.2. この規定の直前の N.C.G.S.A. § 14-458.1 は、未成年者及びその両親や後見人を保護している) がある。

第3 サイバーいじめの多様な行為形式と特徴

1 サイバーいじめの表出形態

サイバーいじめは実に多様な形態で行われ、その分析は容易ではない。Willardの研究等⁽²³⁾では、オンラインでの喧嘩 (flaming)、ハラスメント、噂話等による侮辱 (denigration)、なりすまし (impersonation)、アウトティング (outing)、騙し⁽²⁴⁾ (trickery)、排除 (仲間はずれ、exclusion)、サイバーストーキング⁽²⁵⁾が挙げられている。

本来は、それぞれの行為類型を精密に分析して、侵害される利益の共通項や差異を炙り出していくべきであろう。しかし、調査の結果、行為類型別の検討を行うほど議論が整理されていない状況であることがわかった。そこで、行為類型毎の検討ではなく、サイバーいじめの特徴論を述べ、言及された特徴を有するサイバーいじめに対する対策論として、立法論を含む法律論を検討するという方法を採用したい。

2 サイバーいじめの特徴—伝統的ないじめ (traditional bullying) との相違点—

サイバーいじめはいじめの一種であるから伝統的ないじめと原則的には同様の特徴を有する部分がある⁽²⁶⁾。例えば、サイバーいじめも、通常のいじめと同様に、抑うつ、不安を含む負の心理的及び行動的な効果、危険な行動、自傷行為、並びに自殺と関係がある⁽²⁷⁾。この指摘はサイバーいじめを規制する際の保護法益の特定に資する。

もっとも、サイバーいじめを論じる際に重要なのは、両者の間の類似性ではなく、むしろサイバーいじめ固有の特徴、すなわち両者の間の相違点である⁽²⁸⁾。例えば、サイバーいじめの方が通常のいじめよりも自殺とより関係している、といった類の指摘⁽²⁹⁾が重要である。伝統的ないじめと同様の規制立法が適切か否かの判断において重要な考慮要素になるから、深く掘り下げた考察をすべきであろう。

(1) 場所の無限定性

そもそもサイバーいじめの発生地点を特定するのは容易ではない⁽³⁰⁾

という指摘だけでなく、サイバーいじめには、それが（どこからでもアクセス可能な）サイバースペースにおいて行われるため、場所が学校に限定されない⁽³¹⁾という特徴があることが指摘される。行為が学校のネットワークを使って行われるか否かは物理的な場所とは別の問題であり、このことが議論を複雑化させることもある⁽³²⁾。

〔オンキャンパスとオフキャンパス〕

この文脈でオンキャンパスとオフキャンパスという語が使われることがある。オンキャンパスとは、物理的に学校の中における行為のこと、オフキャンパスとは学校の外における行為のことをいう。多くの場合、学生が当事者となること、そして学校における学生の言論に対しては、通常の大人の言論に対する場合よりもより強い規制が認められ得るので⁽³³⁾、分けて考察することにも理由がありそうに見える。しかし、サイバーいじめがオフキャンパスで（学生の自宅で）行われている、という指摘⁽³⁴⁾からすれば、サイバーいじめの議論においてキャンパス内外を分けることの有意性には疑問が呈され得る。

(2) 匿名性

被害者側において誰が加害者であるかを知っているサイバーいじめの事案もある⁽³⁵⁾。一方で、それは、匿名でデータの送受信が可能であることに基づき⁽³⁶⁾、匿名の攻撃（“anonymous” attack）としても行われ得る⁽³⁷⁾。

① 技術的な特定可能性とは無関係であること

ここでいう匿名とは、技術的な特定可能性がないということではない。サイバーいじめの文脈では、加害者が特定していない段階において、いじめに関するメッセージがやり取りされ、その時点で心理的な被害が発生してしまうことが問題となる⁽³⁸⁾からである。したがって、技術的にみて特定できる場合であっても、しばらく特定できない状態が続き、不安が惹起され得るのであれば匿名の攻撃である。

② 被害の増大—加害行為の激化と被害者の恐怖、不安の増大

被害者が加害者の属性（人数、性別、知り合いか否か等）を識別できな

くなる⁽³⁹⁾、という意味で、匿名性は、被害者の恐怖、不安を増大させ得る要因であり、加害者自身の行為の激化の要因でもある。

すなわち、(リモート環境における行為であるがゆえに)加害者がいじめの作り出す感情的な被害状況を見ない場合があること⁽⁴⁰⁾が原因で、例えば、電話でさえ言わないようなことを告げてしまう等⁽⁴¹⁾、悪影響を明確に察知し得る対面関係と比較して、行き過ぎた行為に至りやすくなる⁽⁴²⁾。結果として、加害者には、抑制されない自信(uninhibited confidence)による、無責任なコメントをする傾向が生じる⁽⁴³⁾。

被害者の不安の増大や加害者の行為の激化が組み合わさることで、典型的に侵害の程度が大きくなりやすい、といえそうである。

(3) コピーの容易性とネットワーク接続から導かれ得る特徴

さらに、デジタルデータのコピーの容易性や一度に多数の者へデータの送付が可能であること⁽⁴⁴⁾及びネットワーク接続を基礎として発生する通信の即時到達性、同時送信可能性等の技術的特性が、サイバーいじめの文脈でも被害の増大を招いている。

① 伝搬容易性(拡散容易性)

まず、emailの多数人への転送やSNSへの投稿等による情報の伝搬・拡散が、他の情報伝達手段と比較すると、容易⁽⁴⁵⁾(=低価かつ時間的コストがかからない)、かつ迅速である⁽⁴⁶⁾。ブログ等のインターネット上での情報の提示については検索が容易であるがゆえに情報が伝わりやすい⁽⁴⁷⁾。無限の聴衆がいる⁽⁴⁸⁾、公開のいじめを行うことができる⁽⁴⁹⁾、といえる状況がある。伝搬の程度が甚だしくなれば、情報源がそもそも誰だったのかがわかりにくくなる⁽⁵⁰⁾。これは(2)で述べた匿名性の助長につながる。

② 侵害の持続性

いじめの内容が特定のウェブサイトに存続することで⁽⁵¹⁾、攻撃から逃げるできない状態が作出される⁽⁵²⁾という特徴が指摘される。(他者の管理下にデータがある場合に)削除が難しいというだけでなく⁽⁵³⁾、コンピュータを閉じて一時的に見ないようにすることはできても、コ

ンピュータを再度起動すれば、そこに残存するメッセージに直面することを余儀なくされる⁽⁵⁴⁾。あるウェブサイトからの削除に成功しても、①で述べた伝搬の容易性に基づき、既に別のサイトにキャッシュされていたりコピーされていたりする場合もある⁽⁵⁵⁾。

もちろん、行為者の行為が1回きりの場合もあり得、その場合には、その行為だけ切り取ってみると、大きな問題にはならないように思えるかもしれない。しかし、上記の状態が作出され得ることは、行為者の行為を傍観する者が存在するという事実が続くことで、行為者と被害者の力の不均衡が発生し、ひいては継続的な攻撃によって被害者がよりぜい弱になる⁽⁵⁶⁾ということも意味する。つまり、多数人に閲覧され得る状態で、行為の痕跡が消えず、これに対する反論もないという事実が継続することで、継続的な侵害が発生するのである。一般論として、いじめにおいては、力の不均衡が関わりとされることが多いが⁽⁵⁷⁾、サイバー空間は、力の不均衡が発生させやすい場、つまりいじめが起りやすい場だといえる。

③ 同時攻撃可能性

複数のコンピュータから特定のターゲットに対し、同時に攻撃が可能である。多くの人が同一のターゲットを同時に攻撃可能⁽⁵⁸⁾であるだけでなく、加害者が複数のIDを用いて被害者とコミュニケーションをとり得るので⁽⁵⁹⁾、物理的には1人の加害者であっても多数人のふりをして複数のメディアを介して攻撃することも可能である⁽⁶⁰⁾。

多数人のふりをする事例は(2)で述べた匿名性が確保されている前提において成功する攻撃であるから、実世界で誰が攻撃を行っているかを検証するのは容易ではないことからすれば、この特徴が発現している事例が相当程度あり得る。

(4) 小括

以上のように、サイバーいじめには、伝統的ないじめと比較して、被害を拡大・助長させる方向の特徴がある。(3)②で述べた被害者が孤立しやすいといった事情はいじめとの固有の関連性が強い特徴だとい

えるだろうが、基本的には、サイバーいじめ固有のものというよりはサイバー犯罪に共通する特徴（匿名性、非対面、コピー容易性、同時攻撃可能性）も相当程度ある。このことはサイバーいじめ自体が多種多様な態様で現われること（1参照）とも関連しよう。

さらに、このような特徴を有するサイバーいじめを抑止するための方策について検討していきたい。数ある対策の有効範囲を簡潔に確認した上で法規制の方法を考えていく。

- (23) Willard, Educator's Guide to Cyberbullying and Cyberthreats (<https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx>), Espelage, Hong and Valido, Cyberbullying in the United States IN International perspectives on cyberbullying, edited by Baldry, Blaya and Farrington, 65 (2018).
- (24) 騙して秘密を暴露させる等。
- (25) 反復的で激しいハラスメント及び侮辱（脅迫や著しい恐怖を覚えさせる行為を含む）。
- (26) Online Safety and Technology Working Group, "Youth Safety on a Living Internet", 13, (2010) (<http://www.ntia.doc.gov/legacy/advisory/onlinesafety/index.html>), Stringer, *supra* note 18, at 1134.
- (27) Espelage, Hong and Valido, *supra* note 23, at 66.
- (28) 最近では、ハラスメントの文脈で、ニューヨーク州刑法 § 240.20 と § 240.30 とを比較し、端的に、電子的手段を介したハラスメントは対面のハラスメントより大きな社会的害悪をもたらすので刑が加重されている、と述べるコンピュータ犯罪に関する論稿もある（Simmons, "The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime", 84 Geo. Wash. L. Rev. 1703, 1706 (2016)）。
- (29) Espelage, Hong and Valido, *supra* note 23, at 66.
- (30) Barnett, *supra* note 8, at 584.
- (31) Brenner & Rehberg, *supra* note 13, at 3. この議論は当然サイバーいじめに限らない（Lipton, *supra* note 6, at 1113 参照。）
- (32) オンキャンパスの類型を、例えば On-Campus Internet Cyberbullying [学校の所有ないし維持するコンピュータ、又は、学校のネットワークにアクセスしている個人用の PC を利用して行われる場合（Barnett, *supra*

- note 8, at 584)〕 と On-Campus Use of Personal Technology That Does Not Access the School's Network [オンキャンパスでの、学校のネットワークにアクセスしない私用の技術の使用 (Barnett, *supra* note 8, at 586)〕に分けることも可能である。
- (33) Bethel School District No. 403 v. Fraser, 478 U.S. 675, 682 (1986).
- (34) Enoc, Combating Cyberbullying: When Legislation Goes Too Far, 45 J.L. & Educ. 435, 440 (2016).
- (35) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 1.
- (36) Burrichter, *supra* note 15, at 144.
- (37) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 1, Leahy, Proof of Cyberstalking and Cyberbullying, 34 Am. Jur. Proof of Facts 3d 115 (August 2016 Update), I § 1, Phillips, *supra* note 3, at 183, Stringer, *supra* note 18, at 1135 等。
- (38) King, *supra* note 10, at 850.
- (39) Kowalski, Limber & Agatston, *supra* note 1, How Cyberbullying Differs from Other Types of Bullying, The enemy you know..., Barnett, *supra* note 8, at 583.
- (40) Barnett, *supra* note 8, at 583, Leahy, Proof of Cyberstalking and Cyberbullying, 34 Am. Jur. Proof of Facts 3d 115 (August 2016 Update), I § 1, Rose, *supra* note 3, at 1005, Stringer, *supra* note 18, at 1135.
- (41) King, *supra* note 10, at 850.
- (42) Leahy, Proof of Cyberstalking and Cyberbullying, 34 Am. Jur. Proof of Facts 3d 115 (August 2016 Update), I § 1, Rose, *supra* note 3, at 1005.
- (43) Burrichter, *supra* note 15, at 144.
- (44) Kowalski, Limber & Agatston, *supra* note 1, How Cyberbullying Differs from Other Types of Bullying, Brady, *supra* note 3, at 23.
- (45) King, *supra* note 10, at 850. Servance, *supra* note 2, at 1219, Lipton, *supra* note 6, at 1112, Fertik & Thompson, *supra* note 12, at 106, Stopbullying.gov, *supra* note 2.
- (46) Lipton, *supra* note 6, at 1112.
- (47) Lipton, *supra* note 6, at 1112.
- (48) Shariff, Cyber-bullying, Chapter 2 Profile of traditional and cyber-bullying, Characteristics of cyber-bullying, An infinite audience (2008) (Kindle version). Stringer, *supra* note 18, at 1136 も参照。
- (49) Brenner & Rehberg, *supra* note 13, at 13.
- (50) Stopbullying.gov, *supra* note 2.
- (51) King, *supra* note 10, at 850, Kowalski, Limber & Agatston, *supra* note 1, 3 What is Cyberbullying, Rose, *supra* note 3, at 1005, Phillips, *supra*

note 3, at 183-184, Lipton, *supra* note 6, at 1112, Fertik & Thompson, *supra* note 12, at 106.

(52) Rose, *supra* note 3, at 1005.

(53) Stopbullying.gov, *supra* note 2.

(54) Kowalski, Limber & Agatston, *supra* note 1, 3 What is Cyberbullying, Stringer, *supra* note 18, at 1135. さらに Lipton, *supra* note 6, at 1113 も参照。

(55) Lipton, *supra* note 6, at 1112.

(56) Shariff, *supra* note 48.

(57) Brenner & Rehberg, *supra* note 13, at 4, Stringer, *supra* note 18, at 1133. ここでいう力には、物理的な力、社会的な権力又は地位が含まれる (Kowalski, Limber & Agatston, *supra* note 1, 2 Children's Experiences with Traditional Forms of Bullying.)。

(58) Leahy, Proof of Cyberstalking and Cyberbullying, 34 Am. Jur. Proof of Facts 3d 115 (August 2016 Update), I § 1.

(59) Kowalski, Limber & Agatston, *supra* note 1, 3 What is Cyberbullying.

(60) Rose, *supra* note 3, at 1005, Phillips, *supra* note 3, at 183.

第4 法規制の導入の是非

法規制は、サイバーいじめの解決のために採り得る唯一の手段ではない。非法的な手段（教育、訓練、カウンセリング等）も実効的なことがあり、併用が求められる⁽⁶¹⁾。

例えば、事前に、学生に対してインターネットの利用法についての教育を行うことは重要である⁽⁶²⁾。もっとも、これだけで全ての事案を抑止できるわけではない。現実にいじめの事案が発生してしまった場合には早期発見を前提とした適切な対応が必要になろう。ここでは、学校等の大人による監視及び処分の実効性の不十分性⁽⁶³⁾に基づく事案の発見の困難さが問題となる。この点は、親や教育機関の事実上の関与によるいじめ防止体制の構築等といった、教育学・社会学的見地からの議論が必要であるゆえに、本稿で網羅的な紹介をすることはできないものの、指摘されている事項は、例えば次のようにまとめることができる。

まず、個別具体的なサイバーいじめ事案の発見や解決に当たっては両親の適切な関与が必要になるものの⁽⁶⁴⁾、両親に絶えず監視を要求するのは、インターネットの総利用時間を考えると現実的でない⁽⁶⁵⁾。そうすると、一定の監視を行うと共に、子供達からの報告にも期待せざるを得ない。しかし、実際には現実にいじめられている子供の一部しかいじめの事実を他人に相談しない（ないし相談することをいやがる）という⁽⁶⁶⁾。例えば、通常のいじめと比較してサイバーいじめを受けた生徒は、大人に報告しにくい傾向があることが指摘されている⁽⁶⁷⁾。本来は、両親が子供に対して技術へ触れることを禁止することは、当該技術を用いることで、教育や雇用の機会、及びヘルスケアに関する情報を得、それにより現代社会に参加することができるという現状を考慮すると妥当ではない⁽⁶⁸⁾。にもかかわらず、現実には、例えば、多くの両親は、子供からいじめの報告を受けるとコンピュータ等の利用をさせないようにし、そのこと自体が被害者の報告を抑制し、被害者を苦しめていると指摘される⁽⁶⁹⁾。例えば、アーカンソー州のサイバーいじめ処罰立法を促したサラ事件では、被害者サラとサラの母親はサイバーいじめの場となった MySpace アカウントにおいてフレンド関係にあったところ、その関係が継続していれば母親による適時の適切な介入が期待できた可能性があったが⁽⁷⁰⁾、いじめの書き込みが始まった時点でサラの方からフレンド関係を消去してしまっただけで母親がサラの受けているいじめを全く閲覧することができなくなってしまい⁽⁷¹⁾、最終的にサラは悪意のあるメッセージを処理しきれなくなって自殺をしてしまった。このような事案の存在も踏まえると、子供、とりわけ現在進行形でいじめられている子供からの大人に対する適時の報告や正しい判断へ期待することは困難だといえそうであり、大人による監視の困難性と相俟って、適時にいじめの発見及び介入ができる、という前提を採ることができなくなる。

次に、いじめを発見できたとしても対応困難な場合がある。相手が誰であるかを高度な蓋然性をもって推認できる場合もあり、場合に

よっては、加害者の両親をも交えたカウンセリングが有効な場合もあるろう⁽⁷²⁾。このような、一定の好条件下における推奨される対応を議論すること（成功事例を共有すること）もいじめの深刻化を未然に防ぐ対策についての議論としては重要かつ有益であることは確かである。しかし、匿名性による監視困難性も原因となって⁽⁷³⁾、相手が誰かわからず対応が困難な場合もあり得る。さらに、サイバーいじめは相当の割合のものが学校の外で行われているが、その場合には、学校の関係者は、介入の義務を相対的に感じない、という指摘もなされており⁽⁷⁴⁾、このような傾向は、学校側の介入を期待できない可能性を示している。

以上のように、法律を使わずにサイバーいじめを適切に事前抑止ないし早期解決することへのハードルは低くない。にもかかわらずサイバーいじめは決してレアな現象ではない⁽⁷⁵⁾。自殺事件もしばしばニュースで報告されてきた。そうであれば、確かに、法律は基本的に事後的解決を図るものであって⁽⁷⁶⁾、それだけでいじめにより受けた被害がなくなるわけではなく、罰則を展開しても子供達が報告に消極的なのであれば証拠収集が困難になってしまうという懸念は指摘されるものの⁽⁷⁷⁾、法律に一定の予防効果に期待することも⁽⁷⁸⁾、解決のための1つのアプローチだといえるだろう。このような状況の下、現実には、サイバーいじめ対策としての方法として、法規制が一定程度なされている。そこで、第5において、本稿の主題たるアメリカにおける刑事実体法的規制について紹介していくことにしたい。

(61) King, *supra* note 10, at 880.

(62) Meredith, *Combating Cyberbullying: Emphasizing Education over Criminalization*, 63 FED. COMM. L.J. 311, 334 (2010).

(63) Burrichter, *supra* note 15, at 142.

(64) Barnett, *supra* note 8, at 588.

(65) Burrichter, *supra* note 15, at 169, Fertik & Thompson, *supra* note 12, at 107.

(66) Kowalski, Limber & Agatston, *supra* note 1, 2 *Children's Experiences with Traditional Forms of Bullying*, Barnett, *supra* note 8, at 588.

- (67) Espelage, Hong and Valido, *supra* note 23, at 66.
- (68) Online Safety and Technology Working Group, “Youth Safety on a Living Internet”, 16 (2010) (<http://www.ntia.doc.gov/legacy/advisory/onlinesafety/index.html>). 社会的に子供達にソーシャルメディアを止めさせることは難しいという指摘もあるが (Phillips, *supra* note 3, at 183)、本文で述べたニュアンスのように、生活の一部になっているので切り離せない (切り離すべきではない) と考えるべきだと思われる。
- (69) Kowalski, Limber & Agatston, *supra* note 1, 3 What is Cyberbullying. これに関連し、例えばソーシャルネットに慣れていないといった理由で (Rose, *supra* note 3, at 1005)、いじめ行為の監視を行う技術的なノウハウを、多くの両親や教師が有していない (Kowalski, Limber & Agatston, *supra* note 1, 5 What parents can do?, Parents often are not present in the online environment of children) と指摘される。本文のような弊害を回避し、両親へのいじめの情報の告白を促進するためには、両親の方で、子供達がオンラインのインタラクションで使っているものに慣れておく必要があるが、技術の早い進展も考慮すると、これは容易ではない。
- (70) Should More Attention be Payed to Suicide (<http://sophiecad.blogspot.jp/2015/06/sarah-lynn-butler.html>).
- (71) Young, Online Teasing Leads to Teen’s Suicide, kait8.com (November 24, 2009), (<http://www.kait8.com/story/11566204/online-teasing-leads-to-teens-suicide?>).
- (72) Kowalski, Limber & Agatston, *supra* note 1, 5 What parents can do?, Contacting the Parents of a Child Who Cyberbullies [サイバーいじめにおける言論は辛辣なものが多いので、加害者の両親も、加害者を弁護しようとせず、事件の解決に前向きになりやすい、ということも指摘される] .
- (73) Burrichter, *supra* note 15, at 143.
- (74) Kowalski, Limber & Agatston, *supra* note 1, 3 What is Cyberbullying.
- (75) Burrichter, *supra* note 15, at 142.
- (76) Stringer, *supra* note 18, at 1143.
- (77) Phillips, *supra* note 3, at 187.
- (78) Rose, Cyber-bullying: Its Recent Emergence and Needed Legislation To Protect Adolescent Victims, 13 Loy. J. Pub. Int. L 219, 234-235 (2012). Stringer, *supra* note 18, at 1143 は、予防効果を肯定しつつも、それは、学生が法律及び法律による示唆に気づいているときにしか実効的ではない、と述べる。

さらに Espelage, Hong and Valido, *supra* note 23, at 71 は、(他者支配の欲求や優越感と併置してはいるものの、) サイバーいじめを許容するような態度が、サイバーいじめの永続化と関係していると述べている。このことは、本文で述べた、サイバーいじめを規制することへの予防効果と関

係し得る。

第5 立法方法論

第4でみたように、立法による法規制への効果が期待されていることは認めてよさそうである。しかし、どのような法規制が妥当なのかは、第2、第3でみてきたサイバーいじめの行為態様の多様さや定義自体の多義性が障害となって、議論が容易ではない。

そもそも、これから議論していく事柄ではあるが、例えば新たにサイバーいじめを連邦の犯罪にしようとする法案に対しては、既存の犯罪で十分であるという反論がなされていた。困惑する事柄を伝えることを規制するハラスメント罪や、触ったり、つきまとい行為をしたりすることを規制するストーキング罪等の罪に該当するレベルに達し次第、それらの罪を利用することで十分だという議論⁽⁷⁹⁾や、広げるとしても既存のストーキング罪の規定を使うべきだ、という議論⁽⁸⁰⁾である。しかし、現在の州法の状況を見る限り、様々な方法で、独立にサイバーいじめの処罰をする規定が整備されつつある。そこで、アメリカにおけるサイバーいじめ罪と他罪との包摂関係を重点的に考えるというよりは、本稿では主にサイバーいじめ立法の方法論について検討していきたい。

検討の前提として重要となるのが、第一に合憲性確保のための基準の議論⁽⁸¹⁾であり、第二に第一の視点で得られた基準への適合性の議論も含めた、主に処罰範囲の合理的な確定という見地からの、実際の立法が行っている規定上の工夫等に関する具体的な規定の作り方に関する議論である。刑事立法学の観点からは双方重要であるが、本稿では、合憲の枠内でのよりよい立法論を検討したいと考えているので、主題を第二の点に置きたい。

- (79) Brenner & Rehberg, *supra* note 13, at 83-84.
 (80) Burrichter, *supra* note 15, at 173.
 (81) アメリカにおけるサイバーいじめ規制立法に対する憲法判断についての邦文の研究については、例えば今出和利「アメリカにおける子どもの「ネットいじめ」(Cyberbullying) 対策と憲法上の問題点—法と判例の動向—」現代社会研究 16 巻 75 頁以下 (2019) を参照されたい。

1 サイバーいじめの規定に対して問題となる合憲性確保のための論点の整理

まず、サイバーいじめ規制立法に関して合憲性確保のために指摘されている議論を簡潔に整理しておく。具体的な議論は 2 以下で紹介し、ここでは議論の軸の紹介に留める。

そもそもサイバーいじめ自体の定義が多義的なことから、不明確な規制になる可能性があるだけでなく、立法による捕捉範囲も広くなりがちで、明確性の原則違反の問題、及び過度に広汎な規制の問題が生じる。これは、実際の立法の評価の項で指摘されている議論を紹介する形で確認していきたい。

次に、サイバーいじめは言論によって行われることが多いが、敵対的な言論の全てを規制すると、言論の自由を保障する合衆国憲法修正 1 条に違反し得るので、言論の自由を侵害しないような立法が求められる。言論の自由の保護範囲内に入る言論であるか否かの判断は、校内処分の是非等において争われてきているが、罰則の議論においても、転用されて議論されるので、必要に応じて紹介していきたい。

2 実際の立法の評価

サイバーいじめに関連する事件に対して適用され得る法律は様々な体系のもとに整理されており、議論を難しくしている⁽⁸²⁾。これは、サイバーいじめの定義の部分でも述べたように、この概念自体が論者により多様に把握されているということにも起因しよう。現状の立法については流動的な点がある。

そこで、検討方法としては、各州や連邦についてのサイバーいじめ

の立法動向に関するサーベイ⁽⁸³⁾ (以下、単に「サーベイ」ということがある) を参考にしながら、サイバーいじめを処罰しているとされる州の立法を一定の観点の下に整理してみることにする。サーベイによると、2018年の段階においてサイバーいじめについての罰則を有する州は44州ある。そのうち一定の議論がなされている州をピックアップして⁽⁸⁴⁾ その議論内容を整理・紹介する。

(82) Willard, Cyberbullying and the Law, *in* Cyberbullying Prevention and Response: Expert Perspectives 36, 52 (Patchin, Hinduja ed., 2012).

(83) Hinduja & Patchin, State Cyberbullying Laws a Brief Review of State Cyberbullying Laws and Policies (2018).

(84) 例えばサーベイ (前掲注(83)) は、罰則を持つ州として44州 (メイン州、ミネソタ州、ネブラスカ州、ニューハンプシャー州、ニューメキシコ州、ワイオミング州以外) に言及している。例えば同資料の2016年版ではわずかに18州が言及されていただけであった。もっとも、数字の変化だけをみて積極的な立法が行われていると推測するのは難しい。2016年版から加えられた州の中には、一般的なサイバーハラスメント規制をもって刑事規制ありと判断されているものもあるように思われ、そうであれば、2016年の時点のサーベイが単に拾い漏れだった可能性もあるからである (隣接犯罪をどこまで拾うかは、サイバーいじめの定義論と密接に関連する難しい問題なので、このような状況は理解できる)。

ただし、アラバマ州 (Ala.Code 1975 § 13A-11-8)、カリフォルニア州 (Cal. Penal Code § 653.2)、コロラド州 (C.R.S.A. § 18-9-111)、コネティカット州 (C.G.S.A. § 53a-182b, § 53a-183)、フロリダ州 (West's F.S.A. § 784.048)、ジョージア州 (Ga. Code Ann., § 16-11-39.1)、ハワイ州 (HRS § 711-1106)、イリノイ州 (720 ILCS 5/26.5-3)、インディアナ州 (IC 35-45-2-1 ~ IC 35-45-2-5)、カンザス州 (K.S.A. 21-6206)、マサチューセッツ州 (M.G.L.A. 265 § 43A)、ミシガン州 (M.C.L.A. 750.411h)、モンタナ州 (MCA 45-8-213、通信のプライバシーという表題)、ニューヨーク州 (McKinney's Penal Law § 240.26 [一般的なハラスメント罪])、ノースダコタ州 (NDCC, 12.1-17-07)、オハイオ州 (R.C. § 2917.21)、オクラホマ州 (21 Okl.St. Ann. § 1172)、オレゴン州 (O.R.S. § 166.065)、ロードアイランド州 (Gen.Laws 1956, § 11-52-4.2)、サウスカロライナ州 (Code 1976 § 16-3-1700 以下)、サウスダコタ州 (SDCL § 49-31-31)、テネシー州 (T. C. A. § 39-17-308)、テキサス州 (V.T.C.A., Penal Code § 42.07 さらに V.T.C.A., Penal Code § 33.07 (オンラインなりすまし) も参照される)、

ユタ州 (U.C.A. 1953 § 76-9-201)、バーモント州 (13 V.S.A. § 1027)、バージニア州 (VA Code Ann. § 18.2-152.7:1)、ワシントン州 (RCWA 9.61.260)、ウィスコンシン州 (W.S.A. 947.0125、942.01) の諸規定はサイバーの文脈を含む一般的なハラスメントやストーキング規制であり、サイバーいじめに特化した規定とはいい難い面があるので、本稿では触れない(サイバーハラスメントやサイバーストーキングの研究を行う際に再検討すべきであろう)。

(1) 処罰範囲の広い立法(案)に対する憲法上の懸念

まず、処罰範囲の広い立法(案)に対しては、憲法上の懸念が提起されている。重要性の見地から連邦の法案を紹介し、その上でアーカンソー州の規定を紹介する。

① 連邦の法案について (Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009))

Megan Meier Cyberbullying Prevention Act は議会を通過したものではないが、激しい議論を呼ぶことになったサイバーいじめ処罰法案である。この法案は、いじめの被害者の名である Megan Meier の自殺をきっかけに提案された。Megan Meier は、13歳のミドルスクールの生徒であったが、MySpace でのコミュニケーションにおける恋愛相手にふられ⁽⁸⁵⁾、失意のうちに自殺してしまった、という事案である。Megan Meier が、恋愛相手だと思っていた、Josh Evans という16歳の少年は架空のものであり、現実世界において Megan Meier のクラスメートの母親 (Lori Drew、47歳) が作り出したものであった。Drew は My Space で Josh という架空の人物になりすましていたのである。

検察はコンピュータへの無権限アクセス罪である Computer Fraud and Abuse Act (以下「CFAA」という) 違反で起訴した⁽⁸⁶⁾。CFAA は無権限⁽⁸⁷⁾を要件としているが、無権限を基礎付ける事実としては、Drew による、MySpace の ToS (Terms of Service、利用規約) に違反したアカウントの使用 (コンピュータの使用) に求めざるを得なかった。これに対し裁判所⁽⁸⁸⁾は、MySpace の規約違反をもって無権限とする主張には

与せないとして、CFAA では処罰できないという結論に至った。無権限アクセス罪 (CFAA) に関する学説は、この帰結を概ね好意的に受け止めている⁽⁸⁹⁾。しかし、規約違反のオンラインのなりすまし行為（+いわば「なりすました上で被害者の人格を蹂躪する行為」）を無権限アクセス罪で処罰ができない、かつ本件がサイバーいじめという意味では当罰性のある事案である、という理解を下に、そうであれば立法が必要ではないか、という議論になり⁽⁹⁰⁾、法案として提出されたのが Megan Meier Cyberbullying Prevention Act である。法案の内容は次の通りである。

18U.S.C. § 881. Cyberbullying

- (a) 州際通商又は国際通商において、威圧する (coerce)、脅えさせる (intimidate)、困らせる (harass) 意図、又は著しい精神的な苦痛 (substantial emotional distress) を与える意図で、激しく (severe)、反復的で (repeated)、かつ敵意のある (hostile) 行動を可能にする (support) 電子的な手段を用いて通信を伝達する者は、このタイトルの下で罰金、若しくは2年を超えない拘禁刑が科されるか、又は双方が併科される。
- (b) このセクションにおいて使用される場合には、
- (1) 「通信」の文言は、ユーザにより特定される2又は3以上のポイント間の、送受信の際にも情報の形式又は内容が変わらない、ユーザが選択する情報の電子的な伝達を意味し、
 - (2) 「電子的な手段」とは、email、インスタントメッセージ、ブログ、ウェブサイト、電話、及びテキストメッセージを含む情報サービスへアクセスするための、電力に依存するあらゆる設備を意味する。

立法提案者 (Ms. Sánchez) は、言論の自由の保護とサイバーいじめの処罰を両立できるとしていた⁽⁹¹⁾。例えば、いらいらさせるチェーンメール、怒りに満ちた政治的なブログの投稿や、怒っている元のポー

イフレンドへのテキストを処罰しないことができると述べていた⁽⁹²⁾。確かに、言論の自由を保護する修正1条で保護されない言論のみを処罰するのであれば、憲法上の大きな論点をクリアできる。例えば、生命に対する真の脅威 (true threat) を与える言論や煽動的な言論であれば、憲法上の保護を欠くがゆえに、修正1条の問題をクリアしつつ立法が可能であろう⁽⁹³⁾。しかし、そのような立法になっていると断定できるわけでもないように思われる。また、そもそも犯罪行為の定義が曖昧であるという観点から、言論の自由を侵害しているという批判もある⁽⁹⁴⁾。「激しく、反復的で、かつ敵意のある行動を可能にする」の要件は、基準の策定が困難だと指摘されている⁽⁹⁵⁾。

さらに、この法案では修正1条で保護されている非常に多くの人々が罪を犯すことになることに疑いがなく、多くの人々に萎縮効果を与える、という⁽⁹⁶⁾。立法提案者の意見とは逆方向の主張ではあるが、具体的には、怒った両親の言動といった、犯罪に値しない行動が犯罪行為になりかねない、とか⁽⁹⁷⁾、威圧する、脅えさせる、困らせる、著しい精神的な苦痛、激しく、及び適意のある行動、といった文言についての定義もなく、訴追側に広汎な裁量を与えられている⁽⁹⁸⁾、さらには反復的な行為への限定もない、と指摘される⁽⁹⁹⁾。

以上の不明確性や過度に広汎な規制に関する批判は、ハラスメント規制全体に対する批判にもなり得るものであろう。上記で批判されている「著しい精神的な苦痛」という要件も、ストーキング罪で既に使われている要件ではある。不明確性等の検証を行うに上記の議論のみの検証だけでは不十分である。そこで、ひとまず、これらの批判についてはその存在のみを紹介することにし、別の問題点をみていきたい。

他の角度からこの法案の内容をみると、別の問題点が浮かび上がる。例えば、法案の理由においては、「インターネットの利用によって生じた精神的な問題を抱える患者の54%が、18歳以下であった⁽¹⁰⁰⁾」というように年齢的な議論が行われていたにもかかわらず、この法案には年齢の限定がなく⁽¹⁰¹⁾、学校に関連する問題への限定もない⁽¹⁰²⁾。また、

立法事実である Megan Meier 事件への適用を考えてみても、Drew の行為が直ちに法案の要件に該当するといえるかも定かではない⁽¹⁰³⁾。これに対し、Drew は Megan Meier 事件の後に辛辣なハラスメントを受けたとされており、この法案では Megan Meier を保護するどころか、むしろ、大人である Drew を保護する結果になってしまっているときえ皮肉られている⁽¹⁰⁴⁾。

いずれにしても、より処罰範囲を限定した規定にする必要があると指摘されている⁽¹⁰⁵⁾。

(85) もはや Megan Meier のことを好きではないとして、“the world would be a better place without her in it.”と述べた。

(86) 事件はミズーリ州で起きたが、当時のミズーリ州法にも十分な処罰規定がなかったと判断されたようである。

(87) 正確には、権限なく、又は権限超過が要件である。

(88) 18 U.S.C. § § 1030 (a)(2)(C)及び 1030 (c)(2)(B)(ii), 詳細は U.S. v. Drew, 259 F.R.D. 449 (2009) 参照。

(89) 無権限の解釈を、検察官のように、コンピュータやサーバの管理者へ不利益を与える目的とか同人との契約違反の態様で行為することと解釈する巡回区連邦控訴裁判所の判例もみられたところ、2009年の第9巡回区連邦控訴裁判所の判例 (Brekka 事件) を皮切りに、最近では、第2、第4、第9の3つの巡回区において、一度アクセス権が与えられた以上は、それを明示的に剥奪しておかない限り、契約違反やアクセス権を与えた者等を害する目的があるというだけでは、無権限アクセス罪の成立に必要な無権限を充たさない、という理解がなされており (ただし、第2巡回区は寛容性のルールの適用による)、連邦最高裁の判断もなく、Circuit Split がなくなった、と断言はできないものの、Drew 事件の判旨と同様の方向の理解が有力になってきている。以上について詳しくは、拙稿「コンピュータ・データへの無権限アクセスと刑事罰(2)」法協135巻3号163頁以下(2018)、拙稿「コンピュータ・データへの無権限アクセスと刑事罰(3)」法協135巻4号187頁以下(2018)も参照。

(90) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 23.

(91) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 23.

(92) Cyberbullying and Other Online Safety Issues for Children, *supra*

- note 3, at 23.
- (93) Meredith, *supra* note 62, at 329-330.
- (94) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 56.
- (95) King, *supra* note 10, at 874.
- (96) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 57.
- (97) Meredith, *supra* note 62, at 330.
- (98) Burrichter, *supra* note 15, at 166.
- (99) Lipton, *supra* note 6, at 1122.
- (100) Megan Meier Cyberbullying Prevention Act, H.R 1966, 111th Cong. § 2 (6) (2009).
- (101) Cyberbullying and Other Online Safety Issues for Children, *supra* note 3, at 67, Meredith *supra* note 62, at 327-328, Lipton, *supra* note 6, at 1122 [被害者が未成年者 (minor) に限定されていない] .
- (102) Burrichter, *supra* note 15, at 153.
- (103) 捜査官は、感情的なハラスメントの目的で行われたものであるとの立証ができなかった、と述べていた (FoxNews.com, Prosecutor: No Criminal Charges in MySpace Suicide, December 03, 2007 (<http://www.foxnews.com/story/2007/12/03/prosecutor-no-criminal-charges-in-myspace-suicide.html>)). それを理由で CFAA での起訴を余儀なくされたのである (Burrichter, *supra* note 15, at 146)。
- (104) 多数の者が Drew に、Drew の住所、電話番号、及び家の衛星写真をインターネットで拡散させ、また、殺すぞという脅迫やキッチンにれんがを投げ入れるなどすることによりハラスメントを行った、という (Burrichter, *supra* note 15, at 165)。
- (105) Burrichter, *supra* note 15, at 177.

② アーカンソー州の立法例

連邦の法案は結局議会を通過しなかったが、連邦と同等以上の処罰範囲を有する規定が、既にアーカンソー州でサイバーいじめ罪として立法されている。アーカンソー州においては、被害者の MySpace アカウントに対するいじめによって自殺をした 12 歳の少女の事件⁽¹⁰⁶⁾を処罰できなかった⁽¹⁰⁷⁾という経過があり、立法へと結びついた⁽¹⁰⁸⁾。

アーカンソー州のサイバーいじめ対策立法

AR ST § 5-71-217 - Cyberbullying

- (a) このセクションにおいて、
- (1) 「通信」とは、送受信時の情報の形式又はないようについて変更せずにある人により特定されたポイント間 (between or among) でその人が選択する電子的な情報の通信を意味する。
 - (2) 「電子的な手段」とは、ローカルな掲示板サービスに限られず、インターネット・チャット・ルーム、電子メール、ソーシャルネットワークキングサービス、又はオンラインメッセージサービスを含むコンピュータのオンラインサービス、インターネットサービス、電話又はその他の電子的な通信手段を用いることによって作成される、あらゆる種類のテキスト、視覚的、書面、又は口頭の通信を意味する。
 - (3) (略、「学校の職員」の定義規定)
- (b) 下記の行為をする者はサイバーいじめ罪を犯す者である。
- (1) 他人を追い立てる (frighten)、威圧する (coerce)、脅えさせる (intimidate)、威嚇する (threaten)、酷使する (abuse)、困らせる (harass)、心配させる (alarm) 目的で、電子的な手段により、通信を伝達 (transmit)、送信 (send)、又は投稿 (post) する場合であって、かつ
 - (2) 当該伝達が、当該他人への激しい (severe)、反復的で (repeated)、又は敵対的な (hostile) 行動を助長している場合。
- (c) (略)
- (d)(1) サイバーいじめは B 級軽罪【注：90 日を超えない拘禁刑及び 1,000\$ を超えない罰金⁽¹⁰⁹⁾】である。
- (2) サイバーいじめは被害者が学校の職員である場合には A 級軽罪【注：1 年を超えない拘禁刑及び 2,500\$ を超えない罰金⁽¹¹⁰⁾】である。

AR ST § 5-71-217 はかなり広い捕捉範囲を有し⁽¹¹¹⁾、違憲の疑いがあるとされている連邦の法案よりも広い処罰範囲を有する⁽¹¹²⁾、とされる。結局、連邦の法案と同じく、この規定に対しても、修正1条が保護する言論までもが犯罪になり得るとして、違憲の疑いがあると評価する声がある⁽¹¹³⁾。

③ 小括

以上からすると、アメリカにおいては、侵害の程度や当事者の限定の可能性といった見地から、処罰範囲の明確化がさらに要請されることになる。以上の規定ないしこれらの規定とほぼ同じ規制態様の規定を参考にする場合には憲法上の疑義に関連した注意を要する。次からは、限定の方法について立法例を参照しながら検討してみることに行いたい。法定刑の調整を行う立法例に関する議論も同時に行いたい。

(106) Young, Online Teasing Leads to Teen's Suicide, kait8.com, (Nov. 24, 2009, 12:40 PM), (<http://www.kait8.com/story/11566204/online-teasing-leads-to-teens-suicide?>).

(107) Rose, *supra* note 3, at 1007.

(108) Brady, *supra* note 3, at 28.

(109) AR ST § § 5-4-401, 5-4-201.

(110) AR ST § § 5-4-401, 5-4-201.

(111) Brady, *supra* note 3, at 29.

(112) Rose, *supra* note 3, at 1012.

(113) Rose, *supra* note 3, at 1026.

(2) 侵害結果の限定

サイバーいじめというのは、相手方に対して恐怖等の感情を覚えさせる情報を伝達する行為だといえる。その場合、行為態様だけでなく、一定の侵害結果を要件とすることが考えられる。その際には、例えば連邦法のストーキング罪⁽¹¹⁴⁾で考慮されている、(A)死又は重大な肉体的傷害についての合理的な恐怖 (reasonable fear of the death of, or serious bodily injury)、又は(B)著しい精神的な苦痛 (substantial emotional distress)

を要件化するべきか否かが問題となる。この点、次の MD Code, Criminal Law, § 3-805 (b)(2) (メリーランド州) は連邦法のストーキング罪と同様の限定方法を採用しているといえよう。

メリーランド州のサイバーいじめ対策立法

MD Code, Criminal Law, § 3-805. 電子メールの不正使用

・定義

(a)

- (1) このセクションにおいて、次の文言は、次に示される意味を有する。
- (2) 「電子的な通信 (Electronic communication)」とは、コンピュータ又はその他の電子的な手段を用いることによる、人に送信され、及び人により受信される情報、データ、又は通信の伝達を意味する。
- (3) 「インタラクティブコンピュータ・サービス」とは、情報サービス、情報システム、又は複数のユーザによるコンピュータ・サーバへのコンピュータアクセスを提供又は可能にするアクセスソフトウェアプロバイダを意味し、インターネットへ及び携帯電話へのアクセスを提供するシステムを含む。

・禁止されること

(b)

- (1) 他人を心配させる (alarm)、又は著しく悩ませる (annoy) 電子的な通信を介して、悪意をもって行為 (in a course of conduct) を行ってはならない。
 - (i) 当該他人を困らせる (harass)、心配させる (alarm)、若しくは悩ませる (annoy) 意図をもって
 - (ii) 当該他人により、又は当該他人に代わって、行為を止めるようにいう、合理的な警告又は要求を受領した後に
 - (iii) 適法な目的を有しないこと

(2) 次のいずれかの意図を有して、重大な精神的苦痛を未成年者に与えるか、又は死若しくは重大な身体的傷害についての合理的な恐怖の下に未成年者を置く行為を、悪意をもって行うために、インタラクティブ・コンピュータ・サービスを利用してはならない。

(i) 当該未成年者を殺す、傷を負わせる、又は当該未成年者に重大な精神的苦痛を惹起させる

(ii) 当該未成年者を死、又は重大な身体的傷害についての合理的な恐怖の下に置く

・セクションの構造

(c) (略)

・例外

(d) このセクションの(b)(1)は、政治的な見解の表現、又は他人に情報を提供することを意図した平和的な活動には適用されない。

・罰

(e) このセクションに違反する者は軽罪で有罪であり、かつ、1年以下の拘禁刑若しくは500 \$以下の罰金、又は双方を併科する。

しかし、サイバーいじめの典型的な被害は何であるかを考えてみると、(A)の類型は、サイバーいじめには使いづらい。なぜなら、サイバーいじめは物理的な暴力の直接的な主張なしに⁽¹¹⁵⁾、感情的及びレピュテーションへの攻撃として行われることが往々にしてあり⁽¹¹⁶⁾、それゆえにオンラインの文脈では身体的な傷害へ直結する言論は多くなく、これに侵害結果を限定しても実効性は見込めないからである⁽¹¹⁷⁾。この点、下記のアラスカ州のハラスメント罪の規定をみると、サイバーいじめの処罰規定として理解される AS § 11.61.120 (a)(7)⁽¹¹⁸⁾ (2014年に追加、次頁参照) は、物理的な傷害について合理的な恐怖の下に置く、という要件があるが、まさにここでの疑問、すなわち捕捉範囲が十分であるか否かについて、疑問が呈されよう。そこで、(B)の方

向性で考えていくことが考えられる。ただし、(B)、すなわち、「著しい精神的な苦痛 (substantial emotional distress)」を要件とする連邦の法案に対しては、処罰範囲が広すぎる、という批判がなされていることは既に述べた。

もっとも、(A)を要件とする場合であっても、これを加重犯罪の加重のための要件にすることが考えられ、その場合には処罰の間隙は生じない。例えば、アイオワ州のハラスメント罪 (I.C.A. § 708.7⁽¹¹⁹⁾) を挙げることができる。アイオワ州では、原則的にハラスメント罪は単純軽罪であるが、例えば、身体的傷害を加えるとの脅迫に係るハラスメントを犯した場合には、重軽罪となる。立法方法としてはこの方法が1つの合理的な方法かもしれない。

AS § 11.61.120. Harassment in the second degree

(B 級軽罪 (AS § 11.61.120 (b)))

(a)(1)から(6)まで省略

(7) 物理的な傷害について合理的な恐怖の下に置く態様で、反復して、18歳未満の者を侮辱する、なじる、喧嘩をふっかける、脅えさせる電子的通信を送信又は公開する

(114) 本稿ではストーキング罪を検討の対象とするものではないが、連邦法のストーキング罪の規定については本稿末尾参照。

(115) King, *supra* note 10, at 872.

(116) Fertik & Thompson, *supra* note 12, at 106.

(117) King, *supra* note 10, at 872, Brenner & Rehberg, *supra* note 13, at FN 109.

(118) 2013 AK S.B. 128 (NS), 2013 Alaska Senate Bill No. 128, Alaska Twenty-Eighth Legislature - Second Session, ALASKA COMMITTEE REPORT (February 19, 2014) では、次のように立法趣旨が紹介されている。「技術やソーシャルメディアの発展に伴い、電子的手段によるハラスメント、又は“サイバーいじめ”が、ますます広くなされるようになってきている。我々の現在の法律は、いくつかの形式での学校システムにおけるいじめ (bullying) を許容している。しかし、学校の所有地内や学校の

所有地の近くで全てのいじめが行われるわけではない。SB128 (この法案) は、学校システム外における処罰を許容するものであり、18歳未満の者の電子的通信によるハラスメントをB級軽罪にするものである。」さらに、2013 AK S.B. 128 (NS), 2013 Alaska Senate Bill No. 128, Alaska Twenty-Eighth Legislature - Second Session, ALASKA COMMITTEE REPORT (February 19, 2014) [MR. STEINER 発言。(少年のサイバーいじめをターゲットにしている。)] や、2013 AK S.B. 128 (NS), 2013 Alaska Senate Bill No. 128, Alaska Twenty-Eighth Legislature - Second Session, ALASKA COMMITTEE REPORT (March 07, 2014) [MS. CARPENETI 発言] も参照。

(119) I.C.A. § 708.7. Harassment

1. a. 他人を脅えさせる (intimidate)、困らせる (annoy)、心配させる (alarm) 意図で次に掲げるいずれかに該当する場合には、その者はハラスメントを行うことになる。
 - (1) 電話、テレグラフ、書面、又は電子的な通信により、正当な目的なく、かつ他人を困らせる又は傷付ける (harm) 原因になりそのような態様で、当該他人とコミュニケーションを行う
 - (2) 他人の占有する、建造物、自動車、飛行機、鉄道のエンジン若しくは鉄道車両、又は船 (boat) の内部又は近くに、爆発物又な放火を装った装置 (device) を置く
 - (3) 他人の名義で商品又は役務を注文する、又は他人に、当該他人に知らせず、又は同意を得ずに、商品又は役務を配達させる
 - (4) 後記の情報が虚偽であることを知りながら、他人が何らかの犯罪活動に関わっているという虚偽の情報を法執行機関に報告する、若しくは、そのような虚偽の情報が法執行機関に報告される原因を作る、又は後記の行為が発生しなかったことを知りながら、犯罪行為の発生を主張する報告を行う
- b. 他人を脅迫し (threaten)、脅えさせ、又は心配させる (alarm) 意図で、わざと (purposefully) かつ正当な目的なく、他人と個人的な接触を有する場合に、その者はハラスメントを行うことになる。このセクションにおいては、特に別の意味が指定されない限り、「個人的な接触」は、2人以上の人が視覚的又は物理的に互いに近接している状態で遭遇することを意味する。「個人的な接触」には、物理的な接触 (touching) 又は口頭のやり取り (communication) が含まれ得るものの、それが必要なわけではない。
2. a. 強制的重罪 (forcible felony) を犯すための脅迫に係るハラスメントを犯す、又はハラスメントを犯し、かつ、ここ10年の間で、以前にこのセクション若しくは類似の法律の下で、ハラスメントで3回以上有罪の判断を受けた者は、1級ハラスメントを犯す者

である。

- b. 1級のハラスメントは加重軽罪 (aggravated misdemeanor) 【注：2年を超えない拘禁刑及び625\$以上6,250\$以下の罰金】である。
- 3. a. 身体的傷害 (bodily injury) を加えるとの脅迫に関するハラスメントを犯す、又はハラスメントを犯し、かつ、以前に、ここ10年の間で、このセクション若しくは類似の法律の下で、ハラスメントで2回有罪の判断を受けた者は、2級ハラスメントを犯す者である。
- b. 2級ハラスメントは重軽罪 (serious misdemeanor) 【注：1年を超えない拘禁刑若しくは315\$以上1,875\$以下の罰金又はこれの併科】である。
- 4. a. その他のあらゆるハラスメントは3級ハラスメントである。
- b. 3級ハラスメントは単純軽罪 (simple misdemeanor) 【注：30日を超えない拘禁刑若しくは65\$以上625\$以下の罰金又はこれの併科】である。
- 5. (略)

(3) 「反復して (repeatedly)」の要件の是非

次に行為態様の観点からの限定が考えられる。ここでは「反復して」の要件を持つ州があることに着目したい。連邦の法案に対して、同法案では即時的な興奮から出てくる特徴のない一度きりの行動でも捕捉され得ることになってしまうという批判があった⁽¹²⁰⁾。反復性を重視する議論だといえる。そして、前述のアラスカ州の AS § 11.61.120 (a)(7) は「反復して」を要件とする。同規定が捕捉する行為態様は電子的通信の送信又は公開である。公開にはソーシャルメディアへの投稿が含まれる⁽¹²¹⁾。ただし、サイバーいじめの特徴として第3 2(3)②で述べた侵害の持続性に照らせば、1回きりのソーシャルメディアへの投稿に関しても、投稿がなされれば持続的な侵害が惹起されかねない。そうすると、持続的な侵害が生じるような場合に限定することには一定の合理性があるように思われるものの、持続的な侵害を惹起するために常に反復的な行為が必要であるとはいえず、行為の反復を要求するような態様 (秘密通信である email のような場合) と、行為の反復が不要な場合とを分けることもあり得る。もっともアメリカのサイバーいじめ

に関する立法状況の分析だけからはこの点の検討が十分にはできないので、反復性を要件とする州とそうでない州が混在することを指摘するに留めておく。

(120) Lipton, *supra* note 6, at 1122.

(121) 2013 AK S.B. 128 (NS), 2013 Alaska Senate Bill No. 128, Alaska Twenty-Eighth Legislature - Second Session, ALASKA COMMITTEE REPORT (March 03, 2014) [Senator Kevin Meyer 発言]。

(4) 当事者の属性

サイバーいじめが主に教育環境において起きる現象であることや、未成年者のせい弱性に着目すれば、被害者の属性（下記①、②）、行為者（加害者）（下記③）といった事項に着目して規制態様を区別するという立法方法が考えられる。

① 被害者の年齢（ないし学生か否か）に着目する場合

まず、コロラド州においては、18歳未満の者（minorをそう定義している）に対するハラスメントに特化した立法提案がなされたが（C.R.S.A. § 18-9-111.5の立法提案）、これは通らなかった⁽¹²²⁾。

一方で、複数の州で被害者の年齢に着目した立法が行われている。例えば AS § 11.61.120 (a)(7)（アラスカ州）は18歳未満の者に着目する。立法趣旨においては、サイバーいじめによる若者の自殺が増加していることや、学校に通う年齢の子供に対するサイバーいじめが既に多く存在することが指摘されていた⁽¹²³⁾。LSA-R.S. 14:40.7（ルイジアナ州⁽¹²⁴⁾）は、18歳未満の者のみをサイバーいじめ罪の客体とする。未成年者（minor）であることを要件とする規定を持つメリーランド州（MD Code, Criminal Law, § 3-805 (b)(2)⁽¹²⁵⁾）や、学生であることを要件とする規定を持つケンタッキー州（KRS § 525.080）の規定⁽¹²⁶⁾も同様といえる。

また、V.A.M.S. 565.090（ミズーリ州）は、被害者の年齢が17歳以下の者であって、かつ21歳以上の行為者の場合に刑を加重している。U.C.A. 1953 § 76-9-201（ユタ州）も被害者の年齢が17歳以下である場

合に刑を加重する⁽¹²⁷⁾。V.T.C.A., Penal Code § 42.07 (テキサス州) も同様に、ハラスメント罪を原則的にB級軽罪にしつつも、被害者が18歳未満であって被害者に自殺をさせる意図等を有する場合にはA級軽罪に格上げする⁽¹²⁸⁾。さらに、18 Pa.C.S.A. § 2709 (ペンシルバニア州) の規定も、ハラスメント罪を原則としてサマリーオフENSEスにしつつ、被害者が子どもの場合には3級軽罪に格上げしている⁽¹²⁹⁾。

若年層の精神的未成熟さに基づく類型的ぜい弱性(自己防衛のつたなき)、及びサイバーいじめの典型的事案では若年層が被害者になるといったことを強調する立法という場合には、年齢等を要件化することに一定の理由があることになろう。

② 被害者の年齢以外の属性に着目する場合

①に対し、サイバーいじめの定義論(第2)でも述べたが、被害者は、学生に限られるわけではなく、学校の職員が被害者になることもある。この点を考慮した立法も考えられる。

まず、ネヴァダ州のN.R.S. 392.915⁽¹³⁰⁾は、客体を限定列挙しながらも、生徒と学校の従業員とを併記して同等に取り扱っている。これに対し、法定刑に差をつけることも考えられ、前述のアーカンソー州のサイバーいじめ罪(AR ST § 5-71-217(d)(2))は、その法定刑を、原則として、B級軽罪(90日以下の拘禁刑又は1,000\$以下の罰金)としつつも、被害者が学校の職員の場合にはA級軽罪(1年以下の拘禁刑又は2,500\$以下の罰金)に加重する⁽¹³¹⁾。

このような学校の職員を被害者とする場合に刑を加重するという規定につき、良好な教育環境の維持に対する侵害を考慮する場合には、刑の加重を正当化し得るように思われるが⁽¹³²⁾、学生のぜい弱性を考慮すると逆の方向の議論にもなり得ること⁽¹³³⁾に注意が必要だと思われる。

③ 加害者の年齢に応じた法定刑の調整等

加害者の年齢に応じた法定刑の調整が立法されることがあり、それはノースカロライナ州法⁽¹³⁴⁾、ミズーリ州法⁽¹³⁵⁾にみられる。

刑の調整以外の手続が予定されることもある。例えばN.

J.S.A.2C:33-4.1 (ニュージャージー州) はサイバーハラスメント罪としての立法であるが、年齢に応じて刑罰を加重するだけでなく、条件を付けるようにする工夫をしている⁽¹³⁶⁾。条件の内容はプログラムの受講であるが、これを受けさせることについて親又は後見人にも不履行に対する罰金の制裁を課すこと⁽¹³⁷⁾で履行を促す制度になっている。また、18 Pa.C.S.A. § 2709(a-1)(2)(i) (ペンシルバニア州) においては、子どもに対するサイバーハラスメント罪において、加害者が未成年の場合にサイバーハラスメントに関する教育プログラムを受けることを命じることができるとする。ノースカロライナ州においても、プロベイション等へ入る手続が用意されている⁽¹³⁸⁾。

④ 小括

サイバーいじめ自体が多義的であるので、州法の規定方法も多様になるのは、調査の結果としては違和感がないものの、統一的な議論は困難になっている。ハラスメント罪等の他の規定との棲分けを考える必要もあり、どのような立法方法が妥当かを論じることは容易ではない。もっとも、いじめ固有の発想として、自由刑や罰金刑のみで問題の解決ができないという議論も必要である。その観点からすると、例えば、法律効果としてプログラムの受講の強制を行えるようにするというニュージャージー州の立法例は参考になるといえよう。

(122) CO H.R. Jour., 2015 Reg. Sess. No. 38, Colorado House Journal, February 13, 2015, 254-255.

(123) 2013 AK S.B. 128 (NS), 2013 Alaska Senate Bill No. 128, Alaska Twenty-Eighth Legislature - Second Session, ALASKA COMMITTEE REPORT (March 03, 2014) [MS. MORELY 発言]。

(124) LSA-R.S. 14:40.7 Cyberbullying

A. サイバーいじめとは、18歳未満の者を威圧する、虐待する、苦痛を与える、又は脅えさせることについて悪意のある及び故意の (willful) 意図をもって、電子的なテキストの、視覚的、又は口頭のコミュニケーションの伝達である。

B. このセクションの目的に照らし、

(1) ケーブルオペレーター (cable operator) とは、ケーブルシステム

上のケーブルサービスを提供し、かつ、直接的に、若しくは、1若しくは2以上の提携会社（affiliates）を介して、そのようなケーブルシステムにより大きな（significant）利益が帰属する、又は何らかの取決め（arrangement）により、そのようなケーブルシステムの管理及び運営を支配している、若しくは、管理及び運営に責任を有する、人又は人的集団のことをいう。

- (2) 電子的テキストの、目に見える又は口頭の通信とは、コンピュータ・オンライン・サービス、又はその他の電子的な通信手段の利用により確立された、あらゆる種類の通信のことをいい、ローカルな掲示板、インターネット・チャット・ルーム、email、ないしオンラインメッセージングサービスを含むがこれらに限られない。
- (3) インタラクティブコンピュータ・サービスとは、複数のユーザによるコンピュータ・サーバへのコンピュータのアクセスを提供又は可能にする、あらゆる情報サービス、システム又はアクセスソフトウェアプロバイダのことをいい、インターネットへのアクセスを提供するサービス又はシステム、及び図書館若しくは教育機関により運営されるシステムやそれらにより提供されるサービスを含む。
- (4) テレコミュニケーションサービスとは、当該設備の使用の有無にかかわらず、料金を取って公衆に直接的にテレコミュニケーションを提供することをいう。

C. このセクションの規定に基づいて行われた犯罪は、通信が、最初に送信された場所、最初に受信された場所、又は最初に誰かに閲覧された場所で行われたものとみなされ得る。

D. (1) このセクションの(2)に規定される場合を除き、サイバーいじめ罪を犯した者は、500\$以下の罰金、6月以下の拘禁刑又は双方の併科とする。

(2) 行為者が17歳未満の場合、事件の処分は、Title VII of the Children's Code. の規定のみによってなされる。

E. このセクションの規定は、このセクションの規定で定義されるインタラクティブコンピュータ・サービス、テレコミュニケーション・サービス、又はケーブルオペレータには適用されないものとする。

F. このセクションの規定は、ルイジアナ州憲法 Article I, Section 8に基づく宗教的な自由な言論を禁止又は制限するように解釈されてはならない。

(125) メリーランド州では、2013年の法改正（Acts 2013, c. 369, § 1, eff. Oct. 1, 2013）によって、未成年者を被害者とする規定（§ 3-805 (b)(2)）が追加された。この改正法は Grace Law と呼ばれているが、隣人により、オンラインで、度重なる、悪意のあるハラスメントを受け続けた結果、自殺をしてしまった当時15歳の Grace McComas の名に由来する。この点に

ついて詳しくは、メリーランド州政府のHPを参照されたい (<http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=billpage&stab=02&id=hb0396&tab=subject3&ys=2013RS>)。

(126) KRS § 525.070 Harassment

- (1) 他人を脅えさせる、困らせる、不安にさせる、又は心配させる意図で次のいずれかに該当する者は harassment で有罪である。
- (a) 当該他人を叩く、押す、蹴る、又はその他の方法で物理的接触にさらす
 - (b) 当該他人を叩く、押す、蹴る、又はその他の方法で物理的接触にさらすことを試みる、又はそうすると脅迫する
 - (c) 公共の空間で、現在する者に対して、攻撃的で粗野な言説、ジェスチャ、又は攻撃的な言葉を表示、若しくは浴びせる
 - (d) 公共の場所において、又は近辺で、人を追いかける
 - (e) 当該他人を心配させる若しくは深刻に困らせる行為を行うか若しくは反復してそのような行為を遂行し、かつこれに正当な目的がない場合
 - (f) 地方の学区に学生として記録されており、かつ学校の所有地、学校が協賛する交通機関において、又は学校が協賛するイベントにおいて、
 1. 他の学生の財産を損壊又はこれのセフトを行う
 2. 学校の業務を大幅に混乱させる、又は
 3. 当該状況下で、他の学生を物理的な害悪、脅迫、屈服、又は、困惑への恐怖にさいなまれる状況にする、と合理的な者であればわかる、ジェスチャ、書面のコミュニケーション、口頭の供述、又は物理的行為を手段として、敵対的な環境を作る
- (2)(a) このセクションの(b)において定められる場合を除き、ハラスメントは違反 (violation) 【250\$を超えない罰金 (KRS § 532.020, KRS § 534.040 (2)(c))】である。
- (b) このセクションの(1)(a)で定義されるハラスメントは、B級軽罪【注：90日を超えない拘禁刑及び250\$を超えない罰金 (KRS § 532.090 (2), KRS § 534.040 (2)(b))】である。

KRS § 525.080 Harassing communications

- (1) 他人を脅えさせる、困らせる、悩ませる、又は心配させる意図をもって、次のいずれかの行為をする者は、harassing communications で有罪である。
- (a) 匿名で、又はその他の方法で、電話、テレグラフ、メール、又はその他の電子的若しくは書面の通信の形式により、悩み又は心配を惹起する態様で人と通信をし、正当な通信を全く提供しない場合
 - (b) 正当な通信の目的なく、会話がその後成立するか否かを問わず、電話の呼出しをする場合

(c) 地方の学区の学生として記載されており、他の学校の学生と、又は他の学校の学生について、匿名又はその他の方法で、電話、インターネット、テレグラフ、メール、又はその他の電子的若しくは書面の通信の形式により、当該状況下で、当該他の学生が、物理的な害、脅迫、屈辱、又は困惑への恐怖にさいなまれることになることが合理的な者であればわかる態様で通信をし、正当な通信を全く提供しない場合

(2) Harassing communications は B 級軽罪【注：90 日を超えない拘禁刑及び 250\$ を超えない罰金（KRS § 532.090 (2), KRS § 534.040 (2)(b)）】である。

(127) 原則 B 級軽罪（U.C.A. 1953 § 76-9-201 (3)(a)(i)）→原則 A 級軽罪（U.C.A. 1953 § 76-9-201 (3)(b)(i)）。

(128) V.T.C.A., Penal Code § 42.07 (c)(2)(A)参照。この部分は 2017 年改正で挿入された（2017 Tex. Sess. Law Serv. Ch. 522 (S.B. 179) (VERNON'S)）。

(129) 18 Pa.C.S.A. § 2709 (c)(1), (2)参照。

(130) N.R.S. 392.915.

1. 何人も口頭、書面、又は cyber-bullying の利用による場合を含むがこれに含まれない電子的通信により、情を知って、学区又はチャータースクールの生徒又は職員を、次のいずれかの意図をもって、身体的な害 (bodily harm) 又は死を惹起させるとして脅迫してはならない。
 - (a) 学区又はチャータースクールの生徒又は職員を、脅えさせる、困らせる、追い立てる、心配させる、又は苦しめる
 - (b) パニック又は精神的な動揺を惹起する
 - (c) チャータースクールを含むがこれに限られない、公立学校の業務を妨害する
2. より重い刑が特定の規定により規定されていない限り、サブセクション 1 の規定に違反する者の法定刑は次の通りとする。
 - (a) (b) の規定が適用される結果が生じていない場合には、軽罪【筆者注：1,000\$ 以下の罰金若しくは 6 月以下の群刑務所への拘禁刑又はこれらの併科（N.R.S. 193.120.3）】。
 - (b) 当該脅迫が、次のいずれかを惹起する場合には、重軽罪【筆者注：364 日以下の群刑務所への拘禁刑若しくは 2,000\$ 以下の罰金又はこれらの併科（N.R.S. 193.140）】
 - (1) 脅迫の対象が学区又はチャータースクールの生徒又は職員であり、脅えさせられる、困らせられる、追い立てられる、不安にさせられる、又は苦しめられる状態にさせられる
 - (2) パニック又は精神的な動揺
 - (3) チャータースクールを含むがこれに限られない、公立学校の業務への妨害
3. このセクションにおいて、

- (a) “Cyber-bullying”はNRS 388.123におけるその意味を持つものとみなす。
- (b) 口頭、書面、又は電子的な通信には、次のいずれかのものを含むが、これらに限られない。
- (1) 手紙、メモ、又はその他の種類の書面による通信文
 - (2) 人又は郵便若しくは配達サービスにより配達されるメールアイテム又はパッケージ
 - (3) テレグラフ若しくは有線サービス又はその他の類似の通信手段
 - (4) 電話、携帯電話、衛星電話、ページ若しくはファクシミリマシン又はその他の類似の通信手段
 - (5) 無線、テレビ、ケーブル、有線、無線、衛星、その他のオーディオ若しくはビデオ放送若しくは伝達又はその他の類似の通信手段
 - (6) オーディオ若しくはビデオの記録若しくは複製又はその他の類似の通信手段
 - (7) emailのアイテム、モデム、若しくはコンピュータ・ネットワーク若しくはインターネット、又はその他の類似の通信手段
- (131) 法定刑についてはAR ST § 5-4-401.
- (132) N.R.S. 392.915.2 (b)(3) (ネヴァダ州)は、公立学校の業務への妨害が発生した場合には、重軽罪に刑を加重している。
- (133) ①で述べたように一定の年齢の者のみを客体とする規制はその現れである。
- (134) N.C.G.S.A. § 14-458.1. 行為者が18歳以上であれば1級軽罪、18歳未満であれば2級軽罪 (N.C.G.S.A. § 14-458.1 (b)参照)。
N.C.G.S.A. § 14-458.1
- (a) この規定 (Article) により不法とされる場合を除き、何人も、次の目的でコンピュータ又はコンピュータ・ネットワークをする場合には不法である。
- (1) 未成年者を脅えさせる又は困らせるという意図を有して次のことを行うこと
 - a. フェイクプロフィール又はフェイクウェブサイトを構築する
 - b. 次の場で未成年者を装う
 1. インターネット・チャット・ルーム、2. 電子的メールメッセージ、若しくは、3. インスタントメッセージ
 - c. オンラインで未成年者を追いかける又はインターネットチャットルームにまで未成年者を追いかける
 - d. 未成年者に関わる私的な、個人的な、又は性的な情報を、投稿する、又は他人が投稿することを促進する【この項は内容規制であり、厳格な基準で求められる事項を充たしていないとして修正1条に違反する、というノースカロライナ州最高裁の判断 (State v. Bishop,

787 S.E.2d 814 (2016) が出ている。】

- (2) 未成年者又はその両親若しくは後見人を脅えさせる又は困らせる意図をもって
- a. インターネット上で未成年者の実際の画像又は修正された画像を投稿する
 - b. パスワードで保護されたアカウントへの侵入又はパスワードを盗む若しくはその他のパスワードへのアクセスを含む、コンピュータ・ネットワーク、コンピュータ・データ、コンピュータ・プログラム、又はコンピュータ・ソフトウェア、へのアクセスを変更、又は消去する
 - c. email 又はその他の伝達を含む、未成年者への反復的、継続的、又は持続的な電子的な通信のためにコンピュータ・システムを利用する
- (3) 真実か否かにかかわらず、第三者に未成年者をストークする、又は困らせる行為を即座に唆すことを意図して、そのような唆しを内容としているような事柄を述べること
- (4) 未成年者を脅えさせる又は困らせる目的で、当該未成年者に関わるデータの無権限コピーをコピーする及び拡散する、又は作成されるようにする（形式は、プリントされた、又はコンピュータ若しくはコンピュータ・ネットワーク内に存在する、これらにより通信される、若しくはこれらにより作成されるコンピュータ・データ、コンピュータ・プログラム、若しくはコンピュータ・ソフトウェアを含むがこれに限られない）
- (5) 未成年者を脅えさせる又は困らせる意図をもって、インターネットのポルノサイトに未成年者を登録する
- (6) 未成年者を脅えさせる又は困らせる意図をもって、未成年者又は未成年者の両親若しくは後見人による権限の付与なく、ジャンク電子メッセージ及びインスタントメッセージを受信するようなメーリングリストに未成年者を登録する
- (b) このセクションに違反する者は、cyber-bullying で有罪である。同罪は、被告人が犯罪行為時に 18 歳以上である場合には 1 級軽罪【45 日以下の community punishment（前科なき場合）及び（裁判所の裁量に基づく）罰金（N.C.G.S.A. § 15A-1340.23）】として可罰的である。被告人が犯罪行為時に 18 歳未満である場合には、同罪は、2 級軽罪【注：30 日以下の community punishment（前科なき場合）及び最大 1,000\$ の罰金（N.C.G.S.A. § 15A-1340.23）】として可罰的である。
- (c) このセクションの下での犯罪について有罪答弁をし、若しくは有罪であって、かつ当該犯罪が当該人が 18 歳になる前に犯されたものである場合にはいつでも、裁判所は、有罪判決に入らず、かつ被告人の同意を

得て、さらなる手続を延期し、そして、当該裁判所が要求する合理的な条件を付して、被告人をプロベイションに置くことができる。このサブセクションにおいて提供されているプロベイションの条件を充たしている場合、当該裁判所は、被告人を釈放し、被告人に対する手続を却下するものとする。このセクションの下での釈放及び却下は、有罪の裁判なくしてなされるものとし、このセクションの目的、又はある犯罪の有罪についての法律により課される資格はく奪若しくは制限の目的のために、有罪とみなされてはならない。このサブセクションに従い釈放及び却下をする場合、その者は、G.S.15A-146に規定される手続及び要求に従い、釈放及び却下に結びついた手続の完全な記録を消去する命令の適用を受け得る。

(135) V.A.M.S. 565.090. ただし、「21歳以上の者による、17歳以下の者に対する行為の場合」としており、被害者の年齢も要件となる。

V.A.M.S. 565.090. Harassment

1. 以下のいずれかを行う者はハラスメント罪を犯すものである
 - (1) 情を知って、他人に対し、重罪を行うとの脅迫をし、それによって、当該他人を追い立てる、脅えさせる、又は当該他人に精神的な苦痛を惹起させる
 - (2) 他人とコミュニケーションをとる際、情を知って、通常感覚を持つ者にとって攻撃的な、粗野な言葉を用いて、それによって、当該者を、攻撃的な物理的接触又は侵害を合理的な不安の下に置く
 - (3) 情を知って、匿名での電話の呼出し又は電子的な通信により、他人を追い立てる、脅えさせる、又は他人に著しい苦痛を惹起させる
 - (4) 情を知って、17歳以下である、又は17歳以下と称する他人とコミュニケーションをとって、それによって、かつ正当な理由なくして、無謀に、当該他人を追い立てる、脅えさせる、又は他人に著しい苦痛を惹起させる
 - (5) 情を知って、反復的に、欲せられないコミュニケーションを他人ととる
 - (6) 正当な理由なくして、他人を脅えさせる、脅えさせる、又は他人に著しい苦痛を惹起させる、他人を追い立てる、脅えさせる、又は他人が著しい苦痛をもつような状態を惹起する目的で、その他の行為を行い、当該行為への当該他人の応答がその者の年齢を考慮すると、平均的な感覚を持つ者によるものである
2. HarassmentはA級軽罪【注：1年を超えない拘禁刑、及び1,000\$を超えない罰金（V.A.M.S. 558.011.(5), V.A.M.S. 560.016.1(1)（原則的なルール））】である。ただし、次のいずれかの場合には、harassmentはD級重罪【注：4年を超えない拘禁刑、5,000\$を超えない罰金（V.A.M.S. 558.011.(4), V.A.M.S. 560.011.1(1)（原則的なルール））】である。

- (1) 21歳以上の者による、17歳以下の者に対する行為の場合
- (2) 有罪答弁を以前にした者、又は以前にこのセクションの違反若しくはこの州でなされた場合における州の群若しくは市の条例、州法、連邦法、又は軍法の罪で有罪と判断された者は、このサブセクションに列挙されている犯罪の違反として、処罰され、又は起訴され得る。

3. このセクションは、連邦、州、群、又は市の法律の違反の捜査に携わっている連邦、州、群、市、又は軍の法執行職員の活動には適用されない。

(136) 規定は次のとおり。N.J.S.A. 2C:33-4.1.

b. Cyber-harassment は、行為者が犯罪時に21歳以上でなく、かつ未成年者を cyber-harass する目的で未成年者になりすます場合でないには4級犯罪であり、このような場合には3級犯罪である。

c. 16歳未満の未成年者が cyber-harassment で非行と判断される場合には、裁判所は、判決に、当該未成年者は、親又は後見人の付き添いの下、十分な態様で、下記のうちのいずれか又は双方を完遂すべしとの条件を付けることができる。

- (1) サイバーハラスメント行為への傾向を抑制することが意図されたクラス又はトレーニングプログラム
- (2) サイバーハラスメントに関係する危険への覚知を導くことが意図されたクラス又はトレーニングプログラム

(137) N.J.S.A. 2C:33-4.1.

d. サブセクション c に基づいて裁判所により課された条件に従わない親又は後見人は、風俗を乱す者 (disorderly person) であり、初めの犯罪について 25\$ 以下、その次以降は、100\$ 以下の罰金に処される。

(138) N.C.G.S.A. § 14-458.1(c) (前掲注(134))

(5) キャンパス内外 (oncampus/offcampus) の理論とサイバーとの関係
サイバーいじめが教育現場において行われるものであるとすると、その現場における学生の言論の自由の限界が問題となり得る。学生に対する学校の処分の可能性が問題になった Tinker 事件はキャンパス内の言論に焦点を当てた判断であったし⁽¹³⁹⁾、Morse 事件は学校が協賛している場合にも学校による処分を可能とした⁽¹⁴⁰⁾。いずれにしてもキャンパス内+ α という限定があるといえる。このようなキャンパス内+ α という限定が有効な指標なのであれば、罰則を考える際にも考慮される要素となろう。

この点を意識したと思われる規定が次に示すアイダホ州法の規定 (I.C. § 18-917A) である⁽¹⁴¹⁾。この規定は「学校内」の要件を持つ点に特徴がある⁽¹⁴²⁾。「学校の所有地上に現在するか又は学校の活動における」という要件は、上記の Morse 事件の連邦最高裁の判断と整合的といえよう。

アイダホ州におけるサイバーいじめ対策立法

I.C. § 18-917A

- (1) 学校の所有地上に現在するか又は学校の活動における、生徒又は未成年者は、意図的に、他の生徒に対するハラスメント行為、おびえさせる行為又はいじめ行為を遂行する、又は遂行することを共謀してはならない。
- (2) このセクションにおいて、「ハラスメント、おびえさせる又はいじめ」とは、学生による、次のいずれかを充たす、あらゆる意図的なジェスチャ、又は意図的な書面、口頭、若しくは物理的な行為又は脅迫を意味する。
 - (a) 次のいずれかの結果を生むだろうことを、合理的な者が、当該状況において知るだろうもの
 - (i) 学生を害する
 - (ii) 学生の財産へ損害を与える
 - (iii) 学生の身体への害に関する合理的な恐怖の下に当該学生を置くこと
 - (iv) 学生の財産への害に関する合理的な恐怖の下に当該学生を置くこと
 - (b) それが、学生にとって、威嚇的で、脅迫的で、又は侮辱的な影響を与える教育環境を生成するのに十分に過酷、連続的で、又は広汎であるもの

ハラスメント行為、脅えさせる行為、又はいじめ行為は、陸線、車載電話、若しくは無線電話の利用、又はコンピュータ、

コンピュータ・システム、若しくはコンピュータ・ネットワークによりアクセスされるデータ若しくはコンピュータ・ソフトウェアの利用によっても実行され得る。

(3) 自らこのセクションの規定に違反した者は、違反罪になり得る。

しかし、サイバーいじめの刑事立法の文脈でキャンパス内+ α で行われた行為に限定するべきだとすることには疑問があり得る。というのは、電子的な通信を用いる場合には、問題となる行為が学校の活動におけるそれであるか否かが重要だとはいえない場合もあり得るからである。そもそもサイバーいじめは、明確に学校外における場においても、学校内におけるいじめの延長線上のコミュニケーションを可能にする点にその危険性があるといえる⁽¹⁴³⁾。現に、既に述べたように、サイバーいじめは家のコンピュータから行われることが多い(第3 2(1))。そうすると、サイバーいじめの処罰を学校内における行為に限ることに合理的理由はないとも考えられる。関連し、アイダホ州法の規定は、I.C. § 18-917A (2)最終文において、サイバーの文脈におけるいじめ行為も要件を充たし得ることを確認しているが、「学校内」の要件との関係が明瞭ではない。

さらに、キャンパス内+ α に限定すると、そもそも連邦のサイバーいじめ対策法案の契機となった Megan Meier 事件の被害者さえも保護できない等⁽¹⁴⁴⁾、規制から外れる行為が多く出てくると評価されることになる⁽¹⁴⁵⁾。結局のところ、対象行為をキャンパス内の行為に限定すべきではないといえそうである。

現に、他の州の規定をみてみると、アイダホ州法の規定と異なり、例えばアーカンソー州の規定は行為が学校教育の文脈で行われるか否かという点を考慮しておらず⁽¹⁴⁶⁾、また、ケンタッキー州の規定(KRS § 525.080⁽¹⁴⁷⁾)も通信が学校の所有地外で行われた場合も捕捉し得る⁽¹⁴⁸⁾と明示的に説明されている。とりわけ、ケンタッキー州の規定は、ハラスメント通信とは別に一般のハラスメント規制(KRS § 525.070⁽¹⁴⁹⁾)

を有しており、そこでは、実質的に学校内の要件を用いていることと比較すれば、通信に関しては、別の行為態様で規制すべきであるという考えの下に立法したことがうかがえる。ケンタッキー州の規定は、ハラスメントの一類型としていじめを位置付けているがゆえにいじめ規制としては徹底していないと批判されもするが⁽¹⁵⁰⁾、サイバーの特徴に即応し得るような規制であるとはいえ、その意味では1つの合理的な立法方法だと考える。

以上からすれば、サイバーの特徴ということを考えれば、キャンパス内外を基準とした限定は罰則の観点からは不要であるべきだといえそうである。

(139) King, *supra* note 10, at 870.

以下は Tinker 事件 (Tinker v. Des Moines Independent Community School Dist, 89 S.Ct. 733 (1969)) の概略。

〔事案〕 Tinker を含む 3 人の学生は、ベトナム戦争に反対する黒い腕章を着用して登校する計画を立てた。これに対し、学校側は、腕章を取るように要求でき、これを拒否した場合には、腕章を取るまで停学にすることができるというポリシーを採用した。Tinker らは、これに気づきつつも、黒い腕章を着用して登校したところ、家に帰され、停学にさせられた。Tinker らは、この処分の差止めを求めて出訴した。1 審は、学校側の行為が校内秩序への妨害の防止のために合理的だとして合憲だとし、2 審も 1 審の判断を是認した。

〔判旨の概要〕 ここでの問題は、学校環境という特殊な場における修正 1 条の権利の限界論である。本件は、スカートの長さ、服装、ヘアスタイル等の態度が問題になった事案とは異なる。また、攻撃的、破壊的な活動又はグループのデモでさえない。我々は、「純粋な言論」と同種の直接、主たる第 1 修正の権利を問題にしている。また、本件の行為は、学校の業務や他の学生の権利を妨害する言論や活動とは関係ない。学校側が特定の意見の表現の禁止を正当化するためには、当該行為が、単なる不快や不愉快を回避したいという欲求を超えるものにより惹き起こされていることを示せなければならない。禁止された行為への従事が、「学校の運営における適切な規律の必要を重大で、著しく妨害する」という認定や示唆がない場合には、当該禁止は維持され得ない。本件ではそのような重大で著しい妨害の証拠はないから、ある特定の意見の表現の禁止は憲法的に許されない。

(140) *Morse v. Frederick*, 127 S.Ct. 2618 (2007).

〔事案〕 学校に許可され、学校により監督されているイベントにおいて、申立人である校長 Morse は、学生が“BONG HiTS 4 JESUS,”と書かれた垂れ幕を掲げているのを発見した。Morse は、その垂れ幕を違法ドラッグの使用を助長するものとして理解した。そのようなメッセージを学校のイベントにおいて禁止する学校のポリシーに基づいて、Morse は垂れ幕を片付けるよう命令した。イベントに垂れ幕をもってきた学生のうちの1人 (Frederick) がこれを拒否したので、Morse は、この垂れ幕をとり上げて、その後、彼を停学に処した。学校の管理部門 (superintendent) は停学を支持し、Frederick は懲戒されるべきである、なぜなら、彼の垂れ幕は、学校のポリシーに違反して、違法なドラッグの使用を助長するように見えるからである、と説明した。教育委員会も停学処分を支持した。これに対し、Frederick は、42 U.S.C. § 1983 に基づき訴えを提起し、修正1条の権利を教育委員会及び Morse が侵害していると主張した。1審は、Frederick の言論の権利は侵害されてはいなかった、としたが、第9巡回区連邦控訴裁判所が逆に修正1条の権利が侵害されたと判断したので、上訴。

〔(学校における言論ではないという主張に対する) 判断の概要〕

イベントは通常の学校の時間帯の中で行われ、校長である Morse により「許された社会イベント又はクラストリップとして」許可されたものである。学区のルールは、「許された社会イベント及びクラス旅行」における生徒は、その行為について学区のルールに服する、と明示している。教師や管理者は、学生の間にもちりばめられ、監督する責任を負っていた。その状況において Frederick は、学校からの路上において他の JDHS の学生達の間にも立って、垂れ幕を学校の方向に向けて、ほとんどの学生達に明白に見えるようにした。以上からすると、学校における (at school) ということの外延は不明確であり得るが、本件は、学校における言論に関する先例を適用すべき場合である。

(141) 違反罪という制裁は、他の州の規定と比較して軽い寛容なものだと評価されている (*Brady, supra* note 3, at 29-30)。

(142) ケンタッキー州の一般のハラスメント罪の規定 (KRS § 525.070) も同様であるが (KRS § 525.070 (1)(f)参照)、同州はハラスメント通信に関する規定を別にもっている点に特殊性がある (KRS § 525.080)。詳しくは後述する。規定自体については前掲注(126))。

(143) 10代の者のオンラインの行動は、オフラインの生活の単なる延長であると指摘する者に *Fertik & Thompson, supra* note12, at 106.

(144) *King, supra* note 10, at 872.

(145) *King, supra* note 10, at 872.

(146) *Brady, supra* note 3, at 29.

(147) 前掲注(126)

(148) Guidelines to Assist School Districts Implement HB 91 (KRS 158.156) (<http://education.ky.gov/school/sdfs/Documents/Guidelines%20to%20Assist%20School%20Districts%20Implement%20HB%2091.doc>). FAQ's (Frequently Asked Questions about Bullying) 12. (<http://education.ky.gov/school/sdfs/Documents/Bullying%20FAQ%20May%202013.doc>) は、キャンパス外でサイバーいじめが起きた場合においても、可罰的であるから警察に届け出るべきだとしている。

いずれもケンタッキー州の教育省の HP 上に存在する資料である。

(149) 前掲注(126)

(150) Enoc, *supra* note 34, at 440.

(6) 小括

以上、サイバーいじめに対する処罰規定をサイバーいじめの定義や特徴を議論する際に用いた軸に基づいて分類しつつ概観してきたが、州によりその規定形式が多様であることがわかる。憲法上の疑義が生じている規定もあり、現実に立法がなされ運用がなされている場合であっても鵜呑みにすることは禁物である。

次の3では、サイバーいじめの一行為形態としてのオンラインなりすましを、いわばサイバーいじめ各論として、サイバーいじめ規制の見地から検討してみたい。

3 サイバーいじめ各論としてのオンラインなりすまし

Megan Meier 事件でみたように、未成年者に対するオンラインにおけるなりすまし⁽¹⁵¹⁾に基づくコミュニケーションが自殺を惹き起こすことがある。1人の加害者が、多数のアカウントを用いて攻撃する場合(同時攻撃可能性(第3 2(3)③))においても、なりすましが相当程度含まれていることは想像に難くない。それゆえ、オンラインなりすましは、サイバーいじめの典型的な類型として議論されることになる。ここでは、サイバーいじめの各論1つとして、このオンラインなりすましを検討してみたい。もっともサイバーいじめの処罰立法の中には学校の所有地において行われることを要件としていること、サイバーいじめは教育に関する法律の違反にしかならないがオンラインなりすま

しは刑法の問題であることを理由としてオンラインなりすましをサイバーいじめの議論から切り離そうとする理解もある⁽¹⁵²⁾。そこで、事前にオンラインなりすましとサイバーいじめとの関係について概観してから、個別論点の検討を行いたい。

まず、オンラインなりすましの危険性を考えてみるに、オンラインなりすましには、非対面的な状況下でなりすましが行われることで、相手の人格の識別自体がより難しくなり、加害者の行為が助長されやすく、結果、被害の助長もみられやすいといえそうである（第3参照）。サイバーいじめの規制との関係では、いじめ目的でのオンラインなりすましには典型的に侵害の助長効果があるといえ、処罰することに一定の理由があるともいえそうである。現に、いじめ目的でのなりすましをサイバーいじめの一類型に入れることを明示する州法の規定⁽¹⁵³⁾もある。

一方で、オンラインなりすましがフィッシング詐欺等、他の犯罪の手段にも使われ得ることも指摘されている。例えば、オンラインなりすましを処罰するカリフォルニア州法の規定（Cal.Penal Code § 528.5⁽¹⁵⁴⁾）のことをサイバーいじめ対策規定に位置付ける理解もあるなかで⁽¹⁵⁵⁾、同法の規定ぶりはそれだけにとどまらず、より一般的なものである、と指摘する理解もある⁽¹⁵⁶⁾。オンラインなりすまは、金銭的な問題以外の弊害も惹き起こすし、被害者の年齢も問わない⁽¹⁵⁷⁾のであり、サイバーいじめの議論のみで、この種の犯罪類型を語ることの適切性には疑問が提起され得る。このような理解からは、なりすまし独自の当罰性はサイバーいじめとは別のものとして議論されるべきともいえそうである。ニューヨーク州（NY PENAL § 190.25⁽¹⁵⁸⁾）のように、いじめ対策ではなく、一般的ななりすまし罪の中にオンラインなりすましを規定するという手法にも妥当な面があり得ることになる。

さらに、今後の課題としておきたいが、オンラインなりすましとIDセフト（及びIDの不正使用）は一定の局面では区別できないのではないかと、とも思われる（逆にいえばまとめて考察すべきだともいえる（後述(4)で

少し紹介する))。

以上を意識しながら、サイバーいじめを検討対象とする本稿の問題意識に基づきつつ、一般的ななりすましの研究は別の機会に行うことにして、オンラインなりすまし罪といえる規定の処罰範囲や限定の工夫についてみていくことにする。一般的なオンラインなりすましの防止についても、例えばソーシャルメディアを運営する会社が一定のポリシーを策定しこれを適切に運用することで法律の外における努力が奏功することも予測され⁽¹⁵⁹⁾、このことは処罰範囲を限定する契機になると思われるが、ここでは、ひとまず、現行の処罰規定を中心に検討したい。

規定の傾向を分析する軸として、誰が保護対象かという法益主体の軸、目的犯たるオンラインなりすまし罪における意図（目的）の内容（金銭目的か、困惑目的か）という目的要件の軸、及びなりすますという行為の内容面という軸等について、規定上の対応の有無をみていきたい。

(151) ここで問題となっているのは別人格であるとコミュニケーションの相手方に思わせる行為であって、我が国の不正アクセス行為の禁止等に関する法律 11 条、3 条に基づく不正アクセス罪に該当する行為のように、他人の識別符号を入力等して達成されるなりすましとは（部分的に重なり合うが、）異なるものであることに注意されたい。

(152) Ramirez, *Online Impersonation A New Forum for Crime on the Internet*, 27 CRIM. JUST. 6, 9 (2012).

(153) 例えば、F.S.A. § 1006.147 (3)(b).

(154) Cal.Penal Code § 528.5.

(a) 法律の他の規定にもかかわらず、他人に害を与える、脅えさせる、脅迫する、又は騙す目的で、情を知って、同意なく、インターネットのウェブサイトを紹介して、若しくはインターネットのウェブサイト上、又はその他の電子的手段により、確実に、現実の他人になりすます者は、サブセクション(d)に基づき有罪である。

(b) このセクションの目的のために、被告人が、なりすまされた者であった、又は、であると、他人が合理的に信じるであろう、又は、信じた場合に、なりすましは確実な (credible) ものである。

- (c) このセクションの目的のために、「電子的手段」は、他人の名前で email アカウント、又はソーシャルネットワークインターネットウェブサイト上のアカウント若しくはプロフィールを開設することを含むものとする。
- (d) サブセクション(a)の違反は、1,000\$ 以下の罰金刑若しくは群の刑務所での1年以下の拘禁刑又は罰金刑と拘禁刑の併科により処罰される。
- (e) その他の民事的救済が可能な場合に加え、(a)の違反を理由として損害又は損失を被った者は、502条の(e)の(1)、(2)、(4)及び(5)、並びに同条の(g)に従い、侵害者に対して、損害賠償、及び差止めの救済、又はその他のエクイティ上の救済を求めて、私訴を提起することができる。
- (f) このセクションは、法律の他の規定の下での起訴を排除しないものとする。
- (155) Andrea Koskey, *New Year Brings New Law Targeting Cyberbullying*, SF Examiner (Dec. 31, 2010), (<http://archives.sfexaminer.com/sanfrancisco/new-year-brings-new-law-targeting-cyberbullying/Content?oid=2167109>), Malone, *Parody or Identity Theft: The High-wire act of Digital Doppelgangers in California*, 34 *Hastings Comm. & Ent L.J.* 275, 310 (2012)
- (156) Wegman, *Cyberbullying and California's Response*, 47 *U.S.F. L. Rev.* 737, 742 (2013). サーベイも、カリフォルニア州がサイバーいじめ対策の処罰規定を有するとは考えていない。
- (157) Reznik, *Comment Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation*, 29 *Touro L. Rev.* 455, 477 (2013).
- (158) NY PENAL § 190.25
- 次のいずれかを行う者は2級のなりすまし罪で有罪である。
1. 利益を得る、若しくは他人を傷つける若しくは騙す意図をもって、他人になりすまし、そしてなりすまされた人物として活動する
 2. 利益を得る、若しくは他人を傷つける若しくは騙す意図をもって、ある者又は組織の代表者のふりをし、そしてなりすまされた権能を行使する
 3. (a)公務員のふりをする、権限なく、そのような公務員であることを適法に識別できるユニフォーム、バッジ、記章若しくはそれらの複製を着用若しくは表示する、又は言葉若しくは行動により、自身は公務員である、若しくは公共機関若しくは公共部門の許可若しくは権限を与えられて行動している旨の内容の虚偽の表現をし、そして(b)なりすまされた公務員の権威に従わせる、資金を求める、又はその他の虚偽の供述に依拠して行動させるという意図をもって行動する
 4. インターネット・ウェブサイト若しくは電子的手段による通信により、

利益を得る、若しくは他人を傷つける若しくは騙す意図をもって、他人になりすます、又はそのような通信により、公務員という権威に従わせたり、虚偽の供述に依拠して行動させたりするために、公務員のふりをする

2級なりすまし罪はA級軽罪【注：1年を超えない拘禁刑及び1,000\$を超えない罰金（NY PENAL § § 70.15.1, 80.05）】である。

(159) Malone, *supra* note 155, at 308-309.

(1) 保護対象

まず、犯人がAになりすまして、Bとコミュニケーションをとる場合には、「なりすまされた者」であるAが保護されるのか、それとも「コミュニケーションの相手方」であるBが保護されるのか、という問題が生じる⁽¹⁶⁰⁾。この点、規定形式から法益主体の推認がある程度可能である。コミュニケーションの相手方を何らかの形で害する意図や目的を要件としている場合には、Bの保護を行おうとしていると推測し、Aの同意がないことを要件としている場合には、Aの保護を行おうとしていると推測することができる。

まず、NY PENAL § 190.25 (4)⁽¹⁶¹⁾は、コミュニケーションの相手方のみを問題にしているように見える。これに対し、ノースカロライナ州の規定⁽¹⁶²⁾ (N.C.G.S.A. § 14-458.1) は、N.C.G.S.A. § 14-458.1 (a)(6)で未成年者等からの権限付与を問題にしているように、なりすまされる対象である当該未成年者に害を与えることを処罰しようとしていると読めるので、なりすまされた者の保護を重視しているといえる。

そのほか、カリフォルニア州の規定 (Cal.Penal Code § 528.5⁽¹⁶³⁾)、ミシシッピ州の規定 (Miss. Code Ann. § 97-45-33⁽¹⁶⁴⁾) はコミュニケーションの相手方を保護している建付けであるが、「同意なく」という要件も有しており、双方を重視している。テキサス州の規定 (V.T.C.A., Penal Code § 33.07⁽¹⁶⁵⁾) も双方を同程度に重視しているようにみえる。

以上の調査結果だけからすると、統一的な理解は難しく、なお、なりすましの本質論が研究課題として残る。他方で、この議論は、次に述べる、なりすましの対象の実在性についても影響を与える。

(2) なりすましの対象—現実の (actual) 人という要件—

規定をみてみると、カリフォルニア州法の Cal.Penal Code § 528.5 は、Megan Meier 事件において CFAA で処罰できないという帰結をもたらした処罰の欠缺に対応するという趣旨も含めて立法された⁽¹⁶⁶⁾。ニューヨーク州の判例もサイバーに特化してはいない規定についてはあるが、なりすまし罪においては現実の人になりすますことが必要だという⁽¹⁶⁷⁾。しかし、カリフォルニア州の規定においてはなりすましの対象は現実の他人である必要が明示されているので、架空の人物になりすました Megan Meier 事件に適用できないとの指摘があり⁽¹⁶⁸⁾、問題が生じる。なぜなら、サイバーいじめの文脈において、非対面通信の濫用による不安の増幅がみられることは既にその特徴論で述べたが、サイバーいじめの議論を巻き起こした Megan Meier 事件においても、被害者は架空の人物の存在を信じていたのであるから、そのような事案のみを捕捉すれば足りるともいえそうだからである。(1)で述べた議論に関連し、通信の相手方ではなく、なりすまされた者を保護する、と考えるのでない限り、かつカリフォルニア州の規定は、文言だけからみればコミュニケーションの相手方の保護にシフトしているといえるのであるから ((1)参照)、少なくともサイバーいじめの文脈においては、この要件は不要ではないか、と思われる。

(3) なりすましの程度

さらに問題になるのは、なりすまし行為が、どの程度、コミュニケーションの相手方に、なりすまされた者が行為していると信用させるものであるか、ということ、いわば誤信の危険性の程度である。例えば、フェイクプロフィールといっても、誤信の危険性が当該プロフィールの内容にも依存することは明らかである。この点、なりすましことにつき、規定上、解釈の手がかりを置かない州 (ノースカロライナ州 (N.C.G.S.A. § 14-458.1⁽¹⁶⁹⁾)、ニューヨーク州 (刑法 § 190.25⁽¹⁷⁰⁾)、テキサス州 (V.T.C.A., Penal Code § 33.07⁽¹⁷¹⁾)) もあるが、通信の相手方がどのような認識を得るか、ということが文言からは明らかではない。

この点、カリフォルニア州法 (Cal.Penal Code § 528.5⁽¹⁷²⁾) は、現実に他人が騙される必要はない⁽¹⁷³⁾とされつつも、「被告人が、なりすまされた者であった、又はその者であると他人が合理的に信じるであろう、又は信じた場合に、なりすましは確実なものである。」という規定を置き⁽¹⁷⁴⁾、これを要件としている。ミシシッピ州 (Miss. Code Ann. § 97-45-33) も同様の規定を置く。しかし、このような定義で十分だろうか。非対面通信下におけるコミュニケーションは、対面している場合の(視覚、聴覚等の観点からの) マルチモーダルなそれと異なり、かなりの種類の情報が落ちているので、それゆえに騙されやすいということができる場合もある反面、特定の誰かであるという確証をも持ちづらい。現に、ニューヨーク州のなりすまし罪のコンメンタールが「匿名で通信が行われることが通常であるインターネットにおいては、他の識別可能な者へなりすますることが通常行われるわけではないから、「他人になりすます」ことをどのように解するかが問題となる」という指摘をする⁽¹⁷⁵⁾。この指摘は、なりすましの態様をなお具体化する必要がある、という現行規定に対する批判的な指摘として読むこともできよう。

結局、なりすます、という要件は、その具体化の試みも含め、オンラインという非対面通信下でのコミュニケーションに即応しているものであるかについてなお分析すべき課題を含んでいる。将来的に VR (Virtual Reality) 技術が普及する社会をも考えると、なりすましの概念を社会科学の観点からのみ考察するのも難しくなるかもしれない。

(4) 意図の内容とその認定

オンラインなりすまし罪は、なりすました後に発生し得る侵害を客観的要件とするのではなく、なりすます目的を主観的要件として掲げることが多い。主観的要件として、ハラスメントやいじめに関連する目的と金銭的なものに関連する目的が掲げられることになる。

主観的要件をいじめることに関連する事実限定すれば、その罪は、自ずと、いじめ対策の意味合いをもってくる。例えば、いじめに特化した目的を有するように規定したノースカロライナ州のサイバーいじ

め罪 (N.C.G.S.A. § 14-458.1⁽¹⁷⁶⁾) は、「脅えさせる、又は困らせるという意図」を問題にするのみである。もっとも同州は、ID セフト罪を別の規定として持ち (N.C.G.S.A. § 14-113.20)、それにより両罪あわせて金銭的な事柄と未成年者保護に関心を有していると評価されている⁽¹⁷⁷⁾ (冒頭で述べたとおり、オンラインなりすましと ID セフトとの間には区別しがたい領域が生じている)。

次に問題となるのは、要件たる意図の認定方法である。意図の認定においては、なりすました上で行為者が何をしたか、ということが重要となる。ニューヨーク州の判例である *People v. Golb*, 23 N.Y.3d 455, 466 (2014) は、他人名義でアカウントを作成するだけでは足りず、さらに、email が他人の名義で送られたものであっても、意見を尋ねたり、批判に答える準備をしているか否かを尋ねたりするにとどまっていた場合にも、例えば害を与える等の意図の立証ができず、犯罪を構成しないと述べる。しかし、これで基準が明確になっているとは言い難いだろう。現に、カリフォルニア州の規定に対して、実際には害意と嫌みやパロディとの区別ができない、とする批判がある⁽¹⁷⁸⁾。

意図の認定問題も、なりすましの程度と同じく、その明確化には課題が残る。

(5) 小括

オンラインなりすましについては、それ自体の当罰性の検討を行うべきだということだけでなく、なりすましの態様や意図の認定方法がオープンであり、具体化された定義が求められていることがわかる。ここでの検討も含めて、オンラインなりすましの本格的な検討は、別の機会に行うことにしたい。

(160) オンラインなりすましの規制においては、コミュニケーションの相手方が保護されるものと考えがちであるが、騙された者ではなく、なりすまされた者の名前やレピュテーションが保護される、と整理する論稿もある (*Derzakarian, The Dark Side of Social Media Romance: Civil Recourse for Catfish Victims*, 50 *Loy. L.A. L. Rev.* 741, 744 (2017))。もっとも、こ

の点こそ検討が必要だと思われる。

(161) 前掲注(158)

(162) 前掲注(134)

(163) 前掲注(154)

(164) 次に示すミシシッピ州の規定 (Miss. Code Ann. § 97-45-33) は、カリフォルニア州の規定 (Cal. Penal Code § 528.5) とほぼ同じであるが、(1)に「確実に」の文言がないという問題を抱えていると思われる。

Miss. Code Ann. § 97-45-33. On-line impersonation; offense; penalty

- (1) 法律の他の規定にもかかわらず、他人に害を与える、脅えさせる (intimidate)、脅迫する (threaten)、又は騙す (defraud) 目的で、情を知って、同意 (consent) なく、インターネットのウェブサイトを通じて、若しくは、インターネットのウェブサイト上、又はその他の電子的手段により現実の (actual) 他人になりすます者は、軽罪である。
 - (2) このセクションの目的のために、被告人が、なりすまされた者であった、又は、であると、他人が合理的に信じるであろう、又は信じた場合に、なりすましは確実な (credible) ものである。
 - (3) このセクションの目的のために、「電子的手段」は、他人の名前で email アカウント、又はソーシャルネットワーキングインターネットウェブサイト上のアカウント若しくはプロフィールを開設することを含むものとする。
 - (4) このセクションの侵害は、250\$ 以上 1,000\$ 以下の罰金若しくは 10 日以上 1 年以下の拘禁刑、又は、双方により処罰される。
 - (5) このセクションは、法律の他の規定の下での起訴を排除せず、それらを補充するものとして考えられるものとする。
- (165) V.T.C.A., Penal Code § 33.07. オンラインなりすまし 【2011 年改正で表題がオンラインハラスメントから変更された。】
- (a) 他人の同意を取得しないで、かつ誰かを傷つける、騙す、脅えさせる、又は脅迫する意図をもって、次のいずれかを行うために、他人の名前又はペルソナを利用する者は、罪を犯すものである。
 - (1) 商用の SNS 又はその他のインターネット・ウェブサイトにおいてウェブページを作成すること
 - (2) 1 又は 2 以上のメッセージを、email プログラム又はメッセージボードプログラム上又はそれらを利用せずに、商用の SNS における又はその他のインターネット・ウェブサイト上又はそれらを介して、投稿又は送信すること
 - (b) 名前、ドメインアドレス、電話番号、又は人に属するその他の識別情報のアイテムを参照する、email、インスタントメッセージ、テキストメッセージ又は類似の通信を送信する者であって、次の全てを充たす者は、罪を犯すものである。

- (1) 当該他人の同意を取得していないこと
 - (2) 通信の受信者において、当該他人が当該通信について権限を与えた、又は当該他人が当該通信を送信したと合理的に信じさせる意図をもっていること
 - (3) 人を傷つける又は騙す意図をもっていること
 - (c) (a)の罪は3級重罪【注：2年以上10年以下の拘禁刑若しくは10,000\$以下の罰金又はこれの併科（V.T.C.A., Penal Code § 12.34）】である。当該犯罪が、行為者が救急隊員（emergency personnel）による応答を求める意図をもって犯される場合で、3級重罪であるときを除き、(b)の罪はA級軽罪【注：1年を超えない拘禁刑若しくは4,000ドルを超えない罰金又はこれの併科（V.T.C.A., Penal Code § 12.21）】である。
 - (d) このセクションの下で犯罪に該当する行為が、他の法律における犯罪にも該当する場合、行為者は、このセクション、当該他の法律、又はその双方で起訴され得る。
 - (e) 行為者が、次のいずれかのエンティティである、又は行為者の行為が、次のいずれかのエンティティの従業員として行われた行為からしか構成されないということは、このセクションの下での起訴に対する抗弁である。
 - (1) 商用 SNS
 - (2) インターネットサービスプロバイダ
 - (3) 47 U.S.C. Section 230 で定義されるインタラクティブコンピュータ・サービス
 - (4) Section 51.002, Utilities Code で定義されるところのテレコミュニケーション・プロバイダ
 - (5) Section 66.002, Utilities Code により定義されるところのビデオサービス・プロバイダ又はケーブルサービス・プロバイダ
 - (f) このセクションにおいて
 - (1) 「商用 SNS」とは、直接又はリアルタイム通信を介して他のユーザとの人的関係を構築する目的、又は公衆若しくは他のユーザ達に利用可能なウェブページ若しくはプロフィールを作成する目的で、登録ユーザになることを可能にするウェブサイトを運営するビジネス、組織又はその他の類似するエンティティのことをいう。この文言は、電子的なメールプログラム又はメッセージボードプログラムを含まない。
 - (2) 「識別情報（identifying information）」は、§ 32.51 によって当てられた意味を持つ。
- (166) SENATE JUDICIARY COMMITTEE, Senator Ellen M. Corbett, Chair, 2009-2010 Regular Session, SB 1411 (Simitian), As Amended March 25, 2010, Page 2, (April 20, 2010) (http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200920100SB1411).

- (167) 本文で紹介している Cal.Penal Code § 528.5 はニューヨーク州刑法 190.25 をモデルにしたとされるところ (SENATE COMMITTEE ON PUBLIC SAFETY, Senator Mark Leno, Chair S, 2009-2010 Regular Session, SB 1411 (Simitian), As Amended March 25, 2010, Page 13, (April 13, 2010) (http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200920100SB1411))、ニューヨーク州刑法 § 190.25 (1) についての判例も、なりすましの対象について現実の (real) 人であることを要求している (People v. Sadiq, 236 A.D.2d 638, 654 N.Y.S.2d 35 (2nd Dept. 1997))。
- (168) Barchie, Online Impersonation Law: Cyber-Bullies Beware? (2011) (http://www.lawlandblog.com/2011/01/online_impersonation_law_cyber.html)
- (169) 前掲注(134)
- (170) 前掲注(158)
- (171) 前掲注(165)
- (172) 前掲注(154)
- (173) SENATE COMMITTEE ON PUBLIC SAFETY, Senator Mark Leno, Chair S, 2009-2010 Regular Session, SB 1411 (Simitian), As Amended March 25, 2010, Page 12, (April 13, 2010) (http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200920100SB1411).
- (174) これに対して憲法上の疑義も提起されてはいるが (Malone, *supra* note 155, at 275)、憲法上の論点に関する検討は見送りたい。
- (175) Practice Commentary by William C. Donnino (3) in Westlaw international.
- (176) 前掲注(134)
- (177) Reznik, *supra* note 157, at 477. これに対して、IDセフトとオンラインなりすましの関係について、前者は利得目的であることが多いが、後者はそうでないという点に差があるという理解もある (Clanton, We Are Not Who We Pretend To Be: ODR Alternatives To Online Impersonation Statutes, 16 Cardozo J. Conflict Resol. 323, 331 (2014), Derzakarian, *supra* note 160, at 750)。しかし、オンラインなりすましの中にも利得目的のものがあることを示す立法例 (特に NY PENAL § 190.25.4) の存在を前提にすると、傾向として述べる以上に動機面で区別する実益はないように思われる。
- (178) Levine, New law confronts cyberbullying (2011) (<http://www.stanforddaily.com/2011/01/06/new-law-confronts-cyberbullying/>), Shiels, California looks to outlaw online impersonation (2010) (<http://www.bbc.com/news/technology-11045070>)

4 【補説】サイバーいじめに関する規定を連邦法で規定することの是非

補説として、連邦法で規定することが望ましい、という見解を紹介したい。サイバーいじめを、最終的には、州法ではなく連邦法で規定すべきという主張がある。すなわち、サイバーいじめは特にインターネットを用いて行われ、データの転送は州をまたいで行われるだろう。そうであれば、データへアクセスする可能性が常にあるインターネットによる行為を規制するルールが、各州のローカルルールで別々に規制されていることは、ネットユーザにとって望ましい事態ではなく、連邦法で規制すべきである、というのである⁽¹⁷⁹⁾。

インターネットへのアクセシビリティの観点からすれば、この主張は合理的なように思われる。

(179) Burrichter, *supra* note 15, at 172. さらに Meredith, *supra* note 62, at 326, 334.

第6 我が国の議論への示唆

—わが国の現状の議論及び法律状態も踏まえて—

以上、アメリカにおけるサイバーいじめの法律論には若くてまだ洗練されていない面もあるが⁽¹⁸⁰⁾、現実の立法を素材とした検討は現時点においても可能であるという理解に基づき、立法方法について一定の分析を行った。

連邦の法案の法制化が憲法上の疑義により頓挫していることと並び、州法においても憲法上の疑義をクリアできているか否かが定かではない規定があることも踏まえると、アメリカの議論の直輸入には慎重になるべきである。それゆえ、我が国における議論を展開する際には、アメリカの議論も一つの要素とした上で、別の国の議論も踏まえたものにしていく必要があり、なお課題が残る。このことを前提としつつ、我が国の議論や現実の立法の精査については他日を期したいが、第5

までの議論から示唆が得られ得る点について若干指摘しておきたい。

我が国の刑罰規定を考える際の処罰範囲の限定等の観点からの重要な視点は保護法益の特定の議論である。アメリカでは保護法益論は正面から詳細に展開されないが、既に述べた侵害結果の限定（第5 2(2)）の議論から保護法益の候補を抽出できると思われる。アメリカにおける侵害結果の限定の工夫からは、死又は重大な肉体的傷害についての合理的な恐怖、及び著しい精神的な苦痛が保護法益の抽出の要素となり得る。いずれも恐怖や精神的な苦痛という意味では、広い意味では精神的な自由が保護法益だといえるが、サイバーの文脈では前者を保護する程度は相対的に低いという指摘がなされており、物理世界におけるいじめと異なり、肉体的傷害についての恐怖を保護する必要はないのではないか、という具体化した知見を得ることができた。アメリカ法からの示唆だけで即断できず、さらなる研究を要する点もあろうが、保護法益を、精神的な自由のうちの、著しい精神的な苦痛を与えられない利益と考えるのは1つの合理的な考え方だと思われる。

保護法益を定式化した後には、構成要件的行為をどのように定義するか、という問題がある。アメリカでは、いじめ一般について、反復的な攻撃が問題とされることがあるが、サイバーいじめの処罰立法を考える際も同様だとして、例えば行為の繰り返しという意味での反復性を要件とすべきであろうか。サイバー空間における、emailを含む電子的通信により送られたメッセージ等の拡散容易性、侵害の持続性に基づく一定のコミュニティ内の人間関係の継続的悪影響を踏まえれば（ラブレターのデータがクラス中に送信頒布される場合）、反復性の要件を外すことも正当化されるとするの一案だと思われる⁽¹⁸¹⁾。むしろ、その場合には、我が国の法律論としては、公然の要件や流布（結果的に不特定又は多数の者が知るように情報を伝達すること）の要件が検討されることになる。今1つの方向性としては、被害者若しくは特定かつ少数の者に対する反復的な情報伝達行為、又は不特定又は多数の者に対する単発の情報伝達行為という2類型に分けて考えるという方法もあり得る。

もっとも後者については、特定かつ少数のコミュニティにおける行為もいじめになるから、不特定又は多数という概念を利用した限定の意義については慎重な検討が必要である。例えば、被害者の所属する学校等のクラス等といったコミュニティの構成員が継続的に当該情報を受信可能であって、被害者がその閲覧可能性を左右できない場合に限定した方が有意な場合もあると思われる。もっとも、この点は、アメリカ法の検討のみから有用な知見が得られたわけではないので、今後の課題となる。

また、規定上、年齢制限や年齢に応じた刑の加重減軽といった方法の是非が問題になり得る。いじめというと主たる当事者は学生となり、典型的にみて精神面での脆弱性を有する学生を保護する必要もあるといい得る。しかし、州法をみてみると年齢や被害者の属性に対する立法としての対応はまちまちであった。立法で対応すると判断が硬直的になるので、年齢制限等を行うべきか否かについては、さらに別の国も参照しながら、よりよい規制方法を探求すべきであり、この段階では結論を出せない。

場所の限定を行うべきかも問題となる。多くのいじめ行為が学校において生起していることに照らし、学校内のいじめ行為というように限ろうとすると、サイバーのもつ場所的非依存性により立法が困難となる。学校内における継続的な人間関係は学校外においても継続し⁽¹⁸²⁾、むしろ、そのような人間関係から逃れられなくなっている点にサイバーいじめの問題点がある⁽¹⁸³⁾。そうすると、学校内で行われる行為等に限定すると、十分な捕捉範囲が得られないことになりかねない。その意味で、アメリカ法の検討(第5 2(5))で得られたように、対象行為をキャンパス内の行為に限定すべきではない。

サイバーいじめの文脈におけるオンラインなりすましは、アメリカにおいては、Megan Meier 事件における Drew の行為によりクローズアップされた。現にカリフォルニア州のオンラインなりすまし罪は Megan Meier 事件のような事案に対応することも立法趣旨の1つとし

ていた。我が国においても、例えば、他人になりすまして犯罪行為を行う類型として、

- ① なりすまされた者が被害者といえるような「他人になりすまして、無断でプロフなどを作成し、その特定の子どもの電話番号やメールアドレスなどの個人情報を掲載した上、『暇だから電話して』などと書き込みをしたことにより、個人情報を掲載された児童生徒に、他人から電話がかかってくるなどの被害がある」事案⁽¹⁸⁴⁾や
- ② コミュニケーションの相手方が被害者になるような「クラスの多くの子どもになりすまして、「死ね、キモイ」などのメールを特定の子どもに何十通も送信した事例⁽¹⁸⁵⁾」

が指摘されている。さらに、中学校の事例として、ある生徒が同じ学校に通う生徒に対して、自宅のパソコンから「なりすましメール」で大量の嫌がらせメールを送信したので、被害生徒が警察に対して被害届を出し、加害生徒は県迷惑防止条例違反で逮捕された、という事例もあるようであり⁽¹⁸⁶⁾、刑事罰の適用を考えるべき事案があり得ることが示されている。

このような事案につき、アメリカにおいては、無権限の解釈の関係でCFAAにより対処できなかつただけでなく、我が国においても、なりすましからの保護を標榜する不正アクセス行為の禁止等に関する法律11条の罪（不正アクセス罪）であっても、アカウントの乗っ取りを介さない、この種の事案への対処は困難である。例えば、Aが実在する他人Bの名前を入力してアカウントを開設して、IDとパスワードをもらう場合、当該ID・パスワードの組み合わせは、Aの識別符号なのであり、他人であるBの識別符号ではないので、それをAが入力する限りは不正アクセス行為にはなり得ないからである⁽¹⁸⁷⁾。

そうすると、オンラインなりすましを立法することにも一定の合理的な理由がありそうである。もっとも現実の立法に関してサイバーいじめの観点からアメリカの現状をみてきたが、これだけの知見からオンラインなりすましの犯罪化についての具体的な議論を行うことは困

難なように思われる。なぜなら、サイバーいじめ規制とは離れるので本稿では検討できなかったが、むしろ、まずは様々な悪しき行為につながり得るオンラインにおけるなりすまし自体の当罰性を議論すべきだと思われるからである。このことは、目的犯的な規定を有することが多いオンラインなりすまし罪の中にはいじめと親和的な害意を要件とする場合もあれば、経済的な利益の獲得を要件とする場合もあって、なりすましが、いじめと必然的な関係を有するものではないことから示唆されよう。

なお、サイバーいじめを規制しようとする場合、インターネットへの利用に関する考え方に地域的な差を見いだすべきでないことを勘案すれば、構成要件を行為者や被害者の所在地によって変えることに合理的な理由はなく、理論的には、条例ではなく、法律で対策を行うべきである（第5-4の議論参照）。

以上が、アメリカにおけるサイバーいじめの処罰立法を概観したところから得た知見である。今回の研究では、サイバーいじめでも存在し、いじめ全体においてもその重要な一部を構成していると思われる、仲間はずれにする行為について、十分な議論の蓄積が得られなかった。この論点についてはさらに検討を重ねていきたい。さらに、オンラインなりすましの性質論や同時に学校の関与のあり方等、総合的な解決に向けたバランスのよい制度構築に関しては未だ調査が十分でなく、さらに研究を進めていく必要がある部分も残っているので、別の国の法制も見つつ今後も研究を続けていきたい。

(180) Wegman, *supra* note 156, at 756 は、2013年の時点で本文のように指摘していた。

(181) 和久田学「ネットいじめのリアル（その1）」*こころの科学* 187号 95頁、97頁-98頁（2016）も、行為自体の反復性以外に着目すべきだという態度を採る。

(182) 荻上チキ『ネットいじめ』101頁-102頁（2008）。

- (183) だからこそ、神陽子「学校教育とインターネット」日本教育法学会編『教育法の現代的争点』158頁、160頁-161頁(2014)が述べるように、サイバーいじめの解決のためにインターネットの使用を制限するのは短絡的であり、子供同士の間関係や子供と教職員との信頼関係の再構築が重要な課題となる。
- (184) 「いじめから子供を守ろうネットワーク」のサイト内の、ネットいじめの説明の部分(<http://mamoro.org/netijime-solution>)、文部科学省「『ネット上のいじめ』に関する対応マニュアル・事例集(学校・教員向け)【マニュアル編】」2頁(2008)。
- (185) 文部科学省・前掲注184)3頁、安川雅史「ネットいじめとその対策」日本教育2013年6月号14頁。
- (186) 文部科学省・前掲注184)6頁。
- (187) 不正アクセス対策法制研究会編著『逐条 不正アクセス行為の禁止等に関する法律 第2版』66頁-67頁(2012)は、「他人名義や架空の名義で取得した識別符号の入力についてみると」「アクセス管理者との関係においては当該識別符号を取得した者が利用権者であるから、その者が当該識別符号を入力しても不正アクセス行為とはならない」という理解である。

【付記】 本稿は南部篤先生の退職記念で献呈させていただくものである。南部先生は、サイバー犯罪を含む、情報に関する犯罪の研究をされる傍ら、本学法学部に設置された学生生活委員会において、長年、同委員会委員長を務めてこられ、大学内の学生に対して生じるトラブル対応もなされてきた。同委員会における南部先生による案件処理からは筆者も大変多くのことを学ばせていただいた。筆者の方で、SNSによる情報発信について学生に対する告知文の内容に関し、コメントという形で協力させていただいたこともあり、同委員会の活動は筆者にとって極めて興味深いものであった。幸いにも筆者の委員在任期間中に実際にサイバーいじめに関する案件が来たという記憶はないが、サイバーいじめ対応は特に教育機関にとって引き続き重要な問題になっていくだろう。サイバーいじめに関する議論は、南部先生がなされてきた研究及び学務の双方に密接に関連するものだと考え、寄稿させていただいた。お世話になった南部先生に少しでも恩返しができるのであれば幸いである。

