研究ノート

# 非公開 URL と 不正アクセス行為概念

## —— いわゆる Zoom-bombing 問題を契機として ——

岡　部　天　俊

目　次



## Ⅰ．はじめに

新型コロナウイルス感染症（COVID-19）の流行に伴い、従来対面で行われてきた活動の非対面化が急速に進みつつある。そのために不可欠なツールの一つとなってきたのが、いわゆるウェブ会議システムである。ウェブ会議システムをめぐっては、利用者の急増に伴い、セキュリティ上の懸念も指摘されるようになった。とりわけ、ウェブ会議システム「Zoom」においては、参加者として想定されていない第三者が悪意をもって参加する “Zoom-bombing” という攻撃が世界中で確認されたとされる。わが国でも、Zoom を利用した香川大学経済学部の新入生ガイダンスにおいて、第三者が侵入し、約２分間にわたり性的な画像が表示されるなどしたという事案が発生している[1]。

こうした事態は、わが国において新たな解釈論的問題を提起しているように思われる。すなわち、Zoom-bombing が問題となった主な要因の一つは、参加しようとする者が会議用の URL（Uniform Resource Locator）を入手するだけで参加することができる点にある。そして、この URL は、（事前申込みなく誰でも参加可能なものを除き）主催者が参加を認めた相手にのみ通知することが前提とされている。そのため、URL のみによって参加可能な会議においては、ID やパスワードを用いる一般的な認証方法を URL が簡便化して代替しているということができる。したがって、ある会議に参加することが認められていない者が会議用の非公開 URL を入手し侵入する行為は、不正アクセス行為の禁止等に関する法律[2]（以下、「不正アクセス禁止法」または単に「法」という）に

---

[1] 朝日新聞2020年４月30日朝刊17頁、読売新聞2020年５月11日大阪夕刊11頁。さらに、https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic（FBI Boston “FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic”）参照。なお、本稿において引用するウェブサイトの最終閲覧は、2020年７月13日である。

[2] 平成11年法律第128号。後に、不正アクセス行為の禁止等に関する法律の一部を改正する法律（平成24年法律第12号）により改正されている。本法の逐条解説として、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』（立花書房、第２版、2012年。以下、「逐条」として引用する）がある。また、立案担当者によるその他の解説等として、大泉雅昭「不正アクセス行為の禁止等に関する法律の概要について」捜研576号（1999年）11頁以下、北村滋「『不正アクセス行為禁止法』の概要と課題」日経コンピュータ483号（1999年）26頁以下、北村博文「不正アクセス行為の禁止等に関する法律の制定の経緯（特集・ハイテク犯罪対策法制の整備――不正アクセス行為禁止法を中心として――）」警論52巻11号（1999年）８頁以下、同「ネットワーク・セキュリティの確保――不正アクセス行為の禁止等に関する法律」時法1609号（2000年）６頁以下、黒澤正和「不正アクセス行為の禁止等に関する法律の制定について（特集・ハイテク犯罪対策法制の整備――不正アクセス行為禁止法を中心として――）」警論52巻11号（1999年）１頁以下、千葉陽一「不正アクセス行為の禁止等に関する法律の概要」警察公論54巻11号（1999年）17頁以下、露木康浩＝砂田務＝檜垣重臣「不正アクセス行為の禁止等に関する法律の解説（特集・ハイテク犯罪対策法制の整備――不正アクセス行為禁止法を中心として――）」警論52巻11号（1999年）28頁以下、檜垣重臣「不正アクセス行為の禁止等に関

おける不正アクセス行為罪（法11条、３条）に問われる可能性がある。しかしながら、従来は、非公開 URL の入力によるアクセスが不正アクセス禁止法上の「不正アクセス行為」に該当し得るかという点は、ほとんど論じられていない[3]。

無論、この問題は、Zoom-bombing との関連においてのみ問題となるものではない。たとえば、クラウド・ストレージ上のファイルの共有（Dropbox、Google ドライブ、OneDrive 等）や非公開ウェブページの共有にあたっては、しばしば非公開 URL が利用される。したがって、特定の者にのみ通知されることが前提とされる非公開 URL を何らかのかたちで入手しそこへアクセスするという行為の不正アクセス行為該当性は、インターネット利用に際し様々な場面で問題となり得、これについて検討を加えておくことには一定の意義があると思われる。そこで、本稿では、非公開 URL の入力によるアクセスと不正アクセス行為概念の関係について検討を加える。

---

する法律について」ジュリ1165号（1999年）51頁以下、同「ハイテク犯罪の現状と対策について」自正51巻10号（2000年）26頁以下、郵政省電気通信局電気通信事業部データ通信課「不正アクセス行為の禁止等に関する法律の概要」NBL674号（1999年）32頁以下（以上、改正前の解説等）、川原匡平「不正アクセス行為の禁止等に関する法律の一部を改正する法律」警察公論67巻７号（2012年）20頁以下、同「不正アクセス行為の禁止等に関する法律の一部を改正する法律について」捜研733号（2012年）13頁以下、蔵原智行「『不正アクセス行為の禁止等に関する法律の一部を改正する法律について」警論65巻６号（2012年）21頁以下、同「フィッシング行為、ID・パスワードの不正取得等の禁止・処罰等」時法1909号（2012年）４頁以下、四方光「不正アクセス禁止法改正の背景・経緯及び不正アクセス対策の今後の課題」警論65巻６号（2012年）13頁以下（以上、改正法の解説等）などがある。

[3]「隠し URL」によるアクセス制御が不正アクセス禁止法上の「アクセス制御機能」に該当するかという点に言及するものとして、田中規久雄「不正アクセス禁止法における不正アクセス行為の概念」阪法60巻６号（2011年）66-67頁がある。この点に触れるウェブサイト上の記事として、https://www.bengo4.com/c_23/n_11182/（弁護士ドットコム「香川大でも『Zoom 爆弾』、ガイダンス中『性的画像』の共有…犯罪にならないの？」）。

## Ⅱ．非公開 URL によるアクセス・コントロールの概要

非公開 URL によるアクセス・コントロールの方式としては、少なくとも次の２種類が存在する。

第一は、認証情報が埋め込まれた URL を用いる方式である（以下、①方式とする）。この方式は、認証自体は ID・パスワード等を用いる一般的なかたちで行われることを前提として、ID・パスワード等の認証情報が既に埋め込まれた URL を特定の者に通知し、アクセスさせるものである。たとえば、Zoom では、設定において「ワンクリックで参加できるように、ミーティングリンクにパスワードを埋め込みます」という項目が存在し、これがオンにすることで、ID と暗号化されたパスワードがミーティング用リンクに組み込まれ、これを用いれば、参加者が別途 ID・パスワードを入力するという手間が省かれる仕様となっている（2020年７月13日現在）。上記の設定がオンになっている場合には、ミーティング ID「XXX XXX XXXX」、パスワード「a1b2c3……」であるミーティングに参加するためのリンクは、「https://us04web.zoom.us/j/XXXXXXXXXX?pwd=b2c3d4.....」などとして生成される（「b2c3d4.....」は本来のパスワード「a1b2c3.....」が暗号化された文字列）。

第二は、文字列が複雑化された URL を用いる方式である（以下、②方式とする）。この方式は、一般的なかたちでの認証を前提とせず、推測することが事実上不可能なかたちで複雑化された URL を特定の者に通知し、アクセスさせるものである。たとえば、クラウド・ストレージ・サービス「Dropbox」では、クラウド・ストレージ上のファイルを共有する際に、共有リンクを用いることができ、その場合、当該ファイルに対して共有リンクが生成され、当該共有リンクを知る者のみが当該ファイルにアクセスすることができる。たとえば、ある PDF データにつき共有リンクを生成すると、その URL は、「https://www.dropbox.com/s/xc7p9mddlukm38c/%E9%9D%9E%E5%85%AC%E9%96%8BURL%E3%81%A8%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E8%A1%8C%E7%82%BA%E6%A6%82%E5%BF%B5.pdf?dl=0」などとして生成される。

以上の２つの方式は、前提となる認証の方法が異なり、不正アクセス禁止法上の位置づけも異なり得るため、以下ではこれらを踏まえつつ検討を進める。

## Ⅲ．不正アクセス行為概念の概要

### （1）総説

現行の不正アクセス禁止法は、２条４項において「不正アクセス行為」について定義した上で、３条によりこれを一般的に禁止し、３条に違反した者に対しての罰則として11条を用意している（３年以下の懲役または100万円以下の罰金）。その保護法益は、アクセス制御機能に対する社会的信頼であるとされる[4]。

２条４項の不正アクセス行為の定義の中で登場する各種文言については、同条１項ないし３項において定義されており、１項が「アクセス管理者」、２項が「識別符号」、３項が「アクセス制御機能」を定義している。以下では、それぞれの一般的な解釈について概観しておく。

### （2）アクセス管理者（法２条１項）

まず、「アクセス管理者」とは、「電気通信回線に接続している電子計算機の利用につき当該特定電子計算機の動作を管理する者」をいう（法２条１項）。

「電気通信回線に接続している電子計算機」とは、電気通信回線設備と結合して電気通信が可能な状態に構成されている電子計算機をいい[5]、不正アクセス禁止法はこうした電子計算機を「特定電子計算機」と略称し、特定電子計算機を電気通信回線を通じて利用することを「特定利用」と略称することとしている。

特定電子計算機の利用につき当該特定電子計算機の「動作」を「管理」するとは、主として、当該特定電子計算機による情報処理を誰に特定利用させるかを

---

[4] 逐条･前掲注（２）140頁、露木＝砂田＝檜垣･前掲注（２）58頁。また、「ネットワーク内部でのデータ処理の確実性とそれへの信頼」あるいは「コンピュータ・データの処理に利害関係を有する不特定多数の者の、データ処理の確実性に対する信頼」が保護法益であるとするものとして、今井猛嘉「『不正アクセス』の意義をめぐって」研修719号（2008年）９頁。不正アクセス行為罪の保護法益をめぐっては、石井徹哉「不正アクセス禁止法の意義と限界」千葉19巻３号（2004年）15-27頁、成瀬幸典「不正アクセス罪についての一考察」阿部純二先生古稀祝賀論文集『刑事法の現代的課題』（第一法規、2004年）357頁以下、渡邉卓也『ネットワーク犯罪と刑法理論』（成文堂、2018年）214-223頁も参照。

[5] 逐条・前掲注（２）36頁。

決定することをいう[6]。

### （3）識別符号（法２条２項）

次に、「識別符号」とは、「特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者及び当該アクセス管理者に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号」であって、１号ないし３号の「いずれかに該当するもの」または１号ないし３号の「いずれかに該当する符号とその他の符号を組み合わせたもの」をいう（法２条２項柱書）。なお、不正アクセス禁止法は「特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者」を利用権者と略称し、この利用権者と当該アクセス管理者を併せて「利用権者等」と略称することとしている。

#### （a）利用権者等

「当該特定利用に係るアクセス管理者」とは、特定電子計算機の特定利用につき当該特定利用がされる特定電子計算機の動作を管理する者をいう[7]。「当該特定利用に係る」という限定が付されているのは、特定利用の対象となる特定電子計算機に係るアクセス管理者が複数存在し得ることから、「許諾」を与える主体を特定する趣旨である[8]。

「許諾」とは、アクセス管理者がその特定利用につき動作を管理している特定電子計算機の特定利用をすることを権原を付与するような形で認めることをいい[9]、その方式に限定はない[10]。なお、不正アクセス禁止法は、アクセス管理者または利用権者が特定利用を個別にまたは一時的に認めることを「承諾」（法２条４項１号・２号）としており、「許諾」とは区別している[11]。

---

[6] 逐条・前掲注（２）37頁、露木＝砂田＝檜垣・前掲注（２）37頁。したがって、アクセス管理者が当該特定電子計算機を所有していることは必要でない（逐条・前掲注（２）38頁）。

[7] 逐条・前掲注（２）39頁。

[8] 逐条・前掲注（２）40頁。

[9] 逐条・前掲注（２）40頁、露木＝砂田＝檜垣・前掲注（２）38頁。

[10] 逐条・前掲注（２）40頁。

[11] 逐条・前掲注（２）40頁。

**（b）利用権者等の識別**

法２条２項の識別符号たり得るには、それが利用権者等に「付される」ものでなければならないから、利用権者等に付されているわけではないIPアドレス等の識別情報は識別符号に該当しない[12]。また、識別符号を「付」す主体に限定はない[13]。

加えて、法２条２項の識別符号たり得るには、「当該利用権者等を他の利用権者等と区別して識別することができるように」付されるものでなければならず、複数の利用権者等に同一の符号が付されないようにすると同時に、どの利用権者等に付されたものであるかが分かるように付されていることが必要である[14]。立案担当者による解説等においても必ずしも明らかではないが、後述のように、この要件は符号を付す客観的な目的を示すものと解されるため、問題となる符号が区別・識別のために付されていることが客観的に明らかとなっている必要があろう。なお、同一の符号を複数の者が利用することが想定されるグループID等も識別符号に含まれ得る[15]ことから、同一の符号を複数の者が利用するという事情があったとしても、この要件は充足され得る。

なお、「符号」とは、番号、記号、模様、単位信号の組合せその他の人が認識することができるしるしをいう[16]。

**（c）なりすましの排除**

識別符号たり得るには、さらに１号ないし３号の「いずれかに該当するもの」または１号ないし３号の「いずれかに該当する符号とその他の符号を組み合わせたもの」でなければならない。

本稿の内容と関係する１号の内容は、「当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号」である。「みだりに」とは、正当な理由がないことをいう[17]。また、「第三者に知らせてはな

---

[12] 逐条・前掲注（２）41頁、露木＝砂田＝檜垣・前掲注（２）38頁。
[13] 逐条・前掲注（２）42頁、露木＝砂田＝檜垣・前掲注（２）38頁。
[14] 逐条・前掲注（２）41頁。
[15] 逐条・前掲注（２）40頁、露木＝砂田＝檜垣・前掲注（２）38頁参照。
[16] 逐条・前掲注（２）43頁。
[17] 逐条・前掲注（２）44頁。

らないものとされている」とは、アクセス管理者によって利用権者等に対しそれを第三者に知らせないよう求められていることをいい[18]、その方法に限定はない[19]。

なお、１号ないし３号の「いずれかに該当する符号とその他の符号を組み合わせたもの」とは、ID とパスワードの対が対象となることを明らかにするものであるが、法２条２項柱書からも明らかなように、必ずしも複数の番号・記号等が用いられる必要はない[20]。

### （４）不正アクセス行為（法２条４項）

不正アクセス禁止法は、不正アクセス行為として３類型を想定しており、それらは、２条４項１号の不正ログインと同項２号および３号のセキュリティ・ホール攻撃に大別される[21]。

本稿の内容と関係する１号の内容は、「アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）」である。

「電気通信回線を通じて」なされることが必要であることから、キーボードを用いて電子計算機に直接識別符号を入力する行為等は除外される[22]。

「入力」とは、電気通信回線を通じて対象となる特定電子計算機に他人の識別符号を送信することをいい、キーボード操作等は必ずしも必要ではなく、自動的に識別符号を送信するコンピュータの機能を用いることをも含む[23]。

---

[18] 逐条・前掲注（２）44頁、露木＝砂田＝檜垣・前掲注（２）39頁。
[19] 逐条・前掲注（２）44頁。
[20] 逐条・前掲注（２）39頁、46頁。
[21] 逐条・前掲注（２）61頁、露木＝砂田＝檜垣・前掲注（２）44頁。
[22] 逐条・前掲注（２）65-66頁、露木＝砂田＝檜垣・前掲注（２）45頁。
[23] 逐条・前掲注（２）67頁、露木＝砂田＝檜垣・前掲注（２）45頁。

## Ⅳ．法２条における非公開 URL の位置づけ

### （1）総説

アクセスにつき許諾を得ていない第三者が、非公開 URL によるアクセス・コントロールがなされている特定電子計算機に、非公開 URL を用いてアクセスする行為が、法２条４項１号の不正アクセス行為に該当するか否かは、とりわけ､非公開 URL（の全部または一部）が「識別符号」（法２条２項）に該当し、かつ当該非公開 URL によるアクセス･コントロールが「アクセス制御機能」（法２条３項）に該当することが必要となる。以下、それぞれ順に検討を加える。

### （2）非公開 URL の識別符号該当性

#### （a）①方式における非公開 URL

まず、①方式における非公開 URL は、識別符号に該当するものと考えられる。①方式における非公開 URL には、ID・パスワード等の認証情報が埋め込まれており、当該 URL にアクセスすると、アプリケーションの実行に加え、当該アプリケーション内での ID・パスワード等の入力が自動的に行われるという仕組みになっている。したがって、①方式における非公開 URL は、識別符号に他ならないということになろう[24]。

なお、ここで前提となる認証につき、パスワードは不要とされており ID のみが必要であるような仕様であったとしても、先述のように、識別符号は必ずしも相異なる符号の組み合わせである必要はないから、当該 ID およびこれを含んでいる URL が第三者への通知が禁じられている限りにおいて、非公開 URL は識別符号に該当し得る。

#### （b）②方式における非公開 URL

②方式における非公開 URL については、①方式におけるそれとは異なり、

[24] これに対し、Zoom の「URL 自体が識別符号であるという解釈もあり得なくもありません」としつつ､「サーバ自体は一般に向けてアクセスを許しており、パスワードを別途入力して入ったわけではない以上、URL を識別符号と見ることは困難だと思われます」とするものとして、前掲注（3）ウェブサイト〔伊藤諭弁護士コメント〕。

そもそも ID・パスワード等による認証を前提としないことから、より慎重な検討を要する。

まず、②方式における非公開 URL は、なりすましの排除の要件については比較的容易に満たすことになる。すなわち、ある URL がアクセスが許された者に対してのみ通知されることとされている限り、当該 URL は、法２条２項１号にいう「当該アクセス管理者によってその内容を第三者に知らせてはならないものとされている符号」に該当することになるからである。

他方で、②方式における非公開 URL がその他の要件を満たすのは、非常に例外的な場面に限られるように思われる。ある符号が利用権者等の識別の要件を満たすためには、まず当該符号が利用権者等に付される符号である必要がある。それゆえ、非公開 URL につきこのことが肯定されるためには、当該非公開 URL がファイル等に付されたものではなく利用権者等に付されたものであると認められる事情が存在しなければならない。そうすると、たとえば、あるウェブサイトを用意しておき、後に当該ウェブサイトを閲覧させたい相手が現れた時にのみ、当該相手に当該ウェブサイトの URL を通知するというような場合、当該 URL は、あくまでも当該ウェブサイトに付された符号であることから、「利用権者等に…付される符号」とはいえない。これに対し、クラウド・ストレージ上のあるファイルにつき、それを誰かと共有する度ごとに、新たに共有リンクを生成してそれを通知するというような場合、当該リンクは、当該ファイルではなく当該相手に付される符号であることから、「利用権者等…に付される符号」であるといえよう。つまり、ここでは、問題となる非公開 URL の利用形態から、当該非公開 URL がファイル等というよりもむしろそれを利用する利用権者等に付されていると評価できる事情が必要であると思われる[25]。

さらに、ある符号が利用権者等の識別の要件を満たすためには、当該符号が「当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号」である必要がある。これはいわば符号を付す目的を示すものであるが、これが満たされるためには、当該符号から

[25] 当然、形式的には URL はファイル等に設定されるものであるが、法２条２項の解釈・適用の問題として、URL が利用権者等に「付される」という評価もあり得るように思われる。

アクセス管理者が利用権者等の区別・識別を目的としていることが客観的に明らかであることが必要であると解される。そうであるとすれば、非公開 URL につきこのことが肯定されるためには、その推測を困難にすることを目的としていることが客観的に明らかであるような文字列の構成になっていることが必要であろう。

以上のように、②方式における非公開 URL が法２条２項にいう識別符号に該当するのは非常に例外的な場合に限られるが、その可能性は十分存在する[26]。具体的には、当該非公開 URL がファイル等ではなく利用権者等に付されたものとであるいえ、かつ当該非公開 URL において利用権者等の区別・識別を目的としていることが明らかであるといえる限りにおいて、識別符号該当性が認められることになる。

### （３）非公開 URL によるアクセス・コントロールのアクセス制御機能該当性

#### （ａ）①方式におけるアクセス・コントロール

①方式におけるアクセス・コントロールは、問題なくアクセス制御機能該当性が肯定される。繰り返し述べているように、①方式の場合には、ID･パスワード等による一般的な認証が前提とされており、ID・パスワード等を入力するためのユーザー側の操作が通常と異なるにすぎないからである。

#### （ｂ）②方式におけるアクセス・コントロール

②方式の場合には、そのアクセス・コントロールのアクセス制御機能該当性についても、慎重な検討を要する。あるアクセス・コントロールが法２条３項にいうアクセス制御機能に該当するには、それが特定電子計算機に「付加」された「当該特定利用をしようとする者により入力された符号が当該特定利用に係る識別符号であることを確認して、当該特定利用の制限の全部又は一部を解除する」機能（以下、確認･解除機能という）と評価できることが必要である。非公開 URL と不正アクセス行為の関係について言及する文献においては、「隠し URL」は識別符号たり得るとしつつ、これによるアクセス・コントロールについては、「URL を入力しさえすれば HP が表示されると言った場合、そこ

[26]「隠し URL」が識別符号に該当する可能性を示唆するものとして、田中・前掲注（３）66頁。

には付加された機能は存在しない」として、アクセス制御機能該当性を否定する見解が示されている[27]。こうした見解から示唆されるように、②方式におけるアクセス・コントロールのアクセス制御機能該当性をめぐっては、そもそも法２条３項が要求している確認・解除機能が存在しているといえるかという点に加えて、（それが肯定されたとして）特定電子計算機の動作内容として認証プロセスを別途追加しているわけではないにもかかわらず確認･解除機能が「付加」されているといえるか、の２点が問題となるように思われる。以下では、これらの点について検討を行う。

まず、②方式におけるアクセス・コントロールが、そもそも法２条３項が要求している確認・解除機能を備えているといえるかについて検討する。ID・パスワード等を用いる通常の認証では、識別符号が入力されると、入力された識別符号とパスワード・ファイル等との照合が行われ、その照合が完了するとアクセス制御が解除され要求されたアクセスが実行されることになる。ここでは、法２条３項の要求する確認・解除機能が独立したプロセスとして存在している。これに対して、②方式におけるアクセス・コントロールでは、先述のように、正しい非公開 URL が入力されると、ただちに要求されたアクセスが実行されることから、確認・解除機能が独立したプロセスとしては存在していない。そのため、②方式におけるアクセス・コントロールには、一見、確認・解除機能が存在しないようにも見える。しかしながら､②方式におけるアクセス･コントロールにおいては、確認・解除のみを目的としたプロセスが省略されているものの、確認・解除機能そのものが存在していないわけではない。そこでは、正しい URL が入力されてアクセス要求がなされたこと自体が、確認・解除の役割を担っているのである。したがって、②方式におけるアクセス・コントロールにおいても、法２条３項が要求する確認・解除機能が存在していると考えられる。

次に、以上のように考えたとしても、②方式におけるアクセス・コントロールでは、確認・解除機能が独立したプロセスとして別途追加されているわけではないことから、その機能が特定電子計算機に「付加」されたものといえるかどうかが問題となる。まず、法２条３項にいう「付加」とは、立案担当者による逐条解説によると、単に特定電子計算機の特定利用を制御する機能をコン

[27] 田中・前掲注（３）66-67頁。

ピュータにもたせることをいうとされており[28]、確認・解除のみを目的とした動作を別途追加することまでは含意していないと考えられる。そうすると、法２条３項がなぜ「付加」という文言を用いたのかが一つの疑問となるが、わが国における不正アクセス行為概念は、法２条４項からも明らかな通り、電気通信回線を通じて、システムに内在する（systemimmanent[29]）アクセス制御を免れる行為を前提とするものであり、法２条３項における「付加」は、アクセス制御機能の定義においてもこのことを明らかにし、アクセス制御機能が特定電子計算機自体に備わっているものである必要があることを確認的に示す趣旨のものと考えられる[30]。したがって、法２条３項にいう「付加」とは、確認・解除

[28] 逐条・前掲注（２）48頁。

[29] Vgl. *Karl Lackner/Kristian Kühl*, Strafgesetzbuch, Kommentar, 29. Aufl., 2018, § 202a Rn. 4.

[30] 締約国に対し「コンピュータ・システムの全部又は一部に対するアクセスが、権限なしに故意に行われること」を犯罪化することを義務づけるサイバー犯罪条約２条（違法アクセス；illegal access）は、後段において、「締約国は、このようなアクセスが防護措置を侵害すること（*infringing security measures*）によって行われること…をこの犯罪の要件とすることができる」と規定しており、比較法的にもこれに対応する要件を設けることが多い（日本、ドイツおよびスイスは、解釈宣言（declaration）によりこれを明確にしている（https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=XIPNEcyx））。ここでいう「防護措置」については、物理的な防護措置をも含むとするかどうかで各国において相違があり、たとえば、ドイツ刑法202a条およびオーストリア刑法118a 条のもとでは、物理的な防護措置でも足りるとされる（siehe [Deutschland] *Jörg Eisele*, Computer- und Medienstrafrecht, 2013, 4. Kapitel Rn. 15; *Klaus Malek/Andreas Popp*, Strafsachen im Internet, 2. Aufl., 2015, Rn. 157; *Annette Marberth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl., 2010, Rn. 93; [Österreich] *Susanne Reindl-Krauskopf/Farsam Salimi/Martin Stricker*, IT-Strafrecht – Cyberdelikte und Ermittlungsbefugnisse, 2018, Rn. 2.22）。これに対し、スイス刑法143条の２の元では、「データ通信装置を用いて（auf dem Wege von Datenübertragungseinrichtungen）、アクセスから特別に保護されている他人のデータ処理システムに、無権限で侵入する」ことが構成要件とされており、このうち方法に関する文言が、防護措置のシステム内在性を要求する趣旨であるとされる（siehe Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes

機能を独立したプロセスとして別途追加することを意味するわけではなく、②方式におけるアクセス・コントロールも、「アクセス制御機能」に該当し得る。

### （4）非公開 URL へのアクセスの不正アクセス行為該当性

非公開 URL が法２条２項にいう「識別符号」に該当し、これによるアクセス・コントロールが法２条３項にいう「アクセス制御機能」に該当する場合には、アクセスの許諾を得ていない第三者が当該非公開 URL を用いてアクセスする行為につき、不正アクセス行為該当性が肯定されることになる。

具体的には、まず①方式の場合には、問題となる非公開 URL にアクセスすると、アプリケーションの実行および当該アプリケーションでの識別符号の入力が自動で行われることになる。したがって、アクセスの許諾を得ていない第三者が問題となる非公開 URL にアクセスした段階で、自動入力機能を用いた他人の識別符号の入力が認められ、認証が完了した段階で、アクセス制御機能により制限されている特定利用をし得る状態に至らしめたことが認められることになる。

他方で、②方式の場合には、アクセスの許諾を得ていない第三者が問題となる非公開 URL にアクセスした段階で、他人の識別符号を入力し、かつアクセス制御機能により制限されている特定利用をし得る状態に至らしめたと評価されることになる。

---

(Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen) vom 24.4.1991 (BBl 1991 II 969), S. 1011; *Niklaus Schmid*, Computer- sowie Check- und Kreditkarten-Kriminalität, 1994, § 5 Rn. 23; vgl. *Christian Schwarzenegger*, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: Andreas Donatsch/Marc Forster/Christian Schwarzenegger (Hrsg.), Festschrift für Stefan Trechsel zum 65. Geburtstag, 2002, S. 316 Fn. 51; *Philippe Weissenberger*, in: Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Strafrecht II, 4. Aufl., 2019, Art. 143$^{bis}$ Rn. 16)。わが国では、スイスと同様に、法２条４項が「電気通信回線を通じて」として行為態様を限定しているが、法２条３項にいう「付加」の文言によってこれが確認的に示されているといえよう。

なお、香川大学経済学部の新入生ガイダンスにおいて発生したZoom-bombingの事例は、①方式が問題となったものであり、ミーティング用URLを利用してガイダンスに侵入した者の行為につき、先述のようなかたちで不正アクセス行為罪の成立が認められると考えられる。

## Ⅴ．非公開URL提供行為の可罰性

ある非公開URLが「識別符号」に該当し、かつこれによるアクセス・コントロールが「アクセス制御機能」に該当する場合には、当該非公開URLを第三者に提供する行為も処罰の対象となる。

まず、非公開URLを単に提供した、すなわち第三者が利用できる状態に置いた段階で不正アクセス助長罪（法13条、５条）が成立する[31]。さらに、提供行為時に「相手方に不正アクセス行為の用に供する目的があること」の情を知っていた場合には、加重類型としての知情提供罪（法12条２号、５条）が成立する[32]。さらに、非公開URLの提供を受けた者による不正アクセス行為が既遂に至った場合には、提供者につき不正アクセス行為罪（法11条、３条）の共犯が成立する[33]。

具体的には、ワンクリックで参加することが可能なミーティング用URLを当該会議等への参加につき許諾を得ていない者に対し伝達したり、SNSにおいて公開するなどの行為は、不正アクセス禁止法による処罰の対象となり得る。また、クラウド・ストレージ上のファイルを共有する際の共有リンク等につい

[31]「提供」の意義につき、逐条・前掲注（２）90頁。不特定多数の者に対して公開する行為等も含まれる。

[32] 知情提供罪の趣旨については、蔵原・前掲注（２）〔警論〕29頁、同・前掲注（２）〔時法〕15頁参照。

[33] その場合、法12条２号の罪はこれに吸収される（逐条・前掲注（２）149頁、露木＝砂田＝檜垣・前掲注（２）60-61頁）。なお、法12条２号の罪は、特定の相手方が不正アクセスの用に供する目的を有していることを知ってなされる提供行為を対象としていると解されるから、誰かが不正アクセスの用に供する可能性を認識しつつ不特定多数の者に対して公開する行為が問題となる場合には、法13条の罪が不正アクセス行為罪の共犯に吸収されるということもあり得よう。

ても、当該共有リンク等がその利用形態からして識別符号と評価され得る限りにおいて、同様である。

## Ⅵ. おわりに

アクセスの許諾を得ていない者が非公開 URL を入手しアクセスするという行為の不正アクセス行為該当性は、従来ほとんど論じられていなかった問題であるが、結論として、こうした行為は不正アクセス行為に該当し得る。①方式の場合には、ID・パスワード等の典型的な識別符号を用いたアクセス制御が前提となっており、その入力が URL を利用するかたちになっているにすぎないことから、当然に不正アクセス行為該当性が問題となり得る。他方で、②方式の場合には、問題となる URL はファイル等に付されたものであって利用権者等に付された符号ではないことが多いことに加え、問題となる URL において利用権者等の区別・識別を目的とする趣旨が表れているとはいえないことが多いことから、原則として、当該 URL は識別符号に該当せず、不正アクセス行為該当性は問題とならない。しかしながら、利用権者等に付され、利用権者等の区別・識別を目的とする趣旨が表れた符号として評価できるような事情の存する場合においては、不正アクセス行為該当性が問題となり得るであろう。

わが国における不正アクセス行為罪は、同じくサイバー犯罪条約２条を担保する諸外国における犯罪類型と比較すると、その処罰範囲は相当程度狭くなっている。というのも、わが国の不正アクセス行為罪は、識別符号によるアクセス制御というものを想定し、これを突破する行為のみを対象とするものであるのに対し、諸外国における同種犯罪は、こうした具体的な限定をしていないため、いわゆるファイアウォールを突破する行為等をも対象としているからである[34]。そうであるからこそ、わが国の不正アクセス行為罪において前提とされ

[34] わが国の不正アクセス禁止法が、ファイアウォールによるアクセス制限を突破する行為を適用対象外としているという点につき、北村（滋）・前掲注（２）28頁、北村（博）・前掲注（２）〔時法〕13-14頁、露木＝砂田＝檜垣・前掲注（２）41頁注６。立法論的にはそうした行為等も不正アクセス行為の対象とすべきであるとするものとして、今井猛嘉「ネットワーク犯罪」法教303号（2005年）56頁、西貝吉晃「コンピュータ・データへの無権限アクセスと刑事罰（１）」法協135巻２号（2018年）301頁、渡邉・前掲注（４）225頁。

る識別符号によるアクセス制御という概念が、新しい形態のアクセス・コントロールとどのような関係にあるのかを考えることが重要になってくるものと思われる。

非公開 URL を利用したアクセス・コントロールの利便性は非常に高く、今後も幅広く利用されていくことが想定されるため、今後の議論の蓄積に期待したい。