論説

サイバーテロリズムの防止
―通信活動における『有害な干渉禁止原則』の観点より

高 屋 友 里

1. はじめに

サイバーテロリズム，サイバー攻撃，サイバー犯罪という一連のサイバー脅威（cyber threat）は，いずれもサイバー空間を介して行われる不法行為であり，従来の国内刑法のみならずテロ防止関連諸条約，国際人道法，国際刑事法，さらに国際電気通信法といった国際法の分野において大きな課題を突き付けている。それは，国家の領域を超えたサイバー空間の特殊性ゆえ，上述のサイバー不法行為の分類が不明瞭な点や，最初の一手を放つ犯人の特定

が技術上難しい点に起因する。例えば，個人ハッカーがサイバーテロリズムを生じさせるためにコンピュータ・ウィルスを作成し，軍事システムの運営を担う民間企業のパソコンに感染させたものの，不具合により軍事システムの機能不全にまで至らなかった場合，政治的意図が発覚しなければ単なるサイバー犯罪として国内刑法が適用される可能性がある。また，国際テロリスト集団もしくは国家主導のテロリスト集団が，単なるサイバー犯罪を目的としてコンピュータ・ウィルスを作成した場合にはテロ防止関連諸条約や国際人道法が適用されるが，個人ハッカーを装った場合，国内刑法の適用のみとなる可能性も拭えない。サイバー不法行為に適用される法の分類はいまだ不明瞭な点が多いのである。

しかし，サイバー空間やサイバー脅威といった新たな用語が国際法の文脈において使われ始めたものの，もともとサイバー活動とはコンピュータを介した電気通信活動である。有線・無線通信活動をはじめとする人類の電気通信活動は，国連機関である国際電気通信連合（ITU）[1]により国際規制を受けており，電気通信活動に妨害を与える行為は ITU 憲章[2]の規定する有害な干渉禁止原則において禁止されている。この点に鑑み，本稿では ITU の有害な干渉禁止原則がサイバーテロリズム防止に寄与する点を明らかにすることを目的とする。構成として，まずサイバーテロリズムの定義［2］および ITU のサイバーセキュリティに関する法的試みを概観し［3］，既存の有害な干渉禁止原則およびその履行制度メカニズムの有用性［4］を確認したのち，サイバー脅威に対抗する目的で ITU 加盟国が批准する 2001 年サイバー犯罪条約の法的課題を考察する［5］。

2. サイバーテロリズムの定義

国際法上，サイバーテロリズムの定義は確立していない[3]。国際テロリズムの定義についてはすでに確立しているとする学説とそうでないとする学説とに分かれ，「国際テロリズム包括的条約草案」において定義に関する審議は停滞している[4]。また，サイバーテロリズムを「サイバー空間のおけるテロ行

為」と位置付けようとしても，国際法におけるサイバー空間の定義もいまだ定まっていない。その理由は情報通信技術（以下，ICTs）の著しい発展に起因している。例えば，国連軍縮研究所（UNIDIR）はサイバー空間を「インターネット，通信ネットワーク，コンピュータ・システム，および内在する情報を含む『デジタル情報および通信インフラ』が連結した国際的なネットワーク」と定義し，国際赤十字委員会（ICRC）は「世界的な連結をもたらす仮想空間」と定義する。さらに，近年では個人がスマートフォンを持ち，インターネット環境のない場所においても専用アプリ，Bluetooth や Wi-Fi，無線ネットワークを通じて E メールや写真，音楽を共有している[5]ため，サイバー空間を「インターネット，通信ネットワーク，コンピュータ・システムを含む情報通信インフラが生み出す連結ネットワーク上の，電気通信による人工的な環境もしくは空間」[6]と定義する学説まである。

このように国際法におけるサイバー空間の定義は複数存在し，また，国際テロリズムの定義も確立していないが，いくつかの国際機関はサイバーテロリズムの定義をすでに試みている。国連薬物犯罪事務所（UN Office of Drugs and Crime）は「コンピュータ・システム，コンピュータ・サーバ，関連インフラのような目標物の適切な機能性を遮断するために攻撃をしかけるためにコンピュータ・ネットワークを意図的に利用すること」[7]と定義しており，国連テロ対策実施タスクフォース（UN Counter-Terrorism Implementation Taskforce: CTITF）は「遠隔操作によりコンピュータ・システム上の情報を変更し，もしくはコンピュータ・システム間におけるデータフローを妨害するテロ攻撃」[8]と定義する。それではサイバーテロリズムに適用される条約はまったくないのであろうか。

サイバーテロリズムの定義やその行為を禁止する国際条約はないが，既存の国際テロ関連諸条約はサイバーテロリズムに適用される。なぜなら，サイバーテロリズムとは新しいテロリズムを意味するのではなく，電気通信手段を用いたテロリストの新しい作戦にすぎないからである。この電気通信手段を用いたテロリズムの防止という観点から，次章は ITU によるサイバーセキュリティ対策を考察する。

3. 国際電気通信連合（ITU）とサイバーセキュリティ

1. ITU とは

ITU は，無線・有線を問わず，通信全般をつかさどる国際機関である。ITU 憲章[9]，ITU 条約[10]，その他規則を含める現行法（以下，ITU 法[11]）に基づき通信活動を国際規制し，その業務は無線周波数スペクトル帯の分配（allocation），無線周波数の割り振り（allotment），周波数割り当て（assignment）の登録や電気通信の標準化を促進することで[12]，電気通信の良好な運用という世界の共通利益を図っている[13]。1964 年に衛星通信も管轄するようになり[14]，「限られた天然資源」[15]と定義される静止軌道[16]の利用における国際調整の役割も担っている。人類の通信技術の発展に伴い，規制対象を拡大し続けているのが特徴で，2006 年にはインターネットを使った IP 電話や SNS アプリによる ICTs のすべてを管轄するようになった。このため通信活動に対するサイバー脅威を警戒するようになり，サイバーセキュリティに関する法的強化を図っている。

2. ITU とサイバーセキュリティ

2003 年 1 月 31 日に採択された国連総会決議 57/239「Creation of a global culture of cybersecurity」[17]および 2005 年情報社会世界サミット（WSIS）で承認された「情報社会におけるチュニス・アジェンダ」[18]を契機に，ITU はインターネット・ガバナンス・フォーラム（IGF）を設置した。さらに 2007 年 5 月 17 日，ITU 事務局長 Hamadoun I. Touré はグローバル・サイバーセキュリティ・アジェンダを打ち出し，具体的な対応策を求めてハイレベル専門家グループ（以下，HLEG）を設け，ICTs に対するサイバー犯罪の取り締まりを検討させた。HLEG は，情報社会における信頼とセキュリティを高める戦略として，欧州評議会が起草した 2 つの条約，2001 年サイバー犯罪条約[19]（以下，サイバー犯罪条約）および 2005 年テロ防止条約[20]を ITU 加盟国に批准するよう提言したが[21]，2014 年の ITU 報告書[22]では前者のみ検討が進められている。

3. 2001 年サイバー犯罪条約

まず ITU がサイバーセキュリティ強化の要として着目する 2001 年サイバー犯罪条約の設立経緯を概観する。1989 年，欧州評議会閣僚会議は，コンピュータ・ネットワークを介した破壊的行為を刑罰化する新たな実定法が必要と認識し，勧告文書を作成した[23]。1995 年，同会議が作成したコンピュータ関連犯罪の刑事手続法が不十分だと指摘されると，翌年 11 月に犯罪問題欧州委員会（European Committee on Crime Problems: CDPC）は専門家委員会の設立を決定した[24]。その背景にあったのは，通信と情報システムの統合，さらに通信および情報サービスの“ユーザ”の結びつきによる「サイバー空間」の創設とそれを悪用する危険性であり，また，サイバー犯罪が領土主権に基づく各国の国内法では対応しきれないとする懸念であった[25]。当時検討されたサイバー空間における犯罪（cyber-space offences）とは，①コンピュータ・システムや通信ネットワークの整合性（integrity）・有用性（availability）・機密性（confidentiality）に対する犯罪，もしくは，②それらネットワークやサービスを使用しての“伝統的（traditional）”な犯罪行為，つまり従来から存在する犯罪行為である[26]。

同委員会の決定に続き，1997 年 2 月 4 日の閣僚委員会決議[27]により，「サイバー空間における犯罪の専門家委員会」（PC-CY）が設置され，同年 4 月にサイバー犯罪条約の起草交渉が開始された[28]。当初は 1999 年 12 月 31 日に作業は終わるはずであったが 2000 年 12 月 31 日まで延長が決定され[29]，その起草過程において 2 度にわたり欧州司法省は条約設立にむけた協力を表明[30]。2001 年 6 月にようやく第 50 回総会において閣僚会議はサイバー犯罪条約の草案を批准・署名公開に至った。日本は 2011 年に批准している。

同条約は，コンピュータ・システムに対する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きの整備，犯罪人引渡などに関する国際協力について規定し[31]，当事国に立法措置を義務付けているが，その義務履行における問題がいくつか指摘されている[32]。例として，現実に送受信されているパケットを，トラフィックデータとコンテントデータとに明確に区分し処理する技術の欠如が挙げられる[33]。もしコンテンツデータも

一緒に傍受せざるを得ない場合，プライバシー侵害を生じ，そもそも同条約前文に規定される人権条約の目的に反する。越境コンピュータにおける捜査[34]やデータの扱い，および，捜査を目的とした通信傍受からプライバシーをどう保護するのかが喫緊の課題となっている。

4. 有害な干渉禁止原則

1. サイバーテロリズムと通信における有害な干渉

前述のようにサイバーテロリズムの定義は確立されていないが，サイバーテロリズムの結果として通信障害を引き起こすのであれば，そのような妨害行為はITU法における「有害な干渉」としてすでに禁止されている[35]。ITU法において「干渉」と「有害な干渉」とでは定義が異なり，サイバーテロリズムに該当するのは後者である。前者は「単数もしくは複数の放出・放射による不必要なエネルギーが無線通信システムの受信に及ぼす効果」[36]と定義され，言い換えれば，技術的に不必要なエネルギーの放出・放射を意味する。一方「有害な干渉」は，「無線航行業務その他の安全業務の運用を妨害し，又は無線通信規則に従って行う無線通信業務の運用機能に重大な悪影響を与え，若しくはこれを反復的に中断し若しくは妨害する干渉（混信）」[37]と定義される。つまり，「有害な干渉」は不要なエネルギーの有無ではなく，運用の妨害を意味し，単なる周波数の混信ではなく，航海・航空・宇宙航行が必要とする無線航行業務および安全業務の運用妨害または通信業務の運用機能を危険にさらす行為を指す。損害規模からすれば，干渉よりも「有害な干渉」の方が深刻な損害を生じさせよう。

この「有害な干渉」はITU法で明示的に禁止されている。ITU憲章第45条1項によれば，「すべての局（stations）は，その目的のいかんを問わず，他の加盟国，認められた事業体その他正当に許可を得て，かつ，無線通信規則に従って無線通信業務を行う事業体の無線通信又は無線業務に有害な混信を生じさせないように設置し及び運用しなければならない」[38]。ITU加盟国のみならず，通信事業社（通信局）に対しても同じ義務が課される[39]。もとも

と通信とは，ITU 憲章前文が「各国に対してその電気通信を規律する主権を十分に認識」するように，国家主権に基づく活動であり，その運用ならびに停止に関しても国家の広範な裁量が付与されている。さらに無線通信規則第 15 条も有害な干渉を禁止し，「不要な伝送，過剰な信号の伝送，間違った若しくは誤解を生じさせる信号の伝送もしくは識別ない信号の伝送を行うこと」を「すべての局に」禁止し[40]，中継局は業務を果たすのに必要なエネルギー（power）しか放射しなくてはならない」[41]と規定する。このように「有害な干渉」の禁止は ITU 法の中核をなし，その強化は無線通信規則の改定により進められている[42]。2002 年（改正）海上における人命の安全のための国際条約（改正 SOLAS 条約）[43]とも呼応し，その義務履行上に必要な周波数を確保するため，無線通信規則第 31 条「全世界的海上安全制度（GMDSS: Global Maritime Distress and Safety Systems）」，第 32 条「遭難通信のための GMDSS 運用手続き」，第 33 条「緊急安全通信のための GMDSS 運用手続き」が追加された。なお ITU 法以外にも国際海洋法および国際航空法において通信の妨害の禁止条項は存在する[44]が，周波数やインターネットによる通信活動には ITU 法が適用される。

2. 有害な干渉禁止原則における義務履行制度

それではサイバーテロリズムの防止という文脈において，「有害な干渉」禁止原則の履行制度はどう機能するのであろうか。ITU 憲章は違反に関する仲裁条項[45]を設けており，干渉が生じた場合には，まず交渉，外交，国際紛争解決のため関係国間で締結された合意に基づいて解決するよう義務付け[46]，それでも問題が解決しなかった場合には仲裁裁判で対応する旨を規定する[47]。強制解決に関する選択議定書も適用されるが[48]，仲裁で解決しない場合に国際司法裁判所へ付託しても勧告にとどまる可能性が高い[49]。なぜなら，前述のように ITU 加盟国は軍用通信に関し他国に干渉されない完全な自由を享受するからである。このため ITU 法は「有害な干渉」の防止措置に重点を置き，①登録制度，②通報制度，③国際監視制度を設けて履行確保を図っている。これら既存の履行制度はサイバーテロリズムの防止に関連するため，以下確認する。

(1) 登録制度　ITU 加盟国は，無線通信規則に従い割り当てられた周波数とそれに付随する軌道の性質について国際周波数登録原簿（Master International Frequency Register）に登録しなくてはならない[50]。この登録により加盟国および通信事業社の権利義務が生じ[51]，また，登録により周波数の取得に関する国際認識（international recognition）が得られ，結果としてその周波数が国際的に保護される仕組みである[52]。各国の主管庁は，ITU の業務別の周波数分配に基づき国内の通信業務の割り当てを行い，その使用実績を無線通信局長に通告し，審査を得て同原簿に登録している。

(2) 通報制度　ITU 憲章，条約，無線通信規則に違反する干渉を探知した管理組織，管理局もしくは査察官は，違反している行政機関に対し通達しなくてはならない[53]。深刻な違反の場合，違反通信局に対して管轄権を有する国家に，それを探知した管理組織から抗議（representations）が付される[54]。もし自国の管轄下にある通信局によって ITU 憲章，条約もしくは無線通信規則の違反（特に ITU 憲章第 45 条の「有害な干渉」および同規則第 15 条が禁止する不要な伝送）があったと情報を得た管理機関は，事実を確かめ，必要な措置をとらなくてはならない[55]。問題解決のために通報制度を適用する際，最大限の善意（the utmost goodwill）と相互支援を実施することが ITU 加盟国にとって必要不可欠（essential）であり[56]，これらの問題解決には，周波数の調整，送受信アンテナの特徴，時間共有，多重チャネル伝送におけるチャンネル変更といった技術・運用に関する要素にも十分な考慮が支払われる[57]。特に遭難安全周波数および航空飛行の安全性と規則性（regularity）に使われる周波数は絶対的な国際保護を要し，その伝送に対する有害な干渉の排除は最重要規則（imperative）と認識され，有害な干渉に気が付いたとき管理機関はただちに措置を取らなくてはならない[58]。同項の表現は ITU 憲章第 45 条をより詳細にしたものである。なお，自国の管轄下にある通信局が有害な干渉の発生源と通報があった場合，その連絡を受け取った旨をできるだけ早く認容しなくてはならないが，この認容自体は（国家）責任の受容したことにはならない[59]点が興味深い。

一方，安全業務（safety services）が有害な干渉を被った場合，被害局に管轄権を有する管理機関は，干渉源である通信局に対して直接に連絡を取るこ

とができ[60]，発生源の通信局に管轄権を有する管理機関は，迅速に対応するため調査し，必要な回復措置をとらなくてはならない[61]。もし有害な干渉の発生源が特定できない場合，監視機関は ITU 関連局に支援を要請することができ，無線通信局（Bureau）は国際監視システムの協力を要請することができる[62]。有害な干渉の発生源が特定できる場合は通報制度で対応するが，特定できない場合は次の国際監視制度に頼ることとなる。

(3) 国際監視制度　ITU 法における国際監視制度[63]は，いわゆる軍縮・軍備管理法における検証制度に類似し，履行確保のための監視および透明性確保および信頼醸成を目的とする。無線通信規則の義務履行を支援し，特に無線周波数スペクトルの合理的かつ経済的な利用を確保するため，管理機関は監視施設の開発および協力に同意している[64]。国際監視制度といっても，監視局自体は ITU-R23-1 および IRU-R SM.1139 に従い選定され，その監視主体は民間企業であったり複数国による共同業務であったりとさまざまである[65]。国際監視制度に参加している管理機関が規則違反を発見した場合，無線通信局に通報するが，無線通信局は違反を犯している局に「注意を向ける」にとどまる[66]。なお，同制度では干渉と有害な干渉との区別はされておらず，単に規則違反を監視する機能を果たしている。

以上の履行制度により，通信に対する「有害な干渉」禁止原則の履行に注力する ITU 法だが，当然ながら，サイバーテロリズムの防止に特化した条項は設けられていない。冒頭で述べたとおり，悪意あるコンピュータ・ウィルスによって運用システムが不正に操作され，他国の通信に有害な干渉を生じさせた場合，加害国の認定が困難になる可能性は高い[67]。自国の電気通信に対し他国からサイバーテロリズムとしての有害な干渉を受けた場合，加盟国は国内法令に従って，国の安全を害すると認められる司法又はその法令，公の秩序若しくは善良の風俗に反すると認められるものを遮断する権利を留保し[68]，他の私用の電気通信であって国の安全を害すると認められるもの又はその法令，公の秩序若しくは善良の風俗に反すると認められるものを遮断する権利を留保する[69]。さらに，国際電気通信業務を全般的に，又は一定の関係若しくは通信の一定の種類（発信，着信又は中継）に限って，停止する権利を留保する[70]。つまり，通信は国家主権に基づくため，サイバー脅威に対する

措置として通信の遮断・停止もその裁量で決定できるのであり，コンピュータ・システムを断絶する電子封鎖（electronic blockade）も可能である[71]。

5. 2001 年サイバー犯罪条約によるサイバーテロリズムの防止可能性と課題

それではサイバーテロリズムの防止という文脈において，2001 年サイバー犯罪条約がどのように機能するのであろうか。そもそもサイバーテロリズムとサイバー犯罪とはまったく異なる性質の行為ではなく，むしろサイバー犯罪はサイバーテロリズムの構成要素の一つとなりうる[72]。本章ではサイバー犯罪の定義，2001 年サイバー犯罪条約の成立経緯，サイバーテロリズムに対する防止機能について述べる。

まず一般的にサイバー犯罪の定義は学術研究者，コンピュータセキュリティ専門家，ユーザによって異なる[73]。サイバー犯罪による企業顧客データや年金機構における個人情報の流出なども時折サイバー攻撃（cyber attack）と称されることもある[74]が，武力攻撃に匹敵する損害を引き起こすサイバー攻撃となれば *jus ad bellum* や *jus in bello* といった国際人道法の適用対象となるはずである。新聞などメディアで使われる用語には一貫性がみられない。一方，国際法におけるサイバー犯罪の定義は，コンピュータ関連犯罪（computer-related crime）の用語とともに議論が重ねられている。簡単に言えば前者の方が後者より概念が狭い。その理由は，後者がコンピュータ・ネットワークとの関連性を含むためであり，コンピュータ・システムのみの損害といった「ネットワークに関係のない」犯罪も含むからである[75]。これら 2 つの用語は狭義・広義のサイバー犯罪定義として 2000 年 4 月にオーストリア・ウィーンで開催された第 10 回「犯罪防止および犯罪者の処遇に関する国連会議」において議論された[76]。

同会議において，狭義（前述サイバー犯罪）は「コンピュータのセキュリティおよびそのデータを攻撃する“電子オペレーション”を手段とする違法な

行為すべて[77]」と定義され，一方，広義のコンピュータ関連犯罪は「コンピュータ・システムまたはネットワークという手段で，もしくはそれに関連して，置かされる違法行為すべて」と定義された。これには違法な所持およびコンピュータ・システムまたはネットワークによって配布する情報の保持といった犯罪も含まれる。さらに，1990 年代の学者による定義は，狭義と広義の中間に位置する。「コンピュータやネットワークが犯罪行為の手段，攻撃対象，もしくは犯行現場である，いかなる行為」[78]という定義であるが，これではパソコンを投げて殺人を犯した場合にも該当してしまう欠点がある[79]。一方，まだ条約に至っていない“スタンドフォード草案の第 1 条 1 項の「サイバー・システムに関する犯罪」というのでは広すぎるであろう[80]。このように，いまだサイバー犯罪という用語は多様な犯罪行為を指すため，実質上の定義の確定は困難である[81]。通信に有害な干渉を引き起こすサイバーテロリズムは，2001 年サイバー犯罪条約におけるどの定義が該当するのであろうか。

サイバー犯罪の定義は，同条約第 2 条から第 10 条までの 9 条項に明記されている。ITU はこれら 9 条項を，グローバル・サイバーセキュリティ・アジェンダ[82]において次の 4 つに分類した。①コンピュータ・データおよびシステムの機密性（confidentiality）・整合性（integrity）・有用性（availability）に対する犯罪，②コンピュータ関連犯罪，③コンテンツ関連犯罪，④著作権関連犯罪[83]，である。この分類は①③④が法的保護の対象にしているのに対し，②だけ犯罪手段に着目しているため[84]，分類間の重複を生じさせるという批判もある[85]。このうちサイバーテロリズムに関連するのは，不正アクセス（第 2 条），違法なデータ取得・傍受（acquisition）（第 3 条），データの傍受（interception）（第 4 条），システムの妨害（第 5 条），装置の濫用（第 6 条），コンピュータ関連の偽造（第 7 条）およびコンピュータに関連する詐欺（第 8 条）の 7 条項である。HLEG 報告書では児童ポルノ犯罪は第 9 条に規定されるが，本節では電気通信に深く関連する第 2 条から第 8 条までを個別に検討する。

不正アクセスについて規定する第 2 条は，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自国の国内法上の犯罪とするよう立法義務を課す。犯罪要件は，防護措置

の侵害，データを取得する意図その他の不正な意図，また他のコンピュータ・システムに接続されているコンピュータ・システムに関連する行為である。不正アクセスはハッキングとも称され，コンピュータ・システムへの不法なアクセスを意味するもので，コンピュータ関連犯罪の中でもっとも古い[86]。インターネットといったコンピュータ・ネットワークの開発に従い，不正アクセス犯罪は急増し，ハッキングの攻撃ターゲットに米国の宇宙機関 NASA をはじめとする各国の宇宙機関も狙われている[87]。その動機には単にハッカーの腕試しというものもあれば，政治的イデオロギーのためにハッキングを行うハクティヴィズム（hacktivism）やサイバープロテスト（cyberprotest）と称する政治活動家が，国連といった極めて公共な機関の HP で政治的メッセージを発する事例もある[88]。概して不正アクセスはサイバー犯罪の第一歩にすぎない[89]もののサイバーテロリズムやサイバー攻撃に発展する可能性は十分にあり，それらの境界が不明確である点はすでに述べたとおりである。

第 3 条はデータ通信におけるプライバシーの権利保護を目的としており，一般にフィッシング（phishing）と呼ばれる違法なデータ傍受について規定する。コンピュータ・データの非公開送信（電磁的放射を含む）が権限なしに行われることを国内法上の犯罪とし，締約国に対して立法措置を義務付ける。同趣旨の欧州人権条約[90]第 8 条にも対応しており，データ取得の対象は，軍事上の機密情報から美術館の作品のアーカイブなど多岐にわたる。データ取得には，被害者のコンピュータに侵入する技術的手段から，人を騙してパスワードを盗むという人的手段まであるが，フィッシングの一番の特徴は，データの漏えい（Data Breach）という事実が巨額の損失をもたらす点である。ビッグ・データという顧客情報を基にした巨大なデータを大企業が利用している場合，違法なデータ取得による流出は巨額の損害をもたらす[91]。企業の信用を落とすことで株価が下がるといった経済的損失を狙う犯罪でもある。

ITU のサイバーセキュリティ強化の文脈で HLEG が特に関連性を指摘したのが第 4 条から第 6 条である。第 4 条はデータの妨害について定めており，コンピュータ・データおよびプログラムにも有形物と同様に，意図的な損害を指す[92]。システム妨害は個人間の E-mail の妨害も含めたインターネッ

ト通信の妨害および有線・無線通信の妨害を含む。なお，インターネット・インフラ・プロバイダーおよびインターネット・サービス・プロバイダ間のデータ転送は，妨害に対するセキュリティで守られているものの，脆弱性はある。公共の場にある無料 Wi-Fi スポットだけでなく，有線の通信も同じく妨害される[93]。電話の通話傍受を違法とする国は多くなっているが，ITU がインターネットに基づく ICTs 全般を管轄する現在，IP 電話やスカイプといった SNS による通話の傍受も犯罪化するよう，国内法整備を加盟国に促している。

データの妨害につづき，第 5 条はシステムの妨害（interference）について規定する。妨害はコンピュータの破損（sabotage）や，コンピュータ・データを用いての「電気通信施設の意図的な妨害（hindering）」も犯罪として国内法整備するよう締約国に義務を課す[94]。Hindering の用語はコンピュータ・システムの適切な機能に干渉する行為を意味し，権限なくして，犯罪に相当するだけの深刻な妨害を指す[95]。

第 6 条は装置の濫用（misuse）は，第 2－5 条の犯罪を意図してコンピュータ機器やデータにアクセスするという濫用を対象とし，コンピュータ・システムやデータの気密性，整合性，有用性に対する犯罪である。これらの犯罪はアクセス手段（hacker's tool）の保持が必要なため，犯罪目的でアクセス手段を入手しようとするインセンティブがかなり高い。また，売り買いを目的とした闇市場まで作られる。このため同条項は，条件付きアクセスの法的保護に関する欧州評議会および欧州の文書基づいて導入され[96]，また，同様の条項はすでに 1929 年偽造通貨の禁圧に関する国際条約[97]に盛り込まれている[98]。

以上，2001 年サイバー犯罪条約におけるサイバー犯罪の定義を概観したが，サイバーテロリズムを目的とした「有害な干渉」を起こすサイバー犯罪に該当するのは，不整合性（第 2 条），データの妨害（第 4 条），システムの妨害（第 5 条）および装置の濫用（第 6 条）である。サイバーテロリズムの初動となるサイバー犯罪を国内刑法で対応することができれば，サイバーテロリズムの脅威は低減されよう。

6. おわりに

本稿では，既存の有害な干渉禁止原則のほか，ITU が加盟国に批准を進める 2001 年サイバー犯罪条約がサイバーテロリズムという脅威の低減および防止に有用である点を確認してきた。しかし国際法において国際テロリズム，サイバー空間，サイバー犯罪，サイバーテロリズムなど主要な用語は定義が確立しておらず，また，サイバーテロリズムとサイバー攻撃との区別も難しいのが現状である。例えば，サイバー攻撃は国家やその主要産業のコンピュータ・システムを攪乱・麻痺させることを目的とし，サイバー犯罪およびサイバーテロリズムと比べて一般にその規模がはるかに大きく，また国家の関与が疑われると考えられるが[99]，実際にはサイバーテロリズムを引き起こす初動はサイバー犯罪と認定される可能性もあり，それらの区別は極めて不明瞭である。さらに国家の関与するサイバーテロリズムに対して 2001 年サイバー犯罪条約は十分に実効的に対応できない[100]。このため ITU の HLEG は，サイバー犯罪のほか「重要な情報インフラの運用に対する大量かつ同調したサイバー攻撃」を犯罪化する立法措置の必要性も指摘している[101]。要するにサイバーテロリズムの防止には既存の有害な干渉禁止原則に加え，2001 年サイバー犯罪条約に基づいた各国の国内法整備および一連のサイバー不法行為の明確な分類基準が必要である。

〔付記〕　本稿は，早稲田大学社会安全政策研究所第 63 回 WIPSS 定例研究会における報告をもとに加筆修正したものであり，科学研究費基盤 C「国際テロリズムの未然防止に関する国際法枠組み」（科研費番号：JP18K01286, 研究代表者：皆川誠）の研究成果の一部である。

---

[1] 1865 年 5 月 17 日に国際電信条約に基づき国際電信連合（International Telegraph Union）として設立した世界最古の国際機関。2019 年現在，加盟国 193 か国および民間事業体約 700 社を有する。ITU, *Overview of ITU's History*. Available at: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/12.28.71.en.pdf [accessed on 15 September 2019].

[2] Constitution and Convention of the International Telecommunication Union, Constitution, 1825 *UNTS* 331; Convention, 1826 *UNTS* 390, 1 July 1994.

[3] B. Saul and K. Heath, "Cyber terrorism", in: N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspac*e, Edward Elgar Publishing, 2015, p. 147.

[4] 皆川誠『国際条約における「テロリズムの定義」確定の課題と展望（秋元浩一教授退職記念号)』名古屋学院大学論集 54, no. 3（2018）167-81 頁.

[5] K. Kittichaisaree, *Public International Law of Cyberspace*, Springer, 2017, p. 2.

[6] *Ibid.*

[7] UNODC はサイバーテロリズムを 6 項目に分類しており（プロパガンダ，資金繰り，訓練，計画，実行，サイバー攻撃），引用した定義は 6 番目のサイバー攻撃の定義として記されている。UNODC, "I. The use of the Internet for terrorist purposes", *The Use of the Internet for Terrorist Purposes*, 2012, p. 11. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [accessed on 27 September 2019].

[8] CTITF, "Countering the use of the Internet for terrorist purposes" (Working Group Report, CTITF Publication Series, Februray 2009).

[9] Constitution and Convention of the International Telecommunication Union, Geneva, 22 December 1992, 1825 *UNTS* 1; *UKTS* 1996 No. 24; Cm. 2539; ATS 1994 No. 28; Final Acts of the Additional Plenipotentiary Conference, Geneva, 1992 (1993), p.1.

[10] *Ibid.*, p. 71.

[11] 本稿では ITU 憲章，ITU 条約および行政規則の総称として ITU 法と称する。行政規則には世界通信会議（World Radiocommunication Conference：WRC）で規定される ITU 憲章条約付属無線通信規則（Radiocommunication Regulations：RR）や国際無線通信規則（International Radiocommunication Regulations：IRR）を含む。

[12] Article 1 (2) (a) of the ITU Constitution of 1994.

[13] 青木節子『商用衛星運用をめぐる法規制 - 岐路に立つ宇宙法ー』No. 97（衛星通信研究, 2002.5）44 頁。

[14] 衛星通信とは，衛星から構成される宇宙部分（space segment）と地球局で構成される地上部分（ground segment）の両方を使い，上り回線（up link）および下り回線（down link）という通信回線をもって通信を可能とするシステムである。宇宙物体を対象とする無線通信は一括して宇宙無線通信と称され，衛星上に開設される無線局を経由して地上の無線局との間を通信することを衛星通信という。飯田尚志編著『衛星通信』（Ohmsha，1997 年）3 頁参照。

[15] Article 44 (2) of ITU Constitution of 1994, " In using frequency bands for radio services, Member States shall bear in mind that radio frequencies and any associated orbits, including the geostationary-satellite orbit, are limited natural resources and that they must be used rationally, efficiently and economically, in conformity with the provisions of the Radio Regulations, so that countries or groups of countries may have equitable access to those orbits and frequencies, taking into account the special needs of the developing countries and the geographical situation of particular countries".

[16] 静止軌道（geostationary orbit）とは，地球表面から約 35.800km の高さの円軌道で，その軌道面は地球の自転を考えて赤道面，しかも衛星は地球の自転と同周期で同じ方向に回れば，いつも空の一か所に静止しているように見える特徴を有する。この軌道を利用すると信号が継続的に受信されるため，受信追跡局の設置が不要となり，科学目的あるいは航行管制，気象業務，エネルギー伝送，通信・放送業務などの応用目的にとって極めて有用である。栗林忠男「静止軌道の法的地位と周波数帯の分配問題」山本草二編『放送衛星－その法制度的研究－』（日本放送出版

協会，1981 年）41 頁参照。

[17] UN Res., A/RES/57/239, “Creation of a global culture of cybersecurity,” 31 January 2003. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf [accessed on 20 September 2014].

[18] World Summit on the Information Society, “Geneva 2003-Tunis 2005.” Available at: http://www.itu.int/wsis/tunis/newsroom/ [accessed on 25 July 2019]. チュニス・アジェンダは ECOSOC に対し，ジュネーブとチュニスの成果を国連システム全体でフォローアップするうえで，監督役を務めるよう要請する。9 月のニューヨークでのサミットで世界の指導者が要請した ECOSOC 改革に沿い，チュニス・サミットの最終文書は ECOSOC に対し，多数のステークホルダーが参加するアプローチを含め，開発科学技術委員会（Commission on Science and Technology for Development）の権能を再検討するよう求めている。国際連合広報センターHP 参照。 Available at: http://www.unic.or.jp/news_press/features_backgrounders/901/ [accessed on 25 July 2019].

[19] The Convention on Cybercrime, Council of Europe, *ETS* no. 189, Budapest, 23 November 2001.

[20] European Convention on the Suppression of Terrorism, *ETS* no. 90, Strasbourg, 27 January 1977.

[21] ITU Report, “Report of the Chairman of HLEG,” *Global Cybersecurity Agenda*, High-Level Experts Group, 2007, p.1. Available at: http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf [accessed on 23 October 2019].

[22] ITU Report, “Understanding cybercrime: Phenomena, challenges and legal response,” November 2014. Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf [accessed on 27 July 2019].

[23] Council of Europe, “Recommendation No. R. (89) of the Committee of Ministers to Member States on Computer-related Crime.” Available at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 [accessed on 25 October 2019].

[24] Council of Europe, CDPC/103/211196, “Explanatory Report to the Convention on Cybercrime,” 23 November 2001. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [accessed on 25 February 2019].

[25] *Ibid.*, p. 2.

[26] *Ibid.*

[27] Council of Europe, The Committee of Ministers, Ministers’ Dispute, Decision no. M/Del/Dec(97)583.

[28] Council of Europe, *supra* note 24.

[29] Council of Europe, The Committee of Ministers, Ministers’ Dispute, Decision no. M/Del/Dec(99)679.

[30] Council of Europe, The European Ministers of Justice, Resolution No.1 of 1997 and No. 3 of 2000. *See* also, *supra* note 24, p. 3.

[31] 外務省『サイバー犯罪に関する条約の説明書』（平成十六年二月）1 頁。Available at: http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4b.pdf [accessed on 29 September 2019].

[32] 例として日本国内法を挙げると，次の 3 点が問題となる。捜査手続きにおいて①データの押収方法としてファイルの複製によるものとすることができなければならない点，②トラフィック

データのリアルタイム傍受を実施できなければならない点，③プロバイダは，技術的能力の範囲内で捜査機関に協力しなければならない点である。夏井高人『サイバー犯罪条約の主要論点』法律論叢 75（2-3）, 2002-12-25, 263 頁。

[33] 夏井『前掲書』。

[34] 王志安「越境コンピューター捜索の法的地位―サイバー犯罪条約が残した課題―」『駒澤大学』第 3 巻 3 号（2004 年 4 月）114-132 頁。

[35] ITU 憲章第 45 条 1 項。なお，「干渉」は日本の電波通信法では「混信」と訳される。

[36] 2012 年無線通信規則第 1.166 条 "[T]he effect of unwanted energy due to one or combination of emission, radiations upon reception in a *radiocommunication* system."

[37] 2012 年無線通信規則第 1.169 条 "[I]nterference which endangers the functioning of a radionavigation service or of other safety services […] seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service […].

[38] "[A]ll stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations," ITU憲章第45条1項。

[39] ITU 憲章第 48 条は「有害な干渉」禁止事項の例外として「加盟国は軍事無線施設に関しては完全な自由を有する」（1 項）と規定する。しかしその自由も救難共助・有害な干渉回避・周波数に関する規定はできる限り遵守し（2 項），公衆（public）通信業務に参加する際は原則，関連規則に従わなくてはならない。

[40] 2012 年無線通信規則第 15 条§1。

[41] 2012 年無線通信規則第 15 条§2。

[42] 1987 年 ITU 開催の「移動業務に関する世界無線通信主管庁会議（WARC MOB-87）」において ITU 憲章条約附属無線通信規則が改定され，2007 年世界通信会議（WRC-07）を経て，「第 15 付属無線通信規則に記載される周波数」への干渉禁止が加わった。

[43] International Convention for the Safety of Life at Sea, entered into force on 25 May 1980, 32 *UST* 47; 1184 *UNTS* 278.

[44] ITU 法以外にも，国際海洋法および国際航空法において通信妨害を禁止する条項がある。1974 年改正海上における人命の安全のための国際条約（SOLAS 条約 4 章 C 第 9 規則）（b）は「無線電信室は［・・］無線電信局の運用を妨害することのあるいかなる目的にも使用してはならない」と規定し，また，国連海洋法条約第 19 条 2 項（k）は無害通航の意味として「沿岸国の通信系又は他の施設への妨害を目的とする行為」と規定する。さらに 1971 年民間航空不法行為防止条約（モントリオール条約）第 1 条 1 項では「不法かつ故意に行う」「(b) 業務中の航空機を破壊し，又は業務中の航空機に対しその飛行を不能にする損害若しくは飛行中のその安全を損なうおそれがある損害を与える行為」又は「(d) 航空施設を破壊し，又はその運用を妨害する行為（飛行中の航空機の安全を損なうおそれがあるものに限る）」および「(e) 虚偽と知っている情報を通報し，それにより飛行中の航空機の安全を損なう行為」を犯罪として規定しており，これらの未遂および加担も含まれる。

[45] ITU 憲章第 56 条および ITU 条約第 41 条。

[46] ITU 憲章第 56 条 1 項。

[47] ITU 憲章第 56 条 2 項。

[48] ITU 憲章第 56 条 3 項。より詳細な手続きについては ITU 条約第 41 条に規定される。

[49] B. Cheng, *Studies in International Space Law,* Clarendon Press Oxford, 1997, p.96.

[50] ITU条約第12条(e) “in accordance with the relevant provisions of the Radio Regulations, effect an orderly recording and registration of frequency assignments and, where appropriate, the associated orbital characteristics, and keep up to date the Master International Frequency Register; review entries in that Register with a view to amending or eliminating, as appropriate, those which do not reflect actual frequency usage, in agreement with the administration concerned.”
[51] “[T]he international rights and obligations of administrations in respect of their own and other administrations’ frequency assignments1 shall be derived from the recording of those assignments in the Master International Frequency Register (the Master Register) or from their conformity, where appropriate, with a plan. Such rights shall be conditioned by the provisions of these Regulations and those of any relevant frequency allotment or assignment plan,” Article 8 (1) of ITU Radiocommunication Rules.
[52] “[A]ny frequency assignment recorded in the Master Register with a favourable finding under No. 11.31 shall have the right to international recognition. For such an assignment, this right means that other administrations shall take it into account when making their own assignments, in order to avoid harmful interference. In addition, frequency assignments in frequency bands subject to coordination or to a plan shall have a status derived from the application of the procedures relating to the coordination or associated with the plan,” Article 8 (3) of ITU Radiocommunication Rules.
[53] 2012 年無線通信規則第 15 条§11。
[54] 2012 年無線通信規則第 15 条§12。
[55] 2012 年無線通信規則第 15 条§13。
[56] 2012 年無線通信規則第 15 条§14。
[57] 2012 年無線通信規則第 15 条§15。
[58] 2012 年無線通信規則第 15 条§20。
[59] 2012 年無線通信規則第 15 条§27。
[60] 2012 年無線通信規則第 15 条§28。
[61] 2012 年無線通信規則第 15 条§29。
[62] 2012 年無線通信規則第 15 条§34 (2)。
[63] 2012 年無線通信規則第 16 条。
[64] 2012 年無線通信規則第 16.1 条。
[65] 2012 年無線通信規則第 16.2 条。
[66] 2012 年無線通信規則第 16.8 条。
[67] H. Harrison-Dinniss, *Cyber Warfare and the Laws of War*, Vol. 92, Cambridge University Press, 2012, pp. 99-102.
[68] 1994 年 ITU 憲章第 34 条 1 項。
[69] 1994 年 ITU 憲章第 34 条 2 項。
[70] 1994 年 ITU 憲章第 35 条。
[71] 中谷和弘「サイバー攻撃と国際法」『国際法研究』第 3 号（2015 年 3 月）, 86 頁。
[72] S.W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford University Press, 2009, pp. 37-45.
[73] S. Gordon and R. Ford, “On the definition and classification of cybercrime,” *Journal in Computer Virology*, 2006, vol. 2, pp. 13-20.
[74] 例として，日本経済新聞朝刊「『年金任せられない』，機構，情報流出で調査報告書―サイバー攻撃，特定は難しく。」2015 年 8 月 21 日，34 頁。
[75] ITU Report, *supra* note 22, p. 11.

[76] 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, p. 5. Texts are available at: http://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf [accessed on 7 September 2019].
[77] ITU Report, *supra* note 22, p. 5. "[A]ny illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them."
[78] *Ibid.*, p. 11.
[79] *Ibid.*
[80] A.D. Sofaer, "Toward an International Convention on Cyber Security," *The Transnational Dimension of Cyber Crime and Terro*, Hoover Press, pp. 221-248. Available at: http://media.hoover.org/documents/0817999825_221.pdf [Accessed: 8th September 2019].
[81] Gordon and Ford, *supra* note73.
[82] ITU Doc., *supra* note 21.
[83] 外務省の資料では「コンピュータ・データ及びコンピュータ・システムの秘密性，完全性及び利用可能性に対する犯罪」と訳されている。
[84] ITU Report, *supra* note 22, p. 12.
[85] *Ibid.*
[86] "Hacking Offences," *High Tech Crime Brief*, Austrian Institute of Criminology, Vol. 5, 2005. Available at: http://www.aic.gov.au/media_library/publications/htcb/htcb005.pdf [accessed on 9 September 2015].
[87] 土屋大洋「第 5 章　第四と第五の作戦空間の登場：宇宙とサイバーの交差」『平成 24 年度外務省委託事業「宇宙に関する各国の外交政策」についての調査研究－提言・報告書－』（公益財団法人日本国際フォーラム，2013 年 3 月）61-69 頁参照。
[88] BBC News, "UN's website breached by hackers." Available at: http://news.bbc.co.uk/2/hi/technology/6943385.stm [accessed on 9 September 2019], cited in *supra* note 22, p. 17.
[89] *See*, M.D. Goodman and S.W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace," *UCLA Journal of Law and Technology*, Vol. 10, Issue 2, 2002, p. 146.
[90] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, *ETS* 5. Available at: http://www.refworld.org/docid/3ae6b3b04.html [accessed on 28 February 2016].
[91] Financial Times, "Target to pay $67m over Visa data breach," 18 August 2015. Available at: http://www.ft.com/cms/s/0/a6b571d8-45c8-11e5-af2f-4d6e0e5eda22.html#axzz3lFCTsVue [accessed on 9 September 2019].
[92] Council of Europe, *supra* note 24, p. 11.
[93] Council of Europe, *Organized Crime Report 2004: Focuses on the Cybercrime*, 23 December 2004, p. 97. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf [accessed on 28 February 2016].
[94] Council of Europe, *supra* note 24, p. 11.
[95] *Ibid.*
[96] European Convention on the legal protection of services based on, or consisting of, conditional access, *ETS* no. 178; and Directive 980840EC of the European Parliament and the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access.
[97] International Convention for the Suppression of Counterfeiting Currency with Protocol and Optional Protocol, *LNTS*, vol.112, 1929, pp.371.

[98] Council of Europe, *supra* note 24, pp. 12-13.
[99] 中谷「前掲論文」（注 71）61-62 頁。
[100] 中谷和弘「テロリズムに対する諸対応と国際法」山口厚＝中谷和弘編『安全保障と国際犯罪（融ける境　超える法　第 2 巻)』（東京大学出版会，2005 年）108 頁参照。
[101] ITU Report, *supra* note 21, p.7.