サイバー犯罪条約（ETS No.185）の説明書

［参考訳］

2016 年 12 月 16 日
明治大学法学部教授
夏　井　高　人

＊＊＊

Explanatory Report to the Convention on Cybercrime (Budapest, 23.XI.2001)のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Web サイトから入手した。

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[2016 年 10 月 29 日確認]

この説明書（以下、単に「説明書」という。）は、欧州評議会のサイバー犯罪条約（Convention on Cybercrime ETS No.185）の説明書[1]として 2001 年 11 月 23 日に公表されたもので、サイバー犯罪条約の条項を解説する文書である[2]。説明書の冒頭には、公式の注釈書ではないと明記されている。しかし、この説明書は、サイバー犯罪条約に定めるサイバー犯罪及びその捜査手続のみならず、関連する EU の法令を解釈する場合においても必読の非常に重要な文献資料となっている。

サイバー犯罪条約の説明書と関連する他の文書としては、サイバー犯罪条約追加議定書（ETS No.189）の解説書（Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 28.I.2003)）がある。サイバー犯罪条約の概要については、経済産業省サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」（2002 年 4 月）及び夏井高人・岡村久道・掛川雅仁編『Q&A インターネットの法務と税務』（新日本法規出版、2001～2016・加除式出版物）の該当箇所を参照されたい。

この参考訳は、あくまでも説明書（Explanatory Report）の私的な和訳である。

---

[1] サイバー犯罪条約の説明書（Explanatory Report）は、条約の起草段階及び条約締結当初においては、説明用覚書（Explanatory Memorandum）との名称が付されていた。この両者は同一の文書であるが、現在の名称は、「説明書（Explanatory Report）」である。説明書は、説明用覚書を浄書した完成版という位置づけになる。

[2] 外務省のサイトで公開されている「説明書」と題する文書は、サイバー犯罪条約の加盟を国会で承認する際に日本国政府外務省の担当部局によって用意されたものであり、欧州評議会の公式文書としての説明書（Explanatory Report）とは異なる。

過日、この説明書の前身となった説明用覚書草案（Draft Explanatory Memorandum）の仮訳を試みたことがある。この説明用覚書の仮訳は、2001 年 5 月 1 日に、下記のサイト上で公開した。

http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/expmemo25.htm [2016 年 11 月 1 日確認]

また、この説明書（Explanatory Report）の中でも触れられている個人データ保護指令 95/46/EC の第 29 条に基づいて設置された個人データの処理と関連する個人の保護に関する作業部会が 2001 年 4 月に公表した「欧州評議会のサイバー犯罪条約草案に関する意見書」（2001 年 3 月 22 日採択）の仮訳は、2001 年 4 月 27 日に下記のサイト上で公表した。

http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/WG-opinion.htm [2016 年 11 月 1 日確認]

説明書は、前文、序文及び本文（条約の各条項の注釈）で構成されている。この参考訳では、原注を含め説明書の全文を訳出した。

今回の説明書の訳出は、2001 年当時の説明用覚書草案と現在の説明書との間に内容的に相違があるか否かを確認するために行った。

この検討の結果として、説明用覚書草案の段階では仮の記述になっていた部分が、現在の説明書では確定版の記述に変更されていることが判明した。また、説明書は、覚書草案中には存在しなかった文章を少なからず含んでいる（例：冒頭の I 及び II、序文の第 22 項ないし第 31 項）。説明書で修正・付加がなされた部分の中にはほぼ置き換えに近いものを含め、大規模な修正が行われている部分もある（例：第 145 項ないし第 148 項、第 173 項、第 177 項、第 184 項、第 190 項、第 234 項、第 269 項、第 286 条、第 316 項ないし第 319 項等）。これらの大規模な修正部分については新たな翻訳ということになる。

加えて、確認可能な限り、誤訳や誤解のあった部分を補筆・修正したほか、その後の研究結果を踏まえ、訳語等を変更した部分がある。

この参考訳で採用した訳語は、外務省のサイトで公表されている公式訳[1]の訳語とは異なる部分がある。公式の訳語については、外務省訳を参照されたい。

参考訳の訳出に際しては、可能な限り直訳に務めたが、日本語として理解しにくい場合については意訳とした部分がある。参考訳の訳文だけではわかりにくい部分については訳注を付した。説明書中にある原注と識別できるようにするため、訳注には[訳注]と記してある。また、必要に応じ、脚注（訳注）内で関連する日本国法との対応関係を示し、現時点における問題点や最近の動向等について述べた。ただし、網羅的ではない。

この参考訳の訳出に際して、過去に作成された説明書の仮訳（前掲経済産業省サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」の中に逐条解説

[1] http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html [2016 年 10 月 29 日確認]

として収録されている抄訳、並びに、瀧波宏文「「サイバー犯罪に関する条約」についてーその意義及び刑事実体法規定」警察学論集 55 巻 5 号 124～145 頁 (2002)、同「「サイバー犯罪に関する条約」についてー手続法及び国際協力規定（上）」同誌 55 巻 9 号 150～173 頁 (2002)、同「「サイバー犯罪に関する条約」についてー手続法及び国際協力規定（中）」同誌 55 巻 10 号 113～137 頁 (2002)、同「「サイバー犯罪に関する条約」についてー手続法及び国際協力規定（下）」同誌 55 巻 11 号 105～125 頁 (2002)に収録されている解説等）を参考にしたが、あくまでも参考程度にとどめ、独自にこの参考訳を作成した。

欧州評議会のサイバー犯罪条約に対応する EU のサイバー犯罪指令 2013/40/EU の条文の参考訳は、法と情報雑誌 1 巻 1 号 51～61 頁にある。

この参考訳の訳出に際しては、丸橋透氏（ニフティ株式会社法務部長・米国ニューヨーク州弁護士・明治大学法科大学院講師）及び金子敏哉氏（明治大学法学部准教授）から助言を得た。

また、この参考訳を作成するに際しては、上掲の文献及び関連する脚注（訳注）内で示した文献のほか、以下の書籍・文献・資料等を参考にした。

日本語の書籍としては、米澤慶治編『刑法等の一部改正法の解説』（立花書房、1988）、的場純男・河村博『コンピュータ犯罪 Q&A』（三協法規、1988）、日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』（三省堂、1990）、岡村久道『情報セキュリティの法律（改訂版）』（商事法務、2011）、井上正仁『捜査手段としての通信・会話の傍受』（有斐閣、1997）、不正アクセス対策法制研究会編『逐条 不正アクセス行為の禁止等に関する法律（第 2 版）』（立花書房、2012）、大橋充直『ハイテク犯罪捜査入門ー基礎編ー』（東京法令出版、2004）、同『ハイテク犯罪捜査入門ー捜査実務編ー』（東京法令出版、2005）、平野龍一・佐々木史朗・藤永幸治編『注解特別刑法 補巻(1) コンピューター犯罪・国家(地方)公務員法・宅地建物取引業法』（青林書院、1990）、ウルリッヒ・ズィーバー（西田典之・山口厚訳）『コンピュータ犯罪と刑法(1)』（成文堂、1986）、同『コンピュータ犯罪と刑法(2)』（成文堂、1988）、西田典之編『責任論とカード犯罪』（成文堂、2007）、NTT データ技術開発本部システム科学研究所『サイバーセキュリティの法と政策』（NTT 出版、2004）、指宿信・サイバーロー研究会編『サイバースペース法ー新たな法的空間の出現とその衝撃』（日本評論社、2000）、山口厚『刑法各論（第 2 版）』（有斐閣、2010）、西田典之『刑法各論（第 6 版）』（弘文堂、2012）、前田雅英『刑法各論講義（第 5 版）』（東京大学出版会、2011）、山中敬一『刑法各論（第 3 版）』（成文堂、2015）、川端博『刑法各論講義（第 2 版）』（成文堂、2010）、前田雅英編『条解刑法（第 3 版）』（弘文堂、2013）、大塚仁・中山善房・古田佑紀・河上和雄編『大コンメンタール刑法第 3 版第 8 巻＜第 148 条～第 173 条＞』（青林書院、2014）、大塚仁・中山善房・古田佑紀・河上和雄編『大コンメンタール刑法第 2 版第 12 巻＜第 230 条～第 245 条＞』（青林書院、2003）、大塚仁・中山善房・古田佑紀・河上和雄編『大コンメンタール刑法第 2 版第 13 巻＜第 246 条～第 264 条＞』（青林書院、2000）、松尾浩也監修・松本

時夫・土本武司・池田修・酒巻匡編『条解刑事訴訟法（第 4 版）』（弘文堂、2009）、神山敏雄・斉藤豊治・浅田和茂・松宮孝明編『新経済刑法入門（第 2 版）』（成文堂、2013）、高橋郁夫・梶谷篤・吉峯耕平・荒木哲郎・岡徹哉・永井徳人編『デジタル証拠の法律実務 Q&A』（日本加除出版、2015）、中山信弘『著作権法（第 2 版）』（有斐閣、2014）、島並良・上野達弘・横山久芳『著作権法入門（第 2 版）』（有斐閣、2016）、園田寿・曽我部真裕編『改正児童ポルノ禁止法を考える』（日本評論社、2014）、園田寿『解説児童買春・児童ポルノ処罰法』（日本評論社、1999）、末道康之『フランス刑法の現状と欧州刑法の展望』（成文堂、2012）、薬師寺公夫・坂元茂樹・浅田正彦編『ベーシック条約集（2016 年版）』（東信堂、2016）、オーガスト・ベックウェイ（堀部政男・堀田牧太郎訳編）『情報犯罪－コンピューター社会のバルネラビリティ』（啓学出版、1986）、ルーク・ハーディング（三木俊哉訳）『スノーデンファイル』（日経 BP 社、2014）、クリフォード・ストール（池央耿訳）『カッコウはコンピュータに卵を産む（上・下）』（草思社、1991）、ジョナサン・リットマン（桑原透訳）『天才ハッカー「闇のダンテ」の伝説』（文藝春秋、1997）、ケビン・ミトニック、ウィリアム・サイモン（峯村利哉訳）『ハッカーズーその侵入の手口ー奴らは常識の斜め上を行く』（インプレスジャパン、2006）、ウラジミール『チャイナ・ハッカーズ』（扶桑社、2014）、ニール・バレット（斉藤隆央訳）『いかにして奴らは、インターネット犯罪を企てるのか』（七賢出版、2000）、日本シーサート協議会『CSIRT－構築から運用まで』（NTT 出版、2016）、矢田篤史・粕谷真紀子・西村忠興・株式会社 NTT データ（編）『実例情報セキュリティマネジメントシステム（ISMS）の本質化・効率化－ISO/IEC 27001:2013（JIS Q 27001:2014）改正対応版』（日本規格協会、2015）、中尾康二・北原幸彦・竹田栄作・中野初美・原田要之助・山下真『ISO/IEC 27002:2013 (JIS Q 27002:2014) 情報セキュリティ管理策の実践のための規範－解説と活用ガイド』（日本規格協会、2015）、中尾康二・山下真・山崎哲・日本情報経済社会推進協会『ISO/IEC 27001:2013（JIS Q 27001:2014）情報セキュリティマネジメントシステム要求事項の解説』（日本規格協会、2014）、三宅功『CXO のための情報セキュリティ』（ダイヤモンド社、2016）、島田裕次『よくわかるシステム監査の実務解説（改訂版）』（同文舘出版、2015）、財団法人関西情報・産業活性化センター情報セキュリティマネジメント研究会編・岡村久道監修『企業活動と情報セキュリティ』（経済産業調査会、2002）、佐々木良一監修『情報セキュリティプロフェッショナル教科書』（アスキー・メディアワークス、2009）、片方善治監修『IT セキュリティソリューション大系（上・下）』（フジ・テクノシステム、2004）、土居範久・佐々木良一・岡本栄司・寺田真敏・内田勝也・菊池浩明・村山優子編『情報セキュリティ事典』（共立出版、2003）、瀬戸洋一『サイバーセキュリティにおける生体認証技術』（共立出版、2002）、佐々木良一・手塚悟・吉浦裕・三島久典『インターネット時代の情報セキュリティー暗号と電子透かし』（共立出版、2000）、辻井重男・笠原正雄編『暗号と情報セキュリティ』（昭晃堂、1990）、John Viega（葛野弘樹監修・夏目大訳）『セキュリティの神話』（オライリージャパン、2010）、内田勝也・高橋正和『有害プログラムーその分類・メカニズム・対策』（共立出版、2004）、新井悠・岩村誠・川古谷裕平・青木一史・星澤裕二『アナライジング・マルウェアーフリーツールを使った感染事案対処』（オライリージャパン、2010）、御池鮎樹『マルウェアー情報化社会の破壊者』（工学社、2009）、甲斐克則・田口守一編『刑事コンプライアンスの国際動向』（信山社、2015）、川崎友巳『企業の刑事責任』（成文堂、成文堂）、

白石賢『企業犯罪・不祥事の法政策－刑事処分から行政処分・社内処分へ』(成文堂、2007)、板倉宏『企業犯罪の理論と現実』(有斐閣、1975)、中村直人・山田和彦・後藤晃輔『平成 26 年改正会社法対応内部統制システム構築の実務』(商事法務、2015)、新日本有限責任監査法人編『企業の内部統制とリスクマネジメントートップダウンアプローチとリスクベースの内部統制評価』(第一法規、2011)、有限責任監査法人トーマツ エンタープライズリスクサービス『海外子会社管理の実践ガイドブック』(中央経済社、2015) 及び総務省総合通信基盤局消費者行政課『改訂増補版プロバイダ責任制限法』(第一法規、2014) を参考にした。

日本語の論説・資料等としては、井上正仁「コンピュータ・ネットワークと犯罪捜査 (1)」法学教室 244 号 49～66 頁 (2001)、同「コンピュータ・ネットワークと犯罪捜査 (2・完)」同誌 245 号 49～58 頁 (2001)、山口厚「サイバー犯罪条約に関連した刑法改正案」エル・アンド・ティ 26 号 4～11 頁 (2005) 、前田雅英「サイバー犯罪と刑事法」罪と罰 48 巻 4 号 6～12 頁 (2011)、南部篤「コンピュータ・ネットワークに関連する犯罪と刑事立法 (一)」日本法學 78 巻 2 号 55～90 頁 (2012)、同「コンピュータ・ネットワークに関連する犯罪と刑事立法 (二・完)」同誌 78 巻 3 号 27～78 頁 (2013)、成耆政・鈴木尚通・田中正敏・葛西和広「高度情報化社会におけるサイバー犯罪に関する論考－その概念と手法を中心に－」松本大学研究紀要 6 号 63～83 頁 (2008)、佐藤隆司「国境を越えるサイバー犯罪に対する「国際共同捜査」についての一考察」同誌 58 巻 11 号 156～180 頁 (2005) 、島田健一「サイバー犯罪捜査とデジタルフォレンジックの実際」同誌 68 巻 3 号 62～82 頁 (2015)、倉持俊宏「ケーススタディ・サイバー犯罪捜査 (1) －不正指令電磁的記録供用事件:プロキシサーバを経由している犯人にたどり着く－」同誌 69 巻 2 号 93～104 頁 (2016)、同「ケーススタディ・サイバー犯罪捜査 (2) －威力業務妨害・脅迫・不正指令電磁的記録供用事件:遠隔操作ウィルス事件を基に－」同誌 69 巻 3 号 129～144 頁 (2016)、同「ケーススタディ・サイバー犯罪捜査 (3・完) －不正アクセス禁止法違反事件:Tor で隠れる犯人を捜す手段を探る－」同誌 69 巻 4 号 113～128 頁 (2016)、Christian Schwarzenegger (夏井高人・笠原毅彦訳)「サイバー犯罪条約 (2001 年 11 月 23 日) によるコンピュータ犯罪法及びインターネット犯罪法の国際調和－ハッキング、違法なデータ入手及び違法な通信傍受を例に」判例タイムズ 1108 号 70～78 頁 (2003)、クリスチャン・シュワルツェネッガー (園田寿訳)「インターネットにおける刑法の場所的適用範囲－ドイツおよびオーストリアと比較した、スイスにおける国境を越えたインターネット犯罪の訴追」關西大學法學論集 49 巻 1 号 125～153 頁 (1999)、山口厚「サイバー犯罪条約の実体法的意義」法とコンピュータ 21 号 51～55 頁 (2003)、酒巻匡「サイバー犯罪条約の手続法規定について」同誌 21 号 57～64 頁 (2003)、指宿信「インターネットを使った犯罪と刑事手続」法律時報 854 号 10～13 頁 (1997)、石井徹哉「サイバー犯罪条約に関する覚書き」奈良法学会雑誌 15 巻 1・2 号 47～58 頁 (2002)、クラウス・ティーデマン (丹羽正夫・城下裕二訳)「コンピューター犯罪と 1986 年の西ドイツ刑法改正」北大法学論集 39 巻 1 号 117～152 頁 (1988)、上林邦充「コンピュータの不正使用と財産罪」群馬大学社会情報学部研究言侖集創刊号 291～306 頁 (1995)、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」警察学論集 52 巻 11 号 8～27 頁 (1999)、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」同誌同号 28～61 頁 (1999)、早川剛史「ハイ

テク犯罪対策に関する技術開発を促進するための新たな法制の整備について－特定公共電気通信システム開発関連技術に関する研究開発の推進に関する法律の解説」同誌同号 62～89 頁 (1999)、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」同誌 65 巻 6 号 21～47 頁 (2012)、豊田兼彦「児童ポルノを受領する行為の可罰性について」近畿大学法科大学院論集 4 号 79～96 頁 (2008) 、丸橋透「データ照合技術とプロバイダの不作為責任」年報知的財産法 2012 34～41 頁 (2012)、独立行政法院情報処理推進機構（IPA）「情報システム等の脆弱性情報の取扱いにおける法律面の調査報告書」 (2004)、川崎友巳「サイバーポルノの刑事規制（一）－イギリス刑事法との比較法的考察－」同志社法學 51 巻 6 号 82～115 頁 (2000)、同「サイバーポルノの刑事規制（一）－イギリス刑事法との比較法的考察－」同誌 52 巻 1 号 1～36 頁 (2000)、上野芳久「フランス注釈刑法・未成年者を危険にさらす罪（1)」湘南工科大学紀要 33 巻 1 号 119～155 頁 (1999)、同「フランス注釈刑法・未成年者を危険にさらす罪（2・完)」同誌 35 巻 1 号 75～114 頁 (2001)、奥村徹「ネット上の児童ポルノに関する擬律の混乱（sexting・ファイル共有・リンク)」法とコンピュ-タ 29 号 83～100 頁 (2011)、金子敏哉「著作権侵害と刑事罰」法とコンピュータ 31 号 99～114 頁 (2013)、江見健一「送信可能化権侵害による著作権法違反の罪について」研修 718 号 39～56 頁 (2008)、丸橋透「プロバイダの捜査対応、ログ保存、被害抑止協力の実務と考え方」比較法雑誌 49 巻 4 号 63～80 頁 (2016)、同「EU データ保持指令と無効判決の検討」情報ネットワーク法学会第 16 回研究大会予稿（2016)、松沢栄一「通信ログの保全 刑事訴訟法の改正」法とコンピュ-タ 23 号 53～62 頁 (2005)、石井夏生利「情報セキュリティ監査人の責任」九州国際大学法学論集 14 巻 3 号 264～235 頁 (2008)、石崎靖敏「セキュリティとプライバシのバランスーEU のデータ保持指令をめぐる議論－」信学技報 106 巻 174 号 51～58 頁 (2006)、松尾浩也「最近の刑事立法」日本學士院紀要 68 巻 2 号 181～195 頁 (2014)及び黒澤睦「ドイツの刑事立法政策の一動向」罪と罰 53 巻 4 号 45～50 頁を参考にした。

外国語の書籍としては、Sarah Summers, Christian Schwarzenegger, Gian Ege & Finlay Young, The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society, Hart Publishing (2014)、Klaus Malek & Andreas Popp, Strafsachen im Internet (2. Auflage), C.F. Müller (2015)、Dieter Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, C.H. Beck (2015)、Müller-Brockhausen, Haftung für den Missbrauch von Zugangsdaten im Internet, Nomos (2014)、Yvonne Jewkes (Ed.), Crime Online, William Publishing (2007)、Theo Tryfonas (Ed.), Human Aspects of Information Security, Privacy, and Trust: 4th International Conference, HAS 2016 Held as of HCI International 2016 Toronto, ON, Canada, July 17-22, 2016 Proceeding, Springer (2016)、Tom Chen, Lee Jarvis & Stuart Macdonald (Eds.), Cyberterrorism: Understanding, Assessment, and Response, Springer (2016)、Jonathan Clough, Principles of Cybercrime 2nd edition, Cambridge University Press (2015)、Magid Yar, Cybercrime and Society 2nd Edition, SAGE (2013)、Jörg Eisele, Computer- und Medienstrafrecht, C.H. Beck (2013)、Gerald L. Kovacich & Andy Jones, Klaus Malek & Andreas Popp, Strafsachen im Internet (2 Auflage), C.F. Müller (2015)、Seymour Goodman, Detmar W. Straub & Richard Baskerville, Information Security: Policy, Processes, and Practices, Routledge (2016)、Thomas K. Clancy, Cyber Crime and Digital Evidence: Materials and Cases (Second Edition), LexisNexis (2014)、John Aycock, Spyware and Adware, Springer (2010)、High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program,

Butterworth-Heinemann (2006)、Orin S. Kerr, Computer Crime Law, Thomson/West (2006)、Hans-Jürgen Lange & Astrid Bötticher (Hrsg.), Cyber-Sicherheit, Springer (2014)、Stein Schjolberg, The History of Cybercrime 1976-2014, Books On Demand (2014)、Jan Baumann, Besitz an Daten, § 184b Abs. 4 StGB im Lichte neuer Medien, Duncker & Humblot (2015)、Helmut Reimer, Norbert Pohlmann & Wolfgang Schneider (Eds.), ISSE 2015: Highlights of the Information Security Solutions Europe 2015 Conference, Springer (2015)、Edward R. Miller-Jones (Ed.), The Threat of Malware: Hijacking Computers, Fastbook publishing (2012)、Wallace Wang, Steal This Computer Book 4.0: What They Won't Tell You About the Internet, no starch press (2006)、Robert F. Smallwood, Safeguarding Critical e-Documents: Implementing a Program for Securing Confidential Information Assets Hardcover, Wiley (2012)、Park Foreman, Vulnerability Management, CRC Press (2010)、Ian Walden, Computer Crimes and Investigation, Oxford University Press (2007)、Max M. Houck (Ed.), Forensic Biology, Academic Press (2015)、Susanne Beck, Bernd-dieter Meier & Carsten Momsen (Hrsg.), Cybercrime und Cyberinvestigations: Neue Herausforderungen Der Digitalisierung fur Strafrecht, Strafprozessrecht und Kriminologie, Nomos (2015)、Sherri Davidoff & Jonathan Ham, Network Forensics: Tracking Hackers through Cyberspace, Prentice Hall (2012)、Mark F. Grady & Francesco Parisi (Eds.), The Law and Economics of Cybersecurity, Cambridge University Press (2005)、Sushil Jajodia, V.S. Subrahmanian, Vipin Swarup & Cliff Wang (Eds.), Cyber Deception: Building the Scientific Foundation, Springer (2016)、S.R. Sharma, Encyclopaedia of Cyber Laws and Crime, Anmol Publishing (2000)、Wolfgang Bär, Der Zugriff auf Computerdaten im Strafverfahren, Carl Heymanns Verlag (1991)、Donn B. Parker, Crime by Computer, Charles Scribner's Sons (1976)及び Jiafu Wan, Iztok Humar & Daqiang Zhang (Eds.), Industrial IoT Technologies and Applications: International Conference, Industrial IoT 2016, GuangZhou, China, March 25-26, 2016, Revised Selected Papers, Springer (2016) を参考にした。

外国語の論説・資料等としては、ITU, Understanding cybercrime: Phenomena, challenges and legal response (September 2012)、Mike McGuire & Samantha Dowling, Cyber crime: A review of the evidence Chapter 1: Cyber-dependent crimes (Home Office Research Report 75), UK Home Office (October 2013)、House of Commons Science and Technology Committee, Malware and cyber crime (Twelfth Report of Session 2010–12)、United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (draft - February 2013)、Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society (1998)、Ben Hayes, Julien Jeandesboz, Francesco Ragazzi, Stephanie Simon & Valsamis Mitsilegas, The law enforcement challenges of cybercrime: are we really playing catch-up?, European Union (Brussels, 2015)、Xingan Li, International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene, Webology Volume 4, Number 3 (September, 2007)、Abraham D. Sofaer, Seymour E. Goodman, Mariano-Florentino Cuéllar, Ekaterina A. Drozdova, David D. Elliott, Gregory D. Grove, Stephen J. Lukasik, Tonya L. Putnam & George D. Wilson, A Proposal for an International Convention on Cyber Crime and Terrorism, Stanford University Center for International Security and Cooperation (August 2000)、David Simms & Solange Ghernaouti, A Report on taxonomy and evaluation of existing inventories, eCrime Project (30 November 2014)、Congressional Research Service, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws (October 15, 2014)、Europol, The Internet Organised Crime Threat Assessment (2015)、Howard Rush, Chris Smith, Erika Kraemer-Mbula and Puay Tang, Crime

online: Cybercrime and illegal innovation, University of Brighton (July 2009)、Stein Schjolberg, The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva (December, 2008)、Amalie M. Weber, The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal Volume 18 Issue 1 pp.425-446 (2003)、Dane Bryce Weber, The Cybernetic Sea: Australia's Approach to the Wave of Cybercrime, Queensland University of Technology Law Review Volume 14 Number 2 pp.52-73 (2014)、Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, New York University Law Review vol.78 no.5 pp.1596-1668 (2003)、Niloufer Selvadurai, Md. Rizwanul Islam & Peter Gillies, Unauthorised access to wireless local area networks: The limitations of the present Australian laws, Computer Law & Security Review vol.25 Issue 6 pp.536-542 (2009)、Armando A. Cottim, Cybercrime, Cyberterrorism and Jurisdiction: An Analysis Article 22 of the COE Convention, European Journal of Legal Studies vol.2 pp.55-79 (2010)、Rizal Rahman, Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application, Computer Law & Security Review vol.28 Issue 4 pp.403-415 (2012)、Peter Csonka, Council of Europe activities related to information technology, data protection and computer crime, Information & Communications Technology Law, vol.5 Issue 3 pp.177-196 (1996)、Antonela Gropeneanu & Adrian Tacob, Investigative issues regarding cybercrime, European Journal of Public Order and National Security vol.3 Issue 10 pp.7-12 (2016)、Elias M. Awad & Data Processing Management Association, Automatic Data Processing: Principles and Procedures 3rd. edition, Prentice-Hall (1973)、Kevin Vilbig, Hack All The History! Hackers 1959-1991, Portland State University: University Honors Theses. Paper 19. (10.15760/honors.20) (June 26, 2013)、M. Mitchell Waldrop, How to hack the hackers: The human side of cybercrime: As cyberattacks grow ever more sophisticated, those who defend against them are embracing behavioural science and economics to understand both the perpetrators and their victims, Nature vol.533 pp.164-167 (11 May 2016) 及び Pavel Biriukov, Criminal liability of legal persons in EU-countries, VSU Publishing House (2015)を参考にした。

＊＊＊

サイバー犯罪条約（ETS No.185）の説明書

I 条約及びその説明書は、欧州評議会閣僚委員会によって、その第 109 回総会（2001 年 11 月 23 日）の際に採択され、そして、条約は、2001 年 11 月 23 日、ブタペストにおいて、サイバー犯罪に関する国際会議の議題として、署名のために開放された。
II この説明書にある文章は、条約に定める条項の適用を促進するという性質を有するものではあるが、条約の公式の注釈を提供する文書となるものではない。

I. 序文

1. 情報技術における革命は、社会を根本的に変化させてきたし、また、予見可能な将来においてもそのようであり続けることであろう。多数の仕事がより処理しやすいものとなった。当初は、社会の幾つかの特別の分野だけで情報技術の支援を伴う業務手順が認められていた。しかし、現在では、社会の中でその影響をまだ受けていない分野を見つけることが難しくなっている。情報技術は、程度の差こそあれ、人間のほぼ全ての活動の場面に浸透してしまっている。
2. 情報技術の際立った特徴は、それが通信技術の発展に影響を与えてきたこと、そして、今後も与えるであろうということにある。人間の音声の伝送を含め、古典的な電話は、音声、文章、音楽並びに静止画及び動画から成る膨大な量のデータ交換によって取って代わられてしまっている。このデータ交換は、今や、人間と人間の間においてのみ起きているのではなく、人間とコンピュータとの間そしてコンピュータとコンピュータの間においても起きている。交換機による接続は、パケット交換ネットワークによって置き換えられた。直接の接続を確立することができるかどうかは、もはや関係のないことである。すなわち、データが受信者のアドレス宛にネットワークに入るだけ、または、データにアクセスすることを望む誰かのために利用可能なものとされることだけで十分なのである。
3. 電子メールの利用及び無数の Web サイトへのインターネットを介したアクセスの普及は、そのような発展の一例である。これらは、我々の社会を根本的に変化させた。
4. コンピュータシステム内にある情報にアクセスできること及びこれを検索できることの容易性は、地理的な距離とは無関係に、データを交換し流通することについて事実上無制限の可能性があることとも相まって、利用可能な情報及びそこから引き出され得る知識の分量の爆発的な増大を導いてきた。
5. このような発展は、かつてない経済的な変化及び社会的な変化を生じさせているのであるが、それらは闇の側面も持っている。すなわち、新たなタイプの犯罪が出現し、そして、新たな技術という手段を用いて在来型の犯罪が実行されている。更に、犯罪行為の結果が以前よりもずっと遠くの場所まで及ぶようになった。それは、そのような犯罪が地理的な限界や国境によって制約されることがないからである。世界規模での近年の有害なコンピュータウイルスの感染拡大は、このような現実の事実を証明している。犯罪行為を防止し検知するための法的な措置に付随するものとして、コンピュータシステムを防護するための技術的な措

置が実装されるべき必要性がある。
6. 新たな技術は、既存の法理論に対しても課題をつきつけている。情報と通信の流れは、世界中で、より容易なものとなっている。国境は、もはやその流れを遮る境界線ではない。犯罪者らは、その犯罪者の行為によって結果が生じる場所とは異なるところに所在するようになってきている。しかしながら、一般に、国内法は、特定の領土に限定して適用される。そして、直面する問題に対する解決は、国際法によって対処されなければならない。それは、適切な国際的法律文書を必要とする。この条約の目的は、新たな情報社会における人権を十分に尊重した上で、このような変化に対応することにある。

II. 起草作業

7. 1996 年 11 月、犯罪問題に関する欧州委員会（CDPC）は、CDPC/103/211196 により、サイバー犯罪を取扱う専門家の委員会を設置することを決定した。CDPC は、以下のような論拠により、その決定を根拠づけた：
8. 「情報技術の急速な発展は、現代社会の全ての分野に対して直接に及んでいる。通信と情報システムの統合は、距離の隔たりとは無関係に、全ての種類の通信の記録保存及び転送を可能にするものであり、全ての範囲での新たな可能性を拓いている。このような発展は、インターネットを含め、情報スーパーハイウェイ[1]及びネットワークの出現によって加速された。それによって、事実上、全ての者が、彼が世界の中のどこに所在しているかとは無関係に、全ての電子情報サービスに対してアクセスできるようになる。通信サービス及び情報サービスと接続することによって、利用者は、『サイバースペース[2]』と呼ばれるある種の共通空間を創り出す。それは、適法な目的のために用いられるものであるが、濫用の対象ともなり得るものである。この『サイバースペースの侵害行為』は、コンピュータシステム及び通信網の完全性、可用性及び機密性に対して実行されるものであると同時に、在来型の侵害行為を実行するためにそのようなサービスのネットワークを利用することによって構成される侵害行為でもある。例えば、インターネットを介して実行される場合のような侵害行為の国境を越える性質は、自国の法執行機関[3]の権限が領土内に限られていることと矛盾している[4]。
9. それゆえ、刑事法は、これらの技術的な発展を直視しなければならない。それは、サイバースペースという場の高度に洗練された濫用の機会を提供し、そして、正当な利益に対する損害を生じさせるものである。情報ネットワークの国境を越える性質に鑑み、そのような濫用を取扱うための協調した国際的な努力が必要である。勧告 No. (89) 9 は、一定のコンピュ

[1] [訳注] 当時の状況を理解するためには、アルバート・ジュニア・ゴア（門馬淳子訳）『情報スーパーハイウェイ』（電通、1994）、Legal Research Network, Rules of the road for the information superhighway: Electronic communications and the law, West Publishing (1996)及び Mark Anstey, A Nation of Opportunity: Realizing the Promise of the Information Superhighway, Diane Publishing (1996)が参考になる。
[2] [訳注] Lawrence Lessig, The Law of the Horse: What Cyberlaw might teach, Harvard Law Review vol.113 pp.501-546 (1999) 参照
[3] [訳注] 捜査機関（警察・検察）及び法務当局のことを意味する。
[4] [訳注] インターネット上で生ずる法的問題に伴う準拠法及び国際的裁判管轄権の問題に関しては、Chris Reed, Internet Law: Text and Materials 2nd Edition, Cambridge University Press (2004) が参考になる。

ータの濫用形態に関する各国の理解を近似させることを結論づける一方で、この新たな現象に対する闘いにおいては、拘束力のある国際的文書のみが必要とされる有効性を確保し得るものだと結論づけている。そのような文書という枠組みの中で、国際的な協力という措置に加え、実体法上の課題及び手続法上の課題並びに情報技術の利用と密接に関係する事柄について定められなければならない」。

10. 加えて、CDPC は、その要請により H.W.K Kaspersen 教授が準備した報告書を考慮に入れた。その報告書は、「…条約のような、勧告よりも強い拘束力のある他の法律文書に着目すべきある。そのような条約は、刑事実体法上の事柄のみならず、刑事手続法上の課題並びに国際的な手続及び協定も扱うものとすべきである」[1]と結論づけている。同様の結論は、実体法との関係では、勧告 No. R (89) 9[2]に添付された報告書によって、そして、情報技術と関連する手続法上の課題との関係では、勧告 No. R (95) 13[3]によっても既に示されていた。

11. 新たな委員会の特別の設置目的は、以下のとおりであった：

i.「コンピュータと関連する犯罪に関する勧告 No. R (89) 9 及び情報技術と関係する刑事訴訟法上の課題に関する勧告 No. R (95) 13 に照らし、とりわけ、以下の事項について検討すべし：

ii. サイバースペースの侵害行為、とりわけ、通信ネットワーク（例：インターネット）の利用を介して実行される侵害行為、例えば、違法な資金移動、違法なサービスの提供、著作権の侵害、並びに、人間の尊厳及び未成年者の保護に対する侵害行為；

iii. 国際的な協力のために共通の手法が必要となり得る場合には、インターネットサービスプロバイダを含め、サイバースペースの中で行動する者の定義、制裁及び責任といったような、それ以外[4]の実体刑事法上の課題；

iv. 国境を越える利用を含め、技術的な環境における強制権限（例：通信の傍受）の利用及び適用可能性、情報ネットワーク（例：インターネット）の電子的な監視、情報処理システム（インターネット上のサイトを含む。）の捜索及び押収、情報セキュリティ上の特別の措置（例：暗号化）によって生じ得る問題を考慮に入れた上で、違法な物に対するアクセスをすることができないようにすること、並びに、サービス提供者に対して、特別の義務に服するように要求すること；

v. 複数の管轄権がある場合の競合[5]の問題を含め、情報技術の侵害行為と関連する管轄権の問題（例：侵害行為が実行された場所（不法行為地[6]）及び適用されるべき法律を決定すること）、並びに、積極的管轄権の抵触をいかに解決するか、及び、消極的管轄権の抵触をいかに回避するかという問題；

---

[1] Implementation of Recommendation No. R (89) 9 on computer-related crime, Report prepared by Professor Dr. H.W.K. Kaspersen (doc. CDPC (97) 5 and PC-CY (97) 5, page 106).

[2] Computer-related crime, Report by the European Committee on Crime Problems, page 86 参照

[3] Problems of criminal procedural law connected with information technology, Recommendation No. R (95) 13, principle no. 17 参照

[4] [訳注] 「それ以外（other）」とは、(i)の通信ネットワークの利用を介して実行される侵害行為以外の実体法上の課題であることを指す。

[5] [訳注] 原文は、「ne bis idem」となっている。

[6] [訳注] 原文は、「locus delicti」となっている。

vi. 刑事分野における欧州諸条約の運営に関する専門家会議（PC-OC）と密接に協力して行われるサイバースペースの侵害行為の場合の国際的な捜査協力の問題。

委員会は、国際的な問題を特に重視して、可能な限り、i ないし v に関する拘束力のある法律文書を起草しなければならず、かつ、それが適切なときは、特定の課題に関する勧告を付さなければならない。委員会は、技術の発展に照らし、その他の課題に関して示唆することができる」。

12. CDPC の決定とは別に、閣僚委員会は、第 583 回閣僚代理会合（1997 年 2 月 4 日開催）の際になされた決議 no. CM/Del/Dec (97) 583 によって、「サイバースペースにおける犯罪に関する専門家委員会（PC-CY）」と呼ばれる新たな委員会を設置した。PC-CY 委員会は、1997 年 4 月に作業を開始し、サイバー犯罪に関する国際条約草案について交渉作業に従事した。その当初の期限として、委員会は、1999 年 12 月 31 日までにその作業を終えるものとされていた。この日までに委員会が条約草案中の幾つかの問題についてその交渉[1]を完全に終えている状態にはなかったため、閣僚代理会議の決議 no. CM/Del/Dec (99) 679 により、その期限は、2000 年 12 月 31 日まで延長された。欧州法務閣僚会議は、この交渉に関し、2 度にわたり支持を表明した。すなわち、その第 21 回会合（プラハ、1997 年 6 月）の際に採択された決議第 1 号は、各国の刑事法の条項を相互に近似するようなものとし、かつ、サイバー犯罪のような侵害行為に関する捜査の効果的な手段[2]を用いることができるようにするため、閣僚委員会に対し、サイバー犯罪に関して CDPC によって行われている作業を支援するように勧告した。また、欧州法務閣僚会議の第 23 回会合（ロンドン、2000 年 7 月）で採択された決議第 3 号は、可能な限り多くの構成国が条約の加盟国となることができるようにするための適切な妥結を得るという観点から、交渉相手となる関係国がその努力を尽くすべきことを勧奨し、そして、サイバー犯罪に対して闘うべき特別の必要性があることを正確に認識し、迅速で効果的な国際的な協力の制度の必要性を認めた。欧州連合の構成国は、1999 年 5 月に採択された共同意見書によって、PC-CY の作業を支援する旨を表明した。

13. 1997 年 4 月から 2000 年 12 月までの間、PC-CY 委員会は、本会議を 10 回開催し、また、そのオープンエンド型の起草グループ会合を 15 回開催した。期限が経過した後、CDPC の後援の下に、専門家らは、説明用覚書の草案を完成するために 3 回以上の会合を開催し、議員会議の意見書に照らして条約草案を検討した。議員総会は、2000 年 10 月、閣僚委員会から条約草案に関する意見書を提出するよう要請を受けた。草案は、2001 年 4 月、本会議の第 2 部の会期に採択された。

14. その後、PC-CY 委員会によって決定がなされ、初期のバージョンの条約草案が機密解除となり、2000 年 4 月に公開された。交渉をする構成国と全ての関係国が協議をすることがで

[1] [訳注] 条約草案の起草過程では、将来の加盟予定国や関連する国際組織等との間で交渉が重ねられた。この交渉は、条約の草案が署名のために公開される日にはその内容について基本的な了承が得られており、速やかに加盟手続が行われるようにするためのものであった。しかし、各国の法制（特に手続法）や判例法に相違があり、また、当時における情報技術の導入・普及の程度もまちまちであったため、その交渉は必ずしも容易なことではなかった。

[2] [訳注] データの保全などサイバー犯罪条約により導入された新たな刑事訴訟法上の証拠収集方法等のことを指す。

きるようにするため、全ての総会の後に、その後の草案が公表された。
15. 修正され確定された条約草案及びその説明用覚書は、2001 年 6 月、CDPC の第 50 回本会議の際に、承認のために送付された。その後、採択及び署名のための開放のために、条約草案の文面が閣僚委員会に対して送付された。

III. 条約

16. 条約の目的は、基本的に、(1)侵害行為の国内法上の刑事実体法の要件及びサイバー犯罪の領域における関係法令の整合性をとること、(2)そのような侵害行為並びにコンピュータシステムによって実行された他の侵害行為の捜査及び訴追のために必要となる国内法上の刑事手続法の権限またはそれらと関連する電子的な方式の証拠について定めること、そして、(3)迅速かつ効果的な国際的な協力体制を構築することである。
17. 条約は、順に、4 つの章を含んでいる。すなわち、(I)用語の使用、(II)国内法のレベルで講じられるべき措置－実体法及び手続法、(III)国際的な協力、(IV)最終条項である。
18. 第 2 章の第 1 節（実体法上の課題）は、犯罪行為に関する条項及びコンピュータ犯罪またはコンピュータと関連する犯罪に関するその他の条項と関係するものである。この部分では、最初に、4 つの異なる範疇に分類された 9 つの侵害行為について定義し、付随的な責任及び制裁を扱っている。この条約において定義されるのは、以下の侵害行為である。すなわち、違法なアクセス、違法な傍受、データの妨害、システムの妨害、機器の濫用、コンピュータと関連する偽造、コンピュータと関連する詐欺、児童ポルノに関連する侵害行為、そして、著作権及び関連諸権利と関連する侵害行為である。
19. 第 2 章の第 2 節（手続法上の課題）は、コンピュータシステムという手段を用いて実行される全ての侵害行為または電子的な方式による証拠に適用されるので、第 2 章の第 1 節において定義される侵害行為よりも広い適用範囲を有するものであるが、最初に、この章における手続法上の権限の全てについて適用される一般的な要件及び安全性確保措置を定める。続いて、以下に挙げる手続法上の権限について定める。すなわち、記録保存されたデータの応急の保全、トラフィックデータの応急の保全及び部分開示、提出命令、コンピュータデータの捜索及び押収、トラフィックデータのリアルタイム収集、コンテントデータの傍受である。第 2 章は、管轄権の条項で締めくくっている。
20. 第 3 章は、在来型の共助及びコンピュータ犯罪と関連する共助並びに犯罪者引渡に関する条項を含んでいる。それは、2 つの状況における在来型の共助と関係している。すなわち、法的根拠（協定、互恵的な法律等）が加盟国間に存在しない場合（この場合、本章の条項が適用される。）、及び、そのような法的根拠が存在する場合（この場合、既存の協定もまたこの条約に基づく援助に適用される。）である。コンピュータ犯罪またはコンピュータと関連する犯罪における特定の援助は、どちらの状況に対しても適用され、そして、特別の条件に従い、第 2 章中で定義されるのと同じ範囲での手続法上の権限が適用される。加えて、第 3 章には、共助を必要とせず（同意に基づいて入手しまたは公衆が利用可能な）記録保存されたコンピュータデータに対する特定のタイプの国境を越えたアクセスに関する条項、そして、加盟国間での迅速な援助を確保するための 24/7 ネットワークの設置に関する条項が含まれ

ている。
21. 最後に、第 4 章は、最終条項を含んでいる。それは、一定の例外条項と共に、欧州評議会の諸条約にある標準的な条項を繰り返している。

条約の各条項の注釈

第 1 章　用語の使用[1]

第 1 条の定義の序

22. 起草者の理解によれば、加盟国は、この条約によって、第 1 条に定義する 4 つの概念を加盟国の国内法の中に逐語的に複製すべき義務を負わない。ただし、加盟国の国内法は、この条約の基本原則と一貫性のとれた方法でそれらの概念を採用しており、かつ、国内法の実装のために均等な枠組みを示していることを要する。

第 1 条(a) コンピュータシステム

23. 条約におけるコンピュータシステムは、デジタルデータの自動的な処理のために開発されたハードウェア及びソフトウェアによって構成される装置である[2]。それは、入力、出力及び記録保存の機能を含むことができる。それは、スタンドアロンのものであり得るし、他の類似する装置とネットワークで接続されたものであり得る[3]。「自動的」は、直接的な人間の

[1] [訳注] 説明用覚書草案（draft Explanatory Memorandum）の段階では、この部分には標題だけがあり、その内容は何も記載されていなかった。

[2] [訳注] 今日においては、自然言語処理を含め、人工知能技術の高度な応用により、デジタルデータを自動処理する装置に限定する意味はほとんどなくなっている。むしろ、人間と機械装置との間で切れ目なく連続するサイバネティクスの一種として理解するのが妥当である。人間と機械装置は、等しくサイバネティクスであるが、それを区別する基準は、物理的な機能や存在形態にあるのではなく、法という社会規範である。すなわち、社会規範において権利主体となり得る存在を人間に限定していることにより、権利主体とはならないサイバネティクスと区別され得ることになる。しかし、近未来においては、その区別も曖昧になってしまうことが必至である。それゆえ、法哲学全体が根本から再構築されなければならない局面を迎えているというのが正しい表現ではないかと考えられる。このことは、人工知能技術を応用したネットワーク型の自律的ロボットやネットワーク全体を構成要素とする多細胞生物的な人工知能システムなどを想定してみると容易に理解することができる。そこでは、私見における処理主義が貫徹され、意思主義の理論はほとんど何の意味ももたない。その結果、人間だけが権利主体となるという理論的根拠も希薄なものとなる。
　なお、サイバネティクスを基礎とする法体系については、夏井高人「サイバー犯罪の研究（九・完）－補遺・最近の法改正と裁判事例－」法律論叢 89 巻 1 号で述べた。

[3] [訳注] 原文にはないが、文脈から、この部分に「.（ピリオド）」があるものとして訳した。誤記の一種と考えられる。

関与がないことを意味し[1]、また、「データの処理」は、コンピュータプログラムの実行によってコンピュータシステムの中でデータが操作されることを意味する。「コンピュータプログラム」は、意図された結果を得るためにコンピュータによって実行され得る一群の命令のことを意味する[2]。コンピュータは、異なるプログラムを実行することができる。通常、コンピュータシステムは、プロセッサまたは中央処理装置と周辺機器として区別される異なる装置によって構成される[3]。「周辺機器」は、プリンタ、ビデオスクリーン[4]、CD の読み書き装置その他の記録装置のように、処理装置とその相互作用によって一定の特別な機能を遂行する装置である。

24. ネットワークは、2 以上のコンピュータシステムの相互接続である[5]。接続は、物理的な

---

[1] [訳注] この定義は、古典的なコンピュータシステムには適用可能であるが、現在の人工知能型のコンピュータシステムには適用することができない。仮に適用するとすれば、人工知能型のシステムは、「コンピュータシステム」に該当しないということになるであろう。なぜならば、人工知能型のシステムは、ルールを自律的に生成、直接的にも間接的にも人間の関与を受けることなく処理を行うことができるからである。ISO の定義における産業用ロボットとは異なり、自律的な人工知能型コンピュータシステムは、その全部または一部について、人間による制御の範囲外にある存在である。

[2] [訳注] 自律的に学習し、ルールを自動生成する人工知能型のシステムでは、人間によって意図または予定された処理が実行されるか否かを予め決定することができない。

[3] [訳注] この定義も古典的なものである。特にデータ駆動型のシステムや真のニューロコンピュータシステムでは、生体である人間の脳神経細胞に相当する多数の回路の集積として存在することが想定されているので、中央処理装置（CPU）とそれ以外の装置を区別することに特段の意味を見出すことができない。コンピュータプログラムとプログラムによって処理される対象であるコンピュータデータとを明確に区別し、それらが処理される装置全体を指すコンピュータシステムとも区別するという古典的な定義は、フォン・ノイマンやチューリングの数理モデルを基礎として構築されているので、現時点で開発されている人工知能型コンピュータの主流で採用されつつあるような別の系に属するシステムにおいては定義としての妥当性をもたない。特に、データ駆動型の人工知能システムや有機体ロボットでは、そうである。このような場合、古典的な意味での「制御」は、成立の前提を欠くことになる。なお、これらの点に関しては、Committee on Legal Affairs, Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))が参考になる。

[4] [訳注] 画像表示装置一般のことを指し、テレビ受像装置型やゴーグル型のものを含め、ディスプレイ装置、画像投影装置、立体映像生成装置等の全てを含む趣旨と解される。現時点では、視覚だけではなく聴覚や触覚に訴える信号を統合的に処理する装置が増えており、近未来においては、人間の生体脳に信号を直接に伝達するようなタイプのものが増えるものと予想される。その段階に至ると、装置または装置から発せされる信号と人間の感覚・意識との間に明瞭な仕切りがなくなってしまうことに留意しなければならない。

[5] [訳注] この定義は、装置としてのコンピュータシステムのみを前提としている。現在の IoT（Internet of Things）の環境の延長上では、機械装置と生体である人間やその他の生物との直接の相互接続を実現する時代に入ることが予想されるが、その場合には、現在の刑事法の基本概念をそのまま適用することができない（前掲「サイバー犯罪の研究（九・完）－補遺・最近の法改正と裁判事例－」143～198 頁参照）。古典的な法哲学の世界とはメタルールのレイヤにおいて全く異なっているからである。しかし、そのような生物と無生物とを区別しないサイバネティクスの時代に適合した法哲学及びそれに基づいた基本的な法理念を新たに構築する必要がある。これらの点に関しては、夏井高人「アシモフの原則の終焉－ロボット法の可能性－」法律論叢 89 巻 4・5 号掲載予定で述べた。

結合[1]（例：電線もしくは光ケーブル）、無線（例：電波、赤外線もしくは衛星通信）またはその両方であり得る。ネットワークは、地理的に狭い範囲に限定されることがあり得るし（ローカルエリアネットワーク）、あるいは、広い領域に拡張されることもあり得る（ワイドエリアネットワーク）。そして、それらのネットワークは、相互接続され得る。インターネットは、多数の相互接続されたネットワークによって構成され、全て同じプロトコルによって利用することができるグローバルなネットワークである。インターネットに接続されていると否とを問わず、コンピュータシステム内においてコンピュータデータを通信することのできる他のタイプのネットワークが存在する。コンピュータシステムは、終端としてネットワークに接続されることもあるし、また、ネットワーク上の通信を支援する手段として接続されることもある。重要な点は、ネットワーク上でデータが交換されるということである[2]。

第 1 条(b) コンピュータデータ

25. コンピュータデータの定義は、ISO のデータの定義[3]に基づいて構成されている。この定義は、「処理に適する」という語を含んでいる。これは、データがコンピュータシステムによって直接に処理され得るような方式になっているということを意味する[4]。この条約においては、データを電子的な方式によるデータその他の直接に処理され得る方式のデータとして理解されるべきであるということを明確なものとするために、「コンピュータデータ」の概念が導入される。自動的に処理されるコンピュータデータは、この条約で定義されている犯罪行為中の 1 つの標的となり得るもの[5]であると同時に、この条約によって定義される捜査手段中の 1 つの適用の対象となるもの[6]である。

---

[1] [訳注] 原文は、「earthbound」となっている。意訳した。

[2] [訳注] ネットワークシステムの本質が「データの交換」にあり、ネットワークシステムを構成する機器の相違や設計・仕様等はそのための手段に過ぎないという意味で本質的な部分ではないとの認識を示すものと解される。しかし、ネットワーク型の人工知能の世界では、センサーが単純にセンサーであるわけではなく、比喩的に言えば生体脳における個々のシナプスと同様の機能を有するようになることがあり得る。ここでも、ネットワークとデータとを明確に区別することがあまり意味をもたなくなってしまうと考えられる。そのことから、この説明文で示されているような理解は、人工知能技術の応用を基本とする世代のネットワークシステムにそのまま適用することができない。

[3] [訳注] ISO/IEC 2382 は、コンピュータデータについて、「reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing」と定義している。日本工業規格（JIS X 0001）では、「情報の表現であって、伝達、解釈または処理に適するように形式化され、再度情報として解釈できるもの」と定義している。ISO の定義を私的に意訳してみると、「通信、解釈または処理のために適するように様式化された情報の表現であって、元の情報へと戻して解釈することができるもの」となる。

[4] [訳注] 日本国の刑法第 7 条の 2 は、「電磁的記録」の定義として、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう」と定めている。

[5] [訳注] 第 4 条のことを指すと解される。

[6] [訳注] 第 16 条及び第 17 条のことを指すと解される。

第 1 条(c) サービス提供者

26. 「サービス提供者[1]」という用語は、コンピュータシステム上のデータの通信または処理と関連する特別の役割を果たす広い範囲の者を包含している（第 2 条の注釈も参照）。この定義の(i)に基づき、利用者に対して相互に通信することができることを提供する公的な組織及び民間の組織の両方に関係するものであることが明確にされている。それゆえ、その利用者が非公開のグループを形成しているかどうか、提供者が公衆に対してそのサービスを提供しているかどうか、有料であるか無料であるかは、関係がない。非公開の利用者グループは、例えば、企業のネットワークからサービスの提供を受ける私企業の従業員であり得る。
27. 定義の(ii)に基づき、「サービス提供者」という用語は、(i)に示す者の代わりにデータを記録保存し、または、その他のデータ処理を行う公的組織または民間の組織にも拡張されることが明確にされている。更に、この用語は、(i)に示す提供者のサービスの利用者の代わりにデータを記録保存し、または、その他のデータ処理を行う公的な組織または民間の組織を含む。例えば、この定義に基づき、サービス提供者は、ホスティングを提供するサービス及びキャッシングのサービス、並びに、ネットワーク接続を提供するサービスのいずれをも含む。しかしながら、当該コンテントの提供者が通信サービスまたは関連するデータ処理サービスをも提供するものではない場合には、（ホスティング会社との間で彼の Web サイトをホストする契約を締結している者のような）単にコンテントを提供するプロバイダ[2]については、この定義の適用対象となるものではない[3]。

第 1 条(d) トラフィックデータ

28. この条約においては、第 1 条の(d)に基づいて定義されるトラフィックデータは、コンピュータデータの一種であって、特別の法制度が適用されるものである。このデータは、通信の連鎖の中で、通信をその発信地からその到達地まで経路設定するために、コンピュータによって生成されるものである。それゆえ、それは、通信それ自体を支援するものである。
29. コンピュータシステムと関係して実行された犯罪行為の捜査の場合、トラフィックデータは、別の証拠を収集するための出発点としての通信の発信地または侵害行為の証拠の一部

[1] [訳注] 原文は、「service provider」となっている。民間のインターネットサービスプロバイダ（ISP）のようなサービス提供者だけではなく行政機関を含む趣旨の用語であるので、この参考訳では、「サービス提供者」と訳すことにした。

[2] [訳注] クラウドコンピューティングサービスの利用者の場合には、単にコンテントを提供するだけの者と認定すべきかどうか不明瞭な場合があり得る。この問題は、個々のサービスの契約内容や当該サービスの基盤となっているクラウドシステムの仕様によって異なる要素が多々あるため、具体的な事案に応じて、個別的に判断されなければならない。

[3] [訳注] 当時、新たなサービスとして注目されていたものの 1 つにビデオテックス（Videotex）がある。オンデマンドにより文字情報と画像情報を組み合わせたコンテンツを提供することを主体とするサービスであり、インターネットが普及する以前においては、各国ともその開発・普及に力を入れていた。ビデオテックスに対する当時の認識や期待を理解することのできる資料として、OECD, New Telecommunications: Videotex Development Strategies (1988) がある。

としての通信の発信地を追跡するために必要である。トラフィックデータは、ほんの短時間だけ存続しており、その応急の保全を命ずる必要性を生じさせるものであり得る。その結果、それが削除される前に別の証拠を収集するため、または、容疑者を特定するため、通信経路を見極めるためには、トラフィックデータの迅速な開示が必要となるかもしれない。コンピュータデータの収集及び開示のための普通の手続は、それゆえ、不適切なものであり得る。更に、このデータの収集は、より機微なものと考えられる通信の内容を明らかにしないようなデータであるが故に、原則として、より侵害的ではないと考えられる。

30. 定義は、この条約中の特別な領域として扱われるトラフィックデータの類型について、余すことなく列挙している。すなわち、通信の発信地、その着信地、経路、時刻（GMT[1]）、日付、サイズ、持続時間及び基盤となっているサービスのタイプである。サービス提供者によってこれらの類型の全てが常に技術的に利用可能であり、処理可能なものであるとは限らず、また、特定の犯罪行為の捜査のために必要であるとは限らない[2]。「発信地」は、電話番号、IP アドレス、または、サービス提供者がサービスを提供する通信機能上のその他の類似の識別子のことを指す。「着信地」は、通信が伝送される通信機能上の対応する指図のことを指す。「基盤となっているサービスのタイプ」は、例えば、ファイル転送、電子メール、または、インスタントメッセージ[3]のような、ネットワーク内で用いられているサービスのタイプのことを指す。

31. 定義は、トラフィックデータの機微性の程度に応じてトラフィックデータの法的保護に相違を設けることができることについては、自国の立法者に任せている。この文脈において、第 15 条は、加盟国に対し、人権及び自由の保護のために適切な要件及び安全性確保措置を定めることを義務付けている[4]。このことは、就中、実体法の分野及び捜査機関に対して適用される手続がデータの機微性の相違に対応して様々なものであり得るということを意味している。

---

[1] [訳注] 現在の国際標準時（UT）と同じである。

[2] [訳注] データ保持指令 2006/24/EC に基づくデータ保持（data retention）の命令では、個々の捜査における特殊性を考慮しないで、包括的かつ事前にデータ保持の命令が発せられる点で、サイバー犯罪条約の第 16 条及び第 17 条に基づく応急の保全（data preservation）の命令とは異なっている。

[3] [訳注] オンラインチャットのようなサービスまたはそれを実行するためのソフトウェア（ツール、ガジェット）のことを指す。

[4] [訳注] この条約の手続条項に基づき捜査機関がトラフィックデータを入手する場合であっても、その入手したデータが捜査等の当該目的以外の目的のために利用されないように法的な保護がなされなければならないという趣旨である。この場合の法的保護のための安全性確保措置としては、例えば、当該データを当該担当者以外の者には解読できないような状態で暗号化して記録保存すること、あるいは、担当者に対して厳重な守秘義務を負わせ、その違反行為に対する刑事処罰を定め、当該データの管理者（サービス提供者など）または当該データのデータ主体を原告とする損害賠償請求についてその主張立証責任を軽減または転換することなどが考えられる。日本国においては、守秘義務違反の場合の罰則の強化や損害賠償請求の場合の主張立証責任の転換については、あまり重視されてこなかった。しかし、個人データ保護指令 95/46/EC 及び一般個人データ保護指令においては、そのような観点が重視されていることから、今後、日本国においても真剣に検討が尽くされるべきである。

第 2 章　自国のレベルで講じられるべき措置

32. 第 2 章（第 2 条ないし第 22 条）は、3 つの節を含んでいる。刑事実体法（第 2 条ないし第 13 条）、手続法（第 14 条ないし第 21 条）及び管轄権（第 22 条）である。

第 1 節　刑事実体法

33. 条約の第 1 節（第 2 条ないし第 13 条）の目的は、関連する侵害行為についてのミニマムの共通基準を設けることによって、コンピュータ犯罪またはコンピュータと関連する犯罪を防止または抑止するための手段を改善することである。この種の整合性をとることは、国内レベル及び国際的レベルでのそのような犯罪に対する闘いを容易なものとする。国内法において一貫性があれば、従前の低い基準をもつ加盟国へと侵害行為が移動することを防止することができる。その結果として、事件の実務的な処理上で有用な共通の経験の交換もまた、拡大されることとなり得る。例えば、双罰性の要求等に関して、国際的な協力（特に、引渡及び司法共助）が容易になる。
34. ここに含まれている侵害行為のリストは、ミニマムの合意事項を表すものであり、国内法における拡張を除外するものではない。このリストは、コンピュータと関連する犯罪に関する欧州評議会の勧告 No. R (89) 9 との関係で策定されたガイドライン[1]及び他の公的な国際機関及び民間の国際機関（OECD、国連、AIDP）の活動の中で策定されたガイドライン[2]に基づくところが非常に大きい。しかし、拡大し続けている通信ネットワークの濫用についてのより現代的な経験を考慮に入れている。
35. この節は、5 つの款に分かれている。第 1 款は、コンピュータと関連する犯罪の中核となる部分、すなわち、コンピュータデータ及びコンピュータシステムの機密性、完全性及び可用性に対する侵害行為を含んでいる。それは、コンピュータの安全性及びデータの安全性に関する議論の中で認識されているように、電子データの処理及び通信システムが直面している基本的な脅威を表現するものである。その見出しは、対象となる犯罪のタイプを示すものである。それは、システム、プログラムまたはデータに対する無権限アクセス行為及び不正な妨害行為である。第 2 款ないし第 4 款は、別のタイプの「コンピュータと関連する犯罪」を含んでいる。これらは、実務上、より大きな役割を果たすものであり、そして、在来型の手段を用いた攻撃に対しては既に刑法によってほとんどが保護されているような一定の法益に対する攻撃手段として、コンピュータシステム及び通信システムが用いられるものである。第 2 款の侵害行為（コンピュータと関連する偽造及びコンピュータと関連する詐欺）は、欧州評議会の勧告 No. R(89) 9 のガイドラインにおける提案に従って追加されたものである。

---

[1] [訳注] European Commission on Crime Problems, Computer-Related Crime: prefaced by August Bequai, Council of Europe Publishing and Documentation Service (Strasbourg, 1990) pp.33-69

[2] [訳注] OECD Guidelines for the Security of Information Systems (1992)、United Nations Manual on the prevention and control of computer-related crime (1994)、AIDP, the resolutions of the XVth International Congress 1994 in Rio de Janeiro, Section II, on computer crimes and other crimes against information technology (1994)

第 3 款は、コンピュータシステムを使用してなされる児童ポルノ[1]の違法な作成行為及び配布行為という「コンテンツと関連する犯罪」を、最近見られる最も危険な違法行為の 1 つとして定めている。この条約の起草委員会は、コンピュータシステムを介してなされる人種差別的なプロパガンダの配布行為のような、他のコンテンツと関連する犯罪を含めることができるかどうかについても検討した。しかしながら、委員会は、そのような行為の犯罪化について合意に達することができなかった。これを犯罪行為として含めることについてはかなりの支持があったが、何人かの参加者は、そのような条項を含めることに関して表現の自由に対する重大な懸念を示した。問題の複雑性に留意して、委員会は、欧州犯罪問題委員会（CDPC）に対してこの条約への追加議定書の策定開始を示唆するということで決着した[2]。

第 4 款は、「著作権及び関連諸権利の侵害と関連する犯罪」について定める[3]。これがこの条約に含まれることになった理由は、著作権の侵害が、最も広範囲に及ぶコンピュータ犯罪またはコンピュータと関連する犯罪の形態の 1 つになっており、その拡大が国際的に懸念されているためである。最後に、第 5 款は、企業の責任に関する最近の国際合意に対応して、未遂、幇助及び教唆、制裁及び措置に関する付随的な条項を含んでいる。

36. 実体法の条項は、情報技術を用いる侵害行為に関連しているが、この条約は、技術的に中立的な文言を用いる。これは、刑事実体法上の侵害行為の条項が、関連する現在の技術と将来の技術の両方について適用され得るようにするためである。

37. 条約の起草者は、第 2 条ないし第 10 条において定義された侵害行為の条項を実装するに際して、加盟国が軽微なまたは些細な違反行為を除外することができると理解している。

38. ここに含まれる行為が「権利なく」実行されることを明示で要するとしていることが、ここに含まれる侵害行為の特徴である。それは、示された行為が、それ自体としては必ずしも処罰の対象となるわけではなく、同意、正当防衛または緊急避難のような古典的な法律上の防御が適用される場合だけではなく、他の原則や利益ゆえに刑事的責任の除外につながるような場合においても、合法とされたり正当化されたりするかもしれないという考えを反映している[4]。「権利なく」という表現は、その表現が使われる文脈によって異なる意味が導き

---

[1] [訳注] 説明用覚書の仮訳では「児童ポルノグラフィ」と訳したが、現時点では「児童ポルノ」が日本語として定着しているので、従前の訳語を改めることにした。

[2] [訳注] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No.189)

[3] [訳注] 関連する指令として、Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society がある。

[4] [訳注] EU の個人データ保護法制においては、何らの法的根拠（legal basis）なくして個人データの処理がなされる場合には、その処理は、違法行為である。法的根拠としては、データ主体（本人）の同意、法律上の義務の履行等がある。個人データ処理においては、適法性の推定がない。それだけではなく、個人データ保護法令に違反して行われた行為により損害が発生した場合には、被告である管理者（事業者や行政機関）が「いかなる意味においても全く責任がないこと」を主張・立証しない限り、その違反行為に基づく損害賠償責任を免れることができない。これに対し、サイバー犯罪条約では、積極的に、「権利なく」行為が実行されたことを検察官が主張・立証しなければならないことになる。日本国の裁判所の通常の表現を用いて言い換えると、「法定の除外事由なく」当該行為が実行されたことが証拠によって証明されない限り、有罪とはならないということになる。この「法定の除外事由」の中には、法令に基づく行為である場合、正当防衛や緊急避難の場合等が含まれる。

出される。そして、加盟国がこの概念を国内法においてどのように導入するかを制限することなく、この概念は、（立法上、執行上, 行政上、司法上、契約上もしくは合意上のいずれであろうと）権限なく実行された行為、または、確立された法律上の防御、免責事由、正当化事由あるいは国内法の下において関連する原則によってカバーされない行為を指すものである。従って、この条約は、（例えば、加盟国政府が、公共の秩序を維持するため、国家の安全を防護するため、または、刑事犯罪を捜査するために行動する場合のように）政府の適法な権限の範囲内で行なわれた行為に対しては、何らの影響も及ぼさない。更に、ネットワークの設計において本来なされる適法で通常の活動、または、適法で通常の運用行為もしくは商業活動は、犯罪とされることがない。このような犯罪行為化の例外についての特定の例は、後述のとおり、説明用覚書[1]中で、特定の犯罪行為にそれぞれ対応する記述部分で提供される。（刑事法その他の法律に基づき）このような例外条項を加盟国の国内法制度の中でどのように実装するかについては、加盟国の判断に任されている。

39. 条約に含まれる全ての侵害行為について、刑事責任を負わせるためには、それが「意図的に」実行されたものでなければならない[2]。一定の場合においては、特定の意図という付加的な要件が、犯罪行為の一部分を構成している。例えば、コンピュータと関連する詐欺に関する第 8 条においては、経済的利益を得ようとする意図が、侵害を成立させるための構成要件要素となっている。条約の起草者は、「意図的に」という用語の正確な意味は、各国の解釈に任されるべきであると合意した。

40. この節の中の一定の条項では、この条約を国内法として実装する場合において、状況の限定を追加することを認めている。他の場合においては、留保の可能性さえも認められている（第 40 条及び第 42 条参照）。このように、犯罪行為化に関してより制限的な手法に関する方法が異なっているのは、そこに含まれる行動の危険性についての評価の相違、または、対抗手段として刑法を利用すべき必要性についての評価の相違を反映するものである。この手法は、政府と議会に対し、この領域における自国の刑事政策の決定に際し、柔軟性を与えている。

41. このような侵害行為を定める法律は、刑事的な制裁を帰結する行為のタイプを適切に予見することができるようにするために、可能な限り十分な明確性と特定性をもって起草されなければならない。

42. 起草の過程においては、起草者らは、いわゆるサイバースクワッティング（すなわち、既に存在しており、かつ、通常よく知られているドメイン名として識別されるドメイン名及び製品の商標もしくは会社の商号そして識別されるドメイン名を登録すること）を含め、第 2 条ないし第 11 条に定義するもの以外の行為を犯罪行為とすることを勧告することができるかどうかについて検討した。サイバースクワッティングをする者らは、そのドメイン名を実際に使用する意図がなく、かつ、関係する組織に対し、間接的にせよ、ドメイン名の保有権

[1] [訳注] 原文は、「Explanatory Memorandum」となっている。「Explanatory Report」と修正すべき部分の修正漏れと推定される。

[2] [訳注] 故意犯を原則とし、過失犯を含まないという趣旨である。これは、条約に基づいて犯罪行為とすべき行為類型に限定されるから、加盟国が自国の法令中において過失犯を処罰可能として法律を制定することは妨げられない。

の譲渡のために支払いを強いることによって、金銭的な利益を得ようとする。現時点においては、この行為は、商標権と関係する問題だと考えられる。商標権の侵害は、この条約によっては規律されないので、起草者らは、そのような行為を犯罪とすべきかどうかという問題を扱うことが適切であるとは考えなかった。

第 1 款　コンピュータデータ及びシステムの機密性、完全性及び可用性に対する侵害行為

43. 以下（第 2 条ないし第 6 条）に定義される犯罪行為は、コンピュータシステムまたはデータの機密性、完全性及び可用性を保護しようとするものであり、ネットワークの設計上当然になされる適法かつ普通の行為または適法かつ普通の運用行為もしくは商業活動を犯罪としようとするものではない。

違法なアクセス（第 2 条）

44. 「違法なアクセス」は、コンピュータシステム及びデータの安全性（すなわち、機密性、完全性及び可用性）に対する危険な脅威及び攻撃という基本的な侵害行為に適用される[1]。保護の必要性は、それらの者のシステムを妨害なく平常どおりに管理運用するという組織及び個人の利益を反映している。単なる無権限の侵入行為、すなわち、「ハッキング」、「クラッキング」または「コンピュータ侵入」は、原則として、それ自体として違法とされなければならない。それは、システム及びデータの正当な利用者に障害をもたらすものであり、そして、再構築のための高額の費用負担を伴う改変または破壊を発生させるかもしれない。このような侵入行為は、対価の支払いなく、システムを利用するための機密のデータ及び機密事項（パスワード、ターゲットとされたシステムに関する情報を含む）に対するアクセスを与えることになるかもしれないし、あるいは、ハッカーに対し、コンピュータと関連する詐欺

[1] [訳注] 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号・以下「不正アクセス禁止法」という。）の第 2 条第 4 項は、不正アクセス行為として、「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。）」（同条同項第 1 号）、「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よる特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その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の承諾を得てするものを除く。次号において同じ。）」（同条同項第 2 号）及び「電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為」（同条同項第 3 号）と定めている。そして、不正アクセス禁止法の第 3 条は、「何人も、不正アクセス行為をしてはならない」と定め、同法第 11 条は、「第 3 条の規定に違反した者は、3 年以下の懲役又は 100 万円以下の罰金に処する」と定めている。

またはコンピュータと関連する偽造のような更に危険な形態のコンピュータと関連する犯罪を実行するよう促すことになってしまうかもしれない。

45. 無権限アクセスを防止するための最も効果的な手段は、もちろん、効果的な防護手段を導入・開発することである。しかしながら、包括的な対応をするには、威嚇と刑法上の手段の利用を導入しなければならない。無権限アクセスを犯罪として禁止することは、早い段階での上記のような危険に対応する付加的なものとして、そのようなシステム及びデータに対する保護を与え得るものである。

46. 「アクセス」は、コンピュータシステム（ハードウェア、コンポーネント、インストールされたシステムの記録保存されたデータ、ディレクトリ、トラフィックデータ及びコンテントに関連するデータ）の全部または一部に入ること[1]を意味する。しかしながら、システムへの電子メールメッセージの単なる送信行為またはその記録行為は、含まれない[2]。アクセスは、公衆通信ネットワークを介して接続された他のコンピュータシステム、または、LAN（ローカルエリアネットワーク）のような同一のネットワーク上にある他のコンピュータシステム、あるいは、同一の組織内でのイントラネットに入ることを含む。（例えば、ワイヤレス・リンクを介したものや非公開のものを含め、遠距離からの）通信のための手段がどのようなものであるかは、問題とならない。

47. また、行為は、「権利なく」実行されるものであることを要する。この表現に関して上記に説明したところに加え、それは、システムの保有者またはその一部の保有者その他の権利者から承認を受けたアクセス（関係するコンピュータシステムについて、承認を受けて検査をする目的または防護の目的のためのような場合）を犯罪とすることはないということを意味する。

48. 例えば、直接になされる Web ページのアクセス、ディープリンキングを含むハイパーテキストリンクを通じてなされる Web ページのアクセス、または、通信のための情報の埋め込みもしくは検索をする「クッキー[3]」もしくは「ボット[4]」を利用することを通じてなされる

---

[1] [訳注] 原文は、「entering」となっている。システムの場合には「入ること」と訳すこともできるが、データの場合には「接近すること」が妥当と思われる。便宜、「入ること」と訳すことにした。

[2] [訳注] 説明書の第 190 項参照

[3] [訳注] 「クッキー（coolie）」は、個人データ保護との関係でも問題とされてきた。その詳細については、法と情報雑誌 1 巻 3 号に収録されている一般個人データ保護規則(EU) 2016/679 の該当する脚注及び参考文献を参照されたい。なお、Article 29 Working Party の報告書としては、Opinion 04/2012 on Cookie Consent Exemption (00879/12/EN) (Adopted on 7 June 2012) が公表されている。

[4] [訳注] 「ボット（bot）」とは、ソフトウェアの形態をとるロボット（robot）の一種を意味する。一般に、ロボット法の領域では、ISO の定義に基づく産業用ロボット（Robotics）のみを考察の対象としている。しかし、ロボット（Robot）の範疇は、かなり広く、人間を含む生物のような有機体で構成されているものやボットのようなソフトウェアで構成されているものも含まれる。ロボットの本来の概念は、サイバネティクス（Cybernetics）の概念及びオートマトン（Automaton）の概念と同じである。それゆえ、ロボットには、人間が制御することのできないものが多数含まれる。一般に、人間が制御することのできない対象については、法規範を適用して制御することもできない。例えば、人間は、法規範によって昆虫を制御することはできない。ソフトウェアの一種であるボットも同じであり、法規範による制御は不可能であるが、自己学習機能を有する人工知能型のボット等を除き、一般的には、プログラムによる制御は可能である。なお、第 1 条(a)の脚注参照。

Web ページのアクセスのような、特別の技術的ツールを使用すると、第 2 条のアクセスと同じ結果になるかもしれない。このようなツールの利用は、それ自体としては、「権利なく」なされるものではない。公開された Web サイト[1]を維持しているということは、そのサイトが他の Web ユーザからアクセスされてもよいというその Web サイトの保有者の同意を意味する[2]。通信プロトコル及び通信プログラムを通常通りに利用するための標準的なツールを用いることは、それ自体としては、「権利なく」なされるものではない。とりわけ、例えば、クッキーの最初のインストールが排除されなかった場合や、クッキーが削除されなかった場合のように、アクセスされるシステムの権利者が、それらのツールを用いることを承認したものと理解され得る場合[3]がそうである。

49. 多数の国内法には、既に、「ハッキング」という侵害行為に関する条項がある。しかし、その適用範囲及び構成要件は、かなり区々なものとなっている。第 2 条の最初の文において犯罪とすることについて緩やかな手法を採っていることについては、異論がなかった。単なる侵入行為に過ぎず何らの損害を発生させなかった場合、ハッキング行為がセキュリティシステムのループホールやシステムの発見を導いたのに過ぎない場合については、反対意見があった[4]。このことは、各国の状況に応じて、付加的な限定のための事項を要件とするという

---

[1] [訳注] 一般に、外部に公表されていない Web サイトやアクセス制御がなされている Web サイトは、公開の Web サイトではない。

[2] [訳注] Web サイトの保有者が、検索エンジンのための自動巡回ロボット（ボット）によるアクセスを拒絶するための技術的な仕組み（タグなど）を導入している場合には、その点に関しては同意していないことになる。

[3] [訳注] 一般に利用されているブラウザには、クッキーによる追跡を拒絶する機能や自動的に削除する機能が組み込まれており、その機能を利用している者は明示で拒絶の意思を表示していると理解すべきである。このような拒絶の設定をしているのにも拘らず、何らかの技術的な方法を用いてクッキーによる追跡を可能とする行為は、拒絶の意思に反して行動追跡をしていることになる。そのような行為が何らかのサイバー犯罪を構成するか否かについては見解が分かれると思われるが、少なくとも、EU の個人データ保護法制の下においては、データ主体の明示の意思に反して個人データを収集する行為すなわち違法行為として評価されることになるであろう。

[4] [訳注] この点に関しては、現在でも議論が続いている。特に、脆弱性要素を発見した場合に、それをどのような手続によりどのタイミングで公表すべきかについては、国際的な合意があり、日本国においても経済産業省の「ソフトウエア等脆弱性関連情報取扱基準」及びこれに基づく JPCIRT/CC の各種ガイドラインがあるものの、現在の国家によるサイバー攻撃（state sponsored Cyber attack）ないしサイバー戦（Cyberwar）というインターネット環境下では当該合意やガイドラインの存在意義それ自体がほとんど無意味なものとなってしまっているだけでなく、国家の諜報機関が積極的に脆弱性情報を利用して諜報活動を実施しているために、当該国の国家政策としての自己矛盾が存在していることとなる。そのため、これらの合意や基準・ガイドライン等は、基本的に無視されているのも同然の状態にある（そのような事実認識に基づかないでなされる政策決定は、全て完全に失敗することであろう。）。翻って考えてみると、短期的な経済的利益や収益の獲得・増加のみを重視し、十分に安全ではない製品やサービスを平然と提供する企業の姿勢にこそ根源的な問題があると言うべきである。完全な解決策はない。しかしながら、公共の安全を確保するためのより妥当で現実的な方法として、例えば、「OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security」に示されているような基本原理を情報関連製品やサービスの中に、バイデフォルト（by default）及びバイデザイン（by design）で組み込むことを必要条件とするような国家的な政策論の構築と実施が望まれる。

より狭い手法を導くことになった。これは、勧告 No. R (89) 9[1]及び OECD 作業部会の 1985 年の提案[2]によっても採用された手法でもある。

50. 加盟国は、第 2 条の最初の文に従い、より広い手法を採用して、単なるハッキング行為を犯罪とすることができる[3]。選択的なものとして、加盟国は、第 2 文に列挙する限定要件の全部または一部を採用することができる。すなわち、防護措置の侵害、コンピュータデータを入手する特別の意図、刑事犯罪として有罪とすることを正当なものとするその他の不誠実な意図、または、侵害行為が他のコンピュータシステムとリモートで接続されたコンピュータシステムと関連して実行されたこと、という要件である。最後のオプションによって、加盟国は、他のコンピュータシステムの使用と無関係なスタンドアロンのコンピュータへの物理的なアクセスの場合を排除することが認められる[4]。それらの国は、（通信サービスによって提供される公衆ネットワーク、イントラネットやエクストラネットのような私的なネットワークを含む）ネットワーク接続されたコンピュータシステムへの違法アクセスを侵害行為として禁止することができる[5]。

---

[1] [訳注] 原文は、「N° (89) 9」となっているが、誤記と解する。以下、同様の箇所について同じ。

[2] [訳注] OECD, Computer-Related Crime: Analysis of Legal Policy (1986)の 69 頁に示されている見解のことを指すと推定される。

[3] [訳注] 日本国の現行の不正アクセス禁止法は、営利の目的や損害の発生等の構成要件の充足を必要とせず、単純なハッキング行為を処罰するタイプの立法例に属する。このことは、犯罪行為の既遂時期及び罪数論に対しても影響を与える。関連する裁判例として、最高裁平成 19 年 8 月 8 日決定・刑集 61 巻 5 号 576 頁がある。同決定は、「不正アクセス行為の禁止等に関する法律 3 条所定の不正アクセス行為を手段として私電磁的記録不正作出の行為が行われた場合であっても、同法 8 条 1 号の罪と私電磁的記録不正作出罪とは、牽連犯の関係にはないと解するのが相当であるから、本件につき両者を併合罪の関係にあるものとして処断した原判断は相当である」と判示している。

[4] [訳注] 日本国の現行の不正アクセス禁止法は、電気通信回線に接続している電子計算機（特定電子計算機）に限定して適用されるので、この限定要件を採用していることになる。しかし、現在及び近未来の電子機器類の技術開発及び社会内での利用の状況に鑑みると、電気通信回線に接続していない電子計算機を適用対象から除外する合理的な根拠は全くないどころか、極めて危険な国家政策であると言える。早急の法改正が望まれる。例えば、電子計算機によって制御され完全に自律型の装置でありながら電気通信回線に接続されていない自律型の産業用ロボットを想定した場合、その産業用ロボットを制御している電子計算機へのアクセス制御を奪い、人間に対して危害を加える凶器として利用する行為については、現実に他の法益侵害の危険性が発生する前に、アクセス制御に対する攻撃の時点で不正アクセス行為として処罰対象とする必要があると考えられる。他方で、無線通信により遠隔操作可能な情報家電の類に属する家庭用ロボットの類は、産業用ロボットの一種であるから、事案により、不正アクセス禁止法所定の特定電子計算機の一種として理解することができ、それゆえ、不正アクセス罪の成立を認めることができる場合があり得る。

[5] [訳注] モノのインターネット（Internet of Things）の一部を構成するコンピュータシステムは、それが TCP/IP のプロトコルによって接続される通信システムである限り、インターネットに接続された機器類として理解することは可能である。ただし、その解釈を採用する場合であっても、既に述べたとおり、犯罪行為の実行の時点においてインターネットに接続された状態にあることを要し、犯罪行為の実行の時点でインターネットその他の通信回線に接続されていない機器類は特定電子計算機の該当性がないと解する。

違法な傍受（第 3 条）

51. 本条は、データ通信上のプライバシーの権利[1]の保護を目的としている。この侵害行為は、以前から存在する私人間の口頭の電話による通話の傍受及び記録と同様の通信上のプライバシーに対する侵害に相当する。通信上のプライバシーの権利は、欧州人権条約第 8 条に掲げられている。第 3 条により設けられる侵害行為は、電話、ファックス、電子メールまたはファイル転送の別を問わず、全ての形態の電子データの伝送に対して、この原則[2]を適用する。
52. 条項の条文は、主として、勧告 No. R (89) 9 に含まれている「無権限の傍受」という侵害行為から採られた。この条約の中で、通信には、「コンピュータデータの伝送」に関するものと並んで、以下に説明する状況の下で、電磁的な放射が含まれる、ということが明確にされた。
53. 「技術的な手段」による傍受は、通信内容の聴取、モニタリングもしくは監視と関連し、あるいは、コンピュータシステムへのアクセスまたはその使用を通じてなされる直接的なデータ内容の入手と、電子的な盗聴用機器またはタッピング用機器の使用を通じてなされる間接的なデータ内容の入手の双方に関連するものである。また、傍受は、記録行為を含むことができる。技術的な手段は、送受信線に設置された技術的機器と無線通信の収集及び記録のための機器とを含む。それらは、ソフトウェア、パスワード及びコードの使用を含むことができる[3]。技術的な手段を使用するという要件は、それが過剰な犯罪行為化を避けるための制約条件であることを意味している[4]。

---

[1] [訳注] 通信当事者の通信の秘密の中には、国家機密、企業秘密及び個人の秘密が含まれる。これらの中で、個人の秘密の実質がプライバシーの権利であることは、欧州評議会の個人データ保護条約（ETS No.108）によっても明らかにされている。同条約の参考訳は、法と情報雑誌 1 巻 4 号 1～20 頁に、同条約の説明書の参考訳は、同誌同号 26～61 頁にある。

[2] [訳注] 通信におけるプライバシーの利益の法的保護のことを指す。

[3] [訳注] 他のサイバー犯罪を実行するための手段であるソフトウェアやコードの製造や販売行為等は、第 6 条の機器の濫用行為として別途処罰されることがある（第 71 項ないし第 78 項参照）。

[4] [訳注] 技術的な手段を用いない傍受の方法としては、他人の口頭の会話を盗み聞きする行為や他人の信書を盗み読む行為等を考えることができる。刑法第 133 条（信書開封罪）は、「正当な理由がないのに、封をしてある信書を開けた者は、1 年以下の懲役又は 20 万円以下の罰金に処する」と規定し、同法 134 条第 1 項（秘密漏示罪）は、「医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは、6 月以下の懲役又は 10 万円以下の罰金に処する」と規定し、同法第 2 項は、「宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときも、前項と同様とする」と規定している。これらの罪に該当する行為のうち、刑法第 133 条の罪が何らかの電子的な手段を用いて実行された場合の罪数関係については、信書開封罪のみが成立し得ると解すべきであろう。この場合において、電子的な透視により開封したのと同じ結果を得ることができても、物理的な開封行為が存在しないときは、信書開封罪が成立しない（前掲前田雅英編『条解刑法（第 3 版）』392 頁）。刑法第 134 条については、情報内容を入手する行為それ自体は適法行為であり、適法に入手した情報を職務上の守秘義務に反して開示する行為を処罰するものであるので、情報の入手行為それ自体についての犯罪である通信傍受行為（電気通信事業法第 179 条に定める通信の秘密を侵害する罪、郵便法 80 条に定め

54. 侵害行為は、コンピュータデータの「非公開の」伝送に対して行われる[1]。「非公開」という用語は、伝送（通信）のプロセスの性質を限定するが、伝送されるデータの性質を限定することはない。通信されるデータは、公衆が利用できる情報であり得るが、通信当事者が機密に通信することを望むものである。あるいは、データは、有料テレビ放送におけるのと同様に、役務に対する対価の支払いがあるまでは、商業上の目的で機密に保たれるものであり得る。従って、「非公開」という用語は、それ自体として、公衆ネットワークを介した通信を排除するものではない。

55. コンピュータデータの伝送という形態による通信は、1 個のコンピュータシステム内でも（例えば、CPU から画面またはプリンタへのデータの流れ）、同一人が保有する 2 台のコンピュータシステムの間でも、相互に通信を行う 2 台のコンピュータ間でも、または、（例えば、キーボードを介して）コンピュータと人との間でも発生し得る。しかしながら、加盟国は、コンピュータシステムの間で伝送される通信であることを、付加的な要件として求めることができる。

56. 「コンピュータシステム」という概念が無線の接続を含むこともできるということは、加盟国が全ての無線の伝送の傍受行為を犯罪とすべき義務を負うということを意味しない、ということに留意しなければならない[2]。無線の伝送は、それが「非公開で」なされる場合であっても、比較的公開で容易にアクセスできるような方法で行われ、それゆえ、例えば、アマチュア無線家によって傍受され得る。

57. 「電磁的な放射[3]」と関連する犯罪行為を創設することは、より広範な適用範囲を確保することになる。電磁的な放射は、コンピュータを運用中にそのコンピュータから放射され得る。このような放射は、第 1 条で規定する定義による「データ」であるとは考えられない。しかしながら、そのような放射からデータを復元することができる。それゆえ、コンピュー

る信書の秘密を侵す罪等）とは異なる犯罪類型に属する。

[1] [訳注] 日本国の電波法（昭和 25 年法律第 131 号）の第 109 条の 2 の罰則は、暗号化された無線通信にのみ適用され、暗号化されていない公開の無線通信には適用されない。すなわち、同法第 109 の 2 第 3 項は、「暗号通信」の意義について「通信の当事者（当該通信を媒介する者であって、その内容を復元する権限を有するものを含む。）以外の者がその内容を復元できないようにするための措置が行われた無線通信をいう」と規定し、第 1 項は、「暗号通信を傍受した者又は暗号通信を媒介する者であって当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用する目的で、その内容を復元したときは、1 年以下の懲役又は 50 万円以下の罰金に処する」と規定し、そして、第 2 項は、「無線通信の業務に従事する者が、前項の罪を犯したとき（その業務に関し暗号通信を傍受し、又は受信した場合に限る。）は、2 年以下の懲役又は 100 万円以下の罰金に処する」と規定している。

[2] [訳注] 説明書の第 54 項の脚注（訳注）参照

[3] [訳注] 原文は、「electromagnetic emissions」となっている。要するに、「電波漏れ」のことを意味する。「電磁波の漏洩」とも訳されることがある。電磁的な放射を傍受して通信内容やコンピュータシステム内での処理内容を探知する攻撃手法として、テンペスト攻撃（TEMPEST attack）がある。この関係では、電気学会電磁環境・情報セキュリティ技術調査専門委員会編『電磁波と情報セキュリティ対策技術』（オーム社、2012）、Changlin Zhou, Qun Yu, and Litao Wang, Investigation of the Risk of Electromagnetic Security on Computer Systems, International Journal of Computer and Electrical Engineering Vol.4 No.1 pp.92-98 (2012)及び Robert Gehling, C. Ryan Ashley & Thomas Griffin, Electronic Emissions Security: Danger in the Air, Information Systems Management Vol. 24 Issue 4 pp.305-301 (2007) が参考になる。

タシステムからの電磁的放射のデータ傍受行為は、本条に基づく侵害行為に含められる。
58. 攻撃に対して刑事責任を負わせるためには、違法な傍受は、「意図的に」かつ「権利なく」実行されるものでなければならない[1]。例えば、傍受をする者がそのような行為を実行する権限を有する場合、（関係する者の同意のある承認された試験または防護活動を含め）伝送と関係する者の指示もしくは承認に基づいて傍受をする場合、または、捜査機関により、国家安全保障または犯罪行為の検知と関係して、正当な権限に基づいて監視が実施される場合には、その行為は、正当化される。また、例えば、「クッキー」を稼働させる場合のような通常の商業活動上の利用に関しては、「権利なく」傍受がなされるのではなく、これを犯罪行為としようとするものではないという了解がなされた[2]。第 3 条に基づいて保護される非公開の通信に関しては（上記第 54 項参照）、国内法は、そのような通信の正当な傍受のための法的根拠を定めることができる。第 3 条に基づき、そのような状況における傍受は、「権利により」実施されるものとみなされるであろう。
59. 幾つかの国々においては、傍受は、コンピュータシステムへの無権限アクセスという犯罪行為と密接な関連を有するものであるかもしれない。禁止と法の適用との一貫性を維持するために、不誠実な意図を要件とする国、または、第 2 条に従い他のコンピュータシステム

[1] [訳注] 日本国の電気通信事業法、有線電気通信法及び電波法では、過失による傍受を処罰対象としていない。また、権限に基づく行為は、刑法第 35 条の正当行為に該当し、処罰されない。

[2] [訳注] クッキー（cookie）は、個人識別のために用いられるときは、EU の一般個人データ保護規則 (EU) 2016/679 の適用を受けるから、その意味では、無条件で適法行為であるというわけではない。この点について、同規則の前文第 30 項は、「自然人は、その利用する機器、アプリケーション、ツール及びプロトコルによって提供されるオンライン識別子と関連付けられることがある。例えば、インターネットプロトコル上のアドレス、クッキー識別子、その他の電波識別タグ（RFID）のような識別子がそうである。これは、追跡のための痕跡を残すことができ、とりわけ、ユニークな 識別子及びサーバによって受信されるその他の識別子と組み合わされている場合には、自然人のプロファイルを生成し、そして、自然人を識別するために用いることができる」と述べている。また、プライバシー及び電子通信指令 2002/58/EC の前文第 25 項は、「例えば、いわゆる『クッキー（cookies）』のような仕組みは、例えば、Web サイトの設計や商業宣伝広告の有効性を解析する場合、また、オンライン商取引をする利用者の同一性を検証する場合には、適法で便利な道具となり得る。例えば、クッキーのような仕組みは、情報社会サービスの提供を促進するためといったような適法な目的のためになされるものである場合には、その利用は、利用者が使用している端末機器にその情報が置かれていることを利用者に気づかせることを確保するために、利用者に対し、指令 95/46/EC に従って、クッキーまたはそれと類似する仕組みに関する明確かつ詳細な情報が提供されることを条件として、許容されるものとしなければならない。利用者は、クッキーまたはそれと類似する仕組みがその端末機器に記録保存されることを拒否する機会を有するべきである。このことは、当初の利用者以外の利用者がその端末機器に対してアクセスをし、それによって、その機器に記録保存されているプライバシー情報ないし機微の情報を含むデータにアクセスする場合には特に重要である。この情報及び拒否する権利は、同じ接続を通じて利用者の端末機器上にインストールされる様々な仕組みの利用について提示され得るものであるし、また、その後の接続を通じて当該機器についてなされるかもしれない別の目的による利用についても適用可能なものである。情報を提供し、拒否の権利を示し、または、同意を求める方法は、可能な限り、利用者にとって使いやすいものでなければならない。特定の Web サイトのコンテントに対するアクセスでは、それが適法な目的のためにそれを行う場合には、クッキーまたはそれと類似する仕組みについての十分に説明を受けた上での承諾を条件とすることができる」と述べている。

に接続されているコンピュータシステムと関連して侵害行為が実行されることを要件とする国に関しては、同様の要件を、本条による刑事責任を負わせるための限定的な要件とすることもできる。これらの要件は、「意図的に」及び「権利なく」といったような他の犯罪行為の成立要件と組み合わせて解釈され、また、適用されるものとしなければならない。

データの妨害（第 4 条）

60. 本条の目的は、有体物について実行される場合と同様に、コンピュータデータ及びコンピュータプログラムについても、意図的な加害行為に対する保護を与えることである。保護される法益は、記録保存されたコンピュータデータもしくはコンピュータプログラムの完全性及び正常な機能またはその使用である[1]。

61. 第 1 項において、重複する行為としての「毀損」及び「劣化」は、とりわけ、データ及びプログラムの完全性またはその情報内容のネガティブな変更と関係している。データの「消去」は、有体物の破壊と同じである。それは、データを破壊し、そして、認識不可能なものとする。コンピュータデータの抑制[2]は、データが記録保存されているコンピュータまたはデータ記録場所へのアクセスを有する者の可用性を妨げまたは終了させてしまう全ての行為を意味する[3]。「改変」という用語は、既存のデータの修正を意味する[4]。ウイルスやトロイの木馬のような悪意あるコードを入力することは、データの修正をもたらすものとして、本項の適用範囲内にある。

62. 上記の各行為は、「権利なく」実行された場合にのみ、処罰され得る。ネットワークの設計において、または、通常の業務遂行もしくは商業活動において、本来的に行われる通常の活動は、権利あるものであり、従って、本条により犯罪とされることはない。例えば、保有者もしくは運営者の承認の下に行われるコンピュータシステムの安全性の検査または防護、あるいは、システムの運営者が新しいソフトウェア（例えば、従前インストールされていたプログラムでは利用できなかったインターネットへのアクセスを許容するソフトウェア）を必要とする場合に生ずるコンピュータのオペレーティングシステムの設定変更がそうであ

---

[1] [訳注] 保護法益がデータの完全性（integrity）及び可用性（availability）であることを示している。

[2] [訳注] 原文は、「Suppression of computer data」となっている。「Suppression」は、「隠蔽」または「隠匿」と訳されることもある。しかし、単にアクセスできないようにする行為のみではなく、削除・消去によって物理的にアクセス不可能な状態にする場合も含むため、外務省の訳は「隠ぺい」であるけれども、物理的には存在していてもアクセスすることができない状況を意味する「隠蔽」及び「隠匿」との訳語は適切ではない（説明書の第 83 項参照）。データの抑制は、データの可用性の阻害と同義である。「suppression」の訳語に関する同じ問題は、欧州連合の情報システムに対する攻撃に関する指令 2013/40/EU の第 5 条（違法なデータ妨害）にもある。同指令の条文の参考訳は、法と情報雑誌 1 巻 1 号 51～61 頁にある。

[3] [訳注] 刑法第 258 条は、「公務所の用に供する文書又は電磁的記録を毀棄した者は、3 月以上 7 年以下の懲役に処する」と規定し、同法第 259 条は、「権利又は義務に関する他人の文書又は電磁的記録を毀棄した者は、5 年以下の懲役に処する」と規定している。

[4] [訳注] 正当な権限に基づくデータの修正（modification）が適法行為であることは、当然の前提である。このことは、説明書の第 62 項で説明されている。

る。匿名の通信をするためのトラフィックデータの修正（例えば、匿名のメール転送システムの活用）、あるいは、機密の通信をするためのデータの修正（例えば、暗号化）は、原則として、プライバシーの正当な保護として理解されなければならず、従って、権利により行われるものとして理解すべきである[1]。しかしながら、加盟国は、犯罪行為を実行する際に加害者の識別を隠蔽するためにパケットのヘッダ情報を修正する場合のような、匿名の通信に関連する一定の侵害行為を犯罪とすることができる[2]。

63. 加えて、加害者は、「意図的に」行為したのでなければならない。

64. 第 2 項は、加盟国に対し、その侵害行為が重大な危険を発生させる行為であることを要するものとすることに関して留保を認めている。どのようなものがそのような重大な危険を構成するかについての解釈は、国内法の立法に任されている[3]。しかし、加盟国は、この留保をすることができるようにする場合には、欧州評議会の事務局長に対し、加盟国の解釈を送付しなければならない。

システムの妨害（第 5 条）

65. これは、コンピュータ妨害に関する勧告 No. R (89) 9 と関連している。本条は、コンピュータデータを使用しまたは感染させることによって、通信施設を含め、コンピュータシステムの適法な利用を意図的に妨害する行為を犯罪とすることを目的としている。保護法益は、コンピュータシステムまたは通信システムが正常に機能し得ることについての、その運営者と利用者の利益である。条文は、全ての種類の機能がそれによって保護されるようにするた

---

[1] [訳注] プライバシー拡張技術（Privacy Enhancing Technologies (PETs)）としての匿名化技術や暗号化技術のことを指している。ENISA は、PETs に関して、Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies (March 31, 2016)という報告書を公表している。PETs と関連して、米国 Apple 社の iPhone に装備されている暗号化機能について、米国の連邦捜査当局（FBI）がテロ対策のためにデータの復号を要求した行為が社会的な批判を受けたことは周知のとおりである。この問題に関しては、下記の記事が参考になる。

EFF to Support Apple in Encryption Battle (February 16, 2016)

https://www.eff.org/ja/deeplinks/2016/02/eff-support-apple-encryption-battle [2016 年 11 月 21 日確認]

[2] [訳注] 特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）の第 5 条は、「当該電子メールの送信に用いた電子メールアドレス」または「当該電子メールの送信に用いた電気通信設備を識別するための文字、番号、記号その他の符号」（送信者情報）を偽って特定電子メールの送信をしてはならないと定め、また、同法第 6 条は、「送信者は、自己又は他人の営業のために多数の電子メールの送信をする目的で、架空電子メールアドレスをそのあて先とする電子メールの送信をしてはならない」と定めている。同法第 7 条は、第 6 条の架空メールの送信等について、措置命令をすることができる旨を定めている。「特定電子メール」とは、商業宣伝広告のために送信される電子メールのことを指し、同法第 2 条第 2 号は、「電子メールの送信（国内にある電気通信設備（電気通信事業法第 2 条第 2 号に規定する電気通信設備をいう。以下同じ。）からの送信又は国内にある電気通信設備への送信に限る。以下同じ。）をする者（営利を目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メールをいう」と定義している。その罰則は、同法第 34 条に定められている。

[3] [訳注] 説明書の第 58 項の脚注（訳注）参照

め、中立的な方法で構成されている。

66. 「妨害」という用語は、コンピュータシステムの本来の機能に対して干渉する行為を指す。このような妨害行為は、コンピュータデータの入力、伝送、毀損、消去、改変または抑制によって生ずるものであることを要する[1]。

67. 妨害行為に対して刑事制裁を加えるためには、更に、それが「重大な」ものでなければならない。各加盟国は、妨害行為が「重大な」ものであると判断されることを充足させるための基準を、自ら決定しなければならない[2]。例えば、妨害行為を重大なものとして判断するために、生じた損害のミニマムの金額を要件とすることができる[3]。起草者は、システムを使用するための、または、他のシステムと通信するための保有者または運営者の可用性に対して重大で決定的な影響を与えるような方式、規模または頻度で（例えば、「サービス拒否[4]」攻撃を生成するプログラム、システムの運用を妨げまたはひどく遅延させるウイルスのような悪意あるコード、あるいは、システムの通信機能を停止させるために、受信者に対し、莫

---

[1] [訳注] 電子計算機に対してコンピュータプログラムやデータを入力することなく実行される業務妨害行為については、刑法第 233 条の業務妨害罪または同法第 234 条の威力御有無妨害罪が成立し得る。妨害の対象となる業務が公務に該当するときは、刑法第 95 条の公務執行妨害罪が成立し得る。また、妨害の対象となる業務が強制執行手続であるときは、刑法第 96 条の 3 の強制執行行為妨害罪及び同法第 96 条の 4 の強制執行関係売却妨害罪が成立し得る。この場合において、妨害行為が強制執行の対象となる財産の隠匿や破壊等であるときは、同法 96 条の 2 の強制執行妨害目的財産損壊等の罪が成立し得る。

[2] [訳注] 日本国の刑法第 234 条の 2 第 1 項は、「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、5 年以下の懲役又は 100 万円以下の罰金に処する」と規定しており、業務妨害の危険の発生を要件としている。ただし、業務妨害の危険が発生しない場合においても未遂罪が成立する（同法第 234 条の 2 第 2 項）。この業務妨害の危険の程度については、第 2 項の追加により未遂罪処罰が明確とされる以前においては、抽象的危険犯か具体的危険犯であるかといった学説・判例上の争いがあったが、第 2 項によって未遂罪処罰が定められている以上、現時点では、抽象的危険犯説が成立する余地は全くなくなったと解すべきである。この点については、夏井高人「サイバー犯罪の研究（一）－DoS 攻撃（DDoS 攻撃）に関する比較法的検討－」法律論叢 85 巻 1 号 197～231 頁（2012）で述べたとおりである。

[3] [訳注] 日本国の刑法第 234 条の 2 は、危険犯として規定されており、結果犯ではないため、損害額による限定がない。ただし、刑事裁判における量刑の判断の際においては、現実に発生した損害額の大小や弁償の有無が量刑事情として考慮に入れられることは、当然のことである。

[4] [訳注] 原文は、「denial of service」である。意味的には「役務の提供を妨害する行為」であり、犯罪類型としては業務妨害行為に該当する。Internet of things (IoT)の進展に伴い、ノート PC やスマートフォンを含むコンピュータシステムだけではなく各種 IoT 機器類（監視カメラ、ルータ、自動車搭載のコンピュータシステム等）にインストールされた攻撃用プログラムにより攻撃用パケットを集中的に送信することによって攻撃対象となったシステムの処理を阻害する結果を発生させる。このような攻撃用パケットを送信するためにハイジャックされたコンピュータや機器類のことを「Command & Control Server (C2 Server)」と呼ぶ例が多い（Joseph Gardiner, Marco Cova & Shishir Nagaraja, Command & Control: Understanding, Denying and Detecting, University of Birmingham (February 2014)が参考になる）。一般に、罪名として「denial of service」を用いる立法例は、米国の各州の刑法（犯罪法）の中に多く見られる。

大な分量の電子メールを送信するプログラム等によって)、特定のシステムにデータを送信するような場合を「重大な」ものであると理解していた。

68. 妨害行為は、「権利なく」行われなければならない。ネットワークの設計において、または、通常の業務遂行もしくは商業活動において、本来なされる通常の活動は、権利あるものである。これらの活動は、例えば、保有者もしくは運営者の承認の下に行われるコンピュータシステムの安全性の検査または防護、あるいは、従前インストールされていたプログラムでは利用できなかったインターネットへのアクセスを許容する新しいソフトウェアをシステムの運営者がインストールする際に生ずるコンピュータのオペレーティングシステムの設定変更を含む[1]。それゆえ、このような行為は、たとえそれが重大な妨害という結果を発生させた場合であっても、本条によって犯罪行為とされることはない[2]。

69. 商業目的その他の目的による望まない電子メールの送信行為は、とりわけ、そのようなメッセージが大量にまたは高頻度で送信される場合（「スパミング」[3]）には、その受信者に損害を発生させ得る。起草者の意見としては、そのような行為は、通信が意図的にひどく妨害されてしまう場合においてのみ、犯罪行為とされるべきである[4]。しかしながら、加盟国は、

---

[1] [訳注] サイバー犯罪条約が締結された当時においては、現在のようにインターネットが一般的に普及しておらず、官公庁や産業界においてもインターネット対応への移行期にあった。

[2] [訳注] 理論的には、過失によって業務妨害の結果を発生させた場合に該当する。日本国の刑法においても処罰対象行為とはなっていない。ただし、当該過失行為者について民事上の損害賠償責任特に民法 709 条の不法行為に基づく損害賠償責任が生じ得ることは別の問題である。

[3] [訳注] いわゆる「スパムメール」を含め、違法な電子メール送信行為及びその刑事処罰については、夏井高人「サイバー犯罪の研究（六）ー違法な電子メールに関する比較法的検討ー」法律論叢 86 巻 6 号 181～243 頁（2014）で詳論したとおりである。

[4] [訳注] 日本国の特定商取引法（昭和 51 年法律第 57 号）の第 12 条の 3 第 1 項柱書は、「販売業者又は役務提供事業者は、次に掲げる場合を除き、通信販売をする場合の商品若しくは指定権利の販売条件又は役務の提供条件について、その相手方となる者の承諾を得ないで電子メール広告（当該広告に係る通信文その他の情報を電磁的方法（電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法であって主務省令で定めるものをいう。以下同じ。）により送信し、これを当該広告の相手方の使用に係る電子計算機の映像面に表示されるようにする方法により行う広告をいう。以下同じ。）をしてはならない」と規定し、同法第 12 条の 3 第 2 項は、「前項に規定する承諾を得、又は同項第一号に規定する請求を受けた販売業者又は役務提供事業者は、当該通信販売電子メール広告の相手方から通信販売電子メール広告の提供を受けない旨の意思の表示を受けたときは、当該相手方に対し、通信販売電子メール広告をしてはならない。ただし、当該表示を受けた後に再び通信販売電子メール広告をすることにつき当該相手方から請求を受け、又は当該相手方の承諾を得た場合には、この限りでない」と規定し、同法第 12 条の 4 第 1 項柱書は、「販売業者又は役務提供事業者から前条第 5 項各号に掲げる業務のすべてにつき一括して委託を受けた者（以下この節並びに第 66 条第 4 項及び第 6 項において「通信販売電子メール広告受託事業者」という。）は、次に掲げる場合を除き、当該業務を委託した販売業者又は役務提供事業者（以下この節において「通信販売電子メール広告委託者」という。）が通信販売をする場合の商品若しくは指定権利の販売条件又は役務の提供条件について、その相手方となる者の承諾を得ないで通信販売電子メール広告をしてはならない」と規定し、同法第 12 条の 4 第 2 項は、「前条第 2 項から第 4 項までの規定は、通信販売電子メール広告受託事業者による通信販売電子メール広告委託者に係る通信販売電子メール広告について準用する」と規定している。罰則は、同法第 72 条第 1 項第 4 号にある。なお、説明書の第 62 項の脚注（訳注）参照。

例えば、行政刑法上の妨害行為となる特別の行為、または、その他の制裁に服する特別の行為を設けることによって、加盟国の法律に基づき、妨害行為について異なる手法を採用することができる。条文は、加盟国の法律に基づいて行政罰または刑罰を科することを正当化する危険性の閾値[1]を画定するためのシステムの機能の妨害の範囲（部分的か全体的か、一時的なものか持続的なものか）の決定については、加盟国に任せている。
70. 侵害行為は、意図的になされるものであることを要し、かつ、加害者が重大な妨害の意図を有していたことを要する。

機器の濫用（第 6 条）

71. 本条は、コンピュータシステムまたはコンピュータデータの機密性、完全性及び可用性を害する上述の侵害行為を実行するために濫用される一定の機器またはアクセスデータに関連する特別の違法行為の意図的な実行について、他の犯罪行為とは別の独立した犯罪行為を設ける。そのような侵害行為の実行は、しばしば、アクセスの手段（「ハッカー・ツール」）その他のツールの保有を必要とするので、犯罪行為のためにそれを入手しようという強い誘因が存在する。そのことは、それらを製造及び頒布するブラックマーケットのようなものを生み出すこととなり得る[2]。このような危険に対してより効果的に闘うためには、刑法は、第 2 条ないし第 5 条に基づく侵害行為の実行の前に行われる特別の潜在的に危険な行為をその根源から禁止するものでなければならない。このような観点から、条項は、欧州評議会（条件付アクセスに基づくまたはこれを構成する役務の法的保護に関する欧州条約－ETS No.178[3]）及び欧州連合（条件付アクセスに基づくまたはこれを構成するサービスの法的保護に関する欧州議会及び欧州評議会の 1998 年 11 月 20 日の指令 98/84/EC[4]）、並びに、幾つかの

[1] [訳注] 欧州連合基本権憲章第 49 条第 3 項は、「過酷な刑罰は、犯罪行為との比例性に反する」と定めている。

[2] [訳注] Lillian Ablon, Martin C. Libicki & Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, RAND Corporation (2014) が参考になる。

[3] [訳注] 説明書として、Explanatory Report to the European Convention on the Legal Protection of Services based on, or consisting of, Conditional Access (Strasbourg, 24 January, 2001) が公開されている。

[4] [訳注] 関連する指令として、Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)及び Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services がある。また、指令 98/84/EC と関連する欧州委員会の報告書として、On the legal protection of electronic pay services - Report from the Commission to the Council, the European Parliament and the European Economic and Social Committee on the implementation of Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, and consisting of, conditional access (COM/2003/0198 final) (May 14, 2003) 及び Report from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Second Report on the implementation of Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access (COM/2008/0593 final) (September 30, 2008) が公表されている。

国々の関連する法令における近時の発展に基づくものである。同様の手法は、紙幣偽造に関する 1929 年ジュネーブ条約の中で既に採用されている。

72. 第 1 項の(a)の第 1 文は、コンピュータプログラムを含め、主としてこの条約の第 2 条ないし第 5 条に設けられるいずれかの侵害行為を実行するために設計されまたは採用される装置の製造、販売、使用のための調達、輸入、配布をする行為、または、その他の利用可能にする行為を犯罪とする。「配布」は、他人に対してデータを転送する行為を指すが、「利用可能にする」は、他人の使用のためにオンライン機器を設置することを指す。また、この用語は、そのような機器へのアクセスを助長するためのハイパーリンクの作成または設置に対しても適用することを意図している。「コンピュータプログラム」に含まれるものとしては、例えば、ウイルスプログラムのように、データを改変もしくは破壊し、または、システムの運用を妨害するために設計されたプログラム[1]、あるいは、コンピュータシステムへのアクセスを入手するために設計または採用されたプログラム[2]のことを指す[3]。

73. 起草者は、専ら犯罪行為を実行するために設計された装置または犯罪行為を実行するために特に設計された装置に限定すべきかどうか、それによって、犯罪用にも非犯罪用にも用いることのできる装置[4]を排除すべきかどうかについて討議した。これでは限定し過ぎると考えられた。このような限定は、刑事手続における証明において打開不能な困難をもたらし、本条を実際には適用不能なものとしてしまうか、または、非常に希な事案においてのみ適用

---

[1] [訳注] 日本国の法令では、刑法第 168 条の 2 及び第 168 条の 3 に規定する不正指令電磁的記録に関する罪並びに刑法第 163 条の 2 ないし第 163 条の 5 に規定する支払用カード電磁的記録に関する罪が相当する。不正指令電磁的記録に関する罪については、夏井高人「サイバー犯罪の研究（三）ー通信傍受に関する比較法的検討ー」法律論叢 85 巻 6 号 363～420 頁（2013）、同「サイバー犯罪の研究（四）ー電子計算機詐欺に関する比較法的検討ー」法律論叢 86 巻 1 号 61～109 頁（2013）及び前掲「サイバー犯罪の研究（六）ー違法な電子メールに関する比較法的検討ー」で述べた。支払用カード電磁的記録に関する罪については、同「サイバー犯罪の研究（二）ーフィッシング（Phishing）に関する比較法的検討ー」法律論叢 85 巻 4・5 号 179～236 頁（2013）で述べた。

[2] [訳注] 日本国の法令では、不正アクセス禁止法第 4 条ないし第 7 条所定の罪が相当する。これらの罪については、夏井高人「サイバー犯罪の研究（五）ーサイバーテロ及びサイバー戦に関する比較法的検討ー」法律論叢 85 巻 2・3 号 85～133 頁（2013）及び前掲「サイバー犯罪の研究（三）ー通信傍受に関する比較法的検討ー」で述べた。

[3] [訳注] いわゆる「ポートスキャン（port scan）」を実行するためのプログラムや機器類については、従来から様々な議論がある。特に、相手から依頼または承認を受けることなく、しかし、害意を有することなく、セキュリティホールの発見のために実行されるような場合については、いわゆるホワイトハッカーとブラックハッカーの問題と同様に、評価が分かれる。ポートスキャンに関しては、Tariq Ahamad Ahanger, Port Scan - A Security Concern, International Journal of Engineering and Innovative Technology (IJEIT), Volume 3 Issue 10 pp.241-246 (2014)、Yousra Chabchoub, Raja Chiky and Betul Dogan, How can sliding HyperLogLog and EWMA detect port scan attacks in IP traffic?, EURASIP Journal on Information Security2014, doi:10.1186/1687-417X-2014-5 及び Prachi Deshpande, Aditi Aggarwal, S.C. Sharma & P. Sateesh Kumar, Distributed Port-Scan Attack in Cloud Environment, IEEE, doi: 10.1109/CASoN.2013.6622595 (2013) が参考になる。SHODAN に関しては、独立行政法院情報処理推進機構セキュリティセンター（IPA）「増加するインターネット接続機器の不適切な情報公開とその対策～「SHODAN」を活用したインターネット接続機器のセキュリティ検査～」（2014 年 2 月 27 日）が参考になる。

[4] [訳注] 原文は、「dual-use devices」となっている。意訳した。以下、同じ。

可能なものとしてしまう。適法に製造または配布されている場合であっても全ての機器を含ませるという代替案もまた否決された。そして、コンピュータの侵害行為を実行する意図という実体的な構成要件のみが刑罰を科すための要件として考慮され得るであろうが、そのような手法は、紙幣偽造の領域においてさえも採用されたことはない。合理的な妥協案として、条約は、その装置が客観的に主として侵害行為を実行する目的で設計または採用された場合を禁止の対象範囲としている。この方法のみが、通常は、犯罪用にも非犯罪用にも用いることのできる装置を排除することになるだろう[1]。

74. 第 1 項の(a)の第 2 文は、コンピュータシステムの全部または一部をアクセス可能な状態にするためのコンピュータのパスワード、アクセスコードまたはこれに類するデータを製造し、販売し、使用のために調達し[2]、輸入し、配布する行為[3]、または、その他それらを利用可能にする行為を犯罪行為とする。

75. 第 1 項の(b)は、第 1 項の(a)の第 1 文または第 1 項の(a)の第 2 文に規定する物を保有する行為[4]を、侵害行為として設けている。加盟国は、第 1 項の(b)の最後の文により、保有される物の数を法律によって要件とすることが認められる[5]。保有される物の数は、直接に、犯罪の意図を示すことになる。刑事責任を負わせる場合の物の数の決定は、各加盟国に任されている。

76. 侵害行為は、意図的に、かつ、権利なく実行される必要がある。例えば、コンピュータシステムへの反撃[6]という正当な目的のために製造され、市場に置かれる装置についての過剰な処罰の危険性を避けるために、侵害行為を禁止するための別の要件[7]が付加された。一般的

---

[1] [訳注] この部分の起草経過が詳しく書かれているのは、それだけ議論の多い領域であることを示すものと考えることができる。

[2] [訳注] 不正アクセス禁止法の第 4 条は、「何人も、不正アクセス行為（第 2 条第 4 項第 1 号に該当するものに限る。第 6 条及び第 12 条第 2 号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない」と規定している。なお、同法第 7 条は、識別符号を取得するためのフィッシング行為を禁止している。罰則は、同法第 12 条。

[3] [訳注] 不正アクセス禁止法の第 5 条は、「何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない」と規定している。罰則は、同法第 12 条。

[4] [訳注] 不正アクセス禁止法の第 6 条は、「何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない」と規定している。罰則は、同法第 12 条。

[5] [訳注] 不正アクセス禁止法の第 6 条は、保管する識別符号の数量については定めていないので、識別符号を 1 個でも保管すれば犯罪が成立する。

[6] [訳注] ソフトウェアのライセンス契約と関連する電子的自救行為（electronic self-help）については、國生一彦『米国の電子情報取引法ーUCITA の解説』（商事法務研究会、2001）218-225 頁、金子宏直「米国における統一コンピュータ情報取引法（UCITA）の取組み」法とコンピュータ 18 号 45～52 頁（2000）が参考になる。

[7] [訳注] 「意図的に（intentionally）」及び「権利なく（without right）」という一般的な要件のほかに、第 2 条ないし第 5 条の行為を実行する目的を要件としていることを指す。日本国の不正アクセス禁止法においても、不正アクセス行為の用に供する目的（第 4 条、第 6 条）及び「業務その他正当な理由」がないこと（第 5 条）を有することが要件とされている。

な意図の要件とは別に、条約第 2 条ないし第 5 条に設けられるいずれかの侵害行為を実行するためにその機器を使用するという特別の（直接の）意図が存在しなければならない。
77. 第 2 項は、承認の下に行われるコンピュータシステムの試験または防護のために製造されるようなツールについては条文の適用外であることを明確に定めている。この考え方は、「権利なく」という表現の中に既に含まれている。例えば、情報技術製品の信頼性を管理するために、または、システムの安全性を試験するために、産業界によって設計された試験用装置（「ハッキング装置」）及びネットワーク分析装置は、正当な目的で製造されるものであり、かつ、「権利ある」ものである。
78. 第 2 条ないし第 5 条中にある異なる種類のコンピュータ侵害行為の全部について「機器の濫用」の侵害行為を適用すべき必要性の評価が異なることから、第 3 項は、留保（第 42 条参照）に基づき、国内法における侵害行為を限定することを認めている[1]。しかしながら、各加盟国は、少なくとも、第 1 項の(a)の第 2 文に規定するコンピュータのパスワードもしくはアクセスデータの販売、配布またはその他の利用可能にする行為については、犯罪とすることが義務付けられる。

第 2 款　コンピュータと関連する侵害行為

79. 第 7 条ないし第 10 条は、しばしばコンピュータシステムの利用を介して実行される普通の犯罪と関係している。大半の国では、既に、これらの普通の犯罪を処罰するものとしている。各国の既存の法律は、コンピュータネットワークに含まれる状況に対して十分な広さの適用範囲をもっているかもしれないし、もっていないかもしれない（例えば、幾つかの国の既存の児童ポルノ法は、電子的な画像には適用されない。）。それゆえ、これらの条項を実装する過程においては、加盟国は、コンピュータシステムまたはネットワークが含まれている状況に対して既存の法律が適用されるか否かを判断するために、既存の法律を検討しなければならない。既存の侵害行為が既にそのような行為に対して適用される場合には、既存の侵害行為について法改正をし、または、新たに侵害行為を定める必要はない。
80. 「コンピュータと関連する偽造」及び「コンピュータと関連する詐欺」は、ある種のコンピュータと関連する犯罪、すなわち、コンピュータシステム及びコンピュータデータの 2 つの特別な種類の不正操作として、コンピュータと関連する偽造及びコンピュータと関連する詐欺を扱っている。これらを採用したのは、多くの国々において、新たな形態による妨害行為と攻撃に対して、従来からの一定の法益が十分に保護されていないという事実を認識したからである[2]。

[1] [訳注] 不正アクセス禁止法第 4 条の「取得」の中には「輸入」による取得も含まれると解される。同法第 5 条の「提供」の中には「頒布」、「配布」その他の流通に置く行為（利用可能にする行為）による提供も含まれると解される。
[2] [訳注] ある財産権に対する侵害行為に対して本当に刑罰法令が適用されないのかどうかについては、慎重な検討を要する場合がある。例えば、従来の法理論や判例が誤っていたために多くの人々が「刑罰法令を適用することができない」と誤解しているような場合がそうである。この場合、考え方を変更するだけで刑罰法令の適用はあることになる。法の欠缺が客観的に存在するというわけではない。

コンピュータと関連する偽造（第 7 条）

81. 本条の目的は、有形の文書の偽造と対応する侵害行為を設けることにある。これは、在来型の偽造と関連する刑法上の間隙を埋めることを目的としている。在来型の偽造は、文章が視覚的に閲読可能であることまたは文書中に陳述が化体されていることを要件としているが、これは、電子的に記録保存されるデータには適用できない[1]。証拠としての価値を有するデータの不正操作は、それによって第三者に錯誤が生ずる場合には、在来型の偽造と同じように、重大な結果を発生させ得る[2]。コンピュータ関連偽造は、記録保存されたデータの無権限による作成及び無権限による改変を含む。それは、データの中に含まれる情報の真正性に信頼を置いて行われる法律行為の過程において、証拠としての価値を変動させる行為であるので、詐欺罪とされるべきである[3]。保護法益は、法律関係に影響を与え得る電子データの安全性と信頼性である。

82. 各国の偽造概念が区々となっていることには留意しなければならない。ある概念では、文書の作成者に関する真正性に基礎を置き、そして、別の概念では、文書内にある文の内容の真実性に基礎を置いている[4]。しかしながら、データ内容の正確性または真実性とは無関係

---

[1] [訳注] 刑法第 155 条第 1 項は、「行使の目的で、公務所若しくは公務員の印章若しくは署名を使用して公務所若しくは公務員の作成すべき文書若しくは図画を偽造し、又は偽造した公務所若しくは公務員の印章若しくは署名を使用して公務所若しくは公務員の作成すべき文書若しくは図画を偽造した者は、1 年以上 10 年以下の懲役に処する」と規定し、同法第 159 条第 1 項は、「行使の目的で、他人の印章若しくは署名を使用して権利、義務若しくは事実証明に関する文書若しくは図画を偽造し、又は偽造した他人の印章若しくは署名を使用して権利、義務若しくは事実証明に関する文書若しくは図画を偽造した者は、3 月以上 5 年以下の懲役に処する」と規定している。これらの条項は、「印章」及び「署名」を構成要件要素として定めているが、電子的なデータでは紙の文書と同じような意味での印章や署名を考えることができない。電子署名法に基づく電子署名は、電子的な認証手段によって電磁的記録の真正性を担保する仕組みの一種であるが、紙の文書における印章や署名とは本質的に異なる。

[2] [訳注] 日本国においては、2012 年、いわゆる「パソコン遠隔操作事件」という一連の出来事が発生し、警察による誤認逮捕が相次いだ（前掲「ケーススタディ・サイバー犯罪捜査（2）」参照）。

一般に、通信中の画像や音声をリアルタイムで書き換える技術は既に存在しているので、モニタカメラによる映像及び音声についても、第三者によって無権限でリモート操作がなされることがあり得る。このような問題については、2003 年 11 月にオーストリアのザルツブルグで開催された CILS Conference における報告用要旨「Online Witness – How to Prevent Fake Evidence」の中で論じた。

[3] [訳注] 一般に、文書偽造罪、偽造文書の行使罪及び詐欺罪との間には、順次、手段・結果の関係があることから、牽連犯と解されており、不正作出された電磁的記録の場合も同様であると解されている。ただし、このような偽造類型の犯罪と詐欺類型の犯罪行為との罪数の問題は、各国の法制の相違により大きく異なることがあるので、注意を要する。

[4] [訳注] 一般に、作成名義を偽る偽造行為を有形偽造と呼び、文章の内容を偽る偽造行為を無形偽造と呼んでいる。日本国の刑法では有形偽造を基本とするが、例外として、同法 156 条は、「公務員が、その職務に関し、行使の目的で、虚偽の文書若しくは図画を作成し、又は文書若しくは図画を変造したときは、印章又は署名の有無により区別して、前 2 条の例による」と定め、また、同法 160 条は、「医師が公務所に提出すべき診断書、検案書又は死亡証書に虚偽の記載をしたときは、3 年以下の禁錮又は 30 万円以下の罰金に処する」と定めており、無形偽造（虚偽文書作成行為）を処罰するものとしている。すなわち、日本国の法制は、折衷的または混合的な法制を採用しているということができる。

に、データの発行者に関する最小限度の真正性に関する欺瞞的な行為であることが合意された。加盟国は、これを拡張して、「真正」という用語の下に、データの真正性を含めることができる[1]。

83. 本条は、私文書または公文書と均等なデータであって、法的効果を持つものに適用される[2]。正確なデータまたは不正確なデータの無権限による「入力」は、虚偽の文書の作成と同じような状況をもたらす。それに続く改変（修正、変形、部分的変更）、消去（データ媒体からのデータの削除）及び抑制[3]（データの隠蔽・隠匿）は、一般に、真正な文章を偽造文書化するのと同じことである。

84. 「法的な目的のために」という用語は、法律行為及び法的に関係する文書をも指す。

85. 本条の最後の文は、国内法中に侵害行為を実装する場合において、詐取の意図またはこれに類する不誠実な意図を、刑事責任を負わせるために付加することを認めている。

コンピュータと関連する詐欺（第 8 条）

86. 技術革新の到来と共に、クレジットカード詐欺[4]を含め、詐欺のような経済犯罪が実行される機会も倍増した。コンピュータシステムで表現または管理される資産（電子的な資金、預貯金）は、従来の形態の財産と同様に、偽造の対象となってきた[5]。これらの犯罪は、主と

---

[1] [訳注] 刑法第 168 条の 2 の不正指令電磁的記録作出罪の保護法益に関しては、一般に、電子計算機で用いられる電磁的記録に対する社会一般の信頼であると解されている（前掲前田雅英編『条解刑法（第 3 版）』467 頁）。

[2] [訳注] 刑法は、私文書に相当する電磁的記録に関しては、第 161 条の 2 第 1 項が「人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、5 年以下の懲役又は 50 万円以下の罰金に処する」と規定し、同条第 3 項が「不正に作られた権利、義務又は事実証明に関する電磁的記録を、第 1 項の目的で、人の事務処理の用に供した者は、その電磁的記録を不正に作った者と同一の刑に処する」と規定している。有価証券に相当する電磁的記録に関しては、同法第 163 条の 2 ないし第 163 条の 5 に規定がある。公文書に相当する電磁的記録に関しては、同法第 157 条第 1 項が「公務員に対し虚偽の申立てをして、登記簿、戸籍簿その他の権利若しくは義務に関する公正証書の原本に不実の記載をさせ、又は権利若しくは義務に関する公正証書の原本として用いられる電磁的記録に不実の記録をさせた者は、5 年以下の懲役又は 50 万円以下の罰金に処する」と規定し、同法第 158 条第 1 項が「第 154 条から前条までの文書若しくは図画を行使し、又は前条第 1 項の電磁的記録を公正証書の原本としての用に供した者は、その文書若しくは図画を偽造し、若しくは変造し、虚偽の文書若しくは図画を作成し、又は不実の記載若しくは記録をさせた者と同一の刑に処する」と規定し、同法第 161 条の 2 第 2 項が「前項の罪が公務所又は公務員により作られるべき電磁的記録に係るときは、10 年以下の懲役又は 100 万円以下の罰金に処する」と規定している。

[3] [訳注] 説明書の第 61 項の脚注（訳注）参照。

[4] [訳注] クレジットカードに用いられる情報に関する取引行為やクレジットカードに用いられる電磁的記録の不正作出行為については、日本国の法令では、刑法第 168 条の 2 及び第 168 条の 3 に規定する不正指令電磁的記録に関する罪並びに刑法第 163 条の 2 ないし第 163 条の 5 に規定する支払用カード電磁的記録に関する罪として処罰される。

[5] [訳注] 本来、「価値」それ自体は抽象的なものであり、極論すれば主観的にしか存在しない。通貨や

して、コンピュータの中に不正なデータを投ずるという入力の偽造行為、または、データ処理の過程におけるプログラムの不正操作行為その他の妨害行為によって構成されている[1]。本条の目的は、財産の違法な移転という効果を意図してなされるデータ処理過程での全ての不正操作を、犯罪行為とすることにある[2]。

87. 関連する全てのあり得る偽造行為を適用範囲とすることを確保するために、第 8 条の(a)にある「入力」、「改変」、「消去」または「抑制」という構成要件は、第 8 条の(b)にある「コンピュータプログラムまたはコンピュータシステムの機能の妨害」という一般的行為によって補われる。「入力、改変、消去もしくは抑制」という要件は、その前の条項の中に規定されるものと同じ意味を持つ。第 8 条の(b)は、ハードウェアの不正操作行為、プリントアウトを抑制する行為、及び、データの記録ないしデータの流れまたはプログラムが走っているシーケンスに悪影響を与える行為のような行為に適用される。

88. コンピュータの詐欺的な不正操作行為は、他の者の財産に対して直接に経済的損失またはその占有喪失を発生させる場合であって、かつ、犯人が、自己または他の者のために違法な経済的利益を得ることを意図している場合に、犯罪となる[3]。「財産の損失」という用語は、

電子データは、その存在を示すためのシンボルまたはトークンの一種に過ぎない。ただ、法制度によって価値の存在を認めるように強制される場合には、社会的な意味をもつ。

[1] [訳注] 電子計算機を用いた詐欺類似行為については、人間に対する欺罔行為が存在せず、機械装置を無権限で捜査して財産上不法の利益を得る行為であるので、本質的には、自動販売機を違法に操作して物品の占有を取得する行為と同様、詐欺類型の行為ではなく、窃盗類型の行為に属する。この点については、前掲「サイバー犯罪の研究（四）－電子計算機詐欺に関する比較法的検討－」で詳論したとおりである。なお、電子計算機使用詐欺罪の裁判事例については、夏井高人「サイバー犯罪の研究（七）－電子計算機詐欺に関する比較法的検討－」法律論叢 87 巻 1 号 163～206 頁（2014）においても検討した。一般に、「利益窃盗は処罰されない」と言われる。しかし、このような見解は、各種自動機械が社会内に普及する以前に成立した古い時代の産業構造・社会構造を基盤とするものであり、現代社会では全く通用しない考え方である。そして、かつて「利益窃盗」として理解されていた事例の多くは、正しくは、可罰的違法性の範囲の問題（実質的に被害のない一時的な利用行為の可罰性の問題）としてとらえられるべきものである。

[2] [訳注] 国際組織犯罪等対策推進本部決定「国際組織犯罪等対策に係る今後の取組みの改訂について」（2003 年 9 月 17 日）は、偽造・変造クレジットカード事犯に対する取締りに関する法務・警察の事項として、「平成 13 年 6 月に、刑法の一部改正により、クレジットカードその他の支払用のカードの社会的信頼を確保するため、支払用カードを構成する電磁的記録等の不正作出、所持、これらの電磁的記録情報の不正取得等の行為についての処罰規定を整備したところであるが、改正刑法を積極的に活用し、これらの行為に対する厳正な取締りを推進する」としている。また、第 17 回日 ASEAN 首脳会議(2014 年 11 月 12 日)において採択された「テロ及び国境を越える犯罪と闘う協力のための日 ASEAN 共同宣言」の中では、「クレジットカード詐欺，通貨偽造，違法な株取引といった国際経済犯罪は，世界中で以前にも増して顕著となっており，ASEAN 地域と日本の経済及び社会の安定に対する深刻な脅威となっている」との認識を前提にした上で、「国際経済犯罪との闘いについて，関連機関でベスト・プラクティスを交換する」こと及び「法執行協力を促進する」こと（外務省仮訳）が明記されている。

[3] [訳注] 刑法第 246 条の 2（電子計算機使用詐欺罪）は、「前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、10 年以下の懲役に処する」と定

広い概念であり、金銭の損失、有形及び無形の経済的価値の損失を含む。

89. 侵害行為は、「権利なく」実行されるものでなければならず、かつ、経済的利益は、権利なく獲得されるものでなければならない。無論、経済的な利益の獲得を意図するものであっても、正当な普通の商業活動は、権利あるものとして行われるものであるので、本条によって設けられる侵害行為に含まれるべきものとして理解されることはない。例えば、影響を受ける当事者間の有効な契約に従って行われる行為は、権利あるものである（例：契約条件による権限に基づくものとして行われる Web サイトの利用停止）[1]。

90. 侵害行為は、「意図的に」実行されるものでなければならない。一般的な意図の要件は、他人の財産の損失をもたらすコンピュータ不正操作行為またはコンピュータ妨害行為のことを指す。また、侵害行為は、自己または他の者のために経済的利益を獲得する特別の詐欺的な意図または不誠実な意図を要する[2]。それゆえ、例えば、誰かに対して経済的な損失を発生させ、または、他人に対して利益を発生させるかもしれない市場における競争行為に関する商業活動は、詐欺的な意図または不誠実な意図で行われるのでない場合には、本条によって設けられる侵害行為に含まれるということを意味するものではない。例えば、インターネット上の比較購買のために情報収集プログラムを用いること（「ボット（bot）」）については、「ボット」が訪問するサイトによって承認されたものでなくても[3]、これを犯罪とすることを意図するものではない。

めている。刑法典の中では詐欺類型の犯罪として規定されているが、前述のとおり、理論的には、窃盗類型に属する犯罪行為（利益窃盗行為）である。なお、電子計算機を用いて実行される利益の横領行為も同じく刑法第 246 条の 2 によって処罰されるべきであるが、この場合において、背任罪及び業務妨害罪との罪数関係が問題となる。この点に関しては、夏井高人「サイバー犯罪の研究（八）－電子的な横領及び類似行為に関する事例検討－」法律論叢 88 巻 2・3 号 1～49 頁で詳論した。なお。同稿中の校正ミスによる誤りの正誤は、前掲「サイバー犯罪の研究（九・完）－補遺・最近の法改正と裁判事例－」の末尾に記載のとおりである。

[1] [訳注] 契約が解除された場合、無効原因があり当初より無効である場合、取消事由があり後に取消権の行使がなされた場合などについては検討の余地が全くないわけではない。一般に、これらの事由の存在を知らず、契約が適法に有効性を維持しているとの認識に基づいて行われる行為については、民事上の損害賠償責任の有無は別として、刑事上の犯罪行為を構成することはないと解される。

[2] [訳注] 刑法第 246 条の 2（電子計算機使用詐欺罪）が成立するためは、「財産上不法の利益」を得ること、または、そのような利益を他人に得させることを要する。ただし、同罪は、結果犯ではなく危険犯として理解されている。そのことから、日本国の法制においては、利益の現実的な獲得という結果が生ずることを要せず、利益の獲得の危険の発生により既遂になる。例えば、銀行のコンピュータシステムを無権限で違法に操作し、真実は送金の事実がないのに、自己または第三者の預金口座に入金があったようにデータ処理をした場合には、その預金口座から現実に預金の払い戻しを受けることがなくても、データ処理が発生した時点で当該銀行から違法に利益を獲得する危険性が発生していることになるため、そのデータ処理によって自己または第三者の口座に入金のデータ処理が完了した時点で電子計算機使用詐欺罪が既遂となる。

[3] [訳注] ボット（bot）による自動巡回と自動的な情報収集等を禁止するためのタグの設定等が行われているサイトについては、別の考慮を要する。この場合には、「承認していない」のではなく「拒否している」と理解すべきである。なお、現在では、人工知能技術を応用した高度な情報収集が行われるようになっており、従来の bot 排除技術だけでは対処できなくなっていることにも留意すべきである。

第 3 款　コンテントと関連する侵害行為

児童ポルノと関連する侵害行為（第 9 条）

91. 児童ポルノに関する第 9 条は、児童に対する保護手段の強化を目指している。この保護には、児童に対する性的侵害行為の実行におけるコンピュータシステムの利用をより効果的に規制するための、刑罰法令の現代化による、性的搾取からの児童の保護が含まれる。
92. 本条は、欧州評議会の第 2 回サミット（ストラスブール、1997 年 10 月 10 日～11 日）における行動計画（項目 III.4）に示されている欧州評議会の構成国首脳及び政府の重点事項に対応するものであり、そして、児童ポルノを禁圧しようとする国際的な趨勢と一致するものである。このことは、児童売買、児童売春及び児童ポルノについての児童の権利に関する国連憲章選択的議定書が近時採択されたこと[1]、児童の性的搾取と児童ポルノとの闘いを欧州委員会が近時首唱していること(COM2000/854)[2]によって証明されている[3]。
93. 本条は、児童ポルノ[4]の電子的な製造、所持及び頒布という様々な側面を犯罪としている。

---

[1] [訳注] 児童の売買、児童買春及び児童ポルノに関する児童の権利に関する条約の選択議定書（児童の売買等に関する児童の権利条約選択議定書）には日本国も加盟している。同議定書は、平成 17 年 1 月 26 日、公布された（平成 17 年条約第 2 号及び外務省告示第 61 号）。同議定書の条文（日本語訳）は、外務省のサイトで公開されている。同議定書の前文には、「児童の権利に関する条約の目的及び同条約の規定（特に、第 1 条、第 11 条、第 21 条、第 32 条、第 33 条、第 34 条、第 35 条及び第 36 条の規定）の実施を更に達成することを目的として、児童の売買、児童買春及び児童ポルノからの児童の保護を保障するために締約国がとるべき措置を拡大することが適当であることを考慮し」とある（外務省訳）。

[2] [訳注] Communication from the Commission to the Council and the European Parliament - Combating trafficking in human beings and combating the sexual exploitation of children and child pornography (22/1/2001-COM (2000) 854 final)

[3] [訳注] 児童ポルノの被写体となっている自然人による「忘れられる権利（right to be forgotten）」の行使について、2016 年 4 月 27 日に採択された一般個人データ保護規則 (EU) 2016/679 の前文第 65 項は、「この権利は、特に、データ主体が、子どもの時に、その処理に含まれるリスクについて完全に理解しないまま彼または彼女の同意を与えたけれども、後になってそのような個人データの削除を望むようになった場合と関連するものであり、とりわけインターネット上のデータと関連するものである。データ主体は、彼または彼女が既に子どもではないという事実とは無関係に、その権利を行使することができる」と述べている。

[4] [訳注] 児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律（平成 11 年法律第 52 号・以下「児童ポルノ禁止法」という。）の第 2 条第 3 項は、児童ポルノについて、写真、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に係る記録媒体その他の物であって」、「児童を相手方とする又は児童による性交又は性交類似行為に係る児童の姿態」（1 号）、「他人が児童の性器等を触る行為又は児童が他人の性器等を触る行為に係る児童の姿態であって性欲を興奮させ又は刺激するもの」（2 号）または「衣服の全部又は一部を着けない児童の姿態であって、殊更に児童の性的な部位（性器等若しくはその周辺部、臀部又は胸部をいう。）が露出され又は強調されているものであり、かつ、性欲を興奮させ又は刺激するもの」（3 号）のいずれかの児童の姿態を視覚により認識することができる方法により描写したものをいう」と定義している。

ほとんどの国は、児童ポルノの在来型の製造及び物的な配布を既に犯罪としている。しかし、そのような物[1]の売買にとっての基本的な手段であるインターネットの利用が絶え間なく増大しているので、この新たな形態による児童の性的搾取及び危殆化と闘うために国際的な法律文書の中に特別の規定を置くことが重要である、ということが強く意識されるようになった。そのような物、そして、児童性愛者の間でのアイデアの交換、妄想及び助言のようなオンライン上の行為が、児童に対する性犯罪を支援し、推奨し、または、促進する役割を果たしていると、広く考えられている[2]。

94. 第 1 項の(a)は、コンピュータシステムを介して配布する目的で行われる児童ポルノの製造を犯罪としている[3]。本条は、その発生源において上記の危険と闘うために必要なものであると考えられた[4]。

95. 第 1 項の(b)は、コンピュータシステムを介して行なわれる児童ポルノの「提供」を犯罪としている[5]。「提供」は、他人に対して児童ポルノを入手するように求める行為に適用することを意図している。このことは、物を提供する者が現実にそれを提供可能であることを意味する。「利用可能にする」は、例えば、児童ポルノのサイトを構築することによって、他人の利用のために児童ポルノをオンライン上に置く行為に適用することを意図している。また、本項は、そのようなサイトへのアクセスを促進するための、児童ポルノのサイトへのハイパーリンクの設置または編纂にも適用することを意図している[6]。

---

[1] [訳注] 原文は、「material」となっている。文脈から、物体である児童ポルノ及び電磁的記録である児童ポルノの両方を含む趣旨と解されるが、便宜、「物」と訳すことにした。以下、同じ。

[2] [訳注] 児童ポルノ禁止法の第 1 条は、「この法律は、児童に対する性的搾取及び性的虐待が児童の権利を著しく侵害することの重大性に鑑み、あわせて児童の権利の擁護に関する国際的動向を踏まえ、児童買春、児童ポルノに係る行為等を規制し、及びこれらの行為等を処罰するとともに、これらの行為等により心身に有害な影響を受けた児童の保護のための措置等を定めることにより、児童の権利を擁護することを目的とする」と定めている。

[3] [訳注] 児童ポルノ禁止法の第 7 条第 3 項、第 4 項及び第 5 項は、様々な態様による児童ポルノの製造行為について、3 年以下の懲役または 300 万円以下の罰金に処する旨を規定している。同条第 7 項は、児童ポルノの不特定の者または多数の者に提供する目的または公然と陳列する目的による児童ポルノの製造行為について、5 年以下の懲役または 500 万円以下の罰金に処する旨を規定している。

[4] [訳注] 児童ポルノ禁止法第 2 条第 3 号所定の姿態をとらせた画像を電磁的記録にかかる記録媒体に記録する行為の合憲性に関しては、最高裁平成 18 年 2 月 20 日決定・刑集 60 巻 2 号 216 頁がある。

[5] [訳注] 児童ポルノ禁止法の第 7 条第 2 項は、児童ポルノの提供行為について、3 年以下の懲役または 300 万円以下の罰金に処する旨を規定している。また、同条第 6 項は、児童ポルノの不特定の者または多数の者に提供する行為及び公然と陳列する行為について、5 年以下の懲役または 500 万円以下の罰金に処する旨を規定している。刑法第 175 条のわいせつ物頒布等の罪の法定刑は 2 年以下の懲役または 250 円以下の罰金もしくは科料であるので、児童ポルノ禁止法第 7 条第 6 項の加重提供罪の法定刑はかなり重いということができる。なお、児童ポルノ禁止法第 7 条第 4 項の罪と刑法第 175 条の罪との罪数関係については、最高裁平成 21 年 7 月 7 日決定・刑集 63 巻 6 号 507 頁がある。

[6] [訳注] 児童ポルノサイトの URL をホームページ上で明らかにする行為に関して、最高裁平成 24 年 7 月 9 日決定・裁判集刑事 308 号 53 頁がある。なお、児童ポルノの提供行為を処罰する児童ポルノ禁止法第 7 条第 2 項の合憲性に関しては、最高裁平成 14 年 6 月 17 日判決・裁判集刑事 281 号 577 頁がある。関連する論説として、上野幸彦「児童ポルノ提供罪と共犯ー最高裁平成 24 年 7 月 9 日決定を契機

96. 第 1 項の(c)は、コンピュータシステムを介して行われる児童ポルノの配布行為または伝送行為を犯罪とする[1]。「配布」は、物を積極的に配る行為である。コンピュータシステムを介して他人に児童ポルノを送信する行為は、児童ポルノの「伝送」という侵害行為が適用されることになるであろう。
97. 第 1 項の(d)中の「自己または他人のために、児童ポルノを調達」[2]という用語は、例えば、それをダウンロードすることによって、児童ポルノを積極的に入手することを意味する[3]。
98. コンピュータシステム内または磁気ディスクもしくは CD-ROM のようなディスク上で児童ポルノを所持する行為は、第 1 項の(e)により犯罪行為となる[4]。児童ポルノの所持は、そのような物を求めることを奨励することになる。児童ポルノの製造を削減させるための効果的な方法は、製造から所持へとつながる一連の流れにおける全ての関与者の行為について刑罰を科すことである[5]。
99. 第 2 項中の「ポルノである物[6]」という用語は、猥褻であり、公序良俗に合致せずまたは

として」情報ネットワーク・ローレビュー14 巻 67～84 頁 (2016)がある。

[1] [訳注] 「配布」及び「伝送」は、児童ポルノ禁止法第 7 条第 2 項の「提供」に該当する。

[2] [訳注] 児童ポルノ禁止法第 7 条の適用との関係では、「所持」、「保管」、日本国への「輸入」が「調達」に該当すると解される。

[3] [訳注] 児童ポルノ禁止法第 7 条第 1 項は、「自己の性的好奇心を満たす目的で、児童ポルノを所持」する行為及び「自己の性的好奇心を満たす目的で、第 2 条第 3 項各号のいずれかに掲げる児童の姿態を視覚により認識することができる方法により描写した情報を記録した電磁的記録を保管」する行為について、1 年以下の懲役または 100 万円以下の罰金に処する旨を規定している。同法同条第 3 項は、提供の目的で自動ポルノを所持またはその電磁的記録を保管する行為について、3 年以下の懲役または 300 万円以下の罰金に処する旨を規定している。同条第 7 項は、児童ポルノの不特定の者または多数の者に提供する目的または公然と陳列する目的により児童ポルノを所持する行為またはその電磁的記録を保管する行為について、5 年以下の懲役または 500 万円以下の罰金に処する旨を規定している。

[4] [訳注] 児童ポルノ禁止法第 7 条第 1 項、同条第 3 項及び第 7 条の「所持」及び「保管」が該当する。

[5] [訳注] 近未来の犯罪学や行刑学の分野では、教育や訓練による犯罪者の改善ではなく、物理的・直接的な脳神経操作による「脳のリセット（brain reset）」が研究されることになるであろう。なお、この関連では、Nicole Rafter, Chad Posick & Michael Rocque, The Criminal Brain: Understanding Biological Theories of Crime (2nd edition), New York University Press (2016)、Dean A. Haycock, Murderous Minds: Exploring the Criminal Psychopathic Brain: Neurological Imaging and the Manifestation of Evil, Pegasus Books (2014)、Renee Pittman, Remote Brain Targeting, Createspace Independent Publishing Platform (2011)、Judith Horstman, The Scientific American Brave New Brain: How Neuroscience, Brain-Machine Interfaces, Neuroimaging, Psychopharmacology, Epigenetics, the Internet, and Our Own Minds are Stimulating and Enhancing the Future of Mental Power, Jossey-Bass (2010)、Satwat Bashir & Abad Shah, Storage, Retrieval and Manipulation Techniques of Human Brain Data, LAP Lambert Academic Publishing (2011)及び Marion Albers, Thomas Hoffmann & Joern Reinhardt (Eds.), Human Rights and Human Nature, Springer (2016)、Mark N. Gasson, Eleni Kosta & Diana M. Bowman (Eds.), Human ICT Implants: Technical, Legal and Ethical Considerations, Springer (2014)、Thomas D. Coates, Neural Interfacing: Forging the Human-Machine Connection, Morgan and Claypool Publishers (2008)、Lyuba Alboul, Dana Damian & Jonathan M. Aitken (Eds.), Towards Autonomous Robotic Systems: 17th Annual Conference, TAROS 2016, Sheffield, UK, June 26--July 1, 2016, Proceedings, Springer (2016)及び Woodrow Barfield, Cyber-Humans: Our Future with Machines, Springer (2015)が参考になる。

[6] [訳注] 原文は、「pornographic material」となっている。

これらと同様に堕落的であるという物の分類に関する各国の基準によって規律される[1]。従って、芸術上、医学上、科学上の利点その他これらに類する利点を有する物は、ポルノであるとは判断されないだろう[2]。視覚的な描写は、コンピュータディスクその他の電子的な記録手段に記録保存されたデータであって、視覚画像へと変換可能なものを含む[3]。

---

[1] [訳注] 典拠は不確実であり、捏造の可能性がないわけではないが、一般に、Nikola Tesla (1856-1943)は、「Alpha waves in the human brain are between 6 and 8 hertz. The wave frequency of the human cavity resonates between 6 and 8 hertz. All biological systems operate in the same frequency range. The human brain's alpha waves function in this range and the electrical resonance of the earth is between 6 and 8 hertz. Thus, our entire biological system in the brain and the Earth itself – work on the same frequencies. If we can control that resonate system electronically, we can directly control the entire mental system of humankind」との趣旨を述べていたと信じられている（なお、Tesla が晩年に電磁的兵器の開発に没頭していたことは、史実として認められる。）。現実問題として、Nikola Tesla が生きていた時代には、そのようなアイデアを実現する技術的手段が存在しなかった。しかし、近未来の社会においては、一定の信号を組み合わせた電波を人間の生体脳に直接に作用させ、性的興奮を高めるような脳神経の直接操作をすることが可能となることは、ほぼ確実である。このような脳機能を直接に操作する技術が普及した場合、現実に性行為をしていなくても性行為をしているように錯覚し性的快感を得ることができるようになるであろう。もしその時点で「猥褻」の概念が存続しているとすれば、そのような脳神経に直接作用する「信号の組み合わせ」についてもポルノの該当性を検討しなければならなくなる。一般に、人間には「心」や「心理」というものは一切存在せず、脳内における一定の化学変化や電位変化の組み合わせという物理現象に過ぎないので、今後は、哲学的な意味での「意思理論」を全て捨て、脳神経科学をベースにした法理論が構築するのでなければ、このような脳に直接作用する技術的手段の法的評価をすることができなくなることは確実である。他方において、現在の意思理論を前提とする場合であっても、猥褻の意識ないし感覚は、ポルノであるか否かとは無関係に、脳内の一定の信号処理によって惹起されるものであることそれ自体を否定することは不可能なことなので、「ポルノ」や「猥褻」の定義それ自体の根本的な見直しが求められていると考えることもできる。なお、スティーヴン・スピルバーグ監督（トム・クルーズ主演）の映画『マイノリティ・リポート』(2002 年）の中に関連する情景描写がある。

[2] [訳注] 児童ポルノ禁止法第 3 条は、「この法律の適用に当たっては、学術研究、文化芸術活動、報道等に関する国民の権利及び自由を不当に侵害しないように留意し、児童に対する性的搾取及び性的虐待から児童を保護しその権利を擁護するとの本来の目的を逸脱して他の目的のためにこれを濫用するようなことがあってはならない」と定めている。

[3] [訳注] 視覚は、脳内の化学反応の一種である。それゆえ、眼球の機能を物理的に完全に喪失している者であっても、脳内に一定の電気信号を直接に作用させることによって、または、視神経から脳内への経路に位置する特定の部位に対して一定の電気的な刺激を与えることによって、あたかも視覚を有しているかのように意識することができる。この仕組みを利用して、機械装置であるセンサーを脳内にインプラントし、視覚を回復または増強するような医療目的または軍事目的でのサイボーグ化の研究もなされている。すると、この第 99 項で説明されている「視覚画像へと変換可能なもの」の範囲も通常の画像だけではなく、脳内において画像として意識させることが可能な一定の電気信号の組み合わせを含むと解釈することとならざるを得ない。なお、この関連では、Baldassare Di Bartolo & John Collins (Eds.), Biophotonics: Spectroscopy, Imaging, Sensing, and Manipulation, Springer (2010)及び Gustavo Carneiro, Diana Mateus, Peter Loïc, Andrew Bradley, João Manuel R. S. Tavares, Vasileios Belagiannis, João Paulo Papa, Jacinto C. Nascimento, Marco Loog, Zhi Lu, Jaime S. Cardoso & Julien Cornebise (Eds.), Deep Learning and Data Labeling for Medical Applications: First International Workshop, LABELS 2016, and Second International Workshop, DLMIA 2016, Held in Conjunction with MICCAI 2016, Athens, Greece, October 21, 2016, Proceedings, Springer (2016)及び、Fabrice Jotterand & Veljko Dubljević (Eds.), Cognitive Enhancement:

100. 「あからさまな性行為」は、少なくとも、現実のまたはシミュレーションによる a) 未成年者間もしくは成人と未成年者間[1]、または、異性間もしくは同性間の性器と性器、口と性器、肛門と性器、口と肛門を含む性交行為、b) 獣姦行為、c) 自慰行為、d) 性的な状況下での嗜虐的または被虐的行為、または e) 未成年者の性器または人目に触れる部位の挑発的な展示[2]に適用される。行為が、現実的に描写されているか、または、シミュレートされて描写されているかの別は、関係がない[3]。

101. 第 1 項に含まれる侵害行為を実行するための第 2 項に規定する 3 つのタイプの物は、現実の児童に対する性的虐待行為の描写（2a）、性的にあからさまな行為を行っている児童のように見える者のポルノ画像（2b）、そして、最後に、「写実的」ではあるが、実際には、あからさまな性行為を行っている現実の児童を含まない画像（2c）に適用される。この最後のシナリオは、生きた人間を修正した写真またはコンピュータによって完全に生成された写真のような変形された写真[4]を含む。

102. 第 2 項が適用される 3 つの場合においては、それらの保護法益が若干異なっている。第 2 項の(a)は、より直接的に、児童虐待に対する保護に焦点を当てている。第 2 項の(b)及び(c)は、現実の児童である必要がないので、その物の中に描写された「児童」に対する危険を作

Ethical and Policy Implications in International Perspectives, Oxford University Press (2016)が参考になる。

[1] [訳注] 児童ポルノ禁止法第 2 条第 3 項第 1 号は、「児童を相手方とする又は児童による性交又は性交類似行為に係る児童の姿態」と規定している。

[2] [訳注] 児童ポルノ禁止法第 2 条第 3 項第 2 号は、「他人が児童の性器等を触る行為又は児童が他人の性器等を触る行為に係る児童の姿態であって性欲を興奮させ又は刺激するもの」と規定し、同項第 3 号は、「衣服の全部又は一部を着けない児童の姿態であって、殊更に児童の性的な部位（性器等若しくはその周辺部、臀部又は胸部をいう。）が露出され又は強調されているものであり、かつ、性欲を興奮させ又は刺激するもの」と規定している。

[3] [訳注] 従来、アニメ作品等における描写がしばしば問題とされてきた。基本的には、児童ポルノ禁止法第 3 条に定める「文化芸術活動」の範疇に含まれるものであるか否か、そして、「児童に対する性的搾取及び性的虐待から児童を保護しその権利を擁護するとの本来の目的」に照らして違法行為であると認められるか否かが慎重に検討されなければならない。ここでの社会的な評価基準としては、表現の自由及び言論の自由に対する過剰な抑制となり得るかどうかという観点から、比例性の原則の適用またはこれに類する思考上の手法によって判断されることになる（説明書の第 103 項参照）。ただし、いずれも評価的な要素（価値判断）を多分に含む要件となっており、裁判官によって判断基準が相当に異なるものとなる可能性があることに留意しなければならない。なお、関連する論文として、原田伸一朗「「わいせつ」コミック裁判の情報メディア論的分析」情報ネットワーク・ローレビュー6 巻 134～149 頁 (2007)がある。

[4] [訳注] 例えば、成人の裸体写真と未成年者の顔の写真とを結合して合成した画像（いわゆる「アイコラ」または「アイドルコラージュ」の場合を含む。）等の場合を指すと解される。このような写真については、児童ポルノ禁止法の適用の問題だけではなく、著作権または著作者人格権の侵害、肖像権の侵害、名誉毀損等の問題も発生し得ることに留意しなければならない。これらの問題の中で、著作権法の適用に関しては、米法におけるフェアユースに関する判例法やパロディと関連する判例法と日本国の裁判所における判断との間に大きな相違があるので、特に注意を要する。知的財産権の問題を含め、関連する論文として、町村泰貴「サイバースペースにおける匿名性とプライバシー（一）」亜細亜法學 34 巻 2 号 71～83 頁 (2000)及び金子敏哉「キャラクターの保護－商標法・不正競争防止法・著作権法を巡る諸論点」パテント 67 巻 4 号 53～63 頁 (2014) がある。

りだしていることは必要ではないが、そのような行為への関与を奨励しまたはそのような行為へと誘惑するために用いられるかもしれず、それゆえに、児童虐待を愛好するサブカルチャーの一部を形成するために用いられるかもしれない行為に対する保護を定めることを目的としている[1]。

103.「権利なく」という用語は、特別の状況下において人を義務から放免する法律上の防御、免責事由、正当化事由またはこれらに類する関連諸原則を排除するものではない。従って、「権利なく」という用語は、加盟国が、思想・信条の自由及びプライバシーのような基本的な権利を考慮に入れることを認めている。加えて、加盟国は、芸術上、医学上、科学上の利点その他これらに類する利点を持つ「ポルノ物」に関連する行為に関する防御を定めることができる[2]。また、第 2 項の(b)に関しては、「権利なく」への参照は、例えば、描写された者が本条の意味における未成年者ではないということが証明された場合には、その者の刑事責任を免責するという要件を加盟国が定めることを認めるものでもある。

104. 第 3 項は、児童ポルノとの関係における「未成年者」という用語について、国際連合の子どもの権利に関する条約（第 1 条）にある「子ども」の定義に従い、一般に、18 歳未満の全ての者を含むものと定義している[3]。年齢に関する統一的な国際基準を設定することは、政策上の重要な事項であると考えられた[4]。この年齢は、性行為の対象としての（現実のまたは

---

[1] [訳注] EU においては「価値観の多様性」を認めているが、全ての価値観を平等に扱うわけではなく、価値観の間に優先劣後や序列または排除の関係が認められる。換言すると、基本的な価値観を基底として承認される価値観についてはその多様性が尊重されるが、基本的な価値観によって排除される価値観は尊重されない。第 102 項は、児童性愛というサブカルチャーを排除するという価値判断を前提としているものと解される。しかし、古代ギリシア～古代ローマの文化史をひもとくと、欧州の文化の基底には明らかに児童性愛が存在している。おそらく、厳格な意味でのキリスト教の教義との関係の中で、古代からのある種の「ヨーロッパ的なもの」が否定されつつある歴史的過程の中にあるのであろう。このような流れは必然的なものと考えられるが、「ヨーロッパ」のアイデンティティの源流を古代のケルト文化に求めるような考え方とは矛盾する要素を含んでいる（比喩的に言えば、ミケランジェロがシスティーナ礼拝堂天井画で描いた力強いイエス・キリストのように「君臨するゼウス」の姿は承認するが、地上の美少女達を次から次へと犯し、自分の子どもを産ませるゼウスとそれに嫉妬するヘラの神話については、それら全てを忘却しようとしている。このような古代ギリシアの神話は、征服者が被征服者の王や王子を殺し、その妻や娘を犯して自分の子どもを産ませ、民衆に対して自己の支配の確立を誇示した時代の記憶をとどめるものとであろうと想像される。）。古代のケルト文化及びその広範な影響に関しては、夏井高人「『懐風藻』の蘭（上）」艸史雑誌 1 巻 1 号 1～66 頁で触れた。

[2] [訳注] 説明書の第 99 項の脚注（訳注）参照

[3] [訳注] 日本国において、成人の年齢を満 20 歳（民法第 4 条）よりも低い年齢とすることが検討されているのは、この文脈との関連性が最も強い。

[4] [訳注] ここでは、児童ポルノをサイバー犯罪の一種として国際的に取り締まることができるようにするための立法政策上の重要事項であるという趣旨で述べられていると解される。なお、一般に、満 18 歳に達すれば、肉体的な意味での繁殖能力が十分なものとなるので、性行為を抑圧するのではなく、積極的に奨励し婚姻させることによって人間の繁殖を促進し、国力を維持・強化したいと考えるのは、どの国の政府でも同じである。すなわち、性交の奨励または抑制は、国家政策（国家による性行為の管理）の一部であり、一般に承認されている社会倫理や道徳観念のようなものとは基本的に無関係なものとなっていることがあり得る。ただし、近未来においては、人間が工場で生産・育成され、生きた人間が子どもを妊娠・出産することはなくなってしまうことが十分に予想される。

虚構の）児童の使用と関係するものであり、それは、性関係のための同意の年齢とは切り離されていることに留意しなければならない。

しかしながら、児童ポルノと関係する国内法の立法においてより低い年齢制限を要件とする一定の国々を考慮し、第 3 項の最後の文言は、加盟国が、16 歳よりも低くないものである限り、異なる年齢制限を要件とすることを認めている。

105. 本条は、児童ポルノに関連する不法な行為について異なるタイプのものを列挙し、第 2 条ないし第 8 条と同様に、「意図的に」実行された場合に犯罪とすることを加盟国に義務付けている。この基準に基づき、児童ポルノの提供、利用可能化、配布、伝送、製造または保有をする意図を有しない者は、刑事責任を問われることはない。加盟国は、より特定された基準によって規律する場合には、その基準を採用することができる（例えば、サービス提供者の責任に関する適用可能な欧州共同体の法律参照[1]）。例えば、伝送される情報または記録保存される情報に対する「認識及び支配」がある場合にのみ、刑事責任を科すことができる。例えば、サービス提供者が、特定の事件において、国内法に基づいて要件とされている意図を持たずに、そのような物を含む Web サイトもしくはニューズルームのための経路を提供し、または、それらをホストしたというだけでは要件を充足しない[2]。更に、サービス提供者は、刑事責任を免れるために、行動を監視することを求められない[3]。

106. 第 4 項は、加盟国に対し、第 1 項の(d)及び(e)並びに第 2 項の(b)及び(c)に関して留保をすることを認めている。同条の各項を適用しない権利は、全部または一部について行うことができる[4]。このような留保は、第 42 条に従い、調印の時点または加盟国の批准書、受諾書、承認書もしくは加入書を寄託する時点において、欧州評議会の事務局長に対し、宣言されなければならない。

---

[1] [脚注] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures、Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')及び Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 等を指すものと解される。日本国の法令では、プロバイダ責任制限法が該当する。

[2] [訳注] 関連する論説として、シュピンドラー・ジェラルト（若林三奈訳）「IT 法における責任」龍谷法学 39 巻 1 号 97～118 頁 (2006)、丸橋透「「青少年有害情報」と民事責任」法とコンピュータ 29 号 65～81 頁 (2011)、同「インターネットとこどもの保護」法とコンピュータ 18 号 61～71 頁 (2000)、千葉直子・藤村明子・高橋克巳「インターネット上の違法有害情報に起因する諸課題と今後の方向性」研究報告コンピュータセキュリティ CSEC 2009(20(2009-CSEC-44))115～120 頁 (2009)、奥村徹「電子媒体上の第三者のデータの没収について」情報処理学会論文誌 46 巻 8 号 2036～2041 頁 (2005)、新保史生「ウェブ・アーカイビングと法」情報の科学と技術 58 巻 8 号 376～382 頁 (2008)、小倉一志「条例によるインターネットの「有害」情報規制」札幌法学 19 巻 2 号 35～54 頁 (2008)がある。

[3] [訳注] データ保持指令 2006/24/EC によるトラフィックデータの保持は、所定の期間内保持するだけであるので、サービスプロバイダが当該トラフィックデータを監視していることになるわけではない。

[4] [訳注] 全部について留保をすることもできるし、どれか一部についてだけ留保をすることもできるという趣旨である。

第 4 款　著作権及び関連諸権利の侵害と関連する侵害行為

著作権及び関連諸権利の侵害と関連する侵害行為（第 10 条）

107. 知的財産権の侵害とりわけ著作権の侵害は、インターネット上においてほとんど最も日常的に実行される侵害行為であり、著作権者とコンピュータネットワークで専門的に仕事をする者の両者に対して関わりを生じさせている。保護された作品を、著作権者の承諾なくしてインターネット上で複製し、配布することが極端に頻繁なものとなっている。そのような保護された作品は、文学作品、写真、音楽作品、視聴覚作品その他の作品を含む。デジタル技術によって無権限の複製をすることが容易であること、電子ネットワークという文脈中での複製及び配布の規模が大きいことの結果として、刑法による制裁に関する条項を盛り込むこと、そして、この分野における国際協力を拡大することが必要となった。

108. 各加盟国は、著作権、並びに、本条に列挙された各合意に基づいて生ずる関連諸権利（時として隣接権として参照される）[1]の故意による侵害行為について、当該侵害行為がコンピュータシステムを用いて商業的な規模で実行された場合に、それを犯罪とすべき義務がある[2]。第 1 項は、コンピュータシステムによる著作権の侵害行為に対する刑事的制裁を規定している。著作権の侵害行為は、既に、ほとんど全ての国において犯罪とされている。第 2 項は、コンピュータシステムによる関連諸権利の侵害を扱っている。

109. 著作権及び関連諸権利の侵害行為は、いずれも、各加盟国の法律で定義するとおりのものであり、そして、国際的の法律文書に関連して各加盟国が約束した一定の義務に従うものである。各加盟国がこのような侵害行為を国内法で定義する方法の詳細は、国によって非常に異なるものとなっているかもしれない。しかしながら、条約に基づいて犯罪とすべき義務は、第 10 条において明確に定めているもの以外の知的財産権の侵害には適用されず、そして、特許権及び商標権と関連する侵害は除外される。

110. 第 1 項との関連で参照されている合意は、文学的及び美術的著作物の保護に関するベルヌ条約に基づく 1971 年 7 月 24 日パリ改正条約、知的財産権の商取引に関連した側面に関する合意（TRIPS 協定）及び世界知的財産機関（WIPO）の著作権条約のことである。第 2 項との関連で引用されている国際的な法律文書は、実演家、レコード製作者及び放送機関の保護のための国際条約（ローマ条約）、知的財産権の商取引に関連した側面に関する合意（TRIPS

[1] [訳注] 原文には括弧はない。読みにくいので、括弧を補って訳した。

[2] [訳注] 日本国の著作権法は、同法第 119 条ないし第 124 条において、著作権の侵害行為等に対する罰則を定めている。サイバー犯罪条約の第 10 条との関係では、日本国の著作権法第 119 条第 1 項が相当しており、同条同項は、「著作権、出版権又は著作隣接権を侵害した者（第 30 条第 1 項（第 102 条第 1 項において準用する場合を含む。第 3 項において同じ。）に定める私的使用の目的をもつて自ら著作物若しくは実演等の複製を行った者、第 113 条第 3 項の規定により著作権若しくは著作隣接権（同条第四項の規定により著作隣接権とみなされる権利を含む。第 120 条の 2 第 3 号において同じ。）を侵害する行為とみなされる行為を行った者、第 113 条第 5 項の規定により著作権若しくは著作隣接権を侵害する行為とみなされる行為を行った者又は次項第 3 号若しくは第 4 号に掲げる者を除く。）は、10 年以下の懲役若しくは 1000 万円以下の罰金に処し、又はこれを併科する」と定めている。

協定）及び世界知的財産機関（WIPO）の実演及びレコード条約である[1]。これら両方の項の中で「約束した義務に従う」という用語を用いているのは、引用した合意の中でこの条約に加盟する加盟国が当事国となっていないものの適用には拘束されないということを明らかにしている。更に、加盟国が留保をした場合、または、各合意中のどれかで認められている宣言をした場合には、その留保によって、この条約に基づく加盟国の義務の範囲を限定することができる。

111. WIPO 著作権条約及び WIPO 実演及びレコード条約は、この条約の締結時点では、まだ発効していなかった[2]。これらの条約は、それでもなお、（とりわけ、インターネット上で、保護された物を「オンデマンド」で「利用可能にする」新たな権利との関連において）知的財産権の国際的な保護を大きくアップデートするものとして重要であり、また、世界中の知的財産権の侵害に対して闘うための手段を向上させるものである。しかしながら、これらの条約により設けられた権利に対する侵害行為については、これらの条約がその加盟国との関係で発効するまでの間は、この条約に基づく侵害行為として処罰できるようにする必要がない、と理解されている。

112. 国際的な法律文書の中で約束した義務に従って著作権及び関連諸権利に対する侵害行を犯罪とすべき義務は、（ベルヌ条約の第 6 条の 2[3]及び WIPO 著作権条約の第 5 条[4]にあるような）上記の法律文書によって授与された人格権には及ばない。

113. 著作権及び関連諸権利の侵害行為について刑事責任を負わせるためには、「故意に」実行されるものであることを要する。著作権の侵害を犯罪とすべき義務を定める TRIPS 協定

---

[1] [訳注] これらの著作権と関連する条約の日本語訳の大部分は、公益社団法人著作権情報センターの Web サイト上で公開されている。

[2] [訳注] WIPO 著作権条約の発効日は、2002 年 3 月 6 日である。WIPO 実演及びレコード条約の発効日は、2002 年 5 月 20 日である。

[3] [訳注] ベルヌ条約（Convention de Berne pour la protection des œuvres littéraires et artistiques）の第 6 条の 2 第 1 項は、「Indépendamment des droits patrimoniaux d'auteur, et même après la cession desdits droits, l'auteur conserve le droit de revendiquer la paternité de l'œuvre et de s'opposer à toute déformation, mutilation ou autre modification de cette œuvre ou à toute autre atteinte à la même œuvre, préjudiciables à son honneur ou à sa réputation（著作者は、その財産的権利とは別個に、この権利が移転された後においても、著作物の創作者であることを主張する権利及び著作物の変更、切除その他の改変又は著作物に対するその他の侵害で自己の名誉又は声望を害するおそれのあるものに対して異議を申し立てる権利を保有する）」と定めている（日本語訳は、公益社団法人著作権情報センターの訳による。）。

[4] [訳注] WIPO 著作権条約（WIPO Copyright Treaty）の第 5 条は、データベースの著作物に関するもので「Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation（素材の選択又は配列によって知的創作物を形成するデータその他の素材の編集物は、その形式のいかんを問わず、知的創作物として保護される。その保護は、当該データその他の素材自体に及ぶものではなく、また、当該編集物に含まれるデータその他の素材について存在する著作権を害するものでもない）」と定めている（日本語訳は、公益社団法人著作権情報センターの訳による。）。説明書の第 112 項がどのような意図で WIPO 著作権条約の第 5 条を引用しているのかについては、不明である。

（第 61 条）において用語として用いられていることから、この条約にある他の全ての実体法条項とは対照的に、第 1 項及び第 2 項中では、「意図的に」の代わりに「故意に[1]」という用語が用いられている。

114. これらの条項は、「商業的規模」の、かつ、コンピュータシステムによる侵害に対して刑事的制裁を定めようとするものである。これは、「商業的規模の海賊行為」の場合についてのみ著作権関連事項に刑事的制裁を要求する TRIPS 協定の第 61 条に沿うものである。しかしながら、加盟国は、「商業的規模」という閾値を超えることが認められ、かつ、他のタイプの著作権侵害についても処罰することができる[2]。

115. 「権利なく」という用語は、冗長だとして、本条の条文からは削除された。それは、「侵害」という用語が、承認なく、著作権のある物を使用することを既に意味しているからである。「権利なく」という用語が存在しないということは、反対解釈として、条約の中に「権利なく」という用語がある場合[3]と関係している刑事責任に関する刑法上の抗弁事由、正当化事由及び刑事免責を規律する諸原則の適用を排除するものではない。

116. 第 3 項は、加盟国に対し、民事上及びまたは行政上の措置を含め、他の効果的な救済手段が利用可能である限りにおいて、「限定された状況」（例えば、並行輸入、貸与権）において、第 1 項及び第 2 項の刑事責任を負わせないことを認めている。本条は、基本的に、刑事責任を負わせる義務について、限定された例外規定を持つことを認めている。ただし、これは、ミニマムの既存の犯罪行為化要求である TRIPS 協定の第 61 条に基づく義務を緩和するものではない。

117. 本条は、いかなる意味においても、国内法及び国際的な合意に適合する基準に合致しない者に対抗するために、著者、映画製作者、実演家、写真製作者、放送機関その他の権利者に対し付与された保護を拡張するものと解釈してはならない。

---

[1] [訳注] 原文は、「wilfully」となっている。「故意に」との訳語は、経済産業省の訳に基づく。「wilfully」との表現は、サイバー犯罪条約の第 10 条のみに見られるものである（他の刑事実体法条項においては、「intentionally」となっている。）。この表現は、説明書の第 113 項にもあるとおり、TRIPS 協定の第 61 条に基づくものである。同条には、「Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale（加盟国は、少なくとも故意による商業的規模の商標の不正使用及び著作物の違法な複製について適用される刑事上の手続及び刑罰を定める）」及び「Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale（加盟国は、知的所有権のその他の侵害の場合、特に故意にかつ商業的規模で侵害が行われる場合において適用される刑事上の手続及び刑罰を定めることができる）」とある（日本語訳は、経済産業省の訳による。）。「wilful」及び「wilfully」は、国際的な法律文書である TRIPS 協定の中で公式に用いられているものであるため、サイバー犯罪でもそれに準拠することとしたものと考えられる。一般に、「wilful」及び「wilfully」は、「intentional」及び「intentionally」と全く同じ意味をもつ。

[2] [訳注] 日本国の著作権法に定める罰則の現実の運用においては、「商業的規模」ではないかなり些細な行為まで起訴され有罪とされている。このことは周知のとおりである。

[3] [訳注] 説明書の第 38 項参照

第 5 款　付随的責任及び制裁

未遂及び教唆または幇助（第 11 条）

118. 本条の目的は、条約中に定義する侵害行為の実行の試み、幇助または教唆と関連する付加的な侵害行為を設けることにある。以下で更に述べるとおり、条約に設けられる侵害行為の実行を試みる行為の全てについて、加盟国が、犯罪とすることが求められているわけではない[1]。

119. 第 1 項は、加盟国に対し、第 2 条ないし第 10 条に基づく侵害行為の全てについて、その実行の幇助行為または教唆行為を犯罪行為として設けることを求めている。条約の中に設けられる犯罪を実行する者が、その犯罪の実行を意図する第三者によって支援される場合には、その幇助行為または教唆行為は、刑事責任を発生させる。例えば、インターネットを介して危険なコンテントや悪意あるコードの転送をするには、経路としてのサービス提供者の支援が必要であるが、犯罪的な意図を有しないサービス提供者は、本節に基づく責任を負うことはない[2]。そして、サービス提供者は、本条に基づく刑事責任を免れるために、積極的に監視をすべき義務を負わない[3]。

120. 未遂に関する第 2 項については、条約中に定義する侵害行為中の幾つかまたはこれらの犯罪構成要件中の幾つかを試みることが理論的に困難であると認識された（例えば、児童ポルノの提供行為もしくは利用を可能とする行為の要件）。そのために、第 3 条、第 4 条、第 5

---

[1] [訳注] 日本国の刑法では、教唆犯及び幇助犯が成立する罪を限定せず、全ての罪について成立するように一般的な教唆及び幇助の構成要件を定めている。すなわち、第 61 条第 1 項は、「人を教唆して犯罪を実行させた者には、正犯の刑を科する」と定め、同条第 2 項は、「教唆者を教唆した者についても、前項と同様とする」と定め、第 62 条第 1 項は、「正犯を幇助した者は、従犯とする」と定め、同条第 2 項は、「従犯を教唆した者には、従犯の刑を科する」と定め、そして、第 63 条は、「従犯の刑は、正犯の刑を減軽する」と定めている。ただし、同法第 64 条は、「拘留又は科料のみに処すべき罪の教唆者及び従犯は、特別の規定がなければ、罰しない」と定めている。

[2] [訳注] サービス提供者の法的責任との関係で、当該プロバイダの管理化にあるサーバ上で行われる違法行為に何も対処しなかったことが不作為による法的責任の有無が議論されてきた。この点に関する論文として、島田聡一郎「不作為による共犯について（一）」立教法学 64 号 1～79 頁 (2003)、同「不作為による共犯について（二・完）」65 号 218～316 頁 (2004)、石井徹哉「アクセスプロバイダの刑事責任(1)－ドイツテレサービス法における展開－」千葉大学法学論集 20 巻 4 号 33～68 頁 (2006)、上野幸彦「日常行為と可罰的幇助」日本法學 77 巻 1 号 63～115 頁 (2011)及び吉田敏雄「不作為犯の体系と構造（九・完）」北海学園大学法学研究 46 巻 2 号 451～496 頁 (2010)がある。

[3] [訳注] ここで述べられていることは、サイバー犯罪条約に定める犯罪行為として処罰されないようにするためにインターネットサービスプロバイダ（ISP）等が監視義務を負うものではないという趣旨である。しかし、民事上の責任については異なる考察をすべき場合がある。特に、ISP の利用契約において、一定の範囲内にあるマルウェアや侵入手口の監視を行って安全を確保することが契約内容となっている場合には、当該契約の本旨に従い、標準的なレベルでの監視を実施するのでなければ債務不履行（不完全履行）に基づく損害賠償責任を負うことがあり得る。利用者との間の契約による場合のほかに、行政法上の監視義務がある場合や条理上の義務に基づき、利用者に対しても何らかの損害賠償責任が発生し得ることがあり得る。

条、第 7 条、第 8 条、第 9 条第 1 項の(a)及び第 9 条第 1 項の(c)に従って設けられる侵害行為に関してのみ、その未遂行為を犯罪とすることが求められている。

121. 条約に従って設けられる侵害行為の全てに関して、その未遂行為、幇助行為または教唆行為は、意図的に実行されるものであることを要する[1]。

122. 第3項は、未遂条項から特定の場合を除外しようとする第2項での努力にもかかわらず、異なる立法例中において非常に広範で態様の異なる概念が存在することに鑑み、第 2 項を採択する際の加盟国の困難を回避するために付加された。加盟国は、第 2 項の全部または一部を適用しない権利を留保すると宣言することができる。このことは、本条によって留保をする加盟国は、未遂行為を犯罪とする義務を全く負わないということを意味し、また、未遂行為について刑事制裁を課すべき侵害行為を選択することができ、あるいは、侵害行為の一部について刑事制裁を課すこともできるということを意味する。留保は、加盟国が各国の基本的な法律概念を維持したままで、広く条約の批准をすることができるようにすることを目的としている。

企業の責任（第 12 条）

123. 第 12 条は、法人の責任を扱っている。企業の責任を認めることは、近時の法律の傾向と適合している[2]。これは、当該法人の利益のために実行される場合、当該法人の中で主動的

[1] [訳注] ファイル共有システム Winny を作成・提供する行為が著作権法違反の罪の幇助となるか否かについて争われた事案について、最高裁平成 23 年 12 月 19 日決定・刑集 65 巻 9 号 1380 頁は、幇助の故意を欠くとして判示している。同最高裁決定及び原審である大阪高裁平成 21 年 10 月 8 日判決については、「適法用途にも著作権侵害用途にも利用できるファイル共有ソフト Winny をインターネットを通じて不特定多数の者に公開,提供し,正犯者がこれを利用して著作物の公衆送信権を侵害することを幇助したとして,著作権法違反幇助に問われた事案につき,幇助犯の故意が欠けるとされた事例[第三小法廷平成 23.12.19 決定] （最高裁判所判例解説：平成 23 年 12 月分 平成 24 年 2,4 月分 平成 25 年 2 月分）」法曹時報 66 巻 10 号 2917～2987 頁 (2014)、矢野直邦「適法用途にも著作権侵害用途にも利用できるファイル共有ソフト Winny をインターネットを通じて不特定多数の者に公開、提供し、正犯者がこれを利用して著作物の公衆送信権を侵害することを幇助したとして、著作権法違反幇助に問われた事案につき、幇助犯の故意が欠けるとされた事例」Law & technology 55 号 69～77 頁 (2012)など、多数の判例評釈等が公表されている。他に関連する判例評釈として、池田秀敏「著作権侵害とインターネット掲示板管理者の責任「ファンブック　罪に濡れたふたり～Kasumi～」事件・控訴審判決　東京高等裁判所平成 17 年 3 月 3 日判決）（判例時報 1893 号 126 頁、判例タイムズ 1181 号 158 頁）信州大学法学論集 7 号 195～220 頁 (2006)がある。

[2] [訳注] この部分の記述は、企業統治（cooperative governance）及び内部統制（internal control）と関係している。これらに関しては、吉田夏彦「CSR 論の展開と課題」憲法論叢 20 号 91～118 頁 (2014)、藤川信夫「英国 Senior Management Regime とコーポレート・ガバナンス・コード： 上級管理者能力(SMFs)と非業務執行取締役ならびに取締役会評価」千葉商大論叢 53 巻 1 号 173～194 頁 (2015)、同「英国スチュワードシップ・コードの理論と実践 : Approved persons と域外適用ならびに監査等委員会と非業務執行取締役、米国の忠実義務の規範化概念と英国会社法の一般義務等の接点」同誌 52 巻 1 号 75～144 頁 (2014)、村田大学「ドイツ企業におけるコンプライアンス担当者の独立性と権限」年報財務管理研究 24 号 26～37 頁 (2013)、南保勝美「取締役の責任軽減の法理ーその批判的検討ー」法律論叢 74 巻 4・

な立場にある者によって実行される犯罪行為について、会社、社団その他これに類する法人に対して、責任を負わせようとするものである。また、第 12 条は、当該法人の労働者もしくは代理人の監督または管理についてそのような主動的な者に誤りがあり、そして、その誤りによって、条約で設けられる犯罪中のどれかがその労働者または代理人による実行が促進されたような場合についても、責任を負わせることを考慮に入れている。

124. 第 1 項に基づき、責任を負わせるためには、4 つの要件に合致しなければならない。第 1 に、条約に規定する侵害行為の中の 1 つが実行されたのでなければならない。第 2 に、その侵害行為は、法人の利益のために実行されたのでなければならない。第 3 に、主動的な地位にある者によってその犯罪行為が実行されたのでなければならない（幇助及び教唆を含む。）。「主導的な地位にある者」という用語は、取締役のように、組織の中での高い地位を有する自然人のことを指す。第 4 に、主導的な地位にある者は、その権限（代表権、決定権または管理権）に基づいて行動したのでなければならず、それは、そのような実際の人間が、法人の責任と関係する彼または彼女の権限の範囲内で行動したということを示すものでなければならない。まとめると、第 1 項は、加盟国に対し、そのような主導的立場にある者によって実行された侵害行為についてのみ、法人に対して責任を負わせることができるようにすることを義務づけている。

125. 加えて、第 2 項は、加盟国に対し、第 1 項に規定する主導的立場にある者によって犯罪が実行されたわけではないが、それ以外の者（例えば、その権限の範囲内で行動するその法人の従業者や代理人中の 1 人）によって、法人の権限に基づいて実行された場合において、法人に対して責任を負わせることができる能力を持つことを義務づけている。責任を負わせるためには、(1)その法人の従業者または代理人によって侵害行為が実行され、(2)法人の利益のために侵害行為が実行され、かつ、(3)主導的な地位にある者が、その従業者または代理人に対する監督に失敗したことによってその侵害行為が可能となったという各要件が充足されなければならない。この文脈において、監督の失敗は、その法人の代わりに従業者または代理人が犯罪行為を実行することを防止するための適切かつ合理的な措置を講ずることの失敗を含むものと解釈されなければならない[1]。そのような適切かつ合理的な措置は、企業の

---

5 号 243～278 頁、柿崎環「Dodd & Frank 法における内部告発者報奨金プログラムとその資本市場規制的意義」証券経済研究 76 号 63～81 頁 (2011)、企業会計審議会「財務報告に係る内部統制の評価及び監査に関する実施基準について（意見書）」（平成 23 年 3 月 30 日）が参考になる。

[1] [訳注] 日本国の会社法第 362 条第 4 項第 6 号は、取締役会が取締役に委任できない事項の 1 つとして「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務並びに当該株式会社及びその子会社から成る企業集団の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」を定め、同法 399 条の 13 第 1 項第 1 号ハは、監査等委員会設置会社の取締役会の職務として、「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務並びに当該株式会社及びその子会社から成る企業集団の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」と定め、同法 416 条第 1 項第 1 号ホは、指名委員会等設置会社の取締役会の職務として、「執行役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務並びに当該株式会社及びその子会社から成る企業集団の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」と定めている。また、金融商品取引法第 24 条の 4 の 4 第 1 項は、「内部統制報告書」の提出について定めている。

形態、その規模、標準または事業遂行上の確立されたベストプラクティス等々といったような様々な要素[1]によって決定され得る。このことは、労働者の通信の一般的な監視体制の構築を要求するものと解釈してはならない（第 54 項参照）。サービス提供者は、顧客、利用者、従業者その他の第三者によってそのシステム上で犯罪が実行されたという事実があっても、そのために責任を負うことはない。なぜならば、「その権限に基づいて行動」という用語は、その権限の範囲内で行動する従業者または代理人に対してのみ適用されるからである。

126. 本条に基づく責任は、刑事責任、民事責任または行政法上の責任のいずれかとすることができる。各加盟国は、第 13 条第 2 項の基準、すなわち、「効果的であり、比例的であり、かつ、抑止効果のある」制裁または措置であり、かつ、金銭的な制裁を含む、という基準に適合するものである限り、各加盟国の法原則に従い、これらの形態による責任のいずれかまたはその全部を定めるための選択の柔軟性を有している[2]。

127. 第 4 項は、法人の責任が個人の責任を排除するものではないということを明らかにしている[3]。

制裁及び措置（第 13 条）

128. 本条は、第 2 条ないし第 11 条と密接に関連している。これらの条項では、刑法に基づいて処罰されるべき様々なコンピュータ犯罪またはコンピュータと関連する犯罪を定義している。これらの条項によって課される義務に従い、本条は、締約国に対し、「効果的であり、比例的であり、かつ、抑止力のある[4]」刑事制裁を定めることによって、これらの侵害行

[1] [訳注] 企業の法令遵守のための国際標準として、ISO 26000（社会的責任に関する手引）がある。

[2] [訳注] 日本国の法制においては、関連する様々な行政法上の制裁措置のほか、民法第 715 条所定の使用者責任の条項が存在する（説明書の第 129 項参照）。

[3] [訳注] 会社法の第 423 条第 1 項は、「取締役、会計参与、監査役、執行役又は会計監査人（以下この節において「役員等」という。）は、その任務を怠ったときは、株式会社に対し、これによって生じた損害を賠償する責任を負う」と定めている。同法 596 条は、業務を執行する社員の持分会社に対する損害賠償責任について定めている。また、同法第 429 条第 1 項は、「役員等がその職務を行うについて悪意又は重大な過失があったときは、当該役員等は、これによって第三者に生じた損害を賠償する責任を負う」と定め、同条第 2 項は、取締役及び執行役、会計参与、監査役、監査等委員及び監査委員並びに会計監査人について、「当該各号に定める行為をしたときも、前項と同様とする。ただし、その者が当該行為をすることについて注意を怠らなかったことを証明したときは、この限りでない」と定め、同法第 430 条は、「役員等が株式会社又は第三者に生じた損害を賠償する責任を負う場合において、他の役員等も当該損害を賠償する責任を負うときは、これらの者は、連帯債務者とする」と定めている。同法第 487 条及び第 653 条は、清算人について、同法 597 条は、業務を執行する有限責任社員について、同様の第三者に対する損害賠償責任を定めている。

[4] [訳注] Roger J. Goebel, The Court of Justice's Third Stage of Enforcement Rules Implementation, Compliance and Effectiveness: Emerging Issues on Compliance and Effectiveness within the European Union, American Society of International Law (ASIL) Proceedings pp.159-164 (1997) によれば、「effective, proportionate and dissuasive」は、判例法によって成立した概念とされている。なお、欧州連合の機能に関する条約（TFEU）の第 83 条第 2 項（統合前の欧州連合条約第 31 条第 2 項）に基づいて制定された Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse

為の深刻さに相応する責任を負わせ、かつ、自然人の場合には、拘禁刑を定めることを求めている。

129. 第 12 条に従って設けられる責任を負う法人は、「効果的であり、比例的であり、かつ、抑止力のある」制裁に服さなければならない。この制裁は、その性質上、刑事制裁、行政上の制裁または民事上の制裁のいずれであってもよい[1]。締約国は、第 2 項の規定に基づき、法人に対しは、金銭的制裁を課すことができるよう定めることが要求される。

130. 本条は、犯罪行為の深刻さの程度に応じて他の制裁を課すことができる余地を残している。例えば、措置は、差止命令や没収[2]を含むことができる。加盟国は、既存の国内法システムと互換性がとれるように、犯罪行為及び制裁のシステムを構築する裁量権を認められている。

---

directive) の第 7 条第 1 項は、「Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by effective, proportionate and dissuasive criminal penalties」と規定している。TFEU の第 83 条第 2 項は、「If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same ordinary or special legislative procedure as was followed for the adoption of the harmonisation measures in question, without prejudice to Article 76」と規定している。

[1] [訳注] 関連する文献として、真島信英「行政罰たる過料による制裁のあり方をめぐる研究ーわが国とドイツの過料手続に関する比較研究を中心としてー」亜細亜法學 49 巻 1 号 25～42 頁 (2014)、神例康博「法人処罰における過失責任法理の限界ー事業主責任論の再検討ー(1)」松山大学論集 13 巻 2 号 138～108 頁 (2001)、同「法人処罰における過失責任法理の限界ー事業主責任論の再検討ー(2・完) 」同誌 13 巻 3 号 124～93 頁 (2001)、瀬谷ゆり子「金融商品取引規制のエンフォースメントー課徴金制度の役割ー」桃山法学 15 号 239～263 頁 (2010)、逸見真「ISM コードの求める会社の責任への対応ーわが国における法人（会社）処罰の問題点ー」日本航海学会論文集 124 号 159～168 頁 (2011)、鈴木孝之「独占禁止法における刑事罰制度の機能」白鴎大学法科大学院紀要 4 号 33～52 頁 (2010) がある。

[2] [訳注] 犯罪により得た利益の没収及び追徴に関しては、刑法第 19 条及び第 19 条の 2 に一般的な規定があるほか、犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号）がある。FATF（Financial Action Task Force）の勧告に基づく同法の近時の改正については、尾嵜亮太「「犯罪による収益の移転防止に関する法律の一部を改正する法律」の概要」警察学論集 68 巻 4 号 8～25 頁 (2016)、同「犯罪による収益の移転防止に関する法律施行令等の一部改正について(1)」同誌 69 巻 2 号 72～90 頁 (2016)、同「犯罪による収益の移転防止に関する法律施行令等の一部改正について(2)」同誌 69 巻 3 号 108～128 頁 (2016)、同「犯罪による収益の移転防止に関する法律施行令等の一部改正について(3)」同誌 69 巻 4 号 89～112 頁 (2016)、同「犯罪による収益の移転防止に関する法律施行令等の一部改正について(4)」同誌 69 巻 5 号 121～132 頁 (2016)、同「犯罪による収益の移転防止に関する法律施行令等の一部改正について(5)」同誌 69 巻 6 号 134～141 頁 (2016)、同「犯罪による収益の移転防止に関する法律施行令等の一部改正について(6・完)」同誌 69 巻 7 号 84～115 頁 (2016)が参考になる。関連するものとして、田中健太郎「アメリカ合衆国及びイタリア共和国におけるマネーロンダリング規制に関する現金決済規制と有罪判決によらない犯罪収益等の没収制度について（上）」警察学論集 67 巻 12 号 157～167 頁 (2014)、同「アメリカ合衆国及びイタリア共和国におけるマネーロンダリング規制に関する現金決済規制と有罪判決によらない犯罪収益等の没収制度について（下）」同誌 68 巻 1 号 81～108 頁 (2015)、奥野省吾「英国における犯罪収益対策の最近の動向ー2002 年犯罪収益法を中心にー」同誌 58 巻 5 号 100～141 頁 (2005)がある。

第 2 節　手続法

131. 本節の各条項は、第 1 節の中に設けられる侵害行為の犯罪捜査のため、コンピュータシステムによって実行されるその他の犯罪行為の犯罪捜査のため、そして、犯罪行為の電子的な形態による証拠収集のために、各国のレベルで講じられる一定の手続上の措置を定める。第 39 条第 3 項[1]に従い、条約中のいかなる条項も、加盟国に対し、この条約に含まれるもの以外の権限または手続を要求または勧奨するものではなく、また、加盟国がそのようにすることを妨げるものでもない。

132. 「電子ハイウェイ[2]」を取り巻く技術革新は、共通の伝送媒体及びキャリアの共有を介して、夥しく多種多様な形態の通信やサービスを相互に関連付け、または、相互に接続させるものである。それは、刑事法及び刑事手続の様相を一変させてしまった。止まることなく拡張し続ける通信ネットワークは、在来型の侵害行為と新たな技術犯罪の双方に関連する犯罪活動に対して新しいドアを開いている[3]。刑事実体法だけではなく、刑事手続法及び捜査技術もまた、これらの新たな侵害行為に遅れをとらないようにしなければならない。それと同時に、新たな技術環境及び新たな手続権限に対応して、安全性確保措置もまた導入または開発されなければならない[4]。

---

[1] [訳注] サイバー犯罪条約第 39 条第 3 項は、「この条約のいかなる規定も、締約国が有する他の権利、制限、義務及び責任に影響を及ぼすものではない」と定めている（外務省訳）。

[2] [訳注]「電子ハイウェイ（electronic highway）」は、「情報スーパーハイウェイ（Information Superhighway）」と同じ意味で用いられていると解される（第 8 項参照）。関連する文献として、Mark Goldstein & Richard Z. Gooding, Electronic Highway Infrastructure Development and Information Services, International Research Center (1997)がある。

[3] [訳注] この参考訳の冒頭の参考文献欄中に示してある情報犯罪者と関連する文献ないしハッカーまたはハッキング（クラッキング）と関連する文献の多くは、1980 年代から 1990 年代のものである。当時、警察・検察当局のみならず、経済界や社会一般においても情報犯罪の脅威が強く意識されるようになったことの証の 1 つでもある。一般に、非常に便利な情報技術は、常に、情報犯罪者やサイバー攻撃者にとっても非常に便利な技術である。そして、情報技術の普通の利用者は、標準的な用法に従った利用しかしないのに対し、情報犯罪者やサイバー攻撃者は、コストや時間を無視してでも、当該情報技術を徹底的に使いこなし、想定外の用法による使用を試み、当該情報技術に含まれている脆弱性や欠陥を発見してそれを悪用・濫用することができるという一般的な特質（非対称性）が存在する。

[4] [訳注] 第 15 条のことを指している。一般に、技術的な安全性確保措置すなわち防護措置（safeguards）としては、暗号技術の開発・導入、関係する警察職員や諜報機関担当者を監視する技術の導入、証拠である電子データの非改竄技術の導入等が考えられる。ただし、現実には、例えば、米国の Snowden 事件にもみられるように、担当職員に対する監視技術が期待されているような効果をあげることができない場合があることも事実である。他方、捜査担当者に対する監視技術や証拠である電子データの非改竄技術が導入されていない組織では、例えば、大阪地検特捜部の主任検事によるフロッピーディスクのデータ改竄事件のような出来事が容易に発生し得る。この事件では、大阪地裁は、2011 年 4 月 12 日、元主任検事に対し、懲役 1 年 6 月の刑を宣告した。

枠組み決定 2008/977/JHA 及びその改正法である指令(EU)2016/680 並びに指令(EU)2016/681 は、法執行機関（警察）、法務当局及び入管当局が保有する個人データと関連するデータ主体の利益を確保するためのデータ保護監督機関の関与を定めるものであるが、これは、データ主体の利益のための社会的（組織的）な安全性確保措置として理解することもできる。特にデータ保持指令 2006/24/EC のような

133. ネットワーク化された環境における犯罪との闘いにおける主要な問題の 1 つは、加害者を特定するのが困難であること、そして、犯罪行為の広がり及び影響の度合いを評価するのが困難であることである。より大きな問題は、秒単位で修正され、移動されまたは削除されるかもしれない電子データの浮動性によって惹起される。例えば、データを管理している利用者は、犯罪捜査の対象となっているデータを消去するためにコンピュータシステムを使用するかもしれないが、それによって、証拠が破壊されてしまう。速度は、そして、時として機密性は、しばしば、捜査を成功させるための死命線である。

134. 条約は、新たな技術環境のために、捜索または押収といったような在来型の捜査手段を採用した。加えて、捜索または押収といったような在来型の証拠収集手段が浮動的な技術環境においてもなお有効なものであるようにするために、データの応急の保全のような新たな手段が創設された。新たな技術環境におけるデータは、常に固定的なものではなく、通信プロセスの中で流動するかもしれないことから、通信プロセスの中にある電子データの収集を許容するために、トラフィックデータのリアルタイム収集、コンテントデータの傍受といったような通信と関係する他の在来型の証拠収集手続もまた採用されなければならなかった。これらの捜査手段の中の幾つかは、情報技術と関連する刑事手続法上の諸問題に関する欧州評議会の勧告 No. R (95) 13[1]の中で既に定められている。

135. 本節の中で示す全ての条項は、特定の犯罪捜査または特定の刑事手続のためのデータの入手または収集を許容することを目的としている。この条約の起草者は、条約によって、サービス提供者に対し、一定の確定された期間内、トラフィックデータの定期的な収集及び保持の義務を課すべきかどうかについて意見交換をしたが、合意を得ることができなかったため、そのような義務を盛り込まなかった[2]。

136. 刑事手続は、一般に、全てのタイプのデータと関係している。それらは、（トラフィックデータ、コンテントデータ及び加入者データという）3 種類の特定のタイプのコンピュータデータを含むものであり、それらは、（記録保存された通信及び通信のプロセスという[3]）2 つの形態で存在し得る。これらの用語中の幾つかの定義は、第 1 条及び第 18 条で定められている。特定のタイプまたは形態の電子データについて手続を適用できるかどうかは、各条項中に個別に規定されているデータの性質及び形態並びに手続の性質によって定まる。

137. 新たな技術環境へ在来型の手続法を接ぎ木する際において、用語の適切性という問題が本節の条項中に生じている。選択肢には、在来型の言葉（「捜索」及び「押収」）を維持する

法令に基づき法執行機関等による包括的なトラフィックデータの収集が行われる場合には、データ保護監督官の関与が社会的・政治的に大きな意味をもち得る。また、指令(EU)2016/1148 は、情報セキュリティにおけるインシデント処理との関係でのデータ保護監督官の関与を認めるものである。なお、枠組み決定 2008/977/JHA 及び指令(EU)2016/680、指令(EU)2016/681 並びに指令(EU)2016/1148 については、夏井高人「欧州連合の構成国における独立の個人データ保護監督官の職務」法律論叢 89 巻 6 号掲載予定で述べた。

[1] [訳注] 説明書の第 10 項及び第 11 項参照

[2] [訳注] EU においては、後に、データ保持指令 2006/24/EC が制定された。ただし、2014 年 4 月 8 日、欧州司法裁判所において、同指令を無効とする先決裁定がなされた（C-293/12 and C-594/12）。

[3] [訳注] 前者は、時期ディスク等の何らかの記録媒体に固定的に記録保存された通信内容のことを指し、後者は、通信回線を流れている通信内容のことを指す。

こと、(G8 ハイテク犯罪対策小委員会[1]のような) 他の国際的な場の文書中において主題として採用されているようなコンピュータ用語を志向する新たなより技術的な用語（「アクセス」及び「複製」）を用いること、または、混合語（「捜索またはこれに類するアクセス」及び「押収またはこれに類する確保」）を用いるという妥協策が含まれる。電子的な環境においては、概念の進化を反映する必要性があると同時に、その概念の本来の由来を識別し維持する必要性があるため、各国が「捜索及び押収」という古い概念と「アクセス及び複製」という新しい概念のいずれの使用も許容するという柔軟性のある手法が採用されている。

138. 本節中の全ての条項は、「職務権限を有する機関[2]」及び特定の犯罪捜査及び刑事手続のためにそれらの行政機関に対して付与される権限と関係している。ある国では、裁判官のみ

[1] [訳注] 外務省は、「G8/G7 においては，G8/G7 各国の刑事司法や法執行等の専門家によって構成される通称リヨン・グループが中心となって，テロ対策の専門家会合であるローマ・グループと合同で，実務的な観点から，国際組織犯罪対策と同分野における国際協力を検討してきており，G8/G7 首脳等に対して，その成果や検討事項等について報告を行ってきています。近年では，児童ポルノやハイテク犯罪，腐敗対策をはじめ，組織犯罪に有効に対処するための捜査手法や司法協力のあり方などについて議論を行っています」と解説している。リヨン・グループは、1997 年に設置された。2001 年 5 月 24 日に日本国（東京）で開催された G8 ハイテク犯罪対策小委員会の会合においては、データ保持（Data Retention）に関して、「Discussion of costs and priorities in terms of resources and business opportunity; Examination of the variety of services, business models and service providers currently in existence; Discussion of practices for data retention taking into consideration legal technical, financial and privacy issues」との事項が、データの保全（Data Preservation）に関して、「Development of a checklist for law enforcement to use when making requests for preservation of data; Development of a list of issues to be considered in a legal framework for data preservation; Discussion of conflicts of laws and jurisdictional issues that can hinder provider cooperation with a preservation request; Development of best practices for law enforcement and industry concerning data preservation」との事項が、そして、脅威の評価及び防止（Threat assessment and prevention）に関して、「Prevention of computer-assisted crimes and computer network attacks requires close cooperation between private and public sectors; Prevention of content related threats can be handled only at end-user level, due to technical and legal reasons; Governments have to be involved more in raising awareness of all users in Information Technology security; Common practices in the G8 and non-G8 countries too, should be identified, and domestic taxonomies of threats be interoperable; Countries should establish mechanisms to aggregate statistics and bring out an accurate picture of high-tech crimes and their impact on the different areas of society.」との事項が議題とされた。

[2] [訳注] 一般に、「職務権限を有する機関（competent authorities）」とは、一般に、法執行機関（警察）や法務当局のことを指し、司法機関及び一般行政事務を掌理する行政機関を含まない（それゆえ、他の参考訳では「職務権限を有する行政機関」との訳語も用いている。）。日本国の行政機関では、法務省（刑事局）、検察庁、警察庁及び都道府県警察等が相当する。法執行機関（警察）が保有する捜査記録中の個人データや法務当局が管理・保存する前科・前歴データ中の個人データの法的保護について定める指令(EU)2016/680 では、原則として、法執行機関及び法務当局に限定された意味を有するものとして「competent authorities」との語が用いられている。しかし、第 139 項で説明されているとおり、サイバー犯罪条約においては、司法機関（裁判所）を含む趣旨で「competent authorities」との語が用いられていることに留意しなければならない。これは、世界各国の法制が異なるため、最も広い理解に基づくものとしてこの概念を採用したことによるものと思われる。それゆえ、EU の他の指令や規則を解釈する際には、当該指令や規則の立法趣旨や全体の構成を丁寧に考察した上で、個別にその概念内容を確定する必要がある。その意味で、「competent authorities」との語について日本語訳を作成する場合には、統一的・固定的な訳語（対応する日本語）が成立しないことになる。

が証拠の収集または提出命令を発する権限または許可の権限を有しているのに対し、他の国では、検察官その他の法執行機関が同様の権限を委任されている。従って、「職務権限を有する機関」とは、特定の犯罪捜査または刑事手続に関して証拠を収集し、または、提供を求めるために、国内法によって、刑事手続上の措置の執行を命令し、許可し、または、それを実施する権限を授与されている司法機関[1]、行政機関[2]またはその他の法執行機関のことを指す。

第 1 款　共通規定

139. この節は、手続法と関連する全ての条項に適用される一般的な性質を有する 2 つの条項で始まっている。

手続条項の適用範囲（第 14 条）

140. 各加盟国は、各国の国内法及び法的枠組みに従い、「特定の犯罪捜査または刑事手続[3]」のために、この節に定める権限及び手続を設ける上で必要な立法及びその他の措置を採るべき義務を負う。
141. 2 つの例外に従い、各加盟国は、(i)条約の第 1 節に従って設けられる犯罪行為、(ii) コン

[1] [訳注] 日本国の刑事訴訟法においては、現行犯逮捕のような特別の場合を除き、原則として、裁判所が発する令状によらなければ、捜査機関が逮捕、捜索、押収等の強制処分を実施することができない。これらの強制処分のための令状は、許可状としての性質を有すると解するのが通説である。その限りにおいて、日本国においても、裁判所は、犯罪捜査において「職務権限を有する機関（competent authorities）」の一種である。しかし、裁判所は、許可と命令とは異なる。命令の場合には、発令をした裁判所が当該令状を執行する。これに対し、許可の場合には、許可を受けた法執行機関が当該令状を執行するのであって、裁判所が執行するのではない。その意味では、日本国を含め、裁判所による許可制を採用している国では、裁判所は、捜査段階における「職務権限を有する機関（competent authorities）」の一種ではない。なお、起訴後の公判の段階において、裁判所が職権で発令する各種強制処分は命令の一種である（命令である以上、裁判所がそれを執行する。）。それゆえ、日本国の刑事訴訟法の解釈においては、捜査段階における捜査機関による強制処分であるのか、それとも、公判の段階での裁判所による強制処分であるのかを明確に分けて理解しなければならない。

[2] [訳注] 日本国における検察庁及び警察庁所管の行政機関以外の行政機関では、海上保安官（海上保安庁）、麻薬取締官（厚生労働省）、麻薬取締員（都道府県）、労働基準監督官（厚生労働省）、漁業監督官（水産庁）等の特別司法警察職員（刑事訴訟法第 190 条）が「職務権限を有する機関（competent authorities）」としての「行政機関」に該当する（前掲松尾浩也監修『条解刑事訴訟法（第 4 版）』360～361 頁参照）。

[3] [訳注] データの保持（retention）のように特定の事件に限定されることなく全ての案件を包含するものとして包括的・継続的に行われるデータ収集ではなく、個々の特定の事件の犯罪捜査のための手続であることが強調されていることに留意しなければならない。このような手続は、あくまでも個々の刑事事件の捜査という枠組みを前提とするものである。それゆえ、包括的・網羅的な探知を必要とするかもしれないテロ対応や戦時対応におけるデータ収集（特に軍当局や諜報機関による情報収集）とはかなり性質の異なるものであることを理解すべきである。

ピュータシステムによって実行されるその他の犯罪行為及び(iii)犯罪行為の電子的な形態の証拠の収集について、本節に従って設けられる権限及び手続を適用しなければならない。そして、特定の犯罪の捜査及び刑事手続のために[1]、本節に示す権限及び手続は、条約に従って設けられる刑事犯罪、コンピュータシステムによって実行されるその他の刑事犯罪及び犯罪行為の電子的な形態の証拠の収集について、適用されなければならない。このことは、本節に規定する権限及び手続によって、電子的な形態の証拠を入手または収集することができるということを確保する。それは、非電子的なデータについて在来型の権限及び手続に基づく既存のものと均等または同等に、コンピュータデータの入手及び収集をすることができることを確保する。

142. この適用範囲には、2 つの例外がある。第 1 に、第 21 条は、コンテントデータの傍受権限が国内法によって規定される重大犯罪の範囲内に限定されなければならないと定めている。多くの国々は、会話及び通信のプライバシー並びにこの捜査方法の侵害性を認識して、会話または通信の傍受権限を重大犯罪の範囲内に制限している。同様に、この条約は、国内法によって規定される重大犯罪の範囲内にある特定のコンピュータ通信上のコンテントデータに関する傍受権限及び傍受手続を設けるべきことを加盟国に求めるのみである[2]。

143. 第 2 に、加盟国は、その留保の中で指定された侵害行為または侵害行為の類型に対してのみ第 20 条（トラフィックデータのリアルタイム収集）の措置を適用する権利を留保することができる。ただし、その侵害行為またはその類型は、第 21 条中に示す傍受措置について適用される侵害行為の範囲よりも限定されたものであってはならない。幾つかの国は、トラフィックデータの収集を、プライバシー及び侵害性の観点から、コンテントデータの収集と均等のものとすることを考えている。留保の権利は、これらの国々が、リアルタイムでトラフィックデータの収集をするための措置の適用について、コンテントデータのリアルタイム傍受の権限及び手続が適用される侵害行為と同じ範囲内に限定することを許容することになる。しかしながら、多くの国々は、プライバシーの利益と侵害性の程度という観点からしても、コンテントデータの傍受とトラフィックデータの収集とが均等であるべきだとは考えていない。トラフィックデータの収集のみでは、通信内容の収集にも開示にもならないからである。トラフィックデータのリアルタイム収集は、コンピュータ通信の発信地または着

---

[1] [訳注] サイバー犯罪条約に定める証拠収集手続等が「特定の犯罪の捜査及び刑事手続」のために定められており、不特定の犯罪の捜査のための包括的な証拠収集手段を定めるものではないということに留意しなければならない。なお、ここで「刑事手続」とは、日本国の刑事訴訟においては、主として公判手続のことを指す。

[2] [訳注] 犯罪捜査のための通信傍受に関する法律（平成 11 年法律第 137 号・以下「通信傍受法」という。）は、同法の別表に定める重大犯罪に対してのみ適用される。同法の別表には、大麻取締法違反の罪（第 1 号）、覚せい剤取締法違反の罪（第 2 号）、出入国管理及び難民認定法違反の罪（第 3 号）、麻薬及び向精神薬取締法違反の罪（第 4 号）、武器製造法違反の罪（第 5 号）、あへん法違反の罪（第 6 号）、銃砲刀剣類所持等取締法違反の罪（第 7 号）、国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等の特例等に関する法律（平成 3 年法律第 94 号）第 5 条（業として行う不法輸入等）の罪（第 8 号）及び組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（平成 11 年法律第 136 号）第 3 条第 1 項第 7 号に掲げる罪に係る同条（組織的な殺人）の罪又はその未遂罪（第 9 号）が限定列挙されている。

信地を追跡する上で（従って、犯罪者を特定する際の補助として）非常に重要なものとなり得るものなので、条約は、加盟国に対し、リアルタイムでのトラフィックデータの収集のために提供される権限及び手続を可能な限り広く適用できるように、各国が留保する範囲を限定してその留保の権利を行使するよう勧奨している[1]。

144. (b)は、条約に加入する時点においてその国内法中に制限が存在するため、公衆が利用可能な通信ネットワークを用いない非公開の利用者グループの利益のために運用されており、他のコンピュータシステムに接続されていないコンピュータシステム上の通信を傍受することができない国々のために、留保を定めている。「非公開の利用者グループ」という用語は、例えば、従業員の間においてのみコンピュータシステムを用いて通信をすることができることを提供している私企業の従業員のような、サービス提供者との一定の関係によって限定された一群の利用者のことを指す。「他のコンピュータシステムに接続されていない」という用語は、第 20 条または第 21 条に基づく命令が発せられた時点において、通信が伝送されているシステムが他のコンピュータネットワークに対して物理的にも論理的にも接続されていないことを意味する。「公衆が利用可能な通信ネットワークを用いない」という用語は、公衆が利用可能なネットワークを利用していることがその利用者にとって明らかであるか否かを問わず[2]、公衆が利用可能なコンピュータネットワーク（インターネットを含む。）、公衆電話網、または、通信の伝送におけるその他の公衆が利用可能な設備を用いるシステムを含まない[3]。

条件及び安全性確保措置（第 15 条）

145. 条約の本節に定める権限及び手続の制定、実装及び適用は、各加盟国の国内法に基づいて定められている条件及び安全性確保措置に従うものとしなければならない。加盟国は、その国内法に一定の手続条項を導入しなければならないが、各国の司法制度の中にこれらの権限及び手続を制定及び実装する様式及び特定の事件におけるその適用は、各加盟国の国内法

[1] [訳注] 第 14 条の(a)が「締約国は、留保において特定する犯罪又は犯罪類型についてのみ第 20 条に定める措置を適用する権利を留保することができる。ただし、当該犯罪又は犯罪類型の範囲が、第 21 条に定める措置を適用する犯罪の範囲よりも制限的とならない場合に限る。締約国は、第 20 条に定める措置を最も幅広く適用することができるように留保を制限することを考慮する」と定めていることを指している（外務省訳）。

[2] [訳注] 利用者の主観的な認識とは無関係に、客観的に、当該ネットワークが公衆に利用可能なネットワークである場合のことを指す。一般に、ネットワークシステムの利用者は、ネットワークシステムの物理構造については無頓着であり、関心もないことが少なくない。このことは、例えば、旅客鉄道の利用者が鉄道会社の運用管理システムそれ自体については一般に関心がないのと同じことである。一般に、利用者の関心はサービス（役務）のほうにあり、そのサービスを提供するためのシステムやネットワークの物理構造そのものにはないと言える。このことが、ネットワークルータや Wi-Fi 接続機器類の脆弱性を含め、ネットワーク全体の大きな脆弱性要素の 1 つになっていることは否定することができない。全ての機器類の潜在的な危険性について広く一般公衆が気づくことが求められている。

[3] [訳注] 例えば、インターネットを用いるシステムは、「公衆が利用可能な通信ネットワークを用いている」ことになる。

及び国内手続に任されている。これらの国内法及び手続は、以下に述べるように、憲法上、立法上、司法上またはその他のものの上で定められている条件または安全性確保措置を含めるものとしなければならない[1]。その様式は、法執行上の要求と人権及び自由の保護とを均衡させる条件または安全性確保措置として、一定の要件を付加することを含むものとしなければならない。多数の相違点のある法制度や法文化を持つ加盟国に対して条約が適用されることから、個々の権限または手続に適用可能な条件及び安全性確保措置の細目を定めることは不可能なことである。加盟国は、条件及び安全性確保措置が人権及び自由の十分な保護を提供することを確保しなければならない。条約の加盟国が従わなければならない幾つかの共通基準またはミニマムの安全性確保措置は存在する。それらは、適用可能な国際的な人権文書に基づいて加盟国が負っている義務から生ずる基準またはミニマムの安全性確保措置を含む。それらの文書は、その加盟国である欧州諸国に関しては、人権及び基本的自由の保護に関する 1950 年欧州条約並びにその第 1 追加議定書、第 4 追加議定書、第 6 追加議定書、第 7 追加議定書及び第 12 追加議定書（ETS No.5[2]、同 No.9、同 No.46、同 No.114、同 No.117 及び同 No.177）、を含む。また、それは、世界の他の領域にある国々に関しては、それらの国々が当該文書の加盟国となっている他の適用可能な人権文書（例 : 1969 年の人権に関するアメリカ条約及び 1981 年の人権及び人々の権利に関するアフリカ憲章）、並びに、より国際的に 1966 年に批准された市民的権利及び政治的権利に関する国際規約を含む。加えて、ほとんどの国々の法律に基づいて定められた類似の保護が存在する[3]。

146. 条約の中にある別の安全性確保措置は、権限及び手続が「比例性の原則と適合するものでなければならない」というものである。比例性の原則は、加盟国の国内法における関連する原則に従い、各加盟国によって実装されなければならない。欧州の諸国については、1950 年の欧州評議会人権条約にある欧州の司法権並びに構成国の立法権及び司法権に適用可能な「権限及び手続は、侵害行為の性質及び状況と比例するものでなければならない」[4]という

---

[1] [訳注] 第 145 項は、全体として、サイバー犯罪条約に定める通信傍受、データの応急の保全、データのリアルタイム収集、データの捜索・押収について、様々な態様による安全性確保措置（safeguards）の中でも、通信の秘密を含め、通信当事者や利用者の基本的な権利及び自由を法的に保護するための法的措置のことを説明している。このような法的措置の中では、特に守秘義務を法律によって定めることが重要とされているが、違反行為に対する処罰や損害賠償制度ないし損失補償制度の設置等も重要である。法律ではなく契約に基づくものとしては、各種保険制度の利用を考えることもできる。

[2] 条約の条文は、1970 年 9 月 21 日に発効した第 3 議定書（ETS No.45）、1971 年 12 月 20 日に発効した第 5 議定書（ETS No.55）、1990 年 1 月 1 日に発効した第 8 議定書（ETS No.118）によって改正され、また、第 2 議定書（ETS No.44）の条文が、その第 5 条第 3 項に従い、1970 年 9 月 21 日に発効した時から条約の一部であるものとして統合された。これらの議定書によって改正または追加された全ての条項は、1998 年 11 月 1 日の発効の日から、第 11 議定書（ETS No.155）によって置き換えられた。1994 年 10 月 1 日に発効した第 9 議定書（ETS No.140）は、その日から廃止となり、第 10 議定書（ETS No.146）はその目的を失った。

[3] [訳注] 日本国憲法の第 35 条第 1 項は、「何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第 33 条の場合を除いては、正当な理由に基づいて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない」と定め、同条第 2 項は、「捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ」と定めている。

[4] [訳注] 原文に括弧はない。読み難いので、括弧を補って訳した。

原則から導き出すことができるであろう[1]。他の国々は、提出命令のオーバーブレドス[2]の制限や捜索及び押収についての合理性の要件[3]といったような、その国の関連する諸原則を適用することになるであろう。また、傍受措置に関する義務は国内法によって定められる重大な侵害の程度を考慮するものとしなければならないという第 21 条の明示の制限は、比例性の原則の適用についての明示の一例である。

147. 適用され得る条件及び安全性確保措置のタイプに制限を加えることなく、条約は、特に、権限または手続の性質に鑑み適切な場合には、そのような制限及び安全性確保措置が、適用または制限を正当化する事由並びに権限または手続の適用範囲及びその期間に関する司法上または他の独立した監督上[4]の制限を含むことを求めている。自国の立法者は、拘束力のある国際的な義務及び確立された国内法上の諸原則を適用するのに際して、その性質上、どの権限及び手続が特別の条件及び安全性確保措置の実装を要する程度まで侵害的なものであるかを判断することになるであろう。第 215 項で述べるとおり、加盟国は、その侵害性に鑑み、通信傍受に関する条件及び安全性確保措置といったような条件及び安全性確保措置を明確に適用しなければならない。それと同時に、例えば、そのような安全性確保措置は、保全の品質に対しては適用されない[5]。国内法に基づいて適用されるべき他の安全性確保措置には、

---

[1] [訳注] 欧州評議会の欧州人権条約の第 8 条第 2 項が最も関係の深い条項であると考えられるが、明文で「比例性の原則（Proportionality principle）が示されているわけではない。この概念は、判例法によって形成されたものと理解されている。欧州評議会（Council of Europe）の Web サイトにある説明の中では、下記のところにある「The margin of Application」に関する説明が最もわかりやすい。

https://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp [2016 年 11 月 29 日確認]

比例性の原則と関連する文献としては、Steven Greer, The Margin of Application: Interpretation and discretion under the European Convention on Human Rights, Council of Europe Publishing (July 2000) 及び Tor-Inge Harbo, The Function of the Proportionality Principle in EU Law, European Law Journal Vol.16 No.2 pp.158–185 (2010) がある。

[2] [訳注] オーバーブレドスの法理（Overbreadth doctrine）は、アメリカ合衆国の憲法修正第 1 条との関係で形成された法概念の一種とされている。関連する文献として、君塚正臣「過度に広汎性ゆえ無効の法理」横浜法学会 23 巻 2 号 1～36 頁 (2014)、宮原均「オーバーブレドス（overbreadth）理論の新展開」法學新報 93 巻 3・4・5 号 77～110 頁 (1986)、藤井俊夫「合衆国違憲審査における制定法解釈の原理」千葉大学教育学部研究紀要第 1 部 25 巻 171～188 頁 (1976)がある。

[3] [訳注] 日本国の刑事訴訟法第 99 条第 1 項は、「裁判所は、必要があるときは、証拠物又は没収すべき物と思料するものを差し押えることができる。但し、特別の定のある場合は、この限りでない」と規定し、形式的には必要性の要件のみを定めているように読める。しかし、一般に、この「必要性」とは、相当性を含むものと解されている（前掲松尾浩也監修『条解刑事訴訟法（第 4 版）』203 頁参照）。ここでいう「相当性」とは、EU の法制における「比例性」と実質的に同じものと理解することができる。また、法学理論上の立場にもよるかもしれないが、「合理性（reasonableness）」を「相当性」と訳すこともできるであろう。

[4] [訳注] 個人データ保護のための監督官（supervisory authorities）が該当する。なお、説明書の第 138 項の脚注（訳注）参照。

[5] [訳注] データの保全の精度等の問題は、結局は、証拠の関連性や証拠力の評価という訴訟法上の問題に全部吸収されてしまうことになる。捜査機関が確実な証拠として裁判所に採用されることを望む場合には、当該データの完全性・機密性・可用性を証明するための技術的・組織的な手段を考えることになる。これは、一般的な意味での法科学（Forensics）の一部である。

自己負罪を拒否する権利[1]、並びに、措置の適用に対して異議を述べる人または場所の法的な特権及び特例が含まれる[2]。

148. 第 3 項の中で検討した事柄に関して、その基本的な重要性は、「公共の利益」、とりわけ、「司法の円滑な運営」に対する配慮にある。公共の利益に適合する範囲内で、加盟国は、サービス提供者を含め、第三者の「権利、責任及び正当な利益」に対して措置が執行される結果として生ずる権限もしくは手続の影響、及び、その影響を緩和するための適切な措置が講じられているか否かといったような要素を検討しなければならない。まとめると、最も重要な点は、司法の円滑な運営及びその他の公共の利益（例えば、被害者の利益や私生活の尊重を含め、公共の安全、公衆衛生その他の利益）が最初に考慮される。公共の利益に適合する範囲内で、消費者サービスの混乱をミニマムなものとすること、本章に基づく開示または開示できるようにすることの責任から保護すること、または、専有的な利益を保護すること[3]といったような問題についても、一般に、考慮されることになるであろう。

第 2 款　記録保存されたデータの応急の保全

149. 第 16 条及び第 17 条の措置は、サービス提供者のようなデータの保有者によって既に収集され保有されている記録保存されたデータに対して適用される。それらの条項は、リアルタイムの収集及び将来のトラフィックデータの保持、または、通信の内容に対するリアルタイムのアクセスについては適用されない。これらについては、第 5 款で規定している。

150. これらの条項に示される措置は、コンピュータデータが既に存在しており、かつ、現時点で記録保存されている場合についてのみ行われる。例えば、正確なデータが収集され保持されないかもしれず、また、それが収集された場合でも保存されないかもしれない。そのデータの刑事訴訟手続上の重要性を誰かが明らかにする前に、データ保護法が重要なデータの破壊を積極的に要求するかもしれない[4]。ときとして、顧客がサービスに対して低額の支払をする場合やサービスが無料である場合のように、データの収集及び保持をすべき経営上の理

---

[1] [訳注] 日本国憲法の第 38 条第 1 項は、「何人も、自己に不利益な供述を強要されない」と定めている。

[2] [訳注] 様々なものを想定することができるが、例えば、刑事訴訟法の第 39 条第 1 項は、「身体の拘束を受けている被告人又は被疑者は、弁護人又は弁護人を選任することができる者の依頼により弁護人となろうとする者（弁護士でない者にあっては、第 31 条第 2 項の許可があつた後に限る。）と立会人なくして接見し、又は書類若しくは物の授受をすることができる」と定めている。

[3] [訳注] 例えば、捜索・押収の対象となる電磁的記録（データ）が著作権法の適用のある著作物である場合、捜査機関の正当な捜査行為の範囲内で当該データの複製をすることは認められるが、正当な捜査権限の範囲を逸脱して行われる場合には著作物の複製権の侵害行為（違法行為）となることがある。そのため、捜査機関にとって、知的財産権の管理も重要な義務となり得る。

[4] [訳注] 個人データの処理の目的が達成された後には、当該データは破棄されるのが原則であり、可能性の問題として当該データが刑事訴訟手続上で重要な証拠となることがあり得る場合であっても、特に別の法令等によって保存が義務付けられているような場合を除き、個人データ保護の目的のためにデータの破棄がなされるのが原則であることを指している。個人データ保護法令によるプライバシーの保護と訴訟手続上の証拠保全の必要性とはトレードオフの関係にたつことがある。

由がないことがある。第 16 条及び第 17 条は、このような問題については対応していない。
151. 「データの保全」は、「データの保持」と区別されなければならない。一般的な言語においては類似する意味があるけれども、それらは、コンピュータの利用との関係では別の意味を有している。データを保全することとは、記録保存された方式で既に存在しているデータについて、現在の品質または状態を変化または劣化させ得ることがないように保護されている状態を維持することを意味する。データを保持することとは、現在生成されているデータを将来に向かって誰かが保有している状態を維持することを意味する[1]。データの保持は、現時点におけるデータの蓄積及び将来の時点に向けたその維持または保有を含意している。データの保持は、データの記録保存の過程である。他方で、データの保全は、記録保存されたデータを防護され安全な状態に維持する行為である。
152. 第 16 条及び第 17 条は、データの保全のみを指し、データの保持を指していない。これらの条項は、サービス提供者その他の組織によってその活動の過程で収集されるデータの全部または一部の収集及び保持を命じていない。保全の措置は、既に存在しているデータを前提として、「コンピュータシステムによって記録保存された」コンピュータデータ、既に収集されたコンピュータデータ及び記録保存されているコンピュータデータについて適用される。更に、第 14 条に示されているように、条約の第 2 節において設けられることが求められている権限及び手続は、「特定の犯罪の捜査または訴訟手続」のためのものであり、それは、この措置の適用を特定の事件における捜査の場合に限定している。従って、加盟国が、何らかの命令という方法によって、保持の措置の効果を与えようとする場合には、その命令は、「その者が保有または管理する特定の記録保存されたコンピュータデータ」と関連するものである。それゆえ、本条は、特定の犯罪捜査または訴訟手続と関連して、他の法的権限によって後にデータが開示されることをひとまず措き、既存の記録保存されたデータの保全を求める権限についてのみ定めている。
153. データの保全を確保すべき義務は、加盟国に対し、その正当な企業活動の一部としてトラフィックデータや加入者データのような一定のタイプのデータを定期的に収集及び保持しないサービスの提供または利用を禁止することを要求することを意図するものではない。のみならず、この義務は、加盟国に対し、例えば、要請または命令に応じて合理的に保全することができないようなほんの短時間だけシステム上に現れ得る一時的なデータを保全するため技術的能力のような、保全をするための新たな技術的能力を実装すべきことを要求するものでもない。
154. 幾つかの構成国には、特定のタイプの保有者によって保有されている個人データのような一定のタイプのデータを保持することはできず、かつ、データを保持するための事業遂行

[1] [訳注] データ保持指令 2006/24/EC において、プロバイダによって保持されたトラフィックデータ等の開示の要請について、構成国の法令の中で裁判所（特別裁判所を含む。）や上級官庁の承認を要するという条項がある場合、そもそも保持（retention）それ自体が包括的かつ継続的なものであるし、開示の要請の承認についても包括的なものであり得ることから、それは、「特定の事件について、既に存在するデータを保全すること」を目的とするものではない。データの保持命令における承認は、刑事訴訟法に基づき特定の事件について、特定のデータに関して認められる応急の保全（preservation）とは全く異なる。なお、データ保持指令 2006/24/EC の参考訳は、法と情報雑誌 1 巻 5 号 47～65 頁にある。

上の目的がなくなったときは削除しなければならないことを求める法律がある。欧州連合においては、指令 95/46/EC[1]によって基本原則が実装されており、特に通信分野の文脈においては、指令 97/66/EC[2]によって実装されている。これらの指令は、データを記録保存する必要がなくなったときは、速やかにデータを削除すべき義務を設けている[3]。しかしながら、構成国は、犯罪行為の防止、捜査及び訴追の目的のために必要な場合には、例外を定める立法を採択することができる。これらの指令は、欧州連合の構成国に対し、構成国の国内法に基づき、特定の捜査のために特定のデータを保全するための権限及び手続を設けることを禁止していない[4]。

155. データの保全は、大半の国々にとっては、国内法における新たな権限及び手続である。それは、コンピュータ犯罪及びコンピュータと関連する犯罪、とりわけ、インターネットを介して実行される犯罪に対処する重要で新たな捜査手段である。そして、不注意な処理及び記録保存業務、証拠の破壊を目的とする意図的な操作や削除、または、保持することが求められなくなったデータの定期的な削除によって、犯罪の重要な証拠が簡単に失われ得る。その完全性を保全するための 1 つの方法は、職務権限を有する機関にとっては、データの捜索もしくはそれに類するアクセスをし、または、データの押収もしくはそれに類する防護をすることである。しかしながら、評判の良い企業のように、データの管理者が信頼に重きを置いている場合には、データの保全を命ずるという方法によって、より迅速に、データの完全性を防護することができる。また、適法な企業にとって、保全命令は、保全の前提として捜索や押収を執行する場合よりも、その通常の活動や評判に対して、破壊的ではない。第 2 に、コンピュータ犯罪やコンピュータと関連する犯罪は、コンピュータシステムを介する通信の伝送の結果として、非常に大きな範囲で実行される。これらの通信は、児童ポルノのような違法なコンテント、コンピュータウイルス、データの侵害やコンピュータシステムの正常な機能の侵害により得られたその他の文書、または、麻薬売買や詐欺のような別の犯罪行為が実行されたことの証拠を含むものであり得る。これらの過去の通信の発信地及び到達地を判断する場合は、加害者の同一性を識別することが助けとなり得る。その発信地及び到達地を判断するためにその通信を追跡するためには、この過去の通信と関係するトラフィックデータが必要となる（後述の第 17 条に基づくトラフィックデータの重要性に関する説明参照）。第 3 に、これらの通信が、違法なコンテントまたは犯罪行為の証拠を含んでおり、かつ、電子メールのように、その通信の複製がサービス提供者によって保持されている場合、これらの通信の保全は、決定的な証拠が失われないことを確保する上で重要なものである。これらの過去の通信の複製（例えば、送信または受信され、記録保存された電子メール）は、犯罪

[1] [訳注] 個人データ保護指令 95/46/EC の参考訳は、法と情報雑誌 1 巻 5 号 1〜46 頁にある。

[2] [訳注] 通信分野データ保護指令 97/66/EC の参考訳は、法と情報雑誌 1 巻 5 号 66〜83 頁にある。

[3] [訳注] 犯罪捜査と関連して法執行機関（警察）が管理者（controller）として保有・管理する個人データについて適用される指令(EU) 2016/680 の第 4 条第 1 項(e)は、当該個人データの処理の目的のために必要な期間内においてのみ個人識別が可能な状態を保つことができる旨を定めている。従って、特定の被疑者に関する個々の事件の捜査の目的を遂げた後には、原則として、当該個人データが当該被疑者に関するものであると識別可能な状態で当該個人データを保有することができない。

[4] [訳注] 犯罪捜査と関連する個人データ保護の問題に関しては、夏井高人「欧州連合の構成国における独立の個人データ保護監督官の職務」法律論叢 89 巻 6 号掲載予定で述べた。

の証拠を明らかにし得るものである。
156. コンピュータデータの応急の保全の権限は、これらの問題に対処するためのものである。それゆえ、加盟国は、法令上の措置として、特定のコンピュータデータの保全を命ずる権限を導入し、それによって、最長 90 日を上限として、必要な期間内、データを保全することが求められる。加盟国は、命令の更新について定めることができる。このことは、保全の時点において、法執行機関に対し、そのデータが開示されるということを意味するものではない。保全されたデータの法執行機関に対する開示に関しては、第 152 項及び第 160 項を参照されたい。
157. また、自国の領土内にある記録保存されたデータについて、加盟国が国際的なレベルで相互に支援することができるようにするために、保全の措置が自国のレベルで存在しているということが重要である。これは、支援の要請を受けた加盟国がそのデータを実際に入手し、支援の要請をしている加盟国に対してこれを開示する従来のしばしば時間を要する司法共助手続が行われている間に、重要なデータが失われてしまわないようにすることを確保するための助けとなることであろう。

記録保存されたコンピュータデータの応急の保全（第 16 条）

158. 第 16 条は、自国の職務権限を有する機関が、特定の犯罪捜査及び刑事手続と関係する特定の記録保存されたコンピュータデータの応急の保全を命ずることができること、または、同様にそれを取得することができることを確保することを目的としている[1]。
159. 「保全」は、記録保存された形態で既に存在しているデータについて、その現在の品質及び状態を改変または劣化させるかもしれないいかなるものからも保護することを求める。保全は、データの改変、劣化または削除に対する防護の維持を求める。保全は、データが「凍結」（例えば、アクセスできなく）されていることを必ずしも意味するものではなく、また、そのデータまたはその複製物を正当な利用者が利用することができないということを意味するものでもない。命令の名宛人は、命令に示された指示に従い、引き続きデータにアクセスすることができる。本条は、データがどのように保全されるべきかについては定めていない。適切な保全の方法の決定は、各加盟国に任されており、また、それが適切な場合には、データの保全でデータの「凍結」を命ずるかどうかを決定することも任されている[2]。
160. 「命令し、または類似の方法によって確保」という指示は、単に、法務当局または行政機関（例：検察庁または警察）からの命令もしくは指図によるだけではなく、保全の目的を

[1] [訳注] 参考となる文献として、Cybercrime Convention Committee (T-CY), Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime (5-6 December 2012)がある。
[2] [訳注] 日本国においては、刑事訴訟法第 197 条第 3 項に基づいて通信履歴に相当する電磁的記録の保全が命ぜられる場合だけではなく、任意捜査の一種として、警察からプロバイダに対してコンテントデータの応急の保全についての協力依頼が行われることがある。刑事訴訟法第 197 条第 1 項について、前掲松尾浩也監修『条解刑事訴訟法（第 4 版）』368～369 頁は、「この本文は、但書と対照すると任意捜査が原則であることを定めていることが分かる。任意捜査は、その手段・方法に特段の制限がなく、捜査機関の判断と裁量によって行うことができる」としている。

達成する他の法的手段の使用を許容することを意図している。幾つかの国においては、保全命令がその国の刑事手続法中に存在せず、そして、データは、捜索命令、押収命令または提出命令によってのみ保全され入手され得るのに過ぎない。「またはその他の確保」という文言を使用することによる柔軟性は、こうした国々が、これらの方法の利用により本条を実装することを許容することを意図している。しかしながら、命令を受ける者が速やかに行動することによって、特定の事件における保全措置をより迅速に実施できるようにするため、各国が、データの保全命令を受ける者に対して実際に命令を発する権限及び手続の設置を検討することを推奨する。

161. 特定のコンピュータデータの応急の保全を命令しまたはその他の類似の方法によって入手する権限は、全てのタイプの記録保存されたコンピュータデータについて適用される。これは、保全されるべきものとして命令中に指定されるデータに、全てのタイプのものを含めることができる。例えば、企業の記録、医療機関の記録、個人の記録その他の記録を含めることができる。措置は、「特に、そのコンピュータデータがとりわけ滅失または改変され易いと信ずるべき根拠がある場合には、特別に」利用するために、加盟国によって設けられる。これは、一定期間経過後にはデータを削除する企業ポリシーが存在する場合、または、記録媒体が他のデータを記録するために使用されるときには、通常はデータが削除されてしまう場合のように、データの保持期間が短い場合を含めることができる。データの管理者の性質またはデータが記録保存される方法が安全でないことを要件とすることもできる。しかしながら、データの管理者を信頼することができない場合[1]には、それに従わないかもしれない命令によるのではなく、捜索及び押収によって、より効果的な保全が確保されることになるだろう[2]。トラフィックデータというタイプのデータに特別に適用される条項について注意を喚起するために、第 1 項の中では、「トラフィックデータ」について特に言及されている。これは、サービス提供者によって収集または保持されているとしても、通常は、ほんの短期間だけ保持されているものである。「トラフィックデータ」への言及は、また、第 16 条及び第 17 条の中にある措置との連携も提供している。

162. 第 2 項は、加盟国が命令によって保全を実現する場合には、その保全命令が「ある者が保有または管理する特定の記録保存されたコンピュータデータ」と関係するものであることを定める[3]。そして、記録保存されたデータは、当該の者が現実に保有しているもの、または、当該の者が管理するどこか別の場所に記録保存されているものであり得る。命令を受ける者

[1] [訳注] 例えば、データ管理者が加害者である場合、あるいは、犯罪組織の構成員である場合などを考えることができる。

[2] [訳注] この部分の記述は、応急の保全命令が任意捜査として実施され、捜索・押収が強制捜査として実施されるような場合を前提にするものと解される。

[3] [訳注] 「特定の記録保存されたデータ（specified stored computer data）」であることを要する結果、保全の命令は、個別になされることを要し、包括的・概括的な命令は認められない。例えば、「命令を受ける者が管理・保有する全てのデータ」といったような記述では、対象となるデータが特定されているとは認められない。ただし、特定の程度には解釈の余地がある。例えば、「特定の期間内において、特定の発信者と特定の受信者との間で行われる通信」というような記述は、少なくとも日本国における通信傍受法その他関連法令の解釈・運用（特に令状実務における解釈・運用）における整合性という観点からは、適法に特定されているものとして判断可能な範囲内にあると解することができる。

は、「職務権限を有する機関がそのコンピュータデータの開示を求めることができるようにするために、最長 90 日の範囲内で、必要な期間、当該コンピュータデータの完全性を保全または維持すること」が義務付けられる。加盟国の国内法は、命令の対象となるデータが保全されるべき最長期間を定めなければならず、そして、その命令は、特定されたデータが保全されるべき確定期間を定めなければならない。この期間は、職務権限を有する機関がデータの開示を得るために、捜索・押収もしくはこれらに類するアクセス・確保または提出命令の発付のような他の法律上の措置を講ずることができるようにするため、最長 90 日の範囲内で、必要な期間とするものでなければならない。加盟国は、提出命令の更新について定めることができる。この点に関しては、コンピュータシステムによって記録保存されたデータの応急の保全を得るための共助要請に関する第29条が参照されなければならない。同条は、共助要請に応じて実施される保全が「当該要請をした加盟国がそのデータの捜索もしくは捜索に類するアクセス、押収もしくは押収に類する確保またはそのデータの開示についての要請を受け入れることができるようにするため、60 日を下回らない期間、維持されなければならない」と定めている[1]。

163. 第 3 項は、保全されるべきデータの管理者またはデータの保全を命ぜられる者に対し、国内法によって設けられる期間内、保全手続を実施することに関して機密保持の義務を課している[2]。同項は、加盟国に対し、記録保存されたデータの応急の保全に関する機密保持の措置を導入し、そして、機密保持の期間に関する時間的制限を導入することを求めている。この措置は、捜査を受けている容疑者が捜査に気づかないようにしようとする法執行機関の必要と、プライバシーに関する個人の権利に対応しようとするものである[3]。法執行機関にとっては、データの応急の保全は、初動捜査の一部を構成するものであり、従って、この場面では、密行性が重要なものとなり得る。保全は、データの入手またはその開示のための他の法的手段が行われるまでの間の一時的措置である。機密保持は、他の者がそのデータに干渉しまたはこれを破壊しようとしないようにするために求められる。命令を受ける者、または、

[1] [訳注] 保全命令の最長有効期間は、60 日以上 90 日以下ということになる。

[2] [訳注] 刑事訴訟法第 197 条第 5 項は、通信履歴の保全命令について、「必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる」と定めている。また、刑事訴訟規則第 93 条は、「押収及び捜索については、秘密を保ち、且つ処分を受ける者の名誉を害しないように注意しなければならない」と定めている。これらの条項は、強制処分（強制捜査）について適用される。これに対し、任意捜査として応急の保全が行われる場合、その任意捜査の要請に応ずる者についてどのような法理論的根拠に基づいて守秘義務を課すことになるかについて、仮に任意に守秘の要請が行われたとした場合、その要請に法的拘束力があるか否かについては、必ずしも明確ではない。従来、この点に関する検討が十分になされてきたとは認め難い。

[3] [訳注] 個人データ保護の観点からは、プライバシーを保護法益とする守秘義務を設けることは、安全性確保措置の一種であることになる。一般に、個人データ保護のための安全性確保措置は、個人データ保護に関する法定中に定められているものだけではなく、関連する他の法令中にも定められていることが普通である。日本国法においても、例えば、国家公務員（国家公務員法第 100 条）や地方公務員（地方公務員法第 34 条）の守秘義務は、個人情報保護のための安全性確保措置の一種として機能している。それゆえ、個人データ保護法制について検討する場合には、個人データ保護に関する基本的な法令だけではなく、関連する法令をできるだけ網羅的に検討した上で考察する必要性があると言える。

当該データの中で記述されもしくは識別されているデータ主体その他の者にとっては、措置の期間についての明確な時間制限があることになる。データを安全かつ防護された状態に保ち、保全措置が講ぜられたという事実に関して機密保持を維持するという二重の義務は、当該データの中で記述されもしくは識別されているデータ主体その他の者のプライバシーを保護するための助けとなる[1]。

164. また、以上に定める制限に加え、第 16 条に示す権限及び手続は、第 14 条及び第 15 条に規定する条件及び安全性確保措置に従う。

トラフィックデータの応急の保全及び部分開示（第 17 条）

165. 本条は、第 16 条に基づくトラフィックデータの保全と関連する特別の義務を設け、特定の通信の伝送に関与していた他のサービス提供者を識別するための、そのトラフィックデータの応急の開示について定めている[2]。「トラフィックデータ」は、第 1 条で定義されている。

166. 過去の通信と関連する記録保存されたデータを取得することは、過去の通信の発信地及び着信地を判定する上で極めて重要なものとなり得る。それは、例えば、児童ポルノの配信者、詐欺の手口の一部としての偽りの表示の配信者、コンピュータウイルスの配信者、コンピュータシステムに違法にアクセスしようとの試みもしくはその違法なアクセスの成功、または、システム内のデータの妨害もしくはシステムの正常な機能の妨害のために行われたコンピュータシステムへの通信の伝送をした者を特定するためにも重要である。しかしながら、このデータは、プライバシーを保護するために制定された法律が禁止していることがあるこ

[1] [訳注] ある者に関する個人データを処理している管理者にとっては、自己が処理しているデータの中に当該の者の個人データが含まれていることは既知のこととなるので、個人データ保護のための一般的な安全性確保義務及び守秘義務を負っていることは当然の前提となっている。ここで述べていることは、保全の命令がなされたことによって、「当該個人について捜査機関が何らかの容疑をもっているかもしれない」という評価要素が当該個人データの属性値として付加されたことになるので、そのような新たに付加された属性値について守秘義務が生ずるという点が重要である。この属性値に関する守秘義務が遵守されなかった場合、その属性値によって当該個人に対する社会的評価が低下することになる（プロッサーの類型では、第 3 類型に属するプライバシーの侵害）。そのような属性情報の暴露が故意に行われた場合には、名誉毀損罪（刑法第 230 条）が成立することがある。それが過失によって行われた場合であっても、不法行為（民法第 709 条）に基づく損害賠償責任が生じ得る。

[2] [訳注] 刑事訴訟法第 197 条第 3 項は、「検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、30 日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至ったときは、当該求めを取り消さなければならない」と定め、同条第 2 項は、「前項の規定により消去しないよう求める期間については、特に必要があるときは、30 日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて 60 日を超えることができない」と定めている。

とや、市場の圧力がそのようなデータを長期間記録保存する意欲を減退させることがあることから、ほんの短時間だけ頻繁に記録保存されるものである。それゆえ、このデータの完全性を防護するために行われる保全の措置が重要となる（前述の保全に関する検討参照）。

167. しばしば、通信の伝送には複数のサービス提供者が関与している。個々のサービス提供者は、当該提供者のシステム内をその通信が通過すること、または、他のサービス提供者によって処理されたことと関連して、当該サービス提供者によって生成され、あるいは、保持された、特定の通信の伝送と関連するトラフィックデータを処理することがある。時として、トラフィックデータは、少なくとも、幾つかのタイプのトラフィックデータは、営利上の目的、防護上の目的または技術上の目的で、通信の伝送に関与するサービス提供者の間で共有されることがある。そのような場合、通信の発信地または着信地を判定するために必要となる重要なトラフィックデータを、それらのサービス提供者の中のいずれかが保有していることがあり得る。しかしながら、しばしば、単独のサービス提供者は、実際の通信の発信地または着信地を判定することのできる重要なトラフィックデータを十分に保有していない。個々のサービス提供者は、パズル[1]の断片のみを保有し、それらの個々の断片は、発信地または着信地を特定するために吟味されなければならない。

168. 第 17 条は、ある通信の伝送に複数のサービス提供者が関与している場合において、トラフィックデータの応急の保全の効果を全てのサービス提供者に対して及ぼすことができることを確保している。条文は、それを達成することのできる手段を細かく定めておらず、加盟国の法制度及び経済制度に適合する手段の決定は、国内法に任されている。職務権限を有する機関が、個々のサービス提供者に対して別々に応急の保全命令を発することは、応急の保全を達成するための手段の 1 つとなるかもしれない。しかし、一連の個々の命令を得ることは、不合理な時間を消費することとなり得る。望ましい代替策は、単一の命令でありながら、特定の通信の伝送について 2 次的に関与していると特定された全てのサービス提供者に対して適用されることを適用範囲とするような命令を得ることであり得る。この包括的な命令は、特定された各サービス提供者に対して、順次執行され得るであろう。他の代替策としては、サービス提供者の参加を含み得る。例えば、命令を受けたサービス提供者に対し、応急の保全命令の存在及びその内容について連鎖の中にある次のサービス提供者に通知すべきことを求めることである。この通知は、国内法に基づき、他の提供者が、それを削除すべき義務に拘らず、関連するトラフィックデータを任意に保全することを認める効果を有すると同時に、また、関連するトラフィックデータの保全を命ずる効果を有することとなり得る。2 番目のサービス提供者は、同様に、その連鎖の中にある更に次のサービス提供者に対して、同様に通知をすることができる[2]。

169. サービス提供者に対して保全命令が命じられたことを根拠としては法執行機関に対してトラフィックデータが開示されることはないので（そうではなく、他の法的措置が講じら

[1] [訳注] ジグソーパスルのようなものを考えると、理解しやすい。なお、刑事訴訟において全ての証拠が完璧に揃っていることは稀であり、元来、断片的な証拠による推論に立脚するものであるから、推定可能な程度との相関性が重要であるということを明確に理解しなければならない。

[2] [訳注] 順次連絡を受けるプロバイダとしては、いわば、順次「不幸の手紙」を受け取り、それを次のプロバイダに手渡すのと同じような状況に置かれることになる。

れることに基づき、その後に取得し、または、開示を受けるだけであるので)、その法執行機関は、重要なトラフィックデータの全てをそのサービス提供者が処理しているかどうか、あるいは、その通信の伝送の連鎖の中に他のサービス提供者が関与しているかどうかを知ることができない。それゆえ、本条は、保全命令または類似の命令を受けたサービス提供者が、職務権限を有する機関その他の定められた者に対して、他のサービス提供者及びその通信が伝送された経路をその職務権限を有する機関が特定するために十分な分量のトラフィックデータを一時的に開示すること求めている。職務権限を有する機関は、開示を求めるトラフィックデータのタイプを明確に特定しなければならない。その情報を受ければ、職務権限を有する機関は、他のサービス提供者との関係でも保全の措置を講ずるべきかどうかを判断することができるであろう。この方法により、捜査機関は、その通信の発信地を遡って追跡し、または、その着信地に向けて追跡することができ、そして、捜査中の特定の犯罪の加害者もしくは加害者らを特定することができる。また、本条の措置は、第 14 条及び第 15 条に定める制限、条件及び安全性確保措置に従う。

第 3 款　提出命令

提出命令（第 18 条）

170. 本条第 1 項は、加盟国に対し、自国の職務権限を有する機関が、自国の領土内にある者に対して特定の記録保存されたコンピュータデータを提供させ、または、加盟国の領土内でサービスを提供するサービス提供者に対して加入者情報を提出させることができるようにすることを求めている[1]。問題となるデータは、記録保存されたデータまたは現存するデータであり、トラフィックデータや将来の通信に関連するコンテントデータのようにまだ存在していないデータは含まれない[2]。加盟国が第三者[3]に対してデータの捜索及び押収のような制度上の強制措置を適用することを求めるのではなく、加盟国が、その国内法の範囲内で、犯罪捜査と関係する情報を入手するという、より侵害的でない措置[4]を提供する別の捜査権限を持つことが基本となっている。

171. 「提出命令」は、法執行機関が、多種多様な事件において、とりわけ、より強制的な措

[1] [訳注] 刑事訴訟法第 99 条の 2 は、「裁判所は、必要があるときは、記録命令付差押え（電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。以下同じ。）をすることができる」と定め、また、同法第 106 条は、「公判廷外における差押え、記録命令付差押え又は捜索は、差押状、記録命令付差押状又は捜索状を発してこれをしなければならない」と定めている。記録命令付差押状の要件や執行方法等については、同法第 107 条ないし第 118 条に定められている。

[2] [訳注] データの保持（retention）とは全く異なる制度（刑事手続上の措置）であることを明確にする趣旨と解される。

[3] [訳注] 文脈から、インターネットサービスプロバイダ（ISP）のようなサービス提供者のことを指すと解される。

[4] [訳注] より侵害的でないか否かについては、当該国の裁判所によって、比例性の原則を含め、刑事手続における基本原則に照らして判断されることになるであろう。

置の使用を必要としない事件において利用することができる柔軟な措置を提供している。そのような手続上の仕組みを実装することは、ISP のような第三者であるデータ管理者にとっても利益となることであろう。ISP は、しばしば、その管理下にあるデータを提供することによって、任意捜査に基づいて法執行機関を支援する用意をしているが、そのような支援について適切な法的根拠を求め、また、彼らがデータを開示することに伴う契約上の責任その他の責任から開放されることを求めている[1]。

172. 提出命令は、個人またはサービス提供者が保有または管理するコンピュータデータまたは加入者情報と関連している[2]。この措置は、その個人またはサービス提供者が当該データもしくは情報を保存している範囲内においてのみ、適用可能である。例えば、幾つかのサービス提供者は、そのサービスの加入者に関する記録を保存していない。

173. 第 1 項の(a)に基づき、加盟国は、職務権限を有する機関が、自国の領土内にある者に対し、コンピュータシステム内または当該の者が保有もしくは管理するデータ記録媒体に記録保存されている特定のコンピュータデータを提供することを命ずる権限を有することを確保しなければならない[3]。「保有または管理」という用語は、命令を発する加盟国の領土内において、関係するデータを物理的に保有すること、及び、作成されるべきデータが当該の者の物理的な保有場所以外のところにあっても、当該の者が命令を発する加盟国の領土内において、任意にそのデータの作成を管理することができる状況にあることを指す（例えば、適用可能な権限に基づき、リモートのオンラインストレージサービスによって彼または彼女のアカウントで記録保存された情報を求める提出命令を受けた者は、そのような情報を提供しなければならない）。それと同時に、リモートで記録保存されたデータに対して技術的にほとんどアクセスすることができないときは（例：リモートで記録保存されたデータに対してネットワークリンクを介してアクセスするための利用者の能力が彼または彼女の正当な管理下にない場合）、本条の意味における「管理」を構成するとは限らない。幾つかの国にお

---

[1] [訳注] 任意捜査としてのデータの提供に応ずる行為は、常に違法性が阻却され、適法行為となるとは限らない。仮に刑事訴訟上の証拠能力の問題が生じない場合であっても、民事上の責任は発生し得る。これに対し、刑事訴訟法に基づき強制捜査としてデータの提供が求められる場合には、原則として、「法令による行為」に該当するものとしてその違法性が阻却され、適法行為となる。強制捜査それ自体の適法性・違法性は、刑事訴訟法に定める手続に従い、裁判所によって、強制捜査に対する不服申立手続の中で判断される（刑事訴訟法第 419 条、第 429 条、第 430 条、第 433 条参照）。

[2] [訳注] 参考となる文献として、Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10 (DRAFT): Production orders for subscriber information (Article 18 Budapest Convention) (15 September 2016)がある。

[3] [訳注] 実際の執行方法については、理論上の問題がないわけではない。例えば、ISP の担当者が命令に服従しない場合、何らかの法的制裁を発動することは可能であるにしても、本人の意に反して強制的にコンピュータシステムを操作させることはできない。このような場合においては、刑事訴訟法に基づいて適法な強制処分として認められる範囲内において、捜査官自身が当該コンピュータシステムを操作し、犯罪捜査を遂行する上で必要なデータを入手するか、所定の手続に従い専門的な知識を有する者に当該コンピュータシステムを操作させて必要なデータを入手するか、または、ディスク等の記録媒体の占有またはその記録内容の複製物を確保した上で（刑事訴訟法第 99 条第 2 項参照）、所定の手続に基づく鑑定や検証等の方法によって当該記録媒体を解析することにより必要なデータを入手する以外に方法はない。なお、単なる不服従のみでは、公務執行妨害罪（刑法第 95 条）に該当しない。

いては、「保有」として法律によって示されている概念は、この「保有または管理」の要件に適合するための十分なブレドスをもつ物理的な保有及び構成的な保有を包含している。

第 1 項の(b)に基づき、加盟国は、また、その領土内でサービスを提供するサービス提供者に対し、「サービス提供者が保有または管理する加入者情報を提供」させる権限を定めなければならない。第 1 項の(b)と同様、「保有または管理」という用語は、サービス提供者が物理的に保有する加入者情報、及び、（例えば、他の会社によって提供されるリモートのデータ記録施設において）サービス提供者の管理の下にリモートで記録保存された加入者情報のことを指す。「そのサービスに関して」という用語は、命令を発する加盟国の領土内において提供されるサービスと関係する加入者情報を入手する目的のために利用可能なものとすべき権限のことを意味する[1]。

174. 本条第 2 項に示す条件及び安全性確保措置は、各加盟国の国内法により、特権のあるデータまたは情報を適用除外とすることができる。加盟国は、特別の類型に属する者またはサービス提供者によって保有されている特定のタイプのコンピュータデータまたは加入者情報の提出に関して、異なる要件、異なる職務権限を有する機関及び異なる安全性確保措置を定めることを望むかもしれない。例えば、公開情報として利用可能な加入者情報のような幾つかのタイプのデータに関しては、加盟国は、他の場合であれば裁判所の命令を要するとしても、法執行機関がそのような命令を発することを許容するかもしれない。他方、場合によっては、加盟国は、一定のタイプのデータを入手できるようにするために、司法機関によってのみ提出命令が発せられるものとするかもしれないし、あるいは、そのようにすべきことが人権宣言上の安全性確保措置となっているかもしれない[2]。加盟国は、そのような情報の開示を命ずる提出命令が司法機関によって発せられた場合のためにおいてのみ、法執行機関に対して当該データを開示するように制限を加えることを望むかもしれない。比例性の原則もまた、例えば、軽微な事案において提出命令が適用されることを除外するために、措置の適用との関係で一定の柔軟性を提供している。

175. 加盟国が更に考慮すべきことは、機密保持に関する措置を可能な限り採り入れることである[3]。提出命令に関して一般的に機密保持義務が課せられていない非電子的な世界とパラレルであることを維持するために、条文は、機密保持についての特別の指示を含んでいない。しかしながら、電子的な世界、とりわけオンラインの世界においては、提出命令は、時として、他のデータの捜索及び押収またはリアルタイム傍受といった別の措置に先立って行われ

[1] [訳注] 現在の世界規模でのクラウド環境においては、自国の領土内に物理サーバが存在せず、自国内ではサービスの提供のみがなされることがむしろ普通となっている。このような場合であっても、この第 173 項の説明が適用される範囲内にあるものと解される。ただし、データが多数の物理サーバに分散して記録保存されるようなシステム設計がなされている場合、解釈上やや面倒な問題が生じ得る。しかし、このような場合であっても、自国内においてサービスの提供が行われているのであれば、同様に考えることができるであろう。この点に関しては、T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group (17 February 2016)が参考になる。

[2] [訳注] 日本国憲法第 35 条参照

[3] [訳注] 日本国の法制においては、この点に関する規律が不明確となっている場合が決して少なくない。これは、特殊日本的な風土的条件または地勢学的な理由による部分がないわけではない。

る捜査上の準備的な措置として機能することがあり得る。機密保持は、捜査を成功させるために不可欠である。

176. 提出の方式に関して、加盟国は、命令の中で定められた方法で、指定されたコンピュータデータまたは加入者情報を提出すべき義務を設けることができる。これは、開示がなされるべき期間についての指示、または、「プレーンテキスト」、オンライン、紙のプリントアウトもしくは磁気ディスクでデータもしくは情報が提供されるものとするように、その方式についての指示を含むことができる。

177. 「加入者情報」は、第 3 項に定義されている[1]。それは、原則として、サービス提供者のサービスを利用する者に関して、その運営者が保持する情報のことを指している。加入者情報は、コンピュータデータと紙の記録のような他の形式のものとを含むことができる。加入者情報はコンピュータデータ以外のデータ形式を含むことがあるので、そのようなタイプの情報に対応するために、条項内に特別の条文が含められた。「加入者」は、固定料金の加入をしている者から、従量制で支払う者、無料でサービスを受ける者まで、幅広くサービス提供者の顧客を含むことを意図している。それはまた、加入者のアカウントを利用する資格を有する関係者の情報を含む。

178. 犯罪捜査の過程においては、加入者情報は、基本的に、2 つの特別の状況下において必要となるであろう。第 1 に、加入者情報は、使用された電話サービスのタイプ（例えば、モバイル）、使用された他の関連サービスのタイプ（例えば、自動転送、ボイスメール等）、電話番号その他の技術的なアドレス（例えば、電子メールアドレス）のように、加入者によって使用された、または、加入者によって現に使用されているサービス及び関連する技術的手段を識別するために必要となる。第 2 に、技術的なアドレスが知られている場合には、加入者情報は、関係者の識別を支援するために必要となる。加入者の課金記録及び支払記録に関する商業上の情報[2]のようなその他の加入者情報もまた、特に捜査中の犯罪がコンピュータ詐欺その他の経済犯罪を含む場合には、犯罪捜査と関係するものとなり得る。

179. 従って、加入者情報は、サービスの利用及びサービスの利用者に関する様々なタイプの情報を含むことになる。サービスの利用に関しては、この用語は、トラフィックデータ及びコンテントデータ以外の何らかの情報であって、それによって、利用されている通信サービスのタイプ、それと関係する技術の提供、当該の者がサービスに加入していた期間を確定することができるものを意味する。「技術の提供」という用語は、提供される通信サービスを

[1] [訳注] 参考となる文献として、Cybercrime Convention Committee (T-CY), Rules on obtaining subscriber information: Report adopted by the T-CY at its 12th Plenary (2-3 December 2014)、Cybercrime Convention Committee (T-CY), T-CY Guidance Note #8: Obtaining subscriber information for an IP address used in a specific communication within a criminal investigation (Strasbourg, 12 November 2013)がある。

[2] [訳注] このような情報については、電子通信分野における個人データの処理及びプライバシー保護に関する欧州議会及び理事会の指令 2002/58/EC が適用される。同規則の第 15 条第 1 項は、「構成国は、当該制限が、指令 95/46/EC の第 13 条第 1 項に示すような自国の安全の確保（国家安全保障）、防衛、公共の安全、犯罪行為または電子通信システムの無権限使用の防止、捜査、検出及び訴追のために、民主的な社会の中において必要であり、適切であり、かつ、比例的な措置となる場合には、この指令の第 5 条、第 6 条、第 8 条第 1 項、第 2 項、第 3 項及び第 4 項に規定する権利及び義務の範囲を制限するための立法的措置を採択することができる」と定めている。

加入者が享受することができるようにするために行われる全ての提供を含む。この提供は、技術的な番号またはアドレスの保有（電話番号、Web サイトのアドレスもしくはドメイン名、電子メールアドレス等）、並びに、受話器、コールセンターまたは LAN（ローカルエリアネットワーク）といったような加入者によって利用される通信機器の提供及び登録情報を含む。

180. 加入者情報は、通信サービスの利用と直接に関係する情報に限定されない。それは、トラフィックデータ及びコンテントデータ以外の何らかの情報であって、それによって、利用者の識別、郵便上の住所もしくは地理上の住所、電話番号その他のアクセス番号、課金情報及び支払情報であり、加入者とサービス提供者との間のサービス合意または約定に基づいて利用可能なものを確定することができるものも意味する。それは、また、トラフィックデータ及びコンテントデータ以外の何らかの情報であって、サービス合意または約定に基づいて利用可能な通信設備が設置されているサイトまたは所在地に関連するものも意味する。この最後の情報は、実務的な観点から、設備に可搬性がない場合にのみ関係するものであるが、（サービス合意または約定に従って提供される情報に基づく）設備の可搬性または仕向地に関する知識は、捜査の助けとなり得るものである。

181. しかしながら、本条は、サービス提供者に対し、その加入者の記録の保存を義務付けるものと解釈してはならない。のみならず、サービス提供者は、条約に基づいて、そのような情報の正確さ確保することを要求されるものと解釈してもならない。このことは、サービス提供者が、例えば、モバイル電話サービスのためのいわゆるプリペイドカードの利用者を識別するための情報を登録することを義務付けるものではないということを意味する[1]。加入者が誰であるかを検証することや、そのサービスの利用者による仮名の利用を制限することも義務付けられているわけではない[2]。

---

[1] [訳注] 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（平成 17 年法律第 31 号）の第 3 条は、「携帯音声通信事業者は、携帯音声通信役務の提供を受けようとする者との間で、役務提供契約を締結するに際しては、運転免許証の提示を受ける方法その他の総務省令で定める方法により、当該役務提供契約を締結しようとする相手方」について、自然人の場合には「氏名、住居及び生年月日」の、法人の場合には「名称及び本店又は主たる事務所の所在地」の確認（本人確認）を行わなければならないと定めている。また、同法第 4 条第 1 項は、「携帯音声通信事業者は、本人確認を行ったときは、速やかに、総務省令で定める方法により、本人特定事項その他の本人確認に関する事項として総務省令で定める事項に関する記録（以下「本人確認記録」という。）を作成しなければならない」と定め、同条第 2 項は、「携帯音声通信事業者は、本人確認記録を、役務提供契約が終了した日から 3 年間保存しなければならない」と定めている。更に、同法第 10 条第 1 項は、通話可能端末設備等を有償で貸与することを業とする者（貸与業者）は、通話可能端末設備等を有償で貸与する契約（貸与契約）を締結するに際しては、当該貸与契約を締結しようとする相手方について、貸与時本人特定事項の確認（貸与時本人確認）を行わずに、「通話可能端末設備等を貸与の相手方に交付してはならない」と定めている。

[2] [訳注] 実名による登録の強制のことを意味する。実名による登録を行うためには、本人確認が必然的に伴う。そして、本人確認のために提出される書類等に含まれる個人データの安全性確保が問題となる。それと同時に、詳細な本人確認情報（特に、生体認証のための生体要素データ）がサイバー犯罪者によって奪われた場合、非常に確実性の高い「なりすまし」のための手段を提供することともなり得る。その意味では、実名登録を要求することは、犯罪捜査の面では一応利点が多いように思われるけれども、反面において、犯罪捜査の困難性を増大させる危険性もあることに留意しなければなら

182. 本条の権限と手続は、特定の犯罪捜査または刑事手続の目的のために設けられているので（第 14 条）、提出命令は、関連する個々の事件、特に特定の加入者について用いられる。例えば、提出命令に記載された特定の名前の提示に基づいて、特定の関連する電話番号または電子メールアドレスを求めることができる。特定の電話番号または電子メールアドレスから、関係する加入者の名前と住所を求めることができる。本条は、加盟国に対し、例えば、データマイニングのために、無限定の分量で、加入者グループに関するサービス提供者の加入者情報の開示を命ずる法的命令を発することを認めるものではない。
183. 「サービス合意または約定」への参照は、広く解釈されるべきであり、そして、顧客である利用者が提供者のサービスを利用する根拠となる全ての種類の関係を含む。

第 4 款　記録保存されたコンピュータデータの捜索及び押収

記録保存されたコンピュータデータの捜索及び押収（第 19 条）

184. 本条は、特定の犯罪捜査及び手続と関係する証拠を入手するための記録保存されたコンピュータデータの捜索及び押収について、各国の国内法を現代化し、それを整合させることを目的としている。刑事手続上の全ての国内法は、有形の目的物の捜索及び押収のための権限を含んでいる。しかしながら、多くの国々において、記録保存されたコンピュータデータは、それ自体としては、有形の目的物であるとは考えられないであろう。それゆえ、それが記録保存されているデータ記録媒体の押収以外には、有形の目的物と同じような方法では、犯罪捜査及び刑事手続のために押収することができない。この条約の第 19 条の目的は、記録保存されたデータに関して、均等な権限を設けることにある[1]。

ない。特に、生体要素の場合には、単なる符号とは異なり、事後に修正することができないという特性を有しているため（例：指紋、光彩、遺伝子等のデータを修正することはできない。）、大規模な生体要素の流出事故が発生すると、かなり多数の者がネットワーク利用から事実上排除され阻害される高度の危険性があると同時に、当該生体認証システムが地球規模で全く使用不能となってしまうという重大なリスクもある（諜報機関においてさえ、職員の生体情報が奪われた事例がある。）。

[1] [訳注] 刑事訴訟法の第 99 条の 2 は、「裁判所は、必要があるときは、記録命令付差押え（電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。以下同じ。）をすることができる」と定めている。これは、「電磁的記録」の差押えに関する規定である。これに対し、同法第 99 条第 2 項は、「差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であって、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる」と定めている（同法第 218 条第 2 項も同旨）。これは、「電子計算機」の差押えに関する規定である。そして、同法第 110 条の 2 柱書は、「差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者は、その差押えに代えて次に掲げる処分をすることができる。公判廷で差押えをする場合も、同様である」と規定し、同条の 2 第 1 号は、「差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること」と、同条の 2 第 2

185. 文書または記録に関する在来型の捜索環境においては、捜索は、紙の上のインクのような有形の形態で過去に記録または登録された証拠の収集を含んでいる。捜査官は、そのような記録されたデータを捜索または捜査し、そして、有形の記録物を押収または物理的に入手する[1]。データの収集は、捜索の期間内に、その時に存在するデータに関してなされる。捜索を実施するための法的権限を入手する要件は、国内法及び人権上の安全性確保措置によって規定されているところに従い、当該データが特定の場所に存在しており、かつ、それが特定の犯罪の証拠となり得るものであると信ずるべき理由が存在することである。

186. 新たな技術環境における証拠の捜索、とりわけ、コンピュータデータの捜索に関しては、在来型の捜索が有する特徴の多くが残存している。例えば、データの収集は、捜索期間内に、その時に存在するデータに関してなされる。捜索を実施するための法的権限を入手する要件も、同じままである。捜索を実施するための法的権限を入手するために必要な確信の度合いは、データが有形のものであるのか電子的な形式によるものであるのかによって一切の相違がない。当該データが既に存在しており、それが特定の刑事犯罪の証拠となり得るものであるということの確信の存在、そして、捜索がそのようなデータに関してなされるものであるということについても、同様である。

187. しかしながら、有形のデータの捜索及び押収と同等に効果的なやり方でコンピュータデータを入手することができるということを確保するために、コンピュータデータの捜索に関しては付加的な手続条項が必要となる。それには幾つかの理由がある。すなわち、第 1 に、データは、電磁的な形態といったような無形の形態になっている。第 2 に、データは、コンピュータ装置を使用して読むことができるが、紙の記録と同じような意味では押収し、入手することができない[2]。無形のデータが記録保存されている物理媒体（例：コンピュータハードディスクまたは磁気ディスク）が押収され、入手されなければならず、あるいは、その複製を含む有形の媒体が押収され、入手される前に、有形の形態によっても（例えば、プリントアウト）、物理媒体（例えば、ディスケット）の上にある無形のデータという形態によっても、その複製が作成さなければならない。データの複製が作成される後者の 2 つの場合に

号は、「差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること」と、それぞれ定めている。これは、「記録媒体」の差押えに関する規定である。これらの条項から、厳密には、コンピュータデータ（電磁的記録）のみを対象とする差押えについて定めているのは、同法第 99 条の 2 のみである。

[1] [訳注] 刑事訴訟法第 102 条第 1 項は、「裁判所は、必要があるときは、被告人の身体、物又は住居その他の場所に就き、捜索をすることができる」と定め、同条第 2 項は、「被告人以外の者の身体、物又は住居その他の場所については、押収すべき物の存在を認めるに足りる状況のある場合に限り、捜索をすることができる」と定めている。また、同法第 218 条第 1 項は、「検察官、検察事務官又は司法警察職員は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、差押え、記録命令付差押え、捜索又は検証をすることができる。この場合において、身体の検査は、身体検査令状によらなければならない」と定めている。同法第 220 条は、逮捕の現場における差押、捜索または検証について定めている。

[2] [訳注] 刑法第 7 条の 2 は、「電磁的記録」について、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう」と定義している。

おいては、データの複製[1]は、なお、コンピュータシステムまたは記録装置内に残されている。国内法は、そのような複製物を作成する権限を定めるものとしなければならない[2]。第 3 に、捜索された特定のコンピュータ内にはデータが記録保存されていないが、他のコンピュータシステムと接続することにより、システムを通じてデータに難なくアクセスすることができるかもしれない。それは、当該コンピュータに直接接続された付随的なデータ記録装置[3]の中に記録保存されているかもしれないし、また、インターネットのような通信システムを介して間接的にコンピュータと接続されたデータ記録装置[4]の中に記録保存されているかもしれない。このことは、データが現実に記録保存されている場所へと捜索を拡張すること（または、捜索されるコンピュータのある場所からデータを検索すること）、あるいは、より共同的で応急的なやり方で、その両方の場所で在来型の捜索権限を使用することを許容するための新たな法律を必要とするかもしれないし、それを必要としないかもしれない[5]。

188. 第 1 項は、加盟国に対し、法執行機関が、コンピュータシステムの中にあるデータまたは（接続されたデータ記録装置のような）システムの一部の中にあるデータもしくは（CD-ROM や磁気ディスクのような）独立した記録媒体上にあるデータに対してアクセスし、そして、それを捜索する権限をもつことを求めている。第 1 条中の「コンピュータシステム」の定義は「何らかの装置または相互接続されもしくは相互に関連する一群の装置」を指していることから、第 1 項は、1 個の独立したコンピュータシステムを相互に構成するものと考えることのできるコンピュータシステム及びそれと関連する機器類（例：プリンタや関連記録装置を伴う PC やローカルエリアネットワークなど）の捜索を関連するものである。時として、他のシステムまたは記録装置に記録保存されているデータは、他の独立したコンピュータシステムとの接続を確立することによって、捜索されるコンピュータシステムを介して適法にアクセスし得る[6]。この場合については、通信ネットワークによって同じ領土内にある他のコンピュータシステムとの間でなされている連携（例えば、ワイドエリアネットワ

---

[1] [訳注] ここで「複製（copy）」と述べているのは、原本に相当するデータのことである。

[2] [訳注] 刑事訴訟法第 99 条第 2 項、第 99 条の 2、第 107 条第 1 項、同条第 2 項、第 110 条の 2、第 123 条第 3 項、第 218 条第 2 項、第 219 条参照

[3] [訳注] ケーブル等によって物理的に直接に接続されたミラーサーバやバックアップサーバまたはデータ記録用の機器類等を指すものと解される。

[4] [訳注] 通信解説を介して論理的に接続された遠隔地にあるミラーサーバやバックアップサーバ、あるいは、クラウドストレージを含め、インターネット上の各種ストレージ等を指すものと解される。

[5] [訳注] 刑事訴訟法第 218 条第 2 項は、「差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であって、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる」と定めている。

[6] [訳注] ネットワーク環境ではむしろ当然のこととだと言えるが、サイバー犯罪条約が締結された時代における技術の状況を考えると、ネットワーク接続が必ずしも一般に普及していたわけではないので、この点が強調されているということを理解することができる。なお、時代背景（特に技術の開発及び普及の状況）を正確に理解することの重要性については、法と情報雑誌 1 巻 4 号に収録した欧州評議会個人データ保護条約の参考訳の脚注でも指摘したとおりである。

ークまたはインターネット）を含め、第 2 項で対応している。

189. 「コンピュータデータを記録保存することができるコンピュータデータ記録媒体」（第 1 項の(b)）の捜索及び押収は、在来型の捜索権限を用いて実施することができるかもしれないが、コンピュータの捜索を実行する場合には、しばしば、直接の攻撃対象となったコンピュータシステムの中にあるコンピュータシステムに対する捜索と関連するコンピュータデータ記録媒体（例えば、磁気ディスク）に対する捜索の両方が必要となる。このような関係があることを考慮して、第 1 条中には、その両方の場合を包含できるようにするための包括的な法的権限が規定されている[1]。

190. 第 19 条は、記録保存されたコンピュータデータについて適用される。この点に関して、名宛人が彼または彼女のコンピュータシステムにそれをダウンロードするまで ISP のメールボックス内で保留状態にある未開封の電子メールメッセージは、記録保存されたコンピュータデータとして理解されるべきか、それとも、伝送中のデータとして理解されるべきか、という問題が生ずる。幾つかの加盟国の法律では、そのような電子メールメッセージは、通信の一部であり、それゆえ、その内容は、通信傍受の権限を適用することによってのみ入手することができる。他方、別の法制度では、そのようなメッセージは、第 19 条の適用のある記録保存されたデータとして理解されている。従って、加盟国は、自国の国内法制度上ではどのようなものが適切であるかを決定するために、この問題に関して、自国の法律を見直さなければならない[2]。

191. 「捜索及び押収」という用語が参照されている。伝統的な言葉である「捜索」を用いる

---

[1] [訳注] 刑事訴訟法第 99 条第 2 項及び同法第 218 条第 2 項が規定する場合がそれに該当すると解することは可能である。

[2] [訳注] 現時点では、暗号化された電子メールの復号を求める手続及びその適法性について議論がある。暗号化された電子メールは、特殊な技術的方法によって封のされた電文であると考えることができ、その開封を求める手続が必要となるからである。刑事訴訟法第 111 条第 1 項は、物理的に開封することのできる紙の封書について、「差押状、記録命令付差押状又は捜索状の執行については、錠をはずし、封を開き、その他必要な処分をすることができる。公判廷で差押え、記録命令付差押え又は捜索をする場合も、同様である」と定めている。ところが、電子的な文書の強制的な開封に相当する同法第 111 条の 2 は、「差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状又は捜索状の執行をする者は、処分を受ける者に対し、電子計算機の操作その他の必要な協力を求めることができる。公判廷で差押え又は捜索をする場合も、同様である」と定めるものの、協力を求められた者（例：暗号化された電文を復号するための復号鍵を記憶している者）が任意の協力を拒んだ場合、その協力を強制する方法が存在しないからである。この設例のような場合、例えば、記憶の開示を強要するための薬剤を投与する方法、催眠術を用いる場合や特殊な電磁波により人工的・強制的に思考させる場合を含め、本人が同意していないのに心理的な誘導によって強制的に記憶を開示させる方法、あるいは、当該の者の脳内の記憶を電磁的に直接に検索する方法等を用いることは、適法な証拠収集行為とは認められず、許されない。同法第 111 条の 2 の「協力」は、被疑者または被告人以外の者によるものであるが、このような場合においても、被告人の供述の場合と同様に任意性を要すると解するべきである。そして、その任意性を欠く「協力」によって得られた証拠は、「毒樹の果実」の理論により、その証拠能力を否定すべきであると解する。このような場合においては、検証または鑑定等の純粋に技術的な方法によって暗号化された電文を復号しなければならない。なお、説明書の第 202 項参照。

ことによって、国家による強制権限の行使という観念が持ち込まれるのであり、そして、本条の中に示す権限が在来型の捜索のアナロジーであることが示されている。「捜索」は、データの探索、閲読、検査または評価を意味する。これは、データを求める捜索とデータの捜索（検討）という意味を含んでいる。他方において、「アクセス[1]」という語は、中立的な意味を有するが、これは、より正確にコンピュータ技術を反映している。これらの用語は、伝統的な概念と現代の技術とを結合するために用いられている。

192. 本節の中の全ての条項がそうであるように、「その領土内において」という指示は、国内法のレベルでとられるべき措置のみに関連することを示す注記である。

193. 第 2 項は、求めるデータが他のコンピュータシステムの中に記録保存されていると信ずる根拠を有する場合には、捜査機関が、当該他のコンピュータシステムまたはその一部に対してその捜索またはこれに類するアクセスを拡張することを許している。しかしながら、当該他のコンピュータシステムまたはその一部は、「その領土内に」所在するのでなければならない[2]。

194. 条約は、捜索の拡張がどのように許容されまたは実施されるのかについては、何も規定していない。それは、国内法に任されている[3]。幾つかの可能な要件の例がある。すなわち、捜索される特定のデータが接続されたコンピュータシステム内に含まれているかもしれないと信ずるべき根拠が存在する場合、特定のコンピュータシステムをコンピュータ捜索する権限を有する司法機関その他の機関に対し、（国内法及び人権上の安全確保措置によって求められる程度で）当該接続されたコンピュータシステムに対する捜索またはこれに類するアクセスを拡張することを認めること、あるいは、他のコンピュータシステム内に捜索される特定のデータが含まれているかもしれないと信ずるべき根拠が存在する場合、特定のコンピュータシステムを捜索する権限を与えられた捜査機関に対し、当該接続されたコンピュータシステムに対する捜索またはこれに類するアクセスを拡張することを認めること、あるいは、協力措置及び応急措置の中で、その両方の場所で、捜索またはこれに類するアクセスを実施することである。これら全ての場合において、捜索されるデータは、当初のコンピュータシステムから適法にアクセス可能なものでなければならない。

195. 本条は、司法共助という通常のチャネルを通じて実施することなく、他の国の領土内にあるデータを捜索及び押収することのできる「国境を越えた捜索及び押収」には適用されない[4]。この問題については、国際協力に関する章において後述する。

---

[1] [訳注] 説明書の第 46 項参照

[2] [訳注] クラウドコンピューティングサービスの場合に関しては、第 173 項の脚注（訳注）参照。

[3] [訳注] 日本国においては、刑事訴訟法第 99 条第 2 項及び同法第 218 条第 2 項が規定する場合がそれに該当すると解することは可能である。

[4] [訳注] 世界規模でのクラウドコンピュータサービスの場合、ある国の法執行機関（警察）による権限の行使が国境を越えて行われているものであるか否かが不明確・不明瞭なものとなる。また、データが断片化され、多数のサーバに分散して所在している場合、あるいは、Bitcoin のようなブロックチェーン技術の応用の場合を含め、多数のサーバが連携してデータを管理している場合等には、その一部に対して捜査権限を行使すると、自動的に他国の領土内にある別のデータにもその影響が及ぶことになる。特に、集中管理型のシステムでは、断片化されたデータを全体として統御する中枢システムを捜索すると、他の国の領土上にある断片化されたデータ全てを捜索するのと同じ結果を得ることが

196. 第 3 項は、第 1 項または第 2 項に基づき、コンピュータデータの捜索またはこれに類するアクセスをする権限の職務権限を有する機関に対する付与に適用される。これは、コンピュータハードウェア及びコンピュータデータ記録媒体を押収する権限を含む。例えば、複製できない特別のオペレーティングシステム上でデータが記録保存されているような場合には、そのデータキャリア全体を押収することが不可避となる。また、上書きされてはいるが、データキャリア上にその痕跡が残されている古いデータを検索するために、データキャリアを調査しなければならない場合にも、それが必要になるかもしれない[1]。

197. この条約においては、「押収」は、データもしくは情報が記録された物理媒体を入手すること、または、当該データもしくは情報の複製を作成し、保存[2]することを意味する。「押収」は、押収されるデータを使用すること、または、それにアクセスするために必要なプロ

できる場合があり、実質的に捜査機関や諜報機関による「big brother」を実現することが技術的に可能な場合がある。それゆえ、そもそも自国の領土内においてのみ権限を行使するように制限することが電子的・技術的に可能なのかどうかという根本的な部分からの再検討を要すると考えられる。

[1] [訳注] 現時点で一般的に普及している製品では、全ての部品が 1 個のもの（ユニット、アセンブリ）として一体化されており、電源部、記録装置部、演算装置部といったようなコンポーネントを個別に分離することができないことが多い。このような場合には、物理的に、当該装置全体を押収せざるを得ない。問題となるのは、複数のユニットが小規模 LAN 等によって連携して動作するようになっている場合である。このような場合には、1 個のユニットだけでは動作せず、関係する全てのユニットを連携させて捜査を遂行しなければならない。例えば、自動車では、複数の各種センサーユニット、電源管理ユニット、エンジン制御ユニット、ブレーキ制御ユニット、車内の環境管理ユニット等が車内無線 LAN を介して連携して動作するようになっている場合がある。そのようなタイプの自動車のコンピュータシステム（ユニット、無線 LAN システム）のいずれかに対してハッキング、DDoS 攻撃またはマルウェア感染等の加害行為が実行され、何らかの犯罪を構成し得る死傷事故が発生したという事例を想定してみると、そのような事例では、疑いのあるユニットだけを個別に吟味してみても事故原因を解明することができず、車内無線 LAN 及び各ユニットとの連携的な処理の全体について検討を加えなければならない。それゆえ、このような事例では、結局、当該車両全部を押収しなければならなくなる。更には、いわゆる「コネクテドカー（connected car）」のように、無線通信を介して外部のクラウドサーバ上のコンピュータ処理と常に連携しながら走行する車両では、実質的な演算処理は、車内のユニットによってではなく、外部にあるクラウドサーバ上で実行されることになることから、個々の車両の事故の場合であっても、極論すれば、当該車両と無線通信を介して連携しているクラウドサーバ及びそれと連携している人工知能システム等の全体を物理的に押収して調査・検討する必要が生ずるような場合があり得る（この場合、無線通信によって接続されているネットワークシステム全体を 1 個のユニットとして理解することになる。）。以上のような問題を考えてみると、サイバー犯罪条約における「捜索」及び「押収」だけでは全く対応できないような時代に入ってしまっていることが明らかであるので、IoT の時代に対応する捜査方法に関する追加議定書（additional protocol）の起草及び締結が急務となっていると考えられる。加えて、各国の普通の警察当局の捜査能力だけでは国際的規模の大規模なクラウドサーバや人工知能システムに対する捜査を効果的に遂行することは事実上不可能と推定されるので、航空機事故の場合や原子力発電所事故の場合と同様に、国際的なレベル及び各国のレベルの両方において、その分野における専門家等によって構成される人工知能システム事故調査委員会のような制度的な仕組みを構築する必要があるのではないかと考えられる。

[2] [訳注] 原文は、「retain」となっているが、データ保持指令 2006/24/EC における「保持（retention）」とは異なる意味で用いられているので、「保存」と訳すことにした。

グラムを押収することを含む。「押収」という在来型の用語を用い、それと並んで、無形のデータを消去し、アクセスできないようにし、または、その管理を奪うためにコンピュータ環境の中で実行される従来の意味以外の意味を反映するために、「それに類する確保」という用語が含められている。この措置は記録保存された無形のデータに関するものであるので、職務権限を有する機関は、データの押収のための付加的な措置が求められる。すなわち、「データの完全性を維持」すること、または、データの「管理の連鎖」を維持することである。それは、複製または消去されるデータを、押収の時点で発見された状態で保存し、そして、刑事訴訟手続がなされている間は変更されない状態にしておくことを意味する[1]。この用語は、データの管理を奪うこと、または、データを入手することを指している。

198. データをアクセス不能な状態にすることは、データの暗号化その他の技術的な方法によって、当該データに対して誰もアクセスできないようにすることを含むものとすることができる[2]。この措置は、通常、ウイルスプログラム、または、ウイルスや爆弾[3]を製造するための命令のような危険もしくは社会的脅威が含まれている場合[4]、あるいは、データまたはコンテントが児童ポルノのような違法なものである場合[5]に適用される。「消去[6]」という用語は、

---

[1] [訳注] この部分の記述は、サイバー犯罪条約が締結された当時の時点における標準的なデータやコンテンツに対する認識・理解を前提としている。今後、ネットワーク環境が更に進展すると、ネットワークシステムとリアルタイムで連携し、生成されるデータやコンテンツが増加することが見込まれる。この場合、固定的という意味でのデータやコンテンツは存在せず、リアルタイムでの何らかのイベントの発生が存在するだけになる。その場合、ある瞬間をとらえたキャプチャとしてのデータの押収は可能かもしれないが、刑事訴訟手続（捜査手続及び公判手続）が維持されている間、完全に不変なものとして維持することは、原理的に不可能である。一般に、事実認定とは、元来、現時点で存在する資料に基づいて過去の出来事を推定する思考作業のことを意味し、過去それ自体を保存することはできない。その意味で、「真相の発見」は、常に、不可能である。

[2] [訳注] 個々のデータまたは記録媒体全体を暗号化するランサムウェア（ransomware）を用い、暗号化されたデータ等を復号するのと引き換えに金銭を要求する恐喝型攻撃（ransom 攻撃）を想定すると理解しやすい。近年、個人に対しても法人に対してもこのような攻撃が頻発するようになった。ランサム攻撃及びその刑事責任については、前掲「サイバー犯罪の研究（六）－違法な電子メールに関する比較法的検討－」で述べた。

[3] [訳注] ここでいう「ウイルス（viruses）」及び「爆弾（bombs）」は、コンピュータウイルス（computer virus）や論理爆弾（logic bomb）のことを指すのではなく、テロ攻撃や戦争において物理的な兵器として用いられる可能性のあるウイルスまたは細菌、爆弾その他の爆発物のことを指すと解される。現在のインターネット上では、このような脅威度の高い生物化学兵器や原子爆弾を含む爆発物の製造方法と関連する情報を比較的容易に入手することが可能である。

[4] [訳注] Cybercrime Convention Committee (T-CY), T-CY Guidance Note #7: New Form of Malware (4-5 June 2013)が参考になる。

[5] [訳注] 児童ポルノに該当する違法なデータや著作権法違反となるような違法なデータのことを指すと解される。わいせつ画像の頒布等を犯罪行為としている国では、わいせつ画像も含まれることになるし、わいせつ性が肯定される場合でなくても、いわゆるリベンジポルノとして脅迫や強要の用に供される画像についても同じである。いわゆるリベンジポルノに関する日本国の法令としては、私事性的画像記録の提供等による被害の防止に関する法律（平成 26 年法律第 126 号）がある。

[6] [訳注] 原文は、「removal」となっている。物理的な破壊による消滅とは異なるものであることを明らかにしている。データの抑制（suppression）の一種として理解することができる（説明書の第 61 項参

データが消去またはアクセス不能となっている間は、それが破壊されず、存在し続けているという考えを表現しようとする趣旨である。容疑者は、一時的にデータから排除されるが、犯罪捜査または刑事手続が終了すれば、その返還を受けることができる[1]。

199. そして、押収されまたはこれに類する確保されたデータは、2 つの機能を有している。すなわち、1) データの複製のような方法によって証拠を収集すること、2) データを複製し、

照)。

[1] [訳注] 刑事訴訟法第 498 条の 2 第 1 項は、「不正に作られた電磁的記録又は没収された電磁的記録に係る記録媒体を返還し、又は交付する場合には、当該電磁的記録を消去し、又は当該電磁的記録が不正に利用されないようにする処分をしなければならない」と定め、同条の 2 第 2 項は、「不正に作られた電磁的記録に係る記録媒体が公務所に属する場合において、当該電磁的記録に係る記録媒体が押収されていないときは、不正に作られた部分を公務所に通知して相当な処分をさせなければならない」と定めている。なお、捜査の目的で電磁的記録の複製物を作成する行為は、刑事訴訟法の適用範囲内にある限り、適法行為となり得る。しかし、公判が終了し、判決が確定した後の時点においては、犯罪捜査の目的も終了していることになることから、当該複製物である証拠が訴訟記録の中に取り込まれた場合において後の裁判記録閲覧の際に適用される法令（民事訴訟法第 91 条、刑事訴訟法第 53 条）等の何らかの特別の法令に基づくものでない限り、捜査段階で作成された複製物が著作権法の適用のある著作物に該当する場合には、観念的には、複製行為及び複製物を所持する行為についての正当な理由（または違法性阻却事由）が消滅していることになるので、著作権法に定める複製権侵害物であることになる。

この点に関して、著作権法第 42 条第 1 項は、「著作物は、裁判手続のために必要と認められる場合及び立法又は行政の目的のために内部資料として必要と認められる場合には、その必要と認められる限度において、複製することができる。ただし、当該著作物の種類及び用途並びにその複製の部数及び態様に照らし著作権者の利益を不当に害することとなる場合は、この限りでない」と定めている。しかし、起訴猶予となった事件の起訴前の手続は、厳密には「裁判手続」ではなく、判決が確定した後の時点においては明らかに「裁判手続」が存在しない。問題は、「行政の目的のために内部資料として必要と認められる場合」の該当性であるが、専ら有罪判決を得るための立証の目的で行われる捜索・押収の結果として入手された電磁的記録の複製物を他の行政目的のために転用して用いることは、強制捜査について令状主義を採用している本旨と完全に矛盾するものであり、行政上の特別の必要性がある場合等を除き、原則として、複製物を保存・維持する行為は認められないと解する。なお、厳密には、還付または破棄すべき複製物を還付または破棄しないで保存・維持する行為が不作為による新たな複製行為を構成すると解することもできる。また、同法第 49 条は、同条に定める行為を「複製を行ったものとみなす」が、同条に列挙される以外の行為が複製行為に該当しないとする解釈は、理論的に成立し得ず、複製行為とみなされなくても証拠によって証明されれば複製行為に該当し得る。

著作権法第 42 条第 1 項の解釈に関する著作権法の通説の見解は、私見と反対である（前掲中山信弘『著作権法（第 2 版）』357～359 頁、岡村久道『著作権法』（商事法務、2010）271～272 頁参照）。しかし、一般に、捜査手続における強制処分としての複製物の作成行為は、公権力の行使による私権の制限の場合に該当するので、私人対私人の関係における公正な利用に関する法理等が適用されることはない。第 42 条第 1 項の解釈・適用に関する限り、私人の権利（著作権法上の権利）の保護を重視した解釈が望ましいことは言うまでもなく、可能な限り厳格にこれを解釈すべきである。ただし、従来、ここで述べたような公判手続に供されなかった証拠である電磁的記録の複製物及び公判終了後の証拠である電磁的記録の複製物と著作権法上の複製権との関係という論点について判示した裁判例はなく、また、この論点に関して重点的に検討を加えた論説等は見当たらない。今後の検討課題とすべきものであるが、立法的な解決を図ることがより望ましいと考える。

そして、元のデータをアクセス不能または消去するなどして、データを差し押さえることである。押収は、押収されたデータを完全に削除することを意味しない[1]。

200. 第 4 項は、コンピュータデータの捜索及び押収を容易にするための強制措置を導入する。これは、処理及び記録保存され得るデータの量、防護措置の設定並びにコンピュータ業務の性質に鑑み、証拠として求めるデータへアクセスすること及びその識別が困難であるかもしれないという実務上の問題に対応するものである。コンピュータシステムに関して特別の知識を有するシステム管理者は、いかにして最善の捜索手続を実施すべきかについての技術的な方式に関し、協議に応じる必要があるかもしれないということが認識された。それゆえ、本項は、法執行機関が、システム運営者に対し、それが合理的であるときは、捜索及び押収の実施を支援するように強制することを認めている[2]。

201. この権限は、捜査機関にとって利益となるだけのものではない。そのような協力がなければ、捜査機関は、捜索をしている間ずっと捜索場所に居座り、そして、捜索が実施されている時間内はコンピュータシステムへのアクセスを禁止するかもしれない[3]。このことは、その間においてデータに対するアクセスを禁止される正当な企業または顧客及び加入者に対して、経済的な負担をかけることになる。知識を有する者に協力を求める措置は、捜査機関のためにも、影響を受ける罪のない個人のためにも、捜索をより効果的なものとし、かつ、費用効率をより良くする助けとなることであろう。支援すべきことをシステム運営者に対して法的に強制することは、データを開示しないことについての契約上の義務その他の義務からシステム運営者を解放することにもなる。

202. 提出を命ずることのできる情報は、捜索もしくは押収またはそれに類するアクセスもしくは確保を実施することができるようにするために必要な情報である。しかしながら、この情報の提出は、「合理性」のあるものに制限されている。ある状況下では、合理性のある提出は、捜査機関に対してパスワードまたはその他の防護手段を開示することまで含むことになるかもしれない。しかしながら、別の状況下では、それは、合理性があるとは言えないか

---

[1] [訳注] 捜査官が複製元のデータを物理的に破壊して消去した場合において、後に、嫌疑不十分により不起訴となった場合、または、無罪判決が確定した場合には、当該捜査官によるデータの破壊・消去行為は、違法行為であることになる。この場合、被告人（被疑者）に対しては国家補償が行われ得るし、また、被告人（被疑者）及び関係者に対しては国家賠償法の適用があり得ると考えられるが、従来の判例における理解を前提とすると、データの破壊について適正な補償・賠償が行われる可能性は著しく低いと考えざるを得ない。特に、既述のとおり、クラウドコンピューティングサービスのプロバイダがシステム全体を押収されてしまった後に無罪が確定したような場合には、天文学的な数字（金額）に及ぶ損失が発生する可能性がありながら、法的には何らの補償もされ得ないという事態が発生し得る。しかしながら、現代社会における電子データやネット上のサービス提供のためのシステム運営の重要性に鑑みると、不起訴や無罪の場合におけるデータ喪失による損失について、国が何らかのかたちで補填する制度を確立し、また、関連する保険契約の設計のための検討が望まれる。

[2] [訳注] 説明書の第 190 項の脚注（訳注）参照

[3] [訳注] 刑事訴訟法第 112 条第 1 項は、「差押状、記録命令付差押状又は捜索状の執行中は、何人に対しても、許可を得ないでその場所に出入りすることを禁止することができる」と定め、同条第 2 項は、「前項の禁止に従わない者は、これを退去させ、又は執行が終わるまでこれに看守者を付することができる」と定めている。

もしれない。例えば、パスワードまたはその他の防護手段の開示によって、捜索されることが承認されていない他の利用者のプライバシーやデータが合理性なく脅かされ得るような場合がそうである。そのような場合、「必要な情報」の提出とは、職務権限を有する機関によって求められる具体的なデータの認識可能で閲読可能な方式による開示となる。

203. 本条の第 5 項により、その措置は、この条約の第 15 条を基礎とする国内法に基づいて定められる条件及び安全性確保措置に従う。そのような条件は、証言及び専門知識の提供及びそのための費用支弁に関する条項を含むことができる。

204. 起草者は、更に、第 5 項の枠組みの中において、押収手続の実施について利害関係者が通知を受けるものとすべきか否かについても討議した[1]。オンラインの世界で行われる捜索または押収（複製）されるデータのほうが、オフラインの世界で行われる押収よりも、押収される対象物が物理的に失われる可能性が低いということが明らかであるとは言えない。幾つかの国々の法律は、在来型の捜索の場合において告知の義務を定めていない[2]。それゆえ、も

[1] [訳注] 原文には「ピリオド（.）」がないが、誤記の一種と判断して訳すことにした。

[2] [訳注] 刑事訴訟法第 113 条第 1 項は、「検察官、被告人又は弁護人は、差押状、記録命令付差押状又は捜索状の執行に立ち会うことができる。ただし、身体の拘束を受けている被告人は、この限りでない」と定め、同条第 2 項は、「差押状、記録命令付差押状又は捜索状の執行をする者は、あらかじめ、執行の日時及び場所を前項の規定により立ち会うことができる者に通知しなければならない。ただし、これらの者があらかじめ裁判所に立ち会わない意思を明示した場合及び急速を要する場合は、この限りでない」と定め、同条第 3 項は、「裁判所は、差押状又は捜索状の執行について必要があるときは、被告人をこれに立ち会わせることができる」と定めている。また、同法第 114 条第 1 項は、「公務所内で差押状、記録命令付差押状又は捜索状の執行をするときは、その長又はこれに代わるべき者に通知してその処分に立ち会わせなければならない」と定め、同条第 2 項は、「前項の規定による場合を除いて、人の住居又は人の看守する邸宅、建造物若しくは船舶内で差押状、記録命令付差押状又は捜索状の執行をするときは、住居主若しくは看守者又はこれらの者に代わるべき者をこれに立ち会わせなければならない。これらの者を立ち会わせることができないときは、隣人又は地方公共団体の職員を立ち会わせなければならない」と定めている。更に、同法第 115 条は、「女子の身体について捜索状の執行をする場合には、成年の女子をこれに立ち会わせなければならない。但し、急速を要する場合は、この限りでない」と定めている。

なお、近未来において、人間の身体に埋め込まれた人工臓器その他のインプラント型 IoT 機器類や電子チップの捜索・押収手続（強制処分）の一種として、当該機器類や電子チップ内に記録保存されているデータの複製物を入手する場合に、同法第 115 条の規定及び関連する他の規定の重要性が増加するかもしれない。問題は、現在普通に使用されている非有機体の機器類（電子チップ等）ではなく、有機体である人工細胞に一定のデータを遺伝子符号として埋め込んだ細胞塊（カルス）である有機体ロボットのようなものを人間の身体内に移植しているような場合である。このような場合には、外形上では人間の身体に同化してその一部となってしまっている細胞または組織の一部を切除して確保し、当該分野における専門的な知識・技能・解析手段を有する者による遺伝子解析を実施するのでなければ、当該細胞内に遺伝子符号という形態で存在しているデータを入手することができない。このような有機コンピュータまたは有機ロボットの応用である細胞（有機質の人工臓器・人工細胞等）の中にある証拠を確保すべき場合については、在来型の通常の捜索・押収・身体検査の方法や通常の情報提出命令では対処できない場合が圧倒的に多くなると見込まれる。今後、新たな刑事上の証拠確保手段が検討されなければならないであろう。その場合において、当該の者を殺害して身体の全ての組織・細胞を細断・検査しなければ必要な情報を入手することができないといったような極限的な状況が発

し条約がコンピュータ捜索に関して告知を求めるとすれば、これらの国々の法律との矛盾を発生させることになるだろう。他方で、幾つかの国々は、（一般に、隠密の措置であることが意図されていない）記録保存されたデータのコンピュータ捜索と（隠密の措置であり、第 20 条及び第 21 条によってなされる）通信中のデータの傍受とを区別するために、告知がこの措置の基本的な特徴であると判断するかもしれない。それゆえ、この告知の問題は、国内法による決定に任される。関係者に対して義務的に告知をする制度が必要だと加盟国が判断する場合、そのような告知が犯罪捜査の妨げとなり得るということに留意すべきである。そのようなリスクがある場合には、告知の延期を検討しなければならない。

第 5 款　コンピュータデータのリアルタイム収集

205. 第 20 条及び第 21 条は、コンピュータシステムによって伝送される特定の通信と関係するトラフィックデータのリアルタイム収集及びコンテントデータのリアルタイム傍受について定めている。これらの条項は、職務権限を有する機関によるそのようなデータのリアルタイム収集及びリアルタイム傍受並びに、サービス提供者によるそれらの収集または傍受を定めるものである[1]。守秘義務についても定めている。

206. 通信傍受は、通常、在来型の通信ネットワークに関するものである[2]。これらのネットワークは、電線または光ケーブルの別を問わず、有線の通信インフラ、並びに、携帯電話システム及びマイクロウェーブ伝送システムを含め、無線ネットワークの相互接続を含むことができる[3]。今日、携帯通信は、特別の衛星ネットワークというシステムによっても促進され

生し得るということも想定した検討がなされるべきである。

[1] [訳注] 前者は、法執行機関（警察）による通常の通信傍受行為のことを意味する。後者は、ISP 等による通信傍受行為を意味する。いずれも特定の被疑者について、特定の犯罪行為の容疑との関係で、到底の通信に関して行われるものであるので、データ保持指令 2006/24/EC に基づくデータの保持（data retention）とは異なる。

[2] [訳注] 通信傍受法第 2 条第 1 項は、「通信」について「電話その他の電気通信であって、その伝送路の全部若しくは一部が有線（有線以外の方式で電波その他の電磁波を送り、又は受けるための電気的設備に附属する有線を除く。）であるもの又はその伝送路に交換設備があるものをいう」と定義し、同条第 2 項は、「傍受」について「現に行われている他人間の通信について、その内容を知るため、当該通信の当事者のいずれの同意も得ないで、これを受けることをいう」と定義し、同条第 3 項は、「通信事業者等」について「電気通信を行うための設備（以下「電気通信設備」という。）を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供する事業を営む者及びそれ以外の者であって自己の業務のために不特定又は多数の者の通信を媒介することのできる電気通信設備を設置している者をいう」と定義している。それゆえ、例えば、人間の脳内にインプラントされた電子機器類を用いて人間とコンピュータ装置との間で直接に通信が行われる場合、または、人間の脳と他の人間の脳との間で直接に通信が行われる場合、複数の人間の脳が連結され関係者全員が全ての脳を共有するような場合、人間の脳が中枢となる人工知能コンピュータに連結されそのパーツとしてのみ機能するような場合について、通信傍受法を適用することができない（説明書の第 98 項の脚注（訳注）参照）。

[3] [訳注] 日本国の法制においては、通信傍受法第 2 条第 1 項により、伝送路に交換設備のない無線通信は通信傍受可能な対象から除外されている。しかし、暗号化されていない無線通信の電磁的放射（エミッション）は、誰でも受信可能なものであり、かつ、誰でも受信することができる通信手段である

ている。コンピュータネットワークもまた、独立した固定ケーブルによる通信インフラにより構成されている場合もあるが、むしろ、通信インフラを介して形成される接続によるバーチャルなネットワークとして運営されることが多く、そして、本質的にグローバルなコンピュータネットワークまたはネットワークの連携を創り上げることを許している。通信とコンピュータ通信との相違及びそのインフラ相互の相違は、通信と情報技術とが相似しているために明瞭ではない。そして、第 1 条にある「コンピュータシステム」の定義[1]は、接続装置または一群の装置が相互に接続され得る手法を制限するものではない[2]。それゆえ、第 20 条及び第 21 条は、コンピュータシステムという手段によって伝送される特定の通信に対して適用される[3]。それは、それが他のコンピュータシステムによって受信される前の通信ネットワークを介した通信の伝送を含めることができる。

207. 第 20 条及び第 21 条は、公的に保有されもしくは民間で保有される通信システムもしくはコンピュータシステムまたはそのシステムの利用と、公開もしくは非公開の利用者グループまたは私的団体に対して提供される通信サービスとの間に、区別を設けていない。第 1 条の中にある「サービス提供者」の定義は、その利用者に対し、コンピュータシステムという手段によって通信をする能力を提供する公的な主体または民間の主体を指している。

208. 本款は、通信がなされている時（すなわち、「リアルタイム」）に収集される現在生成中の通信に含まれる証拠の収集を規律している。データは、その形態において無形である（すなわち、音声または電気信号の伝送という形態である。）。収集によってデータの流れが大きく妨げられることはなく、また、通信は、意図された受信者に到達する。データの物理的な押収の代わりに、通信中のデータの記録（すなわち、複製）が行われる。この証拠の収集は、一定の期間内に実施される。収集の許可をする司法機関は、将来の出来事（例えば、将来の

ことを当該通信手段の利用者が認識可能なものであるので、暗号化されていない無線通信の電磁的放射を警察当局が受信して証拠とすることは、任意捜査の範囲内で可能である（説明書の第 57 項参照）。

[1] [訳注] 説明書の第 23 項、第 24 項、第 35 項及び第 56 項参照

[2] [訳注] サイバー犯罪条約を実装する国内法が「コンピュータシステム」がスタンドアロンのコンピュータシステムに対してのみならず、相互接続され、ネットワークを構成しているコンピュータシステムに対しても適用があるという趣旨と解される。ただし、コンピュータシステムを構成要素としない古典的なアナログの電話網のようなものは除外される。

[3] [訳注] 特定の通信に限定されない包括的な通信傍受は、サイバー犯罪条約に定める「傍受」に含まれない。包括的な傍受の代表例としては、エシュロン（Echelon）による衛星通信の傍受がある。エシュロンについては、Nicky Hager, Secret Power: New Zealand's Role in the International Spy Network, Craig Potton Publishing (1996)及び European Parliament, The ECHELON Affair: The EP and the global interception system 1998-2002 (November 2014)が参考になる。また、各国の軍当局または諜報機関による包括的な傍受一般については、David E. Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, Broadway Books (2013)、Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Broadway Books (2015)、James Bamford, The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America, Anchor (2009)、Matthias Runkel, The Great Firewall of China. Political and economical implications of the Great Shield, GRIN Verlag GmbH (2015)、Richard J. Aldrich, GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency, HarperCollins Publishers (2011)、Nasser Abouzakhar (Ed.), Eccws 2015 - Proceedings of the 14th European Conference on Cyber Warfare and Security, Acpil (2015) 及び江畑謙介『情報と戦争』（NTT 出版、2006）がある。

データ伝送）に関して求められる。

209. 収集可能なデータには、トラフィックデータとコンテントデータという 2 つのタイプのものがある。すなわち、「トラフィックデータ」は、第 1 条の中において、コンピュータシステムによって行われる通信に関するコンピュータデータであって、コンピュータシステムによって生成され、かつ、通信の連鎖の一部を構成し、その通信の発信地、受信地、経路、時刻、日付、サイズ、持続時間またはサービスのタイプを示すものを意味するものとして定義されている[1]。「コンテントデータ」は、条約中では定義されていないが、通信における通信内容を指す。例えば、通信の意味または意図、通信によって運搬される（トラフィックデータ以外の）メッセージまたは情報である[2]。

210. 多くの国々において、この捜査手段を承認するための法律上の要件及びこの措置を実施することができる犯罪に関する要件の両方の要件との関係で、コンテントデータのリアルタイム傍受とトラフィックデータのリアルタイム収集とが区別されている。どちらのタイプのデータもプライバシーの利益と関連することが認識されているが、多くの国々では、コンテントデータと関係するプライバシーの利益は、通信内容またはメッセージというその性質から、より重要なものであると考えられている。コンテントデータのリアルタイム収集については、トラフィックデータのそれよりも大きな制限が加えられ得る。これらの諸国での区別の理解を助けるために、条約は、運用上では、どちらの場合でもデータが収集または記録されることを認めつつも、名目上では、トラフィックデータ収集に関する条項の標題を「リアルタイム収集」とし、コンテントデータの収集の標題を「リアルタイム傍受」としている。

211. 幾つかの国々では、プライバシーの利益に関連して法律上の区別を設けていないという理由、あるいは、どちらの措置でも技術を利用した収集で用いられる技術が非常に良く似ているという理由で、トラフィックデータのリアルタイム収集とコンテントデータのリアルタイム傍受との間に区別を設けていない。そして、措置の実施を承認するための法律上の要件及び措置を実施することのできる犯罪に関する要件は、同じである。条約は、このような状

---

[1] [訳注] 日本国の通信傍受法の適用・実施においては、例えば、電話番号の探知がこのトラフィックデータの収集に該当する。現状では、コンピュータシステムによって自動的に制御・管理される IP 電話が普及しているため、電話番号の探知もコンピュータシステムを用いた通信におけるトラフィックデータに該当することに疑問はない。しかし、かつて、交換機を介してなされるアナログ回線が主流であった時代にあっては、そのような通信回線はコンピュータシステムを用いた通信に該当しないため、単に通信傍受法が制定され存在するというだけでは日本国の法制がサイバー犯罪条約に適合していない可能性があった（このような疑問は、現時点では、事実上、ほぼ解消されていると考えることができる）。なお、説明書の第 30 項及び第 217 項参照。

[2] [訳注] 日本国の通信傍受法の適用・実施においては、例えば、電話の通話内容がこのコンテントデータの収集に該当する。なお、通信傍受法第 29 条に基づき、国（法務省）は、毎年、通信傍受の実施内容を公表している。平成 27 年 2 月 6 日に公表された平成 26 年（2014 年）の実施状況によれば、通信傍受が実施された被疑事件の罪名は、大麻取締法違反（営利目的の大麻栽培）、覚せい剤取締法違反（営利目的の覚醒剤譲渡）、麻薬特例法違反（業として行う覚醒剤等の譲渡等）及び銃砲刀剣類所持等取締法違反（拳銃の発射、拳銃の加重所持）であり、通信手段の種類は、携帯電話のみとなっている。携帯電話による通話については、無線による通信手段であって有線による通信ではないけれども、それは、交換機（コンピュータシステムによって制御される自動交換機）を用いる通信経路を介した通信となるので、通信傍受法の適用がある。

況にあることを認識して、第 20 条及び第 21 条の実際の条文の中においては、「収集または記録」という用語を共通に用いている。

212. コンテントデータのリアルタイム傍受に関しては、法律は、しばしば、重大な侵害行為の捜査または重大な侵害行為の類型に属する行為の捜査に関係する場合にのみ、この措置を適用することができると定めている[1]。これらの侵害行為は、国内法により、しばしば、適用され得る侵害行為のリストの中で列挙するという方法によって、または、侵害行為に対して適用される拘禁刑の一定の最長期間を示すことで侵害行為の類型の中に含めるという方法によって[2]、この措置を適用するための重大な侵害行為として識別されている。それゆえ、コンテントデータの傍受に関して、第 21 条は、加盟国が「国内法によって定められる重大な侵害行為の程度と関連して」措置を設けることを求めるということを特に規定している。

213. 他方、トラフィックデータの収集に関する第 20 条は、そのような制限があるわけではないが、原則として、この条約が適用される刑事犯罪に対して適用される。しかしながら、第 14 条第 3 項は、加盟国が、留保の中で指定する侵害行為または侵害行為の類型についてのみ措置を適用する権利を留保することができると規定している。ただし、侵害行為または侵害行為の類型の幅は、コンテントデータの傍受に適用されるものよりも狭いものであってはならない。そのような留保がなされている場合であっても、加盟国は、トラフィックデータの収集という措置を最大限幅広く適用することができるように、その留保を抑制することを検討すべきである。

214. 幾つかの国々にとって、条約の中で設けられる侵害行為は、コンテントデータの傍受を許容するのに十分なだけ重大であるとは考えないかもしれないし、場合によっては、トラフィックデータの収集についてさえもそうであるかもしれない。けれども、コンピュータシステムに対する違法アクセス、コンピュータウイルスや児童ポルノの配布を含む侵害行為のような条約の中で設けられる幾つかの侵害行為を捜査するためには、しばしば、このような技術が決定的なものとなる。例えば、事案によっては、トラフィックデータのリアルタイム収集なしには侵入または配布の発信地を確定することができない[3]。また、事案によっては、コ

---

[1] [訳注] 通信傍受法が定める重大犯罪については、説明書の第 142 項の脚注（訳注）参照。

[2] [訳注] 例えば、コモンローの諸国では、通例、重罪（felony）という概念を用いて重大な犯罪行為を識別し、重い刑を科すものとしている。例えば、故意による殺人（murder）が重罪（felony）に該当する犯罪行為の例とされる。重罪（felony）は、更に幾つかの等級（degree）に分類され、その重大性評価に差を設けられるのが通例である。英語の「felony」は、語それ自体としては、中世のフランス語である「félonie」に由来するものと考えられている。重罪（felony）の反対概念は、軽罪（misdemeanor）である。

[3] [訳注] 不正アクセス行為のようなサイバー攻撃の範疇に含まれる行為は、犯罪行為を構成し得るものであると同時に、他方では、コンピュータシステムやネットワークの安全性を脅かす脅威または社会の安全を脅かすテロ攻撃の一部でもあり得るので、後者の観点から、情報セキュリティの担当者と警察との連携によって、その発信地の迅速な探知（検出及び追跡）が実施されることが多い。すなわち、犯罪捜査のためのトラフィックデータの通信傍受という方法によってではなく、情報セキュリティ上の防御行為（正当行為）として当該トラフィックデータの調査・分析が行われ、その分析結果を示す情報が情報セキュリティの専門家と警察との間で共有されることが通例である。その結果、通信傍受法の適用によってトラフィックデータの収集が行われることは、基本的にない。この関係では、

ンテントデータのリアルタイム傍受なしには、通信の性質を発見することができない。これらの侵害行為は、その性質または伝送手段によっては、コンピュータ技術の利用を含むものである[1]。それゆえ、これらの侵害行為を捜査するために、技術的な手段の使用が認められなければならない。しかしながら、コンテントデータの傍受という問題を取り巻く機微性のゆえに[2]、条約は、この措置の適用範囲を国内法に任せている。トラフィックデータの収集とコンテントデータの傍受とを法律上では同じものとしている幾つかの国々については、前者の措置の適用範囲について、コンテントデータのリアルタイム傍受措置を加盟国が限定するよりも大きくない範囲内で限定する留保をすることが認められる。ただし、加盟国は、これらコンピュータ犯罪及びコンピュータと関連する犯罪を捜査するための効果的な措置を定めるために、条約の第 2 章第 1 節で設けられる犯罪に対して、これら 2 つの措置を適用することを検討しなければならない。

215. コンテントデータのリアルタイム傍受及びトラフィックデータのリアルタイム収集に関する権限及び手続に関する条件及び安全性確保措置は、第 14 条及び第 15 条による。コンテントデータの傍受は、私生活に対する重大な侵害的措置となるので、司法上の利益と個人の基本的な権利との間の適切なバランスを確保するために、厳格な安全性確保措置が求められる[3]。傍受の領域については、この条約は、それ自体としては、捜査のためにコンテントデータの傍受をする権限を国内法に定める重大な刑事犯罪の範囲内に限定する以外、特に安全性確保措置を設けていない。しかし、この領域における以下のような重要な条件及び安全性確保措置が国内法の中で適用されている[4]。すなわち、司法機関その他の独立の機関による監

情報セキュリティ対策推進会議官民連携のための分科会「情報セキュリティ対策に関する官民連携の在り方について」（平成 24 年 1 月 19 日）、情報セキュリティ対策会議「情報セキュリティ対策における連携の推進について－総合セキュリティ対策会議報告書」（平成 14 年 3 月）が参考になる。

[1] [訳注] 例えば、特定の Web ページを閲覧すると自動的にマルウェアに感染するような仕組みを設けることによる攻撃、攻撃用パケットの送信により実行される DDoS 攻撃、サーバの脆弱性や技術的特性を悪用したリフレクション攻撃等は、純粋に技術的な方法によるサイバー攻撃の一種であり、通信内容の人間による意味内容の理解の可能性の有無とは全く無関係に、当該問題となるパケットの送受信のみによって攻撃対象に対して侵害的な結果を発生させるものである。このようなタイプの侵害行為については、当該問題のあるパケットの発信地を追跡し、1 秒でも早くそのパケットの発信地（IP アドレス）や様々な障害の原因となっているサーバや機器類の所在地（IP アドレス）を検出・特定することが重要となることが多い。

[2] [訳注] 通信内容の探知行為が通信当事者のプライバシー侵害をダイレクトに発生させ得るということを示している（説明書の第 51 項、第 142 項、第 143 項、第 163 項、第 210 項、第 211 項及び第 230 項参照）。

[3] [訳注] 説明書の第 132 項及び第 154 項の脚注（訳注）参照

[4] [訳注] 通信傍受法第 5 条第 2 項は、「裁判官は、傍受令状を発する場合において、傍受の実施（通信の傍受をすること及び通信手段について直ちに傍受をすることができる状態で通信の状況を監視することをいう。以下同じ。）に関し、適当と認める条件を付することができる」と定めている。また、同法第 12 条第 1 項は、「傍受の実施をするときは、通信手段の傍受の実施をする部分を管理する者又はこれに代わるべき者を立ち会わせなければならない。これらの者を立ち会わせることができないときは、地方公共団体の職員を立ち会わせなければならない」と定め、同条第 2 項は、「立会人は、検察官又は司法警察員に対し、当該傍受の実施に関し意見を述べることができる」と定めている。更に、同

督、傍受される通信または傍受される者の特定、必要性、補充性及び比例性（例えば、措置を講ずることを正当化する法律上の事由、他のより侵害的でない措置では効果がないこと）、傍受期間の限定、救済の権利である[1]。これらの安全性確保措置の多くは、欧州人権条約及びその後の判例法に反映されている（Klass 事件[2]、Kruslin 事件[3]、Huvig 事件[4]、Malone 事件[5]、Halford 事件[6]、Lambert 事件[7]の判決参照）。これらの安全性確保措置の幾つかは、トラフィックデータのリアルタイム収集にも適用可能である。

トラフィックデータのリアルタイム収集（第 20 条）

216. しばしば、履歴を示すトラフィックデータがもはや利用されなくなっているかもしれず、あるいは、侵入者が通信経路を変更してしまうことにより、意味のないものとなってしまっているかもしれない。それゆえ、トラフィックデータのリアルタイム収集が重要な捜査手段となる。第 20 条は、特定の犯罪捜査または訴訟手続のためのトラフィックデータのリアルタイム収集及び記録の対象について定めている。

217. 従来、通信に関連するトラフィックデータ（例えば、電話による通話内容）の収集は、発信地または受信地（例えば、電話番号）を確定し、様々なタイプの違法な通信（例えば、犯罪的な脅迫やハラスメント、犯罪の謀議または詐欺的な表現）と関連し、過去または将来の犯罪（例えば、麻薬取引、殺人、経済犯罪等）の証拠となる通信と関連するデータ（例えば、時刻、日付及び通話時間）を確定するための有用な捜査手段であった。

218. コンピュータ通信は、同様のタイプの犯罪を構成し得るものであるし、また、その証拠となり得るものでもある。しかしながら、コンピュータ技術は、書面、視覚画像及び音楽を含め、膨大な量のデータの伝送を可能とするものであるので、違法なコンテント（例えば、児童ポルノ）の配布を含む犯罪を実行することについても大きな可能性を与えてしまっている[8]。同様に、コンピュータは、しばしば私的な性質を有する膨大な量のデータを記録保存す

法第 15 条は、「医師、歯科医師、助産師、看護師、弁護士（外国法事務弁護士を含む。）、弁理士、公証人又は宗教の職にある者（傍受令状に被疑者として記載されている者を除く。）との間の通信については、他人の依頼を受けて行うその業務に関するものと認められるときは、傍受をしてはならない」と定めている。

[1] [訳注] 通信傍受法第 22 条第 5 項は、「検察官又は司法警察員は、傍受をした通信であって、傍受記録に記録されたもの以外のものについては、その内容を他人に知らせ、又は使用してはならない。その職を退いた後も、同様とする」と定めている。

[2] ECHR Judgment in the case of *Klass and others* v. *Germany*, A28, 06/09/1978

[3] ECHR Judgment in the case of *Kruslin* v. *France*, 176-A, 24/04/1990.

[4] ECHR Judgment in the case of *Huvig* v. *France*, 176-B, 24/04/1990.

[5] ECHR Judgment in the case of *Malone* v. *United Kingdom*, A82, 02/08/1984.

[6] ECHR Judgment in the case of *Halford* v. *United Kingdom*, Reports 1997 – III, 25/06/1997.

[7] ECHR Judgment in the case of *Lambert* v. *France*, Reports 1998 – V, 24/08/1998.

[8] [訳注] サイバー犯罪条約の追加議定書（ETS No.189）に加盟している国においては、更に、人種差別的な言動を含む通信が違法な通信となる。日本国の関連法令としては、本邦外出身者に対する不当な差別的言動の解消に向けた取組の推進に関する法律（平成 28 年法律第 68 号）がある。同法第 2 条は、「この法律において「本邦外出身者に対する不当な差別的言動」とは、専ら本邦の域外にある国若

ることができるものであるので、そのデータの完全性が害されると、経済的、社会的または個人的の別を問わず、危害の潜在的可能性がかなり大きなものとなり得る。更に、コンピュータ技術に関する科学は、最終製品としても、運用機能（例えば、コンピュータプログラムの実行）の一部としても、データの処理を基礎とするものであるので、このデータに対する侵害は、コンピュータシステムの本来の運用に対して恐るべき悪影響を与え得る。児童ポルノの違法な配布、コンピュータシステムに対する違法なアクセスまたはコンピュータシステムの本来の機能もしくはデータの完全性に対する干渉が、とりわけインターネットを介してなされる場合にように遠隔地からなされると、被害者から通信経路を遡って容疑者を追跡することが必要的かつ決定的なものとなる。それゆえ、コンピュータ通信と関係するトラフィックデータの収集は、仮に従来から行われていた単純な通信における傍受の重要性よりも大きなものではないとしても、それと同等に重要なものである。この捜査技術は、容疑者の通信の時刻、日付並びに発信地及び受信地と被害者のシステムへの侵入時刻とを関連付け、他の被害者の有無を識別し、あるいは、共犯者との連携を証明することができる。

219. 本条に基づき、関係するトラフィックデータは、加盟国の領土内における特定の通信と関連するものでなければならない[1]。関係者及び受信地を確定するために、複数の通信と関連するトラフィックデータが収集されなければならないかもしれないので、特定の「通信」は、複数形である（例えば、複数の人間が同じ通信機器を使用する家庭内においては、個々の通信と個人がコンピュータシステムを使用する機会とを関係付ける必要があるかもしれない。）。しかしながら、トラフィックデータを収集または記録することのできる通信は、特定されなければならない[2]。そして、条約は、膨大な量のトラフィックデータを一般的にまたは無限定に捜査し収集することを求めてはいないし、それを承認するものでもない。幸運に任せて犯罪行為を見つけようとする「証拠漁り（fishing expeditions）」は、捜査される犯罪の特定性に欠けるので、認められない。裁判所の命令その他の命令によって収集を承認する場合には[3]、それによって関係するトラフィックデータを収集するための通信を特定するものとし

しくは地域の出身である者又はその子孫であって適法に居住するもの（以下この条において「本邦外出身者」という。）に対する差別的意識を助長し又は誘発する目的で公然とその生命、身体、自由、名誉若しくは財産に危害を加える旨を告知し又は本邦外出身者を著しく侮蔑するなど、本邦の域外にある国又は地域の出身であることを理由として、本邦外出身者を地域社会から排除することを煽動する不当な差別的言動をいう」と定義している。

[1] [訳注] 通信傍受法第 6 条は、「傍受令状には、被疑者の氏名、被疑事実の要旨、罪名、罰条、傍受すべき通信、傍受の実施の対象とすべき通信手段、傍受の実施の方法及び場所、傍受ができる期間、傍受の実施に関する条件、有効期間及びその期間経過後は傍受の処分に着手することができず傍受令状はこれを返還しなければならない旨並びに発付の年月日その他最高裁判所規則で定める事項を記載し、裁判官が、これに記名押印しなければならない。ただし、被疑者の氏名については、これが明らかでないときは、その旨を記載すれば足りる」と定めている。

[2] [訳注] 通信傍受法第 8 条は、「裁判官は、傍受令状の請求があった場合において、当該請求に係る被疑事実に前に発付された傍受令状の被疑事実と同一のものが含まれるときは、同一の通信手段については、更に傍受をすることを必要とする特別の事情があると認めるときに限り、これを発付することができる」と定めている。

[3] [訳注] 通信傍受法第 4 条第 1 項は、「傍受令状の請求は、検察官（検事総長が指定する検事に限る。次項及び第 7 条において同じ。）又は司法警察員（国家公安委員会又は都道府県公安委員会が指定する

なければならない。

220. 第 2 項により、加盟国は、第 1 項の(a)に基づき、自国の職務権限を有する機関が技術的手段によってトラフィックデータの収集または記録をする能力を確保することを義務付けられている[1]。条項は、技術的にどのようにして収集がなされるべきかについて定めておらず、また、技術的な要件に関する義務については何も規定されていない[2]。

221. 加えて、第 1 項の(b)に基づき、自国の職務権限を有する機関が、サービス提供者に対し、トラフィックデータを収集もしくは記録させる権限、または、そのようなデータの収集もしくは記録について職務権限を有する機関と協力させまたは援助させる権限を有することを確保するように加盟国を義務付けている。サービス提供者に関するこの義務は、収集もしくは記録または協力もしくは援助についてのサービス提供者の現時点における技術的能力の範囲内においてのみ、適用される[3]。本条は、サービス提供者に対し、サービス提供者が収集、記録、協力または援助を遂行するための技術的能力を持つことを確保するように義務付けていない。本条は、サービス提供者に対し、新たな装置を入手または開発することを求めていないし、費用をかけて専門家の支援を受けることやそのシステムを再構築することを求めてもいない。しかしながら、サービス提供者のシステムまたは人的資源がそのような収集、記録、協力もしくは援助を提供するための技術的能力を実際に有している場合には、本条は、サービス提供者に対し、その技術的能力を用いるために必要な措置を講ずべき義務を課している。例えば、システムは、そのような措置を許容するように構築されているかもしれないし、サービス提供者はそのような措置を許容するコンピュータプログラムを既に有しておりながら、サービス提供者事業の普通の業務遂行においては、通常、それらが実行されておらず、使用されてもいないかもしれない。本条は、法律によって命じられるものとして、サービス提供者がそれらの機能を稼働させ、または、開始させることを要求する。

222. これらは、国内法のレベルで実施されるべき措置であるので、加盟国の領土内にある特定の通信の収集または記録に適用される。そして、実際上の制約により、この義務は、一般

警視以上の警察官、厚生労働大臣が指定する麻薬取締官及び海上保安庁長官が指定する海上保安官に限る。同項及び同条において同じ。）から地方裁判所の裁判官にこれをしなければならない」と定め、同条第 2 項は、「検察官又は司法警察員は、前項の請求をする場合において、当該請求に係る被疑事実の全部又は一部と同一の被疑事実について、前に同一の通信手段を対象とする傍受令状の請求又はその発付があったときは、その旨を裁判官に通知しなければならない」と定めている。

[1] [訳注] 通信傍受法第 10 条第 1 項は、「傍受の実施については、電気通信設備に傍受のための機器を接続することその他の必要な処分をすることができる」と定め、同条第 2 項は、「検察官又は司法警察員は、検察事務官又は司法警察職員に前項の処分をさせることができる」と定めている。

[2] [訳注] 日本の捜査官のサイバー犯罪に関する現実の捜査能力に関しては、前掲「ケーススタディ・サイバー犯罪捜査（1）－不正指令電磁的記録供用事件:プロキシサーバを経由している犯人にたどり着くー」、同「ケーススタディ・サイバー犯罪捜査（2）－威力業務妨害・脅迫・不正指令電磁的記録供用事件:遠隔操作ウィルス事件を基にー」、「ケーススタディ・サイバー犯罪捜査（3・完）－不正アクセス禁止法違反事件:Tor で隠れる犯人を捜す手段を探るー」が参考になる。

[3] [訳注] 通信傍受法第 11 条は、「検察官又は司法警察員は、通信事業者等に対して、傍受の実施に関し、傍受のための機器の接続その他の必要な協力を求めることができる。この場合においては、通信事業者等は、正当な理由がないのに、これを拒んではならない」と定めている。

に、サービス提供者がその措置を遂行することのできる物理的なインフラまたは機器類を加盟国の領土内に持っている場合に負わせることができるが、その主たる事業または経営者の所在地が領土内にあることを要しない。この条約においては、通信当事者（人間もしくはコンピュータ）の一方がその領土内に所在する場合、または、通信が経由するコンピュータ装置もしくは通信装置がその領土内に所在する場合には、その通信は、加盟国の領土内でなされるものである、ということが了解されている。

223. 一般に、第 1 項の(a)及び(b)のトラフィックデータの収集に関する 2 つの可能性は、選択可能なものではない。第 2 項に規定する場合を除き、加盟国は、両方の措置を実施できるようにすることを確保しなければならない。その必要があるのは、サービス提供者がトラフィックデータの収集または記録（第 1 項の(b)）を引き受けることのできる技術的能力を有していない場合には、加盟国は、その法執行機関が自らその職務を遂行することができるようにしなければならないからである（第 1 項の(a)）。同様に、トラフィックデータの収集及び記録について職務権限を有する機関に協力し及び援助すべきものとする第 1 項の(b)(ii)の義務は、職務権限を有する機関が自らトラフィックデータの収集または記録をする権限を有していないのであれば、無意味である。加えて、サービス提供者が何ら関与していないローカルエリアネットワーク（LAN）の場合には、収集または記録を実施するための唯一の方法は、捜査機関が自らそれをすることとなるであろう。第 1 項の(a)及び(b)の措置は、いつでも同時に用いることを要しないが、本条によって、そのどちらの措置も用いることができるようにすることが求められている。

224. しかしながら、この 2 重の義務は、法執行機関がサービス提供者の援助を通じてのみ通信システム中のデータを傍受することができるような国、または、少なくとも、サービス提供者の知識を借りなければ隠密に実施することができないような国に対しては、困難をもたらすことになる。このため、第 2 項は、そのような状況を緩和している。加盟国が、「その国内法の制度上で確立された諸原則を遵守すると」第 1 項の(a)に規定する措置を導入することができない場合には、この措置に代えて、法執行機関によるトラフィックデータのリアルタイム収集を確保するために、サービス提供者に対し必要な技術の提供を強制することのみとするといったような異なる手法を導入することができる。このような場合においても、領土、通信の特定性及び技術的手段の使用に関連する他の全ての要件が適用される。

225. コンテントデータのリアルタイム傍受と同様に、トラフィックデータのリアルタイム収集は、捜査を受けている者が気づいていない間に実施される場合にのみ、効果的である。傍受は、隠密になされるものであり、そして、通信当事者がその捜査が実施されていることに気づかないような方法で実施されなければならない。傍受がなされていることを知っているサービス提供者及びその従業者は、従って、刑事手続が効果的に実施されるようにするために、守秘義務を負うものとしなければならない[1]。

226. 第 3 項は、加盟国が、サービス提供者に対してトラフィックデータのリアルタイム収集

[1] [訳注] 通信傍受法第 28 条は、「検察官、検察事務官及び司法警察職員並びに弁護人その他通信の傍受に関与し、又はその状況若しくは傍受をした通信の内容を職務上知り得た者は、通信の秘密を不当に害しないように注意し、かつ、捜査の妨げとならないように注意しなければならない」と定めている。同条の違反行為については、罰則の適用がある（同法第 30 条）。なお、説明書の第 226 項参照。

に関連して本条に規定する措置の実施についての事実及び情報の秘密を維持すべき義務を負わせるために必要となる立法及びその他の措置を講ずることを、加盟国に義務付けている。この条項は、捜査の機密性を確保するだけではなく、サービス提供者が、加入者に対して、加入者のデータが収集されているということを通知すべき契約上の義務またはその他の法律上の義務から、サービス提供者を解放することにもなる。第 3 項は、法律で、明示の義務を設けることによって、これを有効なものとすることができる。他方において、加盟国は、その措置について告げてしまうことによって犯罪を助ける者を司法妨害として起訴する権限といったような、他の国内法上の条項に基づいて、措置の機密性を確保することができる。（その違反の場合には効果的な制裁を伴う）特定の機密保持の要件を設けることが手続として好まれるとしても、不適切な情報開示を阻止し、かつ、本項の実装を促進するために、司法の妨害となる侵害行為を用いること[1]を選択することができる。明示の機密保持義務が設けられる場合には、その義務は、第 14 条及び第 15 条に規定する条件及び安全性確保措置に従う。これらの安全性確保措置または条件は、犯罪捜査上の措置という隠密的な性格に鑑み、機密保持義務を負わせるための合理的な期間を定めるものとしなければならない[2]。

227. 上述のとおり、プライバシーの利益は、一般に、トラフィックデータの収集に関してはコンテントデータの傍受の場合よりも低いものと考えられている。通信の時刻、接続時間及びサイズに関するトラフィックデータは、個人の個人情報または彼もしくは彼女の思想に関する個人情報を暴露するものでは全くない。しかしながら、通信の発信地または受信地についてのデータ（例えば、訪問した Web サイト）に関しては、より厳しいプライバシー問題があるかもしれない[3]。一定の場合には、このデータの収集は、個人の嗜好、人間関係及び社会的関係のプロファイルの編集を許してしまうことになるかもしれない[4]。従って、加盟国は、第 14 条及び第 15 条に従い、そのような措置を実施するためのしかるべき安全性確保措置及び法律上の要件を設ける場合には、この点に留意しなければならない。

---

[1] [訳注] 犯罪捜査妨害罪または刑事訴訟妨害罪を制定することを指す。

[2] [訳注] 説明書の第 225 項の脚注（訳注）参照

[3] [訳注] 一般個人データ保護規則(EU) 2016/679 の第 4 条の(1)は、「個人データ」の意義について、「識別される自然人または識別可能な自然人（以下「データ主体」という。）に関する全ての情報を意味する。識別可能な自然人とは、とりわけ、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、または、当該自然人の肉体的、生理的、遺伝的、精神的、経済的、文化的または社会的な同一性を示す 1 以上の要素を参照することによって、直接的または間接的に、識別され得る者のことである」と定義し、また、同条の(4)は、「プロファイリング」の意義について、「自然人と関連する一定の人格的側面を評価するために、とりわけ、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析または予測するために、個人データの利用によって構成される全ての形態の個人データの自動的な処理を意味する」と定義している。そして、同規則第 22 条第 1 項は、「データ主体は、プロファイリングを含め、自動化された処理のみに基づいて 、彼もしくは彼女に関する法的効果を発生させ、または、彼もしくは彼女に対して同様に重大な悪影響を及ぼすような判定の対象とされない権利を有する」と定めている。

[4] [訳注] 現時点では、このような自動解析または自動的なプロファイリングが一般に普及してしまっている。個人データの保護との関連では、個人データの目的外利用の規制強化ないし厳罰化という方策以外に適切かつ効果的な法的手段・方法が存在しないのではないかと考えられる。

コンテントデータの傍受（第 21 条）

228. 従来、通信と関連するコンテントデータ（例えば、電話による通話内容）の収集は、その通信が違法な性質を有する通信（例えば、犯罪的な脅迫やハラスメント、犯罪の謀議または詐欺的な表現を構成する通信）であることを確定するための、あるいは、過去または将来の犯罪（例えば、麻薬取引、殺人、経済犯罪等）の証拠を収集するための、有用な捜査手段であった[1]。コンピュータ通信は、同様のタイプの犯罪を構成し得るものであるし、また、その証拠ともなり得る[2]。しかしながら、コンピュータ技術は、書面、視覚画像及び音楽を含め、膨大な量のデータの伝送を可能とするものであるので、違法なコンテント（例えば、児童ポルノ）の配布を含む犯罪の実行についても大きな可能性を与えてしまっている[3]。コンピュータ犯罪の多くは、その実行行為の一部分としてデータの伝送または通信を含んでいる。例えば、コンピュータシステムへの違法アクセスまたはコンピュータウイルスの配布を実行するために送信される通信がそうである。メッセージの傍受なしには、これらの通信が危険で違法な性質を有するかどうかについて、リアルタイムで判定することができない。発展する犯罪の発生を確定し阻止する能力を持つことなしには、法執行機関は、損害が既に発生してしまった場合に、過去に実行された犯罪の捜査のみに捨て置かれることになるだろう[4]。従って、コンピュータ通信上のコンテントデータのリアルタイム傍受は、仮にそれ以上に重要なものではないとしても、電話のリアルタイム傍受とまさに同じ重要性を有するのである[5]。

229. 「コンテントデータ」は、通信上の通信内容を指している。例えば、通信の意味または意図、通信によって運ばれたメッセージまたは情報である。それは、通信の一部分として伝送されたものであって、トラフィックデータではないものの全てである[6]。

230. 本条の要件の大部分は、第 20 条の要件と同じである。それゆえ、トラフィックデータの収集または記録、協力義務及び支援義務並びに機密保持義務に関する上記の解説は、コンテントデータの傍受についても、同様に適用される。コンテントデータと関連する高度なプ

---

[1] [訳注] 通信傍受法の第 1 条は、「この法律は、組織的な犯罪が平穏かつ健全な社会生活を著しく害していることにかんがみ、数人の共謀によって実行される組織的な殺人、薬物及び銃器の不正取引に係る犯罪等の重大犯罪において、犯人間の相互連絡等に用いられる電話その他の電気通信の傍受を行わなければ事案を解明することが著しく困難な場合が増加する状況にあることを踏まえ、これに適切に対処するため必要な刑事訴訟法（昭和 23 年法律第 131 号）に規定する電気通信の傍受を行う強制の処分に関し、通信の秘密を不当に侵害することなく事案の的確な解明に資するよう、その要件、手続その他必要な事項を定めることを目的とする」と定めている。

[2] [訳注] この部分は、説明書の第 214 項とほぼ同じ内容を多く含んでいる。

[3] [訳注] この部分は、説明書の第 218 項と同じである。

[4] [訳注] この部分は、説明書の第 217 項と同じである。

[5] [訳注] この部分は、説明書の第 218 項とほぼ同じ内容を多く含んでいる。

[6] [訳注] 通信されるデータの中からトラフィックデータの部分を控除した残りは、全てコンテントデータであると趣旨と解される。技術論的には疑問が全くないわけではないが、少なくともサイバー犯罪条約におけるトラフィックデータとコンテントデータの区分は、そのような認識を前提とするものであるということを理解する必要がある。ただし、将来、量子通信が普及した状況の下においてもなお、このような区分が合理的なものとして維持可能か否かについては検討すべき余地がある。技術基盤の相違に適切に対応して、捜査手法の見直しが求められることになるであろう。

ライバシーの利益のために、この捜査手段は、「国内法によって定められる重大犯罪の範囲内」に限定される。
231. また、上記の第 20 条の説明にもあるとおり、コンテントデータのリアルタイム傍受に適用され得る条件及び安全性確保措置は、トラフィックデータのリアルタイム傍受または記録保存されたデータの捜索及び押収もしくはこれらに類するアクセスもしくは確保に適用される条件及び安全性確保措置よりも厳格なものとすることができる。

第 3 節　管轄権

管轄権（第 22 条）

232. 本条は、条約の第 2 条ないし第 11 条にある犯罪行為について管轄権を確立する義務を負っている条約加盟国が準拠すべき一連の基準を設けている。
233. 第 1 項の(a)は、属地主義の原則に基づいている。各加盟国は、この条約で設けられる犯罪が、その領土内で実行される場合には、その実行行為を処罰することが求められる。例えば、コンピュータシステムを攻撃する者と攻撃対象システムの両者がその領土内にある場合、また、攻撃者がその領土内に所在していなくても、攻撃を受けたコンピュータシステムがその領土内にある場合には、加盟国は、属地管轄権を主張することになるだろう。
234. 加盟国の名で登録された通信衛星が関与する侵害行為について各加盟国の管轄権を及ぼすことを求める条項を含めることについても討議がなされた。起草者は、通信衛星が関与する違法な通信は、いずれにしても、地球上のいずれかの地から発信され受信されるものであるので、そのような条項は必要がないと判断した[1]。そのことから、第 1 項の(a)ないし(c)に定める加盟国の管轄権は、通信の発信地または受信地のいずれかの地が加盟国内にある場合には、利用可能なものとなる。更に、衛星通信が関与する侵害行為が全ての国の地理的領土範囲の外で加盟国の国民によって実行される場合の適用範囲については、第 1 項の(d)が管轄権の根拠となるであろう。最後に、起草者は、通信衛星が伝送のための経路となることが滅多にないために、多数の事例においては、実行された侵害行為と登録国との間の関連性が存在しないことから、登録が犯罪の管轄権を確定するための根拠となるか否かについても検

[1] [訳注] 通信衛星ではなく、月面上に設置された通信施設を介して通信が行われる場合であっても、その発信地または着信地が地球上にある場合には同様に考えることができる。近未来的には、完全に自律型のロボットである宇宙ステーション施設が加害行為の主体となって、地球上の人類に危害を加えるような事態の発生が全くあり得ないとは言えない。このような場合、人間の加害者は存在しないことになるが、裁判管轄権及びそれに依拠する捜査権は、やはり、地球上の着信地及び被害発生地である国に属すると考えれば足りる。もっとも、もしそのような宇宙ステーション型ロボットから攻撃が行われる場合には、現実には、これをサイバー戦（Cyberwar）の一種として理解すべきか否かの問題はあるものの、いずれにしても当該宇宙ステーションを物理的に破壊する対物防衛行為が実施されることになるであろうと考えられることから、ロボット犯罪の問題として検討される現実の機会はほとんどないであろうと思われる。なお、完全に自律型のロボットの責任能力の有無や権利主体性等と関連する法哲学の領域における問題については、別途検討が必要である。この点については、前掲「アシモフの原則の終焉ーロボット法の可能性ー」で触れた。

討を加えた。

235. 第 1 項の(b)及び(c)は、属地主義からの派生原理を基礎としている。これらの号[1]は、各加盟国に対し、当該の国の国旗を掲げる船舶中で実行され、または、当該の国の法律に従って登録された航空機内で実行された侵害行為について、刑事上の管轄権を設けることを求めている。この義務は、多くの国の法律の中において、一般的な事項として、既に実装されている[2]。なぜなら、そのような船舶や航空機は、しばしば、その国の領土の拡張として考えられているからである[3]。このタイプの管轄権は、犯罪実行の時点ではその船舶や航空機が当該国の領土内に所在しておらず、従って、管轄権を主張するための管轄原因として第 1 項の(a)を用いることができないような場合には、最も有用である。加盟国の領土外にある船舶または航空機内で犯罪が実行された場合、この要件が存在しなければ、他のいかなる国といえども管轄権を行使することができなくなってしまうであろう。加えて、他国の領海上または領空上を通過しているのに過ぎない船舶または航空機の上で犯罪が実行される場合には、当該の国は、自国の管轄権を行使することについて、非常に大きな実務運営上の障碍があり[4]、そ

---

[1] [訳注] 第 1 項の(b)及び(c)のことを指す。

[2] [訳注] 刑法第 1 条第 1 項は、「この法律は、日本国内において罪を犯したすべての者に適用する」と規定し、同条第 2 項は、「日本国外にある日本船舶又は日本航空機内において罪を犯した者についても、前項と同様とする」と規定し、同法第 4 条の 2 は、「第 2 条から前条までに規定するもののほか、この法律は、日本国外において、第 2 編の罪であって条約により日本国外において犯したときであっても罰すべきものとされているものを犯したすべての者に適用する」と規定している。そして、不正アクセス禁止法第 14 条は、「第 11 条及び第 12 条第 1 号から第 3 号までの罪は、刑法（明治 40 年法律第 45 号）第 4 条の 2 の例に従う」と規定している。同様に、電波法第 109 条の 2 第 5 項は、「第 1 項、第 2 項及び前項の罪は、刑法第 4 条の 2 の例に従う」と規定している（電気通信事業法の適用のある暗号化された無線通信でありながら同法の罰則が適用されない事案について、電波法の国外犯処罰条項の適用があるか否かについては、罪数論として、検討の余地がある。特に外国取扱事業者の処罰との関係で問題となり得る。）。他方、刑法第 3 条柱書は、放火罪等の重大な犯罪について、「この法律は、日本国外において次に掲げる罪を犯した日本国民に適用する」と規定し、児童ポルノ禁止法第 10 条は、「第 4 条から第 6 条まで、第 7 条第 1 項から第 7 項まで並びに第 8 条第 1 項及び第 3 項（同条第 1 項に係る部分に限る。）の罪は、刑法（明治 40 年法律第 45 号）第 3 条の例に従う」と規定している。

[3] [訳注] 自動操縦ロボットの場合を含め、人間の関与なく、太陽電池や原子力等を用いてほぼ無補給で長期間運用を続行することのできる航空機や船舶（洋上を航行する船舶、潜水艦、航行・飛行・走行が可能なハイブリッド型のものを含む。）については、今後、検討すべき余地があるものの、前述のロボット型の宇宙ステーションと同様に考えることができるであろう。日本国内において、比較的短時間だけ操縦可能な無人航空機（ドローン）の場合には、日本国内にいる人間によって実行される犯罪行為の手段・手口の一種として理解することが可能な場合が多い。しかし、その操縦者が外国に所在し、日本国籍を有しない者であり、インターネット等を通じてなされる遠隔操作によって日本国内でドローンを操縦しているような場合には、犯罪実行地が日本国内にあるものとした上で、当該日本国籍を有しない操縦者に対する当該処罰法令の適用可能性（管轄権）を検討すべきことになる。なお、無人航空機に関する航空法第 132 条は、行為者の国籍を問わず、全ての者に対して適用されることから、同法第 157 条の 4 に定める罰則もまた全ての者に対して適用されると解すべきである。

[4] [訳注] 理論的には、自国の上空を通過中の航空機に対して軍用機をスクランブル発信させて自国の空港に強制着陸させた上で、自国の防衛権や警察権を行使することは可能である。それが国防上の問題として理解可能である場合には、自由通行に関する条約上の問題も生じない。しかし、それでは、

れゆえ、籍のある国にとっては、この場合にも管轄権を有することが非常に有用である。
236. 第 1 項の(d)は、属人主義の原則に基づいている。属人主義の理論は、国々によって最も頻繁に適用される民事法上の伝統的な理論である。国民は、国の領土外にある場合であっても、国内法に従うべき義務があるとされている[1]。(d)に基づいて、国民が国外で犯罪を実行する場合、その行為が行為地である国の法律によっても犯罪となり、または、その行為がいかなる国の属地管轄権にも属さない場所で実行されたときは、加盟国は、当該の国民を刑事訴追する能力を有しなければならない。
237. 第 2 項は、加盟国に対し、第 1 項の(a)、(b)、(c)及び(d)の管轄原因による管轄権について、留保を認めている。しかしながら、(a)に基づく属地管轄権を設けることに関して、そして、第 3 項に基づく「降伏か裁判か（*aut dedere aut judicare*）」（引渡か訴追か）の原則が適用されることになる場合において管轄権を設けるべき義務に関しては、留保が認められない。この管轄権があれば、例えば、加盟国がその国籍を原因として申し立てられた加害者の引渡を拒絶する場合、その加害者は、当該の国の領土内に所在することになる[2]。第 3 項に基づいて設けられる管轄権は、この条約の第 24 条第 6 項の「引渡」の要請を受けた加盟国が処罰しようとする場合において、その国民の引渡を拒絶した当該加盟国が、引渡をする代わりに、自国において捜査及び訴追をする法的権能を有することを確保することが必要である。
238. 第 1 項に規定する管轄権の管轄原因は、専属管轄ではない。本条第 4 項は、加盟国に対し、その国内法と適合するように、他のタイプの刑事管轄権を設けることも認めている。
239. コンピュータシステムを用いて実行される犯罪の場合、当該犯罪について、複数の加盟国の幾つかまたはその全部が管轄権を有することが同時に発生し得る。例えば、インターネットの使用を介して実行されるウイルス攻撃、詐欺及び著作権侵害行為の多くは、多数の国に位置する攻撃対象を狙っている。努力の重複、証人の無用な不便、関係各国の法執行機関

事実上、世界各国間での自由通行の可能性が著しく制限されてしまうことになる。そのため、少なくとも友好関係にある諸国においては、各国とも、そのような航空機や船舶に対する軍事上の実力の行使または警察権の行使については慎重な態度を示すことが多い（その逆もまた真である。例えば、紛争当事国間においては、対空ミサイルや対艦ミサイルの発射は、むしろ普通の出来事である。）。これは、法解釈の問題ではなく、国際政治上の問題または事実としての実力行使の損得勘定の問題である。

[1] [訳注] 説明書の第 235 項の脚注（訳注）参照

[2] [訳注] 説明書の第 237 項で説明されているとおり、この場合、当該加害者は、引渡を拒絶した国の裁判所において裁判を受けることになる。現実に発生している事例をみると、欧州連合基本権憲章第 19 条第 2 項が「いかなる者も、彼または彼女が死刑、拷問その他の非人間的または人間の尊厳を損なうような扱いまたは刑罰に服するかもしれない重大な危険性のある国に退去を命ぜられ、追放され、または、身柄引渡をされることがない」と定めていることを根拠として、死刑のある国への移送を拒絶する例が比較的多い。しかし、当該犯罪行為について死刑を定めている場合は別として、当該引渡を求める国の法律が当該犯罪行為について死刑を定めてらず、かつ、人間の尊厳を損なうような扱いまたは刑罰に服する可能性も認められない場合において、当該引渡を求める国の法律が当該犯罪行為とは全く関係のない別の重大犯罪について死刑を定めているということを根拠とすることは、欧州連合基本権憲章第 19 条第 2 項が本来予想している事態ではないと考えられる。この場合において、法定刑である拘禁刑が重いか軽いか、あるいは、複数の犯罪行為の刑について単純加算主義を採用しているか併合罪主義を採用しているかは、よほど極端な場合を除いては、原則として、当該国の立法裁量の範囲内に属するものであり、人権保障の問題とは直接の関係はない。

の間の競合を回避し、あるいは、手続の有効性または公正性を向上させるために、関係する加盟国は、適切な訴追地を定めるための協議をしなければならない。ある場合には、関係各国が 1 個の訴追地を選ぶことが有効かもしれない。また、他の場合には、ある加盟国が何人かの者を訴追する一方で、他の国が他の共犯者を訴追するのが最善であるかもしれない。本項は、このいずれの結論を採ることも認めている。最後に、協議すべき義務は絶対的なものではなく、「それが適切な場合に」なされるべきである。従って、例えば、加盟国中のある国が、協議を要しないと認識している場合（例えば、他の加盟国から起訴を予定していないという確認を得ている場合）、または、ある加盟国が、捜査及び刑事手続に対して協議が悪影響を及ぼすかもしれないという見解を持つ場合には、その協議を延期または拒絶することができる。

第 3 章　国際的な協力

240. 第 3 章は、加盟国間での引渡及び司法共助と関連する幾つかの条項を含んでいる。

第 1 節　一般原則

第 1 款　国際的な協力に関する一般原則

国際的な協力に関する一般原則（第 23 条）

241. 第 23 条は、第 3 章に基づく国際的な協力に関して、3 つの基本原則を定めている[1]。
242. 最初に、条文は、加盟国間において、「可能な限り広い範囲で」国際協力がなされなければならないことを明確にしている。この原則は、加盟国に対し、加盟国相互間での広範な協力関係を提供すること求め、そして、情報と証拠の国際的な移転を円滑にし、迅速にすることに対する障碍をミニマムなものとすることを求めている。
243. 第 2 に、協力義務の一般的な適用範囲は、第 23 条に規定するとおりである。すなわち、協力は、コンピュータシステム及びコンピュータデータと関連する全ての犯罪行為（例えば、第 14 条第 2 項の(a)及び(b)が適用される侵害行為）、並びに、犯罪行為の電子的な形態による証拠の収集に対して拡張されなければならない。このことは、犯罪がコンピュータシステムを用いて実行される場合、及び、コンピュータシステムを用いないで実行される普通の犯罪が電子的な証拠を含むものである場合の両方について、第 3 章の要件が適用され得るということを意味している。しかしながら、第 24 条（引渡）、第 33 条（トラフィックデータのリ

[1] [訳注] サイバー犯罪条約に定める基本原則は、ここに説明のある 3 つだけであるが、これらは、共助それ自体に関する基本原則である。しかし、共助に伴う個人データの移転に関しては、別途、法令が定められていることに留意しなければならない。例えば、警察分野における個人データの利用に関する勧告 No. R (87) 15（本誌 141～149 頁）の別紙にある「原則 5－データの送信」について定め、また、指令 (EU) 2016/680 の第 35 条ないし第 41 条は、捜査機関が保有する個人データの第三国移転について定めている。

アルタイム収集に関する共助）及び第 34 条（コンテントデータの傍受に関する共助）は、加盟国がこれらの措置について異なる適用範囲を定めることを認めているということには留意しなければならない。

244. 最後に、協力は、「本章の各条項に従い」、かつ、「刑事における国際協力に関する国際的な文書、統一的または互恵的な法律に基づいてなされた協定及び国内法の適用を通じて」実施されなければならない。後者の文言は、第 3 章の各条項が司法共助及び引渡に関する国際協定中の条項、加盟国間の互恵的な協定中の条項（これらについては、以下の第 27 条の検討中でより詳細に述べられている。）または国際協力を担う国内法上の関連条項を無効にするものではないということを確認している。この基本原則は、第 24 条（引渡）、第 25 条（共助に関する一般原則）、第 26 条（自発的な情報提供）、第 27 条（適用可能な国際合意がない場合における共助要請の手続）、第 28 条（機密性及び利用の制限）、第 31 条（記録保存されたコンピュータデータへのアクセスに関する共助）、第 33 条（トラフィックデータのリアルタイム収集に関する共助）及び第 34 条（コンテントデータの傍受に関する共助）の中において明示的に補強されている。

第 2 款　引渡に関する原則

引渡（第 24 条）

245. 第 1 項は、条約の第 2 条ないし第 11 条に従って設けられる侵害行為であって、関係する加盟国双方の法律に基づき、刑の長期が短くとも 1 年以上である自由刑またはそれよりも重い刑で処罰されるものについてのみ、引渡を適用すべき義務を定める。起草者は、最低刑をさしはさむことを決めた。何故なら、条約に基づき、加盟国は、幾つかの侵害行為（例えば、第 2 条の違法アクセス及び第 4 条のデータ妨害）について、比較的短い刑期の拘禁で処罰するかもしれないからである。だからといって、起草者は、第 2 条ないし第 11 条に設けられる侵害行為のそれぞれが引渡の対象とされるべきものとすることを求めることが適切であるとは考えなかった。その結果として、引渡に関する欧州条約（ETS No. 24）[1]の第 2 条にもあるように、引渡の対象となる侵害行為に科される刑罰が最短でも少なくとも 1 年以上の拘禁刑である場合には、その侵害行為を引渡の対象として考慮することができるという一般原則に到達して合意がなされた[2]。その侵害行為が引渡可能なものであるかどうかの判定は、

[1] [訳注] European Convention on Extradition (Paris, 13 December 1957)

[2] [訳注] 逃亡犯罪人引渡法（昭和 28 年法律第 68 号）の第 1 条第 1 項は、「引渡条約」について、「日本国と外国との間に締結された犯罪人の引渡しに関する条約をいう」と定義し、第 2 条柱書は、「左の各号の一に該当する場合には、逃亡犯罪人を引き渡してはならない。但し、第 3 号、第 4 号、第 8 号又は第 9 号に該当する場合において、引渡条約に別段の定があるときは、この限りでない」と定め、同条第 3 号は、「引渡犯罪が請求国の法令により死刑又は無期若しくは長期 3 年以上の拘禁刑にあたるものでないとき」と定めている。サイバー犯罪条約の第 24 条が逃亡犯罪人引渡法第 1 条第 1 項の「引渡条約」に該当すると解する場合、サイバー犯罪条約の加盟国間においては、同法第 2 条柱書ただし書により、長期 1 年以上の拘禁刑を法定刑とするサイバー犯罪については犯罪人引渡を認めることができることになる。この点について、前掲「「サイバー犯罪に関する条約」についてー手続法及び国際

眼前にある具体的な事件において実際に科された刑[1]に基づくのではなく、引渡が求められている犯罪行為に対して科され得る法定刑の長期によって決定される。

246. それと同時に、第 3 章に基づく国際協力は加盟国間で拘束力のある文書に従って行われなければならないという一般原則に従い、第 1 項は、また、統一的または互恵的な法律に基づいて、2 か国以上の加盟国間で拘束力のある引渡条約または相互協定が存在し（後述の第 27 条の検討におけるこの要件に関する記載を参照。）、それが引渡について異なる最低刑を要件としている場合には、その条約または相互協定に規定された最低刑が適用されなければならないと定めている。例えば、欧州各国と非欧州各国との間の引渡条約の多くは、刑の長期が 1 年の拘禁刑よりも重いかまたはそれよりも厳しい刑である場合にのみ、その犯罪行為が引渡可能であると定めている。このような場合、国際的な引渡の実務担当者は、当該侵害行為が引渡可能であるかどうかを判断するために、彼らの条約実務が基づき、通常の最低刑を適用し続けるだろう。引渡に関する欧州条約（ETS No. 24）に基づく場合においてさえ、引渡しのための異なる最低刑を定める留保をすることができる。その条約の加盟国の間において、そのような留保をした加盟国から引渡が求められた場合には、その侵害行為が引渡をすることができるものであるか否かを判断する際には、留保のために定められた刑罰が適用されなければならない。

247. 第 2 項は、本条第 1 項に示す侵害行為が、加盟国間に存在する引渡条約において引渡可能な侵害行為とみなされなければならず、そして、当該加盟国間で将来締結される引渡条約の中に含められなければならないと定めている。このことは、請求がなされた場合の全てについて引渡が認められなければならないということを意味するものではなく、むしろ、そのような侵害行為のためにその者の引渡を認めるかどうかを選択可能とするものでなければならない。第 5 項に基づき、加盟国は、引渡についてその他の要件を定めることができる。

248. 第 3 項に基づき、請求をする加盟国との間では引渡条約が存在しないという理由、または、この条約に従って設けられる侵害行為に関して行われた請求については既存の条約が適用されないという理由により、引渡を認めることができない加盟国は、請求を受けた者を引渡す根拠としてこの条約それ自体を用いることができる。ただし、そうすべきことが義務付けられているわけではない。

249. 加盟国が、引渡条約による代わりに、引渡を実施するための一般的な制定法というスキームを利用する場合には、第 4 項は、第 1 項の中に規定する全ての侵害行為について引渡を可能とするために、それらの侵害行為をその中に含めることを求める。

250. 第 5 項は、適用可能な引渡条約または法律に規定する全ての要件及び条件が満たされていない場合には[2]、請求を受けた加盟国が引渡をする必要がないと定めている。そして、これは、加盟国間で拘束力のある適用可能な国際文書、互恵的な協定または国内法の要件に従って協力がなされなければならないという原則の、もう 1 つの例である。例えば、引渡に関す

協力規定（中）」126 頁は、逃亡犯罪人引渡法第 2 条柱書ただし書を根拠として、「現行の同法で履行可能である」と解している。また、説明書の第 248 項では、サイバー犯罪条約の引渡に関する条項を根拠とすることができる旨を説明している。

[1] [訳注] 宣告刑のことを指す。

[2] [訳注] 原文はまわりくどい表現を用いているので、意訳した。

る欧州評議会条約（ETS No. 24）及びその追加議定書（ETS No. 86 及び ETS No. 98）の中に規定されている条件及び制限は、これらの合意の加盟国に対して適用され、そして、そのような理由に基づいて引渡を拒絶することができる（例えば、引渡に関する欧州条約第 3 条は、侵害行為が政治的な性質を有するものである場合[1]、または、とりわけ、人種、信教、国籍もしくは政治的意見を理由として訴追または処罰するためにその請求がなされたと考えられる場合には、引渡を拒絶しなければならないと規定している。）[2]。

251. 第 6 項は、「降伏か裁判か（*aut dedere aut judicare*）」（引渡か訴追か）の原則を適用する。多くの国々は、その国民の引渡を拒絶するので、加盟国内で発見された同国の国民である加害者は、国内の機関が訴追を義務付けられているのでない限り、他の加盟国内で実行した犯罪に対する責任を免れ得る。第 6 項に基づき、他の加盟国が加害者の引渡を請求した場合であり、かつ、その加害者が請求を受けた加盟国の国民であることを理由にしてその引渡が拒絶された場合には、その請求を受けた加盟国は、請求をした加盟国の求めにより、訴追のために、その事件を自国の機関に付託しなければならない。引渡請求を拒絶された加盟国が、国内捜査及び刑事訴追のために事件を付託するよう求めない場合には、請求を受けた加盟国は、起訴すべき義務を何ら負うことがない[3]。更に、引渡請求がなされない場合、または、国民であること以外の理由[4]によって引渡が拒絶された場合については、本項は、請求を受けた加盟国に対し、国内で訴追するために事件を付託する義務を負わせるものではない。加えて、第 6 項は、国内の捜査及び訴追が適正に行われるべきことを求めている。すなわち、その案件は、事件の付託をする加盟国において、「その性質が、他の侵害行為と比較しても」悪質なものであるとして扱われるべきである。当該加盟国は、請求をした加盟国に対し、その捜

---

[1] [訳注] 航空機のハイジャック行為が「政治犯罪」に該当するか否かが争われた事案について、該当性なしと判断した事例として、東京高裁平成 2 年 4 月 20 日決定・裁判所サイト（東京高裁平成 2 年（て）第 37 号事件）がある。

[2] [訳注] 説明書の第 237 項の脚注（訳注）参照

[3] [訳注] 逃亡犯罪人引渡法第 9 条第 1 項は、東京高等裁判所は、東京高等検察庁の検察官から審査の請求を受けたときは、速やかに審査を開始し、その決定をするものと定め、同法第 10 条第 1 項柱書は、第 9 条第 1 項の審査結果に基づき、「審査の請求が不適法であるときは、これを却下する決定」（第 1 号）、「逃亡犯罪人を引き渡すことができない場合に該当するときは、その旨の決定」（第 2 号）または「逃亡犯罪人を引き渡すことができる場合に該当するときは、その旨の決定」（第 3 号）をしなければならない旨を定めている。この決定は、「その主文を東京高等検察庁の検察官に通知することによって、その効力を生ずる」（同条第 2 項）。また、同法第 11 条は、審査請求命令の取消について定めている。そして、同法第 12 条は、「東京高等検察庁の検察官は、第 10 条第 1 項第 1 号若しくは第 2 号の決定があつたとき、又は前条の規定により審査請求命令が取り消されたときは、直ちに、拘禁許可状により拘禁されている逃亡犯罪人を釈放しなければならない」と定めている。その結果、引渡を拒否する結果となる判断がなされたときは、原則として、当該の者を釈放することになる。その後、日本国の法令に基づいて日本国の検察官が捜査を遂げ、起訴するか否かについては、日本国の法務大臣及び検察官の裁量に任されている。

[4] [訳注] 東京高裁平成 16 年 3 月 29 日決定・高裁判例集 57 巻 1 号 16 頁は、「逃亡犯罪人の引渡審査請求において、請求国の法令に基づく引渡犯罪の嫌疑が認められなければ、日本国とアメリカ合衆国との間の犯罪人引渡しに関する条約 3 条及び逃亡犯罪人引渡法 2 条 6 号が要求する犯罪の嫌疑は認められない」と判示している。

査及び手続の結果を報告しなければならない。
252. 誰に対して各加盟国が仮拘禁[1]または引渡を請求すべきであるかについて、第 7 条は、加盟国に対し、何ら条約が存在しない場合において、引渡請求をし、引渡請求を受けまたは仮拘禁をすることについて責任を有する機関の名称及び住所を欧州評議会の事務局長に対して通知すべきことを求めている。この条項は、関係加盟国間に拘束力のある引渡条約が存在しない場合に限定された。というのは、加盟国間で（ETS No. 24 のような）2 国間条約または多国間条約が発効している場合には、加盟国は、登録の要請をしなくても、誰に対して仮拘禁または引渡を請求すべきかを知ることができるからである。事務局長に対する通知は、各加盟国の調印時点またはその批准書、受諾書、承認書もしくは加入書の寄託の時点において、なされなければならない。権限ある者による調印は、外交チャネルを通じてすることもできるということを排除しないことに留意すべきである。

第 3 款　共助に関する一般原則

共助に関する一般原則（第 25 条）

253. 共助を提供すべき義務を規律する一般原則は、第 1 項の中に規定されている。共助は、「可能な限り広い範囲」で提供されなければならない。そして、第 23 条（国際的な共助に関する一般原則）の中にもあるように、共助は、原則として、可能な限り広く拡大されるべきものであり、かつ、それに対する障碍は断固として排除されるべきものである。第 2 に、第 23 条にもあるとおり、協力の義務は、原則として、コンピュータシステム及びコンピュータデータと関連する犯罪行為（例えば、第 14 条第 2 項の(a)及び(b)の適用のある侵害行為）、並びに、犯罪行為の電子的な形態による証拠の収集の両方について適用されなければならない。これら両方の範疇に関する国際協力という能率的な仕組みが同等に必要であることから、この広範な類型の犯罪について協力の義務を負わせることが合意された。しかしながら、第 34 条及び第 35 条は、加盟国に対し、これらの措置を異なる適用範囲で提供することを認めている。
254. 本章の他の条項は、共助を提供すべき義務が、一般に、適用可能な司法共助条約、法律及び合意の要件に従って履行されること明らかにする[2]。第 2 項に基づき、各加盟国は、司法共助条約、法律及び合意に中にそのような条項がまだ含まれていない場合には、本章の残りの条項の中に示されている特別の方式による協力を遂行するための法的根拠を持つことが求められる。そのような仕組み、とりわけ、第 29 条ないし第 35 条（特別の条項ー第 1 款、

[1] [訳注] 逃亡者犯罪人引渡法第 23 条ないし第 30 条参照
[2] [訳注] 日本国の関連する法令としては、国際捜査共助等に関する法律（昭和 55 年法律第 69 号）がある。同法の第 2 条は、「共助犯罪が政治犯罪であるとき、又は共助の要請が政治犯罪について捜査する目的で行われたものと認められるとき」、「条約に別段の定めがある場合を除き、共助犯罪に係る行為が日本国内において行われたとした場合において、その行為が日本国の法令によれば罪に当たるものでないとき」及び「証人尋問又は証拠物の提供に係る要請については、条約に別段の定めがある場合を除き、その証拠が捜査に欠くことのできないものであることを明らかにした要請国の書面がないとき」には、共助をすることができない旨を定めている。

第 2 款、第 3 款）の中にある仕組みを利用できることは、コンピュータと関連する刑事上の事項について効果的な協力を行うために必須のものである。

255. 幾つかの加盟国は、第 2 項に示す条項を適用するために、これを実装する立法行為を必要としないだろう。というのは、詳細な共助の仕組みを設けている国際条約の条項は、その性質上、直接に適用のあるものと考えられているからである。加盟国は、それらの条約の条項を直接に適用のあるものとして取扱うことができること、本章に基づいて設けられる共助の措置を行うための既存の共助立法によって既に十分な柔軟性を有していること、または、そのようにすべきことを求める立法を速やかに行うことが期待されている。

256. コンピュータデータは、消えてなくなってしまいやすいものである。ほんの僅かなキーストロークによって、または、自動的なプログラムの実行によって、削除されるかもしれず、犯罪の容疑者を追跡することが不可能にされ、あるいは、有罪とするための決定的な証拠が破壊されるかもしれない。コンピュータデータ中のある形態のものは、それが削除される前のほんの短時間だけ記録保存される。他方では、証拠が迅速に集められないと、個人や財産に対する重大な危険が生ずるかもしれない。そのような緊急の場合には、要請だけではなく、応答もまた応急措置によって実施されるべきである。それゆえ、第 3 項の目的は、データ入手のための共助要請を準備、伝送及び実施するために必要な時間の間に、そのデータが削除されてしまうことにより、決定的な情報や証拠が失われてしまわないようにする共助を得るプロセスの加速を促進することにある。第 3 項は、(1)によって、外交行嚢または郵便配達システムを介して行われる従来の封書の非常に遅い配送によってではなく、通信という応急手段を介して、加盟国が緊急の協力要請をすることを支援しており、また、(2)は、そのような状況下における要請に対して応答するために、要請を受けた加盟国が応急の手段を使用することを求めている。各加盟国は、その共助条約、法律または合意が既にそのような条項を定めていない場合には、この手段を適用することが求められる。ファックス及び電子メールを列挙しているのは、その性質上、例示である。すなわち、眼前の特別の状況下にあっては、他の応急の通信手段も適切なものとして使用することができる。技術の発展によって、共助の要請のために用いることのできる更に迅速な通信手段が開発されることであろう。本項の中に含まれている真正性及び安全性の要件に関して、各加盟国は、通信の真正性をどのように確保するか、または、特に機微性がある場合に必要となるかもしれない情報セキュリティ上の特別の防護措置（例：暗号化）が必要であるかどうかについて、それぞれ自ら決定することができる[1]。最後に、本項は、また、要請を受けた加盟国が選択する場合には、応急の伝送を確実なものとするために、従来の経路を通じて、正式の確認を求めることも認めている。

257. 第 4 項は、共助は適用され得る共助条約（MLAT）[2]及び国内法の要件に従うという原則

[1] [訳注] 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）の第 19 条は、特定個人番号の提供の制限について定め、同法第 20 条は、特定個人番号の利用の制限について定めている。また、同法 25 条は、「情報提供等事務又は情報提供ネットワークシステムの運営に関する事務に従事する者又は従事していた者は、その業務に関して知り得た当該事務に関する秘密を漏らし、又は盗用してはならない」と定めている。しかし、外国の捜査機関等から司法共助の手続については特に定められていない。

[2] [訳注] 参考となる文献として、Jennifer Daskal, The Un-Territoriality of Data, Yale Law Journal vol.125 no.2 pp.326-398 (2015)、Peter Swire & Justin D.Hemmings, Re-Engineering The Mutual Legal Assistance Treaty

を定めている。この枠組みは、要請を受けた加盟国の国内に所在し、共助の要請の対象となり得る個人の権利のための安全性確保措置を提供する。例えば、捜索及び押収のような権利侵害的な措置は、要請を受けた加盟国の国内の事件について適用可能な同様の措置のために必要な基本的要件が充足されていない限り、要請をする加盟国のために実施されることはない。また、加盟国は、司法共助を通じて捜索され提供される物品に関して、個人の権利の保護を確保することができる。

258. しかしながら、第 4 項は、「本章中に特段の規定がある」場合には、適用されない。この文言は、条約が原則に対する幾つかの重要な例外を含んでいるということを警告するためのものである。そのような例外の最初のものは、本条第 2 項の中に見られる。それは、MLAT、共助協定または共助法律が現時点でそのような措置を提供していると否とを問わず、加盟国に対し、本章中の残りの条項に定める（保全、データのリアルタイム収集、捜索及び押収、24/7 ネットワークの維持のような）方法による協力を提供すべき義務を課している[1]。他の例外は、第 27 条中に見つけることができる。それは、要請をした国と要請を受けた国との間に MLAT または共助協定が存在しない場合において、要請を受けた加盟国の国内法が規律する国際協力ではなく、要請の実施について、常に適用されるべきものである。第 27 条は、拒絶のための条件及び理由の制度を定める。本項中に特に定める他の例外は、要請を受けた加盟国は、少なくとも、条約の第 2 条ないし第 11 条に設ける侵害行為が関係する限りは、その要請には「財政」の侵害行為が含まれるとその要請を受けた加盟国が判断したことを根拠として、協力を拒否することができないということである。最後に、第 29 条は、例外であり、この点についての留保をすることができる場合であってもなお、双罰性を理由に保全を拒絶することはできない[2]。

259. 第 5 項は、基本的には、本章に基づく共助のための双罰性の定義である。要請を受けた加盟国は、援助を提供するための条件として双罰性を求めることが認められている場合（例えば、第 29 条第 4 項「記録保存されたコンピュータデータの応急の保全」に基づくデータの保全と関連して、要請を受けた加盟国が双罰性を求める加盟国の権利を留保する場合）には、求められている援助の原因となっている侵害行為が、その要請をした加盟国の法律によっても侵害行為となる行為となる限り、たとえ要請をした国の法律がその犯罪行為を異なる類型に位置付けているとしても、または、その犯罪に関する規定の仕方について異なる用語

Process, Draft for NYU Law and PLSC Conference (May 14, 2015)がある。

[1] [訳注] サイバー犯罪条約第 25 条第 2 項は、「締約国は、第 27 条から第 35 条までに定める義務を履行するため、必要な立法その他の措置をとる」と定めている（外務省訳）。「立法その他の措置」であるので、法律に定めていない措置を講ずることができるように読めないことはない。しかし、行政権の発動は根拠法律に基づいて行われなければならないので、政治判断に基づいて超法規的な措置をとらざるを得ないような非常に特殊かつ例外的な場合を除いては、原則として、いかなる措置も何らかの法律上の根拠に基づくものでなければならない。超法規的な措置が講じられたときは、国民に対して明確に説明がなされ、場合によっては、選挙によってその是非について国民の信任を得なければならない。他方で、立法以外の措置を講ずる場合の法的根拠として、サイバー犯罪条約の中にある関連条項を直接に適用することの可否・妥当性等については、従来、ほとんど論じられていない（説明書の第 255 項参照）。

[2] [訳注] 説明書の第 259 項、第 285 項及び第 286 項参照

を用いているとしても、双罰性は存在するとみなされなければならない。本条は、双罰性の原則が適用される場合に、要請を受けた加盟国が過剰に厳格な検証をしないでも済むことを確保するために必要であると考えられている。国家の法制度の相違を考えると、犯罪行為の用語法及び分類は、多様なものであり得る。その行為が両国の制度上でいずれも犯罪行為を構成するのであれば、そのような技術的な相違点は、援助を妨げてはならない。むしろ、双罰性の原則が適用され得る事項については、援助の付与を促進するような柔軟な方法で、それが適用されるべきである[1]。

自発的な情報提供（第 26 条）

260. 本条は、ロンダリング、捜索、押収及び犯罪の果実の没収に関する条約（ETS No.141）の第 10 条並びに涜職に関する刑事法条約（ETS No.173）のような、欧州評議会の初期の文書中にある条項に由来する。刑事事件の捜査または刑事手続において他の加盟国を支援することになるだろうと思われる価値ある情報をある加盟国が保有しておりながら、捜査または刑事手続を実施している加盟国はその存在に気づいていないというようなことが、より頻繁に生じている。このような場合には、共助要請が行われないであろう。そこで、第 1 項は、事前の要請がなくても、情報を保有している加盟国が、他の加盟国に対して、その情報を転送する権限を認めている。幾つかの国々の法律では、要請がなくても援助を提供するためにはそのような法的根拠を積極的に付与する必要があることから、本条が有用であると判断した。加盟国は、他の加盟国に対して自発的に情報を転送すべき義務を負わない。すなわち、眼前の事案の状況に照らして、その自由裁量権が行使されることになる[2]。更に、情報の自発的な開示を行った場合であっても、開示をする加盟国が、その管轄権を有する限り、開示される事案について捜査または刑事手続を実施することを妨げるものではない[3]。

261. 第 2 項は、ある状況下においては、加盟国は、慎重な取扱いを要する情報について、その使用に関し機密保持その他の条件を維持する義務を負わせることを条件として、自発的に情報を転送することになるという事実に対応している。当該情報が公開されることによって、情報提供をする国の重要な利益が損なわれる可能性がある場合には、機密性の保持が特に重要なものとなる。例えば、情報収集の手段を特定する要素[4]または当該犯罪グループが捜査中

[1] [訳注] 説明書の第 259 項で説明されている事項に関して、日本国内での研究成果は、非常に乏しい。今後、更に研究が深められるべきである。

[2] [訳注] 説明書の第 274 項参照

[3] [訳注] 説明書の第 260 項及び第 261 項で説明されている事項に関して、日本国内における学術上の研究成果は、実務報告的なものを除き、ほとんどない。今後、更に研究が深められるべきである。

[4] [訳注] 例えば、国防目的により諜報機関が特別な探知手段を用いている場合おいて、当該探知手段が国内の警察目的では認められていないときは、当該諜報機関がそのような探知手段を用いているという事実が明らかにされることそれ自体が国防上の利益を害することになる。しかし、このようなタイプの問題は、当該国における政治的な問題とも密接に関連するものであり、非常に難しい。このような場合においては、例えば、個人データ保護のための法令の適用に際しても、適用除外とするための法的根拠が異なることになる。結局のところ、確実に言えることは、戦時と平時が常に共存する状況の下においては、「平時の法に基づくだけでは適正な法解釈を提供することができないし、その逆も

であるという事実を保護すべき必要性があるときは、そうである。情報提供を受ける加盟国が情報提供をする加盟国の求めに応ずることができないことが明らかである場合（例えば、公開の法廷における証拠として当該証拠が必要であることを理由に、機密保持の条件に従うことができない場合）には、情報提供を受ける加盟国は、情報提供をする加盟国に対し、情報の提供をしないという選択肢もあるということを通知しなければならない。しかしながら、情報提供を受ける加盟国が条件に同意する場合には、それは、名誉あることとすべきである。本条に基づいて課される条件は、受領国からの共助要請に応じて提供をする加盟国によって課され得る条件と一致することになるものと予想される。

第 4 款　適用可能な国際合意がない場合における共助要請の手続

適用可能な国際合意がない場合における共助要請の手続（第 27 条）

262. 第 27 条は、加盟国に対し、要請をする加盟国と要請を受ける加盟国との間に統一的または互恵的な法律に基づく共助条約または共助協定が存在しない場合に、一定の共助手続及び条件を適用することを義務付けている。本条は、共助に関連する条約及びこれに類する協定の適用を通じて実施されなければならないという共助の基本原則を補強するものである。起草者は、共助のための他の適用可能な文書及び合意ではなく、それらとは別に、この条約の中で適用することのできる共助の一般的な枠組みを創設することは否決した。起草者は、その代わりに、基本的な事項については、現行の MLAT の枠組みに依拠することがより実際的であるということを合意した。それによって、共助の実務担当者は、最も手慣れた文書や協定を用いることが認められることになるし、また、競合する枠組みを新設することから生ずる混乱を避けることもできる。既に述べたとおり、第 29 条ないし第 35 条（特別規定－第 1 款、第 2 款、第 3 款）における共助のように、刑事と関連するコンピュータについての迅速で効果的な協力のための実務運営上必要な仕組みに関してのみ、各加盟国は、現行の共助条約、共助協定または共助法律が既にそうしているのではないときは、そのような形態での共助を実施できるようにするための法的根拠を設けるべきことを求められる。
263. 従って、この条約に基づくほぼ全ての共助方法は、当該文書の加盟国の間においては、刑事の共助に関する欧州条約（ETS No.30）及びその議定書（ETS No.99）に従うものとして、実施され続けることになるだろう。他方、この条約の加盟国であって、加盟国間で有効な多国間の MLAT を持つ国、または、（欧州連合の構成国間におけるように）刑事事件についての共助を規律する他の 2 国間合意を持つ国は、それらによるのではなく本条の規定の全部または一部を適用することに合意するのでない限り、第 3 章の残りの条項に規定するコンピュータ犯罪もしくはコンピュータと関連する犯罪に対応するための仕組みによって補足されたものとして、その要件を適用し続けなければならない。共助は、刑事の共助に関する欧州条約（第 26 条第 4 項）によっても承認されている北欧諸国間で確立された共助制度や英連邦諸国間で確立された共助制度のように、統一的または互恵的な立法に基づいて合意された協定に基づくものとすることもできる。最後に、統一的または互恵的な立法に基づく共助条

また真である」ということだけである。

約または共助協定という指示は、この条約が発効する時点で発効しているものに限られず、将来発効するかもしれない文書にも適用がある。

264. 第 27 条（適用される国際協定がない場合の共助の要請に関する手続）第 2 項ないし第 10 項は、統一的または互恵的な立法に基づく MLAT または共助協定が存在しない場合において、中央当局[1]を設置すること、条件を課すこと、延期または拒絶の場合の根拠及び手続、要請についての機密保持及び直接の連絡を含め、共助を提供するための数多くの規則を定めている。このような統一的または互恵的な立法に基づく共助合意または共助協定が存在しない場合において、明示的に適用される事項に関しては、共助について規律する他の適用可能な国内法ではなく本条の各条項が適用されるべきである。それと同時に、第 27 条は、国際的共助を規律する国内法の中で典型的に取扱われているその他の事項については、何らの規則も提供していない。例えば、要請の方式及び内容[2]、要請を受けた加盟国または要請をする加盟国内における証人の証言の取扱方法[3]、行政機関の記録または企業の記録の提供、拘束中の証人の移送[4]、没収に関する事項についての共助を取扱う条項は存在しない。このような事項について、第 25 条第 4 項は、この条約に特段の定めがないときは、要請を受けた加盟国の法律がそのようなタイプの援助を提供する特別の方式を規律すべきものとしている。

265. 第 2 項は、援助要請の送付もしくはその応答について責任を負う中央当局の設置を求めている。その中央当局の組織は、刑事の共助を扱う現代の文書に共通の特徴であり、それは、とりわけ、コンピュータ犯罪またはコンピュータと関連する犯罪との闘いにおいて有益なものとなる迅速な反応を確保するための助けとなる。まず、そのような機関相互間での直接の伝送は、外交チャネルを通じた伝送よりも、より迅速であり、より効果的である[5]。加えて、活動的な中央当局を設置することは、要請を送り受けることを誠実に遂行することを確保し、外国の法執行機関に対して、要請を受けた加盟国内での法律上の要件を充足するためにはどのようにするのが最善であるのかについて助言することを確保し、そして、特に緊急性のある要請または機微性のある要請が適正に取扱われることを確保するための重要な機能を提供する。

266. 加盟国は、能率に関する事項として、共助のための 1 個の中央当局を指定することが推奨されている。一般に、本条が適用可能である場合には、中央当局を提供するための加盟国の MLAT または国内法に基づき、共助のための中央当局を指定するのが最も効果的であろう。

---

[1] [訳注] 原文は、「central authority」となっている。外務省訳では、「中央当局」との訳語をあてており、公式には「中央当局」との訳語を用いるべきものとされているので、この訳語に従うことにした。日本国においては、閣議決定により、警察庁が「中央当局」に指定されている。

[2] [訳注] 国際捜査共助等に関する法律第 3 条参照

[3] [訳注] 国際捜査共助等に関する法律第 10 条参照

[4] [訳注] 国際捜査共助等に関する法律第 19 条参照

[5] [訳注] サイバーセキュリティ戦略本部「サイバーセキュリティ 2016」（2016 年 8 月 31 日）は、「警察庁及び法務省において、容易に国境を越えるサイバー犯罪に効果的に対処するため、原則として共助を義務的なものとする日・米、日・韓、日・中、日・香港、日・EU、日・露間の刑事共助条約・協定及びサイバー犯罪に関する条約の発効を受け、これらの条約・協定の下で、中央当局を設置し、外交ルートを経由せずに直接中央当局間で共助実施のための連絡を行うことで共助の迅速化を図る。今後は、更なる刑事共助条約の締結について検討していく」としている。

しかしながら、加盟国は、自国の共助制度上において適切なときは、2 以上の中央当局を指定する柔軟性も有している。2 以上の中央当局が設置される場合には、そのようにする加盟国は、それら各機関が条約を同じように解釈し、かつ、それらの各機関が要請を受け、それを送ることを迅速かつ効果的に取扱うことを確保しなければならない。各加盟国は、欧州評議会の事務局長に対し、本条に基づく共助の要請を受け、それに応答するために指定される中央当局の名称及び住所を（電子メール及びファックス番号を含め）通知しなければならない。また、加盟国は、その指定が最新なものに保たれることを確保する義務を負う。

267. 要請をする国の主要な障碍は、しばしば、要請をする国の国内法が定める証拠能力の要件を充足することを確保すること、そして、その国の裁判所が結論を下す前に証拠を用いることができることを確保することである[1]。このような証拠法上の要件への適合性を確保するために、第 3 項は、要請を受ける加盟国に対し、そのようにすることが自国の法律と適合しないものではない限り、要請をする加盟国が指定した手続に従って要請を実行すべき義務を負わせている[2]。本項は、手続法上の技術的な要件に関する義務のみに関連するものであって、基本的な手続法上の保護に関するものではないということを強調しておく。そして、例えば、要請をする加盟国は、要請を受ける加盟国に対し、要請を受ける加盟国の当該措置に関する基本的な法律上の要件に適合しないような捜索及び押収の実施を求めることはできない。義務の制限的な性質に鑑み、要請を受ける加盟国の法制度がそのような刑事手続を知らないということは、要請をした加盟国から要請された手続の適用を拒絶するための十分な根拠とはならないこと、その代わりに、刑事手続は、要請を受ける加盟国の法律上の諸原則に適合するものでなければならないことが合意された。例えば、要請をする加盟国の法律の下では、証人の証言は宣誓の下に行われなければならないということが手続法上の要件とされることがあり得る。要請を受ける国が、その国内法上、証言が宣誓の下に行われなければならないという要件を有していないとしても、要請をする加盟国の要請を名誉あることとすべきで

[1] [訳注] 要請をする国の法制度上では証拠として許容されないデータ（証拠能力のないデータ）は、犯罪捜査の目的で用いられることはあっても、刑事訴訟法に基づく公判において特定の犯罪を立証するための証拠として用いることができない。ただし、犯罪事実（訴因に該当する事実）の立証のために用いることのできないデータであっても、量刑の事情として斟酌される事実を証明するための証拠として用いられることはある。

[2] [訳注] 共助の要請をする国において原則として証拠能力が認められないデータであっても、要請を受ける国において証拠能力が認められるものであれば、共助の要請を拒むことができないという趣旨である。これは、例えば、原則として証拠能力が認めらないデータであっても、特段の事情（特信状況）等の付加的な要件に該当する事実についての証明があれば例外的に証拠能力が付与されることがあるような場合には、とりわけ重要であると考えられる。そのような場合、要請を受けた国において、要請をした国の法制度や法解釈を詳細に吟味することは難しいことから、実務上の重要性がある。また、いかなる国においても証拠能力が認められないデータは、要請を受ける国においても証拠能力が認められないことは自明である。ただし、このような実務上の必要性だけを重視した場合、被疑者の基本的な権利の保障（特に刑事手続上の権利の保障）との関係で問題が生ずることがないとは言えない。そのような事態に対処すべく、各国の弁護士は、そのような事件における被告人の弁護人となることがあり得ることを想定し、日々研鑽につとめるべきであろう（現実には、各国とも、電子証拠及びそれと関連する法制度・法解釈等について真に精通している弁護士が十分に存在しているとは認め難い。検察官及び裁判官についても同じである。）。

ある。

268. 第 4 項は、本条に基づいて送られた共助の要請に対して拒絶をするできることを定める。援助は、第 25 条第 4 項に規定する事由（例えば、要請を受けた加盟国の法律の中に規定する事由）に基づいて、拒絶することができる。それには、国家の主権、安全、公の秩序その他の基本的な利益に対する妨げが含まれ、また、その侵害行為が政治犯罪または政治犯罪に関係するものであると要請を受けた加盟国が判断する場合が含まれる[1]。可能な限り広範に共助の手段を提供するという優先的な原則を促進するために（第 23 条、第 25 条参照）、要請を受けた加盟国が設ける拒絶事由は、狭く抑制的に行使されるべきである。証拠または情報の範疇が広範であることと関連して、援助を類型的に拒絶し、または、煩雑な条件に服するものとするという潜在的な可能性を作り出す余地は、それほど広いものではい。

269. このような手法に沿って、第 28 条に定める根拠とは別に、特別の場合においてのみ、データ保護[2]を根拠にして援助を拒否することができると判断された[3]。そのような状況は、特別な事案において、重要な諸利益（一方では、法務の円滑な遂行を含め、公的な利益と、他方では、プライバシーの利益）の均衡の上で、要請をする加盟国によって求められる特定のデータを提供することが、要請を受けた加盟国によって拒絶の根拠となる基本的な利益の範囲内にあると判断すべき程度までに基本的な困難を生じさせるようなものであるときに、発生し得る。しかし、共助を拒絶するためにデータ保護の原則を広範で類型的で制度的に適用することは、排除されるべきである。そして、関係する加盟国が異なる個人データ保護制度をもっているという事実（要請をする加盟国が同等に専門化されたデータ保護監督機関を有していないような場合）、または、異なる個人データ保護手段を有しているという事実（要請をする加盟国がプライバシーの保護または法執行機関が取得した個人データの正確性の保護のために削除という処理以外の方法を用いているような場合）は、拒絶の根拠を構成しない。共助を拒絶する根拠として「基本的な利益」を主張する前に、要請された加盟国は、そのデータの移転[4]を許容するような条件を満たすような別の努力を試みるべきである。（第 27 条第 6 項及びこの説明書の第 271 項参照）

---

[1] [訳注] 説明書の第 254 項の脚注（訳注）参照

[2] [訳注] 文脈から、ここでの「データ保護（data protection）」とは、個人データの法的保護のことを指すものと解される。従来、日本国においては、サイバー犯罪の捜査と個人データの保護との関係については、ほとんど論じられることがなかった。

[3] [訳注] 同じ欧州評議会内の組織であっても、個人データの保護を担当する組織とサイバー犯罪の捜査を担当する組織との間には、個人データ保護の重要度の評価に関する温度差のようなものが存在することを示している。このことは、データ保持指令 2006/24/EC をめぐる幾つかの憲法訴訟と無効の先決裁定の遠因ともなっていると考えられる。基本的に、国防やテロ対策のための諜報活動や警察活動と私人のプライバシー保護との間には、矛盾や衝突を発生させるような本質的な問題が常に存在している。欧州評議会の関連する閣僚委員会勧告としては、Recommendation No. R (87) 15 regulating the use of personal data in the police sector があるが、サイバー犯罪条約の説明書の中では、明示による解説がなく、非常に興味深い。なお、警察関係における個人データ保護については、前掲「欧州連合の構成国における独立の個人データ保護監督官の職務」において若干の考察結果を示した。

[4] [訳注] ここでいう「データの移転（transfer of the data）」とは、個人データの第三国移転（国境を越えた個人データの移転）のことを指す。

270. 第 5 項は、要請に直ちに応ずると要請を受けた加盟国の犯罪捜査上または刑事手続を妨げる場合、要請を受けた加盟国が、拒絶するのではなく、延期することを認めている。例えば、要請をした加盟国が、犯罪捜査または公判のための証拠または証言の入手を求めている場合において、同じ証拠または証言が、要請を受けた加盟国において開始される公判において用いるためにも必要である場合には、要請を受けた加盟国は、援助の提供を延期することが正当化される。

271. 第 6 項は、求められた援助が拒絶または延期されない場合において、要請を受けた加盟国が、それらの代わりに、援助に条件を付することができることを定めている。その条件が要請をした加盟国にとって受け入れられるものではないときは、要請を受けた加盟国は、その条件を修正することができ、または、援助の拒絶または延期の権利を行使することができる。要請を受けた加盟国は、援助措置を可能な限り広範に提供すべき義務を負っているので、拒絶及び条件の根拠事由は抑制的に行使されるべきであると合意された[1]。

272. 第 7 項は、要請を受けた加盟国に対し、要請をした国に対してその結果を報告すべき義務を負わせ、また、援助の拒絶または延期の場合には、その理由を通知することを求めている。理由を提供することは、とりわけ、要請を受けた国が本条の要件についてどのように解釈したのかについて、要請をした国が理解する助けとなり、将来の時点における共助の有効性を促進するための協議の基盤を提供するものであり、そして、証言または証拠の利用可能性ないし利用の条件についての未知の事実情報を、要請をした加盟国に対して事前に提供することになる。

273. 特に機微性のある事案、または、要請の基礎となっている事実が一般に公開されると大失敗に至るような事案について、加盟国が要請をすることがある。そこで、第 8 項は、要請をする加盟国が、要請があったという事実及びその内容について機密を保つように求めることを認めている。しかしながら、要請を受けた加盟国が求められている証拠または情報を入手することができないことが想定される範囲内では、機密性を求めることができない。例えば、援助を効果的なものとするために必要な裁判所の命令を得るために、情報が開示されなければならない場合、または、要請を無事に実施するためには、証拠を保有している私人に対して要請があったことを告知しなければならない場合がそうである。要請を受けた加盟国が機密性保持の要請に従うことができないときは、要請をした国に対し、その要請の撤回または修正という選択肢があることを通知しなければならない。

274. 第 2 項により設置される中央当局は、相互に、直接に連絡を取らなければならない[2]。しかしながら、緊急の事態においては、要請をする加盟国の裁判官及び検察官から、要請を受ける加盟国の裁判官及び検察官に対して、直接に、共助要請が送られるかもしれない。この手続を担当する裁判官及び検察官は、要請を受ける側の中央当局へ伝送するという見地から、自国の中央当局に対して、要請書の写しを送付しなければならない[3]。(b)に基づき、国

[1] [訳注] 説明書の第 269 項参照

[2] [訳注] 説明書の第 265 項の脚注（訳注）参照

[3] [訳注] このような場合において、個人データ保護のための独立の監督官（independent supervisory authority）がどのように関与することになるかについては、不明である。なお、説明書の第 269 項参照。

際刑事警察機構（Interpol）を経由して要請をすることができる[1]。要請を受ける加盟国の機関は、その担当権限外のものとして要請を受ける場合には、(c)に従い、二重の義務を負う。第 1 に、その機関は、要請を受けた加盟国の職務権限を有する機関に対し、その要請を回付しなければならない。第 2 に、その機関は、要請をした側の機関に対して、その回付をしたことを通知しなければならない。(d)に基づき、緊急性がない場合においても、要請を受けた加盟国の機関が強制手段を用いなくても要請に応ずることができる限り、中央当局の関与なく直接に、その要請を回付することができる。最後に、(e)は、加盟国が、他の加盟国に対し、それが効果的であることを理由として、直接に中央当局に対して連絡を送付すべきことを欧州評議会の事務局長を介して通知することができるものとしている。

機密性及び利用の制限（第 28 条）

275. 本条は、当該情報または物が特に機微性を有する場合[2]において、要請を受けた加盟国が、援助を承認するために必要なものとしてその使用を制限することを確保し、または、要請をした加盟国の法執行機関の外部それが流出しないようにすることを確保することができるようにするため、情報または物の使用に関する制限を特に定めている。これらの制限は、

[1] [訳注] 国際捜査共助等に関する法律の第 18 条第 1 項は、「国家公安委員会は、国際刑事警察機構から外国の刑事事件の捜査について協力の要請を受けたときは」、「相当と認める都道府県警察に必要な調査を指示すること」または「第 5 条第 1 項第 3 号の国の機関の長に協力の要請に関する書面を送付すること」のいずれかの措置を採る旨を定めている。そして、同条第 3 項は、「国家公安委員会は、第 1 項に規定する措置を採るため必要があると認めるときは、警察庁の職員に関係人の所在その他必要な事項について調査させることができる」と定め、同条第 4 項は、「国家公安委員会は、第 1 項の措置に関し、要請において調査を行う機関が明らかな場合を除き、所管に応じて、同項第 2 号の国の機関の長と協議するものとする」と定め、同条第 5 項は、「国家公安委員会は、第 1 項の措置を採ることとするときは、法務大臣の意見を聴くものとする」と定め、同条第 6 項は、「第 1 項第 1 号の指示を受けた都道府県警察の警察本部長は、その都道府県警察の警察官に調査のための必要な措置を採ることを命ずるものとする」と定め、同条第 7 項は、「第 1 項第 2 号の規定により協力の要請に関する書面の送付を受けた国の機関の長は、司法警察職員であるその機関の職員に当該要請に係る調査のための必要な措置を採ることを命ずることができる」と定め、同条第 8 項は、「警察官又は前項の国の機関の職員は、前 2 項の調査に関し、関係人に質問し、実況見分をし、書類その他の物の所有者、所持者若しくは保管者にその物の提示を求め、又は公務所若しくは公私の団体に照会して必要な事項の報告を求めることができる」と定めている。

[2] [訳注] 原文は、「in which such information or material is particularly sensitive」となっている。この「particularly sensitive」は、一般に、プライバシーの利益のような機密性の高いものであることを指す場合に用いられる。しかし、文脈から考えてみると、ここで「particularly sensitive」と言っているのは、プライバシーの利益のような場合だけではなく、例えば、著作物のように所定の許諾を受けている者以外は複製物を利用することができない場合、営業秘密や特許出願前の発明に関する情報のように公開すること知的財産として成立しなくなってしまう場合、あるいは、児童ポルノのように公衆に提供することが認められない場合等を含む趣旨と解される。説明的な訳語を用いるとすれば、「特に機密性を確保する必要性が高い場合」と訳すこともできる。

とりわけ、データ保護[1]のために用いることのできる安全性確保措置を提供する。

276. 第 27 条の場合と同じように、第 28 条は、要請をする加盟国と要請を受ける加盟国との間において統一的または互恵的な立法に基づく共助条約または共助協定が存在しない場合にのみ適用される。そのような条約または協定が発効している場合には、加盟国間で別段の合意をしない限り、本条の規定ではなく、それらの機密保持及び使用制限に関する条項が適用されなければならない。このことは、2 国間または多国間の共助条約（MLAT）及びこれに類する協定との重複を避けるためであり、それによって、実務担当者は、競合し相互に矛盾するかもしれない 2 つの文書の適用を検討するのではなく、普通の良く理解できる枠組みに基づいて、その運用を継続することができるようになる。

277. 第 2 項は、要請を受けた加盟国が、共助の要請に応ずる場合において、2 つのタイプの条件を付すことを認めている。第 1 に、機密情報であることを示すもの含まれている場合のように、そのような条件なしには要請に応えることができない場合には、提供される情報または物を機密に保つことを要求することができる。要請を受けた加盟国が要請された援助を提供すべき義務を負う場合には、完全な機密性保持を求めることは適切ではない。というのは、そのようにすることは、多くの場合、例えば、（強制的な開示を含め）公開の法廷において証拠として使用する場合[2]のように、要請をする加盟国が、犯罪を成功裏に捜査し起訴することができる能力を遮断することになるからである。

278. 第 2 に、要請を受けた加盟国は、要請中に記述された犯罪捜査または刑事手続以外には使用しないという条件を付して、情報または物の提供をすることができる。この条件を適用するためには、それが要請を受けた加盟国によって明示に示されていなければならない。そうでない場合には、要請をした加盟国による使用についての制限は何も存在しないことになる。条件が示されている場合には、この条件は、情報及び物が要請の中で予定されていた目的のためにのみ使用することができるということを確保することになる。また、それによって、要請を受けた加盟国の同意なしに他の目的で物を使用すれば、ルール違反となる。使用の制限を用いる際の 2 つの例外が交渉担当者によって認識され、それは、本項の要件の中で暗に示されている。第 1 に、多くの国々における法律上の基本原則に基づき、提供される物が起訴された者を弁護する証拠である場合には、それは、弁護人または司法機関に対して開示されなければならない[3]。加えて、共助の枠組みの中で提供された物は、（強制的な開示を含め）通常は公開の手続による裁判の場での使用が意図されている。一度そのような開示が

---

[1] [訳注] 原文は、「data protection」となっている。一般的には、個人データの保護（personal data protection）のことを指す。しかし、文脈から、個人データの場合のみならず、個人データ以外の類型に属するデータについての情報セキュリティ上の防護措置を含む趣旨で「data protection」と表現されていると解される。

[2] [訳注] 営業秘密に関しては、不正競争防止法第 23 条ないし第 31 条が刑事訴訟における特別の証拠調べ方法を定めている。犯罪被害者の保護に関しては、刑事訴訟法第 290 条の 2 が被害者特定事項を公開しないようにするための措置を講ずることができる旨を定めている。また、同法第 53 条第 2 項は、刑事訴訟における事件記録の閲覧に関して一定の制限をすることができることを定めている。

[3] [訳注] 日本国における取扱いは、必ずしも明確なものではない。このことは、共助により得られた証拠に限られるものではないが、サイバー犯罪条約との関係では、条約の履行との関係で非常に重要なことである。今後、十分な検討が尽くされるべきである。

なされると、物は、基本的に、公開のものとなってしまう。このような状況にあるときは、援助が求められた捜査または刑事手続の機密性を確保することは不可能である[1]。

279. 第 3 項は、情報を転送された加盟国が所定の条件に従うことができない場合には、それを提供する加盟国に対して、情報を提供しない選択肢があるということを通知しなければならないと定めている。しかしながら、要請を受ける加盟国が条件に同意する場合には、それは、名誉あることとすべきである。

280. 第 4 項は、要請を受ける加盟国が当該条件の遵守の有無を確認することができるようにするために、要請をする加盟国が第 2 項に示す条件に基づいて受領した情報または物の使用に関して説明を求めることができるということを定めている。要請を受ける加盟国は、例えば、提供された物または情報がアクセスされた時刻といったような瑣末な事項については、問い合わせできないということが合意された。

第 2 節　特別規定

281. この節の目的は、コンピュータと関連する犯罪及び電子的な形式による証拠と関係する事案において、効果的に連携した国際的な活動を遂行するために、特別の仕組みを定めることである。

第 1 款　応急の措置に関する共助

記録保存されたコンピュータデータの応急の保全（第 29 条）

282. 本条は、国内法のレベルで用いるために第 16 条で定めているのと同じレベルの仕組みを国際的なレベルで提供する。本条の第 1 項は、加盟国が要請をする権限を付与する。そして、第 3 項は、各加盟国に対し、データ入手のための共助要請を準備、伝送及び実施するために必要な時間の間に、そのデータが改変、消去または削除されないようにするため、要請を受けた加盟国の領土内でコンピュータシステムによって記録保存されたデータの応急の保全を適法に得ることができるようにすることを求めている[2]。保全は、在来型の共助を実施

[1] [訳注] 公判準備の手続において開示された証拠の機密を守るべき義務については、刑事訴訟法第 281 条の 3 ないし第 281 条の 5 に規定がある。日本国における証拠開示（ディスカバリ）の制度には様々な問題があることが指摘されてきたところであるが、更に検討・改善すべき余地がある。

[2] [訳注] 国際捜査共助等に関する法律の第 8 条第 2 項は、「検察官又は司法警察員は、共助に必要な証拠の収集に関し、必要があると認めるときは、裁判官の発する令状により、差押え、記録命令付差押え、捜索又は検証をすることができる」と定め、同条第 3 項は、「検察官又は司法警察員は、前 2 項の規定により収集すべき証拠が業務書類等（業務を遂行する過程において作成され、又は保管される書類その他の物をいう。以下この項において同じ。）である場合において、当該業務書類等の作成又は保管の状況に関する事項の証明に係る共助の要請があるときは、作成者、保管者その他の当該業務書類等の作成又は保管の状況に係る業務上の知識を有すると認める者に対し、当該要請に係る事項についての証明書の提出を求めることができる」と定め、同条第 1 項第 6 号は、検察官又は司法警察員が、共助に必要な証拠の収集に関して、「電気通信を行うための設備を他人の通信の用に供する事業を営む

する場合よりもずっと迅速なものとすることを意図した限定的で暫定的な措置である。既に述べたとおり[1]、コンピュータデータは、消えてなくなってしまいやすいものである。それは、ほんの僅かなキーストロークによって、または、自動的なプログラムの実行によって、削除され、改変されまたは移動されるかもしれないものであり、犯罪の容疑者を追跡することが不可能にされ、あるいは、有罪とするための決定的な証拠が破壊されてしまうかもしれない。コンピュータデータ中のある形態のものは、それが削除される前のほんの短時間だけ記録保存される。そこで、数週間ないし数ヶ月を要するかもしれない正式の共助要請の実施過程を含む期間よりも長い期間を待っている間に、そのようなデータの利用可能性を確保するための仕組みが必要であると合意された。

283. この措置は、通常の共助の実務よりも迅速なものである一方、それと同時に、より侵害的ではないものである。要請を受けた加盟国の共助担当機関は、データの管理者からデータを確保することを要求されない[2]。加盟国に対して求められる手続は、後の段階になって法執行機関のために実施されるべき手続が開始されるまでの間に、管理者（しばしば、サービス提供者その他の第三者）がそのデータを（削除ではなく）保全することを確保することである[3]。この手続は、迅速であり、当該データと関係する者のプライバシーを保護するものであるという利点を持っている。というのは、そのデータは、通常の共助の枠組みに従った完全な開示のための基準が満たされるまでは、いかなる政府機関によっても開示または調査されることがないからである。それと同時に、要請を受けた加盟国は、データの提出命令または捜索令状の応急の発令及び実施を含め、データの迅速な保全を確保するための他の手続を利用することも認められている[4]。鍵となる要件は、再現不可能な喪失からデータを守るための最高度に迅速な手続を持つことである。

284. 第 2 項は、本条に従って行われる保全要請の内容を定める。この措置が暫定的な措置であること、要請は迅速に準備され伝送されることを要すること、提供される情報は要約であるかもしれず、データの保全を可能とするための必要最小限の情報のみを含むものであるかもしれないということには留意しなければならない。この要請をするためには、保全を求めている機関の指定及び措置を求められる捜査機関の指定に加え、事実の要約、保全されるべきデータ及びその所在を特定するのに十分な情報を提供し、並びに、そのデータが関連する

者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、30 日を超えない期間（延長する場合には、通じて 60 日を超えない期間）を定めて、これを消去しないよう、書面で求める」処分をすることができると定めている。

[1] [訳注] 説明書の第 256 項参照

[2] [訳注] 日本国の刑事訴訟法上の手続に即して考えてみると、日本国の法務大臣（検察庁及び警察庁）は、共助要請のあったデータについて捜索や記録命令付き差押えを実施すべき義務を負わないという趣旨と解される。

[3] [訳注] 通常の国内法的な対応としては、ISP 等に対して任意捜査としての協力要請が行われることになることが多いであろうと考えられる。

[4] [訳注] 正規の手続としては、刑事訴訟法第 197 条第 3 項に基づいて、記録保存されたデータの応急保全と同様の強制捜査が実施される。

犯罪の捜査及び刑事訴追に関係するものであり、かつ、そのデータの保全が必要であることを示す情報を提供しなければならない。最後に、要請をする加盟国は、この措置の後に、データの提出を得ることができるようにするため、共助要請を発出しなければならない。

285. 第 3 項は、保全を提供する条件として双罰性を要しないという原則を定める。一般に、双罰性の原則を適用することは、保全という文脈においては、その意図とは反対の結果を招くことになる。第 1 に、現代の共助実務においては、捜索及び押収または傍受といった最も侵害的な刑事手続上の措置においてさえ、双罰性の要求が無視される傾向がある。起草者が想定する保全は、しかしながら、特別に侵害的なものではない。というのは、管理者は、その保有するデータを適法に保有し続けることができるだけであり、そのデータは、データの開示を求める正式な共助が実施されるまでは、要請を受けた加盟国の捜査機関によって開示または調査されることがないからである。第 2 に、実際上の問題として、双罰性の存在を正確に確認するのに必要な証明するためには、その間に、データが削除、消去または改変されるかもしれないだけの長い時間を要することが多い。例えば、捜査の初動段階では、要請をする加盟国は、自国の領土内に所在するコンピュータへの侵入があったことについて注意を払うかもしれないが、後の段階になるまでは、損害の性質及び範囲について正しい認識を持たないかもしれない[1]。要請を受けた加盟国が、双罰性を確実に確立されるのを待っている間に、侵入行為の発信地を追跡するトラフィックデータの保全が遅延すると、伝送がなされた後のわずか数時間ないし数日間だけ保持されている重要なデータをサービス提供者が日常業務として削除してしまうというようなことがしばしば発生してしまうことになる。その後に要請をした加盟国が双罰性の要件を満たすことができたとしても、重要なトラフィックデータが復元できなくなっており、そして、その犯罪の加害者を特定することができなくなってしまうかもしれない。

286. 従って、一般原則としては、加盟国は、保全の目的では双罰性の要件を免除しなければならない。しかしながら、第 4 項に基づいて、それを制限する留保を利用することはできる。加盟国は、データ提出の共助の要請に応ずるための条件として双罰性を要求する場合であって、かつ、開示の時点では双罰性の要件が充足されていないと信ずるべき根拠を有する場合には、加盟国が保全の条件として双罰性を要求する権利を留保することができる。第 2 条ないし第 11 条に従って設けられる侵害行為に関しては、加盟国の間では、双罰性の条件が自動的に充足されるものと推定される。ただし、条約が許容する場合には、加盟国がこれらの侵害行為について行う留保に従う。それゆえ、加盟国は、条約によって定義されている侵害行為以外の侵害行為に関してのみ、この要件を課すことができる[2]。

---

[1] [訳注] 当該犯罪の構成要件が一定の結果の発生を要するものとしている場合、当該「結果の発生」という構成要件に該当する事実の存在が判明するまでは、当該の行為がどの犯罪構成要件に該当するかを判定することができない道理である。つまり、捜査の段階・状況の変化に応じてかなり流動的なものであり得る犯罪捜査においては、最初から確定的なものとして構成要件該当性の判断を求めることが難しく、仮にそれを可能な限り厳格に求めるとなると、捜査機関としては、現実には何もできなくなってしまう危険性がある。このことは、サイバー犯罪条約に基づくデータの保全に限ったことではなく、刑事事件における令状事務一般においても共通して認められることである。

[2] [訳注] サイバー犯罪条約の加盟国は、条約に基づいて留保が認められる部分を除き、条約の第 3 条ないし第 11 条に規定する行為をいずれも犯罪として処罰することが義務とされている結果、これらの

287. これ以外の場合には、第 5 項に基づき、要請を受けた加盟国は、その要請を実施することによって、自国の主権、安全、公共の秩序その他の基本的な利益を損なう場合、または、その侵害行為が、政治犯罪または政治犯罪に関係するものであると判断する場合に限り、保全の要請を拒絶することができる[1]。コンピュータ犯罪またはコンピュータと関連する犯罪について効果的に捜査及び刑事手続をするためのこの措置の重要性に鑑み、保全の要請を拒絶するための他のいかなる理由を主張することも許されないものとすることが合意された。
288. 要請を受けた加盟国は、時として、データの管理者が、要請をした加盟国の捜査についての機密保持を破る行動その他の違法な行動に走ろうとするような事態に遭遇するかもしれない（例えば、保全されるべきデータが犯罪者グループの支配下にあるサービス提供者によって保有され、または、捜査対象となっている者自身によって保有されている場合）。このような場合には、第 6 項に基づき、保全の要請を実施することによって直面することになるリスクを負担すべきかどうか、または、提出命令または捜索及び押収のようなより侵害的ではあるが安全な共助方法を求めるかどうかについて、要請をした加盟国が評価することができるようにするため、要請をした加盟国に対して、速やかに通知がなければならない[2]。
289. 最後に、第 7 項は、加盟国に対し、本条に従って保全されたデータがそのデータの開示を求める正式の共助要請の受領を保留した状態で、少なくとも 60 日間保存されること、及び、その後の要請の受領を待って、引き続き保存されることを確保しなければならない。

保全されたトラフィックデータの応急の開示（第 30 条）

290. 本条は、第 17 条において国内使用のために設けられる権限と同じ国際的な権限を定める。その発信地へと伝送を遡り、犯罪の容疑者を識別し、決定的な証拠を探し出すために、犯罪が実行された加盟国の要請に際して、要請を受けた加盟国は、しばしば、自国のコンピュータを介してなされた通信に関するトラフィックデータを保全することになるであろう。そのようにする際、要請を受けた加盟国は、自国の領土内で見つけられたトラフィックデータによって、その伝送が、第三国に所在するサービス提供者または要請をした加盟国自身の中に所在するサービス提供者を経由したものだということが判明するかもしれない。このような場合、要請を受けた加盟国は、要請をした加盟国に対し、応急のものとして、他の国に所在するサービス提供者の識別及び他の国からの通信経路の識別を可能とするのに十分な

行為については常に双罰性の要件が充足されていることになる。ただし、サイバー犯罪条約の第 3 条ないし第 11 条の行為の国内法における犯罪構成要件の細部については一定の留保が認められることがあることから、厳密には、留保が可能となっている部分に関しては、相手国において双罰性の要件を満たしているかどうかを確認すべき必要性は残る。

[1] [訳注] 説明書の第 254 項の脚注（訳注）参照

[2] [訳注] サイバー犯罪条約の第 29 条第 6 項は、「要請を受けた締約国は、保全によっては当該要請に係るデータの将来における利用可能性が確保されず、又は当該要請を行った締約国の捜査の秘密性が脅かされ若しくはその他の態様で捜査が害されるであろうと信ずる場合には、当該要請を行った締約国に対し速やかにその旨を通報する。この場合において、当該要請を行った締約国は、それにもかかわらず当該要請が実施されるべきか否かについて決定する」と定めている（外務省訳）。

量のトラフィックデータを提供しなければならない[1]。伝送が第三国から来たものである場合には、その情報は、要請をした国が、その最初の発信地へと伝送を遡るために、当該他の国に対し保全及び応急の共助を要請することができるようにすることであろう。伝送がぐるりと回って要請をした加盟国に戻ってきてしまった場合には、国内法上の手続を通じて、更にトラフィックデータの保全及び開示を得ることができる[2]。

291. 第 2 項に基づき、要請を受けた加盟国は、開示をすることが自国の主権、安全、公の秩序（*ordre public*）その他の基本的な利益を損なうおそれがある場合、あるいは、当該要請を受けた加盟国が、政治犯罪または政治犯罪に関係する犯罪であると判断する場合にのみ、トラフィックデータの開示を拒絶することができる[3]。第 29 条（記録保存されたコンピュータデータの応急の保全）の中にあるように、このタイプの情報は、この条約の範囲内にある犯罪を実行した者を識別し、決定的な証拠を探し出すために非常に重要なものであることから、その拒絶事由は、厳しく限定されている。そして、援助を拒絶するために他の事由を主張することは認められないということが合意されている。

第 2 款　捜査権に関する共助

記録保存されたコンピュータデータのアクセスに関する共助（第 31 条）

292. 各加盟国は、第 19 条（記録保存されたコンピュータデータの捜索及び押収）に基づいて加盟国が国内の目的のためにそのようにしなければならないのと同様に、他の加盟国の利益のために、自国の領土内に所在するコンピュータシステムによって記録保存されたデータを、捜索もしくはこれに類するアクセスをし、押収もしくはこれに類する確保をし、または、開示するための能力を持たなければならない[4]。第 1 項は、加盟国に対し、このタイプの共助を要請する権限を与え、そして、第 2 項は、要請を受ける加盟国に対し、それを提供できるようにすることを求める[5]。また、第 2 項は、刑事における司法共助を規律する適用可能な条約、協定及び国内法の中で定められている要件及び条件をもって、そのような協力を提供するための要件及び条件とすべきであるという原則に従っている。第 3 項に基づき、そのような要請に対しては、(1) 関連するデータがとりわけ滅失または改変され易いと信ずるべき根拠を有する場合、または、(2)そのような条約、協定及び法律がそのように別段の定めをしている場合には、応急ベースで応答しなければならない。

---

[1] [訳注] 他の加盟国に対する要請ではなく、他の加盟国に所属するサービス提供者に対して直接に要する場合について参考となる文献として、Cybercrime Convention Committee, T-CY(2016)13 - Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers: Compilation of replies (July 2016)がある。クラウドに関しては、Cybercrime Convention Committee, T-CY(2016)2 Criminal justice access to data in the cloud: cooperation with "foreign" service providers (May 2016)がある。

[2] [訳注] 説明書の第 282 項の脚注（訳注）参照

[3] [訳注] 説明書の第 254 項の脚注（訳注）参照

[4] [訳注] 説明書の第 137 項参照

[5] [訳注] 説明書の第 282 項の脚注（訳注）参照

同意による場合、または、公衆が利用可能な場合における、記録保存されたコンピュータデータに対する国境を越えたアクセス（第 32 条）

293. 他の加盟国内に所在する記録保存されたコンピュータデータに対し、加盟国が共助要請なしに片面的にアクセスをすることが認められるのはどのような場合かという問題は、条約の起草者がかなりの議論を交わした問題であった[1]。国家が片面的に行動することが承認されている場合、及び、そうではない場合について、詳細な検討が行われた。最終的に、起草者は、この領域を規律するための納得のいく法的拘束力のある枠組みを準備することはまだできないという結論に至った[2]。部分的には、現在のところ、そのような場合に関する確実な経験に欠けているという理由に基づくものであった。また、部分的には、個別事案の仔細な状況を考慮しなければ適切な解決が得られないので、一般的な規則を構築することが困難であるという理由に基づくものであった[3]。結局、起草者は、条約の第 32 条において、片面的アクセスが認められる場合について、全ての起草者の同意を得ることのできるような状況を決定するのにとどめた。起草者は、更に経験が集積され、そして、それに焦点を当てた議論が更になされるような時代になるまで、その他の場合については定めことに同意した。これに関して、第 39 条第 3 項は、その他の場合について、その権限を授与するものではなく、また、排除するわけでもないと定めている。

294. 第 32 条（同意により場合または公衆が利用可能な場合の記録保存されたコンピュータデータへの国境を越えたアクセス）は、2 種類の状況について定めている。すなわち、第 1 に、アクセスされるデータが公衆に利用可能な場合であり、第 2 に、加盟国の領土内にあるコンピュータシステムを介して、その領土外に所在するデータにアクセスし、または、これを受信する場合であって、かつ、加盟国に対し当該システムを介してそのデータを開示する法的な権限を有する者の適法かつ任意の同意を得ている場合である。誰がデータの開示をすることを「法的に認められているのか」については、状況、その者の性質及び適用可能な関連法律によって、多様なものであり得る。例えば、個人の電子メールは、サービス提供者によって他の国で記録保存されているかもしれないし、また、意図的に、他の国でデータを記録保存する者が存在するかもしれない[4]。これらの者は、データを検索することができる。ま

---

[1] [訳注] 参考となる文献として、Sergio Carrera, Gloria González Fuster, Elspeth Guild & Valsamis Mitsilegas, Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights, Center for European Policy Studies (2016)がある。

[2] [訳注] 米国の諜報機関が欧州内のデータに対して一方的にアクセスする行為が EU と米国との間のセーフハーバー協定の実効性を喪失させているとの疑問から協議がなされ、その結果、新たにプライバシーシールド協定が締結されるに至ったことは周知のとおりである。

[3] [訳注] 理論的には、国家の正当防衛や緊急避難を考えることは一応可能である。しかし、その場合の緊急性（切迫性）、必要性（補充性）、相当性（比例性）の判断は、結局のところ、具体的な事案において個別に判断するしかないのであり、具体的な判断基準を構築することがほとんど不可能であるということを示している。

[4] [訳注] 例えば、クラウドサービスにみられるように、仮想的なサーバではなく物理サーバが現実にはどの国に所在しているのかについて、利用者が知ることができないことが珍しくない。また、例えば、Winny のような分散型のファイル共有システムの場合には、1 個の物理サーバに特定のデータが記

た、それらの者が法的に認められていることを条件として[1]、条文に規定しているとおり、法執行機関に対し、任意にデータを開示することができ、あるいは、法執行機関がそのデータにアクセスすることを承認することができる。

トラフィックデータのリアルタイム収集に関する共助（第 33 条）

295. 多くの場合において、捜査官は、過去の伝送記録の上にある痕跡をなぞることによってその通信の発信源まで追跡することを確保することができない。というのは、鍵となるトラフィックデータは、それが保全される前に、伝送の連鎖の中で、サービス提供者によって自動的に削除されてしまっているかもしれないからである。従って、各加盟国の捜査官が、他の加盟国にあるコンピュータシステムを介して行われる通信に関し、リアルタイムでトラフィックデータを入手することのできる能力を持つことが非常に重要である。そこで、第 33 条（トラフィックデータのリアルタイム収集に関する共助）に基づき、各加盟国は、他の加盟国のために、リアルタイムで、トラフィックデータを収集すべき義務を負う[2]。本条は、ここでは、加盟国に対してこれらの事項に関する協力を求める一方、他のところでは、既存の共助方法について別のことを定めている。そして、そのような協力が提供される場合の要件及び条件は、一般に、刑事における司法共助について規律する適用可能な条約、協定及び法律の中で定められている[3]。

296. 多くの国々では、トラフィックデータのリアルタイム収集に関する共助が広く提供され

録保存されているのではなく、多数のサーバに断片化されて記録保存されていることから、外国というよりも複数の国にデータの断片が分散して所在していることがあるということができる。Bitcoin のような電子マネーシステムでも同様のことが言える場合がある。結局、仮想的に特定されるサーバと実際に物理的に存在しているサーバとの関係が希薄化されつつあるという事実を踏まえ、そのような場合における令状事務の方策及び証拠の特定方法について、今後研究が深められるべきであろう。

[1] [訳注] この例の場合、法的に認められている者とは、当該データが記録保存されている外国のサーバの管理者のことを指すと解される。個人データ保護指令 95/46/EC との関係で言うと、個人データを処理する管理者（controller）が法的に認められている者に該当する。これとは別に、個人データのデータ主体（本人）の同意があれば、法執行機関（警察）が当該データにアクセスすることができることは当然のことである。

[2] [訳注] 国際捜査共助等に関する法律の第 8 条第 1 項第 6 号は、トラフィックデータのリアルタイム収集に関する条項ではなく、応急の保全に関する条項である（説明書の第 282 項の脚注（訳注）参照）。他方、国際捜査共助等に関する法律の中には通信傍受法に基づく傍受の共助が定められていない。結局、同法第 8 条第 1 項第 6 号の応急保全と同条第 2 項の記録命令付差押えや検証等の手続の組み合わせによってトラフィックデータのリアルタイム収集の共助を代替する以外の方法はないと解される。ただし、そのような手続の適法性については、批判があり得る（前掲経済産業省サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」41～43 頁参照）。なお、任意捜査として実施された傍受等の結果を共助の要請国に対して提供することの可否及びその法的根拠等については、必ずしも明確ではない。また、国内において立件する事件の捜査として通信傍受法に基づく通信傍受が実施された場合、その傍受記録を共助の要請国に対して提供するための手続も明確ではない。

[3] [訳注] 第 33 条の共助は、「国内法に定める条件及び手続に従って行う」必要があることから、第 33 条を直接に適用して共助のための根拠とすることができない。

ている。というのは、そのような収集は、コンテントデータの傍受、捜索及び押収よりも侵害的ではないと見られているからである。しかしながら、多くの国々では、より狭い手法を採っている。従って、第 3 項は、第 14 条（手続条項の適用範囲）に基づいて加盟国が国内法上の措置と同じ適用範囲で保全を実施することができることを、第 2 項は、加盟国が第 23 条（国際協力に関する一般原則）に規定する侵害行為よりも狭い範囲で、この措置を適用する範囲を限定することを認めている。1 つの制限が定められている。すなわち、侵害行為の範囲は、国内の同種事案においてこの措置を利用することができる侵害行為の範囲よりも狭いものとすることができない。もちろん、トラフィックデータのリアルタイム収集は、時として、犯罪の容疑者の同一性を確認する唯一の方法であるし、また、この措置はより侵害的でないものでもあるので、第 2 項中の「少なくとも」という要件は、例えば、双罰性が存在しない場合でさえ、加盟国が可能な限り広く援助を許容することを期待している。

コンテントデータの傍受に関する共助（第 34 条）

297. 傍受の侵害性が非常に高度なものであるので[1]、コンテントデータの傍受のための共助の提供義務は、制限されている。援助は、加盟国に適用可能な条約及び法律によって許容されている範囲内で、提供されなければならない。コンテントの傍受を求める共助の提供は共助実務の新たな領域に属するので、その共助義務の範囲及び制限に関しては、既存の共助の枠組み及び国内法に任せることが決定された[2]。これらに関しては、第 14 条、第 15 条及び第 21 条の注釈、並びに、通信傍受のための書面照会との関係で刑事関連事項の共助に関する欧州条約の運用実務に関する勧告 No. R (85) 10 を参照すべきである。

第 3 款　24/7 ネットワーク

24/7 ネットワーク（第 36 条）

298. 既に述べたとおり、コンピュータシステムを用いて実行される犯罪と効果的に闘い、電子的な形態による証拠を効果的に収集するためには、非常に迅速な対応を要する。更に、ほんのわずかなキーストロークだけで、何千キロもの距離と幾つものタイム・ゾーンの彼方へと簡単に結果が得られるような世界の中の一部で行動すべきであろう。この理由から、既存の警察上の協力及び共助の様式は、コンピュータ時代からの挑戦に効果的に対応するための補充的なチャネルを必要としている。本条で設けられるチャネルは、G8 諸国グループの賛助により創設され既に機能しているネットワークから得られた経験を基盤としている[3]。本条

[1] [訳注] 説明書の第 328 項の脚注（訳注）参照

[2] [訳注] 説明書の第 282 項の脚注（訳注）参照

[3] [訳注] The G8 24/7 Network of Contact Points: Protocol Statement によれば、2007 年 12 月現在における「G8 24/7 Network」の参加国は、オーストリア、ベルギー、ブラジル、ブルガリア、カナダ、チリ、クロアチア、チェコ、デンマーク、ドミニカ、エストニア、フィンランド、フランス、ドイツ、香港、ハンガリー、インド、インドネシア、イスラエル、イタリア、ジャマイカ、日本、韓国、リトアニア、ル

に基づき、加盟国は、本章とりわけ第 35 条第 1 項の(a)ないし(c)に規定する適用範囲内で、捜査及び刑事手続における即時の援助を確保するために、週 7 日間、24 時間ベースで利用可能な連絡先を指定すべき義務を負う。このネットワークの設立はこの条約によって提供される手段の中でも最も重要なものであること、そして、コンピュータ犯罪またはコンピュータと関連する犯罪によって直面している法執行上の挑戦に対して加盟国が効果的に対応し得る手段であることが合意された。

299. 各加盟国の 24/7 連絡部局[1]は、とりわけ、技術的な助言の提供、データの保全、証拠の収集、法情報の提供及び容疑者の所在特定を促進し、かつ、直接に実施しなければならない。第 1 項中の「法情報」という用語は、公式または非公式な協力の提供のために必要となる法的前提条件について協力を求める他の加盟国に対し、助言をすることを意味する[2]。

300. 各加盟国は、自国の法執行の構造の範囲内で、連絡部局をどこにするのかを決定する自由を有する。幾つかの加盟国は、共助のための中央当局内に 24/7 連絡部局を設置することを望むかもしれないし、また、他の加盟国は、コンピュータ犯罪またはコンピュータと関連する犯罪と闘うための警察の特別部門内にそれを置くのが最善だと考えるかもしれない。しかし、特定の加盟国では、その政治体制及び法制度のために、別の選択をするのが適切であるかもしれない。24/7 の連絡は、攻撃の阻止または追跡のための技術的な助言を提供するためのものであると同時に、容疑者の所在地の特定のような国際的な協力上の義務でもある。そのことから、1 個の正解だけが存在するわけではないし、また、ネットワーク構造は、時代を越えて発展するだろうと予測される。国内の連絡部局を設計するに際には、他の言語を用いる連絡部局との意思疎通の必要性について、しかるべく配慮されなければならない。

301. 第 2 項は、24/7 の連絡によって遂行される重要な職務の中でも、24/7 連絡部局それ自体で直接に実行しない機能を迅速に実行できるようにする能力を持つことがその最も重要なものであると規定している。例えば、加盟国の 24/7 の連絡が警察機構の一部である場合には、昼夜の時間帯を問わず適切な行動をとることができるようにするため、国際的引渡または共助のための中央当局のようなその国の政府内の関連機構と応急的に協働する能力を持たなければならない。更に、第 2 項は、各加盟国の 24/7 の連絡が、応急ベースで、ネットワークの他の構成員と通信を行う能力を持つことを求めている。

302. 第 3 項は、ネットワーク内の各連絡部局が、適切な装置を有することを求めている。ネットワークを円滑に運営するためには、最新の電話、ファックス及びコンピュータ装置が必要である。また、技術の発展に即応して、他の形態の通信や分析装置をシステムの一部とすることを要する。第 3 項は、また、ネットワークのために加盟国チームの一部を構成する要

クセンブルグ、マレーシア、マルタ、モーリシャス、メキシコ、モロッコ、ナミビア、オランダ、ニュージーランド、ナイジェリア、ノルウェー、パキスタン、ペルー、フィリピン、ルーマニア、ロシア、シンガポール、南アフリカ、スペイン、スウェーデン、台湾、タイ、チュニジア、イギリス及びアメリカ合衆国である。

[1] [訳注] 外務省訳では「連絡部局」となっているので、の訳語に従うことにした。

[2] [訳注] 参考となる文献として、Council of Europe Economic Crime Division, The functioning of 24/7 points of contact for cybercrime (2 April 2009)がある。日本国の関連通達としては、警察庁丙総発第 64 号・丙人発第 232 号・丙生企発第 110 号・丙刑企発第 64 号・丙交企発第 120 号・丙備企発第 93 号・丙情企発第 62 号「サイバーセキュリティ重点施策の策定について（通達）」（平成 27 年 9 月 25 日）がある。

員が、コンピュータ犯罪またはコンピュータと関連する犯罪に関して、そして、それに対していかに効果的に対応するかについて、適切に訓練されていることを求めている。

第 4 章　最終条項

303. 幾つかの例外を除き、本章に含まれる条項は、その大部分において、1980 年 2 月に開催された第 315 回代表者会合の際に閣僚委員会によって承認された「欧州評議会の中で締結される条約及び協定のためのモデル最終条項」に基づいている。第 36 条ないし第 48 条のほとんど全部は、モデル条項の標準用語を使用するか、または、欧州評議会における長年の条約起草作業の実務に基づいており、それらについては特に注釈を要しない。しかしながら、標準モデル条項を修正した部分または幾つかの新しい条項については、若干の説明を要する。この文脈においては、条項を拘束しないセットとしてモデル条項を用いたことに留意すべきである。印刷されたモデル条項の序文が示しているように、「これらのモデル最終条項は、専門委員会の職務遂行を促進し、かつ、現実の正当化事由も持たない条文の分岐を避けることのみを意図している。モデルは、いかなる方法によっても条約を拘束するものではなく、かつ、特別の場合に適合させるために別の条項を採用することができる」。

署名及び発効（第 36 条）

304. 第 36 条第 1 項は、欧州評議会の枠組み内で起草された他の条約の中で確立された幾つかの先例に依って起草された。例えば、有罪判決を受けた者の移送に関する条約（ETS No.112）及びロンダリング、捜索、押収及び犯罪の果実の没収に関する条約（ETS No.141）がそうであり、これらは、欧州評議会の構成国のみならず、その起草作業に参加した非構成諸国によっても、その発効以前に調印することが認められている[1]。条項は、単に欧州評議会の構成国に限らず、利害関係のある国の最大多数が可能な限り早期に加盟国となることができることを意図している。このことから、条項は、条約の起草作業に積極的に参加した 4 つの非構成諸国、すなわち、カナダ、日本、南アフリカ及びアメリカ合衆国に適用されることを意図している。ひとたび条約が発効すると、第 3 項に従い、この条項の適用のない他の非構成諸国は、第 37 条第 1 項の要件を満たして条約に加入するよう勧奨されることになるだろう。
305. 第 36 条第 3 項は、条約が発効するために必要な批准、受諾または承認の数を 5 と定めている。この数は、欧州評議会の条約における通常の必要最低数（3）より多いもので、国際的なコンピュータ犯罪またはコンピュータと関連する犯罪からの挑戦に対して、これから取り組み始め、それを成功させる必要のある国のグループが、やや多く存在することを要するという確信を反映するものである。しかしながら、この数は、条約加入の発効を不必要に遅延させるほど多いものではない。最初の 5 か国の中で、少なくとも 3 か国は欧州評議会の

[1] [訳注] サイバー犯罪条約は、平成 13 年 11 月 8 日、ストラスブールで採択され、平成 13 年 11 月 23 日、ブタペストで署名のため開放され、日本国はその際に署名した。条約は、平成 16 年 4 月 21 日、国会承認となり、平成 24 年 7 月 3 日に受諾書寄託、平成 24 年 7 月 4 日に公布及び告示（平成 24 年条約第 7 号及び外務省告示第 231 号）、平成 24 年 11 月 1 日、日本国について効力発生となっている。

構成国でなければならないが、他の 2 か国は、条約の起草作業に参加した 4 つの非構成諸国とすることができる。また、当然のことながら、本条は、欧州評議会の構成国である 5 か国によって締結される同意の表明に基づいて条約を発効させることを認めている。

条約の加入（第 37 条）

306. 第 37 条は、欧州評議会条約において確立された他の先例に基づいて起草されたものであるが、付加的で明示の要件をも伴っている。長年の実務慣行に基づき、閣僚委員会は、率先して、または、要請に基づき、構成国であるか否かにかかわらず、条約の起草作業に関与しなかった非構成諸国に対し、全ての条約加盟国と協議をした後に、条約に加入するよう招請するかどうかを決定する。このことは、協議をする締約国が非構成諸国の加盟に反対する場合には、通例、閣僚委員会は、その国の条約への加入を招請しないということを意味している。しかしながら、公式見解によれば、非構成諸国である加盟国がその加入に反対した場合であっても、（理論上は） 閣僚委員会は、その非構成国に対し、条約への加入を招請することができるはずである。このことは、（理論上は）欧州評議会の条約を他の非構成諸国に拡大する過程において、通例、非構成諸国である加盟国には議決権が与えられていないということを意味する。しかしながら、非構成諸国に対して条約への加入を招請する前に、閣僚会合は、（欧州評議会の構成国のみではなく）全ての締約国と協議し、その全員一致の同意を得るという明示の要件が挿入された。上記に示すとおり、このような要件は、実務と一致するものであり、そして、条約の全ての締約国が、非構成国が条約関係に入るべきであると判断することができるものとしなければならないという認識とも一致するものである。それでもなお、非構成国の加入を招請することについての公式の決定は、通常の実務運営に従い、閣僚委員会への出席権を有する締約国の代表者によって行われることとなるであろう。この決定は、欧州評議会規程の第 20 条 d に定める 3 分の 2 の多数及び閣僚委員会への出席権を有する締約国の代表者の全員一致によるものでなければならない。
307. 第 41 条に基づく宣言をする予定で条約の加入を求める連邦国は、第 41 条第 3 項に示す文言の草稿を事前に送付することが求められる。それによって、当該加盟国は、将来の加盟国による条約の実装に対して、連邦条項の適用がどのような影響を与えるかについての評価をすることのできる位置に立つこととなるであろう（第 320 項参照）。

条約の効力（第 39 条）

308. 第 39 条の第 1 項及び第 2 項は、条約と他の国際協定または合意との関係について定めている。欧州評議会の条約が欧州評議会の外で結ばれた 2 国間の条約または多国間の条約との間においてどのような関係に立つことになるかという課題は、上記に示したモデル条項[1]では扱われてない。刑事法の分野での欧州評議会の条約（例えば、不法海運に関する協定（ETS No.156））で用いられている通常の手法によれば、次のように定められるべきである。すなわち、(1)新たな条約は、特別の事項に関する既存の国際的な多国間条約に由来する権利及び

[1] [訳注] 説明書の第 303 項参照

取扱いに影響を与えない、(2)新たな条約の加盟国は、その条約に具現されている原則の補足もしくは強化またはその原則の適用促進のために、条約によって扱われる事情に関し、相互に 2 国間条約または多国間条約を締結することができる、そして、(3) 新たな条約への 2 か国以上の加盟国が、条約中で扱われている事項に関して既に協定を締結している場合、または、当該の事項に関して既に当事国間で別の関係を設定している場合には、それが国際的な協力関係を促進する限り、当該加盟国は、新たな条約ではなく、当該協定または条約を適用し、または、それに従って当該加盟国間の関係を規律する権限を有するとされている。

309. 一般に、条約は、加盟国間における多国間もしくは 2 国間の合意及び協定を補足しようとするものであって、これらに取って代わろうとするものではないので、起草者は、「特別の事項」への参照を制限し得ることが特に有益なものであるとは考えなかったし、また、それが無用な混乱を招くかもしれないことを怖れた。反対に、第 39 条第 1 項は、単純に、この条約が、加盟国間で適用可能な他の条約または合意を補足するものであることを示し、そして、排除されないものの例として、欧州評議会の 3 つ条約、すなわち、引渡に関する 1957 年の欧州条約（ETS No.24）、刑事に関する 1959 年の欧州条約（ETS No.30）及びその 1978 年の追加議定書（ETS No.99）に特に言及している[1]。それゆえ、一般的な事項に関しては、サイバー犯罪条約の加盟国は、原則として、そのような協定または合意を適用しなければならない。「特別法は一般法を破る（*lex specialis derogat lege generali*）」という解釈原理によれば、加盟国は、この条約だけが取扱っている特別の事項に関しては、この条約を優先して適用すべきであることになる。第 30 条がその例の 1 つであり、特定の通信の経路を識別するために必要な場合には、保全されたトラフィックデータを速やかに開示しなければならないと定められている。この特別の領域においては、条約は、特別法（*lex specialis*）として、より一般的な共助条約の中にある条項よりも優先する優越的な法規範を定めていることになる。

310. 同様に、起草者は、既存のまたは将来の合意を適用することが協力関係を「強化」または「促進」するかどうかについて疑問を生じさせるような語について検討した。何故なら、加盟国は、国際協力の章の中に設けられた手法に基づき、関連する国際的な合意及び協定を適用するだろうと予測されるからである。

311. 協力の根拠として既存の共助条約または共助協定がある場合、この条約は、それが必要な場合には、既存の規範を補充するだけである。例えば、元の条約または協定の中にはそのようにすることができる条項が存在しない場合、この条約は、応急の通信手段 （第 25 条第 3 項参照）による共助要請の伝送を提供することになる。

312. 条約の補充的な性質、そして、とりわけ、条約の国際協力の手法と一致するものとして、第 2 項は、加盟国が既に発効している合意または将来発効するかもしれない合意を適用する自由を有すると定めている。このような表現方法の先例は、有罪の宣告を受けた者の引渡に関する条約（ETS No.112）の中に見られる。確かに、国際協力という文脈の中では、他の国際的な合意（それらの多くは、国際支援のために証明された積年の方式を提供している。）

[1] [訳注] サイバー犯罪条約の第 39 条第 1 項は、「この条約は、締約国間で適用される多数国間又は 2 国間の条約及び取極を補足することを目的とする。これらの条約及び取極には、次のものを含む」と定め（外務省訳）、説明書の第 309 条で述べられている 3 つの条約を列挙している。

を適用することが、事実上、協力を促進するだろうということが期待されている。また、加盟国は、この条約の条件を遵守して、他の合意ではなく、この条約の中の国際協力の条項を適用することに同意することもできる（第 27 条第 1 項参照）。そのような場合、第 27 条に規定している協力と関連する条項は、当該他の合意の中にある関連する法規範に優先する。ミニマムの義務についてこの条約が一般的に定めているとおり、第 39 条第 2 項は、条約の中で扱う事項に関して加盟国の関係を設定する場合には、加盟国は、条約の中で既に定められている義務に付加して、より特別な義務を考慮する自由がある。しかしながら、これは、絶対的な権利ではない。すなわち、加盟国は、そのようにする場合には、条約上の義務及び諸原則を尊重しなければならず、それゆえ、条約の目的を損なうような義務を承諾することができない[1]。

313. 更に、他の国際的な合意と条約との関係を決定する際、起草者は、加盟国が、条約法に関するウィーン条約[2]の中の関連する各条項への追加ガイダンスを参照することができるということにも同意した。

314. 条約は、国際調和のために十分に必要なレベルを提供するものであり、コンピュータ犯罪またはコンピュータと関連する犯罪に関係する全ての未解決の問題に取り組もうとするものではない。それゆえ、第 3 項[3]は、条約がその適用についてのみ影響力を有するようにするために挿入された。存在するとしても条約によって取扱われていない他の権利、規制、義務及び責任は、影響を受けない。このような「救済条項」の先例は、他の国際的な合意（例えば、国連のテロリスト資金条約[4]）の中に見いだすことができる。

宣言（第 40 条）

315. 第 40 条は、主として条約の実体法の節の中で設けられる侵害行為と関連する一定の条項に関するものである。それは、加盟国は、条項の適用範囲を修正する一定の特別の付加的要件を含めることを認めている。そのような付加的な要件は、一定の概念上の相違点または法律上の相違点へ適応することを目的とするものであり、それは、おそらく、純粋に欧州評議会という文脈の中で正当化されるよりも、グローバルであることを目指す条約の中において、より正当化されるものである。宣言は、条約の中にある条項の承認可能な解釈として理解されるもので、留保とは区別されなければならない。留保は、加盟国が条約の中に定められている義務に服さないこと、または、それを修正することを認めるものである。条約の加盟国にとっては、もし宣言が存在するのであれば、他の国によって付加的な要件が付されたことを知ることが重要になるので、調印の時点またはその批准書、受諾書、承認書もしくは

[1] [訳注] 第 39 条第 2 項では、「この条約に規定する事項に関しこの条約が規律する態様以外の態様でそのような関係を確立する場合には、この条約の目的及び原則に反しないように行う」と定められている（外務省訳）。

[2] [訳注] Vienna Convention on the law of treaties (with annex). Concluded at Vienna on 23 May 1969

[3] [訳注] 第 39 条第 3 項は、「この条約のいかなる規定も、締約国が有する他の権利、制限、義務及び責任に影響を及ぼすものではない」と規定している（外務省訳）。

[4] [訳注] International Convention for the Suppression of the Financing of Terrorism (Adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999)

加入書の寄託の時点において、欧州評議会の事務局長に対してそれを宣言する義務がある。この通知は、加盟国が一定の手続上の権限を行使する場合には、双罰性の要件が加盟国によって適合するものであることを要することから、侵害行為の定義との関連で特に重要である。宣言に関しては、数の制限の必要性は感じられなかった[1]。

連邦条項（第 41 条）

316. 可能な限り多数の国々が加盟国となるようにするという目標に沿って、第 41 条は、中央の行政機関と地域的な行政機関の間のそれぞれ特徴を有する権限分配の結果として直面するかもしれない連邦国家[2]の困難に対応するために、留保を認めている。先例は、刑事法以外の領域において、他の国際的な合意[3]への連邦制の宣言または連邦制の留保として存在している。ここに、第 41 条は、連邦国家である加盟国の十分に整備された国内法及び実務の結果として、適用範囲についての重要ではない相違が生じ得ることを認めている。そのような相違は、その連邦国家の憲法を根拠とし、または、その連邦国家の中央政府及び構成国もしくは地域組織の間の刑事司法に関する事柄の権限分配に関するその他の基本原則を根拠とするものでなければならない。条約の起草者の間では、条約の適用に関して重要ではない相違だけを生じさせるように連邦条項を運用するという合意があった。

317. 例えば、合衆国においては[4]、その憲法及び連邦制という基本原則に基づき、連邦の刑事立法は、一般に、行為が州際取引または外国貿易に対して及ぼす影響を根拠として当該行為に対する規制を行う。他方において、些細な事項または純粋に地域的な利害のある事項に関しては、伝統的に、連邦を構成する州によって規律されている。連邦制度のこのような手法は、合衆国の連邦刑法に基づいて、この条約に包含される違法行為に対する幅広い適用を提供するものであるが、些細な影響を有する行為または純粋に地域的な性質を有する行為については連邦を構成する州が規律しようとすることを認めるものである。場合によっては、連邦法ではなく州法が適用される狭い行為の範疇の範囲内にあるのでなければ、連邦を構成する州は、この条約の範囲外にある措置を定めることができない[5]。例えば、スタンドアロン

---

[1] [訳注] サイバー犯罪条約における宣言（declarations）及び留保（reservations）の一覧は、下記の Web サイト上で公表されている。

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations [2016 年 12 月 6 日確認]

[2] [訳注] 非欧州諸国では、カナダ、メキシコ、オーストラリア、インド及びマレーシア等が連邦制を採用している。欧州諸国では、ドイツ、ベルギー、オーストリア及びスイスが連邦制を採用している。

[3] 例えば、Convention Relating to the Status of Refugees of 28 July 1951, Art. 34; Convention Relating to the Status of Stateless Persons of 28 September 1954, Art. 37; Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 10 June 1958, Art. 11; Convention for the Protection of World Cultural and Natural Heritage of 16 November 1972, Art. 34.

[4] [訳注] サイバー犯罪条約が欧州各国とアメリカ合衆国との密接な連携の中で形成されたものだという歴史的事実を証明する条項だと評価することも可能であろう。この連邦条項が存在しなくても、制定法及び判例法の解釈上、同じ結論を導くことが当然できると解される。にもかかわらず第 41 条が存在しているのは、サイバー犯罪条約の実効性を確保するためには、アメリカ合衆国の条約への参加が不可欠と考えられたからである。

[5] [訳注] サイバー犯罪条約の適用範囲外の事項については各国の立法機関が独自の法令を制定するこ

のパーソナルコンピュータまたは1個の建物内で相互に接続されたコンピュータネットワークに対する攻撃は、その攻撃が行われた州の法律によって定められている場合にのみ犯罪となる。しかしながら、インターネットの使用は、連邦法に含まれるべき州際取引または外国貿易に影響を及ぼすのであるから、コンピュータへのアクセスがインターネットを介して発生した場合には、その攻撃は、連邦法上の犯罪となるであろう。合衆国の連邦法を通じてこの条約を実装すること、または、同様の状況にある他の連邦国の法を通じて実装することは、第 41 条の要件を満たすものとなるであろう。

318. 連邦条項の適用範囲は、第 2 章（刑事実体法、手続法及び管轄権）に限定される。本条を利用する連邦国は、その連邦国を構成する州またはそれに類する地域組織であって、逃亡した容疑者や証拠が存在している場所において、当該行為が犯罪とされていない場合、または、この条約に基づいて求められる手続がない場合であっても、第 3 章に基づき他の加盟国と協力する義務を依然として負っている。

319. 加えて、第 41 条第 2 項は、本条の第 1 項に基づいて留保をする場合、連邦国家は、第 2 章に定める措置を定めるべき義務を排除し、または、それを実質的に消滅させることをその留保の条件とすることができないと定めている。全体として、これらの措置に関する法執行機関の広範で効果的な権限が定められなければならない。その連邦国を構成する州またはそれに類する地域組織の立法上の管轄権の範囲内にある事柄の実装に関しては、連邦政府は、その州や組織の機関に対して有益な支援を提供し、それを有効なものとする適切な行動をするように勧奨しなければならない。

留保（第 42 条）

320. 第 42 条は、多数の留保可能な場合について定めている。この手法は、条約が、多くの国々にとって刑法及び刑事手続法の比較的新規な領域に適用されるという事実から生じている。加えて、欧州評議会の構成国及び非構成諸国に対して署名のために開放されるというこの条約のグローバルな性質は、必然的に、そのような留保の可能性を持つことになる。これらの留保の可能性は、それらの国々がその国の国内法と一致する一定の手法及び概念を維持することを可能にしつつ、条約の加盟国となる国の数を最大限にすることを目的としている。同時に、起草者は、加盟国による条約の統一的な運用を可能な最大限まで確保するために、留保をする可能性を制限するように努めた。従って、ここに列挙されている以外の留保は認められない。加えて、留保は、加盟国により、調印の時点またはその批准書、受諾書、承認書もしくは加入書を寄託する時点で行われる場合のみ、可能である。

321. 加盟国の憲法または基本的な法的諸原則との衝突を回避するために、幾つかの加盟国にとって一定の留保をすることが重要であったことを認識して、第 43 条は、留保の撤回に関する時間制限を課していない。その代わりに、留保は、状況が許す限り、速やかに撤回されなければならない。

とができるはずであるが、合衆国の州法の場合には、サイバー犯罪条約の適用範囲外の事項に関するものであり、かつ、州法として制定可能な事項（些細な事項や純粋に地域的な利益のある事項）に関するものでなければならないという 2 重の縛りがあることを説明している。

322. 加盟国に対する何らかの影響力を維持し、少なくとも、加盟国に対してその留保の撤回を考慮させるために、条約は、欧州評議会の事務局長に対して、撤回の見込みについて定期的に照会する権限を与えた。この照会ができるということは、欧州評議会の複数の文書に基づく現行の実務である。そして、加盟国は、特定の条項に関する留保を維持する必要があるか、または、もはや必要がないものとしてそれを撤回するかどうかを示す機会を与えられている。条約の統一的な実装を可能な限り促進するために、時の経過と共に、加盟国がその留保の中の多くのものを削除することが期待される。

改正（第 44 条）

323. 第 44 条は、ロンダリング、捜索、押収及び犯罪の果実の没収に関する条約（ETS No.141）を先例に採った。同条約は、欧州評議会の基本的な枠組みの中で練られた刑事法条約に関連する改革として導入されたものである。改正の手続は、主として、比較的小さな手続上及び技術的な性質の変化のためのものとして想定されている[1]。起草者は、条約の大規模な変更は、追加議定書の形式でなされるべきものと考えた。
324. 加盟国は、自ら、第 46 条に規定する協議手続に基づく改正または追加議定書の必要性の有無について検討することができる。欧州犯罪問題委員会（CDPC）は、この点に関して、定期的に情報提供を受ける状態を維持し、また、条約の改正または補足をする加盟国の努力について、加盟国を支援するために必要な措置を講ずるであろう。
325. 第 5 項に従い、全ての加盟国がその受諾を事務局長に通知した場合に限り、採択された改正が発効する。この要件は、統一的なあり方で条約が発展することを確保しようとするものである。

紛議の解決（第 45 条）

326. 第 45 条第 1 項は、欧州犯罪問題委員会（CDPC）が、条約の中にある条項の解釈及び適用に関する情報提供を受ける状態を維持しなければならないと定めている。第 2 項は、加盟国に対し、条約の解釈または適用に関する全ての紛議を平和的に解決しようとすることを義務付けている。紛議を解決するための手続は、関係する加盟国の交渉によって合意されなければならない。紛議を解決するための可能な 3 つの仕組みは、本条によって示されている。すなわち、欧州犯罪問題委員会（CDPC）それ自体、仲裁裁判所または国際司法裁判所である。

加盟国間の協議（第 46 条）

327. 第 46 条は、条約の実装、コンピュータ犯罪またはコンピュータと関連する犯罪の対象及び電子的な形式による証拠の収集と関係する重要な法律上の影響、政策上の影響または技

[1] [訳注] 関連する文献として、Zahid Jamil & Jamil & Jamil, Cybercrime Model Laws: Discussion paper prepared for the Cybercrime Convention Committee (T-CY)（Version 23 December 2014, Provisional）がある。

術開発の影響、並びに、条約の補充または改正の可能性について、加盟国が協議するための基本的な枠組みを設けている。

328. その手続は柔軟であり、そして、加盟国が望む場合に、いつ、どのようにして協議するかの決定は、加盟国に任されている。条約の起草者は、欧州犯罪問題委員会（CDPC）の権能を維持しつつ、欧州評議会の非構成諸国を含む全ての条約加盟国が（平等な立場で）全てのフォローアップ機能に関与することを確保するための何らかの手続が必要であると判断した。CDPC は、加盟国間で起こる協議に関して定期的に情報提供を受けることを維持するだけではなく、それを促進し、かつ、条約を補足または改正しようとする加盟国の努力について、加盟国を支援するために必要な措置をとらなければならない。サイバー犯罪の効果的な防止及び訴追の必要性と併せ、プライバシーと関係する課題、企業活動に対する潜在的な影響、その他の様々な要素に鑑み、法執行機関、非政府組織及び民間団体を含め[1]、利害関係者の見解は、これらの協議のために有益なものとなるであろう（第 14 項も参照）。

329. 第 3 項は、条約発効の 3 年後の条約の運用見直しについて規定している。その時点で、適切な改正が提案されることになるであろう。CDPC は、加盟国の補佐を受けてその見直しをしなければならない。

330. 第 4 項は、第 46 条第 1 項に従って行なわれる協議について、加盟国自身がその費用負担をすると欧州評議会が想定している場合には、除外となることを示している。しかしながら、欧州犯罪問題欧州委員会（CDPC）とは別に、欧州評議会の事務局は、条約に基づく加盟国の努力を支援しなければならない[2]。

[1] [訳注] 条約の存在それ自体に反対する見解もある。例えば、EFF は、その Web サイト上において、「Dangerous Cybercrime Treaty Pushes Surveillance and Secrecy Worldwide」 (2011 年 8 月 25 日)という声明を公表している。ACLU は、その Web サイト上において、「The Seven Reasons Why The Senate Should Reject The International Cybercrime Treaty」という見解を明らかにしている。

[2] [訳注] 説明書は、第 46 条で終わっている。第 47 条（廃棄）及び第 48 条（通知）に関する条文毎の注釈はない。

コンピュータと関連する犯罪に関する州評議会閣僚委員会勧告 No. R (89) 9

［参考訳］

2016 年 12 月 9 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Recommendation No. R (89) 9 of the Committee to Member States to Member States on computer-related crime のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Web サイトから入手した。

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094
[2016 年 12 月 9 日確認]

この勧告は、欧州評議会のサイバー犯罪条約（Convention on Cybercrime ETS No.185）の説明書（Explanatory Report）の中で触れられているもので、サイバー犯罪条約の起草の発端となった貴重な立法資料の 1 つである。

この参考訳は、あくまでも勧告の私的な和訳（全訳）である。訳出にあたっては、可能な限り直訳とすることに務めたが、部分的に意訳としたところもある。

この参考訳を作成するに際して、「サイバー犯罪条約（ETS No.185）の説明書 [参考訳]」本誌 1〜132 頁の冒頭に掲記の文献を参考にした。

＊＊＊

コンピュータと関連する犯罪に関する欧州評議会閣僚委員会勧告第 9 号（1989 年）

(第 428 回閣僚代理会合に際し 1989 年 9 月 13 日に閣僚委員会において採択)

閣僚委員会は、欧州評議会規程第 15 条 b の要件に基づき、
欧州評議会の目的がその構成国の間におけるより大きな統一を達成することにあることに鑑み；
コンピュータと関連する犯罪からの新たな挑戦に対して十分かつ迅速な対応をすることの重要性を再認識し；
コンピュータと関連する犯罪が国境を越える性質を有していることに鑑み；
法律及び実務の更なる整合性の確保並びに国際的な法的共同活動の促進の必要性という帰結に留意し、
以下のとおり、構成国の政府に対して勧告する：

1. 構成国の立法を見直す場合または新たな立法を検討する場合には、犯罪問題に関する欧州委員会によって起草されたコンピュータ犯罪に関する報告書及びとりわけ国内立法のためのガイドラインを考慮に入れること；
2. コンピュータ犯罪に関する立法、法務上の実務及び国際的な司法共助の経験についての構成国の発展に関して、1993 年中に、欧州評議会の理事長に対して、報告すること。

情報技術と関連する刑事手続法上の問題に関する欧州評議会閣僚委員会勧告

No. R (95) 13

［参考訳］

2016 年 12 月 9 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Recommendation No. R (95) 13 of the Committee of Minister to Member States concerning Problems of criminal procedural law connected with information technology のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Web サイトから入手した。

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76
[2016 年 12 月 9 日確認]

この勧告は、欧州評議会のサイバー犯罪条約（Convention on Cybercrime ETS No.185）の説明書（Explanatory Report）の中で触れられているもので、サイバー犯罪条約の起草の発端となった貴重な立法資料の 1 つである。

この参考訳は、あくまでも勧告の私的な和訳である。訳出にあたっては、可能な限り直訳とすることに務めたが、部分的に意訳としたところもある。

この勧告は、本文及び別紙（Appendix）によって構成されている。この参考訳では、本文及び別紙の全文を訳出した。

この参考訳を作成するに際して、「サイバー犯罪条約（ETS No.185）の説明書 [参考訳]」本誌 1～132 頁の冒頭に掲記の文献を参考にした。

一般に、日本国の刑事訴訟法及び関連法令の中にある電子的な証拠の確保に関する条項は、例えば、トラフィックデータの応急保全に関する条項のように、サイバー犯罪条約の批准に伴い必要になった部分が少なくない。しかし、直接の契機がそうであったとしても、基本的な沿革（立法史）としては、この勧告の別紙にあるガイドラインに沿って検討されてきたものとして認識・理解することが可能である。この点については、従来ほとんど研究がなされてこなかったので、刑事法史学上の調査・検討が更に深められなければならない。

＊＊＊

情報技術と関連する刑事手続法上の問題に関する欧州評議会閣僚委員会勧告

第 13 号（1995 年）

(第 543 回閣僚代理会合に際し 1995 年 9 月 11 日に閣僚委員会において採択)

閣僚委員会は、欧州評議会規程第 15 条 b の要件に基づき、
欧州評議会の目的がその構成国の間におけるより大きな統一を達成することにあることに鑑み；
現代社会の全ての分野にわたる情報技術の前例をみない発展とその応用を考慮し；
電子情報システムの開発が全てのタイプの通信及び関係にとって新たな空間を創り出すことによって、在社の社会を情報社会へと変化させる速度を上げることを実現し；
社会を構成するあり方に対して及び人間社会とその相互関係についてどのように情報社会が影響を及ぼすかについて留意し；
経済関係及び社会関係の発展が電子情報システムを介してまたはそれを用いることによって生ずることに注目し；
電子情報システム及び電子情報が犯罪行為の実行のためにも用いられ得るリスクについて配慮し；
犯罪行為の証拠がこれらのシステムによって記録保存され伝送されることを考慮し；
構成国の法律が、しばしば、その犯罪捜査の過程において、これらのシステムの中にある証拠を捜索し収集するための適切な権限をまだ提供していないことに注目し；
発展しつつある情報技術の開発に直面している捜査機関がその職務を適正に遂行する上で、適切な特別の権限を欠くことがその障害となっていることを考慮し；
電子情報システムの捜査における特別の性質を志向する刑事手続法に基づいて捜査機関に対して与えられる法的手段を導入すべき必要性を認識し；
構成国の領土内において電子情報システムから電子的な証拠を収集する必要がある場合において、構成国が適切な方法で司法共助をすることができないことによる潜在的なリスクを憂慮し；
この分野における国際的な共同活動を強化し、より大きな互換性を得る必要性を理解し；
書証の要件並びにコンピュータ上での文書の複製及び記録の許容性と関連する法令の整合性の確保に関する勧告第 20 号（1981 年）、通信の捜査のための必要文書に関する勧告第 10 号（1885 年）、警察分野における個人データの利用に関する勧告第 15 号（1987 年）、並びに、コンピュータと関連する犯罪に関する勧告第 9 号（1989 年）を想起し；
以下のとおり、構成国の政府に対して勧告する：

1. 国内立法及び実務を見直す場合には、この勧告の別紙に付加された原則に従うこと；及び、
2. 捜査機関及びその他の専門組織の間において、とりわけ情報技術の分野において、その適用について利害を有するかもしれない同原則の公開性を確保すること。

*情報技術と関連する刑事手続法上の問題に関する*勧告第 13 号（1995 年）の別紙

I. 捜索及び押収

1. コンピュータシステムの捜索、コンピュータシステムに記録保存されたデータの押収及び伝送の過程におけるデータの傍受の間の法的相違は、明確に区分され、適用されなければならない。
2. 刑事手続法は、従来の捜査及び押収の権限に基づくのと同様の条件に基づき、捜査機関がコンピュータシステムの捜索及びデータの押収をすることを認めるものとしなければならない。システムの管理担当者は、そのシステムが捜索されること及び押収されるデータの種類について通知受けるものとしなければならない。捜索及び押収に対して一般的に適用される司法救済は、コンピュータシステムの捜索及びその中にあるデータの押収の場合においても同様に適用されなければならない。
3. 捜索を実施している間、捜査機関は、適切な安全性確保措置に従い、その国内においてネットワークによって接続されている他のコンピュータシステムに対して捜索を拡大し、その中にあるデータを押収するための権限を有するものとしなければならない。ただし、迅速な行動を要する場合に限る。
4. 自動的に処理されるデータが機能的に在来の文書と同じである場合には、文書の捜索及び押収に関する刑事手続法の中の条項がデータについても同様に適用されなければならない。

II. 技術的な監視

5. 情報技術及び通信の収斂という観点から、通信の傍受のような犯罪捜査の目的のための技術的な監視を担う法律は、その適用を確保するために、必要に応じて、見直され、改正されなければならない。
6. 法律は、捜査機関が、犯罪の捜査においてトラフィックデータを収集することができるようにするために必要な全ての技術的手段を自ら使うことを許容しなければならない。
7. 犯罪捜査の過程で収集される場合、とりわけ、通信傍受により収集される場合には、法的な保護の対象とされ、コンピュータシステムによって処理されるデータは、適切な方法で防護されなければならない。
8. 通信もしくはコンピュータシステムの機密性、完全性及び可用性に対する重大な侵害行為の捜査において、通信の傍受及びトラフィックデータの収集をすることができるようにするという観点から、刑事手続法の見直しが行われなければならない。

III. 捜査機関との共同活動の義務

9. 法律上の特権及び保護に従い、ほとんどの法制度は、捜査機関が、個人に対し、当該の者が管理する物件について、証拠として提出することを命ずることを認めている。同様の様式

により、個人に対し、コンピュータシステムの中で当該の者が管理する特定のデータについて、捜査機関から求められる方式により、これを提出することを命ずる権限を定める条項を制定しなければならない。
10. 法律上の特権及び保護に従い、捜査機関は、当該の者の管理に基づきコンピュータの中でデータを保有する個人に対し、コンピュータシステム及びその中にあるデータに対してアクセスすることができるようにするために必要となる全ての情報を提出することを命ずる権限を有するものとしなければならない。刑事手続法は、コンピュータシステムの稼働またはその中にあるデータの防護のために適用される措置についての知識を有するその他の者に対し、同様の命令を発することができることを確保しなければならない。
11. 公衆に対して通信サービスを提供する公共ネットワーク及び民間ネットワークの運営者に対し、捜査機関による通信傍受を可能とするために必要となる全ての技術的措置を捜査機関が利用できるようにさせるための特別の義務が課されなければならない。
12. 公共ネットワークまたは民間ネットワークを介して公衆に対し通信サービスを提供するサービス提供者に対し、職務権限を有する捜査機関からそのようにすべきことを命じられたときは、その利用者を識別するための情報を提供させるための特別の義務が課されなければならない。

IV. 電子証拠

13. 国内における訴追及び国際的な共同活動の両方のために、その完全性及び真正性を否認することができないことを最善に確保し、かつ、それを反映するような方法で、電子的な証拠を収集し、保全し、かつ、提示すべき一般的な必要性があることが認識されなければならない。それゆえ、電子的な証拠を取扱うための手続及び技術的措置は、とりわけ構成国の間におけるその互換性を確保する方法によって、別に開発されなければならない。在来の文書に関連する証拠に関する刑事手続法上の条項は、コンピュータシステムの中に記録保存されているデータに対してのみ適用されなければならない。

V. 暗号の利用

14. 特別の必要性を超えて暗号の適法な利用に対して影響を与えることなく、犯罪行為の捜査上において、暗号の利用による悪影響をミニマムなものとするための措置が検討されなければならない。

VI. 調査、統計及び訓練

15. 犯罪行為の実行と関連する情報技術の開発及び適用に含まれているリスクは、持続的なものであると推測されなければならない。職務権限を有する機関がコンピュータと関連する犯罪の領域における新たな現象に後れをとらない状態を維持し、かつ、適切な対抗措置を開発するためには、その運用方法（*modus operandi*）及び技術的な側面を含め、それらの犯罪

行為に関するデータの収集及び解析を促進しなければならない。
16. 侵害行為の捜査のための専門的なユニットの設置、情報技術における特別な専門性が求められる闘いが検討されなければならない。刑事司法担当者がこの分野における専門性を自ら用いることができるようにするための訓練計画を促進しなければならない。

VII. 国際的な協力活動

17. 他のコンピュータシステムに対して捜索を拡大する権限は、そのシステムが外国に所在する場合においても適用されなければならない。ただし、迅速な行動が求められる場合に限る。国家主権または国際法の違反が生ずるような事態を避けるため、そのような捜索及び押収の拡大については明確な法的根拠が設けられなければならない。それゆえ、どのようにして、いつ、及び何についてそのような捜索及び押収の拡大が認められるかに関し、国際的な合意形成のための交渉をすべき緊急の必要性がある。
18. 捜査機関が外国の捜査機関に対して証拠の収集を進めることを求めるためには、望ましくかつ適切な手続及び連絡制度を利用することができなければならない。その目的のために、要請を受けた機関は、その後にデータを伝送するという観点から、コンピュータシステムを捜索し、データを押収することが認められなければならない。要請を受けた機関は、また、特定の通信と関連するトラフィックデータを提供し、特定の通信を傍受し、または、その発信地を特定することが認められなければならない。この目的のために、既存の司法共助文書は、補足されなければならない。

警察分野における個人データの利用に関する勧告 No. R (87) 15

[参考訳]

2016 年 12 月 11 日
明治大学法学部教授
夏　井　高　人

＊＊＊

Recommendation No. R (87) 15 regulating the use of personal data in the police sector のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Web サイトから入手した。

https://www.privacycommission.be/sites/privacycommission/files/documents/recommendation_87_15.pdf
[2016 年 12 月 10 日確認]

この勧告は、情報技術と関連する刑事手続法上の問題に関する欧州評議会閣僚委員会勧告 No. R (95) 13 の中で触れられているものである。

この参考訳は、あくまでも勧告の私的な和訳である。訳出にあたっては、可能な限り直訳とすることに務めたが、部分的に意訳としたところもある。

この勧告は、前文及び別紙（Appendix）によって構成されている。別紙には、目的条項及び定義条項に続けて、8 つの基本原則が規定されている。この参考訳では、前文及び別紙の全文を訳出した。

原文には脚注がある。訳注を付した部分には、原注と識別できるようにするため[訳注]と記載した。

この参考訳を作成するに際して、「サイバー犯罪条約（ETS No.185）の説明書 [参考訳]」本誌 1～132 頁の冒頭に掲記の文献及び法と情報雑誌 1 巻 3 号ないし 1 巻 5 号所収の参考訳の冒頭に掲記の文献を参考にした。

＊＊＊

警察分野における個人データの利用に関する勧告第 15 号（1987 年）

(第 410 回閣僚代理会合に際し 1987 年 9 月 17 日に閣僚委員会において採択)[1]

閣僚委員会は、欧州評議会規程第 15 条 b の要件に基づき、
欧州評議会の目的がその構成国の間におけるより大きな統一を達成することにあることに鑑み；
警察部門において個人データの自動的な処理の利用の増加、並びに、この分野におけるコンピュータ及びその他の技術的な手段の利用によって得ることのできる利益に留意し；
個人のプライバシーに対して自動的な処理方法の濫用により生じ得る脅威についての懸念を考慮に入れ；
一方における犯罪行為の防止及び抑止という社会的な利益並びに公共の秩序と他方における個人の利益並びに彼または彼女のプライバシーの権利とのバランスの必要性を認識し；
個人データの自動処理と関連する個人の保護のための 1981 年 1 月 28 日の条約[2]の条項、とりわけ、第 9 条に基づく特例を念頭に置き；
欧州人権条約の第 8 条の規定にも留意し；
以下のとおり、構成国の政府に対して勧告する：

この勧告に付加された基本原則によって、構成国の自国の法律及び実務を導くこと；及び、
この勧告に付加された条項について、及び、とりわけ、個人に与えられる権利の適用について、その公表を確保すること。

[1] この条約が採択された際：
－閣僚代理会合手続規則の第 10 条の 2c に従い、アイルランドの代表は、その政府が勧告に従うか否かの権利を留保し、英国の代表は、その政府が勧告の原則 2.2 及び原則 2.4 に従うか否かの権利を留保し、ドイツ連邦共和国の代表者は、その政府が勧告の原則 2.1 に従うか否かの権利を留保し；
－閣僚代理会合手続規則の第 10 条の 2d に従い、スイスの代表は、その政府が勧告に従うか否かの権利を留保すると述べることを差し控え、これを差し控えることは、勧告全体について不同意であることを表示するものとして理解してはならないと述べた。

[2] [訳注] 欧州評議会個人データ保護条約と略称される。この条約の参考訳は、法と情報雑誌 1 巻 4 号 1～20 頁にある。

勧告第 15 号（1987 年）の別紙

適用範囲及び定義

この勧告に含まれている基本原則は、自動的な処理の対象である個人データを、警察の目的のために収集し、記録保存し、利用し、及び、送信することに対して適用される。

この勧告の目的のために、「個人データ」という表現は、識別される個人または識別可能な個人に関連する全ての情報に適用される。個人は、識別のために不合理な分量の時間、費用及び労力を要する場合[1]には、「識別可能」とはみなされない。

「警察の目的のために」という表現は、警察機関が犯罪行為の防止及び抑止並びに公共の秩序の維持のために遂行しなければならない全ての職務について適用される。

「責任のある組織」（ファイルの管理者）という表現は、自動的なファイルの目的、記録保存されなければならない個人データの類型、並びに、それらに対して適用されるべき業務について、自国の法律に従って決定する職務権限を有する行政機関、役務提供組織[2]、または、その他の公的組織のことを指す。

構成国は、現在遂行されていない個人データの自動的な処理に対して、この勧告に含まれている基本原則の適用を拡張することができる[3]。

その目的がこの勧告の条項を回避するためである場合には、データの手作業による処理とならない[4]。

構成国は、当該組織が法人であるか否かを問わず、個人の集団、財団、会社、組合、または、直接もしくは間接に個人によって構成されるその他の組織に対して、この勧告に含まれる基本原則の適用を拡張することができる[5]。

この勧告の条項は、それが適切であるときは、国防の目的のために個人データを収集、記録保存及び利用に対して、これらの基本原則中の幾つかのものを構成国が拡張して適用する

---

[1] [訳注] これは、相対的な表現である。例えば、かつては世界で最も高性能なコンピュータによっても解読に時間を要するように暗号化された個人データであっても、現在の普通の PC を用いて簡単に解読できてしまい、その解読結果に基づいて個人を識別することが可能となってしまうことがある。

[2] [訳注] 原文は、「service」となっている。文脈から、一定の役務の提供を目的とする国営企業、公企業または行政組織のことを指し、民間企業を含まないものと解される。

[3] [訳注] 反対解釈として、この勧告は、現在遂行されている個人データの自動処理に対してのみ適用されることになる。構成国は、現在遂行されていない処理であっても、将来遂行されるかもしれない処理に対して勧告の適用を拡張することができる。

[4] [訳注] 勧告の適用を潜脱する目的で手作業による処理をする場合、現実に手作業によって処理されているとしても、その処理は、個人データの自動的な処理であるとみなされ、この勧告の適用を受けるという趣旨である。

[5] [訳注] 反対解釈として、この勧告は、自然人の個人データの処理に対してのみ適用されることになる。構成国は、複数の自然人によって構成される組織と関連する個人データのみならず、自然人ではない法人と関連する個人データであっても、勧告の適用を拡張することができる。

ことができることを制限し、または、その他の悪影響を及ぼすものとして解釈してはならない[1]。

基本原則

原則 1－管理及び通知

1.1. 各構成国は、警察分野の外にあって、この勧告に含まれる基本原則に対する尊重を確保することに責任を有する独立の監督官をもたなければならない[2]。
1.2. データ処理のための新たな技術的手段は、既存のデータ保護立法の精神と適合するその利用を確保するための全ての合理的な措置が講じられている場合においてのみ[3]、これを導入することができる。
1.3. 責任のある組織は、自動的な処理方法を導入することがこの勧告の適用に関して疑問を生じさせる場合には、積極的に、監督官と協議しなければならない[4]。
1.4. 永久保存の自動化されたファイル[5]は、監督官に対して通知されなければならない。通知は、宣言されている個々のファイルの性質、その処理について責任を有する組織、その処理の目的、ファイルに含まれているデータの種別、データが送信される者を特定するものとしなければならない[6]。

---

[1] [訳注] 反対解釈として、この勧告は、警察組織による個人データの処理に対してのみ適用されることになる。しかし、各国の法制の相違により、警察組織の一部が軍または諜報機関と同一の組織であることがあり、また、武装警察として警察組織の一種とされている組織が国防の目的のために行動することから当該組織が実質的には警察組織ではなく軍の一種であるとみなされるような場合もある。このような場合には、警察組織ではない組織に対しても勧告に定める基本原則を適用すべき場合が出てくることになる。構成国は、軍または諜報機関に該当する組織による個人データの処理に対しても勧告の適用を拡張することができる。

[2] [訳注] 欧州評議会個人データ保護条約の追加議定書（ETS No.181）は、独立の監督官（independent supervisory authority）について定めている。この追加議定書の参考訳は、法と情報雑誌 1 巻 4 号 21～25 頁にある。

[3] [訳注] 導入の際の制度設計の一部として（by design）、安全性確保措置（safeguards）を具備すべき旨を定めるものと解される。データ保護影響評価（data protection impact assessment）の趣旨を含むものとも解される。一般個人データ保護規則(EU) 2016/679 の第 25 条及び第 35 条に同旨の条項がある。

[4] [訳注] 事前協議（prior consultation）の必要性について定めるものと解される。一般個人データ保護規則(EU) 2016/679 の第 31 条及び第 36 条に同旨の条項がある。

[5] [訳注] 原文は、「Permanent automated files」となっている。犯歴データベース等がその典型例ではないかと解される。被疑者を自動的に推定するためのプロファイリングに用いられるファイルも同様である。そのようなファイルについて、一般個人データ保護規則(EU) 2016/679 の第 10 条は、法務当局の管理に基づく場合に限り、これを保存することができる旨を定めている。日本国においては、そのようなデータベースの処理・管理について個人情報保護委員会が関与する根拠法令が存在しない。

[6] [訳注] サイバー犯罪条約第 17 条、第 30 条、第 32 条ないし第 34 条に基づく国内の捜査機関及び外国の捜査機関に対するデータの開示（送信）についても適用があるものと解される。しかし、警察における実際の運用状況は不明である。

特別の捜査[1]の際に設定された限定的なファイル[2]は、国内法によって定められる条件に従って、これらのファイルの特別な性質を考慮に入れた上で、または、国内法に従い、監督官に対して通知されなければならない。

原則 2－データの収集

2.1. 警察の目的のための個人データの収集は、現実の被害発生の防止または特定の犯罪行為の抑止のために必要となるような場合に限定されなければならない[3]。この規定の例外は、特別の国内立法によるものとしなければならない。
2.2. 個人に関するデータが、彼が知らない間に収集され、記録保存された場合には、そのデータが削除されていない限り、実際には、警察活動の目的に支障がなくなった後には速やかに、彼に関する情報を保有していることについて、彼に対して通知がなされなければならな

---

[1] [訳注] 原文は、「particular inquiry」となっている。確実ではないが、関係各国の警察当局や諜報機関等と連携して実施されるテロ活動及びテロリストの捜査やそのための特別の情報共有のような場合を指すものではないかと思われる。このような観点からは、「特別の照会」ではなく「特別の捜査」のほうがより正確な訳語であるということになる。この勧告第 15 号は、捜査機関（警察）の活動と関連する個人データの保護に関するものであるので（6.1 参照）、この参考訳では「特別の捜査」と訳すことにした。一般的には、「inquiry and investigation」をまとめて「捜査」と訳す例もある。しかし、例えば、独占禁止法違反の行為の疑いがある場合に、行政措置を発動するための前提として「particular inquiry」が行われることがあり、この場合には、「特別の調査」との訳語が適切である。また、EU の近時のデータ保護法令等の中では、異なる様々な類型に属する行政機関等が実施することのできる措置として「particular inquiry」が用いられていることがある。例えば、一般個人データ保護規則(EU) 2016/679 の前文第 31 項は、第 4 条の(9)に「欧州連合または構成国の法律に従って特別の調査の枠組み内で個人データを取得することができる行政機関は、取得者とはみなされない」とあることの説明として、「その職務権限の行使のために法的義務に従って個人データの開示を受ける行政機関、例えば、証券市場の規制及び監視についての職務を有する税務署及び税関、金融情報機関、公正取引委員会または金融監視機構は、欧州連合法または構成国の法律に従い、一般的な利益にかかわる要求を遂行ために必要なものとして個人データを受領した場合には、個人データの取得者とはみなされない」と述べている。そのような場合には「特別の捜査」との訳語では不適切である。この「particular inquiry」の意義については、更に調査・検討を進めることとしたい。いずれにしても、通常の犯罪捜査の場合を含まないことは、文脈から明らかである。

[2] [訳注] 原文は、「*ad hoc* file」となっている。通常の犯罪捜査と関連するデータを記録する個々のファイル（データベース）は、これに該当するものと解される。しかし、現在のようなクラウド環境では、外見上では「ad hoc」のように見えても、実際には「permanent」に記録保存されることがあることに留意しなければならない。

[3] [訳注] データ保持指令 2002/58/EC に基づくデータの保持（retention）は、明らかに、この原則と矛盾するものと思われる。ただし、国内法によって例外を設けることができることになっているので、そのような例外が欧州連合の基本的な価値に反しないと解される限り、この条項は、無効とはならないはずである。しかし、データ保持指令を無効であると判断した欧州司法裁判所の先決裁定の趣旨からすれば、この条項中の国内法によって例外を定めることができるとする部分は無効になるものとして解すべきではないかと思われる。なお、データ保持指令 2006/24/EC の参考訳は、法と情報雑誌 1 巻 5 号 47～65 頁にある。

い。
2.3. 技術的な監視その他の自動的な手段によるデータの収集[1]は、特別の条項の中で定められなければならない。
2.4. 特別の人種的な出自、特別の宗教的信条、性的行動もしくは政治的意見または法律によって禁止されていない特別の活動もしくは組織への参加のみに基づいて、個人に関するデータを収集することは、禁止されなければならない[2]。これらの要素に関するデータの収集は、特別の捜査の目的のために必須である場合においてのみ、これを行うことができる。

原則 3－データの記録保存

3.1. 警察の目的のための個人データの記録保存は、可能な限り、正確なデータに限定され、並びに、国内法の枠組み及び国際法から生ずる捜査機関の義務の範囲内で捜査機関がその正当な職務を遂行するために必要となるようなデータに限定されなければならない[3]。
3.2. 異なる類型に属する記録保存されたデータは、可能な限り、その正確性または信頼性の程度に応じて、区別しなければならない。とりわけ、事実に基づくデータは、意見や個人評価に基づくデータと区別しなければならない[4]。
3.3. 行政の目的のために収集されたデータが永久保存のものとして記録保存されるべき場合には、分離したファイルの中に記録保存しなければならない。いずれの場合においても、行政のデータに対して警察のデータに適用可能な法令の適用対象となることがないようにする措置が講じられなければならない[5]。

---

[1] [訳注] 監視カメラ（CCTV）による監視等が含まれる。
[2] [訳注] 欧州連合基本権憲章第 21 条第 1 項は、「性、人種、皮膚の色、民族的もしくは社会的な出自、遺伝子上の特性、言語、宗教もしくは信条、政治的意見その他の意見、少数民族の一員であること、財産、出生、身体障害、年齢または性的嗜好に基づく差別は禁止される」と規定している。そして、一般個人データ保護規則(EU) 2016/679 の第 9 条第 1 項は、「民族的もしくは社会的な出自、政治的意見、宗教上もしくは思想上の信条または労働組合への加入を明らかにする個人データの処理、並びに、遺伝子データ、自然人をユニークに識別することを目的とする生体データ 、及び、自然人の健康または性生活もしくは性的傾向性に関するデータの処理は、禁止される」と規定している。
[3] [訳注] いわゆる「マスサーベイランス（mass severance）を禁止する趣旨と解される。ただし、現実は異なる。
[4] [訳注] 同一の電子的な文書の中に事実について記述・記録する部分と誰かの意見や評価を記述する部分とが混在することがしばしばある。このような事実と評価が混在している文書も個人データの一種となるが、そのような場合には当該文書を分割して管理することが妥当ではないことが多い。それゆえ、「可能な限り」との限定が付されているものと思われる。
[5] [訳注] 警察組織は、一般に、行政組織の一種である。それゆえ、広義では、警察組織が収集したデータは行政機関として収集したデータであることになる。しかも、警察組織は、行政機関の一種である以上、犯罪捜査以外の行政活動（一般的な広報活動や防災活動等）も行うのが通例である。しかし、ここでは、警察権の行使として犯罪捜査の目的で収集するデータとそれ以外の一般行政目的で収集するデータとを区別して保存すべきことを述べているものと解される。

原則 4－警察によるデータの利用

4. 原則 5 に従い、警察の目的のために警察によって収集及び記録保存された個人データは、その目的のためにのみ利用されなければならない[1]。

原則 5－データの送信

5.1. *警察部門内での送信*

警察の目的で用いられるデータの警察組織間での送信は、それらの組織の法的権限の枠組み内において当該送信をするための正当な利益が存在する場合にのみ、許容されるものとしなければならない。

5.2.i. *他の公的組織に対する送信*

他の公的組織に対するデータの送信は、特定の事件において、以下のいずれかの場合であるときに限り、許容されるものとしなければならない：

a. 法律上の明確な義務もしくは承認がある場合、または、監督官の承認を得ている場合；または、

b. 取得者にとって彼自身の法律上の職務を彼が遂行することができるようにするためにそのデータが不可欠のものであり、かつ、取得者により行われる収集または処理の目的が当初の処理の目的と適合しないわけではなく、かつ、送信する組織の法律上の義務がこれと矛盾しない場合。

5.2.ii. 更に、他の公的組織に対する送信は、特定の事件において、以下のいずれかの場合であるときに限り、例外的に許容されるものとしなければならない：

a. 送信が疑う余地なくデータ主体の利益となるものであり、かつ、データ主体が同意をした場合、または、そのような同意をしたものと明確に推定することのできるような状況にある場合[2]；または、

b. 重大かつ差し迫った危険を防止するために送信が必要となる場合。

5.3.i. *民間の当事者に対する送信*

民間の当事者に対する送信は、特定の事件において、法律上の明確な義務もしくは承認がある場合、または、監督官の承認を得ている場合に限り、許容されるものとしなければならない。

5.3.ii. 民間の当事者に対する送信は、特定の事件において、以下のいずれかの場合であるときに限り、許容されるものとしなければならない：

---

[1] [訳注] 警察の目的を国内の行政警察のみに限定することができる場合には比較的明瞭な条項であると言える。しかしながら、現在では、例えば、NIS 指令(EU) 2016/1148 やサイバー犯罪条約（ETS No.185）にもみられるとおり、各国の警察相互の連携から発展して、テロ対策や国防の目的で軍や諜報機関等とも連携して職務を遂行すべき場面が増えてきていることから、その区分が曖昧になってきていることに留意しなければならない。なお、NIS 指令(EU) 2016/1148 の参考訳は、法と情報雑誌 1 巻 2 号 34～73 頁にある。

[2] [訳注] いわゆる推定的同意の場合を指すものと解される。

a. 送信が疑う余地なくデータ主体の利益となるものであり、かつ、データ主体が同意をした場合、または、そのような同意をしたものと明確に推定することのできるような状況にある場合；または、

b. 重大かつ差し迫った危険を防止するために送信が必要となる場合。

5.4. *国際的な送信*

外国の機関に対するデータの送信は、警察組織に限定されなければならない。以下の場合においてのみ、許容されるものとしなければならない：

a. 国内法または国際法に基づく明確な法律条項が存在する場合において、

b. そのような条項が存在しない場合には、重大かつ差し迫った危険を防止するために送信が必要となる場合であるか、または、通常の法律に基づく重大な犯罪行為の抑止のために必要となる場合であり、かつ、

個人の保護のための自国の法令を妨げない場合に限る。

5.5.i. *送信の要請*

国内法または国際的な合意に含まれる特別の条項に従い、データの送信の要請は、それを要請している組織または個人に関する識別並びにその要請の理由及びその目的を提供するものでなければならない。

5.5.ii. *送信の条件*

データの品質は、可能な限り、遅くとも、その送信の時点で検証されなければならない。データの全ての送信において、可能な限り、起訴の有無に関する法務当局の判断が示されなければならず、かつ、送信が行われ、その正確性及び信頼性の程度が示される前に、意見または個人の評価に基づくデータの根拠を確認しなければならない。

5.5.iii. *送信の安全性確保措置*

他の公的組織、民間の当事者及び外国の機関に対するデータの送信は、送信を求める要請に指定されている目的以外の目的のために用いてはならない[1]。

他の目的のためのデータの利用は、この原則の 5.2 ないし 5.4 を妨げることなく、送信をする組織の同意に基づくものとしなければならない[2]。

5.6. *ファイルの相互接続及びファイルに対するオンラインアクセス*

異なる目的のために保有されているファイルとファイルの相互接続は、以下のいずれかの条件に従う：

a. 特定の侵害行為の捜査の目的のための監督官による承認の付与；または、

b. 明確な法律条項の遵守。

ファイルの直接的なオンラインのアクセスは、この勧告の原則 3 ないし原則 6 を考慮に入れた国内立法に従っている場合にのみ、許容されるものとしなければならない。

原則 6ー公開性、警察のファイルに対するアクセスの権利、訂正の権利及び不服申立の権利

6.1. 監督官は、通知の対象となるファイルについて及びそのファイルに関する公衆の権利に

[1] [訳注] 目的外利用の禁止を定める趣旨と解される。

[2] [訳注] 管理者の同意に基づく場合以外の利用の禁止を定める趣旨と解される。

ついて、公衆が情報提供を受けることを充足するための措置を講じなければならない。この原則の実装は、限定的なファイルの特別な性質、とりわけ、警察組織の法律上の職務の遂行に対する重大な支障を避けるべき必要性を考慮に入れて行うものとしなければならない。

6.2. データ主体は、合理的な期間内に、過剰な遅滞なく、国内法に定める方式に従い、警察のファイルへのアクセスを得ることができるものとしなければならない。

6.3. データ主体は、それが適切であるときは、ファイルの中に含まれている彼のデータの訂正を得ることができるものとしなければならない。

アクセスの権利の行使により不正確であることが明らかとなったデータ、または、この勧告に含まれる他の原則のいずれかの適用との関係で過剰であり、不正確であり、もしくは、関連性のないものであることが判明したデータは、削除され、訂正され、または、ファイルに訂正文言を付加されるものとしなければならない。

そのような削除または訂正の措置は、可能な限り、警察のファイルに付随する全ての文書に対して拡張されるものとしなければならず、それを即時に実施することができない場合には、遅くとも、次のデータ処理の際に、または、次のデータの送信の際に、実施されなければならない。

6.4. アクセスの権利、訂正の権利及び削除の権利の行使は、警察の法律上の職務の遂行のために制限が不可欠のものである場合、データ主体の保護のために制限が必要な場合、または、他の者の権利及び自由の保護のために制限が必要な場合に限り、制限されるものとしなければならない。

データ主体の利益になる場合、書面による告知は、特定の事件について、法律によって排除され得る[1]。

6.5. これらの権利の拒否または制限は、書面でその理由を告げるものとしなければならない。警察の法律上の職務の遂行のために不可欠のものである場合、または、他の者の権利及び自由の保護のために必要な場合に限り、その理由の通知を拒むことができる。

6.6. アクセスが拒絶された場合には、データ主体は、監督官に対し、または、拒否が十分に根拠あるものであることの充足性を判断することのできる他の独立の組織[2]に対して不服を申し立てることができるものとしなければならない。

原則 7－記録保存の期間及びデータの更新

7.1. それが記録保存された目的のための必要がなくなったときは、警察の目的のために保存された個人データを消去する措置が講じられなければならない[3]。

この目的のために、以下の分野について、特に配慮がなされなければならない。すなわち、ある特定の事件を捜査した結果を考慮に入れた上でのデータを保存すべき必要性；確定判決、

[1] [訳注] 権利の行使に対する制限は、口頭でなされれば足りるとの趣旨と解される。

[2] [訳注] 不服の当否を判定することのできる組織を意味すると解されるが、明確ではない。裁判所のような独立の国家機関のことを指すものではないかと思われる。この部分は、意訳した。

[3] [訳注] クラウド環境においては、物理的に完全に消去されたことを確認することが非常に困難である場合があることに留意しなければならない。

特に無罪判決[1]；社会復帰；拘禁された期間；恩赦；データ主体の年齢；データの特別の類型である。

7.2. 監督官との合意に基づき、または、国内法に従い、異なる類型に属する個人データの保存期間を定めることを目的とする規則、並びに、データの品質の定期的な点検[2]が設けられなければならない。

原則 8－データの安全性

8. 責任のある組織は、データの適切な物理的及び論理的な安全性を確保するために必要となる全ての措置を講じなければならず、かつ、無権限のアクセス、送信または改変を防止しなければならない。

この目的のために、ファイルの性質及び内容の相違を考慮に入れなければならない。

[1] [訳注] 関連する裁判例については、末井誠史「DNA 型データベースをめぐる論点」レファレンス平成 23 年 3 月号が参考になる。

[2] [訳注] ここでいうデータの「品質（quality）」とは、データの完全性（integrity）のことを意味する。